CHECK POINT™

YOU DESERVE THE BEST SECURITY

HARMONY CONNECT IDプロバイダ連携 簡易設定ガイド ~ AZURE AD 編~

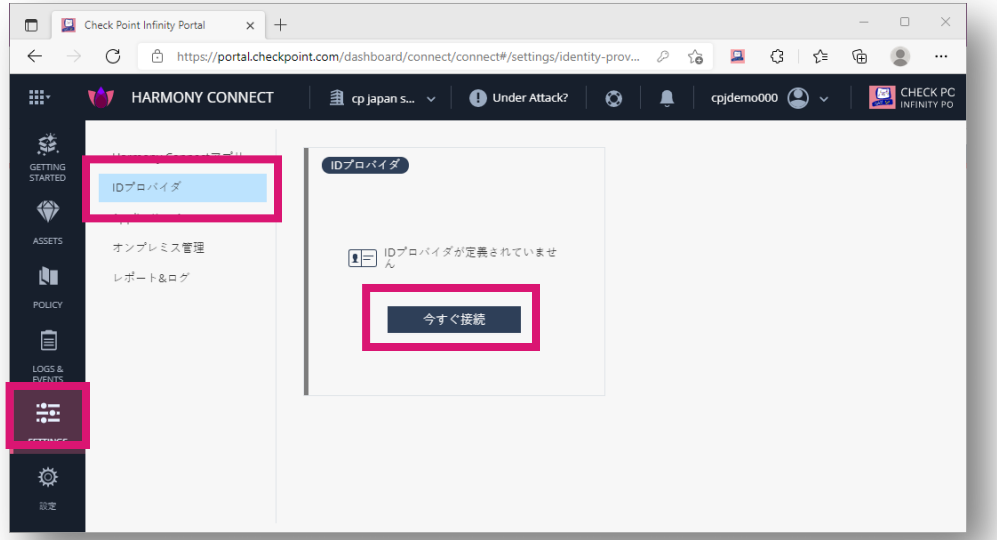
チェック・ポイント・ソフトウェア・テクノロジーズ株式会社
システム・エンジニアリング本部

- 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。

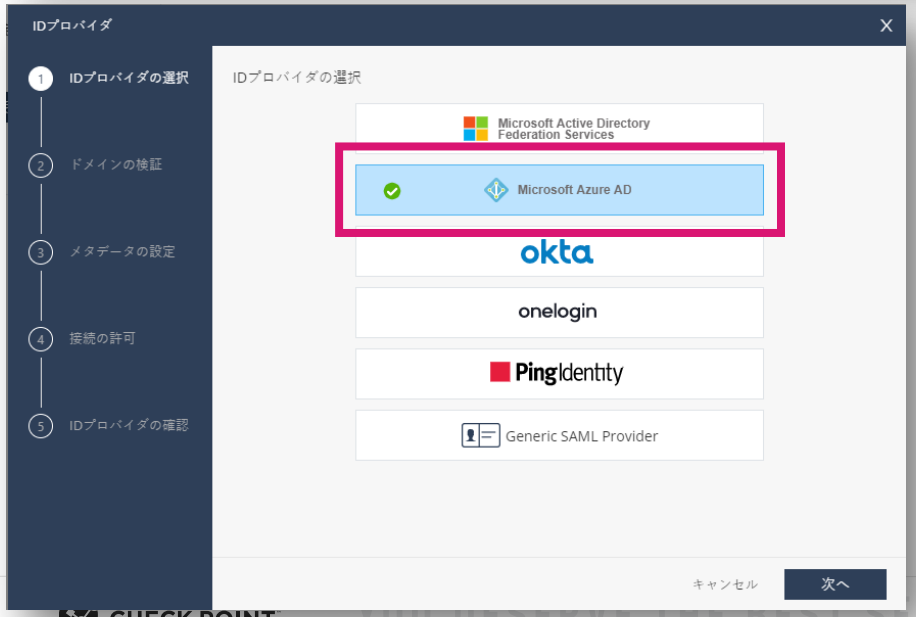
Agenda

- ユーザの作成［Azure AD 連携］
- ConnectApp のマニュアルインストール
- AzureAD での認証連携設定

ユーザの作成［Azure AD 連携］（１／６）

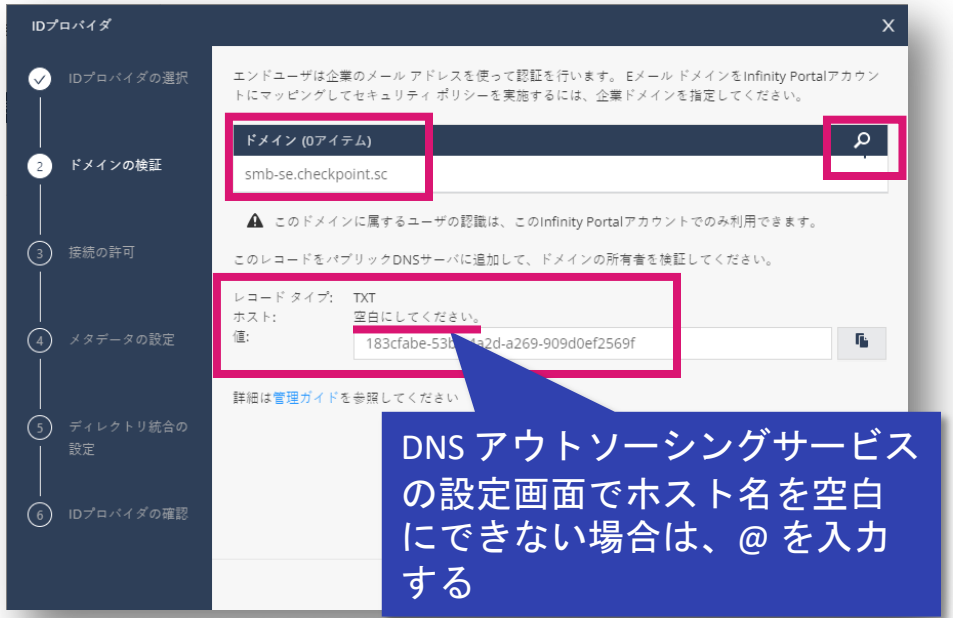


1. 「SETTINGS > ID プロバイダ」を選択する
2. 「今すぐ接続」を押す



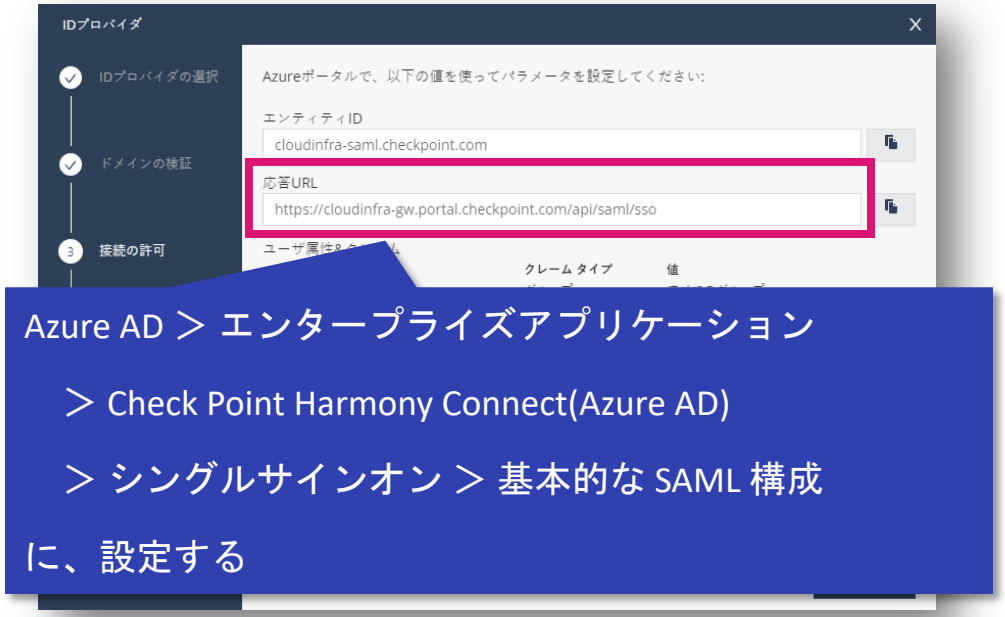
3. 「Microsoft Azure AD」を選択して、「次へ」を押す

ユーザの作成［Azure AD 連携］（２／６）



4. 登録するドメインを管理する DNS サーバの TXTレコードに表示されている値を設定する
5. Azure AD のドメイン名を入力して、「＋」を押す
   - 「＋」は隠れ気味の時があるので注意
6. ドメイン認証に成功したことを確認して、「次へ」を押す

