



HARMONY ENDPOINT 簡易設定ガイド

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社

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

YOU DESERVE THE BEST SECURITY

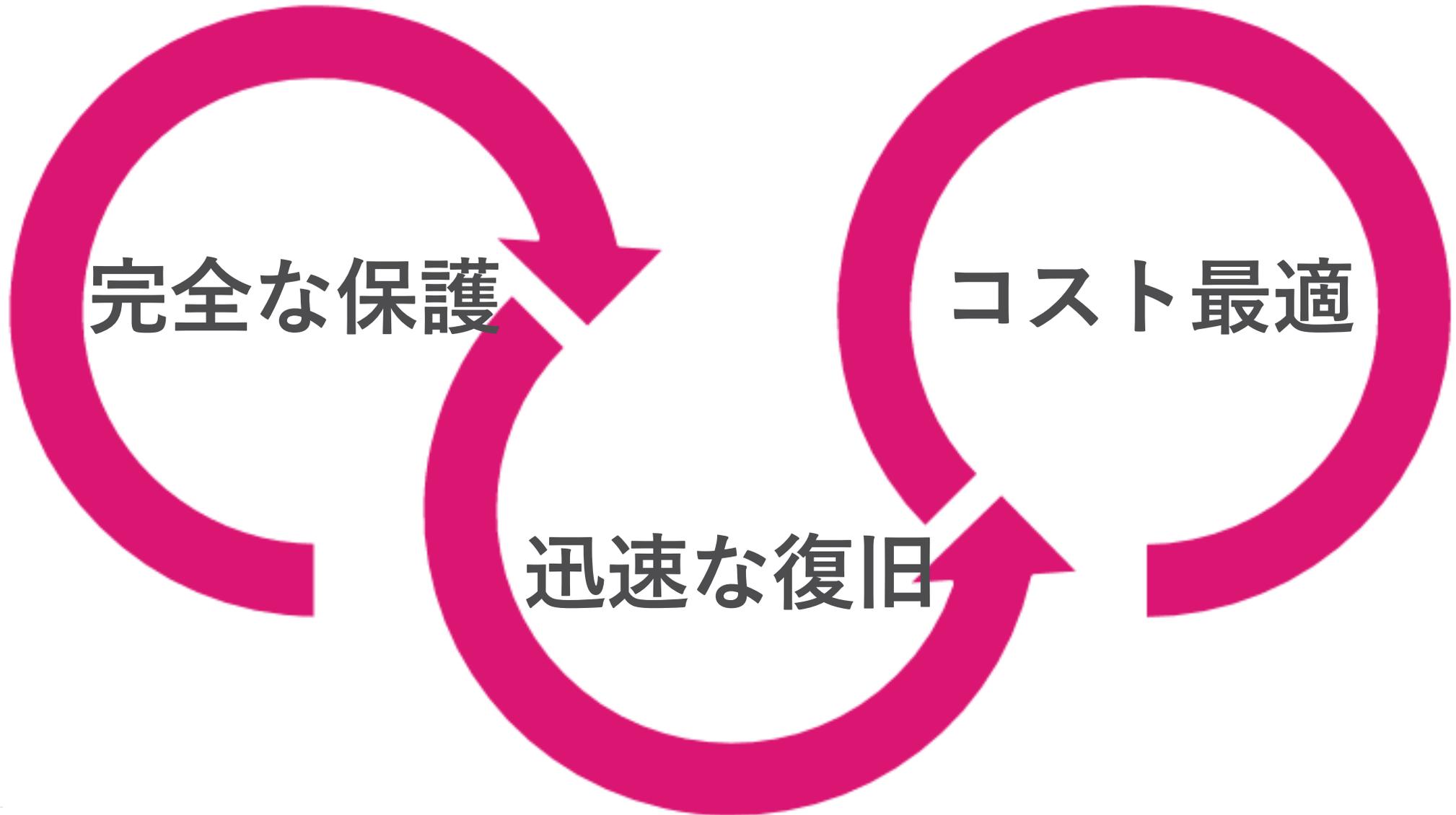
Table of Contents

- Harmony Endpoint の概要
 - サーバ最適化
- Infinity Portal へのサインイン
- Harmony Endpoint の有効化
- 設定画面の概要
- 設定の流れ
- バーチャルグループによる管理
- アンインストールパスワードの設定
- アラート通知設定
- ポリシーの設定
 - ポリシーの SAVE と INSTALL
 - Threat Prevention
 - Client Settings

HARMONY ENDPOINT の概要

YOU DESERVE THE BEST SECURITY

Harmony Endpoint の特徴



エンドポイントに必要なすべての保護を提供

攻撃からの防御

EPP & NGAV

攻撃の検知と対応

EDR

検知 & 防止



アンチ・マルウェア



サンドボックス



ファイル無害化



ゼロ・フィッシング

封じ込め



アンチ・ランサムウェア



アンチ・ボット



アンチ・エクスプロイト

可視化と分析



フォレンジックレポート



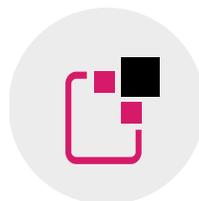
Threat Hunting

Harmony Endpoint の先進の防御技術



サンドボックス

OSレベルとCPUレベルの統合型サンドボックスで攻撃を遮断



ファイル無害化

ファイルの無害化による安全性と生産性の両立



ゼロフィッシング

フィッシングサイトからユーザの認証情報を保護



アンチ・ランサムウェア

ランサムウェアの攻撃を停止し、ファイルを自動復旧



アンチ・ボット

攻撃者との通信を遮断し、攻撃の拡大を阻止



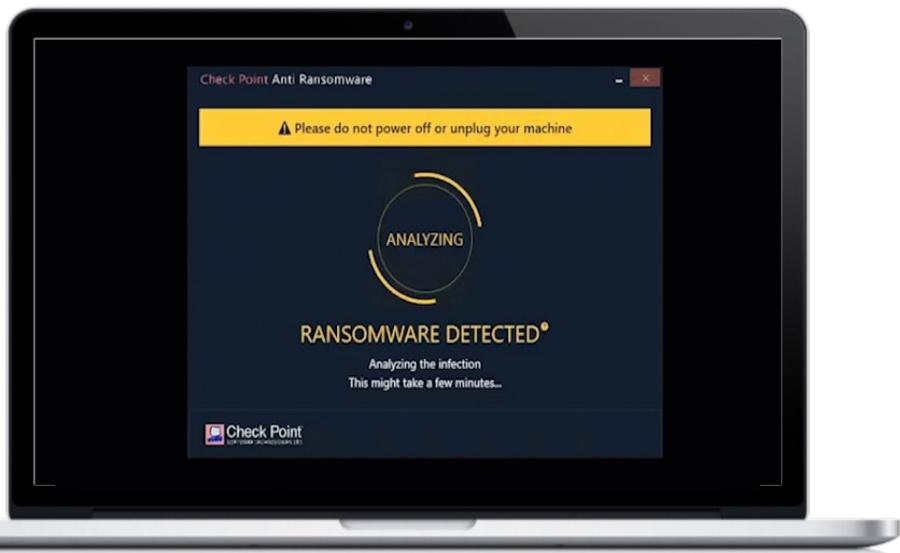
フォレンジックレポート

独自の解析技術による正確性の高い攻撃解析

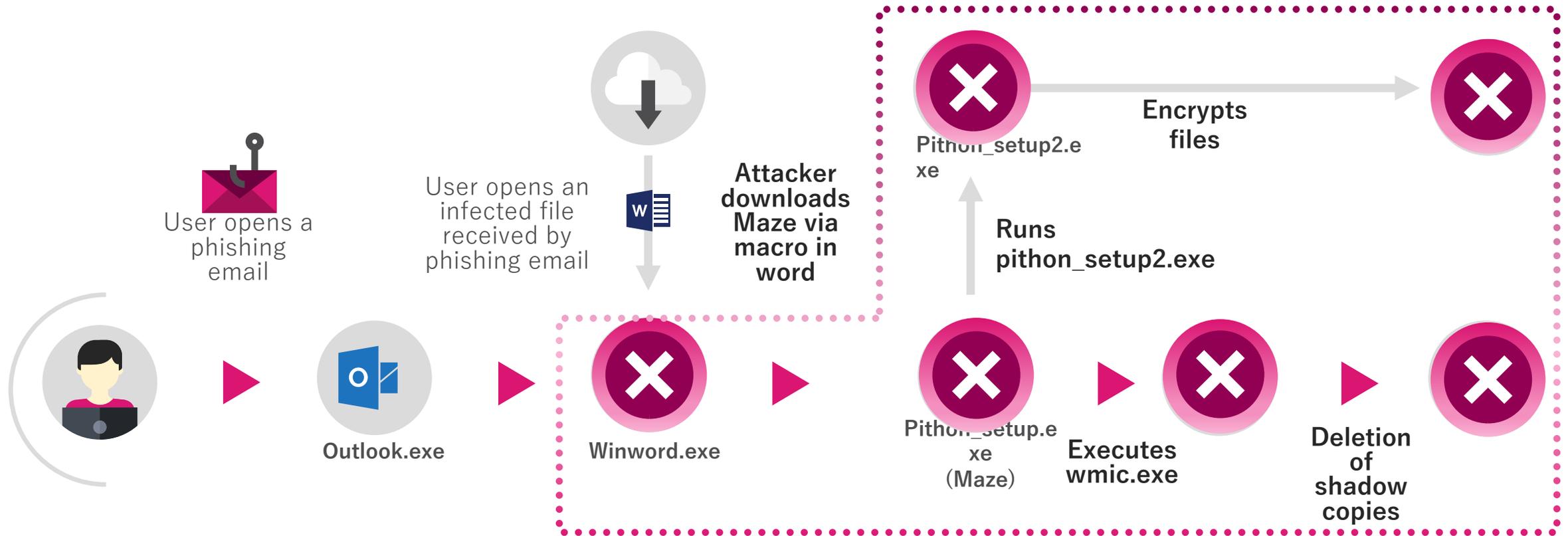
検知、調査、修復作業の 90% を自動化

自動化

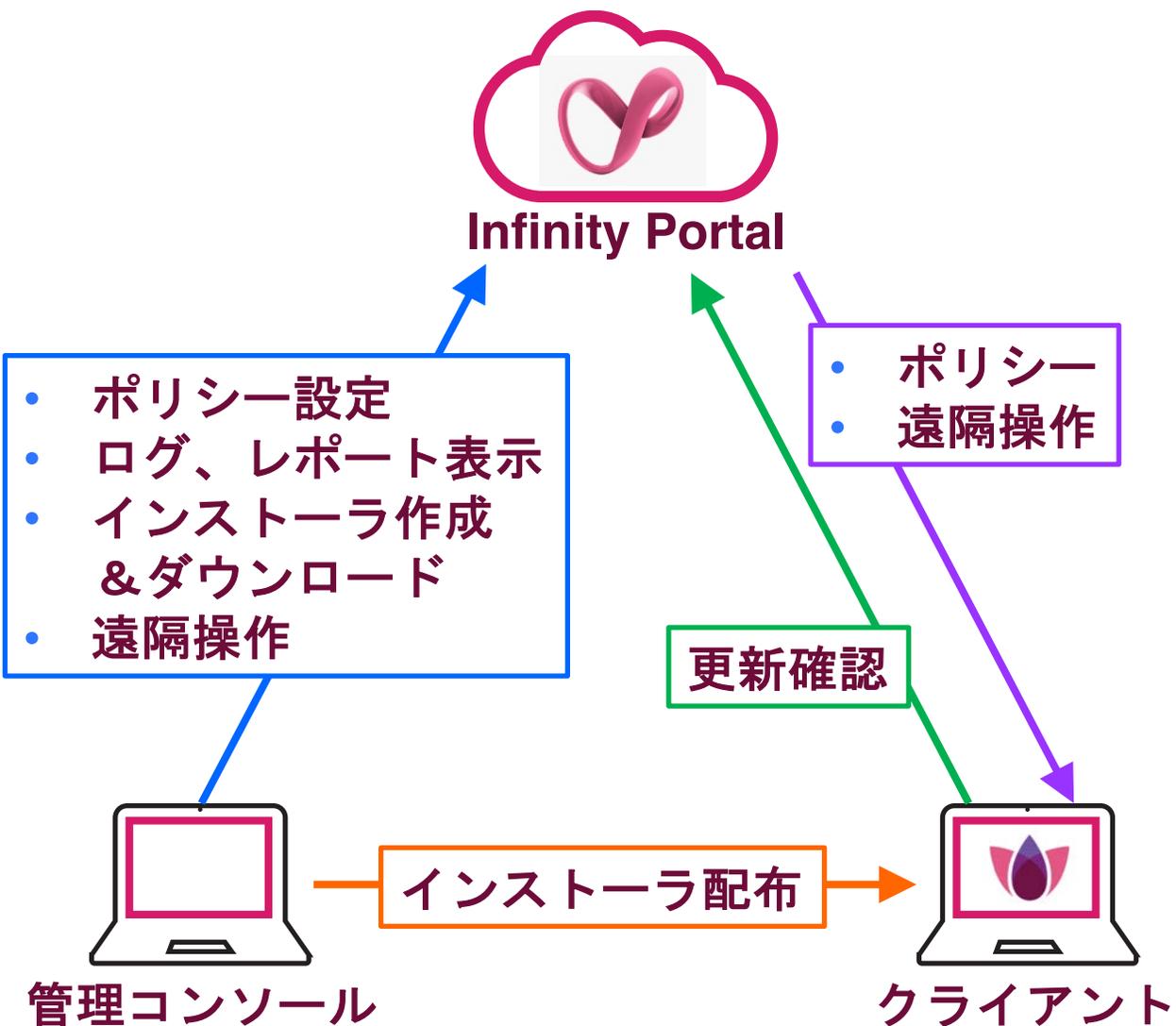
- あらゆるイベントを監視、収集
- 攻撃を検知
- 悪意のある活動を隔離
- サイバーキルチェーン全体をクリーンナップ
- 暗号化されたファイルを復元
- フォレンジックレポートを提供



サイバーキルチェーン全体を自動的かつ完全に修復し、ビジネスの継続性を確保



Harmony Endpoint の構成概要



1. Infinity Portal

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

2. 管理コンソール

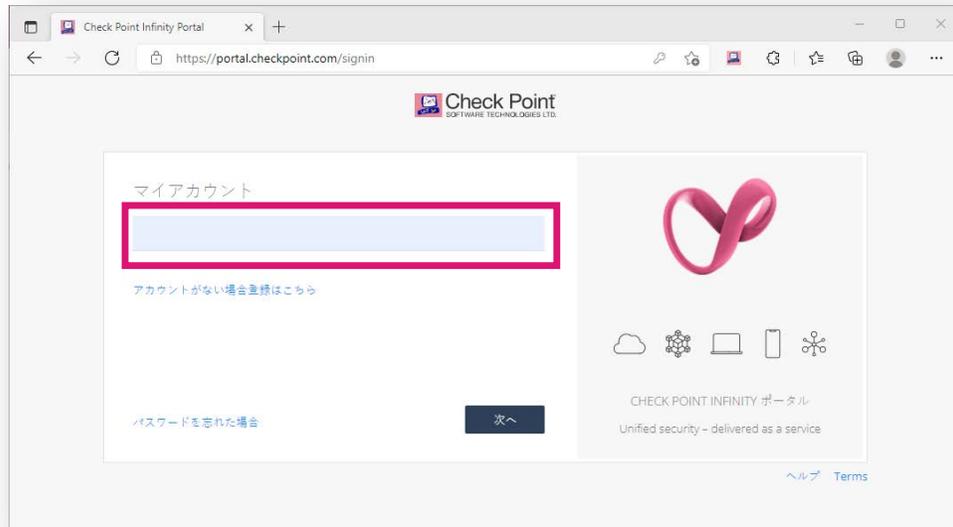
- Infinity Portal にアクセスして管理を行うパソコン
- ブラウザで管理を実施

