

# はじめに

## 対象者

- ・ オンプレミス製品を利用中の既存ユーザ様、パートナー様が対象になります
- ・ 尚、完全クローズド環境やスタンドアロン運用のお客様におかれまして、本移行フローにてご対応ができない可能性がある点についてはあらかじめご了承くださいませ。

## Webinar 内容（約2時間）

- ・ Elements製品の概要と既存ユーザ様向けの移行優遇措置について（30分）
- ・ オンプレミス製品からElements製品への移行について（1時間20分）
  - ・ 移行前の動作要件/環境の確認について
  - ・ 現在の運用構成から移行後の運用構成について
  - ・ 移行フロー概要
  - ・ 移行フローの詳細説明（別紙 ①～⑪手順）
- ・ 質疑応答（10分）

## 注意点

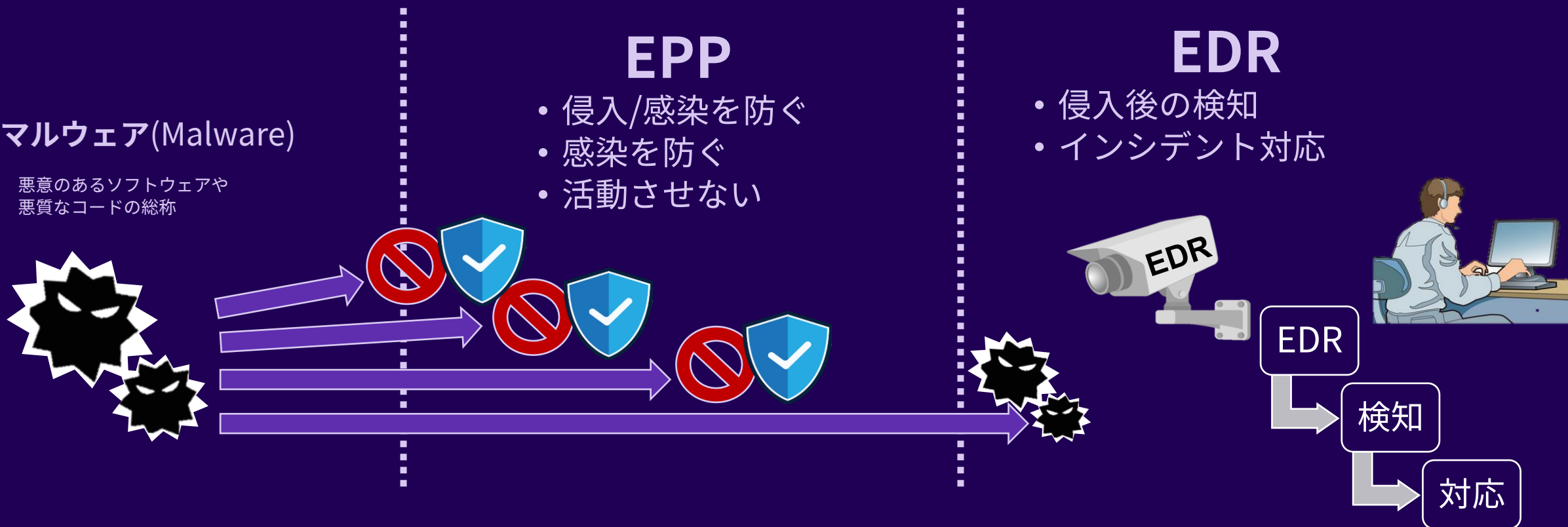
- ・ 本Webinar中はマイク等はオフとなるため、ご質問がある場合は適宜「QA」ボタンにて、テキストにてご質問をお願いいたします。挙手ボタンはございますが、ご利用なさらないようお願いいたします。
- ・ 後日、本ウェビナーへのご参加頂いたお客様、パートナー様向けに当日のウェビナー動画と質疑応答後のQA表をお送りする予定でございます。
- ・ ご不明点やお問い合わせがある場合は、弊社代表アドレス<japan@withsecure.com>宛、件名「8月27日開催ウェビナーについて」にてご連絡をお願い申し上げます。

# WithSecure EPP/EDR 製品紹介

# EPP (Endpoint Protection Platform) と EDR (Endpoint Detection and Response) 役割の違い

マルウェア(Malware)

悪意のあるソフトウェアや  
悪質なコードの総称



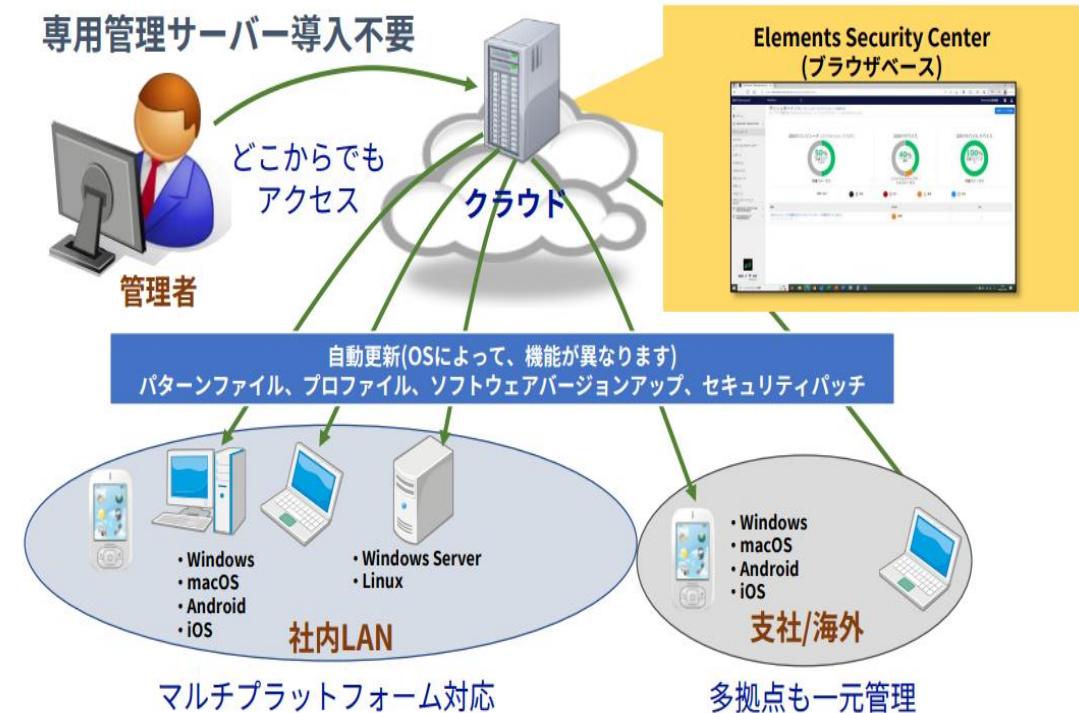
今も昔もエンドポイントセキュリティは最後の砦  
いまの時代は企業規模を問わずEPP+EDRは絶対に必要

# Elements EPP (クラウド) の特長

## Elements EPPのメリット

- 物理サーバ不要 (コストカット)
- どこからでもアクセス可能
- マルチプラットフォーム対応
- 1Lから購入可能
  
- WithSecure Elementsは
  - 1つのエージェント (追加の作業不要)
  - 1つのポータル (一元管理)
  - 資産管理やパッチ管理の機能も搭載

## ウィズセキュアクラウドサービス全体図



# WithSecure Elements Endpoint Protection – 主要機能



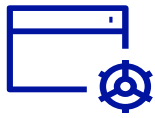
ディープガード  
(振る舞い検知)



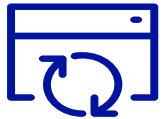
データガード/  
ロールバック  
(ランサムウェア対策)



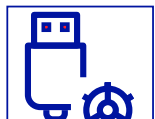
Web保護 &  
カテゴリフィルタリング



アプリケーション制御



ソフトウェアアップデート  
(アップデートパッチ管理)

