CHECK POINT™

YOU DESERVE THE BEST SECURITY

# Harmony Endpoint ハンズオン勉強会

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社

# Agenda

- 攻撃者の行動と対策のポイント
- Harmony Endpoint の概要
- Harmony Endpoint 導入の流れ
- インシデントハンドリングでの活用
- Harmony Endpoint の構成概要
- 設定画面の概要
- クライアントのインストール
- クライアントソフトウェアの概要
- クライアントのアップグレード
- バーチャルグループによる管理
- ポリシーバージョンの確認
- Threat Prevention 設定
- 除外設定
- コンピュータの隔離、解放
- ログの表示
- フォレンジックレポート
- Threat Hunting
- アラート通知設定
- アンインストールパスワードの設定
- クライアントのアンインストール

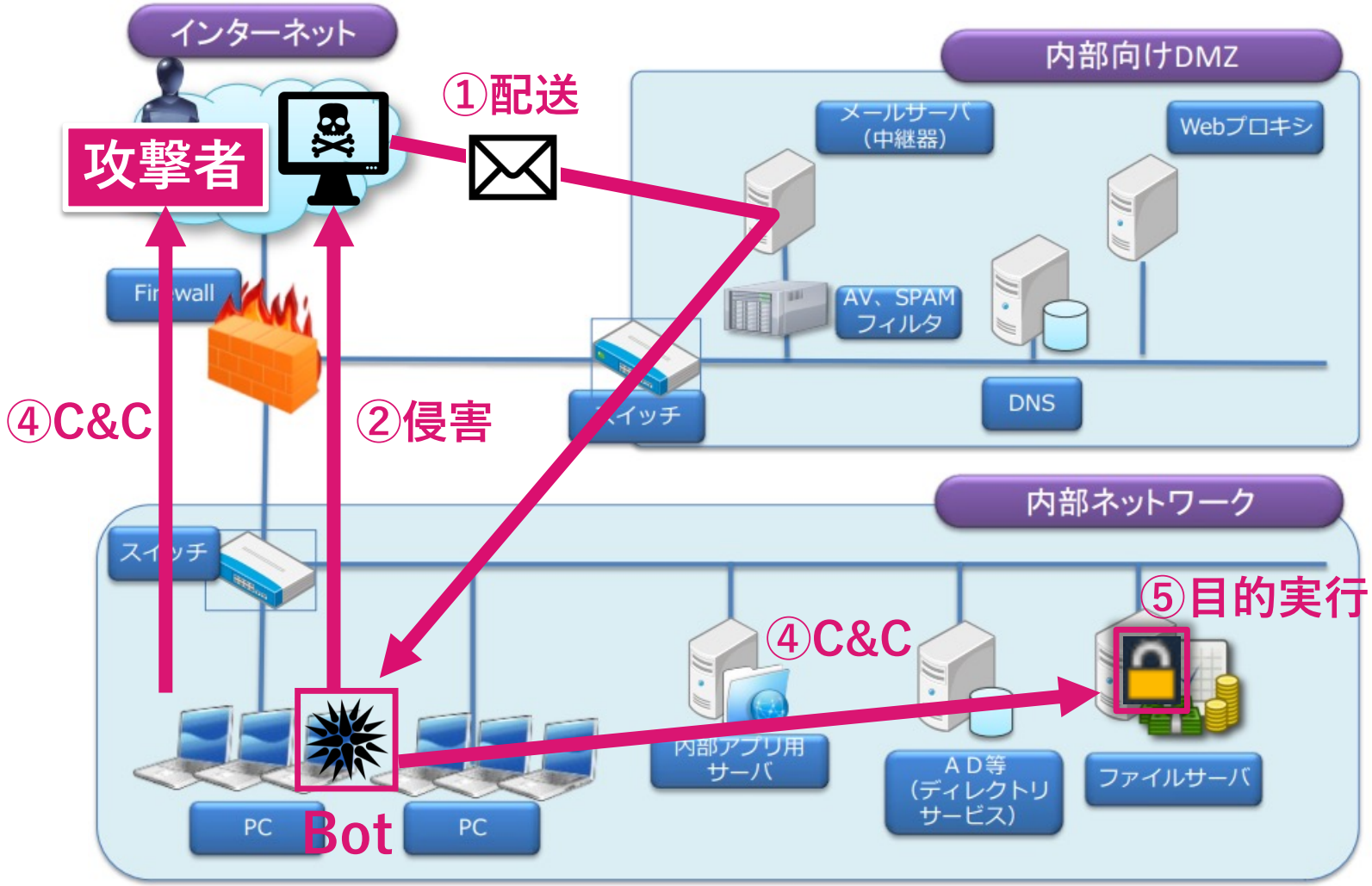
# 攻撃者の行動と対策のポイント

YOU DESERVE THE BEST SECURITY

# サイバーキルチェーンとは

- 2009年に米国のロッキード・マーティン社が提唱したサイバー攻撃のフレームワーク
- サイバー攻撃における攻撃者の行動を７つのフェーズに分類
- 攻撃のチェーンを断ち切ることで攻撃目的の達成を阻止可能

# サイバー攻撃のイメージと防御機能

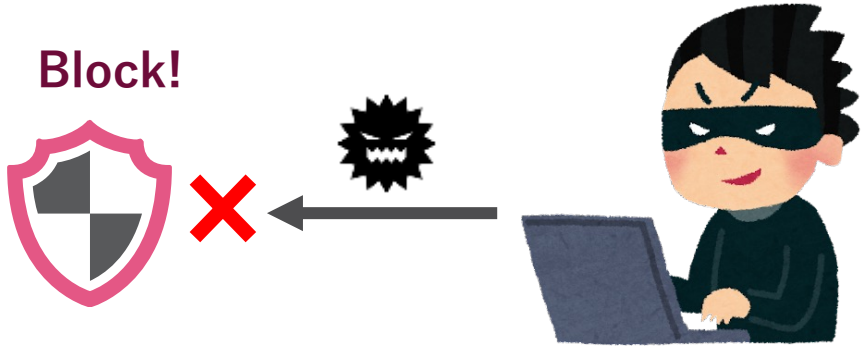



組織内ネットワーク構成のモデル

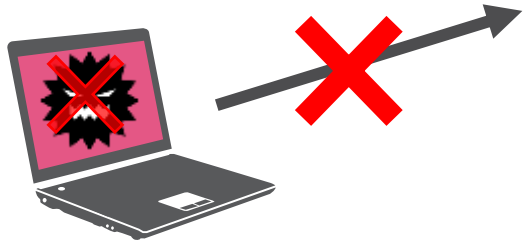
| | |
|---|---|
| 偵察 | • Zero-Phishing |
| 武器化 | • — |
| 配送 | • Anti-Malware |
| 侵害 | • Anti-Malware<br>• URLフィルタ<br>• **Threat Emulation,Threat Extraction**<br>• Anti-Exploit |
| 侵入 | • Anti-Malware |
| C&C | • **Anti-Bot**<br>• Behavioral Guard |
| 実行 | • **Anti-Ransomware** |

# サイバーセキュリティ対策のポイント

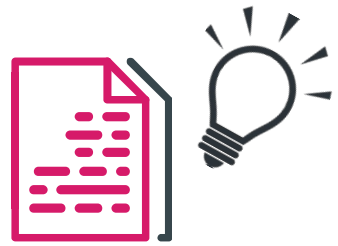
**1** **検知＆防止**
まずはマルウェアに感染しないようにする！




**2** **封じ込め**
万が一感染した場合、マルウェアによる影響を最小限に抑える！



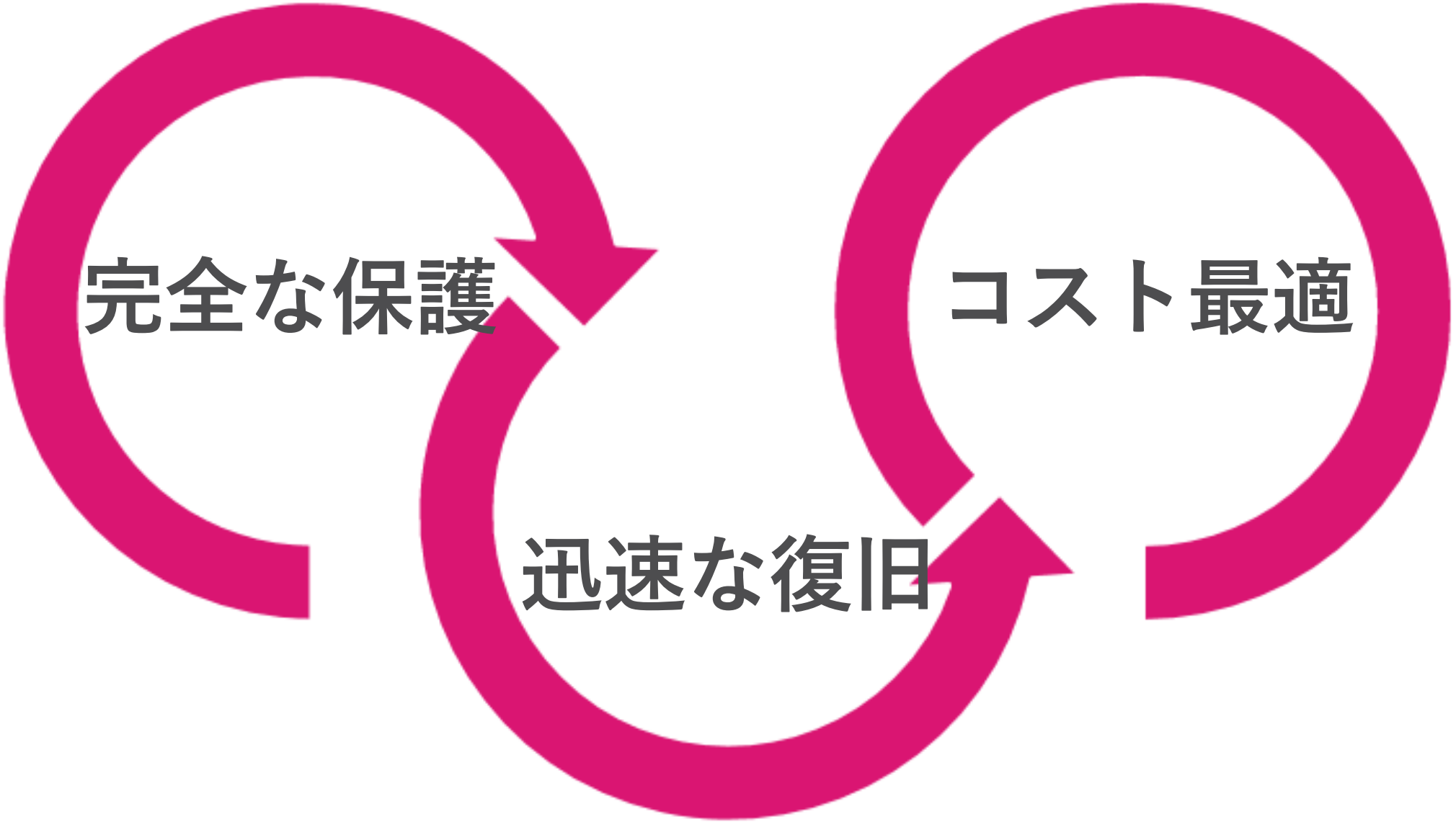
**3** **可視化と分析**
マルウェアを駆除したあと、事後対応や再発防止のために、なにがあったのかを把握する！



# HARMONY ENDPOINT の概要

YOU DESERVE THE BEST SECURITY

# Harmony Endpoint の特徴



# エンドポイントに必要なすべての保護を提供

## 攻撃からの防御
EPP & NGAV

## 攻撃の検知と対応
EDR

### 検知＆防止


アンチ・マルウェア


サンドボックス


ファイル無害化


ゼロ・フィッシング

### 封じ込め


アンチ・ランサムウェア


アンチ・ボット


アンチ・エクスプロイト

### 可視化と分析


フォレンジックレポート


Threat Hunting

# Harmony Endpoint の先進の防御技術

## サンドボックス

OSレベルとCPUレベルの
統合型サンドボックスで
攻撃を遮断

## ファイル無害化

ファイルの無害化による
安全性と生産性の両立

## ゼロフィッシング

フィッシングサイトから
ユーザの認証情報を保護

## アンチ・ランサムウェア

ランサムウェアの攻撃を停止し、
ファイルを自動復旧

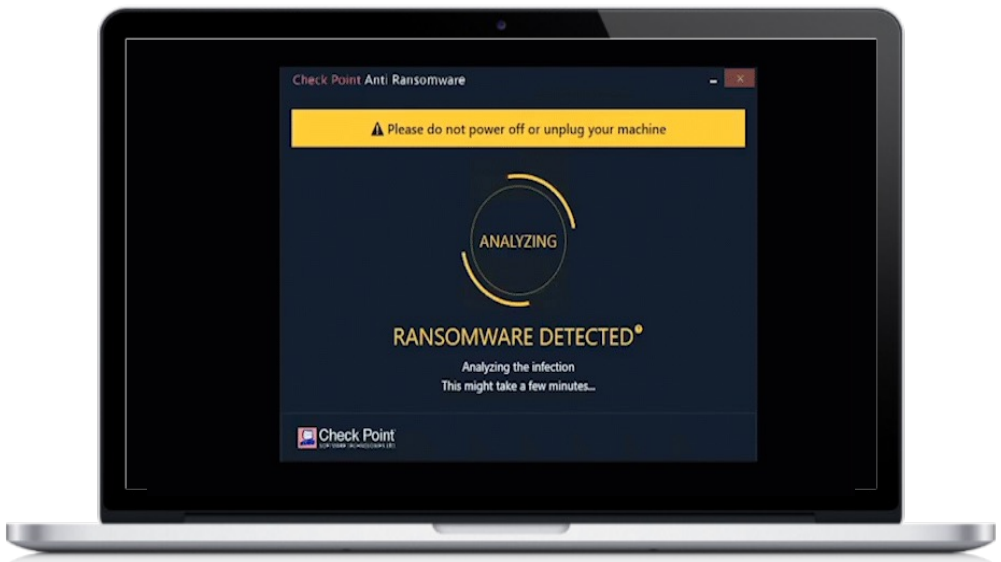
## アンチ・ボット

攻撃者との通信を遮断し、
攻撃の拡大を阻止

## フォレンジックレポート

独自の解析技術による
正確性の高い攻撃解析

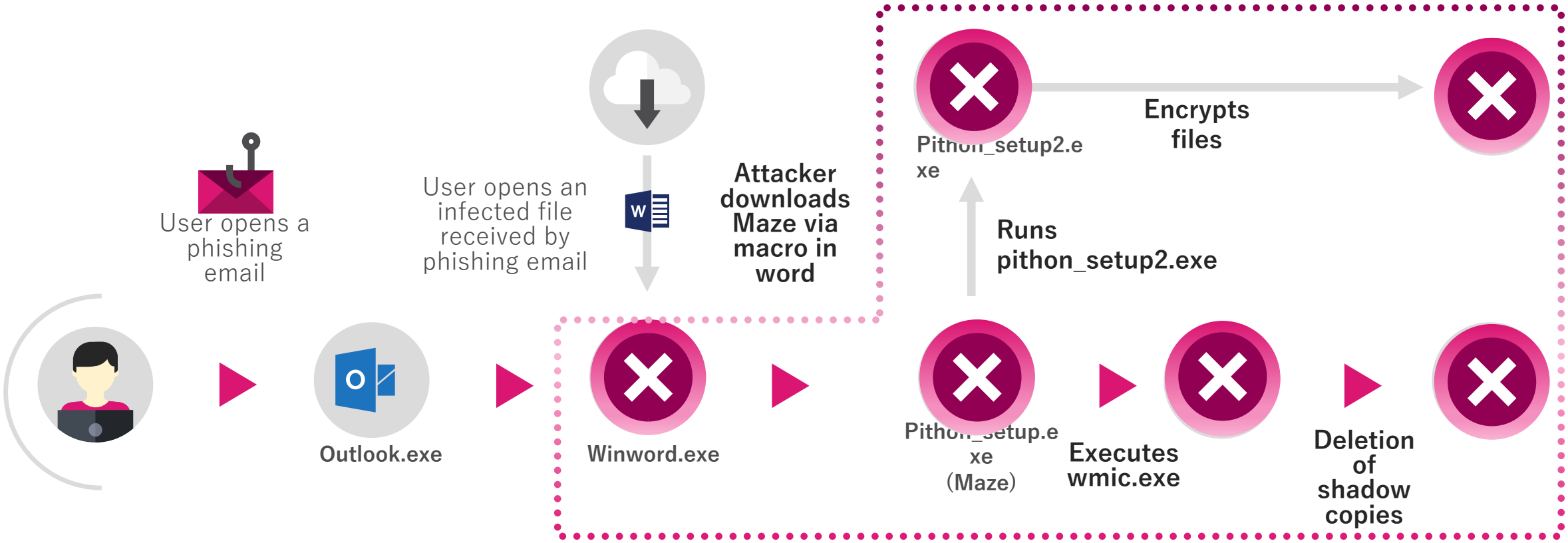
# 検知、調査、修復作業の 90% を自動化




**自動化**

- あらゆるイベントを監視、収集
- 攻撃を検知
- 悪意のある活動を隔離
- サイバーキルチェーン全体をクリーンナップ
- 暗号化されたファイルを復元
- フォレンジックレポートを提供

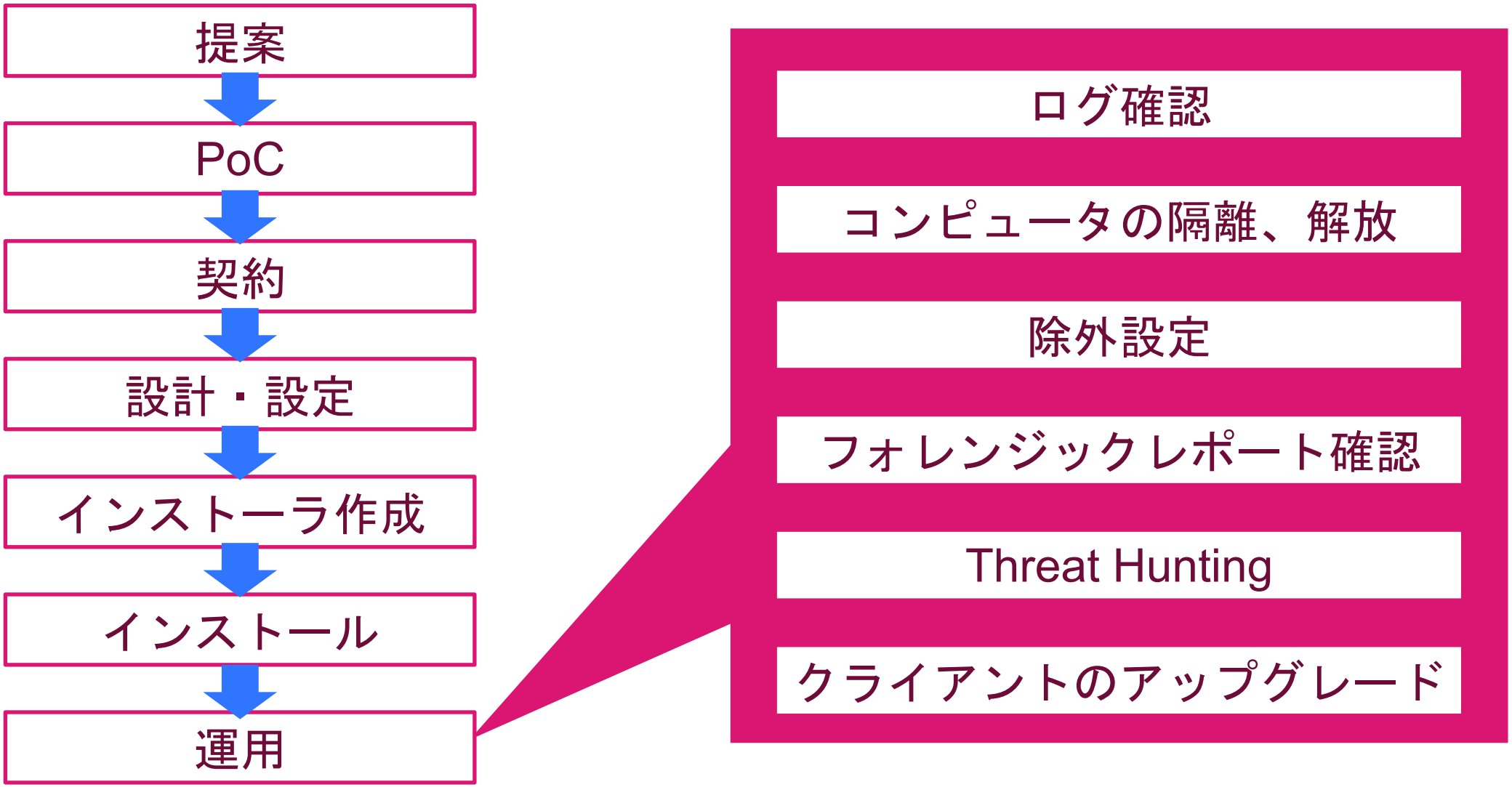
# サイバーキルチェーン全体を自動的かつ完全に修復し、ビジネスの継続性を確保



# HARMONY ENDPOINT 導入の流れ

YOU DESERVE THE BEST SECURITY

# Harmony Endpoint 導入の流れ

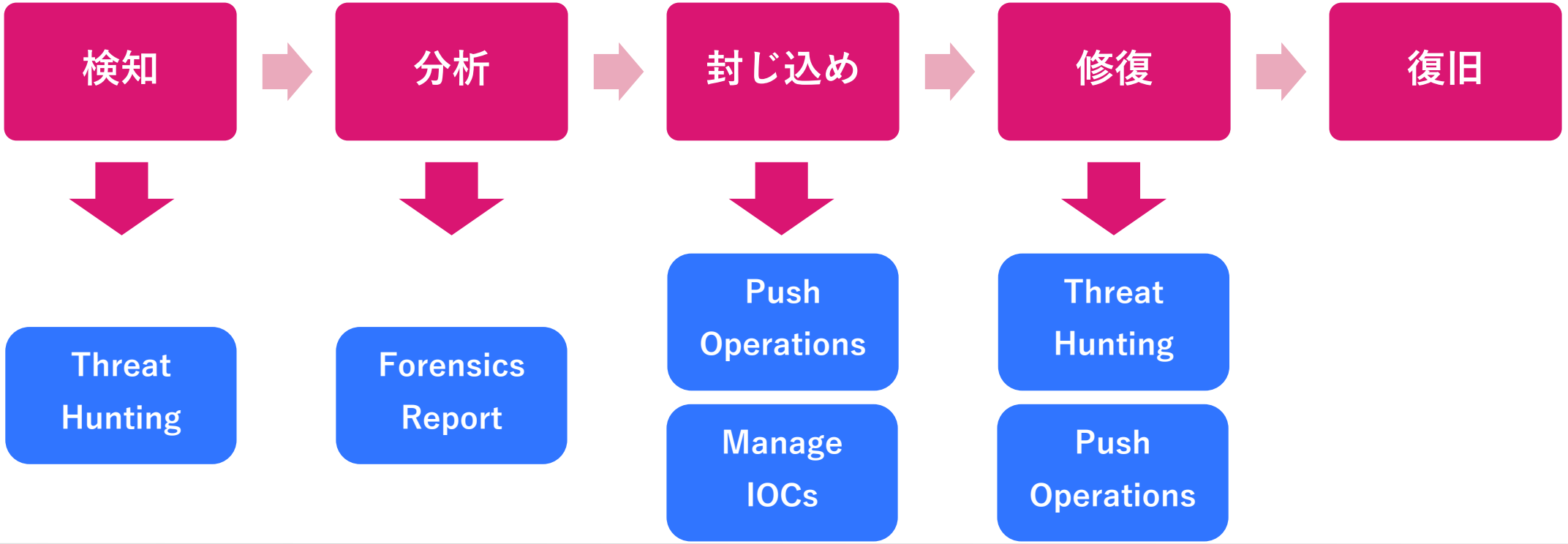


# インシデントハンドリングでの活用

YOU DESERVE THE BEST SECURITY

# インシデントハンドリングでの活用

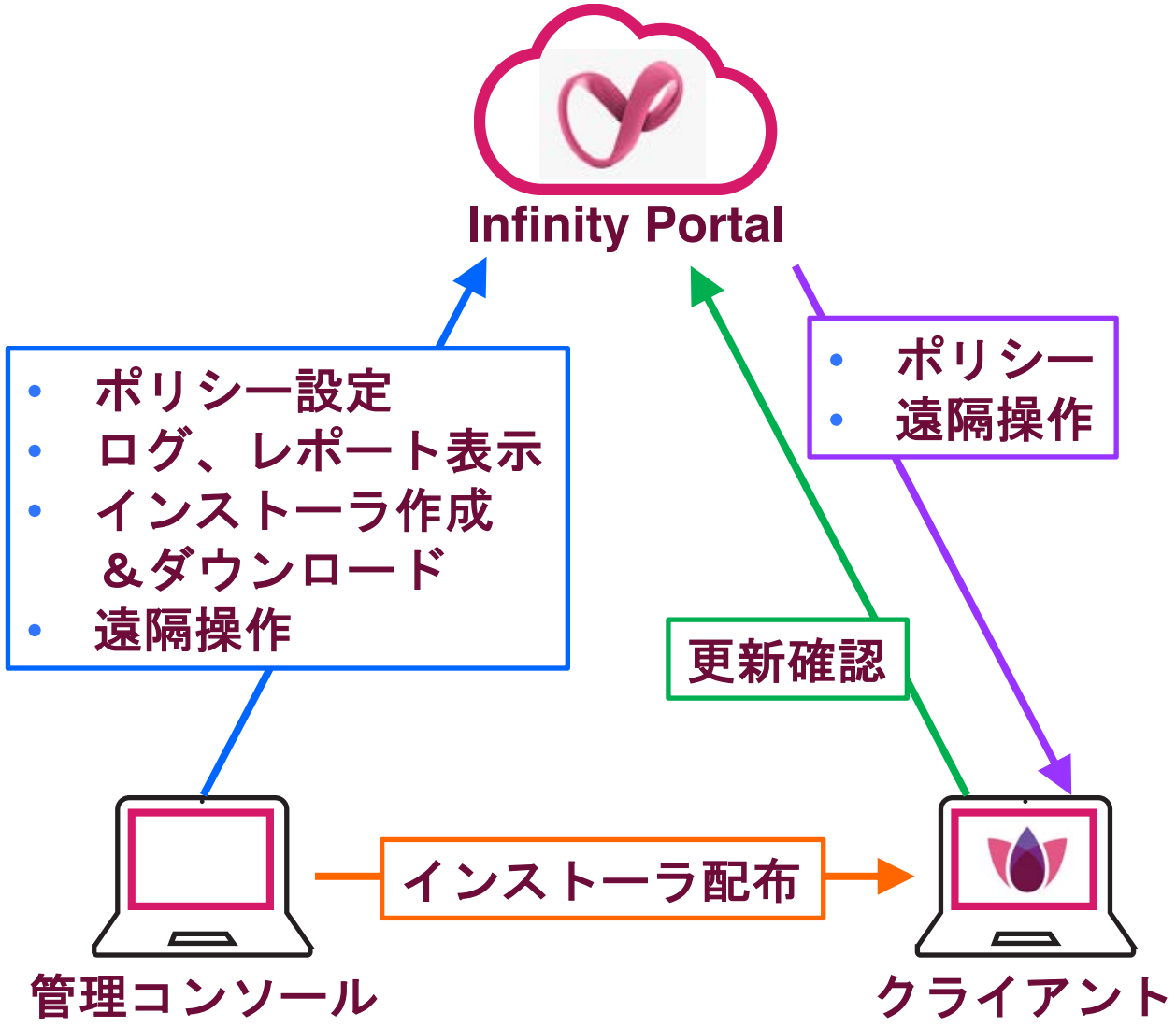
- 検知　　：Threat Hunting により、イベントを検知し、管理者にメール通知をする
- 分析　　：Forensics Report により、攻撃全体を把握し、侵入経路、影響、修復状況を確認する
- 封じ込め：Push Operations により、感染端末をネットワークから隔離する
- 封じ込め：Manage IOCs により、Forensics Report で 確認した IOC に基づくポリシーを適用する
- 根絶　　：Threat Hunting、Push Operations により、攻撃の痕跡を探索し、削除する



# HARMONY ENDPOINT の構成概要

YOU DESERVE THE BEST SECURITY

# Harmony Endpoint の構成概要




1. **Infinity Portal**
   - クラウド上の管理サーバ
   - セキュリティポリシーの設定や、ログ、レポートの確認などを実施

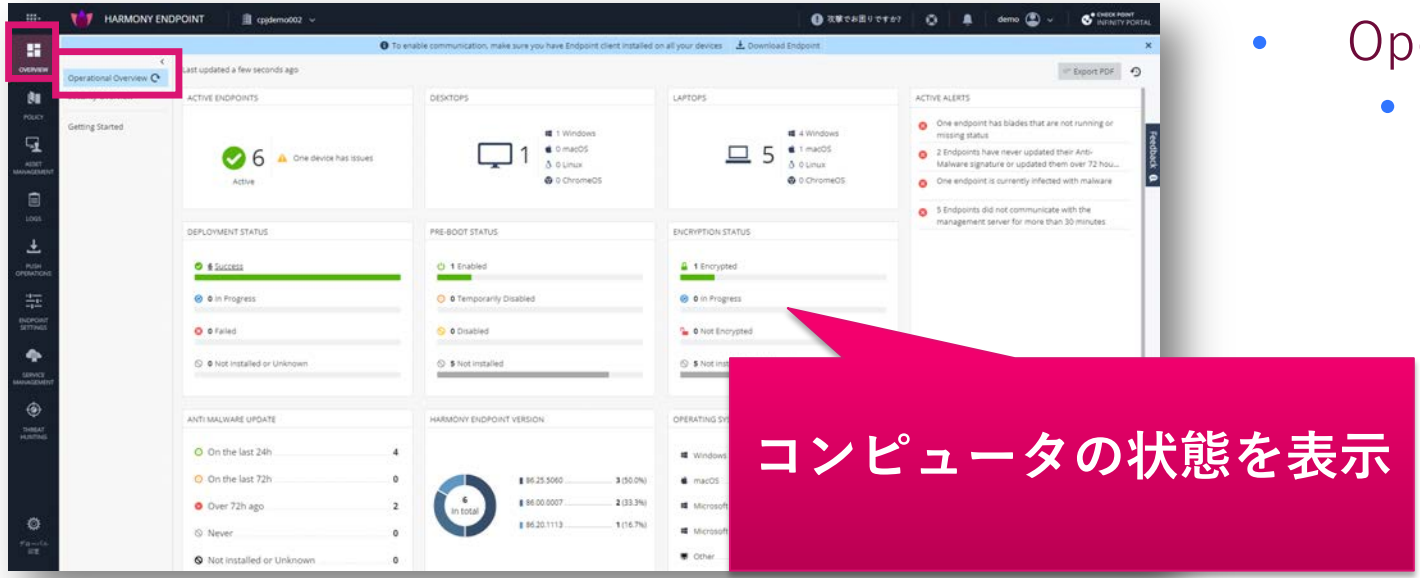
2. **管理コンソール**
   - Infinity Portal にアクセスして管理を行うパソコン
   - ブラウザで管理を実施

3. **クライアント**
   - Harmony Endpoint がインストールされたパソコン
   - 1分毎に Infinity Portal にポリシー等の更新を確認

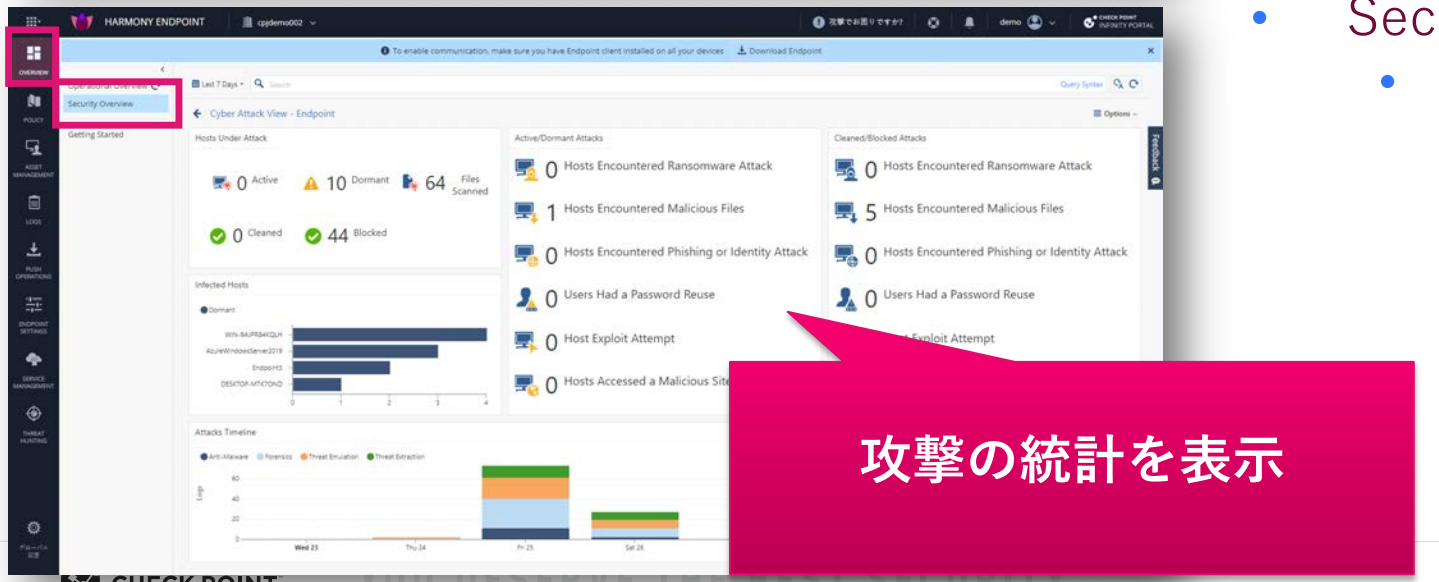
# 設定画面の概要

YOU DESERVE THE BEST SECURITY

# Overview ページ

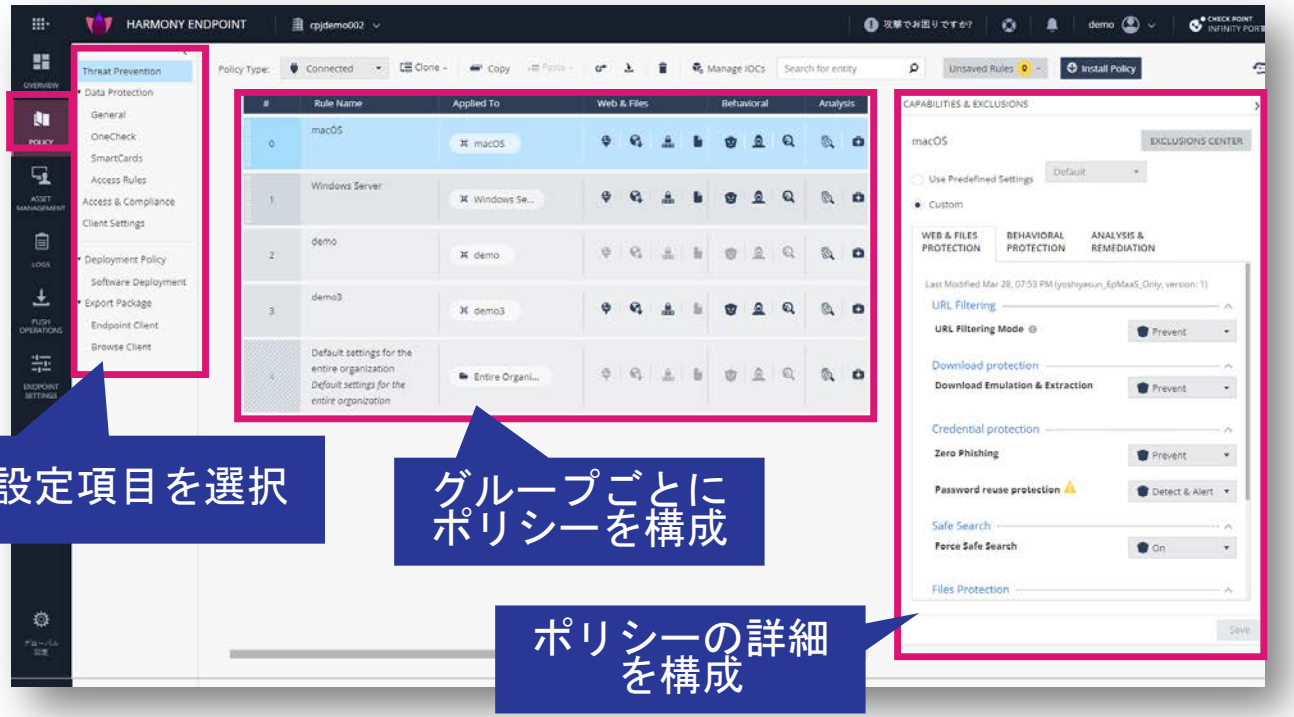



- Operational Overview
  - 組織内のエンドポイントクライアントの展開ステータス、それらのヘルスステータス、クライアントバージョン、およびクライアント上のオペレーティングシステムを表示します




- Security Overview
  - エンドポイントクライアントへの攻撃統計を表示します

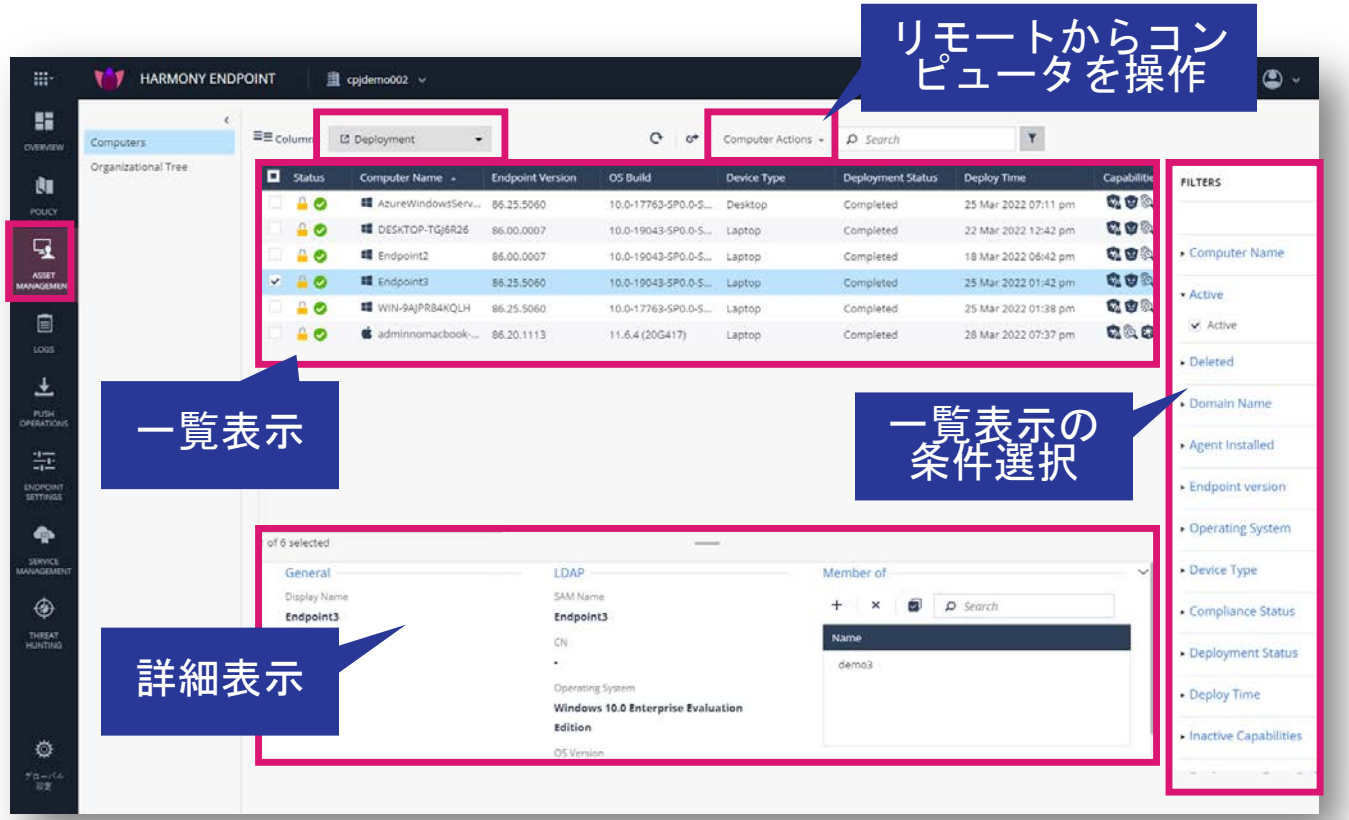
# Policy ページ




**ポリシーを設定**

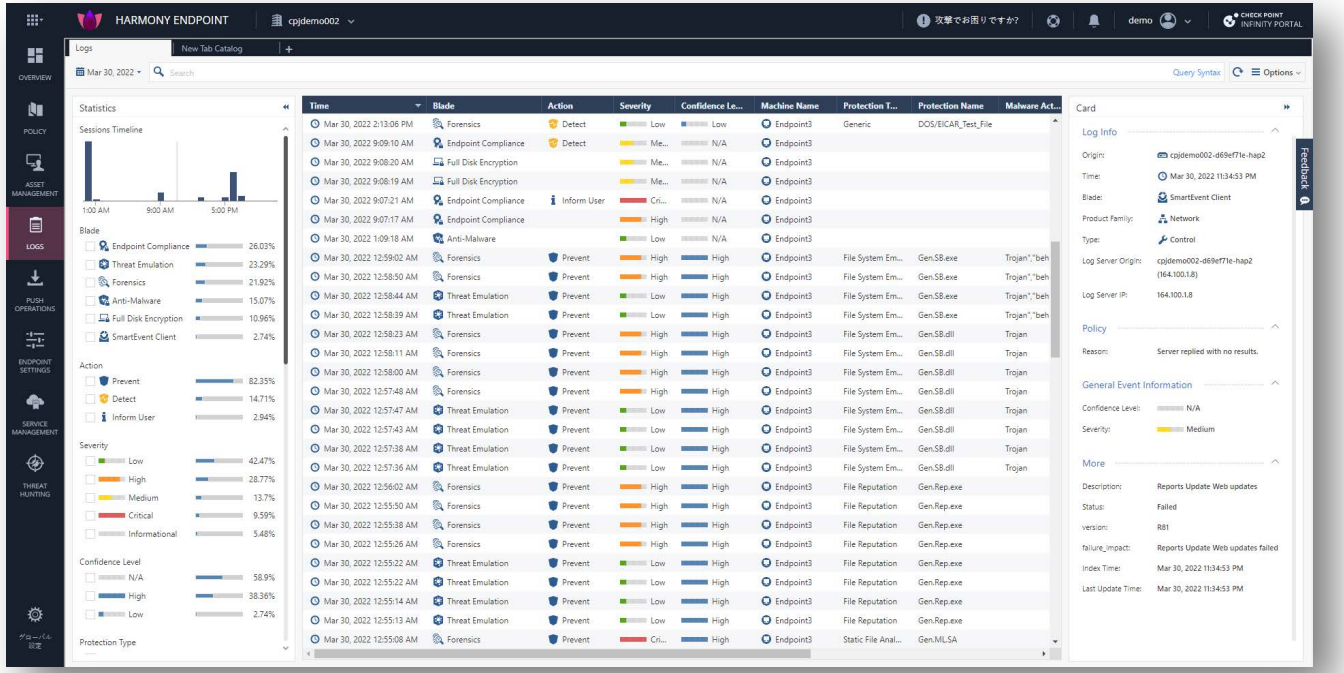
- セキュリティポリシーを構成します
  - 脅威の防止
  - データ保護
  - アクセスとコンプライアンス
- クライアントの設定を構成します
  - ユーザインタフェース
  - ログ
  - インストールとアップグレード
    - アンインストールパスワード
- クライアントの展開ポリシーを構成します
  - バージョン
  - ブレード（セキュリティ機能）
- インストールパッケージを構成します

# Asset Management ページ




- 展開ステータス、コンピューター上のアクティブなコンポーネント、コンピューターにインストールされているクライアントバージョンなど、各コンピューターに関する情報が表示されます
- 事前構成されたビューを選択して表示します
  - 展開
  - コンプライアンス
  - ヘルス
  - フルディスク暗号化
  - マルウェア対策
  - ホストの隔離
  - カスタム（必要な列を選択）

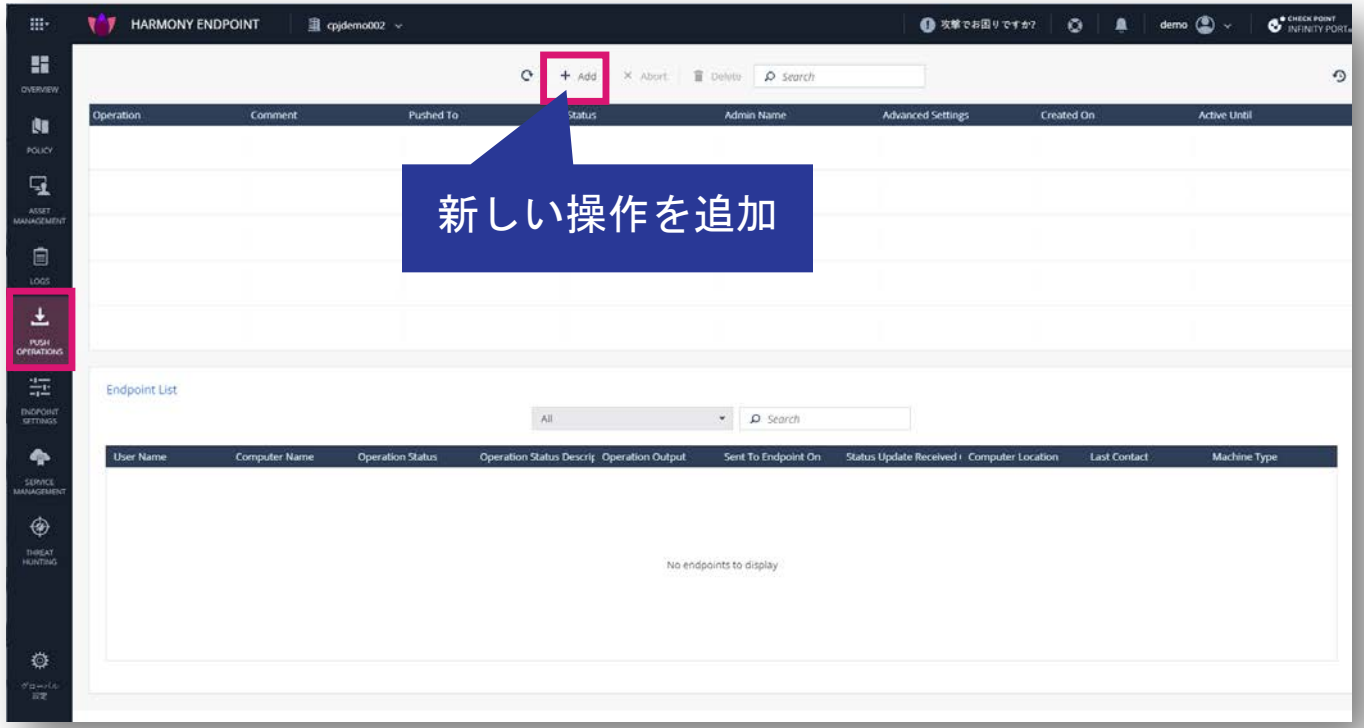
# Logs ページ




- アクティビティのログを表示します
- フォレンジックレポートを表示します
- 事前定義された各種ビューやレポートを表示します

**ログなどを表示**

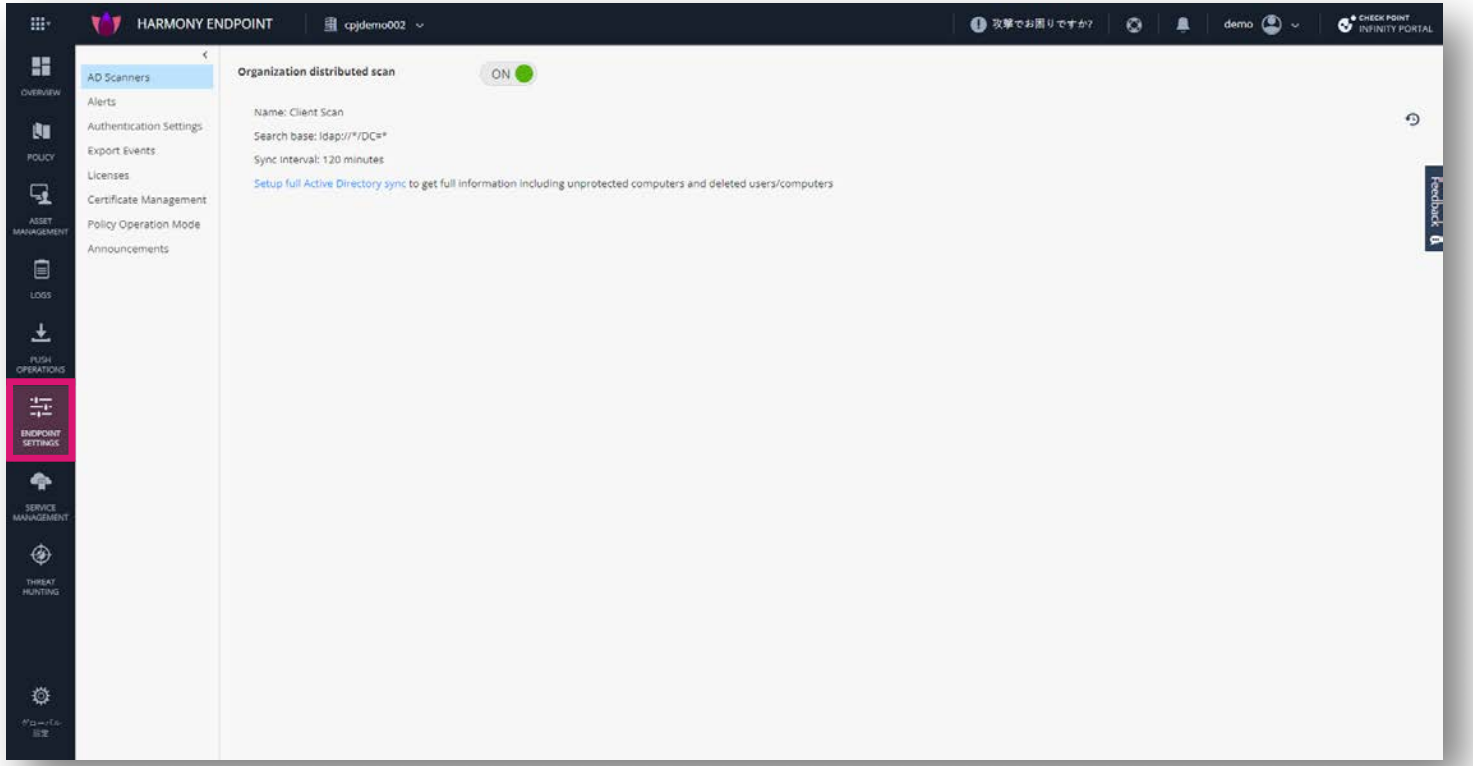
# Push Operations ページ




**遠隔操作を実施**

- リモートからコンピュータを操作します
  - マルウェア対策
    - スキャンの実行
    - シグネチャの更新
    - ファイルを隔離から復元
  - フォレンジックと修復
    - IoC による分析
    - ファイル修復
    - コンピュータの隔離
    - コンピュータの解放
  - エージェント設定
    - クライアントログの収集
    - クライアントソフトの修復
    - シャットダウン
    - 再起動
    - アプリケーションスキャン
    - プロセスの停止
    - リモートコマンド

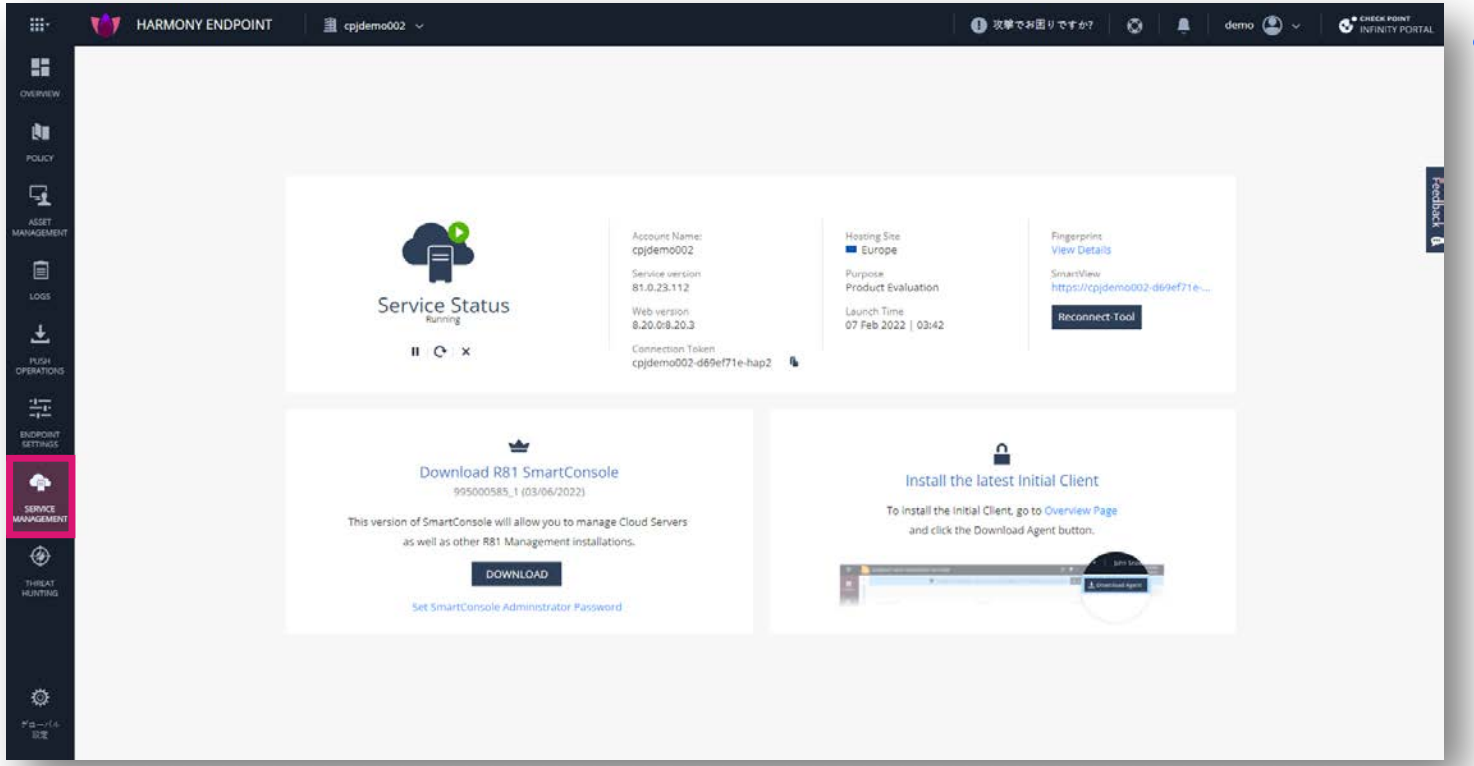
# Endpoint Settings ページ




- AD 連携、ライセンス管理、ログのエクスポート(Syslog 連携)など、全体的な設定を行います

**全体的な設定**

# Service Management ページ




- サービス(管理機能)の管理を行います
  - 一時停止
  - 再起動
  - 停止

**管理サービスの管理**

# Threat Hunting ページ

- Threat Hunting は、コンピュータでの攻撃情報を収集する調査ツールです
- コンピュータで発生したすべての良性と悪性のイベントを収集し、可視化と調査を可能にします


