# Azure Active Directory を利用した認証基盤の構築

MSC0569G-L1-04

**演習ガイド**

# 商標

- アマゾン ウェブ サービス、AWS および Amazon Web Services ロゴは、米国その他の諸国における、Amazon.com, Inc.またはその関連会社の商標です。
- Apple、Apple のロゴ、iPad、iPhone, iTunes は、米国および他の国々で登録された Apple Inc.の商標です。
- Cisco、Cisco Systems、Cisco Systems ロゴ、ネットワーキングアカデミー、Cisco Systems, Inc. および関連会社の米国ならびに他の国における商標もしくは登録商標です。
- Intel、インテル は、米国およびその他の国における Intel Corporation の商標です。
- ITIL は AXELOS Limited の登録商標です。
- Microsoft、Windows は、米国 Microsoft Corporation の、米国およびその他の国における登録商標または商標です。
- Oracle と Java は、Oracle Corporation 及びその子会社、関連会社の米国及びその他の国における登録商標です。
- PMI、PMP、PMBOK は、プロジェクトマネジメント協会（Project Management Institute, Inc.）の登録商標です。
- VMware、VMware ロゴは VMware,Inc.の米国および各国での商標または登録商標です。
- BOOT CAMP、NEW TRAIN、はトレノケート株式会社の登録商標です。

その他の会社名、製品名およびサービス名は、それぞれ各社の商標または登録商標です。

# 目　次

L1

# 演習 1　Azure AD の概要と初期構成

# コンピューター名および役割の確認

この演習で使用する仮想マシンの名前 (コンピューター名) と役割は次のとおりです。

| コンピューター名 | 役割 |
|---|---|
| DC | ・Active Directory ドメインサービス<br>・内部 DNS サーバー<br>・Azure AD Connect |
| CL | ・Windows 10 |

# 演習で使用する各種パラメータ

この演習で使用する各種パラメータは次のとおりです。空欄になっている項目は講師からの指示によって与えられますので、ご確認ください。

| | |
|---|---|
| 受講者番号 (XX) | |
| Microsoft Azure<br>サインイン<br>ユーザー名とパスワード | |
| Azure AD ドメイン名 | |
| Azure AD<br>グローバル管理者 | |
| グローバル管理者の<br>パスワード | |
| カスタムドメイン名 | |

# 演習の目標

Azure Active Directory ドメインの作成とカスタムドメインの設定方法を確認します。

# 演習の概要

- Azure AD ドメインの作成
- カスタムドメインの構成

### 予想所要時間

30 分

# 演習1.1. Office 365 の初期構成

Office 365 の試用版を取得し、Azure Active Directory ドメインを作成します。また、Azure AD で使用するドメイン名に企業で使用するカスタムドメインを追加します。

## 演習1.1.1. Office 365 試用版アカウントのサインアップ

1. ホストコンピューターで操作します。
2. 講師の指示に従い、Azure 管理ポータル (https://portal.azure.com) にアクセスし、ユーザー名とパスワードを入力し、サインインします。
3. Azure 管理ポータル画面で、左ペインの [Virtual Machine] をクリックし、自身が利用する仮想マシン DC をクリックして、[接続] をクリックします。
4. 仮想マシン DC に次の認証情報を使ってサインインを行います。

   ユーザー名 : **vmadmin**

   パスワード : **MSC0569adfs!**
5. ブラウザーを起動し、https://www.google.co.jp にアクセスします。
6. Google 検索で「Office365 E3」のキーワードで検索します。
7. 検索結果から Office 365 E3 のマイクロソフトの Web サイトにアクセスします。
8. 表示されるページで、Enterprise E3 の無料試用版をクリックします。
9. 表示されるページで、必要事項を入力し [次へ] をクリックします。
   (※ただしメールアドレス欄には捨てアドレスを指定するようにしてください)
10. 講師から、あらかじめ指示されたドメイン名/ユーザー名/パスワードを指定して[次へ] をクリックします。
11. クレジットカード番号を入力する画面が表示されたら、ブラウザー画面で新しいタブを開きます。
12. 新しいタブで、URL として「https://admin.microsoft.com」と入力します。
13. [Microsoft 365 管理センター] 画面で、左ペインの [課金情報] - [請求対象アカウント] をクリックします。
14. [請求対象アカウント] 画面で、[課金アカウント] 欄の下段に表示されているドメイン名をクリックします。
15. [課金アカウントの詳細] 画面で、[編集] をクリックします。
16. [販売先住所] 画面で、住所等の必要事項を入力し、[保存] をクリックします。

17. [販売先住所] 画面で、画面右上の×をクリックします。
18. [Microsoft 365 管理センター] 画面で、左ペインの [課金情報] - [サービスを購入する] をクリックします。
19. [サービスを購入する] 画面で、[Office365 E3] 欄の [詳細] をクリックします。
20. (Office365 E3 が表示されない場合、検索窓に E3 と入力してください)
21. [Office365 E3] 画面で、[無料試用の開始] をクリックします。
22. [ロボットではないことを証明してください] 画面で、電話番号を入力し、[お電話ください] をクリックします。
23. 電話の音声案内に従ってコード番号を入手し、コード番号を入力して [無料試用版の開始] をクリックします。
24. [購入手続きへ進む] 画面で、[無料トライアル] をクリックします。
25. [注文の受領書] 画面で、[続行] をクリックします。
26. [Microsoft 365 管理センター] 画面で、左ペインの [ユーザー] - [アクティブなユーザー] をクリックします。
27. [アクティブなユーザー] 画面で、admin ユーザーをクリックし、Office365 E3 ライセンスが割り当てられていることを確認します。

## 演習1.1.2. カスタムドメインの登録

1. 仮想マシン DC で操作します。
2. ブラウザー画面で新しいタブを開き、アドレスに「https://entra.microsoft.com/」と入力して、Enter キーを押します。
3. サインイン画面が表示される場合、Office 365 試用版取得時に作成したユーザー名とパスワード (このユーザー名とパスワードが Azure AD **グローバル管理者**にあたります) を入力してサインインします。
4. Microsoft Entra 管理センター画面で、左ペインの [設定] - [ドメイン名] をクリックします。
5. [カスタム ドメイン名] 画面で、[カスタム ドメインの追加] をクリックします。
6. [カスタム ドメイン名] 画面で、講師から指示されたカスタム ドメイン名を入力し、[ドメインの追加] をクリックします。
7. 続いて表示される画面で、宛先または参照先の値を控えておきます。

