kaspersky

Kaspersky Security Center 14 Linux

目次

Kaspersky Security Center 14 Linux のヘルプ

	**新機能** 最新の製品リリースの新機能を確認できます。		**カスペルスキー製品：ライセンスとアクティベーション** カスペルスキー製品を数ステップでアクティベートする方法を確認できます。
	**システム要件** サポート対象のオペレーティングシステムとアプリケーションのバージョンを確認できます。		**ネットワーク保護の設定** 組織のセキュリティを管理する方法を確認できます。
	**インストール** 管理サーバーと Kaspersky Security Center 14 Web コンソールをインストールします。		**カスペルスキー製品：定義データベースとソフトウェアモジュールのアップデート** 保護システムの信頼性を維持する方法を確認できます。
	**ネットワーク接続されたデバイスの検出** 組織ネットワーク上の既存デバイスと新規デバイスの検出方法について説明しています。		**監視とレポート** インフラストラクチャの状況、保護ステータス、統計情報の確認方法について説明しています。
	**カスペルスキー製品：一元管理による導入** カスペルスキー製品の導入		**ディストリビューションポイントと接続ゲートウェイの調整** ディストリビューションポイントの設定方法を説明しています。

新機能

Kaspersky Security Center 14 Linux

Kaspersky Security Center 14 Linux にはいくつかの新機能と機能強化が追加されています：

- ［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクに加え、［*ディストリビューションポイントのリポジトリにアップデートをダウンロード*］タスクを使用することでもカスペルスキーのセキュリティ製品の定義データベースをダウンロードできるようになりました。

- 管理対象デバイスの定義データベースと製品モジュールは、管理サーバーまたはディストリビューションポイントから反映およびアップデートが可能です。組織に最適なアップデートスキームを選択することで、管理サーバーの負荷を軽減して企業ネットワークのデータトラフィックを最適化することができます。

- カスペルスキーのセキュリティ製品からアップデートの要求があったときのみ、Kaspersky Security Center はカスペルスキーのアップデートサーバーからダウンロードします。これによりダウンロードされるデータのサイズを抑えることができます。

- 定義データベースおよびソフトウェアモジュールのダウンロードに差分ファイルのダウンロード機能を使用することができるようになりました。差分ファイルには、定義データベースファイルまたはソフトウェアモジュールファイルの異なる 2 バージョン間の変更点のみが含まれています。完全な定義データベースファイルまたはソフトウェアモジュールファイルよりも差分ファイルの方が容量が小さいため、差分ファイルを使用することで社内ネットワークのトラフィック量を軽減できます。

- *アップデートの検証*タスクが追加されました。このタスクを使用すると、管理対象デバイスにアップデートを実際にインストールする前に、ダウンロードされたアップデートの操作性やエラーを自動的に検証することができます。

- Kaspersky Security Center が Kaspersky Industrial CyberSecurity for Linux Nodes 1.3 をサポートするようになりました。

Kaspersky Security Center Linux について

このセクションでは、Kaspersky Security Center Linux の目的、主な機能と構成要素、および Kaspersky Security Center Linux の購入方法について説明します。

Kaspersky Security Center Linux（「Kaspersky Security Center」とも表記）を使用して、Linux® 環境の要件を満たす Linux ベースの管理サーバーを使用した Linux デバイスの保護機能を導入および管理できます。

Kaspersky Security Center Linux を使用して、カスペルスキーのセキュリティ製品を企業ネットワーク内にあるデバイスにインストールして、リモートからスキャンやアップデートタスクを実行したり、管理対象デバイスのセキュリティポリシーを管理したりできます。管理者として、企業デバイスのステータスのスナップショット、詳細なレポート、保護ポリシーの詳細な設定などを表示するダッシュボードを使用できます。

Windows® ベースの管理サーバーを持つ Kaspersky Security Center と、Kaspersky Security Center Linux とは機能セットが異なります。

Kaspersky Security Center Linux は、組織内でデバイスの保護を担当する企業ネットワーク管理者および従業員を対象としています。

Kaspersky Security Center を使用して、次のことが実現できます：

- 管理サーバーの階層を作成して、組織内、リモートオフィス内、クライアント組織内のネットワークを管理する。

  *クライアント組織*とは、サービスプロバイダーからアンチウイルスによる保護の提供を受ける組織です。

- 管理グループの階層を作成して、いくつかのクライアントデバイスを1つの単位として管理する。
- カスペルスキー製品をベースに構築されたアンチウイルスによる保護システムを管理する。
- カスペルスキーまたはその他のソフトウェアベンダーの製品のリモートインストールを実行する。
- カスペルスキー製品のライセンスをクライアントデバイスへ一元的に配信し、使用状況を監視したり、ライセンスを更新したりする。
- アプリケーションやデバイスの動作に関する統計情報とレポートを受信する。
- カスペルスキー製品の動作中に発生した緊急イベントに関する通知を受信する。
- 組織のネットワークに接続されたハードウェアのインベントリを作成する。

セキュリティ製品によって隔離またはバックアップに移動されたファイルを一元管理し、セキュリティ製品による処理が延期されたファイルを管理します。Kaspersky Security Center Linux は、カスペルスキー（たとえば、https://www.kaspersky.co.jp）またはパートナー企業を通じて購入できます。

カスペルスキーから Kaspersky Security Center Linux を購入した場合は、当社のウェブサイトからアプリケーションをコピーすることができます。アプリケーションのアクティベーションに必要な情報は、支払い手続き完了後にメールで送信されます。

システム要件

管理サーバー

ハードウェアの最小要件

- CPU：動作周波数が 1 GHz 以上（64 ビット OS の場合、最小周波数は 1.4 GHz）
- メモリ：4 GB
- 使用可能なディスク容量：10 GB

次のオペレーティングシステムがサポートされています：

- Debian GNU/Linux 11.x（Bullseye）32 ビット / 64 ビット
- Debian GNU / Linux 10.x（Buster）32 ビット / 64 ビット
- Debian GNU / Linux 9.x（Stretch）32 ビット / 64 ビット
- Ubuntu Server 20.04 LTS（Focal Fossa）64 ビット
- Ubuntu Server 18.04 LTS（Bionic Beaver）64 ビット
- CentOS 7.x 64 ビット
- Red Hat Enterprise Linux Server 8.x 64 ビット
- Red Hat Enterprise Linux Server 7.x 64 ビット
- SUSE Linux Enterprise Server 12（すべての Service Pack）64 ビット
- SUSE Linux Enterprise Server 15（すべての Service Pack）64 ビット
- Astra Linux Special Edition（Orel、Voronezh、Smolensk）1.7（閉鎖ソフトウェア環境モードおよび強制モードを含む）64 ビット
- Astra Linux Special Edition 1.6（閉鎖ソフトウェア環境モードおよび強制モードを含む）64 ビット
- Astra Linux Common Edition 2.12 64 ビット
- ALT Server 10 64 ビット
- ALT Server 9.2 64 ビット
- ALT 8 SP Server（LKNV.11100-01）64 ビット
- ALT 8 SP Server（LKNV.11100-02）64 ビット
- ALT 8 SP Server（LKNV.11100-03）64 ビット
- Oracle Linux 7 64 ビット
- Oracle Linux 8 64 ビット
- RED OS 7.3 Server 64 ビット
- RED OS 7.3 Certified Edition 64 ビット

次の仮想化プラットフォームがサポートされています：

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware Workstation 16 Pro
- Microsoft Hyper-V Server 2012 64 ビット
- Microsoft Hyper-V Server 2012 R2 64 ビット
- Microsoft Hyper-V Server 2016 64 ビット
- Microsoft Hyper-V Server 2019 64 ビット
- Microsoft Hyper-V Server 2022 64 ビット
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Parallels Desktop 17
- カーネルベースの仮想マシン次のオペレーティングシステムをサポート：
  - ALT 8 SP Server（LKNV.11100-01）64 ビット
  - ALT Server 10 64 ビット
  - Astra Linux Special Edition（Orel、Voronezh、Smolensk）1.7（閉鎖ソフトウェア環境モードおよび強制モードを含む）64 ビット
  - Debian GNU/Linux 11.x（Bullseye）32 ビット / 64 ビット
  - Ubuntu Server 20.04 LTS（Focal Fossa）64 ビット
  - RED OS 7.3 Server 64 ビット
  - RED OS 7.3 Certified Edition 64 ビット

以下のデータベースサーバーがサポートされます（異なるデバイスにインストール可能）：

- MySQL 5.7 Community 32 ビット / 64 ビット
- MySQL 8.0 32 ビット / 64 ビット
- MariaDB 10.5.x 32 ビット / 64 ビット
- MariaDB 10.4.x 32 ビット / 64 ビット
- MariaDB 10.3（ビルド 10.3.22 以降）32 ビット / 64 ビット
- MariaDB 10.3 32 ビット / 64 ビット（InnoDB ストレージエンジンを使用）
- MariaDB Galera Cluster 10.3 32 ビット / 64 ビット（InnoDB ストレージエンジンを使用）
- MariaDB 10.1（ビルド 10.1.30 以降）32 ビット / 64 ビット

Kaspersky Security Center 14 Web コンソール

Kaspersky Security Center 14 Web コンソールサーバー

ハードウェアの最小要件

- CPU：4 コア、動作周波数が 2.5 GHz
- メモリ：8 GB
- 使用可能なディスク容量：40 GB

次のいずれかのオペレーティングシステム（64 ビット版のみ）：

- Debian GNU/Linux 11.x （Bullseye）
- Debian GNU / Linux 10.x（Buster）
- Debian GNU / Linux 9.x（Stretch）
- Ubuntu Server 20.04 LTS（Focal Fossa）
- Ubuntu Server 18.04 LTS（Bionic Beaver）
- CentOS 7.x
- Red Hat Enterprise Linux Server 8.x
- Red Hat Enterprise Linux Server 7.x
- SUSE Linux Enterprise Server 12（すべての Service Pack）
- SUSE Linux Enterprise Server 15（すべての Service Pack）
- SUSE Linux Enterprise Desktop 15（Service Pack 3）ARM 64 ビット
- EulerOS 2.0 SP8 ARM
- Astra Linux Special Edition（Orel, Voronezh, Smolensk）1.7（閉鎖ソフトウェア環境モードおよび強制モードを含む）
- Astra Linux Special Edition 1.6（閉鎖ソフトウェア環境モードおよび強制モードを含む)
- Astra Linux Common Edition 2.12
- ALT Server 10
- ALT Server 9.2
- ALT 8 SP Server（LKNV.11100-01）
- ALT 8 SP Server（LKNV.11100-02）
- ALT 8 SP Server（LKNV.11100-03）

- Oracle Linux 8
- Oracle Linux 7
- RED OS 7.3 Server
- RED OS 7.3 Certified Edition

仮想化プラットフォームでは、Kernel-based Virtual Machine は次のオペレーティングシステムでサポートされます：

- ALT 8 SP Server（LKNV.11100-01）64 ビット
- ALT Server 10 64 ビット
- Astra Linux Special Edition（Orel、Voronezh、Smolensk）1.7（閉鎖ソフトウェア環境モードおよび強制モードを含む）64 ビット
- Debian GNU/Linux 11.x（Bullseye）32 ビット / 64 ビット
- Ubuntu Server 20.04 LTS（Focal Fossa）64 ビット
- RED OS 7.3 Server 64 ビット
- RED OS 7.3 Certified Edition 64 ビット

クライアントデバイス

クライアントデバイス側で Kaspersky Security Center 14 Web コンソールを使用するために必要なのはブラウザーのみです。

デバイスのハードウェアおよびソフトウェア要件は、Kaspersky Security Center 14 Web コンソールの操作で使用するブラウザーと同じです。

ブラウザー：

- Mozilla Firefox Extended Support Release 91.8.0 以降（91.8.0 は 2022 年 4 月 5 日にリリースされています）
- Mozilla Firefox Release 99.0 以降（99.0 は 2022 年 4 月 5 日にリリースされています）
- Google Chrome 100.0.4896.88 以降（Official Build）
- Microsoft Edge 100 以降
- macOS 上の Safari 15

ネットワークエージェント

ハードウェアの最小要件

- CPU：動作周波数が 1 GHz 以上（64 ビット OS の場合、最小周波数は 1.4 GHz）
- メモリ：512 MB

- 使用可能なディスク容量：1 GB

Linux ベースのデバイスのソフトウェア要件：Perl 言語インタープリターのバージョン 5.10 以降をインストールする必要があります。

次のオペレーティングシステムがサポートされています：

- Debian GNU/Linux 11.x（Bullseye）32 ビット / 64 ビット
- Debian GNU / Linux 10.x（Buster）32 ビット / 64 ビット
- Debian GNU / Linux 9.x（Stretch）32 ビット / 64 ビット
- Ubuntu Server 20.04 LTS（Focal Fossa）32 ビット / 64 ビット
- Ubuntu Server 20.04.04 LTS（Focal Fossa）ARM 64 ビット
- Ubuntu Server 18.04 LTS（Bionic Beaver）32 ビット / 64 ビット
- Ubuntu Desktop 20.04 LTS（Focal Fossa）32 ビット / 64 ビット
- Ubuntu Desktop 18.04 LTS（Bionic Beaver）32 ビット / 64 ビット
- CentOS 8.x 64 ビット
- CentOS 7.x 64 ビット
- CentOS 7.x ARM 64 ビット
- Red Hat Enterprise Linux Server 8.x 64 ビット
- Red Hat Enterprise Linux Server 7.x 64 ビット
- Red Hat Enterprise Linux Server 6.x 32 ビット / 64 ビット
- SUSE Linux Enterprise Server 12（すべての Service Pack）64 ビット
- SUSE Linux Enterprise Server 15（すべての Service Pack）64 ビット
- SUSE Linux Enterprise Desktop 15（すべての Service Pack）64 ビット
- SUSE Linux Enterprise Desktop 15（Service Pack 3）ARM 64 ビット
- openSUSE 15 64 ビット
- EulerOS 2.0 SP8 ARM
- Pardus OS 19.1 64 ビット
- Astra Linux Special Edition（Orel、Voronezh、Smolensk）1.7（閉鎖ソフトウェア環境モードおよび強制モードを含む）64 ビット
- Astra Linux Special Edition 1.6（閉鎖ソフトウェア環境モードおよび強制モードを含む）64 ビット
- Astra Linux Common Edition 2.12 64 ビット

- Astra Linux Special Edition 4.7 ARM
- ALT Server 10 64 ビット
- ALT Server 9.2 64 ビット
- ALT Workstation 10 32 ビット / 64 ビット
- ALT Workstation 9.2 32 ビット / 64 ビット
- ALT 8 SP Server（LKNV.11100-01）64 ビット
- ALT 8 SP Server（LKNV.11100-02）64 ビット
- ALT 8 SP Server（LKNV.11100-03）64 ビット
- ALT 8 SP Workstation（LKNV.11100-01）32 ビット / 64 ビット
- ALT 8 SP Workstation（LKNV.11100-02）32 ビット / 64 ビット
- ALT 8 SP Workstation（LKNV.11100-03）32 ビット / 64 ビット
- Mageia 4 32 ビット
- Oracle Linux 7 64 ビット
- Oracle Linux 8 64 ビット
- Linux Mint 19.x 32 ビット
- Linux Mint 20.x 64 ビット
- AlterOS 7.5 以降 64 ビット
- GosLinux IC6 64 ビット
- RED OS 7.3 64 ビット
- RED OS 7.3 Server 64 ビット
- RED OS 7.3 Certified Edition 64 ビット
- ROSA Enterprise Linux Server 7.3 64 ビット
- ROSA Enterprise Linux Desktop 7.3 64 ビット
- ROSA COBALT Workstation 7.3 64 ビット
- ROSA COBALT Server 7.3 64 ビット
- Lotos（Linux コア バージョン 4.19.50、DE: MATE）64 ビット

次の仮想化プラットフォームがサポートされています：

- VMware vSphere 6.7

- VMware vSphere 7.0
- VMware Workstation 16 Pro
- Microsoft Hyper-V Server 2012 64 ビット
- Microsoft Hyper-V Server 2012 R2 64 ビット
- Microsoft Hyper-V Server 2016 64 ビット
- Microsoft Hyper-V Server 2019 64 ビット
- Microsoft Hyper-V Server 2022 64 ビット
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- カーネルベースの仮想マシン次のオペレーティングシステムをサポート：
  - ALT 8 SP Server（LKNV.11100-01）64 ビット
  - ALT Server 10 64 ビット
  - Astra Linux Special Edition（Orel、Voronezh、Smolensk）1.7（閉鎖ソフトウェア環境モードおよび強制モードを含む）64 ビット
  - Debian GNU/Linux 11.x（Bullseye）32 ビット / 64 ビット
  - Ubuntu Server 20.04 LTS（Focal Fossa）64 ビット
  - RED OS 7.3 64 ビット
  - RED OS 7.3 Server 64 ビット
  - RED OS 7.3 Certified Edition 64 ビット

Kaspersky Security Center Linux と同じバージョンの Network Agent for Linux をインストールすることを推奨します。

サポートされていないオペレーティングシステムとプラットフォーム

管理サーバー

管理サーバーは、次のオペレーティングシステムと互換性がありません：

- Debian GNU/Linux 7.x（7.8 まで）32 ビット / 64 ビット
- Debian GNU/Linux 8.x（Jessie）32 ビット / 64 ビット
- Ubuntu Server 14.04 LTS（Trusty Tahr）32 ビット / 64 ビット

- Ubuntu Server 16.04 LTS（Xenial Xerus）32 ビット / 64 ビット
- Ubuntu Server 18.04 LTS（Bionic Beaver）32 ビット
- Ubuntu Server 20.04.04 LTS（Focal Fossa）ARM 64 ビット
- Ubuntu Desktop 14.04 LTS（Trusty Tahr）32 ビット / 64 ビット
- Ubuntu Desktop 16.04 LTS（Xenial Xerus）32 ビット / 64 ビット
- Ubuntu Desktop 18.04 LTS（Bionic Beaver）32 ビット / 64 ビット
- Ubuntu Desktop 20.04 LTS（Focal Fossa）32 ビット / 64 ビット
- CentOS 6.x（6.6 まで）64 ビット
- CentOS 7.x ARM 64 ビット
- CentOS 8.x 64 ビット
- Red Hat Enterprise Linux Server 6.x 32 ビット / 64 ビット
- SUSE Linux Enterprise Desktop 12（すべての Service Pack）64 ビット
- SUSE Linux Enterprise Desktop 15（すべての Service Pack）64 ビット
- SUSE Linux Enterprise Desktop 15（Service Pack 3）ARM 64 ビット
- openSUSE 15 64 ビット
- EulerOS 2.0 SP8 ARM
- Pardus OS 19.1 64 ビット
- Astra Linux Special Edition 1.5 64 ビット
- Astra Linux Special Edition 4.7 ARM
- ALT Workstation 9.2 32 ビット / 64 ビット
- ALT Workstation 10 32 ビット / 64 ビット
- ALT 8 SP Workstation（LKNV.11100-01）32 ビット / 64 ビット
- ALT 8 SP Workstation（LKNV.11100-02）32 ビット / 64 ビット
- ALT 8 SP Workstation（LKNV.11100-03）32 ビット / 64 ビット
- Mageia 4 32 ビット
- Oracle Linux 9 64 ビット
- Linux Mint 19.x 32 ビット
- Linux Mint 20.x 64 ビット

- AlterOS 7.5 以降 64 ビット
- RED OS 7.3 64 ビット
- GosLinux IC6 64 ビット
- ROSA Enterprise Linux Server 7.3 64 ビット
- ROSA Enterprise Linux Desktop 7.3 64 ビット
- ROSA COBALT Workstation 7.3 64 ビット
- ROSA COBALT Server 7.3 64 ビット
- Lotos（Linux コア バージョン 4.19.50、DE: MATE）64 ビット

データベースサーバー：

- PostgreSQL 13 64 ビット
- PostgreSQL 14 64 ビット
- Postgres Pro 13 64 ビット
- Postgres Pro 14 64 ビット
- PostgreSQL 15 64 ビット
- PostgreSQL Pangolin 64 ビット
- Microsoft SQL Server 2005 Express 32 ビット
- Microsoft SQL Server 2005（すべてのエディション）32 ビット / 64 ビット
- Microsoft SQL Server 2008 Express 32 ビット
- Microsoft SQL Server 2008（すべてのエディション）32 ビット / 64 ビット
- Microsoft SQL Server 2008 R2（すべてのエディション）64 ビット
- Microsoft SQL Server 2008 R2 Service Pack 2（すべてのエディション）64 ビット
- Microsoft SQL Server 2012（すべてのエディション）64 ビット
- MySQL 5.0 32 ビット / 64 ビット
- MySQL Enterprise 5.0 32 ビット / 64 ビット
- MySQL Standard Edition 5.5 32 ビット / 64 ビット
- MySQL Enterprise Edition 5.5 32 ビット / 64 ビット
- MySQL Standard Edition 5.6 32 ビット / 64 ビット
- MySQL Enterprise Edition 5.6 32 ビット / 64 ビット

- MySQL Standard Edition 5.7 32 ビット / 64 ビット
- MySQL Enterprise Edition 5.7 32 ビット / 64 ビット
- MySQL 5.6 Community 32 ビット / 64 ビット
- MariaDB 10.3 32 ビット / 64 ビット（InnoDB ストレージエンジンを使用）
- MariaDB Galera Cluster 10.4 32 ビット/64 ビット

次の仮想化プラットフォームはサポートされていません：

- VMware vSphere 4.1
- VMware vSphere 5.0
- VMware vSphere 5.1
- VMware vSphere 5.5
- VMware vSphere 6
- VMware vSphere 6.5
- VMware Workstation 9.x
- VMware Workstation 10.x
- VMware Workstation 11.x
- VMware Workstation 12.x Pro
- VMware Workstation Pro 14
- VMware Workstation Pro 15
- Microsoft Hyper-V Server 2008 64 ビット
- Microsoft Hyper-V Server 2008 R2 64 ビット
- Microsoft Hyper-V Server 2008 R2 Service Pack 1 以降 64 ビット
- Microsoft Virtual PC 2007（6.0.156.0）32 ビット/64 ビット
- Citrix XenServer 5.6
- Citrix XenServer 6.0
- Citrix XenServer 6.1
- Citrix XenServer 6.2
- Citrix XenServer 6.5
- Citrix XenServer 7

- Parallels Desktop 7
- Parallels Desktop 11
- Parallels Desktop 14
- Parallels Desktop 16
- Oracle VM VirtualBox 4.0.4-70112（Windows ゲストログインのみ）
- Oracle VM VirtualBox 5.x（Windows ゲストログインのみ）

Kaspersky Security Center 14 Web コンソール

Kaspersky Security Center 14 Web コンソールサーバー

Kaspersky Security Center 14 Web コンソールサーバーは次のオペレーティングシステムと互換性がありません：

- Debian GNU/Linux 7.x（7.8 まで）32 ビット / 64 ビット
- Debian GNU/Linux 8.x（Jessie）32 ビット / 64 ビット
- Ubuntu Server 14.04 LTS（Trusty Tahr）32 ビット / 64 ビット
- Ubuntu Server 16.04 LTS（Xenial Xerus）32 ビット / 64 ビット
- Ubuntu Server 20.04.04 LTS（Focal Fossa）ARM 64 ビット
- Ubuntu Server 22.04 LTS（Jammy Jellyfish）64 ビット
- Ubuntu Desktop 14.04 LTS（Trusty Tahr）32 ビット / 64 ビット
- Ubuntu Desktop 16.04 LTS（Xenial Xerus）32 ビット / 64 ビット
- Ubuntu Desktop 20.04 LTS（Focal Fossa）32 ビット / 64 ビット
- CentOS 6.x（6.6 まで）64 ビット
- CentOS 7.x ARM 64 ビット
- CentOS 8.x 64 ビット
- Red Hat Enterprise Linux Server 6.x 32 ビット / 64 ビット
- Red Hat Enterprise Linux Server 9.x 64 ビット
- SUSE Linux Enterprise Desktop 12（すべての Service Pack）64 ビット
- SUSE Linux Enterprise Desktop 15（すべての Service Pack）64 ビット
- SUSE Linux Enterprise Desktop 15（Service Pack 3）ARM 64 ビット
- openSUSE 15 64 ビット

- Pardus OS 19.1 64 ビット
- Astra Linux Special Edition 4.7 ARM
- Astra Linux Special Edition 1.7.2（閉鎖ソフトウェア環境モードおよび強制モードを含む）64 ビット
- ALT Workstation 9.2 32 ビット / 64 ビット
- ALT Workstation 10 32 ビット / 64 ビット
- ALT 8 SP Workstation（LKNV.11100-01）32 ビット / 64 ビット
- ALT 8 SP Workstation（LKNV.11100-02）32 ビット / 64 ビット
- ALT 8 SP Workstation（LKNV.11100-03）32 ビット / 64 ビット
- Mageia 4 32 ビット
- Oracle Linux 9 64 ビット
- Linux Mint 19.x 32 ビット
- Linux Mint 20.x 64 ビット
- AlterOS 7.5 以降 64 ビット
- RED OS 7.3 64 ビット
- GosLinux IC6 64 ビット
- ROSA Enterprise Linux Server 7.3 64 ビット
- ROSA Enterprise Linux Desktop 7.3 64 ビット
- ROSA COBALT Workstation 7.3 64 ビット
- ROSA COBALT Server 7.3 64 ビット
- ROSA COBALT 7.9 64 ビット
- ROSA CHROME 12 64 ビット
- Lotos（Linux コア バージョン 4.19.50、DE: MATE）64 ビット

ネットワークエージェント

次のオペレーティングシステムはサポートされていません：

- Debian GNU/Linux 7.x（7.8 まで）32 ビット / 64 ビット
- Debian GNU/Linux 8.x（Jessie）32 ビット / 64 ビット
- Ubuntu Server 14.04 LTS（Trusty Tahr）32 ビット / 64 ビット
- Ubuntu Server 16.04 LTS（Xenial Xerus）32 ビット / 64 ビット

- Ubuntu Desktop 14.04 LTS（Trusty Tahr）32 ビット / 64 ビット
- Ubuntu Desktop 16.04 LTS（Xenial Xerus）32 ビット / 64 ビット
- CentOS 6.x（6.6 まで）64 ビット
- Red Hat Enterprise Linux Server 9.x 64 ビット
- SUSE Linux Enterprise Desktop 12（すべての Service Pack）64 ビット
- Astra Linux Special Edition 1.7.2（閉鎖ソフトウェア環境モードおよび強制モードを含む）
- Oracle Linux 9 64 ビット
- ROSA COBALT 7.9 64 ビット
- ROSA CHROME 12 64 ビット

次の仮想化プラットフォームはサポートされていません：

- VMware vSphere 4.1
- VMware vSphere 5.0
- VMware vSphere 5.1
- VMware vSphere 5.5
- VMware vSphere 6
- VMware vSphere 6.5
- VMware Workstation 9.x
- VMware Workstation 10.x
- VMware Workstation 11.x
- VMware Workstation 12.x Pro
- VMware Workstation Pro 14
- VMware Workstation Pro 15
- Microsoft Hyper-V Server 2008 64 ビット
- Microsoft Hyper-V Server 2008 R2 64 ビット
- Microsoft Hyper-V Server 2008 R2 Service Pack 1 以降 64 ビット
- Citrix XenServer 6.0
- Citrix XenServer 6.1
- Citrix XenServer 6.2

- Citrix XenServer 6.5
- Citrix XenServer 7

Kaspersky Security Center 14 Web コンソールの概要

Kaspersky Security Center 14 Web コンソールは、カスペルスキー製品により保護されるネットワークのセキュリティシステムのステータスを管理する目的で設計された Web アプリケーションです。

このアプリケーションを使用して、次のことができます：

- 組織のセキュリティシステムのステータスの管理
- ネットワーク上のデバイスへのカスペルスキー製品のインストールおよびインストールされた製品の管理
- ネットワーク上のデバイスに対して作成されたポリシーの管理
- ユーザーアカウントの管理
- ネットワーク上のデバイスにインストールされたアプリケーションのタスクの管理
- セキュリティシステムのステータスに関するレポートの表示
- システム管理者や他の IT 担当者へのレポート配信の管理

Kaspersky Security Center 14 Web コンソールは、ブラウザーを使用してデバイスと管理サーバーが交信できるようにする Web インターフェイスを提供します。管理サーバーは、ネットワーク内のデバイスにインストールされたカスペルスキー製品の管理を目的として設計されたアプリケーションです。管理サーバーは、セキュアソケットレイヤー（SSL）プロトコルで保護されたチャネルでネットワークのデバイスに接続します。ブラウザーを使用して Kaspersky Security Center 14 Web コンソールに接続する場合、ブラウザーは Kaspersky Security Center 14 Web コンソールサーバーとの接続を確立します。

Kaspersky Security Center 14 Web コンソールは、次のように操作します：

1. ブラウザーで Kaspersky Security Center 14 Web コンソールに接続すると、Web ポータルのインターフェイスが表示されます。
2. Web ポータルによる管理を使用して、実行するコマンドを選択します。Kaspersky Security Center 14 Web コンソールは次の操作を実行します：
    - 情報を受信する目的でコマンドを実行した場合（デバイスのリストを表示するなど）、Kaspersky Security Center 14 Web コンソールは管理サーバーに対する情報のリクエストを生成し、必要なデータを受信し、表示に適した形式でブラウザーに送信します。
    - 管理用のコマンドを選択した場合（アプリケーションのリモートインストールなど）、Kaspersky Security Center 14 Web コンソールはブラウザーからコマンドを受信し、それを管理サーバーに送信します。その後、管理サーバーからコマンドの結果を受信し、それを表示に適した形式でブラウザーに送信します。

Kaspersky Security Center 14 Web コンソールは多言語で利用できます。本製品を開き直さずに、任意のタイミングでインターフェイスの言語を変更できます。Kaspersky Security Center 14 Web コンソールを Kaspersky Security Center と合わせてインストールする場合、インストールファイルと同じ言語が Kaspersky Security Center 14 Web コンソールのインターフェイス言語として選択されます。Kaspersky Security Center 14 Web コンソールのみをインストールする場合、オペレーティングシステムと同じ言語がインターフェイス言語として選択されます。Kaspersky Security Center 14 Web コンソールでインストールファイルやオペレーティングシステムの言語がサポートされていない場合、既定では英語が選択されます。

サポート対象となるカスペルスキー製品のリスト

Kaspersky Security Center Linux は、以下のカスペルスキー製品の一元的な導入と管理をサポートします：

- Kaspersky Endpoint Security for Linux
- Kaspersky Industrial CyberSecurity for Linux Nodes

これらの製品はワークステーションとファイルサーバーの両方を保護します。製品バージョンについては、製品サポートライフサイクルの Web ページを参照してください。

Kaspersky Security Center の比較：Windows ベースと Linux ベース

カスペルスキーは、Windows と Linux の 2 つのプラットフォームのオンプレミスのソリューションとして Kaspersky Security Center を提供しています。Windows ベースのソリューションでは、Windows デバイスに管理サーバーをインストールし、Linux ベースのソリューションには Linux にインストールされるよう設計されたバージョンの管理サーバーをインストールします。このオンラインヘルプには、Kaspersky Security Center Linux に関する情報が含まれています。Windows ベースのソリューションの詳細については、Kaspersky Security Center Windows オンライン ヘルプを参照してください。

以下の表で Windows ベースのソリューションと Linux ベースのソリューションの Kaspersky Security Center の主要な機能を比較します。

Windows ベースのソリューションと Linux ベースのソリューションとして動作する Kaspersky Security Center の機能比較

機能またはプロパティ	Kaspersky Security Center 14	
	Windows ベースのソリューション	Linux ベースのソリューション
管理サーバーの位置	オンプレミス	オンプレミス
データベース管理システム（DBMS）の位置	オンプレミス	オンプレミス
管理サーバーをインストールするオペレーティングシステム	Windows	Linux
管理コンソールの種別	オンプレミスおよび Web ベース	Web ベース
Web ベースの管理コンソールをインストールするオペレーティングシステム	Windows または Linux	Windows または Linux
管理サーバーの階層構造	✓	✓
管理グループの階層	✓	✓
ネットワークポーリング	✓	✓

		(IP 範囲のみ)
管理対象デバイスの最大数	100000	20000
Windows、macOS、Linux 管理対象デバイスの保護	✓	– (Linux デバイスの保護のみ)
モバイルデバイスの保護	✓	–
仮想マシンの保護	✓	–
パブリッククラウドインフラストラクチャの保護	✓	–
デバイスベースのセキュリティ管理	✓	✓
ユーザーベースのセキュリティ管理	✓	✓
製品ポリシー	✓	✓
カスペルスキー製品のタスク	✓	✓
Kaspersky Security Network	✓	–
KSN プロキシ	✓	–
Kaspersky Private Security Network	✓	–
カスペルスキー製品のライセンスの一元的な配信	✓	✓
仮想管理サーバーのサポート	✓	✓
サードパーティ製ソフトウェアのアップデートのインストールと脆弱性の修正	✓	– (リモートインストールタスクの使用のみ)
管理対象デバイスのイベントに関する通知	✓	✓
ユーザーアカウントの作成と管理	✓	✓
ポリシーとタスクのステータスの監視	✓	✓
カスペルスキーのフェールオーバークラスターの導入	✓	✓

基本概念

このセクションでは、Kaspersky Security Center Linux の基本概念について説明します。

管理サーバー

Kaspersky Security Center のコンポーネントを使用すると、クライアントデバイスにインストールされたカスペルスキー製品をリモート管理できます。

管理サーバーがインストールされたデバイスは、*管理サーバー*（「*サーバー*」とも表記）と呼ばれます。管理サーバーについては、あらゆる不正なアクセスに対して、物理的な保護も含めて保護する必要があります。

管理サーバーは、次の属性を持つサービスとしてデバイスにインストールされます：

- 名称は「Kaspersky Security Center 管理サーバー」
- オペレーティングシステムの起動時に自動実行される
- **ローカルシステム**アカウントまたは管理サーバーのインストール時に選択したユーザーアカウントを使用する

管理サーバーは、次の機能を実行します：

- 管理グループ構造の保管
- クライアントデバイスの設定に関する情報の保管
- アプリケーション配布パッケージのリポジトリの管理
- クライアントデバイスへのアプリケーションのリモートインストールおよびアプリケーションの削除
- カスペルスキー製品の定義データベースおよびソフトウェアモジュールのアップデート
- クライアントデバイスのポリシーとタスクの管理
- クライアントデバイスで発生したイベントに関する情報の保管
- カスペルスキー製品の操作に関するレポートの生成
- クライアントデバイスへのライセンスの配信と、ライセンスに関する情報の保管
- （クライアントデバイスでのウイルスの検知など）タスクの進捗に関する通知の転送

製品のインターフェイスで管理サーバーに名前を付ける

Kaspersky Security Center 14 Web コンソールの製品インターフェイスで、管理サーバーに次の名前をつけることが可能です：

- 「*device_name*」または「管理サーバー：*device_name*」などの管理サーバーデバイスの名前。
- 「*IP_address*」または「管理サーバー：*IP_address*」などの管理サーバーの IP アドレス。

- セカンダリ管理サーバーおよび仮想管理サーバーには、これらをプライマリ管理サーバーに接続する際に指定したカスタム名を使用できます。

- Linux デバイスにインストールした Kaspersky Security Center 14 Web コンソールを使用している場合は、本製品は応答ファイルで信頼済みとして指定した管理サーバーの名前を表示します。

Kaspersky Security Center 14 Web コンソールを使用して管理サーバーに接続できます。

管理サーバーの階層構造

管理サーバーは、階層に配置できます。各管理サーバーは、階層の同一ネスト上に複数のセカンダリ管理サーバー（「*セカンダリサーバー*」とも表記）を保持することも、複数のネストレベル上に複数のサーバーを保持することもできます。セカンダリ管理サーバーのネストレベルに制限はありません。プライマリ管理サーバーの管理グループには、すべてのセカンダリ管理サーバーのクライアントデバイスが含められます。このようにして、ネットワークの独立したセクションを、様々な管理サーバーを使用して管理できます。管理サーバーの管理には、プライマリ管理サーバーが使用されます。

*仮想管理サーバー*はセカンダリ管理サーバーの特殊な例です。

階層構造では、Kaspersky Security Center Linux の管理サーバーは、Windows ベースの Kaspersky Security Center または Kaspersky Security Center Cloud コンソールのプライマリ管理サーバーが管理するセカンダリサーバーとしてのみ動作します。

管理サーバーの階層を使用して、次のことを実現できます：

- （ネットワーク全体で 1 台の管理サーバーがインストールされている場合と比較して）管理サーバーの負荷を軽減する。

- イントラネットのトラフィックを削減して、リモートオフィスとの通信を簡略化する。プライマリ管理サーバーとネットワーク上のすべてのデバイス（他の地域にあるデバイスも含む）との間で接続を確立する必要はありません。各ネットワークセグメントにセカンダリ管理サーバーをインストールし、セカンダリ管理サーバーの管理グループ内にデバイスを配置し、高速通信チャネルを使用してセカンダリ管理サーバーとプライマリ管理サーバー間の接続を確立すれば十分です。

- アンチウイルスセキュリティ管理者間で、責任区分を明確にする。企業ネットワーク内のアンチウイルスセキュリティステータスの一元管理機能と監視機能も利用できます。

- サービスプロバイダーが Kaspersky Security Center を使用する。サービスプロバイダーでインストールする必要があるのは、Kaspersky Security Center と Kaspersky Security Center 14 Web コンソールのみです。サービスプロバイダーが様々な組織の多くのデバイスを管理するには、管理サーバーの階層に仮想管理サーバーを追加します。

管理グループの階層に含まれる各デバイスは、1 台の管理サーバーにしか接続できません。デバイスから管理サーバーへの接続を個別に監視する必要があります。ネットワーク属性に基づいて様々な管理サーバーの管理グループ内でデバイスを検索する機能を使用してください。

仮想管理サーバー

仮想管理サーバー（「*仮想サーバー*」とも表記）は、クライアント組織のネットワークの保護を管理する、Kaspersky Security Center Linux のコンポーネントです。

仮想管理サーバーは特殊なセカンダリ管理サーバーであり、物理管理サーバーと比較すると、次の制限があります：

- 仮想管理サーバーは、プライマリ管理サーバー上にのみ作成できます。
- 仮想管理サーバーは、プライマリ管理サーバーのデータベースを使用します。仮想管理サーバーではデータのバックアップと復元タスク、およびアップデートのスキャンとダウンロードタスクはサポートされていません。
- 仮想サーバーでは、セカンダリ管理サーバー（仮想サーバーを含む）の作成がサポートされていません。

さらに、仮想管理サーバーには次の制限があります：

- 仮想管理サーバーのプロパティウィンドウでは、セクション数が限られています。
- 仮想管理サーバーが管理するクライアントデバイスにカスペルスキー製品をリモートからインストールするには、仮想管理サーバーと通信するためにネットワークエージェントがインストールされたクライアントデバイスが必要です。そのデバイスは、最初に仮想管理サーバーと接続する際、自動的にディストリビューションポイントとして設定され、その他のクライアントデバイスと仮想管理サーバーを接続するゲートウェイとして機能します。
- 仮想サーバーでネットワークをポーリングするためには、ディストリビューションポイントを使用する必要があります。
- 正常に動作しない仮想サーバーが Kaspersky Security Center Linux によって再起動される場合、プライマリ管理サーバーとすべての仮想サーバーが再起動されます。

仮想管理サーバーの管理者は、その仮想管理サーバーにおけるすべての権限を持ちます。

Web サーバー

Kaspersky Security Center *Web サーバー*（略称として単に「*Web サーバー*」とも表記）は、管理サーバーとともにインストールされる Kaspersky Security Center のコンポーネントです。Web サーバーは、スタンドアロンインストールパッケージおよび共有フォルダーのファイルをネットワーク上で伝送できるように設計されています。

スタンドアロンインストールパッケージは作成時に、Web サーバー上に自動的に公開されます。スタンドアロンパッケージをダウンロードするリンクは、作成済みスタンドアロンインストールパッケージのリストに表示されます。必要に応じて、スタンドアロンパッケージの公開を取り消したり、Web サーバー上にスタンドアロンパッケージを再度公開したりできます。

共有フォルダーは、管理サーバーで管理されるデバイスを使用するすべてのユーザーが利用できる情報の保管領域として使用されます。共有フォルダーに直接アクセスできないユーザーには、Web サーバーを使用して、そのフォルダーから情報を提供することができます。

Web サーバーを使用して共有フォルダーからユーザーに情報を提供するには、管理者が共有フォルダー内に public という名前のサブフォルダーを作成し、情報をそのサブフォルダーに貼り付ける必要があります。

情報転送リンクの構文は次の通りです：

`https://<Web サーバー名>:<HTTPS ポート>/public/<オブジェクト>`

説明：

- <Web サーバー名> は、Kaspersky Security Center Web サーバーの名前です。
- <HTTPS ポート> は、管理者が定義した Web サーバーの HTTPS ポートです。HTTPS ポートは、管理サーバーのプロパティウィンドウの［**Web サーバー**］セクションで設定できます。既定のポート番号は 8061 です。
- <オブジェクト> は、ユーザーがアクセス権を持っているサブフォルダーまたはファイルです。

管理者は、メールなど便利な方法を利用して、ユーザーに新しいリンクを送信します。

ユーザーは、そのリンクを使用して、必要な情報をローカルデバイスにダウンロードできます。

ネットワークエージェント

管理サーバーとデバイスとの対話は、Kaspersky Security Center のコンポーネントの*ネットワークエージェント*によって実行されます。ネットワークエージェントは、Kaspersky Security Center を使用してカスペルスキー製品を管理するすべてのデバイスにインストールします。

ネットワークエージェントは、次の属性を持つサービスとしてデバイスにインストールされます：

- 名称は「Kaspersky Security Center 14 Linux ネットワークエージェント」
- オペレーティングシステムの起動時に自動実行される
- ローカルシステムアカウントを使用する

ネットワークエージェントがインストールされたデバイスは「*管理対象デバイス*」または単に「*デバイス*」と呼ばれます。ネットワークエージェントは、次のいずれかのソースから取得できます：

- 管理サーバーの保管領域のインストールパッケージ（管理サーバーをインストールしている必要があります）
- カスペルスキーの Web サーバーにあるインストールパッケージ

管理サーバーをインストールしているデバイスでは、サーバーバージョンのネットワークエージェントが管理サーバーとともに自動的にインストールされるので、手動でネットワークエージェントをインストールする必要はありません。

ネットワークエージェントを起動するプロセスの名前は次のとおりです：

- klnagent64.service（64 ビットオペレーティングシステムの場合）
- klnagent.service（32 ビットオペレーティングシステムの場合）

ネットワークエージェントによって管理対象デバイスと管理サーバーが同期します。*同期*間隔（「ハートビート」とも表記）を管理対象 10,000 台につき 15 分に設定することを推奨します。

管理グループ

管理グループ（以後、*グループ*と表記）は、基準に従ってまとめられた管理対象デバイスの仮想グループで、グループ内のデバイスを Kaspersky Security Center 内で 1 つの単位として管理することを目的としています。

管理グループ内の管理対象デバイスはすべて、次の操作を実行できるように設定されます：

- 同一のアプリケーション設定を使用する（設定はグループポリシーで定義できます）。
- 特定の設定でグループタスクを作成することにより、すべてのアプリケーションで共通の動作モードを使用する。グループタスクの例としては、共通のインストールパッケージの作成とインストール、定義データベースおよびモジュールのアップデート、デバイスのオンデマンドスキャン、リアルタイム保護の有効化などがあります。

1台の管理対象デバイスが所属できる管理グループは1つだけです。

管理サーバーとグループに対して、任意の階層レベル数で階層構造を作成できます。1つの階層レベルに、セカンダリ管理サーバーや仮想管理サーバー、グループ、および管理対象デバイスを含めることができます。デバイスの物理的な位置を動かすことなく、あるグループから別のグループへデバイスを移動できます。たとえば、従業員の配属が経理から開発に異動になった場合、この従業員のコンピューターを経理部門用の管理グループから開発部門用の管理グループに移動できます。これにより、コンピューターでは開発部門向けのセキュリティ製品設定が自動的に取得されます。

管理対象デバイス

*管理対象デバイス*はLinuxを実行していてネットワークエージェントをインストールしているコンピューターです。これらのデバイスにインストールされたセキュリティ製品のタスクとポリシーを作成することで、これらのデバイスを管理できます。管理対象デバイスからのレポートも受信できます。

管理対象デバイスをディストリビューションポイントや接続ゲートウェイとして動作させることができます。

1台のデバイスを管理対象にできる管理サーバーは1台のみです。1台の管理サーバーで、最大100,000台のデバイスを管理できます。

未割り当てデバイス

*未割り当てデバイス*とは、ネットワークに接続されているがどの管理グループにも含まれていないデバイスです。未割り当てデバイスに対して、管理グループへ移動したり、アプリケーションをインストールしたりなどの操作を実行できます。

ネットワーク内で検出された新しいデバイスは、「未割り当てデバイス」管理グループに割り当てられます。検出されたデバイスが自動的に他のグループに移動されるようにルールを設定できます。

管理コンピューター

Kaspersky Security Center 14 Webコンソールサーバーがインストールされているデバイスを「*管理者のワークステーション*」と呼びます。管理者は、これらのデバイスを使用して、クライアントデバイスにインストールされているすべてのカスペルスキー製品を一元的にリモート管理できます。

管理コンピューターの数に制限はありません。任意の管理コンピューターから、ネットワーク上にある複数の管理サーバーで構成される管理グループを一度に管理できます。管理コンピューターは、任意の階層レベルにある管理サーバー（物理または仮想）に接続できます。

管理コンピューターは、管理グループにクライアントデバイスとして含めることができます。

任意の管理サーバーの管理グループ内で、1台のデバイスが管理サーバーのクライアント、管理サーバー、または管理コンピューターとして機能できます。

Web 管理プラグイン

Kaspersky Security Center 14 Web コンソールによるカスペルスキー製品のリモート管理では、*Web 管理プラグイン*という特別なコンポーネントが使用されます。以降、Web 管理プラグインは*管理プラグイン*とも表記されます。管理プラグインは、Kaspersky Security Center 14 Web コンソールと特定のカスペルスキー製品との間のインターフェイスです。管理プラグインを使用して、該当製品のタスクとポリシーを設定できます。

管理 Web プラグインは、カスペルスキーのテクニカルサポートサイトからダウンロードできます。

管理プラグインには次の機能があります：

- カスペルスキーのタスクを作成および編集し、各種設定を編集するインターフェイス
- カスペルスキー製品と管理対象デバイスのリモートからの一元管理に使用できるポリシーおよびポリシーのプロファイルを作成および編集するインターフェイス
- カスペルスキー製品で生成されたイベントの転送
- Kaspersky Security Center 14 Web コンソールでは、転送されたカスペルスキー製品の動作データ、イベント、および統計情報を表示できます

ポリシー

*ポリシー*とは、管理グループとそのサブグループに適用される一連のカスペルスキー製品の設定です。管理グループのデバイスに複数のカスペルスキー製品をインストールできます。Kaspersky Security Center は、管理グループ内のカスペルスキー製品ごとに1つのポリシーを提供します。ポリシーは次のいずれかのステータスを持ちます：

ポリシーのステータス

ステータス	説明
アクティブ	現在デバイスに適用されているポリシー。各管理グループ内のカスペルスキー製品に対してアクティブにできるポリシーは1つだけです。デバイスは、カスペルスキー製品のアクティブポリシーの設定値を適用します。
非アクティブ	現在デバイスに適用されていないポリシー。
モバイルユーザー	このオプションをオンにすると、デバイスが企業ネットワークから離れるとポリシーがアクティブになります。

ポリシーは、次のルールに従って機能します：

- 1つのアプリケーションに対して、異なる値を持つ複数のポリシーを定義することができます。
- 現在のアプリケーションに対してアクティブにできるポリシーは1つだけです。
- ポリシーには子ポリシーを設定できます。

一般には、ウイルス攻撃などの緊急事態への備えとしてポリシーを使用できます。たとえば、フラッシュドライブを介した攻撃が発生した場合は、フラッシュドライブへのアクセスをブロックするポリシーを有効化できます。この場合、現在アクティブなポリシーは自動的に非アクティブになります。

異なる状況で複数の設定の変更のみが想定される場合などで、複数のポリシーを管理することを防ぐために、ポリシープロファイルを使用できます。

*ポリシープロファイル*とは、ポリシーの設定値の代わりに使用される、指定されたポリシー設定値のサブセットです。ポリシープロファイルは、管理対象デバイスでの有効な設定の形成に影響を与えます。*有効な設定*とは、デバイスに現在適用されている一連のポリシー設定、ポリシープロファイル設定、およびローカルアプリケーション設定です。

ポリシープロファイルは、次のルールに従って機能します：

- ポリシープロファイルは、特定の有効化条件下で有効になります。
- ポリシープロファイルには、ポリシー設定とは異なる設定値が含まれます。
- ポリシープロファイルを有効化すると、管理対象デバイスの有効な設定が変更されます。
- 1つのポリシーに最大100個のポリシープロファイルを含めることができます。

ポリシーのプロファイル

別々の管理グループに対応して単一のポリシーから枝分かれした複数のポリシーの作成が必要になる場合があります。また、これらの枝分かれ後のポリシーについても、一元的に設定の変更を行えると便利です。枝分かれ後のポリシー同士では、1つか2つの設定値が異なるだけという場合もあります。たとえば、経理部門の従業員には単一のポリシーが適用されるが、部門内の管理職にはフラッシュドライブの使用が許可され、その他のメンバーには許可されないという点が異なる場合などです。こうした状況では、管理グループの階層のみを使用して適切なポリシーを適用することはそれほど簡単ではありません。

単一のポリシーから枝分かれした複数のポリシーを個別に作成しなくても、Kaspersky Security Centerでは*ポリシーのプロファイル*を作成して対応できます。ポリシーのプロファイルは、同じ管理グループ内にあるデバイスを異なるポリシー設定に従って動作させる場合に必要です。

ポリシーのプロファイルには、ポリシー設定のサブセットが指定されています。このサブセットはポリシーとともに対象デバイスに配信され、*プロファイルの有効化条件*と呼ばれる特定の条件下でポリシーを補完する機能を果たします。プロファイルに含まれるのは、管理対象デバイスでアクティブな「基本」ポリシーとは異なる設定（差分）のみです。プロファイルを有効にすると、元々デバイスで有効になっていた「基本」ポリシーの設定が修正されます。修正後の設定では、プロファイルで指定された値が適用されます。

タスク

Kaspersky Security Centerは、様々な*タスク*を作成して実行することにより、デバイス上にインストールされたカスペルスキー製品を管理します。アプリケーションのインストール、起動、停止、ファイルのスキャン、定義データベースやソフトウェアモジュールのアップデート、アプリケーションでのその他のタスクを実行するには、タスクが必要です。

アプリケーションのタスクを作成できるのは、そのアプリケーション用の管理プラグインがインストールされている場合に限られます。

タスクは管理サーバー上とデバイス上で実行できます。

次のタスクは管理サーバーで実行されます：

- レポートの自動配信
- 管理サーバーのリポジトリへのアップデートのダウンロード
- 管理サーバーデータのバックアップ
- データベースのメンテナンス
- 基準となるデバイスの OS イメージに基づいたインストールパッケージの作成

次の種別のタスクはデバイスで実行されます：

- *ローカルタスク* - 特定の 1 台のデバイスで実行されるタスク

  ローカルタスクを変更するには、管理者が Kaspersky Security Center 14 Web コンソールを使用するか、またはリモートデバイスのユーザーが実行します（たとえば、セキュリティ製品のインターフェイスを使用）。管理対象デバイスの管理者とユーザーが同時にローカルタスクを変更する場合、管理者が行う変更内容の方が優先度が高いため有効になります。

- *グループタスク* - 特定のグループに属するすべてのデバイスで実行されるタスク

  タスクのプロパティで特別な設定を行わない限り、グループタスクは選択したグループのすべてのサブグループに影響します。さらに、グループタスクは該当するグループまたはそのサブグループのいずれかに導入されている、セカンダリおよび仮想管理サーバーに接続されているデバイスにも適用されます（オプション設定による）。

- *グローバルタスク* - 管理グループに含まれるかどうかに関係なく、特定のデバイスで実行されるタスク

アプリケーションごとに、任意の数のグループタスク、グローバルタスク、ローカルタスクを作成できます。

タスクの設定に変更を加え、タスクの進行状況を表示し、タスクをコピー、エクスポート、インポート、および削除できます。

> タスクは、そのタスクを作成した対象のアプリケーションが実行中である場合のみ、デバイス上で開始されます。

タスクの実行結果は、管理サーバー上の Syslog ログと Kaspersky Security Center のイベントログに一元的に保存されます。また、各デバイスのローカルにも保存されます。

> タスクの設定には個人データを使用しないでください。たとえば、ドメイン管理者パスワードを指定することは避けてください。

タスク範囲

*タスク範囲*とは、タスクが実行されるデバイスの範囲です対象範囲には次の種別があります：

- *ローカルタスク*の対象範囲は、そのデバイス自体です。

- *管理サーバータスク*の対象範囲は、管理サーバーです。
- *グループタスク*の対象範囲は、グループに含まれているデバイスのリストです。

*グローバルタスク*の作成時に、次の方法を使用して対象範囲を指定できます：

- 特定のデバイスを手動で指定する

  デバイスのアドレスとして、IP アドレス（または IP アドレス範囲）または DNS 名を使用できます。

- 追加するデバイスのアドレスが記載されている txt ファイルからデバイスのリストをインポートする（各アドレスを独立した行に記載する必要があります）。

  デバイスのリストをファイルからインポートするかまたはリストを手動で作成し、デバイスが名前によって識別される場合、リストに含めることができるのはその情報が管理サーバーのデータベースに登録済みであるデバイスのみです。データベースへの情報の入力は、デバイスの接続時、またはデバイスの検索中に実行されます。

- デバイスの抽出を指定する。

  時間の経過とともに、抽出に含まれるデバイスセットの変更に応じてタスクの範囲が変化します。デバイスの抽出は、デバイスにインストールされているソフトウェアを含むデバイス属性、およびデバイスに割り当てられているタグに基づいて作成できます。デバイスの抽出は、タスクの範囲を定義するための最も柔軟性の高い方法です。

  デバイスの抽出を対象とするタスクは常に、管理サーバーのスケジュールに基づいて実行されます。このタスクは、管理サーバーと接続されていないデバイスでは実行できません。他の方法でタスク範囲が指定されたタスクはデバイス上で直接実行されるため、デバイスと管理サーバーとの接続の有無には左右されません。

  デバイスの抽出を対象とするタスクは、デバイスのローカル時間ではなく管理サーバーのローカル時間に基づいて実行されます。他の方法でタスク範囲が指定されたタスクはデバイスのローカル時間に基づいて実行されます。

ローカルアプリケーション設定とポリシーの関連付け

ポリシーを使用して、グループ内のすべてのデバイスに同じ値のアプリケーション設定を指定できます。

ローカルアプリケーション設定を使用して、ポリシーで指定されている設定値をグループ内の個別のデバイスに再定義できます。設定値を指定できるのは、ポリシーで変更が許可されている設定（ロック解除された設定）だけです。

クライアントデバイスのアプリケーションで使用される値は、その設定がポリシー内でロックされているかどうか（🔒）に基づいて決定されます：

- 設定の変更がロックされている場合、ポリシー内で定義されている値が、すべてのクライアントデバイスで使用される
- 設定の変更がロック解除されている場合、各クライアントデバイスのアプリケーションは、ポリシーで指定されている値ではなくローカル設定の値を使用する。設定は、ローカルアプリケーション設定で変更できます。

このため、クライアントデバイスでタスクを実行する場合、次の 2 つの方法で定義した設定が使用されます：

- タスク設定とローカルアプリケーション設定（ポリシー内の設定の変更がロックされていない場合）
- グループポリシー（設定の変更がロックされている場合）

ローカルアプリケーション設定は、最初にポリシー設定に基づいてポリシーが適用された後で適用されます。

ディストリビューションポイント

ディストリビューションポイント（旧称：アップデートエージェント）とは、ネットワークエージェントがインストールされ、アップデートの配信やアプリケーションのリモートインストール、ネットワーク内のデバイスの情報の収集に使用されるデバイスです。ディストリビューションポイントは、次の機能を実行できます：

- 管理サーバーから受信したアップデートおよびインストールパッケージをグループ内のクライアントデバイスに配布します（UDP を使用したマルチキャストを含む）。アップデートは、管理サーバーまたはカスペルスキーのアップデートサーバーから受信可能です。後者の場合は、ディストリビューションポイントのアップデートタスクを作成する必要があります。

  ディストリビューションポイントにより、アップデートの配信が加速され、管理サーバーのリソースが解放されます。

- UDP を使用して、マルチキャストによってポリシーとグループタスクを配信します。

- 管理グループのデバイスに対して、管理サーバーとの接続のゲートウェイとして動作します。

  グループ内の管理対象デバイスと管理サーバーとの間で直接接続を確立できない場合は、このグループの管理サーバーへの接続ゲートウェイとしてディストリビューションポイントを使用できます。この場合、管理対象デバイスは接続ゲートウェイに接続され、接続ゲートウェイが管理サーバーに接続されます。

  接続ゲートウェイとして動作するディストリビューションポイントを使用することで、管理対象デバイスと管理サーバーとの間の直接接続がブロックされることはありません。接続ゲートウェイは使用できないが、管理サーバーとの直接接続が技術的に可能な場合は、管理対象デバイスは管理サーバーに直接接続されます。

- 新しいデバイスを検出したり既存のデバイスの情報を更新するために、ネットワークを検索します。ディストリビューションポイントは管理サーバーと同じ方法でデバイスを検出できます。

- カスペルスキーおよびその他のソフトウェアベンダーによるアプリケーションのリモートインストールを実行します。これには、ネットワークエージェントを使用しないクライアントデバイスへのインストールが含まれます。

  この機能により、管理サーバーが直接アクセスできないネットワークに配置されているクライアントデバイスに、ネットワークエージェントのインストールパッケージをリモートで転送できます。

管理サーバーからディストリビューションポイントへのファイル転送は、HTTP で、または SSL 接続が有効な場合は HTTPS で実行されます。HTTP または HTTPS を使用すると、トラフィック量が削減され、SOAP と比較して速度が速くなります。

ネットワークエージェントをインストールしたデバイスは、管理者が手動で、または管理サーバーから自動で、ディストリビューションポイントに割り当てることができます。指定された管理グループのディストリビューションポイントの完全なリストは、ディストリビューションポイントのリストのレポートに表示されます。

ディストリビューションポイントの範囲は、管理者により割り当てられている管理グループ、および、埋め込みのすべてのレベルのサブグループです。複数のディストリビューションポイントが管理グループの階層に割り当てられている場合、管理対象デバイスのネットワークエージェントが、階層内の最も近いディストリビューションポイントに接続します。

管理サーバーによってディストリビューションポイントが自動的に割り当てられた場合、管理グループではなくブロードキャストドメインによって割り当てられます。これは、すべてのブロードキャストドメインが管理サーバーで認識済みである場合に発生します。ネットワークエージェントは同じサブネットに存在する他のネットワークエージェントとメッセージを交換し、得た情報を管理サーバーに送信します。管理サーバーはその情報をネットワークエージェントのブロードキャストドメインでのグループ化に利用します。管理グループ内のネットワークエージェントの 70% 以上を検索した後にブロードキャストドメインが管理サーバーに認識されます。管理サーバーはブロードキャストドメインを 2 時間ごとに検索します。ディストリビューションポイントは、ブロードキャストドメイン別に割り当てられた後、管理グループ別に再度割り当てることはできません。

管理者がディストリビューションポイントを手動で割り当てる場合、管理グループまたはネットワークロケーションに割り当てることができます。

アクティブな接続プロファイルを持つネットワークエージェントは、ブロードキャストドメインの検知の対象外となります。

Kaspersky Security Center Linux では、各ネットワークエージェントに対して、他のどのアドレスとも異なる一意の IP マルチキャストアドレスを割り当てます。これにより、IP の重複によって発生するネットワークの過負荷を回避できます。旧バージョンの製品で割り当てられた IP マルチキャストアドレスは変更されません。

2 つ以上のディストリビューションポイントを単一のネットワークエリアまたは単一の管理グループに割り当てると、それらの 1 つがアクティブなディストリビューションポイントとなり、残りがスタンバイディストリビューションポイントとなります。アクティブなディストリビューションポイントはアップデートとインストールパッケージを直接管理サーバーからダウンロードします。一方、スタンバイのディストリビューションポイントはアクティブなディストリビューションポイントからのみアップデートを受信します。この場合、ファイルは管理サーバーから一度ダウンロードされてからディストリビューションポイント間で配信されます。アクティブなディストリビューションポイントが何かの理由で利用不可能になった場合、スタンバイのディストリビューションポイントがアクティブになります。管理サーバーは自動的にディストリビューションポイントをスタンバイとして割り当てます。

ディストリビューションポイントのステータス（「*アクティブ*」または「*スタンバイ*」）とチェックボックスが、klnagchk のレポートに表示されます。

ディストリビューションポイントには、少なくとも 4 GB の空きディスク容量が必要です。ディストリビューションポイントのディスクの空き容量が 2 GB 未満の場合は、重要度「*警告*」のインシデントが作成されます。このインシデントは、デバイスのプロパティの［**インシデント**］セクションに表示されます。

ディストリビューションポイントとして割り当てられているデバイスでリモートインストールタスクを実行するには、追加の空きディスク容量が必要です。空きディスク容量はインストールするすべてのインストールパッケージの合計サイズを上回っていなければなりません。

ディストリビューションポイントとして割り当てられているデバイスでアップデート（パッチ適用）タスクと脆弱性の修正タスクを実行するには、追加の空きディスク容量が必要です。空きディスク容量は、インストールするすべてのパッチの合計サイズの少なくとも 2 倍でなければなりません。

ディストリビューションポイントとして動作するデバイスについては、あらゆる不正なアクセスに対して、物理的な保護も含めて保護する必要があります。

接続ゲートウェイ

*接続ゲートウェイ*は、特別なモードで動作するネットワークエージェントです。接続ゲートウェイは、他のネットワークエージェントからの接続を受け入れ、サーバーとの独自の接続を介してそれらを管理サーバーにトンネリングします。通常のネットワークエージェントとは異なり、接続ゲートウェイは、管理サーバーへの接続を確立するのではなく、管理サーバーからの接続を待機します。

接続ゲートウェイが通信可能なデバイスは 10,000 台までです。

接続ゲートウェイの使用方法は次の 2 つです：

- 非武装地帯（DMZ）への接続ゲートウェイのインストールを推奨します。モバイルユーザーデバイスにインストールされた別のネットワークエージェントのために、接続ゲートウェイを介した管理サーバーへの接続を専用に設定する必要があります。

  いかなる場合でも、ネットワークエージェントから管理サーバーへ転送されるデータを接続ゲートウェイが変更または処理することはありません。また、このデータをバッファに書き込むこともありません。したがって、ネットワークエージェントからデータを受信し、それを管理サーバーへ後で転送することもありません。ネットワークエージェントが接続ゲートウェイを介して管理サーバーへの接続を試行したが接続ゲートウェイが管理サーバーへ接続できない場合、ネットワークエージェントは管理サーバーがアクセス不能であると判断します。データはすべてネットワークエージェントに残ります（接続ゲートウェイには残りません）。

  接続ゲートウェイが別の接続ゲートウェイを介して管理サーバーへ接続することはできません。これは、ネットワークエージェントが同時に接続ゲートウェイとして動作したり、接続ゲートウェイを使用して管理サーバーへ接続したりすることができないことを意味します。

  接続ゲートウェイはすべて、管理サーバーのプロパティにあるディストリビューションポイントのリストに含まれています。

- 接続ゲートウェイは、ネットワーク内で使用することも可能です。たとえば、自動的に割り当てられたディストリビューションポイントは、自身の範囲内の接続ゲートウェイにもなります。ただし、接続ゲートウェイを内部ネットワークで使用しても、大きな利点はありません。管理サーバーが受信するネットワーク接続の数は減少しますが、受信データ量は減少しません。接続ゲートウェイがない場合でも、すべてのデバイスは管理サーバーへ接続可能です。

ライセンス

このセクションでは、Kaspersky Security Center 14 Linux のライセンス付与に関係する一般的な概念に関する情報を提供します。

使用許諾契約書について

*使用許諾契約書*は、ユーザーと AO Kaspersky Lab との間で交わされる契約であり、製品の使用条件が定められています。

製品の使用を開始する前に、使用許諾契約書の条項をよく読んでください。

Kaspersky Security Center Linux とそのコンポーネント（ネットワークエージェントなど）にはそれぞれ個別の使用許諾契約書があります。

Kaspersky Security Center Linux の使用許諾契約書の条項は、次の方法で確認できます：

- Kaspersky Security Center のインストール中に確認する。
- Kaspersky Security Center の配布キットに含まれている license.txt を参照する。
- Kaspersky Security Center のインストールフォルダーにある license.txt を参照する。
- カスペルスキーの Web サイトから ファイル license.txt をダウンロードする。

Linux 用ネットワークエージェントの使用許諾契約書の条項は、次の方法で確認できます：

- カスペルスキーの Web サーバーからのネットワークエージェント配布パッケージのダウンロード時に確認する。
- Linux 向けネットワークエージェントのインストール中に確認する。

  Linux 向けネットワークエージェントをインストールすると、ネットワークエージェントの使用許諾契約書が英語で表示されることに留意してください。インストール中に使用許諾契約書の条項に同意する前に、フォルダー /opt/kaspersky/klnagent64/share/license でネットワークエージェントの使用許諾契約書を他の言語で確認できます。

- Linux 向けネットワークエージェントの配布パッケージに含まれる license.txt を読んで確認する。
- Linux 向けネットワークエージェントのインストールフォルダーにある license.txt を読んで確認する。
- カスペルスキーの Web サイトから ファイル license.txt をダウンロードする。

製品のインストール時に使用許諾契約書に同意することにより、使用許諾契約書の条項を受諾したものと判断されます。使用許諾契約書の条項に同意しない場合は、製品のインストールを中止し、使用しないようにする必要があります。

ライセンスについて

*ライセンス*は、使用許諾契約書の条件に基づいて提供される、製品を使用する期限付きの権利です。

ライセンスにより、次のサービスの使用が許可されます：

- 使用許諾契約書の条項に沿った製品の使用
- テクニカルサポートの利用

サービスの範囲と有効期間に関する条件は、アプリケーションのアクティベーションに使用されたライセンスの種類によって異なります。

次のライセンス種別があります：

- *試用版：*製品の試用を目的とした無償ライセンス。

  試用版ライセンスは通常、有効期間が短く設定されています。試用版ライセンスの有効期間が終了すると、Kaspersky Security Center Linux のすべての機能が無効になります。製品の使用を継続するには、製品版ライセンスを購入する必要があります。

  試用版ライセンスを使用して製品をアクティベートできるのは、一度だけです。

- *製品版：*製品の購入時に提供される有償ライセンス。

  製品版ライセンスの有効期限が切れると、本製品の主要な機能が無効になります。Kaspersky Security Center の使用を継続するには、製品版ライセンスを更新する必要があります。ライセンスを更新する予定がない場合は、コンピューターから本製品を削除する必要があります。

有効期間が終了する前にライセンスを更新し、すべてのセキュリティ脅威から最大限に保護された環境を維持できるようにしてください。

ライセンス証書について

*ライセンス証書*とは、ライセンス情報ファイルまたはアクティベーションコードに付随して受け取る文書です。

ライセンス証書には、提供されたライセンスに関する次の情報が含まれています：

- ライセンス情報の数値または注文番号
- ライセンスが適用されるユーザーの情報
- 提供されたライセンスを使用したアクティベーションが可能である製品の情報
- ライセンスの上限（提供されたライセンスで使用可能な製品が使用できるデバイスの台数など）
- ライセンスの有効期間の開始日
- ライセンスの有効期間または有効期間の終了日
- ライセンス種別

ライセンス情報について

*ライセンス情報*とは、使用許諾契約書の条項に基づいてアクティベーションを適用して製品を使用できる数値の並びです。ライセンス情報は、カスペルスキーによって生成されます。

製品にライセンス情報を追加するには、*ライセンス情報ファイル*を適用するか、*アクティベーションコード*を入力します。ライセンス情報は、製品に追加した後、インターフェイスに一意の英数字の並びで表示されます。

使用許諾契約書の条項に違反した場合、カスペルスキーがライセンス情報をブロックします。ライセンス情報がブロックされた際に、製品を使用したい場合は、別のライセンス情報を追加する必要があります。

ライセンスには、現在のライセンスまたは予備のライセンスがあります。

現在のライセンス：アプリケーションによって現在使用されているライセンス。現在のライセンスは、試用版または製品版のライセンス情報として追加できます。製品に指定できる現在のライセンスは1つのみで、2つ以上の現在のライセンスを指定することはできません。

予備のライセンス：アプリケーションを使用する権限をユーザーに付与する、現在使用されていないライセンス。予備のライセンスは、現在のライセンスの有効期間が終了すると、自動的に適用されます。予備のライセンスは、現在のライセンスが追加済みである場合にのみ、追加できます。

試用版のライセンスは、現在のライセンスとしてのみ追加できます。試用版のライセンスを予備のライセンスとして追加することはできません。

プライバシーポリシーの表示

プライバシーポリシーは、https://www.kaspersky.co.jp/products-and-services-privacy-policy で参照できます。

プライバシーポリシーはオフラインでも使用可能です。

- Kaspersky Security Center のインストール前にプライバシーポリシーを確認することができます。
- プライバシーポリシーは Kaspersky Security Center のインストールフォルダーにある license.txt に含まれています。
- ファイル「privacy_policy.txt」は管理対象デバイスのネットワークエージェントのインストールフォルダーにあります。
- ネットワークエージェントの配布パッケージから privacy_policy.txt を解凍できます。

Kaspersky Security Center のライセンスオプション

Kaspersky Security Center は、企業ネットワークの保護に使用するカスペルスキー製品の一部として配信されます。カスペルスキーの Web サイトからもダウンロードできます。

次の機能を使用できます：

- リモートオフィスまたはクライアント組織のネットワークを管理する仮想管理サーバーの作成
- 特定のデバイスをまとめて管理する管理グループの階層の作成
- 組織のアンチウイルスセキュリティステータスの管理

- アプリケーションのリモートインストール
- リモートインストールに使用できるオペレーティングシステムイメージのリストの表示
- クライアントデバイスにインストールされたアプリケーションの一元的設定
- 既存のライセンス認証済みアプリケーションのグループの表示と編集
- アプリケーションの動作に関する統計、レポートの検索、および緊急イベントの通知
- ネットワークポーリングによって検出されたハードウェアのリストの表示と手動編集
- 隔離フォルダーまたはバックアップフォルダーに移動されたファイルおよび処理が延期されたファイルの一元的管理
- ユーザーロールの管理

ライセンス情報ファイルについて

*ライセンス情報ファイル*は、拡張子が「key」のファイルで、カスペルスキーから提供されます。ライセンス情報ファイルは、製品のアクティベーションに使用します。

ライセンス情報ファイルは、Kaspersky Security Center を購入すると提供されます。

ライセンス情報ファイルでのアクティベーション時には、カスペルスキーのアクティベーションサーバーへの接続は必要ありません。

製品のインストール後にライセンス情報ファイルを紛失した場合は、再入手できます。ライセンス情報ファイルは、カスペルスキーカンパニーアカウントへの登録時などに必要となる場合があります。

ライセンス情報ファイルを再入手するには次の方法があります：

- ご購入元の販売代理店へ問い合わせる
- カスペルスキーの Web サイト で、使用可能なアクティベーションコードを使用してライセンス情報ファイルを取得する

データ提供について

権利者に送信されるデータ

Kaspersky Security Center 14 Linux の使用許諾契約書に記載されています。

ローカル環境で処理されるデータ

Kaspersky Security Center Linux は、組織のネットワークの基本的な管理と保守の一元化を目的として設計されています。管理者は組織のネットワークのセキュリティレベルに関する詳細情報にアクセスし、カスペルスキー製品を使用して構築された保護システムのすべてのコンポーネントを設定できるようになります。Kaspersky Security Center Linux が実行する主要な機能は次の通りです：

- 組織のネットワーク内のデバイスおよびそのユーザーの検出
- デバイス管理用の管理グループ階層の作成
- デバイスへのカスペルスキー製品のインストール
- インストールされた製品の設定およびタスクの管理
- デバイス上でのカスペルスキー製品のアクティベーション
- ユーザーアカウントの管理
- デバイス上でのカスペルスキー製品の動作に関する情報の表示
- レポートの表示

主要な機能を実行するために、Kaspersky Security Center Linux は次の情報を取得し、保存し、処理することができます：

- ネットワーク内のデバイスの検索または IP 区間のスキャンによって取得した、組織のネットワーク内のデバイスに関する情報。管理サーバーは、データを自身で収集するか、ネットワークエージェントからデータを取得します。
- 管理対象デバイスの詳細情報。ネットワークエージェントによって、次に記載されたデータがデバイスから管理サーバーに送信されます。ユーザーはデバイスの表示名と説明を Kaspersky Security Center 14 Web コンソールのインターフェイスに入力します：
  - デバイスの識別に必要な管理対象デバイスとそのコンポーネントの技術的な仕様情報：デバイスの表示名と説明、DNS ドメインと DNS 名、IPv4 アドレス、IPv6 アドレス、ネットワークロケーション、MAC アドレス、オペレーティングシステムの種別、デバイスが仮想マシンかどうかの情報とハイパーバイザーの種別、およびデバイスが VDI の一部としての動的仮想マシンかどうかの情報。
  - 管理対象デバイスの監査および特定のパッチやアップデートが適用可能かどうかの判断に必要となる、管理対象デバイスとそのコンポーネントのその他の仕様情報：おぺれーてぃぐシステムのアーキテクチャ、オペレーティングシステムの製造元、オペレーティングシステムのビルド番号、オペレーティングシステムのリリース識別子、オペレーティングシステムのロケーションフォルダー、仮想マシンの種別（デバイスが仮想マシンの場合）。
  - 管理対象デバイス上の処理の詳細情報：前回のアップデートの日時、デバイスが前回ネットワークで検出された日時、再起動の待機ステータス、デバイスの電源を投入した日時。
  - デバイスのユーザーアカウントとその作業セッションの詳細情報。
- デバイスがディストリビューションポイントである場合、ディストリビューションポイントの動作統計情報。ネットワークエージェントによってデータがデバイスから管理サーバーに送信されます。
- ユーザーが Kaspersky Security Center 14 Web コンソールに入力したディストリビューションポイントの設定。
- デバイスにインストールされたカスペルスキー製品の詳細情報。管理対象アプリケーションによって、データがネットワークエージェント経由でデバイスから管理サーバーに送信されます：
  - 管理対象デバイスにインストールされているカスペルスキー製品の設定：カスペルスキー製品の名前とバージョン、ステータス、リアルタイム保護のステータス、前回のデバイススキャンの日時、検知された脅威の数、駆除に失敗したオブジェクトの数、製品コンポーネントの使用可否の情報とそのステータス、カスペルスキー製品の設定およびタスクの詳細情報、現在のライセンスと予備のライセンスに関する情報、製品のインストールの日付と ID。

- 製品動作の統計情報：管理対象デバイス上のカスペルスキー製品コンポーネントのステータス変化および製品コンポーネントによって開始されたタスクのパフォーマンスに関係するイベント。

- カスペルスキー製品によって定義されたデバイスのステータス。

- カスペルスキー製品によって割り当てられたタグ。

- Kaspersky Security Center Linux のコンポーネントおよび管理対象のカスペルスキー製品からのイベントに含まれるデータ。ネットワークエージェントによってデータがデバイスから管理サーバーに送信されます。

- Kaspersky Security Center Linux のコンポーネント、およびポリシーとポリシーのプロファイルに示される管理対象のカスペルスキー製品の設定。ユーザーが Kaspersky Security Center 14 Web コンソールでデータを入力します。

- Kaspersky Security Center Linux のコンポーネントおよび管理対象のカスペルスキー製品のタスク設定。ユーザーが Kaspersky Security Center 14 Web コンソールでデータを入力します。

- 脆弱性とパッチ管理機能によってデータが処理されます。ネットワークエージェントは、管理対象デバイス上で検出されたハードウェアに関する情報（ハードウェアレジストリ）をデバイスから管理サーバーに転送します。

- アプリケーションのユーザーカテゴリ。ユーザーが Kaspersky Security Center 14 Web コンソールでデータを入力します。

- アプリケーションコントロール機能を使用して管理対象デバイスで検出された実行ファイルの詳細。管理対象アプリケーションによって、データがネットワークエージェント経由でデバイスから管理サーバーに送信されます。データ一覧については、該当する製品のヘルプファイルに記載されています。

- バックアップされたファイルの詳細情報。管理対象アプリケーションによって、データがネットワークエージェント経由でデバイスから管理サーバーに送信されます。データ一覧については、該当する製品のヘルプファイルに記載されています。

- 隔離されたファイルの詳細情報。管理対象アプリケーションによって、データがネットワークエージェント経由でデバイスから管理サーバーに送信されます。データ一覧については、該当する製品のヘルプファイルに記載されています。

- 詳細分析のためにカスペルスキーの担当者から提出を依頼されたファイルの詳細情報。管理対象アプリケーションによって、データがネットワークエージェント経由でデバイスから管理サーバーに送信されます。データ一覧については、該当する製品のヘルプファイルに記載されています。

- デバイスコントロール機能によって検出された、管理対象デバイスに搭載されているデバイスまたは管理対象デバイスに接続している外部デバイス（メモリユニット、情報転送ツール、情報ハードコピーツール、接続バス）の詳細情報。管理対象アプリケーションによって、データがネットワークエージェント経由でデバイスから管理サーバーに送信されます。データ一覧については、該当する製品のヘルプファイルに記載されています。

- 管理対象のプログラマブルロジックコントローラー（PLC）のリスト。管理対象アプリケーションによって、データがネットワークエージェント経由でデバイスから管理サーバーに送信されます。データ一覧については、該当する製品のヘルプファイルに記載されています。

- 入力されたアクティベーションコードの詳細情報。ユーザーが管理コンソールまたは Kaspersky Security Center 14 Web コンソールのインターフェイスでデータを入力します。

- ユーザーアカウント：名前、説明、氏名、メールアドレス、メインの電話番号、パスワード。ユーザーが Kaspersky Security Center 14 Web コンソールでデータを入力します。

- 管理オブジェクトの変更履歴。ユーザーが Kaspersky Security Center 14 Web コンソールでデータを入力します。
- 削除された管理オブジェクトのレジストリ。ユーザーが Kaspersky Security Center 14 Web コンソールでデータを入力します。
- ファイルから作成されたインストールパッケージとインストール設定。ユーザーが Kaspersky Security Center 14 Web コンソールでデータを入力します。
- Kaspersky Security Center 14 Web コンソールでのカスペルスキーからの告知表示に必要なデータ。ユーザーが Kaspersky Security Center 14 Web コンソールでデータを入力します。
- Kaspersky Security Center 14 Web コンソールで管理対象アプリケーションのプラグインが機能するために必要なデータおよび日常の作業中に管理サーバーのデータベースにプラグインによって保存されるデータ。データの説明および提供方法については、対応するアプリケーションのヘルプファイルで説明されています。
- Kaspersky Security Center 14 Web コンソールのユーザー設定：ローカリゼーション言語とインターフェイスのテーマ、監視パネルの表示設定、通知のステータスに関する情報（確認済みまたは未確認）、スプレッドシートの列のステータス（表示または非表示）、トレーニングモードの進捗状況。ユーザーが Kaspersky Security Center 14 Web コンソールでデータを入力します。
- Kaspersky Security Center Linux のコンポーネントおよび管理対象のカスペルスキー製品に関する Kaspersky イベントログ。Kaspersky イベントログは各デバイスに保存され、管理サーバーに送信されることはありません。
- 管理対象デバイスから Kaspersky Security Center Linux コンポーネントへのセキュアな接続を確立するための証明書。ユーザーが Kaspersky Security Center 14 Web コンソールでデータを入力します。
- ユーザーが Kaspersky Security Center 14 Web コンソールで入力したデータ。
- ユーザーが Kaspersky Security Center 14 Web コンソールで入力したあらゆるデータ。

上記のデータは、次の方法のいずれかが適用された場合に Kaspersky Security Center にLinux 表示される場合があります：

- ユーザーが Kaspersky Security Center 14 Web コンソールでデータを入力します。
- ネットワークエージェントが自動的にデータをデバイスから受信して、管理サーバーに送信します。
- ネットワークエージェントが、管理対象のカスペルスキー製品によって取得されたデータを受信して、管理サーバーに送信する。管理対象のカスペルスキー製品によって処理されるデータ一覧については、該当する製品のヘルプファイルに記載されています。
- ディストリビューションポイントを割り当てられた管理サーバーとネットワークエージェントは、ネットワーク接続されたデバイスに関する情報を収集します。

これらのデータは管理サーバーのデータベースに保存されます。ユーザー名とパスワードは暗号化された形式で保存されます。

ローカルで処理されたデータはすべて、ダンプファイル、トレースファイル、または Kaspersky Security Center Linux のコンポーネントのログファイル（インストーラーやユーティリティによって作成されたログファイルを含む）としてのみカスペルスキーに送信されます。

カスペルスキーは、受け取ったすべての情報を法律およびカスペルスキーの内規に基づいて保護します。データはセキュアな接続で送信されます。

管理コンソールまたは Kaspersky Security Center 14 Web コンソールのリンクを使用することで、お客様は次のデータが自動的に送信されることに同意したものとします：

- Kaspersky Security Center Linux のコード
- Kaspersky Security Center Linux のバージョン
- Kaspersky Security Center Linux の言語
- ライセンス識別子
- ライセンス種別
- ライセンスが代理店経由で購入されたかどうか

リンクの目的や位置によってリンク経由で提供されたデータのリスト。

カスペルスキーでは、取得したデータはすべて匿名形式で、また一般的な統計情報としてのみ使用します。統計情報のサマリーが最初に取得した情報から自動的に生成されますが、そのサマリーには個人情報などの機密情報は含まれていません。新しい情報が蓄積された後、以前のデータは即座に破棄されます（年に1回）。統計情報のサマリーは、無期限に保管されます。

定額制サービスについて

*Kaspersky Security Center Linux の定額制サービス*とは、選択した設定（有効期限、保護されるデバイスの台数）でのアプリケーションの使用を注文することです。Kaspersky Security Center Linux の定額制サービスをサービスプロバイダー（インターネットプロバイダーなど）に登録できます。定額制サービスは手動および自動で更新することができ、キャンセルすることもできます。

定額制サービスの期間は制限する（1年間など）ことも、無制限にすることもできます。制限された定額制サービスの期限を過ぎて Kaspersky Security Center を利用するには、更新する必要があります。サービスプロバイダーによって期限までに支払いが行われた場合、無制限の定額制サービスは自動的に更新されます。

制限された定額制サービスの期限が過ぎた場合は、更新するまでの猶予期間が与えられ、その期間はアプリケーションが機能し続けます。猶予期間の長さや利用できる機能はサービスプロバイダーによって定義されます。

Kaspersky Security Center Linux を定額制サービスの形式で利用するには、サービスプロバイダーが提供するアクティベーションコードを適用する必要があります。

異なる Kaspersky Security Center Linux のアクティベーションコードを適用できるのは、定額制サービスの期限の経過後か、定額制サービスをキャンセルした時のみです。

サービスプロバイダーによっては、定額制サービスの管理に伴う操作が異なる可能性があります。サービスプロバイダーが定額制サービスの更新のための猶予期間を設定しないこともあり、その場合はアプリケーションを利用できなくなります。

定額制サービスの形式で利用する目的で購入されたアクティベーションコードで Kaspersky Security Center の旧バージョンをアクティベートすることはできません。

定額制サービスのもとアプリケーションを使用している場合、Kaspersky Security Center Linux は、定額制サービスの有効期間が切れるまで、指定された間隔でアクティベーションサーバーへの接続を自動的に試みます。定額制サービスは、サービスプロバイダーの Web サイトで更新することができます。

ライセンス制限超過のイベント

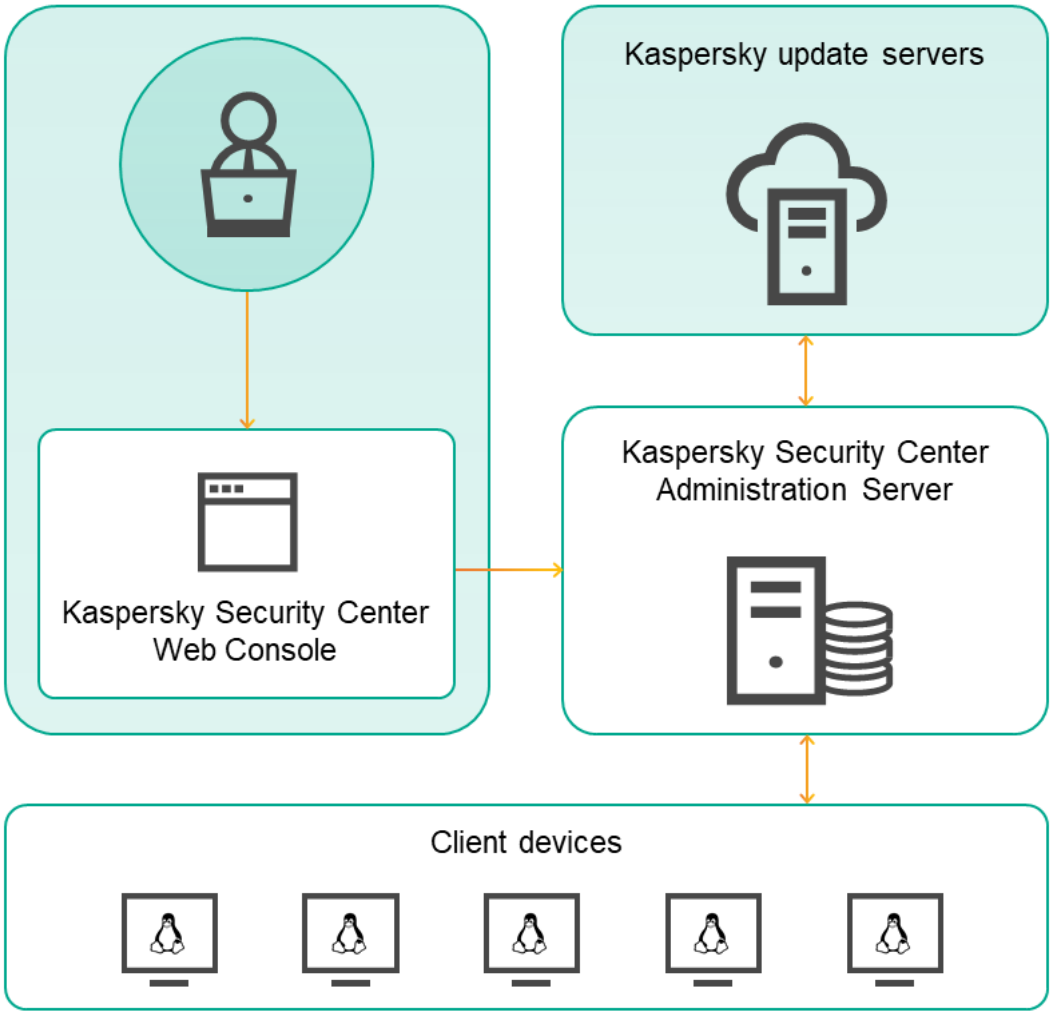
Kaspersky Security Center Linux には、クライアントデバイスにインストールされたカスペルスキー製品がライセンスによる制限を超過した時のイベントに関する情報が表示されます。

ライセンスの制限を超過した時のイベントの重要度は、次のルールに従って決定されます：

- 単一のライセンスが現在適用されている台数が、そのライセンスが対応している合計台数の 90 ～ 100% である場合、重要度が「**情報**」のイベントが発生します。
- 単一のライセンスが現在適用されている台数が、そのライセンスが対応している合計台数の 100 ～ 110% である場合、重要度が「**警告**」のイベントが発生します。
- If the number of currently used units covered by a single license exceeds 110% of the total number of units covered by the license, the event is published with the **Critical event** importance level.