**脅威を探索**

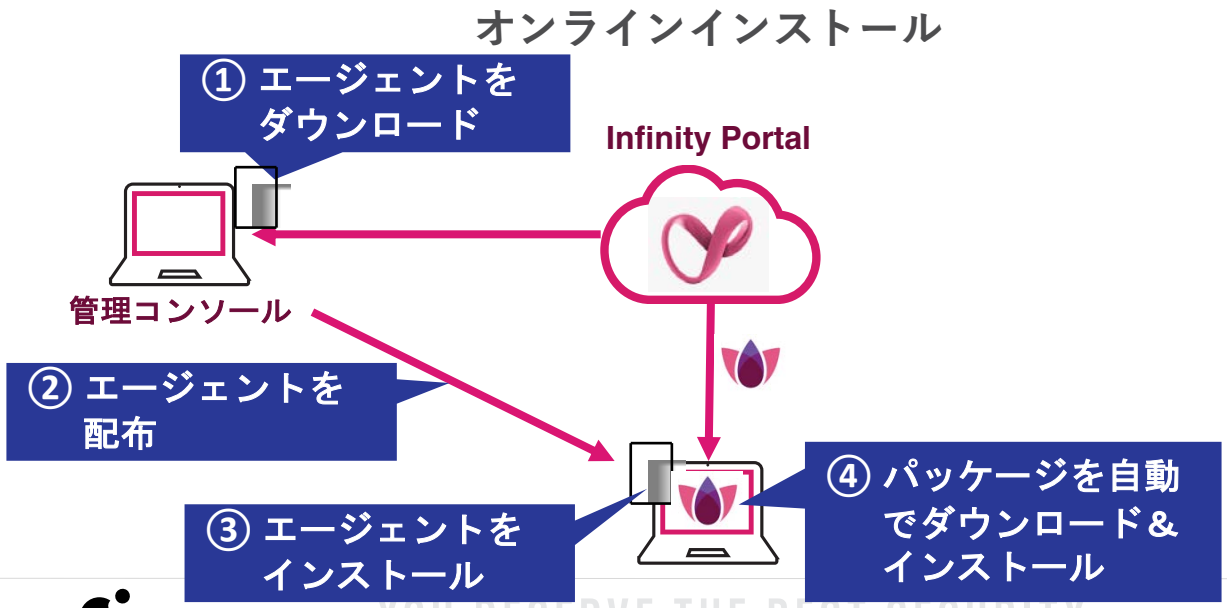
# クライアントのインストール

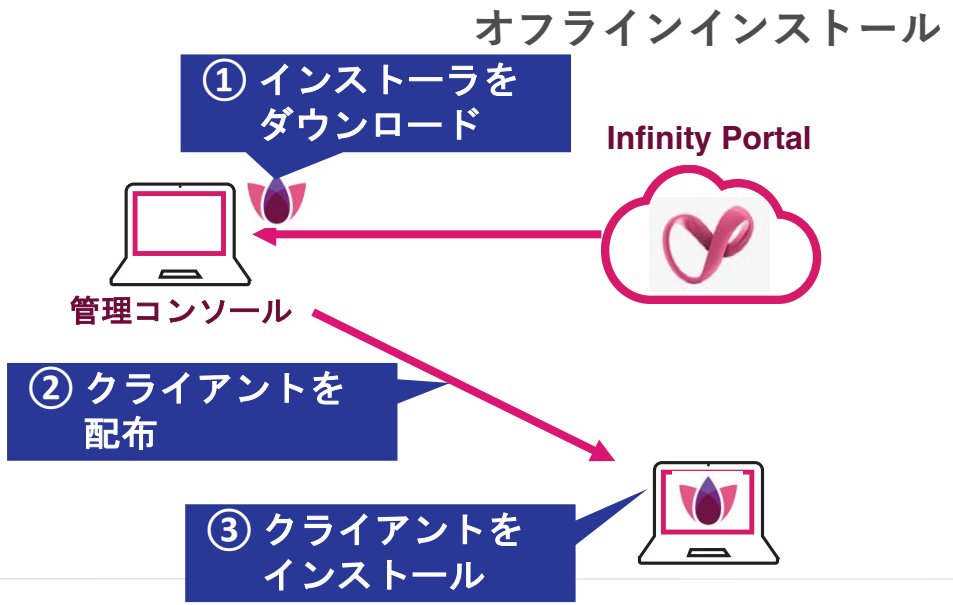
- クライアントの展開方法
- インストールパッケージの概要（オフラインインストール）
- クライアントのインストール

YOU DESERVE THE BEST SECURITY

# クライアントの展開方法

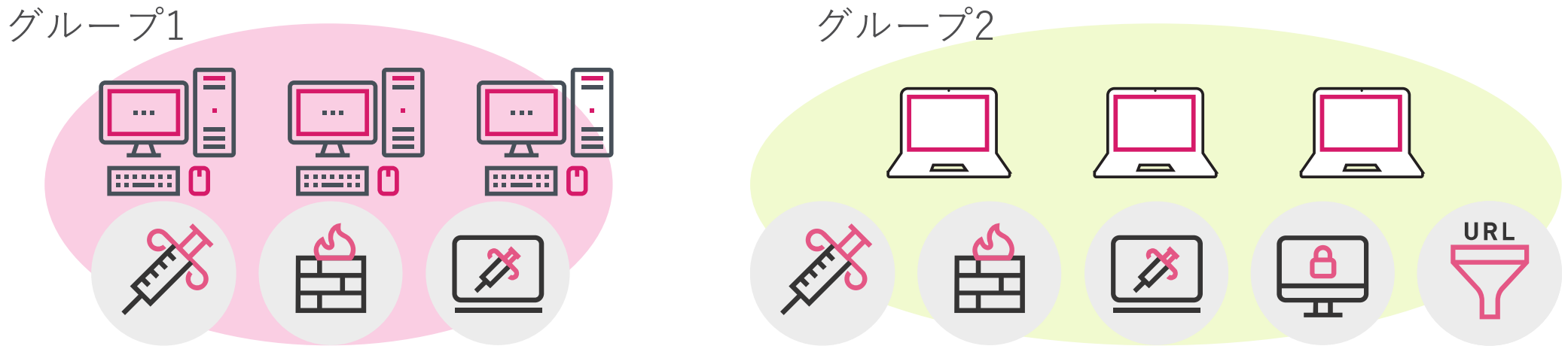
- **オンラインインストール**と、**オフラインインストール**の 2 種類の方法を選択できます
- **オンラインインストール**
  - 軽量なインストーラを用いてエージェントのインストールを行います
  - エージェントのインストール後にパッケージを自動でダウンロードしてインストールします
  - ホームワークやテレワークのコンピューターへのインストールにおすすめです
- **オフラインインストール**
  - 必要なセキュリティ機能を含むインストーラを用いてクライアントのインストールを行います
  - 社内ネットワークに接続されたコンピューターへのインストールにおすすめです
- ファイルサーバやメールでインストーラを共有する以外にも、Active Directory や 3rd Party のツールを使用してインストールすることも可能です



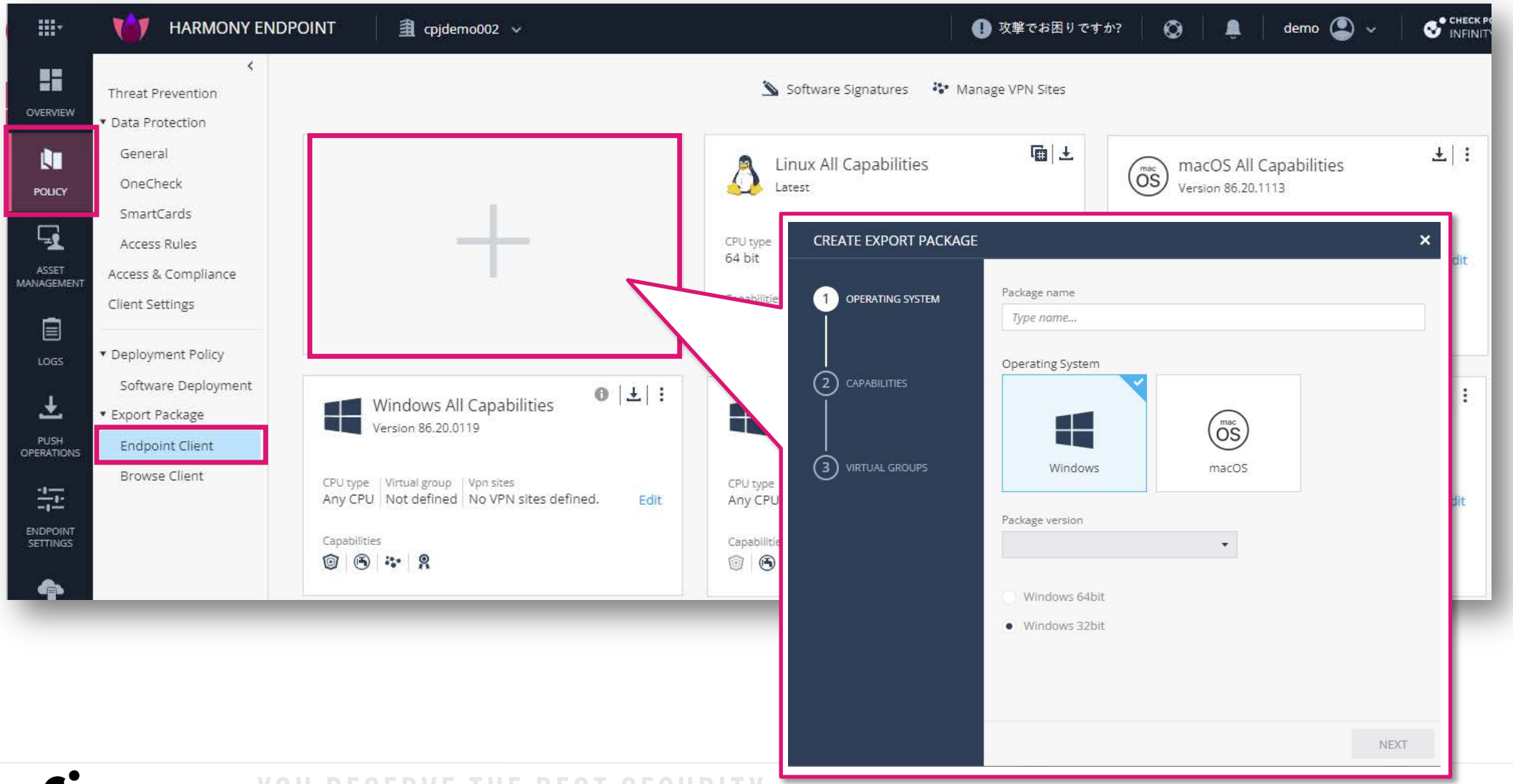
# インストールパッケージの概要（オフラインインストール）

- インストールパッケージを作成する際は、クライアントのバージョン、インストールする機能、バーチャルグループ、VPNサイト（VPN利用時のみ）を構成します
  - バーチャルグループを指定することで、自動的にコンピュータをバーチャルグループに所属させることができます（Web UI でも変更可能です）
  - **Policy > Deployment Policy > Software Deployment の設定は、インストールパッケージ作成時のクライアントバージョン、インストールする機能の構成と同じ設定にしてください。異なる場合、Software Deployment で設定したバージョン、機能にクライアントソフトウェアが更新されます**
- インストールパッケージは、事前定義されたパッケージを使用することも可能です
  - Linux は、事前定義されたパッケージのみを使用可能です



# インストールパッケージの作成（１／５）

Policy > Export Packages > Endpoint Client

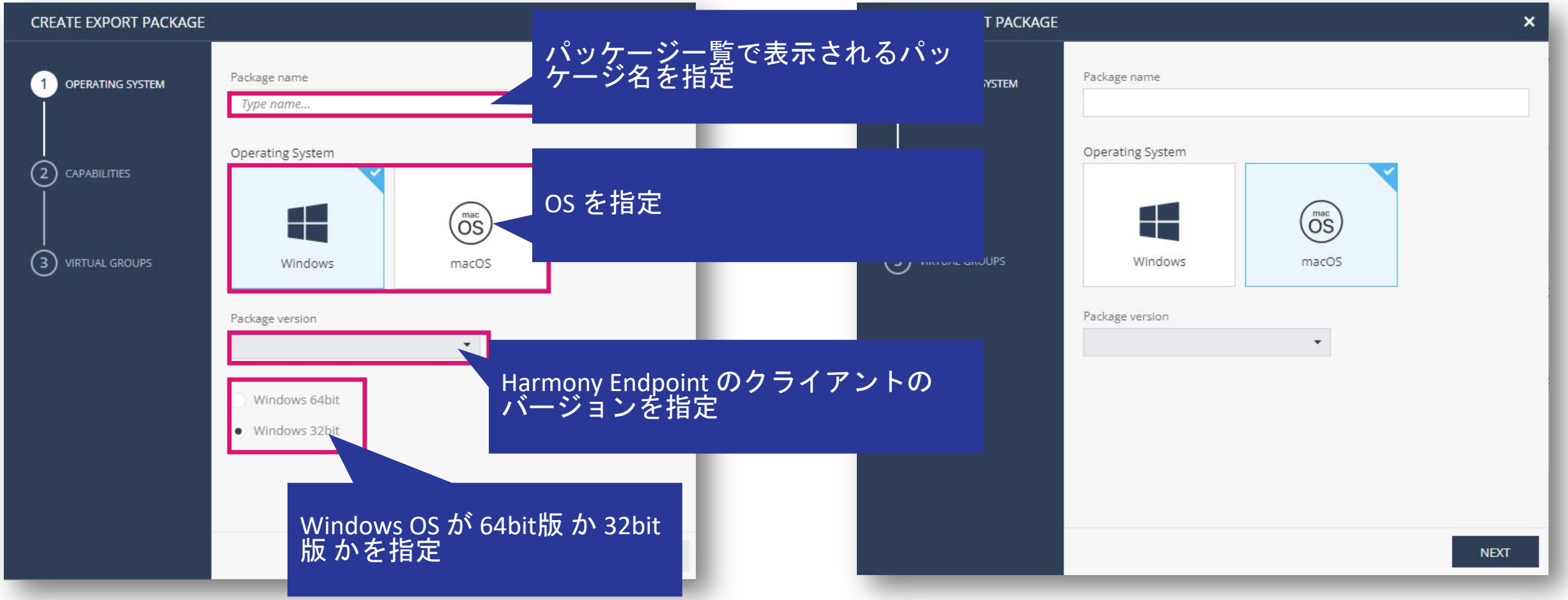


# インストールパッケージの作成（２／５）

Policy > Export Packages > Endpoint Client

Windows

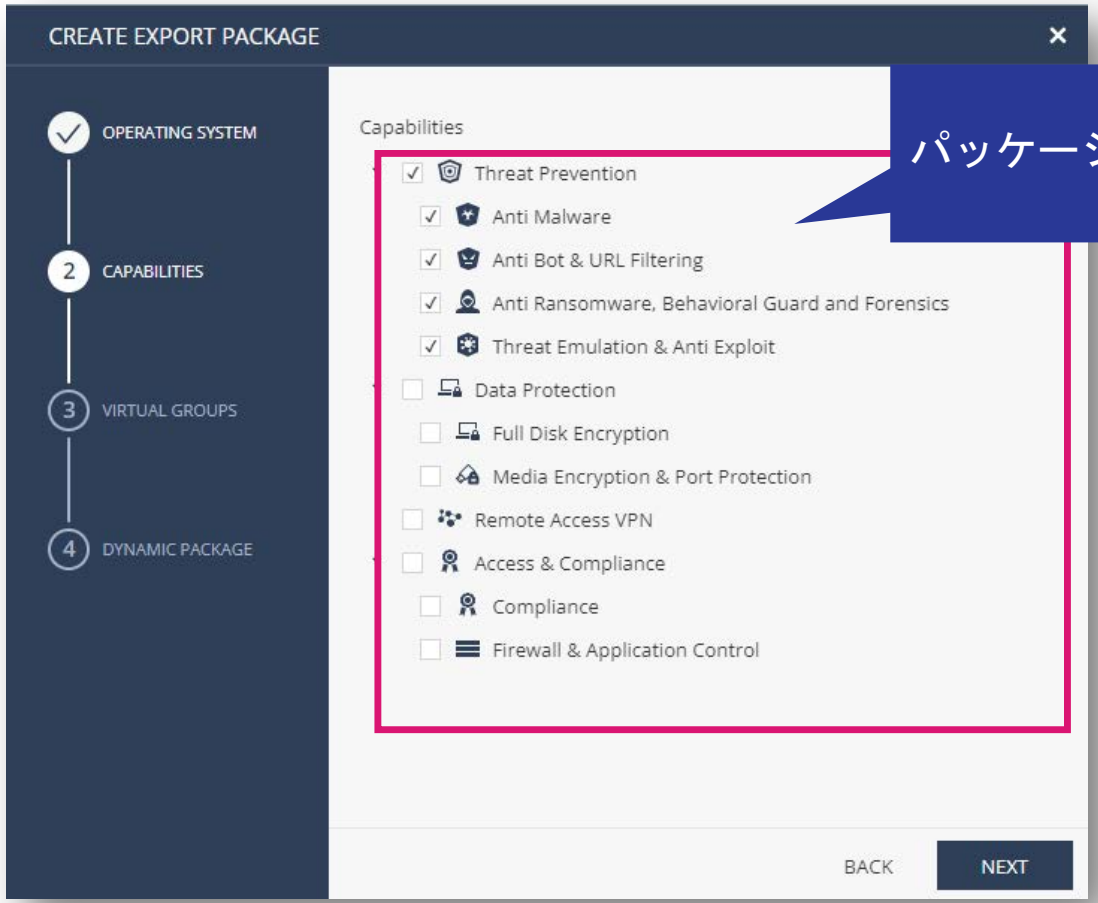
macOS



# インストールパッケージの作成（３／５）

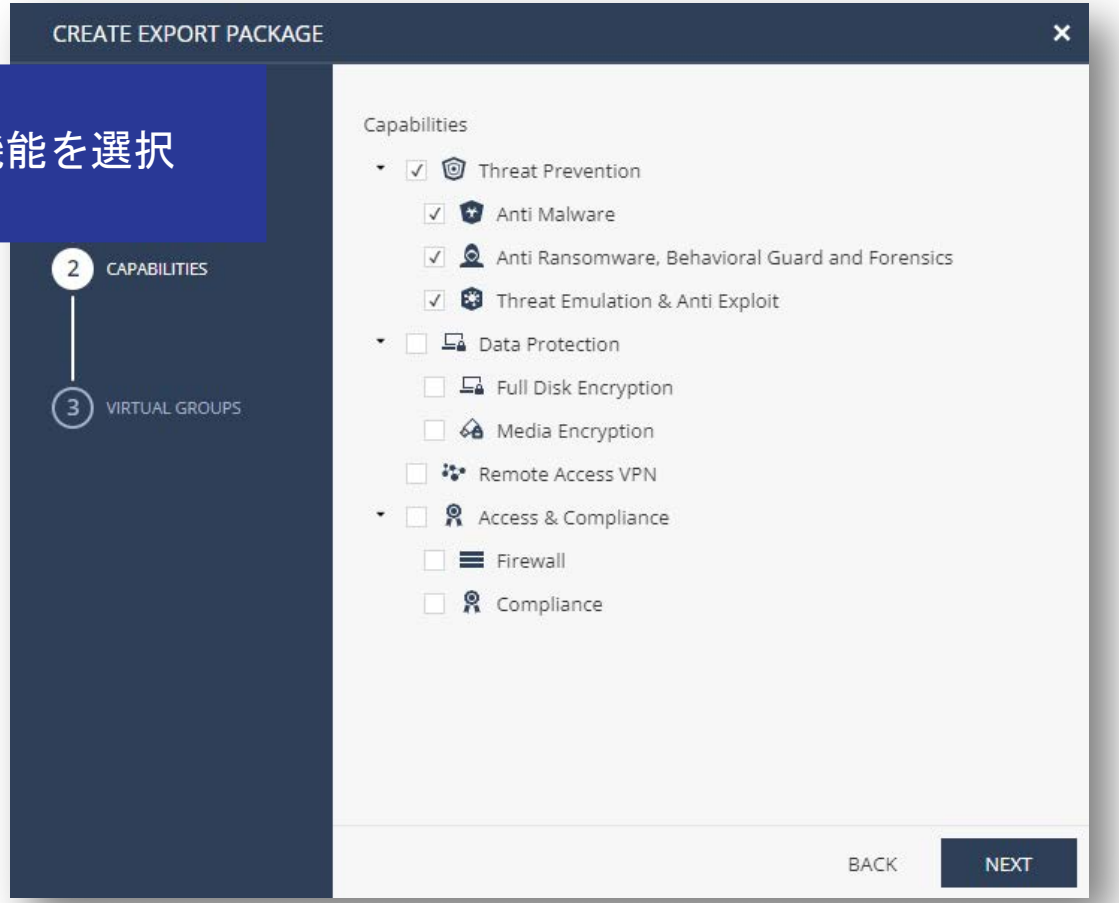
Policy > Export Packages > Endpoint Client

## Windows




パッケージに含める機能を選択

## macOS

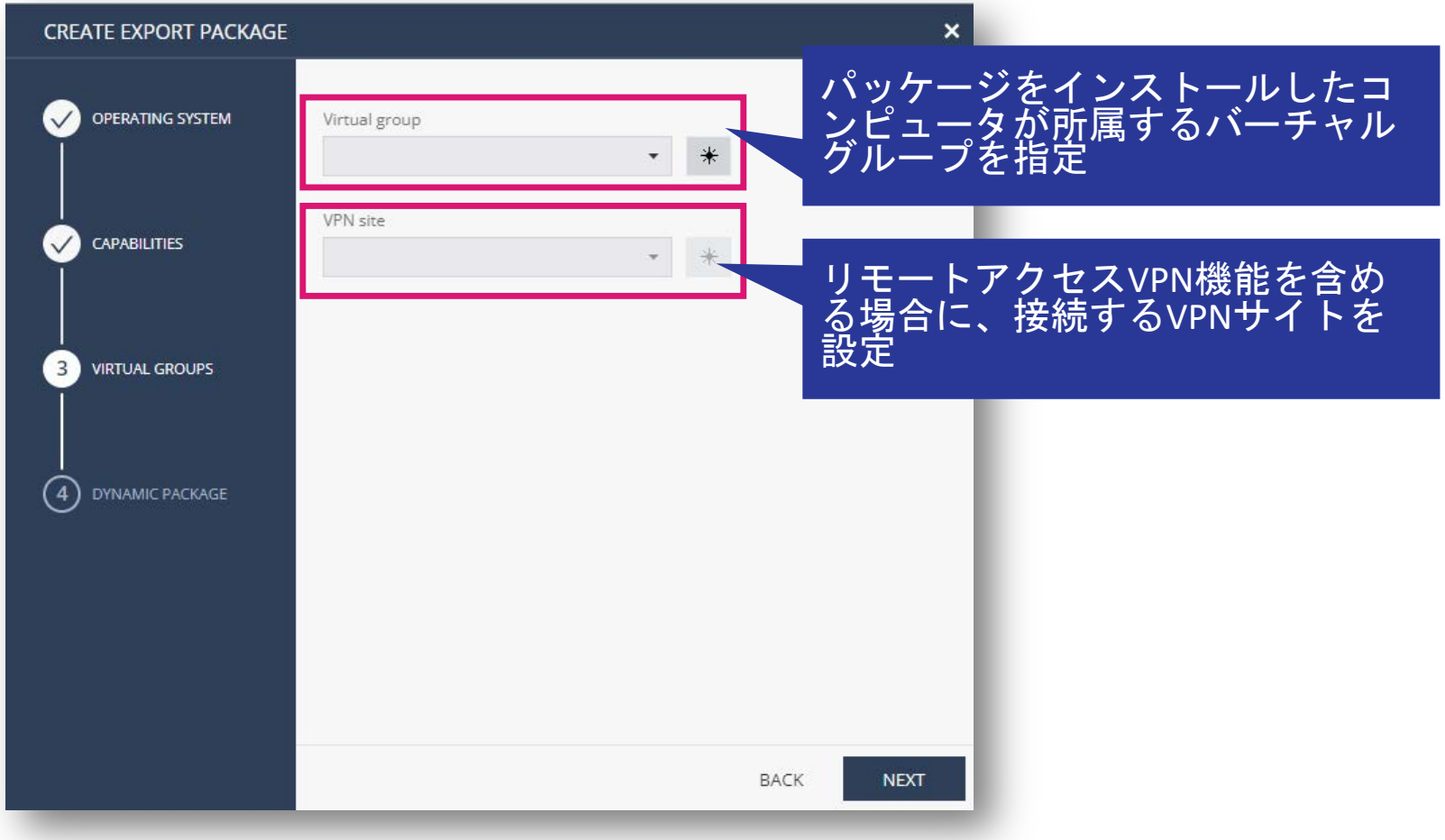



※ PushOperations で端末の隔離を実施する場合は、Firewall Bladeが必要

# インストールパッケージの作成（４／５）

Policy > Export Packages > Endpoint Client

Windows & macOS 共通



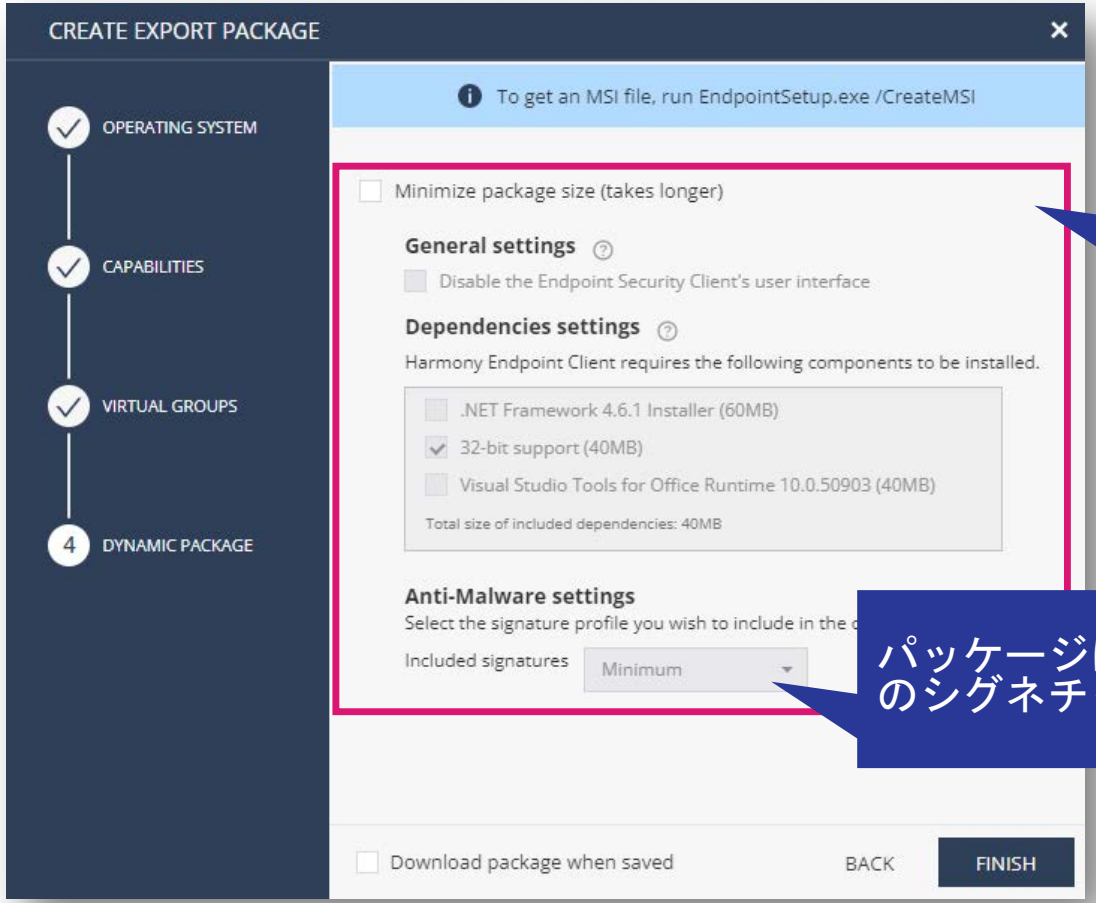

パッケージをインストールしたコンピュータが所属するバーチャルグループを指定

リモートアクセスVPN機能を含める場合に、接続するVPNサイトを設定

# インストールパッケージの作成（５／５）

Policy > Export Packages > Endpoint Client

Windows のみ



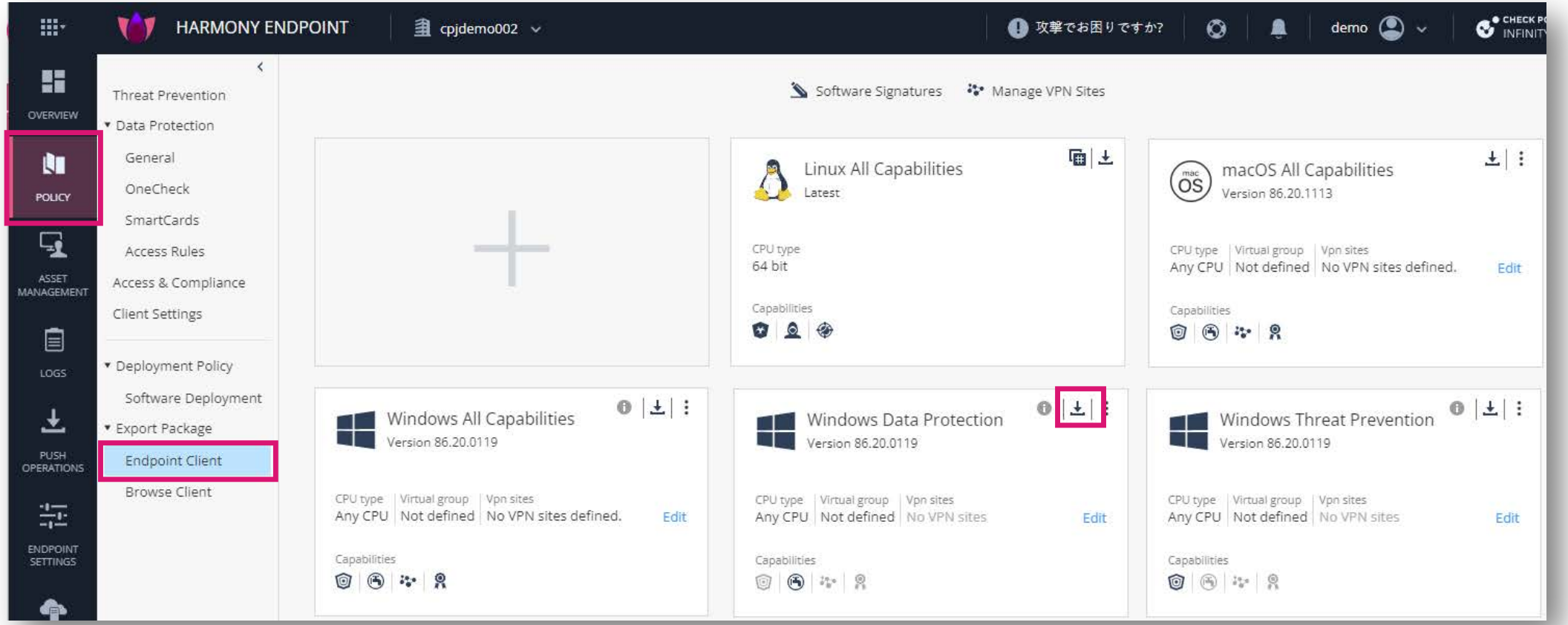

不要な機能を削減して、パッケージサイズを最小化することが可能

パッケージに含める Anti-Malware のシグネチャを選択

# インストールパッケージのダウンロード

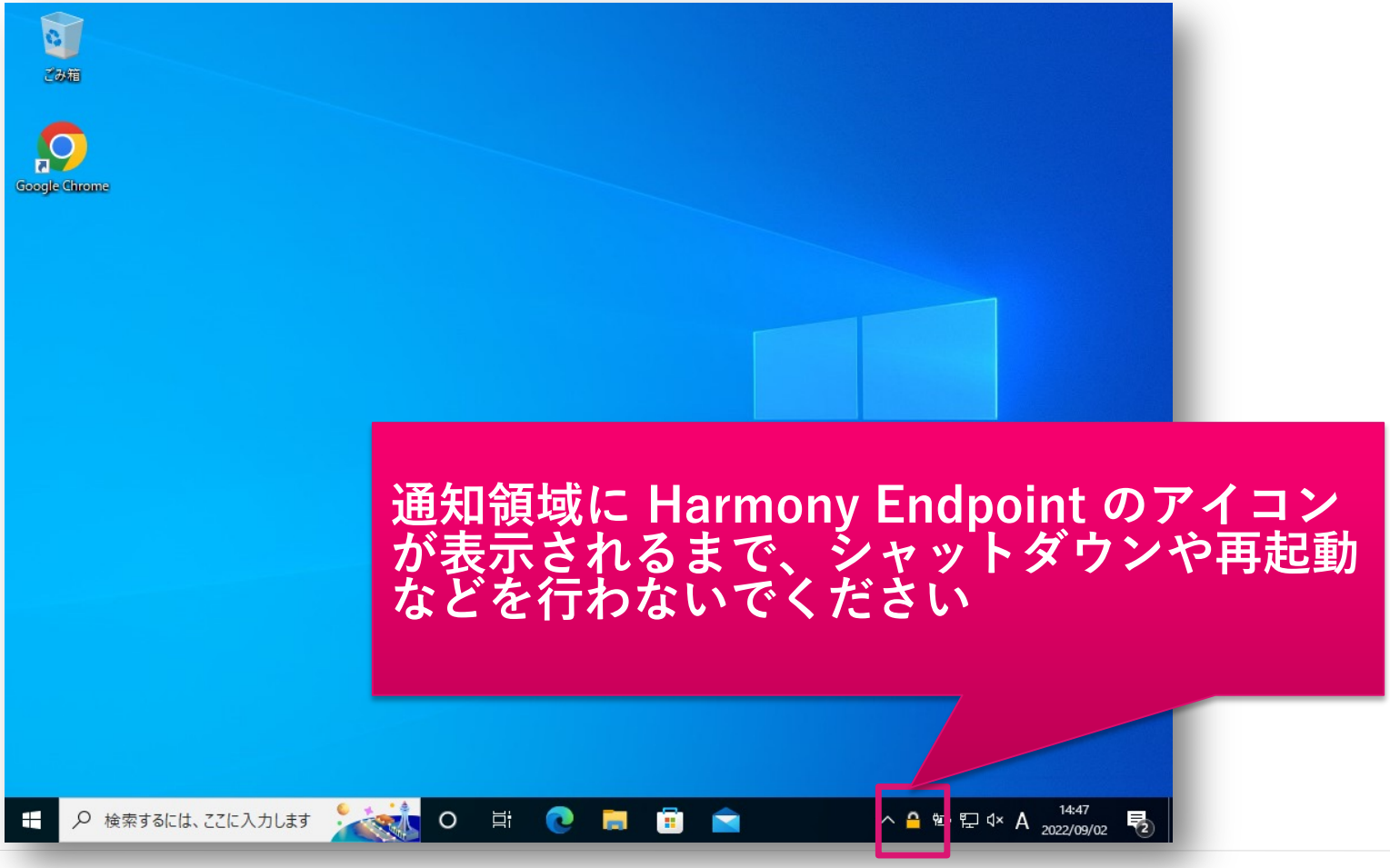
Policy > Export Packages > Endpoint Client

- ダウンロードするパッケージの　　をクリックしてパッケージをダウンロードします



# クライアントのインストール

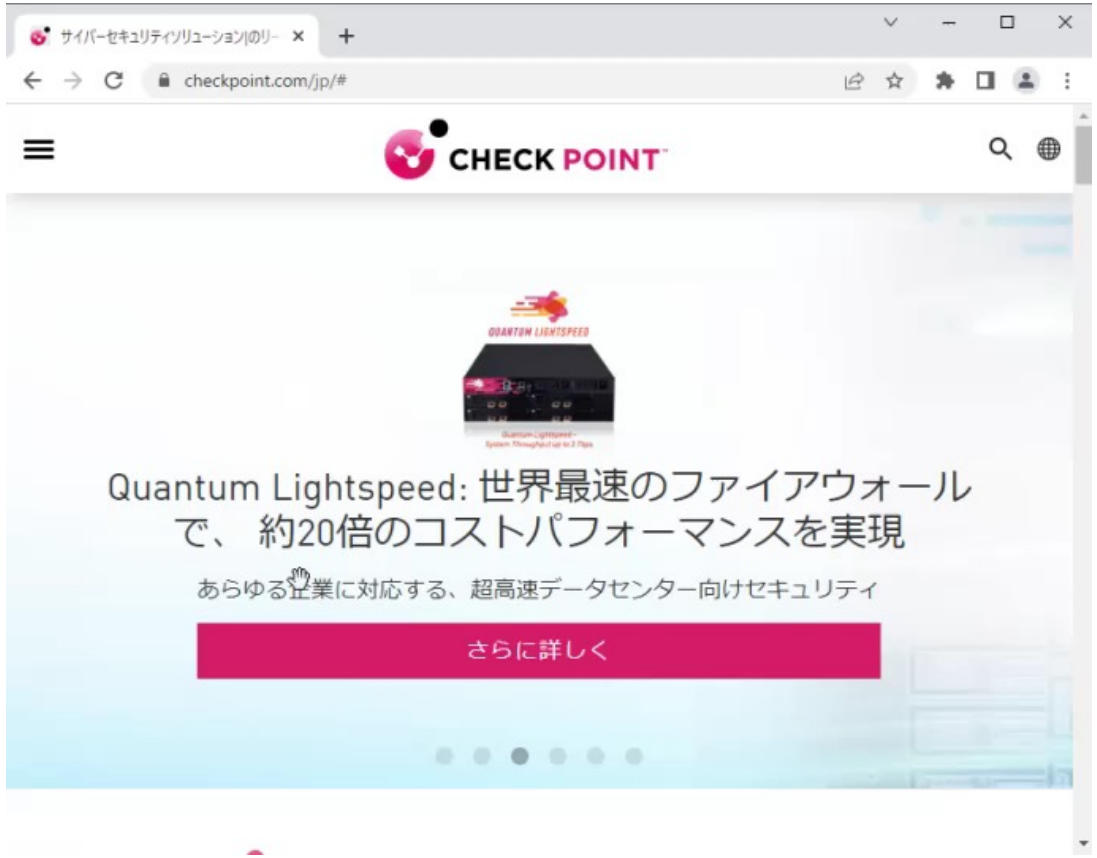
- インストールパッケージをダブルクリックします
- 通知領域に Harmony Endpoint のアイコンが表示されるまで、シャットダウンや再起動などを行わないでください



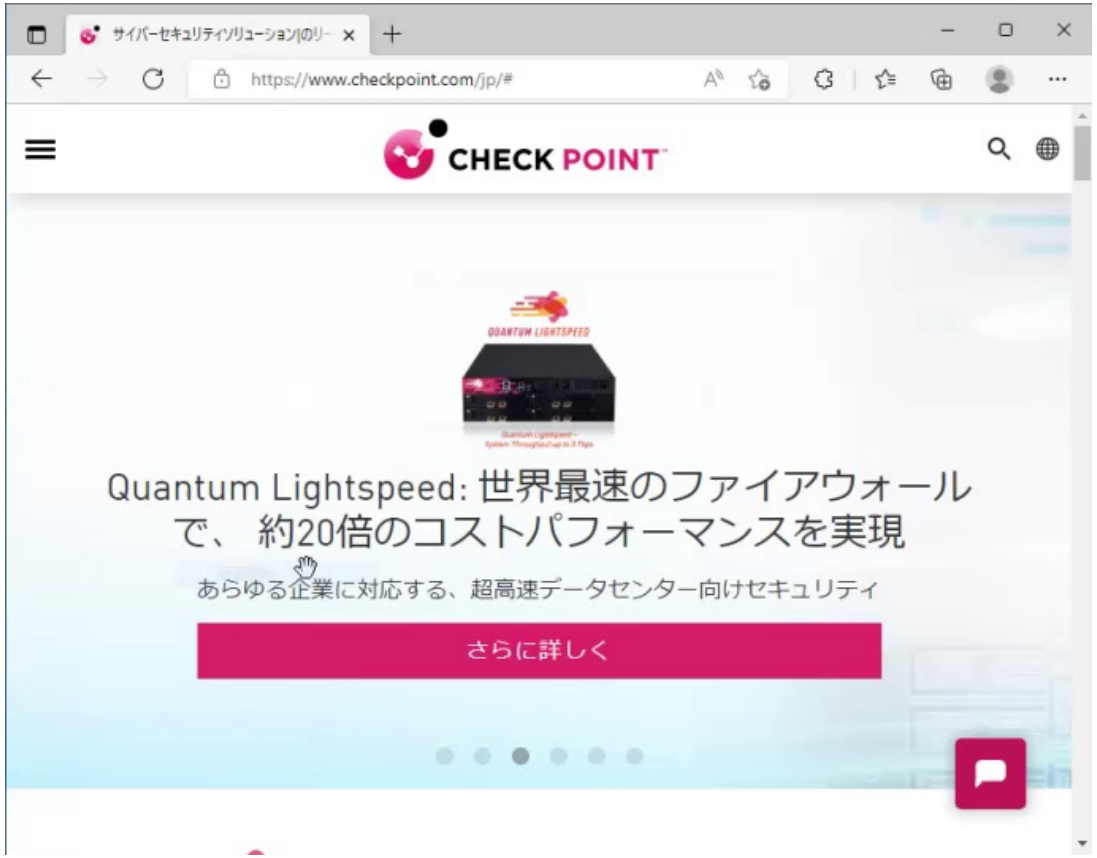
# 【参考】Check Point アイコン の表示方法

- ブラウザにCheck Pointのアイコン が表示されていない場合は、以下の動画を参考にして、表示させてください。

**Check Point アイコンの表示方法（Chrome）**

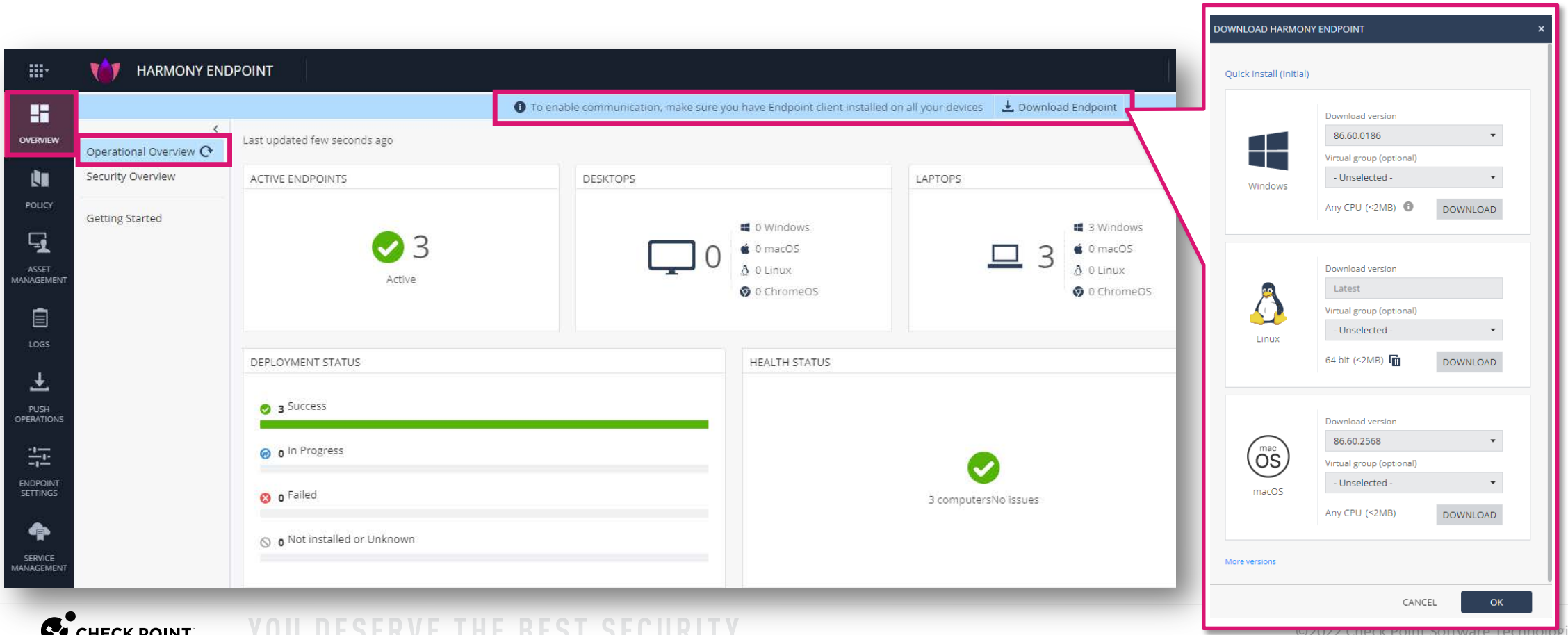



**Check Point アイコンの表示方法（Edge）**



# 【参考】オンラインインストール用インストーラ

- Overview > Operational Overview 上部の「Download Endpoint」からダウンロードします
- OS、クライアントバージョン、バーチャルグループを選択して、ダウンロードします
- Policy > Deployment Policy > Software Deployment の設定に従ってセキュリティ機能がインストールされます



# 【演習】

- インストールパッケージを作成してください
  - バージョンは、最新バージョン以外を選択してください
- インストールパッケージをダウンロードしてください
- クライアントソフトウェアをインストールしてください

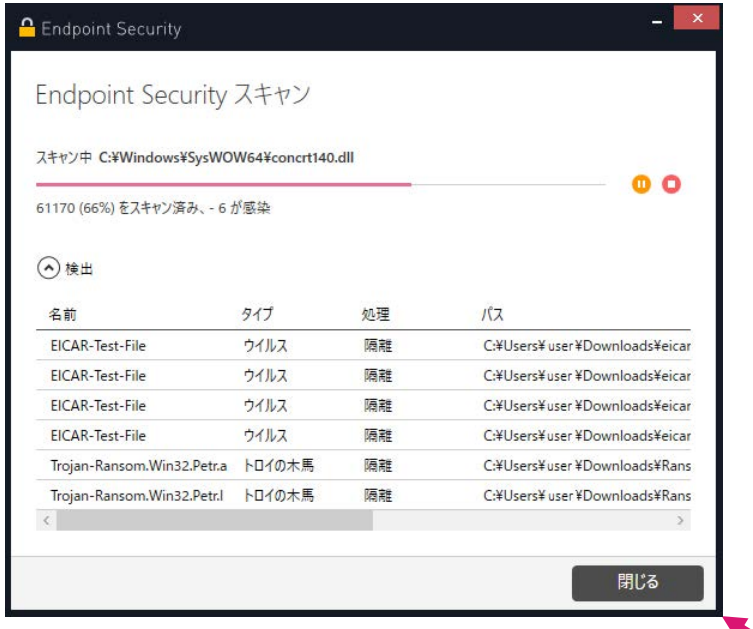
# クライアントの UI

YOU DESERVE THE BEST SECURITY

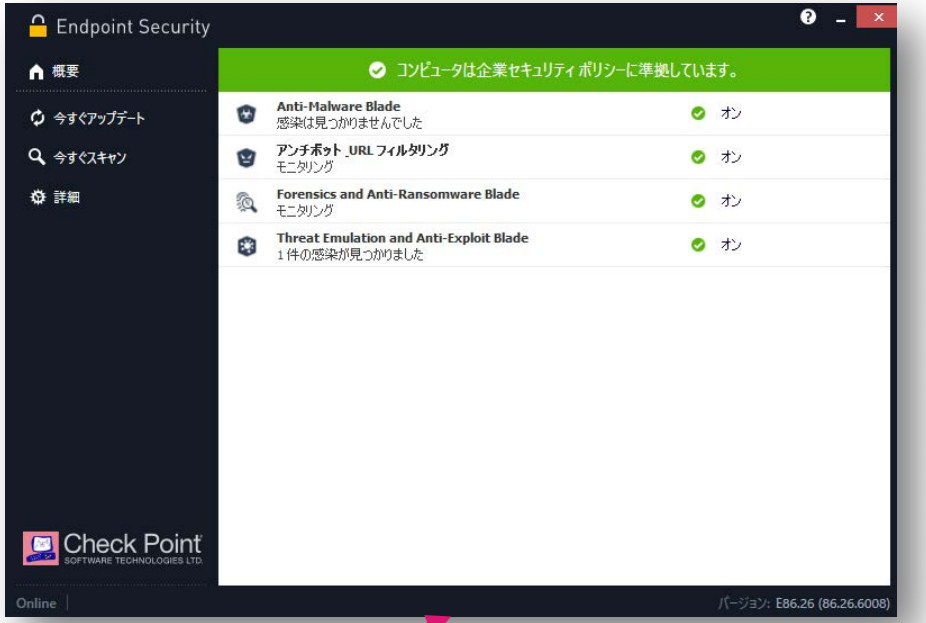
# クライアントの UI 概要（1／4）

- クライアントソフトウェアでは、各種情報を確認、収集できます
  - セキュリティ機能のステータス
  - セキュリティログ
  - クライアントソフトウェアのバージョン
  - セキュリティ Blade のバージョン
  - ポリシーのバージョン
  - テクニカルサポートに提供するログ（CPinfo）
- ポリシーと Anti-Malware のシグネチャを更新できます
- Anti-Malware による Scan を実施できます

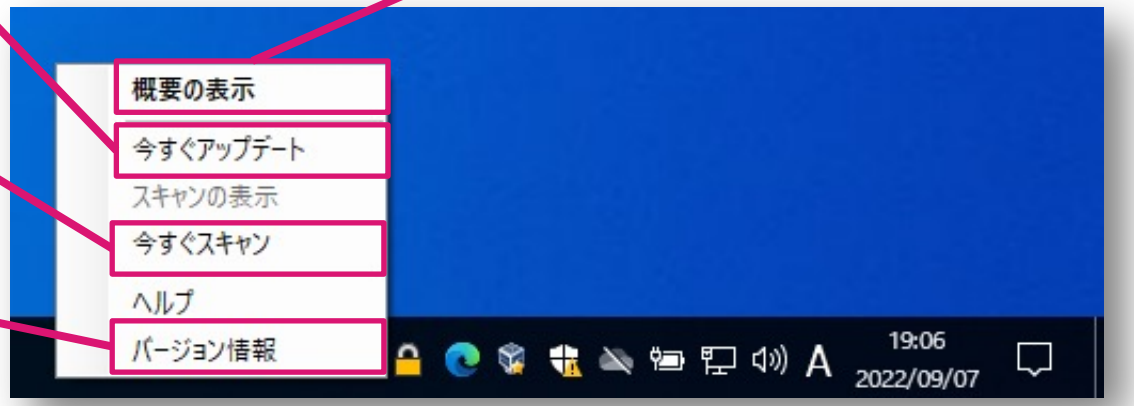
# クライアントの UI 概要（2／4）





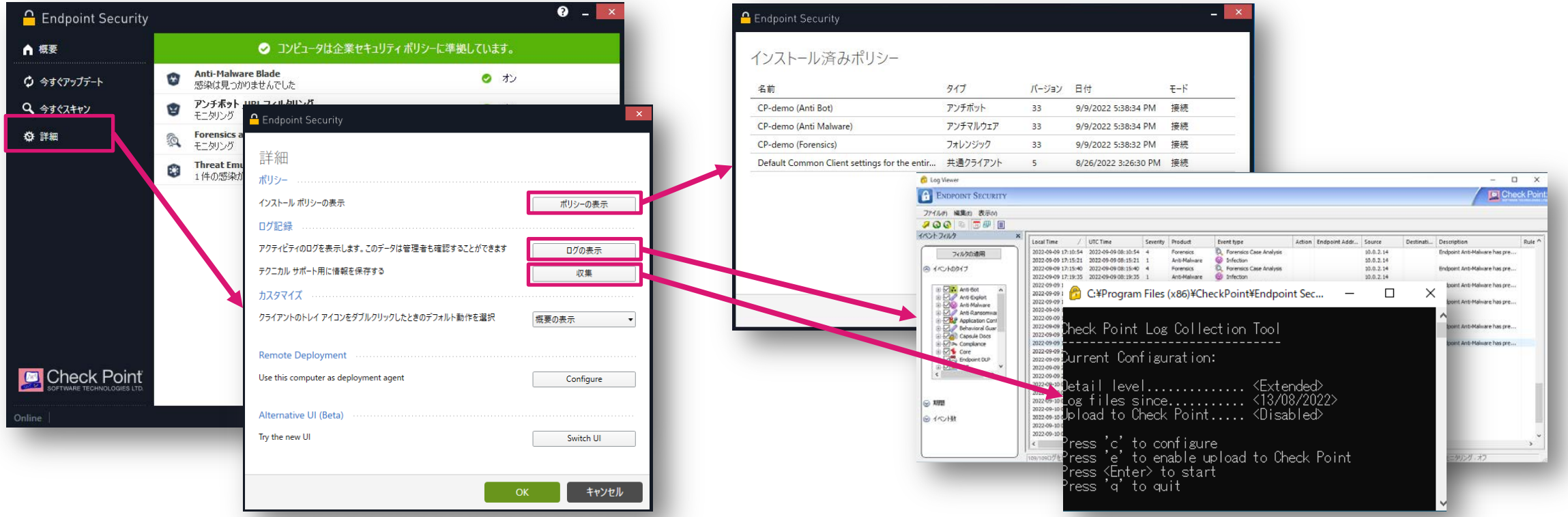






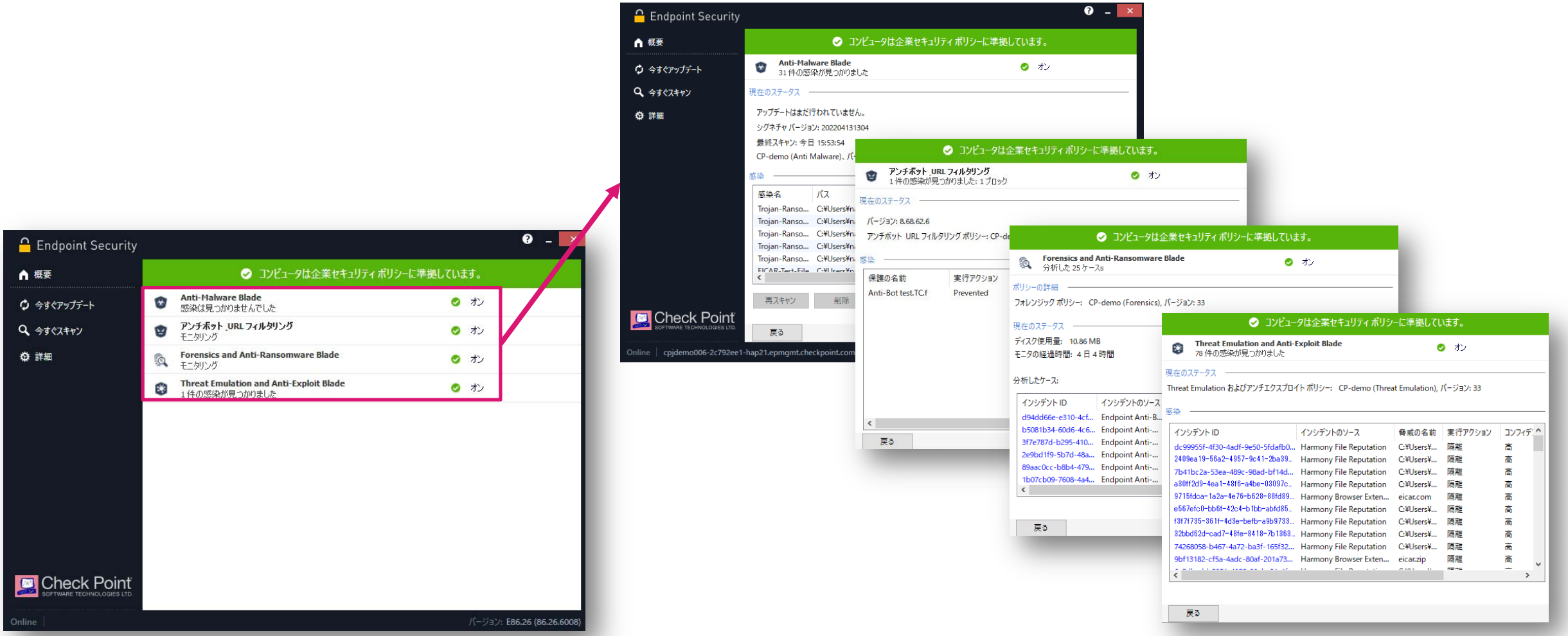
# クライアントの UI 概要（3／4）：詳細

- 「ポリシーの表示」は、パソコンに適用されているポリシーバージョンを確認できます
- 「ログの表示」は、パソコンでのアクティビティを確認できます
- 「収集」は、テクニカルサポート用の情報（CPinfo）を収集します
  - CPinfo は、%UserProfile%¥CPInfo に保存されます



