大学等におけるクラウドサービス利用シンポジウム 2016

学認とOffice 365 の認証連携

日本マイクロソフト株式会社

パブリックセクター統括本部

中田　寿穂 <nahisaho@Microsoft.com>

Azure Active Directory てステキ！

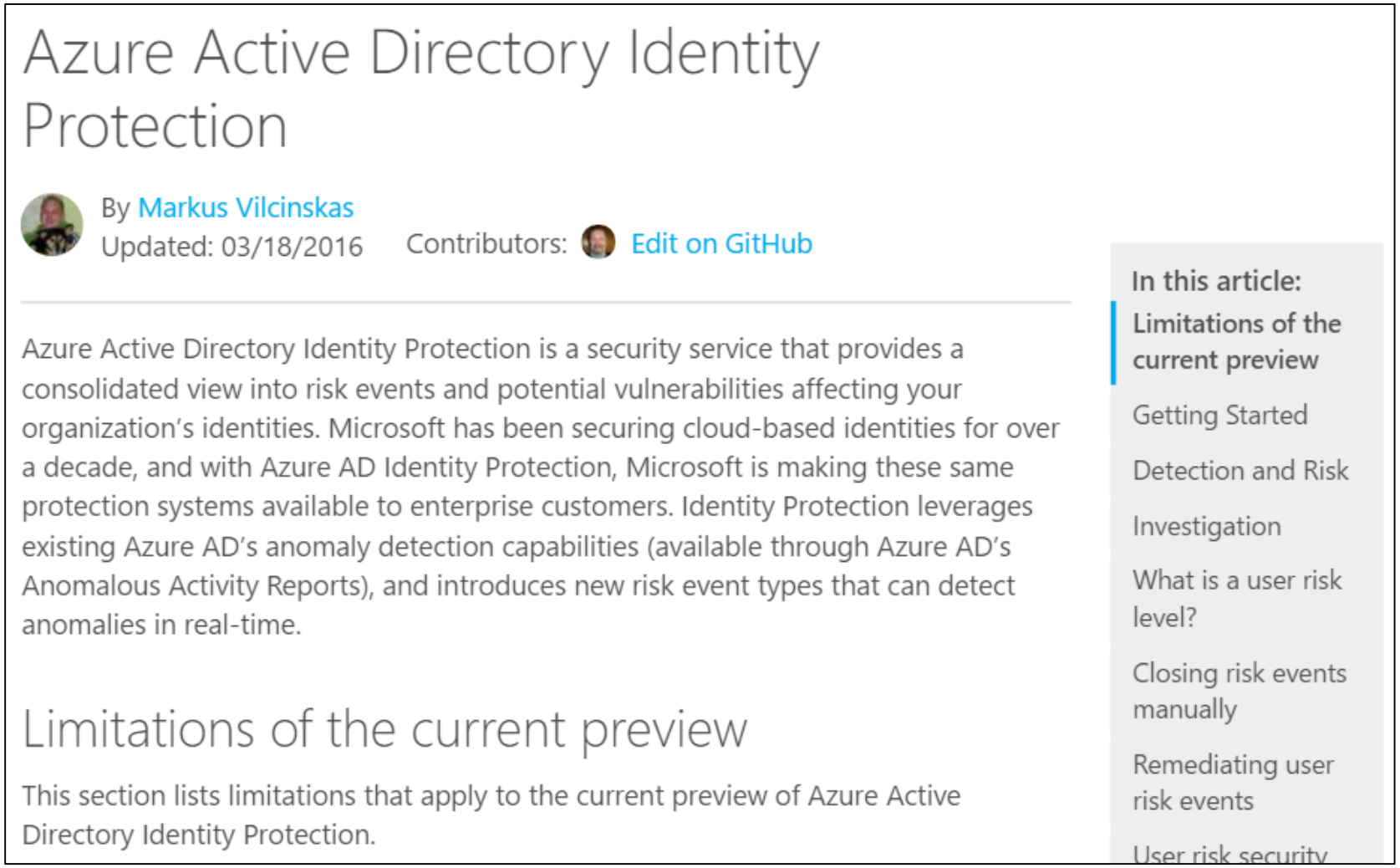
© 2011-2012 Microsoft Corporation All Rights Reserved.

