



# Harmony Endpoint 簡易運用ガイド

## 除外設定：Threat Emulation／Extraction、Zero-Phishing

Policy > Policy Capabilities > Exclusion Center

Policy > Global Exclusion

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

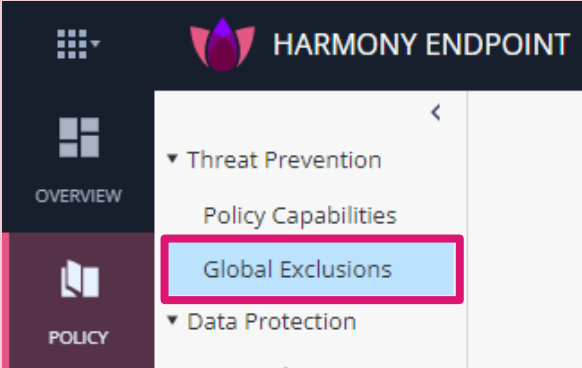
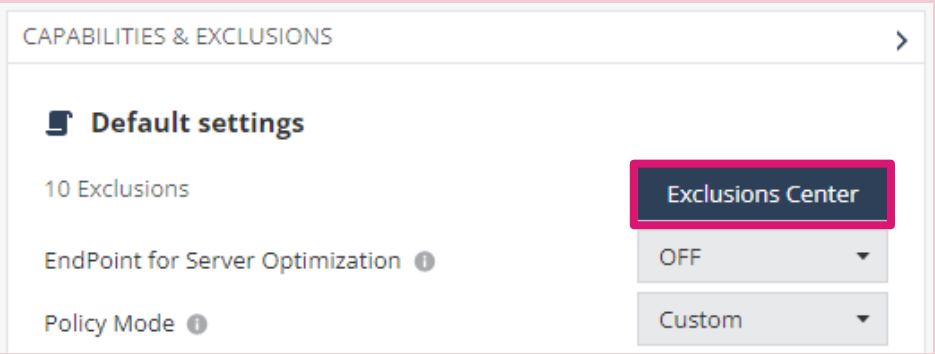
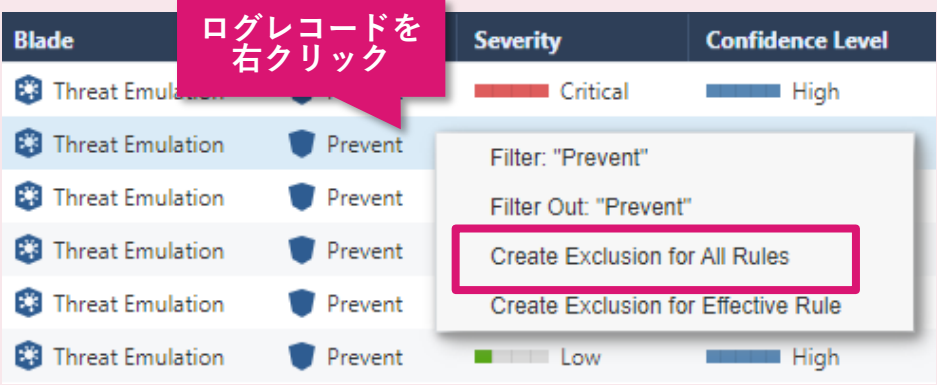
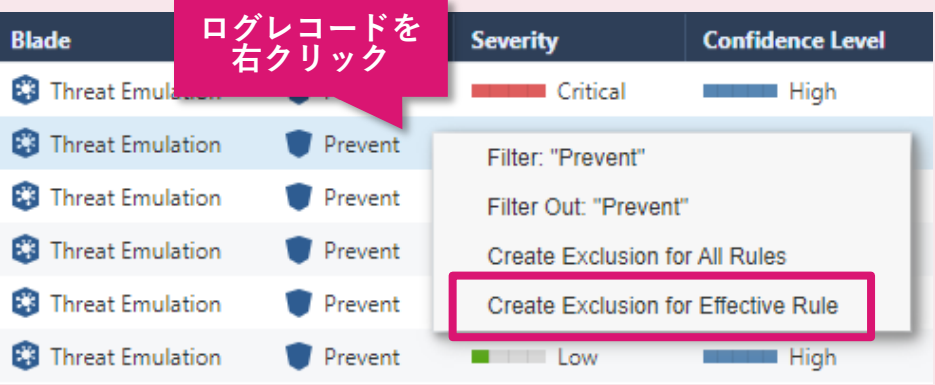
# 目次

