



HARMONY ENDPOINT 簡易運用ガイド

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、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。

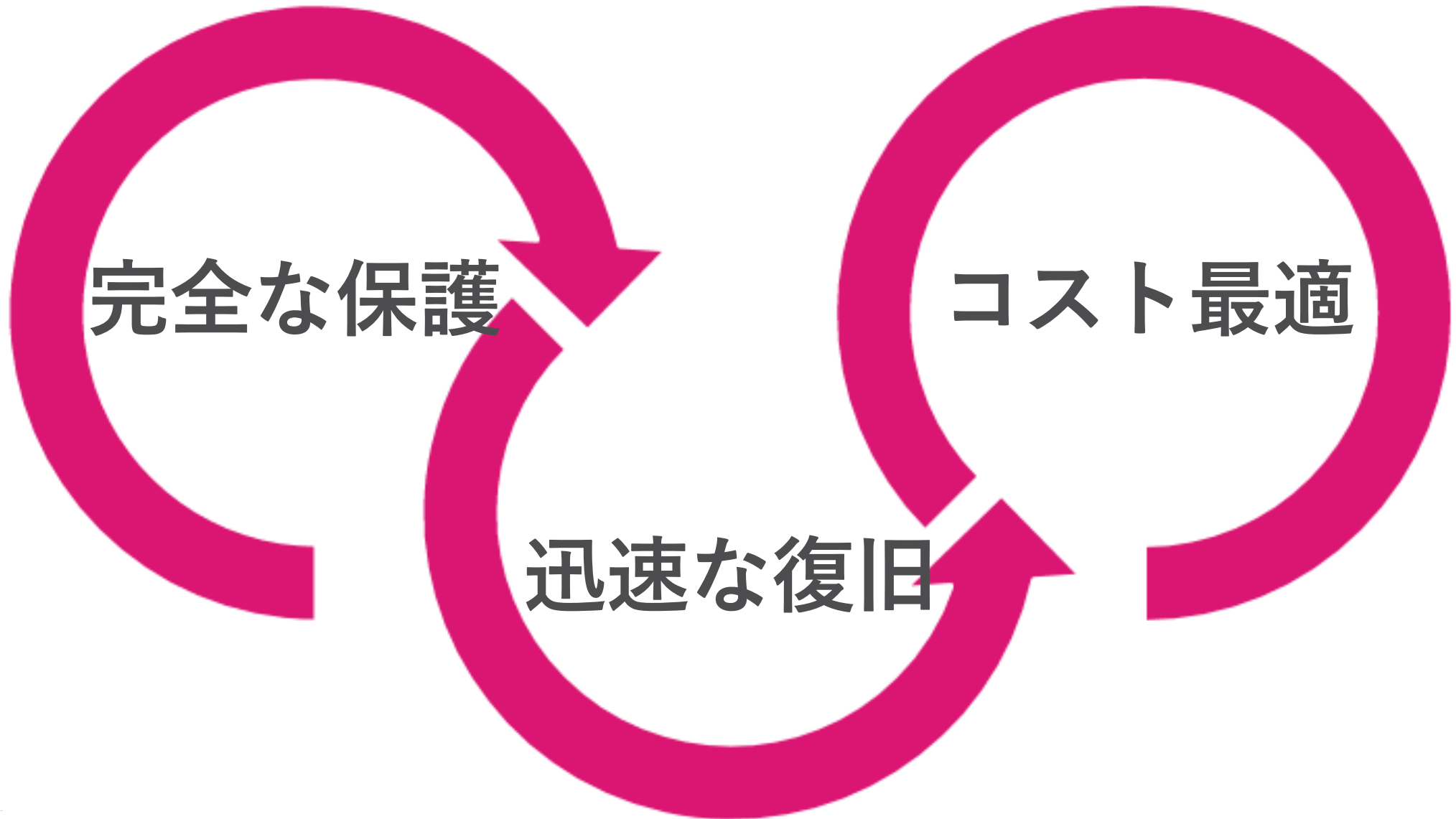
YOU DESERVE THE BEST SECURITY

Table of Contents

- Harmony Endpoint の特徴
- Infinity Portal へのサインイン
- 除外設定（共通）
 - 除外設定の概要
 - 除外メニューでの設定方法
 - ログからの設定方法
- 除外設定（URL フィルタリング）
 - ブラックリスト、ホワイトリストの概要
 - URL フィルタリングのブラックリスト設定
 - URL フィルタリングのホワイトリスト設定
 - ログの表示内容
- 除外設定（Threat Emulation(Web)、Threat Extraction、Zero-Phising）
- コンピュータ情報の管理
- 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
- クライアントのアップグレード
- クライアントのアンインストール
 - Push Operations
 - コントロールパネル
- VPN サイト設定の追加
- CPinfo（サポートログ）の取得

HARMONY ENDPOINTの特徴

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



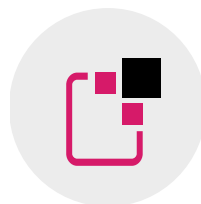
Threat Hunting

Harmony Endpoint の先進の防御技術



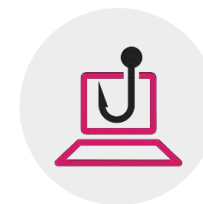
サンドボックス

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

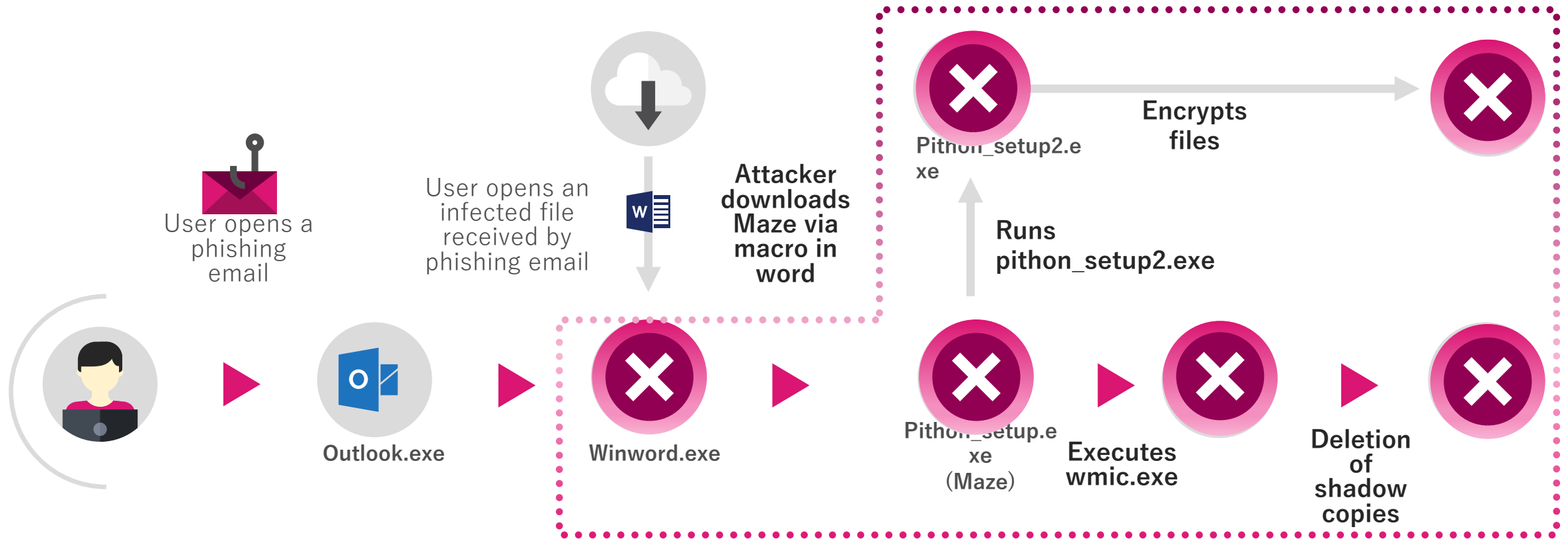
検知、調査、修復作業の 90% を自動化

自動化

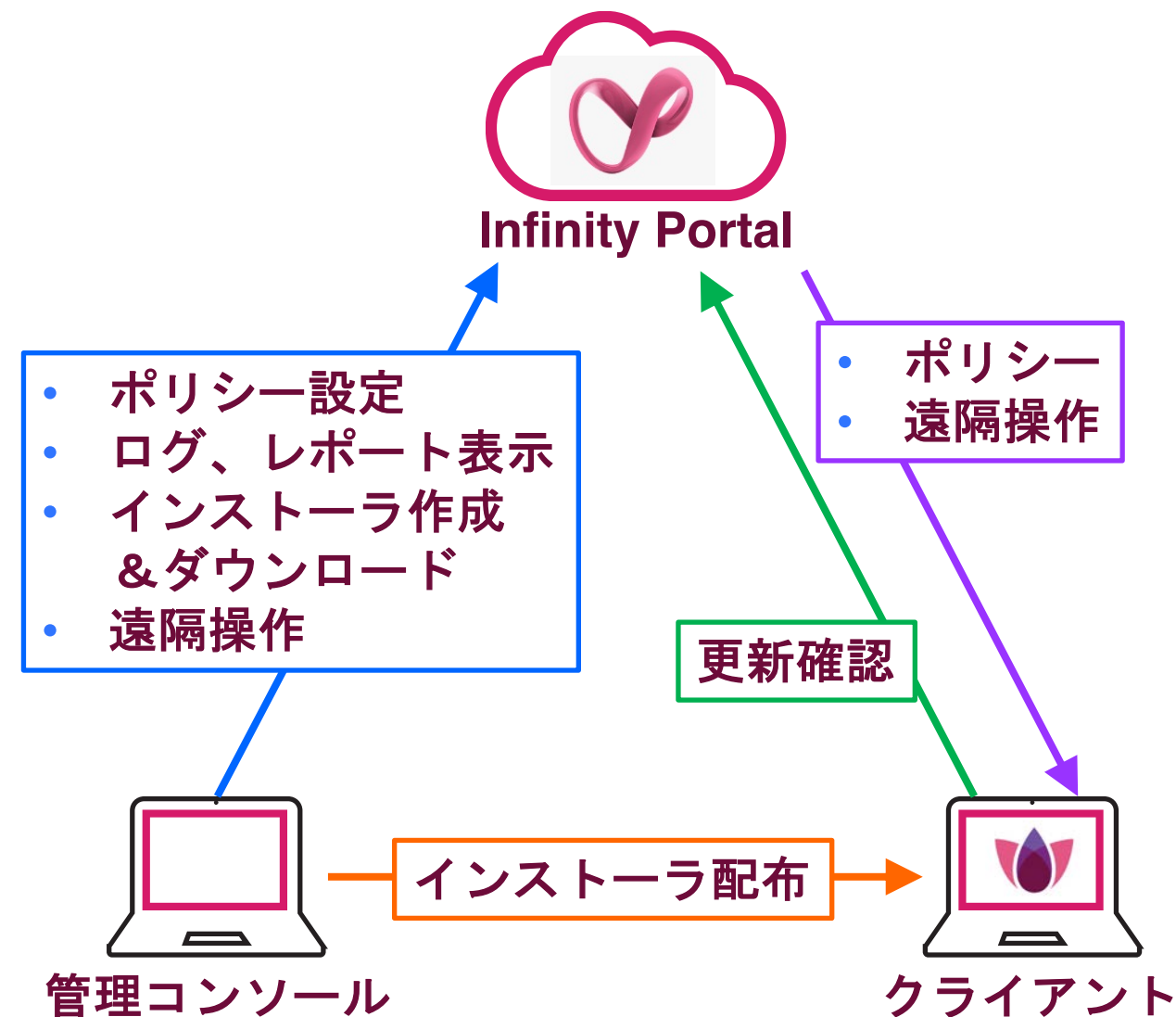
- あらゆるイベントを監視、収集
- 攻撃を検知
- 悪意のある活動を隔離
- サイバーキルチェーン全体をクリーンナップ
- 暗号化されたファイルを復元
- フォレンジックレポートを提供



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

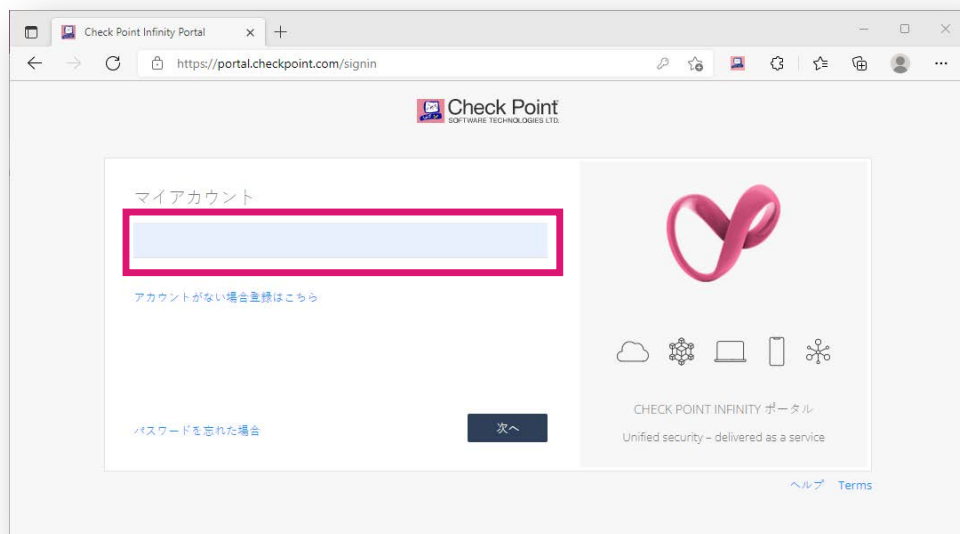
- Infinity Portal にアクセスして管理を行うパソコン
- ブラウザで管理を実施

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

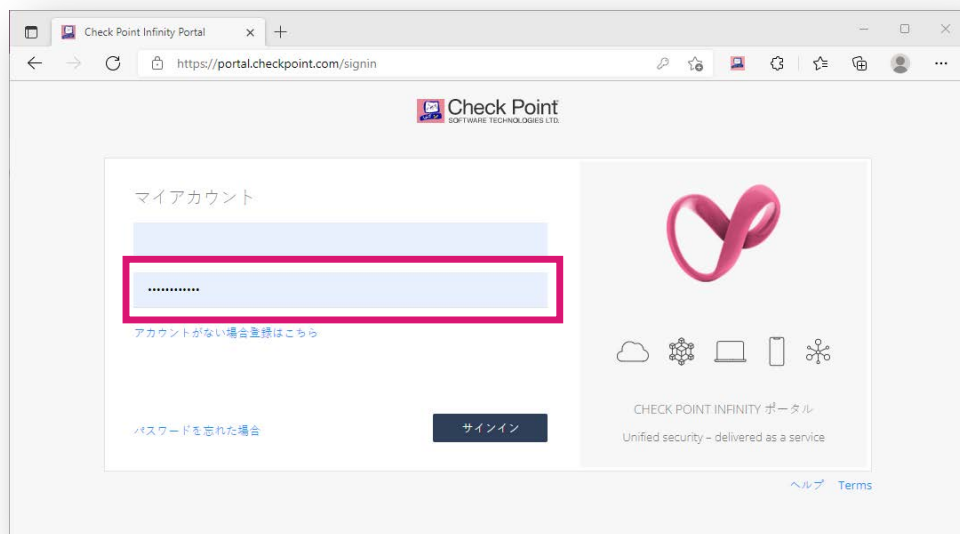
Infinity Portal へのサインイン (1 / 3)



1. Infinity Portal へ接続する

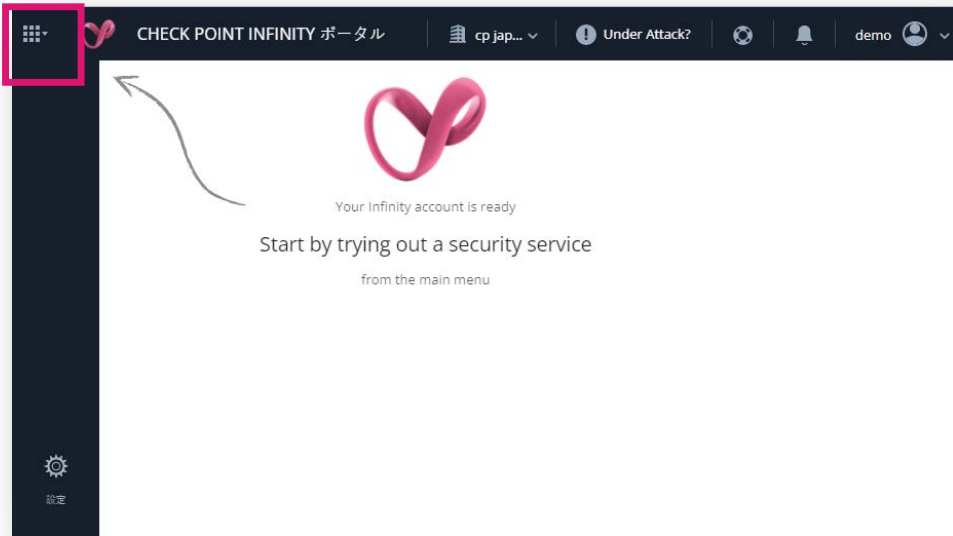
- URL: <https://portal.checkpoint.com/>

2. ユーザー名を入力して、「次へ」を押す



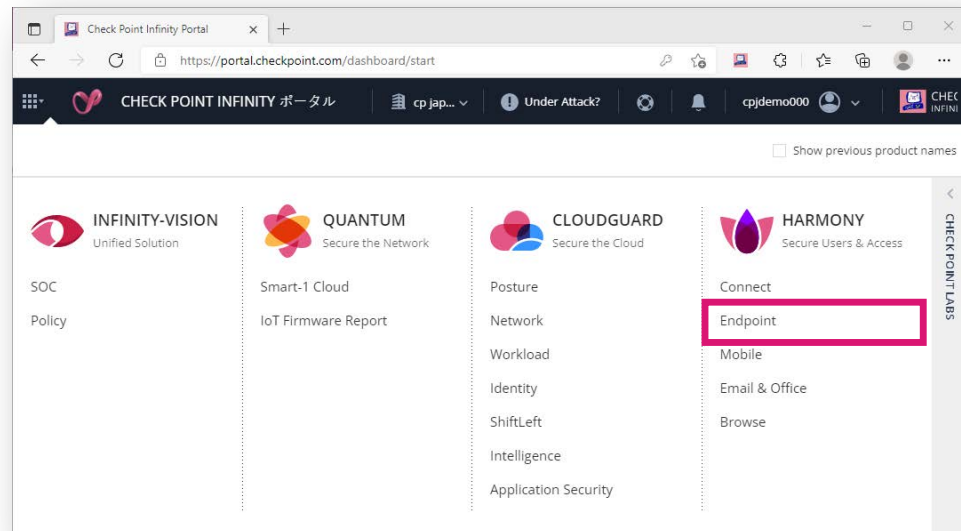
3. パスワードを入力して、「サインイン」を押す

Infinity Portal へのサインイン (2 / 3)



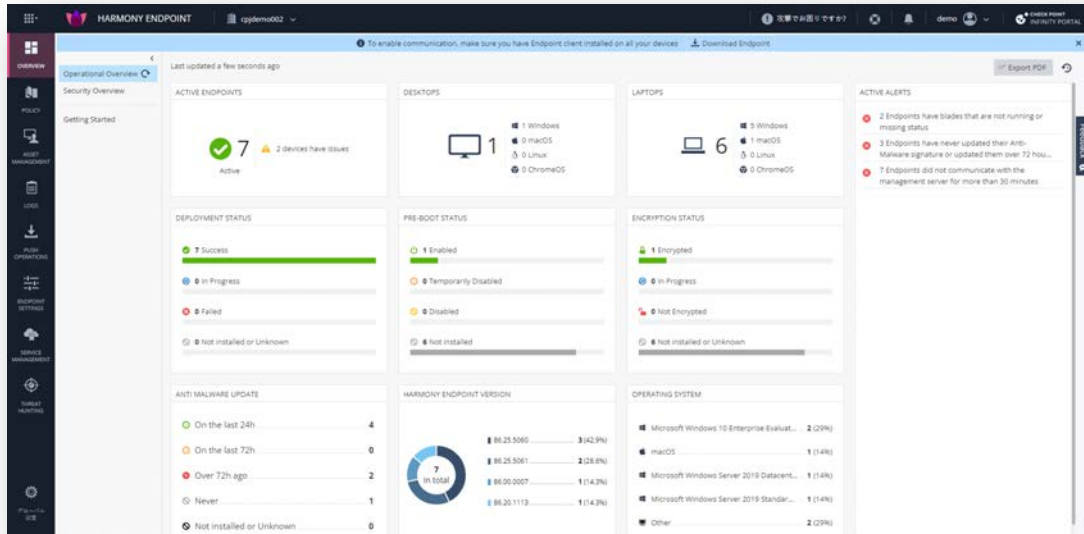
4. サインイン成功

5. 左上のメニューボタン  を押す



6. 「HARMONY Endpoint」を選択する

Infinity Portal へのサインイン (3 / 3)



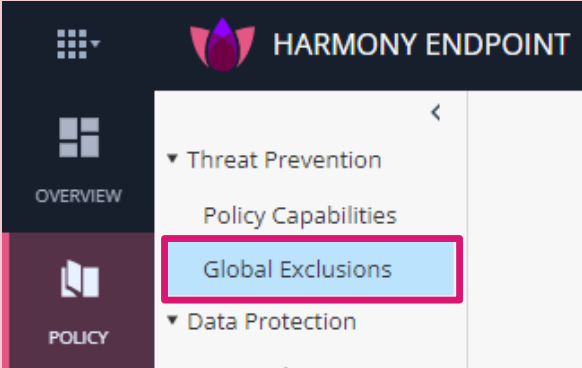
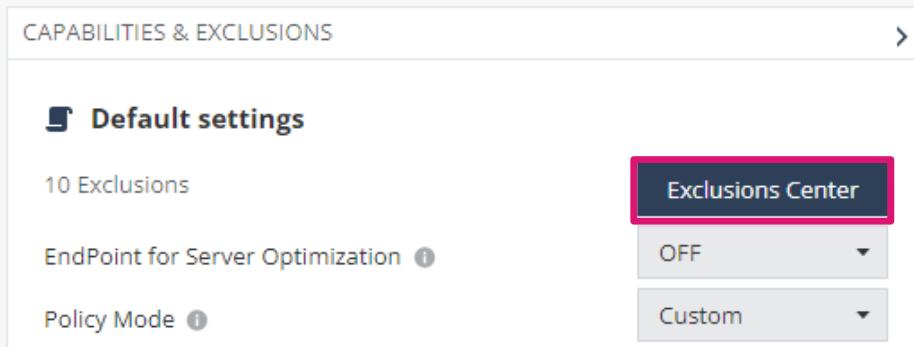
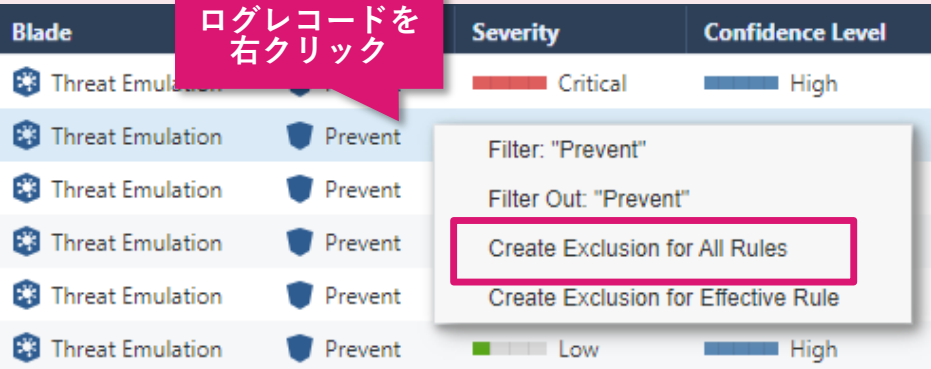

7. Harmony Endpoint の設定画面表示

除外設定（共通）

除外設定の概要

除外設定の概要（1 / 2）

- 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

| 設定方法 \ 適用対象 | 組織全体 | 個別ルール |
|-------------|---|--|
| 除外メニューで作成 |  |  |
| ログから作成 |  |  |

除外設定の概要（2 / 2）

- セキュリティ機能ごとにドメイン名、フォルダパス名、ファイルハッシュ値などで除外指定します
- 除外設定を行うことでセキュリティ機能による脅威の検査が行われなくなります。Web サイトやファイル等の安全性を確認した上で慎重に実施してください

| セキュリティ機能 | 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 | | | | |

除外メニューでの設定方法

Policy 画面から除外設定の一覧画面を表示

- 組織全体に適用する除外設定を作成する場合は、Policy 画面で Global Exclusions をクリックします
- 個別ルールに適用する除外設定を作成する場合は、Policy > Policy Capabilities 画面で除外設定を適用するルールを選択して、Exclusion Center をクリックします
- 除外設定の一覧画面が開きます（次ページ）

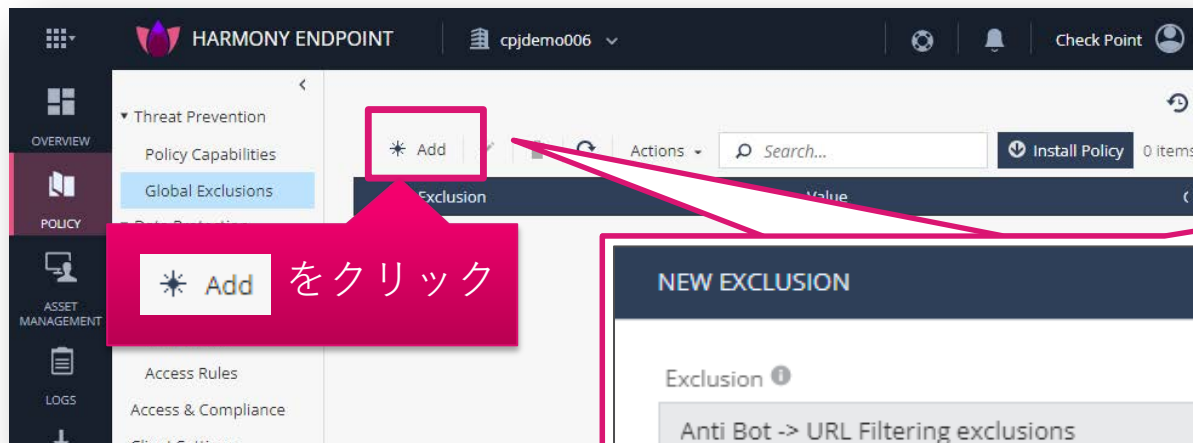
The screenshot shows the 'Policy Capabilities' page in the Check Point Harmony ENX interface. The left sidebar has 'POLICY' highlighted in a red box. A blue callout bubble points to 'Global Exclusions' with the text '② 組織全体に適用する除外設定を作成'. A green callout bubble points to the 'POLICY' menu item with the text '① Policy 画面を表示'. A red callout bubble points to a table row with the text '② 除外設定を適用するルールを選択'. Another red callout bubble points to the 'Exclusions Center' button with the text '③ 個別のルールに適用する除外設定を作成'. The table has columns '#', 'Rule Name', and 'Applied To'. The first row is highlighted in blue and contains '0', 'Eval', and 'Eval'. The right side of the page shows configuration options for 'EndPoint for Server Optimization' and 'Policy Mode'.

| # | Rule Name | Applied To |
|---|------------------|------------|
| 0 | Eval | Eval |
| 1 | Default settings | |
| | Def... | |

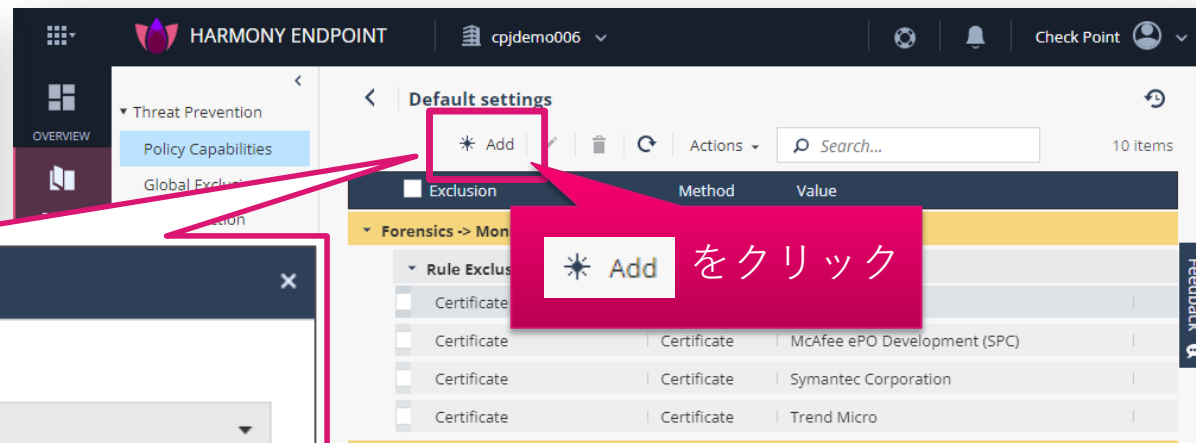
除外設定の作成画面を表示

- Global Exclusions もしくは、Exclusion Center の画面で、* Add をクリックします
- NEW EXCLUSION 画面が開きます

Global Exclusions での全組織への適用



Exclusion Center での個別ルールへの適用



The screenshot shows the 'NEW EXCLUSION' dialog box. The dialog is titled 'NEW EXCLUSION' and contains the following fields and options:

- Exclusion:** Anti Bot -> URL Filtering exclusions
- Method:** Domain/URL
- Value:** (Empty text input field)
- Add to all rules

Buttons: CANCEL, OK

除外設定を作成するセキュリティ機能を選択

1. NEW EXCLUSION の画面で、「Exclusion」のドロップダウンリストをクリックします
2. 除外設定を作成するセキュリティ機能を選択します
 - セキュリティ機能によっては、セキュリティ機能と除外方法がセットになっています
3. 選択したセキュリティ機能の除外設定を作成する画面に切り替わります

NEW EXCLUSION

Exclusion ⓘ

Anti Bot -> URL Filtering exclusions

Anti-Malware -> Exclude Infection by name

Anti-Malware -> Process exclusions (on-access only)

Anti-Malware -> File & Folder exclusions (system, scheduled and on-...

Forensics -> Quarantine Exclusions

Forensics -> Anti Ransomware and Behavioral Guard

Forensics -> Monitoring exclusions

Threat Emulation, Extraction and Zero Phishing Exclusions

Threat Emulation -> Anti Exploit Exclusions

① 「Exclusion」のドロップダウンリストをクリック

② 除外設定を作成するセキュリティ機能を選択

NEW EXCLUSION

Exclusion ⓘ

Threat Emulation, Extraction and Zero Phishing Exclusions

Method

Domain

Value *

Comment

CANCEL OK

③ 選択したセキュリティ機能の除外設定画面に切り替わったことを確認

除外方法を選択し、除外条件を設定

1. 「Method」のドロップダウンリストをクリックします
2. 除外方法を選択します
3. 「Value」に除外条件を入力します
4. 「OK」をクリックします

NEW EXCLUSION

Exclusion ⓘ
Threat Emulation

Method
Domain

Domain
Folder
SHA1 Hash

① 「Method」のドロップダウンリストをクリック

② 除外方法を選択

CANCEL OK



NEW EXCLUSION

Exclusion ⓘ
Threat Emulation, Extraction and Zero Phishing Exclusions

Method
Domain

Value *
www.checkpoint.sc

Comment

③ 除外条件を入力

④ クリック

CANCEL OK

除外設定を適用（組織全体に適用する場合）（2 / 2）

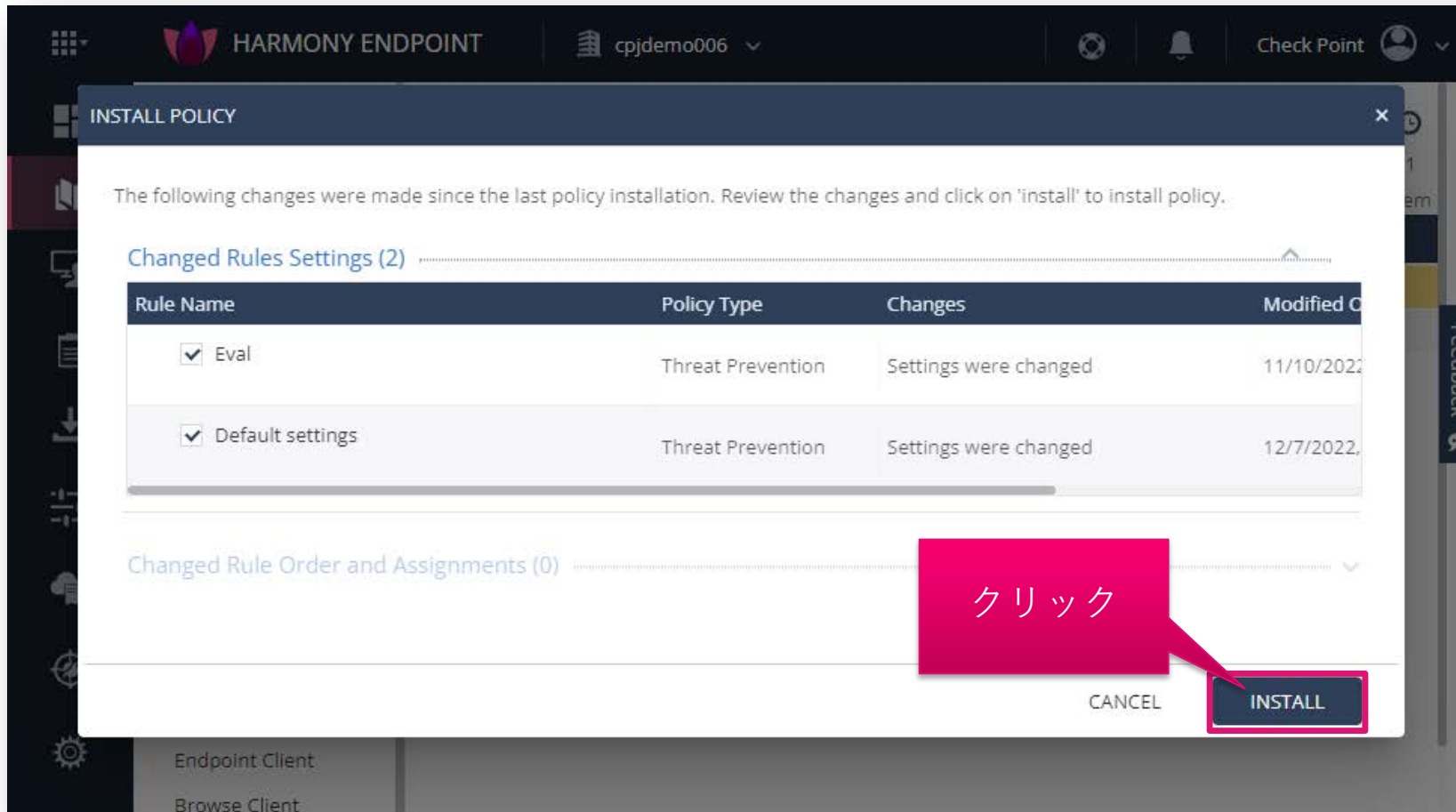
1. Global Exclusions の画面が表示され、除外設定が作成されていることを確認します
2. 「Save」をクリックします
3. 「Install Policy」をクリックします

The screenshot shows the 'Global Exclusions' configuration page in the Harmony Endpoint console. The left sidebar contains a navigation menu with 'Global Exclusions' selected. The main content area shows a table of exclusions. A callout box labeled '① 除外設定が作成されたことを確認' points to a row in the table with the domain 'www.checkpoint.sc'. Another callout box labeled '② クリック' points to the 'Save' button at the bottom right. A third callout box labeled '③ クリック' points to the 'Install Policy' button at the top right.

| Exclusion | Domain | Domain | www.checkpoint.sc |
|-----------|--------|--------|-------------------|
| + | Domain | Domain | www.checkpoint.sc |

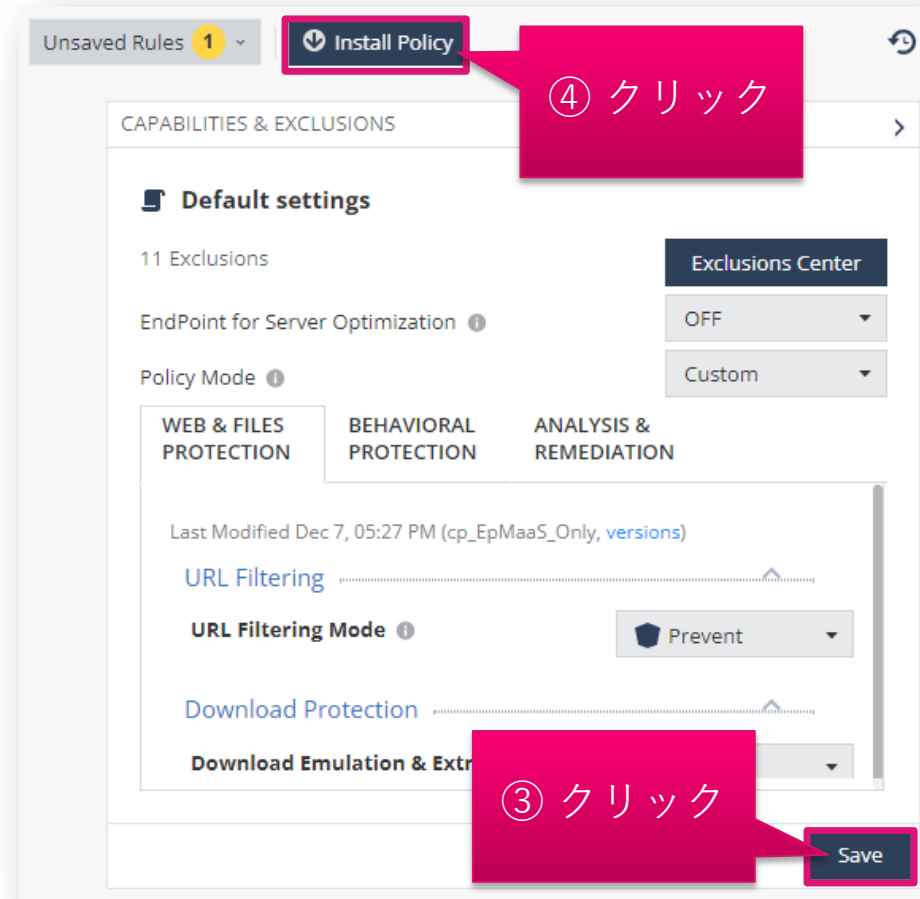
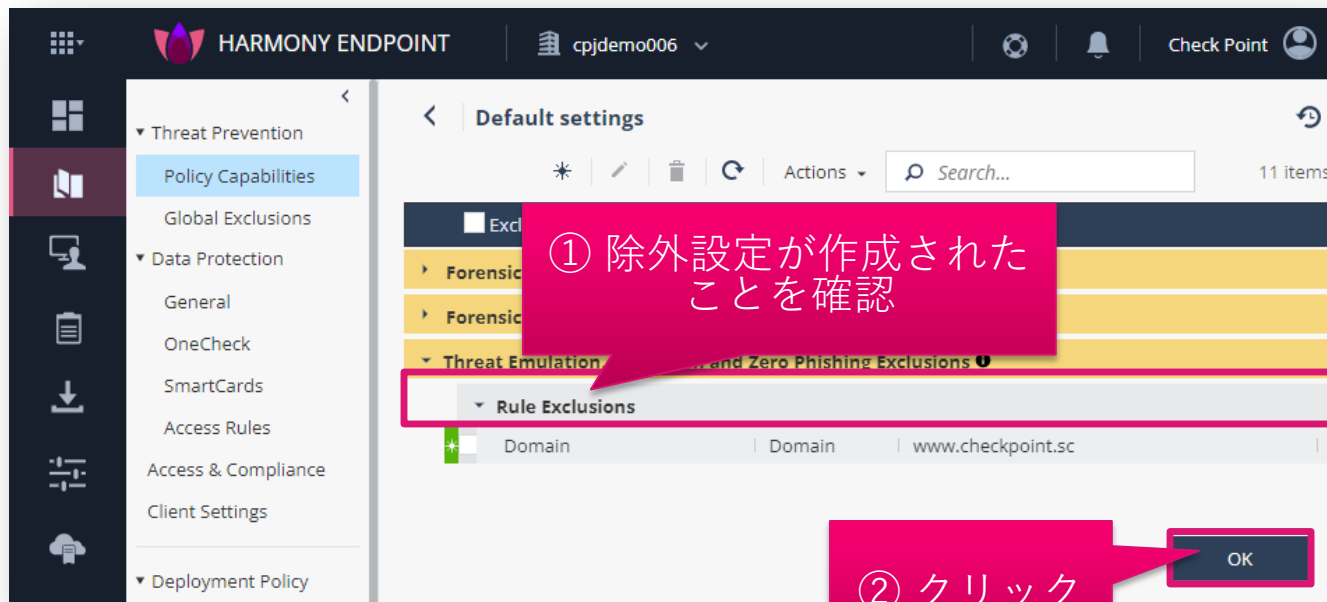
除外設定を適用（組織全体に適用する場合）（2 / 2）

