

OpenAMによる最新認証連携 ～Office365、Googleとの連携～

株式会社野村総合研究所
IT基盤イノベーション事業本部
オープンソースソリューション推進室
和田 広之



野村総合研究所のOpenStandia（オープンスタンディア）は、おかげさまで、2006年のサービス開始から2011年までの5年間で契約数累計が1,000件を突破いたしました！

株式会社 野村総合研究所 情報技術本部 オープンソースソリューション推進室

Mail : ossc@nri.co.jp Web: <http://openstandia.jp/>



1. Office 365との認証連携
2. Googleとの認証連携(OpenID Connect)

はじめに

● 所属部署

- ▶ オープンソースソリューション推進室
- ▶ OSSを使ったシステム構築から運用までワンストップでサポート
- ▶ 対象OSSは50種類以上
- ▶ OpenStandiaの紹介URL (<http://openstandia.jp/>)

● 私の担当

- ▶ OSSをベースとしたソリューション開発を担当
 - ✓ OpenStandia/SSO&IDM V2を11/5リリース
(<http://www.nri.com/jp/news/2014/141105.html>)
- ▶ OpenAM、OpenIDMの機能拡張、バグ修正等を実施しています

Office 365との認証連携

Office 365との認証連携

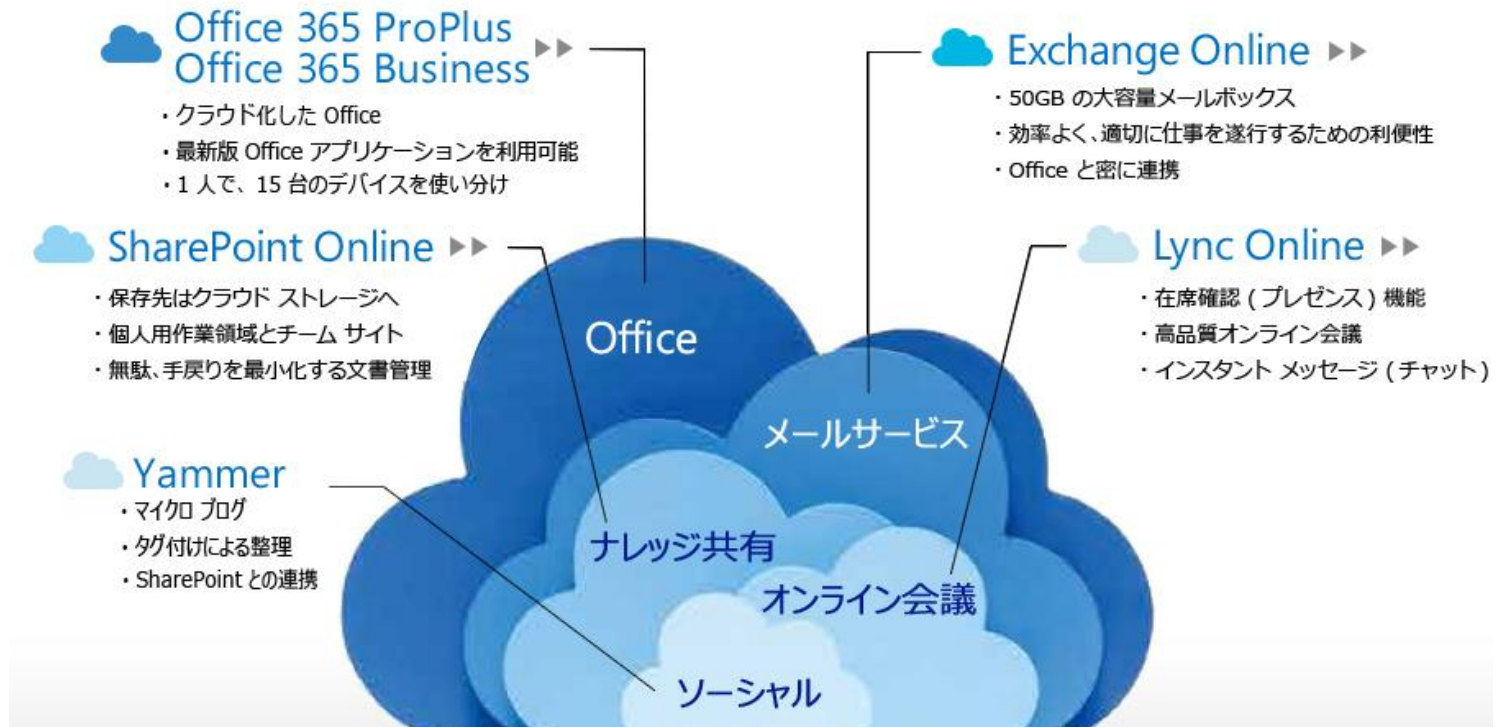
- 企業内だけのSSOから、SaaSも含めたSSOが昨今求められている
- その中でも、Office 365(o365)と認証連携したいニーズが高まっている
- 従来は、Microsoft製品(AD・ADFS)との組み合わせが必要であったが、o365もSAML2.0に対応し、単独で認証連携が可能に

今後活用事例が増えそうな
o365との認証連携をデモを交えて紹介

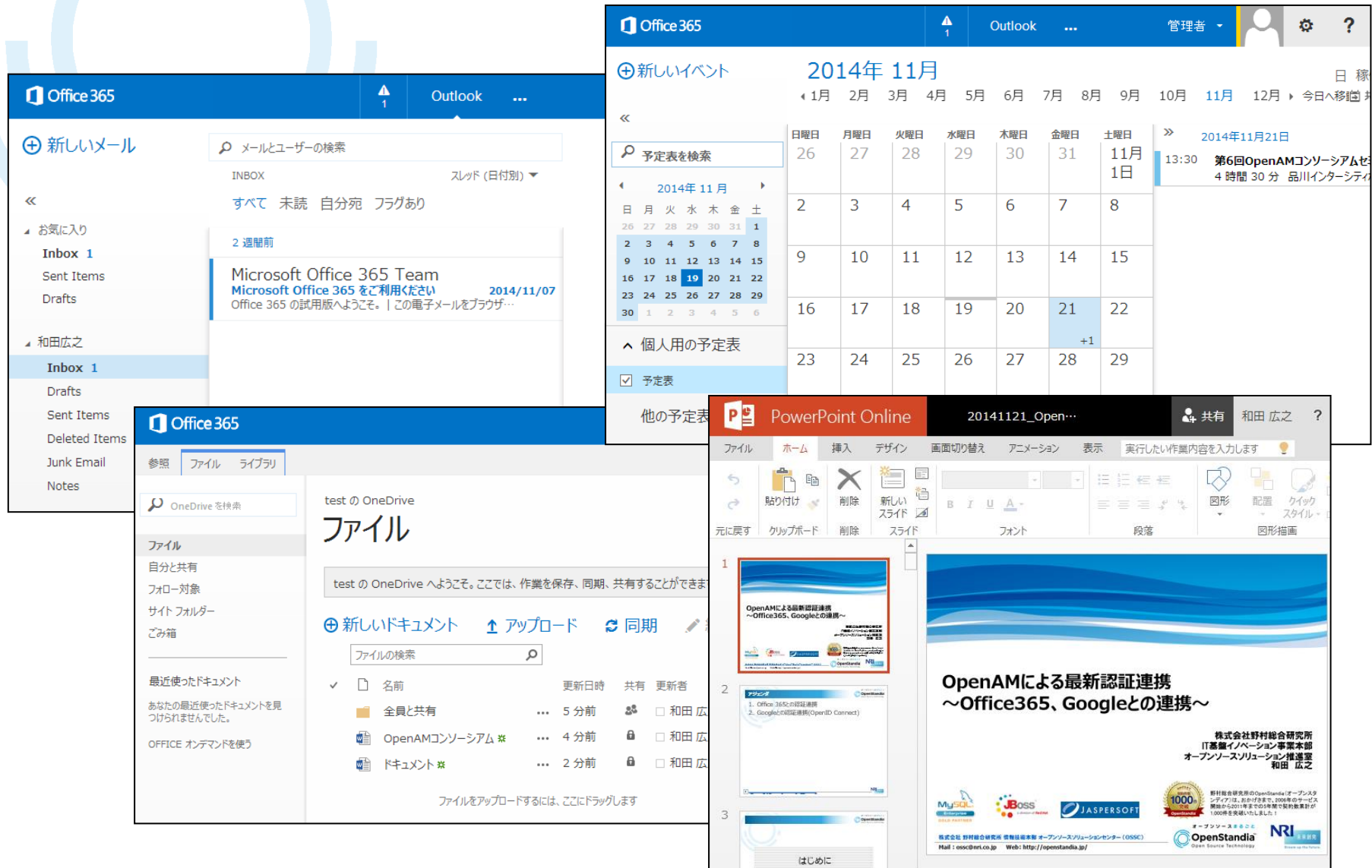
1. Office 365とは
2. 従来の連携方式
3. 新しい連携方式
4. 連携設定のポイント
5. 動作デモ
6. まとめ

