



Harmony Endpoint 簡易運用ガイド

URL フィルタリング – ブラックリスト & ホワイトリスト

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

YOU DESERVE THE BEST SECURITY

目次

- 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 ～除外メニュー編～
- 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～
- ログの表示内容

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

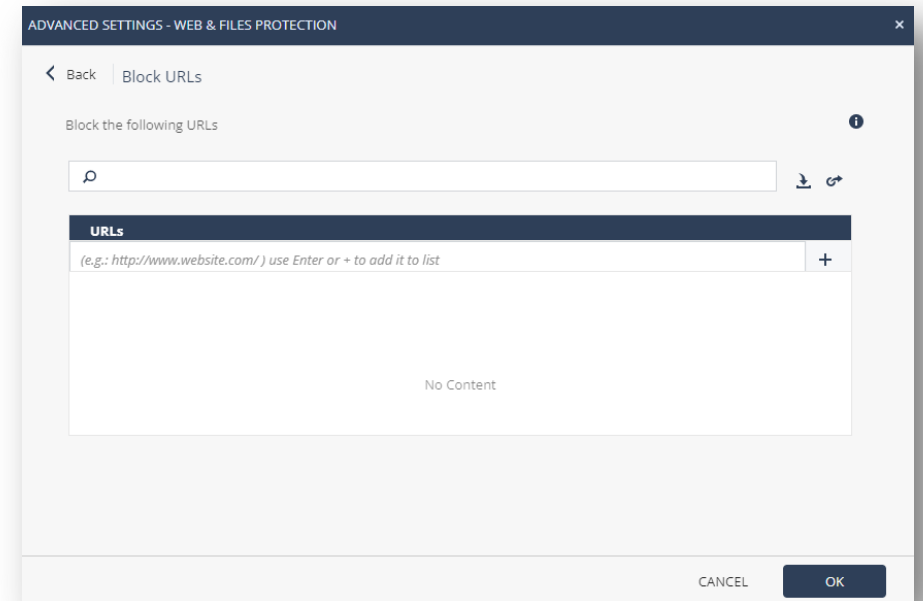
- 閲覧をブロックする Web サイトを URL または ドメイン名で指定できます。IP アドレスでは指定できません
- URL または ドメイン名は、個別もしくはファイルのインポートにより設定できます

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 'Connected'. A modal dialog titled 'ADVANCED SETTINGS - WEB & FILES PROTECTION' is open, showing various configuration options. The 'URL Filtering' section is highlighted, and the 'Advanced Settings' button at the bottom of the dialog is also highlighted. A red callout box with the Japanese text 'クリック' (Click) points to this button. 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 top navigation bar shows 'HARMONY ENDPOINT', 'cpjdemo006', and 'CHECK POINT INFINITY PORTAL'.

Policy Type: **Connected** | Clone | Copy | Paste | Manage IOCs | Search for entity | Unsaved Rule

ADVANCED SETTINGS - WEB & FILES PROTECTION

- Allow user to dismiss the URL Filtering alert and access the website
- Categories**
 - Bandwidth Consumption (0) | Edit...
 - General Use (0) | Edit...
 - Legal Liability / Regulatory Compliance (0) | Edit...
 - Productivity Loss (0) | Edit...
 - Service (10) | Edit...
- Black list (0) | Edit...**
 - Enable Network URL Filtering
- Malicious Script Protection**
 - Block websites where Malicious Scripts are found embedded in the HTML
 - Allow user to dismiss the Malicious Scripts alert and access the website

CANCEL OK

WEB & FILES PROTECTION | BEHAVIORAL PROTECTION | ANALYSIS & REMEDIATION

Last Modified Dec 12, 09:01 PM (cp, versions)

URL Filtering

URL Filtering Mode

Download Protection

Download Emulation & Extraction

Advanced Settings

Save

クリック

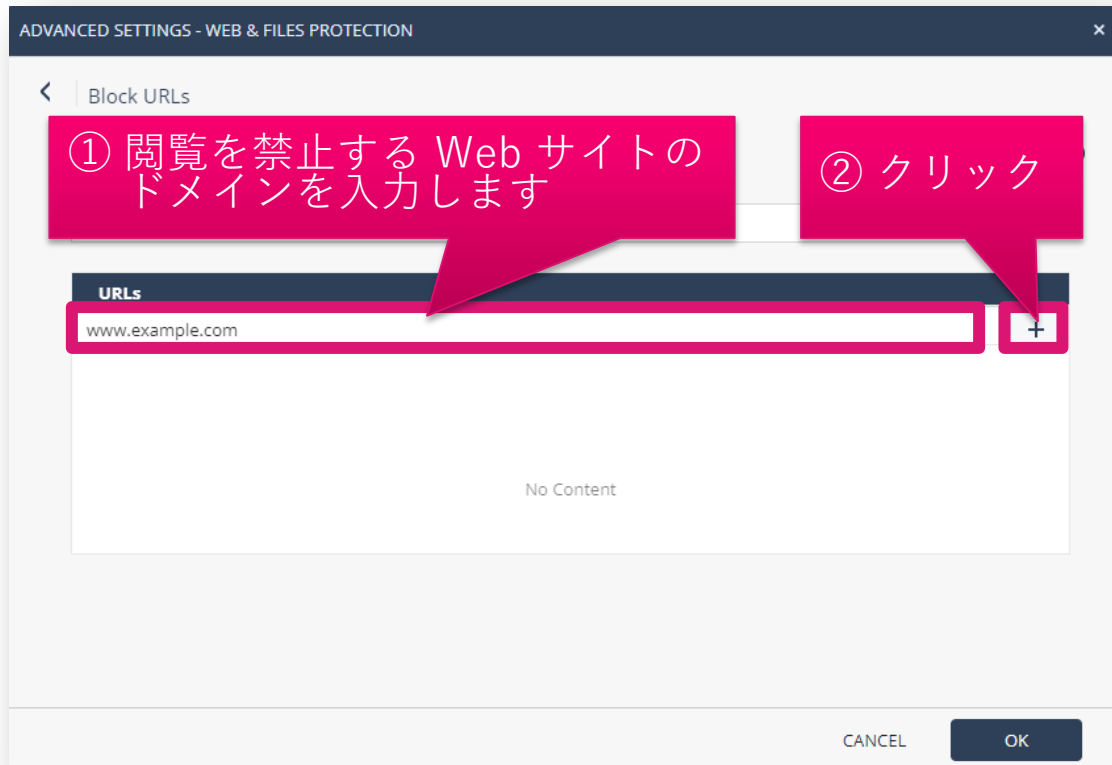
ブラックリストの作成画面を表示

- 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

The image displays two overlapping screenshots from a security management console. The background screenshot shows the 'ADVANCED SETTINGS - WEB & FILES PROTECTION' page. On the left, a sidebar lists various protection categories, with 'Files Protection' expanded to show 'General', 'Signature', and 'Scan'. The 'Black list (0)' section is highlighted, and its 'Edit...' button is enclosed in a red rectangular box. A red callout box with the Japanese text 'クリック' (Click) points to this button. The foreground screenshot is a modal window titled 'ADVANCED SETTINGS - WEB & FILES PROTECTION' with a sub-header 'Block URLs'. It features a 'Back' button, a text input field for entering URLs, and a table with the header 'URLs' and a '+' button for adding entries. The table currently shows 'No Content'. At the bottom of the modal are 'CANCEL' and 'OK' buttons.

