脆弱性とパッチ管理

ESET Vulnerability & Patch Management 機能紹介資料

第3版

2024年4月

Canon

キヤノンマーケティングジャパン株式会社

はじめに（本資料について）

昨今、増加するサイバー攻撃に関する報道の中で「脆弱性※」という言葉を目にすることが多くなりました。

脆弱性はありとあらゆる攻撃の糸口となり、リスクであるとの認識が高まっています。予防対策として脆弱性を管理し、セキュリティパッチを迅速に適用することで、常に最新の修正プログラムが適用されたOSやアプリケーションの状態を保ち、マルウェア感染のリスクを低減します。

本資料は、OSやソフトウェアの脆弱性診断と自動的な修正対応を実現する機能である
脆弱性とパッチ管理「ESET Vulnerability & Patch Management（VAPM）」の機能紹介資料です。

- ESET Vulnerability & Patch Management（VAPM）は、下記いずれかのライセンスをご契約の場合 ご利用いただけます。
  - ESET PROTECT Elite
  - ESET PROTECT Complete
- ESET Vulnerability & Patch Management（VAPM）をご利用いただくためには、クラウド型セキュリティ管理ツールであるESET PROTECT での管理が必要です。※オンプレミス型セキュリティ管理ツール ESET PROTECT on-prem ではご利用いただけません。
- 本資料で使用している画面イメージは使用するバージョンやOSにより異なる場合があり、今後画面イメージや文言が変更される可能性があります。
- Windows, Windows Serverは、米国Microsoft Corporationの、米国、日本およびその他の国における登録商標または商標です。
- ESET、ESET PROTECT、ESET Endpoint アンチウイルス、ESET Endpoint SecurityはESET,spol. s. r. o.の商標です。

※ 脆弱性…コンピュータ関連のプログラムに潜む欠点や盲点、弱点のことで、「セキュリティ・ホール」とも呼ばれる
https://eset-info.canon-its.jp/malware_info/term/detail/00068.html

目次

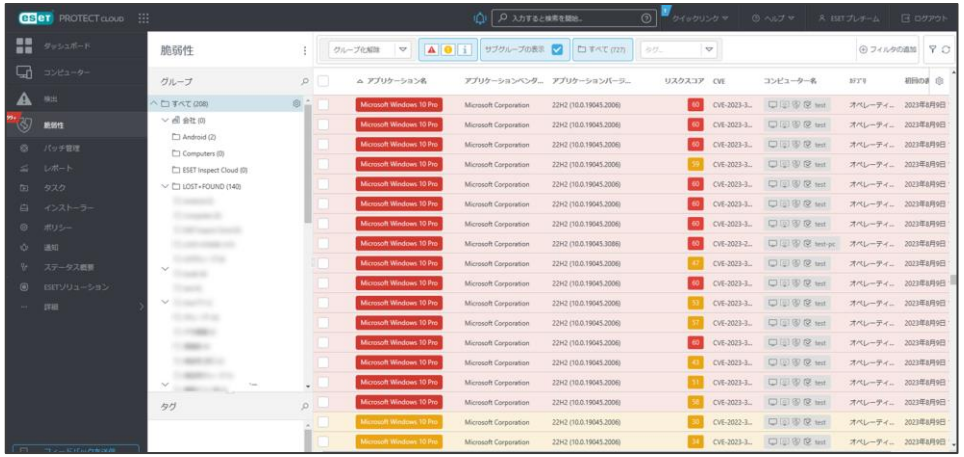
ESET Vulnerability & Patch Management (VAPM) の概要

1. ESET Vulnerability & Patch Managementの概要

(1) VAPMとは？

ESET Vulnerability & Patch ManagementはOSとアプリケーションの脆弱性とパッチ※適用状況を管理するソリューションです。
古いオペレーティングシステムやアプリケーションの脅威からクライアントを守ります。
クライアントの脆弱性情報は重大度（リスクスコア）が付与されるため、重大度の高いものから脆弱性対応するといった運用ができます。
また、パッチ管理につきましては手動またはスケジューリングして自動で適用させることもできます。

