HARMONY ENDPOINT
簡易設定ガイド

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

- 本ドキュメントは、検証、ハンズオン研修等での利用を目的としているため、一部の設定手順のみを記載しています。
- 本番環境の設定は、Administration Guide 等に基づいて行ってください。
- 本手順書と、Administration Guide、SK等の記述内容が異なる場合は、原則、本手順書以外のドキュメントの内容が優先されます。
- 本手順書は、一部を除き、2022年3月現在の設定内容、UI に基づいて作成されています。

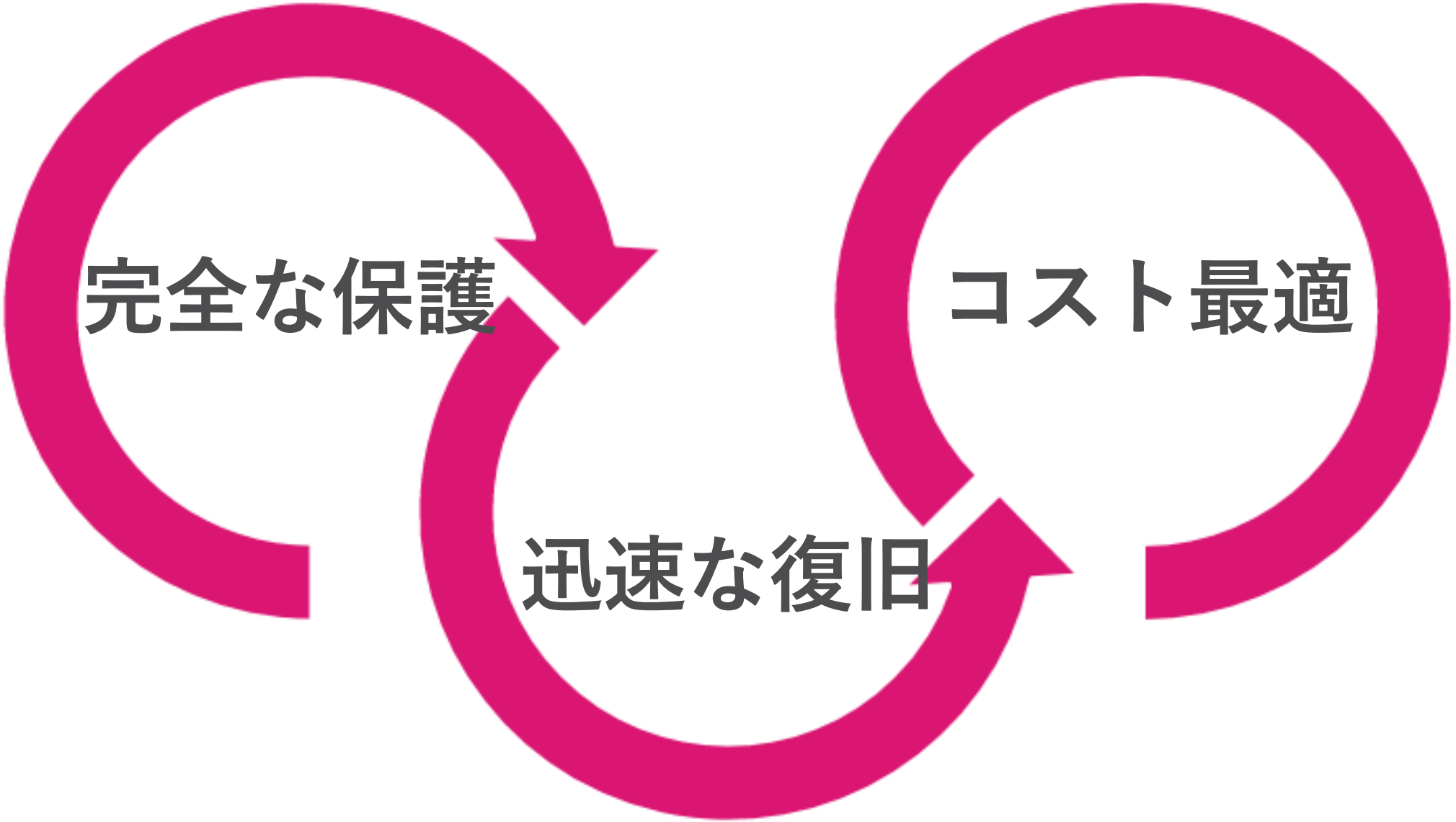
YOU DESERVE THE BEST SECURITY

Table of Contents

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

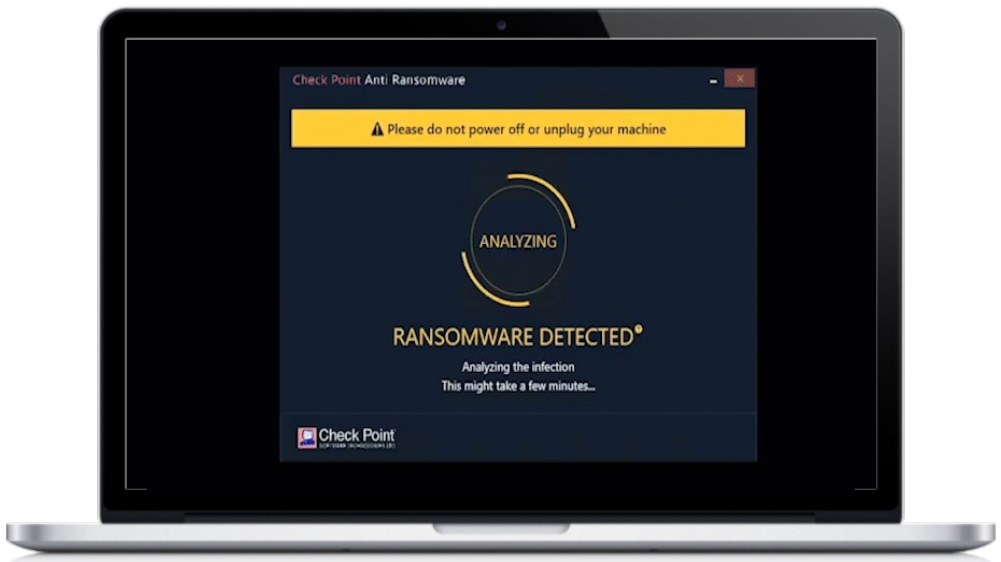
アンチ・ボット

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

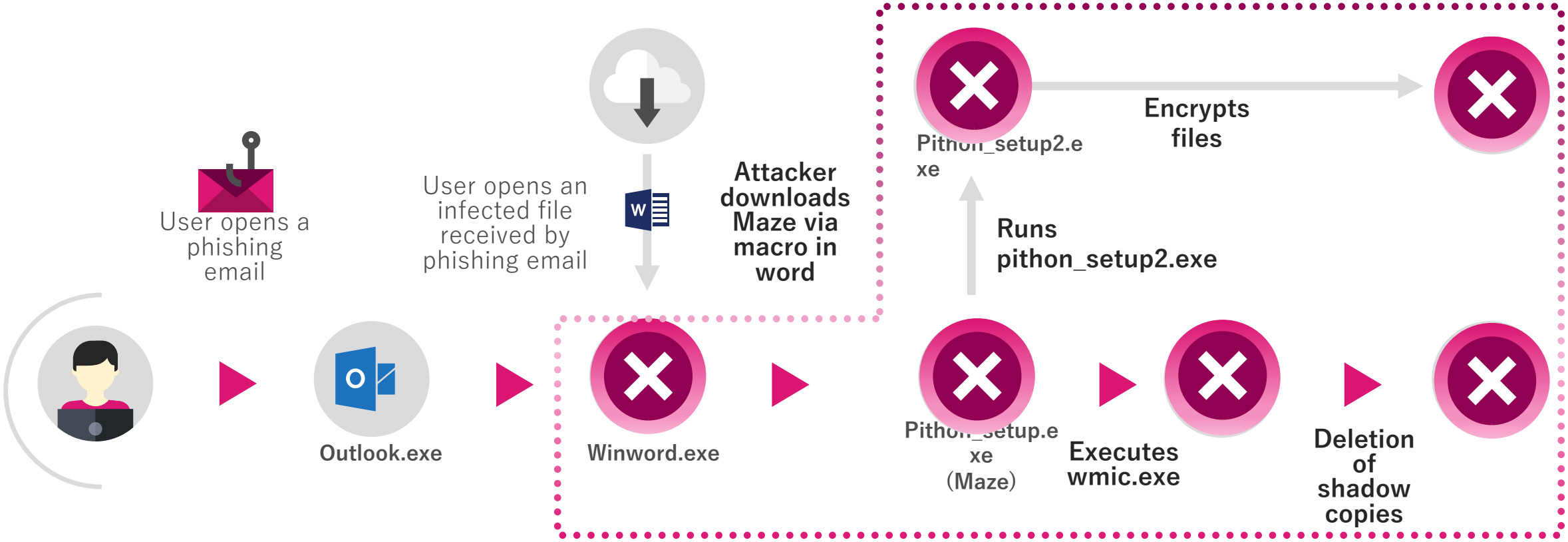
検知、調査、修復作業の 90% を自動化



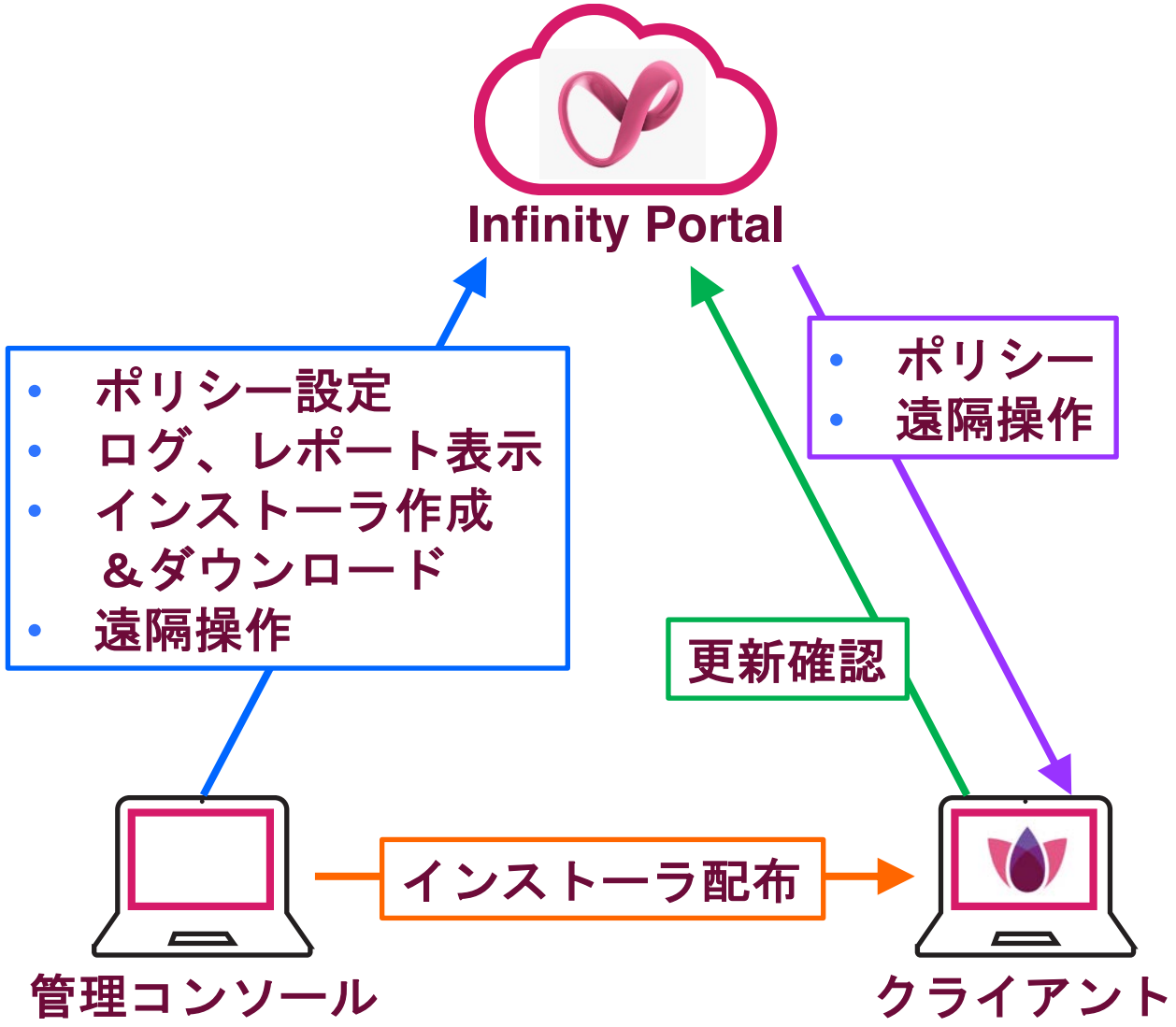
自動化

- 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 の構成概要



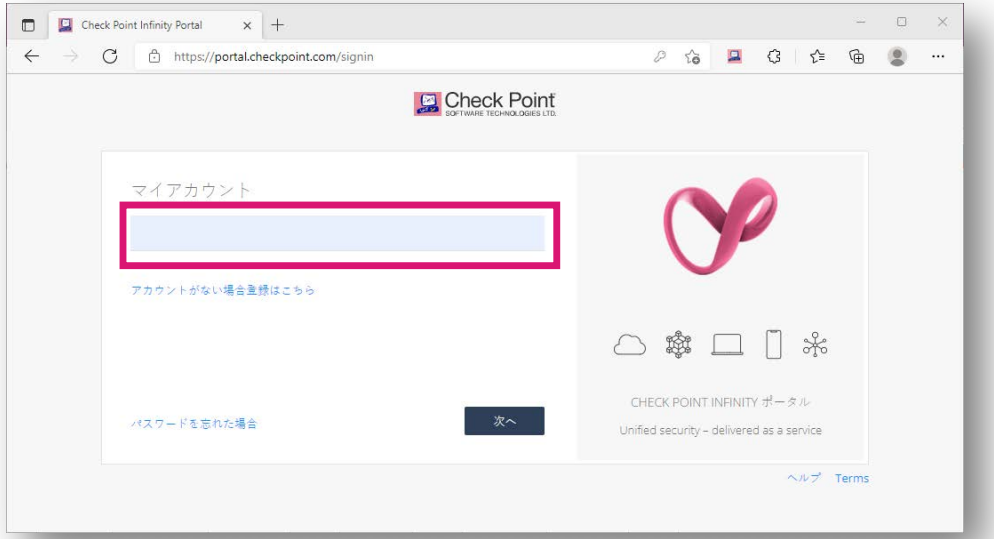
1. **Infinity Portal**
   - クラウド上の管理サーバ
   - セキュリティポリシーの設定や、ログ、レポートの確認などを実施

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

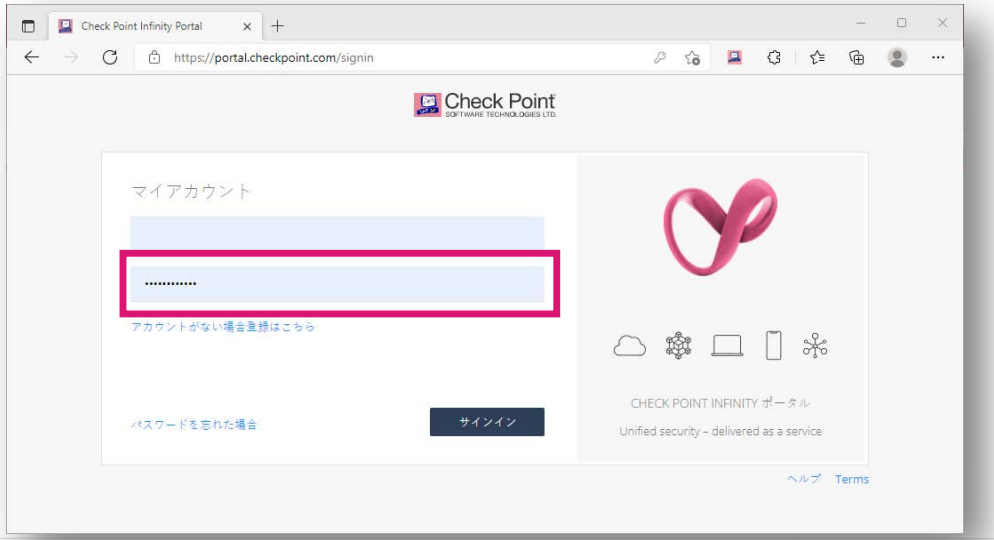
INFINITY PORTAL へのサインイン

Infinity Portal へのサインイン（１／２）



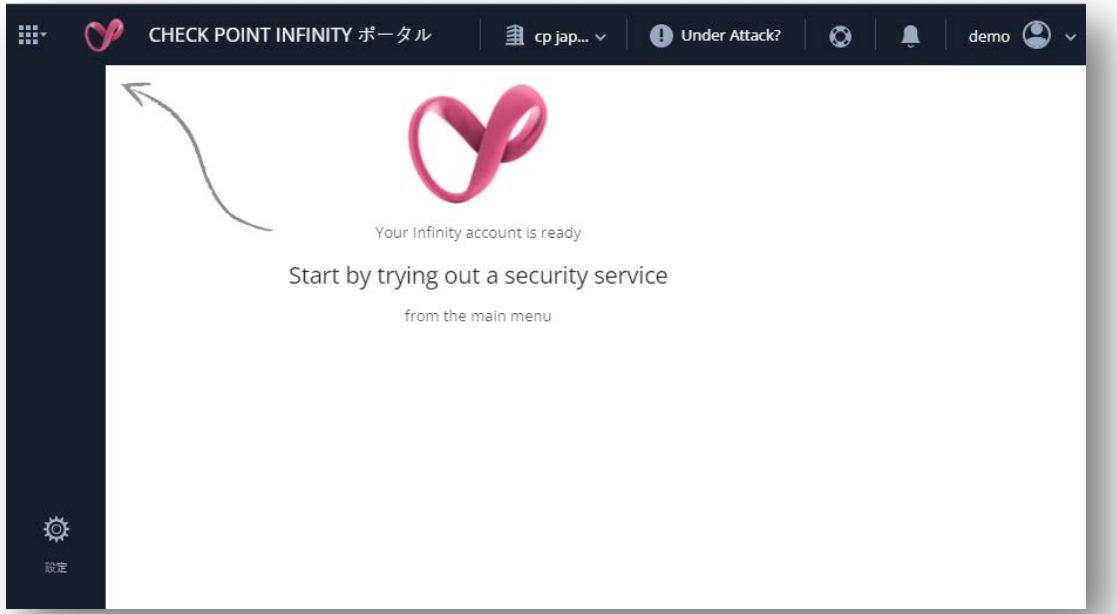
1. Infinity Portal へ接続する
   - URL: https://portal.checkpoint.com/