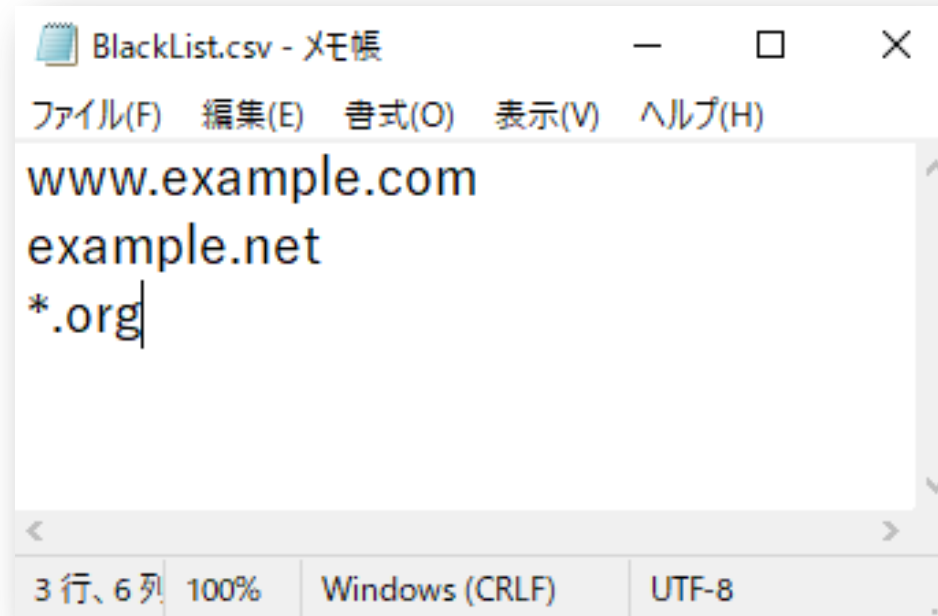
ブラックリストを作成（個別設定）

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




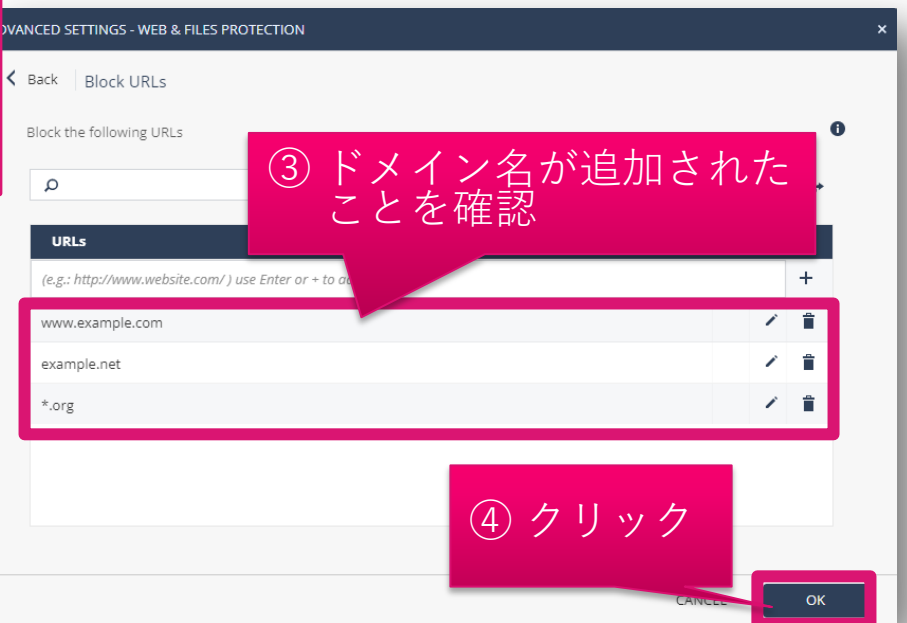
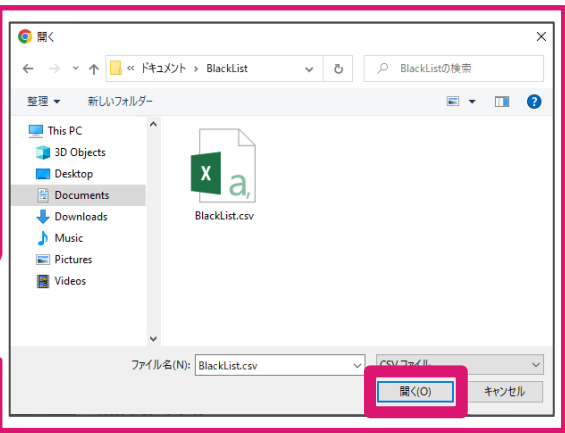
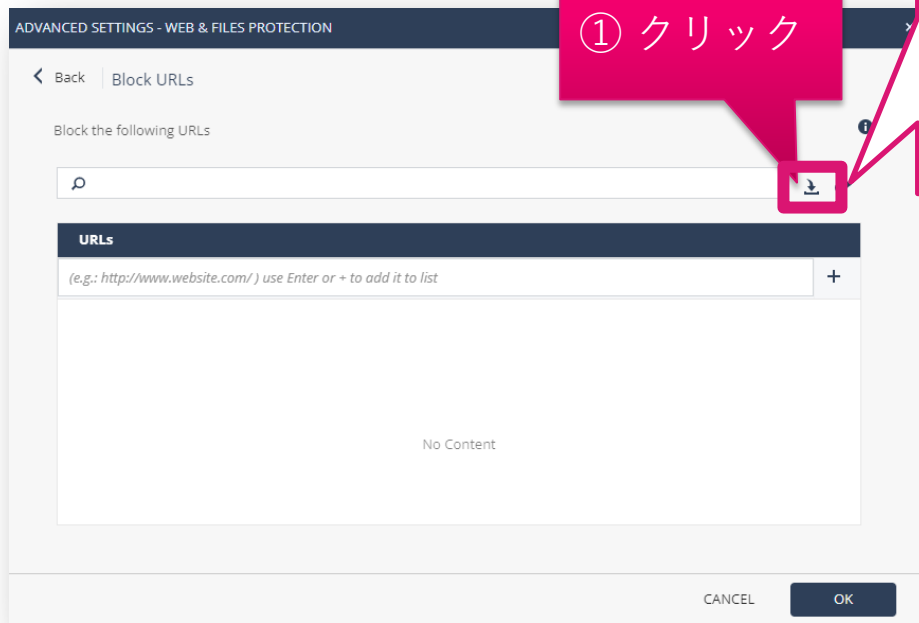
ブラックリストを作成（ファイルインポート）（1 / 2）

