CHECK POINT™

YOU DESERVE THE BEST SECURITY

HARMONY CONNECT INTERNET ACCESS 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

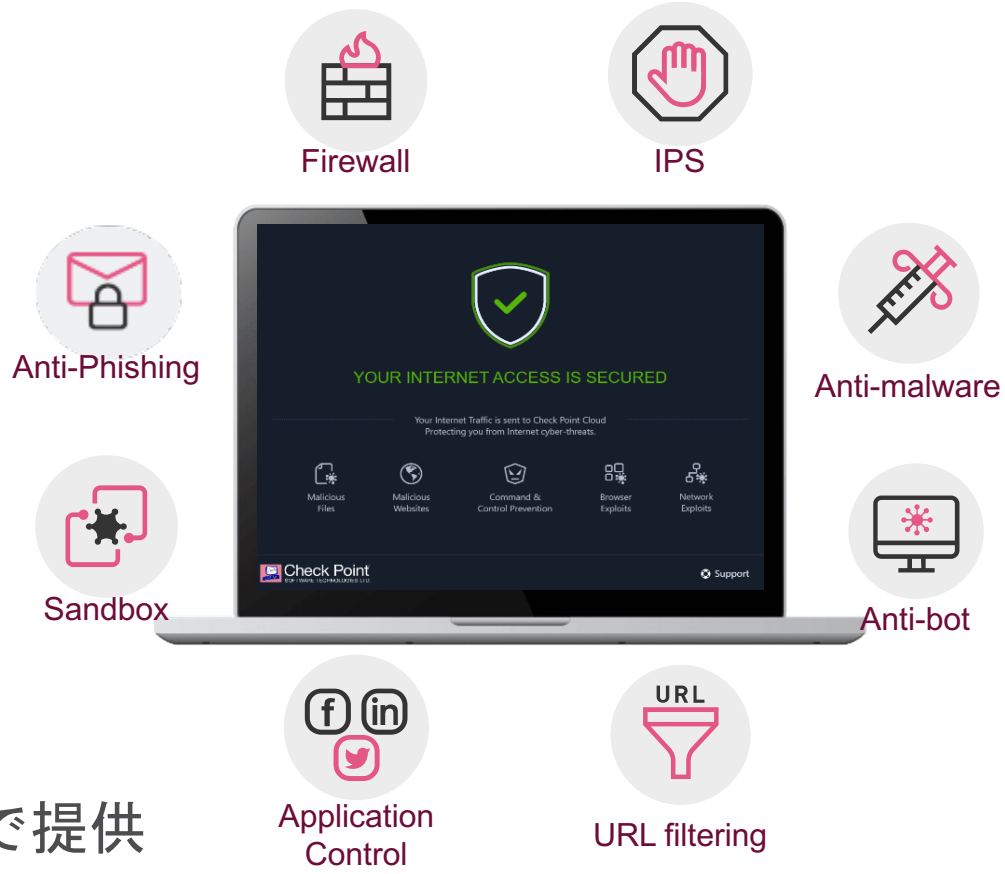
- 本ドキュメントは、検証、ハンズオン研修等での利用を目的としているため、一部の設定手順のみを記載しています。
- 本番環境の設定は、Administration Guide 等に基づいて行ってください。
- 本手順書と、Administration Guide、SK等の記述内容が異なる場合は、原則、本手順書以外のドキュメントの内容が優先されます。
- 本手順書は、2022年1月現在の設定内容、UI に基づいて作成されています。

Agenda

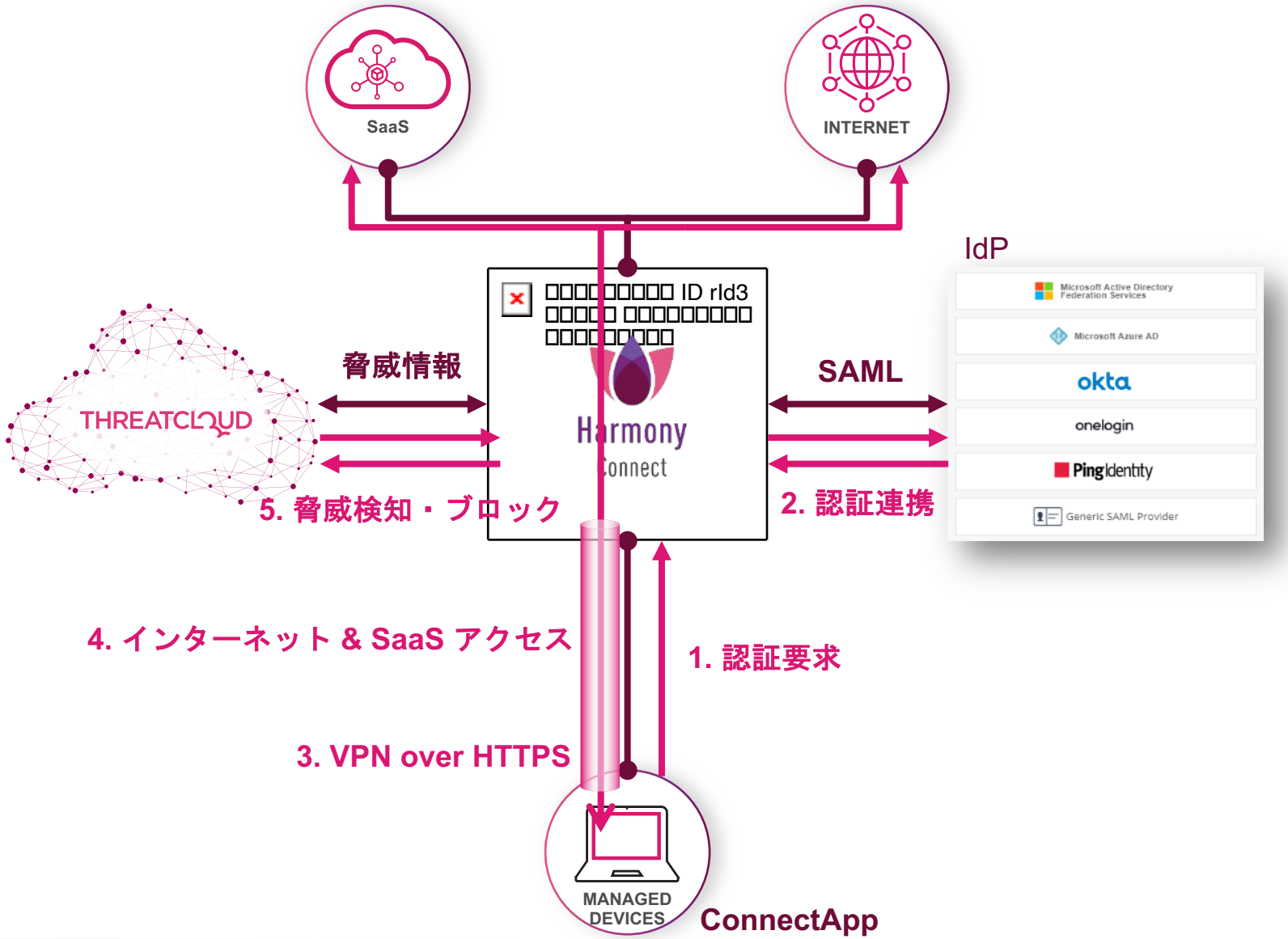
- HC-IA（Harmony Connect Internet Access） の特長
- HC-IA の動作概要
- 設定の流れ
- Infinity Portal へのサインイン
- Hamony Connect の有効化
- クラウドロケーションの設定
- ユーザの作成方法と注意点
- ユーザの作成［E メール］
- SSL INSPECTIONの設定
- インターネットアクセスポリシーの設定
- 注意点

HC-IA（Harmony Connect Internet Access）の特長

- **ゼロデイ・マルウェアやフィッシングからの高度な保護**
  - すべてのポートを対象とするThreat Prevention
  - SSL FULL INSPECTION
  - 第三者機関による評価での高い実績
- **シンプルで使いやすい統合管理機能**
  - 直感的に使えるユーザインタフェース
  - Infinity ソリューションの管理を一元化
  - グラフィカルなWeekly Report
- **コスト最適化されたライセンス体系**
  - すべてのセキュリティ機能をオールインワンで提供