2. ユーザ名を入力して、「次へ」を押す



3. パスワードを入力して、「サインイン」を押す

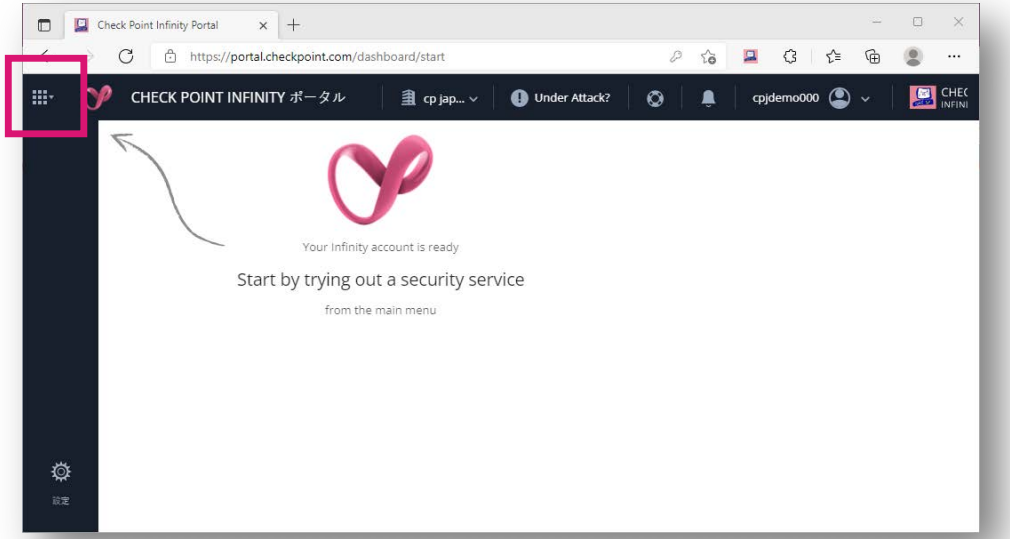
Infinity Portal へのサインイン（２／２）



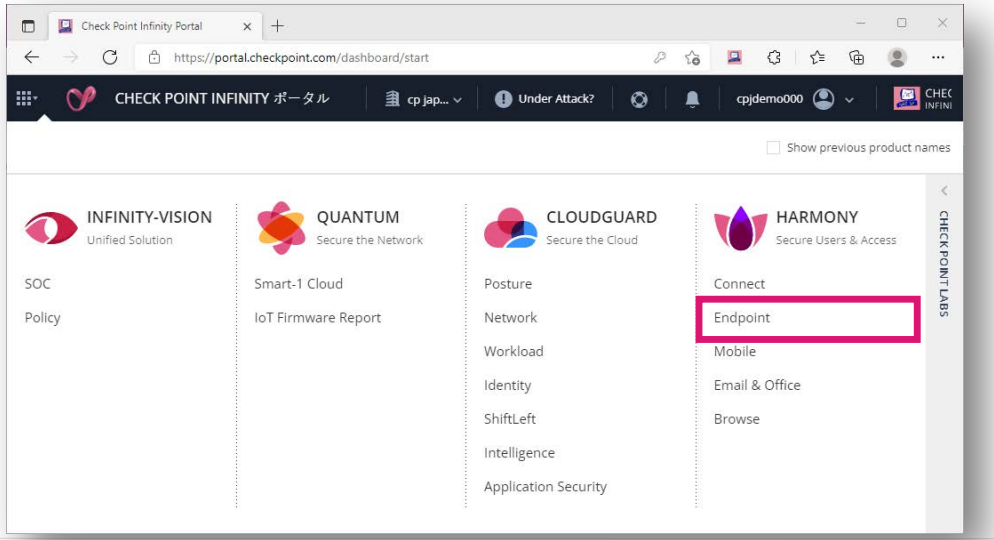
4. サインイン成功

HARMONY ENDPOINT の有効化

Harmony Endpoint の有効化（1／3）

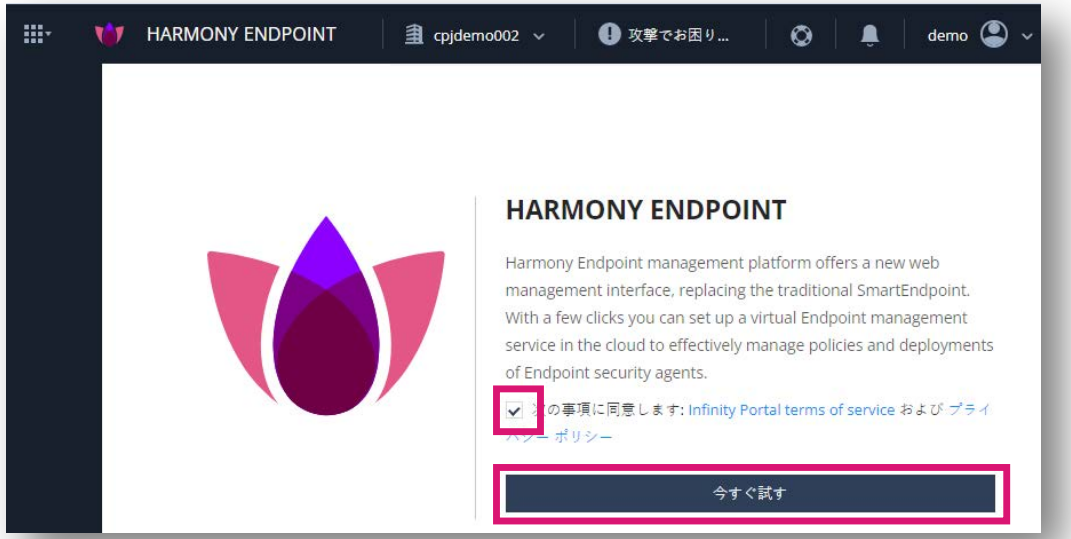


1. 左上のメニューボタン  を押す

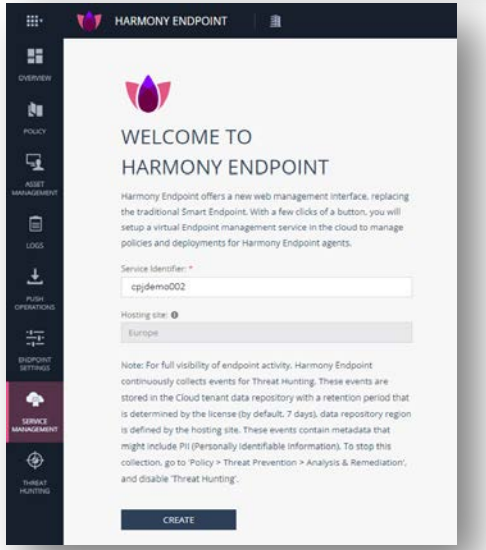


2. 「HARMONY Endpoint」を選択する

Harmony Endpoint の有効化（２／３）

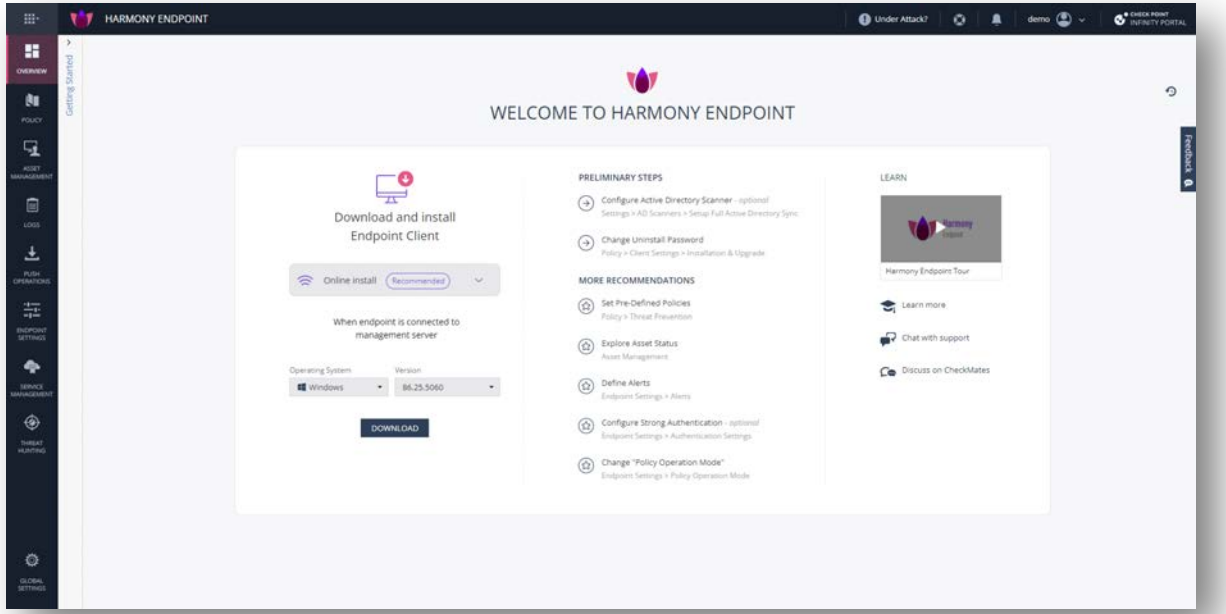


3. Infinity Portal terms of service、個人情報保護方針を確認し、「契約事項に同意する」のチェックボックスにチェックを入れ、「いますぐ試す」を押す



4. 「CREATE」を押す

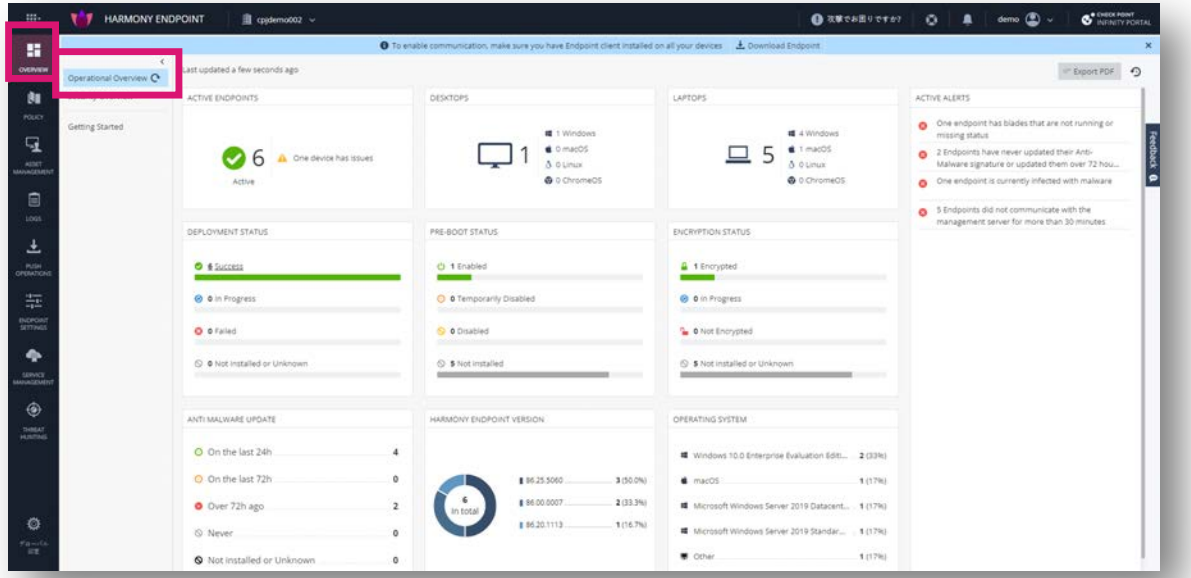
Harmony Endpoint の有効化（3／3）



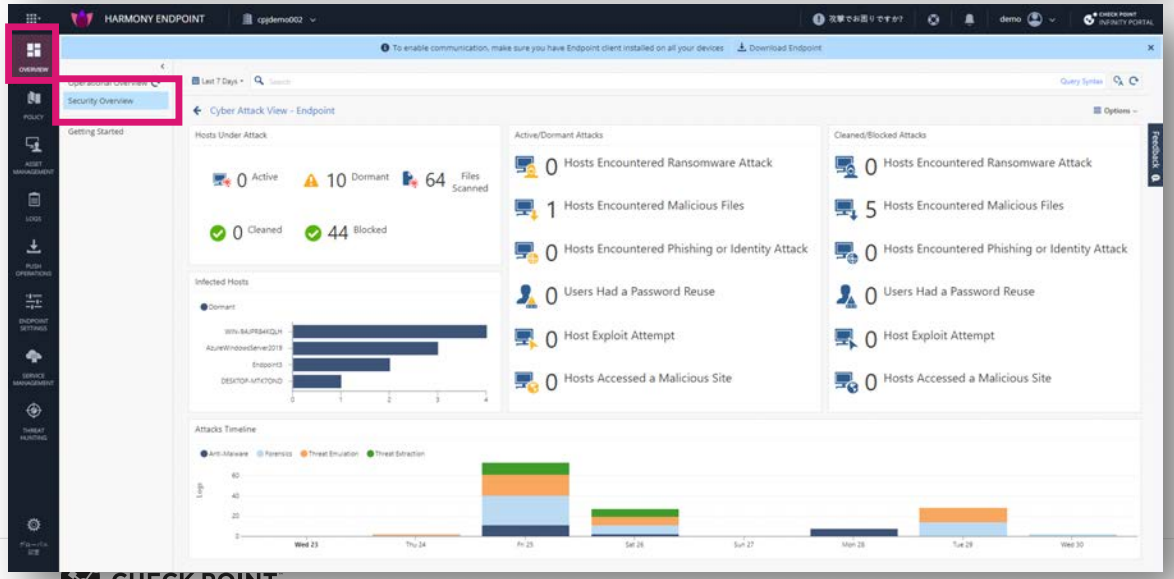
5. HARMONY Endpoint の有効化が完了

設定画面の概要

Overview ページ

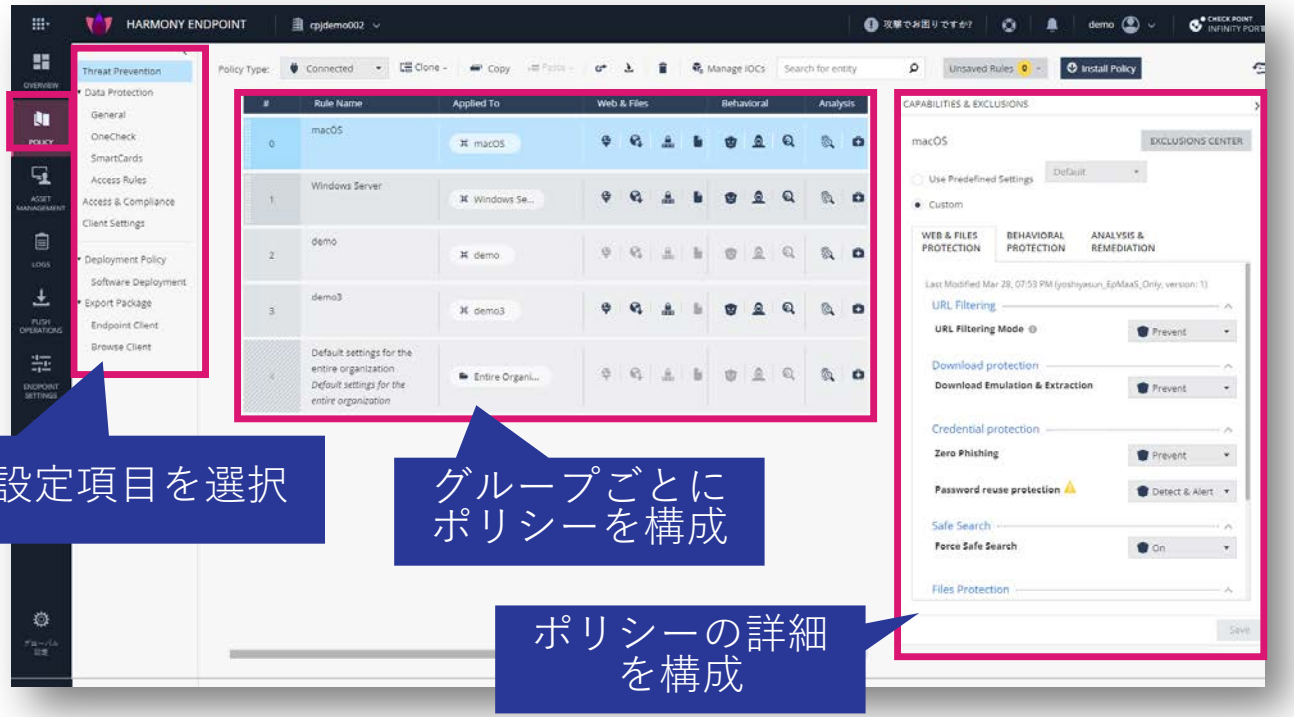


- Operational Overview
  - 組織内のエンドポイントクライアントの展開ステータス、それらのヘルスステータス、クライアントバージョン、およびクライアント上のオペレーティングシステムを表示します



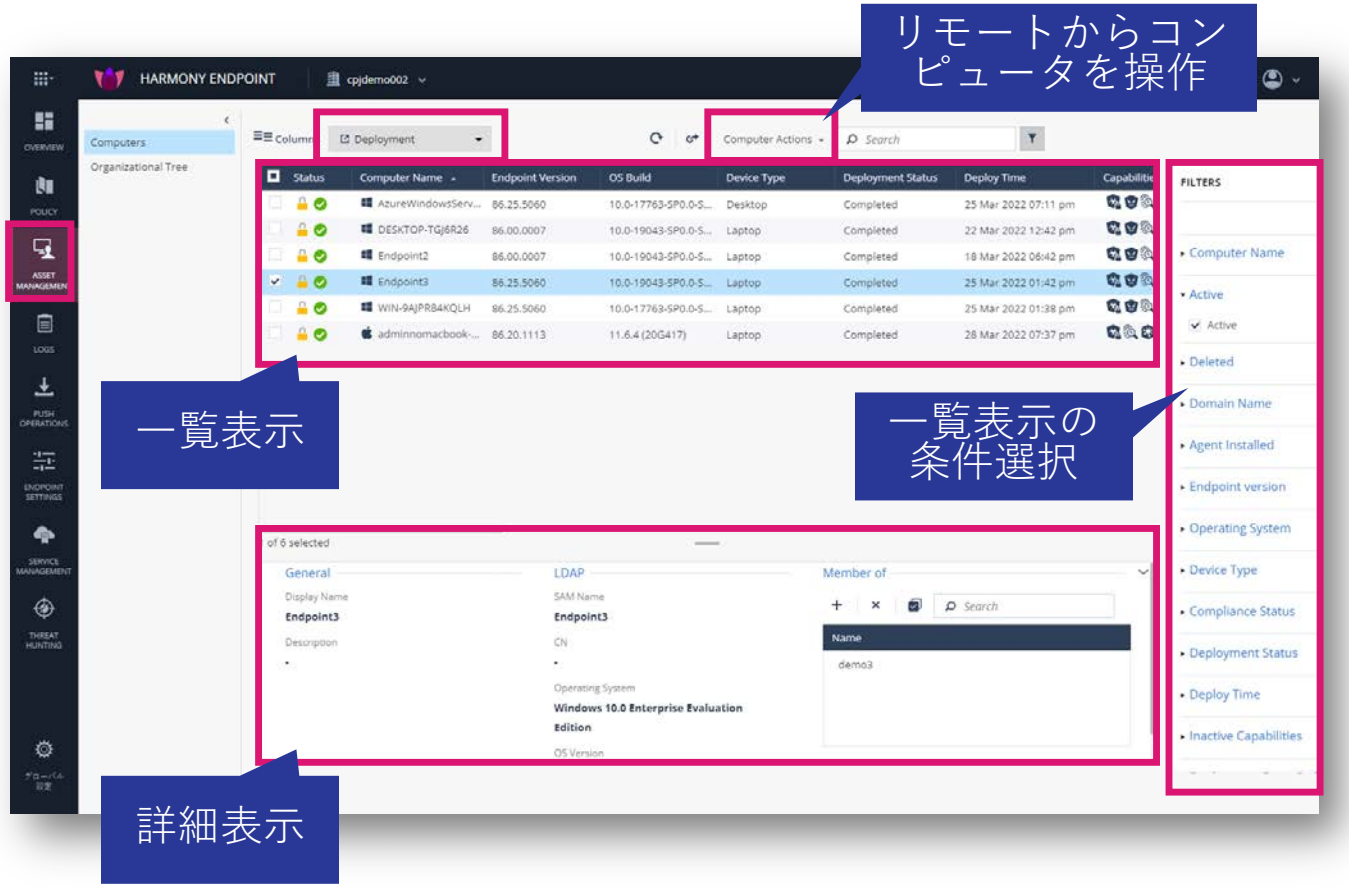
- Security Overview
  - エンドポイントクライアントへの攻撃統計を表示します

Policy ページ



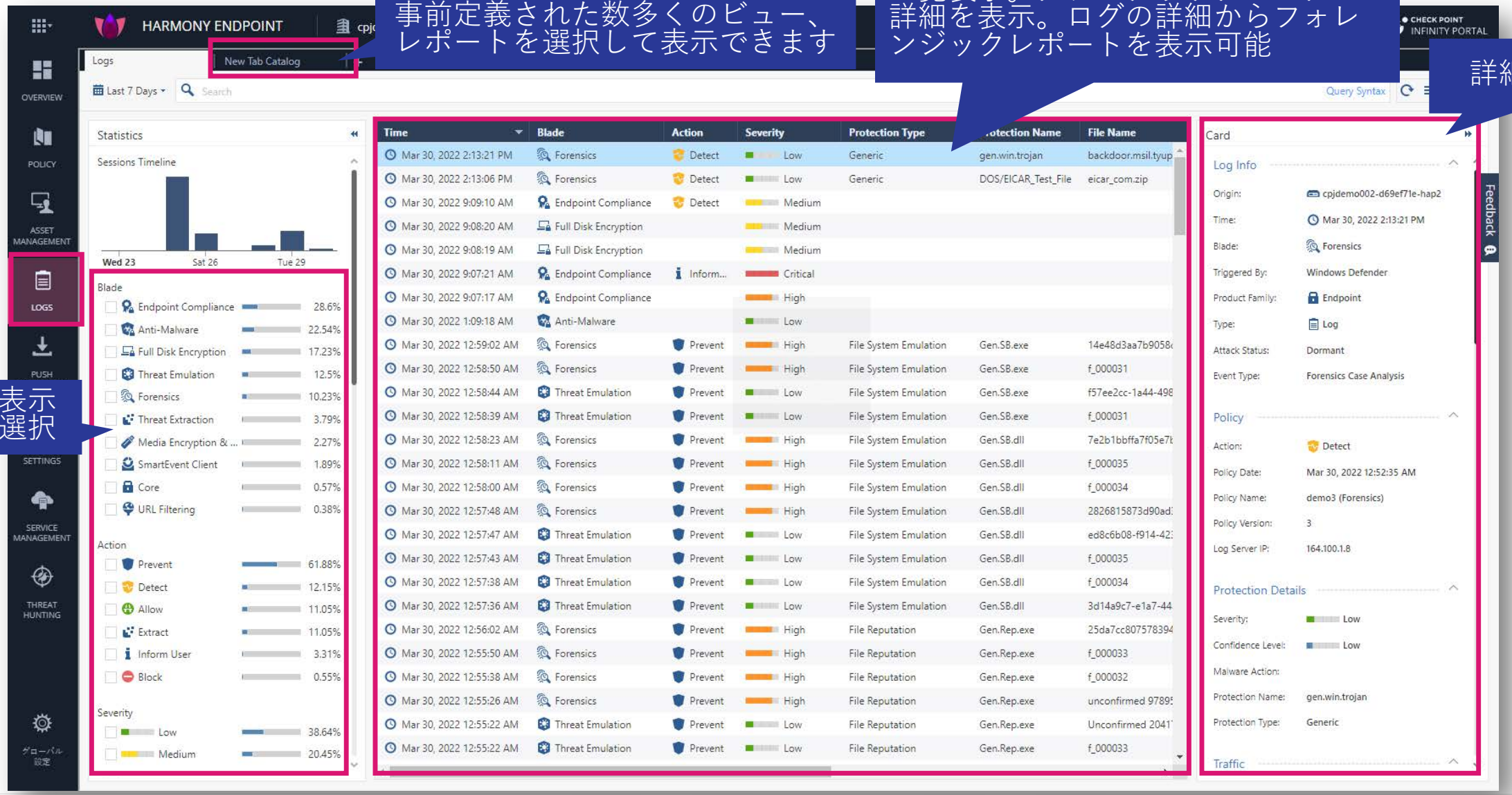
- セキュリティポリシーを構成します
  - 脅威の防止
  - データ保護
  - アクセスとコンプライアンス
- クライアントソフトウェアの設定を構成します
  - ユーザインタフェース
  - ログ
  - インストールとアップグレード
    - アンインストールパスワード
- エンドポイントクライアントソフトウェアの設定を構成します

Asset Management ページ

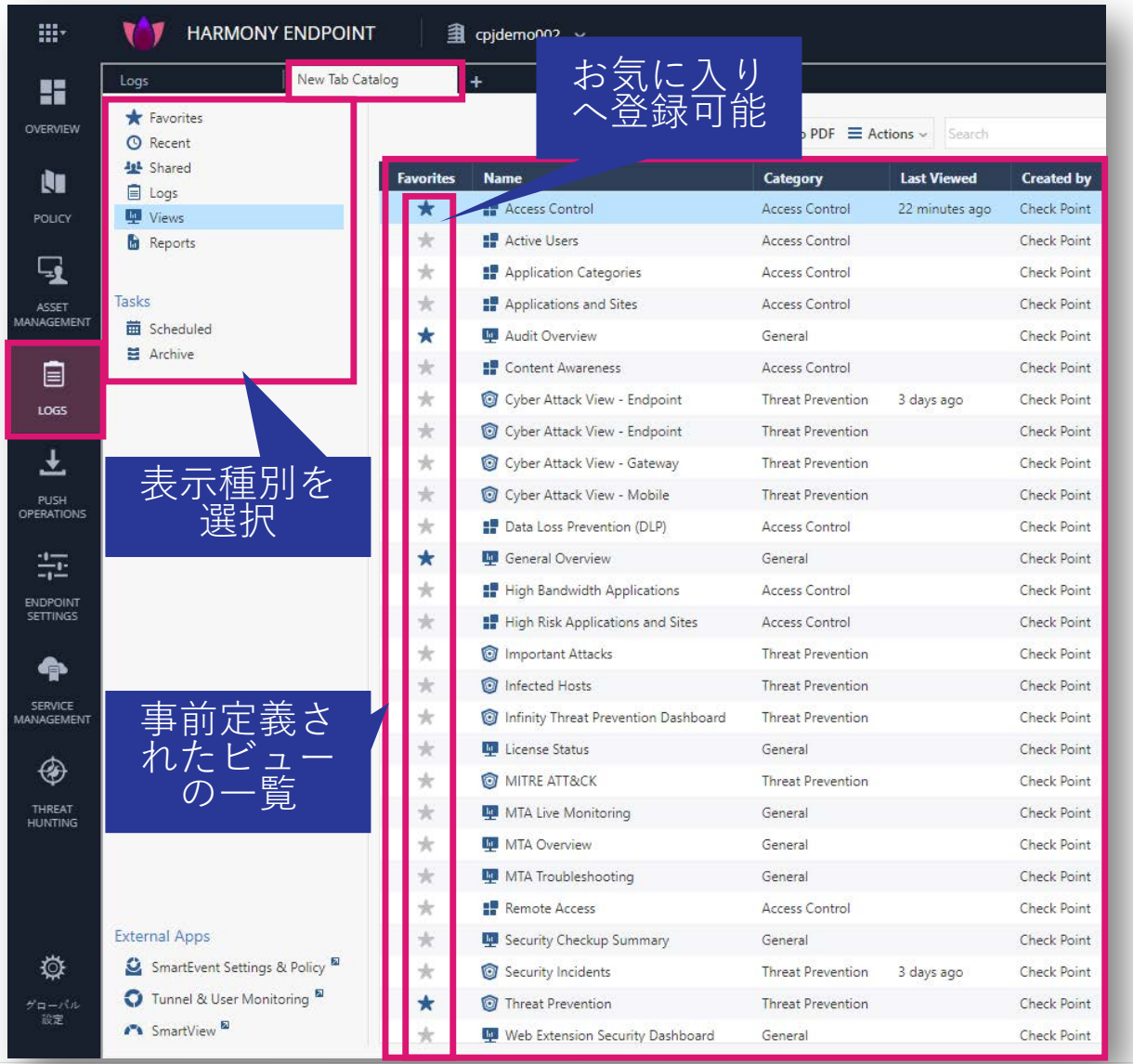


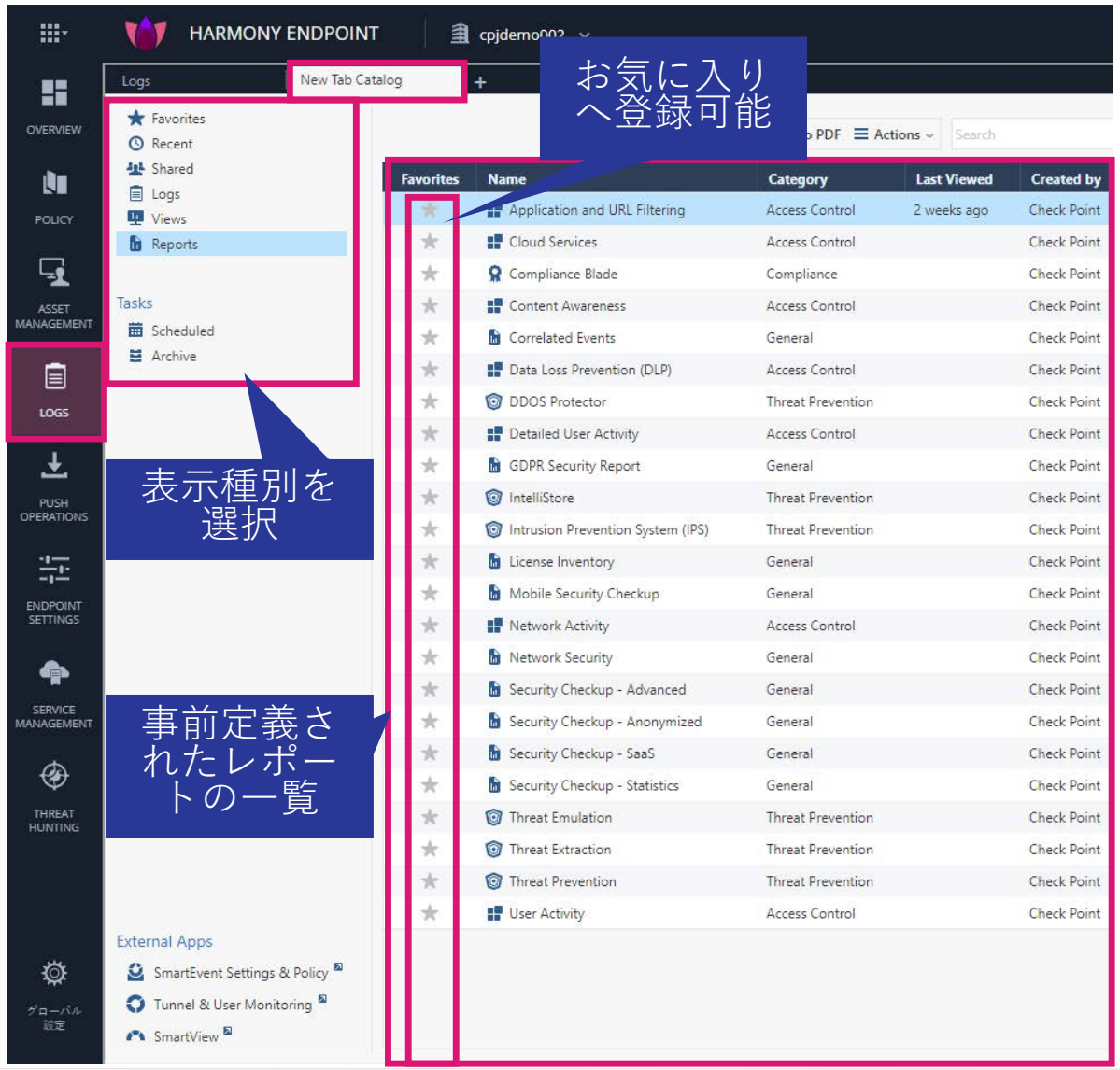
- 展開ステータス、コンピューター上のアクティブなコンポーネント、コンピューターにインストールされているクライアントバージョンなど、各コンピューターに関する情報が表示されます
- 事前構成されたビューを選択して表示します
  - 展開
  - コンプライアンス
  - ヘルス
  - フルディスク暗号化
  - マルウェア対策
  - ホストの隔離
  - カスタム（必要な列を選択）