# クライアントの UI 概要（4／4）：Blade

- 各 Blade をクリックすると、各 Blade での検出状況、ポリシーバージョンを確認できます



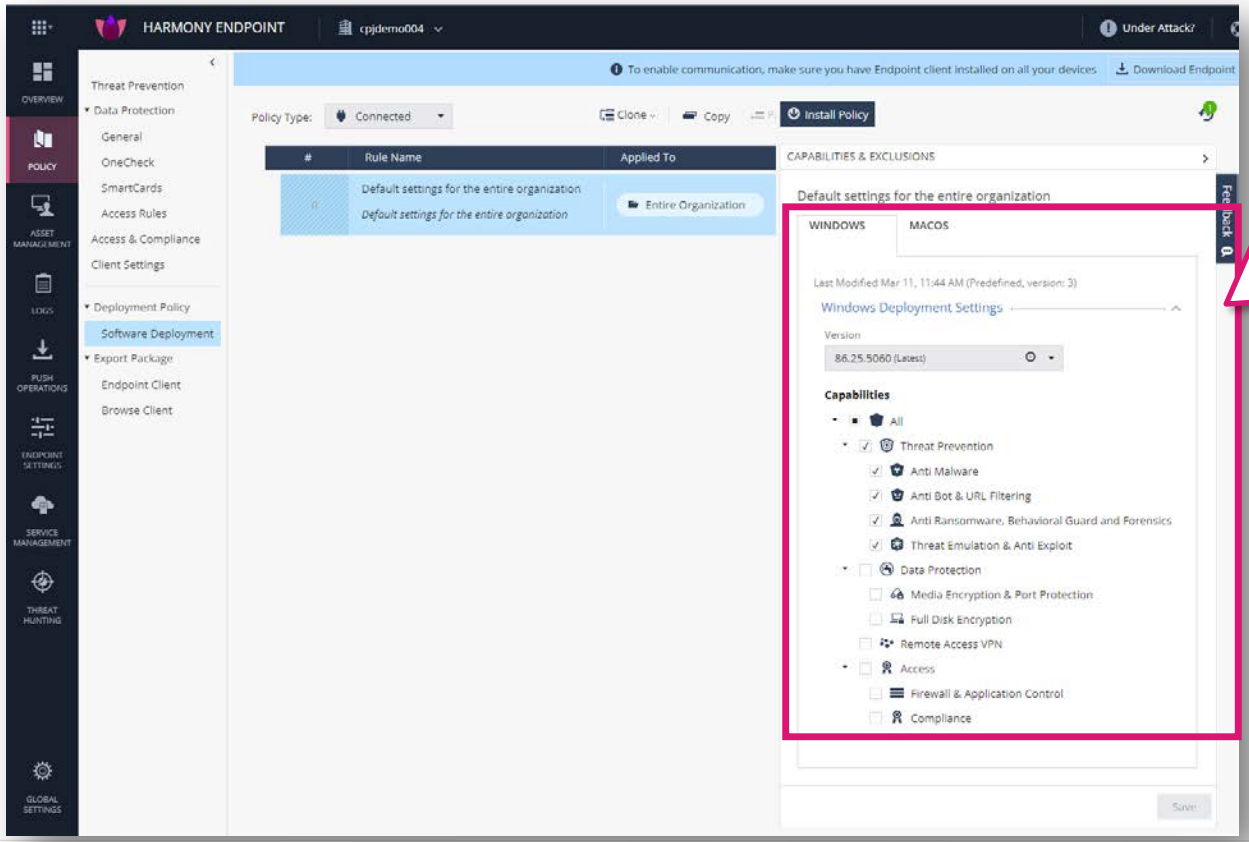
# クライアントのアップグレード

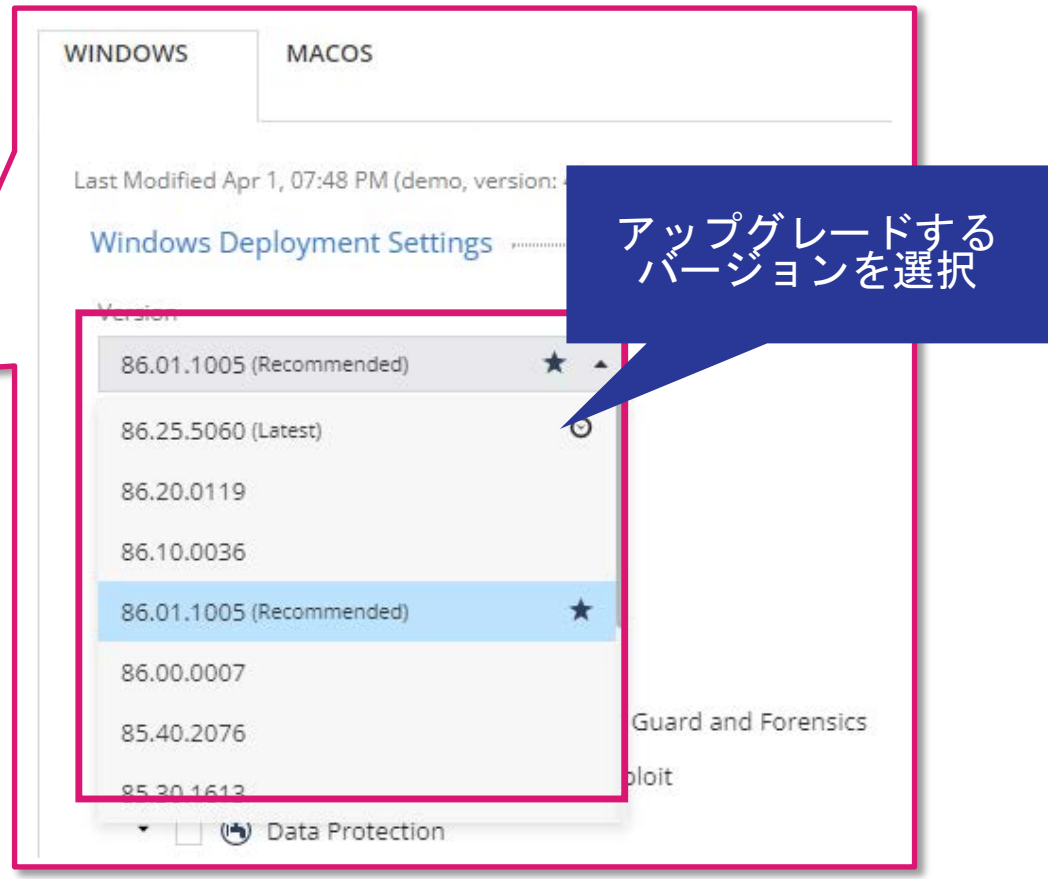
YOU DESERVE THE BEST SECURITY

# クライアントのアップグレード

Policy > Deployment Policy > Software Deployment

- クライアントソフトウェアをコンピュータに展開後に、機能の追加やクライアントのアップグレードがリモートから実施可能です
- ダウングレードはできません
- Save と、 Install Policy を実行します



# 【演習】

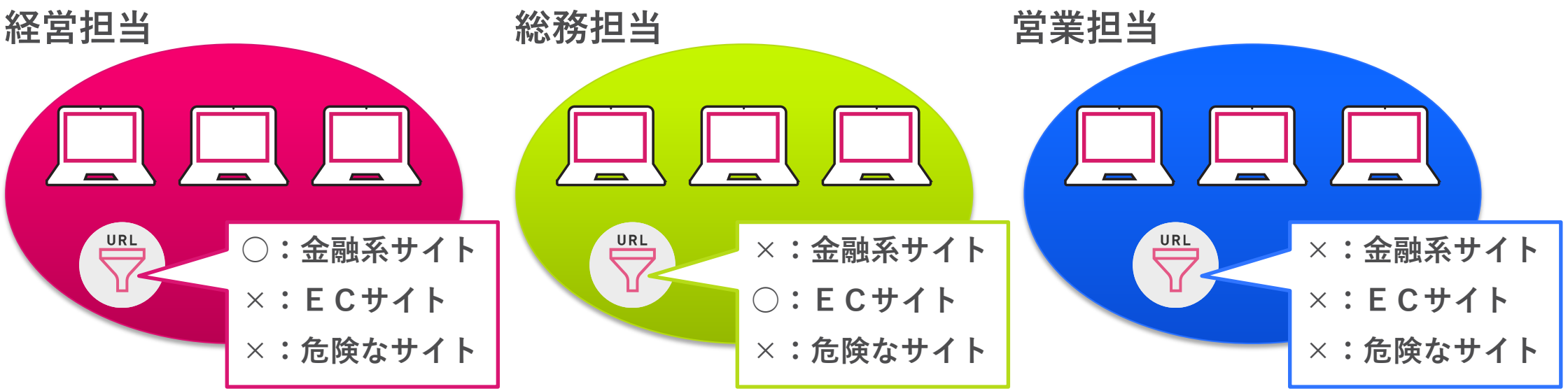
- クライアントのバージョンを最新バージョンにアップグレードしてください

# バーチャルグループによる管理

- バーチャルグループの概要
- バーチャルグループの作成
- バーチャルグループへのコンピュータの追加、削除
- バーチャルグループへのポリシーの適用

# バーチャルグループの概要

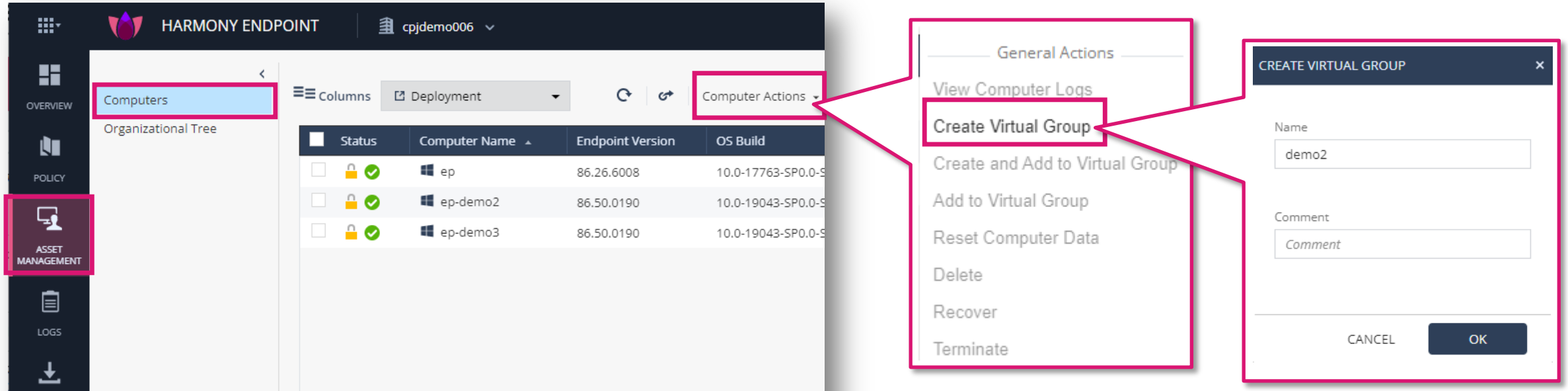
- 組織や役職などに応じて、ポリシーやセキュリティ機能、クライアントのバージョンなどをコンピュータが所属するグループでカスタマイズすることができます
- Harmony Endpoint で作成するグループを、「バーチャルグループ」といいます
- OSやコンピュータ種別に応じて事前定義されたバーチャルグループを使用することもできます
- バーチャルグループは、インストールパッケージを作成する際に指定することも、クライアントをインストール後に追加、削除することもできます



# バーチャルグループの作成（１／２）

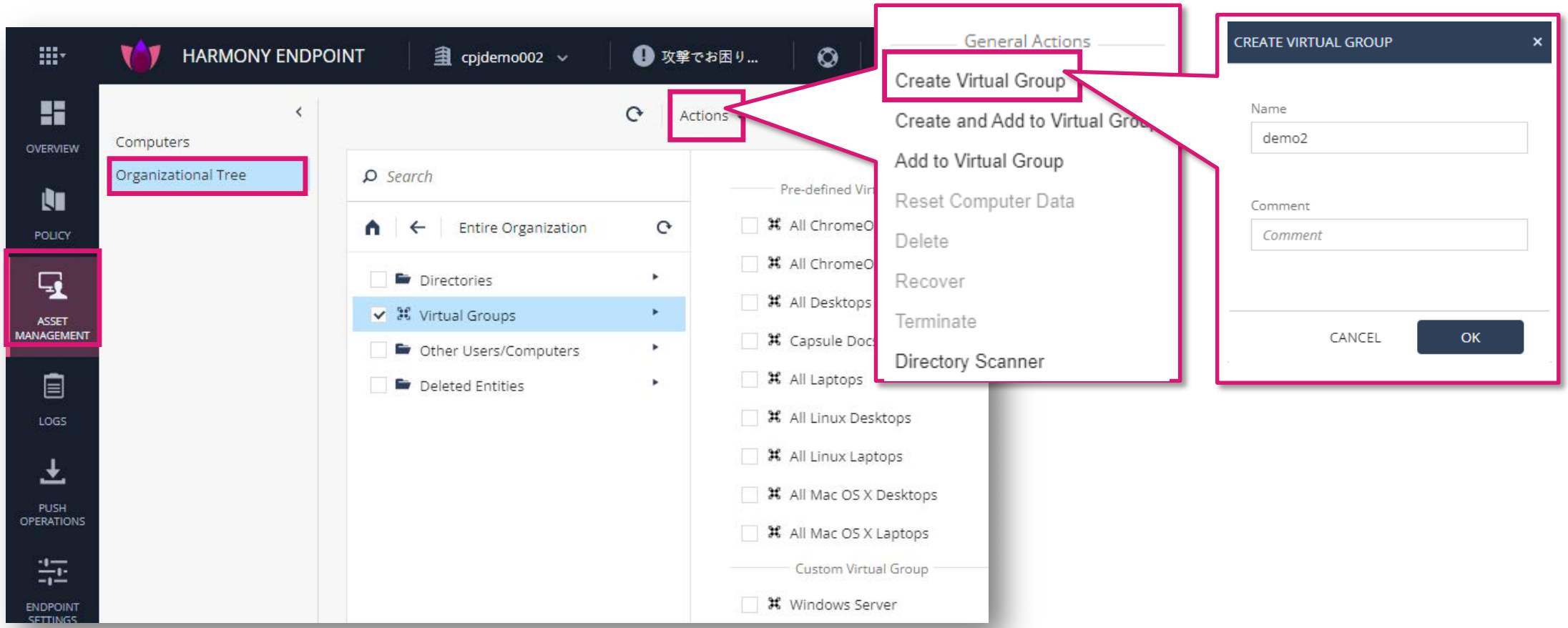
- バーチャルグループの作成は、以下の２つの方法で可能です
  - Asset Management > Computers > Computer Actions
  - Asset Management > Organizational Tree

## Asset Management > Computers > Computer Actions での作成方法



# バーチャルグループの作成（２／２）

## Asset Management > Organizational Tree > Actions での作成方法



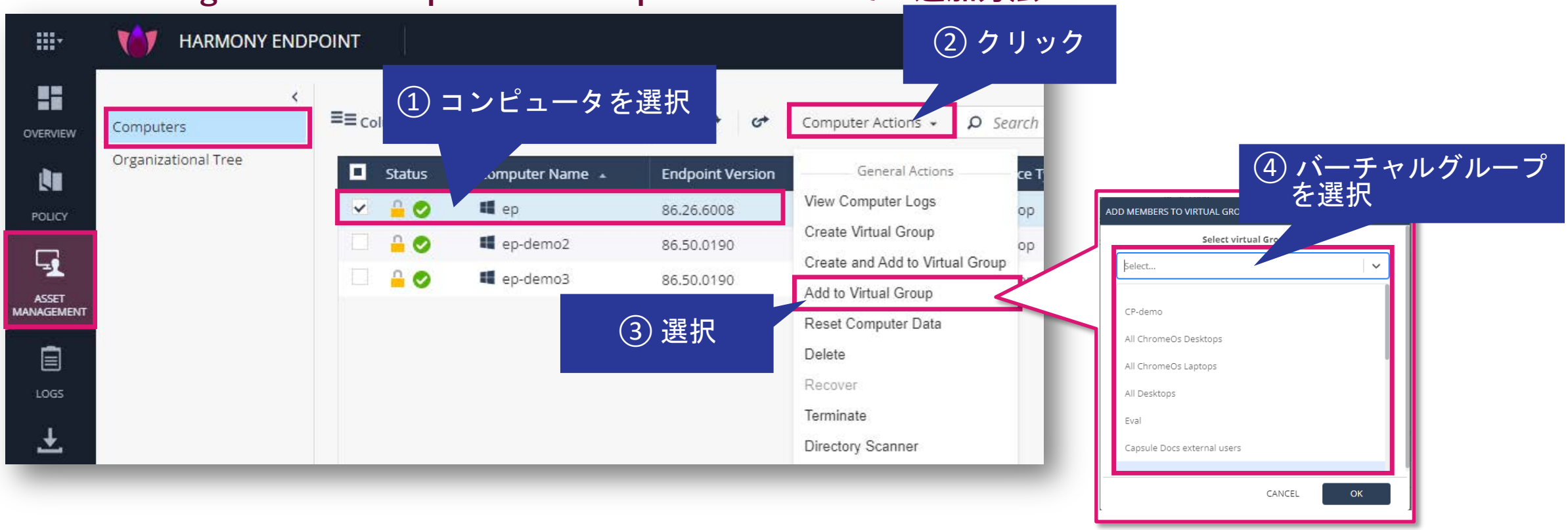
# バーチャルグループへのコンピュータの追加、削除（１／４）

- バーチャルグループ用のインストールパッケージを作成することで、インストール時にバーチャルグループに所属させることができます（後述）
- インストール後にバーチャルグループへの追加、削除を行えます
- バーチャルグループへの追加、削除は、１台ずつもしくは複数台まとめて行えます
- バーチャルグループへのコンピュータの追加、削除は、以下の２つの方法で可能です
  - Asset Management > Computers > Computer Actions
  - Asset Management > Organizational Tree

# バーチャルグループへのコンピュータの追加、削除（２／４）

- コンピューター一覧でコンピュータを選択し、Computer Actions メニューから Add to Virtual Groupを選択する
- 複数台のコンピュータを同時にバーチャルグループへ追加する時は、対象のコンピュータをすべて選択して、Computer Actions > Add to Virtual Group を選択する

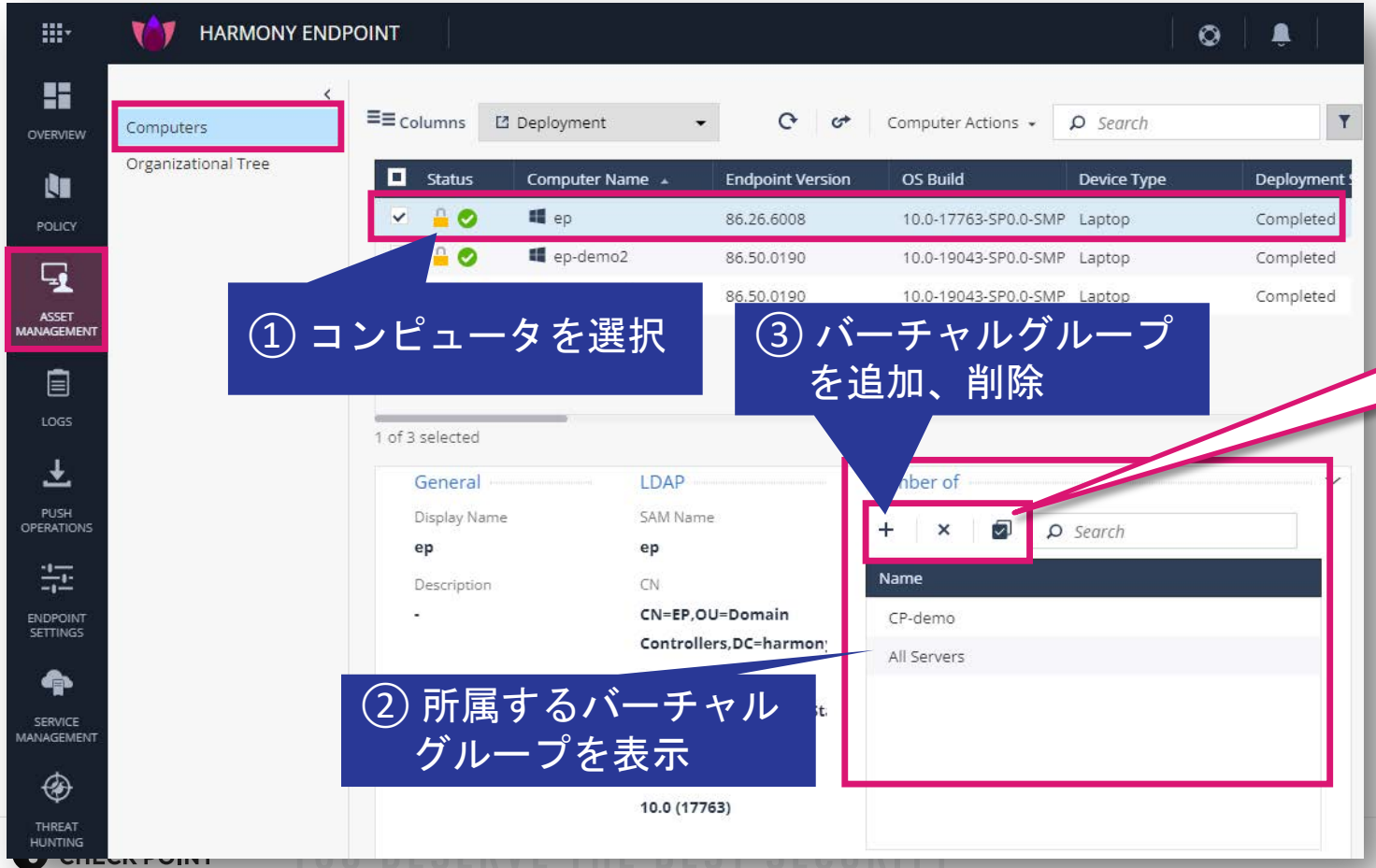
## Asset Management > Computers > Computer Actions での追加方法

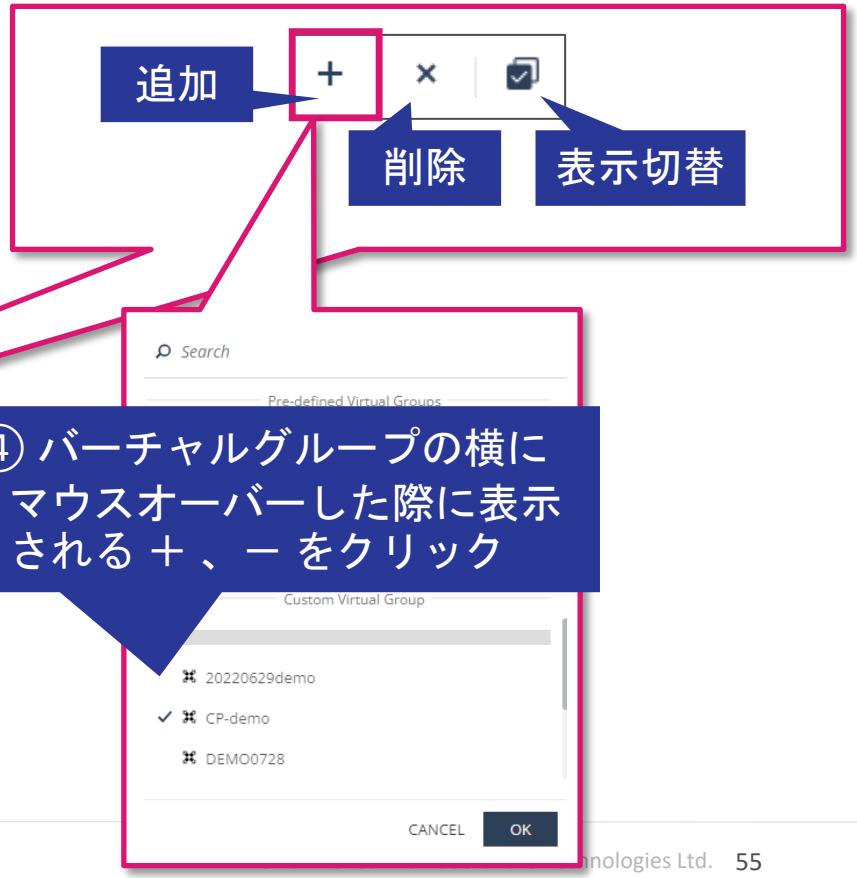


# バーチャルグループへのコンピュータの追加、削除（３／４）

- コンピューター一覧でコンピュータを選択すると、所属するバーチャルグループが表示される
  - 追加： ＋ をクリックし、バーチャルグループの一覧から所属させるグループを選択
  - 削除：表示されたバーチャルグループを選択し、 × をクリック

## Asset Management > Computers での追加、削除方法

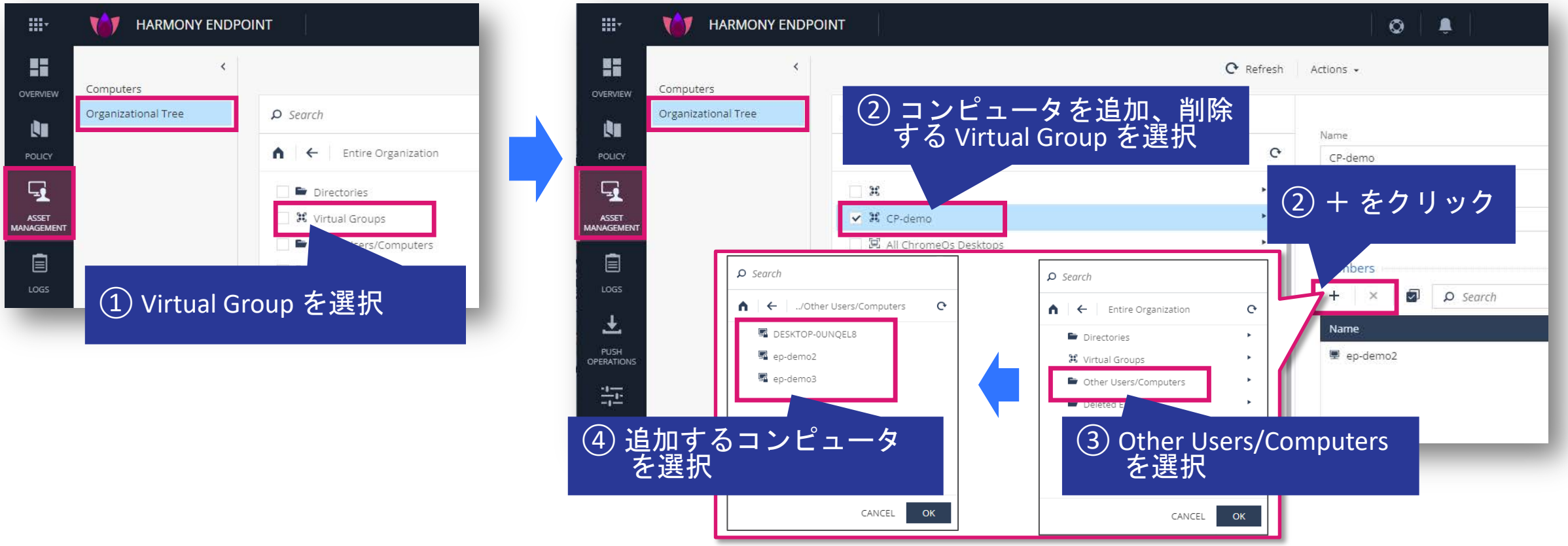


# バーチャルグループへのコンピュータの追加、削除（４／４）

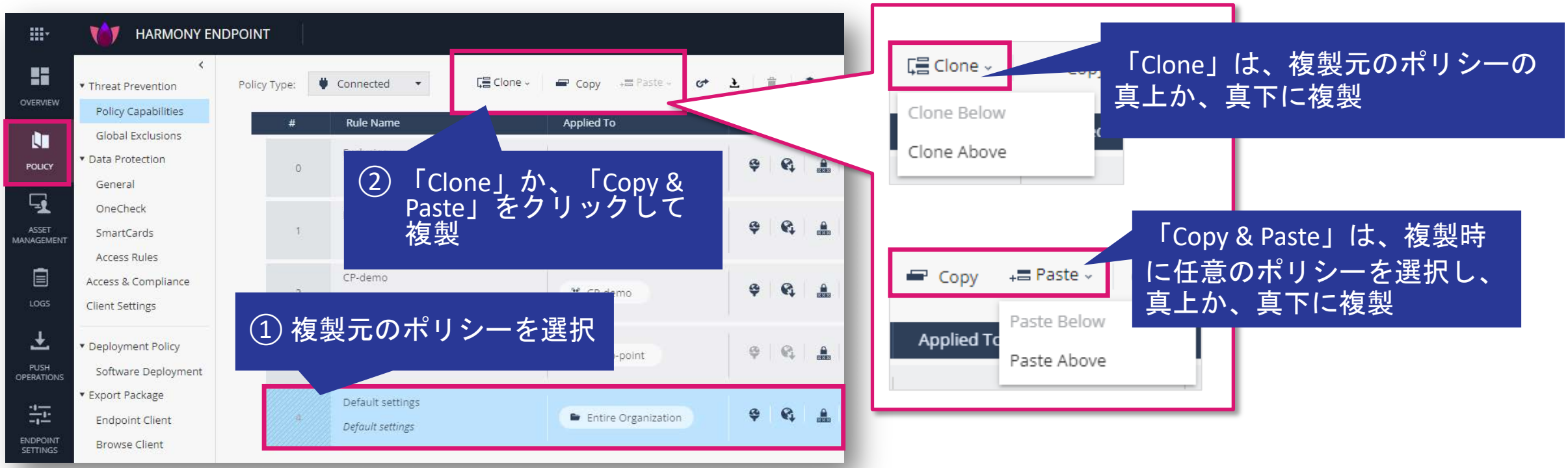
- Organizational Tree で Virtual Group を選択して、コンピュータを追加、削除する

## Asset Management > Organizational Tree での追加方法



# バーチャルグループへのポリシーの適用（1／2）

- バーチャルグループに適用するポリシーを作成する際は、既存のポリシーを複製し、適用するバーチャルグループを選択します
- Threat Prevention、Data Protection、Access & Compliance、Client Settings、Deployment Policy で適用するバーチャルグループを設定できます



# バーチャルグループへのポリシーの適用（2／2）

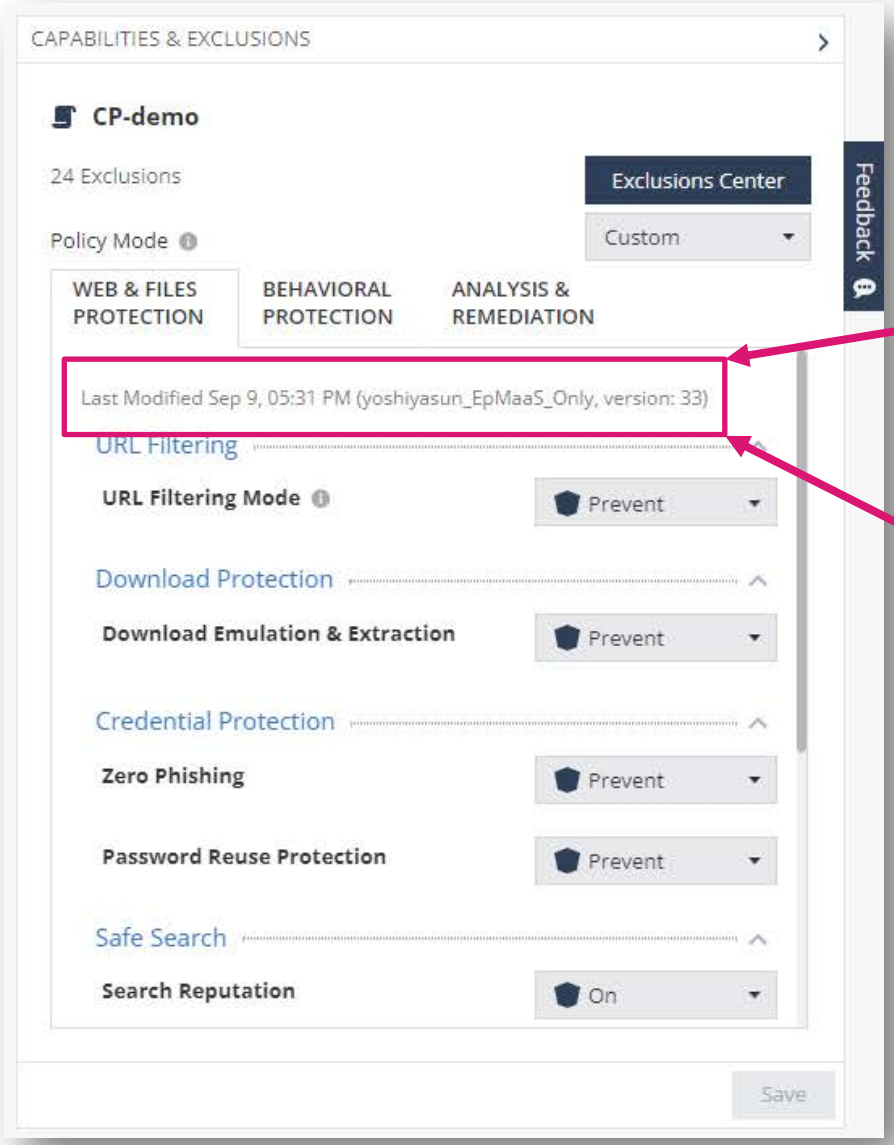
- 表示されたダイアログボックスで、ポリシーの名前と適用対象を設定します
- バーチャルグループ以外に、コンピュータや Active Directory の OU に適用できます
  - Active Directory の OU に適用できるのは、AD Scanners を設定した場合のみです

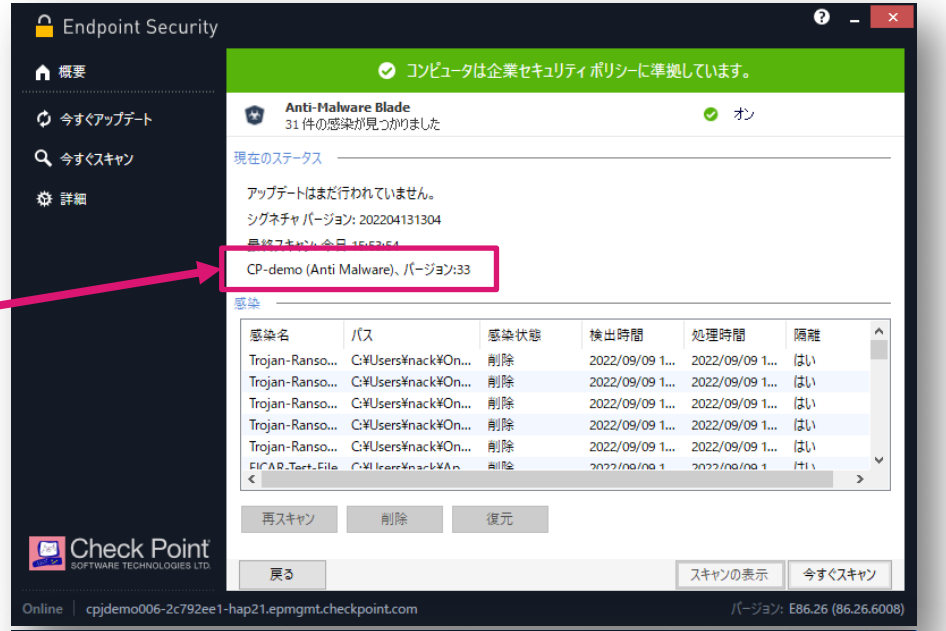
# 【演習】

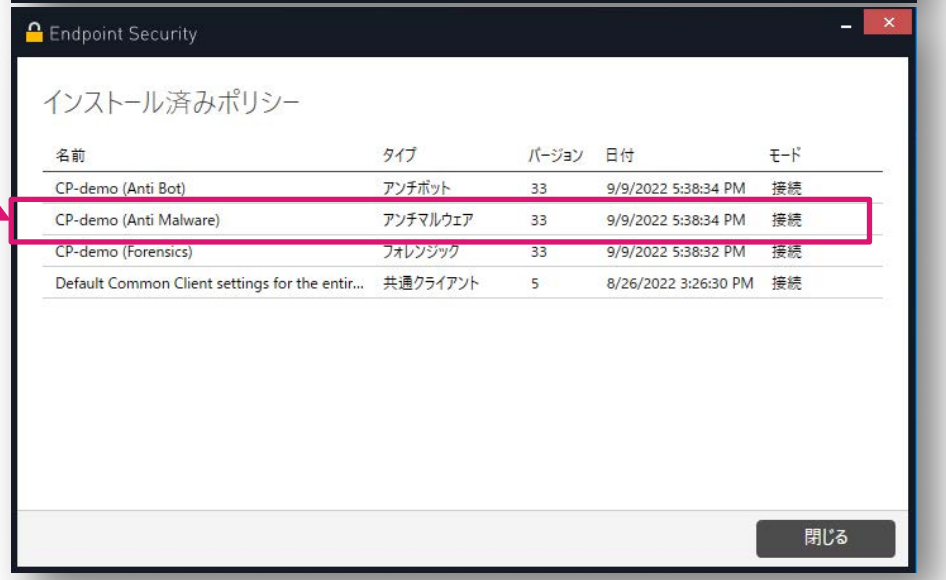
- 任意の名前のバーチャルグループを作成してください。

# ポリシーバージョンの確認

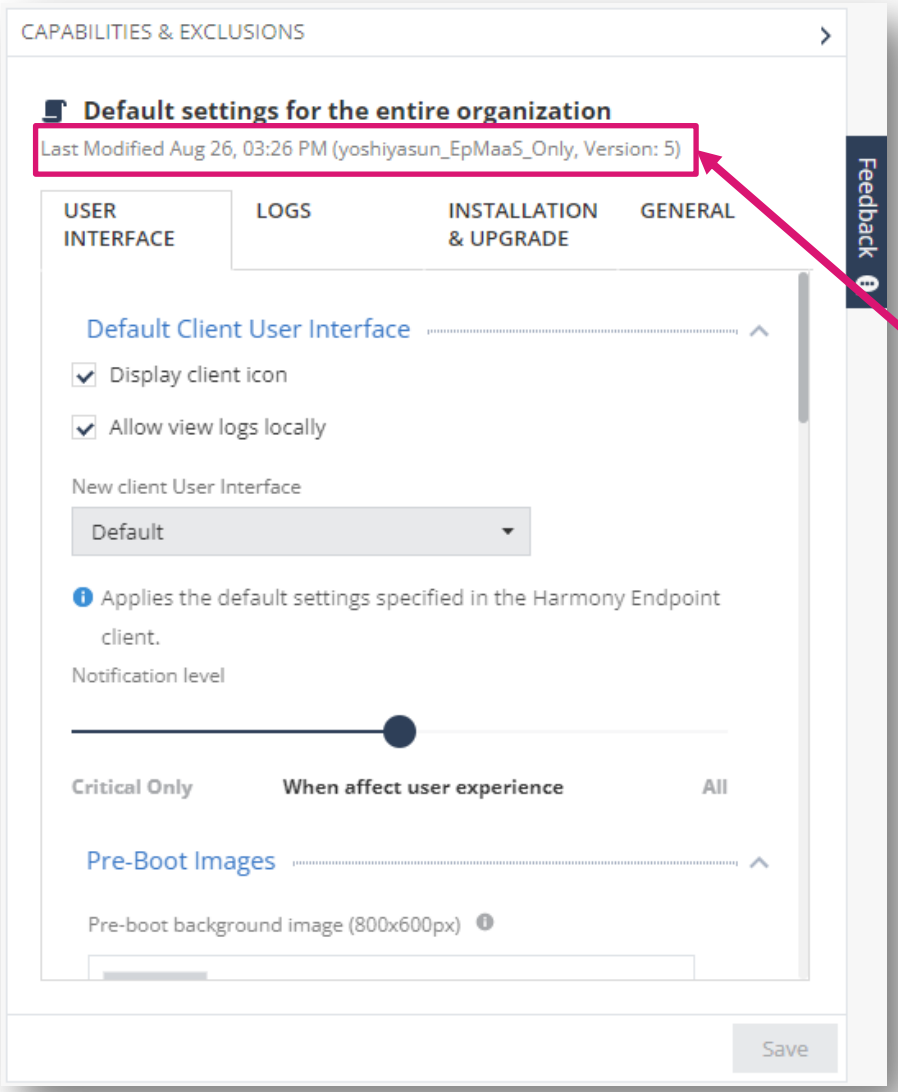
# ポリシーバージョンの確認：Threat Prevention



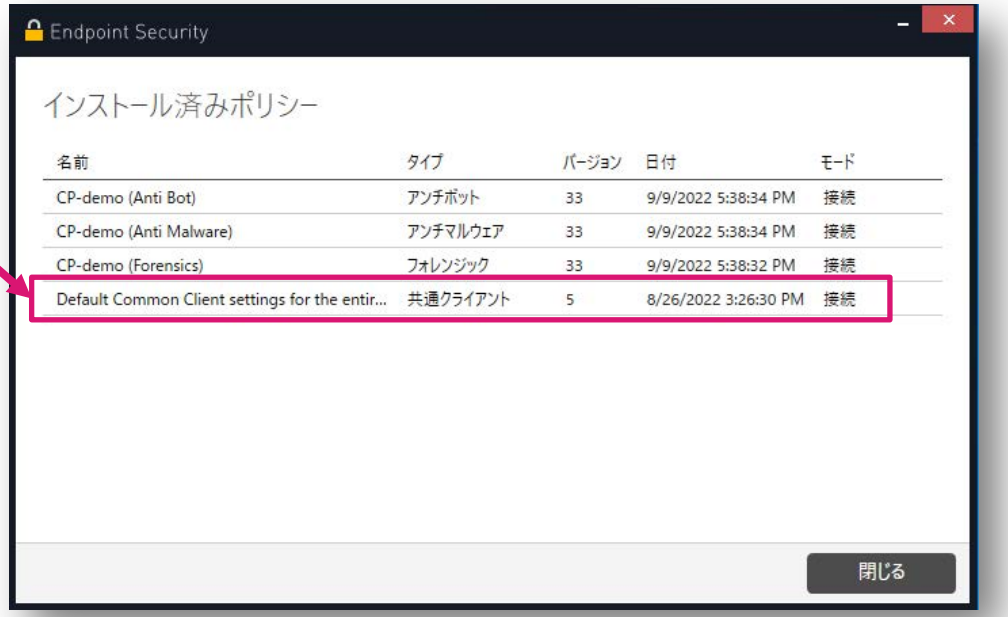



# ポリシーバージョンの確認：Client Settings




Client Settings のポリシーバージョンを確認する際は、クライアントソフトウェアで「概要の表示 > 詳細 > ポリシーの表示」を選択してください。



# THREAT PREVENTION 設定

- 共通
- ダウンロード保護（Threat Emulation、Threat Extraction）
- 認証情報の保護（Zero-Phishing、Password Reuse Protection）
- アンチ・ランサムウェア

YOU DESERVE THE BEST SECURITY

ポリシーの設定

# THREAT PREVENTION
# 共通

YOU DESERVE THE BEST SECURITY

# Threat Prevention：共通（1／5）

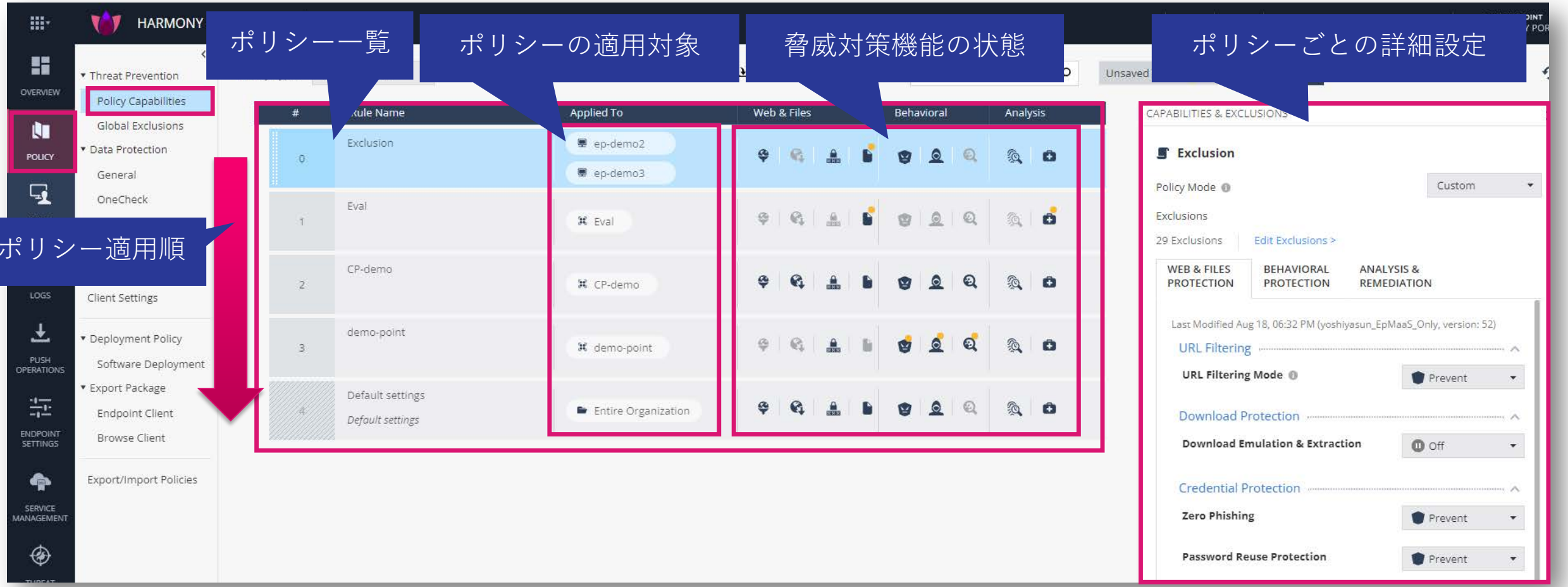
Policy > Threat Prevention

- Threat Prevention では脅威対策機能に関する設定を構成します
  - Web & Files Protection
    - URL フィルタリング
    - ダウンロード保護（サンドボックス、ファイル無害化）
    - 認証情報の保護（ゼロ・フィッシング、企業パスワード保護）
    - 安全な検索（セーフ・レピュテーション、セーフ・サーチ）
    - ファイル保護（アンチ・マルウェア、サンドボックス）
  - Beavioral Protection
    - アンチ・ボット
    - 振る舞い検査
    - アンチ・ランサムウェア
    - アンチ・エクスプロイト
  - Analysis & Remediation
    - 攻撃解析（フォレンジクス）
    - 修復

# Threat Prevention：共通（２／５）

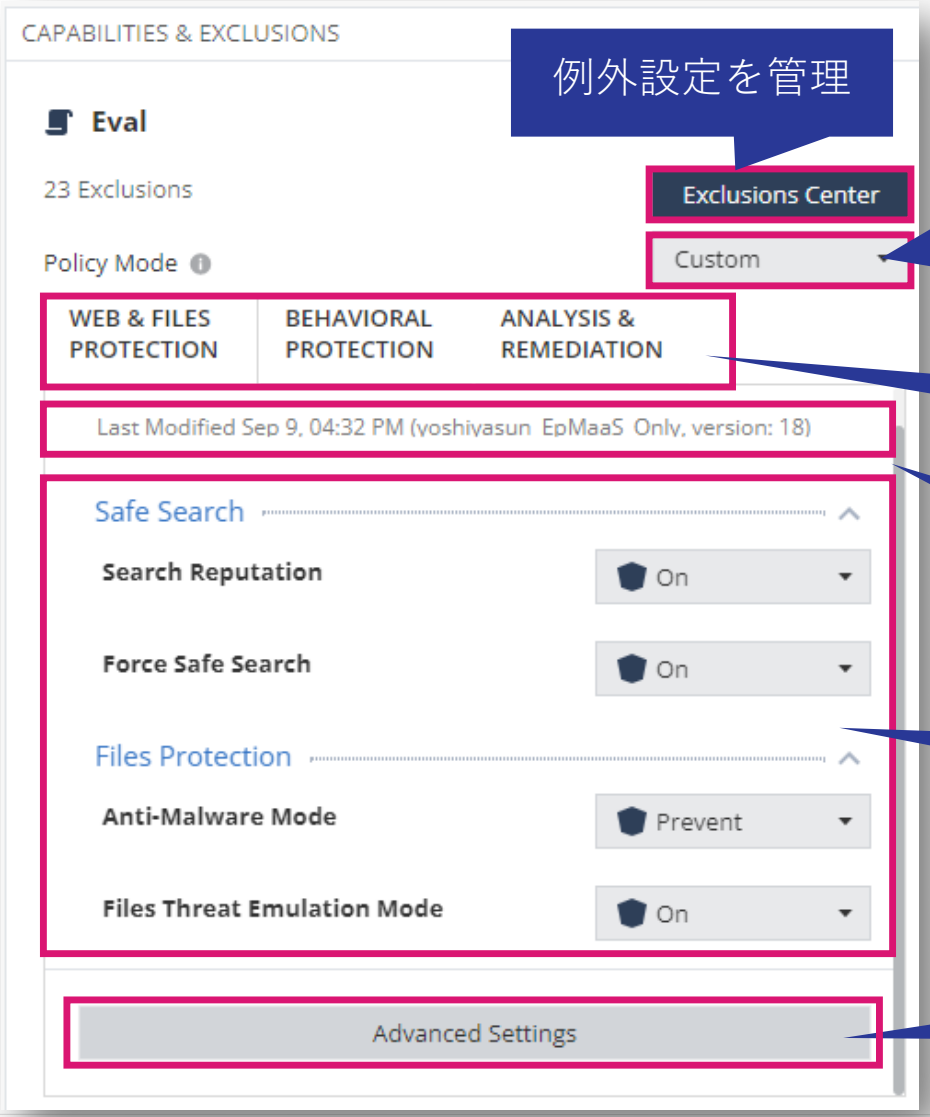
Policy > Threat Prevention

- バーチャルグループを使用して、組織ごとに異なるポリシーを設定できます
- コンピュータが複数のポリシーの適用対象になっている場合、若番のポリシーが適用されます



# Threat Prevention：共通（3／5）

Policy > Threat Prevention




例外設定を管理

事前定義された設定を選択

- Tuning
- Recommended
- Default
- Strict

脅威対策のカテゴリを選択

ポリシーのバージョンを表示

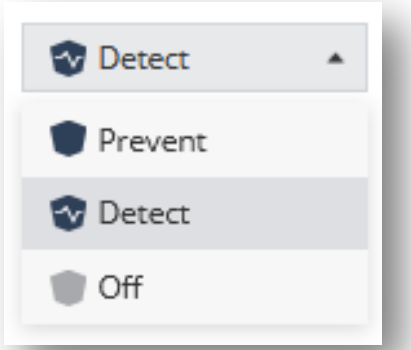
セキュリティ対策機能の動作モードを選択

セキュリティ対策機能の詳細を設定

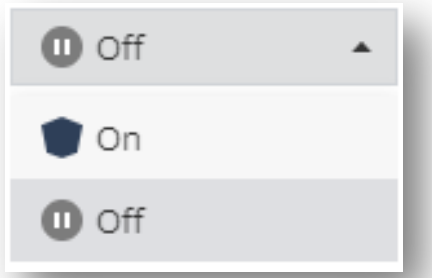
# Threat Prevention：共通（４／５）

Policy > Threat Prevention

- 脅威に対する動作モードの設定方法は、２通りあります
  1) Prevent / Detect / Off
  2) On / Off




- 動作モードの選択肢①
  - Prevent　：脅威を阻止（ブロック）し、ログに記録
  - Detect　：脅威を検出し、ログに記録
  - Off　：機能を無効化

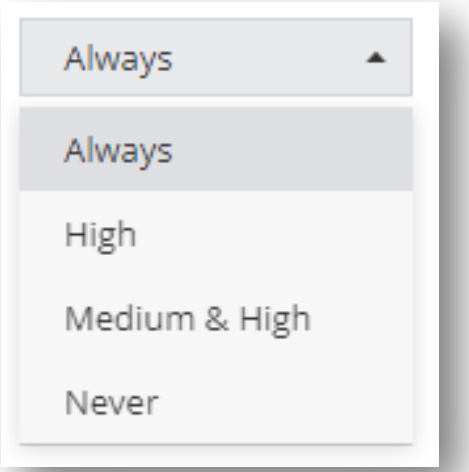



- 動作モードの選択肢②
  - On　：機能を有効化
  - Off　：機能を無効化

# Threat Prevention：共通（５／５）

Policy > Threat Prevention

- Confidence Levelは、インシデントやファイルが悪意があることの確実性です。
- 「High」は、悪意があることがほぼ確実です。
- 「Medium」は、悪意がある可能性が非常に高いです。