   宛先または参照先のアドレス: MS=＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
8. 表示された値を講師に伝えます。
9. 講師がレコードを登録したら、コマンドプロンプトを起動します。
10. コマンドプロンプト画面で、nslookup と入力し、Enter キーを押します。
11. コマンドプロンプト画面で、set type=txt と入力し、Enter キーを押します。
12. コマンドプロンプト画面で、カスタムドメイン名を入力し、Enter キーを押します。
    実行後、MS= で始まる文字列が表示されていることを確認します。
    (表示されない場合は時間をおいてから再度実行してください)
13. コマンドプロンプト画面を閉じます。
14. Microsoft Entra 管理センター画面で、[確認] をクリックします。
15. Microsoft Entra 管理センター画面で、[確認に成功しました] と表示されたことを確認し、[プライマリにする] をクリックして、[はい] をクリックします。([プライマリにする] ボタンが押せない場合、F5 キーを押して再度操作してください。)

## 演習1.1.3. セキュリティ既定値の管理の無効化

1. 仮想マシン DC で操作します。
2. Microsoft Entra 管理センター画面で、左ペインの [概要] をクリックし、[プロパティ] をクリックします。
3. プロパティ画面で、[セキュリティの既定値の管理] をクリックします。
4. [セキュリティの既定値群] 画面で、[無効] を選択し、適当な理由を選択して、[保存] - [無効化] の順にクリックします。

L2

# 演習 2　ユーザーとグループの構成

# 演習の目標

この演習では Azure AD にユーザーとグループを作成し、Azure AD におけるユーザー管理の方法を確認します。

# 演習の概要

- ユーザーの作成
- グループの作成
- Azure AD Connect を利用したユーザーとグループの作成
- EMS ライセンスの割り当て

### 予想所要時間

50 分

# 演習2.1. ユーザーとグループの作成

Microsoft Entra 管理センター画面で Azure AD ユーザーを作成します。

## 演習2.1.1. Microsoft Entra 管理センターからユーザーの作成

1. 仮想マシン DC で操作します。
2. ブラウザー画面で新しいタブを開き、アドレスに「https://entra.microsoft.com/」と入力して、Enter キーを押します。
3. サインイン画面が表示される場合、グローバル管理者となるユーザーのユーザー名とパスワードを入力し、サインインします。
4. Microsoft Entra 管理センター画面で、左ペインの [ユーザー] - [すべてのユーザー] をクリックします。
5. [ユーザー] 画面で、[新しいユーザー] - [新しいユーザーの作成] をクリックします。
6. [新しいユーザーの作成] 画面で、以下の情報を入力します。
   ・ユーザー プリンシパル名 : muto@<カスタムドメイン名>
   ・表示名 : muto@<カスタムドメイン名>
   パスワード : テキストボックス右側のボタンをクリックして表示
7. パスワードは後ほど使用するので、値を控えておきます。

   一時パスワード: _____
8. [新しいユーザーの作成] 画面で[レビューと作成] をクリックします。
9. [新しいユーザーの作成] 画面で[作成] をクリックします。

# 演習2.2. CSV ファイルからユーザーの作成

CSV ファイルにあらかじめ登録されたユーザー一覧を利用して Azure AD ユーザーを作成します。

## 演習2.2.1. CSV ファイルからユーザーを作成

1. 仮想マシン DC で操作します。
2. ブラウザーで http://aka.adfs.jp/aad にアクセスし、CSV ファイル (users.zip) をダウンロードします。
3. ダウンロードした CSV ファイルを右クリックして [プログラムから開く] をポイントし、[メモ帳] をクリックします。
4. 文字列置換で、各ユーザーのユーザー名のドメイン部分を @contoso.com から @<カスタムドメイン名> に変更します。
5. メモ帳画面で、[ファイル] - [名前を付けて保存] をクリックします。
6. [名前を付けて保存] 画面で、[文字コード] 欄から [UTF-8] を選択し、任意のフォルダーに users.csv という名前でファイルを保存し、メモ帳を終了します。
7. Microsoft Entra 管理センター画面で、左ペインの [ユーザー] - [すべてのユーザー] をクリックします。
8. [ユーザー] 画面で、[一括操作] - [一括作成] をクリックします。
9. [ユーザーの一括作成] 画面で、users.csv ファイルをアップロードし、[送信] をクリックします。

# 演習2.3. グループの作成

Azure AD にグループを作成し、グループのメンバーを追加します。

## 演習2.3.1. グループの作成

1. 仮想マシン DC で操作します。
2. Microsoft Entra 管理センター画面で、左ペインの [グループ] - [すべてのグループ] をクリックします。
3. [すべてのグループ] 画面で、[新しいグループ] をクリックします。
4. [グループ] 画面で、以下を入力し、[作成] をクリックします。
   ・グループの種類 ： セキュリティ
   ・名前 : Sales
   ・メンバーシップの種類 ： 割り当て済み
   ・メンバー : admin ユーザーと muto ユーザーを追加
   (名前を入力して検索し、追加)
5. [すべてのグループ] 画面で、グループが作成されていることを確認します。

# 演習2.4. Azure AD Connect によるユーザー/グループの作成

この演習では、Azure AD Connect を利用して、オンプレミスの Active Directory に保存されているユーザーとグループを同期することで、Azure AD にユーザーとグループが作成される様子を確認します。

## 演習2.4.1. オンプレミス環境の構成

1. 仮想マシン DC で操作します。
2. ブラウザーで http://aka.adfs.jp/aad にアクセスし、adinstall0.zip ファイルをデスクトップ画面にコピーします。
3. デスクトップ画面に保存した adinstall0.zip ファイルを展開し、adinstall0.ps1 ファイルを取り出します。
4. adinstall0.ps1 ファイルを右クリックし、[編集] をクリックします。
5. [PowerShell ISE] 画面で、2 行目に記載されているドメイン名のうち、XX 部分を受講者番号に書き換え、上書き保存します。
6. [PowerShell ISE] 画面で、F5 キーを押し、スクリプトを実行します。これにより Active Directory ドメイン サービスのインストールが始まります。しばらくすると、コンピューターが再起動します。
7. 仮想マシン DC に次の認証情報を使ってサインインを行います。

   ユーザー名 : **ContosoXX¥vmadmin**

   パスワード : **MSC0569adfs!**

   ※サインインに失敗する場合、ユーザー名を vmadmin としてください。
   ※Bastion 接続でサインインする場合、ユーザー名を vmadmin としてください。
8. [サーバー マネージャー] を起動します。
9. サーバーマネージャーの [ツール] - [Active Directory ドメインと信頼関係] をクリックします。
10. 左ペインの [Active Directory ドメインと信頼関係] を右クリックし、[プロパティ] をクリックします。