セキュリティ管理ツールでの「脆弱性とパッチ管理」のイメージ



- ESET Vulnerability & Patch Managementの主な機能

✓ クライアントの脆弱性情報を自動で収集
✓ 自動および手動でのパッチ適用
✓ 脆弱性の重大度のレベルづけ
✓ 対象のクライアントのリストの表示　など

※ パッチ… OSやソフトウェアに存在する脆弱性やバグを修正するプログラムを指します。「修正プログラム」「更新プログラム」「アップデート」などと呼ばれることもあります。

1. ESET Vulnerability & Patch Managementの概要

(2) 特長

①組織全体の状況の可視化

組織全体の脆弱性やパッチの適用状況を可視化します。
可視化することにより、組織全体の一元管理を行うことができ、管理者の脆弱性とパッチ管理の負担を軽減することができます。

②脆弱性のリスクレベルによる対応の優先順位づけ

Adobe Acrobat、Mozilla Firefox、Zoom Client などの240※1ものアプリケーションをスキャンすることにより、35,000を超える一般的な脆弱性とCVE※2を検出します。検出した脆弱性はリスクレベルが付与され、リスクレベルを参考に対応する脆弱性の優先順位づけを行うことができます。

※1:2023年10月現在
※1:CVE…脆弱性のデータベースのことを指し、共通脆弱性識別子とも呼ばれます。

③パッチを手動または自動で適用可能

パッチは手動または自動で適用することができます。
パッチの自動適用はアプリケーション毎に個別に設定することができ、自動適用するタイミングをスケジュールすることもできます。

1. ESET Vulnerability & Patch Managementの概要

(3) 動作環境

ESET Vulnerability & Patch Managementの利用にあたっては、以下の環境が必要です。

①クラウド型セキュリティ管理ツールが構築されていること

②クラウド型セキュリティ管理ツールでエンドポイントの管理が行われていること

③エンドポイントにはVAPMに対応した以下のプログラムが導入されていること

※ARM版エンドポイントプログラムは未サポートです。

プログラム名		バージョン	
		V10.0以前	V10.1以降
ESET Endpoint Security (EES)	WindowsクライアントOS向け総合セキュリティプログラム	×	○
ESET Endpoint アンチウイルス (EEA)	WindowsクライアントOS向けウイルス・スパイウェア対策プログラム	×	○
ESET Management Agent (EMエージェント)	クライアント管理用エージェントプログラム	×	○
ESET PROTECT (クラウド版)	クラウド型セキュリティ管理ツール	○	

※ 2024年以降、Windows Server、mac OS、Linuxへ順次対応予定(2024年3月現在)

1. ESET Vulnerability & Patch Managementの概要

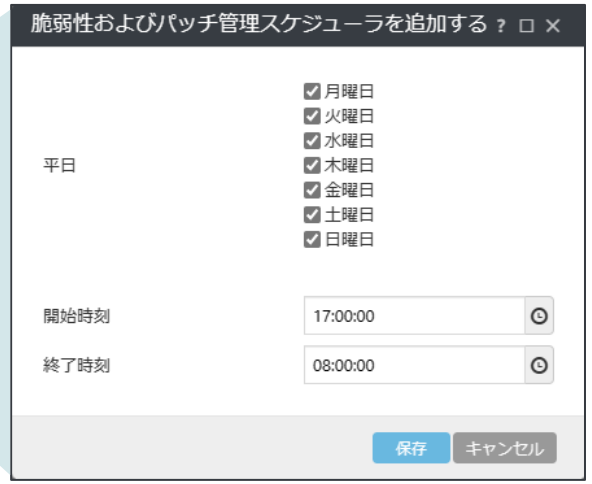
(4) VAPMの主な設定

VAPMの機能を有効にすることで以下の設定を行うことが可能です。

設定項目	内容
自動パッチ管理を有効にする	本項目を有効にすることで以降の項目で設定した内容にてパッチが適用されます。
コンピューターの再起動オプション	パッチ適用実施後、コンピューターの再起動が必要な場合に自動で再起動するか設定できます。
脆弱性およびパッチ管理スケジューラ	スキャンを実施するスケジュール “曜日”、“開始時刻”、“終了時刻”を設定することができます。 右下の画面より設定を変更することができます。