- Confidence Level による動作の選択肢
  - Always　　：常に実行
  - High　　：High の場合のみ実行
  - Medium & High　　：Medium と High の場合に実行
  - Never　　：実行しません

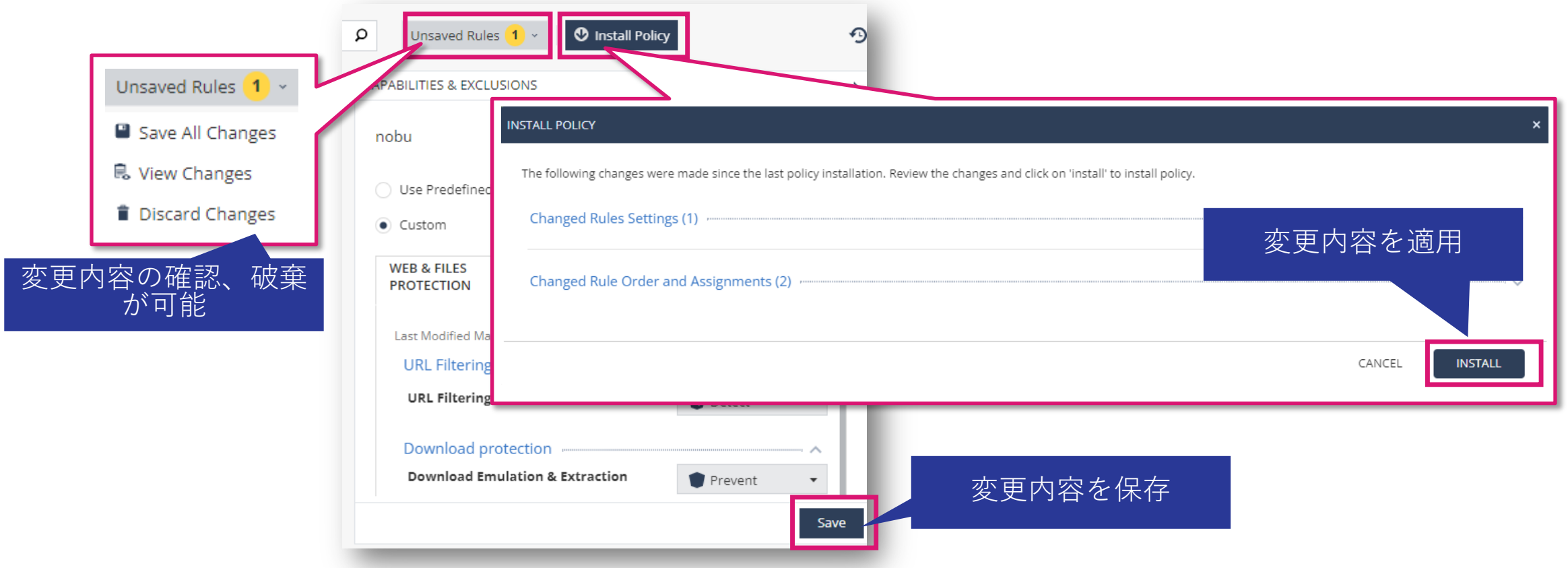
ポリシーの設定

# ポリシーの SAVE と INSTALL

# ポリシーの Save と Install

Policy

- Web UI で設定・変更したポリシーは、ポリシーのインストールを行うまで、コンピュータに適用されません。変更を確定するにはポリシーをセーブして、インストールします
- セーブする前であれば、変更を取り消すことが可能です



ポリシーの設定

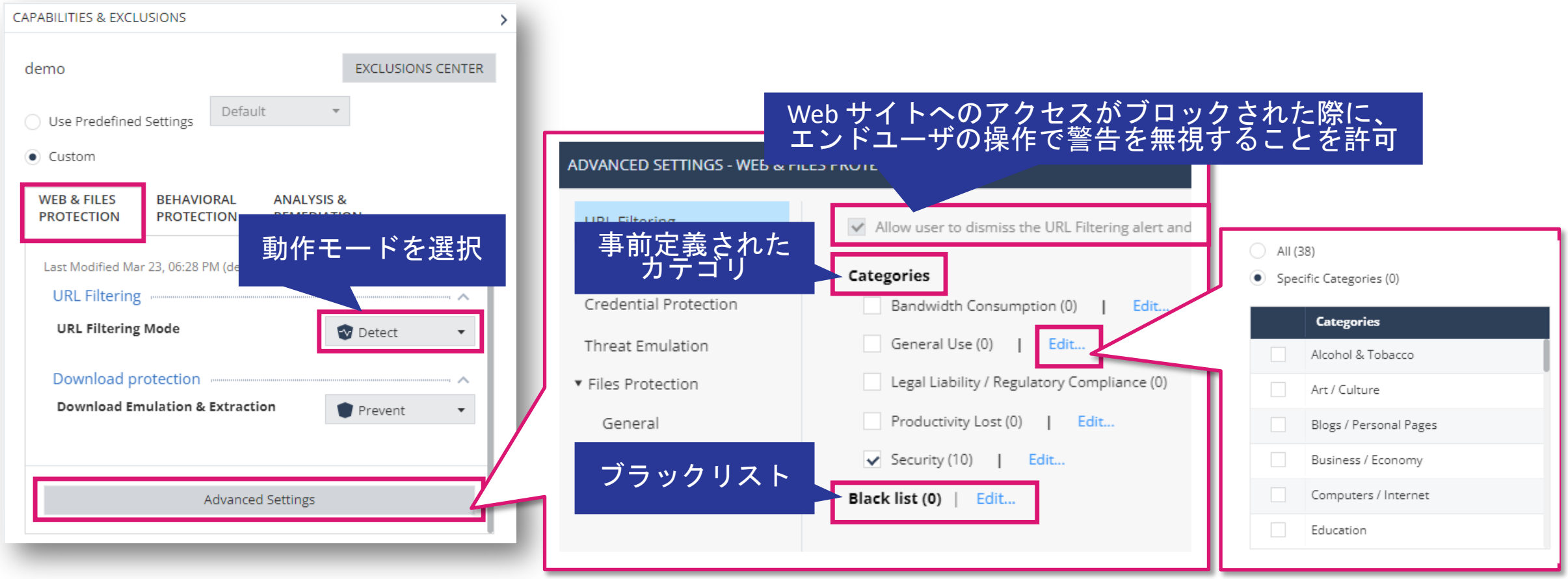
# THREAT PREVENTION
# URL フィルタリング

YOU DESERVE THE BEST SECURITY

# Threat Prevention：URL フィルタリング

Policy > Threat Prevention > Web & Files Protection > URL Filtering

- URL フィルタリングは、組織内でアクセスできるサイトを定義します
- Advanced Settings で、カテゴリの選択、ブラックリストの登録を構成します
- 各カテゴリは、さらに詳細なカテゴリの選択を構成できます



# 【演習】URL フィルタリング

- 以下のカテゴリをブロック設定して、各カテゴリに該当する Web サイトへのアクセスがブロックされることを確認してください。
  - アルコール＆タバコ
  - スポーツ
  - 翻訳
  - 旅行

- ブロック画面で、「詳細」をクリックし、ブロックサイトへのアクセス理由を選択すると、ブロックサイトへアクセスできることを確認してください。
  - 接続先が安全なサイトであることを確認した上でアクセスしてください。

ポリシーの設定

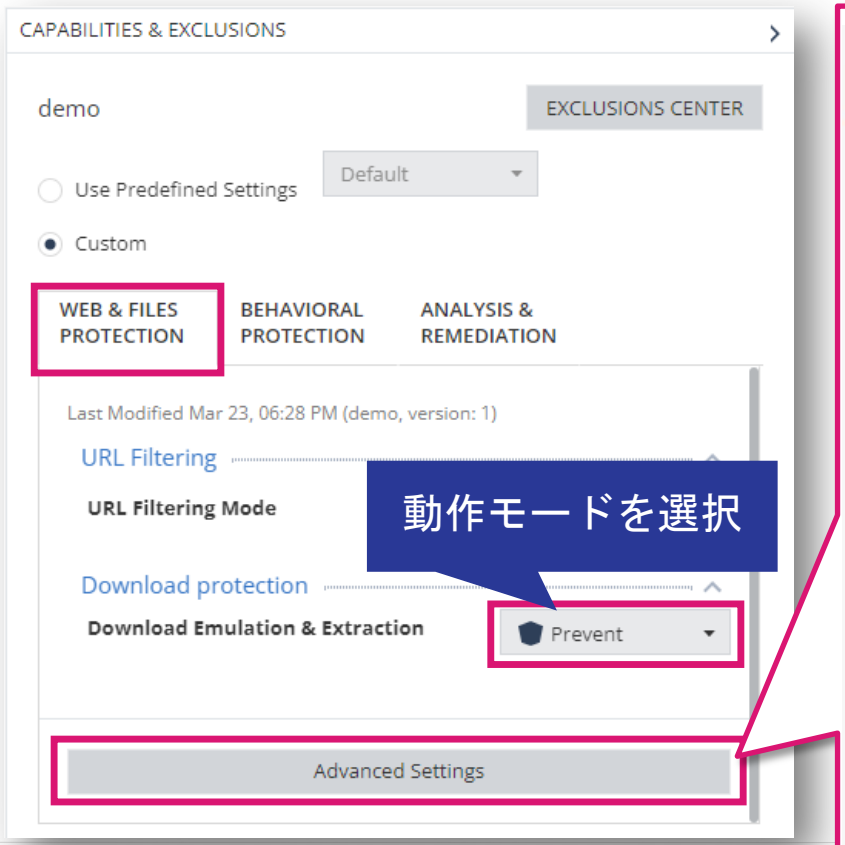
# THREAT PREVENTION DOWNLOAD 保護

- Threat Emulation（Sandbox）
- Threat Extraction（無害化）

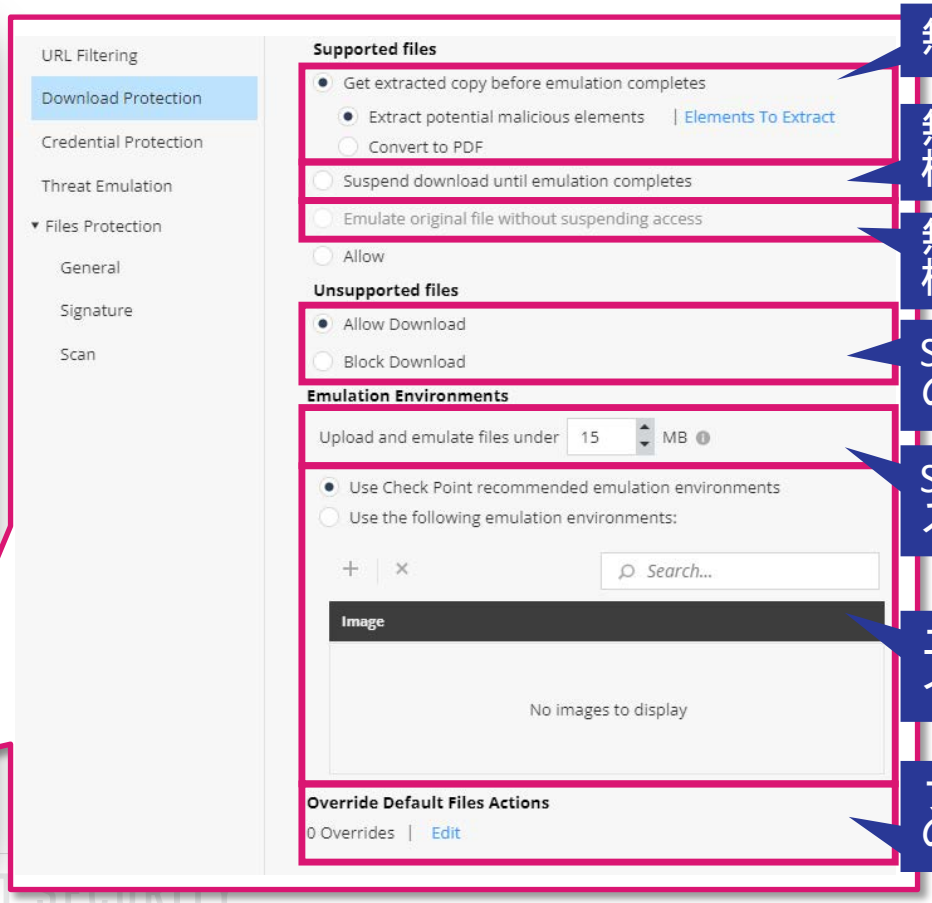
# Threat Prevention：Download 保護（1／2）

Policy > Threat Prevention > Web & Files Protection > Download Protection

- Web ダウンロードに対するThreat Emulationと、Threat Extractionの設定を構成します
- 動作モードを「Detect」にした場合、ファイルへのアクセスを中断せずに Threat Emulation による検査のみ実施し、インシデントをログに記録します




動作モードを選択




無害化の有効化と、モードの選択

無害化を無効化し、Sandbox での検査完了までダウンロードを保留

無害化を無効化し、Sandbox での検査完了前にダウンロードを許可

Sandbox、無害化機能で未サポートのファイルのダウンロード可否

Sandbox で検査するファイルサイズの上限

エミュレーションが実行される OS イメージを選択

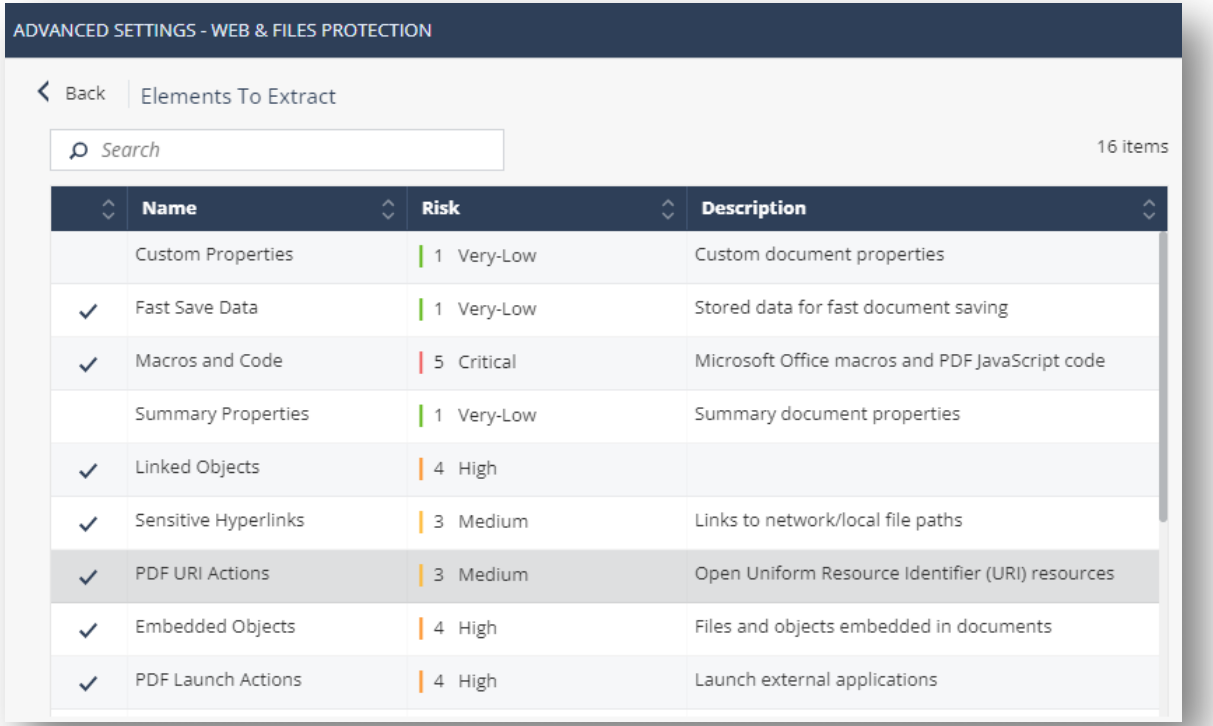
ファイルタイプごとのデフォルトのアクションを上書き

# Threat Prevention：Download 保護（2／2）

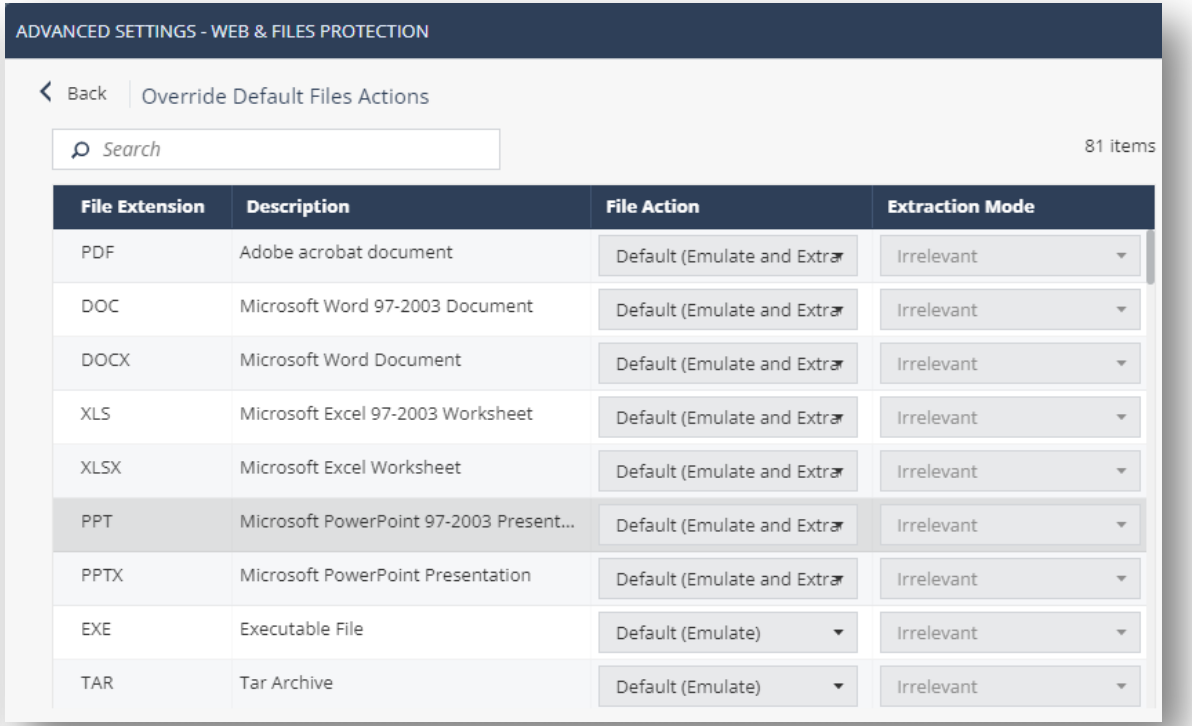
Policy > Threat Prevention > Web & Files Protection > Download Protection > Advance Settings

- Elements To Extract で、無害化を実施する要素を選択します
- Override Default Files Actions で、ファイル拡張子ごとの Threat Emulation と Threat Extraction の動作を構成します

## Elements To Extract




## Override Default Files Actions



# 【演習】サンドボックス＆ファイル無害化

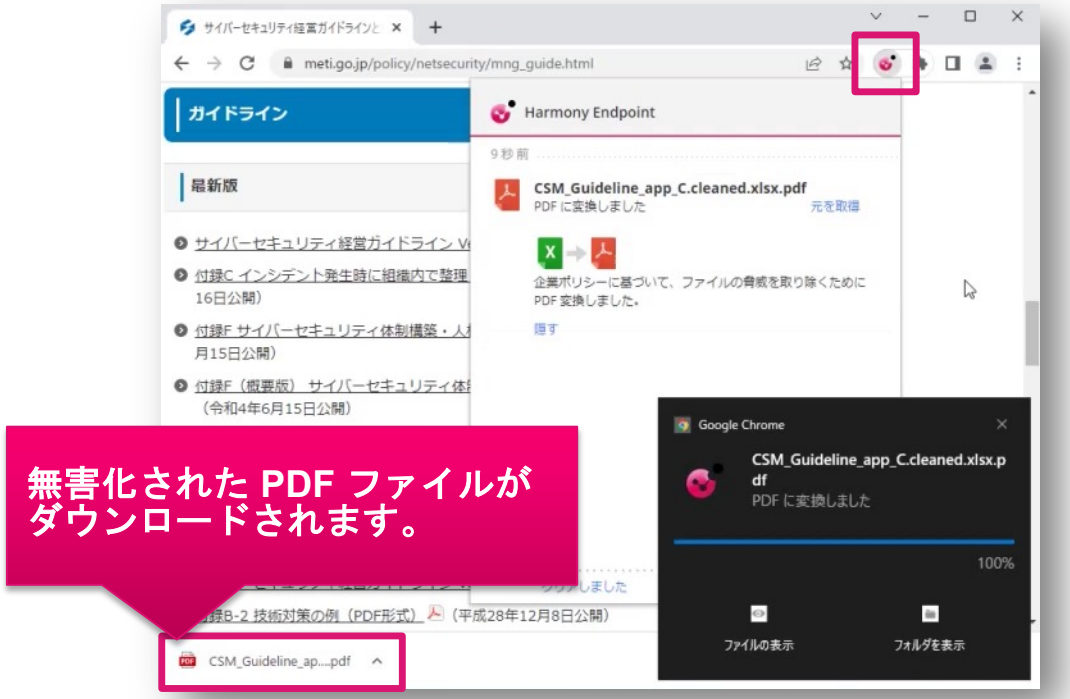
- Override Default Files Actions で、ファイル拡張子が、doc、xlsmの場合の File Action と、Extraction Mode を以下の様に設定して、動作の違いを確認してください

| File Extention | File Action | Extraction Mode |
|---|---|---|
| doc | Emulate and Extract | Convert to PDF |
| xlsm | Emulate and Extract | Extract Elements |

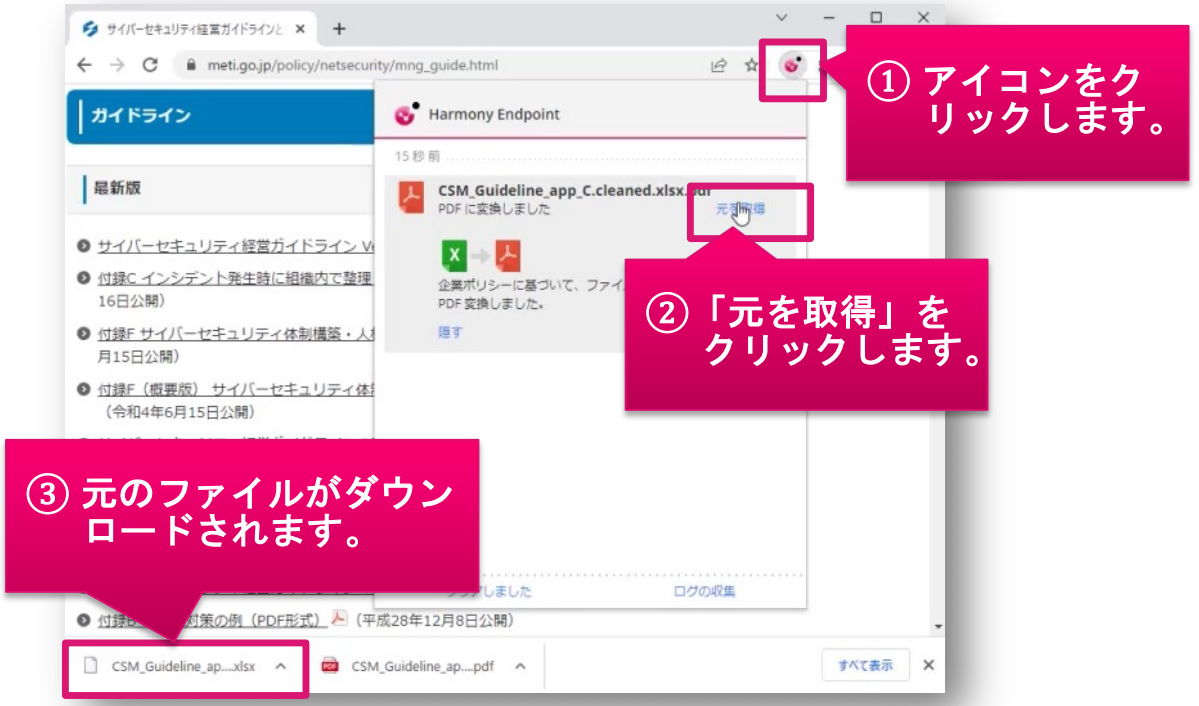
# 【参考】サンドボックス＆ファイル無害化の操作（１／２）

- OfficeファイルやPDFファイルのダウンロード時に、ファイルの無害化を行います
- ファイルの無害化と併行して、クラウドのサンドボックスで元のファイルの検査を行います
- 検査が終了し、元のファイルの安全性が確認できたら、元のファイルを取得することが可能になります

**ファイルの無害化**

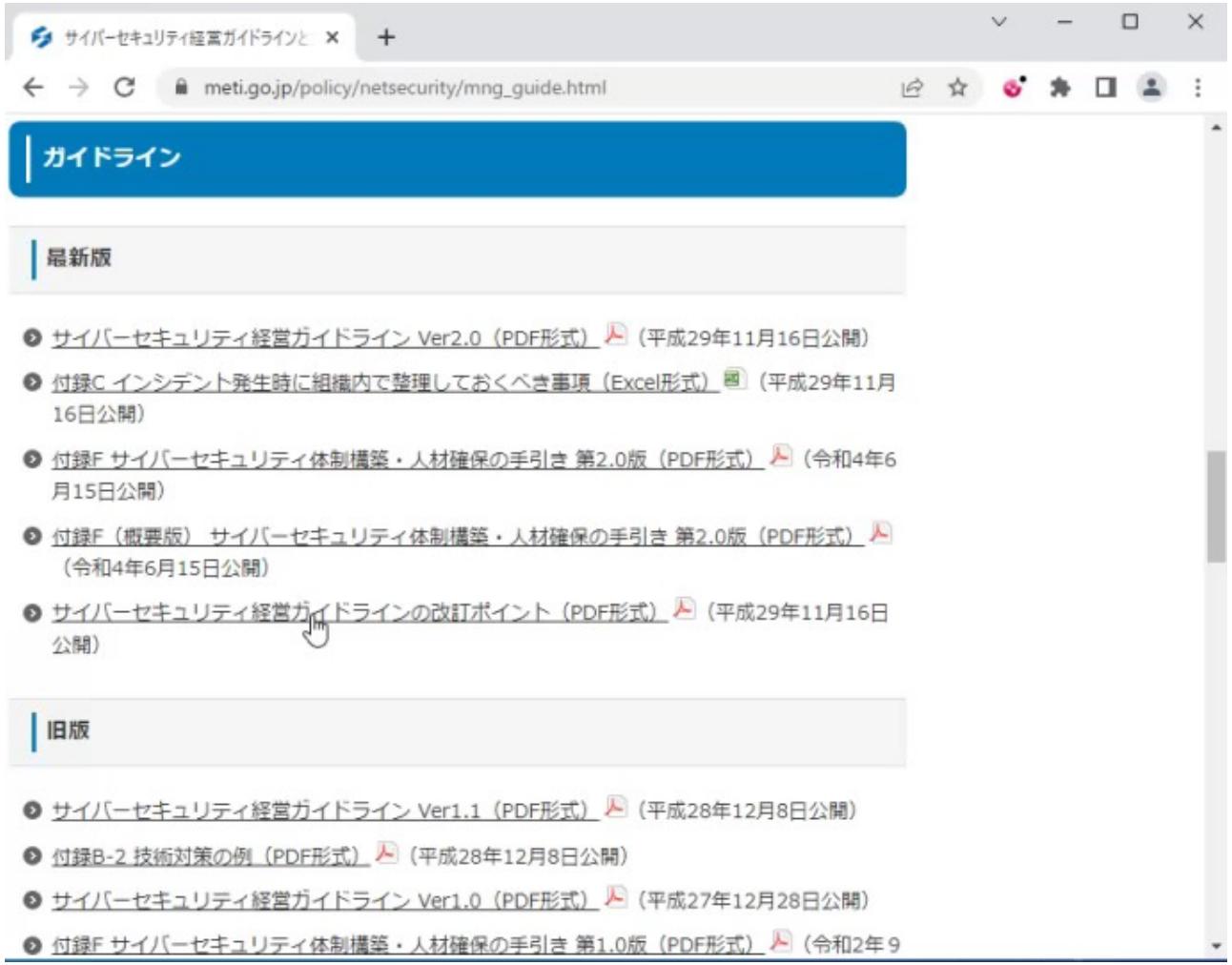



**元のファイルのダウンロード**



# 【参考】サンドボックス＆ファイル無害化の操作（２／２）

サンドボックス＆ファイル無害化の操作



ポリシーの設定

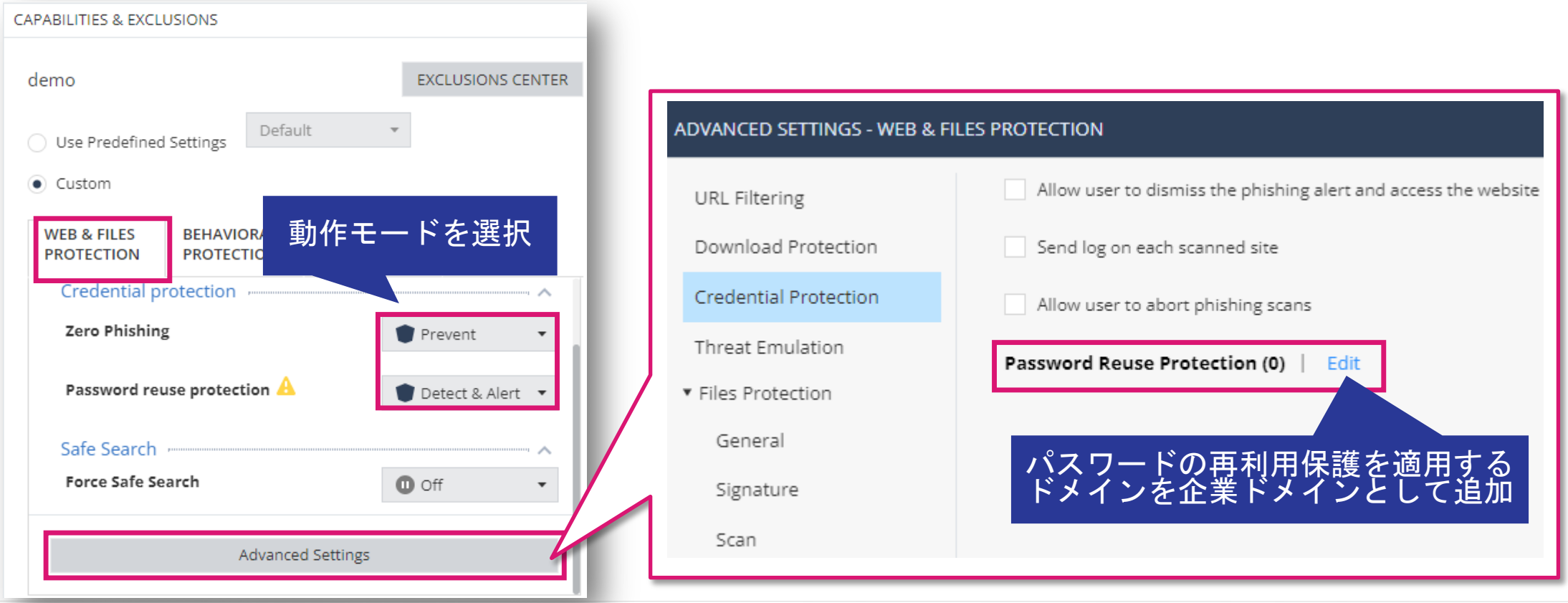
# THREAT PREVENTION
# 認証情報の保護

YOU DESERVE THE BEST SECURITY

# Threat Prevention：認証情報の保護

Policy > Threat Prevention > Web & Files Protection > Credential Protection

- Zero-Phishing は、Webサイトの様々な特性をチェックして、フィッシングサイトを検出します
- パスワードの再利用保護は、企業ドメインで利用されたパスワードのハッシュを記録し、同じパスワードを非企業ドメインで企業パスワードを使用しない様に警告します



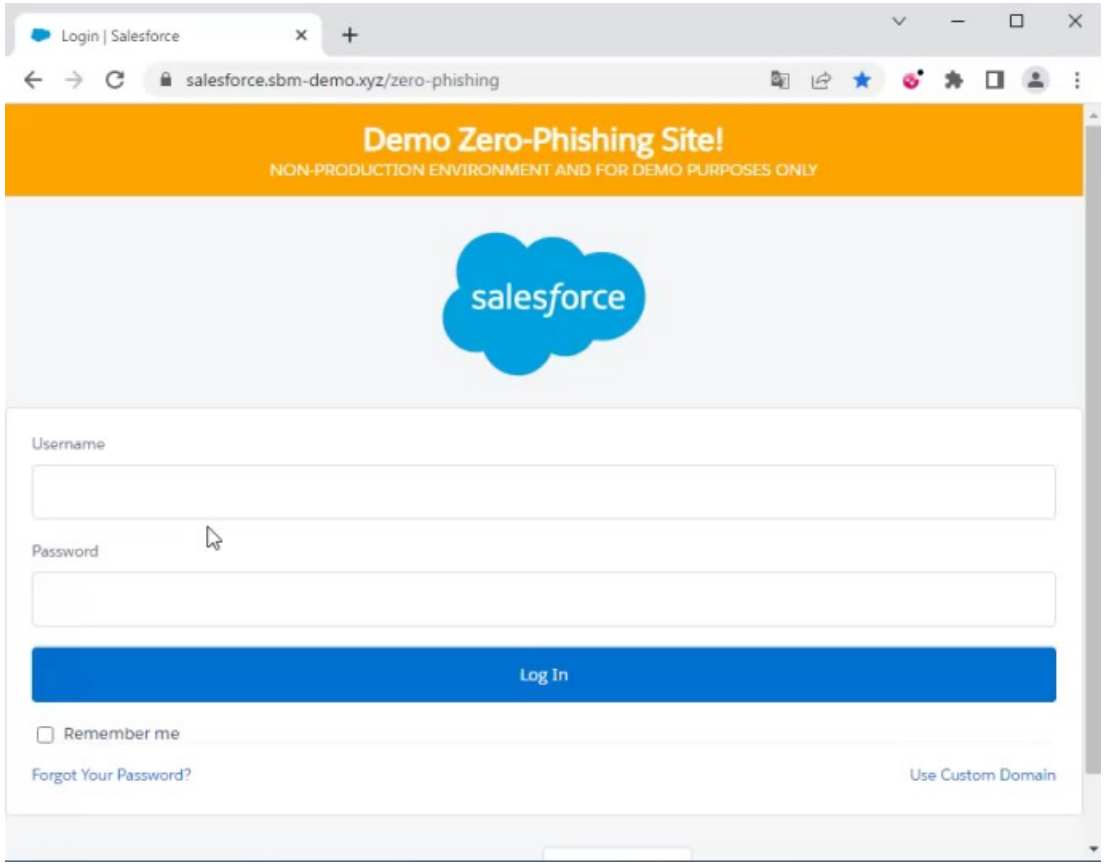
# 【演習】Zero-Phishing

- Google等で、“ログインページ”というキーワードで検索をして、Zero-Phishingの動作を確認してください

# 【参考】ゼロ・フィッシングの動作概要

## 正規のWebサイトへアクセスした際の動作概要

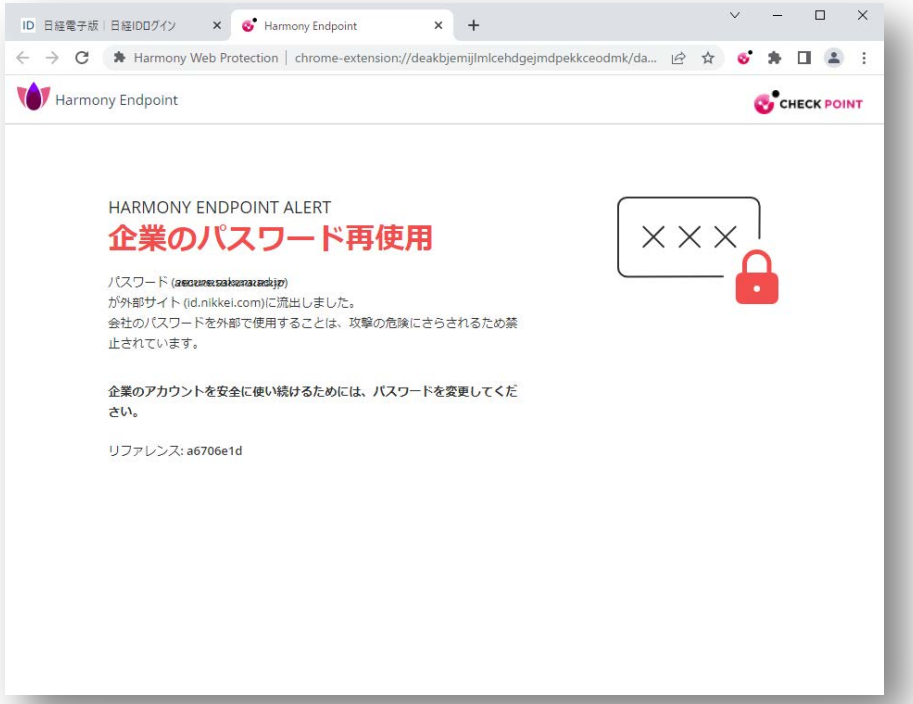

## フィッシングサイトへアクセスした際の動作概要



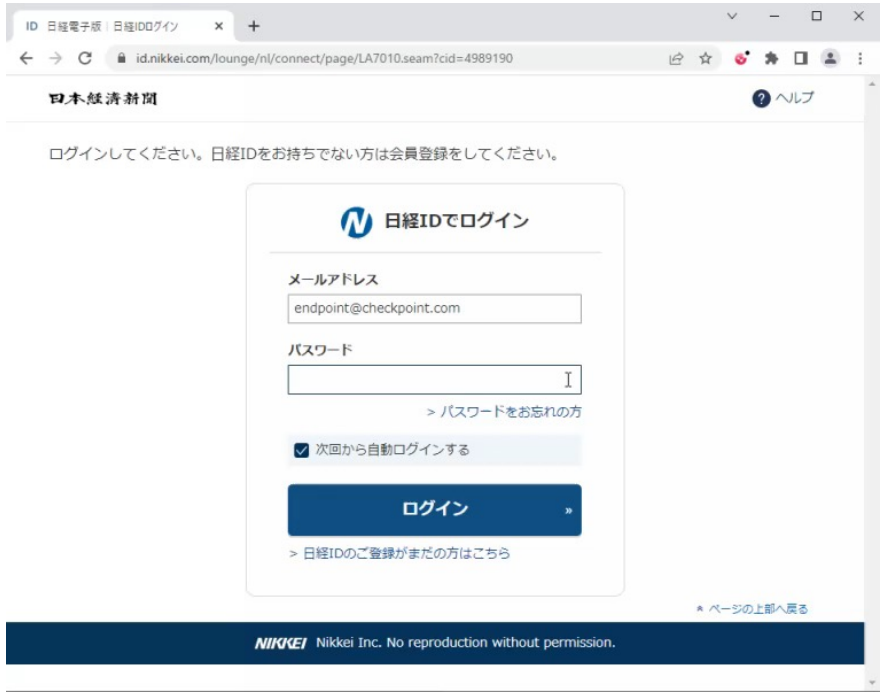
# 【参考】企業パスワード保護機能の動作概要

- 社内システムで使用しているパスワードを、インターネットのWebサイトで使用した際に、警告画面が表示されます。

**企業パスワード保護の警告画面の例**




**企業パスワード保護の動作概要**



ポリシーの設定

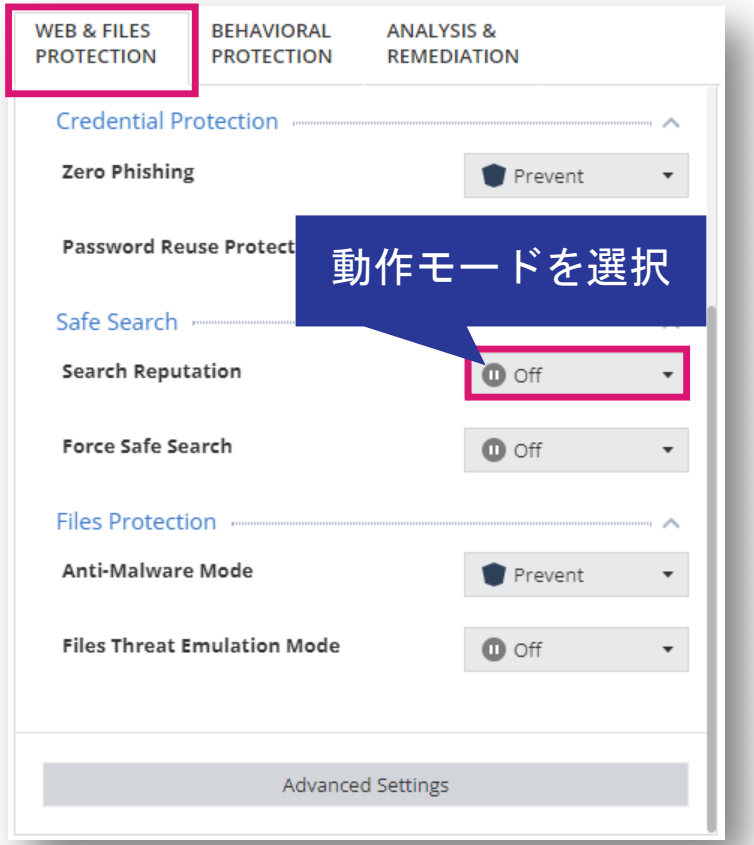
# THREAT PREVENTION
# 安全な検索

YOU DESERVE THE BEST SECURITY

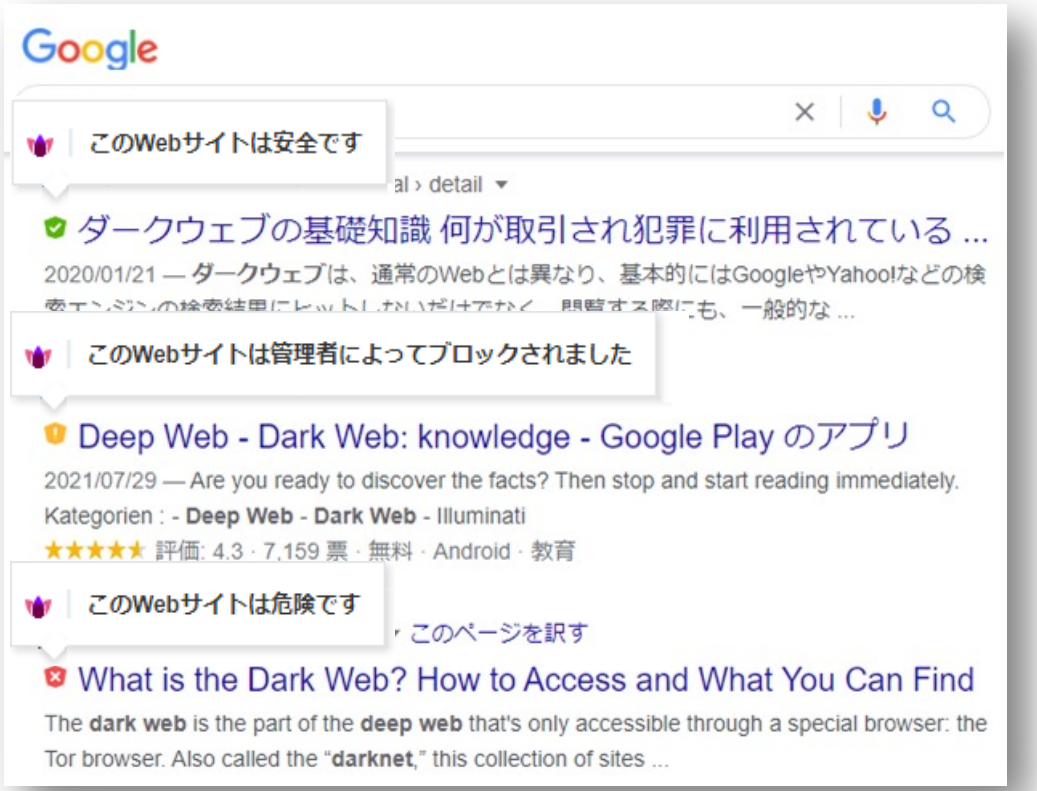
# Threat Prevention：サーチ・レピュテーション

Policy > Threat Prevention > Web & Files Protection > Search Reputation

- Google 検索エンジンでの検索結果をURL のレピュテーションに基づいて分類します。
- この機能を有効にするには、[URL フィルタリング モード] を [Prevent] または [Detect] に設定してください。




検索結果例



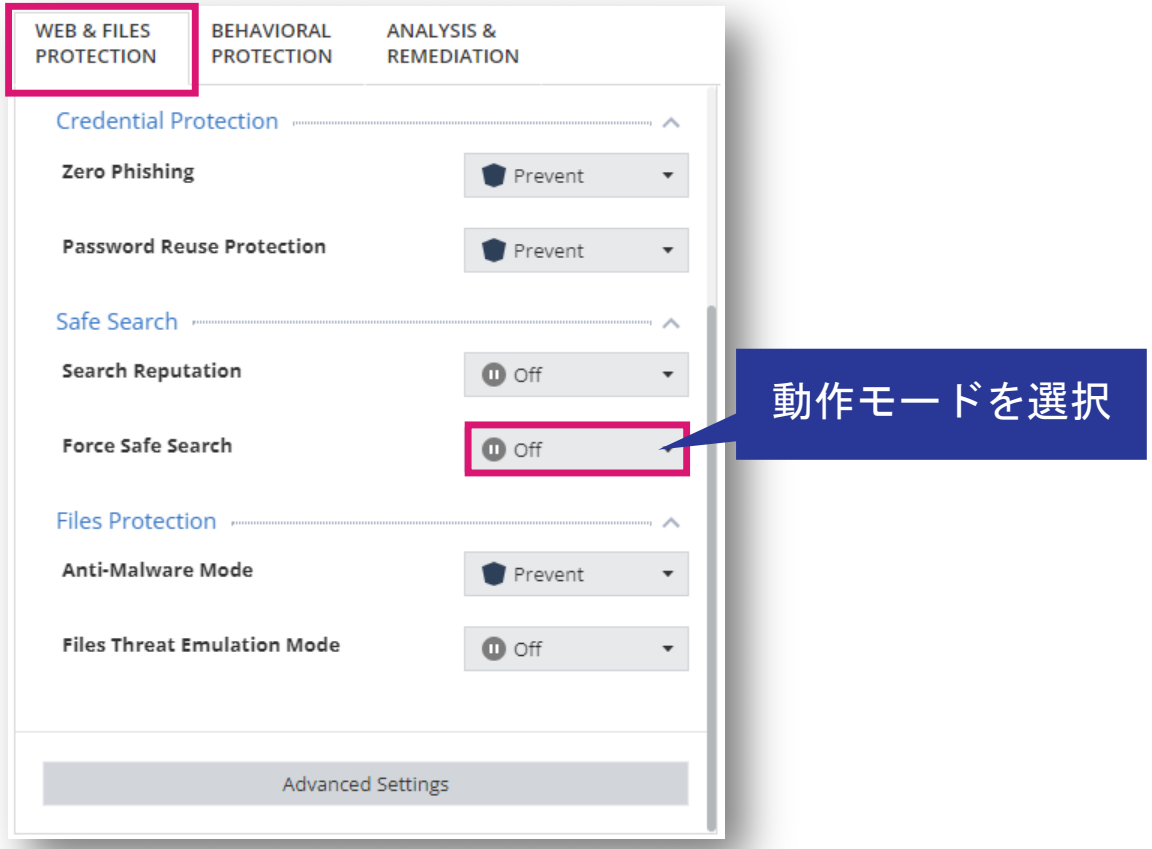

凡例

- 安全なサイト
- 管理者が禁止
- 危険なサイト

# Threat Prevention：セーフ・サーチ

Policy > Threat Prevention > Web & Files Protection > Safe Search

- 検索エンジンでのセーフサーチ機能の適用を制御します
- この機能は、Google、Bing、Yahooでのセーフサーチをサポートしています。



# 【演習】Search Reputation

- Google で任意のキーワードで検索をして、レピュテーションに基づく分類がされることを確認してください

ポリシーの設定

# THREAT PREVENTION
# ファイル保護

YOU DESERVE THE BEST SECURITY

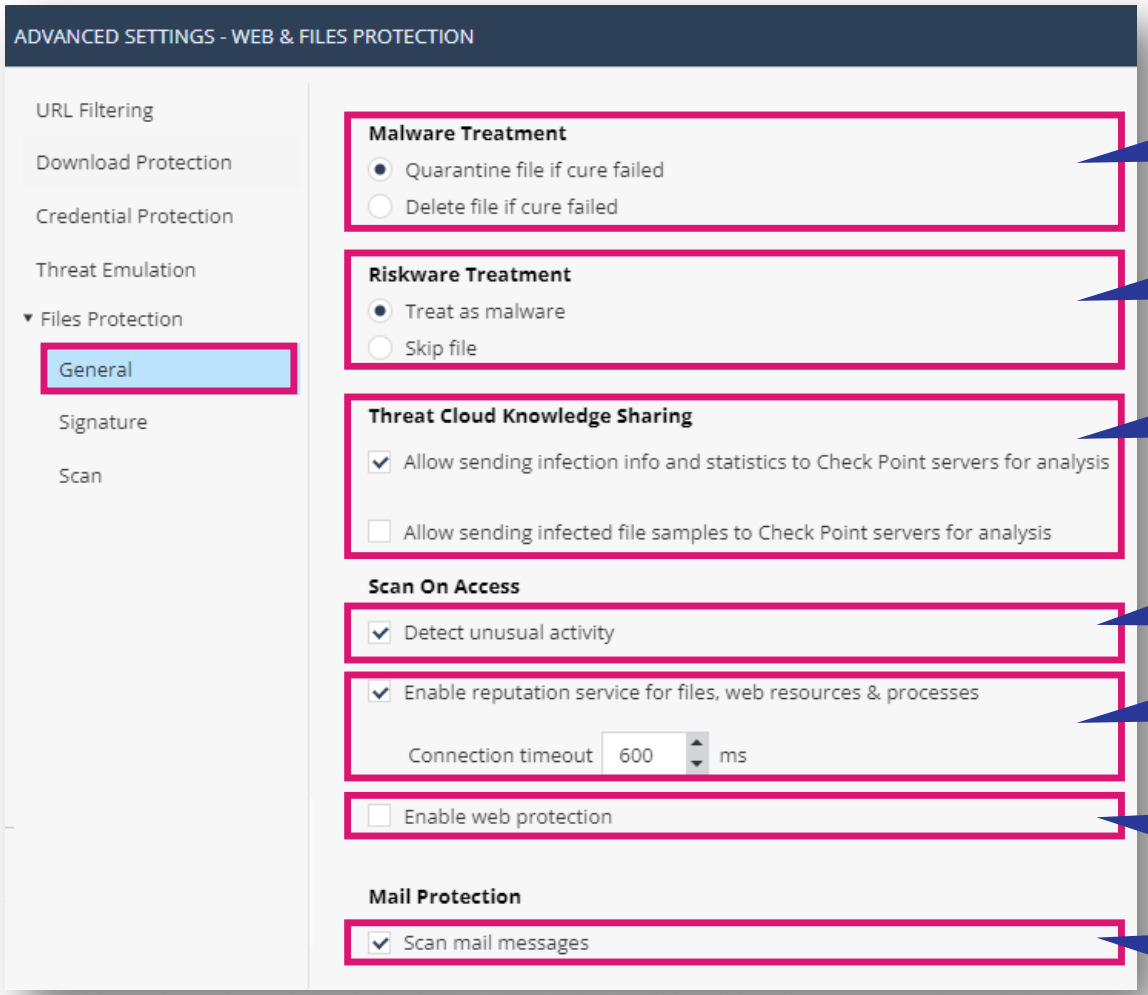
# Threat Prevention ファイル保護（１／４）

Policy > Threat Prevention > Web & Files Protection > Files Protection

- マルウェア対策は、ワームやトロイの木馬、アドウェア、キーロガーなどあらゆる種類のマルウェアからコンピュータを保護します
- Files Threat Emulation は、コンピュータにあるファイルのエミュレーションを行います

# Threat Prevention ファイル保護（２／４）

Policy > Threat Prevention > Web & Files Protection > Files Protection > Advance Settings




Anti-Malware で修復に失敗したファイルへの動作を選択

リスクウェア（危険な可能性のある合法的なソフトウェア）の取り扱い方法を選択

Threat Cloud への情報共有の可否を選択

異常な挙動の監視を有効化するかを選択。信頼できるプロセスは監視しない

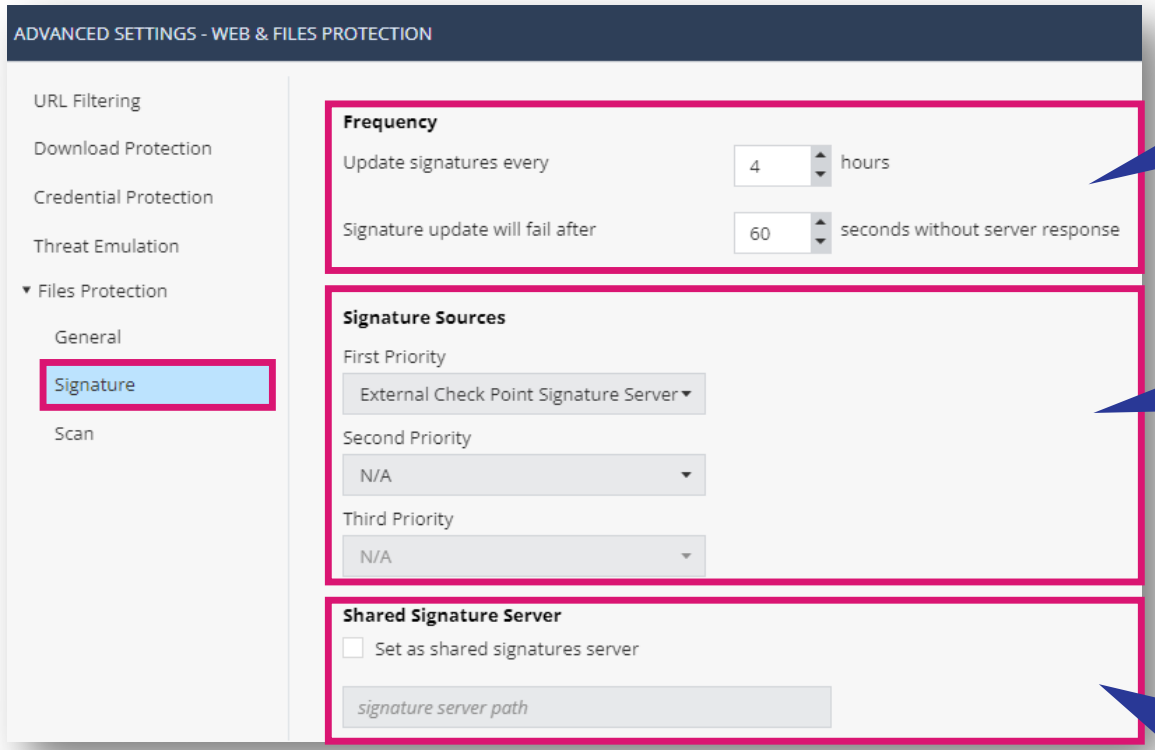
クラウドを使用したファイル、Web リソース、プロセスのレピュテーションの有効化を選択。PCの再起動後に有効