アーキテクチャ

このセクションでは、Kaspersky Security Center のコンポーネントとコンポーネント間の連携について説明します。



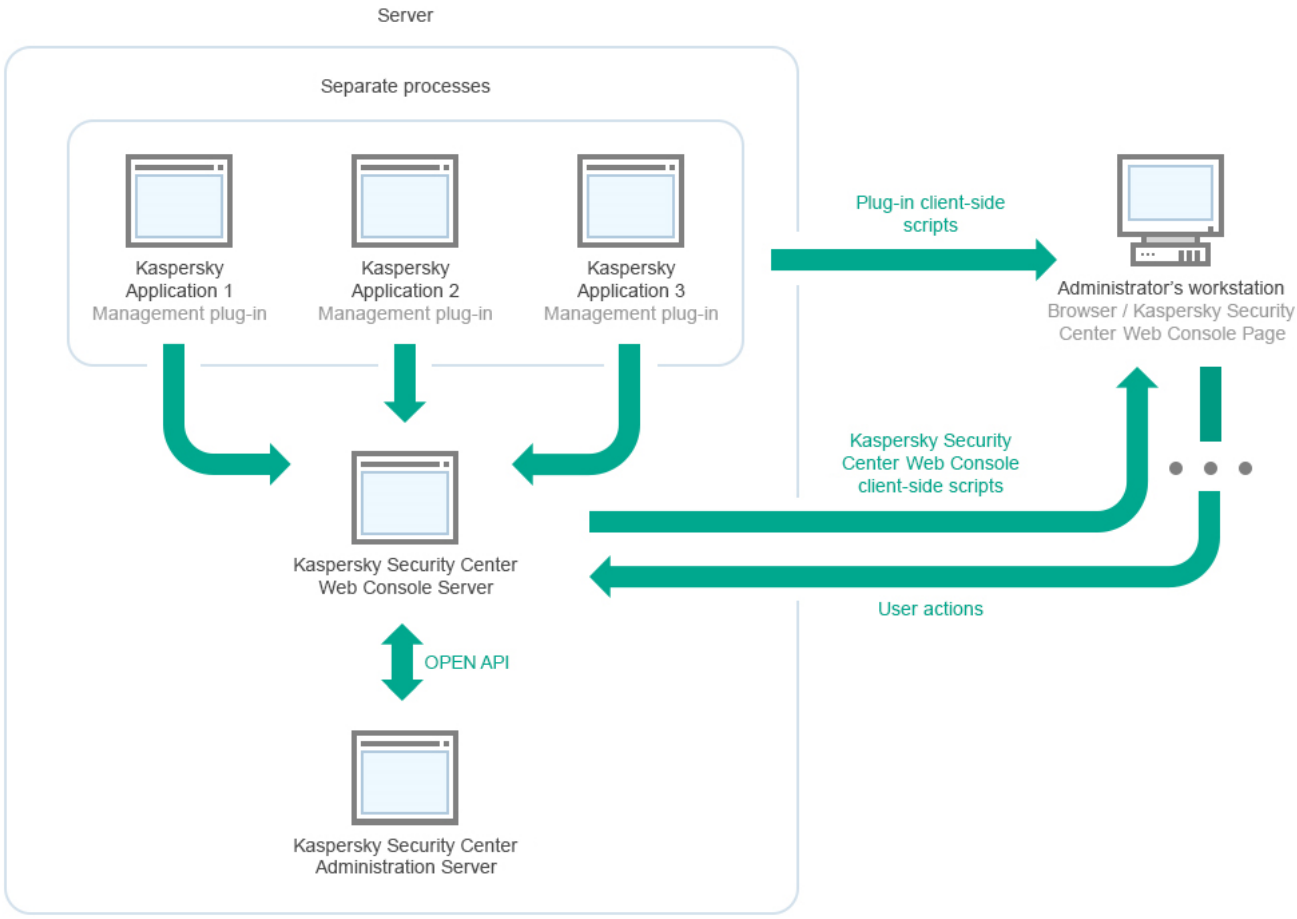
Kaspersky Security Center 14 Linux のアーキテクチャ

Kaspersky Security Center 14 Linux は主に次のコンポーネントで構成されています：

- **Kaspersky Security Center 14 Web コンソール**。Kaspersky Security Center により管理されているクライアント組織のネットワークの保護システムの構築や管理が可能な Web インターフェイスです。
- **Kaspersky Security Center 管理サーバー**（以降「サーバー」とも表記）：組織のネットワークにインストールされているアプリケーションおよびその管理方法に関する情報を一元的に保管します。
- **カスペルスキーのアップデートサーバー**：カスペルスキーの HTTP サーバーで、カスペルスキー製品はこれらのサーバーから定義データベースやソフトウェアモジュールのアップデートをダウンロードします。
- **クライアントデバイス：**Kaspersky Security Center 14 Linux によって保護されているクライアント企業のデバイス。保護する必要がある各デバイスには、カスペルスキーのセキュリティ製品のいずれかがインストールされている必要があります。

Kaspersky Security Center 管理サーバーと Kaspersky Security Center 14 Web コンソールの導入図

Kaspersky Security Center 管理サーバーと Kaspersky Security Center 14 Web コンソールの導入図を示します。



Kaspersky Security Center 管理サーバーと Kaspersky Security Center 14 Web コンソールの導入図

保護対象デバイスにインストールされているカスペルスキー製品の管理プラグイン（1つの製品ごとに1つの管理プラグイン）は、Kaspersky Security Center 14 Web コンソールサーバーがインストールされているサーバーに導入されます。

管理者ユーザーは、自分が使用しているワークステーションのブラウザーを使用して Kaspersky Security Center 14 Web コンソールにアクセスします。

Kaspersky Security Center 14 Web コンソールで個別の操作を実行すると、Kaspersky Security Center 14 Web コンソールサーバーが OpenAPI を通して Kaspersky Security Center 管理サーバーと通信を行います。Kaspersky Security Center 14 Web コンソールサーバーは Kaspersky Security Center 管理サーバーに必要な情報のリクエストを送信し、Kaspersky Security Center 14 Web コンソールでの操作結果を表示します。

Kaspersky Security Center Linux で使用するポート

下記の表に、管理サーバーとクライアントデバイスで開く必要のある既定のポートを示します。必要に応じて、既定のポート番号を変更できます。

Kaspersky Security Center Linux の管理サーバーで使用するポート

ポート番号	ポートを開くプロセスの名前	プロトコル	ポートの目的	範囲
8060	klcsweb	TCP	公開済みインストールパッケージをクライアントデバイスに送信する	インストールパッケージの公開 対象となる既定のポート番号は、管理サーバーのプロパティの［**Web サーバー**］セクションで変更できます。
8061	klcsweb	TCP (TLS)	公開済みインストールパッケージをクライアントデバイスに送信する	インストールパッケージの公開 対象となる既定のポート番号は、管理サーバーのプロパティの［**Web サーバー**］セクションで変更できます。
13000	klserver	TCP (TLS)	ネットワークエージェントおよびセカンダリ管理サーバーからの接続の受信、セカンダリ管理サーバーでのプライマリ管理サーバーからの接続の受信（セカンダリ管理サーバーが DMZ にある場合など）	クライアントデバイスとセカンダリ管理サーバーの管理 ネットワークエージェントから接続を受信する既定のポートの番号は、Kaspersky Security Center Linux のインストール中、接続ポートを設定する時に変更できます。セカンダリ管理サーバーから接続を受信する既定のポートの番号は、管理サーバーの階層を作成する時に変更できます。
13000	klserver	UDP	ネットワークエージェントからオフにされたデバイスに関する情報を受信する	クライアントデバイスの管理。 対象となる既定のポート番号はネットワークエージェントのポリシー設定で変更できます。
13299	klserver	TCP (TLS)	Kaspersky Security Center 14 Web コンソールから管理サーバーへの接続を受信する、OpenAPI 経由での管理サーバーへの接続を受信する	Kaspersky Security Center 14 Web コンソール、OpenAPI 既定のポート番号は、管理サーバーのプロパティ（［**全般**］の［**接続ポート**］サブセクション）、または管理サーバーの階層の作成時に変更することができます。
14000	klserver	TCP	ネットワークエージェントから接続を受信する	クライアントデバイスの管理。 既定のポート番号は、Kaspersky Security Center Linux のインストール中の接続ポートの設定時または管理サーバーにクライアントデバイスを手動で接続する際に変更できます。
13111（KSN プロキシサービスがデバイスで実行されてい	ksnproxy	TCP	管理対象デバイスから KSN プロキシサーバーへの要求を受信する	KSN プロキシサーバー。 対象となる既定のポート番号は管理サーバーのプロパティで変更できます。

る場合のみ）				
15111（KSNプロキシサービスがデバイスで実行されている場合のみ）	ksnproxy	UDP	管理対象デバイスから KSN プロキシサーバーへの要求を受信する	KSN プロキシサーバー。 対象となる既定のポート番号は管理サーバーのプロパティで変更できます。
17000	klactprx	TCP (TLS)	管理対象デバイスから製品のアクティベーション用の接続を受信する	管理対象デバイス用のアクティベーションプロキシサーバー。 既定のポート番号は、管理サーバーのプロパティウィンドウ（［**全般**］セクションの［**追加のポート**］サブセクション）で変更できます。
19170	klserver	HTTPS (TLS)	klsctunnel ユーティリティを使用した管理対象デバイスへの接続のトンネリング	Kaspersky Security Center 14 Web コンソールを使用した管理対象デバイスへのリモート接続。 klscflag ユーティリティを使用して既定のポート番号を変更できます。

管理サーバーとデータベースを異なるデバイス上にインストールする場合、データベースを配置したデバイス上で必要なポートを使用可能な状態に設定する必要があります（例：MariaDB Server 用のポート 3306など）。関連する情報については、DBMS のドキュメントを参照してください。

下記の表に、Kaspersky Security Center 14 Web コンソールサーバーで開く必要のある既定のポートを示します。管理サーバーがインストールされている同じデバイスでも、別のデバイスでも問題ありません。

Kaspersky Security Center 14 Web コンソールサーバーで使用するポート

ポート番号	ポートを開くプロセスの名前	プロトコル	ポートの目的	範囲
8080	Node.js: Server-side JavaScript	TCP (TLS)	ブラウザーから Kaspersky Security Center 14 Web コンソールへの接続を受信する	Kaspersky Security Center 14 Web コンソール。 Kaspersky Security Center 14 Web コンソールのインストール時に、既定のポート番号を変更できます。Linux ALT オペレーティングシステム上に Kaspersky Security Center 14 Web コンソールをインストールする場合、ポート番号 8080 はオペレーティングシステムによって使用されているため、ポート番号には 8080 以外の数字を指定する必要があります。

下記の表に、ネットワークエージェントがインストールされている管理対象デバイスの管理で開く必要のある既定のポートを示します。

ネットワークエージェントが使用するポート

ポート番号	ポートを開くプロセスの名前	プロトコル	ポートの目的	範囲

15000	klnagent	UDP	管理サーバーからネットワークエージェントへの管理信号	クライアントデバイスの管理。 対象となる既定のポート番号はネットワークエージェントのポリシー設定で変更できます。
15000	klnagent	UDP ブロードキャスト	同じブロードキャストドメイン内の他のネットワークエージェントに関するデータの取得（データは管理サーバーに送信されます）	アップデートおよびインストールパッケージの提供。
15001	klnagent	UDP	ディストリビューションポイント（使用している場合）からマルチキャスト要求を受信する	ディストリビューションポイントからアップデートとインストールパッケージを受信する。 既定のポート番号は、ディストリビューションポイントのプロパティで変更できます。

klnagent プロセスは、エンドポイントオペレーティングシステムの動的ポート範囲から空きポートを要求することもできます。これらのポートは、オペレーティングシステムによって自動的に klnagent プロセスに割り当てられるため、klnagent プロセスは別のソフトウェアで使用されている一部のポートを使用できます。klnagent プロセスがそのソフトウェアの動作に影響を与える場合は、このソフトウェアのポート設定を変更するか、オペレーティングシステムの既定の動的ポート範囲を変更して、影響を受けるソフトウェアに使用されるポートを除外します。

下記の表に、ディストリビューションポイントとして動作するネットワークエージェントがインストールされたデバイスで開く必要がある既定のポートを示します。ネットワークエージェントで使用されるポートに加えて、リストにあるポートをディストリビューションポイントデバイスで開いておく必要があります（上記の表を参照）。

ディストリビューションポイントとして動作するネットワークエージェントが使用するポート

ポート番号	ポートを開くプロセスの名前	プロトコル	ポートの目的	範囲
13000	klnagent	TCP (TLS)	ネットワークエージェントから接続を受信する	クライアントデバイスの管理、アップデートおよびインストールパッケージの提供。 既定のポート番号は、ディストリビューションポイントのプロパティで変更できます。
13111（KSN プロキシサービスがデバイスで実行されている場合のみ）	ksnproxy	TCP	管理対象デバイスから KSN プロキシサーバーへの要求を受信する	KSN プロキシサーバー。 既定のポート番号は、ディストリビューションポイントのプロパティで変更できます。
15111（KSN プロキシサービスがデバイスで実行されている場合のみ）	ksnproxy	UDP	管理対象デバイスから KSN プロキシサーバーへの要求を受信する	KSN プロキシサーバー。 既定のポート番号は、ディストリビューションポイントのプロパティで変更できます。

Kaspersky Security Center 14 Web コンソールで使用されるポート

下表には、Kaspersky Security Center 14 Web コンソールサーバー（単に「Kaspersky Security Center 14 Web コンソール」とも表記）がインストールされたデバイスで開放しておく必要があるポートが一覧で表示されています。

Kaspersky Security Center 14 Web コンソールで使用されるポート

ポート番号	サービス名	プロトコル	ポートの目的	範囲
2001	KSCWebConsolePlugin	HTTPS	管理プラグインのプロセスが KSCWebConsoleManagementService からのリクエストを受信するために使用される API ポート	管理プラグインの node プロセスの実行
1329、2003	KSCWebConsoleManagementService	HTTPS	同一のデバイスで実行中のサービス KSCWebConsole からのリクエストを受信するために使用される API ポート	Kaspersky Security Center 14 Web コンソールコンポーネントのアップデート
2005	KSCWebConsole	HTTPS	同一のデバイスで実行中のサービス KSCWebConsoleManagementService からのリクエストを受信するために使用される API ポート	Kaspersky Security Center 14 Web コンソールのノードプロセスの実行
8200	—	HTTP	HashiCorp Vault を使用して証明書を生成するために使用される API ポート（詳細については、HashiCorp Vault の Web サイトを参照してください）	Kaspersky Security Center 14 Web コンソールのインストールと Kaspersky Security Center 14 Web コンソールコンポーネントのアップデート
4150、4151、4152	KSCWebConsoleMessageQueue	HTTPS	Kaspersky Security Center 14 Web コンソールと管理プラグインの処理間で発生する通信に使用されるメッセージブローカーの API ポート	Kaspersky Security Center 14 Web コン

				ソールと管理プラグインとの対話

インストール

このセクションでは、Kaspersky Security Center と Kaspersky Security Center 14 Web コンソールのインストールについて説明しています。

主要なインストールシナリオ

このシナリオに従うことで、Kaspersky Security Center 14 Linux 管理サーバーと Kaspersky Security Center 14 Web コンソールのインストール、クイックスタートウィザードを使用した管理サーバーの初期セットアップ、および製品導入ウィザードを使用した管理対象デバイスへのカスペルスキー製品のインストールが実行できます。

必須条件

Kaspersky Endpoint Security for Business のライセンス（アクティベーションコード）またはカスペルスキーセキュリティ製品のライセンス（アクティベーションコード）を持っている必要があります。

Kaspersky Security Center 14 Linux を試用版で使用する場合は、カスペルスキーの Web サイトで 30 日間有効な試用版を取得できます。

実行するステップ

主要なインストールシナリオは、次の手順で進みます：

1. **組織を保護する仕組みの選択**

   Kaspersky Security Center Linux コンポーネントの詳細をご確認ください。分散ネットワークを運用している場合、ネットワークの設定と通信チャネルのスループットに基づき、使用する管理サーバーの数と、使用する管理サーバーを組織内で分配すべき方法を定義します。

   管理サーバーの階層を使用するかどうかを定義します。これを定義するには、すべてのクライアントデバイスを 1 台の管理サーバーでカバーすることが可能かつ有益か、または管理サーバーの階層を構築することが必要か、いずれかを評価する必要があります。また、保護対象のネットワークが属する組織の組織構造と同一の管理サーバーの階層を構築する必要がある場合があります。

2. **カスタム証明書を使用するための準備**

   組織の公開鍵インフラストラクチャ（PKI）で、特定の認証局（CA）によって発行されたカスタム証明書を使用する必要がある場合は、それらの証明書を準備し、すべての要件を満たしていることを確認してください。

3. **DBMS（データベース管理システム）のインストール**

   Kaspersky Security Center 用の DBMS（データベース管理システム）をインストールするか、既存の DBMS を使用します。

4. **ポートの設定**

   選択したセキュリティ構造に従ったコンポーネント間の対話に必要なすべてのポートが開いていることを確認します。

   インターネットアクセスを管理サーバーに提供する必要がある場合、ネットワーク設定に応じてポートを設定し、接続設定を指定します。

5. **Kaspersky Security Center のインストール**

管理サーバーとして使用する Linux デバイスを選択します。このデバイスがシステム要件を満たしていることを確認してから Kaspersky Security Center をデバイスにインストールします。サーバー向けネットワークエージェントが、管理サーバーとともに自動的にインストールされます。

6 Kaspersky Security Center 14 Web コンソールと管理プラグインのインストール

管理者のワークステーションとして使用する Linux デバイスを選択します。このデバイスがシステム要件を満たしていることを確認してから Kaspersky Security Center 14 Web コンソールをデバイスにインストールします。Kaspersky Security Center 14 Web コンソールは、管理サーバーがインストールされている同じデバイスまたは別のデバイスにインストールできます。

Kaspersky Endpoint Security for Linux 管理 Web プラグインをダウンロードしてから Kaspersky Security Center 14 Web コンソールがインストールされているものと同じデバイスにインストールします。

7 管理サーバーデバイスへの Kaspersky Endpoint Security for Linux およびネットワークエージェントのインストール

既定では、管理サーバーデバイスは管理対象デバイスとして認識されません。管理サーバーをウイルスやその他の脅威から保護し、またそのデバイスをその他の管理対象デバイス同様に管理するには、Kaspersky Endpoint Security for Linux および Linux 向けネットワークエージェントを管理サーバーデバイスにインストールすることをお勧めします。この場合、Linux 向けネットワークエージェントは、管理サーバーと一緒にインストールしたサーバー版のネットワークエージェントとは別にインストールされ、動作します。

8 初期セットアップの実行

管理サーバーのインストールが完了すると、管理サーバーへの最初の接続時にクイックスタートウィザードが自動的に開始します。既存要件に従って、管理サーバーの初期設定を行います。初期設定段階中に、ウィザードが既定値設定を使用して、保護の導入に必要なポリシーとタスクを作成します。しかしながら、既定の設定は組織のニーズに対して十分ではない場合があります。必要に応じて、ポリシーやタスクの設定を編集できます。

9 ネットワーク上のデバイスの検出

デバイスを手動で検出します。Kaspersky Security Center Linux は、ネットワークで検出されたすべてのデバイスのアドレスと名前を受信します。その後、Kaspersky Security Center Linux を使用してカスペルスキー製品と他社製ソフトウェアを、検出されたデバイスにインストールできます。Kaspersky Security Center Linux はデバイスの検索を定期的に開始するため、新しいインスタンスがネットワークに現れると、それらのインスタンスは自動的に検出されます。

10 管理グループ内へのデバイスの配置

一部のケースでは、ネットワーク接続デバイスへ最も便利な方法で保護を導入する目的で、組織の構造を考慮してデバイスのプール全体を管理グループに分割しなければならない場合があります。グループにデバイスを配置する移動ルールを作成するか、デバイスを手動で配置することができます。管理グループへのグループタスクの割り当て、ポリシーの範囲の定義、およびディストリビューションポイントの割り当てが可能です。

すべての管理対象デバイスが適切な管理グループに正しく割り当てられ、ネットワーク上に未割り当てデバイスが存在しないことを確認します。

11 ディストリビューションポイントの割り当て

管理グループにディストリビューションポイントが自動的に割り当てられますが、必要に応じて手動で割り当てることもできます。大規模なネットワークにはディストリビューションポイントを使用することを推奨します。その理由は、低いスループットレートのチャネルを介して通信するデバイス（またはデバイスグループ）へのアクセスを管理サーバーに提供するために使用する分散構造ネットワーク上、および管理サーバーで、負荷を減らすためです。

12 ネットワーク接続されたデバイスへのネットワークエージェントとセキュリティ製品のインストール

企業ネットワークへの保護の導入時には、デバイス検出中に管理サーバーによって検出されたデバイスにネットワークエージェントとセキュリティ製品をインストールする必要があります。

リモートで製品をインストールするには、製品導入ウィザードを実行します。

セキュリティ製品は、脅威をもたらすウイルスなどのプログラムからデバイスを保護します。ネットワークエージェントは、デバイスと管理サーバー間の通信が確実に行われるようにします。ネットワークエージェントは自動的に設定されるようになっています。

ネットワーク接続されたデバイスへのネットワークエージェントとセキュリティ製品のインストールを開始する前に、それらのデバイスがアクセス可能である（電源が入っている）ことを確認してください。

13. **ライセンスのクライアントデバイスへの導入**

    クライアントデバイスにライセンスを導入し、デバイス上の管理対象セキュリティ製品をアクティベートします。

14. **カスペルスキー製品のポリシーの設定**

    異なるデバイスに異なる設定を適用するには、デバイスベースのセキュリティ管理とユーザーベースのセキュリティ管理を使用できます。デバイスベースのセキュリティ管理は、ポリシーとタスクを使用することで実施できます。タスクは特定の条件を満たすデバイスに対してのみ適用できます。デバイスのフィルター処理の条件を設定するには、デバイスの抽出とタグを使用します。

15. **ネットワーク保護ステータスの監視**

    ダッシュボードにあるウィジェットを使用したネットワーク監視、カスペルスキー製品からのレポートの生成、管理対象デバイス上のアプリケーションから受信したイベントの抽出の設定と表示、通知リストの表示ができます。

DBMS（データベース管理システム）のインストール

Kaspersky Security Center で使用する DBMS（データベース管理システム）をインストールします。サポート対象の DBMS のいずれかを選択します。

選択した DBMS のインストール方法については、該当製品のマニュアルを参照してください。

MariaDB を使用する場合は、DBMS と Kaspersky Security Center が最適な状態で動作するため、推奨される設定を指定する必要があります。

Kaspersky Security Center Linux 14 と動作する MariaDB x64 サーバーの設定

Kaspersky Security Center に MariaDB サーバーを使用する場合、InnoDB および MEMORY ストレージおよび UTF-8 と UCS-2 のエンコーディングのサポートを有効にします。

my.cnf ファイルの推奨設定

my.cnf ファイルを設定するには：

1. テキストエディターで my.cnf ファイルを開きます。

2. my.cnf ファイルに次の行を入力します：

```
sort_buffer_size=10M
join_buffer_size=100M
join_buffer_space_limit=300M
join_cache_level=8
tmp_table_size=512M
max_heap_table_size=512M
```

```
key_buffer_size=200M
innodb_buffer_pool_size= <値>
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
```

`Innodb_buffer_pool_size` の値は、想定される KAV データベースのサイズの 80% 以上に設定する必要があります。指定されたメモリは、サーバーの起動時に割り当てられることに注意してください。データベースのサイズが指定されたバッファサイズより小さい場合、必要なメモリのみが割り当てられます。MariaDB 10.4.3 以前を使用する場合、割り当てられたメモリの実際のサイズは、指定されたバッファー サイズよりも約 10% 大きくなります。

このパラメータの値を「1」または「2」にすると MariaDB の動作速度に悪影響を及ぼす可能性があるため、パラメータには「`innodb_flush_log_at_trx_commit=0`」を使用してください。

既定では、オプティマイザのアドオン「`join_cache_incremental`、「`join_cache_hashed`」、「`join_cache_bka`」は有効になっています。 これらのアドオンが無効になっている場合は、有効にする必要があります。

オプティマイザのアドオンが有効になっているかどうかを確認するには：

1. MariaDB クライアントコンソールで、次のコマンドを実行してください：

   ```
   SELECT @@optimizer_switch;
   ```

2. 出力に次の行が含まれていることを確認します：

   ```
   join_cache_incremental=on
   join_cache_hashed=on
   join_cache_bka=on
   ```

   これらの行が存在して値に「on」が指定されている場合は、オプティマイザのアドオンは有効です。

   これらの行が存在しない、または値に「`off`」が指定されている場合は、以下を実行する必要があります：

   a. テキストエディターで my.cnf ファイルを開きます。

   b. 次の行を my.cnf ファイルに追加します：

   ```
   optimizer_switch='join_cache_incremental=on'
   optimizer_switch='join_cache_hashed=on'
   optimizer_switch='join_cache_bka=on'
   ```

アドオン「`join_cache_incremental`」、「`join_cache_hash`」および「`join_cache_bka`」が有効になりました。

Kaspersky Security Center のインストール

Kaspersky Security Center をインストールする方法について説明します。

インストールする前に：

- DBMS（データベース管理システム）をインストールします。

- Kaspersky Security Center をインストールするデバイスで、サポート対象の Linux ディストリビューション を使用していることを確認します。

デバイスにインストールされている Linux ディストリビューションに応じて、「ksc64_[バージョン番号]_amd64.deb」または「 ksc64-[バージョン番号].x86_64.rpm」のいずれかのインストールファイルを使用してください。インストールファイルは、カスペルスキーの Web サイトからダウンロードして取得できます。

Kaspersky Security Center をインストールするには：

1. コマンドラインで、ルート権限を持つアカウントを使用してこの手順にあるコマンドを実行します。

2. グループ「kladmins」と特権のないアカウント「ksc」を作成します。このアカウントは「kladmins」グループに属するメンバーである必要があります。このためには、次のコマンドを順に実行します：

   ```
   # adduser ksc
   # groupadd kladmins
   # gpasswd -a ksc kladmins
   # usermod -g kladmins ksc
   ```

3. Kaspersky Security Center のインストールを実行します。Linux ディストリビューションに応じて、次のコマンドを実行します：

   - `# apt install /<path>/ksc64_[` バージョン番号 `]_amd64.deb`

   - `# yum install /<path>/ksc64-[` バージョン番号 `].x86_64.rpm -y`

4. Kaspersky Security Center の設定を実行します：

   ```
   # /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

5. 使用許諾契約書（EULA）およびプライバシーポリシーを読みます。テキストはコマンドラインウィンドウに表示されます。次のテキストセグメントを表示するにはスペースキーを押します。確認が表示されてから次の値を入力します：

   a. EULA の内容を確認して同意する場合は「y」を入力します。EULA の内容に同意しない場合は「n」を入力します。Kaspersky Security Center を使用するには、EULA の内容に同意する必要があります。

   b. プライバシーポリシーの内容を確認して同意し、またデータがプライバシーポリシーに記載される方法で処理されて送信されること（第三国への送信を含む）に同意する場合は「y」を入力します。プライバシーポリシーの内容に同意しない場合は「n」を入力します。Kaspersky Security Center を使用するには、プライバシーポリシーの内容に同意する必要があります。

6. 確認が表示されてから次の設定を入力します：

   a. 管理サーバーの DNS 名または静的 IP アドレスを入力します。

   b. 管理サーバーのポート番号を入力します。既定では、ポート 14000 が使用されます。

   c. 管理サーバーの SSL ポート番号を入力します。既定では、ポート 13000 が使用されます。

   d. 管理するデバイスの概数を見積もります：

      - ネットワーク上のデバイス数が 1～100 の場合は、「1」を入力します。

      - ネットワーク上のデバイス数が 101～1000 の場合は、「2」を入力します。

      - ネットワーク上のデバイス数が 1000 以上の場合は、「3」を入力します。

e. サービス用のセキュリティグループ名を入力します。既定では、「kladmins」グループが使用されます。

f. 管理サーバーサービスを開始するアカウント名を入力します。アカウントは入力したセキュリティグループのメンバーである必要があります。既定では「ksc」アカウントが使用されます。

g. その他のサービスを開始するアカウント名を入力します。アカウントは入力したセキュリティグループのメンバーである必要があります。既定では「ksc」アカウントが使用されます。

h. データベースがインストールされるデバイスの IP アドレスを入力します。

i. データベースのポート番号を入力します。このポートは管理サーバーとの通信に使用されます。既定では、ポート 3306 が使用されます。

j. データベースの名前を入力します。

k. データベースへのアクセスに使用するデータベースのルートアカウントのログイン名を入力します。

l. データベースへのアクセスに使用するデータベースのルートアカウントのパスワードを入力します。

サービスが追加され自動的に開始されるまで待ちます。

- `klnagent_srv`
- `kladminserver_srv`
- `klactprx_srv`
- `klwebsrv_srv`

m. 管理サーバーの管理者とするアカウントを作成します。ユーザー名とパスワードを入力します。

パスワードは次のルールに従う必要があります：

- ユーザーパスワードは 8 文字以上 16 文字以下である必要があります。
- パスワードでは、次の文字種別のうち 3 つ以上を組み合わせてください。
  - アルファベット大文字（A-Z）
  - アルファベット小文字（a-z）
  - 数字（0 - 9）
  - 特殊文字（@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;）

ユーザーが追加され、Kaspersky Security Center がインストールされます。

サービスの検証

サービスが実行されているかどうかを確認するには、次のコマンドを実行します：

- `# systemctl status klnagent_srv.service`
- `# systemctl status kladminserver_srv.service`

- `# systemctl status klactprx_srv.service`
- `# systemctl status klwebsrv_srv.service`

Kaspersky Security Center をサイレント モードでインストールする

Kaspersky Security Center を Linux デバイスにインストールするには、応答ファイルを使用してサイレント（非対話型）モードで、つまりユーザーの参加なしでインストールを実行します。応答ファイルには、インストールパラメータのカスタムセット（変数とそれぞれの値）が含まれています。

インストールする前に：

- DBMS（データベース管理システム）をインストールします。
- Kaspersky Security Center をインストールするデバイスで、サポート対象の Linux ディストリビューション を使用していることを確認します。

Kaspersky Security Center をサイレントモードでインストールするには：

1. 使用許諾契約書をお読みください。次の手順は、使用許諾契約書の内容を理解して条項に同意する場合にのみ使用してください。
2. グループ「kladmins」および非特権アカウント「ksc」を作成します。これは「kladmins」グループのメンバーである必要があります。これを行うには、ルート権限を持つアカウントで次の順番でコマンドを実行します：
   ```
   # adduser ksc
   # groupadd kladmins
   # gpasswd -a ksc kladmins
   # usermod -g kladmins ksc
   ```
3. 応答ファイル（TXT 形式）を作成し、変数のリストを `VARIABLE_NAME=variable_value` 形式で応答ファイルに追加します。1 行に 1 つずつ追加します。応答ファイルには、次の表に示す変数を含める必要があります。
4. たとえば、次のコマンドを使用して、パスを含む応答ファイルの完全な名前を含むルート環境で `KLAUTOANSWERS` 環境変数の値を設定します：

   ```
   export KLAUTOANSWERS=/tmp/ksc_install/answers.txt
   ```
5. Kaspersky Security Center のインストールをサイレントモードで実行します。Linux ディストリビューションに応じて、次のいずれかのコマンドを実行します：
   - `# apt install /<path>/ksc64_[` バージョン番号 `]_amd64.deb`
   - `# yum install /<path>/ksc64-[` バージョン番号 `].x86_64.rpm -y`
6. Kaspersky Security Center 14 Web コンソールで作業するユーザーを作成します。これを行うには、ルート権限を持つアカウントで次のコマンドを実行します：

   `/opt/kaspersky/ksc64/sbin/kladduser -n ksc -p <password>` では、パスワードには少なくとも 8 文字が含まれている必要があります。

   -

サイレントモードでの Kaspersky Security Center インストールのパラメータとして使用される応答ファイルの変数

変数名	必須	説明	指定可能
EULA_ACCEPTED	使用する	使用許諾契約書を理解した上で条項に同意することを確認します。	1
PP_ACCEPTED	使用する	プライバシーポリシーの条件を理解し、同意することを確認します。	1
KLSRV_UNATT_SERVERADDRESS	使用する	管理サーバーの DNS 名または静的 IP アドレス。	DNS 名または ス
KLSRV_UNATT_PORT_SRV	使用しない	管理サーバーのポート番号。オプショナル型の既定値は 14000 です。	ポート番号
KLSRV_UNATT_PORT_SRV_SSL	使用しない	管理サーバーの SSL ポート番号。オプショナル型の既定値は 13000 です。	ポート番号
KLSRV_UNATT_PORT_KLOAPI	使用しない	管理サーバーの KLOAPI ポート番号。オプショナル型の既定値は 13299 です。	ポート番号
KLSRV_UNATT_PORT_GUI	使用しない	管理サーバーの GUI ポート番号。オプショナル型の既定値は 13291 です。	ポート番号
KLSRV_UNATT_NETRANGETYPE	使用しない	管理するデバイスの概数。オプショナル型の既定値は 1 です。	1 ～ 100 のネ デバイスの場 101 ～ 1000 台 ークデバイス 2 。1000 を トワークデバ は 3。
KLSRV_UNATT_DBMS_INSTANCE	使用する	データベースサーバーの IP アドレス。	IP アドレス
KLSRV_UNATT_DBMS_PORT	使用する	データベースサーバーのポート。	3306
KLSRV_UNATT_DB_NAME	使用する	データベースの名前。	kav
KLSRV_UNATT_DBMS_LOGIN	使用する	データベースにアクセスできるユーザーのユーザー名。	
KLSRV_UNATT_DBMS_PASSWORD	使用する	データベースにアクセスできるユーザーのパスワード。	
KLSRV_UNATT_KLADMINSGROUP	使用する	サービス用のセキュリティグループ名。	kladmins
KLSRV_UNATT_KLSRVUSER	使用する	管理サーバーサービスを開始するアカウント名。アカウントは、KLSRV_UNATT_KLADMINSGROUP 変数で指定されたセキュリティグループのメンバーである必要があります。	ksc
KLSRV_UNATT_KLSVCUSER	使用する	その他のサービスを開始するアカウント名。アカウントは、KLSRV_UNATT_KLADMINSGROUP 変	ksc

		数で指定されたセキュリティグループのメンバーである必要があります。	
管理サーバーを Kaspersky フェールオーバークラスターとして展開する場合は、応答ファイルに次の追加る必要があります：			
KLFOC_UNATT_NODE	使用する	ノード番号（1 または 2）。	1 または 2
KLFOC_UNATT_STATE_SHARE_MOUNT_PATH	使用する	状態共有のマウントポイント。	
KLFOC_UNATT_DATA_SHARE_MOUNT_PATH	使用する	データ共有のマウントポイント。	
KLFOC_UNATT_CONN_MODE	使用する	フェールオーバークラスターの接続モード。	VirtualAdap または ExternalLoa
KLFOC_UNATT_CONN_MODE 変数に VirtualAdapter 値がある場合、応答ファイルには次の追加変数を含めあります：			
KLFOC_UNATT_CONN_MODE_VA_NAME	これらの変数のいずれかが必要です	仮想ネットワークアダプター名。	
KLFOC_UNATT_CONN_MODE_VA_IPV4		仮想ネットワークアダプターの IP アドレス。	IP アドレス
KLFOC_UNATT_CONN_MODE_VA_IPV6		仮想ネットワークアダプターの IPv6 アドレス。	IPv6 アドレス

Kaspersky Security Center をクローズド ソフトウェア環境モードで Astra Linux にインストールする

このセクションでは、Astra Linux Special Edition オペレーティング システムにKaspersky Security Centerをインストールする方法について説明します。

インストールする前に：

- DBMS（データベース管理システム）をインストールします。
- Kaspersky Security Center をインストールするデバイスで、サポート対象の Linux ディストリビューションを使用していることを確認します。
- kaspersky_astra_pub_key.gpg アプリケーション キーを取得するには、テクニカル サポートにお問い合わせください。

ksc64_[version_number]_amd64.deb インストール ファイルを使用します。インストールファイルは、カスペルスキーの Web サイトからダウンロードして取得できます。

コマンドラインで、ルート権限を持つアカウントを使用してこの手順にあるコマンドを実行します。

Kaspersky Security Center を Astra Linux Special Edition (運用アップデート 1.7) および Astra Linux Special Edition (運用アップデート 1.6) オペレーティング システムにインストールするには、次の手順を実行します。

1. /etc/digsig/digsig_initramfs.conf ファイルで次の設定を指定します。

   ```
   DIGSIG_ELF_MODE=1
   ```

2. 互換性パッケージをインストールします。

   ```
   apt install astra-digsig-oldkeys
   ```

3. アプリケーション キーのディレクトリを作成します。

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

4. 前の手順で作成したディレクトリでアプリケーション キーを見つけます。

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

5. RAM ディスクを更新します。

   ```
   update-initramfs -u -k すべて
   ```

6. グループ「kladmins」と特権のないアカウント「ksc」を作成します。このアカウントは「kladmins」グループに属するメンバーである必要があります。このためには、次のコマンドを順に実行します：

   ```
   # adduser ksc
   # groupadd kladmins
   # gpasswd -a ksc kladmins
   # usermod -g kladmins ksc
   ```

7. Kaspersky Security Center のインストールを実行します：

   - `# apt install /<path>/ksc64_[ バージョン番号 ]_amd64.deb`

8. Kaspersky Security Center の設定を実行します：

   ```
   # /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

9. 使用許諾契約書（EULA）およびプライバシーポリシーを読みます。テキストはコマンドラインウィンドウに表示されます。次のテキストセグメントを表示するにはスペースキーを押します。確認が表示されてから次の値を入力します：

   a. EULA の内容を確認して同意する場合は「y」を入力します。EULA の内容に同意しない場合は「n」を入力します。Kaspersky Security Center を使用するには、EULA の内容に同意する必要があります。

   b. プライバシーポリシーの内容を確認して同意し、またデータがプライバシーポリシーに記載される方法で処理されて送信されること（第三国への送信を含む）に同意する場合は「y」を入力します。プライバシーポリシーの内容に同意しない場合は「n」を入力します。Kaspersky Security Center を使用するには、プライバシーポリシーの内容に同意する必要があります。

10. 確認が表示されてから次の設定を入力します：

    a. 管理サーバーの DNS 名または静的 IP アドレスを入力します。

    b. 管理サーバーのポート番号を入力します。既定では、ポート 14000 が使用されます。

c. 管理サーバーの SSL ポート番号を入力します。既定では、ポート 13000 が使用されます。

d. 管理するデバイスの概数を見積もります：

- ネットワーク上のデバイス数が 1 ～ 100 の場合は、「1」を入力します。
- ネットワーク上のデバイス数が 101 ～ 1000 の場合は、「2」を入力します。
- ネットワーク上のデバイス数が 1000 以上の場合は、「3」を入力します。

e. サービス用のセキュリティグループ名を入力します。既定では、「kladmins」グループが使用されます。

f. 管理サーバーサービスを開始するアカウント名を入力します。アカウントは入力したセキュリティグループのメンバーである必要があります。既定では「ksc」アカウントが使用されます。

g. その他のサービスを開始するアカウント名を入力します。アカウントは入力したセキュリティグループのメンバーである必要があります。既定では「ksc」アカウントが使用されます。

h. データベースがインストールされるデバイスの IP アドレスを入力します。

i. データベースのポート番号を入力します。このポートは管理サーバーとの通信に使用されます。既定では、ポート 3306 が使用されます。

j. データベースの名前を入力します。

k. データベースへのアクセスに使用するデータベースのルートアカウントのログイン名を入力します。

l. データベースへのアクセスに使用するデータベースのルートアカウントのパスワードを入力します。

サービスが追加され自動的に開始されるまで待ちます。

- `klnagent_srv`
- `kladminserver_srv`
- `klactprx_srv`
- `klwebsrv_srv`

m. 管理サーバーの管理者とするアカウントを作成します。ユーザー名とパスワードを入力します。

パスワードは次のルールに従う必要があります：

- ユーザーパスワードは 8 文字以上 16 文字以下である必要があります。
- パスワードでは、次の文字種別のうち 3 つ以上を組み合わせてください。
  - アルファベット大文字（A-Z）
  - アルファベット小文字（a-z）
  - 数字（0 - 9）
  - 特殊文字（@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;）

ユーザーが追加され、Kaspersky Security Center がインストールされます。

サービスの検証

サービスが実行されているかどうかを確認するには、次のコマンドを実行します：

- `# systemctl status klnagent_srv.service`
- `# systemctl status kladminserver_srv.service`
- `# systemctl status klactprx_srv.service`
- `# systemctl status klwebsrv_srv.service`

Kaspersky Security Center 14 Web コンソールのインストール

このセクションでは、Linux オペレーティングシステムを使用しているデバイスに Kaspersky Security Center 14 Web コンソールサーバー（単に「Kaspersky Security Center 14 Web コンソール」とも表記）をインストールする方法について説明しています。インストールの前に、データベース管理システムと Kaspersky Security Center 管理サーバーをインストールする必要があります。

デバイスにインストールされている Linux ディストリビューションに応じて、次のインストールファイルのいずれかを使用します：

- Debian の場合 — ksc-web-console-[ビルド番号].x86_64.deb
- RPM ベースのオペレーティングシステムの場合 — ksc-web-console-[ビルド番号].x86_64.rpm
- ALT 8 SP の場合 — ksc-web-console-[ビルド番号]-alt8p.x86_64.rpm

インストールファイルは、カスペルスキーの Web サイトからダウンロードして取得できます。

Kaspersky Security Center 14 Web コンソールをインストールするには：

1. Kaspersky Security Center 14 Web コンソールをインストールするデバイスで、サポート対象の Linux ディストリビューションを使用していることを確認します。
2. 使用許諾契約書（EULA）をお読みください。Kaspersky Security Center 配布キットに EULA のテキストを含む TXT ファイルが含まれていない場合は、カスペルスキーの Web サイトからファイルをダウンロードできます。使用許諾契約書の条項に同意しない場合は、製品をインストールすることはできません。
3. Kaspersky Security Center 14 Web コンソールを管理サーバーに接続するためのパラメータを入力した応答ファイルを作成します。ファイル名を「ksc-web-console-setup.json」とし、フォルダーに次のように配置します：/etc/ksc-web-console-setup.json

   最小限のパラメータと、既定のアドレスとポートの内容を記載した応答ファイルの作成例は次のようになります：

```
{
"address": "127.0.0.1",
"port": 8080,
"trusted":
"127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC
Server",
"acceptEula": true
}
```

Linux ALT オペレーティングシステム上に Kaspersky Security Center 14 Web コンソールをインストールする場合、ポート番号 8080 はオペレーティングシステムによって使用されているため、ポート番号には 8080 以外の数字を指定する必要があります。

同じ rpm インストールファイルを使用して Kaspersky Security Center 14 Web コンソールをアップデートすることはできません。応答ファイルの設定を変更し、変更後の応答ファイルを使用して Web コンソールの再インストールを行いたい場合、Web コンソールをまずアンインストールしてから変更後の応答ファイルを使用して再インストールを行います。

4. root 権限のあるアカウントでコマンドラインを使用し、Linux ディストリビューションに応じて拡張子が「.deb」または「.rpm」のセットアップファイルを実行します。

   - deb ファイルから Kaspersky Security Center 14 Web コンソールをインストールまたはアップグレードするには、次のコマンドを使用します：
     ```
     $ sudo dpkg -i ksc-web-console-[ビルド番号].x86_64.deb
     ```
   - 「.rpm」ファイルから Kaspersky Security Center 14 Web コンソールを実行するには、次のコマンドのいずれかを使用します：
     ```
     $ sudo rpm -ivh --nodeps ksc-web-console-[ビルド番号].x86_64.rpm
     ```
     または
     ```
     $ sudo alien -i ksc-web-console-[ビルド番号].x86_64.rpm
     ```
   - Kaspersky Security Center 14 Web コンソールを以前のバージョンからアップグレードするには、次のコマンドのいずれかを実行します：
     - RPM ベースのオペレーティングシステムのデバイスの場合：
       ```
       $ sudo rpm -Uvh --nodeps --force ksc-web-console-[ビルド番号].x86_64.rpm
       ```
     - Debian ベースのオペレーティングシステムのデバイスの場合：
       ```
       $ sudo dpkg -i ksc-web-console-[ビルド番号].x86_64.deb
       ```

   これにより、セットアップファイルの展開が始まります。インストールが完了するまで待機します。Kaspersky Security Center 14 Web コンソールが「/var/opt/kaspersky/ksc-web-console」ディレクトリにインストールされます。

5. 次のコマンドを実行してすべての Kaspersky Security Center 14 Web コンソールサービスを再起動します：
   ```
   $ sudo systemctl restart KSC*
   ```

インストールが完了したら、ブラウザーを使用して Kaspersky Security Center 14 Web コンソールを開き、Web コンソールにログインします。

Kaspersky Security Center 14 Web コンソールのインストールパラメータ

Linux で動作するデバイスに Kaspersky Security Center 14 Web コンソールサーバーをインストールする場合、応答ファイルとして Kaspersky Security Center 14 Web コンソールと管理サーバーの接続用のパラメータを含む「.json」ファイルを作成する必要があります。

最小限のパラメータと、既定のアドレスとポートの内容を記載した応答ファイルの作成例は次のようになります：

```
{
"address": "127.0.0.1",
"port": 8080,
"defaultLangId": 1049,
"enableLog"：false、
"trusted": "127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC
Server",
"acceptEula": true,
"certPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer",
"webConsoleAccount": "Group1：User1",
"managementServiceAccount": "Group1：User2",
"serviceWebConsoleAccount": "Group1：User3",
"pluginAccount": "Group1：User4",
"messageQueueAccount": "Group1：User5"
}
```

Linux ALT オペレーティングシステム上に Kaspersky Security Center 14 Web コンソールをインストールする場合、ポート番号 8080 はオペレーティングシステムによって使用されているため、ポート番号には 8080 以外の数字を指定する必要があります。

次の表で、応答ファイルで指定できるパラメータについて説明しています。

Linux で動作するデバイスへの Kaspersky Security Center 14 Web コンソールのインストール用のパラメータ

パラメータ	説明	設定可能な
address	Kaspersky Security Center 14 Web コンソールサーバーのアドレス（必須）	文字列値
port	Kaspersky Security Center 14 Web コンソールサーバーが管理サーバーに接続する際に使用するポート番号（必須）	数値
defaultLangId	ユーザーインターフェイスの言語設定（既定では 1033）	対象言語を示す数字コード • ドイツ語：1031 • 英語：1033 • スペイン語：3082 • スペイン語（メキシコ）：2058 • フランス語：1036 • 日本語：1041 • カザフ語：1087 • ポーランド語：1045

		• ポルトガル語（ブラジル）：1046 • ロシア語：1049 • トルコ語：1055 • 簡体字中国語：4 • 繁体字中国語：31748 値を指定しなかった場合は、言語設定て す。
enableLog	Kaspersky Security Center 14 Web コンソールの動作ログを有効にするかどうかの設定	ブール値： • true：ログ記録が有効になります（ • false：ログ記録が無効になります
trusted	Kaspersky Security Center 14 Web コンソールと接続する資格を付与する信頼する管理サーバーのリスト。各管理サーバーの指定内容には次のパラメータを含める必要があります： • 管理サーバーアドレス • Kaspersky Security Center 14 Web コンソールで管理サーバーへの接続に使用する OpenAPI ポート（既定では 13299） • 管理サーバーの証明書のパス • ログインウィンドウで表示される管理サーバー名 パラメータは縦線（パイプ、|）で区切ります。複数の管理サーバーを指定する場合は、2 本の縦線（||）で区切ります。	文字列の形式は次の通りです： "<サーバーアドレス> | <ポート> | <証 例： "X.X.X.X|13299|/cert/server-1.ce 1||Y.Y.Y.Y|13299|/cert/server-2.
acceptEula	使用許諾契約書（EULA）の条項に同意するかどうかの設定使用許諾契約書の内容を記載したファイルは、インストールファイルと合わせてダウンロードされます。	ブール値： • true - 使用許諾契約書の内容をすべに同意します。 • false - 使用許諾契約書の条項に同意 値が指定されていない場合、Kaspersky ソールのインストーラーは EULA を表示かどうかを尋ねます。
certDomain	新しい証明書を生成する場合は、このパラメータを使用して新しい証明書を生成するドメイン名を指定します。	文字列値

certPath	既存の証明書を使用する場合は、このパラメータを使用して証明書ファイルへのパスを指定します。	文字列値 パス "/var/opt/kaspersky/klnagent_srv を指定し、既存の証明書を使用します。のカスタム証明書が保存されるパスを指
keyPath	既存の証明書を使用する場合は、このパラメータを使用してライセンス情報ファイルへのパスを指定します。	文字列値
webConsoleAccount	KSCWebConsoleサービスを実行するアカウントの名前。	文字列の形式は次の通りです："<グル- 例："Group1:User1"。 値が指定されていない場合、Kaspersky ソールのインストーラーは、既定の名前「user_management_%uid%」で新しい
managementServiceAccount	KSCWebConsoleManagement サービスが実行される特権アカウントの名前。	文字列の形式は次の通りです："<グル- 例："Group1:User1"。 値が指定されていない場合、Kaspersky ソールのインストーラーは、既定の名前新しいアカウントを作成します。
serviceWebConsoleAccount	KSCSvcWebConsole サービスを実行するアカウントの名前。	文字列の形式は次の通りです："<グル- 例："Group1:User1"。 値が指定されていない場合、Kaspersky ソールのインストーラーは、既定の名前「user_svc_nodejs_%uid%」で新しい
pluginAccount	KSCWebConsolePlugin サービスが実行されるアカウントの名前。	文字列の形式は次の通りです："<グル- 例："Group1:User1"。 値が指定されていない場合、Kaspersky ソールのインストーラーは、既定の名前「user_web_plugin_%uid%」で新しい
messageQueueAccount	KSCWebConsoleMessageQueue サービスが実行されるアカウントの名前。	文字列の形式は次の通りです："<グル- 例："Group1:User1"。 値が指定されていない場合、Kaspersky ソールのインストーラーは、既定の名前「user_message_queue_%uid%」で新す。

webConsoleAccount、managementServiceAccount、serviceWebConsoleAccount、pluginAccount、または messageQueueAccount パラメータを指定する場合は、カスタムユーザーアカウントが同じセキュリティグループに属していることを確認してください。これらのパラメータが指定されていない場合、Kaspersky Security Center 14 Web コンソールのインストーラーは既定のセキュリティグループを作成してから、このグループ内に既定の名前でユーザーアカウントを作成します。

カスペルスキーのフェールオーバークラスターノードにインストールされた管理サーバーに接続する Kaspersky Security Center 14 Web コンソールのインストール

このセクションでは、カスペルスキーのフェールオーバークラスターノードにインストールされた管理サーバーに接続する Kaspersky Security Center 14 Web コンソールサーバー（以降、「Kaspersky Security Center 14 Web コンソール」と表記）をインストールする方法について説明します。Kaspersky Security Center 14 Web コンソールをインストールする前に、データベース管理システムと Kaspersky Security Center 管理サーバーをカスペルスキーのフェールオーバークラスターノードにインストールします。

カスペルスキーのフェールオーバークラスターノードにインストールされた管理サーバーに接続する Kaspersky Security Center 14 Web コンソールをインストールするには：

1. Kaspersky Security Center 14 Web コンソールのインストールのステップ 1 とステップ 2 を実行します。

2. ステップ 3 で、応答ファイルの `trusted` インストールパラメータを指定して、カスペルスキーのフェールオーバークラスターが Kaspersky Security Center 14 Web コンソールに接続できるようにします。このパラメータの文字列値の形式は次の通りです：
   `"trusted": "<サーバーアドレス>|<ポート>|<証明書のパス>|<サーバー名>"`

   `trusted` インストールパラメータのコンポーネントを指定します：

   - **管理サーバーアドレス**クラスターノードの準備時に仮想ネットワークアダプターを作成した場合は、アダプターの IP アドレスをカスペルスキーのフェールオーバークラスターのアドレスとして使用します。そうでない場合は、使用するサードパーティのロードバランサーの IP アドレスを指定します。

   - **管理サーバーのポート**Kaspersky Security Center 14 Web コンソールが管理サーバーへの接続に使用する OpenAPI ポート（既定値は 13299）。

   - **管理サーバー証明書**管理サーバーの証明書は、カスペルスキーのフェールオーバークラスターの共有データストレージにあります。証明書ファイルの既定のパス：<共有データフォルダー>\1093\cert\klserver.cer。証明書ファイルを共有データストレージから Kaspersky Security Center 14 Web コンソールをインストールするデバイスにコピーします。管理サーバーの証明書のローカルパスを指定します。

   - **管理サーバー名**Kaspersky Security Center 14 Web コンソールのログインウィンドウに表示されるカスペルスキーのフェールオーバークラスター名。

3. Kaspersky Security Center 14 Web コンソールの標準インストールを実行します。

インストールが正常に完了したら、デスクトップにショートカットが作成され、Kaspersky Security Center 14 Web コンソールにログインできます。

［**検出と製品の導入**］→［**未割り当てデバイス**］の順に移動して、クラスターノードとファイルサーバーに関する情報を表示できます。

Linux 用ネットワークエージェントのサイレントモードでのインストール（応答ファイルを使用）

Linux デバイスにネットワークエージェントをインストールするには、インストールパラメータのカスタムセット（変数と各変数の値）を含むテキストファイルである応答ファイルを使用します。この応答ファイルを使用すると、インストールをサイレント（非インタラクティブ）モードで、つまりユーザーの参加なしで実行できます。

Linux 用ネットワークエージェントのインストールをサイレントモードで実行するには：

1. SUSE Linux Enterprise Server 15 オペレーティングシステムを搭載したデバイスにネットワークエージェントをインストールする場合は、ネットワークエージェントの設定前に、insserv-compat パッケージをインストールします。

2. 使用許諾契約書をお読みください。次の手順は、使用許諾契約書の内容を理解して条項に同意する場合にのみ使用してください。

3. たとえば、次のように、応答ファイルの完全名（パスを含む）を入力して、KLAUTOANSWERS 環境変数の値を設定します。

   ```
   export KLAUTOANSWERS=/tmp/nagent_install/answers.txt
   ```

4. 環境変数で指定したディレクトリに応答ファイル（TXT 形式）を作成します。応答ファイルに、VARIABLE_NAME=variable_value 形式の変数のリストを追加します。各変数は個別の行に配置します。

   応答ファイルを正しく使用するには、3 つの必須変数の最小セットをファイルに含める必要があります：

   - KLNAGENT_SERVER
   - KLNAGENT_AUTOINSTALL
   - EULA_ACCEPTED

   オプションの変数を追加して、リモートインストールに関するより具体的なパラメータを使用することもできます。次の表に、応答ファイルに含めることができるすべての変数を一覧で示します：

   サイレントモードでの Linux 用ネットワークエージェントインストールのパラメータとして使用される応答ファイルの変数

サイレントモードでの Linux 用ネットワークエージェントインストールのパラメータとして使用される応答ファイルの変数

変数名	必須	説明	指定可能な値
KLNAGENT_SERVER	使用する	完全修飾ドメイン名（FQDN）または IP アドレスとして提示される管理サーバー名が含まれます。	DNS 名または IP アドレス。
KLNAGENT_AUTOINSTALL	使用する	サイレント（非インタラクティブ）インストールモードを有効にするかどうかを定義します。	1 - サイレントモードが有効です。ユーザーが、インストール中に操作を要求されることはありません。 その他 - サイレントモードは無効です。ユーザーは、インストール中に操作を要求される場合があります。
EULA_ACCEPTED	使用する	ユーザーがネットワークエージェントの使用許諾契約書（EULA）に同意するかどうかを定義します。定義されていない場合は、EULA に同意しないものとして解釈できます。	1 - この使用許諾契約書の内容をすべて確認し、理解した上で条項に同意する その他の値または値なし - 使用許諾契約書の条項に同意しない（インストールは実行されません）
KLNAGENT_PROXY_USE	使用しない	管理サーバーとの接続でプロキシ設定を使用するかどうかを定義します。既定値は 0 です。	1 - プロキシ設定が使用されます。 その他 - プロキシ設定は使用されません。
KLNAGENT_PROXY_ADDR	使用しない	管理サーバーとの接続に使用されるプロキシサーバーのアドレスを定義します。	DNS 名または IP アドレス。
KLNAGENT_PROXY_LOGIN	使用しない	プロキシサーバーへのログインに使用するユーザー名を定義します。	既存のユーザー名。
KLNAGENT_PROXY_PASSWORD	使用しない	プロキシサーバーへのログインに使用するパスワードを定義します。	オペレーティングシステムのパスワード形式で許可されている英数字のセット。
KLNAGENT_VM_VDI	使用しない	動的仮想マシンを作成するために、ネットワークエージェントをイメージにインストールするかどうかを定義します。	1 - ネットワークエージェントがイメージにインストールされ、その後、

			動的仮想マシンの作成に使用されます。 その他 - インストール中にイメージは使用されません。
KLNAGENT_VM_OPTIMIZE	使用しない	ネットワークエージェントの設定をハイパーバイザー向けに最適化するかどうかを定義します。	1 - ネットワークエージェントの既定のローカル設定が変更され、ハイパーバイザーでの使用が最適化されます。
KLNAGENT_TAGS	使用しない	ネットワークエージェントのインスタンスに割り当てられたタグを一覧表示します。	セミコロンで区切られた 1 つまたは複数のタグ名。
KLNAGENT_UDP_PORT	使用しない	ネットワークエージェントが使用する UDP ポートを定義します。既定値は 15000 です。	既存のポート番号。
KLNAGENT_PORT	使用しない	ネットワークエージェントが使用する非 TLS ポートを定義します。既定値は 14000 です。	既存のポート番号。
KLNAGENT_SSLPORT	使用しない	ネットワークエージェントが使用する TLS ポートを定義します。既定値は 13000 です。	既存のポート番号。
KLNAGENT_USESSL	使用しない	接続にトランスポート層セキュリティ（TLS）を使用するかどうかを定義します。	1（既定） - TLSが使用されます。 その他 - TLS は使用されません。
KLNAGENT_GW_MODE	使用しない	接続ゲートウェイを使用するかどうかを定義します。	1（既定） - 現在の設定は変更されません（最初の呼び出しで、接続ゲートウェイは指定されません）。 2 - 接続ゲートウェイは使用されません。 3 - 接続ゲートウェイが使用されます。 4 - ネットワークエージェントのインスタンスが、非武装地帯（DMZ）で接続ゲートウェイとして使用されます。

KLNAGENT_GW_ADDRESS	使用しない	接続ゲートウェイのアドレスを定義します。この値は、KLNAGENT_GW_MODE=3 の場合にのみ適用されます。	DNS 名または IP アドレス：

5. ネットワークエージェントをインストールします：

- RPM パッケージから 32 ビットオペレーティングシステムにネットワークエージェントをインストールするには、次のコマンドを実行します：
  `# rpm -i klnagent-<ビルド番号>.i386.rpm`
- RPM パッケージから 64 ビットオペレーティングシステムにネットワークエージェントをインストールするには、次のコマンドを実行します：
  `# rpm -i klnagent64-<ビルド番号>.x86_64.rpm`
- RPM パッケージから ARM アーキテクチャの 64 ビットオペレーティングシステムにネットワークエージェントをインストールするには、次のコマンドを実行します：
  `# rpm -i klnagent64-<ビルド番号>.aarch64.rpm`
- DEB パッケージから 32 ビットオペレーティングシステムにネットワークエージェントをインストールするには、次のコマンドを実行します：
  `# apt-get install ./klnagent_<ビルド番号>_i386.deb`
- DEB パッケージから 64 ビットオペレーティングシステムにネットワークエージェントをインストールするには、次のコマンドを実行します：
  `# apt-get install ./klnagent64_<ビルド番号>_amd64.deb`
- ARM アーキテクチャの 64 ビットオペレーティングシステムに DEB パッケージからネットワークエージェントをインストールするには、次のコマンドを実行します：
  `# apt-get install ./klnagent64_<ビルド番号>_arm64.deb`

Linux 用ネットワークエージェントのインストールはサイレントモードで開始されます。ユーザーが、プロセス中に操作を要求されることはありません。

DBMS に使用するアカウント

管理サーバーをインストールして操作するには、内部 DBMS アカウントの作成が必要です。このアカウントは、DBMS へのアクセスを許可し、特定の権限を必要とします。DBMS アカウントに権限と許可を付与するときは、最小権限の原則に従います。つまり、付与する権限は、必要なアクションを実行するのに必要最低限にすべきです。管理サーバーをインストールして起動する前に、DBMS アカウントに権限を付与する必要があることに注意してください。

Kaspersky Security Center 14 Linux は、MySQL および MariaDB DBMS をサポートしています。これらの DBMS のいずれかの内部アカウントを作成したら、このアカウントに必要な権限を付与します。内部 MySQL アカウントと内部 MariaDB アカウントの権限セットは同じであることに注意してください。必要な権限は次の通りです：

- スキーマ権限：
  - 管理サーバーデータベース：ALL（GRANT OPTION を除く）。
  - システムスキーム（mysql および sys）：SELECT、SHOW VIEW。

- sys.table_exists ストアドプロシージャ：EXECUTE（MariaDB 10.5 以前を DBMS として使用する場合、EXECUTE 権限を付与する必要はありません）。

- すべてのスキームに対するグローバル権限：PROCESS、SUPER。

アカウント権限を設定する方法の詳細は、「MySQL および MariaDB を使用するための DBMS アカウントの設定」を参照してください。

内部 DBMS アカウントに付与した権限は、管理サーバーのデータをバックアップから復元するのに十分です。

MySQL および MariaDB を使用するための DBMS アカウントの設定

必須条件

DBMS アカウントに権限を割り当てる前に、次のアクションを実行します：

1. ローカル管理者アカウントでシステムにログインしていることを確認します。
2. MySQL または MariaDB を使用するための環境をインストールします。

管理サーバーをインストールするための DBMS アカウントの設定

管理サーバーのインストール用に DBMS アカウントを設定するには：

1. DBMS のインストール時に作成した root アカウントで、MySQL または MariaDB を使用するための環境を実行します。
2. パスワード付きの内部 DBMS アカウントを作成します。管理サーバーインストーラー（以降、インストーラーとも表記）と管理サーバーサービスは、この内部 DBMS アカウントを使用して DBMS にアクセスします。

   パスワード付きの DBMS アカウントを作成するには、次のコマンドを実行します：

   ```
   /* KSCAdmin という名前のユーザーを作成し、KSCAdmin のパスワードを指定します */
   CREATE USER 'KSCAdmin' IDENTIFIED BY '<パスワード>';
   ```

   MySQL 8.0 以前を DBMS として使用する場合、これらのバージョンでは「caching_sha2_password」認証がサポートされていないことに注意してください。既定の認証を「Caching SHA2 password」から「MySQL native password」に変更します：

   - 「mysql_native_password」認証を使用する DBMS アカウントを作成するには、次のコマンドを実行します：

     ```
     CREATE USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '<パスワード>';
     ```

   - 既存の DBMS アカウントの認証を変更するには、次のコマンドを実行します：

     ```
     ALTER USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '<パスワード>';
     ```

3. 作成した DBMS アカウントに次の権限を付与します：

   - スキーマ権限：

     - 管理サーバーデータベース：ALL（GRANT OPTION を除く）

- システムスキーム（mysql および sys）：SELECT、SHOW VIEW
- sys.table_exists ストアドプロシージャ：EXECUTE

- すべてのスキームに対するグローバル権限：PROCESS、SUPER

作成した DBMS アカウントに必要な権限を付与するには、次のスクリプトを実行します：

```
/* KSCAdmin に権限を付与します */
GRANT USAGE ON *.* TO 'KSCAdmin';
GRANT ALL ON kav.* TO 'KSCAdmin';
GRANT SELECT, SHOW VIEW ON mysql.* TO 'KSCAdmin';
GRANT SELECT, SHOW VIEW ON sys.* TO 'KSCAdmin';
GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'KSCAdmin';
GRANT PROCESS ON *.* TO 'KSCAdmin';
GRANT SUPER ON *.* TO 'KSCAdmin';
```

MariaDB 10.5 以前を DBMS として使用する場合、EXECUTE 権限を付与する必要はありません。この場合、次のコマンドをスクリプトから除外します：`GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'KSCAdmin'.`

4. DBMS アカウントに付与された権限のリストを表示するには、次のコマンドを実行します：

   ```
   SHOW grants for 'KSCAdmin'
   ```

5. 管理サーバーデータベースを手動で作成するには、次のスクリプトを実行します（このスクリプトでは、管理サーバーデータベース名は *kav* です）：

   ```
   CREATE DATABASE kav
   DEFAULT CHARACTER SET 'ascii'
   COLLATE 'ascii_general_ci';
   ```

   DBMS アカウントを作成するスクリプトで指定したものと同じデータベース名を使用します。

6. 管理サーバーをインストールします。

インストールが完了すると、管理サーバーデータベースが作成され、管理サーバーを使用できるようになります。

カスペルスキーのフェールオーバークラスターの導入

このセクションでは、カスペルスキーのフェールオーバークラスターに関する全般的な情報と、ネットワークにカスペルスキーのフェールオーバークラスターを導入するための準備に関する手順の両方を説明します。

シナリオ：カスペルスキーのフェールオーバークラスターの導入

カスペルスキーのフェールオーバークラスターは Kaspersky Security Center の高可用性を提供し、障害時の管理サーバーのダウンタイムを最小限に抑えます。フェールオーバークラスターは 2 台のコンピューターにインストールされた 2 つの同一な Kaspersky Security Center のインスタンスから構成されます。インスタンスの 1 つはアクティブノードとして、もう 1 つはパッシブノードとして動作します。アクティブノードはクライアントデバイスの保護を管理し、パッシブノードはアクティブノードの障害発生時にすべての機能を継承するよう準備されています。障害が発生した場合、パッシブノードはアクティブノードに、アクティブノードはパッシブノードになります。

必須条件

フェールオーバークラスターの要件を満たすハードウェアを持っている。

カスペルスキー製品の導入シナリオは、以下の手順で進みます：

1. **Kaspersky Security Center サービス用のアカウントの作成**

   アクティブノード、パッシブノード、およびファイルサーバーで次の手順を実行します：

   1. 「kladmins」という名前のドメイングループを作成し、3 つのグループすべてに同じ GID を割り当てます。これらのグループにローカル管理者権限を付与します。
   2. 「ksc」という名前のユーザーアカウントを作成し、3 つのユーザーアカウントすべてに同じ UID を割り当てます。これらのアカウントを「kladmins」ドメイングループに追加します。
   3. 「rightless」という名前のユーザーアカウントを作成し、3 つのユーザーアカウントすべてに同じ UID を割り当てます。これらのアカウントを「kladmins」ドメイングループに追加します。

2. **ファイルサーバーの準備**

   カスペルスキーのフェールオーバークラスターのコンポーネントとして動作するファイルサーバーを準備します。ファイルサーバーがシステム要件を満たしていることを確認して、Kaspersky Security Center のデータ用に 2 つの共有フォルダーを作成し、それらの共有フォルダーのアクセス権を設定します。

   実行手順の説明：カスペルスキーのフェールオーバークラスター向けのファイルサーバーの準備

3. **アクティブおよびパッシブノードの準備**

   アクティブおよびパッシブノードとして動作する同一のハードウェアおよびソフトウェアを持つ 2 台のコンピューターを準備します。

   実行手順の説明：カスペルスキーのフェールオーバークラスター向けのノードの準備

4. **DBMS（データベース管理システム）のインストール**

   次の 2 つがあります：

   - MariaDB Galera Cluster を使用する場合は、DBMS 専用のコンピューターは必要ありません。MariaDB Galera Cluster を各ノードにインストールします。
   - その他のサポート対象の DBMS を使用する場合は、選択した DBMS を専用のコンピューターにインストールします。

5. **Kaspersky Security Center のインストール**

   両方のノードのフェールオーバークラスターモードで Kaspersky Security Center をインストールします。最初にアクティブノードに Kaspersky Security Center インストールしてからパッシブノードにもインストールします。

   さらに、クラスターノードではない別のデバイスに Kaspersky Security Center 14 Web コンソールをインストールできます。

6 **フェールオーバークラスターのテスト**

フェールオーバークラスターが正しく設定され、問題なく動作していることを確認してください。たとえば、アクティブノードの Kaspersky Security Center のサービス（kladminserver、klnagent、ksnproxy、klactprx または klwebsrv）のうち 1 つを停止します。サービスが停止された後、保護管理は自動的にパッシブノードに切り替わります。

結果

カスペルスキーのフェールオーバークラスターが導入されます。アクティブおよびパッシブノードの切り替えが発生するイベントについてはしっかりと把握するようにしてください。

カスペルスキーのフェールオーバークラスターについて

カスペルスキーのフェールオーバークラスターは Kaspersky Security Center の高可用性を提供し、障害時の管理サーバーのダウンタイムを最小限に抑えます。フェールオーバークラスターは 2 台のコンピューターにインストールされた 2 つの同一な Kaspersky Security Center のインスタンスから構成されます。インスタンスの 1 つはアクティブノードとして、もう 1 つはパッシブノードとして動作します。アクティブノードはクライアントデバイスの保護を管理し、パッシブノードはアクティブノードの障害発生時にすべての機能を継承するよう準備されています。障害が発生した場合、パッシブノードはアクティブノードに、アクティブノードはパッシブノードになります。

カスペルスキーのフェイルオーバークラスターでは、すべての Kaspersky Security Center サービスは自動で管理されます。手動でサービスを再起動しないでください。

システム要件

カスペルスキーのフェールオーバークラスターを導入するには、次のハードウェアを準備する必要があります：

- 同一のハードウェアおよびソフトウェアを持つ 2 台のコンピューター。これらのコンピューターはアクティブおよびパッシブノードとして動作します。
- EXT4 ファイルシステムの Linux を実行しているファイルサーバー。ファイルサーバーとして動作する専用のコンピューターを準備する必要があります。

  ファイルサーバーとアクティブおよびパッシブノードには高帯域幅ネットワークを使用していることを確認してください。

- DBMS（データベース管理システム）がインストールされたコンピューター。MariaDB Galeria Cluster を DBMS として使用している場合は、DBMS 専用のコンピューターは必要ありません。

切り替えの条件

アクティブノードに次のイベントが発生した場合、フェールオーバークラスターはクライアントデバイスの保護の管理をアクティブノードからパッシブノードに切り替えます：

- ソフトウェアまたはハードウェアの障害によりアクティブノードが破損した。

- メンテナンス操作のためアクティブノードが一時的に停止した。
- Kaspersky Security Center のサービスまたはプロセスで障害が発生したかユーザーにより意図的に中断された。Kaspersky Security Center のサービスは次の通りです：kladminserver、klnagent、klactprx および klwebsrv。
- アクティブノードとファイルサーバー上の保管領域のネットワーク接続が中断または切断された。

カスペルスキーのフェールオーバークラスター向けのファイルサーバーの準備

ファイルサーバーはカスペルスキーのフェールオーバークラスターの必須コンポーネントとして動作します。

ファイルサーバーを準備するには：

1. ファイルサーバーがシステム要件を満たしていることを確認してください。
2. NFS サーバーをインストールして設定します：
   - NFS サーバー設定で、両方のノードに対してファイルサーバーへのアクセスが有効になっている必要があります。
   - NFS プロトコルのバージョンは 4.0 または 4.1 である必要があります。
   - Linux カーネルの最小要件：
     - 3.19.0-25（NFS4.0 を使用する場合）
     - 4.4.0-176（NFS 4.1 を使用する場合）
3. ファイルサーバーで、2 つのフォルダーを作成して NFS を使用して共有します。2 つのうち 1 つは、フェールオーバークラスターの状態に関する情報を保持するために使用されます。別の 1 つは Kaspersky Security Center のデータおよび設定を保存するために使用されます。Kaspersky Security Center のインストールの設定時に共有フォルダーのパスを指定することになります。

   次のコマンドを実行します：

   ```
   sudo yum install nfs-utils
   sudo mkdir -p /mnt/KlFocStateShare
   sudo mkdir -p /mnt/KlFocDataShare_klfoc
   sudo chown ksc:kladmins /mnt/KlFocStateShare
   sudo chown ksc:kladmins /mnt/KlFocDataShare_klfoc
   sudo chmod -R 777 /mnt/KlFocStateShare /mnt/KlFocDataShare_klfoc
   sudo sh -c "echo /mnt/KlFocStateShare *\(rw,sync,no_subtree_check,no_root_squash\) >>
   /etc/exports"
   sudo sh -c "echo /mnt/KlFocDataShare_klfoc *\
   (rw,sync,no_subtree_check,no_root_squash\) >> /etc/exports"
   sudo cat /etc/exports
   sudo exportfs -a
   sudo systemctl start rpcbind
   sudo service nfs start
   ```

   次のコマンドを実行して自動実行を有効にします：

   ```
   sudo systemctl enable rpcbind
   ```

4. ファイルサーバーを再起動します。

ファイルサーバーの準備ができました。カスペルスキーのフェールオーバークラスターを導入するには、シナリオの手順に従ってください。

カスペルスキーのフェールオーバークラスター向けのノードの準備

カスペルスキーのフェールオーバークラスターのアクティブノードとパッシブノードとして動作する 2 台のコンピューターを準備します。

カスペルスキーのフェールオーバークラスター向けのノードを準備するには：

1. 2 台のコンピューターがシステム要件を満たしていることを確認してください。これらのコンピューターはフェールオーバークラスターのアクティブノードおよびパッシブノードとして動作します。

2. NFS クライアントでノードを動作させるために、各ノードに nfs-utils パッケージをインストールします。

   次のコマンドを実行します：

   ```
   sudo yum install nfs-utils
   ```

3. 次のコマンドを実行してマウントポイントを作成します：

   ```
   sudo mkdir -p /mnt/KlFocStateShare
   sudo mkdir -p /mnt/KlFocDataShare_klfoc
   ```

4. 共有フォルダーが正常にマウントされたことを確認します（この手順は省略可能です）。

   次のコマンドを実行します：

   ```
   sudo mount -t nfs -o vers=4,nolock,local_lock=none,auto,user,rw {サーバー}:
   {KlFocStateShare フォルダーのパス} /mnt/KlFocStateShare
   sudo mount -t nfs -o vers=4,nolock,local_lock=none,noauto,user,rw {サーバー}:
   {KlFocDataShare_klfoc フォルダーのパス} /mnt/KlFocDataShare_klfoc
   ```

   ここでは、{サーバー}:{KlFocStateShare フォルダーのパス}および{サーバー}:{KlFocDataShare_klfoc フォルダーのパス}はファイルサーバー上の共有フォルダーへのネットワークパスです。

   共有フォルダーが正常にマウントされた後、次のコマンドを実行してマウントを解除します：

   ```
   sudo umount /mnt/KlFocStateShare
   sudo umount /mnt/KlFocDataShare_klfoc
   ```

5. マウントポイントと共有フォルダーをマッチさせます。

   ```
   sudo vi /etc/fstab
   {サーバー}:{KlFocStateShare フォルダーのパス} /mnt/KlFocStateShare nfs
   vers=4,nolock,local_lock=none,auto,user,rw 0 0
   {サーバー}:{KlFocDataShare_klfoc フォルダーのパス} /mnt/KlFocDataShare_klfoc nfs
   vers=4,nolock,local_lock=none,noauto,user,rw 0 0
   ```

   ここでは、{サーバー}:{KlFocStateShare フォルダーのパス}および{サーバー}:{KlFocDataShare_klfoc フォルダーのパス}はファイルサーバー上の共有フォルダーへのネットワークパスです。

6. 両方のノードを再起動します。

7. 次のコマンドを実行して共有フォルダーをマウントします：

   ```
   mount /mnt/KlFocStateShare
   mount /mnt/KlFocDataShare_klfoc
   ```

8. 共有フォルダーにアクセスする権限が ksc:kladmins に属していることを確認してください。

次のコマンドを実行します：

```
sudo ls -la /mnt/
```

9. 各ノードでネットワークアダプターを作成します。次のいずれかの手順を実行します：

- 仮想ネットワークアダプターを使用します。

  a. 次のコマンドを使用して、物理アダプターの管理に NetworkManager が使用されていることを確認します：

  ```
  nmcli デバイスのステータス
  ```

  出力に物理アダプターが管理対象外として表示される場合は、物理アダプターを管理するように NetworkManager を構成します。具体的な構成手順は、ディストリビューションによって異なります。

  b. 次のコマンドを使用して、インターフェイスを識別します：

  ```
  ip a
  ```

  c. 新しい構成プロファイルを作成します：

  ```
  nmcli connection add type macvlan dev <物理インターフェイス> mode bridge
  ifname <仮想インターフェイス> ipv4.addresses <アドレスマスク> ipv4.method
  manual autoconnect no
  ```

- 物理ネットワークアダプターまたはハイパーバイザーを使用します。このシナリオでは、ソフトウェア NetworkManager を無効にします。

  a. 対象のインターフェイスの NetworkManager 接続を削除します：

  ```
  nmcli con del <接続名>
  ```

  次のコマンドを使用して、対象のインターフェイスに接続があるかどうかを確認します：

  ```
  nmcli con show
  ```

  b. ファイル NetworkManager.conf を編集します。keyfile セクションを見つけて、対象のインターフェイスを unmanaged-devices パラメータに割り当てます。

  ```
  [keyfile]
  unmanaged-devices=インターフェイス名:<インターフェイス名>
  ```

  c. NetworkManager を再起動します。

  ```
  systemctl reload NetworkManager
  ```

  次のコマンドを使用して、対象のインターフェイスが管理対象外であることを確認します：

  ```
  nmcli dev status
  ```

- サードパーティのロードバランサーを使用している。たとえば、nginx サーバーを使用できます。この場合、次の操作を行ってください：

  a. Linux ベースで nginx がインストールされた専用のコンピューターを準備します。

  b. ロードバランシングの設定をします。アクティブノードをメインサーバー、パッシブノードをバックアップサーバーとして設定します。

  c. nginx サーバーで、管理サーバーのポートをすべて開きます： TCP 13000、UDP 13000、TCP 13291、TCP 13299、TCP 17000。

ノードの準備ができました。カスペルスキーのフェールオーバークラスターを導入するには、シナリオの手順に従ってください。

カスペルスキーのフェールオーバークラスターノードへの Kaspersky Security Center のインストール

ここでは、カスペルスキーのフェールオーバークラスターのノードに Kaspersky Security Center をインストールする方法について説明します。Kaspersky Security Center はカスペルスキーのフェールオーバークラスターの両方のノードに個別にインストールされます。まず最初にアクティブなノードに製品をインストールしてから、パッシブなノードにインストールします。インストール中に、どのノードがアクティブでどのノードがパッシブになるかを選択します。

デバイスにインストールされている Linux ディストリビューションに応じて、「ksc64_[バージョン番号]_amd64.deb」または「ksc64-[バージョン番号].x86_64.rpm」のいずれかのインストールファイルを使用してください。インストールファイルは、カスペルスキーの Web サイトからダウンロードして取得できます。

すべてのノードに Kaspersky Security Center をインストールできるのは KLAdmins ドメイングループのユーザーのみです。

プライマリー（アクティブ）ノードへのインストール

プライマリーノードに Kaspersky Security Center をインストールするには：

1. Kaspersky Security Center をインストールするデバイスで、サポート対象の Linux ディストリビューションを使用していることを確認します。
2. コマンドラインで、ルート権限を持つアカウントを使用してこの手順にあるコマンドを実行します。
3. Kaspersky Security Center のインストールを実行します。Linux ディストリビューションに応じて、次のコマンドを実行します：
   - `sudo apt install /<path>/ksc64_[バージョン番号]_amd64.deb`
   - `sudo yum install /<path>/ksc64-[バージョン番号].x86_64.rpm -y`
4. Kaspersky Security Center の設定を実行します：

   ```
   sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

5. 使用許諾契約書（EULA）およびプライバシーポリシーを読みます。テキストはコマンドラインウィンドウに表示されます。次のテキストセグメントを表示するにはスペースキーを押します。確認が表示されてから次の値を入力します：
   a. EULA の内容を確認して同意する場合は「y」を入力します。EULA の内容に同意しない場合は「n」を入力します。Kaspersky Security Center を使用するには、EULA の内容に同意する必要があります。
   b. プライバシーポリシーの内容を確認して同意し、またデータがプライバシーポリシーに記載される方法で処理されて送信されること（第三国への送信を含む）に同意する場合は「y」を入力します。プライバシーポリシーの内容に同意しない場合は「n」を入力します。Kaspersky Security Center を使用するには、プライバシーポリシーの内容に同意する必要があります。
6. 管理サーバーのインストールモードとして**プライマリークラスターノード**を選択します
7. 確認が表示されてから次の設定を入力します：

a. State share のマウントポイントにローカルパスを入力します。

b. Data share のマウントポイントにローカルパスを入力します。

c. フェールオーバークラスターの接続モードを選択します：仮想ネットワークアダプターまたは外部のロードバランサー。

d. 仮想ネットワークアダプターを使用する場合は、名前を入力します。

e. 管理サーバーの DNS 名または静的 IP アドレスを入力するよう要求された場合は、仮想ネットワークアダプターまたは外部ロードバランサーの IP アドレスを入力します。

f. 管理サーバーのポート番号を入力します。既定では、ポート 14000 が使用されます。

g. 管理サーバーの SSL ポート番号を入力します。既定では、ポート 13000 が使用されます。

h. 管理するデバイスの概数を見積もります：

- ネットワーク上のデバイス数が 1 ～ 100 の場合は、「1」を入力します。
- ネットワーク上のデバイス数が 101 ～ 1000 の場合は、「2」を入力します。
- ネットワーク上のデバイス数が 1000 以上の場合は、「3」を入力します。

i. サービス用のセキュリティグループ名を入力します。既定では、「kladmins」グループが使用されます。

j. 管理サーバーサービスを開始するアカウント名を入力します。アカウントは入力したセキュリティグループのメンバーである必要があります。既定では「ksc」アカウントが使用されます。

k. その他のサービスを開始するアカウント名を入力します。アカウントは入力したセキュリティグループのメンバーである必要があります。既定では「ksc」アカウントが使用されます。

l. データベースがインストールされるデバイスの IP アドレスを入力します。

m. データベースのポート番号を入力します。このポートは管理サーバーとの通信に使用されます。既定では、ポート 3306 が使用されます。

n. データベースの名前を入力します。

o. データベースへのアクセスに使用するデータベースのルートアカウントのログイン名を入力します。

p. データベースへのアクセスに使用するデータベースのルートアカウントのパスワードを入力します。

サービスが追加され自動的に開始されるまで待ちます。

- klnagent_srv
- kladminserver_srv
- klactprx_srv
- klwebsrv_srv

q. 管理サーバーの管理者とするアカウントを作成します。ユーザー名とパスワードを入力します。ユーザーパスワードは 8 文字以上 16 文字以下である必要があります。

ユーザーが追加され、Kaspersky Security Center がプライマリーノードにインストールされます。

セカンダリー（パッシブ）ノードへのインストール

セカンダリーノードに Kaspersky Security Center をインストールするには：

1. Kaspersky Security Center をインストールするデバイスで、サポート対象の Linux ディストリビューションを使用していることを確認します。
2. コマンドラインで、ルート権限を持つアカウントを使用してこの手順にあるコマンドを実行します。
3. Kaspersky Security Center のインストールを実行します。Linux ディストリビューションに応じて、次のコマンドを実行します：
   - `sudo apt install /<path>/ksc64_[ バージョン番号 ]_amd64.deb`
   - `sudo yum install /<path>/ksc64-[ バージョン番号 ].x86_64.rpm -y`
4. Kaspersky Security Center の設定を実行します：

   ```
   sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

5. 使用許諾契約書（EULA）およびプライバシーポリシーを読みます。テキストはコマンドラインウィンドウに表示されます。次のテキストセグメントを表示するにはスペースキーを押します。確認が表示されてから次の値を入力します：
   a. EULA の内容を確認して同意する場合は「y」を入力します。EULA の内容に同意しない場合は「n」を入力します。Kaspersky Security Center を使用するには、EULA の内容に同意する必要があります。
   b. プライバシーポリシーの内容を確認して同意し、またデータがプライバシーポリシーに記載される方法で処理されて送信されること（第三国への送信を含む）に同意する場合は「y」を入力します。プライバシーポリシーの内容に同意しない場合は「n」を入力します。Kaspersky Security Center を使用するには、プライバシーポリシーの内容に同意する必要があります。
6. 管理サーバーのインストールモードとして**セカンダリークラスターノード**を選択します
7. プロンプトが表示されたら、State share のマウントポイントにローカルパスを入力します。

Kaspersky Security Center がセカンダリーノードにインストールされます。

サービスの検証

サービスが実行されているかどうかを確認するには、次のコマンドを実行します：

- `systemctl status klnagent_srv.service`
- `systemctl status kladminserver_srv.service`
- `systemctl status klactprx_srv.service`
- `systemctl status klwebsrv_srv.service`

カスペルスキーのフェールオーバークラスターが正しく設定され、クラスターが正しく動作するか確認するためテストできる状態になりました。

手動でのクラスターノードの開始と終了

カスペルスキーのフェールオーバークラスター全体を停止したり、メンテナンスでクラスターのノードの一部を一時的に分離したりする必要がある場合があります。その場合はこのセクションの手順に従ってください。別の方法でフェールオーバークラスターに関連するサービスやプロセスを開始または停止しないでください。データを損失する可能性があります。

メンテナンス目的でのフェールオーバークラスター全体の開始および停止

フェールオーバークラスター全体を開始または停止するには：

1. アクティブノードで、/opt/kaspersky/ksc64/sbin に移動します。
2. コマンドラインを開いて、次のコマンドのうち1つを実行してください：
   - クラスターを停止するには、 `klfoc -stopcluster --stp klfoc` を実行します。
   - クラスターを開始するには、 `klfoc -startcluster --stp klfoc` を実行します。

フェールオーバークラスターは実行したコマンドに基づいて開始または停止されます。

ノードの一部のメンテナンス

ノードの一部をメンテナンスするには：

1. アクティブなノードで、コマンド「 `klfoc -stopcluster --stp klfoc` 」を使用してフェールオーバークラスターを停止します。
2. メンテナンス対象のノードで、/opt/kaspersky/ksc64/sbin に移動します。
3. コマンドラインを開き、コマンド「`detach_node.sh`」を実行してクラスターからノードを分離します。
4. アクティブなノードで、コマンド「 `klfoc -startcluster --stp klfoc` 」を使用してフェールオーバークラスターを開始します。
5. メンテナンスを行います。
6. アクティブなノードで、コマンド「 `klfoc -stopcluster --stp klfoc` 」を使用してフェールオーバークラスターを停止します。
7. メンテナンスしたノードで、/opt/kaspersky/ksc64/sbin に移動します。
8. コマンドラインを開き、コマンド「`attach_node.sh`」を実行してクラスターにノードを接続します。
9. アクティブなノードで、コマンド「 `klfoc -startcluster --stp klfoc` 」を使用してフェールオーバークラスターを開始します。

ノードのメンテナンスは完了し、フェールオーバークラスターに接続されます。

Kaspersky Security Center を使用するための証明書

このセクションでは、Kaspersky Security Center の証明書に関する情報と、Kaspersky Security Center 14 Web コンソール向けの証明書を発行および置き換える方法、サーバーが Kaspersky Security Center 14 Web コンソールと連携している場合に管理サーバー向けの証明書を更新する方法について説明します。

Kaspersky Security Center の証明書について

Kaspersky Security Center では、次の種類の証明書を使用することで、製品コンポーネント間の安全な対話を可能にしています。

- 管理サーバー証明書
- Web サーバーの証明書
- Kaspersky Security Center 14 Web コンソールの証明書

既定では、Kaspersky Security Center は自己署名証明書（つまり、Kaspersky Security Center 自体によって発行された証明書）を使用しますが、組織のネットワークの要件をより適切に満たし、セキュリティ標準に準拠するために、それらをカスタム証明書に置換することができます。カスタム証明書が該当するすべての要件を満たしているかどうかを管理サーバーが検証し、その後、この証明書は自己署名証明書と同じ機能範囲があると判断されます。唯一の違いは、カスタム証明書は期限切れ時に自動的に再発行されないことです。証明書のタイプに応じて、klsetsrvcert ユーティリティを使用するか、Kaspersky Security Center 14 Web コンソールの［管理サーバーのプロパティ］セクションを介して、証明書をカスタム証明書に置換します。Klsetsrvcert ユーティリティを使用している際には、次の値のいずれかを使用して証明書を指定する必要があります：

- C：（ポート 13000 と 13291 に共通の証明書）
- CR：（ポート 13000 と 13291 に共通の予備の証明書）

管理サーバー証明書の最大有効期間は 397 日以下である必要があります。

管理サーバー証明書

管理サーバー証明書は、次の目的のために必要です：

- Kaspersky Security Center 14 Web コンソールへの接続時における管理サーバーの認証
- 管理対象デバイスでの管理サーバーとネットワークエージェントとの安全な連携
- プライマリ管理サーバーがセカンダリ管理サーバーに接続されている場合の認証

管理サーバー証明書は、管理サーバーのインストール中に自動的に作成され、フォルダー「/var/opt/kaspersky/klnagent_srv/1093/cert/」に格納されます。Kaspersky Security Center 14 Web コンソールをインストールするための応答ファイルを作成する際に管理サーバーの証明書を指定しています。この証明書は共通（「C」）と呼ばれます。

管理サーバーの証明書は 397 日間有効です。Kaspersky Security Center は、共通証明書の有効期限が切れる 90 日前に予備の共通証明書（「CR」）を自動的に生成します。その後、共通予備証明書を使用して、管理サーバー証明書はシームレスに置換されます。共通証明書の有効期限が近づくと、共通予備証明書を使用して、管理対象デバイスにインストールされているネットワークエージェントインスタンスとの接続が維持されます。この目的で、共通予備証明書は、古い共通証明書の有効期限が切れる 24 時間前に自動的に新しい共通証明書になります。

管理サーバー証明書の最大有効期間は 397 日以下である必要があります。

必要に応じて、カスタム証明書を管理サーバーに割り当てることができます。たとえば、企業の既存の PKI とのより容易な統合や、証明書フィールドの設定のカスタマイズなどの理由で、こうした操作が必要になる場合があります。証明書を置換すると、以前 SSL を介して管理サーバーに接続したすべてのネットワークエージェントの接続が切断され、「管理サーバー証明書エラー」が返されます。このエラーを解消するには、証明書の置換後に接続を復元する必要があります。

管理サーバー証明書を紛失した場合、その証明書を復元するには、管理サーバーを再インストールしてデータを復元する必要があります。

データを失うことなく管理サーバーをあるデバイスから別のデバイスに移動するために、他の管理サーバー設定とは別に管理サーバー証明書をバックアップすることもできます。

Web サーバーの証明書

特別な種類の証明書は、Kaspersky Security Center 管理サーバーのコンポーネントである Web サーバーによって使用されます。この証明書は、後で管理対象デバイスにダウンロードするネットワークエージェントインストールパッケージの公開に必要です。この目的のために、Web サーバーは様々な証明書を使用できます。

Web サーバーは次の証明書を優先度順に使用します：

1. Kaspersky Security Center 14 Web コンソールを使用して手動で指定したカスタム Web サーバー証明書
2. 共通管理サーバー証明書（「C」）

Kaspersky Security Center 14 Web コンソールの証明書

Kaspersky Security Center 14 Web コンソール（以降「Web コンソール」と表記）のサーバーには、独自の証明書があります。Web サイトを開く際に、ブラウザは接続が信頼できるかどうかを確認します。Web コンソール証明書を使用して、Web コンソールを認証できます。この証明書は、ブラウザーと Web コンソールの間のトラフィックの暗号化にも使用されます。

Web コンソールを開くと、ブラウザーから Web コンソールとの接続がプライベートでなく Web コンソールの証明書が無効であると通知される場合があります。この警告は、Web コンソールの証明書が自己署名で、Kaspersky Security Center によって自動で生成されているために表示されます。この警告が表示されないようにするには、次の操作のうち 1 つを実行します：

- カスタム証明書と Web コンソールの証明書を置き換える（推奨）。企業のインフラストラクチャで信頼済みで、かつ、カスタム証明書の要件を満たす証明書を作成する。
- ブラウザーの信頼済み証明書のリストに Web コンソールの証明書を追加する。カスタム証明書を作成できない場合には、この方法を推奨します。

Kaspersky Security Center で使用されるカスタム証明書の要件

次の表は、Kaspersky Security Center の様々なコンポーネントに指定されているカスタム証明書の要件を示しています。

Kaspersky Security Center 証明書の要件

証明書の種別	要件	コメント
共通証明書、予備の共通証明書（「C」「CR」）	最短鍵長：2048 Basic Constraints（基本制約）： • CA：true • Path Length Constraint（パス長制約）：None Key Usage（鍵用途）： • デジタル署名 • 証明書の署名の検証 • 鍵の暗号化 • 証明書失効リスト（CRL）の署名の検証 Extended Key Usage（拡張鍵用途）（任意）：サーバー認証、クライアント認証。	Extended Key Usage パラメータは任意です。 Path Length Constraint の値は「None」ではなく、「1」以上の整数である場合があります。
Web サーバーの証明書	Extended Key Usage（拡張鍵用途）：サーバー認証。 証明書が指定されている PKCS ＃12 コンテナーや PEM コンテナーには、公開鍵のチェーン全体が含まれています。 証明書のサブジェクト代替名（SAN）が存在します。つまり、`subjectAltName` フィールドの値は有効です。 証明書は、サーバー証明書に適用された Web ブラウザーの有効な要件、および CA/Browser Forum の現在のベースライン要件を満たしています。	適用不可。
Kaspersky Security Center 14 Web コンソールの証明書	証明書が指定される PEM コンテナーには、公開鍵のチェーン全体が含まれます。 証明書のサブジェクト代替名（SAN）が存在します。つまり、`subjectAltName` フィールドの値は有効です。 証明書は、サーバー証明書に対する Web ブラウザーの有効な要件、および CA /Browser Forum の現在のベースライン要件を満たしています。	暗号化された証明書は、Kaspersky Security Center 14 Web コンソールではサポートされていません。

Kaspersky Security Center 14 Web コンソールの証明書の再発行

ほとんどの Web ブラウザーは、証明書の有効期間に制限があります。この制限内に収まるように、Kaspersky Security Center 14 Web コンソール証明書の有効期間は 397 日間に制限されています。新しい自己署名証明書を手動で発行することにより、証明機関（CA）から受け取った既存の証明書を置き換えることができます。または、有効期限切れの Kaspersky Security Center 14 Web コンソール証明書を再発行することもできます。

Web コンソールを開くと、ブラウザーから Web コンソールとの接続がプライベートでなく Web コンソールの証明書が無効であると通知される場合があります。この警告は、Web コンソールの証明書が自己署名で、Kaspersky Security Center によって自動で生成されているために表示されます。この警告が表示されないようにするには、次の操作のうち 1 つを実行します：

- 再発行する場合はカスタム証明書を指定する（推奨オプション）。企業のインフラストラクチャで信頼済みで、かつ、カスタム証明書の要件を満たす証明書を作成する。
- 証明書を再発行した後で、ブラウザーの信頼済み証明書のリストに Web コンソールの証明書を追加する。カスタム証明書を作成できない場合には、この方法を推奨します。

有効期限切れの Kaspersky Security Center 14 Web コンソール証明書を再発行するには：

以下のいずれかを実行して Kaspersky Security Center 14 Web コンソールを再インストールします：

- Kaspersky Security Center 14 Web コンソールと同じインストールファイルを使用する場合は、Kaspersky Security Center 14 Web コンソールを削除してから同じバージョンの Kaspersky Security Center 14 Web をインストールします。
- アップグレードバージョンのインストールファイルを使用する場合は、アップグレードコマンドを実行します。

Kaspersky Security Center 14 Web コンソールの証明書が再発行されます。有効期間は 397 日です。

Kaspersky Security Center 14 Web コンソールの証明書の置き換え

既定では、Kaspersky Security Center 14 Web コンソールサーバー（単に「Kaspersky Security Center 14 Web コンソール」とも表記）をインストールすると、Web コンソールのブラウザー証明書が自動的に生成されます。必要に応じて、自動的に生成された証明書をカスタム証明書で置き換えることができます。

Kaspersky Security Center 14 Web コンソールの証明書をカスタム証明書で置き換えるには：

1. Kaspersky Security Center 14 Web コンソールのインストールに必要な新しい応答ファイルを作成します。
2. このファイルには、`certPath` パラメータおよび `keyPath` パラメータを使用してカスタム証明書ファイルとライセンス情報ファイルのパスを指定します。
3. 新しい応答ファイルを使用して Kaspersky Security Center 14 Web コンソールを再インストールします。次のいずれかの手順を実行します：
   - Kaspersky Security Center 14 Web コンソールと同じインストールファイルを使用する場合は、Kaspersky Security Center 14 Web コンソールを削除してから同じバージョンの Kaspersky Security Center 14 Web をインストールします。
   - アップグレードバージョンのインストールファイルを使用する場合は、アップグレードコマンドを実行します。

指定した証明書を使用して Kaspersky Security Center 14 Web コンソールが動作するようになります。

PFX 証明書を PEM 形式に変換する

Kaspersky Security Center 14 Web コンソールで PFX 証明書を使用するには、まず、OpenSSL ベースの簡便に使用できる任意のクロスプラットフォームユーティリティを使用して PEM 形式に変換する必要があります。

Linux オペレーティングシステムで PFX 証明書を PEM 形式に変換するには：

1. OpenSSL ベースのクロスプラットフォームユーティリティで、次のコマンドを実行します。

   ```
   openssl pkcs12 -in <filename.pfx> -clcerts -nokeys | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > server.crt
   ```

   ```
   openssl pkcs12 -in <filename.pfx> -nocerts -nodes | sed -ne '/-BEGIN PRIVATE KEY-/,/-END PRIVATE KEY-/p' > key.pem
   ```

2. 証明書ファイルと秘密鍵が、.pfx ファイルが格納されているのと同じディレクトリに生成されていることを確認してください。

3. Kaspersky Security Center 14 Web コンソールはパスフレーズで保護された証明書はサポートしていません。そのため、OpenSSL ベースのクロスプラットフォームユーティリティで次のコマンドを実行して .pem ファイルからパスフレーズを削除します：

   ```
   openssl rsa -in key.pem -out key-without-passphrase.pem
   ```

   > 入力と出力用の .pem ファイルに同じ名前を使用しないでください。

   結果、.pem ファイルが非暗号化となります。ファイルを使用する際にパスフレーズを入力する必要はありません。

.crt ファイルと .pem ファイルを使用する準備ができたので、Kaspersky Security Center 14 Web コンソールのインストーラーでそれらを指定できるようになります。

シナリオ：管理サーバーのカスタム証明書の指定

管理サーバーのカスタム証明書を割り当てることができます。目的の例として、企業で使用する既存の公開鍵インフラストラクチャ（PKI）との連携の改善、証明書フィールドのカスタム設定などがあります。管理サーバーのインストール直後、かつクイックウィザードの終了前に、証明書を置換することを推奨します。

> 管理サーバー証明書の最大有効期間は 397 日以下である必要があります。

必須条件

新規の証明書は、PKCS#12 形式（たとえば、組織の PKI を使用）で作成し、信頼する認証局（CA）で発行する必要があります。また、新規の証明書には、チェーンの全体と秘密鍵を含め、それらを拡張子 pfx または p12 のファイルに保管する必要があります。その新規の証明書は、以下にリストされた要件を満たす必要があります。

証明書の種別：共通証明書、予備の共通証明書（「C」「CR」）

要件：

- 最短鍵長：2048
- Basic Constraints（基本制約）：
  - CA：true
  - Path Length Constraint（パス長制約）：None
    Path Length Constraint の値は「None」ではなく、「1」以上の整数である場合があります。
- Key Usage（鍵用途）：
  - デジタル署名
  - 証明書の署名の検証
  - 鍵の暗号化
  - 証明書失効リスト（CRL）の署名の検証
- Extended Key Usage（EKU：拡張鍵用途）：サーバー認証、クライアント認証。EKU は任意ですが、証明書に含まれる場合、サーバーとクライアントの認証データは EKU で指定されている必要があります。

パブリック CA によって発行された証明書には、証明書署名の許可がありません。このような証明書を使用するには、ネットワークのディストリビューションポイントまたは接続ゲートウェイに、ネットワークエージェントのバージョン 13 以降がインストールされていることを確認してください。そうしないと、署名の許可なしに証明書を使用できなくなります。

実行するステップ

管理サーバー証明書の指定は段階的に進行します。

1. **管理サーバー証明書の置換**
   この目的のために、コマンドラインで klsetsrvcert ユーティリティを使用します。
2. **新しい証明書を指定し、ネットワークエージェントの管理サーバーへの接続を復元**
   証明書を置換すると、以前 SSL を介して管理サーバーに接続したすべてのネットワークエージェントの接続が切断され、「管理サーバー証明書エラー」が返されます。新しい証明書を指定して接続を復元するには、コマンドラインで klmover ユーティリティを使用します。

結果

このシナリオを終了すると、管理サーバー証明書が置換され、管理対象デバイスのネットワークエージェントでサーバーが認証されます。

klsetsrvcert ユーティリティを使用した管理サーバー証明書の置換

管理サーバーの証明書を手動で置換するには：

コマンドラインから、次のユーティリティを実行します：

```
klsetsrvcert[-t <種別> {-i <入力ファイル> [-p <パスワード>] [-o <証明書の検証パラメータ>] |
-g <DNS 名>}][-f <時刻>][-r <CA のリストファイル>][-l <ログファイル>]
```

klsetsrvcert ユーティリティをダウンロードする必要はありません。Kaspersky Security Center の配布キットに含まれています。Kaspersky Security Center の以前のバージョンとは互換性がありません。

klsetsrvcert ユーティリティのパラメータの説明を次の表に示します。

klsetsrvcert ユーティリティのパラメータ値

パラメータ	値
-t <種別>	置換する証明書の種別。<種別>パラメータに指定可能な値： • C：ポート 13000 と 13291 の共通証明書を置換 • CR：ポート 13000 と 13291 の予備の証明書を置換
-f <時刻>	証明書の変更の予定時刻。形式は「DD-MM-YYYY hh:mm」です（ポート 13000 と 13291 向け）。 有効期間の終了前に、共通証明書または予備の共通証明書を置換する場合は、このパラメータを使用します。 管理対象デバイスが新しい証明書で管理サーバーと同期する必要がある時間を指定します。
-i <入力ファイル>	PKCS#12 形式の証明書と秘密鍵を持つコンテナー（拡張子が .p12 または .pfx のファイル）。
-p <パスワード>	p12 コンテナーの保護に使用されるパスワード 証明書と秘密鍵はコンテナに保存されているため、コンテナでファイルを復号化するにはパスワードが必要です。
-o <証明書の検証パラメータ>	証明書の検証パラメータ（セミコロン区切り）。 証明書署名の権限なしにカスタム証明書を使用するには、klsetsrvcert ユーティリティで -o NoCA を指定します。これは、パブリック認証局（CA）によって発行された証明書に役立ちます。
-g <DNS 名>	指定した DNS 名に対する新しい証明書が作成されます。
-r <CA のリストファイル>	信頼済みのルート証明機関のリスト（PEM 形式）。
-l <ログファイル>	結果出力ファイル。既定では、出力は標準出力ストリームにリダイレクトされます

例えば、カスタム管理サーバー証明書を指定するには、次のコマンドを使用します。

```
klsetsrvcert -t C -i <入力ファイル> -p <パスワード> -o NoCA
```

証明書が置換されると、SSL を介して管理サーバーに接続されているすべてのネットワークエージェントの接続は切断されます。復元するには、コマンドライン klmoverユーティリティを使用します。

ネットワークエージェントの接続が切断されないようにするには、次のコマンドを使用します：

```
klsetsrvcert -f "DD-MM-YYYY hh:mm" -t CR -i <入力ファイル> -p <パスワード> -o NoCA
```

"DD-MM-YYYY hh:mm" は、現在より 3 ～ 4 週間先の日付です。時間を変えて証明書をバックアップに変更することにより、新しい証明書をすべてのネットワークエージェントに配信できます。

klmover ユーティリティを使用したネットワークエージェントの管理サーバーへの接続

コマンドラインで klsetsrvcert ユーティリティを使用して管理サーバー証明書を置換した後は、接続が切断されているため、ネットワークエージェントと管理サーバー間の SSL 接続を確立する必要があります。

新しい管理サーバー証明書を指定して接続を復元するには：

コマンドラインから、次のユーティリティを実行します：

```
klmover [-address <サーバーアドレス>] [-pn <ポート番号>] [-ps <SSL ポート番号>] [-nossl] [-cert <証明書ファイルのパス>]
```

このユーティリティは、ネットワークエージェントがクライアントデバイスにインストールされると、ネットワークエージェントのインストールフォルダーに自動的にコピーされます。

klsetsrvcert ユーティリティのパラメータの説明を次の表に示します。

klmover ユーティリティのパラメータ値

パラメータ	値
`-address <サーバーアドレス>`	接続する管理サーバーのアドレス。 IP アドレスまたは DNS 名を指定できます。
`-pn <ポート番号>`	管理サーバーへの暗号化されていない接続が確立されるポートの番号。 既定のポート番号は 14000 です。
`-ps <SSL ポート番号>`	SSL を使用した管理サーバーへの暗号化接続の確立に使用する SSL ポートの番号。 既定のポート番号は 13000 です。
`-nossl`	管理サーバーへの暗号化されていない接続を使用します。 このキーを使用しない場合、ネットワークエージェントは暗号化された SSL プロトコルを使用して管理サーバーに接続されます。
`-cert <証明書ファイルのパス>`	管理サーバーへのアクセス認証で使用する証明書ファイル。

共有フォルダーの定義

管理サーバーのインストール後、管理サーバーのプロパティで共有フォルダーの場所を指定できます。既定では、共有フォルダーは管理サーバーがインストールされたデバイスに作成されます。ただし、特定のケース（高負荷、分離されたネットワークからのアクセスが必要な場合など）においては、共有フォルダーを専用ファイルリソースに置くのが適切な方法です。

共有フォルダーは、ネットワークエージェントの導入時に使用されることもあります。

共有フォルダーでは、大文字と小文字の区別を無効にする必要があります。

Kaspersky Security Center Linux のアップグレード

管理サーバーのバージョン 14 をそれより前のバージョンの管理サーバー（バージョン 13 以降）がインストールされたデバイスにインストールすることができます。バージョン 14 にアップグレードすると、旧バージョンの管理サーバーのデータと設定がすべて維持されます。

アップグレード中、管理サーバーと別のアプリケーションで同時に DBMS を使用することは厳重に禁じられています。

次のいずれかの方法を使用して、管理サーバーのバージョンをアップグレードできます：

- Kaspersky Security Center インストールファイルを使用する
- 管理サーバーのデータのバックアップを作成し、管理サーバーの新しいバージョンをインストールして、バックアップから管理サーバーのデータを復元する

ネットワークに複数の管理サーバーが含まれている場合は、それぞれのサーバーを手動でアップグレードする必要があります。Kaspersky Security Center Linux では集中アップグレードはサポートされません。

Kaspersky Security Center Linux を旧バージョンからアップグレードすると、サポート対象のカスペルスキー製品のインストール済みプラグインはすべて残ります。管理サーバープラグインとネットワークエージェントプラグインは自動的にアップグレードされます。

インストールファイルを使用した Kaspersky Security Center Linux のアップグレード

管理サーバーを旧バージョン（バージョン 13 以降）からバージョン 14 にアップグレードするには、 Kaspersky Security Centerインストールファイルを使用して、旧バージョンに新しいバージョンを上書きインストールできます。

インストールファイルを使用して旧バージョンの管理サーバーをバージョン 14 にアップグレードするには：

1. カスペルスキーの Web サイトから、バージョン 14 の完全なパッケージを含む Kaspersky Security Center インストールファイルをダウンロードします：
   - RPM ベースのオペレーティングシステムを実行しているデバイスの場合 — ksc64-<バージョン番号>-11247.x86_64.rpm
   - Debian ベースのオペレーティングシステムを実行しているデバイスの場合 — ksc64_<バージョン番号>-11247_amd64.deb
2. 管理サーバーで使用するパッケージマネージャーを使用して、インストールパッケージをアップグレードします。たとえば、ルート権限を持つアカウントで、コマンドラインターミナルを使用して次のコマンドを使用できます：
   - RPM ベースのオペレーティングシステムのデバイスの場合：
     `$ sudo rpm -Uvh --nodeps --force ksc64-<バージョン番号>-11247.x86_64.rpm`
   - Debian ベースのオペレーティングシステムのデバイスの場合：
     `$ sudo dpkg -i ksc64_<バージョン番号>-11247_amd64.deb`

コマンドが正常に実行されると、/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl スクリプトが作成されます。これに関するメッセージがターミナルに表示されます。

3. アップグレードされた管理サーバーを設定するには、/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl スクリプトを実行します。

4. コマンドラインターミナルに表示される使用許諾契約書とプライバシーポリシーを読みます。使用許諾契約書とプライバシーポリシーの諸条件すべてに同意する場合：

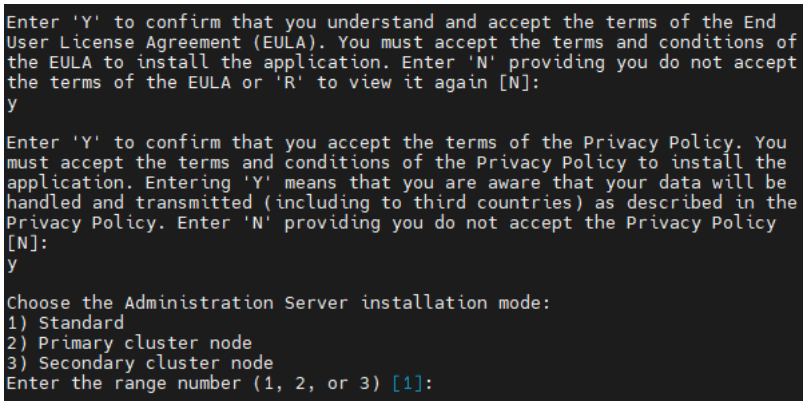
   a. 「Y」と入力して、EULA の諸条件をすべて読み、理解した上で条項に同意することを確認します。

   b. 「Y」ともう一度入力して、データの取り扱い方法を記載しているプライバシーポリシーをすべて読み、理解した上で条項に同意することを確認します。

   「Y」と 2 回入力すると、製品のデバイスへのインストールが続行されます。

5. 「1」と入力して、管理サーバーの標準インストールモードを選択します。

   下の図は、最後の 2 つの手順を示しています。



EULA とプライバシーポリシーの条項に同意し、コマンドラインターミナルで管理サーバーの標準インストールモードを選択する

   次に、スクリプトにより管理サーバーのアップグレードが設定され、終了します。アップグレード中は、アップグレード前に変更した管理サーバーの設定は変更することができません。

6. 旧バージョンのネットワークエージェントがインストールされているデバイスの場合は、新バージョンのネットワークエージェントのリモートインストールタスクを作成して実行します。

   Network Agent for Linux を Kaspersky Security Center Linux と同じバージョンにアップグレードすることを推奨します。

   リモートインストールタスクが完了すると、ネットワークエージェントのバージョンがアップグレードされます。

バックアップによる Kaspersky Security Center Linux のアップグレード

管理サーバーを旧バージョン（バージョン 13 以降）からバージョン 14 にアップグレードするには、管理サーバーデータのバックアップを作成し、新しいバージョンの Kaspersky Security Center をインストールした後でこのデータを復元します。インストール中に問題が発生した場合は、アップグレード操作の前に作成した管理サーバーデータのバックアップを使用して管理サーバーを前のバージョンに戻すことが可能です。

バックアップを使用して旧バージョンの管理サーバーをバージョン 14 にアップグレードするには：

1. アップグレードする前に、旧バージョンのアプリケーションで管理サーバーデータをバックアップします。
2. 旧バージョンの Kaspersky Security Center をアンインストールします。
3. 以前の管理サーバーに Kaspersky Security Center バージョン 14 をインストールします。
4. アップグレード前に作成したバックアップから管理サーバーデータを復元します。
5. 旧バージョンのネットワークエージェントがインストールされているデバイスの場合は、新バージョンのネットワークエージェントのリモートインストールタスクを作成して実行します。

   Network Agent for Linux を Kaspersky Security Center Linux と同じバージョンにアップグレードすることを推奨します。

   リモートインストールタスクが完了すると、ネットワークエージェントのバージョンがアップグレードされます。

Kaspersky Security Center 14 Web コンソールへのサインインとサインアウト

管理サーバーと Web コンソールサーバーのインストールが完了すると、Kaspersky Security Center 14 Web コンソールにサインインできます。インストール中に指定した管理サーバーのアドレスとポート番号の情報が必要になります（既定のポート番号は 8080 です）。ブラウザーでは、JavaScript が有効になっている必要があります。

Kaspersky Security Center 14 Web コンソールにサインインするには：

1. ブラウザーで、「<管理サーバーの Web アドレス>:<ポート番号>」にアクセスします。

   サインインページが表示されます。

2. 複数台の信頼する管理サーバーを追加している場合、管理サーバーのリストから接続する管理サーバーを選択します。

   管理サーバーを 1 台しか追加していない場合、**ユーザー名**と**パスワード**の入力フィールドのみが表示されます。

3. 次のいずれかの手順を実行します：

   - 物理管理サーバーにサインインするには、ローカル管理者のユーザー名とパスワードを入力します。
   - サーバー上に 1 つ以上の仮想管理サーバーが作成されており、仮想サーバーにサインインしたい場合：

     a. ［**詳細設定**］をクリックします。

     b. 仮想サーバーの作成時に指定した仮想管理サーバー名を入力します。

     c. 仮想管理サーバーの権限を持つ管理者のユーザー名とパスワードを入力します。

サインイン後、ダッシュボードが表示されます。言語設定とテーマは、前回使用したものが使用されます。Kaspersky Security Center 14 Web コンソールを操作して、Kaspersky Security Center Linux による処理を実行できます。

Kaspersky Security Center 14 Web コンソールからサインアウトするには：

メインメニューで、アカウント設定に移動して、［**ログアウト**］を選択します。

Kaspersky Security Center 14 Web コンソールが終了し、サインインページが表示されます。

クイックスタートウィザード

Kaspersky Security Center Linux では、セキュリティ上の脅威から社内ネットワークを保護するための一元的な管理システムを構築する上で調整が必要な最小限の設定項目が選定されており、これらの設定を編集してセキュリティ管理システムを構築できます。この設定は、クイックスタートウィザードを使用して行います。ウィザードの実行中、次の変更をアプリケーションに対して行うことができます：

- 管理グループ内のデバイスに自動配信可能なライセンス情報ファイルを追加するか、アクティベーションコードを入力します。
- 管理サーバーと管理対象アプリケーションの動作中に発生したイベントを通知するメール配信を設定します（通知が正しく送信されるようにするには、管理サーバーとすべての受信側デバイスで Messenger サービスが稼働している必要があります）。
- 管理対象デバイスの最上位階層で、ワークステーションとサーバーの保護ポリシー、およびウイルススキャンタスク、アップデートのダウンロードタスク、データバックアップタスクを作成します。