● Microsoftが提供する統合的なクラウドサービス

- ▶ メールサービスのExchange Online
- ▶ ナレッジ共有のSharePoint Online
- ▶ オンライン会議のLync Online
- ▶ Office 365 ProPlus



(出所) <http://www.microsoft.com/ja-jp/office/365/about/default.aspx/>



The collage illustrates the integration of various Office 365 services:

- Outlook (Top Left):** Shows the '新しいメール' (New Mail) section with an inbox containing a message from 'Microsoft Office 365 Team' dated 2014/11/07.
- Outlook (Top Right):** Displays the '新しいイベント' (New Event) calendar for November 2014, highlighting a meeting on November 21st.
- OneDrive (Bottom Left):** Shows the 'test の OneDrive' file explorer interface with a list of files and folders, including '全員と共有' (Shared with Everyone).
- PowerPoint Online (Bottom Right):** Displays a presentation slide titled 'OpenAMによる最新認証連携 ~Office365、Googleとの連携~' (Latest authentication integration using OpenAM ~Integration with Office365, Google~).

1. Office 365とは
2. 従来の連携方式
3. 新しい連携方式
4. 連携設定のポイント
5. 動作デモ
6. まとめ

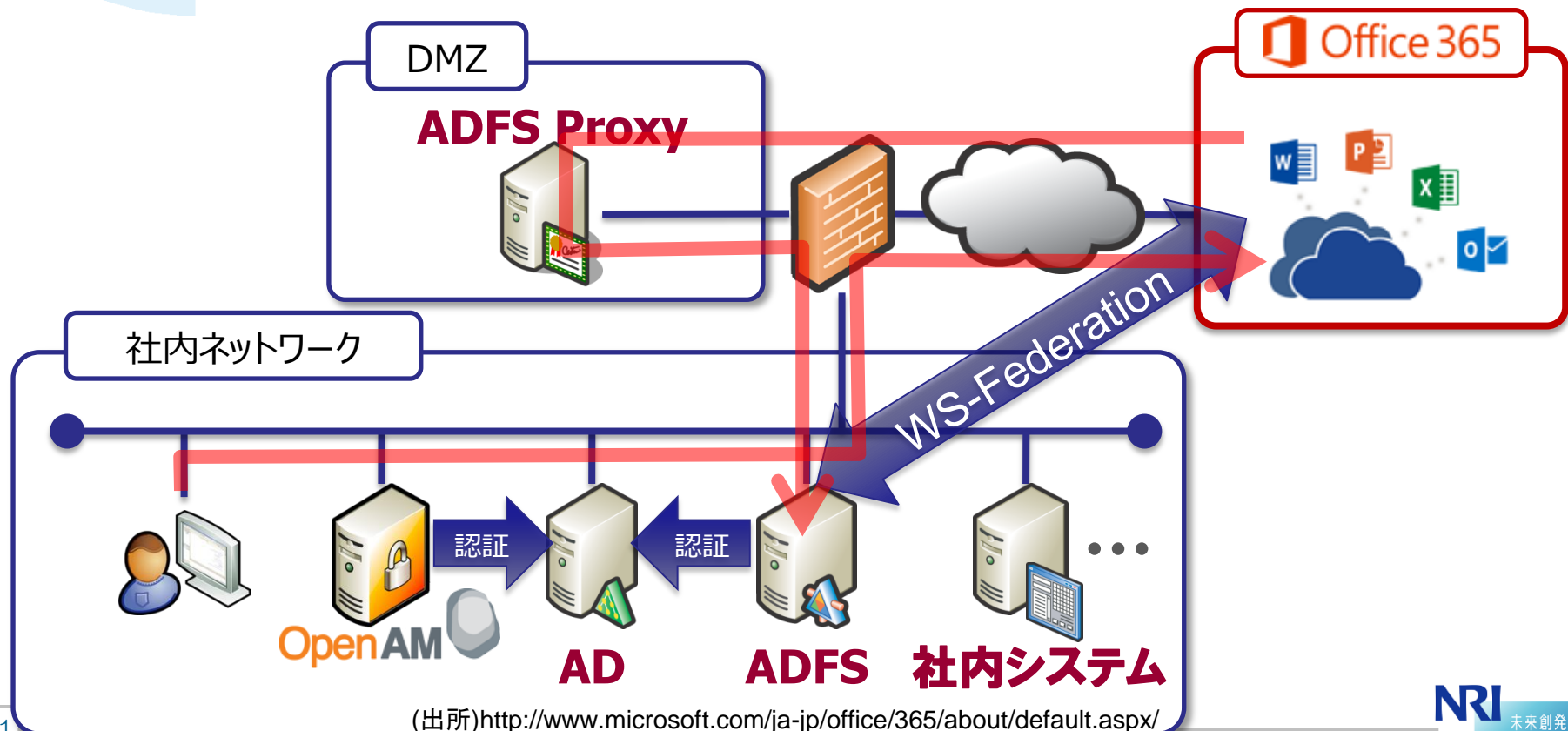
従来の連携方式

- 社内にADがある場合
- 社内にADがない場合

従来の連携方式

● 社内にADがある場合

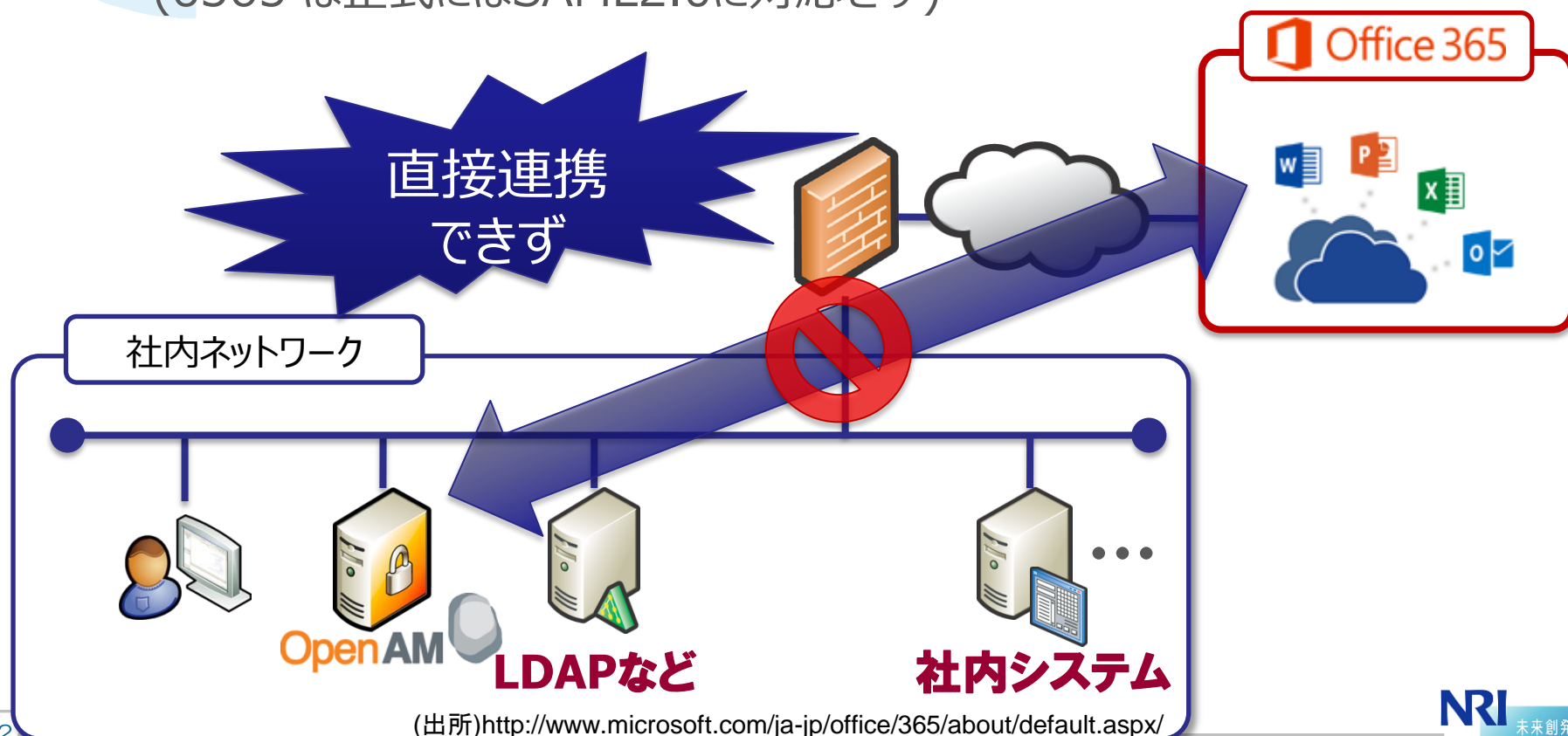