Logsページ（1／2）

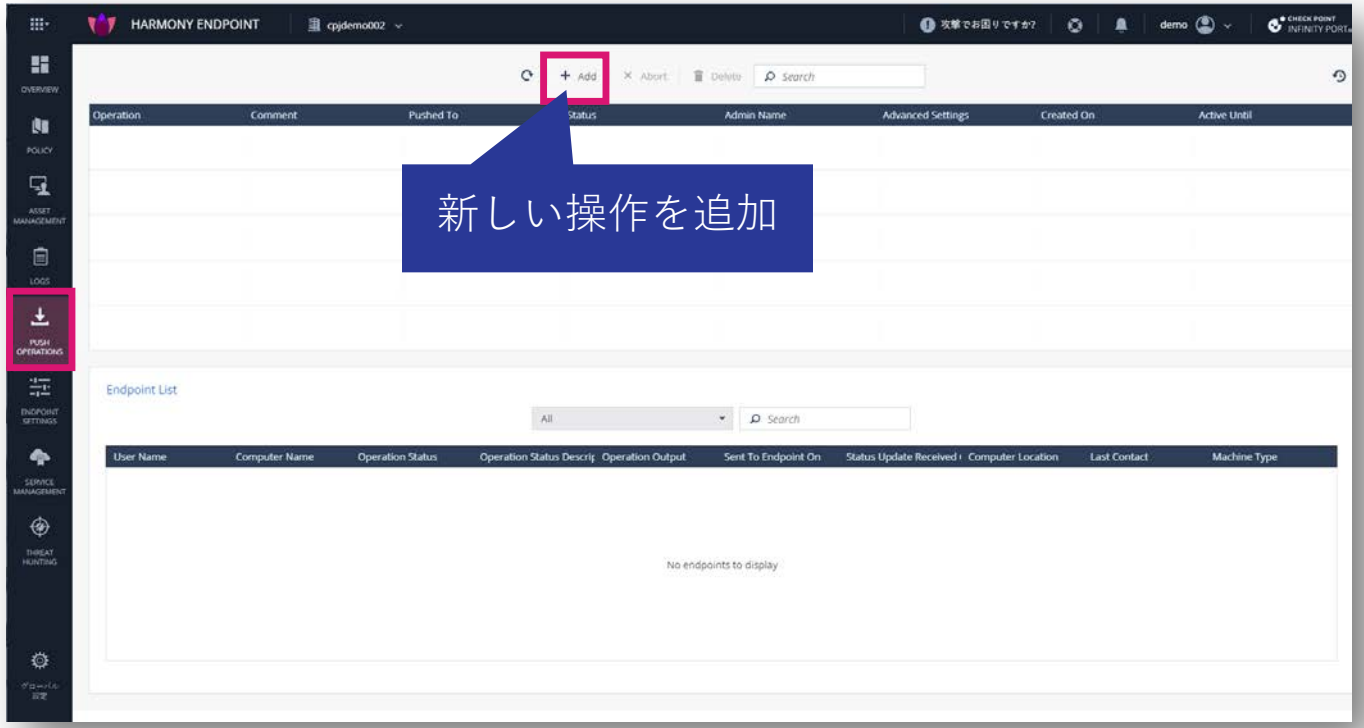


Logsページ（2／2）



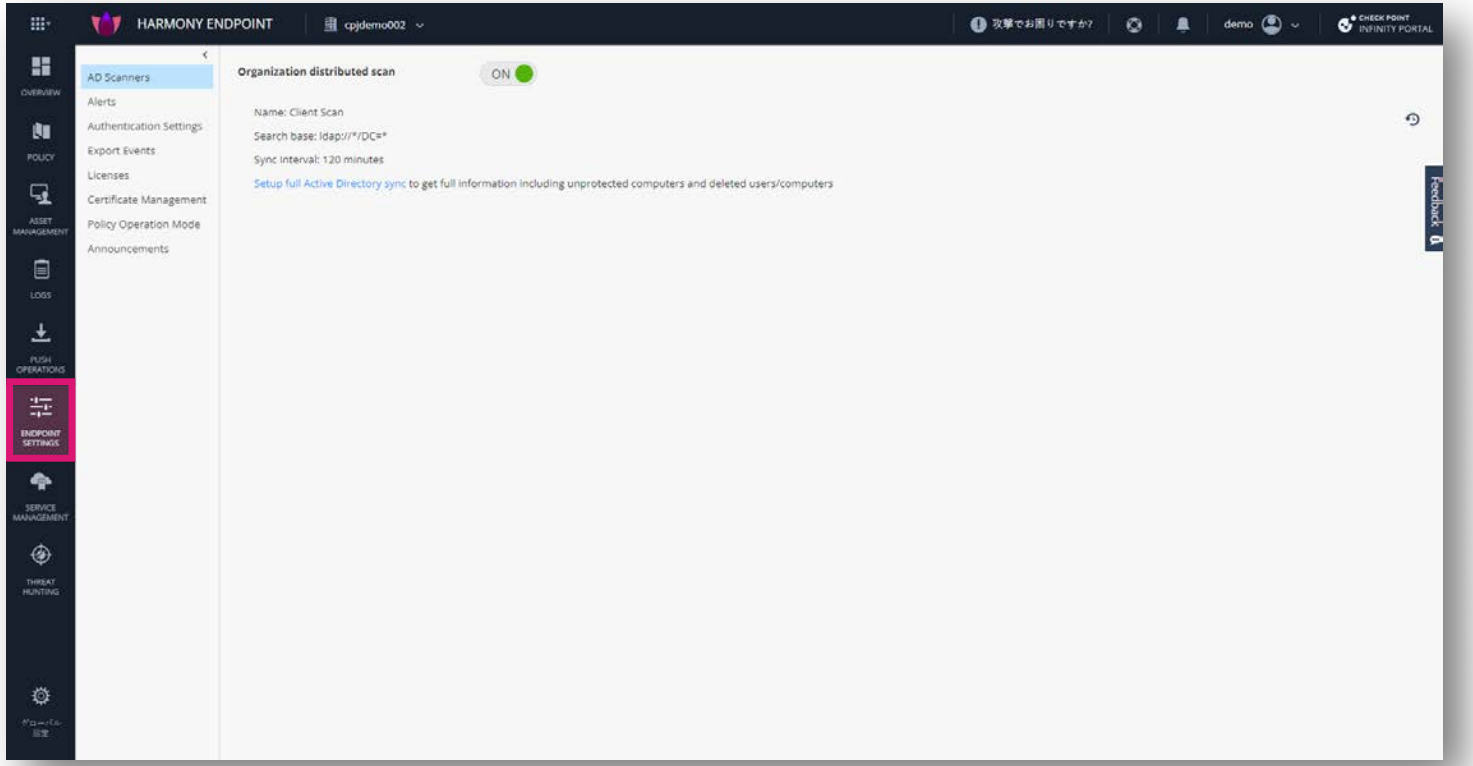


Push Operationsページ



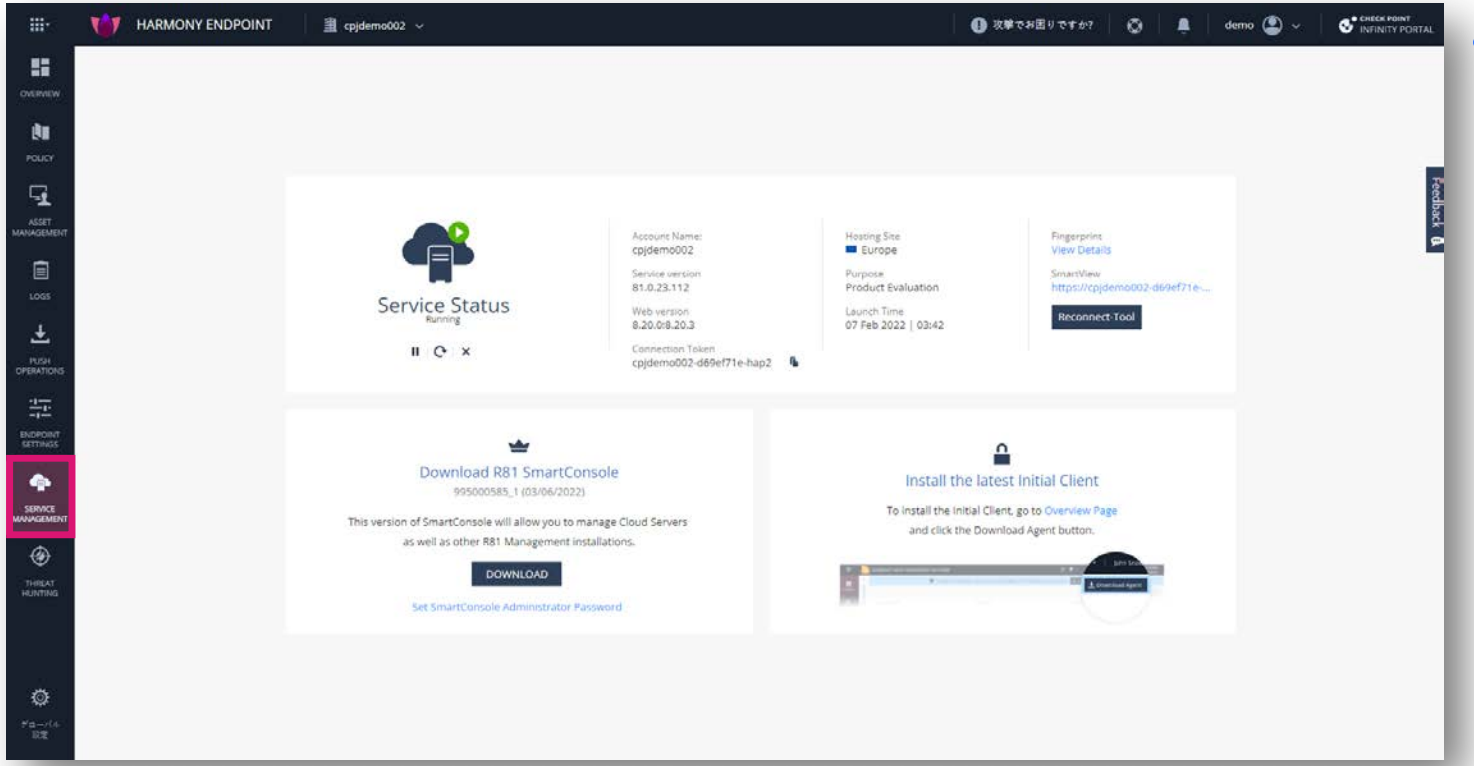
- リモートからコンピュータを操作します
  - マルウェア対策
    - スキャンの実行
    - シグネチャの更新
    - ファイルを隔離から復元
  - フォレンジックと修復
    - IoC による分析
    - ファイル修復
    - コンピュータの隔離
    - コンピュータの解放
  - エージェント設定
    - クライアントログの収集
    - クライアントソフトの修復
    - シャットダウン
    - 再起動
    - アプリケーションスキャン
    - プロセスの停止
    - リモートコマンド

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

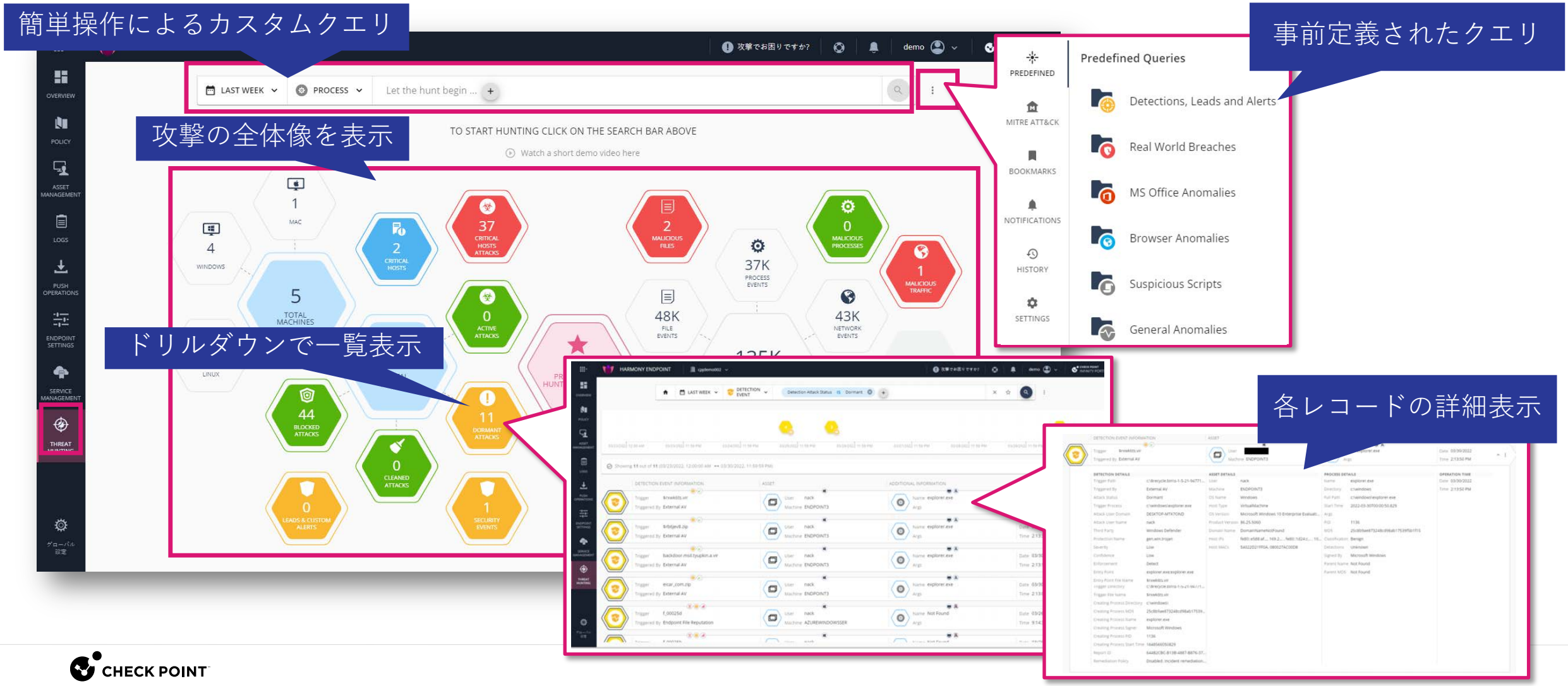
Service Management ページ



- 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

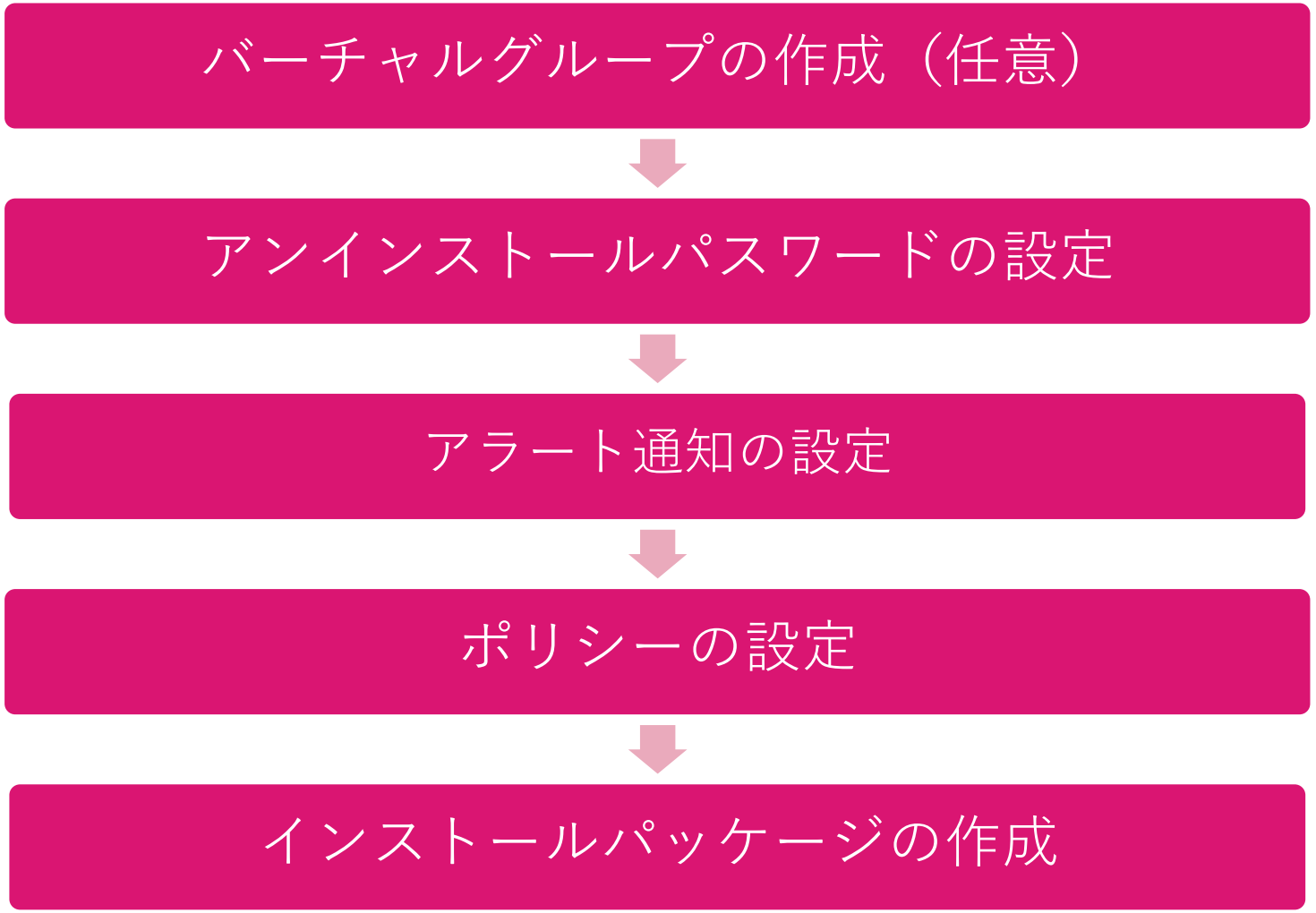
Threat Hunting ページ

- 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



設定の流れ

設定の流れ

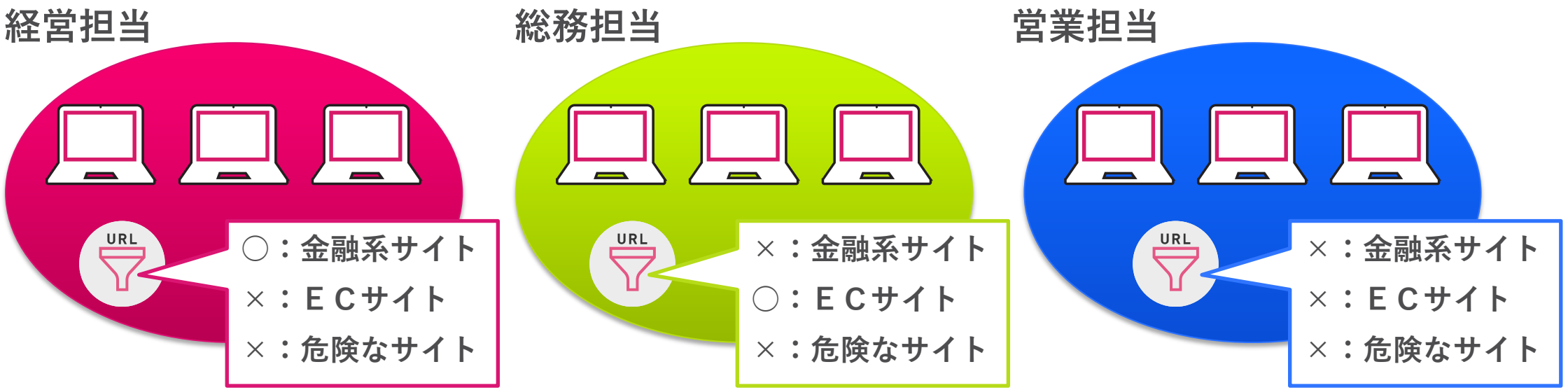


バーチャルグループによる管理

- 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

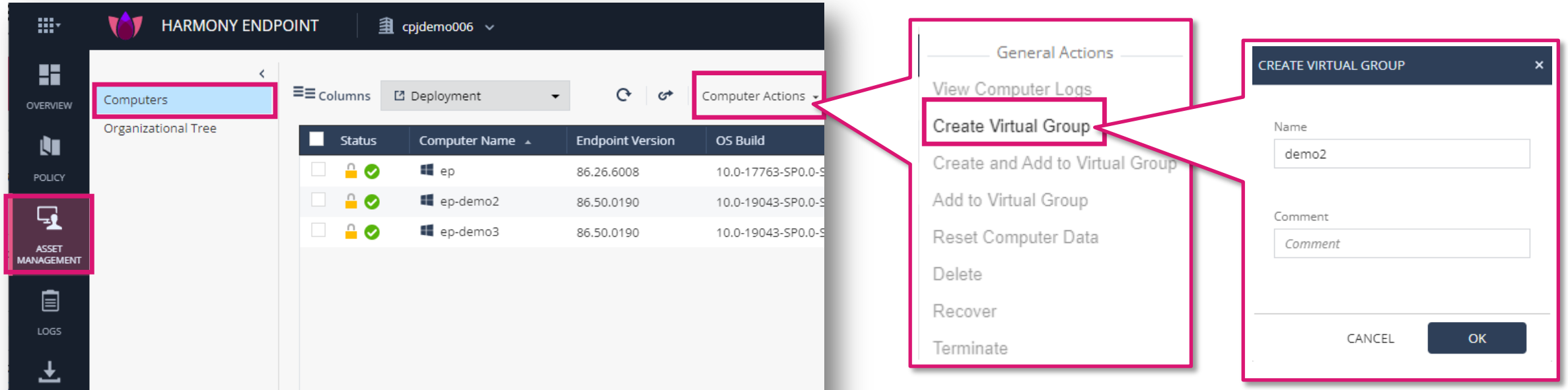
- 組織や役職などに応じて、ポリシーやセキュリティ機能、クライアントのバージョンなどをコンピュータが所属するグループでカスタマイズすることができます
- Harmony Endpoint で作成するグループを、「バーチャルグループ」といいます
- OSやコンピュータ種別に応じて事前定義されたバーチャルグループを使用することもできます
- バーチャルグループは、インストールパッケージを作成する際に指定することも、クライアントをインストール後に追加、削除することもできます



バーチャルグループの作成（１／２）

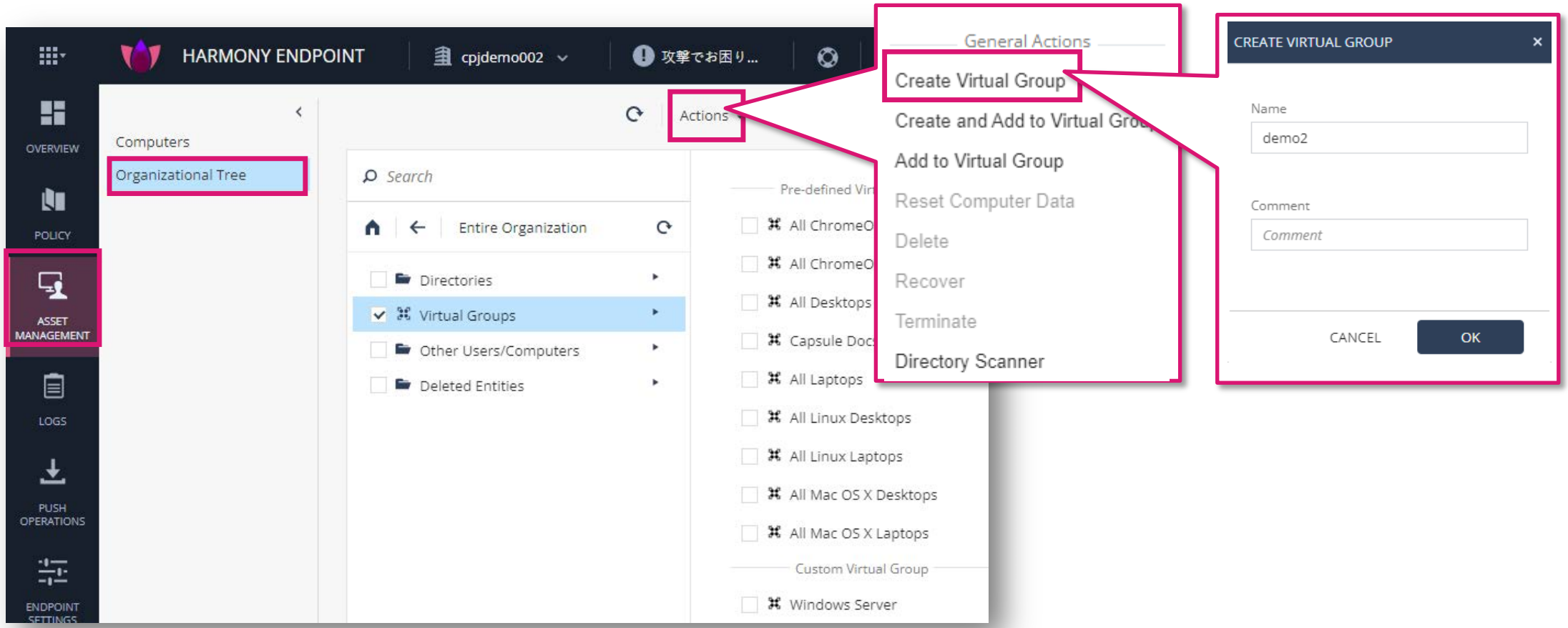
- バーチャルグループの作成は、以下の２つの方法で可能です
  - Asset Management > Computers > Computer Actions
  - Asset Management > Organizational Tree