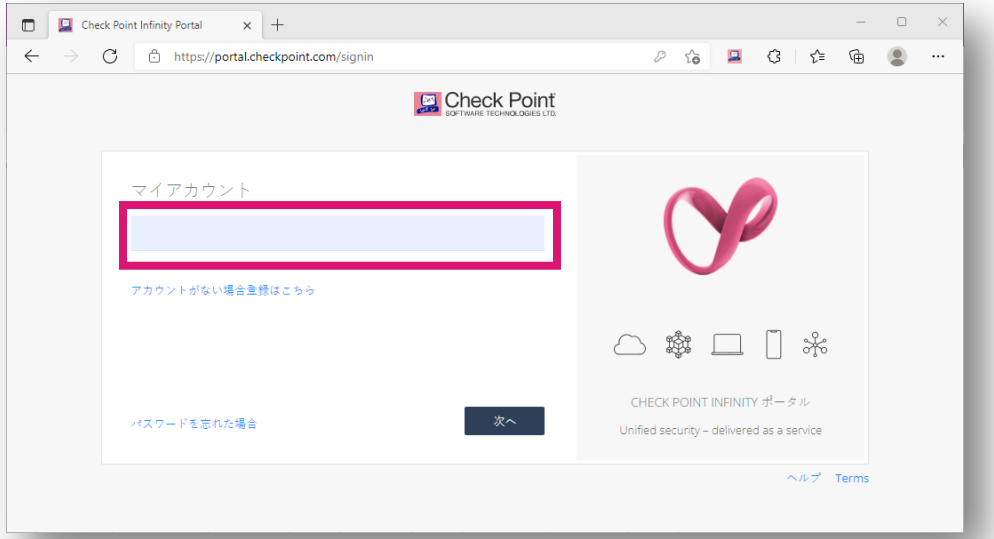
HC-IA の動作概要



1. ConnectAppがHamony Connect へ認証要求
2. Hamony Connect とIdPが認証連携
3. Hamony Connect にVPN over HTTPS で接続
4. インターネットや SaaS へアクセス
5. Harmony Cloud と Threat Cloud が連携して脅威を検知、ブロック

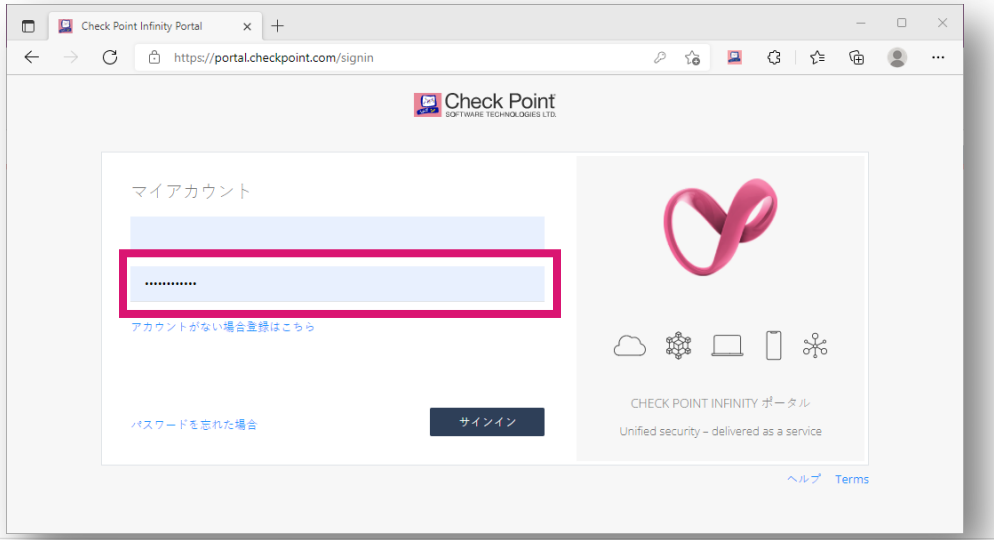
設定の流れ

Infinity Portal へのサインイン



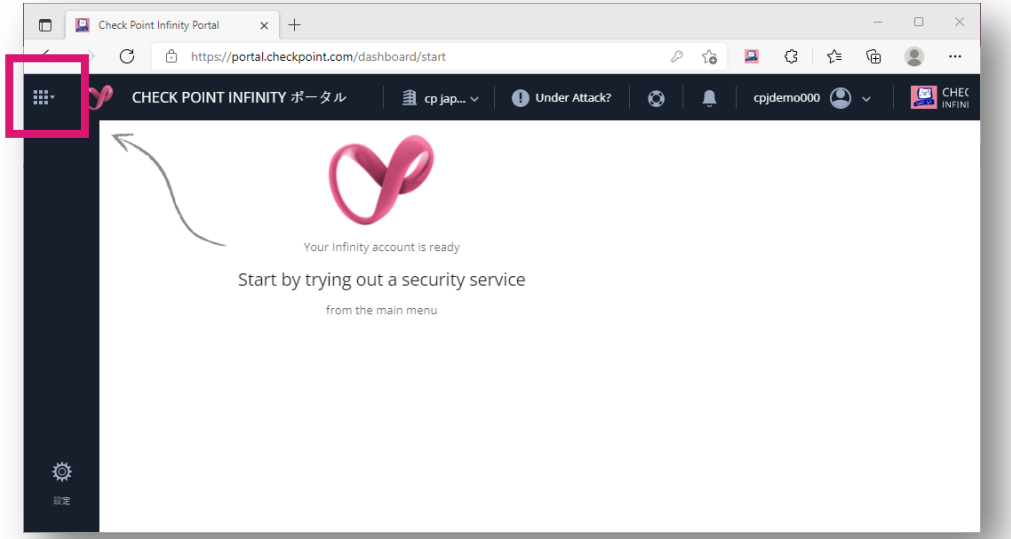
1. Infinity Portal へ接続する
   - URL: https://portal.checkpoint.com/