- 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

② クリック

③ ドメイン名が追加されたことを確認

④ クリック

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

The screenshot shows the 'CAPABILITIES & EXCLUSIONS' section of the management console. A red box highlights the 'Install Policy' button in the top right corner, with a callout bubble containing the text '② クリック'. Another red box highlights the 'Save' button at the bottom right, with a callout bubble containing the text '① クリック'. The interface includes sections for 'Default settings', '11 Exclusions', and 'Policy Mode' (set to Custom). There are also tabs for 'WEB & FILES PROTECTION', 'BEHAVIORAL PROTECTION', and 'ANALYSIS & REMEDIATION'.



The screenshot shows the 'INSTALL POLICY' dialog box. It contains the text: 'The following changes were made since the last policy installation. Review the changes and click on 'install' to install policy.' Below this is a table titled 'Changed Rules Settings (1)'. A red box highlights the 'INSTALL' button at the bottom right, with a callout bubble containing the text '③ クリック'.

Rule Name	Policy Type	Changes	Modified On
<input checked="" type="checkbox"/> Default settings	Threat Prevention	Settings were changed	12/9/2022, 10:00 AM

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 *

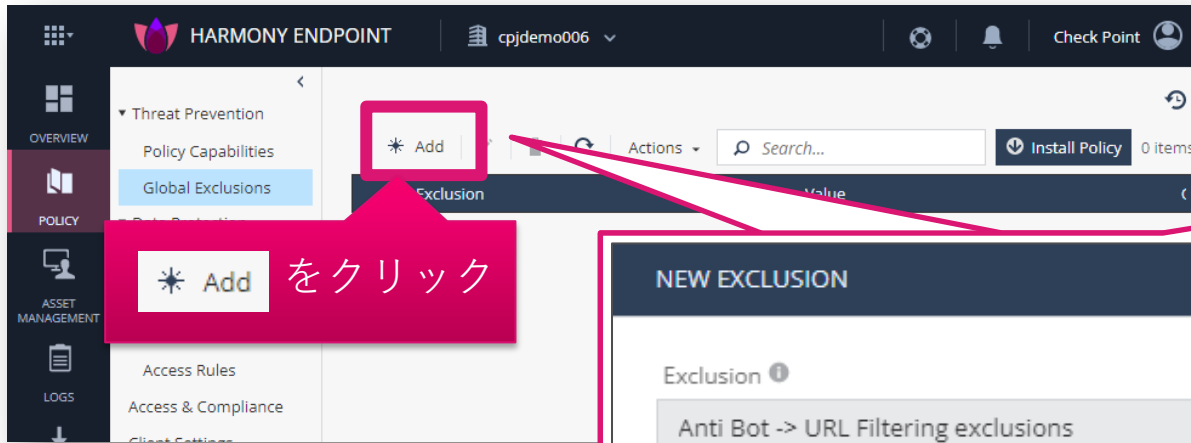
Add to all rules ⓘ

CANCEL OK

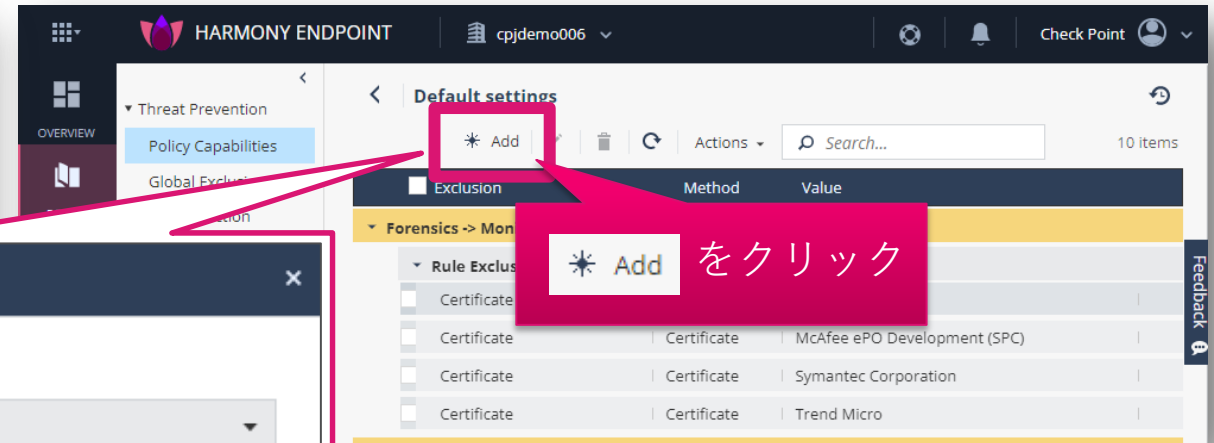
ホワイトリストの作成画面を表示

- 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

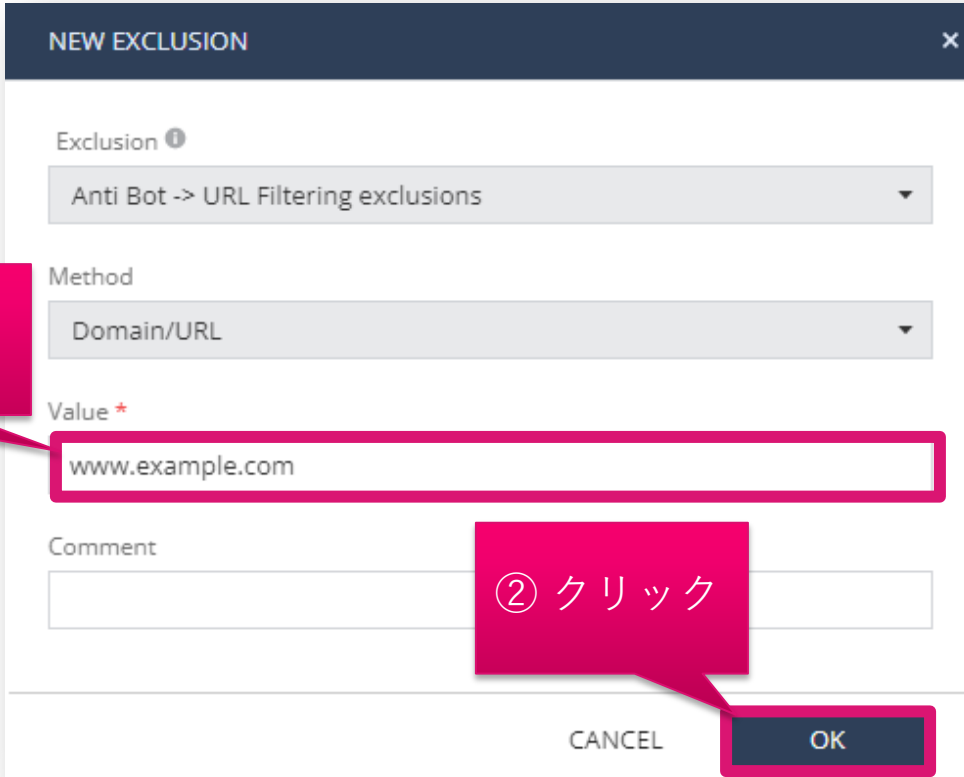
Value *

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

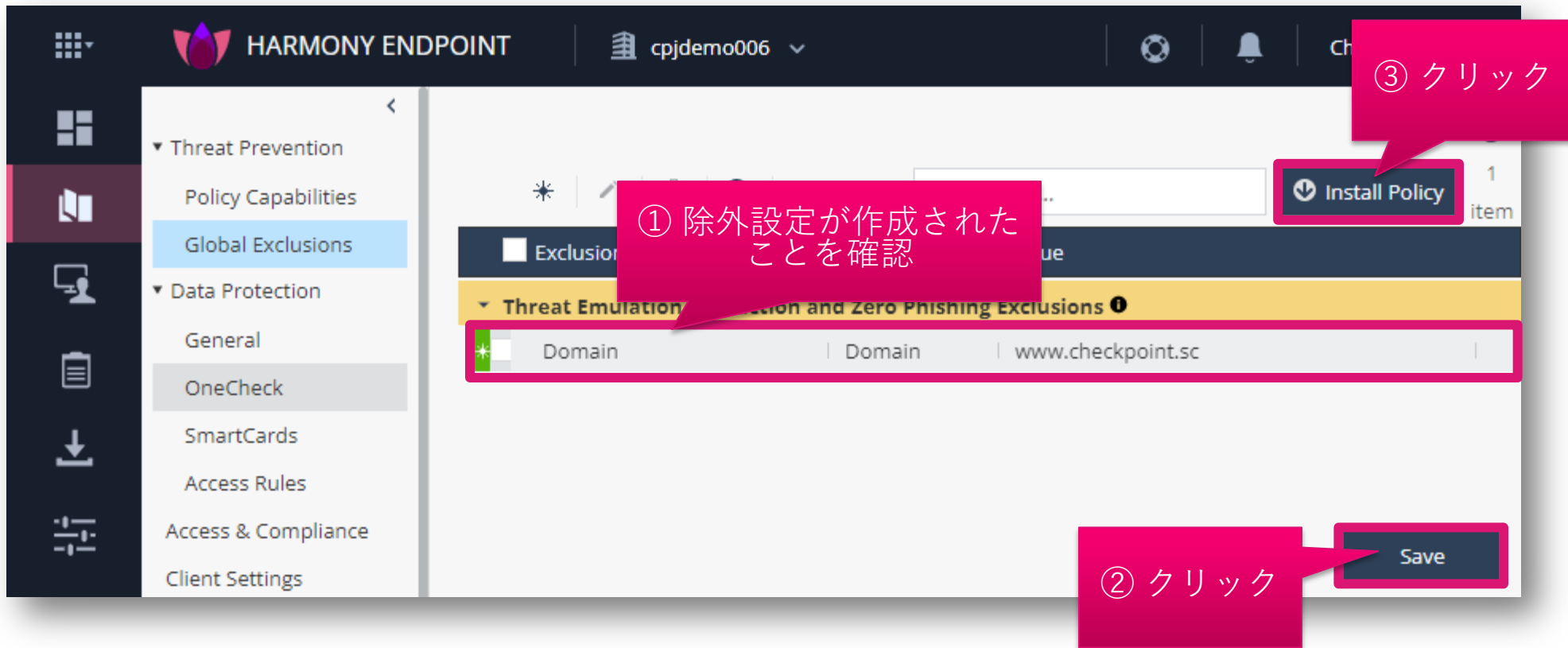


The screenshot shows a 'NEW EXCLUSION' dialog box with the following fields and annotations:

- 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', highlighted with a red box and a callout bubble labeled '① 除外条件を入力'.
- Comment:** An empty text input field, with a red box and callout bubble labeled '② クリック' pointing to the 'OK' button.
- Buttons:** 'CANCEL' and 'OK' buttons at the bottom, with the 'OK' button highlighted by a red box.