疑わしい Web サイトへのアクセスと悪意のあるスクリプトの実行防止を有効化するかを選択

電子メールがファイルとして保存される時に、電子メールの検査を有効化するかを選択

# Threat Prevention ファイル保護（３／４）

Policy > Threat Prevention > Web & Files Protection > Files Protection > Advance Settings



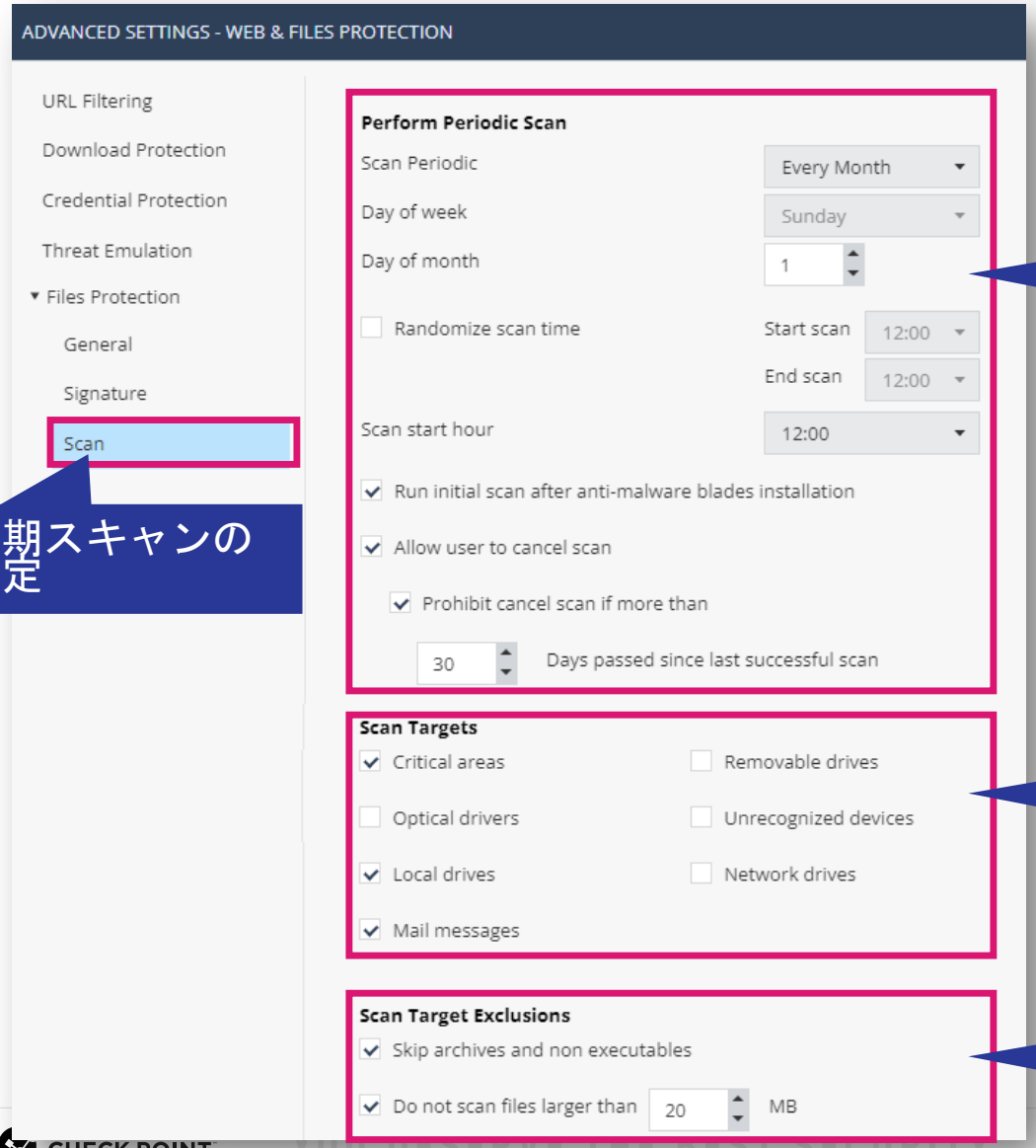

シグネチャの更新間隔とタイムアウト時間

シグネチャの配信元

VDI 環境の非永続的な仮想デスクトップ向けの共有フォルダからのシグネチャ取得設定

# Threat Prevention ファイル保護（４／４）

Policy > Threat Prevention > Web & Files Protection > Files Protection > Advance Settings




定期スキャンの設定

定期的なスキャン実行の設定

スキャン対象の選択（定期スキャンのみ）

スキャン対象の除外設定（定期スキャンのみ）

# 【演習】Anti-Malware

- 以下の Web ページからテストファイルをダウンロードして、Anti-Malware 等で検出することを確認してください

- https://www.eicar.org/download-anti-malware-testfile/

ポリシーの設定

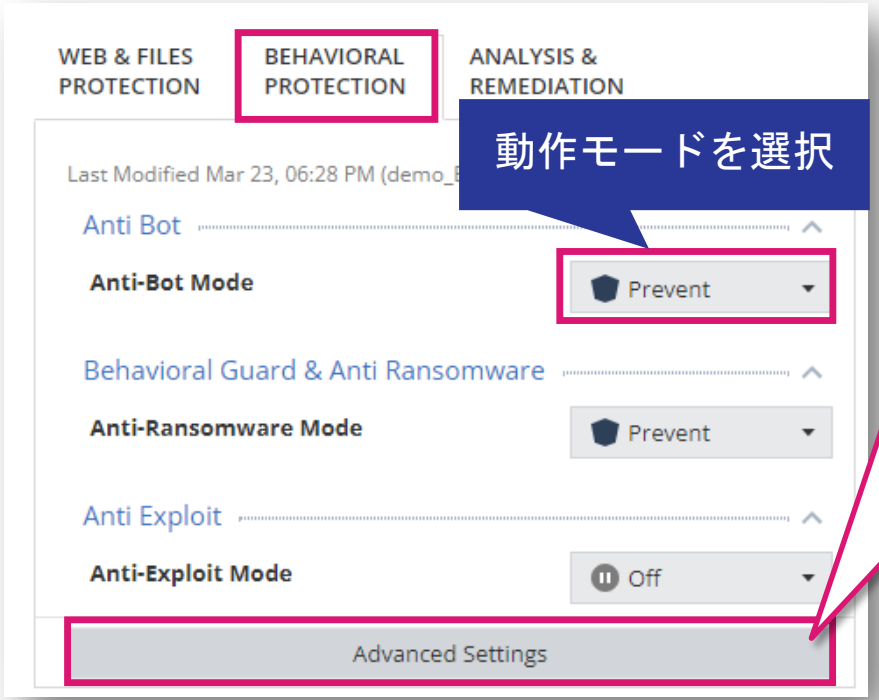
# THREAT PREVENTION
# ANTI-BOT

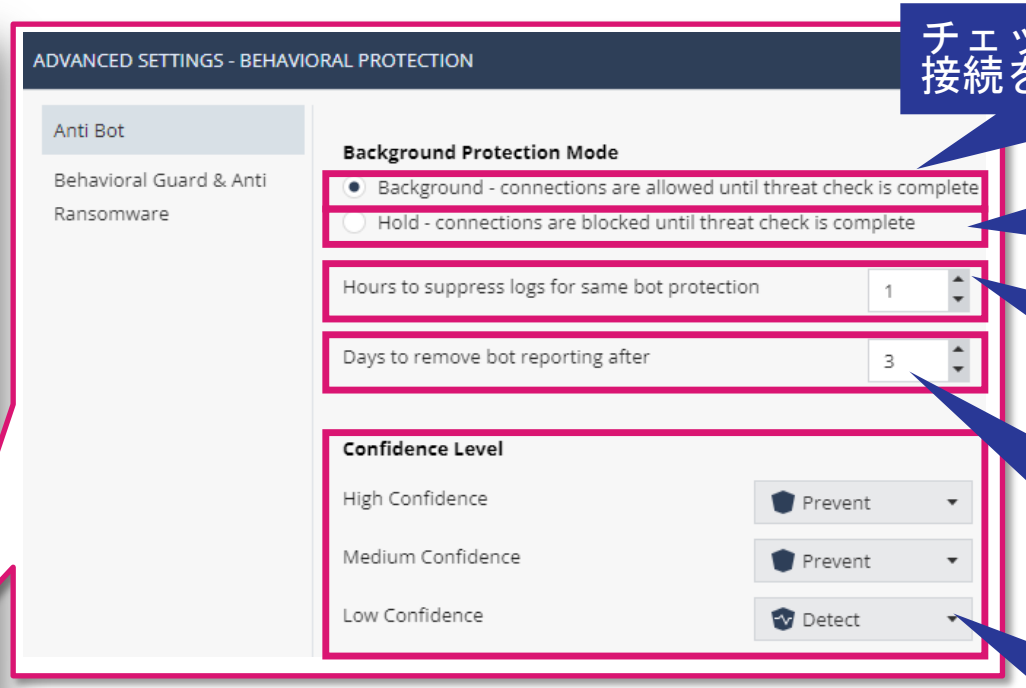
YOU DESERVE THE BEST SECURITY

# Threat Prevention：Anti-Bot

Policy > Threat Prevention > Behaivioral Protection> Anti Bot

- Anti-Botは、C&C サーバへのボット通信をブロックすることで被害を防ぎ、機密情報が盗まれたり組織から送信されたりしないようにします
- ThreatCloud には、ボットを検出するためのアドレスと、ボットネットの通信パターンが含まれています




※ デフォルトは、１時間。変更する場合は、時間数を選択

チェックが完了する前に、接続を許可（デフォルト）

チェックが完了するまで、接続をブロック

同じボットのアクションをログに記録する間隔※

選択した日数が経過してもボットがC&Cサーバに接続しない時、感染報告を停止

ボット検出の確実性（高／中／低）ごとのアクションを選択

ポリシーの設定

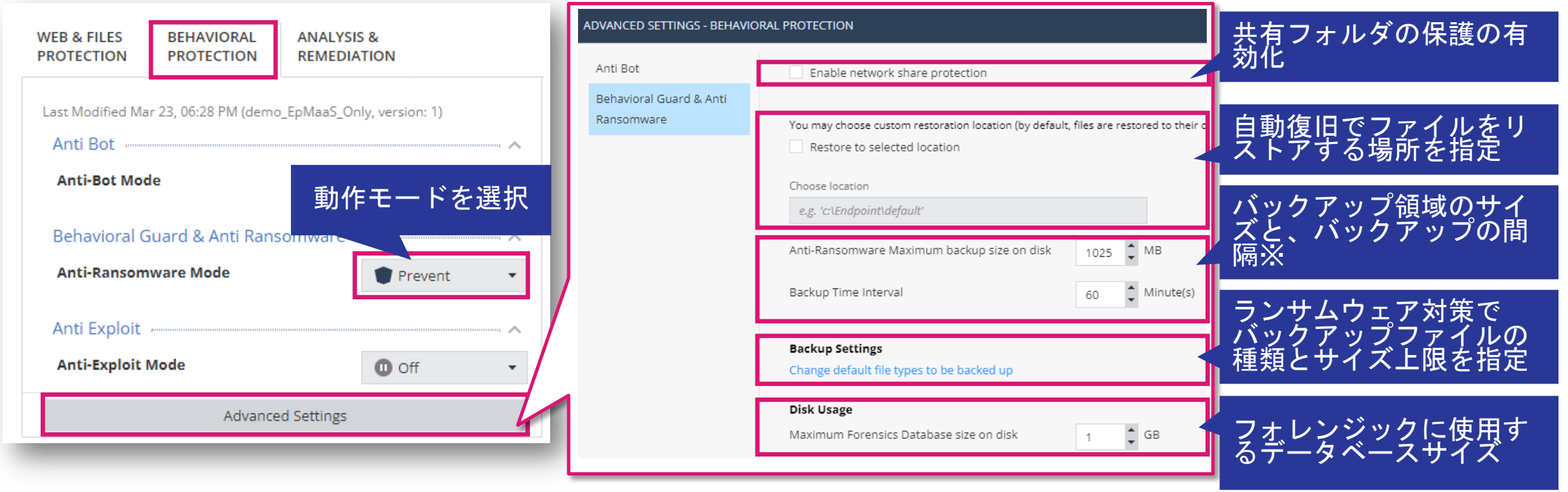
# THREAT PREVENTION
# BEHAVIORAL GUARD & ANTI-RANSOMWARE

YOU DESERVE THE BEST SECURITY

# Threat Prevention：Behavioral Guard & Anti Ransomware

Policy > Threat Prevention > Behaivioral Protection > Behabioral Guard & Anti Ransomware

- 疑わしい動作がないか、ファイルとネットワークアクティビティを常に監視します。
- パソコンにハニーポットファイルを作成し、ファイルの変更を検出するとすぐに攻撃を停止します。




**※ バックアップを取得してから、バックアップ間隔で設定した時間が経過するまでは、バックアップを再取得しません。**

# 【参考】Anti-Ransomware のバックアップ対象ファイル拡張子（デフォルト）

- 3gp
- aif
- aiff
- asf
- avi
- bmp
- bpg
- csv
- dib
- dibl
- doc
- docb
- docm
- docx
- dot
- dotm
- dotx
- emf
- eps
- flv
- gam
- gif
- hdr
- heif
- htm
- html
- jfif
- jpegl
- jpg
- m4a
- m4v
- mov
- mp3
- mp4
- mpa
- mpeg
- mpg
- pbm
- pdf
- pgm
- png
- pnm
- pot
- potx
- ppm
- pps
- ppsx
- ppt
- pptm
- pptx
- prn
- ps
- rle
- rtf
- sldx
- swf
- tif
- tiff
- txt
- wav
- webp
- wma
- wmv
- wpd
- xlm
- xls
- xlsb
- xlsm
- xlsx
- xlt
- xltm
- xltx

**※ バックアップ対象ファイルのサイズ上限の初期値は、25MBです**

# 【参考】Anti-Ransomware の動作概要

ポリシーの設定

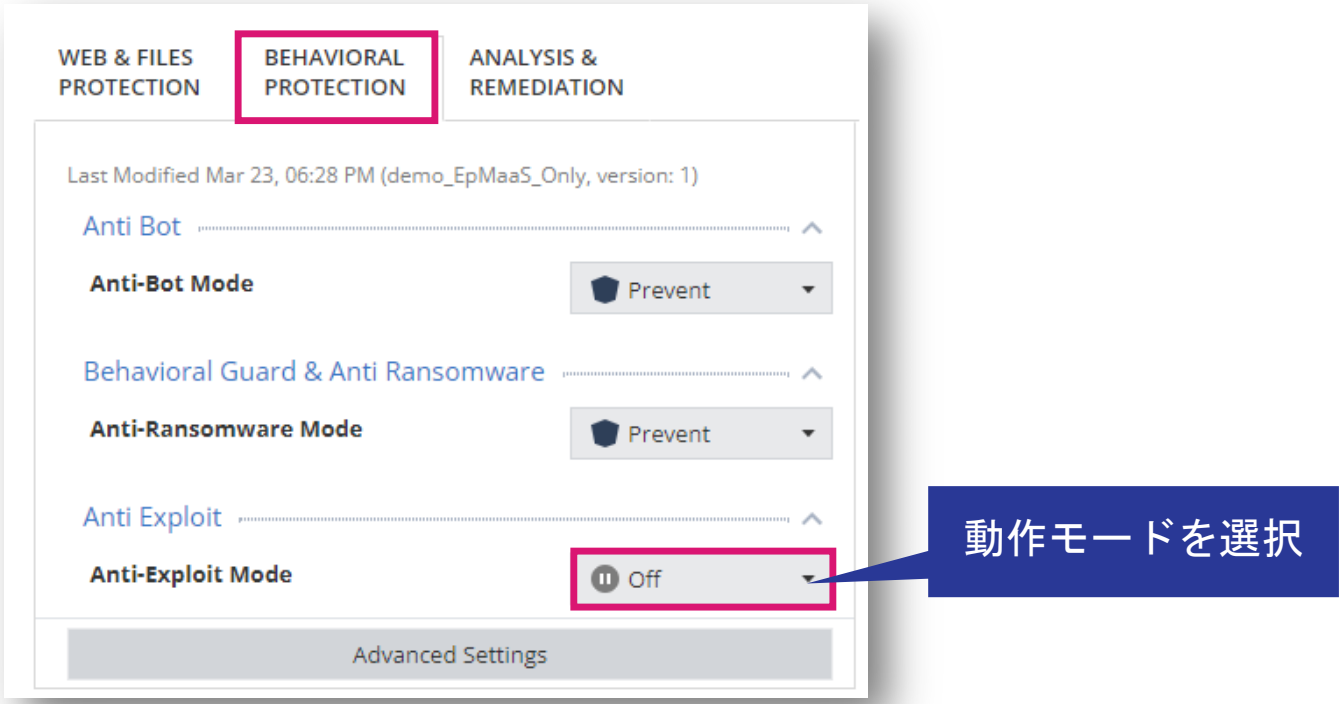
# THREAT PREVENTION
# ANTI-EXPLOIT

YOU DESERVE THE BEST SECURITY

# Threat Prevention：Anti Exploit

Policy > Threat Prevention > Behaivioral Protection > Anti Exploit

- Anti-Exploit は、ブラウザや Office のエクスプロイトベースの攻撃に対する保護を提供します。
- Anti-Exploit は悪意のあるペイロードのダウンロードまたは実行を防ぎます。
- Anti-Exploit は、検出時に悪用されているプロセスをシャットダウンし、フォレンジックレポートを生成します。



ポリシーの設定

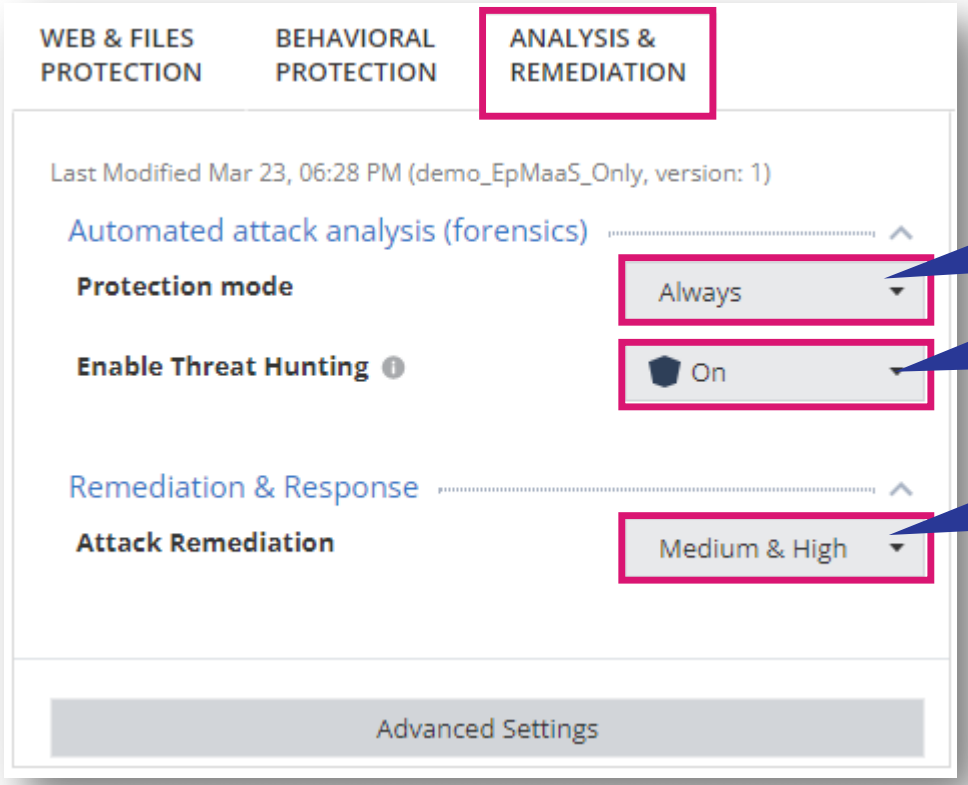
# THREAT PREVENTION FORENSICS & REMEDIATION

YOU DESERVE THE BEST SECURITY

# Threat Prevention：Analysis & Remediation（1／2）

Policy > Threat Prevention > Analysis & Remediation

- Anti-RansomwareやBehavioral Guardなどによって悪意のあるイベントまたはファイルが検出されると、フォレンジック分析が自動的に開始されます
- File Remediationは、悪意のあるファイルを検出すると、ポリシーに基づいてそれらのファイルを自動的に隔離し、必要に応じて修正します




インシデントを分析するコンフィデンスレベル

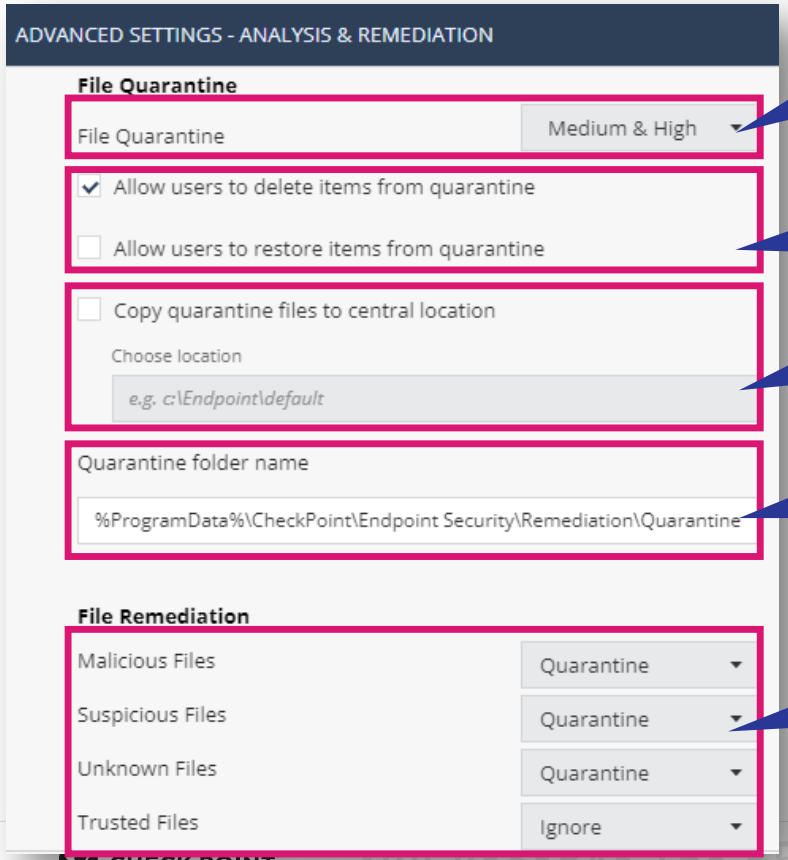
Threat Huntingの有効／無効を選択

修復を実行するコンフィデンスレベル

# Threat Prevention：Analysis & Remediation（2／2）

Policy > Threat Prevention > Analysis & Remediation

- File Quarantine（ファイル隔離）では、隔離されるファイルの設定を定義します。
- デフォルトでは、アイテムは 90 日間隔離され、ユーザーは隔離からアイテムを削除できます。
- File Remediation（ファイル修復）では、フォレンジックによって検出された攻撃に関連するファイルの処理をカテゴリごとに定義します。




ファイルを隔離する際のコンフィデンスレベルを選択

隔離されたファイルの削除、復元をユーザに許可するか選択

隔離されたファイルのコピーの保存場所を指定

隔離フォルダの場所を指定

ファイルのカテゴリごとに動作を指定

# 除外設定

YOU DESERVE THE BEST SECURITY

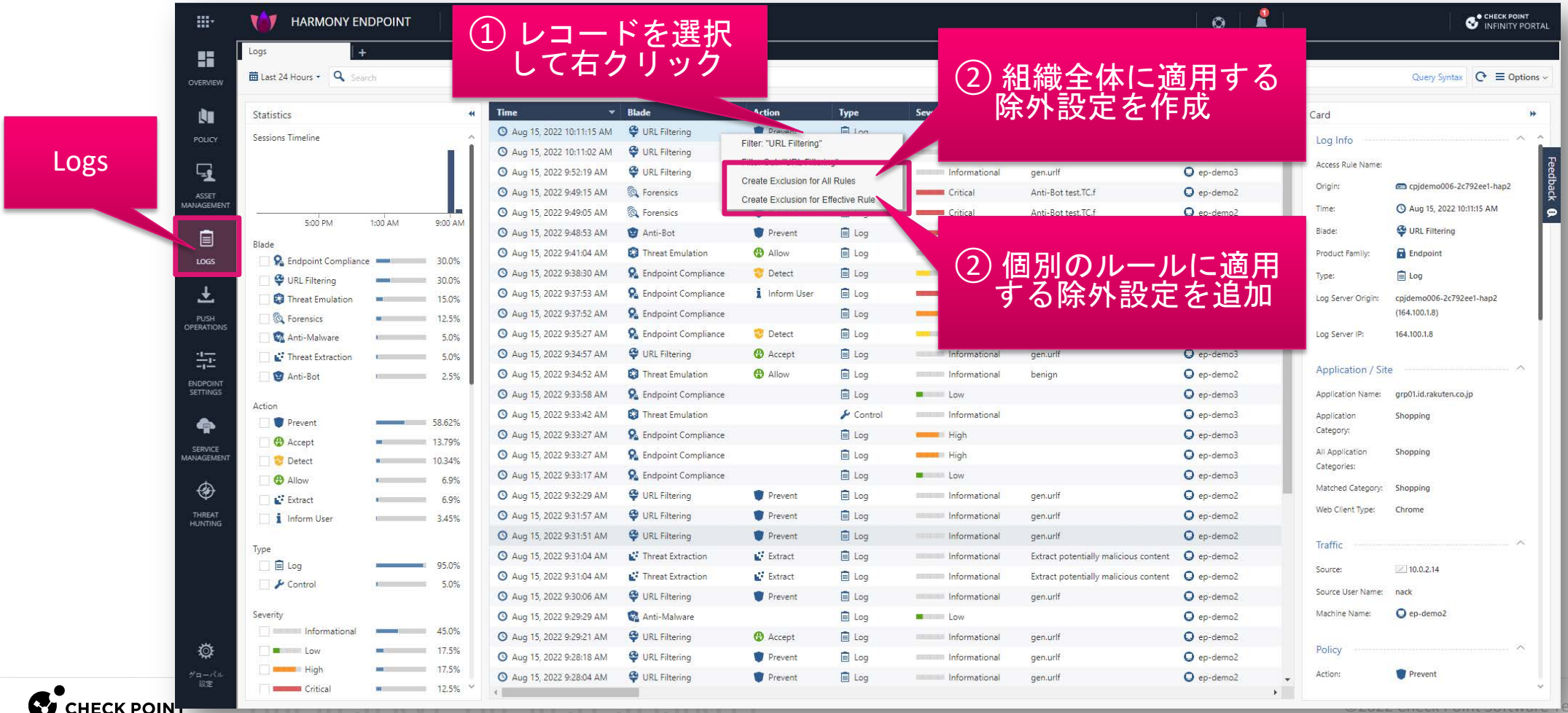
# 除外設定の概要

- Harmony Endpointによる検査から特定のオブジェクトを除外できます
- 除外設定は、[ログ] のレコードから右クリックで作成するか、除外設定追加メニューで作成します
- 組織全体に適用することも、個別ルールに適用することもできます

| 機能 | 除外指定方法 | | | | | |
|---|---|---|---|---|---|---|
| **URL フィルタ** | Domain/URL | | | | | |
| **Anti-Malware** | Infection by name | Process Path | File Path | Folder Path | | |
| **Threat Emulation** | Domain | SHA-1 Hash | Folder Path | | | |
| **Threat Extraction** | Domain | SHA-1 Hash | | | | |
| **Zero Phishing** | Domain | | | | | |
| **Anti-Ransomware** | Folder Path | Certificate | Protection Name | Process Path | | |
| **Behavioral Guard** | Folder Path | Certificate | Protection Name | Process Path | | |
| **Anti-Bot** | Domain | URL | Protection Name | Process | IP Range | |
| **Anti-Exploit** | Process Path | Protection Name | | | | |
| **Forensics - Quarantine** | Certificate | File Path | Folder Path | MD5 Hash | SHA-1 Hash | File Extension |
| **Forensics - Monitoring** | Process Path | Certificate | | | | |

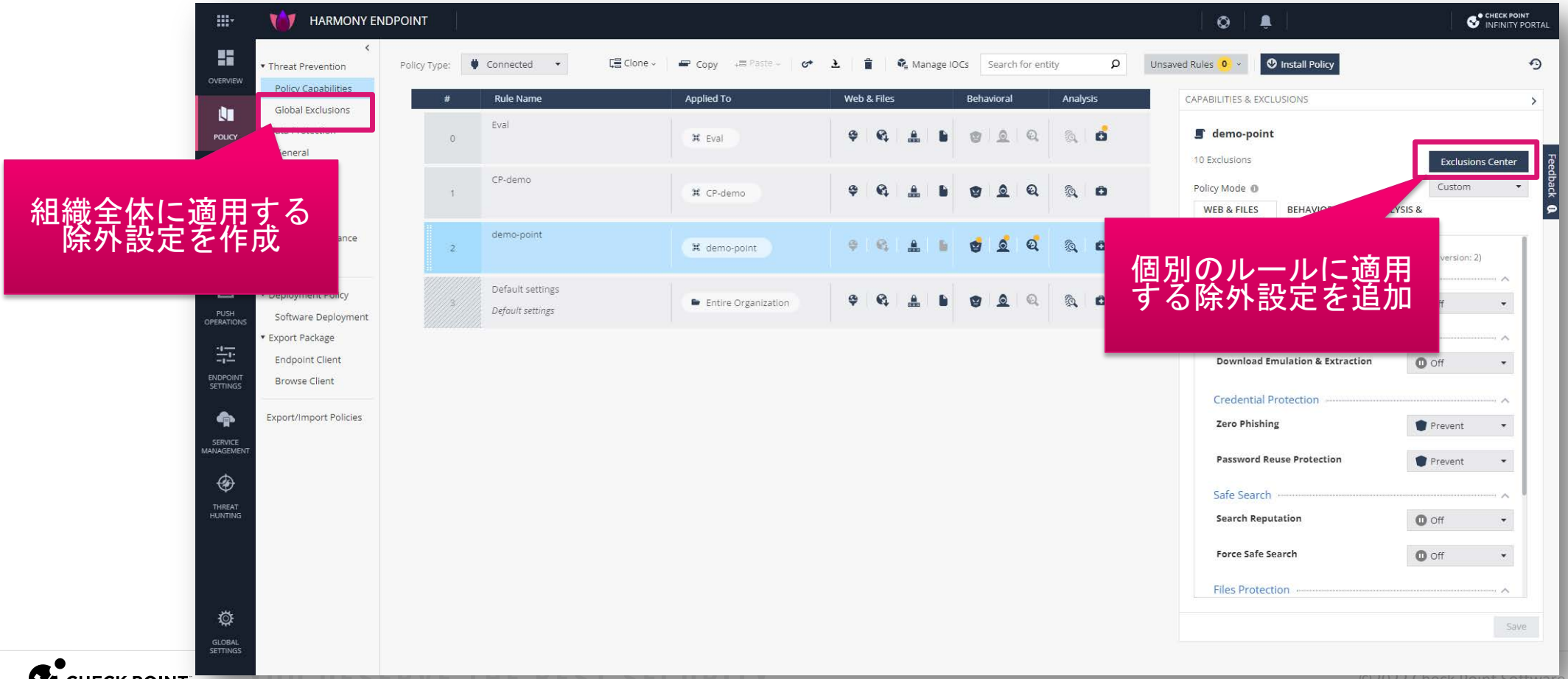
# 除外設定の方法：ログから作成

- Logs で表示されるログのレコードを右クリックする
- 織全体に適用する場合は、「Create Exclusion for All Rules」 を選択する
- 個別のルールに適用する場合は、「Create Exclusion for Effective Rule」を選択する

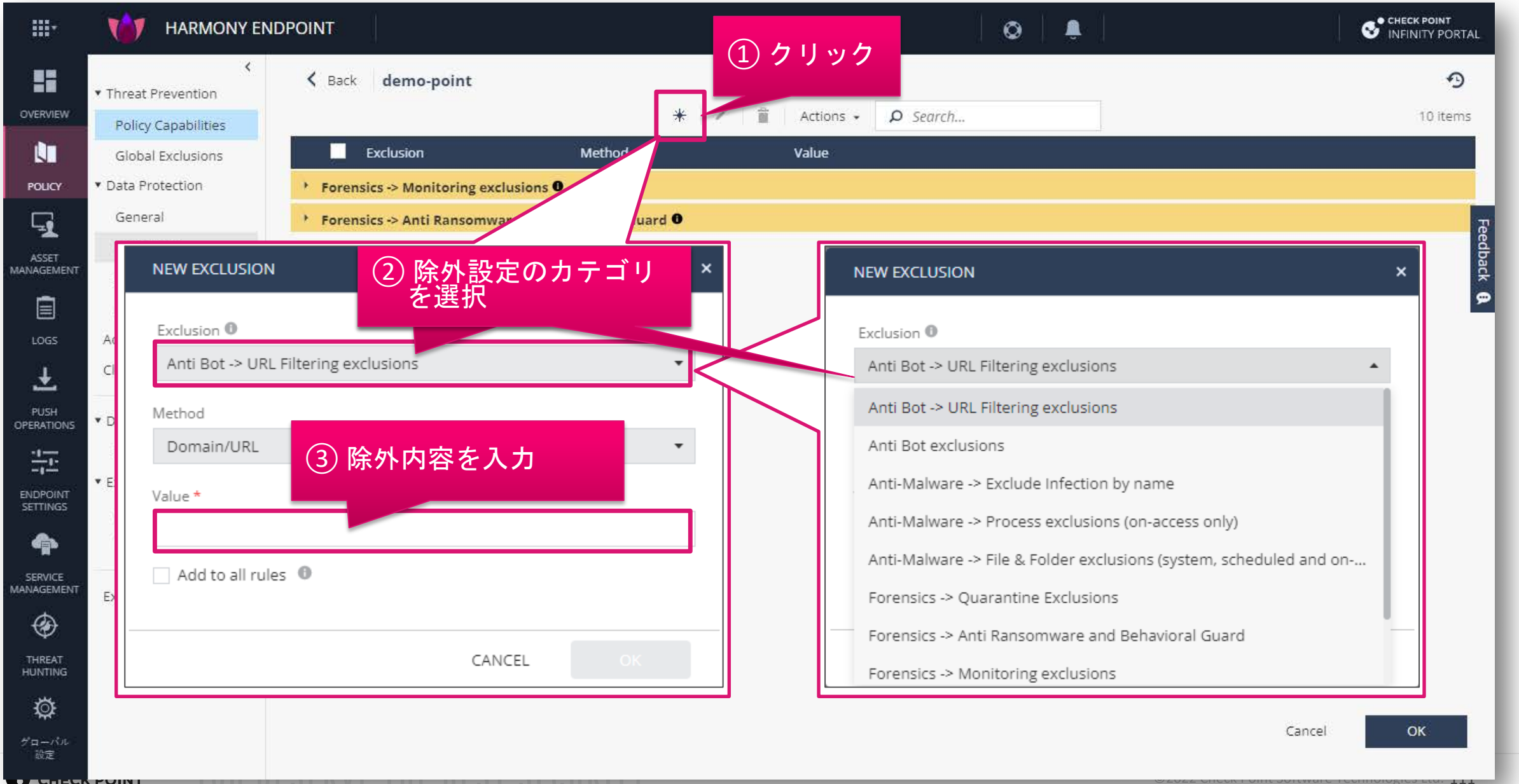


# 除外設定の方法：編集メニューから作成（1／2）

- Policy > Threat Prevention > Global Exclusions で、組織全体に適用する除外設定を追加
- Policy > Threat Prevention > Policy Capabilityes > Capabilities & Exclusions > Edit Exclusions で、ルールごとの除外設定を追加
- 除外設定を追加後は、Save と Install を実施する



# 除外設定の方法：編集メニューから作成（２／２）



# 【演習】除外設定

- Anti-Malware の除外設定で、テストファイル（eicar）を除外するルールを作成し、検出されなくなることを確認してください。

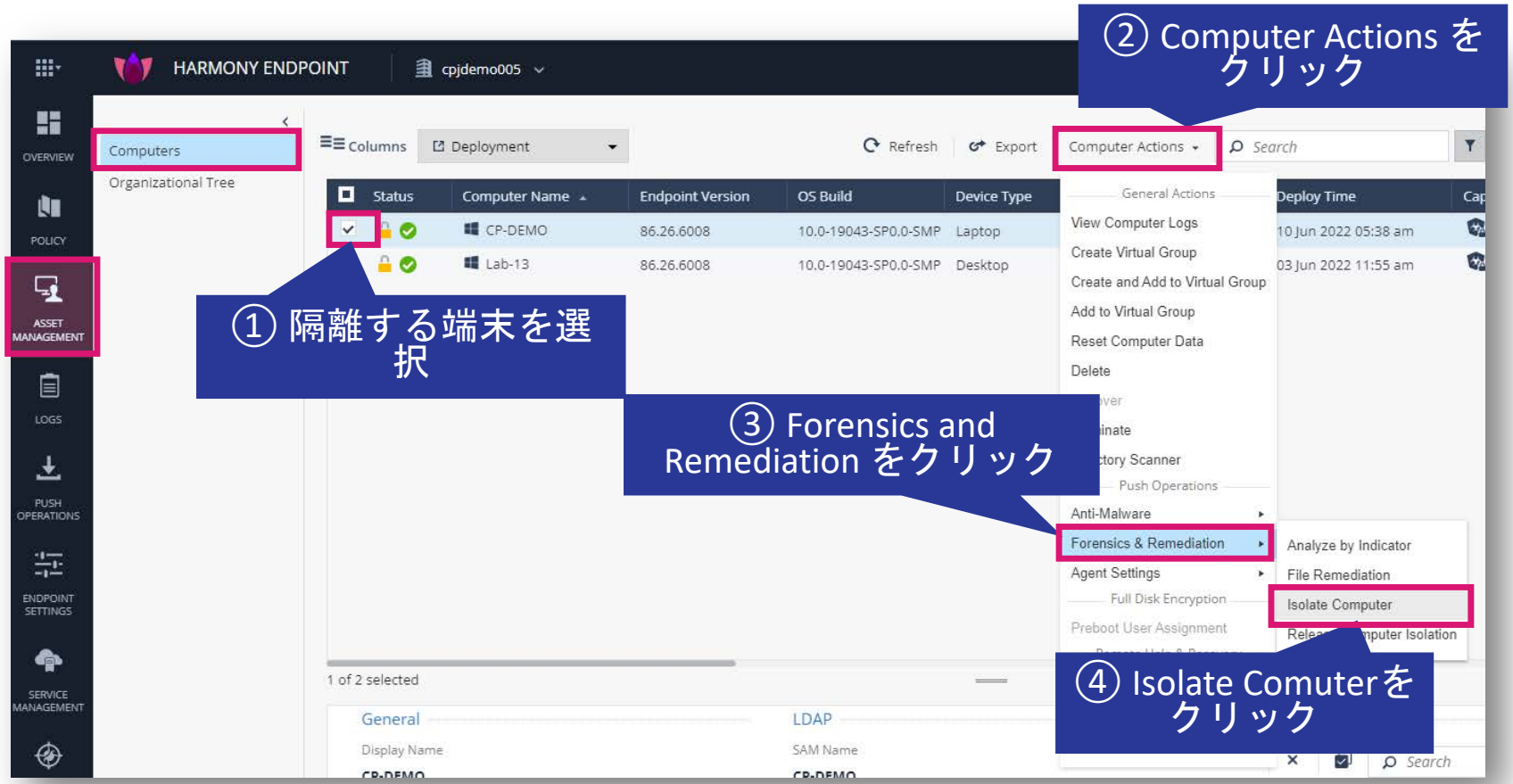
# コンピュータの隔離、解放

YOU DESERVE THE BEST SECURITY

# 隔離方法その１：Asset Magement 画面からの端末の隔離、解放

Asset Management > Computers > Computer Actions > Forensics & Remediation > Isolate Computer

- リモートから端末の隔離、解放を実行できます。
- 端末の隔離をするためには、Firewall Bladeが必要です。



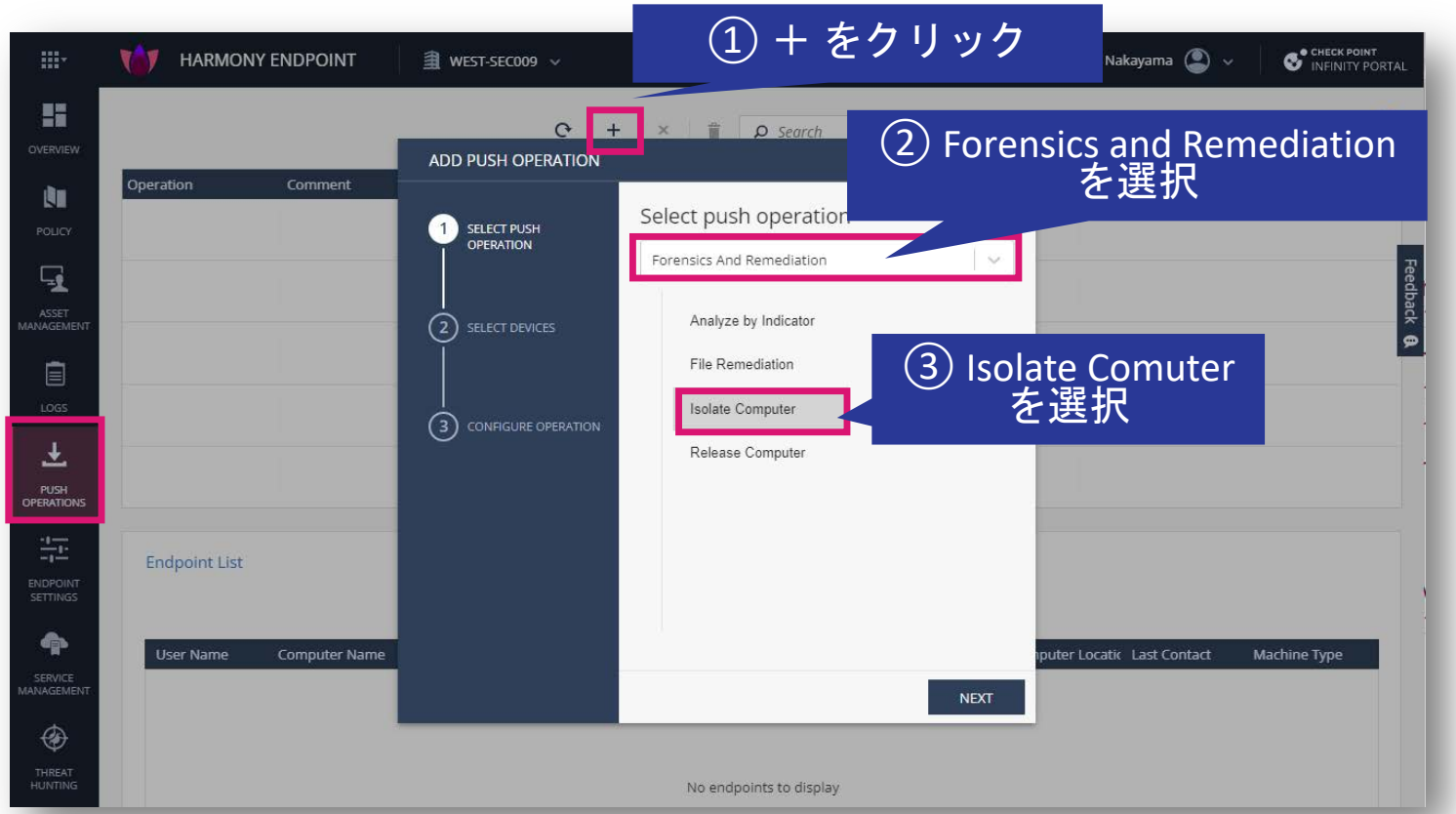


※ 端末を解放する際は、Computer Actions > Forensics & Remediations > Release Computer Isolation を選択してください。

# 隔離方法その２：Push Operations 画面からの端末の隔離、解放

Push Operations

- リモートから端末の隔離を実行できます。
- 端末の隔離をするためには、Firewall Bladeが必要です。



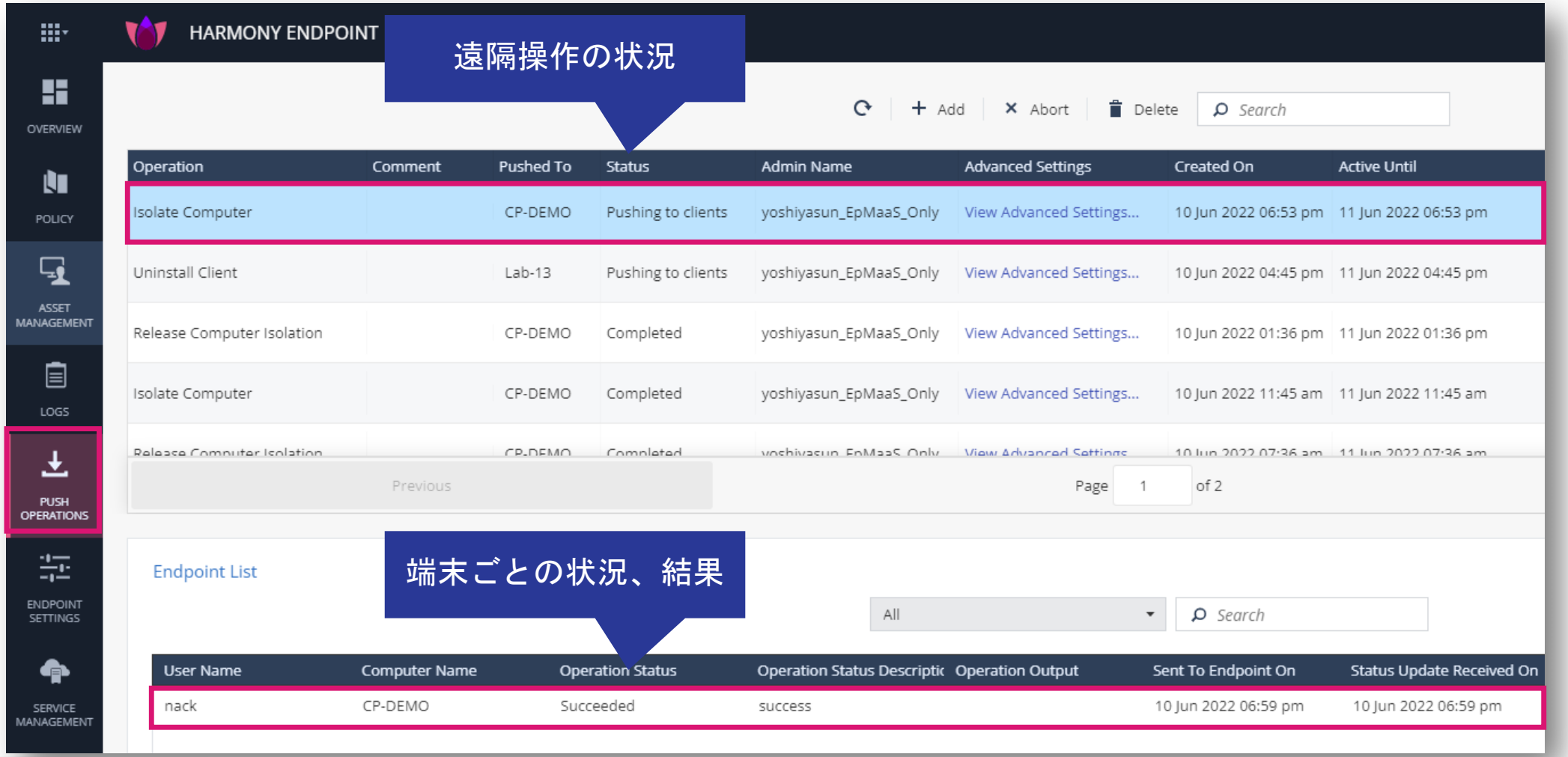


※ 端末を解放する際は、Forensics & Remediations > Release Computer を選択してください

# 遠隔操作の状況確認

## Push Operations

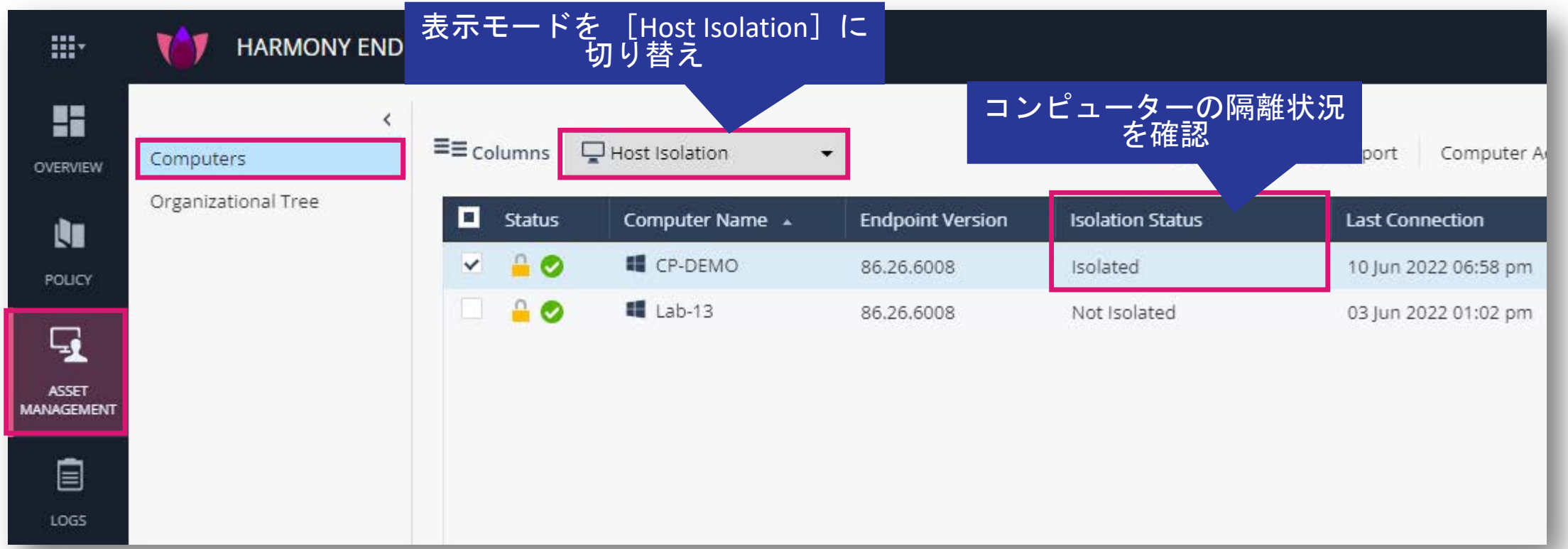
- Push Operations で遠隔操作の状況を確認



# Asset Management 画面での端末の状況確認

Asset Management > Computers

- Host Isolation 表示に切り替えることで、端末の隔離状況を表示可能



# 【演習】コンピュータの隔離、開放

- コマンドプロンプトを起動して以下のコマンドを実行してください
  - ping –t 8.8.8.8

- コンピュータの隔離と解放を行い、ping の応答の変化を確認してください

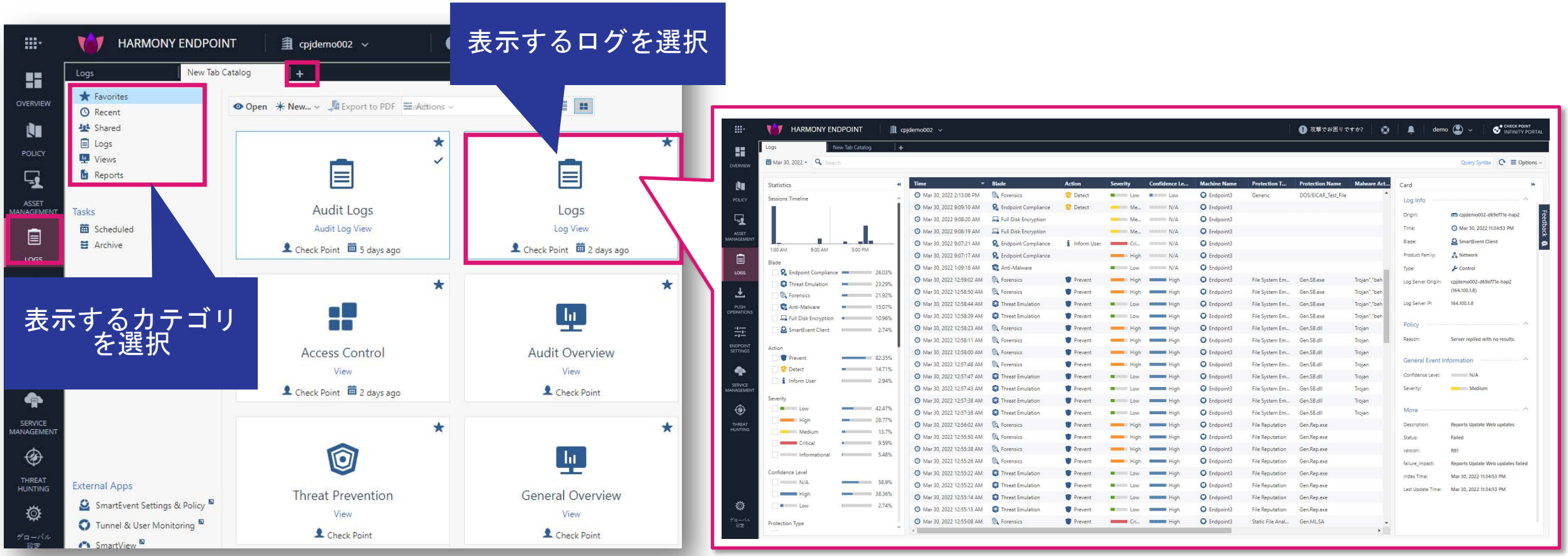
# ログの表示

YOU DESERVE THE BEST SECURITY

# ログの表示（1／2）

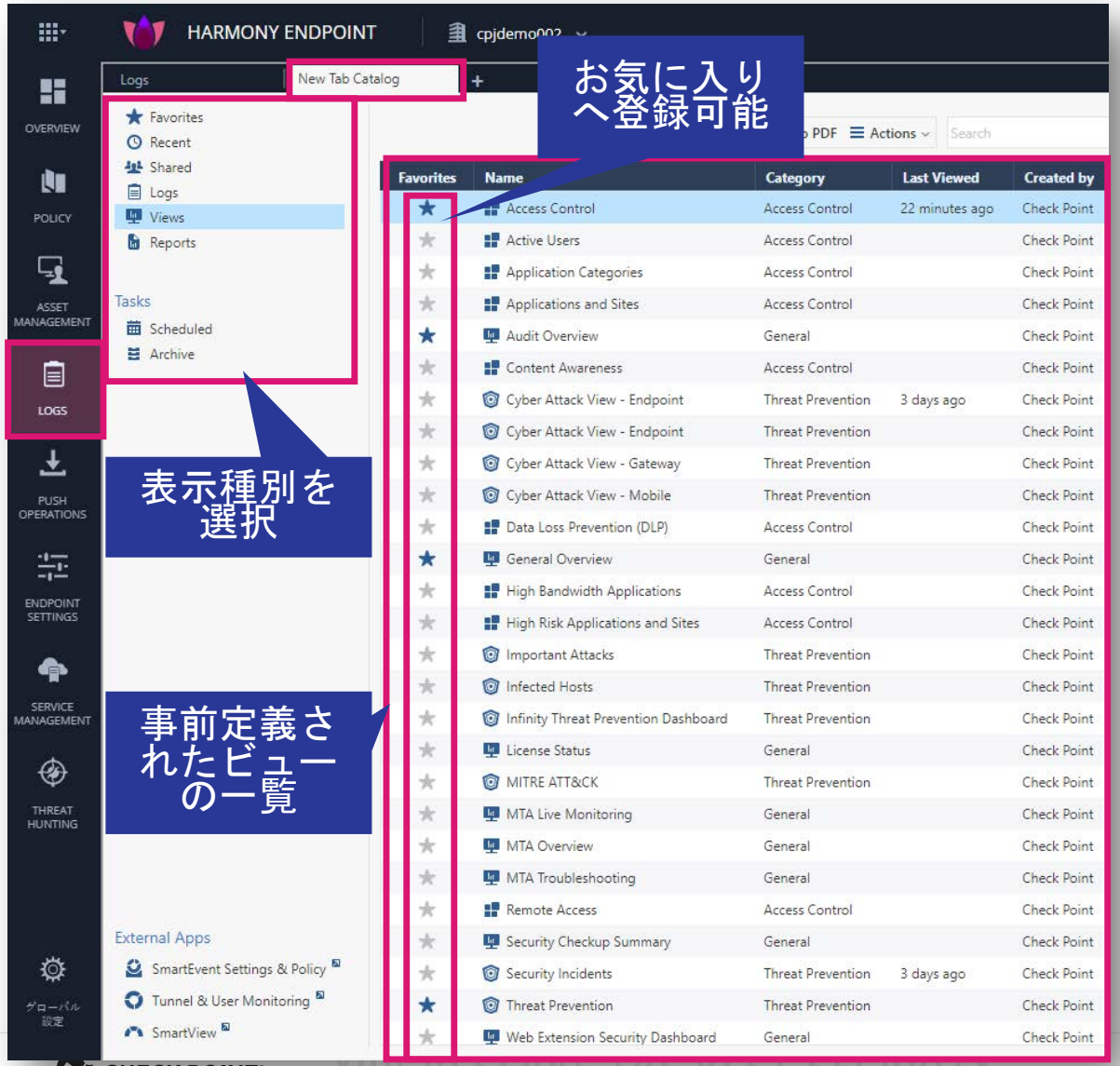
Logs > New Tab Catalog > Favorites（もしくは、Logs） > Logs