- 除外設定の概要
- Webダウンロード時のThreat Emulation／Extraction、Zero-Phishingの除外設定

# 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	 <p>ログレコードを右クリック</p>	 <p>ログレコードを右クリック</p>

# 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				

# Webダウンロード時の Threat Emulation/Extraction の除外設定

# 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

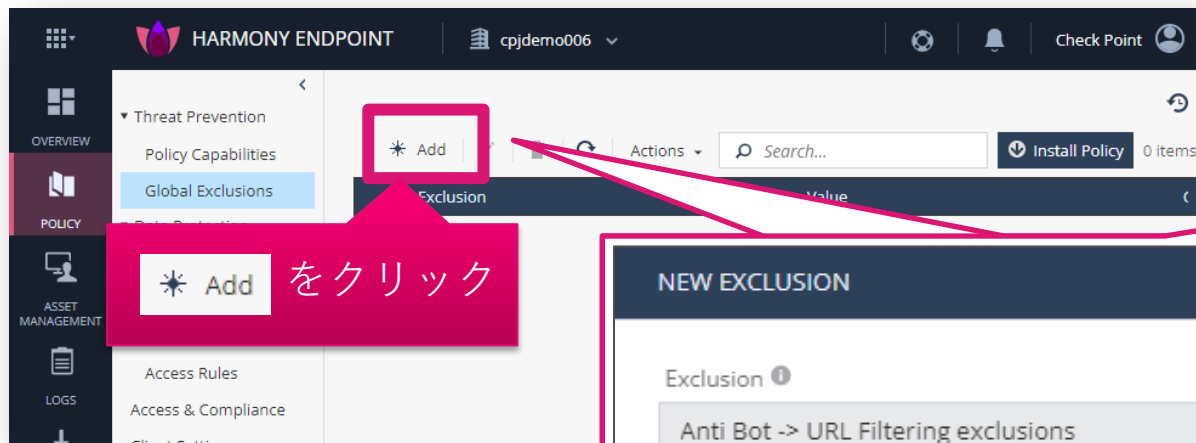
Comment

CANCEL OK

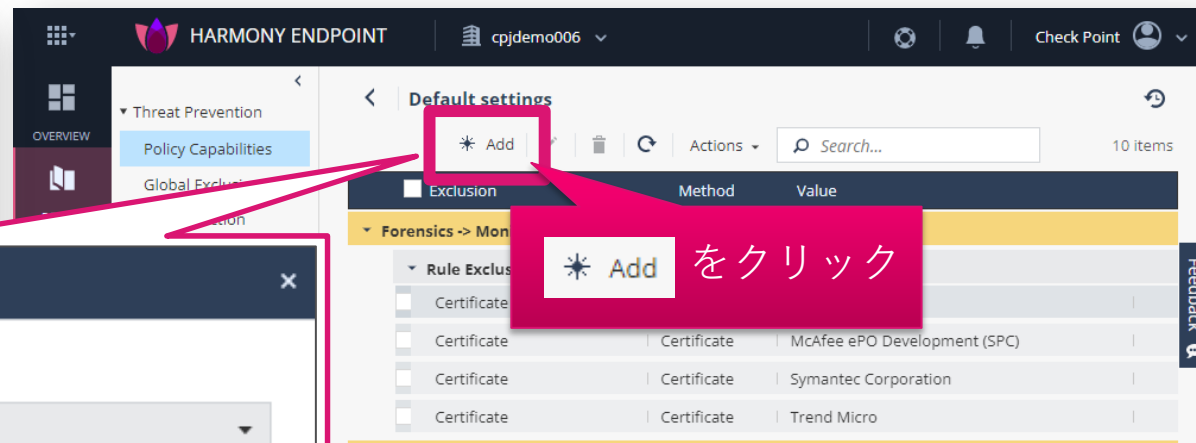
# 除外設定の作成画面を表示

- 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 画面のスクリーンショット。以下の設定が確認できます。

