Kaspersky Vulnerability and Patch Management

複雑な脆弱性の管理を自動化し、セキュリティシステムを最新の状態で保護

特長

- 脆弱性の検知と優先順位付けの自動化
- 150 種類以上のアプリケーションから提供されるパッチやアップデートの自動配信
- パッチのテストモードのサポート
- パッチのスケジュール配信
- トラフィック量の最適化
- 脆弱性監視とレポート
- 多機能なクライアント管理ツール
- ソフトウェアのリモートインストールとトラブルシューティング
- オペレーティングシステムの自動導入

アプリケーションの脆弱性に対しパッチが適用されていない状態は、企業の IT セキュリティにとって大きな脅威となります。また、問題になるのは脆弱性を悪用したゼロディ攻撃による脅威だけではありません。IT インフラストラクチャが複雑化することで、脆弱性のあるソフトウェアを迅速に修正する作業がさらに複雑化し、対応に多くの時間を必要とします。脆弱性を正確に把握せずして、脅威から保護することはできません。

常時潜在的な脆弱性を監視しながらソフトウェアのアップデートを管理することは、IT 部門が直面している最も重要な課題で、中でもパッチ適用は多くの作業工数を必要とする管理業務のひとつです。Kaspersky Vulnerability and PatchManagement は、脆弱性情報の収集と検知、パッチおよびアップデートの自動配信、IT 資産管理、アプリケーションの運用などに必要なセキュリティ、設定、管理タスクを一元管理し、一連の作業を自動化することで、脆弱性管理に要する作業時間を短縮し、さらに高度なセキュリティシステムの運用を実現します。

完全なシステムの可視化

単一の管理コンソールからネットワーク全体を可視化することで、ネットワーク上のアプリケーションとデバイスの状況を適切に把握できます。IT ポリシーおよびコンプライアンスの要件に沿って、組織のデータやアプリケーションにアクセスするユーザーおよびデバイスを一元管理できます。

セキュリティの強化

自動化されたパッチ適用とアップデートによって IT セキュリティを強化し、定型的なタスクの作業工数を削減します。

Kaspersky Vulnerability and Patch Management でシステム全体を可視化でき、システム管理者は業務を安全に遂行するための対策に必要な情報を正確に把握できます。脆弱性の検知と優先順位付け、パッチとアップデートのダウンロード、テストと配信、タスクの実行監視とレポートを含む脆弱性監査からパッチ適用の作業工程全体を自動化することで、運用効率を高め、管理業務の作業負荷を大幅に軽減します。

IT タスクの効率化

Kaspersky Vulnerability and Patch Management は、IT 管理機能を自動化するクライアント管理ツールを提供します。アプリケーションのプロビジョニング自動化、リモートから利用者の操作を監査またはトラブルシューティング、新しいコンピューターのセットアップと新しいアプリケーションの導入に要する作業工数を削減します。

一元管理

Kaspersky Vulnerability and Patch Management は Kaspersky Security Center で提供される管理コンポーネントのひとつです。一元化された管理コンソールで直感的で操作しやすい管理用のユーザーインターフェイスで効率的に各機能を設定、定型的な IT タスクを自動化することで作業効率が向上します。

脆弱性監査とパッチ管理

ネットワーク上のデバイスおよびソフトウェア情報を検出し、ハードウェアおよびソフトウェアのインベントリを作成

脆弱性の自動検出およびハードウェアとソフトウェア情報の自動収集によって、システム管理者は企業ネットワークで利用されているすべての IT 資産を詳細に把握できます。自動的にソフトウェア情報をスキャンすることで、セキュリティのリスクがありアップデートが必要な可能性のあるソフトウェアを迅速に自動検出します。

脆弱性の検知と優先順位付け

脆弱性スキャンの自動化によって脆弱性を迅速に検知、優先順位付けおよび修復まで自動的に実行でき、スケジュール機能を利用して任意の時間に実行させることもできます。柔軟にポリシーを設定できる管理機能を利用することで、アップデートされた互換性のあるソフトウェアの配信や例外処理も設定できます。