- New Tab Catalog から表示したいログ、ビュー、レポートを選択します
- デフォルトでは、Logs が表示されます（その他のログ等を見たい場合は、＋を押して New Tab Catalogを表示させます）

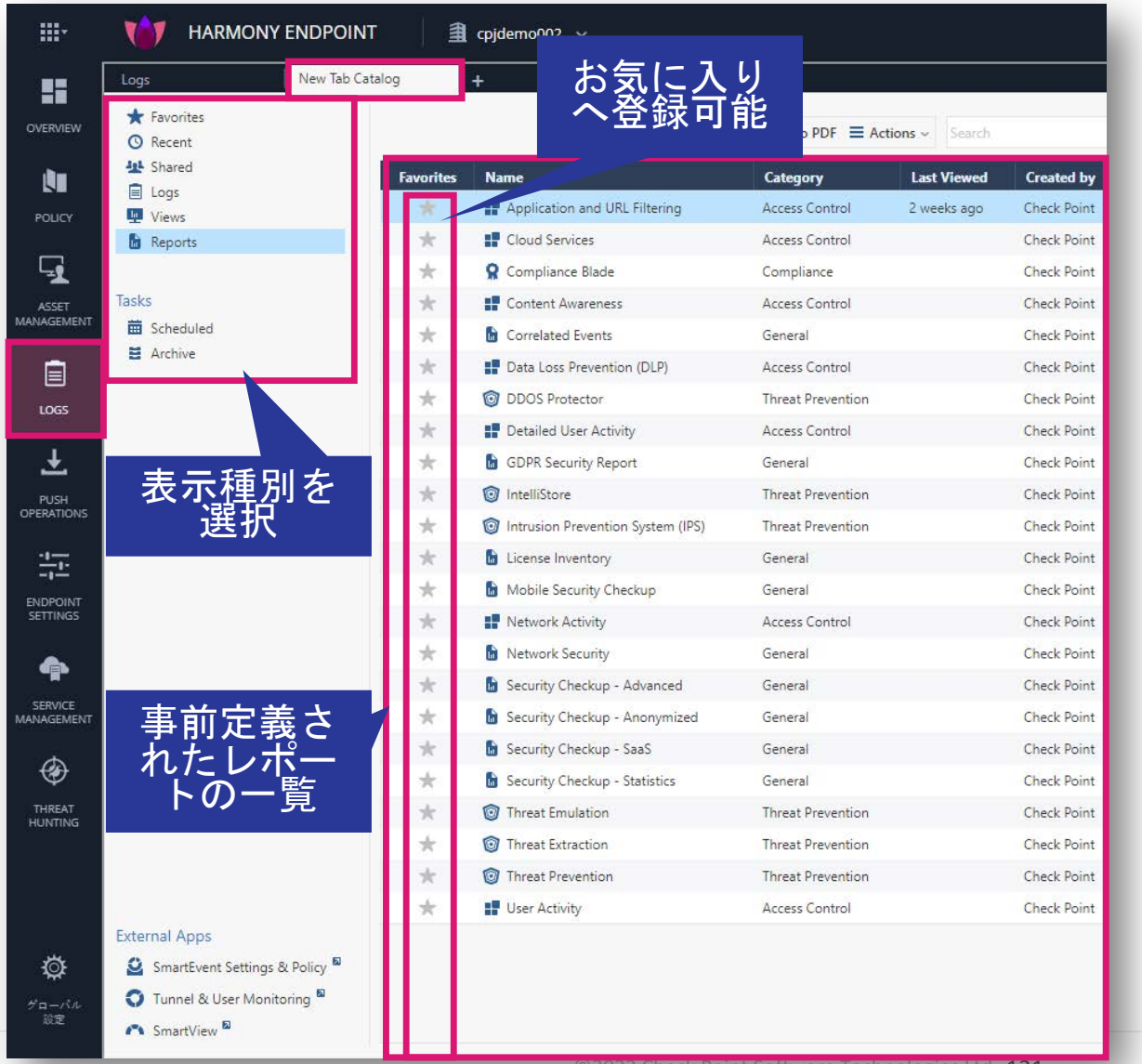


# ログの表示（2／2）

## 事前定義されたビューの一覧



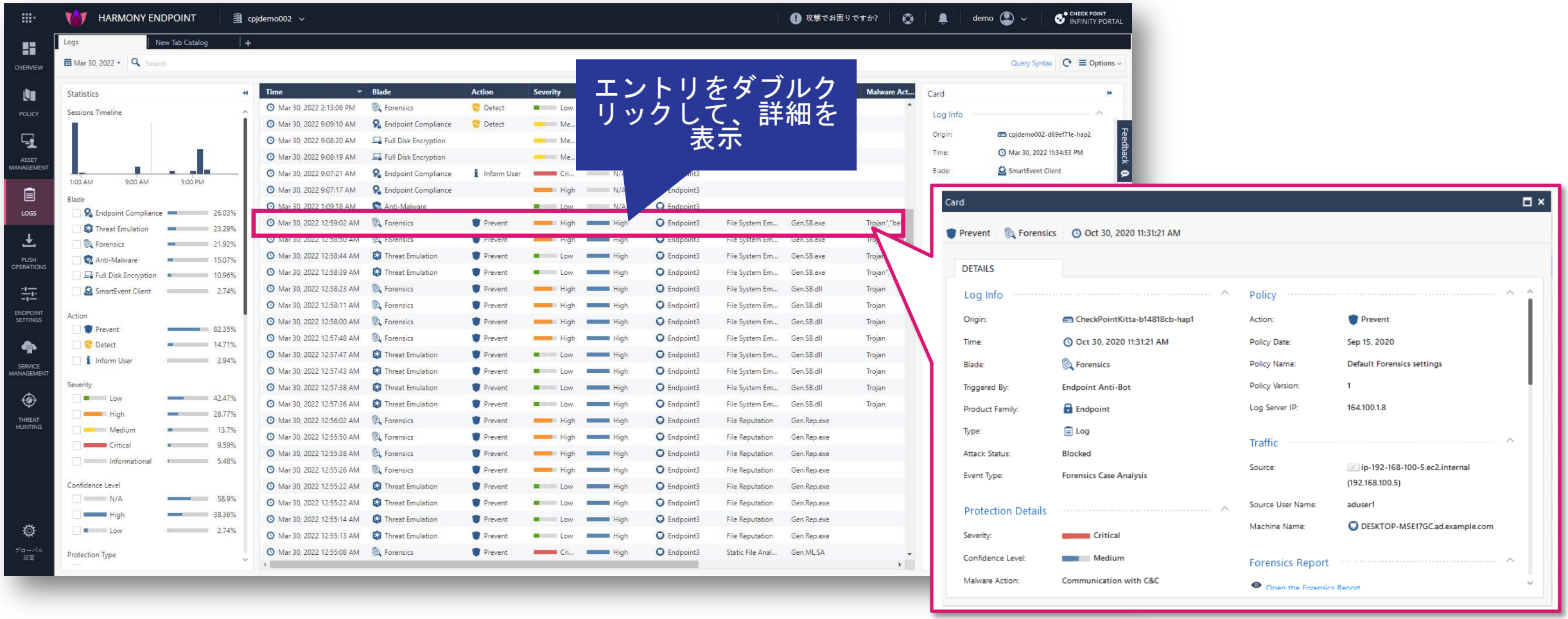

## 事前定義されたレポートの一覧



# ログの表示：一覧表示・詳細表示（１／２）

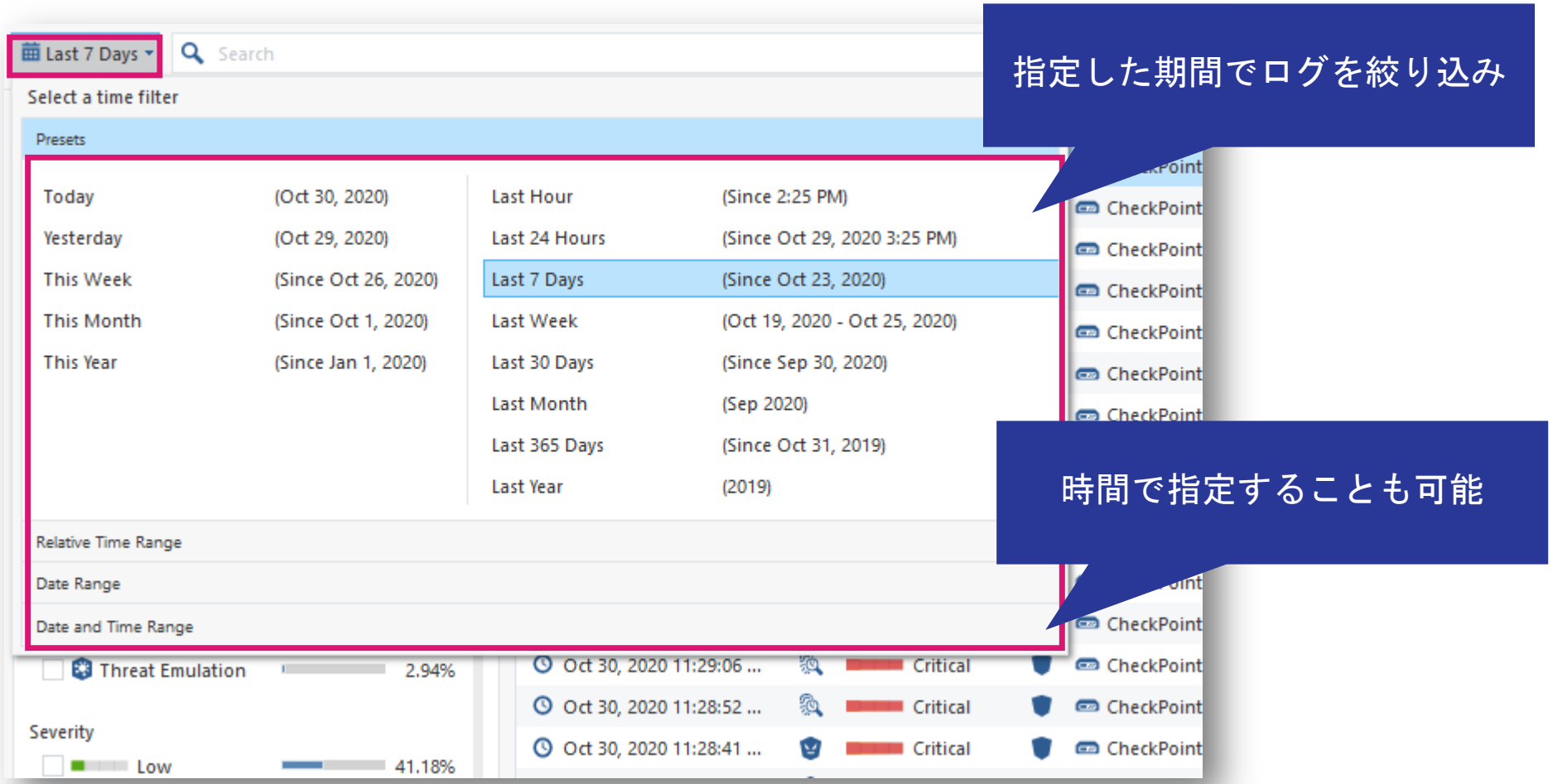
# ログの表示：一覧表示・詳細表示（２／２）

- 一覧表示されたログの詳細を表示できます



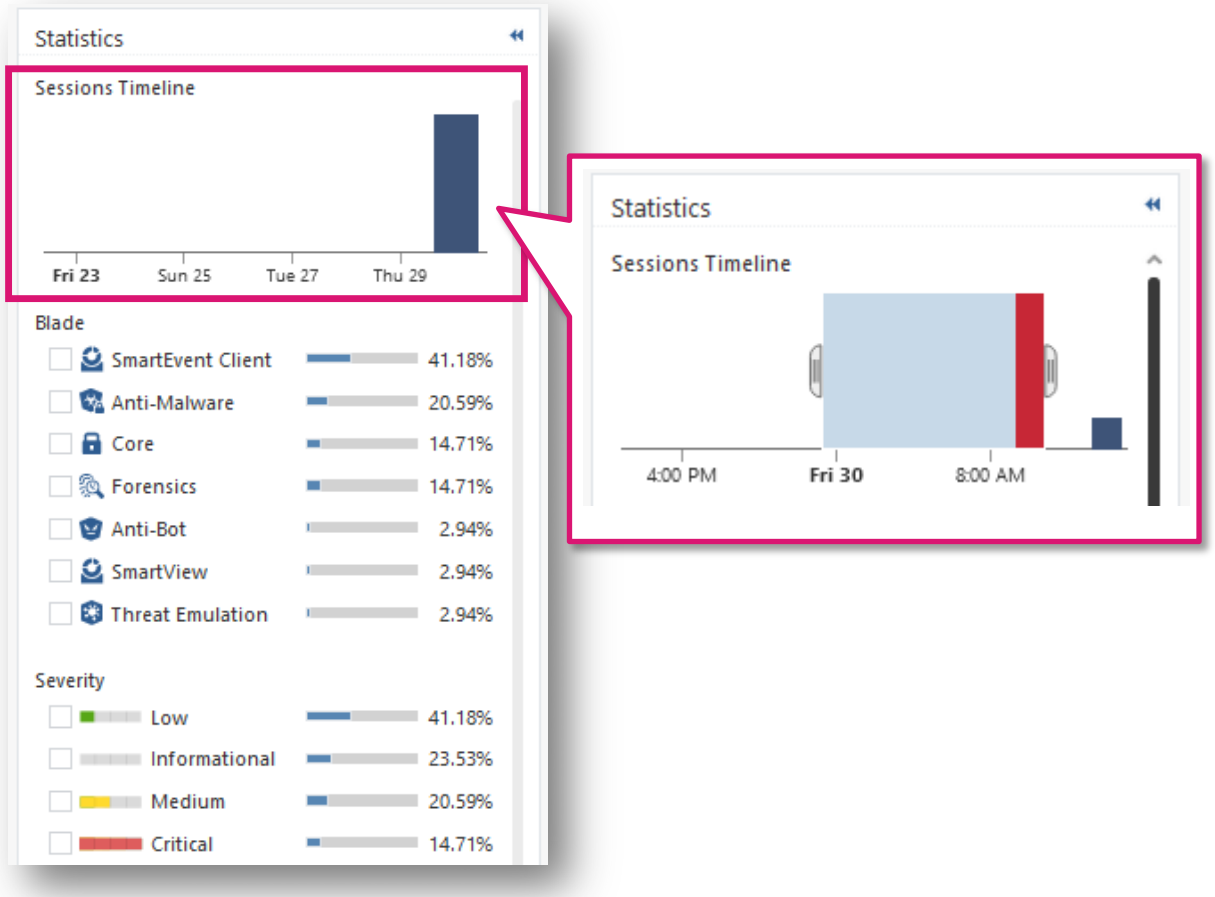
# ログの表示：期間指定

- 指定した期間でログを絞り込むことができます



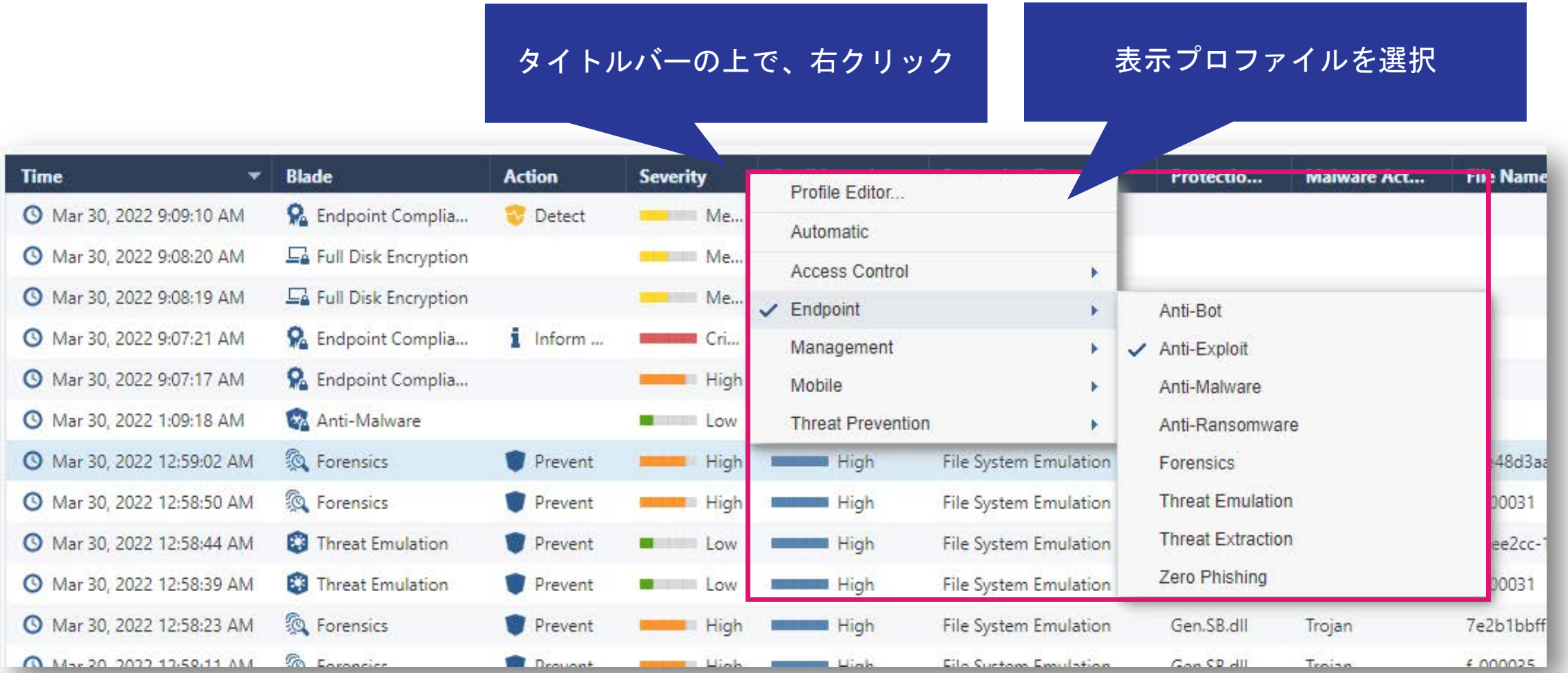
# ログの表示： Statistics パネル

- 簡単な統計情報が表示されます
- チェックボックスをクリックすると、それぞれの項目で簡単にフィルタをかけることができます
- タイムライン上で表示期間を選択することも可能です



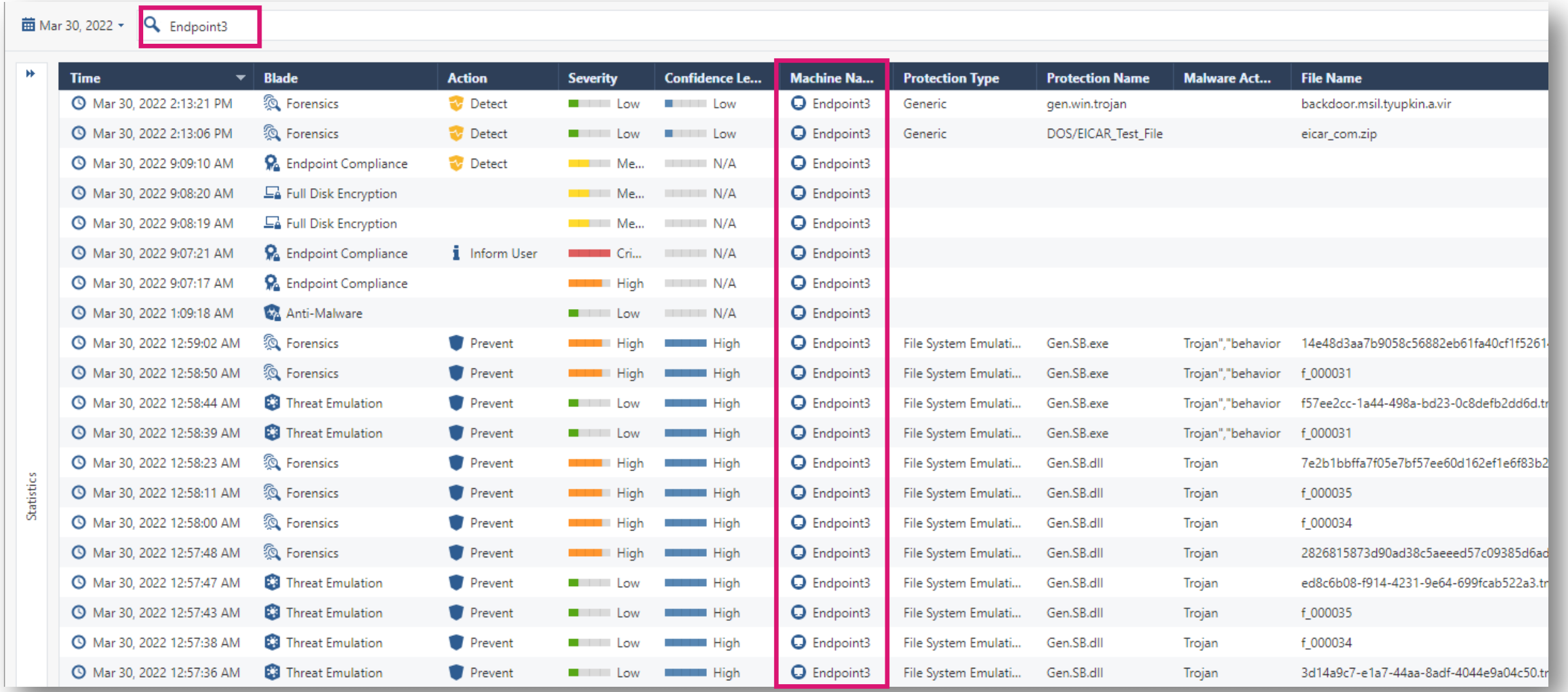
# ログの表示：カラム指定

- ログのカラム表示を変更できます



# ログの表示：キーワードでの検索

- キーワードを入力して、ユーザ名やコンピュータ名などでログを絞り込むことができます




| Time | Blade | Action | Severity | Confidence Le... | Machine Na... | Protection Type | Protection Name | Malware Act... | File Name |
|---|---|---|---|---|---|---|---|---|---|
| Mar 30, 2022 2:13:21 PM | Forensics | Detect | Low | Low | Endpoint3 | Generic | gen.win.trojan | | backdoor.msil.tyupkin.a.vir |
| Mar 30, 2022 2:13:06 PM | Forensics | Detect | Low | Low | Endpoint3 | Generic | DOS/EICAR_Test_File | | eicar_com.zip |
| Mar 30, 2022 9:09:10 AM | Endpoint Compliance | Detect | Me... | N/A | Endpoint3 | | | | |
| Mar 30, 2022 9:08:20 AM | Full Disk Encryption | | Me... | N/A | Endpoint3 | | | | |
| Mar 30, 2022 9:08:19 AM | Full Disk Encryption | | Me... | N/A | Endpoint3 | | | | |
| Mar 30, 2022 9:07:21 AM | Endpoint Compliance | Inform User | Cri... | N/A | Endpoint3 | | | | |
| Mar 30, 2022 9:07:17 AM | Endpoint Compliance | | High | N/A | Endpoint3 | | | | |
| Mar 30, 2022 1:09:18 AM | Anti-Malware | | Low | N/A | Endpoint3 | | | | |
| Mar 30, 2022 12:59:02 AM | Forensics | Prevent | High | High | Endpoint3 | File System Emulati... | Gen.SB.exe | Trojan","behavior | 14e48d3aa7b9058c56882eb61fa40cf1f5261 |
| Mar 30, 2022 12:58:50 AM | Forensics | Prevent | High | High | Endpoint3 | File System Emulati... | Gen.SB.exe | Trojan","behavior | f_000031 |
| Mar 30, 2022 12:58:44 AM | Threat Emulation | Prevent | Low | High | Endpoint3 | File System Emulati... | Gen.SB.exe | Trojan","behavior | f57ee2cc-1a44-498a-bd23-0c8defb2dd6d.tr |
| Mar 30, 2022 12:58:39 AM | Threat Emulation | Prevent | Low | High | Endpoint3 | File System Emulati... | Gen.SB.exe | Trojan","behavior | f_000031 |
| Mar 30, 2022 12:58:23 AM | Forensics | Prevent | High | High | Endpoint3 | File System Emulati... | Gen.SB.dll | Trojan | 7e2b1bbffa7f05e7bf57ee60d162ef1e6f83b2 |
| Mar 30, 2022 12:58:11 AM | Forensics | Prevent | High | High | Endpoint3 | File System Emulati... | Gen.SB.dll | Trojan | f_000035 |
| Mar 30, 2022 12:58:00 AM | Forensics | Prevent | High | High | Endpoint3 | File System Emulati... | Gen.SB.dll | Trojan | f_000034 |
| Mar 30, 2022 12:57:48 AM | Forensics | Prevent | High | High | Endpoint3 | File System Emulati... | Gen.SB.dll | Trojan | 2826815873d90ad38c5aeeed57c09385d6ac |
| Mar 30, 2022 12:57:47 AM | Threat Emulation | Prevent | Low | High | Endpoint3 | File System Emulati... | Gen.SB.dll | Trojan | ed8c6b08-f914-4231-9e64-699fcab522a3.tr |
| Mar 30, 2022 12:57:43 AM | Threat Emulation | Prevent | Low | High | Endpoint3 | File System Emulati... | Gen.SB.dll | Trojan | f_000035 |
| Mar 30, 2022 12:57:38 AM | Threat Emulation | Prevent | Low | High | Endpoint3 | File System Emulati... | Gen.SB.dll | Trojan | f_000034 |
| Mar 30, 2022 12:57:36 AM | Threat Emulation | Prevent | Low | High | Endpoint3 | File System Emulati... | Gen.SB.dll | Trojan | 3d14a9c7-e1a7-44aa-8adf-4044e9a04c50.tr |

# クエリ言語の概要

- クエリ言語を使用すると、条件に従ってログから選択したレコードのみを表示できます
- 複雑なクエリを作成するには、ブール演算子、ワイルドカード、フィールド、範囲を使用します

- 基本的なクエリ構文は次のとおりです

```
[<Field>:] <Filter Criterion>
```

ほとんどのキーワードやクエリ条件で、大文字小文字は区別されませんが、一部例外があります
クエリ結果に期待される結果が表示されない場合、大文字小文字を変更してみます
　　例：source:<X>は、大文字小文字が区別されます。Source:<X>では一致しません

- 1つのクエリに複数の条件を含めるには、ブール演算子を使用します

```
[<Field>:] <Filter Criterion> {AND | OR | NOT} [<Field>:] <Filter Criterion> ...
```

複数の基準値を持つクエリを使用する場合、ANDは自動的に暗黙指定されるため、追加する必要はありません
必要に応じて、 ORまたはその他のブール演算子を入力します

# クエリ言語の概要

- 1単語の文字列の例
  - Alice
  - inbound
  - 192.168.2.1
  - some.example.com
  - dns_udp
- フレーズの例
  - "Alice Pleasance Liddell"
  - “Log Out"
  - “VPN-1 Embedded Connector"
- IPアドレス
  - ログクエリで使用されるIPアドレスは、1単語としてカウントされます
    - 192.168.2.1
    - 2001:db8::f00:d
  - ワイルドカード' *'文字と標準のネットワークサフィックスを使用して、範囲内のIPアドレスに一致するログを検索することもできます
    - src:192.168.0.0/16
    - src:192.168.2.0/24
    - src:192.168.2.*
    - 192.168.*

# クエリ言語の概要

- NOT 値
  - 次のとおり、ログクエリのキーワードでNOT<Field>値を使用して、フィールドの値がクエリの値ではないログを検索できます
    - `NOT <field>: <value>`
    - NOT src:192.168.2.100

- ワイルドカード
  - クエリで標準のワイルドカード文字（*および?）を使用して、ログレコードの変数文字または文字列を照合できます
    - '*' は、文字列と一致します
    - '?' は、1文字に一致します
    - Ali* は、Aliceや、Alia、 Alice Pleasance Liddell などが一致します
    - Ali? は、AliaやAlisなどが一致しますが、AliceやAlice Pleasance Liddellなどは一致しません

# クエリ言語の概要

- フィールドキーワード
  - フィルタ条件のキーワードとして、事前定義されたフィールド名を使用できます
  - `<field name>:<values>`
    - source:192.168.2.1
    - action:(Reject OR Block)

| Keyword | Keyword Alias | Description |
|---|---|---|
| severity | | Severity of the event |
| app_risk | | Potential risk from the application, of the event |
| Protection | | Name of the protection |
| protection_type | | Type of protection |
| confidence_level | | Level of confidence that an event is malicious |
| action | | Action taken by a security rule |
| blade | product | Software Blade |
| destination | dst | Traffic destination IP address, DNS name or Check Point network object name |
| origin | orig | Name of originating Security Gateway |
| service | | Service that generated the log entry |
| source | src | Traffic source IP address, DNS name or Check Point network object name |
| user | | User name |
| Rule | | Rule Number |

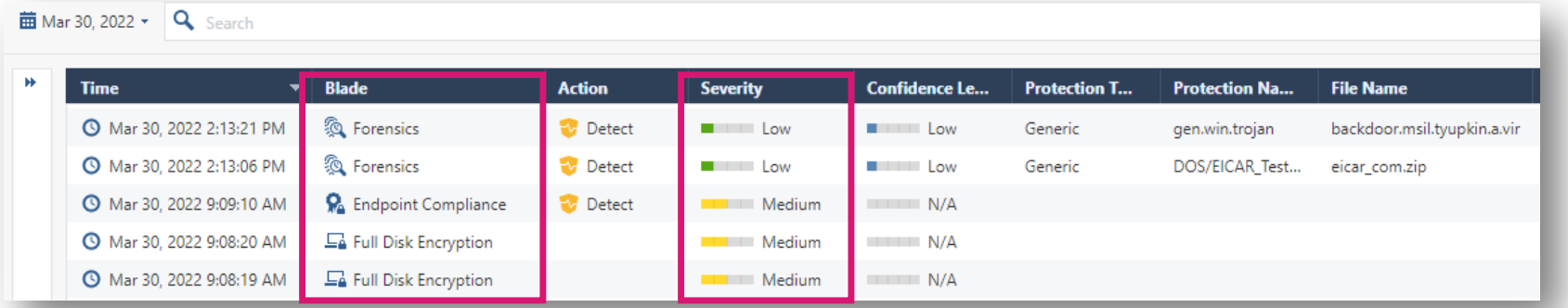
  - フィールド名を使用しない場合、いずれかのフィールドが条件に一致するレコードが表示されます

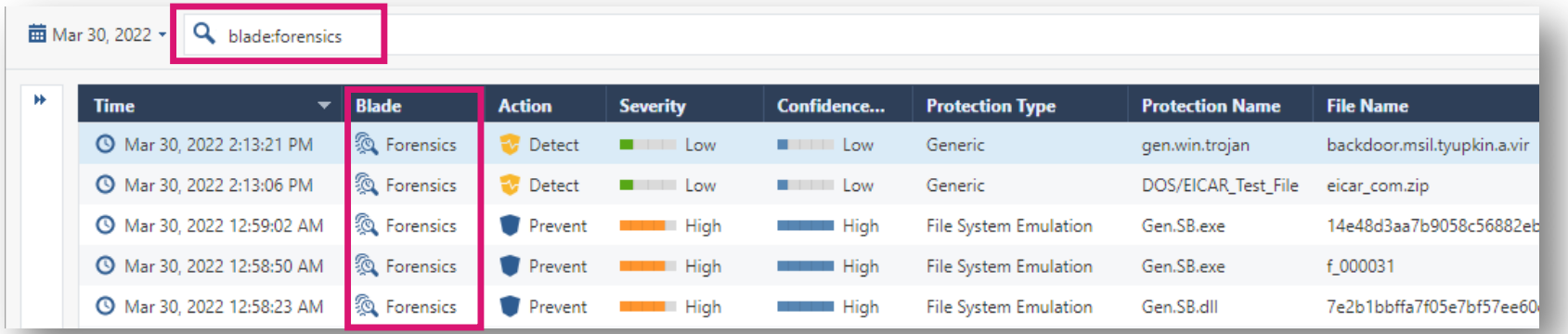
# クエリ言語の概要

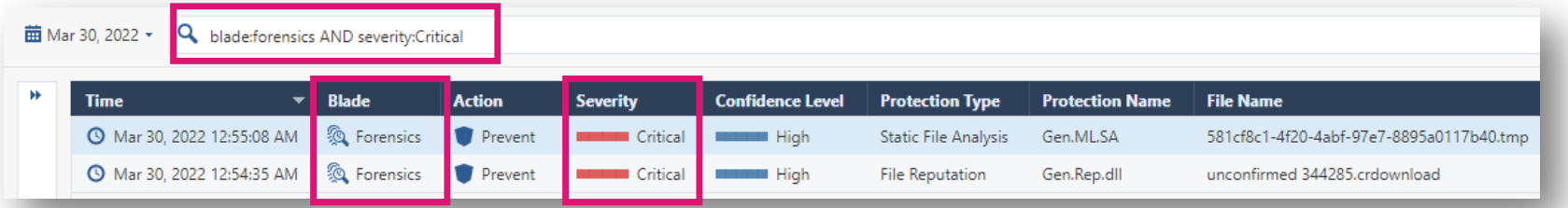
- ブール演算子
  - ブール演算子AND、OR、およびNOTを使用して、複数条件を持つフィルターを作成できます
  - 数のブール式を括弧で囲むことができます
  - ブール演算子なしで複数の条件を入力すると、AND演算子が暗黙指定されます
  - 括弧なしで複数の基準を使用する場合、OR演算子はAND演算子の前に適用されます

  - 例
    - blade:"application control" AND action:block
    - 192.168.2.133 10.19.136.101
    - 192.168.2.133 OR 10.19.136.101
    - (blade: Firewall OR blade: IPS OR blade:VPN) AND NOT action:drop
    - source:(192.168.2.1 OR 192.168.2.2) AND destination:17.168.8.2

# クエリ言語の概要



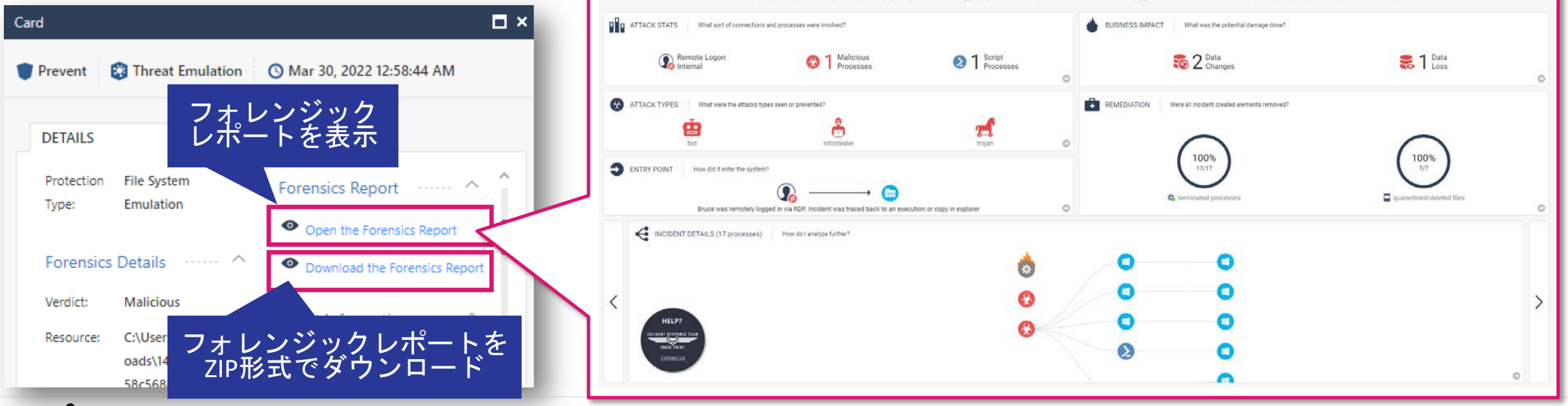



# フォレンジックレポート

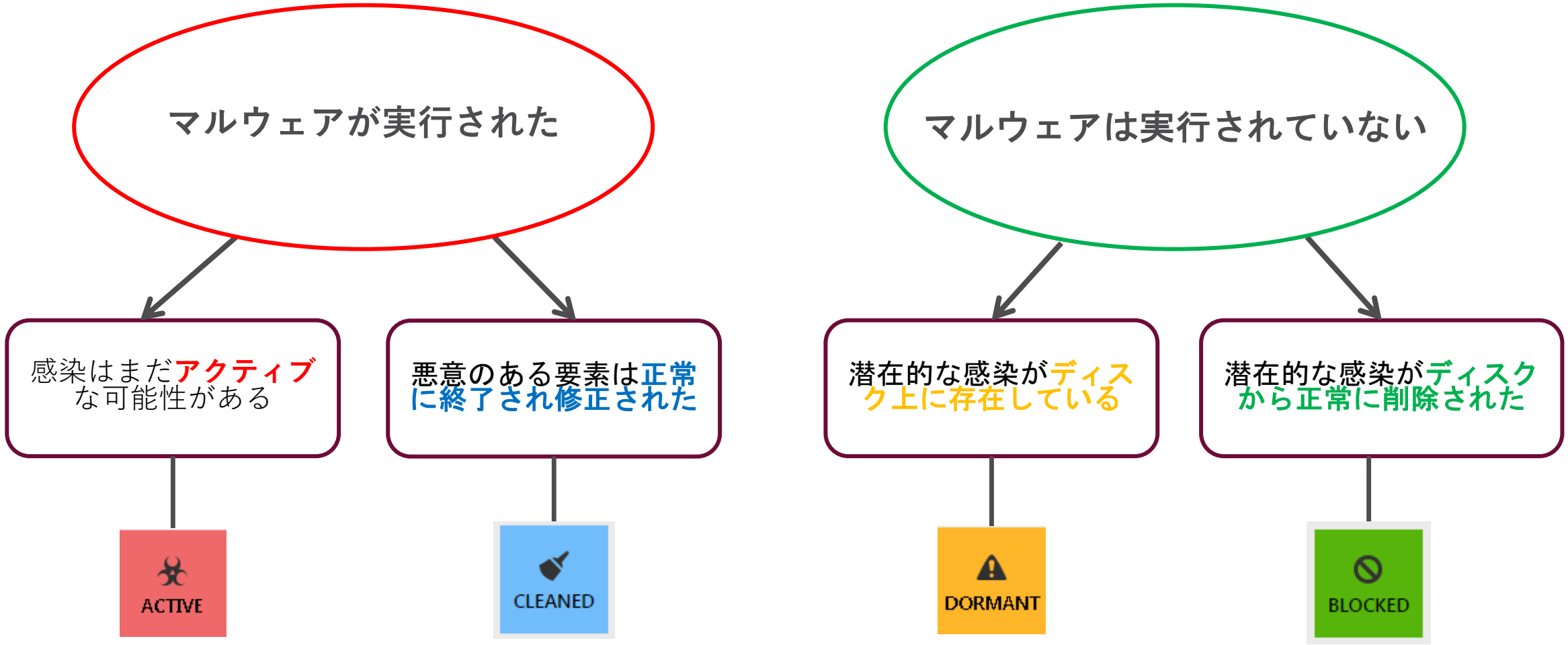
YOU DESERVE THE BEST SECURITY

# フォレンジックレポートの生成と表示

- インシデント発生時には、フォレンジックレポートが自動的に生成されます
- インシデント・ログの Forensics Report > Open the Forensics Report からアクセス可能です
- フォレンジックレポートは、次の質問に対する回答を提供します
  - どのようにしてシステムに入りましたか？
  - 感染はまだ存在していますか、それとも除去されましたか？
  - どんな被害が発生しましたか？



# インシデントのステータス（１／２）

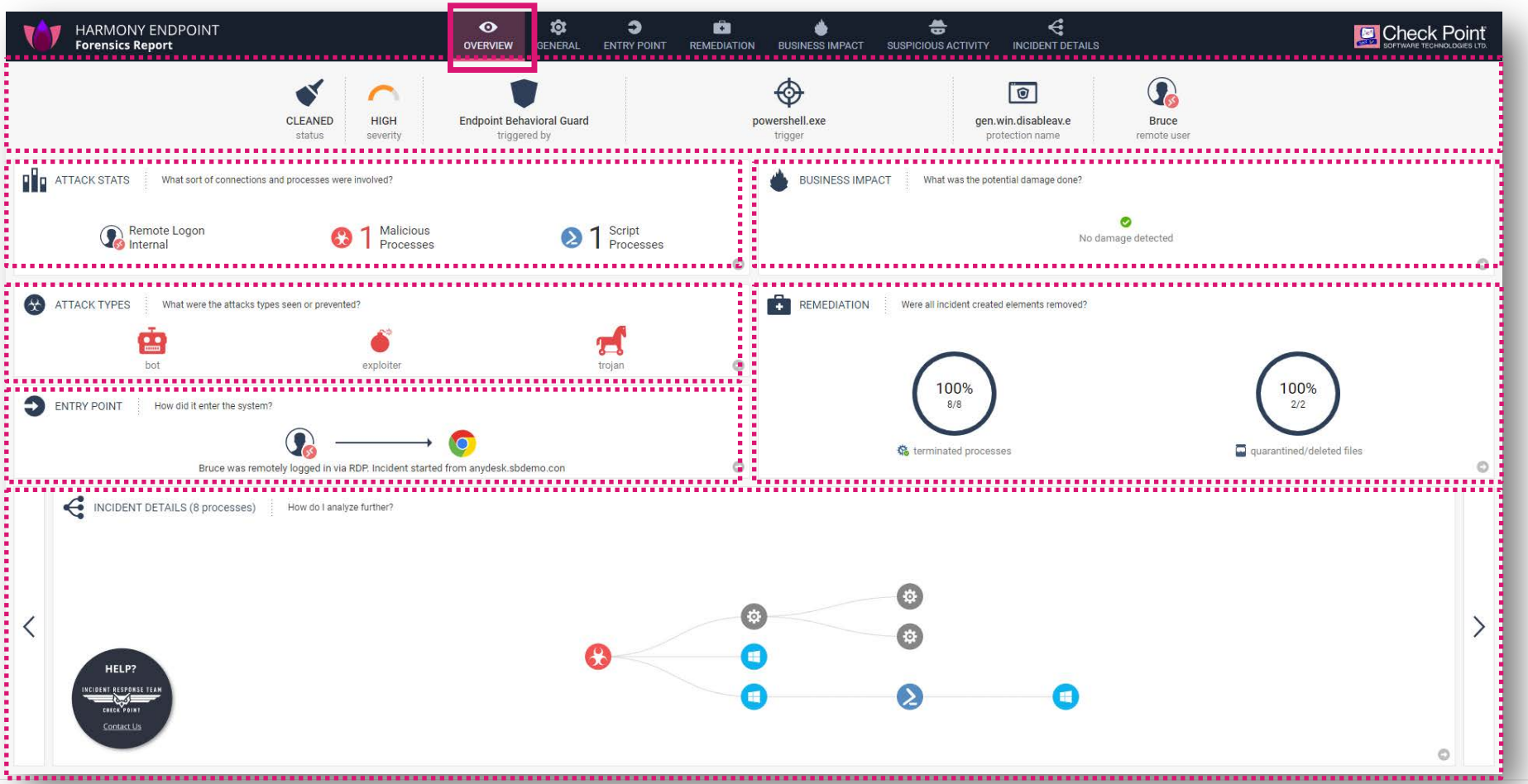


# インシデントのステータス（2／2）

- 攻撃分析中に、修復プロセスを実行しています。 インシデントの判断（または現在のコンピュータのステータス）は、このプロセスの結果によって異なります
- **Active:**
  - 悪意のあるプロセスが実行され、システムが感染しました
  - プロセスまたは攻撃の他の要素の終了と隔離は、ポリシーで無効になっているか、失敗しています
- **Cleaned:**
  - 悪意のあるプロセスが実行され、システムが感染しましたが、攻撃要素の終了と隔離が成功しました
  - システムがまだ損傷している可能性があります
- **Dormant:**
  - 悪意のあるプロセスは実行されませんでしたが、システムは感染していました
  - 検出されたファイルの隔離に失敗しました
- **Blocked:**
  - 悪意のあるプロセスは実行されませんでした。
  - 検出されたすべてのファイルの隔離に成功しました
  - 攻撃は即座にブロックされ、システムは感染していなかったため、被害はありませんでした

# フォレンジックレポート：Overview

- Overview で攻撃の全体像を把握することができます
- 各項目をドリルダウンするか、画面上部のメニューバーからアイコンを選択することで詳細な情報を表示することができます




攻撃概要

攻撃統計

攻撃タイプ

侵入経路

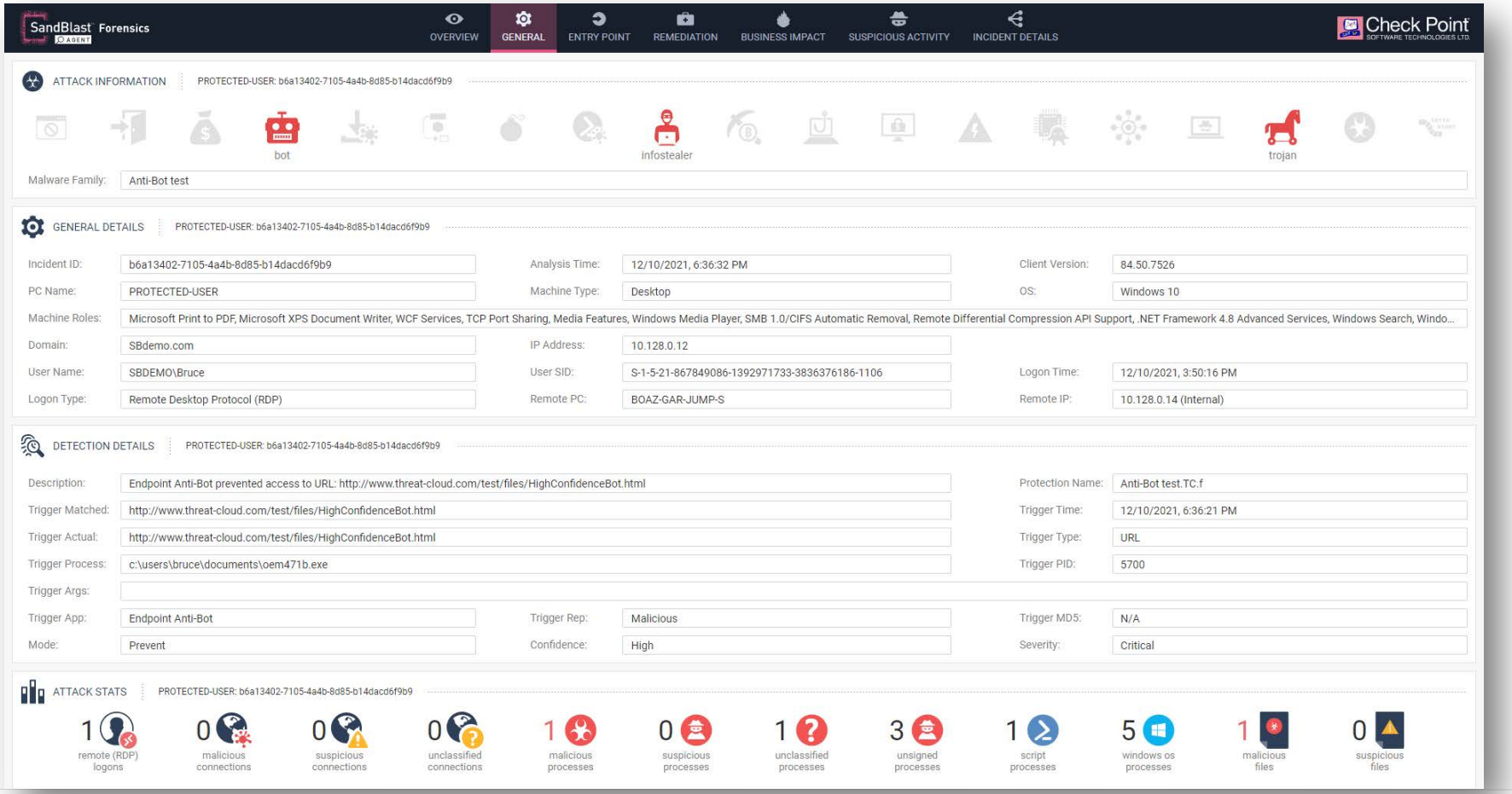
プロセスツリー

被害状況

修復状況

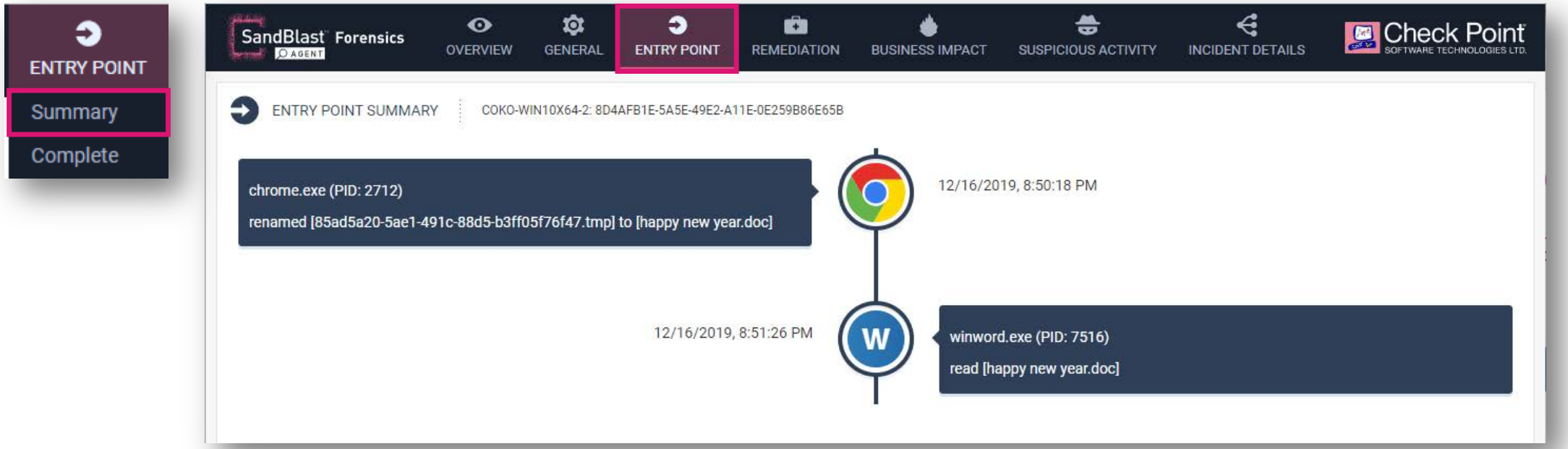
# フォレンジックレポート：General

- インシデントと検出に関する一般的な情報を表示します
- 一般的な情報には、時間、コンピュータ名、ドメイン、ユーザー名、OS、IDが含まれます
- 検出の詳細には、トリガーが含まれます：時間、プロセス、PID、トリガーを送信したAP