2. ユーザ名を入力して、「次へ」を押す

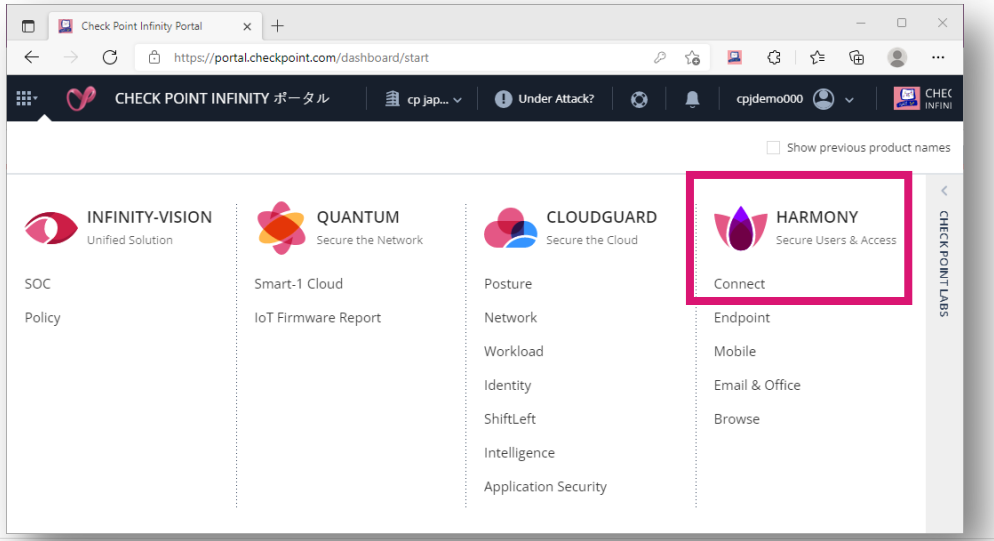


3. パスワードを入力して、「サインイン」を押す

Harmony Connect の有効化（１／２）

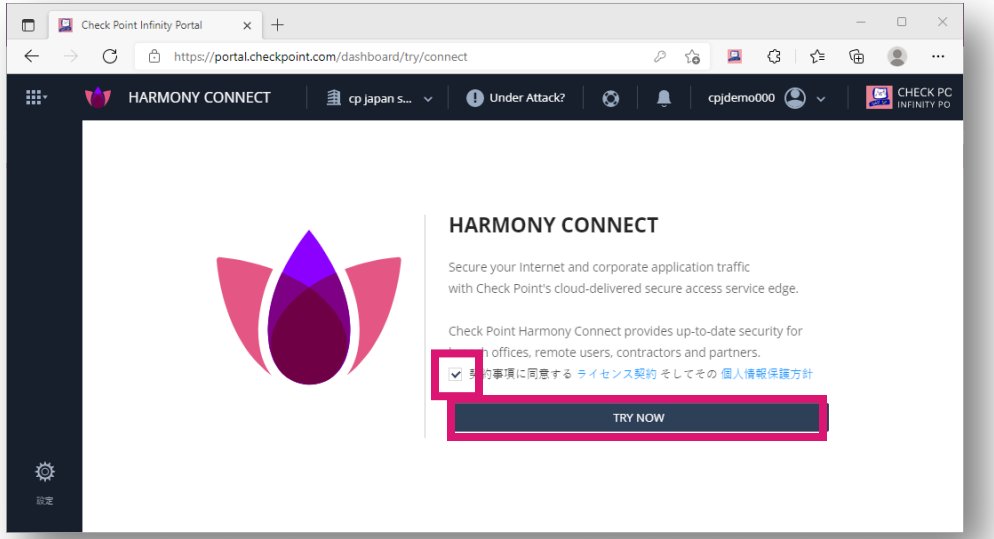


1. 左上のメニューボタン  を押す

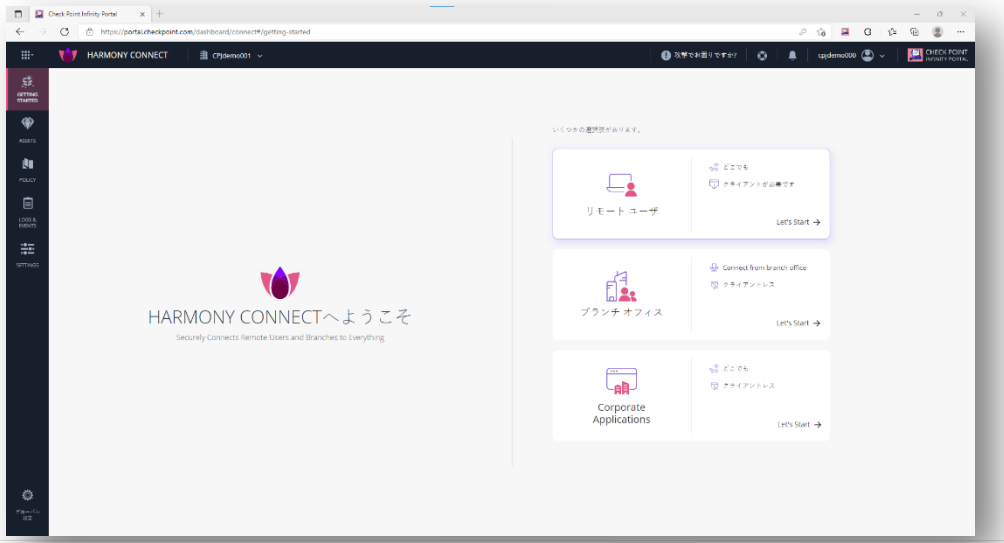


2. 「HARMONY Connect」を選択する

Harmony Connect の有効化（２／２）

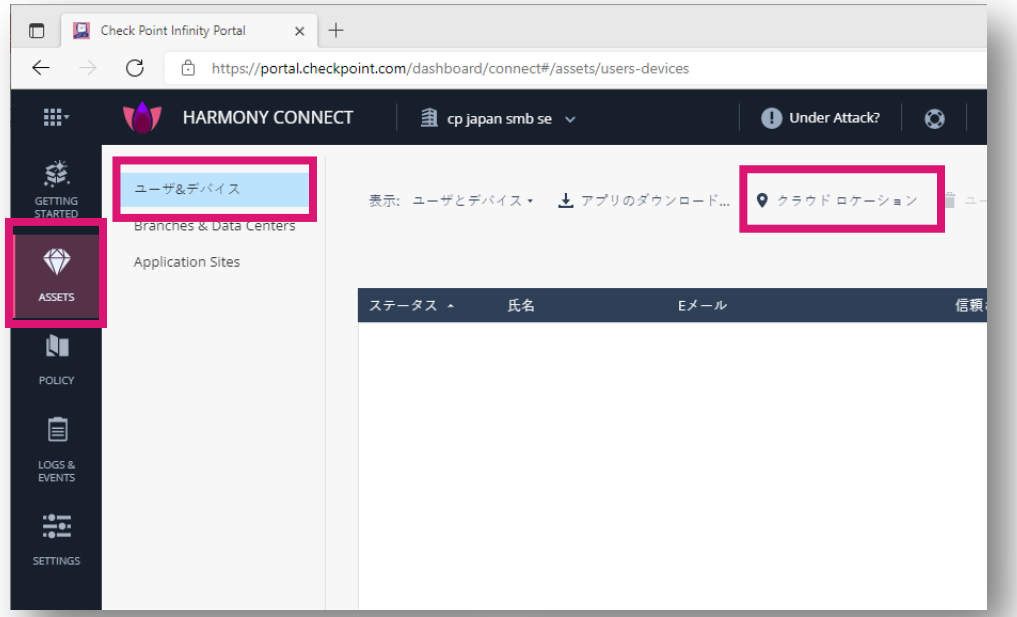


3. 「契約事項に同意する」のチェックボックスにチェックを入れ、「TRY NOW」を押す



4. HARMONY Connect の有効化が完了

クラウドロケーションの設定



1. 「ASSETS ＞ ユーザ＆デバイス」を選択する
2. 「クラウドロケーション」を押す

3.  を押してロケーションを表示する
4. 「Asia: Japan East」か、「Asia: Japan West」を選択して、「アップデート」を押す
5. ロケーションの設定が完了

ユーザの作成方法と注意点

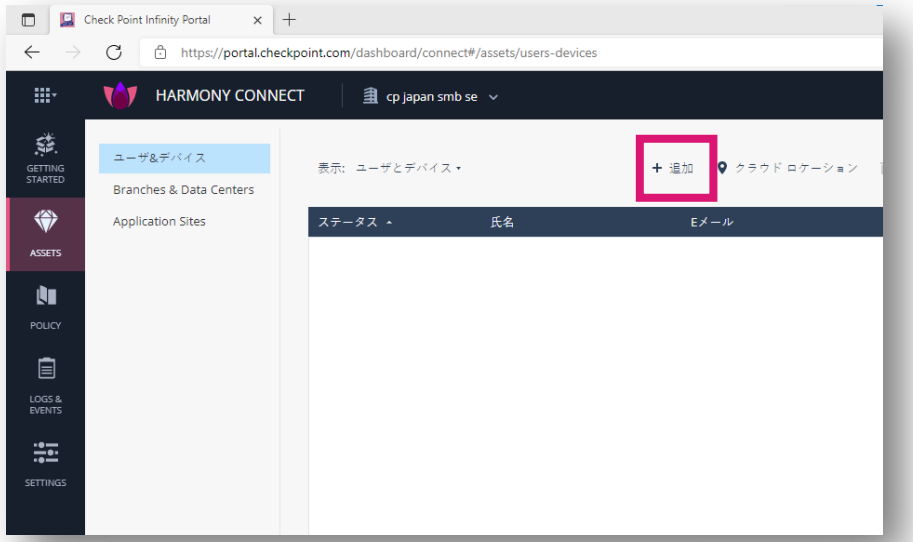
- Hamony Connect のユーザの作成方法は、２通り
  - E メール（by email）→ ローカル DB
  - ID プロバイダを使用
    - ２つの方法の比較は、sk173623 を参照する