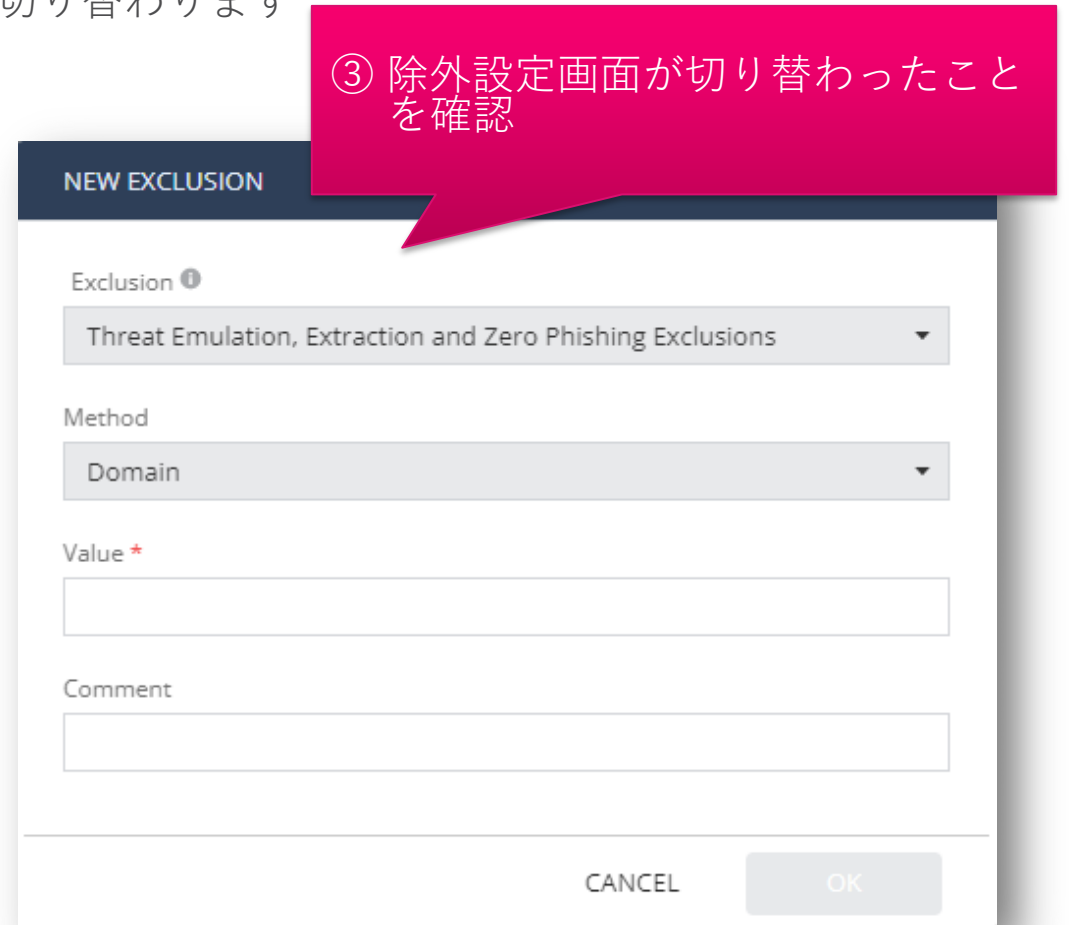
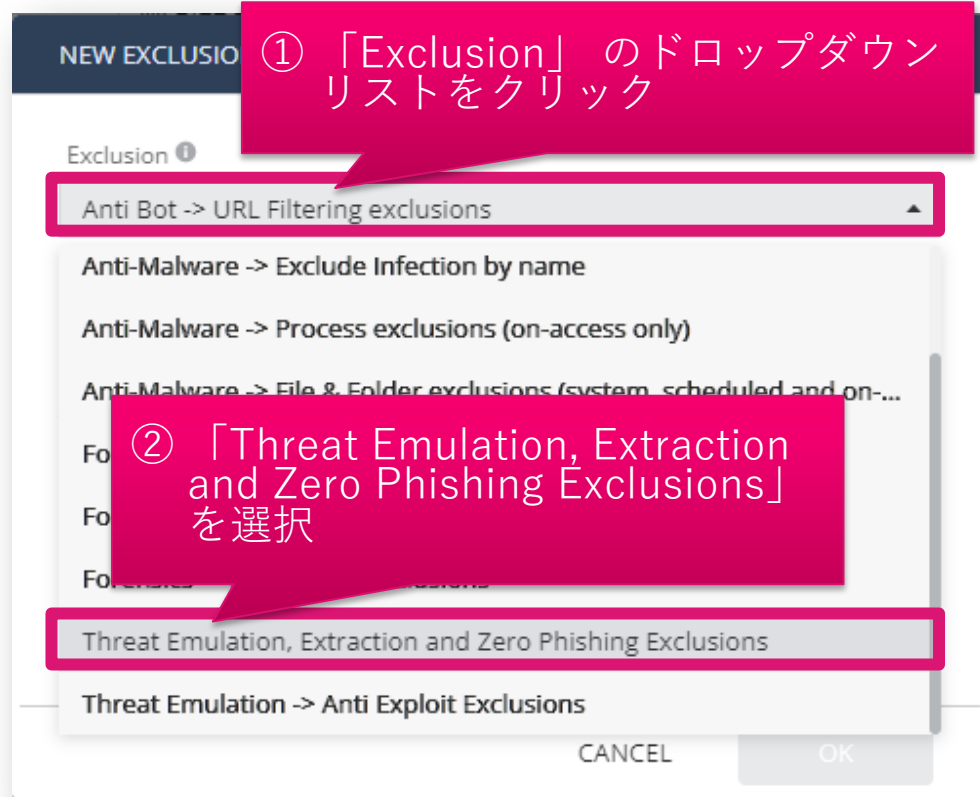
- Exclusion: Anti Bot -> URL Filtering exclusions
- Method: Domain/URL
- Value: (空欄)
- Add to all rules

