HPE IceWall 技術レポート：

Microsoft 365（旧 Office 365）と IceWall の SAML 認証連携

2024.7.31 新規掲載

日本ヒューレット・パッカード合同会社
サービスデリバリー統括本部 認証コンサルティング部
神原 健太

目次

1. はじめに

本技術レポートでは、Microsoft 365（旧 Office 365）と IceWall の SAML での認証連携について説明します。

2. IceWall 製品と Microsoft サービスとの SAML 連携

IceWall 製品と Microsoft サービスとの SAML 連携する場合、2 種類の構成があります。

◎Microsoft 365 と IceWall Federation の連携

（IceWall が SAML IdP のパターン）

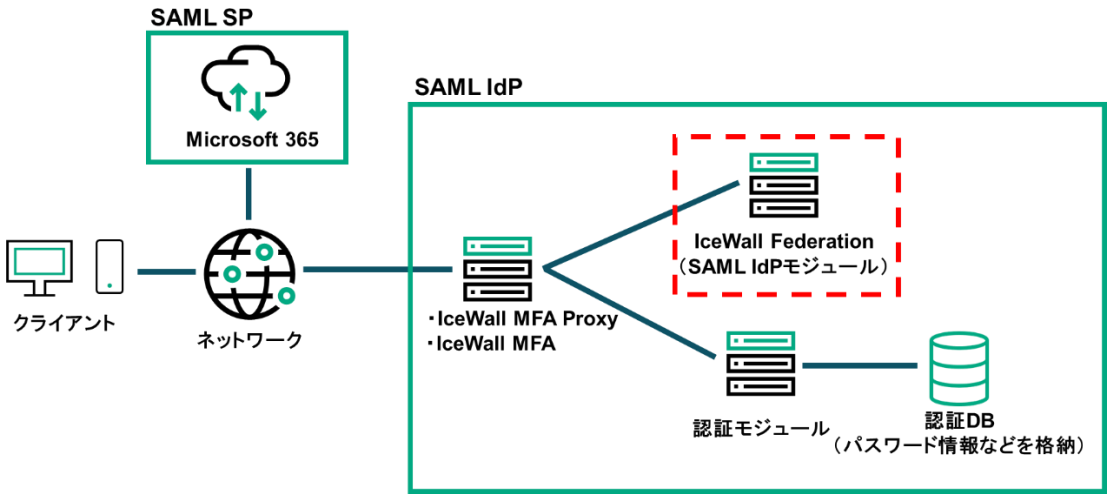
◎Microsoft Entra ID（旧 Azure Active Directory）と IceWall MFA の連携

（IceWall が SAML SP のパターン）

2.1. Microsoft 365 と IceWall Federation の連携

IceWall 側でパスワード照合などユーザー認証を行い、Microsoft 365 側では認証連携を行います。
この場合は SAML 構成の役割としては、IceWall Federation が IdP（Identify Provider）となり、Microsoft 365 が SP（Service Provider）となります。