- ID プロバイダを使用すると、E メールでのユーザ作成はできなくなる

- インターネットアクセスポリシーのソース（送信元）にグループを指定できるのは、ID プロバイダを使用した時のみ

- ユーザとグループを自動同期できる ID プロバイダは、Azure AD、Okta、PingID のみ

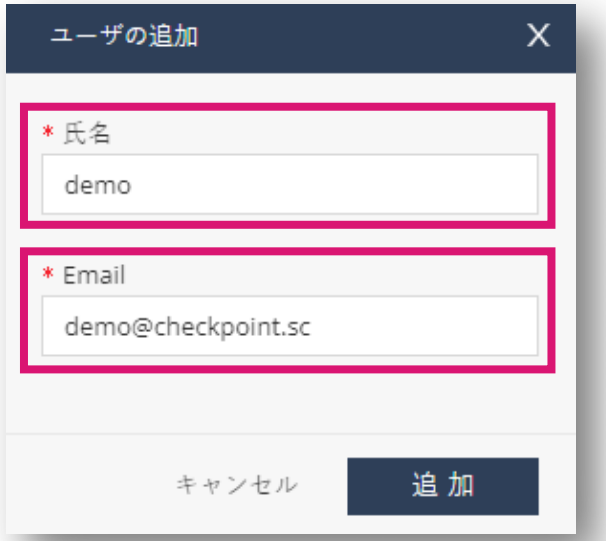
ユーザの作成［E メール］（１／３）



1. 「ASSETS > ユーザ＆デバイス」を選択する
2. 「追加」を押す

3. 「新規」を押す

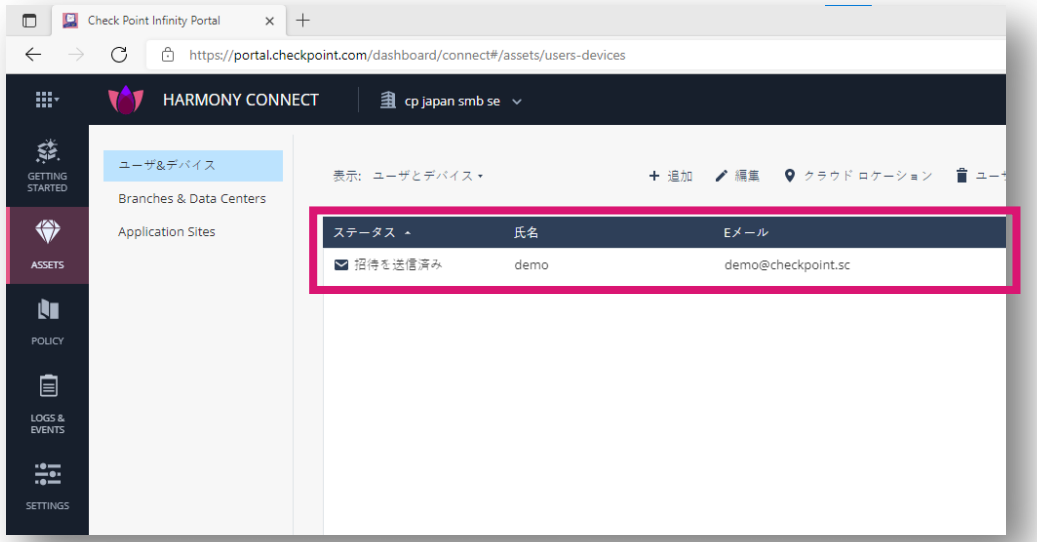
ユーザの作成［E メール］（２／３）



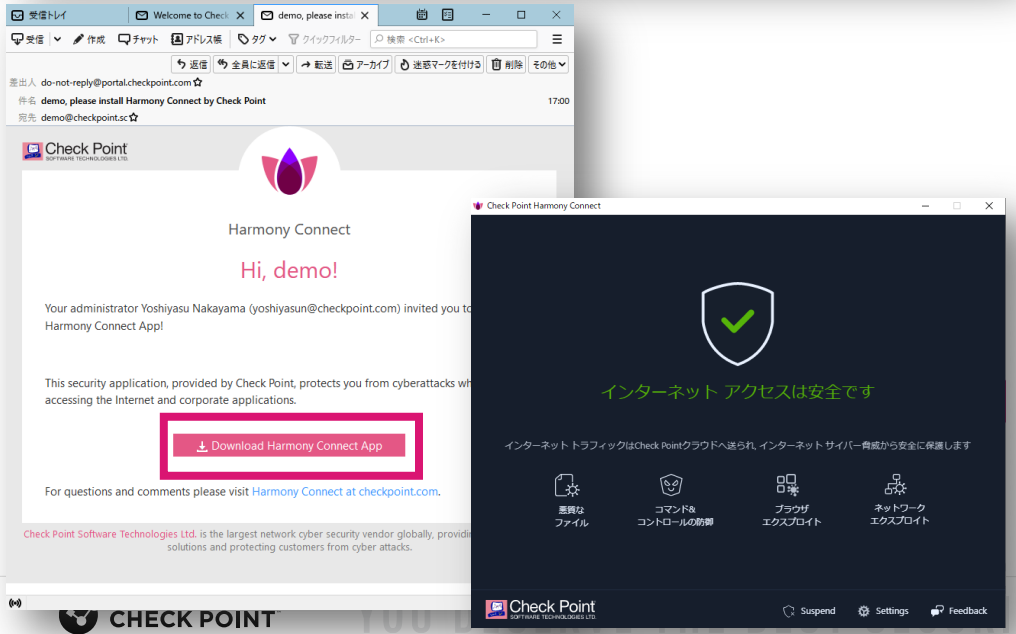
4. 「氏名」、「Email」を入力して「追加」を押す

5. 「Harmony Connectアプリをインストールしてインターネット アクセスを保護」にチェックを入れて、「OK」を押す
   - Harmony Connect Remote Accessを利用する際は、「ユーザ アプリ ポータルで企業のアプリケーション アクセスを安全に保護」にもチェックを入れる

ユーザの作成［E メール］（３／３）

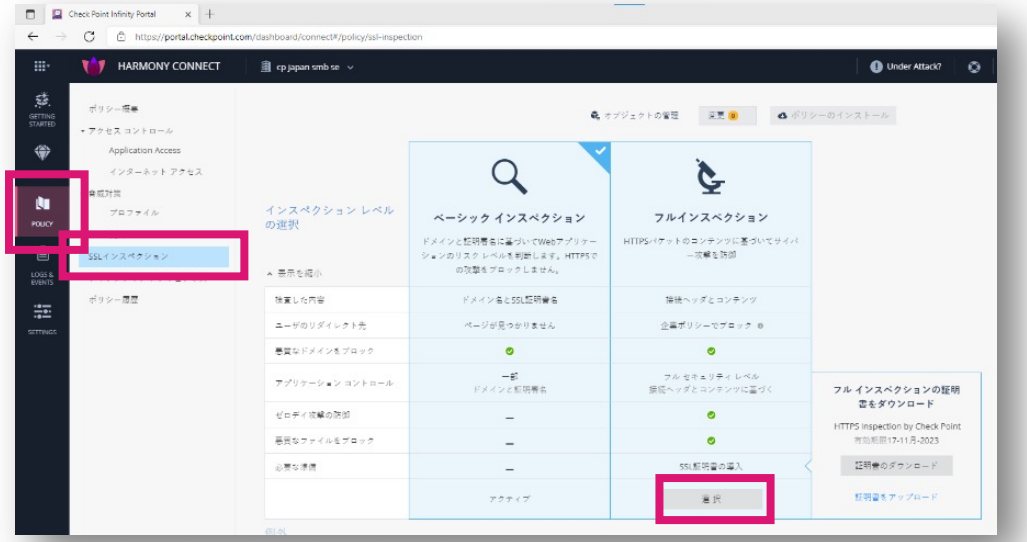


6. Infinity Portalから、ユーザに招待メールが送信される



7. 招待メールを受信したユーザは、メール本文の「Download Harmony Connect App」をクリックし、インストーラをダウンロードする
8. インストーラをダブルクリックしてインストールすると、自動でHarmony Connectへの接続が完了する

