



Microsoft Azure

Microsoft Azure 自習書シリーズ No.18

Microsoft Azure Active Directory の活用

Published: 2015年4月3日
株式会社ソフィアネットワーク



本書に含まれる情報は本書の制作時のものであり、将来予告なしに変更されることがあります。提供されるソフトウェアおよびサービスは市場の変化に対応する目的で随時更新されるため、本書の内容が最新のものではない場合があります。本書の記述が実際のソフトウェアおよびサービスと異なる場合は、実際のソフトウェアおよびサービスが優先されます。Microsoft および Cloudlive は、本書の内容を更新したり最新の情報を反映することについて一切の義務を負わず、これらを行わないことによる責任を負いません。また、Microsoft および Cloudlive は、本書の使用に起因するいかなる状況についても責任を負いません。この状況には、過失、あらゆる破損または損失（業務上の損失、収益または利益などの結果的な損失、間接的な損失、特別の事情から生じた損失を無制限に含む）などが含まれます。

Microsoft、SQL Server、Visual Studio、Windows、Windows Server、MSDN は米国 Microsoft Corporation および、またはその関連会社の、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。その他、記載されている会社名および製品名は、各社の商標または登録商標です。

Microsoft Azure 自習書 No.18
Microsoft Azure Active Directory の活用

本ドキュメントの更新について

バージョン	更新日	内容
v1.0	2015/4/3	・初稿

目次

STEP 1. はじめに.....	6
1.1 はじめに.....	7
STEP 2. Microsoft Azure Active Directory の概要	8
2.1 Microsoft Azure Active Directory とは.....	9
2.2 Enterprise Mobility Suite	12
2.3 ユーザーとグループの管理.....	14
2.4 オンプレミスの Active Directory との統合	15
2.5 SaaS 型クラウド サービスへのアクセス管理	16
2.6 アプリケーション プロキシ	17
2.7 グループ ベースのアクセス制御.....	18
2.8 セルフサービス パスワード リセット	19
2.9 多要素認証	20
2.10 デバイス登録サービス	22
2.11 サインイン画面のカスタマイズ	23
2.12 レポート.....	24
2.13 Microsoft Azure Active Directory / Basic / Premium の違い.....	26
STEP 3. 前提条件と評価環境	27
3.1 前提条件	28
3.2 評価環境	31
STEP 4. Microsoft Azure Active Directory によるユーザーとグループの管理.....	34
4.1 ユーザー/グループの管理方法.....	35
4.2 Azure AD ドメインの作成.....	38
4.3 【参考】自己所有パブリック ドメインの追加	43
4.4 ユーザーの作成	48
4.5 グループの作成	61
4.6 ディレクトリ同期による Active Directory ドメインとの ユーザー/グループ同期.....	66
4.7 Azure AD Premium ライセンスの割り当て	109
4.8 グループ管理の委任	115
4.9 セルフサービス パスワード リセット	124
4.10 ブランドのカスタマイズ.....	153
STEP 5. Microsoft Azure Active Directory を利用したアプリケーションへのアクセス	158
5.1 Azure AD ユーザーによる SaaS アプリへのアクセス	159
5.2 アプリケーション プロキシによるオンプレミス アプリケーションの公開	176
5.3 レポートによるアプリケーション アクセスの確認.....	193
STEP 6. セキュアな Microsoft Azure Active Directory の利用	195

6.1	多要素認証の管理	196
6.2	多要素認証サービスの実装.....	197
6.3	多要素認証プロバイダーの実装.....	205
6.4	デバイスの登録	228

STEP 1. はじめに

この STEP では、本書の目的について説明します。

1.1 はじめに

Microsoft Azure Active Directory の評価を行う上で必要な環境の構築手順と、Microsoft Azure Active Directory による一元的な ID 管理を行うために必要な一連の手順を記述したものです。

本書の構成

章段	説明
1 はじめに	このドキュメントの概要について説明します。
2 Microsoft Azure Active Directory の概要	Microsoft Azure Active Directory で提供する各種機能について説明します。
3 前提条件と評価環境	Microsoft Azure Active Directory の各機能を利用開始するための前提となる評価環境について説明します。
4 Microsoft Azure Active Directory によるユーザーとグループの管理	この章では、Microsoft Azure Active Directory の初期設定としてユーザーやグループを作成し、管理するための設定について説明します。
5 Microsoft Azure Active Directory を利用したアプリケーションへのアクセス	この章では、Microsoft Azure Active Directory に作成したユーザーやグループを利用してアプリケーションにアクセスするための設定について説明します。
6 セキュアな Microsoft Azure Active Directory の利用	より安全に Microsoft Azure Active Directory を利用するための利用可能な設定について説明します。
7 まとめ	

STEP 2. Microsoft Azure Active Directory の 概要

この STEP では、Microsoft Azure Active Directory の概要と Microsoft Azure Active Directory で提供する様々なコンポーネントについて説明します。

2.1 Microsoft Azure Active Directory とは

クラウド コンピューティングが登場する以前の時代は Active Directory ドメインを組織内ネットワーク（オンプレミス）に配置し、ファイアウォールで保護することにより、インターネットとオンプレミスを安全に分離させると同時に、社内リソースへのアクセス管理の一元化（シングルサインオン）を実現させてきました。

しかし、クラウド コンピューティングの登場により、オンプレミスの Active Directory による管理が届かない範囲での認証や承認（認可）を必要とするケースが登場するようになりました。このことは Active Directory による一元管理ができなくなることを意味し、組織のセキュリティや IT 統制（ガバナンス）を維持する上で、とても大きな課題となっています。

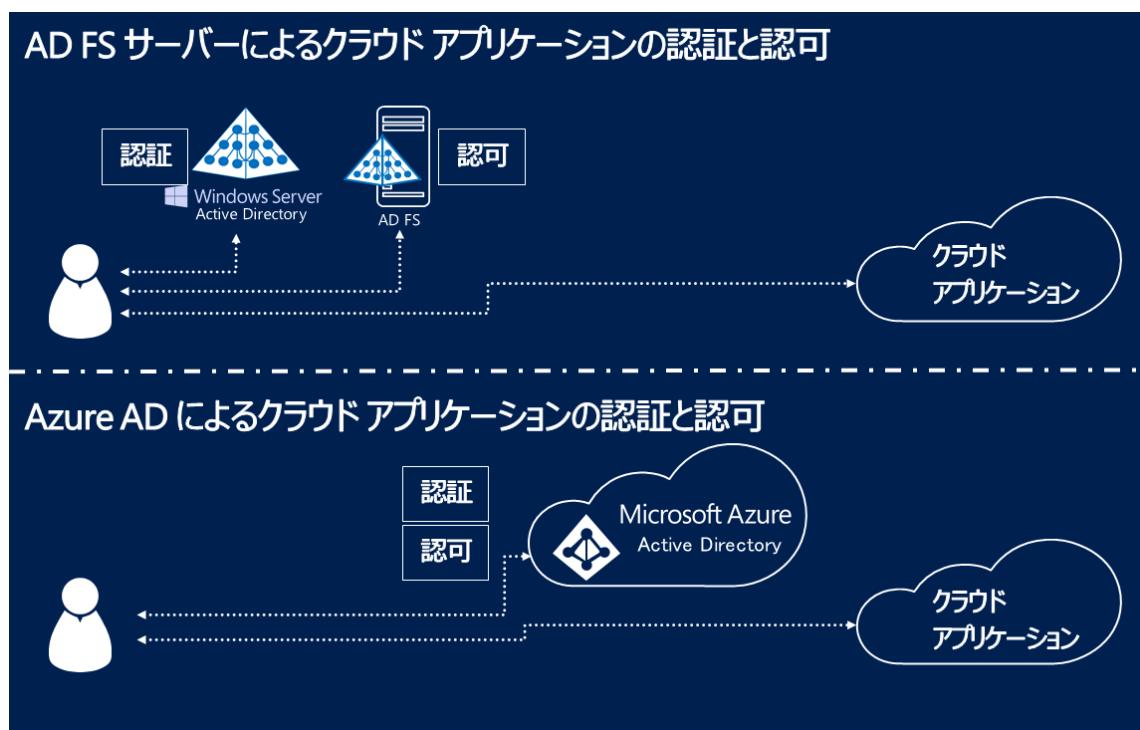
このような課題に対して、マイクロソフトでは 2 つの方法によって、認証と認可の範囲をクラウドにまで拡大し、オンプレミス/クラウドを問わず、安全なアプリケーションへのアクセスを提供します(図 2.1-1)。

ひとつは Active Directory フェデレーションサービス (AD FS) を利用したクラウドへのアクセスです。AD FS サーバーではオンプレミスの Active Directory ドメインでサインイン（認証）した情報に基づいて AD FS サーバーがクラウドへの認可の手続きを行う仕組みで、オンプレミスの Active Directory を活用してクラウドへアクセスする点が最大の特徴です。

そしてもうひとつの方法が本書で取り上げる Microsoft Azure Active Directory (以下、Azure AD) を利用したアクセスです。Azure AD はこれまでオンプレミスの Active Directory が担ってきた認証と認可機能をクラウドに実装することで、オンプレミスの Active Directory の有無を問わず、手軽にクラウド上のアプリケーションにアクセスするための認証や認可機能を利用できます。

(なお、2 つのアクセス方法を組み合わせた実装方法もあります。これについては「2.4 オンプレミスの Active Directory との統合」で解説します。)

図 2.1-1 クラウド アプリケーションに対する一元的な認証と認可の 2 つのアプローチ



これまで、クラウド上のアプリケーションを利用する場合、それぞれのクラウド サービスが提供する認証・認可機能を利用することが一般的でした。しかし、クラウド サービスにアクセスするごとに必要とされるユーザー名とパスワードはパスワードを使いまわしてしまうという問題を引き起こしています。

そこで、Azure AD では Azure AD へ一度サインイン（認証）するだけで、Azure AD で用意されたポータル サイト（アクセス パネル）からショートカットをクリックするだけで、それぞれのクラウド上のアプリケーションにアクセス（認可）が実現します（図 2.1-2）。このようなシンプルな認証と認可の仕組みによって、オンプレミスの Active Directory と同様に安全かつ便利なクラウドへのアクセスを実現します。

図 2.1-2 Azure AD の認証を利用することによるメリット

Azure AD には、認証と認可に関わる基本機能のみを提供する、無償で利用可能な Azure AD と組織の ID 管理に不可欠な様々なコンポーネントを備えた有償版のエディションである Azure AD Premium と Azure AD Basic が用意されています。それぞれのエディションで提供するコンポーネントの違いについては、後続の節で解説します。

2.2 Enterprise Mobility Suite

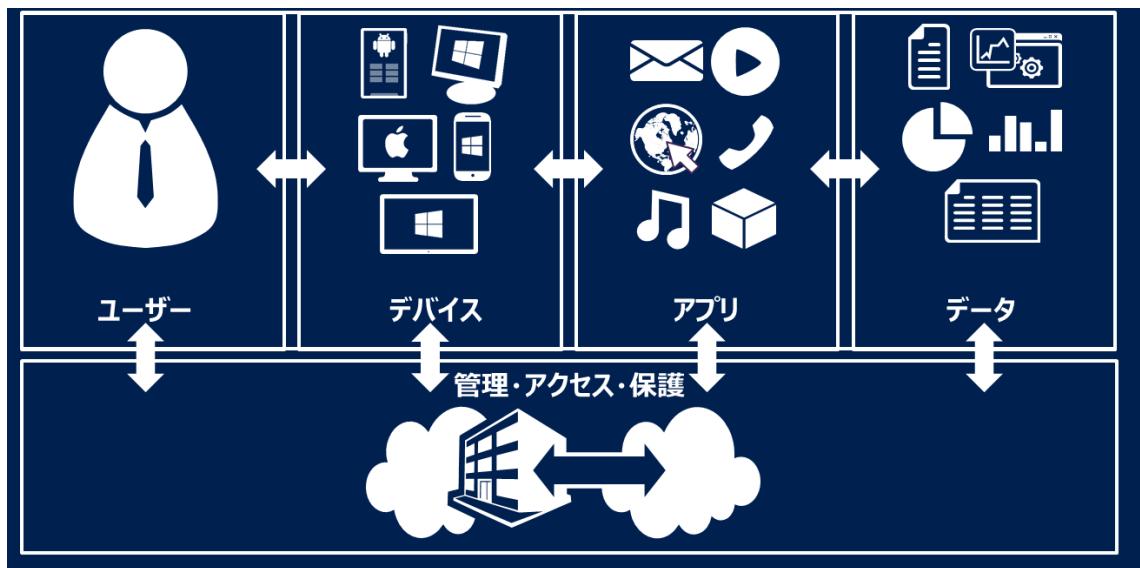
前の節では Azure AD について解説し、クラウドにおける認証と承認機能を提供する、ID 管理サービスであることを確認しました。

一方、私たちが組織の中で保護しなければならない分野は ID 管理だけではありません。クラウド/オンプレミスを問わず、いつでも、どこでも仕事ができるような環境を整備するにあたり、組織のセキュリティポリシーにあった運用や IT 統制（ガバナンス）の実装は欠かせません。

組織によるアプリケーションのアクセス範囲がクラウドにまで拡大される状況で、これまでと同じようなセキュリティ レベルで業務を遂行するためには、セキュリティの世界における多層防御と同じように、クラウドのアクセスに関わる、すべての要素に対する対策が重要です。

Enterprise Mobility Suite (以下、EMS) では、クラウドまたはオンプレミスへのアクセスを行う、ユーザー、デバイス、アプリ、データの各分野に対する管理を一元化し、組織の要件にあつた運用を実現します（図 2.2-1）。具体的には、ユーザー、デバイス、アプリ、データの各分野に合わせて、次のソリューションを提供しています。

図 2.2-1 モバイルデバイスで保護すべき分野と EMS におけるソリューション



EMS で提供されるコンポーネントは以下のとおりです。

- Microsoft Azure Active Directory Premium

Microsoft Azure Active Directory Premium (以下、Azure AD Premium) はユーザーの管理に必要な機能を提供します。具体的には認証と認可を中心とする ID 管理サービスをクラウドで提供し、様々なサービスへの認証と認可の一元化を実現します。本書では、Microsoft Azure Active Directory Premium で提供される、様々な機能について次の節から順番に解説します。

- Microsoft Intune

Microsoft Intune はユーザーが利用するデバイスやアプリをクラウド ベースで管理するサービスです。デバイスの資産管理、デバイスにインストールされるアプリケーションの管理、設定を一元化するためのポリシー管理、マルウェア対策などが含まれます。

また、管理対象のデバイスには Windows PC だけでなく、Windows RT 等の Windows タブレット、iOS、Android などのモバイル デバイスの管理もまとめて行うことができます。

詳しくは姉妹ドキュメント「Microsoft Intune 評価ガイド」をご覧ください

Microsoft Intune 評価ガイド

http://download.microsoft.com/download/8/3/F/83F4F0D1-DFCA-4104-A6BF-7E1A5A49A0AF/EMS_Windows_Intune_Evalguide_v1.0.docx

- Microsoft Azure Rights Management

Microsoft Azure Rights Management はデータ（ドキュメント）の保護をクラウド ベースで行うソリューションで、ドキュメントにアクセスするユーザーに合わせて詳細なアクセス制御（権限）を行うことができます。EMS で提供される Microsoft Azure Rights Management は Office 365 E3/E4 のプランで提供される、同名のサービスを拡張したもので、Office ドキュメントだけでなく、その他のファイルに対する権限を設定することもできます。また、メールに対する保護も組織内/組織外を問わず行うことが可能です。

詳しくは姉妹ドキュメント「モバイル環境管理の評価ガイド」をご覧ください

モバイル環境管理の評価ガイド

http://download.microsoft.com/download/8/3/F/83F4F0D1-DFCA-4104-A6BF-7E1A5A49A0AF/EMS_AAD_ARMS_Evalguide_v1.0.docx

2.3 ユーザーとグループの管理

Azure AD の最も基本となるサービスがユーザーとグループの管理機能です。組織内でユーザーの一元管理を行うために Active Directory ドメイン サービスをインストールし、ユーザーやグループを作成して管理するように、クラウドに存在する様々なサービスにアクセスするためのユーザーやグループを管理する機能を Azure AD では提供します。

Azure AD ではユーザーを作成することにより、様々なクラウド サービスへのサインインの一元化（シングル サインオン）を行ったり、サインインしたユーザー情報に基づくサービスへのアクセス制御（アクセス権管理）を行ったりと、クラウドにおける認証と認可の機能を提供できるようになります。無償版の Azure AD ではユーザーとグループを合わせて 50 万オブジェクトまで、Azure Premium と Azure AD Basic では無制限にオブジェクトを作成できます。

一方、Azure AD のグループはメンバーシップの管理を Azure AD の全体管理者だけでなく、一般ユーザーも行うように構成できます（Azure AD 全体管理者だけがメンバーシップの管理ができるように構成することも可能です）。メンバーシップの管理をユーザー自身が行えるようになることで、自分でメンバーになるグループを選択できるようになります。

Azure AD のユーザーとグループは、Azure ポータル サイトから直接作成することができるほか、Windows PowerShell を利用して作成する方法や、ディレクトリ同期ツールを利用して社内設置の Active Directory ドメインコントローラーに登録されたユーザーとグループを同期させて、作成することができます。

図 2.3-1 Azure AD にユーザー／グループを作成する方法



Azure ポータルサイトから作成する方法については「4.4 ユーザーの作成」、「4.5 グループの作成」にて、ディレクトリ同期ツールによる作成方法については「4.6 ディレクトリ同期ツールによる Active Directory ドメインとのユーザー／グループの同期」にて、それぞれ解説します。

2.4 オンプレミスの Active Directory との統合

「2.3 ユーザーとグループの管理」でも解説したように Azure AD に登録し、利用するユーザー やグループは Azure ポータル サイトに直接作成して利用するだけでなく、オンプレミスの Active Directory ドメイン コントローラーに作成されたユーザー やグループを Azure AD と同期させて作成することができます。

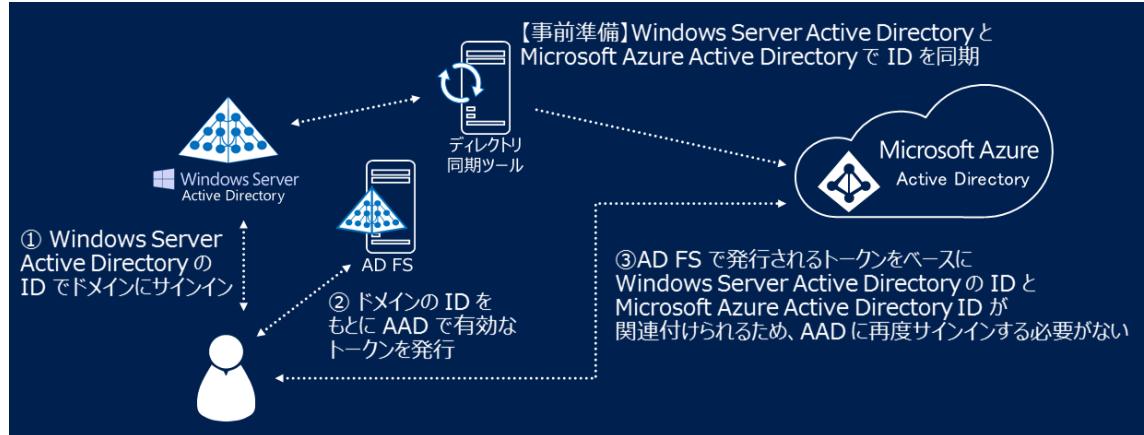
社内に Active Directory ドメインが既にある場合、社内でサインインを行うためのユーザー名とパスワードを既に利用しているため、ディレクトリ同期ツールを利用して同期を行えば、社内でサインインを行うときに使用するユーザー名とパスワードをそのまま Azure AD のサインインにも流用することができます。

ディレクトリ同期ツールは Azure AD が無償で提供するツールで、オンプレミスの Active Directory ドメインに参加する、任意のサーバーにインストールして利用します。ディレクトリ同期ツールがインストールされたサーバーは定期的に（既定では 3 時間ごと）オンプレミスの Active Directory ドメイン コントローラーと Azure AD の間で同期を行い、オンプレミスの Active Directory ドメイン コントローラーと同じユーザー/グループが Azure AD にも作成されます。

ディレクトリ同期は一部の例外を除き、オンプレミスの Active Directory ドメイン コントローラーから Azure AD へ一方向に同期されるため、同期されるユーザーの管理（ユーザーの名字や名前の変更など）はオンプレミスの Active Directory ドメイン コントローラー側で管理します。

また、ディレクトリ同期することによって作られた Azure AD のユーザーは図 2.4-1 のようにオンプレミスの Active Directory のユーザーと ID 連携を行うことにより、Active Directory にサインインした情報をを利用して Azure AD にアクセスすることができます。このような設定を行うことにより、Azure AD にアクセスする際に改めてサインイン操作を行う必要がありません。

図 2.4-1 AD FS と Azure AD によるシングルサインオン環境



2.5 SaaS 型クラウド サービスへのアクセス管理

Azure AD にユーザーを作成し、ユーザーにサインインを行わせる目的はクラウド上のアプリケーションにアクセスすることにあります。Azure AD では、Office 365 や Microsoft Intune などのマイクロソフトが提供する SaaS 型クラウド サービス（アプリケーション）はもちろんのこと、2000 以上の SaaS 型クラウド サービスを登録し、Azure AD 経由でアクセスすることができます。これにより登録されたクラウド サービスは、それぞれのサービスで提供されるユーザー名とパスワードを毎回入力しなくても、Azure AD のユーザー名とパスワードを利用してサインインするだけでサービスにアクセスできるようになります。

Azure AD ユーザーを利用して、様々なアプリケーションにアクセスするときは Azure AD がユーザー向けに提供する「アクセス パネル」と呼ばれる Web サイトにアクセスし、アクセス パネルが提供するアイコンをクリックしてサービスにアクセスします（図 2.5-1）。

図 2.5-1 アクセス パネル画面



アクセス パネルに配置されたアイコンは Azure AD が提供する ID 連携技術により、それぞれのクラウド サービスにアクセスするために必要な認証作業（に相当する操作）を自動的に行い、シングルサインオンを実現します。

アクセス パネルに登録可能なアプリケーションの数は無償版の Azure AD ではユーザー当たり 10 アプリケーションまで、Azure Premium と Azure AD Basic では無制限にアプリケーションに登録できます。

アクセス パネルへのアプリケーションの登録方法については「5.1 Azure AD ユーザーによる SaaS アプリへのアクセス」にて解説します。

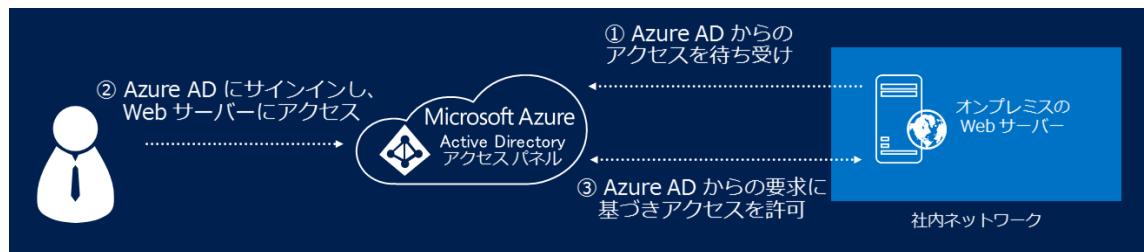
2.6 アプリケーション プロキシ

Azure AD にサインインすることによりアクセスできるサービスはクラウド上のアプリケーションだけではありません。オンプレミスの SharePoint Server のような Web サーバーを外部に公開し、アクセス パネル経由でアクセスすることも可能です。

オンプレミスの Web サーバーを外部に公開する場合、Azure AD Premium で提供されるアプリケーション プロキシ機能を利用します。Azure AD のアプリケーション プロキシは単純に外部に公開されたサーバーをアクセス パネルに関連付けるだけでなく、Web サーバーを外部に公開する作業自体も提供します。

アプリケーション プロキシでは、アプリケーション プロキシ コネクタ ツールを提供しており、アプリケーション プロキシ コネクタを Web サーバーにインストールすると、Web サーバーは Azure AD からのアクセス要求を待ち受けします。これにより、組織内ネットワークからインターネットへのネットワーク セッションを利用して Azure AD にサインインしたユーザーによるアクセス パネル経由での Web サーバーへのアクセスを実現するため、境界ネットワーク (DMZ) を用意したり、ファイアウォールに外部向けのアクセスルールを作成したりする必要がありません。

図 2.6-1 アプリケーション プロキシの動作



アプリケーション プロキシは DMZ を用意したり、ファイアウォールに新たなルールを作成するなどの新たなセキュリティ上の脅威となるような設定を行うことなく、外部にオンプレミスのサーバーを公開し、いつでも、どこからでもクライアントからのアクセスを受け付けることができます。

アプリケーション プロキシを利用してオンプレミスのサーバーを公開する方法については「5.2 アプリケーション プロキシによるオンプレミス アプリケーションの公開」にて解説します。

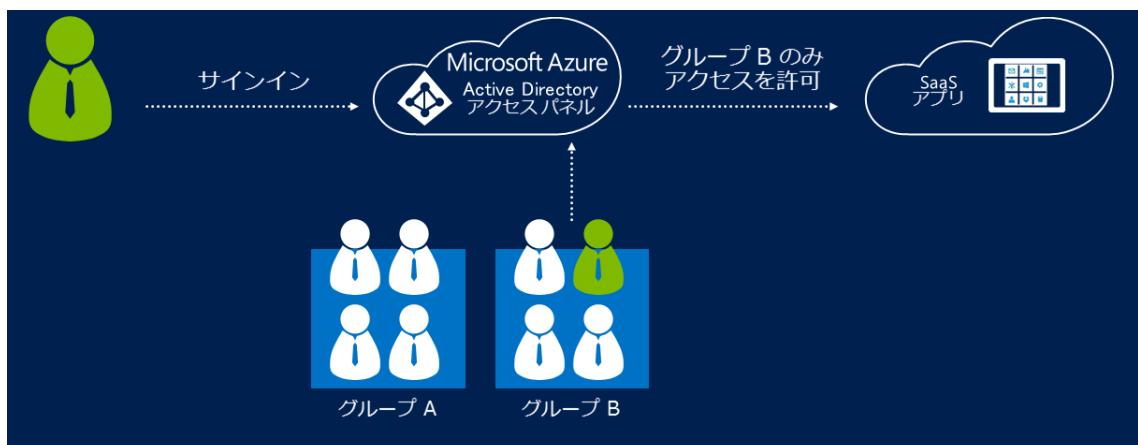
2.7 グループ ベースのアクセス制御

SaaS 型クラウド サービス（アプリケーション）を Azure AD に登録する際、そのアプリケーションを利用するユーザーを選択することで、アクセス許可を設定できます。アクセス許可が割り当てられたユーザーは Azure AD にサインインするとアクセスパネルのアプリケーション一覧に登録されたアプリケーションが表示され、アプリケーションへアクセスできるようになります。このように、Azure AD へのアプリケーションの登録はユーザーをベースとしてアクセス制御を行うことが可能です。

一方、Azure AD Premium ではユーザーをベースとしてアクセス制御に加えて、グループをベースにしたアクセス制御を行うことも可能です（図 2.3-1）。アプリケーションを Azure AD に登録する際、そのアプリケーションを利用できるグループを選択できるようになっており、グループを選択することによって、グループのメンバー全員に対してアプリケーションへのアクセス許可をまとめて割り当てられます。

一般的に多くのユーザーを抱える組織では、ユーザーを単位とするアクセス制御は管理が煩雑になります。そのため、複数のユーザーをグループにまとめ、グループを単位としてアクセス制御を行えることは大きな利点といえるでしょう。

図 2.7-1 グループを利用したクラウドへのアクセス制御



グループ ベースのアクセス制御については「5.1 Azure AD ユーザーによる SaaS アプリへのアクセス」にて解説します。

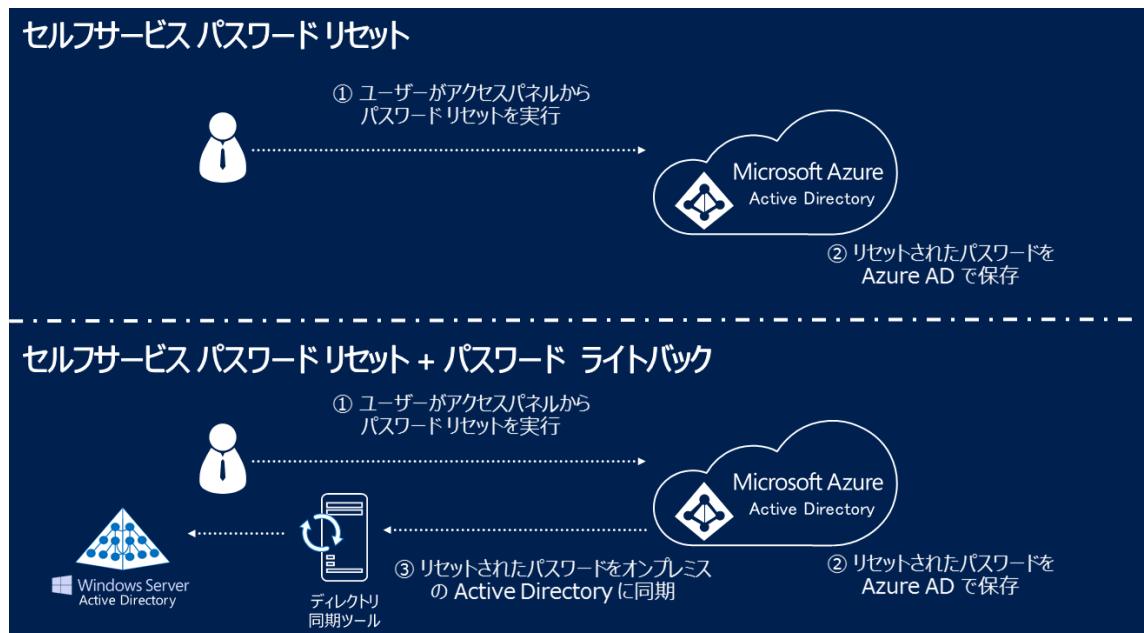
2.8 セルフサービス パスワード リセット

Azure AD ユーザーが自身のパスワードを忘れたときに、ユーザー自身でパスワードのリセットを行うことができる機能がセルフサービス パスワード リセットです。セルフサービス パスワード リセットはユーザーがパスワードを忘れたときに、あらかじめ登録した携帯電話にテキストメッセージを送信するなどして本人確認を行った後、新しいパスワードを設定します。

本人確認の手段には、携帯電話による通話、携帯電話のショート メッセージ (SMS)、メールアドレスのいずれかを使用します。利用する本人確認の手段は、あらかじめユーザーがアクセス パネルで定義することができます。

セルフサービス パスワード リセットは Azure AD Premium または Basic で利用可能な機能ですが、Azure AD Premium ではセルフサービス パスワード リセット機能に加えて Azure AD でリセットされたユーザーのパスワードをオンプレミスの Active Directory に同期するパスワード ライトバックと呼ばれる機能が実装されています（図 2.8-1）。これにより、Azure AD ユーザーのパスワードと同時にオンプレミスの Active Directory ユーザーのパスワードもリセットされるため、パスワード リセット後も引き続き Azure AD とオンプレミスの Active Directory で同じユーザー名とパスワードを使い続けることができます。

図 2.8-1 セルフ サービス パスワード リセットの動作とパスワード ライトバックの組み合わせによる動作



セルフサービス パスワード リセットとパスワード ライトバックの設定方法については「4.9 セルフサービス パスワード リセット」にて解説します。

2.9 多要素認証

Azure AD へのサインインを行う際、ユーザー名とパスワードによる認証に加えて、追加の認証要素を組み合わせる、多要素認証を実装することができます。多要素認証を利用することにより、ユーザー名とパスワードが不正に利用されるようなケースがあっても、追加の認証要素によって物理的なデバイスを保有していることが求められるため、Azure AD へのサインイン認証をより安全に行うことができます。

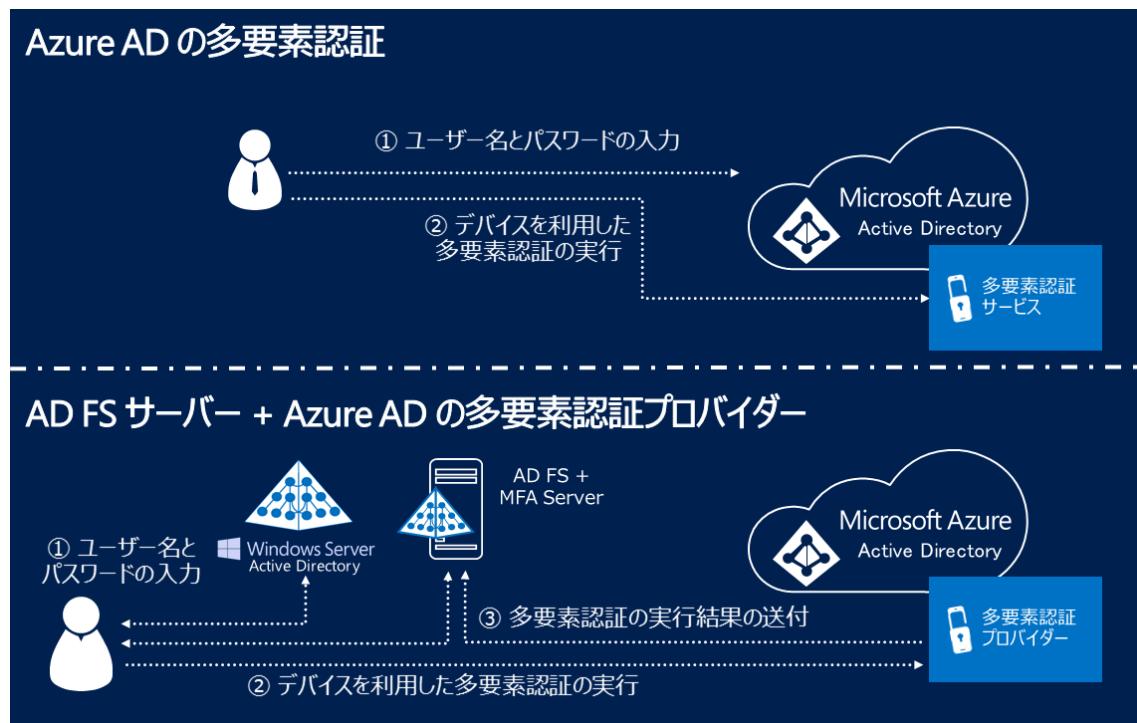
Azure AD の多要素認証では、電話による音声確認、携帯電話の SMS による確認、モバイル アプリによる確認方法などの、物理的なデバイスを用いた追加の認証要素を選択できます。

