



# 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。

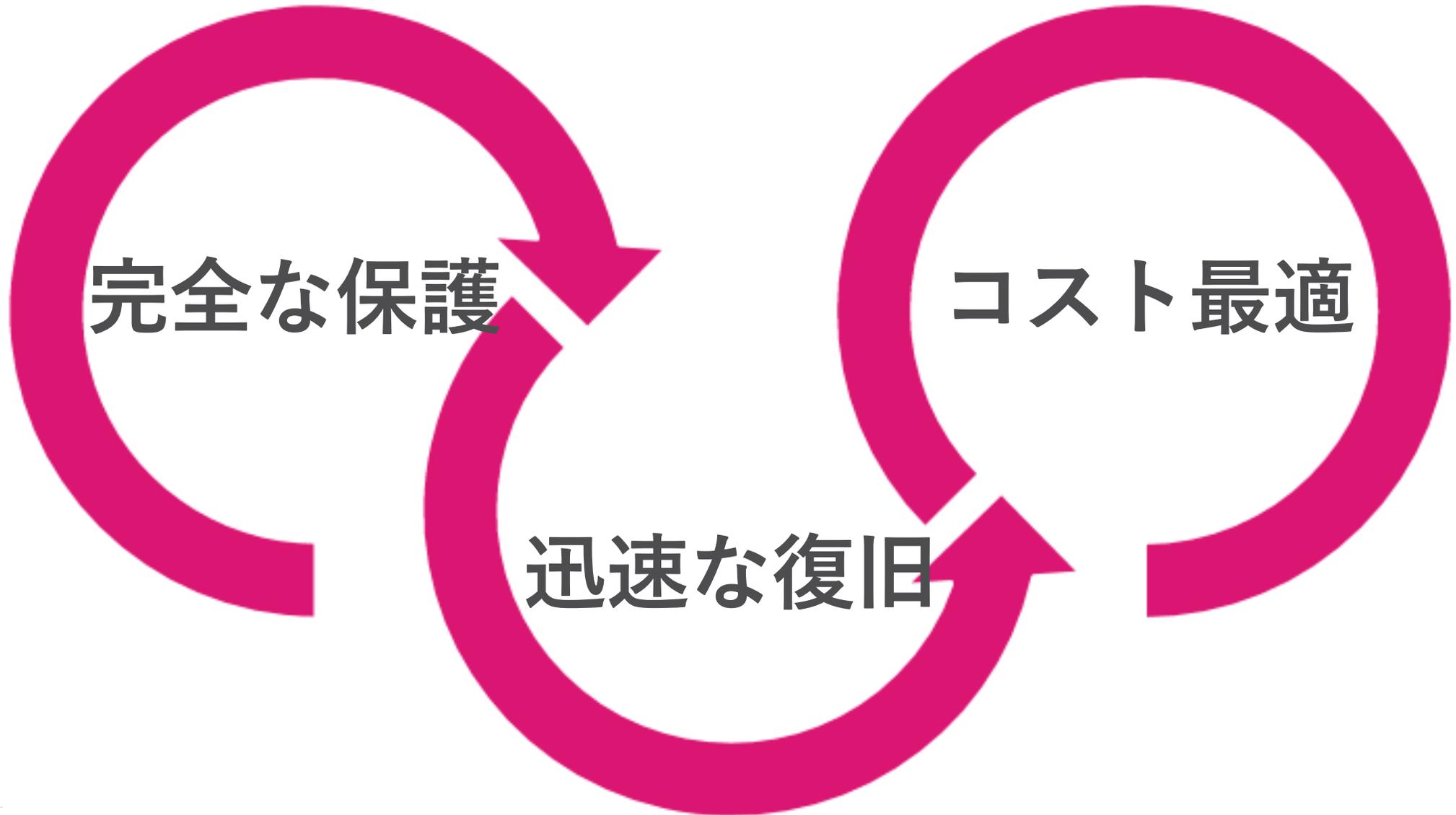
YOU DESERVE THE BEST SECURITY

# Table of Contents

- Harmony Endpoint の特徴
- Infinity Portal へのサインイン
- インストールパッケージの作成とダウンロード
- クライアントのインストール
- クライアントの UI

# 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



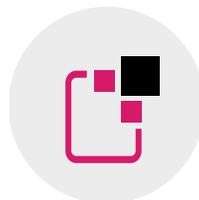
Threat Hunting

# 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



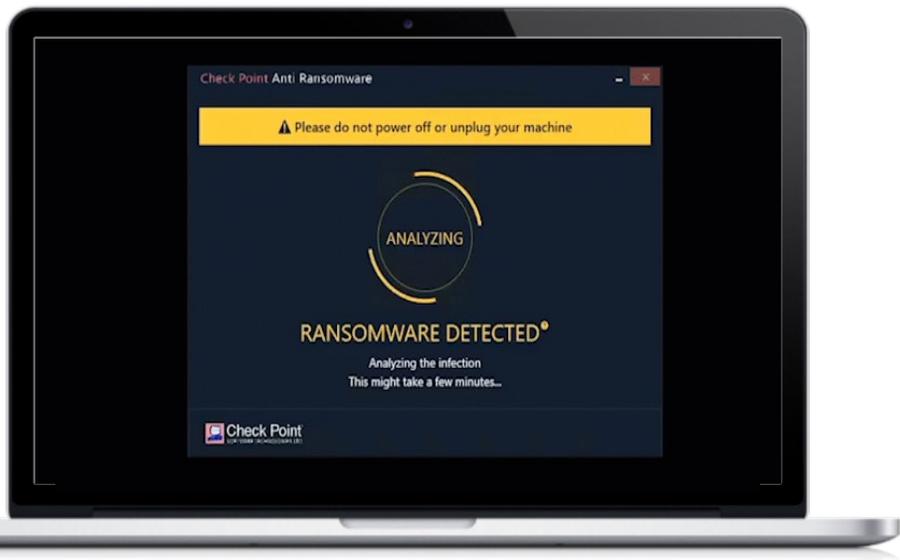
## フォレンジックレポート

独自の解析技術による  
正確性の高い攻撃解析

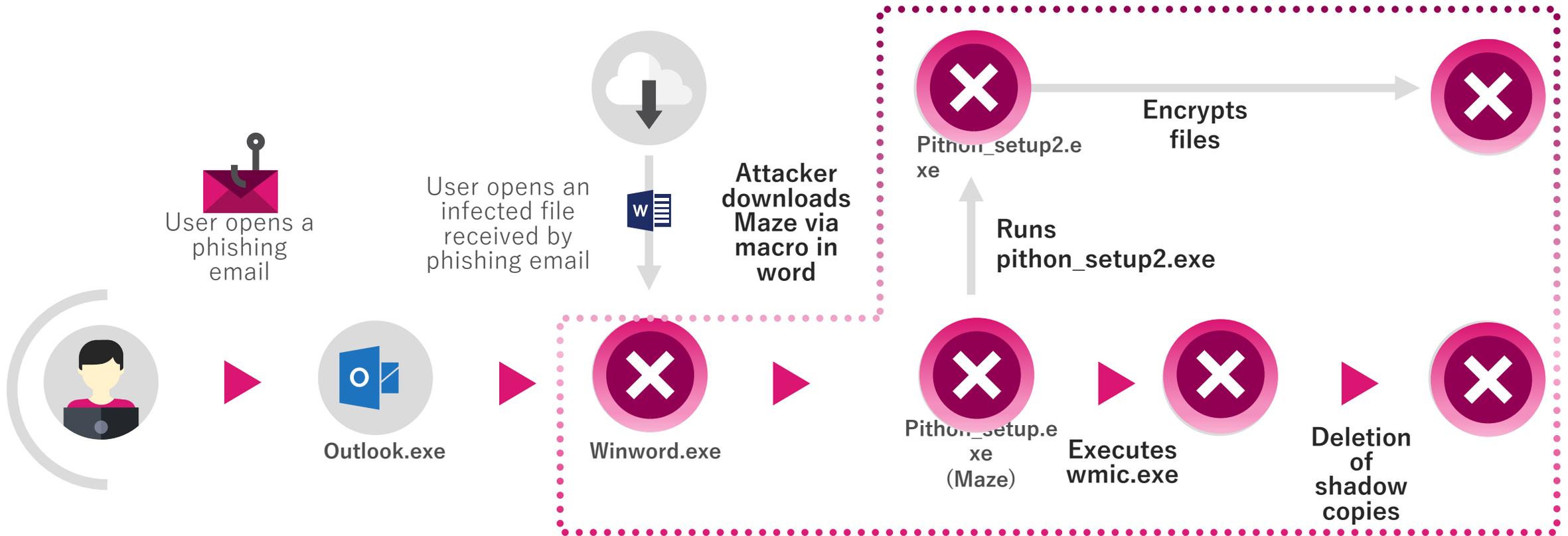
# 検知、調査、修復作業の 90% を自動化

## 自動化

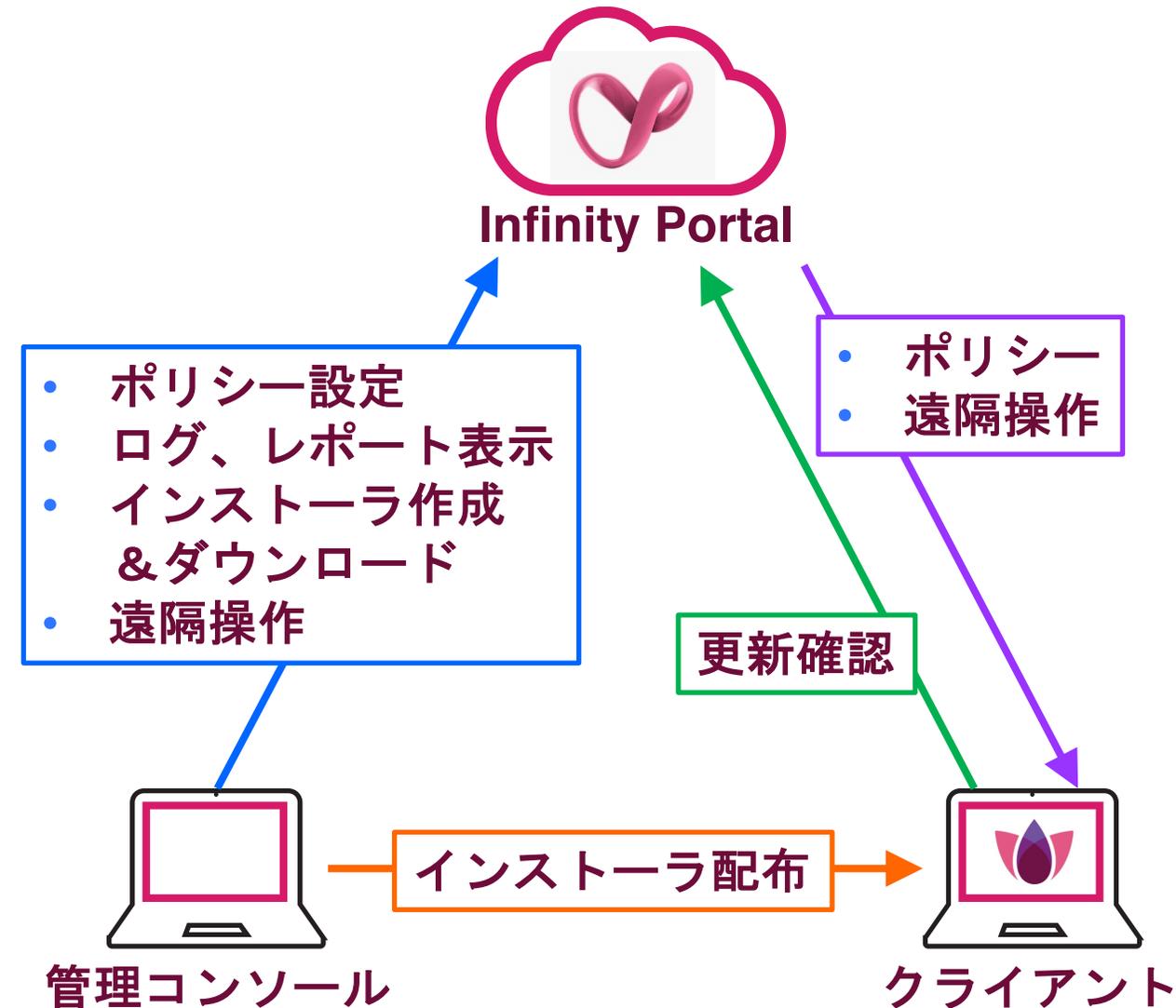
- あらゆるイベントを監視、収集
- 攻撃を検知
- 悪意のある活動を隔離
- サイバーキルチェーン全体をクリーンナップ
- 暗号化されたファイルを復元
- フォレンジックレポートを提供



# 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

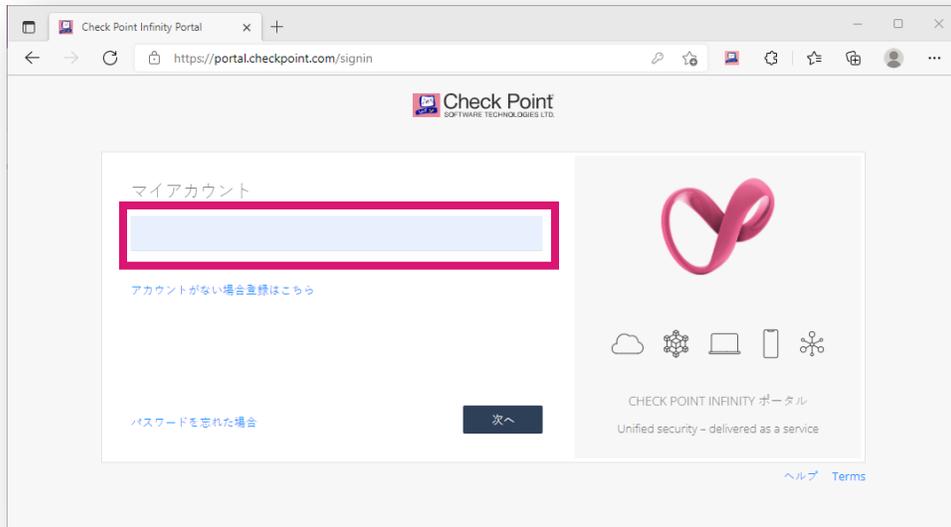
- Infinity Portal にアクセスして管理を行うパソコン
- ブラウザで管理を実施