3. クライアント

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

INFINITY PORTAL へのサインイン

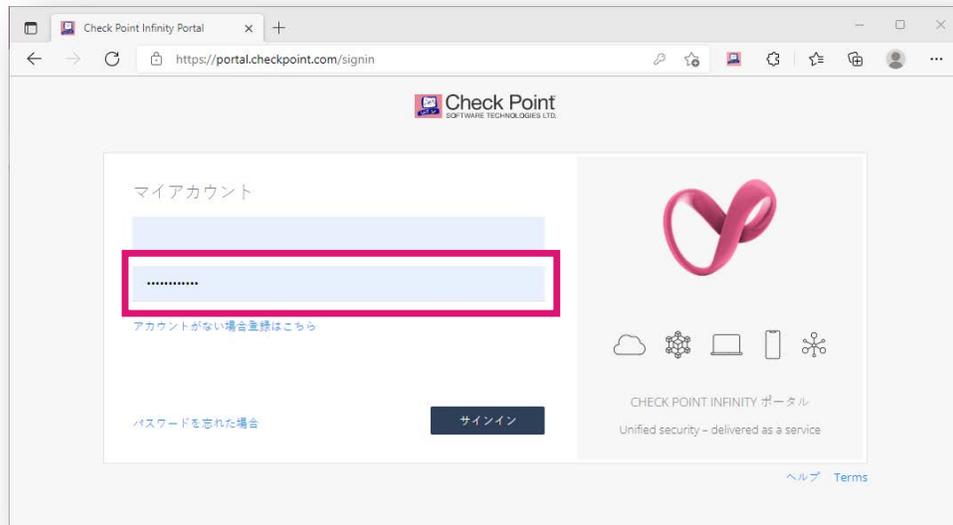
Infinity Portal へのサインイン (1 / 2)



1. Infinity Portal へ接続する

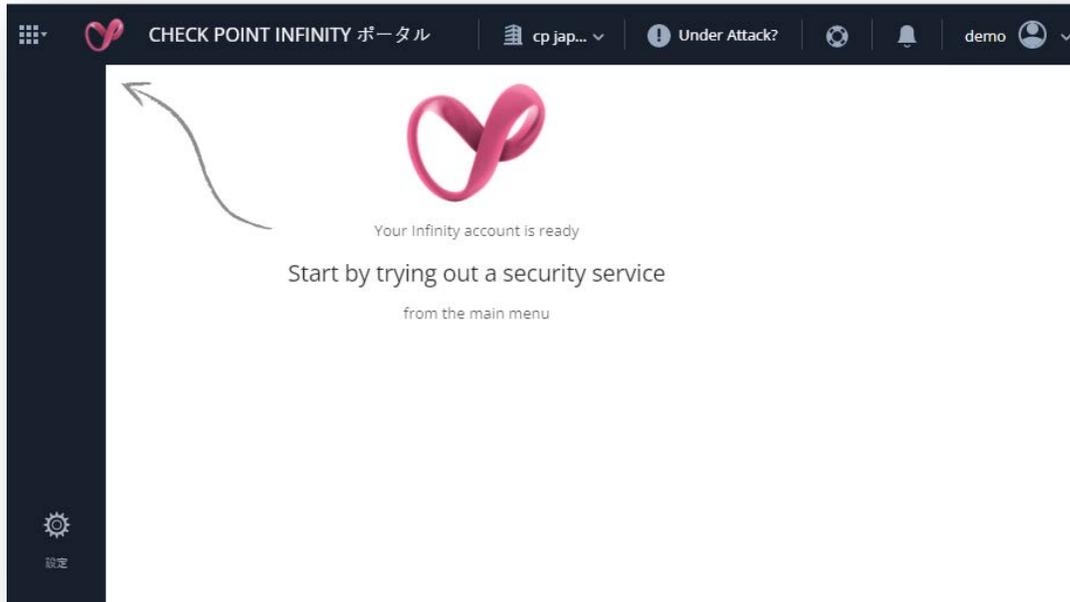
- URL: <https://portal.checkpoint.com/>

2. ユーザー名を入力して、「次へ」を押す



3. パスワードを入力して、「サインイン」を押す

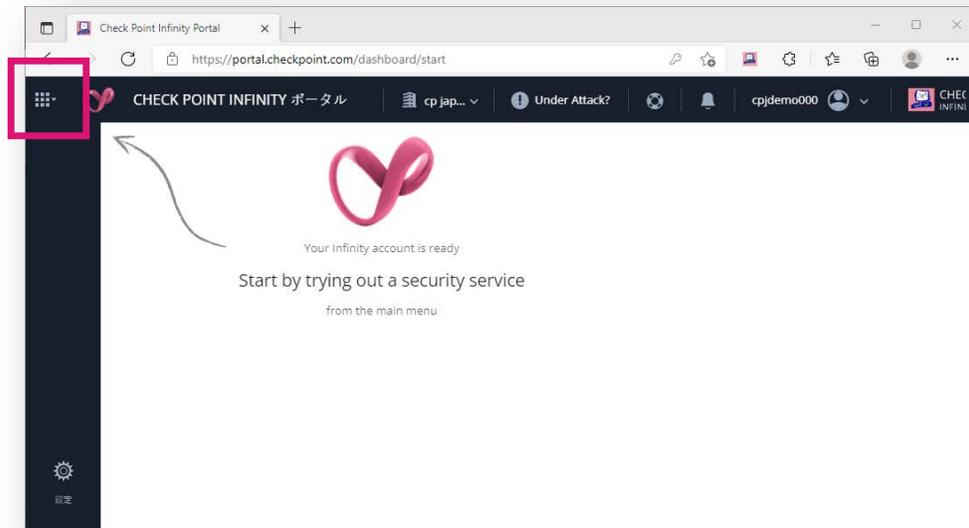
Infinity Portal へのサインイン (2 / 2)



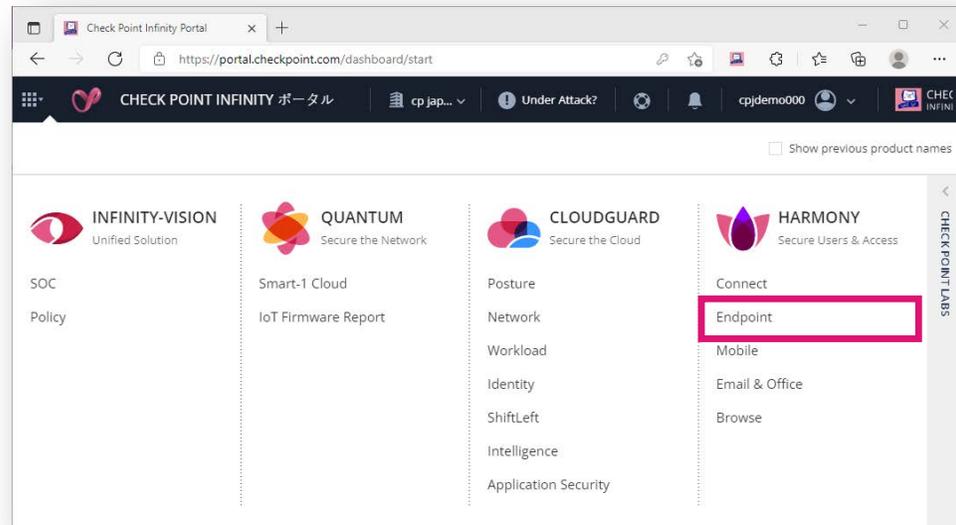
4. サインイン成功

HARMONY ENDPOINT の有効化

Harmony Endpoint の有効化 (1 / 3)

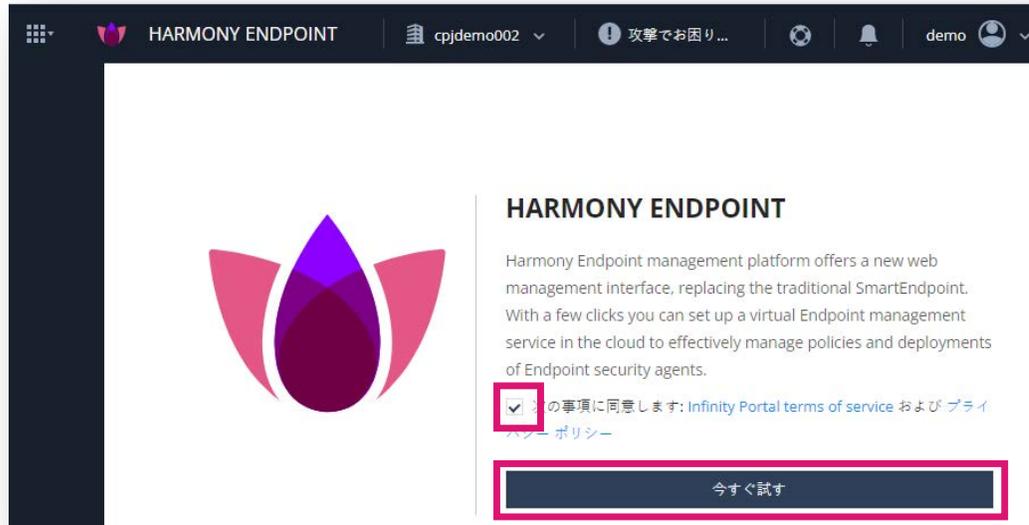


1. 左上のメニューボタン  を押す

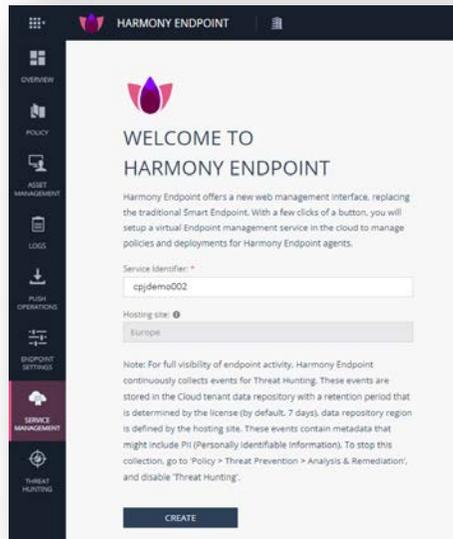


2. 「HARMONY Endpoint」を選択する

Harmony Endpoint の有効化 (2 / 3)

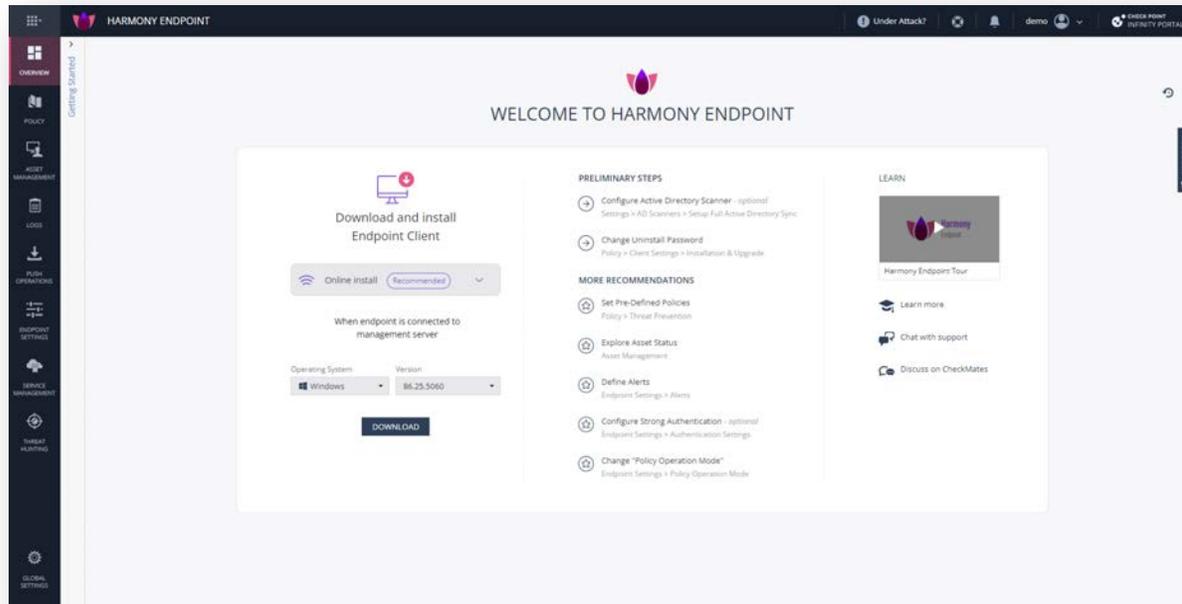


3. Infinity Portal terms of service、個人情報保護方針を確認し、「契約事項に同意する」のチェックボックスにチェックを入れ、「今すぐ試す」を押す



4. 「CREATE」を押す

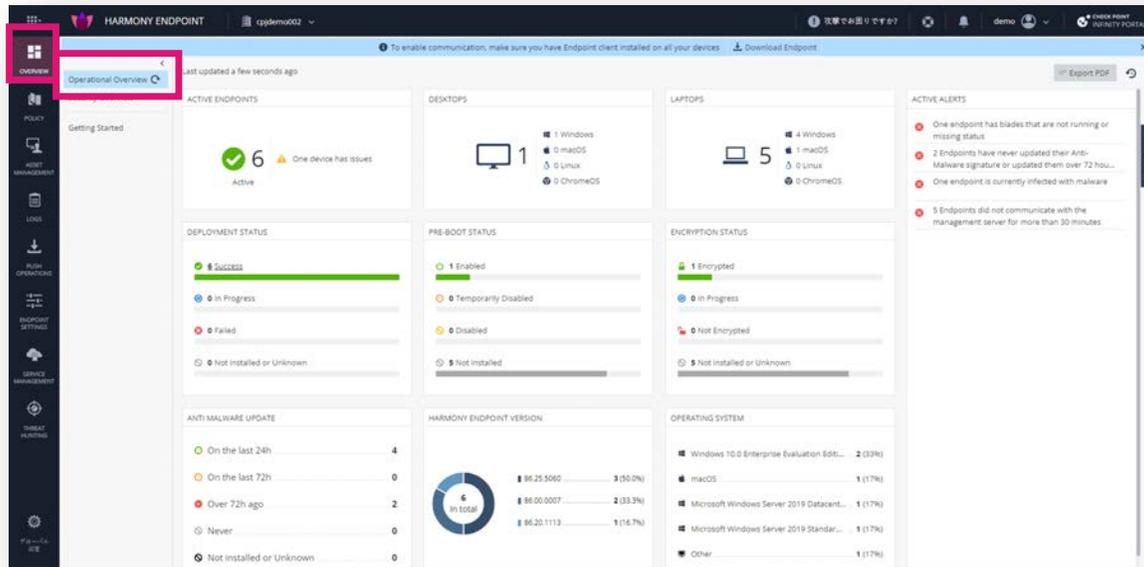
Harmony Endpoint の有効化 (3 / 3)



5. HARMONY Endpoint の有効化が完了

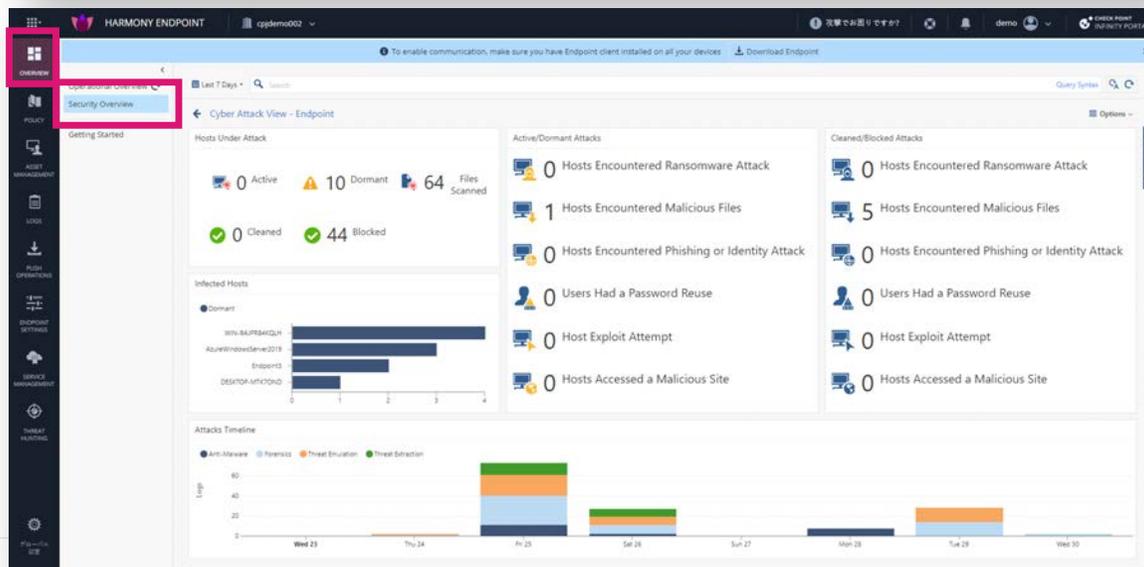
設定画面の概要

Overview ページ



Operational Overview

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



Security Overview

- エンドポイントクライアントへの攻撃統計を表示します

Policy ページ

設定項目を選択

グループごとにポリシーを構成

ポリシーの詳細を構成

#	Rule Name	Applied To	Web & Files	Behavioral	Analysis
0	macOS	macOS			
1	Windows Server	Windows Se...			
2	demo	demo			
3	demo3	demo3			
4	Default settings for the entire organization	Entire Organ...			
5	Default settings for the entire organization	Entire Organ...			