ユーザの作成［Azure AD 連携］（３／６）



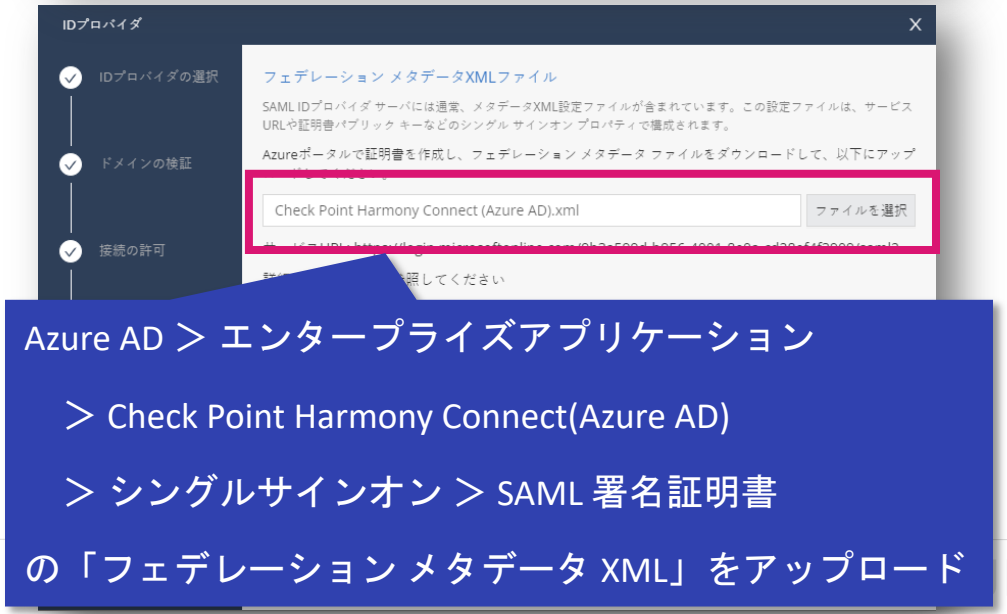
Azure AD ＞ エンタープライズアプリケーション

＞ Check Point Harmony Connect(Azure AD)

＞ シングルサインオン ＞ 基本的な SAML 構成

に、設定する

7. 応答 URL を、Azure AD へ設定して、「次へ」を押す
   - Azure AD のギャラリーアプリケーションを使用する場合、エンティティ ID は設定済みのため入力不要



Azure AD ＞ エンタープライズアプリケーション

＞ Check Point Harmony Connect(Azure AD)

＞ シングルサインオン ＞ SAML 署名証明書

の「フェデレーション メタデータ XML」をアップロード

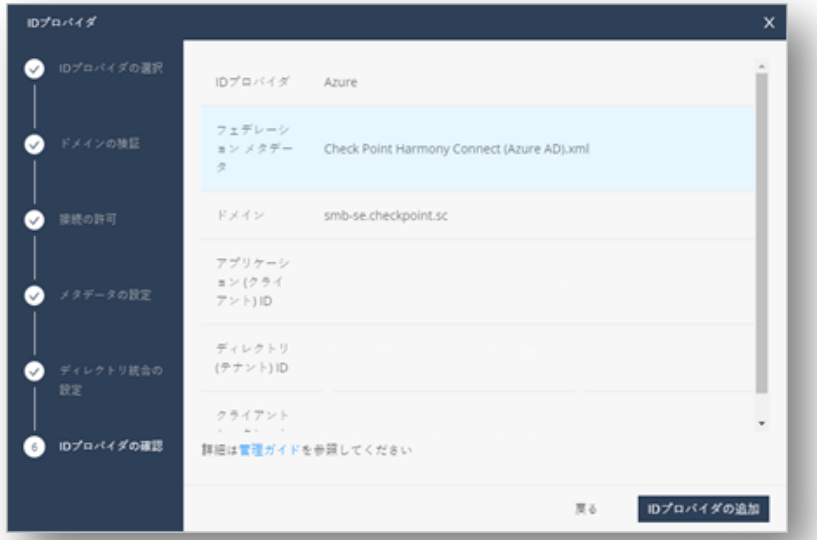
8. Azure AD からダウンロードした、「フェデレーション メタデータ XML」ファイルをアップロードして、「次へ」を押す

ユーザの作成［Azure AD 連携］（４／６）

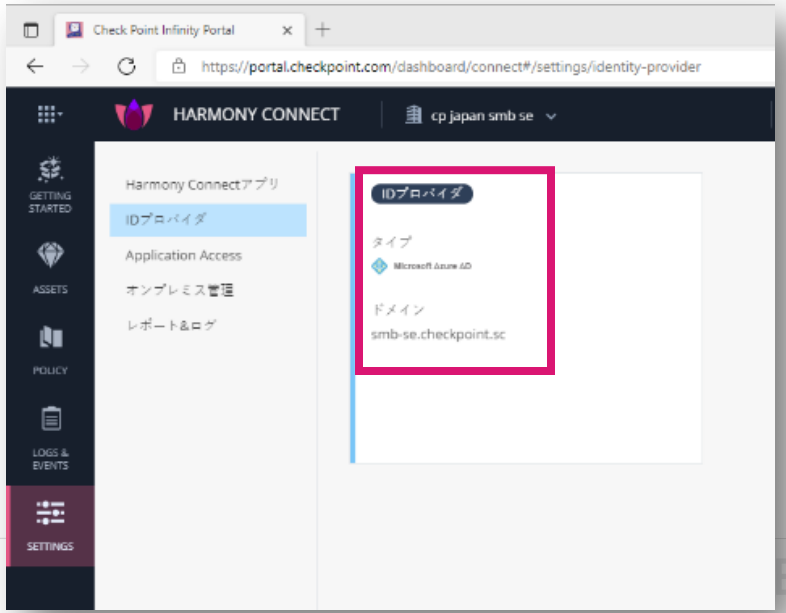
9. Azure AD から以下の３つの値をコピーして、入力する
10. 「次へ」を押す

- アプリケーション ID
  - アプリの登録 ＞ Check Point Harmony Connect (Azure AD) の 概要ページ
- ディレクトリ(テナント) ID
  - アプリの登録 ＞ Check Point Harmony Connect (Azure AD) の 概要ページ
- クライアントシークレット
  - アプリの登録 ＞ 証明書とシークレットで、新しいクライアントシークレットを作成し、クライアントシークレットの「値」をコピー