## 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

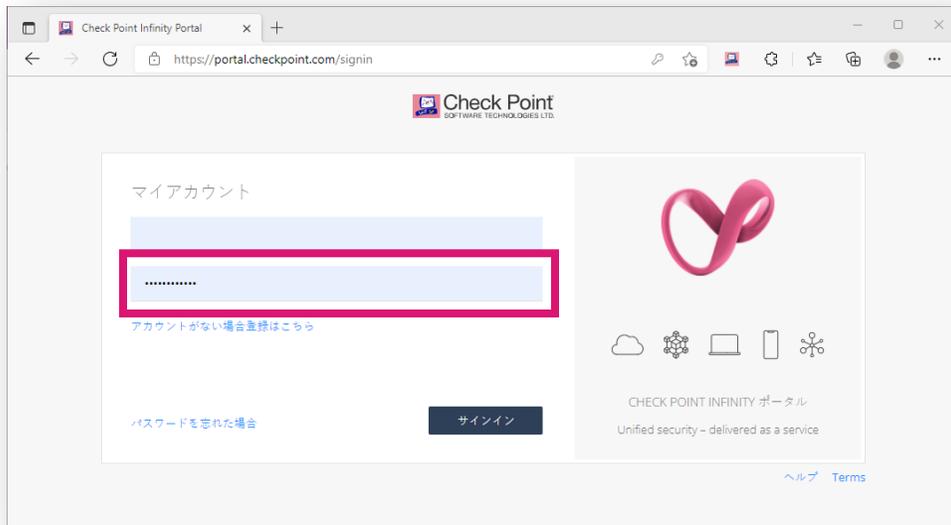
# Infinity Portal へのサインイン (1 / 3)



1. Infinity Portal へ接続する

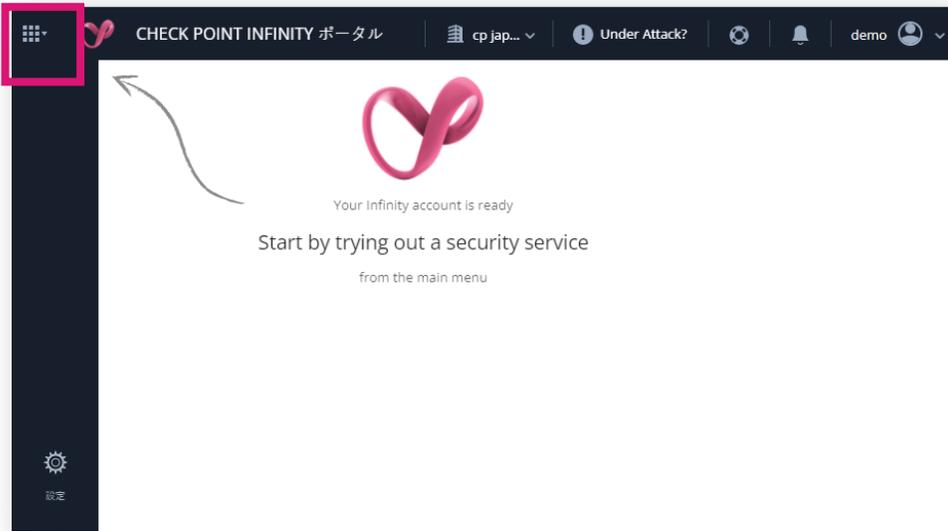
- URL: <https://portal.checkpoint.com/>

2. ユーザー名を入力して、「次へ」を押す



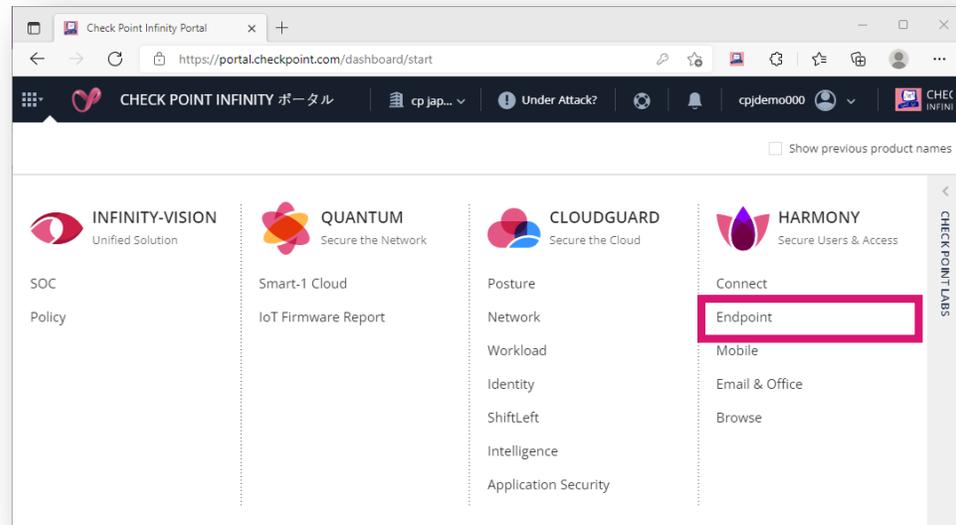
3. パスワードを入力して、「サインイン」を押す

# Infinity Portal へのサインイン (2 / 3)



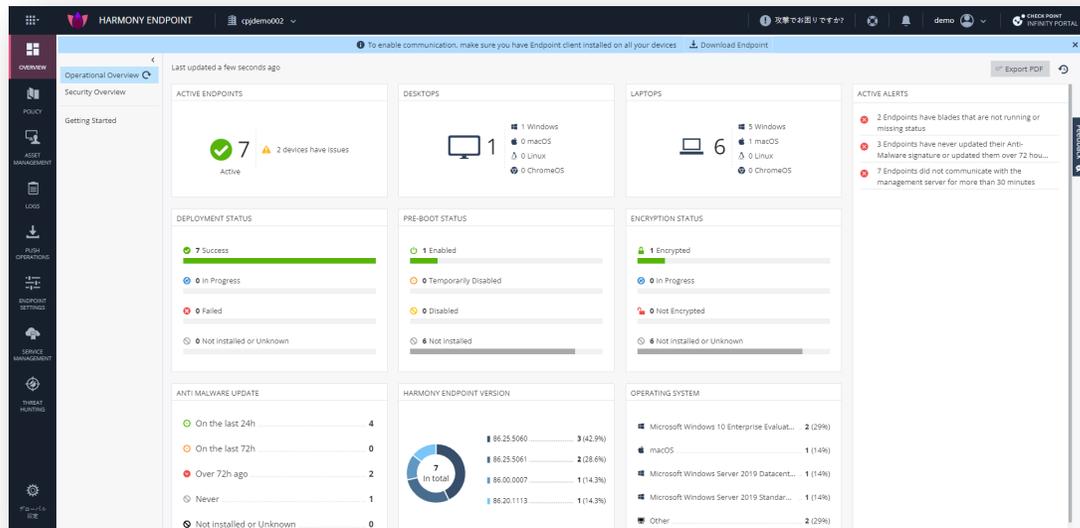
4. サインイン成功

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)



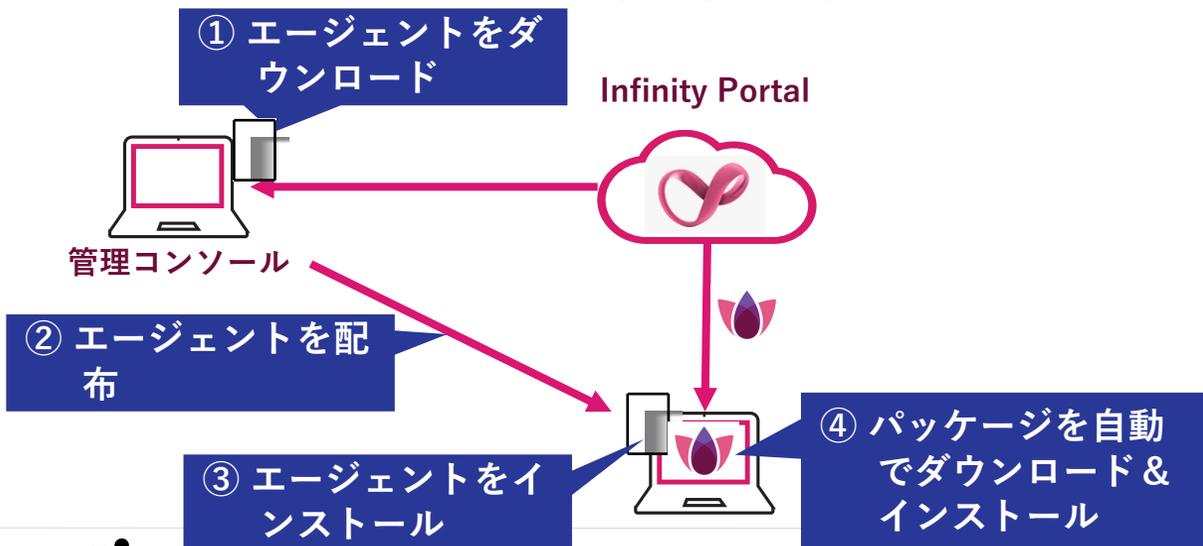
## 7. Harmony Endpoint の設定画面表示

# インストールパッケージの作成と ダウンロード

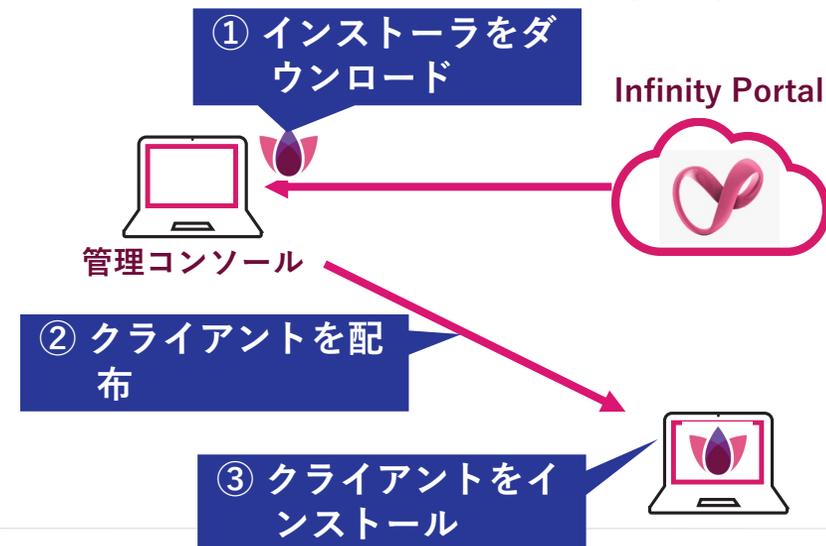
# クライアントの展開方法

- オンラインインストールと、オフラインインストールの2種類の方法を選択できます
- **オンラインインストール**
  - 軽量なインストーラを用いてエージェントのインストールを行います
  - エージェントのインストール後にパッケージを自動でダウンロードしてインストールします
  - ホームワークやテレワークのコンピュータへのインストールにおすすめです
- **オフラインインストール**
  - 必要なセキュリティ機能を含むインストーラを用いてクライアントのインストールを行います
  - 社内ネットワークに接続されたコンピュータへのインストールにおすすめです
- ファイルサーバやメールでインストーラを共有する以外にも、Active Directory や 3rd Party のツールを使用してインストールすることも可能です

## オンラインインストール



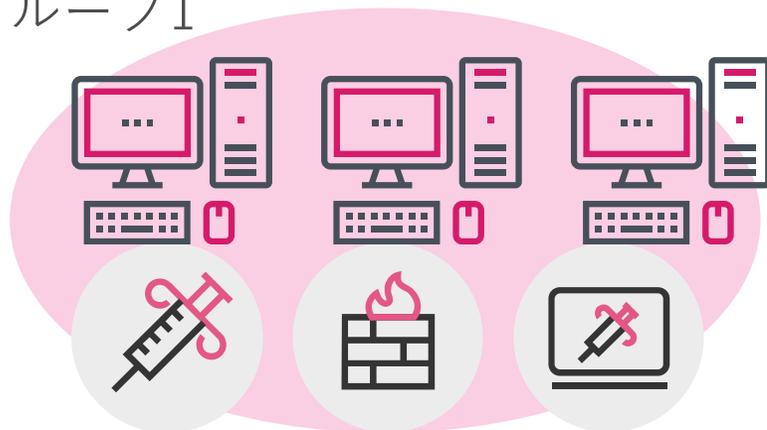
## オフラインインストール



# インストールパッケージの概要

- コンピュータに Harmony Endpoint クライアントをインストールするための、インストールパッケージを作成します。事前定義されたパッケージを使用することも可能です
- クライアントのバージョン、インストールする機能、バーチャルグループ、VPNサイト（VPN利用時）を構成します
- バーチャルグループを指定することで、クライアントインストール後にコンピュータを自動的にバーチャルグループに所属させることができます（Web UI で変更可能です）
- Policy > Deployment Policy > Software Deployment の設定は、インストールパッケージ作成時のクライアントバージョン、インストールする機能の構成と同じ設定にしてください。異なる場合、Software Deployment で設定したバージョン、機能にクライアントソフトウェアが更新されます

グループ1



グループ2



# インストールパッケージの作成 (1 / 5)

Policy > Export Packages > Endpoint Client

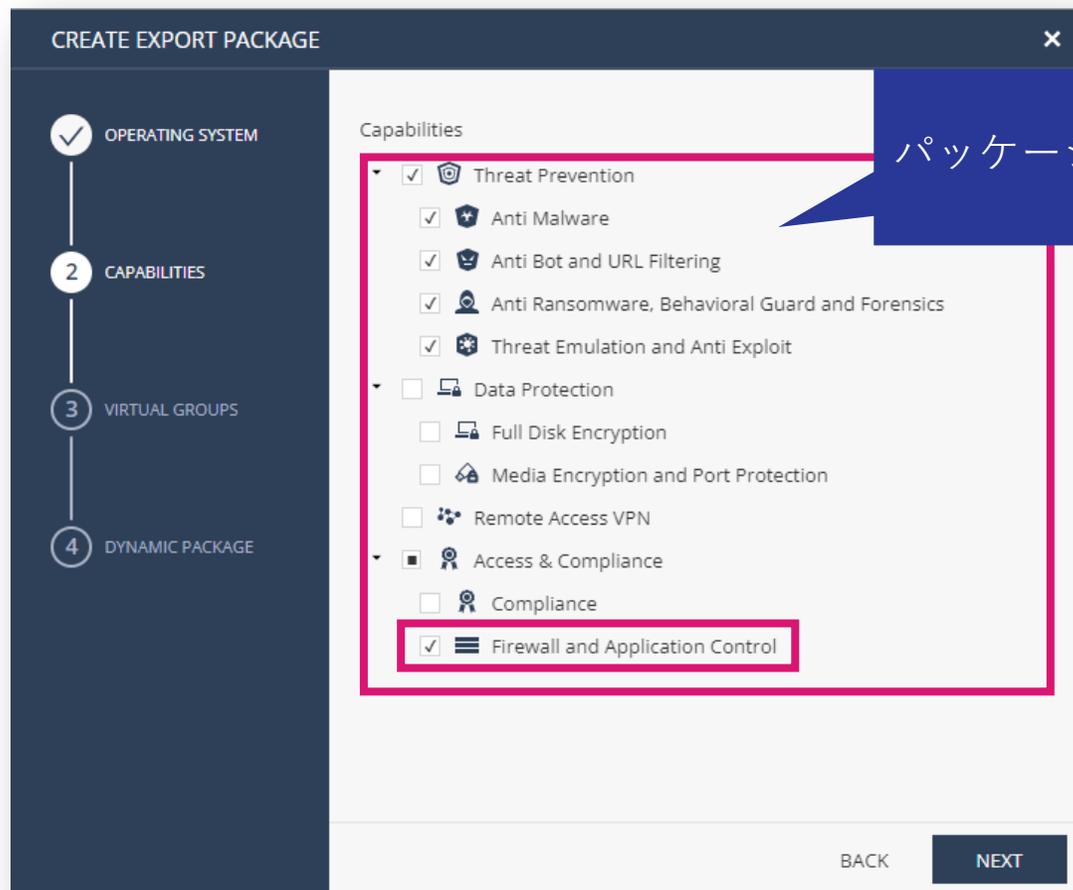
The screenshot displays the Check Point Harmony Endpoint console interface. The left sidebar shows the navigation menu with 'POLICY' and 'Endpoint Client' highlighted. The main content area shows the 'Export Package' section with a large empty box containing a plus sign, indicating the start of a new package creation. Below this, there are cards for 'Linux All Capabilities', 'macOS All Capabilities', and 'Windows All Capabilities'. A 'CREATE EXPORT PACKAGE' dialog box is open, showing the 'OPERATING SYSTEM' step. The dialog has three steps: 1. OPERATING SYSTEM, 2. CAPABILITIES, and 3. VIRTUAL GROUPS. In the 'OPERATING SYSTEM' step, the 'Package name' field is empty with a placeholder 'Type name...'. The 'Operating System' section shows two options: 'Windows' (selected with a blue checkmark) and 'macOS'. The 'Package version' dropdown is set to 'Any CPU'. At the bottom, there are radio buttons for 'Windows 64bit' and 'Windows 32bit', with 'Windows 32bit' selected. A 'NEXT' button is visible at the bottom right of the dialog.