Shibboleth IdP と 認証連携すれば、Azure AD の 多要素認証や
Risk-based 認証が使えるようになるのよ

Azure AD のリバースプロキシを使用すれば、
レガシーなWeb 認証のサービスだって SSO できちゃうワ

クラウドサービスの認証連携だってまかせて
200 以上のサービスに SSO できるのよ

リスクベース認証をサポートした Azure Active Directory



Azure Active Directory Identity Protection

By Markus Vilcinskas
Updated: 03/18/2016 Contributors: Edit on GitHub

Azure Active Directory Identity Protection is a security service that provides a consolidated view into risk events and potential vulnerabilities affecting your organization's identities. Microsoft has been securing cloud-based identities for over a decade, and with Azure AD Identity Protection, Microsoft is making these same protection systems available to enterprise customers. Identity Protection leverages existing Azure AD's anomaly detection capabilities (available through Azure AD's Anomalous Activity Reports), and introduces new risk event types that can detect anomalies in real-time.

Limitations of the current preview

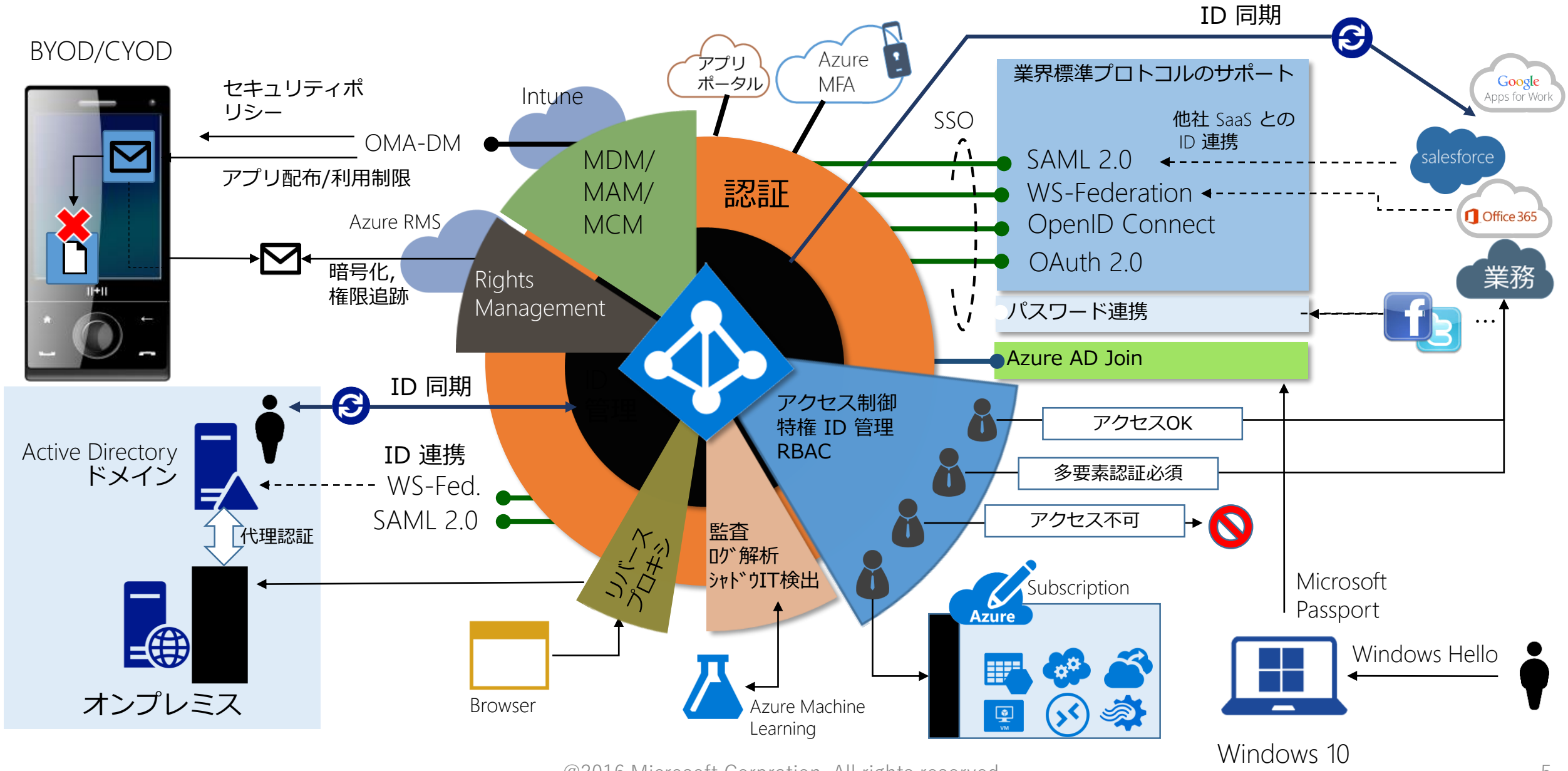
This section lists limitations that apply to the current preview of Azure Active Directory Identity Protection.