ユーザの作成［Azure AD 連携］（５／６）

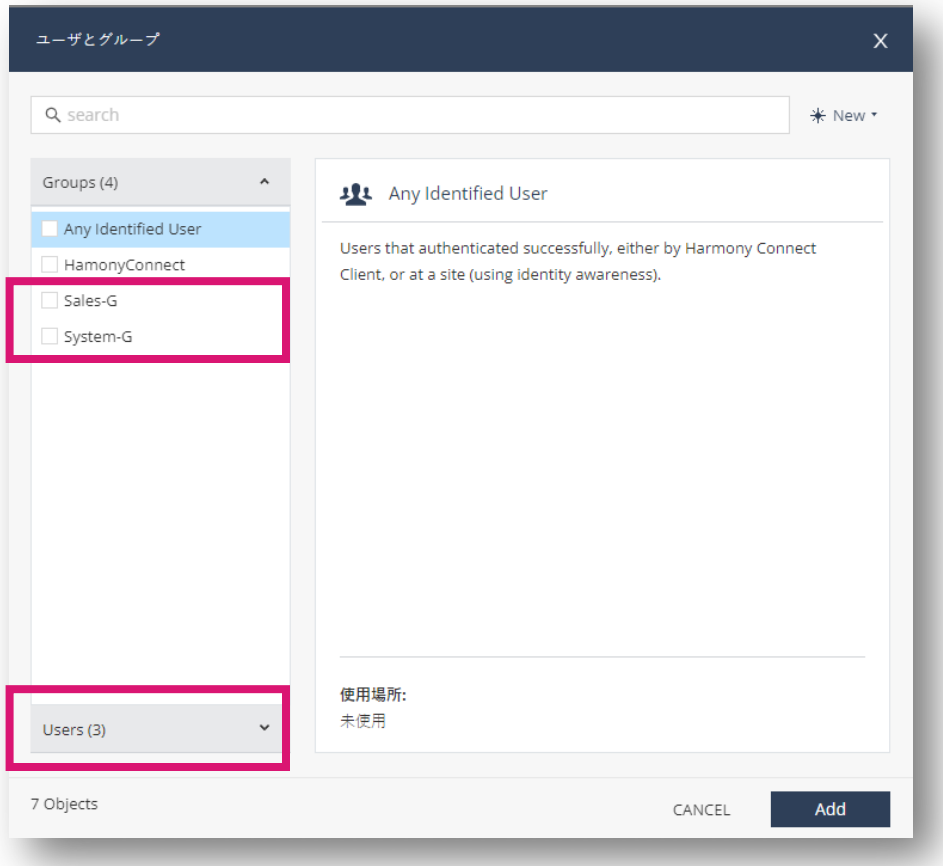


11. ID プロバイダの設定内容を確認して、「ID プロバイダの追加」を押す



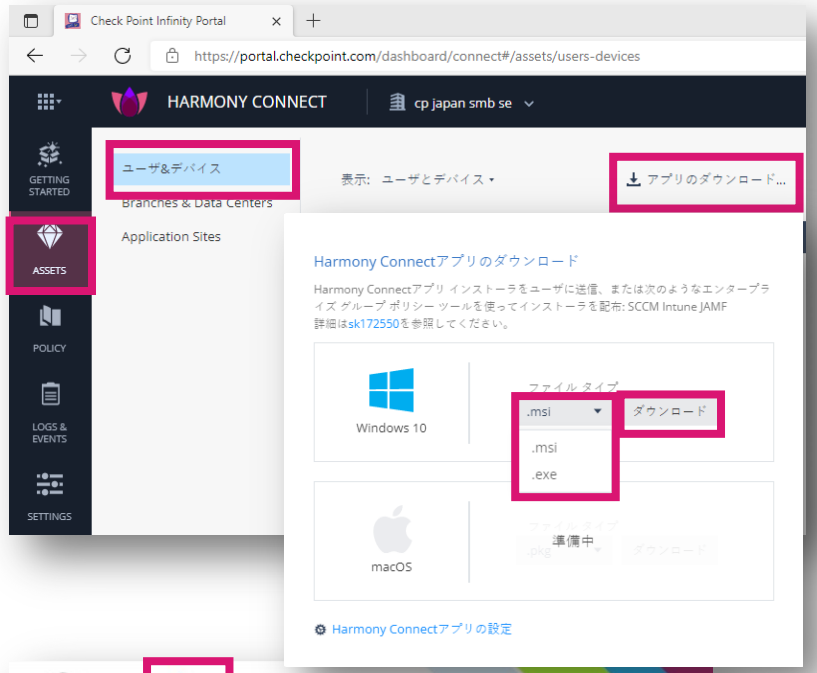
12. Harmony Connect への ID プロバイダの追加が完了

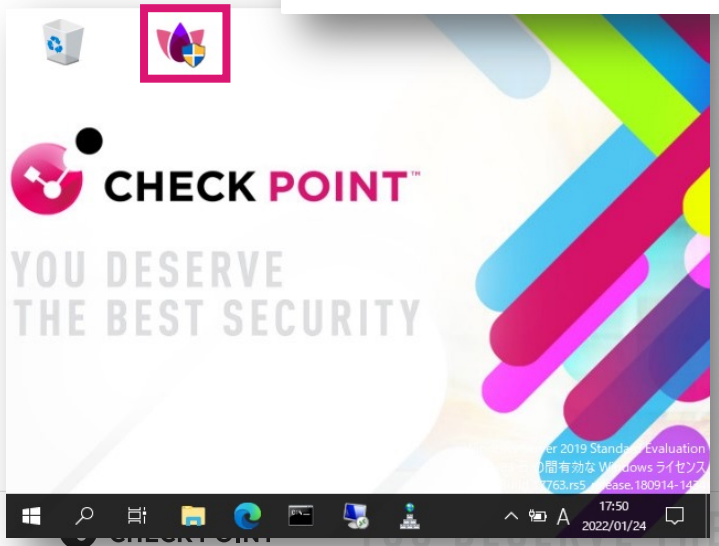
ユーザの作成［Azure AD 連携］（６／６）



13. ID プロバイダと Harmony Connect との間で、ユーザとグループの同期が完了すると、「POLICY > アクセスコントロール > インターネットアクセス」のオブジェクトに 、ID プロバイダの「ユーザ」と「グループ」が自動追加される
    - 「ユーザ、「グループ」の同期が可能な ID プロバイダは、 Azure AD、Okta、PingID のみ
14. 「ユーザ」と「グループ」は、Access Control のルール作成時に「ソース（送信元）」として指定可能