セキュリティ管理ツール ESET PROTECT (クラウド版) のVAPMに関するポリシー画面

脆弱性およびパッチ管理のスケジューラ設定画面



1. ESET Vulnerability & Patch Managementの概要

(4) VAPMの主な設定

VAPMの機能を有効にすることで以下の設定を行うことが可能です。

設定項目		内容
自動パッチ管理カスタマイズ		
	自動パッチ戦略	パッチ管理を以下の2種類から選択。 ・「許可されたアプリケーションにのみパッチ適用」 ・「除外されたアプリケーションを除くすべてのアプリケーションにパッチ適用」
	許可されたアプリケーション	上記での設定に応じて、“許可“もしくは”除外”するアプリケーションを編集画面に表示される「パッチ適用可能な製品」一覧から選択。
	対象外アプリケーション	

セキュリティ管理ツール ESET PROTECT (クラウド版) のVAPMに関するポリシー画面

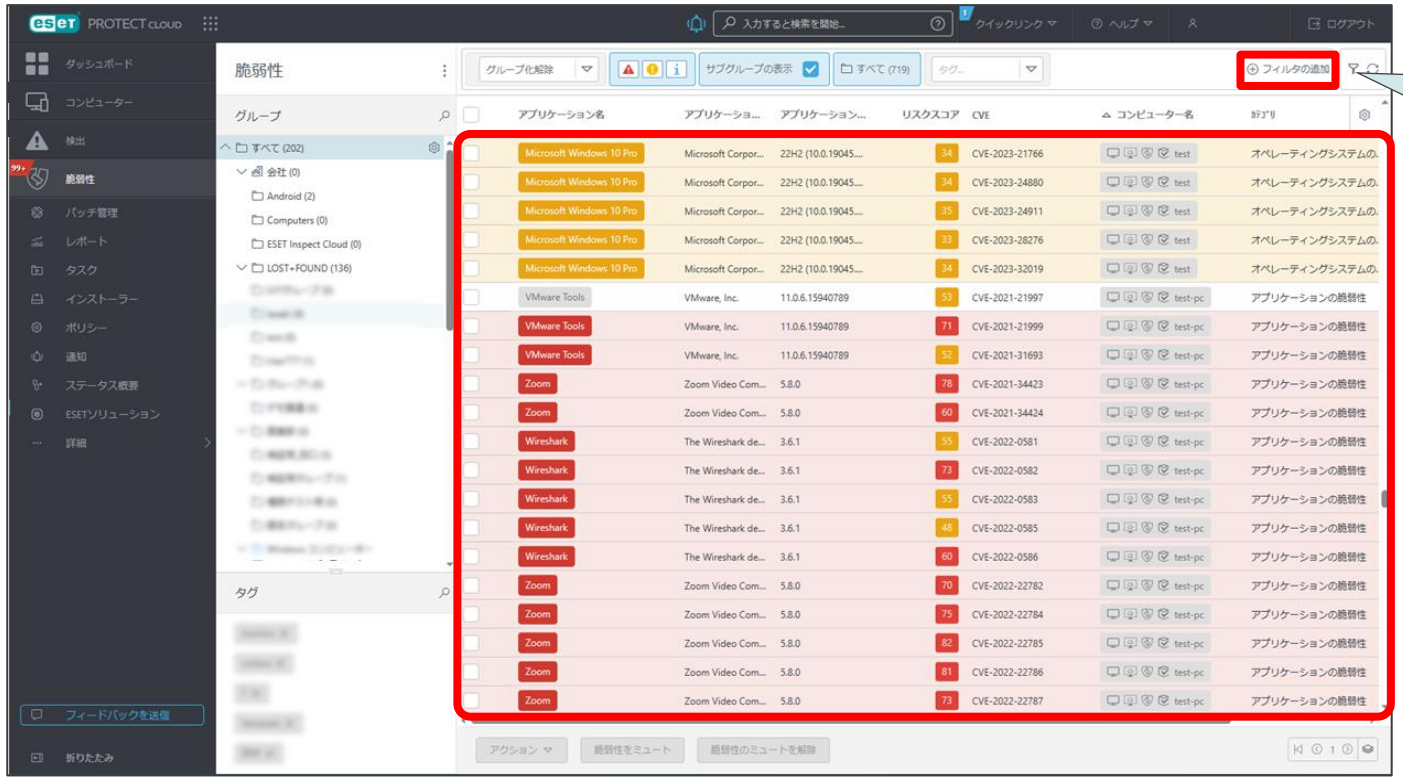
“許可するアプリケーション” または、
“除外するアプリケーション“を
選択できます。