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

Asset Management ページ

リモートからコンピュータを操作

一覧表示

一覧表示の条件選択

詳細表示

Status	Computer Name	Endpoint Version	OS Build	Device Type	Deployment Status	Deploy Time	Capabilities
Completed	AzureWindowsServ...	86.25.5060	10.0-17763-SP0.0-S...	Desktop	Completed	25 Mar 2022 07:11 pm	
Completed	DESKTOP-TGj6R26	86.00.0007	10.0-19043-SP0.0-S...	Laptop	Completed	22 Mar 2022 12:42 pm	
Completed	Endpoint2	86.00.0007	10.0-19043-SP0.0-S...	Laptop	Completed	18 Mar 2022 06:42 pm	
Completed	Endpoint3	86.25.5060	10.0-19043-SP0.0-S...	Laptop	Completed	25 Mar 2022 01:42 pm	
Completed	WIN-9AJPRB4KQLH	86.25.5060	10.0-17763-SP0.0-S...	Laptop	Completed	25 Mar 2022 01:38 pm	
Completed	adminnomaacbook...	86.20.1113	11.6.4 (20G417)	Laptop	Completed	28 Mar 2022 07:37 pm	

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

Logsページ (1 / 2)

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

LOGS

Time	Blade	Action	Severity	Protection Type	Protection Name	File Name
Mar 30, 2022 2:13:21 PM	Forensics	Detect	Low	Generic	gen.win.trojan	backdoor.msil.tyup
Mar 30, 2022 2:13:06 PM	Forensics	Detect	Low	Generic	DOS/EICAR_Test_File	eicar_com.zip
Mar 30, 2022 9:09:10 AM	Endpoint Compliance	Detect	Medium			
Mar 30, 2022 9:08:20 AM	Full Disk Encryption		Medium			
Mar 30, 2022 9:08:19 AM	Full Disk Encryption		Medium			
Mar 30, 2022 9:07:21 AM	Endpoint Compliance	Inform...	Critical			
Mar 30, 2022 9:07:17 AM	Endpoint Compliance		High			
Mar 30, 2022 1:09:18 AM	Anti-Malware		Low			
Mar 30, 2022 12:59:02 AM	Forensics	Prevent	High	File System Emulation	Gen.SB.exe	14e48d3aa7b9058x
Mar 30, 2022 12:58:50 AM	Forensics	Prevent	High	File System Emulation	Gen.SB.exe	f_000031
Mar 30, 2022 12:58:44 AM	Threat Emulation	Prevent	Low	File System Emulation	Gen.SB.exe	f57ee2cc-1a44-498
Mar 30, 2022 12:58:39 AM	Threat Emulation	Prevent	Low	File System Emulation	Gen.SB.exe	f_000031
Mar 30, 2022 12:58:23 AM	Forensics	Prevent	High	File System Emulation	Gen.SB.dll	7e2b1bbffa7f05e7k
Mar 30, 2022 12:58:11 AM	Forensics	Prevent	High	File System Emulation	Gen.SB.dll	f_000035
Mar 30, 2022 12:58:00 AM	Forensics	Prevent	High	File System Emulation	Gen.SB.dll	f_000034
Mar 30, 2022 12:57:48 AM	Forensics	Prevent	High	File System Emulation	Gen.SB.dll	2826815873d90ad:
Mar 30, 2022 12:57:47 AM	Threat Emulation	Prevent	Low	File System Emulation	Gen.SB.dll	ed8c6b08-f914-42:
Mar 30, 2022 12:57:43 AM	Threat Emulation	Prevent	Low	File System Emulation	Gen.SB.dll	f_000035
Mar 30, 2022 12:57:38 AM	Threat Emulation	Prevent	Low	File System Emulation	Gen.SB.dll	f_000034
Mar 30, 2022 12:57:36 AM	Threat Emulation	Prevent	Low	File System Emulation	Gen.SB.dll	3d14a9c7-e1a7-44
Mar 30, 2022 12:56:02 AM	Forensics	Prevent	High	File Reputation	Gen.Rep.exe	25da7cc807578394
Mar 30, 2022 12:55:50 AM	Forensics	Prevent	High	File Reputation	Gen.Rep.exe	f_000033
Mar 30, 2022 12:55:38 AM	Forensics	Prevent	High	File Reputation	Gen.Rep.exe	f_000032
Mar 30, 2022 12:55:26 AM	Forensics	Prevent	High	File Reputation	Gen.Rep.exe	unconfirmed 9789!
Mar 30, 2022 12:55:22 AM	Threat Emulation	Prevent	Low	File Reputation	Gen.Rep.exe	Unconfirmed 2041
Mar 30, 2022 12:55:22 AM	Threat Emulation	Prevent	Low	File Reputation	Gen.Rep.exe	f_000033

Statistics

Sessions Timeline

Blade

- 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%
- URL Filtering 0.38%

Action

- Prevent 61.88%
- Detect 12.15%
- Allow 11.05%
- Extract 11.05%
- Inform User 3.31%
- Block 0.55%

Severity

- Low 38.64%
- Medium 20.45%

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

Protection Details

Severity: Low

Confidence Level: Low

Malware Action:

Protection Name: gen.win.trojan

Protection Type: Generic

Logsページ (2 / 2)

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

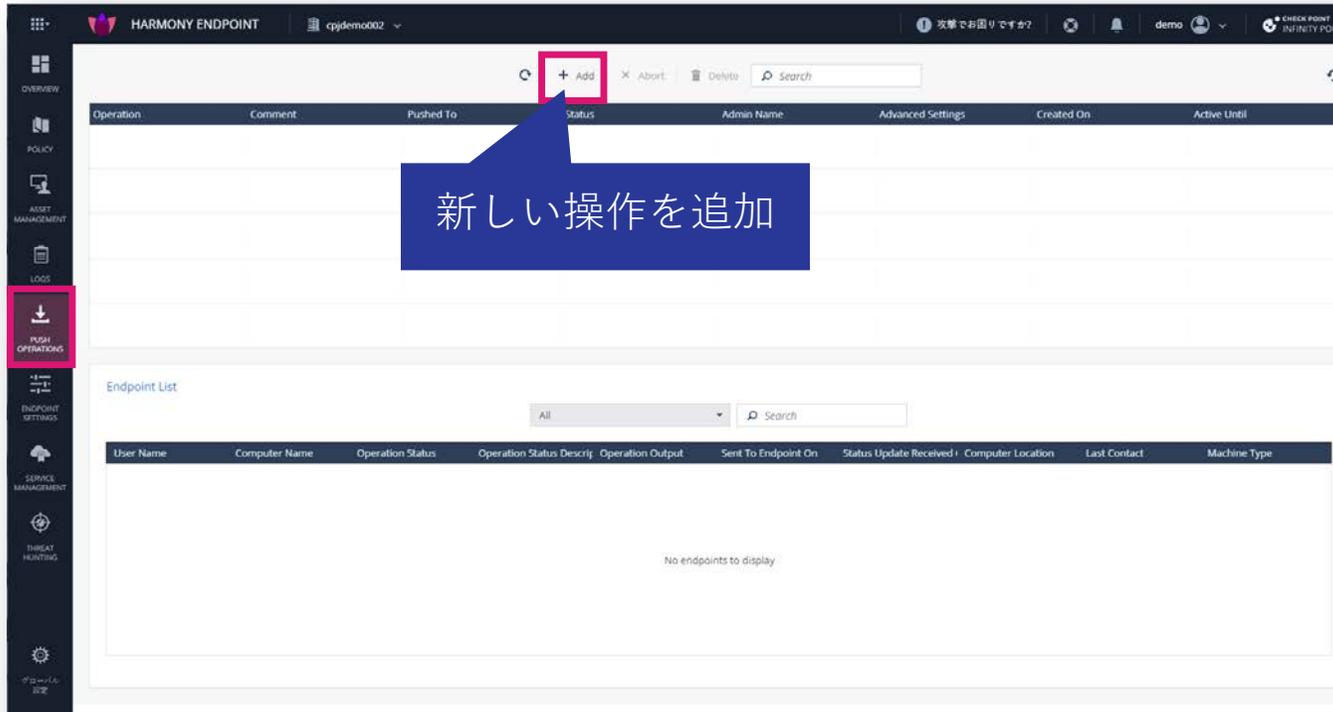
お気に入りへ登録可能

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

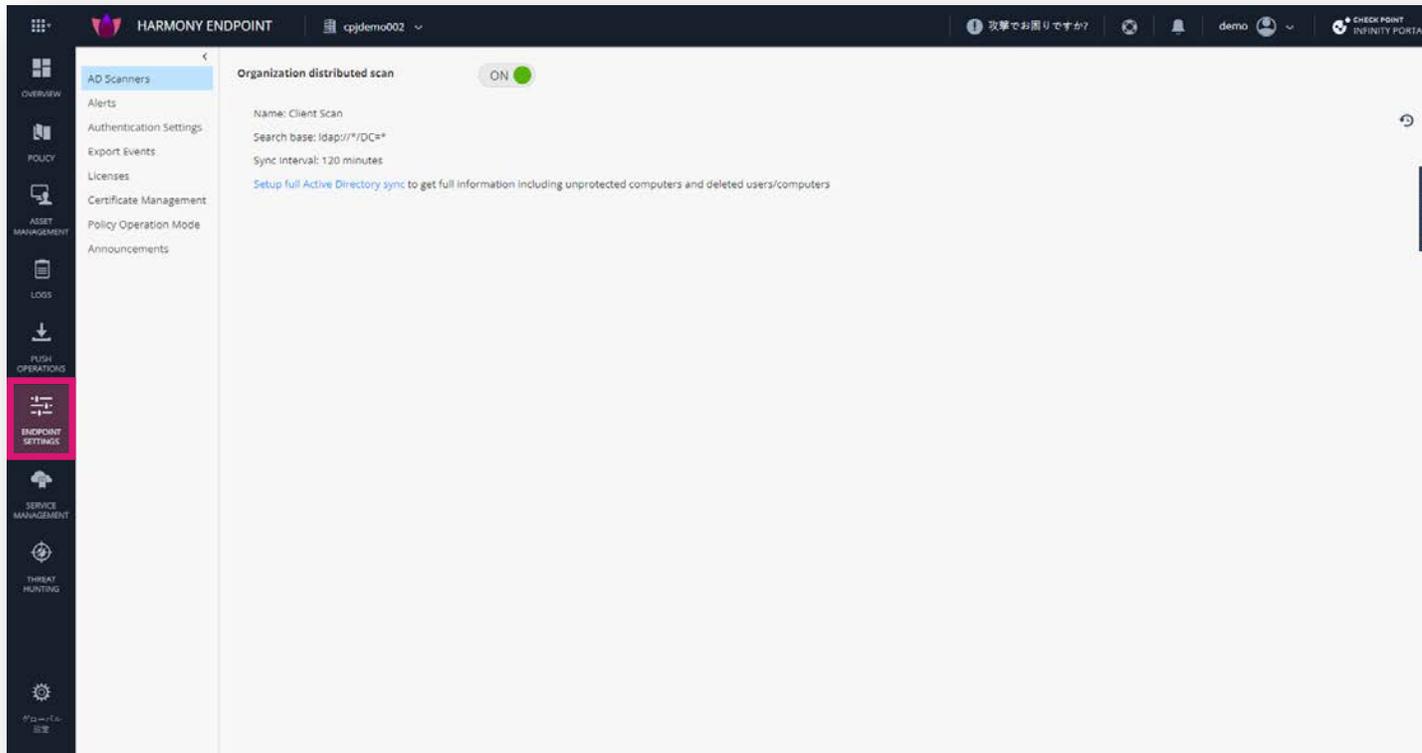
Push Operationsページ



リモートからコンピュータを操作します

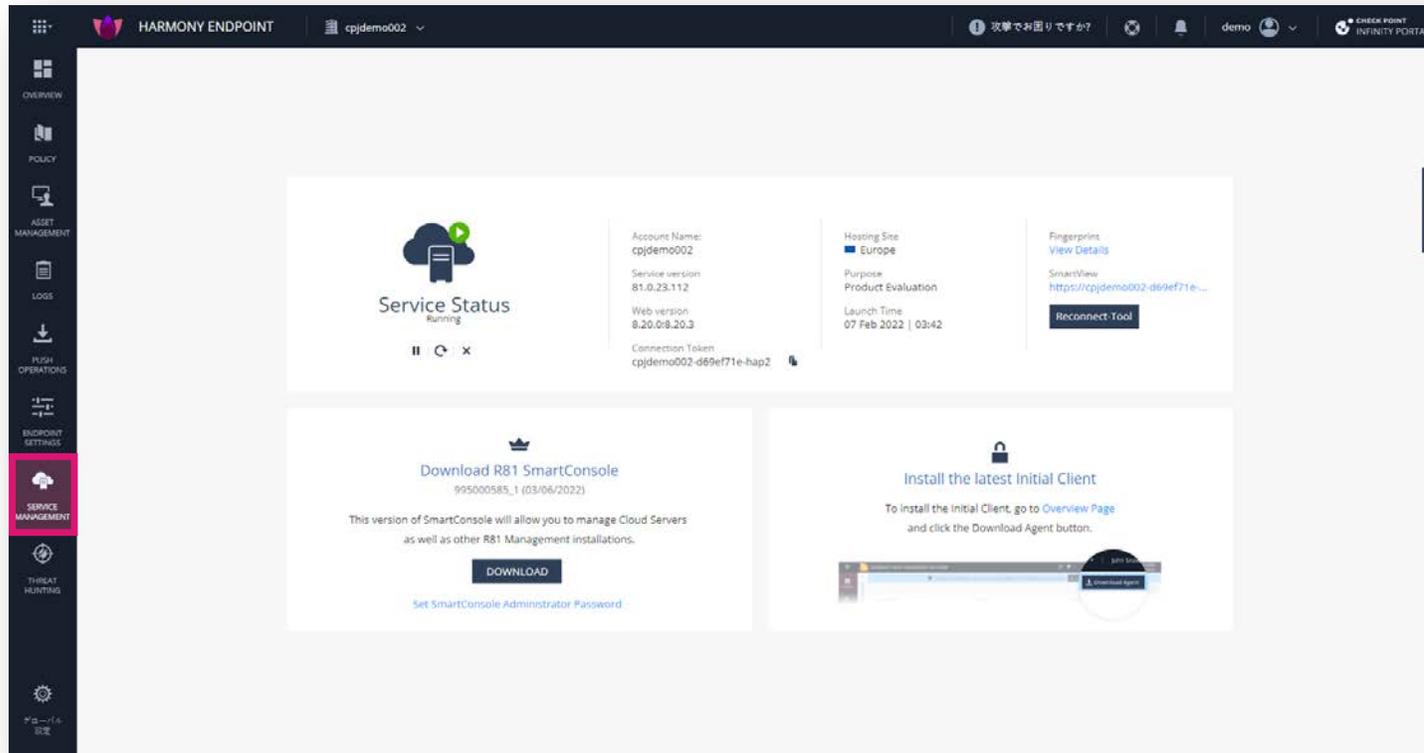
- マルウェア対策
 - スキャンの実行
 - シグネチャの更新
 - ファイルを隔離から復元
- フォレンジックと修復
 - IoC による分析
 - ファイル修復
 - コンピュータの隔離
 - コンピュータの解放
- エージェント設定
 - クライアントログの収集
 - クライアントソフトの修復
 - シャットダウン
 - 再起動
 - アプリケーションスキャン
 - プロセスの停止
 - リモートコマンド