11. UPN サフィックスで、[代わりの UPN サフィックス] 欄に講師から与えられたカスタムドメイン名を入力し、[追加] をクリックして、[OK] をクリックします。
12. [サーバー マネージャー] 画面で、[ツール] - [Active Directory ユーザーとコンピューター] をクリックします。
13. [Active Directory ユーザーとコンピューター] 画面で、[contosoXX.com] ドメイン名を右クリックし、[新規作成] - [ユーザー] をクリックします。
14. [新しいオブジェクト ユーザー] 画面で、[フルネーム] 欄と [ユーザー ログオン名]欄に「yamada」と入力し、@以降の欄でカスタムドメイン名を選択して、[次へ] をクリックします。
15. [新しいオブジェクト ユーザー] 画面で、[パスワード] と [パスワードの確認入力] 欄にそれぞれ「Pa$$w0rd」と入力し、[パスワードを無期限にする] にチェックをつけ、[次へ] をクリックします。
16. [新しいオブジェクト ユーザー] 画面で、[完了] をクリックします。
17. [Active Directory ユーザーとコンピューター] 画面で、 [contosoXX.com] ドメイン名を右クリックし、[新規作成] - [グループ] をクリックします。
18. [新しいオブジェクト グループ] 画面で、[グループ名] 欄に 「Marketing」と入力し、[グループのスコープ] で、[グローバル] を選択し、[グループの種類] で、[セキュリティ] を選択し、[OK] をクリックします。
19. [Active Directory ユーザーとコンピューター] 画面で、 [contosoXX.com] ドメイン名で、作成したグループ [Marketing] を選択し、右クリックで [プロパティ] をクリックします。
20. [Maketing のプロパティ] 画面で、 [メンバー] タブをクリックし、[所属するメンバー] 欄で、 [追加] ボタンをクリックします。
21. [選択するオブジェクト名を入力してください] 欄で、「yamada」 と入力し、[名前の確認] をクリックします。
22. メンバー] タブの [所属するメンバー] 欄に [yamada] ユーザーが表示されていることを確認し、[OK] ボタンをクリックします。

## 演習2.4.2. Azure AD Connect のインストール

1. 仮想マシン DC で操作します。
2. ブラウザーで http://aka.adfs.jp/aadc にアクセスし、Azure AD Connect ツールをダウンロードします。
3. ダウンロードした **AzureADConnect.msi** ファイルをダブルクリックします。
4. [Azure AD Connect へようこそ] 画面が表示される場合、[ライセンス条項およびプライバシーに関する声明に同意します。] にチェックをつけ、[続行] をクリックします。
5. [Microsoft Azure AD Connect] 画面で、[カスタマイズ] をクリックします。
6. [必須コンポーネントのインストール] ページで、[インストール] をクリックします。
7. [ユーザーサインイン] ページで、[パスワードハッシュの同期] を選択し、[次へ] をクリックします。
8. [Azure AD に接続] ページで、admin ユーザーのユーザー名とパスワードを入力し、[次へ] をクリックします。
9. [ディレクトリの接続] ページで、[ディレクトリの追加] をクリックし、[AD フォレスト アカウント] 画面から [新しい AD アカウントを作成] を選択し、[ユーザー名] 欄に **ContosoXX¥vmadmin**、 [パスワード] 欄に **MSC0569adfs!** と入力して、[OK] をクリックします。ドメインが追加されたら [次へ] をクリックします。
   ※追加に失敗する場合、ユーザー名を vmadmin@contosoXX.com のように設定し、追加してみてください。
10. [Azure AD サインイン構成] 画面で、[一部の UPN サフィックスが確認済みドメインへのすべての UPN サフィックスに一致しなくても続行する] にチェックをつけ、[次へ] をクリックします。
11. [ドメインと OU のフィルタリング] 画面で、[次へ] をクリックします。
12. [一意のユーザー識別] ページで、[次へ] をクリックします。
13. [ユーザーおよびデバイスのフィルタリング] ページで、[次へ] をクリックします。
14. [オプション機能] ページで、[次へ] をクリックします。
15. [構成の準備完了] ページで、[インストール] をクリックします。
16. [構成が完了しました] ページで、[終了] をクリックします。

## 演習2.4.3. 同期結果の確認

1. 仮想マシン DC で操作します。

2. Microsoft Entra 管理センター画面で、左ペインの [ユーザー] - [すべてのユーザー] をクリックします。
3. [ユーザー] 画面で、Active Directory に作成したユーザー (yamada ユーザー) が同期され、追加されていることを確認します。
4. Azure AD ドメイン画面で、左ペインの [グループ] - [すべてのグループ] をクリックします。Active Directory に作成したグループ (Marketing グループ) が同期され、追加されていることを確認します。
   ※結果が確認できるまでに時間を要する場合があります。

# 演習2.5. Azure AD Premium ライセンスの割り当て

この演習では、作成したグループに対して、Azure AD Premium が含まれる Enterprise Mobility＋Security (EMS) ライセンスの割り当てを行います。

## 演習2.5.1. EMS ライセンス取得

1. 仮想マシン DC で操作します。
2. Microsoft Entra 管理センター画面で、左ペインの [表示数を増やす] をクリックし、[課金] - [ライセンス] をクリックします。
3. [ライセンス] 画面で、[すべての製品] をクリックします。
4. [製品] 画面で、[試用/購入] をクリックします。
5. [アクティブ化] 画面で、[ENTERPRISE MOBILITY + SECURITY] 欄にある [無料試用版] をクリックします。
6. [Enterprise Mobility + Security 評価版のライセンス認証] 画面で、[アクティブ化] をクリックします。
7. Microsoft Entra 管理センター画面で、左メニューの [Azure Active Directory] をクリックします。
8. Microsoft Entra 管理センター画面で、左ペインの [ユーザー] - [すべてのユーザー] をクリックします。
9. [ユーザー] 画面で、muto ユーザーをクリックします。
10. muto ユーザー画面で、設定メニューの [プロパティの編集] をクリックし、[利用場所] 欄から Japan を選択し、[保存]をクリックします。
11. 同様にして、yamada ユーザーの利用場所も Japan に設定します。

## 演習2.5.2. EMS ライセンスの割り当て

1. 仮想マシン DC で操作します。
2. Microsoft Entra 管理センター画面で、左ペインの [ユーザー] - [すべてのユーザー] をクリックします。
3. [ユーザー] 画面で、admin ユーザーをクリックします。
4. ユーザー画面で、[ライセンス] をクリックします。
5. [ライセンス] 画面で、[割り当て] をクリックします。
6. [ライセンス割り当ての更新] 画面で、[Enterprise Mobility + Security E5] 欄にチェックを付け、[保存] をクリックします。
(表示されない場合は F5 キーを押してください)
7. Microsoft Entra 管理センター画面で、左メニューの [Azure Active Directory] をクリックします。
8. Microsoft Entra 管理センター画面で、左ペインの [グループ] - [すべてのグループ] をクリックします。
9. [グループ] 画面で、[新しいグループ] をクリックします。
10. [新しいグループ] 画面で、[グループ名] 欄に「License」と入力し、[メンバーシップの種類] 欄から [動的ユーザー]を選択し、[動的クエリの追加] をクリックします。
(動的更新が表示されない場合、F5 キーを押して Web ブラウザーを更新します)
11. [動的メンバーシップ ルール] 画面で、usageLocation Equals JP となるように式を入力し、[保存] をクリックします。
12. [新しいグループ] 画面で、[作成] をクリックします。
13. [グループ] 画面で、License をクリックします。
14. License グループ画面で、[ライセンス] をクリックします。
15. [ライセンス] 画面で、[割り当て] をクリックします。
16. [割り当て] 画面で、[Enterprise Mobility + Security E5] 欄にチェックを付け、[保存] をクリックします。
17. 以上の操作により、グループのメンバーとなるユーザーたちに EMS のライセンスが自動的に割り当てられます。