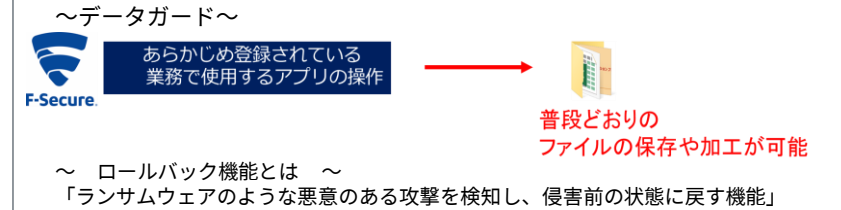


デバイス制御

## ディープガードによる多層防御



## ランサムウェア対策： データガード(プレミアム版)/ロールバック



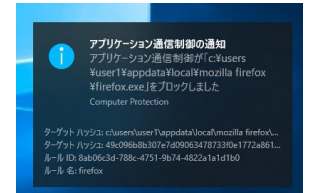
## Webサイトのカテゴリフィルタリング

管理ポータルでWebサイトのカテゴリフィルタリングを一元管理  
32のカテゴリをグループ毎に設定可能

中絶	ハッキング
広告の提供	憎悪表現
アダルト	就活
アルコール・タバコ	

## アプリケーション制御 (プレミアム版)

アプリケーションを実行する条件を設定し、制御します。  
例: cmd.exeはWordファイルのマクロからの実行は不可、他は可。



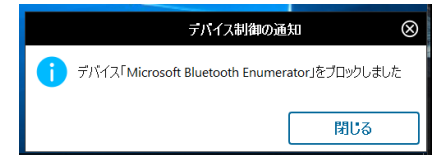
## パッチ管理：脆弱性対策

アップデートパッチを最新にバージョンアップすることで、脆弱性  
を利用したマルウェアの攻撃を回避することができます



## デバイス制御

大容量記憶装置、USB カメラ、プリンタなどのUSB デバイスへの  
アクセス制限を設定



# オンプレミス製品との機能差分

機能	機能の概要	クライアントセキュリティ	クライアントセキュリティ プレミアム	Elements EPP for Computers	Elements EPP for Computers Premium
マルウェア・スパイウェア防御	パターンファイルによる既知のマルウェア、スパイウェア防御	●	●	●	●
ディープガード	機械学習を用いた振る舞い検知による未知のマルウェア・スパイウェアの対策	●	●	●	●
ファイアウォール	Windowsファイアウォールを使用したネットワークアクセスの制御	●	●	●	●
デバイス制御	ハードウェアデバイスの制御	●	●	●	●
Webトラフィックスキャン	Webトラフィック(HTTP)に含まれる怪しいファイルの対策	●	●	●	●
ブラウザ保護	怪しいWebサイトへの接続の対策	●	●	●	●
Webコンテンツ制御	コンテンツに基づいて、Webサイトへの接続の制御		●	●	●
接続制御	金融サイト接続時の情報漏洩対策として、他のネットワーク通信の制御		●	●	●
ソフトウェアアップデート	Windowsやサードパーティ製品のセキュリティパッチの適用・管理		●	●	●
データガード	フォルダ、ファイルにアクセス出来る実行ファイルの制御		●		● ランサムウェア対策に
アプリケーション制御	アプリケーションの起動、動作の制御		●		● EMOTET対策に
製品自体の自動更新	自動的に製品のバージョンアップやモジュールの自動更新			●	●
非インターネット環境	非インターネット環境での利用について	●	●	Elements Connector (無償ソフト)を併用し対応を予定	Elements Connector (無償ソフト)を併用し対応を予定
集中管理	製品の集中管理ソフト (無償)	ポリシーマネージャ	ポリシーマネージャ	Elements Security Center	Elements Security Center

- ・ Elementsシリーズは製品の自動バージョンアップ機能があるため、オンプレミス製品のような手動バージョンアップ作業が不要となります。
- ・ Elementsシリーズは弊社クラウド上のElements Security Centerで管理するため、各端末にインターネット接続環境が必要となります。
- ・ ポリシーマネージャで集中管理された各端末にElementsシリーズをポリシーベースでインストールできるため、短時間で移行が可能です。

※非インターネット環境でのElementsシリーズの利用については、今後リリース予定のElements Connectorを併用することで運用可能となります。Elements Connectorを導入した端末がインターネットに接続されていれば、配下の端末をクラウド管理できるようになります。ただしElements Connector導入端末だけはインターネット接続が必要となるので、完全クローズ環境ではご利用いただけません。

# ランサムウェア対策に特化した機能が充実①

## ➤ ロールバック機能

- ランサムウェアのような悪意のある攻撃を検知し、侵害前の状態に戻す機能

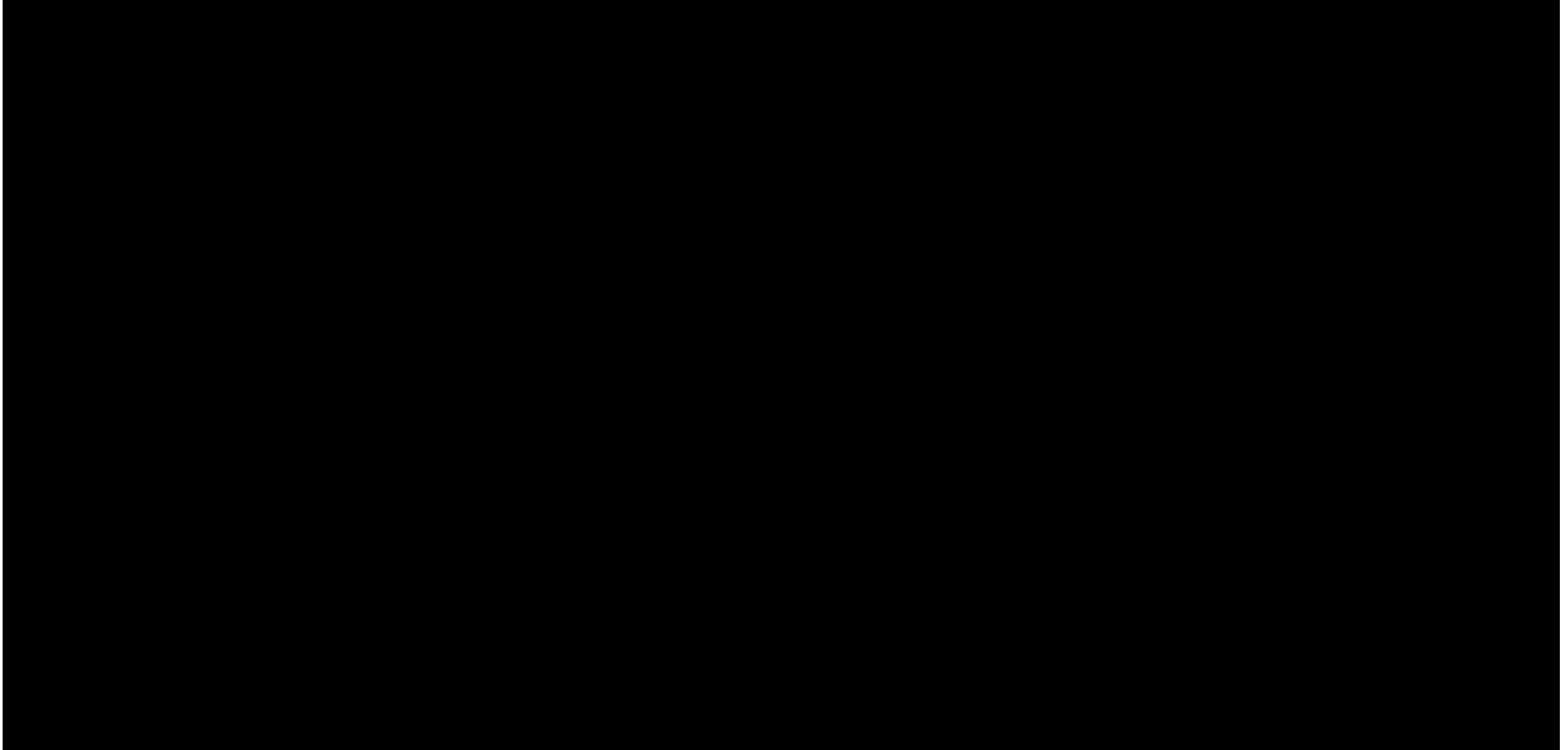
The screenshot displays the WithSecure Elements Agent interface. The main window shows the 'Security Events' section with a table of events. Two notification pop-ups are overlaid on the right side of the interface, connected to the event table by red arrows.

Time	Severity	Source	Device	Description
8 minutes ago May 23, 2023, 14:50:17	Information	Rollback	DESKTOP-8RQD	Changed files and system settings have been restored successfully. The original changes and files are backed up and may be restored from quarantine.
8 minutes ago May 23, 2023, 14:50:17	Action needed	Rollback	DESKTOP-8RQD	Malware has infected the operating system and changed files and system settings.

**WithSecure™ Elements Agent**  
**Rollback**  
Changed files and system settings have been backed up and restored successfully.  
Activate Windows  
Go to Settings to activate Windows.  
Reason: TestFileW32/ActivityMonitor.A

**WithSecure™ Elements Agent**  
**Rollback**  
Ransomware has infected the operating system and changed files and system settings.  
The number of affected files: 2, Windows  
The number of processes affected: 0, activate Windows.  
Reason: TestFileW32/ActivityMonitor.A

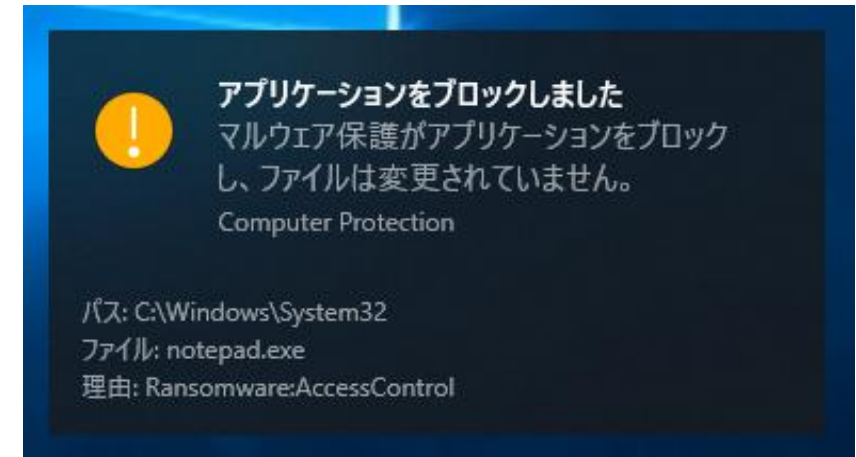
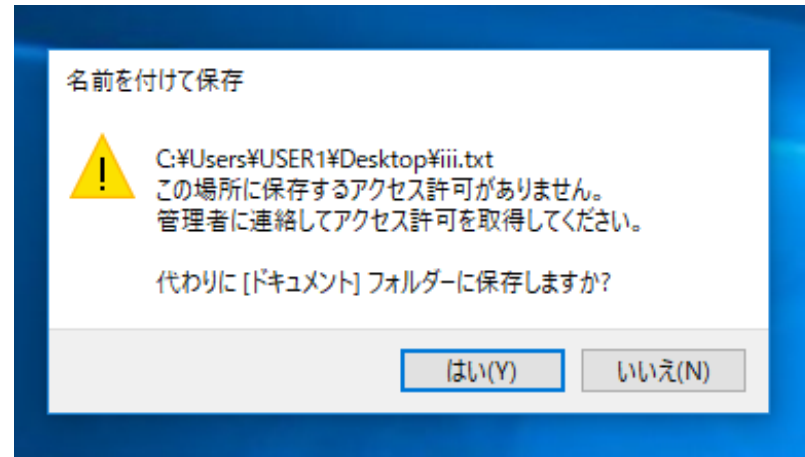
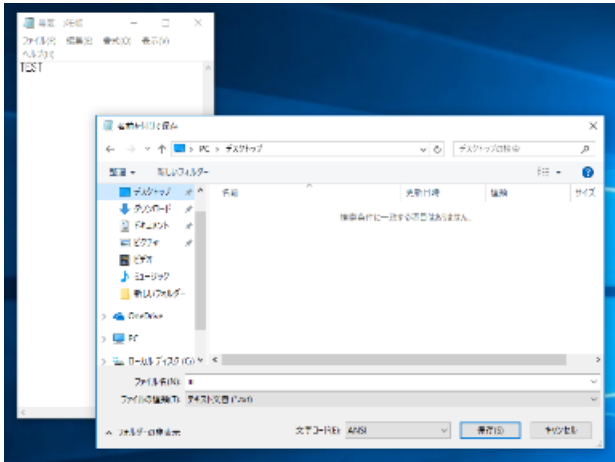
# ロールバック デモ動画