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



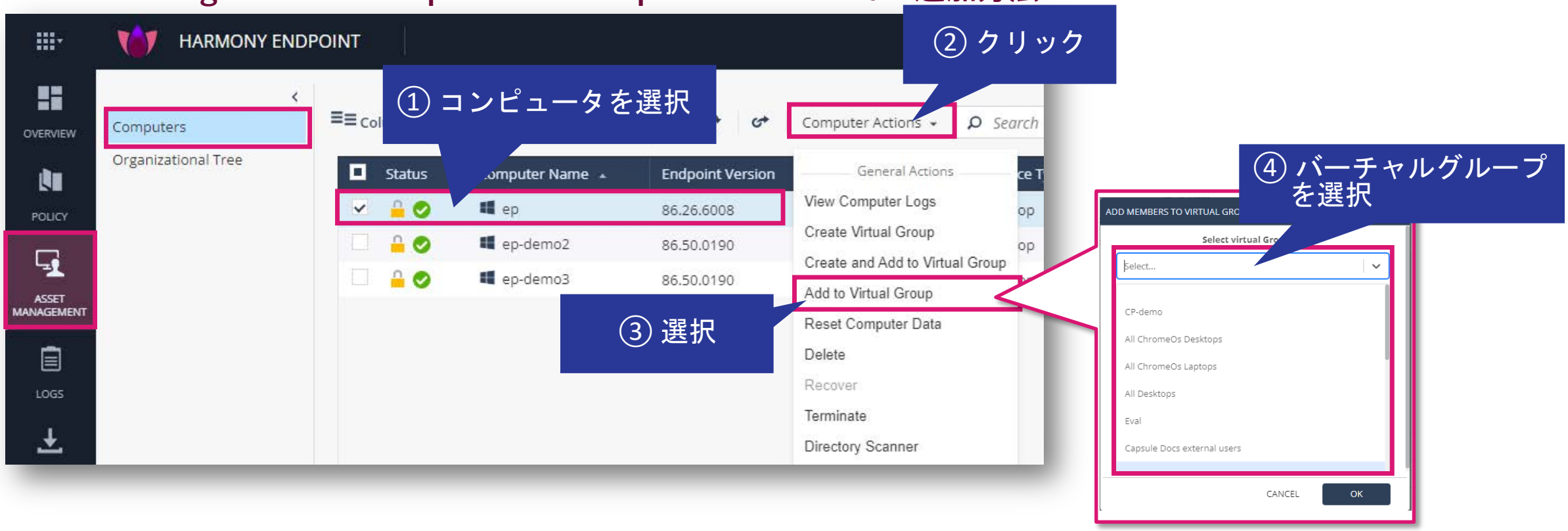
バーチャルグループへのコンピュータの追加、削除（１／４）

- 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

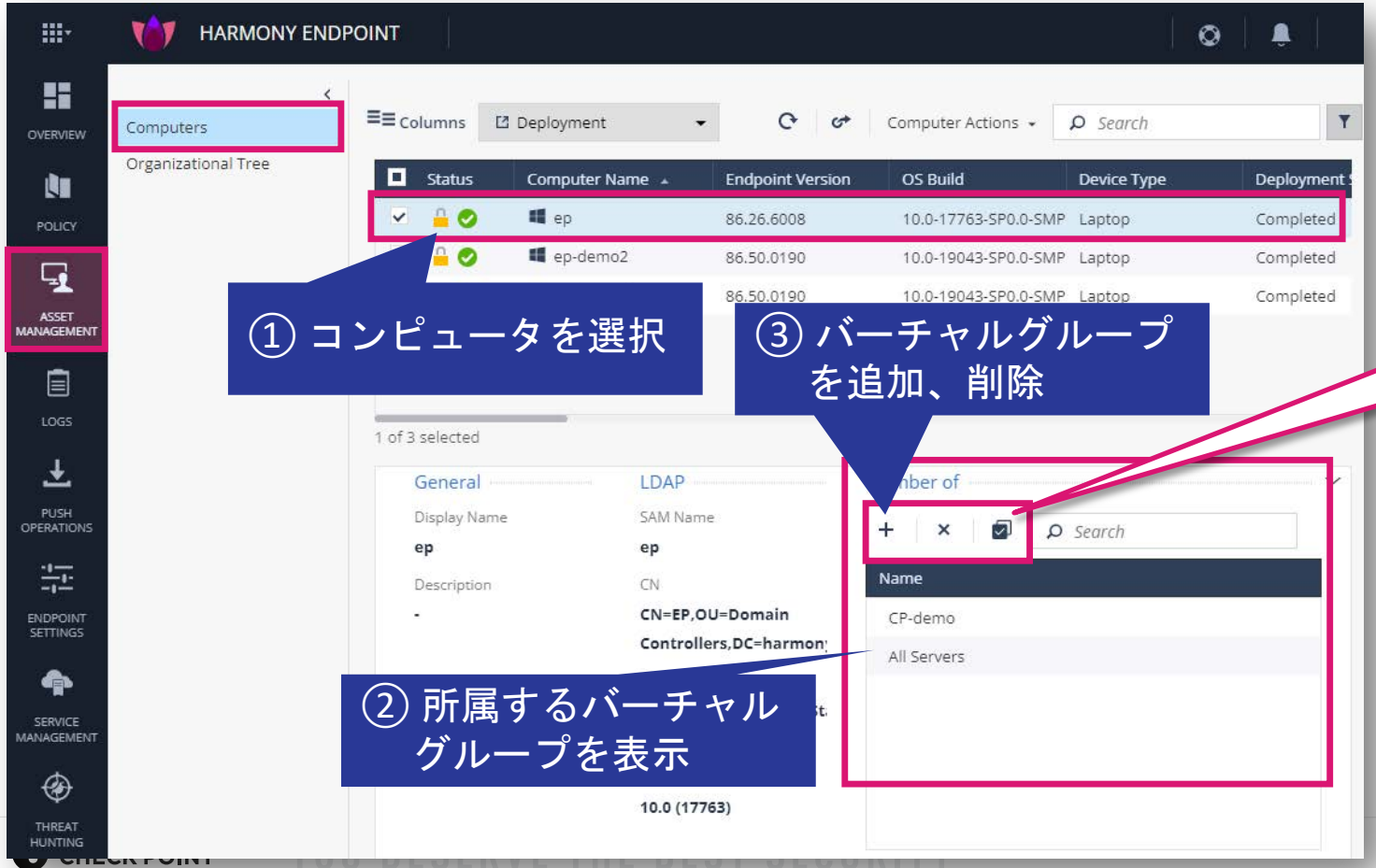
Asset Management > Computers > Computer Actions での追加方法

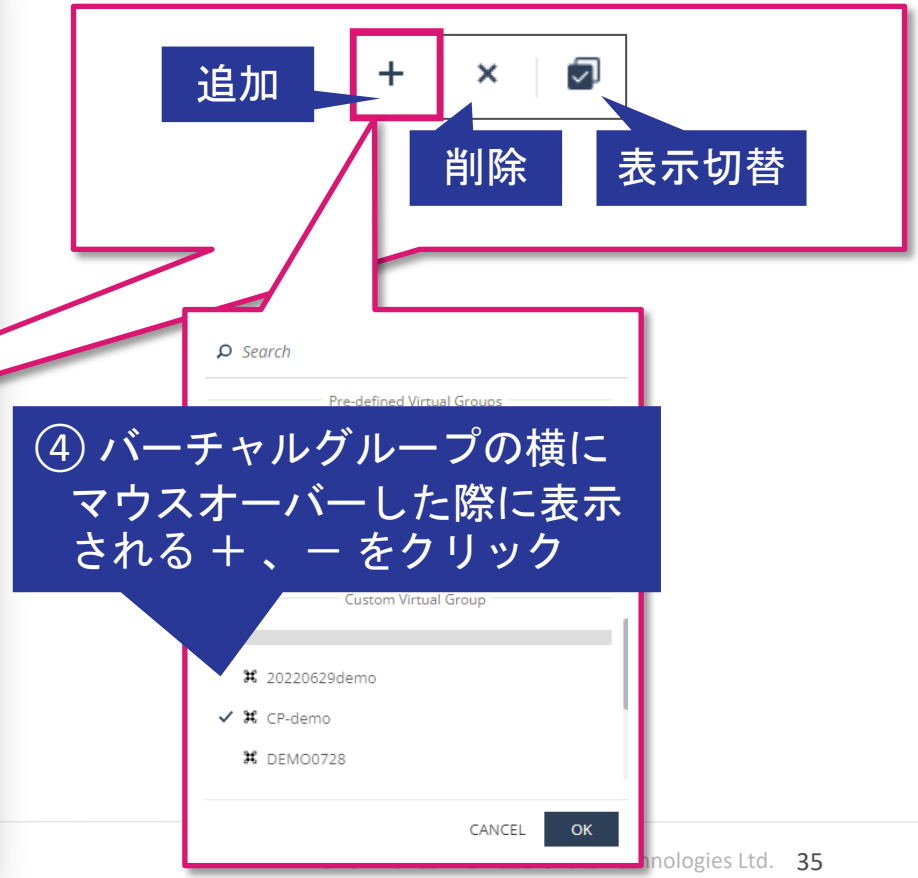


バーチャルグループへのコンピュータの追加、削除（３／４）

- 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

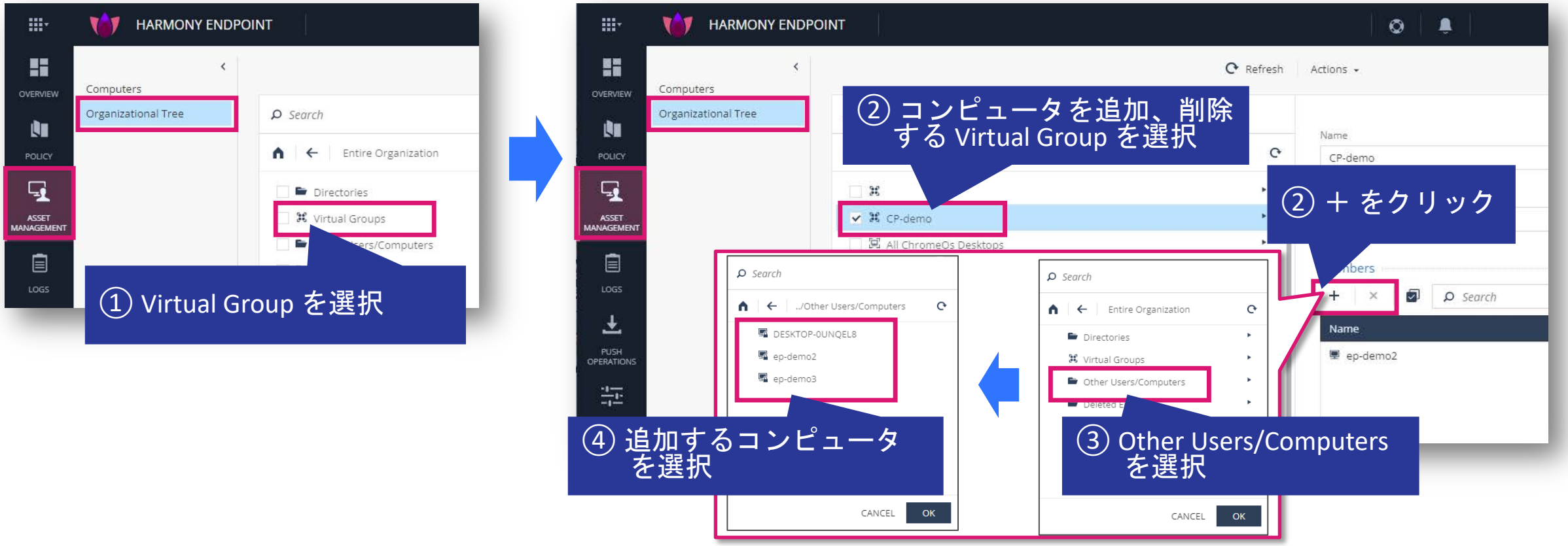




バーチャルグループへのコンピュータの追加、削除（４／４）

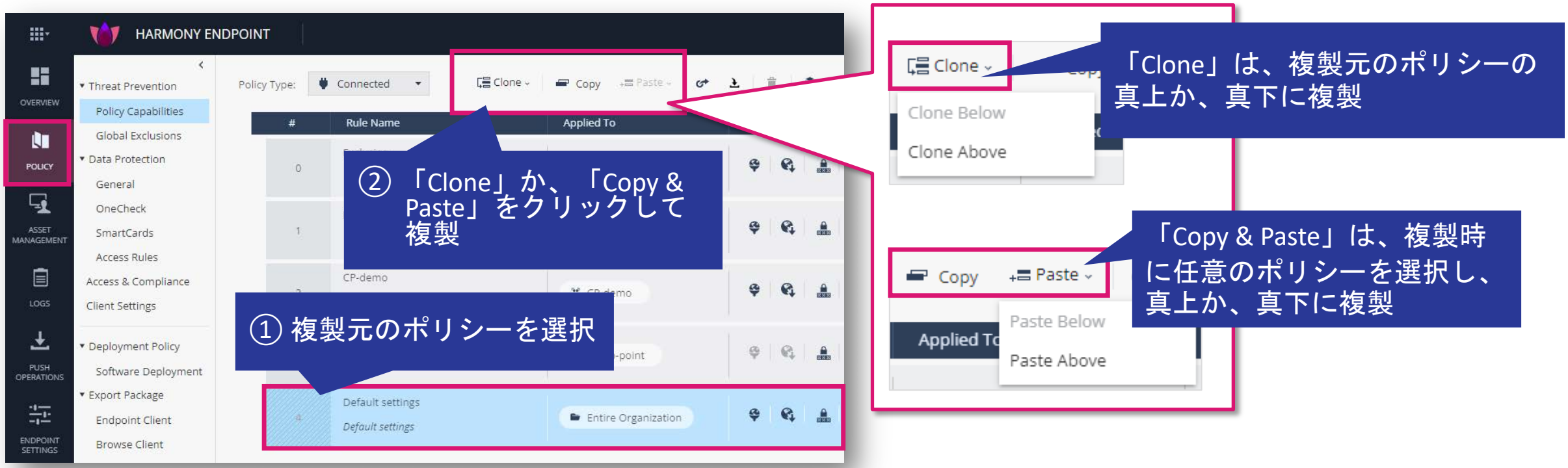
- Organizational Tree で Virtual Group を選択して、コンピュータを追加、削除する

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）

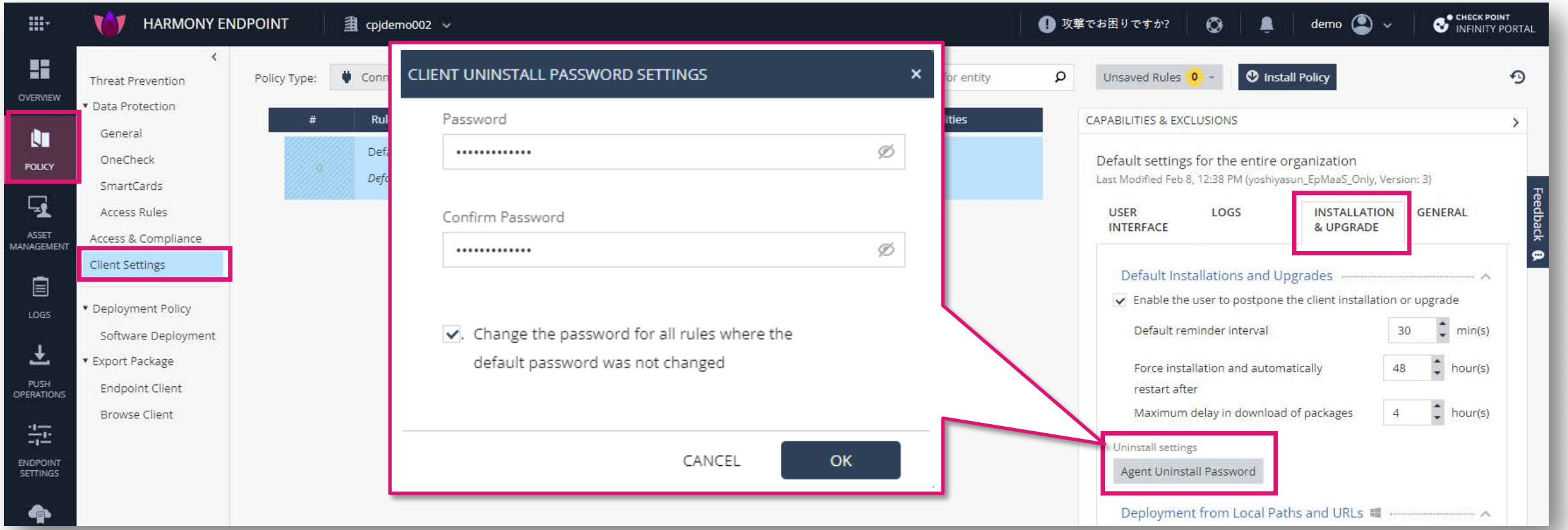
- 表示されたダイアログボックスで、ポリシーの名前と適用対象を設定します
- バーチャルグループ以外に、コンピュータや Active Directory の OU に適用できます
  - Active Directory の OU に適用できるのは、AD Scanners を設定した場合のみです

アンインストールパスワードの設定

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



アラート通知設定

アラート通知設定（1／4）

Threat Hunting

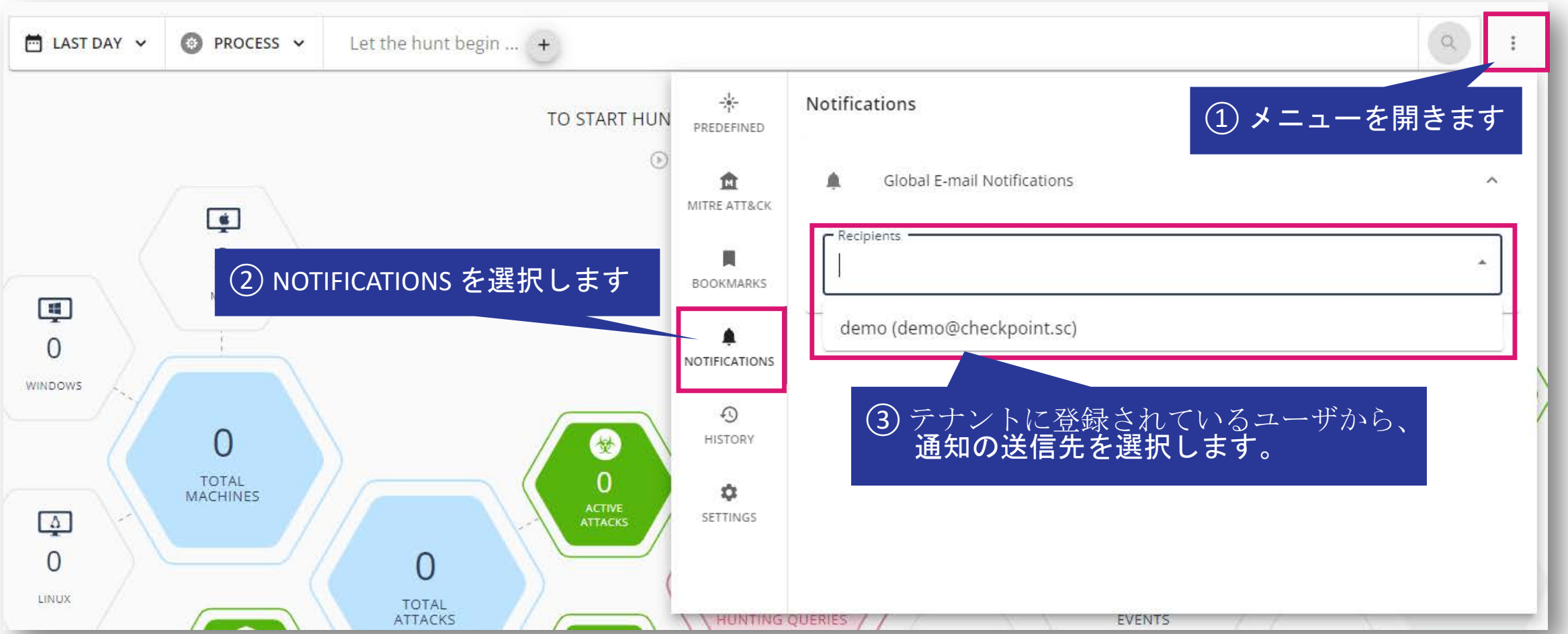
- 事前設定した条件で Threat Hunting を定期実行し、新規にイベントを発見した際に、管理者に通知できます
- Threat Hunting 画面で、通知したいイベントと通知先メールアドレスを設定します

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

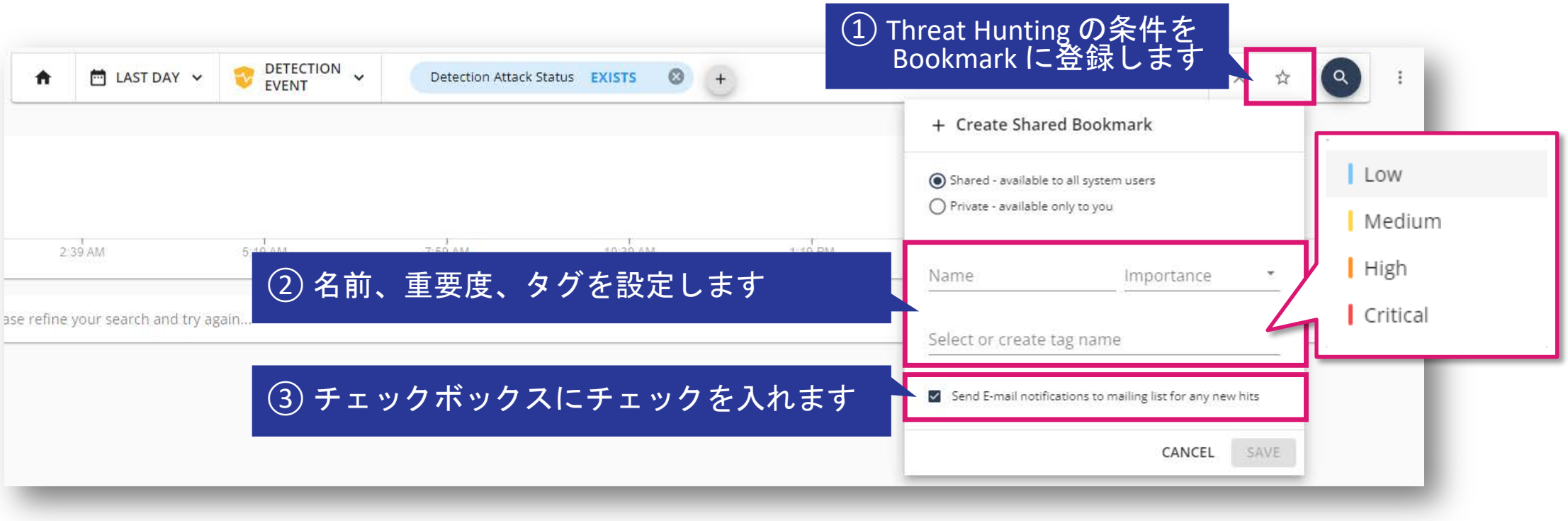
- Threat Hunting の Notifications に、アラートの通知先メールアドレスを設定します
- テナントの管理者からアラートの通知先を選択します