- ▶ **ADFS**(Active Directoryフェデレーションサービス)をo365連携に利用
- ▶ **OpenAM**は**ADを認証先**としてデスクトップSSOを行う
- ▶ Outlookなどのメールクライアントを利用する場合は**ADFS Proxy**が必要



(出所) <http://www.microsoft.com/ja-jp/office/365/about/default.aspx/>

● 社内にADがない場合

- ▶ 認証DBにOpenLDAPやOpenDJなどの**LDAP**、MySQLなどの**RDB**を使用しているケース
- ▶ OpenAMではオフィシャルには認証連携できず
(o365 は正式にはSAML2.0に対応せず)



(出所)<http://www.microsoft.com/ja-jp/office/365/about/default.aspx/>

1. Office 365とは
2. 従来の連携方式
3. 新しい連携方式
4. 連携設定のポイント
5. 動作デモ
6. まとめ

- 2014/03/06に、正式にSAML2.0の対応がMicrosoftよりアナウンスされた

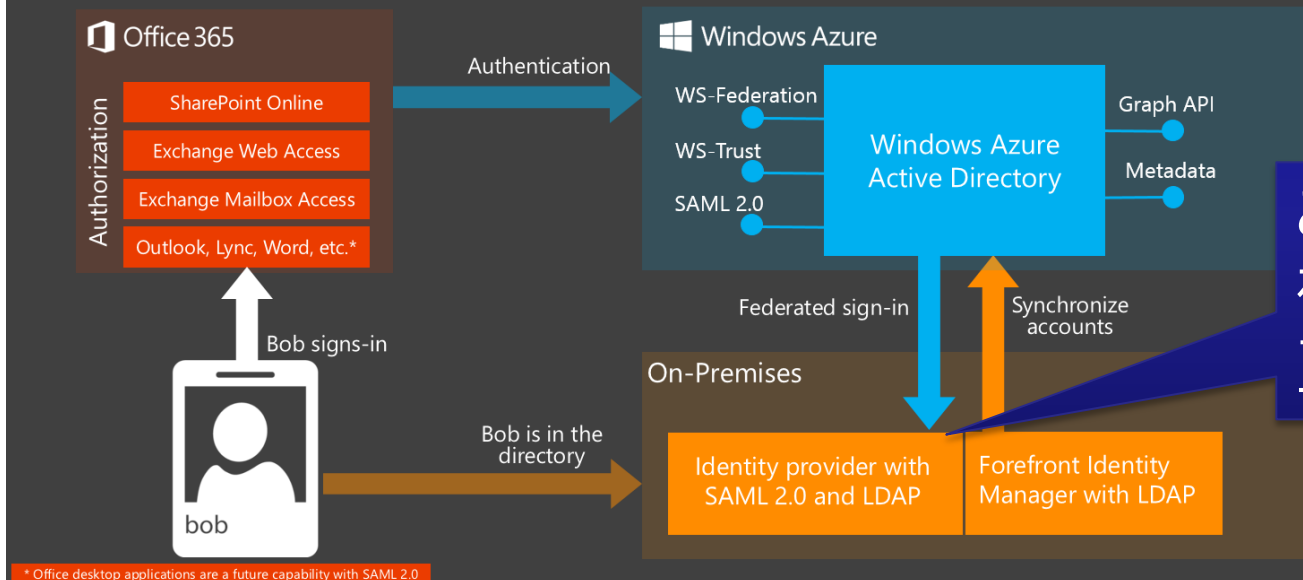
マイクロソフトは、Office 365 ユーザーを対象に、**Security Assertion Markup Language (SAML) 2.0** によるフェデレーションをサポートすることを発表しました。これは、**Active Directory** 以外のオンプレミスの **ID プロバイダー** を利用している Office 365 ユーザーに向けた**新機能**の 1 つで、他の機能と併せて、Web ベースの Office アプリケーションで、アカウントの同期、サインインのフェデレーション、およびシングル サインオンを可能にするパッシブ認証の利用範囲の拡大を実現します。

(出所) http://community.office365.com/ja-jp/b/office_365_community_blog/archive/2014/03/07/office-365-saml-2-0.aspx

新しい連携方式 - o365 のSAML2.0対応

- o365ではAzure ADがアカウント管理・認証に使われている
- Azure ADがSPとなり、OpenAM(IdP)と認証連携(フェデレーション)を行う