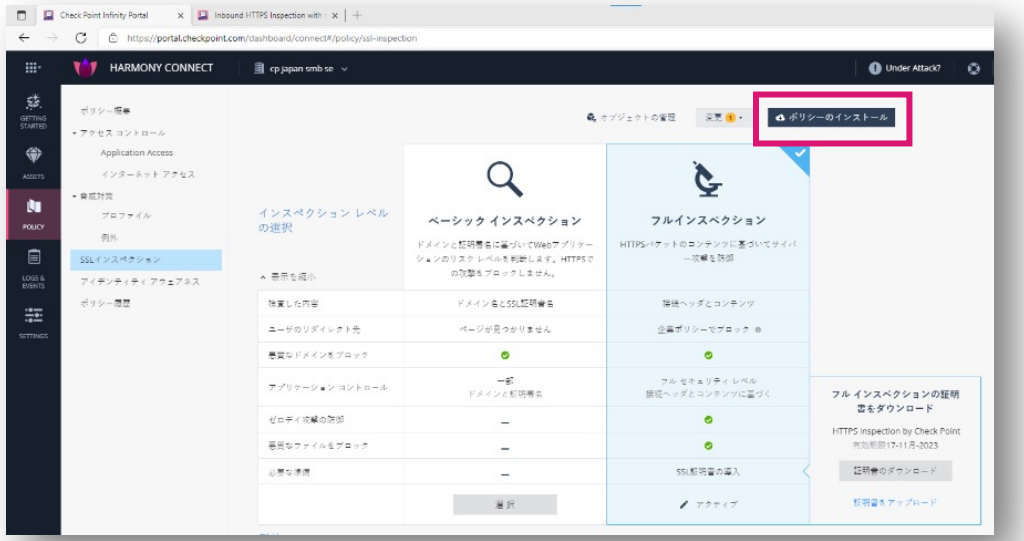
SSL INSPECTIONの設定（１／３）



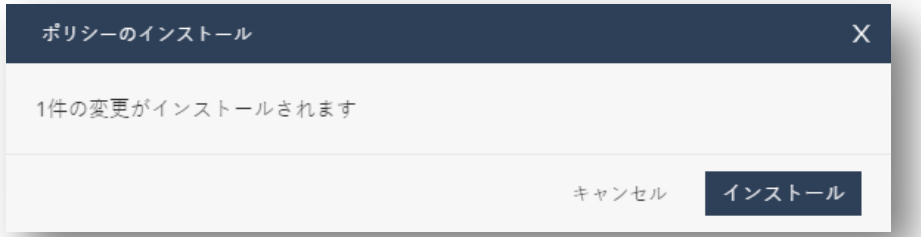
1. 「POLICY ＞ SSL インスペクション」を選択する
2. 「フルインスペクション」の「選択」を押す