L3

# 演習 3　アプリケーションの登録

# 演習の目標

この演習では Azure AD にアプリケーションを登録する手順を確認します。登録するアプリケーションには Salesforce、Gmail、OAuth 2.0 対応 Web アプリ、オンプレミス Web サイトを使用します。

# 演習の概要

- Salesforce の登録
- Gmail の登録
- OAuth 2.0 対応アプリの実装
- Web サイトの登録

### 予想所要時間

80 分

# 演習3.1. Salesforce の登録

この手順では、Salesforce のテナントを新規作成し、作成したテナントに Azure AD から SAML プロトコルによる ID 連携によって、シングルサインオンアクセスができる様子を確認します。

## 演習3.1.1. Salesforce アカウントの取得

1. 仮想マシン DC で操作します。
2. ブラウザーを起動し、アドレスに「https://myapplications.microsoft.com/」を入力し、Enter キーを押します。
3. サインイン画面で、グローバル管理者 (admin ユーザー) のユーザー名とパスワードを入力し、サインインします。
4. ポータル画面で、outlook をクリックし、Outlook on the Web のサイトにアクセスします。
5. Outlook on the Web のサイトで、タイムゾーンを選択する画面が表示される場合、適切なゾーンを選択し、メールボックスにアクセスできることを確認します。(画面は閉じないでください)
6. ブラウザー画面で、新しいタブを開き、アドレスに「http://developer.salesforce.com/signup」と入力して、Enter キーをクリックします。
7. 登録画面で、自身の情報を入力し、登録します。なお、メールアドレス欄とユーザー名欄には admin ユーザーの名前である「admin@****.onmicrosoft.com」を入力します。
8. Outlook on the Web 画面で、Salesforce から送信されたメールを開き、メール本文内のリンクをクリックします。([Outlook On the Web] 画面は閉じないでください)
9. [パスワードを変更する] 画面で、パスワードとして Pa$$w0rd を設定し、[セキュリティの質問] を設定して、[パスワードを変更] をクリックします。
10. Salesforce の設定画面で、左ペインの [会社の設定] - [私のドメイン] をクリックします。
11. [私のドメイン] 画面で、[現在の [私のドメイン] の URL] 欄に表示されるドメイン名を控えておきます。

    私のドメイン名: _____

## 演習3.1.2. SaaS アプリとして Salesforce を登録

1. 仮想マシン DC で操作します。
2. ブラウザー画面で新しいタブを開き、アドレスに「https://entra.microsoft.com/」と入力して、Enter キーを押します。
3. サインイン画面が表示される場合、グローバル管理者となるユーザーのユーザー名とパスワードを入力し、サインインします。
4. Microsoft Entra 管理センター画面で、左ペインの [アプリケーション] - [エンタープライズアプリケーション] をクリックします。
5. [エンタープライズアプリケーション] 画面で、[新しいアプリケーション] をクリックします。
6. [アプリケーションの追加] 画面で、検索窓に「Salesforce」と入力し、検索結果から [Salesforce] をクリックします。
7. [Salesforce] 画面で、[作成] をクリックします。
8. Microsoft Entra 管理センター画面で、左メニューの [Azure Active Directory] をクリックします。
9. Azure AD ドメイン画面で、[エンタープライズ アプリケーション] をクリックします。
10. [エンタープライズ アプリケーション] 画面で、[すべてのアプリケーション] をクリックします。
11. [エンタープライズ アプリケーション - すべてのアプリケーション] 画面で、[Salesforce] をクリックします。
12. [Salesforce] 画面で、左ペインの [シングルサインオン] をクリックし、[SAML] を選択します。

13. [SAML によるシングル サインオンのセットアップ] 画面で、[基本的な SAML 構成] 欄の編集ボタンをクリックし、[サインオン URL] 欄、[応答 URL ] 欄、[識別子] 欄に前の手順で作成した私のドメイン名を https:// から始まるように入力し、[保存] をクリックします。
※既存の設定が入っている場合、その設定を削除して入力してください。

14. [SAML によるシングル サインオンのセットアップ] 画面で、[SAML 証明書] 欄の [証明書 (未加工)] 欄のダウンロード リンクをクリックして、ファイルを保存します。
(Microsoft Edge の場合、証明書のダウンロード時にエラーが出ますが、エラーメッセージから […] をクリックして [保存] をクリックすると、保存が可能です)

15. [SAML によるシングル サインオンのセットアップ] 画面で、[⑤Salesforce のセットアップ] 欄から [構成 URL] をクリックし、Azure AD 識別子をコピーします。

16. Salesforce 画面に切り替え、左ペインの [ID] - [シングルサインオン設定] をクリックします。

17. [シングルサインオン設定] 画面で、[SAML シングルサインオン設定] の [新規] をクリックします。

18. [SAML シングルサインオン設定] 画面で、以下のように入力します。
(指定のない項目は、すべて既定値で進めます)
・名前:AzureAD
・発行者:手順 15 でコピーした URL を張り付け
・ID プロバイダーの証明書:手順 12 でダウンロードした証明書をアップロード
・エンティティ ID:私のドメイン名 (https:// から入力)
・サービスプロバイダの起動要求バインド:HTTP リダイレクト
(まだ保存しないでください)

19. Microsoft Entra 管理センター画面に切り替え、[SAML によるシングル サインオンのセットアップ] 画面で、[⑤Salesforce のセットアップ] 欄から [構成 URL] をクリックし、ログイン URL をコピーします。

20. ブラウザー画面を切替え、Salesforce 1 の設定画面で、[ID プロバイダーのログイン URL] 欄に手順 17 でコピーした URL を貼り付け、[保存] をクリックします。

21. Salesforce の設定画面で、左ペインの [ID] - [シングルサインオン設定] をクリックします。

22. [シングルサインオン設定] 画面で、画面上部の [編集] をクリックします。

23. [シングルサインオン設定] 画面で、[SAML を有効化] にチェックをつけ、[保存] をクリックします。

24. 左ペインの [会社の設定] - [私のドメイン] をクリックします。
25. [私のドメイン] 画面で、[認証設定] の [編集] をクリックします。
26. [認証設定]画面で、[認証サービス] 欄に [AzureAD] 欄のみにチェックをつけ、[保存] ボタンをクリックします。