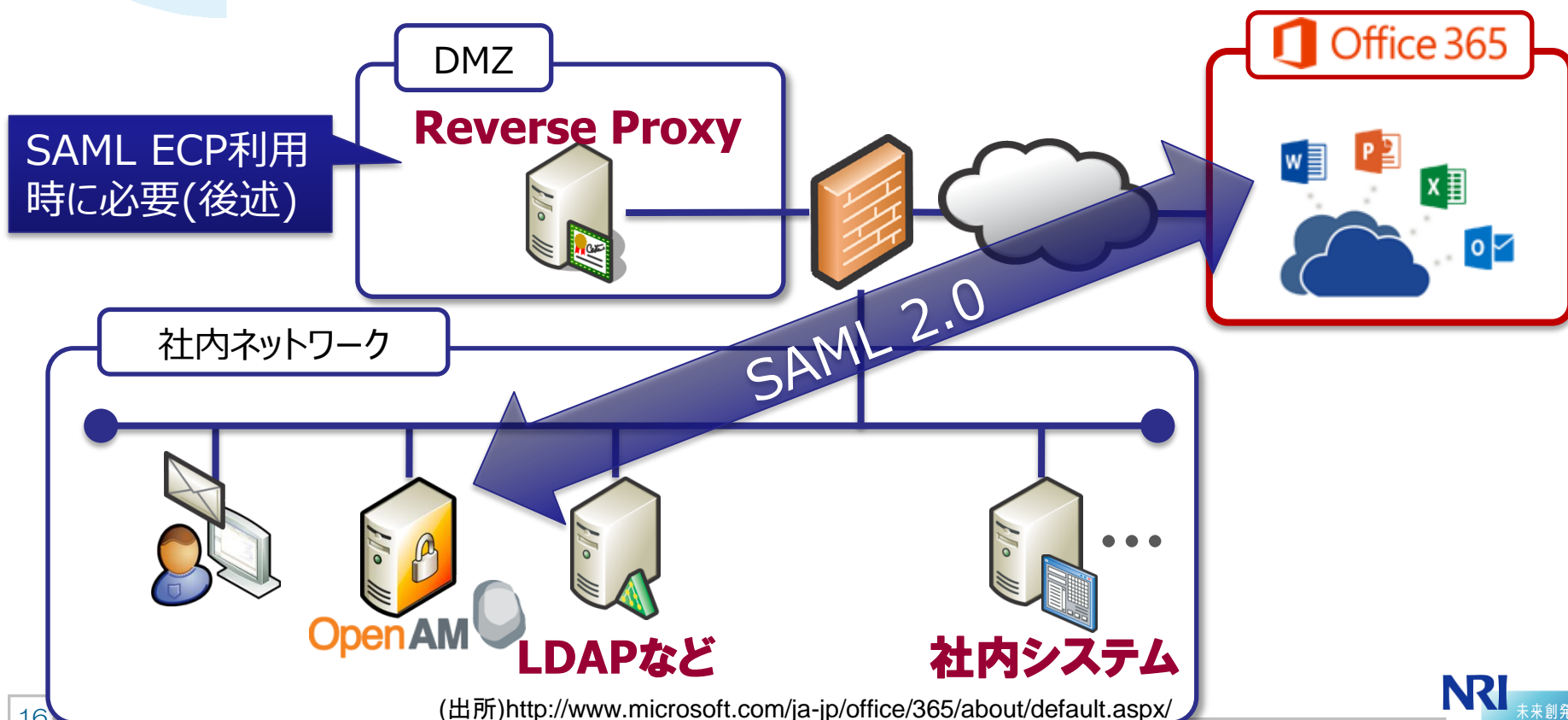
Federated Sign-In using SAML 2.0



* Office desktop applications are a future capability with SAML 2.0

(出所) http://community.office365.com/ja-jp/b/office_365_community_blog/archive/2014/03/07/office-365-saml-2-0.aspx

- ForgeRock社も9月にo365連携の設定方法を公開
 - ▶ <https://wikis.forgerock.org/confluence/display/openam/Microsoft+Office+365+Integration>
- 構成例



(出所) <http://www.microsoft.com/ja-jp/office/365/about/default.aspx/>

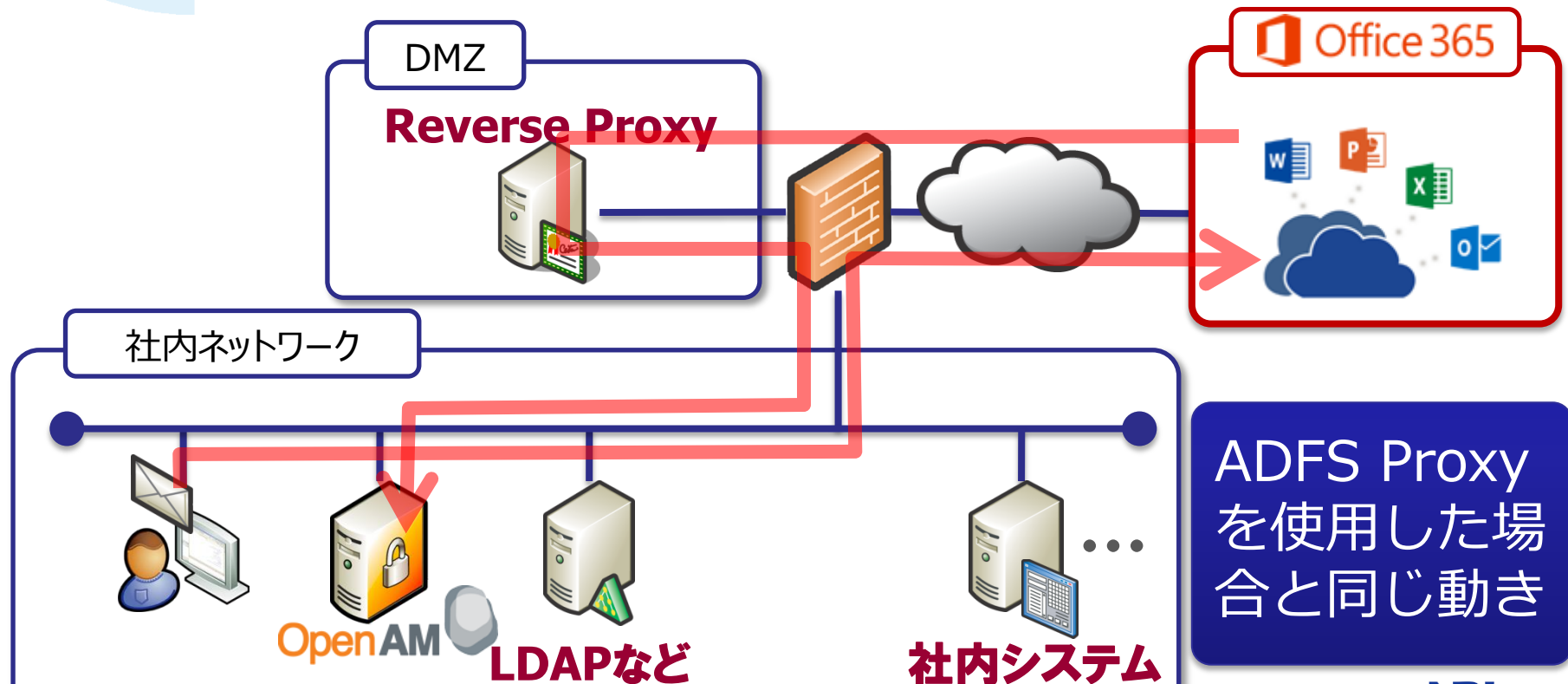
注意点:SAML 2.0による連携時の制約

- Office デスクトップアプリケーションは対象外
 - ▶ Lync デスクトップ クライアントの使用
 - ▶ ただし、2014年後半にSAML 2.0にも対応予定との話もある
- メールクライアントを利用する場合はSAML ECPへの対応が必要
 - ▶ Outlook デスクトップ クライアントの使用
 - ▶ モバイル クライアントから Exchange Online への接続

※ECPについては次のスライドで補足

SAML ECP (Enhanced Client or Proxy) とは

- 大まかに言うとブラウザ以外(リダイレクトに対応していない)のクライアントをSAMLで認証するための仕様
- o365の場合、Outlookなどのメールクライアントが対象
- o365を経由してOpenAMにSOAPで認証要求が渡ってくる



