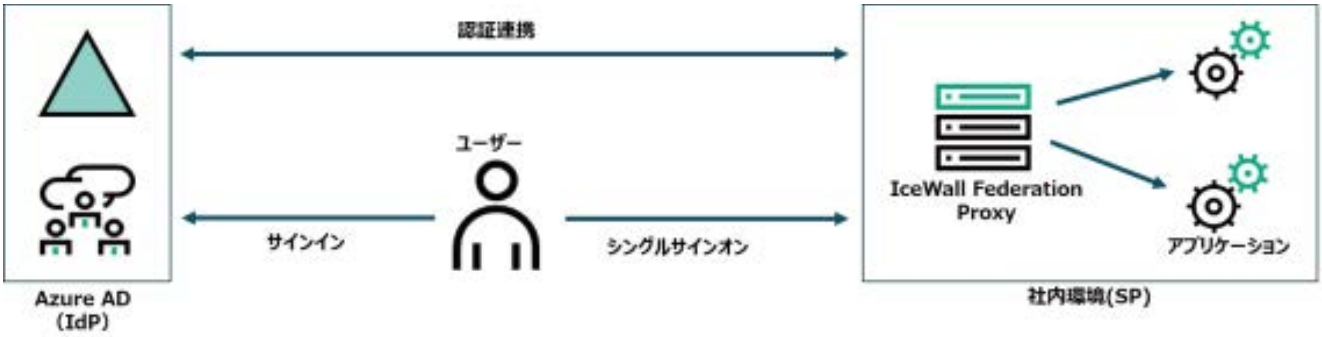
IceWall Federation ProxyとAzure ADのSAML認証連携の手順