Azure AD の多要素認証には 2 種類の実装方法があります。

ひとつは Azure AD 自身が提供する多要素認証（多要素認証サービス）を利用する方法で、クラウドで多要素認証を含む、認証に関わるすべての操作を完結する方法です（図 2.9-1 上）。

もうひとつは認証と認可にオンプレミスの AD FS サーバーを利用し、多要素認証の部分だけ（多要素認証プロバイダー）を Azure AD に担当させる方法です（図 2.9-1 下）。多要素認証プロバイダーは Azure AD Premium で提供する機能です。

図 2.9-1 Azure AD の多要素認証と AD FS サーバー/多要素認証プロバイダーの実装



Microsoft Azure Active Directory の活用

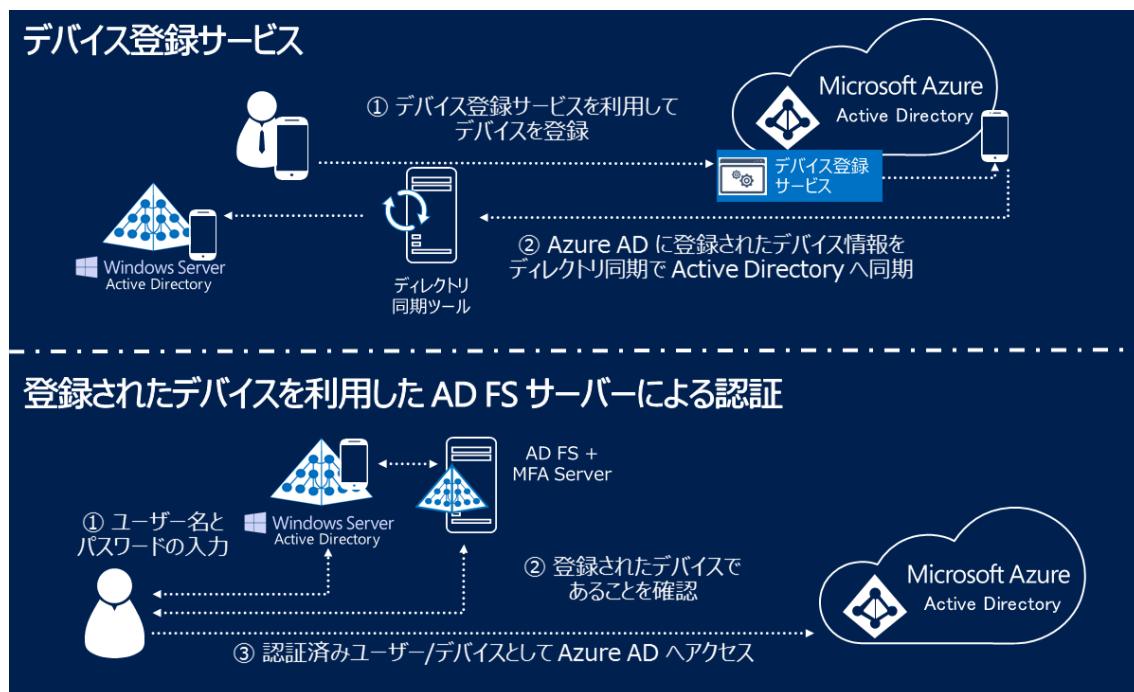
2 つの多要素認証の実装方法の違いは多要素認証を利用する条件の違いにあります。Azure AD 自身が提供する多要素認証サービスの場合、多要素認証の利用有無はユーザー単位で設定するのに対して、AD FS サーバーと組み合わせて実装する多要素認証では外部ネットワーク/内部ネットワーク、Active Directory グループのメンバーなど細かな条件をもとに利用有無を設定できます。

多要素認証については「6.1 多要素認証の管理」、「6.2 多要素認証サービスの実装」、「6.3 多要素認証プロバイダーの実装」にて、それぞれ解説します。

2.10 デバイス登録サービス

あらかじめ決められたデバイスによる Azure AD へのアクセスだけを許可する、デバイス認証機能を利用するにあたり、“決められたデバイス”を登録するためのサービスがデバイス登録サービスです。デバイス認証はオンプレミスの AD FS サーバーで提供される機能（図 2.10-1 下）であり、Azure AD ではデバイス認証のためのデバイス登録だけを担当します（図 2.10-1 上）。

図 2.10-1 デバイス登録サービスと登録されたデバイスの認証



デバイス登録は Windows 8.1 などの Windows PC のほか、iOS や Android などのモバイルデバイスを対象に行うことができ、Windows 8.1 ではワークプレイス参加 (Workplace Join)、iOS や Android ではあらかじめ決められた URL にアクセスして登録します。

登録されたデバイスは Azure AD ユーザーと関連付けて保存され、同時にディレクトリ同期ツールを利用してオンプレミスの Active Directory にも同期されます。

AD FS サーバーはオンプレミスでの認証・認可時に Active Directory に保存されたデバイス情報をもとに、登録されたデバイスであるかを見極め、アクセス可否の判断を行います。

デバイス登録サービスについては「6.4 デバイスの登録」にて解説します。

2.11 サインイン画面のカスタマイズ

Azure AD Premium または Basic では、サインインページとアクセスパネルのページに組織のロゴや色合いなどを配した、オリジナルのページを構成することができます。

図 2.11-1 Azure AD 標準のサインイン画面



図 2.11-2 カスタマイズされたサインイン画面



2.12 レポート

一般的な ID 管理の基本的な要素として、AAA（認証、認可、アカウンティング）が挙げられますが、Azure AD を利用した ID 管理を行う場合でも、この要素は重要であることに変わりありません。Azure AD では認証と認可のための要素についてはこれまでの節で確認してきましたが、アクセス情報の管理を担当するアカウンティングについては Azure AD のレポートがその役割を担います。

Azure AD のレポート機能は [監査レポート] と呼ばれる Azure AD に対して行われた操作を記録するレポートをはじめ、アクセスパネルに登録されたアプリケーションへのアクセス状況を記録する [アプリケーションの使用状況] レポートやパスワード リセット機能の利用を記録する [パスワード リセット アクティビティ] レポートなど様々な角度からアクセス状況を分析するために必要なレポートが用意されています。

加えて Azure AD Premium では機械学習ベースのレポートが用意されています。機械学習ベースのレポートとは、セキュリティイベントをレポートに記録する際に、単純に発生したことを記録するのではなく、Azure AD Premium で用意されたアルゴリズムに基づいて不正アクセスを見極め、記録するものです。[不規則なサインイン アクティビティ] や [疑わしいアクティビティを示す IP アドレスからのサインイン] などが機械学習ベースで生成される、主なレポートです。

表 2.12-1 Azure AD で用意されているレポートの種類

異常なアクティビティ	
不明なソースからのサインイン	追跡されないサインインの試行を示す場合があります。
複数のエラー発生後のサインイン	ブルート フォース攻撃の成功を示す場合があります。
複数の地域からのサインイン	複数のユーザーが同じアカウントでサインインしていることを示す場合があります。
疑わしいアクティビティを示す IP アドレスからのサインイン	持続的な侵入の試行後のサインインの成功を示す場合があります。
感染の疑いのあるデバイスからのサインイン	感染の疑いのあるデバイスからサインインしようとした可能性があります。
不規則なサインイン アクティビティ	ユーザーのサインイン パターンに対して異常なイベントを示す場合があります。
異常なサインイン アクティビティのユーザー	アカウントが侵害された可能性があるユーザーを示します。

展開済みアクティビティ ログ	
監査レポート	ディレクトリの監査されたイベント
パスワード リセット アクティビティ	組織内で行われたパスワード リセットに関する詳しい情報を示します。
パスワード リセット登録アクティビティ	組織内で行われたパスワード リセット登録の詳しい情報を示します。
グループ アクティビティ	ディレクトリ内のすべてのグループ関連アクティビティに関するアクティビティ ログを提供します。
展開済み統合アプリケーション	
アプリケーションの使用状況	ディレクトリと統合されたすべての SaaS アプリケーションの利用状況の概要を提供します。
アカウント プロビジョニングのアクティビティ	外部アプリケーションにアカウントのプロビジョニングを試行した回数の履歴を示します。
アカウント プロビジョニング エラー	外部アプリケーションへのユーザーのアクセスに対する影響を示します。

レポートの操作については「5.3 レポートによるアプリケーション アクセスの確認」にて解説します。

2.13 Microsoft Azure Active Directory / Basic / Premium の違い

これまでの節で確認したように、Azure AD には様々な機能があります。これらの機能は無償で提供される Azure Active Directory、有償のサービスとして提供される、Azure Active Directory Premium、Azure Active Directory Basic に分かれており、それぞれのサービスで提供する機能は次のとおりです。

表 2.13-1 3 つの Azure AD サービスの違い

	Azure AD	Azure AD Basic	Azure AD Premium
サービスとしてのディレクトリ（オブジェクト数）	500,000	無制限	無制限
ユーザー / グループ管理	○	○	○
事前統合された SaaS アプリ/カスタム アプリに対する SSO	ユーザーあたり 最大 10	ユーザーあたり 最大 10	無制限
ディレクトリ同期ツール	○	○	○
ユーザーベースのアクセス管理/プロビジョニング	○	○	○
クラウド ユーザーのセルフサービス パスワード変更	○	○	○
基本的なセキュリティ レポート	○	○	○
セルフサービス パスワード リセット		○	○
サインイン画面のカスタマイズ		○	○
99.9% の SLA		○	○
セルフサービス グループ管理			○
セルフサービス パスワード リセットによる 社内設置型 Active Directory ユーザーのパスワード リセット			○
機械学習ベースのセキュリティ レポート			○
多要素認証プロバイダー			○
Microsoft Identity Management (MIM)			○

STEP 3. 前提条件と評価環境

この STEP では、Microsoft Azure Active Directory Premium の評価を行うにあたり、必要となる前提条件と評価環境について説明します。

3.1 前提条件

本書では、Azure AD Premium に含まれる機能を評価するための手順を解説します。その評価に当たり、前提条件によって異なる手順を実行する必要があるため、本節では、評価に当たっての前提条件を解説します。

◆ 評価環境となるドメイン

Azure AD で使用するユーザー アカウントは「ユーザー名@ドメイン名」の形式によって作成・管理されます。そのため、Azure AD の利用に当たっては最初にドメイン名を定義する必要があります。Azure AD で使用するドメイン名には次の 2 つのパターンがあるため、どちらの方法で評価を行うか、最初に決定してください。

contoso.com のような組織で所有するドメイン名（自己所有パブリック ドメイン名）がある場合には、Azure AD に自己所有パブリック ドメイン名を登録し、利用することが可能です。本書の評価を行うにあたり、自己所有パブリック ドメイン名を利用する場合は Azure AD に登録可能な自己所有パブリック ドメインをドメイン レジストラ事業者から事前に取得し、「4.3 【参考】自己所有パブリック ドメインの追加」の手順に沿って登録してください。

自己所有パブリック ドメイン名を利用する場合は、本書のすべての手順を評価することが可能です。

Azure AD では既定のドメイン名として *****.onmicrosoft.com (*****は契約者が定義した名前) となるドメイン名が割り当てられます。組織が本来使用するドメイン名とは異なるため、本書の運用で利用するケースは少ないですが、本書では評価目的のため *****.onmicrosoft.com となるドメイン名を利用して評価を行うことも可能です。

ただし、自己所有パブリックドメインを登録していることを前提としている以下の節の手順は評価できませんので、ご注意ください。

- 4.3 【参考】自己所有パブリックドメインの追加
- 4.6 ディレクトリ同期による Active Directory ドメインとのユーザー / グループ同期
- 4.9 セルフサービス パスワード リセット 節内の
 - ディレクトリ同期ユーザーのパスワード リセット (AADSync の場合)
 - ディレクトリ同期ユーザーのパスワード リセット (DirSync の場合)
- 6.3 多要素認証プロバイダーの実装
- 6.4 デバイスの登録

◆ Azure テナント/ Azure AD ディレクトリの登録・管理方法

Azure AD Premium の各機能を利用する場合、Microsoft Azure テナントを保有していることが前提となります。そのため、Azure テナントをお持ちでない場合は事前に Azure テナントを取得します。

Azure AD Premium は「ディレクトリ」と呼ばれる単位で、Azure テナントから管理します。そのため、Azure テナントが用意できたら、Azure テナントに Azure AD のディレクトリを登録し、Azure AD の管理ができるようにします。

このとき、Azure テナントと Azure AD ディレクトリの契約と管理方法には次のパターンがあるため、どの方法で登録・管理を行うか、最初に決定してください。

outlook.com や OneDrive 等の個人を対象とした顧客向けに提供されるアカウントである、マイクロソフト アカウントを利用して Azure テナントにサインインし、Azure AD ディレクトリの管理も行います。

マイクロソフト アカウントおよび Azure テナントをお持ちでない場合、マイクロソフトの Web サイトから事前に作成・取得してください。

マイクロソフト アカウントの登録手続き

<http://www.microsoft.com/ja-jp/msaccount/signup/default.aspx>

Azure サブスクリプションの申し込み

<http://msdn.microsoft.com/ja-jp/windowsazure/ee943806.aspx>

Azure テナントを用意したのち、Azure テナントに Azure AD ディレクトリを登録する場合、Azure AD ディレクトリを新規に作成し登録する方法と、Office 365 や Microsoft Intune の契約を通じて既に作られた Azure AD ディレクトリを Azure テナントに関連付けて登録する方法があります。

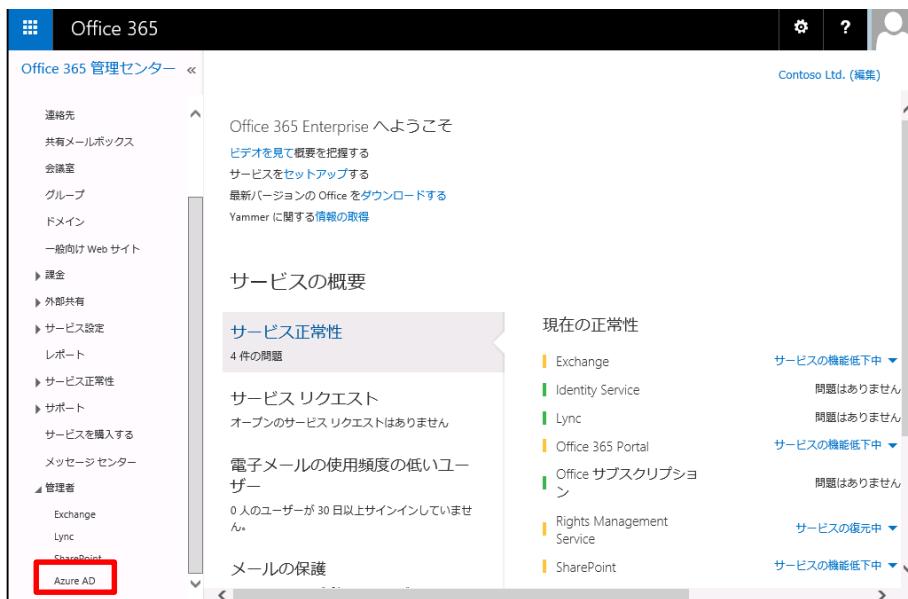
Azure テナントに Azure AD ディレクトリを登録する方法については、「4.2 Azure AD ドメインの作成」で行います。

【Note:】

一般的にユーザーを管理する場合、ドメイン内のひとりのユーザーが管理者になります（たとえば、Active Directory ドメインの管理者である Administrator ユーザーはドメイン内に作られたユーザーです）。しかし、この方法で管理する場合、Azure AD ディレクトリに作られたユーザー（組織アカウント）ではないユーザー（マイクロソフト アカウント）が Azure AD ディレクトリの管理者となる点に注意してください。

現在、Office 365 や Microsoft Intune を契約している場合、Office 365 や Microsoft Intune を通じて Azure AD ディレクトリを作成し、Azure AD のユーザー アカウント（組織アカウント）を保有しているため、マイクロソフト アカウントではなく、既に作成された組織アカウントを利用して Azure AD ディレクトリの管理を行うことができます。

組織アカウントを利用して Azure AD ディレクトリを管理する場合、Azure AD ディレクトリを管理するための Azure テナントを新規に作成（サインアップ）します。Office 365 管理センター サイト (<https://portal.office.com/>) にアクセスし、[Azure AD] リンクをクリックすると、組織アカウントを利用して Azure テナントを新しくサインアップできます。



The screenshot shows the 'Office 365 Management Center' interface. On the left, there is a navigation menu with various service links like 'Office 365 Enterpriseへようこそ', 'Exchange', 'Identity Service', 'Lync', 'Office 365 Portal', 'Officeサブスクリプション', 'Rights Management Service', and 'SharePoint'. At the bottom of this menu, the 'Azure AD' link is highlighted with a red rectangle. The main content area is titled 'サービスの概要' (Service Summary) and contains sections for 'サービス正常性' (Service Health), 'サービス リクエスト' (Service Requests), and 'メールの保護' (Email Protection). The 'サービス正常性' section lists several services with their current status: Exchange (サービスの機能低下中), Identity Service (問題はありません), Lync (問題はありません), Office 365 Portal (サービスの機能低下中), Officeサブスクリプション (問題はありません), Rights Management Service (サービスの復元中), and SharePoint (サービスの機能低下中).

以上の方針により、Azure テナントに Azure AD ディレクトリが登録されるため、「4.2 Azure AD ドメインの作成」の手順は不要です。

3.2 評価環境

本書では、Azure AD Premium に含まれる機能を確認しますが、STEP 6 の一部の手順では AD FS サーバーを配置し、Azure AD とオンプレミスの Active Directory での ID 連携を実装した状態で評価を行う必要があります。そのため、STEP 4~5 の前提条件と STEP 6 の前提条件が異なります。

◆ STEP 4~5 の評価環境

STEP 4~5 で利用する、各コンピューターの情報は以下の通りです。

表 3.2-1 評価環境 コンピューター情報

コンピューター名	説明
WS2012-DC01	Microsoft Azure Active Directory とディレクトリ同期を行う Active Directory ドメインコントローラー。 ドメイン名 : contoso.com Windows Server 2012 R2 を実行。
W81CL01	Microsoft Azure Active Directory を利用するコンピューター。 contoso.com ドメインに参加。 Windows 8.1 Enterprise または Pro を実行 (x86/x64)。

評価環境のアカウント情報は以下の通りです。

表 3.2-2 評価環境アカウント情報

アカウント名	パスワード	説明
Contoso\\$Administrator	P@ssw0rd	ドメイン管理者アカウント

コンピューターのネットワーク情報は以下の通りです。

表 3.2-3 評価環境 ネットワーク情報

コンピューター名	IP アドレス	サブネット マスク	デフォルト ゲートウェイ	DNS
WS2012-DC01	192.168.1.110	255.255.255.0	192.168.1.1	127.0.0.1
W81CL01	192.168.1.120	255.255.255.0	192.168.1.1	192.168.1.110

実際に評価環境を構築する際は、適宜、お手元のネットワーク環境に置き換えてください。

(*1) デフォルトゲートウェイおよび DNS サーバーの IP アドレスは、インターネットへの接続ができるように構成しておいてください。

◆ STEP 6 の評価環境

STEP 6 では AD FS サーバーを実装し、Azure AD との間での ID 連携（シングルサインオン）を実装していることが前提条件です。STEP 6 の評価を行う前に、以下のサイトよりダウンロード可能なドキュメントを参考に AD FS サーバーの実装と ID 連携環境の実装を行ってください。（STEP 5 の評価の後で実装することも可能です）

企業内システムと Microsoft Azure の VPN 接続、ADFS、Office 365 との連携:

http://download.microsoft.com/download/4/D/E/4DEC2B01-85B1-4FF0-961E-AE9CB86597A1/06_VPN%20connection%20of%20Microsoft%20Azure%20and%20enterprise%20systems%20ADFS%20O365.pdf

STEP 6 で利用する、各コンピューターの情報は以下の通りです。

表 3.21-4 評価環境 コンピューター情報

コンピューター名	説明
WS2012-DC01	Microsoft Azure Active Directory とディレクトリ同期を行う Active Directory ドメインコントローラー。 Active Directory Federation Service (AD FS) ドメイン名 : contoso.com Windows Server 2012 R2 を実行。
W81CL01	Microsoft Azure Active Directory を利用するコンピューター。 contoso.com ドメインに参加。 Windows 8.1 Enterprise または Pro を実行 (x86/x64)。

評価環境のアカウント情報は以下の通りです。

表 3.21-5 評価環境アカウント情報

アカウント名	パスワード	説明
Contoso\\$Administrator	P@ssw0rd	ドメイン管理者アカウント

コンピューターのネットワーク情報は以下の通りです。

表 3.2-6 評価環境 ネットワーク情報

コンピューター名	IP アドレス	サブネット マスク	デフォルト ゲートウェイ	DNS
WS2012-DC01	192.168.1.110	255.255.255.0	192.168.1.1	127.0.0.1
W81CL01	192.168.1.120	255.255.255.0	192.168.1.1	192.168.1.110

実際に評価環境を構築する際は、適宜、お手元のネットワーク環境に置き換えてください。

(*1) デフォルトゲートウェイおよび DNS サーバーの IP アドレスは、インターネットへの接続ができるように構成しておいてください。

◆ 必要なソフトウェアとソフトウェアライセンス

本書で構築する環境の画面ショット内では、TechNet サブスクリプションまたは MSDN サブスクリプションライセンスを用いた製品を使用しています。

TechNet サブスクリプション、MSDN サブスクリプション及びボリュームライセンスをお持ちでない場合は、以下のサイトより評価版ライセンスを利用して下さい。

Windows Server 2012 R2 評価版:

<http://technet.microsoft.com/ja-jp/evalcenter/dn205286.aspx>

Windows 8.1 Enterprise (x86/x64) 評価版:

<http://technet.microsoft.com/ja-jp/evalcenter/hh699156.aspx>

また、Microsoft Azure の評価版の契約（テナント）を本書では使用します。評価版であるかに関わらず、Microsoft Azure のテナントをお持ちでない場合は、以下のサイトよりテナントを事前に取得してください。

Microsoft Azure 評価版:

<http://azure.microsoft.com/ja-jp/pricing/free-trial/>

STEP 4. Microsoft Azure Active Directory によるユーザーとグループの管理

本章では、Azure AD の初期設定ならびにユーザー管理方法について解説します。

この STEP では、次のことを学習します。

- ✓ Azure AD ドメインの登録
- ✓ ユーザー/グループの作成と管理
- ✓ オンプレミス Active Directory とのユーザー/グループの同期
- ✓ Azure AD Premium ライセンスの割り当て
- ✓ グループ管理の委任
- ✓ ユーザー パスワードのリセット
- ✓ サインイン ページのカスタマイズ

4.1 ユーザー/グループの管理方法

Azure AD を経由して様々なクラウドサービスにアクセスする場合、アクセスするための ID 情報（ユーザー/グループ）を作成する必要があります。ただし、Azure AD には 3 種類のユーザー管理方法があり、それぞれの方法によって、行うべき作業が異なります。

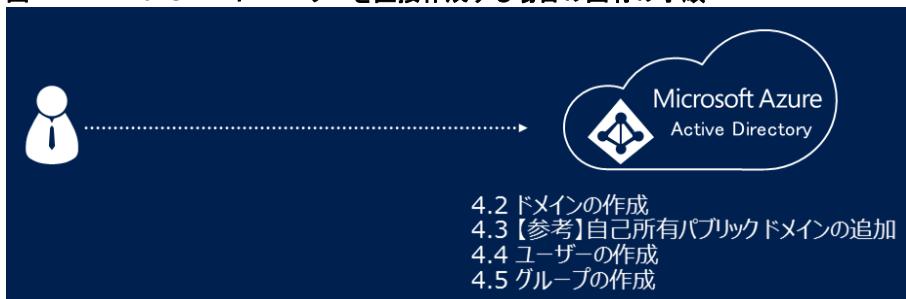
図 4.1-1 サインイン方法別 Azure AD ユーザー/グループの管理手順



Azure AD へのユーザー作成とサインインの方法には次の 3 つのパターンがあります。

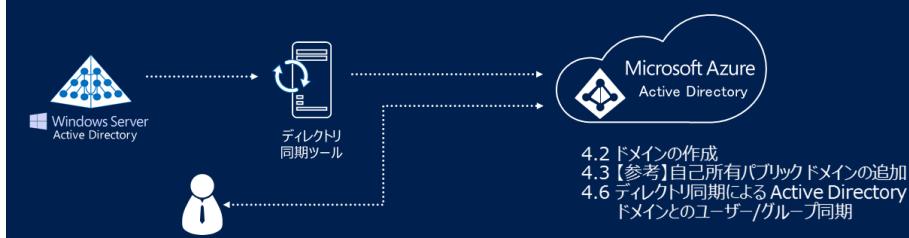
- Azure AD に直接ユーザーを作成し、作成したユーザーでサインイン
最もシンプルな方法です。オンプレミスの Active Directory ドメインが存在しない場合や、オンプレミスの Active Directory ドメインとの連携が必要ない場合に、この方法を選択します。本書の手順「4.2 ドメインの作成」、「4.3 【参考】自己所有パブリック ドメインの追加」、「4.4 ユーザーの作成」、「4.5 グループの作成」を実行することで、このパターンのユーザー管理が行えるようになります。

図 4.1-2 Azure AD にユーザーを直接作成する場合の固有の手順



- オンプレミスの Active Directory ドメインと同期を行い、Azure AD に作成されたユーザーでサインイン
ディレクトリ同期ツールを利用して、オンプレミスの Active Directory ドメインと同期を行うことで、社内で使用する PC と同じユーザー名/パスワードで Azure AD にもサインインできます。本書の手順「4.2 ドメインの作成」、「4.3 【参考】自己所有パブリック ドメインの追加」、「4.6 ディレクトリ同期による Active Directory ドメインのユーザー/グループの同期」を実行することで、このパターンのユーザー管理が行えるようになります。

図 4.1-3 オンプレミスの Active Directory と同期することでユーザーを作成する場合の固有の手順



- オンプレミスの Active Directory ドメインと同期を行い、AD FS サーバーを利用してシングルサインオン
オンプレミスの Active Directory ドメインでサインインしたときの情報をもとに、様々なアプリケーションやサービスにシングルサインオンを行う ID 連携を実装する場合には、この方法を選択します。この方法では、オンプレミスに Active Directory フェデレーション サービス（以下、AD FS）サーバーの実装が必要です。本書では、AD FS サーバーを利用したシングルサインオンの実装方法については解説しません。Microsoft Azure 自習書シリーズ「06: 企業内システムと Microsoft Azure の VPN 接続、ADFS、Office 365 との連携」を参考に AD FS サーバーを利用したシングルサインオン環境の実装を行ってください。
その後、本書の「4.2 ドメインの作成」を実行することで、このパターンのユーザー管理が行えるようになります。

図 4.1-4 AD FS サーバーを利用する場合におけるユーザー作成の固有の手順



Microsoft Azure 自習書 No.18
Microsoft Azure Active Directory の活用

企業内システムと Microsoft Azure の VPN 接続、ADFS、Office 365 との連携：

http://download.microsoft.com/download/4/D/E/4DEC2B01-85B1-4FF0-961E-AE9CB86597A1/06_VPN%20connection%20of%20Microsoft%20Azure%20and%20enterprise%20systems%20ADFS%20O365.pdf

以上 3 つのユーザー管理方法について、それぞれの特徴を確認した上で、組織で使用するサインイン方法を決定し、それぞれの方法に合わせた環境評価を行ってください。

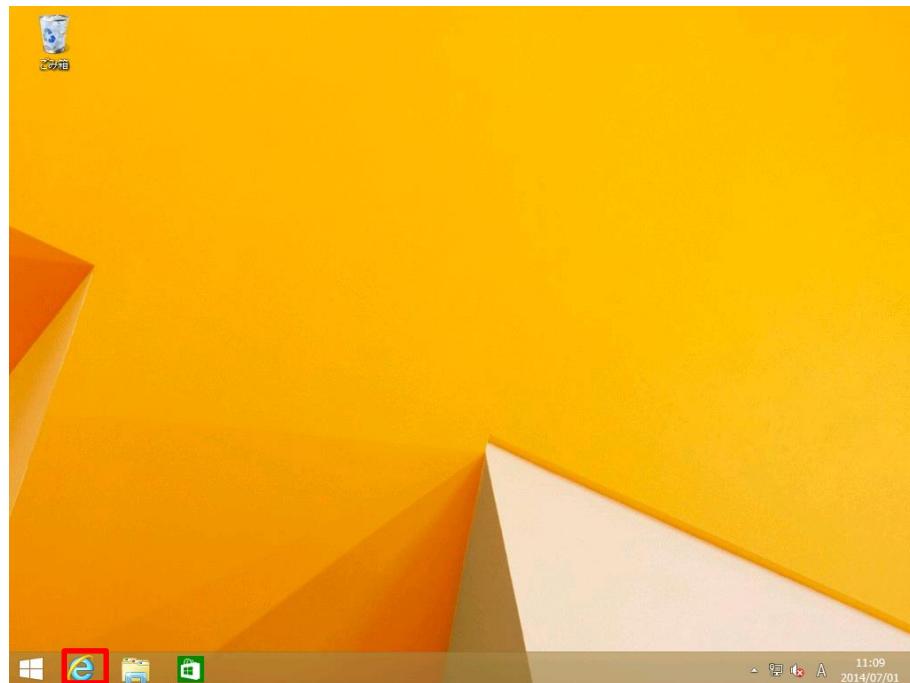
4.2 Azure AD ドメインの作成

Microsoft Azure 管理ポータルにアクセスし、Azure AD ドメインを新しく作成します。「3.1 前提条件」でも解説したように、マイクロソフト アカウントを利用して Azure AD ディレクトリを新規に作成する方法と、Office 365 や Microsoft Intune によって既に作られた Azure AD ディレクトリを Azure テナントに関連付けする方法があります。この 2 つ方法では、それぞれ手順 5 の操作が異なります。事前にどちらの方法で Azure AD ディレクトリの関連付けを行うか、決定してから操作してください。

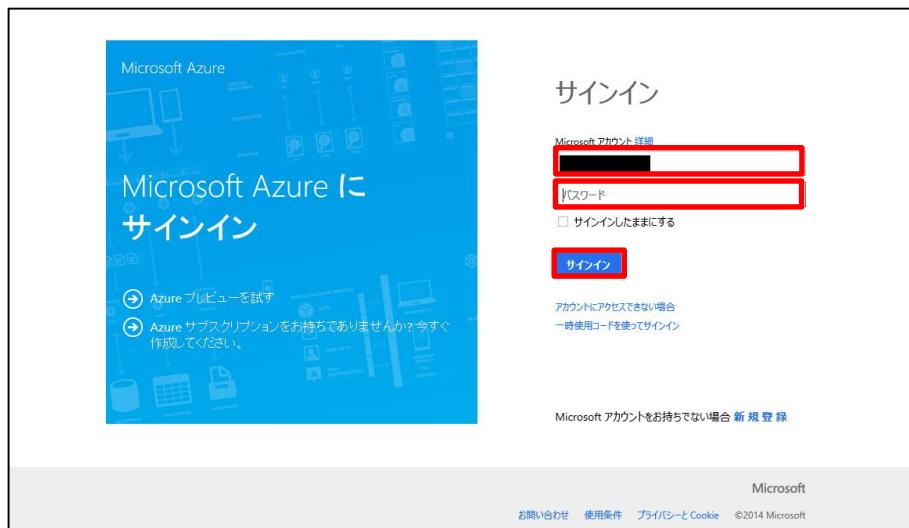
また、組織アカウントを利用して Azure AD ディレクトリの管理を行う場合は本手順は不要です。

1. W81CL01 コンピューターで操作します。

Internet Explorer を起動します。



2. Internet Explorer 画面で、URL として「<https://manage.windowsazure.com>」と入力し、Microsoft Azure 管理ポータルにアクセスします。Microsoft Azure 管理ポータルのサインイン画面で、Azure テナントの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] をクリックします。



3. Microsoft Azure 管理ポータル画面で、[新規] をクリックします。



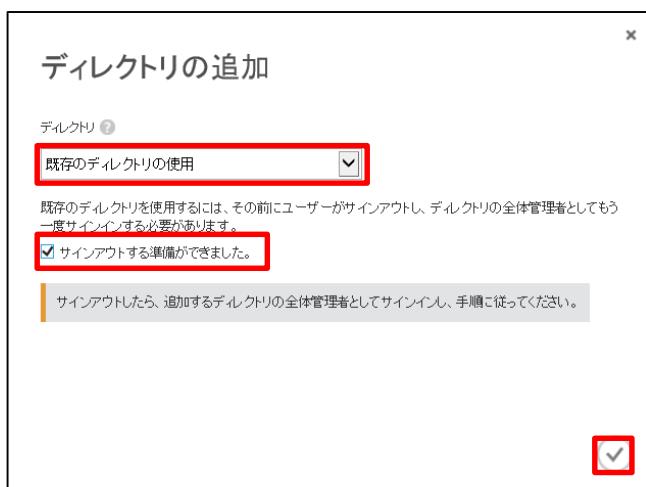
4. [新規] 画面で、[アプリケーション サービス] - [ACTIVE DIRECTORY] - [ディレクトリ] - [カスタム作成] の順にクリックします。



5. [ディレクトリの追加] 画面で、マイクロソフト アカウントを利用して Azure AD ディレクトリを登録する場合、新しく Azure AD ドメインを作成するため、[ディレクトリ] 欄に [新しいディレクトリの作成] を選択し、[名前] 欄にドメインの利用者等を表す名前、[ドメイン名] 欄にドメイン名、[国/地域] 欄に[日本] をそれぞれ選択し、チェック マークをクリックします。



一方、既に Office365 や Microsoft Intune の契約をしており、組織アカウントをお持ちの場合は組織アカウントを利用して既存の Azure AD ディレクトリを登録する場合には、[ディレクトリ] 欄に [既存のディレクトリの使用] を選択し、[サインアウトする準備ができました。] にチェックをつけ、チェック マークをクリックします。



6. [active directory] 画面で、新しく AAD ドメインが作成されたことを確認します。

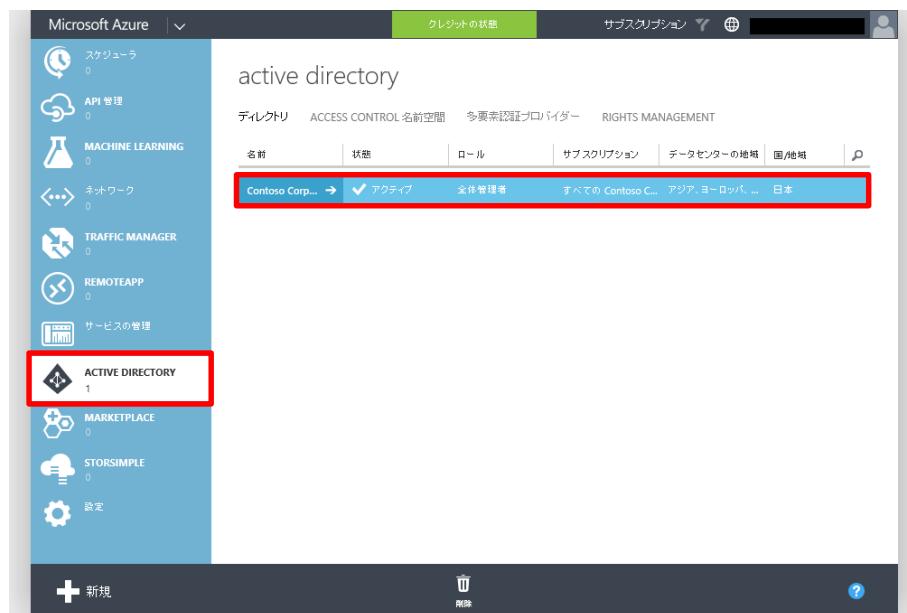
The screenshot shows the Microsoft Azure Active Directory blade. On the left, there's a sidebar with various service icons and a 'New' button. The main area is titled 'active directory' and contains tabs for 'ディレクトリ', 'ACCESS CONTROL', '名前空間', '多要素認証プロバイダー', and 'RIGHTS MANAGEMENT'. Below these tabs, there are filters for '名前', '状態', 'ロール', 'サブスクリプション', 'データセンターの地図', '国/地域', and '検索'. A red box highlights the search bar and the results below it. The results list 'Contoso Corporation' with an 'アクティベート' (Activate) button next to it. Other items listed include 'すべての Contoso Corpor...', 'アジア', 'ヨーロッパ', '米国', and '日本'. At the bottom right of the blade, there are navigation icons for back, forward, and help.