In this article:

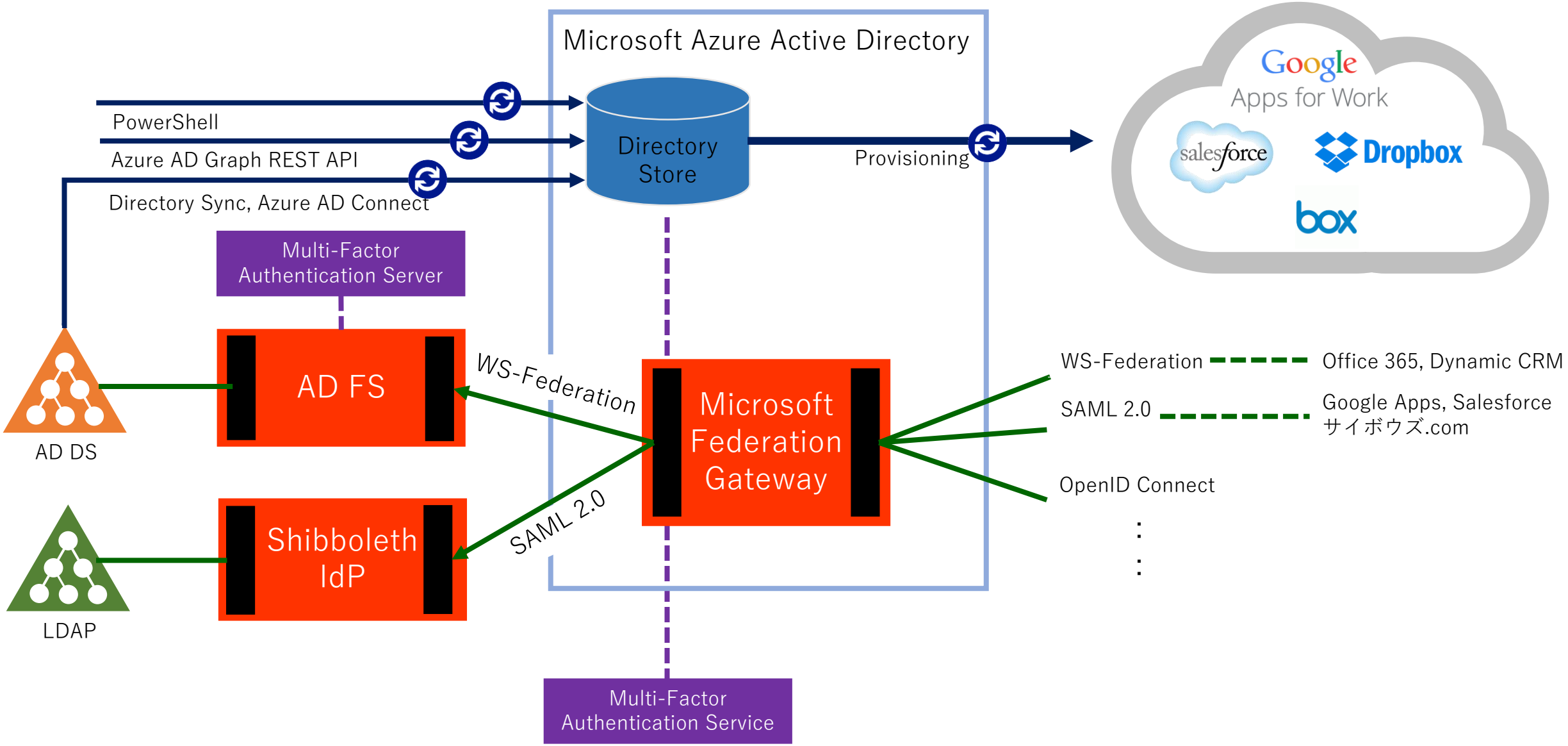
- Limitations of the current preview
- Getting Started
- Detection and Risk
- Investigation
- What is a user risk level?
- Closing risk events manually
- Remediating user risk events
- User risk security

Azure Active Directory とは

Azure Active Directory の機能一覧 Identity as a Service



Azure Active Directory の機能一覧 Identity as a Service



Azure AD の機能

認証

- 外部認証システム(ADFS, Shibboleth)が利用できます。
- 多要素認証が利用できます。
- 業界標準の認証プロトコル(WS-Fed, SAML, OpenID Connect, OAuth 2.0)に対応してます。
- R-Proxy 方式の SSO にも対応できます。