ボタン: 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

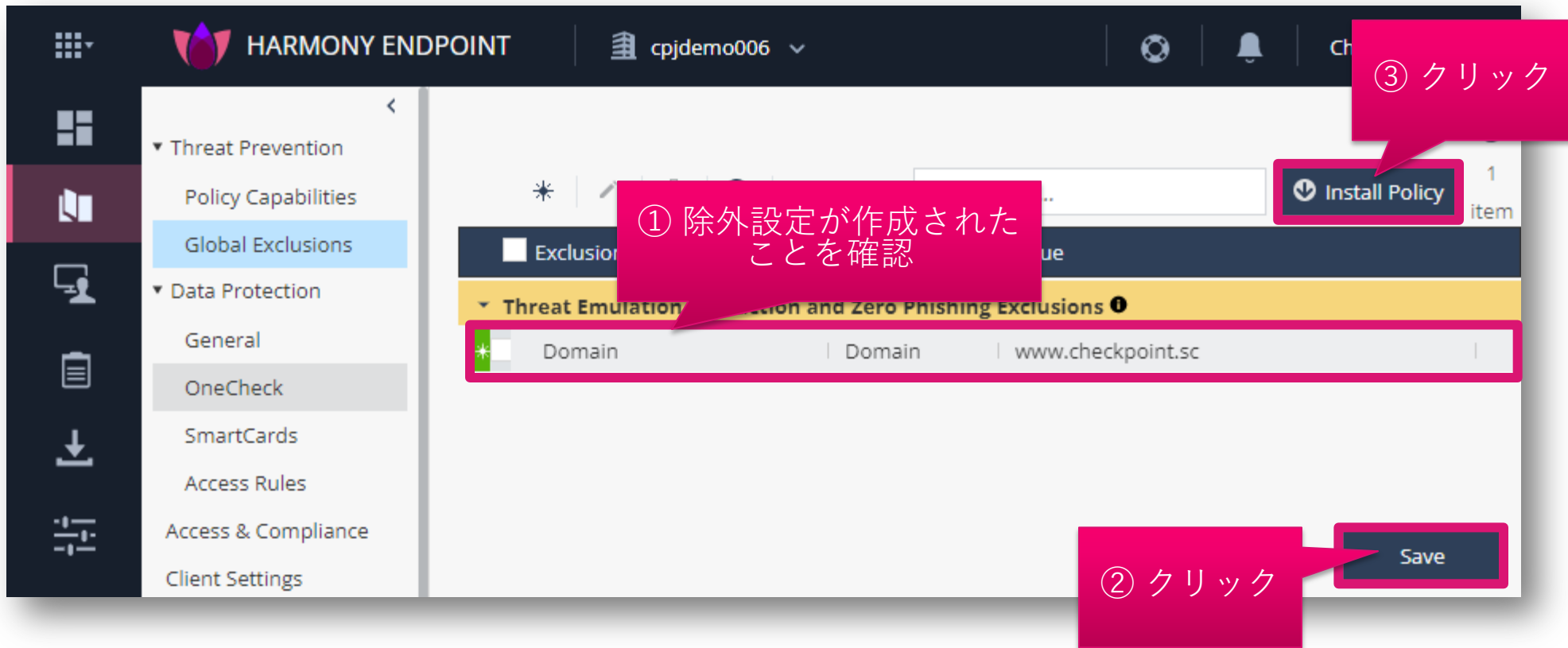
Value \*  
www.checkpoint.sc