  クイックスタートウィザードでは、［**管理対象デバイス**］フォルダーにポリシーがないアプリケーションに対してのみポリシーが作成されます。管理対象デバイスの最上位階層で同じ名前のタスクが作成済みの場合、クイックスタートウィザードではタスクが作成されません。

管理サーバーのインストール後に初めて接続すると、クイックスタートウィザードを実行することを指示するメッセージが自動的に表示されます。また、クイックスタートウィザードはいつでも手動で起動できます。

クイックスタートウィザードを手動で起動するには：

1. メインメニューで、管理サーバーの名前の横にある設定アイコン（）をクリックします。

   管理サーバーのプロパティウィンドウが開きます。
2. ［**全般**］タブで、［**全般**］セクションを選択します。
3. ［**クイックスタートウィザードを開始**］をクリックします。

   管理サーバーの初期設定を実行するように指示されます。ウィザードの指示に従ってください。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

ステップ 1.インターネット接続設定の指定

管理サーバーのインターネットアクセスを設定します。Kaspersky Security Network を使用し、Kaspersky Security Center Linux 向けおよび管理対象カスペルスキー製品向けの定義データベースのアップデートをダウンロードするには、インターネットアクセスを設定する必要があります。

インターネットへの接続時にプロキシサーバーを使用する場合は、［**プロキシサーバーを使用する**］をオンにします。このオプションをオンにすると、設定を入力するフィールドが使用可能になります。プロキシサーバーの接続を次のように設定します：

- **アドレス**

  インターネットへの Kaspersky Security Center Linux の接続に使用するプロキシサーバーのアドレス。

- **ポート番号**

  Kaspersky Security Center Linux でプロキシサーバーへの接続を確立するポートの番号。

- **ローカルアドレスにプロキシサーバーを使用しない**

  ローカルネットワークのデバイスへの接続にプロキシサーバーを使用しません。

- **プロキシサーバー認証**

  このチェックボックスをオンにすると、入力フィールドでプロキシサーバーの資格情報を指定できます。

  ［**プロキシサーバーを使用する**］をオンにすると、この入力フィールドが使用可能になります。

- **ユーザー名**

  プロキシサーバーへの接続の確立に使用されるユーザーアカウント（［**プロキシサーバー認証**］をオンにした場合に有効になります）。

- **パスワード**

  プロキシサーバーへの接続の確立に使用されるアカウントのユーザーが設定したパスワード（［**プロキシサーバー認証**］をオンにした場合に有効になります）。

  入力したパスワードを表示するには、確認する間だけ［**入力した文字を表示する**］をクリックしたままにします。

クイックスタートウィザードを使用せずに、後からインターネットアクセスを設定することもできます。

ステップ 2：アプリケーションのアクティベート方法の選択

Kaspersky Security Center Linux のアクティベーションオプションのいずれかを選択します：

- **アクティベーションコードを入力**

  *アクティベーションコード*は、英数字 20 文字の一意な並びで構成されます。アクティベーションコードを入力すると、Kaspersky Security Center Linux をアクティベートするライセンス情報を追加することができます。アクティベーションコードは、Kaspersky Security Center を購入すると、指定したメールアドレスに届きます。

  アクティベーションコードで製品をアクティベートするには、カスペルスキーのアクティベーションサーバーと接続を確立するためのインターネット接続が必要です。

  このアクティベーションオプションを選択すると、［**管理対象デバイスにライセンスを自動的に配信する**］を有効にできます。

  このオプションを有効にすると、ライセンスが管理対象デバイスに自動的に適用されます。

  このオプションをオフにすると、メインメニューの［**操作**］→［**ライセンス管理**］→［**カスペルスキーのライセンス**］で、後で管理対象デバイスにライセンスを適用できます。

- **ライセンス情報ファイルを指定**

  *ライセンス情報ファイル*は、拡張子「key」のファイルであり、カスペルスキーから提供されます。ライセンス情報ファイルを製品に追加し、製品をアクティベートする目的で作成されています。

  ライセンス情報ファイルは、Kaspersky Security Center を購入すると、指定したメールアドレスに届きます。

  ライセンス情報ファイルでのアクティベーション時には、カスペルスキーのアクティベーションサーバーへの接続は必要ありません。

  このアクティベーションオプションを選択すると、［**管理対象デバイスにライセンスを自動的に配信する**］を有効にできます。

  このオプションを有効にすると、ライセンスが管理対象デバイスに自動的に適用されます。

  このオプションをオフにすると、メインメニューの［**操作**］→［**ライセンス管理**］→［**カスペルスキーのライセンス**］で、後で管理対象デバイスにライセンスを適用できます。

- アプリケーションのアクティベーションを後で実行

アプリケーションのアクティベーションを延期する場合は、メニューの［**操作**］→［**ライセンス管理**］を選択して後でいつでもライセンスを追加できます。

有料 AMI または月単位の従量課金の SKU から導入した Kaspersky Security Center で作業を行う場合は、ライセンス情報ファイルを指定したりアクティベーションコードを入力することはできません。

ステップ 3：基本的なネットワーク保護の設定情報の作成

作成されたポリシーとタスクのリストを確認できます。

ポリシーとタスクの作成が完了してから、ウィザードの次のステップに進んでください。

ステップ 4：メール通知の設定

クライアントデバイス上のカスペルスキー製品の実行中に登録されたイベントに関する通知の配信方法を設定します。この設定は、アプリケーションポリシーの既定の設定として使用されます。

カスペルスキー製品で発生したイベントに関する通知の配信を設定するには、次の設定を使用します：

- **受信者（メールアドレス）**

  通知が送られるユーザーのメールアドレスです。1つ以上のアドレスを入力できます。複数のアドレスを入力する場合はセミコロンで区切ってください。

- **SMTP サーバーアドレス**

  組織のメールサーバーのアドレスです。

  複数のアドレスを入力する場合はセミコロンで区切ってください。次の値を使用できます：

  - IPv4 / IPv6 アドレス
  - SMTP サーバーの DNS 名

- **SMTP サーバーのポート**

  SMTP サーバーの通信ポート番号。複数の SMTP サーバーを使用する場合、それらサーバーへの接続は指定された通信ポートを介して確立されます。既定のポート番号は 25 です。

- **ESMTP 認証を使用する**

  ESMTP 認証のサポートを有効にします。チェックボックスをオンにすると、［**ユーザー名**］と［**パスワード**］で ESMTP 認証を設定できます。既定では、このチェックボックスはオフです。

［**テストメッセージの送信**］をクリックして、新しいメール通知設定をテストできます。

ステップ 5.クイックスタートウィザードの終了

ウィザードを終了するには、［**終了**］をクリックします。

クイックスタートウィザードを終了したら、製品導入ウィザードを実行して、セキュリティプログラムまたはネットワークエージェントをネットワーク上のデバイスに自動的にインストールできます。

製品導入ウィザード

カスペルスキー製品をインストールするには、製品導入ウィザードを使用できます。製品導入ウィザードにより、専用に作成されたインストールパッケージを使用するか、または配布パッケージから直接、アプリケーションをリモートインストールすることができます。

製品導入ウィザードにより、次の操作が実行できます：

- アプリケーションをインストールするためのインストールパッケージをダウンロードします（まだ作成されていない場合）。［**検出と製品の導入**］→［**導入と割り当て**］→［**インストールパッケージ**］の順に移動すると、インストールパッケージにアクセスできます。今後アプリケーションをインストールする時に、このインストールパッケージを使用できます。
- 特定のデバイスまたは管理グループに対するリモートインストールタスクを作成して実行します。新しく作成されたリモートインストールタスクは、［**タスク**］セクションに保存されます。このタスクは後から手動で開始できます。タスクの種別は［**アプリケーションのリモートインストール**］になります。

SUSE Linux Enterprise Server 15 オペレーティングシステムを搭載したデバイスにネットワークエージェントをインストールする場合は、ネットワークエージェントの設定前に、insserv-compat パッケージをインストールします。

製品導入ウィザードの開始

また、製品導入ウィザードはいつでも手動で起動できます。

製品導入ウィザードを手動で起動するには：

メインメニューで、［**検出と製品の導入**］→［**導入と割り当て**］→［**製品導入ウィザード**］の順にクリックします。

製品導入ウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

ステップ 1.インストールパッケージの選択

インストールする製品のインストールパッケージを選択します。

目的の製品のインストールパッケージがリストに含まれていない場合、［**追加**］をクリックしてリストから製品を選択します。

ステップ 2.ライセンス情報ファイルまたはアクティベーションコードの配信方法の選択

ライセンス情報ファイルまたはアクティベーションコードの配信方法を選択します：

- **インストールパッケージにライセンスを含めない**

次の条件を満たす場合、ライセンスは互換性のあるすべてのデバイスへ自動的に配信されます：

- ライセンスのプロパティで［自動配信］が有効になっている場合。
- ［**ライセンスの追加**］タスクが作成されている場合。

- **インストールパッケージにライセンスを含める**

ライセンスはインストールパッケージと共にデバイスへ配信されます。

共有読み取りアクセス権がインストールパッケージのリポジトリに対して有効になっているため、この方法はできるだけ使用しないでください。

インストールパッケージに既にライセンス情報ファイルまたはアクティベーションコードが含まれる場合も、同様のウィンドウが表示されますが、ライセンスの詳細情報のみが表示され、オプションは指定できません。

ステップ 3.ネットワークエージェントのバージョンの選択

ネットワークエージェント以外の製品のインストールパッケージを選択した場合でも、各製品と Kaspersky Security Center 管理サーバーとを接続するために、ネットワークエージェントのインストールが必要になります。

最新バージョンのネットワークエージェントを選択してください。

ステップ 4.デバイスの選択

アプリケーションをインストールするデバイスを指定します。

- **管理対象デバイスにインストール**

このオプションをオンにすると、デバイスのグループに対してリモートインストールタスクが作成されます。

- **インストールするデバイスの選択**

デバイスの抽出に属するデバイスにタスクを割り当てます。既存の抽出のいずれかを選択できます。

たとえば、特定のバージョンのオペレーティングシステムを使用しているデバイスを対象にタスクを実行する時に、このオプションを使用すると便利です。

ステップ 5.リモートインストールタスクの設定

［**リモートインストールタスク設定**］ウィンドウで、アプリケーションのリモートインストール設定を指定します。

［**インストールパッケージの強制ダウンロード**］セクションで、アプリケーションのインストールに必要なファイルをクライアントデバイスに配布する方法を指定します。

- **ネットワークエージェントを使用する**

  このオプションをオンにすると、インストールパッケージのクライアントデバイスへの配布は、クライアントデバイスにインストールされたネットワークエージェントによって行われます。

  このオプションをオフにすると、インストールパッケージはクライアントデバイスのオペレーティングシステムのツールを使用して配信されます。

  ネットワークエージェントがインストールされたデバイスにタスクが割り当てられている場合は、このチェックボックスをオンにすることを推奨します。

  既定では、このオプションはオンです。

- **ディストリビューションポイントを通じてオペレーティングシステムの共有フォルダーを使用する**

  このオプションをオンにすると、ディストリビューションポイントがオペレーティングシステムのツールを使用してインストールパッケージをクライアントデバイスに送信します。この機能が使用できるのは、ネットワークに少なくとも1つのディストリビューションポイントがある場合です。

  ［**ネットワークエージェントを使用する**］をオンにすると、ネットワークエージェントのツールが使用できない場合に限り、ファイルがオペレーティングシステムのツールで配布されます。

  既定では、仮想管理サーバーで作成されたリモートインストールタスクに対して、このオプションはオンです。

  Network Agent がインストールされていないデバイスに Windows 用のアプリケーション（Windows 用ネットワークエージェントを含む）をインストールするには、Windows ベースのディストリビューションポイントを使用するのが唯一の方法です。したがって、Windows アプリケーションをインストールする場合：

  - このオプションをオンにします。
  - ターゲットのクライアントデバイスにディストリビューションポイントが割り当てられていることを確認します。
  - ディストリビューションポイントが Windows ベースであることを確認します。

詳細設定を行います：

アプリケーションが既にインストールされている場合再インストールしない

このオプションをオンにすると、選択したアプリケーションがクライアントデバイスに既にインストールされていた場合、インストールされません。

このオプションをオフにすると、アプリケーションは常にインストールされます。

既定では、このオプションはオンです。

ステップ6：インストール前に競合アプリケーションを削除する

この手順の実施ウィンドウは、インストール対象の製品に既知の競合アプリケーションが存在する場合にのみ表示されます。

インストール対象の製品と互換性がないアプリケーションを自動的に削除するには、オプションをオンにします。

互換性がない競合アプリケーションのリストも表示されます。

このオプションをオフにした場合、インストール対象の製品は、競合アプリケーションがインストールされていないデバイスにのみインストールされます。

ステップ 7：管理対象デバイスへのデバイスの移動

ネットワークエージェントのインストール後に、デバイスを管理グループに移動するかどうかを指定します。

- **デバイスを移動しない**

  デバイスは、現在配置されているグループから移動しません。どのグループにも割り当てられていないデバイスは、未割り当てのままとなります。

- **未割り当てデバイスをグループへ移動**

  指定した管理グループにデバイスが移動されます。

既定では［**デバイスを移動しない**］がオンになっています。セキュリティ上の理由のため、場合によってはデバイスを手動で移動する必要があります。

ステップ 8：デバイスにアクセスするアカウントの選択

必要に応じて、リモートインストールタスクの開始に使用するアカウントを追加できます：

- **アカウントが不要（ネットワークエージェントインストール済み）**

  このオプションをオンにすると、アプリケーションのインストーラーを実行するアカウントを指定する必要はありません。タスクは管理サーバーのサービスを実行しているアカウントで実行されます。

  クライアントデバイスにネットワークエージェントがインストールされていない場合、このオプションは使用できません。

- **アカウントが必要（ネットワークエージェントの使用なし）**

  リモートインストールタスクを割り当てるデバイスにネットワークエージェントがインストールされていない場合は、このオプションをオンにします。この場合、ユーザーアカウントを指定して、アプリケーションをインストールできます。

  アプリケーションインストーラーを実行するユーザーアカウントを指定するには、［**追加**］をクリックし、［**ローカルアカウント**］を選択して、ユーザーアカウントの資格情報を指定します。

  タスクを割り当てるすべてのデバイスで必要なすべての権限をどのアカウントも持たない場合などのために、複数のユーザーアカウントを追加できます。この場合、追加されたすべてのアカウントが上から下へ順番に使用され、タスクが実行されます。

ステップ 9：インストールの開始

このウィンドウがこのウィザードでの最後のステップです。このステップを完了すると、**リモートインストールタスク**の作成と設定が完了します。

既定では、［**ウィザードの終了後にタスクを実行**］はオフになっています。このオプションをオンにすると、ウィザードの完了後すぐに**リモートインストールタスク**が開始されます。このオプションをオフにすると、**リモートインストールタスク**は開始されません。このタスクは後から手動で開始できます。

製品導入ウィザードを完了するには、［**OK**］をクリックします。

管理サーバーの設定

このセクションでは、Kaspersky Security Center Linux 管理サーバーの設定手順とプロパティについて説明しています。

Kaspersky Security Center 14 Web コンソールから管理サーバーへの接続の設定

管理サーバーへの接続ポートを設定するには：

1. 画面上部の管理サーバー名のセクションで目的の管理サーバーを選択し、隣接する設定アイコン（）をクリックします。

   管理サーバーのプロパティウィンドウが開きます。

2. ［**全般**］タブで、［**接続ポート**］セクションを選択します。

選択したサーバーのメインの接続設定が表示されます。

Kaspersky Security Center にログインするための IP アドレスの許可リストの設定

既定では、ユーザーは、Kaspersky Security Center 14 Web コンソール（以降「Web コンソール」と表記）を開くことができる任意のデバイスで Kaspersky Security Center にログインできます。ただし、管理サーバーを設定することで、ユーザーが許可された IP アドレスを持つデバイスからのみ管理サーバーに接続できるように設定できます。こうすると、侵入者が Kaspersky Security Center アカウントを盗んだとしても、侵入者のデバイスの IP アドレスが許可リストに登録されていないため、Kaspersky Security Center にログインすることはできません。

ユーザーが Kaspersky Security Center にログインするか、Kaspersky Security Center OpenAPI を介して管理サーバーと連携するアプリケーションを実行した場合に IP アドレスが検証されます。この時点で、ユーザーのデバイスは管理サーバーとの接続を確立しようとします。デバイスの IP アドレスが許可リストにない場合、認証エラーが発生し、KLAUD_EV_SERVERCONNECT イベントが管理サーバーとの接続が確立されていないことを通知します。

IP アドレスの許可リストの要件

次のアプリケーションが管理サーバーに接続しようとした際にのみ IP アドレスが検証されます：

- Web コンソールサーバー

  Web コンソールを介して Kaspersky Security Center にログオンすると、オペレーティングシステムの標準の方法で、Web コンソールサーバーがインストールされているデバイスのファイアウォールを設定することができます。誰かがあるデバイスから Kaspersky Security Center にログインしようとした場合、Web コンソールサーバーが別のデバイスにインストールされていると、ファイアウォールが侵入者の干渉防止に役立ちます。

- Klakaut 自動化オブジェクト経由で管理サーバーと連携しているアプリケーション

- Kaspersky Anti Targeted Attack Platform または Kaspersky Security for Virtualization のような、OpenAPI 経由で管理サーバーと連携するアプリケーション

このため、上のリストにあるアプリケーションがインストールされているデバイスのアドレスを指定してください。

IPv4 と IPv6 アドレスを指定できます。IP アドレスの範囲を指定することはできません。

IP アドレスの許可リストを設定する方法

事前に許可リストを設定していなかった場合は、次の手順に従ってください。

Kaspersky Security Center にログインするための IP アドレスの許可リストを設定するには：

1. 管理サーバーデバイスで、管理者権限を持つアカウントでコマンドプロンプトを実行します。
2. カレントディレクトリを Kaspersky Security Center のインストールフォルダ（通常は /opt/kaspersky/ksc64/sbin）に変更します。
3. 管理者権限を使用して次のコマンドを入力します：
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<IP アドレス>" -t s`

   前述の要件を満たす IP アドレスを指定します。複数の IP アドレスを指定する場合はセミコロンで区切ります。

   単一のデバイスに対して管理サーバーへの接続を許可する方法の例：

   ```
   klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0" -t s
   ```

   複数のデバイスに対して管理サーバーへの接続を許可する方法の例：

   ```
   klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0; 198.51.100.0; 203.0.113.0" -t s
   ```
4. 管理サーバーサービスを再起動します。

管理サーバーの SysLog イベントログで、IP アドレスの許可リストが正常に設定されているかどうかを確認できます：

IP アドレスの許可リストを変更する方法

最初に許可リストを作成した方法と同じ方法で許可リストを変更できます。同じコマンドを実行して新しい許可リストの名前を指定します。

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<IP アドレス>" -t s
```

許可リストから一部の IP アドレスを削除する場合は、書き直します。たとえば、許可リストに IP アドレス「198.51.100.0; 203.0.113.0」が含まれているとします。IP アドレス「198.51.100.0」を削除したいとします。この場合、コマンドプロンプトで次のコマンドを入力します：

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0; 203.0.113.0" -t s
```

管理サーバーサービスを忘れずに再起動してください。

設定済みの IP アドレスの許可リストをリセットする方法

既に設定済みの IP アドレスの許可リストをリセットするには：

1. 管理者権限を使用し、コマンドプロンプトで次のコマンドを入力します：
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "" -t s`

2. 管理サーバーサービスを再起動します。

その後、IP アドレスは検証されなくなります。

管理サーバーへの接続のログの表示

動作中の管理サーバーへの接続と接続試行の履歴がログファイルに保存されます。ログファイル内の情報により、ネットワークインフラストラクチャ内の接続だけでなく、サーバーに対する不正アクセスの試行についても追跡できます。

管理サーバーへの接続イベントのログを記録するには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。

2. ［**全般**］タブで、［**接続ポート**］セクションを選択します。

3. ［**管理サーバーへの接続イベントを記録する**］をオンにします。

管理サーバーの受信接続イベント、認証の結果、SSL エラーが「%ProgramData%\KasperskyLab\adminkit\logs\sc.syslog」ファイルに記録されます。

イベントのリポジトリに保管できるイベントの最大数の設定

管理サーバーのプロパティウィンドウ内にある［**イベントリポジトリ**］セクションで、管理サーバーデータベース内で保管するイベントの設定を編集できます。編集可能な設定項目は、イベントのレコード数上限やレコードの保管期間があります。保管するイベント数の上限を指定すると、指定した数に応じて必要なディスク容量の概算値が算出されます。データベースのオーバーフローを避けるために十分な空き容量があるかどうかのこの概算値を使用できます。既定の設定では、管理サーバーデータベース内に保管できるイベント数は 400,000 件までとなっています。データベースで推奨される範囲でのイベント数の上限は、45,000,000 件です。

データベースのイベント数が管理者によって指定された上限に達すると、最も古いイベントが削除されて、新しいイベントに置き換えられます。管理サーバーが古いイベントを削除する際に、新しいイベントのデータベースへの保存は行えません。この期間、拒否したイベントの情報は Kaspersky イベントログに書き込まれます。新しいイベントはキューに追加され、削除操作が完了した後にデータベースに保存されます。

管理サーバーのイベントリポジトリに保存できるイベント数を制限するには：

1. 画面上部の管理サーバー名のセクションで目的の管理サーバーを選択し、隣接する設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。

2. ［**全般**］タブで、［**イベントリポジトリ**］セクションを選択します。データベースに記録するイベント数の上限を指定します。

3. ［**保存**］をクリックします。

管理サーバーデータのバックアップと復元

データバックアップにより、データを失わずに、管理サーバーをデバイス間で移動できます。バックアップを使用すると、管理サーバーのデータベースを別のデバイスに移動した時や、新しいバージョンの Kaspersky Security Center にアップグレードした時に、データを復元できます。

インストールされている管理プラグインはバックアップされないこと留意してください。管理サーバーのデータをバックアップコピーから復元した後で、管理対象アプリケーション用のプラグインをダウンロードして再インストールする必要があります。

次の方法のいずれかを使用して、管理サーバーデータのバックアップコピーを作成できます。

- Kaspersky Security Center 14 Web コンソールで、データバックアップタスクを作成して実行する。
- 管理サーバーがインストールされているデバイスで klbackup ユーティリティを実行する。このユーティリティは、Kaspersky Security Center の配布キットに含まれています。管理サーバーをインストールすると、このユーティリティは、アプリケーションのインストール時に指定したインストール先フォルダー（通常は /opt/kaspersky/ksc64/sbin/klbackup）のルートに格納されます。

次のデータが管理サーバーのバックアップコピー内に保存されます：

- 管理サーバーのデータベース（管理サーバーに保存されているポリシー、タスク、アプリケーション設定、イベント）
- 管理グループとクライアントデバイスの構造についての設定情報
- リモートインストール用アプリケーション配布パッケージのリポジトリ
- 管理サーバー証明書

管理サーバーデータを復元するには、klbackup ユーティリティを使用する必要があります。

管理サーバーのデータバックアップタスクの作成

バックアップタスクは管理サーバーのタスクであり、クイックスタートウィザードで作成されます。クイックスタートウィザードで作成されたバックアップタスクが削除された場合、手動で作成することができます。

［*管理サーバーデータのバックアップ*］タスクは1つのみ作成できます。管理サーバーの管理サーバーデータのバックアップタスクが既に作成されている場合は、タスク種別選択ウィンドウには表示されません。

管理サーバーのデータバックアップタスクを作成するには：

1. ［**デバイス**］→［**タスク**］の順に選択します。
2. ［**追加**］をクリックします。
   タスク追加ウィザードが開始されます。
3. ウィザードの最初のページで、［**アプリケーション**］リストから［**Kaspersky Security Center 14**］を選択し、［**タスク種別**］リストから［**管理サーバーデータのバックアップ**］を選択します。
4. ウィザードの対応するページで、次の情報を指定します：
   - バックアップコピーの保管用のフォルダー
   - バックアップのパスワード（省略可能）
   - 保存するバックアップコピー数の最大値
5. ［**タスク作成の終了**］ページで［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにした場合、既定のタスク設定を編集できます。このオプションをオフにすると、既定の設定でタスクが作成されます。既定の設定からの変更は、後からいつでも実行できます。
6. ［**終了**］をクリックします。

タスクが作成され、タスクリストに表示されます。

klbackup ユーティリティーを使用してデータをバックアップおよびリカバリーする

バックアップと将来の復元に備えて、Kaspersky Security Center 配布キットに含まれている klbackup ユーティリティを使用して、管理サーバーのデータをコピーできます。

非対話モードで管理サーバーデータをバックアップまたは復元するには：

管理サーバーがインストールされているデバイスのコマンドラインで、必要なキーを指定して klbackup を実行します。

ユーティリティのコマンドライン構文は次の通りです：

```
klbackup -path <バックアップパス> [-logfile <ログファイル名>] [-use_ts]|[-restore] [-password <パスワード>] [-online]
```

> klbackup ユーティリティのコマンドラインでパスワードを指定しないと、対話形式でパスワードを入力するように指示されます。

キーの説明：

- `-path <バックアップパス>` – <バックアップパス> で指定したフォルダーに情報を保存します。または、<バックアップパス> で指定したフォルダーのデータを使用して復元を実行します（必須パラメータ）。
- `-logfile <ログファイル名>` – 管理サーバーデータのバックアップと復元に関するレポートを保存します。

データベースサーバーのアカウントと klbackup ユーティリティには、<バックアップパス> で指定したフォルダーのデータを変更するアクセス権を付与する必要があります。

- `-use_ts` – データを保存する時に、<バックアップパス> で指定したフォルダーの、現在のシステム日付と処理時刻が付いたサブフォルダー（`klbackup YYYY-MM-DD # HH-MM-SS` 形式）に情報をコピーします。キーを指定しない場合は、<バックアップパス> で指定したフォルダーのルートに保存されます。

  既にバックアップコピーがあるフォルダーに情報を保存しようとすると、エラーメッセージが表示されます。情報は更新されません。

  `-use_ts` キーを使用することで、管理サーバーデータのアーカイブを保持することができます。たとえば、`-path` キーにフォルダー `C:\KLBackups` を指定した場合、フォルダー `klbackup 2022/6/19 # 11-30-18` には、2022 年 6 月 19 日午前 11 時 30 分 18 秒時点の管理サーバーのステータス情報が保存されます。

- `-restore` – 管理サーバーデータを復元します。データ復元は <バックアップパス> で指定したフォルダーの情報に基づいて実行されます。このキーを指定しない場合、データは <バックアップパス> で指定したフォルダーにバックアップされます。

- `-password` <パスワード> – 管理サーバー証明書を保存または復元します。証明書の暗号化と復号化には、<パスワード> で指定したパスワードが使用されます。

  パスワードを忘れた場合、復元できません。パスワードに条件はありません。パスワードの長さは無制限です。また、0 文字（パスワードを設定しない）も可能です。

  データを復元する時は、バックアップ時に入力したパスワードを指定します。共有フォルダーへのパスがバックアップ後に変更された場合は、復元されたデータを使用するタスクの操作（復元タスクとリモートインストールタスク）を確認します。必要に応じて、これらのタスクの設定を編集します。バックアップファイルからのデータの復元中は、共有フォルダーまたは管理サーバーにアクセスしないでください。klbackup ユーティリティを開始するアカウントは、共有フォルダーへのフルアクセスの権限を持っている必要があります。新しくインストールした管理サーバーでユーティリティを実行することを推奨します。

- `-online` – 不具合などによる管理サーバーのオフライン時間を最小限にするために、ボリュームスナップショットを作成して管理サーバーのデータをバックアップします。データを復元するためにこの機能を使用する場合は、このオプションは必要ありません。

管理サーバーの別のデバイスへの移動

新しいデバイスで管理サーバーを使用する必要がある場合は、次のいずれかの方法で移動できます：

- 管理サーバーとデータベースサーバーを新しいデバイスに移動する。
- データベースサーバーを以前のデバイスに保持し、管理サーバーのみを新しいデバイスに移動する。

管理サーバーとデータベースサーバーを新しいデバイスに移動するには：

1. 以前のデバイスで、管理サーバーデータのバックアップを作成します。

   このためには、Kaspersky Security Center 14 Web コンソールからデータバックアップタスクを実行するか、 klbackup ユーティリティを実行します。

2. 管理サーバーをインストールする新しいデバイスを選択します。選択したデバイスのハードウェアとソフトウェアが、管理サーバー、 Kaspersky Security Center 14 Web コンソール、およびネットワークエージェントの要件を満たしていることを確認してください。また、管理サーバーで使用されるポートが使用可能であることを確認してください。

3. 新しいデバイスで、管理サーバーが使用するデータベース管理システム（DBMS）をインストールします。
   DBMS を選択する際は、管理サーバーが対応するデバイスの数を考慮してください。

4. 新しいデバイスに管理サーバーをインストールします。
   データベースサーバーを新しいデバイスに移動する場合は、データベースがインストールされているデバイスの IP アドレスとして、ローカルアドレスを指定してください（Kaspersky Security Center のインストール手順の「h」項目）。データベースサーバーを以前のデバイスに保持する必要がある場合は、Kaspersky Security Center のインストール手順の「h」項目で以前のデバイスの IP アドレスを入力します。

5. インストールが完了したら、klbackup ユーティリティを使用して、新しいデバイスで管理サーバーのデータを復元します。

   以前のデバイスと新しいデバイスで SQL Server を DBMS として使用する場合、新しいデバイスにインストールされている SQL Server のバージョンは、以前のデバイスにインストールされている SQL Server のバージョンと同じかそれ以降である必要があります。それ以外のバージョンの場合、新しいデバイスで管理サーバーのデータを復元できません。

6. Kaspersky Security Center 14 Web コンソールを開き、管理サーバーに接続します。

7. すべてのクライアントデバイスが管理サーバーに接続されていることを確認します。

8. 以前のデバイスから管理サーバーとデータベースサーバーをアンインストールします。

仮想管理サーバーの作成

仮想管理サーバーを作成して、管理グループに追加できます。

仮想管理サーバーを作成して追加するには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。

2. 表示されるウィンドウで、［**管理サーバー**］タブに移動します。

3. 仮想管理サーバーを追加する管理グループを選択します。
   仮想管理サーバーは選択したグループ（サブグループを含む）からデバイスを管理します。

4. メニューのリストから［**新しい仮想管理サーバー**］を選択します。

5. 表示されるウィンドウで、新しい仮想管理サーバーのプロパティを指定します。

   - **仮想管理サーバー名**
   - **管理サーバー接続用アドレス**
     管理サーバーの名前または IP アドレスを指定できます。

6. ユーザーのリストから、仮想管理サーバーの管理者を選択します。必要に応じて、既存のアカウントを管理者ロールに割り当てる前にこのアカウントを編集したり、新しいアカウントを作成したりできます。

7. ［**保存**］をクリックします。

新しい仮想管理サーバーが作成され、［**管理サーバー**］タブで表示されていた管理グループに追加されます。

Kaspersky Security Center 14 Web コンソールでプライマリ管理サーバーに接続しており、セカンダリ管理サーバーによって管理されている仮想管理サーバーに接続できない場合は、次のいずれかの方法を使用できます：

- **Kaspersky Security Center 14 Web コンソールの既存のインストールを変更して、セカンダリサーバーを信頼できる管理サーバーのリストに追加します**。その後、 Kaspersky Security Center 14 Web コンソールで仮想管理サーバーに接続できるようになります。

  1. Kaspersky Security Center 14 Web コンソールがインストールされているデバイスで、デバイスにインストールされている Linux ディストリビューションに対応する Web コンソールのインストールファイルを管理者権限を持つアカウントで実行します。
  2. セットアップウィザードが起動します。
  3. ウィザードの最初のページで、［**アップグレード**］を選択します。
  4. ［**変更の種別**］ページで、［**接続設定の編集**］を選択します。
  5. ［**信頼済みの管理サーバー**］ページで、必要なセカンダリ管理サーバーを追加します。
  6. セットアップウィザードの最終ページで［**変更**］をクリックし、新しい設定を適用します。
  7. Web コンソールの再設定が正常に完了したら、［**終了**］をクリックします。

- Kaspersky Security Center 14 Web コンソールを使用して、仮想サーバーが作成されたセカンダリ管理サーバーに直接接続します。その後、Kaspersky Security Center 14 Web コンソールで仮想管理サーバーに切り替えられるようになります。

管理サーバーの階層

1 台の MSP で、複数台の管理サーバーを稼働させる場合があります。複数台の別の管理サーバーを管理するのは不便であるため、1 つの階層を適用することができます。

階層構造では、Kaspersky Security Center Linux の管理サーバーは、Windows ベースの Kaspersky Security Center または Kaspersky Security Center Cloud コンソールのプライマリ管理サーバーが管理するセカンダリサーバーとしてのみ動作します。

2 台の管理サーバーのプライマリおよびセカンダリ設定には、次のオプションがあります：

- セカンダリ管理サーバーは、プライマリ管理サーバーからポリシーとタスクを継承することにより、設定の重複を防ぎます。
- プライマリ管理サーバーのデバイスには、セカンダリ管理サーバーのデバイスを含めることができます。
- プライマリ管理サーバーのレポートには、セカンダリ管理サーバーのデータ（詳細情報を含む）を含めることができます。

管理サーバーの階層の作成：セカンダリ管理サーバーの追加

階層構造では、Kaspersky Security Center Linux の管理サーバーは、Windows ベースの Kaspersky Security Center または Kaspersky Security Center Cloud コンソールのプライマリ管理サーバーが管理するセカンダリサーバーとしてのみ動作します。

セカンダリ管理サーバーの追加（プライマリ管理サーバーとして指定する管理サーバーで実行）

管理サーバーをセカンダリ管理サーバーとして追加し、プライマリとセカンダリの階層を確立することができます。

Kaspersky Security Center 14 Web コンソールから接続できる管理サーバーをセカンダリ管理サーバーとして追加するには：

1. プライマリ管理サーバーとして指定する管理サーバーのポート 13000 にセカンダリ管理サーバーから接続できることを確認します。
2. プライマリ管理サーバーとして指定する管理サーバーで、［設定］アイコン（）をクリックします。
3. 表示されたプロパティページで、［**管理サーバー**］タブをクリックします。
4. 管理サーバーを追加する管理グループの名前に隣接するチェックボックスをオンにします。
5. メニューのリストから［**セカンダリ管理サーバーの接続**］を選択します。
   セカンダリ管理サーバーの接続ウィザードが起動します。
6. ウィザードの最初のページで、次のフィールドに値を入力します：

- **セカンダリ管理サーバーの表示名**

  階層で表示する、セカンダリ管理サーバーの名前。必要に応じて、IP アドレスを名前として入力するか、「グループ 1 のセカンダリサーバー」などの名前を使用できます。

- **セカンダリ管理サーバーアドレス（任意）**

  セカンダリ管理サーバーの IP アドレスまたはドメイン名を指定します。

- **管理サーバーの SSL ポート**

  プライマリ管理サーバー上の SSL ポート番号を指定します。既定のポート番号は 13000 です。

- **管理サーバーの API ポート**

  OpenAPI 経由の接続を受信するためのプライマリ管理サーバー上のポート番号を指定します。既定のポート番号は 13299 です。

- **プライマリ管理サーバーを DMZ 内のセカンダリ管理サーバーに接続する**

セカンダリ管理サーバーが非武装地帯（DMZ）にある場合は、このオプションをオンにします。

このオプションを選択すると、プライマリ管理サーバーがセカンダリ管理サーバーへの接続を開始します。あるいは、セカンダリ管理サーバーがプライマリ管理サーバーへの接続を開始します。

- **プロキシサーバーを使用する**

  プロキシサーバーを使用してセカンダリ管理サーバーに接続する場合は、このオプションをオンにします。

  この場合、プロキシサーバーの次の設定も指定する必要があります：

  - **アドレス**
  - **ユーザー名**
  - **パスワード**

7. ウィザードの以降の指示に従います。

ウィザードが完了すると、プライマリとセカンダリの階層が構築されます。プライマリとセカンダリの管理サーバー間の接続は、ポート 13000 で確立されます。プライマリ管理サーバーからのタスクとポリシーが受信および適用されます。プライマリ管理サーバー上の追加先の管理グループにセカンダリ管理サーバーが表示されます。

セカンダリ管理サーバーの追加（セカンダリ管理サーバーとして指定する管理サーバーで実行）

セカンダリ管理サーバーとして指定する管理サーバーが一時的に切断されていた、または使用できなかったため、この管理サーバーに接続できなかった場合も、セカンダリ管理サーバーを追加できます。

Kaspersky Security Center 14 Web コンソールから接続できない管理サーバーをセカンダリ管理サーバーとして追加するには：

1. セカンダリ管理サーバーとして指定する管理サーバーがあるオフィスのシステム管理者に、プライマリ管理サーバーとして指定する管理サーバーの証明書ファイルを渡します（たとえば、フラッシュドライブなどの外部デバイスにファイルを書き込んで送付したり、メールで送信したりできます）。

   証明書ファイルは、プライマリ管理サーバーとして指定する管理サーバーの /var/opt/kaspersky/klnagent_srv/1093/cert/ にあります。

2. セカンダリ管理サーバーとして指定する管理サーバーを担当しているシステム管理者に、次の操作を依頼します：

   a. 設定アイコン（）をクリックします。

   b. 表示されるプロパティページで、［**全般**］タブの［**管理サーバーの階層**］セクションに移動します。

   c. ［**この管理サーバーをセカンダリ管理サーバーとして使用する**］を選択します。

   d. ［**プライマリ管理サーバーのアドレス**］に、プライマリ管理サーバーのネットワーク名を入力します。

   e. ［**参照**］をクリックして、プライマリ管理サーバーとして指定する管理サーバーの保存した証明書ファイルを選択します。

f. 必要に応じて、［**プライマリ管理サーバーを DMZ 内のセカンダリ管理サーバーに接続する**］をオンにします。

g. プロキシサーバーを使用してセカンダリ管理サーバーとして指定する管理サーバーに接続する場合、［**プロキシサーバーを使用する**］をオンにして接続設定を指定します。

h. ［**保存**］をクリックします。

プライマリとセカンダリの階層が構築されます。ポート 13000 を使用して、セカンダリ管理サーバーからプライマリ管理サーバーへの接続が開始されます。プライマリ管理サーバーからのタスクとポリシーが受信および適用されます。プライマリ管理サーバー上の追加先の管理グループにセカンダリ管理サーバーが表示されます。

セカンダリ管理サーバーのリストの表示

セカンダリ管理サーバー（仮想管理サーバーを含む）のリストを表示するには：

メインメニューで、設定アイコン（）の横にある管理サーバーの名前をクリックします。

セカンダリ管理サーバー（仮想管理サーバーを含む）のドロップダウンリストが表示されます。

表示されている管理サーバーの名前をクリックすると、そのサーバーに移動できます。

管理グループも表示されますが、グレーアウトされており、このメニュー内では管理できません。

Kaspersky Security Center 14 Web コンソールでプライマリ管理サーバーに接続しており、セカンダリ管理サーバーによって管理されている仮想管理サーバーに接続できない場合は、次のいずれかの方法を使用できます：

- **Kaspersky Security Center 14 Web コンソールの既存のインストールを変更して、セカンダリサーバーを信頼できる管理サーバーのリストに追加します**。その後、 Kaspersky Security Center 14 Web コンソールで仮想管理サーバーに接続できるようになります。

  1. Kaspersky Security Center 14 Web コンソールがインストールされているデバイスで、デバイスにインストールされている Linux ディストリビューションに対応する Web コンソールのインストールファイルを管理者権限を持つアカウントで実行します。
  2. セットアップウィザードが起動します。
  3. ウィザードの最初のページで、［**アップグレード**］を選択します。
  4. ［**変更の種別**］ページで、［**接続設定の編集**］を選択します。
  5. ［**信頼済みの管理サーバー**］ページで、必要なセカンダリ管理サーバーを追加します。
  6. セットアップウィザードの最終ページで［**変更**］をクリックし、新しい設定を適用します。
  7. Web コンソールの再設定が正常に完了したら、［**終了**］をクリックします。

- Kaspersky Security Center 14 Web コンソールを使用して、仮想サーバーが作成されたセカンダリ管理サーバーに直接接続します。その後、Kaspersky Security Center 14 Web コンソールで仮想管理サーバーに切り替えられるようになります。

不正な変更からのユーザーアカウントの保護を有効にする

追加のオプションを有効にして不正な変更からのユーザーアカウントの保護を有効にすることができます。このオプションをオンにすると、ユーザーアカウントの編集にはユーザー認証が要求されます。

不正な変更からのユーザーアカウントの保護を有効または無効にする

1. メインメニューで、［**ユーザーとロール**］→［**ユーザー**］の順に移動します。
2. 不正な変更からの保護を指定する内部ユーザーアカウントの名前をクリックします。
3. ユーザー設定ウィンドウが表示されたら、［**認証セキュリティ**］を選択します。
4. アカウントの設定が変更または更新された際に毎回ユーザーの資格情報を要求するよう設定するには、［**認証セキュリティ**］タブで、［**認証を要求してユーザーアカウントの変更権限をチェックする**］を選択します。そうでない場合は、［**追加の認証なしでのこのアカウントの変更をユーザーに対して許可する**］を選択します。
5. ［**保存**］をクリックします。

二段階認証

このセクションでは、Kaspersky Security Center 14 Web コンソールへの不正なアクセスのリスクを軽減するために二段階認証を使用する方法について説明します。

シナリオ：すべてのユーザーに対して二段階認証を設定する

このシナリオでは、すべてのユーザーに対して二段階認証を有効にする方法と、二段階認証からユーザーアカウントを除外する方法について説明します。別のユーザーに対する二段階認証を有効にする前に自分のアカウントの二段階認証を有効にしなかった場合、本製品は最初にお使いのアカウントの二段階認証を有効にするウィンドウを開きます。このシナリオでは、自分のアカウントに対して二段階認証を有効にする方法についても説明します。

自分のアカウントの二段階認証を有効にした後、すべてのユーザーに対して二段階認証を有効にする手順に進んでください。

必須条件

開始する前に：

- ご自分のアカウントに、別のユーザーのアカウントのセキュリティ設定を変更するための［**一般的な機能：ユーザー権限**］機能領域のオブジェクト ACL の変更権限があることを確認してください。
- 管理サーバーの他のユーザーがデバイス上に認証アプリケーションをインストール済みであることを確認してください。

実行するステップ

すべてのユーザーに対して二段階認証を段階的に有効にするには：

1. **認証アプリケーションをデバイスにインストールする**

   Google Authenticator、Microsoft Authenticator など、Time-based One-time Password（時間に基づいて生成されるワンタイムパスワード）アルゴリズムをサポートする認証アプリケーションを使用してください。

2. **管理サーバーがインストールされているデバイスの時刻と、認証アプリケーションの時刻を同期する**

   認証アプリケーションと管理サーバーの時刻が同期されていることを確認してください。

3. **自分のアカウントの二段階認証を有効にし、アカウントの秘密鍵を受け取る**

   自分のアカウントの二段階認証を有効にした後、すべてのユーザーに対して二段階認証を有効にできるようになります。

4. **すべてのユーザーに対して二段階認証を有効にする**

   二段階認証を有効にしたユーザーは、管理サーバーにログインする際に二段階認証を使用する必要があります。

5. **セキュリティコードの発行元の名前を変更する**

   同じ名前の管理サーバーがある場合は、異なる管理サーバーとして認識できるように、セキュリティコードの発行元の名前を別のものに変更する必要があります。

6. **二段階認証を有効にする必要のないユーザーアカウントを除外する**

   必要に応じて、二段階認証からユーザーを除外することができます。アカウントが除外されたユーザーは管理サーバーへのログインの際に二段階認証が不要となります。

結果

このシナリオの完了時には：

- 自分のアカウントの二段階認証が有効になります。
- 除外したユーザーアカウント以外の管理サーバーのすべてのユーザーアカウントに対して、二段階認証が有効になります。

アカウントの二段階認証について

Kaspersky Security Center Linux では、 Kaspersky Security Center 14 Web コンソールのユーザーに対して二段階認証をサポートしています。自分のアカウントに二段階認証が適用されると、Kaspersky Security Center 14 Web コンソールにログインするたびに、ユーザー名、パスワードおよび追加で一回のみ使用するセキュリティコードを入力するようになります。このセキュリティコードを受け取るには、お使いのコンピューターまたは携帯電話などに認証アプリケーションがインストールされている必要があります。

セキュリティコードには、*発行元の名前*として参照される識別子があります。セキュリティコードの発行元の名前は、認証アプリケーションの管理サーバーの識別子として使用されます。セキュリティコードの発行元の名前を変更することができます。既定では、セキュリティコードの発行元の名前は管理サーバーの名前と同じです。発行元の名前は、認証アプリケーションの管理サーバーの識別子として使用されます。セキュリティコードの発行元の名前を変更した後は、新しい秘密鍵を発行して認証アプリケーションに渡す必要があります。セキュリティコードは1度のみ使用可能で、最大90秒間有効です（正確な時間は異なる場合があります）。

二段階認証が有効になっているユーザーは自分の秘密鍵を再発行できます。ユーザーが再発行された秘密鍵で認証しログインに使用した場合、管理サーバーはユーザーアカウントの新しい秘密鍵を保存します。ユーザーが新しい秘密鍵を誤って入力した場合、管理サーバーは新しい秘密鍵を保存せず、以降の認証は現在使用している秘密鍵を有効なままとします。

Google Authenticator など、Time-based One-time Password（時間に基づいて生成されるワンタイムパスワード）アルゴリズムをサポートする認証アプリケーションを認証アプリケーションとして使用できます。セキュリティコードを生成するためには、認証アプリケーションと管理サーバーの時刻を同期する必要があります。

認証アプリケーションは次のようにセキュリティコードを生成します：

1. 管理サーバーが特別な秘密鍵および QR コードを作成します。
2. 生成された秘密鍵または QR コードを認証アプリケーションに入力します。
3. 認証アプリケーションが、管理サーバーの認証ウィンドウに入力する、1度のみ使用するセキュリティコードを生成します。

認証アプリケーションは複数のモバイルデバイスにインストールしてください。秘密鍵または QR コードを保存し、安全な場所に保管します。これは、モバイルデバイスにアクセスできなかった際に Kaspersky Security Center 14 Web コンソールへのアクセスを復元するために必要です。

Kaspersky Security Center を安全に使用するため、自分のアカウントに対して二段階認証を設定し、すべてのユーザーに対して二段階認証を有効にできます。

二段階認証からアカウントを除外することができます。これは認証のためのセキュリティコードを受信できないサービスアカウントで必要となる場合があります。

二段階認証は次のルールに準拠して動作します：

- ［**一般的な機能：ユーザー権限**］機能領域のオブジェクト ACL の変更権限を持つユーザーアカウントのみがすべてのユーザーに対して二段階認証を有効にすることができます。
- 自分のアカウントに対して二段階認証を有効にしたユーザーのみが、すべてのユーザーに対する二段階認証を有効にできます。
- 自分のアカウントに対して二段階認証を有効にしたユーザーのみが、すべてのユーザーに対して有効にされた二段階認証からユーザーを除外できます。
- ユーザーは自分のアカウントに対してのみ二段階認証を有効にできます。
- ［**一般的な機能：ユーザー権限**］機能エリアのオブジェクト ACL の変更権限を持ち、二段階認証を使用して Kaspersky Security Center 14 Web コンソールにログインしたユーザーアカウントが、次の両方の条件が一致する場合にすべてのユーザーに対して二段階認証を無効にすることができます：すべてのユーザーに

対する二段階認証が無効になっているその他のユーザー、すべてのユーザーに対して有効にされた二段階認証のリストから除外されたユーザー。

- 二段階認証を使用して Kaspersky Security Center 14 Web コンソールにログインしたすべてのユーザーは自分の秘密鍵を再発行できます。
- 現在作業中の管理サーバーに対してすべてのユーザーに対する二段階認証を有効にすることができます。管理サーバーのこのオプションをオンにすると、管理サーバーの仮想管理サーバーのユーザーアカウントに対してもこのオプションをオンにすることになり、セカンダリ管理サーバーのユーザーアカウントの二段階認証は有効にされません。

自分のアカウントの二段階認証を有効にする

自分のアカウントの二段階認証を有効にすることができます。

アカウントの二段階認証を有効にする前に、お使いのモバイルデバイスに認証アプリケーションがインストールされていることを確認してください。認証アプリケーションと管理サーバーがインストールされているデバイスの時刻が同期されていることを確認します。

ユーザーアカウントの二段階認証を有効にするには：

1. メインメニューで、［**ユーザーとロール**］→［**ユーザー**］の順に移動します。
2. 自分のアカウントの名前をクリックします。
3. ユーザー設定ウィンドウが表示されたら、［**アカウント保護**］を選択します。
4. ［**アカウント保護**］タブ：
   - ユーザーアカウントに二段階認証を有効にする場合は［**ユーザー名、パスワード、セキュリティコードを要求（二段階認証）**］を選択します。
     - 表示された二段階認証のウィンドウで、認証アプリケーションの秘密鍵を入力するか、QR コードをスキャンしてワンタイムセキュリティコードを受け取ります。

       この秘密鍵を認証アプリケーションで手動で指定するか、お使いのモバイルデバイスで QR コードをスキャンします。
     - 二段階認証のウィンドウで、認証アプリケーションが生成したセキュリティコードを入力し、［**チェックして適用**］をクリックします。
5. ［**保存**］をクリックします。

自分のアカウントの二段階認証が有効になります。

すべてのユーザーに対して二段階認証を有効にする

お客様自身のアカウントに［**一般的な機能：ユーザー権限**］機能領域のオブジェクト ACL の変更権限があり、二段階認証を使用して認証済みである場合、管理サーバーのすべてのユーザーに対して二段階認証を有効にすることができます。すべてのユーザーに対する二段階認証を有効にする前に自分のアカウントの二段階認証を有効にしなかった場合、本製品は最初に自分のアカウントの二段階認証を有効にするウィンドウを開きます。

すべてのユーザーに対して二段階認証を有効にするには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. プロパティウィンドウの**[認証セキュリティ]**タブで、**全ユーザーに対する二段階認証**の切り替えスイッチを有効の位置に移動します。

すべてのユーザーに対して二段階認証が有効になります。以降、すべてのユーザーに対する二段階認証を有効にする前に追加されたユーザーを含む管理サーバーのユーザーは、アカウントが二段階認証の対象から除外されたユーザー以外全員、アカウントに二段階認証を設定する必要があります。

ユーザーアカウントの二段階認証を無効にする

ご自分のアカウント、または別のユーザーの二段階認証を無効にすることができます。

ご自分のアカウントに［**一般的な機能：ユーザー権限**］機能領域のオブジェクト ACL の変更権限がある場合のみ、他のユーザーのアカウントの二段階認証を無効にすることができます。

ユーザーアカウントの二段階認証を無効にするには：

1. メインメニューで、［**ユーザーとロール**］→［**ユーザー**］の順に移動します。
2. 二段階認証を無効にする内部ユーザーアカウントの名前をクリックします。この名前は、ご自分のアカウントまたは別のユーザーのアカウントです。
3. ユーザー設定ウィンドウが表示されたら、［**アカウント保護**］を選択します。
4. ［**アカウント保護**］タブで、［**ユーザー名とパスワードのみ要求**］を選択してユーザーアカウントの二段階認証を無効にします。
5. ［**保存**］をクリックします。

このユーザーアカウントの二段階認証が無効になります。

すべてのユーザーに対して二段階認証を無効にする

自分のアカウントで二段階認証が有効になっており、［**一般的な機能：ユーザー権限**］のオブジェクト ACL の変更権限がある場合にすべてのユーザーに対する二段階認証を無効にすることができます。ご自身のアカウントで二段階認証が有効にされていない場合、すべてのユーザーに対して二段階認証を無効にする前にご自身のアカウントの二段階認証を有効にする必要があります。

すべてのユーザーに対して二段階認証を無効にするには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. プロパティウィンドウの[**認証セキュリティ**]タブで、**全ユーザーに対する二段階認証**オプションの切り替えスイッチを無効の位置に移動します。
3. 認証ウィンドウでアカウントの認証情報を入力します。

すべてのユーザーに対して二段階認証が無効になります。

二段階認証からアカウントを除外する

使用中のアカウントに［**一般的な機能：ユーザー権限**］機能領域のオブジェクト ACL の変更権限がある場合は、二段階認証からアカウントを除外することができます。

ユーザーアカウントがすべてのユーザーに対する二段階認証のリストから除外されている場合、このユーザーは二段階認証を使用する必要はありません。

> 認証中にセキュリティコードをパスできないサービスアカウントの場合、二段階認証からアカウントを除外する必要がある場合があります。

二段階認証から複数のユーザーアカウントを除外する場合：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. プロパティウィンドウの[**認証セキュリティ**]タブで、二段階認証の除外のテーブルで[**追加**]をクリックします。
3. 表示されたウィンドウで以下を実行します：
   a. 除外するユーザーアカウントを選択します。
   b. ［**OK**］をクリックします。

選択したユーザーアカウントが二段階認証から除外されます。

新しい秘密鍵の作成

使用するアカウントの二段階認証用の新しい秘密鍵は、二段階認証を使用してアカウントが認証された場合のみ生成できます。

ユーザーアカウントに対する新しい秘密鍵を生成するには：

1. メインメニューで、［**ユーザーとロール**］→［**ユーザー**］の順に移動します。
2. 二段階認証用の新しい秘密鍵を生成するユーザーアカウントの名前をクリックします。

3. ユーザー設定ウィンドウが表示されたら、［**アカウント保護**］を選択します。

4. ［**アカウント保護**］タブで、［**新しい秘密鍵を生成**］をクリックします。

5. 表示された二段階認証ウィンドウで、認証アプリケーションによって作成された新しい秘密鍵を指定します。

6. ［**チェックして適用**］をクリックします。

新しい秘密鍵が生成されました。

モバイルデバイスを紛失した場合は、別のモバイルデバイスに認証アプリケーションをインストールし、新しい秘密鍵を生成して、Kaspersky Security Center 14 Web コンソールへのアクセスを復元できます。

セキュリティコードの発行元の名前を変更する

異なる管理サーバーに対して、複数の識別子（発行元）を設定することができます。別の管理サーバーに同じようなセキュリティコードの発行元の名前が使用されている場合などに、別のセキュリティコードの発行元の名前に変更することができます。既定では、セキュリティコードの発行元の名前は管理サーバーの名前と同じです。

セキュリティコードの発行元の名前を変更した後は、新しい秘密鍵を発行して認証アプリケーションに渡す必要があります。

セキュリティコードの発行元の名前を指定するには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。

2. ユーザー設定ウィンドウが表示されたら、［**アカウント保護**］を選択します。

3. ［**アカウント保護**］で、［**編集**］リンクをクリックします。
   ［**セキュリティコード発行元の編集**］セクションが開きます。

4. 新しいセキュリティコードの発行元の名前を設定します。

5. ［**OK**］をクリックします。

管理サーバーに新しいセキュリティコードの発行元の名前が設定されます。

許可されるパスワード入力試行回数の変更

Kaspersky Security Center Linux のユーザーが無効なパスワードを入力できる回数には上限があります。入力回数が上限に達すると、ユーザーアカウントが 1 時間ブロックされます。

既定では、許可されるパスワードの入力試行回数の上限は 10 回です。このセクションの手順に従って、許可されるパスワード入力試行回数を変更できます。

許可されるパスワード入力試行回数を変更するには：

1. 管理サーバーデバイスで、Linux コマンドラインを実行します。
2. klscflag ユーティリティ用に、次のコマンドを実行します：

   ```
   sudo /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n SrvSplPpcLogonAttempts -t d -v N
   ```

   N はパスワードの入力試行回数です。
3. 変更を適用するため、管理サーバーサービスを再起動します。

許可されるパスワードの入力試行回数の上限が変更されます。

DBMS 資格情報の変更

たとえば、セキュリティ目的で資格情報のローテーションを実行するために、DBMS 資格情報の変更が必要になる場合があります。

Linux 環境で klsrvconfig ユーティリティを使用して DBMS 資格情報を変更するには：

1. Linux コマンドラインを開始します。
2. 表示されたコマンドラインウィンドウで klsrvconfig ユーティリティを指定します：

   ```
   sudo /opt/kaspersky/ksc64/sbin/klsrvconfig -set_dbms_cred
   ```
3. 新しいアカウント名を指定します。DBMS に存在するアカウントの資格情報を指定する必要があります。
4. 新しいパスワードを入力します。
5. 確認のため新しいパスワードを再入力します。

DBMS 資格情報が変更されます。

管理サーバーの階層の削除

管理サーバーの階層構造が不要になった場合は、管理サーバーを階層構造から離脱させることができます。

管理サーバーの階層を削除するには：

1. 画面上部の管理サーバー名のセクションでプライマリ管理サーバーを選択し、横にある設定アイコン（）をクリックします。
2. 表示されたページで、［**管理サーバー**］タブに移動します。
3. セカンダリ管理サーバーを削除する管理グループで、目的のセカンダリ管理サーバーを選択します。
4. メニューヘッダーから［**削除**］を選択します。
5. 表示されるウィンドウで、［**OK**］をクリックし、セカンダリ管理サーバーを削除する処理を確定させます。

プライマリ管理サーバーとして動作していた管理サーバーと、セカンダリ理サーバーとして動作していた管理サーバーは、互いに独立して動作するようになります。これにより、階層構造が解消されます。

インターフェイスの設定

Kaspersky Security Center 14 Web コンソールのインターフェイスを設定して、使用している機能に応じてセクションとインターフェイス要素を表示または非表示にすることができます。

現在使用している機能に基づいて Kaspersky Security Center 14 Web コンソールのインターフェイスを設定するには：

1. メインメニューで、アカウントのメニューをクリックします。
2. ドロップダウンメニューから［**インターフェイスのオプション**］を選択します。
3. 表示される［**インターフェイスのオプション**］ウィンドウで、必要なオプションをオンまたはオフにします。
4. ［**保存**］をクリックします。

その後、コンソールは有効なオプションに従ってメインメニューにセクションを表示します。たとえば、［**EDR アラートを表示**］をオンにした場合、メイン メニューに［**監視とレポート**］→［**アラート**］セクションが表示されます。

ネットワーク接続されたデバイスの検出

このセクションでは、ネットワーク接続されたデバイスを検出するプロセスについて説明します。

Kaspersky Security Center では、条件を指定してデバイスを検索できます。検索結果をテキストファイルに保存できます。

デバイスの検出機能により、次のデバイスを見つけることができます：

- Kaspersky Security Center の管理サーバーとセカンダリ管理サーバーの管理グループに属する管理対象デバイス
- Kaspersky Security Center の管理サーバーとセカンダリ管理サーバーで管理される未割り当てデバイス

ネットワーク接続されたデバイスの検出シナリオ

セキュリティ製品のインストール前にデバイスの検索を実行する必要があります。ネットワーク接続されたデバイスがすべて検出されると、これらのデバイスに関する情報を取得しポリシーを通してデバイスを管理できます。ネットワーク内に新しいデバイスが存在するか、また過去に検出されたデバイスが現在もネットワーク内に存在するかを確認するには、定期的なネットワークポーリングが必要です。

ネットワーク上のデバイスの検出は、以下の手順で進みます：

1. **最初のデバイス検出**

   クイックスタートウィザードを完了したら、デバイスの検索を手動で実行してください。

2. **ポーリングのスケジュール設定**

   IP アドレス範囲のポーリングがオンになっていることと、ポーリングのスケジュール設定が社内で要求される条件を満たしていることを確認します。ポーリングのスケジュールを設定する際には、ネットワークポーリングの頻度に関する推奨事項を参照してください。

   ネットワークに Ipv6 デバイスが含まれている場合は Zeroconf ポーリングを有効にすることができます。

3. **検出されたデバイスを管理グループに追加するルールの設定（任意）**

   ネットワーク内に新しいデバイスが追加された場合、これらのデバイスは定期的なポーリング中に検出され、［**未割り当てデバイス**］グループに含まれます。必要に応じて、［**管理対象デバイス**］にこれらのデバイスを自動的に移動するルールを設定できます。また、保持ルールを確立することもできます。

   このルール設定のステップを省略した場合、新しく検出されたデバイスはすべて［**未割り当てデバイス**］グループに割り当てられ、そこから移動しません。必要に応じて、これらのデバイスを［**管理対象デバイス**］グループに手動で移動できます。デバイスを［**管理対象デバイス**］グループに手動で移動する場合、各デバイスの情報を分析し、管理グループに移動するかどうかやどの管理グループに移動するかを決定できます。

結果

これらのステップがすべて完了すると、次の状態を実現できます：

- Kaspersky Security Center Linux 管理サーバーがネットワーク内のデバイスを検出し、その情報を利用できるようになります。
- ポーリングのスケジュールが設定され、指定したスケジュールに従ってポーリングが実行されます。

新しく検出されたデバイスは、設定されたルールに従って配置されます（または、ルールが設定されていない場合、デバイスは［**未割り当てデバイス**］グループに割り当てられたままになります）。

IP アドレス範囲のポーリング

Kaspersky Security Center は、通常の DNS 要求を使用して、指定された範囲のすべての IPv4 アドレスに対して、IP アドレスを DNS 名へ解決する逆引きの名前解決を試行します。この処理が成功すると、取得した名前に対してサーバーは「`ICMP ECHO REQUEST`（Ping コマンドと同一）」を送信します。これに対してデバイスが応答した場合、デバイスの情報が Kaspersky Security Center のデータベースに追加されます。逆引きの名前解決は、IP アドレスを付与されているがコンピューターではないネットワークデバイス（ネットワークプリンターやルーターなど）を除外するために必要です。

このポーリング方法は、ローカル DNS サービスが適切に構成されているかどうかに依存します。ローカル DNS サービスで、逆引きの検索ゾーンが設定されている必要があります。逆引きの検索ゾーンが設定されていない場合、IP アドレス範囲のポーリングを実行しても、ポーリング結果は得られません。

Kaspersky Security Center は最初、ポーリングを行う IP アドレスを、Kaspersky Security Center がインストールされているデバイスのネットワーク設定から取得します。デバイスアドレスが 192.168.0.1 でサブネットマスクが 255.255.255.0 の場合、Kaspersky Security Center は 192.168.0.0/24 ネットワークをポーリング対象のアドレスのリストに自動的に含めます。Kaspersky Security Center は 192.168.0.1 から 192.168.0.254 までのすべてのアドレスのポーリングを実行します。

IP アドレス範囲のポーリングのみが有効になっている場合、Kaspersky Security Center は Ipv4 アドレスを持つデバイスのみを検出します。ネットワークに Ipv6 デバイスが含まれる場合は、デバイスの Zeroconf ポーリングをオンにします。

IP アドレス範囲のポーリング設定の表示と変更

IP アドレス範囲のポーリング設定の表示と変更を行うには：

1. ［**検出と製品の導入**］ - ［**検出**］ - ［**IP アドレス範囲**］の順に選択します。
2. ［**プロパティ**］をクリックします。
   IP ポーリングのプロパティウィンドウが開きます。
3. ［**ポーリングを許可**］を使用して、IP ポーリングをオンまたはオフにします。
4. ポーリングスケジュールを設定します。既定では、IP ポーリングは 420 分（7 時間）ごとに実行されます。
   ポーリング間隔の指定時には、指定する値が［IP アドレスの有効期間］の値を超えないように注意してください。IP アドレスの有効期間の間にポーリングによって IP アドレスが確認されなかった場合、この IP アドレスはポーリングの結果から自動的に削除されます。既定では、（DHCP プロトコルを使用して割り当てられる）動的 IP アドレスは 24 時間ごとに変更されるので、ポーリング結果の有効期間は 24 時間です。
   ポーリングスケジュールのオプション：
   - **N 日ごと**
     指定した日時から、日単位で指定した間隔ごとにポーリングを定期的に実行します。
     既定では、現在のシステム日時から、1 日ごとにポーリングが実行されます。
   - **N 分ごと**

指定した時刻から、分単位で指定した間隔ごとにポーリングを定期的に実行します。

- **曜日ごと**

  指定した曜日（複数可）の指定した時刻にポーリングを定期的に実行します。

- **毎月、選択した週の指定日**

  毎月、指定した週・曜日の指定した時刻にポーリングを定期的に実行します。

- **未実行のタスクを実行する**

  ポーリングの実行がスケジュールされていた時刻に管理サーバーがオフまたは接続できなかった場合は、管理サーバーがオンになった時に即座にポーリングを実行させるか、ポーリングの次回のスケジュールまで待機するかを選択できます。

  このオプションをオンにすると、管理サーバーがオンになるとすぐにポーリングを開始します。

  このオプションをオフにすると、管理サーバーはポーリングの次回のスケジュールまでポーリングの実行を待機します。

  既定では、このオプションはオフです。

5. ［**保存**］をクリックします。

プロパティが保存され、すべての IP アドレス範囲に適用されます。

手動でのポーリングの実行

手動でポーリングを実行するには：

［**ポーリングを開始する**］をクリックします。

IP アドレス範囲の追加と変更

Kaspersky Security Center は最初、ポーリングを行う IP アドレスを、Kaspersky Security Center がインストールされているデバイスのネットワーク設定から取得します。デバイスアドレスが 192.168.0.1 でサブネットマスクが 255.255.255.0 の場合、Kaspersky Security Center は 192.168.0.0/24 ネットワークをポーリング対象のアドレスのリストに自動的に含めます。Kaspersky Security Center は 192.168.0.1 から 192.168.0.254 までのすべてのアドレスのポーリングを実行します。自動的に定義された IP アドレス範囲を編集したり、カスタム IP アドレス範囲を追加できます。

IPv4 アドレスに対してのみ範囲を作成できます。Zeroconf ポーリングを有効にしている場合は、Kaspersky Security Center はネットワーク全体をポーリングします。

新しい IP アドレス範囲を追加するには：

1. ［**検出と製品の導入**］→［**検出**］→［**IP アドレス範囲**］の順に選択します。

2. 新しい IP アドレス範囲を追加するには、［**追加**］をクリックします。

3. 表示されたウィンドウで、次の設定を行います：

   - **IP アドレス範囲の名前**

     IP アドレス範囲の名前。「192.168.0.0/24」のように、指定した IP アドレス範囲自体を名前として使用することもできます。

   - **IP 区間またはサブネットアドレスとマスク**

     開始 IP アドレスと終了 IP アドレスを指定するか、サブネットアドレスとサブネットマスクを指定して、IP アドレス範囲を設定します。［**参照**］をクリックして、既存の IP アドレス範囲を選択することもできます。

   - **IP アドレスの有効期間（時間）**

     このパラメータの指定時には、値がポーリングのスケジュールで指定したポーリング間隔を超えるように指定してください。IP アドレスの有効期間の間にポーリングによって IP アドレスが確認されなかった場合、この IP アドレスはポーリングの結果から自動的に削除されます。既定では、（DHCP プロトコルを使用して割り当てられる）動的 IP アドレスは 24 時間ごとに変更されるので、ポーリング結果の有効期間は 24 時間です。

4. 追加したサブネットまたは IP アドレスの区間をポーリングするには、［**IP アドレス範囲のポーリングを有効にする**］をオンにします。そうでない場合、追加したサブネットまたは IP 区間を対象としたポーリングは実行されません。

5. ［**保存**］をクリックします。

IP アドレス範囲のリストに新しい IP アドレス範囲が追加されます。

［**ポーリングを開始する**］を使用して、IP アドレス範囲ごとに個別にポーリングを実行できます。ポーリングの完了後、［**デバイス**］を使用して、検出されたデバイスのリストを表示できます。既定では、ポーリング結果の有効期間は 24 時間で、これは IP アドレスの有効期間と同じ長さです。

既存の IP アドレス範囲にサブネットを追加するには：

1. ［**検出と製品の導入**］→［**検出**］→［**IP アドレス範囲**］の順に選択します。

2. サブネットを追加する IP アドレス範囲の名前をクリックします。

3. ウィンドウが表示されたら、［**追加**］をクリックします。

4. サブネットアドレスとサブネットマスクを指定するか、開始 IP アドレスと終了 IP アドレスを指定して、IP アドレス範囲を指定します。または、［**参照**］をクリックして既存のサブネットを追加することもできます。

5. ［**保存**］をクリックします。

   IP アドレス範囲に新しいサブネットが追加されます。

6. ［**保存**］をクリックします。

IP アドレス範囲の新しい設定が保存されます。

サブネットは、個数の制限なく必要な数だけ追加できます。名前のあるIPアドレス範囲同士での範囲の重複は許可されていませんが、1つのIPアドレス範囲内の名前のないサブネット（IP区間同士）にはそうした制限はありません。IPアドレス範囲ごとのポーリングを個別にオンまたはオフに切り替えることができます。

Zeroconf ポーリング

この検索方法はLinuxベースのディストリビューションポイントでのみサポートされます。

Kaspersky Security CenterはIPv6アドレスのデバイスを含むネットワークを検索できるようになりました。この場合、IP範囲は指定されず、Kaspersky Security Centerはネットワーク全体をゼロコンフィギュレーションネットワーキング（「*Zeroconf*」とも表記）を使用して検索します。Zeroconfの使用を開始するには、ネットワークをポーリングするLinuxデバイス（管理サーバーまたはディストリビューションポイント）でavahi-browseユーティリティをインストールする必要があります。

Zeroconfポーリングを有効にするには：

1. ［**検出と製品の導入**］→［**検出**］→［**IPアドレス範囲**］の順に選択します。
2. ［**プロパティ**］をクリックします。
3. ウィンドウが表示されたら、［**Zeroconfを使用してIPv6ネットワークのポーリングを実行する**］をオンにします。

その後、Kaspersky Security Centerはネットワークの検索を開始します。この場合、指定されたIP範囲は無視されます。

デバイスのタグ

このセクションでは、デバイスタグの概要と、デバイスタグの作成、編集、手動または自動でのデバイスのタグ付けを行う方法を説明しています。

デバイスタグの概要

Kaspersky Security Centerでは、デバイスに*タグ付け*できます。タグは、デバイスのグループ化、説明、または検索に使用することができるデバイスのラベルです。デバイスに割り当てられたタグは、抽出の作成、デバイスの検索、および各管理グループへのデバイスの割り当てに使用できます。

デバイスには、手動または自動でタグ付けできます。個々のデバイスにタグ付けする必要がある場合は、手動のタグ付けを使用することができます。自動タグ付けは、指定したタグ付けルールに従い、Kaspersky Security Centerによって実行されます。

デバイスには、指定されたルールが適合する場合に自動的にタグ付けされます。個々のルールは各タグに対応します。ルールは、デバイス、オペレーティングシステム、デバイスにインストールされたアプリケーションのネットワークプロパティ、およびその他のデバイスのプロパティに適用されます。たとえば、CentOSオペレーティングシステムが実行されているすべてのデバイスに `[CentOS]` タグを割り当てるルールを設定できます。その後、デバイスの抽出を作成する場合にこのタグを使用できます。これにより、すべてのCentOSのデバイスを抽出し、タスクを割り当てることができます。

次の場合は、デバイスからタグが自動的に削除されます：

- タグの割り当てルールの条件をデバイスが満たさなくなった場合。
- タグを割り当てるルールがオフになったあるいは削除された場合。

管理サーバーごとのタグのリストとタグ付けルールのリストは、プライマリ管理サーバーとセカンダリ管理サーバーを含むその他のすべての管理サーバーとは影響関係を持ちません。タグ付けのルールは、ルールが作成された管理サーバーのデバイスに対してのみ適用されます。

デバイスタグの作成

デバイスのタグを作成するには：

1. メインメニューで、［**デバイス**］→［**タグ**］→［**デバイスのタグ**］の順に選択します。
2. ［**追加**］をクリックします。
   新規タグの入力ウィンドウが表示されます。
3. ［**タグ**］にタグ名を入力します。
4. ［**保存**］をクリックして変更内容を保存します。

   デバイスタグのリストに新しいタグが表示されます。

デバイスタグの名前変更

デバイスタグの名前を変更するには：

1. メインメニューで、［**デバイス**］→［**タグ**］→［**デバイスのタグ**］の順に選択します。
2. 名前を変更するタグの名前をクリックします。
   タグのプロパティウィンドウが表示されます。
3. ［**タグ**］でタグ名を変更します。
4. ［**保存**］をクリックして変更内容を保存します。

   デバイスタグのリストに更新したタグが表示されます。

デバイスタグの削除

デバイスタグを削除するには：

1. メインメニューで、［**デバイス**］→［**タグ**］→［**デバイスのタグ**］の順に選択します。
2. リストから削除するデバイスタグを選択します。
3. ［**削除**］をクリックします。

4. 表示されたウィンドウで［**はい**］をクリックします。

デバイスタグが削除されます。削除されたタグが割り当てられていたすべてのデバイスから、このタグが自動的に削除されます。

削除したタグは、自動タグルールから自動的に削除されません。タグの削除後も、タグを割り当てるルールの条件に初めて合致した場合にのみ、新規デバイスに対してタグが割り当てられます。

このタグがアプリケーションまたはネットワークエージェントによってデバイスに割り当てられている場合、削除されたタグはデバイスから自動的に削除されません。デバイスからタグを削除するには、klscflag ユーティリティを使用します。

タグを割り当てられているデバイスの表示

タグを割り当てられているデバイスを表示するには：

1. メインメニューで、［**デバイス**］→［**タグ**］→［**デバイスのタグ**］の順に選択します。
2. 割り当て先のデバイスを確認するタグの横の［**デバイスの表示**］をクリックします。
   タグの横に［**デバイスの表示**］が表示されていない場合、タグはどのデバイスにも割り当てられていません。

表示されるデバイスのリストには、タグが割り当てられているデバイスのみが表示されます。

デバイスタグのリストに戻るには、ブラウザーの「**戻る**」をクリックします。

デバイスに割り当てられているタグの表示

デバイスに割り当てられているタグを表示するには：

1. メインメニューで、［**デバイス**］→［**管理対象デバイス**］の順に移動します。
2. タグを表示するデバイスの名前をクリックします。
3. デバイスのプロパティウィンドウが開いたら、［**タグ**］タブをクリックします。

選択したデバイスに割り当てられているタグのリストが表示されます。

デバイスに別のタグを割り当てたり、割り当て済みのタグを削除することができます。管理サーバーに存在するすべてのタグを表示することもできます。

デバイスへの手動でのタグ付け

デバイスを手動でタグ付けするには：

1. メニューを移動して、別のタグを追加するデバイスに割り当てられているタグを表示します。
2. ［**追加**］をクリックします。
3. 表示されたウィンドウで、次のいずれかを実行します：
   - 新しいタグを作成して割り当てるには、［**新しいタグを作成する**］を選択して新しいタグの名前を入力します。
   - 既存のタグを選択するには、［**既存のタグを割り当てる**］を選択し、ドロップダウンリストから目的のタグを選択します。
4. ［**OK**］をクリックして変更を適用します。
5. ［**保存**］をクリックして変更内容を保存します。

選択したタグがデバイスに割り当てられます。

デバイスに割り当てたタグの削除

デバイスからタグを削除するには：

1. メインメニューで、［**デバイス**］→［**管理対象デバイス**］の順に選択します。
2. タグを表示するデバイスの名前をクリックします。
3. デバイスのプロパティウィンドウが開いたら、［**タグ**］タブをクリックします。
4. 削除するタグに隣接するチェックボックスをオンにします。
5. リストの上部にある［**タグを解除する**］をクリックします。
6. 表示されたウィンドウで［**はい**］をクリックします。

タグがデバイスから削除されます。

解除されたタグ自身は削除されません。必要に応じて、手動で削除できます。

アプリケーションまたはネットワークエージェントによってデバイスに割り当てられたタグを手動で削除することはできません。これらのタグを削除するには、klscflag ユーティリティを使用します。

デバイスの自動タグルールの表示

デバイスの自動タグルールを表示するには：

次のいずれかの手順を実行します：

- メインメニューで、［**デバイス**］→［**タグ**］→［**自動タグルール**］の順に選択します。
- メインメニューで、［**デバイス**］→［**タグ**］の順に選択し、［**自動タグルールの設定**］をクリックします。
- デバイスに割り当てられているタグを確認し、［**設定**］をクリックします。

デバイスの自動タグルールのリストが表示されます。

デバイスの自動タグルールの編集

デバイスの自動タグルールを編集するには：

1. デバイスの自動タグルールを表示します。
2. 編集するルールの名前をクリックします。
   ルールの設定ウィンドウが表示されます。
3. ルールのプロパティ全般を編集します：
   a. ［**ルール名**］で、ルール名を変更します。
      名前は 256 文字以下でなければなりません。
   b. 次のいずれかの手順を実行します：
      - スイッチを［**ルールが有効**］に切り替えるとルールを有効にできます。
      - スイッチを［**ルールが無効**］に切り替えるとルールを無効にできます。
4. 次のいずれかの手順を実行します：
   - 新しい条件を追加する場合は、［**追加**］をクリックし、開いたウィンドウで新しい条件の設定を指定します。
   - 既存の条件を編集するには、編集する条件の名前をクリックし、条件設定を編集します。
   - 条件を削除するには、削除する条件の横のチェックボックスを選択し、［**削除**］をクリックします。
5. 設定ウィンドウで、［**OK**］をクリックします。
6. ［**保存**］をクリックして変更内容を保存します。

編集後のルールがリストに表示されます。

デバイスの自動タグルールの作成

デバイスの自動タグルールを作成するには：

1. デバイスの自動タグルールを表示します。
2. ［**追加**］をクリックします。
   新規ルールの設定ウィンドウが表示されます。
3. ルールのプロパティ全般を設定します：
   a. ［**ルール名**］で、ルール名を入力します。
      名前は 256 文字以下でなければなりません。
   b. 次のいずれかの手順を実行します：
      - スイッチを［**ルールが有効**］に切り替えるとルールを有効にできます。
      - スイッチを［**ルールが無効**］に切り替えるとルールを無効にできます。
   c. ［**タグ**］で、新しいデバイスタグの名前を入力するか、リストから既存のデバイスタグを選択します。
      名前は 256 文字以下でなければなりません。
4. 条件セクションで［**追加**］をクリックして新しい条件を追加します。
   新しい条件の設定ウィンドウが表示されます。
5. 条件の名前を入力します。
   名前は 256 文字以下でなければなりません。名前は、1 つのルール内で一意である必要があります。
6. 次の条件によりルールのトリガーを設定します：複数の条件を選択できます。
   - **ネットワーク** - デバイスのネットワークプロパティ（デバイスの DNS 名、デバイスが IP サブネットに含まれるかなど）。

     Kaspersky Security Center で使用するデータベースに大文字と小文字を区別する照合が設定されている場合は、デバイスの DNS 名の指定時に大文字と小文字を区別してください。そうしないと、自動タグ付けルールが機能しません。

   - **アプリケーション** - デバイス上のネットワークエージェントの存在、オペレーティングシステムの種別、バージョン、アーキテクチャ。
   - **仮想マシン** - デバイスが仮想マシンの特定の種別に属しているかどうか。
   - **アプリケーションレジストリ** - デバイス上の異なる製造元によるアプリケーションの存在。
7. ［OK］をクリックして変更内容を保存します。
   必要に応じて、1 つのルールに対して複数の条件を設定できます。この場合、タグは少なくとも 1 つの条件を満たすデバイスに割り当てられます。
8. ［**保存**］をクリックして変更内容を保存します。

新しく作成されたルールは、選択した管理サーバーによって管理されているデバイスに適用されます。デバイスの設定がルールの条件を満たす場合、そのデバイスにタグが割り当てられます。

設定後、ルールは次の状況で適用されます：

- サーバーの負荷に応じて、自動的かつ定期的に適用
- ルールの編集後に適用
- 手動でのルール実行時に適用
- ルールの条件に合致するデバイスの設定の変更やデバイスのグループの設定の変更を管理サーバーが検知した後に適用

複数のタグ付けルールを作成できます。複数のタグ付けルールを作成しており、それらのルールのそれぞれの条件が同時に満たされる場合は、1つのデバイスに複数のタグを割り当てることができます。すべての割り当てられたタグのリストは、デバイスのプロパティで確認できます。

デバイスの自動タグルールの実行

ルールを実行すると、ルールのプロパティで指定されたタグが、ルールのプロパティで指定された条件に合致するデバイスに割り当てられます。有効なルールのみを実行できます。

デバイスの自動タグルールを実行するには：

1. デバイスの自動タグルールを表示します。
2. 実行する有効なルールに隣接するチェックボックスをオンにします。
3. ［**ルールを実行**］をクリックします。

   選択したルールが実行されます。

デバイスの自動タグルールの削除

デバイスの自動タグルールを削除するには：

1. デバイスの自動タグルールを表示します。
2. 削除するルールに隣接するチェックボックスをオンにします。
3. ［**削除**］をクリックします。
4. 表示されるウィンドウで、もう一度［**削除**］をクリックします。

   選択したルールが削除されます。このルールのプロパティで指定されていたタグは、このタグが割り当てられていたすべてのデバイスから割り当て解除されます。

> 解除されたタグ自身は削除されません。必要に応じて、手動で削除できます。

アプリケーションタグ

このセクションでは、サードパーティ製品を対象としたアプリケーションタグの概要と、アプリケーションタグの作成、編集、製品への割り当てを行う方法を説明しています。

アプリケーションタグの概要

Kaspersky Security Center Linux では、サードパーティ製品（カスペルスキー以外の製造元が作成した製品）にタグを付与できます。タグとは、アプリケーションに割り当てるラベルで、アプリケーションのグループ化と検索に使用できます。アプリケーションに割り当てたタグは、デバイスの抽出の条件として使用できます。

たとえば、「ブラウザー」というタグを作成し、すべてのブラウザー（Microsoft Internet Explorer、Google Chrome、Mozilla Firefox など）に割り当てるなどの使い方ができます。

アプリケーションタグの作成

アプリケーションタグを作成するには：

1. メインメニューで、［**操作**］→［**サードパーティ製品**］→［**アプリケーションタグ**］の順に選択します。
2. ［**追加**］をクリックします。
   新規タグの入力ウィンドウが表示されます。
3. タグの名前を入力します。
4. ［**OK**］をクリックして変更内容を保存します。

アプリケーションタグのリストに新しいタグが表示されます。

アプリケーションタグの名前変更

アプリケーションタグの名前を変更するには：

1. メインメニューで、［**操作**］→［**サードパーティ製品**］→［**アプリケーションタグ**］の順に選択します。
2. 名前を変更するタグの横のチェックボックスをオンにし、［**編集**］をクリックします。
   タグのプロパティウィンドウが表示されます。
3. タグの名前を変更します。
4. ［**OK**］をクリックして変更内容を保存します。

アプリケーションタグのリストに更新したタグが表示されます。

アプリケーションへのタグの割り当て

アプリケーションにタグを割り当てるには：

1. メインメニューで、［**操作**］→［**サードパーティ製品**］→［**アプリケーションレジストリ**］の順に選択します。
2. タグを割り当てるアプリケーションの名前をクリックします。
3. ［**タグ**］タブを選択します。
   タブには管理サーバー上のすべてのアプリケーションタグが表示されます。選択したアプリケーションに割り当てられているタグでは、［**タグの割り当て**］列のチェックボックスがオンになっています。
4. 新たに割り当てるタグの［**タグの割り当て**］列のチェックボックスをオンにします。
5. ［**保存**］をクリックして変更内容を保存します。

アプリケーションにタグが割り当てられます。

アプリケーションに割り当てたタグの削除

アプリケーションからタグを削除するには：

1. メインメニューで、［**操作**］→［**サードパーティ製品**］→［**アプリケーションレジストリ**］の順に選択します。
2. タグを削除するアプリケーションの名前をクリックします。
3. ［**タグ**］タブを選択します。
   タブには管理サーバー上のすべてのアプリケーションタグが表示されます。選択したアプリケーションに割り当てられているタグでは、［**タグの割り当て**］列のチェックボックスがオンになっています。
4. 削除するタグの［**タグの割り当て**］列のチェックボックスをオフにします。
5. ［**保存**］をクリックして変更内容を保存します。

アプリケーションからタグが解除されます。

解除されたアプリケーションタグ自身は削除されません。必要に応じて、手動で削除できます。

アプリケーションタグの削除

アプリケーションタグを削除するには：

1. メインメニューで、［**操作**］→［**サードパーティ製品**］→［**アプリケーションタグ**］の順に選択します。
2. リストから削除するアプリケーションタグを選択します。
3. ［**削除**］をクリックします。

4. 表示されたウィンドウで［**OK**］をクリックします。

アプリケーションタグが削除されます。削除されたタグが割り当てられていたすべてのアプリケーションから、このタグが自動的に削除されます。

カスペルスキー製品の導入

このセクションでは、Kaspersky Security Center 14 Web コンソールを使用して、企業ネットワーク内のクライアントデバイスにカスペルスキー製品を導入する方法について説明しています。

シナリオ：カスペルスキー製品の導入

このシナリオは、Kaspersky Security Center 14 Web コンソールを使用したカスペルスキー製品の導入方法を説明しています。導入には、クイックスタートウィザードと製品導入ウィザードを使用する方法と、すべての必要なステップを手動で完了させる方法があります。

カスペルスキー製品の導入シナリオは、以下の手順で進みます：

1. **アプリケーションの Web 管理プラグインのダウンロード**

   カスペルスキーの Web サイトから Kaspersky Endpoint Security for Linux 向けの Web 管理プラグインをダウンロードしてから、Kaspersky Security Center 14 Web コンソールにプラグインを追加します。

2. **ネットワークエージェントのインストールパッケージのダウンロードおよび作成**

   カスペルスキーの Web サイトからネットワークエージェントの配布パッケージをダウンロードしてから、ネットワークエージェントのインストールパッケージを作成します。

   ダウンロードした配布パッケージを使用してネットワークエージェントをローカルにインストールすることができます。Kaspersky Endpoint Security for Linux の製品のヘルプまたはガイドに示される手順に従ってください。

3. **Kaspersky Endpoint Security for Linux のインストールパッケージのダウンロードと作成**

   カスペルスキーの Web サイトから Kaspersky Endpoint Security for Linux 配布パッケージをダウンロードしてから Kaspersky Endpoint Security for Linux のインストールパッケージを作成します。

4. **スタンドアロンインストールパッケージの作成（省略可能）**

   Kaspersky Security Center Linux を使用してカスペルスキー製品をインストールできないデバイスがある場合（リモートワークで働く従業員のデバイスなど）、製品のスタンドアロンインストールパッケージを作成できます。カスペルスキー製品をスタンドアロンパッケージを使用してインストールする場合、手順の 5 と 6 はスキップできます。

5. **リモートインストールタスクの作成、設定、実行**

   このステップは製品導入ウィザードの一部です。製品導入ウィザードを実行しない場合は、手動でこのタスクを作成して設定する必要があります。

   異なる管理グループや異なるデバイスの抽出を対象に、複数のリモートインストールタスクを手動で作成することもできます。これらのタスクでは、同一製品の異なるバージョンを導入できます。

   ネットワーク上ですべてのデバイスが検出済みであることを確認してから、リモートインストールタスクを実行します。

   > SUSE Linux Enterprise Server 15 オペレーティングシステムを搭載したデバイスにネットワークエージェントをインストールする場合は、ネットワークエージェントの設定前に、insserv-compat パッケージをインストールします。

6. **タスクの作成と設定**

   Kaspersky Endpoint Security for Linux のアップデートタスクを設定する必要があります。

このステップはクイックスタートウィザードの一部です：既定の設定を使用してタスクは自動的に作成、設定されます。ウィザードを実行しない場合は、手動でこのタスクを作成して設定する必要があります。クイックスタートウィザードを使用する場合、タスクのスケジュールが要件を満たすことを確認してください（既定では、タスクの実行予定は［**手動**］に設定されていますが、別のオプションも選択できます）。

7. **ポリシーの作成**

   手動またはクイックスタートウィザードを使用して Kaspersky Endpoint Security for Linux のポリシーを作成します。ポリシーは既定の設定を使用できます。また、いつでも必要に応じてポリシーの既定の設定を変更できます。

8. **結果の検証**

   導入が正しく完了しているかの確認：アプリケーションごとにポリシーとタスクが設定済みで、これらのアプリケーションが管理対象デバイスにインストールされていることを確認します。

結果

これらのステップがすべて完了すると、次の状態を実現できます：

- すべての必要なポリシーとタスクが、選択したアプリケーションに対して作成されている。
- タスクのスケジュールが必要に応じて設定されている。
- 指定したデバイス上で、選択したアプリケーションが導入されているか、導入スケジュールが設定されている。

カスペルスキー製品向けの管理プラグインの追加

Kaspersky Endpoint Security for Linux などのカスペルスキー製品を導入するには、製品の Web 管理プラグインを追加してインストール必要があります。

カスペルスキー製品の Web 管理プラグインを追加してインストールするには：

1. カスペルスキーの Web サイトから Kaspersky Endpoint Security for Linux 向けの Web 管理プラグインをダウンロードします。
2. Kaspersky Security Center 14 Web コンソールを開きます。
3. ［**コンソールの設定**］ドロップダウンリストから、［**Web プラグイン**］を選択します。
   使用可能な管理プラグインのリストが表示されます。
4. ［**ファイルから追加**］をクリックします。
   ［**ファイルから追加**］ウィンドウが表示されます。
5. ［**ZIP ファイルのアップロード**］をクリックします。
6. ダウンロードした Web プラグインの ZIP ファイルを指定します。
7. ［**署名のアップロード**］をクリックします。
8. ダウンロードした Web プラグインの署名の TXT ファイルを指定します。

9. ［**追加**］をクリックします。

   Kaspersky Security Center はアップロードされたファイルを検証し、Web プラグインを追加およびインストールします。

10. インストールが完了したら、［**OK**］をクリックします。

Web 管理プラグインが既定の設定でインストールされ、Web 管理プラグインのリストに表示されます。

ファイルからのインストールパッケージの作成

以下のような用途でカスタムインストールパッケージを使用できます：

- タスクなどを使用して、サードパーティ製を含む任意のアプリケーション（例：テキストエディター）をクライアントデバイスにインストールするため。
- スタンドアロンインストールパッケージを作成するため。

カスタムインストールパッケージは、複数のファイルを含んだフォルダーです。カスタムインストールパッケージは、*圧縮ファイル*を元に作成します。圧縮ファイルには、カスタムインストールパッケージに含める必要のあるファイルが含まれているようにします。

カスタムインストールパッケージを作成するときに、コマンドラインのパラメータを指定できます（例：製品をサイレントモードでインストールするためのパラメータ）。

カスタムインストールパッケージを作成するには：

1. 次のいずれかの手順を実行します：

   - ［**検出と製品の導入**］→［**導入と割り当て**］→［**インストールパッケージ**］の順に選択します。
   - ［**操作**］→［**リポジトリ**］→［**インストールパッケージ**］の順に選択します。

   管理サーバーで使用可能なインストールパッケージのリストが表示されます。

2. ［**追加**］をクリックします。

   新規パッケージウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

3. ウィザードの最初のページで、［**インストールパッケージをファイルから作成する**］を選択します。

4. ウィザードの次のページで、パッケージ名を入力して［**参照**］をクリックします。

5. 表示されるウィンドウで、使用可能なディスクにあるアーカイブファイルを選択します。

   ZIP、CAB、TAR、または TAR.GZ ファイルをアップロードできます。インストールパッケージを SFX ファイル（自己解凍型の圧縮ファイル）から作成することはできません。

   管理サーバーへのファイルのアップロードが開始されます。

6. カスペルスキー製品のファイルを指定した場合、製品の使用許諾契約書（EULA）を確認して同意するよう求められることがあります。続行するには、EULA に同意する必要があります。EULA の条項をすべて確認して理解した上で同意する場合にのみ［**この使用許諾契約書の条項に同意する**］を選択します。

また、プライバシーポリシーについても確認と同意を求められることがあります。続行するには、プライバシーポリシーに同意する必要があります。プライバシーポリシーに従ってデータが処理されて送信されること（第三国への送信を含む）を理解し、同意する場合にのみ［**プライバシーポリシーに同意する**］を選択します。

7. ウィザードの次のページで、（指定された圧縮ファイルから展開されたファイルのリストから）実行ファイルを選択し、コマンドラインのパラメータを指定します。

   インストールパッケージから製品をサイレントモードでインストールするためのコマンドラインのパラメータを指定できます。コマンドラインのパラメータの指定は省略可能です。

   カスタムインストールパッケージを作成するプロセスが開始されます。

   プロセスが終了すると、ウィザードで通知されます。

   インストールパッケージが作成されなかった場合も、メッセージで通知されます。

8. ［**終了**］をクリックしてウィザードを終了します。

作成したインストールパッケージは、管理サーバーの共有フォルダーのパッケージ用のサブフォルダーにダウンロードされます。ダウンロード後、インストールパッケージがインストールパッケージのリストに表示されます。

管理サーバーで利用できるインストールパッケージのリストで、カスタムインストールパッケージの名前をクリックすることで次の操作を実行できます：

- インストールパッケージのプロパティとして以下の情報を表示する：
  - **名前**：カスタムインストールパッケージの名前。
  - **ソース**：アプリケーションの開発元の名前。
  - **アプリケーション**：カスタムインストールパッケージに含まれるアプリケーションの名前。
  - **バージョン**：アプリケーションのバージョン。
  - **言語**：カスタムインストールパッケージに含まれるアプリケーションの言語。
  - **サイズ（MB）**：インストールパッケージのサイズ。
  - **オペレーティングシステム**：インストールパッケージが対象とするオペレーティングシステムの種別。
  - **作成**：インストールパッケージの作成日時。
  - **変更**：インストールパッケージの変更日時。
  - **種別**：インストールパッケージの種別。
- コマンドラインのパラメータを変更します。

スタンドアロンインストールパッケージの作成

組織内の管理者とユーザーがデバイスに手動でアプリケーションをインストールするために、スタンドアロンインストールパッケージを使用できます。

スタンドアロンインストールパッケージは実行ファイル形式で（Installer.exe）、Web サーバーや共有フォルダーへの配置あるいはメールへの添付などを利用してクライアントデバイスに受け渡すことができます。クライアントデバイスで受け取った実行ファイルをローカルで起動することで、Kaspersky Security Center Linux を使用せずにアプリケーションをインストールすることが可能となります。カスペルスキー製品およびサードパーティ製品のスタンドアロンインストールパッケージを作成できます。サードパーティ製品のインストールパッケージを作成するには、カスタムインストールパッケージを作成する必要があります。

スタンドアロンインストールパッケージが第三者にアクセスされないように必ず注意してください。

スタンドアロンインストールパッケージを作成するには：

1. 次のいずれかの手順を実行します：

   - ［**検出と製品の導入**］→［**導入と割り当て**］→［**インストールパッケージ**］の順に選択します。
   - ［**操作**］→［**リポジトリ**］→［**インストールパッケージ**］の順に選択します。

   管理サーバーで利用可能なインストールパッケージのリストが表示されます。

2. インストールパッケージのリストでインストールパッケージを選択し、リストの上にある［**製品の導入**］をクリックします。

3. ［**スタンドアロンパッケージを使用**］を選択します。

   スタンドアロンインストールパッケージ作成ウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

4. 選択したアプリケーションとネットワークエージェントを合わせてインストールする場合、ウィザードの最初のページで［**このアプリケーションと同時にネットワークエージェントをインストールする**］がオンであることを確認します。

   既定では、このオプションはオンです。デバイスにネットワークエージェントがインストール済みかどうかが不明な場合は、このオプションをオンにすることを推奨します。ネットワークエージェントがデバイスにインストールされている場合、ネットワークエージェントを含めたインストールパッケージがインストールされたときにネットワークエージェントが新しいバージョンにアップデートされます。

   このオプションがオフの場合、デバイスにはネットワークエージェントはインストールされず、デバイスは管理対象外のデバイスになります。

   選択したアプリケーションのスタンドアロンインストールパッケージが既に管理サーバー上に存在する場合、ウィザードに通知が表示されます。この場合、次のいずれかのオプションを選択する必要があります：

   - **スタンドアロンインストールパッケージの作成**：新しいバージョンのアプリケーションのスタンドアロンインストールパッケージを新規に作成し、なおかつ旧バージョンのアプリケーションで作成したスタンドアロンインストールパッケージも保持する場合などにこのオプションを選択します。新しいスタンドアロンインストールパッケージは別のフォルダーに配置されます。
   - **既存のスタンドアロンインストールパッケージを使用する**：既存のスタンドアロンインストールパッケージを使用する場合は、このオプションをオンにします。パッケージの作成プロセスは開始されません。
   - **既存のスタンドアロンインストールパッケージを再構築する**：同じアプリケーションのインストールパッケージを再作成する場合、このオプションを選択します。スタンドアロンインストールパッケージは、同じフォルダーに保存されます。

5. ウィザードの［**管理対象デバイスのリストへ移動**］ページで、既定では［**デバイスを移動しない**］が選択されています。ネットワークエージェントのインストール後にクライアントデバイスをどの管理グループにも移動したくない場合は、オプションの選択を変更しないでください。

ネットワークエージェントのインストール後にクライアントデバイスを移動したい場合は、［**未割り当てデバイスをこのグループへ移動**］を選択し、クライアントデバイスの移動先の管理グループを指定します。既定では、デバイスは［**管理対象デバイス**］グループに移動されます。

6. ウィザードの次のページで、スタンドアロンインストールパッケージの作成プロセスが完了したら、［**終了**］をクリックします。

［スタンドアロンインストールパッケージ作成ウィザード］が閉じます。

スタンドアロンインストールパッケージが作成され、管理サーバーの共有フォルダーのパッケージ用のサブフォルダーにダウンロードされます。インストールパッケージのリストの上にある［**スタンドアロンパッケージリストの表示**］をクリックすると、スタンドアロンパッケージのリストを確認できます。

スタンドアロンインストールパッケージのリストの表示

スタンドアロンインストールパッケージのリストを表示し、それぞれのスタンドアロンインストールパッケージのプロパティを確認できます。

すべてのインストールパッケージについて、対応するスタンドアロンインストールパッケージのリストを表示するには：

リストの上にある［**スタンドアロンパッケージリストの表示**］をクリックします。

スタンドアロンインストールパッケージのリストで、パッケージのプロパティが次のように表示されます。

- **パッケージ名**：パッケージに含まれるアプリケーション名とバージョン番号を組み合わせて自動的に作成されるスタンドアロンインストールパッケージの名前。
- **アプリケーション名**：スタンドアロンインストールパッケージに含まれるアプリケーションの名前。
- **アプリケーションのバージョン**。
- **ネットワークエージェントのインストールパッケージ名**。このプロパティは、スタンドアロンインストールパッケージにネットワークエージェントが含まれる場合にのみ表示されます。
- **ネットワークエージェントのバージョン**。このプロパティは、スタンドアロンインストールパッケージにネットワークエージェントが含まれる場合にのみ表示されます。
- **サイズ**：ファイルのサイズ（MB 単位）。
- **グループ**：ネットワークエージェントのインストール後にクライアントデバイスが移動する管理グループの名前。
- **作成日時**：スタンドアロンインストールパッケージが作成された日時。
- **変更日時**：スタンドアロンインストールパッケージが変更された日時。
- **パス**：スタンドアロンインストールパッケージが保存されているフォルダーのパス。
- **URL**：スタンドアロンインストールパッケージをダウンロードできる URL。
- **ファイルのハッシュ**：このプロパティは、スタンドアロンインストールパッケージが第三者による改竄を受けておらず、管理者が作成してユーザーに送信したのと同じファイルがユーザーの手元にあるかどうかを検証するために使用します。

特定のインストールパッケージについて、対応するスタンドアロンインストールパッケージのリストを表示するには：

リストからインストールパッケージを選択し、リストの上にある［**スタンドアロンパッケージリストの表示**］をクリックします。

スタンドアロンインストールパッケージのリストを使用して、次の操作を実行できます：

- ［**公開**］をクリックして、スタンドアロンインストールパッケージを Web サーバーに公開する。スタンドアロンインストールパッケージへのリンクを管理者から受け取ったユーザーは、公開されたスタンドアロンインストールパッケージをダウンロードできます。
- ［**公開の取り消し**］をクリックして、スタンドアロンインストールパッケージの Web サーバーへの公開を中止する。公開を取り消したスタンドアロンインストールパッケージは、取り消し操作を行った管理者およびその他の管理者しかダウンロードできません。
- ［**ダウンロード**］をクリックして、スタンドアロンインストールパッケージを操作中のデバイスにダウンロードする。
- ［**メールで送信**］をクリックして、スタンドアロンインストールパッケージへのリンクをメールで送信する。
- ［**削除**］をクリックして、スタンドアロンインストールパッケージを削除する。

ネットワークエージェントのリモートインストール用の Linux デバイスの準備

Linux で動作するデバイスにネットワークエージェントをリモートインストールのために準備するには：

1. 対象となる Linux デバイスに次のソフトウェアがインストールされていることを確認します：
   - Sudo
   - Perl 言語インタープリターのバージョン 5.10 以降
2. デバイスの構成をテストします：
   a. デバイスに SSH クライアント（PuTTY など）で接続できることを確認します。
   デバイスに接続できない場合、/etc/ssh/sshd_config ファイルを開き、次の設定をそれぞれの値に変更します：
   ```
   PasswordAuthentication no
   ChallengeResponseAuthentication yes
   ```

デバイスに問題なく接続できる場合は、/etc/ssh/sshd_config ファイルを変更しないでください。そうしないと、リモート インストール タスクの実行時に SSH 認証エラーが発生する可能性があります。

必要に応じてファイルを保存し、`sudo service ssh restart` コマンドを使用して SSH サービスを再起動します。

a. デバイスへの接続に使用するユーザーアカウントで sudo パスワードを無効にします。

b. sudo で `visudo` コマンドを使用し、sudoers 構成ファイルを開きます。

開いたファイルで、`%sudo`（CentOS オペレーティングシステムを使用している場合は、`%wheel`）で開始される行を探します。該当の行で、次を指定します：`<username> ALL = (ALL) NOPASSWD: ALL` この場合、`<username>` は、SSH を経由してデバイスを接続するために使用するユーザーアカウントです。Astra Linux オペレーティングシステムを使用している場合は、ファイル /etc/sudoers の最後の行に次のテキストを追加します：`%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL`

c. sudoers ファイルを保存して閉じます。

d. SSH を使用して再度デバイスに接続し、sudo サービスがパスワードの入力を要求しないことを確認します。そのためには `sudo whoami` コマンドを使用できます。