- INSTALL POLICY の画面が表示されたら、「INSTALL」をクリックします
- 以上で、除外設定の適用は完了です
- 10分程度でクライアントにポリシーが反映されます



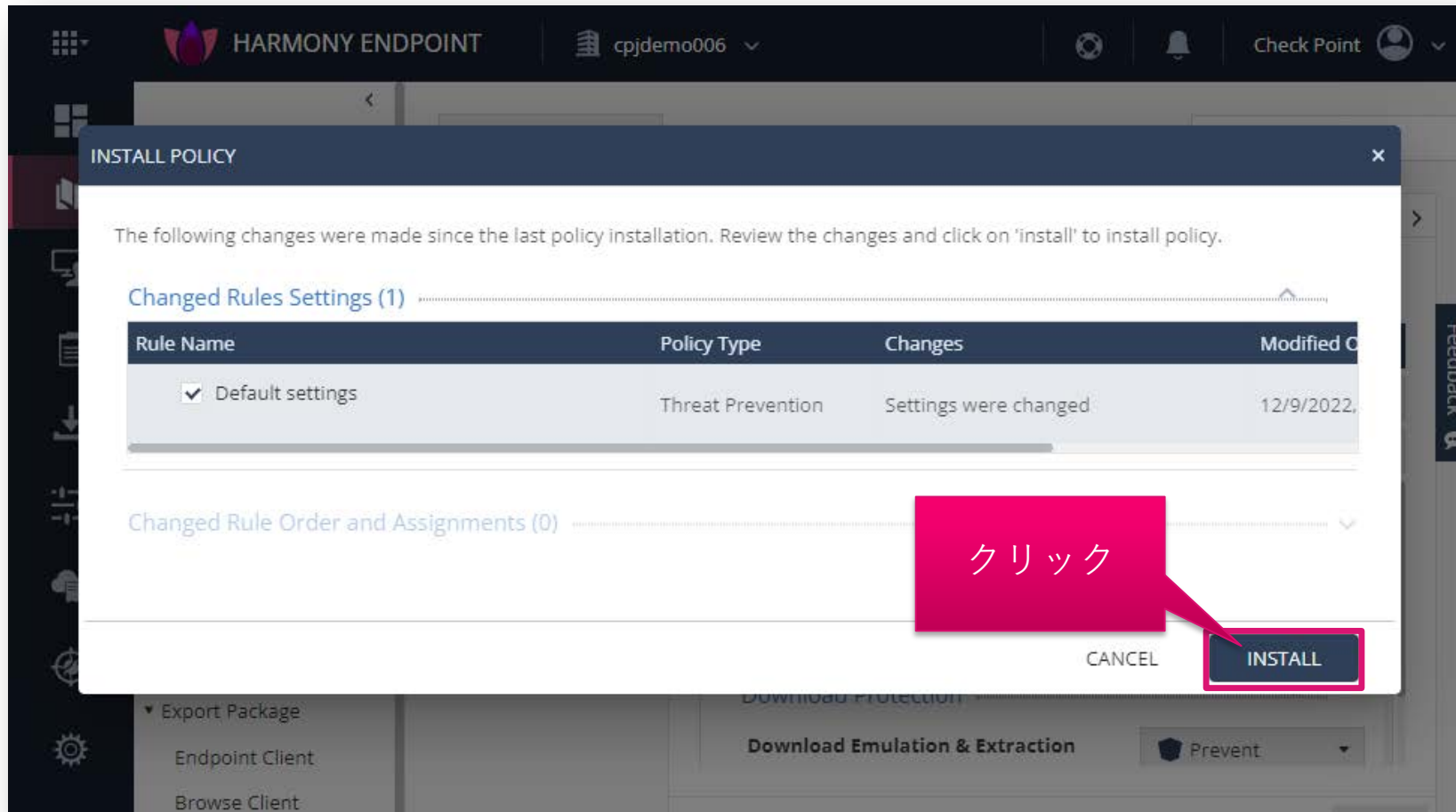
除外設定を適用（個別ルールに適用する場合）（1 / 2）

1. Exclusion Center の画面が表示され、除外設定が作成されていることを確認します
2. 「OK」をクリックします
3. Policy Capabilities 画面が表示されたら、「Save」をクリックします
4. 「Install Policy」をクリックします



除外設定を適用（個別ルールに適用する場合）（2 / 2）

- INSTALL POLICY の画面が表示されたら、「INSTALL」をクリックします
- 以上で、除外設定の適用は完了です
- 10分程度でクライアントにポリシーが反映されます



ログからの設定方法

ログレコードを選択して除外設定を作成

- Logs で表示されるログのレコードを右クリックする
- 織全体に適用する除外設定を作成する場合は、「Create Exclusion for All Rules」を選択する
- 個別のルールに適用する除外設定を作成する場合は、「Create Exclusion for Effective Rule」を選択する
- 除外メニューに自動的に除外設定が追加されます（次ページ）

① Logs ページを表示

② ログレコードを選択して右クリック

③ 組織全体に適用する除外設定を作成

③ 個別のルールに適用する除外設定を作成

| Time | Blade | Action | Severity | Action Type |
|--------------------------|------------------|---------|----------|----------------------|
| Oct 31, 2022 2:26:26 PM | Threat Emulation | Prevent | High | HTTP Emulation |
| Oct 31, 2022 2:26:26 PM | Threat Emulation | Prevent | Critical | HTTP Emulation |
| Oct 14, 2022 12:02:34 PM | Threat Emulation | Prevent | High | File Reputation |
| Oct 14, 2022 12:02:34 PM | Threat Emulation | Prevent | High | File Reputation |
| Oct 14, 2022 12:02:34 PM | Threat Emulation | Prevent | High | File Reputation |
| Oct 14, 2022 12:02:34 PM | Threat Emulation | Prevent | High | File Reputation |
| Oct 14, 2022 12:02:34 PM | Threat Emulation | Prevent | High | File Reputation |
| Oct 14, 2022 12:02:34 PM | Threat Emulation | Prevent | High | File Reputation |
| Oct 12, 2022 10:53:51 AM | Threat Emulation | Prevent | High | Static File Analysis |

除外設定を適用（組織全体に適用する場合）（1 / 2）

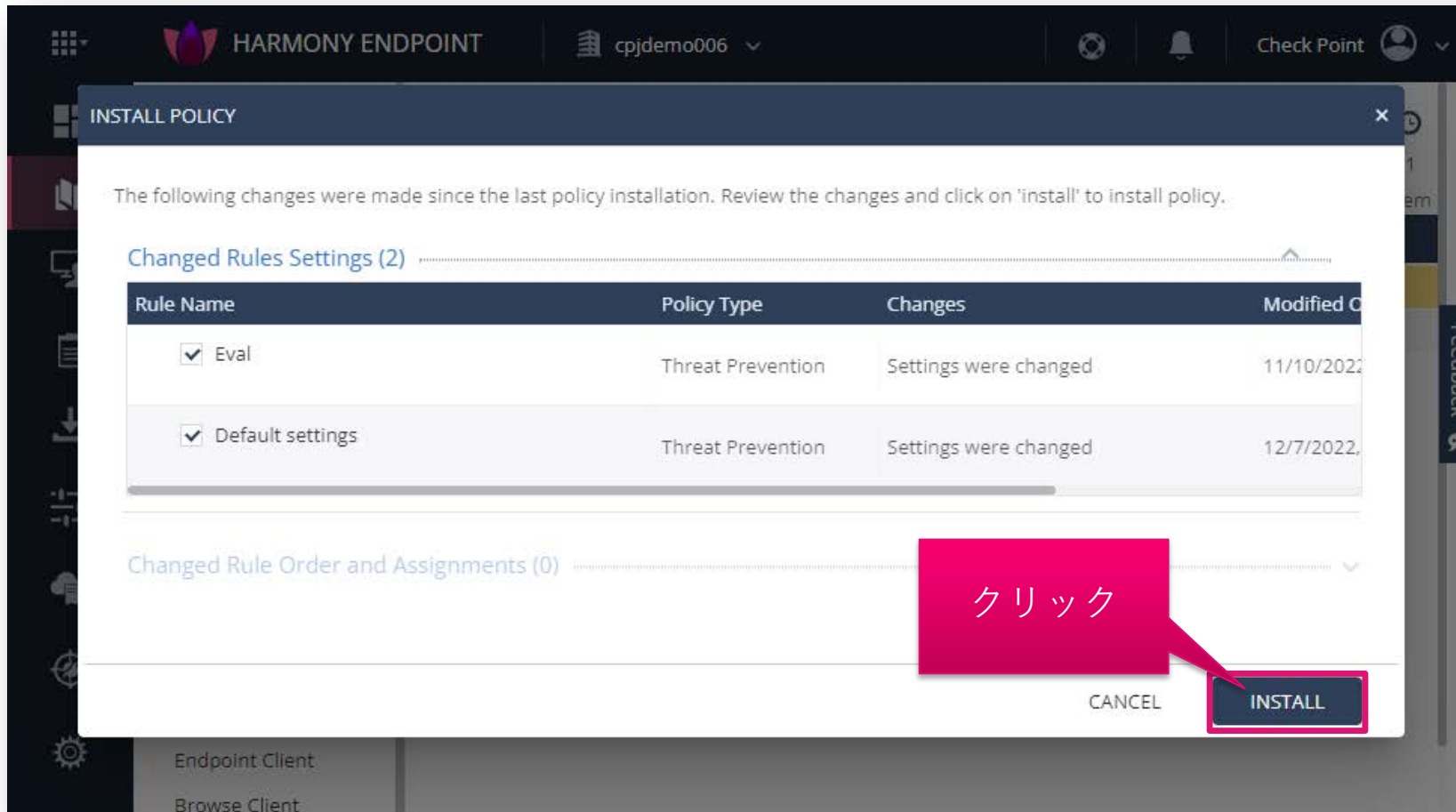
1. Global Exclusions の画面が表示され、除外設定が作成されていることを確認します
2. 「Save」をクリックします
3. 「Install Policy」をクリックします

The screenshot shows the Harmony Endpoint console interface. The left sidebar contains navigation options under Threat Prevention, Data Protection, and Client Settings. The main content area is titled 'Global Exclusions' and shows a table with one exclusion rule. The table has columns for 'Exclusion', 'Domain', and 'www.checkpoint.sc'. A callout box labeled '① クリック' points to the exclusion rule. Another callout box labeled '② クリック' points to the 'Save' button at the bottom right. A third callout box labeled '③ クリック' points to the 'Install Policy' button at the top right.

| Exclusion | Domain | www.checkpoint.sc |
|-----------|--------|-------------------|
| + | Domain | www.checkpoint.sc |

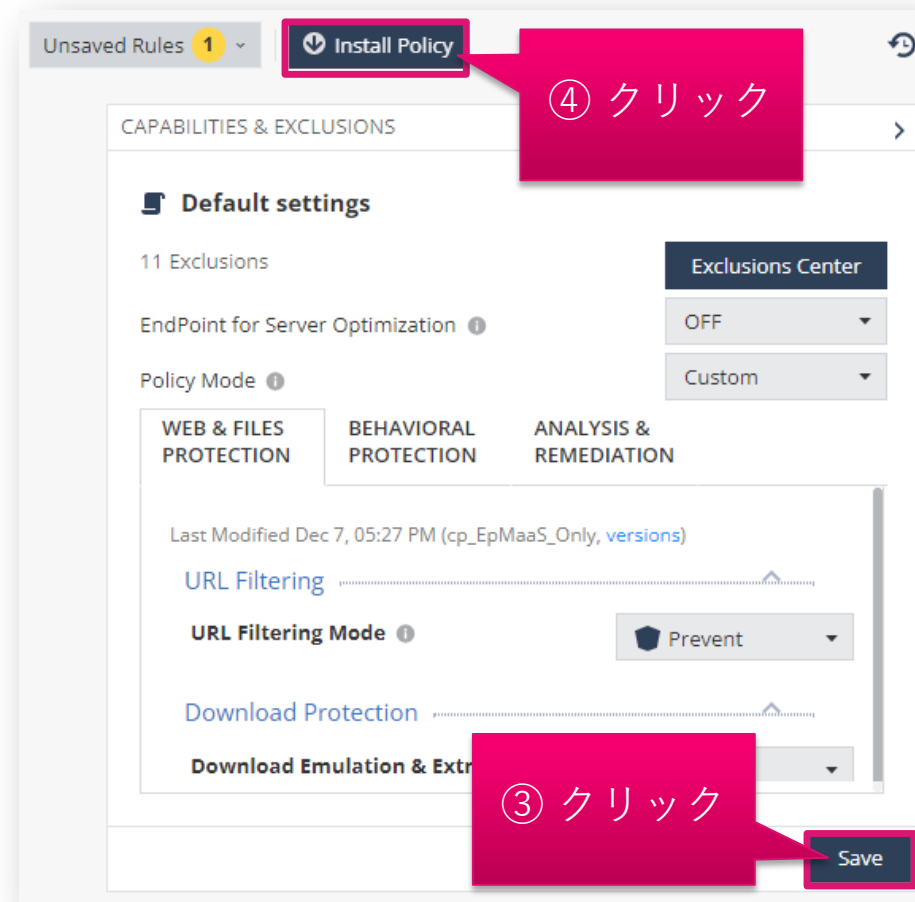
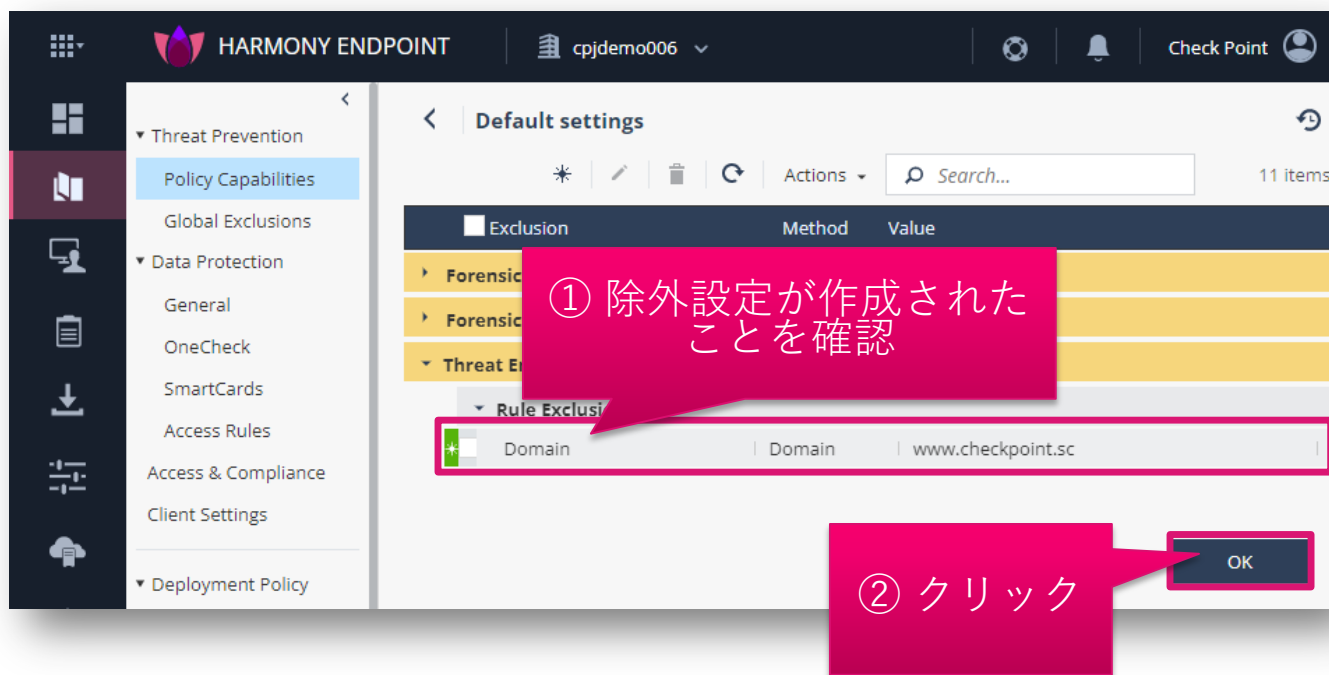
除外設定を適用（組織全体に適用する場合）（2 / 2）

- INSTALL POLICY の画面が表示されたら、「INSTALL」をクリックします
- 以上で、除外設定の適用は完了です
- 10分程度でクライアントにポリシーが反映されます



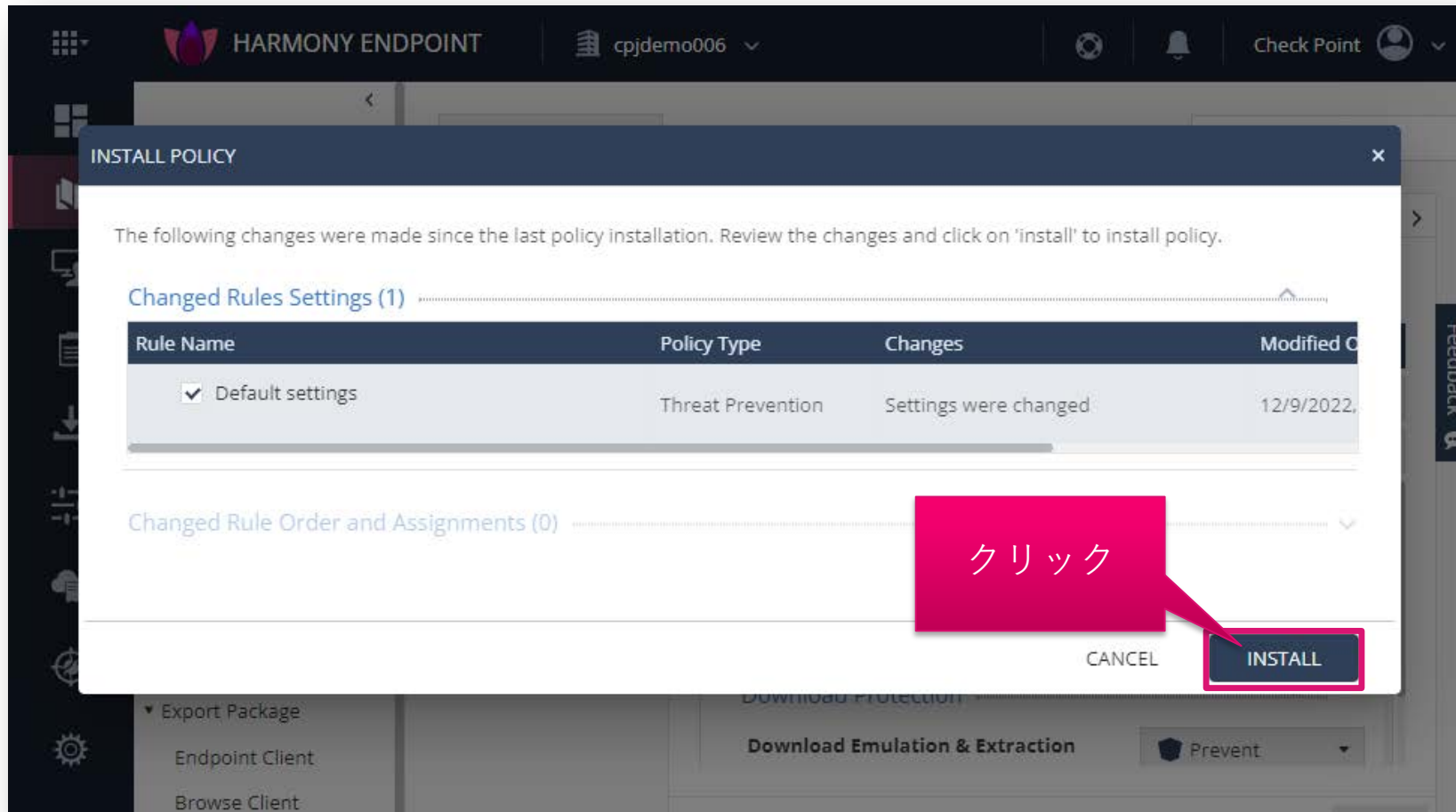
除外設定を適用（個別ルールに適用する場合）（1 / 2）

1. Exclusion Center の画面が表示され、除外設定が作成されていることを確認します
2. 「OK」をクリックします
3. Policy Capabilities 画面が表示されたら、「Save」をクリックします
4. 「Install Policy」をクリックします



除外設定を適用（個別ルールに適用する場合）（2 / 2）

- INSTALL POLICY の画面が表示されたら、「INSTALL」をクリックします
- 以上で、除外設定の適用は完了です
- 10分程度でクライアントにポリシーが反映されます



除外設定 (URL フィルタリング)

URL フィルタリング

ブラックリスト、ホワイトリストの概要

ブラックリスト、ホワイトリストの概要

- ブラックリストは、URL フィルタリングのカテゴリベースの制御で許可されている Web サイトを個別に指定して、閲覧を禁止します
 - 例: Computers / Internet カテゴリは閲覧を許可するが、ソフトウェア配布サイトは閲覧を禁止する
- ホワイトリストは、URL フィルタリングのカテゴリベースの制御で禁止されている Web サイトを個別に指定して、閲覧を許可します
 - 例: Shopping カテゴリは閲覧を禁止するが、会社で使用しているオフィス用品購入サイトは閲覧を許可する



URL フィルタリングのブラックリスト設定

ブラックリスト設定の概要

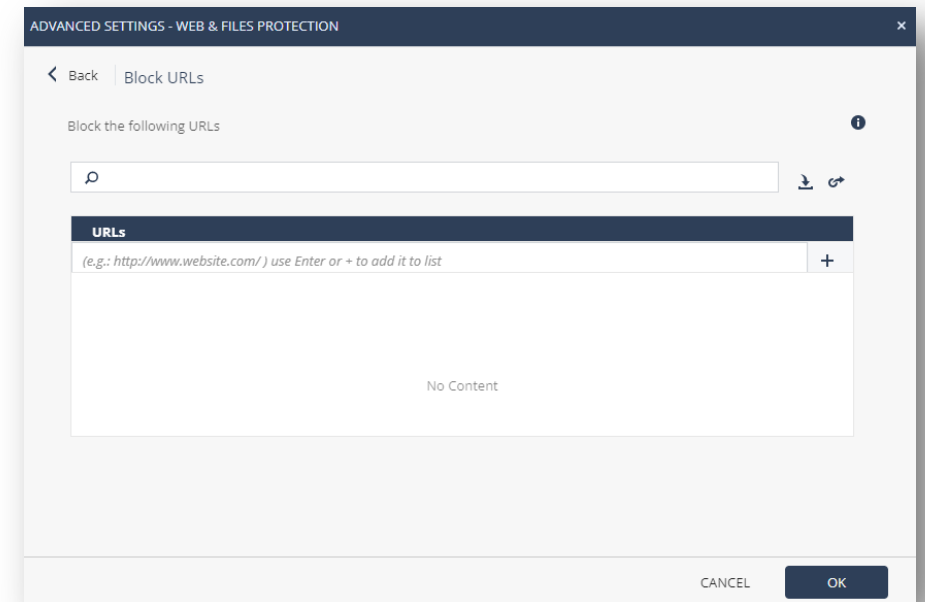
- 閲覧をブロックする Web サイトを URL または ドメイン名で指定できます。IP アドレスでは指定できません
- URL または ドメイン名は、個別もしくはファイルのインポートにより設定できます

1. ドメイン名の指定方法

- FQDN を指定できます
 - 例1-1：www.example.com
- ドメイン名を指定できます
 - トップレベルドメインを指定することはできません
 - 例1-2：example.com
 - www.example.com、www2.example.com などもブロックされます
 - * もしくは ? を使用して指定できます
 - トップレベルドメインを指定する場合は、* とともに指定します
 - 例1-3：*.com
 - すべての .com ドメインが除外されます

1. URLの指定方法

- パス名を含めた URL を指定できます
 - 例2-1：https://www.example.com/directory1/
 - https://www.example.com/ や、https://www.example.com/directory2/ には影響しません



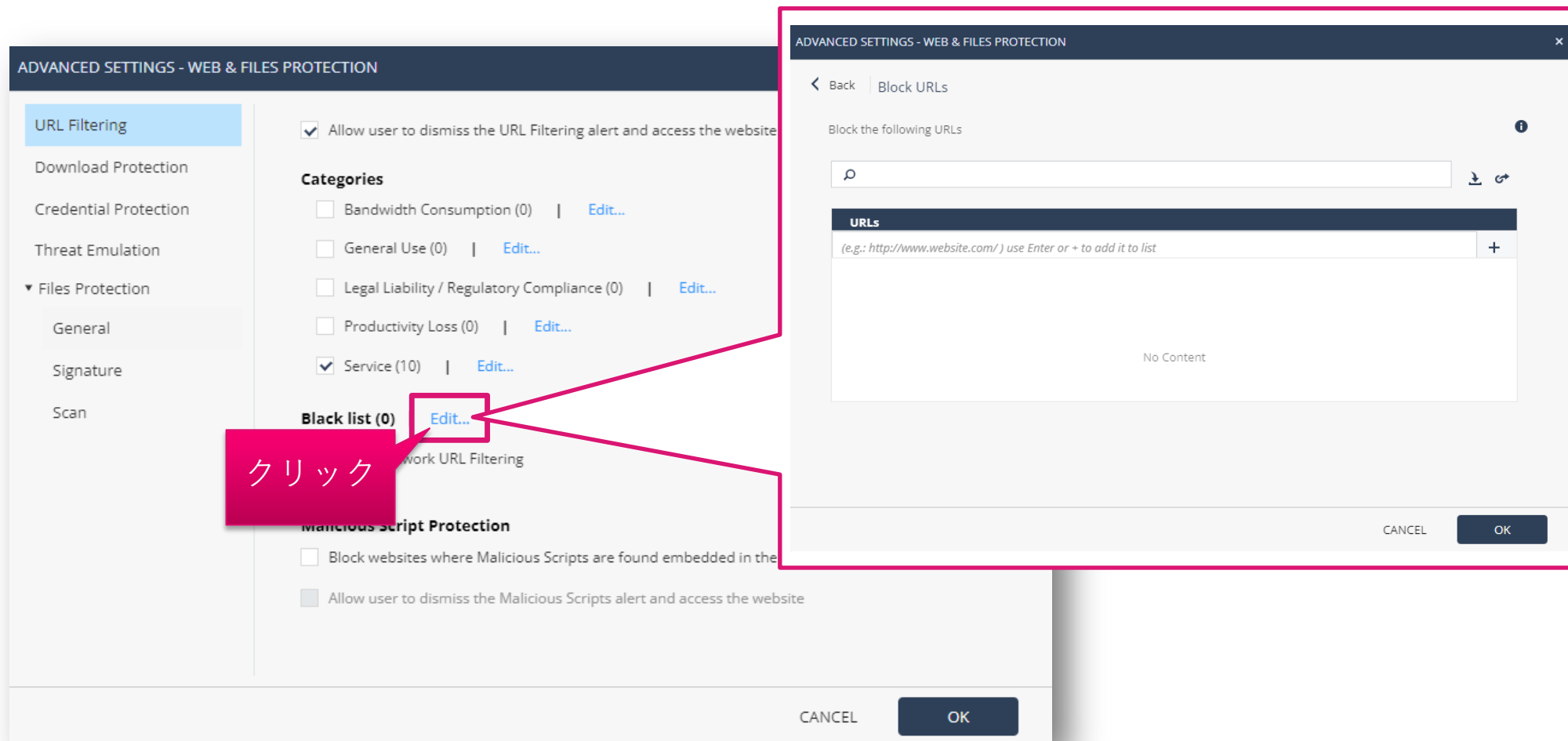
詳細設定画面を表示

- Policy 画面で、WEB & FILE PROTECTION の Advanced Settings をクリックします
- ADVANCED SETTINGS 画面が開きます

The screenshot displays the Check Point Harmony Endpoint console interface. The main window shows the 'Policy Capabilities' section for a policy named 'cpjdemo006'. A modal dialog titled 'ADVANCED SETTINGS - WEB & FILES PROTECTION' is open, showing various configuration options. The 'URL Filtering' section is selected, and the 'Advanced Settings' button at the bottom of the dialog is highlighted with a red box and a callout bubble containing the Japanese text 'クリック' (Click). The background interface includes a sidebar with navigation options like 'OVERVIEW', 'POLICY', 'ASSET MANAGEMENT', 'LOGS', 'PUSH OPERATIONS', 'ENDPOINT SETTINGS', 'SERVICE MANAGEMENT', 'THREAT HUNTING', and 'GLOBAL SETTINGS'. The main content area shows a table of 'Global Exclusions' and a 'CAPABILITIES & EXCLUSIONS' section with tabs for 'WEB & FILES PROTECTION', 'BEHAVIORAL PROTECTION', and 'ANALYSIS & REMEDIATION'. The 'WEB & FILES PROTECTION' tab is active, showing settings for 'URL Filtering Mode' and 'Download Protection'.

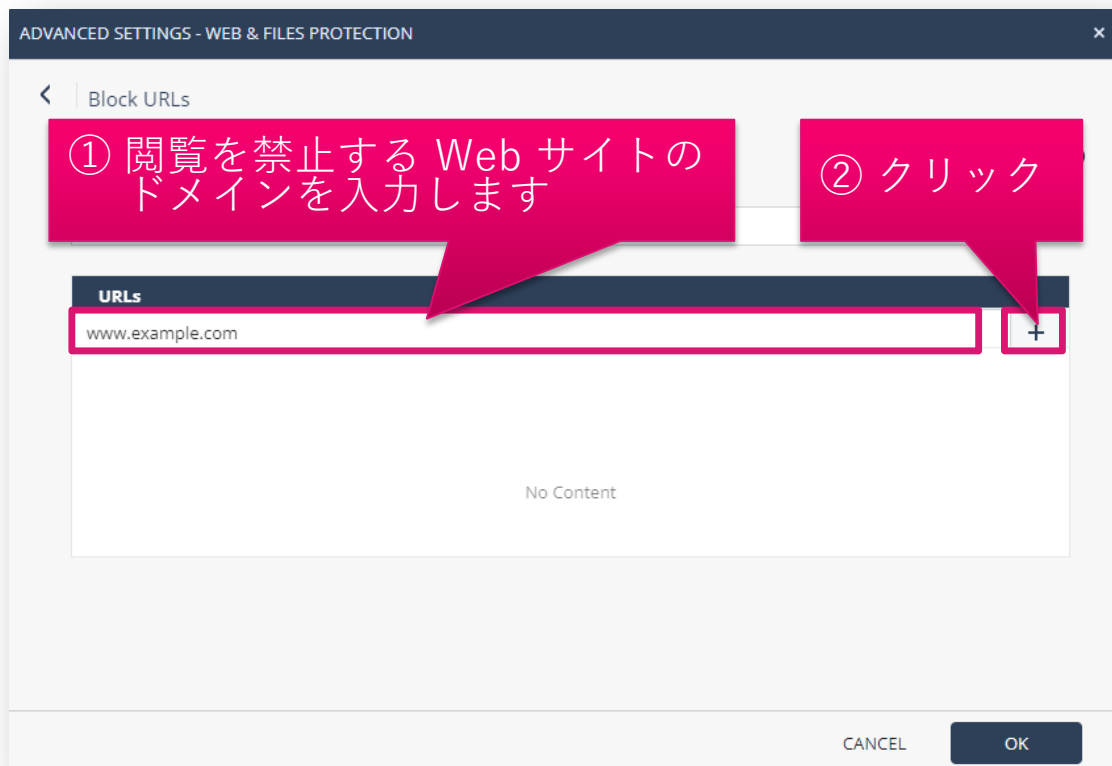
ブラックリストの作成画面を表示

- URL フィルタリングの詳細設定画面で、Black list の Edit をクリックします
- Block URLs 設定画面が開きます



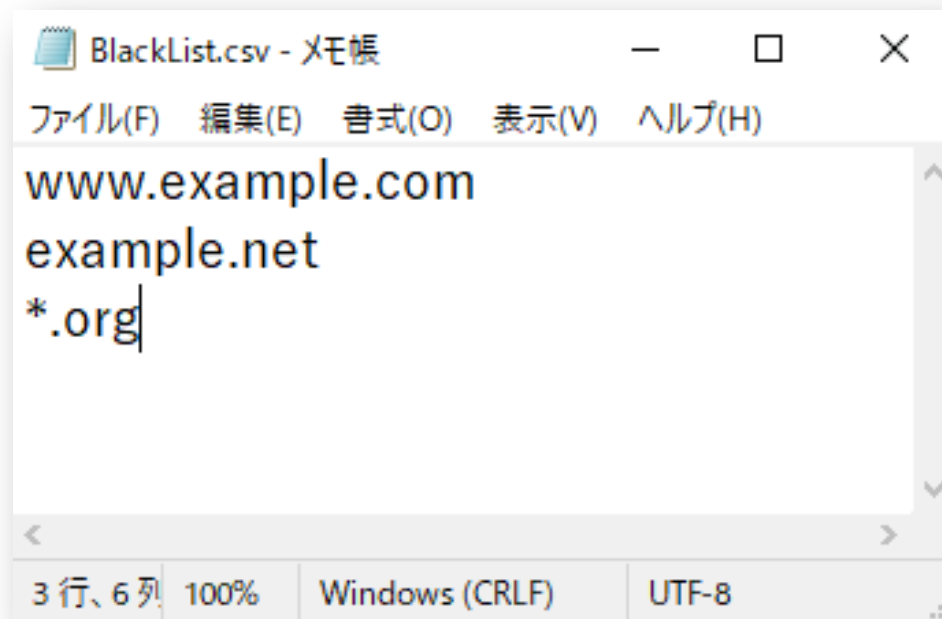
ブラックリストを作成（個別設定）

1. URLs 欄に、閲覧を禁止する Web サイトのドメイン名を入力します
2. **+** をクリックするか、Enter キーを押します
3. URL 一覧にドメイン名が追加されたことを確認します
4. 「OK」 をクリックします




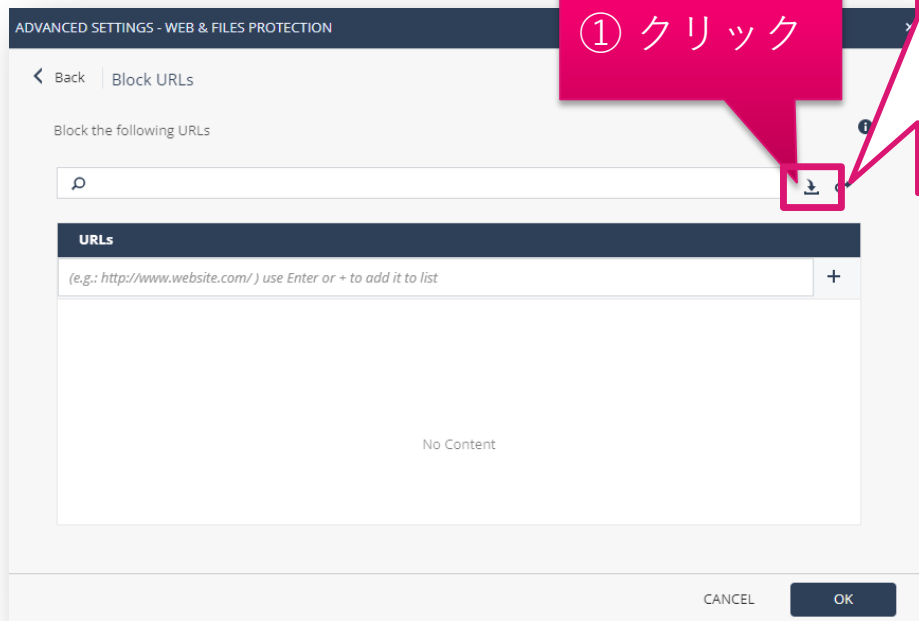
ブラックリストを作成（ファイルインポート）（1 / 2）

- テキストエディタを開きます
- ドメイン名または URL を 1 行に、1 レコード記述します
- ファイル拡張子を csv にして任意のフォルダに保存します

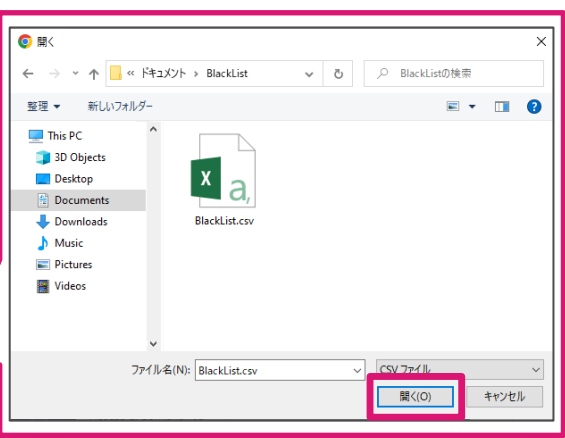


ブラックリストを作成（ファイルインポート）（2 / 2）

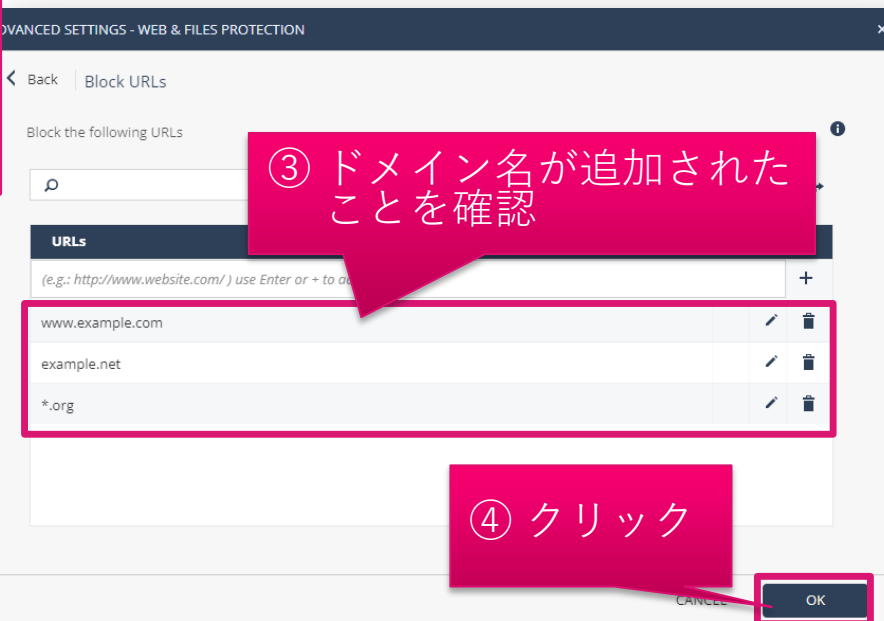
1.  をクリックします
2. ダイアログボックスでファイルを選択して「開く」をクリックします
3. ドメイン名が追加されたことを確認します
4. 「OK」をクリックします



① クリック



開く(O)



③ ドメイン名が追加されたことを確認

④ クリック

The image illustrates the process of importing a blacklist file. It shows three sequential steps: 1. Clicking the 'Import' button in the 'Block URLs' settings. 2. A Windows File Explorer window opening to the 'Documents' folder, where the file 'BlackList.csv' is selected and the 'Open' button is clicked. 3. The 'Block URLs' settings page showing the imported domains: 'www.example.com', 'example.net', and '*.org'. 4. Clicking the 'OK' button to confirm the changes.