# ランサムウェア対策に特化した機能が充実②

## ➤ データガード機能 (\*プレミアム)

- 信頼できるアプリケーションのみ監視対象のフォルダにアクセスを許可する機能。



# ランサムウェア対策に特化した機能が充実③

## ➤ サーバー共有保護の設定および動作概要

### Windowsサーバー用プロファイルでON/OFFおよびオプションを設定

Windows Serversのプロファイル  
JP\_PROMOTION

サーバ共有保護

[サーバ共有保護] タブでは、除外フォルダーと除外ユーザーを追加することができます。サーバ共有保護は共有フォルダーを監視し、ランサムウェアがネットワーク経由で変更したファイルをそのフォルダーから復元することを可能にします。特定の共有フォルダーを監視したくない場合は、そのフォルダーを除外することができます。除外されたユーザーとは、サーバ共有保護が監視しないユーザーで、共有フォルダー内のファイルの編集が許可されているユーザーを指します。

設定項目	状態	オプション
サーバ共有保護	ON	⊞
許可およびレポートモード	ON	⊞
元に戻したファイルの復元を許可する	ON	⊞
ユーザーのアクセスをブロックする(分)	0	⊞
バックアップファイルを保存するためのカスタムフォルダー		⊞

値は0～10,080分(7日間)の整数値である必要があります。

保存して発行

1. サーバー共有に対して新しいユーザーがファイル変更を行うと、特定のプロセスIDとともに変更したユーザーのSIDが記録される
2. ロールバック機能と同様に、ファイル変更手順を記録しながらバックアップを作成
3. ファイル変更が不正なものと判断された場合、該当ユーザーは一定期間接続が解除される
4. ロールバック機能と同様に、自動的にバックアップファイルからオリジナルファイルを復旧

# 脆弱性対策：パッチ管理

パッチ管理 ...

[適用されていないアップデート](#) [インストールログ](#)

フィールドを選択 ▼ に等しい ▼ 値を選択してください ▼ 適用 キャンセル すべてのフィルタを消去

1 - 19 / 19 < >

<input type="checkbox"/>	ベンダー	ソフトウェア	現行のバージョン	ターゲットバージョン	カテゴリ	CVE ID
<input checked="" type="checkbox"/>	Microsoft Corporation	2025-08 Cumulative Update for Microsoft server operating system version 21H2 for x64-based Systems (KB5063880)	該当なし	該当なし	● 重大なセキュリティ	
<input type="checkbox"/>	Igor Pavlov	7-Zip exe (x64)	19.00	25.01	● 中セキュリティ	<span>7.8</span> CVE-2024
<input type="checkbox"/>	Zoom Video Communications, Inc.	Zoom	6.4.12	6.5.10	● セキュリティに関連しない	
<input type="checkbox"/>	Microsoft Corporation	Windows Malicious Software Removal Tool x64 - v5.134 (KB890830)	該当なし	該当なし	● セキュリティに関連しない	
<input type="checkbox"/>	Slack Technologies, Inc.	Slack	4.40.133	4.45.64	● セキュリティに関連しない	
<input type="checkbox"/>	Microsoft Corporation	Microsoft Visual C++ Redistributable 2013 (x86)	12.0.30501.0	12.0.40664.0	● セキュリティに関連しない	
<input type="checkbox"/>	Microsoft Corporation	Microsoft Visual C++ Redistributable 2013 (x64)	12.0.30501.0	12.0.40664.0	● セキュリティに関連しない	
<input type="checkbox"/>	Microsoft Corporation	Microsoft Visual C++ 2015-2022 Redistributable (x86)	14.30.30708.0	14.44.35211.0	● セキュリティに関連しない	
<input type="checkbox"/>	Microsoft Corporation	Microsoft Visual C++ 2015-2022 Redistributable (x86)	14.34.31938.0	14.44.35211.0	● セキュリティに関連しない	

パッチ管理機能により最新のソフトウェアにアップデートが可能。  
デフォルトで常時最新適用もしくは都度パッチ適用として対応が可能

1件のアップデートを選択しました

実行中のアプリケーションを強制終了

アップデートをすぐにインストールする ▼

更新するワークステーションが見つかりませ  
ん

1台のサーバーで更新があります

アップデートするデバイスの選択

# デバイスのセキュリティポスチャ

JP\_PROMOTION  
Ohta L2 test

Free trials

環境 / デバイスのセキュリティポスチャ

## デバイスのセキュリティポスチャ

セキュリティに関する推奨事項

● 準拠: 6 ● 非準拠: 9

フィールドを選択 | に等しい | 値を選択してください

セキュリティに関する推奨事項	ステータス	デバイス	プロファイル	対応
パスワードの最小文字数が指定されていないか、または8文字未満です	!	6	0	Windows Apple iOS Linux
アカウントロックアウトの閾値が設定されていません	!	4	0	Windows Apple iOS Linux
ワークステーションの10%以上で、最終ログインしたユーザーは管理者です。	!	4	0	Windows Apple iOS Linux
ユーザーは、プロファイルでパスワードなしでクライアントをアンインストールできます	!	4	31	Windows Apple iOS Linux
プロファイルでディープガードが有効になっていません	!	3	2	Windows Apple iOS Linux
RDPが有効で、アカウントロックアウトの閾値が設定されていません	!	2	0	Windows Apple iOS Linux
システムドライブの暗号化が無効になっています	!	2	0	Windows Apple iOS Linux
サポート終了のOS	!	1	0	Windows Apple iOS Linux

端末管理として、  
端末の弱点の把握

# Elements管理ポータル：簡易版IT資産管理

デバイス

コンピューター モバイルデバイス コネクタ 管理されていないデバイス デバイスの検出 脆弱性アセット

フィールドを選択  に等しい  値を選択してください  適用 キャンセル 全てのフィルタを消去

表示 全体のステータス

列の選択

1 - 50 / 70

<input type="checkbox"/>	タイプ	名前	オンライン	登録日	OS名前	指定プロファイル	ステータスの更新日時	クライアントバージョン
<input type="checkbox"/>	Apple	klmacmini	いいえ	Nov 19, 2024	macOS	Yusri Test	Jul 28, 2025, 6:54:13 PM	25.3.54466
<input type="checkbox"/>	PC	WIN10-M22	いいえ	Nov 27, 2023	Windows 10	Hirasawa_Test_3	Dec 3, 2023, 8:57:08 PM	23.8
<input type="checkbox"/>	PC	WIN11-M43	いいえ	Feb 11, 2025	Windows 11	Hirasawa_Test_2	Mar 30, 2025, 6:17:39 PM	22.8
<input type="checkbox"/>	Server	WINSVR2019-2	いいえ	Jun 10, 2023	Windows Server 2019	WithSecure™ Server	Jun 11, 2023, 1:47:15 PM	23.4
<input type="checkbox"/>	PC	LAPTOP-MIGU246K	いいえ	Mar 21, 2024	Windows 11	ooki01	Mar 5, 2025, 5:50:43 AM	25.1
<input type="checkbox"/>	PC	Test Alias	いいえ	Mar 20, 2020	Windows	FW test	Feb 6, 2019, 9:06:10 PM	
<input type="checkbox"/>	PC	DESKTOP-MCH19GC	いいえ	Mar 18, 2020	Windows	koshida-test	Aug 26, 2020, 10:37:25 PM	

デバイスを検索

有効期限

サブスクリプションタイプ

使用可能な列 160/177

コメント

重要

保護ステータスの概要

全体保護

プロファイルの指定ステータス

OSバージョン

ファイアウォール

デバイス制御

アプリケーション制御 (Premium)

DataGuard (Premium)

ネットワークの隔離

EDRセンサー

アドバンスド・レスポンス

Active Directory組織単位

OSのサポート終了

最終再開時間

再起動が必要です

再起動リクエストの理由

オフロードスキャンの状態

オフロードスキャンが切断されました

オフロードスキャンの平均アップロード速度

BIOSメーカー

コンピュータモデル

プロセッサコア

システムドライブの容量

システムドライブの空き容量

物理メモリサイズ

空き物理メモリ

シリアル番号

BIOSバージョン

BIOSリリース日

Computer Description

ディスクタイプ

ボリューム情報

RAM情報

管理者がログインしています

ディスク暗号化ステータス

Disk encryption policy

暗号化されたドライブ

BitLocker回復キーの収集が有効になっています

BitLocker回復キーの収集が成功しました

BitLocker全体の保護ステータス

ゲスト アカウント

パスワードの最小文字数

EPPの情報だけではなく、インストールしている端末のインベントリ情報の取得が可能。

簡易版IT資産管理ツールとしても活用ができる。

例：OSバージョン、BIOSメーカー、システムドライブ空き容量等

# Elements管理ポータル：アクションボタン

☰ 環境 / デバイス

WIN10-M22 [エイリアスを追加](#)