Endpoint Settings ページ



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

Service Management ページ



サービス(管理機能)の管理を行います

- 一時停止
- 再起動
- 停止

Threat Hunting ページ

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

簡単操作によるカスタムクエリ

事前定義されたクエリ

The screenshot displays the Threat Hunting interface with several callouts:

- 攻撃の全体像を表示** (Show overall attack overview): Points to the dashboard metrics.
- ドリルダウンで一覧表示** (Drill down for list view): Points to the 'PR HUNT' button.
- 事前定義されたクエリ** (Predefined queries): Points to the 'Predefined Queries' sidebar.
- 各レコードの詳細表示** (Show details for each record): Points to the 'DETECTION EVENT INFORMATION' table.

Category	Count
Windows	4
MAC	1
Critical Hosts	2
Critical Hosts Attacks	37
Malicious Files	2
Process Events	37K
Malicious Processes	0
Active Attacks	0
File Events	48K
Network Events	43K
Malicious Traffic	1
Total Machines	5
Blocked Attacks	44
Dormant Attacks	11
Cleaned Attacks	0
Leads & Custom Alerts	0
Security Events	1

Trigger	Asset	Additional Information
Trigger: brwskit.jar Triggered By: External AV	User: nack Machine: ENDPOINTS	Name: explorer.exe Argv:
Trigger: sldjnlv.zip Triggered By: External AV	User: nack Machine: ENDPOINTS	Name: explorer.exe Argv:
Trigger: backdoor.mal.typhoon.a.vr Triggered By: External AV	User: nack Machine: ENDPOINTS	Name: explorer.exe State: 133 Time: 213
Trigger: mcar.com.zip Triggered By: External AV	User: nack Machine: ENDPOINTS	Name: explorer.exe State: 133 Time: 213
Trigger: f_00025d Triggered By: Endpoint File Reputation	User: nack Machine: AZUREWINDOWSSEK	Name: Not Found State: 032 Time: 914

Trigger	Asset	Process Details	Operation Time
Trigger: brwskit.jar Triggered By: External AV	User: nack Machine: ENDPOINTS	Name: explorer.exe Directory: c:\windows Full Path: c:\windows\explorer.exe Start Time: 2022-03-09T00:56:23 Argv: /	Date: 03/09/2022 Time: 21:33:00 PM

設定の流れ

設定の流れ

バーチャルグループの作成 (任意)



アンインストールパスワードの設定



アラート通知の設定



ポリシーの設定



インストールパッケージの作成

バーチャルグループによる管理

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

YOU DESERVE THE BEST SECURITY

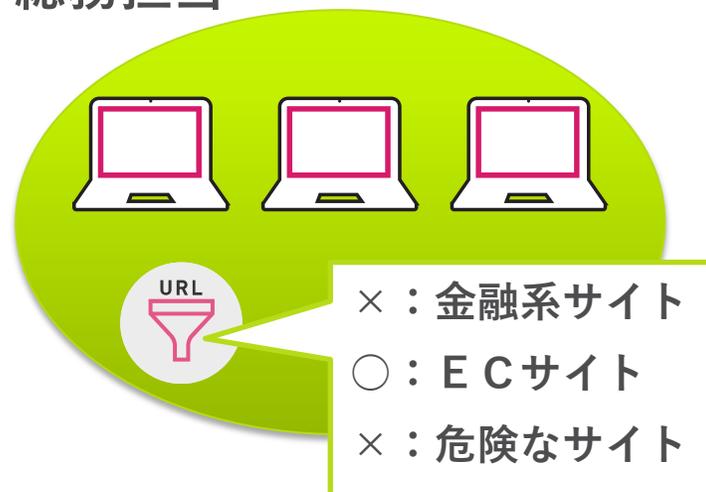
バーチャルグループの概要

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

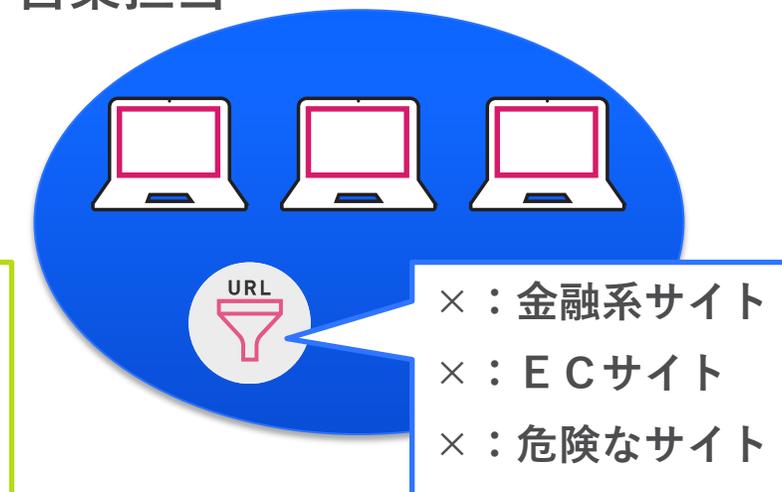
経営担当



総務担当



営業担当



バーチャルグループの作成（1 / 2）

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

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

The screenshot shows the Harmony Endpoint console interface. The left sidebar has 'ASSET MANAGEMENT' highlighted. The main area shows 'Computers' selected in the left pane, and a table of computer assets. The 'Computer Actions' dropdown menu is open, with 'Create Virtual Group' highlighted. A callout box shows the 'CREATE VIRTUAL GROUP' dialog with 'demo2' entered in the Name field.

Status	Computer Name	Endpoint Version	OS Build
<input type="checkbox"/>	ep	86.26.6008	10.0-17763-SP0.0-S
<input type="checkbox"/>	ep-demo2	86.50.0190	10.0-19043-SP0.0-S
<input type="checkbox"/>	ep-demo3	86.50.0190	10.0-19043-SP0.0-S

CREATE VIRTUAL GROUP

Name: demo2

Comment: Comment

CANCEL OK

バーチャルグループの作成 (2 / 2)

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

The screenshot displays the Harmony Endpoint console interface. On the left sidebar, the 'ASSET MANAGEMENT' section is highlighted, and 'Organizational Tree' is selected. The main area shows the 'Entire Organization' view with 'Virtual Groups' selected. The 'Actions' menu is open, and 'Create Virtual Group' is highlighted. A dialog box titled 'CREATE VIRTUAL GROUP' is open, showing the 'Name' field with 'demo2' and a 'Comment' field with 'Comment'. The 'OK' button is visible at the bottom right of the dialog.

バーチャルグループへのコンピュータの追加、削除（1 / 4）

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

バーチャルグループへのコンピュータの追加、削除（2 / 4）

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

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

The screenshot illustrates the steps to add a computer to a virtual group in the Harmony Endpoint console. The interface is divided into several sections:

- ASSET MANAGEMENT:** The sidebar menu is highlighted.
- Computers:** A table lists computers with columns for Status, Computer Name, and Endpoint Version. The first row (ep) is selected.
- Computer Actions:** A dropdown menu is open, showing options like 'Add to Virtual Group'.
- Select virtual Group:** A dialog box is open, showing a list of virtual groups to choose from.

Annotations in blue callouts indicate the following steps:

- ① コンピューターを選択 (Select computer)
- ② クリック (Click)
- ③ 選択 (Select)
- ④ バーチャルグループを選択 (Select virtual group)

Status	Computer Name	Endpoint Version
<input checked="" type="checkbox"/>	ep	86.26.6008
<input type="checkbox"/>	ep-demo2	86.50.0190
<input type="checkbox"/>	ep-demo3	86.50.0190

Computer Actions menu items:

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

Select virtual Group dialog box items:

- CP-demo
- All ChromeOs Desktops
- All ChromeOs Laptops
- All Desktops
- Eval
- Capsule Docs external users

バーチャルグループへのコンピュータの追加、削除（3 / 4）

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

Asset Management > Computers での追加、削除方法

① コンピューターを選択

② 所属するバーチャルグループを表示

③ バーチャルグループを追加、削除

④ バーチャルグループの横にマウスオーバーした際に表示される +、- をクリック

追加 + x 表示切替

削除 表示切替

Status	Computer Name	Endpoint Version	OS Build	Device Type	Deployment
✓	ep	86.26.6008	10.0-17763-SP0.0-SMP	Laptop	Completed
✓	ep-demo2	86.50.0190	10.0-19043-SP0.0-SMP	Laptop	Completed
✓		86.50.0190	10.0-19043-SP0.0-SMP	Laptop	Completed

1 of 3 selected

General | LDAP

Display Name: ep | SAM Name: ep

Description: - | CN: CN=EP,OU=Domain

Controllers,DC=harmon...

10.0 (17763)

Number of

+ x 表示切替

Pre-defined Virtual Groups

Search

Custom Virtual Group

- 20220629demo
- ✓ CP-demo
- DEMO0728

CANCEL OK

バーチャルグループへのコンピュータの追加、削除（4 / 4）

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

Asset Management > Organizational Tree での追加方法

① Virtual Group を選択

② コンピュータを追加、削除する Virtual Group を選択

② + をクリック

③ Other Users/Computers を選択

④ 追加するコンピュータを選択

バーチャルグループへのポリシーの適用（1 / 2）

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

① 複製元のポリシーを選択

② 「Clone」か、「Copy & Paste」をクリックして複製

「Clone」は、複製元のポリシーの真上か、真下に複製

「Copy & Paste」は、複製時に任意のポリシーを選択し、真上か、真下に複製

バーチャルグループへのポリシーの適用（2 / 2）

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

CLONE RULE

Name *

New Rule 1

ポリシーの名前を入力

Applied to ⓘ *

Search for entity...

Select from organization tree

適用対象を選択

Affected Devices (0)

Clone Configuration From

CANCEL OK

アンインストールパスワードの設定

アンインストールパスワードの設定

Policy > Client Settings > Install & Upgrade > Uninstall Settings

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

The screenshot displays the Check Point Harmony Endpoint management console. The left sidebar shows the navigation menu with 'POLICY' and 'Client Settings' highlighted. The main content area shows the 'CLIENT UNINSTALL PASSWORD SETTINGS' dialog box, which is open and contains the following fields and options:

- Password:** A text input field with a masked password (represented by dots).
- Confirm Password:** A text input field with a masked password (represented by dots).
- Change the password for all rules where the default password was not changed**

At the bottom of the dialog box are 'CANCEL' and 'OK' buttons. In the background, the 'INSTALLATION & UPGRADE' settings page is visible, showing various configuration options for client installations and upgrades, including a section for 'Uninstall settings' with an 'Agent Uninstall Password' field.

アラート通知設定

アラート通知設定（1 / 4）

Threat Hunting

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

アラート通知フロー



アラート通知設定（2 / 4）：アラート通知宛先設定

Threat Hunting

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

① メニューを開きます

② NOTIFICATIONS を選択します

③ テナントに登録されているユーザから、通知の送信先を選択します。

アラート通知設定（3 / 4）：アラート通知イベント設定

Threat Hunting

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

① Threat Hunting の条件を Bookmark に登録します

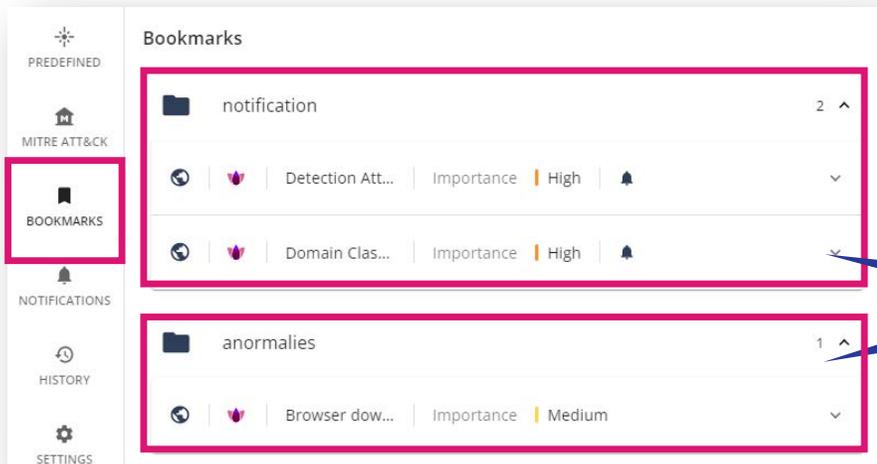
② 名前、重要度、タグを設定します

③ チェックボックスにチェックを入れます

アラート通知設定（3 / 4）：アラート通知イベント設定

Threat Hunting

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



Bookmark は、タグごとにまとまって表示されます

ポリシーの設定

ポリシーの設定

ポリシーの **SAVE** と **INSTALL**

ポリシーの Save と Install

Policy

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

Unsaved Rules 1

Install Policy

Unsaved Rules 1

- Save All Changes
- View Changes
- Discard Changes

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)
- Changed Rule Order and Assignments (2)

CANCEL INSTALL

Save

変更内容の確認、破棄が可能

変更内容を適用

変更内容を保存

ポリシーの設定

THREAT PREVENTION
共通

YOU DESERVE THE BEST SECURITY

Threat Prevention : 共通 (1 / 5)

Policy > Threat Prevention

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

Threat Prevention : 共通 (2 / 5)

Policy > Threat Prevention

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

The screenshot displays the Check Point Harmony Threat Prevention interface. The left sidebar shows the navigation menu with 'POLICY' selected. The main area is divided into several sections:

- ポリシー一覧 (Policy List):** A table listing policies with columns for #, Rule Name, Applied To, Web & Files, Behavioral, and Analysis. The table shows five rows: 0 (Exclusion), 1 (Eval), 2 (CP-demo), 3 (demo-point), and 4 (Default settings). A red arrow labeled 'ポリシー適用順' (Policy Application Order) points downwards from the top row.
- ポリシーの適用対象 (Policy Targets):** A callout box highlights the 'Applied To' column, showing targets like 'ep-demo2', 'ep-demo3', 'Eval', 'CP-demo', 'demo-point', and 'Entire Organization'.
- 脅威対策機能の状態 (Threat Prevention Function Status):** A callout box highlights the 'Web & Files', 'Behavioral', and 'Analysis' columns, showing various protection icons.
- ポリシーごとの詳細設定 (Policy Specific Settings):** A callout box highlights the right-hand panel showing detailed settings for the 'Exclusion' policy, including 'Policy Mode' (Custom), 'Exclusions' (29), and various protection modes like 'URL Filtering Mode' (Prevent), 'Download Protection' (Off), 'Credential Protection' (Prevent), and 'Password Reuse Protection' (Prevent).