(出所) <http://www.microsoft.com/ja-jp/office/365/about/default.aspx/>

- OpenAMに対してインターネットからアクセス許可が必要
 - ▶ 何も考えないで構築すると、社外からのo365アクセスでメールが使えるしまうので注意
 - ▶ 社外からの利用を禁止する場合は、アクセス元のIPアドレスにてアクセス制限を適切に行う必要がある
- SSL証明書が必要
 - ▶ o365からのアクセスはSSLが必須
 - ▶ アクセス元はMSなので、MSが対応している認証局が発行した物が必要
- OpenAMではECPに対応しているが、現状そのままでは動作しない
 - ▶ ECPのモジュール拡張が必要(BASIC認証でアクセス許可するように)

ECPに対応しない場合は、メール機能はWebメール
(OWA:Outlook Web App)の利用に限定させる必要あり

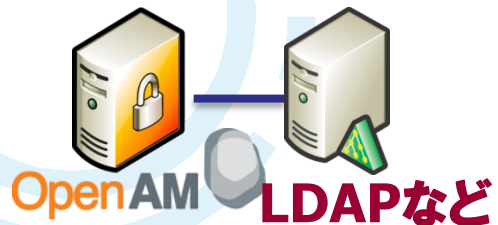
o365のSAMLメッセージの要件

- HTTPSが必須
- サポート対象のバインディング方式
 - ▶ ログインはHTTP POST、ログアウトはREDIRECT
- 必須属性
 - ▶ NameID: o365ユーザの**ImmutableID**と同じ値
 - ▶ IDPEmail: o365ユーザの**UserPrincipalName(UPN)**と同じ値
 - ▶ Issuer: IdPのURIで、o365に設定された物と同じ値
- NameIDフォーマットURI
 - ▶ urn:oasis:names:tc:SAML:2.0:nameid-format:**persistent**

※<http://technet.microsoft.com/ja-jp/library/dn641269.aspx> に詳細は記載

アカウント紐づけ情報をOpenAM側で永続化する必要あり

SAML利用時のアカウントの紐づけ



Account
Linking

Office 365



uid: demo1
 sn: 野村
 givenName: 太郎
 mail: demo1@openamdemo.mydns.jp
 sun-fm-saml2-nameid-info: https://sso.openamdemo.mydns.jp:443/openam|urn:federation:MicrosoftOnline|demo1|https://sso.openamdemo.mydns.jp:443/openam|urn:oasis:names:tc:SAML:2.0:nameid-format:persistent|urn:microsoftonline:IDPRole|false
 ...

SAML レスポンス

```
<samlp:response ...>
...
<saml:subject>
...
  <saml:nameid ...>demo1</saml:nameid>
</saml:subject>
...
<saml:attribute statement>
  <saml:attribute name="IDPEmail">
    <saml:attributevalue ...>
      demo1@openamdemo.mydns.jp
    </saml:attributevalue>
  </saml:attribute>
</saml:attribute statement>
</saml:assertion>
</samlp:response>
```

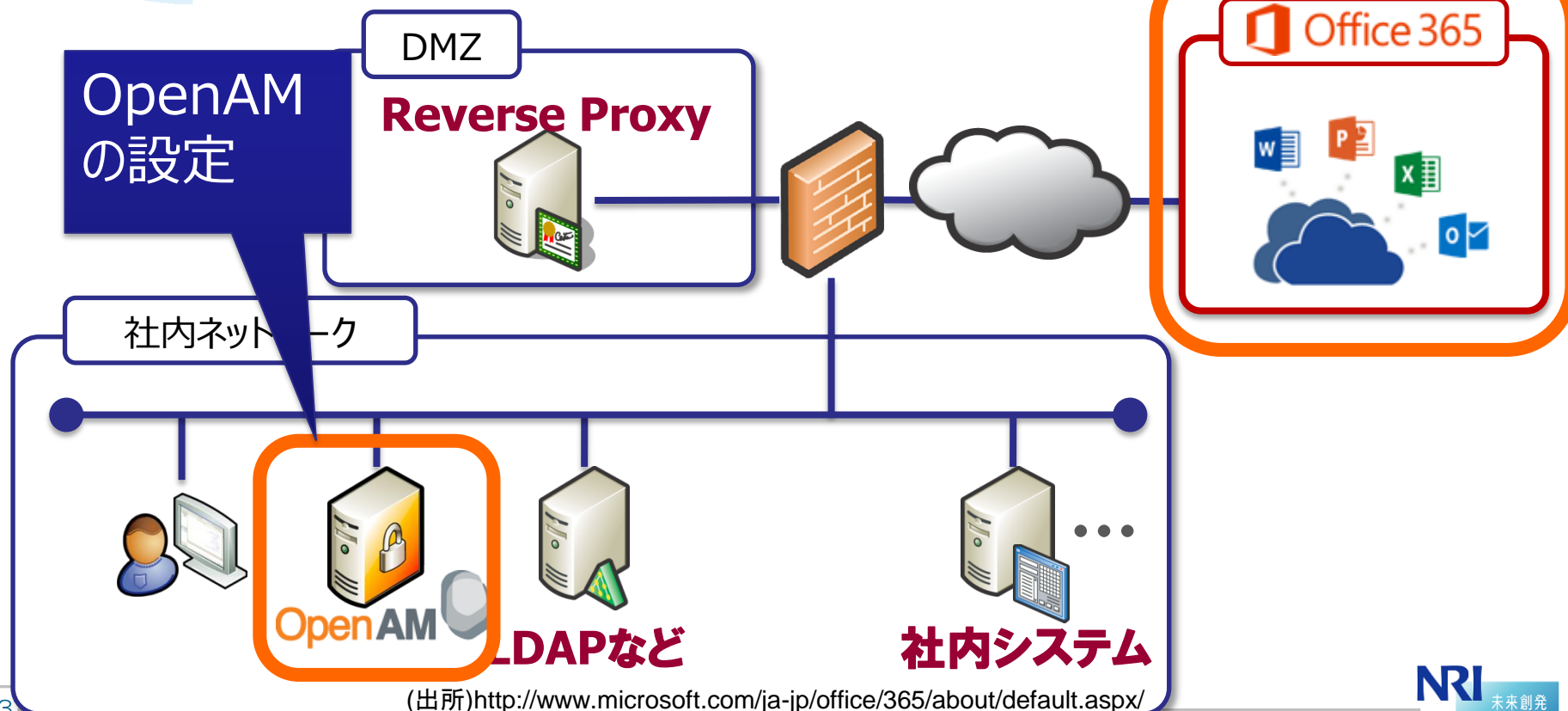
UserPrincipalName: demo1@openamdemo.mydns.jp
 ImmutableID: demo1
 LastName: 野村
 FirstName: 太郎
 UsageLocation: JP
 ...