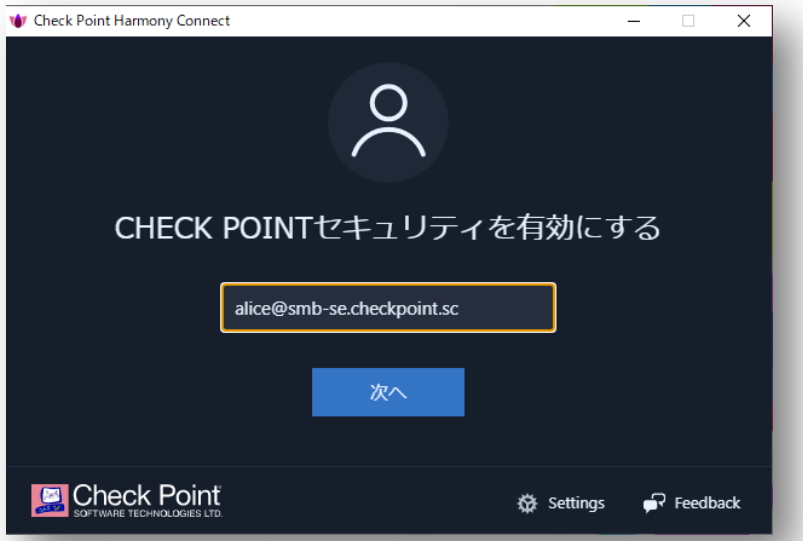
ConnetApp のマニュアルインストール（１／４）



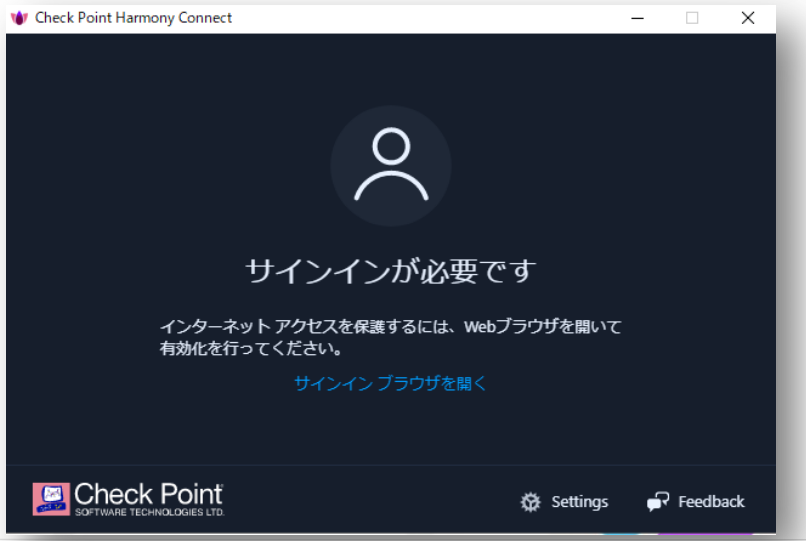


1. 「ASSETS > ユーザ＆デバイス」を選択する
2. 「アプリのダウンロード」を押す
3. ファイルタイプを選択して「ダウンロード」を押してダウンロードする
4. インストールファイルをダブルクリックする