IceWall技術レポート

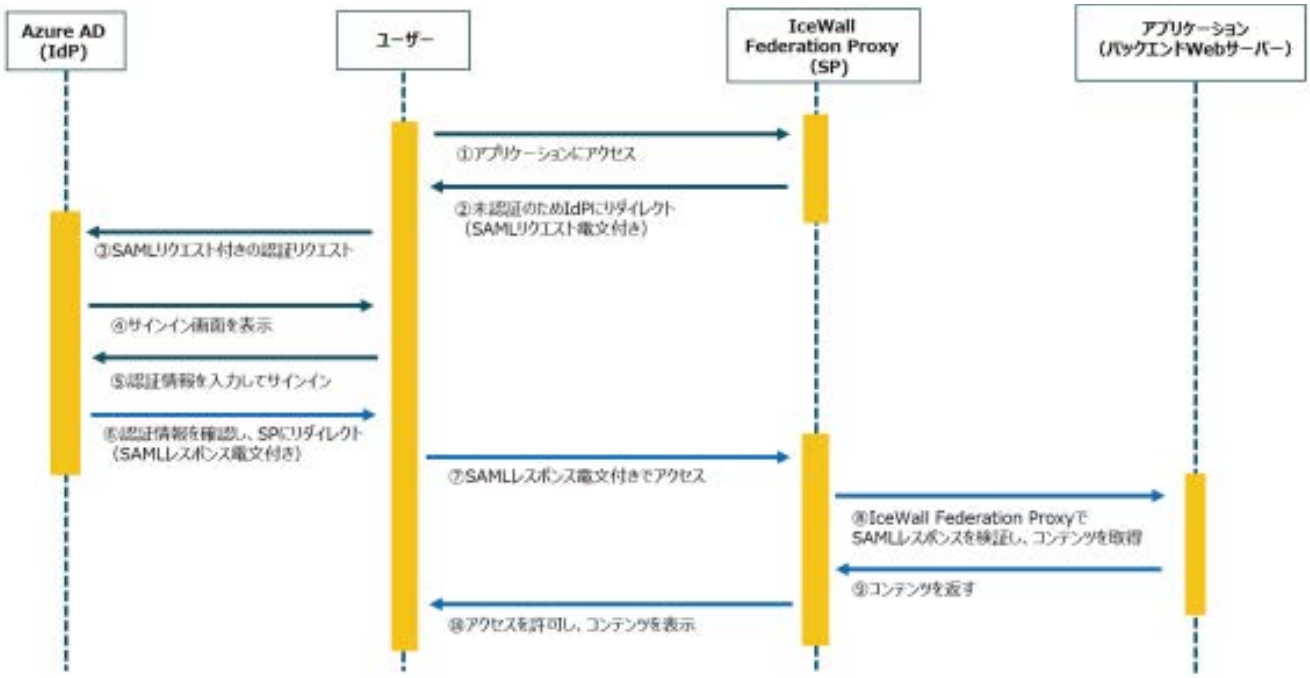
1. はじめに

近年、シングルサインオン基盤としてIDaaS（Azure AD等）を選択するケースが増えています。
Azure ADで認証を行い、社内環境のレガシー（SAML非対応）なWebアプリケーションにシングルサインオンする場合、IceWall Federation Proxyで認証連携が可能です。
認証連携はSAMLプロトコルで行います。
SAMLの用語として、AzureADをIdentity Provider (IdP) 、社内アプリケーションをService Provider (SP)で説明します。



本技術レポートでは、Azure ADとIceWall Federation Proxyの設定手順をご紹介します。

2.認証連携シーケンス



ユーザーが認証連携を行って、社内環境のアプリケーションにアクセスするまでのシーケンスを説明します。

今回の認証シーケンスは、最初に社内環境にアクセスする場合 (SP起動) のケースについて説明します。

3. 構築手順

構築手順を説明します。

3.1 構成

各サーバーの設定値の例として、以下で説明します。

分類	項目	内容
FQDN	IceWall Federation Proxy	iwfp01.sp
	バックエンドWebサーバー	backend01.sp
SP関連設定	識別子 (エンティティ ID)	https://iwfp01.sp/
	SPがリクエストを受信するURL (Assertion Consumer Service URL)	https://iwfp01.sp/samlsp

3.2.1 Azure AD 設定手順 概要

設定手順の概要は以下の通りです。

1. アプリケーションの作成
2. アプリケーションのシングルサインオンの設定
3. SAML設定に関するメタデータの取得
4. アクセスを許可するユーザー、及びグループを設定

3.2.2 Azure AD 設定手順

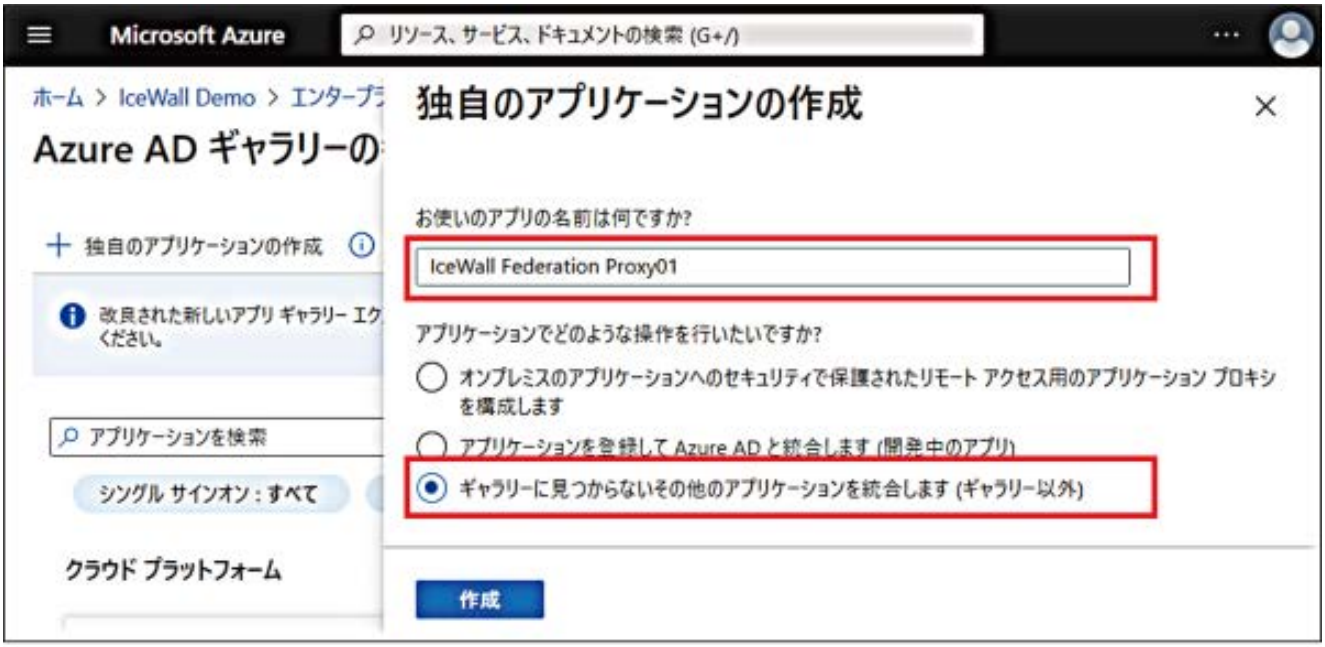
1. Azure ADの管理ユーザーでサインインします。
2.「すべてのサービス」から「Azure Active Directory」を選択します。