1. /Etc/systemd/logind.conf ファイルを開き、次のいずれかを実行します：

   - KillUserProcesses 設定の値として「no」を指定します：`KillUserProcesses=no`
   - KillExcludeUsers の設定にリモートインストールを実行するアカウントのユーザー名を入力します。例：`KillExcludeUsers=root`

   変更した設定を適用するには、Linux デバイスを再起動するか、次のコマンドを実行してください：

   ```
   $ sudo systemctl restart systemd-logind.service
   ```

2. SUSE Linux Enterprise Server 15 オペレーティングシステムを搭載したデバイスにネットワークエージェントをインストールする場合は、ネットワークエージェントの設定前に、insserv-compat パッケージをインストールします。

3. インストールパッケージをダウンロードして作成します：

   a. パッケージのインストール前に、このパッケージが依存するプログラムやライブラリのすべてがデバイスにインストールされていることを確認してください。

   パッケージの依存関係は、パッケージのインストール先の Linux ディストリビューションに含まれるユーティリティで確認できます。それらのユーティリティについて詳しくは、オペレーティングシステムのマニュアルを参照してください。

   b. ネットワークエージェントのインストールパッケージをダウンロードします。

   c. リモートインストールパッケージを作成するには、次のファイルを使用します：

      - klnagent.kpd
      - akinstall.sh
      - ネットワークエージェントの DEB または RPM パッケージ

4. 次の設定でリモートインストールタスクを作成します：

   - 新規タスクウィザードの［**設定**］ページで、［**管理サーバーを通じてオペレーティングシステムの共有フォルダーを使用する**］をオンにします。それ以外のチェックボックスはすべてオフにします。
   - ［**タスクを実行するアカウントの選択**］ページで、SSH でデバイスに接続するために使用するユーザーアカウントの設定を指定します。

5. リモートインストールタスクを実行します。`su` コマンドのオプションを使用して、環境を保持します: `-m, -p, --preserve-environment`。

バージョン 20 より前の Fedora で動作しているデバイスにネットワークエージェントを SSH でインストールすると、エラーになることがあります。その場合、ネットワークエージェントをインストールするには、/etc/sudoers で Defaults requiretty オプションをコメントアウト（つまりコメント構文で囲むように）します。SSH での接続中に、Defaults requiretty オプションが問題になる条件の詳細は、Bugzilla バグトラッキング Web サイトを参照してください。

リモートインストールタスクを使用したアプリケーションのインストール

Kaspersky Security Center Linux では、リモートインストールタスクを使用してデバイスにアプリケーションをリモートインストールできます。このタスクは、専用のウィザードを使用して作成しデバイスに割り当てます。タスクを簡単にデバイスに割り当てるには、次のいずれかの方法を使用し、ウィザードウィンドウでデバイスを指定できます：

- **ネットワークの管理サーバーによって検出されたデバイスを選択する**：この場合、タスクを特定のデバイスに割り当てます。特定のデバイスには、管理グループに属するデバイスと管理グループが割り当てられていないデバイスの両方を含めることができます。
- **デバイスのアドレスを手動で指定するか、リストからアドレスをインポートする**：タスクを割り当てるデバイスの DNS 名、IP アドレス、IP サブネットを指定できます。
- **デバイスの抽出にタスクを割り当てる**：この場合、既に作成された抽出に属するデバイスにタスクを割り当てます。既定の抽出または作成済みのカスタム抽出を指定できます。
- **管理グループにタスクを割り当てる**：この場合、既に作成された管理グループに属するデバイスにタスクを割り当てます。

ネットワークエージェントがインストールされていないデバイスでリモートインストールを正常に行うには、次のポートを開いておく必要があります：TCP 139 および 445、UDP 137 および 138。既定では、これらのポートはドメイン内のすべてのデバイスで開いています。これらは、リモート導入準備ユーティリティによって自動的に開かれます。

特定のデバイスへのアプリケーションのインストール

このセクションでは、管理グループ、特定の IP アドレスを持つデバイス、またはさまざまな管理対象デバイスにアプリケーションをリモートインストールする方法について説明します。

アプリケーションを特定のデバイスにインストールするには：

1. メインメニューで、［**デバイス**］→［**タスク**］の順に移動します。
2. ［**追加**］をクリックします。
   新規タスクウィザードが起動します。
3. ［**タスク種別**］で、［**アプリケーションのリモートインストール**］を選択します。
4. 次のいずれかのオプションをオンにします：
   - **管理グループにタスクを割り当てる**

任意の管理グループに属するデバイスにタスクを割り当てます。既存のグループを指定するか、新規グループを作成できます。

たとえば、特定の管理グループに含まれるデバイスのみが対象のメッセージをユーザーに送信する時に、このオプションを使用すると便利です。

- **デバイスのアドレスを手動で指定するか、リストからアドレスをインポートする**

  タスクを割り当てるデバイスの DNS 名、IP アドレス、IP サブネットを指定できます。

  特定のサブネットワークでタスクを実行する時に、このオプションを使用すると便利です。たとえば、経理担当者のデバイスにのみ特定のアプリケーションをインストールしたり、感染した可能性のあるサブネットワークでデバイスをスキャンする場合などです。

- **デバイスの抽出にタスクを割り当てる**

  デバイスの抽出に属するデバイスにタスクを割り当てます。既存の抽出のいずれかを選択できます。

  たとえば、特定のバージョンのオペレーティングシステムを使用しているデバイスを対象にタスクを実行する時に、このオプションを使用すると便利です。

5. ウィザードの指示に従ってください。

   新規タスクウィザードは、ウィザードで選択したアプリケーションを指定したデバイスにリモートインストールするタスクを作成します。［**管理グループにタスクを割り当てる**］オプションを選択した場合、タスクはグループ 1 になります。

6. 手動でタスクを実行するか、タスク設定で指定したスケジュールに基づいてタスクが起動するのを待ちます。

リモートインストールタスクが完了すると、指定したデバイスに選択したアプリケーションがインストールされます。

Active Directory グループポリシーを使用したアプリケーションのインストール

Kaspersky Security Center では、Active Directory グループポリシーを使用して、管理対象デバイスにカスペルスキー製品をインストールできます。

Active Directory グループポリシーを使用したインストールは、ネットワークエージェントを含むインストールパッケージからのみ可能です。

Active Directory グループポリシーを使用してアプリケーションをインストールするには：

1. 製品導入ウィザードを実行します。ウィザードの指示に従ってください。
2. 製品導入ウィザードの［**リモートインストールタスク設定**］ウィンドウで、［**Active Directory のグループポリシーにパッケージのインストールを割り当てる**］オプションをオンにします。

3. ［デバイスにアクセスするアカウントの選択］ウィンドウで、［**アカウントが必要（ネットワークエージェントの使用なし）**］オプションをオンにします。

4. Kaspersky Security Center をインストールするデバイスの管理者権限があるアカウントまたは Group Policy Creator Owners ドメイングループに含まれるアカウントを追加します。

5. 選択したアカウントに権限を付与するには：

   a. ［**コントロールパネル**］→［**管理ツール**］の順に選択し、［**グループポリシーの管理**］を開きます。

   b. 必要なドメインのフォルダーをクリックします。

   c. ［**委任**］セクションをクリックします。

   d. ［**権限**］のドロップダウンリストから［**GPO をリンク**］を選択します。

   e. ［**追加**］をクリックします。

   f. 開いた［**ユーザー、コンピューター、またはグループの選択**］ウィンドウで、必要なアカウントを選択します。

   g. ［**OK**］をクリックして、［**ユーザー、コンピューター、またはグループの選択**］ウィンドウを閉じます。

   h. ［**グループとユーザー**］の一覧で、先ほど追加したアカウントを選択して、［**詳細**］→［**詳細**］の順にクリックします。

   i. ［**権限エントリ**］リストで、追加したアカウントをダブルクリックします。

   j. 次の権限を付与します：

      - **グループオブジェクトの作成**
      - **グループオブジェクトの削除**
      - **グループポリシーコンテナーオブジェクトの作成**
      - **グループポリシーコンテナーオブジェクトの削除**

   k. ［**OK**］をクリックして変更内容を保存します。

6. ウィザードの指示に従って、他の設定を定義します。

7. 作成されたリモートインストールタスクを手動で実行するか、スケジュール済みの開始まで待機します。

リモートインストールが次の順番で開始されます：

1. タスクの実行時に、指定したすべてのクライアントデバイスが属する各ドメインに次の項目が作成されます：

   - ［**Kaspersky_AK{GUID}**］という名前のグループポリシーオブジェクト（GPO）。
   - GPO に対応するセキュリティグループこのセキュリティグループには、タスクが適用されるクライアントデバイスが含まれます。セキュリティグループの内容によって、GPO の範囲が定義されます。

2. Kaspersky Security Center は、選択されたカスペルスキー製品を、本製品の共有ネットワークフォルダー「Share」から直接クライアントデバイスにインストールします。Kaspersky Security Center のインストールフォルダーでは、アプリケーションをインストールするための MSI ファイルを含む補助的なサブフォルダーが作成されます。

3. 新しいデバイスをタスク範囲に追加すると、次回のタスク開始時に、新しいデバイスがセキュリティグループに追加されます。タスクスケジュールで［**未実行のタスクを実行する**］をオンにしていると、デバイスはすぐにセキュリティグループに追加されます。

4. デバイスがタスク範囲から削除されると、次回のタスク開始時にセキュリティグループからも削除されます。

5. タスクを Active Directory から削除すると、GPO、GPO へのリンクおよび対応するセキュリティグループも削除されます。

Active Directory を使用して別のインストールスキームを適用する場合は、必要な設定を手動で指定できます。手動での設定が必要な可能性がある場合は次の通りです：

- アンチウイルスによる保護の管理者が一部のドメインの Active Directory で変更権限を持っていない場合
- 元のインストールパッケージを別のネットワークリソースに保存する必要がある場合
- 特定の Active Directory ユニットに GPO をリンクする場合

Active Directory で別のインストールスキームのオプションは次の通りです：

- インストールが Kaspersky Security Center の共有フォルダーから直接実行される場合、GPO プロパティで、目的のアプリケーションのインストールパッケージフォルダーのサブフォルダー exec にある MSI ファイルを指定する必要があります。
- インストールパッケージを別のネットワークリソースに配置する必要がある場合は、フォルダー exec の内容全部をネットワークリソースにコピーする必要があります。これは、このフォルダーには MSI ファイルの他に、パッケージの作成時に生成された構成ファイルが含まれているためです。アプリケーションと同時にライセンスをインストールするには、ライセンス情報ファイルもこのフォルダーにコピーします。

セカンダリ管理サーバーへのアプリケーションのインストール

セカンダリ管理サーバーにアプリケーションをインストールするには：

1. 目的のセカンダリ管理サーバーを制御する管理サーバーとの接続を確立します。

2. インストールするアプリケーションに対応するインストールパッケージが、選択したそれぞれのセカンダリ管理サーバー上で使用可能であるか確認してください。セカンダリサーバーのいずれにもインストールパッケージが見つからない場合は、配布します。この目的のために、タスク種別［**インストールパッケージの配布**］でタスクを作成します。

3. セカンダリ管理サーバーでリモートアプリケーションのインストール用のタスクを作成します。タスク種別として［**セカンダリ管理サーバーへのアプリケーションのリモートインストール**］を選択します。

   タスク追加ウィザードは、ウィザードで選択したアプリケーションを特定のセカンダリ管理サーバーにリモートインストールするタスクを作成します。

4. 手動でタスクを実行するか、タスク設定で指定したスケジュールに基づいてタスクが起動するのを待ちます。

リモートインストールタスクが完了すると、選択したアプリケーションがセカンダリ管理サーバーにインストールされます。

Unix デバイスのリモートインストールを設定する

リモートインストールタスクを使用して Unix デバイスにアプリケーションをインストールする際、タスクに Unix 固有の設定を指定することができます。これらの設定はタスクが作成された後にタスクのプロパティで利用できるようになります。

Unix 固有の設定をリモートインストールタスクで指定するには：

1. メインメニューで、［**デバイス**］→［**タスク**］の順に選択します。
2. Unix 固有の設定を指定するリモートインストールタスクの名前をクリックします。
   タスクのプロパティウィンドウが開きます。
3. ［**アプリケーション設定**］→［**Unix 固有の設定**］の順に移動します。
4. 次の設定を指定します：
   - **root アカウントのパスワードを設定する（SSH での導入時のみ）**

     パスワードを指定しないと対象のデバイスで sudo コマンドが使用できない場合、このオプションを選択してルートアカウントのパスワードを指定します。Kaspersky Security Center 14 Linux は対象デバイスにパスワードを暗号化して転送し、復号化してからこのパスワードを使用してルートアカウントに代わってインストール手順を開始します。

     Kaspersky Security Center 14 Linux は SSH 接続を作成するためにユーザーアカウントや指定したパスワードを使用しません。

   - **ターゲットデバイスへの実行権限がある一時ディレクトリへのパスを指定する（SSH での導入時のみ）**

     対象デバイスの /tmp ディレクトリに実行権限がない場合、このオプションを選択してから実行権限のあるディレクトリへのパスを指定します。Kaspersky Security Center 14 Linux は SSH 経由でアクセスする一時ディレクトリとして指定されたディレクトリを使用します。アプリケーションはインストールパッケージをそのディレクトリに配置し、インストールプロセスを実行します。
5. ［**保存**］をクリックします。

   指定したタスク設定が保存されます。

サードパーティのセキュリティ製品からの移行とアンインストールの実施

カスペルスキーのセキュリティ製品を Kaspersky Security Center Linux を使用してインストールする場合、インストールするアプリケーションと競合するサードパーティ製ソフトウェアを削除しなければならない場合があります。Kaspersky Security Center では、サードパーティ製品を削除する複数の方法が用意されています。

競合するアプリケーションの削除をアプリケーションのリモートインストールの設定時に指定

製品導入ウィザードのセキュリティ製品のリモートインストールの設定時に［**競合アプリケーションを自動的にアンインストールする**］をオンにできます。このオプションをオンにすると、管理対象デバイスにセキュリティ製品をインストールする前に、Kaspersky Security Center は競合するアプリケーションを削除します。

実行手順の説明：セキュリティ製品をインストールする前に競合するアプリケーションを削除する

専用タスクを使用した競合アプリケーションの削除

競合アプリケーションを削除するには、**アプリケーションのリモートアンインストール**タスクを使用します。このタスクは、セキュリティ製品のインストールタスクの前にデバイスで実行する必要があります。たとえば、インストールタスクのスケジュール種別として［**他のタスクが完了次第**］を選択し、条件の対象となるタスクとして［**アプリケーションのリモートアンインストール**］を指定できます。

このアンインストール方法は、セキュリティ製品のインストーラーでは競合アプリケーションを適切に削除できない場合に有用です。

実行手順の説明：タスクの作成

アプリケーションまたはソフトウェアのアップデートのリモートでの削除

Linux を実行している管理対象デバイスのアプリケーションまたはソフトウェアアップデートは、ネットワークエージェントを使用した場合のみリモートから削除することができます。

選択したデバイスからリモートでアプリケーションまたはソフトウェアのアップデートを削除するには：

1. メインメニューで、［**デバイス**］→［**タスク**］の順に移動します。
2. ［**追加**］をクリックします。
   タスク追加ウィザードが開始されます。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。
3. Kaspersky Security Center を対象アプリケーションとするタスクから、［**アプリケーションのリモートアンインストール**］タスク種別を選択します。
4. 作成中のタスク名を入力します。
   タスク名は 100 文字以下で、特殊文字（"*<>?\:|）を含めることはできません。
5. タスクを割り当てるデバイスを選択します。
6. 削除するソフトウェアの種類を選択してから、削除する特定のアプリケーション、アップデート、またはパッチを選択します。

   - **管理対象アプリケーションをアンインストールする**

     カスペルスキー製品のリストが表示されます。削除するアプリケーションを選択します。

   - **競合アプリケーションをアンインストールする**

カスペルスキーのセキュリティ製品または Kaspersky Security Center と互換性のないアプリケーションのリストが表示されます。削除するアプリケーションの隣にあるチェックボックスをオンにします。

- **アプリケーションレジストリからアプリケーションを削除する**

既定では、ネットワークエージェントは管理対象デバイスにインストールされているアプリケーションに関する情報を管理サーバーに送信します。インストールされているアプリケーションのリストは、アプリケーションレジストリに保存されます。

アプリケーションレジストリからアプリケーションを選択するには：

a. ［**アンインストールするアプリケーション**］をクリックし、削除するアプリケーションを選択します。

b. アンインストールオプションを指定します：

- **アンインストールモード**

アプリケーションを削除する方法を選択します：

- **アンインストールコマンドを自動的に定義する**

  アプリケーションの製造元によって定義されたアンインストールコマンドがアプリケーションにある場合、Kaspersky Security Center はこのコマンドを使用します。このオプションをオンにすることを推奨します。

- **アンインストールコマンドを指定する**

  アプリケーションのアンインストール用のコマンドを指定する場合は、このオプションをオンにします。

  まず、［**アンインストールコマンドを自動的に定義する**］をオンにしてアプリケーションを削除してみてください。自動的に定義されたコマンドによるアンインストールが失敗した場合は、独自のコマンドを使用してください。

  フィールドにインストールコマンドを入力し、次のオプションをオンにします。

  既定コマンドが自動検知されない場合、このアンインストール用コマンドを使用

  Kaspersky Security Center は、選択されたアプリケーションに、アプリケーションの製造元が定義したアンインストールコマンドがあるかどうかを確認します。コマンドが見つかった場合、Kaspersky Security Center は、［**アプリケーションのアンインストール用コマンド**］で指定されたコマンドの代わりにそのコマンドを使用します。

  このオプションをオンにすることを推奨します。

- **アプリケーションのアンインストール後に再起動する**

アンインストールが正常に完了した後で、アプリケーションが管理対象デバイスでオペレーティングシステムを再起動する必要がある場合、オペレーティングシステムは自動的に再起動されます。

7. クライアントデバイスがアンインストールユーティリティをダウンロードする方法を指定します：

- **ネットワークエージェントを使用する**

  ファイルは、クライアントデバイスにインストールされているネットワークエージェントによってクライアントデバイスに配布されます。

  このオプションをオフにすると、ファイルはLinuxオペレーティングシステムツールを使用して配信されます。

  ネットワークエージェントがインストールされたデバイスにタスクが割り当てられている場合は、このチェックボックスをオンにすることを推奨します。

- **管理サーバーを通じてオペレーティングシステムの共有フォルダーを使用する**

  このオプションは廃止されました。代わりに、［**ネットワークエージェントを使用する**］または［**ディストリビューションポイントを通じてオペレーティングシステムの共有フォルダーを使用する**］オプションを使用してください。

  ファイルは、管理サーバーのオペレーティングシステムツールを使用してクライアントデバイスに送信されます。このオプションは、クライアントデバイスにネットワークエージェントがインストールされていないものの、クライアントデバイスが管理サーバーと同じネットワークに存在する場合にオンにできます。

- **ディストリビューションポイントを通じてオペレーティングシステムの共有フォルダーを使用する**

  ファイルは、オペレーティングシステムのツールを使用してディストリビューションポイント経由でクライアントデバイスに送信されます。このオプションをオンにできるのは、ネットワークに少なくとも1つのディストリビューションポイントがある場合です。

  ［**ネットワークエージェントを使用する**］をオンにすると、ネットワークエージェントのツールが使用できない場合に限り、ファイルがオペレーティングシステムのツールを使用して配布されます。

- **同時ダウンロード数の上限**

  管理サーバーが同時にファイルを送信できるクライアントデバイスの最大許容数。この数が大きいほど、アプリケーションのアンインストールは高速になりますが、管理サーバーの負荷が増大します。

- **アンインストール試行回数の上限**

*アプリケーションのリモートアンインストール*タスクの実行時に、パラメータで指定されたインストーラーの実行回数の範囲内で、管理対象デバイスから対象製品をアンインストールすることに失敗した場合、Kaspersky Security Center はこの管理対象デバイスへのインストールユーティリティの配布を中止し、そのデバイス上でインストーラーを起動しなくなります。

［**アンインストール試行回数の上限**］パラメータを使用することで、管理対象デバイス上でのリソースの消費量とネットワークのトラフィック量を軽減できます（アンインストールの実行や MSI ファイルの実行によるリソース消費、エラーメッセージのトラフィック）。

タスクの開始が繰り返し試行されることは、デバイス上でインストールを阻害する問題が発生していることを示している可能性があります。管理者は、指定されたアンインストールの試行回数内で問題を解決してから、タスクを（手動でまたはスケジュールによって）再起動する必要があります。

指定された試行回数以内にアンインストールを実行できなかった場合、問題は解決不可能なものとして認識され、それ以上タスクの開始を試行することは不必要にリソースとトラフィックを消費してしまうものと判断されます。

タスクが作成されると、試行回数のカウンターは「`0`」にセットされます。デバイス上でインストーラーを実行してエラーが返されるたびに、カウンターの値が 1 ずつ増加します。

パラメータで指定した回数のインストールの試行が既に実行された後に、デバイスでアンインストールの準備が完了した場合は、［**アンインストール試行回数の上限**］パラメータの値を増やすことでアプリケーションをアンインストールするタスクを開始できます。または、［*アプリケーションのリモートアンインストール*］タスクを新規に作成することもできます。

- **ダウンロード前に OS の種別を確認する**

ファイルをクライアントデバイスに送信する前に、Kaspersky Security Center Linux はインストールユーティリティの設定がクライアントデバイスのオペレーティングシステムに適用可能であるかどうかを確認します。設定を適用できない場合、Kaspersky Security Center はファイルを送信せず、アプリケーションのインストールを試行しません。たとえば、様々なオペレーティングシステムを実行しているデバイスが存在する管理グループのデバイスにアプリケーションをインストールするには、インストールタスクを管理グループに割り当ててから、このオプションをオンにして、必要なオペレーティングシステム以外を実行しているデバイスをスキップできます。

8. OS の再起動設定を指定します。

- **デバイスを再起動しない**

操作後に、クライアントデバイスは自動的には再起動されません。操作を完了するには、デバイスを再起動する必要があります（手動で、またはデバイスの管理タスクを使用して）。必要な再起動についての情報は、タスク履歴とデバイスのステータスに保存されます。このオプションは、継続的な稼働が不可欠なサーバーなどのデバイスで実行するタスクに適切です。

- **デバイスを再起動する**

インストールの完了に再起動が必要な場合は常に、クライアントデバイスは自動的に再起動されます。このオプションは、定期的に稼働が一時停止（シャットダウンまたは再起動）するデバイスのタスクに有用です。

- **セッションがブロックされたアプリケーションを強制終了する**

アプリケーションを実行すると、クライアントデバイスの再起動が妨げられる場合があります。たとえば、ドキュメント作成アプリケーションでドキュメントを編集しており、その内容が保存されていない場合、アプリケーションはデバイスの再起動を許可しません。

このオプションをオンにすると、ブロックされたデバイス上のアプリケーションが、再起動の前に強制的に閉じられます。これにより、保存していなかった作業内容が失われる場合があります。

このオプションをオフにすると、ブロックされたデバイスは再起動されません。このデバイス上のタスクのステータスでは、デバイスの再起動が必要であることが表示されます。ブロックされたデバイスでは、実行中のアプリケーションすべてをユーザーが手動で終了し、デバイスを再起動する必要があります。

既定では、このオプションはオフです。

9. 必要に応じて、リモートアンインストールタスクの開始に使用するアカウントを追加できます：

- **アカウントが不要（ネットワークエージェントインストール済み）**

  このオプションをオンにすると、アプリケーションのインストーラーを実行するアカウントを指定する必要はありません。タスクは管理サーバーのサービスを実行しているアカウントで実行されます。

  クライアントデバイスにネットワークエージェントがインストールされていない場合、このオプションは使用できません。

- **アカウントが必要（ネットワークエージェントの使用なし）**

  *アプリケーションのリモートアンインストール*タスクを割り当てるデバイスにネットワークエージェントがインストールされていない場合は、このオプションをオンにします。

  アプリケーションのインストーラーを実行するユーザーアカウントを指定します。［**追加**］をクリックし、［**アカウント**］を選択してから、ユーザーアカウントの資格情報を指定します。

  タスクを割り当てるすべてのデバイスで必要なすべての権限をどのアカウントも持たない場合などのために、複数のユーザーアカウントを追加できます。この場合、追加されたすべてのアカウントが上から下へ順番に使用され、タスクが実行されます。

10. 既定のタスク設定を編集する場合、［**タスク作成の終了**］ページで、［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにします。このオプションをオフにすると、既定の設定でタスクが作成されます。既定の設定からの変更は、後からいつでも実行できます。

11. ［**終了**］をクリックします。

    タスクが作成され、タスクリストに表示されます。

12. 作成したタスクの名前をクリックし、タスクのプロパティウィンドウを開きます。

13. タスクのプロパティウィンドウで、タスクの全般的な設定を指定します。

14. ［**保存**］をクリックします。

15. 手動でタスクを実行するか、タスク設定で指定したスケジュールに基づいてタスクが起動するのを待ちます。

リモートアンインストールタスクが完了すると、選択したアプリケーションが選択したデバイスから削除されます。

ネットワークエージェントをインストールする SUSE Linux Enterprise Server 15 デバイスの準備

SUSE Linux Enterprise Server 15 オペレーティングシステムのデバイスにネットワークエージェントを準備するには：

ネットワークエージェントのインストール前に、次のコマンドを実行します：

```
$ sudo zypper install insserv-compat
```

これにより、insserv-compat パッケージのインストールと、ネットワークエージェントの適切な設定が可能になります。

`rpm -q insserv-compat` コマンドを実行し、パッケージがインストール済みかどうかをチェックします。

多くの SUSE Linux Enterprise Server 15 デバイスがネットワークに存在する場合、会社のインフラストラクチャを設定、管理する専用のソフトウェアを使用できます。このソフトウェアを使用することで、必要なすべてのデバイスに insserv-compat パッケージを一度に自動的にインストールできます。たとえば、Puppet、Ansible、Chef を使用したり、独自のスクリプトを作成したりできます。都合のよい方法を使用してください。

SUSE Linux Enterprise Server 15 デバイスの準備が完了したら、ネットワークエージェントを配信してインストールします。

カスペルスキー製品：ライセンスとアクティベーション

このセクションでは、管理対象のカスペルスキー製品のライセンスを Kaspersky Security Center で操作する方法について説明します。

Kaspersky Security Center Linux では、クライアントデバイスにカスペルスキー製品のライセンスを一元的に配信し、使用状況の監視およびライセンスの更新を実行できます。

Kaspersky Security Center でライセンスを追加すると、ライセンスの設定が管理サーバーで保存されます。アプリケーションでは、この情報に基づいて、ライセンス使用レポートを生成し、ライセンスの有効期限と、ライセンスのプロパティで設定されるライセンスの制限事項の違反について管理者に通知します。ライセンス使用の通知の設定は管理サーバーで設定できます。

管理対象アプリケーションのライセンスの管理

管理対象デバイスにインストールされているカスペルスキー製品には、各製品のライセンス情報ファイルまたはアクティベーションコードを適用してライセンスを付与する必要があります。ライセンス情報ファイルとアクティベーションコードは次の方法で展開できます：

- 自動配信
- 管理対象アプリケーションのインストールパッケージ
- 管理対象アプリケーションへのライセンスの追加タスク
- 管理対象アプリケーションの手動アクティベーション

上記のいずれかの方法で、新しい現在のライセンスまたは予備のライセンスを追加できます。カスペルスキー製品は、現時点で現在のライセンスを使用し、現在のライセンスの有効期限が切れた後に適用する予備のライセンスを保存します。ライセンスを追加するアプリケーションは、ライセンスが現在のライセンスか予備のライセンスかを定義します。ライセンスの定義は、新しいライセンスの追加方法には依存しません。

自動配信

異なる複数の管理対象アプリケーションを使用し、特定のライセンス情報ファイルまたはアクティベーションコードをデバイスに配信する必要がある場合は、他の配信方法を選択してください。

Kaspersky Security Center を使用して、使用可能なライセンスをデバイスに配信できます。ここでは、3 個のライセンスが管理サーバーのリポジトリに保管されている場合を例にします。［**自動配信されるライセンス**］を 3 個のライセンスすべてに対してオンにしていると仮定します。カスペルスキーのセキュリティ製品（例：Kaspersky Endpoint Security for Linux）が、組織内のデバイスにインストールされているとします。ライセンスを配信する必要がある新しいデバイスが検出されます。リポジトリ内に保管されている、名前がそれぞれ「*Key_1*」「*Key_2*」である 2 個のライセンス情報ファイルが、そのデバイスに配信可能であると本製品が判断します。そのうち 1 個のライセンス情報ファイルが、デバイスに配信されます。この場合、どのライセンス情報ファイルがデバイスに適用されるかは予測ができません。自動配信されるライセンスに対して、管理者が設定可能な項目がないからです。

ライセンスが配信されると、そのライセンスを適用中のデバイスの台数が再度計上されます。ライセンスが適用可能な台数を超えないように、適用中のデバイスの台数を確認しておく必要があります。ライセンスを適用可能な台数の上限を超えると、ライセンスが適用されていないデバイスのステータスが「*緊急*」になります。

配信前に、管理サーバーのリポジトリにライセンス情報ファイルまたはアクティベーションコードを追加する必要があります。

実行手順の説明：

- ライセンスの管理サーバーリポジトリへの追加
- ライセンスの自動配信

ライセンス情報ファイルまたはアクティベーションコードを管理対象アプリケーションのインストールパッケージに追加

セキュリティ上の理由から、このオプションの使用は推奨されません。インストールパッケージに追加したライセンス情報ファイルまたはアクティベーションコードは、漏洩などの危険にさらされる可能性があります。

インストールパッケージを使用して管理対象アプリケーションをインストールする場合、パッケージ内またはアプリケーションのポリシー内に含まれるアクティベーションコードまたはライセンス情報ファイルを指定できます。ライセンスが管理対象デバイスに配信されるのは、デバイスと管理サーバーの次回の同期時です。

実行手順の説明：インストールパッケージへのライセンスの追加

管理対象アプリケーションへのライセンスの追加タスクを使用して配信

管理対象アプリケーションへのライセンスの追加タスクを使用する場合、配信する必要があるライセンスを選択後、対象デバイスを都合のよい方法で選択できます。たとえば、管理グループを選択したり、デバイスの抽出を使用したりすることが可能です。

配信前に、管理サーバーのリポジトリにライセンス情報ファイルまたはアクティベーションコードを追加する必要があります。

実行手順の説明：

- ライセンスの管理サーバーリポジトリへの追加
- ライセンスのクライアントデバイスへの配信

アクティベーションコードまたはライセンス情報ファイルを手動でデバイスに追加

インストール済みのカスペルスキー製品を、製品インターフェイス内のツールを使用してローカルでアクティベーションできます。詳しくは、インストールされているアプリケーションのヘルプを参照してください。

ライセンスの管理サーバーリポジトリへの追加

ライセンスを管理サーバーリポジトリに追加するには：

1. メインメニューで、［**操作**］→［**ライセンス管理**］→［**カスペルスキーのライセンス**］の順に選択します。
2. ［**追加**］をクリックします。

3. 目的の対象を追加します：

- **ライセンス情報ファイルの追加**
  ［**ライセンス情報ファイルの選択**］をクリックし、追加するライセンス情報ファイルを指定します。
- **アクティベーションコードの入力**
  テキストフィールドにアクティベーションコードを入力し、［**送信**］をクリックします。

4. ［**閉じる**］をクリックします。

管理サーバーのリポジトリにライセンスが追加されます。

ライセンスのクライアントデバイスへの配信

Kaspersky Security Center 14 Web コンソールでは、*ライセンス配信タスク*によってクライアントデバイスにライセンスを配信できます。

配信前に、ライセンスを管理サーバーリポジトリに追加します。

クライアントデバイスにライセンスを配信するには：

1. メインメニューで、［**デバイス**］→［**タスク**］の順に移動します。
2. ［**追加**］をクリックします。
   タスク追加ウィザードが開始されます。
3. ライセンスを追加する製品を選択します。
4. ［**タスク種別**］リストから、［**ライセンスの追加**］を選択します。
5. ウィザードの指示に従ってください。
6. 既定のタスク設定を編集する場合、［**タスク作成の終了**］ページで、［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにします。このオプションをオフにすると、既定の設定でタスクが作成されます。既定の設定からの変更は、後からいつでも実行できます。
7. ［**作成**］をクリックします。
   タスクが作成され、タスクリストに表示されます。
8. タスクを実行するには、タスクリストで目的のタスクを選択し、［**開始**］をクリックします。

タスクが実行されると、選択したデバイスにライセンスが追加されます。

ライセンスの自動配信

Kaspersky Security Center Linux では、管理サーバーのライセンスリポジトリにあるライセンスを管理対象デバイスに自動配信できます。

管理対象デバイスにライセンスを自動配信するには：

1. メインメニューで、［**操作**］→［**ライセンス管理**］→［**カスペルスキーのライセンス**］の順に選択します。
2. デバイスに自動配信するライセンスをクリックします。
3. 表示されるライセンスのプロパティウィンドウで［**管理対象デバイスにライセンスを自動的に配信する**］をオンにします。
4. ［**保存**］をクリックします。

ライセンスは、互換性のあるすべてのデバイスに自動的に配信されます。

ライセンスはネットワークエージェント経由で配信されます。アプリケーションに対するライセンスの配信タスクは作成されません。

ライセンスが自動配信される際、デバイス数へのライセンスの制限が適用されます。ライセンスの制限は、ライセンスのプロパティで設定済みです。ライセンス数の上限に達した場合は、デバイスへの配信は自動的に停止します。

ライセンスのプロパティウィンドウで［**管理対象デバイスにライセンスを自動的に配信する**］がオンになっている場合、ライセンスキーはネットワークにすぐに配布されます。このオプションを選択しない場合は、後から手動でライセンスを配信することができます。

使用中のライセンスに関する情報の表示

管理サーバーのリポジトリに追加されているライセンスのリストを表示するには：

メインメニューで、［**操作**］→［**ライセンス管理**］→［**カスペルスキーのライセンス**］の順に選択します。

管理サーバーのリポジトリに追加されているライセンス情報ファイルとアクティベーションコードのリストが表示されます。

ライセンスの詳細情報を表示するには：

1. メインメニューで、［**操作**］→［**ライセンス管理**］→［**カスペルスキーのライセンス**］の順に選択します。
2. 目的のライセンスの名前をクリックします。

ライセンスのプロパティウィンドウが表示され、次の情報を確認できます：

- ［**全般**］タブ：ライセンスに関する主要な情報
- ［**デバイス**］タブ：このライセンスが、インストールされているカスペルスキー製品のアクティベーションに使用されたクライアントデバイスのリスト

特定のクライアントデバイスにどのライセンスが追加されたかを表示するには：

1. メインメニューで、［**デバイス**］→［**管理対象デバイス**］の順に移動します。

2. 目的のデバイスの名前をクリックします。

3. デバイスのプロパティウィンドウが開いたら、［**アプリケーション**］タブをクリックします。

4. ライセンスの情報を確認するアプリケーションの名前をクリックします。

5. 表示されるアプリケーションのプロパティウィンドウで、［**全般**］タブを選択し、［**ライセンス**］セクションを表示します。

   現在のライセンスと予備のライセンスに関する主要な情報が表示されます。

仮想管理サーバーのライセンスの最新の設定を定義するため、管理サーバーはカスペルスキーのアクティベーションサーバーに少なくとも毎日1度はリクエストを送信します。

リポジトリからのライセンスの削除

管理対象デバイスに追加済みの現在のライセンスを管理サーバーのリポジトリから削除した場合、管理対象デバイスにインストールされている製品は動作を継続します。

管理サーバーのリポジトリからライセンス情報ファイルまたはアクティベーションコードを削除するには：

1. ［**操作**］→［**ライセンス管理**］→［**カスペルスキーのライセンス**］の順に選択します。

2. リポジトリから削除するライセンス情報ファイルまたはアクティベーションコードを選択します。

3. ［**削除**］をクリックします。

4. ［**OK**］をクリックして処理を確定します。

   選択したライセンス情報ファイルまたはアクティベーションコードが削除されます。

削除されたライセンスの再追加や、新しいライセンスの追加も可能です。

使用許諾契約書による同意の取り消し

一部のクライアントデバイスの保護を停止する場合、任意の管理対象カスペルスキー製品の使用許諾契約書（EULA）への同意を取り消すことができます。EULA への同意を取り消す前に、選択したアプリケーションをアンインストールする必要があります。

管理対象のカスペルスキー製品の EULA を取り消すには：

1. 管理サーバーのプロパティウィンドウを開き、［**全般**］タブの［**使用許諾契約書**］セクションに移動します。

   インストールパッケージの作成時、アップデートのシームレスインストール時、または Kaspersky Security for Mobile の導入時に同意した EULA のリストが表示されます。

2. リストから、同意を取り消す EULA を選択します。

   EULA の以下のプロパティを確認できます：

- EULA に同意した日付
- EULA に同意したユーザーの名前

3. EULA に同意した日付のうち任意のものをクリックし、次のデータが表示されるプロパティウィンドウを開きます：
   - EULA に同意したユーザーの名前
   - EULA に同意した日付
   - EULA の一意な識別子（UID）
   - EULA のテキスト
   - EULA に関連するオブジェクト、および各オブジェクトの名前と種別のリスト（インストールパッケージ、シームレスアップデート、モバイルアプリ）
4. EULA のプロパティウィンドウの下部で、［**使用許諾契約書への同意を取り消す**］をクリックします。

   EULA への同意の取り消しを妨げるオブジェクト（インストールパッケージ、およびそのパッケージを使用するタスク）が存在する場合、そのオブジェクトに関する通知が表示されます。これらのオブジェクトを削除するまで、取り消しの動作を続行できません。

   表示されたウィンドウで、この EULA に対応するカスペルスキー製品を最初にアンインストールすることが必要であることが示されます。
5. ボタンをクリックして取り消しを確定します。

これで EULA が取り消されました。［**使用許諾契約書** ］セクションの使用許諾契約書のリストに表示されなくなります。EULA のプロパティウィンドウが閉じ、製品がインストールされなくなります。

カスペルスキー製品のライセンスの更新

有効期間の終了した、または有効期間がまもなく終了する（残り 30 日以内）のカスペルスキー製品のライセンスを更新できます。

有効期間が終了した、もしくは有効期間がまもなく終了するライセンスを更新するには：

1. 次のいずれかの手順を実行します：
   - メインメニューで、［**操作**］→［**ライセンス管理**］→［**カスペルスキーのライセンス**］の順に選択します。
   - ［**監視とレポート**］→［**ダッシュボード**］の順に移動し、通知に隣接する［**有効期間がまもなく終了するライセンスを表示**］をクリックします。

   ［**カスペルスキーのライセンス** ］ウィンドウが表示され、ライセンスを表示および更新できます。
2. 目的のライセンスに隣接する［**ライセンスの更新**］をクリックします。

ライセンスの更新リンクをクリックすることで、お客様はカスペルスキーに次の情報を送信することに同意したものとします：バージョン、使用中の言語版、本ソフトウェアのライセンス識別子（更新しているライセンスの識別子）、および本製品を販売代理店経由でライセンスを購入したかどうかの情報。

3. 表示されるライセンス更新サービスのウィンドウで、ライセンスを更新する手順に従ってください。

   ライセンスが更新されました。

Kaspersky Security Center 14 Web コンソールでは、ライセンスの有効期間の終了間近になると次のスケジュールで通知が表示されます：

- 有効期限の 30 日前
- 有効期限の 7 日前
- 有効期限の 3 日前
- 有効期限の 24 時間前
- ライセンスの有効期間が終了した時

マーケットプレイスを使用してカスペルスキーの法人向けソリューションを選択する

［**マーケットプレイス**］はカスペルスキーのビジネスソリューションを全体的に表示できるメインメニューのセクションです。必要なものを選択してカスペルスキーの Web サイトに移動して購入プロセスに進むことができます。フィルターを使用してお客様の組織や情報セキュリティシステムの要件に一致するソリューションのみを表示することが可能です。ソリューションを選択すると、Kaspersky Security Center 14 Linux はそのソリューションの詳細について関連する Web ページにリダイレクトします。各 Web ページで、製品の購入に進んだり、購入に関する手順を確認したりできます。

［**マーケットプレイス**］セクションでは、次の条件を使用してカスペルスキー製品をフィルターすることができます：

- 保護対象のデバイスの数（エンドポイント、サーバー、その他の種別の資産）：
  - 50～250
  - 250～1000
  - 1000 以上
- 組織の情報セキュリティチームの成熟度：
  - **基本のセキュリティ**

    このレベルは IT チームを 1 つのみ持つ企業に典型的なレベルです。脅威は、自動的に可能な最大数ブロックされます。
  - **最適なセキュリティ**

このレベルは IT チーム内に IT セキュリティ機能を持つ特定の IT チームを持つ企業に典型的なレベルです。このレベルでは、企業はコモディティ型の脅威や既存の防御メカニズムを回避する脅威などに対応するソリューションを必要とします。

- **高度なセキュリティ**

  このレベルは複雑で分散化された IT 環境を持つ機能に典型的なレベルです。IT セキュリティチームの熟練度が高い、または企業が SOC（セキュリティオペレーションセンター）チームを持っているなどのレベルです。必要とされるソリューションは、複雑な脅威および標的型攻撃に対応するものです。

- 保護対象の資産の種別：

  - **エンドポイント**：物理および仮想マシン、埋め込みシステムなどの社員のワークステーション
  - **サーバー**：物理および仮想サーバー
  - **クラウド**：パブリック、プライベート、またはハイブリッドのクラウド環境およびクラウドサービス
  - **ネットワーク**：ローカルエリアネットワーク、IT インフラストラクチャ
  - **サービス**：カスペルスキーによって提供されるセキュリティ関連のサービス

カスペルスキーのビジネスソリューションを検索および購入するには：

1. メインメニューで、［**マーケットプレイス**］に移動します。

   既定では、セクションにはすべての使用可能なカスペルスキーのビジネスソリューションが表示されています。

2. 企業に合ったソリューションのみを表示するには、フィルターで必要な値を選択します。

3. 購入する、もしくは詳細を確認したいソリューションをクリックします。

ソリューションの Web ページにリダイレクトされます。画面上の説明に従って、購入プロセスを進められます。

ネットワーク保護の設定

このセクションには、ポリシーとタスクの手動設定、ユーザーロール、管理グループの構造とタスクの階層構造の構築に関する情報を記載しています。

シナリオ：ネットワーク保護の設定

クイックスタートウィザードにより、既定の設定でポリシーとタスクが作成されます。これらの設定は、組織のルールなどに照らして最適でない、または許容できない内容を含む可能性があります。したがって、ネットワークの必要性に応じて、これらのポリシーとタスクを調整し、他のポリシーとタスクを作成してください。

必須条件

導入を開始する前に、次が完了していることを確認してください：

- Kaspersky Security Center 管理サーバーをインストール済み
- Kaspersky Security Center 14 Web コンソールをインストール済み
- Kaspersky Security Center の主要なインストールシナリオを完了済み
- クイックスタートウィザードを完了済みまたは［**管理対象デバイス**］管理グループで以下のポリシーとタスクを手動で作成済み：
  - Kaspersky Endpoint Security のポリシー
  - Kaspersky Endpoint Security をアップデートするグループタスク
  - ネットワークエージェントのポリシー

ネットワーク保護の設定は、次の手順で進みます：

1. **カスペルスキー製品のポリシーとポリシーのプロファイルの設定と各デバイスへの反映**

   管理対象デバイスにインストールされているカスペルスキー製品のポリシーとポリシーのプロファイルを設定しデバイスに反映するには、デバイスベースとユーザーベースの 2 種類のセキュリティ管理方法を使用できます。これらの 2 つの管理方法を組み合わせることもできます。

2. **カスペルスキー製品のリモート管理用のタスクの設定**

   必要に応じて、クイックスタートウィザードを使用して作成したタスクを確認、調整します。

   実行手順の説明：Kaspersky Endpoint Security をアップデートするグループタスクの設定

   必要に応じて、クライアントデバイスにインストールされているカスペルスキー製品を管理するためのタスクを追加で作成します。

3. **データベースでのイベント情報による負荷の評価と制限**

   管理対象アプリケーションの動作中のイベントに関する情報は、クライアントデバイスから送信され、管理サーバーデータベースに記録されます。管理サーバーの負荷を軽減するには、データベースに保管される可能性のあるイベント数の最大値を評価し、上限を設定します。

   実行手順の説明：イベントの最大数の設定

結果

この手順を完了すると、カスペルスキー製品、タスク、管理サーバーで取得されるイベントの設定によってネットワークの保護が機能するようになります。

- ポリシーとポリシーのプロファイルに従ってカスペルスキー製品が設定されます。
- 製品が一連のタスクによって管理されるようになります。
- データベースに保存されるイベント数の上限が設定されます。

ネットワーク保護の設定が完了すると、定義データベースとカスペルスキー製品の定期アップデートの設定ステップに進むことができます。

デバイスベースのセキュリティ管理とユーザーベースのセキュリティ管理の概要

セキュリティ設定を、デバイスの仕様の観点やユーザーロールの観点から管理できます。1つ目のアプローチは*デバイスベースのセキュリティ管理*、2つ目のアプローチは*ユーザーベースのセキュリティ管理*と呼ばれます。異なるデバイスに異なる設定を適用するには、いずれかの管理方法あるいは両者を組み合わせた管理方法を使用できます。

デバイスベースのセキュリティ管理では、デバイスごとの状況などに合わせて、セキュリティ製品について複数の異なる設定を管理対象デバイスに適用できます。たとえば、異なる管理グループに属するデバイスに、異なる設定を適用できます。

ユーザーベースのセキュリティ管理を使用すると、ユーザーロールに応じて、異なるセキュリティ設定を適用できます。複数のユーザーロールを作成し、ユーザーごとに適切なユーザーロールを割り当てた上で、デバイスの所有者のユーザーロールに応じて、異なるセキュリティ設定をデバイスに適用できます。たとえば、経理部門の従業員と人事部門の従業員それぞれのデバイスに異なるアプリケーション設定を適用する場合などがありえます。これにより、ユーザーベースのセキュリティ管理を実施すると、経理部門の従業員と人事部門の従業員のカスペルスキー製品に対して、それぞれ独自の設定が適用されます。詳細設定により、製品設定のどの部分をユーザー側で設定でき、どの部分は管理者による設定が強制的に適用されるかを指定できます。

ユーザーベースのセキュリティ管理を使用すると、特定の1人のユーザーに特定の製品設定を適用できます。該当する従業員が社内で固有のロールを担っていたり、特定のユーザーのデバイスに関連したセキュリティインシデントを監視したい場合などに、こうした処理が必要になることがあります。社内でのこの従業員のロールに基づいて、ユーザーが製品設定を変更できる権限を拡張したり制限できます。たとえば、ローカルオフィスのクライアントデバイスを管理しているシステム管理者の権限を拡張する場合などです。

デバイスベースのセキュリティ管理とユーザーベースのセキュリティ管理を組み合わせることもできます。たとえば、管理グループごとに製品ポリシーを設定した上で、企業内の1つ以上のユーザーロールを対象としたポリシープロファイルを作成するなどの方法を使用できます。この場合、ポリシーとポリシープロファイルは次の順序で適用されます。

1. デバイスベースのセキュリティ管理用に作成されたポリシーが適用されます。
2. ポリシーは、ポリシープロファイルの優先度に応じてポリシープロファイルで変更されます。
3. ポリシーは、ユーザーロールと関連付けられたポリシープロファイルで変更されます。

ポリシーの設定と継承先への反映：デバイスベースの管理

この手順を完了すると、すべての管理対象デバイスにインストールされている製品が、定義した製品ポリシーとポリシープロファイルに従って設定されます。

必須条件

手順を開始する前に、Kaspersky Security Center 管理サーバーと Kaspersky Security Center 14 Web コンソールのインストールが完了していることを確認してください。また、デバイスベースの管理方法の代替案もしくは追加で組み合わせて使用する管理方法としてユーザーベースのセキュリティ管理も検討すると有益な場合があります。2 種類の管理方法について詳しくは、こちらのページを参照してください。

実行するステップ

カスペルスキー製品のデバイスベースの管理シナリオは、次の 2 つの手順からなります。

1. **製品ポリシーの設定**

   管理対象デバイスにインストールされているカスペルスキー製品ごとにポリシーを作成して、製品の設定を指定します。これらのポリシーはクライアントデバイスに反映されます。

   クイックスタートウィザードを使用してネットワークの保護を設定する場合、Kaspersky Security Center は Kaspersky Endpoint Security for Linux の既定のポリシーを作成します。このウィザードを使用して設定プロセスを完了した場合、この製品の新しいポリシーを作成する必要はありません。

   複数の管理サーバーと管理グループからなる階層構造が存在する場合、既定では、セカンダリ管理サーバーと子管理グループはプライマリ管理サーバーのポリシーを継承します。子グループとセカンダリ管理サーバーでの継承を強制的に適用して、上位のポリシーで指定された設定の変更を禁止することもできます。一部の設定のみを強制的に継承させたい場合は、上位のポリシーで該当する設定項目をロックできます。残りのロックされていない設定は下位のポリシーで変更できます。ポリシーの階層を作成することで、管理グループ内の管理対象デバイスを効果的に管理できます。

   実行手順の説明：ポリシーの作成

2. **ポリシーのプロファイルの作成（任意）**

   同じ管理グループ内にあるデバイスを異なるポリシー設定に従って動作させる場合には、ポリシーのプロファイルを作成します。ポリシーのプロファイルには、ポリシー設定のサブセットが指定されています。このサブセットはポリシーとともに対象デバイスに配信され、*プロファイルの有効化条件*と呼ばれる特定の条件下でポリシーを補完する機能を果たします。プロファイルに含まれるのは、管理対象デバイスでアクティブな「基本」ポリシーとは異なる設定（差分）のみです。

   プロファイルの有効化条件を使用することで、たとえば、特定のハードウェア設定のデバイス、特定のタグが付与されているデバイスなどの条件に応じて異なるポリシープロファイルを適用できます。タグを使用すると特定の基準を満たすデバイスをフィルタリングできます。たとえば、「*CentOS*」というタグを作成し、CentOS オペレーティングシステムを実行しているデバイスすべてにこのタグを付与し、ポリシープロファイルの有効化条件としてこのタグを指定します。これにより、CentOS を実行しているすべてのデバイスにインストールされているカスペルスキー製品は該当するポリシープロファイルで管理されます。

   実行手順の説明：

   - ポリシーのプロファイルの作成
   - ポリシーのプロファイルの有効化ルールの作成

3. **ポリシーとポリシープロファイルの管理対象デバイスへの反映**

既定では、管理サーバーは 15 分ごとに管理対象デバイスと自動的に同期します。同期中に、新しいまたは変更されたポリシーとポリシープロファイルが管理対象デバイスに反映されます。自動同期を回避して、［強制同期］コマンドを使用して手動で同期を実行できます。同期が完了すると、ポリシーとポリシープロファイルが配信され、インストールされているカスペルスキー製品に適用されます。

ポリシーとポリシーのプロファイルがデバイスに配信されたかを確認できます。Kaspersky Security Center では、デバイスのプロパティで該当する配信日時が表示されます。

実行手順の説明：強制同期

結果

デバイスベースの管理の導入手順が完了すると、ポリシーの階層を通して指定または反映された設定がカスペルスキー製品に適用されます。

管理グループに新しく追加されたデバイスには、設定された製品ポリシーとポリシープロファイルが自動的に適用されます。

ポリシーの設定と継承先への反映：ユーザーベースの管理

このセクションでは、管理対象デバイスにインストールされているカスペルスキー製品の設定をユーザーベースで一元的に行う手順について説明します。この手順を完了すると、すべての管理対象デバイスにインストールされている製品が、定義した製品ポリシーとポリシープロファイルに従って設定されます。

必須条件

手順を開始する前に、Kaspersky Security Center 管理サーバーのインストールと Kaspersky Security Center 14 Web コンソールのインストールが正常に完了しており、さらに主要な導入シナリオが完了していることを確認してください。また、ユーザーベースの管理方法の代替案もしくは追加で組み合わせて使用する管理方法としてデバイスベースのセキュリティ管理も検討すると有益な場合があります。2 種類の管理方法について詳しくは、こちらのページを参照してください。

プロセス

カスペルスキー製品のユーザーベースの管理シナリオは、次の 2 つの手順からなります。

1. **製品ポリシーの設定**

   管理対象デバイスにインストールされているカスペルスキー製品ごとにポリシーを作成して、製品の設定を指定します。これらのポリシーはクライアントデバイスに反映されます。

   クイックスタートウィザードを使用してネットワークの保護を設定する場合、Kaspersky Security Center は Kaspersky Endpoint Security の既定のポリシーを作成します。このウィザードを使用して設定プロセスを完了した場合、この製品の新しいポリシーを作成する必要はありません。

   複数の管理サーバーと管理グループからなる階層構造が存在する場合、既定では、セカンダリ管理サーバーと子管理グループはプライマリ管理サーバーのポリシーを継承します。子グループとセカンダリ管理サーバーでの継承を強制的に適用して、上位のポリシーで指定された設定の変更を禁止することもできます。一部の設定のみを強制的に継承させたい場合は、上位のポリシーで該当する設定項目をロックできます。残りのロックされていない設定は下位のポリシーで変更できます。ポリシーの階層を作成することで、管理グループ内の管理対象デバイスを効果的に管理できます。

   実行手順の説明：ポリシーの作成

2. **デバイスの所有者の指定**

管理対象デバイスを対応するユーザーに割り当てます。

実行手順の説明：デバイスの所有者ユーザーの指定

3. **組織内の主なユーザーロールの定義**

組織内の従業員が行う様々な業務の主要なものを検討します。すべての従業員がロールに従って振り分けられるようにする必要があります。たとえば、所属部門、職務内容、役職などで振り分けを行うことができます。この検討が完了したら、各グループに対応するユーザーロールを作成する必要があります。各ユーザーロールには、そのロールに固有の製品設定を含む独自のポリシープロファイルが割り当てられることを念頭において作業してください。

4. **ユーザーロールの作成**

前の手順で定義した従業員のグループごとにユーザーロールの作成と設定を行うか、あるいは事前定義されたユーザーロールを使用します。ユーザーロールには製品の各機能に対するアクセス権限が組み合わされたかたちで付与されます。

実行手順の説明：ユーザーロールの作成

5. **各ユーザーロールの対象範囲の指定**

作成したユーザーロールごとに、ロールを割り当てるユーザーやセキュリティグループ、管理グループを指定します。ユーザーロールと関連付けられた設定は、ロールに関連付けられたグループ（子グループを含む）にデバイスが属し、なおかつそのロールを割り当てられたユーザーが所有しているデバイスのみに適用されます。

実行手順の説明：各ユーザーロールの対象範囲の編集

6. **ポリシーのプロファイルの作成**

組織内のユーザーロールごとに、ポリシープロファイルを作成します。ポリシープロファイルによって、ユーザーのデバイスにインストールされている製品にユーザーロールに応じてどの設定が適用されるかが定義されます。

実行手順の説明：ポリシープロファイルの作成

7. **ポリシープロファイルとユーザーロールの関連付け**

作成したポリシープロファイルをユーザーロールに関連付けます。完了すると、指定されたロールを割り当てられたユーザーに対してポリシープロファイルが有効になります。ユーザーのデバイスにインストールされているカスペルスキー製品に、ポリシープロファイルで指定した設定が適用されます。

実行手順の説明：ポリシーのプロファイルとロールの関連付け

8. **ポリシーとポリシープロファイルの管理対象デバイスへの反映**

既定では、Kaspersky Security Center 管理サーバーと管理対象デバイスは 15 分ごとに同期します。同期中に、新しいまたは変更されたポリシーとポリシープロファイルが管理対象デバイスに反映されます。自動同期を回避して、［強制同期］コマンドを使用して手動で同期を実行できます。同期が完了すると、ポリシーとポリシープロファイルが配信され、インストールされているカスペルスキー製品に適用されます。

ポリシーとポリシーのプロファイルがデバイスに配信されたかを確認できます。Kaspersky Security Center では、デバイスのプロパティで該当する配信日時が表示されます。

実行手順の説明：強制同期

結果

ユーザーベースの管理の導入手順が完了すると、ポリシーの階層を通して指定または反映された設定がカスペルスキー製品に適用されます。

新規ユーザーに対しては、新しいアカウントを作成して作成済みのユーザーロールのいずれかを割り当て、デバイスをユーザーに割り当てる必要があります。このユーザーのデバイスには、設定された製品ポリシーとポリシープロファイルが自動的に適用されます。

Kaspersky Endpoint Security のグループアップデートタスクの手動セットアップ

［**タスクの開始を自動的かつランダムに遅延させる**］がオンの場合、Kaspersky Endpoint Security での最適かつ推奨されるスケジュールオプションは［**新しいアップデートがリポジトリにダウンロードされ次第**］です。

ネットワークエージェントのポリシー設定

ネットワークエージェントのポリシーを設定するには：

1. メインメニューで、［**デバイス**］→［**ポリシーとプロファイル**］の順に移動します。
2. ネットワークエージェントポリシーの名前をクリックします。

   ネットワークエージェントポリシーのプロパティウィンドウが表示されます。

全般

このタブでは、ポリシーステータスを変更したり、継承ポリシーを設定したりすることができます：

- ［**ポリシーのステータス**］セクションで、ポリシーのステータスを選択します：
  - **アクティブポリシー**

    このオプションをオンにすると、ポリシーがアクティブになります。
    既定では、このオプションがオンです。

  - **非アクティブポリシー**

    このオプションをオンにすると、ポリシーは非アクティブになりますが［**ポリシー**］フォルダーに保持されます。必要に応じて、ポリシーをアクティブにすることができます。

- ［**設定の継承**］セクションでは、ポリシーの継承を設定できます。
  - **親ポリシーから設定を継承する**

    このオプションをオンにすると、ポリシーの設定値は上位レベルグループのポリシーから継承されるため、ロックされます。
    既定では、このオプションはオンです。

  - **設定を子ポリシーへ強制的に継承させる**

このオプションをオンにすると、ポリシーの変更を適用した後に次の処理が実行されます：

- 管理サブグループのポリシー（子ポリシー）に、ポリシーの設定値が継承されます。
- 各子ポリシーのプロパティウィンドウの［**全般**］セクションにある［**設定の継承**］ブロックで、［**親ポリシーから設定を継承する**］が自動的にオンになります。

このオプションをオンにすると、子ポリシーの設定はロックされます。

既定では、このオプションはオフです。

イベントの設定

このタブでは、イベントの記録と通知を設定できます。イベントは、［**イベントの設定**］タブの次のセクションの重要度に応じて配信されます：

- **機能エラー**
- **警告**
- **情報**

それぞれのセクションのリストには、イベントの種別と、管理サーバーでイベントが保存される既定の日数が表示されます。イベント種別をクリックすると、リストで選択したイベントについてのイベントログとイベント通知を設定できます。既定では、すべてのイベント種別で、管理サーバー全体を対象に指定された共通の通知設定が使用されます。しかしながら、目的のイベント種別の特定の設定を変更できます。

たとえば、［**警告**］セクションでは、［**インシデントが発生しました**］イベント種別の設定を編集できます。このようなイベントは、たとえばディストリビューションポイントのディスク空き容量が 2 GB 未満の場合などに発生します（アプリケーションのインストール、アップデートのダウンロードをリモートで実行するには、少なくとも 4 GB が必要となります）。［**インシデントが発生しました**］イベントをクリックし、発生したイベントを保存する場所とその通知方法を指定します。

ネットワークエージェントがインシデントを検出した場合は、管理対象デバイスの設定を使用してこのインシデントを管理できます。

アプリケーション設定

設定

［**設定**］セクションでは、ネットワークエージェントのポリシーを設定できます。

- **イベントキュー最大サイズを MB で指定**

  このフィールドでは、イベントキューが使用できるドライブの最大サイズを指定できます。

  既定値は 2 メガバイト（MB）です。

- **アプリケーションがポリシーの拡張データをデバイスから取得可能である**

管理対象デバイスにインストールされたネットワークエージェントは、適用されたセキュリティ製品のポリシーに関する情報をセキュリティ製品（たとえば、Kaspersky Endpoint Security for Linux）に転送します。転送された情報は、セキュリティ製品のインターフェイスで表示できます。

ネットワークエージェントは次の情報を転送します：

- 管理対象デバイスへのポリシー導入の時間
- 管理対象デバイスへポリシー導入の時点でのアクティブポリシーまたはモバイルユーザーポリシーの名前
- 管理対象デバイスへポリシー導入の時点で管理対象デバイスが含まれていた管理グループの名前とフルパス
- アクティブポリシーのプロファイルのリスト

  情報を使用して、デバイスに正しいポリシーが適用されていることを確認し、トラブルシューティングを行うことができます。既定では、このオプションはオフです。

リポジトリ

［**リポジトリ**］セクションでは、情報ネットワークエージェントから管理サーバーに詳細が送信されるオブジェクトの種別を選択できます。このセクションの設定の一部を変更することがネットワークエージェントのポリシーで禁止されている場合、それらの設定を変更することはできません。

- **インストール済みアプリケーションの詳細**

  このオプションをオンにすると、クライアントデバイスにインストールされたアプリケーションに関する情報が管理サーバーに送信されます。

  既定では、このオプションはオンです。

- **ハードウェアレジストリの詳細**

  デバイスにインストールされたネットワークエージェントから、そのデバイスのハードウェアに関する情報が管理サーバーに送信されます。ハードウェアの詳細は、デバイスのプロパティで確認できます。

ネットワーク

［**ネットワーク**］セクションには 3 つのサブセクションが含まれます：

- **接続**
- **接続プロファイル**
- **接続スケジュール**

［**接続**］サブセクションでは、管理サーバーからクライアントコンピューターへの接続を設定したり、UDP ポートの使用を有効化したり、UDP ポート番号を定義したりできます。

- ［**管理サーバーに接続**］セクションでは、管理サーバーへの接続を設定し、クライアントデバイスと管理サーバーを同期する間隔を指定できます：

- **同期間隔（分）**

  ネットワークエージェントによって管理対象デバイスと管理サーバーが同期します。同期間隔（「ハートビート」とも表記）を管理対象 10,000 台につき 15 分に設定することを推奨します。

  同期間隔が 15 分以下に設定された場合、同期は 15 分ごとに実行されます。同期間隔が 15 分以上に設定されている場合は、指定された間隔で同期が実行されます。

- **ネットワークトラフィックを圧縮する**

  このオプションをオンにすると、送信される情報量が減ることでネットワークエージェントによるデータ送信速度が向上し、これにより管理サーバーの負荷が軽減されます。

  > クライアントコンピューターの CPU の負荷は増加する可能性があります。

  既定では、このチェックボックスはオンです。

- **SSL 接続を使用**

  このオプションをオンにすると、SSL を使用してセキュアなポート経由で管理サーバーへの接続が確立されます。

  既定では、このオプションはオンです。

- **既定の接続設定でディストリビューションポイントの接続ゲートウェイを使用する（使用可能な場合）**

  このオプションをオンにすると、ディストリビューションポイントの接続ゲートウェイが、管理グループのプロパティで指定された設定で使用されます。

  既定では、このオプションはオンです。

- **UDP ポートを使用**

  UDP ポートを経由して KSN プロキシサーバーと管理対象デバイスを接続する場合は、［**UDP ポートを使用**］をオンにして、［**UDP ポート**］でポート番号を指定します。既定では、このオプションはオンです。KSN プロキシサーバーに接続する既定の UDP ポートは 15111 です。

- **UDP ポート番号**

  このフィールドに、UDP ポート番号を入力できます。既定のポート番号は 15000 です。

  レコードには 10 進法が使用されます。

［**ネットワーク**］セクションの［**接続プロファイル**］サブセクションで、ネットワークロケーションを設定したり、管理サーバーが使用できない際のモバイルユーザーモードを有効にしたりできます。［**接続プロファイル**］セクションの設定は、Windows を実行しているデバイスでのみ使用できます：

- **ネットワークロケーションの設定**

ネットワークロケーションの設定では、クライアントデバイスが接続するネットワークの特性を定義し、ネットワークの特性が変更された時にネットワークエージェントが管理サーバーの接続プロファイルを切り替えるためのルールを指定します。

- **管理サーバー接続プロファイル**

  接続プロファイルは、Windows を実行しているデバイスでのみサポートされます。使用はお勧めしません。

  ネットワークエージェントから管理サーバーへの接続のプロファイルを表示して追加することができます。次のイベントの発生時、ネットワークエージェントから別の管理サーバーに切り替えるルールを作成することもできます：

  - クライアントデバイスが別のローカルネットワークに接続した場合
  - デバイスから組織のローカルネットワークへの接続が切断した場合
  - 接続ゲートウェイアドレスまたは DNS サーバーアドレスが変更された場合

［**接続プロファイル**］設定グループでは、［**管理サーバー接続プロファイル**］に新しい項目は追加できないため、［**追加**］は無効になっています。設定済みの接続プロファイルも変更できません。

- **管理サーバーが使用できない時にモバイルユーザーモードを有効にする**

  このオプションをオンにすると、このプロファイルで接続しているクライアントデバイスにインストールされているアプリケーションは、モバイルユーザーモードおよびモバイルユーザーポリシーを使用します。モバイルユーザーポリシーがアプリケーションに対して定義されていない場合は、アクティブポリシーが使用されます。

  このオプションを無効にすると、アプリケーションはアクティブポリシーを使用します。

  既定では、このオプションはオフです。

［**接続スケジュール**］サブセクションでは、ネットワークエージェントから管理サーバーにデータを送信する時間間隔を指定できます。

- **要求時に接続**

  このオプションをオンにすると、ネットワークエージェントが管理サーバーへのデータ送信を要求された時に、接続が確立されます。

  既定では、このオプションがオンです。

- **指定の時間間隔で接続**

  このオプションをオンにすると、ネットワークエージェントは指定した時間に管理サーバーへ接続します。複数の接続時間帯を追加できます。

ディストリビューションポイント別のネットワークポーリング

［**ディストリビューションポイント別のネットワークポーリング**］セクションでは、ネットワークの自動ポーリングを設定できます。次のオプションを使用してポーリングを有効にしたり、頻度を設定できます：

- **Zeroconf**

  このオプションをオンにすると、ディストリビューションポイントは自動的にゼロコンフィギュレーションネットワーキング（「*Zeroconf*」とも表記）を使用して IPv6 ネットワークを検索します。この場合、ディストリビューションポイントはネットワーク全体を検索するため、有効な IP 範囲の検索は無視されます。

  Zeroconf の使用を開始するには、次の条件が満たされている必要があります：

  - ディストリビューションポイントが Linux を実行している必要があります。
  - ディストリビューションポイントで avahi-browse ユーティリティをインストールする必要があります。

  このオプションをオフにすると、ディストリビューションポイントは IPv6 デバイスを持つネットワークを検索しません。

  既定では、このオプションはオフです。

- **IP アドレス範囲**

  このオプションをオンにすると、［**ポーリングのスケジュールを設定する**］をクリックして設定したスケジュールに従って、管理サーバーによって IP アドレス範囲が自動的にポーリングされます。

  このオプションをオフにすると、管理サーバーは IP アドレス範囲をポーリングしません。

  ネットワークエージェントのバージョンが 10.2 より前の場合、IP アドレス範囲のポーリング頻度は、［**ポーリング間隔（分）**］で設定できます。このフィールドは、オプションをオンにすると使用可能になります。

  既定では、このオプションはオフです。

ディストリビューションポイントのネットワーク設定

［**ディストリビューションポイントのネットワーク設定**］セクションで、インターネットアクセス設定を指定できます：

- **プロキシサーバーを使用する**
- **アドレス**
- **ポート番号**
- **ローカルアドレスにプロキシサーバーを使用しない**

  このオプションをオンにすると、ローカルネットワークのデバイスへの接続にプロキシサーバーが使用されません。

  既定では、このオプションはオフです。

- **プロキシサーバー認証**

このチェックボックスをオンにすると、入力フィールドでプロキシサーバー認証の資格情報を指定できます。

既定では、このチェックボックスはオフです。

- **ユーザー名**
- **パスワード**

アップデート（ディストリビューションポイント）

［**アップデート（ディストリビューションポイント）**］セクションでは、差分ファイルのダウンロード機能を有効にすることができます。そのため、ディストリビューションポイントはカスペルスキーのアップデートサーバーから差分ファイルの形式でアップデートを取得します。

変更履歴

このタブでは、必要に応じて、ポリシーのリビジョンのリストを表示したり、ポリシーで行われた変更をロールバックすることができます。

タスク

このセクションでは、Kaspersky Security Center で使用できるタスクについて説明します。

タスクの概要

Kaspersky Security Center は、様々な*タスク*を作成して実行することにより、デバイス上にインストールされたカスペルスキー製品を管理します。アプリケーションのインストール、起動、停止、ファイルのスキャン、定義データベースやソフトウェアモジュールのアップデート、アプリケーションでのその他のタスクを実行するには、タスクが必要です。

Kaspersky Security Center 14 Web コンソールを使用してアプリケーションのタスクを作成できるのは、そのアプリケーション用の管理プラグインが Kaspersky Security Center 14 Web コンソールサーバーにインストールされている場合に限られます。

タスクは管理サーバー上とデバイス上で実行できます。

次の種別のタスクは管理サーバーで実行されます：

- レポートの自動配信
- リポジトリへのアップデートのダウンロード
- 管理サーバーデータのバックアップ
- データベースのメンテナンス

次の種別のタスクはデバイスで実行されます：

- *ローカルタスク* - 特定の 1 台のデバイスで実行されるタスク

  ローカルタスクを変更するには、管理者が Kaspersky Security Center 14 Web コンソールを使用するか、またはリモートデバイスのユーザーが実行します（たとえば、セキュリティ製品のインターフェイスを使用）。管理対象デバイスの管理者とユーザーが同時にローカルタスクを変更する場合、管理者が行う変更内容の方が優先度が高いため有効になります。

- *グループタスク* - 特定のグループに属するすべてのデバイスで実行されるタスク

  タスクのプロパティで特別な設定を行わない限り、グループタスクは選択したグループのすべてのサブグループに影響します。さらに、グループタスクは該当するグループまたはそのサブグループのいずれかに導入されている、セカンダリおよび仮想管理サーバーに接続されているデバイスにも適用されます（オプション設定による）。

- *グローバルタスク* - 管理グループに含まれるかどうかに関係なく、特定のデバイスで実行されるタスク

アプリケーションごとに、任意の数のグループタスク、グローバルタスク、ローカルタスクを作成できます。

タスクの設定に変更を加え、タスクの進行状況を表示し、タスクをコピー、エクスポート、インポート、および削除できます。

タスクは、そのタスクを作成した対象のアプリケーションが実行中である場合のみ、デバイス上で開始されます。

タスクの実行結果は、各デバイスのオペレーティングシステムのイベントログと管理サーバーのオペレーティングシステムのイベントログ、および管理データベースに保存されます。

タスクの設定には個人データを使用しないでください。たとえば、ドメイン管理者パスワードを指定することは避けてください。

タスクの対象範囲

*タスク範囲*とは、タスクが実行されるデバイスの範囲です対象範囲には次の種別があります：

- *ローカルタスク*の対象範囲は、そのデバイス自体です。
- *管理サーバータスク*の対象範囲は、管理サーバーです。
- *グループタスク*の対象範囲は、グループに含まれているデバイスのリストです。

*グローバルタスク*の作成時に、次の方法を使用して対象範囲を指定できます：

- 特定のデバイスを手動で指定する

  デバイスのアドレスとして、IP アドレス（または IP アドレス範囲）または DNS 名を使用できます。

- 追加するデバイスのアドレスが記載されている txt ファイルからデバイスのリストをインポートする（各アドレスを独立した行に記載する必要があります）。

デバイスのリストをファイルからインポートするかまたはリストを手動で作成し、デバイスが名前によって識別される場合、リストに含めることができるのはその情報が管理サーバーのデータベースに登録済みであるデバイスのみです。データベースへの情報の入力は、デバイスの接続時、またはデバイスの検索中に実行されます。

- デバイスの抽出を指定する。

  時間の経過とともに、抽出に含まれるデバイスセットの変更に応じてタスクの範囲が変化します。デバイスの抽出は、デバイスにインストールされているソフトウェアを含むデバイス属性、およびデバイスに割り当てられているタグに基づいて作成できます。デバイスの抽出は、タスクの範囲を定義するための最も柔軟性の高い方法です。

  デバイスの抽出を対象とするタスクは常に、管理サーバーのスケジュールに基づいて実行されます。このタスクは、管理サーバーと接続されていないデバイスでは実行できません。他の方法でタスク範囲が指定されたタスクはデバイス上で直接実行されるため、デバイスと管理サーバーとの接続の有無には左右されません。

デバイスの抽出を対象とするタスクは、デバイスのローカル時間ではなく管理サーバーのローカル時間に基づいて実行されます。他の方法でタスク範囲が指定されたタスクはデバイスのローカル時間に基づいて実行されます。

タスクの作成

タスクを作成するには：

1. メインメニューで、［**デバイス**］→［**タスク**］の順に選択します。
2. ［**追加**］をクリックします。

   タスク追加ウィザードが開始されます。表示される指示に従ってください。
3. 既定のタスク設定を編集する場合、［**タスク作成の終了**］ページで、［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにします。このオプションをオフにすると、既定の設定でタスクが作成されます。既定の設定からの変更は、後からいつでも実行できます。
4. ［**終了**］をクリックします。

タスクが作成され、タスクリストに表示されます。

タスクの手動での開始

タスクは、各タスクのプロパティで指定されたスケジュール設定に従って、開始されます。タスクはいつでも手動で起動できます。

タスクを手動で開始するには：

1. メインメニューで、［**デバイス**］→［**タスク**］の順に移動します。
2. リスト内で、削除するタスクに隣接するチェックボックスをオンにします。
3. ［**開始**］をクリックします。

タスクが開始します。タスクのステータスは、［**ステータス**］列で、または［**結果**］をクリックして確認できます。

タスクリストの表示

Kaspersky Security Center Linux で作成されたタスクのリストを表示できます。

タスクのリストを表示するには：

［**デバイス**］→［**タスク**］の順に選択します。

タスクのリストが表示されます。タスクは、関連するアプリケーションの名前でグループ化されます。たとえば、*アプリケーションのリモートインストール*タスクは管理サーバーに関連付けられ、*アップデート*タスクは Kaspersky Endpoint Security for Linux に関連付けられています。

タスクのプロパティを表示するには：

タスクの名前をクリックします。

タスクのプロパティウィンドウにいくつかの名前付きタブが表示されます。たとえば、［**タスク種別**］は［**全般**］タブに、タスクスケジュールは［**スケジュール**］タブに表示されます。

タスクの全般的な設定

このセクションでは、ほとんどのタスクで表示および構成できる設定について説明します。使用可能な設定のリストは、構成しているタスクによって異なります。

タスク作成時に指定する設定

タスク作成時に次の設定を指定できます。これらの設定の一部は、作成したタスクのプロパティから変更することもできます。

- OS の再起動設定：
  - **デバイスを再起動しない**

    操作後に、クライアントデバイスは自動的には再起動されません。操作を完了するには、デバイスを再起動する必要があります（手動で、またはデバイスの管理タスクを使用して）。必要な再起動についての情報は、タスク履歴とデバイスのステータスに保存されます。このオプションは、継続的な稼働が不可欠なサーバーなどのデバイスで実行するタスクに適切です。

  - **デバイスを再起動する**

    インストールの完了に再起動が必要な場合は常に、クライアントデバイスは自動的に再起動されます。このオプションは、定期的に稼働が一時停止（シャットダウンまたは再起動）するデバイスのタスクに有用です。

- **セッションがブロックされたアプリケーションを強制終了する**

  アプリケーションを実行すると、クライアントデバイスの再起動が妨げられる場合があります。たとえば、ドキュメント作成アプリケーションでドキュメントを編集しており、その内容が保存されていない場合、アプリケーションはデバイスの再起動を許可しません。

  このオプションをオンにすると、ブロックされたデバイス上のアプリケーションが、再起動の前に強制的に閉じられます。これにより、保存していなかった作業内容が失われる場合があります。

  このオプションをオフにすると、ブロックされたデバイスは再起動されません。このデバイス上のタスクのステータスでは、デバイスの再起動が必要であることが表示されます。ブロックされたデバイスでは、実行中のアプリケーションすべてをユーザーが手動で終了し、デバイスを再起動する必要があります。

  既定では、このオプションはオフです。

- タスクスケジュールの設定：
  - **実行予定設定：**
    - **N 時間ごと**

      指定した日時から、時間単位で指定した間隔ごとにタスクを定期的に実行します。

      既定では、現在のシステム日時から、6 時間ごとにタスクが実行されます。

    - **N 日ごと**

      日単位で指定した間隔ごとにタスクを定期的に実行します。さらに、最初にタスクを実行する日時を指定できます。この詳細設定項目は、タスクを作成中の製品でこの項目の使用がサポートされている場合に利用できます。

      既定では、現在のシステム日時から、1 日ごとにタスクが実行されます。

    - **N 週間ごと**

      指定した日時から、週単位で指定した間隔ごとに、指定した曜日の指定した時刻にタスクを定期的に実行します。

      既定では、毎週、月曜日の現在のシステム時刻にタスクが実行されます。

    - **N 分ごと**

      タスク作成日の指定した時刻から、分単位で指定した間隔ごとにタスクを定期的に実行します。

      既定では、現在のシステム時刻から、30 分ごとにタスクが実行されます。

    - **毎日（サマータイムはサポートしていません）**

      日単位で指定した間隔ごとにタスクを定期的に実行します。このスケジュールではサマータイム（DST）の適用はサポートされません。つまり、サマータイムの開始または終了に伴い、時刻を 1 時間早めたまたは遅らせた場合でも、実際にタスクが開始される時刻は変化しません。

      このスケジュールの使用は推奨されません。Kaspersky Security Center Linux の旧バージョンとの後方互換性を維持するために用意されているオプションとなります。

      既定では、毎日、現在のシステム時刻にタスクが実行されます。

- **毎週**

  毎週、指定した曜日の指定した時刻にタスクを実行します。

- **曜日ごと**

  指定した曜日（複数可）の指定した時刻にタスクを定期的に実行します。
  既定では、毎週金曜日の午後 6 時にタスクが実行されます。

- **毎月**

  毎月、指定した日付の指定した時刻にタスクを定期的に実行します。
  指定した日付が存在しない月には、月の最終日にタスクを実行します。
  既定では、各月の初日の現在のシステム時刻にタスクが実行されます。

- **手動**

  タスクは、自動的には実行されません。手動でのみ開始できます。
  既定では、このオプションはオンです。

- **毎月、選択した週の指定日**

  毎月、指定した週・曜日の指定した時刻にタスクを定期的に実行します。
  既定では、月内のいかなる日付も選択されておらず、開始時刻は午後 6 時です。

- **新しいアップデートがリポジトリにダウンロードされ次第**

  アップデートのリポジトリへのダウンロードが完了すると、タスクが実行されます。たとえば、アップデートタスクのスケジュールを設定する時に、このオプションを使用すると便利です。

- **他のタスクが完了次第**

  他のタスクが完了した後に、現在のタスクを開始します。現在のタスクを実行する条件として、先に実行されるタスクの実行結果（「正常終了」または「エラー終了」）を選択できます。

- **未実行のタスクを実行する**

このオプションは、タスクの開始予定時刻にクライアントデバイスがネットワーク上で可視でない場合のタスクの処理方法を指定します。

このオプションをオンにすると、クライアントデバイスでのカスペルスキー製品の次回起動時に、タスクの開始を試行します。タスクスケジュール設定が［**手動**］、［**1回**］または［**即時**］に設定されている場合、ネットワーク上でデバイスが認識されるかデバイスがタスク範囲に追加されるすぐにタスクが開始されます。

このオプションをオフにすると、スケジュール設定されたタスクだけがクライアントデバイス上で開始され、［**手動**］、［**1回**］、および［**即時**］に設定したタスクはネットワーク上で可視になっているクライアントデバイスでのみ開始されます。そのため、たとえばリソース消費量が多いので業務時間外にのみ実行したいタスクなどで、このオプションをオフにすることが有効な場合があります

既定では、このオプションはオンです。

- **タスクの開始を自動的かつランダムに遅延させる**

  このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始され、*タスクの分散開始*を実現します。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

  分散開始の開始時刻は、タスクの作成時に自動的に計算されます。計算の結果は、タスクに割り当てられるクライアントデバイスの台数によって異なります。以降は、タスクは常に計算された開始時刻に開始されます。ただし、タスクの設定が変更されたりタスクが手動で開始された場合、計算によるタスク開始時刻は変更されます。

  このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

- **タスクの開始を次の時間範囲内でランダムに遅延させる（分）**

  このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始されます。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

  このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

  既定では、このオプションはオフです。既定の時間は1分です。

- タスクを割り当てるデバイス：

  - **ネットワークの管理サーバーによって検出されたデバイスを選択する**

    タスクを特定のデバイスに割り当てます。特定のデバイスには、管理グループに属するデバイスと管理グループが割り当てられていないデバイスの両方を含めることができます。

    たとえば、未割り当てデバイスでネットワークエージェントのインストールタスクを実行する時に、このオプションを使用すると便利です。

  - **デバイスのアドレスを手動で指定するか、リストからアドレスをインポートする**

タスクを割り当てるデバイスの DNS 名、IP アドレス、IP サブネットを指定できます。

特定のサブネットワークでタスクを実行する時に、このオプションを使用すると便利です。たとえば、経理担当者のデバイスにのみ特定のアプリケーションをインストールしたり、感染した可能性のあるサブネットワークでデバイスをスキャンする場合などです。

- **デバイスの抽出にタスクを割り当てる**

  デバイスの抽出に属するデバイスにタスクを割り当てます。既存の抽出のいずれかを選択できます。

  たとえば、特定のバージョンのオペレーティングシステムを使用しているデバイスを対象にタスクを実行する時に、このオプションを使用すると便利です。

- **管理グループにタスクを割り当てる**

  任意の管理グループに属するデバイスにタスクを割り当てます。既存のグループを指定するか、新規グループを作成できます。

  たとえば、特定の管理グループに含まれるデバイスのみが対象のメッセージをユーザーに送信する時に、このオプションを使用すると便利です。

- アカウントの設定：

  - **既定のアカウント**

    タスクを実行するアプリケーションと同じアカウントでタスクが実行されます。

    既定では、このオプションがオンです。

  - **アカウントの指定**

    ［**アカウント**］と［**パスワード**］に、タスクを実行するアカウントの情報を入力します。アカウントには、当該タスクの実行に必要な権限が付与されている必要があります。

  - **アカウント**

    タスクを実行するアカウント。

  - **パスワード**

    タスクが実行されるアカウントのパスワード。

タスク作成後に指定する設定

次の設定は、タスク作成後にのみ指定できます。

- グループタスクの設定：

  - **サブグループへ導入**

このオプションはグループタスクの設定内でのみ使用可能です。

このオプションをオンにすると、タスク範囲には次のものが含まれます：

- タスクの作成中に選択した管理グループ。
- 選択された管理グループに属する管理グループのすべてのレベルはグループ階層の下にあります。

このオプションをオフにすると、タスク範囲にはタスクの作成中に選択された管理グループのみが含まれます。

既定では、このオプションはオンです。

- **セカンダリまたは仮想管理サーバーに配信**

このオプションをオンにすると、プライマリ管理サーバーに対して有効なタスクがセカンダリ管理サーバーに対しても適用されます（仮想管理サーバーも含まれます）。同じ種別のタスクがセカンダリ管理サーバーに既に存在する場合は、既存のタスクとプライマリ管理サーバーから継承した両方のタスクがセカンダリ管理サーバーに適用されます。

このオプションは［**サブグループへ導入**］がオンになっている場合にのみ使用可能です。

既定では、このオプションはオフです。

- スケジュールの詳細設定
  - **Wake on LAN の機能を使用してタスク開始前にデバイスを起動する（分）**

タスク開始よりも指定した時間だけ前に、デバイス上のオペレーティングシステムが起動します。既定では、時間は 5 分です。

タスクの開始予定時刻が近づいても電源がオフだったデバイスも含めて、タスク範囲に含まれるすべてのクライアントデバイスでタスクを実行するには、このオプションをオンにします。

タスクの完了後にデバイスの電源を自動的にオフにする場合は、［**タスク完了後にデバイスをシャットダウンする**］を有効にします。このオプションは同じウィンドウ内にあります。

既定では、このオプションはオフです。

  - **タスクの完了後にデバイスの電源を切る**

たとえば、毎週金曜日の業務時間終了後にクライアントデバイスへのアップデートのインストールを行い、その後デバイスの電源を切りたい時に、アップデートインストールタスクでこのオプションを使用できます。

既定では、このオプションはオフです。

  - **実行時間が次を超える場合はタスクを停止する（分）**

指定した時間が経過すると、タスクが完了したかどうかに関係なくタスクが自動的に停止します。

実行に時間がかかり過ぎているタスクを中断したい時に、このオプションを使用します。

既定では、このオプションはオフです。既定のタスク実行時間は 120 分です。

- 通知の設定：

- ［**タスク履歴の保存**］セクション：
  - **管理サーバーのデータベースに保存（日）**

    タスク範囲に含まれるすべてのクライアントデバイスでのタスク実行に関するアプリケーションイベントが、指定した日数の間、管理サーバーに保存されます。この期間が過ぎると、情報が管理サーバーから削除されます。

    既定では、このオプションはオンです。

  - **デバイスの OS イベントログに保存**

    タスク実行に関するアプリケーションイベントが、各クライアントデバイスの Syslog イベントログにローカルで保存されます。

    既定では、このオプションはオフです。

  - **管理サーバーの OS イベントログに保存**

    タスク範囲に含まれるすべてのクライアントデバイスでのタスク実行に関するアプリケーションイベントが、管理サーバーのオペレーティングシステムの Syslog イベントログに一元的に保存されます。

    既定では、このオプションはオフです。

  - **すべてのイベントを保存**

    このオプションをオンにすると、タスクに関するすべてのイベントがイベントログに保存されます。

  - **タスクの進捗に関連したイベントを保存**

    このオプションをオンにすると、タスク実行に関するイベントのみがイベントログに保存されます。

  - **タスク実行結果のみ保存**

    このオプションをオンにすると、タスクの実行結果に関するイベントのみがイベントログに保存されます。

- **管理者にタスク実行結果を通知**

  管理者がタスク実行結果の通知を受け取る方法を、メール、SMS、実行ファイルの実行から選択できます。通知を設定するには、［**設定**］をクリックします。

  既定では、すべての通知方法がオフです。

- **エラーのみ通知**

このオプションをオンにすると、管理者はタスクでエラーが発生して終了した場合にのみ通知を受け取ります。

このオプションをオフにすると、管理者はタスク終了時に常に通知を受け取ります。

既定では、このオプションはオンです。

- セキュリティ設定
- タスク範囲の設定
  タスク範囲の指定方法に応じて、次の設定が表示されます：
  - **デバイス**

    タスク範囲が管理グループを使用して指定されている場合、該当するグループを表示できます。ここでは、設定を変更することはできません。ただし、［**タスク範囲からの除外**］を設定できます。

    タスク範囲がデバイスのリストを使用して指定されている場合、デバイスを追加したり削除してこのリストを変更できます。

  - **デバイスの抽出**

    タスクが適用されるデバイスの抽出を変更できます。

  - **タスク範囲からの除外**

    タスクを適用しないデバイスのグループを指定できます。タスク範囲から除外できるのは、タスクが適用されない管理グループのサブグループのみです。

- **変更履歴**

タスクのパスワード変更ウィザードの起動

非ローカルタスクの場合、タスクを実行するアカウントを指定できます。アカウントは、タスクの作成時または既存のタスクのプロパティで指定できます。指定されたアカウントが組織のセキュリティ指示に従って使用されている場合、その指示によってアカウントパスワードの変更が必要になる場合があります。アカウントパスワードの有効期限が切れて新しいパスワードを設定すると、タスクプロパティで新しい有効なパスワードを指定するまで、タスクを開始しません。

タスクのパスワード変更ウィザードを使用すると、アカウントが指定されているすべてのタスクで、古いパスワードを新しいパスワードに自動的に置換できます。または、各タスクのプロパティで、このパスワードを手動で変更できます。

タスクのパスワード変更ウィザードを起動するには：

1. ［**デバイス**］タブで、［**タスク**］を選択します。
2. ［**タスク開始に使用するアカウントの資格情報の管理**］をクリックします。

   ウィザードの指示に従ってください。

ステップ 1.資格情報の指定

システムで現在有効な新しい証明書を指定します。ウィザードの次のステップに進むと、指定されたアカウント名が、非ローカルタスクそれぞれのプロパティのアカウント名と一致するかどうか確認されます。アカウント名が一致すると、タスクのプロパティのパスワードは自動的に新しいものに置換されます。

新しいアカウントを指定するには、オプションを選択します：

- **現在のアカウントを使用**

  ウィザードは、Kaspersky Security Center 14 Web コンソールに現在サインインしているアカウントの名前を使用します。次に、［**タスクで使用する現在のパスワード**］で、アカウントのパスワードを手動で指定します。

- **別のアカウントを指定**

  タスクを起動する必要があるアカウントの名前を指定します。次に、［**タスクで使用する現在のパスワード**］で、アカウントのパスワードを指定します。

［**以前のパスワード（任意。現在のパスワードに置換したい場合に使用）**］フィールドに手動で入力した場合、アカウント名と古いパスワードの両方が見つかったタスクの、パスワードのみが置換されます。置換は自動で実行されます。その他の場合はすべて、ウィザードの次の手順で、実行する処理を選択する必要があります。

ステップ 2.実行する処理の選択

ウィザードの最初の手順で古いパスワードを指定しなかった場合、または指定した古いパスワードがタスクのプロパティのパスワードと一致しない場合、見つかったタスクに対して実行する処理を選択する必要があります。

タスクに対する処理を選択するには：

1. 処理を選択するタスクに隣接するチェックボックスをオンにします。
2. 次のいずれかを実行します：
   - タスクのプロパティのパスワードを削除するには、［**資格情報の削除**］をクリックします。
     タスクは既定のアカウントで実行されるように切り替わります。
   - パスワードを新しいパスワードに置換するには、［**古いパスワードが正しくないか未入力の場合でもパスワードの変更を強制する**］をクリックします。
   - パスワードの変更をキャンセルするには、［**処理が選択されていません**］をクリックします。

ウィザードの次のステップに移動すると、選択した処理が適用されます。

ステップ 3.結果の表示

ウィザードの最後のステップで、見つかった各タスクの結果を表示します。ウィザードを終了するには、［**終了**］をクリックします。

管理サーバーに保存されているタスク実行結果の確認

Kaspersky Security Center Linux では、グループタスク、特定のデバイスに対するタスク、管理サーバータスクの実行結果を確認できます。ローカルタスクの実行結果は表示できません。

タスク結果を表示するには：

1. タスクのプロパティウィンドウで［**全般**］セクションを選択します。
2. ［**履歴**］をクリックして、［**タスク履歴**］ウィンドウを開きます。

クライアントデバイスの管理

このセクションでは、管理グループ内のデバイスを管理する方法について説明します。

管理対象デバイスの設定

管理対象デバイスの設定を表示するには：

1. ［**デバイス**］→［**管理対象デバイス**］の順に選択します。
   管理対象デバイスのリストが表示されます。
2. 管理対象デバイスのリストで、目的のデバイス名のリンクをクリックします。

選択したデバイスのプロパティウィンドウが表示されます。

全般

［**全般**］セクションには、クライアントデバイスに関する全般的な情報が表示されます。情報は、クライアントデバイスと管理サーバーとの前回の同期中に受信されたデータに基づいて提供されます：

- **名前**

  このフィールドでは、管理グループ内のクライアントデバイスの名前を表示したり変更したりできます。

- **説明**

このフィールドでは、クライアントデバイスの補足的な説明を入力できます。

- **グループ**

  クライアントデバイスが属する管理グループ。

- **前回のアップデート**

  定義データベースまたはアプリケーションをデバイス上で前回アップデートした日付。

- **前回の可視**

  デバイスが前回ネットワークで検出された日時。

- **管理サーバーへの接続**

  クライアントデバイスにインストールされたネットワークエージェントが管理サーバーに最後に接続した日時。

- **管理サーバーから切断しない**

  このオプションをオンにすると、管理対象デバイスと管理サーバー間の継続的な接続が維持されます。このような接続を提供するプッシュサーバーを使用していない場合は、このオプションを使用することをお勧めします。

  このオプションがオフで、プッシュサーバーが使用されていない場合、管理対象デバイスは、データの同期または情報の送信のためにのみ管理サーバーに接続します。

  ［**管理サーバーから切断しない**］をオンにできるデバイスの合計数の上限は 300 です。

  このオプションは、管理対象デバイスでは既定でオフになっています。このオプションは、管理サーバーがインストールされているデバイスでは既定でオンになっており、オフにしようとしてもオンのままになります。

ネットワーク

［**ネットワーク**］セクションには、クライアントデバイスのネットワークプロパティに関する次の情報が表示されます：

- **IP アドレス**

  デバイスの IP アドレス。

- **Windows ドメイン**

  デバイスを含むワークグループ。

- **DNS 名**

クライアントデバイスの DNS ドメイン名。

- **NetBIOS 名**

  クライアントデバイスの名前。

システム

［**システム**］セクションには、クライアントデバイスにインストールされているオペレーティングシステムに関する情報が表示されます。

プロテクション

［**プロテクション**］セクションには、クライアントデバイスにおけるアンチウイルスによる保護に関する現在のステータスが表示されます：

- **デバイスのステータス**

  管理者によって定義された基準に基づいて、デバイス上のアンチウイルスによる保護のステータスとデバイスのネットワーク動作に対して割り当てられたクライアントデバイスのステータス。

- **すべての問題**

  この表には、クライアントデバイスにインストールされた管理対象アプリケーションで検知されたすべての問題のリストが表示されます。問題ごとに、アプリケーションがデバイスへの割り当てを推奨するステータスも表示されます。

- **リアルタイム保護**

  クライアントデバイスのリアルタイム保護に関する現在のステータスが表示されます。

  デバイスのステータスに変更があると、新しいステータスは、クライアントデバイスと管理サーバーが同期された後にのみデバイスのプロパティウィンドウに表示されます。

- **前回のオンデマンドスキャン**

  クライアントデバイスで前回のマルウェアスキャンが実行された日時。

- **検知した脅威の数**

  アンチウイルス製品のインストール後（最初のスキャンの場合）またはウイルスカウンターを前回リセットした後に、クライアントデバイスで検知された脅威の合計数。

- **アクティブな脅威**

クライアントデバイスにおける未処理ファイルの数。
このフィールドは、モバイルデバイス上の未処理ファイルの数をスキップします。

デバイスのステータスが製品によって定義済み

［**デバイスのステータスが製品によって定義済み**］セクションには、デバイスにインストールされている管理対象アプリケーションによって定義されたデバイスのステータスに関する情報が表示されます。このデバイスのステータスは、Kaspersky Security Center Linux によって定義されたものとは異なる場合があります。

アプリケーション

［**アプリケーション**］セクションには、クライアントデバイスにインストールされているすべてのカスペルスキー製品のリストが表示されます。アプリケーション名をクリックすると、アプリケーションに関する一般情報、デバイスで発生したイベントのリスト、およびアプリケーション設定が表示されます。

アクティブなポリシーとポリシーのプロファイル

［**アクティブなポリシーとポリシーのプロファイル**］セクションには、管理対象デバイスで現在アクティブなポリシーとポリシーのプロファイルが一覧表示されます。

タスク

［**タスク**］タブでは、既存タスクのリストの表示、新規タスクの作成、タスクの削除、タスクの開始と停止、タスク設定の変更、実行結果の表示など、クライアントデバイスのタスクを管理できます。タスクのリストは、管理サーバーとの前回のクライアント同期セッション中に受信されたデータに基づいて提供されます。管理サーバーは、タスクステータスに関する情報をクライアントデバイスに要求します。接続に失敗すると、ステータスは表示されません。

イベント

［**イベント**］タブでは、選択したクライアントデバイスについて管理サーバーに記録されたイベントが表示されます。

タグ

［**タグ**］タブでは、クライアントデバイスの検索に使用されるキーワードのリストを管理できます。また、既存のタグのリストの表示、リストからのタグの割り当て、自動タグ付けルールの設定、新規タグの追加、既存のタグの名称変更、タグの削除なども可能です。

実行ファイル

［**実行ファイル**］セクションには、クライアントデバイスにある実行ファイルが表示されます。

ディストリビューションポイント

このセクションでは、デバイスがインタラクトするディストリビューションポイントのリストについて説明します。

- **ファイルへのエクスポート**

  ［**ファイルへのエクスポート**］をクリックすると、デバイスがインタラクトするディストリビューションポイントのリストがファイルに保存されます。既定では、デバイスのリストは CSV ファイルにエクスポートされます。

- **プロパティ**

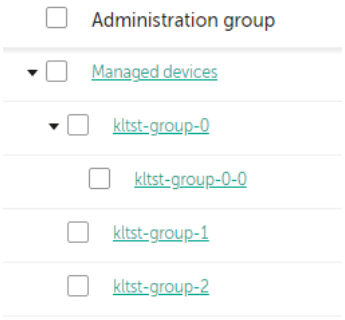
  ［**プロパティ**］をクリックすると、デバイスがインタラクトするディストリビューションポイントが表示および設定されます。

ハードウェアレジストリ

［**ハードウェアレジストリ**］セクションでは、クライアントデバイスで使用されているハードウェアに関する情報を表示できます。

管理グループの作成

Kaspersky Security Center のインストール直後に、［**管理対象デバイス**］と呼ばれる管理グループが 1 つだけ管理グループの階層に含まれます。管理グループの階層の作成時に、仮想マシンおよびデバイスを［**管理対象デバイス**］グループに追加したり、ネストされたグループを追加したりできます。



管理グループ階層の表示

管理グループを作成するには：

1. ［**デバイス**］→［**グループ階層構造**］の順に選択します。
2. 管理グループの構成で、新しい管理グループを含める管理グループを選択します。
3. ［**追加**］をクリックします。
4. 表示される［**新しい管理グループの名前**］ウィンドウで、グループの名前を入力して［**追加**］をクリックします。

   指定した名前の新しい管理グループが管理グループの階層に表示されます。

管理グループの構造を作成するには：

1. ［**デバイス**］→［**グループ階層構造**］の順に選択します。

2. ［**インポート**］をクリックします。

新規管理グループ構造作成ウィザードが開始します。ウィザードの指示に従ってください。

デバイス移動ルール

*デバイス移動ルール*を使用して、管理グループにデバイスへの割り当てを自動化することを推奨します。デバイス移動ルールは、3 つのメイン部分から構成されます。それは、名前、実行条件（デバイス属性を使用した論理式）、および対象管理グループです。デバイス属性がルールの実行条件を満たしている場合は、このルールによりデバイスが対象管理グループに移動されます。

デバイス移動ルールにはすべて優先度が設定されています。管理サーバーは優先度の昇順に従って、デバイス属性が各ルールの実行条件を満たしているかどうかを確認します。デバイス属性がルールの実行条件を満たしている場合、そのデバイスは対象グループに移動され、このデバイスに対するルール処理が完了します。デバイス属性が複数のルールの条件を満たしている場合、そのデバイスは優先度が最も高いルールの対象グループに移動されます（つまり、ルールのリスト内で最高ランク）。

デバイス移動ルールは暗黙的に作成できます。たとえば、インストールパッケージまたはリモートインストールタスクのプロパティで、ネットワークエージェントをデバイスにインストールした後にそのデバイス移動先の管理グループを指定できます。さらに、［**デバイス**］→［**移動ルール**］セクションで Kaspersky Security Center Linux の管理者が、デバイス移動ルールを明示的に作成できます。

既定では、デバイス移動ルールは、管理グループに対してデバイスを最初にワンタイムで割り当てることを目的としています。このルールにより、［未割り当てデバイス］グループから一度だけデバイスが移動されます。デバイスがこのルールによって一度移動されている場合は、デバイスを手動で［未割り当てデバイス］グループに戻したとしても、このデバイスが再度移動されることはありません。これは移動ルールを適用する際に推奨される方法です。

一部の管理グループに割り当て済みであるデバイスを移動できます。これを実行するには、ルールのプロパティで［**どの管理グループにも属していないデバイスのみ移動する**］をオフにします。

一部の管理グループに割り当て済みのデバイスに対して移動ルールを適用すると、管理サーバーの負荷が大幅に増大します。

単一のデバイスに繰り返し適用される移動ルールを作成することができます。

単一のデバイスをあるグループから別のグループに繰り返し移動させないでください（たとえば、該当するデバイスに特別なポリシーを適用するために、特別なグループタスクを実行するか、または特定のディストリビューションポイントを使用してデバイスをアップデートする）。

このような処理は、管理サーバーとネットワークのトラフィックの負荷を極端に増大させるため、サポートされていません。また、Kaspersky Security Center Linux の操作原理と競合する可能性もあります（特に、アクセス権限、イベント、レポートの分野において）。ポリシーのプロファイル、デバイス抽出のタスク、標準シナリオに従ったネットワークエージェントの割り当てなどを使用して、別のソリューションを見つける必要があります。

デバイス移動ルールの作成

デバイスを自動的に管理グループに割り当てるデバイス移動ルールを設定できます。

移動ルールを作成するには：

1. メインメニューで、［**デバイス**］→［**移動ルール**］タブの順に選択します。
2. ［**追加**］をクリックします。
3. 表示されたウィンドウの［**全般**］タブで、次の情報を指定します：