# フォレンジックレポート：Entry Point - Summary

- Entry Point は、攻撃者がマルウェアを展開することに成功した弱点を示すことで、セキュリティに潜む脆弱なベクターを明らかにする可能性があります

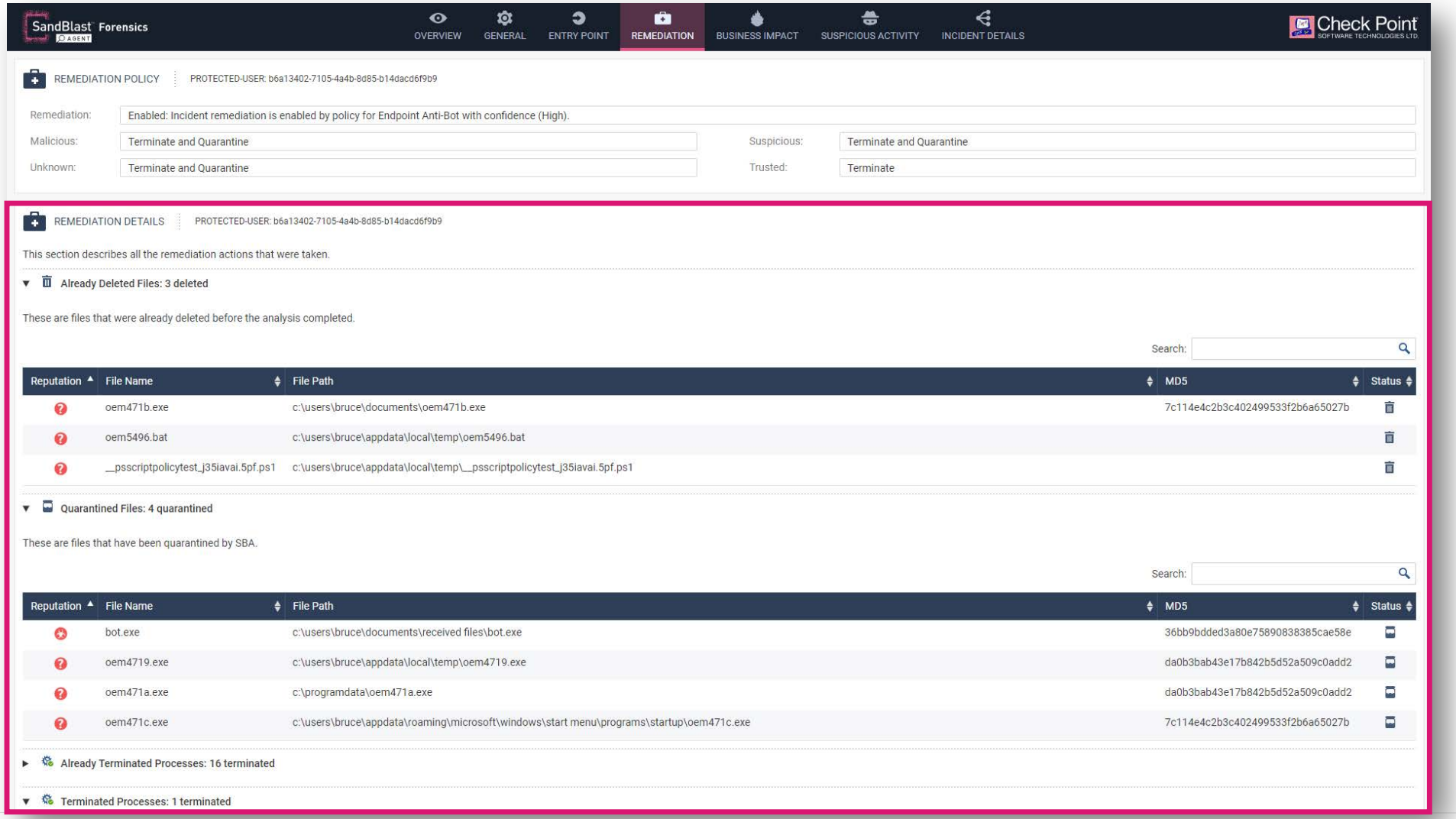


# フォレンジックレポート：Entry Point - Complete

- Entry Point は、攻撃者がマルウェアを展開することに成功した弱点を示すことで、セキュリティに潜む脆弱なベクターを明らかにする可能性があります

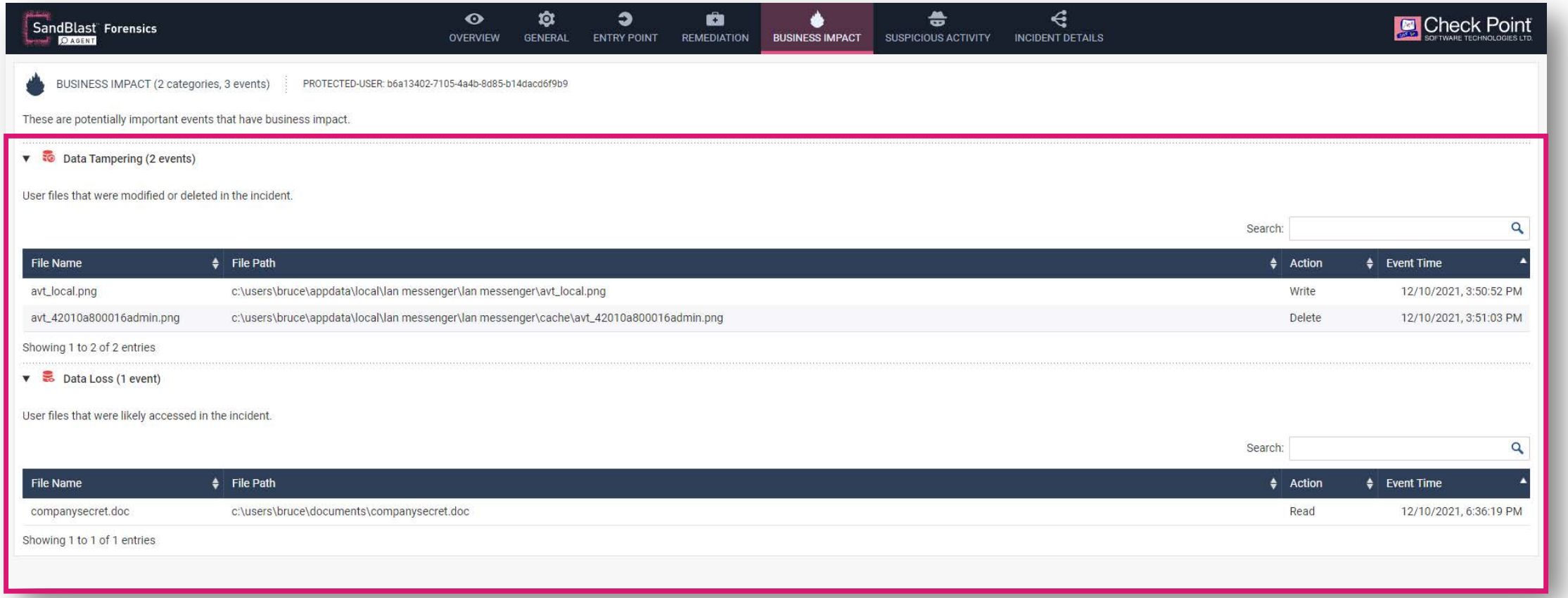
# フォレンジックレポート：Remediation

- Remediation は、ファイルの修復状況（削除、隔離）や、プロセスの停止状況を表示します



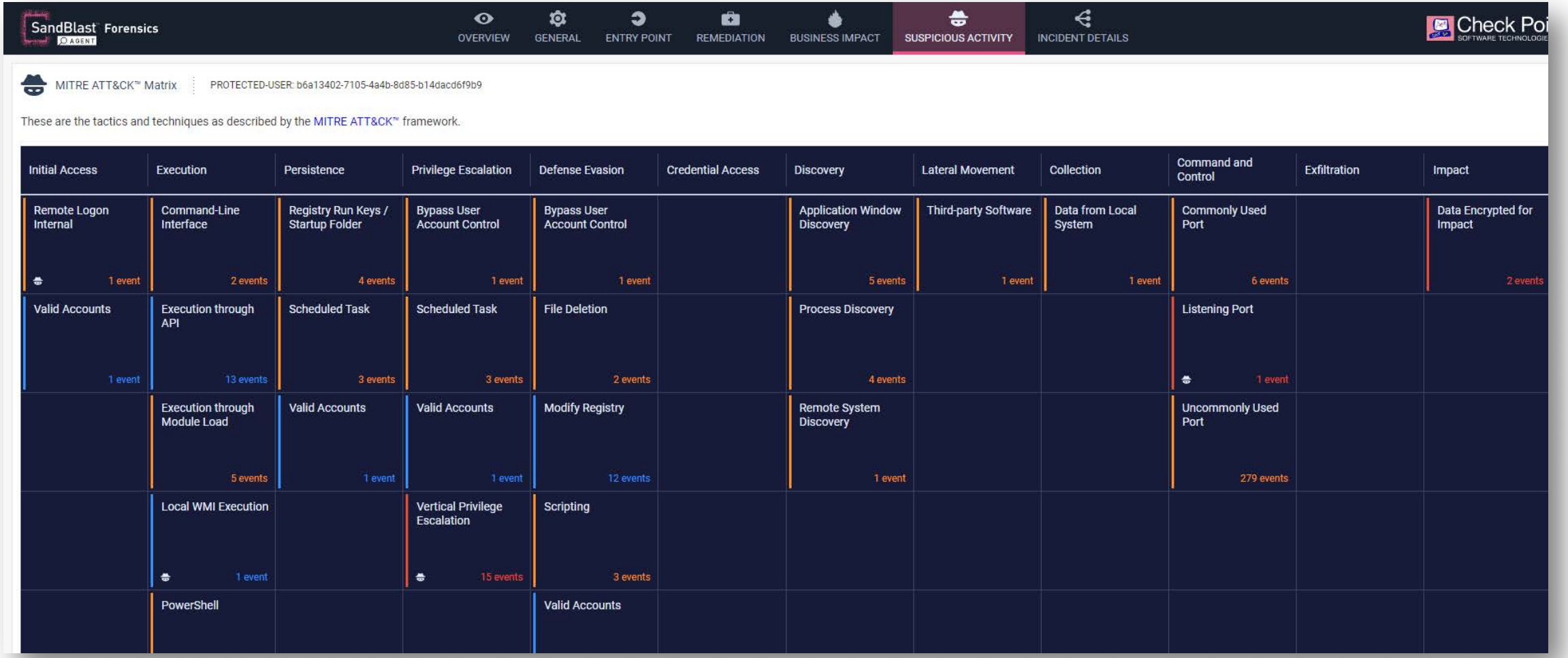
# フォレンジックレポート：Business Impact

- Business Impactは、コンピュータおよびコンピュータに直接接続されている他のデバイス（外部ストレージデバイス、ネットワーク共有など）のデータを侵害するためにマルウェアによって行われた損害またはアクションを表示します
- ビジネスへの影響のセクションは、修正と復元が行われた後に更新されます



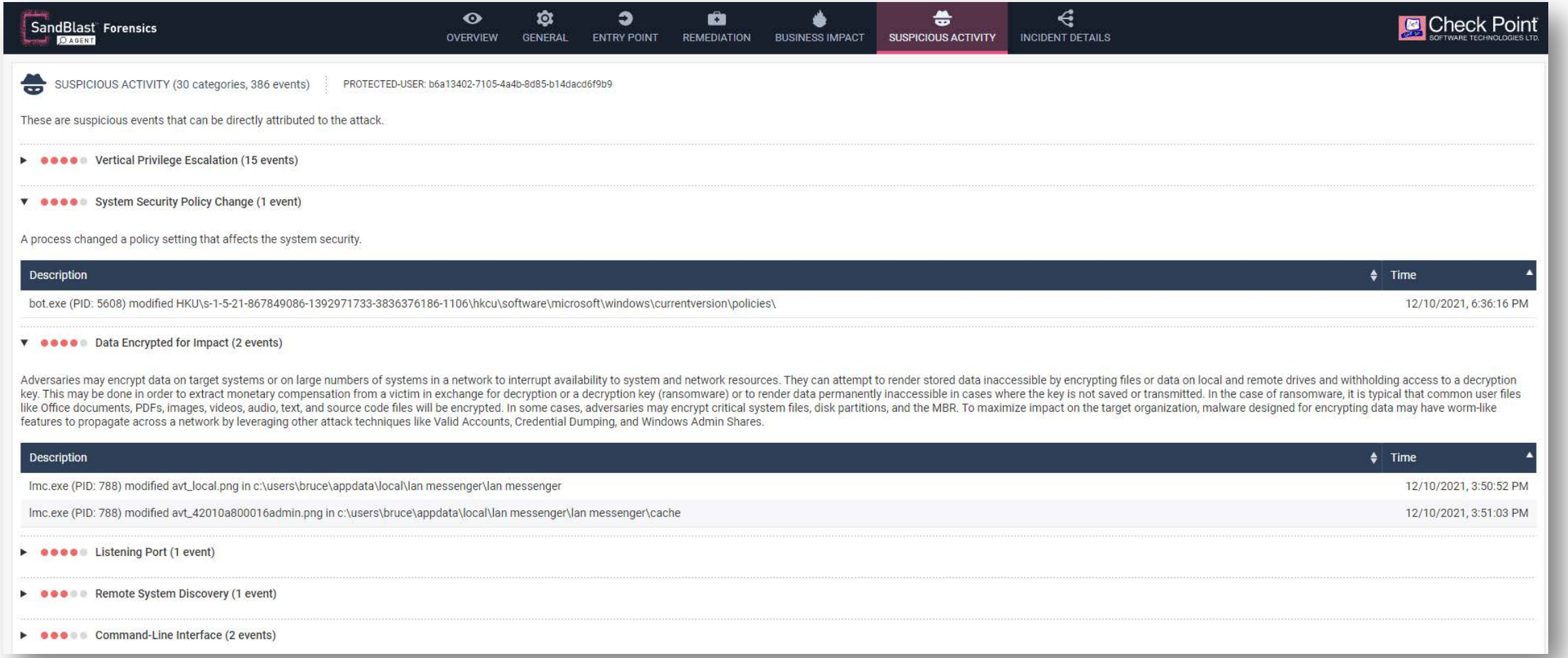
# フォレンジックレポート：Suspicious Activity（1／3）

- MITREATT＆CK™ Matrix ビューは、攻撃と疑わしいアクティビティを MITREATT＆CK™ Framework の戦術と手法にマッピングして表示します



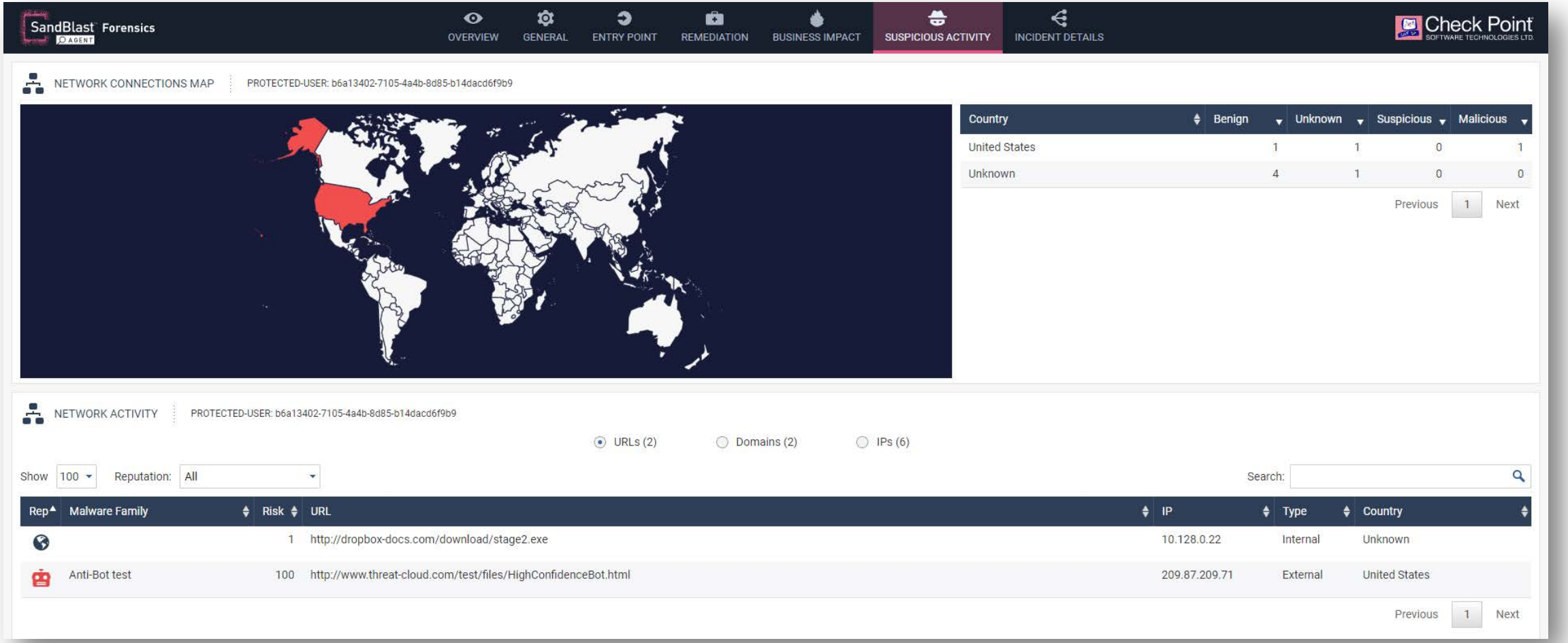
# フォレンジックレポート：Suspicious Activity（2／3）

- Suspicious Events ビューは、悪意のあるアクティビティを示すさまざまなカテゴリで構成され、重大度レベルごとに整理して表示します



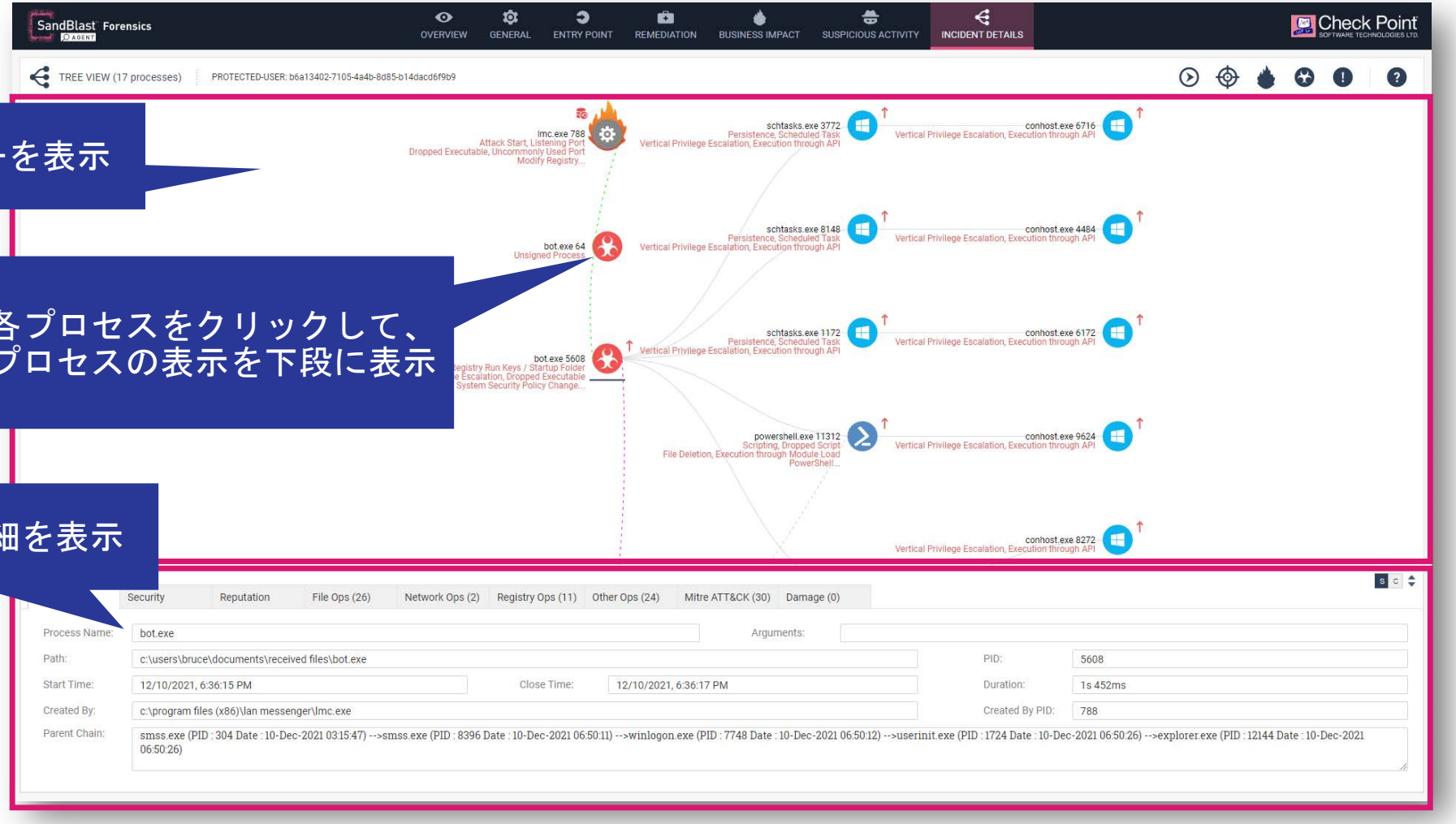
# フォレンジックレポート：Suspicious Activity（3／3）

- Network Events ビューは、攻撃で発生したネットワークイベント（外部、内部へのネットワーク接続）を表示します



# フォレンジックレポート： Incident Details（1／3）

- Tree ビューは、攻撃に使用されたプロセスのプロセスツリーと各プロセスの詳細を表示します



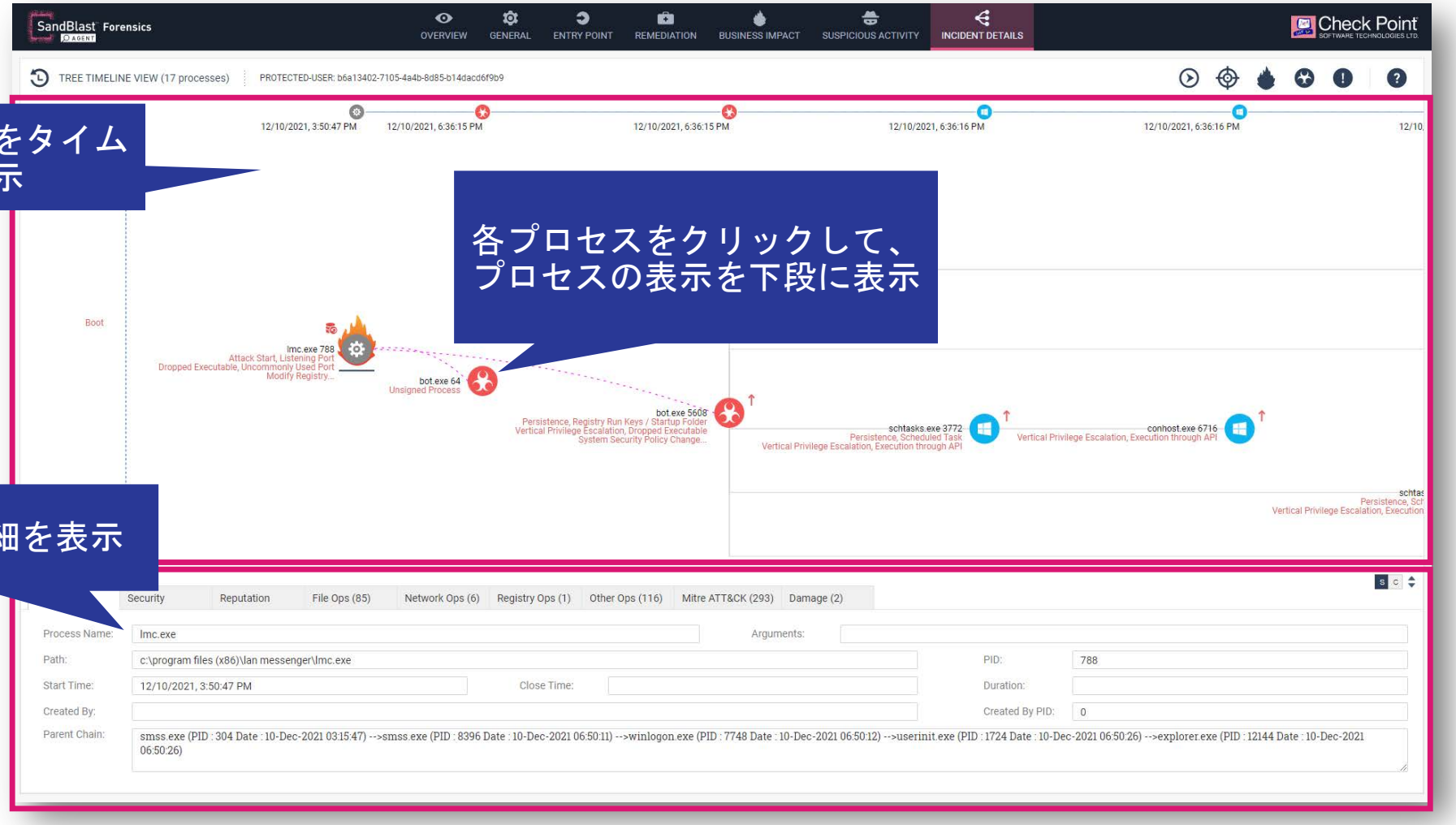

プロセスツリーを表示

各プロセスをクリックして、
プロセスの表示を下段に表示

プロセスの詳細を表示

# フォレンジックレポート： Incident Details（2／3）

- Tree Timelineビューは、攻撃に使用されたプロセスのプロセスツリーをタイムラインで表示します



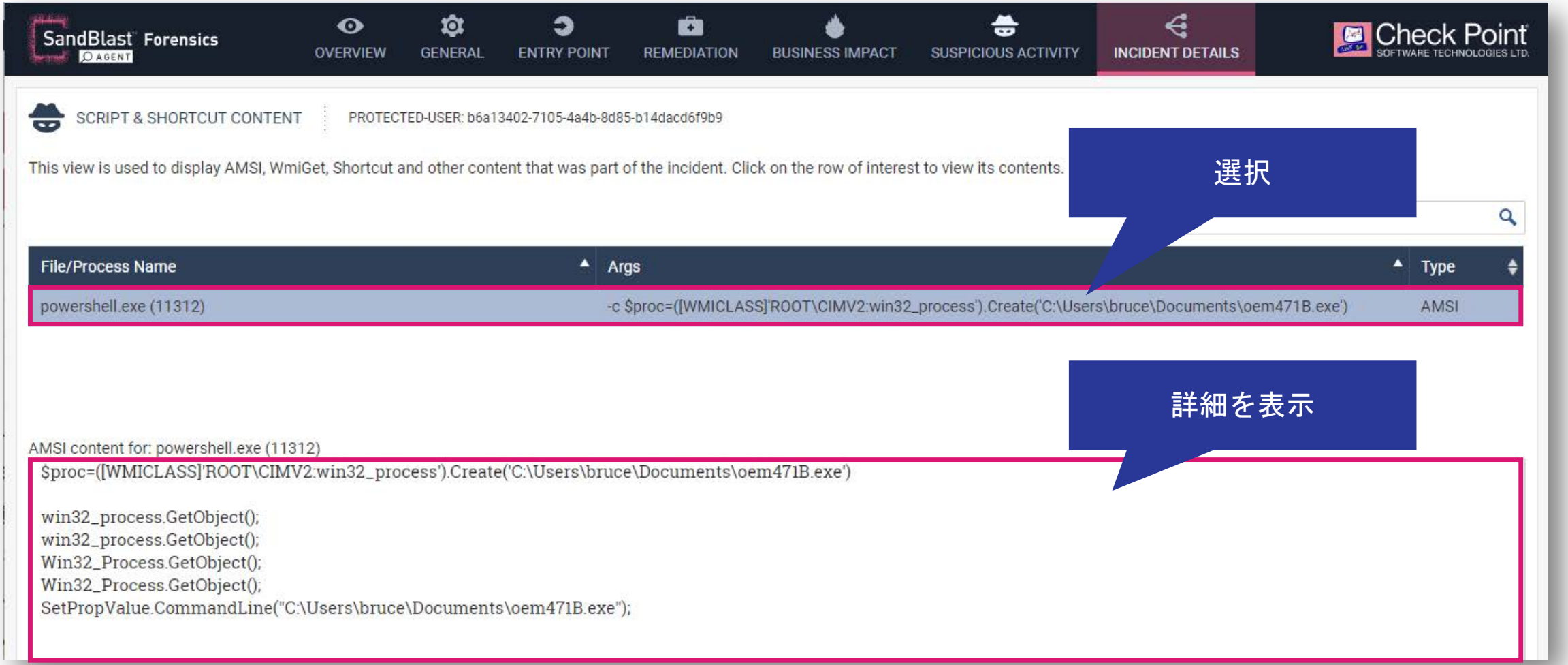

プロセスツリーをタイムライン表示

各プロセスをクリックして、プロセスの表示を下段に表示

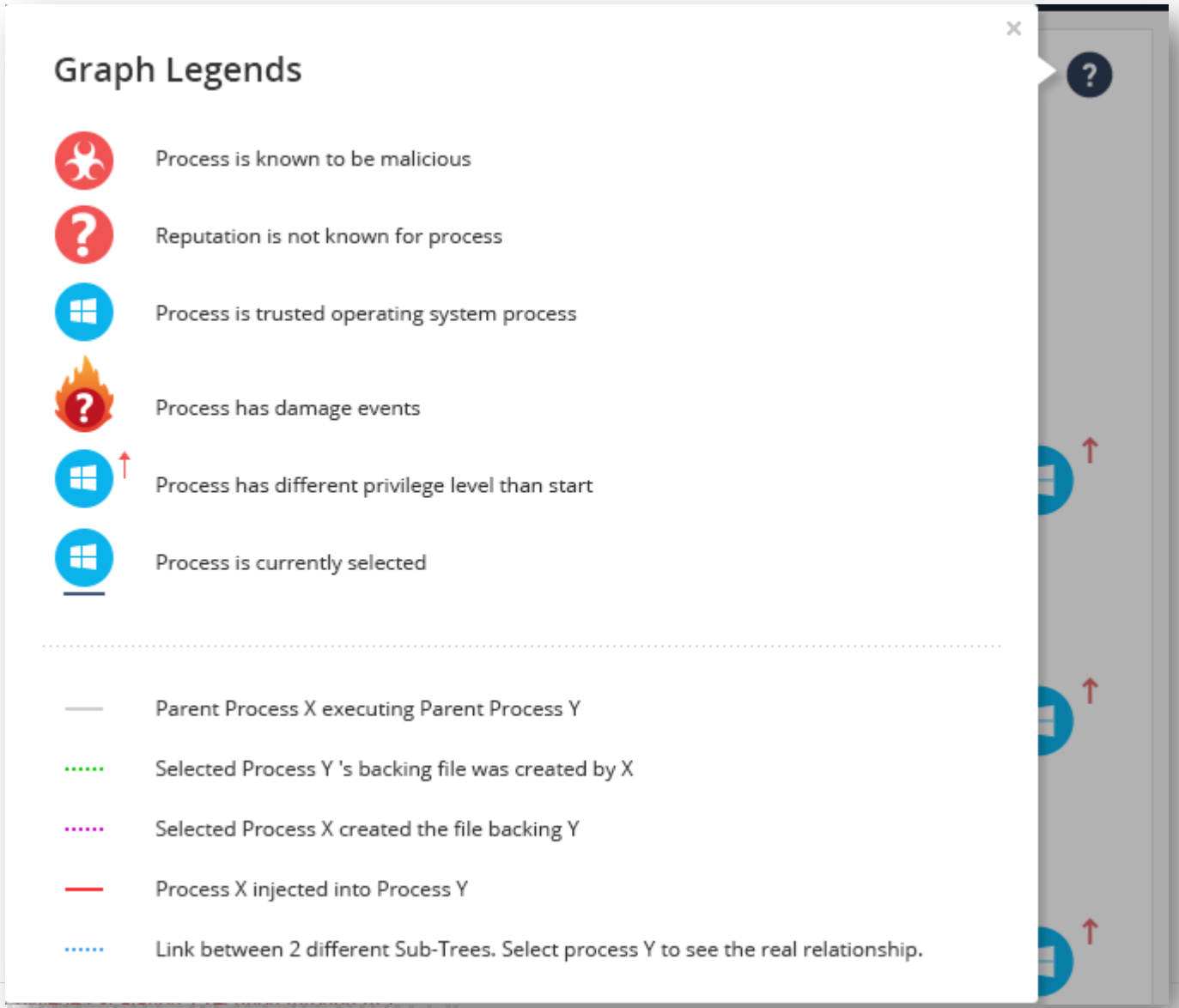
プロセスの詳細を表示

# フォレンジックレポート： Incident Details（3／3）

- Script & Shortcut Content ビューは、AMSIや、WmiGet、ショートカット、インシデントの一部であったコンテンツなどを表示するために使用されます



# フォレンジックレポート：凡例

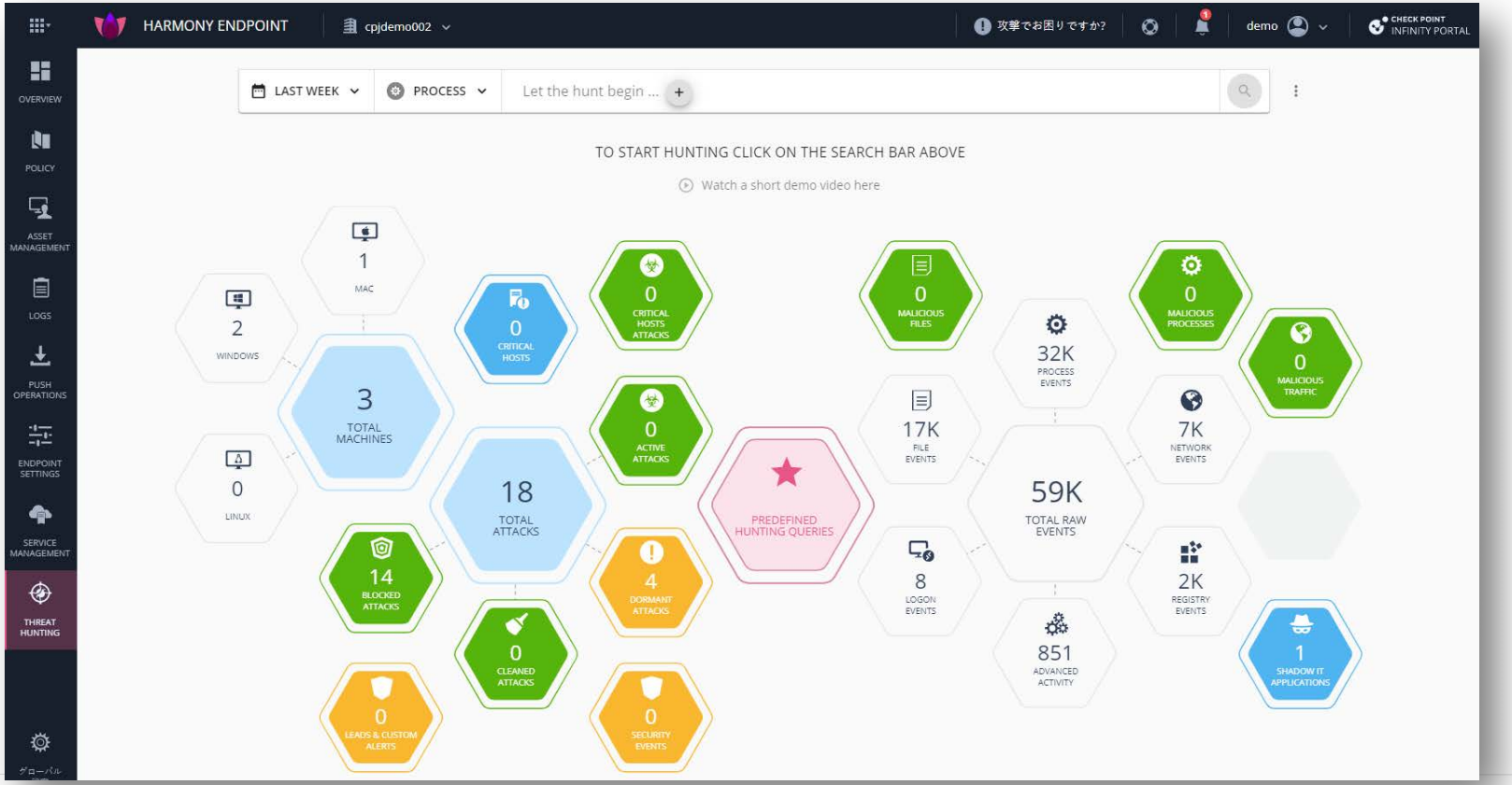


# THREAT HUNTING

YOU DESERVE THE BEST SECURITY

# Threat Hunting の概要（1／2）

- Threat Hunting は、エンドポイントからすべてのイベントを収集し、調査するツールです
- イベントには、良性のデータと悪意のある可能性のあるデータの両方が含まれます
- Threat Hunting により、すべてのイベントを完全に可視化して、攻撃の全範囲を理解し、ステルス攻撃を明らかにすることができます
  - ※ データ保持期間は、デフォルトで 7 日間です（オプション購入で最長1年まで延長できます）



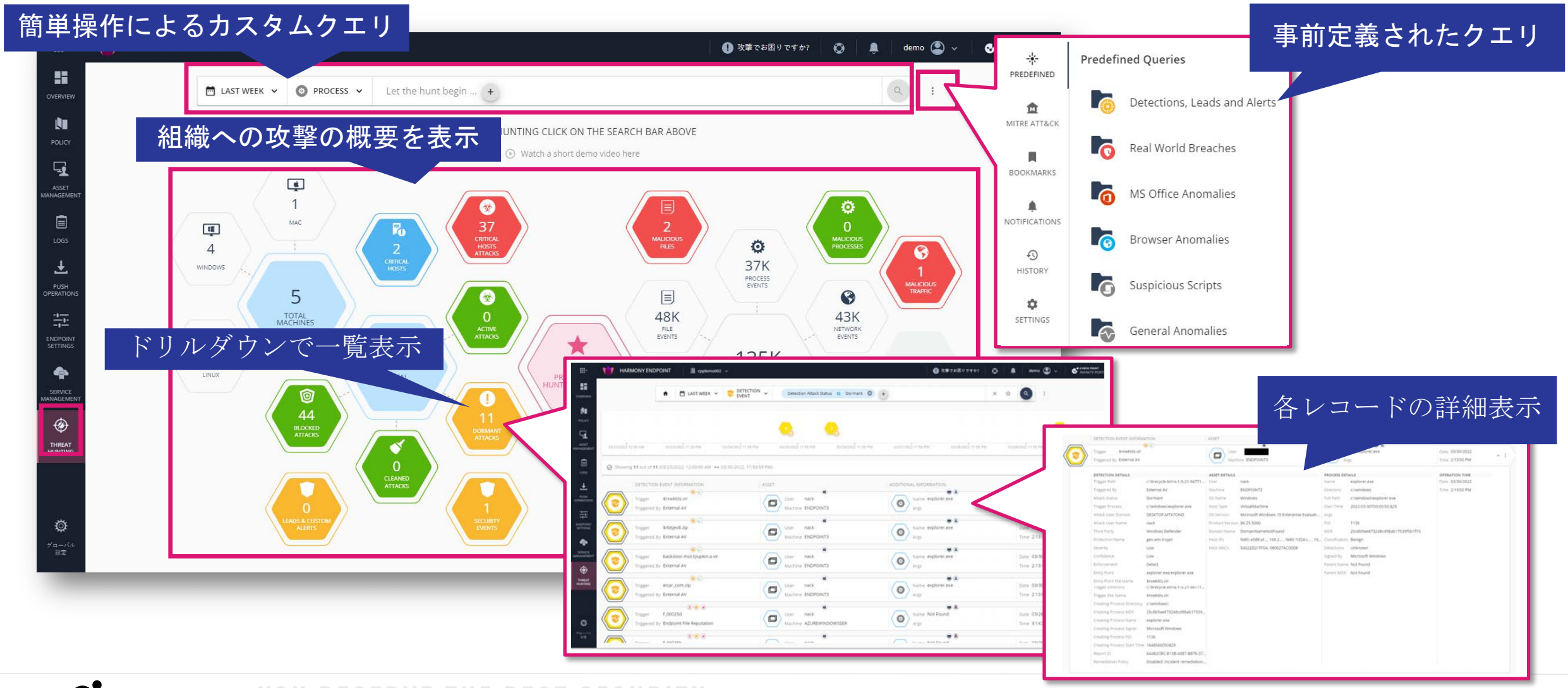
# Threat Hunting の概要（2／2）

- Threat Hunting には、次の利点があります
  - アラートだけでなく、すべてのエンドポイントのすべてのイベントに対する完全な可視性
  - 攻撃の全範囲の調査
  - 疑わしいアクティビティを明らかにする
  - 複数の修復アクションによる、疑わしいアクティビティの修復
  - 調査、ハンティング、修復を簡単にする

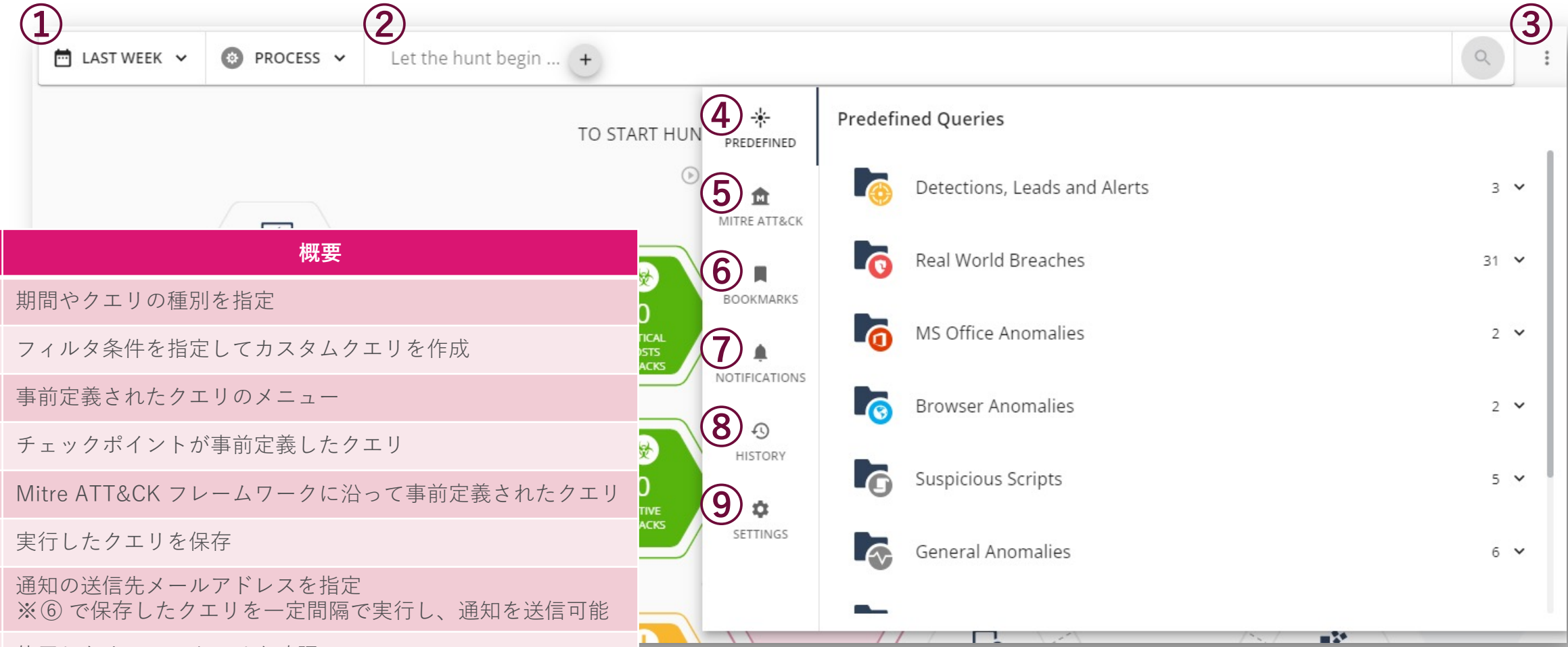
- 発見されたイベントに対して以下の修復を行えます
  - プロセスを強制終了
  - ファイルを隔離
  - コンピュータを隔離
  - フォレンジックを利用して攻撃を分析
  - フォレンジック分析によって検出されたプロセスを強制終了
  - フォレンジック分析によって検出されたファイルを隔離

# ハンティング画面の概要（1／2）

- 事前定義された条件や、カスタム条件により組織に潜む脅威を探索します



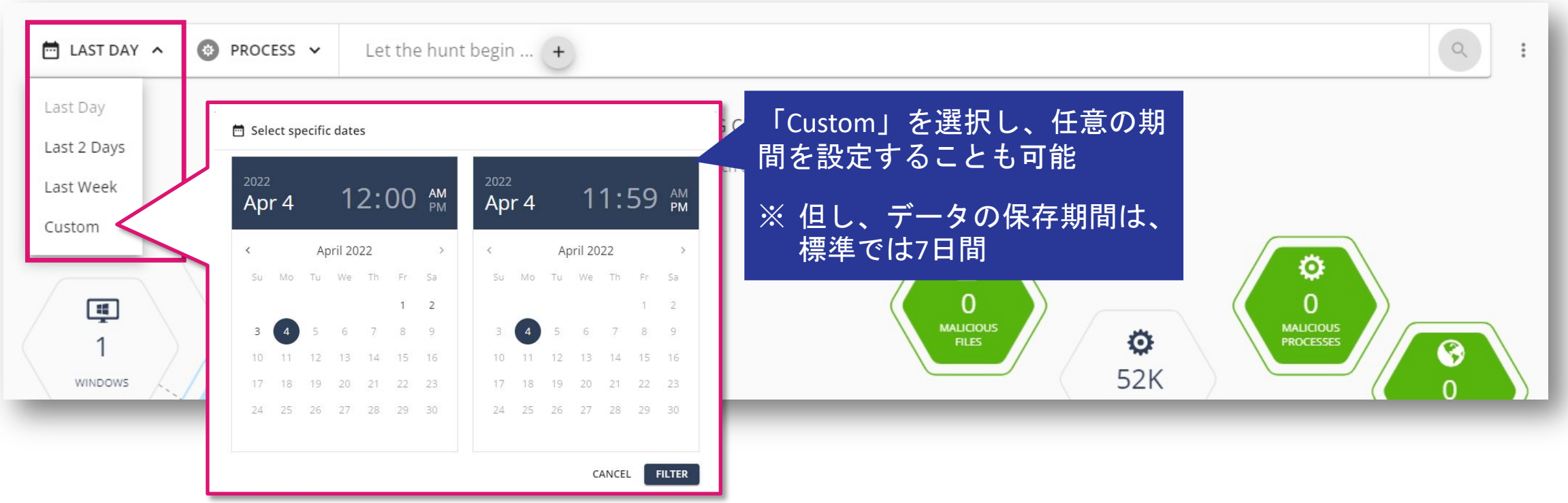
# ハンティング画面の概要（2／2）




| 項番 | 概要 |
|---|---|
| ① | 期間やクエリの種別を指定 |
| ② | フィルタ条件を指定してカスタムクエリを作成 |
| ③ | 事前定義されたクエリのメニュー |
| ④ | チェックポイントが事前定義したクエリ |
| ⑤ | Mitre ATT&CK フレームワークに沿って事前定義されたクエリ |
| ⑥ | 実行したクエリを保存 |
| ⑦ | 通知の送信先メールアドレスを指定<br>※⑥ で保存したクエリを一定間隔で実行し、通知を送信可能 |
| ⑧ | 使用したすべてのクエリを確認 |
| ⑨ | UI の見た目を設定 |

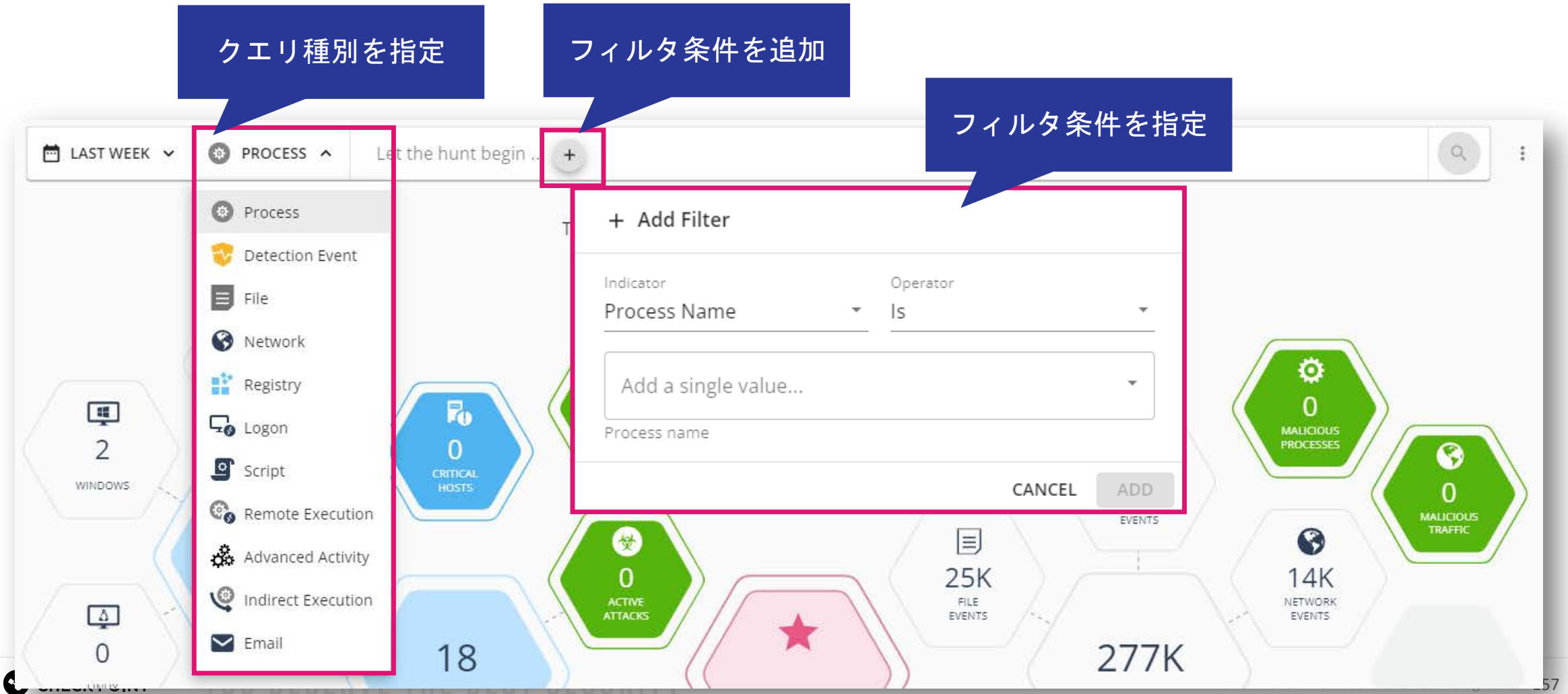
# Threat Hunting：期間の指定

- Threat Hunting する期間を、Last Day、Last 2 Days、Last Week、Custom から指定可能です
  ※ 但し、データの保存期間は、標準では7日間です



# Threat Hunting：クエリ種別、フィルタ条件の指定

- クエリ種別には、プロセスや検知イベント、ファイル、ネットワーク接続などを指定します
- フィルタ条件には、プロセスやファイルの名称・ハッシュ値、ドメイン名、IPアドレスなどを指定します



# （参考）フィルタ条件のキー

- Activity Details
- Activity Name
- Activity Target PID
- Activity Target Directory
- Activity Target Name
- Activity Type
- Browser Name
- Browser Version
- Process Start Time
- Detection Attack Status

- Detection Trigger Process
- Detection Attack User Domain
- Detection Attack User Name
- Detection Creating Process Start Time
- Detection Creating Process PID
- Detection Description
- Detection Email Attachment

- Detection Email Delivery Date
- Detection Email Embedded URL
- Detection Email Sender
- Detection Email ID
- Detection Email Subject
- Detection Email Recipient
- Detection Enforcement
- Detection Entry Point Process

- Detection Entry Point File MD5
- Detection Entry Point File Name
- Detection Entry Point Network
- Detection Entry Point Browser Tab
- Detection General Info
- Detection Impersonated Brand
- Detection Impersonated Domain

- Detection Impersonated Type
- Detection Confidence
- Detection Report ID
- Detection Severity
- Detection Trigger Path
- Detection Malware Family
- Detection Protection Name
- Detection Protection Type
- Detection Remediation Policy

- Detection Remediation Policy
- Detection Third Party
- Detection Trigger MD5
- Detection Triggered By
- Domain Classification
- Email Attachments Count
- Email BCC
- Email CC
- Email From
- Email Message Id

- Email Message Id
- Number Of Recipients
- Email Server Name
- Source country
- Email Status
- Email Subject
- Email To
- Email Direction
- Email URLs Count
- Logon Event

- Execution Details
- Execution Name
- Execution Target PID
- Execution Target Directory
- Execution Target Name
- Execution Type
- File Classification
- File Directory
- File MD5
- File Name

- New File Directory
- New File Name
- File Operations
- File Path
- File Signer
- File Size
- File Type
- Gateway Blade
- Host IPs
- Host MACs

- Host Type
- Logon Account Type
- Logon ID
- Logon Origin
- Machine Name
- Network Bytes Received
- Network Bytes Sent
- Network Connection Direction
- Network Dest IP
- Network Dest Port

- Network Email Display URL
- Network Domain
- Network HTTP Method
- Network Is Listening
- Network Path
- Network Protocol
- Network Referer
- Network Status Code
- Network Src IP

- Network Src Port
- Network Sensor
- Network URL
- Network User Agent
- OS Name
- OS Version
- Original File Classification
- Parent Process Args
- Parent Process Directory
- Parent Process Integrity Level