ConnetApp のマニュアルインストール（２／４）

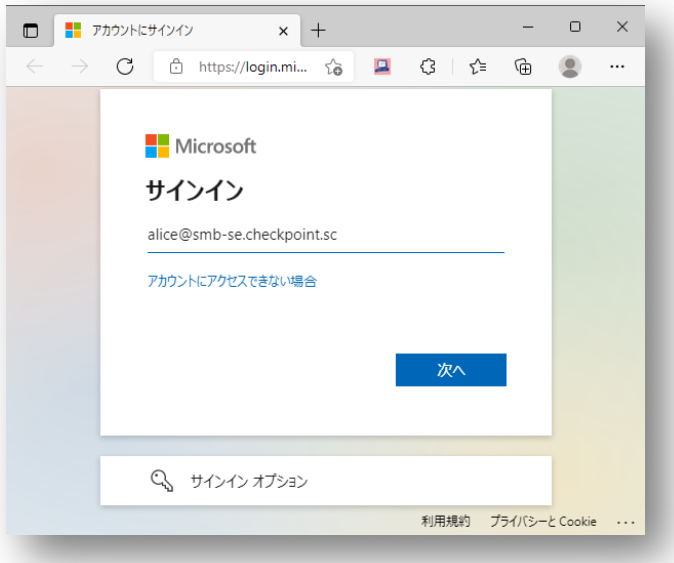


6. 認証ダイアログボックスが表示されるので、「ユーザ名（メールアドレス形式）」を入力し、「次へ」を押す

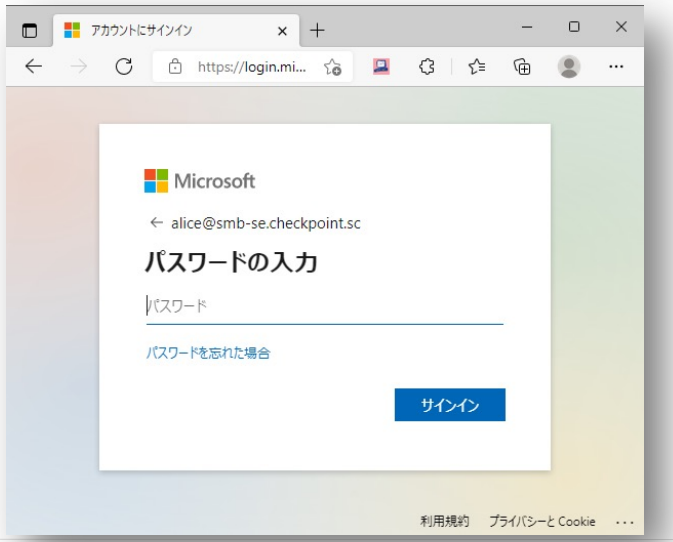


7. サインインを求められるので、「サインイン ブラウザを開く」を押す

ConnetApp のマニュアルインストール（３／４）

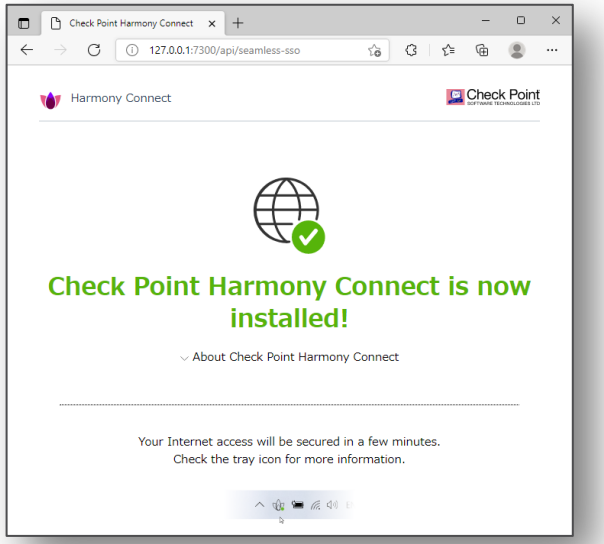


8. サインインページで「ユーザ名（メールアドレス形式）」を入力し、「次へ」を押す

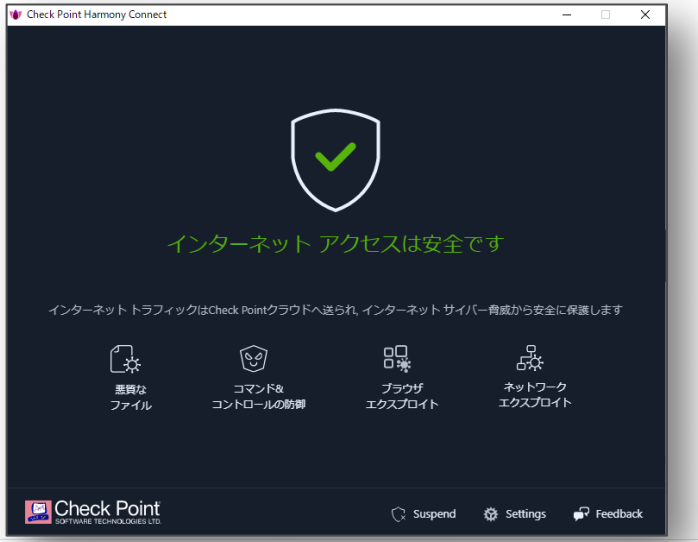


9. 「パスワード」を入力し、「サインイン」を押す

ConnetApp のマニュアルインストール（４／４）

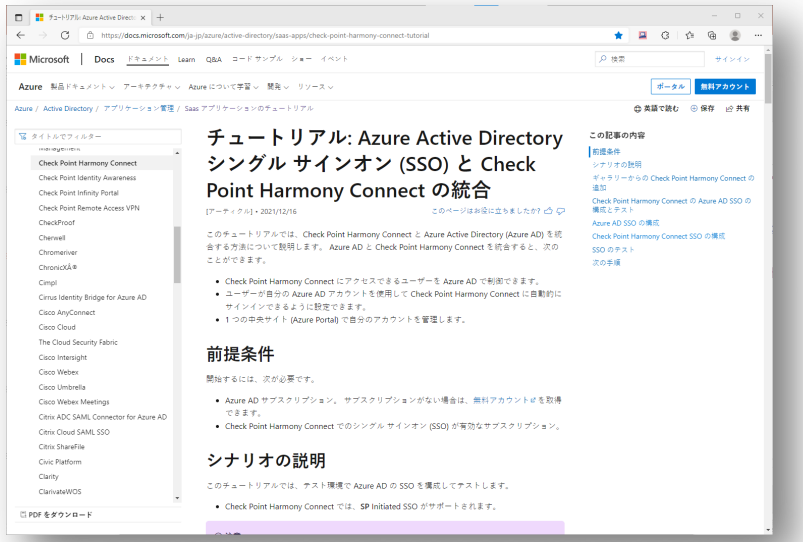


10. サインインが完了すると、ConnectApp のインストールが完了する



11. インストールが完了すると、自動的に Harmony Connect がトラフィックの保護を開始する

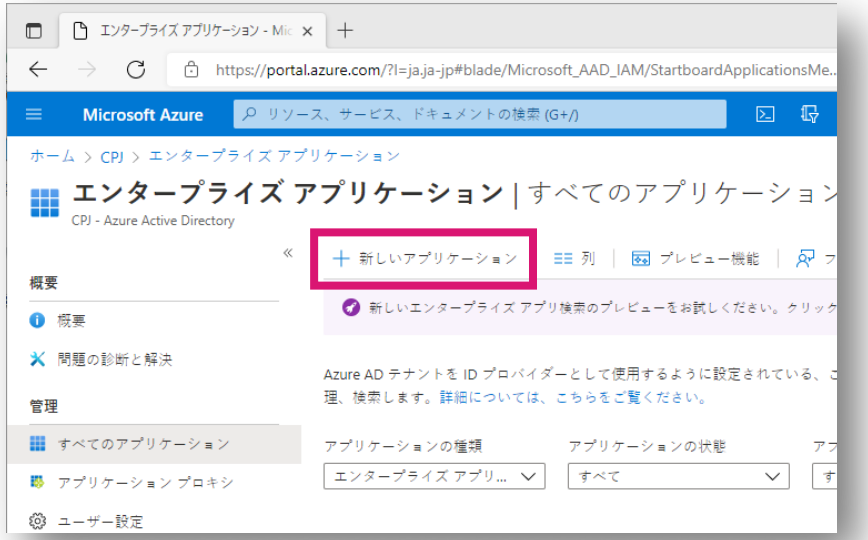
Azure AD での認証連携設定（１／１０）



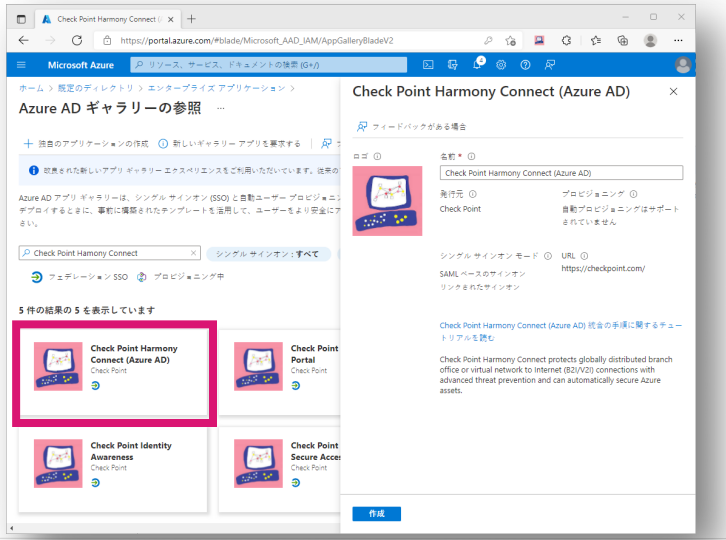
1. 基本的には Microsoft が公開しているチュートリアルに沿って設定すればよいが、一部設定が不足している
   - チュートリアル: Azure Active Directory シングル サインオン (SSO) と Check Point Harmony Connect の統合
   - https://docs.microsoft.com/ja-jp/azure/active-directory/saas-apps/check-point-harmony-connect-tutorial
2. Azure AD SSO の構成の流れ
   I. エンタープライズアプリケーションの作成
   II. SSO 方式の選択
   III. SAML 構成の設定
   IV. 属性とクレームの確認
   V. フェデレーション メタデータ XMLのダウンロード
   VI. クライアントシークレットの作成
   VII. APIのアクセス許可設定
   VIII. ユーザ、グループの割り当て

Azure AD での認証連携設定（２／１０）

エンタープライズアプリケーション > すべてのアプリケーション（プレビュー）



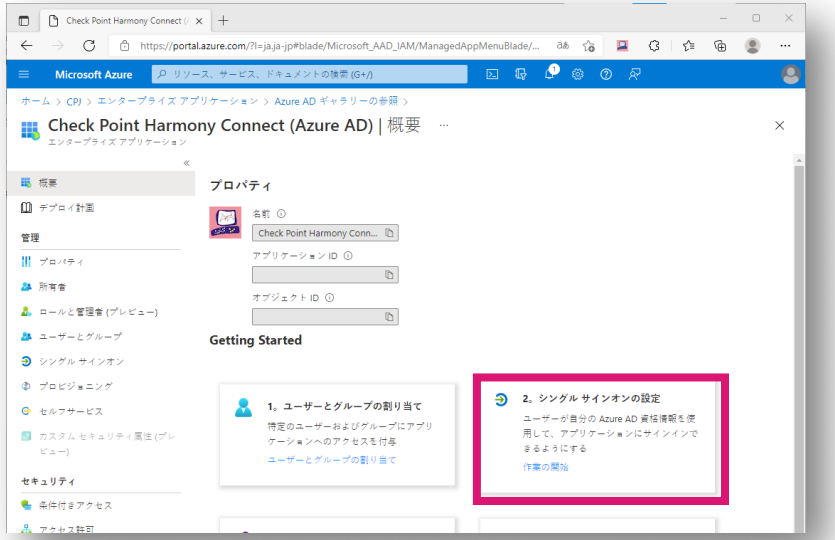
3. エンタープライズアプリケーション画面で、「新しいアプリケーション」をクリックする



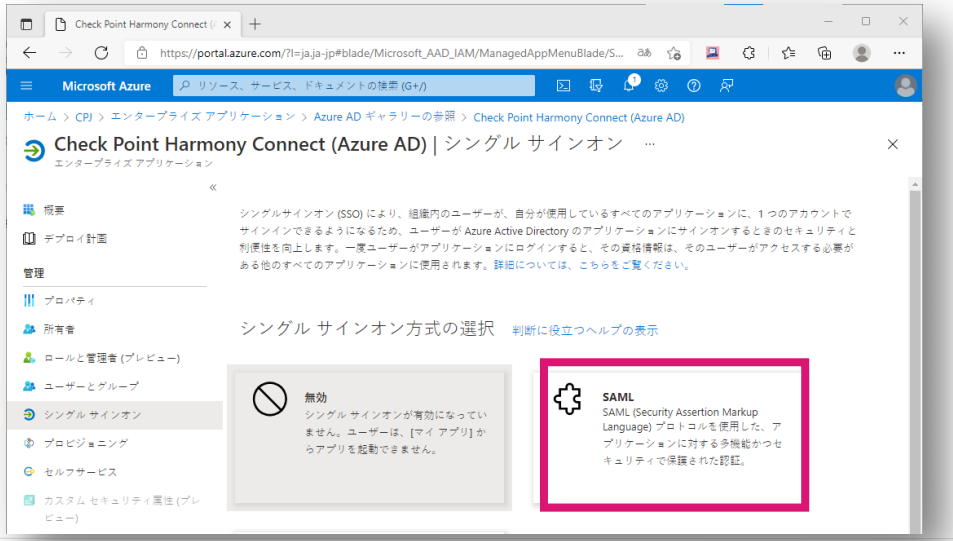
4. Azure AD ギャラリーで、「Check Point Harmony Connect」のキーワードで検索する
5. 「Check Point Harmony Connect (Azure AD)」を選択する
6. 「作成」を押す