アラート通知設定（３／４）：アラート通知イベント設定

Threat Hunting

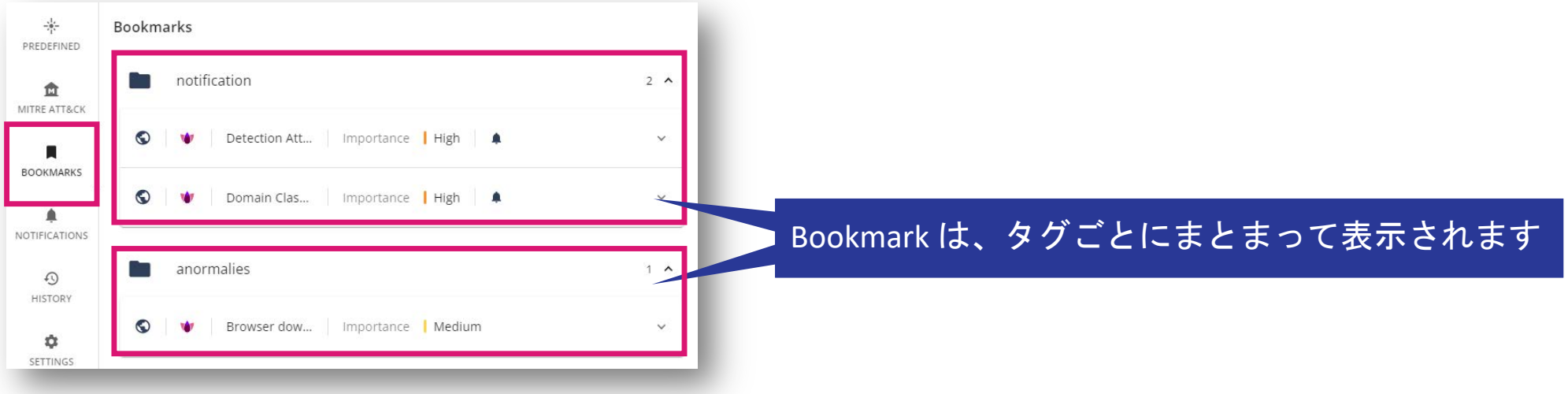
- 管理者に通知するイベントの条件を設定します
- 検索窓の ☆ マークをクリックし、検索条件を Bookmark に登録します
- Bookmark に登録された検索条件で定期的に Threat Hunting が行われます
- 検知した攻撃の状態（Detection Attack Status）や、検出したBlade（Detection Triggered by）、Severity（Detection Severity）などを検索条件に設定できます



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



ポリシーの設定

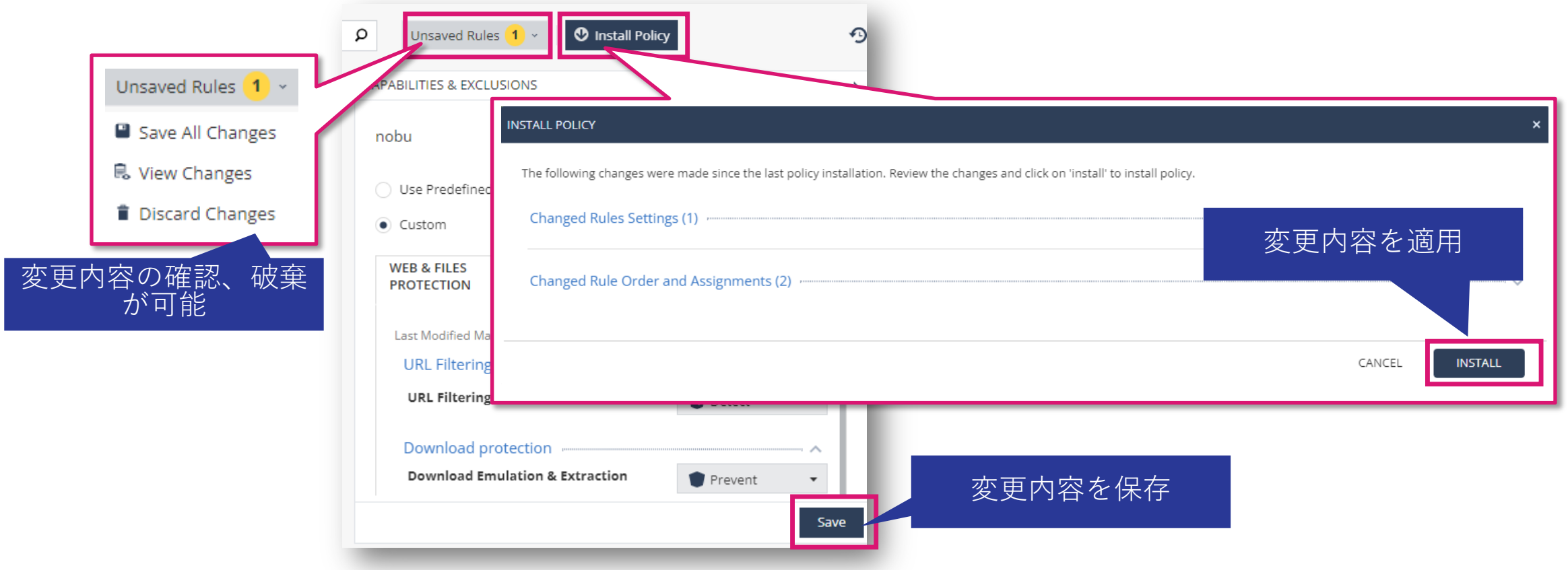
ポリシーの設定

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
共通

YOU DESERVE THE BEST SECURITY

Threat Prevention：共通（1／5）

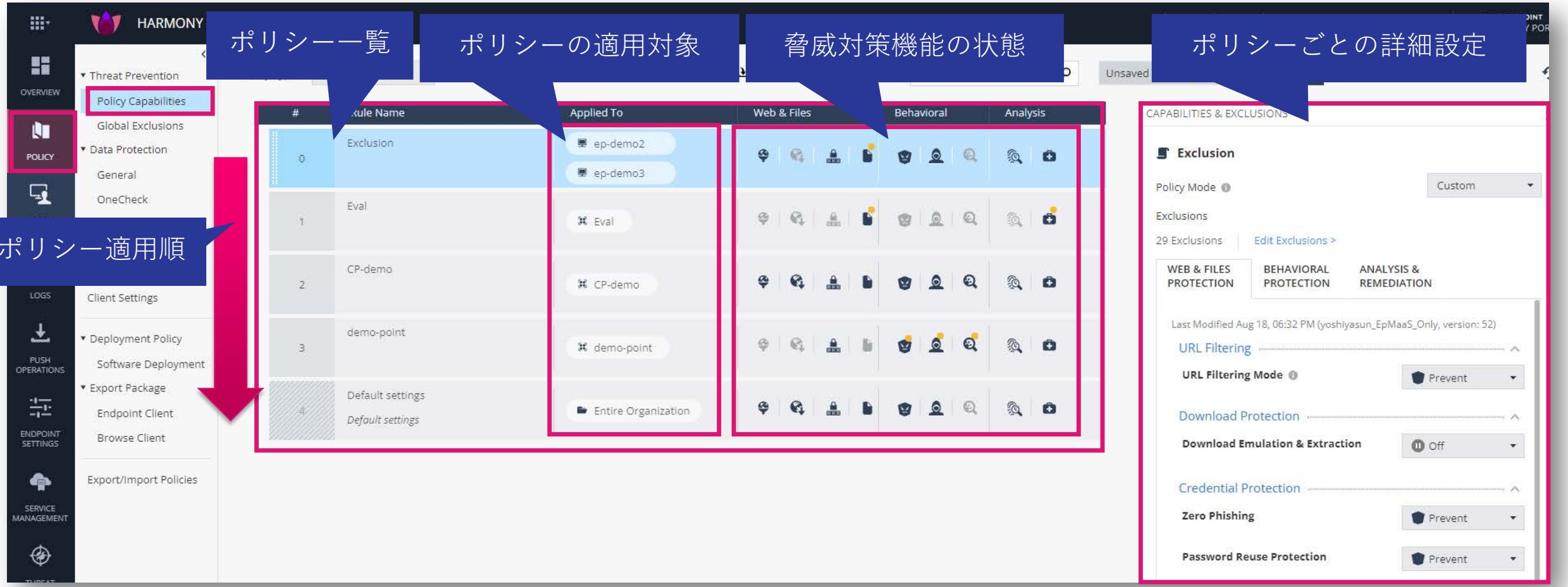
Policy > Threat Prevention

- 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）

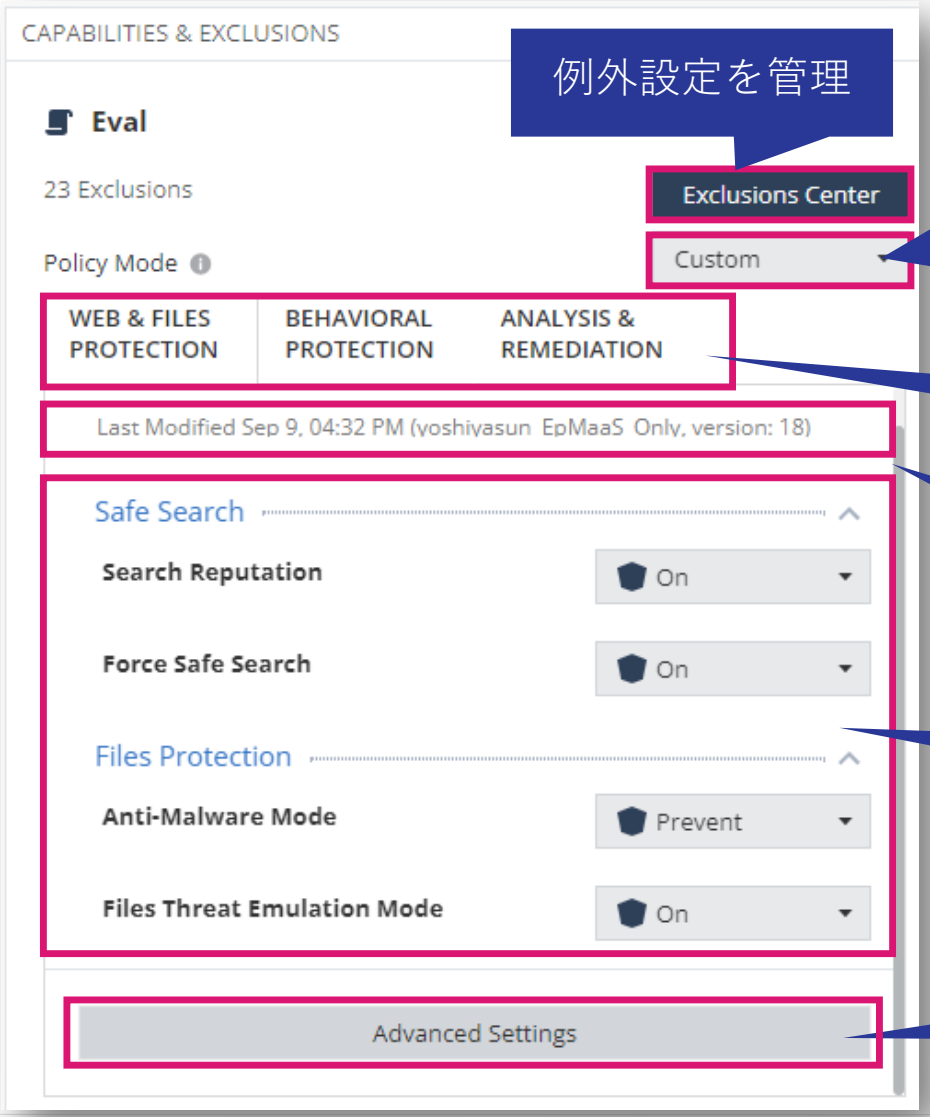
Policy > Threat Prevention

- 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

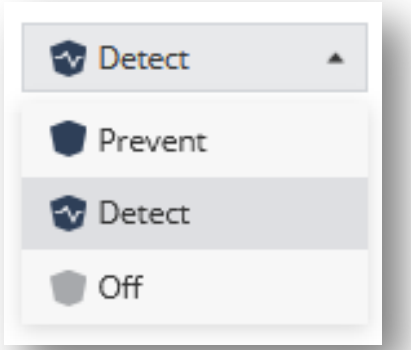
セキュリティ対策機能の動作モードを選択

セキュリティ対策機能の詳細を設定

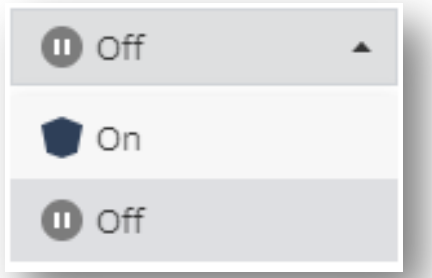
Threat Prevention：共通（４／５）

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

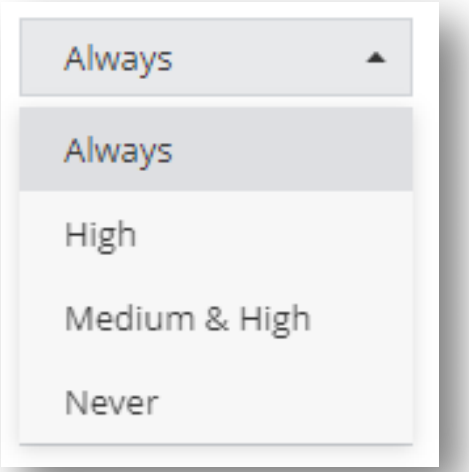


- 動作モードの選択肢②
  - On　：機能を有効化
  - Off　：機能を無効化

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

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

ポリシーの設定

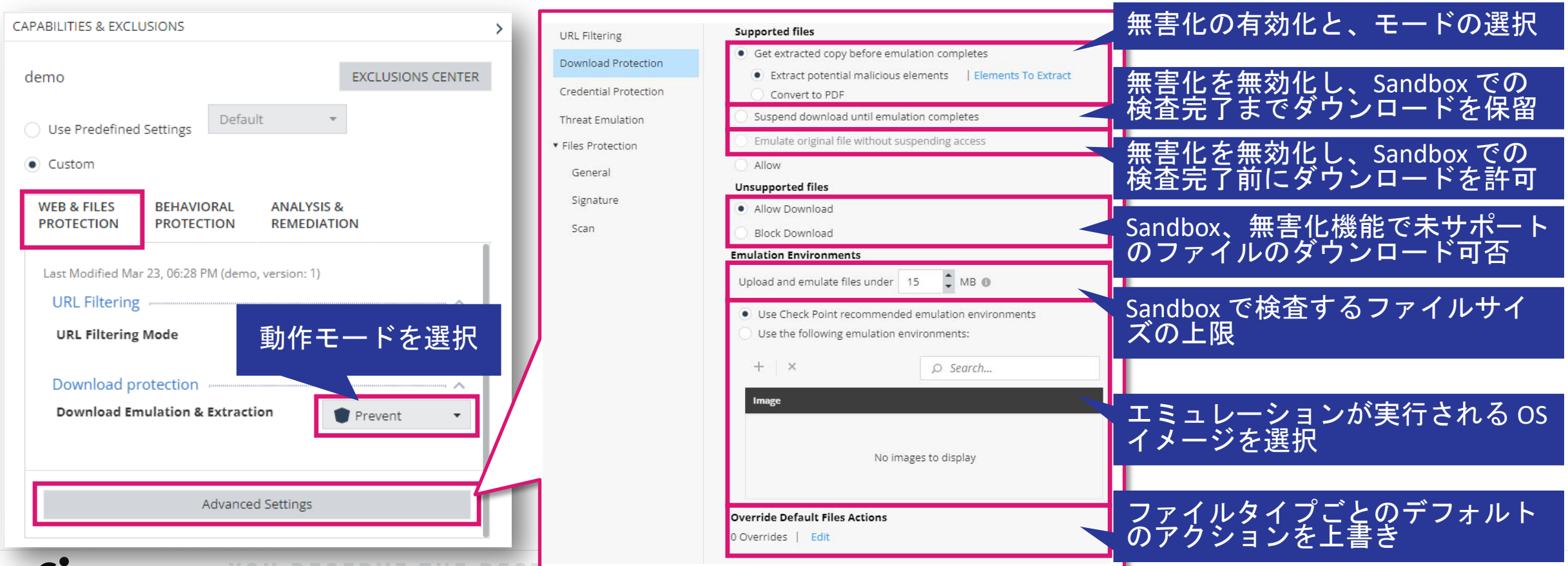
THREAT PREVENTION DOWNLOAD 保護

- 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

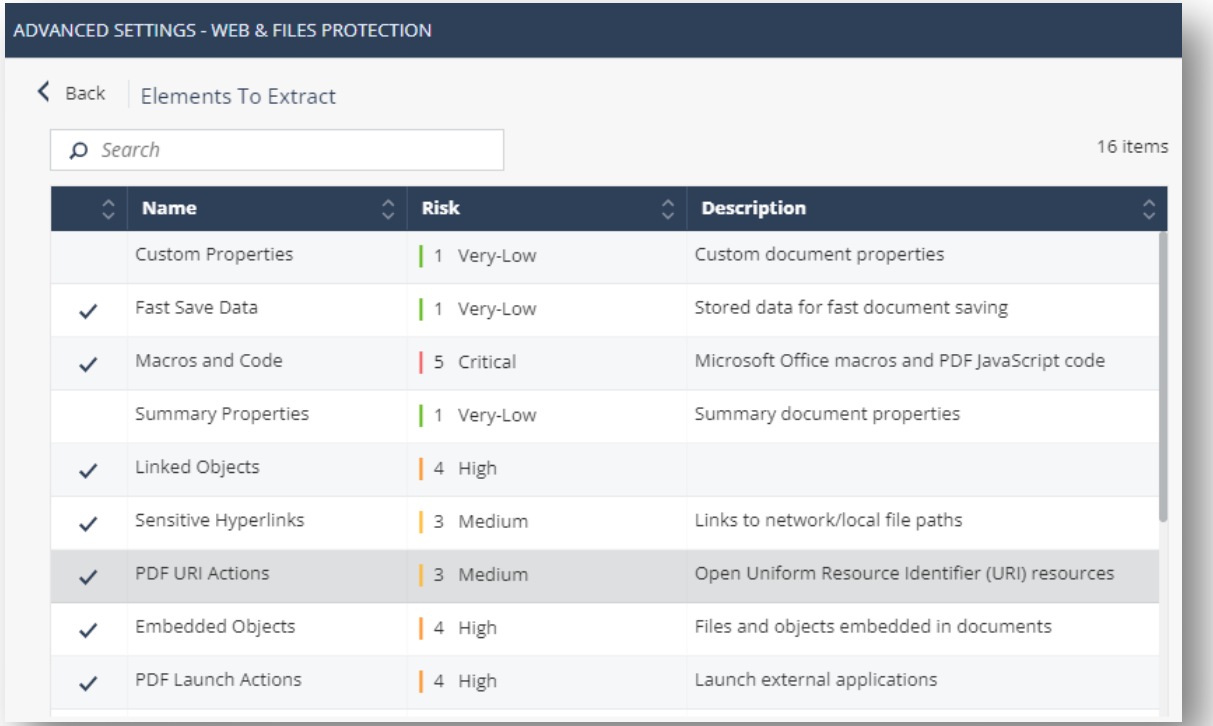


Threat Prevention：Download 保護（2／2）

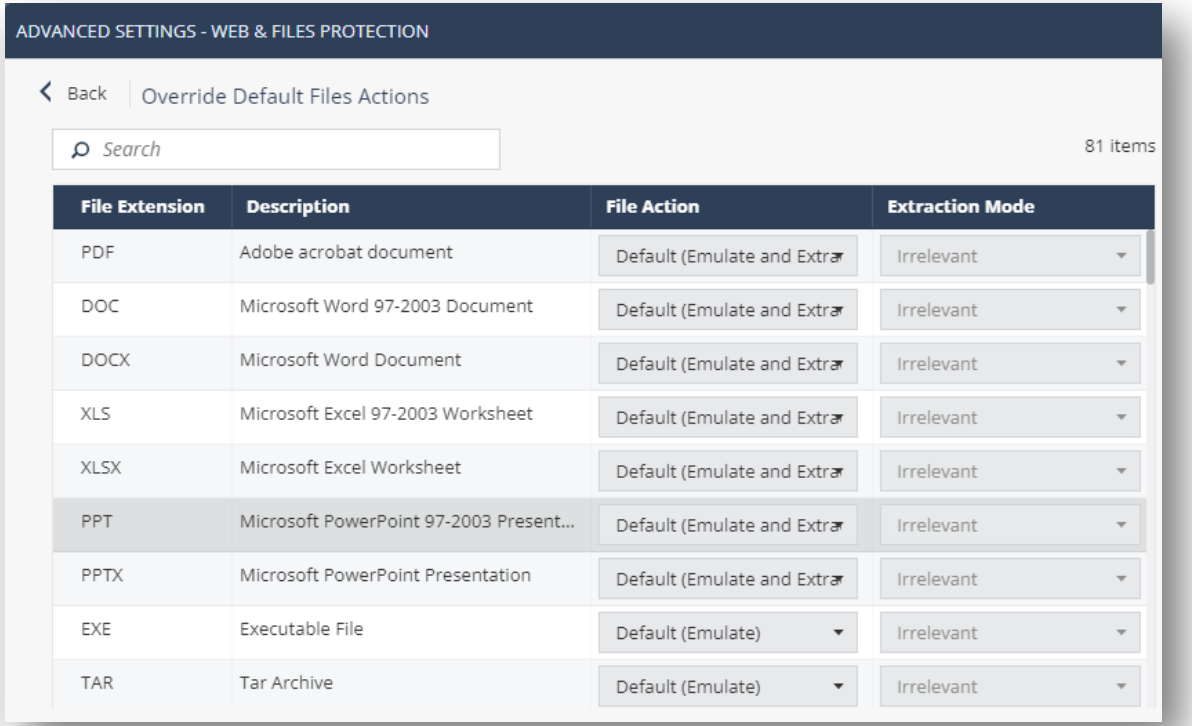
Policy > Threat Prevention > Web & Files Protection > Download Protection > Advance Settings