4.3 【参考】自己所有パブリック ドメインの追加

本手順では、前の手順で作成した Azure AD ドメインに contoso.com のような組織で使用するドメイン名（自己所有パブリック ドメイン）を追加する方法を確認します。なお、自己所有パブリック ドメインを追加するにはインターネットで利用可能なドメイン名を保有しており、ドメインの DNS サーバーにアクセスできることが前提です。

評価のための自己所有パブリック ドメインを保有していない場合は本手順を省略することも可能です。

1. Microsoft Azure の管理ポータルサイト [ACTIVE DIRECTORY] をクリックし、[Contoso corporation] をクリックします。



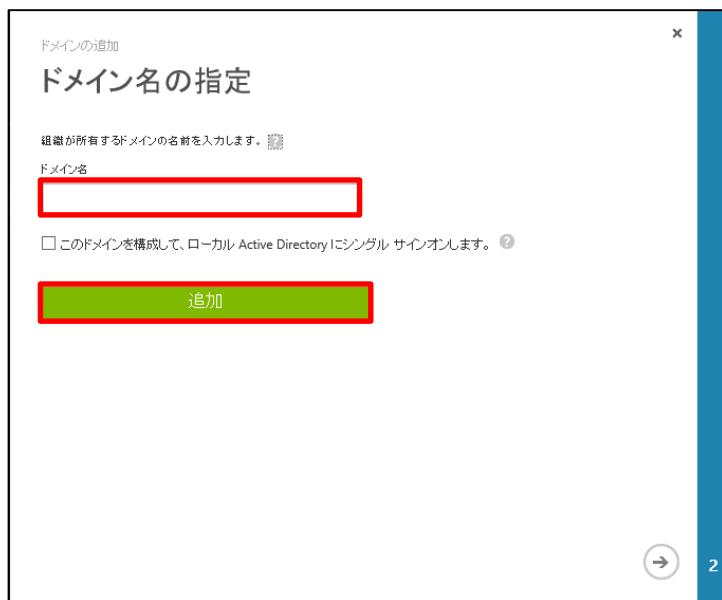
2. [Contoso corporation] 画面で、[ドメイン] をクリックします。

The screenshot shows the Microsoft Azure Active Directory interface for the 'contoso corporation' tenant. The top navigation bar includes 'Microsoft Azure', 'サブスクリプション' (Subscription), a user icon, and a 'Domains' tab which is highlighted with a red box. Below the navigation is a large blue diamond icon with three nodes connected by lines. To its right, the text reads: 'ディレクトリを使用する準備ができました。作業開始するためのオプションは次のとおりです。' (The directory is ready for use. The following options are available to start working.) A checkbox below says '□ 次回アクセス時はクイックスタートをスキップする' (Skip quick start on next access). At the bottom, there's a section titled '作業を開始する' (Start working) with a numbered step 1: 'ユーザー サインイン エクスペリエンスの向上' (User sign-in experience improvement), which includes a note about adding custom domains. A 'New' button (+) is at the bottom left.

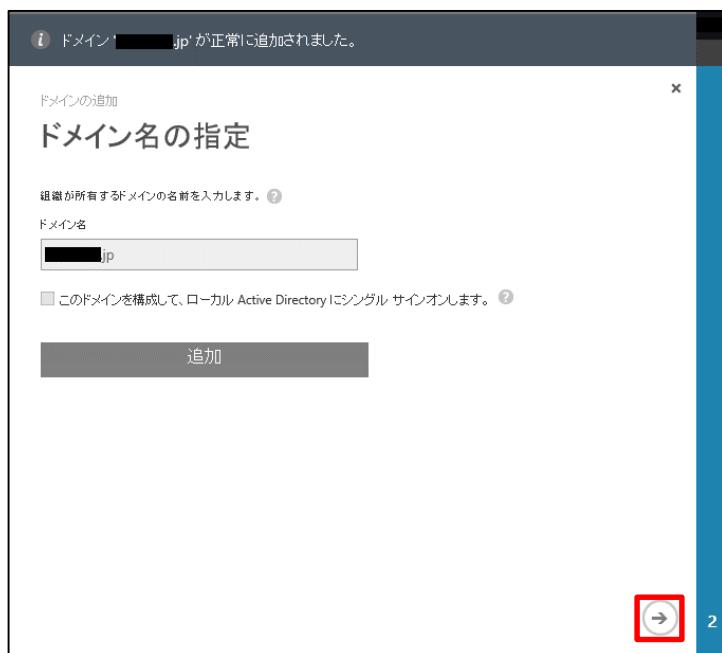
3. [ドメイン] 画面で、[カスタムドメインの追加]をクリックします。

This screenshot shows the same 'Domains' page after a custom domain has been added. The 'Domains' tab is still selected. A message box appears in the center stating: 'ディレクトリで既定のドメイン [REDACTED] が使用されています。サインオン環境をカスタマイズするには、カスタムドメインを追加してください。' (The directory uses the default domain [REDACTED]. To customize the sign-on environment, add a custom domain.) Below this message is a red box around the 'カスタムドメインの追加' (Add custom domain) button, which is now visible. The rest of the interface remains the same, including the sidebar with various Azure service icons and the 'New' button at the bottom.

4. [ドメイン名の指定] 画面で、[ドメイン名] に自己所有パブリック ドメイン名を入力し、[追加] をクリックします。

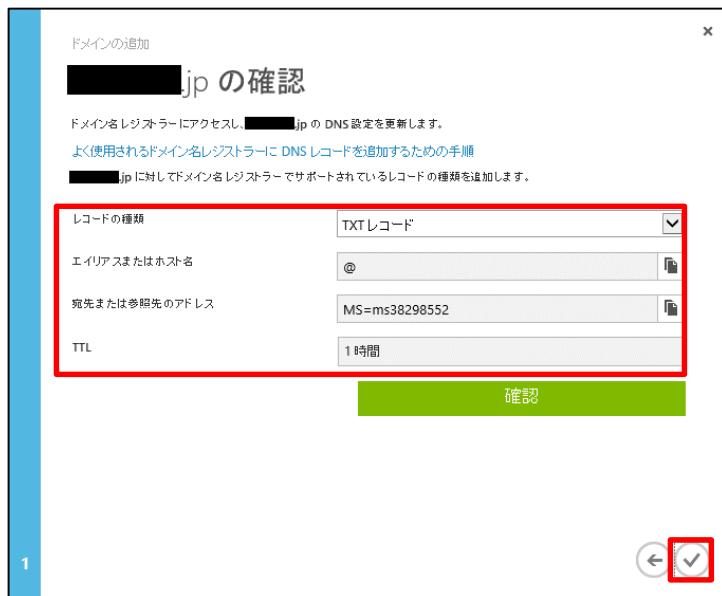


5. [ドメイン名の指定] 画面で、ドメイン名が追加されたことを確認し、[→] をクリックします。



Microsoft Azure Active Directory の活用

6. [(ドメイン名) の確認] 画面で、自己所有パブリック ドメインで使用する DNS サーバーに必要なレコードを確認し、自身が利用しているドメイン名レジストラーでこの DNS レコードを登録します。その後 チェックマークをクリックします。(DNS サーバー登録にはしばらく時間がかかる場合があります。)



7. [contoso corporation] 画面で、ドメイン名の確認を行います。(ドメイン名) を選択し、[確認] をクリックします。

8. [(ドメイン名) の確認] 画面で、[確認] をクリックします。



9. [(ドメイン名) の確認] 画面で、ドメイン名が正常に確認されたことを確認し、チェックマークをクリックします。



4.4 ユーザーの作成

Azure AD ドメイン内にユーザーを作成する手順について確認します。本手順では、全体管理者のロールが割り当てられる admin ユーザーと、一般ユーザーの aaduser1 ユーザーの 2 つのユーザーを作成します。

1. Microsoft Azure 管理ポータル画面で、[ACTIVE DIRECTORY] をクリックし、[Contoso corporation] をクリックします。

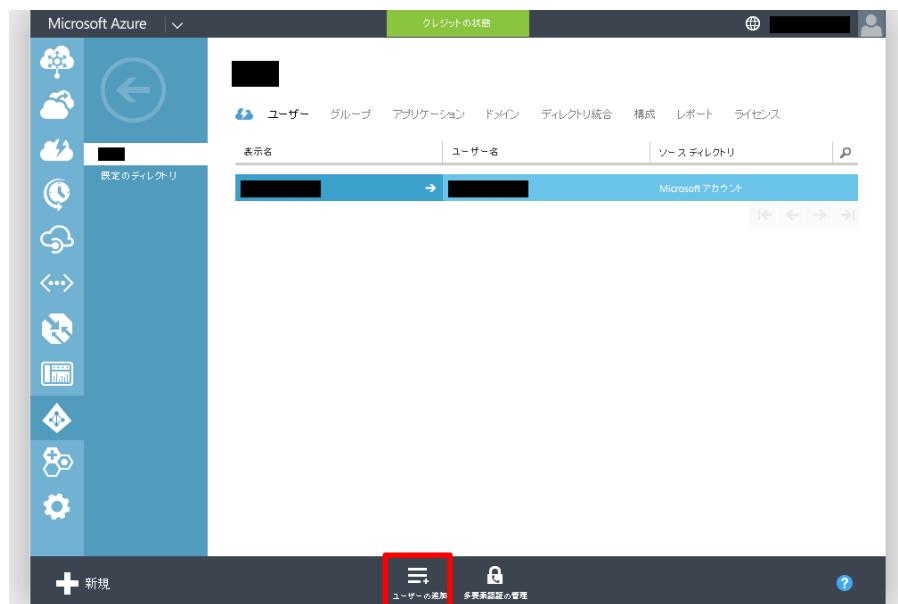
The screenshot shows the Microsoft Azure Management Portal interface. On the left, there's a sidebar with various service icons. The 'ACTIVE DIRECTORY' icon is highlighted with a red box. The main content area is titled 'active directory' and shows the 'Contoso Corp...' directory. The top navigation bar includes 'ACTIVE DIRECTORY', 'ACCESS CONTROL', '多要素認証プロバイダー', 'RIGHTS MANAGEMENT', and tabs for '名前', '状態', 'ロール', 'サブスクリプション', 'データセンターの地域', and '国/地域'. A red box highlights the 'Contoso Corp...' link in the top navigation.

2. [ディレクトリを使用する準備ができました。] 画面で、[ユーザー] をクリックします。

The screenshot shows the Microsoft Azure Management Portal interface. The sidebar now has a 'USER' icon highlighted with a red box. The main content area is titled 'contoso corporation' and features a large blue diamond graphic with the text 'ディレクトリを使用する準備ができました。' (Directory ready to use). Below it, there's a message: '作業開始するためのオプションは次のとおりです。' (Options for starting work are as follows) and a checkbox for '次回アクセス時はクイックスタートをスキップする' (Skip quick start on next access). At the bottom, there's a section titled '作業を開始する' (Start working) with a step 1: 'ユーザー サインイン エクスペリエンスの向上' (Improve user sign-in experience). A note below says: 'ユーザーが使ったユーザー名でサインインできるように、カスタムドメインを追加します。たとえば、純粋のドメインが "contoso.com" である場合、ユーザーは Azure AD に "joe@contoso.com" のようなユーザー名でサインインできます。' (A custom domain will be added so users can sign in with their chosen username. For example, if the pure domain is "contoso.com", users can sign in with "joe@contoso.com").

Microsoft Azure 自習書 No.18
Microsoft Azure Active Directory の活用

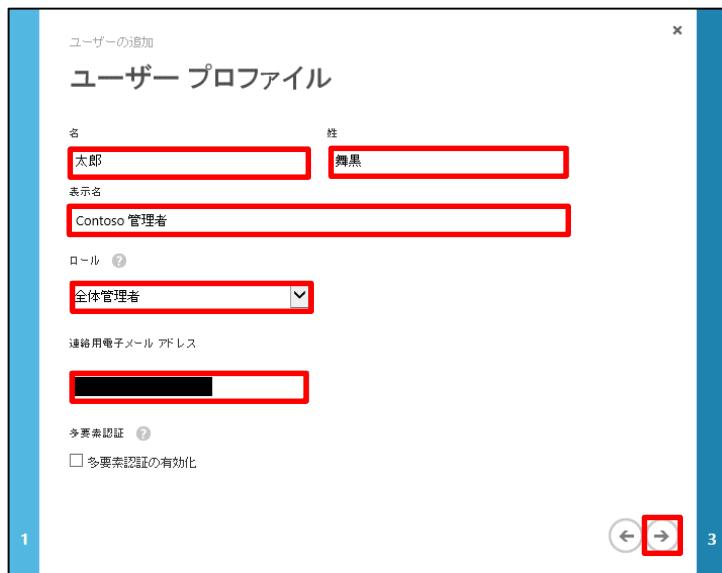
3. 画面下部の [ユーザーの追加] をクリックします。



4. [このユーザーに関する情報の入力] 画面で、[ユーザー名] に追加したいユーザー名 (@マーク前部分) を入力します。ここでは「admin」を入力し、[→] をクリックします。

The screenshot shows the 'Add user' input form. It has a title 'このユーザーに関する情報の入力' (Information about this user). There are two dropdown menus for 'ユーザーの種類' (User type) and '組織内の新しいユーザー' (New user in the organization). Below these is a 'ユーザー名' (User name) field containing 'admin'. To the right of the field is an '@' symbol followed by a dropdown menu with a red box around it. At the bottom right of the form is a large red-bordered '→' button, which is also highlighted with a red box. Below the form, there are page navigation numbers '2' and '3'.

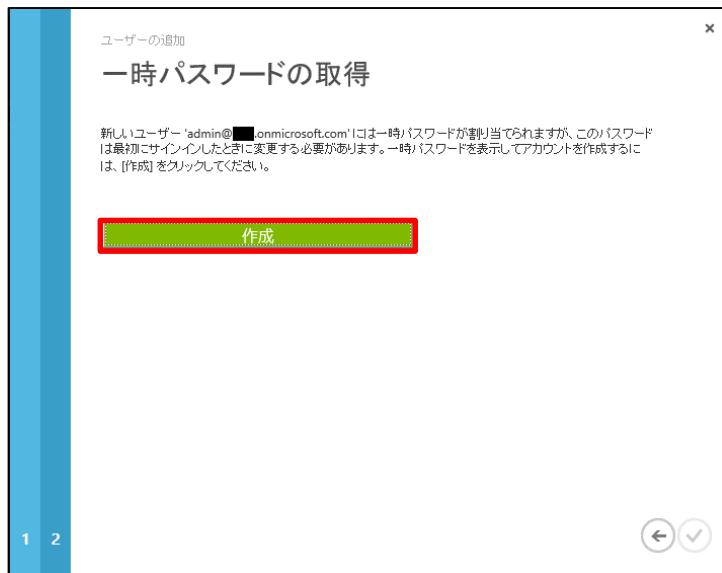
5. [ユーザー プロファイル] 画面で、ユーザーの情報 [名]、[姓]、[表示名] を入力します。[ロール] 欄で [全体管理者] を選択し、[連絡用電子メール アドレス] 欄に連絡先として使用するメールアドレスを入力します。入力が完了したら、[→] をクリックします。



【Note:】

Azure AD ユーザーに [ロール] を割り当てると、Azure AD に対する管理者権限を割り当てる ことができます。Azure AD ドメインに最初のユーザーを作成するときは必ず、すべての管理が 可能な [全体管理者] のロールを割り当ててください。

6. [一時パスワードの取得] 画面で、[作成] をクリックします。



7. [一時パスワードの取得] 画面で、[新しいパスワード] に初期パスワードが表示されます。このパスワードを控えておくか、もしくは右側のボタンをクリックすると [コピー済み] と表示されます。パスワードを確認できたら、チェック マークをクリックします。

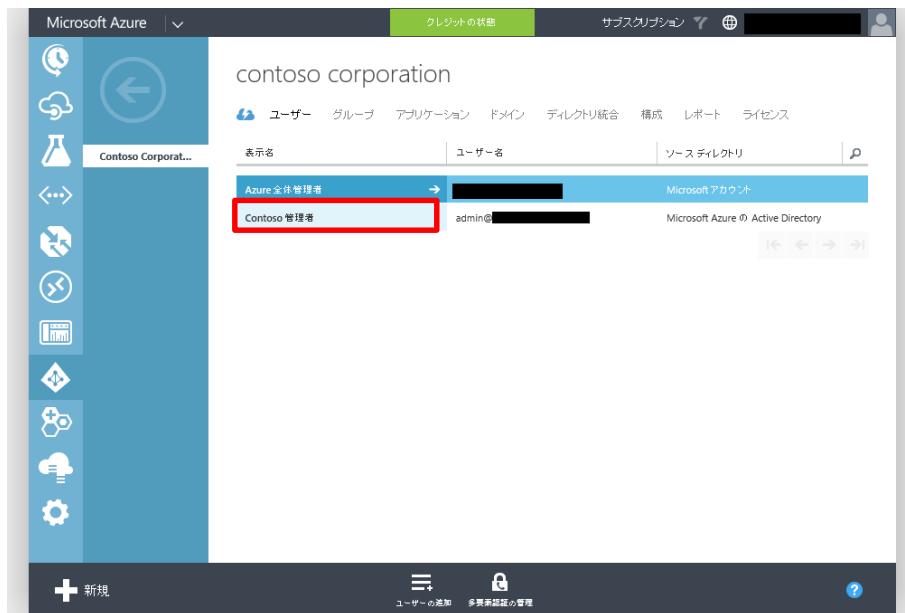


【Note:】

この手順で生成されるパスワードは一時パスワードであり、初めてサインインを行うタイミングで改めてパスワードを設定することになります。

Microsoft Azure Active Directory の活用

8. 新しいユーザーが作成されたことを確認した上で、新しいユーザーの名前をクリックします。



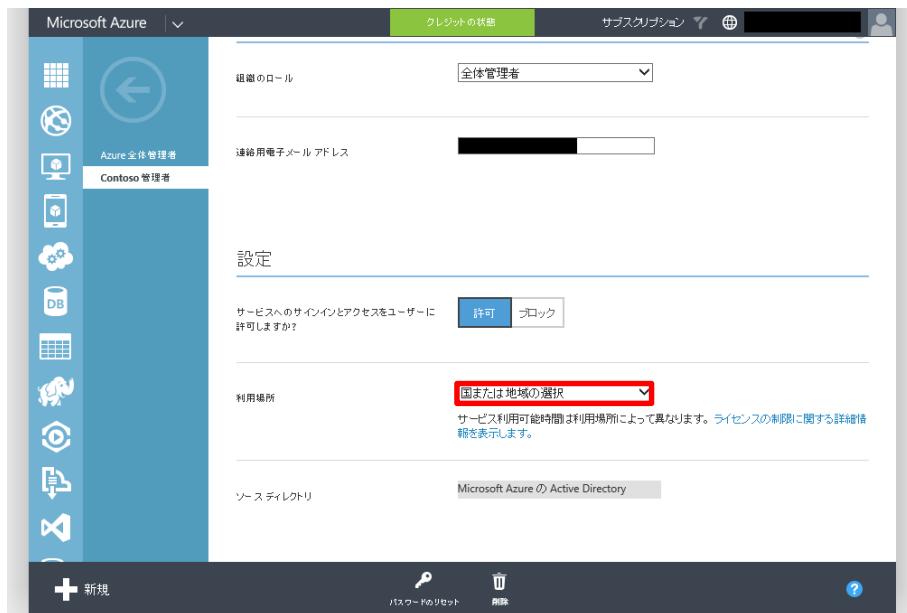
The screenshot shows the Microsoft Azure Active Directory user list. The left sidebar has icons for various services like Azure Active Directory, Storage, and App Service. The main area is titled 'contoso corporation'. It shows a table with columns: 表示名 (Display Name), ユーザー名 (User Name), and ソースディレクトリ (Source Directory). One row is selected, showing 'Contoso 管理者' in the first column and 'admin@[REDACTED]' in the second. The third column shows 'Microsoft アカウント' and 'Microsoft Azure の Active Directory'. A red box highlights the 'Contoso 管理者' entry.

9. 新しく作成したユーザーのプロファイルを確認することができます。画面を下にスクロールします。

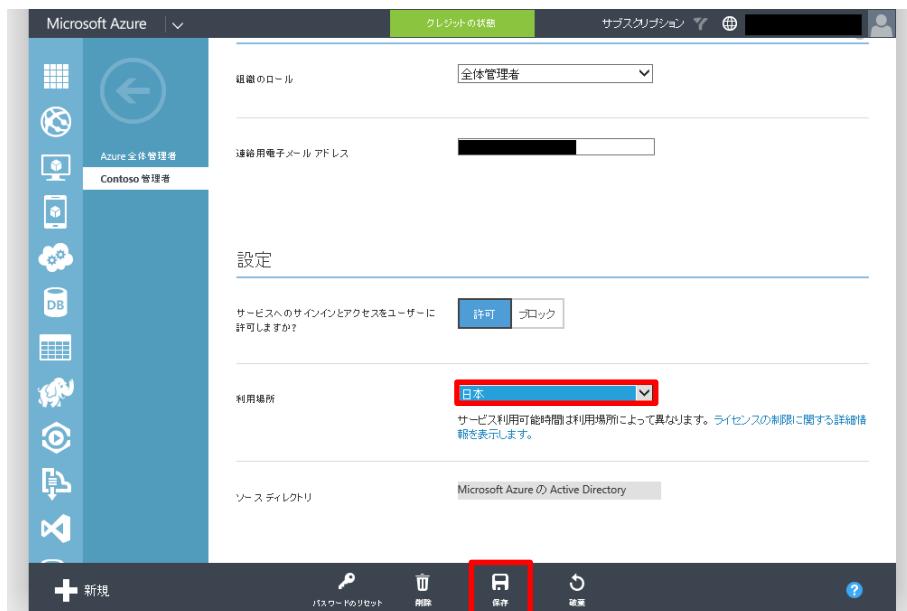


The screenshot shows the Microsoft Azure Active Directory user profile for 'Contoso 管理者'. The left sidebar has icons for various services. The main area is titled 'contoso 管理者'. It shows a form with fields: id (filled with 'id'), 名 (filled with '太郎'), 性 (filled with '男'), 表示名 (filled with 'Contoso 管理者'), and ユーザー名 (filled with 'admin@[REDACTED] @ [REDACTED]'). At the bottom, there are buttons for '新規' (New), 'パスワードのリセット' (Password Reset), and '削除' (Delete). A blue question mark icon is also present.

10. [利用場所] 欄の [国または地域の選択] をクリックします。

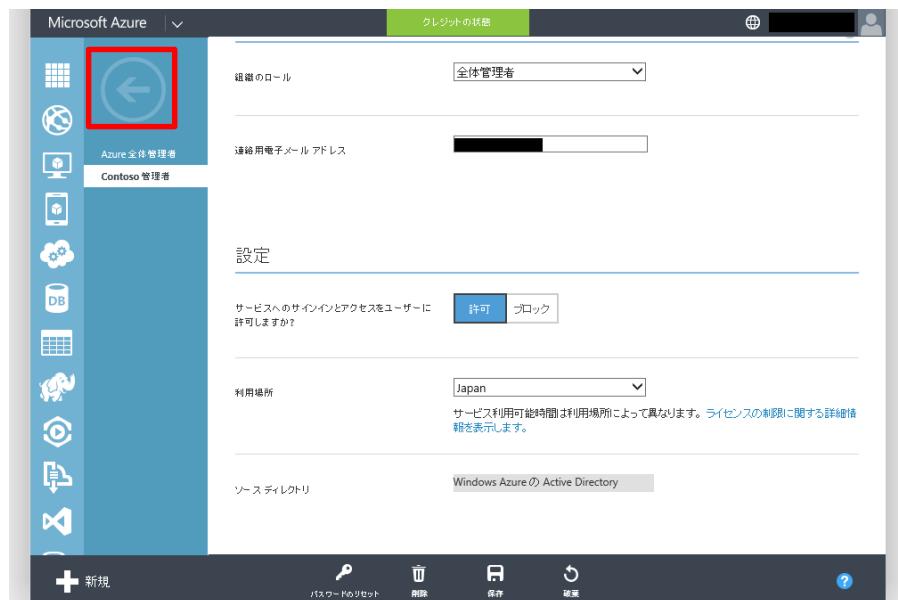


11. [日本] を選択し、[保存] をクリックします。



12. 左ペインの [戻る] ボタンをクリックします。

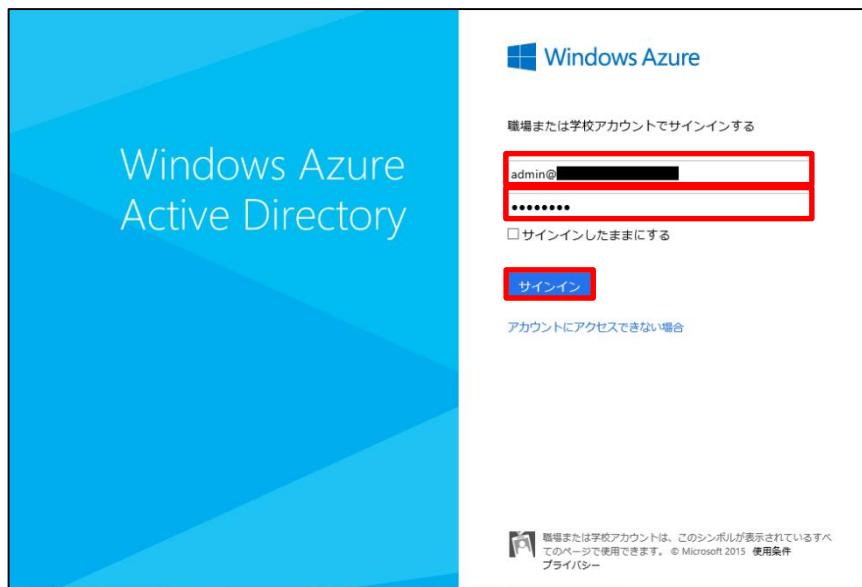
(画面は閉じないでください)



13. InPrivate ブラウズで Internet Explorer を起動し、アクセス パネルの URL である

<http://myapps.microsoft.com/> にアクセスします。

admin@<Microsoft Azure に登録されたドメイン名>ユーザーでサインインします。



【Note:】

アクセス パネル Web ページは Azure AD ユーザーのために用意されたポータル サイトです。ここでは、初めてのサインインを行い、初期パスワードからパスワードを変更することを目的としてアクセスします。

14. [パスワードの変更] 画面で、[古いパスワード] 欄に一時パスワード、[新しいパスワード] と [新しいパスワードの確認入力] 画面に新しいパスワードをそれぞれ入力し、[送信] をクリックします。



15. サインイン画面に戻ったら、InPrivate ブラウズ画面を終了します。



16. 手順 12 の画面に戻ります。Azure AD ドメインのユーザー一覧画面で新しく、もうひとりのユーザーを作成するため、[ユーザーの追加] をクリックします。

The screenshot shows the Microsoft Azure Active Directory user list interface. The left sidebar contains various icons for different services. The main area displays a list of users under the 'Contoso Corporation' tenant. At the bottom of the page, there is a dark footer bar with several buttons. The 'Add User' button, which is white with a blue outline and has a plus sign icon, is highlighted with a red box.

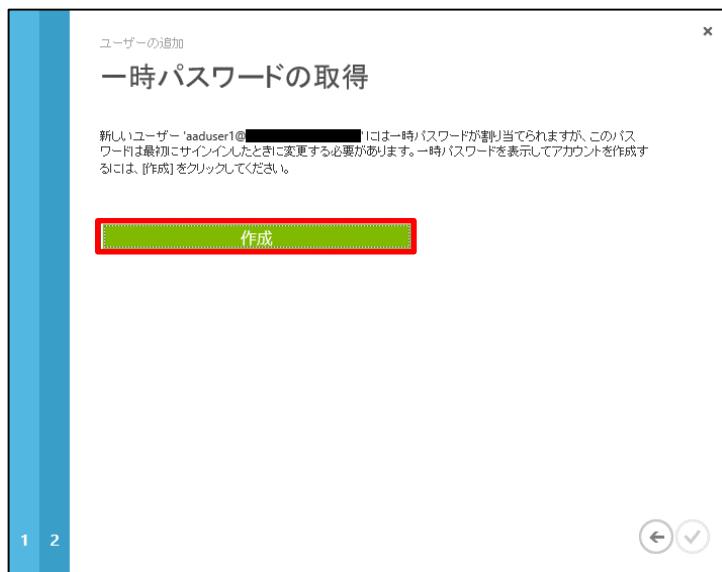
17. [このユーザーに関する情報の入力] 画面で、[ユーザー名] に追加したいユーザー名 (@マーク前部分) を入力します。ここでは「aaduser1」と入力し、[→] をクリックします。

The screenshot shows the 'User Add' input form. It has a title 'このユーザーに関する情報の入力'. Under 'User Type', it says '組織内の新しいユーザー'. The 'User Name' field contains 'aaduser1' followed by an '@' symbol. In the bottom right corner, there is a 'Next Step' button with a right-pointing arrow, which is highlighted with a red box.

18. [ユーザー プロファイル] 画面で、[表示名] に「aaduser1」と入力して、[→] をクリックします。



19. [一時パスワードの取得] 画面で、[作成] をクリックします。



Microsoft Azure Active Directory の活用

20. [一時パスワードの取得] 画面で、[新しいパスワード] に初期パスワードが表示されます。このパスワードを控えておくか、もしくは右側のボタンをクリックすると [コピー済み] と表されます。パスワードを確認できたら、チェックマークをクリックします。



【Note:】

この手順で生成されるパスワードは一時パスワードであり、初めてサインインを行うタイミングで改めてパスワードを設定することになります。

21. 新しいユーザーが作成されたことを確認した上で、新しいユーザーの名前をクリックします。

22. ユーザーのプロファイル画面で、画面を下にスクロールし、[利用場所] 欄として

[日本] を選択して、[保存] をクリックします。

**23. 左ペインの [戻る] ボタンをクリックします。**

24. Azure AD ドメインのユーザー一覧画面に戻ります。

The screenshot shows the Microsoft Azure Active Directory User list interface. On the left, there's a sidebar with various icons for managing resources like users, groups, applications, domains, and more. The main area displays a table of users:

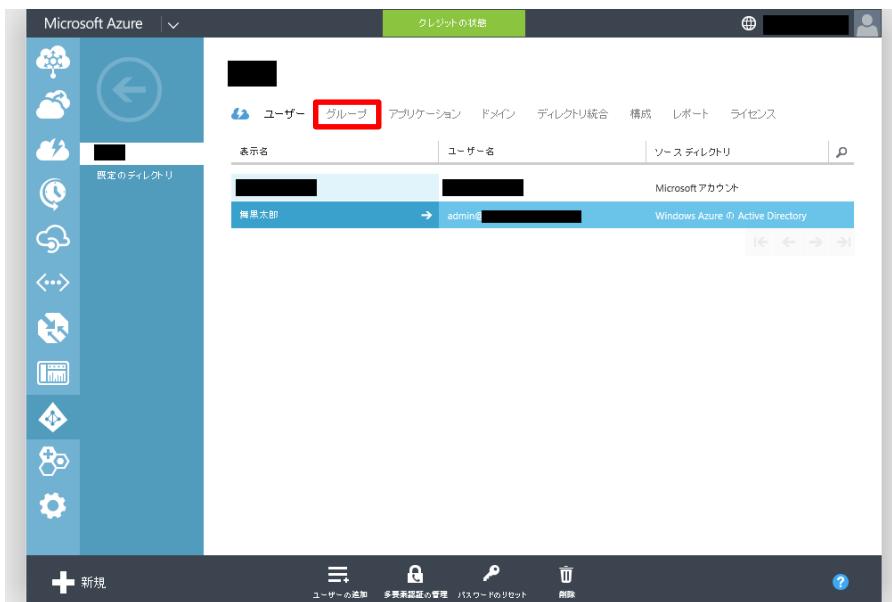
表示名	ユーザー名	ソースディレクトリ
AADUser1	AADUser1@████████.onmicrosoft.com	Windows Azure の Active Directory
████████	████████@████████.onmicrosoft.com	Microsoft アカウント
舞黒太郎	admin@████████.onmicrosoft.com	Windows Azure の Active Directory

At the bottom of the interface, there are buttons for '新規' (New), 'ユーザーの追加' (Add user), '多要素認証の管理' (Manage multi-factor authentication), 'パスワードクリエット' (Create password), and '削除' (Delete). There are also navigation arrows at the bottom right.