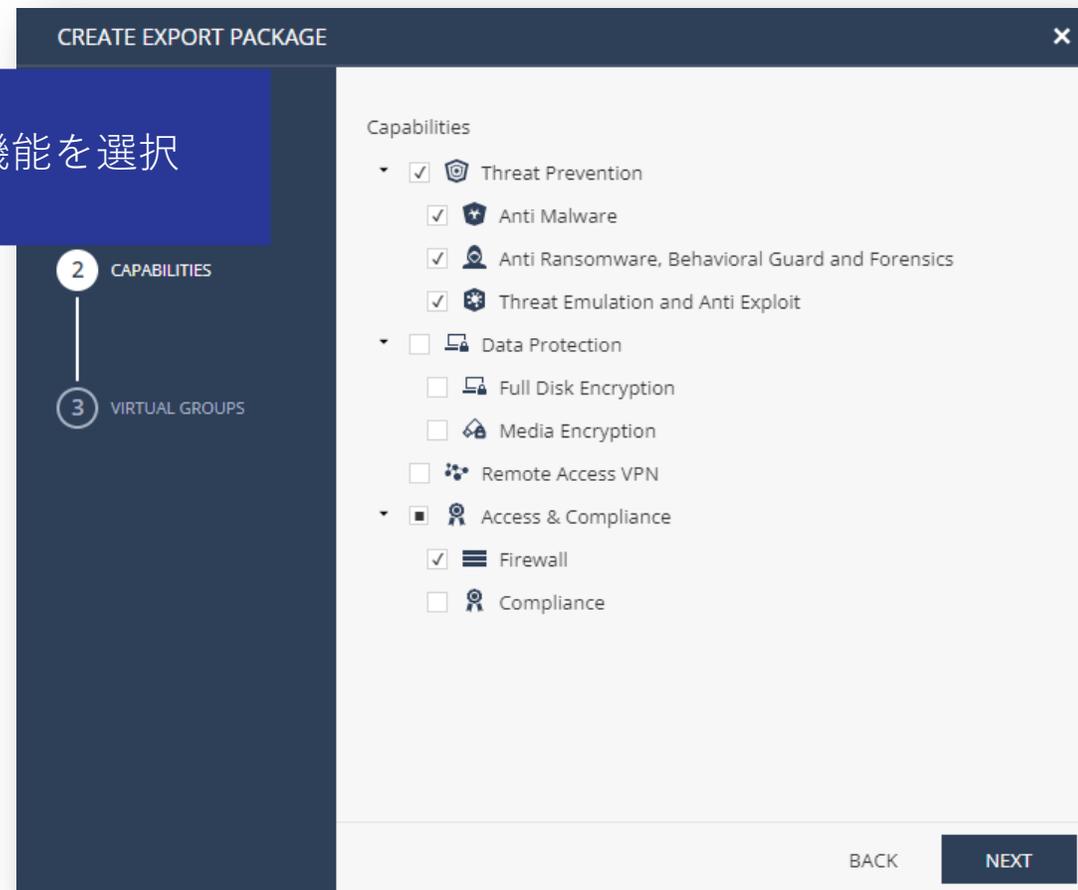
# インストールパッケージの作成 (3 / 5)

Policy > Export Packages > Endpoint Client

Windows



macOS



※ PushOperations で端末の隔離を実施する場合は、Firewall Bladeが必要

※ リモートアクセス VPN クライアント導入環境に、上書きインストールする場合は Remote Access VPN Blade が必要 (詳細は別冊参照)

# インストールパッケージの作成 (4 / 5)

Policy > Export Packages > Endpoint Client

Windows & macOS 共通

CREATE EXPORT PACKAGE

OPERATING SYSTEM

CAPABILITIES

3 VIRTUAL GROUPS

4 DYNAMIC PACKAGE

Virtual group

VPN site

BACK NEXT

パッケージをインストールしたコンピュータが所属するバーチャルグループを指定

リモートアクセスVPN機能を含める場合に、接続するVPNサイトを設定

# インストールパッケージの作成 (5 / 5)

Policy > Export Packages > Endpoint Client

Windows のみ

CREATE EXPORT PACKAGE

To get an MSI file, run EndpointSetup.exe /CreateMSI

Minimize package size (takes longer)

**General settings**

Disable the Endpoint Security Client's user interface

**Dependencies settings**

Harmony Endpoint Client requires the following components to be installed.

.NET Framework 4.6.1 Installer (60MB)

32-bit support (40MB)

Visual Studio Tools for Office Runtime 10.0.50903 (40MB)

Total size of included dependencies: 40MB

**Anti-Malware settings**

Select the signature profile you wish to include in the package.

Included signatures:

Download package when saved

BACK FINISH

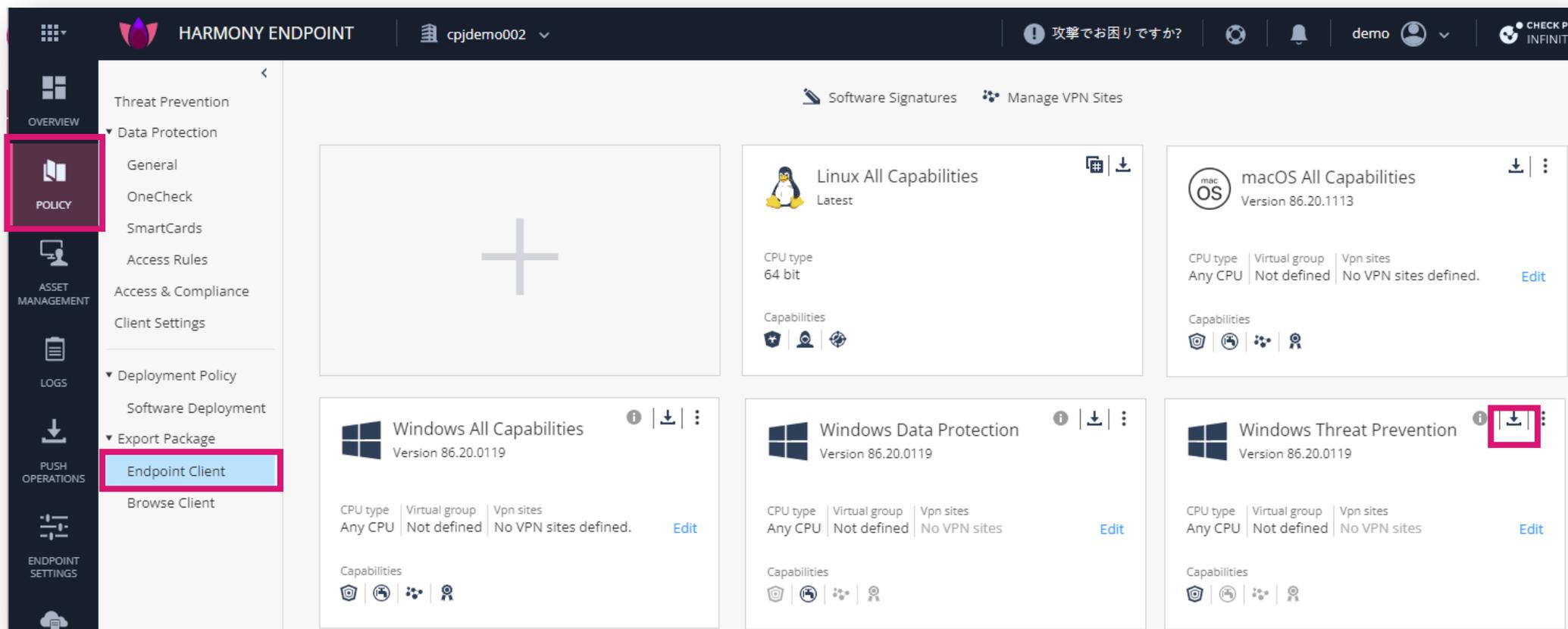
不要な機能を削減して、パッケージサイズを最小化することが可能

パッケージに含める Anti-Malware のシグネチャを選択

# インストールパッケージのダウンロード

Policy > Export Packages > Endpoint Client

- ダウンロードするパッケージの  をクリックしてパッケージをダウンロードします



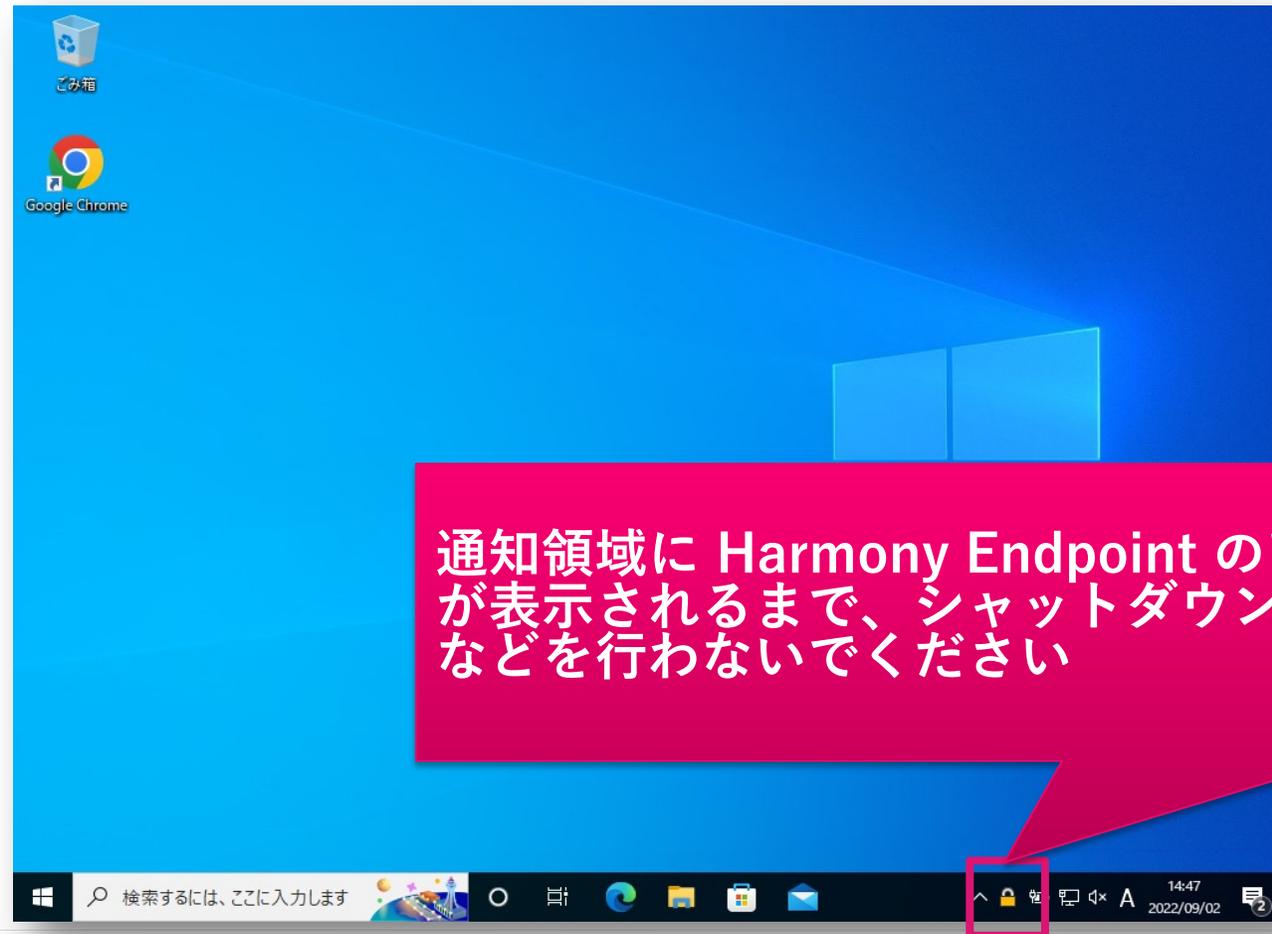
The screenshot displays the Harmony Endpoint management console. The left sidebar shows the navigation menu with 'POLICY' and 'Export Package' highlighted. The main content area shows a grid of packages available for download:

- Linux All Capabilities** (Latest): CPU type 64 bit. Capabilities include Threat Prevention, Data Protection, and SmartCards.
- macOS All Capabilities** (Version 86.20.1113): CPU type Any CPU, Virtual group Not defined, Vpn sites No VPN sites defined. Capabilities include Threat Prevention, Data Protection, SmartCards, and Access Rules.
- Windows All Capabilities** (Version 86.20.0119): CPU type Any CPU, Virtual group Not defined, Vpn sites No VPN sites defined. Capabilities include Threat Prevention, Data Protection, SmartCards, and Access Rules.
- Windows Data Protection** (Version 86.20.0119): CPU type Any CPU, Virtual group Not defined, Vpn sites No VPN sites. Capabilities include Threat Prevention, Data Protection, SmartCards, and Access Rules.
- Windows Threat Prevention** (Version 86.20.0119): CPU type Any CPU, Virtual group Not defined, Vpn sites No VPN sites. Capabilities include Threat Prevention, Data Protection, SmartCards, and Access Rules.