Azure AD での認証連携設定（３／１０）

エンタープライズアプリケーション > Check Point Harmony Connect (Azure AD) > 概要



7. 「シングルサインオンの設定」をクリックする

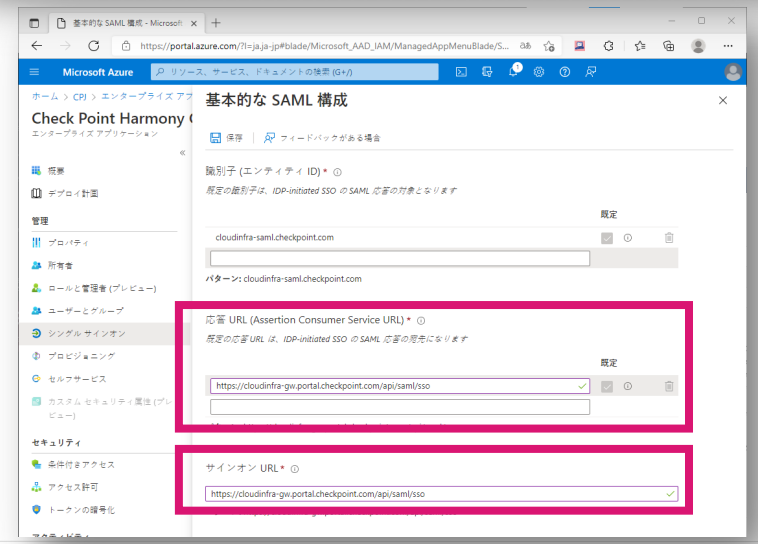


8. 「SAML」をクリックする

Azure AD での認証連携設定（４／１０）

エンタープライズアプリケーション > Check Point Harmony Connect (Azure AD) > シングルサインオン

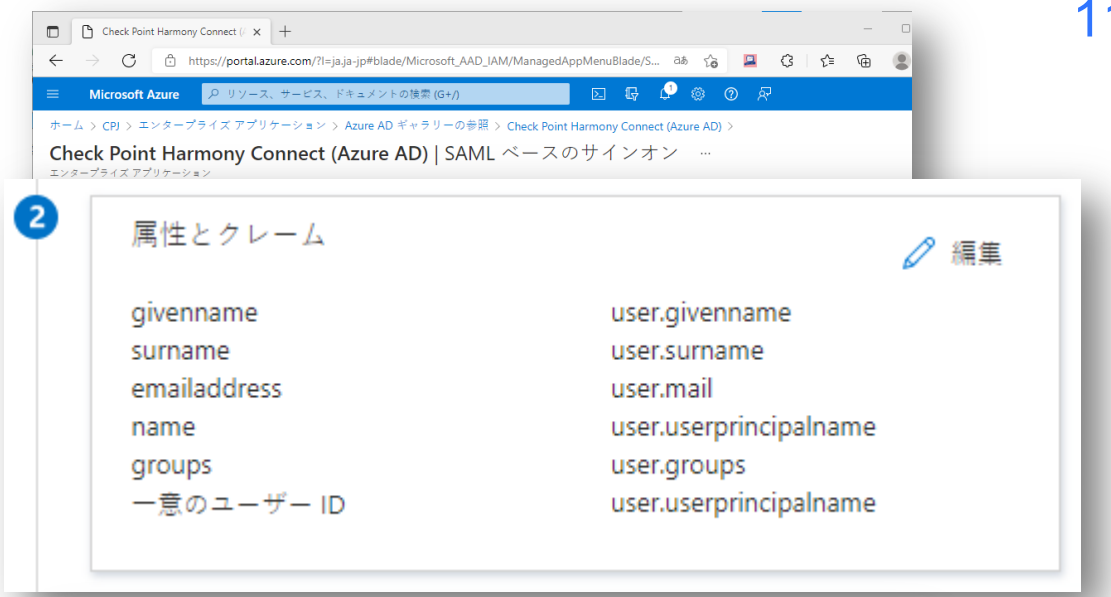
9. 「基本的な SAML 構成」欄の「編集」をクリックする



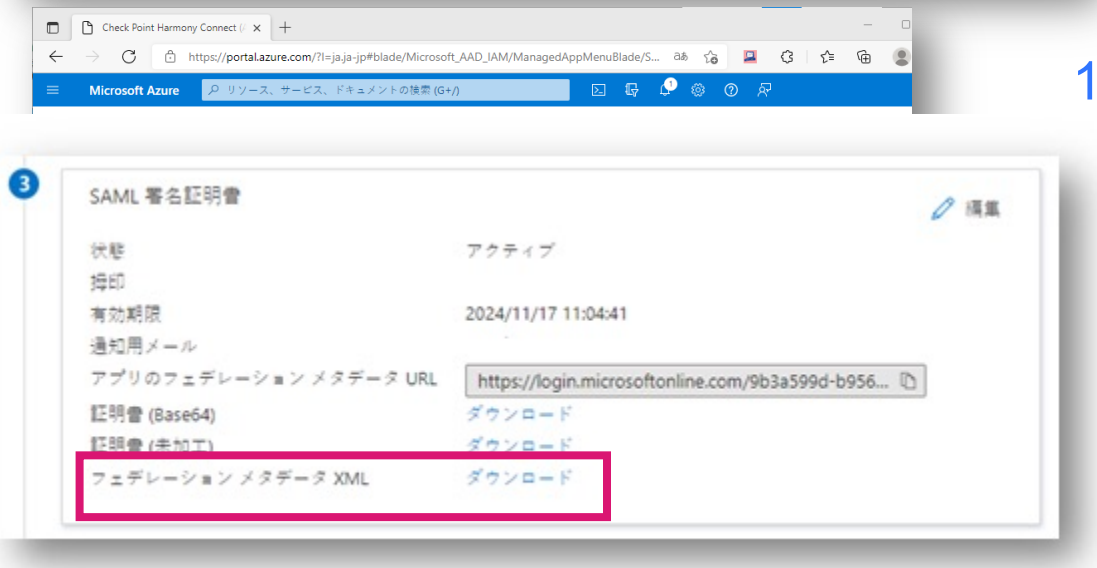
10. 「応答URL」、「サインオンURL」欄に、以下のURLを入力する
    - https://cloudinfra-gw.portal.checkpoint.com/api/saml/sso

Azure AD での認証連携設定（５／１０）

エンタープライズアプリケーション > Check Point Harmony Connect (Azure AD) > シングルサインオン



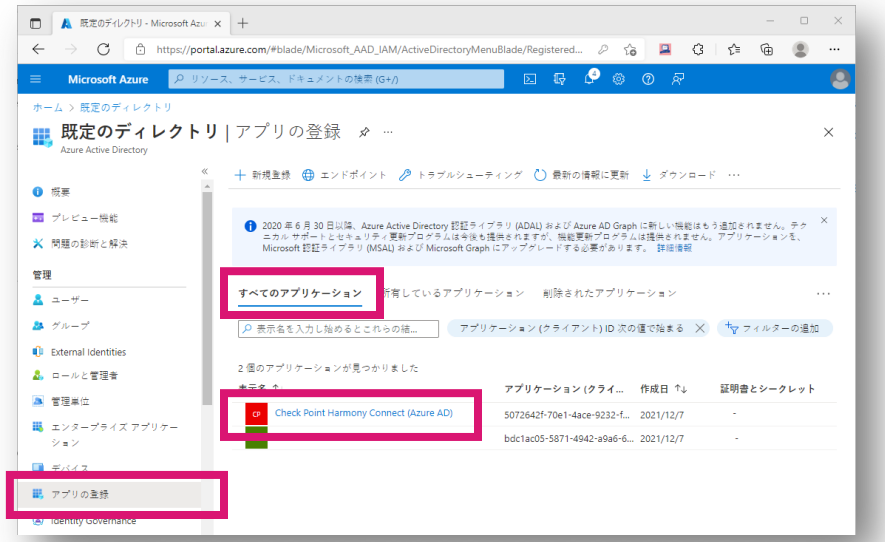
11. 「属性とクレーム」の表示と、Hamony Connect の「接続の許可」の画面の「ユーザ属性とクレーム」とが同じであることを確認する