Threat Prevention : 共通 (3 / 5)

Policy > Threat Prevention

The screenshot displays the 'CAPABILITIES & EXCLUSIONS' section of a security policy configuration. It includes a 'Policy Mode' dropdown set to 'Custom', three main protection categories: 'WEB & FILES PROTECTION', 'BEHAVIORAL PROTECTION', and 'ANALYSIS & REMEDIATION'. Below these, there are sections for 'Safe Search' (with 'Search Reputation' and 'Force Safe Search' both set to 'On') and 'Files Protection' (with 'Anti-Malware Mode' set to 'Prevent' and 'Files Threat Emulation Mode' set to 'On'). An 'Advanced Settings' button is located at the bottom. A 'Last Modified' timestamp is also visible.

例外設定を管理

Exclusions Center
Custom

事前定義された設定を選択

- Tuning
- Recommended
- Default
- Strict

脅威対策のカテゴリを選択

ポリシーのバージョンを表示

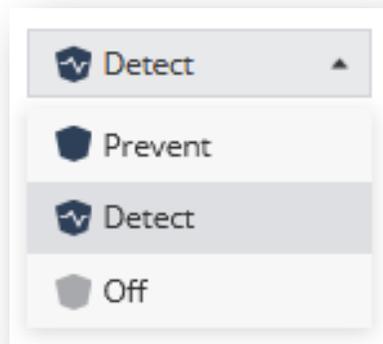
セキュリティ対策機能の動作モードを選択

セキュリティ対策機能の詳細を設定

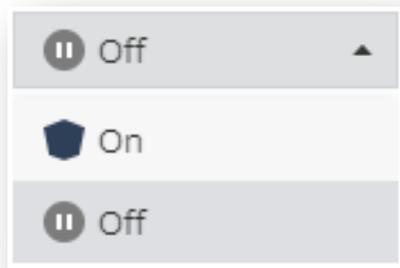
Threat Prevention : 共通 (4 / 5)

Policy > Threat Prevention

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



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

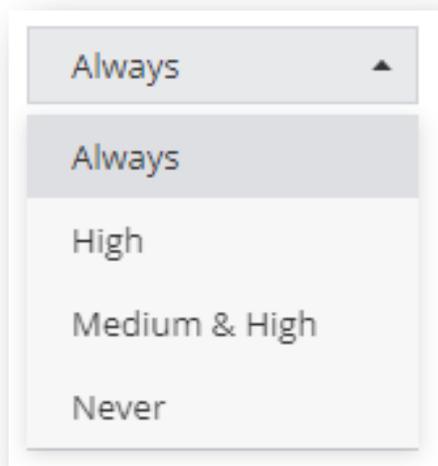


- 動作モードの選択肢②
 - On : 機能を有効化
 - Off : 機能を無効化

Threat Prevention : 共通 (5 / 5)

Policy > Threat Prevention

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



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

ポリシーの設定

THREAT PREVENTION
URL フィルタリング

YOU DESERVE THE BEST SECURITY

Threat Prevention : URL フィルタリング

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

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

The image shows a screenshot of the Check Point Threat Prevention configuration interface, specifically the URL Filtering settings. The interface is divided into several sections, with red boxes highlighting key areas and blue callout boxes providing Japanese annotations.

Annotations:

- 動作モードを選択** (Select operation mode): Points to the "URL Filtering Mode" dropdown menu, which is currently set to "Detect".
- 事前定義されたカテゴリ** (Predefined categories): Points to the "Categories" section, which lists various predefined categories like "Bandwidth Consumption", "General Use", "Legal Liability", "Productivity Lost", and "Security".
- ブラックリスト** (Blacklist): Points to the "Black list (0)" section, which allows for the registration of specific URLs to be blocked.
- Web サイトへのアクセスがブロックされた際に、エンドユーザの操作で警告を無視することを許可** (Allow user to dismiss the URL Filtering alert and...): Points to the checkbox "Allow user to dismiss the URL Filtering alert and...", which is checked.

Interface Elements:

- Left Panel:** "CAPABILITIES & EXCLUSIONS" section with "demo" and "EXCLUSIONS CENTER" tabs. It shows "Use Predefined Settings" (Default) and "Custom" options. The "WEB & FILES PROTECTION" tab is selected.
- URL Filtering Mode:** A dropdown menu with "Detect" selected.
- Download protection:** A dropdown menu with "Prevent" selected.
- Advanced Settings:** A button at the bottom of the left panel.
- Advanced Settings - WEB & FILES PROTECTION:** The main configuration area for URL Filtering.
- Categories:** A list of predefined categories with checkboxes and "Edit..." links. The "Security" category is checked.
- Black list (0):** A section for managing a blacklist of URLs.
- Right Panel:** A section for selecting categories, with "All (38)" and "Specific Categories (0)" options. A table lists various categories like "Alcohol & Tobacco", "Art / Culture", "Blogs / Personal Pages", "Business / Economy", "Computers / Internet", and "Education".

ポリシーの設定

THREAT PREVENTION DOWNLOAD 保護

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

YOU DESERVE THE BEST SECURITY

Threat Prevention : Download 保護 (1 / 2)

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

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

The screenshot shows the 'Download Protection' configuration page in Check Point Threat Prevention. The left sidebar has 'WEB & FILES PROTECTION' selected. The main content area is divided into 'Supported files', 'Unsupported files', 'Emulation Environments', and 'Override Default Files Actions'. Callouts provide detailed explanations for various settings:

- 無害化の有効化と、モードの選択**: Points to the 'Get extracted copy before emulation completes' section.
- 無害化を無効化し、Sandboxでの検査完了までダウンロードを保留**: Points to the 'Extract potential malicious elements' radio button.
- 無害化を無効化し、Sandboxでの検査完了前にダウンロードを許可**: Points to the 'Suspend download until emulation completes' radio button.
- Sandbox、無害化機能で未サポートのファイルのダウンロード可否**: Points to the 'Emulate original file without suspending access' radio button.
- Sandboxで検査するファイルサイズの上限**: Points to the 'Upload and emulate files under' dropdown set to 15 MB.
- エミュレーションが実行されるOSイメージを選択**: Points to the 'Image' selection area.
- ファイルタイプごとのデフォルトのアクションを上書き**: Points to the 'Override Default Files Actions' section.

Additional callouts include:

- 動作モードを選択**: Points to the 'Download Emulation & Extraction' dropdown menu set to 'Prevent'.
- Advanced Settings**: Points to the 'Advanced Settings' button at the bottom.

Threat Prevention : Download 保護 (2 / 2)

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

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

Elements To Extract

ADVANCED SETTINGS - WEB & FILES PROTECTION

< Back Elements To Extract

Search 16 items

Name	Risk	Description
Custom Properties	1 Very-Low	Custom document properties
✓ Fast Save Data	1 Very-Low	Stored data for fast document saving
✓ Macros and Code	5 Critical	Microsoft Office macros and PDF JavaScript code
Summary Properties	1 Very-Low	Summary document properties
✓ Linked Objects	4 High	
✓ Sensitive Hyperlinks	3 Medium	Links to network/local file paths
✓ PDF URI Actions	3 Medium	Open Uniform Resource Identifier (URI) resources
✓ Embedded Objects	4 High	Files and objects embedded in documents
✓ PDF Launch Actions	4 High	Launch external applications

Override Default Files Actions

ADVANCED SETTINGS - WEB & FILES PROTECTION

< Back Override Default Files Actions

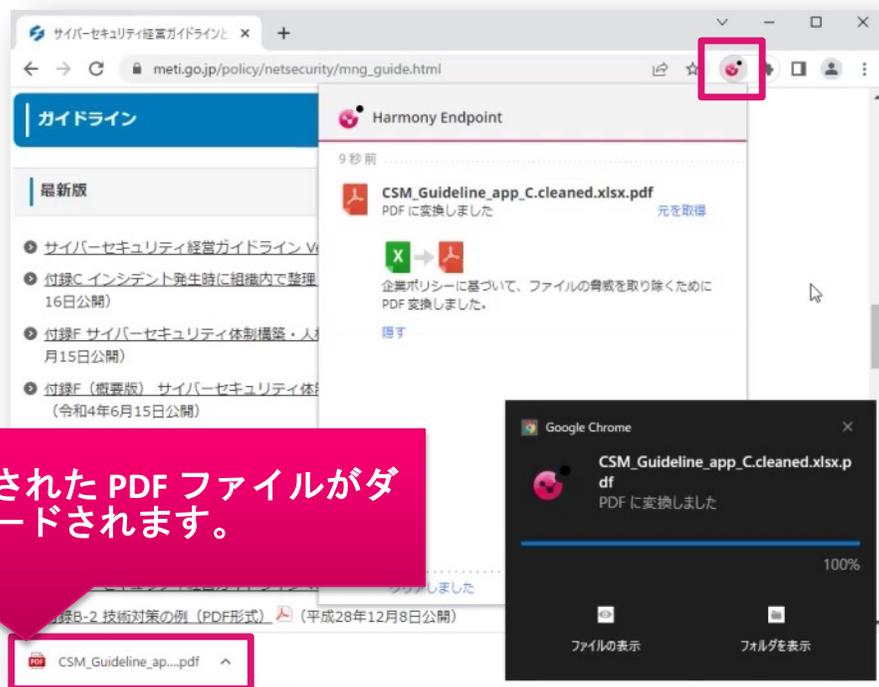
Search 81 items

File Extension	Description	File Action	Extraction Mode
PDF	Adobe acrobat document	Default (Emulate and Extrac	Irrelevant
DOC	Microsoft Word 97-2003 Document	Default (Emulate and Extrac	Irrelevant
DOCX	Microsoft Word Document	Default (Emulate and Extrac	Irrelevant
XLS	Microsoft Excel 97-2003 Worksheet	Default (Emulate and Extrac	Irrelevant
XLSX	Microsoft Excel Worksheet	Default (Emulate and Extrac	Irrelevant
PPT	Microsoft PowerPoint 97-2003 Present...	Default (Emulate and Extrac	Irrelevant
PPTX	Microsoft PowerPoint Presentation	Default (Emulate and Extrac	Irrelevant
EXE	Executable File	Default (Emulate)	Irrelevant
TAR	Tar Archive	Default (Emulate)	Irrelevant

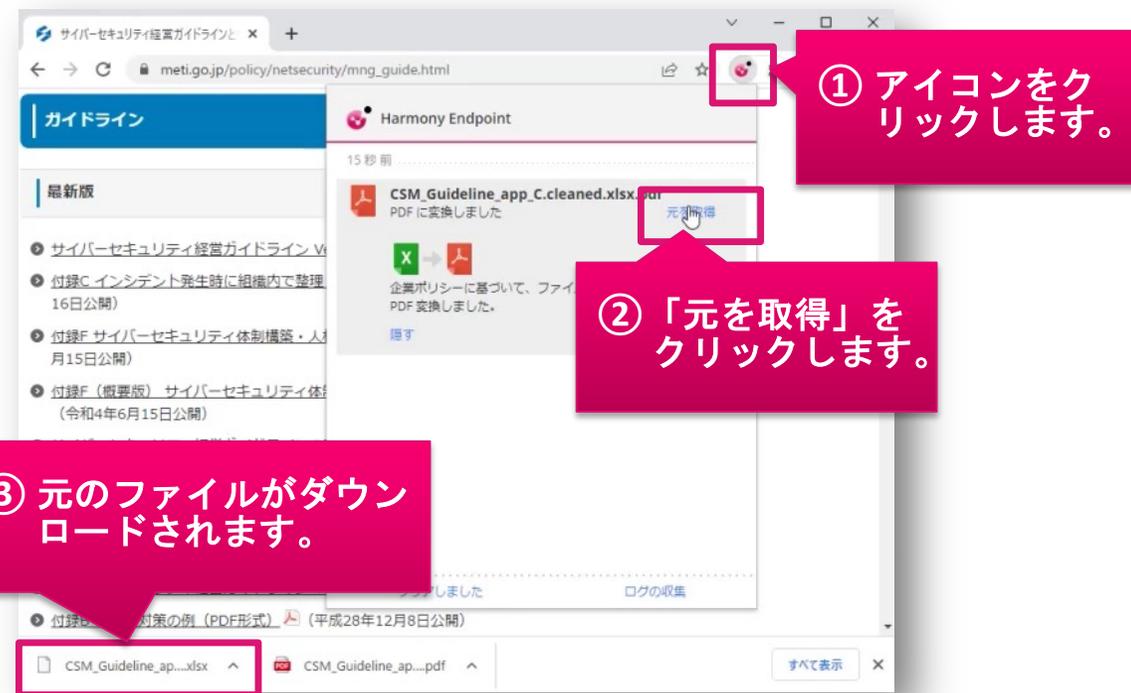
【参考】 サンドボックス & ファイル無害化の操作 (1 / 2)