# クライアントのインストール

# クライアントのインストール

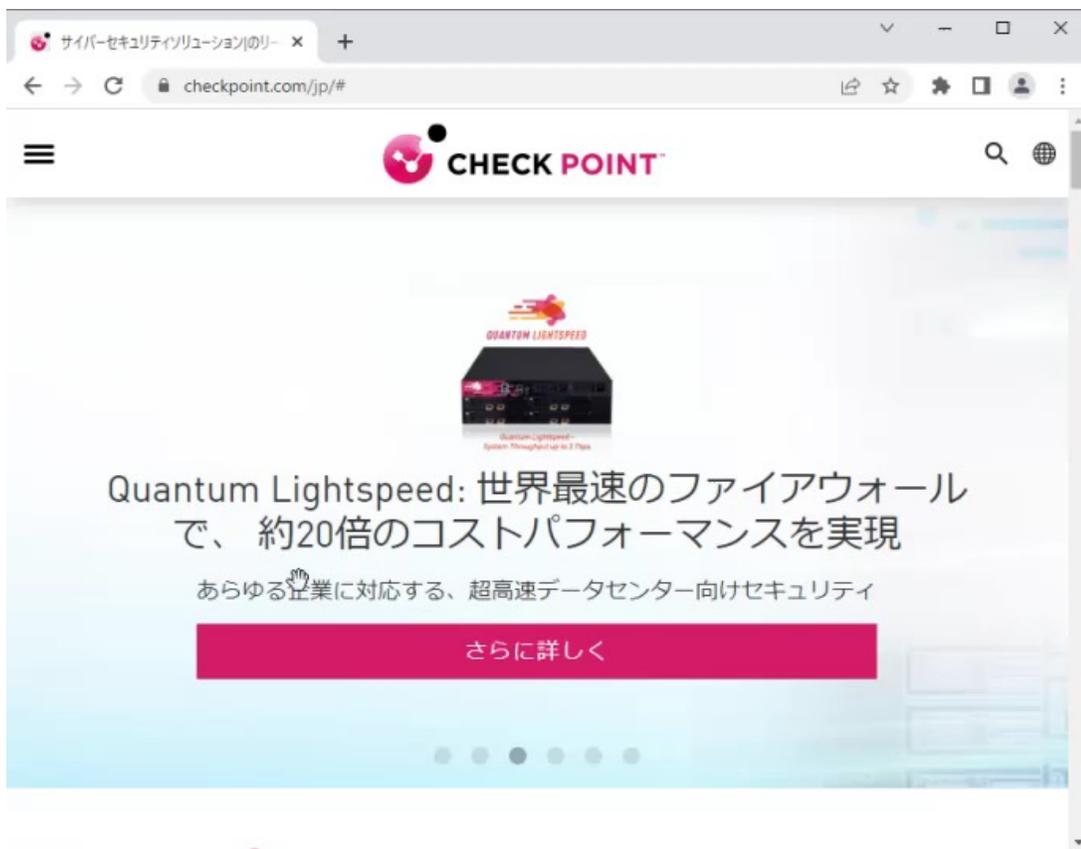
- インストールパッケージをダブルクリックします
- 通知領域に Harmony Endpoint のアイコン  が表示されるまで、シャットダウンや再起動などを行わないでください



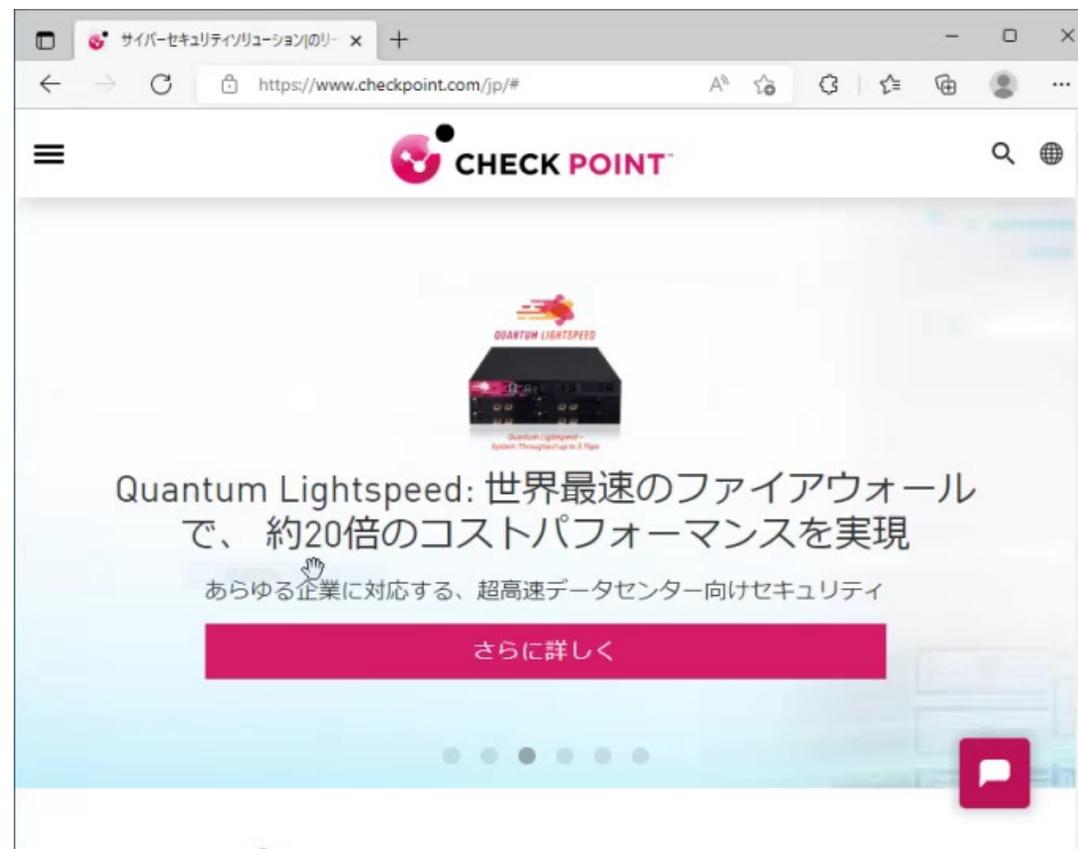
# 【参考】 Check Point アイコン の表示方法

- ブラウザにCheck Pointのアイコン  が表示されていない場合は、以下の動画を参考にして、表示させてください。

Check Point アイコンの表示方法 (Chrome)



Check Point アイコンの表示方法 (Edge)



# 【参考】オンラインインストール用インストーラ

- Overview > Operational Overview 上部の「Download Endpoint」からダウンロードします
- OS、クライアントバージョン、バーチャルグループを選択して、ダウンロードします
- Policy > Deployment Policy > Software Deployment の設定に従ってセキュリティ機能がインストールされます

The screenshot displays the Check Point Harmony Endpoint management console. The main interface shows the 'Operational Overview' page with a navigation menu on the left. A red box highlights the 'Operational Overview' link in the menu and the 'Download Endpoint' button in the top right corner of the main content area. A tooltip message reads: 'To enable communication, make sure you have Endpoint client installed on all your devices'. Below this, the console provides a summary of active endpoints (3 Active), deployment status (3 Success, 0 In Progress, 0 Failed, 0 Not installed or Unknown), and health status (3 computers, No issues). A modal dialog titled 'DOWNLOAD HARMONY ENDPOINT' is open, showing download options for Windows, Linux, and macOS. Each OS section includes a 'Download version' dropdown, a 'Virtual group (optional)' dropdown, and a 'DOWNLOAD' button. The Windows section shows version 86.60.0186, Linux shows 'Latest', and macOS shows 86.60.2568. All sections specify 'Any CPU (<2MB)'. The dialog also includes a 'More versions' link and 'CANCEL' and 'OK' buttons.

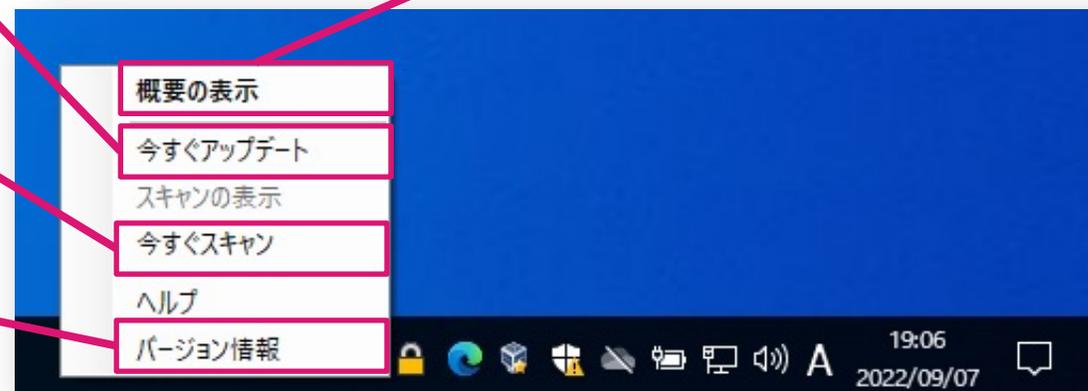
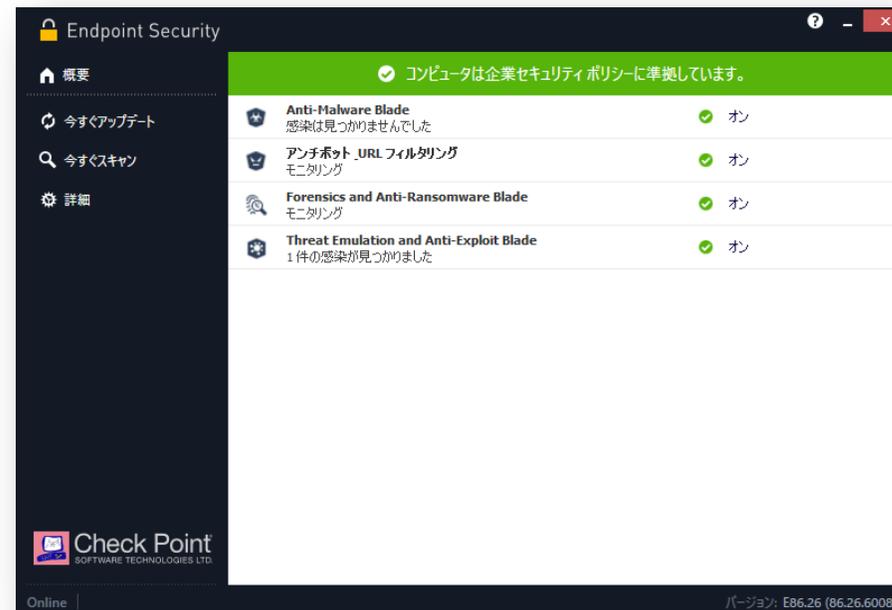
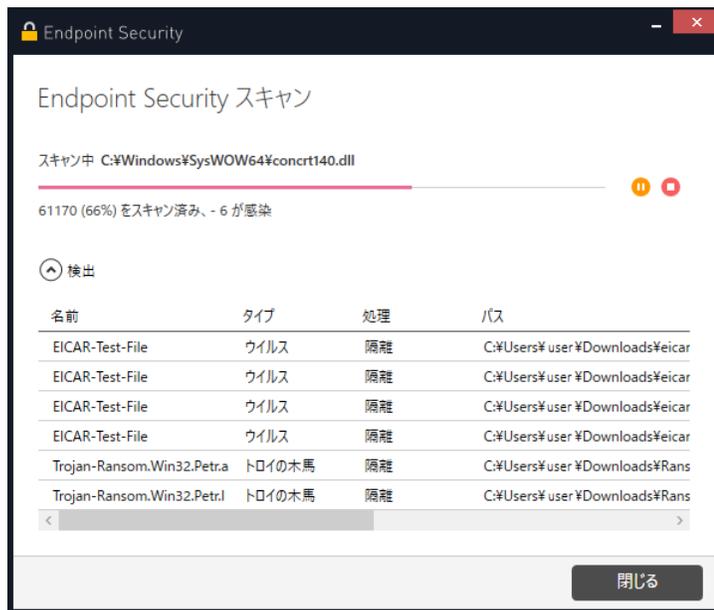
クライアントの UI

YOU DESERVE THE BEST SECURITY

# クライアントの UI 概要（1 / 4）

- クライアントソフトウェアでは、各種情報を確認、収集できます
  - セキュリティ機能のステータス
  - セキュリティログ
  - クライアントソフトウェアのバージョン
  - セキュリティ Blade のバージョン
  - ポリシーのバージョン
  - テクニカルサポートに提供するログ（CPinfo）
- ポリシーと Anti-Malware のシグネチャを更新できます
- Anti-Malware による Scan を実施できます

# クライアントの UI 概要 (2 / 4)



# クライアントの UI 概要（3 / 4）：詳細

- 「ポリシーの表示」は、パソコンに適用されているポリシーバージョンを確認できます
- 「ログの表示」は、パソコンでのアクティビティを確認できます
- 「収集」は、テクニカルサポート用の情報（CPinfo）を収集します
  - CPinfo は、%UserProfile%\CPInfo に保存されます

The image displays the Endpoint Security client interface with several windows open. The main window shows the '詳細' (Details) section, which is highlighted with a red box. Within this section, three buttons are highlighted with red boxes: 'ポリシーの表示' (Show Policy), 'ログの表示' (Show Log), and '収集' (Collect). Arrows point from these buttons to other windows:

- 'ポリシーの表示' points to the 'インストール済みポリシー' (Installed Policies) table in the 'Endpoint Security' window.
- 'ログの表示' points to the 'Log Viewer' window.
- '収集' points to the 'Check Point Log Collection Tool' terminal window.

The 'インストール済みポリシー' table contains the following data:

名前	タイプ	バージョン	日付	モード
CP-demo (Anti Bot)	アンチボット	33	9/9/2022 5:38:34 PM	接続
CP-demo (Anti Malware)	アンチマルウェア	33	9/9/2022 5:38:34 PM	接続
CP-demo (Forensics)	フォレンジック	33	9/9/2022 5:38:32 PM	接続
Default Common Client settings for the entire...	共通クライアント	5	8/26/2022 3:26:30 PM	接続

The 'Log Viewer' window shows a table of log events with columns for Local Time, UTC Time, Severity, Product, Event type, Action, Endpoint Addr., Source, Destination, Description, and Rule. The 'Check Point Log Collection Tool' terminal window shows the following output:

```
Check Point Log Collection Tool
Current Configuration:
Detail level..... <Extended>
Log files since..... <13/08/2022>
Upload to Check Point..... <Disabled>
Press 'c' to configure
Press 'e' to enable upload to Check Point
Press <Enter> to start
Press 'q' to quit
```

# クライアントの UI 概要（4 / 4）：Blade

- 各 Blade をクリックすると、各 Blade での検出状況、ポリシーバージョンを確認できます

The screenshot shows the Check Point Endpoint Security interface. The main window displays the configuration for various security blades. A red box highlights the list of blades, and a red arrow points to the detailed view of the 'Anti-Malware Blade' configuration.