ESET Vulnerability & Patch Management
の機能紹介

2. ESET Vulnerability & Patch Managementの機能紹介

(1)「脆弱性」の一覧

セキュリティ管理ツールより、クライアントにて検出されている脆弱性の一覧を確認することができます。
脆弱性情報は並べ替え、アプリケーション名・リスクスコアの値などでフィルタで特定の値のみを抽出して表示できます。



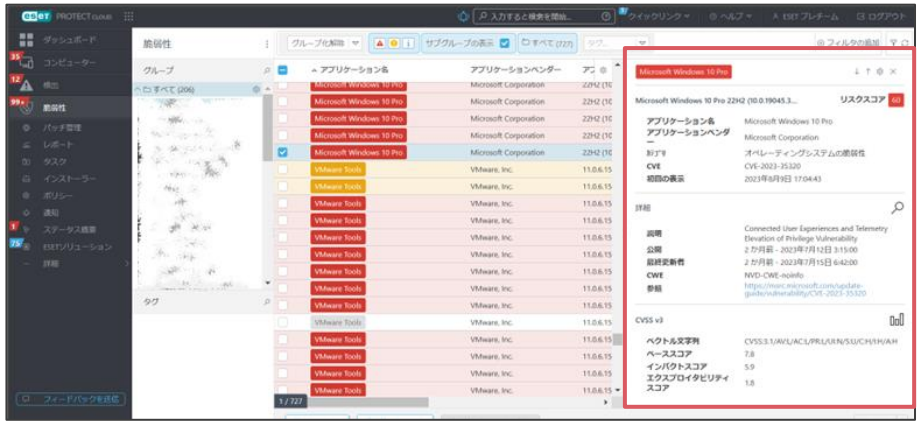
フィルタを利用し、条件を追加することで脆弱性を絞り込むことができます。
「≦リスクスコアの値」 にてリスクレベルの高い脆弱性を確認することができます。

- ≦ リスクスコアの値
- ≧ リスクスコアの値
- CVE
- アプリケーションバージョン
- アプリケーション名
- ｶﾃｺﾞﾘ
- コンピューター名
- ベンダー
- ミュートされた脆弱性