● オフライン | ステータスの更新日時 Dec 3, 2023, 8:57:08 PM | 登録日 Nov 27, 2023 | 前回のユーザー WIN10-M22¥konary | ラベル workgroup | アセットグループ 平澤商店

[セキュリティイベントを表示](#) | [監査ログを表示する](#) | [インストールされているソフトウェアアップデートを表示する](#) | [Collaboration Protectionでユーザー検出を表示する](#) | [履歴の表示](#) | [RDPで接続する](#)

保護ステータス 操作 スキャンレポート 接続されているデバイス:

⚠ 全体保護	
✔ ネットワーク接続が有効になっています	
✔ 発生状況	
▼ ✔ ライセンス	
✔ ファイアウォール	
現在のファイアウォールプロファイル	
✔ デバイス制御	
▼ ⚠ マルウェア保護	

指定プロファイル  
Hirasawa\_Test\_3

使用中のプロファイル  
Hirasawa\_Test\_2

プロファイルの指定ステータス  
割り当て中

サブスクリプションタイプ  
EPP and EDR for Computers Premium

リモートでデバイスに対して「アクション」ボタンから操作が可能：ネットワークの隔離、再起動、アンインストール等

☰ アクション

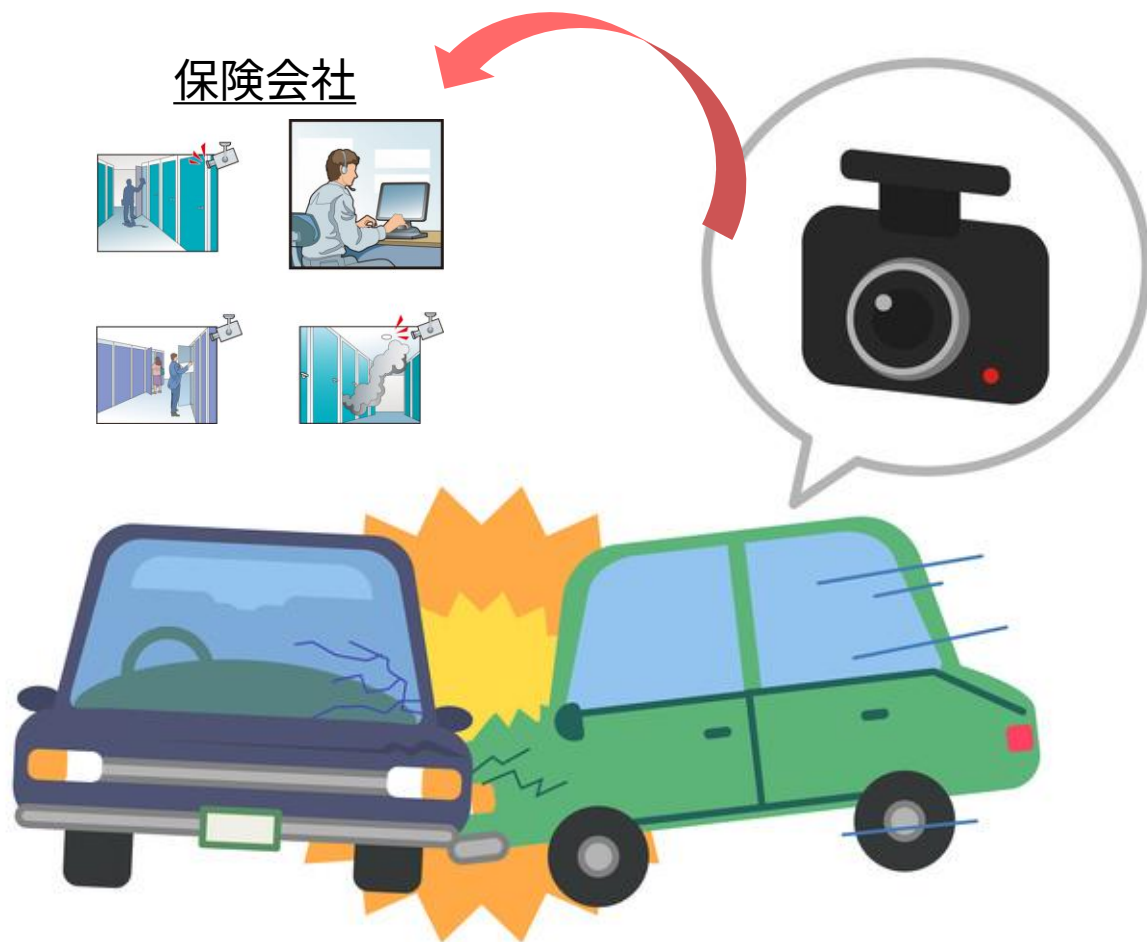
ステータスアップデートを送る	延期された操作をキャンセルする	ソフトウェアアップデートをインストール	マルウェアをスキャンする	適用されていないソフトウェアのアップデートをスキャン	プロファイルを指定する	ラベルを管理する
重要性の更新	コメントを更新	Vulnerability Managementスキャン	ライセンスを変更する	デバイスを削除する	ネットワークの隔離	再起動
ドライブの暗号化	診断ファイルを要求する	デバッグログをオンにする	デバイスにメッセージを送信する	セキュリティ機能をオフにする	セキュリティ機能を復元する	除外されたローカルのパスを削除する
アンインストール	アセットグループの管理					

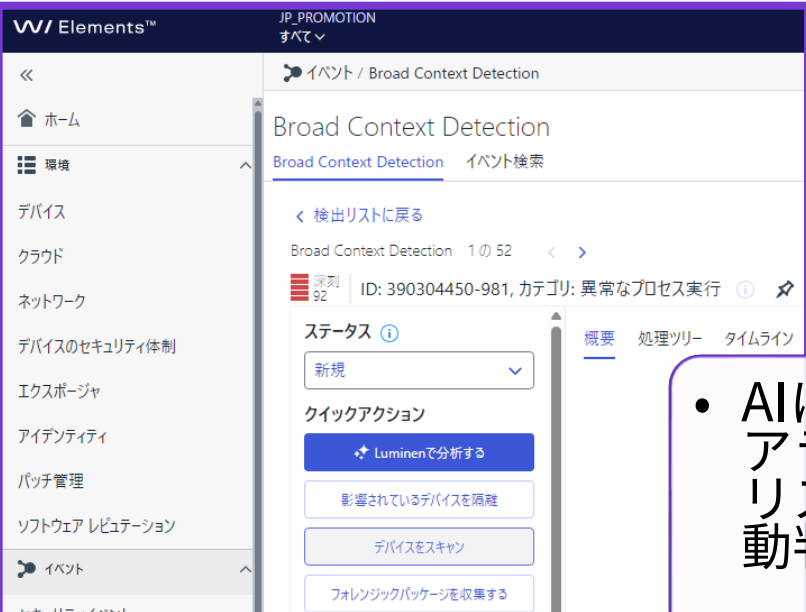
# WithSecure Elements EPP おすすめポイント

- ✓ウィズセキュア独自のディープガードやAIによる**多層防御**（他社EPPとの差別化）
- ✓**ランサムウェア対策**に最適なロールバックとデータガード機能を搭載
- ✓簡易版IT資産管理機能として活用可能（OS情報の可視化、システムドライブの容量等）
- ✓パッチ管理による脆弱性対策