Comment

CANCEL OK

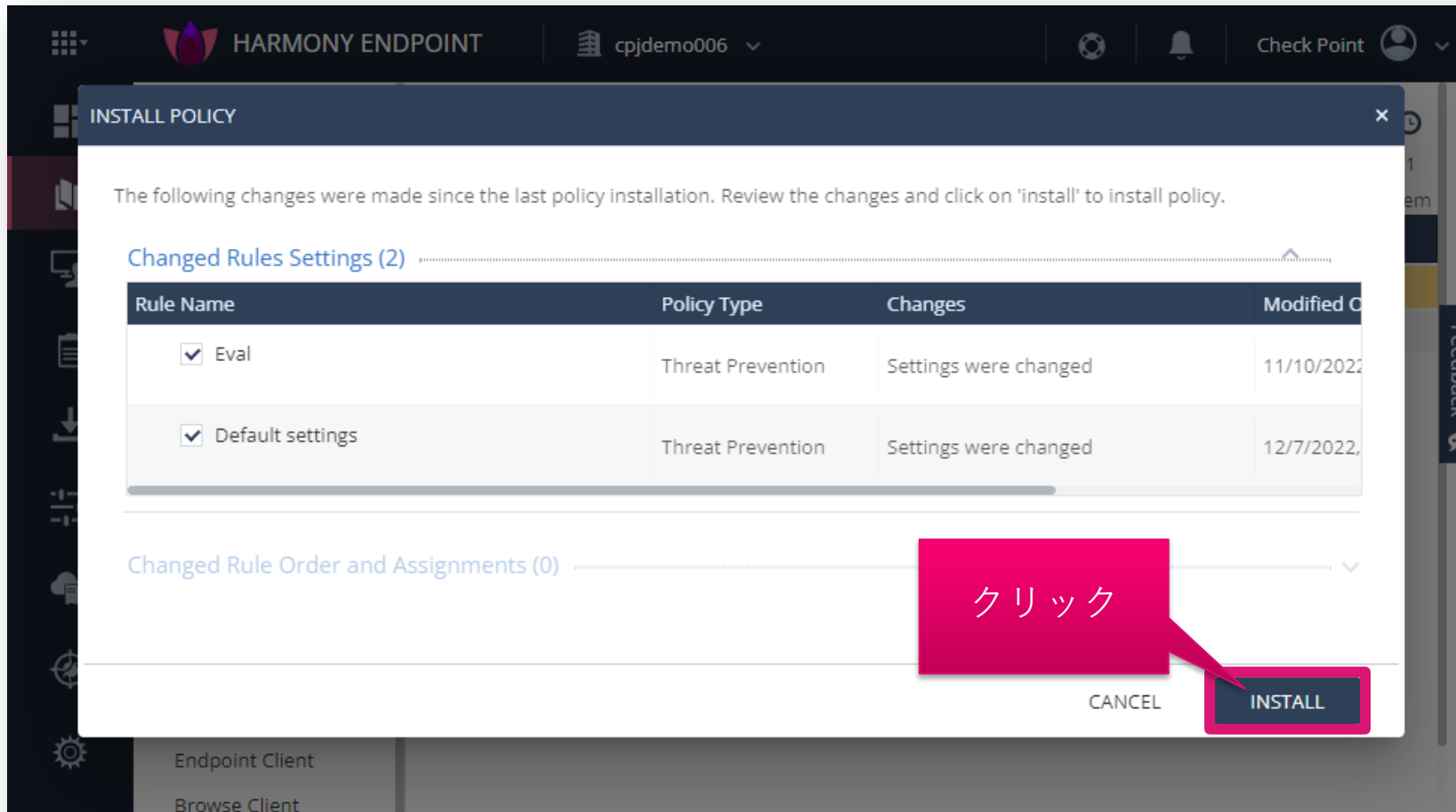
# 除外設定を適用（組織全体に適用する場合）（1 / 2）

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