## 演習3.1.3. Salesforce へのユーザーのプロビジョニング

1. 仮想マシン DC で操作します。
2. Salesforce の設定画面で、画面右上のユーザーアイコンをクリックし、[設定] をクリックします。
3. [個人情報] 画面で、左ペインの [私のセキュリティ トークンのリセット] をクリックします。
4. [私のセキュリティ トークンのリセット] 画面で、[セキュリティ トークンのリセット] をクリックします。
5. [Outlook On the Web] 画面で、Salesforce から送信されたメールを開き、メールで送られたセキュリティ トークンを控えておきます。

   セキュリティ トークン: _____
6. Microsoft Entra 管理センターに画面を切り替え、[Salesforce - シングルサインオン] 画面で、左ペインの [プロビジョニング] をクリックします。
7. [プロビジョニング] 画面で、[作業の開始] をクリックします。
8. [プロビジョニング] 画面で、[プロビジョニング モード] 欄から [自動] を選択し、 [管理者資格情報] 欄に次のように入力し、[テスト接続] をクリックします。
   ・管理ユーザー名 : admin@****.onmicrosoft.com
   ・パスワード : Pa$$w0rd
   ・シークレット トークン : 手順 5 で入手した文字列
9. [プロビジョニング] 画面で、[保存] をクリックします。
10. [プロビジョニング] 画面で、画面上部のパンくずリストから [Salesforce] リンクをクリックします。
11. [Salesforce | プロビジョニング] 画面で、[プロビジョニングの編集] をクリックします。
12. [プロビジョニング] 画面で、[プロビジョニング状態] 欄からオンをクリックします。
13. [プロビジョニング] 画面で、[保存] をクリックします。

## 演習3.1.4. Salesforce へのアクセス許可割り当て

1. 仮想マシン DC で操作します。
2. Microsoft Entra 管理センターの [Salesforce] 画面で、[ユーザーとグループ] タブをクリックし、[ユーザーの追加] をクリックします。
3. [割り当ての追加] 画面で、admin ユーザーを選択し、[選択] をクリックします。
4. [割り当ての追加] 画面で、[ロールの選択] をクリックし、[Chatter Free User] を選択して、[選択] をクリックします。
5. [割り当ての追加] 画面で、[割り当て] をクリックします。

## 演習3.1.5. Salesforce へのアクセス

1. ホストコンピューターで操作します。
2. 講師の指示に従い、Azure 管理ポータル (https://portal.azure.com) にアクセスし、ユーザー名とパスワードを入力し、サインインします。
3. Azure 管理ポータル画面で、左ペインの [Virtual Machine] をクリックし、自身が利用する仮想マシン CL をクリックして、[接続] をクリックします。
4. 仮想マシン CL に次の認証情報を使ってサインインを行います。

   ユーザー名 : **vmadmin**

   パスワード : **MSC0569adfs!**

5. ブラウザー画面を起動し、アドレスに「https://myapplications.microsoft.com/」を入力し、Enter キーを押します。
6. サインイン画面で、グローバル管理者 (admin ユーザー) のユーザー名とパスワードを入力し、サインインします。
7. ポータル画面で、Salesforce のアイコンをクリックします。すると、Salesforce のサイトにシングルサインオンアクセスできることを確認します。

# 演習3.2. Zoom の登録

この手順では、オンラインストレージクラウドである Zoom の評価版を取得し、作成したアカウントに Azure AD からパスワード連携によるシングルサインオンアクセスができる様子を確認します。

## 演習3.2.1. Zoom の評価版取得

1. 仮想マシン DC で操作します。
2. ブラウザーを起動し、アドレスに「https://myapplications.microsoft.com/」を入力し、Enter キーを押します。
3. ポータル画面で、outlook をクリックし、Outlook on the Web のサイトにアクセスします。
4. Outlook on the Web 画面を表示させておきます。
5. ブラウザー画面で、新しいタブを開き、アドレスに「http://www.google.co.jp/」を入力して、Enter キーを押します。
6. 検索結果から Zoom の Web サイトにアクセスします。
7. 表示されるページで、[無料でサインアップ] をクリックします。
8. 生まれ年を入力する画面が表示される場合は画面の指示に従い、次へ進みます。
9. [始めましょう] 画面で、メールアドレスとして Azure AD グローバル管理者のユーザー名を入力し、[続ける] をクリックします。
10. Outlook on the Web 画面で、新しいメールが届くことを確認し、メールに記載されているコード番号を控えておきます。
11. [メールを開いてコードを確認してください] 画面で、控えておいたコード番号を入力し、[検証] をクリックします。
12. [アカウントを作成] 画面で、苗字、名前を入力し、パスワードとして Pa$$w0rd を入力して [続ける] をクリックします。
13. Zoom 画面にアクセスできることが確認できたら、画面右上のボタンをクリックし、サインインします。
14. Zoom 画面で、改めて画面右上の [サインイン] をクリックし、サインイン画面の URL を控えておきます。

## 演習3.2.2. SaaS アプリとして Zoom を登録

1. 仮想マシン DC で操作します。
2. Microsoft Entra 管理センター画面で、左ペインの [アプリケーション] - [エンタープライズアプリケーション] をクリックします。
3. [エンタープライズアプリケーション] 画面で、[新しいアプリケーション] をクリックします。
4. [Azure AD ギャラリーの参照] 画面で、[独自のアプリケーションの作成] をクリックします。
5. [独自のアプリケーションの作成] 画面で、[入力名] 欄に「Zoom」と入力し、[作成] をクリックします。
6. [Zoom] 画面で、左ペインの [シングルサインオン] をクリックし、[パスワード ベース] を選択します。
7. [Zoom] 画面で、[サインオン URL] 欄に控えておいた URL を入力し、[保存] をクリックします。
8. [Zoom] 画面で、左ペインの [ユーザーとグループ] をクリックし、[ユーザーの追加] をクリックします。
9. [割り当ての追加] 画面で、グローバル管理者となるユーザーを選択し、[選択] をクリックします。
10. [割り当ての追加] 画面で、[資格情報の割り当て] 欄にある [不明] をクリックします。
11. [割り当ての追加] 画面で、[ユーザーの代わりに資格情報を割り当てますか?] 欄から [はい] を選択し、ユーザー名とパスワードとして Zoom の評価版を取得したときに入力したグローバル管理者のユーザー名とパスワード (Pa$$w0rd) を入力して、[OK] をクリックします。
12. [割り当ての追加] 画面で、[割り当て] をクリックします

## 演習3.2.3. Zoom へのアクセス確認

1. 仮想マシン CL で操作します。
2. 開いているブラウザーがある場合、一度すべて閉じます。
3. ブラウザーを起動し、アドレスに「http://myapplications.microsoft.com/」を入力し、Enter キーを押します。
4. サインイン画面で、グローバル管理者のユーザー名とパスワードを入力し、サインインします。
5. ポータル画面で、Zoom のアイコンをクリックします。
6. [アプリによるセキュリティで保護されたサインイン拡張機能] 画面で、[今すぐインストール] をクリックします。
7. [My Apps Secure Sign-in Extension] 画面で、[他のストアからの拡張機能を許可する] メニューが表示される場合はクリックし、[許可] をクリックします。(本手順は表示されない場合があります。その際は次へお進みください)
8. [My Apps Secure Sign-in Extension] 画面で、[Chrome に追加] をクリックし、[拡張機能の追加] をクリックします。
9. マイアプリ画面に戻り、Zoom のアイコンをクリックします。
(再度、[アプリによるセキュリティで保護されたサインイン拡張機能] 画面が表示される場合、F5 キーを押してください)
10. Zoom のサイトにシングルサインオンアクセスできることを確認します。
(ログインボタンは手動で押さなければならない場合があります。)