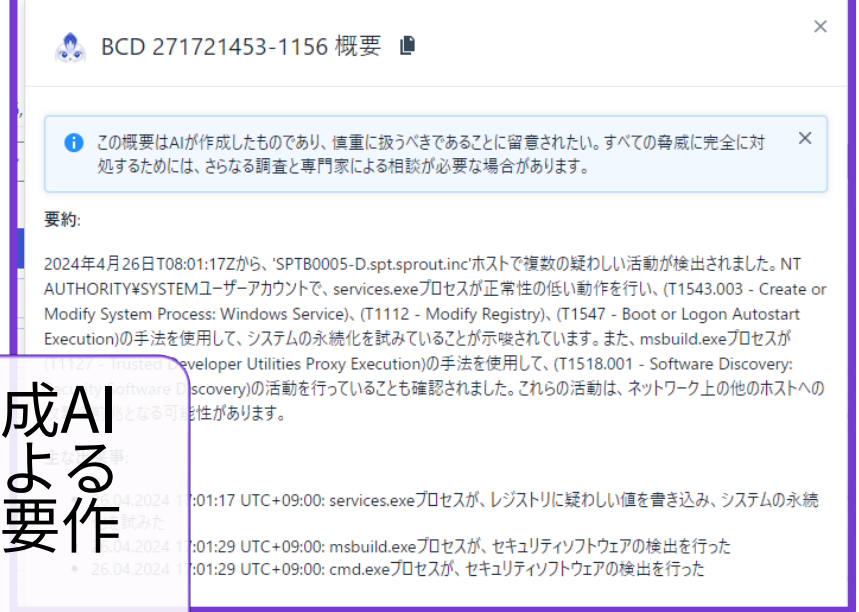


# EDRを車に例えると



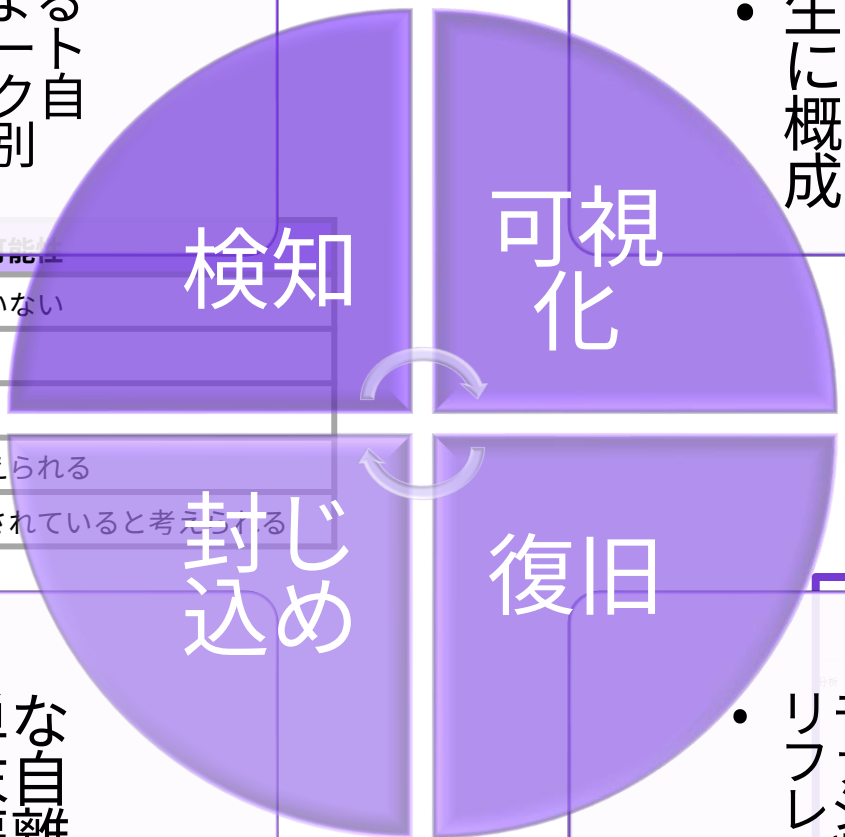


# Elements EDR の特長



- AIによるアラートリスク自動判別

- 生成AIによる要作生成



スコア	重大度	異常なサイバー活動の可能性
0		可能性があるがリスクとしては判断できていない
36 ~ 65		可能性はあるがリスクとしては低い
66 ~ 75		可能性はあるが大きな影響はない
76 ~ 90		可能性は高く、深刻な被害をもたらすと考えられる
91 ~ 100		可能性は高く、重要なホストが危険にさらされていると考えられる