- **ルール名**

  新しいルールの名前を入力します。
  ルールのコピー時には、新しいルールでは、元のルールと同じ名前に「(1)」のようなインデックス「(数字)」が追加されます。

- **管理グループ**

  デバイスを自動的に移動する移動先の管理グループを選択します。

- **ルールの適用**

  次の中からいずれかを選択できます：
  - 各デバイスにつき1回
    指定した条件に合致するデバイスで各デバイスにつき1回だけルールが適用されます。
  - 各デバイスで1度実行、以降はネットワークエージェントの再インストールごとに実行
    指定した条件に合致するデバイスで各デバイスにつき1回ルールが適用され、その後はデバイスにネットワークエージェントが再インストールされた場合にのみ適用されます。
  - ルールを永続的に適用
    管理サーバーで自動的に設定されるスケジュールに従ってルールが適用されます（通常は数時間ごと）。

- **どの管理グループにも属していないデバイスのみ移動する**

  このオプションをオンにすると、未割り当てデバイスのみが選択したグループに移動します。
  このオプションをオフにすると、既に管理グループに割り当てられているデバイスと未割り当てデバイスの両方が選択したグループに移動します。

- **ルールを有効にする**

  このオプションをオンにすると、ルールの保存後にルールが有効になり適用されます。
  このオプションをオフにすると、ルールは作成されますがオフの状態です。このオプションをオンにするまで、ルールは適用されません。

4. ［**ルールの条件**］タブで、デバイスを管理グループに移動する基準を少なくとも1つ指定します。
5. ［**保存**］をクリックします。

移動ルールが作成されます。新しいルールが移動ルールのリストに表示されます。

リストでの順位が高いほど、ルールの優先度が高くなります。移動ルールの優先度を上げたり下げたりするには、マウスを使用してルールをリスト内でそれぞれ上下に移動します。

デバイス属性が複数のルールの条件を満たしている場合、そのデバイスは優先度が最も高いルールの対象グループに移動されます（つまり、ルールのリスト内で最高ランク）。

デバイス移動ルールのコピー

異なる管理グループで同一のルールを使用する場合などに、移動ルールをコピーできます。

既存の移動ルールをコピーするには：

1. メインメニューで、［**デバイス**］→［**移動ルール**］タブの順に選択します。

   また、［**検出と製品の導入**］→［**導入と割り当て**］の順に選択し、メニューで［**移動ルール**］を選択することもできます。

   移動ルールのリストが表示されます。

2. コピーするルールに隣接するチェックボックスをオンにします。

3. ［**コピー**］をクリックします。

4. 表示されるウィンドウで、必要に応じて［**全般**］タブで次の情報を変更します。ただし、設定を変更せずにルールのコピーのみを行う場合は、設定を変更する必要はありません：

   - **ルール名**

     新しいルールの名前を入力します。

     ルールのコピー時には、新しいルールでは、元のルールと同じ名前に「(1)」のようなインデックス「(数字)」が追加されます。

   - **管理グループ**

     デバイスを自動的に移動する移動先の管理グループを選択します。

   - **ルールの適用**

次の中からいずれかを選択できます：

- 各デバイスにつき1回

  指定した条件に合致するデバイスで各デバイスにつき1回だけルールが適用されます。

- 各デバイスで1度実行、以降はネットワークエージェントの再インストールごとに実行

  指定した条件に合致するデバイスで各デバイスにつき1回ルールが適用され、その後はデバイスにネットワークエージェントが再インストールされた場合にのみ適用されます。

- ルールを永続的に適用

  管理サーバーで自動的に設定されるスケジュールに従ってルールが適用されます（通常は数時間ごと）。

- **どの管理グループにも属していないデバイスのみ移動する**

  このオプションをオンにすると、未割り当てデバイスのみが選択したグループに移動します。

  このオプションをオフにすると、既に管理グループに割り当てられているデバイスと未割り当てデバイスの両方が選択したグループに移動します。

- **ルールを有効にする**

  このオプションをオンにすると、ルールの保存後にルールが有効になり適用されます。

  このオプションをオフにすると、ルールは作成されますがオフの状態です。このオプションをオンにするまで、ルールは適用されません。

5. ［**ルールの条件**］タブで、自動的に移動するデバイスの基準を少なくとも1つ指定します。
6. ［**保存**］をクリックします。

新しい移動ルールが作成されます。新しいルールが移動ルールのリストに表示されます。

デバイス移動ルールの条件

クライアントデバイスを管理グループに移動するルールを作成またはコピーする場合、［**ルールの条件**］タブで、デバイスを移動するための条件を設定します。次の基準に従って、移動するデバイスを決定できます：

- クライアントデバイスに割り当てられたタグ。
- ネットワークパラメータ。たとえば、指定した範囲の IP アドレスを持つデバイスを移動することができます。
- ネットワークエージェントや管理サーバーなど、クライアントデバイスにインストールされた管理対象アプリケーション。
- クライアントデバイスである仮想マシン。

以下では、デバイス移動ルールにこの情報を指定する方法について説明します。

ルールに複数の条件を指定すると、AND 論理演算子が機能し、すべての条件が同時に適用されます。オプションを何も選択しない場合や、一部のフィールドを空白のままにした場合には、そのような条件は適用されません。

［タグ］タブ

このタブでは、クライアントデバイスの説明に追加済みのデバイスタグに基づいてデバイス移動ルールを設定できます。このためには、必要なタグを選択します。また、次のオプションをオンにすることもできます：

- **指定したタグのないデバイスに適用する**

  このオプションをオンにすると、指定したタグを持つすべてのデバイスがデバイス移動ルールから除外されます。このオプションをオフにすると、選択したすべてのタグを持つデバイスにデバイス移動ルールが適用されます。

  既定では、このオプションはオフです。

- **少なくとも 1 個のタグが一致する場合に適用する**

  このオプションをオンにすると、選択したタグを少なくとも 1 個持つクライアントデバイスにデバイス移動ルールが適用されます。このオプションをオフにすると、選択したすべてのタグを持つデバイスにデバイス移動ルールが適用されます。

  既定では、このオプションはオフです。

［ネットワーク］タブ

このタブでは、デバイス移動ルールで考慮するデバイスのネットワークデータを指定できます：

- **デバイスの DNS 名**

  移動するクライアントデバイスの DNS ドメイン名。ネットワークに DNS サーバーが含まれている場合は、このフィールドに入力します。

  Kaspersky Security Center で使用するデータベースに大文字と小文字を区別する照合が設定されている場合は、デバイスの DNS 名の指定時に大文字と小文字を区別してください。そうしないと、デバイス移動ルールは機能しません。

- **DNS ドメイン**

  デバイス移動ルールは、指定されたメイン DNS サフィックスに含まれるすべてのデバイスに適用されます。ネットワークに DNS サーバーが含まれている場合は、このフィールドに入力します。

- **IP アドレス範囲**

  このオプションをオンにすると、検索されるデバイスが属する IP アドレス範囲の最初と最後の IP アドレスを入力できます。

  既定では、このオプションはオフです。

- **管理サーバー接続用 IP アドレス**

  このオプションを有効にすると、クライアントデバイスを管理サーバーに接続するための IP アドレスを設定できます。これを行うには、必要なすべての IP アドレスが含まれる IP 範囲を指定します。

  既定では、このオプションはオフです。

- **接続プロファイルが変更されました**

  次のいずれかの値を選択します：

  - **はい**デバイス移動ルールは、接続プロファイルが変更されたクライアントデバイスにのみ適用されます。
  - **いいえ**：デバイス移動ルールは、接続プロファイルが変更されていないクライアントデバイスにのみ適用されます。
  - **値を選択しない**：条件は当てはまりません。

- **別の管理サーバーの管理対象**

  次のいずれかの値を選択します：

  - **はい**デバイス移動ルールは、他の管理サーバーによって管理されているクライアントデバイスにのみ適用されます。これらのサーバーは、デバイス移動ルールを設定するサーバーとは異なります。
  - **いいえ**：デバイス移動ルールは、現在の管理サーバーによって管理されているクライアントデバイスにのみ適用されます。
  - **値を選択しない**：条件は当てはまりません。

［アプリケーション］タブ

このタブでは、クライアントデバイスにインストールされている管理対象アプリケーションとオペレーティングシステムに基づいてデバイス移動ルールを設定できます：

- **ネットワークエージェントがインストールされています**

  次のいずれかの値を選択します：

  - **はい**デバイス移動ルールは、ネットワークエージェントがインストールされたクライアントデバイスにのみ適用されます。
  - **いいえ**：デバイス移動ルールは、ネットワークエージェントがインストールされていないクライアントデバイスにのみ適用されます。
  - **値を選択しない**：条件は当てはまりません。

- **アプリケーション**

クライアントデバイスにインストールされている必要がある管理対象アプリケーションを指定して、デバイス移動ルールがこれらのデバイスに適用されるようにします。たとえば、**Kaspersky Security Center 14 ネットワークエージェント** や **Kaspersky Security Center 14 管理サーバー** を選択できます。

管理対象アプリケーションを選択しない場合、条件は適用されません。

- **OS のバージョン**

  オペレーティングシステムのバージョンに基づいてクライアントデバイスを選別できます。この目的のために、クライアントデバイスにインストールされている必要があるオペレーティングシステムを指定します。その結果、選択したオペレーティングシステムがインストールされたクライアントデバイスにデバイス移動ルールが適用されます。

  このオプションを有効にしない場合、条件は適用されません。既定では、このオプションはオフです。

- **OS のビット数**

  オペレーティングシステムのビットサイズによってクライアントデバイスを選別できます。［**OS のビット数**］フィールドで、次のいずれかの値を選択できます：

  - **不明**
  - **x86**
  - **AMD64**
  - **IA64**

  クライアントデバイスのオペレーティングシステムのビットサイズを確認するには：

  1. メインメニューで、［**デバイス**］→［**管理対象デバイス**］セクションの順に選択します。
  2. 右側にある［**列の設定**］（ ）をクリックします。
  3. ［**OS のビット数**］オプションを選択し、［**保存**］ボタンをクリックします。

     その後、管理対象デバイスごとにオペレーティングシステムのビットサイズが表示されます。

- **OS サービスパックのバージョン**

  このフィールドでは、オペレーティングシステムのパッケージバージョンを「*X.Y*」形式で指定できます。これによって、デバイスに対する移動ルールの適用方法が決定されます。既定では、バージョンの値は指定されていません。

- **ユーザー証明書**

次のいずれかの値を選択します：

- **インストール済み**：デバイス移動ルールは、モバイル証明書を持つモバイルデバイスにのみ適用されます。
- **未インストール**：デバイス移動ルールは、モバイル証明書のないモバイルデバイスにのみ適用されます。
- **値を選択しない**：条件は当てはまりません。

- **OS のビルド**

この設定は Windows オペレーティングシステムにのみ適用できます。

選択したオペレーティングシステムのビルド番号が、入力したビルド番号と「等しい」「それより古い」「それより新しい」かを指定して検索できます。また、指定したビルド番号を除くすべてのビルド番号に対してデバイス移動ルールを設定することもできます。

- **OS のリリース番号**

この設定は Windows オペレーティングシステムにのみ適用できます。

選択したオペレーティングシステムのリリース ID が、入力したリリース番号と「等しい」「それより古い」「それより新しい」かを指定して検索できます。また、指定したリリース番号を除くすべてのリリース番号に対してデバイス移動ルールを設定することもできます。

［仮想マシン］タブ

このタブでは、クライアントデバイスが仮想マシンであるか仮想デスクトップインフラストラクチャ（VDI）の一部であるかに応じて、デバイス移動ルールを設定できます：

- **仮想マシン**

このドロップダウンリストで、次のいずれかのオプションを選択できます：

- **該当なし**：条件は当てはまりません。
- **いいえ**：仮想マシンでないデバイスを移動します。
- **はい**仮想マシンであるデバイスを移動します。

- **仮想マシンの種別**
- **仮想デスクトップインフラストラクチャの一部**

このドロップダウンリストで、次のいずれかのオプションを選択できます：

- **該当なし**：条件は当てはまりません。
- **いいえ**：VDI の一部ではないデバイスを移動します。
- **はい**VDI を構成するデバイスを移動します。

デバイスを管理グループへ手動で追加

デバイス移動ルールを作成してデバイスを管理グループに自動的に移動したり、選択した管理グループにデバイスを追加することで、デバイスを管理グループ間で手動で移動したりすることができます。このセクションでは、デバイスを管理グループに手動で追加する手順を説明します。

特定の管理グループに 1 台以上のデバイスを手動で追加するには：

1. ［**デバイス**］ - ［**管理対象デバイス**］の順に選択します。
2. リストの上にある［**現在のパス：**<現在のパス>］をクリックします。
3. 表示されるウィンドウで、デバイスを追加する管理グループを選択します。
4. ［**デバイスの追加**］をクリックします。
   デバイス移動ウィザードが起動します。
5. 管理グループに追加するデバイスのリストを作成します。

   デバイスへの接続時に、またはデバイスの検出後に、管理サーバーのデータベースに既に情報が追加されているデバイスのみを追加できます。

   デバイスをリストに追加する方法を選択します：

   - ［**デバイスの追加**］をクリックして、次のいずれかの方法でデバイスを指定します：
     - 管理サーバーによって検出されたデバイスのリストからデバイスを選択します。
     - デバイスの IP アドレスまたは IP アドレス範囲を指定します。
     - デバイスの DNS 名を指定します。

       デバイス名のフィールドには、空白文字、バックスペース、および禁止されている文字（, \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %）を含めることはできません。

   - ［**デバイスをファイルからインポート**］をクリックして、テキストファイルからデバイスのリストをインポートします。各デバイスのアドレスまたは名前をそれぞれの行に指定する必要があります。

ファイルには、空白文字、バックスペース、および禁止されている文字（, \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %）を含めることはできません。

6. 管理グループに追加するデバイスのリストを表示します。デバイスを追加または削除することでリストを編集できます。

7. リストが正しいことを確認したら、［**次へ**］をクリックします。

ウィザードによってデバイスリストが処理され、結果が表示されます。正常に処理されたデバイスが管理グループに追加され、管理サーバーによって作成された名前でデバイスのリストに表示されます。

管理グループへの手動でのデバイスの移動

管理グループ間で、または未割り当てデバイスのグループから管理グループにデバイスを移動できます。

特定の管理グループに1台以上のデバイスを移動するには：

1. デバイスの移動元の管理グループを開きます。開くには、次のいずれかの操作を行います：

   - 管理グループを開くには、［**デバイス**］→［**管理対象デバイス**］の順に移動し、［**現在のパス**］フィールドのパスリンクをクリックして、開いた左側のペインで管理グループを選択します。
   - ［**未割り当てデバイス**］グループを開くには、［**検出と製品の導入**］→［**未割り当てデバイス**］の順に選択します。

2. 別のグループに移動するデバイスに隣接するチェックボックスをオンにします。

3. ［**グループへ移動**］をクリックします。

4. 管理グループの階層で、選択したデバイスの移動先の管理グループに隣接するチェックボックスをオンにします。

5. ［**移動**］をクリックします。

選択したデバイスが、選択した管理グループに移動します。

クライアントデバイスの管理サーバーの変更

特定のクライアントデバイスの管理サーバーを別のものに変更することができます。このためには、［*管理サーバーの変更*］タスクを使用します。

クライアントデバイスを管理する管理サーバーを別のサーバーに変更するには：

1. デバイスを管理する管理サーバーに接続します。

2. 管理サーバーの変更タスクを作成します。

   タスク追加ウィザードが開始されます。ウィザードの指示に従ってください。タスク追加ウィザードの［**新規タスク**］ウィンドウで、［**Kaspersky Security Center 14**］を選択してタスク種別に［**管理サーバーの変更**］を選択します。その後、管理サーバーを変更するデバイスを指定します：

- **管理グループにタスクを割り当てる**

  任意の管理グループに属するデバイスにタスクを割り当てます。既存のグループを指定するか、新規グループを作成できます。

  たとえば、特定の管理グループに含まれるデバイスのみが対象のメッセージをユーザーに送信する時に、このオプションを使用すると便利です。

- **デバイスのアドレスを手動で指定するか、リストからアドレスをインポートする**

  タスクを割り当てるデバイスの DNS 名、IP アドレス、IP サブネットを指定できます。

  特定のサブネットワークでタスクを実行する時に、このオプションを使用すると便利です。たとえば、経理担当者のデバイスにのみ特定のアプリケーションをインストールしたり、感染した可能性のあるサブネットワークでデバイスをスキャンする場合などです。

- **デバイスの抽出にタスクを割り当てる**

  デバイスの抽出に属するデバイスにタスクを割り当てます。既存の抽出のいずれかを選択できます。

  たとえば、特定のバージョンのオペレーティングシステムを使用しているデバイスを対象にタスクを実行する時に、このオプションを使用すると便利です。

3. 作成したタスクを実行します。

タスクが完了すると、タスクの対象となったクライアントデバイスは、タスク設定で指定した管理サーバーの管理下に置かれます。

デバイスが不可視の時の処理の表示と設定

グループ内のクライアントデバイスがアクティブでない場合、通知を受け取ることができます。こうしたデバイスを自動的に削除することもできます。

グループ内のデバイスがアクティブでない場合の処理を表示したり設定するには：

1. メインメニューで、［**デバイス**］→［**グループ階層構造**］の順に選択します。
2. 目的の管理グループの名前をクリックします。

   管理グループのプロパティウィンドウが開きます。
3. プロパティウィンドウで［**設定**］タブに移動します。
4. ［**継承**］セクションで、次のオプションの有効と無効を切り替えます：

- **親グループから継承する**

  クライアントデバイスが属する親グループからこのセクションの設定が継承されます。このオプションをオンにすると、［**ネットワーク上のデバイスのアクティビティ**］の設定がロックされ変更できなくなります。

  このオプションは管理グループに親グループが存在する場合にのみ利用できます。

  既定では、このオプションはオンです。

- **設定を子グループへ強制的に継承させる**

  設定値が子グループに配信され、子グループのプロパティではそれらの設定がロックされます。

  既定では、このオプションはオフです。

5. ［**デバイスのアクティビティ**］セクションで、次のオプションの有効と無効を切り替えます：

- **次の期間デバイスが不可視の場合管理者に通知（日）**

  このオプションをオンにすると、管理者が非アクティブなデバイスについて通知を受け取ります。［**デバイスがネットワーク上で長期間アクティブになっていません**］イベントが作成されるまでの期間を指定できます。既定の期間は 7 日です。

  既定では、このオプションはオンです。

- **次の期間デバイスが不可視の場合グループから削除（日）**

  このオプションをオンにすると、デバイスをグループから自動的に削除するまでの期間を指定できます。既定の期間は 60 日です。

  既定では、このオプションはオンです。

6. ［**保存**］をクリックします。

変更内容が保存され、適用されます。

デバイスのステータスの概要

Kaspersky Security Center Linux は、各管理対象デバイスにステータスを割り当てます。特定のステータスは、ユーザーが定義した条件を満たしているかどうかによって異なります。場合によっては、デバイスにステータスを割り当てるときに、Kaspersky Security Center Linux はネットワーク内のデバイスの可視性フラグを考慮します（下の表を参照）。Kaspersky Security Center Linux が 2 時間以内にネットワーク内のデバイスを見つけられない場合、デバイスの可視性フラグは「*不可視*」に設定されます。

ステータスは次の通りです：

- *緊急*または*緊急 / 可視*
- *警告*または*警告 / 可視*
- *OK* または *OK / 可視*

次の表では、「*緊急*」または「*警告*」ステータスをデバイスに割り当てるために満たすべき既定の条件を、可能なすべての値とともに一覧で表示します。

デバイスにステータスを割り当てる条件

条件	条件の説明	設定可能な値
セキュリティ製品がインストール	デバイスにネットワークエージェントはインストールされていますが、セキュリティ製品はインストールされていません。	• 切り

されていません		替えスイッチをオン • 切り替えスイッチをオフ
ウイルスが多数検知されました	ウイルススキャンタスクなどのウイルス検知タスクによりデバイスでウイルスが検知され、検知数が指定された値を超えました。	0 より大きい値
リアルタイム保護レベルが管理者の設定と異なります	デバイスはネットワーク上で可視ですが、リアルタイム保護レベルがデバイスのステータスの条件として管理者によって設定されたレベルと異なっています。	• 停止 • 一時停止 • 実行中
スキャンが長期間実行されていません	デバイスはネットワーク上で可視でセキュリティ製品もインストールされていますが、*マルウェアのスキャンタスク*もローカルスキャンタスクも実行されていない状態が指定期間を越えて続いています。この条件は、7 日以上前に管理サーバーデータベースに追加されたデバイスにのみ適用されます。	1日より大きい値
定義データベースがアップデートされていません	デバイスはネットワーク上で可視でセキュリティ製品もインストールされていますが、このデバイスで定義データベースがアップデートされていない状態が指定期間を越えて続いています。この条件は、1日以上前に管理サーバーデータベースに追加されたデバイスにのみ適用されます。	1日より大きい値
長期間接続されていません	デバイスにネットワークエージェントはインストールされていますが、デバイスがオフになっており、デバイスが管理サーバーに接続されていない状態が指定期間を越えて続いています。	1日より大きい値
アクティブな脅威を検知しました	［**アクティブな脅威**］フォルダー内の未処理オブジェクトの数が指定の値を上回っています。	0 項目より大

		きい値
再起動が必要です	デバイスはネットワーク上で可視ですが、アプリケーションが選択した理由でデバイスの再起動を必要とする状態が指定期間を越えて続いています。	0 分より大きい値
競合アプリケーションがインストールされています	デバイスはネットワーク上で可視ですが、ネットワークエージェントから実行されたソフトウェアインベントリにより、競合するアプリケーションがデバイスにインストールされていることを検知しました。	• 切り替えスイッチをオフ • 切り替えスイッチをオン
ライセンスの有効期間が終了しました	デバイスはネットワーク上で可視ですが、ライセンスの有効期間が終了しています。	• 切り替えスイッチをオフ • 切り替えスイッチをオン
ライセンスの有効期間	デバイスはネットワーク上で可視ですが、ライセンスの有効期間の残り日数が指定した期間以下しかありません。	0 日より

がまもなく終了します		大きい値
未処理のインシデントが検出されました	処理されていないインシデントがデバイス上で見つかりました。インシデントは、クライアントデバイスにインストールしたカスペルスキー製品によって自動で作成されるか、管理者が手動で作成します。	• 切り替えスイッチをオフ • 切り替えスイッチをオン
製品が定義したデバイスのステータス	デバイスのステータスが管理対象アプリケーションによって定義されています。	• 切り替えスイッチをオフ • 切り替えスイッチをオン
デバイスに空き容量がありません	デバイスの空き容量が指定された値未満またはデバイスと管理サーバーを同期できませんでした。デバイスが管理サーバーと正常に同期されなおかつデバイスの空き容量が指定値以上になった場合、ステータスが［*緊急*］または［*警告*］から［*OK*］に変更されます。	0 MB より大きい値
デバイスが管理対象外	デバイスの検索中、デバイスはネットワークで認識されましたが、管理サーバーとの同期に 3 回以上失敗しました。	• 切

になりました		り替えスイッチをオフ • 切り替えスイッチをオン
プロテクションが無効です	デバイスはネットワーク上で可視ですが、デバイス上でセキュリティ製品が無効になっている状態が指定期間を越えて続いています。	0 分より大きい値
セキュリティ製品が実行されていません	デバイスはネットワーク上で可視でセキュリティ製品もインストールされていますが、セキュリティ製品が実行されていません。	• 切り替えスイッチをオフ • 切り替えスイッチをオン

Kaspersky Security Center Linux では、指定した条件が満たされると、管理グループのデバイスのステータスが自動的に切り替わるように設定できます。指定した条件が満たされると、クライアントデバイスには、「*緊急*」または「*警告*」のステータスのいずれかが割り当てられます。指定した条件を満たしていない場合、クライアントデバイスには「*OK*」ステータスが割り当てられます。

1つの条件の複数の値に対して異なるステータスを対応させることができます。たとえば、［**定義データベースがアップデートされていません**］条件の値が「**3日より大きい値**」の場合はクライアントデバイスに「*警告*」ステータスが割り当てられ、条件値が「**7日より大きい値**」の場合は「*緊急*」ステータスが割り当てられます。

Kaspersky Security Center Linuxを旧バージョンからアップグレードしても、ステータスを「*緊急*」または「*警告*」に割り当てるための［**定義データベースがアップデートされていません**］条件の値は変更されません。

Kaspersky Security Center Linuxによってデバイスにステータスが割り当てられると、一部の条件（条件説明の列を参照）で可視性フラグが考慮されます。たとえば、ある管理対象デバイスは［定義データベースがアップデートされていません］条件を満たしていたために「*緊急*」ステータスが割り当てられました。のちにデバイスには可視性フラグが設定され、その後、そのデバイスは「*OK*」ステータスが割り当てられます。

デバイスのステータスの切り替えの設定

デバイスに「*緊急*」または「*警告*」ステータスを割り当てる条件を変更できます。

デバイスのステータスの「緊急」への切り替えを有効にするには：

1. 次のいずれかの方法で、プロパティウィンドウを開きます：
   - ［**ポリシー**］フォルダーの管理サーバーポリシーのコンテキストメニューで［**プロパティ**］を選択します。
   - 管理グループのコンテキストメニューで［**プロパティ**］を選択します。
2. **プロパティ**ウィンドウが表示されたら、［**セクション**］ペインで［**デバイスのステータス**］を選択します。
3. 右側の［**ステータスを「緊急」にする条件**］セクションで、リスト内の各条件に隣接するチェックボックスをオンにします。

   親ポリシーでロック状態になっていない設定のみ変更できます。
4. 選択した条件に対して適切な値を設定します。

   一部の条件では値を指定できますが、値を指定できない条件もあります。
5. ［**OK**］をクリックします。

指定した条件が満たされると、管理対象デバイスには「*緊急*」ステータスが割り当てられます。

デバイスのステータスの「警告」への切り替えを有効にするには：

1. 次のいずれかの方法で、プロパティウィンドウを開きます：
   - ［**ポリシー**］フォルダーの管理サーバーポリシーのコンテキストメニューで［**プロパティ**］を選択します。

- 管理グループのコンテキストメニューで［**プロパティ**］を選択します。

2. **プロパティ**ウィンドウが表示されたら、［**セクション**］ペインで［**デバイスのステータス**］を選択します。
3. 右側の［**ステータスを「警告」にする条件**］セクションで、リスト内の各条件に隣接するチェックボックスをオンにします。

   親ポリシーでロック状態になっていない設定のみ変更できます。

4. 選択した条件に対して適切な値を設定します。

   一部の条件では値を指定できますが、値を指定できない条件もあります。
5. ［**OK**］をクリックします。

指定した条件が満たされると、管理対象デバイスには「*警告*」ステータスが割り当てられます。

ポリシーとポリシーのプロファイル

Kaspersky Security Center 14 Web コンソールを使用して、カスペルスキー製品のポリシーを作成できます。このセクションでは、ポリシーおよびポリシーのプロファイルの概要、作成方法、編集方法を説明しています。

ポリシーとポリシープロファイルについて

*ポリシー*とは、管理グループとそのサブグループに適用される一連のカスペルスキー製品の設定です。管理グループのデバイスに複数のカスペルスキー製品をインストールできます。Kaspersky Security Center は、管理グループ内のカスペルスキー製品ごとに1つのポリシーを提供します。ポリシーは次のいずれかのステータスを持ちます：

ポリシーのステータス

ステータス	説明
アクティブ	現在デバイスに適用されているポリシー。各管理グループ内のカスペルスキー製品に対してアクティブにできるポリシーは1つだけです。デバイスは、カスペルスキー製品のアクティブポリシーの設定値を適用します。
非アクティブ	現在デバイスに適用されていないポリシー。
モバイルユーザー	このオプションをオンにすると、デバイスが企業ネットワークから離れるとポリシーがアクティブになります。

ポリシーは、次のルールに従って機能します：

- 1つのアプリケーションに対して、異なる値を持つ複数のポリシーを定義することができます。

- 現在のアプリケーションに対してアクティブにできるポリシーは1つだけです。
- ポリシーには子ポリシーを設定できます。

一般には、ウイルス攻撃などの緊急事態への備えとしてポリシーを使用できます。たとえば、フラッシュドライブを介した攻撃が発生した場合は、フラッシュドライブへのアクセスをブロックするポリシーを有効化できます。この場合、現在アクティブなポリシーは自動的に非アクティブになります。

異なる状況で複数の設定の変更のみが想定される場合などで、複数のポリシーを管理することを防ぐために、ポリシープロファイルを使用できます。

*ポリシープロファイル*とは、ポリシーの設定値の代わりに使用される、指定されたポリシー設定値のサブセットです。ポリシープロファイルは、管理対象デバイスでの有効な設定の形成に影響を与えます。*有効な設定*とは、デバイスに現在適用されている一連のポリシー設定、ポリシープロファイル設定、およびローカルアプリケーション設定です。

ポリシープロファイルは、次のルールに従って機能します：

- ポリシープロファイルは、特定の有効化条件下で有効になります。
- ポリシープロファイルには、ポリシー設定とは異なる設定値が含まれます。
- ポリシープロファイルを有効化すると、管理対象デバイスの有効な設定が変更されます。
- 1つのポリシーに最大100個のポリシープロファイルを含めることができます。

「ロック」属性とロックされた設定の概要

各ポリシー設定には、ロックのアイコン（🔒）があります。次の表は、ロックのステータスを示しています。

ロックのステータス

ステータス	説明
Undefined	設定の横に開いたロックが表示され、切り替えスイッチが無効になっている場合、その設定はポリシーで指定されていません。ユーザーは管理対象アプリケーションのインターフェイスを使用してこれらの設定を変更できます。このような設定を「*ロック解除*」と呼びます。
Enforce	設定の横に閉じたロックが表示され、切り替えスイッチが有効になっている場合、その設定はポリシーが適用されるデバイスに適用されます。ユーザーは、管理対象アプリケーションのインターフェイスでこれらの設定の値を変更することはできません。このような設定を「*ロック*」と呼びます。

管理対象デバイスに適用するポリシー設定のロックを閉じておくことを強く推奨します。ロックが解除されたポリシー設定は、管理対象デバイスのカスペルスキーのアプリケーション設定によって再度割り当てられます。

ロックを使用して、次の操作を実行します：

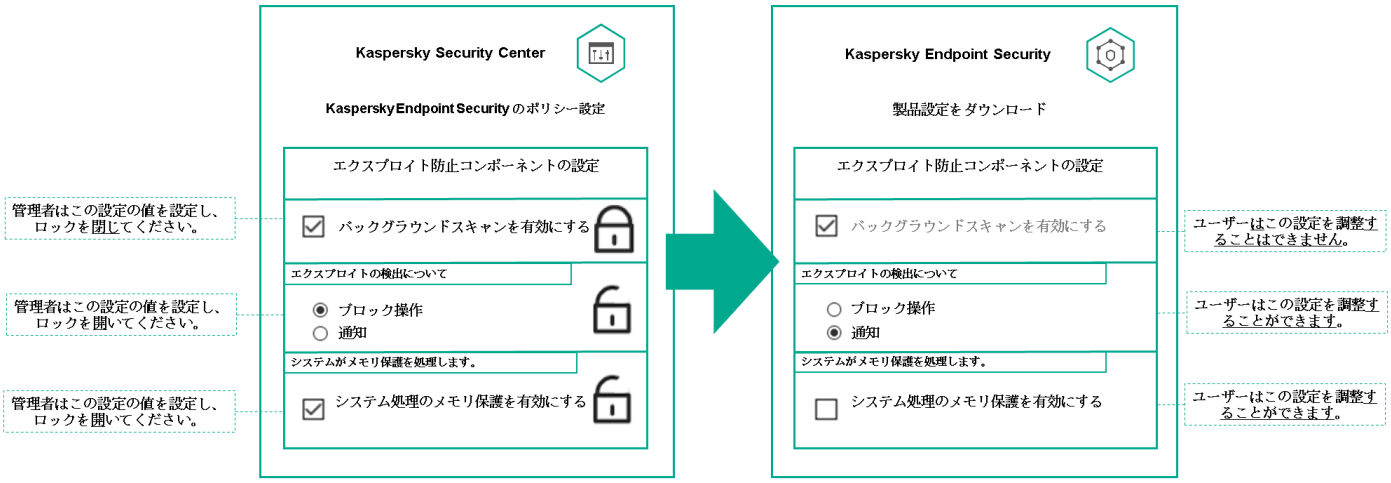
- 管理サブグループのポリシーの設定をロックする
- 管理対象デバイス上のカスペルスキー製品の設定をロックする

したがって、ロックされた設定は、有効な設定を管理対象デバイスに実装するために使用されます。

有効な設定の実装プロセスには、次の操作が含まれます：

- 管理対象デバイスが、カスペルスキー製品の設定値を適用する
- 管理対象デバイスが、ポリシーのロックされた設定の値を適用する

ポリシーおよび管理対象のカスペルスキー製品には、同じ設定内容が含まれています。ポリシー設定を構成すると、管理対象デバイスでカスペルスキー製品設定値が変更されます。管理対象デバイスのロックされた設定をユーザーが調整することはできません（下図を参照）：



ロックとカスペルスキー製品の設定

ポリシーとポリシーのプロファイルの継承

このセクションでは、ポリシーとポリシープロファイルの階層と継承について説明します。

ポリシーの階層

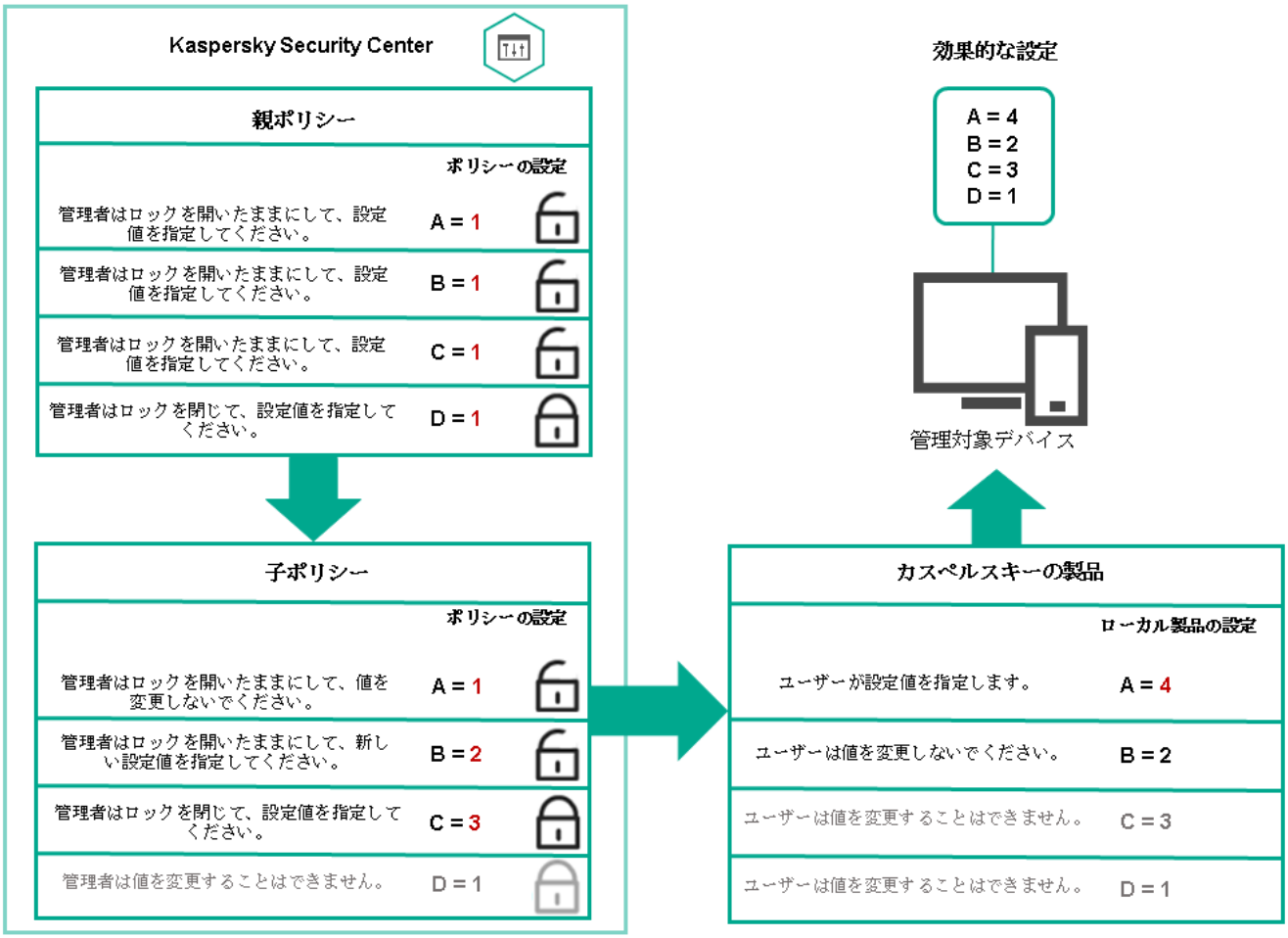
デバイスごとに異なる設定が必要な場合は、デバイスを管理グループに整理できます。

単一の管理グループにポリシーを1つ指定できます。ポリシー設定は*継承できます*。継承とは、上位（親）の管理グループのポリシーからサブグループ（子グループ）にポリシー設定値を受け取ることを意味します。

以降の説明では、親グループで設定されているポリシーを「*親ポリシー*」と表記する場合があります。サブグループ（子グループ）のポリシーを「*子ポリシー*」と表記する場合があります。

既定では、管理サーバーには少なくとも1つの管理対象デバイスグループが存在します。カスタムグループを作成する場合、それらは管理対象デバイスグループ内のサブグループ（子グループ）として作成されます。

同じアプリケーションのポリシーは、管理グループの階層に従って互いに影響を与えます。上位（親）管理グループのポリシーのロック済みの設定は、サブグループのポリシー設定値を再割り当てします（下の図を参照）。

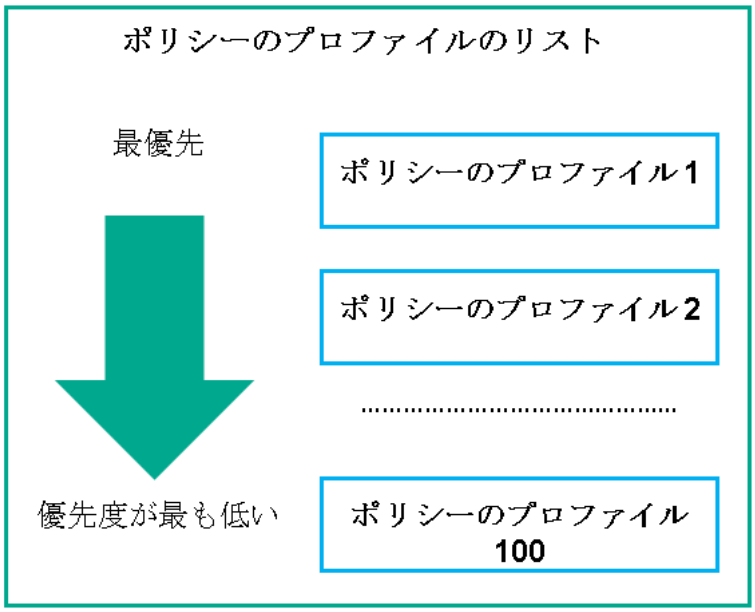


ポリシーの階層

ポリシーの階層内のポリシープロファイル

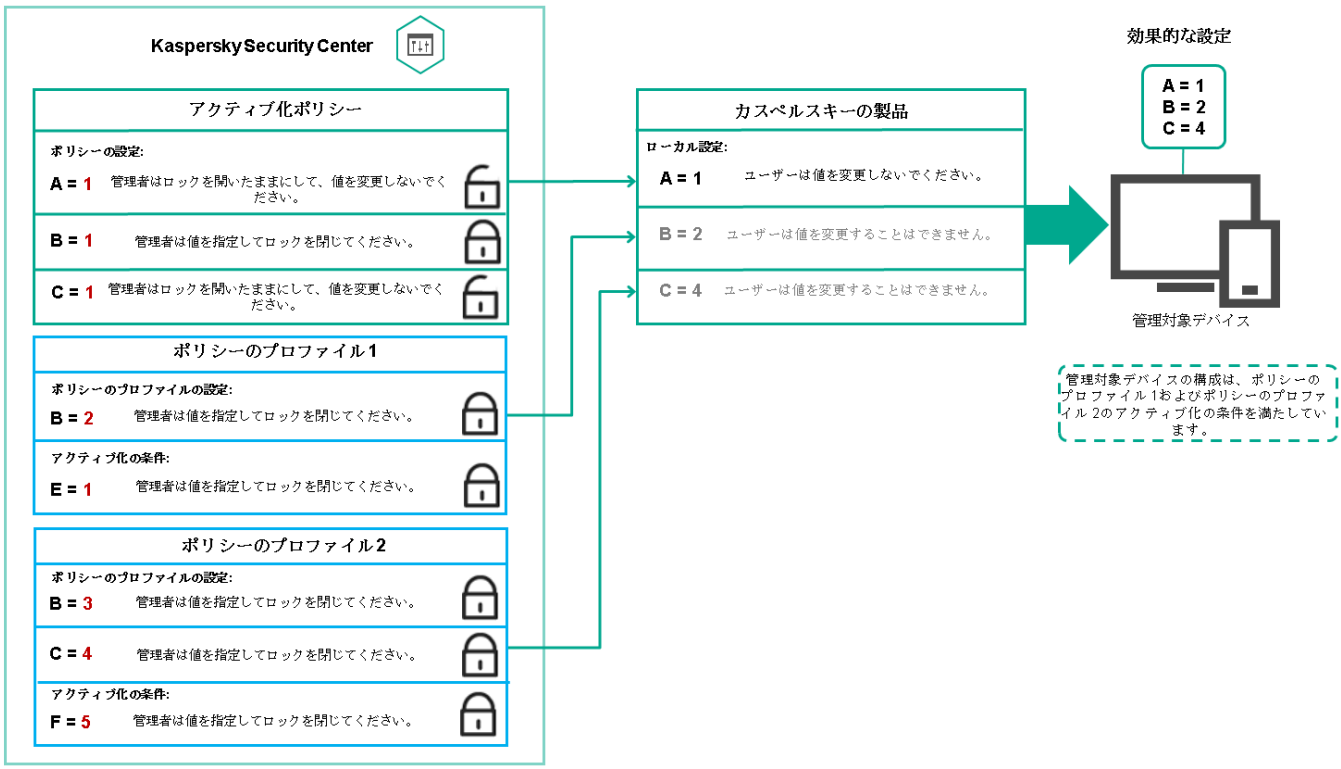
ポリシープロファイルでの優先順位の割り当て条件は次の通りです：

- ポリシープロファイルリスト内のプロファイルの位置は、そのプロファイルの優先度を示します。ポリシーのプロファイルの優先順位を変更できます。リストの一番上にある場合、優先順位が最も高くなります（下の図を参照）。



ポリシープロファイルの優先度の定義

- ポリシープロファイルの有効化条件は相互に依存しません。複数のポリシープロファイルを同時に有効化できます。複数のポリシープロファイルが同じ設定に影響を与える場合、デバイスは最も優先度の高いポリシープロファイルから設定値を取得します（下の図を参照）。



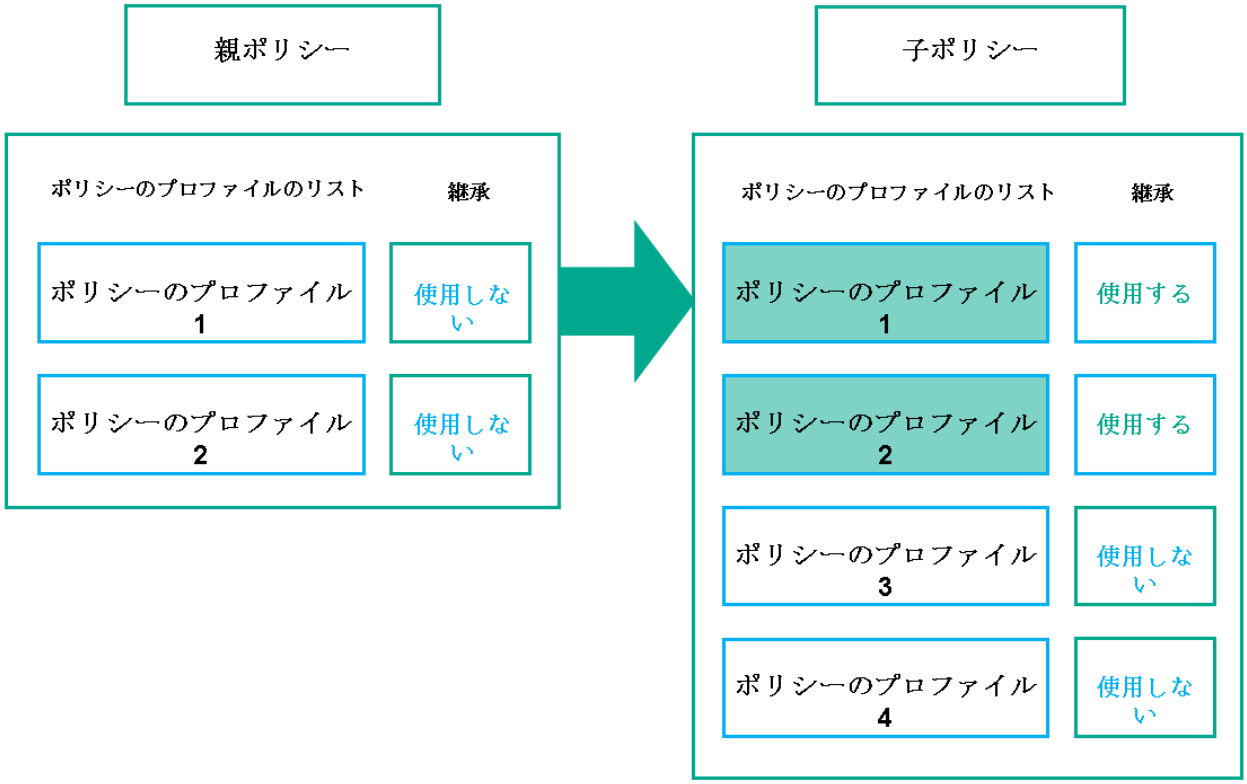
管理対象デバイスの構成が、複数のポリシープロファイルの有効化条件を満たしている

継承の階層におけるポリシープロファイル

様々な階層レベルにあるポリシーのポリシープロファイルは、次の条件を満たします：

- 下位のポリシーは、上位のポリシーからポリシープロファイルを継承します。上位のポリシーから継承されたポリシープロファイルは、元のポリシープロファイルのレベルよりも優先度が高くなります。

- 継承されたポリシープロファイルの優先度を変更することはできません（下の図を参照）。

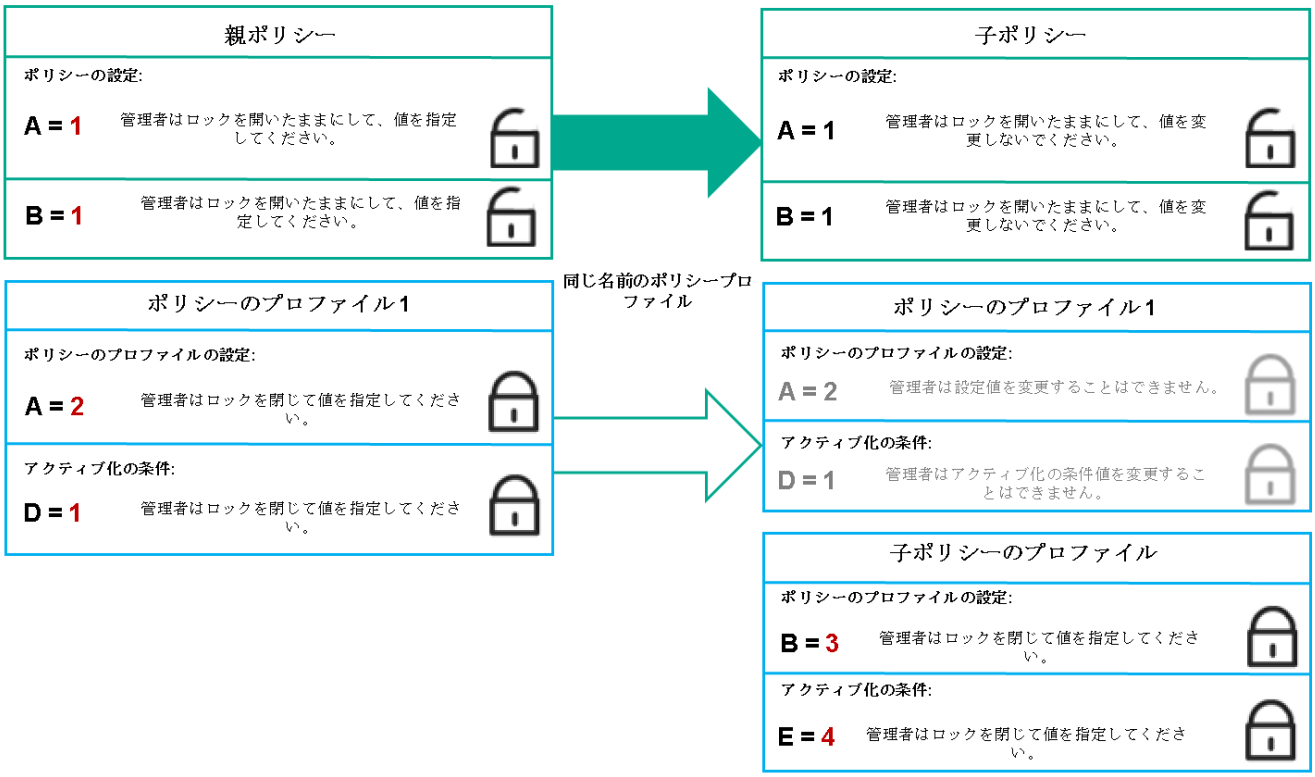


ポリシープロファイルの継承

同じ名前のポリシープロファイル

異なる階層レベルに、同じ名前の 2 つのポリシーがある場合、これらのポリシーは次のルールに従って機能します：

- ロックされた設定および上位のポリシープロファイルのプロファイル有効化条件により、下位のポリシープロファイルの設定およびプロファイル有効化条件が変更されます（下図を参照）。



子プロファイルは親ポリシープロファイルから設定値を継承する

- ロック解除された設定および上位のポリシープロファイルのプロファイル有効化条件により、下位のポリシープロファイルの設定およびプロファイル有効化条件が変更されません。

管理対象デバイスに設定が実装される方法

管理対象デバイスでの有効な設定の実装は、次のように説明できます：

- ロックされていないすべての設定の値は、有効なポリシーから取得されます。
- 次に、管理対象アプリケーション設定の値で上書きされます。
- 次に、有効なポリシーのロックされた設定値が適用されます。ロックされた設定値は、ロックされていない有効な設定値を変更します。

ポリシーの管理

このセクションでは、ポリシーの管理について説明します。ポリシーのリストの表示、ポリシーの作成、ポリシーの変更、ポリシーのコピー、ポリシーの移動、強制同期、ポリシー導入ステータス図の表示、およびポリシーの削除に関する情報を提供します。

ポリシーのリストの表示

管理サーバーまたは任意の管理グループを対象に作成されたポリシーのリストを表示できます。

ポリシーのリストを表示するには：

1. メインメニューで、［**デバイス**］→［**グループ階層構造**］の順に選択します。
2. 管理グループのリストで、ポリシーのリストを表示する管理グループを選択します。

ポリシーのリストが表形式で表示されます。ポリシーが存在しない場合、表は空です。表の列の表示と非表示の切り替え、列の順序の変更、指定した値を含む行のみの表示、検索の使用などを実行できます。

ポリシーの作成

ポリシーの作成と、既存のポリシーの変更と削除を行うことができます。

ポリシーを作成するには：

1. ［**デバイス**］→［**ポリシーとプロファイル**］の順に選択します。
2. ［**追加**］をクリックします。
   ［**アプリケーションの選択**］ウィンドウが表示されます。
3. ポリシーを作成するアプリケーションを選択します。
4. ［**次へ**］をクリックします。
   新規ポリシーの設定ウィンドウの［**全般**］タブが表示されます。
5. 必要に応じて、ポリシーの既定の名前、ステータス、継承設定を変更します。
6. ［**アプリケーション設定**］タブを選択します。
   あるいは、［**保存**］をクリックして作成を完了します。ポリシーのリストに新しいポリシーが表示されます。ポリシーの設定は後で編集できます。
7. ［**アプリケーション設定**］タブの左側のペインで目的のカテゴリを選択し、右側の結果ペインでポリシーの設定を編集します。ポリシーの各カテゴリ（セクション）の設定を編集できます。
   設定内容は、作成するポリシーの対象となる製品に応じて異なります。詳細は、次を参照してください：
   - 管理サーバーの設定
   - ネットワークエージェントのポリシー設定
   - Kaspersky Endpoint Security for Linux のヘルプ
   その他のカスペルスキー製品の設定の詳細については、該当する製品のヘルプまたはガイドを参照してください。
   設定の編集時、［**キャンセル**］をクリックすると、最後に行った操作を取り消すことができます。
8. ［**保存**］をクリックしてポリシーを保存します。

ポリシーのリストに新しいポリシーが表示されます。

ポリシーの全般的な設定

全般

［**全般**］タブでは、ポリシーステータスを変更したり、継承ポリシーを設定したりすることができます：

- ［**ポリシーのステータス**］セクションで、ポリシーのステータスを選択します：
  - **アクティブ**

    このオプションをオンにすると、ポリシーがアクティブになります。

    既定では、このオプションがオンです。

  - **モバイルユーザー**

    このオプションをオンにすると、デバイスが企業ネットワークから離れるとポリシーがアクティブになります。

  - **非アクティブ**

    このオプションをオンにすると、ポリシーは非アクティブになりますが［**ポリシー**］フォルダーに保持されます。必要に応じて、ポリシーをアクティブにすることができます。

- ［**設定の継承**］セクションでは、ポリシーの継承を設定できます。
  - **親ポリシーから設定を継承する**

    このオプションをオンにすると、ポリシーの設定値は上位レベルグループのポリシーから継承されるため、ロックされます。

    既定では、このオプションはオンです。

  - **設定を子ポリシーへ強制的に継承させる**

    このオプションをオンにすると、ポリシーの変更を適用した後に次の処理が実行されます：
    - 管理サブグループのポリシー（子ポリシー）に、ポリシーの設定値が継承されます。
    - 各子ポリシーのプロパティウィンドウの［**全般**］セクションにある［**設定の継承**］ブロックで、［**親ポリシーから設定を継承する**］が自動的にオンになります。

    このオプションをオンにすると、子ポリシーの設定はロックされます。

    既定では、このオプションはオフです。

イベントの設定

［**イベントの設定**］タブでは、イベントの記録と通知を設定できます。イベントは、重要度に応じて次のタブに分類されます：

- **緊急**
  ［**緊急**］セクションは、ネットワークエージェントのポリシーのプロパティに表示されません。
- **機能エラー**
- **警告**
- **情報**

それぞれのセクションのリストには、イベントの種別と、管理サーバーでイベントが保存される既定の日数が表示されます。イベントの種別をクリックすると、次の設定を指定できます：

- **イベント登録**
  イベントの保存期間を指定し、保存場所を選択できます：
  - **Syslog 経由で SIEM システムにエクスポートする**
  - **デバイスの OS イベントログに保存**
  - **管理サーバーの OS イベントログに保存**
- **イベント通知**
  次の通知方法ごとに、通知を受け取るかどうかを指定できます：
  - **メールで通知**
  - **SMS で通知**
  - **実行ファイルまたはスクリプトの実行で通知**
  - **SNMP 経由で通知**

  既定では、通知に利用する設定（受信アドレスなど）は、管理サーバーのプロパティで指定された設定を使用します。［**メール**］タブ、［**SMS**］タブ、［**実行ファイル**］タブで、必要に応じてそれぞれの設定を変更できます。

変更履歴

［**変更履歴**］タブでは、必要に応じて、ポリシーのリビジョンのリストを表示したり、ポリシーで行われた変更をロールバックすることができます。

ポリシーの変更

ポリシーを変更するには：

1. ［**デバイス**］→［**ポリシーとプロファイル**］の順に選択します。
2. 変更するポリシーを選択します：
   ポリシーの設定ウィンドウが表示されます。

3. 作成するポリシーの一般設定とアプリケーションの設定を指定します。詳細については、次を参照してください：

   - 管理サーバーの設定
   - ネットワークエージェントのポリシー設定
   - Kaspersky Endpoint Security for Linux のヘルプ

   その他のカスペルスキー製品の設定の詳細については、該当する製品のヘルプまたはガイドを参照してください。

4. ［**保存**］をクリックします。

ポリシーに加えた変更は、ポリシーのプロパティに保存され、［**変更履歴**］セクションに表示されます。

ポリシー継承オプションの有効化と無効化

ポリシーで継承オプションを有効または無効にするには：

1. 必要なポリシーを開きます。
2. ［**全般**］タブを開きます。
3. ポリシーの継承をオンまたはオフにします。

   - 子ポリシーで［**親ポリシーから設定を継承する**］をオンにし、管理者が親ポリシーの設定の一部をロック状態にすると、子ポリシーでこれらの設定を変更することはできません。
   - 子ポリシーで［**親ポリシーから設定を継承する**］をオフにすると、親ポリシーでロック状態の設定も含めて、子ポリシー側ですべての設定を変更できます。
   - 親グループで［**設定を子ポリシーへ強制的に継承させる**］をオンにすると、各子ポリシーで［**親ポリシーから設定を継承する**］がオンになります。この場合、子ポリシーの側でこのオプションをオフにすることはできません。親ポリシーでロックされている設定はすべて強制的に子ポリシーに継承され、子グループ側でこれらの設定を変更することはできません。

4. ［**保存**］ボタンをクリックして変更を保存するか、［**キャンセル**］ボタンをクリックして変更を破棄します。

既定では、新規に作成したポリシーでは［**親ポリシーから設定を継承する**］はオンです。

ポリシーにポリシープロファイルが存在する場合、子ポリシーでもこれらのプロファイルが継承されます。

ポリシーのコピー

ポリシーを任意の管理グループから別の管理グループにコピーできます。

ポリシーを別の管理グループにコピーするには：

1. メインメニューで、［**デバイス**］→［**ポリシーとプロファイル**］の順に選択します。

2. コピーするポリシーに隣接するチェックボックスをオンにします。

3. ［**コピー**］をクリックします。
   画面の右側に管理グループのツリーが表示されます。

4. ツリーで、ポリシーのコピー先となるグループ（ターゲットグループ）を選択します。

5. ページの一番下にある［**コピー**］をクリックします。

6. ［OK］をクリックして処理内容を確定します。

すべてのプロファイルと合わせてターゲットグループにポリシーのコピーが作成されます。ターゲットグループにコピーして作成したポリシーのステータスは［**非アクティブ**］です。いつでもステータスを［**アクティブ**］に変更できます。

新たに移動されるポリシー名と同じ名前のポリシーがターゲットグループに既に存在している場合、新たに移動されるポリシー名に、たとえば (1)、(2) のようなインデックス「(<次の連番>)」が追加されます。

ポリシーの移動

ポリシーを任意の管理グループから別の管理グループに移動できます。たとえば、削除したいグループがあるが、そのグループのポリシーは別のグループで使用したいとします。その場合、グループを削除する前に、ポリシーを別のグループに移動できます。

ポリシーを別の管理グループに移動するには：

1. メインメニューで、［**デバイス**］→［**ポリシーとプロファイル**］の順に選択します。

2. 移動するポリシーに隣接するチェックボックスをオンにします。

3. ［**移動**］をクリックします。
   画面の右側に管理グループのツリーが表示されます。

4. ツリーで、ポリシーの移動先となるグループ（ターゲットグループ）を選択します。

5. ページの一番下にある［**移動**］をクリックします。

6. ［OK］をクリックして処理内容を確定します。

ポリシーがソースグループから継承されていない場合、ポリシーはすべてのプロファイルと合わせてターゲットグループに（コピーではなく）移動されます。ターゲットグループに作成したポリシーのステータスは［**非アクティブ**］です。いつでもステータスを［**アクティブ**］に変更できます。

ポリシーがソースグループから継承されている場合、ポリシーは元のグループにも残ります。そして、すべてのプロファイルと合わせてターゲットグループにコピーが作成されます。ターゲットグループに作成したポリシーのステータスは［**非アクティブ**］です。いつでもステータスを［**アクティブ**］に変更できます。

新たに移動されるポリシー名と同じ名前のポリシーがターゲットグループに既に存在している場合、新たに移動されるポリシー名に、たとえば (1)、(2) のようなインデックス「(<次の連番>)」が追加されます。

強制同期

Kaspersky Security Center Linux では、管理対象デバイスのステータス、設定、タスク、ポリシーは自動的に同期されます。定められた時点で、特定のデバイスで同期が実行されているかどうかを、管理者が正確に把握する必要がある場合があります。

単一デバイスの同期

管理サーバーと管理対象デバイスの同期を強制的に実行するには：

1. ［**デバイス**］→［**管理対象デバイス**］の順に選択します。
2. 管理サーバーと同期させるデバイスの名前をクリックします。
   プロパティウィンドウの［**全般**］セクションが表示されます。
3. ［**強制同期**］をクリックします。

指定したデバイスと管理サーバーの同期が実行されます。

複数デバイスの同期

管理サーバーと複数の管理対象デバイスの同期を強制的に実行するには：

1. 管理グループまたはデバイスの抽出からデバイスリストを開きます：
   - メインメニューで［**デバイス**］→［**管理対象デバイス**］の順に移動し、管理対象デバイスのリストの上にある［**現在のパス**］フィールドのパスリンクをクリックして、同期するデバイスを含む管理グループを選択します。
   - デバイスの抽出を実行してデバイスリストを表示します。
2. 管理サーバーと同期するデバイスに隣接するチェックボックスをオンにします。
3. 管理対象デバイスのリストの上にある省略記号ボタン（**...**）、［**強制同期**］をクリックします。
   指定したデバイスと管理サーバーの同期が実行されます。
4. デバイスリストで、指定したデバイスでの前回の管理サーバーへの接続の時間が現在の時間に変更されていることが確認できます。時間が変更されていない場合は、［**更新**］をクリックしてページの内容を更新します。

選択したデバイスのデータが管理サーバーと同期します。

ポリシーの配信時間の表示

管理サーバーでカスペルスキー製品のポリシーを変更した後、変更後のポリシーが特定の管理対象デバイスに配信されたかどうかを管理者は確認できます。ポリシーは、定期的な同期または強制的な同期によって配信されます。

管理対象デバイスに製品ポリシーが配信された日時を表示するには：

1. ［**デバイス**］→［**管理対象デバイス**］の順に選択します。
2. 管理サーバーと同期させるデバイスの名前をクリックします。
   プロパティウィンドウの［**全般**］セクションが表示されます。
3. ［**アプリケーション**］タブをクリックします。
4. ポリシーを同期した日時を表示する製品を選択します。
   製品ポリシーのプロパティウィンドウの［**全般**］セクションが表示され、ポリシーの配信日時を確認できます。

ポリシー導入ステータス図の表示

Kaspersky Security Center では、各デバイスのポリシー適用のステータスをポリシー導入ステータス図で表示できます。

各デバイスのポリシー導入ステータスを表示するには：

1. ［**デバイス**］-［**ポリシーとプロファイル**］の順に選択します。
2. デバイスの導入ステータスを表示するポリシーの名前に隣接するチェックボックスをオンにします。
3. 表示されたメニューで、［**導入**］リンクを選択します。
   ［**<ポリシー名> 導入結果**］ウィンドウが開きます。
4. 開いた［**<ポリシー名> 導入結果**］ウィンドウに、ポリシーの**ステータスの説明**が表示されます。

ポリシーの導入結果のリストに表示されるデバイス数を変更できます。推奨されるデバイス数の上限は、100000 台です。

ポリシーの導入結果のリストに表示されるデバイスの数を変更するには：

1. ツールバーの［**インターフェイスのオプション**］セクションに移動します。
2. ［**ポリシーの導入結果に表示するデバイス数の上限**］に、デバイスの数（最大 100,000）を入力します。
   既定では、この数は 5,000 です。
3. ［**保存**］をクリックします。
   設定が保存され、適用されます。

ポリシーの削除

必要ないポリシーは削除できます。ただし、削除できるのは上位のグループから継承されたのではないポリシーのみです。上位のグループから継承されたポリシーは、そのポリシーが作成された上位のグループでのみ削除できます。

ポリシーを削除するには：

1. メインメニューで、［**デバイス**］→［**ポリシーとプロファイル**］の順に選択します。

2. 削除するポリシーの横のチェックボックスをオンにし、［**削除**］をクリックします。

   上位のポリシーから設定を継承したポリシーを選択した場合、［**削除**］はグレーアウトされ選択できなくなります。

3. ［**OK**］をクリックして処理内容を確定します。

ポリシーとそのすべてのプロファイルが削除されます。

ポリシーのプロファイルの管理

このセクションでは、ポリシープロファイルの管理について説明します。ポリシーのプロファイルの表示、ポリシープロファイルの優先度の変更、ポリシープロファイルの作成、ポリシープロファイルのコピー、ポリシープロファイルの有効化ルールの作成、およびポリシープロファイルの削除に関する情報を提供します。

ポリシーのプロファイルの表示

ポリシーのプロファイルを表示するには：

1. メインメニューで、［**デバイス**］→［**ポリシーとプロファイル**］の順に選択します。
2. プロファイルを表示するポリシーの名前をクリックします：

   ポリシーのプロパティウィンドウの［**全般**］タブが表示されます。
3. ［**ポリシーのプロファイル**］タブを開きます。

ポリシーのプロファイルのリストが表形式で表示されます。ポリシーにプロファイルがない場合、表は空です。

ポリシーのプロファイルの優先順位の変更

ポリシーのプロファイルの優先順位を変更するには：

1. 目的のポリシーのプロファイルのリストに移動します。

   ポリシーのプロファイルのリストが表示されます。
2. ［**ポリシーのプロファイル**］タブで、優先度を変更するポリシープロファイルの横にあるチェックボックスをオンにします。
3. ［**優先度を高く設定**］または［**優先度を低く設定**］をクリックして、ポリシープロファイルの新しい位置を指定します。

   リスト内でポリシーの位置が上にあるほど、優先度も高くなります。
4. ［**保存**］をクリックします。

選択したポリシーのプロファイルの優先順位が変更され、適用されます。

ポリシーのプロファイルの作成

ポリシーのプロファイルを作成するには：

1. 目的とするポリシーのプロファイルのリストに移動します。

   ポリシーのプロファイルのリストが表示されます。ポリシーにプロファイルが設定されていない場合、表は空です。

2. ［**追加**］をクリックします。

3. 必要に応じて、プロファイルの既定の名前と継承設定を変更します。

4. ［**アプリケーション設定**］タブを選択します。

   または、［**保存**］をクリックして完了します。ポリシープロファイルのリストに作成したプロファイルが表示されます。プロファイルの設定は後で編集できます。

5. ［**アプリケーション設定**］タブの左側のペインで目的のカテゴリを選択し、右側の結果ペインでプロファイルの設定を編集します。ポリシーのプロファイルの各カテゴリ（セクション）の設定を編集できます。

   設定の編集時、［**キャンセル**］をクリックすると、最後に行った操作を取り消すことができます。

6. ［**保存**］をクリックしてプロファイルを保存します。

ポリシーのプロファイルのリストに新しいプロファイルが表示されます。

ポリシーのプロファイルのコピー

ポリシーのプロファイルを現在の割り当て先のポリシーや別のポリシーにコピーして、同じポリシーを別のポリシーで使用できます。また、プロファイルのコピー機能は、一部の設定だけが異なる複数のプロファイルを作成する場合にも活用できます。

ポリシーのプロファイルをコピーするには：

1. 目的のポリシーのプロファイルのリストに移動します。

   ポリシーのプロファイルのリストが表示されます。ポリシーにプロファイルが設定されていない場合、表は空です。

2. ［**ポリシーのプロファイル**］タブで、コピーするポリシープロファイルを選択します。

3. ［**コピー**］をクリックします。

4. 表示されるウィンドウで、プロファイルのコピー先にするポリシーを選択します。

   ポリシーのプロファイルを、現在割り当てられているのと同じポリシーまたは指定した別のポリシーにコピーできます。

5. ［**コピー**］をクリックします。

ポリシーのプロファイルが指定したポリシーにコピーされます。コピーして作成された新しいプロファイルには、最も低い優先度が設定されます。プロファイルを現在割り当てられているのと同じポリシーにコピーした場合、プロファイル名に (1)、(2) のようなインデックス「<数字>」が追加されます。

コピーの完了後、プロファイル名や優先度も含めてプロファイルの設定を変更できます。この変更によりコピー元のプロファイルが影響を受けることはありません。

ポリシーのプロファイルの有効化ルールの作成

ポリシーのプロファイルの有効化ルールを作成するには：

1. 目的のポリシーのプロファイルのリストに移動します。
   ポリシーのプロファイルのリストが表示されます。
2. ［**ポリシーのプロファイル**］タブで、有効化ルールを作成するポリシープロファイルをクリックします。
   ポリシープロファイルのリストが空の場合は、ポリシーのプロファイルを作成できます。
3. ［**有効化ルール**］タブで、［**追加**］をクリックします。
   ポリシーのプロファイルの有効化ルールのウィンドウが表示されます。
4. ルールの名前を入力します。
5. 作成しているポリシープロファイルの有効化に作用する条件の横にあるチェックボックスをオンにします：

   - **ポリシープロファイルの有効化に対する全般ルール**

     このチェックボックスをオンにすると、デバイスのオフラインモードのステータス、管理サーバーへの接続ルール、デバイスに割り当てられているタグに応じて、デバイス上でポリシープロファイルの有効化ルールを設定できます。

     このオプションでは、次の項目を設定できます：

     - **デバイスのステータス**

       ネットワーク内にデバイスが存在するかどうかを指定します：
       - **オンライン** - デバイスはネットワーク内にあるため、管理サーバーを使用できます。
       - **オフライン** - デバイスは外部ネットワーク内にあるため、管理サーバーは使用できません。
       - **該当なし** - 基準は適用されません。

     - **管理サーバー接続のルールがこのデバイスでアクティブです**

       ポリシーのプロファイルを有効化する条件（ルールを実行する条件）を選択し、ルールの名前を指定します。

       ルールでは、管理サーバーへの接続に関するデバイスのネットワークロケーションを指定します。ポリシープロファイルを有効にするためにネットワークロケーションの説明の条件を満たす（または満たさない）必要があります。

       管理サーバーへの接続に関するデバイスのネットワークロケーションの説明は、ネットワークエージェント切り替えルールで作成または設定できます。

- **特定のデバイス所有者向けのルール**

  このオプションでは、次の項目を設定できます：

  - **デバイスの所有者**

    このオプションをオンにして、デバイスの所有者に応じたプロファイルの有効化ルールを設定を有効にします。このチェックボックスの下のドロップダウンリストで、プロファイルの有効化の基準を選択できます：

    - デバイスが特定の所有者のものである（「=」記号）
    - デバイスが特定の所有者のものでない（「#」記号）

      このオプションをオンにすると、設定された基準に従ってデバイス上でプロファイルが有効化されます。このオプションをオンにすると、デバイスの所有者を指定できます。このオプションをオフにすると、プロファイルの有効化の基準は適用されません。既定では、このオプションはオフです。

  - **デバイスの所有者が属する内部セキュリティグループ**

    このオプションをオンにして、デバイスの所有者の Kaspersky Security Center Linux の内部セキュリティグループの所属に応じたプロファイルの有効化ルールを有効にします。このチェックボックスの下のドロップダウンリストで、プロファイルの有効化の基準を選択できます：

    - デバイスの所有者が特定のセキュリティグループのメンバーである（「=」記号）
    - デバイスの所有者が特定のセキュリティグループのメンバーでない（「?」記号）

      このオプションをオンにすると、設定された基準に従ってデバイス上でプロファイルが有効化されます。Kaspersky Security Center Linux のセキュリティグループを指定できます。このオプションをオフにすると、プロファイルの有効化の基準は適用されません。既定では、このオプションはオフです。

- **ハードウェアの仕様のルール**

  このチェックボックスをオンにすると、メモリサイズと論理プロセッサの数に応じて、デバイス上でポリシープロファイルの有効化ルールを設定できます。

  このオプションでは、次の項目を設定できます：

  - **RAM サイズ（MB）**

    このオプションをオンにして、デバイスで使用可能な RAM サイズに応じたプロファイルの有効化のルールを有効にします。このチェックボックスの下のドロップダウンリストで、プロファイルの有効化の基準を選択できます：

    - デバイスの RAM サイズは指定された値以下である（「<」記号）。
    - デバイスの RAM サイズは指定された値以上である（「>」記号）。

    このオプションをオンにすると、設定された基準に従ってデバイス上でプロファイルが有効化されます。デバイスの RAM ボリュームを指定できます。このオプションをオフにすると、プロファイルの有効化の基準は適用されません。既定では、このオプションはオフです。

  - **論理プロセッサの数**

このオプションをオンにして、デバイスの論理プロセッサの数に応じたプロファイルの有効化ルールを有効にします。このチェックボックスの下のドロップダウンリストで、プロファイルの有効化の基準を選択できます：

- デバイスの論理プロセッサの数は指定された値以下である（「<」記号）。
- デバイスの論理プロセッサの数は指定された値以上である（「>」記号）。

このオプションをオンにすると、設定された基準に従ってデバイス上でプロファイルが有効化されます。デバイス上の論理プロセッサの数を指定できます。このオプションをオフにすると、プロファイルの有効化の基準は適用されません。既定では、このオプションはオフです。

- **ロールの割り当てルール**

  このオプションでは、次の項目を設定できます：

  - **デバイス所有者のロールに応じてポリシープロファイルを有効化する**

    このオプションをオンにすると、デバイスの所有者のロールに応じたプロファイルの有効化ルールを設定し、オンにすることができます。既存のロールのリストからロールを手動で選択して追加します。

    このオプションをオンにすると、設定された基準に従ってデバイス上でプロファイルが有効化されます。

- **タグの使用ルール**

  このチェックボックスをオンにすると、デバイスに割り当てられたタグに応じて、デバイス上でポリシープロファイルの有効化ルールを設定できます。選択したタグが割り当てられているデバイスまたは割り当てられていないデバイスのいずれかで、ポリシーのプロファイルを有効にできます。

  このオプションでは、次の項目を設定できます：

  - **タグリスト**

    このタグのリストで、目的のタグのチェックボックスをオンにすると、ポリシーのプロファイルにデバイスを含めるためのルールを指定できます。

    リストの上のフィールドに新しいタグを入力して、［**追加**］をクリックすると、新しいタグをリストに追加できます。

    選択したタグのすべてを説明に含むデバイスがポリシーのプロファイルに含まれます。チェックボックスをオフにすると、基準は適用されません。既定では、これらのチェックボックスはオフです。

  - **指定したタグのないデバイスに適用する**

    タグの選択状態を反転させる必要がある場合は、このオプションをオンにします。

    このオプションをオンにすると、選択されたタグのいずれも説明に含まないデバイスがポリシープロファイルに含まれます。このオプションをオフにすると、基準が適用されません。

    既定では、このオプションはオフです。

ウィザードで表示されるウィンドウ数は、最初のステップで選択した設定によります。ポリシープロファイルの有効化ルールは後で変更することができます。

6. 設定したパラメータのリストを確認します。リストのパラメータが正しいことが確認できたら、［**作成**］をクリックします。

プロファイルが保存されます。プロファイルは、有効化ルールが適合すると、デバイスで有効になります。

プロファイル用に作成したポリシープロファイルの有効化ルールが、［**有効化ルール**］タブのポリシープロファイルのプロパティに表示されます。ポリシープロファイルの有効化ルールはいずでも変更または削除することができます。

複数の有効化ルールを同時に適合させることができます。

ポリシーのプロファイルの削除

ポリシーのプロファイルを削除するには：

1. 目的のポリシーのプロファイルのリストに移動します。

ポリシーのプロファイルのリストが表示されます。

2. ［**ポリシーのプロファイル**］タブで、削除するポリシープロファイルに隣接するチェックボックスをオンにし、［**削除**］をクリックします。

3. 表示されるウィンドウで、もう一度［**削除**］をクリックします。

ポリシープロファイルが削除されます。下位のグループでこのポリシーが継承されている場合、該当する下位のグループでプロファイルが維持されますが、プロファイルの所属先がこの下位のグループのポリシーに変更されます。この処理は、下位グループのデバイスにインストールされている管理対象製品の設定が大幅に変更されてしまわないようにするために実装されています。

ユーザーとユーザーロール

このセクションでは、ユーザーとユーザーロールの概要および作成と編集の手順、ユーザーへのロールとグループの割り当て方法、ポリシーのプロファイルとロールの関連付けの方法について説明しています。

ユーザーロールの概要

ユーザーロール（省略して「*ロール*」とも表記）は、複数の権限をまとめたものと捉えることができます。ロールは、ユーザーのデバイスにインストールされているカスペルスキー製品の設定と関連付けることができます。ロールは、管理グループの任意の階層のユーザーまたはセキュリティグループに割り当てることができます。

ユーザーロールはポリシーのプロファイルに関連付けることができます。ユーザーにロールを割り当てることで、このユーザーには、担当業務を実行する上で必要なセキュリティ設定が適用されます。

ユーザーロールは、特定の管理グループのデバイスのユーザーに関連付けることができます。

ユーザーロールの対象範囲

*ユーザーロールの対象範囲*は、「ユーザーへの割り当て」と「管理グループへの関連付け」の 2 つの要素の組み合わせとして定義されます。ユーザーロールと関連付けられた設定は、ロールに関連付けられたグループ（子グループを含む）にデバイスが属し、なおかつそのロールを割り当てられたユーザーが所有しているデバイスのみに適用されます。

ロールを使用する利点

ロールを使用する利点として、管理対象デバイスごとあるいはユーザーごとに個別にセキュリティ設定を指定しなくて済む点があります。社内のユーザー数とデバイス数は組織の規模に応じて膨大になる場合がありますが、個別のセキュリティ設定を指定すべき担当業務の区分の数はそれほど多くはないはずです。

ポリシーのプロファイルの使用との相違点と関連性

ポリシーのプロファイルは、各カスペルスキー製品に対して個別に作成されているポリシーのプロパティとして指定されています。ロールは、そうした様々なカスペルスキー製品に対して作成されている多数のプロファイルに 1 つのロールを関連付けることができます。つまり、ロールは、特定の種別のユーザーを対象とする複数の製品の設定を一元的に管理する目的で使用できます。

製品機能のアクセス権の設定：ロールベースのアクセス制御

Kaspersky Security Center Linux には、Kaspersky Security Center Linux と管理対象のカスペルスキー製品の機能へロールに基づくアクセスを提供する機能があります。

Kaspersky Security Center Linux ユーザーのアプリケーション機能へのアクセス権は、次のいずれかの方法で設定できます：

- 各ユーザーまたはユーザーグループに対する権限を個別に設定します。
- 事前定義された一連の権限を持つ標準のユーザーロールを作成し、職務の範囲に応じてそれらのロールをユーザーに割り当てる。

ユーザーロールの適用は、アプリケーション機能に対するユーザーのアクセス権を設定する定型的な手順を簡素化および短縮することを目的としています。ロール内のアクセス権は、標準タスクとユーザーの職務範囲に従って設定されます。

ユーザーロールには、それぞれの目的に対応する名前を割り当てることができます。作成できるロール数に制限はありません。

事前定義されたユーザーロールを設定済みの権限セットで使用することも、新しいロールを作成して必要な権限を自分で設定することもできます。

製品機能のアクセス権

次の表は、関連するタスク、レポート、設定を管理し、関連するユーザー操作を実行するためのアクセス権を備えた Kaspersky Security Center Linux の機能を示しています。

表に一覧表示されているユーザー操作を実行するには、ユーザーは操作内容の横に指定された権限を有している必要があります。

読み取り、**変更**、および**実行**の権限は、すべてのタスク、レポート、または設定に適用されます。これらの権限に加えて、ユーザーは、デバイスの抽出でタスクとレポートおよび設定を管理するため、**デバイスの抽出操作を実行**する権限を持っている必要があります。

表にないすべてのタスク、レポート、設定、およびインストールパッケージは、**一般的な機能：基本機能**にあります。

製品機能のアクセス権

機能領域	権限	ユーザー操作：操作を実行するために必要な権限	タスク	レポート	その他
一般的な機能：管理グループの管理	**変更**	• 管理グループへのデバイスの追加：**変更** • 管理グループからのデバイスの削除：**変更** • 別の管理グループへの管理グループの追加：**変更** • 別の管理グループからの管理グループの削除：**変更**	なし	なし	なし
一般的な機能：ACL にかかわらずオブジェクトにアクセスする	**読み取り**	すべてのオブジェクトへの読み取り権限の取得：**読み取り**	なし	なし	なし
一般的な機能：基本的な機能	• **読み取り** • **変更** • **実行** • **デバイスの抽出での操作の実行**	• 仮想サーバーのデバイス移動ルール（作成、変更、または削除）：**変更**、**デバイスの抽出に対する操作の実行** • モバイル（LWNGT）プロトコルのカスタム証明書の取得：**読み取り** • モバイル（LWNGT）プロトコルのカスタム証明書の取得：**書き込み** • NLA 定義のネットワークリストの取得：**読み取り**	• ［管理サーバーのリポジトリへのアップデートのダウンロード］ • ［レポートの配信］ • ［インストールパッケージの配布］ • ［セカンダリ管理サーバーへのアプリケーションのリモートインストール］	• ［保護ステータスレポート］ • ［脅威レポート］ • ［感染が多いデバイスのレポート］ • ［定義データベースのステータスレポート ］ • ［エラーレポート］ • ［ネットワーク攻撃のレポート］	なし

		• NLA 定義のネットワークリストの追加、変更、または削除：**変更** • グループのアクセスコントロールリストの表示：**読み取り** • Kaspersky イベントログの表示：**読み取り**		• ［インストールされている境界防御製品のサマリーレポート］ • ［インストールされているアプリケーションの種別のサマリーレポート］ • ［感染したデバイスのユーザーに関するレポート］ • ［インシデントのレポート］ • ［イベントのレポート］ • ［ディストリビューションポイントのアクティビティレポート］ • 「セカンダリ管理サーバーのレポート」 • ［デバイスコントロールイベントのレポート］ • ［ブロック対象アプリケーションのレポート］ • 「ウェブコントロールレポート」 • 「有効なユーザー権限のレポート」 • ［ユーザー権限のレポート］	
一般的な機能：削除されたオブジェクト	• **読み取り** • **変更**	• ごみ箱に削除されたオブジェクトの表示：**読み取り** • オブジェクトのごみ箱からの削除：**変更**	なし	なし	なし

一般的な機能：イベント処理	• **イベントの削除** • **イベント通知設定の編集** • **イベントログ設定の編集** • **変更**	• イベント登録設定の変更：**イベントログ設定の編集** • イベント通知設定の変更：**イベント通知設定の編集** • イベントの削除：**イベントの削除**	なし	なし	設定： • データベース内に保存されるイベント数の上限 • 削除されたデバイスからのイベントを保存する期間
一般的な機能：管理サーバー上での操作	• **読み取り** • **変更** • **実行** • **オブジェクト ACL の変更** • **デバイスの抽出での操作の実行**	• ネットワークエージェント接続用の管理サーバーのポートの指定：**変更** • 管理サーバーで開始された Activation Proxy のポートの指定：**変更** • 管理サーバーで開始された Activation Proxy for Mobile のポートの指定：**変更** • スタンドアロンパッケージを配布するための Web サーバーのポートの指定：**変更** • MDM プロファイルを配布するための Web サーバーのポートの指定：**変更** • Web コンソール経由で接続するための管理サーバーの SSL ポートを指定：**変更** • モバイル接続用の管理サーバーのポートの指定：**変更**	• ［管理サーバーデータのバックアップ］ • データベースのメンテナンス	なし	なし

		• 管理サーバーデータベースに記録するイベント数の上限の指定：**変更** • 管理サーバーが送信できるイベントの最大数の指定：**変更** • 管理サーバーがイベントを送信できる期間の指定：**変更**			
一般的な機能：カスペルスキー製品の導入	• **カスペルスキー製品のパッチの管理** • **読み取り** • **変更** • **実行** • **デバイスの抽出での操作の実行**	パッチのインストールの承認または拒否：**カスペルスキー製品のパッチの管理**	なし	• ［仮想管理サーバーによるライセンス使用のレポート］ • ［カスペルスキー製品バージョンレポート］ • ［互換性のないアプリケーションのレポート］ • ［カスペルスキー製品のモジュールアップデートのバージョンに関するレポート］ • ［製品導入レポート］	インストールパッケージ：「カスペルスキー」
一般的な機能：ライセンス管理	• **ライセンス情報ファイルのエクスポート** • **変更**	• ライセンス情報ファイルのエクスポート：**ライセンス情報ファイルのエクスポート** • 管理サーバーのライセンス情報の設定の変更：**変更**	なし	なし	なし
一般的な機能：適用されたレポートの管理	• **読み取り** • **変更**	• ACL にかかわらずレポートを作成：**書き込み** • ACL にかかわらずレポートを実行：**読み**	なし	なし	なし

		取り			
一般的な機能：管理サーバーの階層構造	**管理サーバー階層の設定**	• セカンダリ管理サーバーの登録、アップデート、または削除：**管理サーバー階層の設定**	なし	なし	なし
一般的な機能：ユーザー権限	**オブジェクト ACL の変更**	• 任意のオブジェクトのセキュリティプロパティの変更：**オブジェクト ACL の変更** • ユーザーロールの管理：**オブジェクト ACL の変更** • 内部ユーザーの管理：**オブジェクト ACL の変更** • セキュリティグループの管理：**オブジェクト ACL の変更** • エイリアスの管理：**オブジェクト ACL の変更**	なし	なし	なし
一般的な機能：仮想管理サーバー	• **仮想管理サーバーの管理** • **読み取り** • **変更** • **実行** • **デバイスの抽出での操作の実行**	• 仮想管理サーバーのリストの取得：**読み取り** • 仮想管理サーバーに関する情報の取得：**読み取り** • 仮想管理サーバーの作成、更新、または削除：**仮想管理サーバーの管理** • 仮想管理サーバーの別のグループへの移動：**仮想管理サーバーの管理** • 仮想管理サーバーの権限の設定：**仮想管理サーバーの管理**	なし	なし	なし

事前定義のユーザーロール

Kaspersky Security Center Linux のユーザーに割り当てられたユーザーロールによって、アプリケーション機能への一連のアクセス権がユーザーに付与されます。

一連の権限が既に設定されている事前定義済みのユーザーロールを使用するか、新規のロールを作成して必要な権限を自分で設定できます。Kaspersky Security Center Linux で使用可能な事前定義済みのユーザーロールの一部は、**監査**、**セキュリティ責任者**、**監督者**などの特定の役職に関連付けることができます。これらのロールのアクセス権は、関連する役職の標準タスクと職務の範囲に従って事前設定されています。次の表に、役割を特定の職位に関連付ける方法を示します。

特定の職位の役割の例

ロール	コメント
監査	削除されたオブジェクトの表示を含む、すべてのタイプのレポートでのすべての操作、すべての表示操作を許可します（［**削除されたオブジェクト**］領域で［**読み取り**］および［**書き込み**］の許可を付与します）。他の操作は許可されません。このロールは、組織の監査を実行する人に割り当てることができます。
上長・監督者	すべての表示操作を許可します。他の操作は許可されません。組織の IT セキュリティを担当しているセキュリティ責任者やその他のマネージャーにこのロールを割り当てることができます。
セキュリティ責任者	すべての表示操作を許可し、レポート管理を許可します。**システム管理**：**接続**領域で制限付きのアクセス許可を付与します。組織の IT セキュリティを担当しているセキュリティ責任者にこのロールを割り当てることができます。

次の表に、事前定義された各ユーザーロールに割り当てられているアクセス権を示します。

機能領域［**モバイルデバイス管理：全般**］および［**システム管理**］の機能は Kaspersky Security Center Linux では使用できません。「**脆弱性とパッチ管理の管理者 / オペレーター**」、および「**モバイルデバイス管理の管理者 / オペレーター**」には［**一般的な機能**：**基本**］機能領域の権限のみにアクセス権があります。

事前定義されたユーザーロールのアクセス権

ロール	説明
管理サーバーの管理者	［**一般的な機能**］の次の機能領域におけるすべての操作を許可します： • **基本機能** • **イベント処理** • **管理サーバーの階層構造** • **仮想管理サーバー**
管理サーバーのオペレーター	［**一般的な機能**］の次のすべての機能領域で、**読み取り**および**実行**権限を付与します： • **基本機能**

	• **仮想管理サーバー**
監査	［**一般的な機能**］の次の機能領域におけるすべての操作を許可します： • **ACL にかかわらずオブジェクトにアクセスする** • **削除されたオブジェクト** • **適用されたレポートの管理** このロールは、組織の監査を実行する人に割り当てることができます。
インストールの管理者	［**一般的な機能**］の次の機能領域におけるすべての操作を許可します： • **基本機能** • **カスペルスキー製品の導入** • **ライセンス管理** ［**一般的な機能：仮想管理サーバー**］機能領域における**読み取り**と**実行**の権限を付与します。
インストールのオペレーター	［**一般的な機能**］の次のすべての機能領域で、**読み取り**および**実行**権限を付与します： • **基本機能** • **カスペルスキー製品の導入**（この領域での**カスペルスキー製品のパッチ管理**の権限も付与します） • **仮想管理サーバー**
Kaspersky Endpoint Security の管理者	次の機能領域でのすべての操作を許可します： • **一般的な機能：基本的な機能** • すべての機能を含む Kaspersky Endpoint Security のエリア
Kaspersky Endpoint Security オペレーター	次のすべての機能領域で**読み取り**および**実行**権限を付与します： • **一般的な機能：基本的な機能** • すべての機能を含む Kaspersky Endpoint Security のエリア
メインの管理者	次の領域を*除く*、**一般的な機能**の機能領域でのすべての操作を許可します。 • **ACL にかかわらずオブジェクトにアクセスする** • **適用されたレポートの管理**
メインのオペレーター	次のすべての機能領域で**読み取り**および**実行**（該当する場合）権限を付与します： • **一般的な機能**： • **基本機能** • **削除されたオブジェクト**

	• **管理サーバー上での操作** • **カスペルスキー製品の導入** • **仮想管理サーバー** • すべての機能を含む Kaspersky Endpoint Security のエリア
モバイルデバイス管理の管理者	［**一般的な機能：基本機能**］の機能領域ですべての操作を許可します。
セキュリティ責任者	［**一般的な機能**］の次の機能領域におけるすべての操作を許可します： • **ACL にかかわらずオブジェクトにアクセスする** • **適用されたレポートの管理** **読み取り**、**変更**、**実行**、**デバイスから管理者のワークステーションへのファイルの保存**、［**システム管理：接続**］機能領域での［**デバイスの抽出での操作の実行**］を許可します。 組織の IT セキュリティを担当しているセキュリティ責任者にこのロールを割り当てることができます。
セルフサービスポータルのユーザー	［**モバイルデバイス管理：セルフサービスポータル**］機能領域におけるすべての操作を許可します。この機能は、Kaspersky Security Center のバージョン 11 以降ではサポートされていません。
上長・監督者	［**一般的な機能**：**ACL に依存せずオブジェクトにアクセスする**］と［**一般的な機能**：**適用されたレポートの管理**］の機能領域における**読み取り**権限を付与します。 組織の IT セキュリティを担当しているセキュリティ責任者やその他のマネージャーにこのロールを割り当てることができます。

内部ユーザーのアカウントの追加

Kaspersky Security Center Linux に新しい内部ユーザーアカウントを追加するには：

1. メインメニューで、［**ユーザーとロール**］→［**ユーザー**］の順に選択します。
2. ［**追加**］をクリックします。
3. ［**エンティティの新規作成**］ウィンドウで、新しいユーザーアカウントの設定を指定します：
   - **ユーザー**：既定でオンになっているのでこれを選択したままにします。
   - **名前**
   - **パスワード**：Kaspersky Security Center Linux へのユーザーの接続用。
     パスワードは次のルールに従う必要があります：
     - パスワードは、8 文字以上 16 文字以下にしてください。
     - パスワードでは、次の文字種別のうち 3 つ以上を組み合わせてください。

- アルファベット大文字（A-Z）
- アルファベット小文字（a-z）
- 数字（0 - 9）
- 特殊文字（@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;）

- パスワードに空白文字や Unicode 文字を含めることはできません。また「.」の後に続けて「@」を入力することは避けてください。

入力した文字を表示するには、［**表示**］を押し続けます。

パスワードの入力試行回数には制限があります。既定では、許可されるパスワードの入力試行回数の上限は 10 回です。「許可されるパスワード入力試行回数の変更」の説明に従って、許可されるパスワードの入力試行回数を変更できます。

ユーザーが無効なパスワードを指定された回数以上入力すると、ユーザーアカウントは 1 時間ブロックされます。パスワードを変更することでのみ、ユーザーアカウントのロックを解除できます。

- **完全名**
- **説明**
- **メールアドレス**
- **電話番号**

4. ［OK］をクリックして変更内容を保存します。

ユーザーとユーザーグループのリストに新しいユーザーアカウントが表示されます。

ユーザーグループの作成

ユーザーグループを作成するには：

1. メインメニューで、［**ユーザーとロール**］→［**ユーザー**］の順に選択します。
2. ［**追加**］をクリックします。
3. 表示される［**エンティティの新規作成**］ウィンドウで、［**グループ**］をオンにします。
4. 新しいユーザーグループに次の設定を行います：
   - **グループ名**
   - **説明**
5. ［OK］をクリックして変更内容を保存します。

ユーザーとユーザーグループのリストに新しいユーザーグループが表示されます。

内部ユーザーのアカウントの編集

Kaspersky Security Center Linux で内部ユーザーアカウントを編集するには：

1. メインメニューで、［**ユーザーとロール**］→［**ユーザー**］の順に選択します。
2. 編集するユーザーアカウントの名前をクリックします。
3. ユーザー設定ウィンドウが表示されるので、［**全般**］タブで、ユーザーアカウントの設定を変更します：
   - **説明**
   - **完全名**
   - **メールアドレス**
   - **電話番号**
   - **パスワード**：Kaspersky Security Center Linux へのユーザーの接続用。
     パスワードは次のルールに従う必要があります：
     - パスワードは、8 文字以上 16 文字以下にしてください。
     - パスワードでは、次の文字種別のうち 3 つ以上を組み合わせてください。
       - アルファベット大文字（A-Z）
       - アルファベット小文字（a-z）
       - 数字（0 - 9）
       - 特殊文字（@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;）
     - パスワードに空白文字や Unicode 文字を含めることはできません。また「.」の後に続けて「@」を入力することは避けてください。

     入力したパスワードを表示するには、［**入力した文字を表示する**］をクリックしたままにします。

     > パスワードの入力試行回数には制限があります。既定では、許可されるパスワードの入力試行回数の上限は 10 回です。許可される試行回数は変更することができます。ただし、セキュリティ上の理由から、この回数を減らすことはお勧めしません。ユーザーが無効なパスワードを指定された回数以上入力すると、ユーザーアカウントは 1 時間ブロックされます。パスワードを変更することでのみ、ユーザーアカウントのロックを解除できます。
   - 必要に応じて、スイッチを［**無効**］に切り替えることで、ユーザーの本製品への接続をブロックできます。たとえば、従業員が退職したあとなどにアカウントを無効化できます。
4. ［**認証セキュリティ**］タブで、このアカウントに対するセキュリティ設定を指定できます。

5. ［**グループ**］タブで、セキュリティグループにユーザーを追加できます。
6. ［**デバイス**］タブで、ユーザーにデバイスを割り当てることができます。
7. ［**ロール**］タブで、ユーザーにロールを割り当てることができます。
8. ［**保存**］をクリックして変更内容を保存します。

ユーザーとセキュリティグループのリストに更新したユーザーアカウントが表示されます。

ユーザーグループの編集

編集できるのは内部グループのみです。

ユーザーグループを編集するには：

1. メインメニューで、［**ユーザーとロール**］→［**ユーザー**］の順に選択します。
2. 編集するユーザーグループの名前をクリックします。
3. グループの設定ウィンドウが表示されるので、ユーザーグループの設定を変更します。
   - **名前**
   - **説明**
4. ［**保存**］をクリックして変更内容を保存します。

ユーザーとユーザーグループのリストに更新したユーザーグループが表示されます。

内部グループへのユーザーアカウントの追加

内部グループに追加できるのは内部ユーザーのアカウントのみです。

ユーザーアカウントを内部グループに追加するには：

1. メインメニューで、［**ユーザーとロール**］→［**ユーザー**］の順に選択します。
2. グループに追加するユーザーアカウントに隣接するチェックボックスをオンにします。
3. ［**グループの割り当て**］をクリックします。
4. 表示される［**グループの割り当て**］ウィンドウで、ユーザーアカウントを追加するグループを選択します。
5. ［**割り当て**］をクリックします。

ユーザーアカウントがグループに追加されます。

デバイスの所有者ユーザーの指定

ユーザーをモバイルデバイスの所有者として割り当てる方法の詳細については、Kaspersky Security for Mobile のヘルプを参照してください。

デバイスの所有者ユーザーを指定するには：

1. メインメニューで、［**ユーザーとロール**］→［**ユーザー**］の順に選択します。
2. デバイスの所有者に割り当てるユーザーアカウントの名前をクリックします。
3. ユーザー設定ウィンドウが表示されたら、［**デバイス**］を選択します。
4. ［**追加**］をクリックします。
5. デバイスリストから、ユーザーに割り当てるデバイスを選択します。
6. ［**OK**］をクリックします。

選択したデバイスが、ユーザーに割り当てられているデバイスのリストに追加されます。

［**デバイス**］→［**管理対象デバイス**］で割り当てるデバイスをクリックし、［**デバイスの所有者の管理**］をクリックする方法でも、同じ処理を実行できます。

ユーザーとセキュリティグループの削除

削除できるのは内部ユーザーまたは内部セキュリティグループのみです。

ユーザーまたはセキュリティグループを削除するには：

1. メインメニューで、［**ユーザーとロール**］→［**ユーザー**］の順に選択します。
2. 削除するユーザーまたはセキュリティグループの隣にあるチェックボックスをオンにします。
3. ［**削除**］をクリックします。
4. 表示されたウィンドウで［**OK**］をクリックします。

選択したユーザーまたはセキュリティグループが削除されます。

ユーザーロールの作成

ユーザーロールを作成するには：

1. メインメニューで、［**ユーザーとロール**］→［**ロール**］の順に選択します。
2. ［**追加**］をクリックします。
3. ［**新しいロール名**］ウィンドウが開いたら、新しいロールの名前を入力します。
4. ［**OK**］をクリックして変更を適用します。
5. ロールのプロパティウィンドウが開いたら、ロールの設定を変更します：
   - ［**全般**］タブで、ロール名を編集します。
     事前定義のロールの名前は編集できません。
   - ［**設定**］タブで、ロールの範囲とポリシー、ロールに関連付けられているプロファイルを編集します。
   - ［**アクセス権**］タブで、カスペルスキー製品へのアクセス権を編集します。
6. ［**保存**］をクリックして変更内容を保存します。

ユーザーロールのリストに新しいロールが表示されます。

ユーザーロールの編集

ユーザーロールを編集するには：

1. メインメニューで、［**ユーザーとロール**］→［**ロール**］の順に選択します。
2. 編集するロールの名前をクリックします。
3. ロールのプロパティウィンドウが開いたら、ロールの設定を変更します：
   - ［**全般**］タブで、ロール名を編集します。
     事前定義のロールの名前は編集できません。
   - ［**設定**］タブで、ロールの範囲とポリシー、ロールに関連付けられているプロファイルを編集します。
   - ［**アクセス権**］タブで、カスペルスキー製品へのアクセス権を編集します。
4. ［**保存**］をクリックして変更内容を保存します。

ユーザーロールのリストに更新したロールが表示されます。

各ユーザーロールの対象範囲の編集

*ユーザーロールの対象範囲*は、「ユーザーへの割り当て」と「管理グループへの関連付け」の 2 つの要素の組み合わせとして定義されます。ユーザーロールと関連付けられた設定は、ロールに関連付けられたグループ（子グループを含む）にデバイスが属し、なおかつそのロールを割り当てられたユーザーが所有しているデバイスのみに適用されます。

ユーザーロールの対象範囲にユーザー、セキュリティグループ、管理グループを追加するには、次のいずれかの方法を使用できます：

方法 1：

1. メインメニューで、［**ユーザーとロール**］→［**ユーザー**］の順に選択します。
2. ユーザーロールの対象範囲に追加するユーザーとセキュリティグループに隣接するチェックボックスをオンにします。
3. ［**ロールの割り当て**］をクリックします。
   ロールの割り当てウィザードが開始します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。
4. ウィザードの［**ロールの選択**］ウィンドウで、割り当てるロールを選択します。
5. ウィザードの［**範囲の定義**］ウィンドウで、ユーザーロールの対象範囲に追加する管理グループを選択します。
6. ［**ロールの割り当て**］をクリックしてウィザードを終了します。