アカウントプロビジョニング

- 様々なクラウドサービスにアカウント連携できます。
- SCIM によるアカウント連携に対応します。

フェデレーションを実現するための Azure AD の ID 管理

フェデレーションで利用できる ID を作成するには

① Azure AD Connect を使用して ADDS から Azure AD にアカウント同期をとる。

② LDAP Manager の LDAP → Office 365 を利用して Azure AD にアカウントを作成する。

フェデレーションを実現するための Azure AD の ID 管理

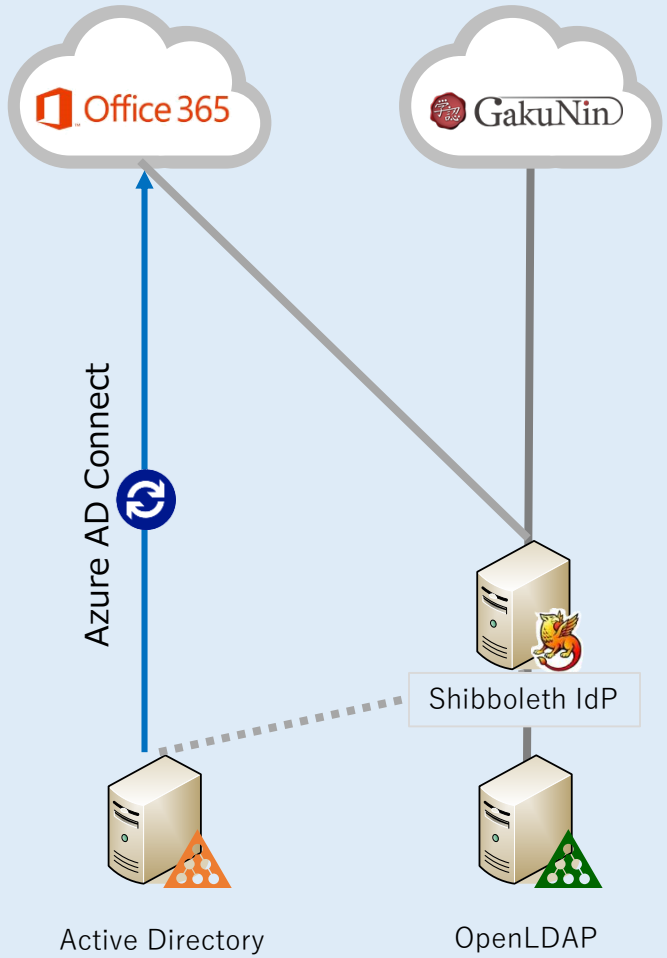
- Azure AD の Immutable ID に適切な属性値をいれることが重要
- Immutable ID = Base64{Object SID}