- 簡単な端末自動隔離

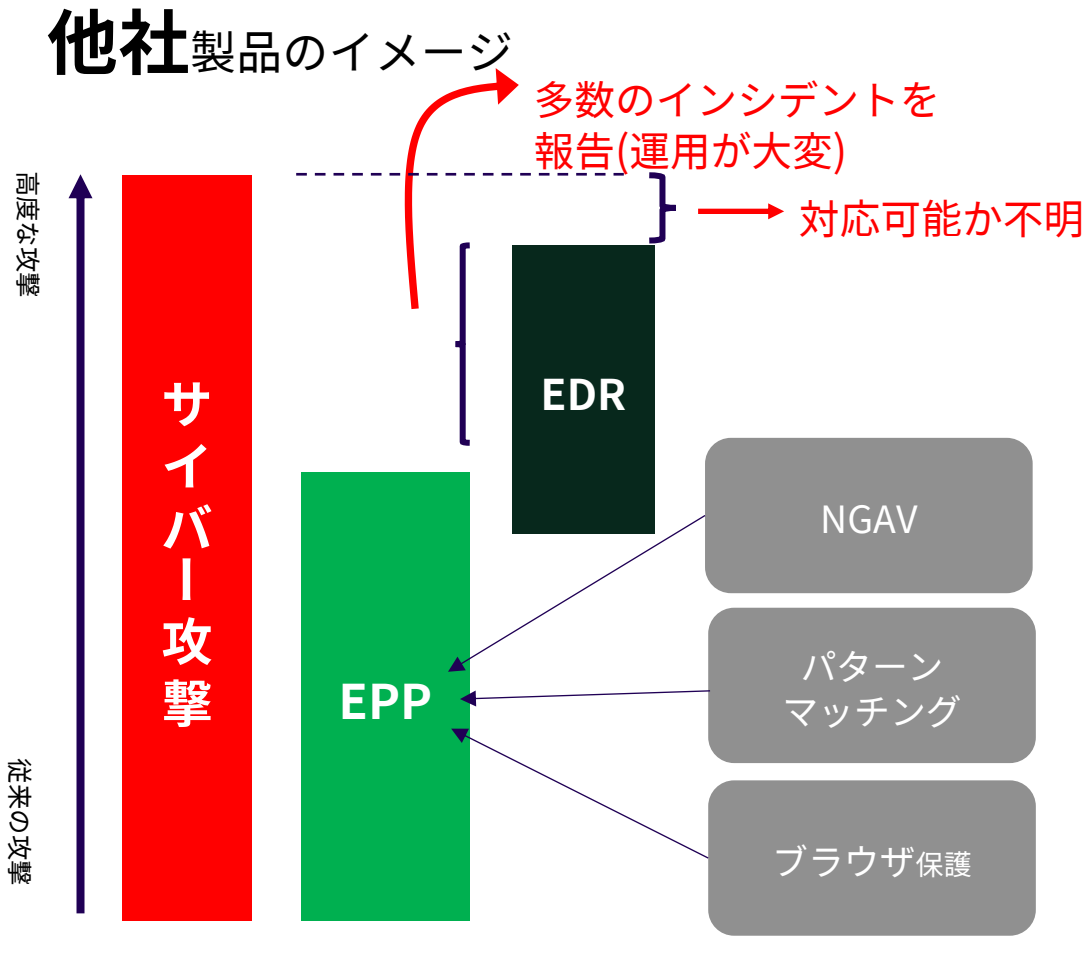
- リモートファイル、レジストリ削除



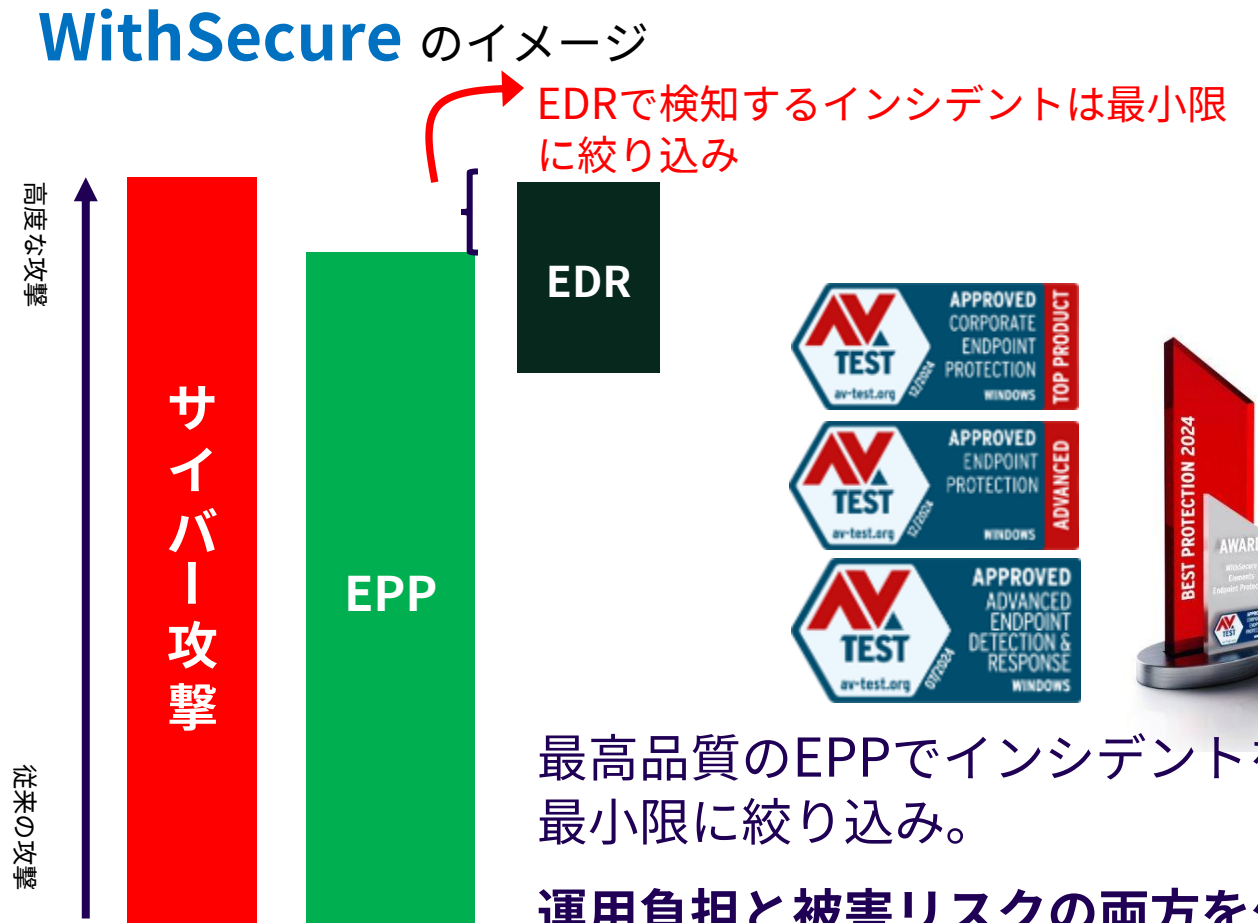
- プロセスの停止
- ファイル取得
- ファイル削除

# WithSecure Elements EDR

最高性能のEPPと組み合わせることで運用負荷を最小限に抑える！



EPPでカバー出来る範囲が少ない



最高品質のEPPでインシデントを最小限に絞り込み。

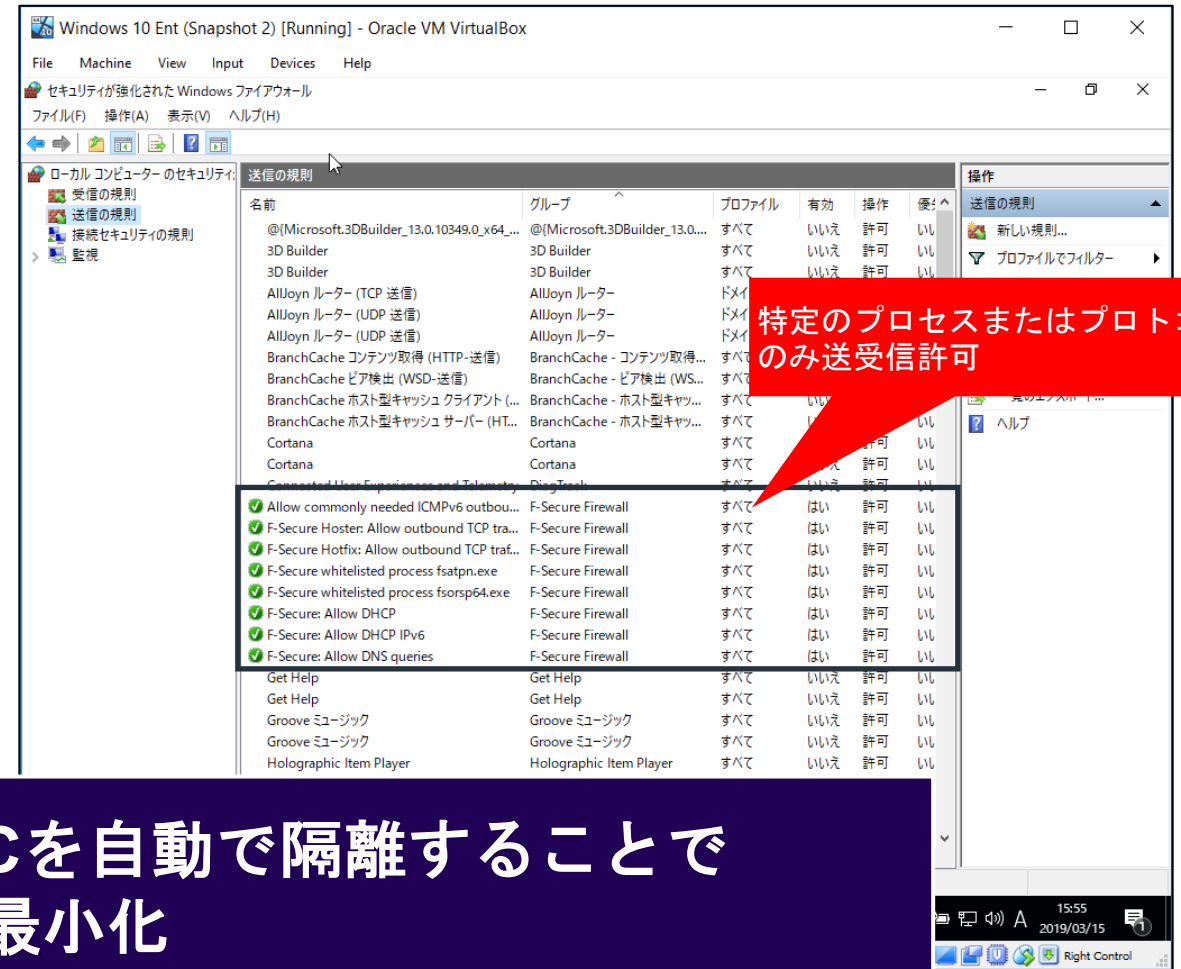
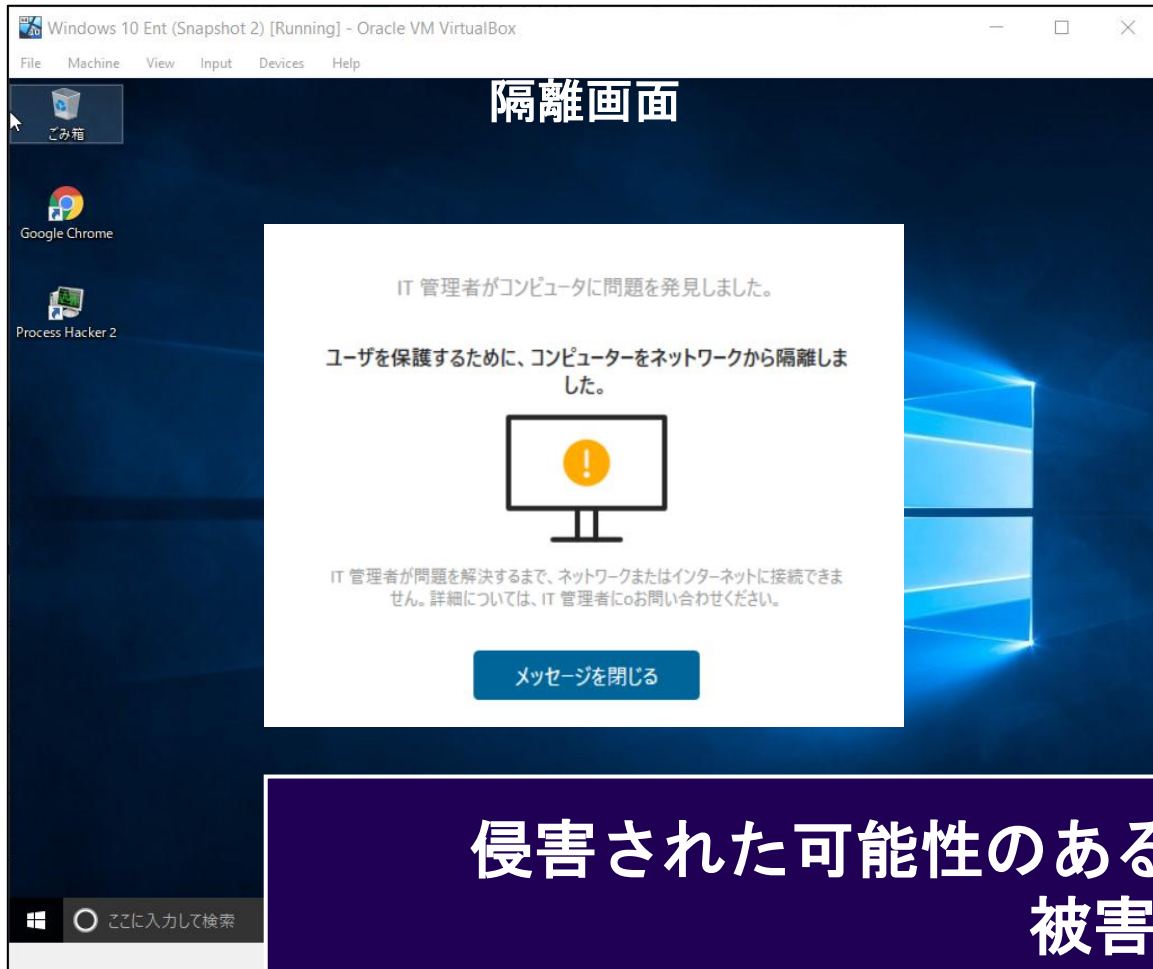
運用負担と被害リスクの両方を少なくできる！



# WithSecure Elements EDR : ホストを隔離

リスクレベルの設定により自動隔離可能

隔離後のWindows Firewallの設定



侵害された可能性のあるPCを自動で隔離することで被害を最小化

# WithSecure Elements EPP + EDR おすすめポイント

- ✓ウィズセキュア独自のEPPで高度な検知が前提なため **運用負担が少ない**
- ✓危険を検知したら、設定した危険度に応じて **自動隔離**し 被害拡大防止
- ✓EDRへライセンス変更したら **ワンクリック** でEDR機能がONにできる

# EPP移行に伴う優遇措置について（既存ユーザ様向け）

ビジネススイート製品は **2027年12月31日**に製品の提供・サポートの終了予定となるため、以下の通り移行優遇措置をいたします。

✓ **Elements 製品でのご契約後から最大1年間**はビジネススイート製品の併用を許諾いたします  
(ビジネススイート製品の証書発行はされない為、従来使用頂いているキーコードをご流用ください)

✓ **2025年中※<sup>1</sup>**にビジネススイート製品から Elements 製品に移行頂けるお客様におかれましては、**従来の据え置き価格**にてご提供いたしますので、**1年以内の移行完了**をお願いいたします

※1：2025年12月22日ご注文到着分まで

※2：特価対応分などは除く

(参考) [ビジネススイート製品の価格改定ならびに EOL に関するお知らせ](https://www.withsecure.com/content/dam/with-secure/ja/resources/2025-04-01_Important_Notice-BS_Price_Change_and_EOL_Notification.pdf)

[https://www.withsecure.com/content/dam/with-secure/ja/resources/2025-04-01\\_Important\\_Notice-BS\\_Price\\_Change\\_and\\_EOL\\_Notification.pdf](https://www.withsecure.com/content/dam/with-secure/ja/resources/2025-04-01_Important_Notice-BS_Price_Change_and_EOL_Notification.pdf)