1. Office 365とは
2. 従来の連携方式
3. 新しい連携方式
4. 連携設定のポイント
5. 動作デモ
6. まとめ

OpenAM – o365 連携設定のポイント

- OpenAMの設定
- o365の設定

o365の設
定



- IDPの作成(CoTの作成)
- リモートSPの登録(o365のメタデータのインポート)
- 属性マッピング設定
- IDPメタデータのエクスポート
- 接続テスト用ユーザの登録

● 管理画面から設定ウィザードを開き作成

このサーバー上に SAMLv2 アイデンティティプロバイダを作成します

このページにより、OpenAM サーバーのこのインスタンスをアイデンティティプロバイダ (IDP) として設定し、証明書を設定できます。OOT とは、相互に信頼しており、実質的にすべての連携通信が実行される範囲を表行するために必要な設定や、この設定を OOT 内のほかのエンティティ (たとえば、SP) に伝えるための情報がある場合は、このプロバイダのレルムを選択する必要があります。そうしない場合、このプロバイダは re

このプロバイダのメタデータがありますか? ☐ はい ☒ いいえ ⓘ

メタデータ

* 名前: ⓘ

署名鍵: 「test」は、インストール時にテストの目的で設定された自己署名付き証明書であることを示します。

トラストサークル

表示されている既存のトラストサークルから選択するか、またはこの IDP を含むように作成するトラストサークル (IDP と SP のグループ) です。

* 新しいトラストサークル:

リモートSPの登録 (o365のメタデータのインポート)

- o365のメタデータを下記URLから取得
 - ▶ <https://nexus.microsoftonline-p.com/federationmetadata/saml20/federationmetadata.xml>
- 取得したXMLから、
<signature>...</signature>を削除してから
OpenAMにインポート

SAMLv2 リモートサービスプロバイダを作成します

このページにより、リモートサービスプロバイダ (SP) を登録できます。トラストサークル (COT)、およびプロバイダのメタデータは、連携プロトコル (たとえば、SAMLv2) を実行するために必要な設定や、この設定を COT 内のほかのエンテ...

メタデータファイルはどこに存在しますか?:

☐ URL ☒ ファイル 

* メタデータが配置されている URL:



アップロード...

C:\fakepath#federationmetadata.xml

- SAMLレスポンスの**IDPEmail**属性にメールアドレスを設定するようにマッピング定義を行う

SP			
表明コンテンツ	表明処理	サービス	高度

urn:federation:MicrosoftOnline

▼ 属性マッパー

▼ アーティファクトメッセージのエンコーディング

属性マッパー

属性マップ

現在の値

削除

新しい値

IDPEmail=mail

追加

「IDPEmail=mail」を
SP側の属性マッパーに設
定しておく

このマッピングは、属性マッパーで使用する設定です。マッピングは、表明内で SAML ATTRIBL

● OpenAMのメタデータ出力URLにアクセスし保存

▶例)

<https://sso.openamdemo.mydns.jp/openam/saml2/jsp/exportmetadata.jsp?realm=/&entityid=https://sso.openamdemo.mydns.jp:443/openam>

▶青字の部分をo365側の設定時に利用する

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<EntityDescriptor entityID="https://sso.openamdemo.mydns.jp:443/openam" xmlns="urn:oasis:names:tc:SAML:2.0:metadata">
  <IDPSSODescriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>
MIICQDCCAa ... ==
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </KeyDescriptor>
    ...
    <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://sso.openamdemo.mydns.jp:443/openam/IDPSloRedirect/metaAlias/idp"
ResponseLocation="https://sso.openamdemo.mydns.jp:443/openam/IDPSloRedirect/metaAlias/idp"/>
    ...
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://sso.openamdemo.mydns.jp:443/openam/SSOPOST/metaAlias/idp"/>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="https://sso.openamdemo.mydns.jp:443/openam/SSOSoap/metaAlias/idp"/>
    ...
  </IDPSSODescriptor>
</EntityDescriptor>
```

● o365側のアカウントとの紐づけのため、下記情報を追加設定

- ▶ o365側のUserPrincipalNameと同じ値(メールアドレス)を**mail**属性に
- ▶ o365側のImmutableIDと同じ値(デモではuidの値を利用)を**sun-fm-saml2-nameid-info**に登録

uid: demo1

sn: 野村

givenName: 太郎

mail: demo1@openamdemo.mydns.jp

sun-fm-saml2-nameid-info: https://sso.openamdemo.mydns.jp:443/openam|urn:federation:MicrosoftOnline|demo1|https://sso.openamdemo.mydns.jp:443/openam|urn:oasis:names:tc:SAML:2.0:nameid-format:persistent|null|urn:federation:MicrosoftOnline|IDPRole|false

...

o365側の設定

- ドメインの追加
- フェデレーションドメインの設定
- テスト用のユーザ追加

ドメインの追加

- デフォルトのドメインではフェデレーションの設定ができないため、o365に独自ドメインを追加する
 - ▶ **所有しているドメインが必要**
 - ▶ ドメインの所有権確認用に、**DNSサーバに対してTXTまたはMXレコードの設定が必要**
 - ▶ デモではフリーのDDNSサービスであるmydns.jpで取得したドメインを利用

ドメインを追加する

1. ドメイン名の指定

2. 所有権の確認

3. 完了

ドメイン名の入力

既に所有しているドメイン名のみを追加することができます。まだドメインをお持ちでない場合は、Gの代わりに設定いたします。

例: contoso.com

● PowerShellで設定

- ▶ Azure AD Module のインストールも必要
- ▶ Connect-MsolService で接続(ログイン)
- ▶ Set-MsolDomainAuthentication で追加したドメインをフェデレーション用に設定する

フェデレーションドメインの設定

- ▶ 設定値にOpenAMのメタデータに記載の値を指定
 - ✓ ECPの設定は、HTTPSでないとエラーになるので注意
 - ✓ ECPを使用しない場合は、-ActiveLogOnUriの設定なしでコマンドを実行すればOK

```
$dom = "openamdemo.mydns.jp"  
$url = "https://sso.openamdemo.mydns.jp/openam/SSOPOST/metaAlias/idp"  
$ecp="https://sso.openamdemo.mydns.jp/openam/SSOSoap/metaAlias/idp"  
$entity = "https://sso.openamdemo.mydns.jp:443/openam"  
$logout = "https://sso.openamdemo.mydns.jp/openam/IDPSloRedirect/metaAlias/idp"  
$cert = "MIIC...0Q=="
```

```
Set-MsolDomainAuthentication -DomainName $dom `  
-FederationBrandName $dom `  
-Authentication Federated `  
-PassiveLogOnUri $url `  
-SigningCertificate $cert `  
-IssuerUri $entity `  
-ActiveLogOnUri $ecp `  
-LogOffUri $logout `  
-PreferredAuthenticationProtocol SAML
```

OpenAMのメタデータXMLから該当箇所をコピー

● PowerShellの下記コマンドでテスト用ユーザを作成

- ▶ この時指定する**UserPrincipalName**と**ImmutableId**が重要
- ▶ OpenAM側のユーザとの紐づけに使用される