クラウド ID で運用していたものを フェデレーション ID に変更できますか？

変更可能です。
Azure AD Connect を利用する場合は、 SMTP matching の機能を利用してアカウント同期を行ってください。

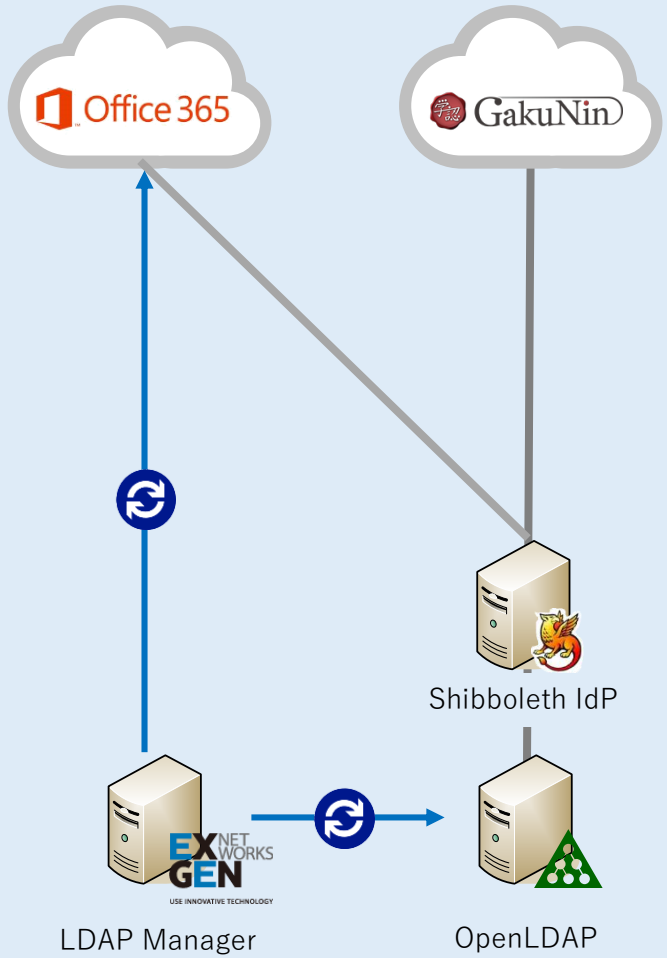
学認、Office 365 認証連携のベストプラクティス

Shibboleth IdP のみで実現 ①



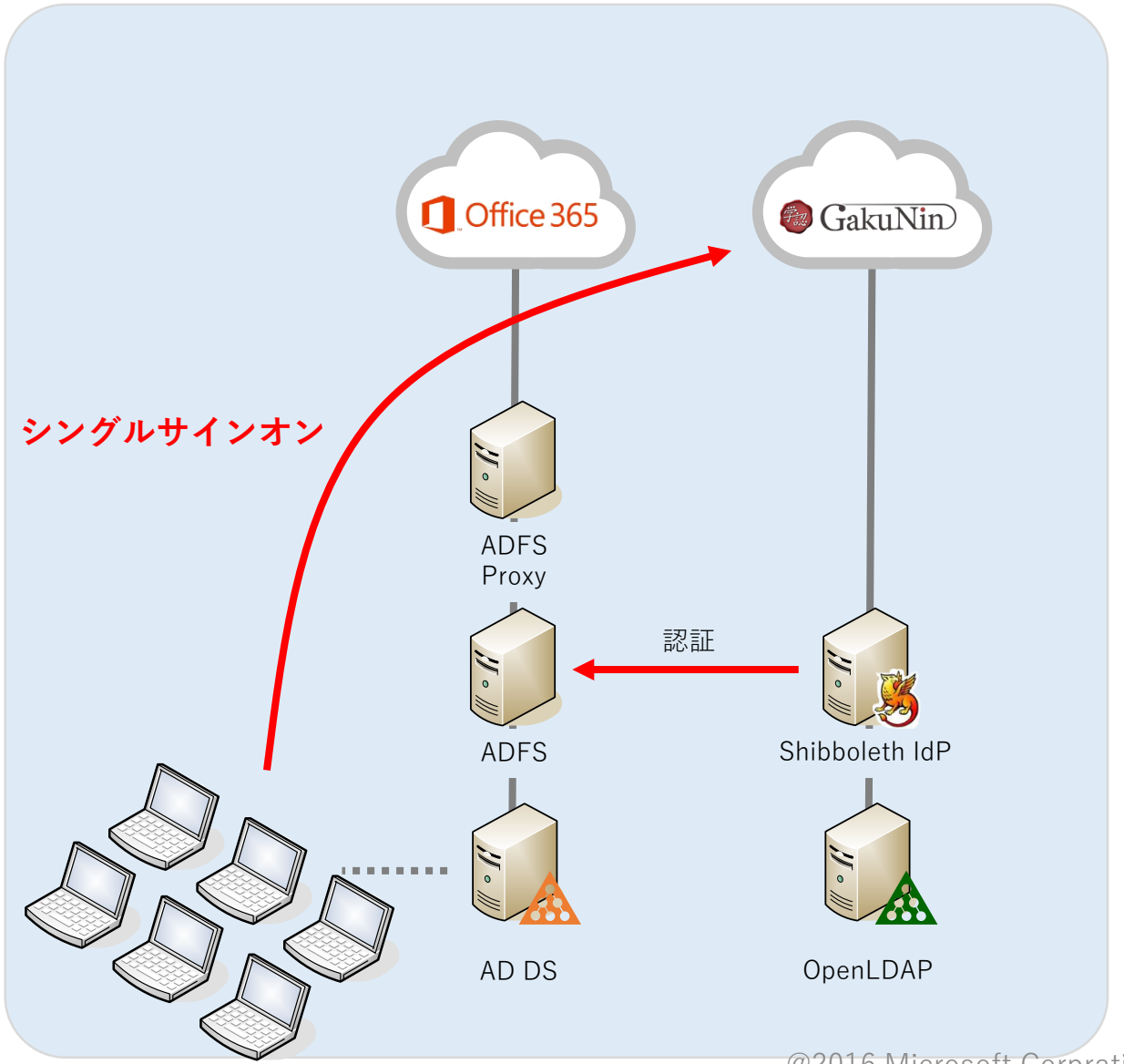
- Azure AD へのアカウント連携は、AD DS を源泉とし、Azure AD Connect で行う。Office 365 の認証を Shibboleth IdP で行う。
- メールクライアントから利用する場合は、Shibboleth IdP の ECP 拡張を行う必要がある。

