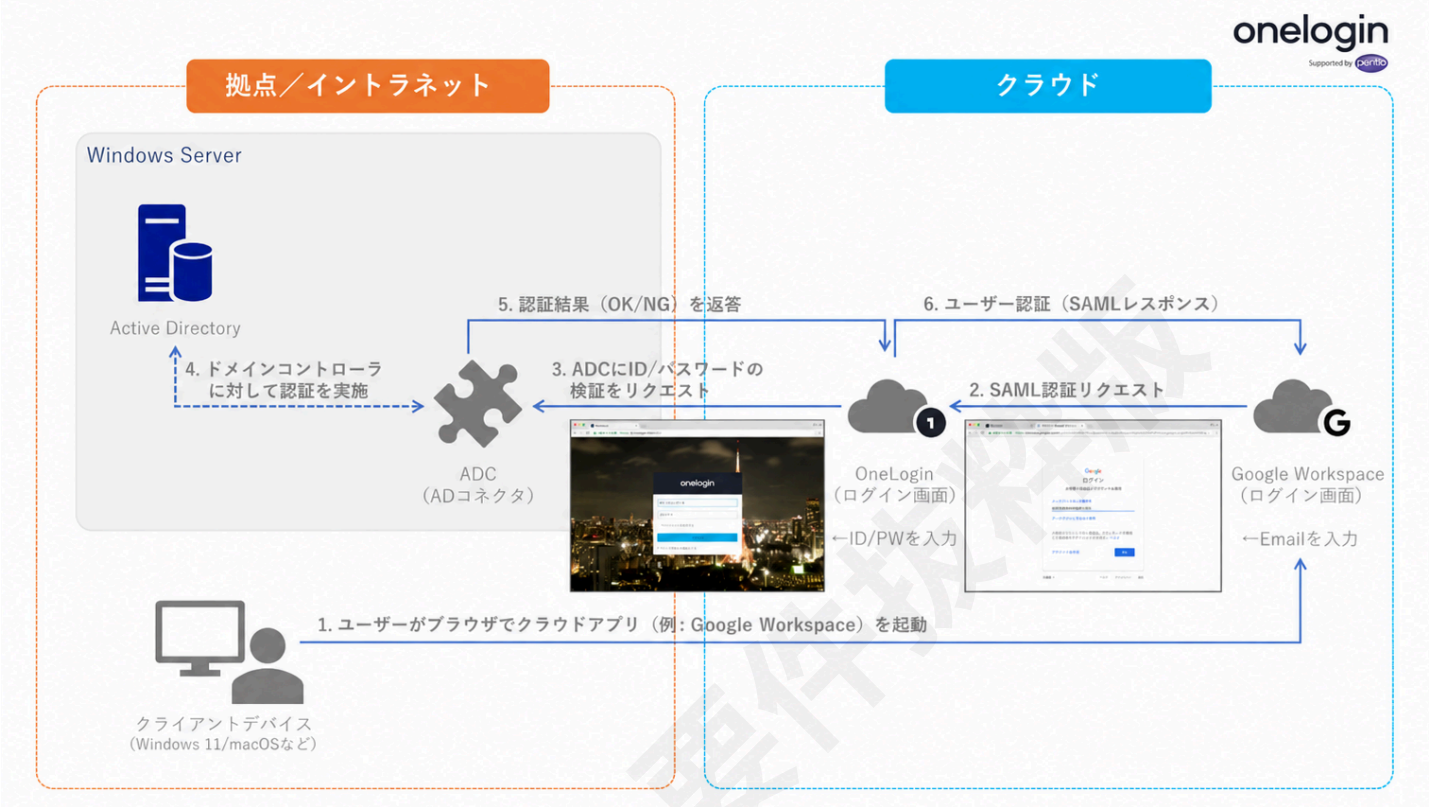
Active Directoryとディレクトリを統合する

長田 紘典
作成日・ 2018年4月23日・ 更新日・ 2026年11月17日



本記事では、OneLoginとActive DirectoryをOneLogin Active Directory Connectorを利用してディレクトリ連携し、ユーザー情報の同期とOneLoginのログイン認証をActive Directoryで実施するための設定について解説いたします。

目次

- Windows Server 2025への対応状況
- 前提条件
- ご利用・ご設定の前に
  1. OneLogin Active Directory Connectorとは
  2. OneLogin Active Directory Connectorと連携できるWindows Serverについて
- ご利用上の注意
  1. マネージドADサービスご利用上の注意点
  2. その他の注意点
- OneLogin Active Directory Connectorシステム要件
- Active Directoryユーザー項目について
  1. 必須項目
  2. 標準同期項目
  3. 標準同期項目以外を同期する

Windows Server 2025への対応状況

Windows Server 2025にはOneLogin Active Directory Connectorのバージョン7.0.2以上で対応しております。Windows Server 2025をご利用、もしくはリプレースを行うお客様は必ずバージョン7.0.2以上のOneLogin Active Directory Connectorをご利用ください。

前提条件

- OneLoginのライセンスプラン が **SSO**（1ディレクトリまで）, **Advanced**, **Professional** または旧ライセンスプラン **Starter**, **Enterprise**, **Unlimited** のいずれかであること
- OneLoginの **Super User** または **Account Owner** 権限を持つアカウントを所有していること
- OneLogin Active Directory Connectorをホストするサーバーの **Domain Admins** 権限を持つアカウントを所有していること
- **Active Directoryのドメインコントローラーの設定が完了し、正常に稼働していること**

ご利用・ご設定の前に

1. OneLogin Active Directory Connectorとは

OneLogin Active Directory Connector（以下、OneLogin ADC）とは、OneLoginとActive Directoryを接続して下記の機能を提供・実現するWindowsアプリケーションです。