- 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



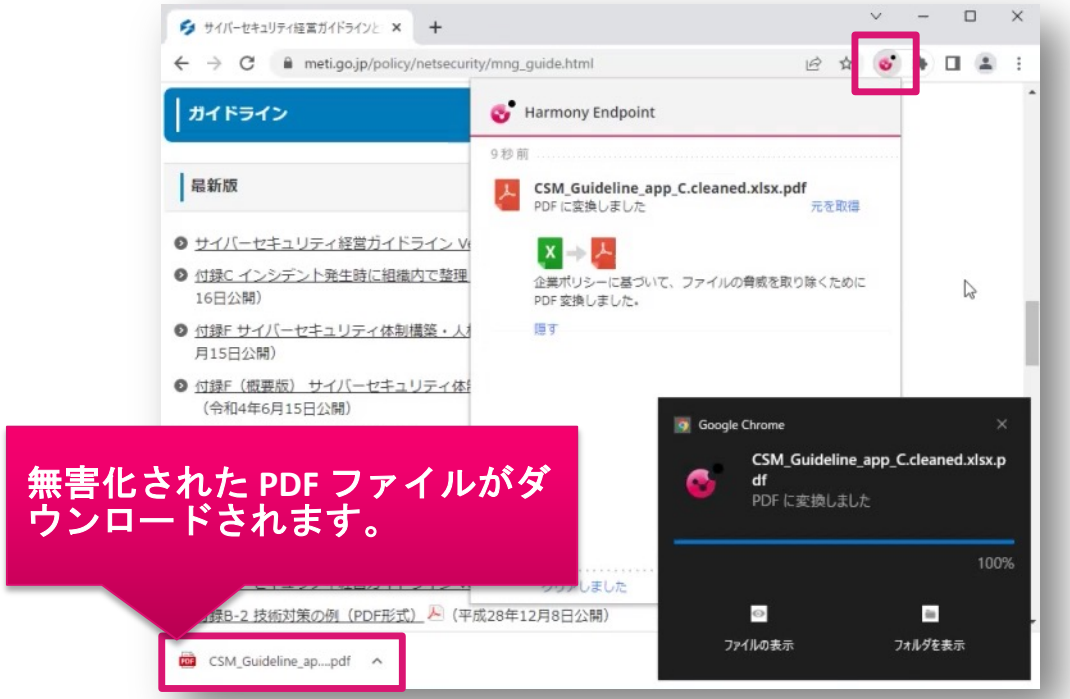
Override Default Files Actions



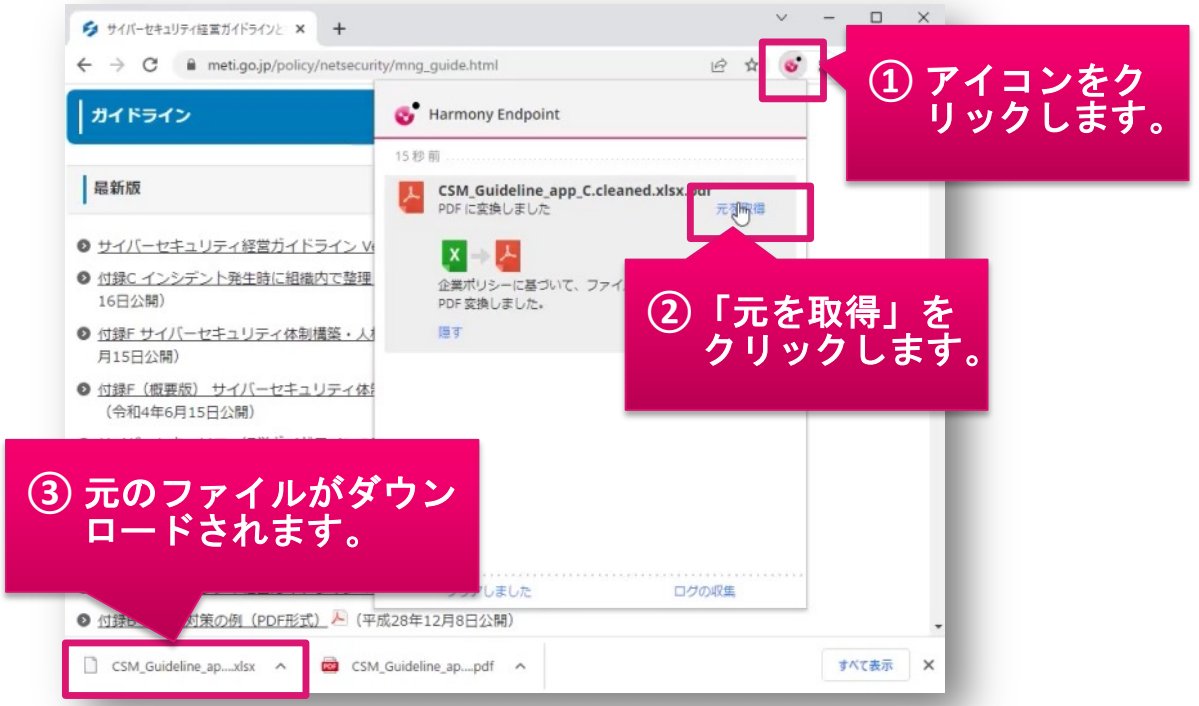
【参考】サンドボックス＆ファイル無害化の操作（１／２）

- 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

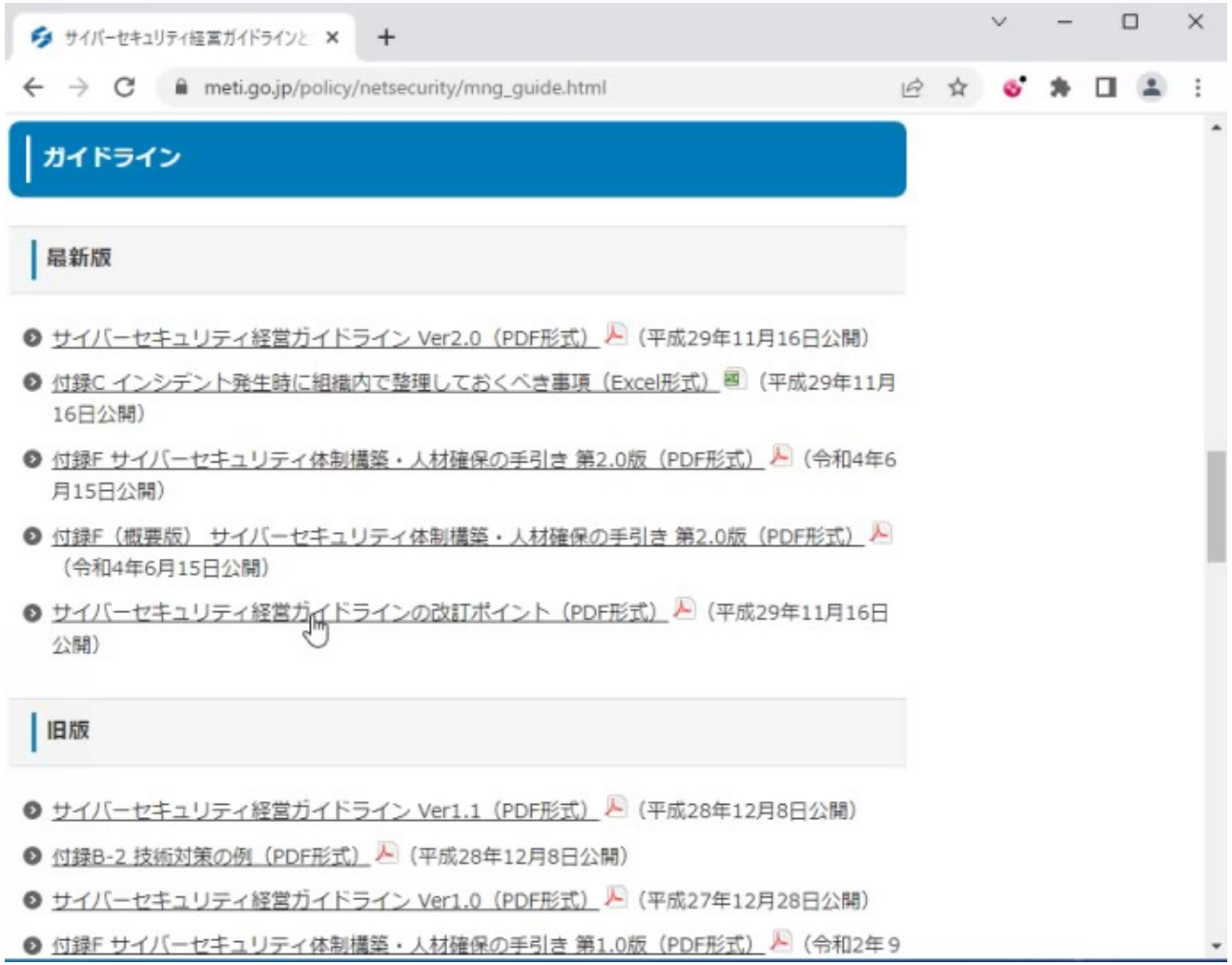


元のファイルのダウンロード



【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

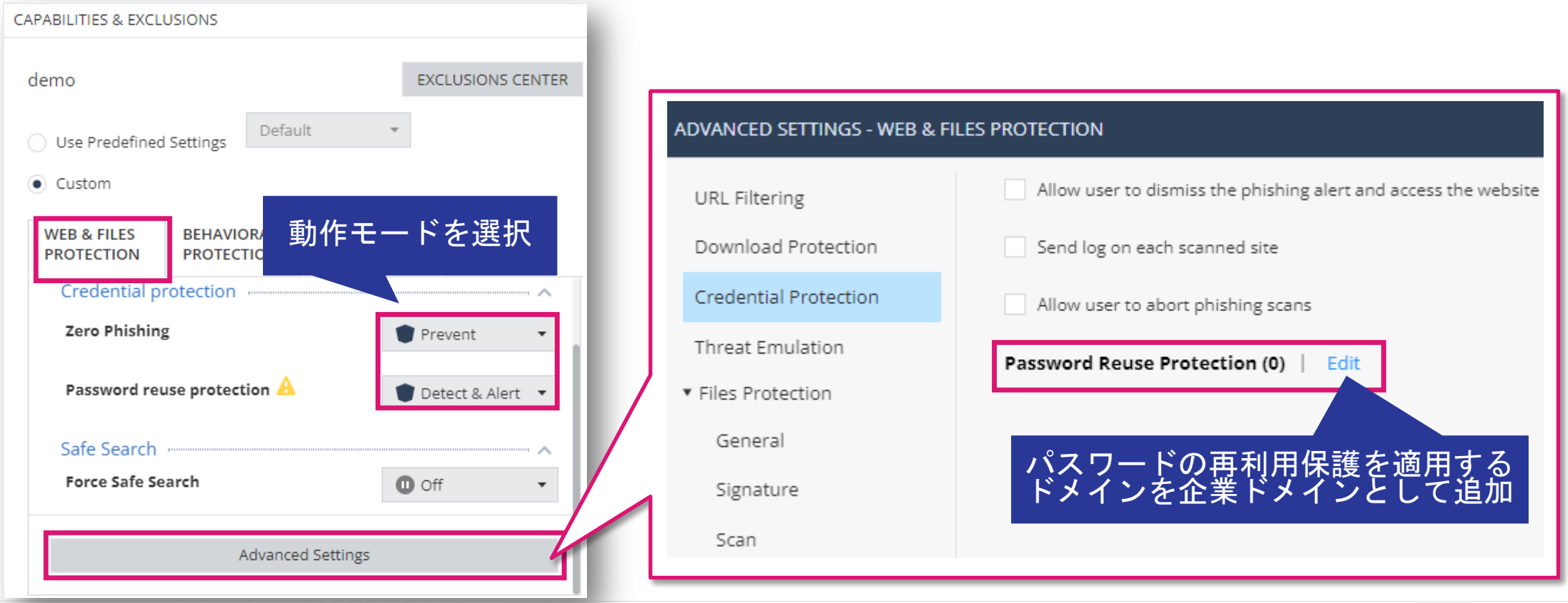
THREAT PREVENTION
認証情報の保護

YOU DESERVE THE BEST SECURITY

Threat Prevention：認証情報の保護

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

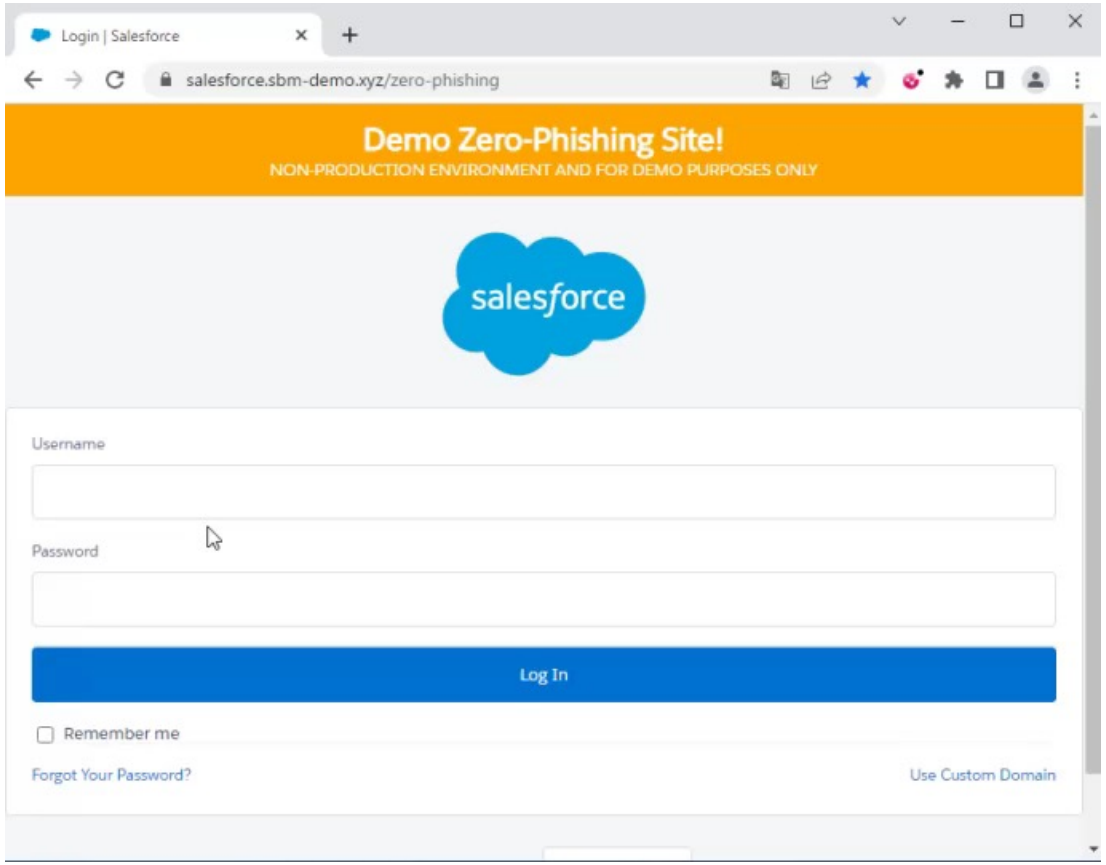
- Zero-Phishing は、Webサイトの様々な特性をチェックして、フィッシングサイトを検出します
- パスワードの再利用保護は、企業ドメインで利用されたパスワードのハッシュを記録し、同じパスワードを非企業ドメインで企業パスワードを使用しない様に警告します