3. 左メニューより「エンタープライズ アプリケーション」を選択します。

4. 「新しいアプリケーション」を選択します。

5. 「独自のアプリケーションの作成」を選択します。

6. 任意の名前を入力し、「ギャラリーに見つからないその他のアプリケーションを統合します（ギャラリー以外)」を選択します。
「作成」ボタンを選択します。



7. 「シングルサインオン」を選択します。

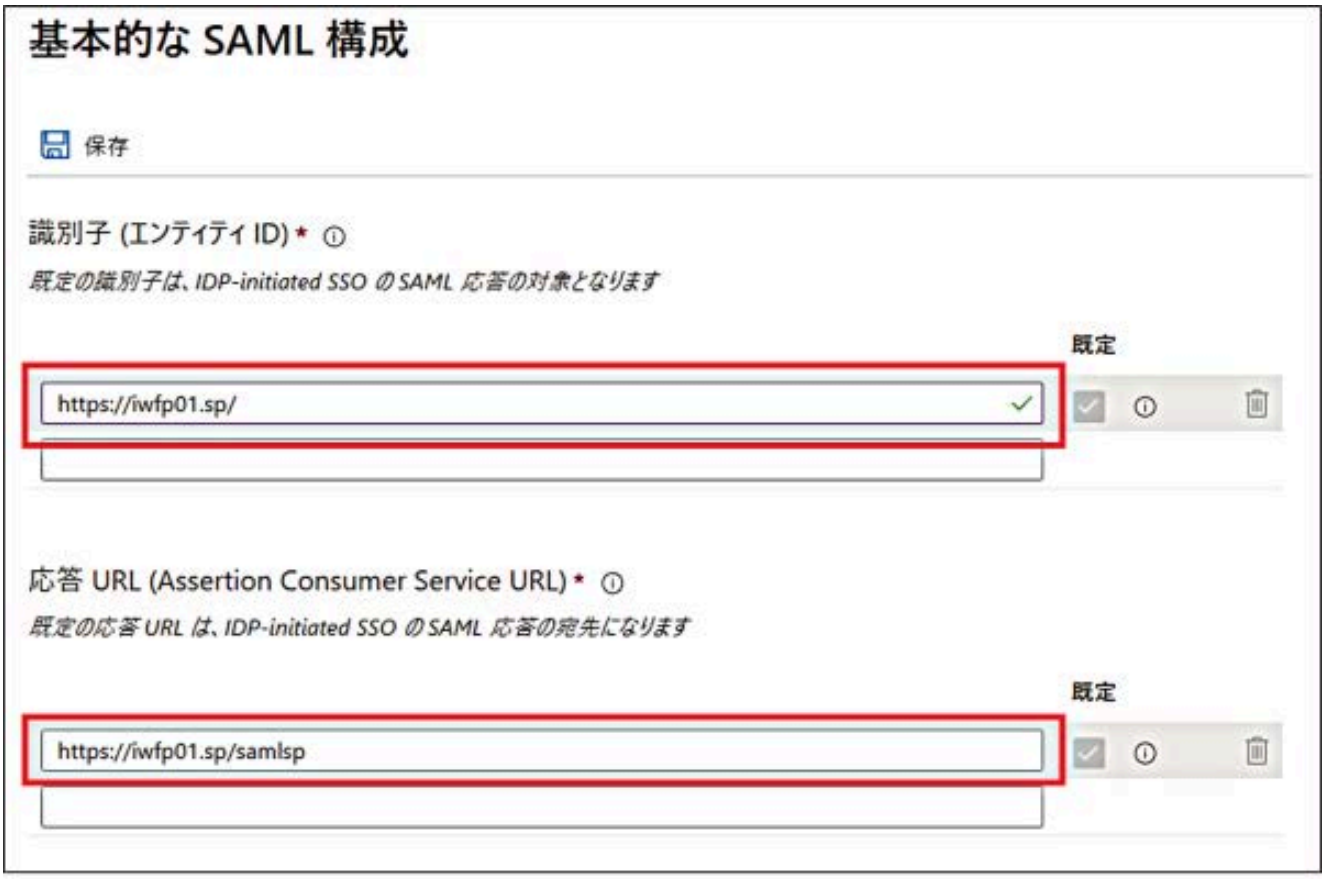
8. 「SAML」を選択します。

9. 「基本的なSAML構成」の「編集」を選択します。

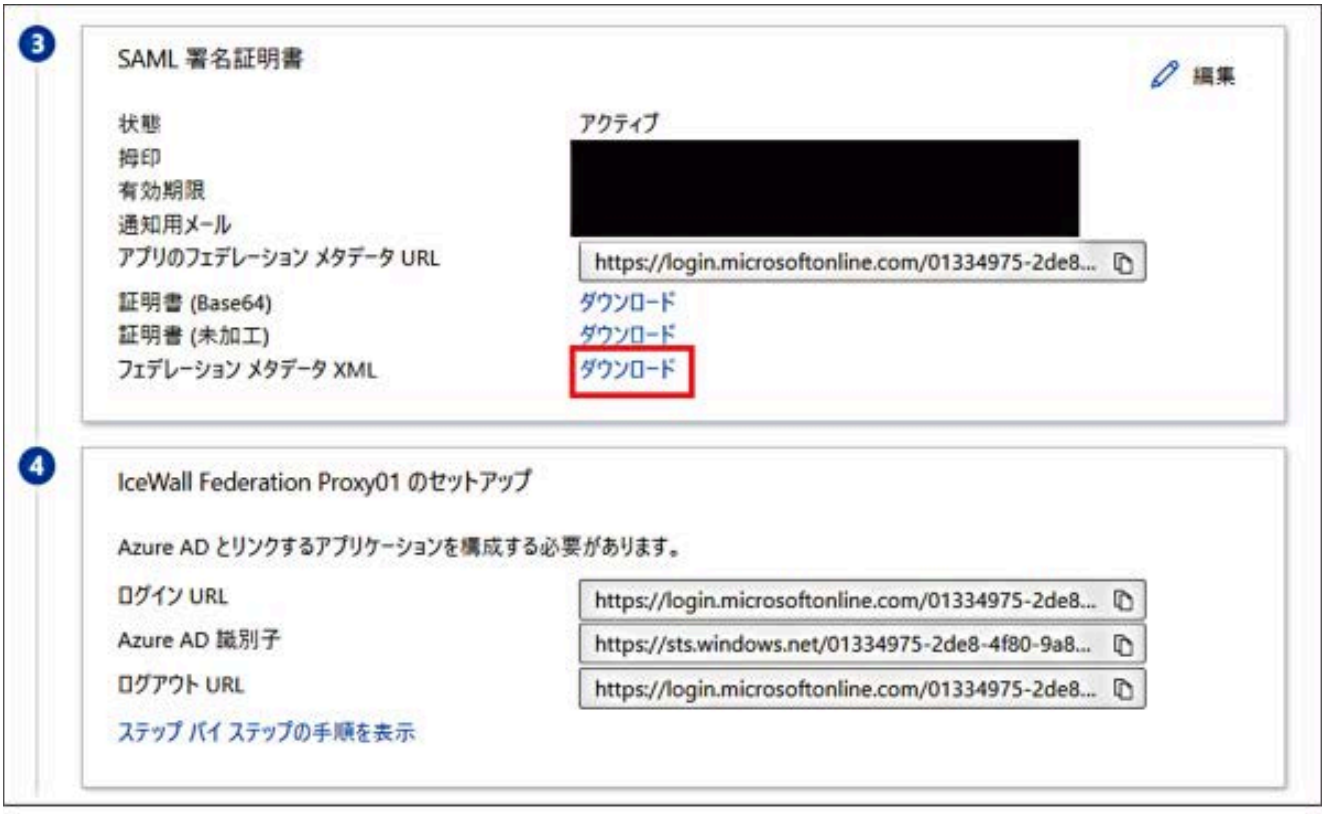
10.「識別子（エンティティID)」と「応答URL（Assertion Consumer Service URL)」を入力し、「既定」を有効に選択します。
「保存」ボタンを選択します。