Shibboleth IdP のみで実現 ②



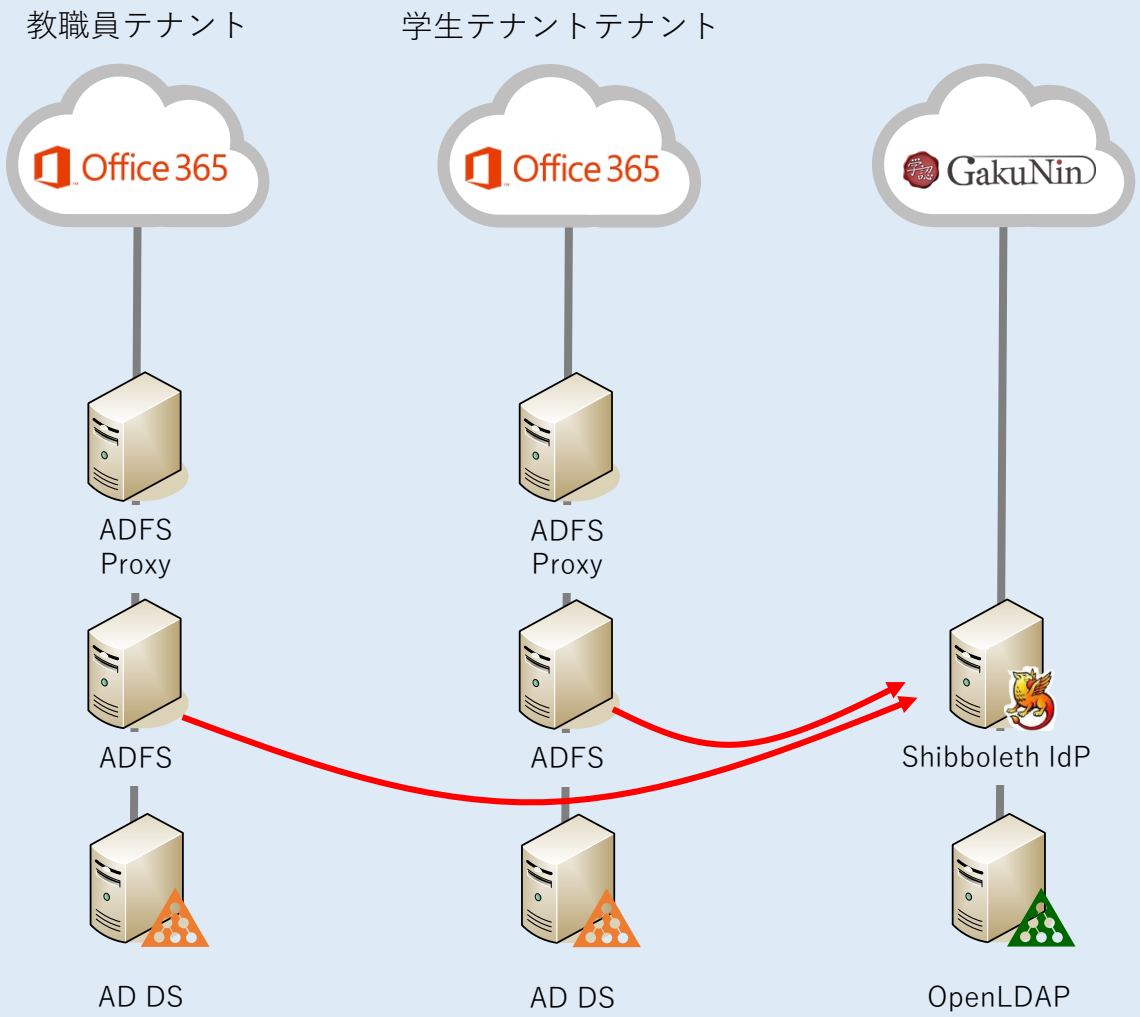
- LDAP Manager を使用して Azure AD のアカウント管理を行う
- メールクライアントから利用する場合は、Shibboleth IdP の ECP 拡張を行う必要がある。
- Windows User CAL は必要としない。

ADFS – Shibboleth IdP 連携 ①



- Shibboleth IdP の認証を AD FS で行う。
- AD ドメインに参加している PC からは、Windows ログイン認証で、学認 SP、Office 365 にシングルサインオンできる。
- Office 365 はシングルテナントにしか対応できない。