選択したユーザーまたはセキュリティグループと、選択した管理グループが、ユーザーロールの対象範囲に追加されます。

方法 2：

1. メインメニューで、［**ユーザーとロール**］→［**ロール**］の順に選択します。
2. 対象範囲を指定するロールの名前をクリックします。
3. ロールのプロパティウィンドウが開いたら、［**設定**］タブをクリックします。
4. ［**ロールの対象範囲**］セクションで、［**追加**］をクリックします。
   ロールの割り当てウィザードが開始します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。
5. ウィザードの［**範囲の定義**］ウィンドウで、ユーザーロールの対象範囲に追加する管理グループを選択します。
6. ウィザードの［**ユーザーを選択してください**］ウィンドウで、ユーザーロールの対象範囲に追加するユーザーとセキュリティグループを選択します。
7. ［**ロールの割り当て**］をクリックしてウィザードを終了します。
8. ロールのプロパティウィンドウを閉じます。

選択したユーザーまたはセキュリティグループと、選択した管理グループが、ユーザーロールの対象範囲に追加されます。

ユーザーロールの削除

ユーザーロールを削除するには：

1. メインメニューで、［**ユーザーとロール**］→［**ロール**］の順に選択します。
2. 削除するロールに隣接するチェックボックスをオンにします。
3. ［**削除**］をクリックします。
4. 表示されたウィンドウで［**OK**］をクリックします。

選択したユーザーロールが削除されます。

ポリシーのプロファイルとロールの関連付け

ユーザーロールはポリシーのプロファイルに関連付けることができます。この場合、ポリシーのプロファイルの有効化ルールがベースにしているのはロールです：ポリシーのプロファイルは、指定したロールを持つユーザーに対してアクティブにされます。

たとえば、管理グループ内のすべてのデバイスに対して GPS ナビゲーションソフトウェアの使用を禁止するポリシーがあるとします。管理グループ「ユーザー」内に配達担当者が所有するデバイスが1台存在しており、そのデバイスでのみ GPS ナビゲーションソフトウェアを使用する必要があるとします。この場合、デバイスの所有者に「配達担当者」ロールを割り当てて、「配達担当者」ロールが割り当てられた所有者のデバイスでのみ使用できるように、GPS ナビゲーションソフトウェアを許可するポリシーのプロファイルを作成できます。その他のポリシー設定はいずれも変更されません。「配達担当者」ロールが割り当てられたユーザーのみが、GPS ナビゲーションソフトウェアを使用できるようになります。後で別の担当者に「配達担当者」ロールを割り当てた場合、その新規担当者も組織のデバイスでナビゲーションソフトウェアを使用できるようになります。同じ管理グループ内の他のデバイスでは、GPS ナビゲーションソフトウェアの使用は禁止されたままになります。

ロールとポリシーのプロファイルを関連付けるには：

1. メインメニューで、［**ユーザーとロール**］→［**ロール**］の順に選択します。
2. ポリシーのプロファイルと関連付けるロール名をクリックします。
   ロールのプロパティウィンドウの［**全般**］タブが表示されます。
3. ［**設定**］タブを選択して、［**ポリシーとプロファイル**］セクションまでスクロールします。
4. ［**編集**］をクリックします。
5. ロールを関連付けるには：
   - **既存のポリシーのプロファイル**– 該当するポリシー名の横にあるアイコン（>）をクリックして、ロールを関連付けるプロファイルの横にあるチェックボックスをオンにします。
   - **新しいポリシーのプロファイル**：
     a. プロファイルを作成するポリシーの横にあるチェックボックスをオンにします。

b. ［**ポリシーのプロファイルの新規作成**］をクリックします。

c. 新しいプロファイル名を指定して、プロファイルを設定します。

d. ［**保存**］をクリックします。

e. 新しいプロファイルの横にあるチェックボックスをオンにします。

6. ［**ロールへの割り当て**］をクリックします。

プロファイルがロールに関連付けられてロールのプロパティに表示されます。担当者が当該ロールに割り当てられているデバイスに対して、プロファイルが自動的に適用されます。

オブジェクトリビジョンの管理

このセクションでは、オブジェクトのリビジョン管理について説明します。Kaspersky Security Center Linux では、オブジェクトの変更を追跡できます。オブジェクトに変更を加えるたびに、*リビジョン*が作成されます。各リビジョンには番号が付いています。

リビジョン管理に対応するアプリケーションオブジェクトは次の通りです：

- 管理サーバー
- ポリシー
- タスク
- 管理グループ
- ユーザーアカウント
- インストールパッケージ

オブジェクトのリビジョンには次の処理を行うことができます：

- 選択したリビジョンを現在のリビジョンと比較する
- 選択したリビジョンを比較
- 同じ種別の別のオブジェクトのリビジョンを比較対象として選択し、オブジェクトと比較する
- 選択したリビジョンを表示する
- オブジェクトに対して行った変更を、選択したリビジョンにロールバックする
- リビジョンをテキストファイルとして保存する

リビジョン管理に対応するオブジェクトのプロパティウィンドウの［**変更履歴**］セクションには、オブジェクトのリビジョンのリストが次の詳細とともに表示されます：

- オブジェクトのリビジョン番号
- オブジェクトが変更された日時

- オブジェクトを変更したユーザーの名前
- オブジェクトに対する操作
- オブジェクト設定に対して行われた変更に関連するリビジョンの説明

  既定では、オブジェクトのリビジョンの説明は空になっています。リビジョンに説明を追加するには、関連するリビジョンを選択して、［**説明**］をクリックします。［**オブジェクトのリビジョンの説明**］ウィンドウで、リビジョンの説明を入力します。

オブジェクトリビジョンについて

オブジェクトのリビジョンには次の処理を行うことができます：

- 選択したリビジョンを現在のリビジョンと比較する
- 選択したリビジョンを比較
- 同じ種別の別のオブジェクトのリビジョンを比較対象として選択し、オブジェクトと比較する
- 選択したリビジョンを表示する
- オブジェクトに対して行った変更を、選択したリビジョンにロールバックする
- リビジョンをテキストファイルとして保存する

リビジョン管理に対応するオブジェクトのプロパティウィンドウの［**変更履歴**］セクションには、オブジェクトのリビジョンのリストが次の詳細とともに表示されます：

- オブジェクトのリビジョン番号
- オブジェクトが変更された日時
- オブジェクトを変更したユーザーの名前
- オブジェクトに対する操作
- オブジェクト設定に対して行われた変更に関連するリビジョンの説明

以前のリビジョンへのオブジェクトのロールバック

必要に応じて、オブジェクトの変更をロールバックできます。たとえば、ポリシーの設定を特定の日付の状態まで戻さなければならない場合があります。

オブジェクトの変更をロールバックするには：

1. オブジェクトのプロパティウィンドウで［**変更履歴**］タブを表示します。
2. オブジェクトのリビジョンのリストで、変更のロールバック先となるリビジョンを選択します。
3. ［**ロールバック**］をクリックします。

4. ［OK］をクリックして処理内容を確定します。

オブジェクトが、選択したリビジョンにロールバックされます。オブジェクトのリビジョンのリストには、実行された処理の記録が表示されます。リビジョンの説明には、オブジェクトを元に戻したリビジョン番号に関する情報が表示されます。

ロールバック操作は、ポリシーオブジェクトとタスクオブジェクトでのみ使用できます。

オブジェクトの削除

このセクションでは、オブジェクトの削除と、削除後にオブジェクトの情報を表示する方法について説明します。

次のオブジェクトを削除できます：

- ポリシー
- タスク
- インストールパッケージ
- 仮想管理サーバー
- ユーザー
- セキュリティグループ
- 管理グループ

オブジェクトを削除しても、オブジェクトの情報はデータベースに保存されます。削除されたオブジェクトの情報の保存期間は、オブジェクトの履歴の保存期間（推奨期間は 90 日）と同じです。［**削除されたオブジェクト**］領域の権限で**変更**権限を付与されたユーザーのみが、保存期間を変更できます。

klscflag を使用したポート 13291 の開放

管理サーバーのポート 13291 は管理コンソール（MMC ベースの管理コンソールを含みます）からの接続を受け取るために使用されます。Windows 以外のコンピューターでは、既定でこのポートは閉じられています。

MMC ベースの管理コンソールへの接続を許可する、または klakaut ユーティリティを使用する場合は、klscflag ユーティリティを使用してこのポートを開くことができます。Kaspersky Security Center に接続すると、MMC ベースの管理コンソールの機能が低下することに注意してください。

klscflag ユーティリティは KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN パラメータの値を変更します。

Web コンソールを使用して Kaspersky Security Center に接続することを推奨します。

ポート 13291 を開くには：

1. コマンドラインで次のコマンドを実行します：
   ```
   $ /opt/kaspersky/ksc64/sbin/klscflag -ssvset -pv klserver -s 87 -n
   KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -sv true -svt BOOL_T -ss "|ss_type =
   \"SS_SETTINGS\";"
   ```

2. 次のコマンドを実行して Kaspersky Security Center 管理サーバーサービスを再起動します：
   ```
   $ sudo systemctl restart kladminserver_srv
   ```

ポート 13291 が開きます。

ポート 13291 が正常に開かれたことを確認するには：

コマンドラインで次のコマンドを実行します：

```
$ /opt/kaspersky/ksc64/sbin/klscflag -ssvget -pv klserver -s 87 -n
KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"
```

このコマンドは次の結果を返します：

```
+--- (PARAMS_T)
+---KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN = (BOOL_T)true
```

値「`true`」はポートが開かれていることを意味します。それ以外の場合は値「`false`」が表示されます。

定義データベースとカスペルスキー製品のアップデート

このセクションでは、次の対象の定期的なアップデートに必要な手順について説明します。

- 定義データベースとソフトウェアモジュール
- インストール済みのカスペルスキー製品（Kaspersky Security Center コンポーネントとセキュリティ製品を含む）

シナリオ：定義データベースとカスペルスキー製品の定期的なアップデート

このセクションでは、定義データベース、ソフトウェアモジュール、カスペルスキー製品の定期的なアップデートを行う手順について説明します。ネットワーク保護の設定手順の完了後、管理サーバーと管理対象デバイスがウイルス、ネットワーク攻撃、フィッシング攻撃などの様々な脅威から常に保護されるよう、保護システムの信頼性を維持する必要があります。

ネットワーク保護を最新の状態に維持する定期的なアップデートは次の通りです：

- 定義データベースとソフトウェアモジュール
- インストール済みのカスペルスキー製品（Kaspersky Security Center コンポーネントとセキュリティ製品を含む）

この手順を完了すると、次の状態を実現できます：

- ネットワークが最新のカスペルスキー製品（Kaspersky Security Center Linux コンポーネントとセキュリティ製品を含む）で保護されている。
- ネットワークのセキュリティレベルにとって重要な定義データベースとその他のカスペルスキーのデータベースが常に最新である。

必須条件

管理対象デバイスが管理サーバーに接続している必要があります。接続していない場合は、定義データベースとソフトウェアモジュールの手動アップデート、またはカスペルスキーのアップデートサーバーからの直接アップデートを検討してください。

管理サーバーはインターネットに接続している必要があります。

導入を開始する前に、次が完了していることを確認してください：

1. Kaspersky Security Center 14 Web コンソールを使用したカスペルスキー製品の導入手順に従って、カスペルスキーのセキュリティ製品を管理対象デバイスに導入した。
2. ネットワーク保護の設定手順に従って、必要なすべてのポリシー、ポリシーのプロファイル、タスクを作成して設定した。
3. 管理対象デバイスの数とネットワークトポロジーに従って、適切な数のディストリビューションポイントを割り当てた。

定義データベースとカスペルスキー製品のアップデート手順は次の通りです：

1 アップデートスキームの選択

Kaspersky Security Center コンポーネントとセキュリティ製品に対するアップデートのインストールには、複数のスキームを使用できます。ネットワークの要件に最も合致するスキームを選択してください（複数のスキームを組み合わせることもできます）。

2 ［管理サーバーのリポジトリへのアップデートのダウンロード］タスクの作成

このタスクは、Kaspersky Security Center のクイックスタートウィザードによって自動的に作成されます。ウィザードを実行していない場合は、次の手順に進む前にタスクを作成してください。

カスペルスキーのアップデートサーバーから管理サーバーのリポジトリへのアップデートのダウンロード、および定義データベースと Kaspersky Security Center のソフトウェアモジュールのアップデートには、このタスクが必要です。アップデートのダウンロード後、管理対象デバイスにこれらのアップデートを配信できます。

ネットワークにディストリビューションポイントが割り当てられている場合、アップデートは管理サーバーのリポジトリからディストリビューションポイントのリポジトリに自動的にダウンロードされます。この場合、ディストリビューションポイントの範囲に含まれる管理対象デバイスは、管理サーバーのリポジトリではなくディストリビューションポイントのリポジトリからアップデートをダウンロードします。

実行手順の説明：［管理サーバーのリポジトリへのアップデートのダウンロード］タスクの作成

3 ［ディストリビューションポイントのリポジトリにアップデートをダウンロード］タスクの作成（オプション）

既定では、管理サーバーからディストリビューションポイントにアップデートがダウンロードされます。カスペルスキーのアップデートサーバーからディストリビューションポイントにアップデートを直接ダウンロードするように Kaspersky Security Center を設定できます。ディストリビューションポイントのリポジトリへのダウンロードが推奨されるのは、管理サーバーとディストリビューションポイント間の通信の方がディストリビューションポイントとカスペルスキーのアップデートサーバー間の通信よりも費用がかかる場合や、管理サーバーがインターネットにアクセスできない場合などです。

ネットワークにディストリビューションポイントが割り当てられており、［*ディストリビューションポイントのリポジトリにアップデートをダウンロード*］タスクが作成されている場合、ディストリビューションポイントは、管理サーバーのリポジトリではなくカスペルスキーのアップデートサーバーからアップデートをダウンロードします。

実行手順の説明：［ディストリビューションポイントのリポジトリにアップデートをダウンロード］タスクの作成

4 ディストリビューションポイントの設定

ネットワークにディストリビューションポイントが割り当てられている場合、設定が必要なすべてのディストリビューションポイントのプロパティで［**アップデートの配信**］がオンになっていることを確認します。ディストリビューションポイントでこのオプションがオフになっていると、ディストリビューションポイントの範囲に含まれるデバイスは管理サーバーのリポジトリからアップデートをダウンロードします。

5 差分ファイルの使用によるアップデート処理の最適化（省略可能）

差分ファイルを使用することで管理サーバーと管理対象デバイス間のトラフィックを最適化することができます。この機能を有効にすると、管理サーバーまたはディストリビューションポイントは定義データベースまたはソフトウェアモジュールのファイル全体ではなく差分ファイルをダウンロードします。差分ファイルには、定義データベースファイルまたはソフトウェアモジュールファイルの異なる 2 バージョン間の変更点のみが含まれています。したがって、差分ファイルの方がファイル全体より容量が小さくなります。これにより、管理サーバーと管理対象デバイス間またはディストリビューションポイントと管理対象デバイス間のトラフィックを削減できます。この機能を使用するには、［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクや、［*ディストリビューションポイントのリポジトリにアップデートをダウンロード*］タスク、またはその両方のプロパティで［**差分ファイルのダウンロード**］をオンにします。

実行手順の説明：カスペルスキー製品の定義データベースとソフトウェアモジュールのアップデートでの差分ファイルの使用

6 セキュリティ製品のアップデートとパッチの自動インストールの設定

管理対象の製品の *アップデート*タスクを作成して、ソフトウェアモジュール、および定義データベースをタイムリーにアップデートします。タイムリーにアップデートされるようにするため、タスクスケジュールの設定時に［**新しいアップデートがリポジトリにダウンロードされ次第**］をオンにすることを推奨します。

ネットワークに IPv6 のみのデバイスが含まれていて、それらのデバイス上にインストールされているセキュリティ製品を定期的にアップデートする場合、管理対象デバイス上にバージョン 13.2 の管理サーバーとバージョン 13.2 のネットワークエージェントがインストールされていることを確認してください。

使用許諾契約書の条項の確認と同意がアップデートに必要な場合は、最初に条項に同意する必要があります。その後、アップデートを管理対象デバイスに配信できます。

結果

すべての手順を完了すると、管理サーバーのリポジトリにアップデートがダウンロードされた後で、カスペルスキーのデータベースをアップデートするように Kaspersky Security Center Linux が設定されます。続いて、ネットワークステータスの監視を設定できます。

定義データベース、ソフトウェアモジュール、カスペルスキー製品のアップデートの概要

管理サーバーと管理対象デバイスの保護が最新の状態であるようにするには、次の項目のタイムリーなアップデートが必要です：

- 定義データベースとソフトウェアモジュール

  Kaspersky Security Center は、カスペルスキーのデータベースとソフトウェアをダウンロードする前にカスペルスキーのサーバーがアクセス可能かどうかをチェックします。システム DNS を使用したサーバーへのアクセスが不可能な場合は、パブリック DNS を使用します。これは、定義データベースを最新の状態に保ち、管理対象デバイスのセキュリティレベルを確実に管理するために必要です。

- インストール済みのカスペルスキー製品（Kaspersky Security Center コンポーネントとセキュリティ製品を含む）

  Kaspersky Security Center はカスペルスキー製品を自動でアップデートすることはできません。製品をアップデートするには、カスペルスキーの Web サイトから最新バージョンの製品をダウンロードして、手動でインストールしてください：

  - Kaspersky Security Center 管理サーバー、Kaspersky Security Center 14 Web コンソール
  - ネットワークエージェント、Kaspersky Endpoint Security for Linux、Web 管理プラグイン

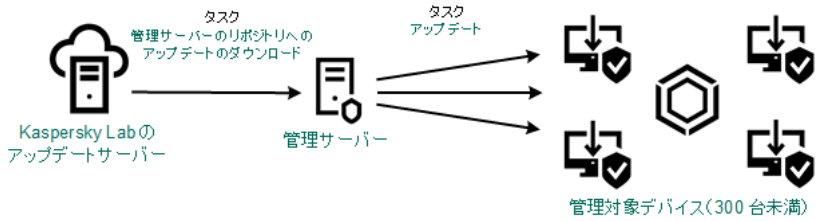
ネットワークの設定に応じて、管理対象デバイスへの必要なアップデートのダウンロードと配信に次のスキームを使用できます：

- 単一のタスク［*管理サーバーのリポジトリへのアップデートのダウンロード*］の使用
- 次の 2 つのタスクの使用：
  - *［管理サーバーのリポジトリへのアップデートのダウンロード］タスク*
  - *ディストリビューションポイントのリポジトリにアップデートをダウンロードタスク*
- ローカルフォルダー、共有フォルダー、または FTP サーバーを使用して手動で実行

- カスペルスキーのアップデートサーバーから管理対象デバイスの Kaspersky Endpoint Security for Linux を直接アップデート
- 管理サーバーがインターネットに接続されていない場合は、ローカルまたはネットワークフォルダー経由

管理サーバーのリポジトリへのアップデートのダウンロードタスクの使用

このスキームでは、Kaspersky Security Center は *管理サーバーのリポジトリへのアップデートのダウンロード* タスクを使用してアップデートをダウンロードします。単一のネットワークセグメントで構成され管理対象デバイスが 300 台未満、または複数のセグメントに分かれているが各ネットワークセグメントに含まれる管理対象デバイスが 10 台未満の小規模ネットワークでは、管理サーバーのリポジトリから管理対象デバイスにアップデートが直接配信されます（次の図を参照）。



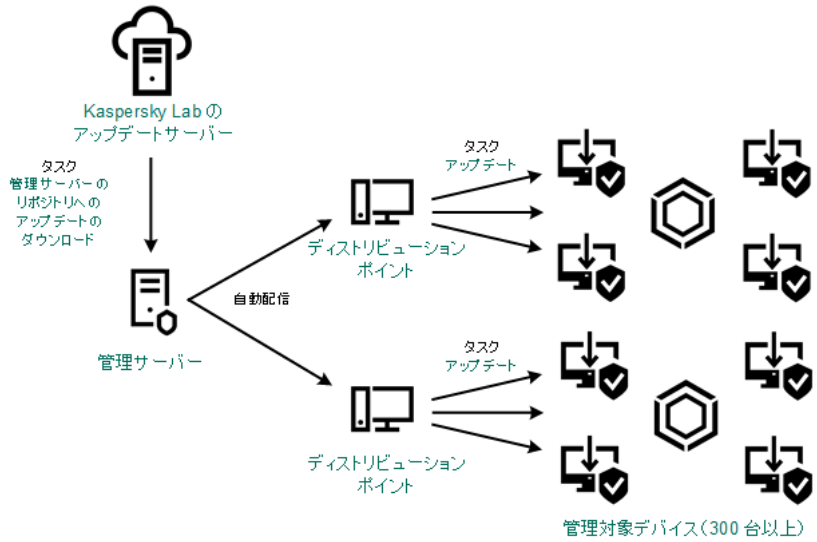
ディストリビューションポイントを使用しない、管理サーバーのリポジトリへのアップデートのダウンロードタスクによるアップデート

アップデート元として、カスペルスキーのアップデートサーバーだけでなく、ローカルまたはネットワークフォルダーを使用することもできます：

既定では、管理サーバーは HTTPS プロトコルを使用してカスペルスキーのアップデートサーバーに接続し、アップデートをダウンロードします。必要に応じて、管理サーバーで HTTPS プロトコルの代わりに HTTP プロトコルを使用するように設定を編集できます。

単一のネットワークセグメントで構成され管理対象デバイスが 300 台以上、または複数のセグメントに分かれていて各ネットワークセグメントに含まれる管理対象デバイスが 10 台以上のネットワークの場合は、ディストリビューションポイントを使用して管理対象デバイスにアップデートを配信することを推奨します（次の図を参照）。ディストリビューションポイントは管理サーバーの負荷を低減し、管理サーバーと管理対象デバイス間のトラフィックを最適化します。ネットワークに必要なディストリビューションポイントの数と設定を計算できます。

このスキームでは、アップデートは管理サーバーのリポジトリからディストリビューションポイントのリポジトリに自動的にダウンロードされます。ディストリビューションポイントの範囲に含まれる管理対象デバイスは、管理サーバーのリポジトリではなくディストリビューションポイントのリポジトリからアップデートをダウンロードします。



ディストリビューションポイントを使用した、管理サーバーのリポジトリへのアップデートのダウンロードタスクによるアップデート

［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクが完了すると、カスペルスキーのデータベースと Kaspersky Endpoint Security for Linux ソフトウェアモジュールのアップデートが管理サーバーのリポジトリにダウンロードされます。これらのアップデートは、Kaspersky Endpoint Security for Linux のアップデートタスクを使用してインストールされます。

仮想管理サーバーでは［管理サーバーのリポジトリへのアップデートのダウンロード］タスクは利用できません。仮想管理サーバーのリポジトリには、プライマリ管理サーバーにダウンロードされたアップデートが表示されます。

テストデバイスを指定してアップデートの動作とエラーが検証されるように設定できます。検証に成功すると、アップデートが他の管理対象デバイスに配信されます。

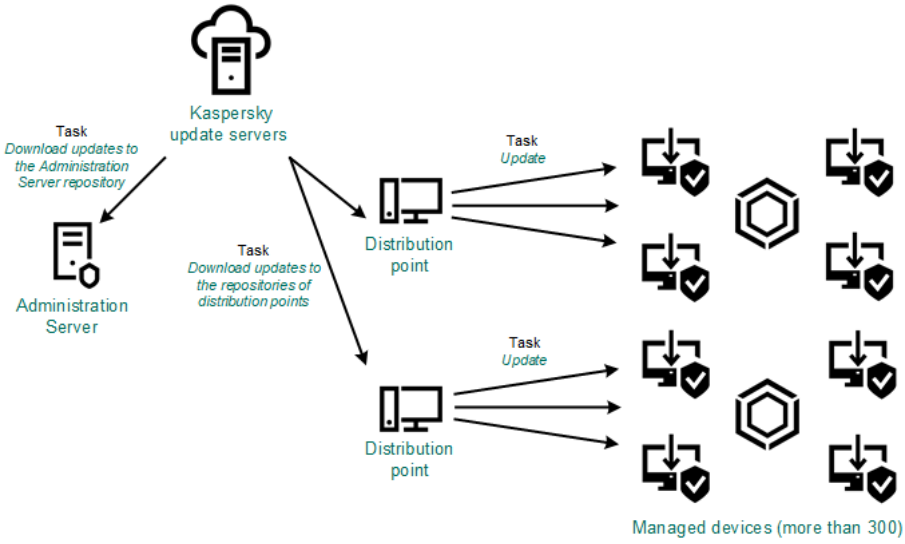
各カスペルスキー製品は、管理サーバーに必要なアップデートを要求します。管理サーバーはこれらの要求を集計した上で、いずれかの製品で要求されたアップデートのみをダウンロードします。これにより、同一のアップデートが複数回ダウンロードされたり、不必要なアップデートがダウンロードされることを防ぐことができます。［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクを実行中、関連するバージョンの定義データベースとソフトウェアモジュールを確実にダウンロードする目的で、次の情報が管理サーバーからカスペルスキーのアップデートサーバーに自動的に送信されます：

- 製品 ID およびバージョン
- 製品セットアップ ID
- 現在のライセンス ID
- ［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクの実行 ID

送信される情報には、個人データや機密データは含まれません。カスペルスキーでは、法律で定められた要件に従って情報を保護しています。

2 つのタスク（［管理サーバーのリポジトリへのアップデートのダウンロード］タスクおよび［ディストリビューションポイントのリポジトリにアップデートをダウンロード］タスク）の使用

管理サーバーのリポジトリを経由させずに、カスペルスキーのアップデートサーバーからディストリビューションポイントのリポジトリにアップデートを直接ダウンロードして、管理対象デバイスにアップデートを配信できます（次の図を参照）。ディストリビューションポイントのリポジトリへのダウンロードが推奨されるのは、管理サーバーとディストリビューションポイント間の通信の方がディストリビューションポイントとカスペルスキーのアップデートサーバー間の通信よりも費用がかかる場合や、管理サーバーがインターネットにアクセスできない場合などです。



管理サーバーのリポジトリへのアップデートのダウンロードタスクおよびディストリビューションポイントのリポジトリにアップデートをダウンロードタスクによるアップデート

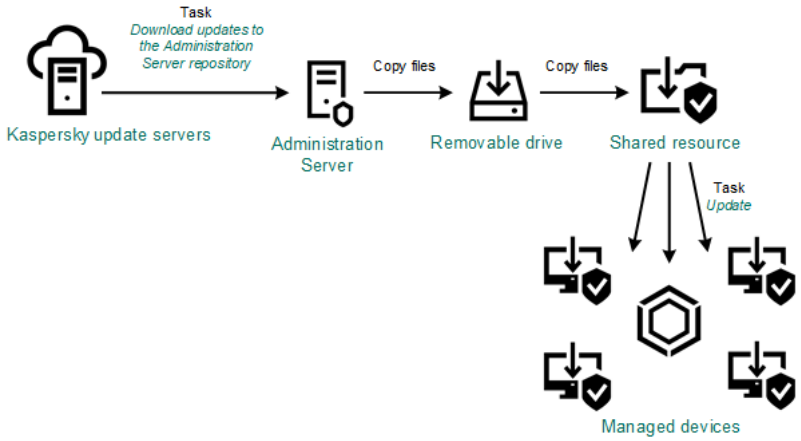
既定では、管理サーバーとディストリビューションポイントは HTTPS プロトコルを使用してカスペルスキーのアップデートサーバーに接続し、アップデートをダウンロードします。必要に応じて、管理サーバー、ディストリビューションポイント、またはその両方で HTTPS プロトコルの代わりに HTTP プロトコルを使用するように設定を編集できます。

このスキームを実装するには、*［管理サーバーのリポジトリへのアップデートのダウンロード］*タスクに加えて*［ディストリビューションポイントのリポジトリにアップデートをダウンロード］*タスクを作成します。その後、ディストリビューションポイントは、管理サーバーのリポジトリではなくカスペルスキーのアップデートサーバーからアップデートをダウンロードします。

定義データベースと Kaspersky Security Center のソフトウェアモジュールは*［管理サーバーのリポジトリへのアップデートのダウンロード］*タスクを使用してダウンロードされるため、このスキームでもこのタスクが必要です。

ローカルフォルダー、共有フォルダー、または FTP サーバーを使用して手動で実行

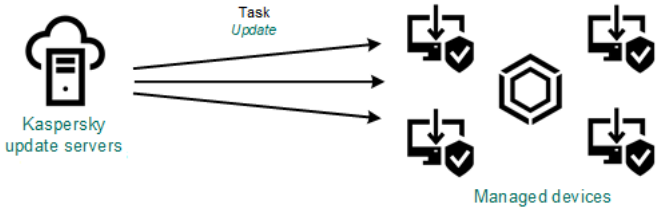
クライアントデバイスが管理サーバーに接続できない場合、ローカルフォルダーまたは共有リソースを使用して定義データベース、ソフトウェアモジュール、カスペルスキー製品をアップデートできます。このスキームでは、管理サーバーのリポジトリからリムーバブルドライブに必要なアップデートをコピーして、Kaspersky Endpoint Security for Linux の設定でアップデート元として指定したローカルフォルダーまたは共有リソースにアップデートをコピーする必要があります（次の図を参照）。



ローカルフォルダー、共有フォルダー、または FTP サーバーを使用したアップデート

カスペルスキーのアップデートサーバーから管理対象デバイスの Kaspersky Endpoint Security for Linux を直接アップデート

管理対象デバイスで、カスペルスキーのアップデートサーバーから直接アップデートを受信するように Kaspersky Endpoint Security for Linux を設定できます（次の図を参照）。



カスペルスキーのアップデートサーバーからセキュリティ製品を直接アップデート

このスキームでは、セキュリティ製品は Kaspersky Security Center が提供するリポジトリを使用しません。カスペルスキーのアップデートサーバーからアップデートを直接受信するには、セキュリティ製品でカスペルスキーのアップデートサーバーをアップデート元として指定します。これらの設定の詳細な説明については、Kaspersky Endpoint Security for Linux のヘルプを参照してください。

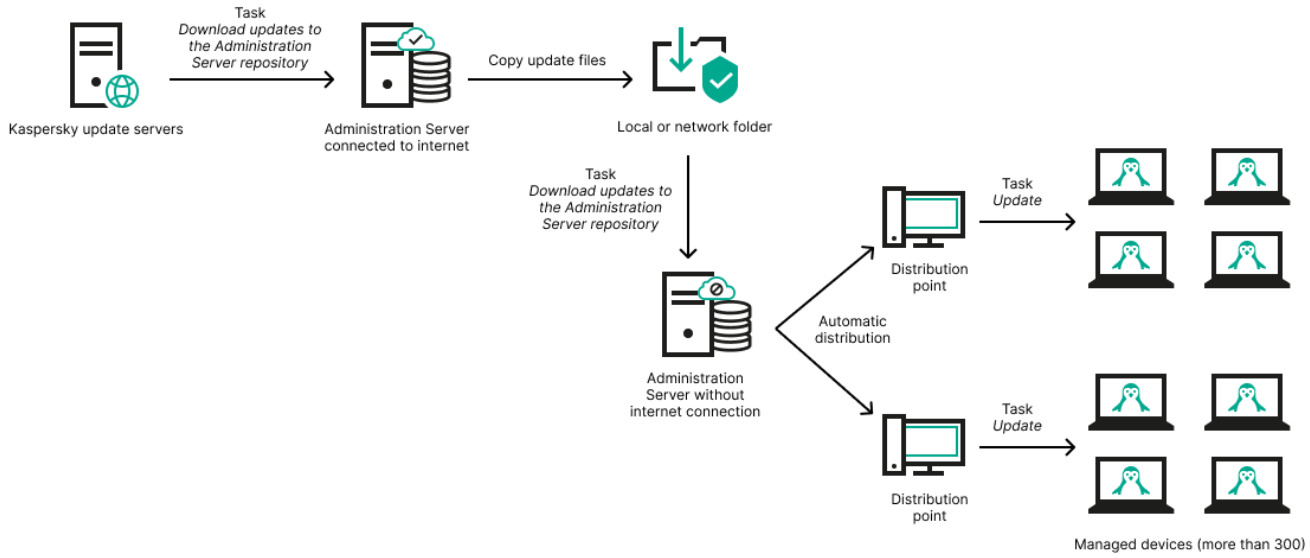
管理サーバーがインターネットに接続されていない場合は、ローカルまたはネットワークフォルダー経由

管理サーバーがインターネットに接続されていない場合は、［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクを設定して、ローカルまたはネットワークフォルダーからアップデートをダウンロードできます。この場合、指定したフォルダーに必要なアップデートファイルを定期的にコピーする必要があります。たとえば、次のいずれかのソースから、必要なアップデートファイルをコピーできます：

- インターネットに接続されている管理サーバー（下図を参照）

  管理サーバーは、セキュリティ製品が要求したアップデートのみをダウンロードするため、管理サーバーによって管理されるセキュリティ製品のセット（インターネット接続があるものとないもの）が一致している必要があります。

  アップデートのダウンロードに使用する管理サーバーのバージョンが 13.2 以前の場合、［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクのプロパティを開き、［**旧スキームを使用してアップデートをダウンロード**］オプションをオンにします。



管理サーバーがインターネットに接続されていない場合のローカルまたはネットワーク フォルダー経由のアップデート

- Kaspersky Update Utility

  このユーティリティは旧スキームを使用してアップデートをダウンロードするため、［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクのプロパティを開き、［*旧スキームを使用してアップデートをダウンロード*］オプションをオンにします。

［管理サーバーのリポジトリへのアップデートのダウンロード］タスクの作成

［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクを使用すると、カスペルスキーのアップデートサーバーから管理サーバーのリポジトリに、カスペルスキーセキュリティ製品の定義データベースおよびソフトウェアモジュールのアップデートをダウンロードできます。

Kaspersky Security Center クイックスタートウィザードは、管理サーバーの［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクを自動的に作成します。タスクリストには［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクが1つだけ表示されます。このタスクが管理サーバーのタスクリストから削除された場合、再度作成できます。

［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクが完了し、アップデートがダウンロードされたら、管理対象デバイスにこれらのアップデートを配信できます。

管理対象デバイスへのアップデートの配信前に、*アップデート検証*タスクを実行できます。これにより、管理サーバーが正しいアップデートをインストールし、アップデートによりセキュリティレベルが下がることがないことを確認できます。配信前に検証するには、［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクの設定で［**アップデートの検証の実行**］オプションをオンにします。

［管理サーバーのリポジトリへのアップデートのダウンロード］タスクを作成するには：

1. ［**デバイス**］→［**タスク**］の順に選択します。
2. ［**追加**］をクリックします。

   新規タスクウィザードが起動します。ウィザードの指示に従ってください。

3. Kaspersky Security Center を対象アプリケーションとするタスクから、［**管理サーバーのリポジトリへのアップデートのダウンロード**］タスク種別を選択します。

4. 作成中のタスク名を入力します。タスク名は 100 文字以下で、特殊文字（"*<>?\:|）を含めることはできません。

5. ［**タスク作成の終了**］ページで［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにして、タスクのプロパティウィンドウを開き、既定のタスク設定を変更できます。変更しない場合、後でいつでもタスク設定を変更できます。

6. ［**終了**］をクリックします。
   タスクが作成され、タスクリストに表示されます。

7. 作成したタスクの名前をクリックし、タスクのプロパティウィンドウを開きます。

8. タスクのプロパティウィンドウの［**アプリケーション設定**］タブで、次の設定を指定します：

- **アップデート元**

  アップデート元としては、 カスペルスキーのアップデートサーバー、ローカルフォルダーまたはネットワークフォルダー、プライマリ管理サーバーのいずれかを使用できます。

  ［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクおよび［*ディストリビューションポイントのリポジトリにアップデートをダウンロード*］タスクで、パスワード保護されたローカルフォルダーまたはネットワークフォルダーをアップデート元として選択した場合はユーザー認証が動作しません。この問題を解決するには、最初にパスワード保護されたフォルダーをマウントしてから、オペレーティングシステムを使用するなどして必要な資格情報を指定します。この後、アップデートのダウンロードタスクでこのフォルダーをアップデート元として選択することができます。Kaspersky Security Center は資格情報の入力を求めません。

- **アップデート保存先フォルダー**

  保存したアップデートを保管するためのフォルダーのパス。指定したフォルダーのパスをクリップボードにコピーすることができます。グループタスクに対して指定されたフォルダーのパスを変更することはできません。

- **ダウンロード済みのアップデートを追加のフォルダーにコピー**

  管理サーバーがアップデートを受信すると、指定されたフォルダーにコピーします。ネットワークでのアップデートの配信を手動で管理する場合は、このオプションをオンにします。

  このオプションの使用を検討する状況としては、たとえば、組織のネットワークが複数の独立したサブネットワークで構成され、各サブネットワークに属するデバイスは別のサブネットワークへのアクセス権を付与されていない場合があります。ただし、すべてのサブネットワークのデバイスは共通のネットワーク共有へのアクセス権は付与されています。この場合、いずれかのサブネットワークの管理サーバーでカスペルスキーのアップデートサーバーからアップデートをダウンロードするように設定した後、このオプションをオンにし、ネットワーク共有をコピー先に指定します。他の管理サーバーでは、リポジトリへのアップデートのダウンロードタスクのアップデート元として、このネットワーク共有を指定します。

  既定では、このオプションはオフです。

- **差分ファイルのダウンロード**

このオプションで差分ファイルのダウンロードを有効にすることができます。

既定では、このオプションはオフです。

- **旧スキームを使用してアップデートをダウンロード**

  Kaspersky Security Center のバージョン 14 から、データベースのアップデートとソフトウェアモジュールのダウンロードには新しいスキームが使用されるようになりました。新しいスキームを使用してアップデートをダウンロードするには、アップデート元に、新しいスキームと互換性のあるメタデータを持つアップデートファイルが含まれている必要があります。アップデート元のアップデートファイルのメタデータが旧スキームのみと互換性がある場合は、［**旧スキームを使用してアップデートをダウンロード**］をオンにしてください。オフにした場合、アップデートのダウンロードタスクは失敗します。

  たとえば、アップデート元としてローカルまたはネットワークフォルダーが指定されており、そのフォルダー内のアップデートファイルが次のアプリケーションによってダウンロードされた場合にはこのオプションをオンにする必要があります：

  - Kaspersky Update Utility

    このユーティリティは旧スキームを使用してアップデートをダウンロードします。

  - Kaspersky Security Center 13 Linux

    例えば、管理サーバー 1 はインターネットに接続していないものとします。この場合、インターネットに接続できる管理サーバー 2 を使用してアップデートをダウンロードし、このアップデートを管理サーバー 1 のアップデート元として使用するために、ローカルまたはネットワークフォルダーに保存します。管理サーバー 2 に Kaspersky Security Center のバージョン 13 がインストールされていた場合、管理サーバー 1 向けのタスクでは［**旧スキームを使用してアップデートをダウンロード**］をオンにしてください。

  既定では、このオプションはオフです。

- **アップデートの検証の実行**

  管理サーバーはアップデート元からアップデートをダウンロードし、それらを一時リポジトリに保存して、［**アップデート検証タスク**］で定義されたタスクを実行します。タスクが正常に終了すると、アップデートは一時保管領域から管理サーバーの共有フォルダーにコピーされ、この管理サーバーをアップデート元とするすべてのデバイスに配信されます（［**新しいアップデートがリポジトリにダウンロードされ次第**］のスケジュールが設定されたタスクが開始されます）。アップデートをリポジトリにダウンロードするタスクが完了するのは、*アップデートの検証*タスクの完了後のみです。

  既定では、このオプションはオフです。

9. タスクのプロパティウィンドウの［**スケジュール**］タブで、タスクの開始スケジュールを作成します。必要に応じて、次の設定を指定します：

- **実行予定**：

  タスクを実行するスケジュールを選択し、そのスケジュールを設定します。

  - **手動**（既定で選択）

    タスクは、自動的には実行されません。手動でのみ開始できます。

    既定では、このオプションはオンです。

- **N 分ごと**

  タスク作成日の指定した時刻から、分単位で指定した間隔ごとにタスクを定期的に実行します。

  既定では、現在のシステム時刻から、30 分ごとにタスクが実行されます。

- **N 時間ごと**

  指定した日時から、時間単位で指定した間隔ごとにタスクを定期的に実行します。

  既定では、現在のシステム日時から、6 時間ごとにタスクが実行されます。

- **N 日ごと**

  日単位で指定した間隔ごとにタスクを定期的に実行します。さらに、最初にタスクを実行する日時を指定できます。この詳細設定項目は、タスクを作成中の製品でこの項目の使用がサポートされている場合に利用できます。

  既定では、現在のシステム日時から、1 日ごとにタスクが実行されます。

- **N 週間ごと**

  指定した日時から、週単位で指定した間隔ごとに、指定した曜日の指定した時刻にタスクを定期的に実行します。

  既定では、毎週、月曜日の現在のシステム時刻にタスクが実行されます。

- **毎日（サマータイムはサポートしていません）**

  日単位で指定した間隔ごとにタスクを定期的に実行します。このスケジュールではサマータイム（DST）の適用はサポートされません。つまり、サマータイムの開始または終了に伴い、時刻を 1 時間早めたまたは遅らせた場合でも、実際にタスクが開始される時刻は変化しません。

  このスケジュールの使用は推奨されません。Kaspersky Security Center Linux の旧バージョンとの後方互換性を維持するために用意されているオプションとなります。

  既定では、毎日、現在のシステム時刻にタスクが実行されます。

- **毎週**

  毎週、指定した曜日の指定した時刻にタスクを実行します。

- **曜日ごと**

  指定した曜日（複数可）の指定した時刻にタスクを定期的に実行します。

  既定では、毎週金曜日の午後 6 時にタスクが実行されます。

- **毎月**

  毎月、指定した日付の指定した時刻にタスクを定期的に実行します。

  指定した日付が存在しない月には、月の最終日にタスクを実行します。

  既定では、各月の初日の現在のシステム時刻にタスクが実行されます。

- **毎月、選択した週の指定日**

  毎月、指定した週・曜日の指定した時刻にタスクを定期的に実行します。

  既定では、月内のいかなる日付も選択されておらず、開始時刻は午後 6 時です。

- **他のタスクが完了次第**

  他のタスクが完了した後に、現在のタスクを開始します。現在のタスクを実行する条件として、先に実行されるタスクの実行結果（「正常終了」または「エラー終了」）を選択できます。

- 追加タスクの設定：

  - **未実行のタスクを実行する**

    このオプションは、タスクの開始予定時刻にクライアントデバイスがネットワーク上で可視でない場合のタスクの処理方法を指定します。

    このオプションをオンにすると、クライアントデバイスでのカスペルスキー製品の次回起動時に、タスクの開始を試行します。タスクスケジュール設定が［**手動**］、［**1 回**］または［**即時**］に設定されている場合、ネットワーク上でデバイスが認識されるかデバイスがタスク範囲に追加されるすぐにタスクが開始されます。

    このオプションをオフにすると、スケジュール設定されたタスクだけがクライアントデバイス上で開始され、［**手動**］、［**1 回**］、および［**即時**］に設定したタスクはネットワーク上で可視になっているクライアントデバイスでのみ開始されます。そのため、たとえばリソース消費量が多いので業務時間外にのみ実行したいタスクなどで、このオプションをオフにすることが有効な場合があります

    既定では、このオプションはオンです。

  - **タスクの開始を自動的かつランダムに遅延させる**

    このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始され、*タスクの分散開始*を実現します。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

    分散開始の開始時刻は、タスクの作成時に自動的に計算されます。計算の結果は、タスクに割り当てられるクライアントデバイスの台数によって異なります。以降は、タスクは常に計算された開始時刻に開始されます。ただし、タスクの設定が変更されたりタスクが手動で開始された場合、計算によるタスク開始時刻は変更されます。

    このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

  - **タスクの開始を次の時間範囲内でランダムに遅延させる（分）**

    このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始されます。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

    このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

    既定では、このオプションはオフです。既定の時間は 1 分です。

  - **実行時間が次を超える場合はタスクを停止する（分）**

指定した時間が経過すると、タスクが完了したかどうかに関係なくタスクが自動的に停止します。

実行に時間がかかり過ぎているタスクを中断したい時に、このオプションを使用します。

既定では、このオプションはオフです。既定のタスク実行時間は 120 分です。

10. ［**保存**］をクリックします。

タスクが指定した設定で作成されます。

管理サーバーが［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクを実行すると、アップデート元からデータベースとソフトウェアモジュールのアップデートがダウンロードされ、管理サーバーの共有フォルダーに保存されます。管理グループに対してこのタスクを作成すると、指定された管理グループにあるネットワークエージェントにのみ適用されます。

アップデートは管理サーバーの共有フォルダーからクライアントデバイスとセカンダリ管理サーバーに配信されます。

ダウンロードされたアップデートの表示

管理サーバーが［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクを実行すると、アップデート元からデータベースとソフトウェアモジュールのアップデートがダウンロードされ、管理サーバーの共有フォルダーに保存されます。ダウンロードしたアップデートは［**定義データベースとカスペルスキー製品モジュールのアップデート**］セクションで確認できます。

ダウンロードされたアップデートのリストを表示するには：

メインメニューで、［**操作**］→［**カスペルスキー製品**］→［**定義データベースとカスペルスキー製品モジュールのアップデート**］の順に選択します。

適用可能なアップデートのリストが表示されます。

ダウンロードされたアップデートの検証

管理対象デバイスにアップデートをインストールする前に、*アップデート検証*タスクを使用してアップデートの動作およびエラーがないかどうかを検証できます。*アップデート検証*タスクは、［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクの一部として自動的に実行されます。アップデート元からアップデートがダウンロードされて、一時リポジトリに保存された後、*アップデート検証*タスクが実行されます。タスクが正常に完了すると、一時リポジトリから管理サーバーの共有フォルダーにアップデートがコピーされます。アップデートのコピーは、管理サーバーがアップデート元として指定されているすべてのクライアントデバイスに配信されます。

*アップデート検証*タスクの結果、一時リポジトリにあるアップデートが正しくないことが判明した場合、または*アップデート検証*タスクがエラーで終了した場合、それらのアップデートは共有フォルダーにコピーされません。管理サーバーでは、以前のアップデートが維持されます。また、スケジュール種別として［**新しいアップデートがリポジトリにダウンロードされ次第**］が指定されたタスクも開始されません。新しいアップデートのスキャンが正常に完了した場合、［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクの次の開始時に、それらのタスクが実行されます。

少なくとも1台のテストデバイスで次のいずれかの条件が当てはまる場合、アップデートは正しくないと判断されます：

- アップデートタスクエラーが発生した
- セキュリティ製品のリアルタイム保護のステータスがアップデートの適用後に変更された
- オンデマンドスキャンタスクの実行中に、感染したオブジェクトが検知された
- カスペルスキー製品の実行時にエラーが発生した

すべてのテストデバイスの場合に挙げられた条件が当てはまらない場合、そのアップデートは正常とみなされ、*アップデート検証*タスクは正常に終了したと判断されます。

*アップデート検証*タスクを作成する前に、次の前提条件を実行してください：

1. 複数のテストデバイスで管理グループを作成する。このグループはアップデートの検証に必要になります。

   ネットワーク内で、最も信頼性の高い保護が適用されており、最も一般的なアプリケーション設定が行われているデバイスを使用してください。このアプローチにより、スキャン中のウイルス検知の精度が向上し、誤検知のリスクを最小限に抑えます。テストデバイスでウイルスが検知された場合、*アップデート検証*タスクは失敗と判断されます。

2. Kaspersky Endpoint Security for Linux など、Kaspersky Security Center のサポート対象のアプリケーション向けにアップデートおよびスキャンタスクを作成します。アップデートおよびスキャンタスクの作成時に、テストデバイスの管理グループを指定します。

   *アップデート検証*タスクは順次テストデバイスでアップデートとスキャンタスクを実行し、すべてのアップデートが有効であることを確認します。また、*アップデート検証*タスクの作成中にアップデートおよびスキャンタスクを指定する必要があります。

3. ［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクをクリックします。

ダウンロードしたアップデートを、クライアントデバイスに配信する前に Kaspersky Security Center Linux で検証するには：

1. メインメニューで、［**デバイス**］→［**タスク**］の順に移動します。
2. ［**管理サーバーのリポジトリへのアップデートのダウンロード**］タスクをクリックします。
3. タスクのプロパティウィンドウが開いたら、［**アプリケーション設定**］タブに移動し、［**アップデートの検証の実行**］オプションをオンにします。
4. *アップデート検証*タスクがある場合は、［**タスクの選択**］をクリックします。表示されたウィンドウで、テストデバイスの管理グループで*アップデート検証*タスクを選択します。
5. 事前に*アップデート検証*タスクを作成していなかった場合は、次の操作を実行します：

   a. ［**新規タスク**］をクリックします。

   b. タスクの追加ウィザードが表示されるので、事前設定されたタスク名を変更する場合は名前を指定します。

   c. 事前に作成しておいたテストデバイスの管理グループを選択します。

   d. 最初に Kaspersky Security Center がサポートする必要なアプリケーションのアップデートタスクを選択し、次にスキャンタスクを選択します。

その後、次のオプションが表示されます。オプションはオンのままにしておくことを推奨します。

- **定義データベースのアップデート後にデバイスを再起動する**

  デバイス上で定義データベースをアップデートした後には、デバイスの再起動を推奨します。

  既定では、このオプションはオンです。

- **定義データベースのアップデートとデバイス再起動の後にリアルタイム保護のステータスを確認する**

  このオプションをオンにすると、*アップデート検証*タスクは、管理サーバーのリポジトリにダウンロードされたアップデートが有効であるかどうか、また定義データベースのアップデート後にデバイスが再起動された後に保護レベルが低下することがないかを確認します。

  既定では、このオプションはオンです。

e. *アップデート検証タスク*を実行するアカウントを指定します。自身のアカウントの使用も可能で、［**既定のアカウント**］オプションをオンのままにします。または、必要なアクセス権を持つ別のアカウントを指定してタスクを実行することもできます。この場合は［**アカウントの指定**］をオンにしてそのアカウントの資格情報を入力してください。

6. ［**保存**］をクリックして、［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクのプロパティウィンドウを閉じます。

アップデートの自動的な検証が有効になります。これで、［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクを実行できるようになりました。タスクはアップデートの検証から開始します。

［ディストリビューションポイントのリポジトリにアップデートをダウンロード］タスクの作成

［*ディストリビューションポイントのリポジトリにアップデートをダウンロード*］タスクを管理グループに対して作成できます。このタスクは、指定の管理グループ内のディストリビューションポイントに対して実行されます。

このタスクの使用例としては、管理サーバーとディストリビューションポイント間の通信の方が、ディストリビューションポイントとカスペルスキーのアップデートサーバー間の通信よりも費用がかかる場合や、管理サーバーがインターネットにアクセスできない場合などがあります。

このタスクは、カスペルスキーのアップデートサーバーからディストリビューションポイントのリポジトリにアップデートをダウンロードするために必要です。アップデートのリストには次の内容が含まれます：

- カスペルスキーのセキュリティ製品の定義データベースおよびソフトウェアモジュールのアップデート
- Kaspersky Security Center コンポーネントのアップデート
- カスペルスキーのセキュリティ製品のアップデート

アップデートのダウンロード後、管理対象デバイスにこれらのアップデートを配信できます。

ディストリビューションポイントのリポジトリにアップデートをダウンロード*タスクを、特定の管理グループに対して作成するには：*

1. メインメニューで、［**デバイス**］→［**タスク**］の順に選択します。

2. ［**追加**］をクリックします。

   タスク追加ウィザードが開始されます。ウィザードの指示に従ってください。

3. Kaspersky Security Center を対象アプリケーションとするタスクから、［**タスク種別**］で［**ディストリビューションポイントのリポジトリにアップデートをダウンロード**］を選択します。

4. 作成中のタスク名を入力します。タスク名は 100 文字以下で、特殊文字（"*<>?\:|）を含めることはできません。

5. タスクの適用対象として、管理グループ、デバイスの抽出、または指定したデバイスを選択します。

6. ［**タスク作成の終了**］ステップで、既定のタスク設定を変更する場合、［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにします。このオプションをオフにすると、既定の設定でタスクが作成されます。既定の設定からの変更は、後からいつでも実行できます。

7. ［**作成**］をクリックします。

   タスクが作成され、タスクリストに表示されます。

8. 作成したタスクの名前をクリックし、タスクのプロパティウィンドウを開きます。

9. タスクのプロパティウィンドウの［**アプリケーション設定**］タブで、次の設定を指定します：

   - アップデート元

ディストリビューションポイントのアップデート元として、使用できるものは次の通りです：

- カスペルスキーのアップデートサーバー

  カスペルスキーの HTTP サーバーで、カスペルスキー製品はこれらのサーバーから定義データベースやソフトウェアモジュールのアップデートをダウンロードします。

  既定ではこのオプションが選択されます。

- プライマリ管理サーバー

  セカンダリ管理サーバーまたは仮想管理サーバーを対象とするタスクに適用されます。

- ローカルまたはネットワーク上のフォルダー

  最新のアップデートが保存されたローカルフォルダーまたはネットワークフォルダー：ネットワークフォルダーとしては FTP サーバー、HTTP サーバー、または SMB 共有を指定できます。ネットワークフォルダーに認証が必要な場合、SMB プロトコルのみがサポートされています。ローカルフォルダーの選択時には、管理サーバーがインストールされているデバイスのフォルダーを指定する必要があります。

  > アップデート元で使用される FTP/HTTP サーバーまたはネットワークフォルダーは、アップデートを含み、フォルダーの構造がカスペルスキーのアップデートサーバーの使用時に作成された構造と一致する必要があります。

  > ［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクおよび［*ディストリビューションポイントのリポジトリにアップデートをダウンロード*］タスクで、パスワード保護されたローカルフォルダーまたはネットワークフォルダーをアップデート元として選択した場合はユーザー認証が動作しません。この問題を解決するには、最初にパスワード保護されたフォルダーをマウントしてから、オペレーティングシステムを使用するなどして必要な資格情報を指定します。この後、アップデートのダウンロードタスクでこのフォルダーをアップデート元として選択することができます。Kaspersky Security Center は資格情報の入力を求めません。

- **アップデート保存先フォルダー**

  保存したアップデートを保管するためのフォルダーのパス。指定したフォルダーのパスをクリップボードにコピーすることができます。グループタスクに対して指定されたフォルダーのパスを変更することはできません。

- **差分ファイルのダウンロード**

  このオプションで差分ファイルのダウンロードを有効にすることができます。

  既定では、このオプションはオフです。

- **旧スキームを使用してアップデートをダウンロード**

Kaspersky Security Center のバージョン 14 から、データベースのアップデートとソフトウェアモジュールのダウンロードには新しいスキームが使用されるようになりました。新しいスキームを使用してアップデートをダウンロードするには、アップデート元に、新しいスキームと互換性のあるメタデータを持つアップデートファイルが含まれている必要があります。アップデート元のアップデートファイルのメタデータが旧スキームのみと互換性がある場合は、［**旧スキームを使用してアップデートをダウンロード**］をオンにしてください。オフにした場合、アップデートのダウンロードタスクは失敗します。

たとえば、アップデート元としてローカルまたはネットワークフォルダーが指定されており、そのフォルダー内のアップデートファイルが次のアプリケーションによってダウンロードされた場合にはこのオプションをオンにする必要があります：

- Kaspersky Update Utility

  このユーティリティは旧スキームを使用してアップデートをダウンロードします。

- Kaspersky Security Center 13 Linux

  たとえば、ディストリビューションポイントがローカルまたはネットワークフォルダーからアップデートを取得するように設定されているものとします。この場合、インターネットに接続できる管理サーバーを使用してアップデートをダウンロードし、このアップデートをディストリビューションポイントのローカルフォルダーに配置します。管理サーバーにバージョン 13 がインストールされている場合、［*ディストリビューションポイントのリポジトリにアップデートをダウンロード*］タスクで［**旧スキームを使用してアップデートをダウンロード**］をオンにしてください。

既定では、このオプションはオフです。

10. タスクの開始スケジュール作成。必要に応じて、次の設定を指定します：

- **実行予定**

  タスクを実行するスケジュールを選択し、そのスケジュールを設定します。

  - **手動**（既定で選択）

    タスクは、自動的には実行されません。手動でのみ開始できます。
    既定では、このオプションはオンです。

  - **N 分ごと**

    タスク作成日の指定した時刻から、分単位で指定した間隔ごとにタスクを定期的に実行します。
    既定では、現在のシステム時刻から、30 分ごとにタスクが実行されます。

  - **N 時間ごと**

    指定した日時から、時間単位で指定した間隔ごとにタスクを定期的に実行します。
    既定では、現在のシステム日時から、6 時間ごとにタスクが実行されます。

  - **N 日ごと**

日単位で指定した間隔ごとにタスクを定期的に実行します。さらに、最初にタスクを実行する日時を指定できます。この詳細設定項目は、タスクを作成中の製品でこの項目の使用がサポートされている場合に利用できます。

既定では、現在のシステム日時から、1日ごとにタスクが実行されます。

- **N週間ごと**

  指定した日時から、週単位で指定した間隔ごとに、指定した曜日の指定した時刻にタスクを定期的に実行します。

  既定では、毎週、月曜日の現在のシステム時刻にタスクが実行されます。

- **毎日（サマータイムはサポートしていません）**

  日単位で指定した間隔ごとにタスクを定期的に実行します。このスケジュールではサマータイム（DST）の適用はサポートされません。つまり、サマータイムの開始または終了に伴い、時刻を1時間早めたまたは遅らせた場合でも、実際にタスクが開始される時刻は変化しません。

  このスケジュールの使用は推奨されません。Kaspersky Security Center Linuxの旧バージョンとの後方互換性を維持するために用意されているオプションとなります。

  既定では、毎日、現在のシステム時刻にタスクが実行されます。

- **毎週**

  毎週、指定した曜日の指定した時刻にタスクを実行します。

- **曜日ごと**

  指定した曜日（複数可）の指定した時刻にタスクを定期的に実行します。

  既定では、毎週金曜日の午後6時にタスクが実行されます。

- **毎月**

  毎月、指定した日付の指定した時刻にタスクを定期的に実行します。

  指定した日付が存在しない月には、月の最終日にタスクを実行します。

  既定では、各月の初日の現在のシステム時刻にタスクが実行されます。

- **毎月、選択した週の指定日**

  毎月、指定した週・曜日の指定した時刻にタスクを定期的に実行します。

  既定では、月内のいかなる日付も選択されておらず、開始時刻は午後6時です。

- **ウイルスアウトブレイク検知次第**

［*ウイルスアウトブレイク*］イベントの発生後にタスクを実行します。ウイルスアウトブレイクを監視するアプリケーションの種別を選択します。次のアプリケーション種別があります：

- ワークステーションとファイルサーバー向けアンチウイルス製品
- 境界防御向けアンチウイルス製品
- メールサーバー向けアンチウイルス製品

既定では、すべてのアプリケーション種別がオンです。

ウイルスアウトブレイクを検知したアンチウイルス製品の種別ごとに、異なるタスクを実行したい場合、該当するタスクで必要ないアプリケーションの種別をオフにします。

- **他のタスクが完了次第**

他のタスクが完了した後に、現在のタスクを開始します。現在のタスクを実行する条件として、先に実行されるタスクの実行結果（「正常終了」または「エラー終了」）を選択できます。

- **未実行のタスクを実行する**

このオプションは、タスクの開始予定時刻にクライアントデバイスがネットワーク上で可視でない場合のタスクの処理方法を指定します。

このオプションをオンにすると、クライアントデバイスでのカスペルスキー製品の次回起動時に、タスクの開始を試行します。タスクスケジュール設定が［**手動**］、［**1回**］または［**即時**］に設定されている場合、ネットワーク上でデバイスが認識されるかデバイスがタスク範囲に追加されるすぐにタスクが開始されます。

このオプションをオフにすると、スケジュール設定されたタスクだけがクライアントデバイス上で開始され、［**手動**］、［**1回**］、および［**即時**］に設定したタスクはネットワーク上で可視になっているクライアントデバイスでのみ開始されます。そのため、たとえばリソース消費量が多いので業務時間外にのみ実行したいタスクなどで、このオプションをオフにすることが有効な場合があります

既定では、このオプションはオンです。

- **タスクの開始を自動的かつランダムに遅延させる**

このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始され、*タスクの分散開始*を実現します。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

分散開始の開始時刻は、タスクの作成時に自動的に計算されます。計算の結果は、タスクに割り当てられるクライアントデバイスの台数によって異なります。以降は、タスクは常に計算された開始時刻に開始されます。ただし、タスクの設定が変更されたりタスクが手動で開始された場合、計算によるタスク開始時刻は変更されます。

このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

- **タスクの開始を次の時間範囲内でランダムに遅延させる（分）**

このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始されます。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

既定では、このオプションはオフです。既定の時間は1分です。

11. ［**保存**］をクリックします。

タスクが指定した設定で作成されます。

タスクの作成時に指定した設定およびタスクのその他のプロパティは、いつでも変更できます。

*ディストリビューションポイントのリポジトリにアップデートをダウンロード*タスクを実行すると、定義データベースとソフトウェアモジュールのアップデートがアップデート元からダウンロードされ、共有フォルダーに保存されます。指定の管理グループに含まれていて、ディストリビューションポイントタスクが明示的に設定されていないディストリビューションポイントにしか、ダウンロードされたアップデートは使用されません。

［管理サーバーのリポジトリへのアップデートのダウンロード］タスクに対するアップデート元の追加

管理サーバーのリポジトリにアップデートをダウンロードするタスクを作成または使用する場合、次のアップデート元を選択することができます：

- カスペルスキーのアップデートサーバー
- プライマリ管理サーバー

  セカンダリ管理サーバーまたは仮想管理サーバーを対象とするタスクに適用されます。
- ローカルまたはネットワークフォルダー

［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクおよび［*ディストリビューションポイントのリポジトリにアップデートをダウンロード*］タスクで、パスワード保護されたローカルフォルダーまたはネットワークフォルダーをアップデート元として選択した場合はユーザー認証が動作しません。この問題を解決するには、最初にパスワード保護されたフォルダーをマウントしてから、オペレーティングシステムを使用するなどして必要な資格情報を指定します。この後、アップデートのダウンロードタスクでこのフォルダーをアップデート元として選択することができます。Kaspersky Security Center は資格情報の入力を求めません。

既定ではカスペルスキーのアップデートサーバーが使用されますが、ローカルまたはネットワークフォルダーにアップデートをダウンロードすることもできます。インターネットにアクセスできないネットワークを使用する場合にフォルダーを使用することがあります。この場合、カスペルスキーのアップデートサーバーから手動でアップデートをダウンロードして、フォルダーにダウンロードしたファイルを配置することができます。

ローカルまたはネットワークフォルダーに指定できるパスは1つのみです。ローカルフォルダーとして使用できるのは管理サーバー上にあるフォルダーのみで、ネットワークフォルダーとして使用できるのは、FTP または HTTP サーバーのみです。

カスペルスキーのアップデートサーバーとローカルまたはネットワークフォルダーの両方を追加した場合は、アップデートはフォルダーから先にダウンロードされます。ダウンロードにエラーが発生すると、カスペルスキーのアップデートサーバーが使用されます。

アップデートが含まれる共有フォルダーがパスワードで保護されている場合は、［**アップデート元の共有フォルダーにアクセスするアカウントを指定する（存在する場合）**］をオンにして、アクセスに必要なアカウント資格情報を入力します。

アップデート元を追加するには：

1. ［**デバイス**］→［**タスク**］の順に選択します。
2. ［**管理サーバーのリポジトリへのアップデートのダウンロード**］をクリックします。
3. ［**アプリケーション設定**］タブに移動します。
4. ［**アップデート元**］行で、［**設定**］をクリックします。
5. ウィンドウが表示されたら、［**追加**］をクリックします。
6. アップデート元のリストで、必要なアップデート元を追加します。［**ローカルまたはネットワークフォルダー**］を選択した場合は、フォルダーのパスを指定します。
7. ［OK］をクリックしてアップデート元のプロパティウィンドウを閉じます。
8. ［アップデート元］ウィンドウで、［OK］をクリックします。
9. タスクのウィンドウで［**保存**］をクリックします。

指定したアップデート元から管理サーバーのリポジトリにアップデートがダウンロードされるようになります。

カスペルスキー製品の定義データベースとソフトウェアモジュールのアップデートでの差分ファイルの使用

Kaspersky Security Center Linux がカスペルスキーのアップデートサーバーからアップデートをダウンロードする時、差分ファイルを使用することでトラフィックが最適化されます。また、ネットワーク内の他のデバイスからアップデートを取得するデバイス（管理サーバー、ディストリビューションポイント、クライアントデバイス）についても、差分ファイルの使用を有効化できます。

差分ファイルのダウンロード機能の概要

差分ファイルには、定義データベースファイルまたはソフトウェアモジュールファイルの異なる 2 バージョン間の変更点のみが含まれています。完全な定義データベースファイルまたはソフトウェアモジュールファイルよりも差分ファイルの方が容量が小さいため、差分ファイルを使用することで社内ネットワークのトラフィック量を軽減できます。管理サーバーまたはディストリビューションポイントで［*差分ファイルのダウンロード*］機能が有効になっている場合、該当する管理サーバーまたはディストリビューションポイントに差分ファイルが保存されます。これにより、この管理サーバーまたはディストリビューションポイントからアップデートを取得するデバイスでは、保存されている差分ファイルを使用して定義データベースとソフトウェアモジュールのアップデートを実行できます。

差分ファイルをより効果的に使用するには、デバイス側でのアップデートスケジュールを、アップデートの取得元となる管理サーバーやディストリビューションポイント側のアップデートスケジュールと同期することを推奨します。ただし、このような設定を行わなくても、デバイス側のアップデート頻度がアップデートの取得元となる管理サーバーやディストリビューションポイント側のアップデート頻度より低いだけでもトラフィックの軽減につながります。

ディストリビューションポイントは差分ファイルの自動配信に IP マルチキャストを使用しません。

差分ファイルのダウンロード機能の有効化：シナリオ

実行するステップ

1. **管理サーバーでこの機能を有効にする**

   *管理サーバーのリポジトリへのアップデートのダウンロード*タスクの設定でこの機能を有効にします。

2. **ディストリビューションポイントでこの機能を有効にする**

   ［*ディストリビューションポイントのリポジトリにアップデートをダウンロード*］タスクを使用してアップデートを取得するディストリビューションポイントでこの機能を有効にします。

   管理サーバーからアップデートを受け取るディストリビューションポイントのネットワークエージェントのポリシー設定でこの機能を有効にします。

   管理サーバーからアップデートを取得するディストリビューションポイントでこの機能を有効にします。

   ネットワークエージェントのポリシー設定と（ディストリビューションポイントを手動で割り当てていてポリシー設定を上書きしたい場合）管理サーバーのプロパティの［**ディストリビューションポイント**］セクションで機能を有効にできます。

［差分ファイルのダウンロード］機能が有効になっているかどうかを確認する方法としては、これらの手順を実行する前後での内部トラフィックを測定することができます。

ディストリビューションポイントによるアップデートのダウンロード

Kaspersky Security Center Linux では、ディストリビューションポイントはアップデートを管理サーバー、カスペルスキーのサーバー、ローカルまたはネットワークフォルダーから取得できます。

ディストリビューションポイントによるアップデートのダウンロードを設定するには：

1. メインウィンドウ上部の管理サーバー名のセクションで目的の管理サーバーを選択し、横にある設定アイコン（）をクリックします。

   管理サーバーのプロパティウィンドウが開きます。

2. ［**全般**］タブで、［**ディストリビューションポイント**］セクションを選択します。

3. このグループのクライアントデバイスにアップデートを配信するディストリビューションポイントの名前をクリックします。

4. ディストリビューションポイントのプロパティウィンドウで、［**アップデート元**］セクションを選択します。

5. ディストリビューションポイントのアップデート元を選択します：

- **アップデート元**

  ディストリビューションポイントのアップデート元を選択します：

  - ディストリビューションポイントが管理サーバーからアップデートを取得できるようにするには、［**管理サーバーから取得**］をオンにします。
  - タスクを使用してディストリビューションポイントがアップデートを受信できるようにするには、［**アップデートのダウンロードタスクを使用**］をオンにして、［*ディストリビューションポイントのリポジトリにアップデートをダウンロード*］タスクを指定します：
    - そのようなタスクが既にデバイスにある場合は、リストからタスクを選択します。
    - タスクがデバイスに存在しない場合、［**タスクの作成**］をクリックし、タスクを作成します。タスク追加ウィザードが開始されます。ウィザードの指示に従ってください。

- **差分ファイルのダウンロード**

  このオプションで差分ファイルのダウンロードを有効にすることができます。

  既定では、このオプションはオンです。

ディストリビューションポイントは指定されたアップデート元からアップデートを取得します。

オフラインデバイスの定義データベースとソフトウェアモジュールのアップデート

管理対象デバイスの定義データベースとソフトウェアモジュールのアップデートは、ウイルスやその他の脅威からデバイスを継続して保護するために重要なタスクです。通常、管理者は管理サーバーのリポジトリを使用するように指定して、定期的なアップデートを設定します。

管理サーバー（プライマリまたはセカンダリ）、ディストリビューションポイント、インターネットのいずれにも接続されていないデバイス（またはデバイスのグループ）のデータベースとソフトウェアモジュールをアップデートする必要がある場合は、FTP サーバーまたはローカルフォルダーなどの代替のアップデート元を使用する必要があります。この場合、フラッシュドライブまたは外付けハードディスクなどの大容量ストレージデバイスを使用して必要なアップデートのファイルを受け渡しする必要があります。

必要なアップデートは次からコピーできます：

- 管理サーバー：

  オフラインデバイスにインストールされているセキュリティ製品に必要なアップデートが管理サーバーのリポジトリに含まれるようにするには、少なくとも1台のオンラインの管理対象デバイスに同じセキュリティ製品がインストールされている必要があります。また、この製品が［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクを使用して管理サーバーのリポジトリからアップデートを受信するように設定されている必要があります。

- 同じセキュリティ製品がインストールされていて、管理サーバーのリポジトリやディストリビューションポイントのリポジトリからアップデートを受信するか、カスペルスキーのアップデートサーバーからアップデートを直接受信するように設定されている任意のデバイス

管理サーバーのリポジトリからアップデートをコピーして、データベースおよびソフトウェアモジュールのアップデートを設定する例を次に示します。

オフラインデバイスの定義データベースとソフトウェアモジュールをアップデートするには：

1. 管理サーバーがインストールされているデバイスにリムーバブルドライブを接続します。
2. アップデートファイルをリムーバブルドライブにコピーします。

   既定では、アップデートは「\\<サーバー名>\KLSHARE\Updates」に保存されています。

   または、選択したフォルダーにアップデートを定期的にコピーするように Kaspersky Security Center を設定できます。これには、［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクのプロパティにある［**ダウンロード済みのアップデートを追加のフォルダーにコピー**］を使用します。フラッシュドライブまたは外付けハードディスクのフォルダーをこのオプションのターゲットフォルダーに指定した場合、この大容量ストレージデバイスには常にアップデートの最新バージョンが含まれることになります。
3. オフラインデバイスで、ローカルフォルダーまたは FTP サーバーや共有フォルダーなどの共有リソースからアップデートを受信するように Kaspersky Endpoint Security for Linux を設定 します。
4. リムーバブルドライブからローカルフォルダーまたはアップデート元として使用する共有リソースにアップデートファイルをコピーします。
5. アップデートのインストールが必要なオフラインデバイスで、Kaspersky Endpoint Security for Linux のアップデートタスクを開始します。

アップデートタスクが完了すると、デバイスの定義データベースとソフトウェアモジュールが最新の状態になります。

ディストリビューションポイントと接続ゲートウェイの調整

Kaspersky Security Center Linux の管理グループ構造では、次の機能が実行されます：

- ポリシー範囲の設定

  関連する設定をデバイスに適用する別の方法として、*ポリシーのプロファイル*を使用する方法があります。
- グループタスク範囲の設定

  管理グループの階層に基づいていない、グループタスク範囲の定義方法が存在します。これは、デバイス選択用のタスクと特定のデバイス用のタスクを使用することです。
- デバイス、仮想管理サーバー、およびセカンダリ管理サーバーへのアクセス権限の設定
- ディストリビューションポイントの割り当て

管理グループ構造を構築する際には、ディストリビューションポイントを最適に割り当てるために、組織ネットワークのトポロジーを考慮する必要があります。ディストリビューションポイントを最適に分散配置すると、組織ネットワークのトラフィック量を軽減できます。

組織の組織図とネットワークトポロジーに応じて、管理グループ構造に次の標準設定を適用できます：

- 単一のオフィス

- 複数の小規模なリモートオフィス

ディストリビューションポイントとして動作するデバイスについては、あらゆる不正なアクセスに対して、物理的な保護も含めて保護する必要があります。

ディストリビューションポイントの標準設定：単一のオフィス

標準の「単一のオフィス」設定では、すべてのデバイスが組織ネットワーク内に置かれているため、お互いを「見る」ことができます。組織ネットワークは、いくつかの部分に区切られ（ネットワークまたはネットワークセグメント）、狭い帯域幅によって連結されるかたちで構成されている場合があります。

管理グループの構造は、次の方法で構築することが可能です：

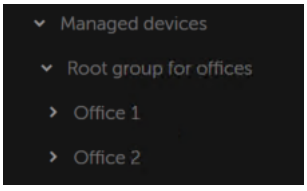
- ネットワークトポロジーを考慮に入れて管理グループの構造を構築します。管理グループの構造が、厳密にネットワークトポロジーを反映していなくても問題ありません。ネットワークが区切られた各部分と特定の管理グループの間に一致があれば十分です。ディストリビューションポイントの自動割り当てを使用するか、または手動で割り当てることができます。

- ネットワークトポロジーを考慮に入れずに管理グループの構造を構築します。この場合は、ディストリビューションポイントの自動割り当てを無効にしてから、ディストリビューションポイントとして動作する1台以上のデバイスをネットワークの区切られた各部分のルート管理グループ（たとえば、**管理対象デバイス**グループ）に対して割り当てる必要があります。ディストリビューションポイントは、すべて同じレベルに置かれ、組織ネットワーク内のすべてのデバイスを包含する同じ範囲を対象とします。この場合、各ネットワークエージェントは最短経路のディストリビューションポイントに接続します。ディストリビューションポイントへの経路は、tracert ユーティリティによって追跡できます。

ディストリビューションポイントの標準設定：複数の小規模なリモートオフィス

この標準設定は、インターネットを介して本社と通信する可能性のある多数の小規模なリモートオフィス向けの設定です。各リモートオフィスは NAT を介するようにその背後に配置されています。つまり、2 つのオフィスはお互いに分離されているため、お互いに接続することはできません。

管理グループ構造内で設定を反映させる必要があります。つまり、各リモートオフィスに対して、個別の管理グループを作成する必要があります（下の図のグループ［**Office 1**］と［**Office 2**］）。



管理グループ構造に含まれているリモートオフィス

1つのオフィスに対応する各管理グループに対して、1つまたは複数個のディストリビューションポイントを割り当てる必要があります。ディストリビューションポイントは、リモートオフィスに配置された空きディスク容量が十分なデバイスである必要があります。たとえば、［**Office 1**］グループに導入されているデバイスは、［**Office 1**］管理グループに割り当てられているディストリビューションポイントにアクセスできます。

ノート PC を持ち運んでオフィス間を移動するユーザーが存在する場合は、各リモートオフィスで 2 台以上のデバイス（既存のディストリビューションポイントに加えて）を選択し、それらのデバイスをトップレベルの管理グループ（上の図の［**Root group for offices**］）用のディストリビューションポイントとして動作するように割り当てる必要があります。

例：［**Office 1**］管理グループ内にノート PC を導入しましたが、［**Office 2**］管理グループに対応するオフィスにマシンを持って移動するとします。ノート PC を移動させると、ネットワークエージェントは［**Office 1**］グループに割り当てられているネットワークエージェントへのアクセスを試行しますが、これらのディストリビューションポイントは使用不可の状態です。次に、ネットワークエージェントは、［**Root group for offices**］に割り当てられているディストリビューションポイントへのアクセスの試行を開始します。リモートオフィスはお互いに分離されているため、［**Root group for offices**］管理グループに割り当てられているディストリビューションポイントへのアクセスの試行は、ネットワークエージェントが［**Office 2**］グループ内にあるディストリビューションポイントへのアクセスを試行した際にのみ正常に実行されます。つまり、ノート PC は最初のオフィスに対応する管理グループ内に残りますが、ディストリビューションポイントについては移動後のオフィスに存在するディストリビューションポイントを使用します。

ディストリビューションポイントの数の計算と設定

ネットワークに存在するクライアントデバイスの数に応じて、必要となるディストリビューションポイントの数も多くなります。ディストリビューションポイントの自動割り当ては、できるだけ使用しないでください。ディストリビューションポイントの自動割り当てが有効になっており、クライアントデバイスの数が非常に多い場合、管理サーバーがディストリビューションポイントの割り当てと設定を行います。

用途専用のディストリビューションポイントの使用

特定のデバイスをディストリビューションポイントとして使用する場合（たとえば、この用途専用で割り当てられたサーバー）、ディストリビューションポイントの自動割り当ては使用しないでください。また、ディストリビューションポイントとして使用するデバイスは、十分な空きディスク容量があること、定期的にシャットダウンされないこと、スリープモードが無効になっていることを確認してください。

単一のセグメントで構成されるネットワーク上での、デバイス数に応じた用途専用のディストリビューションポイントの数

ネットワークセグメントでのクライアントデバイスの数	ディストリビューションポイントの数
300 台未満	0（ディストリビューションポイントを割り当てない）
300 以上	許容：N/10,000 + 1、推奨：N/5,000 + 2（N はネットワーク上のデバイスの数）

複数のセグメントで構成されるネットワーク上での、デバイス数に応じた用途専用のディストリビューションポイントの数

各ネットワークセグメントでのクライアントデバイスの数	ディストリビューションポイントの数
10 台未満	0（ディストリビューションポイントを割り当てない）
10～100	1
100 以上	許容：N/10,000 + 1、推奨：N/5,000 + 2（N はネットワーク上のデバイスの数）

通常のクライアントデバイス（ワークステーション）のディストリビューションポイントとしての使用

通常のクライアントデバイス（ワークステーション）をディストリビューションポイントとして使用する場合、管理サーバーと通信チャネルの負荷低減のために、下表に従ってディストリビューションポイントを割り当ててください。

単一のセグメントで構成されるネットワーク上での、デバイス数に応じた、ディストリビューションポイントとして動作するワークステーションの数

ネットワークセグメントでのクライアントデバイスの数	ディストリビューションポイントの数
300 台未満	0（ディストリビューションポイントを割り当てない）
300 以上	N/300 + 1（N はネットワーク上のデバイスの数。ただし、ディストリビューションポイントは 3 台以上必要）

複数のセグメントで構成されるネットワーク上での、デバイス数に応じた、ディストリビューションポイントとして動作するワークステーションの数

各ネットワークセグメントでのクライアントデバイスの数	ディストリビューションポイントの数
10 台未満	0（ディストリビューションポイントを割り当てない）
10～30	1
31～300	2
300 以上	N/300 + 1（N はネットワーク上のデバイスの数。ただし、ディストリビューションポイントは 3 台以上必要）

ディストリビューションポイントがシャットダウンされた（もしくは、何らかの理由により使用できない）場合も、ディストリビューションポイントの対象範囲に含まれる管理対象デバイスは管理サーバーにアクセスしてアップデートを取得できます。

ディストリビューションポイントの自動的な割り当て

ディストリビューションポイント用デバイスは、自動的に割り当てることを推奨します。自動的に割り当てる場合、ディストリビューションポイントに指定するデバイスを Kaspersky Security Center Linux が選択します。

ディストリビューションポイントを自動的に割り当てるには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. ［**全般**］タブで、［**ディストリビューションポイント**］セクションを選択します。
3. ［**ディストリビューションポイントを自動的に割り当て**］をオンにします。

   ディストリビューションポイントとしてのデバイスの自動割り当てが有効な場合、手動でディストリビューションポイントを設定したりディストリビューションポイントのリストを編集したりすることはできません。

4. ［**保存**］をクリックします。

管理サーバーが自動的にディストリビューションポイントを割り当てて設定します。

ディストリビューションポイントの手動での割り当て

Kaspersky Security Center Linux で、ディストリビューションポイントとして動作するデバイスを手動で指定できます。

ディストリビューションポイント用デバイスは、自動的に割り当てることを推奨します。自動的に割り当てる場合、ディストリビューションポイントに指定するデバイスを Kaspersky Security Center Linux が選択します。何らかの理由（たとえば、この用途専用で割り当てられたサーバーを使用する、など）により自動割り当てが選択できない場合、ディストリビューションポイント数の計算と設定を行った後に、手動でディストリビューションポイントを割り当てることができます。

ディストリビューションポイントとして動作するデバイスについては、あらゆる不正なアクセスに対して、物理的な保護も含めて保護する必要があります。

ディストリビューションポイントとして動作するデバイスを手動で指定するには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. ［**全般**］タブで、［**ディストリビューションポイント**］セクションを選択します。
3. ［**ディストリビューションポイントを手動で割り当て**］をオンにします。
4. ［**割り当て**］をクリックします。
5. ディストリビューションポイントとして動作させるデバイスを選択します。
   デバイスを選択する際は、ディストリビューションポイントの動作とディストリビューションポイントとして動作するデバイスの要件を確認してください。
6. 選択したディストリビューションポイントの受け持ち範囲に含める管理グループを選択します。
7. ［OK］をクリックします。
   追加されたディストリビューションポイントが、［**ディストリビューションポイント**］セクションのディストリビューションポイントのリストに表示されます。
8. 新しく追加したディストリビューションポイントをリストからクリックし、プロパティウィンドウを開きます。
9. プロパティウィンドウでディストリビューションポイントを設定します。
   - ［General］セクションには、ディストリビューションポイントとクライアントデバイスの間の通信の設定があります。
     - **SSL ポート**
       SSL を使用したクライアントデバイスとディストリビューションポイントの間の暗号化接続で使用する SSL ポートの番号。
       既定では、ポート 13000 が使用されます。
     - **マルチキャストを使用する**

このオプションをオンにすると、グループ内にあるクライアントデバイスへのインストールパッケージの自動配布に IP マルチキャストが使用されます。

IP マルチキャストを使用すると、インストールパッケージからクライアントデバイスのグループに製品をインストールするのに必要な時間が短縮されます。一方で、1 台のクライアントデバイスに製品をインストールする場合は、インストールの時間は長くなります。

- **マルチキャスト IP アドレス**

  マルチキャストで使用される IP アドレス。224.0.0.0 ～ 239.255.255.255 の範囲で IP アドレスを定義できます。

  既定では、Kaspersky Security Center Linux は定められた範囲内で一意の IP マルチキャストアドレスを自動的に割り当てます。

- **IP マルチキャストポート番号**

  IP マルチキャストのポート番号。

  既定では、ポート番号は 15001 です。管理サーバーがインストールされたデバイスがディストリビューションポイントとして指定された場合、既定では SSL 接続でポート 13001 が使用されます。

- **リモートデバイスのゲートウェイアドレス**

  リモートデバイスがディストリビューションポイントに接続するために使用する IPv4 アドレス。

- **アップデートの配信**

  アップデートは、次のアップデート元から管理対象デバイスに配布されます：

  - このオプションがオンの場合は、このディストリビューションポイントです。
  - このオプションがオフの場合は、管理サーバーやカスペルスキーのアップデートサーバーなどその他のディストリビューションポイントです。

  アップデートの配信にディストリビューションポイントを使用している場合は、ダウンロード数を減らすため、トラフィックを節約できます。また、管理サーバーの負荷を軽減し、ディストリビューションポイント間の負荷を移動することもできます。ネットワークのディストリビューションポイントの数を計算して、トラフィックと負荷を最適化できます。

  このオプションをオフにすると、アップデートのダウンロード数が増えて管理サーバーの負荷が増加する可能性があります。既定では、このオプションはオンです。

- **インストールパッケージの配布**

インストールパッケージは、次の配布元から管理対象デバイスに配布されます：

- このオプションがオンの場合は、このディストリビューションポイントです。
- このオプションがオフの場合は、管理サーバーやカスペルスキーのアップデートサーバーなどその他のディストリビューションポイントです。

インストールパッケージの配信にディストリビューションポイントを使用すると、ダウンロード数を減らすため、トラフィックを節約できます。また、管理サーバーの負荷を軽減し、ディストリビューションポイント間の負荷を移動することもできます。ネットワークのディストリビューションポイントの数を計算して、トラフィックと負荷を最適化できます。

このオプションをオフにすると、アップデートのダウンロード数が増えて管理サーバーの負荷が増加する可能性があります。既定では、このオプションはオンです。

- **プッシュサーバーを実行**

Kaspersky Security Center で、ディストリビューションポイントをモバイルプロトコルを使用して管理されているデバイスおよび Network Agent により管理されているデバイスのプッシュサーバーとして動作させることができます。たとえば、KasperskyOS デバイスと管理サーバー間の強制同期を実行可能にする時に、プッシュサーバーを有効にする必要があります。プッシュサーバーの管理デバイスの範囲は、プッシュサーバーを有効にするディストリビューションポイントの範囲と同じです。同一の管理グループに複数のディストリビューションポイントを割り当てている場合は、各ディストリビューションポイントに対してプッシュサーバーを有効に設定できます。この場合、管理サーバーはディストリビューション間の負荷を分散します。

- **プッシュサーバーのポート**

プッシュサーバー用のポート番号です。使用されていないポートの番号を入力できます。

- ［**Scope**］セクションで、ディストリビューションポイントがアップデートを配信する管理グループを指定します。
- ［**アップデート元**］セクションで、ディストリビューションポイントのアップデート元を選択します。
  - **アップデート元**

ディストリビューションポイントのアップデート元を選択します：

- ディストリビューションポイントが管理サーバーからアップデートを取得できるようにするには、［**管理サーバーから取得**］をオンにします。
- タスクを使用してディストリビューションポイントがアップデートを受信できるようにするには、［**アップデートのダウンロードタスクを使用**］をオンにして、［*ディストリビューションポイントのリポジトリにアップデートをダウンロード*］タスクを指定します：
  - そのようなタスクが既にデバイスにある場合は、リストからタスクを選択します。
  - タスクがデバイスに存在しない場合、［**タスクの作成**］をクリックし、タスクを作成します。タスク追加ウィザードが開始されます。ウィザードの指示に従ってください。

  - **差分ファイルのダウンロード**

このオプションで差分ファイルのダウンロードを有効にすることができます。

既定では、このオプションはオンです。

- ［**インターネット接続設定**］サブセクションでは、インターネットアクセスを設定できます。
  - **プロキシサーバーを使用する**

    このチェックボックスをオンにすると、入力フィールドでプロキシサーバー接続を設定できます。
    既定では、このチェックボックスはオフです。

  - **プロキシサーバーアドレス**

    プロキシサーバーのアドレス。

  - **ポート番号**

    接続に使用されるポート番号。

  - **ローカルアドレスにプロキシサーバーを使用しない**

    このオプションをオンにすると、ローカルネットワークのデバイスへの接続にプロキシサーバーが使用されません。
    既定では、このオプションはオフです。

  - **プロキシサーバー認証**

    このチェックボックスをオンにすると、入力フィールドでプロキシサーバー認証の資格情報を指定できます。
    既定では、このチェックボックスはオフです。

  - **ユーザー名**

    プロキシサーバーへの接続の確立に使用されるユーザーアカウント。

  - **パスワード**

    タスクが実行されるアカウントのパスワード。

- ［**接続ゲートウェイ**］セクションでは、ネットワークエージェントインスタンスと管理サーバー間の接続のゲートウェイとして機能するようにディストリビューションポイントを設定できます。
  - **接続ゲートウェイ**

ネットワークの構成が原因で、管理サーバーとネットワークエージェント間の直接接続を確立できない場合は、ディストリビューションポイントを使用して、管理サーバーとネットワークエージェント間の接続ゲートウェイとして機能させることができます。

ディストリビューションポイントがネットワークエージェントと管理サーバー間の接続ゲートウェイとして機能する必要がある場合は、このオプションをオンにします。既定では、このオプションはオフです。

- **管理サーバー側からゲートウェイ接続を確立する（ゲートウェイが DMZ 内にある場合）**

  管理サーバーがローカル エリア ネットワーク上の非武装地帯（DMZ）の外にある場合、リモートデバイスにインストールされたネットワークエージェントは管理サーバーに接続できません。ディストリビューションポイントをリバース接続の接続ゲートウェイとして使用できます（管理サーバーがディストリビューションポイントへの接続を確立します）。

  管理サーバーを DMZ の接続ゲートウェイに接続する必要がある場合は、このオプションをオンにします。

- **Kaspersky Security Center 14 Web コンソール用にローカルポートを開く**

  DMZ 内またはインターネット上にある Web コンソールのポートを開くために DMZ 内の接続ゲートウェイが必要な場合は、このオプションをオンにします。Web コンソールからディストリビューションポイントへの接続に使用するポート番号を指定します。既定のポート番号は 13299 です。

  このオプションは、［**管理サーバー側からゲートウェイ接続を確立する（ゲートウェイが DMZ 内にある場合）**］をオンにした場合に使用できます。

- **モバイルデバイス用にポートを開く(管理サーバーの SSL 認証のみ)**

  接続ゲートウェイでモバイル デバイス用のポートを開き、モバイルデバイスがディストリビューションポイントへの接続に使用するポート番号を指定する必要がある場合は、このオプションをオンにします。既定のポート番号は 13292 です。接続を確立するときは、管理サーバーのみが認証されます。

- **モバイルデバイス用にポートを開く（SSL 相互認証）**

  管理サーバーとモバイル デバイスの双方向認証に使用されるポートを開くために接続ゲートウェイが必要な場合は、このオプションをオンにします。次のパラメータを指定します：

  - モバイル デバイスがディストリビューションポイントへの接続に使用するポート番号。既定のポート番号は 13293 です。
  - モバイル デバイスで使用される接続ゲートウェイの DNS ドメイン名。ドメイン名はコンマで区切ります。指定したドメイン名は、ディストリビューションポイント証明書に含まれます。モバイル デバイスが使用するドメイン名がディストリビューションポイント証明書の共通名と一致しない場合、モバイル デバイスはディストリビューションポイントに接続しません。

    デフォルトの DNS ドメイン名は、接続ゲートウェイの FQDN 名です。

- ディストリビューションポイントによる IP 範囲のポーリングを設定します。

  - **IP アドレス範囲**

デバイスの検索は IPv4 範囲および IPv6 ネットワークで有効にできます。

［**IP アドレス範囲のポーリングを有効にする**］をオンにすると、対象範囲を追加して実行スケジュールを設定できます。スキャン対象範囲のリストに IP アドレス範囲を追加できます。

［**Zeroconf を使用して IPv6 ネットワークのポーリングを実行する**］をオンにすると、ディストリビューションポイントは自動的にゼロコンフィギュレーションネットワーキング（「*Zeroconf*」とも表記）を使用して IPv6 ネットワークのポーリングを行います。この場合、ディストリビューションポイントはネットワーク全体を検索するため、指定した IP 範囲は無視されます。ディストリビューションポイントが Linux を実行している場合は、［**Zeroconf を使用して IPv6 ネットワークのポーリングを実行する**］を使用できます。Zerocong IPv6 ポーリングを使用するには、ディストリビューションポイントで avahi-browse ユーティリティをインストールする必要があります。

- ［**詳細**］セクションで、配信されたデータの格納用にディストリビューションポイントが使用するフォルダーを指定します。
  - **既定のフォルダーを使用する**

    このオプションをオンにすると、ディストリビューションポイント上でネットワークエージェントがインストールされているフォルダーが使用されます。

  - **指定したフォルダーを使用する**

    このオプションをオンにすると、この下のフィールドで、フォルダーのパスを指定できます。ディストリビューションポイントのローカルフォルダーまたは組織ネットワーク内の任意のデバイス上にあるフォルダーを指定できます。

    ネットワークエージェントの実行時にディストリビューションポイントで使用されるユーザーアカウントには、指定したフォルダーへの読み取りおよび書き込みアクセス権限が必要です。

10. ［**OK**］をクリックします。

選択されたデバイスがディストリビューションポイントとして使用されます。

管理グループに割り当てられたディストリビューションポイントのリストの編集

特定の管理グループに割り当てられたディストリビューションポイントのリストを表示し、ディストリビューションポイントを追加または削除してこのリストを編集できます。

管理グループに割り当てられたディストリビューションポイントのリストの表示と編集を行うには：

1. メインメニューで、［**デバイス**］→［**管理対象デバイス**］の順に移動します。
2. 管理対象デバイスのリストの上にある［**現在のパス**］フィールドで、パスリンクをクリックします。
3. 表示される左側のペインで、割り当てられたディストリビューションポイントを表示する管理グループを選択します。

   これにより、［**ディストリビューションポイント**］メニュー項目をオンにします。
4. メインメニューで、［**デバイス**］→［**ディストリビューションポイント**］の順に選択します。

5. 管理グループに新しいディストリビューションポイントを追加するには、［**割り当て**］をクリックします。

6. 割り当てられたディストリビューションポイントを削除するには、リストからデバイスを選択し、［**割り当て解除**］をクリックします。

変更内容に応じて、新しいディストリビューションポイントがリストに追加されるか、既存のディストリビューションポイントがリストから削除されます。

プッシュサーバーの有効化

Kaspersky Security Center で、ディストリビューションポイントをモバイルプロトコルを使用して管理されているデバイスおよび Network Agent により管理されているデバイスのプッシュサーバーとして動作させることができます。たとえば、KasperskyOS デバイスと管理サーバー間の強制同期を実行可能にする時に、プッシュサーバーを有効にする必要があります。プッシュサーバーの管理デバイスの範囲は、プッシュサーバーを有効にするディストリビューションポイントの範囲と同じです。同一の管理グループに複数のディストリビューションポイントを割り当てている場合は、各ディストリビューションポイントに対してプッシュサーバーを有効に設定できます。この場合、管理サーバーはディストリビューション間の負荷を分散します。

ディストリビューションポイントをプッシュサーバーとして使用して、管理対象デバイスと管理サーバー間の継続的な接続を確認できます。ローカルタスクの実行と停止、管理対象アプリケーションの統計の受信、トンネルの作成など、一部の操作には継続的な接続が必要です。ディストリビューションポイントをプッシュサーバーとして使用する場合は、管理対象デバイスで［**管理サーバーから切断しない**］をオンにしたり、ネットワークエージェントの UDP ポートにパケットを送信したりする必要はありません。

プッシュサーバーは、最大 50,000 件の同時接続の負荷をサポートします。

ディストリビューションポイントでプッシュサーバーを有効にするには：

1. 目的の管理サーバーを選択し、横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。

2. ［**全般**］タブで、［**ディストリビューションポイント**］セクションを選択します。

3. プッシュサーバーを有効にするディストリビューションポイントの名前をクリックします。
   ディストリビューションポイントのプロパティウィンドウが開きます。

4. ［**全般**］セクションで、［**プッシュサーバーを実行**］をオンにします。

5. ［**プッシュサーバーのポート**］フィールドで、ポート番号を入力します。使用されていないポートの番号を入力できます。

6. ［**リモートホストのアドレス**］フィールドで、ディストリビューションポイントデバイスの IP アドレスまたは名前を指定します。

7. ［OK］をクリックします。

選択したディストリビューションポイントでプッシュサーバーが有効になります。

クライアントデバイス上のサードパーティ製品の管理

このセクションでは、クライアントデバイスで実行されているサードパーティ製ソフトウェアの管理に関わるKaspersky Security Center Linuxの機能について説明します。

シナリオ：アプリケーションの管理

ユーザーデバイス上でのアプリケーションの起動を管理できます。管理対象デバイス上でのアプリケーションの起動を許可またはブロックできます。この用途には、アプリケーションコントロール機能を使用します。

アプリケーションコントロールはKaspersky Endpoint Security 11.2 for Linux以降のバージョンで使用可能です。

必須条件

- 組織内にKaspersky Security Center Linuxが導入されている。
- Kaspersky Endpoint Security for Linuxポリシーを作成済みで、ポリシーがアクティブになっている。

実行するステップ

アプリケーションコントロールのユーザーシナリオは次のステップに分かれています：

1. **クライアントデバイス上の実行ファイルのリストの作成と表示**

   このステップでは、管理対象デバイスでどのような実行ファイルが検知されたかを把握できます。実行ファイルのリストを表示して、許可対象の実行ファイルと禁止対象の実行ファイルのリストと照合してください。組織の情報セキュリティポリシーに関連した制限が実行ファイルに対して必要になる場合もあります。管理対象デバイスにどのような実行ファイルが存在するかを、既に正確に把握できている場合は、このステップをスキップできます。

   実行手順の説明：クライアントデバイス上の実行ファイルのリストの取得と表示

2. **組織内で使用されているアプリケーションのアプリケーションカテゴリの作成**

   管理対象デバイスに保管されている実行ファイルのリストを分析します。分析結果に基づいて、アプリケーションカテゴリを作成します。組織内で標準的に使用されているアプリケーションで構成される「作業アプリケーション」カテゴリを作成すると有用です。様々なユーザーグループが仕事で異なるアプリケーションセットを使用している場合は、ユーザーグループごとに別個のアプリケーションカテゴリを作成できます。

   実行手順の説明：コンテンツが手動で追加されるアプリケーションカテゴリの作成

3. **Kaspersky Endpoint Security for Linuxポリシーでのアプリケーションコントロール機能の設定**

   上述したステップで作成したアプリケーションカテゴリを使用して、Kaspersky Endpoint Security for Linuxポリシー内でアプリケーションコントロール機能を設定します。

4. **アプリケーションコントロールの設定の検証**

   次の手順がすべて完了していることを確認してください：

   - アプリケーションカテゴリの作成

- アプリケーションカテゴリを使用するアプリケーションコントロールルールの設定

結果

すべての手順を完了すると、管理対象デバイスでのアプリケーションの起動コントロールが実現します。ユーザーは、組織で許可されているアプリケーションのみを実行でき、禁止されているアプリケーションは実行できなくなります。

アプリケーションコントロールの詳細については、「Kaspersky Endpoint Security for Linux Help」を参照してください。

アプリケーションコントロールの概要

アプリケーションコントロールは、アプリケーションを起動しようとするユーザーの試みを監視し、アプリケーションコントロールルールによってアプリケーションの起動を制御します。

アプリケーションコントロールは Kaspersky Endpoint Security 11.2 for Linux以降のバージョンで使用可能です。

パラメータがいずれのアプリケーションコントロールルールとも一致していないアプリケーションの起動は、アプリケーションコントロール機能の動作モードに応じて次のように制御されます：

- *拒否リスト*：ブロックルールで指定しているアプリケーション以外のすべてのアプリケーションの起動を許可するには、このモードを使用します。既定ではこのモードが選択されます。
- *許可リスト*。許可ルールで指定しているアプリケーション以外のすべてのアプリケーションの起動をブロックするには、このモードを使用します。

アプリケーションコントロールルールは、アプリケーションカテゴリを通じて実装されます。どのようなアプリケーションをカテゴリに含めるかの基準を指定してアプリケーションカテゴリを作成できます。Kaspersky Security Center Linux では、手動でコンテンツを追加するカテゴリのみ作成できます。ファイルのメタデータ、ハッシュコード、証明書、KL カテゴリ、ファイルパスなど、実行ファイルをカテゴリに含める条件を指定します。

アプリケーションコントロールの詳細については、「Kaspersky Endpoint Security for Linux Help」を参照してください。

クライアントデバイス上の実行ファイルのリストの取得と表示

管理対象デバイス上に保管された実行ファイルのリストを取得できます。実行ファイルのインベントリを実行するには、インベントリタスクを作成する必要があります。

実行ファイルのインベントリ機能は Kaspersky Endpoint Security 11.2 for Linux 以降のバージョンで使用できます。

クライアントデバイス上の実行ファイルのインベントリタスクを作成するには：

1. ［**デバイス**］→［**タスク**］の順に選択します。
   タスクのリストが表示されます。

2. ［**追加**］をクリックします。

   新規タスクウィザードが起動します。ウィザードの指示に従ってください。

3. ［**新規タスク**］ウィンドウの［**アプリケーション**］ドロップダウンリストで、Kaspersky Endpoint Security for Linux を選択します。

4. ［**タスク種別**］ドロップダウンリストから、［**インベントリ**］を選択します。

5. ［**タスク作成の終了**］ページで、［**終了**］をクリックします。

   新規タスクウィザードの終了後、指定した設定で**インベントリ**タスクが作成されます。必要に応じて、作成したタスクの設定を編集できます。作成したタスクはタスクリストに表示されます。

インベントリタスクについて詳しくは、Kaspersky Endpoint Security for Linux のオンラインヘルプを参照してください。

インベントリタスクの実行が完了すると、管理対象デバイス上に保管された実行ファイルのリストが作成され、このリストを表示できるようになります。

インベントリでは、次の形式の実行ファイルが検出されます：MZ、COM、PE、NE、SYS、CMD、BAT、PS1、JS、VBS、REG、MSI、CPL、DLL、JAR、HTML。

クライアントデバイス上に保管された実行ファイルのリストを表示するには：

［**操作**］→［**サードパーティ製品**］ドロップダウンリストで、［**実行ファイル**］を選択します。

クライアントデバイス上に保管された実行ファイルのリストが表示されます。

コンテンツが手動で追加されるアプリケーションカテゴリの作成

組織内で起動を許可またはブロックする実行ファイルのテンプレートとしての条件を、単独でまたは組み合わせて指定できます。一定の条件に一致する実行ファイルをまとめて管理するために、アプリケーションカテゴリを作成してアプリケーションコントロールの設定で使用できます。

コンテンツが手動で追加されるアプリケーションカテゴリを作成するには：

1. ［**操作**］→［**サードパーティ製品**］ドロップダウンリストから、［**アプリケーションカテゴリ**］を選択します。

   アプリケーションカテゴリのリストが表示されます。

2. ［**追加**］をクリックします。

   新規カテゴリウィザードが起動します。ウィザードの指示に従ってください。

3. ウィザードの［**カテゴリの作成方法の選択**］ページで、［**手動でコンテンツを追加するカテゴリ：実行ファイルのデータを手動でカテゴリに追加します**］を選択します。