ブラックリストを適用

1. Policy Capabilities 画面が表示されたら、「Save」をクリックします
2. 「Install Policy」をクリックします
3. INSTALL POLICY 画面が表示されたら、「INSTALL」をクリックします。10分程度でクライアントにポリシーが反映されます

Unsaved Rules 1

Install Policy

② クリック

CAPABILITIES & EXCLUSIONS

Default settings

11 Exclusions

Exclusions Center

EndPoint for Server Optimization OFF

Policy Mode Custom

WEB & FILES PROTECTION

BEHAVIORAL PROTECTION

ANALYSIS & REMEDIATION

Last Modified Dec 7, 05:27 PM (cp_EpMaaS_Only, versions)

URL Filtering

URL Filtering Mode Prevent

Download Protection

Download Emulation & Extr

Save

① クリック



INSTALL POLICY

The following changes were made since the last policy installation. Review the changes and click on 'install' to install policy.

Changed Rules Settings (1)

| Rule Name | Policy Type | Changes | Modified C |
|--|-------------------|-----------------------|------------|
| <input checked="" type="checkbox"/> Default settings | Threat Prevention | Settings were changed | 12/9/2022, |

Changed Rule Order and Assignments (0)

CANCEL

INSTALL

③ クリック

URL フィルタリングのホワイトリスト設定 ～除外メニュー編～

ホワイトリスト設定の概要

- 閲覧を許可する Web サイトをドメイン名で指定できます
- ホワイトリストは、除外設定機能を使用して作成します

1. ドメイン名の指定方法

- 閲覧を許可する Web サイトを FQDN で指定します
 - 例1-1：www.example.com、example.com
 - www.example.com もしくは example.com のどちらかを指定すると、その両方の閲覧が許可されます
- ホスト名を省略した場合は、ドメイン名
- ワイルドカードを使用して、任意のホスト名、任意のサブドメインの閲覧を許可できます
 - 例1-2：*.example.com
 - www.example.com、www2.example.com、www.sub.example.com などの閲覧が許可されます

NEW EXCLUSION

Exclusion ⓘ
Anti Bot -> URL Filtering exclusions

Method
Domain/URL

Value *

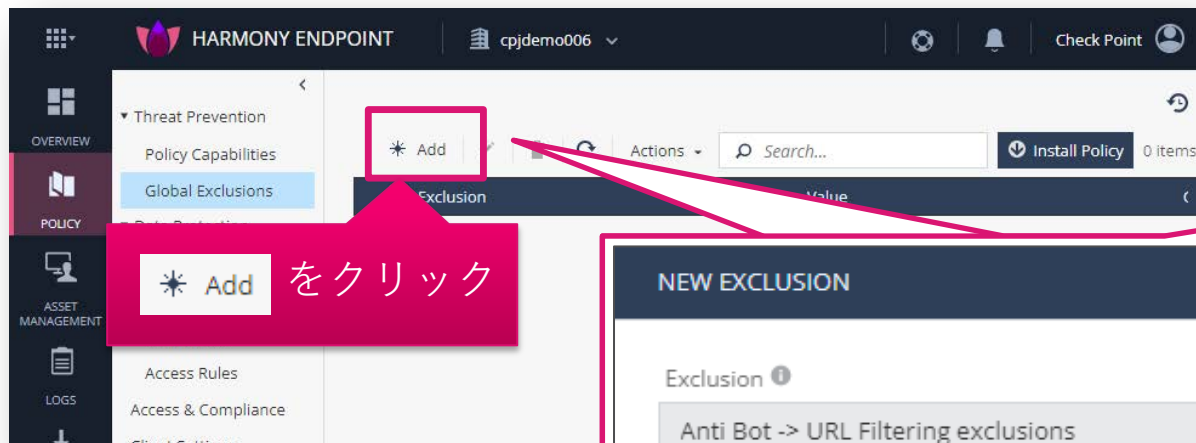
Add to all rules ⓘ

CANCEL OK

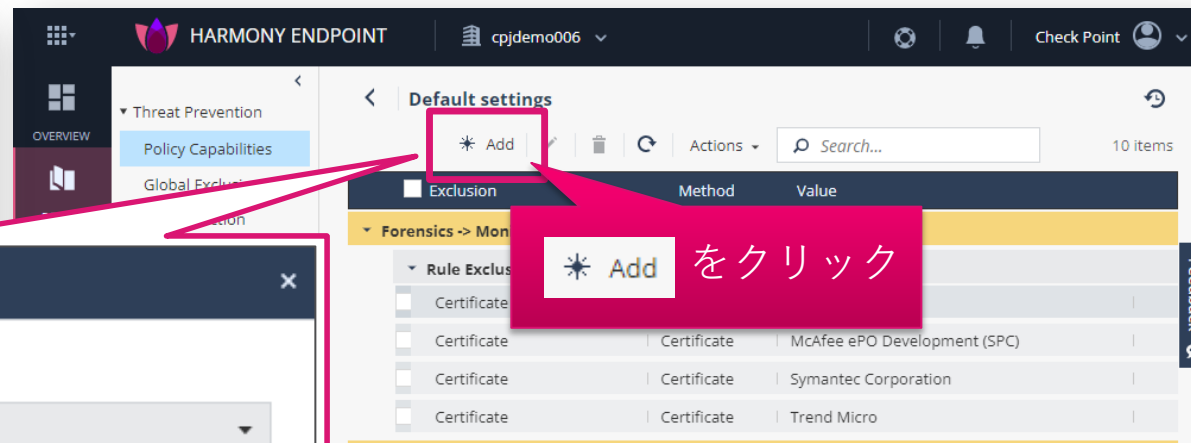
ホワイトリストの作成画面を表示

- Global Exclusionsもしくは、Exclusion Center の画面で、* Add をクリックします
- NEW EXCLUSION 画面が開きます

Global Exclusions での全組織への適用



Exclusion Center での個別ルールへの適用



NEW EXCLUSION

Exclusion ⓘ
Anti Bot -> URL Filtering exclusions

Method
Domain/URL

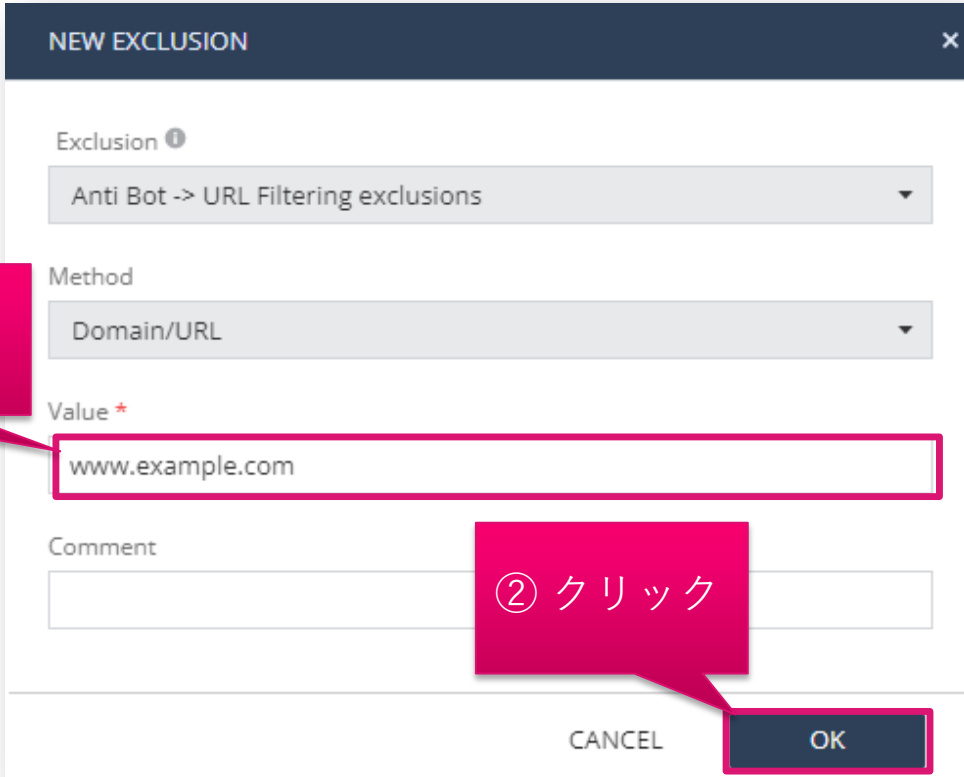
Value *

Add to all rules ⓘ

CANCEL OK

ホワイトリストを作成

1. 「Value」 に除外条件を入力します
2. 「OK」 をクリックします



The screenshot shows a 'NEW EXCLUSION' dialog box with the following fields and annotations:

- Exclusion:** A dropdown menu set to 'Anti Bot -> URL Filtering exclusions'.
- Method:** A dropdown menu set to 'Domain/URL'.
- Value *:** A text input field containing 'www.example.com'. A red callout bubble with the text '① 除外条件を入力' (1. Enter exclusion condition) points to this field.
- Comment:** An empty text input field. A red callout bubble with the text '② クリック' (2. Click) points to the 'OK' button.
- Buttons:** 'CANCEL' and 'OK' buttons at the bottom right. The 'OK' button is highlighted with a red border.

ホワイトリストを適用（組織全体に適用する場合）（1 / 2）

1. Global Exclusions の画面が表示され、除外設定が作成されていることを確認します
2. 「Save」をクリックします
3. 「Install Policy」をクリックします

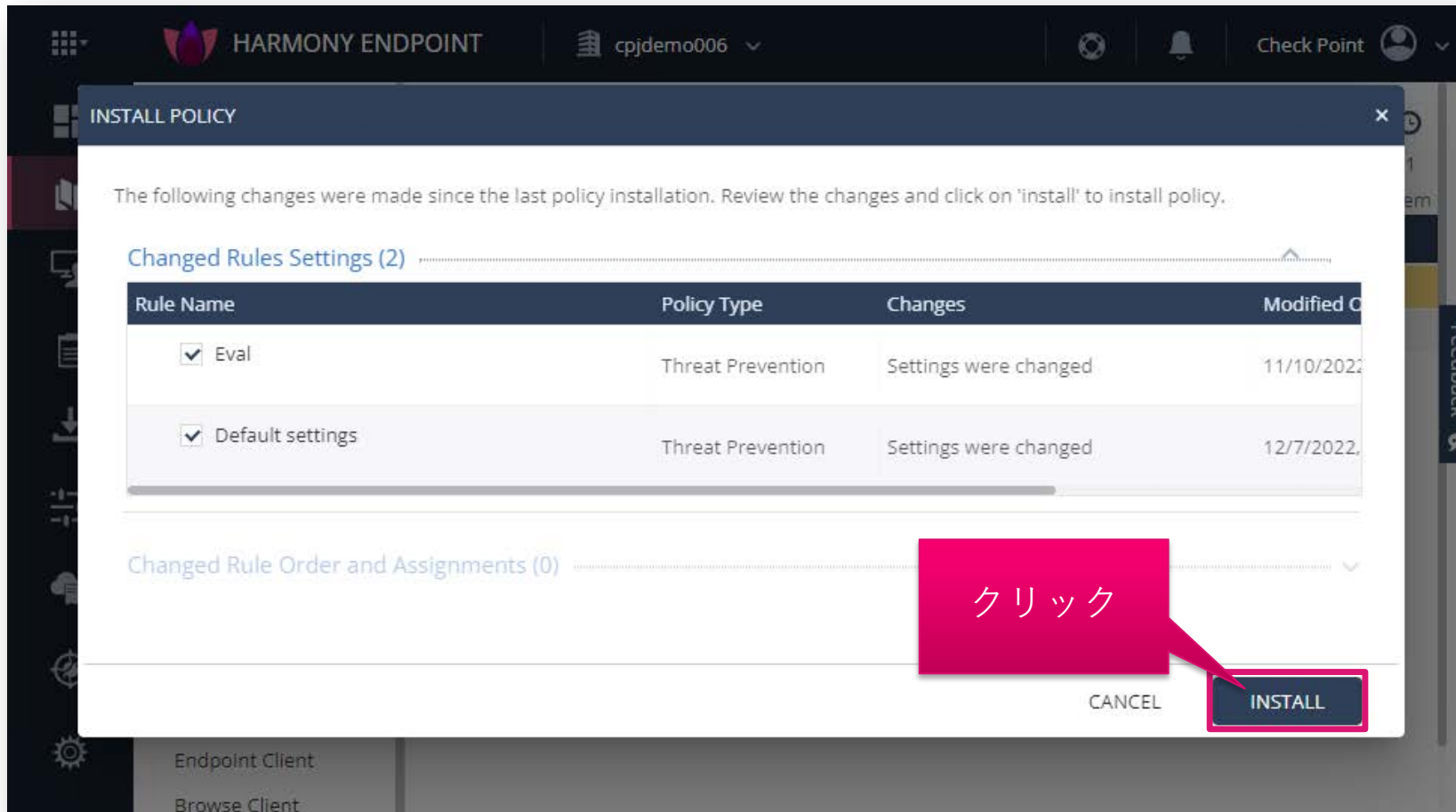
The screenshot shows the HARMONY ENDPOINT console interface. The left sidebar contains navigation options under 'Threat Prevention', with 'Global Exclusions' selected. The main content area shows a table of exclusions. A callout box labeled '① 除外設定が作成されたことを確認' points to a row in the table with the following details:

| Exclusion | Domain | Domain | www.checkpoint.sc |
|-------------------------------------|--------|--------|-------------------|
| <input checked="" type="checkbox"/> | Domain | Domain | www.checkpoint.sc |

Other callouts include '② クリック' pointing to the 'Save' button at the bottom right, and '③ クリック' pointing to the 'Install Policy' button at the top right.

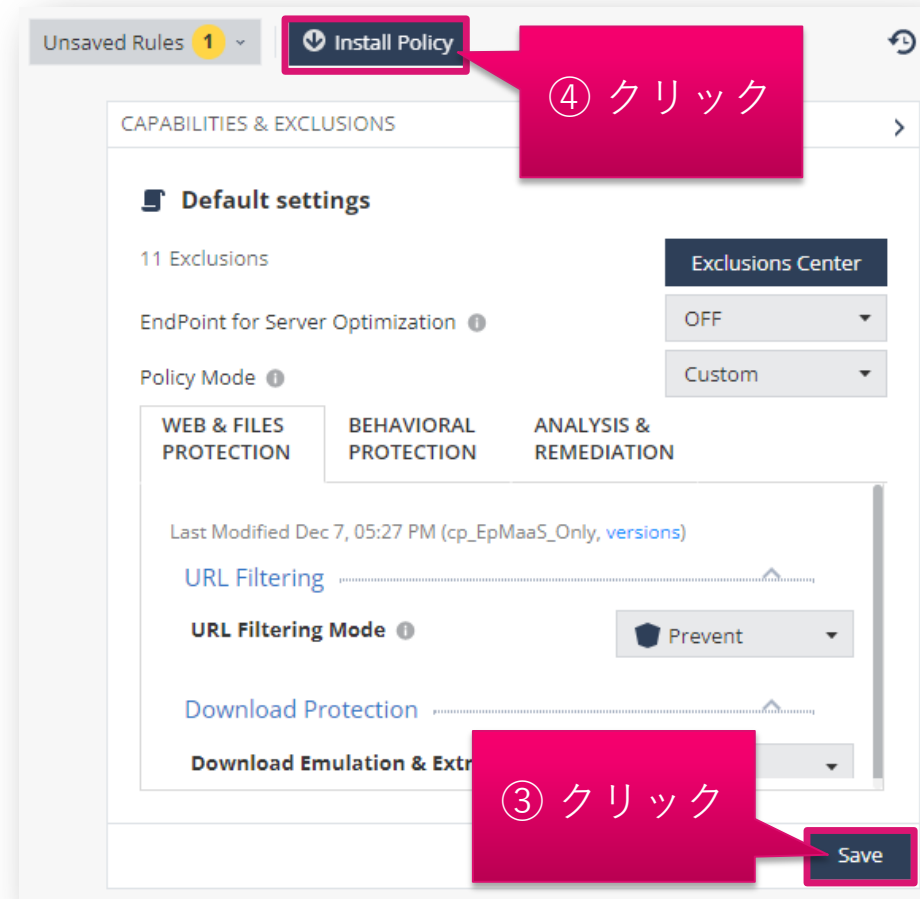
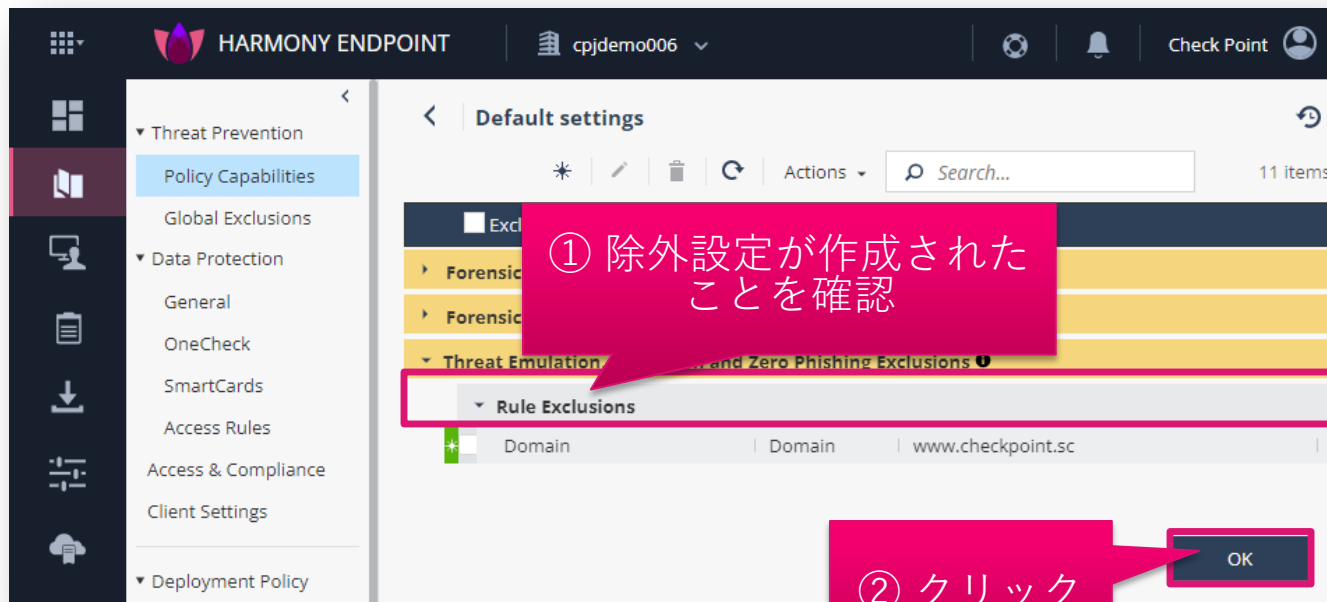
ホワイトリストを適用（組織全体に適用する場合）（2 / 2）

- INSTALL POLICY の画面が表示されたら、「INSTALL」をクリックします
- 以上で、除外設定の適用は完了です
- 10分程度でクライアントにポリシーが反映されます



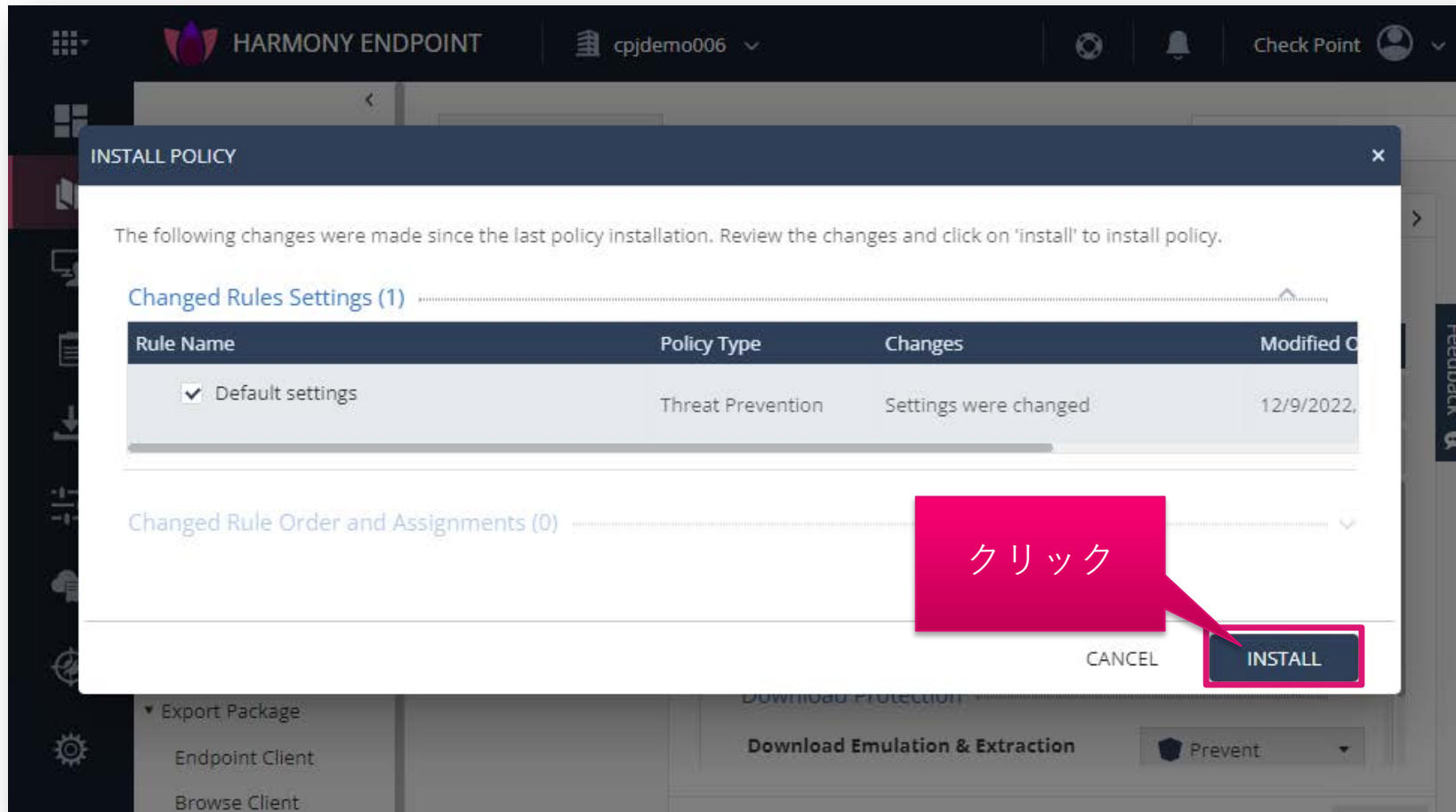
ホワイトリストを適用（個別ルールに適用する場合）（1 / 2）

1. Exclusion Center の画面が表示され、除外設定が作成されていることを確認します
2. 「OK」をクリックします
3. Policy Capabilities 画面が表示されたら、「Save」をクリックします
4. 「Install Policy」をクリックします



ホワイトリストを適用（個別ルールに適用する場合）（2 / 2）

- INSTALL POLICY の画面が表示されたら、「INSTALL」をクリックします
- 以上で、除外設定の適用は完了です
- 10分程度でクライアントにポリシーが反映されます



URL フィルタリングのホワイトリスト設定 ～ログレコード編～

ログレコードを選択してホワイトリストを作成

- Logs で表示されるログのレコードを右クリックする
- 織全体に適用するホワイトリストを作成する場合は、「Create Exclusion for All Rules」を選択する
- 個別のルールに適用するホワイトリストを作成する場合は、「Create Exclusion for Effective Rule」を選択する
- 除外メニューに自動的にホワイトリストが追加されます（次ページ）

The screenshot shows the HARMONY ENDPOINT interface. The 'Logs' page is active, displaying a table of log records. A context menu is open over a selected record, showing options to create exclusions. Three callout boxes provide instructions:

- ① Logs ページを表示 (Show Logs page)
- ② ログレコードを選択して右クリック (Right-click the log record)
- ③ 組織全体に適用する除外設定を作成 (Create exclusion for all rules)
- ③ 個別のルールに適用する除外設定を作成 (Create exclusion for effective rule)

| Time | B. | Matched Category | Action |
|--------------------------|----|------------------|---------|
| Dec 15, 2022 12:31:20 PM | | | |
| Dec 15, 2022 12:27:27 PM | | | |
| Dec 15, 2022 12:25:55 PM | | | |
| Dec 15, 2022 12:25:43 PM | | Shopping | Prevent |
| Dec 15, 2022 12:25:18 PM | | | |
| Dec 15, 2022 12:25:01 PM | | | |
| Dec 15, 2022 12:17:21 PM | | | |
| Dec 15, 2022 12:04:13 PM | | Shopping | Prevent |
| Dec 15, 2022 12:04:13 PM | | Shopping | Prevent |

Context Menu Options:

- Filter: "https://kaiyasu.net/fro..."
- Filter Out: "https://kaiyasu.net..."
- Create Exclusion for All Rules
- Create Exclusion for Effective Rule

Log Record Details:

- URL: https://kaiyasu.net/front/
- URL: https://shopping.yahoo.co.jp/
- URL: https://shopping.google.com/?pli=1
- URL: https://www.ebay.com/
- URL: https://www.amazon.com/

ホワイトリストを適用（組織全体に適用する場合）（1 / 2）

1. Global Exclusions の画面が表示され、除外設定が作成されていることを確認します
2. 「Save」をクリックします
3. 「Install Policy」をクリックします

The screenshot shows the 'Global Exclusions' configuration page in the Check Point Harmony Endpoint console. The left sidebar contains a navigation menu with 'Global Exclusions' selected. The main content area shows a table with the following structure:

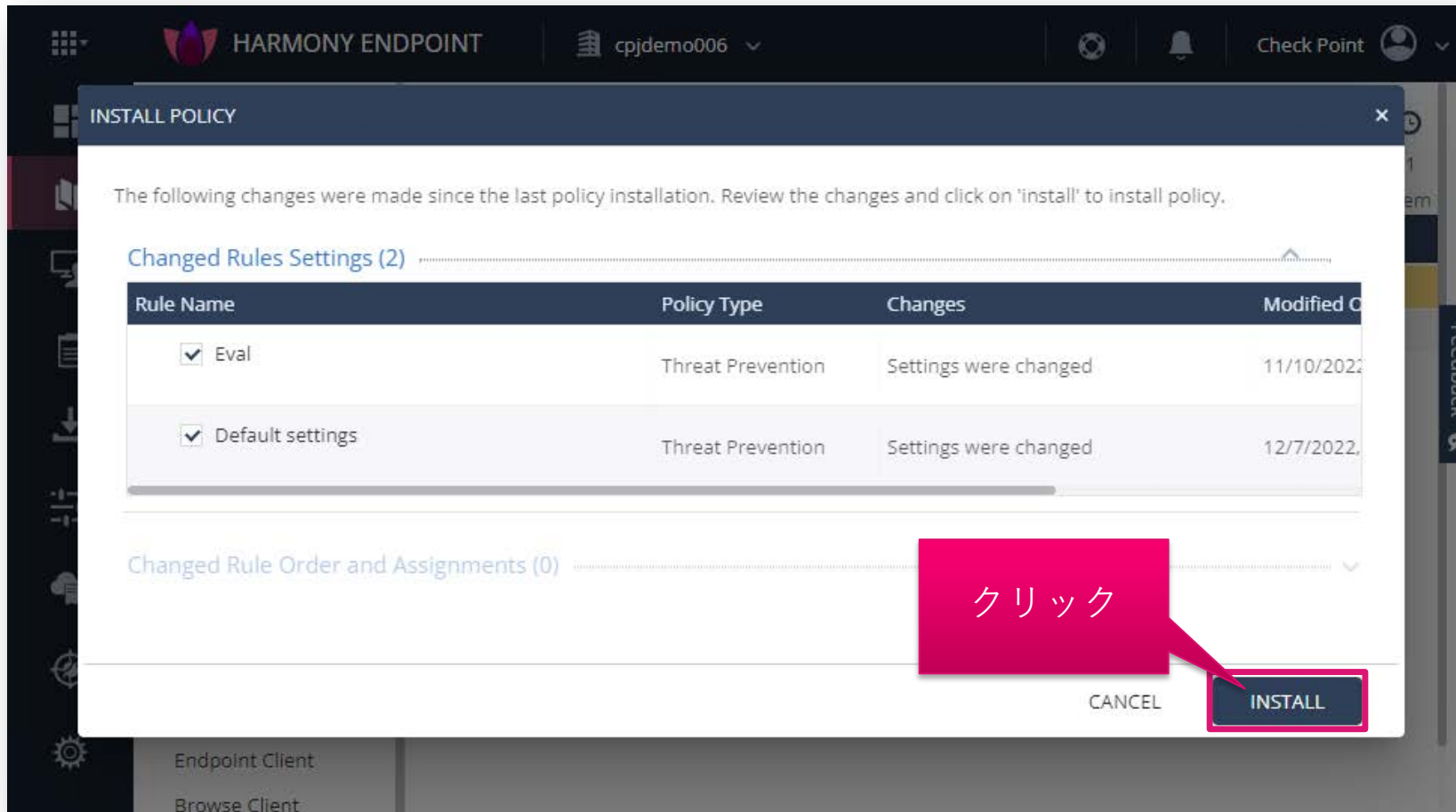
| Exclusion | Value | |
|-----------------------------------|------------|-------------|
| Anti Bot -> URL Filter Exclusions | | |
| <input type="checkbox"/> | Domain/URL | kaiyasu.net |

Three callout boxes provide instructions:

- ① 除外設定が作成されたことを確認 (Confirm that the exclusion setting has been created) - points to the table row.
- ② クリック (Click) - points to the 'Save' button.
- ③ クリック (Click) - points to the 'Install Policy' button.

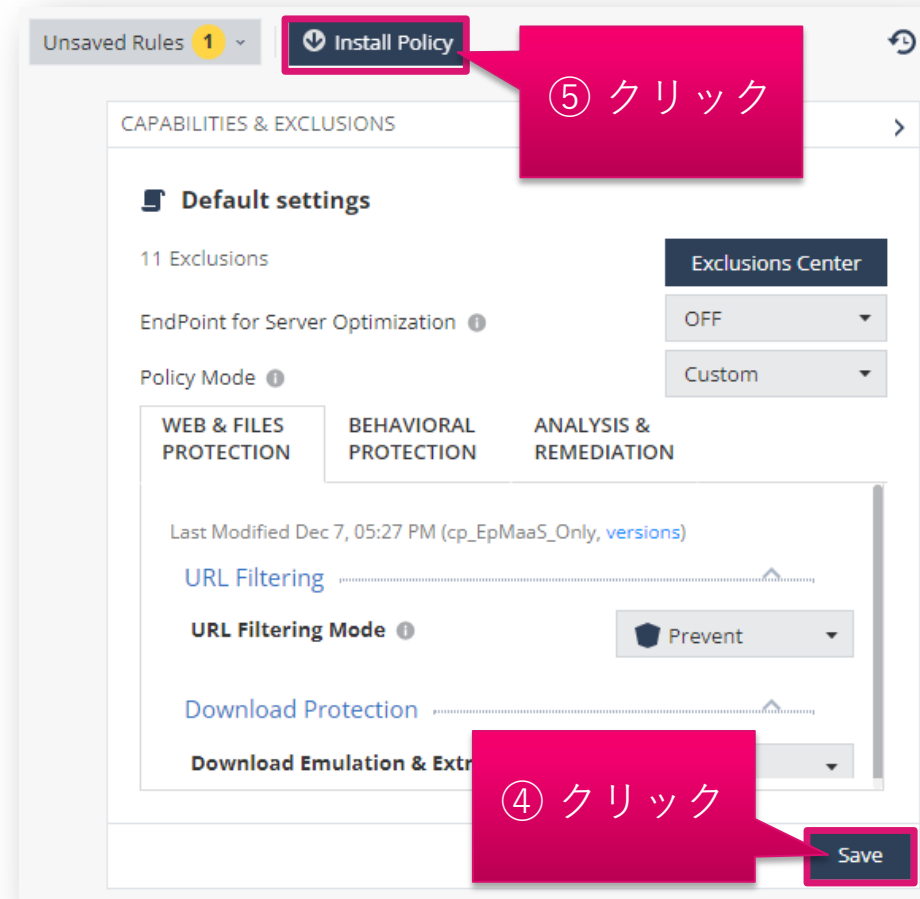
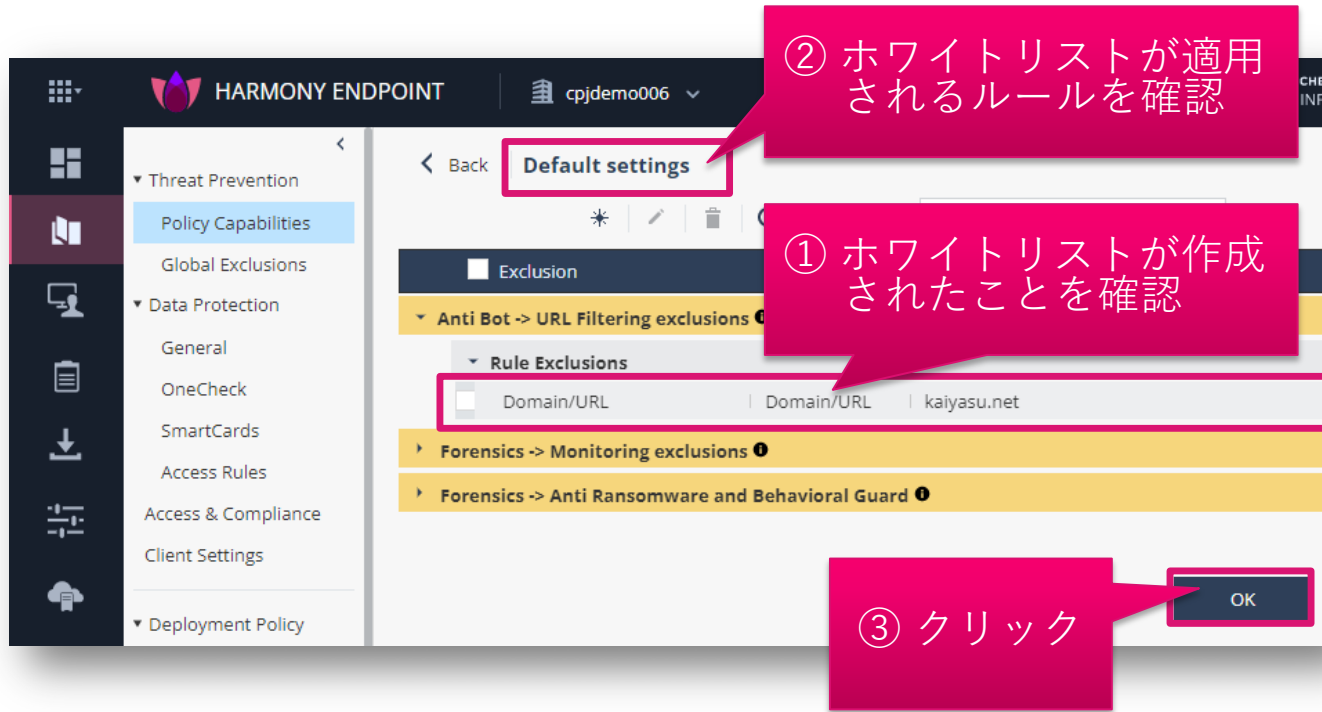
ホワイトリストを適用（組織全体に適用する場合）（2 / 2）

- INSTALL POLICY の画面が表示されたら、「INSTALL」をクリックします
- 以上で、除外設定の適用は完了です
- 10分程度でクライアントにポリシーが反映されます



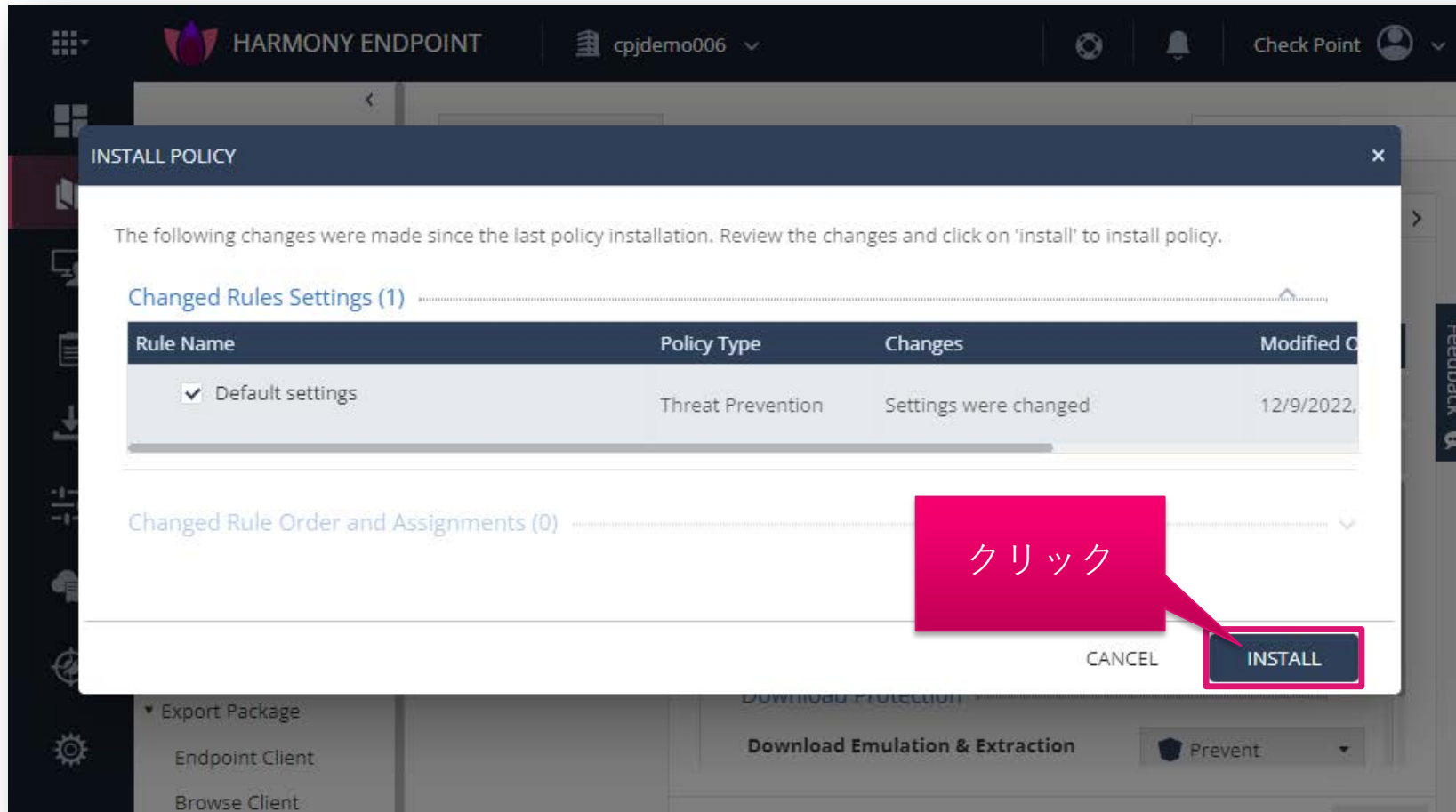
ホワイトリストを適用（個別ルールに適用する場合）（1 / 2）

1. Exclusion Center の画面が表示され、ホワイトリストが作成されていることを確認します
2. 適用されるルールを確認します
3. 「OK」をクリックします
4. Policy Capabilities 画面が表示されたら、「Save」をクリックします
5. 「Install Policy」をクリックします



ホワイトリストを適用（個別ルールに適用する場合）（2 / 2）

- INSTALL POLICY の画面が表示されたら、「INSTALL」をクリックします
- 以上で、除外設定の適用は完了です
- 10分程度でクライアントにポリシーが反映されます



ログの表示内容

ログの表示内容

- ブラックリストサイトへアクセスした際のログは、「Matched Category」欄に Blacklisted と表示されます
- ホワイトリストサイトへアクセスした際のログは、「Matched Category」欄に Whitelisted と表示されます

| Time | Blade | Matched Category | Action | Resource |
|-------------------------|---------------|------------------|---------|----------------------------|
| Dec 15, 2022 3:28:14 PM | URL Filtering | Blacklisted | Prevent | https://github.com/ |
| Dec 15, 2022 1:08:11 PM | URL Filtering | Whitelisted | Accept | https://kaiyasu.net/front/ |