2. ESET Vulnerability & Patch Managementの機能紹介

(1)「脆弱性」の一覧

脆弱性の詳細情報は、脆弱性一覧画面より選択することで右側に表示されます。



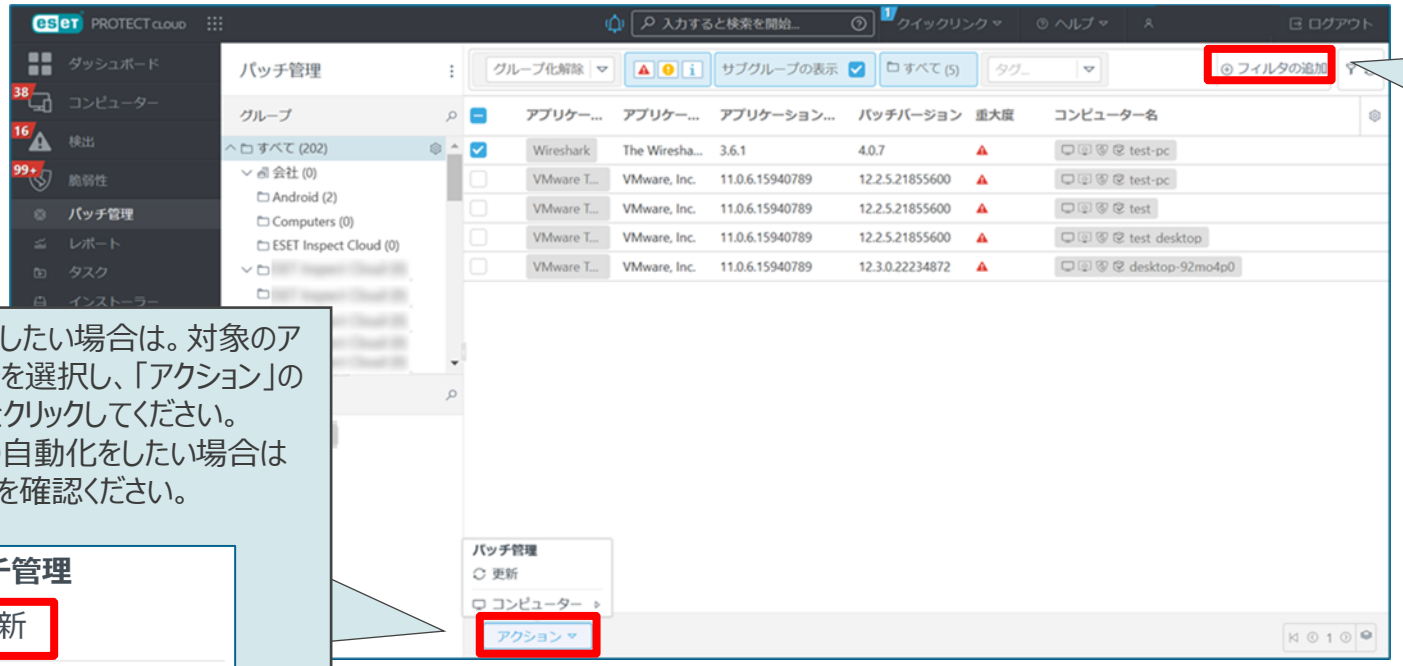
項目	説明
アプリケーション名	脆弱性のあるアプリケーション名
リスクスコア	脆弱性の重大度の評価※ ・グレー（0~29）：重大度低 ・黄色　（30~59）：重大度中 ・赤　　(60~100)：重大度高
アプリケーションベンダー	脆弱性を持つアプリケーションベンダー名
カテゴリ	脆弱性カテゴリ ex) オペレーティングシステムの脆弱性、アプリケーションの脆弱性
CVE	脆弱性の識別番号であるCVE (共通脆弱性識別子)番号
初回の表示	デバイスで脆弱性が最初に検出された日時

※脆弱性-リスクスコア
https://help.eset.com/protect_cloud/ja-JP/vulnerabilities.html

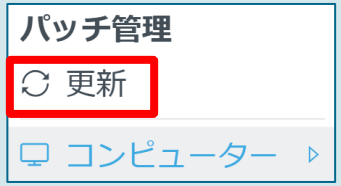
2. ESET Vulnerability & Patch Managementの機能紹介

(2)「パッチ管理」の一覧

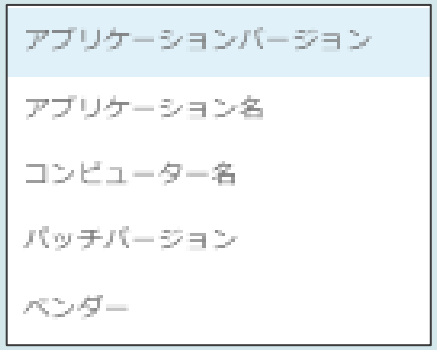
セキュリティ管理ツールより、クライアントにて検出された脆弱性を修正するために利用可能なパッチの一覧を確認することができます。
こちらにより修復対応（パッチ適用）を容易に実施することができます。



パッチ適用をしたい場合は。対象のアプリケーションを選択し、「アクション」の「更新」をクリックしてください。
パッチ適用の自動化をしたい場合は本資料P17を確認ください。



フィルタを利用し、条件を追加することでパッチを絞り込むことができます。
「アプリケーション」 にて特定のアプリケーションの情報のみ確認することができます。



ESET Vulnerability & Patch Management
の設定手順

3. ESET Vulnerability & Patch Managementの設定手順

(1) VAPMの設定方法

VAPMは以下の方法で有効化できます。有効化、設定変更はセキュリティ管理ツールからのみ実施可能です。
お客様の環境に合わせて方法を選択してください。操作手順については次ページ以降に案内します。