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

ファイルの無害化

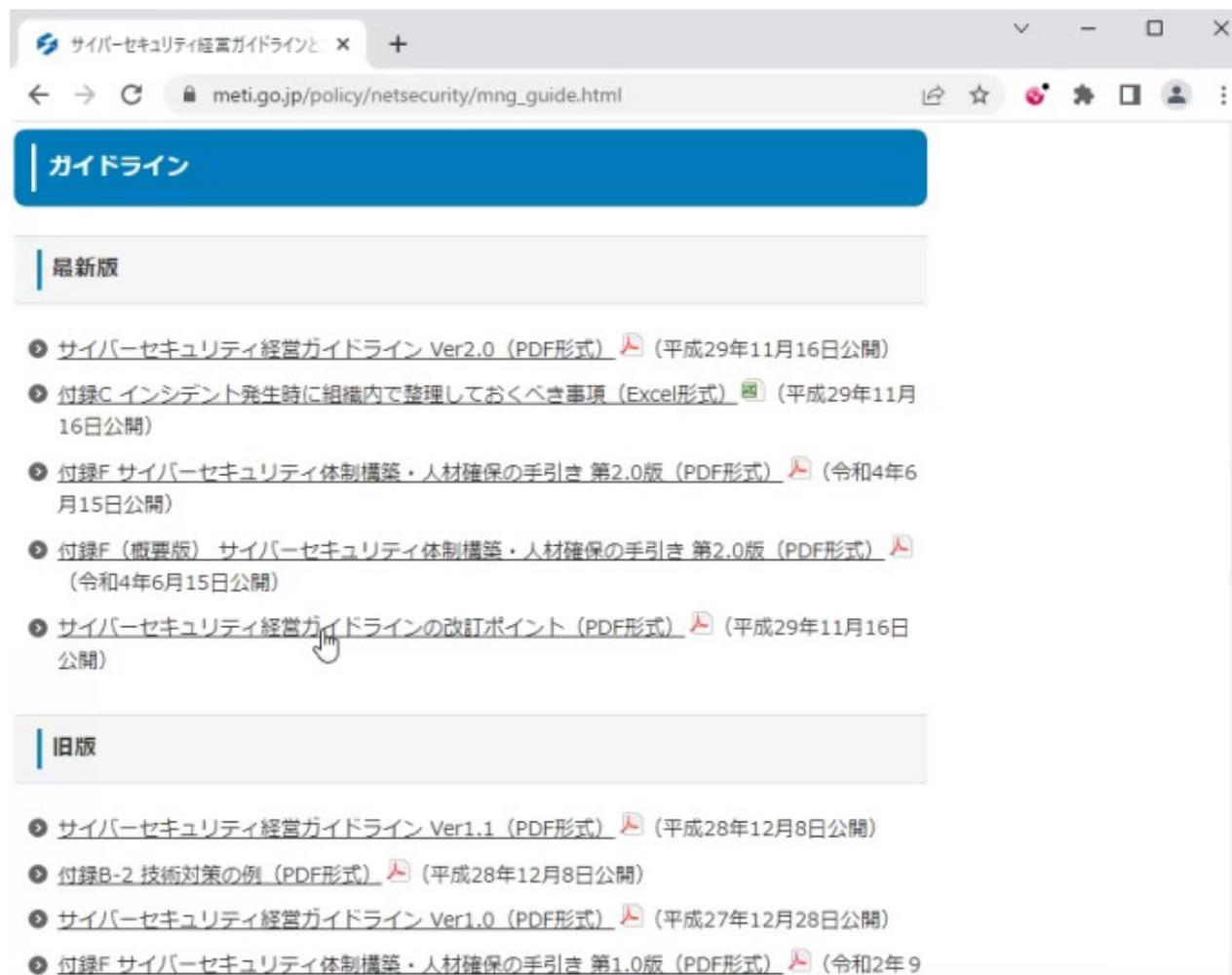


元のファイルのダウンロード



【参考】 サンドボックス&ファイル無害化の操作 (2 / 2)

サンドボックス&ファイル無害化の操作



The screenshot shows a web browser window with the URL `meti.go.jp/policy/netsecurity/mng_guide.html`. The page title is "サイバーセキュリティ経営ガイドライン" (Cybersecurity Management Guidelines). The main content is organized into sections: "ガイドライン" (Guidelines), "最新版" (Latest Version), and "旧版" (Old Version). Under "最新版", there are five items listed, each with a download icon and a date. A mouse cursor is pointing at the fifth item, "サイバーセキュリティ経営ガイドラインの改訂ポイント (PDF形式)".

ガイドライン

最新版

- サイバーセキュリティ経営ガイドライン Ver2.0 (PDF形式) (平成29年11月16日公開)
- 付録C インシデント発生時に組織内で整理しておくべき事項 (Excel形式) (平成29年11月16日公開)
- 付録F サイバーセキュリティ体制構築・人材確保の手引き 第2.0版 (PDF形式) (令和4年6月15日公開)
- 付録F (概要版) サイバーセキュリティ体制構築・人材確保の手引き 第2.0版 (PDF形式) (令和4年6月15日公開)
- サイバーセキュリティ経営ガイドラインの改訂ポイント (PDF形式) (平成29年11月16日公開)

旧版

- サイバーセキュリティ経営ガイドライン Ver1.1 (PDF形式) (平成28年12月8日公開)
- 付録B-2 技術対策の例 (PDF形式) (平成28年12月8日公開)
- サイバーセキュリティ経営ガイドライン Ver1.0 (PDF形式) (平成27年12月28日公開)
- 付録F サイバーセキュリティ体制構築・人材確保の手引き 第1.0版 (PDF形式) (令和2年9月)

ポリシーの設定

THREAT PREVENTION
認証情報の保護

YOU DESERVE THE BEST SECURITY

Threat Prevention : 認証情報の保護

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

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

CAPABILITIES & EXCLUSIONS

demo EXCLUSIONS CENTER

Use Predefined Settings Default

Custom

WEB & FILES PROTECTION BEHAVIOR PROTECTION **動作モードを選択**

Credential protection

Zero Phishing Prevent

Password reuse protection Detect & Alert

Safe Search

Force Safe Search Off

Advanced Settings

ADVANCED SETTINGS - WEB & FILES PROTECTION

URL Filtering

Download Protection

Credential Protection

Threat Emulation

Files Protection

General

Signature

Scan

Allow user to dismiss the phishing alert and access the website

Send log on each scanned site

Allow user to abort phishing scans

Password Reuse Protection (0) | Edit

パスワードの再利用保護を適用するドメインを企業ドメインとして追加

【参考】ゼロ・フィッシングの動作概要

正規のWebサイトへアクセスした際の動作概要

The screenshot shows the legitimate Resona Bank migration page. The browser address bar displays the URL `ib.resonabank.co.jp/IB/0102/SC_N_0102_010.aspx`. The page header includes the Resona Bank logo and the text "りそな銀行 マイグレート". Below the header, there is a security notice from "SaT Netizen" regarding virus protection software. The main content area features the Resona Bank logo and a login form with the instruction "ログインIDをご入力ください." (Please enter your login ID). The form includes a text input field for the login ID, a checkbox for "ソフトウェアキーボードを使用して入力する" (Use software keyboard for input), and a numeric keypad. A mouse cursor is positioned over the login ID input field.

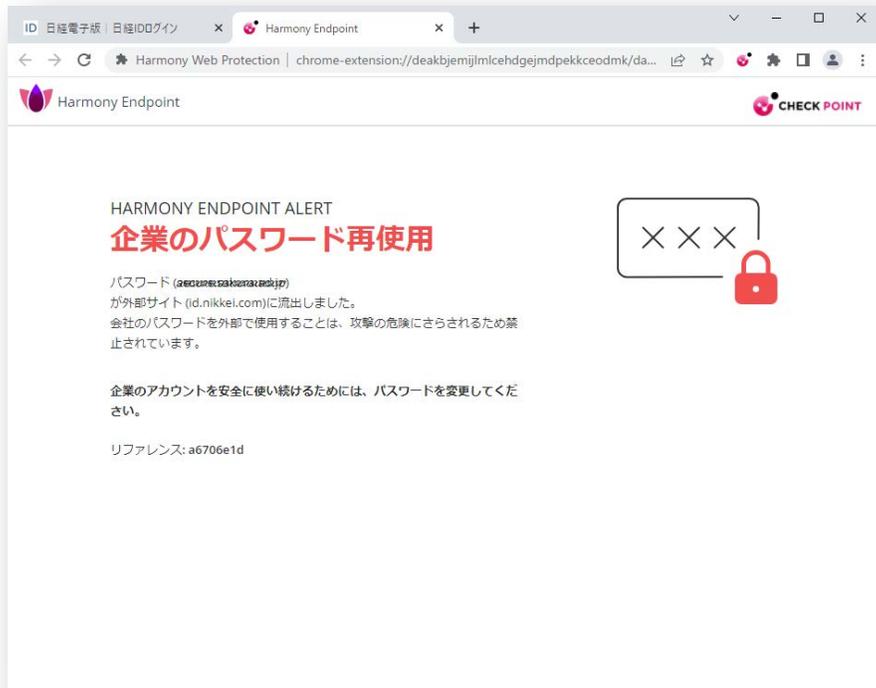
フィッシングサイトへアクセスした際の動作概要

The screenshot shows a demo zero-phishing site. The browser address bar displays the URL `salesforce.sbm-demo.xyz/zero-phishing`. The page header features a yellow banner with the text "Demo Zero-Phishing Site!" and "NON-PRODUCTION ENVIRONMENT AND FOR DEMO PURPOSES ONLY". The main content area displays the Salesforce logo. Below the logo, there is a login form with the instruction "Username" and "Password" labels. The form includes two text input fields for the username and password, a blue "Log In" button, a "Remember me" checkbox, and a "Forgot Your Password?" link. A mouse cursor is positioned over the password input field.

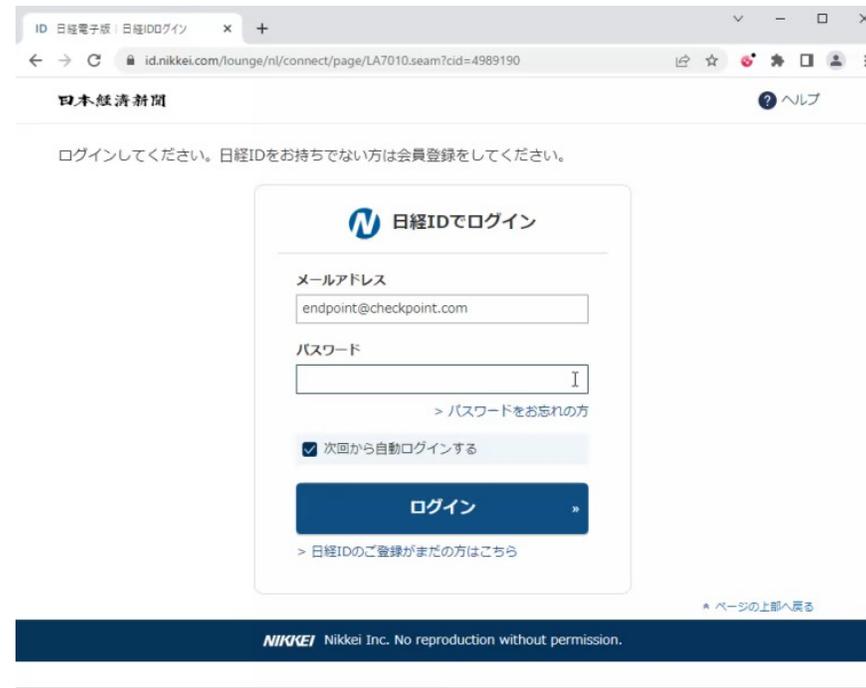
【参考】企業パスワード保護機能の動作概要

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

企業パスワード保護の警告画面の例



企業パスワード保護の動作概要



ポリシーの設定

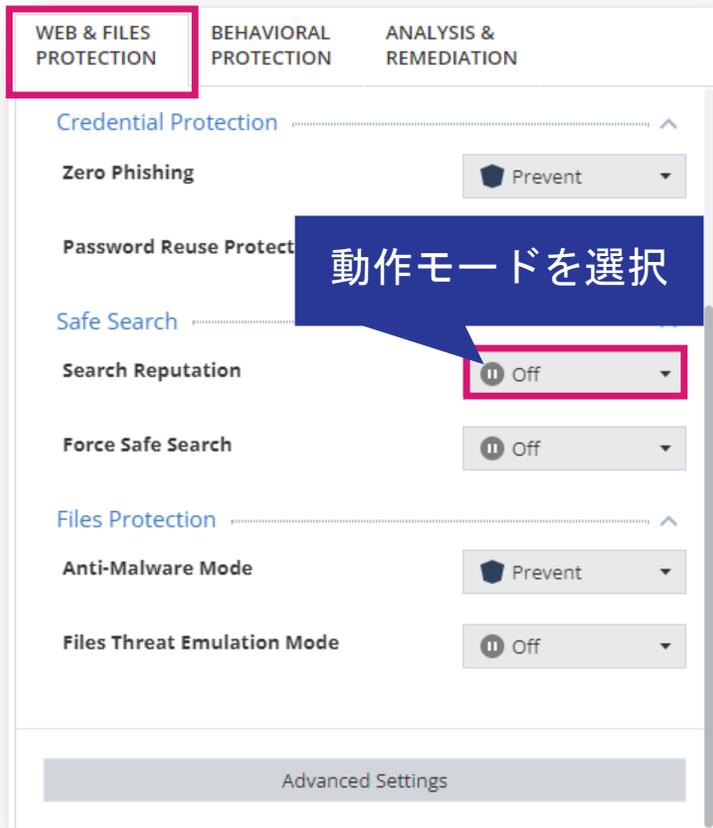
THREAT PREVENTION
安全な検索

YOU DESERVE THE BEST SECURITY

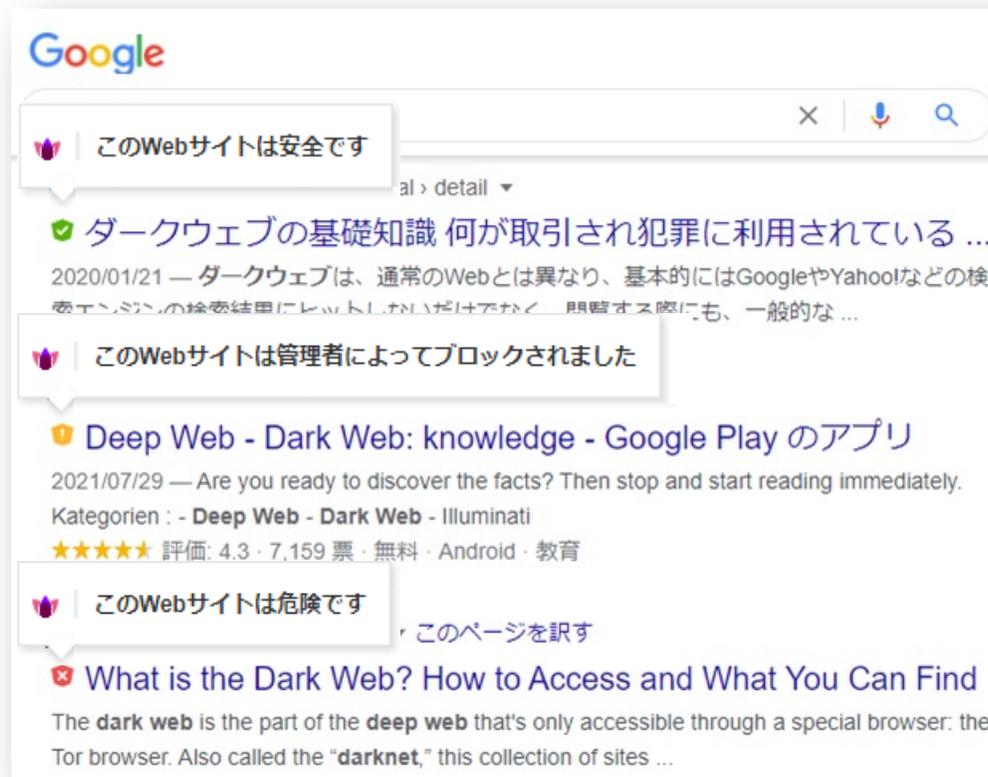
Threat Prevention : サーチ・レピュテーション

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

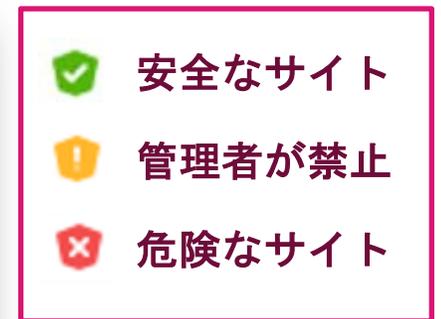
- Google 検索エンジンでの検索結果をURL のレピュテーションに基づいて分類します。
- この機能を有効にするには、[URL フィルタリング モード] を [Prevent] または [Detect] に設定してください。