# 演習3.3. OAuth 2.0 対応アプリの実装

この演習では、Web サーバーに OAuth 2.0 対応の Web アプリケーションを実装し、Azure AD で認証したうえで Web アプリケーションにアクセスできるよう、連携設定を行います。

## 演習3.3.1. オンプレミス Web サーバーの設定

1. 仮想マシン DC で操作します。
2. ブラウザーで http://aka.adfs.jp/aad にアクセスし、spa.zip ファイルをダウンロードします。
3. ダウンロードしたファイルを展開し、C:¥SPA フォルダーにコピーします。(SPA フォルダーも同時に作成してください。)
4. [サーバー マネージャー] 画面で、[管理] - [役割と機能の追加] をクリックします。
5. [役割と機能の追加] 画面で、[次へ] を 3 回クリックします。
6. [サーバーの役割の選択] 画面で、[Web サーバー(IIS)] を展開し、
7. [Web サーバー(IIS)] - [Web サーバー] - [アプリケーション開発] - [CGI] にチェックを付けます。
8. [サーバーの役割の選択] 画面で、[Web サーバー(IIS)] - [Web サーバー] - [状態と診断] 項目から [要求の監視] と [ログツール] 欄にチェックを付け、[次へ] を 2 回クリックします。
9. [インストール オプションの確認] 画面で、[インストール] をクリックします。
10. [インストールの進行状況] 画面で、[閉じる] をクリックします。
11. [サーバー マネージャー] 画面で、[ツール] - [インターネット インフォメーション サービス (IIS) マネージャー] をクリックします。
12. [インターネット インフォメーション サービス (IIS) マネージャー] 画面で、左ペインの [サイト] を右クリックし、[Web サイトの追加] をクリックします。
13. [Web サイトの追加] 画面で、以下のように入力し、[OK] をクリックします。
    - サイト名 SPA
    - 物理パス C:¥SPA
    - ポート 44316

14. Microsoft Entra 管理センター画面で、左ペインの [アプリケーション] - [アプリの登録] をクリックします。
15. [アプリの登録] 画面で、[新規登録] をクリックします。
16. [アプリの登録] 画面で、以下のように入力し、[登録] をクリックします。
    - 名前 SPA
    - サポートされているアカウントの種類
      任意の組織のディレクトリ内のアカウントと、個人用の Microsoft アカウント
    - プラットフォームの選択
      シングルページアプリケーション
    - リダイレクト URI
      http://localhost:44316
17. [SPA] 画面で、アプリケーション ID を控えておきます。
18. [SPA] 画面で、[認証] をクリックし、[暗黙的な許可およびハイブリッド フロー] 項目から [アクセス トークン] 欄と [ID トークン] 欄にチェックを付け、[保存] をクリックします。
19. エクスプローラー画面で、C:¥SPA¥msalconfig.js ファイルをメモ帳で開きます。
20. メモ帳画面で、「client ID:"」以降の部分に前の手順で控えておいたアプリケーション ID を入力します (client ID:”480d180a-e5f0-419d-ac4c-c537e3db28ba” のように入力します)。
21. ブラウザーを開き、http://localhost:44316 と入力し、Web ページにアクセスします。
22. ブラウザー画面で、[Call Microsoft Graph API] をクリックします。
23. サインイン画面で、グローバル管理者 (admin ユーザー) のユーザー名を入力し、[次へ] をクリックします。
24. ブラウザー画面で、パスワードを入力し、サインインします。
25. ブラウザー画面で、[承諾] をクリックします。
26. Web ページにアクセスできること、Graph API で収集したサインインユーザーの情報が確認できること、Graph API 利用時に必要な ID トークンとアクセス トークンが見えることを確認します。

# 演習3.4. オンプレミス Web サイトの登録

この演習では、オンプレミスに設置された Web サーバーに Azure AD にサインインしたユーザーからアクセスできるように構成します。

## 演習3.4.1. アプリケーション プロキシの設定

1. 仮想マシン DC で操作します。
2. スタートボタンをクリックし、「cmd」と入力してコマンドプロンプトを起動します。
3. コマンドプロンプト画面で、「hostname」と入力し、コンピューター名を控えておきます。
4. Microsoft Entra 管理センター画面で、左ペインの [アプリケーション] - [エンタープライズアプリケーション] をクリックします。
5. [エンタープライズアプリケーション] 画面で、[アプリケーション プロキシ] をクリックします。
6. [アプリケーション プロキシ] 画面で、[コネクタ サービスのダウンロード] をクリックします。
7. [アプリケーション プロキシ コネクタのダウンロード] 画面で、[規約に同意してダウンロード] をクリックし、コネクタをダウンロード フォルダーにダウンロードします。
8. ダウンロードしたセットアッププログラムを仮想マシン DC にコピーします。
9. AADApplicationProxyConnectorInstaller をダブルクリックします。
10. インストールウィザード画面で、使用許諾に同意するチェックをつけ、[Install] をクリックします。
11. サインイン画面で、グローバル管理者 (admin ユーザー) のユーザー名とパスワードを入力し、サインインします。
12. インストールウィザード画面で、Setup Successful と表示されたことを確認し、画面を閉じます。
13. [エンタープライズアプリケーション - アプリケーション プロキシ] 画面で、コネクタとして DCXX が登録されていることを確認します (必要に応じて F5 キーを押してください)。
14. [エンタープライズアプリケーション - アプリケーション プロキシ] 画面で、左ペインの [アプリの構成] をクリックします。

15. [独自のオンプレミスのアプリケーションの追加] 画面で、以下の情報を入力し、[追加] をクリックします。
    ・名前:contosoXX
    ・内部 URL:http://<仮想マシン DC のコンピューター名>/
16. 画面左側の [アプリケーション] - [エンタープライズアプリケーション] をクリックします。
17. [すべてのアプリケーション] 画面で、[contosoXX] をクリックします。
18. [contosoXX] 画面で、[シングルサインオン] をクリックします。
19. [contosoXX - シングルサインオン] 画面で、[リンク] をクリックします。
20. [サインオン URL の構成] 画面で、「http://<仮想マシン DC のコンピューター名>/」と入力し、[保存] をクリックします。
21. [contosoXX] 画面で、[ユーザーとグループ] をクリックします。
22. [contosoXX - ユーザーとグループ] 画面で、[ユーザーの追加] をクリックします。
23. [割り当ての追加] 画面で、Marketing グループを選択し、[選択] をクリックします。
24. [割り当ての追加] 画面で、[割り当て] をクリックします。