**Blade Configuration Summary:**

Blade Name	Status
Anti-Malware Blade	オン
アンチボット URL フィルタリング	オン
Forensics and Anti-Ransomware Blade	オン
Threat Emulation and Anti-Exploit Blade	オン

**Anti-Malware Blade Configuration Details:**

- コンピュータは企業セキュリティポリシーに準拠しています。
- 現在のステータス: オン
- 31 件の感染が見つかりました
- アップデートはまだ行われていません。
- シグネチャバージョン: 202204131304
- 最終スキャン: 今日 15:53:54
- CP-demo (Anti Malware), パ

**Anti-Malware Blade Infection List:**

感染名	パス
Trojan-Ranso...	C:\Users\In...
FileCAD_Test...	C:\Users\In...

**Anti-Bot URL Filtering Configuration Details:**

- コンピュータは企業セキュリティポリシーに準拠しています。
- 現在のステータス: オン
- 1 件の感染が見つかりました: 1 ブロック
- バージョン: 8.68.62.6
- アンチボット URL フィルタリング ポリシー: CP-

**Forensics and Anti-Ransomware Blade Configuration Details:**

- コンピュータは企業セキュリティポリシーに準拠しています。
- 現在のステータス: オン
- 分析した 25 ケース
- ポリシーの詳細: フォレンジック ポリシー: CP-demo (Forensics), バージョン: 33
- ディスク使用量: 10.86 MB
- モニタの経過時間: 4 日 4 時間

**Threat Emulation and Anti-Exploit Blade Configuration Details:**

- コンピュータは企業セキュリティポリシーに準拠しています。
- 現在のステータス: オン
- 78 件の感染が見つかりました
- Threat Emulation およびアンチエクスプロイト ポリシー: CP-demo (Threat Emulation), バージョン: 33

**Threat Emulation and Anti-Exploit Blade Infection List:**

インシデント ID	インシデントのソース	脅威の名前	実行アクション	コソフデ
dc99955f-4f30-4adf-9e50-5fda7b0...	Harmony File Reputation	C:\Users\K...	隔離	高
2409ea19-56a2-4957-9c41-2ba39...	Harmony File Reputation	C:\Users\K...	隔離	高
7b41bc2a-53ea-489c-98ad-bf14d...	Harmony File Reputation	C:\Users\K...	隔離	高
a30f2d9-4ea1-48f8-a4be-03097c...	Harmony File Reputation	C:\Users\K...	隔離	高
9715fda-1a2a-4e76-b628-88fd89...	Harmony Browser Exten...	eicar.com	隔離	高
e567efc0-bb6f-42c4-b1bb-abfd85...	Harmony File Reputation	C:\Users\K...	隔離	高
f3f7735-361f-4d3e-befb-a9b9783...	Harmony File Reputation	C:\Users\K...	隔離	高
32bbd62d-cad7-48fe-8418-7b1368...	Harmony File Reputation	C:\Users\K...	隔離	高
74268058-b467-4a72-ba3f-165f32...	Harmony File Reputation	C:\Users\K...	隔離	高
9bf13182-cf5a-4adc-80af-201a73...	Harmony Browser Exten...	eicar.zip	隔離	高

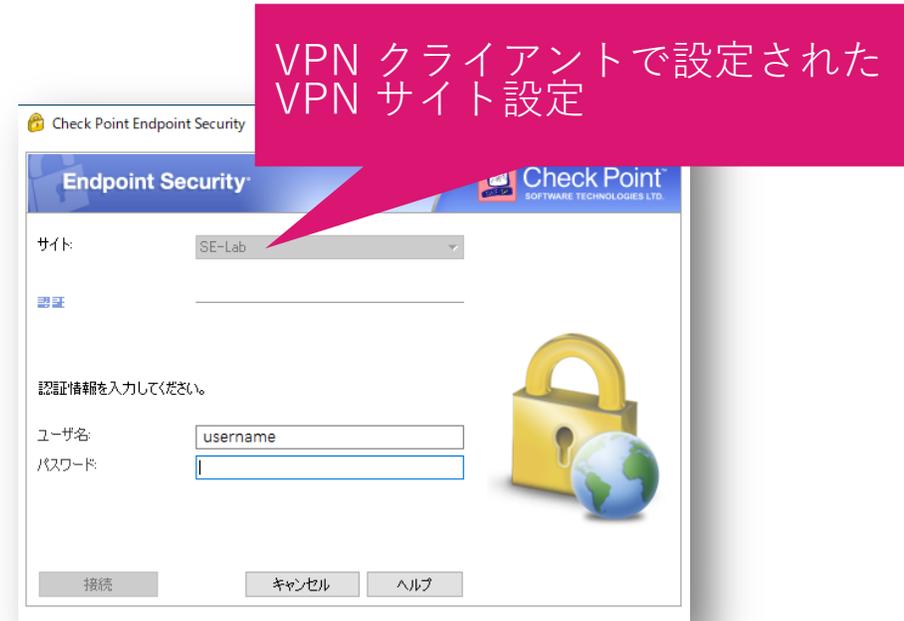
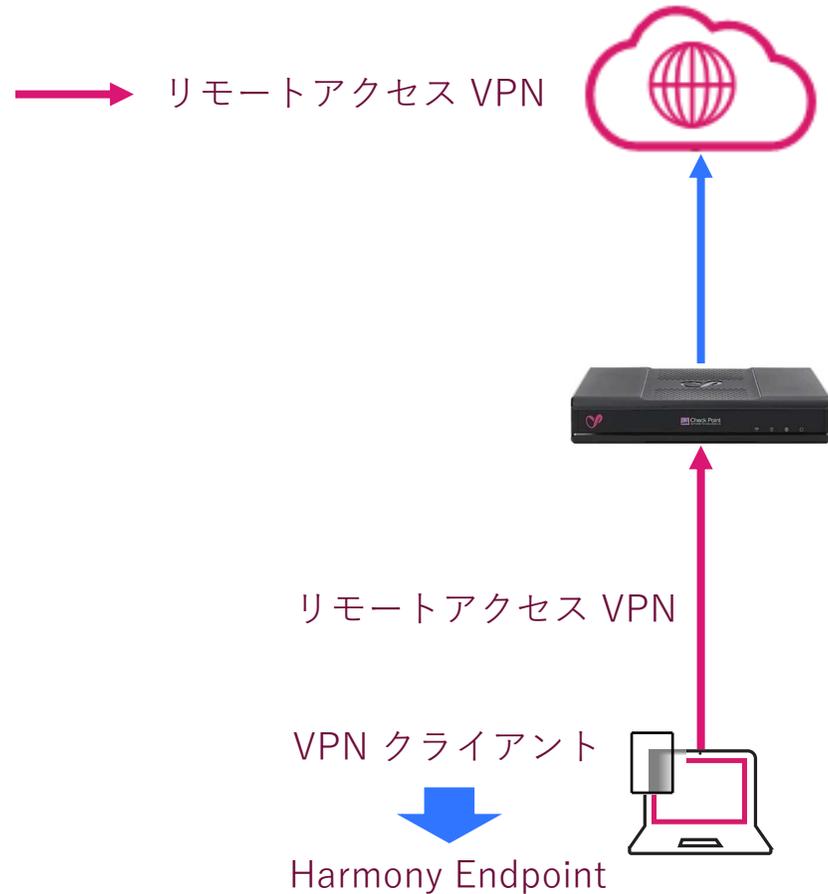
# リモートアクセス VPN 導入済環境への クライアントインストール

# 概要



# 概要

- 既に Quantum Spark でリモートアクセス VPN を実施しているエンドユーザへの Harmony Endpoint 導入時のクライアントインストール方法について説明します



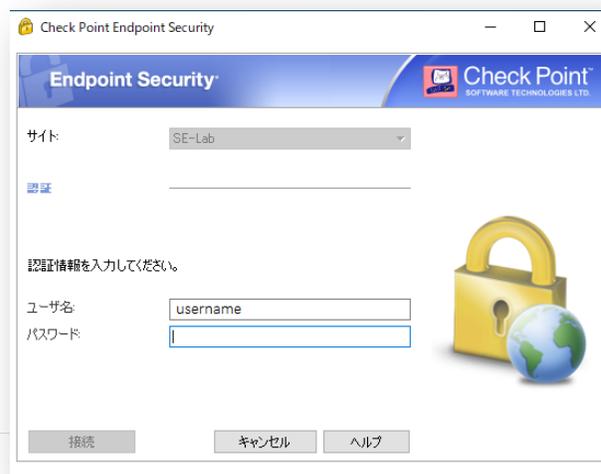
# 上書きインストール

# 上書きインストール

- Harmony Endpoint のインストールパッケージを作成する際に、Remote Access VPN Blade を含んだパッケージを作成し、クライアントのインストールを行うと、VPN クライアントがアンインストールされ Harmony Endpoint のクライアントがインストールされる
- Remote Access VPN Blade を含んでいないインストールパッケージでインストールを試みると、以下のエラーメッセージが表示される



- Harmony Endpoint クライアントのインストール時には、VPN クライアントで設定されていた VPN の設定は引き継がれるので、あらためて設定する必要はない



# AD グループポリシーでのソフトウェア配布

# MSI パッケージの作成

# MSI パッケージの作成

- Harmony Endpoint クライアントインストールパッケージのMSIバージョンを抽出可能
- Windowsコマンドプロンプトを起動し、 Harmony Endpointクライアントインストールパッケージを保存したフォルダへ移動
- コマンドプロンプトで、インストールパッケージを /CreateMSI オプションを付けて実行

```
選択C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19043.1706]
(c) Microsoft Corporation. All rights reserved.

C:\Users\alice>cd Downloads

C:\Users\alice\Downloads>EPS_2022-05-12T06_00_03.227_V86.26.6008.exe /CreateMSI

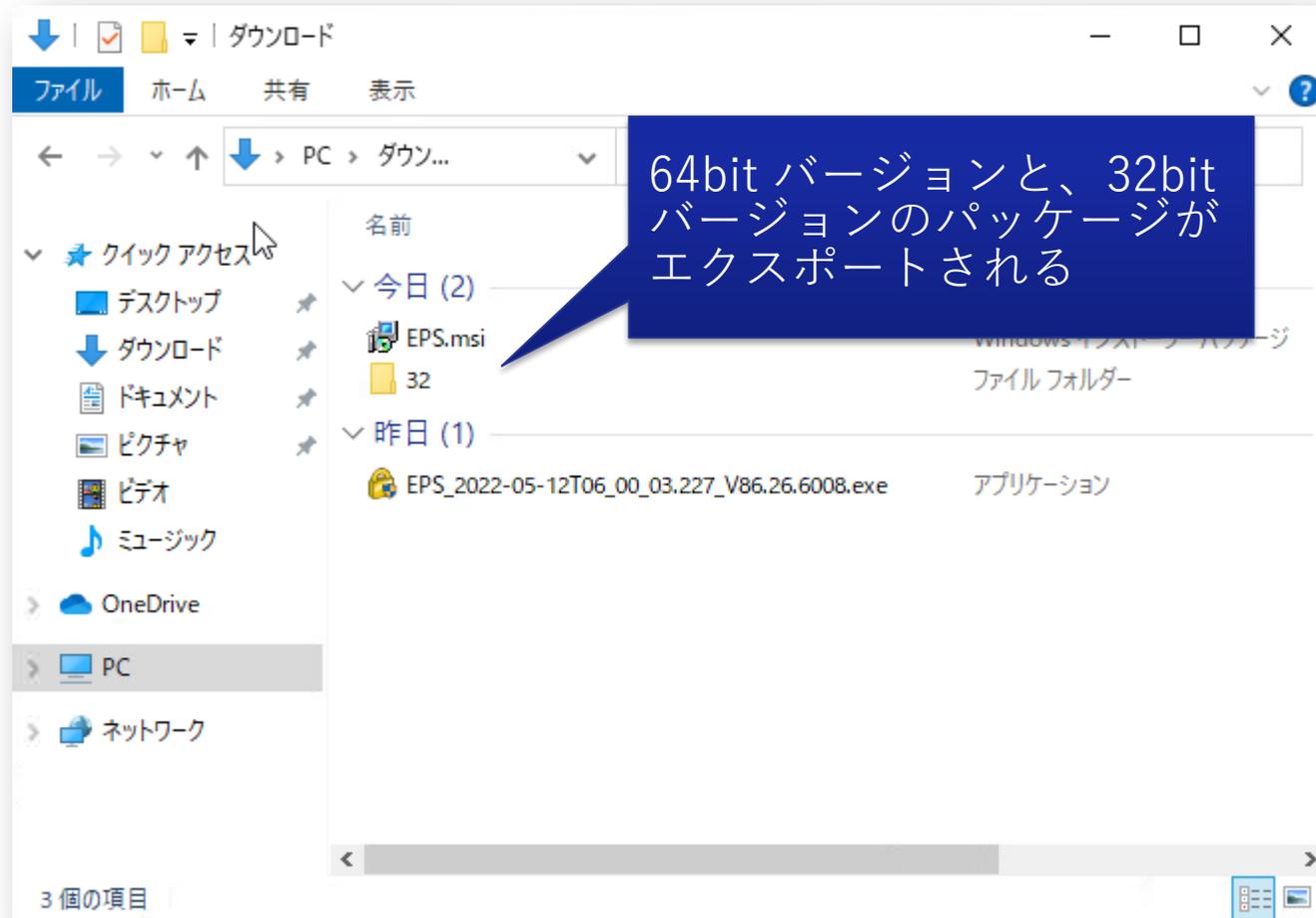
C:\Users\alice\Downloads>
```

```
Convert2MSI.exe
USERINSTALLMODE=200769
Generating MSIs. It will take a few minutes.
Please wait...
==> C:\Users\alice\Downloads\EPS.msi
==> C:\Users\alice\Downloads\32\EPS.msi

Press any key to close this window
```