4.5 グループの作成

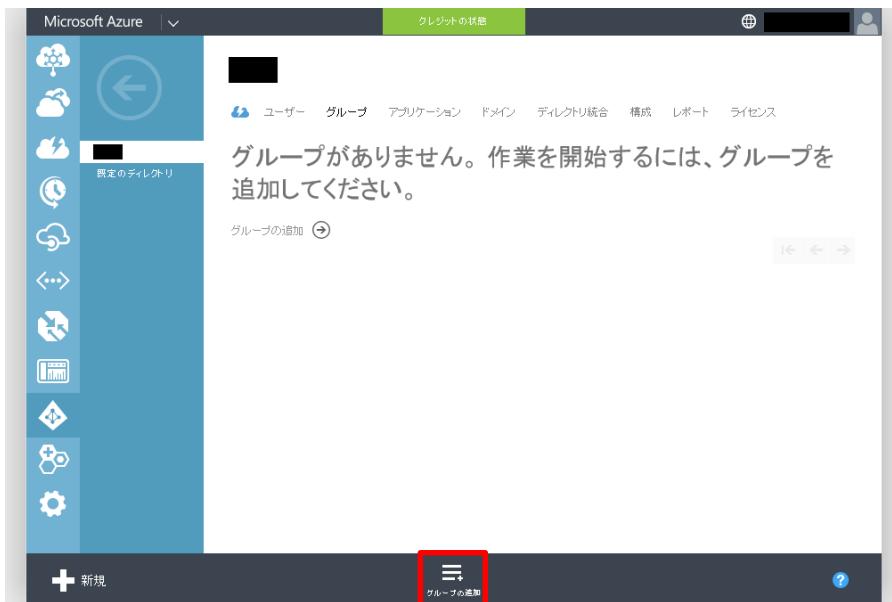
Azure AD ドメインで作成したグループは Azure AD Premium の機能の中でアクセス許可を割り当てる単位として活用できます。本手順では、管理者が含まれるグループとして、admins という名前のグループを作成する手順について確認します。

1. Azure AD ドメイン画面で、[グループ] をクリックします。



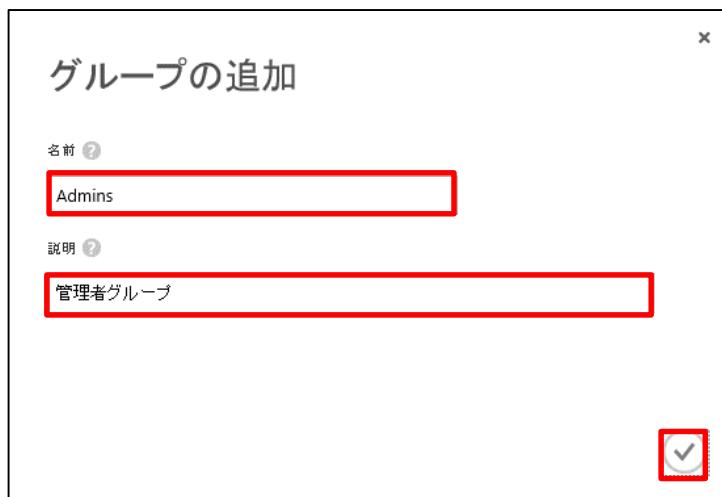
The screenshot shows the Microsoft Azure Active Directory Groups page. The 'Groups' tab is highlighted with a red box. The main area displays a table with columns for '表示名' (Display Name), 'ユーザー名' (User Name), and 'ソースディレクトリ' (Source Directory). One row is visible, showing '高橋太郎' and 'admin' under 'Microsoft Account'. Below the table, there's a note about 'Windows Azure Active Directory'. At the bottom, there are buttons for '新規' (New) and other management options.

2. Azure AD ドメイン画面で、[グループの追加] をクリックします。



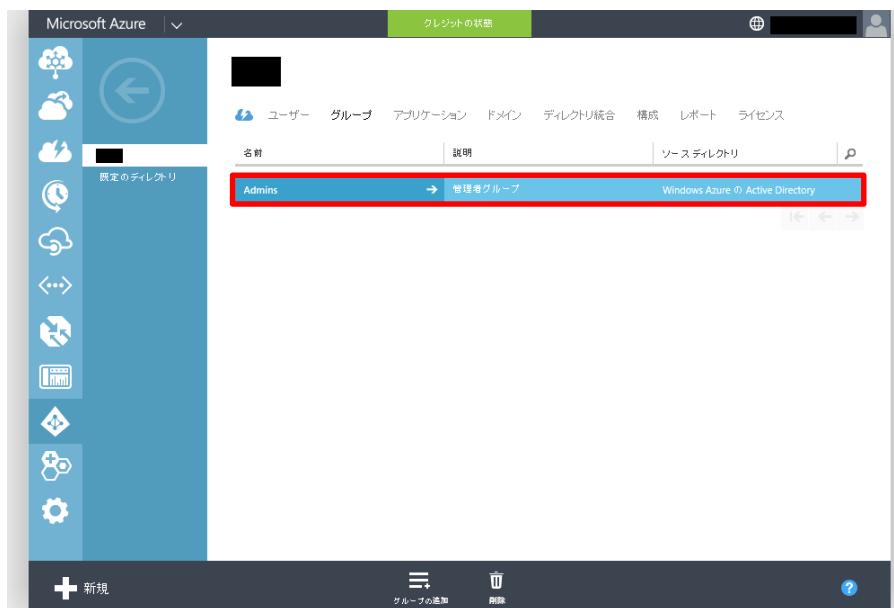
The screenshot shows the Microsoft Azure Active Directory Groups page. The 'Groups' tab is selected. A message in the center says 'グループがありません。作業を開始するには、グループを追加してください。' (There are no groups. To get started, add a group.). Below this, a list of groups is shown, including '高橋太郎'. At the bottom, there is a large red box highlighting the 'Groups' button, which has a plus sign icon and the text 'グループの追加' (Add Group).

3. [グループの追加] 画面で、グループの [名前]、[説明] を入力し、チェック マークをクリックします。



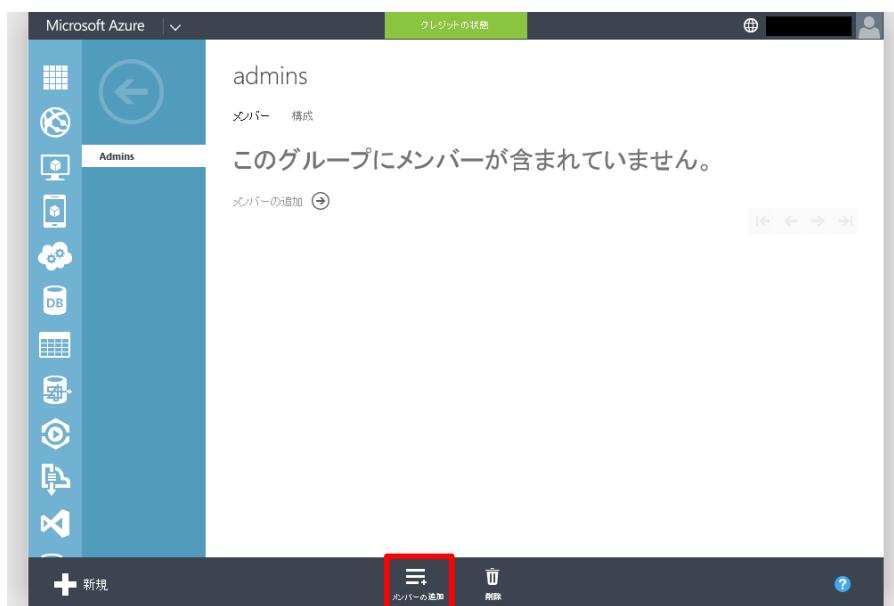
4. Azure AD ドメイン画面で、グループが作成されたことを確認します。

5. Azure AD ドメイン画面で、前の手順で作成したグループをクリックします。



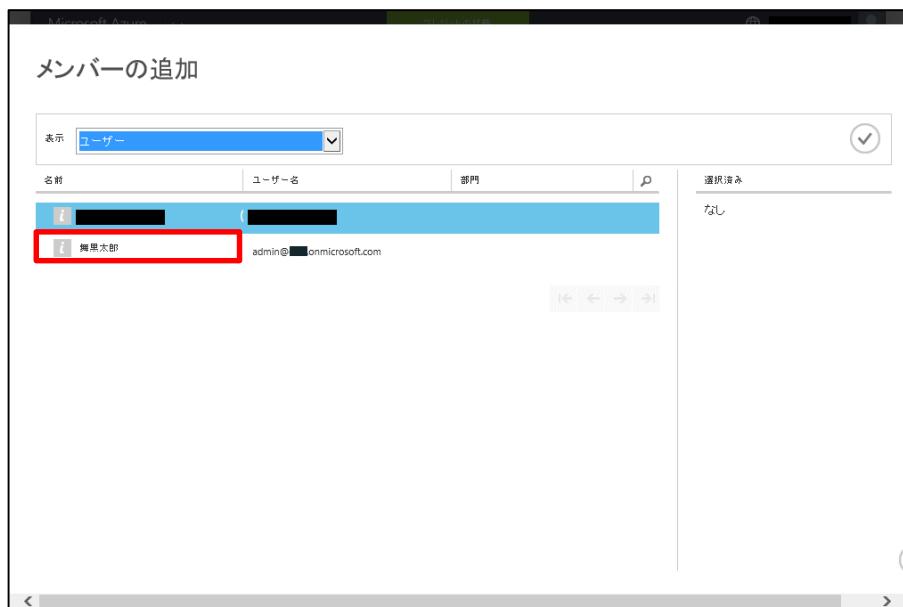
The screenshot shows the Microsoft Azure Active Directory Groups page. On the left, there's a sidebar with various icons. In the center, a table lists groups. One group, 'admins', is selected and highlighted with a red box. The table columns are '名前' (Name), '説明' (Description), and 'ソース ディレクトリ' (Source Directory). The status bar at the bottom right indicates 'Windows Azure の Active Directory'.

6. グループの画面で、[メンバーの追加] をクリックします。

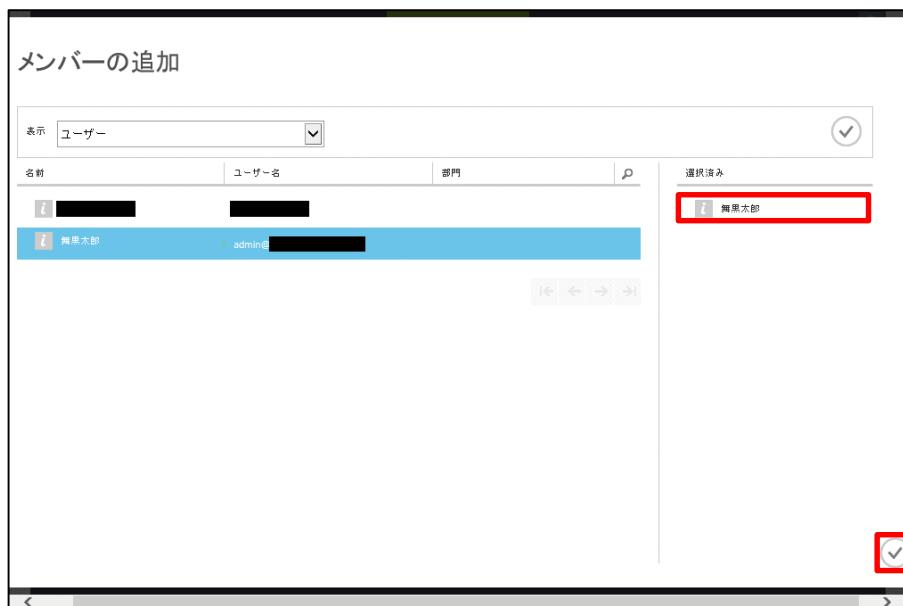


The screenshot shows the Microsoft Azure Active Directory Group 'admins' page. The sidebar on the left shows the group 'admins' is selected. The main area displays the message 'このグループにメンバーが含まれていません。' (No members are included in this group.) and a 'メンバーの追加' (Add member) button. The 'メンバーの追加' button is highlighted with a red box at the bottom.

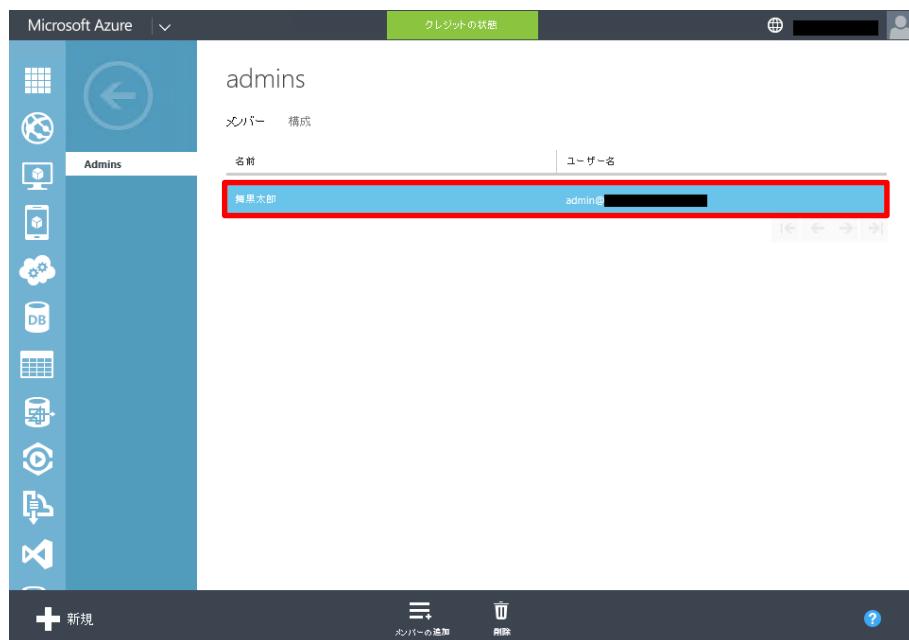
7. [メンバーの追加] 画面で、グループに追加するメンバーとして、前の手順で作成した Admin ユーザーをクリックします。



8. 右ペインの [選択済み] で、追加したいメンバーが選択されていることを確認し、チェック マークをクリックします。



9. グループの画面で、グループに追加したメンバーの情報が表示されることを確認します。



The screenshot shows the Microsoft Azure Active Directory Groups page. On the left, there's a sidebar with various icons for different services like Storage, Network, and Compute. The main area shows a group named 'admins'. Below it, there are two tabs: 'メンバー' (Members) and '構成' (Configuration). Under the 'メンバー' tab, there's a table with columns '名前' (Name) and 'ユーザー名' (User Name). A row is selected, highlighted with a red box, showing '舞黒太郎' (Makino Tarou) and 'admin@...' (User name partially obscured). At the bottom of the table, there are buttons for 'メンバーの追加' (Add member) and '削除' (Delete). The bottom navigation bar includes a '新規' (New) button, a help icon, and a question mark icon.

4.6 ディレクトリ同期による Active Directory ドメインとのユーザー/グループ同期

Azure AD ドメインに登録するユーザーやグループは直接作成する方法以外にも、オンプレミスの Active Directory ドメインに登録されているユーザーやグループを同期することで、Azure AD に登録することができます。

ディレクトリ同期ツールには、Microsoft Azure Active Directory Sync (AADSync) と DirSync の 2 種類があります。どちらも本書で解説する機能を評価する上で必要なユーザーとグループの作成を同期で行なうことができますが、「6.4 デバイスの登録」の節で解説する機能を評価する場合は必ず DirSync ツールを実装してください。

本手順では、AADSync によるディレクトリ同期ツールの実装方法と DirSync によるディレクトリ同期ツールの実装方法をそれぞれ解説するため、「6.4 デバイスの登録」の評価を行う方は DirSync ツール、それ以外の方は AADSync によるディレクトリ同期ツールの実装手順を実行してください。

【Note:】

AADSync は GUI による豊富なメニューで DirSync に比べて操作しやすいことが特徴です。そのため、「6.4 デバイスの登録」の実装を行わない場合は AADSync をお使いいただくことをお勧めします。

【Note:】

マイクロソフトでは AAD Connect と呼ばれるツールを提供しており（本書執筆時点ではベータ版）、シングルサインオン環境やディレクトリ同期ツールなどの実装をウィザード形式で行なうことができます。AAD Connect ツールを実装することにより、AADSync のインストールも同時に行われます。

➡ AADSync によるディレクトリ同期の実装

1. Microsoft Azure 管理ポータル画面で、[ACTIVE DIRECTORY] をクリックし、[Contoso corporation] をクリックします。

The screenshot shows the Microsoft Azure Management Portal. On the left sidebar, the 'ACTIVE DIRECTORY' icon is highlighted with a red box. The main content area is titled 'active directory' and shows a table for 'Contoso Corp...'. The table has columns for '名前' (Name), '状態' (Status), 'ロール' (Role), 'サブスクリプション' (Subscription), 'データセンターの地域' (Region), and '国/地域' (Country/Region). A row for 'Contoso Corp...' is selected, indicated by a red box around the status column. The status is 'アクティブ' (Active). Other columns show '全登録者' (All registrants) and 'すべての Contoso C...' (All Contoso C...).

2. [Contoso corporation] 画面で、[ディレクトリ統合] をクリックします。

The screenshot shows the 'contoso corporation' blade in the Microsoft Azure Active Directory service. The top navigation bar includes 'ユーザー' (User), 'グループ' (Group), 'アプリケーション' (Application), 'ドメイン' (Domain), and 'ディレクトリ統合' (Directory Integration), which is highlighted with a red box. Below the navigation, there's a large blue diamond icon with three white circles connected by lines. Text inside the diamond says 'ディレクトリを使用する準備ができました。作業開始するためのオプションは次のとおりです。' (Directory preparation is complete. Options for starting work are as follows.) There's also a checkbox for '次回アクセス時はクイックスタートをスキップする' (Skip quick start next time I access). At the bottom, there are tabs for '行う操作' (Actions to take), 'ディレクトリのセットアップ' (Directory setup), 'アクセスの管理' (Access management), and 'アプリケーションの削除' (Delete application). A green progress bar at the bottom indicates the task 'ユーザー サインイン エクスペリエンスの向上' (User sign-in experience improvement) is 100% complete.

Microsoft Azure Active Directory の活用

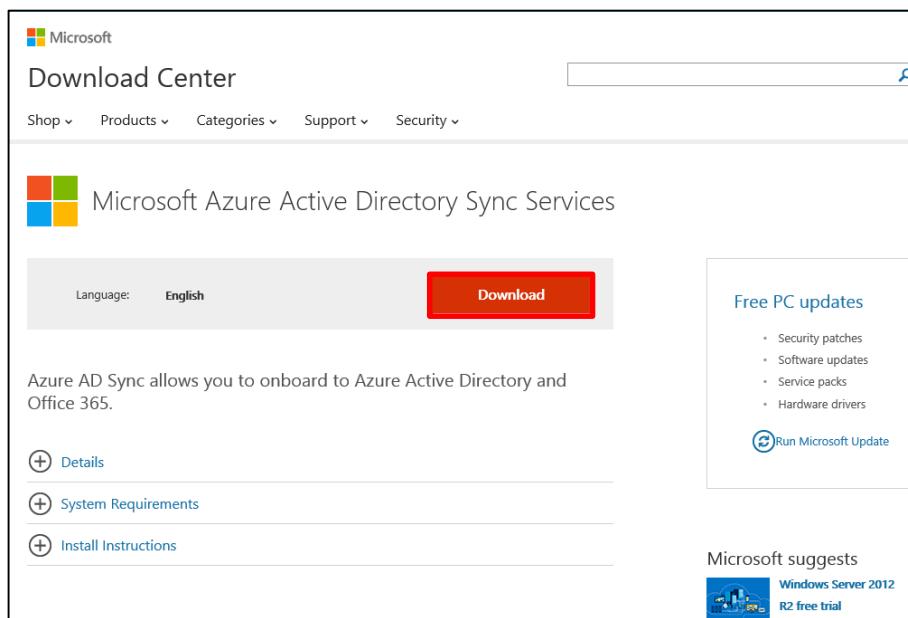
3. [ディレクトリ統合] 画面で、[ローカルとの統合 active directory] - [ディレクトリ同期] の[アクティブ化済み] をクリックします。

4. [ディレクトリ統合] 画面で、[アクティブ化済み] となったことを確認し、[保存] をクリックします。

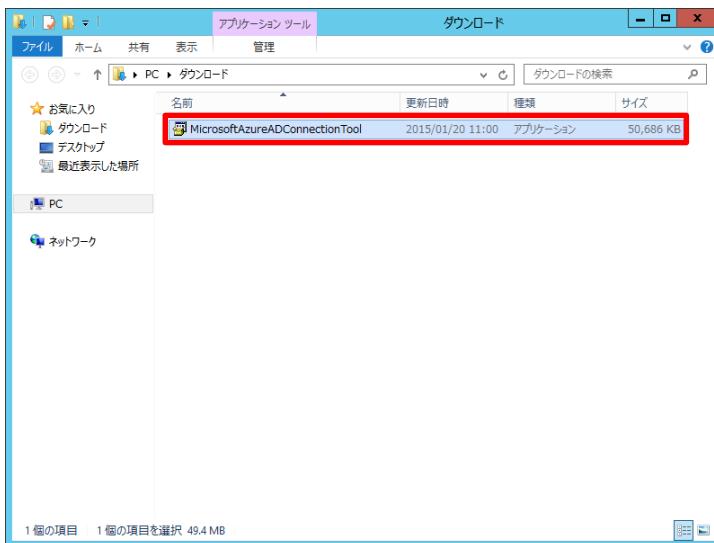
5. [ディレクトリ同期をアクティブ化しますか?] 画面で、[はい] をクリックします。

6. WS2012-DC01 コンピューターで操作します。

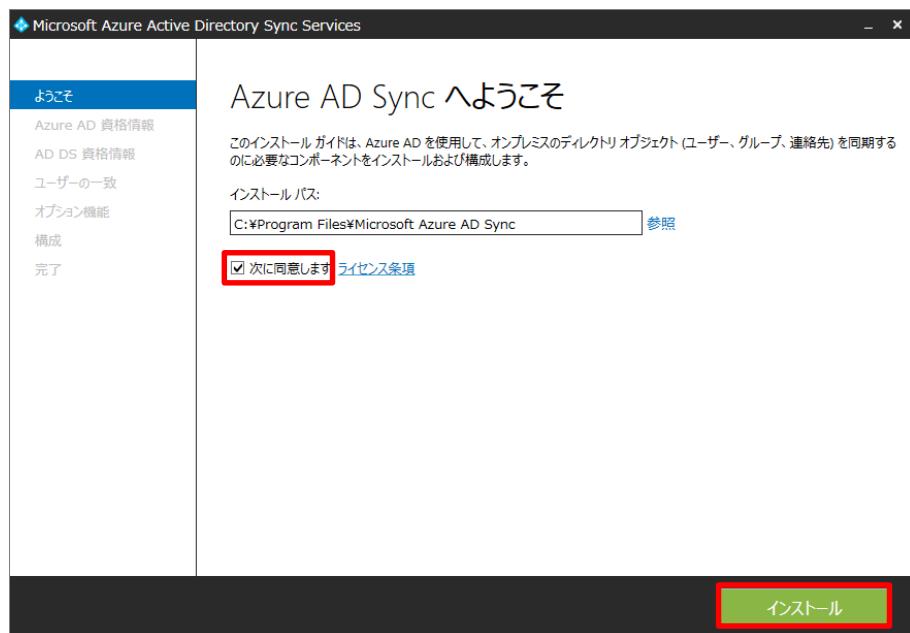
Internet Explorer を起動し、Microsoft Download Center にアクセスします。[Microsoft Azure Active Directory Sync Services] をダウンロードします。



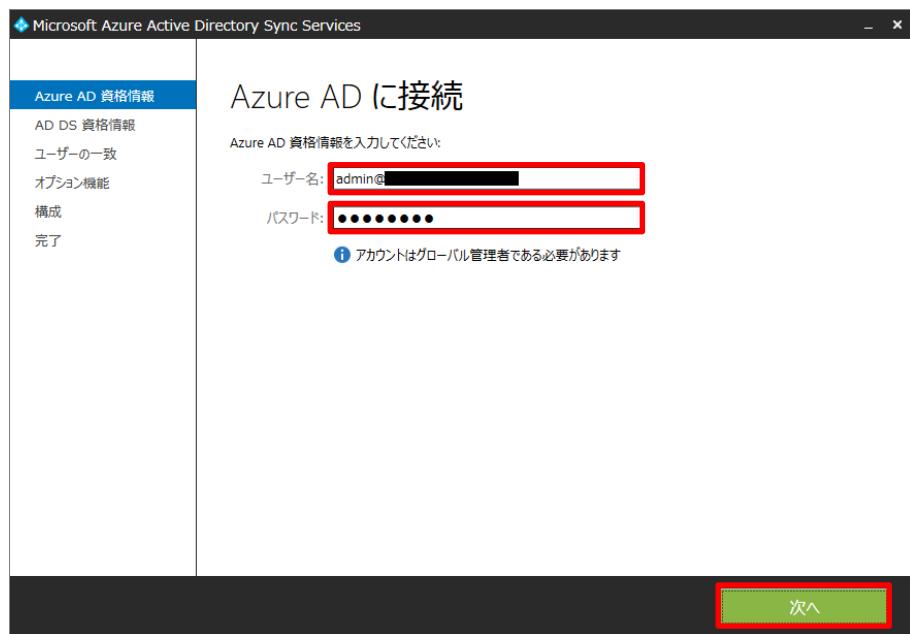
7. Microsoft Azure Active Directory Sync Services をダウンロードした後、
[MicrosoftAzureADConnectionTool] をダブルクリックして実行します。



8. [Azure AD Sync へようこそ] 画面で、[インストール パス] を確認し、[次に同意します] にチェックを入れ、[インストール] をクリックします。

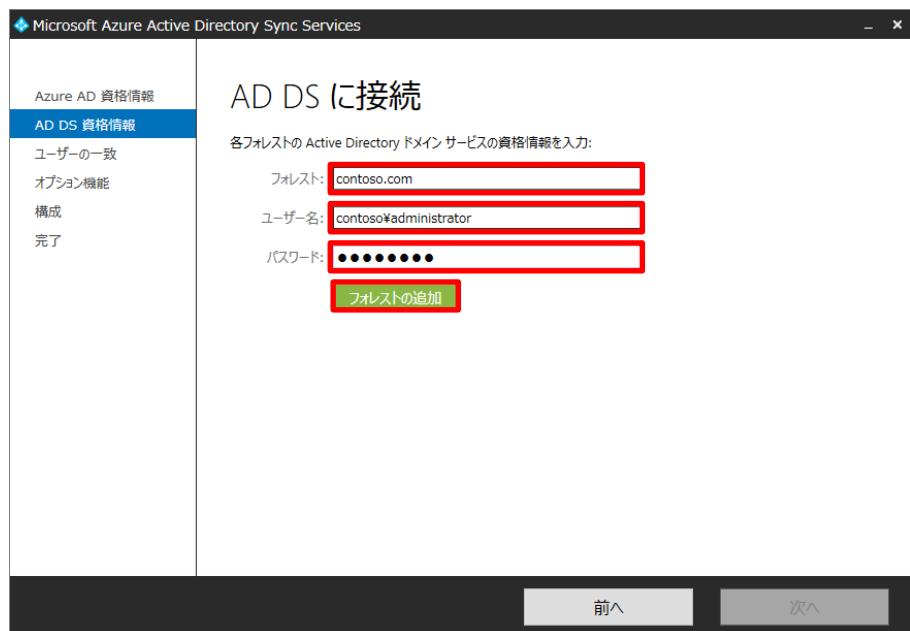


9. [Azure AD に接続] 画面で、[ユーザー名]、[パスワード] は Azure AD に登録を行った全体管理者 (admin ユーザー) のユーザー名とパスワードを入力し、[次へ] をクリックします。

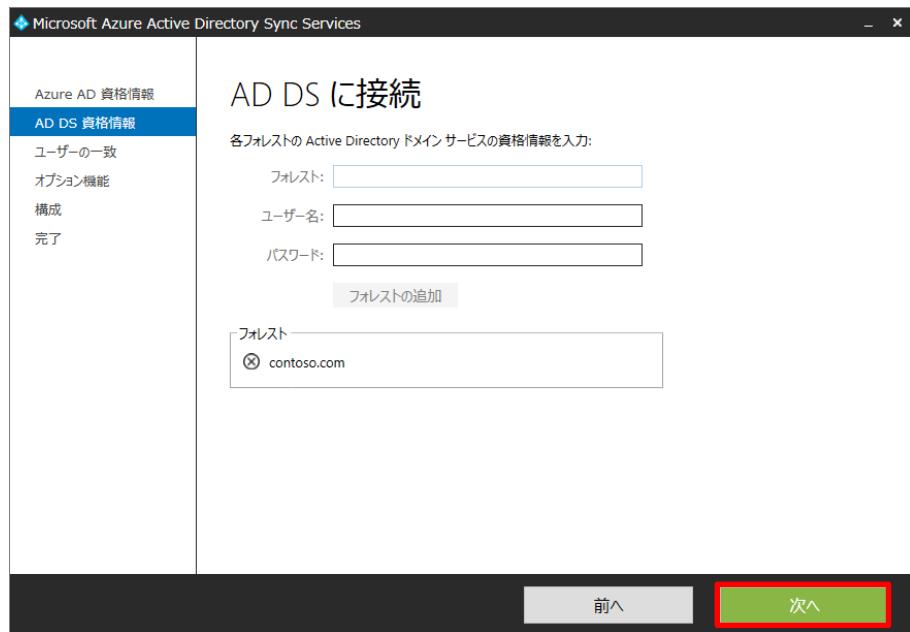


Microsoft Azure Active Directory の活用

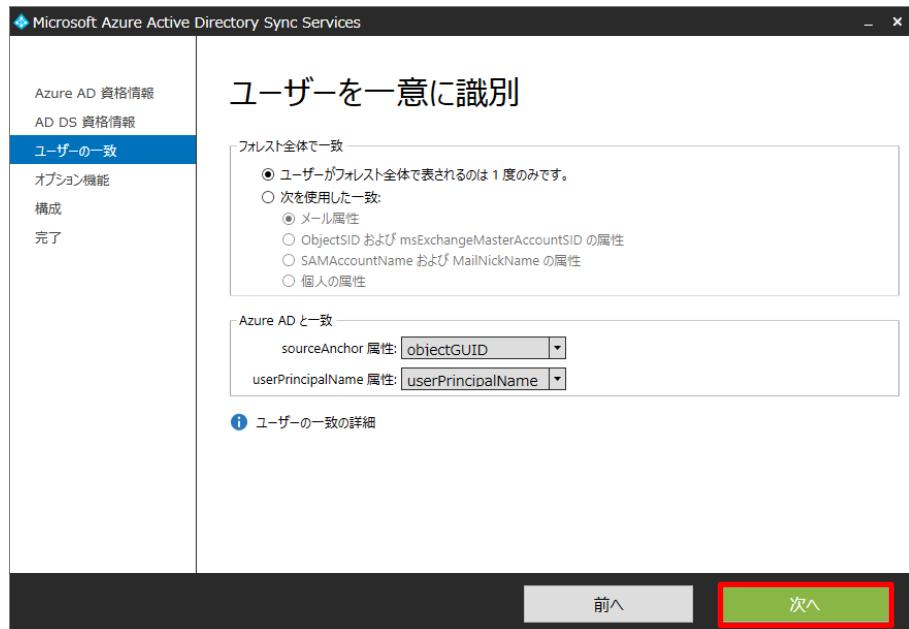
10. [AD DS に接続] 画面で、[フォレスト] にオンプレミス Active Directory のドメイン名、[ユーザー名] と [パスワード] にはオンプレミス Active Directory ドメインの管理者ユーザー名とパスワードをそれぞれ入力し、[フォレストの追加] をクリックします。



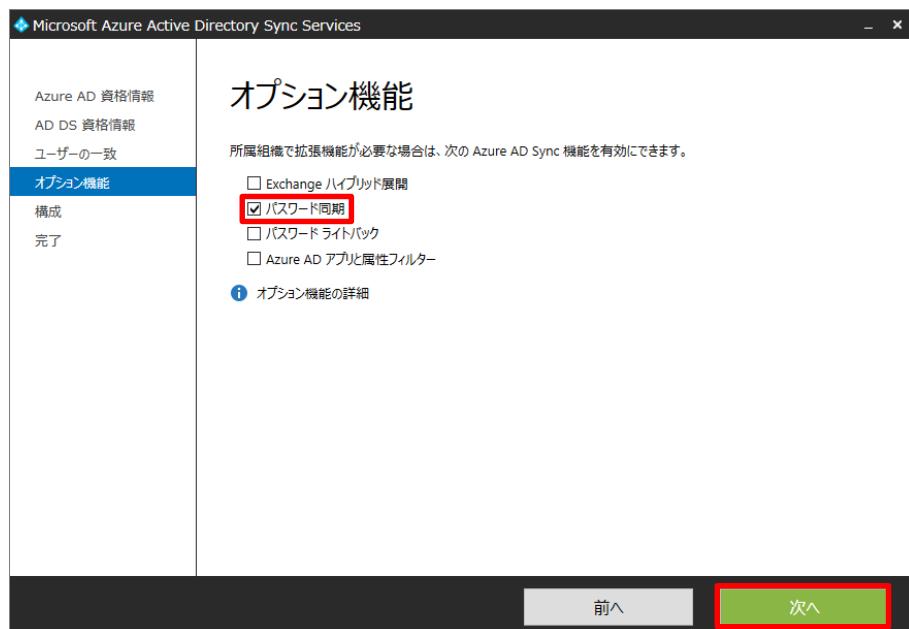
11. [AD DS に接続] 画面で、フォレストが追加されたことを確認し、[次へ] をクリックします。