W / T H<sup>®</sup>  
secure

# Appendix

# 製品比較表 - クライアントセキュリティ(Windows) vs. Elements EPP for Computers

機能	機能の概要	クライアントセキュリティ	クライアントセキュリティ プレミアム	Elements EPP for Computers	Elements EPP for Computers Premium
マルウェア・スパイウェア防御	パターンファイルによる既知のマルウェア、スパイウェア防御	●	●	●	●
ディープガード	機械学習を用いた振る舞い検知による未知のマルウェア・スパイウェアの対策	●	●	●	●
ファイアウォール	Windowsファイアウォールを使用したネットワークアクセスの制御	●	●	●	●
デバイス制御	ハードウェアデバイスの制御	●	●	●	●
Webトラフィックスキャン	Webトラフィック(HTTP)に含まれる怪しいファイルの対策	●	●	●	●
ブラウザ保護	怪しいWebサイトへの接続の対策	●	●	●	●
Webコンテンツ制御	コンテンツに基づいて、Webサイトへの接続の制御		●	●	●
接続制御	金融サイト接続時の情報漏洩対策として、他のネットワーク通信の制御		●	●	●
ソフトウェアアップデート	Windowsやサードパーティ製品のセキュリティパッチの適用・管理		●	●	●
データガード	フォルダ、ファイルにアクセス出来る実行ファイルの制御		●		●
アプリケーション制御	アプリケーションの起動、動作の制御		●		●
製品自体の自動更新	自動的に製品のバージョンアップやモジュールの自動更新			●	●
非インターネット環境	非インターネット環境での利用について	●	●	Elements Connector (無償ソフト)を併用し対応を予定	Elements Connector (無償ソフト)を併用し対応を予定
集中管理	製品の集中管理ソフト (無償)	ポリシーマネージャ	ポリシーマネージャ	Elements Security Center	Elements Security Center

- Elementsシリーズは製品の自動バージョンアップ機能があるため、オンプレミス製品のような手動バージョンアップ作業が不要となります。
- Elementsシリーズは弊社クラウド上のElements Security Centerで管理するため、各端末にインターネット接続環境が必要となります。
- ポリシーマネージャで集中管理された各端末にElementsシリーズをポリシーベースでインストールできるため、短時間で移行が可能です。

※非インターネット環境でのElementsシリーズの利用については、Elements Connectorを併用することで運用可能となります。  
Elements Connectorを導入した端末がインターネットに接続されていれば、配下の端末をクラウド管理できるようになります。  
ただしElements Connector導入端末だけはインターネット接続が必要となるので、完全クローズ環境ではご利用いただけません。

# 製品比較表 - Windowsサーバセキュリティ vs. Elements EPP for Servers

機能	機能の概要	Windowsサーバセキュリティ	Windowsサーバセキュリティプレミアム	Elements EPP for Servers	Elements EPP for Servers Premium
マルウェア・スパイウェア防御	パターンファイルによる既知のマルウェア、スパイウェア防御	●	●	●	●
ディープガード	機械学習を用いた振る舞い検知による未知のマルウェア・スパイウェアの対策	●	●	●	●
ファイアウォール	Windowsファイアウォールを使用したネットワークアクセスの制御	●	●	●	●
デバイス制御	ハードウェアデバイスの制御	●	●	●	●
Webトラフィックスキャン	Webトラフィック(HTTP)に含まれる怪しいファイルの対策	●	●	●	●
ブラウザ保護	怪しいWebサイトへの接続の対策	●	●	●	●
Webコンテンツ制御	コンテンツに基づいて、Webサイトへの接続の制御		●	●	●
ソフトウェアアップデート	Windowsやサードパーティ製品のセキュリティパッチの適用・管理		●	●	●
データガード	フォルダ、ファイルにアクセス出来る実行ファイルの制御		●		●
アプリケーション制御	アプリケーションの起動、動作の制御		●		●
製品自体の自動更新	自動的に製品のバージョンアップやモジュールの自動更新			●	●
非インターネット環境	非インターネット環境での利用について	●	●	Elements Connector (無償ソフト) を併用し対応を予定	Elements Connector (無償ソフト) を併用し対応を予定
集中管理	製品の集中管理ソフト (無償)	ポリシーマネージャ	ポリシーマネージャ	Elements Security Center	Elements Security Center

- Elementsシリーズは製品の自動バージョンアップ機能があるため、オンプレミス製品のような手動バージョンアップ作業が不要となります。
- Elementsシリーズは弊社クラウド上のElements Security Centerで管理するため、各端末にインターネット接続環境が必要となります。
- ポリシーマネージャで集中管理された各端末にElementsシリーズをポリシーベースでインストールできるため、短時間で移行が可能です。

※非インターネット環境でのElementsシリーズの利用については、Elements Connectorを併用することで運用可能となります。Elements Connectorを導入した端末がインターネットに接続されていれば、配下の端末をクラウド管理できるようになります。ただしElements Connector導入端末だけはインターネット接続が必要となるので、完全クローズ環境ではご利用いただけません。

# 製品比較表 - Linux Security 64 vs. Elements EPP for Linux

機能	機能の概要	Linux Security 64	Elements EPP for Linux
マルウェア・スパイウェア防御	パターンファイルによる既知のマルウェア、スパイウェア防御	●	●
マニュアルスキャン	コマンドによるスキャンの実行	●	●
スケジュールスキャン	スケジュールによる定期スキャン	●	●
完全性検査	登録したファイルに対してファイルの改竄を検出	●	●
スタンドアロン対応	集中管理せずスタンドアロンでの運用	●	
製品自体の自動更新	自動的に製品のバージョンアップやモジュールの自動更新	●	●
製品バージョンの固定化	自動バージョンアップせずバージョンを固定（特定バージョンのみ）	●	
非インターネット環境	非インターネット環境での利用について	●	Elements Connector (無償ソフト) を併用し対応予定
集中管理	製品の集中管理ソフト（無償）	ポリシーマネージャ	Elements Security Center

- Elementsシリーズは弊社クラウド上のElements Security Centerで管理するため、各端末にインターネット接続環境が必要となります。

※非インターネット環境でのElementsシリーズの利用については、今後リリース予定のElements Connector（Linux版）を併用することで運用可能となります。Elements Connectorを導入した端末がインターネットに接続されていれば、配下の端末をクラウド管理できるようになります。ただしElements Connector導入端末だけはインターネット接続が必要となるので、完全クローズ環境ではご利用いただけません。

1ライセンスから購入可能  
コスト最強、クラウド管理型エンドポイントセキュリティ

## WithSecure™ Elements Endpoint Protection (EPP)

クラウド管理型製品は専用の管理サーバーの導入が不要で、マルチプラットフォームに対応しています。  
(対応OS: Windows | Mac | Linux | Android | iOS)



### WithSecure™ Elements EPPの特長

- 1ライセンスから購入が可能
- ウィズセキュア独自のディープガードやAIによる**多層防御**
- ランサムウェア対策**に最適なロールバックとデータガード機能を搭載
- バンキングサイト接続保護機能により、**安全に銀行のサイトへアクセス可能**
- 3階層に対応した**マルチテナント**により、販売店様による管理を実現

### ランサムウェア対策に特化した機能 (Windows版のみ)

- Dataguard(データガード)**
  - ランサムウェアに感染時に指定したファイルを暗号化ブロック
- Rollback (ロールバック) 機能**
  - ランサムウェアのような悪意のある攻撃を検知し、侵害前 (暗号化前) の状態に戻すことが可能

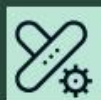
### 多様な機能を搭載!



Deepguard\*



WEBコンテンツ  
制御



統合パッチ  
管理



デバイス  
制御\*



アプリケーション  
制御\*



Dataguard\*

\* Windows版に搭載されている機能です。

◇ Dataguard 及びアプリケーション制御はプレミアム版に搭載されている機能です。

### 販売店様の管理に最適な最大3階層マルチテナント

販売店様が販売したユーザー様については、3階層までElementsのクラウド管理ポータル上で保有ライセンスの状態が確認可能!

- 2階層以上管理希望の場合は諸条件ありのため、メーカーまで要問合せ。



### WithSecure™ Elements EPPシリーズ



Windows/Mac向け:	WithSecure™ Elements EPP for Computers (スタンダード or プレミアム)
Windowsサーバー向け:	WithSecure™ Elements EPP for Servers (スタンダード or プレミアム)
Linuxサーバー向け:	WithSecure™ Elements EPP for Linux
iOS/Android向け:	WithSecure™ Elements EPP for Mobiles

### ウィズセキュア株式会社パートナー営業本部

〒105-0004 東京都港区新橋2丁目2番9号 KDX 新橋ビル2階  
Tel: 03-4578-7710 | E-mail: [japan@withsecure.com](mailto:japan@withsecure.com) | <https://www.withsecure.com/>

中小企業に最適！1ライセンスから購入可能  
クラウド管理型EDRソリューション

## WithSecure™ Elements EDR & EPP

侵害時の被害を最小化しビジネスを止めない運用を実現

WithSecure™ Elements EDR & EPPは  
企業のIT環境とセキュリティ状況を単一の統  
合管理コンソール上に可視化し、サイバー攻  
撃を迅速に検知・表示し、ガイダンスに沿っ  
た侵害の対応が可能  
(対応OS: Windows/Mac/Linux)



### 自動車保険に例えると…



ドラレコやエアバッグを装着する感覚でEDR導入がおすすめ  
**安全装置があると万が一の時に安心！**

ドラレコ搭載していると、事故発生時の運転状況を可視化  
エアバッグを装着していると、事故発生時の被害を最小化

### EDRを導入すると

感染時の感染経路が確認でき、  
自動隔離で被害拡大を阻止し、被害を最小限にできます。

## WithSecure™ Elements EDR & EPP のポイント

- 1ライセンスから購入が可能
- W/Elements EPPは高度な検知機能を備えており、**運用負担を大幅に減らせます**
- 危険を検知したら、設定した危険度に応じて **自動隔離**し被害拡大を阻止
- Elements Security Center (管理ポータル) 上から **ワンクリック** でEDR機能をONにできる