4. ウィザードの［**条件**］ページで［**Add**］をクリックして、作成中のカテゴリに含めるファイルの条件を追加します。

5. ［**条件の基準**］ページで、カテゴリを作成するルールの種別をリストから選択します：

- **リポジトリから証明書を選択**

  このオプションをオンにすると、保管領域の証明書を指定できます。指定された証明書に従って署名された実行ファイルが、アプリケーションカテゴリに追加されます。

- **アプリケーションのパスを指定（マスクをサポート）**

  このオプションをオンにすると、クライアントデバイス上のフォルダーのパスを指定できます。そのフォルダーに含まれる実行ファイルが、アプリケーションカテゴリに追加されます。

- **リムーバブルドライブ**

  このオプションをオンにすると、アプリケーションを実行するメディアの種別（任意のドライブまたはリムーバブルドライブ）を指定できます。指定した種別のドライブ上で実行されたアプリケーションが、アプリケーションカテゴリに追加されます。

- **ハッシュ、メタデータ、証明書のいずれか**：

  - **実行ファイルリストから選択**

    このオプションをオンにすると、クライアントデバイス上の実行ファイルのリストを使用して、アプリケーションを選択してカテゴリに追加できます。

  - **アプリケーションレジストリから選択**

    このオプションをオンにすると、アプリケーションレジストリが表示されます。アプリケーションをレジストリから選択し、次のようなファイルのメタデータを指定できます：

    - ファイル名。
    - ファイルバージョン。バージョンの正確な数字を指定することも、「次より多い：5.0」のような条件を指定することもできます。
    - アプリケーション名。
    - アプリケーションのバージョン。バージョンの正確な数字を指定することも、「次より多い：5.0」のような条件を指定することもできます。
    - 製造元。

  - **手動で指定**

このオプションをオンにした場合、ファイルのハッシュ、メタデータ、証明書のいずれかを、アプリケーションカテゴリにアプリケーションを追加する条件として指定する必要があります。

ファイルのハッシュ

ネットワーク内のデバイスにインストールされているセキュリティ製品のバージョンに応じて、このカテゴリ内のファイルに、Kaspersky Security Center Linux によるハッシュ値計算のアルゴリズムを選択する必要があります。計算されたハッシュ値に関する情報は、管理サーバーのデータベースに保存されます。ハッシュ値の保存でデータベースのサイズが大幅に増えることはありません。

暗号学的ハッシュ関数 SHA-256 はアルゴリズムに脆弱性が発見されておらず、現在最も信頼できる暗号化機能とみなされています。Kaspersky Endpoint Security for Linux は、SHA-256 コンピューティングをサポートしています。

カテゴリ内のファイルに、Kaspersky Security Center Linux によるハッシュ値計算のオプションを選択します：

- ネットワークにインストールされているセキュリティ製品のすべてのインスタンスが Kaspersky Endpoint Security for Linux である場合は、［**SHA-256**］をオンにします。
- Kaspersky Endpoint Security for Windows を使用する場合にのみ、［**MD5 ハッシュ**］をオンにします。Kaspersky Endpoint Security for Linux は、MD5 ハッシュ関数をサポートしません。

メタデータ

このオプションをオンにすると、ファイル名、バージョン、製造元などのファイルのメタデータを指定できます。メタデータが管理サーバーに送信されます。同じメタデータを含む実行ファイルがアプリケーションカテゴリに追加されます。

証明書

このオプションをオンにすると、保管領域の証明書を指定できます。指定された証明書に従って署名された実行ファイルが、アプリケーションカテゴリに追加されます。

- **アーカイブフォルダーから選択**

このオプションをオンにすると、アーカイブフォルダーのファイルを指定でき、ユーザーカテゴリにアプリケーションを追加するために使用する条件を選択できます。アーカイブフォルダーが解凍され、選択した条件がフォルダー内にあるファイルに適用されます。条件として、以下の基準のいずれかを選択することができます：

- **ファイルのハッシュ**

  MD5 または SHA-256 のどちらを使用してハッシュ値を計算するかを選択します。アーカイブフォルダーにあるファイルとハッシュ値が同じであるアプリケーションが、アプリケーションカテゴリに追加されます。

  Kaspersky Endpoint Security for Windows を使用する場合にのみ、MD5 ハッシュ関数を選択します。Kaspersky Endpoint Security for Linux は、MD5 ハッシュ関数をサポートしません。

- **メタデータ**

  基準として使用するメタデータを選択します。同じメタデータを含む実行ファイルがアプリケーションカテゴリに追加されます。

- **証明書**

  基準として使用する証明書のプロパティ（証明書の発行先、フィンガープリント、発行元）を選択します。同じプロパティを持つ証明書で署名された実行ファイルはユーザーカテゴリに追加されます。

選択した基準が、条件のリストに追加されます。

アプリケーションカテゴリの作成基準は、個数の制限なく必要な数だけ追加できます。

6. ウィザードの［**除外**］ページで［**追加**］をクリックして、作成中のカテゴリから除外するファイルの条件を追加します。

7. ［**条件の基準**］ページで、カテゴリ作成用のルールの種別を選択したときと同様に、リストからルールの種別を選択します。

ウィザードを最後まで完了すると、アプリケーションカテゴリが作成されます。新しいルールがアプリケーションカテゴリのリストに表示されます。アプリケーションコントロールを設定時に作成したアプリケーションカテゴリを使用できます。

アプリケーションコントロールの詳細については、「Kaspersky Endpoint Security for Linux Help」を参照してください。

アプリケーションカテゴリのリストの表示

設定済みのアプリケーションカテゴリのリストと各アプリケーションカテゴリの設定を表示できます。

アプリケーションカテゴリのリストを表示するには：

［**操作**］タブの［**サードパーティ製品**］ドロップダウンリストから、［**アプリケーションカテゴリ**］を選択します。

アプリケーションカテゴリのリストが表示されます。

アプリケーションカテゴリのプロパティを表示するには、

アプリケーションカテゴリの名前をクリックします。

アプリケーションカテゴリのプロパティウィンドウが表示されます。プロパティはいくつかのタブにグループ化されています。

イベントに関連する実行ファイルのアプリケーションカテゴリへの追加

Kaspersky Endpoint Security for Linux のポリシーでアプリケーションコントロールの設定を完了させると、イベントのリストに次のイベントが表示されます：

- **アプリケーションの起動が禁止されました**（*緊急*イベント）：このイベントは、アプリケーションコントロールの設定で、実際にルールを適用するように指定した場合に表示されます。
- **アプリケーションの起動がテストモードでブロックされています**（*情報*イベント）：このイベントは、アプリケーションコントロールの設定で、ルールをテストするように指定した場合に表示されます。
- **アプリケーションの起動ブロックに関するメッセージが管理者に送信されました**（*警告*）：このイベントは、アプリケーションコントロールの設定で実際にルールを適用するように指定しており、起動時にブロックされたアプリケーションへのアクセスをユーザーが要求した場合に表示されます。

アプリケーションコントロールの動作に関するイベントを表示するために、イベントの抽出を作成しておくことを推奨します。

アプリケーションコントロールイベントの対象となった実行ファイルを、既存のアプリケーションカテゴリや新規に作成するアプリケーションカテゴリに追加できます。実行ファイルは、手動でコンテンツを追加するタイプのアプリケーションカテゴリにのみ追加できます。

アプリケーションコントロールイベントの対象となった実行ファイルをアプリケーションカテゴリに追加するには：

1. ［**監視とレポート**］→［**イベントの抽出**］の順に選択します。
   イベントの抽出のリストが表示されます。

2. アプリケーションコントロールに関するイベントを表示するためのイベントの抽出を選択し、イベントの抽出を実行します。
   アプリケーションコントロールに関するイベントを表示するためのイベントの抽出をまだ作成していない場合は、代わりに「**最近のイベント**」などの事前定義済みのイベントの抽出を選択して実行することもできます。
   イベントのリストが表示されます。

3. 対象となった実行ファイルをアプリケーションカテゴリに追加するイベントを選択し、［**カテゴリへ割り当て**］をクリックします。
   新規カテゴリウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

4. ウィザードのウィンドウで、関連する設定を指定します：

   - ［**イベントに関係する実行ファイルへの処理**］セクションで、次のいずれかのオプションをオンにします：

     - **新規アプリケーションカテゴリへ追加**

       イベントに関連する実行ファイルを元に新しいアプリケーションカテゴリを作成する場合は、このオプションをオンにします。
       既定では、このオプションがオンです。
       このオプションを選択する場合は、新しいカテゴリ名を指定してください。

     - **アプリケーションカテゴリへ追加**

       イベントに関連する実行ファイルを既存のアプリケーションカテゴリに追加する場合は、このオプションをオンにします。
       既定では、このオプションはオフです。
       このオプションを選択する場合は、実行ファイルの追加先として、手動でコンテンツを追加するタイプのアプリケーションカテゴリを選択してください。

   - ［**ルールの種別**］セクションで、次のいずれかを選択します：

     - **除外しない場合のルール**
     - **除外に追加する場合のルール**

   - ［**条件として使用する情報**］セクションで、次のいずれかのオプションをオンにします：

- **証明書の詳細情報（証明書がないファイルの場合 SHA-256 ハッシュ）**

  ファイルが証明書によって署名されていることがあります。複数のファイルが同じ証明書で署名されていることがあります。たとえば、同じアプリケーションの異なるバージョンが同じ証明書で署名されていたり、同じ開発元の様々なアプリケーションが同じ証明書で署名されていたりすることがあります。証明書を選択した場合、アプリケーションの複数のバージョンまたは同じ開発元の複数のアプリケーションが同じカテゴリに属す場合があります。

  それぞれのファイルには固有の SHA-256 ハッシュ関数があります。SHA-256 ハッシュ関数を選択した場合、1つのファイル（たとえばアプリケーションの特定のバージョン）のみがカテゴリに属します。

  実行ファイルの証明書の詳細（または証明書がないファイルの SHA-256 ハッシュ機能）をカテゴリルールに追加する場合は、このオプションを選択します。

  既定では、このオプションがオンです。

- **証明書の詳細情報（証明書のないファイルはスキップ）**

  ファイルが証明書によって署名されていることがあります。複数のファイルが同じ証明書で署名されていることがあります。たとえば、同じアプリケーションの異なるバージョンが同じ証明書で署名されていたり、同じ開発元の様々なアプリケーションが同じ証明書で署名されていたりすることがあります。証明書を選択した場合、アプリケーションの複数のバージョンまたは同じ開発元の複数のアプリケーションが同じカテゴリに属す場合があります。

  実行ファイルの証明書の詳細をカテゴリルールに追加する場合は、このオプションを選択します。実行ファイルに証明書がない場合、そのファイルはスキップされます。このファイルに関する情報は、カテゴリに追加されません。

- **SHA-256 のみ（ハッシュのないファイルはスキップ）**

  それぞれのファイルには固有の SHA-256 ハッシュ関数があります。SHA-256 ハッシュ関数を選択した場合、1つのファイル（たとえばアプリケーションの特定のバージョン）のみがカテゴリに属します。

  実行ファイルの SHA-256 ハッシュ機能の詳細だけを追加する場合、このオプションを選択します。

- **MD5 のみ（非推奨、Kaspersky Endpoint Security 10 Service Pack 1 の場合のみ）**

  Kaspersky Endpoint Security for Windows を使用する場合にのみ、このオプションを選択します。Kaspersky Endpoint Security for Linux は、MD5 ハッシュ関数をサポートしません。

  それぞれのファイルには固有の MD5 ハッシュ関数があります。MD5 ハッシュ関数を選択した場合、1つのファイル（たとえばアプリケーションの特定のバージョン）のみがカテゴリに属します。

5. ［OK］をクリックします。

ウィザードが完了すると、アプリケーションコントロールのイベントに関連付けられていた実行ファイルが、既存のアプリケーションカテゴリまたは新規に作成したアプリケーションカテゴリに追加されます。変更または新規に作成したアプリケーションカテゴリの設定を表示できます。

アプリケーションコントロールの詳細については、「Kaspersky Endpoint Security for Linux Help」を参照してください。

監視とレポート

このセクションでは Kaspersky Security Center Linux の監視機能とレポート機能について説明しています。これらの機能を使用して、インフラストラクチャの状況、保護ステータス、統計情報を確認できます。

Kaspersky Security Center Linux の導入後または運用中に、必要に応じて監視とレポート機能の設定を最適な状態に編集できます。

シナリオ：監視とレポート

このセクションでは、Kaspersky Security Center Linux の監視機能とレポート機能を設定する手順を説明しています。

必須条件

組織のネットワークへの Kaspersky Security Center Linux の導入後、監視を開始し、動作状況のレポートを生成できます。

組織のネットワークにおける監視の実施とレポートの利用は、以下の手順で進みます：

1. **デバイスのステータスの切り替えの設定**

   特定の条件に応じたデバイスのステータスの設定方法を確認します。各種設定を変更することで、重要度レベルが「*緊急*」または「*警告*」のイベントの数を変えることができます。デバイスのステータスの切り替えを設定する時には、次の点に注意してください：

   - 新しい設定が組織の情報セキュリティポリシーと矛盾しない。
   - 組織のネットワークにおける重要なセキュリティイベントに迅速に対応できる。

2. **クライアントデバイスで発生したイベントに関する通知の設定**

   実行手順の説明：

   クライアントのデバイス上でイベントの通知（メール、SMS、ファイルの実行）を設定します。

3. **緊急および警告の通知について推奨される処理の実行**

   実行手順の説明：

   組織のネットワークに応じて、推奨される処理を実行する

4. **組織のネットワークのセキュリティステータスの確認**

   実行手順の説明：

   - ［保護ステータス］ウィジェットを確認する
   - ［保護ステータスレポート］を生成し確認する
   - ［エラーに関するレポート］を生成し確認する

5. **保護されていないクライアントデバイスの検出**

   実行手順の説明：

   - ［新しいデバイス］ウィジェットを確認する

- ［製品導入レポート］を生成し確認する

6. **クライアントデバイスの保護状態の確認**

   実行手順の説明：

   - ［保護ステータス］および［脅威の統計］カテゴリからレポートを生成して確認する
   - ［緊急］についてのイベント抽出を開始して確認する

7. **データベースでのイベント情報による負荷の評価と制限**

   管理対象アプリケーションの動作中に発生したイベントに関する情報は、クライアントデバイスから送信され、管理サーバーデータベースに記録されます。管理サーバーの負荷を軽減するには、データベースに保管される可能性のあるイベント数の最大値を評価し、上限を設定します。

   実行手順の説明：

   - イベント数の上限の設定

8. **ライセンス情報の確認**

   実行手順の説明：

   - ［ライセンス使用状況］ウィジェットをダッシュボードに追加して確認をする
   - ［ライセンス使用レポート］を生成し確認する

結果

これらの手順が完了すると、組織のネットワークの保護に関する情報を確認できるようになり、今後のセキュリティ対策の計画や脅威への対応に役立てることができます。

監視機能とレポート機能の種別の概要

組織ネットワーク内のセキュリティ関連のイベントに関する情報は管理サーバーデータベースに保存されます。イベントの情報に基づいて、Kaspersky Security Center 14 Web コンソールでは、組織ネットワークを対象とした次の種別の監視機能とレポート機能を利用できます。

- ダッシュボード
- レポート
- イベントの抽出
- 通知

ダッシュボード

ダッシュボードでは、組織ネットワーク内でのセキュリティトレンドをグラフや表などを通して視覚的に把握し、監視できます。

レポート

レポート機能を使用することで、組織ネットワークのセキュリティに関する詳細な数値データを取得し、これらの情報をファイルに保存したり、メールで送信したり、印刷することができます。

イベントの抽出

イベントの抽出は、管理サーバーのデータベース内に保存されているイベントを一定の条件を指定して抽出し、画面上に表示できる機能です。これらのイベントは、次のカテゴリに従ってグループ化されます：

- 重要度：**緊急イベント**、**機能エラー**、**警告**、**情報イベント**
- 発生時期：**最近のイベント**
- 種別：**ユーザー要求**、**監査イベント**

また、Kaspersky Security Center 14 Web コンソールで編集可能な設定を使用して、ユーザー定義のイベントの抽出を作成し表示できます。

通知

通知機能を使用してイベントのアラート通知を受け取ることで、推奨される処理や担当者が適切と考える対応を行うまでの時間を短縮できます。

ダッシュボードとウィジェット

このセクションでは、ダッシュボードとダッシュボードで利用できるウィジェットについて説明します。このセクションでは、ウィジェットを管理する方法と、ウィジェットの設定について説明します。

ダッシュボードの使用

ダッシュボードでは、組織ネットワーク内でのセキュリティトレンドをグラフや表などを通して視覚的に把握し、監視できます。

Kaspersky Security Center 14 Web コンソールの［**監視とレポート**］セクションで、［**ダッシュボード**］をクリックすると、ダッシュボードが表示されます。

ダッシュボードでは、カスタマイズ可能なウィジェットを利用できます。円グラフや表、棒グラフ、リストなどの各種形式で表示できる様々なウィジェットを選択できます。ウィジェットに表示される情報は自動的に更新されます。更新には1～2分かかります。更新の間隔はウィジェットごとに異なります。設定メニューを使用して、任意のタイミングで手動でウィジェットを更新できます。

既定では、ウィジェットには管理サーバーのデータベースに保存されているイベントの情報が含まれています。

Kaspersky Security Center 14 Web コンソールには、次のカテゴリのウィジェットが既定のウィジェットのセットとして指定されています：

- **保護ステータス**
- **製品の導入**
- **アップデート**

- **脅威の統計**
- **その他**

一部のウィジェットのテキスト情報にはリンクが含まれている場合があります。リンクをクリックすると詳細情報を確認できます。

ダッシュボードの設定では、必要に応じて、ウィジェットの追加、非表示への変更、サイズや表示の変更、移動、設定の変更を行うことができます。

ダッシュボードへのウィジェットの追加

ダッシュボードにウィジェットを追加するには：

1. メインメニューで、［**監視とレポート**］→［**ダッシュボード**］に移動します。
2. ［**Web ウィジェットを追加または復元**］をクリックします。
3. 使用可能なウィジェットのリストから、ダッシュボードに追加するウィジェットを選択します。

   ウィジェットはカテゴリ別にグループ化されています。カテゴリに含まれるウィジェットのリストを表示するには、カテゴリ名の横にあるアイコン（›）をクリックします。
4. ［**追加**］をクリックします。

選択したウィジェットがダッシュボードの一番下に追加されます。

追加したウィジェットの表示と設定を変更できます。

ダッシュボードでウィジェットを非表示にする操作

ダッシュボードで表示中のウィジェットを非表示にするには：

1. メインメニューで、［**監視とレポート**］→［**ダッシュボード**］に移動します。
2. 非表示にするウィジェットに隣接する設定アイコン（⚙）をクリックします。
3. ［**Web ウィジェットを非表示にする**］を選択します。
4. ［**警告**］ウィンドウが表示されたら、［**OK**］をクリックします。

選択したウィジェットが表示されなくなります。いつでも、このウィジェットをもう一度ダッシュボードに追加できます。

ダッシュボードでのウィジェットの移動

ダッシュボードでウィジェットを移動するには：

1. メインメニューで、［**監視とレポート**］→［**ダッシュボード**］に移動します。
2. 移動するウィジェットに隣接する設定アイコン（⚙）をクリックします。
3. ［**移動**］を選択します。
4. ウィジェットを移動する場所をクリックします。選択できるのは別のウィジェットの表示位置のみです。

選択したウィジェットの表示位置が入れ替わります。

ウィジェットのサイズと表示形式の変更

グラフを表示するウィジェットでは、グラフの形式（棒グラフまたは折れ線グラフ）を変更できます。一部のウィジェットではウィジェットのサイズを「コンパクト」「中サイズ」「最大」に変更できます。

ウィジェットの表示形式を変更するには：

1. メインメニューで、［**監視とレポート**］→［**ダッシュボード**］に移動します。
2. 編集するウィジェットに隣接する設定アイコン（⚙）をクリックします。
3. 次のいずれかの手順を実行します：
   - ウィジェットを棒グラフとして表示するには、［**グラフの種別：棒**］をオンにします。
   - ウィジェットを折れ線グラフとして表示するには、［**グラフの種別：折れ線**］をオンにします。
   - ウィジェットの表示領域を変更するには、次の値のうちの1つを選択してください：
     - **コンパクト**
     - **コンパクト（棒グラフのみ）**
     - **中サイズ（円グラフ）**
     - **中サイズ（棒グラフ）**
     - **最大**

選択したウィジェットの表示形式が変更されます。

ウィジェットの設定の変更

ウィジェットの設定を変更するには：

1. メインメニューで、［**監視とレポート**］→［**ダッシュボード**］に移動します。
2. 変更するウィジェットに隣接する設定アイコン（⚙）をクリックします。
3. ［**設定を表示する**］を選択します。

4. ウィジェットの設定ウィンドウが表示されるので、必要に応じてウィジェットの設定を変更します。

5. ［**保存**］をクリックして変更内容を保存します。

選択したウィジェットの設定が変更されます。

どのような設定項目が存在するかは、ウィジェットごとに異なります。一般的な設定項目としてはたとえば次のような設定があります：

- **Web ウィジェットの範囲**（管理グループやデバイスの抽出など、ウィジェットが情報を表示する対象オブジェクトの範囲）。
- **タスクの選択**（ウィジェットが情報を表示する対象タスクの範囲）。
- **時間**（［開始日から終了日まで］、［開始日から現在まで］、［今日から指定した日数だけ過去にさかのぼった範囲を対象］のいずれかの形式で指定できる、ウィジェットが情報を表示する対象期間）。
- **ステータスを「緊急」にする条件**および**ステータスを「警告」にする条件**（ステータス信号の色を決定するルール）。

ダッシュボードのみモードについて

幹部社員など、ネットワークを管理してはいないが、Kaspersky Security Center でネットワークの保護ステータスを表示する必要がある社員に対して［ダッシュボードのみモード］を設定することができます。ユーザーがこのモードを有効にすると、事前設定されたウィジェットのあるダッシュボードのみが表示されます。このように、すべての管理対象デバイスの保護ステータスや、最近検知された脅威数、またはネットワーク内で頻繁に検知される脅威など、ウィジェットで指定された統計情報を管理できます。

ユーザーがダッシュボードのみモードで作業する場合、次の制限事項が適用されます：

- ユーザーにはメインメニューは表示されません。そのためネットワーク保護の設定などを変更することはできません。
- ユーザーはウィジェットに対して表示もしくは非表示にするなどの操作を行うことはできません。そのため、オブジェクトの計算ルールや時間間隔の指定など、ユーザーに必要なすべてのウィジェットをダッシュボードに表示できるように設定する必要があります。

自分自身にダッシュボードのみモードを割り当てることはできません。このモードで作業したい時は、システム管理者、マネージドサービスプロバイダー（MSP）、または［**一般的な機能：ユーザー権限**］機能領域の**オブジェクト ACL の変更**権限を持つユーザーに問い合わせてください。

ダッシュボードのみモードの設定

ダッシュボードのみモードの設定を始める前に、次の要件を満たしていることを確認してください：

- ［**一般的な機能：ユーザー権限**］機能領域の**オブジェクト ACL の変更**権限を持っている。この権限を持っていない場合、モードの設定用タブは表示されません。
- ［**一般的な機能:：基本機能**］の機能領域の**読み取り**権限を持っている。

ネットワークで管理サーバーの階層が配置されている場合、ダッシュボードのみモードを設定するには［**ユーザーとロール**］→［**ユーザー**］セクションでユーザーアカウントが使用できるサーバーに移動します。プライマリサーバーまたは物理セカンダリサーバーを選択できます。仮想サーバーでモードを調整することはできません。

ダッシュボードのみモードを設定するには：

1. メインメニューで、［**ユーザーとロール**］→［**ユーザー**］の順に移動します。
2. ダッシュボードのウィジェットを調整するユーザーアカウント名をクリックします。
3. アカウント設定ウィンドウが表示されたら、［**ダッシュボード**］を選択します。
   表示されたタブに、ユーザーに表示されるものと同じダッシュボードが表示されます。
4. ［**ダッシュボードのみモードでコンソールを表示**］オプションがオンになっている場合は切り替えスイッチをオフにします。
   このオプションがオンになっていると、自身もダッシュボードを変更することができません。このオプションをオフにした後、ウィジェットを管理できるようになります。
5. ダッシュボードの表示を設定します。カスタマイズ可能なアカウントを持つユーザー向けに、［**ダッシュボード**］タブで事前設定されたウィジェットのセットが使用可能です。ユーザーはウィジェットのサイズや設定を変更したり、ダッシュボードからウィジェットを追加したり削除したりすることはできません。そのため、ユーザーに対してネットワーク保護の統計が表示されるようにウィジェットを調整します。［**監視とレポート**］→［**ダッシュボード**］セクションで行うのと同様の操作を［**ダッシュボード**］タブで実行します：
   - ダッシュボードに新しいウィジェットを追加します。
   - ユーザーに必要ないウィジェットを非表示にします。
   - 必要な順番にウィジェットを移動します。
   - ウィジェットの表示方法やサイズを変更します。
   - ウィジェットの設定を変更します。
6. ［**ダッシュボードのみモードでコンソールを表示**］オプションの切り替えスイッチをオンにします。
   その後、ユーザーはダッシュボードのみを使用できるようになります。ユーザーは統計情報を監視できますが、ネットワーク保護の設定やダッシュボードの表示を変更することはできません。ユーザーとお客様ご自身にも同じダッシュボードが表示され、お客様もダッシュボードを変更することはできません。
   このオプションをオフにしておくと、ユーザーにはメインメニューが表示され、ユーザーは Kaspersky Security Center でセキュリティ設定やウィジェットの変更を含む、様々な操作を実行することができます。
7. ダッシュボードのみモードの設定を完了したら、［**保存**］をクリックします。この後、準備したダッシュボードがユーザーに表示されます。
8. ユーザーが、サポートされるカスペルスキー製品の統計を表示するアクセス権を必要とする場合は、ユーザーの権限を設定します。設定すると、カスペルスキー製品のデータがユーザーのこれらのアプリケーションのウィジェットに表示されるようになります。

ユーザーはカスタマイズされたアカウントで Kaspersky Security Center にログインし、ダッシュボードのみモードでネットワーク保護の統計を監視できるようになりました。

レポート

このセクションでは、レポートの使用、カスタムレポートテンプレートの管理、レポートテンプレートを使用した新規レポートの作成、レポートの配信タスクの作成について説明します。

レポートの使用

レポート機能を使用することで、組織ネットワークのセキュリティに関する詳細な数値データを取得し、これらの情報をファイルに保存したり、メールで送信したり、印刷することができます。

Kaspersky Security Center 14 Web コンソールの［**監視とレポート**］セクションで、［**レポート**］をクリックすると、レポートが表示されます。

既定では、レポートには過去 30 日の情報が含まれます。

Kaspersky Security Center Linux には、次のカテゴリのレポートが既定のレポートのセットとして指定されています：

- **保護ステータス**
- **製品の導入**
- **アップデート**
- **脅威の統計**
- **その他**

カスタムレポートテンプレートの作成、レポートテンプレートの編集、レポートテンプレートの削除を行うことができます。

既存のテンプレートに基づくレポートの作成、ファイルへのレポートのエクスポート、レポートの配信タスクの作成を行うことができます。

レポートテンプレートの作成

レポートテンプレートを作成するには：

1. メインメニューで、［**監視とレポート**］→［**レポート**］に移動します。
2. ［**追加**］をクリックします。

   新規レポートテンプレートウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。
3. ウィザードの最初のページで、レポート名の入力とレポート種別の選択を行います。
4. ウィザードの［**範囲**］ウィンドウで、このレポートテンプレートに基づいたレポートでデータの表示対象にするクライアントデバイスを指定します（管理グループ、デバイスの抽出、指定したデバイス、ネット

ワーク内のすべてのデバイス）。

5. ウィザードの［**レポート期間**］ウィンドウで、レポートの対象期間を指定します。次の値を設定できます：

   - 指定した 2 つの日付の間の期間
   - 指定日からレポート作成日までの期間
   - レポート作成日から指定した日数だけ過去にさかのぼった期間

   一部のレポートではこのページが表示されない場合もあります。

6. ［**OK**］をクリックしてウィザードを終了します。

7. 次のいずれかの手順を実行します：

   - ［**保存して実行**］をクリックすると、新しいレポートテンプレートを保存して、テンプレートに基づくレポートを実行できます。
     レポートテンプレートが保存されます。レポートが生成されます。
   - ［**保存**］をクリックすると、新しいレポートテンプレートを保存できます。
     レポートテンプレートが保存されます。

新しいテンプレートを使用して、レポートの作成と表示ができます。

レポートテンプレートのプロパティの表示と編集

レポートテンプレートについて、レポートテンプレートの名前やレポートに表示されるフィールドなどの基本的なプロパティを表示し、編集できます。

レポートテンプレートのプロパティを表示したり編集するには：

1. メインメニューで、［**監視とレポート**］→［**レポート**］に移動します。

2. プロパティの表示と編集を行うレポートテンプレートに隣接するチェックボックスを選択します。
   あるいは、まずレポートを生成して、次に［**編集**］をクリックします。

3. ［**レポートテンプレートのプロパティを開く**］をクリックします。
   ［**レポート「<レポート名>」の編集**］ウィンドウの［**全般**］タブが表示されます。

4. レポートテンプレートのプロパティを編集します。

   - ［**全般**］タブ：
     - レポートテンプレート名
     - **表示する項目数の上限**

このオプションをオンにすると、詳細なレポートデータの表に表示されるエントリ数に、指定した上限値が設定されます。

レポートのエントリは、レポートテンプレートの［**フィールド**］→［**詳細フィールド**］セクションで指定したルールに従って並べ替えられ、合致するエントリのうち表示順が上のエントリだけが維持されます。詳細レポートのタイトルには、レポートテンプレートで設定したその他の条件に合致するエントリの合計数と表示されている数が表示されます。

このオプションをオフにすると、詳細なレポートデータの表にはすべての使用可能なエントリが表示されますこのオプションをオフにすることは推奨されません。表示されるレポートエントリの数を制限することにより、DBMS（データベース管理システム）の負荷を減らし、レポートの生成とエクスポートの所要時間を削減できます。一部のレポートではエントリ数が多すぎる場合があります。このような場合、すべてのエントリに目を通し分析することは困難です。また、こうしたレポートの生成中にデバイスのメモリ不足が発生し、レポート自体を表示できない可能性もあります。

既定では、このオプションはオンです。既定値は 1000 です。

- **グループ**

  レポートの作成対象にするクライアントデバイスを変更するには、［**設定**］をクリックします。一部のレポートの種別では、このボタンを使用できない場合があります。実際の設定は、レポートテンプレートの作成時に指定した設定によって異なります。

- **時間**

  レポートの対象期間を変更するには、［**設定**］をクリックします。一部のレポートの種別では、このボタンを使用できない場合があります。次の値を設定できます：

  - 指定した 2 つの日付の間の期間
  - 指定日からレポート作成日までの期間
  - レポート作成日から指定した日数だけ過去にさかのぼった期間

- **セカンダリまたは仮想管理サーバーのデータを含める**

  このオプションをオンにすると、レポートテンプレートを作成する管理サーバーに属するセカンダリ管理サーバーおよび仮想管理サーバーからの情報をレポートに含めます。

  現在の管理サーバーのデータのみを表示する場合は、このオプションをオフにします。

  既定では、このオプションはオンです。

- **ネスト数の上限**

  対象の管理サーバーに属するセカンダリ管理サーバーおよび仮想管理サーバーのうち、指定したネスト数以内のサーバーのデータをレポートに含めます。

  既定値は 1 です。ツリー内でより下位に位置するセカンダリ管理サーバーの情報を取得する必要がある場合、この値を変更することができます。

- **データの待機時間（分）**

レポートを生成する前に、レポートテンプレートを作成する管理サーバーは、セカンダリ管理サーバーからデータが送信されるのを、指定した分数だけ待機します。指定した時間が経過してもセカンダリ管理サーバーからデータを取得できなかった場合は、これらのデータを除外してレポートが実行されます。［**セカンダリ管理サーバーのデータをキャッシュする**］を有効にすると、実際のデータの代わりにキャッシュデータがレポートに表示されます。無効にすると、［**該当なし**］と表示されます。

既定値は 5 分です。

- **セカンダリ管理サーバーのデータをキャッシュする**

  セカンダリ管理サーバーからレポートテンプレートを作成する管理サーバーに定期的にデータが送信されます。送信されたデータはキャッシュに保存されます。

  レポートの生成時に現在の管理サーバーがセカンダリ管理サーバーからデータを取得できなかった場合、キャッシュから取得したデータがレポートに表示されます。データがキャッシュに送信された日付も合わせて表示されます。

  このオプションをオンにすると、最新のデータを取得できなかった場合でもセカンダリ管理サーバーの情報を表示できます。ただし、表示されるデータが最新のものではない場合があります。

  既定では、このオプションはオフです。

- **キャッシュの更新頻度（時間）**

  セカンダリ管理サーバーからレポートテンプレートを作成する管理サーバーに定期的にデータが送信されます。この期間は時間単位で指定できます。0 時間を指定すると、レポートの生成時にのみデータが送信されます。

  既定値は 0 です。

- **セカンダリ管理サーバーから詳細情報を転送する**

  生成されたレポートの詳細なレポートデータの表に、レポートテンプレートを作成する管理サーバーのセカンダリ管理サーバーから取得したデータを含めます。

  このオプションをオンにすると、レポートの生成にかかる時間が長くなり、管理サーバー間のトラフィックも増大します。ただし、1つのレポートですべてのデータを表示できるメリットもあります。

  このオプションをオンにする他に、先に詳細なレポートデータを分析してエラーが発生しているセカンダリ管理サーバーを特定した上で、エラーが発生している管理サーバーのみを対象にレポートを生成するという方法も活用できます。

  既定では、このオプションはオフです。

- ［**フィールド**］タブ

  レポートで表示されるフィールドを選択し、［**上へ**］と［**下へ**］を使用して、フィールドの順序を変更します。［**追加**］または［**編集**］をクリックすると、該当するフィールドに基づいて情報の並べ替えとフィルター処理を行えるかどうかを設定できます。

  ［**詳細フィールドのフィルター**］で、［**フィルターの変換**］をクリックすることでも拡張フィルタリング形式の使用を開始できます。この形式は、論理演算子「OR」を使用することで様々なフィールドに指定された条件を結合できます。ボタンをクリックした後、［**フィルターの変換**］パネルが右側に開きます。［**フィルターの変換**］をクリックして変換を確定します。［**詳細フィールド**］セクションで論理演算子「OR」を使用することで適用される条件付きの変換されたフィルターを定義できるようになります。

複雑なフィルタリング条件をサポートする形式にレポートを変換すると、以前の Kaspersky Security Center (11 より前のバージョン) でレポートを使用できなくなることがあります。また、このような互換性のないバージョンの製品を実行しているセカンダリの管理サーバーからのデータは、変換されたレポートに含めることができません。

5. ［**保存**］をクリックして変更内容を保存します。
6. ［**レポート <レポート名> の編集**］ウィンドウを閉じます。

レポートテンプレートのリストに更新したレポートテンプレートが表示されます。

レポートのファイルへのエクスポート

レポートを、XML ファイル、HTML ファイル、または PDF ファイルにエクスポートできます。

レポートをファイルにエクスポートするには：

1. メインメニューで、［**監視とレポート**］→［**レポート**］に移動します。
2. ファイルにエクスポートするレポートに隣接するチェックボックスをオンにします。
3. ［**レポートのエクスポート**］をクリックします。
4. 表示されるウィンドウの［**名前**］でレポートファイル名を変更できます。既定では、ファイル名は選択したレポートテンプレートの名前に一致します。
5. レポートのファイル種別（XML、HTML、PDF）を選択します。

   wkhtmltopdf ツールはレポートを PDF に変換するために必要です。PDF を選択すると、管理サーバーはデバイスに wkhtmltopdf ツールがインストールされているかどうか確認します。ツールがインストールされていない場合は、管理サーバーデバイスにツールをインストールする必要があることに関するメッセージが表示されます。手動でツールをインストールして次の手順に進みます。
6. ［**レポートのエクスポート**］をクリックします。

   選択した形式のレポートがデバイス（の既定のフォルダー）にダウンロードされるか、あるいはブラウザー標準の「**名前を付けて保存**」ウィンドウが開いてファイルの保存先を指定できます。

レポートがファイルに保存されます。

レポートの生成と表示

レポートを作成および表示するには：

1. メインメニューで、［**監視とレポート**］→［**レポート**］に移動します。
2. レポートの作成に使用するレポートテンプレートの名前をクリックします。

選択したテンプレートを使用してレポートが作成され、表示されます。

レポートデータは、管理サーバーのローカリゼーションセットに従って表示されます。

作成されたレポートの図で、一部のフォントが正しく表示されない場合があります。この問題を解決するには、fontconfig ライブラリをインストールします。また、オペレーティングシステムのロケールに対応するフォントがオペレーティングシステムにインストールされていることを確認してください。

レポートには次のデータが表示されます：

- ［**サマリー**］タブ：
  - レポート名とレポート種別、概要説明、レポート期間、レポートが作成されたデバイスグループに関する情報。
  - 代表的なレポートのデータを示している図表。
  - 計算されたレポートの指標を含む表。
- **[詳細]**タブで、詳細レポートデータの表が表示されます。

レポート配信タスクの作成

選択したレポートを配信するタスクを作成できます。

レポート配信タスクを作成するには：

1. ［**監視とレポート**］→［**レポート**］の順に選択します。
2. レポート配信タスクを作成するレポートテンプレートに隣接するチェックボックスをオンにします（後の手順でも選択できるため、省略可能です）。
3. ［**レポート配信タスクの新規作成**］をクリックします。
4. 新規タスクウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。
5. ウィザードの最初のページで、タスク名を入力します：既定の名前は「**レポートの配信（<タスクの連番>）**」です。
6. ウィザードのタスク設定のページで、次の設定を指定します：
   a. タスクでレポートを配信するレポートテンプレート。ステップ 2 で選択済みの場合は、このステップを省略できます。
   b. レポート形式（HTML、XLS、PDF）。
      wkhtmltopdf ツールはレポートを PDF に変換するために必要です。PDF を選択すると、管理サーバーはデバイスに wkhtmltopdf ツールがインストールされているかどうか確認します。ツールがインストールされていない場合は、管理サーバーデバイスにツールをインストールする必要があることに関するメッセージが表示されます。手動でツールをインストールして次の手順に進みます。
   c. レポートをメールで送信するかどうかと、送信する場合のメール通知設定。

d. レポートをフォルダーに保存するかどうかと、保存する場合に同じフォルダーにある以前のレポートを上書きするかどうか、および（共有フォルダーの場合に）フォルダーへのアクセスに特定のアカウントを使用するかどうか。

7. タスク作成後に、続けてタスクのその他の設定を編集する場合、ウィザードの［**タスク作成の終了**］ページで、［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにします。

8. タスクを作成しウィザードを終了するには、［**作成**］をクリックします。

   レポート配信タスクが作成されます。［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにした場合、タスク設定ウィンドウが表示されます。

レポートテンプレートの削除

レポートのテンプレートを削除するには：

1. メインメニューで、［**監視とレポート**］→［**レポート**］の順に選択します。

2. 削除するレポートテンプレートの隣にあるチェックボックスをオンにします。

3. ［**削除**］をクリックします。

4. 表示されたウィンドウで、［**OK**］をクリックして処理を確定します。

   選択したレポートテンプレートが削除されます。これらのレポートテンプレートがレポートの配信タスクに含まれていた場合、タスクからも該当するレポートテンプレートが削除されます。

イベントとイベントの抽出

このセクションでは、イベントとイベントの抽出、Kaspersky Security Center Linux コンポーネントで発生するイベントの種別、頻出イベントのブロック管理について説明します。

イベントの抽出の使用

イベントの抽出は、管理サーバーのデータベース内に保存されているイベントを一定の条件を指定して抽出し、画面上に表示できる機能です。これらのイベントは、次のカテゴリに従ってグループ化されます：

- 重要度：**緊急イベント**、**機能エラー**、**警告**、**情報イベント**
- 発生時期：**最近のイベント**
- 種別：**ユーザー要求**、**監査イベント**

また、Kaspersky Security Center 14 Web コンソールで編集可能な設定を使用して、ユーザー定義のイベントの抽出を作成し表示できます。

Kaspersky Security Center 14 Web コンソールの［**監視とレポート**］セクションで、［**イベントの抽出**］をクリックすると、イベントの抽出が表示されます。

既定では、イベントの抽出には過去 7 日の情報が含まれます。

Kaspersky Security Center Linux には、事前定義された次の既定のイベントの抽出のセットが用意されています：

- 重要度別のイベント：
  - **緊急イベント**
  - **機能エラー**
  - **警告**
  - **情報メッセージ**
- **ユーザー要求**（管理対象製品のイベント）
- **最近のイベント**（過去1週間を対象）
- **監査イベント**

ユーザー定義の抽出を追加で作成し設定できます。ユーザー定義の抽出では、イベントが発生したデバイスの属性（デバイス名、IP アドレスの範囲、管理グループ）、イベントの種別と重要度、製品名とコンポーネント名、および対象期間によってイベントをフィルターできます。検索対象に、タスクの実行結果を含めることもできます。また、1つ以上の単語を入力して検索する、シンプルな検索フィールドも使用できます。この場合、入力した単語のいずれかが、いずれかの属性（イベント名、説明、コンポーネント名など）に含まれるイベントがすべて一致対象として表示されます。

事前定義の抽出とユーザー定義の抽出の両方で、表示するイベント数と検索対象にするレコード数を制限できます。両方のオプションの値が、Kaspersky Security Center Linux でイベントの抽出が表示されるまでの所要時間に影響します。データベースのサイズが大きいほど、プロセスの所要時間が長くなります。

次のことができます：

- イベントの抽出のプロパティの編集
- イベントの抽出の生成
- イベントの抽出の詳細の表示
- イベントの抽出の削除
- 管理サーバーのデータベースからのイベントの削除

イベントの抽出の作成

イベントの抽出を作成するには：

1. メインメニューで、［**監視とレポート**］→［**イベントの抽出**］の順に移動します。
2. ［**追加**］をクリックします。
3. ［**新規のイベントの抽出**］ウィンドウで、新しいイベントの抽出の設定を指定します。必要に応じて、ウィンドウの各セクションでこの操作を行います。

4. ［**保存**］をクリックして変更内容を保存します。
   確認ウィンドウが開きます。

5. イベントの抽出の結果を表示するには、［**抽出の結果に移動**］をオンにしたままにします。

6. ［**保存**］を選択して、イベントの抽出の作成を確定させます。

［**抽出の結果に移動**］をオンにしたままの場合、イベントの抽出結果が表示されます。オフにした場合、新しいイベントの抽出が追加されたイベントの抽出のリストが表示されます。

イベントの抽出の編集

イベントの抽出を編集するには：

1. メインメニューで、［**監視とレポート**］→［**イベントの抽出**］の順に選択します。

2. 編集するイベントの抽出に隣接するチェックボックスをオンにします。

3. ［**プロパティ**］をクリックします。
   イベントの抽出の設定ウィンドウが表示されます。

4. イベントの抽出のプロパティを編集します。

> 製品導入時から利用できる定義済みのイベントの抽出では、［**全般**］タブ（抽出の名前以外）、［**時間**］タブ、［**アクセス権**］タブのプロパティのみを編集できます。

   ユーザー定義の抽出では、すべてのプロパティを編集できます。

5. ［**保存**］をクリックして変更内容を保存します。

編集したイベントの抽出がリストに表示されます。

イベントの抽出のリストの表示

イベントの抽出を表示するには：

1. メインメニューで、［**監視とレポート**］→［**イベントの抽出**］の順に選択します。

2. 開始するイベントの抽出に隣接するチェックボックスをオンにします。

3. 次のいずれかの手順を実行します：

- イベントの抽出結果の表示で並べ替えを設定したい場合は、次の操作を実行します：

  a. ［**並べ替えを再設定して実行**］をクリックします。

  b. ［**イベントの抽出の並べ替えの再設定**］ウィンドウが表示されるので、並べ替えの設定を指定します。

c. 抽出名をクリックします。

- 管理サーバーでの並べ替え順序を変更せずにイベントのリストを表示する場合は、抽出名をクリックします。

イベントの抽出結果が表示されます。

イベントの詳細の表示

イベントの詳細を表示するには：

1. イベントの抽出を開始します。
2. 目的のイベントの時刻をクリックします。
   ［**イベントのプロパティ**］ウィンドウが開きます。
3. 表示されたウィンドウでは、次の操作を実行できます：
   - 選択したイベントの情報の表示
   - イベントの抽出結果の1つ前または1つ後のイベントへの移動
   - イベントが発生したデバイスの情報への移動
   - イベントが発生したデバイスが属する管理グループへの移動
   - （タスクに関係しているイベントの場合）該当タスクへの移動

イベントのファイルへのエクスポート

イベントをファイルにエクスポートするには：

1. イベントの抽出を開始します。
2. 目的のイベントに隣接するチェックボックスをオンにします。
3. ［**ファイルへのエクスポート**］をクリックします。

選択したイベントがファイルにエクスポートされます。

イベントに含まれるオブジェクトの履歴の表示

リビジョン管理をサポートするオブジェクトの作成イベントまたは変更イベントからは、オブジェクトの履歴画面に移動することができます。

イベントからオブジェクトの履歴を表示するには：

1. イベントの抽出を開始します。
2. 目的のイベントに隣接するチェックボックスをオンにします。
3. ［**変更履歴**］をクリックします。

オブジェクトの変更履歴が表示されます。

イベントの削除

イベントを削除するには：

1. イベントの抽出を開始します。
2. 目的のイベントの横にあるチェックボックスをオンにします。
3. ［**削除**］をクリックします。

選択したイベントは削除され、このイベントは復元できません。

イベントの抽出の削除

削除できるのはユーザー定義のイベントの抽出のみです。製品組み込みで定義済みのイベントの抽出は削除できません。

イベントの抽出を削除するには：

1. メインメニューで、［**監視とレポート**］→［**イベントの抽出**］の順に選択します。
2. 削除するイベントの抽出に隣接するチェックボックスをオンにします。
3. ［**削除**］をクリックします。
4. 表示されたウィンドウで［**OK**］をクリックします。

イベントの抽出が削除されます。

イベントの保管期間の設定

Kaspersky Security Center Linux では、管理サーバーと管理対象デバイスにインストールされた他のカスペルスキー製品の動作中に発生したイベントの情報を受信できます。イベントに関する情報は管理サーバーデータベースに保存されます。一部のイベントを既定値より長くまたは短く保管することが必要な場合があります。イベントの既定の保管期間を変更できます。

管理サーバーのデータベースに保存しなくてよいイベントがある場合は、管理サーバーポリシーとカスペルスキー製品ポリシー、または管理サーバーのプロパティ（管理サーバーのイベントのみ）で適切な設定を無効にできます。これにより、データベースに保存されるイベント種別の数を減らすことができます。

イベントの保管期間が長いほど、データベースが容量の上限に達するのが早くなります。一方で、イベントの保管期間が長いほど、より長い対象期間を設定して監視とレポートのタスクを実行できます。

管理サーバーデータベースへのイベントの保管期間を指定するには：

1. ［**デバイス**］→［**ポリシーとプロファイル**］を順に選択します。
2. 次のいずれかの手順を実行します：
   - ネットワークエージェントまたは管理対象カスペルスキー製品のイベントの保存期間を設定するには、対応するポリシーの名前をクリックします。

     ポリシーのプロパティページが表示されます。
   - 管理サーバーのイベントを設定するには、画面上部の管理サーバー名のセクションで目的の管理サーバーを選択し、横にある設定アイコン（）をクリックします。

     管理サーバーのポリシーがある場合は、このポリシーの名前をクリックできます。

     管理サーバーのプロパティページまたは管理サーバーポリシーのプロパティページが表示されます。
3. ［**イベントの設定**］タブを選択します。

   ［**緊急**］セクションのイベント種別のリストが表示されます。
4. ［**機能エラー**］、［**警告**］、［**情報**］のいずれかのセクションを選択します。
5. 右側のペインのイベント種別のリストで、保存期間を変更するイベントのリンクをクリックします。

   表示されるウィンドウの［**イベント登録**］セクションで、［**管理サーバーのデータベースに保存（日）**］が有効になっています。
6. このスイッチの下に、イベントを保存する日数を入力します。
7. 管理サーバーのデータベースにイベントを保存しない場合は、［**管理サーバーのデータベースに保存（日）**］を無効にします。

   管理サーバーのプロパティウィンドウで管理サーバーのイベントを設定し、Kaspersky Security Center Linux 管理サーバーのポリシーでイベントの設定がロックされている場合、この画面でイベントの保管期間を編集することはできません。
8. ［**OK**］をクリックします。

   ポリシーのプロパティウィンドウが閉じます。

以降、選択した種別のイベントを管理サーバーが受け取ったイベントの保存期間は、変更した期間保存されるようになります。管理サーバーが以前受け取ったイベントの保存期間は変更されません。

イベント種別

Kaspersky Security Center Linux の各コンポーネントには、独自のイベント種別のセットがあります。このセクションでは、Kaspersky Security Center Linux 管理サーバーとネットワークエージェントで発生するイベントの種別について説明します。カスペルスキー製品で発生する可能性のあるイベントの種別は、このセクションの説明には含まれていません。

イベント種別のデータ構造の説明

イベント種別ごとに、表示名、識別子（ID）、英字コード、内容の説明、既定の保管期間を記載しています。

- **イベント種別の表示名**：イベントを設定してそれが発生すると、この列のテキストが Kaspersky Security Center Linux で表示されます。
- **イベント種別の ID**：イベント解析用のサードパーティ製品を使用してイベントを処理すると、この列の数字コードが使用されます。
- **イベント種別**（英字コード）：Kaspersky Security Center Linux データベースで提供されるパブリックビューを使用してイベントの参照と処理を行う場合とイベントを SIEM システムにエクスポートする場合に、この列のコードが使用されます。
- **説明**：この列では、イベントが発生する状況と可能な対応が説明されています。
- **既定の保管期間**：この列には、イベントが管理サーバーデータベースに保管され、管理サーバーのイベントリストに表示される日数が記載されています。この期間が過ぎると、イベントが削除されます。イベントの保管期間の値が「0」の場合、これらのイベントについては検知のみが行われ、管理サーバーのイベントリストへの表示は行われません。こうしたイベントをオペレーティングシステムのイベントログに保存するように設定した場合、それらの保存先でイベントを確認できます。

  イベントの保管期間を変更できます：イベントの保管期間の設定

管理サーバーのイベント

このセクションには、管理サーバーに関するイベントの情報が記載されています。

管理サーバーの緊急イベント

次の表は、重要度が「**緊急**」に分類される Kaspersky Security Center Linux 管理サーバーのイベントを示します。

管理サーバーの緊急イベント

イベント種別の表示名	イベント種別の ID	イベント種別	説明	既定の保管期間
ライセンス数の上限を超えました	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	1 日に 1 回、Kaspersky Security Center Linux はライセンスの上限の超過が発生していないかどうかを確認します。	180 日間

			この種別のイベントは、クライアントデバイスにインストールされているカスペルスキー製品で、ライセンスの上限の超過を管理サーバーが検出しており、単一のライセンスに紐付けられていて現在使用中のライセンス単位数がそのライセンスで本来許可されている合計ライセンス単位数の 110% を超えている場合に記録されます。 このイベントが発生した場合でも、クライアントデバイスの保護は継続されます。 このイベントには、次の方法で対応できます： • 管理対象デバイスのリストを確認します。使用されていないデバイスを削除します。 • 製品を使用できるデバイス数の上限が増えるように、ライセンスを追加します（有効なアクティベーションコードまたはライセンス情報ファイルを管理サーバーに追加）。 Kaspersky Security Center Linux では、ライセンス数の上限を超過した時にイベントを生成するルールを指定できます。	
デバイスが管理対象外になりました	4111	KLSRV_HOST_OUT_CONTROL	この種別のイベントは、デバイスはネットワーク上で可視だが管理サーバーに接続していない状態が指定期間を越えて継続すると記録されます。 デバイス上でネットワークエージェントの正常な動作を妨げている要素を特定します。原因としては、ネットワークの問題や、ネットワークエージェントがデバイスから削除された状況などが考えられます。	180 日間
デバイスのステータスが「緊急」です	4113	KLSRV_HOST_STATUS_CRITICAL	この種別のイベントは、管理対象デバイスに「*緊急*」ステータスが割り当てられると記録されます。デバイスのステータスが「*緊急*」に切り替わる条件を設定できます。	180 日間
このライセンス情報ファイルは拒否リストに追	4124	KLSRV_LICENSE_BLACKLISTED	この種別のイベントは、使用しているアクティベーションコードまたはライセンス情報ファイルがカスペルスキーで拒否リストに登録されると記録されます。 詳細は、テクニカルサポートに問い合わせてください。	180 日間

加されています				
ライセンスの有効期間がまもなく終了します	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	この種別のイベントは、製品版ライセンスの有効期限が近づいている時に発生します。 1日に1回、Kaspersky Security Center はライセンス有効期間の終了日が近づいているかどうかを確認します。この種別のイベントは、ライセンスの有効期限まで残り 30 日、15 日、5 日および1日となった時に発生します。この日数は変更できません。管理サーバーがライセンスの有効期限より前に指定された日にオフになった場合は翌日までイベントは発生しません。 製品版ライセンスの有効期間が終了した場合は、Kaspersky Security Center Linux は基本機能のみを提供します。 このイベントには、次の方法で対応できます： • 予備のライセンスが管理サーバーに追加されていることを確認します。 • 定額制サービスをご利用の場合は、必ず更新してください。支払い期日までに決済された場合、無制限の定額制サービスは自動的に更新されます。	180日間
証明書の有効期間が終了しています	4132	KLSRV_CERTIFICATE_EXPIRED	このタイプのイベントは、モバイルデバイス管理用の管理サーバー証明書の有効期間が終了すると発生します。 期限切れの証明書をアップデートする必要があります。 証明書の自動アップデートを設定するには、証明書発行の設定で［**可能であれば証明書を自動で再発行**］をオンにします。	180日間

管理サーバーの機能エラーイベント

次の表は、重要度が「**機能エラー**」に分類される Kaspersky Security Center Linux 管理サーバーのイベントを示します。

管理サーバーの機能エラーイベント

イベント種別	イベ	イベント種別	説明	既定

の表示名	ント種別の ID			の保管期間
実行時エラー	4125	KLSRV_RUNTIME_ERROR	この種別のイベントは、不明な問題が生じた時に記録されます。 ほとんどの場合、問題は DBMS の問題、ネットワークの問題、またはソフトウェアやハードウェアの問題から発生しています。 エラー情報の詳細は、イベントの説明で参照できます。	180 日間
インストール数の上限を超えたライセンス認証済みアプリケーショングループがあります	4126	KLSRV_INVLICPROD_EXCEDED	この種別のイベントは、管理サーバーによって 1 時間ごとに生成されます。この種別のイベントは、Kaspersky Security Center Liux でサードパーティ製品を管理していて、サードパーティ製品のライセンスで設定された上限を超えると記録されます。 このイベントには、次の方法で対応できます： • 管理対象デバイスのリストを確認します。該当するサードパーティ製品が使用されていないデバイスからサードパーティ製品を削除します。 • 製品を使用できるデバイス数の上限が増えるように、サードパーティ製品のライセンスを追加します。 ライセンス認証済みアプリケーショングループ機能を使用することで、サードパーティ製品のライセンスを管理できます。ライセンス認証済みアプリケーショングループには、管理者が設定した基準を満たすサードパーティ製品が含まれます。	180 日間
指定フォルダーにアップデートをコピーできませんでした	4123	KLSRV_UPD_REPL_FAIL	この種別のイベントは、ソフトウェアアップデートが指定したフォルダーでなく共有フォルダーにコピーされた場合に記録されます。 このイベントには、次の方法で対応できます： • 指定したフォルダーへのアクセスに使用されたユ	180 日間

			ーザーアカウントに、書き込み権限があるかどうかを確認します。 • フォルダーにアクセスするためのユーザー名とパスワードが変更されていないかどうか確認します。 • インターネット接続がイベント発生の原因の可能性もあるので、これをチェックします。定義データベースとソフトウェアモジュールのアップデート手順に従って操作します。	
ディスクに空き容量がありません	4107	KLSRV_DISK_FULL	この種別のイベントは、管理サーバーがインストールされているデバイスのハードディスクの空き容量が不足すると発生します。 デバイスのディスク領域を解放します。	180日間
共有フォルダーが使用できません	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	この種別のイベントは、管理サーバーの共有フォルダーが利用できない場合に記録されます。 このイベントには、次の方法で対応できます： • （共有フォルダーのある）管理サーバーが起動されていて利用可能な状態であることを確認します。 • フォルダーにアクセスするためのユーザー名とパスワードが変更されていないかどうか確認します。 • ネットワーク接続の問題がないか確認します。	180日間
管理サーバーデータベースが使用できません	4109	KLSRV_DATABASE_UNAVAILABLE	この種別のイベントは、管理サーバーのデータベースが利用できなくなっている場合に記録されます。 このイベントには、次の方法で対応できます： • SQL サーバーがインストールされているリモート	180日間

			サーバーが利用できる状態になっているかを確認します。 • DBMS ログを確認し、管理サーバーデータベースを使用できなくなっている理由を特定します。たとえば、メンテナンスの実施が原因となって、SQL サーバーがインストールされているリモートサーバーが利用できなくなっている可能性などがあります。	
管理サーバーデータベースに空き容量がありません	4110	KLSRV_DATABASE_FULL	この種別のイベントは、管理サーバーのデータベースに空き容量がないと記録されます。 管理サーバーのデータベースが容量の上限に達してデータベースへの情報の記録ができなくなると、管理サーバーが正常に機能しなくなります。 このイベントが発生する主な原因は使用中の DBMS の種別に応じて 2 つあり、それぞれ適切な対応方法が異なります： • SQL Server Express Edition を DBMS として使用している場合： • SQL Server Express のヘルプを参照して、使用中のバージョンのデータベースサイズの上限を確認します。管理サーバーのデータベースが、このデータベースサイズの上限に達した可能性があります。 • 管理サーバーデータベースに保存されるイベントの数を制限してください。 • 管理サーバーデータベースにアプリケーションコントロールコンポーネントから送信されたイベントの数が多すぎます。これには、管理サーバーデータベースでのアプリケーショ	180 日間

			ンコントロールイベントの保管期間に関するKaspersky Endpoint Security for Linuxポリシーの設定を変更することで対応できます。 • SQL Server Express Edition以外のDBMSを使用している場合： • 管理サーバーのデータベースに保存されるイベントの数を制限しないでください。 • 管理サーバーデータベースへの保存対象に含めるイベント種別を減らしてください。 DBMSの選定に関する情報を確認します。	

管理サーバーの警告イベント

次の表は、重要度が「**警告**」に分類されるKaspersky Security Center Linux管理サーバーのイベントを示します。

管理サーバーの警告イベント

イベント種別の表示名	イベント種別のID	イベント種別	説明	既定の保管期間
頻出イベントが検出されました		KLSRV_EVENT_SPAM_EVENTS_DETECTED	このタイプのイベントは、管理サーバーが管理対象デバイスで頻出イベントを検知した時に発生します。詳細については、次のセクションを参照してください：［頻出イベントのブロック］。	90日間
ライセンス数の上限を超えました	4098	KLSRV_EV_LICENSE_CHECK_100_110	1日に1回、Kaspersky Security Center Linuxはライセンスの上限の超過が発生していないかどうかを確認します。	90日間

			この種別のイベントは、クライアントデバイスにインストールされているカスペルスキー製品でライセンスの上限の超過が発生していることを管理サーバーが検知し、なおかつ単一のライセンスに紐付けられていて現在使用中のライセンス単位数がそのライセンスで本来許可されている合計ライセンス単位数の 100% から 110% の範囲内の場合に記録されます。 このイベントが発生した場合でも、クライアントデバイスの保護は継続されます。 このイベントには、次の方法で対応できます： • 管理対象デバイスのリストを確認します。使用されていないデバイスを削除します。 • 製品を使用できるデバイス数の上限が増えるように、ライセンスを追加します（有効なアクティベーションコードまたはライセンス情報ファイルを管理サーバーに追加）。 Kaspersky Security Center Linux では、ライセンス数の上限を超過した時にイベントを生成するルールを指定できます。	
デバイスがネットワーク上で長期間アクティブになっていません	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	この種別のイベントは、管理対象デバイスが一定時間休止状態である場合に発生します。 このイベントが最も高頻度で発生するのは、管理対象デバイスが廃止された場合です。 このイベントには、次の方法で対応できます： • 管理対象デバイスのリストからデバイスを手動で削除します。Kaspersky Security Center 14 Web コンソールを使用して［**デバイスがネットワーク上で長期間アクティブになっていません**］イベントが作成されるまでの期間を指定します。	90 日間

			• Kaspersky Security Center 14 Web コンソールを使用して、デバイスがグループから自動的に削除されるまでの期間を指定します。	
デバイスの名前が競合しています	4102	KLSRV_EVENT_HOSTS_CONFLICT	この種別のイベントは、管理サーバーが 2 つ以上の管理対象デバイスを単一のデバイスと判断した場合に発生します。 このイベントが最も高頻度で発生するのは、クローンされたハードディスクが管理対象デバイスでのソフトウェアの導入に使用され、ネットワークエージェントを参照デバイスの専用ディスククローンモードに切り替えなかった場合です。 この問題を回避するには、このデバイスのハードディスクを複製する前に、参照デバイスでネットワークエージェントをディスククローンモードに切り替えます。	90 日間
デバイスのステータスが「警告」です	4114	KLSRV_HOST_STATUS_WARNING	この種別のイベントは、管理対象デバイスに「*警告*」ステータスが割り当てられると記録されます。デバイスのステータスが「*警告*」に切り替わる条件を設定できます。	90 日間
インストール数が上限に近づいているライセンス認証済みアプリケーショングループがあります	4127	KLSRV_INVLICPROD_FILLED	この種別のイベントは、ライセンス認証済みアプリケーショングループに含まれるサードパーティ製品のインストール数が、ライセンスのプロパティで指定された最大許容値の 90% に達すると発生します。 このイベントには、次の方法で対応できます： • 一部の管理対象デバイスでサードパーティ製品を使用していない場合は、これらのデバイスからアプリケーションを削除します。 • サードパーティ製品のインストール数が近い将来に許可される最大数を超えることが予想される場合は、事前にサードパーティのライセンスを取得	90 日間

			する対象デバイスの数を増やすことを検討してください。 ライセンス認証済みアプリケーショングループ機能を使用することで、サードパーティ製品のライセンスを管理できます。	
証明書が要求されました	4133	KLSRV_CERTIFICATE_REQUESTED	この種別のイベントは、モバイルデバイス管理用の証明書を自動的に再発行できない場合に発生します。 考えられるイベントの原因と適切な対応について以下に示します。 • ［**可能であれば証明書を自動で再発行**］がオフにされている証明書に対して自動再発行が開始された。これは、証明書の作成中に発生したエラーが原因であると考えられます。証明書の手動再発行が必要になる場合があります。 • 公開鍵インフラストラクチャと統合している場合、PKI との統合および証明書の発行に使用されるアカウントの SAM-Account-Name 属性の欠落が原因であると考えられます。アカウントのプロパティを確認します。	90 日間
証明書が削除されました	4134	KLSRV_CERTIFICATE_REMOVED	この種別のイベントは、管理者がモバイルデバイス管理用の任意の種別の証明書（一般、メール、VPN）を削除した場合に発生します。 証明書を削除すると、この証明書を介して接続されたモバイルデバイスは、管理サーバーへの接続に失敗します。 このイベントは、モバイルデバイスの管理に関連した誤動作を調査する際に有用な場合があります。	90 日間
APNs 証明書の有効期間が終了しています	4135	KLSRV_APN_CERTIFICATE_EXPIRED	この種別のイベントは、APNs証明書の有効期限が切れた場合に発生します。	保管されません

			手動で APNs 証明書を更新し、iOS MDM サーバーにインストールする必要があります。	
APNs 証明書の有効期間がまもなく終了します	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	この種別のイベントは、APNs 証明書の有効期限が切れるまでの残日数が14日未満の場合に発生します。 APNs 証明書の有効期限が切れた場合は、手動で APNs 証明書を更新し、iOS MDM サーバーにインストールする必要があります。 有効期限に達する前に APNs 証明書の更新スケジュールを設定することを推奨します。	保管されません
モバイルデバイスに FCM メッセージを送信できませんでした	4138	KLSRV_GCM_DEVICE_ERROR	この種別のイベントは、Android オペレーティングシステムを搭載した管理対象のモバイルデバイスに接続するために Google Firebase Cloud Messaging（FCM）を使用するようにモバイルデバイス管理が設定されており、FCM サーバーが管理サーバーから受信したリクエストの一部を処理できない場合に発生します。これは、一部の管理対象モバイルデバイスがプッシュ通知を受信しないことを意味します。 イベントの説明の詳細に記載されている HTTP コードを読み、適宜対応します。FCM サーバーから受信した HTTP コードと関連エラーの詳細については、Google Firebase サービスのドキュメントを参照してください（「ダウンストリームメッセージのエラー応答コード」の章を参照）。	90 日間
FCM メッセージを FCM サーバーに送信している時に HTTP エラーが発生しました	4139	KLSRV_GCM_HTTP_ERROR	この種別のイベントは、モバイルデバイス管理が Android オペレーティングシステムを搭載した管理対象モバイルデバイスに接続するために Google Firebase Cloud Messaging （FCM）を使用するように設定されており、FCM サーバーが 200（OK）以外の HTTP コードで管理サーバーのリクエストに応答する場合に発生します。 考えられるイベントの原因と適切な対応について以下に示します。	90 日間

			• FCM サーバー側の問題。イベントの説明の詳細に記載されている HTTP コードを読み、適宜対応します。FCM サーバーから受信した HTTP コードと関連エラーの詳細については、Google Firebase サービスのドキュメントを参照してください（「ダウンストリームメッセージのエラー応答コード」の章を参照）。 • プロキシサーバー側の問題（プロキシサーバーを使用している場合）。イベントの詳細で HTTP コードを読み取り、適宜対応します。	
FCM メッセージを FCM サーバーに送信できませんでした	4140	KLSRV_GCM_GENERAL_ERROR	この種別のイベントは、Google Firebase Cloud Messaging HTTP プロトコルを使用する際の管理サーバー側での予期しないエラーが原因で発生します。 イベントの説明に記載されている詳細情報を読み、適宜対応します。 ご自分で問題の解決方法を見つけられない場合は、カスペルスキーのテクニカルサポートへのお問い合わせを推奨します。	90 日間
ハードディスクの空き容量が残りわずかです	4105	KLSRV_NO_SPACE_ON_VOLUMES	この種別のイベントは、管理サーバーがインストールされているデバイスのハードディスク容量が不足した場合に発生します。 デバイスのディスク領域を解放します。	90 日間
管理サーバーデータベースに空き容量が残りわずかです	4106	KLSRV_NO_SPACE_IN_DATABASE	この種別のイベントは、管理サーバーのデータベースの空き容量が非常に少なくなっている場合に記録されます。状況を修正しないと、すぐに管理サーバーデータベースの容量が上限に達し、管理サーバーが正常に動作しなくなります。 使用されている DBMS の種別に応じた、このイベントが発生する原因と適切な対応方法を次に示します。	90 日間

			SQL Server Express Edition を DBMS として使用している場合： • SQL Server Express のヘルプを参照して、使用中のバージョンのデータベースサイズの上限を確認します。管理サーバーのデータベースが、もうすぐこのデータベースサイズの上限に達する可能性があります。 • 管理サーバーデータベースに保存されるイベントの数を制限してください。 • 管理サーバーデータベースにアプリケーションコントロールコンポーネントから送信されたイベントの数が多すぎます。これには、管理サーバーデータベースでのアプリケーションコントロールイベントの保管期間に関する Kaspersky Endpoint Security for Linux ポリシーの設定を変更することで対応できます。 SQL Server Express Edition 以外の DBMS を使用している場合： • 管理サーバーのデータベースに保存されるイベントの数を制限しないでください • 管理サーバーデータベースへの保存対象に含めるイベント種別を減らしてください DBMS の選定に関する情報を確認します。	
セカンダリ管理サーバーとの接続が中断されました	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	この種別のイベントは、セカンダリ管理サーバーへの接続が中断された場合に発生します。 セカンダリ管理サーバーがインストールされているデバイスの Kaspersky イベントログを読み、適宜対応します。	90 日間
プライマリ管理サーバ	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	この種別のイベントは、プライマリ管理サーバーへの接続	90 日間

ーとの接続が中断されました			が中断された場合に発生します。 プライマリ管理サーバーがインストールされているデバイスの Kaspersky イベントログを読み、適宜対応します。	
カスペルスキー製品モジュールの新しいアップデートが登録されました	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	この種別のイベントは、インストールの承認が必要な管理対象デバイスにインストールされているカスペルスキーソフトウェアの新しいアップデートを管理サーバーが登録する場合に発生します。 Kaspersky Security Center Web コンソールを使用して、アップデートを承認または拒否します。	90 日間
データベースのイベントの上限数を超えました。イベントの削除が開始されました	4145	KLSRV_EVP_DB_TRUNCATING	この種別のイベントは、管理サーバーのデータベース容量が上限に達して、データベース内の古いイベントの削除が開始された時に記録されます。 このイベントには、次の方法で対応できます： • 管理サーバーデータベースに保管されるイベント数の上限を変更してください • 管理サーバーデータベースへの保存対象に含めるイベント種別を減らしてください	保管されません
データベースのイベントの上限数を超えました。このイベントは削除されました	4146	KLSRV_EVP_DB_TRUNCATED	この種別のイベントは、管理サーバーのデータベース容量が上限に達して、データベース内の古いイベントが削除された時に記録されます。 このイベントには、次の方法で対応できます： • 管理サーバーデータベースに保管できるイベント数の上限を変更してください • 管理サーバーデータベースへの保存対象に含めるイベント種別を減らしてください	保管されません

管理サーバーの情報イベント

次の表は、重要度が「**情報**」に分類される Kaspersky Security Center Linux 管理サーバーのイベントを示します。

管理サーバーの情報イベント

イベント種別の表示名	イベント種別の ID	イベント種別	既定の保管期間	備考
ライセンス使用率が 90% を超えています	4097	KLSRV_EV_LICENSE_CHECK_90	30 日間	
新しいデバイスが検出されました	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 日間	
デバイスが自動的にグループに追加されました	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 日間	
デバイスがグループから削除されました：ネットワーク上で長期間アクティブになっていません	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 日間	
インストール数が上限に近づいている（95% を超える数を使用済み）ライセンス認証済みアプリケーショングループがあります	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 日間	
カスペルスキーへ分析のために送付するファイルが見つかりました	4131	KLSRV_APS_FILE_APPEARED	30 日間	
このモバイルデバイス上で FCM 送信者 ID が変更されました	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 日間	
指定のフォルダーにアップデートがコピーされました	4122	KLSRV_UPD_REPL_OK	30 日間	
セカンダリ管理サーバーとの接続が確立されました	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 日間	
プライマリ管理サーバーとの接続が確立されました	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 日間	
定義データベースがアップデートされました	4144	KLSRV_UPD_BASES_UPDATED	30 日間	
監査：管理サーバーとの接続が確立されました	4147	KLAUD_EV_SERVERCONNECT	30 日間	
監査：オブジェクトが変更されました	4148	KLAUD_EV_OBJECTMODIFY	30 日間	このイベントは次のオブジェクトの変更を追跡し

				ます： • 管理グループ • セキュリティグループ • ユーザー • パッケージ • タスク • ポリシー • サーバー • 仮想サーバー
監査：オブジェクトのステータスが変更されました	4150	KLAUD_EV_TASK_STATE_CHANGED	30日間	たとえば、このイベント

				タスクエラーで失敗した時に発生します。
監査：グループ設定が変更されました	4149	KLAUD_EV_ADMGROUP_CHANGED	30日間	
監査：管理サーバーへの接続が切断されました	4151	KLAUD_EV_SERVERDISCONNECT	30日間	
監査：オブジェクトのプロパティが変更されました	4152	KLAUD_EV_OBJECTPROPMODIFIED	30日間	このイベントは、次のプロパティの変更を追跡します： • ユーザー • ライセンス • サーバー • 仮想サーバー
監査：ユーザーの権限が変更されました	4153	KLAUD_EV_OBJECTACLMODIFIED	30日間	

ネットワークエージェントのイベント

このセクションには、ネットワークエージェントに関するイベントの情報が記載されています。

ネットワークエージェントの警告イベント

次の表は、重要度が「**警告**」に分類される Kaspersky Security Center Linux のネットワークエージェントのイベントを示します。

ネットワークエージェントの警告イベント

イベント種別の表示名	イベント種別の ID	イベント種別	既定の保管期間
インシデントが発生しました	549	GNRL_EV_APP_INCIDENT_OCCURED	30 日間

ネットワークエージェントの情報イベント

次の表は、重要度が「**情報**」に分類される Kaspersky Security Center Linux ネットワークエージェントのイベントを示します。

ネットワークエージェントの情報イベント

イベント種別の表示名	イベント種別の ID	イベント種別	既定の保管期間
アプリケーションがインストールされました	7703	KLNAG_EV_INV_APP_INSTALLED	30 日間
アプリケーションがアンインストールされました	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 日間
監視対象アプリケーションがインストールされました	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 日間
監視対象アプリケーションがアンインストールされました	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 日間
新しいデバイスが追加されました	7708	KLNAG_EV_DEVICE_ARRIVAL	30 日間
デバイスが削除されました	7709	KLNAG_EV_DEVICE_REMOVE	30 日間
新しいデバイスが検出されました	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 日間
デバイスが認証されました	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 日間

頻出イベントのブロック

このセクションでは、頻出イベントのブロックの管理および頻出イベントのブロックの解除について説明します。

頻出イベントのブロックについて

単一または複数の管理対象デバイスにインストールされた Kaspersky Endpoint Security for Linux などの管理対象アプリケーションは、管理サーバーに対して同様の種別のイベントを大量に送信することがあります。頻出イベントを受信すると、管理サーバーのデータベース高負荷がかかり、他のイベントが上書きされる場合があります。管理サーバーは、受信したイベントの総量がデータベースで指定した制限を超えた場合、頻出イベントをブロックします。

管理サーバーは頻出イベントの受信を自動的にブロックします。ユーザー自身による頻出イベントのブロックや、ブロックするイベントの選択はできません。

イベントがブロックされているかどうかを確認したい場合、通知リストを表示するか、そのイベントが管理サーバーのプロパティの［**頻出イベントのブロック**］セクションに存在するかどうかで確認できます。イベントがブロックされている場合、次を実行します：

- データベースの上書きを防止したい場合、このような種別のイベントの受信のブロックを継続できます。
- たとえば、管理サーバーに頻出イベントが送信される原因を見つける場合などには、頻出イベントのブロックを解除してこの種別のイベントの受信を継続できます。
- 頻出イベントの受信が再度ブロックされるまで受信を継続する場合は、頻出イベントのブロック対象から削除することができます。

頻出イベントのブロックの管理

管理サーバーは頻出イベントの自動受信をブロックしますが、ブロックを解除してイベントの受信を継続することができます。また、以前にブロック解除したイベントを再度ブロックすることもできます。

頻出イベントのブロックを管理するには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. ［**全般**］タブで、［**頻出イベントのブロック**］セクションを選択します。
3. ［**頻出イベントのブロック**］セクションで次を実行します：
   - 頻出イベントの受信のブロックを解除する場合：
     a. ブロック解除する頻出イベントを選択し、［**除外**］をクリックします。
     b. ［**保存**］をクリックします。

- 頻出イベントをブロックする場合は：

  a. ブロックする頻出イベントを選択し、［**ブロック**］をクリックします。

  b. ［**保存**］をクリックします。

管理サーバーはブロック解除された頻出イベントを受け取り、ブロック対象の頻出イベントは受け取りません。

頻出イベントのブロックの解除

頻出イベントのブロックを解除して、管理サーバーが再度ブロックするまでこれらの頻出イベントを受信できます。

頻出イベントのブロックを解除するには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. ［**全般**］タブで、［**頻出イベントのブロック**］セクションを選択します。
3. ［**頻出イベントのブロック**］セクションで、ブロックを解除したいイベントの行をクリックします。
4. ［**ブロック解除**］をクリックします。

イベントは頻出イベントのリストから削除されます。管理サーバーはこの種別のイベントを受信します。

管理サーバーでのイベントの処理と保管

アプリケーションの動作および管理対象デバイスでのイベントに関する情報は、管理サーバーデータベースに保存されます。イベントにはそれぞれ種別と重要度（*緊急イベント*、*機能エラー*、*警告*、*情報*）という属性があります。イベントが発生した条件に応じて、同じ種別のイベントに異なる重要度を割り当てることができます。

イベントに割り当てられた種別および重要度は、管理サーバーのプロパティウィンドウの［**イベントの設定**］セクションに表示されます。［**イベントの設定**］セクションでは、管理サーバーによる各イベントの処理を設定することもできます。

- 管理サーバーにおけるイベントの登録、およびデバイスと管理サーバーのオペレーティングシステムのイベントログにおけるイベントの登録
- 管理者へのイベントの通知方法（例：SMS、メール）

管理サーバーのプロパティウィンドウ内にある［**イベントリポジトリ**］セクションで、管理サーバーデータベース内で保管するイベントの設定を編集できます。編集可能な設定項目は、イベントのレコード数上限やレコードの保管期間があります。保管するイベント数の上限を指定すると、指定した数に応じて必要なディスク容量の概算値が算出されます。データベースのオーバーフローを避けるために十分な空き容量があるかどうかのこの概算値を使用できます。既定の設定では、管理サーバーデータベース内に保管できるイベント数は 400,000 件までとなっています。データベースで推奨される範囲でのイベント数の上限は、45,000,000 件です。

データベースのイベント数が管理者によって指定された上限に達すると、最も古いイベントが削除されて、新しいイベントに置き換えられます。管理サーバーが古いイベントを削除する際に、新しいイベントのデータベースへの保存は行えません。この期間、拒否したイベントの情報は Kaspersky イベントログに書き込まれます。新しいイベントはキューに追加され、削除操作が完了した後にデータベースに保存されます。

通知とデバイスのステータス

このセクションでは、通知の表示、通知の配信の設定、デバイスのステータスの使用、デバイスのステータス変更を有効にする方法について説明します。

通知機能の使用

通知機能を使用してイベントのアラート通知を受け取ることで、推奨される処理や担当者が適切と考える対応を行うまでの時間を短縮できます。

次の種別の通知を、通知方法の選択に応じて使用できます：

- 画面表示による通知
- SMS 通知
- メール通知
- 実行ファイルまたはスクリプトの実行で通知

画面表示による通知

画面表示による通知では、重要度別にアラート通知を確認できます（*緊急*、*警告*、*情報*）。

画面表示による通知には 2 種類のステータスがあります：

- *確認済み*：推奨される処理として記載されている処理を行ったか、通知に手動でこのステータスを割り当てた場合に、このステータスが付与されます。
- *未確認*：推奨される処理として記載されている処理を未実行か、通知に「確認済み」のステータスを手動で割り当てていない場合に、このステータスが付与されます。

既定では、通知リストには「*未確認*」ステータスの通知が表示されます。

画面表示される通知を確認し、リアルタイムでの対応を行うことで、組織ネットワークの監視業務を実行できます。

メール、SMS、または実行ファイルやスクリプトの実行による通知

Kaspersky Security Center Linux では、必要に応じて、重要だと考えられる任意のイベントに対して通知の送信を設定し、組織ネットワークの監視に役立てることができます。任意のイベントで、メール、SMS、または実行ファイルやスクリプトの実行による通知を設定できます。

メールまたはSMSで通知を受け取った場合、イベント内容を確認して必要な対応を決定できます。この対応は組織のネットワークに対して最も適切なものである必要があります。実行ファイルまたはスクリプトの実行を設定する場合は、イベントに対する対応を事前に指定できます。また、実行ファイルまたはスクリプトの実行による対応を、イベントに対する初期対応として考えることもできます。この場合、実行ファイルの実行後に、イベントに対して必要な追加対応を担当者自身が実施できます。

画面表示による通知の確認

通知は次の3通りの方法で画面表示できます：

- ［**監視とレポート**］→［**通知**］セクション。ここで定義済みのカテゴリに関連する通知を確認できます。
- どのセクションからもメニュー上部のアイコンを使用して開くことができる別のウィンドウ。この方法を使用すると、通知を確認済みとしてマークできます。
- ［**監視とレポート**］→［**ダッシュボード**］セクションの［**選択した深刻度別の通知**］ウィジェット。ウィジェットで、重要度が*緊急*と*警告*のイベントの通知のみ確認できます。

イベントに応答するなど、処理を実行できます。

定義済みのカテゴリから通知を確認するには：

1. メインメニューで、［**監視とレポート**］→［**通知**］に移動します。
   ［**すべての通知**］カテゴリが左側のペインで選択されており、右側のペインですべての通知が表示されます。
2. 左側のペインで、次のカテゴリのいずれかを選択します：
   - **製品の導入**
   - **デバイス**
   - **プロテクション**
   - **アップデート**（ダウンロード可能なカスペルスキー製品とダウンロードされた定義データベースのアップデートに関する通知が含まれます）
   - **脆弱性攻撃ブロック**
   - **管理サーバー**（管理サーバーのみに関するイベントが含まれます）
   - **参考リンク**（カスペルスキーのリソース（たとえば、カスペルスキーのテクニカルサポート、カスペルスキーのコミュニティ、販売代理店リストのページ、ウイルス百科事典など）へのリンクが含まれます）
   - **カスペルスキーニュース**（カスペルスキー製品のリリースに関する情報が含まれます）

   選択したカテゴリの通知のリストが表示されます。リストには次が含まれます：

- 情報の内容に関連するアイコン：導入、保護、アップデート、デバイスの管理、脆弱性攻撃ブロック、管理サーバー。
- 通知の重要度：重要度が、**緊急の通知**（）、**警告の通知**（）、**情報の通知**の通知が表示されます。リスト内の通知は重要度に応じてグループ化されています。

- **通知**：通知の説明が含まれます。
- **処理**：コンソールで実行可能な、推奨される処理へのリンクが含まれます。それぞれのリンクをクリックすると、たとえば、リポジトリに移動してデバイスにセキュリティ製品をインストールしたり、デバイスまたはイベントのリストを確認できます。通知に推奨される処理を実行すると、この通知に*確認済み*のステータスが割り当てられます。
- **ステータス登録後の時間**：通知が管理サーバーに登録された時点から経過した日数または時間数が含まれます。

別のウィンドウで、画面表示による通知を重要度別に確認するには：

1. Kaspersky Security Center 14 Web コンソールの右上端で、フラグアイコン（）をクリックします。

   フラグアイコンに赤い丸印が表示されている場合は、確認されていない通知があります。

   通知のリストを含むウィンドウが開きます。既定では、［**すべての通知**］タブが選択されており、*緊急*、*警告*、*情報*の重要度別に通知がグループ化されています。

2. ［**システム**］タブを選択します。

   重要度が*緊急*（）と*警告*（）の通知のリストが表示されます。通知のリストには以下が含まれます：

   - カラーマーカー：緊急の通知には赤色のマーカーが使用されます。警告の通知には黄色のマーカーが使用されます。
   - 情報の内容を示すアイコン：導入 ()、保護 ()、アップデート()、デバイスの管理 ()、脆弱性攻撃ブロック ()、管理サーバー ()。
   - 通知の説明。
   - フラグアイコン：通知に*未確認*のステータスが割り当てられている場合、［フラグ］アイコンは灰色です。灰色の［フラグ］アイコンを選択して通知に*確認済み*のステータスを割り当てると、アイコンは白色に変更されます。
   - 推奨される処理へのリンク：リンクをクリックした後で推奨される処理を実行すると、通知は*確認済み*のステータスになります。
   - 通知が管理サーバーに登録された時点から経過した日数または時間数。

3. ［**詳細**］タブを選択します。

   重要度が*情報*の通知のリストが表示されます。

   リストの各項目の構成は、［**システム**］タブのリスト（前述の説明を参照）と同じです。カラーマーカーが使用されない点のみ異なります。

通知が管理サーバーに登録された期間で通知をフィルタリングできます。フィルターを管理するには、［**フィルターの表示**］をオンにします。

ウィジェットで画面表示による通知を確認するには：

1. ［**ダッシュボード**］セクションで、［**Web ウィジェットを追加または復元**］を選択します。
2. 表示されたウィンドウで、［**その他**］のカテゴリをクリックし、［**選択した深刻度別の通知**］ウィジェットを選択して、［追加］をクリックします。

これによりウィジェットが［**ダッシュボード**］タブに表示されます。既定では、重要度が*緊急*の通知がウィジェットに表示されます。

ウィジェットの［**設定**］をクリックしてウィジェットの設定を変更すると、重要度が*警告*の通知を表示できます。または、*警告*の重要度を指定して［**選択した深刻度別の通知**］ウィジェットを追加できます。

通知リストのウィジェットには表示領域のサイズの制限があるため、表示される通知は 2 つまでです。これらの 2 つの通知は最新のイベントに関連します。

通知リストのウィジェットには以下が含まれます：

- 情報の内容に関連するアイコン：導入 ()、保護 ()、アップデート()、デバイスの管理 ()、脆弱性攻撃ブロック ()、管理サーバー ()。
- 推奨される処理へのリンクを含む通知の説明：リンクをクリックした後で推奨される処理を実行すると、通知は「*確認済み*」のステータスになります。
- 通知が管理サーバーに登録された時点から経過した日数または時間数。
- その他の通知へのリンク：このリンクをクリックすると、［**監視とレポート**］セクションの［**通知**］セクションに表示される通知リストの画面に移動します。

デバイスのステータスの概要

Kaspersky Security Center Linux は、各管理対象デバイスにステータスを割り当てます。特定のステータスは、ユーザーが定義した条件を満たしているかどうかによって異なります。場合によっては、デバイスにステータスを割り当てるときに、Kaspersky Security Center Linux はネットワーク内のデバイスの可視性フラグを考慮します（下の表を参照）。Kaspersky Security Center Linux が 2 時間以内にネットワーク内のデバイスを見つけられない場合、デバイスの可視性フラグは「*不可視*」に設定されます。

ステータスは次の通りです：

- *緊急*または*緊急 / 可視*
- *警告*または*警告 / 可視*
- *OK* または *OK / 可視*

次の表では、「*緊急*」または「*警告*」ステータスをデバイスに割り当てるために満たすべき既定の条件を、可能なすべての値とともに一覧で表示します。

デバイスにステータスを割り当てる条件

条件	条件の説明	設定可能な値
セキュリティ製品がインストールされていません	デバイスにネットワークエージェントはインストールされていますが、セキュリティ製品はインストールされていません。	• 切り替えスイッチを

		オン • 切り替えスイッチをオフ
ウイルスが多数検知されました	ウイルススキャンタスクなどのウイルス検知タスクによりデバイスでウイルスが検知され、検知数が指定された値を超えました。	0 より大きい値
リアルタイム保護レベルが管理者の設定と異なります	デバイスはネットワーク上で可視ですが、リアルタイム保護レベルがデバイスのステータスの条件として管理者によって設定されたレベルと異なっています。	• 停止 • 一時停止 • 実行中
スキャンが長期間実行されていません	デバイスはネットワーク上で可視でセキュリティ製品もインストールされていますが、*マルウェアのスキャン*タスクもローカルスキャンタスクも実行されていない状態が指定期間を越えて続いています。この条件は、7 日以上前に管理サーバーデータベースに追加されたデバイスにのみ適用されます。	1日より大きい値
定義データベースがアップデートされていません	デバイスはネットワーク上で可視でセキュリティ製品もインストールされていますが、このデバイスで定義データベースがアップデートされていない状態が指定期間を越えて続いています。この条件は、1日以上前に管理サーバーデータベースに追加されたデバイスにのみ適用されます。	1日より大きい値
長期間接続されていません	デバイスにネットワークエージェントはインストールされていますが、デバイスがオフになっており、デバイスが管理サーバーに接続されていない状態が指定期間を越えて続いています。	1日より大きい値
アクティブな脅威を検知しました	［**アクティブな脅威**］フォルダー内の未処理オブジェクトの数が指定の値を上回っています。	0 項目より大きい値
再起動が必要です	デバイスはネットワーク上で可視ですが、アプリケーションが選択した理由でデバイスの再起動を必要とする状態が指定期間を越えて続いています。	0 分より大きい値
競合アプリ	デバイスはネットワーク上で可視ですが、ネットワークエージェントから実行さ	

ケーションがインストールされています	れたソフトウェアインベントリにより、競合するアプリケーションがデバイスにインストールされていることを検知しました。	• 切り替えスイッチをオフ • 切り替えスイッチをオン
ライセンスの有効期間が終了しました	デバイスはネットワーク上で可視ですが、ライセンスの有効期間が終了しています。	• 切り替えスイッチをオフ • 切り替えスイッチをオン
ライセンスの有効期間がまもなく終了します	デバイスはネットワーク上で可視ですが、ライセンスの有効期間の残り日数が指定した期間以下しかありません。	0 日より大きい値
未処理のインシデントが検出されました	処理されていないインシデントがデバイス上で見つかりました。インシデントは、クライアントデバイスにインストールしたカスペルスキー製品によって自動で作成されるか、管理者が手動で作成します。	• 切り替えス

		イッチをオフ • 切り替えスイッチをオン
製品が定義したデバイスのステータス	デバイスのステータスが管理対象アプリケーションによって定義されています。	• 切り替えスイッチをオフ • 切り替えスイッチをオン
デバイスに空き容量がありません	デバイスの空き容量が指定された値未満またはデバイスと管理サーバーを同期できませんでした。デバイスが管理サーバーと正常に同期されなおかつデバイスの空き容量が指定値以上になった場合、ステータスが［*緊急*］または［*警告*］から［*OK*］に変更されます。	0 MB より大きい値
デバイスが管理対象外になりました	デバイスの検索中、デバイスはネットワークで認識されましたが、管理サーバーとの同期に 3 回以上失敗しました。	• 切り替えスイッチを

		オフ • 切り替えスイッチをオン
プロテクションが無効です	デバイスはネットワーク上で可視ですが、デバイス上でセキュリティ製品が無効になっている状態が指定期間を越えて続いています。	0 分より大きい値
セキュリティ製品が実行されていません	デバイスはネットワーク上で可視でセキュリティ製品もインストールされていますが、セキュリティ製品が実行されていません。	• 切り替えスイッチをオフ • 切り替えスイッチをオン

Kaspersky Security Center Linux では、指定した条件が満たされると、管理グループのデバイスのステータスが自動的に切り替わるように設定できます。指定した条件が満たされると、クライアントデバイスには、「*緊急*」または「*警告*」のステータスのいずれかが割り当てられます。指定した条件を満たしていない場合、クライアントデバイスには「*OK*」ステータスが割り当てられます。

1つの条件の複数の値に対して異なるステータスを対応させることができます。たとえば、［**定義データベースがアップデートされていません**］条件の値が「**3 日より大きい値**」の場合はクライアントデバイスに「*警告*」ステータスが割り当てられ、条件値が「**7 日より大きい値**」の場合は「*緊急*」ステータスが割り当てられます。

Kaspersky Security Center Linux を旧バージョンからアップグレードしても、ステータスを「*緊急*」または「*警告*」に割り当てるための［**定義データベースがアップデートされていません**］条件の値は変更されません。

Kaspersky Security Center Linux によってデバイスにステータスが割り当てられると、一部の条件（条件説明の列を参照）で可視性フラグが考慮されます。たとえば、ある管理対象デバイスは［定義データベースがアップデートされていません］条件を満たしていたために「*緊急*」ステータスが割り当てられました。のちにデバイスには可視性フラグが設定され、その後、そのデバイスは「*OK*」ステータスが割り当てられます。

デバイスのステータスの切り替えの設定

デバイスに「*緊急*」または「*警告*」ステータスを割り当てる条件を変更できます。

デバイスのステータスの「緊急」への切り替えを有効にするには：

1. メインメニューで、［**デバイス**］→［**グループ階層構造**］の順に選択します。
2. グループのリストが開いたら、デバイスのステータスの切り替えを設定するグループ名をクリックします。
3. プロパティウィンドウが開いたら、［**デバイスのステータス**］タブを選択します。
4. 左側のペインで、［**緊急**］を選択します。
5. 右側のペインの［**指定されている場合は「緊急」に設定**］セクションで、デバイスに［*緊急*］ステータスを割り当てる条件をオンにします。

   親ポリシーでロック状態になっていない設定のみ変更できます。

6. リスト内の条件の横にあるラジオボタンをオンにします。
7. リストの左上にある［**編集**］をクリックします。
8. 選択した条件に対して適切な値を設定します。
   すべての条件に値を設定できるわけではありません。
9. ［**OK**］をクリックします。

指定した条件が満たされると、管理対象デバイスには「*緊急*」ステータスが割り当てられます。

デバイスのステータスの「警告」への切り替えを有効にするには：

1. メインメニューで、［**デバイス**］→［**グループ階層構造**］の順に選択します。
2. グループのリストが開いたら、デバイスのステータスの切り替えを設定するグループ名をクリックします。
3. プロパティウィンドウが開いたら、［**デバイスのステータス**］タブを選択します。
4. 左側のペインで、［**警告**］を選択します。
5. 右側のペインの［**指定されている場合は「警告」に設定**］セクションで、デバイスに［*警告*］ステータスを割り当てる条件をオンにします。

親ポリシーでロック状態になっていない設定のみ変更できます。

6. リスト内の条件の横にあるラジオボタンをオンにします。
7. リストの左上にある［**編集**］をクリックします。
8. 選択した条件に対して適切な値を設定します。
   すべての条件に値を設定できるわけではありません。
9. ［**OK**］をクリックします。

指定した条件が満たされると、管理対象デバイスには「*警告*」ステータスが割り当てられます。

通知の設定

Kaspersky Security Center Linux で発生するイベントに関する通知を設定できます。次の種別の通知を、通知方法の選択に応じて使用できます：

- メール：イベントが発生すると、指定されたメールアドレスに通知を送信します。
- SMS：イベントが発生すると、指定された電話番号に通知を送信します。
- 実行ファイル：イベントが発生すると、管理サーバーで実行ファイルが実行されます。

Kaspersky Security Center Linux で発生したイベントの通知の配信を設定するには：

1. 画面上部の管理サーバー名のセクションで目的の管理サーバーを選択し、隣接する設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウの［**全般**］タブが表示されます。
2. ［**通知**］セクションをクリックし、右側のペインで、設定する通知方法のタブを選択します：
   - **メール**

［**メール**］タブでは、メールによるイベントの通知を設定できます。

［**SMTP サーバー**］に、メールサーバーのアドレスをセミコロンで区切って指定します。次の値を使用できます：

- IPv4 / IPv6 アドレス
- SMTP サーバーの DNS 名

［**SMTP サーバーのポート**］に、SMTP サーバーの通信ポート番号を指定します。既定のポート番号は 25 です。

［**DNS MX ルックアップを使用**］を有効にすると、IP アドレスの複数の MX レコードを、SMTP サーバーの同一の DNS 名に使用できます。同一 DNS 名に複数の MX レコードが存在し、各レコードのメール受信の優先度の値が異なる場合があります。管理サーバーは SMTP サーバーへのメール通知の 送信を、MX レコードの優先度の昇順に試行します。

［**DNS MX ルックアップを使用**］を有効にし、TLS 設定の使用は有効にしない場合、メール通知を保護する追加の方法として、サーバーデバイスで DNSSEC 設定を使用することを推奨します。

［**ESMTP 認証を使用する**］をオンにすると、［**ユーザー名**］および［**パスワード**］フィールドに ESMTP 認証の設定を指定できます。既定ではこのオプションはオフで、ESMTP 認証設定が使用できない状態になっています。

SMTP サーバーとの接続の TLS 設定を指定できます：

- **TLS を使用しない**

メールの暗号化を無効にする場合に、このオプションを選択できます。

- **TLS を使用する（SMTP サーバーがサポートする場合）**

SMTP サーバーに TLS 接続を使用する場合に、このオプションを選択できます。SMTP サーバーが TLS をサポートしていない場合、管理サーバーは TLS を使用せずに SMTP サーバーへ接続します。

- **TLS を常に使用し、サーバー証明書の有効性をチェックする**

TLS 認証設定を使用する場合に、このオプションを選択できます。SMTP サーバーが TLS をサポートしていない場合、管理サーバーは SMTP サーバーへ接続できません。

SMTP サーバーの接続の保護をより強化する目的で、このオプションを使用することを推奨します。このオプションを選択すると、TLS 接続の認証設定を指定できます。

［**TLS を常に使用し、サーバー証明書の有効性をチェックする**］の値を選択する場合は、SMTP サーバーの認証用の証明書を指定し、TLS の任意のバージョンを介した通信を有効にするか、TLS 1.2 以降のバージョンのみを介した通信を有効にするかを選択できます。また、SMTP サーバーでクライアント認証に使用する証明書を指定することもできます。

［**証明書を指定** ］をクリックして TLS 接続用の証明書を指定できます。

- SMTP サーバーの証明書ファイルを参照します：

信頼できる証明書認証局から証明書のリストを含むファイルを受け取り、ファイルを管理サーバーへアップロードできます。Kaspersky Security Center Linux は、SMTP サーバーの証明書も信頼できる証明書認証局によって署名されているかどうかをチェックします。信頼できる証明書認証局から SMTP サーバーの証明書を受け取っていない場合、Kaspersky Security Center Linux は SMTP サーバーに接続できません。

- クライアント証明書ファイルを参照します：

信頼できる認証局など、任意の発行元から受け取った証明書を使用できます。次のいずれかの証明書タイプを使用して、証明書とその秘密鍵を指定する必要があります：

- X-509証明書：

証明書を含むファイルと秘密鍵を含むファイルを指定する必要があります。両方のファイルは相互に依存せず、ファイルを読み込む順序は重要ではありません。両方のファイルを読み込む時は、秘密鍵をデコードするためのパスワードを指定する必要があります。秘密鍵がエンコードされていない場合、パスワードの値は空である可能性があります。

- pkcs12 コンテナー：

証明書とその秘密鍵を含む単一のファイルをアップロードする必要があります。ファイルの読み込み時に、秘密鍵をデコードするためのパスワードを指定する必要があります。秘密鍵がエンコードされていない場合、パスワードの値は空である可能性があります。

［**テストメッセージの送信**］をクリックすると、通知が正しく設定されているか確認することができます。指定したメールアドレスにテスト通知が送信されます。

［**受信者（メールアドレス）**］に、通知の送信先となるメールアドレスを指定します。このフィールドでは、複数のアドレスをセミコロンで区切って指定することができます。

［**件名**］で、メールの件名を指定できます。このフィールドを空白にすることもできます。

［**件名のテンプレート**］ドロップダウンリストで、件名のテンプレートを選択できます。選択したテンプレートに対応する変数が［**件名**］に自動的に入力されます。複数の件名のテンプレートを選択して、メールの件名を構成できます。

［**送信者のメールアドレス：指定されていない場合は、受信者のアドレスを使用します。 注意：実在しないアドレスは使用しないことを推奨します**］で、送信者のメールアドレスを指定します。このフィールドを空白にした場合、既定では、宛先のアドレスが使用されます。実在しないアドレスを使用することは避けてください。

［**通知メッセージ**］には、イベントが発生した時に送信される、イベントに関する情報を含む標準的なメッセージが表示されます。このメッセージには、イベント名、デバイス名、ドメイン名といった代替パラメータが含まれます。イベントのより詳細な情報についての代替パラメータを追加して、メッセージを編集することができます。

通知テキストにパーセント記号「%」が含まれる場合、メッセージを送信するには 2 つ続けて入力する必要があります。たとえば、「CPU の負荷 100%%」のように入力します。

［**通知数の上限を設定する**］をクリックすると、指定した時間内に送信できる最大通知数を指定できます。

- SMS

［**SMS**］タブでは、携帯電話へ送信する様々なイベントの SMS 通知を設定できます。SMS メッセージはメールゲートウェイを通して送信されます。

［**SMTP サーバー**］に、メールサーバーのアドレスをセミコロンで区切って指定します。次の値を使用できます：

- IPv4 / IPv6 アドレス
- SMTP サーバーの DNS 名

［**SMTP サーバーのポート**］に、SMTP サーバーの通信ポート番号を指定します。既定のポート番号は 25 です。

［**ESMTP 認証を使用する**］をオンにすると、［**ユーザー名**］および［**パスワード**］フィールドに ESMTP 認証の設定を指定できます。既定ではこのオプションはオフで、ESMTP 認証設定が使用できない状態になっています。

SMTP サーバーとの接続の TLS 設定を指定できます：

- **TLS を使用しない**

メールの暗号化を無効にする場合に、このオプションを選択できます。

- **TLS を使用する（SMTP サーバーがサポートする場合）**

SMTP サーバーに TLS 接続を使用する場合に、このオプションを選択できます。SMTP サーバーが TLS をサポートしていない場合、管理サーバーは TLS を使用せずに SMTP サーバーへ接続します。

- **TLS を常に使用し、サーバー証明書の有効性をチェックする**

TLS 認証設定を使用する場合に、このオプションを選択できます。SMTP サーバーが TLS をサポートしていない場合、管理サーバーは SMTP サーバーへ接続できません。

SMTP サーバーの接続の保護をより強化する目的で、このオプションを使用することを推奨します。このオプションを選択すると、TLS 接続の認証設定を指定できます。

［**TLS を常に使用し、サーバー証明書の有効性をチェックする**］の値を選択する場合は、SMTP サーバーの認証用の証明書を指定し、TLS の任意のバージョンを介した通信を有効にするか、TLS 1.2 以降のバージョンのみを介した通信を有効にするかを選択できます。また、SMTP サーバーでクライアント認証に使用する証明書を指定することもできます。