ADFS – Shibboleth IdP 連携 ②



- 教職員、学生間で情報共有したくない場合は、テナントを分ける必要がある。
- Office 365 をマルチテナントで運用したい場合のシステム構成。

シングルテナント/マルチドメインの運用時の注意事項

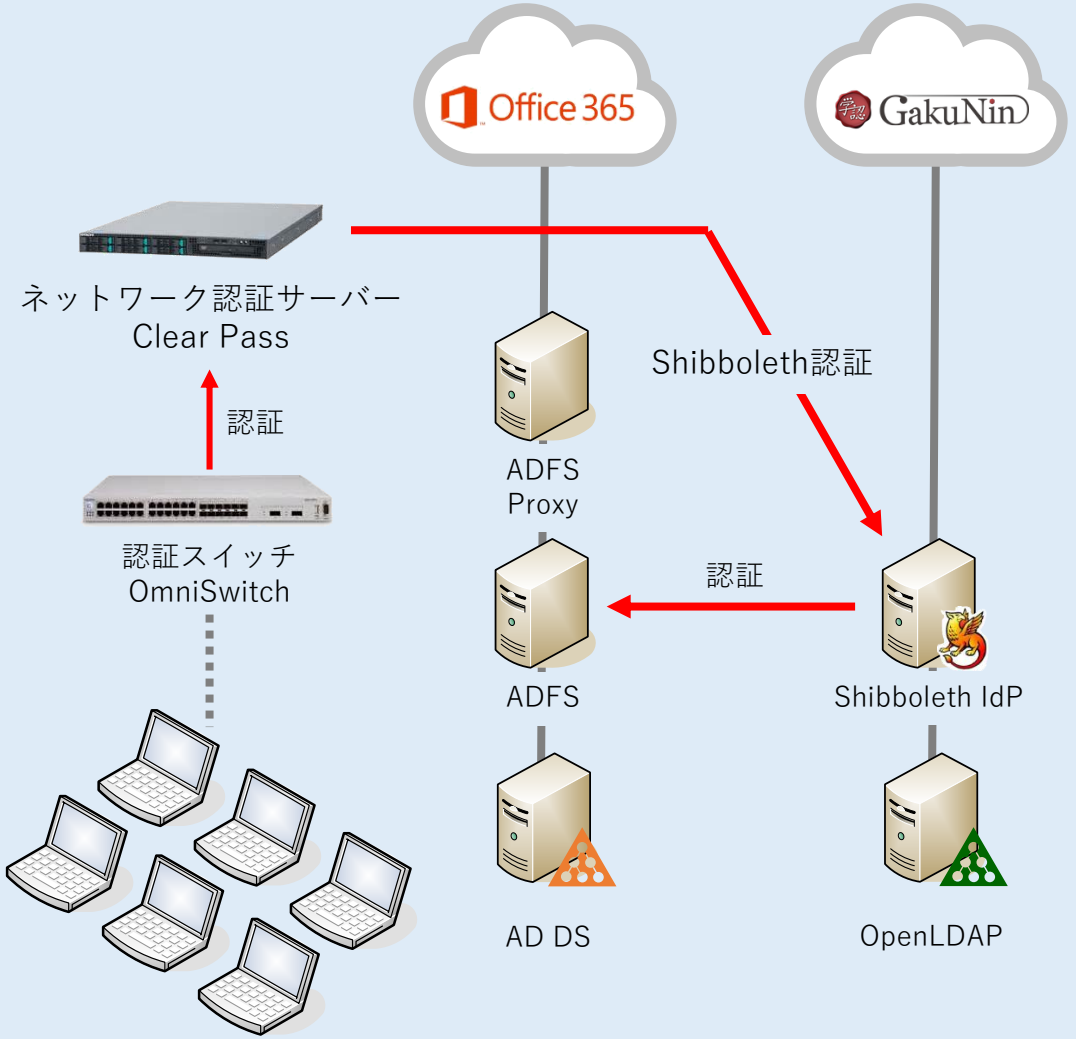
教職員用と学生用の認証方式は同じになってしまう。

教職員用	consoto-u.ac.jp
学生用	st.consoto.ac.jp

教職員用はフェデレーション認証、学生はクラウド認証にしたい場合。

教職員用	staff.consoto-u.ac.jp
学生用	st.consoto.ac.jp

ネットワーク認証による Office 365 と 学認の SSO



- ネットワーク認証を Shibboleth IdP で行うことで、Office 365 と学認SP との SSO が実現可能。

検証協力会社

NTT東日本　ARUBA networks

EXEO　協和エクシオ　SIOS

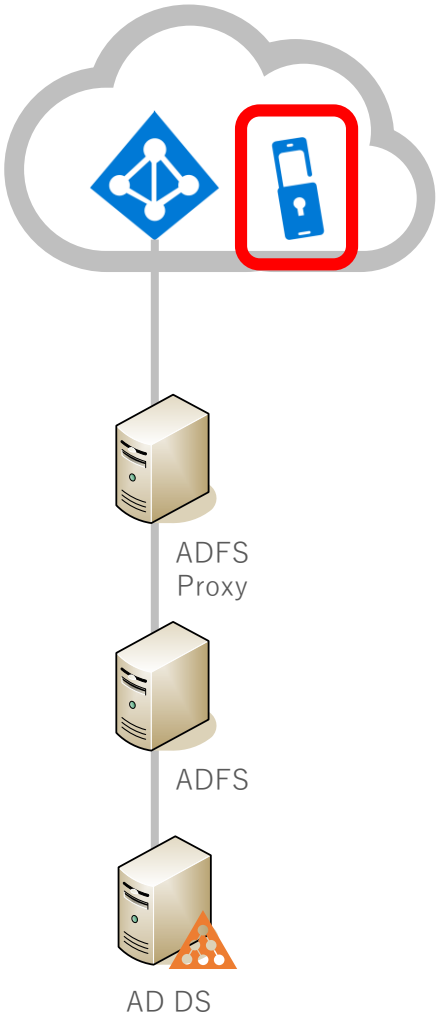
Azure AD Premier の多要素認証