【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

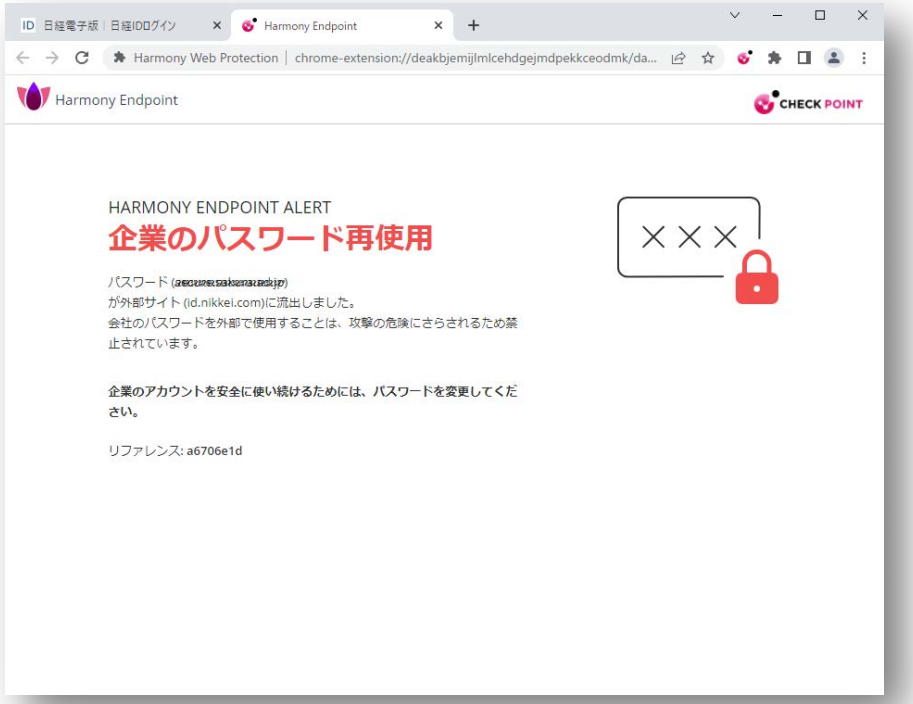
フィッシングサイトへアクセスした際の動作概要



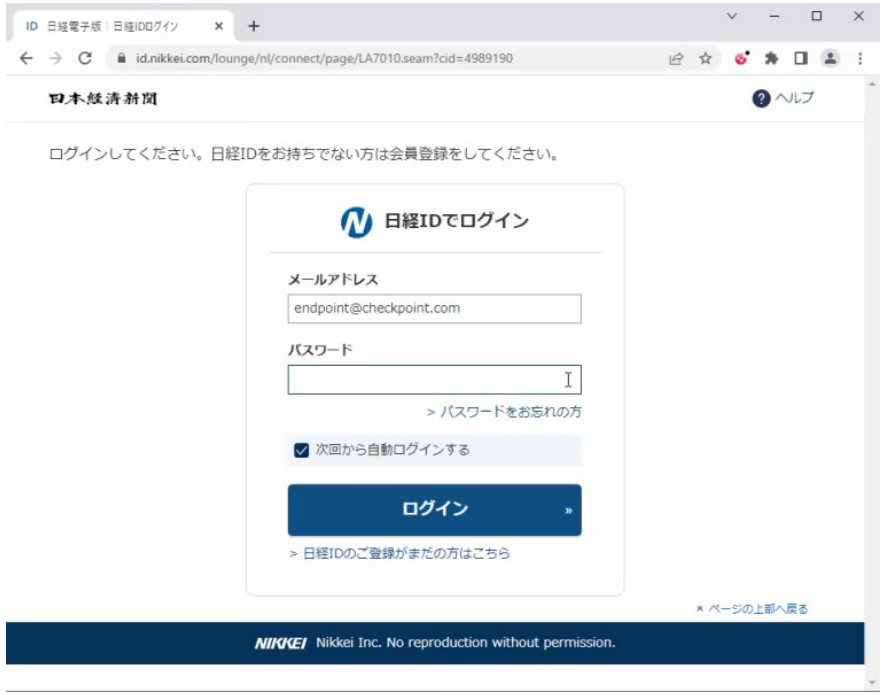
【参考】企業パスワード保護機能の動作概要

- 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

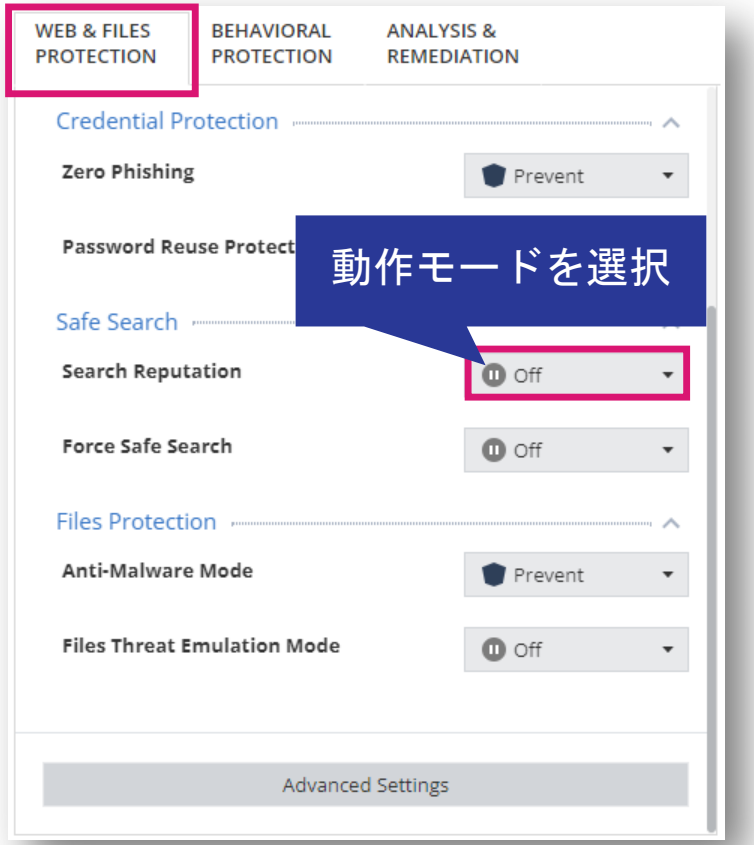
THREAT PREVENTION
安全な検索

YOU DESERVE THE BEST SECURITY

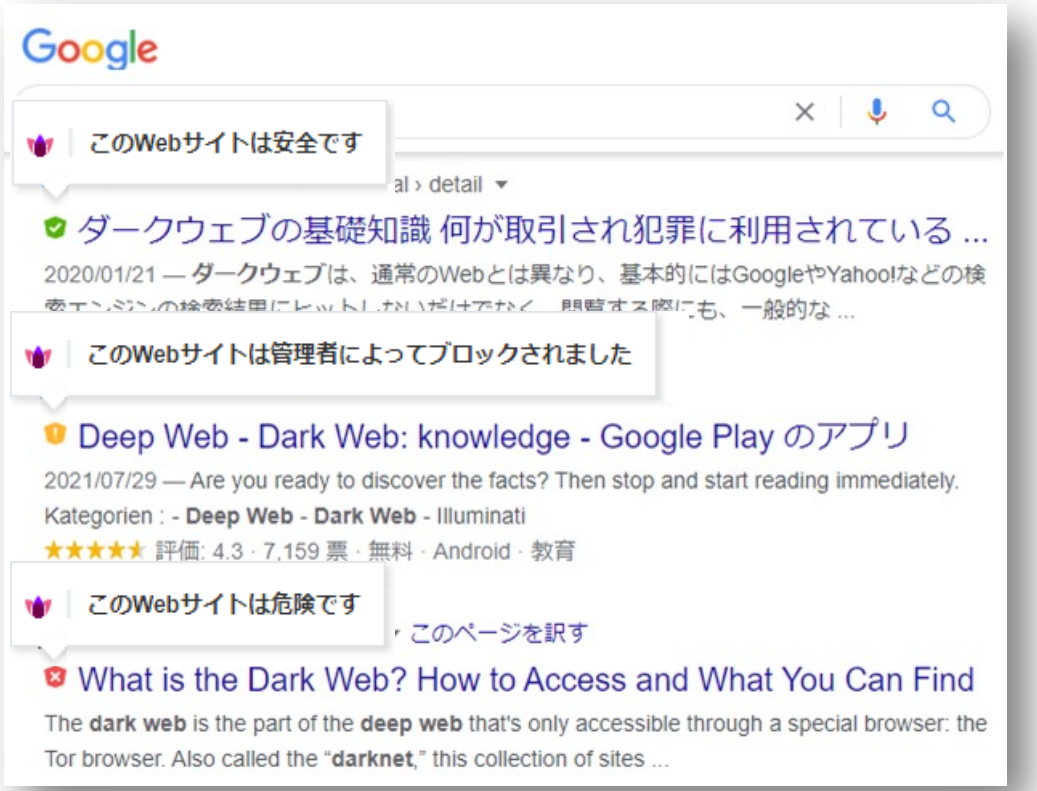
Threat Prevention：サーチ・レピュテーション

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



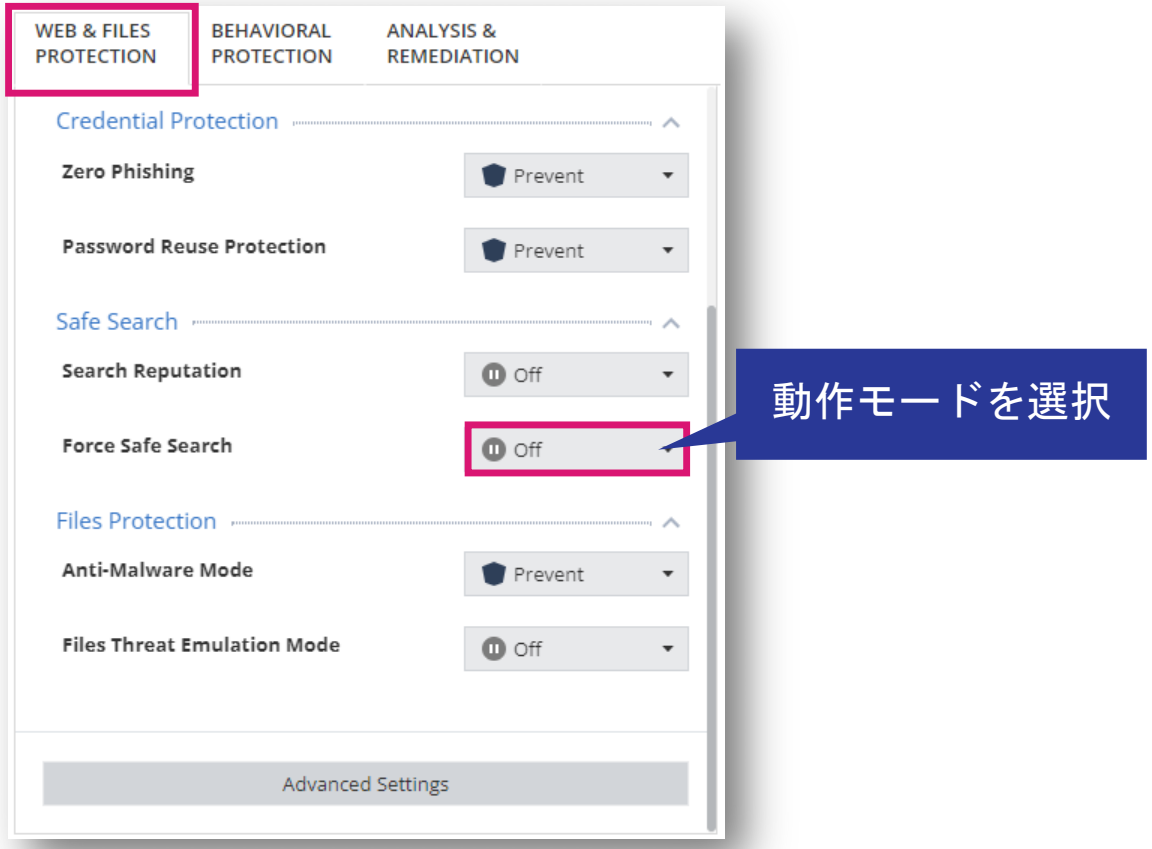
凡例

- 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。



ポリシーの設定

THREAT PREVENTION
ファイル保護

YOU DESERVE THE BEST SECURITY

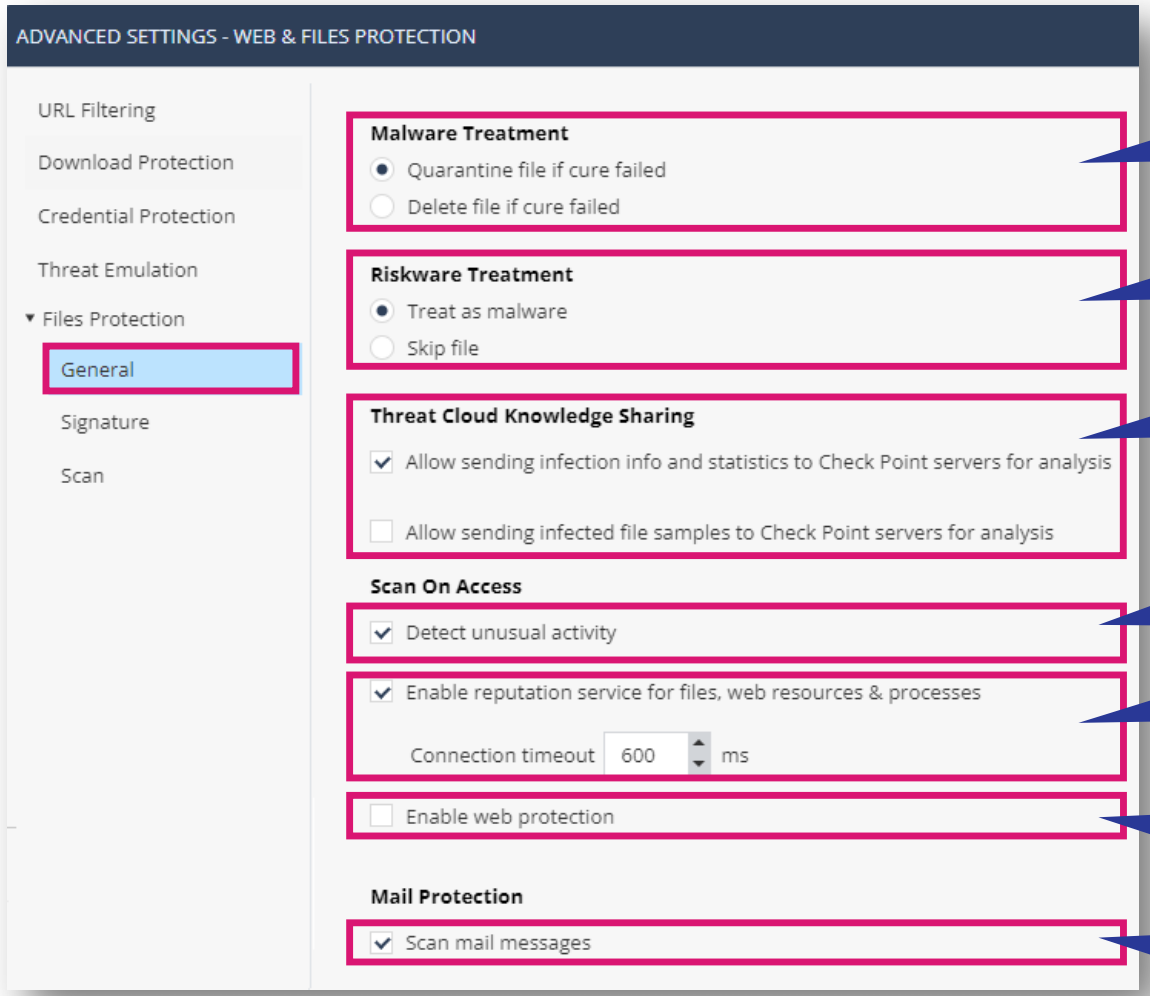
Threat Prevention ファイル保護（１／４）

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

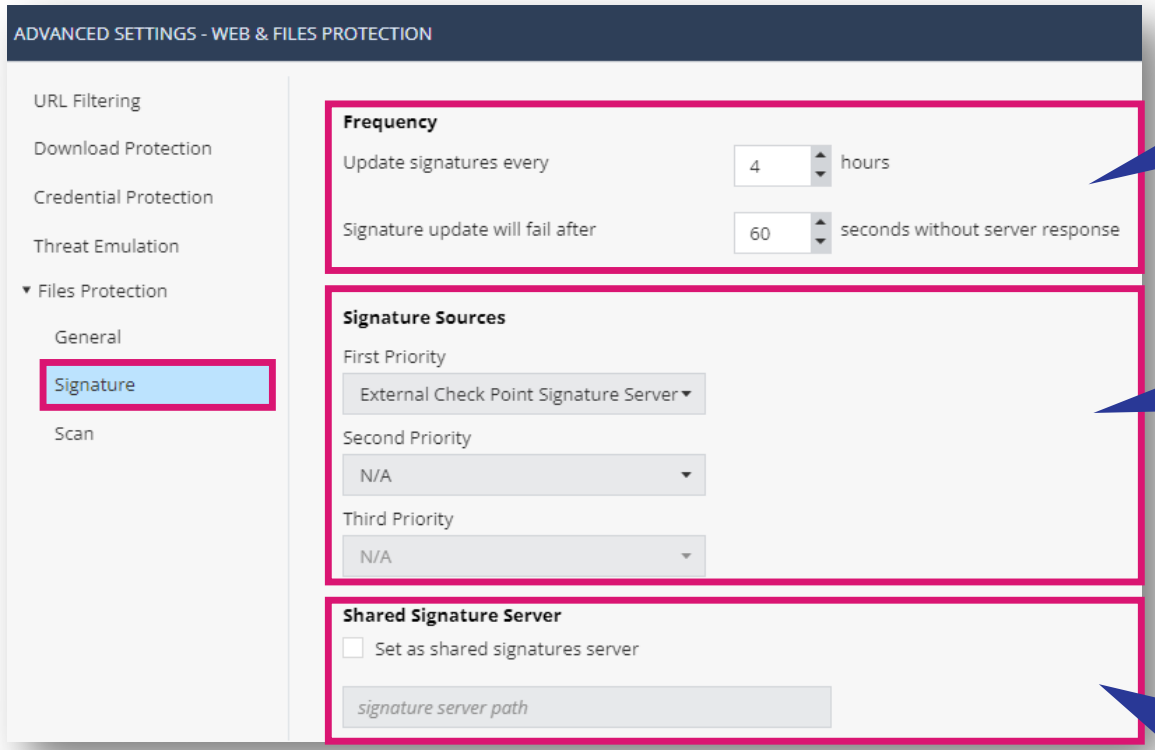
クラウドを使用したファイル、Web リソース、プロセスのレピュテーションの有効化を選択。PCの再起動後に有効

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



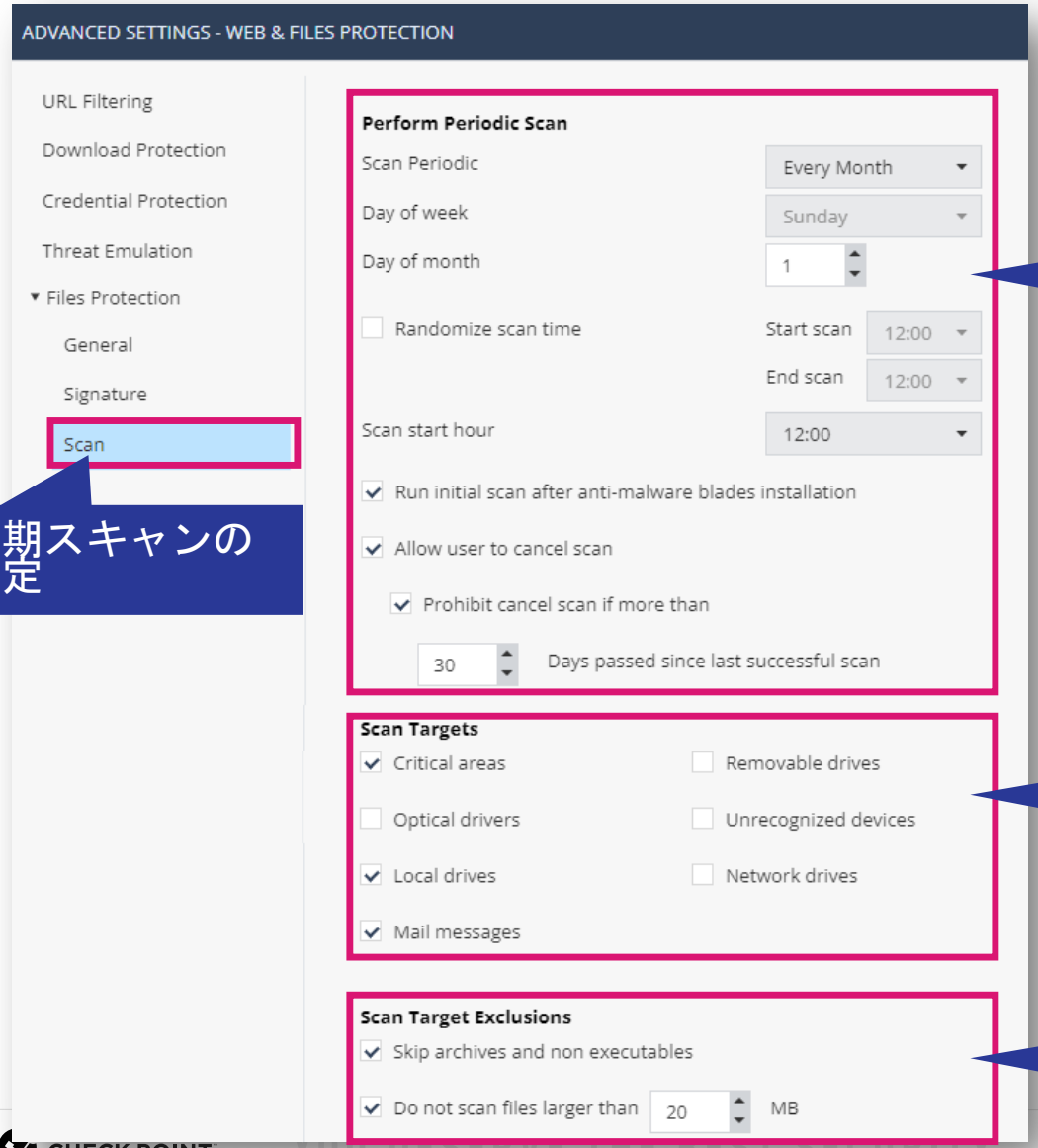
シグネチャの更新間隔とタイムアウト時間

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）

ポリシーの設定

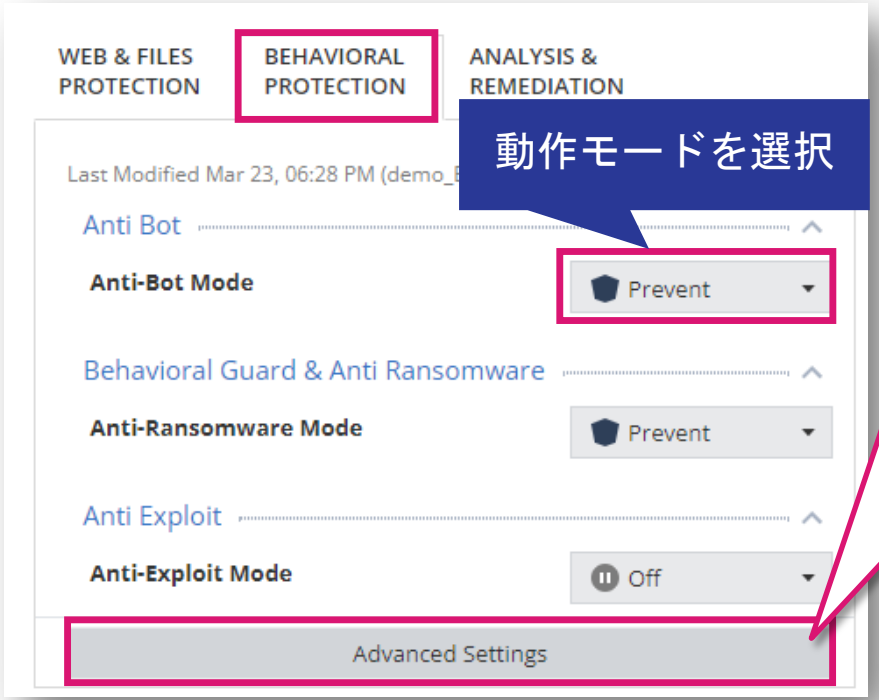
THREAT PREVENTION
ANTI-BOT

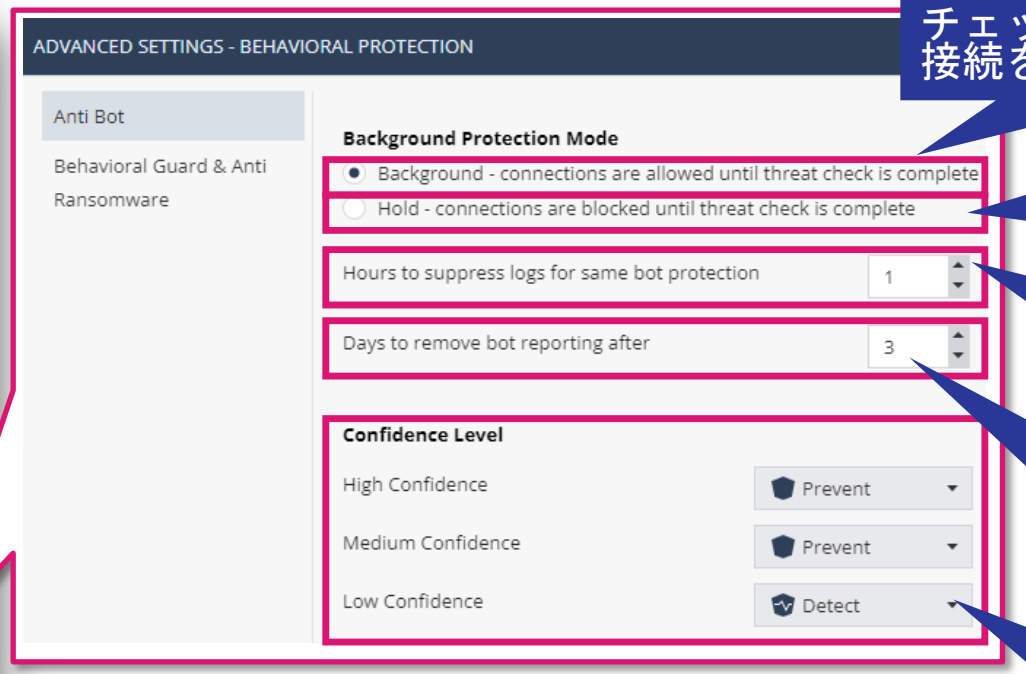
YOU DESERVE THE BEST SECURITY

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

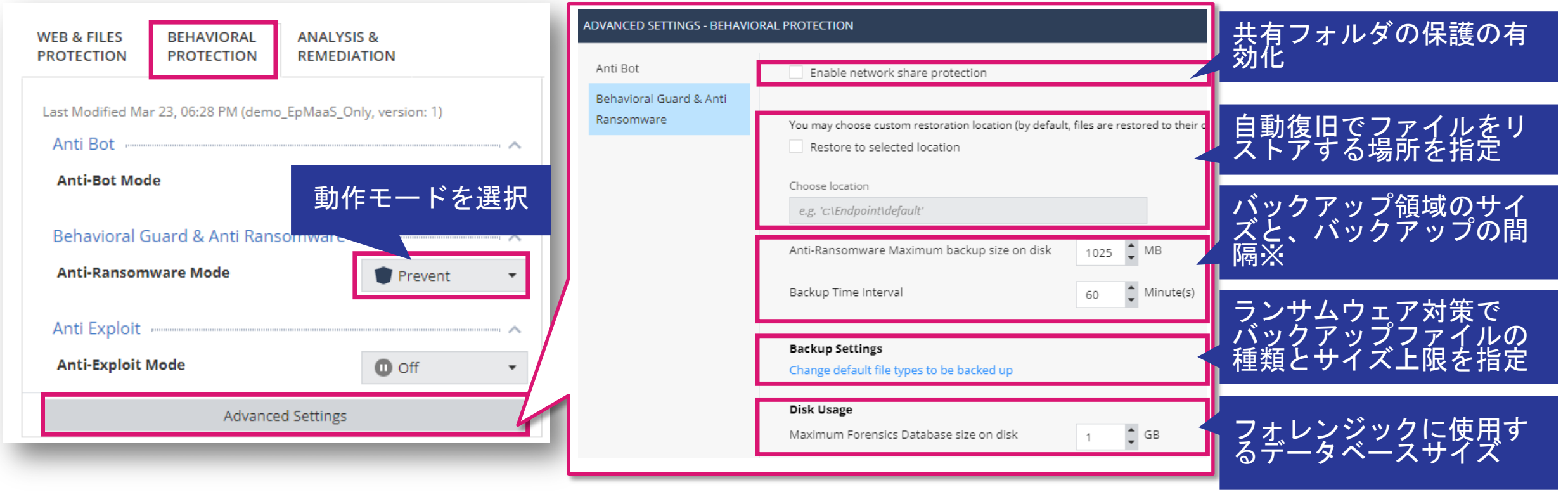
THREAT PREVENTION
BEHAVIORAL GUARD & ANTI-RANSOMWARE

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

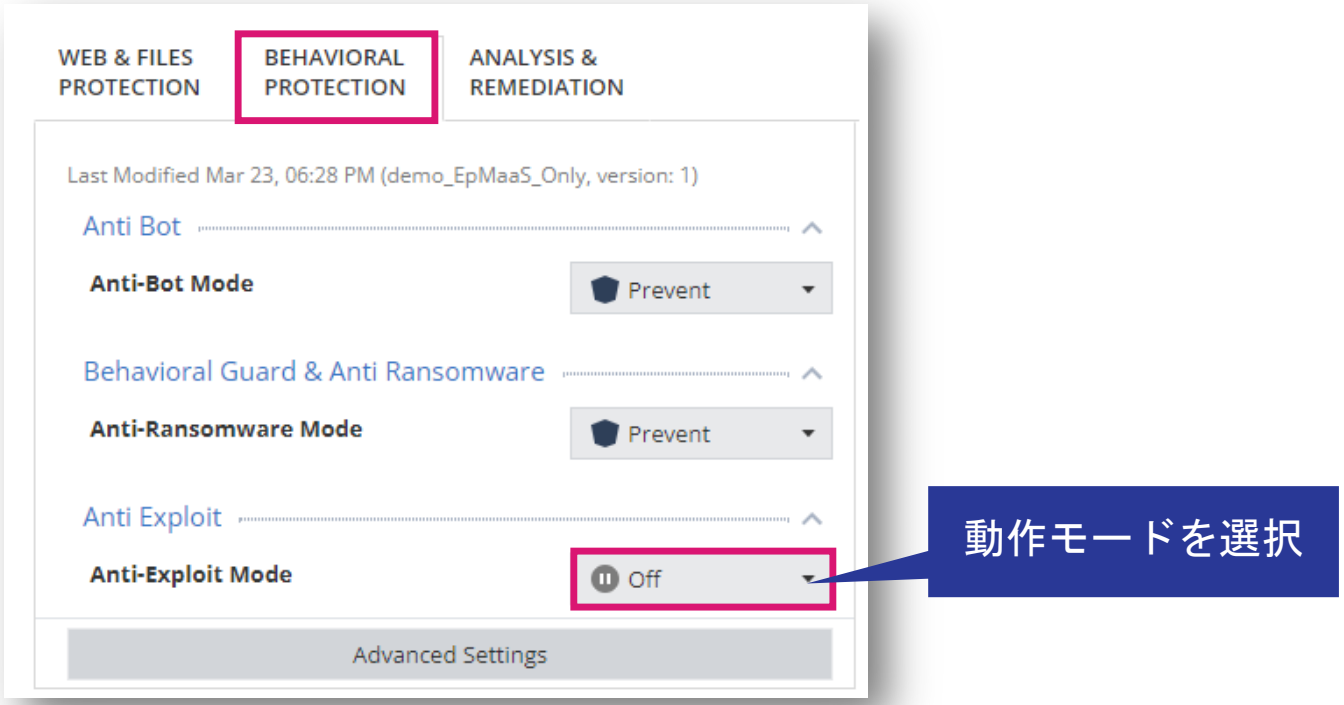
THREAT PREVENTION
ANTI-EXPLOIT

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

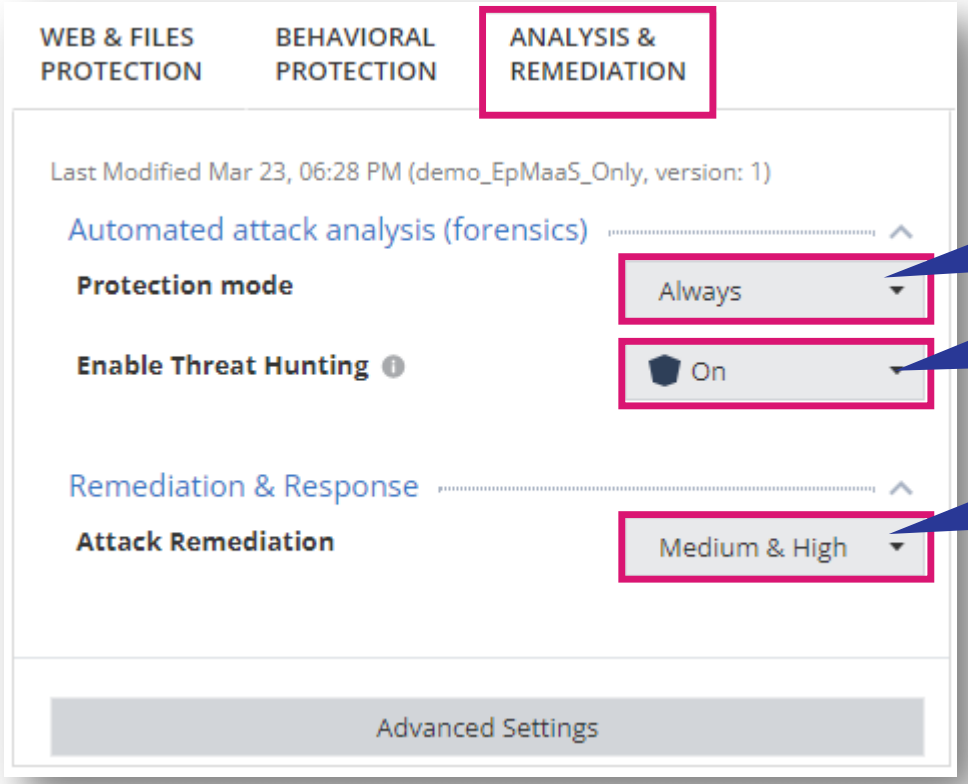
THREAT PREVENTION FORENSICS & REMEDIATION