構成例は以下のとおりです。

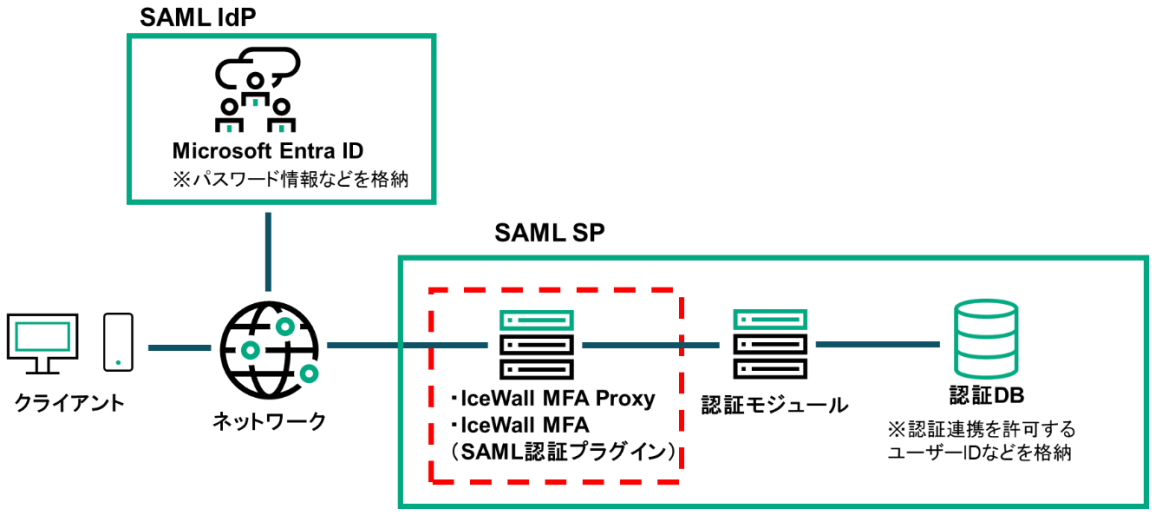


本技術レポートでは、この構成について詳細を説明します。

2.2. Microsoft Entra ID と IceWall MFA の連携

Microsoft Entra ID 側でパスワード照合などのユーザー認証を行い、IceWall 側では認証連携を行います。
この場合は SAML 構成の役割としては、Microsoft Entra ID が IdP（Identify Provider）となり、IceWall MFA の SAML 認証プラグインが SP（Service Provider）となります。

構成例は以下のとおりです。



本技術レポートでは、この構成は詳細説明の対象外となります。

3. Microsoft 365 との認証連携設定の流れ

本章は、Microsoft 365 と IceWall の認証連携の設定の流れについて、概要を説明します。
詳細な設定手順は IceWall マニュアル「IceWall Federation Version 4.0 SAML IdP Microsoft 365　認証連携ガイド」をご参照ください。

本章の前提として、IceWall マニュアル「IceWall Federation Version 4.0 SAML IdP 導入ガイド」に従い SAML IdP のインストール、設定が完了している前提で説明します。
設定画面などは 2024 年 6 月時点の Microsoft 365 の仕様に基づいた説明です。

3.1. 事前に準備が必要なもの

認証連携の設定を行うにあたって、事前に以下の準備が必要となります。

- Microsoft 365 ライセンス
- ドメイン取得

3.2. 主な設定の流れ

1. Microsoft 365 ドメイン作成、認証連携設定を行います。
ドメインの作成は、Azure AD ツール(PowerShell)のコマンドで実施します。

2. ドメインへの役割付与を行います。
Microsoft 365 の管理画面から、「Exchange」など使用するサービスを選択し、表示される DNS レコードを登録します。

3. Microsoft 365 のユーザーを作成します。
ユーザーの作成は、Azure AD ツール(PowerShell)のコマンドで実施します。

4. Microsoft 365 のユーザーにライセンスを付与します。

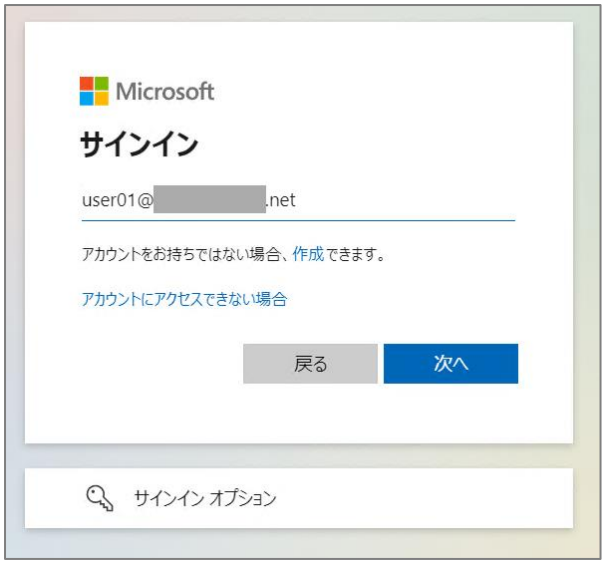
5. IceWall 側の認証 DB に以下の 2 項目を登録します。
・UPN（Microsoft 365 認証画面に入力するユーザーID）
・ImmutableID（認証連携する際の固有識別 ID）