ここでは以下の値の例で説明します。

項目名	設定例	備考
識別子 (エンティティ ID)	https://iwfp01.sp/	ー
応答 URL (Assertion Consumer Service URL)	https://iwfp01.sp/samlsp	「https://<FQDN>/samlsp」の形式で入力



11.「フェデレーション メタデータXML」の「ダウンロード」を選択し、IceWall Federation Proxyに設定するメタデータを取得します。



12.「ユーザーとグループ」を選択します。

13. 「ユーザーまたはグループの追加」を選択します。

14. アクセスを許可するユーザー、またはグループを追加します。

15.「割り当て」を選択します。

3.3.1 IceWall Federation Proxy 設定手順 概要

IceWall Federation Proxyの設定手順は、以下の前提で説明します。

- 「IceWall Federation Proxy 導入ガイド」の手順が完了している
- 「IceWall Federation Proxy サンプル設定ガイド」の手順が未実施の状態
- 認証モジュールは認証DB 不要機能（DBLESS)を使用する

設定手順の概要は以下の通りです。

1. SAML SPモジュールの設定
2. MFA Proxyの設定
3. 認証モジュールの設定

3.3.2 IceWall Federation Proxy のSAML SPモジュール設定手順

1. 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」を以下に配置します。
/opt/icewall-fedagt/samlsp/config/idp-meta.xml

2. 配置したメタデータのアクセス権を変更します。
cd /opt/icewall-fedagt/samlsp/config
chmod 644 idp-meta.xml
chown apache:apache idp-meta.xml

3. SAML SP設定ファイル(/opt/icewall-fedagt/samlsp/config/samlsp.conf)を次のように設定します。

項目名	設定例	備考
URL_GATEWAY	https://iwfp01.sp/samlsp	SAML SPがリクエストを受信するURLを設定します。
CERT	https://127.0.0.1:14143	認証モジュールのホストおよびポートを設定します。
CONF	IDP1,/opt/icewall-fedagt/samlsp/config/idp-interface.conf,https://sts.windows.net/***-***-***/	SPと連携するIdPの情報を設定します。 末尾のURLは、Azure ADのメタデータXMLのentityIDに設定されている値に置き換えます。
AGENT_KEY	AGENT_SAMLSP	SAML SPーエージェント連携時の識別キーワードを設定します。