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

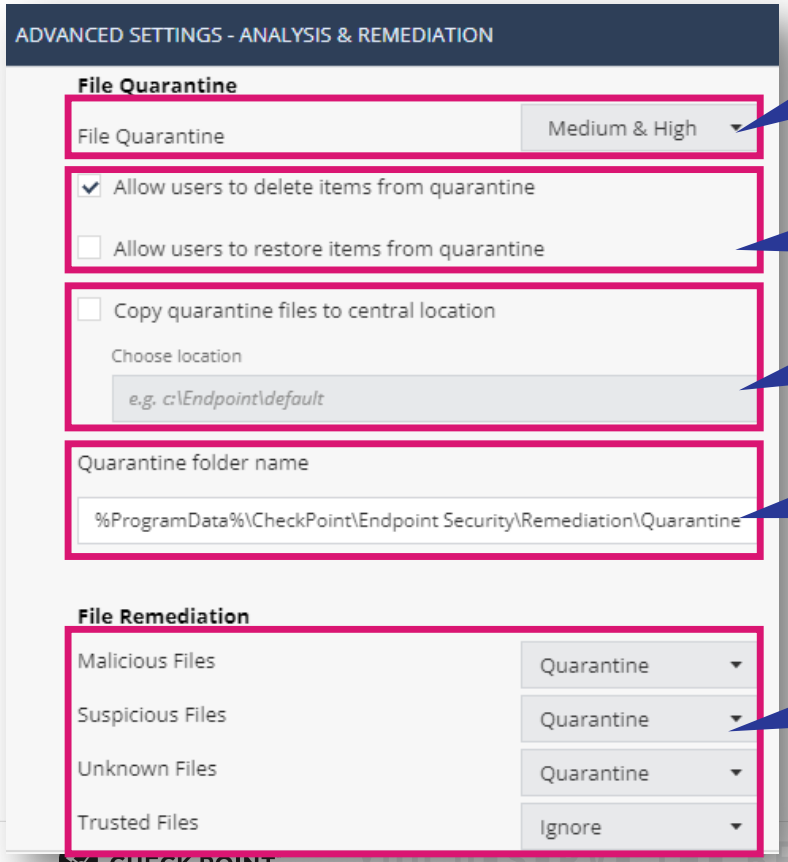
Threat Huntingの有効／無効を選択

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

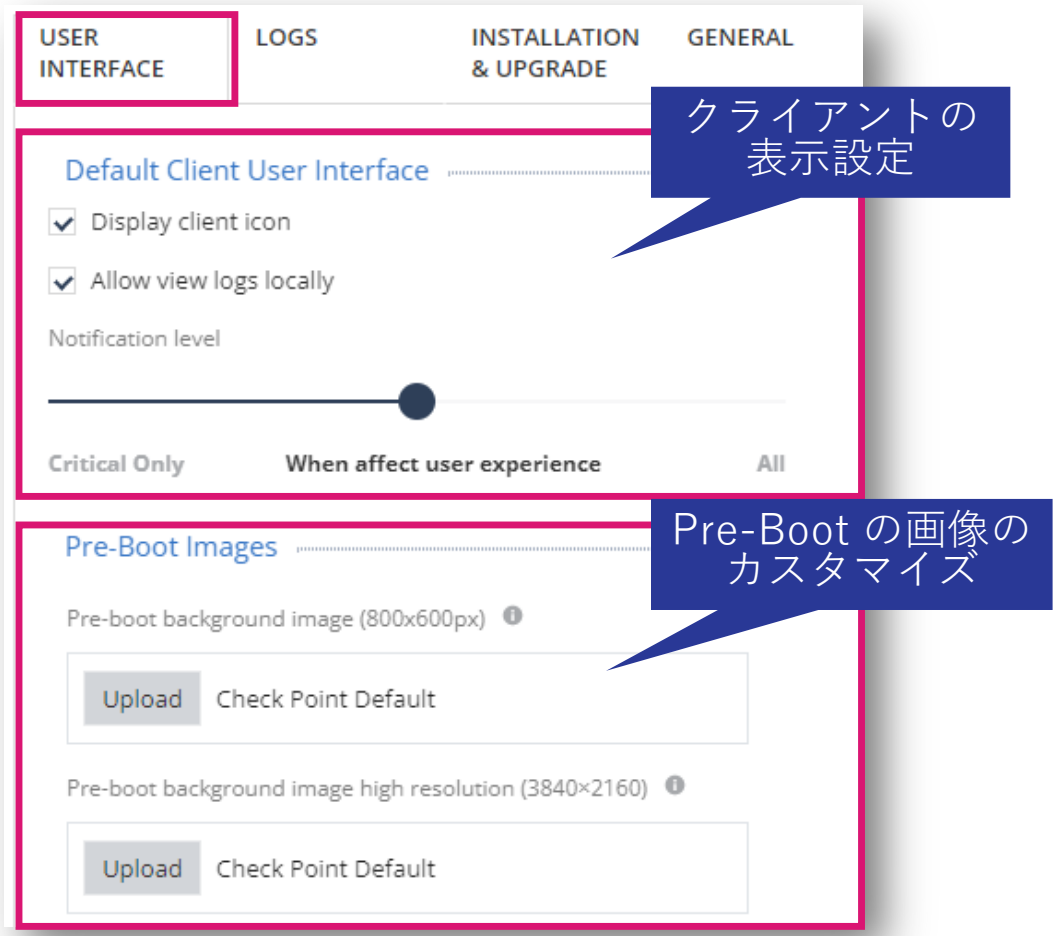
ポリシーの設定

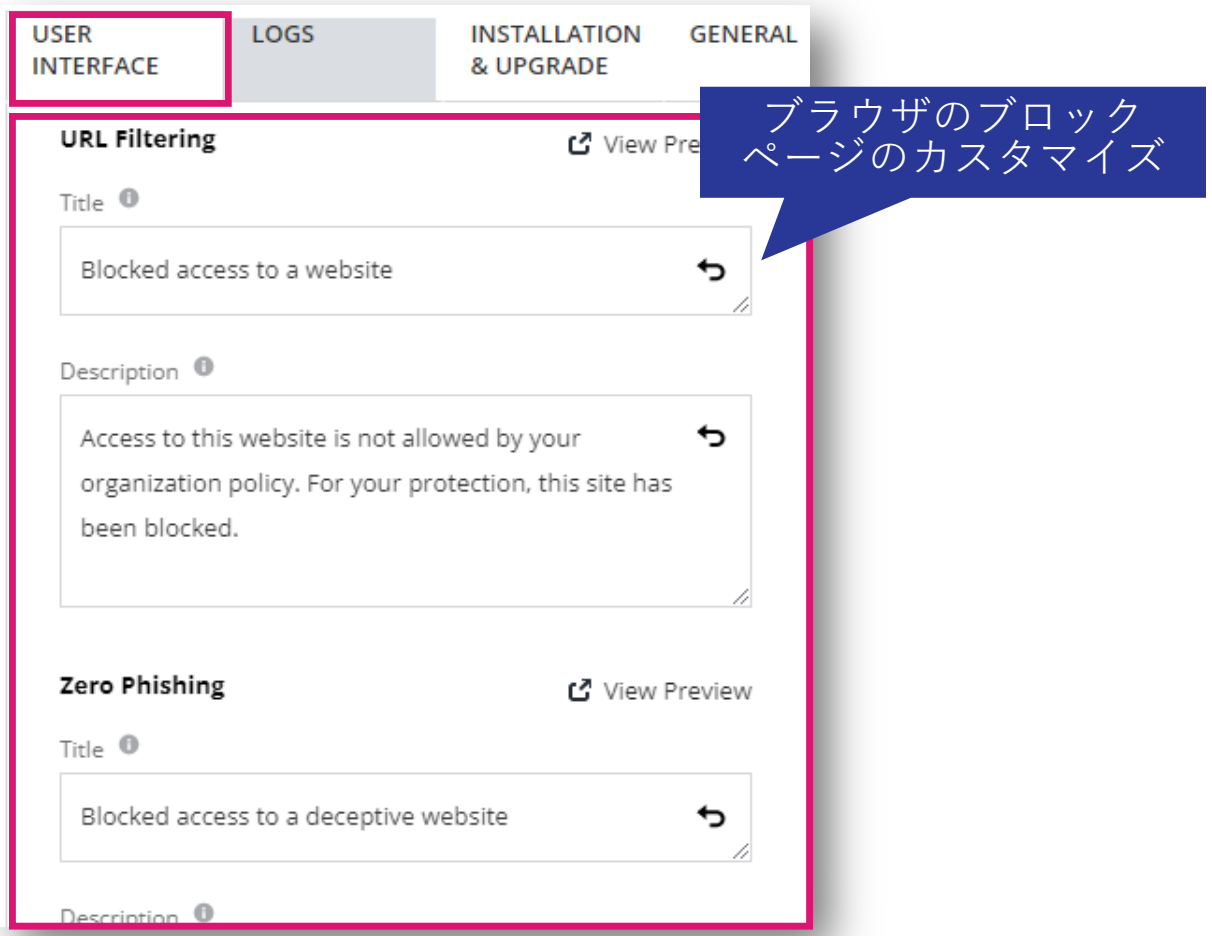
CLIENT SETTINGS USER INTERFACE

Client Settings：User Interface

Policy > Client Settings > User Interface

- クライアントアイコンの表示、ローカルでのログの表示、ユーザへ通知するメッセージのタイプ、画像のカスタマイズ、ブラウザのブロックページのカスタマイズを構成します





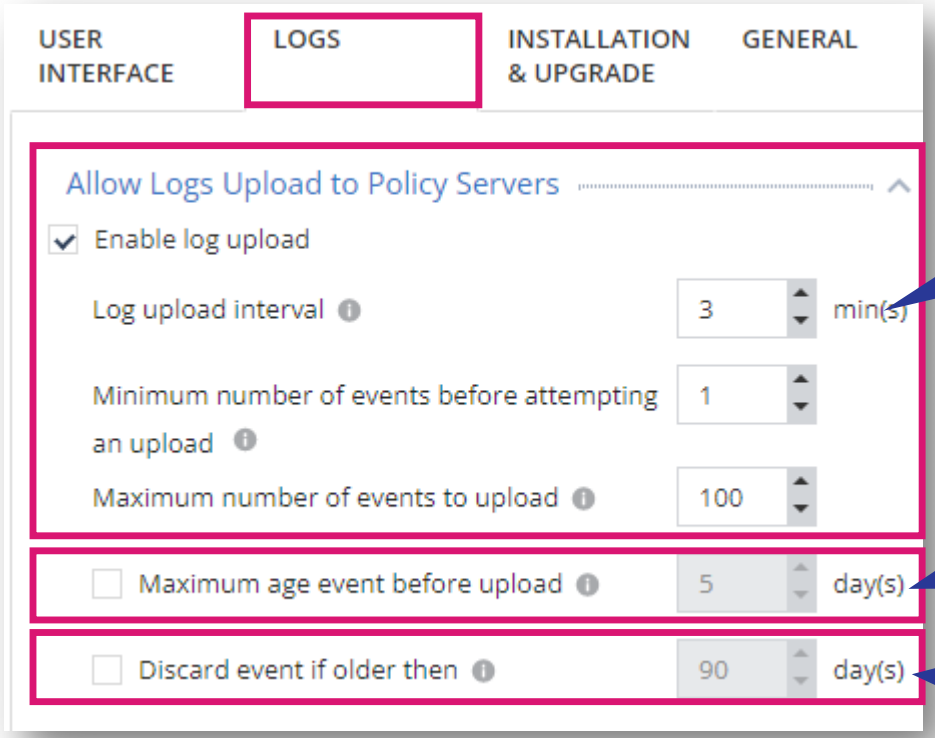
ポリシーの設定

CLIENT SETTINGS LOGS

Client Settings：Logs

Policy > Client Settings > Logs

- ログのアップロードに関する設定を構成します



ログのアップロードの有効化、ログのアップロード間隔などを指定

指定した日数以前にログに記録されたイベントのみアップロードする

指定した日数以前にログに記録されたイベントはアップロードしない

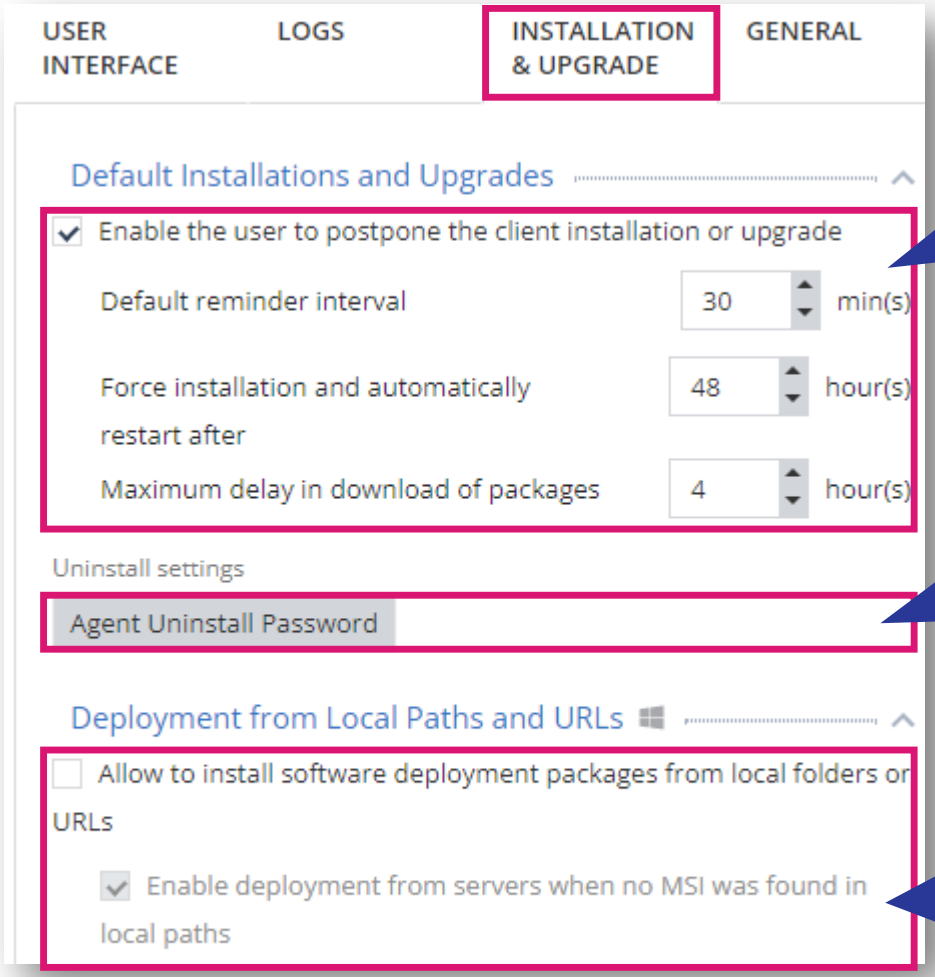
ポリシーの設定

CLIENT SETTINGS
INSTALLATION & UPGRADE

Client Settings：Installation & Upgrade

Policy > Client Settings > Installation & Upgrade

- クライアントのインストール、アンインストール、アップグレードに関する設定を構成します



ユーザによるインストールやアップグレードの延期の許可と設定を構成

クライアントのアンインストールパスワードの設定

オンラインインストール時にクラウド以外からパッケージをインストールする場合の設定（対象：Windows）

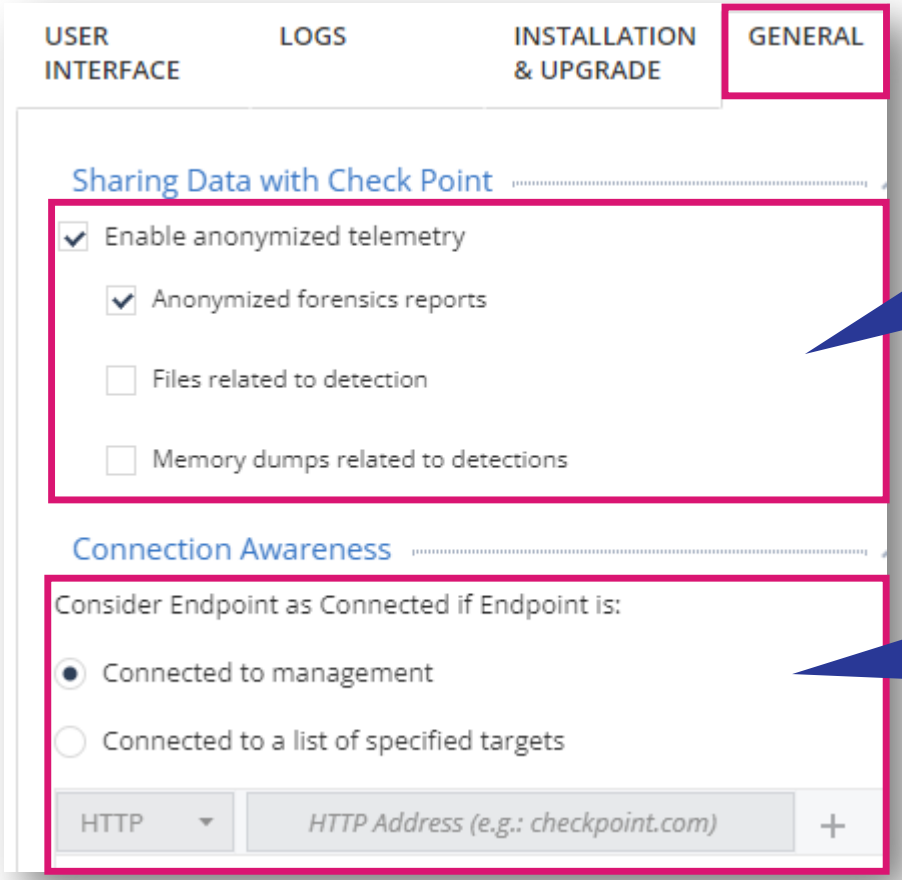
ポリシーの設定

CLIENT SETTINGS GENERAL

Client Settings：General

Policy > Client Settings > General

- 検出された感染やボットに関する情報をチェックポイントと共有する設定を構成します
- コンピュータの接続状態を判断する方法を構成します



チェックポイントとの情報共有設定を構成

コンピュータの接続状態を判断する方法を構成

サーバ最適化

サーバ最適化とは

サーバ最適化とは

- Policy 設定で「サーバ最適化」を有効にすることで、Windows サーバの役割ごとに事前定義された除外設定が自動的に適用されます
- サーバ最適化は、以下の Windows サーバに対して適用できます
  - Domain Controller
  - Exchange Server
  - SharePoint 2016 / 2013 / 2010 / 2007
  - SQL Server
  - Terminal Server

注: サーバ最適化による除外設定は、Exclusion Center には表示されません

サーバ最適化設定

設定シナリオ

1. サーバ最適化を設定する Windows サーバの役割ごとに、バーチャルグループを作成します
   - 簡易設定ガイドの「バーチャルグループによる管理」を参照してください

2. 作成したバーチャルグループを指定したインストールパッケージを作成します
   - 簡易導入ガイドの「インストールパッケージの作成とダウンロード」を参照してください

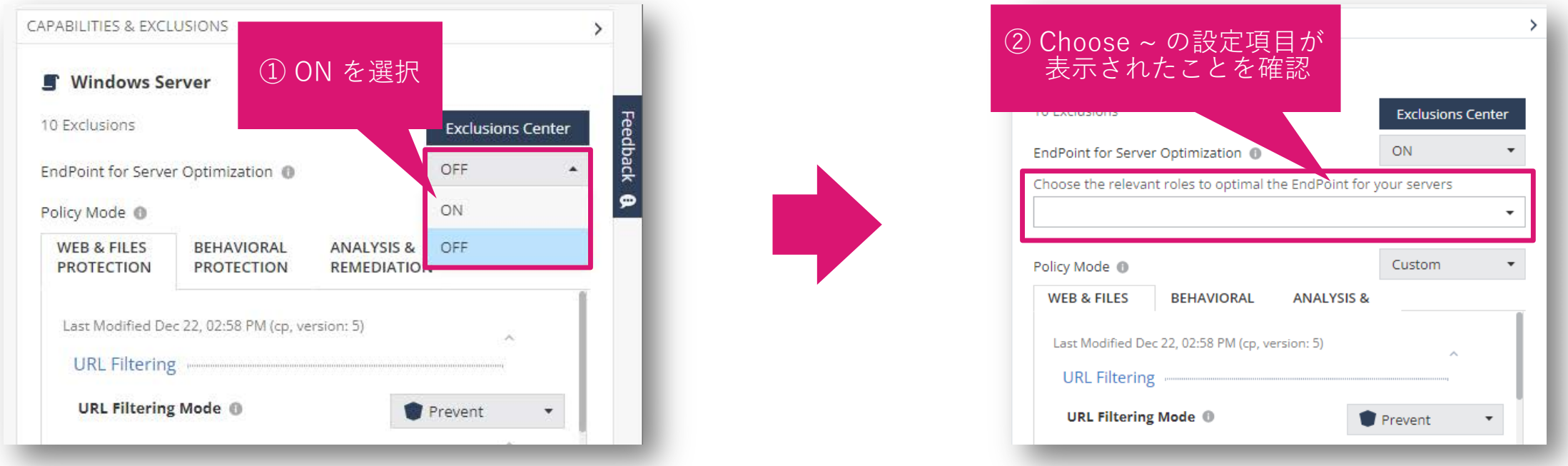
3. 作成したバーチャルグループ に適用する Policy ルールを作成します
   - 簡易設定ガイドの「バーチャルグループによる管理」を参照してください

4. Policy ルールで「サーバ最適化」を有効化します

5. Windows サーバに、クライアントソフトウェアをインストールします

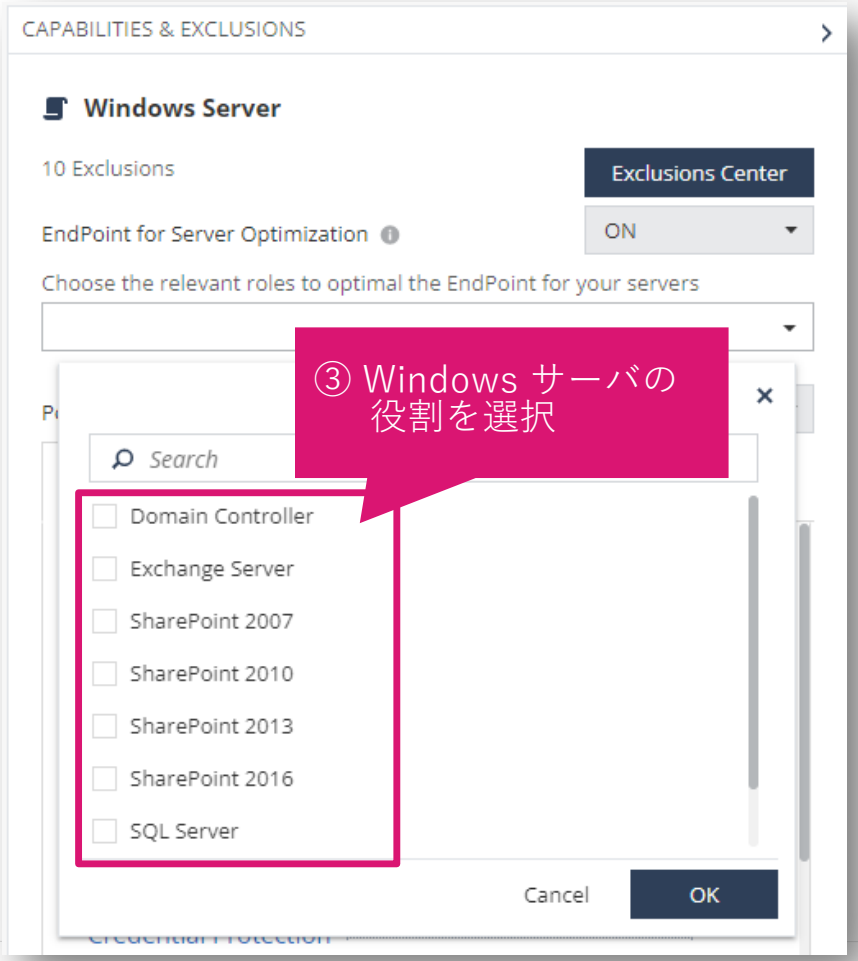
サーバ最適化設定（１／３）

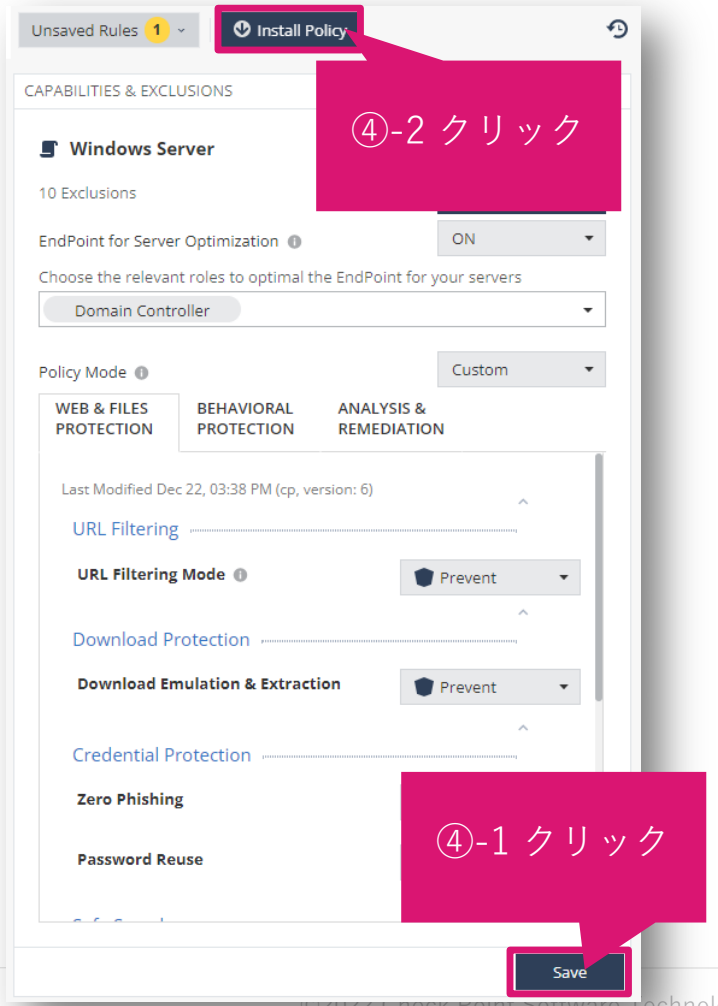
1. Policy 画面の EndPoint for Server Optimization のドロップダウンリストで、「ON」を選択します
2. Choose the relevant roles to optimal the EndPoint for your servers のドロップダウンリストが表示されます



サーバ最適化設定（２／３）

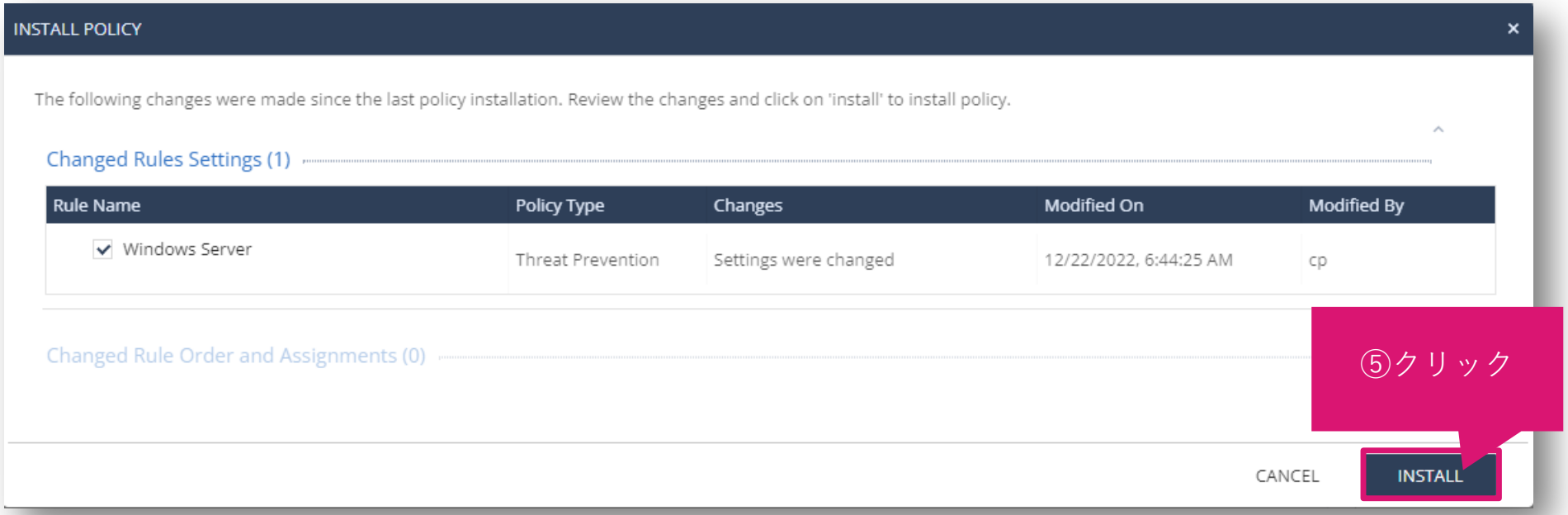
3. Choose the relevant roles to optimal the EndPoint for your servers のドロップダウンリストで、Windows サーバの役割を選択し、「OK」をクリックします
4. 「Save」をクリックし、「Install Policy」をクリックします





サーバ最適化設定（３／３）

5. INSTALL POLICY の画面が表示されたら、 「INSTALL」をクリックします



THANK YOU

YOU DESERVE THE BEST SECURITY