検索結果例



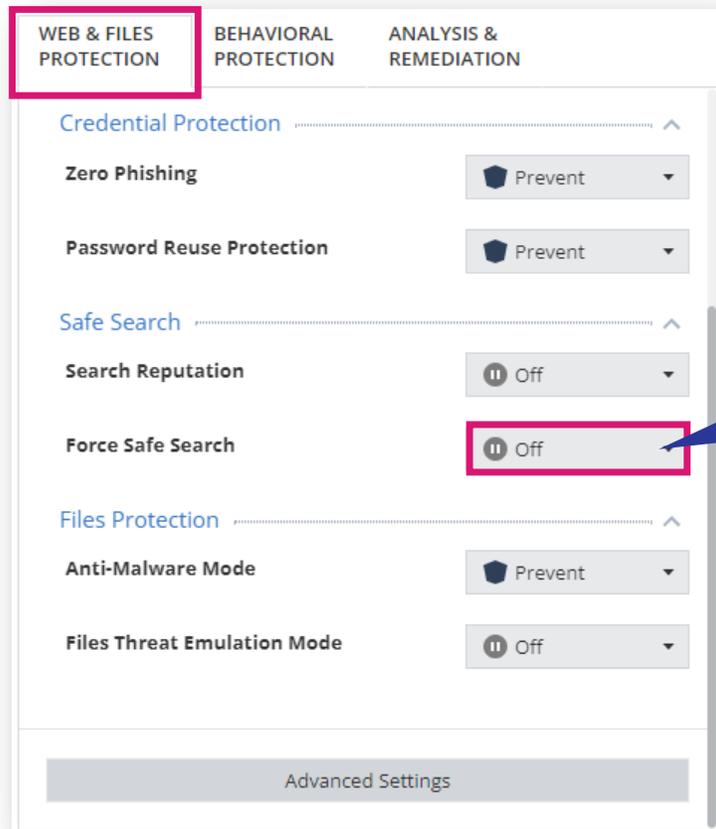
凡例



Threat Prevention : セーフ・サーチ

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

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



動作モードを選択

ポリシーの設定

THREAT PREVENTION
ファイル保護

YOU DESERVE THE BEST SECURITY

Threat Prevention ファイル保護 (1 / 4)

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

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

demo EXCLUSIONS CENTER

Default

Use Predefined Settings

Custom

WEB & FILES PROTECTION BEHAVIORAL PROTECTION

Files Protection

Anti-Malware Mode Prevent

Files Threat Emulation Mode On

Advanced Settings

ファイル拡張子ごとの動作を選択

ADVANCED SETTINGS - WEB & FILES PROTECTION

Back Override Default Files Actions 81 items

Search

File Extension	Description	File Action
PDF	Adobe acrobat document	Default (Emulate)
DOC	Microsoft Word 97-2003 Document	Default (Emulate)
DOCX	Microsoft Word Document	Default (Emulate)
XLS	Microsoft Excel 97-2003 Worksheet	Default (Emulate)
XLSX	Microsoft Excel Worksheet	Default (Emulate)
PPT	Microsoft PowerPoint 97-2003 Presentation	Default (Emulate)
PPTX	Microsoft PowerPoint Presentation	Default (Emulate)
EXE	Executable File	Default (Emulate)
TAR	Tar Archive	Default (Emulate)

ADVANCED SETTINGS - WEB & FILES PROTECTION

URL Filtering

Download Protection

Credential Protection

Threat Emulation

Files Protection

Override Default Files: 0 Overrides Edit

CANCEL OK

Threat Prevention ファイル保護 (2 / 4)

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

ADVANCED SETTINGS - WEB & FILES PROTECTION

- URL Filtering
- Download Protection
- Credential Protection
- Threat Emulation
- Files Protection
 - General**
 - Signature
 - Scan

Malware Treatment

- Quarantine file if cure failed
- Delete file if cure failed

Riskware Treatment

- Treat as malware
- Skip file

Threat Cloud Knowledge Sharing

- Allow sending infection info and statistics to Check Point servers for analysis
- Allow sending infected file samples to Check Point servers for analysis

Scan On Access

- Detect unusual activity
- Enable reputation service for files, web resources & processes
 - Connection timeout: 600 ms
- Enable web protection

Mail Protection

- Scan mail messages

Callout Texts:

- Anti-Malware で修復に失敗したファイルへの動作を選択
- リスクウェア（危険な可能性のある合法的なソフトウェア）の取り扱い方法を選択
- Threat Cloud への情報共有の可否を選択
- 異常な挙動の監視を有効化するかを選択。信頼できるプロセスは監視しない
- クラウドを使用したファイル、Web リソース、プロセスのレピュテーションの有効化を選択。PCの再起動後に有効
- 疑わしい Web サイトへのアクセスと悪意のあるスクリプトの実行防止を有効化するかを選択
- 電子メールがファイルとして保存される時に、電子メールの検査を有効化するかを選択

Threat Prevention ファイル保護 (3 / 4)

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

Frequency

Update signatures every 4 hours

Signature update will fail after 60 seconds without server response

Signature Sources

First Priority: External Check Point Signature Server

Second Priority: N/A

Third Priority: N/A

Shared Signature Server

Set as shared signatures server

signature server path

シグネチャの更新間隔とタイムアウト時間

シグネチャの配信元

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

Threat Prevention ファイル保護 (4 / 4)

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

ADVANCED SETTINGS - WEB & FILES PROTECTION

- URL Filtering
- Download Protection
- Credential Protection
- Threat Emulation
- Files Protection
 - General
 - Signature
 - Scan

Perform Periodic Scan

Scan Periodic: Every Month
Day of week: Sunday
Day of month: 1
 Randomize scan time
Start scan: 12:00
End scan: 12:00
Scan start hour: 12:00

Run initial scan after anti-malware blades installation
 Allow user to cancel scan
 Prohibit cancel scan if more than 30 Days passed since last successful scan

Scan Targets

Critical areas Removable drives
 Optical drivers Unrecognized devices
 Local drives Network drives
 Mail messages

Scan Target Exclusions

Skip archives and non executables
 Do not scan files larger than 20 MB

定期スキャンの設定

定期的なスキャン実行の設定

スキャン対象の選択 (定期スキャンのみ)

スキャン対象の除外設定 (定期スキャンのみ)

ポリシーの設定

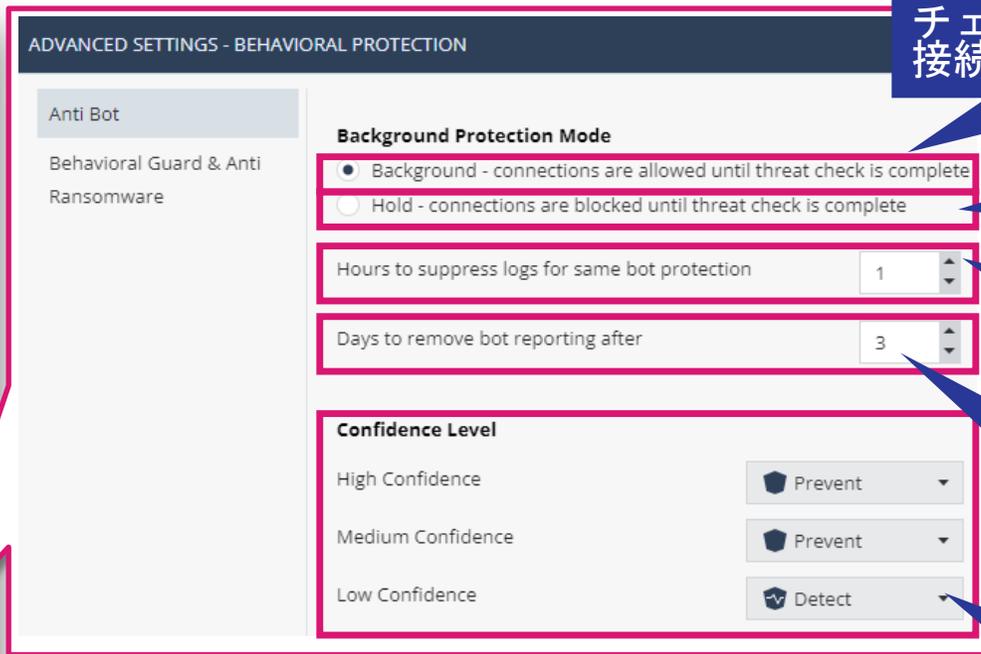
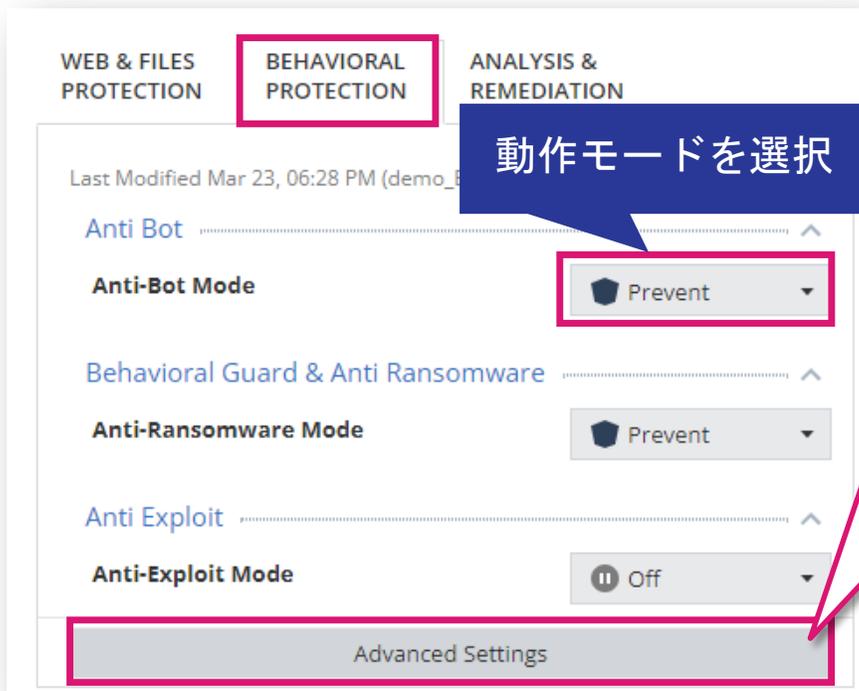
THREAT PREVENTION ANTI-BOT

YOU DESERVE THE BEST SECURITY

Threat Prevention : Anti-Bot

Policy > Threat Prevention > Behavioral Protection > Anti Bot

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



チェックが完了する前に、接続を許可 (デフォルト)

チェックが完了するまで、接続をブロック

同じボットのアクションをログに記録する間隔※

選択した日数が経過してもボットがC&Cサーバに接続しない時、感染報告を停止

ボット検出の確実性 (高/中/低) ごとのアクションを選択

※ デフォルトは、1時間。変更する場合は、時間数を選択

ポリシーの設定

**THREAT PREVENTION
BEHAVIORAL GUARD & ANTI-RANSOMWARE**

YOU DESERVE THE BEST SECURITY

Threat Prevention : Behavioral Guard & Anti Ransomware

Policy > Threat Prevention > Behavioral Protection > Behavioral Guard & Anti Ransomware

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

動作モードを選択

共有フォルダの保護の有効化

自動復旧でファイルをリストアする場所を指定

バックアップ領域のサイズと、バックアップの間隔※

ランサムウェア対策でバックアップファイルの種類とサイズ上限を指定

フォレンジックに使用するデータベースサイズ

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

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

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

※ バックアップ対象ファイルのサイズ上限の初期値は、25MBです

【参考】Anti-Ransomware の動作概要



ポリシーの設定

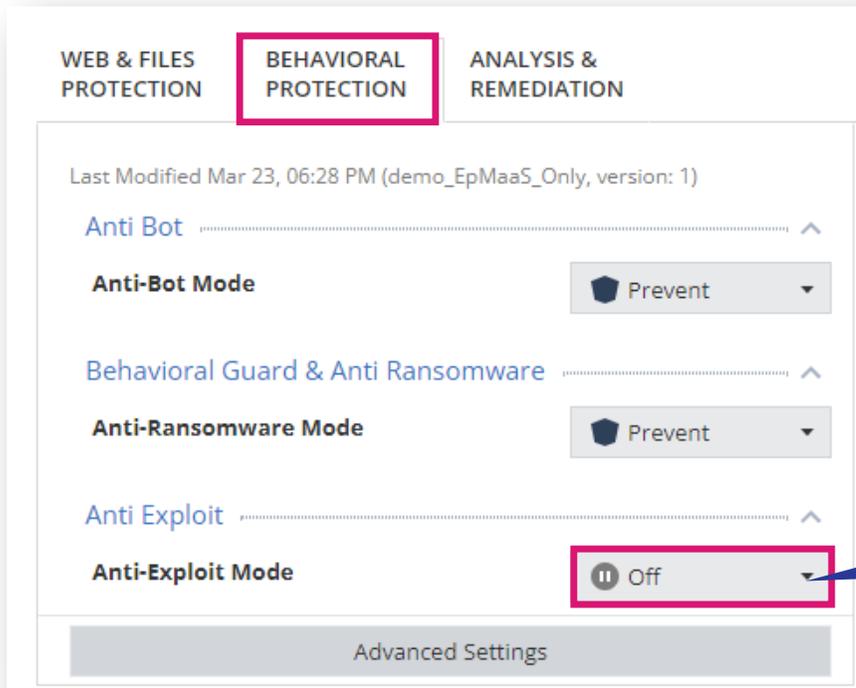
THREAT PREVENTION
ANTI-EXPLOIT

YOU DESERVE THE BEST SECURITY

Threat Prevention : Anti Exploit

Policy > Threat Prevention > Behavioral Protection > Anti Exploit

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



動作モードを選択

ポリシーの設定

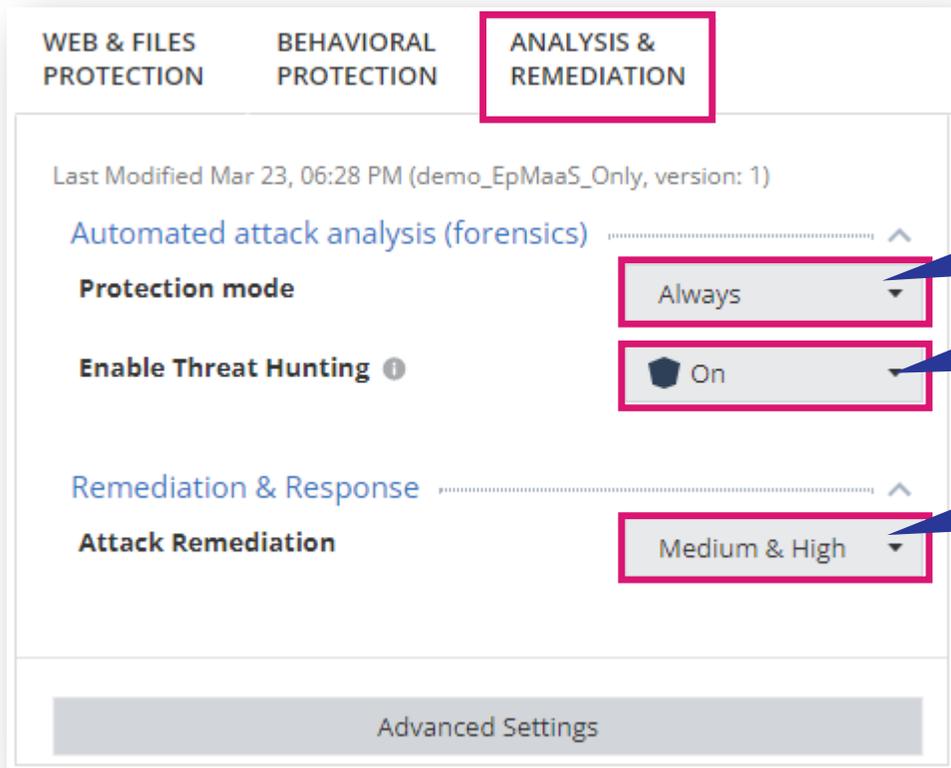
**THREAT PREVENTION
FORENSICS & REMEDIATION**

YOU DESERVE THE BEST SECURITY

Threat Prevention : Analysis & Remediation (1 / 2)

Policy > Threat Prevention > Analysis & Remediation

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



インシデントを分析するコンフィデンスレベル

Threat Huntingの有効/無効を選択

修復を実行するコンフィデンスレベル

Threat Prevention : Analysis & Remediation (2 / 2)

Policy > Threat Prevention > Analysis & Remediation

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

ADVANCED SETTINGS - ANALYSIS & REMEDIATION

File Quarantine

File Quarantine Medium & High

Allow users to delete items from quarantine

Allow users to restore items from quarantine

Copy quarantine files to central location

Choose location

e.g. c:\Endpoint\default

Quarantine folder name

%ProgramData%\CheckPoint\Endpoint Security\Remediation\Quarantine

File Remediation

Malicious Files	Quarantine
Suspicious Files	Quarantine
Unknown Files	Quarantine
Trusted Files	Ignore

ファイルを隔離する際のコンフィデンスレベルを選択

隔離されたファイルの削除、復元をユーザに許可するか選択

隔離されたファイルのコピーの保存場所を指定

隔離フォルダの場所を指定

ファイルのカテゴリごとに動作を指定

ポリシーの設定

CLIENT SETTINGS
USER INTERFACE

Client Settings : User Interface

Policy > Client Settings > User Interface

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

USER INTERFACE LOGS INSTALLATION & UPGRADE GENERAL

Default Client User Interface

Display client icon

Allow view logs locally

Notification level

Critical Only When affect user experience All

Pre-Boot Images

Pre-boot background image (800x600px)

Upload Check Point Default

Pre-boot background image high resolution (3840x2160)

Upload Check Point Default

USER INTERFACE LOGS INSTALLATION & UPGRADE GENERAL

URL Filtering View Preview

Title

Blocked access to a website

Description

Access to this website is not allowed by your organization policy. For your protection, this site has been blocked.