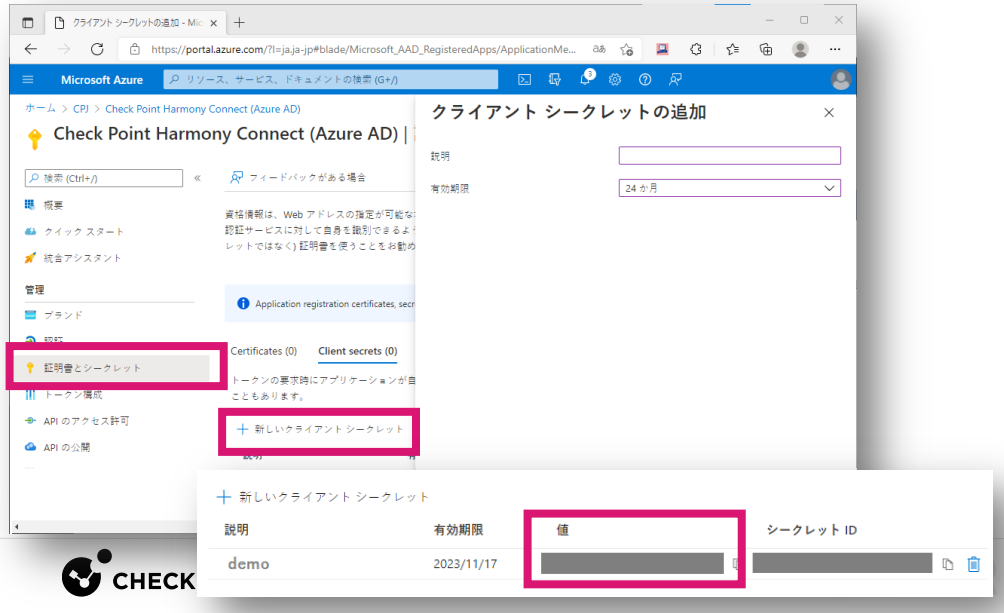
12. 「SAML 署名証明書」欄の「フェデレーション メタデータ XML」をダウンロードし、Harmony Connect の「メタデータの設定」の画面でアップロードする

Azure AD での認証連携設定（６／１０）

アプリの登録 > Check Point Harmony Connect (Azure AD)



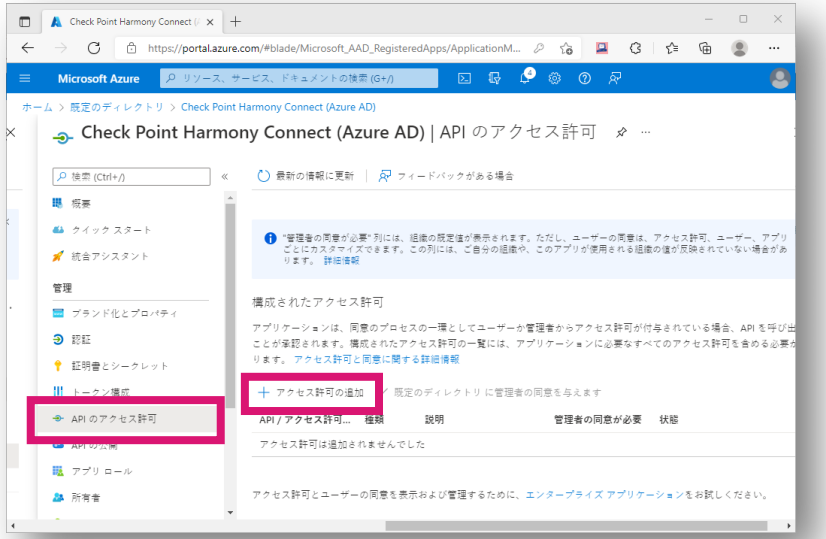
13. 「アプリの登録」画面で、「すべてのアプリケーション」をクリックする
14. 「Check Point Harmony Connect (Azure AD)」が表示されるのでクリックする



15. 「証明書とシークレット」をクリックする
16. 「新しいクライアントシークレット」をクリックして、クライアントシークレットを追加する
    - 「説明」、「有効期限」は、任意
17. 作成されたクライアントシークレットの「値」をコピーして、Harmony Connect の「ディレクトリ統合の設定」画面に入力する

Azure AD での認証連携設定（７／１０）

アプリの登録 > Check Point Harmony Connect (Azure AD)