入れておくだけで安心できる

- インシデントのリスクレベルに応じて、端末の**自動隔離**が可能
- 調査する場合に**追跡のためのデータを遠隔操作**でも簡単に取得可能

自動隔離ができるのは  
ウィズセキュアだけ

他社は手動隔離のみ



### SOCサービスによるセキュリティ体制の堅牢化



- W/ Elements EDRはSOCサービスなしでも効果的です。
- より堅牢なセキュリティ体制構築のため、EDR導入後に弊社パートナー様のSOCサービスを導入できます。

### 生成AIアシスタント W/ Luminen が検知した脅威を要約

- 標準搭載の生成AIアシスタント **W/ Luminen** が、感染時の感染経路の分析の要約など、セキュリティイベントの概略を要約。
- **W/ Luminen**は、ワンクリックで社内やお客様への報告ツールとして活用できるため、EDRの運用工数の削減にお役立ていただけます。

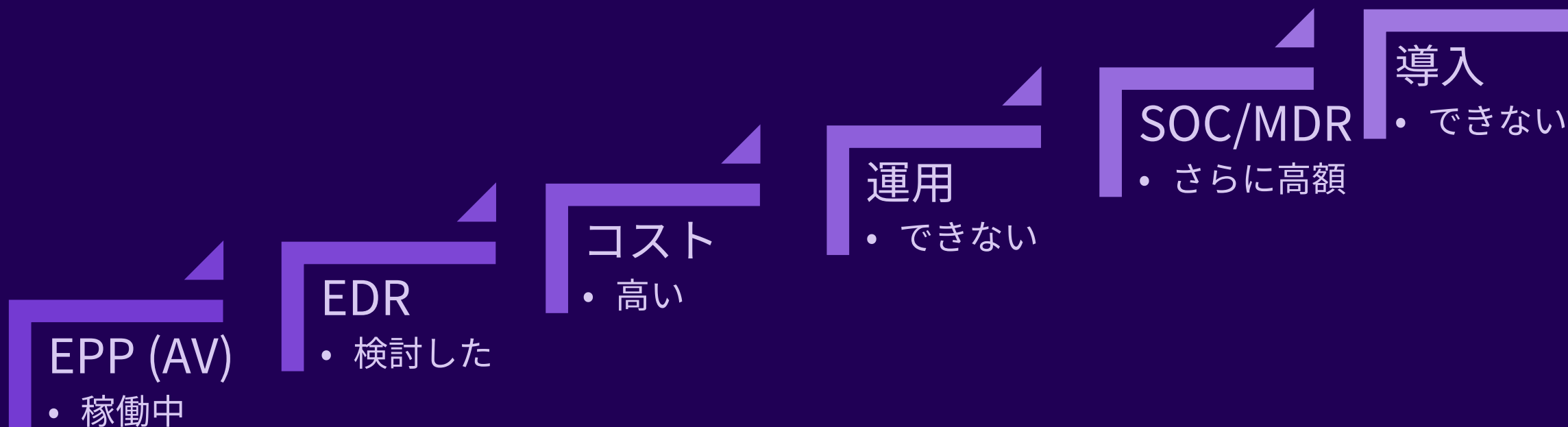


### お問い合わせ先

ウィズセキュア株式会社 パートナー営業本部

- ・ 〒105-0004 東京都港区新橋2丁目2番9号 KDX 新橋ビル 2階
- ・ E-mail: [japan@withsecure.com](mailto:japan@withsecure.com) | <https://www.withsecure.com/>

# EDRあるある (ハードルが高い?)



- EDRは導入コストもかかるうえ、その後の運用も難しいイメージ
  - EPPだけでは防げない脅威がある (ゼロデイ攻撃・ゼロトラスト等)
- いまの時代の企業としての責任
  - EPP+EDRは説明責任を果たすためにも最低限必要なものに
- 難しくて高いイメージのEDRをどう訴求・説得・導入したらいいのか…

✓ 必須項目：EDRはEPPを含めて比較する

WithSecure EPP+EDR

他社(例:EDR発祥ベンダー)



非常に強い

EPPの防御力

あまり強くない



高くない

EDRの運用負荷

高い



1年

ログ保存期間

30日



あとから解析可

解析

消失前に対処要



ニーズに応じて

監視体制

常時監視必要



よかった!!

その結果？

後悔？



# WithSecure Elements EDR:生成AI“Luminen”

## 生成AI「Luminen」活用によるインシデントの要約が可能

Broad Context Detection

Broad Context Detection イベント検索

< 検出リストに戻る

Broad Context Detection 1の2 < >

ID: 390304450-3, カテゴリ: システムまたはツールの誤用

ステータス

新規

クイックアクション

Luminenで分析する

影響されているデバイスを隔離

デバイスをスキャン

フォレンジックパッケージを収集する

タスクを列挙する

プロセスを列挙する

詳細 応答アクション - プロセスの詳細から入手できます。

WithSecureにエスカレーション

エスカレーション

概要 処理ツリー タイムライン 分析 デバイスの詳細 コメント ログ



NLS-WP-01



EXPLO



BCD 390304450-3 概要

要約:

2025年2月26日23:48:23Zから23:48:24Zの間、NLS-WP-01ホストのユーザー'umegu'によって、いくつかの疑わしいPowerShellアクティビティが検出されました。cmd.exeプロセスの子プロセスとして、PowerShellが起動され、隠しウィンドウを使用したり、Invoke-Expressionを使用したりするなど、パイロードの特徴を示す動作が確認されました。これらの動作は、(T1059.001 - Command and Scripting Interpreter: PowerShell)および(TA0002 - Execution)に関連付けられています。検出された動作の重大度は中から高レベルでした。

主要なイベント:

- 26.02.2025 23:48:23 UTC+00:00: cmd.exeプロセスの子プロセスとしてPowerShellが起動され、隠しウィンドウを使用したり、Invoke-Expressionを使用したりするなど、パイロードの特徴を示す動作が確認されました。
- 26.02.2025 23:48:24 UTC+00:00: PowerShellコマンドラインがパイロードの特徴を示すことが検出されました。
- 26.02.2025 23:48:24 UTC+00:00: PowerShellでInvoke-Expressionが使用されたことが検出されました。

生成AIが作成する平易な日本語でインシデントを解説  
SOCからの詳細解析、対応の前に簡易的な状況把握がし易い

# WithSecureの 生成AI:Luminen



Hoot there!  
How can I assist you today?

- W/Luminenは、多忙で人員不足のサイバー防御担当者向けに、複雑なサイバーセキュリティタスクを簡単に理解しやすく、効率的に行うための、状況に応じた実行可能なガイダンスを提供します。
- WithSecureは、AIアルゴリズムを責任を持って使用することで、高品質と厳格なプライバシー基準を維持し、エネルギー消費量と環境への影響を最小限に抑えています
- Luminenのビジョンは、より深い分析でテクノロジーと連携し、アクションを自動化し、より豊富なコンテキストを提供し、データと柔軟に会話することです。

# “Luminen” 新搭載！ 生成AIでEDRの運用をラクにしませんか？

「中」以上

プロセスの詳細

WIN10-M37  
8追加されたプロセス

userinit.exe 解除

パス %systemroot%\system32

explorer.exe 解除

ユーザ名 WIN10-M37\konary  
PID 7408  
パス %systemroot%\system32  
SHA1 f2b5e530b453a69cf23f2166e48bcf5749a9429aef  
実行開始 21.09.2024 11:41:22 UTC+00:00  
実行終了 21.09.2024 11:41:29 UTC+00:00

検出: すべて展開 すべて閉じる

検出 1/3: Recon activities by injected process [High]  
21.09.2024 11:41:22 UTC+00:00

検出 2/3: Remote thread creation by detected process [High]  
21.09.2024 11:41:23 UTC+00:00

検出 3/3: Suspicious remote thread by detected process

検出: Interactive command prompt launched by compromised process [中] 21.09.2024 11:34:21 UTC+00:00

notepad.exe spawned the interactive command line process cmd.exe. This is sign that a compromised process is used to launch an interactive shell that can be used to run commands interactively.  
T1059.003 検出 TA0002 検出  
bddd99fc-780d-11ef-8f93-0242ac1



EDRイベント…  
ログがいっぱい出力されるけど  
何のことだかわからない…



こんにちは！Luminenです。  
ボタンひとつでEDRイベントを要約  
して分かりやすく表示しますよ。



すごい!!  
これなら何が  
起きたかわかる!!

## Luminen使用時 「概要」 サンプル

BCD 1586476-18985 概要

この概要はAIが作成したものであり、慎重に扱うべきであることに留意されたい。すべての脅威に完全に対処するためには、さらなる調査と専門家による相談が必要な場合があります。

要約:

2024年9月21日 11時34分07秒に、WIN10-M37ホストのユーザー konary によって新しいプロセス process\_ghosting.exe が実行されました(T1204 - ユーザー実行)。その後、プロセスの即時注入(T1055 - プロセスの注入)や、notepad.exe から cmd.exe への異常なプロセス実行(T1059.003 - コマンドとスクリプト インタープリター: Windows コマンド シェル、T1059.001 - コマンドとスクリプト インタープリター: PowerShell、T1002 - 実行)が検出されました。さらに、ホスト上で複数の情報収集活動(T1016 - システム ネットワーク構成の検出、T1033 - システム所有者/ユーザーの検出、T1049 - システム ネットワーク接続の検出、T1057 - プロセスの検出、T1082 - システム情報の検出)が行われました。

主要な出来事:

- 21.09.2024 11:34:07 UTC+00:00: ユーザー konary が新しいプロセス process\_ghosting.exe を実行
- 21.09.2024 11:34:09 UTC+00:00/21.09.2024 11:41:22 UTC+00:00: プロセスの注入、異常なプロセス実行、情報収集活動が検出
- 21.09.2024 11:41:22 UTC+00:00: explorer.exe プロセスが注入された可能性があり、さらに情報収集活動が行われた