```
new-msoluser `
-DisplayName "野村 太郎" `
-UserPrincipalName demo1@openamdemo.mydns.jp `
-UsageLocation JP `
-ImmutableId demo1
```

● 作成ユーザにライセンス付与



パスワードのリセット 削除
編集 グループ

プライマリ電子メール アドレス:
このユーザーには Exchange メールボックス

割り当て済みのライセンス:
ライセンスなし 編集



保存 破棄

ライセンスの割り当て

利用できるサービスは所在地によって異なります。 [ライセンスの制限に関する詳細情報](#)

ユーザーの所在地の設定

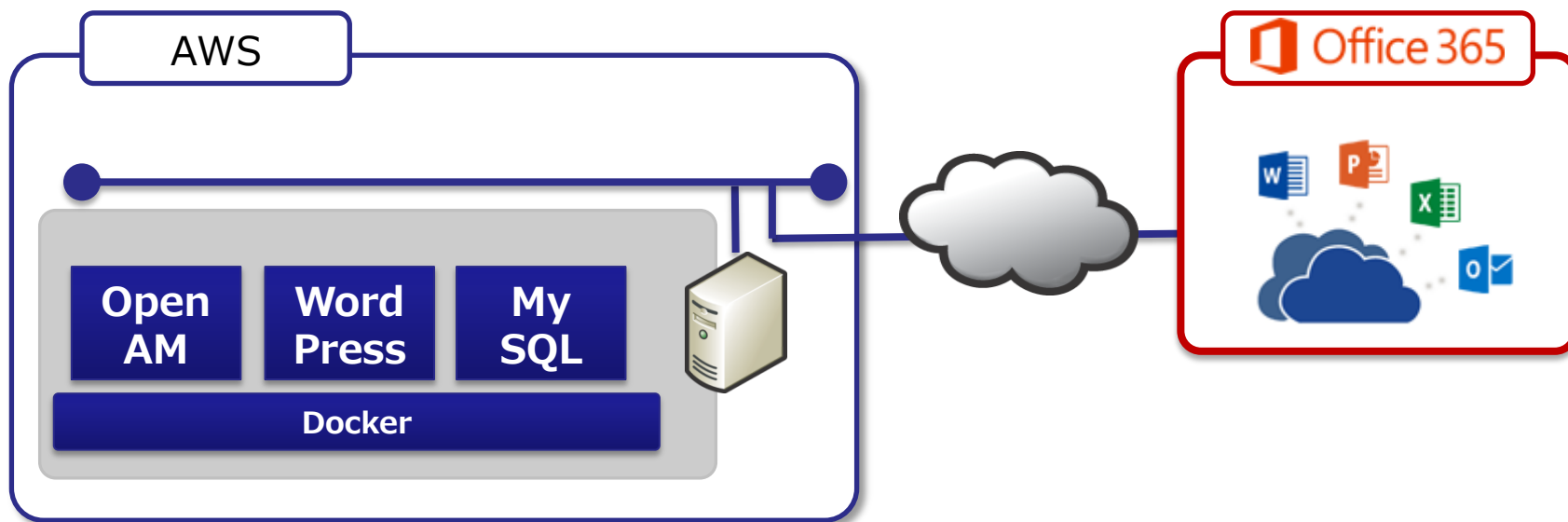
日本

☒ Office 365 Business Premium
25 ライセンス中 22 ライセンスが使用可能 [さらに購入](#)

1. Office 365とは
2. 従来の連携方式
3. 新しい連携方式
4. 連携設定のポイント
5. 動作デモ
6. まとめ

● 構成

- ▶ AWSを利用しインターネット上に構築
- ▶ 認証・データストアにはOpenAMに付属の組込OpenDJを利用
- ▶ SSO保護対象アプリケーションとしてWordPressを構築



● SP起点でログイン

- ▶ ユーザはSP(o365)にまずアクセス
 - ✓ <https://login.microsoftonline.com/login.srf>
- ▶ IdP(OpenAM)で認証
- ▶ SP(o365)にアクセス

● IdP起点でログイン

- ▶ ユーザはIdP(OpenAM)にまずアクセス
 - ✓ <https://sso.openamdemo.mydns.jp/openam/saml2/jsp/idpSSOInit.jsp?metaAlias=/idp&spEntityID=urn:federation:MicrosoftOnline&NameIDFormat=urn:oasis:names:tc:SAML:2.0:nameid-format:persistent>
- ▶ IdP(OpenAM)で認証
- ▶ SP(o365)にアクセス

- SP起点の場合、ログインIDの入力が必要
 - ▶ 共通ログイン画面にてログインIDの入力が求められる
 - ▶ Office 365は入力されたログインIDのドメイン名をもとに、IdPへのリダイレクトを行う仕様
 - ▶ ポータルサイトなどにIdP起点のURLリンクをつけるなどの対応が必要

1. Office 365とは
2. 従来の連携方式
3. 新しい連携方式
4. 連携設定のポイント
5. 動作デモ
6. まとめ

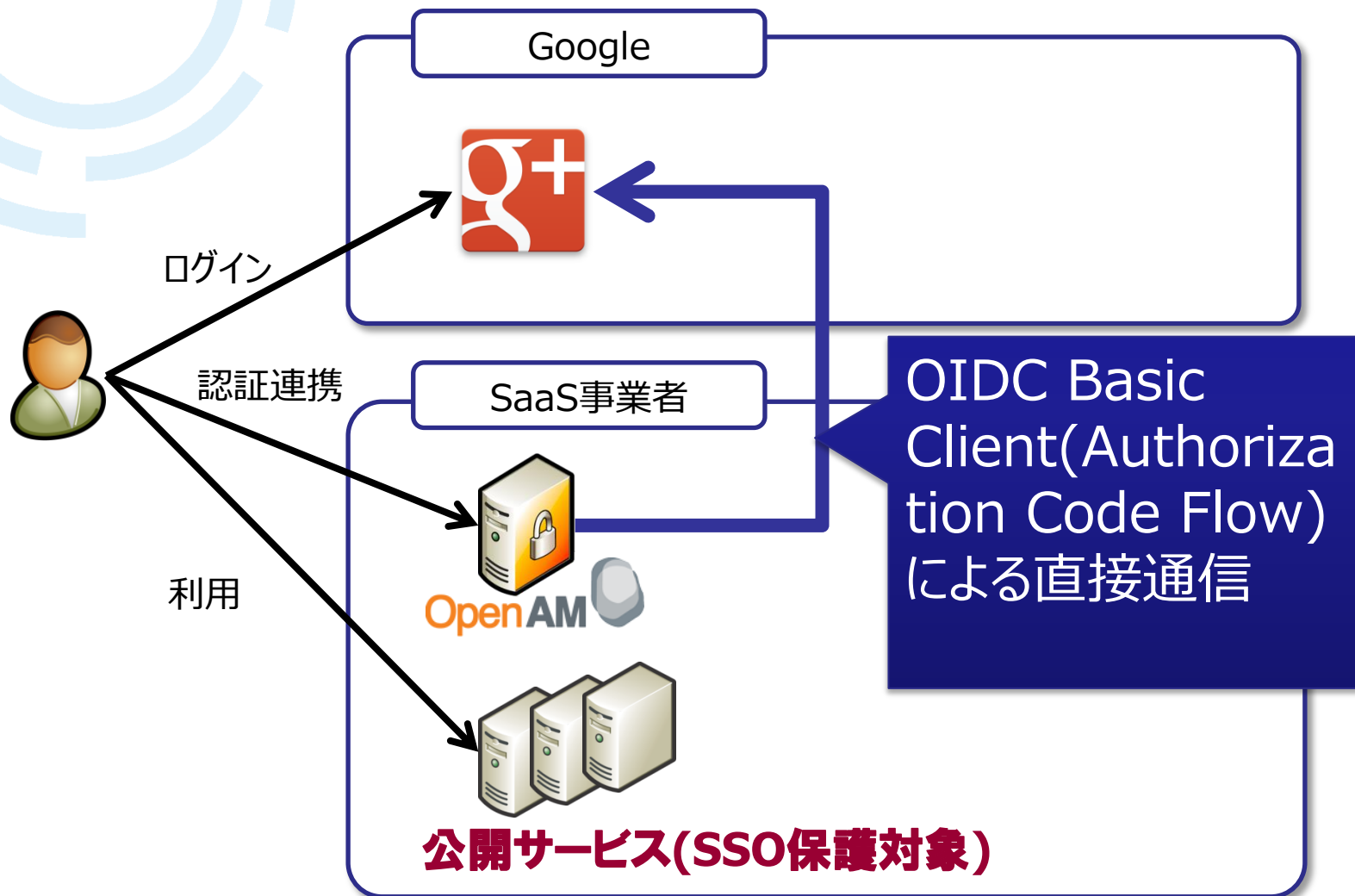
- AD・ADFSがない環境でもOpenAMとo365の認証連携が可能に
 - ▶ ただし機能制限は現状あるので注意(今後解消される見込みはあり)
- o365との認証連携設定には独自ドメインの取得が必要
- 実運用を考慮すると、o365(Azure AD)/OpenAMユーザの自動プロビジョニングが必要
 - ▶ MSのo365用のID同期のツールもあるが制限がある(ADが必要、FIMが必要など)
 - ▶ Azure AD Graph API(REST API)が使用できるため、自前でID連携のコードを書くことも可能(OpenAMもREST APIがあります)
 - ▶ 運用負荷や内部統制、その他の認証連携先へのプロビジョニングも考慮すると、OpenIDM等の専用のID管理ツールの導入も合わせて検討すべき

Googleとの認証連携 (OpenID Connect)

- 自社サービスをSaaSとして公開する際に、Googleなどの外部IDと認証連携しシングルサインオンする企業も増えてきている
- OpenAMはバージョン10からOAuth2連携に対応
- バージョン12ではOpenID Connect(OIDC)による認証連携にも対応
- 加えて、OAuth2/OIDCの簡単設定機能が追加

Googleを例にOIDCによる
連携設定をデモを交えて紹介

●OIDC Basic Clientで認証連携



設定の流れ

● Google側の設定

- ▶ Google+ APIの有効化
- ▶ 認証情報の作成

● OpenAM側の設定

- ▶ Googleとの接続情報をウィザードで設定

● Google Developers Console から **Google+ API** を有効化する

<div>プロジェクト</div> <div>openamdemo</div> <div>概要</div> <div>権限</div> <div>課金と設定</div> <div>APIと認証</div> <div>API</div> <div>認証情報</div> <div>同意画面</div> <div>プッシュ</div> <div>監視</div> <div>ソースコード</div> <div>計算処理</div> <div>ネットワーキング</div> <div>ストレージ</div> <div>ビッグデータ</div>	Google Maps JavaScript API V3	1,000,000リクエスト数/日	無効
	Google Maps SDK for iOS	なし	無効
	Google Maps Tracks API	なし	無効
	Google Mirror API	1,000リクエスト数/日	無効
	Google Picker API	10,000リクエスト数/日	無効
	Google Play Android Developer API	200,000リクエスト数/日	無効
	Google Play Game Management	1,000,000リクエスト数/日	無効
	Google Play Game Services	50,000,000リクエスト数/日	無効
	Google Spectrum Database API	1,000リクエスト数/日	無効
	Google Webmaster Tools API	1,000,000リクエスト数/日	無効
	Google+ API	10,000リクエスト数/日	無効
	Google+ Domains API	10,000リクエスト数/日	無効

● プロジェクト > APIと認証 > 認証情報 > OAuthから作成する

▶ APIと認証 > 同意画面 にてメールアドレスの選択を忘れないように

< プロジェクト

openamdemo

概要

権限

課金と設定

API と認証

API

認証情報

同意画面

ブッシュ

監視

ソースコード

計算処理

ネットワーク

OAuth

OAuth 2.0 を使用すると、ユーザー名やパスワードなどの情報は非公開のまま、ユーザーの固有のデータ(連絡先リストなど)を共有できます。

詳細

新しいクライアント ID を作成

ウェブアプリケーションのクライアント ID

クライアント ID	923495621128-irlemhrp3jrqq9eevh2kgdh8rpih3mh5.apps.googleusercontent.com
メールアドレス	923495621128-irlemhrp3jrqq9eevh2kgdh8rpih3mh5@developer.gserviceaccount.com
クライアント シークレット	
リダイレクト URI	https://sso.openamdemo.mydns.jp:443/openam/oauth2c/OAuthProxy.jsp