64bit バージョンと、32bit バージョンのパッケージがエクスポートされる

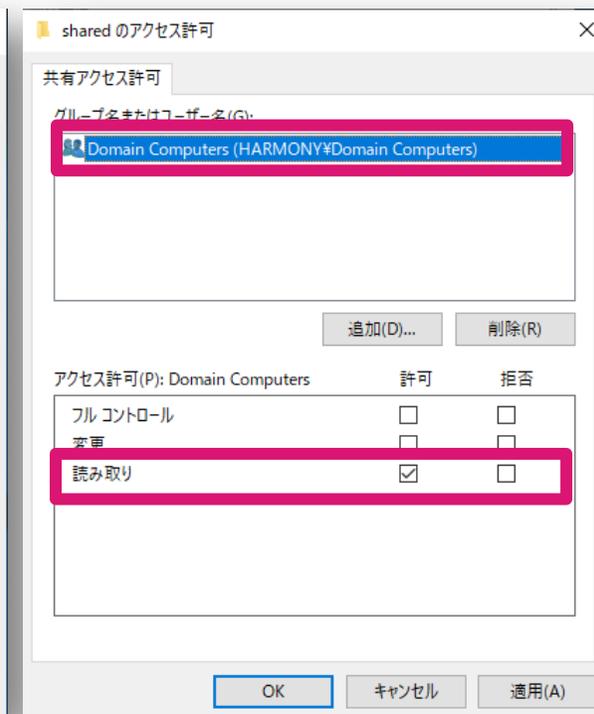
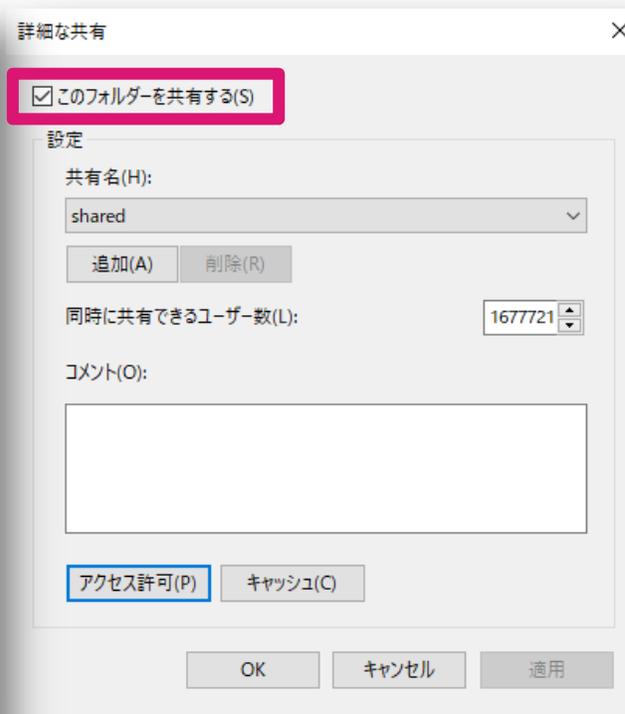
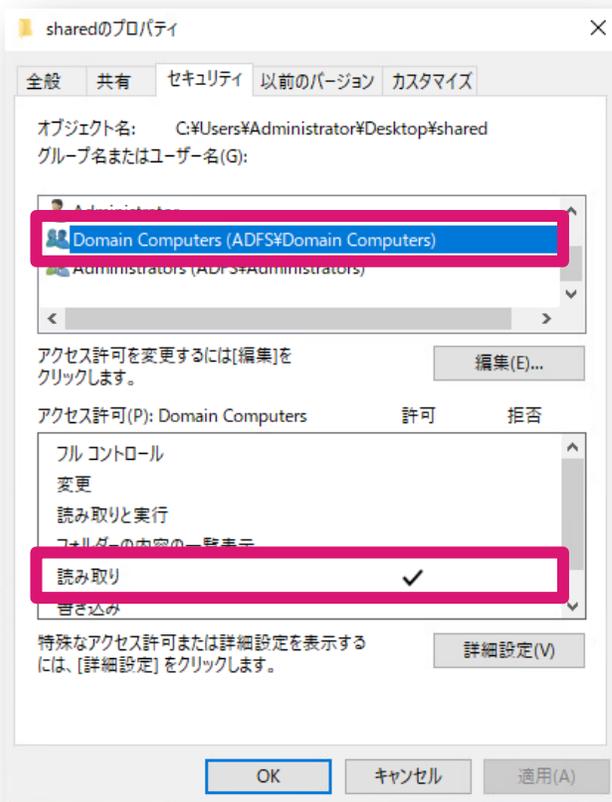
# MSI パッケージの作成



# 配布ポイントの作成

# 配布パッケージのファイル共有設定

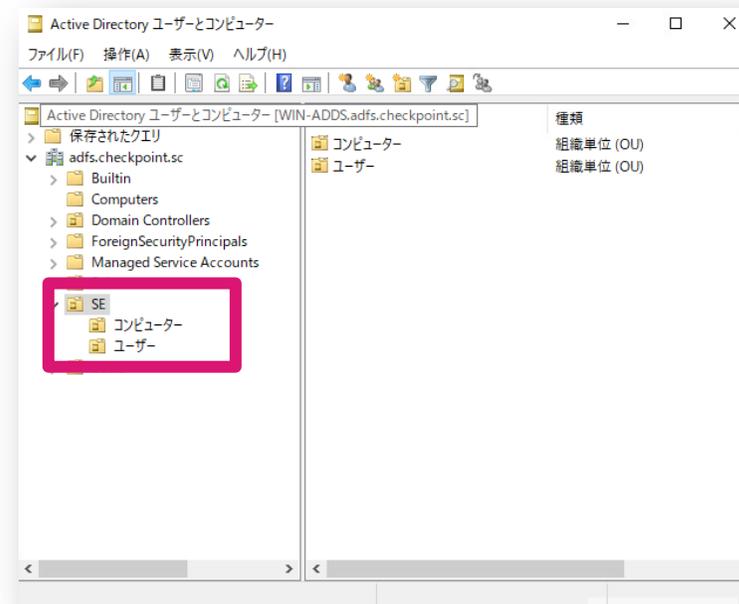
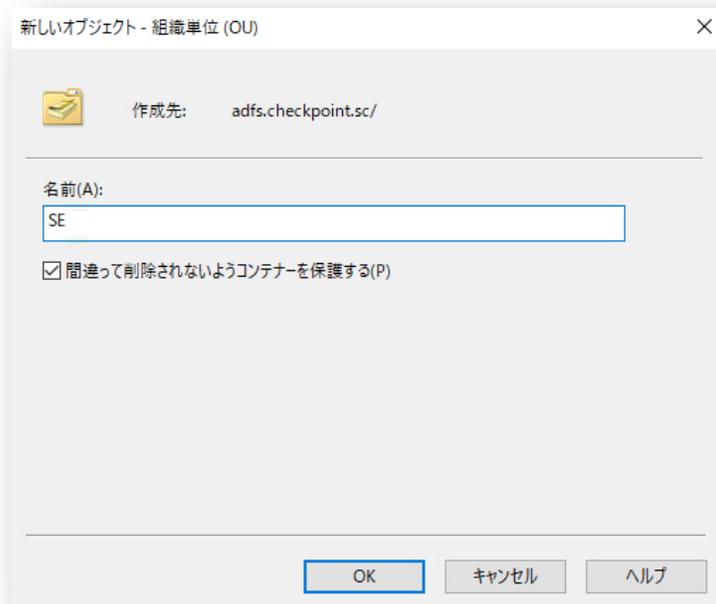
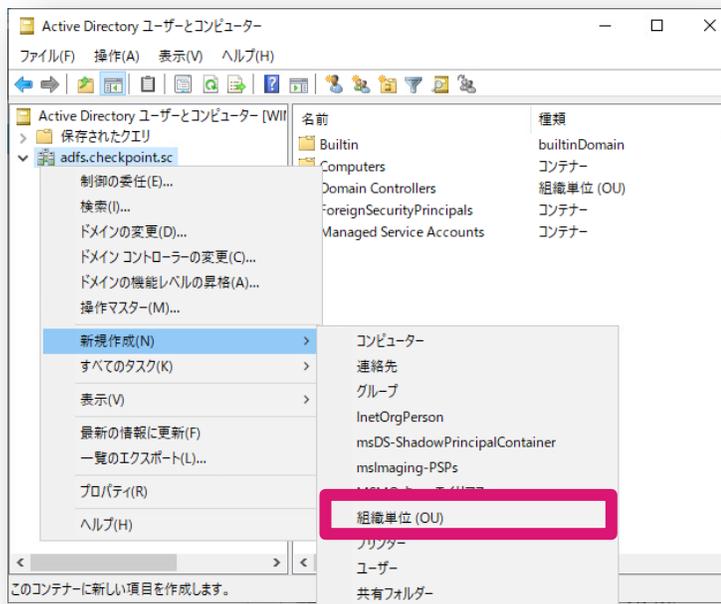
- 共有フォルダを作成
- ソフトウェアをインストールするコンピューターに対して、読み取りのアクセス権を設定
- 共有フォルダにMSIパッケージを保存



# OU（組織単位）の作成

# OU（組織単位）の作成

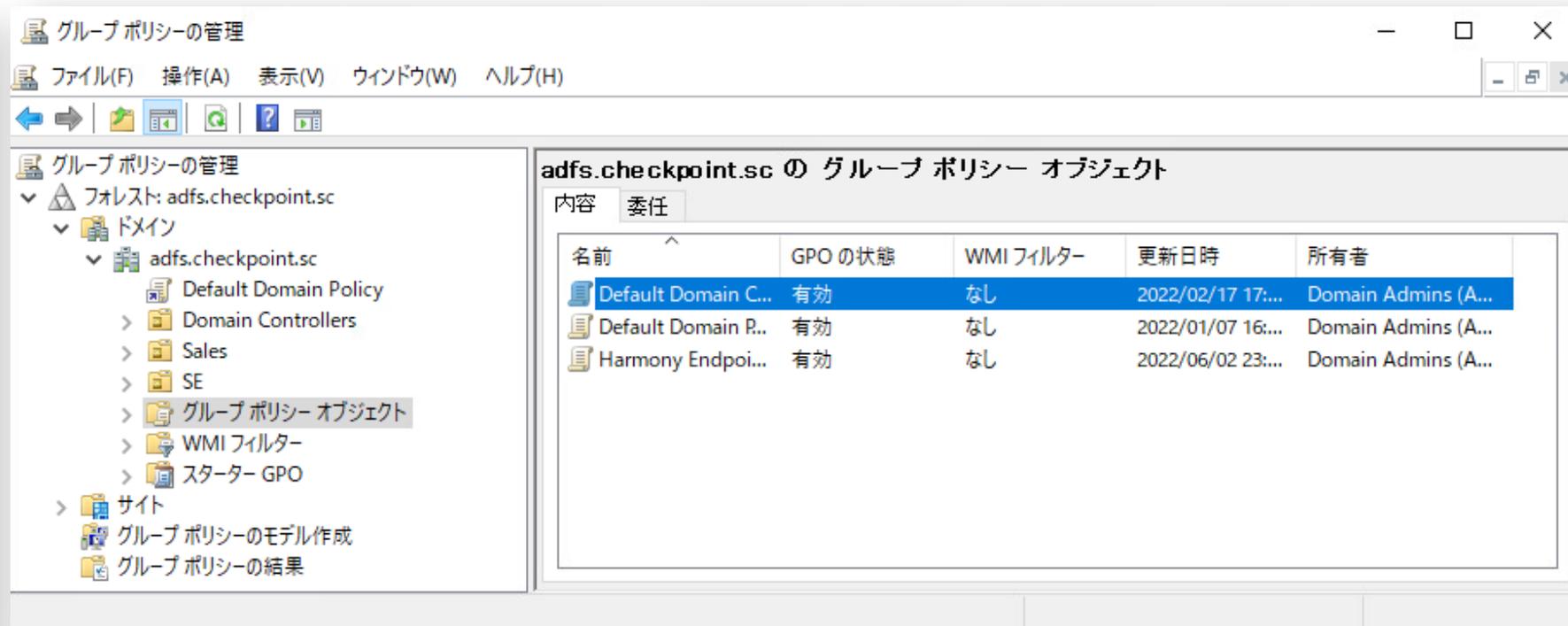
- Active Directory ユーザーとコンピューターを開き、ドメイン名を右クリックして、[新規作成]、[組織単位 (OU)] を選択
- OU の名前を入力して、OKをクリック
- 作成した OU に、Harmony Endpoint をインストールするコンピューターのオブジェクトを移動  
※ 適宜、作成した OU 内に [コンピューター] と [ユーザー] というOUを作成して管理



# GPO（グループポリシーオブジェクト）の作成

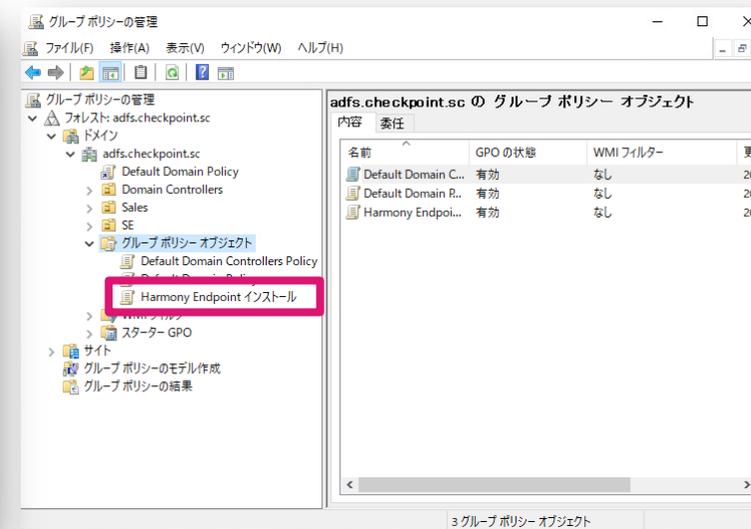
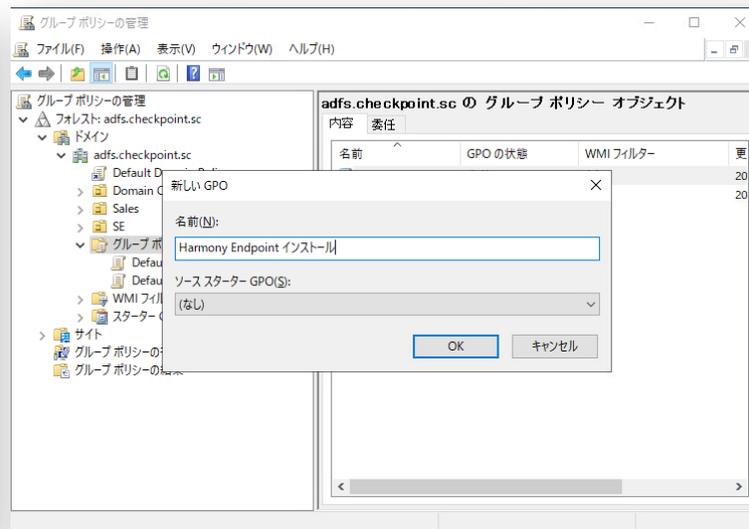
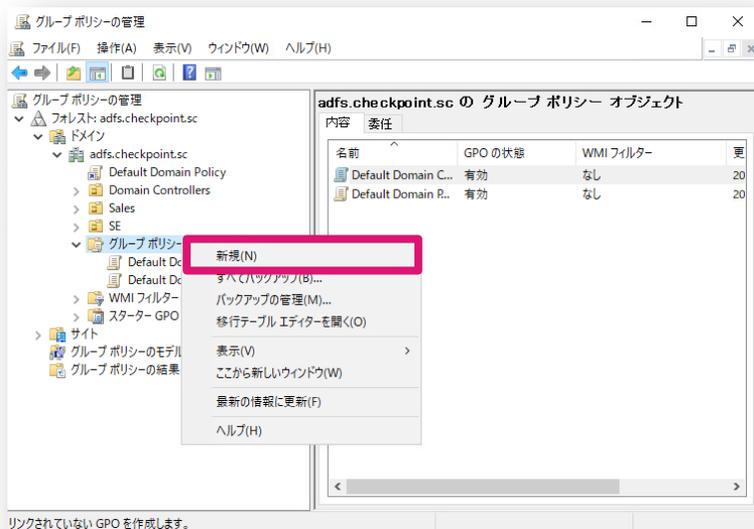
# 「グループポリシーの管理」を開く