3. 「HTTS フルインスペクションを有効にする」ダイアログボックスで、「“HTTPS（略）に導入しました」チェックボックスにチェックを入れ「続行」を押す

SSL INSPECTIONの設定（２／３）

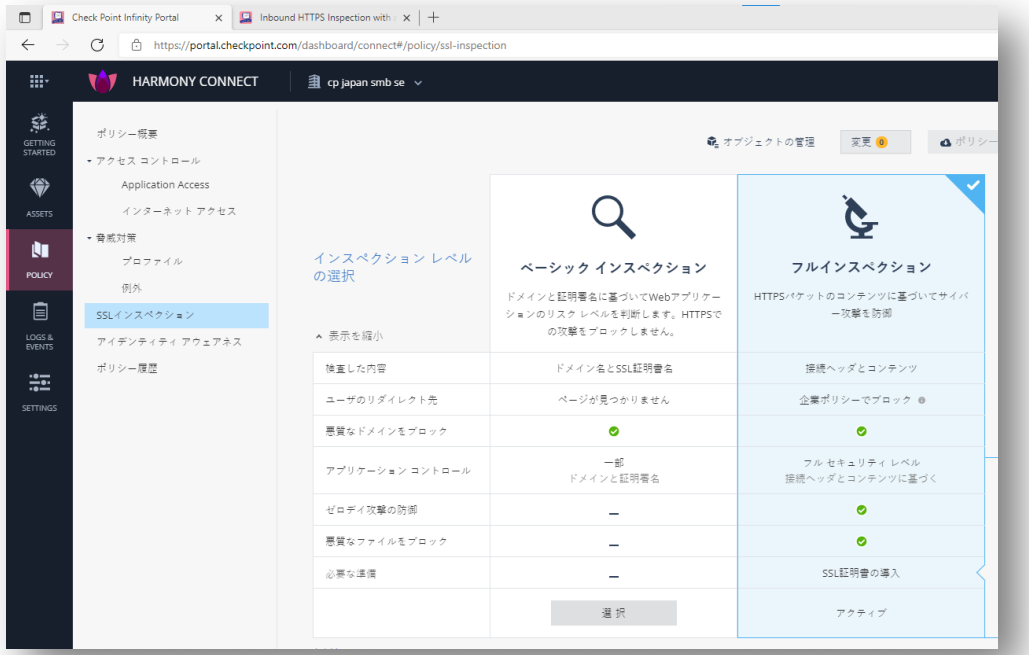


4. 「ポリシーのインストール」を押す



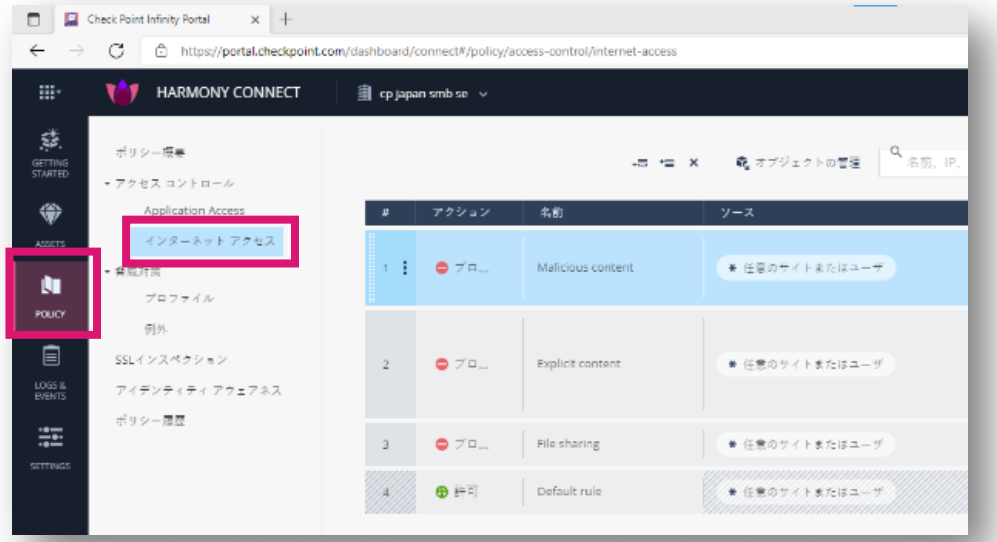
5. 「ポリシーのインストール」ダイアログボックスで、「インストール」を押す

SSL INSPECTIONの設定（３／３）

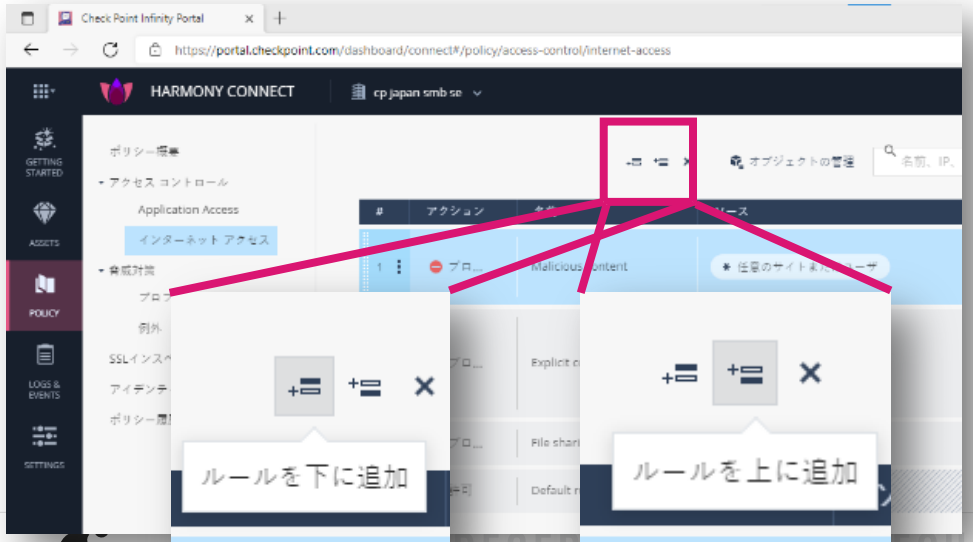


6. フルインスペクションの設定が完了

インターネットアクセスポリシーの設定



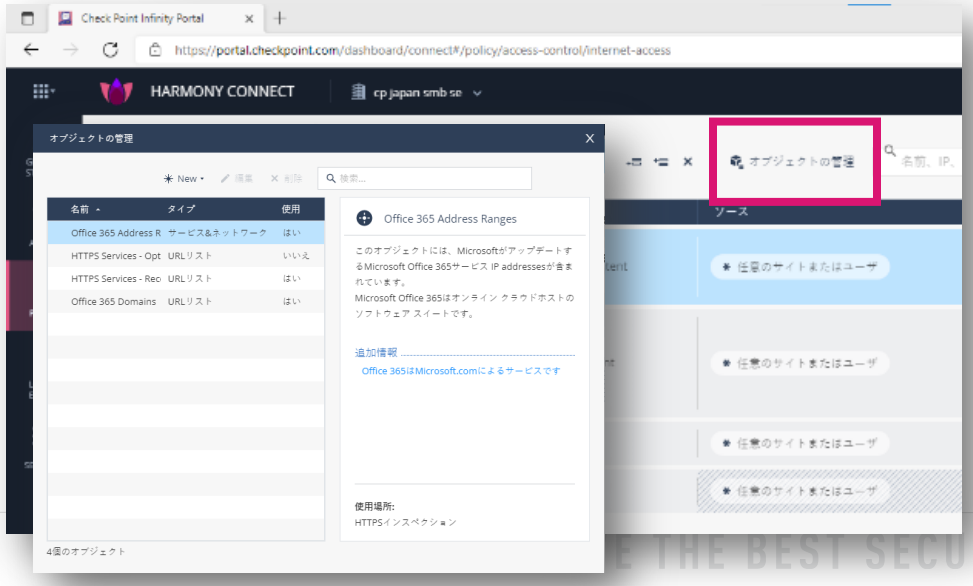
1. 「POLICY ＞ インターネットアクセス」を選択する



2. 新規ルールを追加する