## 演習3.4.2. アプリケーション プロキシの実行

1. 仮想マシン CL で操作します。
2. 開いているブラウザーがある場合、一度すべて閉じます。
3. ブラウザーを起動し、アドレスに「http://myapplications.microsoft.com/」 を入力し、Enter キーを押します。
4. サインイン画面で、ユーザー名として「yamada@カスタムドメイン名」、パスワードとして「Pa$$w0rd」をそれぞれ入力し、サインインします。
5. [アプリケーション] 画面で、[contosoXX] をクリックします。
6. 社内 Web サーバー(IIS) の Web ページが表示されることを確認します。
7. ブラウザーを終了します。

L4

# 演習 4　デバイス管理

# 演習の目標

この演習では Azure AD によるデバイス管理の実装を行います。

# 演習の概要

- ハイブリッド Azure AD 参加
- Azure AD 参加

### 予想所要時間

20 分

# 演習4.1. Azure AD 登録

この演習では、Azure AD 登録設定を行います。なお、本節の演習を行った場合、4.2 節または 4.3 節の演習を行うことはできません。

## 演習4.1.1. Azure AD 登録設定

1. 仮想マシン CL で操作します。
2. スタートメニューから [設定] をクリックします。
3. [設定] 画面で、[アカウント] をクリックし、[職場または学校にアクセスする] をクリックして、[接続] をクリックします。
4. [職場または学校アカウントのセットアップ] 画面で、グローバル管理者 (admin ユーザー) のユーザー名を入力し、[次へ] をクリックします。
5. サインイン画面で、グローバル管理者 (admin ユーザー) のパスワードを入力し、サインインします。
6. [これで完了です] 画面で、[完了] をクリックします。
7. ブラウザー画面をすべて閉じます。
8. Microsoft Edge を起動します。
9. Microsoft Edge 画面で、アドレスに「https://myapplications.microsoft.com/」を入力し Enter キーをクリックします。
10. 認証画面が表示されることなく、[アプリケーション] 画面が表示されることを確認します。

# 演習4.2. Azure AD 参加 (オプション)

この演習では、Azure AD 参加設定を行います。

## 演習4.2.1. Azure AD 参加設定

1. 仮想マシン CL で操作します。
2. スタートメニューから [設定] をクリックします。
3. [設定] 画面で、[アカウント] をクリックし、[職場または学校にアクセスする] をクリックして、[接続] をクリックします。
4. [職場または学校アカウントのセットアップ] 画面で、[このデバイスを Azure Active Directory に参加させる] をクリックします。
5. [サインインしましょう] 画面で、グローバル管理者 (admin ユーザー) のユーザー名を入力し、[次へ] をクリックします。
6. [パスワードの入力] 画面で、グローバル管理者 (admin ユーザー) のパスワードを入力し、サインインします。
7. [これがあなたの組織のネットワークであることを確認してください] 画面で、[参加する] をクリックします。
8. [これで完了です] 画面で、[完了] をクリックします。
9. スタートボタンを右クリックし、[ファイル名を指定して実行] を実行します。
10. [ファイル名を指定して実行] 画面で、「sysdm.cpl」と入力し、Enter キーを押します。
11. [システムのプロパティ] 画面で、[リモート] タブをクリックし、[ネットワーク レベル認証で～] の項目からチェックを外し、[ユーザーの選択] をクリックします。
12. [リモートデスクトップユーザー] 画面で、Authenticated Users グループを追加して、すべての画面で、[OK] をクリックします。
13. コンピューターをサインアウトします。
14. ホストコンピューターで操作します。
15. 仮想マシン CL の RDP ファイルをメモ帳で開きます。
16. メモ帳画面で、最後の行に以下の文字列を追記して、上書き保存します。
    enablecredsspsupport:i:0
    authentication level:i:2
17. RDP ファイルを実行し、リモートデスクトップ接続を開始します。

18. サインイン画面で、グローバル管理者 (admin ユーザー) のユーザー名とパスワードを入力し、サインインします。(サインインできない場合、ユーザー名を「AzureAD¥<admin ユーザーのユーザー名>」としてサインインしてください。)
19. [デスクトップ] 画面で、[すべてのアプリ] - [Windows アクセサリ] から Microsoft Edge を起動します。
20. Microsoft Edge 画面で、アドレスに「https://myapplications.microsoft.com/」を入力し Enter キーをクリックします。
21. 認証画面が表示されることなく、[アプリケーション] 画面が表示されることを確認します。

# 演習4.3. ハイブリッド Azure AD 参加 (オプション)

この演習では、ハイブリッド Azure AD 参加設定を行います。演習を開始するにあたり、**Azure 仮想マシンの DNS 設定を変更しておく必要があります**。詳しくは講師にご確認ください。

## 演習4.3.1. Azure AD Connect でのハイブリッド Azure AD 参加設定

1. 仮想マシン DC で操作します。
2. デスクトップに保存されている Azure AD Connect アイコンをダブルクリックします。
3. [Azure AD Connect へようこそ] 画面で、[構成] をクリックします。
4. [追加のタスク] 画面で、[デバイス オプションの構成] をクリックし、[次へ] をクリックします。
5. [概要] 画面で、[次へ] をクリックします。
6. [Azure AD に接続] 画面で、admin ユーザーのユーザー名とパスワードを入力して、[次へ] をクリックします。
7. [デバイス オプション] 画面で、[ハイブリッド Azure AD 参加の構成] を選択し、[次へ] をクリックします。
8. [デバイスのオペレーティング システム] 画面で、[Windows 10 以降のドメインに参加しているデバイス] 欄にチェックをつけ、[次へ] をクリックします。
9. [SCP の構成] 画面で、contosoXX.com ドメインにチェックをつけ、[認証サービス] 欄から [Azure Active Directory] を選択して、[追加] をクリックします。
10. 資格情報の入力画面で、[ユーザー名] 欄に **ContosoXX¥vmadmin**、 [パスワード] 欄に **MSC0569adfs!** と入力し、[OK] をクリックします。
11. [SCP の構成] 画面で、[次へ] をクリックします。
12. [構成の準備完了] ページで、[構成] をクリックします。
13. [構成が完了しました] ページで、[終了] の順にクリックします。

## 演習4.3.2. Active Directory へのドメイン参加

1. 仮想マシン CL で操作します。
2. [デスクトップ] 画面で、スタートメニューをクリックし、[設定] アプリをクリックします。
3. [設定] 画面で、[アカウント] をクリックし、[職場または学校にアクセスする] をクリックして、[接続] をクリックします。
4. [職場または学校アカウントのセットアップ] 画面で、[このデバイスをローカルの Active Directory に参加させる] をクリックします。
5. [ドメインに参加] 画面で、ドメイン名として、contosoXX.com と入力し、Enter キーを押します。
6. [ドメインに参加] 画面で、ユーザー名 **contosoXX¥vmadmin**、パスワード **MSC0569adfs!** と入力して、[OK] をクリックします。
7. [アカウントを追加する] 画面で、ユーザー名に **contosoXX¥vmadmin** と入力し、[次へ] をクリックします。
8. 指示に従い、コンピューターを再起動します。
9. 次の認証情報を使ってサインインを行います。

