インフラシステム

NES株式会社

Microsoft Azure ADで実現

ゼロトラスト構築サービス

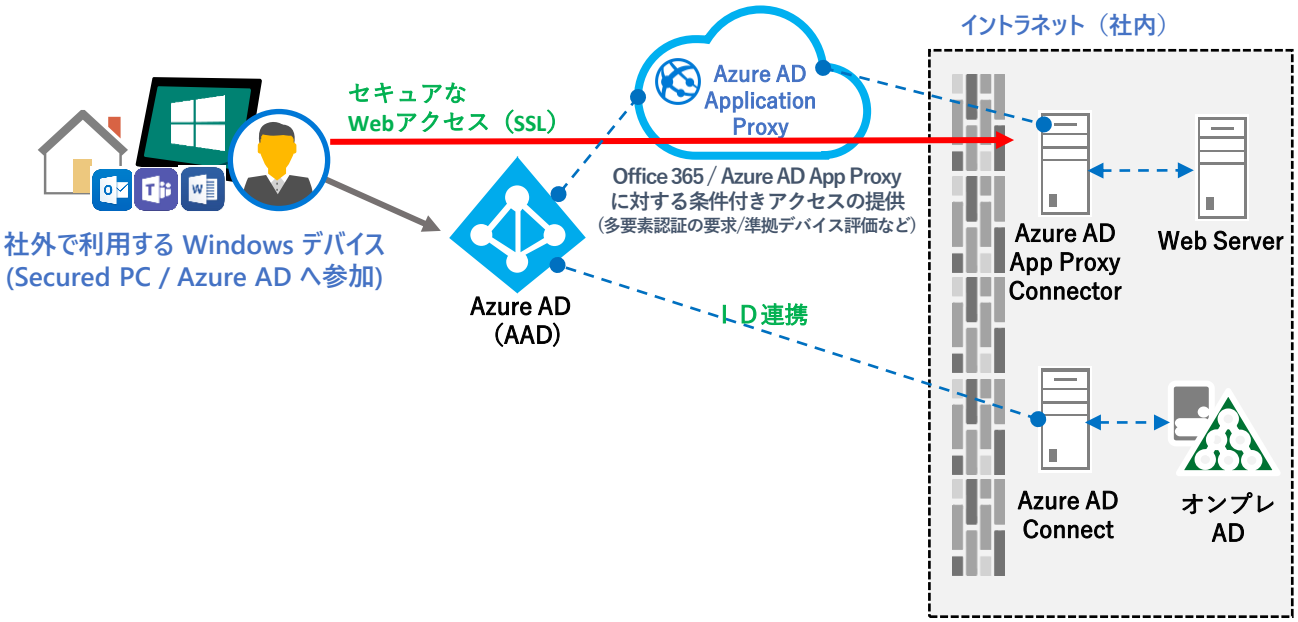
Azure ADを活用した認証基盤の構築事例を紹介します。
既存のオンプレ環境の認証基盤であるActiveDirectory（AD)とクラウドサービスであるMicrosoft Azure AD（AAD）を連携し、ゼロトラスト実現に向けた新たな１歩を踏み出しましょう。

ゼロトラストとは

「ゼロトラスト」とは、「何も信頼しない」を前提に対策を講じるセキュリティの考え方。
この考えのもと、全てのトラフィックに対して信用をスコアで評価し、対策を行う、次世代のセキュリティモデルです。社内からのアクセスなど従来は信用できると評価されてきたトラフィックであっても、信用評価を都度行うことで、内外どこからの脅威に対しても備えることができるという特長があります。

AzureADによる利用者認証の実現とアプリケーションプロキシ

Azure AD（AAD）とオンプレのADをマイクロソフト社から提供されるAzure AD Connectサーバを社内側に構築することで、ID連携が実現されます。ID連携しただけではユーザーにとってメリットが無さそうですが、あわせてAzure AD App Proxy Connectorサーバを社内に構築することで、社外からAAD認証されたユーザーは、Azure AD Application Proxyを経由し、SSLで暗号化された通信で社内のWebサイトへアクセス出来るようになります。



利用者認証について

ここでは、あらためて「ゼロトラスト」と「境界防御」の違いについて確認する事にしましょう。
ゼロトラストの実現にはセキュリティの機能毎に実装が必要となりますが、今回はゼロトラスト実現の第一歩として、「利用者認証」と「利用者のWebアクセス管理」に着目して、構築を行います。