除外設定 (Threat Emulation(Web)、
Threat Extraction、Zero-Phising)

除外設定の概要

- ファイルをダウンロードもしくは、認証情報を入力する Web サーバのドメイン名、IP アドレスを指定して、Web ダウンロード時のThreat Emulation/Extraction、Zero-Phishing による検査、無害化の除外設定を行えます

1. ドメイン名の指定方法

- http/s、*、またはその他の特殊文字を使用せずにドメイン名を指定してください
 - 例1-1：www.checkpoint.com
- ホスト名を省略すると、指定したドメインのすべての FQDN が除外されます
 - 例1-2：checkpoint.com
 - www.checkpoint.com、www2.checkpoint.com などが除外されます
- ドメイン名を指定すると、指定したドメインのサブドメイン、下位ドメインも除外されます
 - 例1-3：com
 - すべての com ドメインが除外されます

2. IP アドレスの指定方法

- URL の FQDN 部分が IP アドレスの場合、IP アドレスを指定してください
 - 例2-1：192.168.100.100
- 複数の IP アドレスを範囲指定する際は、ネットマスクを指定してください
 - 例2-2：192.168.100.0/24

NEW EXCLUSION

Exclusion ⓘ
Threat Emulation, Extraction and Zero Phishing Exclusions

Method
Domain

Value *
www.checkpoint.com

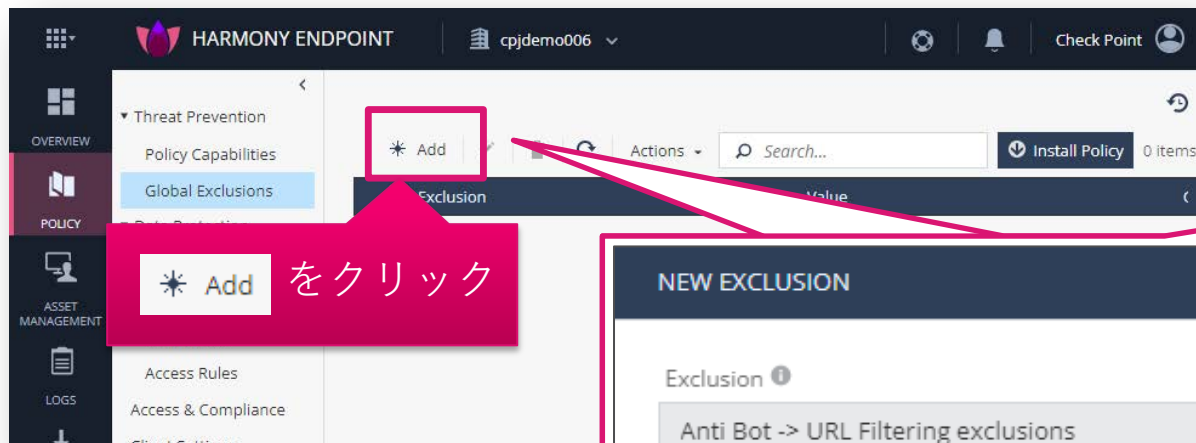
Comment

CANCEL OK

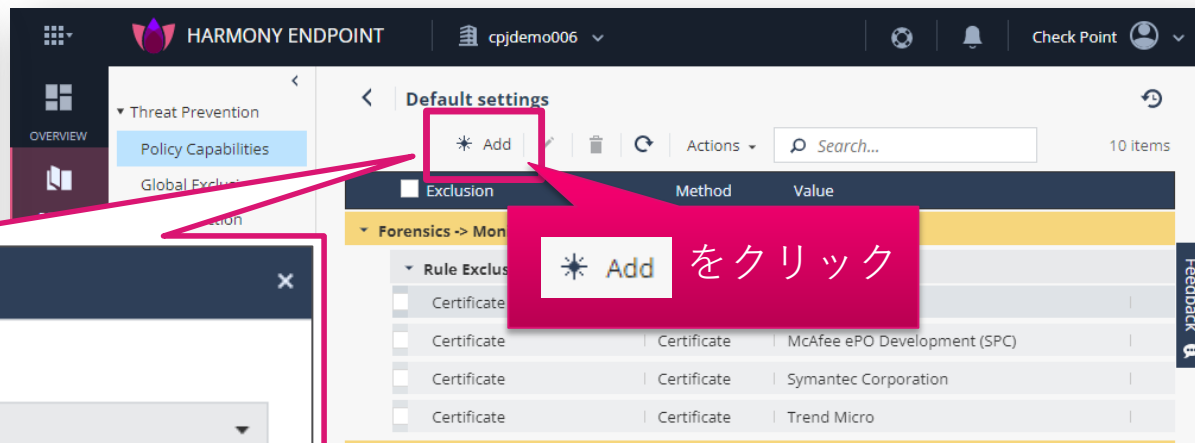
除外設定の作成画面を表示

- Global Exclusionsもしくは、Exclusion Center の画面で、* Add をクリックします
- NEW EXCLUSION 画面が開きます

Global Exclusions での全組織への適用



Exclusion Center での個別ルールへの適用



NEW EXCLUSION

Exclusion ⓘ
Anti Bot -> URL Filtering exclusions

Method
Domain/URL

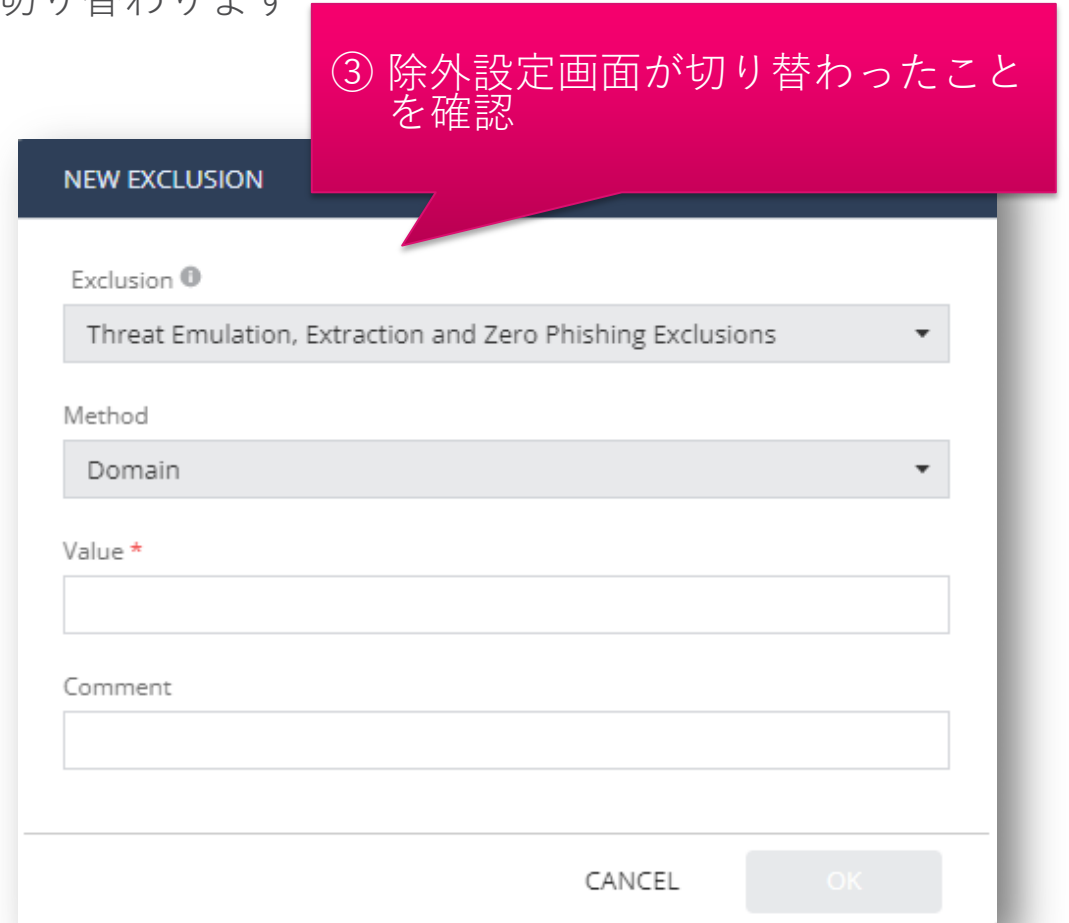
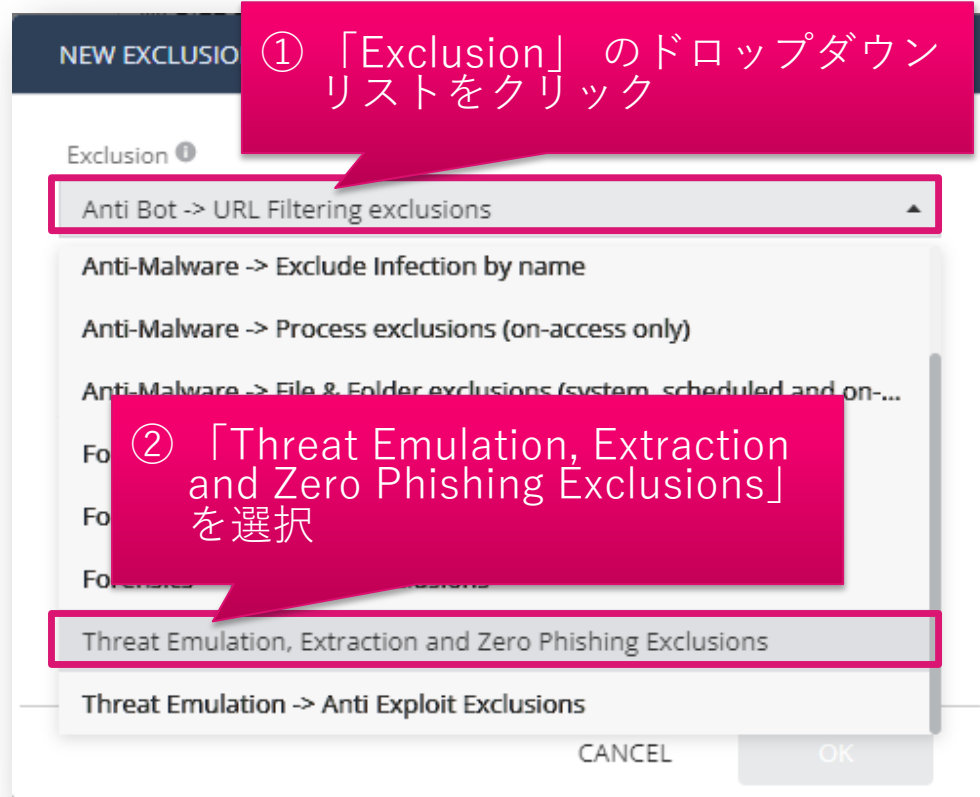
Value *

Add to all rules ⓘ

CANCEL OK

Threat Emulation の除外設定画面を表示

1. NEW EXCLUSION の画面で、「Exclusion」のドロップダウンリストをクリックします
2. 「Threat Emulation, Extraction and Zero Phishing Exclusions」を選択します
3. Threat Emulation、Extraction、Zero-Phishing の除外設定画面に切り替わります



除外条件を設定

1. 「Method」が Domain となっていることを確認します
2. 「Value」に除外条件を入力します
3. 「OK」をクリックします

① Domain となっていることを確認

② 除外条件を入力

③ クリック

NEW EXCLUSION

Exclusion ⓘ
Threat Emulation, Extraction and Zero Phishing Exclusions

Method
Domain

Value *
www.checkpoint.sc

Comment

CANCEL OK

除外設定を適用（組織全体に適用する場合）（1 / 2）

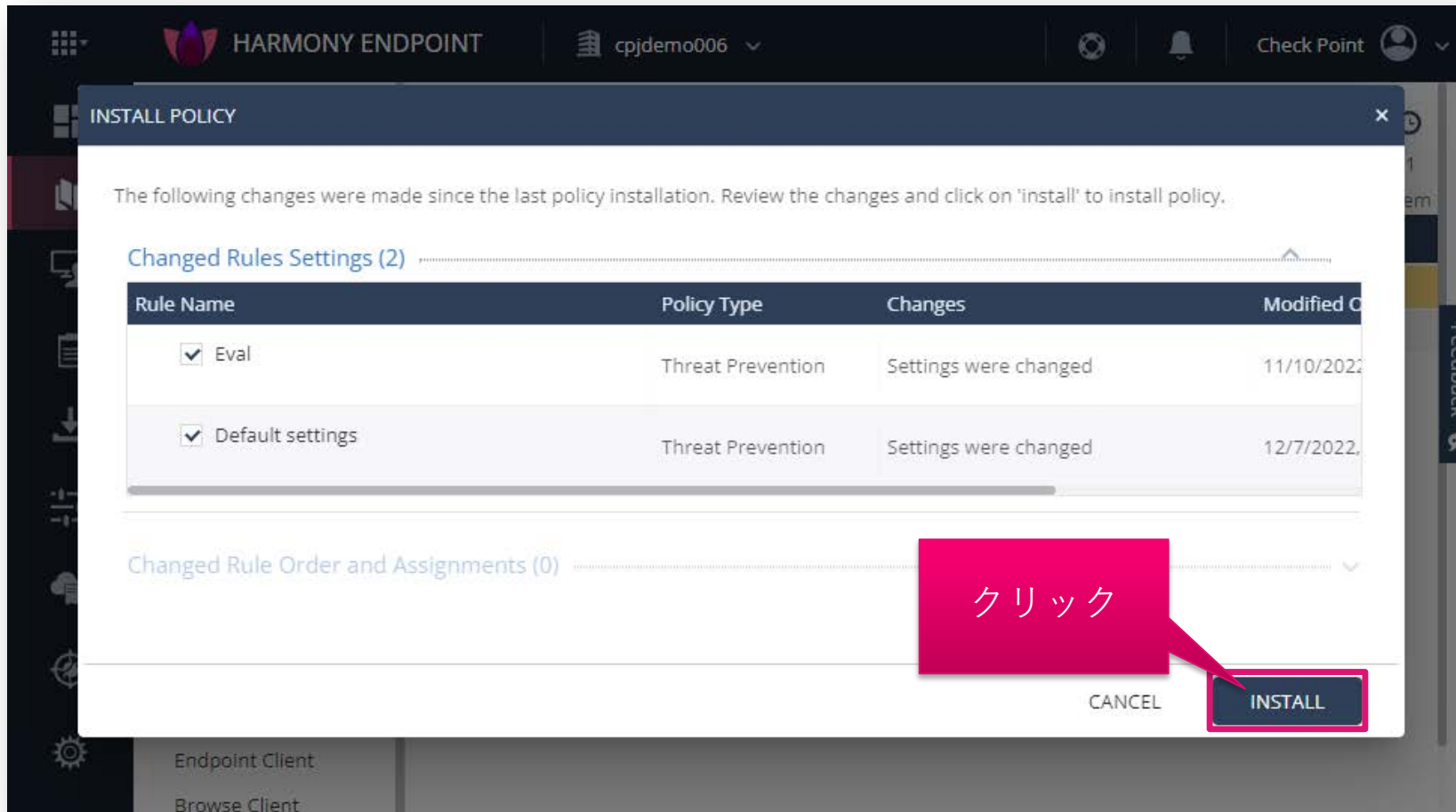
1. Global Exclusions の画面が表示され、除外設定が作成されていることを確認します
2. Save ボタンをクリックします
3. Install Policy ボタンをクリックします

The screenshot shows the Harmony Endpoint console interface. The left sidebar contains a navigation menu with 'Global Exclusions' selected. The main content area shows a table of exclusion rules. A callout box labeled '① 除外設定が作成されたことを確認' points to a row in the table with the domain 'www.checkpoint.sc'. Another callout box labeled '② クリック' points to the 'Save' button at the bottom right. A third callout box labeled '③ クリック' points to the 'Install Policy' button at the top right.

| Exclusion | Domain | Domain | www.checkpoint.sc |
|-----------|--------|--------|-------------------|
| + | Domain | Domain | www.checkpoint.sc |

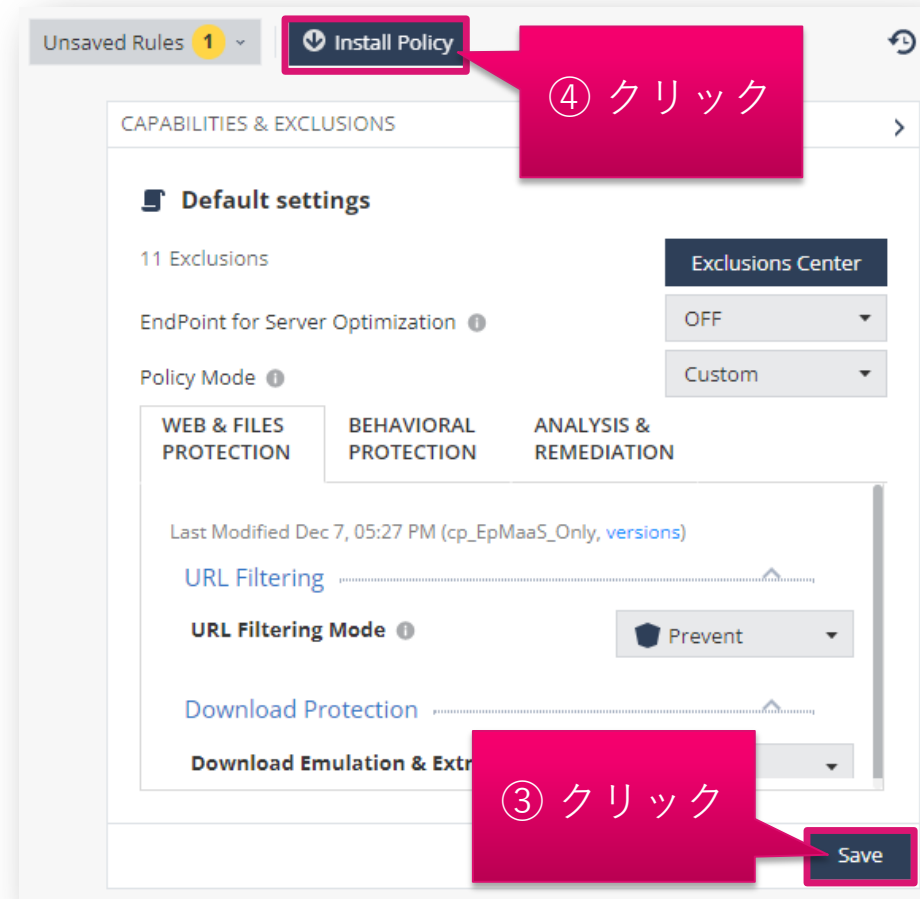
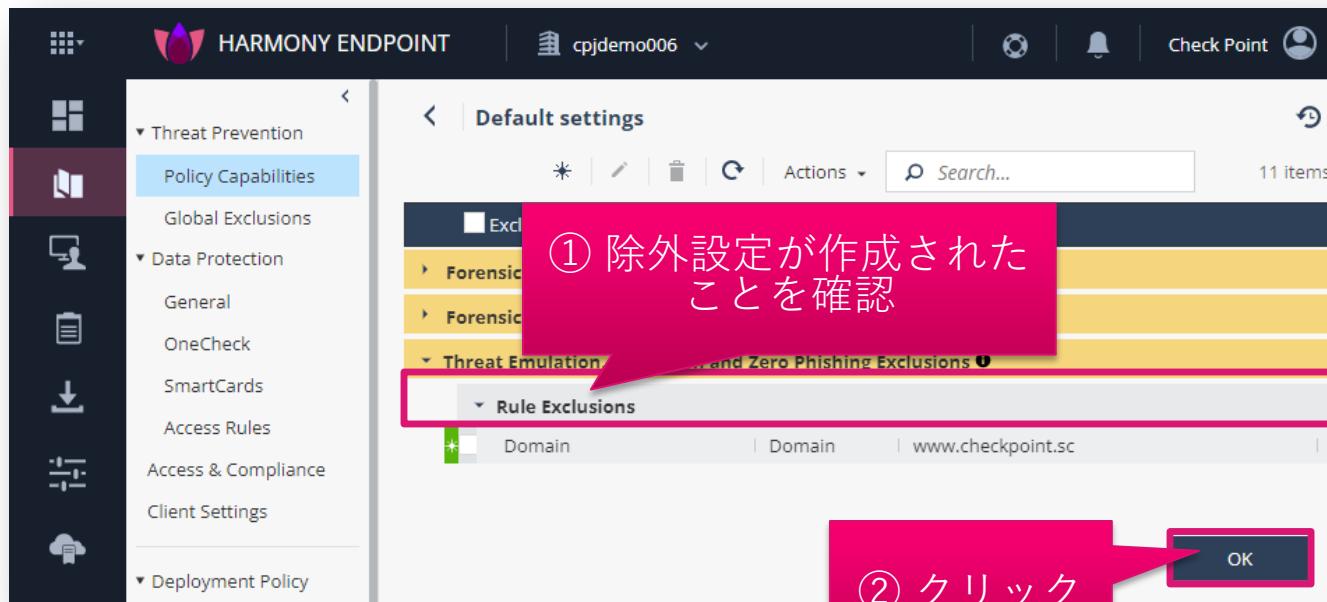
除外設定を適用（組織全体に適用する場合）（2 / 2）

- INSTALL POLICY の画面が表示されたら、「INSTALL」をクリックします
- 以上で、除外設定の適用は完了です
- 10分程度でクライアントにポリシーが反映されます



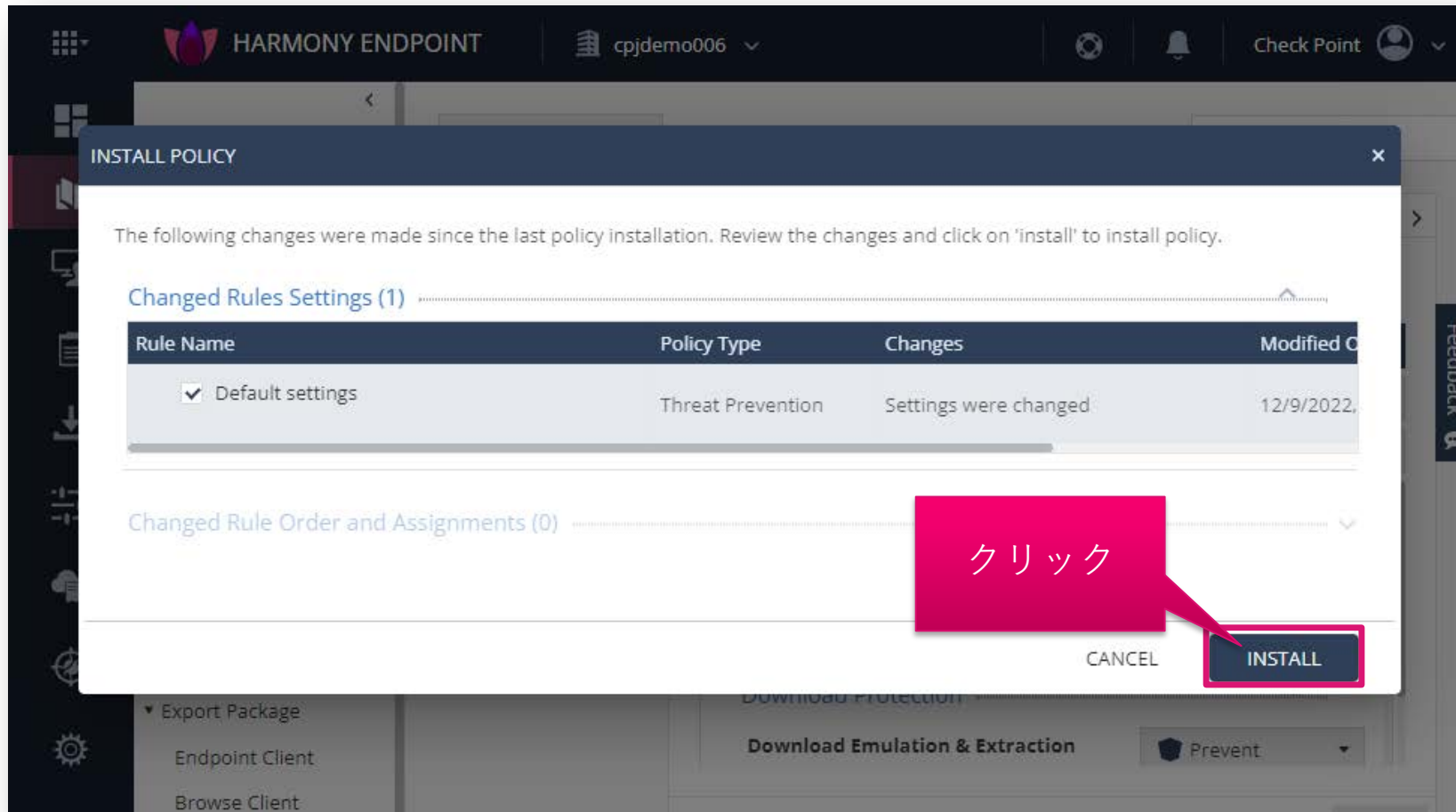
除外設定を適用（個別ルールに適用する場合）（1 / 2）

1. Exclusion Center の画面が表示され、除外設定が作成されていることを確認します
2. OK ボタンをクリックします
3. Policy Capabilities 画面が表示されたら、Save ボタンをクリックします
4. Install Policy ボタンをクリックします



除外設定を適用（個別ルールに適用する場合）（2 / 2）

- INSTALL POLICY の画面が表示されたら、「INSTALL」をクリックします
- 以上で、除外設定の適用は完了です
- 10分程度でクライアントにポリシーが反映されます



コンピュータ情報の管理

Asset Management > Computers ページ概要

- 展開ステータス、コンピュータ上のアクティブなコンポーネント、コンピュータ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
- ビュー（表示項目）の変更、カスタマイズや、フィルタツール、検索ツールによる表示結果の絞り込みができます
- 表示結果は、xlsx 形式でエクスポートできます

The screenshot shows the HARMONY ENDPOINT interface for the 'Computers' page. The top navigation bar includes 'HARMONY ENDPOINT', a user profile 'cpjdemo0', and a 'Check Point' status. The main content area displays a table of active endpoints. A sidebar on the left contains navigation icons for Overview, Policy, Asset Management (selected), Logs, Push Operations, Endpoint Settings, Service Management, Threat Hunting, and Global Settings. A bottom panel shows detailed information for the selected endpoint 'ep-demo2'.

Callouts and Annotations:

- ビューの変更** (View Change): Points to the 'View: Deployment' dropdown menu.
- フィルタツール** (Filter Tool): Points to the 'Active: Active' filter button.
- 検索ツール** (Search Tool): Points to the search input field.
- エクスポート** (Export): Points to the export icon.
- 一覧表示** (List View): Points to the table of endpoints.
- 詳細表示** (Detailed View): Points to the expanded details panel for 'ep-demo2'.

| Status | Computer Name | Endpoint Version | OS Build | Device Type | Deployment Status | Deploy Time | Capabilities | Deployment Error Code | Deployment Error |
|--------|-----------------|------------------|----------------------|-------------|-------------------|----------------------|--------------|-----------------------|------------------|
| Active | DESKTOP-KS61VT2 | 86.26.6008 | 10.0-19044-SP0.0-SMP | Desktop | Completed | 16 Sep 2022 11:05 am | 🔒 🛡️ 🧰 📡 | N/A | N/A |
| Active | EP | 86.26.6008 | 10.0-17763-SP0.0-SMP | Laptop | Completed | 23 Aug 2022 08:08 pm | 🔒 🛡️ 🧰 📡 | N/A | N/A |
| Active | Mixed-Nu2 | 86.40.0169 | 10.0-19043-SP0.0-SMP | Laptop | Completed | 05 Oct 2022 01:11 pm | 🔒 🛡️ 🧰 📡 📄 📊 | N/A | N/A |
| Active | ep-demo2 | 86.40.0169 | 10.0-19043-SP0.0-SMP | Laptop | Completed | 20 Sep 2022 02:05 pm | 🔒 🛡️ 🧰 📡 📄 📊 | N/A | N/A |
| Active | ep-demo3 | 86.50.0190 | 10.0-19043-SP0.0-SMP | Laptop | Completed | 23 Aug 2022 10:57 am | 🔒 🛡️ 🧰 📡 📄 📊 | N/A | N/A |

1 of 5 selected

General

Display Name: **ep-demo2**

Description: .

LDAP

SAM Name: **EP-DEMO2**

CN: .

Operating System: **Microsoft Windows 10 Enterprise Evaluation**

OS Version: **10.0-19043-SP0.0-SMP**

Member of

+ × 📄 🔍 Search

- All Laptops
- All Windows Laptops
- CP-demo
- Remote Access.VPN

コンピュータ情報の一覧表示

- Asset Management > Computers でコンピュータ情報を一覧表示できます
- Active Directory と連携すると、クライアントがインストールされていないコンピュータを表示できます

View: Deployment Active: Active Search

| Status | Computer Name | Endpoint Version | OS Build | Device Type | Deployment Status | Deploy Time | Capabilities | Deployment Error Code | Deployment Error |
|--------|-----------------|------------------|----------------------|-------------|-------------------|----------------------|--------------|-----------------------|------------------|
| | DESKTOP-KS61VT2 | 86.26.6008 | 10.0-19044-SP0.0-SMP | Desktop | Completed | 16 Sep 2022 11:05 am | | N/A | N/A |
| | EP | 86.26.6008 | 10.0-17763-SP0.0-SMP | Laptop | Completed | 23 Aug 2022 08:08 pm | | N/A | N/A |
| | Mixed-Nu2 | 86.40.0169 | 10.0-19043-SP0.0-SMP | Laptop | Completed | 05 Oct 2022 01:11 pm | | N/A | N/A |
| | ep-demo2 | 86.40.0169 | 10.0-19043-SP0.0-SMP | Laptop | Completed | 20 Sep 2022 02:05 pm | | N/A | N/A |
| | ep-demo3 | 86.50.0190 | 10.0-19043-SP0.0-SMP | Laptop | Completed | 23 Aug 2022 10:57 am | | N/A | N/A |

5 items

コンピュータが一覧表示されます

凡例

| ステータスアイコン | 説明 |
|-----------|--|
| | Harmony Endpointクライアントを示します。 |
| | ハーモニー ブラウズクライアントを示します。 |
| | クライアント接続がアクティブであることを示します。 |
| | クライアントがインストールされていない新しいコンピューターが検出されたことを示します。 |
| | コンピュータがActive Directoryまたは組織ツリーから削除されたことを示します。 |

コンピュータ情報の詳細表示

- 一覧表示されたコンピュータを選択すると、OS、所属するバーチャルグループを表示できます

The screenshot displays the Harmony Endpoint console interface. The left sidebar contains navigation options: OVERVIEW, POLICY, ASSET MANAGEMENT (highlighted), LOGS, PUSH OPERATIONS, ENDPOINT SETTINGS, SERVICE MANAGEMENT, THREAT HUNTING, and GLOBAL SETTINGS. The main content area shows a table of computers under the 'Computers' section. The table has columns for Status, Computer Name, Endpoint Version, OS Build, Device Type, Deployment Status, Deploy Time, Capabilities, Deployment Error Code, and Deployment Error. The row for 'ep-demo3' is selected and highlighted in blue. Below the table, a detailed view for the selected computer is shown, including fields for General, LDAP, and Operating System. A dropdown menu for 'Virtual Groups' is open, showing 'All Laptops' and 'All Windows Laptops' as options.

| Status | Computer Name | Endpoint Version | OS Build | Device Type | Deployment Status | Deploy Time | Capabilities | Deployment Error Code | Deployment Error |
|-----------|-----------------|------------------|----------------------|-------------|-------------------|----------------------|--------------|-----------------------|------------------|
| Completed | DESKTOP-KS61VT2 | 86.26.6008 | 10.0-19044-SP0.0-SMP | Desktop | Completed | 16 Sep 2022 11:05 am | | N/A | N/A |
| Completed | EP | 86.26.6008 | 10.0-17763-SP0.0-SMP | Laptop | Completed | 23 Aug 2022 08:08 pm | | N/A | N/A |
| Completed | Mixed-Nu2 | 86.40.0169 | 10.0-19043-SP0.0-SMP | Laptop | Completed | 05 Oct 2022 01:11 pm | | N/A | N/A |
| Completed | ep-demo2 | 86.40.0169 | 10.0-19043-SP0.0-SMP | Laptop | Completed | 20 Sep 2022 02:05 pm | | N/A | N/A |
| Completed | ep-demo3 | 86.50.0190 | 10.0-19043-SP0.0-SMP | Laptop | Completed | 23 Aug 2022 10:57 am | | N/A | N/A |

1 of 5 selected

選択したコンピュータの詳細情報が表示されます

所属するバーチャルグループが表示されます

Name

- All Laptops
- All Windows Laptops

ビューの変更

- View のドロップダウンリストから事前構成されたビューを選択して表示できます



The screenshot displays the Harmony Endpoint management interface. On the left is a navigation sidebar with sections: OVERVIEW, POLICY, ASSET MANAGEMENT (highlighted), LOGS, and PUSH OPERATIONS. The main content area shows 'Computers' with an 'Organizational Tree' on the left and a table of endpoints on the right. A 'View: Deployment' dropdown menu is open, listing various views: Deployment, Compliance, Health, Full Disk Encryption, Anti-Malware, Host Isolation, Anti-Bot, and Policy Information. A 'Filter: Active: Active' button is visible above the table. Two red callout boxes with white text provide instructions: 'ドロップダウンリストを表示' (Show dropdown list) points to the dropdown menu, and '事前構成されたビューを選択' (Select pre-configured view) points to the 'Deployment' option in the list.

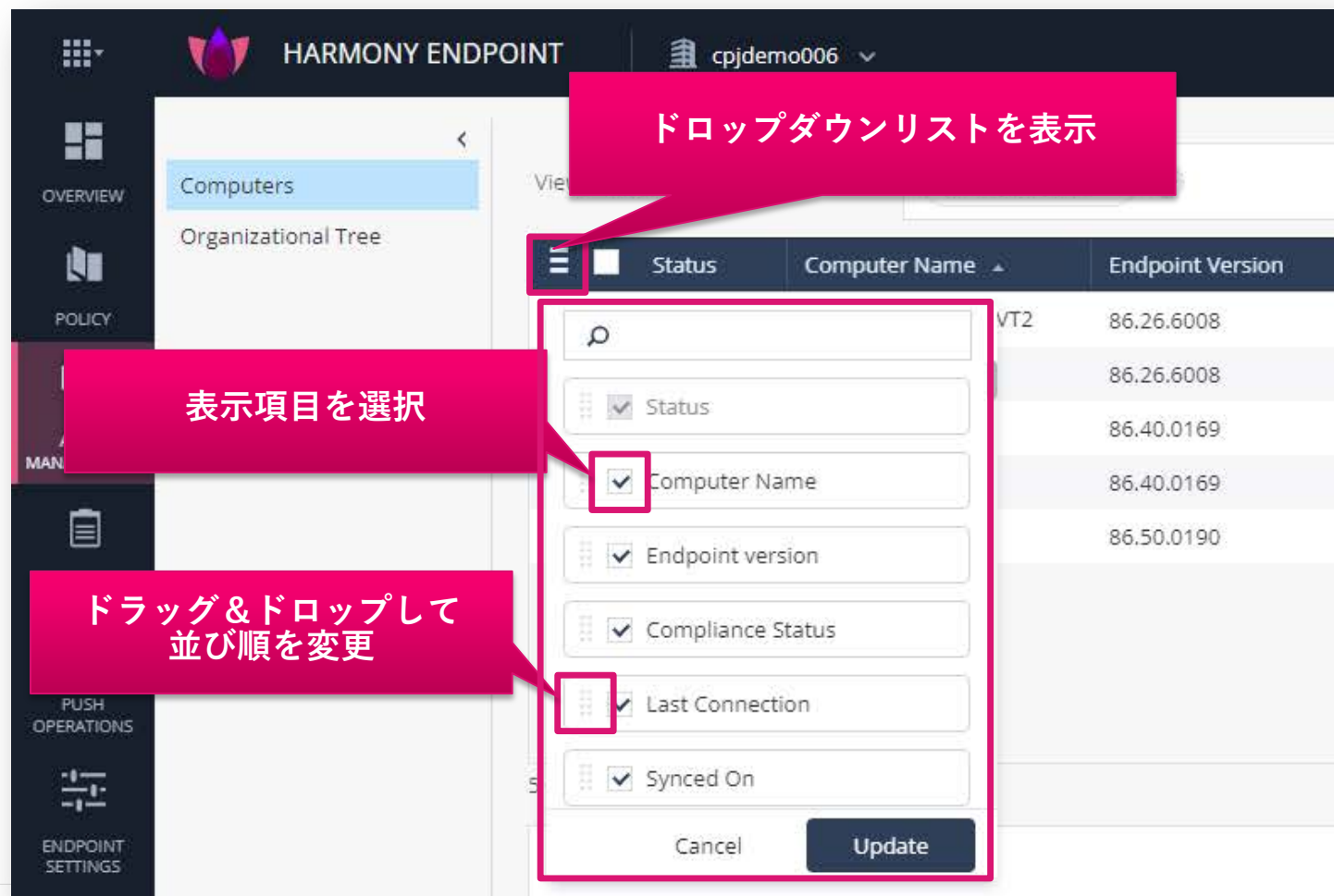
| Name | Endpoint Version |
|-------|------------------|
| OP-K9 | |
| Nu2 | 86.40.0169 |
| no2 | 86.40.0169 |
| no3 | 86.50.0190 |

【参考】事前構成ビューの表示内容

| ビュー | 表示内容 (デフォルト) | | | | | | | | | | |
|----------------------|-------------------------|-------------------------|-------------------------|----------------------------------|------------------------------------|----------------------------------|----------------------------------|------------------------------------|------------------------------------|----------------------------------|----------------------------------|
| Deployment | Status | Computer Name | Endpoint Version | OS Build | Device Type | Deployment Status | Deploy Time | Capabilities | Deployment Error Code | Deployment Error Description | Computer Location |
| | Status Summary | Policy Name | Policy Version | Package Name | Package Version | Last Connection | Synced On | Last Contacted Policy Server IP | Last Contacted Policy Server Name | Pre-Boot Status Updated On | Smartcard Status |
| Compliance | Status | Computer Name | Endpoint Version | Compliance Status | Last Connection | Synced On | Device Type | Computer Location | Compliance Version | | |
| Health | Status | Computer Name | Capabilities | Endpoint Version | OS Build | Virtual Group | Last Connection | Synced On | Last Logged in User | Computer Location | |
| Full Disk Encryption | Status | Computer Name | Endpoint Version | OS Build | FDE Status | Pre-Boot Status | Last Logged in FDE User | FDE Progress Percentage | Computer Location | Status Summary | FDE Version |
| | FDE Last Recovery Date | Recovery Type | | | | | | | | | |
| Anti-Malware | Status | Computer Name | Endpoint Version | Anti-Malware Status | Anti-Malware Updated On | Device Type | Computer Location | Anti-Malware Dat Version | Dat Date | Total Infected | Anti-Malware Version |
| | Scanned On | Total Quarantined | Anti-Malware Infections | | | | | | | | |
| Host Isolation | Status | Computer Name | Endpoint Version | Isolation Status | Last Connection | Synced On | Device Type | Computer Location | | | |
| Anti-Bot | Status | Computer Name | Anti-Bot Statte | Protection Name | | | | | | | |
| Policy Information | Status | Computer Name | Endpoint Version | Threat Prevention Install Policy | Threat Prevention Effective Policy | Data Protection Installed Policy | Data Protection Effective Policy | Access Compliance Installed Policy | Access Compliance Effective Policy | Client Settings Installed Policy | Client Settings Effective Policy |
| | Installed Modified Date | Effective Modified Date | | | | | | | | | |

ビューのカスタマイズ：表示項目の選択

- メニューボタン  をクリックして表示されるドロップダウンリストから、ビューに表示する項目を選択できます
- 表示したい項目のチェックボックスにチェックを入れて Update ボタンを押します
- 項目名の左に表示されている  をドラッグ&ドロップすると、列の並び順を変更できます