Zero Phishing View Preview

Title

Blocked access to a deceptive website

Description

ポリシーの設定

CLIENT SETTINGS
LOGS

Client Settings : Logs

Policy > Client Settings > Logs

- ログのアップロードに関する設定を構成します

USER INTERFACE | LOGS | INSTALLATION & UPGRADE | GENERAL

Allow Logs Upload to Policy Servers

Enable log upload

Log upload interval ① 3 min(s)

Minimum number of events before attempting an upload ① 1

Maximum number of events to upload ① 100

Maximum age event before upload ① 5 day(s)

Discard event if older then ① 90 day(s)

ログのアップロードの有効化、ログのアップロード間隔などを指定

指定した日数以前にログに記録されたイベントのみアップロードする

指定した日数以前にログに記録されたイベントはアップロードしない

ポリシーの設定

CLIENT SETTINGS INSTALLATION & UPGRADE

Client Settings : Installation & Upgrade

Policy > Client Settings > Installation & Upgrade

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

USER INTERFACE LOGS **INSTALLATION & UPGRADE** GENERAL

Default Installations and Upgrades

Enable the user to postpone the client installation or upgrade

Default reminder interval: 30 min(s)

Force installation and automatically restart after: 48 hour(s)

Maximum delay in download of packages: 4 hour(s)

Uninstall settings

Agent Uninstall Password

Deployment from Local Paths and URLs

Allow to install software deployment packages from local folders or URLs

Enable deployment from servers when no MSI was found in local paths

ユーザによるインストールやアップグレードの延期の許可と設定を構成

クライアントのアンインストールパスワードの設定

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

ポリシーの設定

CLIENT SETTINGS GENERAL

Client Settings : General

Policy > Client Settings > General

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

USER INTERFACE LOGS INSTALLATION & UPGRADE **GENERAL**

Sharing Data with Check Point

- Enable anonymized telemetry
 - Anonymized forensics reports
 - Files related to detection
 - Memory dumps related to detections

Connection Awareness

Consider Endpoint as Connected if Endpoint is:

- Connected to management
- Connected to a list of specified targets

HTTP +

チェックポイントとの情報共有設定を構成

コンピュータの接続状態を判断する方法を構成

サーバ最適化

サーバ最適化とは

サーバ最適化とは

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

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

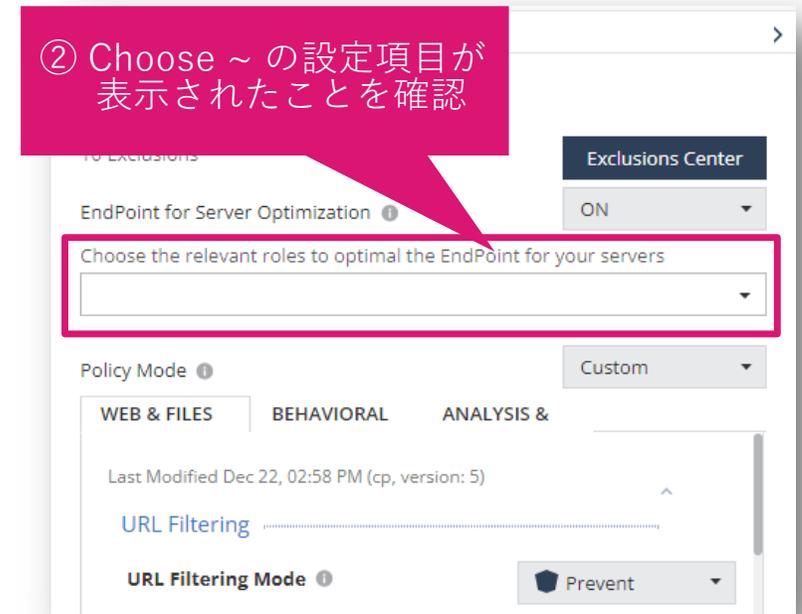
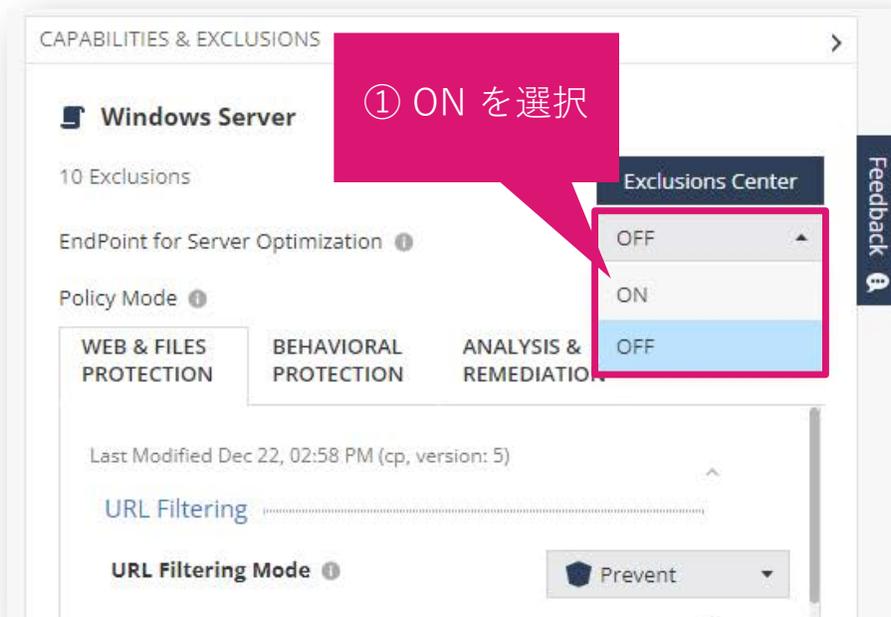
サーバ最適化設定

設定シナリオ

1. サーバ最適化を設定する Windows サーバの役割ごとに、バーチャルグループを作成します
 - 簡易設定ガイドの「バーチャルグループによる管理」を参照してください
2. 作成したバーチャルグループを指定したインストールパッケージを作成します
 - 簡易導入ガイドの「インストールパッケージの作成とダウンロード」を参照してください
3. 作成したバーチャルグループに適用する Policy ルールを作成します
 - 簡易設定ガイドの「バーチャルグループによる管理」を参照してください
4. Policy ルールで「サーバ最適化」を有効化します
5. Windows サーバに、クライアントソフトウェアをインストールします

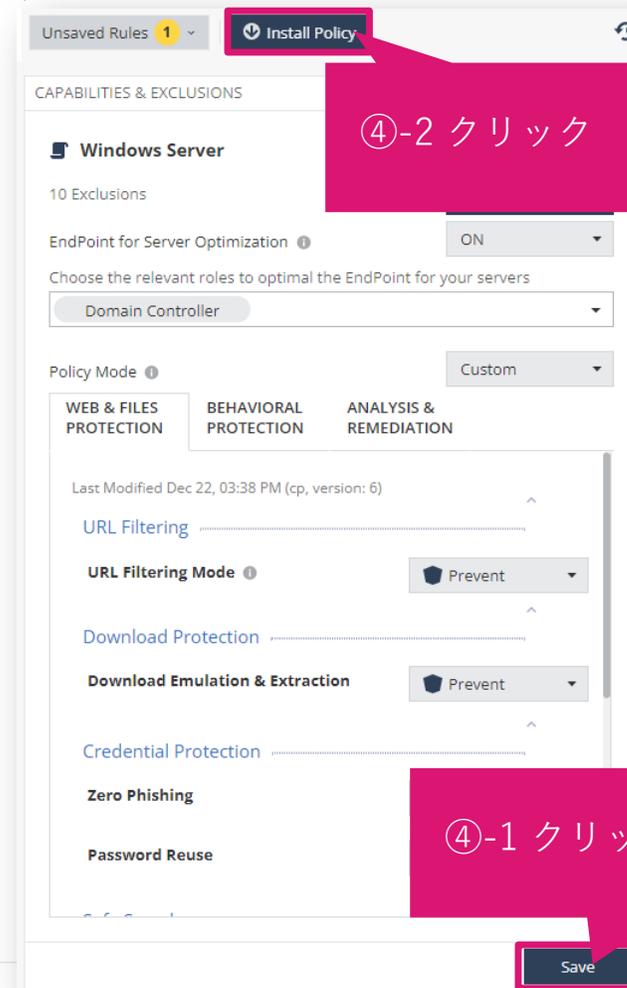
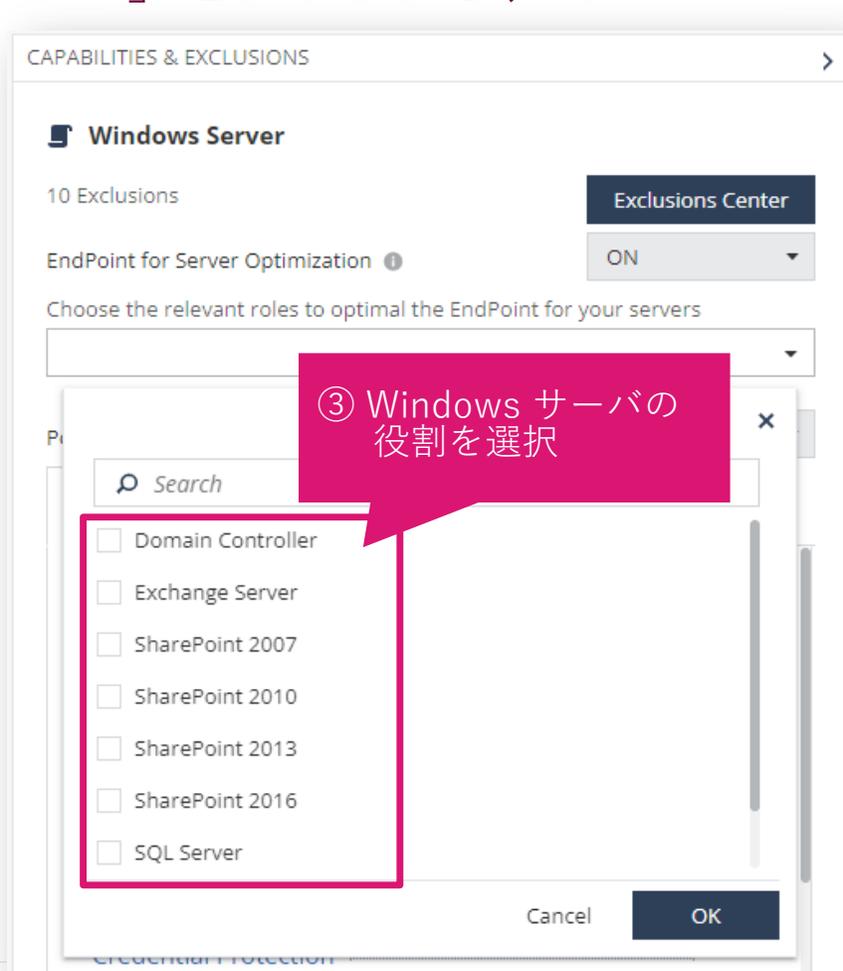
サーバ最適化設定（1 / 3）

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



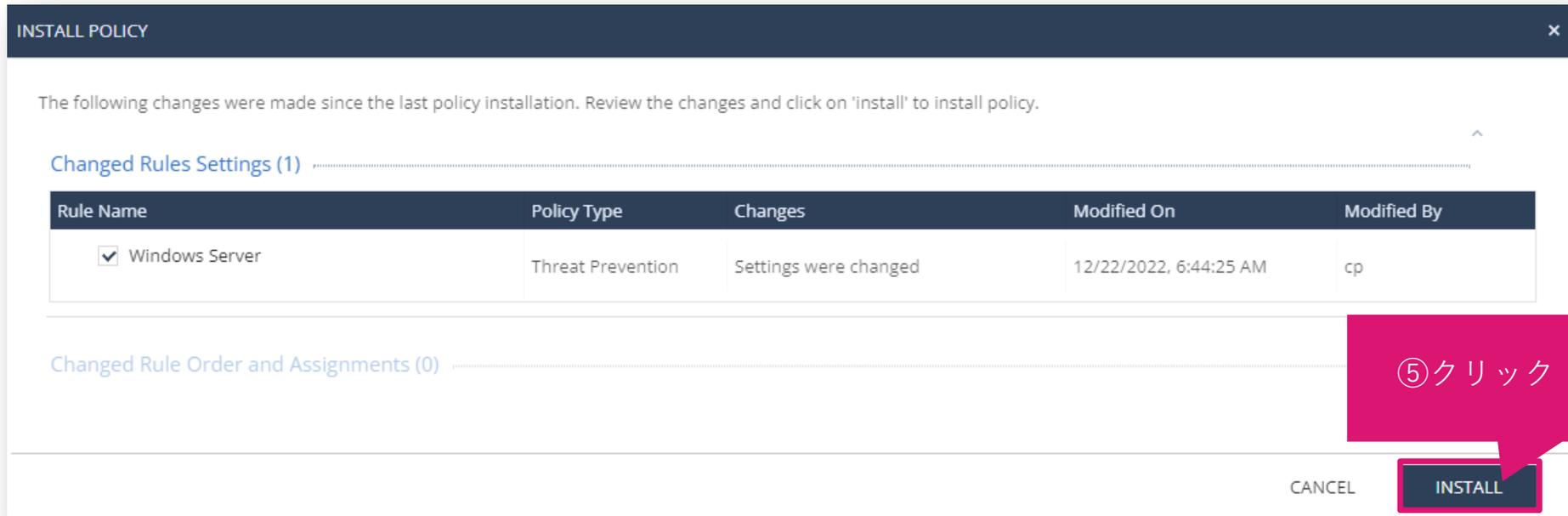
サーバ最適化設定（2 / 3）

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



サーバ最適化設定（3 / 3）

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





THANK YOU

YOU DESERVE THE BEST SECURITY