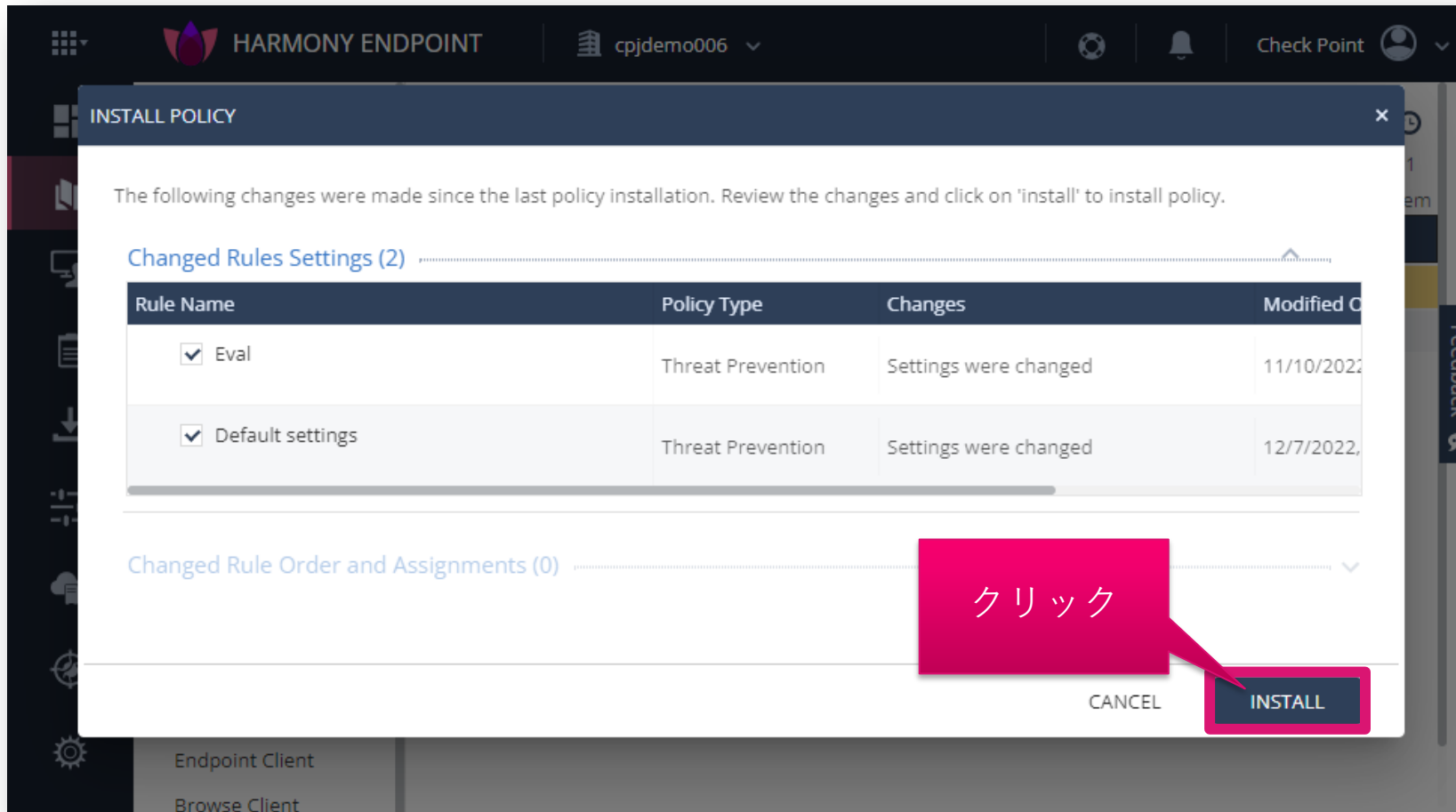
ホワイトリストを適用（組織全体に適用する場合）（1 / 2）

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



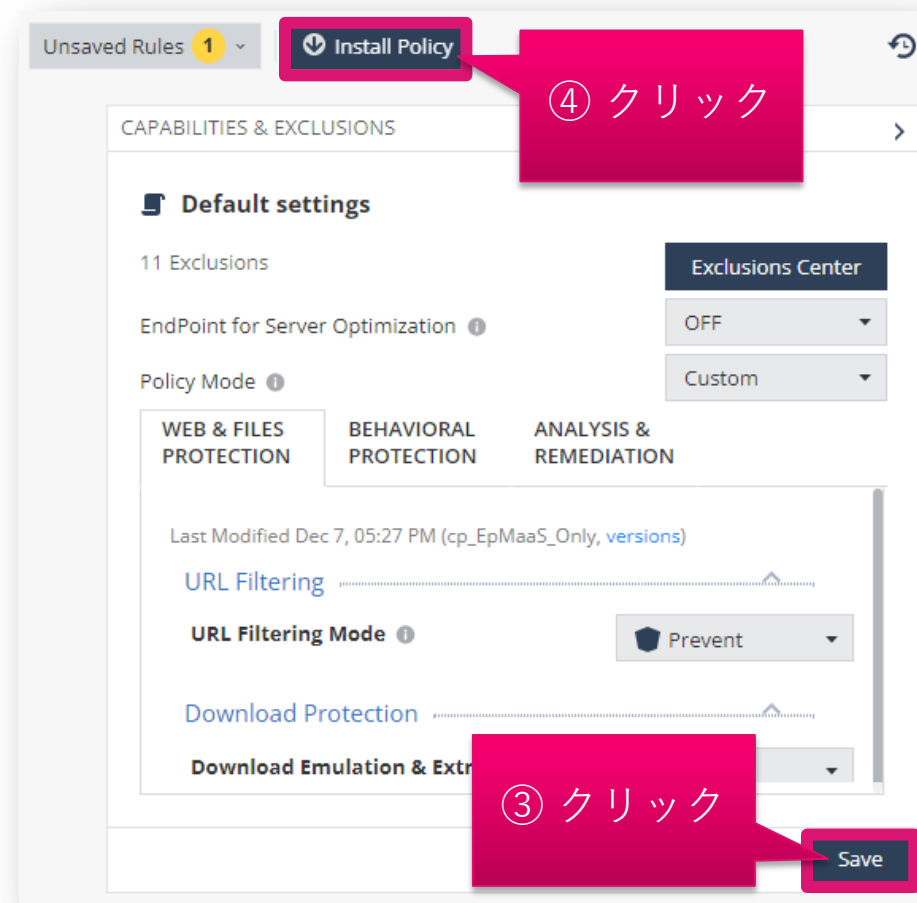
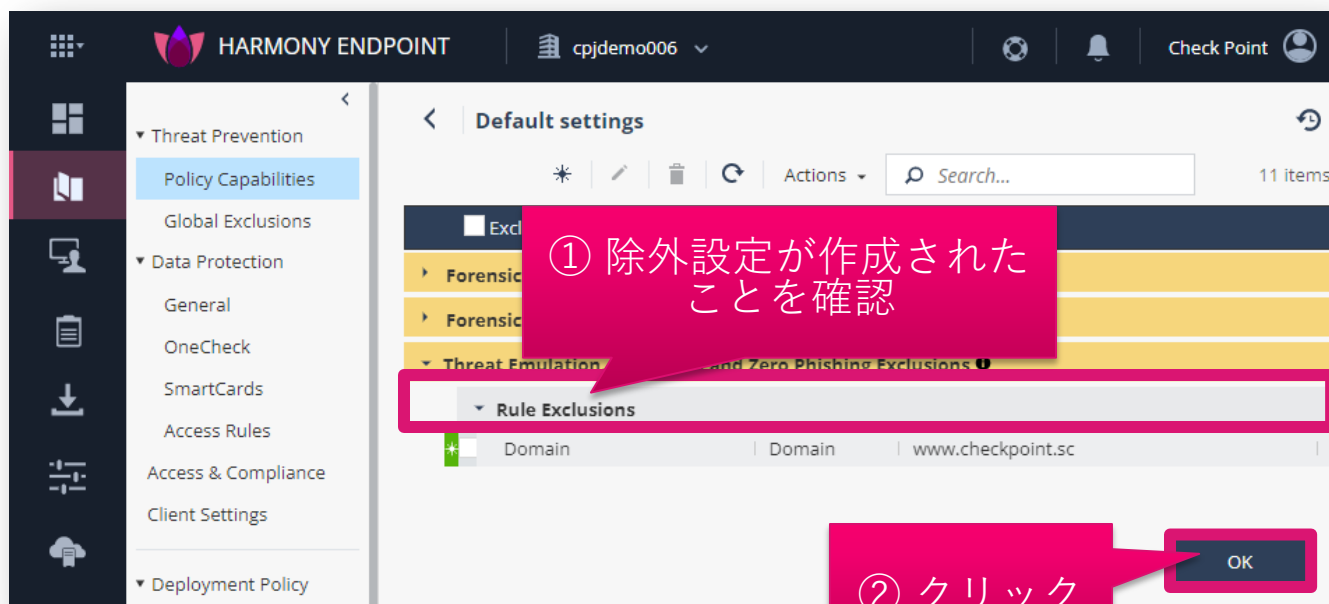
ホワイトリストを適用（組織全体に適用する場合）（2 / 2）