4. IDPインターフェイス設定ファイル(/opt/icewall-fedagt/samlsp/config/idp-interface.conf)を次のように設定します。

項目名	設定例	備考

SP_ENTITY_ID	https://iwfp01.sp/	SPのエンティティ ID を設定します。 Azure ADに設定した識別子(エンティティ ID)を設定します。
ASSERTION_RECIPIENT	https://iwfp01.sp/samlsp	アサーション受信時、アサーションのRecipientと比較するURLを設定します。 Azure ADに設定した応答URL(Assertion Consumer Service URL)を設定します。

5. 「IceWall Federation Proxy サンプル設定ガイド」の章「SAML SPの鍵ファイルの作成」の手順を実施します。

6. AuthnRequest 電文のテンプレートファイル(/opt/icewall-fedagt/samlsp/config/authn-request.xml)を以下のとおり修正します。

◎修正前
Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">

◎修正後
>

3.3.3 IceWall Federation Proxy のMFA Proxy設定手順

1. エージェント設定ファイル(/opt/icewall-mfa/proxy/agent/config/agent.conf)を次のように設定します。

項目名	設定例	備考
AGENT_KEY	AGENT_SAMLSP	SAML SPーエージェント連携時の識別キーワードを設定します。 SAML SP設定ファイルのAGENT_KEY項目に設定した値と同一の値を指定 します。
DFW_PATH	https://iwfp01.sp/samlsp	エージェントからのリクエストを受け取るSAML SPのURLを設定します。 SAML SP設定ファイルのURL_GATEWAY項目に設定した値を指定します。
CERT	https://127.0.0.1:14143	認証モジュールのホストおよびポートを設定します。

NOCHK_URL	/samlsp /favicon.ico /res/	SAML SPの動作パス、favicon.ico、MFA Proxyのコンテンツを認証不要パスに設定します。

2. RPモジュール設定ファイル(/opt/icewall-mfa/proxy/iwproxy/config/iwproxy.conf)を次のように設定します。
HOST=bk01=backend01.hpe.com:80
SVRFILE=bk01,/opt/icewall-mfa/proxy/iwproxy/config/sample.conf

3.3.4 IceWall Federation Proxy の認証モジュール設定手順

1. リクエスト制御設定ファイル(/opt/icewall-sso/certd/config/acl/request.acl)にSPからのリクエストを受信許可する設定を行います。

```
TARGET=SOURCE_ADDR=（SPサーバーのIPアドレス）
{
ACCEPT=L_ANON_AUTH
ACCEPT=L_READ_SESSION
ACCEPT=P_LOGOUT_SID
ACCEPT=AGENT_ICP3
}
```

2. グループ設定ファイル(/opt/icewall-sso/certd/config/acl/cert.grp)に匿名(SAML)認証するユーザーの所属グループを設定します。

```
GRP01,USERID="."
```

3. 親アクセスコントロールファイル(/opt/icewall-sso/certd/config/acl/parent.acl)にSPサーバー上のコンテンツへのアクセス制御設定を行います。

```
https://;;child/child.acl
```

4. 子アクセスコントロールファイル(/opt/icewall-sso/certd/config/acl/child/child.acl)にSPサーバー上のコンテンツへのアクセス制御設定を行います。