ドロップダウンリストを表示

表示項目を選択

ドラッグ&ドロップして並び順を変更

| Status | Computer Name | Endpoint Version |
|--------|---------------|------------------|
| VT2 | | 86.26.6008 |
| | | 86.26.6008 |
| | | 86.40.0169 |
| | | 86.40.0169 |
| | | 86.50.0190 |


ビューのカスタマイズ：フィルタの適用

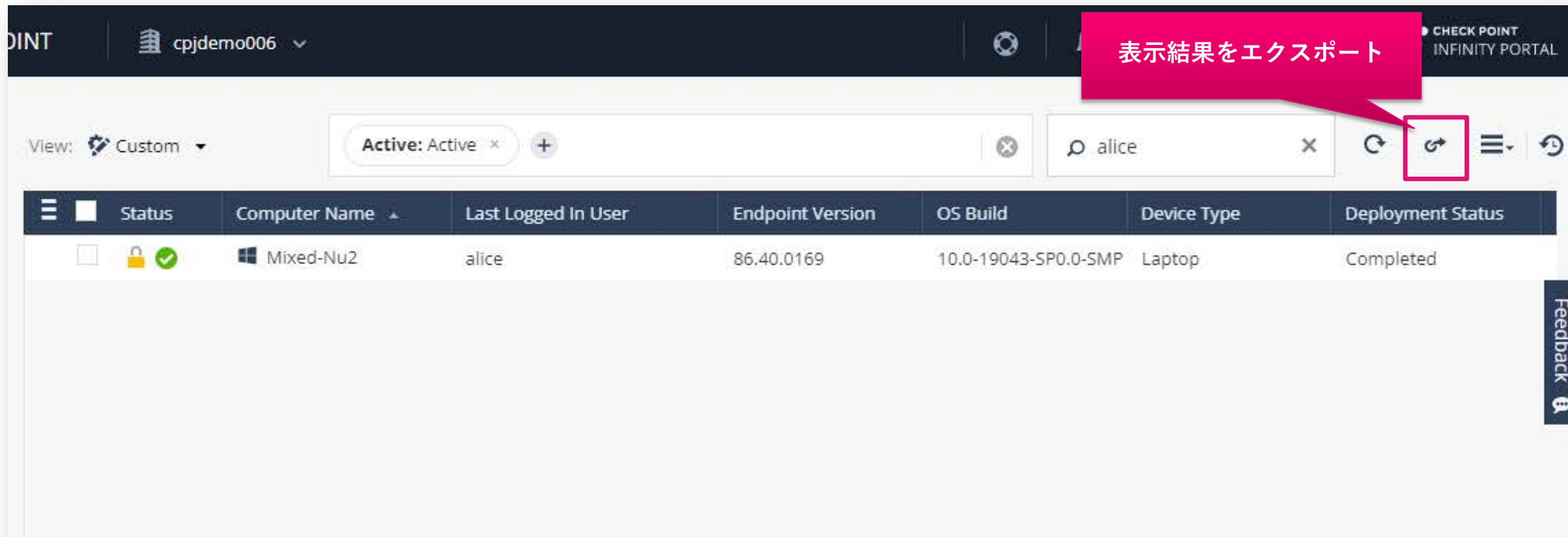
- ページ上部のフィルタツール、検索ツールを使用して、表示結果を絞り込むことができます
- フィルタツールの **+** をクリックすると、フィルタ条件を選択できます
- 検索ツールにキーワードを入力して、コンピュータを抽出することができます

The screenshot displays a security dashboard interface. At the top, there is a navigation bar with a user profile 'cpjdemo006'. Below this, a 'View: Compliance' dropdown is visible. The main content area features a table of endpoints and a 'Quick filters' panel. A search bar is located to the right of the filter panel. Three callout boxes highlight key features: 'フィルタ条件を表示' (Show filter conditions) points to the '+' icon in the filter panel; '検索キーワードを入力' (Enter search keyword) points to the search input field; and 'フィルタ条件を選択' (Select filter condition) points to the 'Active' filter option in the list.

| Status | Computer Name | Endpoint | Synced On | Device Type | Computer Location |
|--------|-----------------|-----------|-----------|-------------|-------------------|
| 🔒✅ | DESKTOP-KS61VT2 | 86.26.600 | 11:58 pm | Desktop | N/A |
| 🔒✅ | EP | 86.26.600 | 03:02 pm | Laptop | harmony.d |
| 🔒✅ | Mixed-Nu2 | 86.40.016 | 09:59 am | Laptop | N/A |
| 🔒✅ | ep-demo2 | 86.40.016 | 05:51 pm | Laptop | N/A |
| 🔒✅ | ep-demo3 | 86.50.019 | 10:00 am | Laptop | N/A |

表示結果のエクスポート

- ページ上部のエクスポートボタン  を押すと、表示結果を xlsx ファイルとしてエクスポートできます
- 表示項目のカスタマイズや、フィルタが適用された表示結果がエクスポートされます



The screenshot shows the Check Point Infinity Portal interface. At the top, there is a navigation bar with the text "DINT" and "cpjdemo006". Below this, there is a search bar containing "alice" and a filter bar with "Active: Active". The main content area displays a table with the following columns: Status, Computer Name, Last Logged In User, Endpoint Version, OS Build, Device Type, and Deployment Status. A single row is visible with the following data: Status (Active), Computer Name (Mixed-Nu2), Last Logged In User (alice), Endpoint Version (86.40.0169), OS Build (10.0-19043-SP0.0-SMP), Device Type (Laptop), and Deployment Status (Completed). The export button, represented by a document with an arrow icon, is highlighted with a red box. A red callout bubble points to this button with the text "表示結果をエクスポート".

| Status | Computer Name | Last Logged In User | Endpoint Version | OS Build | Device Type | Deployment Status |
|--------|---------------|---------------------|------------------|----------------------|-------------|-------------------|
| Active | Mixed-Nu2 | alice | 86.40.0169 | 10.0-19043-SP0.0-SMP | Laptop | Completed |

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。

The screenshot illustrates the process of isolating a computer through the HARMONY ENDPOINT interface. The interface is divided into several sections:

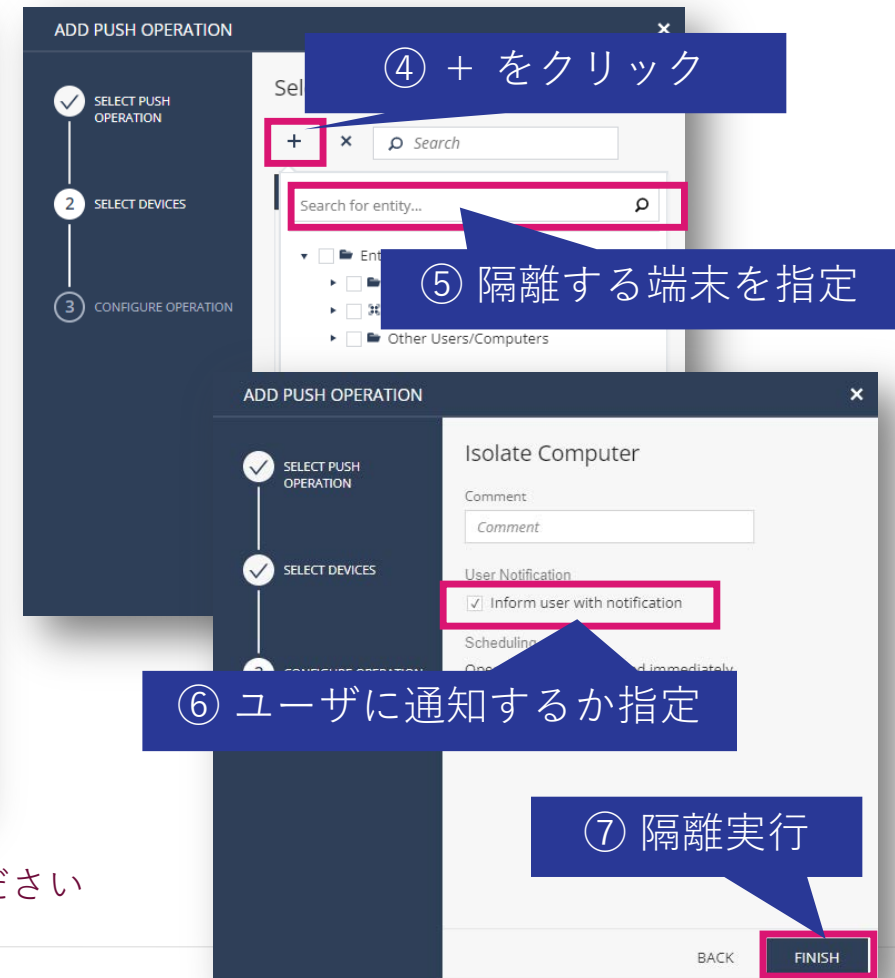
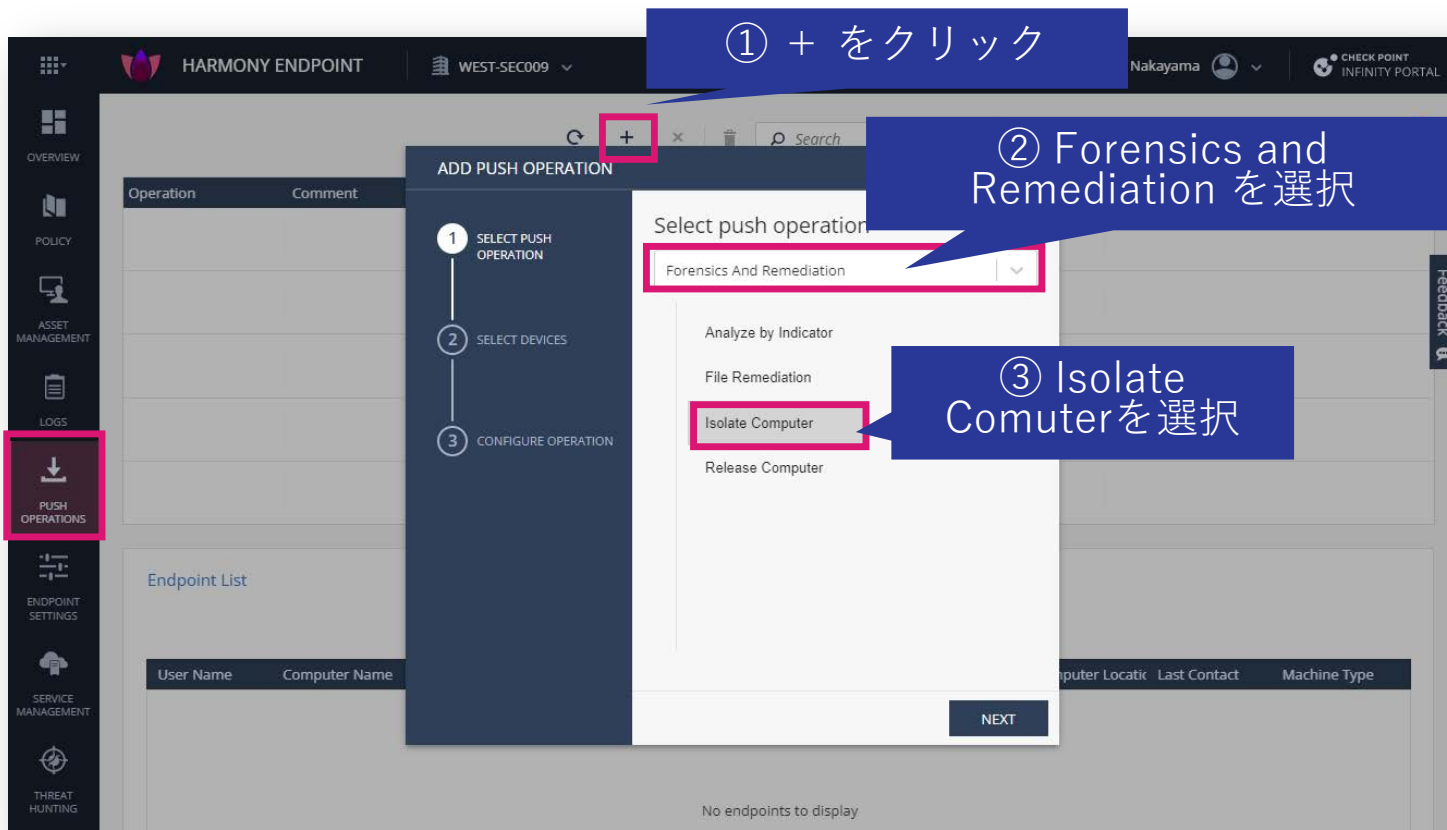
- ASSET MANAGEMENT:** The sidebar on the left has 'ASSET MANAGEMENT' selected.
- Computers Table:** The main area displays a table of computers. The first row, 'CP-DEMO', is selected. A blue callout box labeled '① 隔離する端末を選択' points to the selection checkbox.
- Computer Actions:** A dropdown menu is open, showing various actions. A blue callout box labeled '② Computer Actions をクリック' points to the 'Computer Actions' dropdown.
- Forensics & Remediation:** The 'Forensics & Remediation' option is highlighted in the dropdown menu. A blue callout box labeled '③ Forensics and Remediation をクリック' points to this option.
- Isolate Computer:** The 'Isolate Computer' option is highlighted within the 'Forensics & Remediation' submenu. A blue callout box labeled '④ Isolate Comuter をクリック' points to this option.
- PUSH OPERATION CREATION DIALOG:** A dialog box titled 'Isolate Computer' is shown on the right. It includes a 'Comment' field, a 'User Notification' section with a checked 'Inform user with notification' checkbox, and a 'Scheduling' section indicating 'Operation will be executed immediately'. A blue callout box labeled '⑤ 隔離実行' points to the 'Create' button at the bottom right of the dialog.

※ 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

The screenshot displays the Harmony Endpoint management interface. The left sidebar contains navigation options: OVERVIEW, POLICY, ASSET MANAGEMENT, LOGS, PUSH OPERATIONS (highlighted with a red box), ENDPOINT SETTINGS, and SERVICE MANAGEMENT. The main content area is titled '遠隔操作の状況' (Remote Operation Status) and features a table of operations. Below this, the 'Endpoint List' section shows the status of the operation on a specific endpoint, with a red box highlighting the 'Succeeded' status.

遠隔操作の状況

| Operation | Comment | Pushed To | Status | Admin Name | Advanced Settings | Created On | Active Until |
|----------------------------|---------|-----------|--------------------|------------------------|---|----------------------|----------------------|
| Isolate Computer | | CP-DEMO | Pushing to clients | yoshiyasun_EpMaaS_Only | View Advanced Settings... | 10 Jun 2022 06:53 pm | 11 Jun 2022 06:53 pm |
| Uninstall Client | | Lab-13 | Pushing to clients | yoshiyasun_EpMaaS_Only | View Advanced Settings... | 10 Jun 2022 04:45 pm | 11 Jun 2022 04:45 pm |
| Release Computer Isolation | | CP-DEMO | Completed | yoshiyasun_EpMaaS_Only | View Advanced Settings... | 10 Jun 2022 01:36 pm | 11 Jun 2022 01:36 pm |
| Isolate Computer | | CP-DEMO | Completed | yoshiyasun_EpMaaS_Only | View Advanced Settings... | 10 Jun 2022 11:45 am | 11 Jun 2022 11:45 am |
| Release Computer Isolation | | CP-DEMO | Completed | yoshiyasun_EpMaaS_Only | View Advanced Settings... | 10 Jun 2022 07:36 am | 11 Jun 2022 07:36 am |

Previous Page 1 of 2

Endpoint List

端末ごとの状況、結果

| User Name | Computer Name | Operation Status | Operation Status Descriptio | Operation Output | Sent To Endpoint On | Status Update Received On |
|-----------|---------------|------------------|-----------------------------|------------------|----------------------|---------------------------|
| nack | CP-DEMO | Succeeded | success | | 10 Jun 2022 06:59 pm | 10 Jun 2022 06:59 pm |

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

The screenshot shows the HARMONY END interface. The left sidebar has 'ASSET MANAGEMENT' highlighted. The main content area shows 'Computers' selected in the 'Organizational Tree'. The 'Columns' dropdown is set to 'Host Isolation'. A table displays the isolation status for two computers: CP-DEMO (Isolated) and Lab-13 (Not Isolated).

表示モードを [Host Isolation] に切り替え

コンピュータの隔離状況を確認

| Status | Computer Name | Endpoint Version | Isolation Status | Last Connection |
|-------------------------------------|---------------|------------------|------------------|----------------------|
| <input checked="" type="checkbox"/> | CP-DEMO | 86.26.6008 | Isolated | 10 Jun 2022 06:58 pm |
| <input type="checkbox"/> | Lab-13 | 86.26.6008 | Not Isolated | 03 Jun 2022 01:02 pm |

ログの表示

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)

The image shows two screenshots of the Check Point Harmony Endpoint console. The left screenshot displays the 'New Tab Catalog' with a grid of categories: Audit Logs, Access Control, Audit Overview, Threat Prevention, and General Overview. A blue callout box points to the 'Logs' category with the text '表示するカテゴリを選択' (Select the category to display). Another blue callout box points to the '+' icon in the top right of the catalog with the text '表示するログを選択' (Select the log to display). The right screenshot shows the 'Logs' view, which includes a 'Statistics' section with a bar chart and a table of log events. The table has columns for Time, Blade, Action, Severity, Confidence Level, Machine Name, Protection Type, Protection Name, and Malware Action. A blue callout box points to the 'Logs' category in the left sidebar of this view with the text '表示するログを選択'.

| Time | Blade | Action | Severity | Confidence L... | Machine Name | Protection T... | Protection Name | Malware Act... |
|--------------------------|----------------------|-------------|----------|-----------------|--------------|---------------------|--------------------|----------------|
| Mar 30, 2022 2:13:06 PM | Forensics | Detect | Low | Low | Endpoint3 | Generic | DOS/ICAR_Test_File | |
| 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 | Crit... | 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 Em... | Gen.SB.exe | Trojan", "beh |
| Mar 30, 2022 12:58:50 AM | Forensics | Prevent | High | High | Endpoint3 | File System Em... | Gen.SB.exe | Trojan", "beh |
| Mar 30, 2022 12:58:44 AM | Threat Emulation | Prevent | Low | High | Endpoint3 | File System Em... | Gen.SB.exe | Trojan", "beh |
| Mar 30, 2022 12:58:39 AM | Threat Emulation | Prevent | Low | High | Endpoint3 | File System Em... | Gen.SB.exe | Trojan", "beh |
| Mar 30, 2022 12:58:23 AM | Forensics | Prevent | High | High | Endpoint3 | File System Em... | Gen.SB.dll | Trojan |
| Mar 30, 2022 12:58:11 AM | Forensics | Prevent | High | High | Endpoint3 | File System Em... | Gen.SB.dll | Trojan |
| Mar 30, 2022 12:58:00 AM | Forensics | Prevent | High | High | Endpoint3 | File System Em... | Gen.SB.dll | Trojan |
| Mar 30, 2022 12:57:48 AM | Forensics | Prevent | High | High | Endpoint3 | File System Em... | Gen.SB.dll | Trojan |
| Mar 30, 2022 12:57:39 AM | Threat Emulation | Prevent | Low | High | Endpoint3 | File System Em... | Gen.SB.dll | Trojan |
| Mar 30, 2022 12:57:43 AM | Threat Emulation | Prevent | Low | High | Endpoint3 | File System Em... | Gen.SB.dll | Trojan |
| Mar 30, 2022 12:57:38 AM | Threat Emulation | Prevent | Low | High | Endpoint3 | File System Em... | Gen.SB.dll | Trojan |
| Mar 30, 2022 12:57:36 AM | Threat Emulation | Prevent | Low | High | Endpoint3 | File System Em... | Gen.SB.dll | Trojan |
| Mar 30, 2022 12:56:02 AM | Forensics | Prevent | High | High | Endpoint3 | File Reputation | Gen.Rep.exe | |
| Mar 30, 2022 12:55:50 AM | Forensics | Prevent | High | High | Endpoint3 | File Reputation | Gen.Rep.exe | |
| Mar 30, 2022 12:55:38 AM | Forensics | Prevent | High | High | Endpoint3 | File Reputation | Gen.Rep.exe | |
| Mar 30, 2022 12:55:26 AM | Forensics | Prevent | High | High | Endpoint3 | File Reputation | Gen.Rep.exe | |
| Mar 30, 2022 12:55:22 AM | Threat Emulation | Prevent | Low | High | Endpoint3 | File Reputation | Gen.Rep.exe | |
| Mar 30, 2022 12:55:22 AM | Threat Emulation | Prevent | Low | High | Endpoint3 | File Reputation | Gen.Rep.exe | |
| Mar 30, 2022 12:55:14 AM | Threat Emulation | Prevent | Low | High | Endpoint3 | File Reputation | Gen.Rep.exe | |
| Mar 30, 2022 12:55:13 AM | Threat Emulation | Prevent | Low | High | Endpoint3 | File Reputation | Gen.Rep.exe | |
| Mar 30, 2022 12:55:08 AM | Forensics | Prevent | Crit... | High | Endpoint3 | Static File Anal... | Gen.MLSA | |

ログの表示 (2 / 2)

事前定義されたビューの一覧

お気に入りへ登録可能

表示種別を選択

事前定義されたビューの一覧

| Favorites | Name | Category | Last Viewed | Created by |
|-----------|--------------------------------------|-------------------|----------------|-------------|
| ★ | Access Control | Access Control | 22 minutes ago | Check Point |
| ★ | Active Users | Access Control | | Check Point |
| ★ | Application Categories | Access Control | | Check Point |
| ★ | Applications and Sites | Access Control | | Check Point |
| ★ | Audit Overview | General | | Check Point |
| ★ | Content Awareness | Access Control | | Check Point |
| ★ | Cyber Attack View - Endpoint | Threat Prevention | 3 days ago | Check Point |
| ★ | Cyber Attack View - Endpoint | Threat Prevention | | Check Point |
| ★ | Cyber Attack View - Gateway | Threat Prevention | | Check Point |
| ★ | Cyber Attack View - Mobile | Threat Prevention | | Check Point |
| ★ | Data Loss Prevention (DLP) | Access Control | | Check Point |
| ★ | General Overview | General | | Check Point |
| ★ | High Bandwidth Applications | Access Control | | Check Point |
| ★ | High Risk Applications and Sites | Access Control | | Check Point |
| ★ | Important Attacks | Threat Prevention | | Check Point |
| ★ | Infected Hosts | Threat Prevention | | Check Point |
| ★ | Infinity Threat Prevention Dashboard | Threat Prevention | | Check Point |
| ★ | License Status | General | | Check Point |
| ★ | MITRE ATT&CK | Threat Prevention | | Check Point |
| ★ | MTA Live Monitoring | General | | Check Point |
| ★ | MTA Overview | General | | Check Point |
| ★ | MTA Troubleshooting | General | | Check Point |
| ★ | Remote Access | Access Control | | Check Point |
| ★ | Security Checkup Summary | General | | Check Point |
| ★ | Security Incidents | Threat Prevention | 3 days ago | Check Point |
| ★ | Threat Prevention | Threat Prevention | | Check Point |
| ★ | Web Extension Security Dashboard | General | | Check Point |

事前定義されたレポートの一覧

お気に入りへ登録可能

表示種別を選択

事前定義されたレポートの一覧

| Favorites | Name | Category | Last Viewed | Created by |
|-----------|-----------------------------------|-------------------|-------------|-------------|
| ★ | Application and URL Filtering | Access Control | 2 weeks ago | Check Point |
| ★ | Cloud Services | Access Control | | Check Point |
| ★ | Compliance Blade | Compliance | | Check Point |
| ★ | Content Awareness | Access Control | | Check Point |
| ★ | Correlated Events | General | | Check Point |
| ★ | Data Loss Prevention (DLP) | Access Control | | Check Point |
| ★ | DDOS Protector | Threat Prevention | | Check Point |
| ★ | Detailed User Activity | Access Control | | Check Point |
| ★ | GDPR Security Report | General | | Check Point |
| ★ | IntelliStore | Threat Prevention | | Check Point |
| ★ | Intrusion Prevention System (IPS) | Threat Prevention | | Check Point |
| ★ | License Inventory | General | | Check Point |
| ★ | Mobile Security Checkup | General | | Check Point |
| ★ | Network Activity | Access Control | | Check Point |
| ★ | Network Security | General | | Check Point |
| ★ | Security Checkup - Advanced | General | | Check Point |
| ★ | Security Checkup - Anonymized | General | | Check Point |
| ★ | Security Checkup - SaaS | General | | Check Point |
| ★ | Security Checkup - Statistics | General | | Check Point |
| ★ | Threat Emulation | Threat Prevention | | Check Point |
| ★ | Threat Extraction | Threat Prevention | | Check Point |
| ★ | Threat Prevention | Threat Prevention | | Check Point |
| ★ | User Activity | Access Control | | Check Point |

ログの表示：一覧表示・詳細表示 (1 / 2)

The screenshot displays the Harmony Endpoint console interface. On the left, a sidebar contains navigation options: OVERVIEW, POLICY, ASSET MANAGEMENT, LOGS (highlighted), PUSH, SETTINGS, SERVICE MANAGEMENT, and THREAT HUNTING. The main area is divided into three sections:

- Statistics:** A bar chart titled 'Sessions Timeline' showing activity for Wed 23, Sat 26, and Tue 29. Below it, a 'Blade' filter section shows percentages for various blades like Endpoint Compliance (28.6%), Anti-Malware (22.54%), Full Disk Encryption (17.23%), Threat Emulation (12.5%), Forensics (10.23%), Threat Extraction (3.79%), Media Encryption & ... (2.27%), SmartEvent Client (1.89%), Core (0.57%), and URL Filtering (0.38%). An 'Action' filter section shows Prevent (61.88%), Detect (12.15%), Allow (11.05%), Extract (11.05%), Inform User (3.31%), and Block (0.55%). A 'Severity' filter section shows Low (38.64%) and Medium (20.45%).
- Table:** A table of log entries with columns: Time, Blade, Action, Severity, Protection Type, Protection Name, and File Name. The table lists various events such as 'Detect' and 'Prevent' actions across different blades like Forensics, Endpoint Compliance, and Threat Emulation.
- Card:** A detailed view of a selected log entry. It includes 'Log Info' (Origin: cpjdemo002-d69e71e-hap2, Time: Mar 30, 2022 2:13:21 PM, Blade: Forensics, Triggered By: Windows Defender, Product Family: Endpoint, Type: Log, Attack Status: Dormant, Event Type: Forensics Case Analysis), 'Policy' (Action: Detect, Policy Date: Mar 30, 2022 12:52:35 AM, Policy Name: demo3 (Forensics), Policy Version: 3, Log Server IP: 164.100.1.8), and 'Protection Details' (Severity: Low, Confidence Level: Low, Malware Action, Protection Name: gen.win.trojan, Protection Type: Generic).

事前定義された数多くのビュー、レポートを選択して表示できます

一覧表示。ダブルクリックでログの詳細を表示。ログの詳細からフォレンジックレポートを表示可能

詳細表示

ログの表示条件を選択

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

The screenshot displays the Check Point Harmony Endpoint interface. The main window shows a list of logs with columns for Time, Blade, Action, and Severity. A blue callout box with white text says "エンTRIESをダブルクリックして、詳細を表示" (Double-click the entries to display details). A red box highlights a specific log entry: "Mar 30, 2022 12:59:02 AM | Forensics | Prevent | High | High | Endpoint3 | File System Em... | Gen.SB.exe | Trojan", which is also highlighted by a red arrow pointing to the detailed view on the right.

Log List (Highlighted Row):

| Time | Blade | Action | Severity | Category | Process | Malware Action |
|--------------------------|-----------|---------|----------|----------|-----------|-------------------------------------|
| Mar 30, 2022 12:59:02 AM | Forensics | Prevent | High | High | Endpoint3 | File System Em... Gen.SB.exe Trojan |

Log Details (Highlighted Card):

| Section | Value |
|------------------|---|
| Origin | CheckPointKitta-b14818cb-hap1 |
| Time | Oct 30, 2020 11:31:21 AM |
| Blade | Forensics |
| Triggered By | Endpoint Anti-Bot |
| Product Family | Endpoint |
| Type | Log |
| Attack Status | Blocked |
| Event Type | Forensics Case Analysis |
| Severity | Critical |
| Confidence Level | Medium |
| Malware Action | Communication with C&C |
| Action | Prevent |
| Policy Date | Sep 15, 2020 |
| Policy Name | Default Forensics settings |
| Policy Version | 1 |
| Log Server IP | 164.100.1.8 |
| Source | ip-192-168-100-5.ec2.internal (192.168.100.5) |
| Source User Name | aduser1 |
| Machine Name | DESKTOP-M5E17GCad.example.com |

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

The screenshot shows a web interface for log management. At the top left, there is a dropdown menu currently set to 'Last 7 Days'. Below it, a section titled 'Select a time filter' contains a 'Presets' table with various time-based filters. A red rectangular box highlights the 'Last 7 Days' preset and the 'Relative Time Range' section below it. To the right of the interface, a blue callout box contains the text '指定した期間でログを絞り込み'. Below that, another blue callout box contains the text '時間で指定することも可能'. The main log area shows several entries with timestamps, severity levels (Critical), and source information (CheckPoint).

| Presets | |
|---------------|-------------------------------|
| Today | (Oct 30, 2020) |
| Yesterday | (Oct 29, 2020) |
| This Week | (Since Oct 26, 2020) |
| This Month | (Since Oct 1, 2020) |
| This Year | (Since Jan 1, 2020) |
| Last Hour | (Since 2:25 PM) |
| Last 24 Hours | (Since Oct 29, 2020 3:25 PM) |
| Last 7 Days | (Since Oct 23, 2020) |
| Last Week | (Oct 19, 2020 - Oct 25, 2020) |
| Last 30 Days | (Since Sep 30, 2020) |
| Last Month | (Sep 2020) |
| Last 365 Days | (Since Oct 31, 2019) |
| Last Year | (2019) |

Relative Time Range

Date Range

Date and Time Range

Threat Emulation 2.94%

Severity Low 41.18%

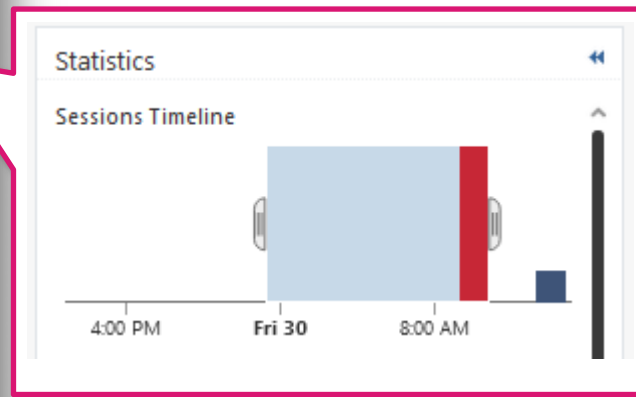
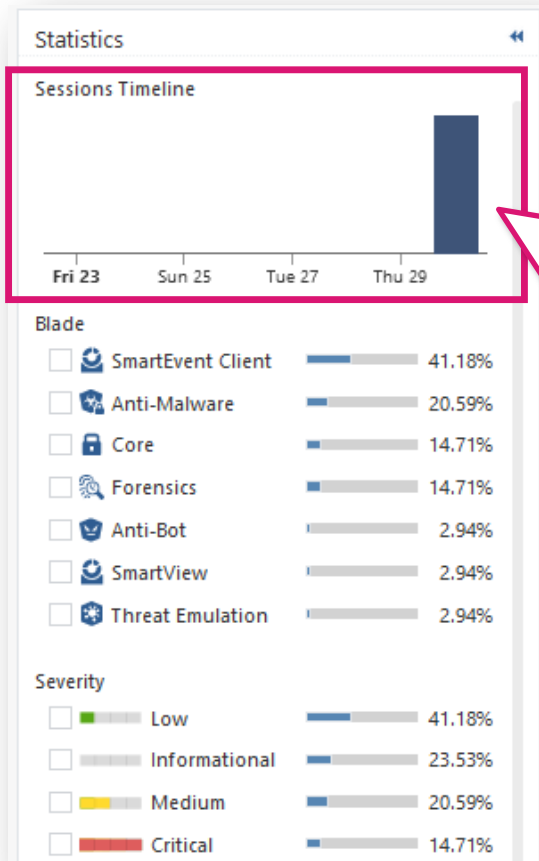
Oct 30, 2020 11:29:06 ... Critical CheckPoint

Oct 30, 2020 11:28:52 ... Critical CheckPoint

Oct 30, 2020 11:28:41 ... Critical CheckPoint

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

タイトルバーの上で、右クリック

表示プロファイルを選択

The screenshot shows a security log table with columns: Time, Blade, Action, Severity, and a context menu. The context menu is open, showing a list of display profiles. The 'Endpoint' profile is selected, and its sub-menu is also open, showing various security features like Anti-Bot, Anti-Exploit, etc. The 'Anti-Exploit' option is checked in the sub-menu.

| Time | Blade | Action | Severity | Profile | Severity | File Name | Blade | Action | Severity |
|--------------------------|----------------------|------------|----------|----------|----------|-----------|-------|--------|----------|
| Mar 30, 2022 9:09:10 AM | Endpoint Complia... | Detect | Me... | Endpoint | High | | | | |
| Mar 30, 2022 9:08:20 AM | Full Disk Encryption | | Me... | Endpoint | High | | | | |
| Mar 30, 2022 9:08:19 AM | Full Disk Encryption | | Me... | Endpoint | High | | | | |
| Mar 30, 2022 9:07:21 AM | Endpoint Complia... | Inform ... | Cri... | Endpoint | High | | | | |
| Mar 30, 2022 9:07:17 AM | Endpoint Complia... | | High | Endpoint | High | | | | |
| Mar 30, 2022 1:09:18 AM | Anti-Malware | | Low | Endpoint | High | | | | |
| Mar 30, 2022 12:59:02 AM | Forensics | Prevent | High | Endpoint | High | | | | |
| Mar 30, 2022 12:58:50 AM | Forensics | Prevent | High | Endpoint | High | | | | |
| Mar 30, 2022 12:58:44 AM | Threat Emulation | Prevent | Low | Endpoint | High | | | | |
| Mar 30, 2022 12:58:39 AM | Threat Emulation | Prevent | Low | Endpoint | High | | | | |
| Mar 30, 2022 12:58:23 AM | Forensics | Prevent | High | Endpoint | High | | | | |
| Mar 30, 2022 12:58:11 AM | Forensics | Prevent | High | Endpoint | High | | | | |

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

Mar 30, 2022 Endpoint3

| 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 | 2826815873d90ad38c5aeed57c09385d6ac |
| 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ブネットマスクを使用して、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

Mar 30, 2022 Search

| Time | Blade | Action | Severity | Confidence Le... | Protection T... | Protection Na... | File Name |
|-------------------------|----------------------|--------|----------|------------------|-----------------|-------------------|-----------------------------|
| Mar 30, 2022 2:13:21 PM | Forensics | Detect | Low | Low | Generic | gen.win.trojan | backdoor.msil.tyupkin.a.vir |
| Mar 30, 2022 2:13:06 PM | Forensics | Detect | Low | Low | Generic | DOS/EICAR_Test... | eicar_com.zip |
| Mar 30, 2022 9:09:10 AM | Endpoint Compliance | Detect | Medium | N/A | | | |
| Mar 30, 2022 9:08:20 AM | Full Disk Encryption | | Medium | N/A | | | |
| Mar 30, 2022 9:08:19 AM | Full Disk Encryption | | Medium | N/A | | | |

Mar 30, 2022 blade:forensics

| Time | Blade | Action | Severity | Confidence... | Protection Type | Protection Name | File Name |
|--------------------------|-----------|---------|----------|---------------|-----------------------|---------------------|-----------------------------|
| Mar 30, 2022 2:13:21 PM | Forensics | Detect | Low | Low | Generic | gen.win.trojan | backdoor.msil.tyupkin.a.vir |
| Mar 30, 2022 2:13:06 PM | Forensics | Detect | Low | Low | Generic | DOS/EICAR_Test_File | eicar_com.zip |
| Mar 30, 2022 12:59:02 AM | Forensics | Prevent | High | High | File System Emulation | Gen.SB.exe | 14e48d3aa7b9058c56882eb |
| Mar 30, 2022 12:58:50 AM | Forensics | Prevent | High | High | File System Emulation | Gen.SB.exe | f_000031 |
| Mar 30, 2022 12:58:23 AM | Forensics | Prevent | High | High | File System Emulation | Gen.SB.dll | 7e2b1bbffa7f05e7bf57ee60 |

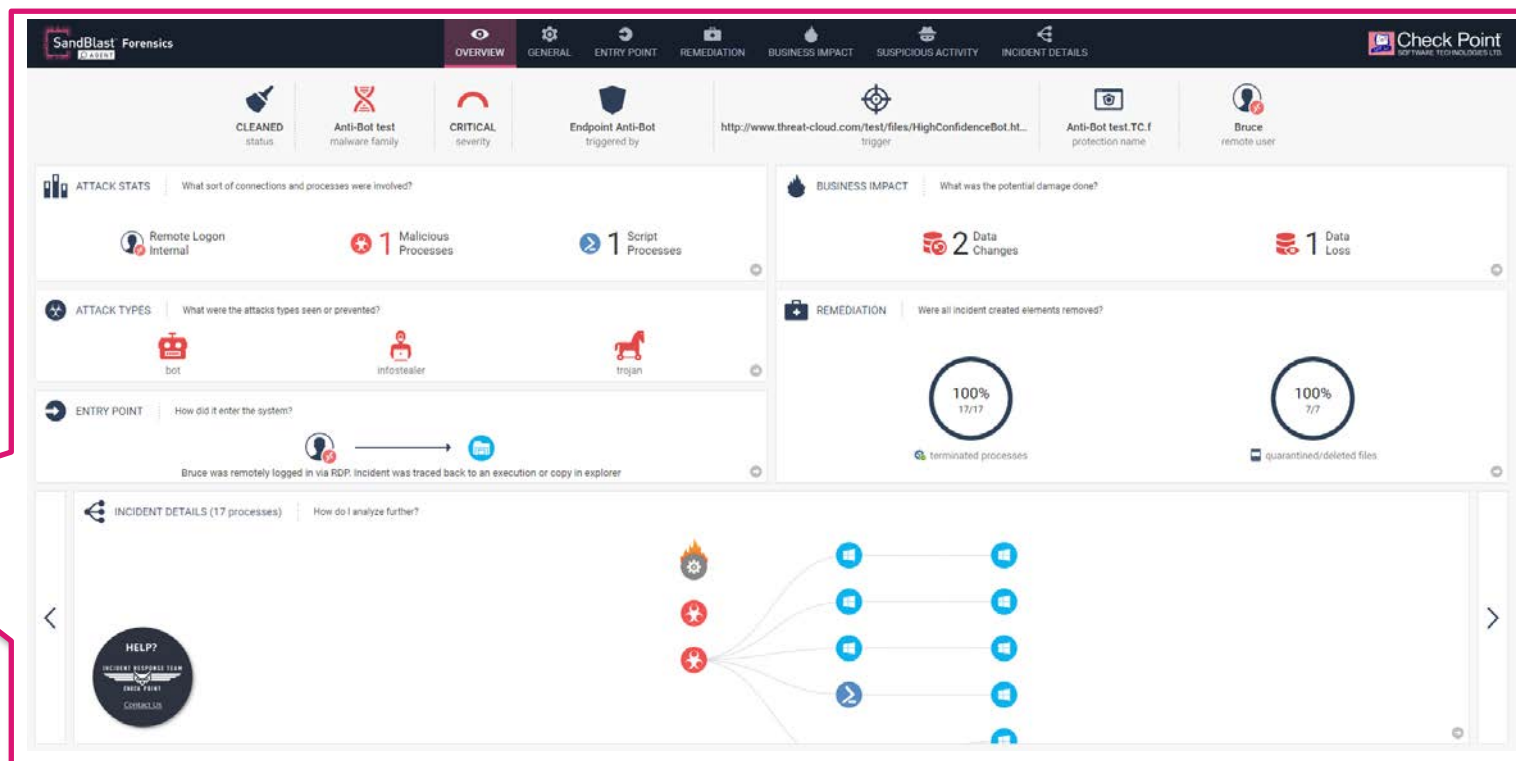
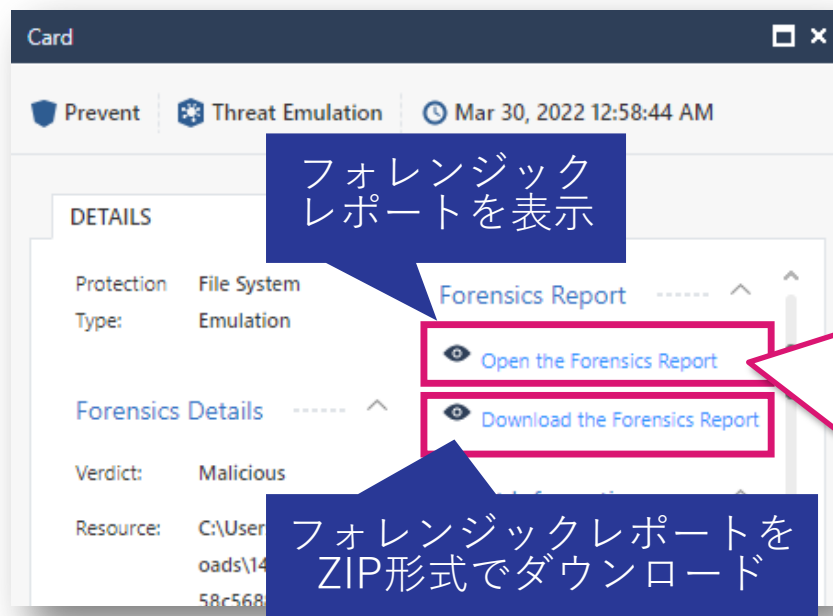
Mar 30, 2022 blade:forensics AND severity:Critical

| Time | Blade | Action | Severity | Confidence Level | Protection Type | Protection Name | File Name |
|--------------------------|-----------|---------|----------|------------------|----------------------|-----------------|--|
| Mar 30, 2022 12:55:08 AM | Forensics | Prevent | Critical | High | Static File Analysis | Gen.MLSA | 581cf8c1-4f20-4abf-97e7-8895a0117b40.tmp |
| Mar 30, 2022 12:54:35 AM | Forensics | Prevent | Critical | High | File Reputation | Gen.Rep.dll | unconfirmed 344285.crdownload |