- 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



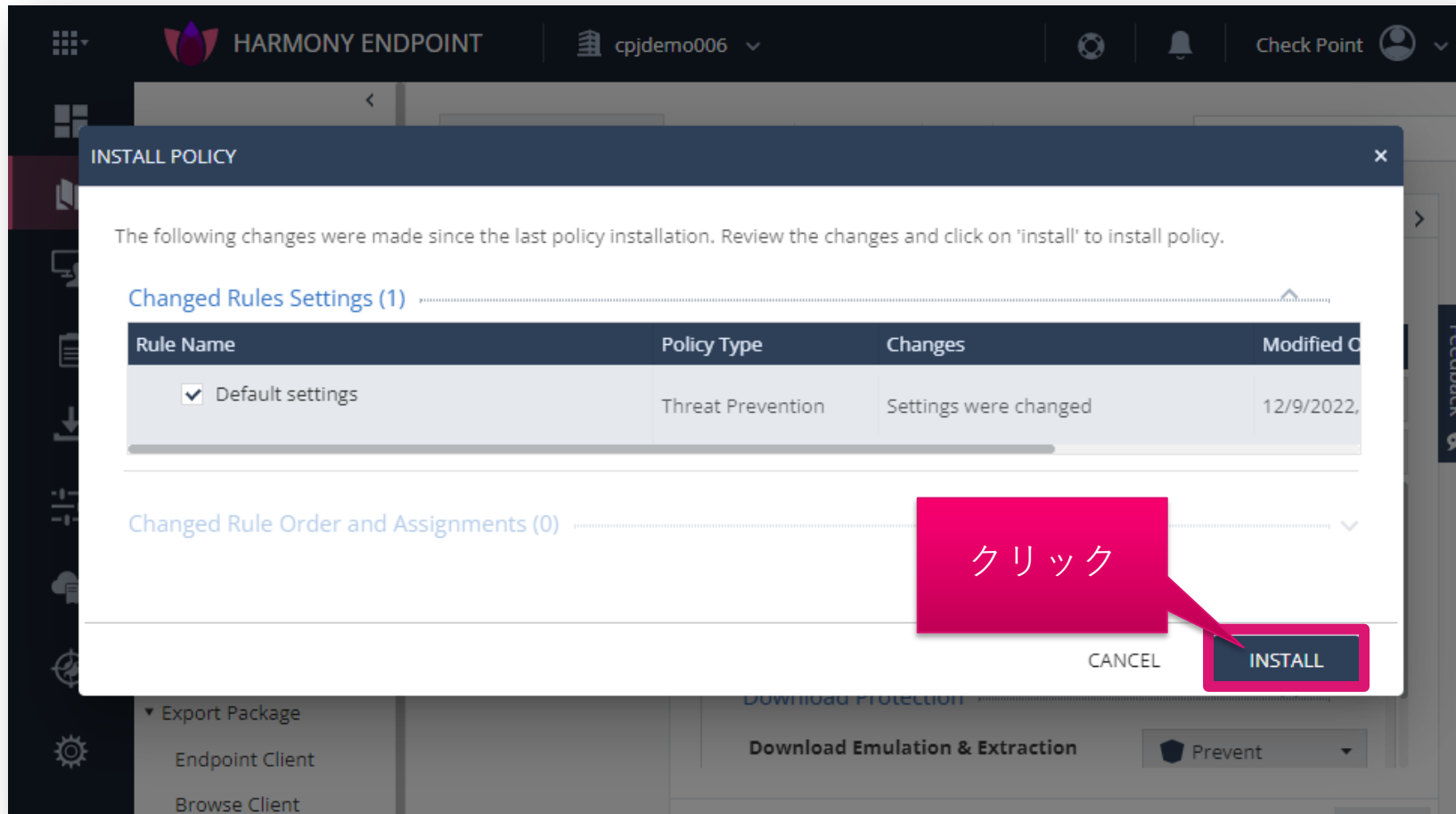
ホワイトリストを適用（個別ルールに適用する場合）（1 / 2）

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 displays the HARMONY ENDPOINT interface. The left sidebar shows navigation options: OVERVIEW, POLICY, and ASSET MANAGEMENT. The main area is titled 'Logs' and includes a search bar and a 'Last 7 Days' filter. A 'Statistics' section shows a 'Sessions Timeline' bar chart. Below this, a 'Blade' section lists 'Firewall' (41.24%), 'URL Filtering' (35.26%), and 'Anti-Malware' (8.87%). The central table lists log entries with columns for 'Time', 'B.', 'Matched Category', and 'Action'. A context menu is open over a log entry for 'https://kaiyasu.net/front/'. The menu options are 'Filter: \"https://kaiyasu.net/fro...\", 'Filter Out: \"https://kaiyasu.net...\", 'Create Exclusion for All Rules', and 'Create Exclusion for Effective Rule'. The 'LOGS' button in the sidebar is highlighted with a red box and labeled ①. A red callout box ② points to the log entry. Two red callout boxes ③ point to the 'Create Exclusion for All Rules' and 'Create Exclusion for Effective Rule' options in the menu.