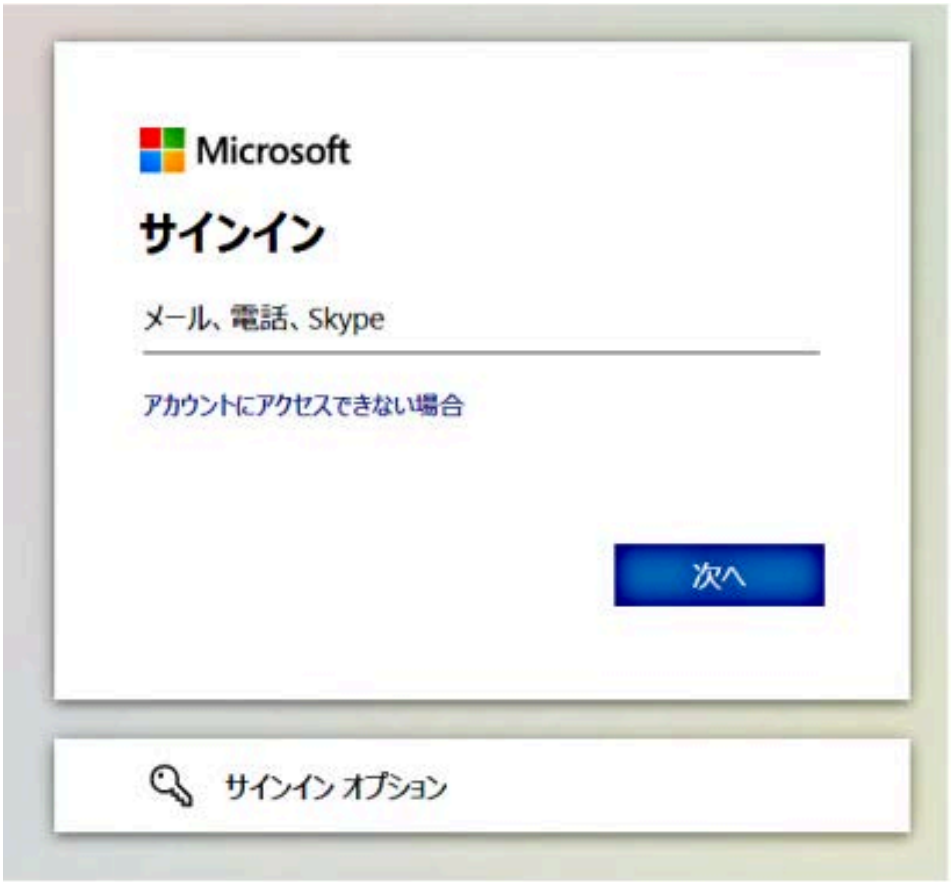
```
https://iwfp01.sp/=GRP01;;ANON
```

4. 動作確認

動作確認の手順を説明します。

1. ブラウザを起動し、以下のURLにアクセスします。

```
https://iwfp01.sp/iwproxy/bk01/
```



2. Azureのサインイン画面が表示されます。

3. サインインが成功すると、最初にアクセスしたURLのコンテンツが表示されます。

5. まとめ

Azure ADでID管理した場合でも、IceWall Federation Proxyを使用することで社内環境のWebサーバーとのシングルサインオンが可能です。今回はその手順をご紹介しました。
社内環境の特定のURLのみワンタイムパスワードを必要とする場合は、AzureADに複数のアプリケーションを作成し、IceWall Federation Proxyをアプリケーションと同数構築することで、複数の認証方式に設定することも可能です。

IDaaSから社内環境のレガシー（SAML非対応）なWebアプリケーションを利用する際は、今回のシステムをぜひご検討ください。

2021.6.30

執筆者　：日本ヒューレット・パッカード合同会社

Pointnext事業統括　Pointnextデリバリー統括本部
クロス・インダストリー・ソリューション本部 認証技術開発センター

神原 健太

技術レポート一覧へ →

お問い合わせ先一覧

企業情報

- 会社情報
- アクセス
- お問い合わせ
- 採用情報
- HPEについて
- インクルージョン & ダイバーシティ
- サステナビリティと企業責任
- 経営幹部

お知らせ

- ニュースルーム
- イベント・セミナー
- 新着情報
- 重要なお知らせ

パートナー

- パートナープログラム
- 認定資格制度
- OEMソリューション

サポート

製品サポート

ソフトウェア & ドライバー

標準保証確認

オペレーショナルサポート

教育とトレーニング

製品リサイクル

機器部品の妥当性確認

コミュニティ

HPE Japan ブログ

リソース

お客様事例

ご購入方法

オンラインストア

HPE Customer Center

Eメール登録

ドキュメントライブラリ

Resource Library

ビデオギャラリー

金融サービス

日本 (ja)