1. **ユーザー情報のリアルタイム同期**
2. **Active Directoryの認証情報を用いたOneLoginへのログイン**
3. 統合Windows認証を用いたOneLoginへのSSO

本記事では **1. ユーザー情報のリアルタイム同期** および **2. Active Directoryの認証情報を用いたOneLoginへのログイン** の設定手順を解説いたします。統合Windows認証を用いたOneLoginへのSSOについては統合Windows認証を追加する：Windows Domain Authenticationインストールガイドをご覧ください。

2. OneLogin Active Directory Connectorと連携できるWindows Serverについて

OneLogin ADCのインストール先として、下記のWindows Serverを利用できます。必ずしもドメインコントローラーにインストールする必要はありません。

- Active Directory ドメインコントローラー
- Active Directory ドメインに参加したメンバーサーバー

ベスト事件技術版

ご利用上の注意

1. マネージドADサービスご利用上の注意点

- AWS Directoryが提供するManaged ADなど、マネージドADサービスとOneLoginを **直接的に** 連携することはできません。これはOneLogin ADCがWindows Serverにインストールして動作するプログラムであるため、プログラムをインストールするWindows Server環境が必須となるためです
- マネージドADサービスとOneLoginのディレクトリ連携をご希望される場合は、中継用のWindows Serverをご用意頂き、中継用サーバーがOneLogin ADCのシステム要件を満たすようにご設定ください
- マネージドADサービスにより、一部機能に制約が発生することがございます。これは本来OneLogin ADCはActive Directory ドメイン管理者権限を利用する必要があるサービスですが、マネージドADサービスではお客様に完全なドメイン管理権限が付与されないケースがあるためです。事前にマネージドADサービス提供会社に対して、ドメイン管理権限が取得できるかをご確認ください。OneLoginが必要とする詳細な権限については、下記米国One Identityのサポート記事に記載しております
  Create a Domain Service Account to run Active Directory Connector

2. その他の注意点

- Active Directoryのユーザー設定により、ユーザーがログインできるワークステーション制限を設定すると当該ユーザーはOneLoginにログインできません。OneLoginとの連携をご希望の場合には、必ずワークステーション制限は解除する必要があります

OneLogin Active Directory Connectorシステム要件

オペレーションシステム	Windows Server 2012 R2以降 *** Windows Server 2025でのご利用はOneLogin ADC 7.0.2以上が必要です** * FIPS準拠モードでは起動が失敗するためご注意ください
.NET Framework	.NET Framework 4.5.1以降
CPU	Pentium 4 以上
メモリ	512MB 以上
ストレージ	120MB 以上
ネットワーク	アウトバウンド 443ポート ** 通信先IPアドレスは次のネットワークレンジを参照*

ネットワークレンジ	• 23.183.113.12 • 23.183.112.12 • 52.34.225.194/31 • 52.34.255.196/30 • 52.34.255.200/29 • 52.34.255.208/28 • 52.34.255.224/27 • 18.216.23.64/26 (18.216.23.64 - 18.216.23.127) • 52.24.165.42 • 52.15.145.203 • 13.52.4.72/29 (13.52.4.72 - 13.52.4.79) • 23.183.112.0/24 • 23.183.113.0/24
プロキシ	インターネットオプションで設定したプロキシを利用可能 ** OneLogin ADCインストール時に指定したADCサービス実行アカウントでWindows Serverにログインし、インターネットオプションからプロキシ設定が必要です*
機能レベル	フォレスト / ドメイン 2003以上
リモートサーバー管理ツール	Active Directory Domain ServicesとActive Directory Lightweight Directory Services管理ツール ** Active Directory Connectorが動作するサーバーがドメインコントローラーでない場合は個別にインストールが必要です（ドメインコントローラーの場合はすでにインストール済みです）*

Active Directoryユーザー項目について

必須項目

OneLoginに同期するActive Directoryユーザーのアカウントは以下の4項目の登録が必須となっております。

Active Directory側の項目名（表示タブ）	OneLogin側の項目名
姓（全般）	Last name
名（全般）	First name
電子メール（全般）	Email
表示名（全般）	Active Directory側の必須項目であり、通常OneLogin側へは同期されません

システム要件抜粋版

標準同期項目

必須項目に加え以下の項目がOneLoginへ同期可能です。

Active Directory側の項目名（表示タブ）	OneLogin側の項目名
所属するグループ（所属するグループ）	MemberOf
ステータス（全般）	Status
会社名（組織）	Company
部署（組織）	Department
役職（組織）	Title
上司（組織）	Manager
Object GUID（属性エディター）	Object GUID ** 本項目の編集はできません*
ユーザーログオン名（アカウント）	UserPrincipalName ** 本項目の編集はできません*
Distinguished name（属性エディター）	Distinguished name ** 本項目の編集はできません*
sAMAccountName（属性エディター）	ユーザーログオン名（Windows 2000より前） ** 本項目の編集はできません*

標準同期項目以外を同期する

上記の標準同期項目以外はCustom User Fieldsを用いることで同期が可能です。例えば、Active Directoryの表示名（全般）をOneLoginのdisplayNameに表示するなどが可能です。設定手順はActive Directoryから標準同期項目以外の属性を追加同期するをご覧ください

Active Directory ディレクトリ連携のよくあるトラブルシューティングも合わせてご確認ください。

CONFIDENTIAL
当ウェブサイトに掲載されている情報は一般公開されているコンテンツを除き、当社の承諾なくご契約者様以外への開示・転送・転載することはできません