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

ホワイトリストを適用（組織全体に適用する場合）（1 / 2）

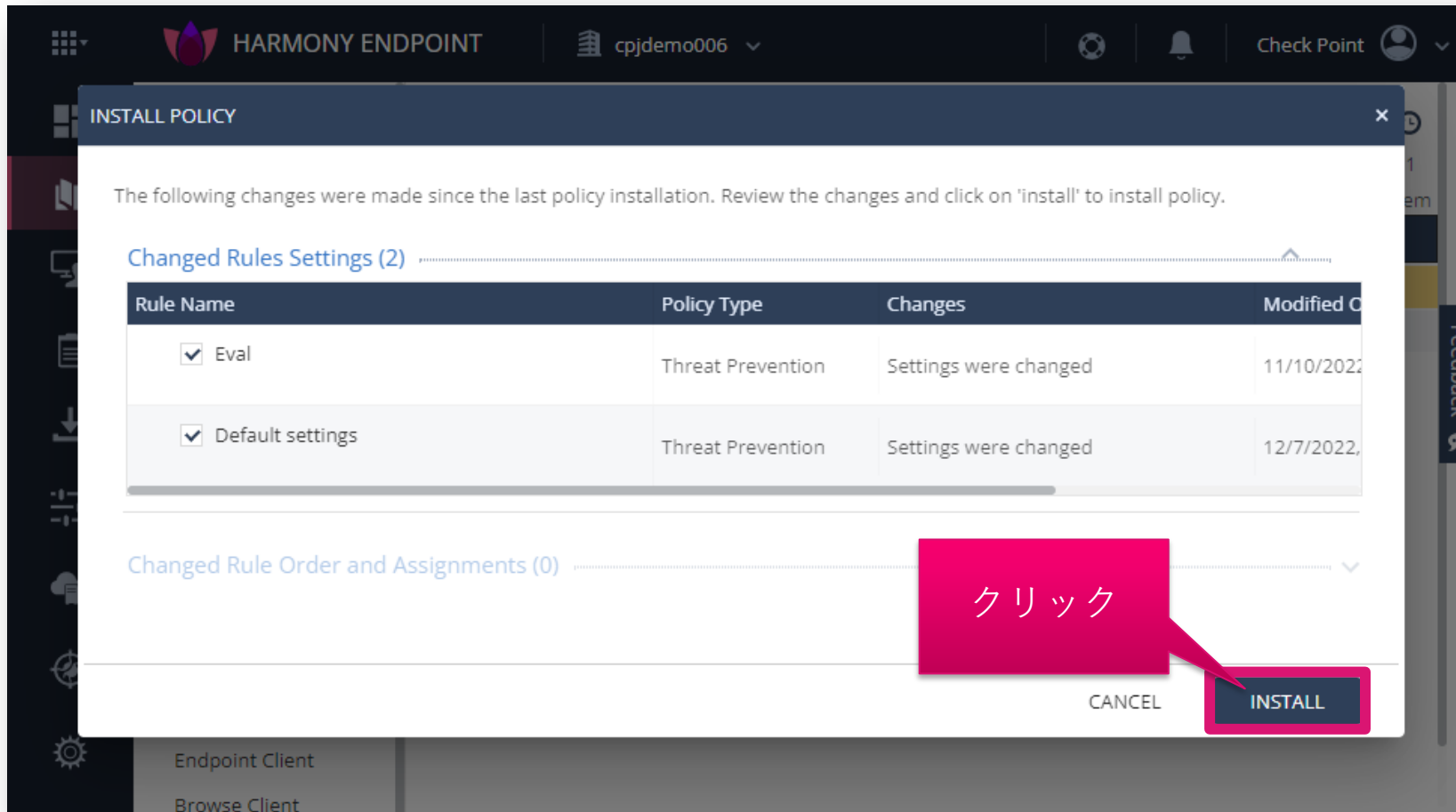
1. Global Exclusions の画面が表示され、除外設定が作成されていることを確認します
2. 「Save」 をクリックします
3. 「Install Policy」 をクリックします

The screenshot shows the 'Global Exclusions' configuration page in the Check Point Harmony Endpoint console. The left sidebar shows the navigation menu with 'Global Exclusions' selected. The main content area displays 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 value 'kaiyasu.net'. 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	Value
Anti Bot -> URL Filter Exclusions	
<input type="checkbox"/> Domain/URL	Domain/URL kaiyasu.net

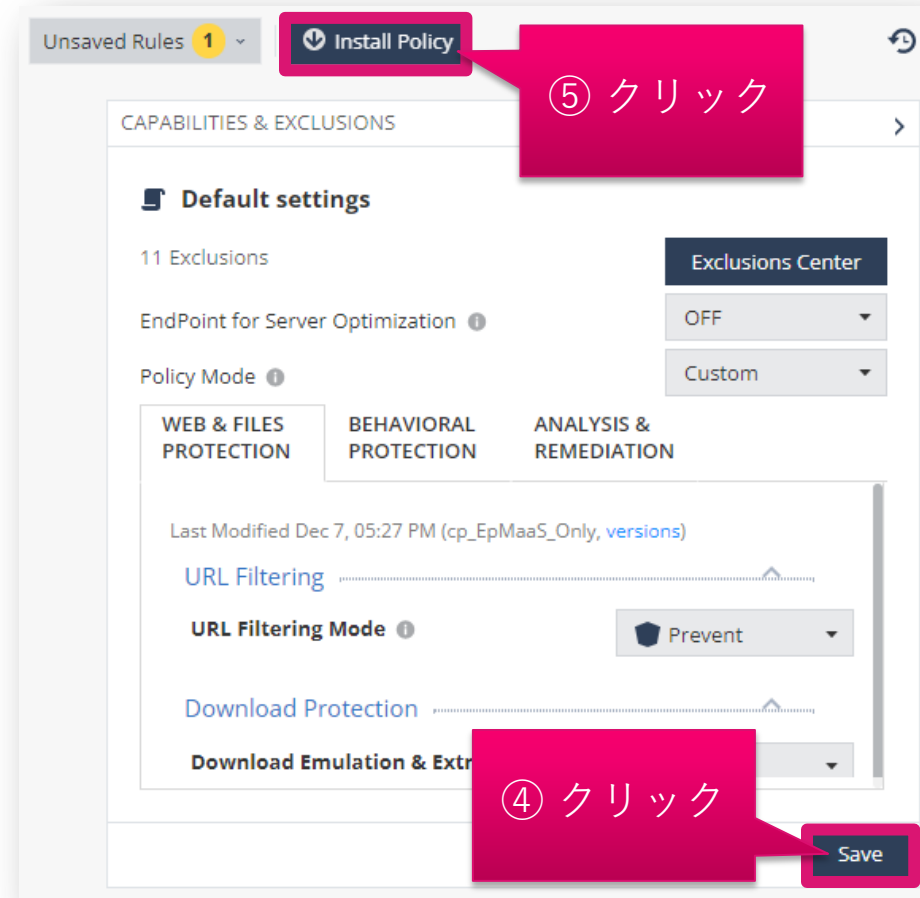
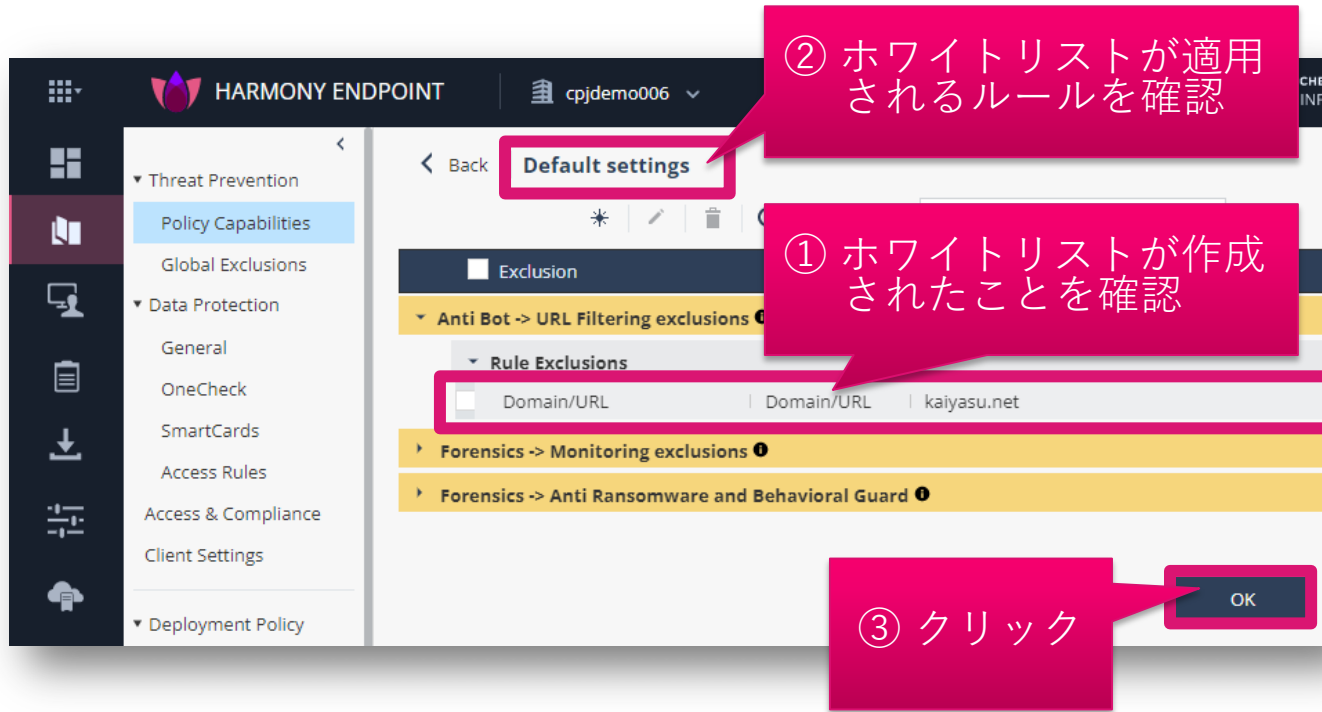
ホワイトリストを適用（組織全体に適用する場合）（2 / 2）