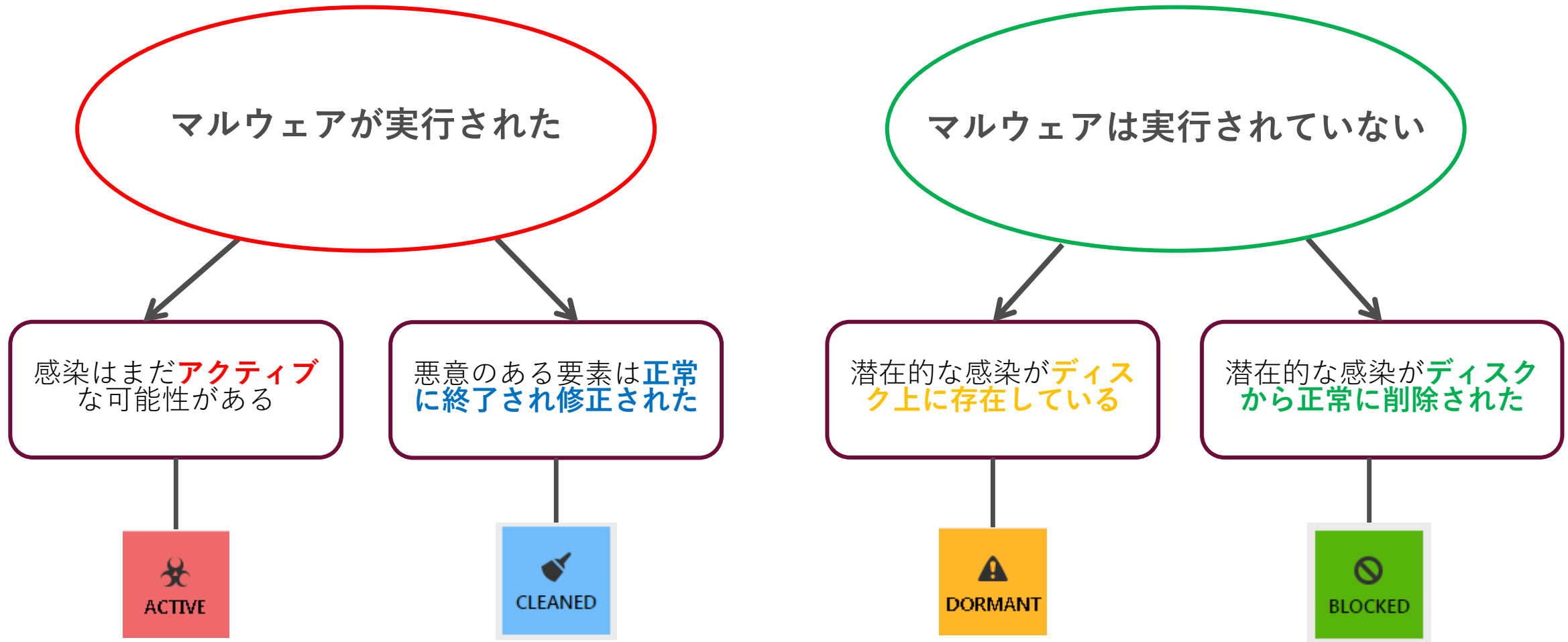
フォレンジックレポート

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

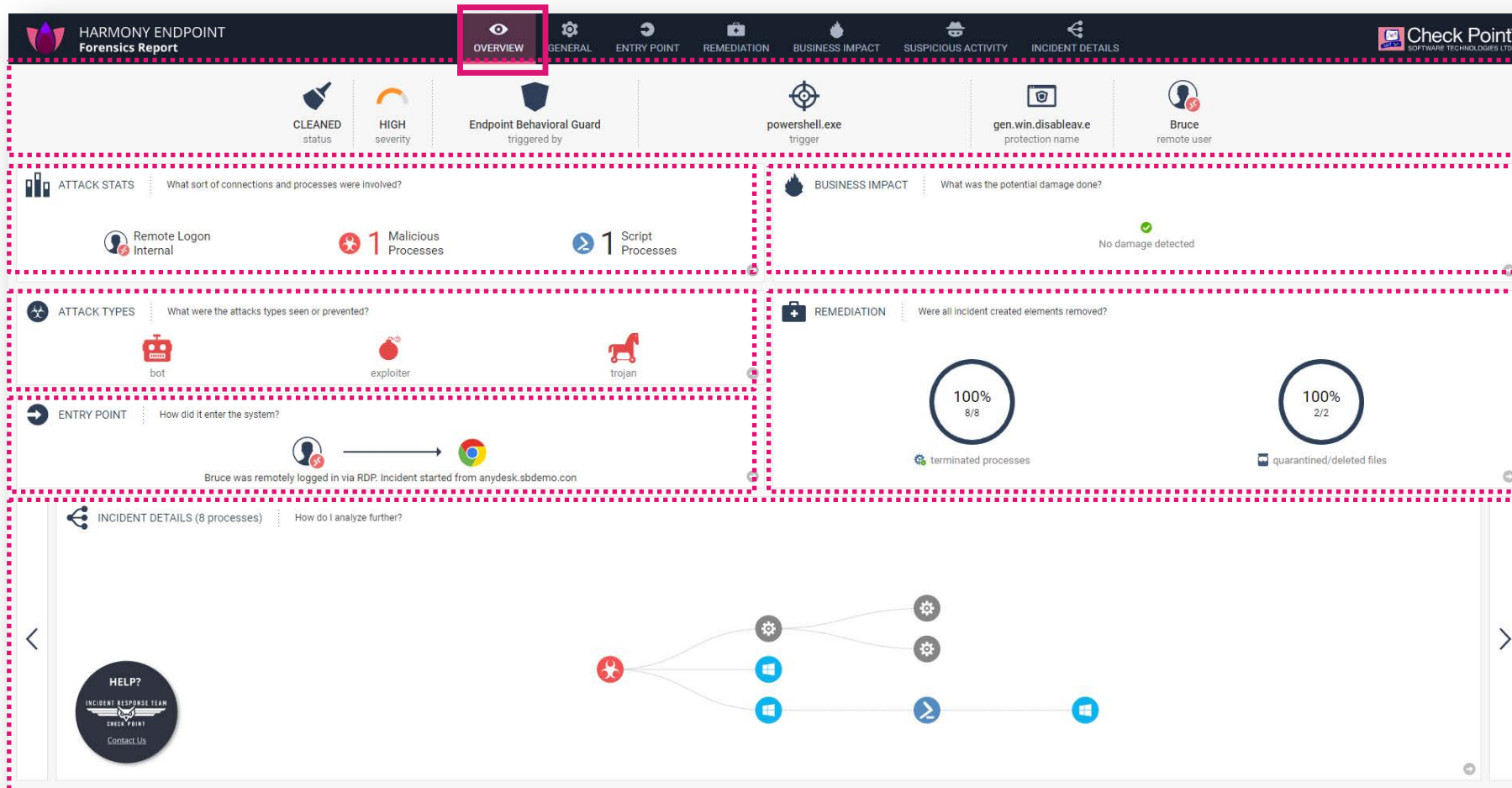
攻撃概要

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

The screenshot displays the SandBlast Forensics interface for an incident. The top navigation bar includes tabs for OVERVIEW, GENERAL (selected), ENTRY POINT, REMEDIATION, BUSINESS IMPACT, SUSPICIOUS ACTIVITY, and INCIDENT DETAILS. The main content is divided into three sections:

- ATTACK INFORMATION:** Shows the Malware Family as "Anti-Bot test" and lists detected threats: bot, infostealer, and trojan.
- GENERAL DETAILS:** Provides a comprehensive overview of the incident, including:
 - Incident ID: b6a13402-7105-4a4b-8d85-b14dacc6f9b9
 - Analysis Time: 12/10/2021, 6:36:32 PM
 - Client Version: 84.50.7526
 - PC Name: PROTECTED-USER
 - Machine Type: Desktop
 - OS: Windows 10
 - Machine Roles: Microsoft Print to PDF, Microsoft XPS Document Writer, WCF Services, TCP Port Sharing, Media Features, Windows Media Player, SMB 1.0/CIFS Automatic Removal, Remote Differential Compression API Support, .NET Framework 4.8 Advanced Services, Windows Search, Windo...
 - Domain: SBdemo.com
 - IP Address: 10.128.0.12
 - User Name: SBDEMO\Bruce
 - User SID: S-1-5-21-867849086-1392971733-3836376186-1106
 - Logon Time: 12/10/2021, 3:50:16 PM
 - Logon Type: Remote Desktop Protocol (RDP)
 - Remote PC: BOAZ-GAR-JUMP-S
 - Remote IP: 10.128.0.14 (Internal)
- DETECTION DETAILS:** Details the specific detection event:
 - Description: Endpoint Anti-Bot prevented access to URL: http://www.threat-cloud.com/test/files/HighConfidenceBot.html
 - Trigger Matched: http://www.threat-cloud.com/test/files/HighConfidenceBot.html
 - Trigger Actual: http://www.threat-cloud.com/test/files/HighConfidenceBot.html
 - Trigger Process: c:\users\bruce\documents\oem471b.exe
 - Trigger Args: (empty)
 - Trigger App: Endpoint Anti-Bot
 - Trigger Rep: Malicious
 - Trigger MD5: N/A
 - Mode: Prevent
 - Confidence: High
 - Severity: Critical
 - Protection Name: Anti-Bot test.TC.f
 - Trigger Time: 12/10/2021, 6:36:21 PM
 - Trigger Type: URL
 - Trigger PID: 5700
- ATTACK STATS:** A summary of attack metrics:
 - remote (RDP) logons: 1
 - malicious connections: 0
 - suspicious connections: 0
 - unclassified connections: 0
 - malicious processes: 1
 - suspicious processes: 0
 - unclassified processes: 1
 - unsigned processes: 3
 - script processes: 1
 - windows os processes: 5
 - malicious files: 1
 - suspicious files: 0

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

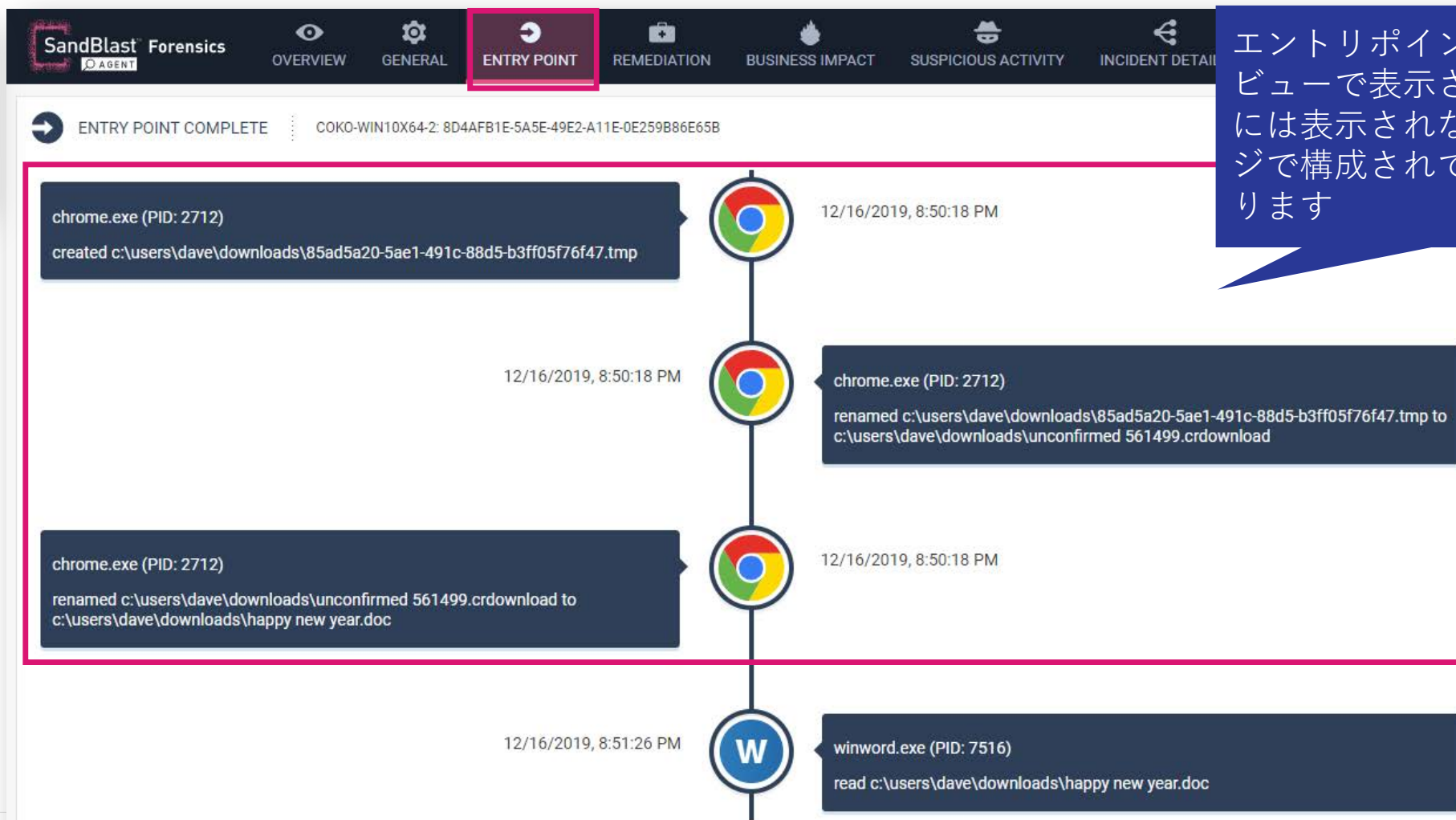
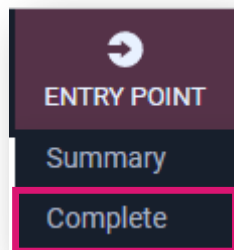
The screenshot displays the SandBlast Forensics interface. On the left, a sidebar menu includes 'ENTRY POINT', 'Summary', and 'Complete'. The main content area shows the 'ENTRY POINT SUMMARY' for a specific incident (COKO-WIN10X64-2: 8D4AFB1E-5A5E-49E2-A11E-0E259B86E65B). The summary is a flow diagram with two nodes:

- Node 1 (Top):** A Chrome icon with a text box stating: "chrome.exe (PID: 2712) renamed [85ad5a20-5ae1-491c-88d5-b3ff05f76f47.tmp] to [happy new year.doc]". The timestamp is "12/16/2019, 8:50:18 PM".
- Node 2 (Bottom):** A Word icon with a text box stating: "winword.exe (PID: 7516) read [happy new year.doc]". The timestamp is "12/16/2019, 8:51:26 PM".

The nodes are connected by a vertical line, indicating a sequence of events.

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



エントリーポイントは、完全なビューで表示され、**Summary**には表示されない複数のステージで構成されていることが分かります

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

The screenshot displays the SandBlast Forensics interface, specifically the Remediation section. The top navigation bar includes tabs for OVERVIEW, GENERAL, ENTRY POINT, REMEDIATION (selected), BUSINESS IMPACT, SUSPICIOUS ACTIVITY, and INCIDENT DETAILS. The user is logged in as 'PROTECTED-USER: b6a13402-7105-4a4b-8d85-b14dacd6f9b9'.

REMEDIATION POLICY

Remediation: Enabled: Incident remediation is enabled by policy for Endpoint Anti-Bot with confidence (High).

Malicious: Terminate and Quarantine

Unknown: Terminate and Quarantine

Suspicious: Terminate and Quarantine

Trusted: Terminate

REMEDIATION DETAILS

This section describes all the remediation actions that were taken.

Already Deleted Files: 3 deleted

These are files that were already deleted before the analysis completed.

| Reputation | File Name | File Path | MD5 | Status |
|------------|---|--|----------------------------------|---------|
| ? | oem471b.exe | c:\users\bruce\documents\oem471b.exe | 7c114e4c2b3c402499533f2b6a65027b | Deleted |
| ? | oem5496.bat | c:\users\bruce\appdata\local\temp\oem5496.bat | | Deleted |
| ? | __psscscriptpolicytest_j35iavai.5pf.ps1 | c:\users\bruce\appdata\local\temp_psscscriptpolicytest_j35iavai.5pf.ps1 | | Deleted |

Quarantined Files: 4 quarantined

These are files that have been quarantined by SBA.

| Reputation | File Name | File Path | MD5 | Status |
|------------|-------------|--|----------------------------------|-------------|
| * | bot.exe | c:\users\bruce\documents\received files\bot.exe | 36bb9bdded3a80e75890838385cae58e | Quarantined |
| ? | oem4719.exe | c:\users\bruce\appdata\local\temp\oem4719.exe | da0b3bab43e17b842b5d52a509c0add2 | Quarantined |
| ? | oem471a.exe | c:\programdata\oem471a.exe | da0b3bab43e17b842b5d52a509c0add2 | Quarantined |
| ? | oem471c.exe | c:\users\bruce\appdata\roaming\microsoft\windows\start menu\programs\startup\oem471c.exe | 7c114e4c2b3c402499533f2b6a65027b | Quarantined |

Already Terminated Processes: 16 terminated

Terminated Processes: 1 terminated

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

The screenshot displays the SandBlast Forensics interface for a Business Impact report. The top navigation bar includes tabs for OVERVIEW, GENERAL, ENTRY POINT, REMEDIATION, BUSINESS IMPACT (selected), SUSPICIOUS ACTIVITY, and INCIDENT DETAILS. The report title is "BUSINESS IMPACT (2 categories, 3 events)" for a "PROTECTED-USER: b6a13402-7105-4a4b-8d85-b14dacd6f9b9".

The main content area is divided into two sections:

- Data Tampering (2 events):** User files that were modified or deleted in the incident. A search bar is present. The table below shows two entries:

| File Name | File Path | Action | Event Time |
|---------------------------|--|--------|------------------------|
| avt_local.png | c:\users\bruce\AppData\Local\lan messenger\lan messenger\avt_local.png | Write | 12/10/2021, 3:50:52 PM |
| avt_42010a800016admin.png | c:\users\bruce\AppData\Local\lan messenger\lan messenger\cache\avt_42010a800016admin.png | Delete | 12/10/2021, 3:51:03 PM |

Showing 1 to 2 of 2 entries

- Data Loss (1 event):** User files that were likely accessed in the incident. A search bar is present. The table below shows one entry:

| File Name | File Path | Action | Event Time |
|-------------------|--|--------|------------------------|
| companysecret.doc | c:\users\bruce\documents\companysecret.doc | Read | 12/10/2021, 6:36:19 PM |

Showing 1 to 1 of 1 entries

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

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

MITRE ATT&CK™ Matrix: PROTECTED-USER: b6a13402-7105-4a4b-8d85-b14dacd6f9b9

These are the tactics and techniques as described by the MITRE ATT&CK™ framework.

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command and Control | Exfiltration | Impact |
|----------------------------------|---|--|--|--|-------------------|--|---------------------------------|-----------------------------------|------------------------------------|--------------|---------------------------------------|
| Remote Logon Internal 1 event | Command-Line Interface 2 events | Registry Run Keys / Startup Folder 4 events | Bypass User Account Control 1 event | Bypass User Account Control 1 event | | Application Window Discovery 5 events | Third-party Software 1 event | Data from Local System 1 event | Commonly Used Port 6 events | | Data Encrypted for Impact 2 events |
| Valid Accounts 1 event | Execution through API 13 events | Scheduled Task 3 events | Scheduled Task 3 events | File Deletion 2 events | | Process Discovery 4 events | | | Listening Port 1 event | | |
| | Execution through Module Load 5 events | Valid Accounts 1 event | Valid Accounts 1 event | Modify Registry 12 events | | Remote System Discovery 1 event | | | Uncommonly Used Port 279 events | | |
| | Local WMI Execution 1 event | | Vertical Privilege Escalation 15 events | Scripting 3 events | | | | | | | |
| | PowerShell | | | Valid Accounts | | | | | | | |

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

The screenshot displays the SandBlast Forensics interface. The top navigation bar includes tabs for OVERVIEW, GENERAL, ENTRY POINT, REMEDIATION, BUSINESS IMPACT, SUSPICIOUS ACTIVITY (selected), and INCIDENT DETAILS. The main content area shows a list of suspicious activity categories for a specific user (PROTECTED-USER: b6a13402-7105-4a4b-8d85-b14dacd6f9b9). The categories are:

- Vertical Privilege Escalation (15 events)
- System Security Policy Change (1 event)
- Data Encrypted for Impact (2 events)
- Listening Port (1 event)
- Remote System Discovery (1 event)
- Command-Line Interface (2 events)

The 'Data Encrypted for Impact' category is expanded, showing a detailed description: "Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted. In the case of ransomware, it is typical that common user files like Office documents, PDFs, images, videos, audio, text, and source code files will be encrypted. In some cases, adversaries may encrypt critical system files, disk partitions, and the MBR. To maximize impact on the target organization, malware designed for encrypting data may have worm-like features to propagate across a network by leveraging other attack techniques like Valid Accounts, Credential Dumping, and Windows Admin Shares."

Below the description, a table lists specific events:

| Description | Time |
|--|------------------------|
| bot.exe (PID: 5608) modified HKU\s-1-5-21-867849086-1392971733-3836376186-1106\hku\software\microsoft\windows\currentversion\policies\ | 12/10/2021, 6:36:16 PM |
| lmc.exe (PID: 788) modified avt_local.png in c:\users\bruce\appdata\local\lan messenger\lan messenger | 12/10/2021, 3:50:52 PM |
| lmc.exe (PID: 788) modified avt_42010a800016admin.png in c:\users\bruce\appdata\local\lan messenger\lan messenger\cache | 12/10/2021, 3:51:03 PM |

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

The screenshot displays the SandBlast Forensics interface for a specific user. The top navigation bar includes tabs for OVERVIEW, GENERAL, ENTRY POINT, REMEDIATION, BUSINESS IMPACT, SUSPICIOUS ACTIVITY (selected), and INCIDENT DETAILS. The main content area is divided into two sections: NETWORK CONNECTIONS MAP and NETWORK ACTIVITY.

NETWORK CONNECTIONS MAP: A world map showing network connections. The United States is highlighted in red. To the right, a table summarizes activity by country:

| Country | Benign | Unknown | Suspicious | Malicious |
|---------------|--------|---------|------------|-----------|
| United States | 1 | 1 | 0 | 1 |
| Unknown | 4 | 1 | 0 | 0 |

NETWORK ACTIVITY: A table showing network activity for the user. The user ID is PROTECTED-USER: b6a13402-7105-4a4b-8d85-b14dacc6f9b9. The view is set to URLs (2). The table shows the following activity:

| Rep | Malware Family | Risk | URL | IP | Type | Country |
|-----|----------------|------|---|---------------|----------|---------------|
| 1 | | | http://dropbox-docs.com/download/stage2.exe | 10.128.0.22 | Internal | Unknown |
| 100 | Anti-Bot test | | http://www.threat-cloud.com/test/files/HighConfidenceBot.html | 209.87.209.71 | External | United States |

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

The screenshot displays the SandBlast Forensics interface. At the top, there are navigation tabs: OVERVIEW, GENERAL, ENTRY POINT, REMEDIATION, BUSINESS IMPACT, SUSPICIOUS ACTIVITY, and INCIDENT DETAILS. The main area shows a 'TREE VIEW (17 processes)' for a 'PROTECTED-USER: b6a13402-7105-4a4b-8d85-b14dacc6f9b9'. The process tree includes nodes like 'lmc.exe 788' (Attack Start, Listening Port, Dropped Executable, Uncommonly Used Port, Modify Registry...), 'bot.exe 64' (Unsigned Process), and 'bot.exe 5608' (Registry Run Keys / Startup Folder Escalation, Dropped Executable, System Security Policy Change...). Other processes shown include 'schtasks.exe' and 'conhost.exe' instances. A detailed view for 'bot.exe' is shown at the bottom, including fields for Process Name, Path, Start Time, Close Time, Created By, Parent Chain, Arguments, PID, Duration, and Created By PID.

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

The screenshot displays the SandBlast Forensics interface in the 'INCIDENT DETAILS' view. The main area shows a 'TREE TIMELINE VIEW (17 processes)' for a 'PROTECTED-USER: b6a13402-7105-4a4b-8d85-b14dacd6f9b9'. The timeline spans from 12/10/2021, 3:50:47 PM to 12/10/2021, 6:36:16 PM. A process tree is visible with nodes for 'lmc.exe 788', 'bot.exe 64', 'bot.exe 5608', 'schtasks.exe 3772', and 'conhost.exe 6716'. Each node includes a brief description of its activity, such as 'Attack Start, Listening Port Dropped Executable, Uncommonly Used Port Modify Registry...' for lmc.exe and 'Persistence, Registry Run Keys / Startup Folder Vertical Privilege Escalation, Dropped Executable System Security Policy Change...' for bot.exe 5608. A blue callout box points to the tree with the text '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'. Below the timeline, a detailed view for 'lmc.exe' is shown, including its path, start time, and parent chain.

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

| Process Name | Path | Start Time | Close Time | PID | Duration | Created By | Created By PID |
|--------------|--|------------------------|------------|-----|----------|------------|----------------|
| lmc.exe | c:\program files (x86)\lan messenger\lmc.exe | 12/10/2021, 3:50:47 PM | | 788 | | | 0 |

Parent Chain: smss.exe (PID : 304 Date : 10-Dec-2021 03:15:47) -->smss.exe (PID : 8396 Date : 10-Dec-2021 06:50:11) -->winlogon.exe (PID : 7748 Date : 10-Dec-2021 06:50:12) -->userinit.exe (PID : 1724 Date : 10-Dec-2021 06:50:26) -->explorer.exe (PID : 12144 Date : 10-Dec-2021 06:50:26)

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

SandBlast Forensics AGENT

OVERVIEW GENERAL ENTRY POINT REMEDIATION BUSINESS IMPACT SUSPICIOUS ACTIVITY INCIDENT DETAILS

Check Point SOFTWARE TECHNOLOGIES LTD.

SCRIPT & SHORTCUT CONTENT PROTECTED-USER: b6a13402-7105-4a4b-8d85-b14dacd6f9b9

This view is used to display AMSI, WmiGet, Shortcut and other content that was part of the incident. Click on the row of interest to view its contents.

| File/Process Name | Args | Type |
|------------------------|---|------|
| powershell.exe (11312) | -c \$proc=([WMICLASS]ROOT\CIMV2:win32_process).Create('C:\Users\bruce\Documents\oem471B.exe') | AMSI |

AMSI content for: powershell.exe (11312)







```
$proc=([WMICLASS]ROOT\CIMV2:win32_process).Create('C:\Users\bruce\Documents\oem471B.exe')  
  
win32_process.GetObject();  
win32_process.GetObject();  
Win32_Process.GetObject();  
Win32_Process.GetObject();  
SetPropValue.CommandLine("C:\Users\bruce\Documents\oem471B.exe");
```






選択

詳細を表示

フォレンジックレポート：凡例

Graph Legends

-  Process is known to be malicious
-  Reputation is not known for process
-  Process is trusted operating system process
-  Process has damage events
-  Process has different privilege level than start
-  Process is currently selected

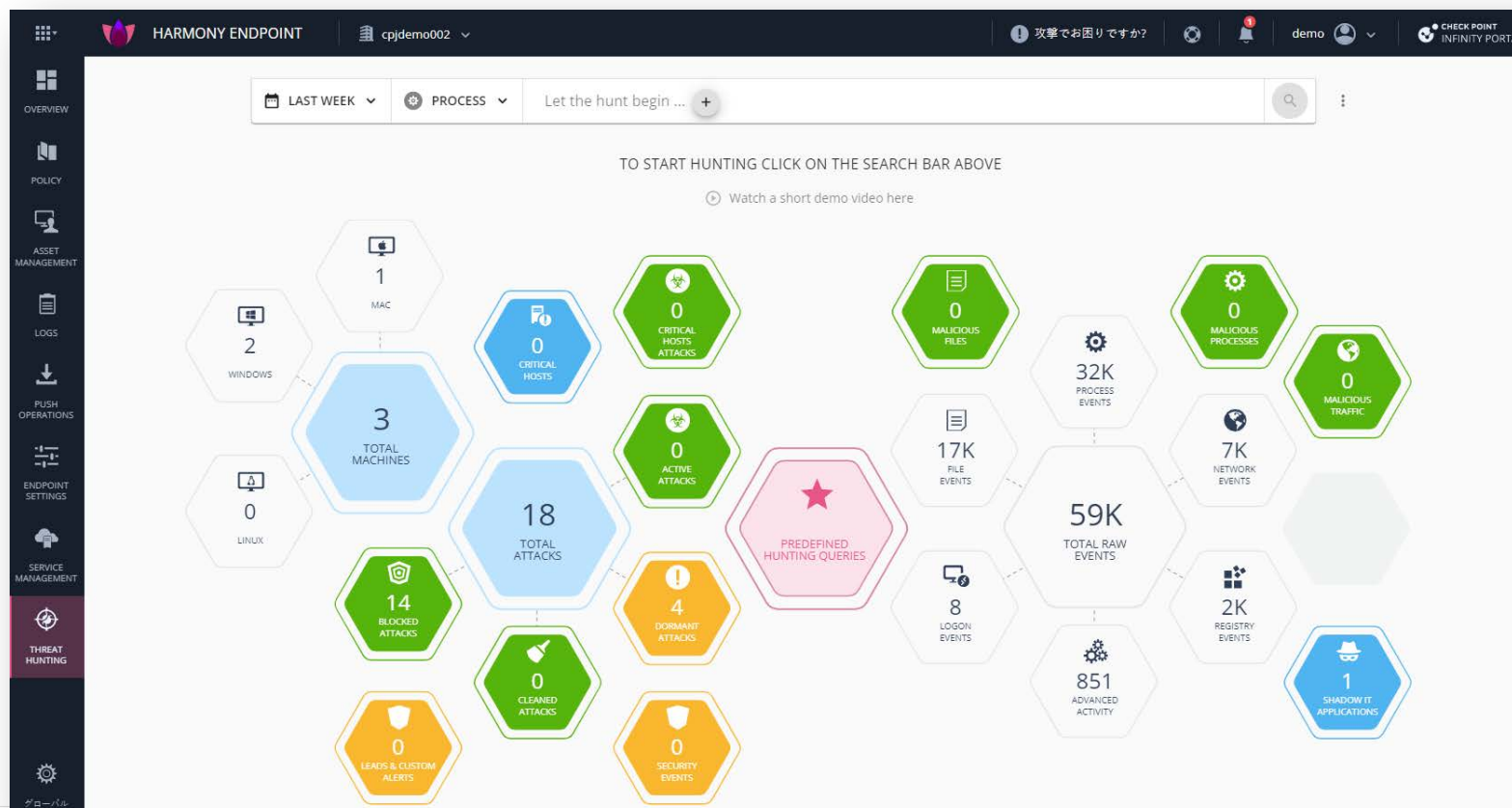
-  Parent Process X executing Parent Process Y
-  Selected Process Y 's backing file was created by X
-  Selected Process X created the file backing Y
-  Process X injected into Process Y
-  Link between 2 different Sub-Trees. Select process Y to see the real relationship.

THREAT HUNTING

The background features a series of overlapping, rounded rectangular shapes in various shades of purple, magenta, and pink. These shapes are arranged in a way that creates a sense of depth and movement, with some appearing to be in front of others. The overall color palette is vibrant and modern.

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

簡単操作によるカスタムクエリ

事前定義されたクエリ

組織への攻撃の概要を表示

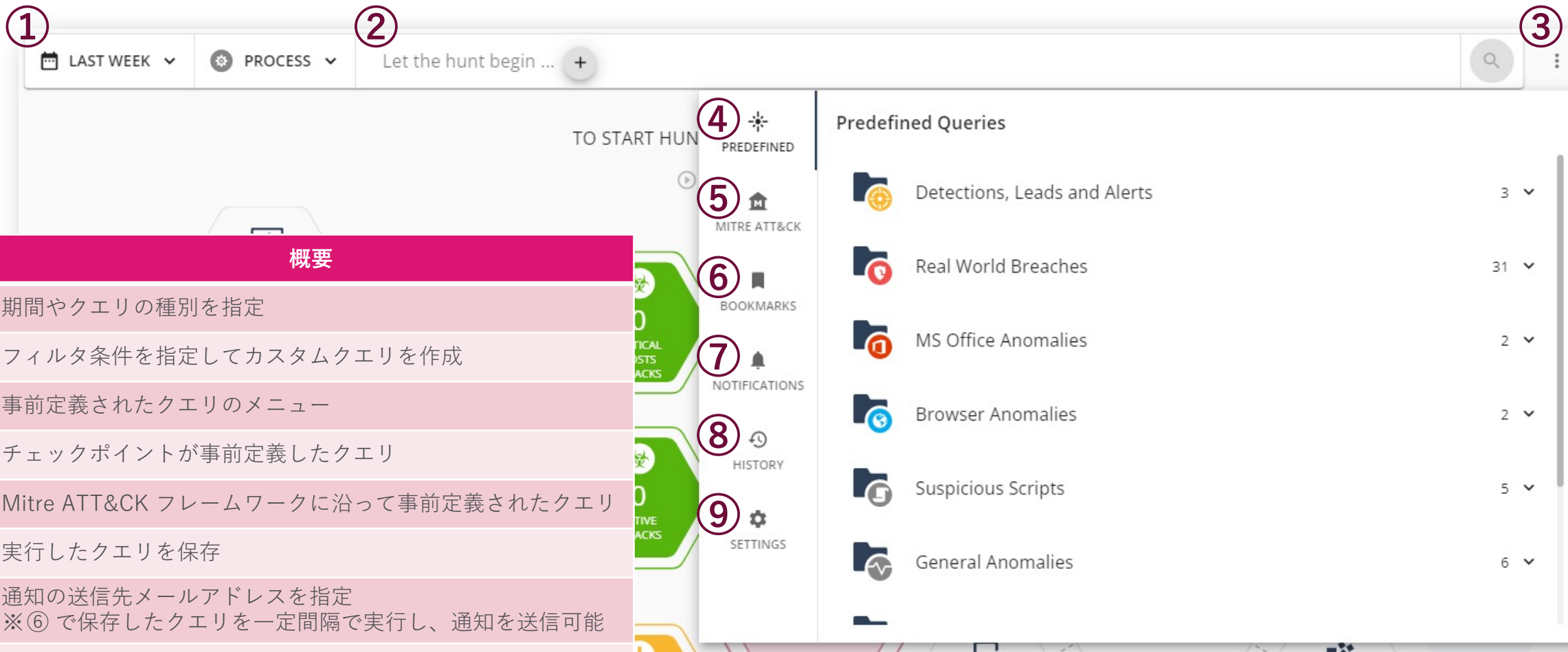
ドリルダウンで一覧表示

各レコードの詳細表示

| DETECTION EVENT INFORMATION | ASSET | ADDITIONAL INFORMATION |
|--|--|--|
| Trigger: <i>breakfast</i> Triggered By: External A/I | User: <i>nack</i> Machine: <i>ENDPOINTS</i> | Name: <i>explorer.exe</i> Arg: <i>Arg</i> |
| Trigger: <i>bridge4.jp</i> Triggered By: External A/I | User: <i>nack</i> Machine: <i>ENDPOINTS</i> | Name: <i>explorer.exe</i> Arg: <i>Arg</i> |
| Trigger: <i>backdoor.mal.exploit.a.v</i> Triggered By: External A/I | User: <i>nack</i> Machine: <i>ENDPOINTS</i> | Name: <i>explorer.exe</i> Arg: <i>Arg</i> |
| Trigger: <i>msar.com.jp</i> Triggered By: External A/I | User: <i>nack</i> Machine: <i>ENDPOINTS</i> | Name: <i>explorer.exe</i> Arg: <i>Arg</i> |
| Trigger: <i>f_00025d</i> Triggered By: Endpoint File Reputation | User: <i>nack</i> Machine: <i>AZUREWINDOWSSER</i> | Name: <i>Not Found</i> Arg: <i>Arg</i> |

| DETECTION DETAILS | ASSET DETAILS | PROCESS DETAILS | OPERATION NAME |
|--|---|---|---|
| Trigger Path: <i>C:\ProgramData\1-5-21-94771...</i> Triggered By: <i>External A/I</i> Attack Status: <i>Detected</i> Trigger Process: <i>C:\Windows\explorer.exe</i> Attack User Domain: <i>DESKTOP-MFYATQND</i> Attack User Name: <i>nack</i> Third Party: <i>Windows Defender</i> Security: <i>Low</i> Confidence: <i>Low</i> Enforcement: <i>Detect</i> Binary Path: <i>explorer.exe\explorer.exe</i> Binary File Name: <i>explorer.exe</i> Trigger File Name: <i>C:\ProgramData\1-5-21-94771...</i> Trigger File Name: <i>explorer.exe</i> Creating Process: <i>C:\Windows\explorer.exe</i> Creating Process MD5: <i>25b0fbae72248d9f6a617519f1611739...</i> Creating Process Name: <i>explorer.exe</i> Creating Process Signer: <i>Microsoft Windows</i> Creating Process PID: <i>1136</i> Creating Process Start Time: <i>164856504029</i> Report ID: <i>64432BC8118-48E7-8476-31...</i> Remediation Policy: <i>Disabled: incident remediation...</i> | User: <i>nack</i> Machine: <i>ENDPOINTS</i> OS Name: <i>Windows</i> Host Type: <i>VirtualMachine</i> OS Version: <i>Microsoft Windows 10 Enterprise Evaluation...</i> Product Version: <i>10.0.22000</i> User Name: <i>Domain\user\Nack</i> User ID: <i>210856e72248d9f6a617519f1611739...</i> Classification: <i> benign</i> Signed By: <i>Microsoft Windows</i> Parent Name: <i>Not Found</i> Parent PID: <i>Not Found</i> | Name: <i>explorer.exe</i> Directory: <i>C:\Windows</i> Full Path: <i>C:\Windows\explorer.exe</i> Start Time: <i>2022-05-30T09:00:50.625</i> PID: <i>1136</i> Process ID: <i>210856e72248d9f6a617519f1611739...</i> | <i>explorer.exe</i> Date: <i>03/30/2022</i> Time: <i>2:13:50 PM</i> |

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 ※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

The screenshot displays the Threat Hunting interface. At the top, there is a search bar with the text "Let the hunt begin ..." and a search icon. Below the search bar, there is a dropdown menu for "LAST DAY" which is currently expanded to show options: "Last Day", "Last 2 Days", "Last Week", and "Custom". A red box highlights this dropdown menu. Below the dropdown menu, there is a "PROCESS" dropdown menu. In the center, there is a "Select specific dates" dialog box. This dialog box contains two calendar views for April 2022. The first calendar shows the date "Apr 4" at "12:00 AM PM". The second calendar shows the date "Apr 4" at "11:59 AM PM". A red box highlights the "Select specific dates" dialog box. A blue callout box with white text points to the "Custom" option in the dropdown menu and contains the following text: 「Custom」を選択し、任意の期間を設定することも可能
※ 但し、データの保存期間は、標準では7日間

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

The screenshot displays the Threat Hunting interface. A blue callout box labeled "クエリ種別を指定" (Specify query type) points to the "PROCESS" dropdown menu, which is open and shows a list of categories: Process, Detection Event, File, Network, Registry, Logon, Script, Remote Execution, Advanced Activity, Indirect Execution, and Email. Another blue callout box labeled "フィルタ条件を追加" (Add filter condition) points to a "+" button in the header. A third blue callout box labeled "フィルタ条件を指定" (Specify filter condition) points to the "Add Filter" dialog box. This dialog box contains a table with columns "Indicator" and "Operator". The "Indicator" dropdown is set to "Process Name" and the "Operator" dropdown is set to "Is". Below the table is a text input field containing "Add a single value...". At the bottom of the dialog are "CANCEL" and "ADD" buttons. The background of the interface shows various hexagonal tiles representing different event categories and counts: 2 WINDOWS, 0 CRITICAL HOSTS, 0 ACTIVE ATTACKS, 25K FILE EVENTS, 14K NETWORK EVENTS, 277K, 0 MALICIOUS PROCESSES, and 0 MALICIOUS TRAFFIC.