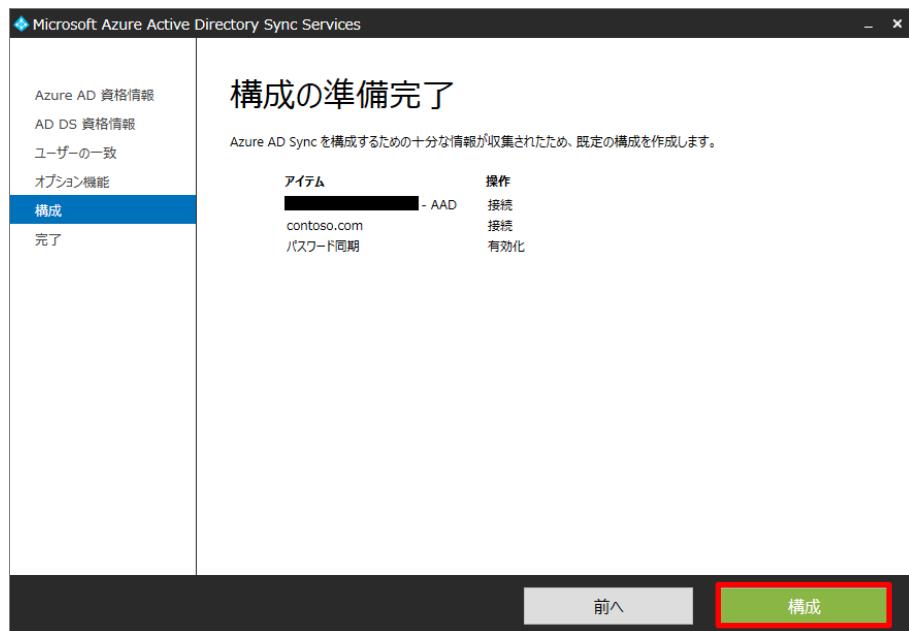
12. [ユーザーを一意に識別] 画面で、[次へ] をクリックします。



13. [オプション機能] 画面で、[パスワード同期] にチェックをし、[次へ] をクリックします。



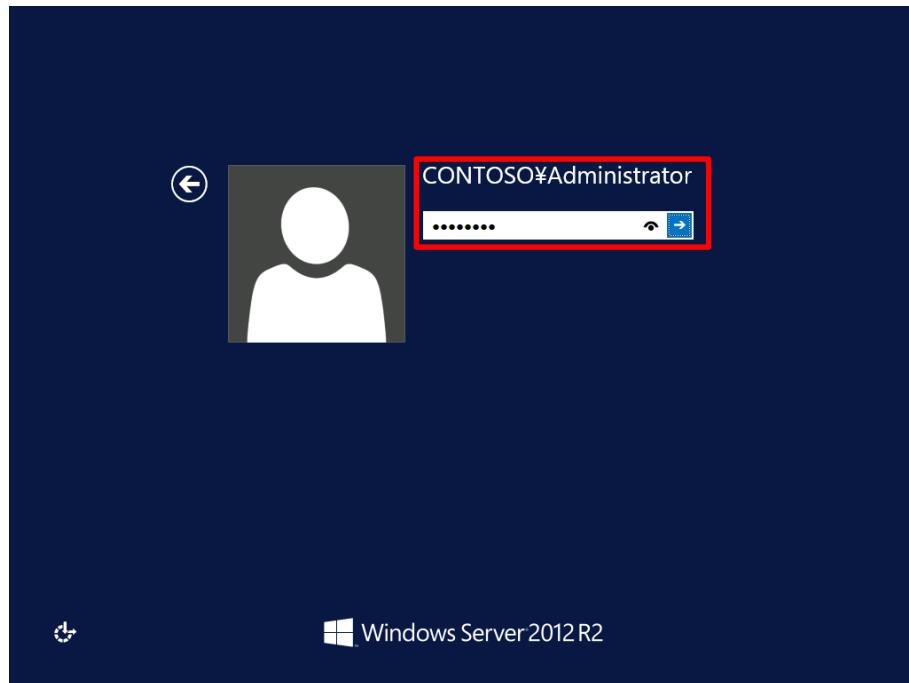
14. [構成の準備完了] 画面で、[構成] をクリックします。



15. [完了] 画面で、[今すぐ同期] のチェックを外し、[完了] をクリックします。



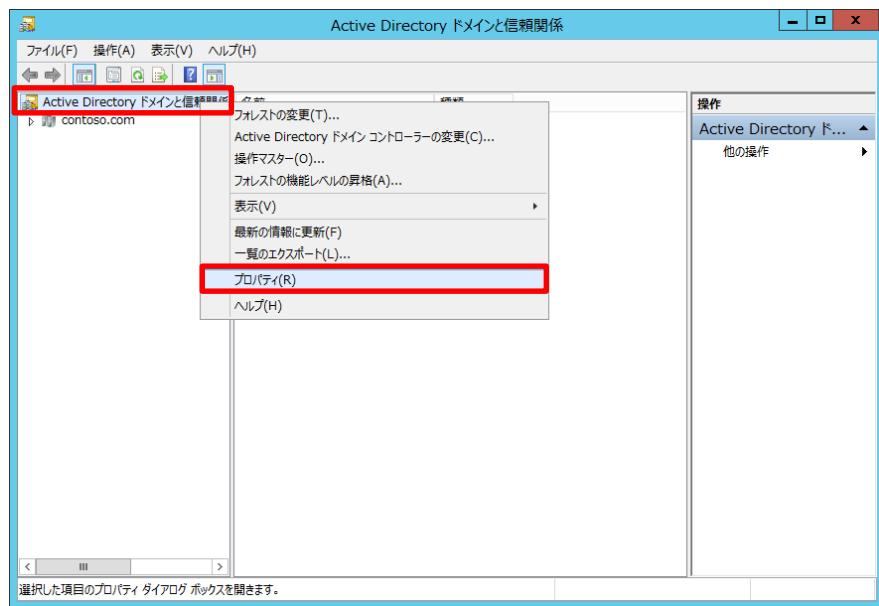
16. WS2012-DC01 コンピューターでサインアウトし、Administrator ユーザーでサインインしなおします。



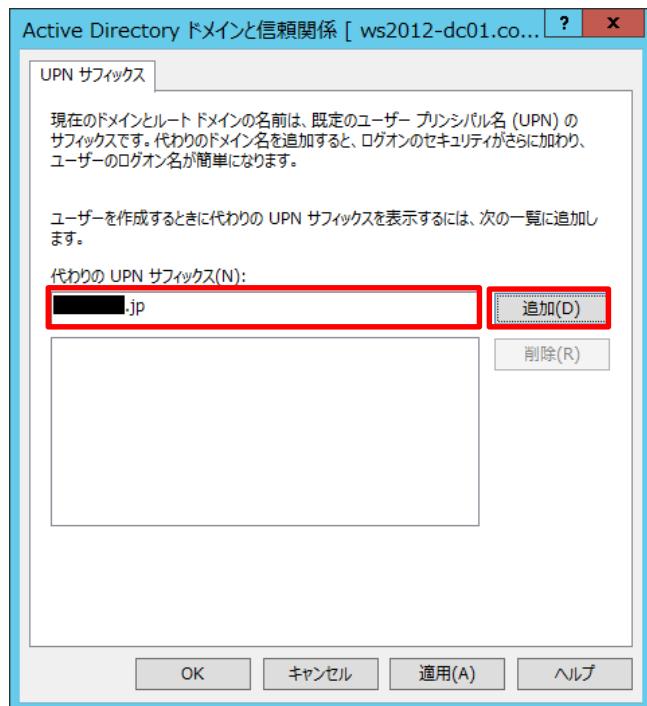
17. [サーバー マネージャー] 画面で、[ツール] - [Active Directory ドメインと信頼関係] をクリックします。



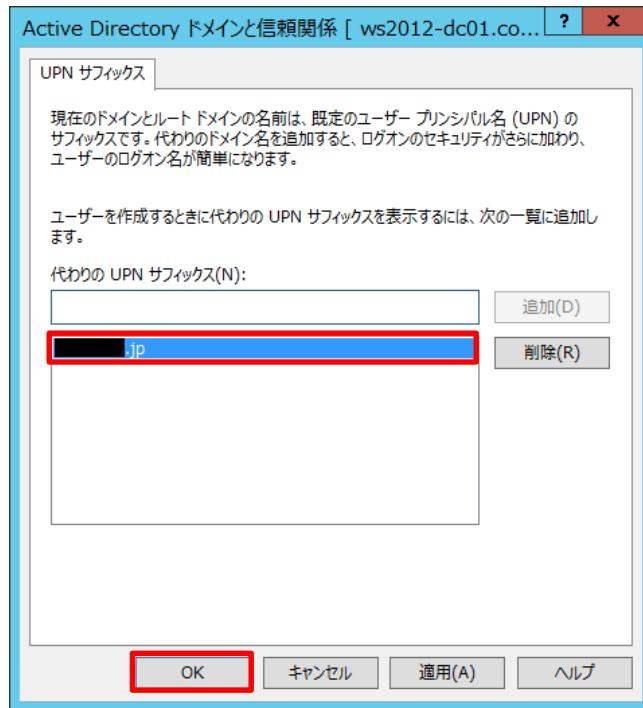
18. [Active Directory ドメインと信頼関係] 画面で、[Active Directory ドメインと信頼関係]を右クリックし、[プロパティ] をクリックします。



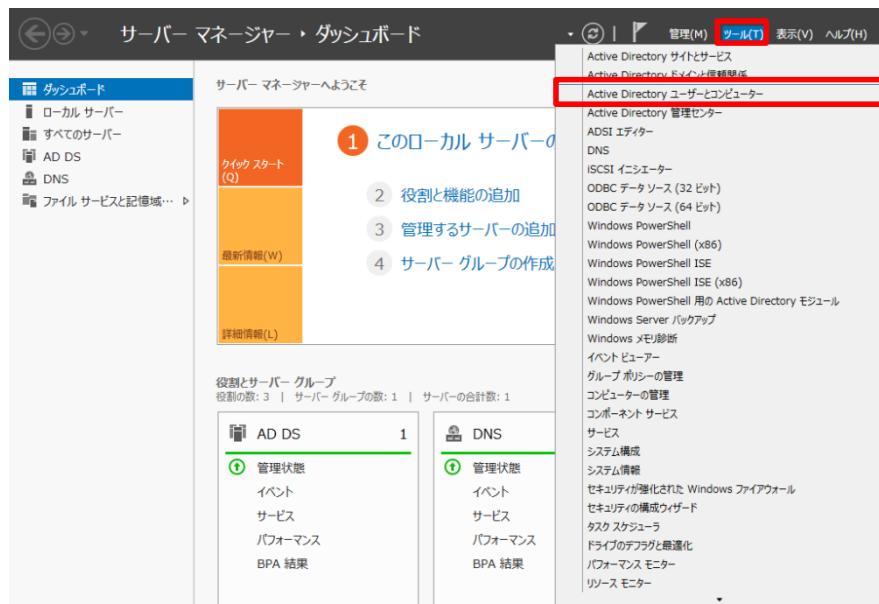
19. [Active Directory ドメインと信頼関係] 画面で、[代わりの UPN サフィックス] に Azure AD で使用している自己所有パブリック ドメイン名を入力し、[追加] をクリックします。



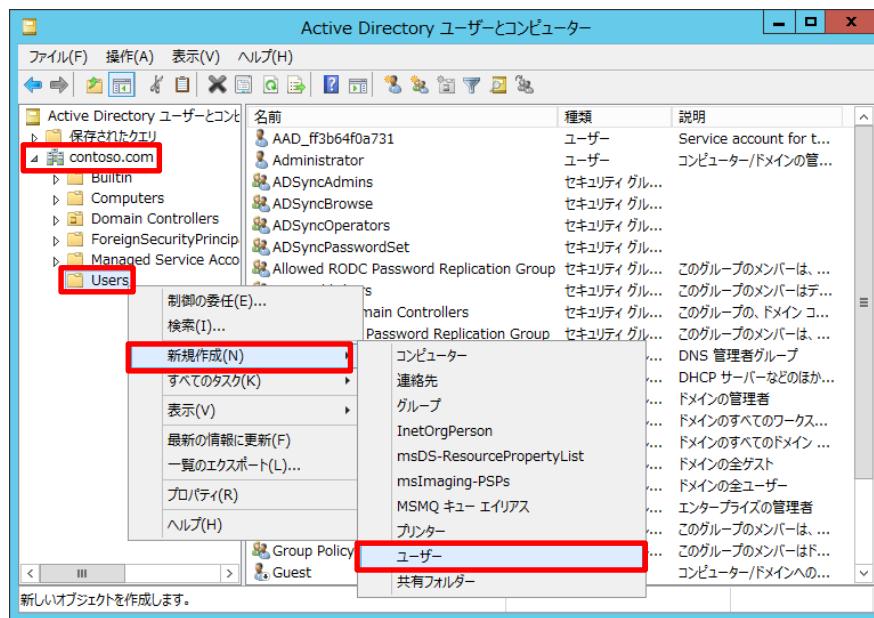
20. [Active Directory ドメインと信頼関係] 画面で、追加されたことを確認し [OK] をクリックします。



21. [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。



22. [Active Directory ユーザーとコンピューター] 画面で、[Active Directory ユーザーとコンピューター] - [contoso.com] から [Users] を右クリックし、[新規作成] - [ユーザー] をクリックします。



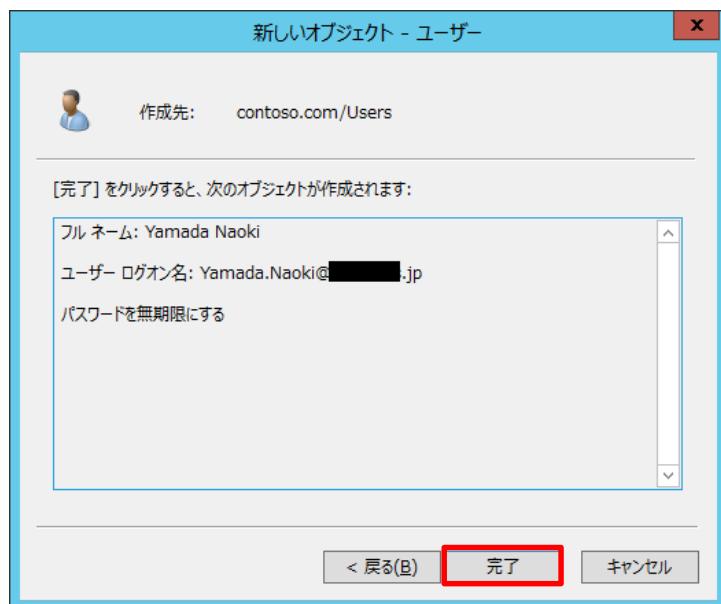
23. [新しいオブジェクト - ユーザー] 画面で、ユーザーを新規作成します。[姓]、[名前]、[フル ネーム]、[ユーザー ログオン名] をそれぞれ入力し、[ユーザー ログオン名] のサフィックス欄で Azure AD に登録されたドメイン名を選択して、[次へ] をクリックします。



24. [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] でパスワードを入力します。また、[ユーザーは次回ログオン時にパスワード変更が必要] のチェックを外し、[パスワードを無期限にする] にチェックをして、[次へ] をクリックします。

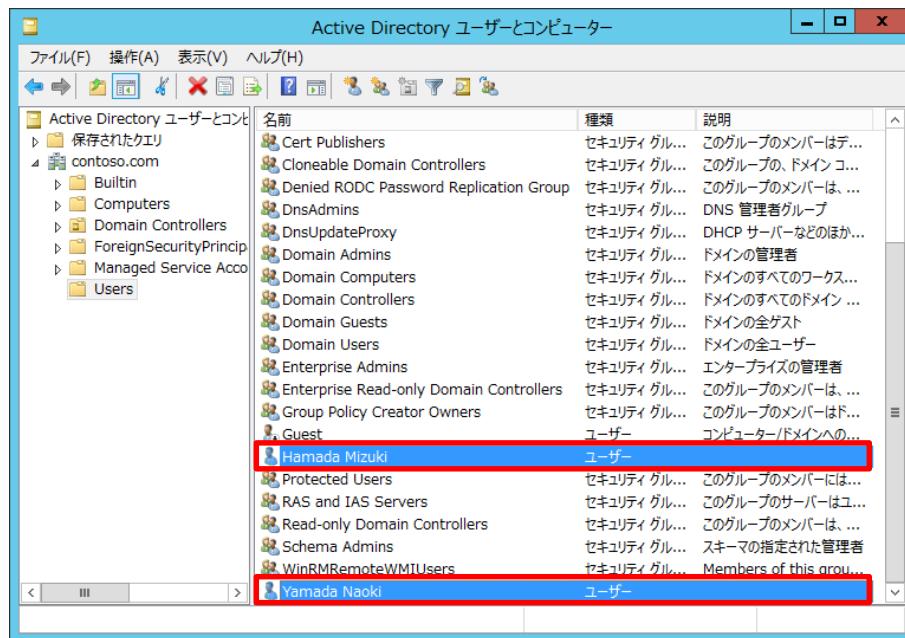


25. [新しいオブジェクト - ユーザー] 画面で、[完了] をクリックします。



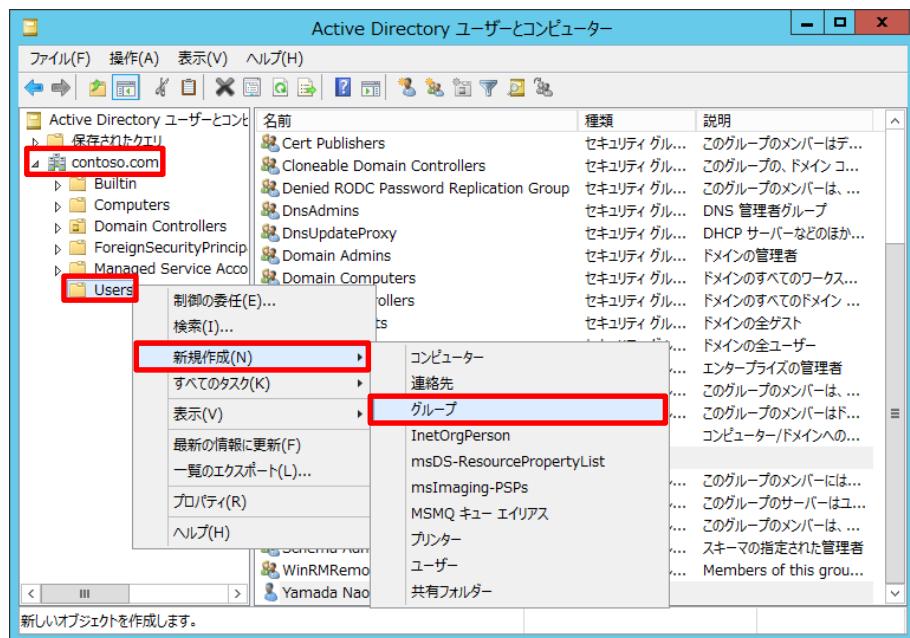
26. 同様に 22~25 の手順を繰り返し、もう 1 ユーザーを以下の要領で新規作成します。[Active Directory ユーザーとコンピューター] 画面で、Yamada ユーザー、Hamada ユーザーを作成したことを確認します。

姓	Hamada
名	Mizuki
フルネーム	Hamada Mizuki
ユーザー ログオン名	Hamada.Mizuki
パスワード	P@ssw0rd
ユーザーは次回ログオン時にパスワード変更が必要	チェックを外す
パスワードを無期限にする	チェックをつける



Microsoft Azure Active Directory の活用

27. [Active Directory ユーザーとコンピューター] 画面で、[Active Directory ユーザーとコンピューター] - [contoso.com] から [Users] を右クリックし、[新規作成] - [グループ] をクリックします。

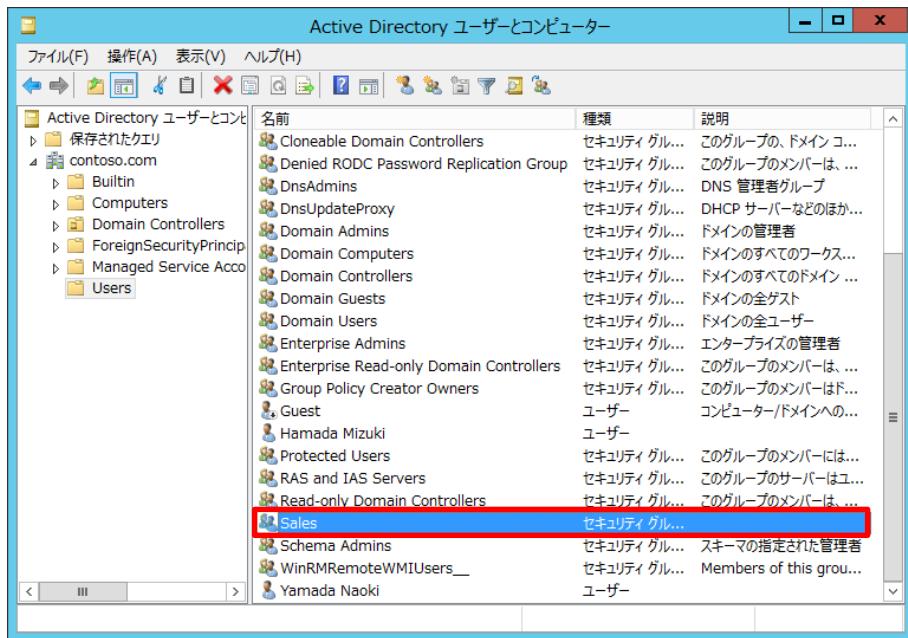


28. [新しいオブジェクト - グループ] 画面で、グループを新規作成します。[グループ名] を入力し、[OK] をクリックします。

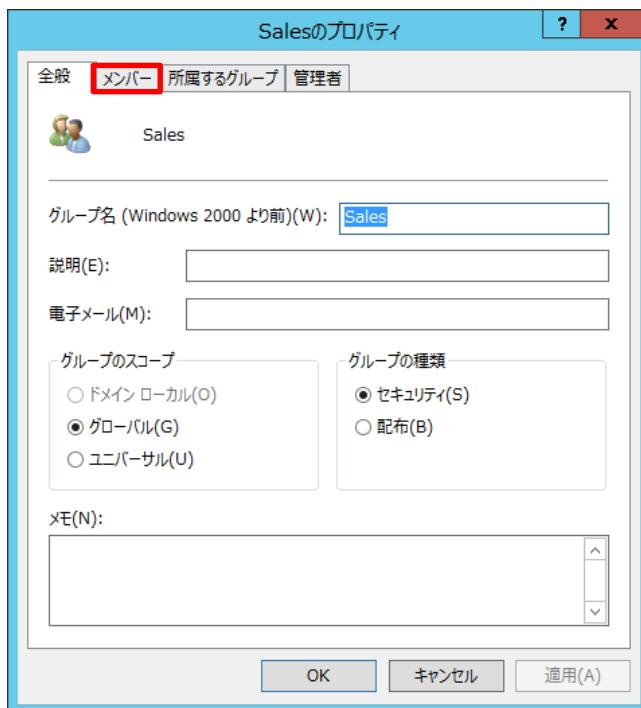


Microsoft Azure Active Directory の活用

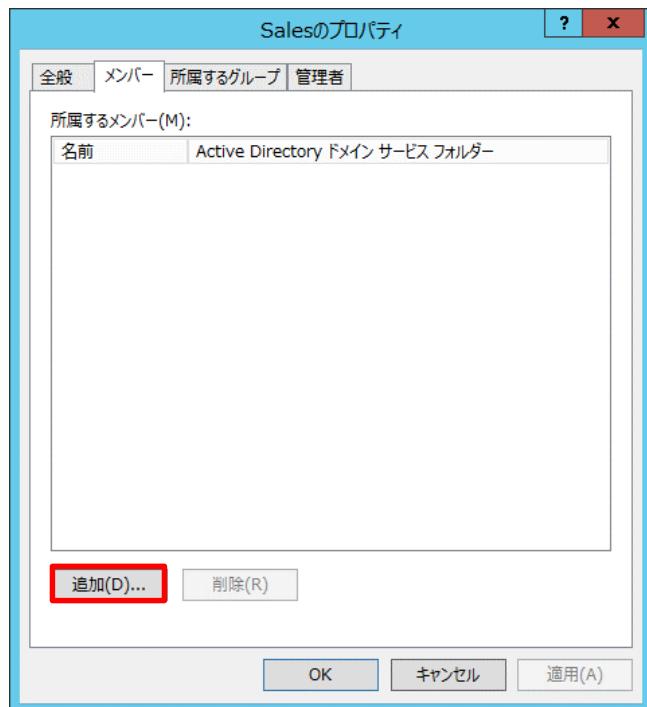
29. [Active Directory ユーザーとコンピューター] 画面で、作成された Sales グループをダブルクリックします。



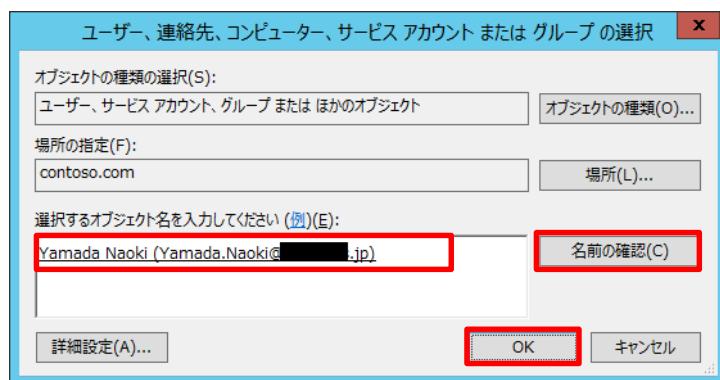
30. [Sales のプロパティ] 画面で、[メンバー] タブをクリックします。



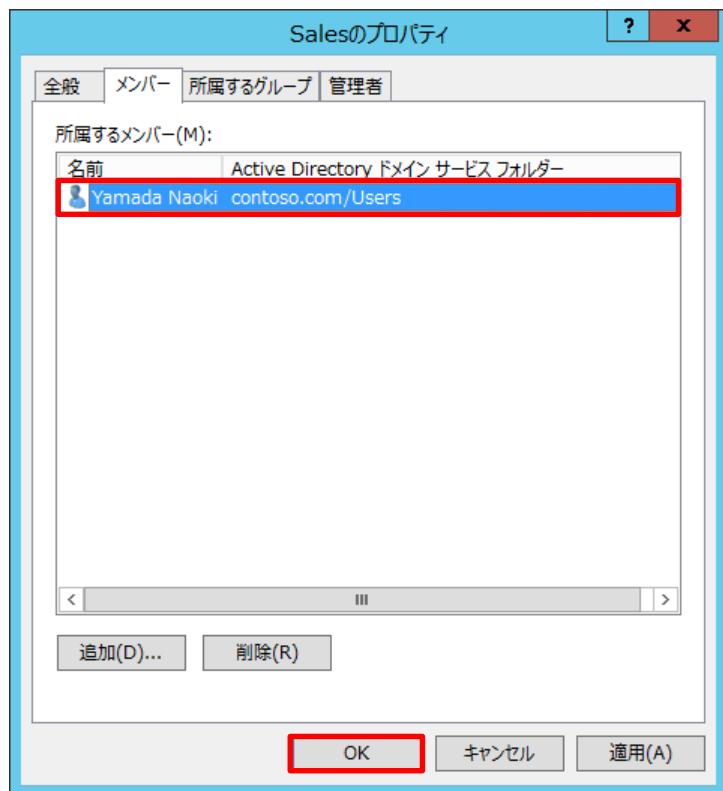
31. [メンバー] タブで、[追加] をクリックします。



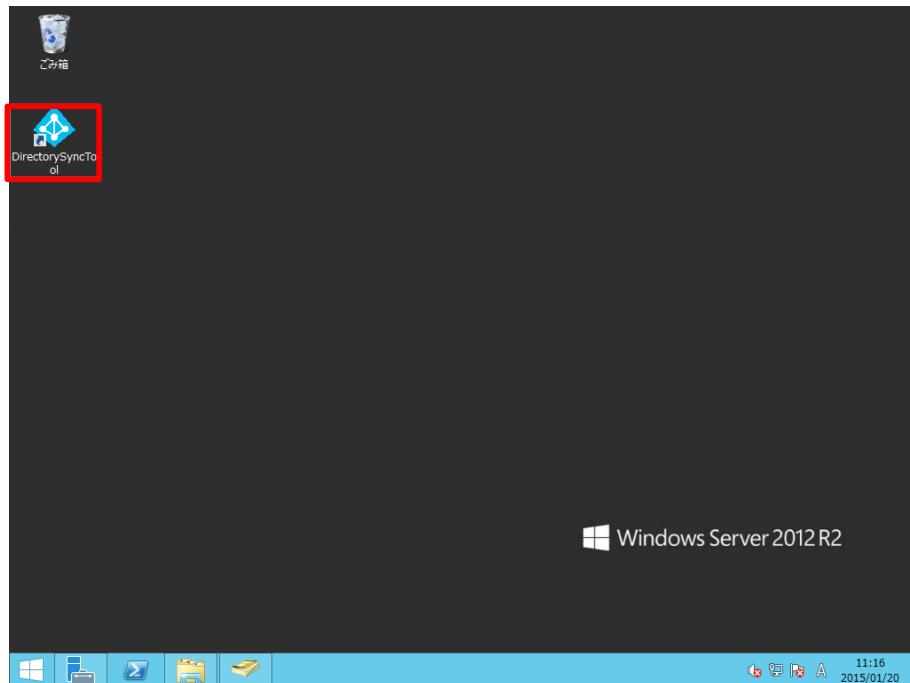
32. [ユーザー、連絡先、コンピューター、サービス アカウント または グループ の選択] 画面で、[選択するオブジェクト名を入力してください] の欄にユーザー名として Yamada と入力し、[名前の確認] をクリックするとオブジェクト名が表示されます。下線が引かれた状態を確認し、[OK] をクリックします。



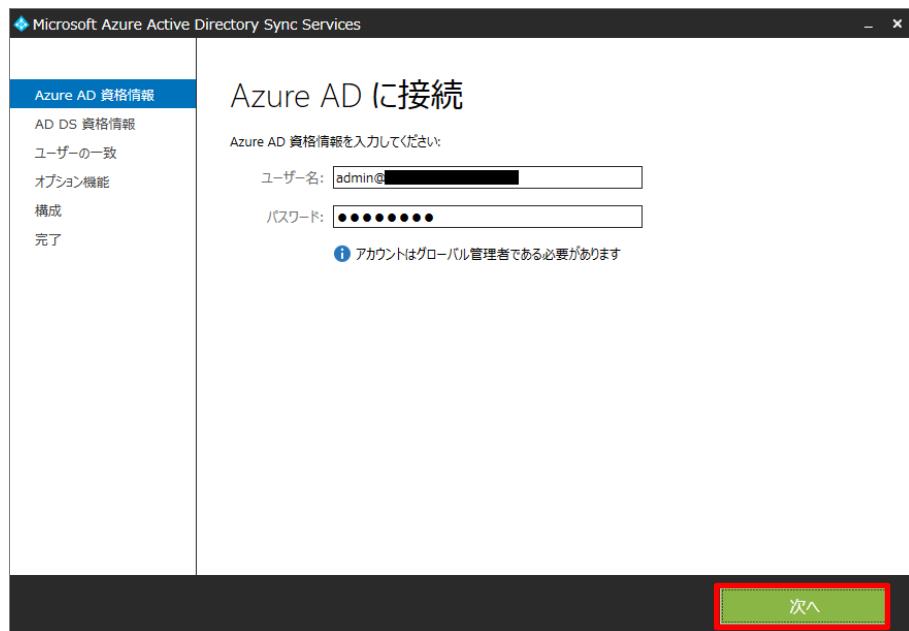
33. [Sales のプロパティ] 画面で、[所属するメンバー] に Yamada Naoki ユーザーが追加されたことを確認し、[OK] をクリックします。



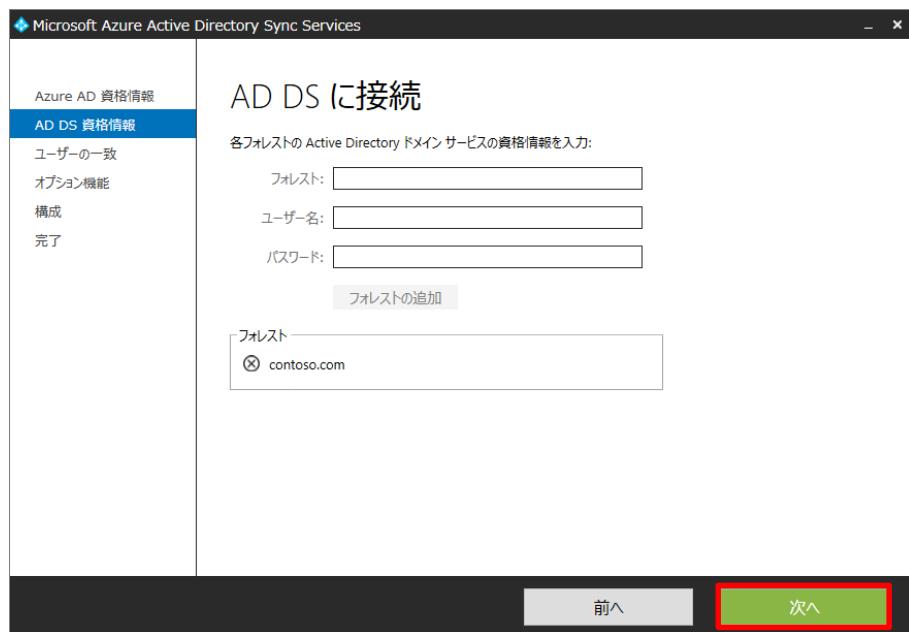
34. デスクトップ画面で、[DirectorySyncTool] アイコンをダブルクリックします。