［**証明書を指定**］をクリックして SMTP サーバーのクライアント認証用の証明書を指定できます。信頼できる証明書認証局から証明書のリストを含むファイルを受け取り、ファイルを管理サーバーへアップロードできます。Kaspersky Security Center Linux は、SMTP サーバーの証明書も信頼できる証明書認証局によって署名されているかどうかをチェックします。信頼できる証明書認証局から SMTP サーバーの証明書を受け取っていない場合、Kaspersky Security Center Linux は SMTP サーバーに接続できません。

［**受信者（メールアドレス）**］に、通知の送信先となるメールアドレスを指定します。このフィールドでは、複数のアドレスをセミコロンで区切って指定することができます。通知は、指定したメールアドレスに関連付けられている電話番号に送信されます。

［**件名**］で、メールの件名を指定できます。

［**件名のテンプレート**］ドロップダウンリストで、件名のテンプレートを選択できます。選択したテンプレートに対応する変数が［**件名**］に入力されます。複数の件名のテンプレートを選択して、メールの件名を構成できます。

［**送信者のメールアドレス：指定されていない場合は、受信者のアドレスを使用します。 注意：実在しないアドレスは使用しないことを推奨します**］で、送信者のメールアドレスを指定します。このフィールドを空白にした場合、既定では、宛先のアドレスが使用されます。実在しないアドレスを使用することは避けてください。

［**SMS メッセージの受信者の電話番号**］フィールドで、SMS 通知の受信者の携帯電話番号を指定します。

［**通知メッセージ**］では、イベントが発生した時に送信される、イベントに関する情報を含む標準的なメッセージを指定できます。このメッセージには、イベント名、デバイス名、ドメイン名などの代替パラメータを含めることができます。

通知テキストにパーセント記号「%」が含まれる場合、メッセージを送信するには 2 つ続けて入力する必要があります。たとえば、「CPU の負荷 100%%」のように入力します。

［**テストメッセージの送信**］をクリックして、通知が正しく設定されているか確認します。指定した宛先にテスト通知が送信されます。

［**通知数の上限を設定する**］をクリックし、指定した時間内に送信できる最大通知数を指定します。

- **実行ファイル**

この通知方法を選択すると、イベントの発生時に起動するアプリケーションを入力フィールドで選択できます。

［**イベント発生時に管理サーバーで実行される実行ファイル**］で、実行するファイルのあるフォルダーとファイル名を指定します。ファイルを指定する前に、通知メッセージで送信されるイベントの詳細を定義するファイルを準備してプレースホルダを指定してください。指定するフォルダーとファイルは、管理サーバー上に配置する必要があります。

［**通知数の上限を設定する**］をクリックすると、指定した時間内に送信できる最大通知数を指定できます。

3. タブで通知の設定を指定します。
4. ［OK］をクリックして、管理サーバーのプロパティウィンドウを閉じます。

保存した通知の配信設定は、Kaspersky Security Center Linux で発生するすべてのイベントに適用されます。

管理サーバーの設定、ポリシーの設定、またはアプリケーションの設定で、［**イベントの設定**］で指定された設定を特定のイベントについて上書きできます。

テストの通知

イベント通知が送信されているかどうかを確認するには、クライアントデバイスで EICAR テストウイルスを検知したことの通知を使用します。

イベント通知の送信を検証するには：

1. クライアントデバイスでファイルシステムのリアルタイム保護タスクを停止し、EICAR テストウイルスをクライアントデバイスにコピーします。ファイルシステムのリアルタイム保護タスクを再び有効にします。
2. EICAR テストウイルスがあるクライアントデバイスを含む管理グループまたはそのデバイスに対してスキャンタスクを実行します。

   スキャンタスクが正しく設定されていれば、テストウイルスが検知されます。通知が正しく設定されていれば、ウイルスが検知されたと通知されます。

テストウイルスの検知記録を開くには：

1. メインメニューで、［**監視とレポート**］→［**イベントの抽出**］の順に選択します。

2. 抽出名［**最近のイベント**］をクリックします。
   表示されるウィンドウに、テストウイルスに関する通知が表示されます。

EICAR テストウイルスには、デバイスに損害を与えるコードは含まれていません。ただし、ほとんどの製造元のセキュリティ製品で、このファイルはウイルスと判断されます。このテストウイルスは、EICAR の公式 Web サイトからダウンロードできます。

実行ファイルの起動により表示されるイベント通知

Kaspersky Security Center Linux は、実行ファイルを起動することにより、クライアントデバイスでのイベントについて管理者に通知できます。この実行ファイルには、管理者にリレーするイベントのプレースホルダーを持つ別の実行ファイルを含める必要があります。

イベントを説明するためのプレースホルダー

プレースホルダー	プレースホルダーの説明
%SEVERITY%	イベントの重要度
%COMPUTER%	イベントが発生したデバイスの名前
%DOMAIN%	ドメイン
%EVENT%	イベント
%DESCR%	イベントの説明
%RISE_TIME%	作成時刻
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	タスク名
%KL_PRODUCT%	Kaspersky Security Center Linux ネットワークエージェント
%KL_VERSION%	ネットワークエージェントのバージョン番号
%HOST_IP%	IP アドレス
%HOST_CONN_IP%	接続 IP アドレス

例：
イベント通知は、%COMPUTER% プレースホルダーを持つ実行ファイル（script2.bat など）を内部で起動する別の実行ファイル（script1.bat など）によって送信されます。イベントが発生すると、管理者のデバイスでファイル script1.bat が起動され、それが %COMPUTER% プレースホルダーを持つファイル script2.bat を起動します。次に管理者は、イベントが発生したデバイスの名前を受信します。

カスペルスキーからの通知

このセクションでは、カスペルスキーからの通知の使用、設定、無効にする方法について説明します。

カスペルスキーからの通知について

カスペルスキーからの通知（［**監視とレポート**］→［**カスペルスキーからの通知**］）には、Kaspersky Security Center のバージョンと、管理対象デバイスにインストールされている管理対象アプリケーションに関連する情報が提供されます。このセクションの情報は、古い通知を削除し、新しい情報を追加することで定期的に更新されます。

Kaspersky Security Center は、現在接続されている管理サーバーおよび管理サーバーの管理対象デバイスにインストールされているカスペルスキー製品に関連するカスペルスキーからの通知のみ表示します。プライマリ、セカンダリ、または仮想サーバーなど管理サーバーの種別に関係なく個別に通知が表示されます。

カスペルスキーからの通知を受け取るために、管理サーバーにはインターネット接続が必要です。

通知には次の種別の情報が含まれます：

- セキュリティ関連告知

  お客様のネットワーク内にインストールされたカスペルスキー製品を最新かつ機能の制限がない状態に保つためのセキュリティ関連告知通知には、カスペルスキー製品の重要なアップデート、既知の脆弱性に対する修正、カスペルスキー製品の問題を修正する方法に関する情報が含まれることがあります。既定では、セキュリティ関連の通知は有効になっています。通知が必要ない場合は、この機能を無効にできます。

  お客様のネットワーク保護の設定に対応した情報を表示するために、Kaspersky Security Center はデータをカスペルスキーのクラウドサーバーに送信し、ネットワーク内にインストールされたカスペルスキー製品に関連する通知のみを受け取ります。サーバーに送信される可能性のあるデータセットに関しては、Kaspersky Security Center の管理サーバーをインストールする際に同意いただいた使用許諾契約書で説明されています。

- マーケティング関連告知

  マーケティング関連告知には、カスペルスキー製品に関するお得な情報やキャンペーン、カスペルスキーからのニュースなどが含まれます。マーケティング関連の告知は既定で無効になっています。この種類の告知は Kaspersky Security Network (KSN) を有効にした場合のみ受け取ります。KSN を無効にすることでマーケティング関連告知を無効にできます。

  お客様のネットワークのデバイスの保護や日々の作業に役立つ可能性のある情報のみを表示するため、Kaspersky Security Center はカスペルスキーのクラウドサーバーにデータを送信し、適切な通知を受け取ります。サーバーに送信される可能性のあるデータセットは、KSN に関する声明の処理されるデータに関する項で説明されています。

新しい情報は、重要度に基づいて次のカテゴリに分類されます：

1. 緊急の情報
2. 重要なニュース
3. 警告
4. 情報

カスペルスキーからの通知セクションに新しい情報が表示された際に、Kaspersky Security Center 14 Web コンソールには通知の重要度のレベルに応じた通知ラベルが表示されます。ラベルをクリックして、［カスペルスキーからの通知］セクションで通知を表示できます。

カスペルスキーからの通知の設定で、表示する通知のカテゴリや通知を表示する位置を含む設定ができます。通知が必要ない場合は、この機能を無効にできます。

カスペルスキーからの通知を設定する

［カスペルスキーからの通知］セクションで、表示する通知のカテゴリおよび通知を表示する位置を含むカスペルスキーからの通知の設定を変更できます。

カスペルスキーからの通知を設定するには：

1. メインメニューで、［**監視とレポート**］→［**カスペルスキーからの通知**］の順に選択します。
2. ［**設定**］をクリックします。
   カスペルスキーからの通知の設定ウィンドウが開きます。
3. 次の設定を指定します：
   - 表示する通知の重要度を選択します。その他のカテゴリの通知は表示されません。
   - 通知ラベルを表示する場所を選択します。ラベルはすべてのコンソールセクション、または［**監視とレポート**］セクションおよびそのサブセクションに表示することができます。
4. ［**OK**］をクリックします。
   カスペルスキーからの通知が設定されました。

カスペルスキーからの通知を無効にする

カスペルスキーからの通知（［**監視とレポート**］→［**カスペルスキーからの通知**］）には、Kaspersky Security Center のバージョンと、管理対象デバイスにインストールされている管理対象アプリケーションに関連する情報が提供されます。通知が必要ない場合は、この機能を無効にできます。

カスペルスキーからの通知を無効にするには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. ［**全般**］タブで、［**カスペルスキーからの通知**］を選択します。
3. ［**セキュリティ関連告知が［無効］です**］にします。
4. ［**保存**］をクリックします。
   カスペルスキーからの通知が無効になります。

SIEM システムへのイベントのエクスポート

このセクションでは、SIEM システムへのイベントのエクスポートの設定について説明します。

シナリオ：SIEM システムへのイベントのエクスポートの設定

Kaspersky Security Center Linux では、Syslog 形式を使用する SIEM システムへエクスポートする方法、または Kaspersky Security Center のデータベースから直接 SIEM システムにイベントをエクスポートする方法のどちらかで SIEM システムへのイベントのエクスポートを許可します。このシナリオを完了すると、管理サーバーはイベントを SIEM システムに自動的に送信します。

必須条件

Kaspersky Security Center Linux でイベントのエクスポートの設定を開始する前に：

- イベントのエクスポート方法の詳細を参照してください。
- システムの設定値を確認してください。

このシナリオのステップは、任意の順序で実行できます。

イベントを SIEM システムにエクスポートするプロセスは、次の手順で構成されます：

- **Kaspersky Security Center Linux からイベントを受信するように SIEM システムを設定する**

  手順：SIEM システムへのイベントのエクスポートの設定

- **SIEM システムにエクスポートするイベントの選択**

  SIEM システムにエクスポートするイベントをマークします。最初に、すべての管理対象のカスペルスキー製品内で発生する一般的なイベントをマークします。それから、特定の管理対象のカスペルスキー製品のイベントをマークします。

- **SIEM システムへのイベントのエクスポートの設定**

  次のいずれかの方法でイベントをエクスポートします：

  - TCP / IP、UDP、または TLS overTCP プロトコルを使用
  - Kaspersky Security Center データベースからのイベントの直接エクスポートを使用（データベースでは定義済みのパブリックビューのセットを使用できます。これらのパブリックビューの詳細については、klakdb.chm のドキュメントを参照してください）

結果

エクスポートするイベントを選択した場合、SIEM システムへのイベントのエクスポートの設定後にエクスポート結果を表示できます。

事前準備

Kaspersky Security Center Linux 管理コンソールでイベントの自動エクスポートを設定する場合は、SIEM システム設定の一部を指定する必要があります。Kaspersky Security Center Linux の設定を準備できるように、SIEM システムの設定を事前に確認しておいてください。

SIEM システムへのイベントの自動送信を正しく設定するには、次の設定の値を把握する必要があります：

- **SIEM システムサーバーアドレス**

  現在使用している SIEM システムがインストールされているサーバーの IP アドレスです。SIEM システム設定でこの値を確認してください。

- **SIEM システムサーバーのポート**

  Kaspersky Security Center Linux と SIEM システムサーバー間の接続を確立するために使用するポート番号。Kaspersky Security Center Linux の設定と SIEM システムのレシーバ設定でこの値を指定します。

- **プロトコル**

  Kaspersky Security Center Linux から SIEM システムへのメッセージの送信に使われるプロトコル。Kaspersky Security Center Linux の設定と SIEM システムのレシーバ設定でこの値を指定します。

Kaspersky Security Center Linux のイベントについて

Kaspersky Security Center Linux では、管理サーバーと管理対象デバイスにインストールされた他のカスペルスキー製品の動作中に発生したイベントの情報を受信できます。イベントに関する情報は管理サーバーデータベースに保存されます。この情報は外部 SIEM システムにエクスポートできます。イベント情報を外部 SIEM システムにエクスポートすると、SIEM システムの管理者は、管理対象デバイスまたはデバイスのグループで発生したセキュリティシステムイベントに迅速に対処できます。

種別ごとのイベント

Kaspersky Security Center Linux には、次のイベント種別があります：

- 一般イベント：管理対象となるカスペルスキー製品すべてで共通して発生するイベントです。一般イベントの例としては「ウイルスアウトブレイク」があります。一般イベントでは、構文と形式が厳密に定義されています。一般イベントは、レポートやダッシュボードなどで使用されます。

- 管理対象のカスペルスキー製品それぞれに固有のイベント：管理対象となるカスペルスキーの各製品には、独自のイベントのセットがあります。

ソース別イベント

製品によって生成されるイベントの完全なリストは、アプリケーションポリシーの［**イベントの設定**］タブで確認できます。管理サーバーの場合、管理サーバーのプロパティでもイベントリストを表示できます。

イベントは、次の製品で生成される可能性があります：

- Kaspersky Security Center Linux のコンポーネント：

  - 管理サーバー

- ネットワークエージェント

- 管理対象のカスペルスキー製品

  管理対象のカスペルスキー製品によって生成されるイベントの詳細は、該当する製品のドキュメントを参照してください。

重要度別イベント

各イベントには固有の重要度があります。発生した状況に応じて、イベントには様々な重要度が割り当てることができます。イベントの重要度には次の 4 つがあります：

- *緊急イベント*は、データの損失、誤動作、または重大なエラーを招きかねない重大な問題が発生したことを示すイベントです。

- *機能エラー*は、アプリケーションの動作中または手順の実行中に重大な問題、エラー、または誤動作の発生を示すイベントです。

- *警告*は、必ずしも重大ではなくても、将来問題が発生する可能性があることを示すイベントです。こうしたイベントの発生後、データや機能を失わずにアプリケーションを復元できるのであれば、ほとんどのイベントは警告を意味します。

- *情報*イベントは、操作が適切に完了したこと、アプリケーションが適切に動作していること、手順が完了したことを伝えるために発生するイベントです。

各イベントには保管期間が定義されており、保管期間中、ユーザーは Kaspersky Security Center Linux でイベントを表示または変更することができます。一部のイベントは既定により、管理サーバーデータベースに保管されません。保管期間がゼロと定義されているためです。管理サーバーデータベースに 1 日以上保管されるイベントだけを外部システムにエクスポートできます。

イベントのエクスポートについて

イベントのエクスポートは、組織および技術レベルでセキュリティ問題に対処し、セキュリティ監視サービスを提供し、各種ソリューションからの情報を統合できる、一元化されたシステム内で使用できます。これらは SIEM システムで、ネットワークのハードウェアとアプリケーション、またはセキュリティオペレーションセンター（SOC）によって生成されたセキュリティアラートとイベントをリアルタイムで分析します。

これらのシステムは、ネットワーク、セキュリティ、サーバー、データベース、アプリケーションなど多くのソースからのデータを受信します。SIEM システムは、重要なイベントを見逃すことがないように、監視対象データを統合する機能も提供します。さらに、緊急のセキュリティ問題を管理者に通知するために、相互に関連するイベントとアラートの分析を自動的に実行します。アラートはダッシュボードから発することも、メールなどのサードパーティのチャネルから送信することもできます。

Kaspersky Security Center Linux から外部 SIEM システムにイベントをエクスポートするプロセスには、イベントの送信元である Kaspersky Security Center Linux とイベントのレシーバである SIEM システムの 2 つが関係します。イベントを正常にエクスポートするには、SIEM システムと Kaspersky Security Center Linux の両方で設定する必要があります。どちらを先に設定してもかまいません。Kaspersky Security Center Linux からのイベントの送信を設定してから、SIEM システムによるイベントの受信を設定することも、逆の順序で設定することもできます。

イベントのエクスポートの Syslog 形式

Syslog 形式のイベントを任意の SIEM システムに送信できます。Syslog 形式を使用すると、管理サーバーおよび管理対象デバイスにインストールされたカスペルスキー製品で発生したイベントをすべてリレーできます。Syslog 形式でイベントをエクスポートする場合は、SIEM システムにリレーするイベントの種別を正確に選択できます。

SIEM システムによるイベントの受信

SIEM システムは、Kaspersky Security Center Linux からイベントを受信して適切に解析する必要があります。これらの目的に対応できるように、SIEM システムを適切に設定する必要があります。設定は、利用する具体的な SIEM システムによります。ただし、レシーバとパーサーの設定など、すべての SIEM システムの設定で一般的なステップがいくつかあります。

SIEM システムでのイベントのエクスポートの設定について

Kaspersky Security Center Linux から外部 SIEM システムにイベントをエクスポートするプロセスには、イベントの送信元である Kaspersky Security Center Linux とイベントのレシーバである SIEM システムの 2 つが関係します。イベントのエクスポートは、SIEM システムと Kaspersky Security Center Linux の両方で設定する必要があります。

SIEM システムで指定する設定は、使用している個々のシステムにより異なります。一般に、すべての SIEM システムでレシーバを設定する必要があり、受信イベントを解析するためのメッセージパーサーを任意で設定します。

レシーバの設定

Kaspersky Security Center Linux から送信されたイベントを受信するには、SIEM システムでレシーバを設定する必要があります。一般に、SIEM システムで次の設定を指定する必要があります：

- **エクスポートプロトコル**

  メッセージ送信プロトコル（UDP、TCP、TLS over TCP）。このプロトコルは、Kaspersky Security Center Linux で指定したプロトコルと同じにする必要があります。

- **Port**

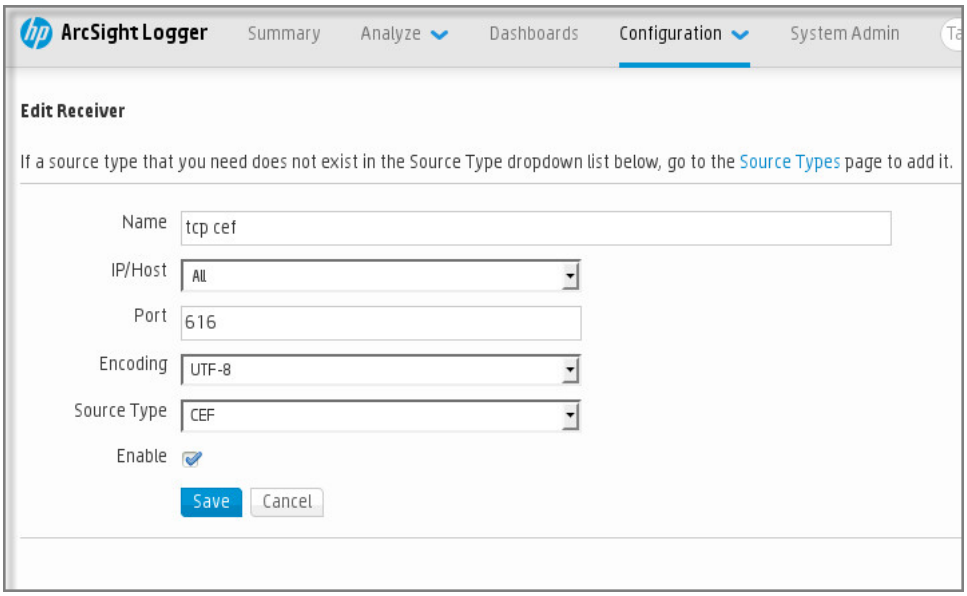
  Kaspersky Security Center Linux に接続するポート番号を指定します。このポートは SIEM システムの設定中に Kaspersky Security Center Linux で指定したポートと同じポートである必要があります。

- **データ形式**

  Syslog 形式を指定します。

使用する SIEM システムによっては、受信者の設定を一部追加で指定する必要があります。

次の図は、ArcSight の受信者のセットアップ画面を示します。



ArcSight でのレシーバのセットアップ

メッセージパーサー

エクスポートされたイベントはメッセージとして SIEM システムに渡されます。SIEM システムでイベントに関する情報が利用できるように、これらのメッセージを適切に解析する必要があります。メッセージパーサーは SIEM システムの一部です。イベントの ID、重大度、説明、パラメータなど関連フィールドにメッセージの内容を分けるために使用します。メッセージの内容を分けることで、SIEM システムは Kaspersky Security Center Linux から受信したイベントを処理して、SIEM システムデータベースに保管することができます。

各 SIEM システムには、一連の標準メッセージパーサーがあります。カスペルスキーでは、QRadar や ArcSight など、一部の SIEM システム向けのメッセージパーサーも提供しています。これらのメッセージパーサーは、対応する SIEM システムの Web サイトからダウンロードできます。レシーバを設定する時に、標準メッセージパーサーまたはカスペルスキーが提供するメッセージパーサーのいずれかを選択できます。

Syslog 形式で SIEM システムにエクスポートするイベントのマーキング

このセクションでは、SIEM システムに Syslog 形式でエクスポートするイベントをマークする方法について説明します。

Syslog 形式で SIEM システムにエクスポートするイベントのマーキングについて

イベントの自動エクスポートを有効にしたら、外部 SIEM システムにエクスポートするイベントを選択する必要があります。

次の条件のいずれかに基づいて、外部システムへの Syslog 形式でのイベントのエクスポートを設定できます：

- 一般的なイベントのマーキング。イベントの設定または管理サーバーの設定でエクスポートするイベントをポリシー内でマークすると、特定のポリシーで管理されているすべてのアプリケーションで発生した選択済みのイベントが SIEM システムに送信されます。エクスポートされたイベントがポリシー内で選択され

ている場合、このポリシーで管理されている個別アプリケーションの当該イベントを再定義することはできません。

- 管理対象アプリケーションのイベントのマーキング。管理対象デバイスにインストールされた管理対象アプリケーションへエクスポートするイベントをマークすると、そのアプリケーションで発生したイベントのみが SIEM システムに送信されます。

Syslog 形式でエクスポートするカスペルスキー製品のイベントのマーキング

管理対象デバイスにインストールされた特定の管理対象アプリケーションで発生したイベントをエクスポートする場合は、エクスポートするイベントをそのアプリケーションのポリシーでマークします。この場合、マークされたイベントが、ポリシーの範囲に含まれるすべてのデバイスからエクスポートされます。

特定の管理対象アプリケーションからエクスポートするイベントをマークするには：

1. メインメニューで、［**デバイス**］→［**ポリシーとプロファイル**］の順に移動します。
2. イベントをマークするアプリケーションのポリシーをクリックします。
   ポリシーの設定ウィンドウが表示されます。
3. ［**イベントの設定**］セクションに移動します。
4. SIEM にエクスポートするイベントに隣接するチェックボックスをオンにします。
5. ［**Syslog を使用しての SIEM システムへのエクスポート用にマークする**］をクリックします。

   SIEM システムにエクスポートするイベントは、イベントのリンクをクリックして開く［**イベント登録**］セクションでマーキングすることもできます。

6. チェックマーク（✓）がイベントまたは SIEM システムにエクスポートするためにマーキングしたイベントの［**Syslog**］列に表示されます。
7. ［**保存**］をクリックします。

管理対象アプリケーションからマークされたイベントを、SIEM システムへエクスポーされる準備ができています。

特定の管理デバイスのために、SIEM システムへエクスポートするイベントをマークできます。以前エクスポートしたイベントがアプリケーションのポリシーでマークされた場合、管理対象デバイスのためにマークされたイベントを再定義することはできません。

管理対象デバイスにエクスポートするイベントをマークするには：

1. メインメニューで、［**デバイス**］→［**管理対象デバイス**］の順に選択します。
   管理対象デバイスのリストが表示されます。
2. 管理対象デバイスのリストで、必要なデバイスの名前のリンクをクリックします。
   選択したデバイスのプロパティウィンドウが表示されます。

3. ［**アプリケーション**］セクションに移動します。

4. アプリケーションのリストで、必要なアプリケーションの名前のリンクをクリックします。

5. ［**イベントの設定**］セクションに移動します。

6. SIEM にエクスポートするレイベントに隣接するチェックボックスをオンにします。

7. ［**Syslog を使用しての SIEM システムへのエクスポート用にマークする**］をクリックします。

SIEM システムにエクスポートするイベントは、イベントのリンクをクリックして開く［**イベント登録**］セクションでマークすることもできます。

8. チェックマーク（✓）がイベントまたは SIEM システムにエクスポートするためにマーキングしたイベントの［**Syslog**］列に表示されます。

これで、SIEM システムへのエクスポートが設定済みの場合は、マーキングされたイベントが管理サーバーから SIEM システムへ送信されるようになりました。

Syslog 形式でエクスポートする一般的なイベントのマーキング

Syslog 形式を使用して、管理サーバーが SIEM システムにエクスポートする一般的なイベントをマーキングすることができます。

SIEM システムにエクスポートする一般的なイベントをマークするには：

1. 次のいずれかの手順を実行します：

   - 目的の管理サーバーを選択し、横にある設定アイコン（  ）をクリックします。
   - メインメニューで、［**デバイス**］→［**ポリシーとプロファイル**］の順に移動し、ポリシーのリンクをクリックします。

2. 表示されたウィンドウで、［**イベントの設定**］タブを選択します。

3. ［**Syslog を使用しての SIEM システムへのエクスポート用にマークする**］をクリックします。

SIEM システムにエクスポートするイベントは、イベントのリンクをクリックして開く［**イベント登録**］セクションでマーキングすることもできます。

4. チェックマーク（✓）がイベントまたは SIEM システムにエクスポートするためにマーキングしたイベントの［**Syslog**］列に表示されます。

これで、SIEM システムへのエクスポートが設定済みの場合は、マーキングされたイベントが管理サーバーから SIEM システムへ送信されるようになりました。

Syslog 形式を使用したイベントのエクスポートについて

Syslog 形式を使用すると、管理サーバー、管理対象デバイスにインストールされた他のカスペルスキー製品で発生したイベントを SIEM システムにエクスポートできます。

Syslog は標準メッセージロギングプロトコルです。メッセージを生成するソフトウェア、メッセージを保管するシステム、メッセージを報告、分析するソフトウェアを分けることができます。各メッセージには、メッセージを生成したソフトウェアの種別を示す機能コードのラベルが付けられ、重要度が割り当てられます。

Syslog 形式は、インターネット技術タスクフォース（インターネット標準）によって公開されている RFC（Request for Comments）の文書で定義されています。Kaspersky Security Center Linux から外部システムへのイベントのエクスポートには、RFC 5424 標準が使用されます。

Kaspersky Security Center Linux で、Syslog 形式を使用して外部システムにイベントがエクスポートされるように設定できます。

エクスポートのプロセスは次の 2 つのステップで構成されます：

1. イベントの自動エクスポートの有効化。このステップでは、イベントを SIEM システムに送信するように Kaspersky Security Center Linux を設定します。自動エクスポートを有効にすると、Kaspersky Security Center Linux は即座にイベントの送信を開始します。
2. 外部システムにエクスポートするイベントの選択。このステップでは、SIEM システムにエクスポートするイベントを選択します。

イベントを SIEM システムにエクスポートするための Kaspersky Security Center Linux の設定

イベントを SIEM システムにエクスポートするには、Kaspersky Security Center Linux でエクスポートプロセスを設定する必要があります。

Kaspersky Security Center 14 Web コンソールで SIEM システムへのエクスポートを設定するには：

1. ［**コンソールの設定**］ドロップダウンリストで、［**連携**］を選択します。
   コンソールの設定ウィンドウが表示されます。
2. ［**連携**］タブを選択します。
3. ［**連携**］タブで、［**SIEM**］セクションを選択します。
4. ［**設定**］をクリックします。
   ［**エクスポート設定**］セクションが開きます。
5. ［**エクスポート設定**］セクションで設定を指定します：
   - **SIEM システムサーバーアドレス**

     現在使用している SIEM システムがインストールされているサーバーの IP アドレスです。SIEM システム設定でこの値を確認してください。

   - **SIEM システムのポート**

Kaspersky Security Center Linux と SIEM システムサーバー間の接続を確立するために使用するポート番号。Kaspersky Security Center Linux の設定と SIEM システムのレシーバ設定でこの値を指定します。

- **プロトコル**

メッセージを SIEM システムに送信するために使用するプロトコルを選択します。TCP/IP、UDP、TCP プロトコルのいずれかを選択できます。

TLS over TCP プロトコルを選択した場合は、次の TLS 設定を指定します：

- **サーバー認証**

  ［**サーバー認証**］フィールドでは、**信頼する証明書**または **SHA フィンガープリント**を選択できます：

  - **信頼できる証明書**：信頼できる証明書認証局（CA）から証明書のリストを含むファイルを受け取り、ファイルを Kaspersky Security Center Linux にアップロードできます。Kaspersky Security Center Linux は、SIEM システムサーバーの証明書も CA によって署名されているかどうかを確認します。

    信頼できる証明書を追加するには、［**CA 証明書を参照**］をクリックして、証明書をアップロードします。

  - **SHA フィンガープリント**：SIEM システム証明書の SHA-1 サムプリントを Kaspersky Security Center で指定できます。SHA-1 サムプリントを追加するには、［**サムプリント**］フィールドでサムプリントを入力し、［**追加**］をクリックします。

  ［**クライアント認証を追加する**］を使用して、Kaspersky Security Center を認証する証明書を生成することができます。このようにして、Kaspersky Security Center が発行した自己署名証明書を使用します。この場合、SIEM システムサーバーの認証に、信頼できる証明書と SHA フィンガープリントの両方を使用することができます。

- **サブジェクト名 / サブジェクト代替名を追加する**

  サブジェクト名は、証明書を受け取るドメインの名前です。SIEM システムサーバーのドメイン名が SIEM システムサーバー証明書のサブジェクト名と一致しない場合、Kaspersky Security Center Linux は SIEM システムサーバーに接続できません。しかし、SIEM システムサーバーは証明書内で名前が変更された場合にドメイン名を変更することがあります。この場合、サブジェクト名を［**サブジェクト名 / サブジェクト代替名を追加する**］で指定することができます。指定されたサブジェクト名のいずれかが SIEM システム証明書のサブジェクト名と一致する場合、Kaspersky Security Center Linux は SIEM システムサーバー証明書を検証します。

- **クライアント認証を追加する**

  クライアント認証用に、自身の証明書を挿入するか、Kaspersky Security Center で生成することができます。

  - **証明書を挿入する**:CA など、任意の発行元から受け取った証明書を使用できます。次のいずれかの証明書タイプを使用して、証明書とその秘密鍵を指定する必要があります：

    - **X.509 証明書 PEM**：［**証明書のファイル**］フィールドに証明書のファイルをアップロードし、［**鍵のファイル**］フィールドに秘密鍵のファイルをアップロードします。両方のファイルは相互に依存せず、ファイルを読み込む順序は重要ではありません。両方のファイルがアップロードされたら、秘密鍵をデコードするためのパスワードを［**パスワードまたは証明書の検証**］で指定します。秘密鍵がエンコードされていない場合、パスワードの値は空である可能性があります。

    - **X.509 証明書 PKCS12**：証明書と秘密鍵を含む単一のファイルを［**証明書のファイル**］フィールドにアップロードします。ファイルをアップロードしたら、秘密鍵をデコードするためのパスワードを［**パスワードまたは証明書の検証**］で指定します。秘密鍵がエンコードされていない場合、パスワードの値は空である可能性があります。

- **鍵を生成する**：Kaspersky Security Center で自己署名証明書を生成できます。Kaspersky Security Center Linux は生成された自己署名証明書を保存し、証明書の公開部分または SHA-1 フィンガープリントを SIEM システムに渡すことができます。

6. 必要に応じて、管理サーバーデータベースからアーカイブイベントをエクスポートし、アーカイブイベントのエクスポートを開始する日付を設定できます：

   a. ［**エクスポートの開始日を設定**］をクリックします。

   b. 表示されたセクションの［**エクスポートの開始日**］に、開始日を指定します。

   c. ［**OK**］をクリックします。

7. オプションを［**SIEM システムデータースへのイベントの自動エクスポートが［有効］です**］に切り替えます。

8. ［**保存**］をクリックします。

SIEM システムへのエクスポートが設定されました。これで、イベントの受信を SIEM システムで設定した場合は、マーキングされたイベントが管理サーバーから SIEM システムにエクスポートされます。エクスポートの開始日を設定した場合、管理サーバーは指定された日付からも管理サーバーデータベース内のマーキングされたイベントをエクスポートします。

データベースからのイベントの直接エクスポート

Kaspersky Security Center Linux インターフェイスを使わなくても、Kaspersky Security Center Linux のデータベースから直接イベントを取得できます。パブリックビューに対して直接クエリを実行してイベントデータを取得することも、既存のパブリックビューを基に独自のビューを作成して、必要なデータを取得するようにアドレス指定することもできます。

パブリックビュー

Kaspersky Security Center Linux のデータベースには、パブリックビューの便利なセットをご用意しています。これらのパブリックビューの詳細は、klakdb.chm のドキュメントを参照してください。

v_akpub_ev_event パブリックビューには、データベース内のイベントパラメータを表す一連のフィールドが含まれています。klakdb.chm ドキュメントには、デバイス、アプリケーション、ユーザーなど、他の Kaspersky Security Center Linux のエンティティに対応するパブリックビューに関する情報も含まれています。この情報はクエリに使用できます。

このセクションでは、klsql2 ユーティリティを使って SQL クエリを作成する手順について説明し、クエリの例を示します。

SQL クエリまたはデータベースビューを作成する時には、データベースと連携する他のプログラムも使用できます。Kaspersky Security Center Linux のデータベースへの接続に必要なインスタンス名やデータベース名などのパラメータの表示方法についても、該当セクションを参照してください。

klsql2 ユーティリティを使用した SQL クエリの作成

このセクションでは、klsql2 ユーティリティを使用する方法、このユーティリティを使用して SQL クエリを作成する方法について説明します。klsql2 ユーティリティを使用して SQL クエリを作成する場合は、クエリによって Kaspersky Security Center Linux のパブリックビューが直接アドレス指定されるため、データベース名とアクセスパラメータを指定する必要はありません。

klsql2 ユーティリティを使用するには：

1. Kaspersky Security Center Linux 管理サーバーがインストールされたデバイスのディレクトリ /opt/kaspersky/ksc64/sbin/klsql2 に移動します。
2. このディレクトリに、ブランクファイル src.sql を作成します。
3. テキストエディターで src.sql ファイルを開きます。
4. 必要な SQL クエリを src.sql ファイルに入力して、ファイルを保存します。
5. Kaspersky Security Center Linux 管理サーバーがインストールされたデバイスで、次のコマンドをコマンドラインに入力して、src.sql ファイルから SQL クエリを実行し、結果を result.xml ファイルに保存します：
   ```
   sudo ./klsql2 -i src.sql -o result.xml
   ```
6. 新しく作成された result.xml ファイルを開いて、クエリの結果を確認します。

src.sql ファイルを編集して、パブリックビューへのクエリを作成できます。次に、コマンドラインからクエリを実行して、結果をファイルに保存します。

klsql2 ユーティリティでの SQL クエリの例

このセクションでは、klsql2 ユーティリティによって作成された SQL クエリの例を示します。

次の例では、過去 7 日間にデバイスで発生したイベントを取得し、発生した順にイベントを表示します。イベントは新しい順から表示されます。

例：

```
SELECT
e.nId, /* イベントの識別子 */
e.tmRiseTime, /* イベントが発生した時間 */
e.strEventType, /* イベント種別の内部名 */
e.wstrEventTypeDisplayName, /* イベント種別の表示名 */
e.wstrDescription, /* イベントについて表示される説明 */
e.wstrGroupName, /* デバイスが配置されているグループの名前 */
h.wstrDisplayName, /* イベントが発生したデバイスの表示名 */
CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp) & 255) AS varchar(4)) as strIp /* イベントが発生したデバイスの IP アドレス */
FROM v_akpub_ev_event e
INNER JOIN v_akpub_host h ON h.nId=e.nHostId
WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
ORDER BY e.tmRiseTime DESC
```

Kaspersky Security Center Linux データベース名の表示

SQL Server、MySQL、MariaDB のいずれかのデータベース管理ツールで Kaspersky Security Center Linux のデータベースにアクセスする場合は、SQL スクリプトエディターから接続できるようにその定義データベースの名前を調べる必要があります。

Kaspersky Security Center Linux のデータベースの名前を表示するには：

1. 目的の管理サーバーを選択し、横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。

2. ［**全般**］タブで、［**現在のデータベースの詳細**］セクションを選択します。

   データベース名は［**データベース名**］フィールドに指定されます。このデータベース名を使用して、SQL クエリ内のデータベースのアドレスを指定します。

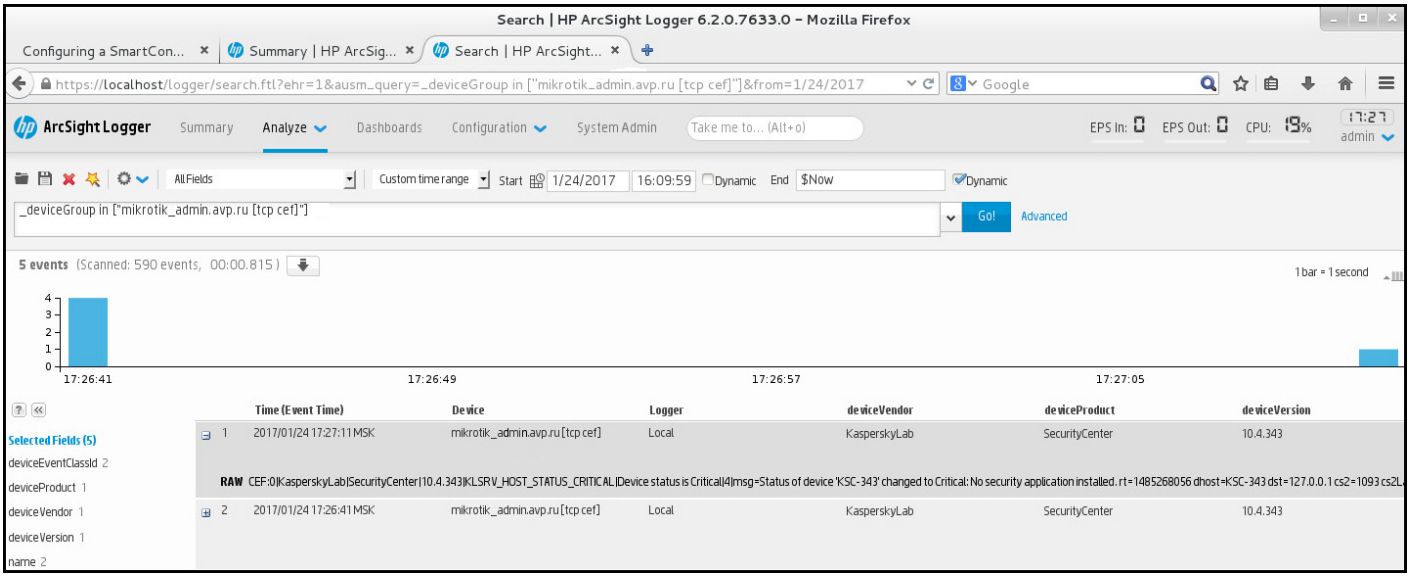
エクスポート結果の表示

イベントのエクスポート手順が正常に完了するようにコントロールすることができます。それには、イベントのエクスポートとともにメッセージが SIEM システムで受信されているかどうかを確認します。

Kaspersky Security Center Linux から送信されたイベントが SIEM システムで受信され、適切に解析されている場合、設定は両者で適切に行われています。イベントが受信されない場合は、Kaspersky Security Center Linux で指定した設定を SIEM システムの設定と比べて確認してください。

次の図は、ArcSight にエクスポートされたイベントを示します。たとえば、最初のイベントは重大な管理サーバーイベントです：「*デバイスのステータスが「緊急」です。*」

エクスポートされたイベントの SIEM システムでの表示は、使用している SIEM システムによって異なります。



イベントの例

デバイスの抽出

*デバイスの抽出*は、特定の条件を指定してデバイスをフィルタリングできる機能です。デバイスの抽出を使用して、複数のデバイスを管理できます。たとえば、デバイスの抽出に含まれるデバイスのみを対象とするレポートを表示したり、デバイスの抽出に含まれるデバイスすべてを別のグループに移動したりできます。

Kaspersky Security Center では、様々な*定義済みの抽出*（例：**「緊急」ステータスのデバイス**、**プロテクションが無効です**、**アクティブな脅威を検知しました**）を使用できます。定義済みの抽出は削除できません。*ユーザー定義の抽出*を追加で作成し設定できます。

ユーザー定義の抽出では、抽出範囲を「すべてのデバイス」「管理対象デバイス」「未割り当てデバイス」から選択できます。抽出条件のパラメータを指定できます。デバイスの抽出では、異なるパラメータを指定した複数の抽出条件を作成できます。たとえば、2 つの条件を作成し、それぞれに異なる IP アドレス範囲を指定できます。複数の条件を指定した場合、デバイスの抽出はいずれかの条件に 1 つでも一致するデバイスを表示します。これに対して、1 つの条件内で複数のパラメータが指定されている場合、すべてのパラメータを満たすことが求められます。たとえば、1 つの条件内で IP アドレス範囲とインストールされている製品名の両方が指定されている場合、該当する製品がインストールされていてなおかつ IP アドレスが指定した範囲内のデバイスのみが表示されます。

デバイスの抽出を表示するには：

1. メインメニューで、［**デバイス**］→［**デバイスの抽出**］、または［**検出と製品の導入**］→［**デバイスの抽出**］セクションの順に選択します。
2. 抽出のリストで、対応する抽出の名前をクリックします。

デバイスの抽出結果が表示されます。

デバイスの抽出の作成

デバイスの抽出を作成するには：

1. メインメニューで、［**デバイス**］→［**デバイスの抽出**］の順に移動します。
   デバイスの抽出のリストが表示されます。
2. ［**追加**］をクリックします。
   ［**デバイスの抽出の設定**］ウィンドウが表示されます。
3. 新しい抽出の名前を入力します。
4. デバイスの抽出に含めるデバイスの種別を指定します。
5. ［**追加**］をクリックします。
6. 表示されたウィンドウで、この抽出に含めるデバイスが満たす必要のある条件を指定し、［**OK**］をクリックします。
7. ［**保存**］をクリックします。

デバイスの抽出が作成され、リストに追加されます。

デバイスの抽出の設定

デバイスの抽出を設定するには：

1. ［**デバイス**］→［**デバイスの抽出**］の順に選択します。
   デバイスの抽出のリストが表示されます。
2. 関連するデバイスの抽出をクリックします。
   ［**デバイスの抽出の設定**］ウィンドウが表示されます。
3. ［**全般**］タブで、この抽出に含めるデバイスが満たす必要のある条件を指定します。
4. ［**保存**］をクリックします。

   設定が適用され保存されます。

以下に、デバイスを抽出に割り当てる条件について説明します。条件は論理演算子「OR」を使用して結合されます。抽出には、少なくとも1つの条件を満たすデバイスが含まれます。

全般

［**全般**］セクションでは、抽出条件の名前を変更したり、条件を反転させたりすることができます：

抽出の条件を反転させる

このオプションをオンにすると、指定した抽出条件の選択状態が反転します。指定した条件に合致しないすべてのデバイスが、抽出に含まれるようになります。

既定では、このオプションはオフです。

ネットワーク

［**ネットワーク**］セクションでは、ネットワークデータを基にデバイスを抽出に含める場合に使用する基準を指定できます：

- **デバイス名または IP アドレス**
- **Windows ドメイン**

  指定したワークグループに含まれるデバイスをすべて表示します。
- **管理グループ**

  指定した管理グループに含まれるデバイスを表示します。
- **説明**

デバイスのプロパティウィンドウ（［**全般**］セクションの［**説明**］）のテキスト。

［**説明**］で検索に使用する表現として、次の文字を使用できます：

- 1つの単語：
  - ***** -文字数不定の任意の文字列を表します。

    例：

    Server または **Server's** などの単語を記述するには、**Server*** と入力します。
  - **?** -任意の1文字を表します。

    例：

    SUSE Linux Enterprise Server 12 や **SUSE Linux Enterprise Server 15** などの単語を記述するには、「**SUSE Linux Enterprise Server 1?**」と入力します。

    アスタリスク（*****）または疑問符（**?**）は、クエリの先頭文字としては使用できません。
- 複数の単語による検索：
  - スペース -指定した単語のいずれかがコメントに含まれているデバイスがすべて表示されます。

    例：

    Secondary または **Virtual** という単語が含まれている語句を検索する場合は、クエリに **Secondary Virtual** と入力します。
  - **+** -単語の前にプラス記号を付けると、すべての検索結果にその単語が含まれます。

    例：

    Secondary と **Virtual** の両方が含まれた語句を検索するには、クエリに **+Secondary+Virtual** と入力します。
  - **-** -単語の前にマイナス記号を付けると、すべての検索結果にその単語が含まれません。

    例：

    Secondary が含まれ、**Virtual** が含まれない語句を検索するには、クエリに **+Secondary-Virtual** と入力します。
  - **"<任意のテキスト>"** -引用符で囲まれたテキストを含むテキストが検索されます。

    例：

    Secondary Server という語句を検索する場合は、クエリに **"Secondary Server"** と入力します。

- **IP アドレス範囲**

  このオプションをオンにすると、検索されるデバイスが属する IP アドレス範囲の最初と最後の IP アドレスを入力できます。

  既定では、このオプションはオフです。

タグ

［**タグ**］セクションでは、管理対象デバイスの説明に追加済みのキーワード（タグ）を基にデバイスを抽出に含めるための基準を設定できます：

- **少なくとも1個のタグが一致する場合に適用する**

  このオプションをオンにすると、選択されたタグを1つ以上説明に含むデバイスが検索結果に表示されます。

  このオプションをオフにすると、選択されたすべてのタグを説明に含むデバイスのみが検索結果に表示されます。

  既定では、このオプションはオフです。

- **タグを含む**

  このオプションをオンにすると、検索結果には、選択したタグが説明内に含まれるデバイスが表示されます。デバイスを検索するため、文字数不定の任意の文字列を表すアスタリスクを使用できます。

  既定では、このオプションがオンです。

- **タグを含まない**

  このオプションをオンにすると、検索結果には、選択したタグが説明内に含まれないデバイスが表示されます。デバイスを検索するため、文字数不定の任意の文字列を表すアスタリスクを使用できます。

ネットワーク活動

［**ネットワーク活動**］セクションでは、ネットワークアクティビティを基にデバイスを抽出に含める場合に使用する基準を指定できます：

- **ディストリビューションポイント**

  検索を実行する場合、抽出に含めるデバイスの基準を、ドロップダウンリストで設定できます：
  - **はい**ディストリビューションポイントとして動作するデバイスが抽出に含まれます。
  - **いいえ**：ディストリビューションポイントとして機能するデバイスが抽出に含まれません。
  - **値を選択しない**：基準は適用されません。

- **管理サーバーから切断しない**

  検索を実行する場合、抽出に含めるデバイスの基準を、ドロップダウンリストで設定できます：
  - **有効**：［**管理サーバーから切断しない**］をオンにしたデバイスが抽出に含まれます。
  - **無効**：［**管理サーバーから切断しない**］をオフにしたデバイスが抽出に含まれます。
  - **値を選択しない**：基準は適用されません。

- **接続プロファイルが切り替えられました**

検索を実行する場合、抽出に含めるデバイスの基準を、ドロップダウンリストで設定できます：

- **はい**接続プロファイルを切り替えた結果として管理サーバーに接続されたデバイスが抽出に含まれます。
- **いいえ**：接続プロファイルを切り替えた結果として管理サーバーに接続されたデバイスが抽出に含まれません。
- **値を選択しない**：基準は適用されません。

- **前回の管理サーバーへの接続**

このチェックボックスを使用して、管理サーバーに前回接続した日時によるデバイスの検索の基準を設定できます。

このチェックボックスをオンにすると、入力フィールドで、クライアントデバイスにインストールされたネットワークエージェントと管理サーバーとの間に前回接続が確立された日時の範囲を指定できます。指定された間隔内のデバイスが抽出に含まれます。

このチェックボックスをオフにすると、この基準は適用されません。

既定では、このチェックボックスはオフです。

- **ネットワークポーリングで検出された新規デバイス**

過去数日間のネットワークポーリングで検出された新規デバイスを検索します。

このオプションをオンにすると、［**検出期間（日）**］フィールドで指定した期間中のデバイスの検索で検出された新規デバイスのみが、抽出に含まれます。

このオプションをオフにすると、デバイスの検索で検出された新規デバイスがすべて抽出に含まれます。

既定では、このオプションはオフです。

- **デバイスが可視**

検索を実行する場合、抽出に含めるデバイスの基準を、ドロップダウンリストで設定できます：

- **はい**ネットワークで現在可視のデバイスを抽出に含めます。
- **いいえ**：ネットワークで現在不可視のデバイスを抽出に含めます。
- **値を選択しない**：基準は適用されません。

アプリケーション

［**アプリケーション**］セクションでは、選択した管理対象アプリケーションを基にデバイスを抽出に含めるための基準を設定できます：

- **アプリケーション名**

カスペルスキー製品の名前で検索を実行する場合、抽出に含めるデバイスの基準を、ドロップダウンリストで設定できます。

リストには、管理コンピューターに管理プラグインがインストールされているアプリケーションの名前のみが表示されます。

アプリケーションが選択されていない場合、この基準は適用されません

- **アプリケーションのバージョン**

  カスペルスキー製品のバージョン番号で検索を実行する場合、抽出に含めるデバイスの基準を、入力フィールドで設定できます。

  バージョン番号が指定されていない場合、この基準は適用されません。

- **重要なアップデート名**

  製品の名前またはアップデートパッケージ番号で検索する場合の、抽出に含めるデバイスの基準を、入力フィールドで設定できます。

  このフィールドが空白の場合、この基準は適用されません。

- **前回のモジュールアップデート**

  このオプションを使用して、デバイスにインストールされているソフトウェアモジュールの前回のアップデート日時でデバイスを検索する基準を設定できます。

  このチェックボックスをオンにすると、入力フィールドで、デバイスにインストールされているアプリケーションモジュールの前回のアップデートが実行された日時の範囲を指定できます。

  このチェックボックスをオフにすると、この基準は適用されません。

  既定では、このチェックボックスはオフです。

- **デバイスを Kaspersky Security Center 14 で管理する**

  ドロップダウンリストで、Kaspersky Security Center Linux で管理されているデバイスを抽出に含めることができます：

  - **はい**Kaspersky Security Center Linux で管理されているデバイスが抽出に含まれます。
  - **いいえ**：Kaspersky Security Center Linux により管理されていないデバイスが抽出に含まれます。
  - **値を選択しない**：基準は適用されません。

- **セキュリティ製品がインストールされている**

  ドロップダウンリストで、セキュリティ製品がインストールされているすべてのデバイスを抽出に含めることができます：

  - **はい**セキュリティ製品がインストールされているすべてのデバイスが抽出に含まれます。
  - **いいえ**：セキュリティ製品がインストールされていないすべてのデバイスが抽出に含まれます。
  - **値を選択しない**：基準は適用されません。

オペレーティングシステム

［**オペレーティングシステム**］セクションでは、オペレーティングシステム種別を基にデバイスを抽出に含める場合に使用する基準を指定できます。

- **オペレーティングシステムのバージョン**

  このチェックボックスをオンにすると、オペレーティングシステムをリストから選択できます。指定したオペレーティングシステムがインストールされたデバイスが検索結果に含まれます。

- **OS のビット数**

  ドロップダウンリストで、オペレーティングシステムのアーキテクチャを選択できます。これによって、デバイスに対する移動ルールの適用方法が決定されます（［**不明**］、［**x86**］、［**AMD64**］、［**IA64**］）。既定では、リストでオプションが選択されていないため、オペレーティングシステムのアーキテクチャは定義されていません。

- **OS サービスパックのバージョン**

  このフィールドでは、オペレーティングシステムのパッケージバージョンを「*X.Y*」形式で指定できます。これによって、デバイスに対する移動ルールの適用方法が決定されます。既定では、バージョンの値は指定されていません。

- **OS のビルド**

  この設定は Windows オペレーティングシステムにのみ適用できます。

  オペレーティングシステムのビルド番号です。選択したオペレーティングシステムのビルド番号が、入力したビルド番号と「等しい」「それより古い」「それより新しい」かを指定して検索できます。また、指定したビルド番号を除くすべてのビルド番号を検索するようにも設定できます。

- **OS のリリース ID**

  この設定は Windows オペレーティングシステムにのみ適用できます。

  オペレーティングシステムのリリース ID です。選択したオペレーティングシステムのリリース ID が、入力したリリース ID と「等しい」「それより古い」「それより新しい」かを指定して検索できます。また、指定したリリース ID を除くすべてのリリース ID を検索するようにも設定できます。

デバイスのステータス

［**デバイスのステータス**］セクションでは、管理対象アプリケーションからのデバイスのステータスの説明を基にデバイスを抽出に含めるための基準を設定できます：

- **デバイスのステータス**

ドロップダウンリストからデバイスのステータス（「*OK*」「*緊急*」「*警告*」）を選択します。

- **デバイスのステータスの説明**

  このフィールドで、「*OK*」「*緊急*」「*警告*」のいずれかのステータスをデバイスに割り当てる条件に対応するチェックボックスをオンにできます。

- **製品が定義したデバイスのステータス**

  リアルタイム保護のステータスを選択できるドロップダウンリスト。指定されたリアルタイム保護ステータスのデバイスが抽出に含まれます。

保護コンポーネント

［**保護コンポーネント**］セクションでは、保護ステータスを基にデバイスを抽出に含めるための基準を設定できます：

- **定義データベースの公開日時**

  このオプションをオンにすると、定義データベースの公開日時でクライアントデバイスを検索できます。入力フィールドで設定した期間に基づいて検索が実行されます。

  既定では、このオプションはオフです。

- **前回のスキャン**

  このオプションをオンにすると、前回ウイルススキャンを実行した日時でクライアントデバイスを検索できます。入力フィールドで、前回ウイルススキャンを実行した期間を指定できます。

  既定では、このオプションはオフです。

- **検知した脅威の数**

  このオプションをオンにすると、検知されたウイルスの数でクライアントデバイスを検索できます。入力フィールドで、ウイルス検知数の上下のしきい値を設定できます。

  既定では、このオプションはオフです。

アプリケーションレジストリ

［**アプリケーションレジストリ**］セクションでは、インストール済みのアプリケーションを基にデバイスを検索するための基準を設定できます：

- **アプリケーション名**

  アプリケーションを選択できるドロップダウンリスト。指定したアプリケーションがインストールされているデバイスが抽出に含まれます。

- **アプリケーションのバージョン**

選択したアプリケーションのバージョンを指定できる入力フィールド。

- **製造元**

  デバイスにインストールされているアプリケーションの製造元を選択できるドロップダウンリスト。

- **アプリケーションのステータス**

  アプリケーションのステータス（*インストール済み*、*未インストール*）を選択できるドロップダウンリスト。指定のアプリケーションがインストール済みまたは未インストールのデバイスが、選択したステータスに応じて抽出に含まれます。

- **アップデートによって検索**

  このオプションをオンにすると、該当するデバイスにインストールされているアプリケーションのアップデートに関する情報を使用して検索が実行されます。このチェックボックスをオンにすると、［**アプリケーション名**］、［**アプリケーションのバージョン**］、［**アプリケーションのステータス**］というフィールドがそれぞれ、［**アップデート名**］、［**アップデートのバージョン**］、［**ステータス**］に変わります。

  既定では、このオプションはオフです。

- **競合するセキュリティ製品**

  サードパーティのセキュリティ製品を選択できるドロップダウンリスト。指定したアプリケーションがインストールされているデバイスが、検索時に抽出に含まれます。

- **アプリケーションタグ**

  このドロップダウンリストでは、アプリケーションタグを選択できます。選択したタグが説明にあるアプリケーションをインストール済みのすべてのデバイスが、デバイスの抽出に含まれます。

- **指定したタグのないデバイスに適用する**

  このオプションをオンにすると、選択したタグがいずれも説明に含まれないデバイスが抽出に含まれます。

  このオプションをオフにすると、基準が適用されません。

  既定では、このオプションはオフです。

ハードウェアレジストリ

［**ハードウェアレジストリ**］セクションでは、取り付けたハードウェアを基にデバイスを抽出に含めるための基準を設定できます：

- **デバイス**

このドロップダウンリストでは、装置の種別を選択できます。その装置を備えたすべてのデバイスが検索結果に含まれます。

このフィールドでは全文検索が可能です。

- **製造元**

  このドロップダウンリストで、装置の製造元の名前を選択できます。その装置を備えたすべてのデバイスが検索結果に含まれます。

  このフィールドでは全文検索が可能です。

- **デバイス名**

  指定された名前のデバイスが抽出に含まれます。

- **説明**

  デバイスまたはハードウェア装置の説明。このフィールドで指定された説明が付けられたデバイスが抽出に含まれます。

  デバイスの説明は、そのデバイスのプロパティウィンドウにあらゆる形式で入力できます。このフィールドでは全文検索が可能です。

- **デバイスの製造元**

  デバイスの製造元の名前。このフィールドで指定された製造元のデバイスが抽出に含まれます。

  コンピューターの製造元名は、デバイスのプロパティウィンドウで入力できます。

- **シリアル番号**

  このフィールドで指定されたシリアル番号が付けられたすべてのハードウェアユニットが抽出に含まれます。

- **インベントリ番号**

  このフィールドで指定されたインベントリ番号が付けられた機器が抽出に含まれます。

- **ユーザー**

  このフィールドで指定されたユーザーのすべてのハードウェアユニットが抽出に含まれます。

- **場所**

  デバイスまたはハードウェアユニットの場所（本社、支社など）。このフィールドで指定された場所に導入されるコンピューターまたはその他のデバイスが抽出に含まれます。

  デバイスの場所は、そのデバイスのプロパティウィンドウにおいて、あらゆる形式で記載できます。

- **CPU の周波数(MHz)**

  CPU の周波数範囲。これらのフィールドで指定された CPU の周波数範囲に適合するデバイスが抽出に含まれます。

- **仮想 CPU コア**

  仮想 CPU コア数の範囲。これらのフィールドで指定された CPU の範囲に適合するデバイスが抽出に含まれます。

- **ハードディスク容量（GB）**

  デバイスのハードディスクの容量の範囲。これらの入力フィールドで指定されたハードディスクの容量の範囲に適合するデバイスが抽出に含まれます。

- **RAM サイズ（MB）**

  デバイスの RAM サイズの値の範囲。この範囲の値（指定した値を含む）のサイズの RAM を実装するデバイスが抽出に含まれます。

仮想マシン

［**仮想マシン**］セクションでは、仮想マシンであるか仮想デスクトップインフラストラクチャ（VDI）の一部であるかによってデバイスを抽出に含めるための基準を設定できます：

- **仮想マシン**

  このドロップダウンリストで、次のオプションを選択できます：

  - **判断しない**。
  - **いいえ**：仮想マシンでないデバイスを検索します。
  - **はい**仮想マシンであるデバイスを検索します。

- **仮想マシンの種別**

  このドロップダウンリストで、仮想マシンの製造元を選択できます。

  このドロップダウンリストは、［**仮想マシン**］の値が［**はい**］または［**判断しない**］である場合に使用できます。

- **仮想デスクトップインフラストラクチャの一部**

このドロップダウンリストで、次のオプションを選択できます：

- **判断しない**。
- **いいえ**：仮想デスクトップインフラストラクチャの一部でないデバイスを検索します。
- **はい**仮想デスクトップインフラストラクチャ（VDI）の一部であるデバイスを検索します。

ユーザー

［**ユーザー**］セクションでは、オペレーティングシステムにログインしたユーザーのアカウントを基にデバイスを抽出に含めるための基準を設定できます。

- **前回システムにログインしたユーザー**

  このオプションをオンにする場合は、［**参照**］をクリックしてユーザーアカウントを指定します。指定したユーザーがシステムの前回のログインを実行したデバイスが検索結果に含まれます。

- **少なくとも1回システムにログインしたユーザー**

  このオプションをオンにする場合は、［**参照**］をクリックしてユーザーアカウントを指定します。指定したユーザーがシステムに少なくとも1回ログインしたデバイスが検索結果に含まれます。

管理対象アプリケーションのステータスに影響がある問題

［**管理対象アプリケーションのステータスに影響がある問題**］セクションでは、管理対象アプリケーションで検知される可能性のある問題のリストを基にデバイスを抽出に含めるために使用する基準を設定できます：選択した問題のうち1つ以上の問題が存在するデバイスが抽出に含まれます複数のアプリケーションを対象とする問題については、同じ問題をすべてのアプリケーションのリストで自動的に選択するオプションがあります。

デバイスステータスの説明

管理対象アプリケーションからのステータスの説明に対応するチェックボックスをオンにできます。これらのステータスが受信されると、デバイスが抽出に含まれます。複数のアプリケーションを対象とするステータスについては、同じステータスをすべてのアプリケーションのリストで自動的に選択するオプションがあります。

管理対象アプリケーションのコンポーネントのステータス

［**管理対象アプリケーションのコンポーネントのステータス**］セクションでは、管理対象アプリケーションのコンポーネントのステータスを基にデバイスを抽出に含めるための基準を設定できます：

- **データ漏洩対策のステータス**

  データ漏洩対策のステータス（*デバイスからのデータなし*、*停止*、*開始中*、*一時停止*、*実行中*、*失敗*）を基にデバイスを検索します。

- **コラボレーションサーバーの保護ステータス**

  サーバーコラボレーションの保護ステータス（*デバイスからのデータなし*、*停止*、*開始中*、*一時停止*、*実行中*、*失敗*）を基にデバイスを検索します。

- **メールサーバーの保護ステータス**

  メールサーバーの保護のステータス（*デバイスからのデータなし*、*停止*、*開始中*、*一時停止*、*実行中*、*失敗*）を基にデバイスを検索します。

- **Endpoint Sensor のステータス**

  Endpoint Sensor のステータス（*デバイスからのデータなし*、*停止*、*開始中*、*一時停止*、*実行中*、*失敗*）を基にデバイスを検索します。

製品コンポーネント

このセクションでは、対応する管理プラグインが管理コンソールにインストールされているアプリケーションのコンポーネントのリストが表示されます。

［**製品コンポーネント**］セクションでは、選択したアプリケーションの管理下にあるコンポーネントのステータスとバージョン番号を基にデバイスを抽出に含めるための基準を設定できます：

- **ステータス**

  アプリケーションから管理サーバーに送信されたコンポーネントのステータスに基づいてデバイスを検索します。*デバイスからのデータなし*、*停止*、*開始中*、*一時停止*、*実行中*、*エラー*、*未インストール*のいずれかのステータスを選択できます。管理対象デバイスにインストールされたアプリケーションの選択したコンポーネントのステータスが指定したステータスと一致する場合、そのデバイスが抽出に含まれます。

  製品から送信されるステータス：

  - *開始中* - コンポーネントが利用開始プロセスを実行中です。
  - *実行中* - コンポーネントが有効で正常に動作しています。
  - *一時停止* - コンポーネントの動作が中断中です（例：管理対象製品でユーザーが保護を一時停止した）。
  - *エラー* - コンポーネントの動作中にエラーが発生しました。
  - *停止* - コンポーネントが無効で、現在動作していません。
  - *未インストール* - 製品のカスタムインストールの設定時に、ユーザーがコンポーネントをインストール対象として選択しませんでした。

  他のステータスとは異なり、［*デバイスからのデータなし*］ステータスはアプリケーションから送信されたものではありません。このステータスは、選択したコンポーネントのステータスについて、アプリケーションに情報がないことを示します。たとえば、デバイスにインストールされているアプリケーションのいずれにも選択したコンポーネントが属していない場合や、デバイスの電源がオフの場合などです。

- **バージョン**

  リストで選択したコンポーネントのバージョン番号に基づいてデバイスを検索します。`3.4.1.0` などのバージョン番号を入力し、選択したコンポーネントのバージョン番号がこれと「等しい」「それより古い」「それより新しい」かを指定できます。また、指定したバージョンを除くすべてのバージョンを検索するようにも設定できます。

API リファレンスガイド

この Kaspersky Security Center OpenAPI リファレンスガイドは、次のタスクを支援する目的で作成されています：

- 自動化とカスタマイズ。手動で扱う必要がないタスクを自動化できます。たとえば、管理者として Kaspersky Security Center OpenAPI を使用し、管理グループ構造の作成を支援するスクリプトを作成、実行することで、その構造の最新の状態を維持できます。
- カスタム開発。OpenAPI を使用して、クライアントアプリケーションを開発できます。

画面右側の検索フィールドを使用して OpenAPI リファレンスガイドから必要な情報を見つけることができます。

OPENAPI リファレンスガイド（英語）

スクリプトのサンプル

OpenAPI リファレンスガイドには、次の表に示す Python スクリプトのサンプルが含まれています。これらのサンプルは、OpenAPI メソッドを呼び出して、ネットワークを保護するための様々なタスクを自動的に実行する方法を示しています。たとえば、「プライマリ」と「セカンダリ」の階層の作成、Kaspersky Security Centerでのタスクの実行、ディストリビューションポイントの割り当てなどの方法です。サンプルをそのまま実行することも、サンプルを基に独自のスクリプトを作成することもできます。

OpenAPI メソッドを呼び出してスクリプトを実行するには：

1. KlAkOAPI.tar.gz アーカイブをダウンロードします。このアーカイブには、KlAkOAPI パッケージとサンプルが含まれています（アーカイブまたは OpenAPI リファレンスガイドからコピーできます）。
2. 管理サーバーがインストールされているデバイス上の KlAkOAPI.tar.gz アーカイブから KlAkOAPI パッケージをインストールします。

   OpenAPI メソッドを呼び出し、サンプルや独自のスクリプトを実行するのは、管理サーバーと KlAkOAPI パッケージがインストールされているデバイスでのみ実行できます。

ユーザーシナリオと Kaspersky Security Center OpenAPI メソッドのサンプルの一致

サンプル	サンプルの目的	シナリオ
KlAkParams のログ記録	`KlAkParams` データ構造を使用してデータを抽出、処理できます。サンプルには、このデータ構造の使用方法を示しています。 サンプル出力は、様々な方法で表示される場合があります。データを取得して HTTP メソッドを送信したり、自分のコードで使用したりできます。	監視とレポート
プライマリ / セカンダリ階層の作成と削除（英語）	管理サーバーをセカンダリ管理サーバーとして追加し、プライマリとセカンダリの階層を確立できます。または、セカンダリ管理サーバーを階層から切断することもできます。	管理サーバーの階層の作成、セカンダリ管理サーバーの追加、管理サーバーの階層の削除
接続ゲートウェイを使用してネットワークリストファイルを指定したホストにダウンロード	接続ゲートウェイを使用して、必要なデバイスでネットワークエージェントに接続できます。次に、ネットワークリストを含むファイルをデバイスにダウンロードします。	ディストリビューションポイントと接続ゲートウェイの調整

プライマリ管理サーバーリポジトリに保存されたライセンスキーのセカンダリ管理サーバーへのインストール	プライマリ管理サーバーに接続し、そこから必要なライセンスをダウンロードして、このライセンスを階層内のすべてのセカンダリ管理サーバーに送信できます。	管理対象アプリケーションのライセンスの管理
有効なユーザー権限のレポートの作成	様々なレポートを作成できます。たとえば、このサンプルを使用して、有効なユーザー権限のレポートを生成できます。このレポートでは、ユーザーのグループと役割に応じて、ユーザーが持つ権限について説明します。 レポートは、HTML、PDF、Excel 形式でダウンロードできます。	レポートの生成と表示
デバイスタスクの開始	接続ゲートウェイを使用して、必要なデバイスでネットワークエージェントに接続できます。次に必要なタスクを実行します。	タスクの手動での開始
デバイスのディストリビューションポイントのグループへの登録（英語）	管理対象デバイスをディストリビューションポイント（以前はアップデートエージェントと呼ばれていました）として割り当てることができます。	定義データベースとカスペルスキー製品のアップデート
すべてのグループの列挙（英語）	管理グループに対して、様々な処理を実行できます。サンプルでは、次の実行方法を例示しています： • ［管理対象デバイス］ルートグループの識別子の取得 • グループ階層の移動 • グループの完全な拡張階層を、名前とネスト構造とともに取得	管理サーバーの設定
タスクの列挙、タスクの統計のクエリ、タスクの実行（英語）	参照可能な情報は次の通りです： • タスクの進捗履歴 • 現在のタスクステータス • 様々なステータスのタスクの数 タスクの実行も可能です。既定では、サンプルは統計の出力後にタスクを実行します。	タスク実行の監視
タスクの作成と実行（英語）	タスクを作成できます。サンプルにある次のタスクパラメータを指定します： • 種別 • 実行方法 • 名前 • タスクが使用されるデバイスグループ 既定では、サンプルは「メッセージを表示する」種別のタスクを作成します。このタスクは、管理サーバーのすべての管理対象デバイスに対して実行できます。必要に応じて、タスクパラメータを独自に指定できます。	タスクの作成

ライセンスの列挙（英語）	管理サーバーが管理するデバイスにインストールされたカスペルスキー製品の、現在のライセンスがすべてリストされた一覧を取得できます。リストには、全ライセンスの詳細データ（名前、種別、有効期限日など）が含まれています。	使用中のライセンスに関する情報の表示
内部ユーザーの作成および検索（英語）	さらなる作業のためにアカウントを作成できます。	管理サーバーを開始するアカウントの選択
カスタムカテゴリの作成（英語）	必要なパラメータとともに、アプリケーションカテゴリを作成できます。	コンテンツが手動で追加されるアプリケーションカテゴリの作成
SrvView を使用したユーザーの列挙（英語）	SrvView クラスを使用して、管理サーバーからの詳細な情報をリクエストできます。たとえば、このサンプルを使用してユーザーのリストを取得できます。	ユーザーアカウントの管理

OpenAPI 経由で Kaspersky Security Center と連携するアプリケーション

一部のアプリケーションは、OpenAPI 経由で Kaspersky Security Center と連携します。Kaspersky Anti Targeted Attack Platform または Kaspersky Security for Virtualization などがこのようなアプリケーションに含まれます。また、OpenAPI に基づいて開発されたカスタムクライアントアプリケーションであることもあります。

OpenAPI 経由で Kaspersky Security Center と連携するアプリケーションは管理サービスに接続します。管理サーバーへの接続用に IP アドレスの許可リストを設定している場合は、Kaspersky Security Center の OpenAPI を使用するアプリケーションをインストールしているデバイスの IP アドレスを追加してください。使用しているアプリケーションが OpenAPI によって動作しているかどうかについては、そのアプリケーションのヘルプを参照してください。

Kaspersky Security Center 14 Web コンソールとその他のカスペルスキー製品の連携

このセクションでは、Kaspersky Security Center 14 Web コンソールから Kaspersky Endpoint Detection and Response や Kaspersky Managed Detection and Response など、別のカスペルスキー製品へのアクセスを設定する方法について説明します。

KATA / KEDR Web コンソールへのアクセスの設定

KATA（Kaspersky Anti Targeted Attack）と KEDR（Kaspersky Endpoint Detection and Response）は Kaspersky Anti Targeted Attack Platform を構成する 2 つのコンポーネントです。Kaspersky Anti Targeted Attack Platform 用の Web コンソール（KATA / KEDR Web コンソール）を使用して、KATA と KEDR を管理できます。Kaspersky Security Center 14 Web コンソールと KATA / KEDR Web コンソールの両方を使用している場合、Kaspersky Security Center 14 Web コンソールのインターフェイスから KATA / KEDR Web コンソールに直接移動できるようにリンクを設定できます。

KATA / KEDR Web コンソールへのアクセスを設定するには：

1. メインウィンドウの右上部にある［**コンソールの設定**］をクリックします。
2. ドロップダウンメニューから［**連携**］を選択します。
   ［コンソールの設定］ウィンドウが表示されます。
3. ［**連携**］タブの［**KATA / KEDR Web コンソールの URL**］で、KATA / KEDR Web コンソールの URL を入力します。
4. ［**保存**］をクリックします。

製品のメインウィンドウに［**高度な管理**］ドロップダウンリストが追加されます。このメニューを使用して KATA / KEDR Web コンソールに移動できます。［**次世代サイバーセキュリティ**］をクリックすると、ブラウザーの新しいタブが開き、指定した URL が表示されます。

バックグラウンド接続の確立

Kaspersky Security Center と Kaspersky Managed Detection and Response（MDR とも表記）など、その他のカスペルスキー製品またはソリューションとの間の連携を設定するには、Kaspersky Security Center 14 Web コンソールと管理サーバー間でバックグラウンド接続を確立する必要があります。使用中のアカウントに［**一般的な機能：ユーザー権限**］機能領域のオブジェクト ACL の変更権限がある場合のみ、この接続を確立することができます。

> 連携は、Kaspersky Managed Detection and Response と Windows ベースの Kaspersky Security Center 間でのみ設定できます。

バックグラウンド接続を確立するには：

1. ［**コンソールの設定**］ドロップダウンリストで、［**連携**］を選択します。
   コンソールの設定ウィンドウが表示されます。

2. ［**連携**］タブを選択します。

3. ［**連携**］タブで、［**連携**］を選択します。

4. バックグラウンド接続を確立する切り替えスイッチを使用して［**連携用のバックグラウンド接続の確立が［有効］です**］にします。

5. 表示された［**バックグラウンド接続を確立するサービスが、Kaspersky Security Center Web コンソールサーバーで開始されます**］セクションで、［**OK**］をクリックします。

Kaspersky Security Center 14 Web コンソールと管理サーバーのバックグラウンド接続が確立されました。管理サーバーはバックグラウンド接続用のアカウントを作成し、このアカウントは Kaspersky Security Center と別のカスペルスキー製品またはソリューション間での連携を管理するサービスアカウントとして使用されます。このサービスアカウントの名前には NWCSvcUser プレフィックスが含まれます。セキュリティの理由から、管理サーバーはサービスアカウントのパスワードを 30 日ごとに自動で変更します。サービスアカウントは手動で削除できません。管理サーバーは、サービス連携接続を無効にした際にこのアカウントを自動で削除します。管理サーバーは、それぞれの Kaspersky Security Center 14 Web コンソールと管理コンソールに対して単一のサービスアカウントを作成し、すべてのサービスアカウントを「ServiceNwcGroup」という名前のセキュリティグループに割り当てます。管理サーバーはこのセキュリティグループを Kaspersky Security Center のインストールプロセス中に自動で作成します。このセキュリティグループは手動で削除できません。

テクニカルサポートへの問い合わせ

このセクションでは、サポートを受ける方法および提供条件について説明します。

テクニカルサポートのご利用方法

Kaspersky Security Center Linux のドキュメントや Kaspersky Security Center Linux の情報源で問題のソリューションが見つからない場合、カスペルスキーのテクニカルサポートに問い合わせてください。テクニカルサポート担当者が、Kaspersky Security Center Linux のインストール方法や使用方法についてのお問い合わせに回答いたします。

カスペルスキーによる Kaspersky Security Center Linux のサポートは、本製品のライフサイクル期間中に提供されます（製品のサポートライフサイクルページを参照）。テクニカルサポートに連絡する前に、サポートサービス規約をご確認ください。

テクニカルサポートサービスの内容については、サポートセンターのご案内を参照してください。

- テクニカルサポートサイトにアクセスする
- カスペルスキーカンパニーアカウントからテクニカルサポートへリクエストを送信

カスペルスキーカンパニーアカウントによるテクニカルサポート

カスペルスキーカンパニーアカウントは、カスペルスキー製品を使用する法人向けのポータルです。このポータルは、オンラインリクエストを通じてユーザーとカスペルスキーのエキスパートの交流を促進するよう設計されています。また、オンラインリクエストの進捗をモニターでき、リクエストの履歴を保存することができます。

カスペルスキーカンパニーアカウントでは、シングルアカウントで組織の全従業員を登録できます。シングルアカウントによって、登録従業員からカスペルスキーまでのオンラインリクエストを一元管理でき、カスペルスキーカンパニーアカウントを介して従業員の権限を管理することもできます。

カスペルスキーカンパニーアカウントのポータルは、次の言語で利用できます：

- 英語
- スペイン語
- イタリア語
- ドイツ語
- ポーランド語
- ポルトガル語
- ロシア語
- フランス語

- 日本語

カスペルスキーカンパニーアカウントについて詳しくは、テクニカルサポートサイトをご覧ください。

製品の情報源

カスペルスキーの Web サイトの Kaspersky Security Center のページ

カスペルスキー Web サイトの Kaspersky Security Center のページで、本製品と機能、使用に関する一般的な情報を確認できます。

ナレッジベースの Kaspersky Security Center のページ

カスペルスキーのテクニカルサポートサイトに*ナレッジベース*のセクションがあります。

ナレッジベースの Kaspersky Security Center Linux のページに、製品の購入、インストール、使用の方法について、役立つ情報、推奨事項、および FAQ への回答が掲載されています。

ナレッジベースの記事では、本製品だけではなく他のカスペルスキー製品に関連した質問にも回答しています。ナレッジベースの記事に、テクニカルサポートからのニュースが掲載されることもあります。

カスペルスキー製品の Web コミュニティの利用

特に緊急の対応が必要ではない場合は、カスペルスキーのフォーラムをご利用ください。ここでは、カスペルスキーのエキスパートやカスペルスキー製品のユーザーが、様々なトピックで意見交換しています。

フォーラムでは、これまでに公開されたトピックの閲覧、コメントの書き込み、新しいトピックの作成が可能です。

> オンラインの情報源を使用するには、インターネット接続が必要です。

問題の解決策が見つからない場合は、カスペルスキーのテクニカルサポートまでお問い合わせください。

既知の問題

Kaspersky Security Center Linux には、本製品の動作には大きな影響を与えない複数の制限があります：

- リストに 20 を超えるアイテムが含まれている場合（この場合、アイテムは複数のページに表示されます）、［**すべて選択**］をオンにすると、Web コンソールは現在のページに表示されているアイテムのみを抽出します。

- ［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクおよび［*ディストリビューションポイントのリポジトリにアップデートをダウンロード*］タスクで、パスワード保護されたローカルフォルダーまたはネットワークフォルダーをアップデート元として選択した場合はユーザー認証が動作しません。この問題を解決するには、最初にパスワード保護されたフォルダーをマウントしてから、オペレーティングシステムを使用するなどして必要な資格情報を指定します。この後、アップデートのダウンロードタスクでこのフォルダーをアップデート元として選択することができます。Kaspersky Security Center は資格情報の入力を求めません。

- タスクのスケジュールでオプション［**即時**］を選択して変更を保存した後に*管理サーバーの変更*タスクが自動で開始されません。

- 別のブラウザーで Kaspersky Security Center 14 Web コンソールを開いて、管理サーバーの証明書ファイルを管理サーバーのプロパティウィンドウでダウンロードすると、ダウンロードされたファイルに異なる名前が付与されます。

- **バックアップ**リポジトリ（［**操作**］→［**リポジトリ**］→［**バックアップ**］）からオブジェクトを復元しようとする、もしくはオブジェクトをカスペルスキーに送信しようとするとエラーが発生します。

- Kaspersky Endpoint Security for Linux の親ポリシーでロックされた設定は子ポリシーに継承されますが、子ポリシーではロックされません。

- 管理対象デバイスから管理サーバーに送信されたハードウェアの情報の内容が不完全になる場合があります。一部のハードウェア項目が指定されていないことがあります。

- Kaspersky Endpoint Security for Linux のアプリケーションコントロール機能に追加したアプリケーションカテゴリが削除されることがあります。

- 1つ以上のネットワークアダプターを持つ管理対象デバイスが管理サーバーにネットワークアダプターの MAC アドレスに関する情報を送信する際、管理サーバーへの接続に使用されていないものの情報を送信することがあります。

- Kaspersky Security Center 14 Web コンソールのインストール用の応答ファイル内で webConsoleAccount および managementServiceAccount パラメータにカスタムユーザーアカウントを指定しており、これらのアカウントが異なるセキュリティグループに属する場合、インストール後に Kaspersky Security Center 14 Web コンソールは動作しなくなります。

- Astra Linux 64 ビットエディションでは、klnagent-astra パッケージを klnagent64_14 パッケージでアップグレードすることはできません。古いパッケージの klnagent64-astra は削除され、アップグレードの代わりに新しいパッケージ klnagent64 がインストールされます。そのため、デバイスに klnagent64_14 パッケージの新しいアイコンが追加されます。このデバイスの古いアイコンは削除できます。

HTTPS

データ転送用のセキュアプロトコル。ブラウザーと Web サーバーの通信に暗号を使用します。HTTPS は、企業データや財務データなどの制限付き情報へのアクセスに使用されます。

JavaScript

Web ページのパフォーマンスを拡張するプログラミング言語。JavaScript を使用して作成された Web ページでは、Web サーバーからの新しいデータでブラウザーの表示をアップデートすることなく、インターフェイス要素の表示を変更したり、新しいウィンドウを表示したりできます。JavaScript を使用して作成されたページを表示するには、ブラウザーの設定で JavaScript のサポートを有効にします。

Kaspersky Private Security Network（KPSN）

Kaspersky Private Security Network は、カスペルスキー製品がインストールされたデバイスのユーザーがデバイスから Kaspersky Security Network にデータを送信することなく、Kaspersky Security Network の評価データベースとその他の統計データにアクセスできるようにするソリューションです。Kaspersky Private Security Network は、次のいずれかの理由で Kaspersky Security Network にアクセスできない法人ユーザーの方を対象として開発されています：

- デバイスがインターネットに接続されていない。
- 国外や企業 LAN の外へのデータの送信が、法律または社内のセキュリティポリシーで禁止されている。

Kaspersky Security Center 管理者

Kaspersky Security Center システムを使用して、アプリケーションの動作をリモートで一元管理する担当者。

Kaspersky Security Center Web サーバー

管理サーバーとともにインストールされる Kaspersky Security Center のコンポーネントの 1 つ。Web サーバーは、スタンドアロンインストールパッケージ、iOS MDM プロファイル、および共有フォルダーのファイルをネットワーク上で伝送できるように設計されています。

Kaspersky Security Center オペレーター

Kaspersky Security Center システムで管理している保護システムのステータスと動作を監視するユーザー。

Kaspersky Security Center システム正常性検証ツール（SHV）

Kaspersky Security Center のコンポーネントの1つで、Kaspersky Security Center と Microsoft NAP を同時運用している場合のオペレーティングシステムの操作性をチェックします。

SSL

インターネットおよびローカルネットワークで使用されるデータ暗号化プロトコル。Secure Sockets Layer（SSL）は Web アプリケーションで使用され、クライアントとサーバーの間のセキュアな接続を確立します。

アップデート

カスペルスキーのアップデートサーバーから取得した新しいファイル（定義データベースまたはソフトウェアモジュール）を置換または追加する処理。

アプリケーションの一元管理

Kaspersky Security Center が備える管理サービスを使用した、アプリケーションのリモート管理。

アプリケーションの直接管理

ローカルインターフェイスを使用したアプリケーション管理。

アプリストア

Kaspersky Security Center のコンポーネント。アプリストアを使用すると、Android デバイスの所有者が自分でアプリケーションをインストールできます。アプリストアでは、アプリケーションの APK ファイルや Google Play のリンクを公開できます。

アンチウイルスサービスプロバイダー

クライアント組織にカスペルスキー製品に基づくアンチウイルスサービスを提供する組織。

イベントの重要度

カスペルスキー製品の動作時に発生したイベントのプロパティ。次のレベルに分かれています：

- 緊急
- 機能エラー
- 警告

- 情報

イベント発生の状況によって、同じ種別のイベントで重要度が異なる場合があります。

イベントリポジトリ

管理サーバーデータベースのうち、Kaspersky Security Center Linux で発生するイベントに関する情報の保管専用の領域です。

インストールパッケージ

カスペルスキー製品のリモートインストール用に作成されるファイルセット。リモート管理システム Kaspersky Security Center を使用して作成します。インストールパッケージには、アプリケーションをインストールし、インストール後にすぐに実行させるのに必要な設定の範囲が含まれます。設定は、アプリケーションの既定値になります。インストールパッケージは、配布キットに含まれる拡張子が kpd および kud のファイルを使用して作成されます。

カスペルスキーのアップデートサーバー

カスペルスキーの HTTP サーバーで、カスペルスキー製品はこれらのサーバーから定義データベースやソフトウェアモジュールのアップデートをダウンロードします。

仮想管理サーバー

クライアント組織のネットワークの保護システムを管理する Kaspersky Security Center のコンポーネント。

仮想管理サーバーは特殊なセカンダリ管理サーバーであり、物理管理サーバーと比較すると、次の制限があります：

- 仮想管理サーバーは、プライマリ管理サーバー上にのみ作成できます。
- 仮想管理サーバーは、プライマリ管理サーバーのデータベースを使用します。仮想管理サーバーではデータのバックアップと復元タスク、およびアップデートのスキャンとダウンロードタスクはサポートされていません。
- 仮想サーバーでは、セカンダリ管理サーバー（仮想サーバーを含む）の作成がサポートされていません。

管理グループ

機能およびインストールされているカスペルスキー製品に応じてデバイスをまとめたグループ。複数のデバイスを1つのグループとして管理できます。1つのグループに下位のグループとして他のグループを含めることができます。グループにインストールされている各アプリケーションに対してグループポリシーやグループタスクを作成することができます。

管理コンソール

Windows ベースの Kaspersky Security Center（別名「MMC ベースの管理コンソール」）のコンポーネント。このコンポーネントは、管理サーバーとネットワークエージェントの管理サービスに対してユーザーインターフェイスを提供します。管理コンソールは、 Kaspersky Security Center 14 Web コンソールに類似しています。

管理コンピューター

Kaspersky Security Center 14 Web コンソールを開いたデバイス。このコンポーネントにより、Kaspersky Security Center の管理に使用できるインターフェイスが提供されます。

管理コンピューターは、Kaspersky Security Center のサーバー部分の設定と管理に使用されます。管理コンピューターを使用して、カスペルスキー製品に基づいて一元化されたアンチウイルスによる企業内 LAN の保護を構築および管理します。

管理サーバー

企業ネットワークにインストールされているすべてのカスペルスキー製品に関する情報を一元的に保管する Kaspersky Security Center のコンポーネント。製品の管理にも使用できます。

管理サーバークライアント（クライアントデバイス）

ネットワークエージェントがインストールされ管理対象のカスペルスキー製品が実行されているデバイス、サーバー、またはワークステーション。

管理サーバー証明書

管理サーバーが次の目的で使用する証明書：

- Kaspersky Security Center 14 Web コンソールへの接続時における管理サーバーの認証
- 管理対象デバイスでの管理サーバーとネットワークエージェントとの安全な連携
- プライマリ管理サーバーをセカンダリ管理サーバーに接続する際の管理サーバーの認証

証明書は、管理サーバーをインストールすると自動的に作成され、管理サーバーに保存されます。

管理サーバーデータのバックアップ

管理サーバーのデータをバックアップし、後でバックアップユーティリティを使用して復元できるようにコピーすること。ユーティリティで保存できるデータは次の通りです：

- 管理サーバーのデータベース（管理サーバーに保存されているポリシー、タスク、アプリケーション設定、イベント）
- 管理グループとクライアントデバイスの構造についての設定情報
- アプリケーションリモートインストール用のインストールファイルのリポジトリ（フォルダーの内容としては、Packages と Uninstall Updates が含まれます）
- 管理サーバー証明書

管理サーバーデータの復元

バックアップユーティリティを使用して、バックアップに保存されている情報から管理サーバーデータを復元すること。ユーティリティで復元できるデータは次の通りです：

- 管理サーバーのデータベース（管理サーバーに保存されているポリシー、タスク、アプリケーション設定、イベント）
- 管理グループとクライアントコンピューターの構造についての設定情報
- アプリケーションリモートインストール用のインストールファイルのリポジトリ（フォルダーの内容としては、Packages と Uninstall Updates が含まれます）
- 管理サーバー証明書

管理者権限

Exchange 組織内の Exchange オブジェクトの管理に必要な、ユーザー権限および特権のレベル。

管理対象デバイス

管理グループに含まれる企業ネットワークデバイス。

共有証明書

ユーザーのモバイルデバイスを識別することを目的とした証明書。

クライアント管理者

クライアント組織のスタッフ。アンチウイルスのステータスを監視します。

グループタスク

管理グループに定義され、そのグループ内のすべてのクライアントデバイスで実行されるタスク。

現在のライセンス

アプリケーションによって現在使用されているライセンス。

互換性がないアプリケーション

サードパーティ製のアンチウイルス製品、または Kaspersky Security Center Linux を使用した管理に対応していないカスペルスキー製品。

サービスプロバイダーの管理者

アンチウイルスサービスプロバイダーのスタッフ。サービスプロバイダーの管理者は、カスペルスキー製品に基づき、アンチウイルスシステムをインストールおよび管理し、テクニカルサポートを顧客に提供します。

手動インストール

配布パッケージからの、企業ネットワーク上のデバイスへのセキュリティ製品のインストール。手動インストールには、管理者または別の IT スペシャリストの参加が必要です。通常、手動インストールは、リモートインストールでエラーが発生した場合に行います。

接続ゲートウェイ

*接続ゲートウェイ*は、特別なモードで動作するネットワークエージェントです。接続ゲートウェイは、他のネットワークエージェントからの接続を受け入れ、サーバーとの独自の接続を介してそれらを管理サーバーにトンネリングします。通常のネットワークエージェントとは異なり、接続ゲートウェイは、管理サーバーへの接続を確立するのではなく、管理サーバーからの接続を待機します。

設定プロファイル

iOS MDM モバイルデバイスの設定と制限事項に関するポリシー。

タスク

カスペルスキー製品によって実行される機能はタスクとして実装されます。ファイルのリアルタイム保護、デバイスの完全スキャン、定義データベースのアップデートなどのタスクがあります。

タスク設定

各タスク種別に固有のアプリケーション設定です。

追加の定額制サービスのライセンス

製品を使用する権限を認定する、現在使用されていないライセンス。

定義データベース

定義データベースの公開時点で、カスペルスキーが把握しているコンピューターセキュリティへの脅威についての情報を含むデータベース。定義データベース内のエントリによって、スキャンしているオブジェクトで悪意のあるコードを検知できます。定義データベースはカスペルスキーのエキスパートにより作成され、1時間ごとにアップデートされます。

ディストリビューションポイント

ネットワークエージェントがインストールされており、アップデートの配信やアプリケーションのリモートインストール、管理グループやブロードキャストドメインでのコンピューター情報の取得に使用されるコンピューター。ディストリビューションポイントは、アップデート配信時の管理サーバーの負荷軽減およびネットワークトラフィックの最適化の目的で設計されています。ディストリビューションポイントは、管理サーバーによって自動的に、または管理者によって手動で割り当てられます。ディストリビューションポイントは、以前のバージョンの製品ではアップデートエージェントという名称でした。

適用可能なアップデート

カスペルスキーのソフトウェアモジュールに関する一連のアップデート（一定期間に蓄積された重大なアップデート、アプリケーションのアーキテクチャへの変更を含む）

デバイスの所有者

デバイスで特定の操作が必要になった際に管理者が連絡できるユーザー。

特定のデバイスに対するタスク

任意の管理グループに属する一連のクライアントデバイスに割り当てられ、それらのデバイスで実行されるタスク。

内部ユーザー

内部ユーザーのアカウントは、仮想管理サーバーを操作するために使用します。Kaspersky Security Center によって、実際のユーザーの権限がアプリケーションの内部ユーザーに付与されます。

内部ユーザーのアカウントは、Kaspersky Security Center 内でのみ作成および使用されます。内部ユーザーに関するデータは、オペレーティングシステムには送信されません。Kaspersky Security Center が内部ユーザーを認証します。

認証エージェント

起動可能なハードディスクの暗号化後に、暗号化されたハードディスクへのアクセス権を取得してオペレーティングシステムを読み込むための認証手順を完了することができるインターフェイス。

ネットワークエージェント

管理サーバーと特定のネットワークノード（ワークステーションまたはサーバー）にインストールされているカスペルスキー製品との間のやり取りを受け持つ Kaspersky Security Center のコンポーネント。このコンポーネントは、カスペルスキーの Microsoft® Windows® 用の製品に共通した機能です。Unix 系の OS および macOS 用には、それぞれ異なるバージョンのネットワークエージェントがあります。

ネットワークのアンチウイルスによる保護

組織のネットワークにウイルスやスパムが侵入する危険性を軽減し、ネットワーク攻撃やフィッシングなどの脅威を防ぐ一連の技術的、組織的対策。ネットワークセキュリティは、セキュリティ製品およびサービスを使用して企業のセキュリティポリシーに従い、正しく適用することで向上します。

ネットワーク保護ステータス

企業ネットワーク内のデバイスのセキュリティレベルを定義する現在の保護ステータス。ネットワーク保護ステータスには、インストール済みセキュリティ製品、ライセンスの使用、検知された脅威の数と種類のような要因を含みます。

バックアップフォルダー

管理サーバーデータのコピーを保管するための特別なフォルダー。バックアップユーティリティによって作成されます。

非武装地帯（DMZ）

非武装地帯は、サーバーを含むローカルネットワークのセグメントで、グローバル Web からの要求に応えます。組織のローカルネットワークのセキュリティを確保するために、非武装地帯から LAN へのアクセスがファイアウォールで保護されます。

復元

隔離またはバックアップ内のオブジェクトを、隔離、感染駆除、削除される前の元のフォルダーまたはユーザーが指定したフォルダーに移動すること。

ブロードキャストドメイン

OSI 基本参照モデル（Open Systems Interconnection Basic Refernce Model）のレベルにおける、ブロードキャストチャネルを使用してすべてのノードがデータ交換を行えるネットワークの論理領域。

プログラム設定

あらゆる種類のタスクに共通していて、アプリケーションの動作全体を管理するアプリケーション設定（アプリケーションパフォーマンス設定、レポート設定、バックアップ設定など）。

プロビジョニングプロファイル

iOS モバイルデバイスでのアプリケーションの動作に関する設定の集まり。プロビジョニングプロファイルには、ライセンスに関する情報が書き込まれています。このプロファイルは、特定のアプリケーションにリンクされています。

プロファイル

Exchange モバイルデバイス に関する一連の設定。Microsoft Exchange サーバーへの接続時の動作を定義します。

ホーム管理サーバー

ネットワークエージェントのインストール中に指定した管理サーバー。ホーム管理サーバーは、ネットワークエージェントの接続プロファイルを設定するために使用できます。

保護ステータス

コンピューターのセキュリティレベルを定義する現在の保護ステータス。

ポリシー

ポリシーは、アプリケーションの設定を決定するとともに、管理グループ内のコンピューターにインストールされたアプリケーションを設定する権限を管理します。各アプリケーションについて個別にポリシーを作成する必要があります。各管理グループのコンピューターにインストールされたアプリケーションについて複数のポリシーを作成できますが、各管理グループ内で1つのアプリケーションについて一度に適用されるポリシーは1つだけです。

ライセンス情報ファイル

拡張子が「KEY」のファイル。このファイルを使用することで、カスペルスキー製品を試用版または製品版ライセンスで使用できます。

ライセンス認証済みアプリケーショングループ

管理者が設定した基準（製造元別など）に基づいて作成されるアプリケーションのグループ。クライアントデバイスへのインストールのグループごとの統計情報が保持されます。

ライセンスの有効期間

ユーザーがアプリケーションの機能および追加サービスへのアクセス権を有する期間。使用できるサービスは、ライセンスの種別によって異なります。

リモートインストール

Kaspersky Security Center Linux を使用した、カスペルスキー製品のインストール。

ローカルインストール

組織のネットワーク上のデバイスにセキュリティ製品をインストールするには、セキュリティ製品の配布パッケージからインストールを手動で開始する方法、またはコンピューターに事前にダウンロードしておいた公開済みインストールパッケージを手動で起動する方法があります。

ローカルタスク

1台のクライアントコンピューターを対象として定義、実行されるタスク。

ロールグループ

同一の管理者権限を許可されている、Exchange ActiveSync モバイルデバイスユーザーのグループ。

サードパーティ製のコードに関する情報

サードパーティのコードに関する情報は、ファイル legal_notices.txt に記載され、カスペルスキー製品のインストールディレクトリに保存されています。

商標に関する通知

登録商標とサービスマークに関する権利は各所有者に帰属します。

Adobe、Acrobat、Flash、Shockwave、PostScript は、Adobe の米国および他の国における登録商標または商標です。

AMD、AMD64 は、Advanced Micro Devices, Inc. の商標または登録商標です。

Amazon、Amazon Web Services、AWS、Amazon EC2、AWS Marketplace は、Amazon.com, Inc. またはその関連会社の商標です。

Apache および Apache の羽根のロゴは、Apache Software Foundation が所有する商標です。

AirPlay、AirDrop、AirPrint、App Store、Apple、Apple Configurator、AppleScript、FaceTime、FileVault、iBook、iBooks、iCloud、iPad、iPhone、iTunes、Leopard、macOS、Mac、Mac OS、OS X、Safari、Snow Leopard、Tiger、QuickTime、Touch ID は、Apple Inc. の商標です。

Arm は、Arm Limited（またはその子会社）の米国および / またはその他の国における登録商標です。

Bluetooth の表記、マークおよびロゴは、Bluetooth SIG, Inc. に所有権があります。

Ubuntu LTS は Canonical Ltd の登録商標です。

Cisco、Cisco Systems、IOS は、米国およびその他の国における Cisco Systems, Inc. およびその子会社の登録商標です。

Citrix および XenServer は、米国特許商標庁およびその他の国における Citrix Systems, Inc. およびその子会社の登録商標です。

Corel は、カナダ、米国およびその他の国における Corel Corporation およびその子会社の商標または登録商標です。

Cloudflare、Cloudflare のロゴ、および Cloudflare Workers は、米国およびその他の法域における Cloudflare, Inc. の商標や登録商標です。

Dropbox は、Dropbox, Inc. の商標です。

Firebird は、Firebird Foundation の登録商標です。

Foxit は、Foxit Corporation の登録商標です。

FreeBSD は、FreeBSD Foundation の登録商標です。

Google、Android、Chrome、Chromium、Dalvik、Firebase、Google Chrome、Google Earth、Google Play、Google Maps、Google Public DNS、Hangouts、YouTube は、Google LLC の商標です。

EulerOS、FusionCompute、FusionSphere は、Huawei Technologies Co., Ltd. の商標です。

Intel、Core、Xeon は米国およびその他の国における Intel Corporation の商標です。

IBM および QRadar は、世界各国で International Business Machines Corporation が所有する登録商標です。

Node.js は Joyent Inc. の商標です。

Linux は、米国およびその他の国における Linus Torvalds 氏の登録商標です。

Microsoft、Active Directory、ActiveSync、BitLocker、Excel、Forefront、Internet Explorer、InfoPath、Hyper-V、Microsoft Edge、MultiPoint、MS-DOS、PowerShell、PowerPoint、SharePoint、SQL Server、OneNote、Outlook、Skype、Tahoma、Visio、Win32、Windows、Windows PowerShell、Windows Media、Windows Server、Windows Phone、Windows Vista、Windows Azure は、Microsoft グループ企業が所有する商標です。

Mozilla、Firefox、Thunderbird は、米国およびその他の国における Mozilla Foundation の商標です。

Novell は、米国およびその他の国における Novell Enterprises Inc. の登録商標です。

Oracle、Java、JavaScript、TouchDown は、Oracle とその関連会社の両方またはいずれかの登録商標です。

Parallels、Parallels ロゴ、および Coherence は、Parallels International GmbH の商標または登録商標です。

Chef は、Progress Software Corporation およびその子会社または関連会社の、米国およびその他の国における商標または登録商標です。

Puppet は、Puppet, Inc. の商標または登録商標です。

Python は Python Software Foundation の登録商標または商標です。

Red Hat、CentOS、Fedora、Red Hat Enterprise Linux は、Red Hat, Inc. またはその子会社の米国および他の国における商標または登録商標です。

Ansible は、米国およびその他の国における Red Hat, Inc. の登録商標です。

CentOS は、Red Hat, Inc. またはその子会社の米国および他の国における商標または登録商標です。

BlackBerry は、Research In Motion Limited の米国における登録商標であり、その他の国における登録商標または登録出願中の商標です。

Debian は、Software in the Public Interest, Inc. の登録商標です。

Splunk、SPL は、Splunk, Inc. の米国およびその他の国における登録商標です。

SUSE は、米国およびその他の国における SUSE LLC の登録商標です。

Symbian の商標は Symbian Foundation Ltd. が所有します。

OpenAPI は、Linux Foundation の登録商標です。

VMware、VMware vSphere、VMware Workstation は、VMware, Inc. の米国およびその他の国における商標または登録商標です。

UNIX は米国およびその他の国における登録商標で、X/Open Company Limited のライセンス契約の下で排他的に使用されています。

Zabbix は Zabbix SIA の登録商標です。