   ユーザー名: **contosoXX¥vmadmin**

   パスワード: **MSC0569adfs!**

10. スタートボタンを右クリックし、[ファイル名を指定して実行] を実行します。
11. [ファイル名を指定して実行] 画面で、「sysdm.cpl」と入力し、Enter キーを押します。
12. [システムのプロパティ] 画面で、[リモート] タブをクリックし、[ネットワーク レベル認証で～] の項目からチェックを外し、[ユーザーの選択] をクリックします。
13. [リモートデスクトップユーザー] 画面で、Domain Users グループを追加して、すべての画面で、[OK] をクリックします。
14. Windows からサインアウトします。
15. 次の認証情報を使ってサインインを行います。

   ユーザー名: **contosoXX¥yamada**

   パスワード: **Pa$$w0rd**

16. コマンドプロンプトを起動し、「gpupdate /force」と入力し、実行します。
17. コマンドプロンプト画面で、「dsregcmd.exe /status」と入力し、実行します。

18. AzureADJoined 項目が YES と表示されていることを確認します。また、AzureAdPrt 項目が YES と表示されることも同時に確認してください。なお、それぞれの項目が YES と表示されるまでに 1-2 時間程度要する場合があります。

L5

# 演習 5　安全なアプリケーションへのアクセス

# 演習の目標

この演習では条件付きアクセスや多要素認証の設定を通じて、Azure AD による認証・認可の操作に対する制限を行い、その特徴を確認します。

# 演習の概要

- 条件付きアクセスの設定

### 予想所要時間

40 分

# 演習5.1. 場所単位のアクセス制御

この演習では、特定の IP アドレスからアクセスした場合のみ、Azure AD でアプリケーションの認可が行われるよう、Azure AD を構成し、他の IP アドレスからアプリケーションにアクセスできなくなる様子を確認します。

## 演習5.1.1. 場所の設定

1. 仮想マシン CL で操作します。
2. ブラウザー画面を起動します。
3. ブラウザー画面で、アドレスに「http://www.ugtop.com/」と入力し、Enter キーをクリックします。Web サイトに表示される IP アドレスを控えておきます。

   IP アドレス: _____
4. 仮想マシン DC で操作します。
5. ブラウザー画面で新しいタブを開き、アドレスに「https://entra.microsoft.com/」と入力して、Enter キーを押します。
6. サインイン画面が表示される場合、グローバル管理者となるユーザーのユーザー名とパスワードを入力し、サインインします。
7. Microsoft Entra 管理センター画面で、左ペインの [保護] - [条件付きアクセス] をクリックします。
8. [条件付きアクセス] 画面で、[ネームドロケーション] をクリックします。
9. [ネームドロケーション] 画面で、[IP 範囲の場所] をクリックします。
10. [新しい場所 (IP 範囲)] 画面で、＋をクリックし、IP アドレスとして「手順 3 の IP アドレス/32」となるように入力し、[追加] をクリックします。
11. [新しい場所 (IP 範囲)] 画面で、[名前] 欄に「社内」と入力し、[作成] をクリックします。
12. [ネームドロケーション] 画面で、画面左側の [ポリシー] をクリックします。
13. [ポリシー] 画面で、[新しいポリシー] - [新しいポリシーを作成する] をクリックします。
14. [新規] 画面で、[名前] 欄に「社内アクセス」と入力します。
15. [新規] 画面で、[ユーザーまたはワークロード ID] をクリックし、[すべてのユーザー] をクリックします。

16. [新規] 画面で、[クラウドアプリまたは操作] をクリックし、[アプリを選択] をクリックします。
17. [選択] 画面で、[Office 365 Exchange Online] をクリックし、[選択] をクリックします。
18. [新規] 画面で、[条件] - [場所] をクリックします。
19. [場所] 画面で、[構成] 欄から [はい] を選択し、[対象外] タブをクリックして、[選択された場所] をクリックし、[なし] をクリックします。
20. [選択] 画面で、[社内] をクリックし、[選択] をクリックします。
21. [新規] 画面で、[アクセス制御] 欄配下の [許可] をクリックします。
22. [許可] 画面で、[アクセスのブロック] をクリックし、[選択] をクリックします。
23. [新規] 画面で、[ポリシーの有効化] 欄から [オン] をクリックして、[作成] をクリックします。

## 演習5.1.2. 社内ネットワークからのアクセス

1. 仮想マシン CL で操作します。
2. ブラウザー画面で、URL として「https://myapplications.microsoft.com/」にアクセスします。
3. サインイン画面で、グローバル管理者 (admin ユーザー) のユーザー名とパスワードでサインインします。
4. マイアプリ画面で、[Outlook] をクリックし、Web サイトにアクセスできることを確認します。

## 演習5.1.3. 社外ネットワークからのアクセス

1. ホストコンピューターで操作します。
2. ブラウザー画面で、URL として「https://myapplications.microsoft.com/」にアクセスします。
3. サインイン画面で、admin ユーザーでサインインします。
4. マイアプリ画面で、[Outlook] をクリックします。すると、アクセスが拒否されることが確認できます。
5. ブラウザー画面を閉じます。

# 演習5.2. 条件付きアクセスの設定

この演習では、与えられた課題に対して必要な設定をご自身で考え、設定を行います。後ほど、講師と答え合わせしますので、まずはご自身で課題に合わせた設定を行ってみてください。

## 演習5.2.1. 条件付きアクセスの課題

1. 演習 5.1 で作成したポリシーに対して、特定ユーザーのみポリシーが適用されないようにしてください。

2. グローバル管理者による Salesforce へのアクセスを行うときは多要素認証を必須となるように構成してください。

3. Azure AD 登録された Windows デバイスだけが SharePoint Online にアクセスできるように構成してください。

4. 社内からのアクセスは Windows デバイスまたは iOS、社外からのアクセスは iOS からのみアクセスできるように構成してください。

**Azure Active Directory を利用した**
**認証基盤の構築 演習ガイド**



2015 年 11 月 30 日　第 1 版　発行
2017 年　2 月　1 日　第 2 版　発行　著　者
2021 年 11 月　1 日　第 3 版　発行　発行者
2023 年　5 月 22 日　第 4 版　発行

トレノケート株式会社

〒 163-6019
東京都新宿区西新宿 6 丁目 8 番 1 号
住友不動産新宿オークタワー19 階
電話 03-3347-9686 FAX 03-3347-9699

http://www.trainocate.co.jp/
フリーダイヤル 0120-009686



MSC0569G-L1-04