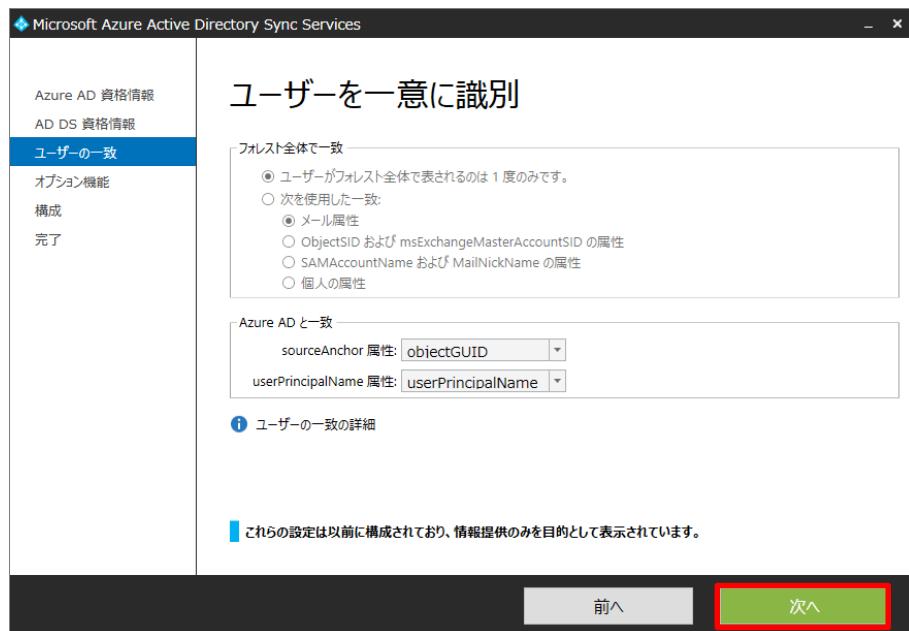
35. [Azure AD に接続] 画面で、[次へ] をクリックします。



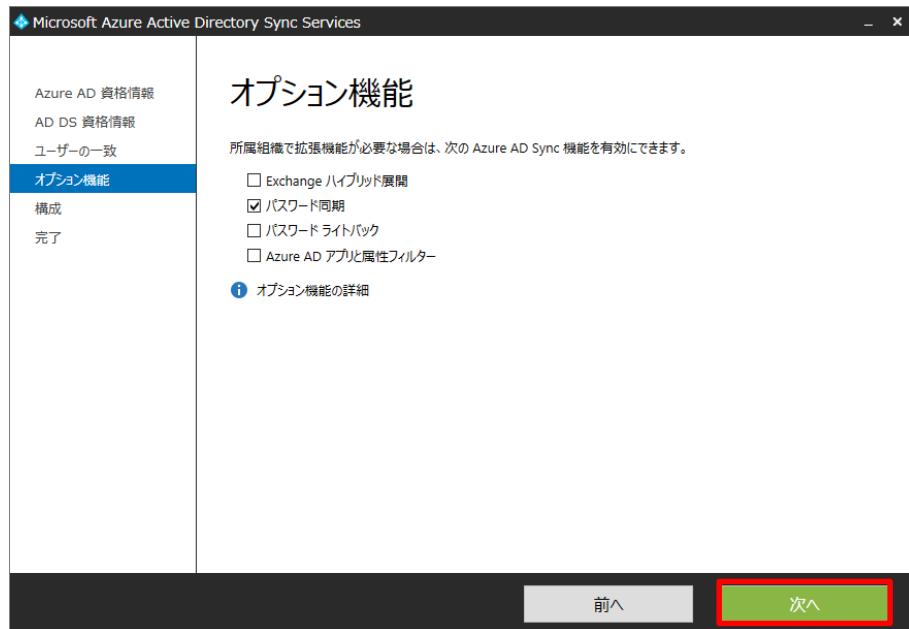
36. [AD DS に接続] 画面で、[次へ] をクリックします。



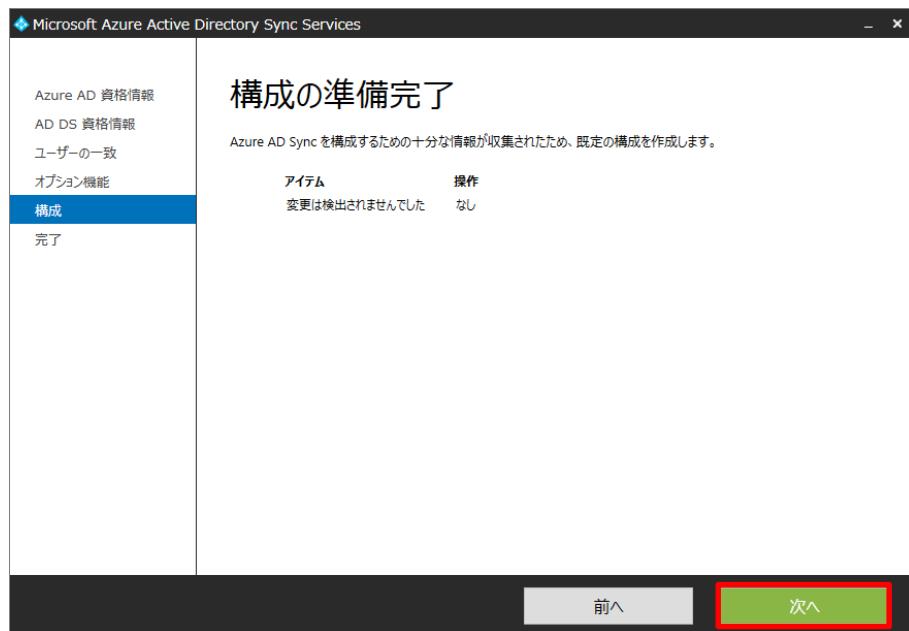
37. [ユーザーを一意に識別] 画面で、[次へ] をクリックします。



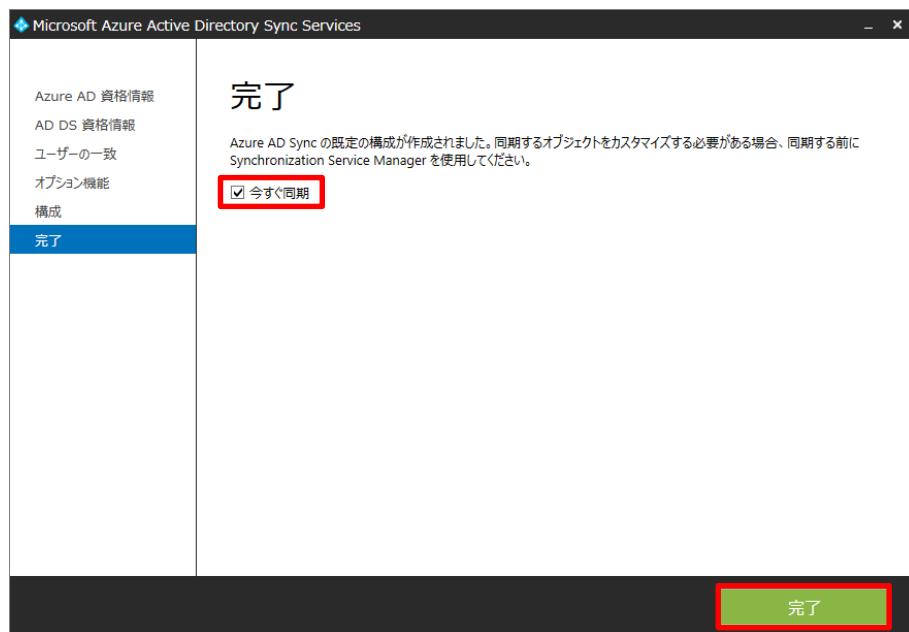
38. [オプション機能] 画面で、[次へ] をクリックします。



39. [構成の準備完了] 画面で、[次へ] をクリックします。



40. [完了] 画面で、[今すぐ同期] にチェックを入れ、[完了] をクリックします。



➡ DirSync によるディレクトリ同期の実装

1. Microsoft Azure 管理ポータル画面で、[ACTIVE DIRECTORY] をクリックし、[Contoso corporation] をクリックします。

The screenshot shows the Microsoft Azure Management Portal. On the left sidebar, the 'ACTIVE DIRECTORY' icon is highlighted with a red box. In the main content area, the 'active directory' blade for 'Contoso Corp...' is displayed. The top navigation bar includes 'active directory', 'ACCESS CONTROL', '名前空間', '多要素認証プロバイダー', 'RIGHTS MANAGEMENT', and other tabs. A search bar at the top right contains 'Contoso Corp...'. Below the search bar, there are filters for '状態' (Active), '全管理者', and location ('すべての Contoso C...', 'アジア・ヨーロッパ...', '日本'). The main table lists one item: 'Contoso Corp...'.

2. [Contoso corporation] 画面で、[ディレクトリ統合] をクリックします。

The screenshot shows the Microsoft Azure Management Portal for 'contoso corporation'. The top navigation bar includes 'ユーザー', 'グループ', 'アプリケーション', 'ドメイン', 'ディレクトリ統合' (which is highlighted with a red box), '構成', 'レポート', and 'ライセンス'. The main content area displays a message: 'ディレクトリを使用する準備ができました。作業開始するためのオプションは次のとおりです。' (Directory preparation is complete. Options for starting work are as follows). Below this, there is a section titled '作業を開始する' (Start working) with a single item: '1 ユーザー サインイン エクスペリエンスの向上' (User sign-in experience improvement). A note states: 'ユーザーが使い慣れたユーザー名でサインインできるように、カスタムドメインを追加します。たとえば、組織のドメインが "contoso.com" である場合、ユーザーは Azure AD に "joe@contoso.com" のようなユーザー名でサインインできます。' (To allow users to sign in with their familiar user names, a custom domain will be added. For example, if the organization's domain is "contoso.com", users can sign in with a user name like "joe@contoso.com").

Microsoft Azure Active Directory の活用

3. [ディレクトリ統合] 画面で、[ローカルとの統合 active directory] - [ディレクトリ同期] の[アクティブ化済み] をクリックします。

4. [ディレクトリ統合] 画面で、[アクティブ化済み] となったことを確認し、[保存] をクリックします。

5. [ディレクトリ同期をアクティブ化しますか?] 画面で、[はい] をクリックします。

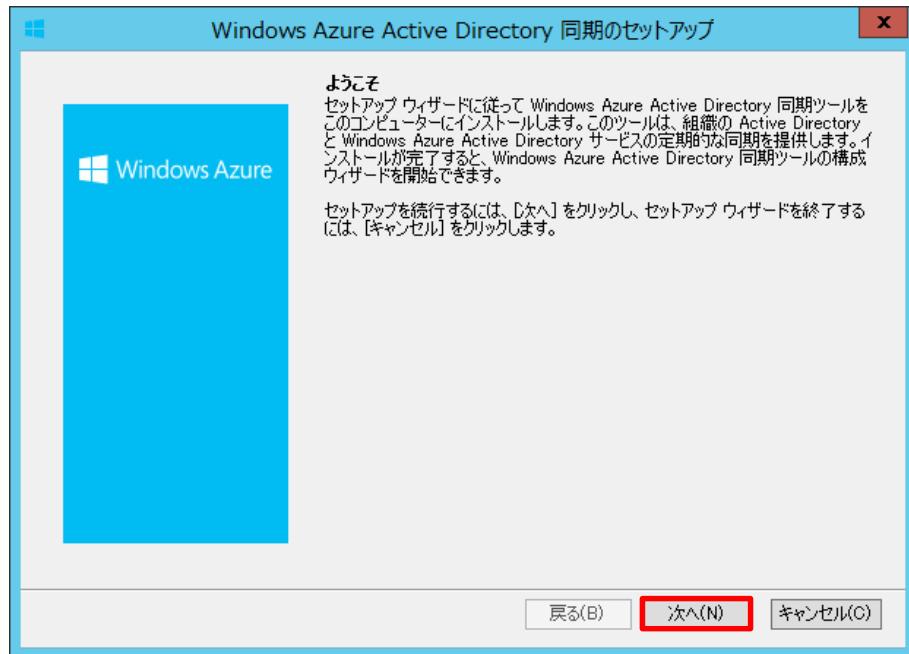


6. [ディレクトリ統合] 画面で、[ダウンロード] 欄の [ここ] リンクをクリックし、ディレクトリ同期ツールをダウンロードします。

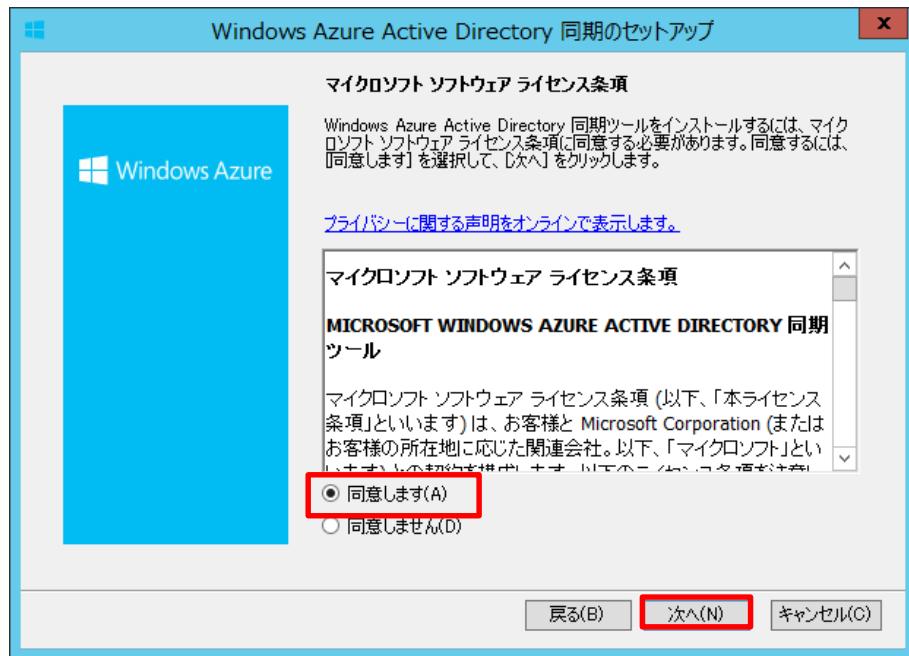
The screenshot shows the Microsoft Azure Active Directory 'Directory Integration' page. The left sidebar lists various services: Clock, Cloud, Lab, Share, Groups, Applications, Domains, Directory Integration (which is selected), Structure, Reports, and Licenses. The main content area is titled 'contoso corporation'. It displays a table with one row: 'Directory sync for the verified domain' with status 'Active'. Below this is a section titled 'Deploy and Manage' with three steps: 1. Add domain, 2. Prepare directory sync, and 3. Install and run directory sync tool. Step 3 contains a 'Download' link and an 'Install and run' link. The 'Download' link is highlighted with a red box. At the bottom of the page, there are 'New', 'Save' (highlighted with a red box), and 'Cancel' buttons.

7. ダウンロードしたディレクトリ同期ツールのセットアッププログラム dirsync.exe ファイルを WS2012-DC01 コンピューターの任意のフォルダーにコピーします。
8. WS2012-DC01 コンピューターから操作します。
dirsync.exe ファイルをダブルクリックして実行します。

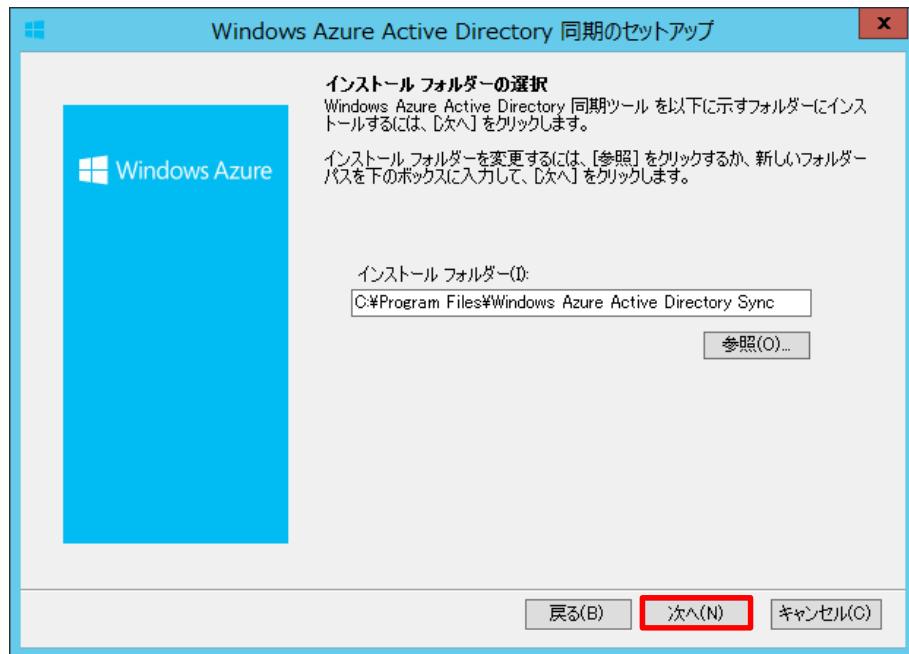
9. [ようこそ] 画面で、[次へ] をクリックします。



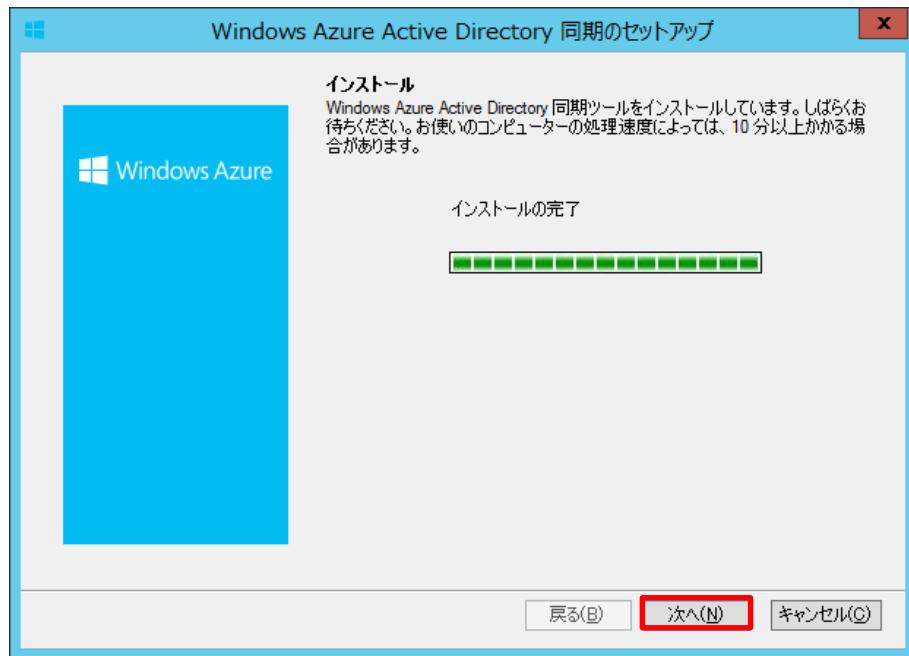
10. [マイクロソフト ソフトウェア ライセンス条項] 画面で、内容を確認し、[同意する] をクリックして、[次へ] をクリックします。



11. [インストール フォルダーの選択] 画面で、[次へ] をクリックします。ここまで手順により、インストールが開始します。



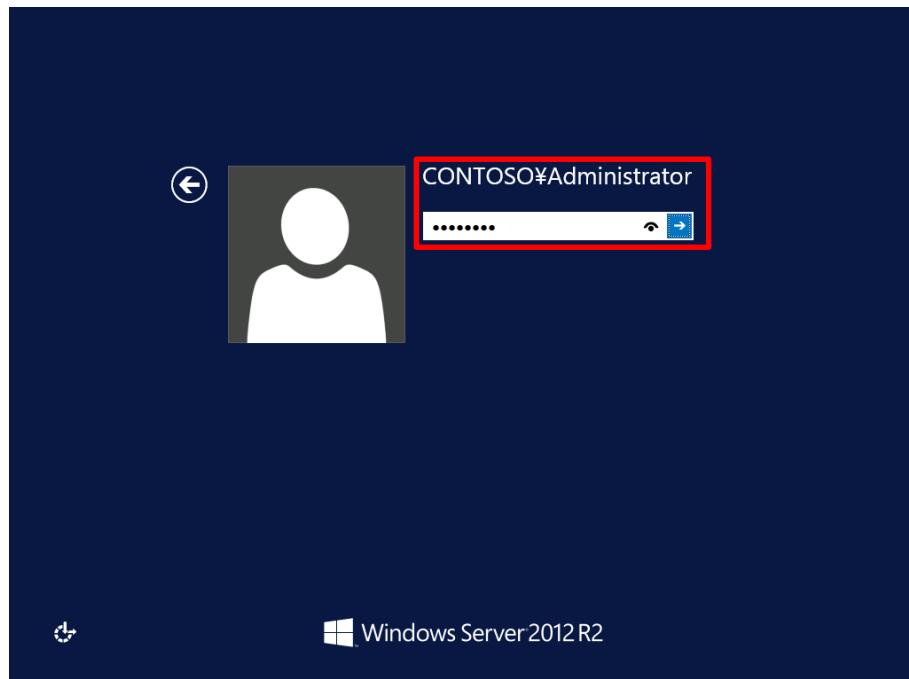
12. [インストール] 画面で、[次へ] をクリックします。



13. [終了] 画面で、[構成ウィザードを今すぐ開始する] 欄のチェックを外し、[完了] をクリックします。また、ウィザードが終了したら、サインアウトします。

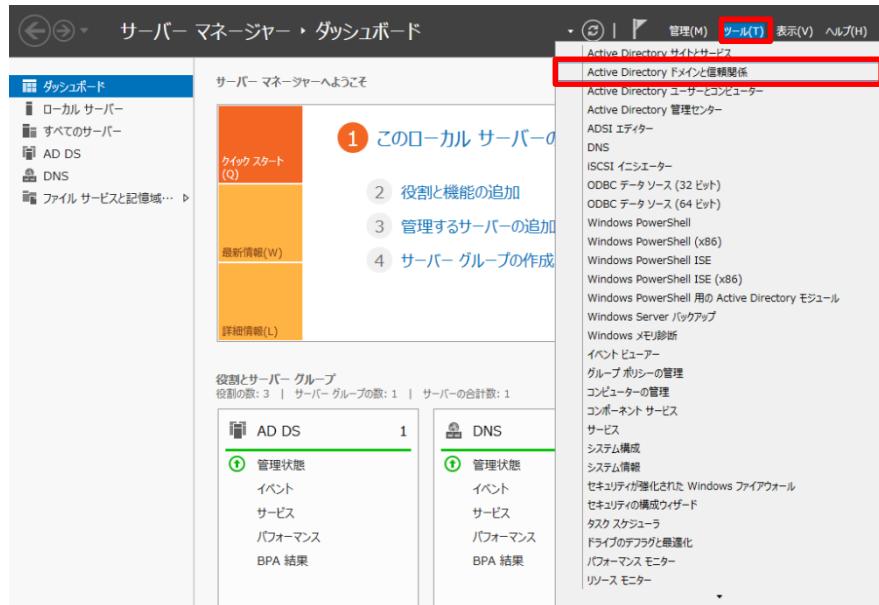


14. WS2012-DC01 コンピューターでサインアウトし、Administrator ユーザーでサインインしなおします。

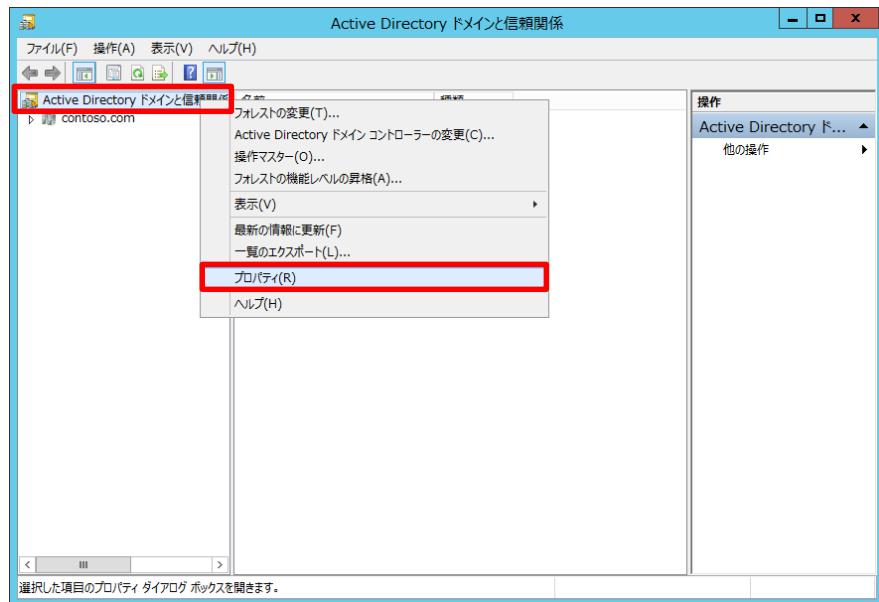


Microsoft Azure Active Directory の活用

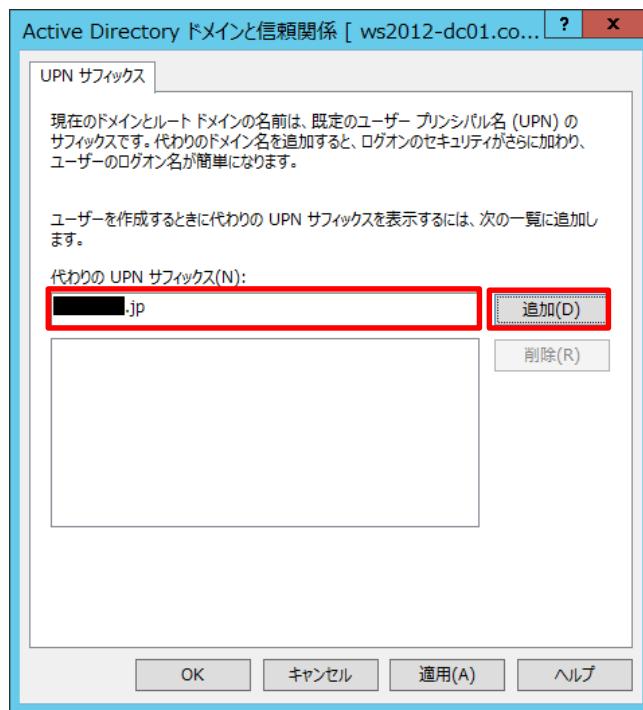
15. [サーバー マネージャー] 画面で、[ツール] - [Active Directory ドメインと信頼関係] をクリックします。



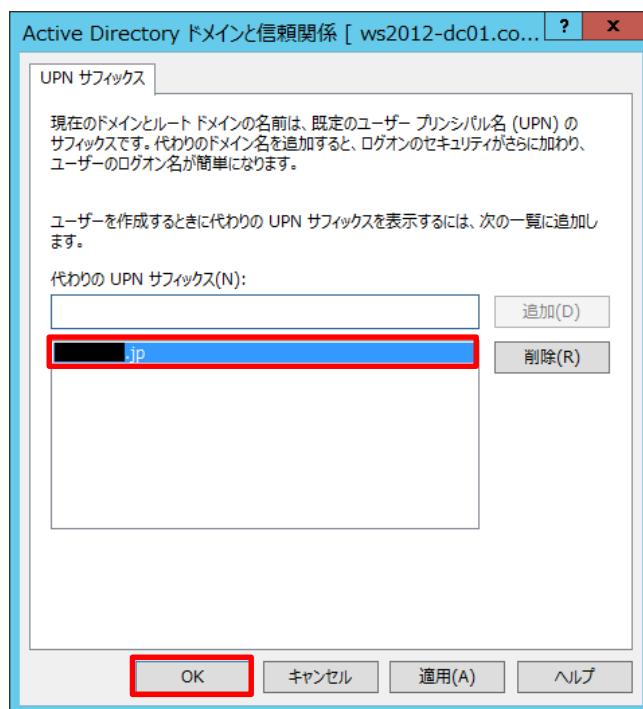
16. [Active Directory ドメインと信頼関係] 画面で、[Active Directory ドメインと信頼関係]を右クリックし、[プロパティ] をクリックします。



17. [Active Directory ドメインと信頼関係] 画面で、[代わりの UPN サフィックス] に Azure AD で使用している自己所有パブリック ドメイン名を入力し、[追加] をクリックします。

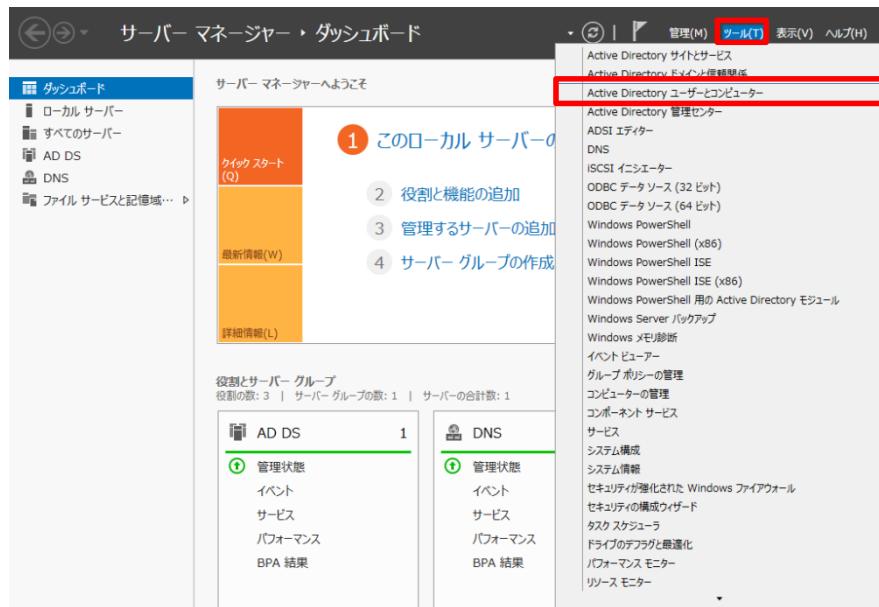


18. [Active Directory ドメインと信頼関係] 画面で、追加されたことを確認し [OK] をクリックします。

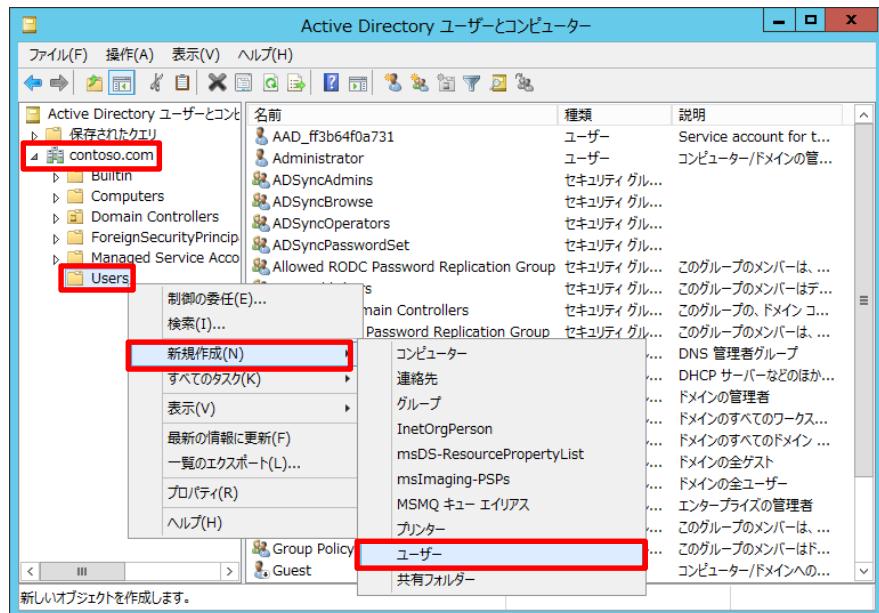


Microsoft Azure Active Directory の活用

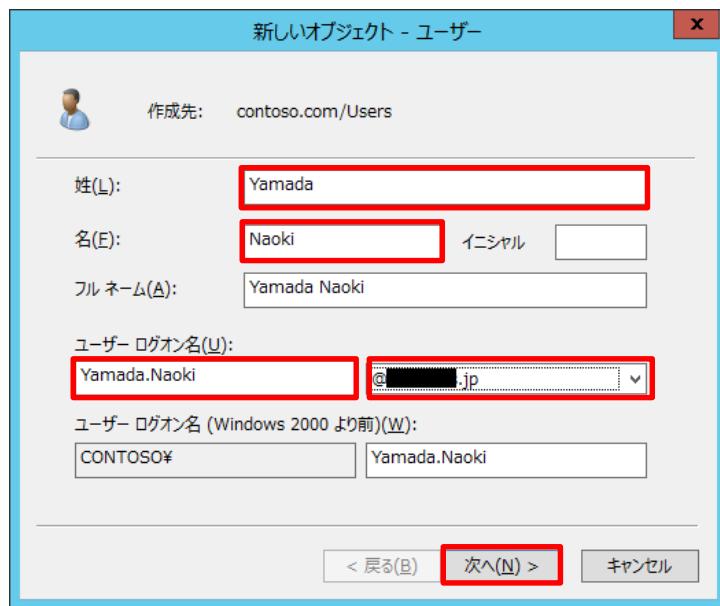
19. [サーバー マネージャー] 画面で、[ツール] - [Active Directory ユーザーとコンピューター] をクリックします。