- サーバーマネージャを開いて、ツール > グループポリシーの管理を選択
- グループポリシーの管理ウィンドウが開く



# GPO（グループポリシーオブジェクト）の作成

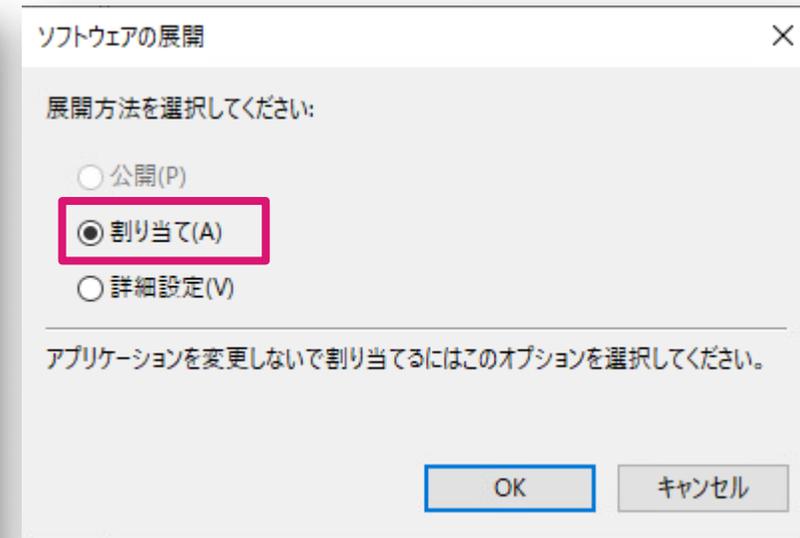
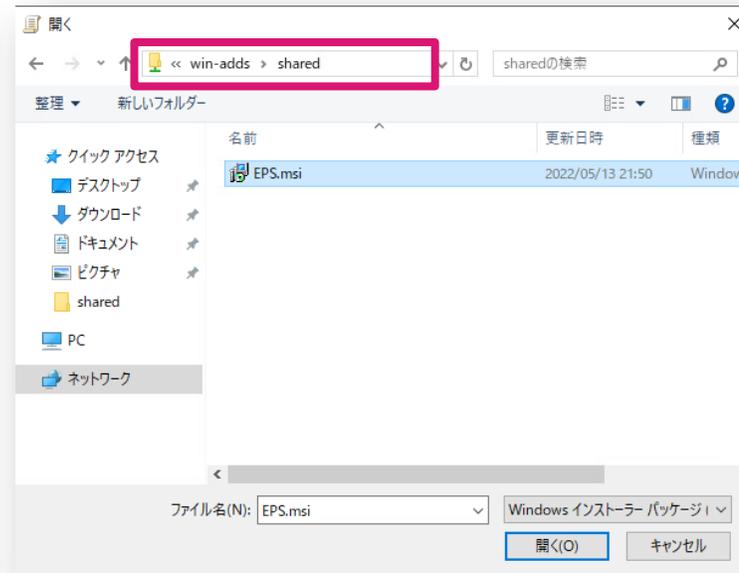
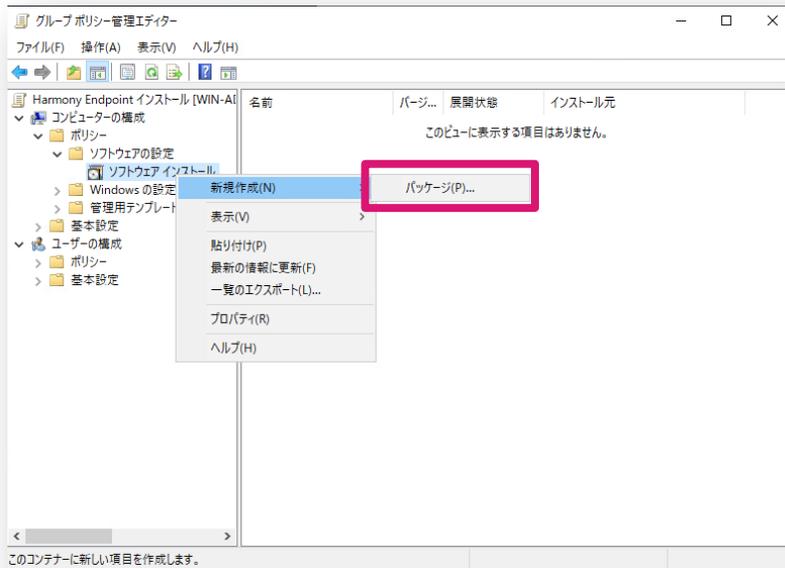
- [グループポリシーオブジェクト] を右クリックして、[新規] を選択
- GPOの名前を入力して、OKをクリック



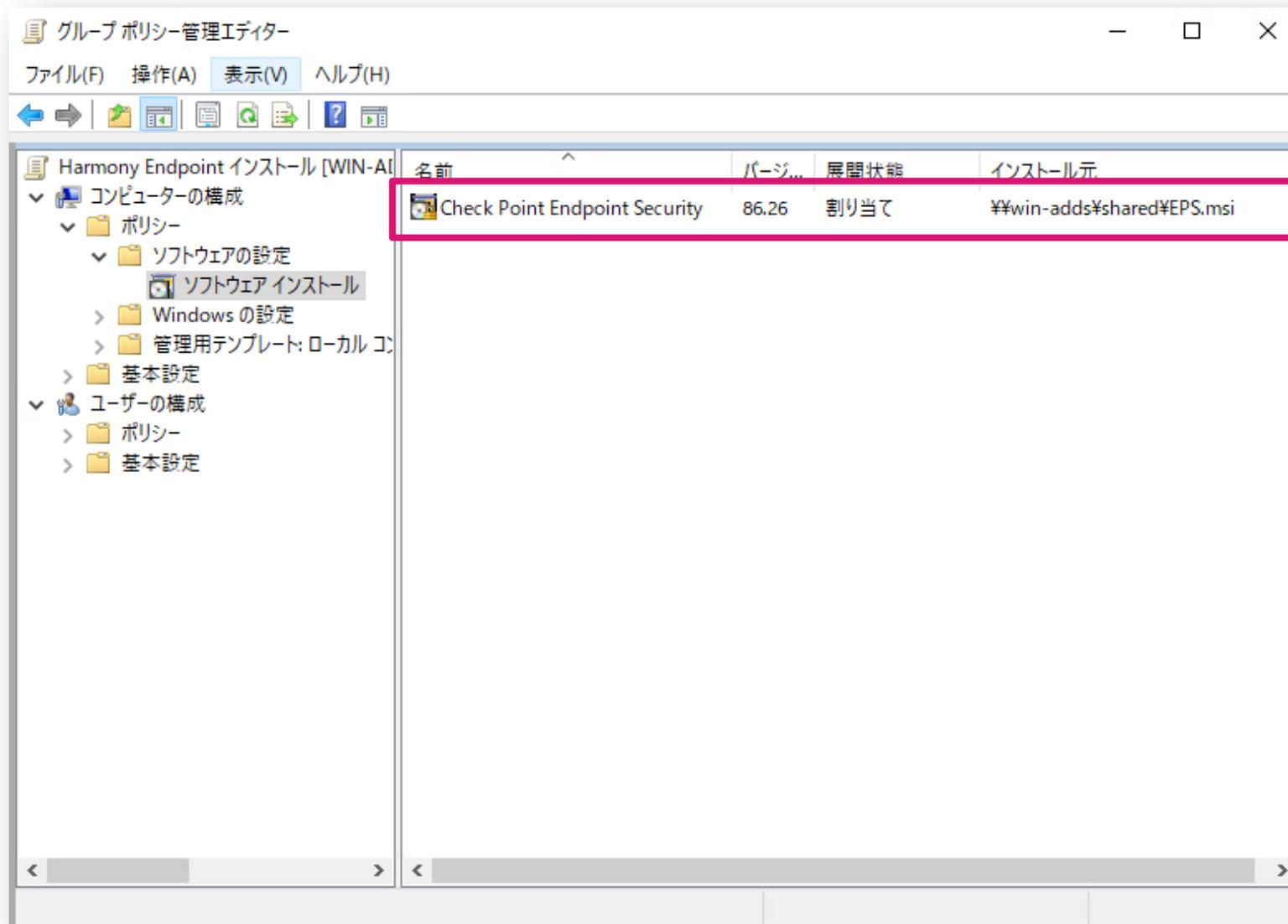
# パッケージの割り当て

# パッケージの割り当て

- グループポリシー管理エディタで、コンピューターの構成 > ソフトウェアの設定 > ソフトウェアインストール > 新規作成 > パッケージを選択
- インストーラパッケージを保存した共有フォルダのパスをUNCパスで指定
- ソフトウェアの展開方法で [割り当て] を選択



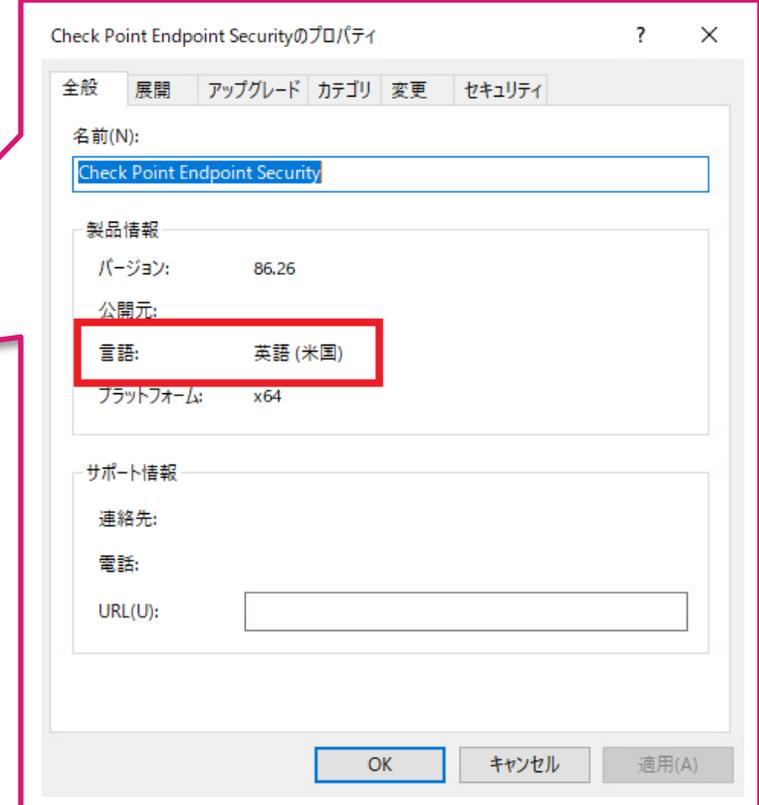
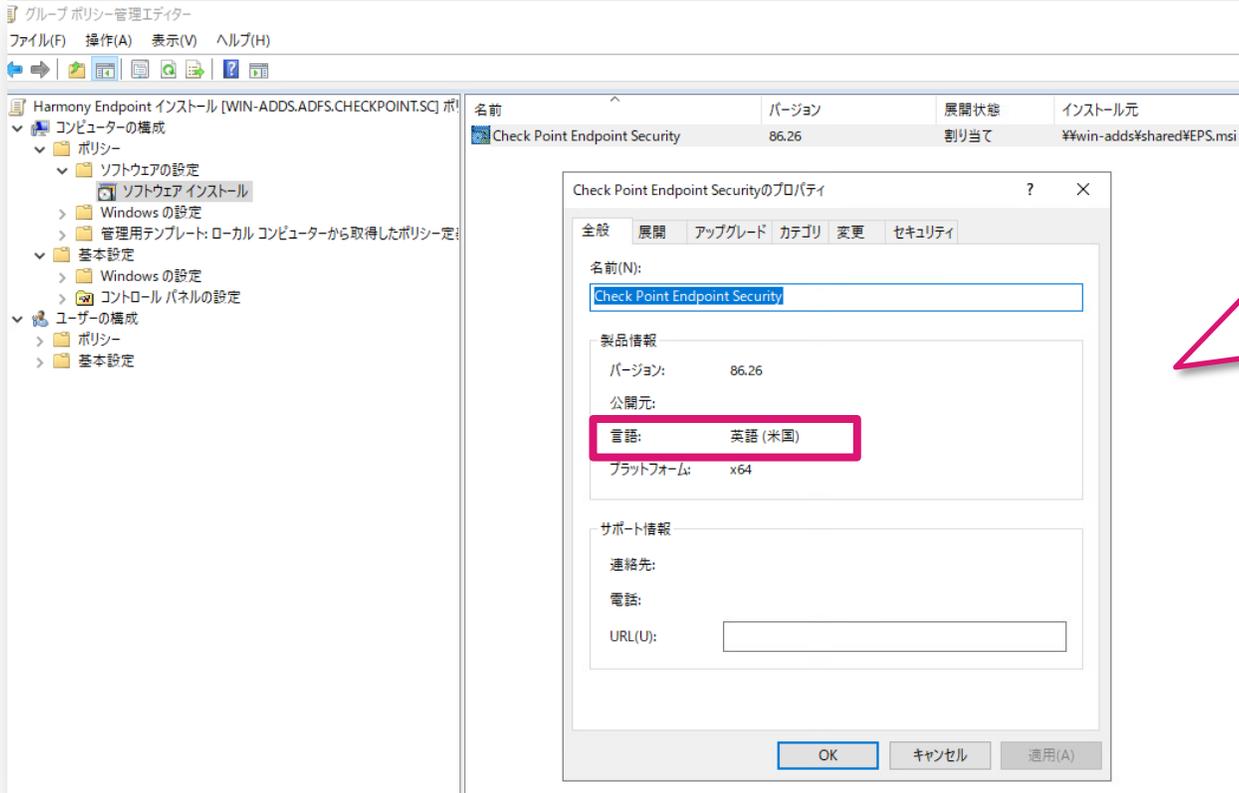
# パッケージの割り当て