   -  を押す
   - 選択しているルールの下もしくは、上にルールが追加される

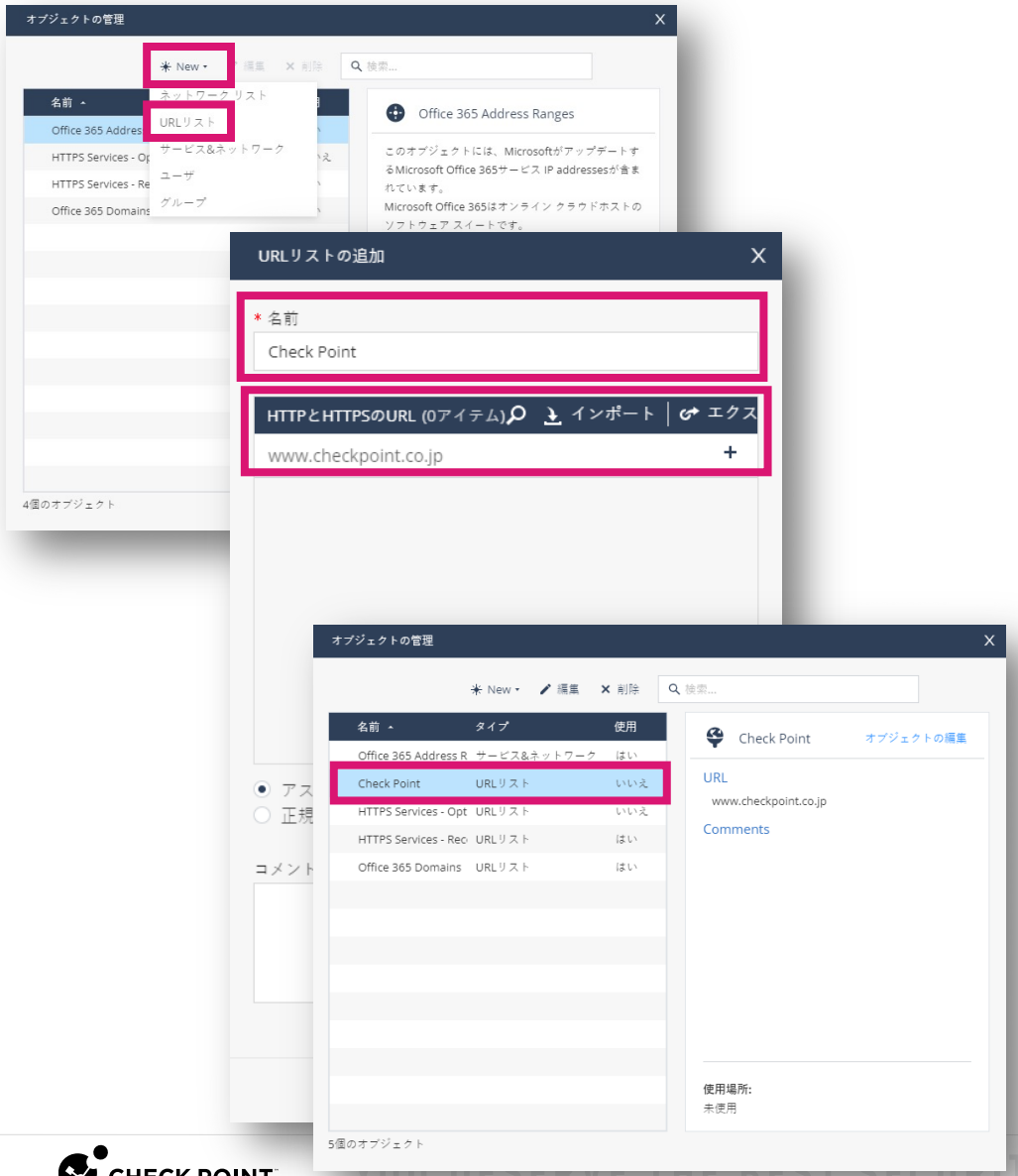
インターネットアクセスポリシーの設定

3. ルール名を付与する
   - 「名前」欄をクリックすると、ルール名を入力できる



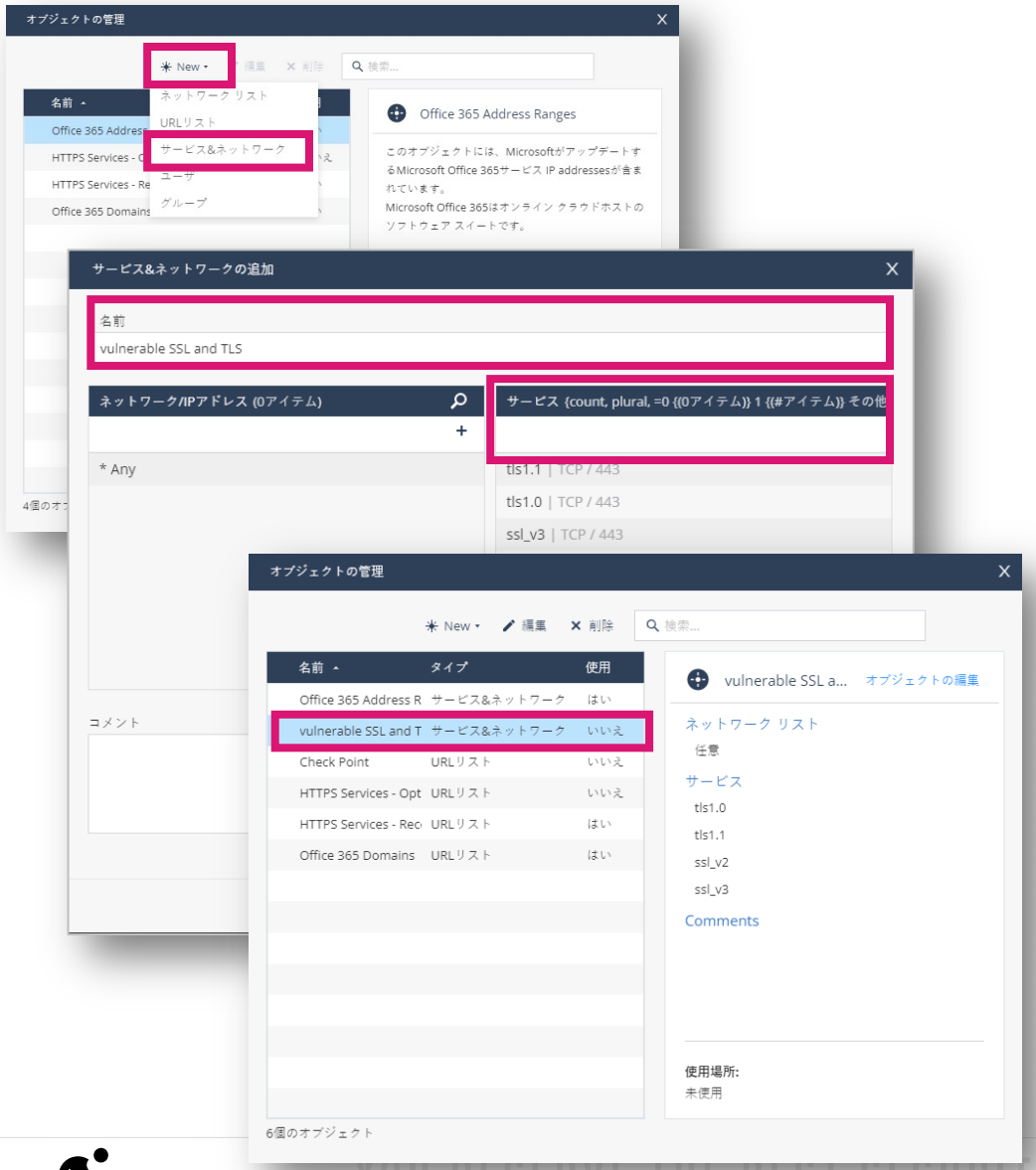
4. オブジェクトを追加する
   - 「オブジェクトの管理」を押すと、「オブジェクトの管理」ダイアログボックスが表示される

インターネットアクセスポリシーの設定



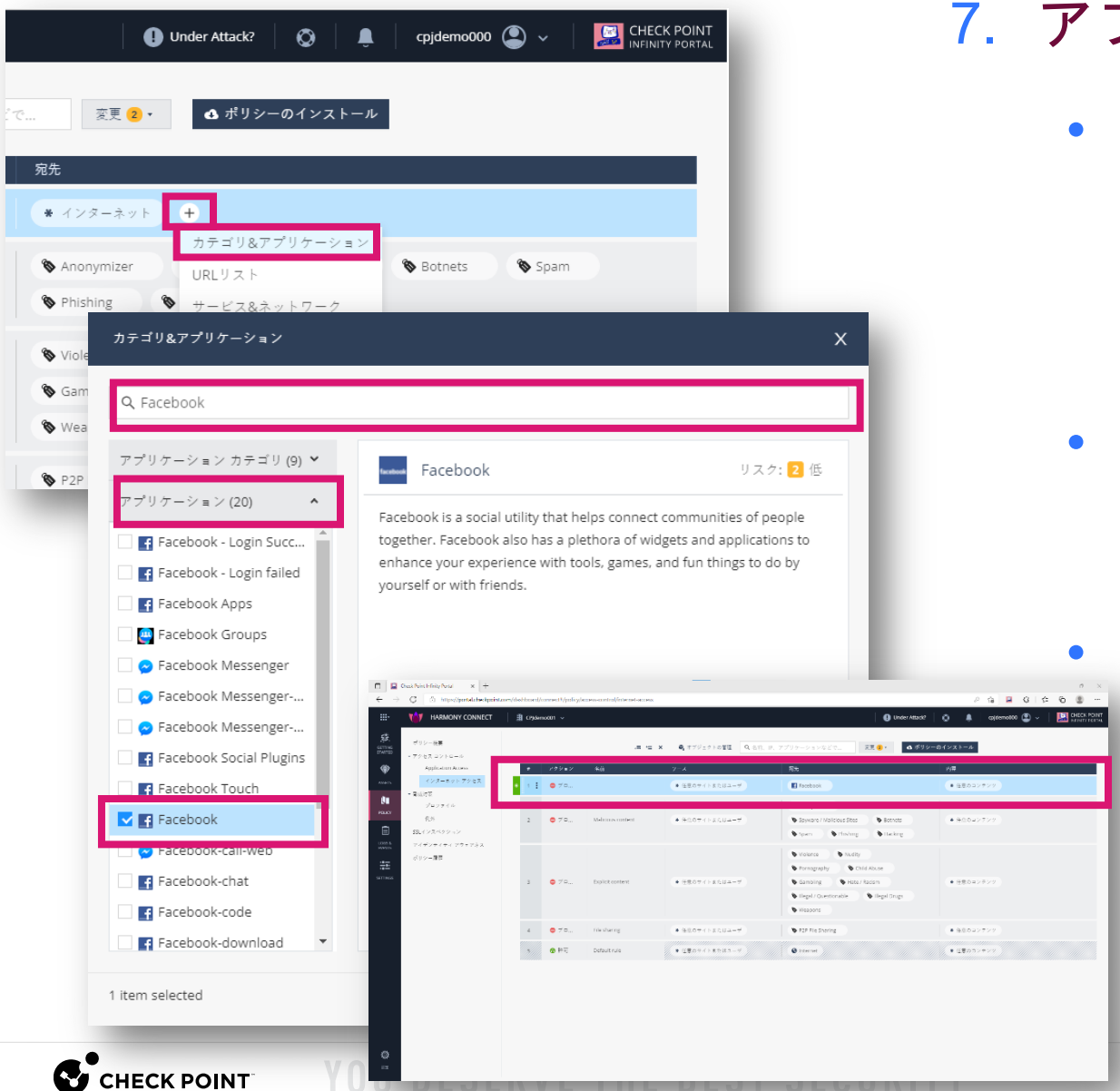
5. URLリストを追加する
   - 「New」を押して「URLリスト」を選択する
   - 「URLリストの追加」ダイアログボックスが表示される
   - 「名前」と宛先の「ドメイン」を入力して、「追加」を押すとオブジェクトに追加される