20. [Active Directory ユーザーとコンピューター] 画面で、[Active Directory ユーザーとコンピューター] - [contoso.com] から [Users] を右クリックし、[新規作成] - [ユーザー] をクリックします。



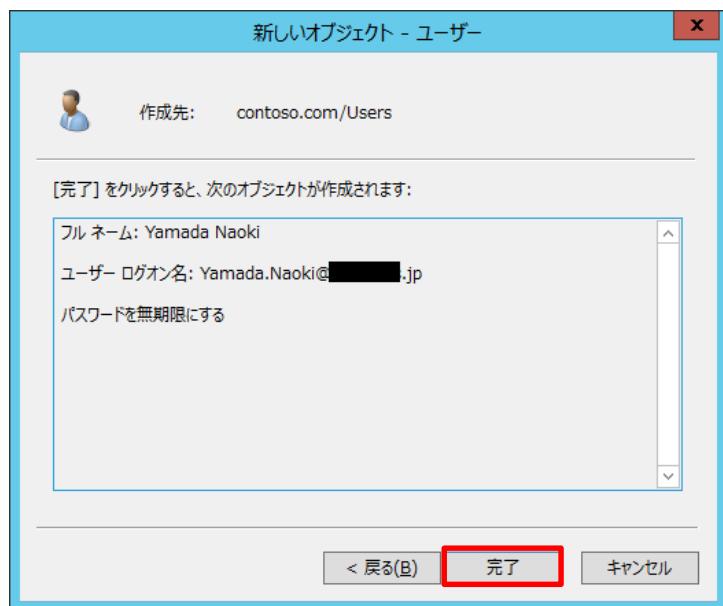
21. [新しいオブジェクト - ユーザー] 画面で、ユーザーを新規作成します。[姓]、[名前]、[フル ネーム]、[ユーザー ログオン名] をそれぞれ入力し、[ユーザー ログオン名] のサフィックス欄で Azure AD に登録されたドメイン名を選択して、[次へ] をクリックします。



22. [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] でパスワードを入力します。また、[ユーザーは次回ログオン時にパスワード変更が必要] のチェックを外し、[パスワードを無期限にする] にチェックをして、[次へ] をクリックします。

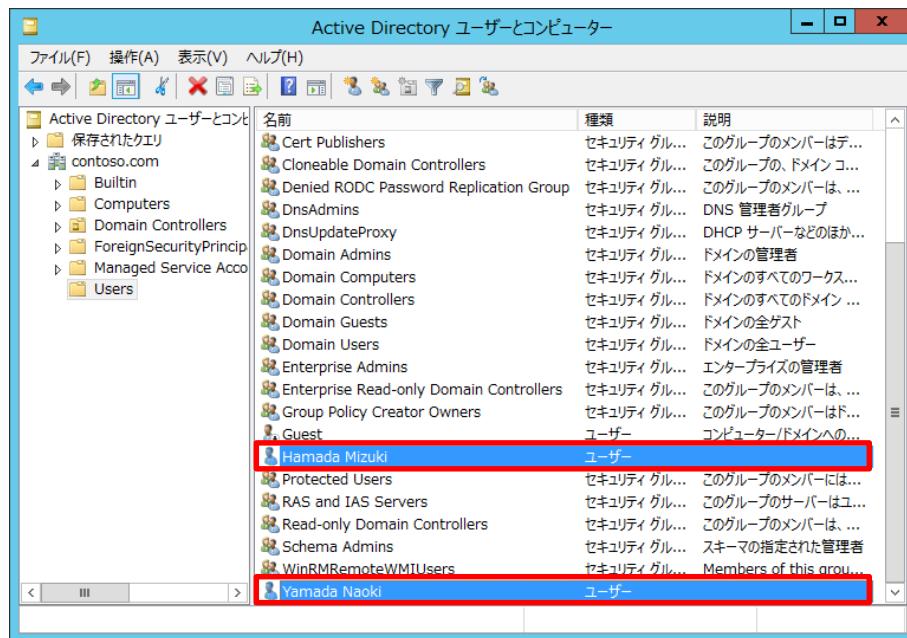


23. [新しいオブジェクト - ユーザー] 画面で、[完了] をクリックします。



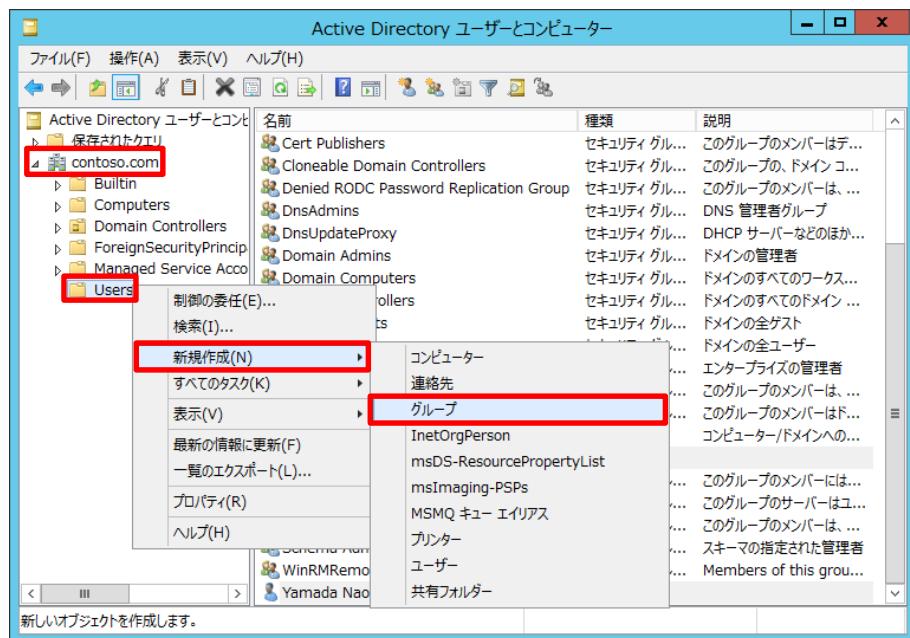
24. 同様に 20~23 の手順を繰り返し、もう 1 ユーザーを以下の要領で新規作成します。[Active Directory ユーザーとコンピューター] 画面で、Yamada ユーザー、Hamada ユーザーを作成したことを確認します。

姓	Hamada
名	Mizuki
フルネーム	Hamada Mizuki
ユーザー ログオン名	Hamada.Mizuki
パスワード	P@ssw0rd
ユーザーは次回ログオン時にパスワード変更が必要	チェックを外す
パスワードを無期限にする	チェックをつける



Microsoft Azure Active Directory の活用

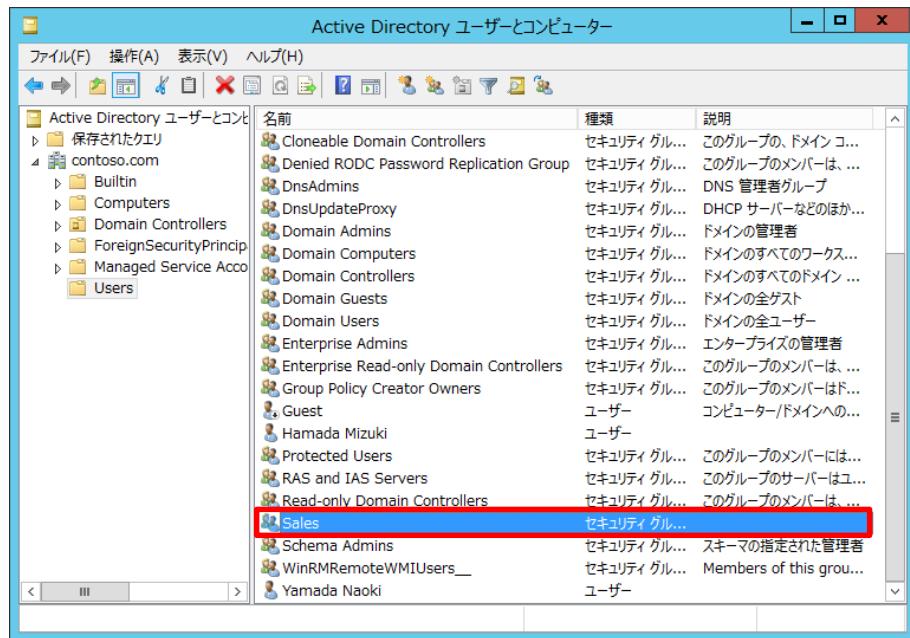
25. [Active Directory ユーザーとコンピューター] 画面で、[Active Directory ユーザーとコンピューター] - [contoso.com] から [Users] を右クリックし、[新規作成] - [グループ] をクリックします。



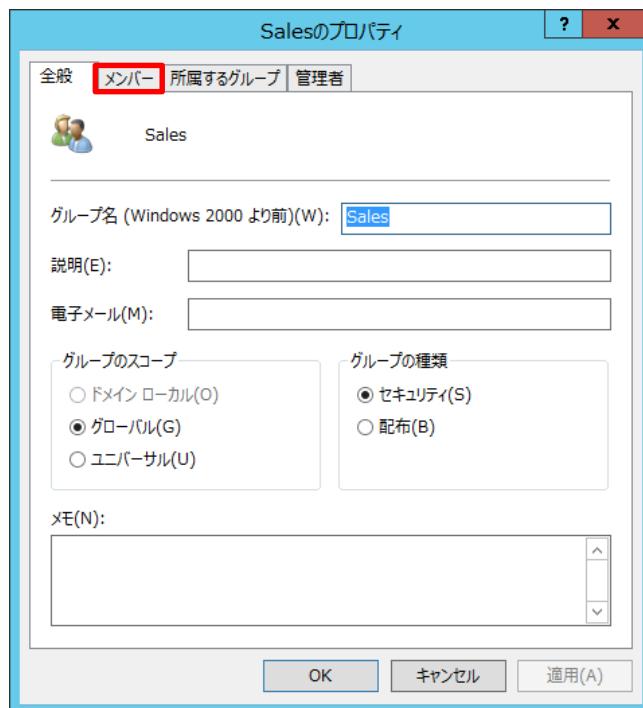
26. [新しいオブジェクト - グループ] 画面で、グループを新規作成します。[グループ名] を入力し、[OK] をクリックします。



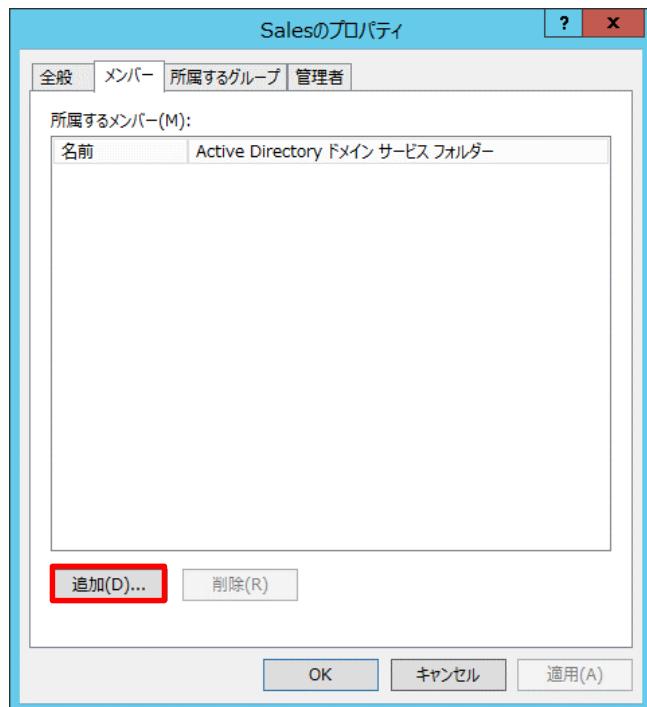
27. [Active Directory ユーザーとコンピューター] 画面で、作成された Sales グループをダブルクリックします。



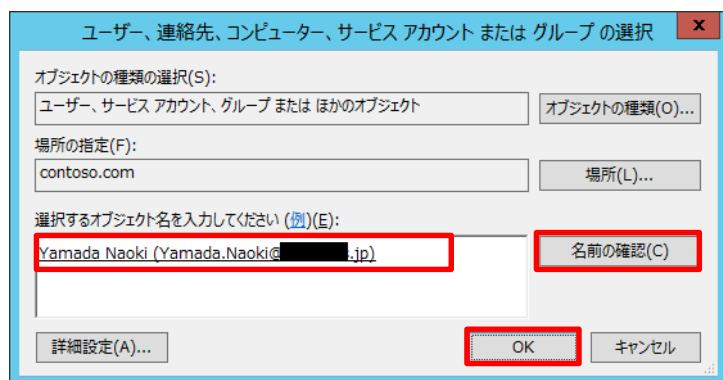
28. [Sales のプロパティ] 画面で、[メンバー] タブをクリックします。



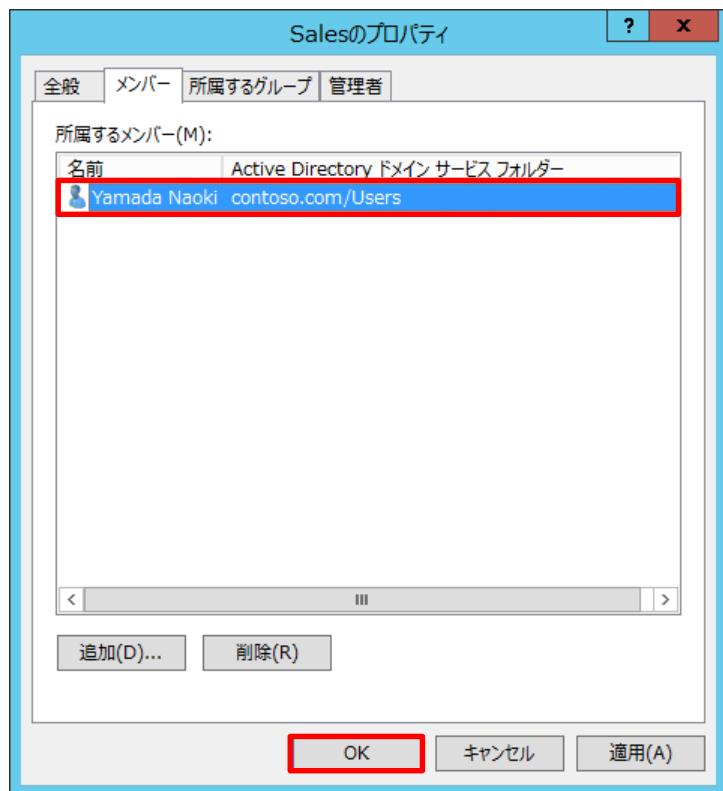
29. [メンバー] タブで、[追加] をクリックします。



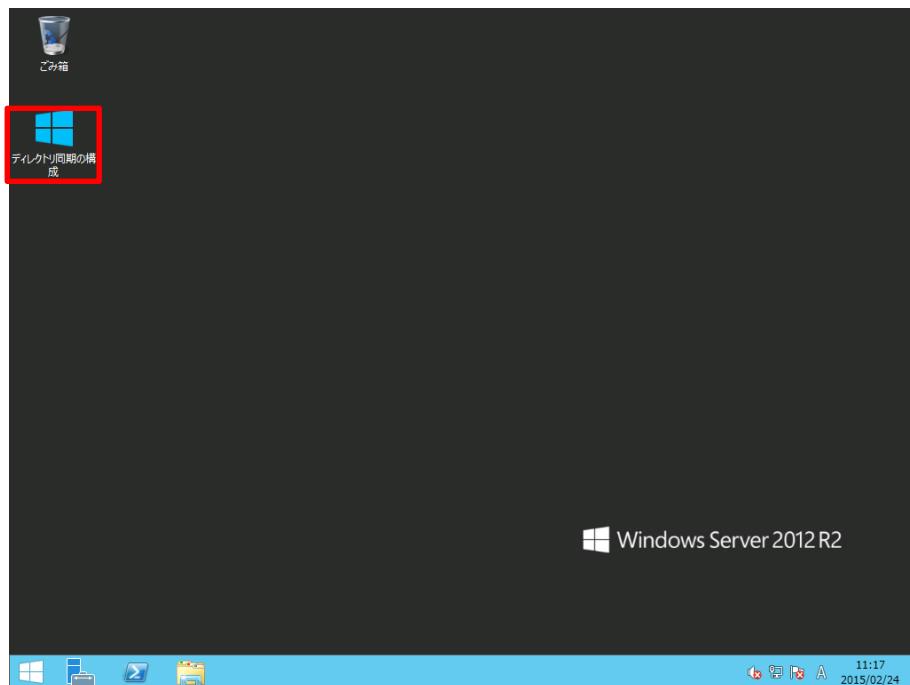
30. [ユーザー、連絡先、コンピューター、サービス アカウント または グループ の選択] 画面で、[選択するオブジェクト名を入力してください] の欄にユーザー名として Yamada と入力し、[名前の確認] をクリックするとオブジェクト名が表示されます。下線が引かれた状態を確認し、[OK] をクリックします。



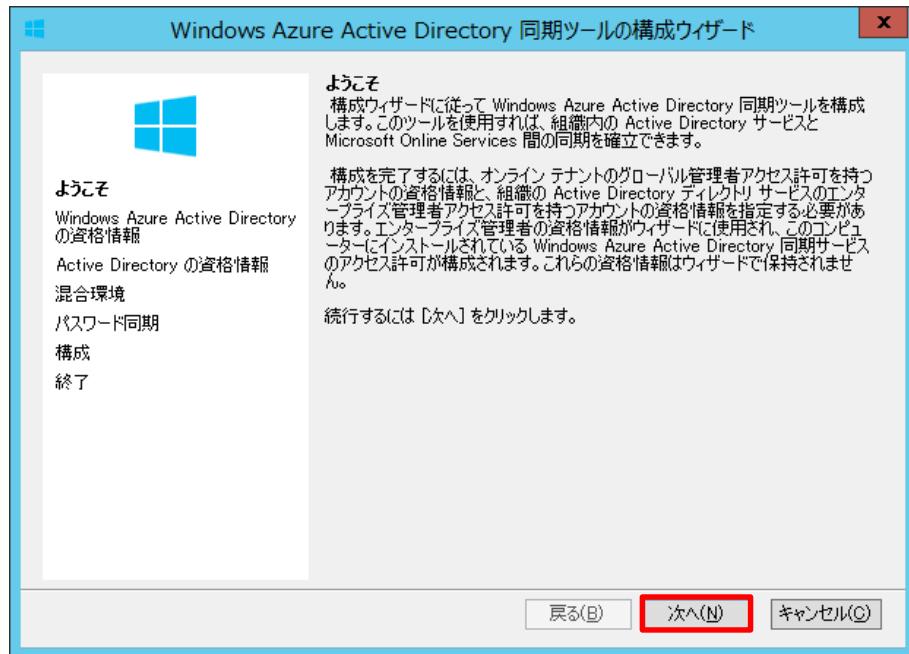
31. [Sales のプロパティ] 画面で、[所属するメンバー] に Yamada Naoki ユーザーが追加されたことを確認し、[OK] をクリックします。



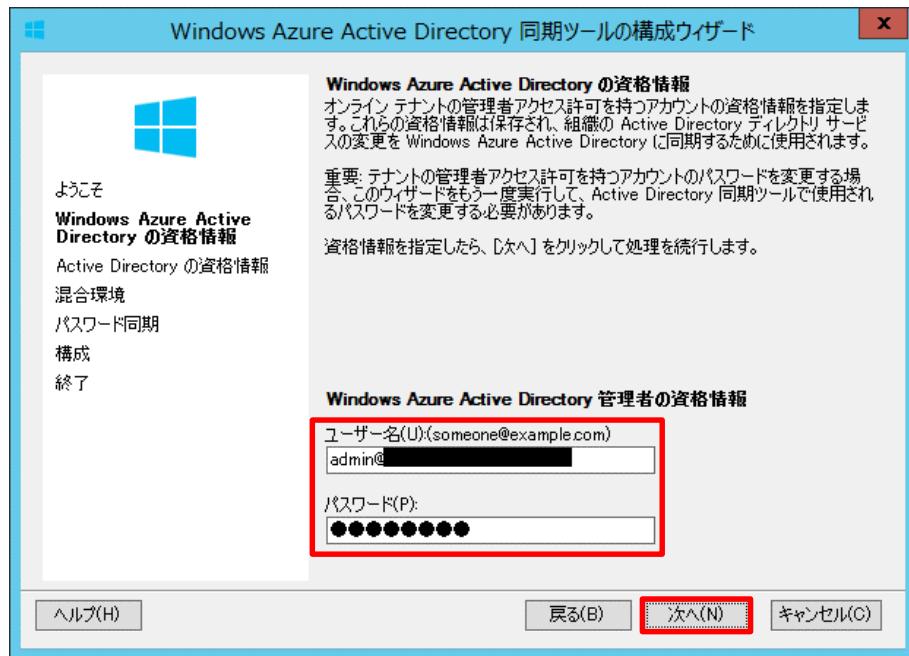
32. デスクトップ画面で、[ディレクトリ同期の構成] アイコンをダブルクリックします。



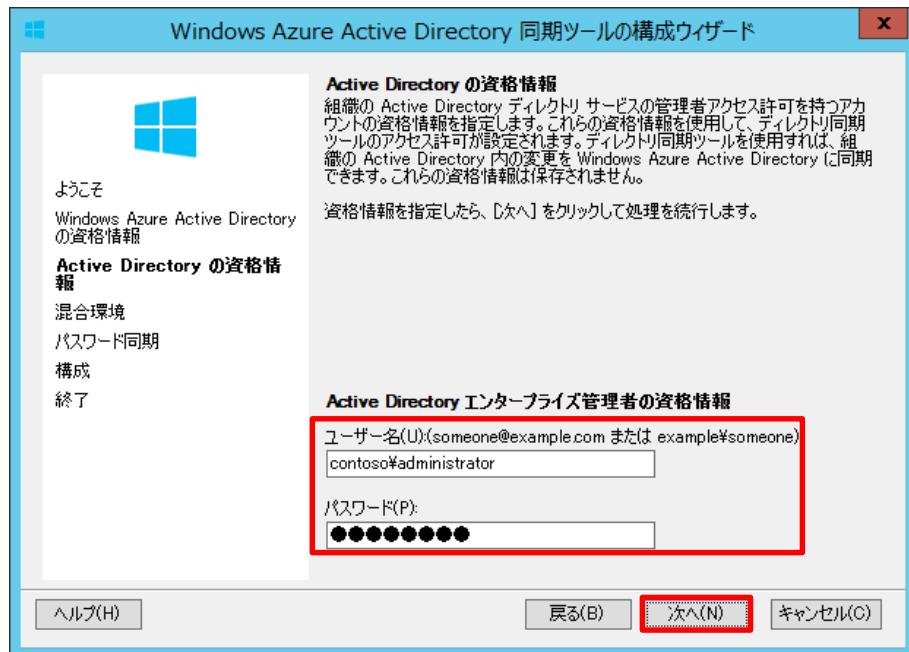
33. [ようこそ] 画面で、[次へ] をクリックします。



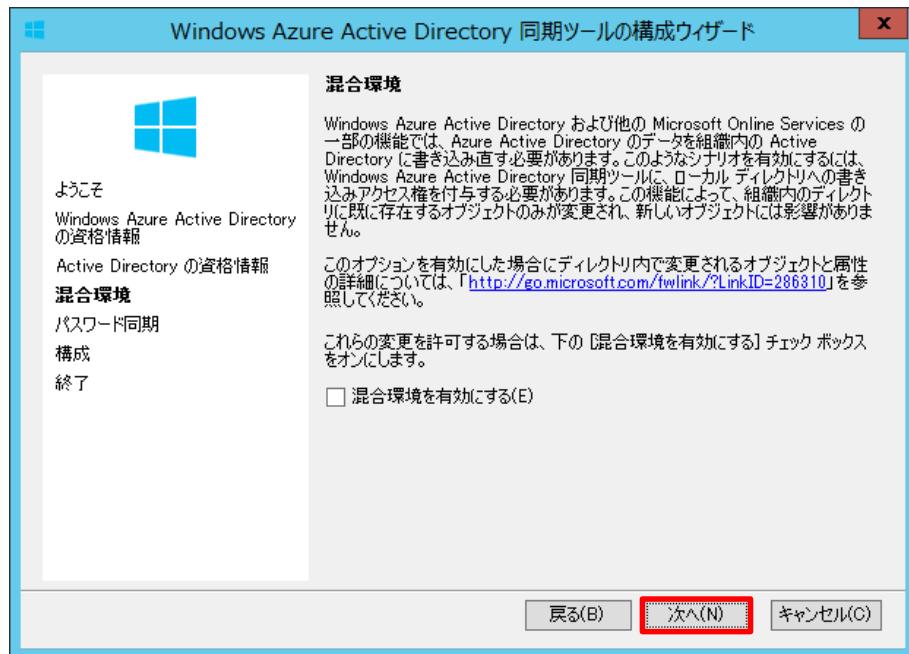
34. [Windows Azure Active Directory の資格情報] 画面で、Azure AD の全体管理者のユーザー名とパスワードを入力し、[次へ] をクリックします。



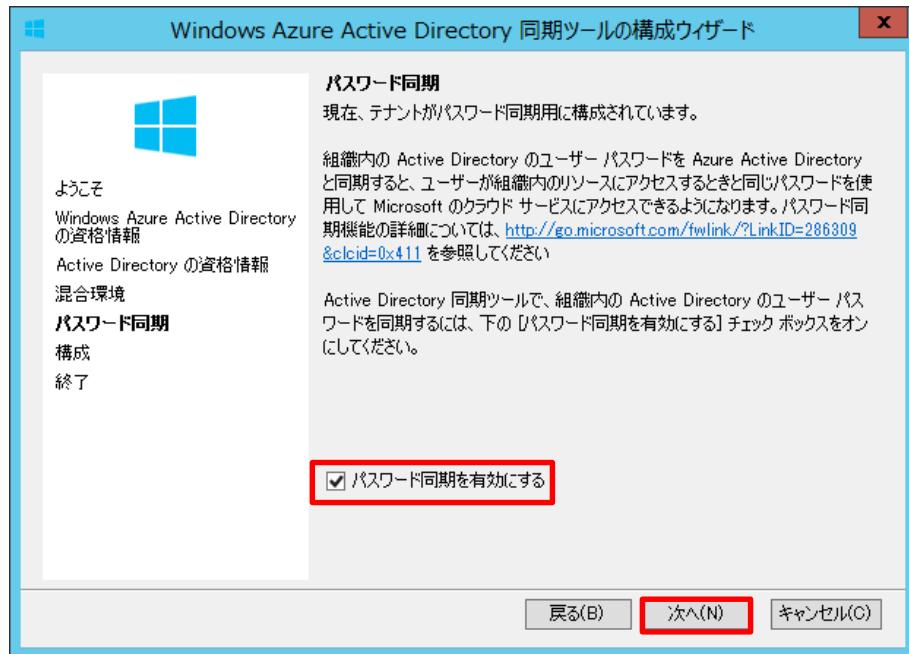
35. [Active Directory の資格情報] 画面で、Active Directory 管理者のユーザー名とパスワードを入力し、[次へ] をクリックします。



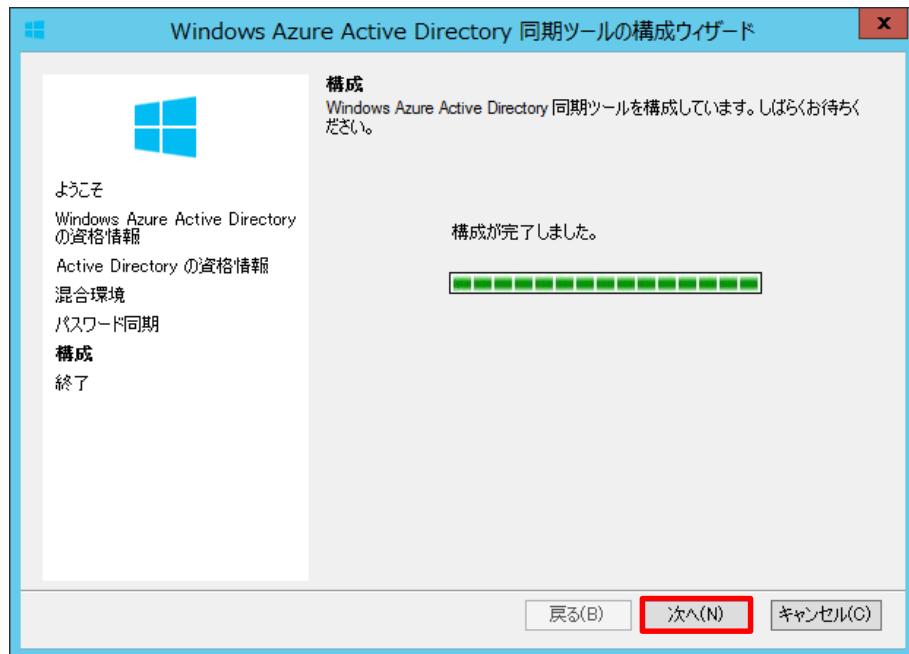
36. [混合環境] 画面で、[次へ] をクリックします。



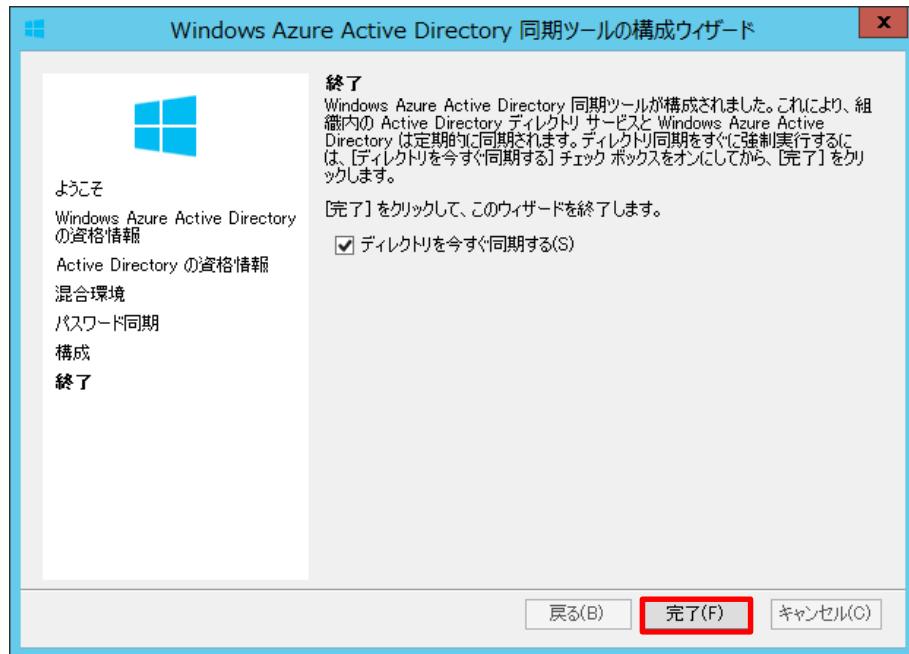
37. [パスワード同期] 画面で、[パスワード同期を有効にする] にチェックをつけ、[次へ] をクリックします。



38. [構成] 画面で、[次へ] をクリックします。



39. [終了] 画面で、[完了] をクリックします。



40. [Windows Azure Active Directory 同期ツールの構成ウィザード] 画面で、[OK] をクリックします。



➡ ディレクトリ同期後の確認

本手順では、AADSync または DirSync を利用してパスワード リセットの設定を行った結果を確認するため、パスワード リセットを実行できることを確認します。

1. Internet Explorer を起動し、URL として「<https://manage.windowsazure.com>」と入力し、Microsoft Azure 管理ポータルにアクセスします。Microsoft Azure 管理ポータルのサインイン画面で、Microsoft アカウントのユーザー名とパスワードを入力し、[サインイン] をクリックします。



2. Microsoft Azure 管理ポータル画面で、[Contoso Corporation] をクリックします。



3. [Contoso corporation] 画面で、[ユーザー] タブをクリックし、Yamada ユーザーと Hamada ユーザーが同期されていることを確認します。

表示名	ユーザー名	ソース ディレクトリ
aaduser1	aaduser1@██████████	Microsoft Azure の Active Directory
Azure 全体管理者	admin@██████████	Microsoft アカウント
Contoso 管理者	admin@██████████	Microsoft Azure の Active Directory
Hamada Mizuki	Hamada.Mizuki@██████████	ローカル Active Directory
Yamada Naoki	Yamada.Naoki@██████████	ローカル Active Directory

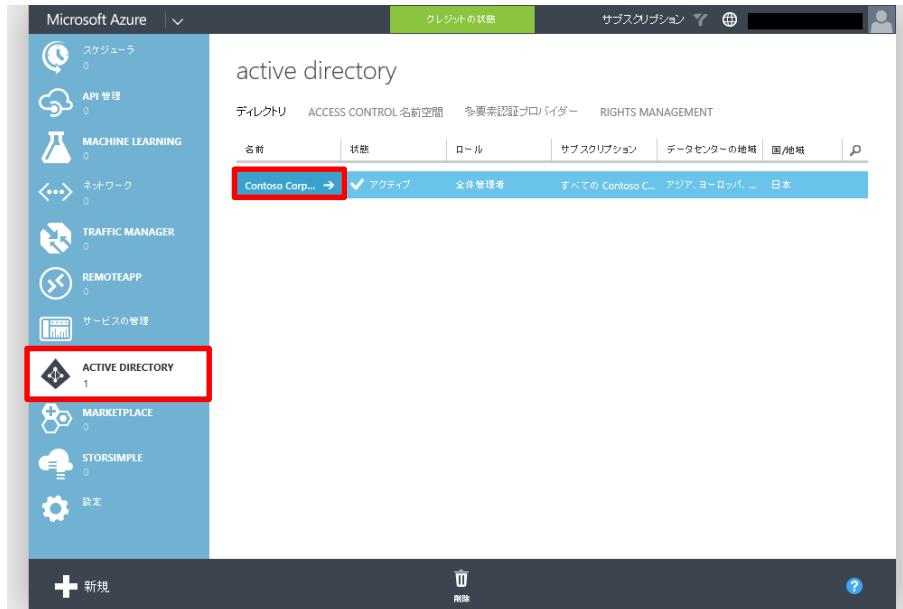
4. [Contoso corporation] 画面で、[グループ] をクリックします。Sales グループが同期されていることを確認します。

名前	説明	ソース ディレクトリ
ADSyncAdmins		ローカル Active Directory
ADSyncBrowse		ローカル Active Directory
ADSyncOperators		ローカル Active Directory
ADSyncPasswordSet		ローカル Active Directory
DnsAdmins	DNS 管理者グループ	ローカル Active Directory
DnsUpdateProxy	DHCP サーバーなどのほかのクライアントに代... ローカル Active Directory	ローカル Active Directory
Sales		ローカル Active Directory
WinRMRemoteWMIUsers_	Members of this group can access WMI resou... ローカル Active Directory	ローカル Active Directory

4.7 Azure AD Premium ライセンスの割り当て

Azure AD に登録されたユーザーに対して Azure AD Premium ライセンスを割り当てます。本手順では、評価版ライセンスを利用してユーザーにライセンスを割り当てます。

1. Microsoft Azure 管理ポータル画面で、[ACTIVE DIRECTORY] をクリックし、[Contoso corporation] をクリックします。



2. [Contoso corporation] 画面で、[ユーザー] をクリックします。



3. [Contoso corporation] 画面で、Azure AD Premium ライセンスを割り当てるユーザーをクリックします。

The screenshot shows the Microsoft Azure Active Directory interface for the 'contoso corporation' tenant. On the left, there's a sidebar with various icons. The main area displays a table of users. One user, 'Azure 全体管理者', is highlighted with a red box. The table columns include '表示名' (Display Name), 'ユーザー名' (User Name), and 'ソース ディレクトリ' (Source Directory). The 'Azure 全体管理者' row shows 'aaduser1' as the display name, 'aaduser1@[REDACTED]' as the user name, and 'Microsoft Azure の Active Directory' as the source directory.