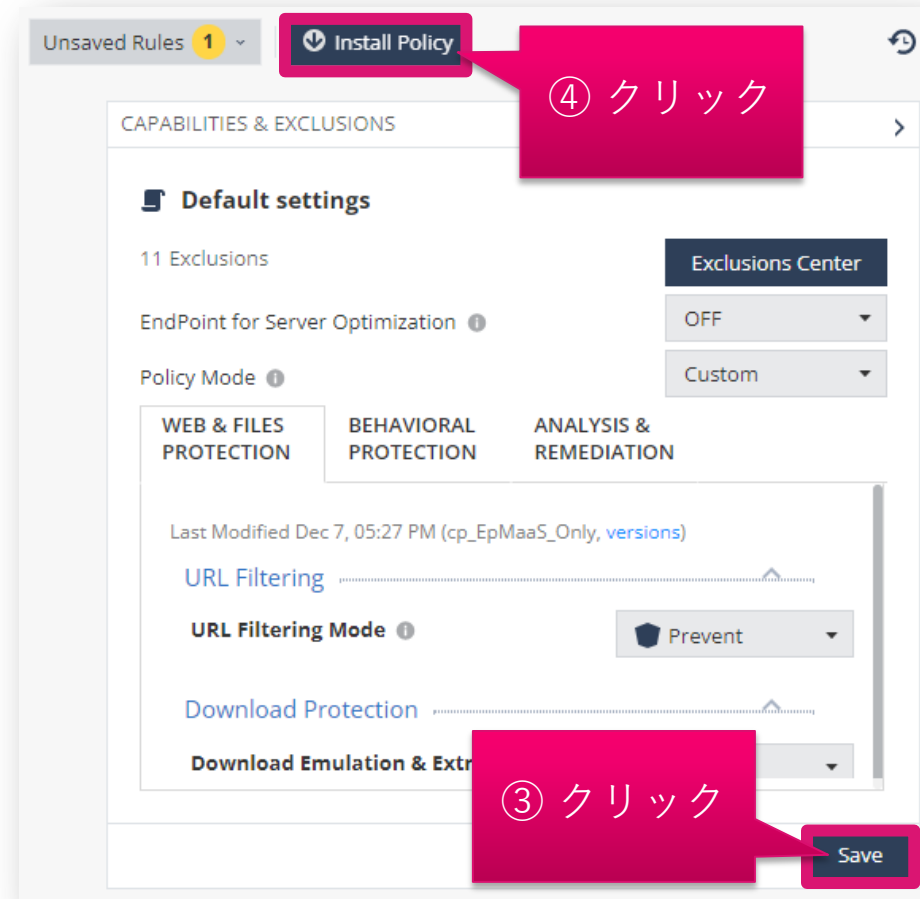
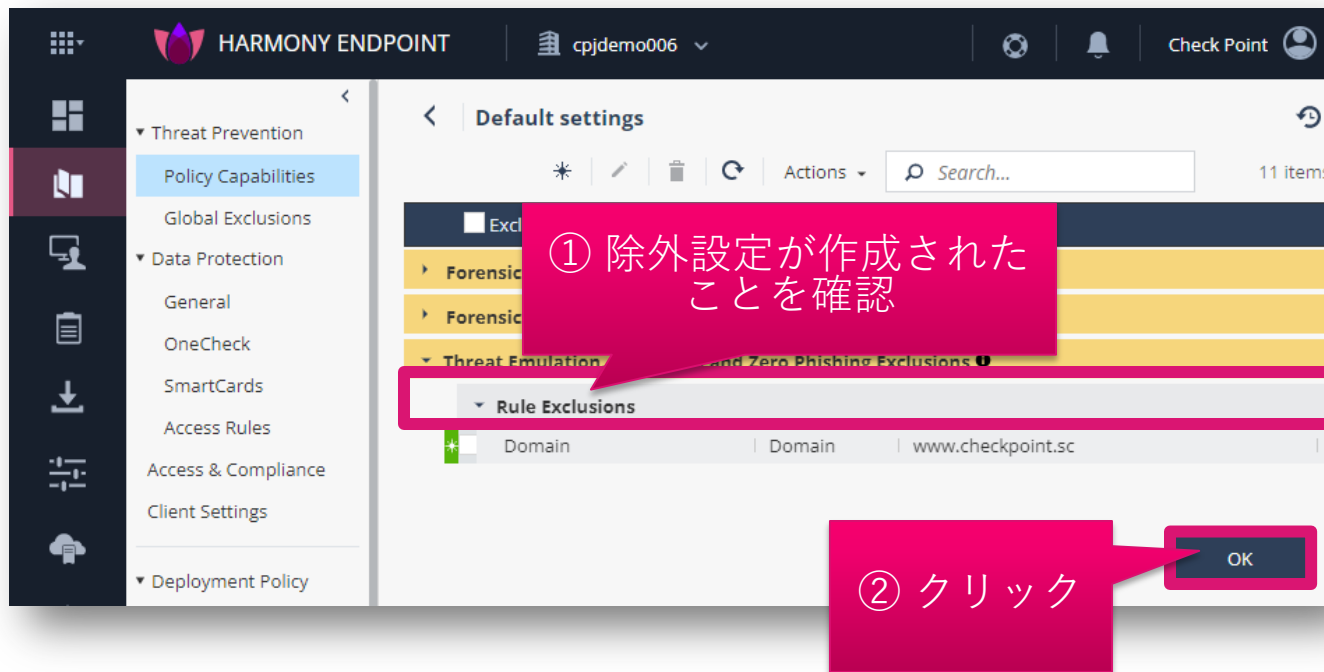
# 除外設定を適用（組織全体に適用する場合）（2 / 2）