(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 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

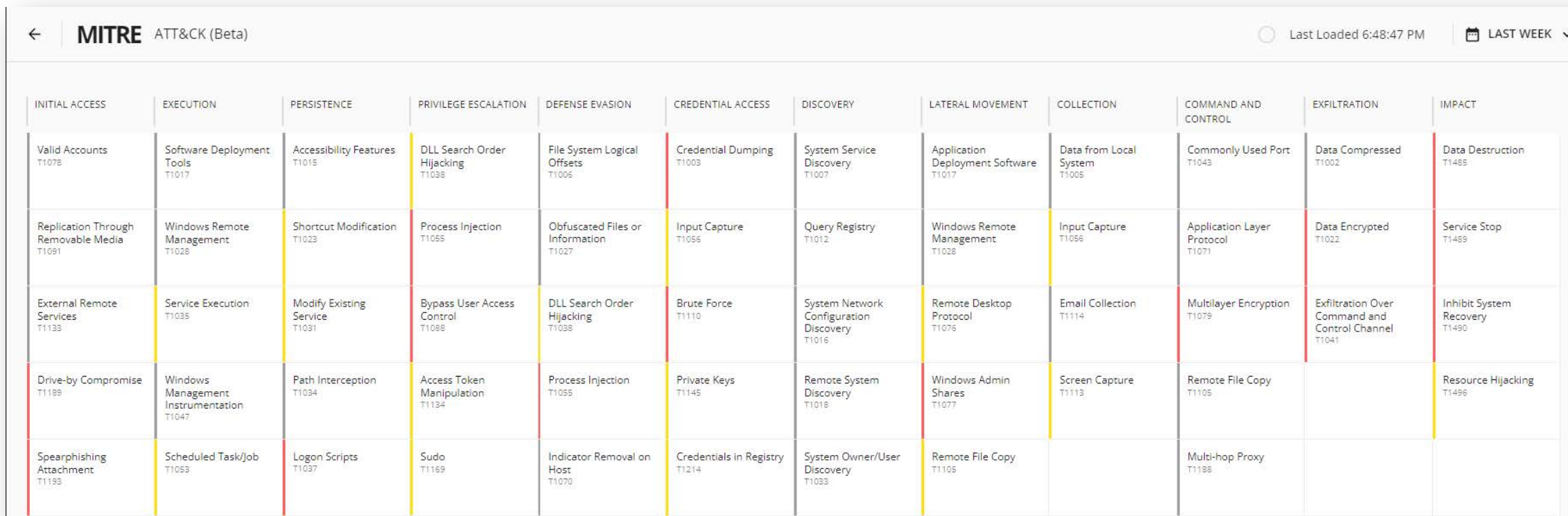
- 事前定義されたクエリを使用することで簡単に脅威をハンティングすることができます

| Query Category | Count | Action |
|---|-------|--------|
| Detections, Leads and Alerts | 3 | ^ |
| Active attacks Attacks detected by the endpoint client that are still active on the device | | ▶ ▼ |
| Attacks detected All attacks detected by the endpoint client | | ▼ |
| Alerts detected All user defined alerts detected by our notification service | | ▼ |
| Real World Breaches | 31 | ▼ |
| MS Office Anomalies | 2 | ▼ |

| Query Category | Count | Action |
|--------------------|-------|--------|
| Browser Anomalies | 2 | ▼ |
| Suspicious Scripts | 5 | ▼ |
| General Anomalies | 6 | ▼ |
| Persistence | 5 | ▼ |
| Shadow IT | 2 | ▼ |
| Reputation | 3 | ▼ |

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



The screenshot shows the MITRE ATT&CK (Beta) dashboard. At the top, there is a navigation bar with a back arrow, the text "MITRE ATT&CK (Beta)", a refresh icon, "Last Loaded 6:48:47 PM", and a calendar icon with "LAST WEEK" and a dropdown arrow. Below the navigation bar is a grid of 12 categories, each with a header and a list of techniques. The categories are: INITIAL ACCESS, EXECUTION, PERSISTENCE, PRIVILEGE ESCALATION, DEFENSE EVASION, CREDENTIAL ACCESS, DISCOVERY, LATERAL MOVEMENT, COLLECTION, COMMAND AND CONTROL, EXFILTRATION, and IMPACT. Each category has a list of techniques with their respective IDs (T1078, T1017, T1015, T1038, T1006, T1003, T1007, T1017, T1005, T1043, T1002, T1485, T1091, T1028, T1023, T1055, T1027, T1056, T1012, T1028, T1056, T1071, T1071, T1071, T1022, T1485, T1133, T1035, T1031, T1088, T1038, T1110, T1016, T1016, T1076, T1114, T1079, T1079, T1041, T1490, T1189, T1047, T1034, T1134, T1055, T1145, T1018, T1077, T1113, T1105, T1496, T1193, T1053, T1037, T1169, T1070, T1214, T1093, T1105, T1188).

| INITIAL ACCESS | EXECUTION | PERSISTENCE | PRIVILEGE ESCALATION | DEFENSE EVASION | CREDENTIAL ACCESS | DISCOVERY | LATERAL MOVEMENT | COLLECTION | COMMAND AND CONTROL | EXFILTRATION | IMPACT |
|--|---|----------------------------------|-------------------------------------|--|----------------------------------|---|--|---------------------------------|-------------------------------------|--|----------------------------------|
| Valid Accounts T1078 | Software Deployment Tools T1017 | Accessibility Features T1015 | DLL Search Order Hijacking T1038 | File System Logical Offsets T1006 | Credential Dumping T1003 | System Service Discovery T1007 | Application Deployment Software T1017 | Data from Local System T1005 | Commonly Used Port T1043 | Data Compressed T1002 | Data Destruction T1485 |
| Replication Through Removable Media T1091 | Windows Remote Management T1028 | Shortcut Modification T1023 | Process Injection T1055 | Obfuscated Files or Information T1027 | Input Capture T1056 | Query Registry T1012 | Windows Remote Management T1028 | Input Capture T1056 | Application Layer Protocol T1071 | Data Encrypted T1022 | Service Stop T1485 |
| External Remote Services T1133 | Service Execution T1035 | Modify Existing Service T1031 | Bypass User Access Control T1088 | DLL Search Order Hijacking T1038 | Brute Force T1110 | System Network Configuration Discovery T1016 | Remote Desktop Protocol T1076 | Email Collection T1114 | Multilayer Encryption T1079 | Exfiltration Over Command and Control Channel T1041 | Inhibit System Recovery T1490 |
| Drive-by Compromise T1189 | Windows Management Instrumentation T1047 | Path Interception T1034 | Access Token Manipulation T1134 | Process Injection T1055 | Private Keys T1145 | Remote System Discovery T1018 | Windows Admin Shares T1077 | Screen Capture T1113 | Remote File Copy T1105 | | Resource Hijacking T1496 |
| Spearphishing Attachment T1193 | Scheduled Task/Job T1053 | Logon Scripts T1037 | Sudo T1169 | Indicator Removal on Host T1070 | Credentials in Registry T1214 | System Owner/User Discovery T1093 | Remote File Copy T1105 | | Multi-hop Proxy T1188 | | |

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

The screenshot shows the Check Point Harmony Endpoint console interface. The top navigation bar includes 'HARMONY ENDPOINT' and 'CHECK POINT INFINITY PORTAL'. The main area displays a timeline of detection events. A specific event is selected, showing the following details:

| DETECTION EVENT INFORMATION | | ASSET | | ADDITIONAL INFORMATION | | TIME | |
|-----------------------------|-----------------------|---------|----------|------------------------|--------|------|------------|
| Trigger | locky.b64 | User | nack | Name | b2.exe | Date | 09/09/2022 |
| Triggered By | Endpoint Anti-Malware | Machine | EP-DEMO2 | Args | | | |

| DETECTION DETAILS | | ASSET DETAILS | | PROCESS DETAILS | |
|--------------------|---|-----------------|---|------------------|--|
| Trigger Path | c:\users\nack\documents\becky2\631... | User | nack | Name | b2.exe |
| Triggered By | Endpoint Anti-Malware | Machine | EP-DEMO2 | Directory | c:\program files (x86)\rimarts\b2 |
| Attack Status | Active | OS Name | Windows | Full Path | c:\program files (x86)\rimarts\b2\b2.exe |
| Trigger Process | c:\program files (x86)\rimarts\b2\b2.e... | Host Type | VirtualMachine | Start Time | 2022-09-09T17:02:20.429 |
| Attack User Domain | EP-DEMO2 | OS Version | Microsoft Windows 10 Enterprise Evaluation (10... | Args | |
| Attack User Name | nack | Product Version | 86.26.6008 | PID | 8432 |
| Protection Name | Trojan-Ransom.Win32.Locky.d | Domain Name | DomainNameNotFound | MD5 | 3a3848ca63b94ad04cfd4a4a4ce33172c |
| Trigger MD5 | 7a8290fdad2a7b06fc03491932ae8e9 | Host IPs | fe80::84fd:e643:4ee0:96d%13, 10.0.2.14 | Classification | Benign |
| Severity | Critical | Host MACs | 080027CEF971 | Reclassification | Benign |
| Confidence | High | | | Detections | VirusTotal 0 out of 69 |
| Enforcement | Prevent | | | Signed By | RimArts Inc. |
| Attack Root | b2.exe | | | Parent Name | explorer.exe |
| Entry Point | explorer.exe | | | Parent MD5 | 7a413ddd10e81adb6bb5d5e38f399d08 |

A context menu is open over the event, listing the following actions:

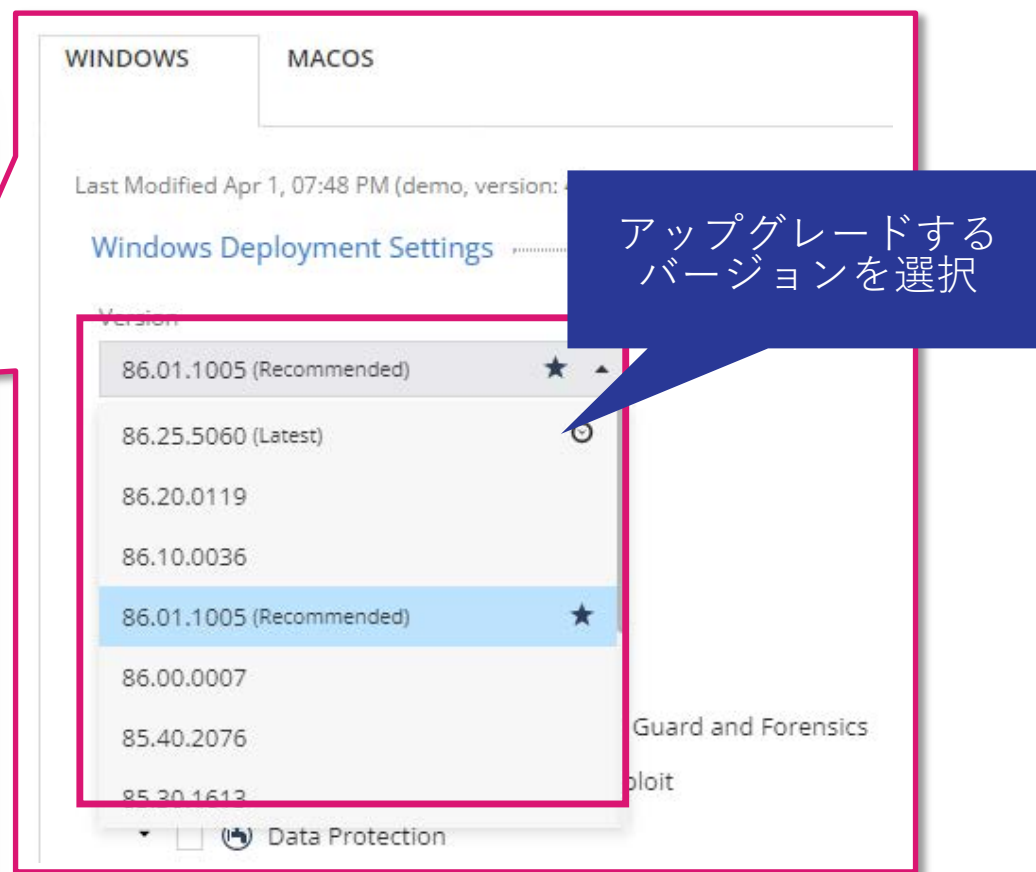
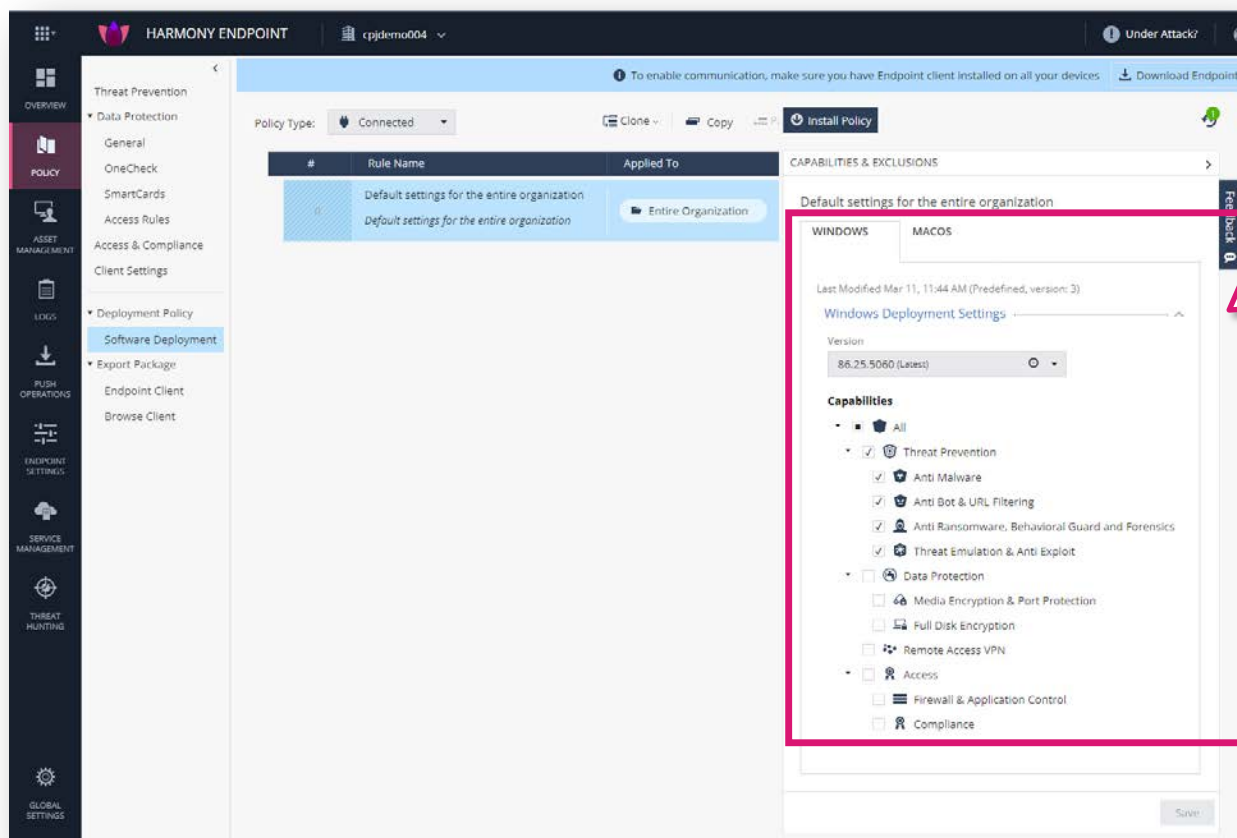
- Terminate Process
- Quarantine File
- Trigger Forensic Analysis
- Isolate Machine
- View Forensics Report
- Download Forensics Report

クライアントのアップグレード

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
- ダウングレードには対応していません



クライアントのアンインストール

YOU DESERVE THE BEST SECURITY

PUSH OPERATIONS



Asset Management 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。

The screenshot illustrates the process of uninstalling a client from the Asset Management interface. The interface is divided into several sections:

- ASSET MANAGEMENT:** The sidebar on the left has 'ASSET MANAGEMENT' selected.
- Computers:** The main table lists computers. The 'CP-DEMO' computer is selected, indicated by a checkmark in the selection column.
- Computer Actions:** A context menu is open over the 'CP-DEMO' computer, showing various actions. 'Agent Settings' is selected, and the 'Uninstall Client' option is highlighted.
- PUSH OPERATION CREATION DIALOG:** A dialog box titled 'Uninstall Client' is shown. It includes a 'Comment' field, 'User Notification' options (checked for 'Inform user with notification'), and 'Scheduling' options (radio buttons for 'Execute operation immediately' and 'Schedule operation for:'). The 'Create' button is highlighted.

Numbered callouts indicate the steps:

- ① アンインストールする端末を選択
- ② Computer Actions をクリック
- ③ Agent Settings をクリック
- ④ Uninstall Client をクリック
- ⑤ Create をクリック

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。

The screenshot displays the 'ADD PUSH OPERATION' workflow in the Check Point Harmony Endpoint console. The interface includes a sidebar with navigation options like Overview, Policy, Asset Management, Logs, and Push Operations. The main area shows a table of operations and an 'Endpoint List' table. The workflow is annotated with seven steps:

- ① + をクリック (Click +)
- ② Agent Settings を選択 (Select Agent Settings)
- ③ Uninstall Client を選択 (Select Uninstall Client)
- ④ + をクリック (Click +)
- ⑤ 端末を指定 (Specify device)
- ⑥ ユーザに通知するか指定 (Specify if notify user)
- ⑦ アンインストール実行 (Execute uninstall)

遠隔操作の状況確認

Push Operations

- Push Operations で遠隔操作の状況を確認

The screenshot displays the Harmony Endpoint management interface. The top navigation bar includes the logo, the text 'HARMONY ENDPOINT', and the instance name 'cpjdemo005'. A blue callout bubble with the text '遠隔操作の状況' (Remote Operation Status) points to the 'Push Operations' table. The table lists various operations such as 'Uninstall Client', 'Release Computer Isolation', and 'Isolate Computer', with columns for 'Operation', 'Comment', 'Pushed To', 'Status', 'Admin Name', 'Advanced Settings', 'Created On', and 'Active Until'. A red box highlights the first row of this table. Below the table, a 'Previous' button and 'Page 1 of 3' are visible. A second blue callout bubble with the text '端末ごとの状況、結果' (Status and Results by Device) points to the 'Endpoint List' table. The 'Endpoint List' table has columns for 'User Name', 'Computer Name', 'Operation Status', 'Operation Status Descriptio...', 'Operation Output', 'Sent To Endpoint On', and 'Status Update Received O'. A red box highlights the first row of this table, showing 'nack' as the user name and 'CP-DEMO' as the computer name.

| Operation | Comment | Pushed To | Status | Admin Name | Advanced Settings | Created On | Active Until |
|----------------------------|---------|-----------|--------------------|------------|---------------------------|----------------------|----------------------|
| Uninstall Client | | CP-DEMO | Pushing to clients | | View Advanced Settings... | 10 Jun 2022 07:18 pm | 11 Jun 2022 07:18 pm |
| Release Computer Isolation | | CP-DEMO | Completed | | View Advanced Settings... | 10 Jun 2022 07:09 pm | 11 Jun 2022 07:09 pm |
| Isolate Computer | | CP-DEMO | Completed | | View Advanced Settings... | 10 Jun 2022 06:53 pm | 11 Jun 2022 06:53 pm |
| Uninstall Client | | Lab-13 | Pushing to clients | | View Advanced Settings... | 10 Jun 2022 04:45 pm | 11 Jun 2022 04:45 pm |
| Release Computer Isolation | | CP-DEMO | Completed | | View Advanced Settings... | 10 Jun 2022 01:36 pm | 11 Jun 2022 01:36 pm |

| User Name | Computer Name | Operation Status | Operation Status Descriptio... | Operation Output | Sent To Endpoint On | Status Update Received O |
|-----------|---------------|----------------------|--------------------------------|------------------|----------------------|--------------------------|
| nack | CP-DEMO | Waiting For Endpoint | | | 10 Jun 2022 07:18 pm | 10 Jun 2022 07:18 pm |

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

表示モードを [Deployment] に切り替え

OVERVIEW

Computers Columns Deployment Refresh

Organizational Tree

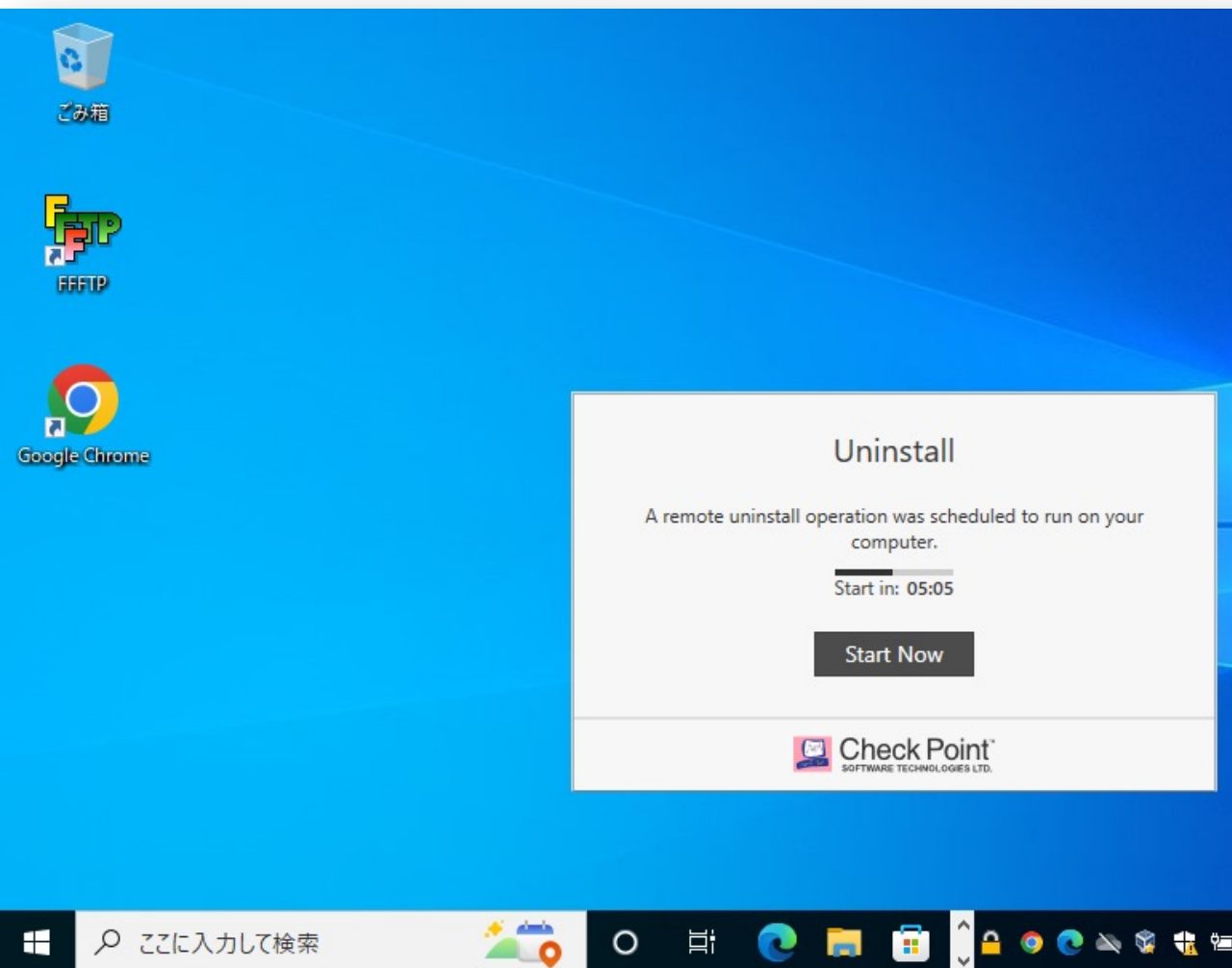
| Status | Computer Name | Endpoint Version | OS Build |
|--------------------------|---------------|------------------|----------------------|
| <input type="checkbox"/> | Lab-13 | 86.26.6008 | 10.0-19043-SP0.0-SMP |

アンインストールした端末 (今回の例では、CP-DEMO) が表示されないことを確認

ASSET MANAGEMENT

LOGS

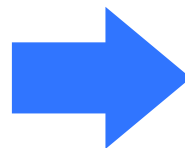
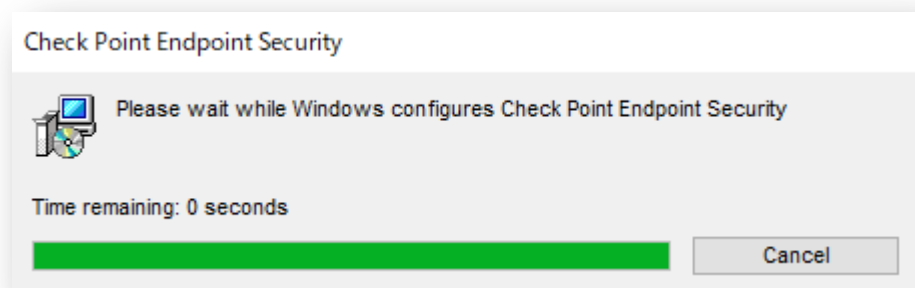
<参考> クライアントへの通知画面



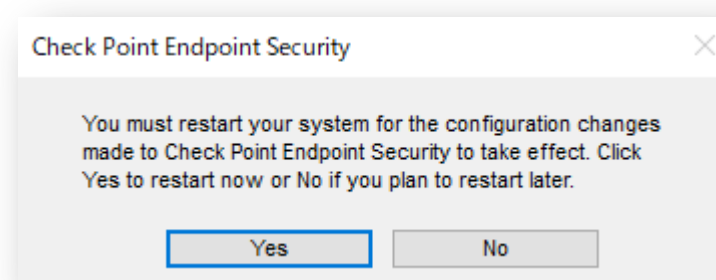
クライアントアンインストール時の注意事項

- 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

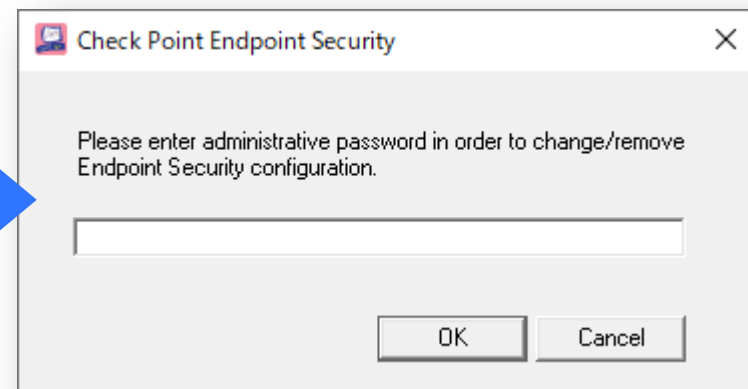
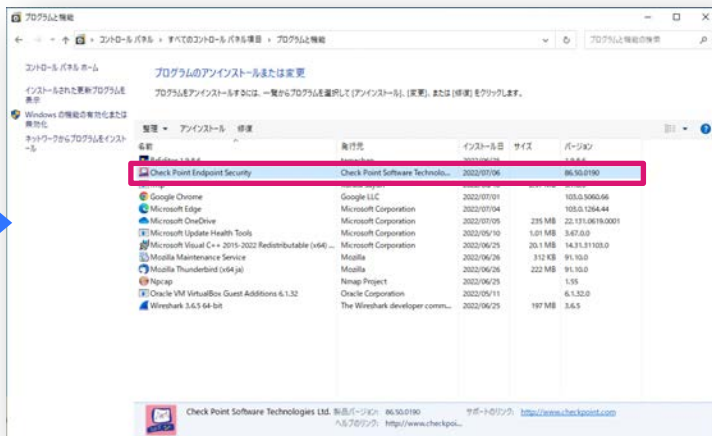
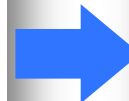
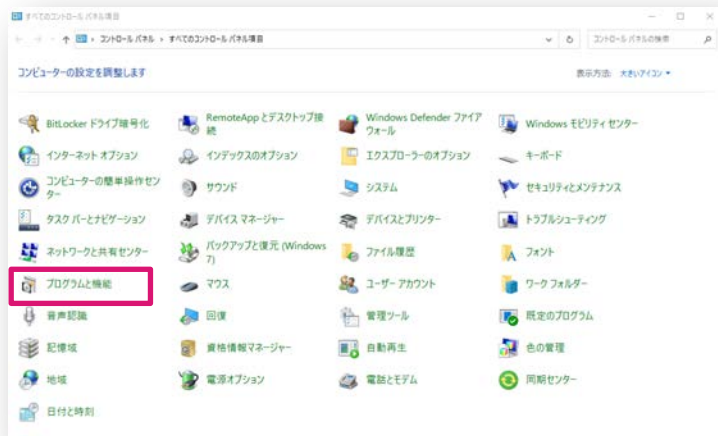
コントロールパネルからのアンインストール

- 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します
- 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

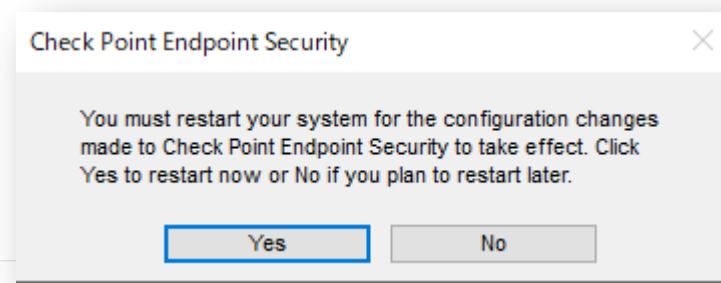
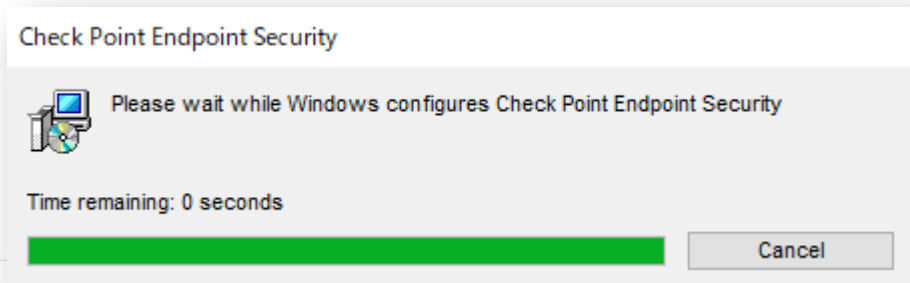
プログラムと機能

アンインストールパスワード



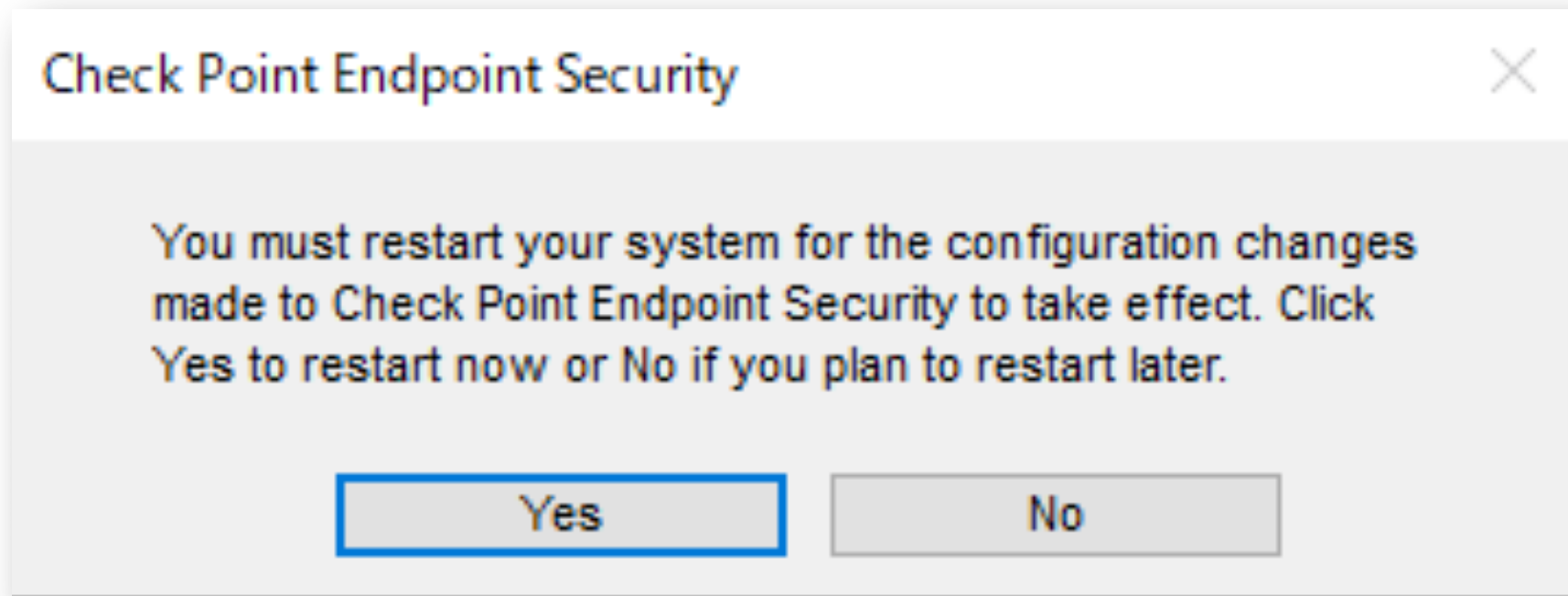
ダイアログボックス-1

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



VPN サイト設定の追加

概要

概要

- Harmony Endpoint 導入後に、Quantum Spark でのリモートアクセスVPNを追加導入するケースを想定しています
- Harmony Endpoint クライアントの VPN サイトの設定を、Push Operations で遠隔から実施することができます
- Push Operations で設定追加することで、クライアントパソコンでの設定が不要となります

制限

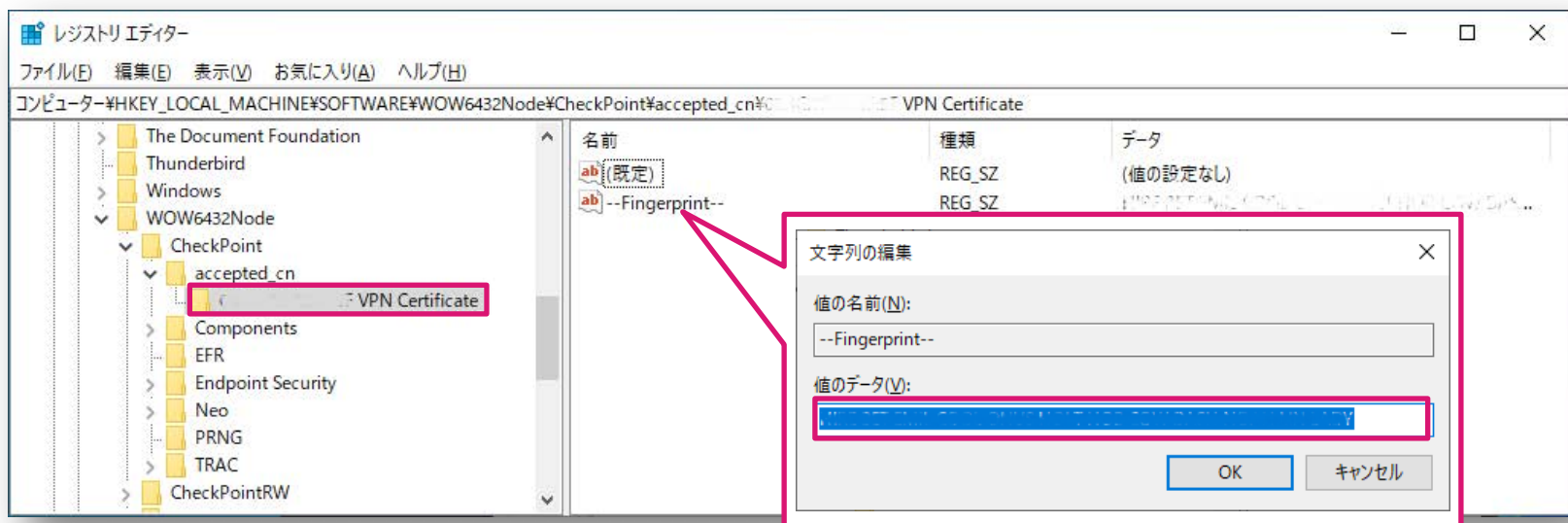
制限

- Push Operations での VPN Site の追加／削除は、Harmony Endpoint のクライアントバージョン E86.40 以降の Windows クライアントのみで対応している
- Harmony Endpoint クライアントでリモートアクセス VPN を行う場合は、クライアントに Remote Access VPN Blade がインストールされている必要がある
- クライアントのユーザーごとに個別の VPN サイトを作成することはできない。同じVPNサイトがすべてのユーザーに適用される
- クライアントが VPN サイトに接続している場合、新しい VPN サイトを追加したり、VPN サイトを削除したりすることはできない。新しいVPNサイトを追加／削除する前に、VPN を切断する必要がある

準備

準備：パラメータの取得

- Push Operations で指定する以下のパラメータを取得するために、クライアントでVPN サイトの追加設定を実施する
 - Remote Access Gateway Name
 - Fingerprint
- レジストリエディタで、¥HKEY_LOCAL_MACHINE¥SOFTWARE¥WOW6432Node¥CheckPoint¥accepted_cn へ移動する
- Remote Access Gateway Name は、accepted_cn 直下に表示されたキー名（フォルダ名）です
- Fingerprint は、Remote Access Gateway Name のキーを選択した際に、右ペインに表示される --Fingerprint-- をダブルクリックして表示される「文字列の編集」ダイアログボックスの「値のデータ」欄に表示されます



準備：バーチャルグループの作成

- 一部のコンピュータのみ VPN を有効化する場合は、バーチャルグループを利用すると Blade や、VPN Site の追加を効率的に行えます

Asset Management > Organizational Tree > Actions

The screenshot displays the Harmony Endpoint console interface. The left sidebar shows the navigation menu with 'ASSET MANAGEMENT' highlighted. The main area shows the 'Organizational Tree' view under 'Computers'. The 'Actions' menu is open, and the 'Create Virtual Group' option is selected. A dialog box titled 'CREATE VIRTUAL GROUP' is shown, with the 'Name' field containing 'demo2' and a 'Comment' field. The 'OK' button is highlighted.