# [言語を無視する] 設定

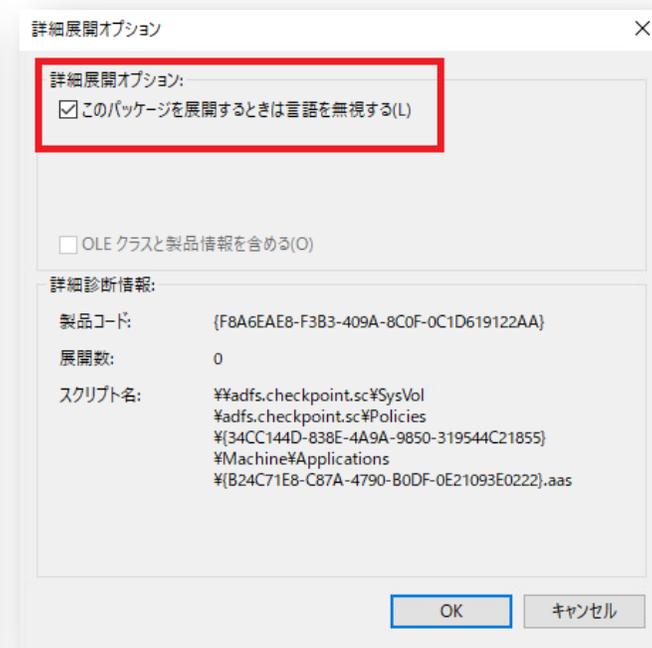
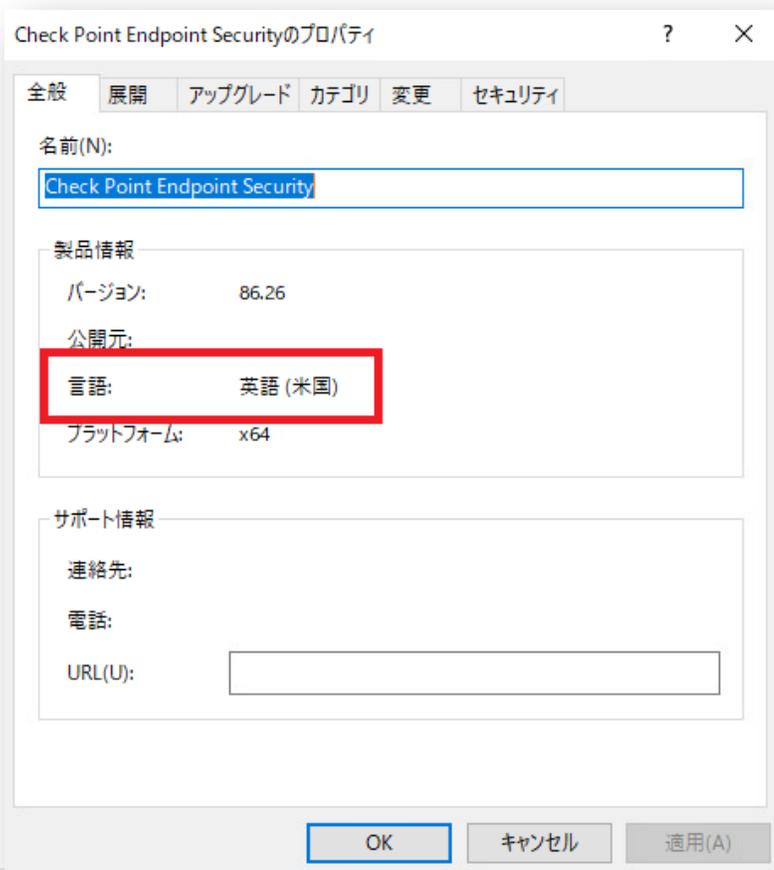
# 配布ソフトウェアの言語の確認

- 配布するソフトウェアのプロパティを表示
- [全般] タブに表示される [言語] を確認
- 表示された言語がクライアントパソコンのOSの言語設定と異なる場合、 [言語を無視する] 設定を行う必要がある



# [言語を無視する] 設定

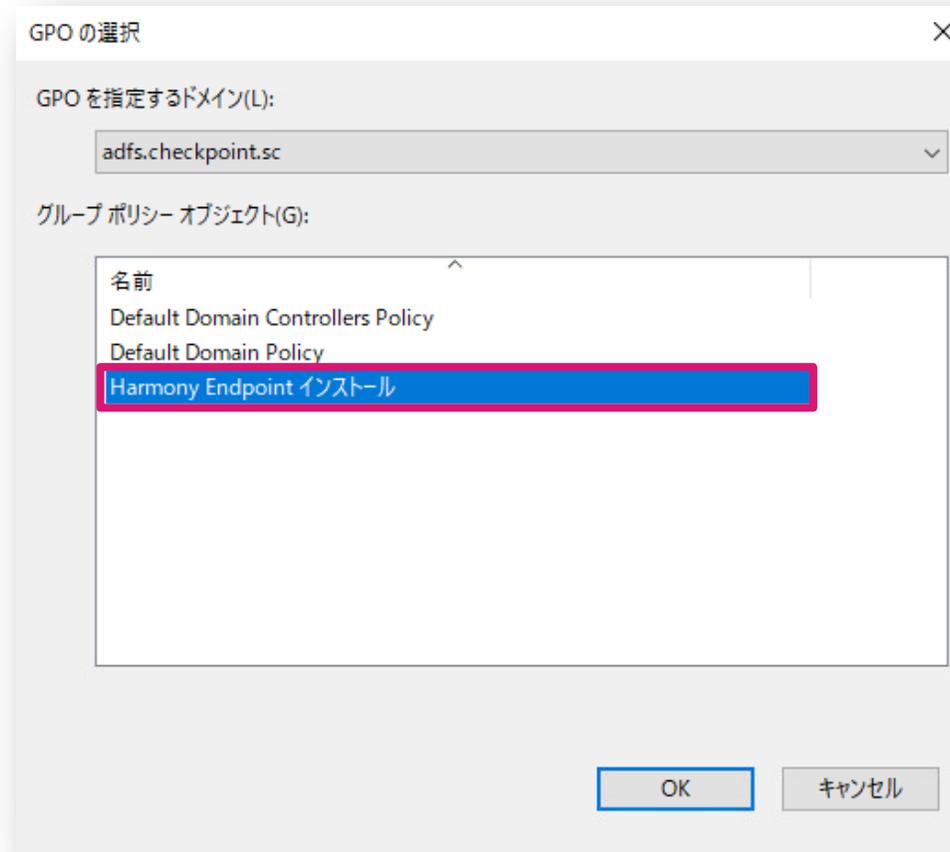
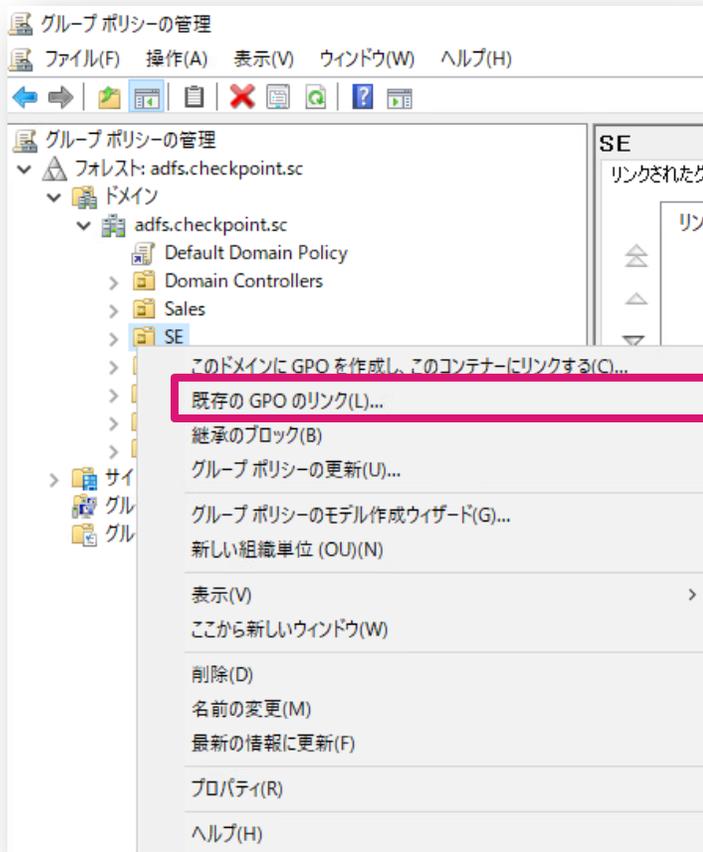
- 割り当てたパッケージを右クリックしてプロパティを表示
- [展開] タブの [詳細設定] をクリック
- [このパッケージを展開するときは言語を無視する] にチェックを入れ、OKを押下



GPOをOUへリンク

# GPOをOUへリンク

- GPOをリンクさせるOUを右クリックして、[既存のGPOのリンク] をクリック
- リンクさせるGPOを選択してOKを押下



# GPOをOUへリンク

The screenshot displays the Group Policy Management console with two windows. The background window shows the hierarchy of Group Policy Objects (GPOs) under the 'SE' folder. The foreground window shows the 'Harmony Endpoint インストール' GPO configuration page, specifically the 'リンク' (Link) tab.

**グループポリシーの管理 (Background Window)**

- グループポリシーの管理
- ファイル(F) 操作(A) 表示(V) ウィンドウ(W) ヘルプ(H)
- グループポリシーの管理
- フォレスト: adfs.checkpoint.sc
- ドメイン
- adfs.checkpoint.sc
- Default Domain Policy
- Domain Controllers
- Sales
- SE
- Harmony Endpoint インストール
- コンピューター
- ユーザー
- soumu
- グループポリシー オブジェクト
- WMI フィルター
- スターター GPO
- サイト
- グループポリシーのモデル作成
- グループポリシーの結果

**グループポリシーの管理 (Foreground Window)**

- グループポリシーの管理
- ファイル(F) 操作(A) 表示(V) ウィンドウ(W) ヘルプ(H)
- グループポリシーの管理
- フォレスト: adfs.checkpoint.sc
- ドメイン
- adfs.checkpoint.sc
- Default Domain Policy
- Domain Controllers
- Sales
- SE
- Harmony Endpoint インストール
- コンピューター
- ユーザー
- soumu
- グループポリシー オブジェクト
- WMI フィルター
- スターター GPO
- サイト
- グループポリシーのモデル作成
- グループポリシーの結果

**Harmony Endpoint インストール (Foreground Window)**

スコープ 詳細 設定 委任

**リンク**

表示するリンクの場所(L): adfs.checkpoint.sc

次のサイト、ドメイン、および OU がこの GPO にリンクされています(T):

場所	強制	リンクの有効化	パス
SE	いいえ	はい	adfs.checkpoint.sc/SE

**セキュリティ フィルター処理**

この GPO での設定は、次のグループ、ユーザーおよびコンピューターにのみ適用されます(S):

名前

Authenticated Users

追加(D)... 削除(R) プロパティ(P)

**WMI フィルター処理**

この GPO は次の WMI フィルターにリンクされています(W):

<なし> 開く(O)

# グループポリシーの適用結果の確認

# グループポリシーの適用結果の確認

- クライアント端末が起動する際に、グループポリシーが適用される
- クライアント端末でコマンドプロンプトを管理者権限で起動し、gpresult /R コマンドを実行

```
管理: コマンドプロンプト
Microsoft Windows [Version 10.0.19043.1706]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>gpresult /R

Microsoft (R) Windows (R) Operating System グループ ポリシーの結果ツール v2.0
Microsoft Corporation. All rights reserved.

作成日 2022/ 06/ 03 時刻 9:18:43

SOP のデータ ADFS#char - LAB-13 : ログ モード
-----
OS 構成:                メンバー ワークステーション
OS バージョン:          10.0.19043
サイト名:                Default-First-Site-Name
移動プロファイル:      N/A
ローカル プロファイル  C:\Users#char
低速リンクで接続:      いいえ

コンピューター設定
-----
DN=LAB-13,OU=コンピューター,OU=SE,DC=adfs,DC=checkpoint,DC=sc
前回のグループ ポリシーの適用時: 2022/06/03 (8:58:13)
グループ ポリシーの適用元:      WIN-ADDS.adfs.checkpoint.sc
グループ ポリシーの低速リンクのしきい値: 500 kbps
ドメイン名:              ADFS
ドメインの種類:          Windows 2008 またはそれ以降

適用されたグループ ポリシー オブジェクト
-----
Harmony Endpoint インストール
Default Domain Policy

次の GPO はフィルターで除外されたため適用されませんでした。
-----
ローカル グループ ポリシー
フィルター: 未適用 (空)

システムは次のセキュリティ グループの一部です
-----
BUILTIN\Administrators
Everyone
BUILTIN\Users
NT AUTHORITY\NETWORK
NT AUTHORITY\Authenticated Users
This Organization
Lab-13$
Harmony Endpoint Install
Domain Computers
登録期間によりアサートされた ID
System Mandatory Level

ユーザー設定
-----
DN=char,OU=ユーザー,OU=SE,DC=adfs,DC=checkpoint,DC=sc
前回のグループ ポリシーの適用時: 2022/06/03 (9:01:45)
グループ ポリシーの適用元:      WIN-ADDS.adfs.checkpoint.sc
グループ ポリシーの低速リンクのしきい値: 500 kbps
ドメイン名:              ADFS
ドメインの種類:          Windows 2008 またはそれ以降

適用されたグループ ポリシー オブジェクト
-----
N/A
```

```
管理: コマンドプロンプト
Microsoft Windows [Version 10.0.19043.1706]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>gpresult /R

Microsoft (R) Windows (R) Operating System グループ ポリシーの結果ツール v2.0
Microsoft Corporation. All rights reserved.

作成日 2022/ 06/ 03 時刻 9:13:43

RSOP のデータ ADFS#char - LAB-13 : ログ モード
-----
OS 構成:                メンバー ワークステーション
OS バージョン:          10.0.19043
サイト名:                Default-First-Site-Name
移動プロファイル:      N/A
ローカル プロファイル  C:\Users#char
低速リンクで接続:      いいえ

コンピューター設定
-----
DN=LAB-13,OU=コンピューター,OU=SE,DC=adfs,DC=checkpoint,DC=sc
前回のグループ ポリシーの適用時: 2022/06/03 (8:59:13)
グループ ポリシーの適用元:      WIN-ADDS.adfs.checkpoint.sc
グループ ポリシーの低速リンクのしきい値: 500 kbps
ドメイン名:              ADFS
ドメインの種類:          Windows 2008 またはそれ以降

適用されたグループ ポリシー オブジェクト
-----
Harmony Endpoint インストール
Default Domain Policy
```

# グループポリシーの適用結果の確認

- クライアント端末のイベントビューアーで、[Windows ログ > システム] を確認

The screenshot shows the Windows Event Viewer application. The left pane shows the navigation tree with 'Windows ログ' expanded to 'システム'. The main pane displays a list of events, with event ID 302 selected. The details pane shows the event message: 'アプリケーション Check Point Endpoint Security (ポリシー Harmony Endpoint インストール) が正しくインストールされました。' Below the message, the event properties are listed:

ログの名前(M):	システム	ログの日付(D):	2022/06/03 9:00:30
ソース(S):	Application Management Gro	タスクのカテゴリ(Y):	なし
イベント ID(E):	302	キーワード(K):	クラシック
レベル(L):	情報	コンピューター(R):	Lab-13.adfs.checkpoint.sc
ユーザー(U):	SYSTEM		
オペコード(O):	情報		
詳細情報(D):	<a href="#">イベント ログのヘルプ</a>		



THANK YOU

YOU DESERVE THE BEST SECURITY