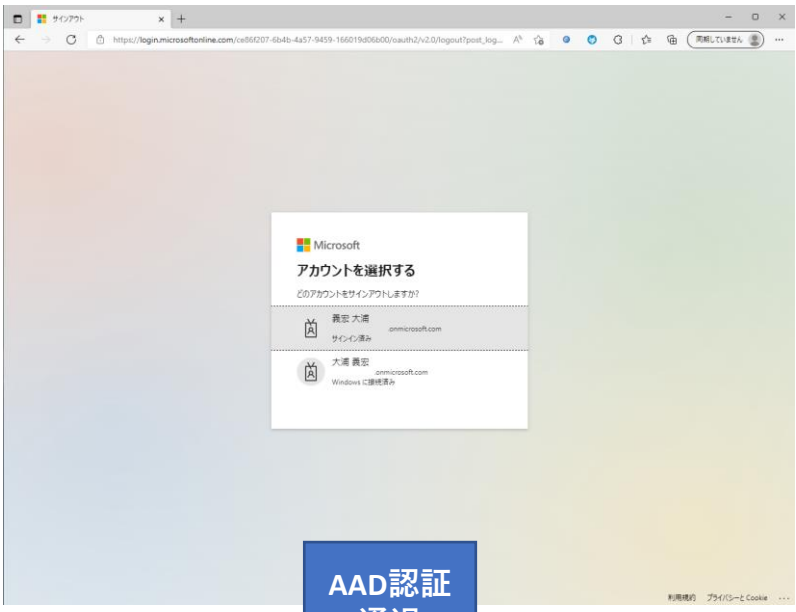
ゼロトラストと境界防御の違い

セキュリティー機能	境界防御による実装	ゼロトラストによる実装
利用者認証	ＩＤとパスワード	多要素認証、リスクベース認証を使いシングルサインオン
業務アプリケーションの利用認可	業務アプリケーションごとに個別に設定	アクセスポリシーに照らして都度判断
サーバー攻撃の検知・防御	境界に置いたファイアウォールやＵＴＭ	セキュリティ情報イベント管理
利用者のＷｅｂアクセス管理	境界に置いたプロキシサーバ	セキュアＷｅｂゲートウェイやクラウド・アクセス・セキュリティー・ブローカー
外部からの業務アプリケーション利用	ＶＰＮ・ＶＤＩ（リモート接続）	アイデンティティ認識型プロキシー
端末管理	資産管理システムなど	モバイルデバイス管理／モバイルアプリケーション管理
端末保護（エンドポイントセキュリティー）	パーソナルファイアウォールとウイルス対策ソフト	エンドポイント・ディテクション＆レスポンス

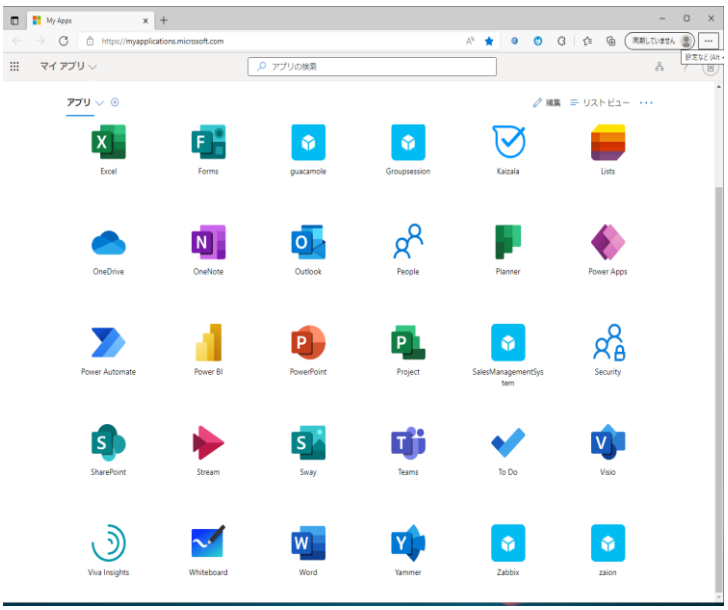
アプリケーションプロキシ利用のメリット

以下は、AADのログインとマイアプリの画面です。
従来はVPNで社内ネットワークに接続後アクセスしていたグループウェアや、勤怠管理ツール、監視ツールのZabbix等がAzure AD Application Proxy経由で利用出来ます。多少処理は重いですが、guacamole等の画面転送型のアプリケーションも動作しています。
これまで、社外からのアクセスを実現する為にネットワークの構築からSSL証明書の取得、その後のメンテナンス作業等に奔走されていたSEの方の負担を軽減します。