JAVASSRIPT 生成元	https://sso.openamdemo.mydns.jp

設定を編集 シークレットをリセット JSON をダウンロード 削除

● Googleとの認証連携を行うウィザードを起動

The screenshot shows the OpenAM administration console interface. At the top, there's a header with 'バージョン' (Version) and 'ログアウト' (Logout) buttons. Below that, the user 'amAdmin' and server '75899f4227ce' are displayed. The 'FORGEROCK' logo is prominent. A navigation bar contains '共通タスク' (Common Tasks), 'アクセス制御' (Access Control), '連携' (Integration), '設定' (Settings), and 'セッション' (Sessions). The '設定' (Settings) tab is active, showing various configuration options. On the left, under 'SAMLv2 プロバイダを作成' (Create SAMLv2 Provider), there are buttons for creating host and remote providers. Below that, 'OAuth2 の設定' (Configure OAuth2) is highlighted. On the right, 'Salesforce CRM の設定' (Configure Salesforce CRM) is shown. Further down, 'Configure Social Authentication' is displayed, with a list of options: 'Configure Facebook Authentication', 'Configure Google Authentication' (highlighted with an orange box), 'Configure Microsoft Authentication', and 'Configure Other Authentication'. The 'Configure Google Authentication' option is the target of the tutorial.

バージョン ログアウト

ユーザー: amAdmin サーバー: 75899f4227ce

FORGEROCK

共通タスク アクセス制御 連携 設定 セッション

SAMLv2 プロバイダを作成
これらのワークフローを使用して、SAMLv2 連携のホストまたはリモートのアイデンティティとサービスプロバイダを作成します。

- ホストアイデンティティプロバイダの作成
- ホストサービスプロバイダの作成
- リモートアイデンティティプロバイダを登録
- リモートサービスプロバイダを登録

OAuth2 の設定
このタスクはレルムごとに OAuth2 を設定します。レルム単位に認可サーバとして動作することができます。

OAuth2 の設定

Fedlet を作成

Salesforce CRM の設定
OpenAM と Salesforce CRM を統合して、シングルサインオン環境を作成します。最初に、SAMLv2 ホストアイデンティティプロバイダとトラストサークルを設定する必要があります。

Salesforce CRM の設定

Configure Social Authentication
Add social authentication options per realm. This task configures authentication through third parties such as Facebook, Google and Microsoft.

- Configure Facebook Authentication
- Configure Google Authentication**
- Configure Microsoft Authentication
- Configure Other Authentication

● Googleとの接続情報を設定

- ▶ Client ID
- ▶ Client Secret
- ▶ Redirect URL

Configure Google Authentication

Configure Social Authentication using Google as the identity provider. Use the [Google Developers Console](#) to register your application with "Credentials" in the "APIs & auth" section and then click the "Create new Client ID" button under "OAuth" to be guided through creating it. Once created, copy the CLIENT ID and CLIENT SECRET values into the respective fields below to complete the configuration.

Realm

* Realm:

Client Details

* Client ID:

For more information on the OAuth client_id parameter refer to the [OAuth IETF draft](#), chapter 2.1

* Client Secret:

For more information on the OAuth client_secret parameter refer to the [OAuth IETF draft](#), chapter 2.1

* Confirm Client Secret:

* Redirect URL:

This URL should only be changed from the default, if an external server is performing the GET to POST proxying.
[/openam/oauth2c/OAuthProxy.jsp](#)

- OIDCによる認証連携設定
- Googleアカウントでログイン & JITプロビジョニング

- OpenAM12からOIDCによる認証連携も可能に
- ウィザード機能で初期設定も簡単に！

OpenAMの最新認証連携として以下を紹介

- Office 365との認証連携
- Google との認証連携

社内の認証基盤、自社サービスの認証
基盤 の両方に対応可能

- OpenStandiaは、「攻めのIT」を支援します。
- オープンソースのことなら、なんでもご相談ください！

オープンソースまるごと



お問い合わせは、NRIオープンソースソリューション推進室へ



osscc@nri.co.jp



<http://openstandia.jp/>

本資料に掲載されている会社名、製品名、サービス名は各社の登録 商標、又は商標です。