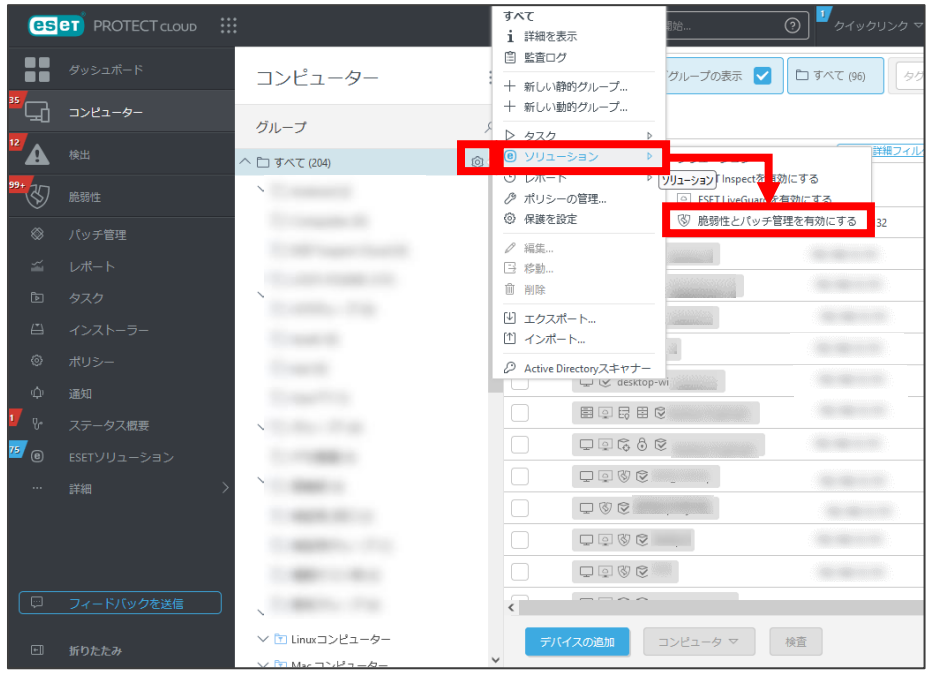
	設定方法	ページ数
(2)VAPMの導入方法	i. **コンピューターの一覧画面より、VAPMを有効化を行う** ※グループへ一括適用したい場合はこちらをご利用ください	P15
	ii. **コンピューターの詳細画面より、VAPMを有効化を行う** ※端末ごとに個別設定したい場合はこちらをご利用ください	P16
(3)パッチ適用の自動化設定方法	iii. **ポリシーにて、パッチ適用の自動化設定を行う**	P17

3. ESET Vulnerability & Patch Managementの設定手順

(2) VAPMの導入方法

i. コンピューターの一覧画面より、VAPMを有効化を行う

VAPMを有効したいグループまたはクライアントを選択し、「⚙」→「ソリューション」→「脆弱性とパッチ管理を有効にする」の順にクリックします。その後、利用するライセンスなどを設定し、有効にすることができます。



3. ESET Vulnerability & Patch Managementの設定手順

(2) VAPMの導入方法

ii. コンピューターの詳細画面より、VAPMを有効化を行う

VAPMを有効化したいクライアントの詳細画面の「概要」より、「脆弱性とパッチ管理」の「有効」をクリックします。
その後、利用するライセンスなどを設定し、有効にすることができます。

3. ESET Vulnerability & Patch Managementの設定手順

(3) パッチ適用の自動化設定方法

iii. ポリシーにて、パッチ適用の自動化設定を行う

自動的にパッチを適用する設定はポリシーで行うことができます。ポリシーの「Common features」にてVAPMの各種設定をカスタマイズできますので、お客様の環境に合わせてポリシーを作成できます。

■パッチ適用の自動化設定項目の詳細

・製品を選択：Common features

・設定項目　：[脆弱性パッチおよび管理]
▼脆弱性パッチおよび管理
▼自動パッチ管理を有効にする

※上記設定を実施する際は、事前に「脆弱性およびパッチ管理を有効にする」を有効化してください。
有効化されていない場合、設定項目がグレーアウトした状態となり、操作を行うことができませんのでご注意ください。