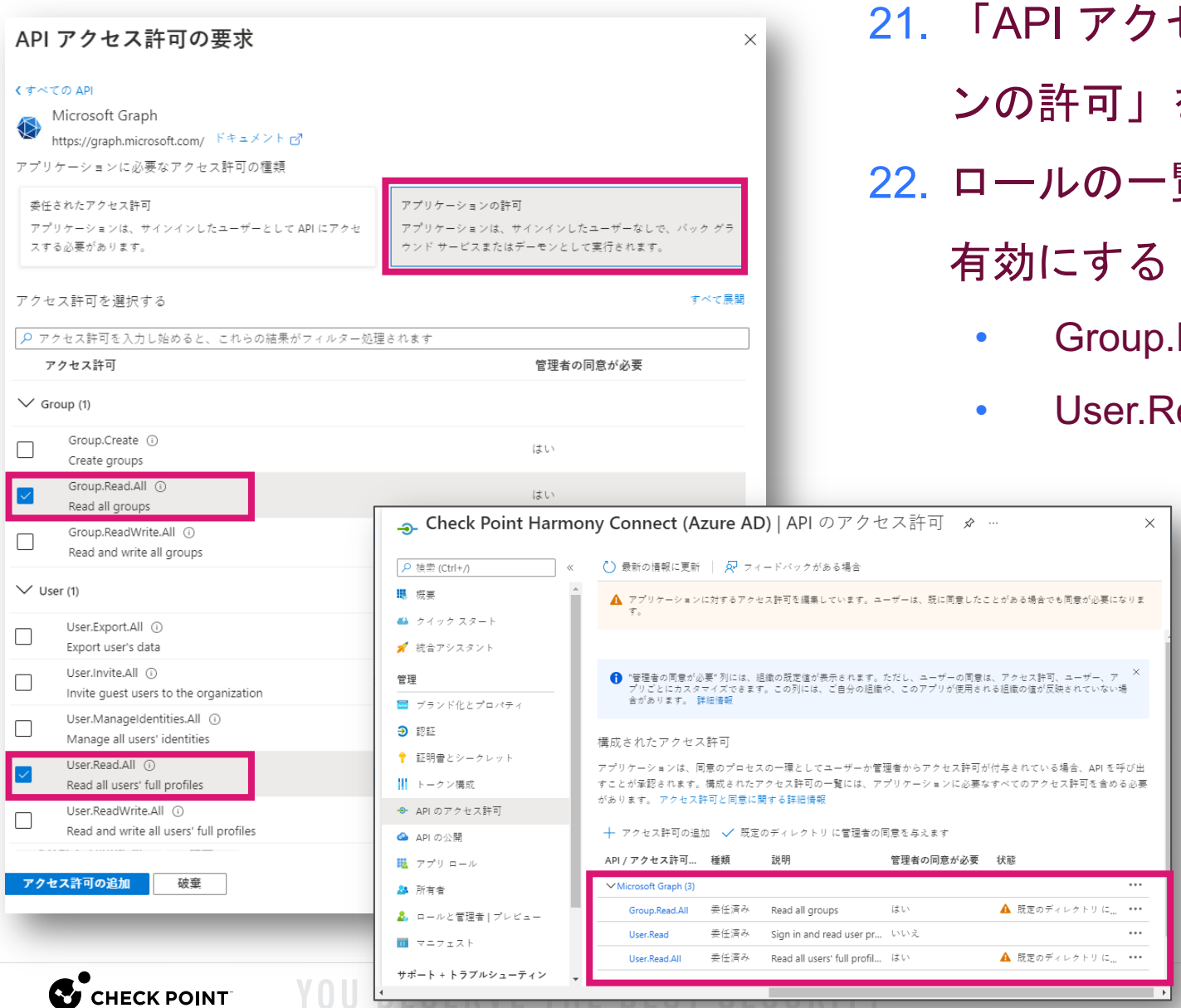


18. 「API のアクセス許可」をクリックする
19. 「アクセス許可の追加」をクリックする

20. 「API アクセス許可の要求」画面で、「Microsoft Graph」を選択する

Azure AD での認証連携設定（８／１０）

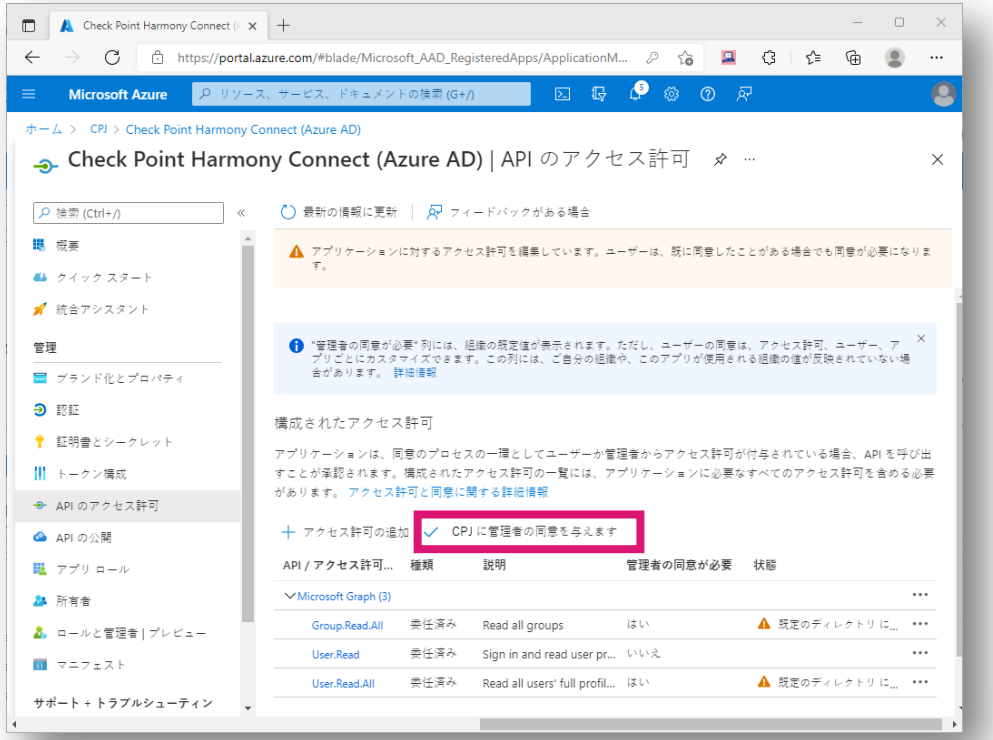
アプリの登録 > Check Point Harmony Connect (Azure AD)



21. 「API アクセス許可の要求」画面で、「アプリケーションの許可」を選択する
22. ロールの一覧が表示されるので、以下のアクセス許可を有効にする
    - Group.Read.All
    - User.Read.All

Azure AD での認証連携設定（９／１０）

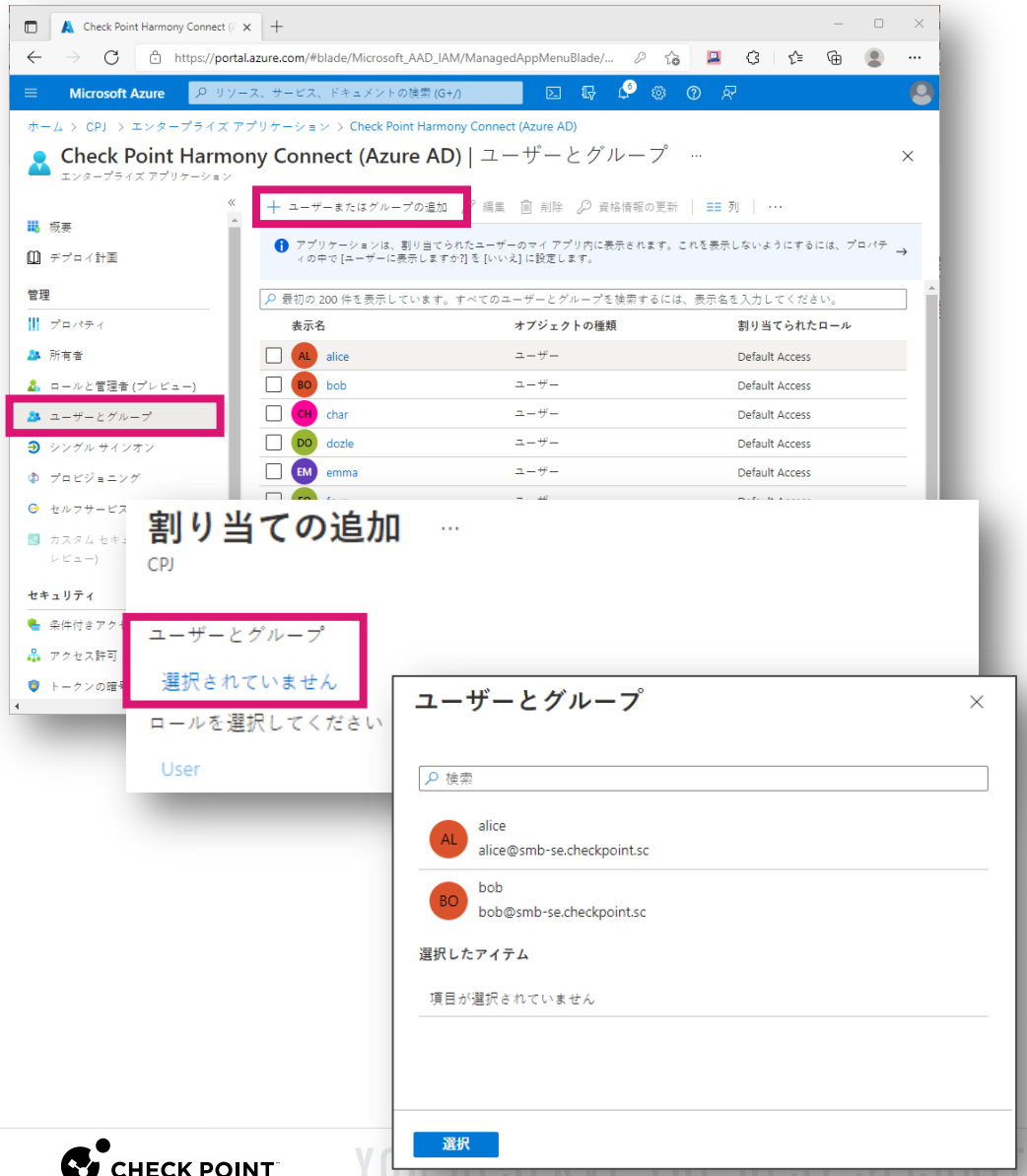
アプリの登録 > Check Point Harmony Connect (Azure AD)



22. 「［ディレクトリ名］に管理者の同意を与えます」をクリックして、API アクセス許可に管理者の同意を与える。

Azure AD での認証連携設定（１０／１０）

エンタープライズアプリケーション > Check Point Harmony Connect (Azure AD)



23. 「ユーザーまたはグループの追加」をクリックする
24. 「割り当ての追加」画面で、「ユーザーとグループ」をクリックする
25. 「ユーザーとグループ」画面に、Azure AD のユーザーとグループが表示されるので、Harmony Connect を利用するユーザー、グループを選択する
    - Harmony Connect に「グループ」を割り当てるためには、Azure AD Premium P1、P2 等のライセンスが必要です

YOU DESERVE THE BEST SECURITY

THANK YOU