パッチとアップデートのダウンロード、テスト、配信

パッチとアップデートは、Kaspersky Labが管理しているサーバーから自動的にダウンロードすることができます。配信する前に動作上問題がないかテストして、システムのパフォーマンスや利用者の作業に影響しないことを確認できます。パッチとアップデートは、手動また任意に設定した時間に実行できます。

タスクの実行監視と脆弱性レポートの実行

Kaspersky Vulnerability and Patch Management はシステム管理者にパッチのインストール状況を通知し、管理者が脆弱性スキャンに関するレポートの作成、潜在的な脆弱性の検索、変更の監視、組織全体の IT セキュリティや、企業ネットワーク上のすべてのデバイスとシステムに関する情報を自動的に収集します。

効率的なソフトウェア配信

リモートから単一の管理コンソールを利用してソフトウェアの導入およびアップデートできます。Kaspersky Labのデータベースには一般に広く普及している150種類以上のアプリケーションの情報も蓄積されているため、自動的にインストール、または必要に応じて任意に設定した時間にインストールすることもできます。ローカルサイト側のソフトウェア配信向けマルチキャスト技術を利用することで、リモートサイト側のネットワーク通信の負荷を低減できます。

クライアント管理ツール

リモートからのトラブルシューティング

問題解決時間の短縮、作業効率の向上、リモートからの効率的なサポート業務を遂行するために、Kaspersky Security Center は リモートデスクトッププロトコルおよびWindows デスクトップ共有技術（Windows リモートアシスタンスで使用されている技術と同様）を使用します。管理対象のコンピューターでTCPポートやUDPポートが利用不可の状態であっても、管理者はネットワークエージェントを利用して管理対象のコンピューターにリモートから接続でき、コンピューターに保存されているデータやインストールされているアプリケーションにアクセスできます。認証メカニズムによって不正な遠隔操作を防止したり、またリモートから実行されたすべての操作履歴を記録できるため、記録した情報を不正利用の監視や監査に活用することもできます。

オペレーティングシステムの導入

Kaspersky Vulnerability and Patch Management は、保護されたシステムイメージの作成、保存、クローンの作成を自動化し、一元的に管理します。また、新しいコンピューターへオペレーティングシステム（OS）の導入や再インストールすることもできます。すべてのOSイメージは特別に保護されたインベントリに格納され、導入する際にそのインベントリにアクセスします。コンピューターイメージの導入は、PXE サーバーか、Kaspersky Vulnerability and Patch Management のタスクを使用して行うことができます。PXE（Preboot eXecution Environment）サーバーは、OS が導入されていない新しいコンピューターにも適用できます。Kaspersky Vulnerability and Patch Management の タスクは、OS イメージを管理対象コンピューターに導入する際に使用されます。Wake on LAN シグナルをクライアントコンピューターに送信することで、任意に設定した時間に OS イメージを自動配信できます。また、UEFI（Unified Extensible Firmware Interface）搭載したコンピューターもサポートします。

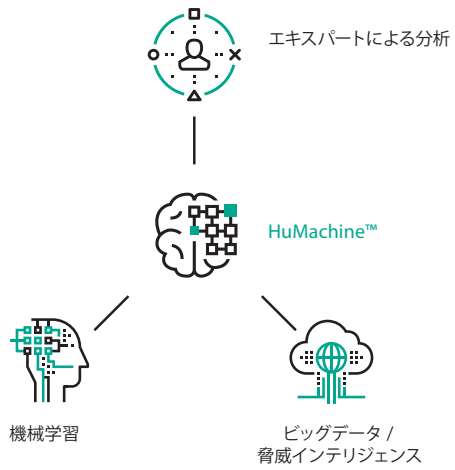
Kaspersky Vulnerability and Patch Management は、以下のライセンスに含まれます。

- Kaspersky Endpoint Security for Business Advanced
- Kaspersky Vulnerability and Patch Management（個別製品）

株式会社カスペルスキー

製品情報：www.kaspersky.co.jp/business-security/systems-management
ご購入相談窓口：jp-sales@kaspersky.com

www.kaspersky.co.jp
#truecybersecurity



PMM-1019-201705