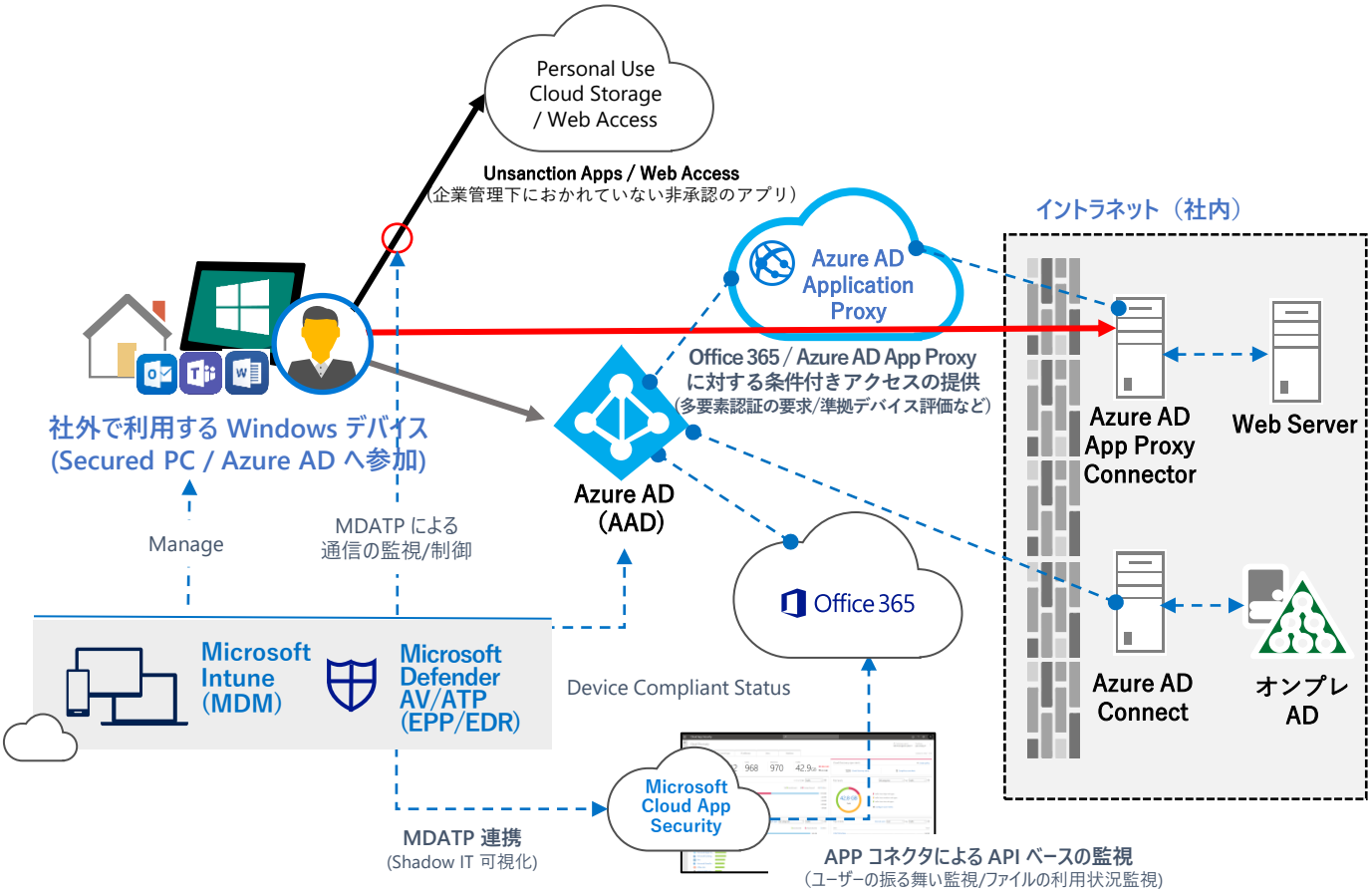
Azure AD（AAD）ログイン画面



マイアプリ画面



ゼロトラストの全体像



NES株式会社
https://www.neskk.co.jp
[本社] 〒930-0138 富山市呉羽町西16番2 Tel 076-403-9100 Fax 076-403-6999
[金沢支店] 〒920-8051 金沢市黒田1丁目33 Tel 076-249-6606 Fax 076-249-6766
[福井営業所] 〒910-0851 福井市米松1丁目16－26 Tel 0776-37-4777 Fax 0776-37-3533