インターネットアクセスポリシーの設定



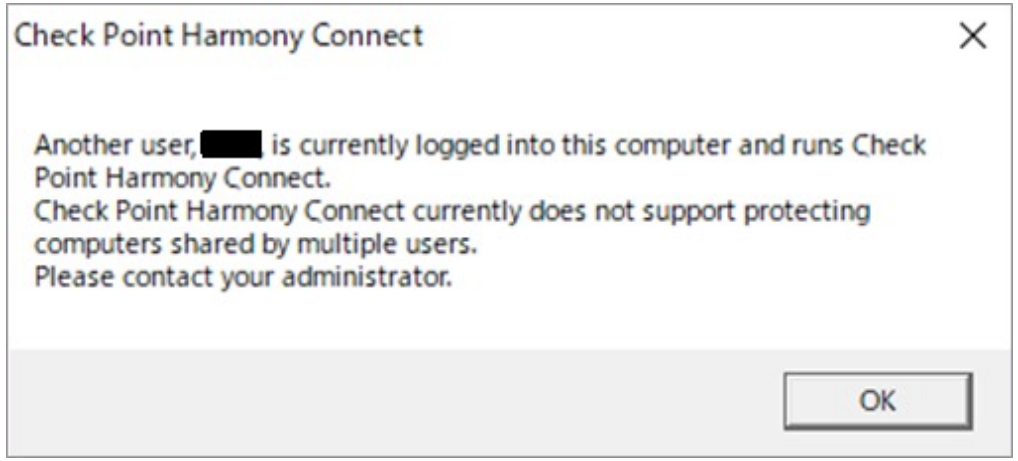
6. サービス＆ネットワークを追加する
   - 「New」を押して「サービス＆ネットワーク」を選択する
   - 「サービス＆ネットワークの追加」ダイアログボックスが表示される
   - 「名前」と、宛先の「ネットワークIPアドレス」、「サービス」を入力して、「追加」を押すとオブジェクトに追加される

インターネットアクセスポリシーの設定



7. アプリケーションを禁止する
   - 編集したいルールの「宛先」欄の「＋」を押して、「カテゴリ＆アプリケーション」を選択する
   - 「カテゴリ＆アプリケーション」ダイアログが表示される
   - 禁止したいアプリケーション名を入力し、「アプリケーション」欄からアプリケーションを選択し、「Add」ボタンを押す

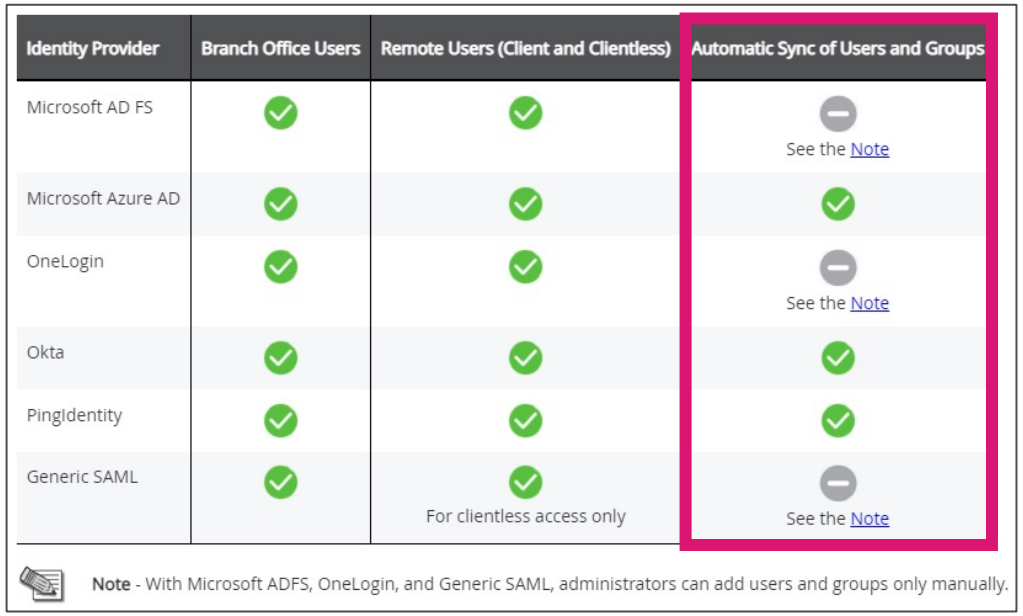
注意点（１／３）



Threat Prevention Function	Supported Protocol
Threat Emulation	HTTP/HTTPS
IPS	ANY
Anti-Bot	ANY
Anti-Virus	HTTP/HTTPS
URL Filter	HTTP/HTTPS
Application Control	ANY

1. 現在は、共用端末での複数のユーザの保護はサポートしていない。最初にConnect Appをインストールしたユーザのみ保護可能
   - あるユーザで Harmony Connect へのサインインを完了した後に、別のユーザが ConnectApp の起動を試みるとエラーメッセージが表示される
2. Threat Prevention の各機能に対応しているプロトコルは、左表のとおり

注意点（２／３）

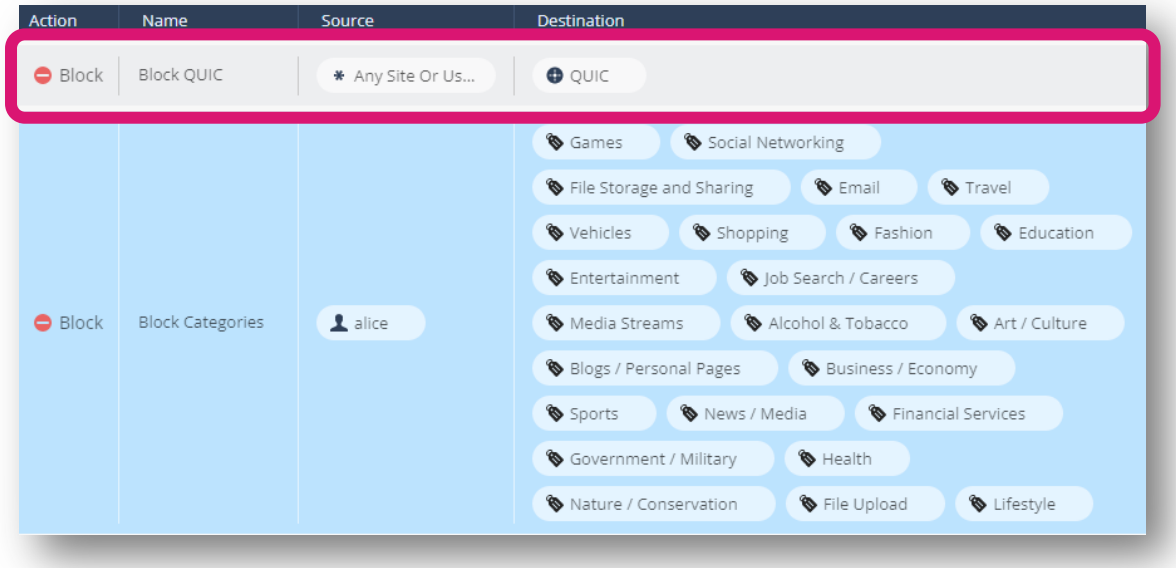


Identity Provider	Branch Office Users	Remote Users (Client and Clientless)	Automatic Sync of Users and Groups
Microsoft AD FS	✓	✓	⊖ See the Note
Microsoft Azure AD	✓	✓	✓
OneLogin	✓	✓	⊖ See the Note
Okta	✓	✓	✓
PingIdentity	✓	✓	✓
Generic SAML	✓	✓ For clientless access only	⊖ See the Note

Note - With Microsoft ADFS, OneLogin, and Generic SAML, administrators can add users and groups only manually.

3. ID プロバイダ使用時に、「ユーザ」と「グループ」が自動同期して、アクセスポリシーのソース（送信元）オブジェクトとして使用できるのは、Azure AD、Okta、PingID のみ
   - Microsoft AD FS、OneLogin、Generic SAML 使用時は、「ユーザ」と「グループ」は、手動で追加する必要がある
   - E メールでユーザを作成した場合は、アクセスポリシーのソース（送信元）としてグループを指定することはできない。グループを指定できるのは ID プロバイダを使用した場合のみ

注意点（３／３）



4. SSL FULL INSPECTIONは、QUIC プロトコルに対応していないため、QUICプロトコルを使用する Web サイトへのアクセスを制御するためには、QUIC プロトコルを Block するルールを作成する必要がある

YOU DESERVE THE BEST SECURITY

THANK YOU