- 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



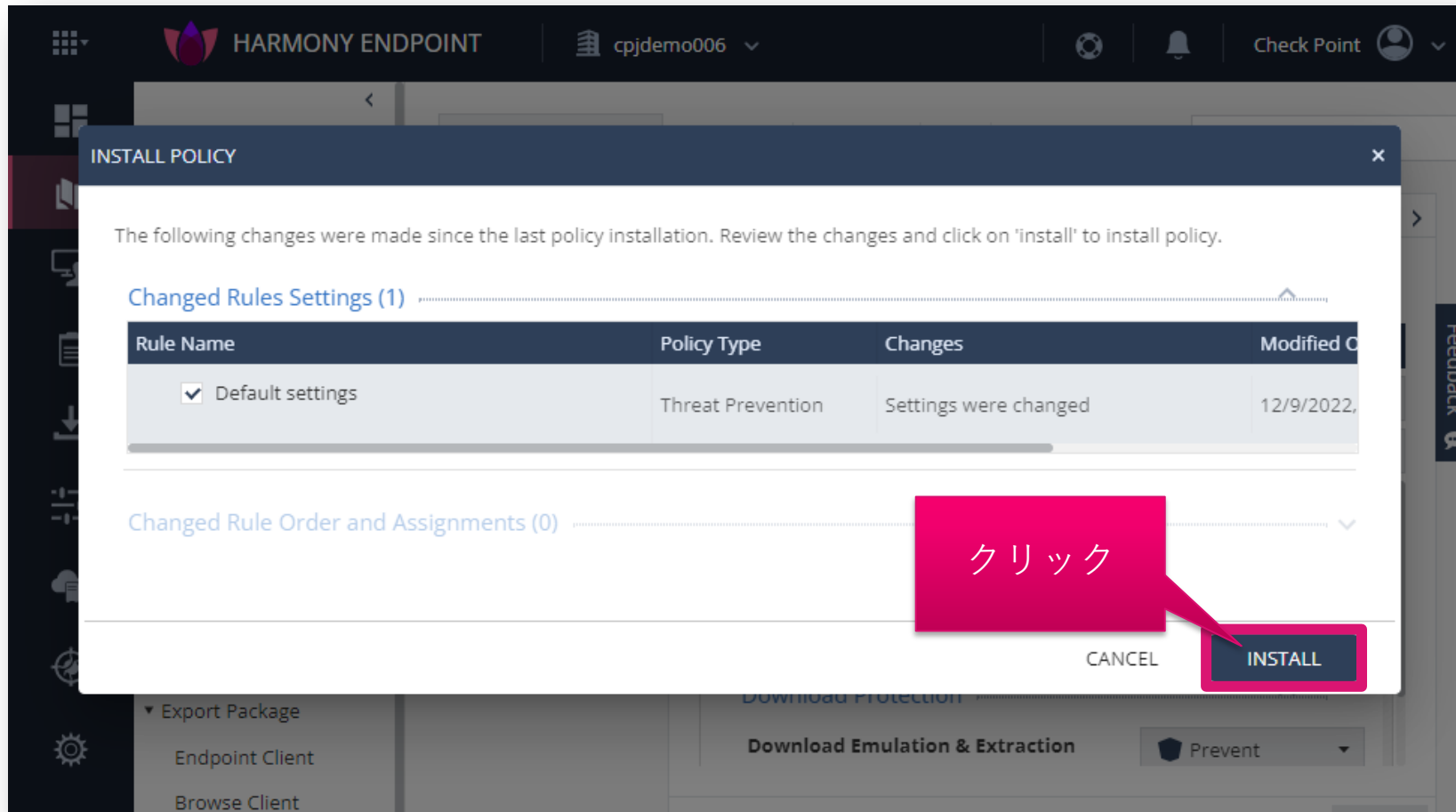
ホワイトリストを適用（個別ルールに適用する場合）（1 / 2）

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/



THANK YOU

YOU DESERVE THE BEST SECURITY