General Actions

- Create Virtual Group
- Create and Add to Virtual Group
- Add to Virtual Group
- Reset Computer Data
- Delete
- Recover
- Terminate
- Directory Scanner

CREATE VIRTUAL GROUP

Name: demo2

Comment: Comment

CANCEL OK

準備：Remote Access VPN Blade の追加

- Policy > Deployment Policy > Software Deployment でクライアントのバージョンとRemote Access VPN Blade を設定

The screenshot displays the Check Point Harmony Endpoint console interface. The left sidebar shows the navigation menu with 'POLICY' and 'Software Deployment' highlighted. The main content area shows a table of policies:

| # | Rule Name | Applied To | Version | Action |
|---|--|---------------------|------------|----------------|
| 0 | Remote Access VPN | Remote Access VPN | 86.40.0169 | Do not install |
| 1 | Default settings for the entire organization | Entire Organization | 86.26.6008 | Do not install |

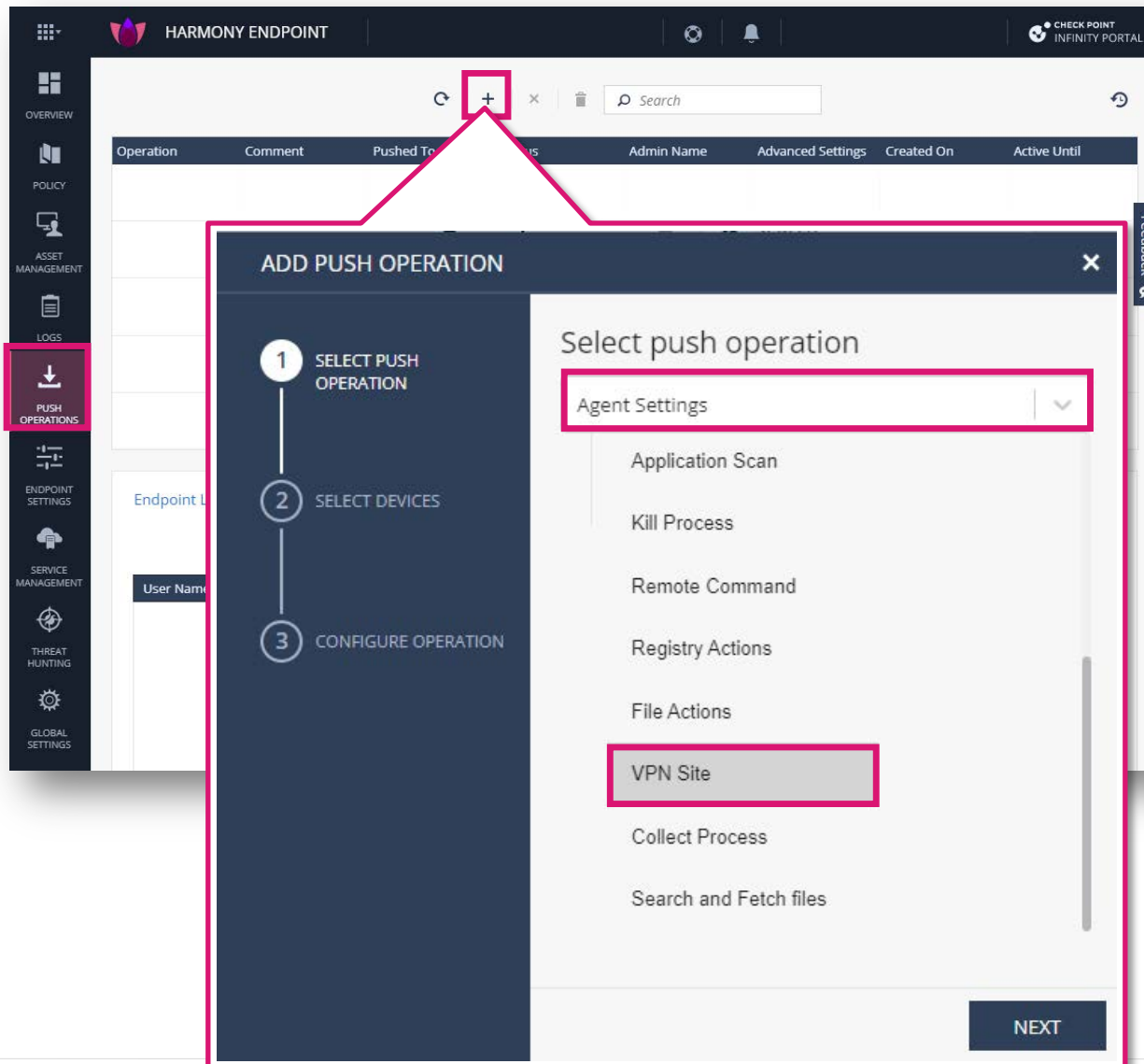
Below the table, the configuration details for the 'Remote Access VPN' policy are shown. The 'Version' dropdown is set to '86.40.0169'. Under the 'Capabilities' section, the 'Remote access VPN' checkbox is checked.

Annotations in the image provide additional context:

- A callout box points to the 'Remote Access VPN' rule in the table, stating: "一部のコンピュータのみ VPN を有効にする場合は、バーチャルグループを使用してポリシーを作成する" (When enabling VPN for only some computers, create the policy using a virtual group).
- A callout box points to the 'Version' dropdown, stating: "Version は、86.40 以降を選択する" (Select version 86.40 or later).
- A callout box points to the 'Remote access VPN' checkbox, stating: "Remote Access VPN にチェックを入れる" (Check Remote Access VPN).

PUSH OPERATIONS での操作

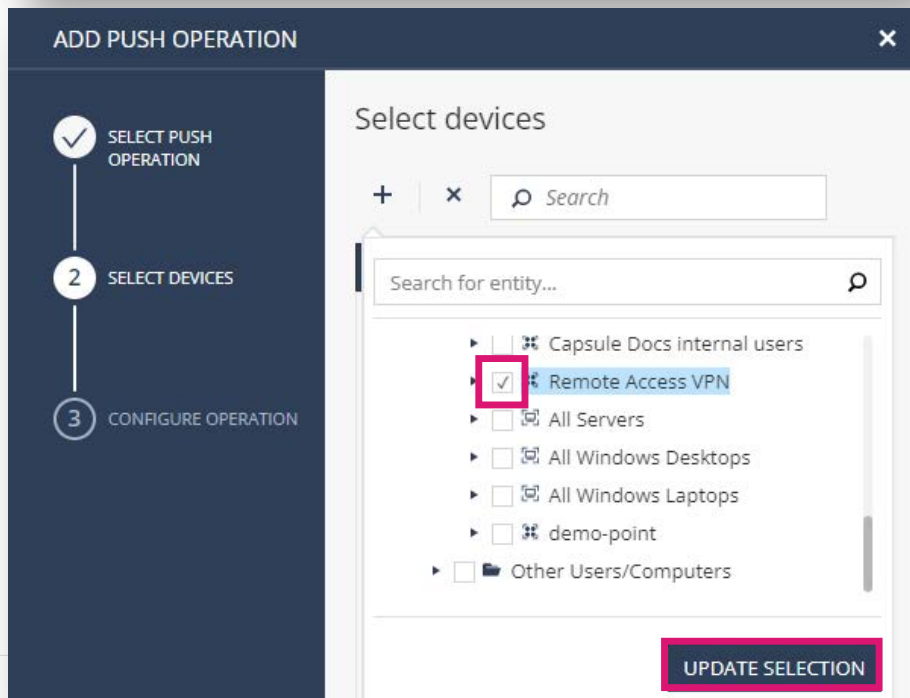
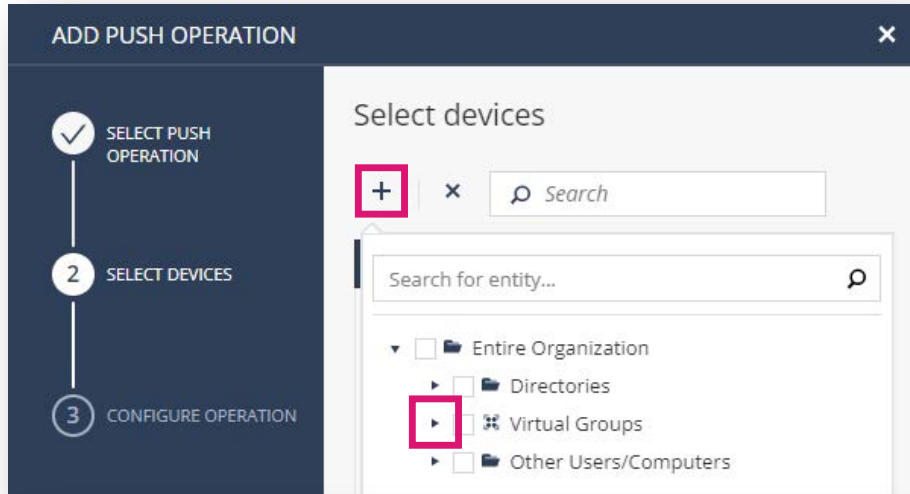
Push Operations での操作 (1 / 6)



- Push Operations の画面で + をクリックする
- Add Push Operation ダイアログボックスの Select push operation で「Agent Settings」を選択する
- Agent Settings の Operation から「VPN Site」を選択する
- NEXT をクリックする

Push Operations での操作 (2 / 6)

- Select devices で + クリックする
- Virtual Groups を展開する
- リモートアクセス VPN 用に作成したバーチャルグループを選択する
- UPDATE SELECTION をクリックする



Push Operations での操作 (3 / 6)

- 対象のコンピュータが表示されたら NEXT をクリックする

ADD PUSH OPERATION

SELECT PUSH OPERATION

2 SELECT DEVICES

3 CONFIGURE OPERATION

Select devices

+ × Search

| Name | IP Address |
|-----------------------------------|------------|
| <input type="checkbox"/> ep-demo2 | 10.0.2.14 |

BACK NEXT

Push Operations での操作 (4 / 6)

ADD PUSH OPERATION

VPN Site

Comment
Comment

Action *
Add VPN Site

Server Name *
Server Name

Use Custom Display Name
Display Name
Display Name

Use Custom Login Option

Login Option
Standard

Authentication Method *
Select...

Fingerprint *
Fingerprint

Remote Access Gateway Name *
Remote Access Gateway Name

User Notification
 Inform user with notification
 Allow user to postpone operation

Scheduling
 Execute operation immediately
 Schedule operation for:

Schedule operation for:
[Calendar icon]

BACK FINISH

- Action で、「Add VPN Site」を選択する
- Server Name に、VPN ゲートウェイの IP アドレス/FQDN を入力する
- Server Name と異なる表示名をクライアントソフトに表示する場合は、「Use Custom Display Name」にチェックを入れ、Display Name に表示名を入力する
- Authentication Method で、「username-password」を選択する
- Fingerprint に、準備で取得した値を入力する
- Remote Access Gateway Name に、準備で取得した値を入力する
- ユーザに通知メッセージを表示する場合は、User Notification の Inform user with notification にチェックを入れる
- ユーザに Push Operation の延期を許可する場合は、User Notification の Allow user to postpone operation にチェックを入れる
- 直ちに実行しない場合は、Scheduling で Schedule operation for: を選択し、実行スケジュールを設定する
- FINISH をクリックする

Push Operations での操作 (5 / 6)

- 設定例

ADD PUSH OPERATION

- ✓ SELECT PUSH OPERATION
- ✓ SELECT DEVICES
- 3 CONFIGURE OPERATION

VPN Site

Comment

Action *

Server Name *

Use Custom Display Name

Display Name *

Use Custom Login Option

Login Option


Authentication Method *

Fingerprint *

Remote Access Gateway Name *

User Notification
 Inform user with notification
 Allow user to postpone operation

Scheduling
 Execute operation immediately
 Schedule operation for:

Schedule operation for:



BACK FINISH

Push Operations での操作 (6 / 6)

The screenshot displays the Check Point Harmony Endpoint console interface. The top navigation bar includes the 'HARMONY ENDPOINT' logo, a user profile for 'Yoshiyasu Nakayama', and the 'CHECK POINT INFINITY PORTAL' logo. The left sidebar contains navigation icons for Overview, Policy, Asset Management, Logs, Push Operations (highlighted in red), Endpoint Settings, Service Management, Threat Hunting, and Global Settings.

The main content area is divided into two sections:

- Push Operations:** A table with columns: Operation, Comment, Pushed To, Status, Admin Name, Advanced Settings, Created On, and Active Until. A row for 'VPN Site' is highlighted in blue, with the 'Status' column value 'Completed' circled in red. Above the table, a refresh icon (circular arrow) is also circled in red.
- Endpoint List:** A table with columns: User Name, Computer Name, Operation Status, Operation Status, Operation Output, Sent To Endpoint, Status Update, Computer Location, Last Contact, and Machine Type. A row for user 'nack' on computer 'ep-demo2' is shown with 'Operation Status' 'Succeeded' circled in red. Below this row, a tooltip displays the operation output: 'Connection was successfully created', which is also circled in red.

-  をクリックし、Status が Completed になったことを確認する
- Push Operations 以外のページを表示し、再度、Push Operations のページを表示する
- Endpoint List の Operation Status が、Succeeded になったことを確認する
- Operation Output の表示が文字化けしている場合は、マウスオーバーして、Connection was successfully created と表示されることを確認する

クライアントでの確認

クライアントでの確認

The screenshot shows the 'Endpoint Security' application window. The main area displays the status of the 'Remote Access VPN Blade' as 'オフライン' (Offline). Below this, there are sections for '接続状態' (Connection Status), '接続の詳細' (Connection Details), and '暗号化設定' (Encryption Settings). The '接続の詳細' section includes fields for 'サイト名' (Site Name), 'ゲートウェイ IP アドレス' (Gateway IP Address), and '最終接続時刻' (Last Connection Time). The '暗号化設定' section shows statistics for '復号パケット' (Decrypted Packets), '復号済み (KB)' (Decrypted (KB)), '暗号化パケット' (Encrypted Packets), and '暗号化済み (KB)' (Encrypted (KB)). A red box highlights the '設定の管理' (Manage Settings) link in the '接続の詳細' section.

The screenshot shows the 'Check Point Endpoint Security - オプション' dialog box. The 'サイト' (Site) tab is selected, displaying a message: '接続する組織がサイトに表示されます。' (The organization to connect is displayed on the site). Below this message is a table for 'VPN Gateway' with columns for 'サイト' and '詳細'. To the right of the table are three buttons: '新規' (New), 'プロパティ' (Properties), and '削除' (Delete). At the bottom of the dialog are '保存して閉じる' (Save and Close) and 'ヘルプ' (Help) buttons.

参考

参考

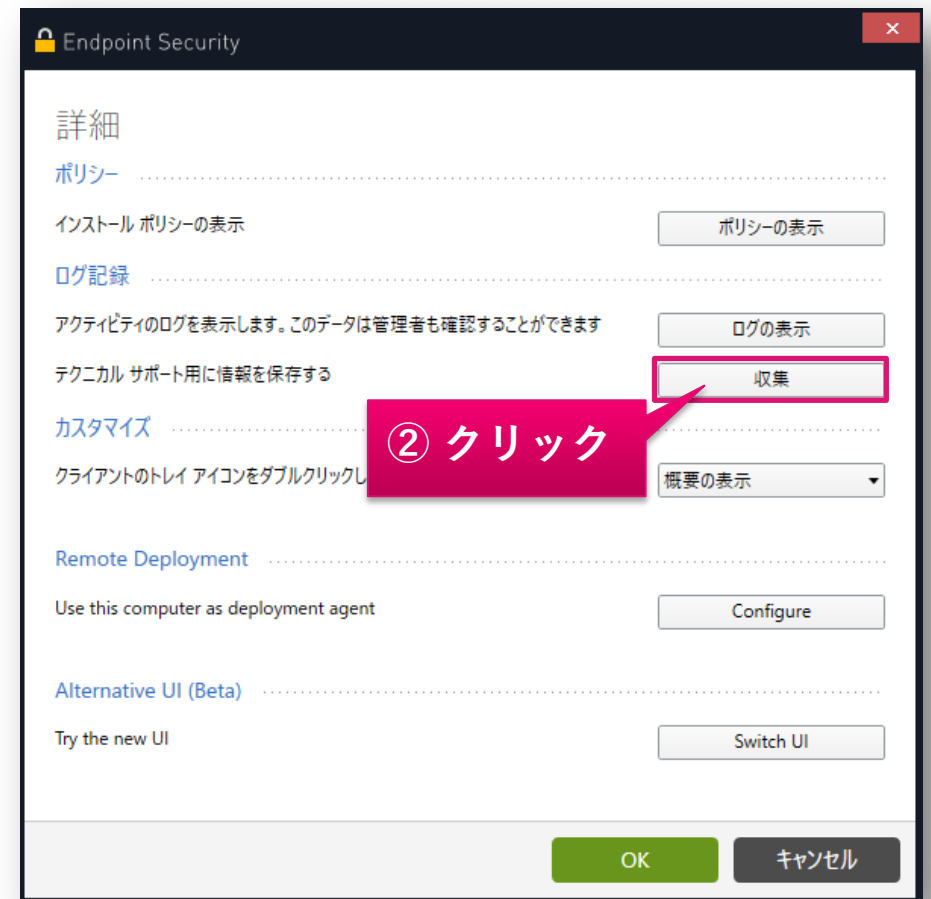
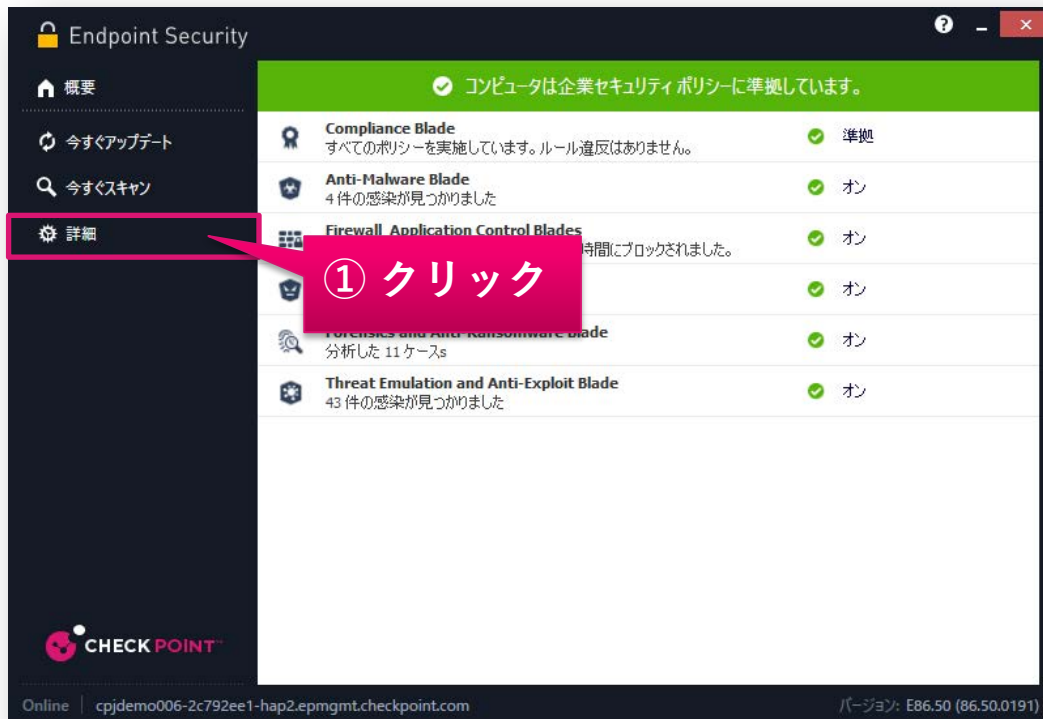
- Harmony Endpoint Administration Guide – Performing Push Operations
 - https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Harmony-Endpoint-Admin-Guide/Topics-HEP/Performing-Push-Operations.htm
- Endpoint Security Client for Windows ユーザガイド
 - https://sc1.checkpoint.com/documents/HarmonyEndpoint/Endpoint_Security_Clients_for_Windows_UserGuide-JP/Topics/Introduction.htm

Cpinfo（サポートログ）の取得

クライアントアプリケーションでの取得

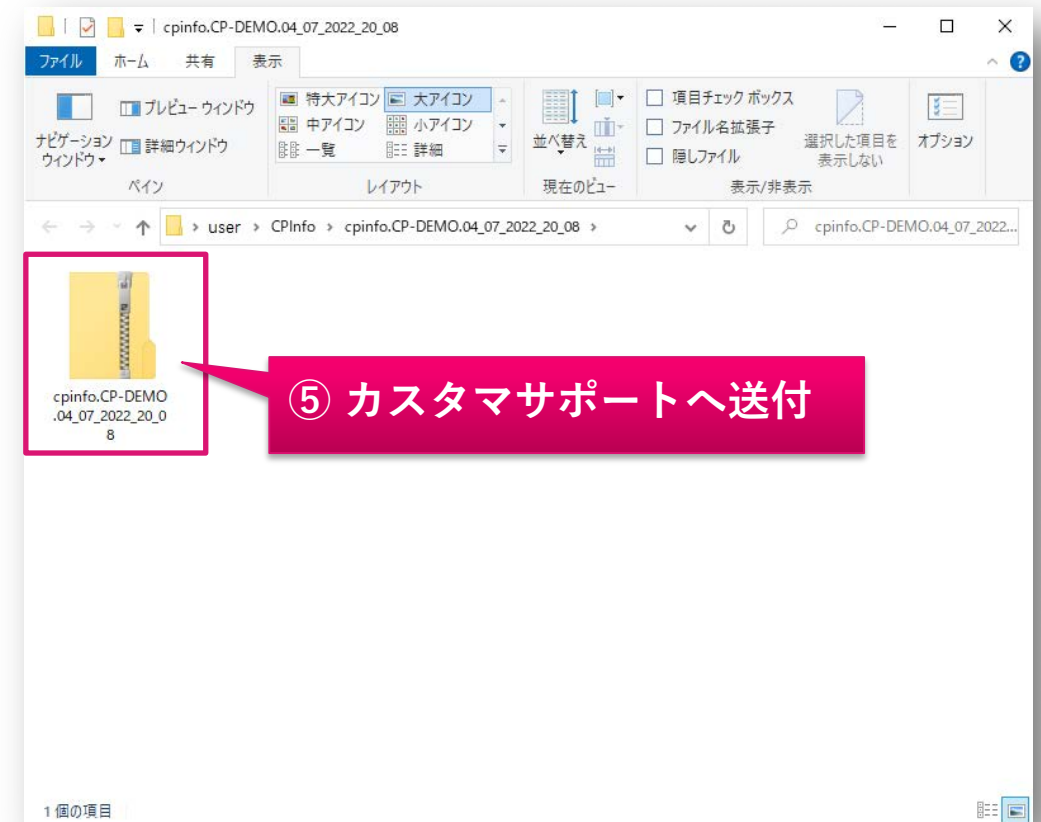
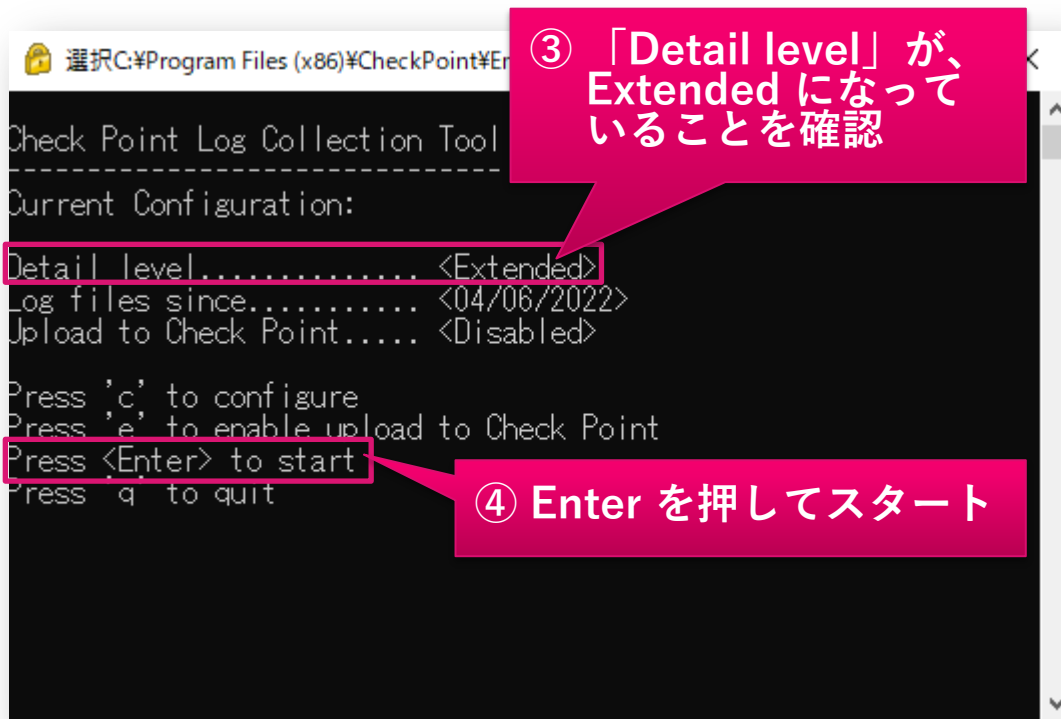
クライアントアプリケーションでの取得（1 / 2）

1. クライアントソフトウェアを開き、「詳細」をクリックします
2. 詳細画面が開いたら、「収集」をクリックします

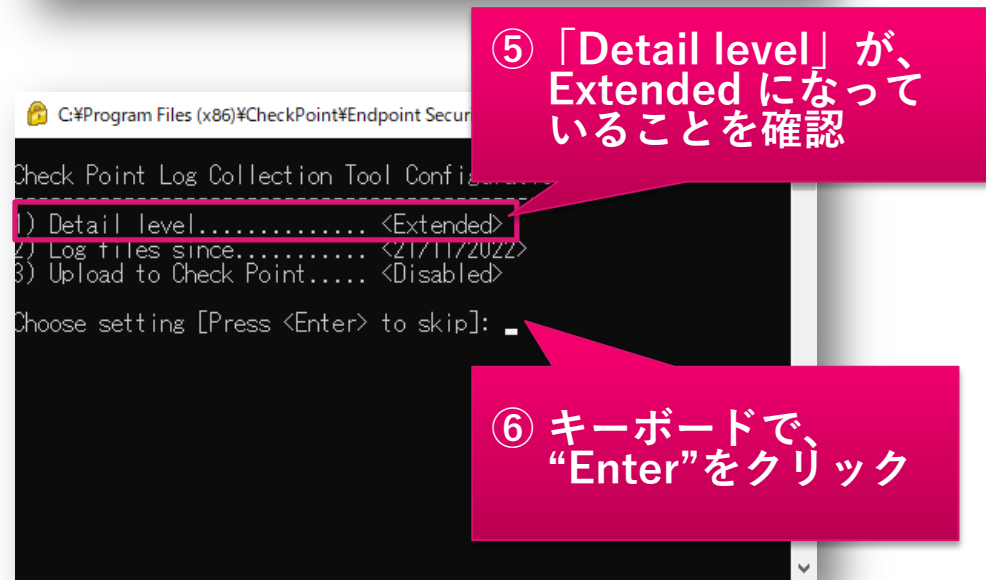
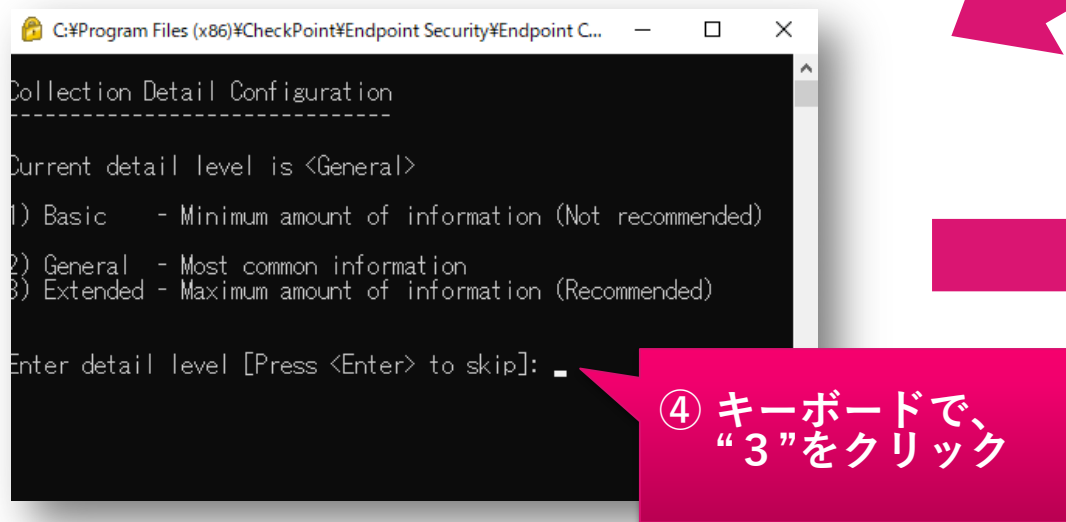
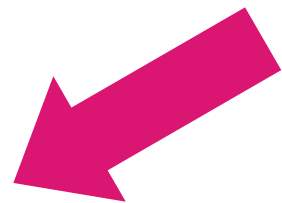
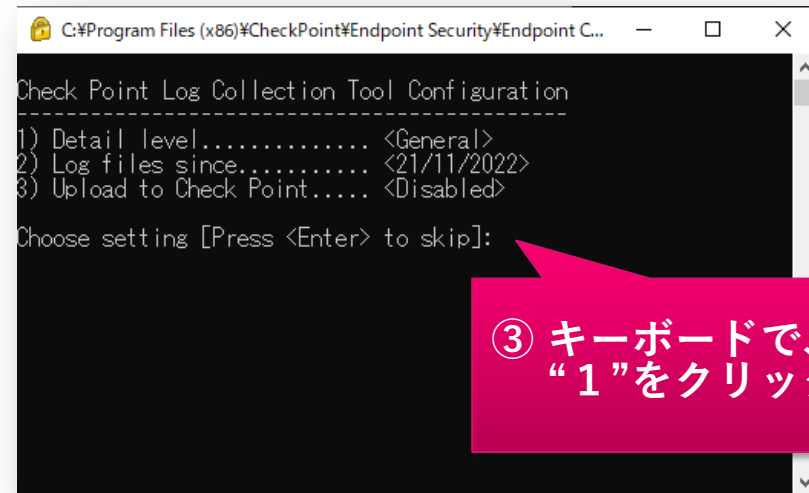
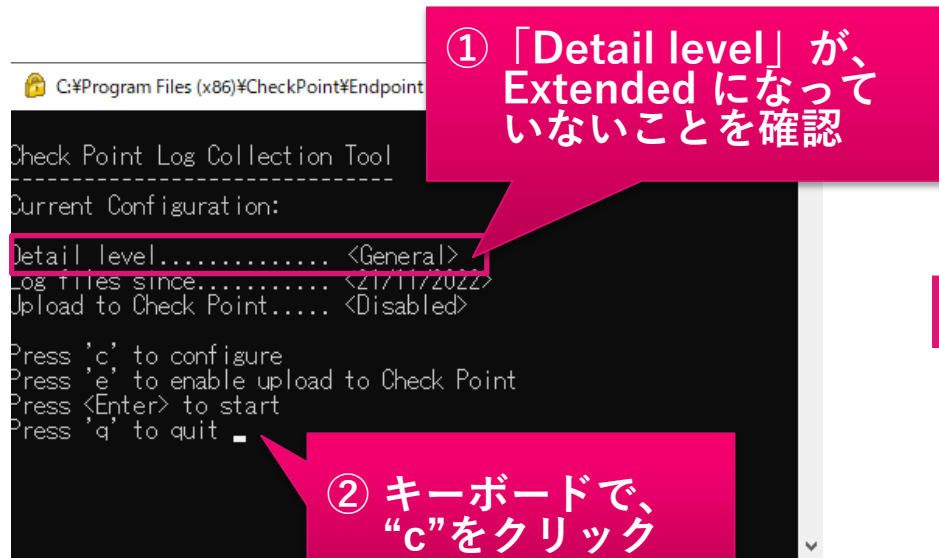


クライアントアプリケーションでの取得（2 / 2）

3. 「Detail level」が、Extended になっていることを確認します
4. クライアントソフトウェアを開き、「詳細」をクリックします
5. %userprofile%\cpinfo フォルダが自動で開くので、フォルダ内に保存された cpinfo～.zip ファイルをカスタマサポートへ送付します



【参考】「Detail level」の変更方法



Push Operations での取得

Push Operations での取得 (1 / 5)

1. Push Operations 画面で、**+ Add** をクリックします
2. Select push operations 画面で、「Agent Settings」を選択します
3. 「Collect Client Logs」を選択します
4. 「Next」をクリックします

The screenshot displays the HARMONY ENDPOINT interface. The main area shows a table of operations with columns for Operation, Client, Status, and ID. A '+ Add' button is highlighted in the top right of the table. A callout box labeled '① クリック' points to this button. Below the table, there is a 'Previous' button and a 'Page 1' indicator. On the left sidebar, the 'PUSH OPERATIONS' icon is highlighted. A second callout box labeled '② Agent Settings を選択' points to a dropdown menu in the 'ADD PUSH OPERATION' dialog. The dialog shows a list of operations: Deploy New Endpoints, Collect Client Logs, Repair Client, Shutdown Computer, Restart Computer, and Uninstall Client. The 'Collect Client Logs' option is highlighted. A third callout box labeled '③ Collect Client Logs を選択' points to this option. A fourth callout box labeled '④ クリック' points to the 'NEXT' button at the bottom of the dialog.

Push Operations での取得 (2 / 5)

5. Select devices 画面で、 をクリックします
6. コンピュータ名や、バッチ グループ名で検索します
7. コンピュータを選択します
8. 「UPDATE SELECTION」をクリックします
9. 「NEXT」をクリックします

① クリック

② コンピュータ名等で検索

③ コンピュータを選択

④ クリック

⑤ クリック

The screenshots show the 'ADD PUSH OPERATION' dialog box. The first screenshot shows the 'Select devices' screen with a '+' button highlighted. The second screenshot shows the search bar with 'Harmony-3' entered and selected. The third screenshot shows the 'UPDATE SELECTION' button highlighted.

| Name | IP Address |
|------------------------------------|---------------|
| <input type="checkbox"/> Harmony-3 | 192.168.2.129 |

Push Operations での取得 (3 / 5)

- 「Log set to collect」が、Maximum amount of information (recommended) になっていることを確認します
- 「Finish」をクリックします

ADD PUSH OPERATION

Collect Client Logs

Comment
Comment

Log set to collect
Maximum amount of information (recommended)

Debug info upload

Upload CPInfo reports to Check Point servers

Upload CPInfo reports to corporate servers

Corporate Server Info

User Notification

Inform user with notification

Allow user to postpone operation

BACK FINISH

⑨ Maximum amount of information (recommended) になっていることを確認

⑩ クリック

Push Operations での取得 (4 / 5)

11. Push Operations 画面に、Operation が作成されます。Status 欄が、Completed になったら処理が完了です
12. Endpoint List の Operation Output 欄に表示された、CPinfo のファイル名を確認します

The screenshot displays the Harmony Endpoint console interface. At the top, the navigation bar includes 'HARMONY ENDPOINT', the user 'cpjdemo006', and the 'CHECK POINT INFINITY PORTAL' logo. A sidebar on the left contains navigation icons for Overview, Policy, Asset Management, Logs, Push Operations, Endpoint Settings, and Service Management. The main content area is divided into two sections. The upper section, titled 'Operation', contains a table with columns: Operation, Comment, Pushed To, Status, Admin Name, Advanced Settings, Created On, and Active Until. The first row is highlighted in blue and has a red callout box pointing to the 'Status' column with the text '⑪ Statusを確認'. The lower section, titled 'Endpoint List', contains a table with columns: User Name, Computer Name, Operation Status, Operation Status Descript, Operation Output, Time To Endpoint On, Status Update Received On, Computer Location, Last Contact, and Machine Type. The first row in this table has a red callout box pointing to the 'Operation Output' column with the text '⑫ ファイル名を確認'. The 'Operation Output' cell contains the text 'File name: cpinfo.H...'.

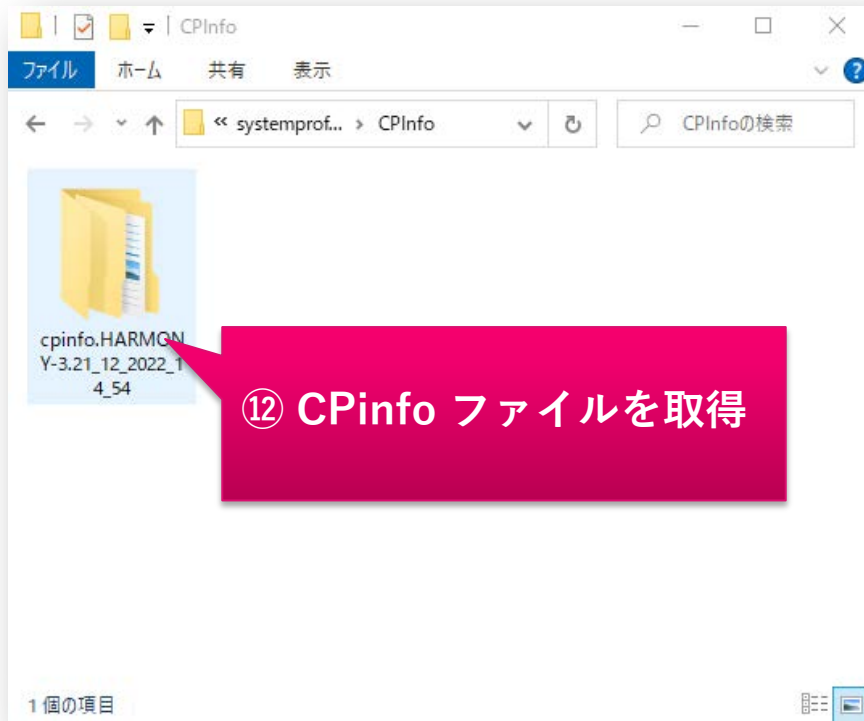
| Operation | Comment | Pushed To | Status | Admin Name | Advanced Settings | Created On | Active Until |
|----------------------|---------|-----------|-----------|----------------|---------------------------|----------------------|----------------------|
| Collect Client Logs | | Harmony-3 | Completed | cp_EpMaa5_Only | View Advanced Settings... | 21 Dec 2022 02:49 pm | 22 Dec 2022 02:49 pm |
| Collect Client Logs | | Harmony-3 | Completed | cp_EpMaa5_Only | View Advanced Settings... | 21 Dec 2022 02:08 pm | 22 Dec 2022 02:08 pm |
| Analyze by Indicator | | ep-demo2 | Completed | cp_EpMaa5_Only | View Advanced Settings... | 30 Nov 2022 07:03 pm | 01 Dec 2022 07:03 pm |
| File Remediation | | ep-demo2 | Completed | cp_EpMaa5_Only | View Advanced Settings... | 30 Nov 2022 06:56 pm | 01 Dec 2022 06:56 pm |
| File Actions | | ep-demo2 | Completed | cp_EpMaa5_Only | View Advanced Settings... | 30 Nov 2022 06:43 pm | 01 Dec 2022 06:43 pm |

| User Name | Computer Name | Operation Status | Operation Status Descript | Operation Output | Time To Endpoint On | Status Update Received On | Computer Location | Last Contact | Machine Type |
|-----------|---------------|------------------|---------------------------|------------------------|----------------------|---------------------------|-------------------|----------------------|--------------|
| alice | Harmony-3 | Succeeded | Logs were collected. | File name: cpinfo.H... | 21 Dec 2022 02:58 pm | 21 Dec 2022 02:58 pm | | 21 Dec 2022 03:01 pm | Laptop |

Push Operations での取得 (5 / 5)

- クライアントコンピュータの以下のフォルダに CPinfo が保存されています。手順 11 で確認したファイル名のファイルをカスタマサポートに送付します

C:\Windows\SysWOW64\config\systemprofile\CPInfo\





THANK YOU

YOU DESERVE THE BEST SECURITY