4. クライアント端末での操作画面

本章では、ブラウザでの認証時の操作画面と、デスクトップアプリケーションの Outlook での操作画面を説明します。

4.1. ブラウザでの認証画面

1. Microsoft 365 の認証画面を表示されるので、Microsoft 365 のユーザー名を入力します。



2. Microsoft 365 の認証画面で入力したユーザー名のドメインに対応する IdP に自動でリダイレクトされます。IceWall の認証画面が表示されるので、IceWall のユーザー情報で認証を行います。

3. 認証が成功すると自動でリダイレクトが行われ、Microsoft 365 の画面が表示されます。

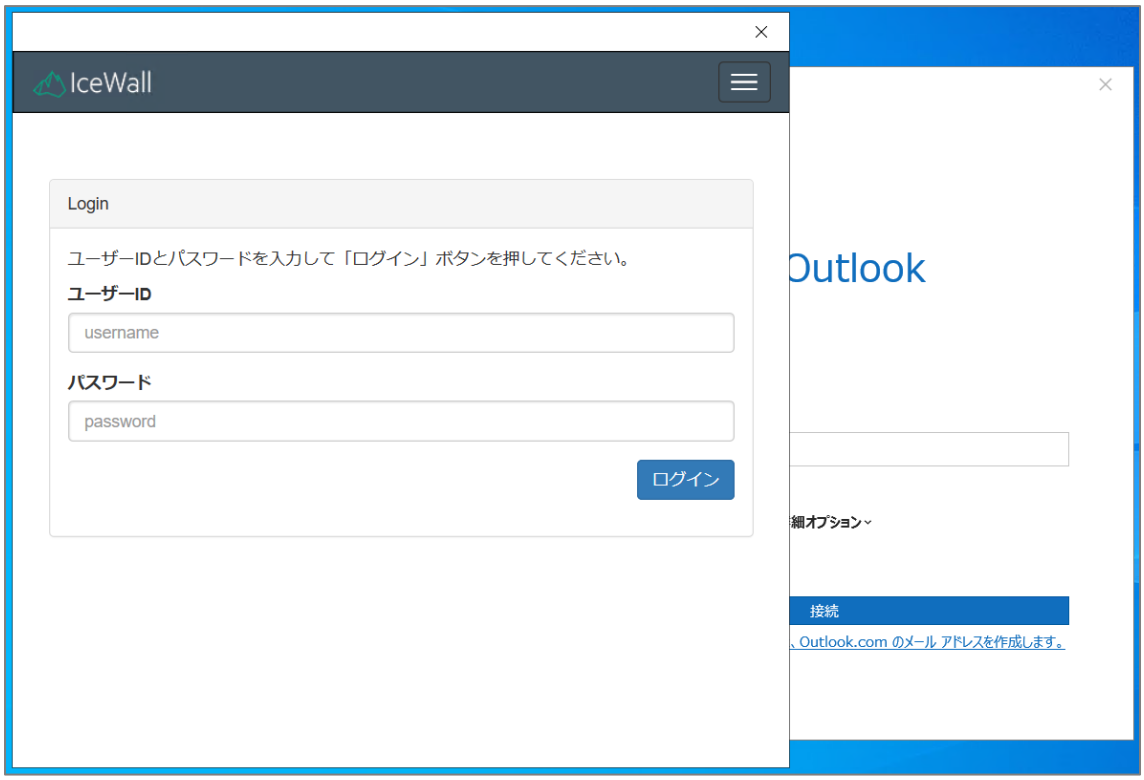
4.2. Outlook での認証画面

※以下の手順 1～5 は、初回 Outlook 起動時のみ表示される画面であり、次回以降は直接ログイン後画面（メール閲覧画面）が表示されます。

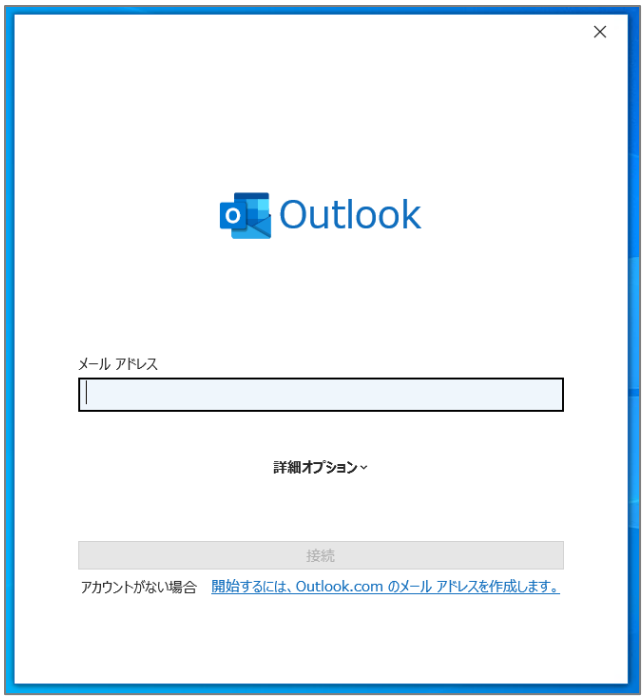
1. Outlook を起動し、「アカウントにサインインまたはアカウントを作成」をクリックします。