Multi-Factor Authentication for Office 365 と Microsoft Azure Multi-Factor Authentication の違い

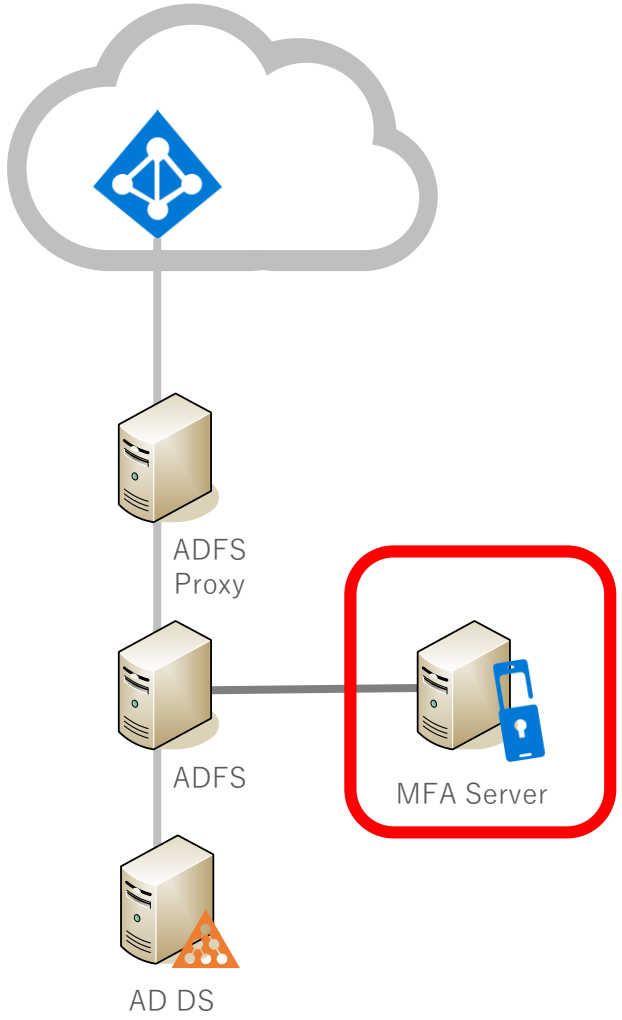
	Multi-Factor Authentication for Office 365	Microsoft Azure Multi-Factor Authentication
管理者がエンドユーザーに対し多要素認証を有効化/強制	○	○
モバイルアプリ	○	○
SMS	○	○
アプリパスワード	○	○
認証用電話音声を変更		○
不正アクセスのアラート		○
イベント確認		○
セキュリティレポート		○
ユーザーのブロック/ブロック解除		○
ワンタイムバイパス		○
認証用発信元電話番号変更		○
MFA サーバー（オンプレアプリ用）		○
MFA SDK（MFAのカスタム）		○

Azure AD Premier の多要素認証

Azure AD 側の多要素認証を使用する



MFAサーバーを使用して多要素認証を使用する



Shibboleth IdP で Azure の MFA を利用するためのシステム構成