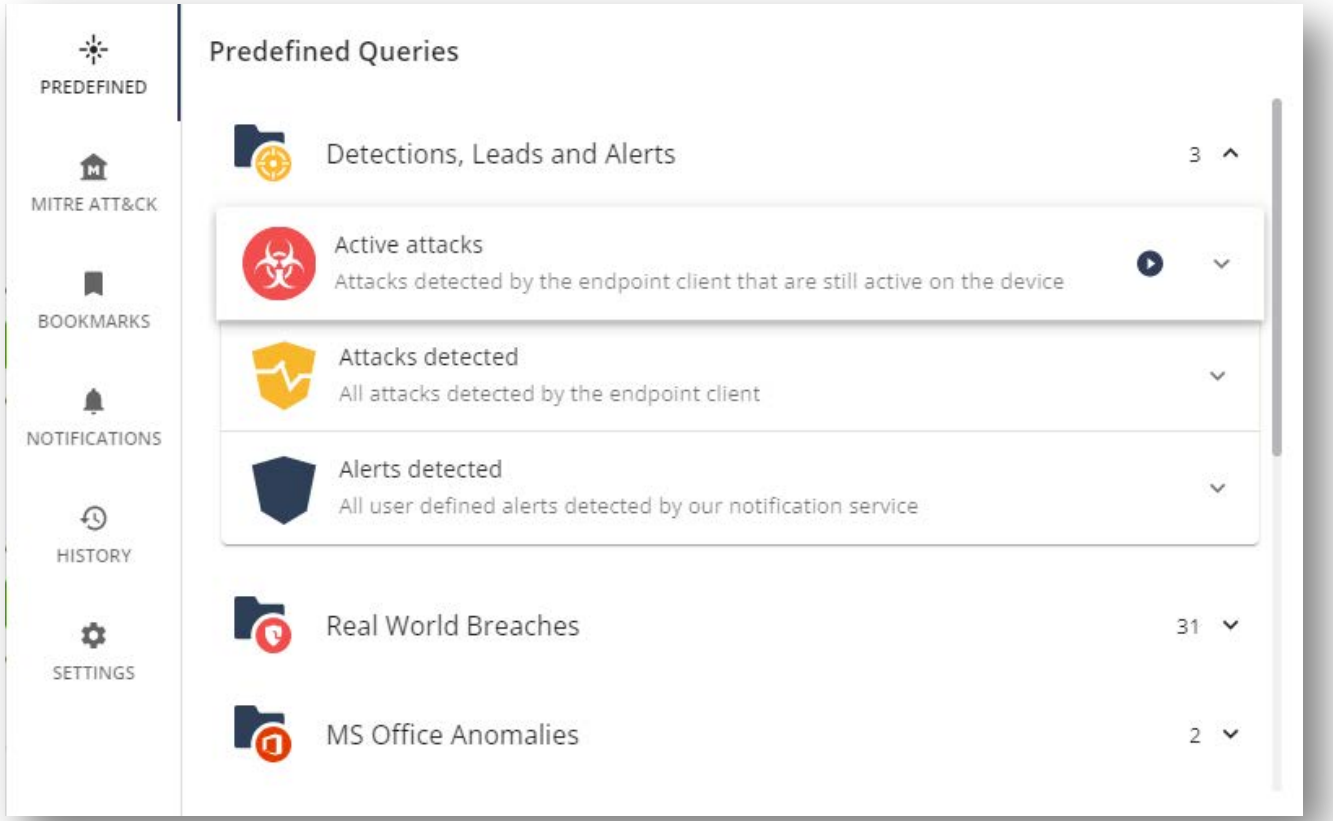
- Process Signer Is Invalid
- Logon Session
- Process MD5
- Process Name
- Process Original Name
- Parent PID
- Process Path
- Process Signer
- Process Trusted Signer
- Product Version

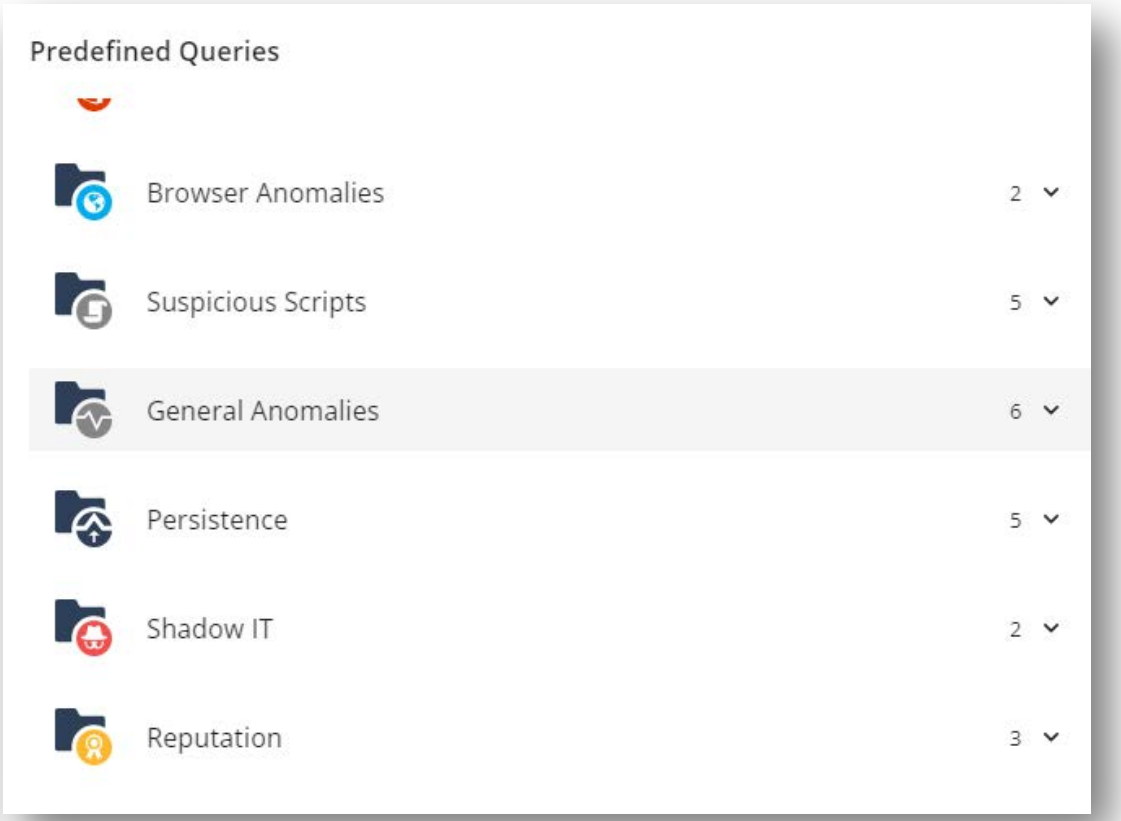
- Registry Key
- Registry New Data
- Registry Old Data
- Registry Operations
- Registry Value
- Remote Ip Address
- Remote Machine Name
- Logon Event ID
- Remote Execution Type
- Logon Type

- Connection Count
- Logon User Domain
- Logon User Name
- Reputation Risk
- Script Data
- User Name

# Threat Hunting：事前定義されたクエリ

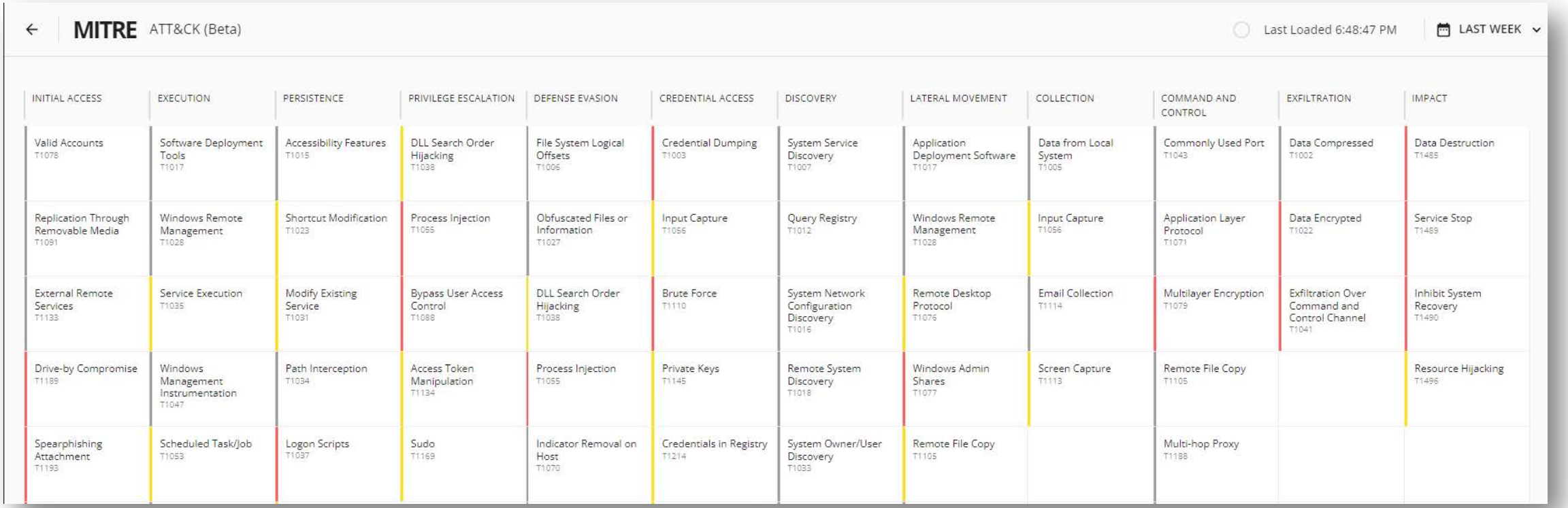
- 事前定義されたクエリを使用することで簡単に脅威をハンティングすることができます



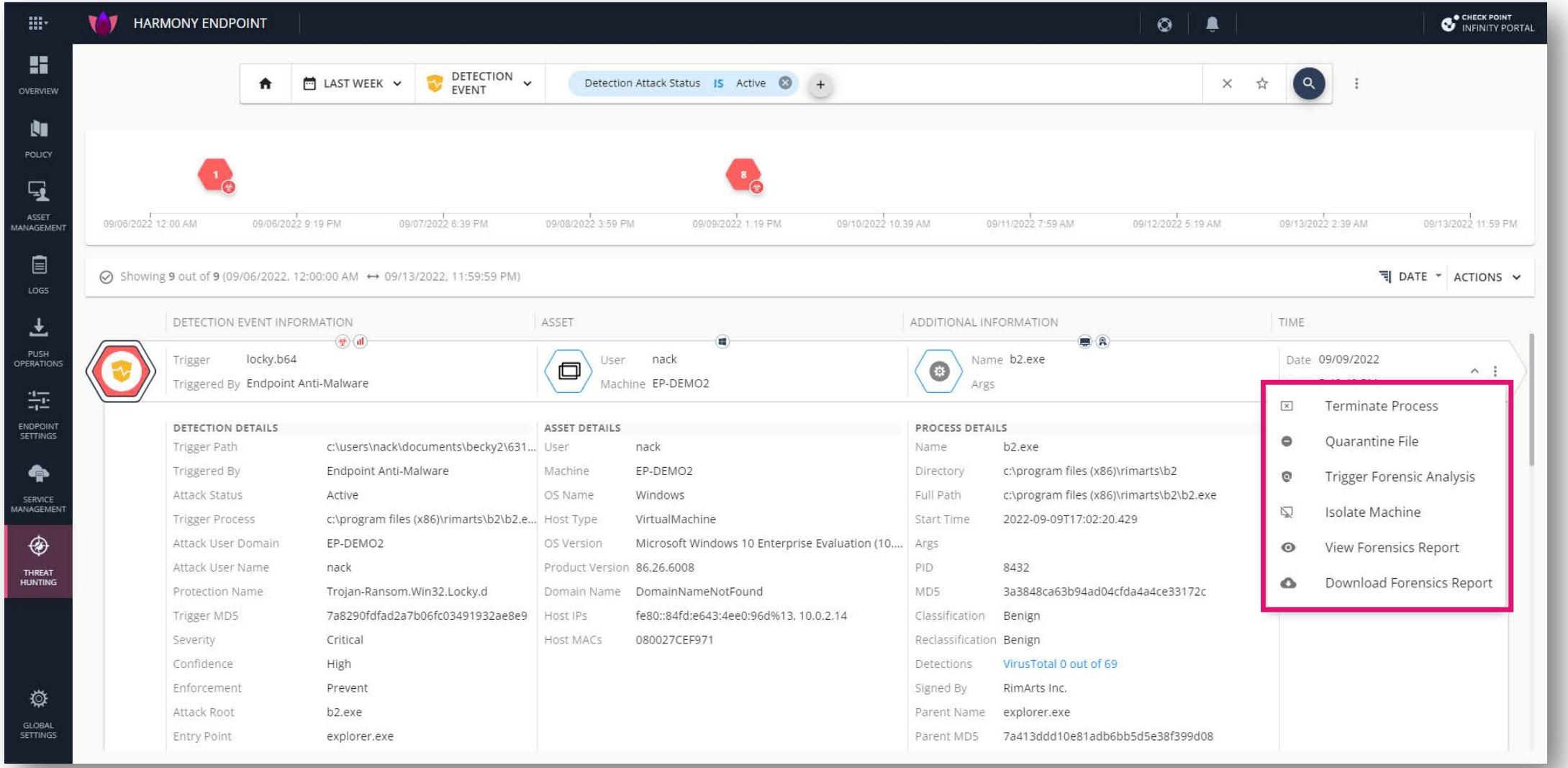
# Threat Hunting： MITER ATT＆CKダッシュボード

- MITER ATT＆CKダッシュボードは12のカテゴリに分けられ、各カテゴリは攻撃のステージです
- 各カテゴリには、複数の攻撃手法が含まれています。テクニックをクリックすると、テクニックの説明と事前定義されたクエリのリストが表示されたウィンドウが開きます。クエリを実行して、特定の手法の実装が使用されたイベントのリストを取得します
- 悪意のある、疑わしい、または良性であるかどうかに関係なく、すべての生のイベントをMITRE TTPにマップします



# Threat Hunting：修復

- 発見されたイベントに対して、プロセスの停止やファイルの隔離などの修復を行えます



# アラート通知設定

YOU DESERVE THE BEST SECURITY

# アラート通知設定（1／4）

Threat Hunting

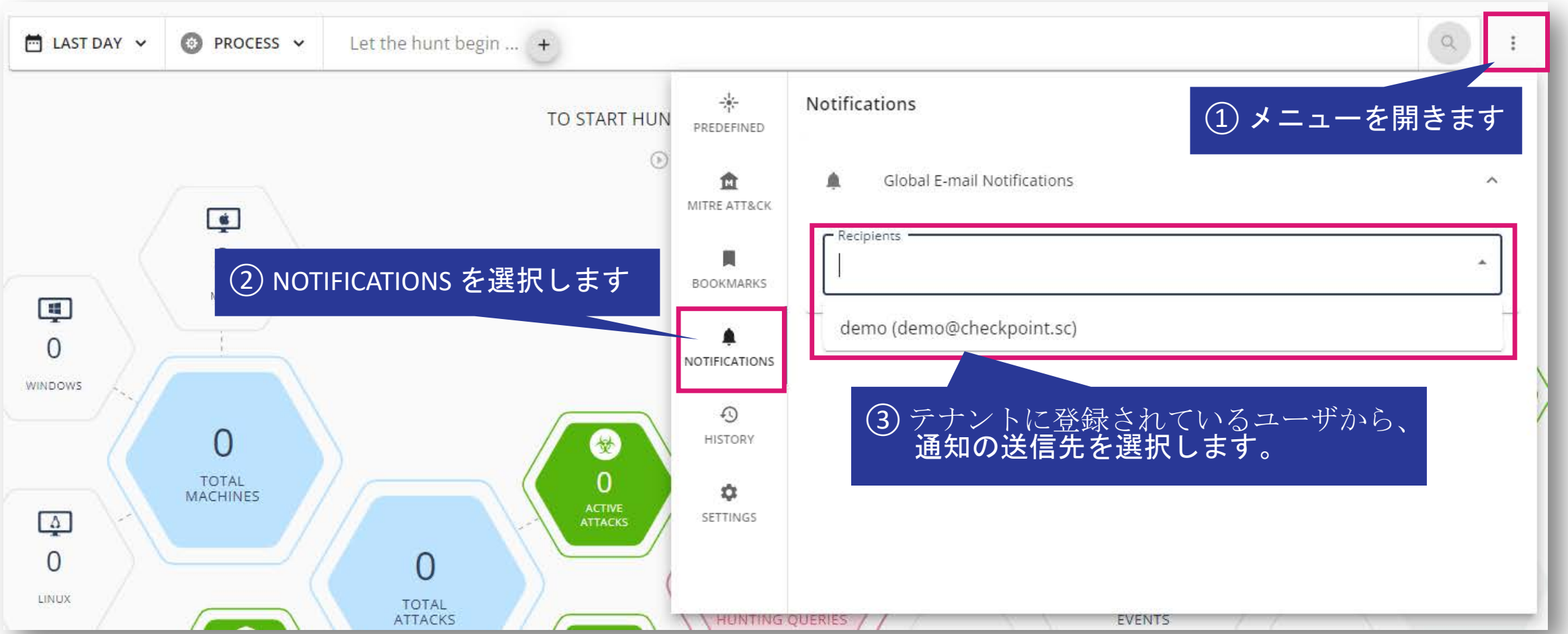
- 事前設定した条件で Threat Hunting を定期実行し、新規にイベントを発見した際に、管理者に通知できます
- Threat Hunting 画面で、通知したいイベントと通知先メールアドレスを設定します

## アラート通知フロー

# アラート通知設定（2／4）：アラート通知宛先設定

Threat Hunting

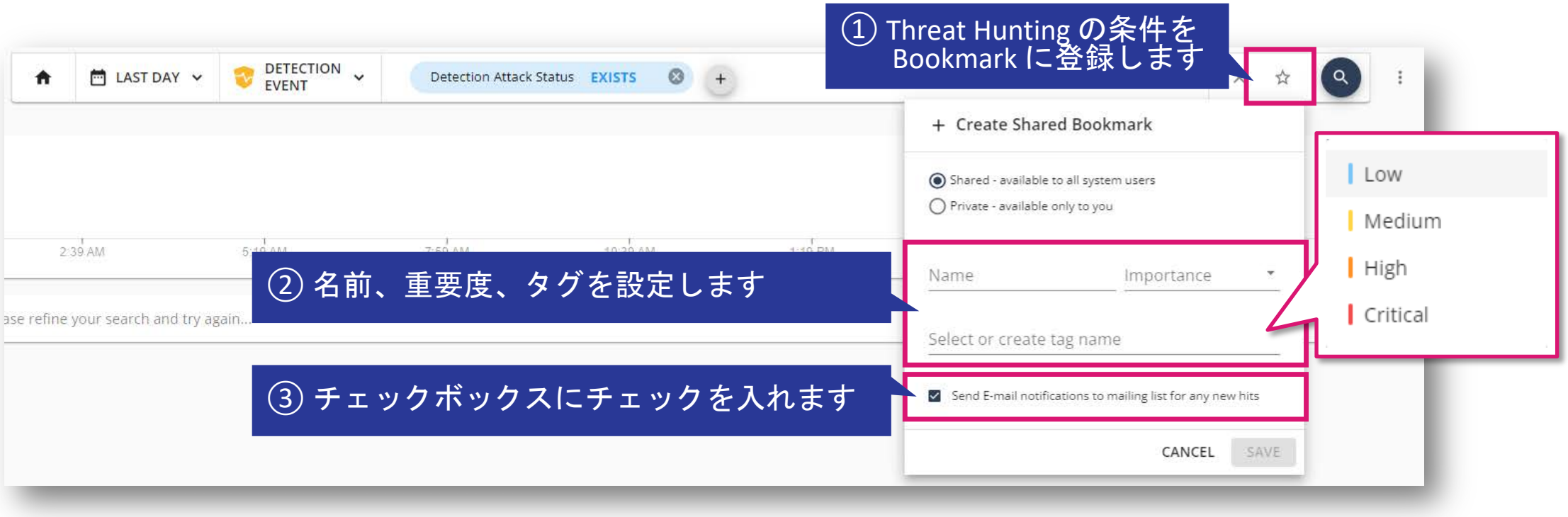
- Threat Hunting の Notifications に、アラートの通知先メールアドレスを設定します
- テナントの管理者からアラートの通知先を選択します



# アラート通知設定（3／4）：アラート通知イベント設定

Threat Hunting

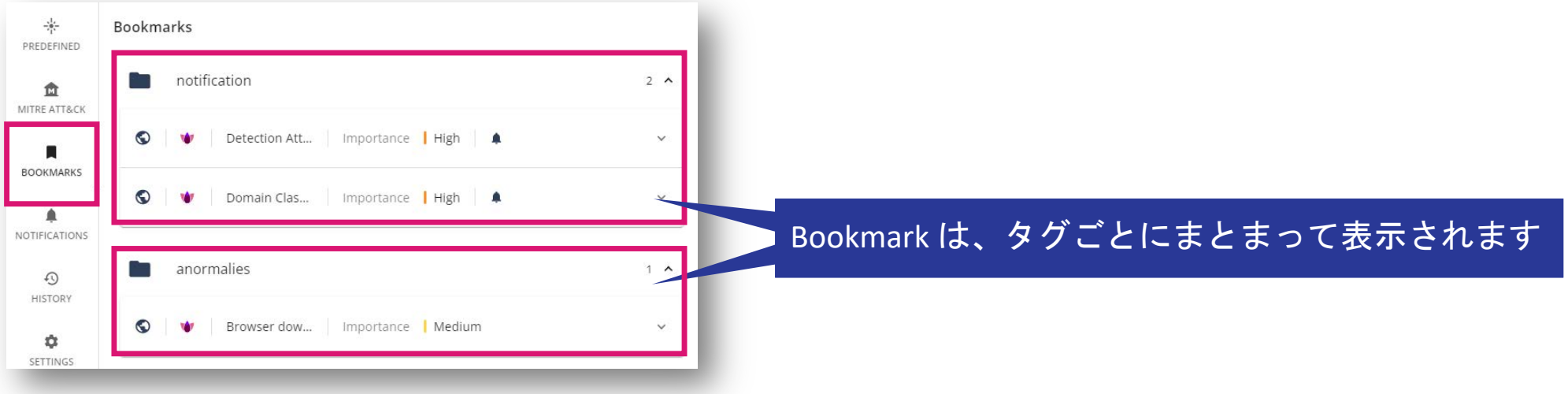
- 管理者に通知するイベントの条件を設定します
- 検索窓の ☆ マークをクリックし、検索条件を Bookmark に登録します
- Bookmark に登録された検索条件で定期的に Threat Hunting が行われます
- 検知した攻撃の状態（Detection Attack Status）や、検出したBlade（Detection Triggered by）、Severity（Detection Severity）などを検索条件に設定できます



# アラート通知設定（３／４）：アラート通知イベント設定

Threat Hunting

- Bookmark への登録時に「Tag」を設定すると、Bookmark がタグごとにまとめて表示されます



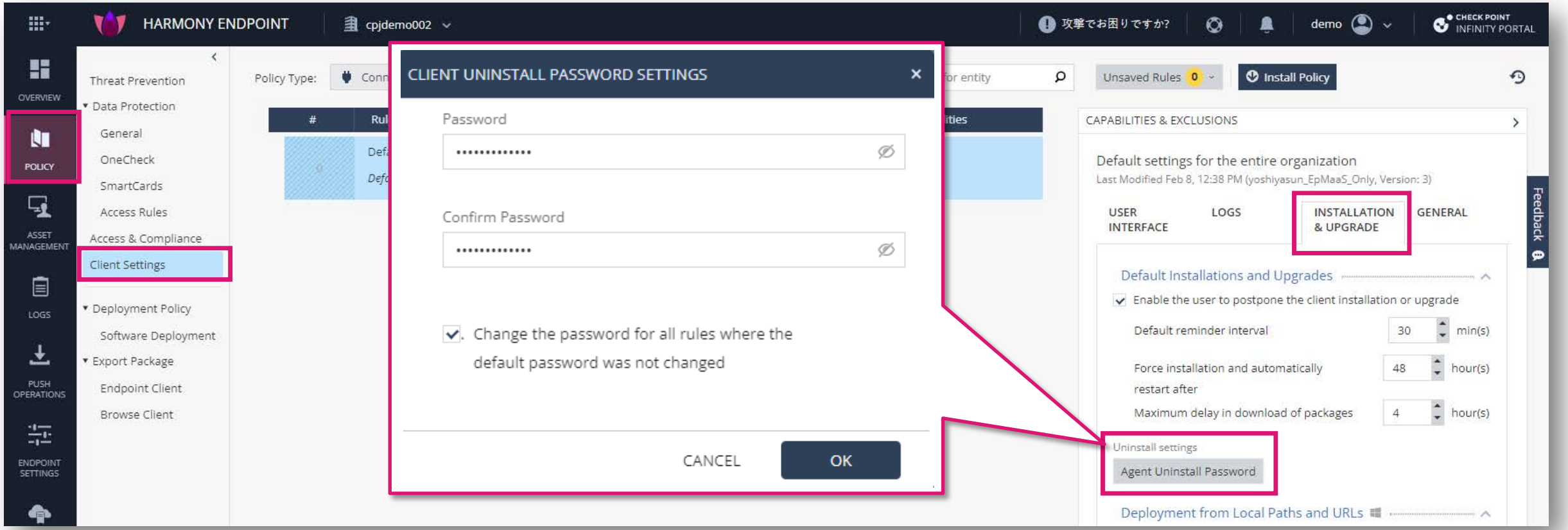
# アンインストールパスワードの設定

YOU DESERVE THE BEST SECURITY

# アンインストールパスワードの設定

Policy > Client Settings > Install & Upgrade > Uninstall Settings

- コンピュータの管理者がHarmony Endpointをアンインストールできない様に、アンインストールパスワードを設定します
- Push Operations でアンインストールをする場合は、アンインストールパスワードは不要です



# クライアントのアンインストール

YOU DESERVE THE BEST SECURITY

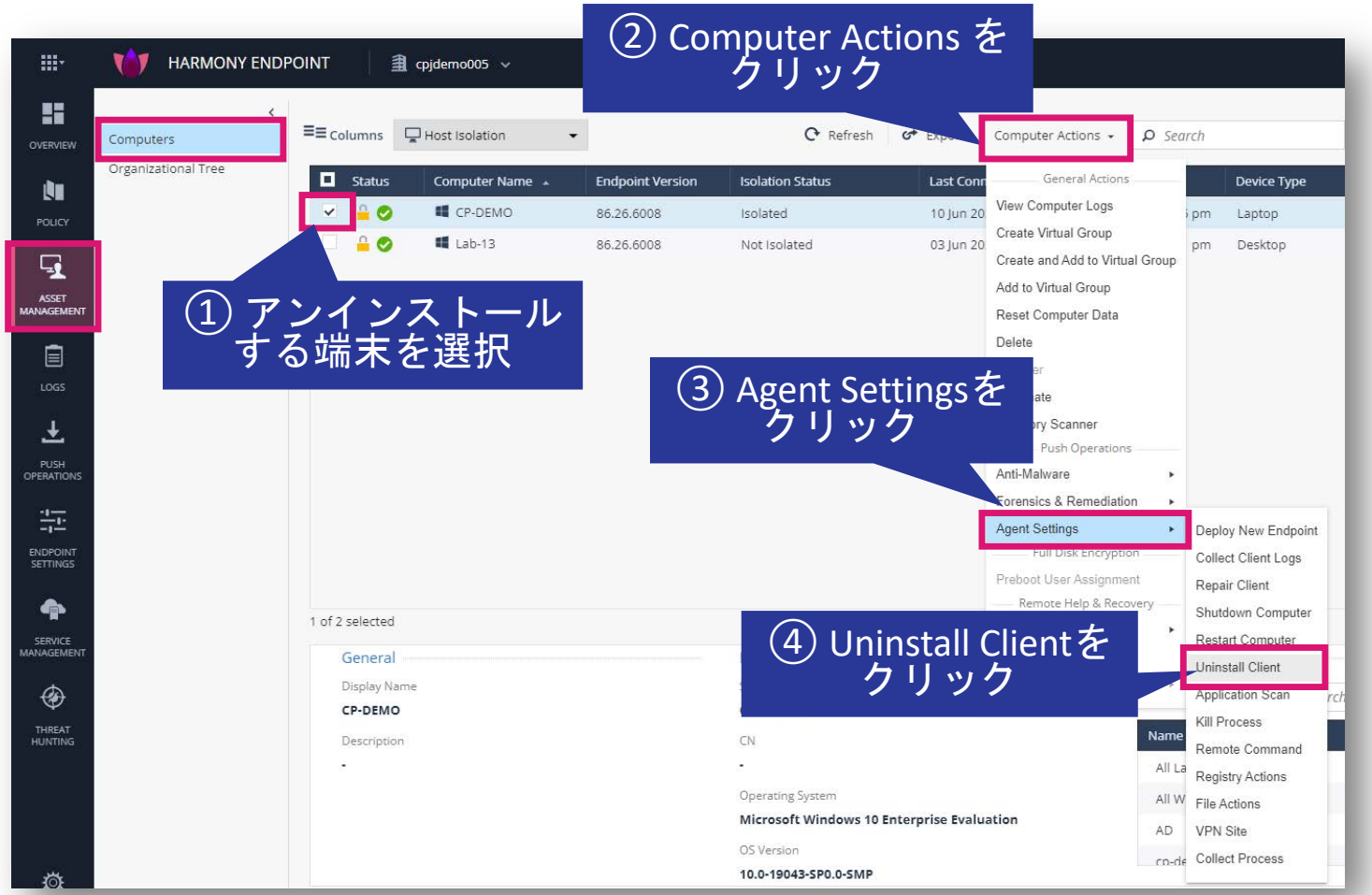
# PUSH OPERATIONS

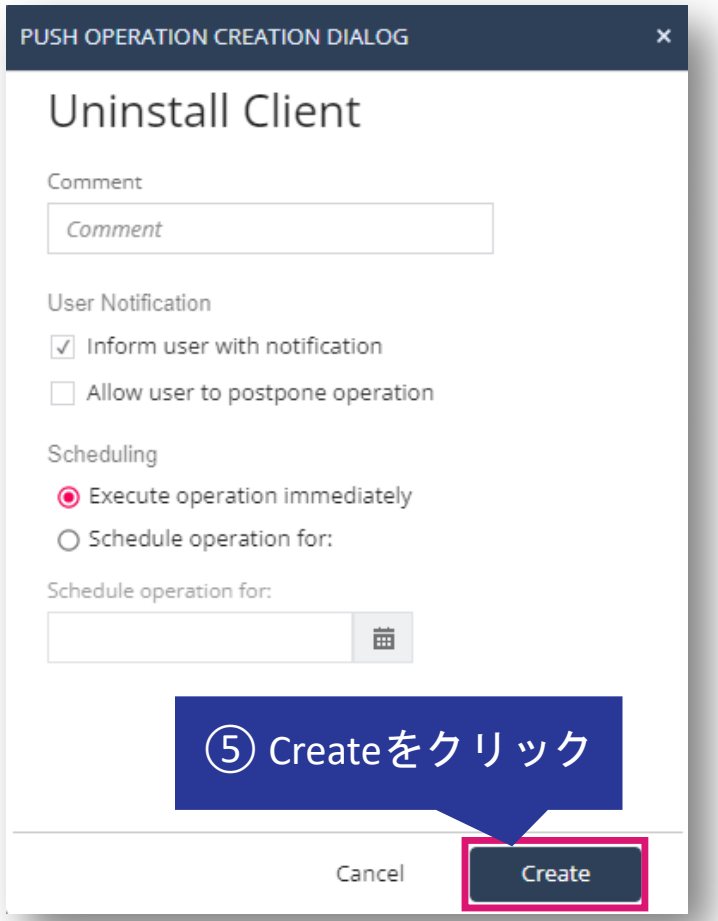
YOU DESERVE THE BEST SECURITY

# Asset Magement 画面からのアンインストール

Asset Management > Computers > Computer Actions > Agent Settings > Uninstall Client

- リモートからクライアントソフトウェアをアンインストールできます。

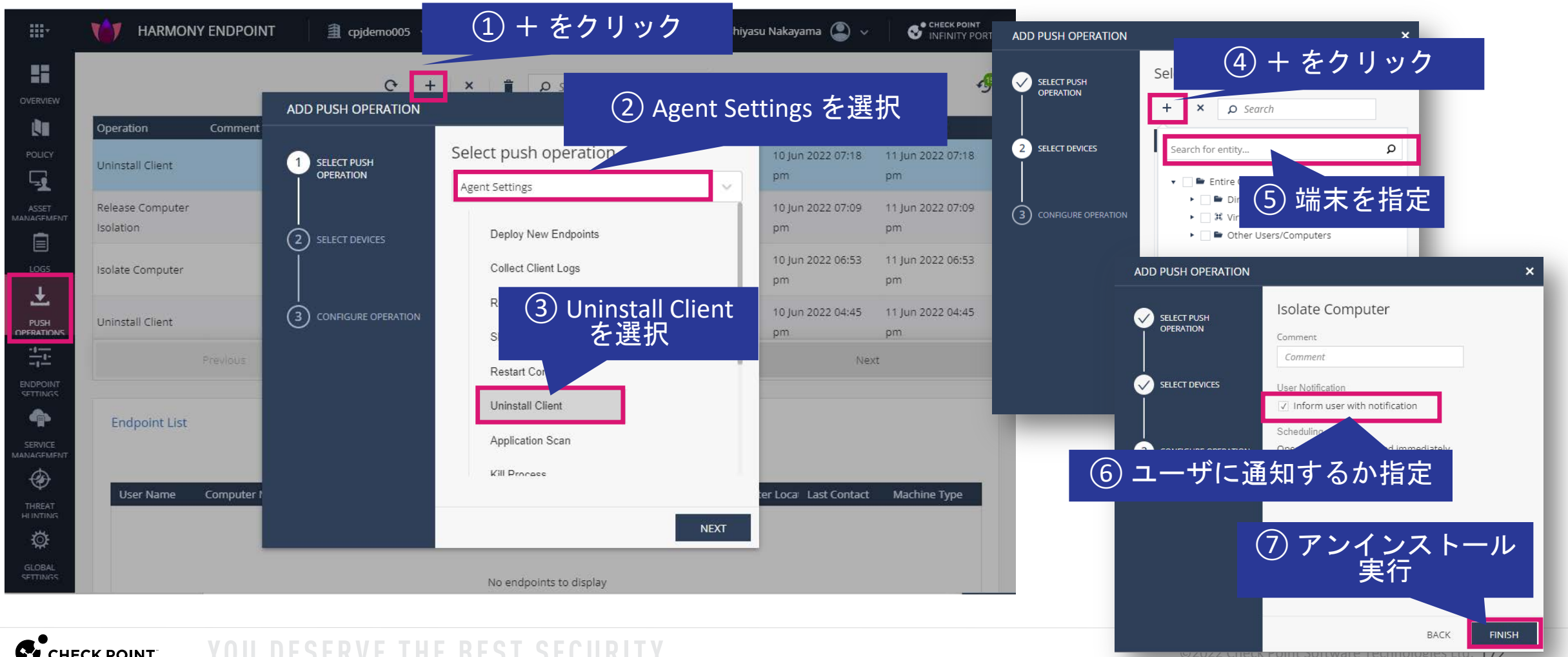


# Push Operations 画面からのアンインストール

Push Operations

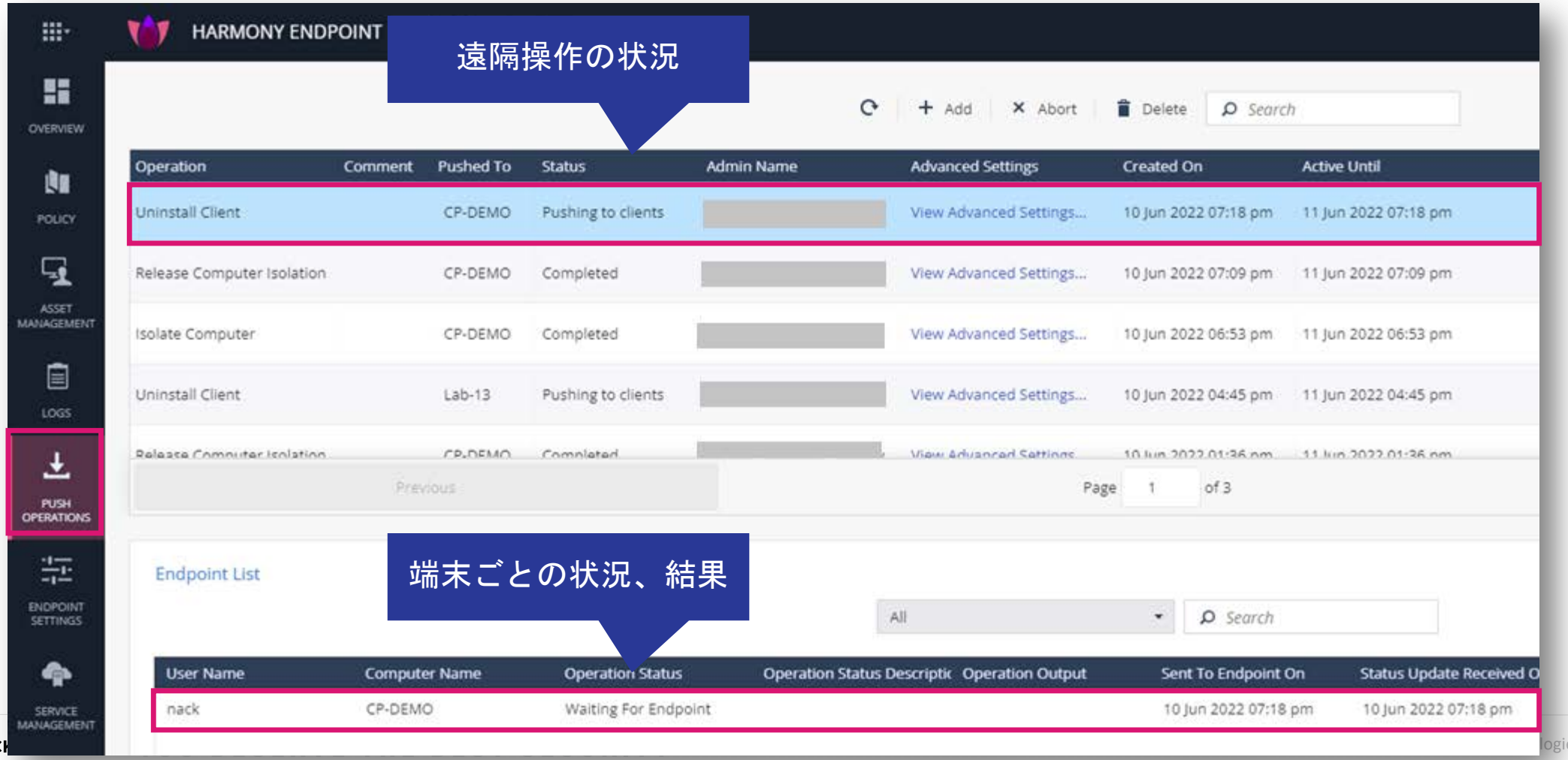
- リモートから端末のクライアントソフトウェアをアンインストールできます。



# 遠隔操作の状況確認

Push Operations

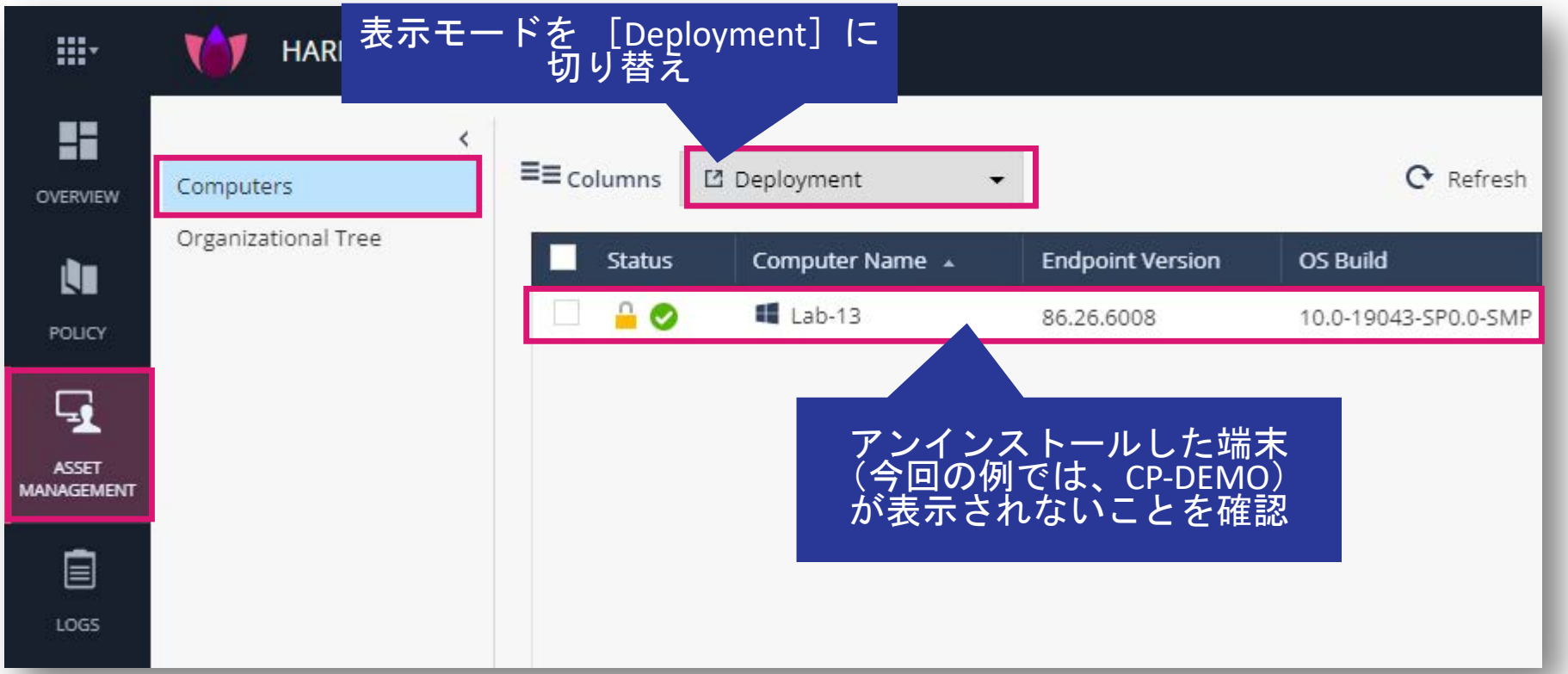
- Push Operations で遠隔操作の状況を確認



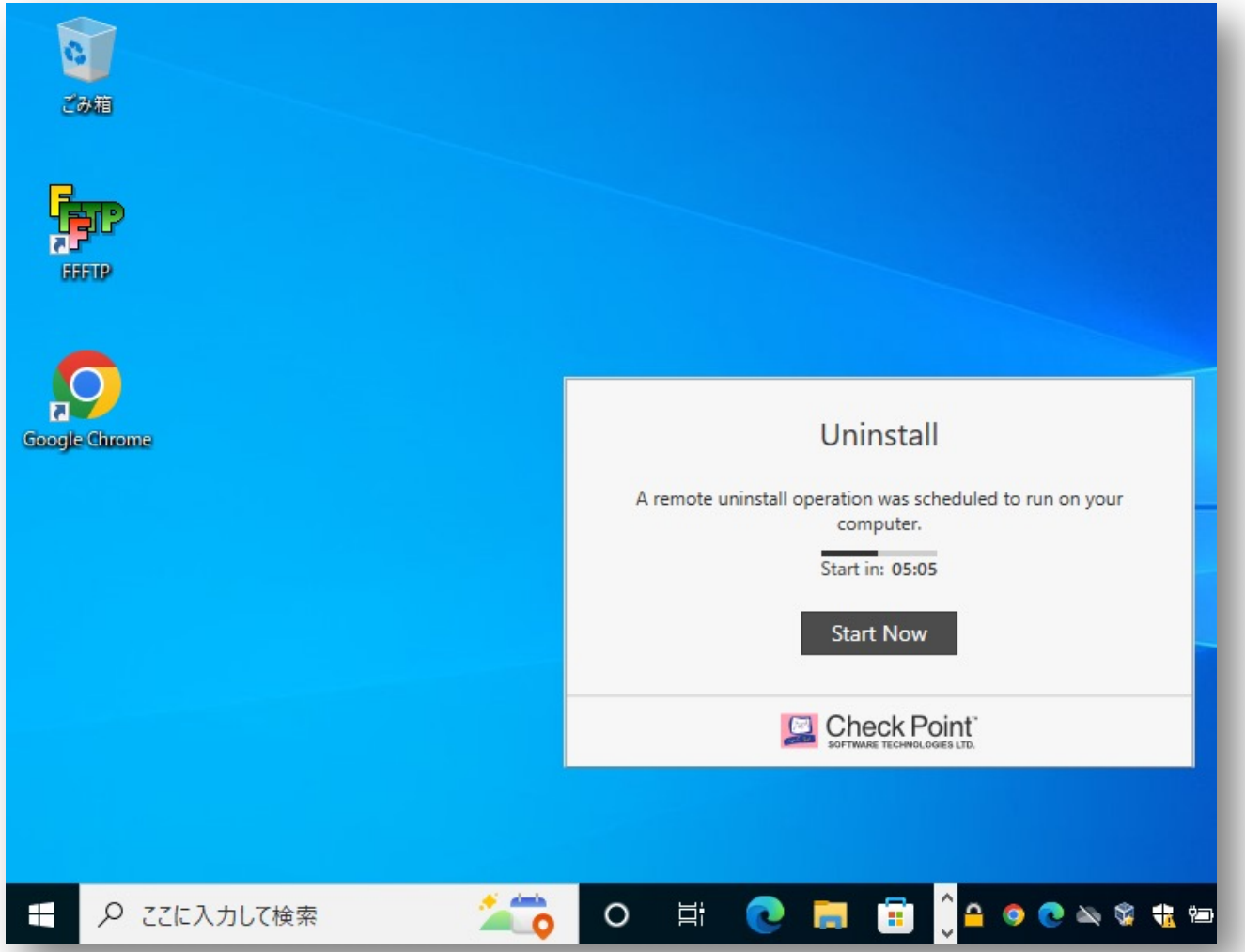
# Asset Management 画面での端末の状況確認

Asset Management > Computers

- Host Isolation 表示に切り替えることで、端末の隔離状況を表示可能



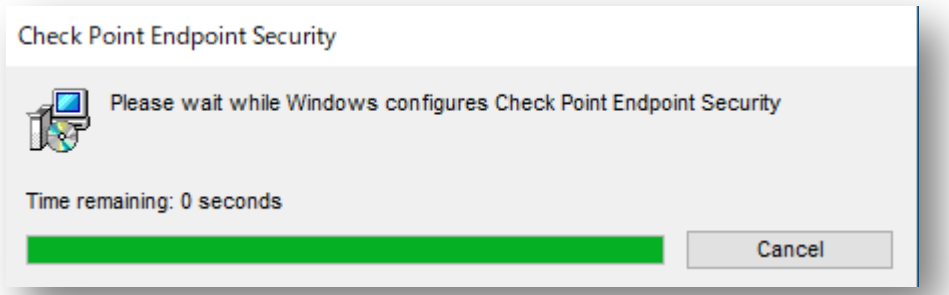
# ＜参考＞クライアントへの通知画面



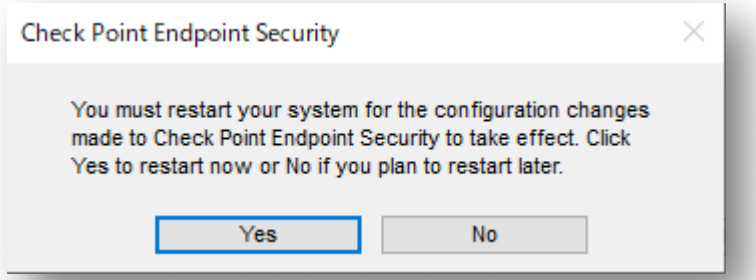
# クライアントアンインストール時の注意事項

- 再起動を促すダイアログボックスが表示されるまで、パソコンのシャットダウンや再起動などを行わないでください

**ダイアログボックス-1**




**ダイアログボックス-2**



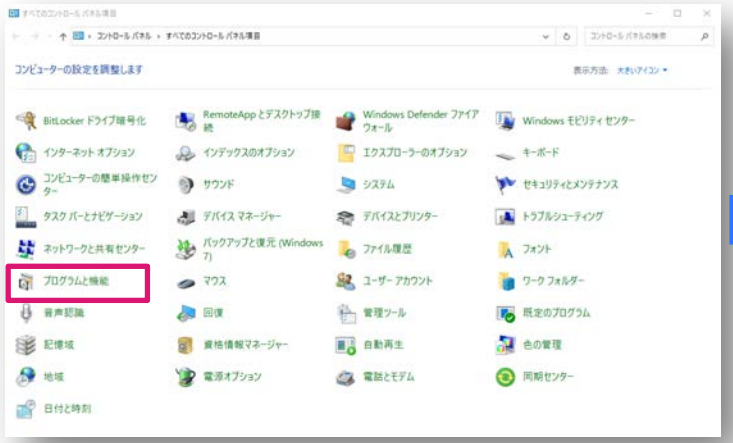
# コントロールパネル

YOU DESERVE THE BEST SECURITY

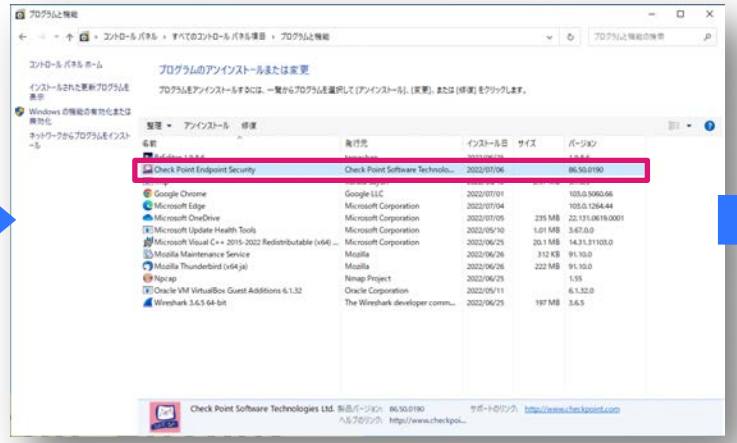
# コントロールパネルからのアンインストール

- コントロールパネルの「プログラムと機能」を開きます
- 「Check Point Endpoint Security」を選択して、「アンインストール」をクリックします
- アンインストールパスワードを入力ます
- 再起動を促すダイアログボックスが表示されたら、Yes を押して再起動してください

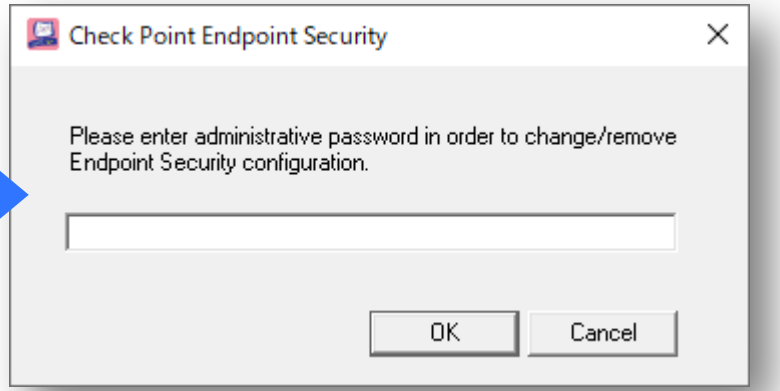
**コントロールパネル**



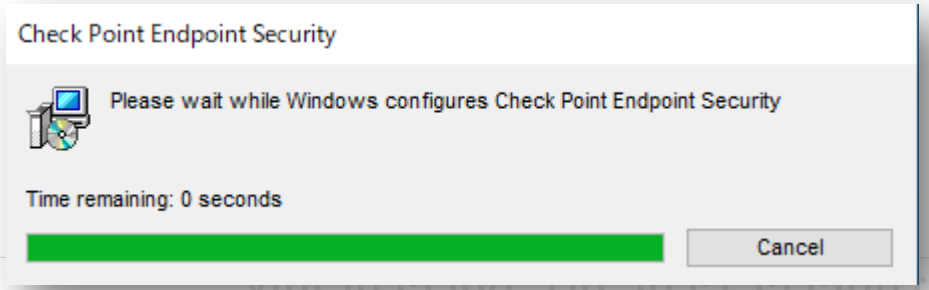
**プログラムと機能**



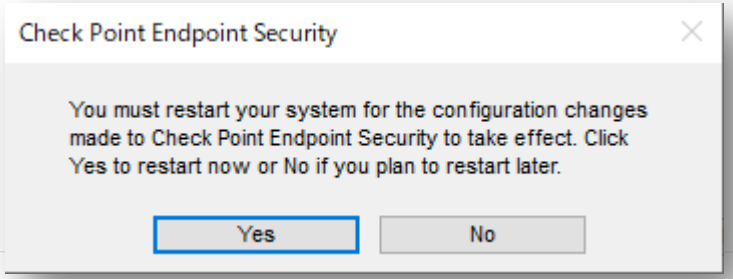
**アンインストールパスワード**




**ダイアログボックス-1**

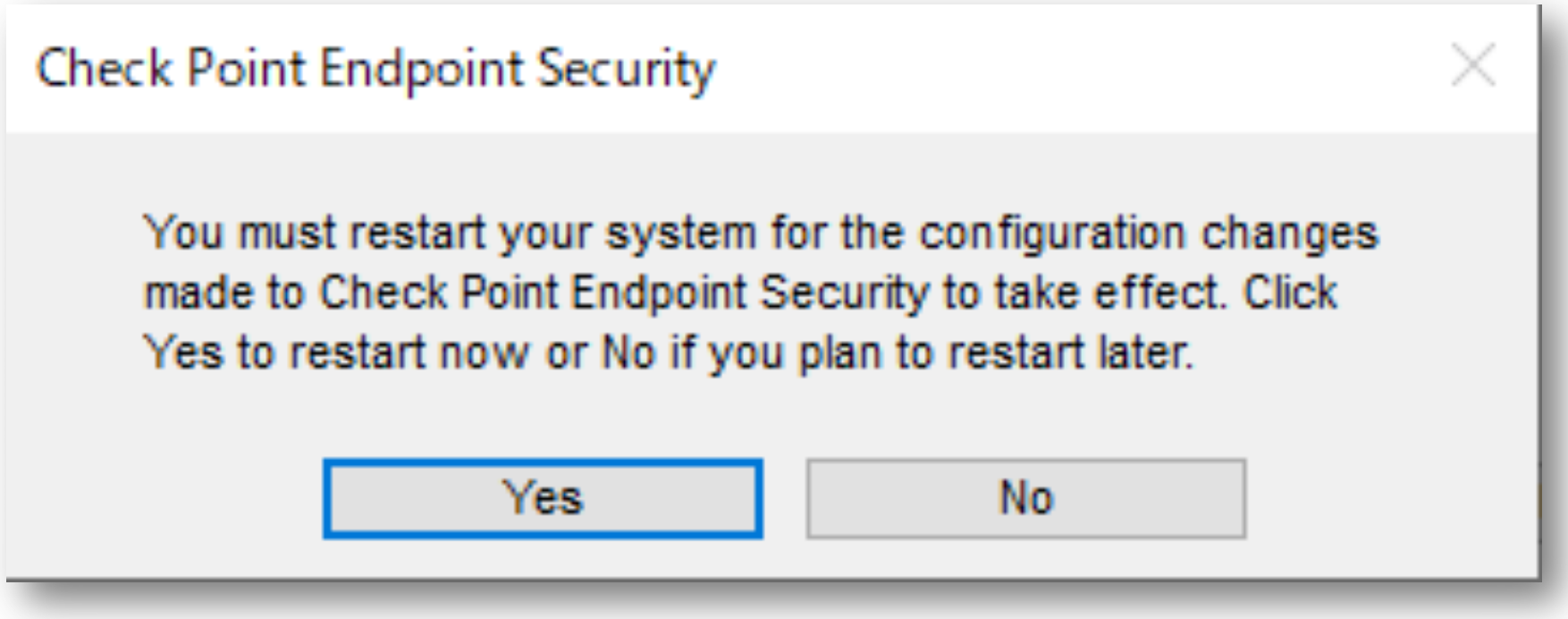



**ダイアログボックス-2**



# クライアントアンインストール時の注意事項

- 再起動を促すダイアログボックスが表示されるまで、パソコンのシャットダウンや再起動などを行わないでください




CHECK POINT™
Thank You
YOU DESERVE THE BEST SECURITY