2. Outlook の認証画面とは別に、小さいブラウザのウインドウが表示されます。
Microsoft 365 のユーザー名を入力し「次へ」をクリックします。

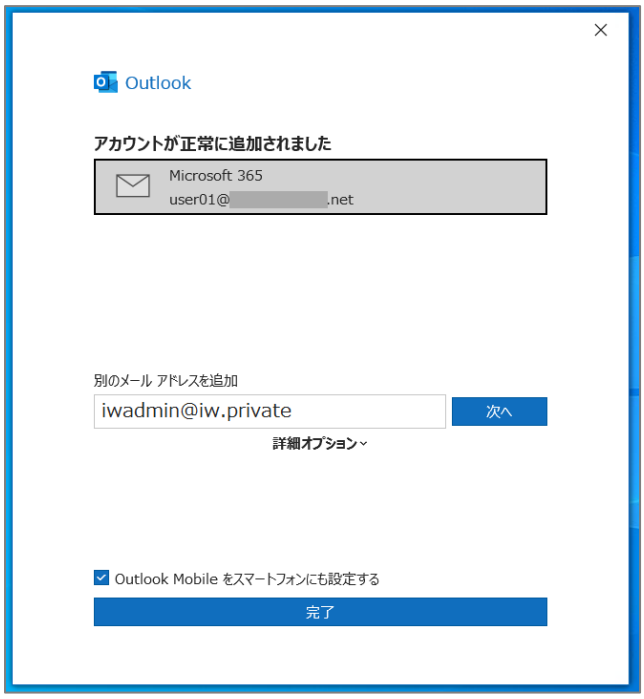
3. IceWall の認証画面が表示されるので、IceWall のユーザー情報で認証を行います。



4. Outlook で使用するメールアドレスの入力画面が表示されるので、Microsoft 365 のユーザー名を入力します。



5. アカウント追加の成功画面が表示されるので、「完了」ボタンをクリックすると Outlook のメール閲覧画面が表示されます。



5. まとめ

Microsoft 365 と IceWall を SAML 認証設定を行うことで、Microsoft 365 の認証を IceWall 側で行うことが可能となります。
IceWall を導入している環境に対して、Microsoft 365 サービスの使用追加をご検討の際は、SAML での認証連携をご検討下さい。

HPE IceWall 技術レポート一覧はこちらをご覧ください。
www.hpe.com/jp/iw-report