- 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



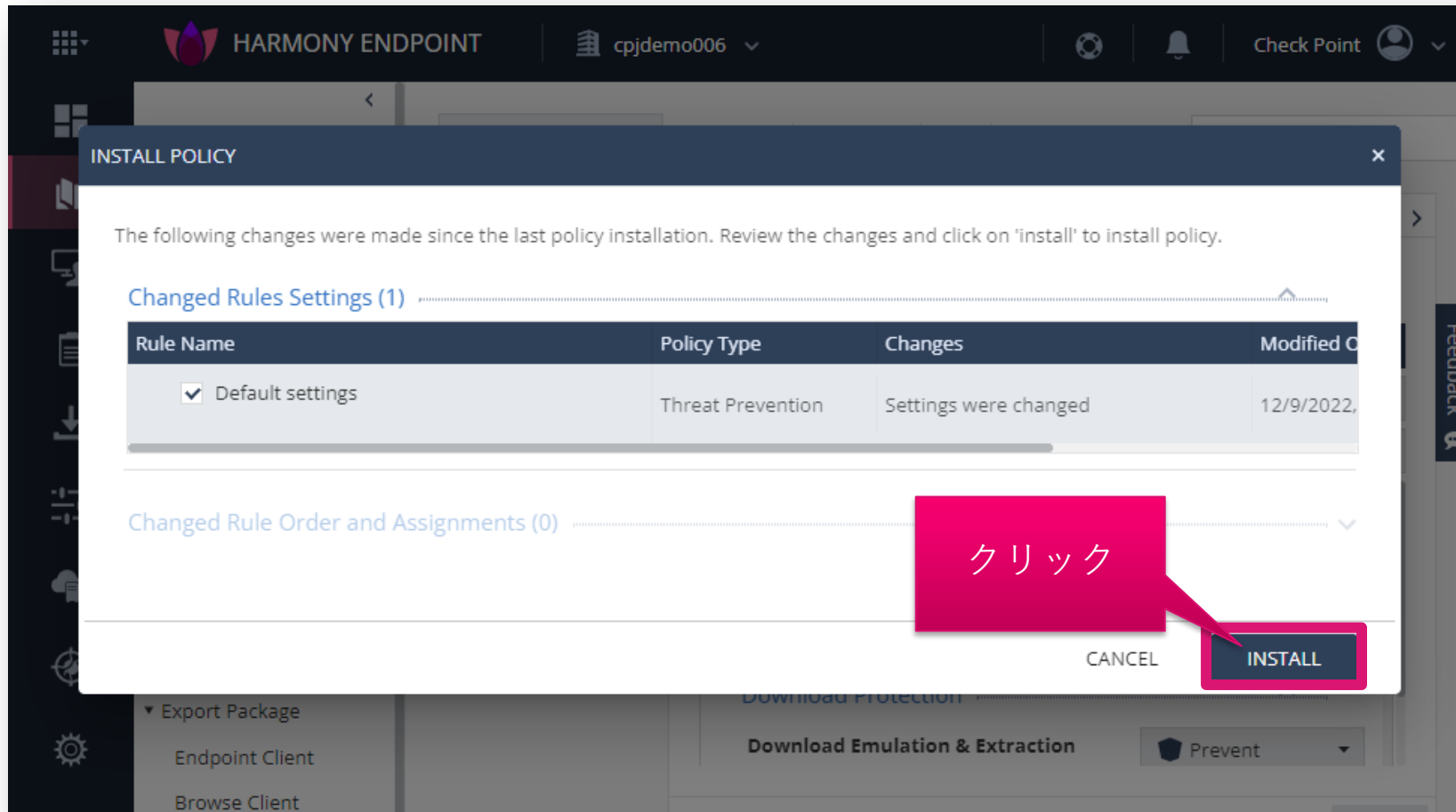
# 除外設定を適用（個別ルールに適用する場合）（1 / 2）

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





*THANK YOU*

YOU DESERVE THE BEST SECURITY