4. [Contoso 管理者] 画面で、[設定] - [利用場所] から [国または地域の選択] プルダウンメニューを選択します。

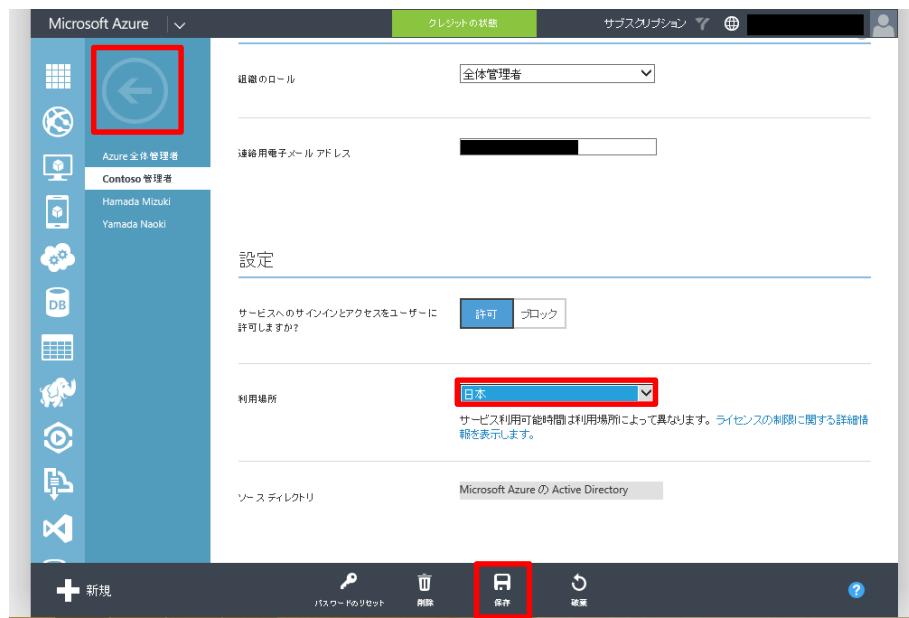
The screenshot shows the 'Settings' section of the Microsoft Azure Active Directory management portal for the 'Contoso' tenant. Under the 'Azure Active Directory' role, there's a 'Location' dropdown menu. This menu is highlighted with a red box. Below it, there's a note about service sign-in and access restrictions based on location.

【Note:】

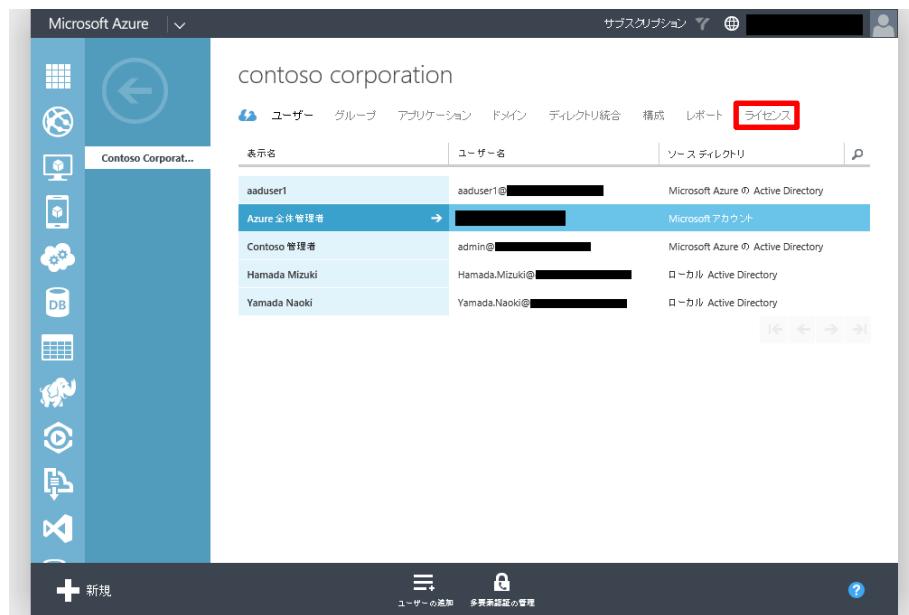
Azure AD Premium のライセンスを割り当てるユーザーは利用場所となる国または地域が設定されていることが前提です。Azure 管理ポータルで Azure AD Premium 機能の操作を行うユーザーにもライセンスが割り当られている必要があるため、Azure 管理ポータルにサインインするマイクロソフト アカウントにも [利用場所] の設定を必ず行ってください。

Microsoft Azure Active Directory の活用

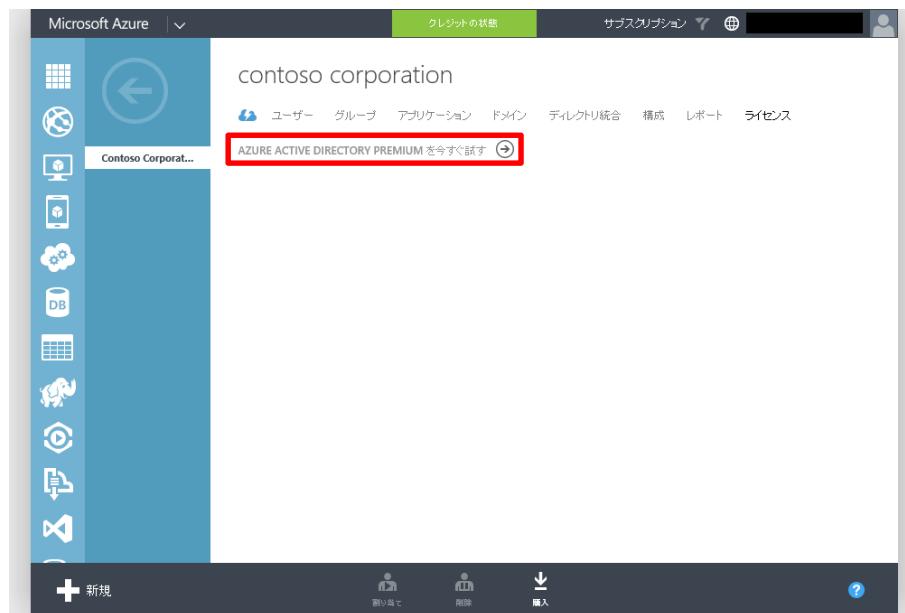
5. [Contoso 管理者] 画面で、[利用場所] に [日本] を選択し、[保存] をクリックします。その後、表示されるチェックマークで [保存] をクリックし、[←] で [Contoso corporation] 画面に戻ります。



6. [Contoso corporation] 画面で、[ライセンス] をクリックします。



7. [Contoso corporation] 画面で、[AZURE ACTIVE DIRECTORY PREMIUM を今すぐ試す] をクリックします。

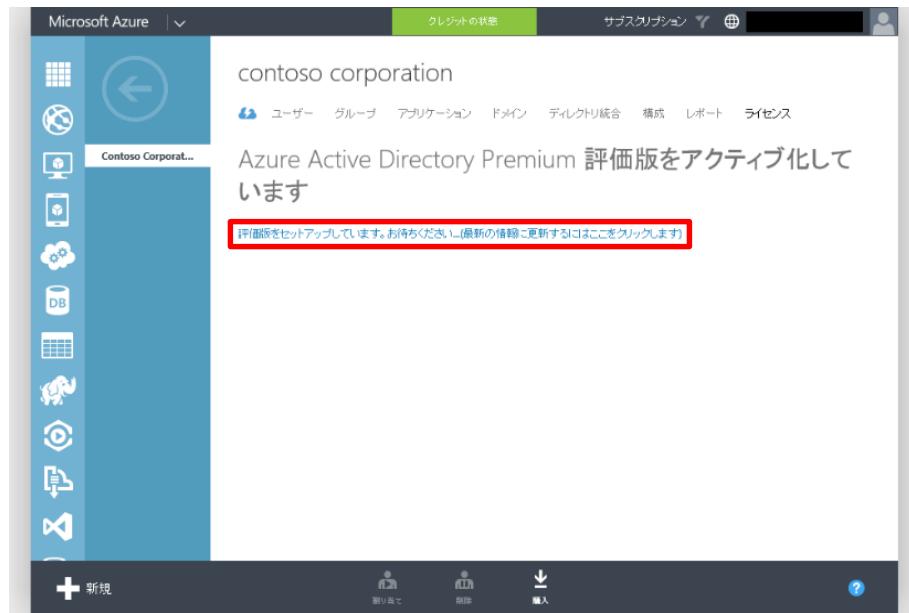


8. [Azure AD Premium 評価版のアクティブ化] 画面で、チェック マークをクリックします。

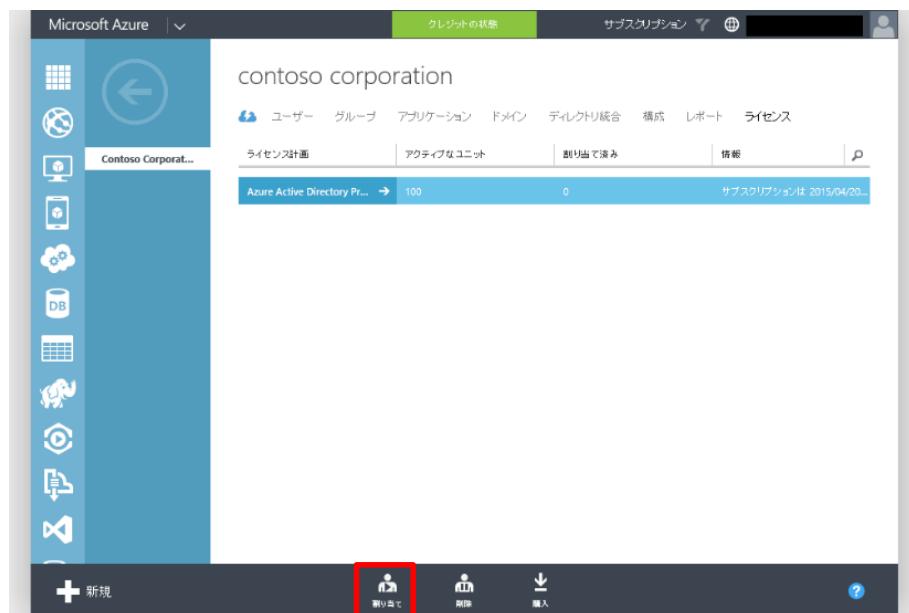


Microsoft Azure Active Directory の活用

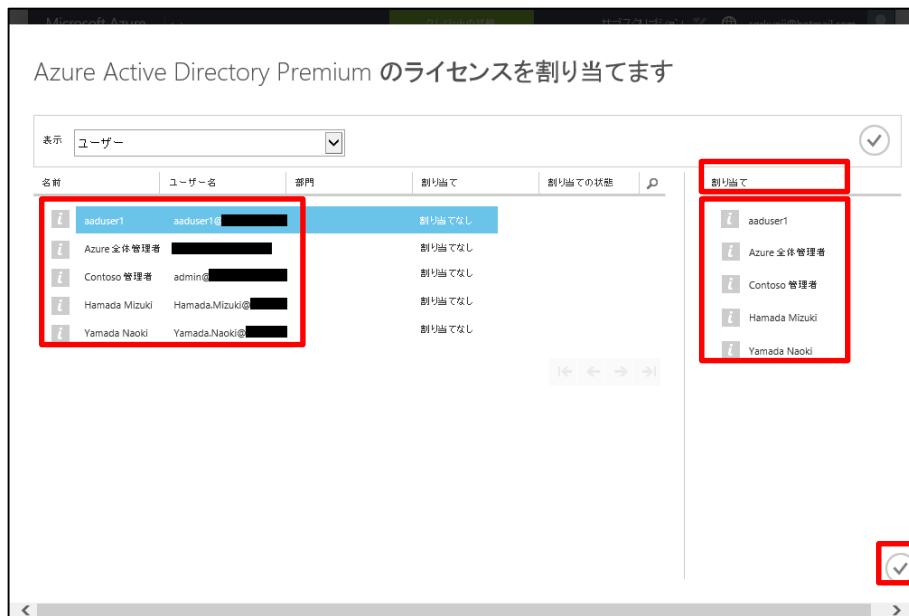
9. [Contoso corporation] 画面で、[評価版をセットアップしています。お待ちください…(最新の情報に更新するにはここをクリックします)] をしばらく、時間をおいてからクリックします。



10. [Contoso corporation] 画面で、[割り当て] をクリックします。



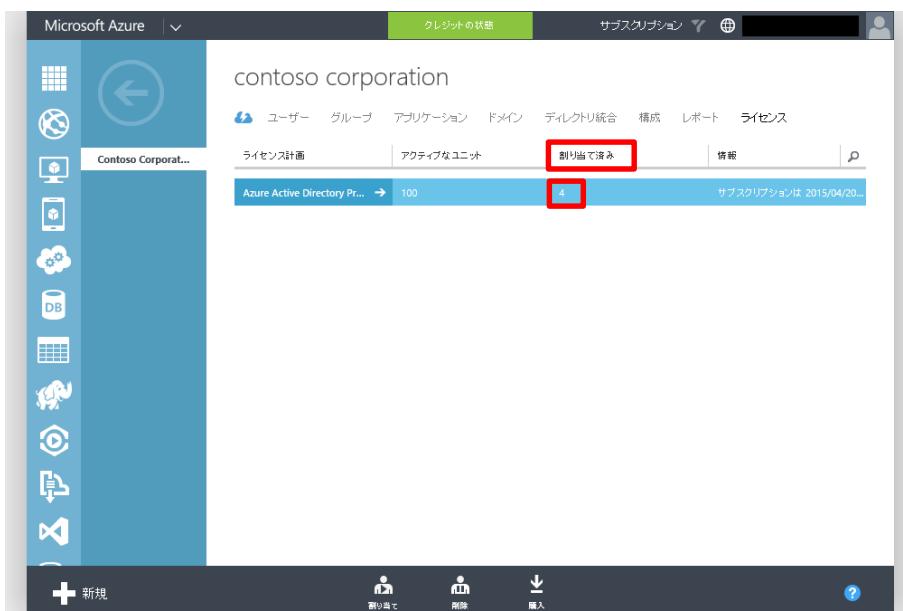
11. [Azure Active Directory Premium のライセンスを割り当てます] 画面で、割り当てたいユーザーをそれぞれ選択します。選択したユーザーは [割り当て] に表示されます。割り当て後はチェック マークをクリックし、完了します。



【Note:】

Azure AD Premium のライセンスは Azure 管理ポータルにサインインするマイクロソフト アカウントにも割り当ててください。

12. [Contoso corporation] 画面で、ユーザーにライセンスが割り当てられたことを確認します。([割り当て済み] に、割り当てたユーザー数が 0 から増えていることで確認できます)



4.8 グループ管理の委任

本手順では、Azure AD Premium の機能であるグループ管理の委任機能を設定し、Microsoft Azure の全体管理者以外のユーザーが Microsoft Azure 管理ポータルを使わずに、グループのメンバーシップを変更できる様子を確認します。

1. Microsoft Azure 管理ポータル画面で、[ACTIVE DIRECTORY] をクリックし、[Contoso corporation] をクリックします。

The screenshot shows the Microsoft Azure Management Portal interface. On the left, there's a sidebar with various service icons. The 'ACTIVE DIRECTORY' icon is highlighted with a red box. The main area is titled 'active directory' and shows the 'Contoso Corp...' group details. The group name is 'Contoso Corp...', status is 'アクティブ' (Active), and it has '全権管理者' (Full administrator) assigned. Below this, it lists 'すべての Contoso C...' (All Contoso C...), 'アジア・ヨーロッパ, ...' (Asia-Pacific, ...), and '日本' (Japan). At the bottom of the main area, there are '戻る' (Back) and '?' buttons.

2. [Contoso corporation] 画面で、[構成] をクリックします。

contoso corporation

ユーザー グループ アプリケーション ドメイン ディレクトリ統合 **構成** レポート ライセンス

ディレクトリを使用する準備ができました。

作業開始するためのオプションは次のとおりです。

□ 次回アクセス時はクリックスタートをスキップする

1 ユーザー サインイン エクスペリエンスの向上

ユーザーが使い慣れたユーザー名でサインインできるように、カスタムドメインを追加します。たとえば、組織のドメインが 'contoso.com' である場合、ユーザーは Azure AD に 'joe@contoso.com' のようなユーザー名でサインインできます。

3. [構成] 画面で、[グループ管理] - [委任されたグループ管理を有効にしました] が [はい] になっていることを確認します。[はい] でない場合は、[はい] に設定し、[保存] してください。

グループ管理

委任されたグループ管理を有効にしました **はい** いいえ

ユーザーはセキュリティグループを作成できます **はい** いいえ フレビュー

USERS WHO CAN USE SELF-SERVICE FOR SECURITY GROUPS **すべて** SOME フレビュー

ユーザーは O365 グループを作成できます **はい** いいえ フレビュー

USER WHO CAN USE SELF-SERVICE FOR O365 GROUPS **すべて** SOME フレビュー

専用グループの有効化 **はい** いいえ フレビュー

Microsoft Azure 自習書 No.18
Microsoft Azure Active Directory の活用

4. [構成] 画面で、[グループ] をクリックします。

The screenshot shows the Microsoft Azure Active Directory 'Configure' page for the 'contoso corporation' tenant. The top navigation bar includes tabs for 'User', 'Groups' (which is highlighted with a red box), 'Application', 'Domain', 'Directory Integration', 'Configure' (highlighted with a red box), 'Report', and 'License'. The main content area displays the 'Contoso Corporation' configuration settings, including sections for 'Directors' properties, 'Notification' (with language set to 'Japanese'), and 'Multi-factor authentication'. At the bottom, there is a 'New' button and a help icon.

5. [Contoso corporation] 画面で、管理者グループの [Admins] をクリックします。

The screenshot shows the Microsoft Azure Active Directory 'Groups' page for the 'contoso corporation' tenant. The 'Groups' tab is selected. A red box highlights the 'Admins' group in the list. The table lists various groups, including 'ADSyncAdmins', 'ADSyncBrowse', 'ADSyncOperators', 'ADSyncPasswordSet', 'DnsAdmins', 'DnsUpdateProxy', 'Sales', 'SSPR セキュリティ グループ ユーザー', and 'WinRMRremoteWMIUsers_'. The 'Admins' group is identified as a 'Administrators group' under 'Microsoft Azure Active Directory'. At the bottom, there are buttons for 'Groups addition' and 'Delete'.

Microsoft Azure 自習書 No.18
Microsoft Azure Active Directory の活用

6. [admins] 画面で、[所有者] をクリックします。

The screenshot shows the Microsoft Azure Active Directory Admin Center interface. On the left, there's a sidebar with various icons and a list of groups: Admins, ADSyncAdmins, ADSyncBrowse, ADSyncOperators, ADSyncPasswordSet, DnsAdmins, DnsUpdateProxy, Sales, SSPR セキユリティ..., and WinRMRemoteWM... A red box highlights the 'Owners' tab in the top navigation bar. The main area displays the 'admins' group details, including a table with columns '名前' (Name) and 'ユーザー名' (User name). One entry is shown: 'Contoso 管理者' with the user name 'admin@contoso.com'. Navigation arrows are at the bottom of the table.

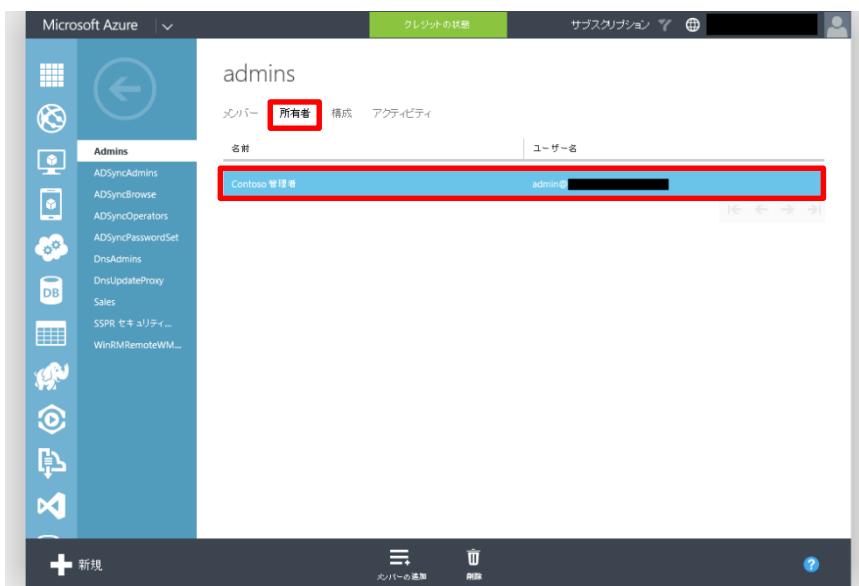
7. [admins] 画面で、[所有者の追加] をクリックします。

The screenshot shows the Microsoft Azure Active Directory Admin Center interface. The 'Owners' tab is selected. A message 'このグループには所有者がいません。' (No owners are present in this group) is displayed. Below this message, there is a button labeled '所有者の追加' with a plus sign icon, which is highlighted with a red box. The rest of the interface is identical to the previous screenshot, showing the group list and navigation elements.

8. [所有者の追加] 画面で、[Contoso 管理者] をクリックし、チェック マークをクリックして完了します。



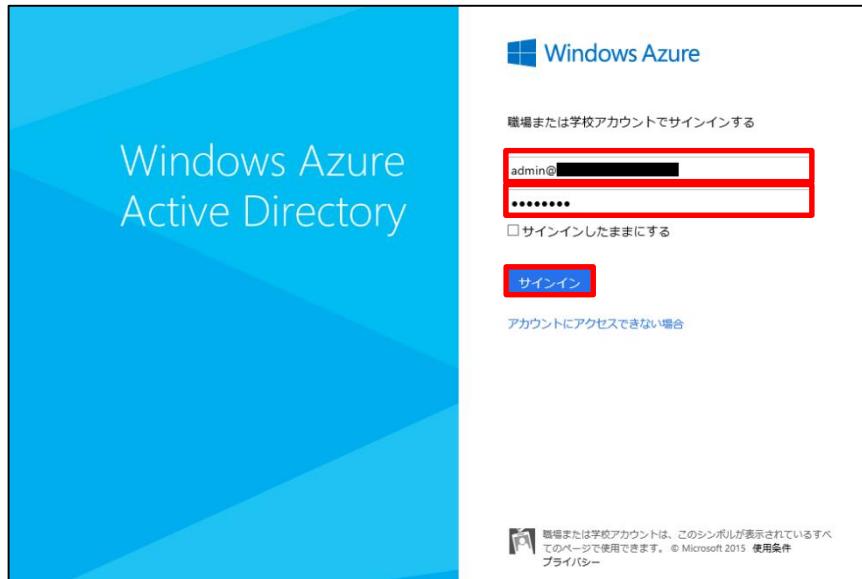
9. [admins] 画面で、[所有者] に [Contoso 管理者] が追加されたことを確認します。



10. InPrivate ブラウズで Internet Explorer を起動し、アクセス パネルの URL である

<http://myapps.microsoft.com/> にアクセスします。

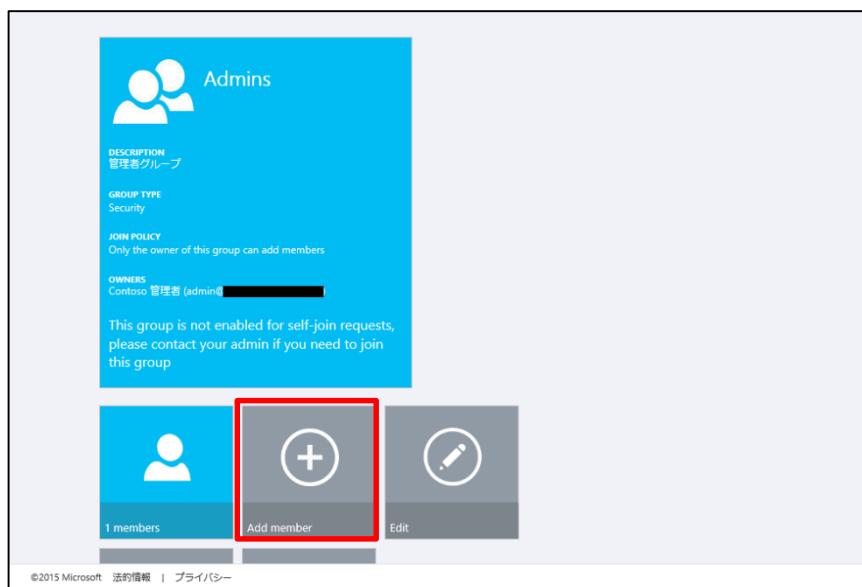
アクセス パネルの Web サイトで、admin@<Microsoft Azure に登録されたドメイン名>ユーザーでサインインします。

**11.** アクセス パネル画面で、[グループ] メニューをクリックします。

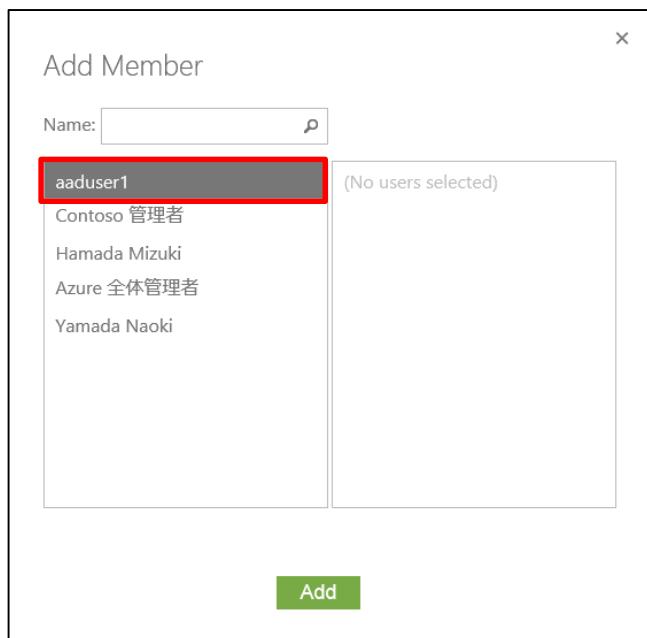
12. [グループ] 画面で、[Admins] グループをクリックします。



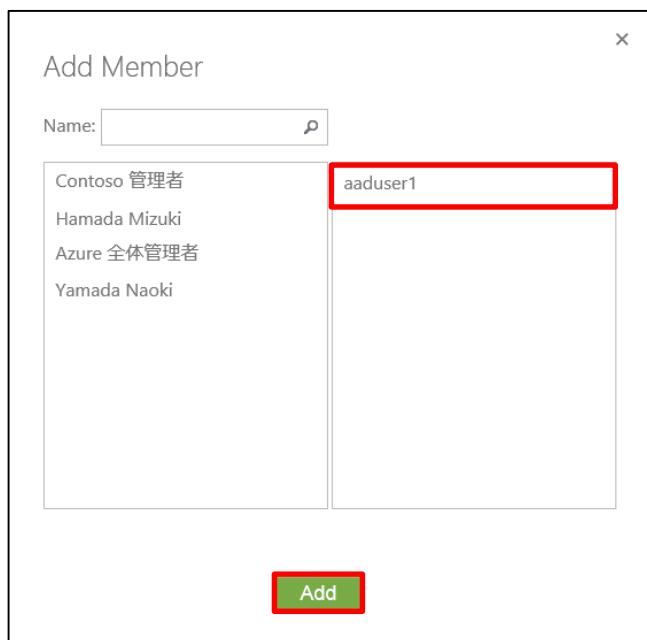
13. アクセス パネル画面で、[Admins] グループの詳細が確認できます。メニューから [Add member] をクリックします。



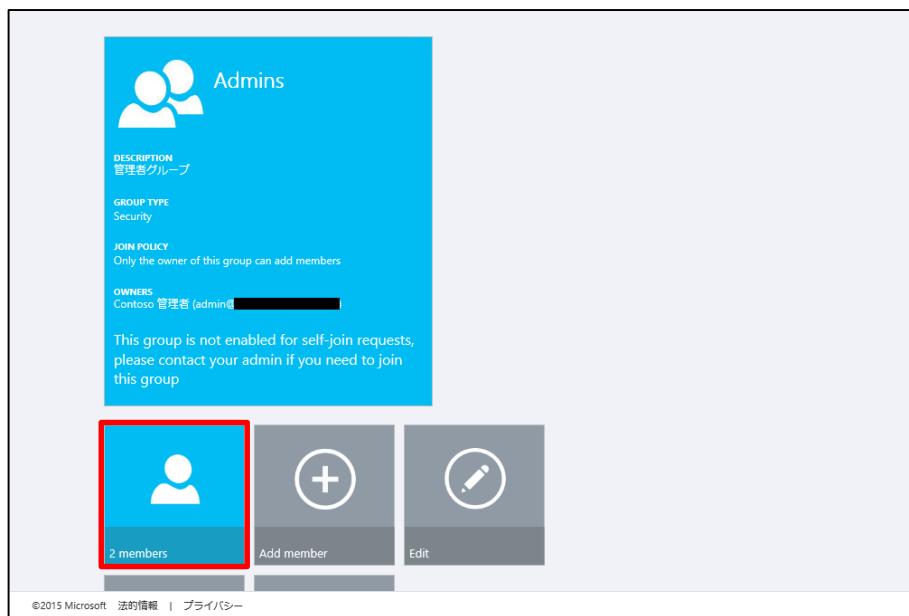
14. [Add member] 画面で、[aaduser1] をクリックします。



15. [Add member] 画面で、[aaduser1] が右側に移動したことを確認し、[Add] をクリックします。



16. アクセス パネル画面で、[2 members] をクリックします。



17. [Admins] 画面で、Admins グループに aaduser1 ユーザーが追加されていることを確認します。



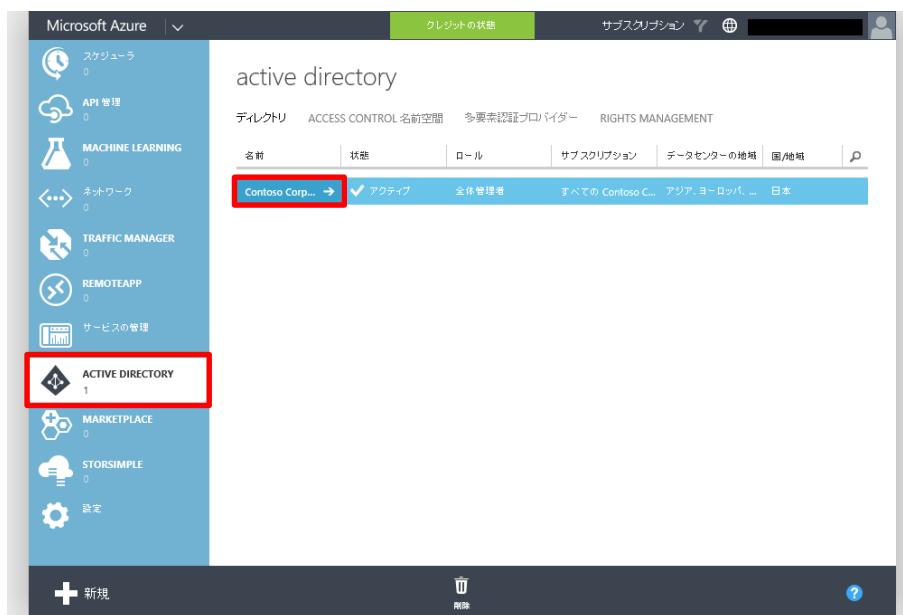
4.9 セルフサービス パスワード リセット

本手順では、Azure AD Premium ライセンスで提供されるセルフサービス パスワード リセットを設定し、パスワードを忘れたユーザーが本人確認を行った後、パスワードをリセットできる様子を確認します。

なお、前半部分では「Azure AD ユーザーのパスワード リセット」として Azure AD に直接作成されたユーザー aaduser1 のパスワード リセットを行います。

また、後半部分ではディレクトリ同期ツールを利用して作成された Hamada.Mizuki ユーザーのパスワード リセットを行い、ディレクトリ同期によってオンプレミス Active Directory のユーザーのパスワードもリセットされることを確認します。ディレクトリ同期ツールに AADSync と DirSync を利用している場合で手順が異なるため、利用しているディレクトリ同期ツールに合わせた手順に沿って進めてください。

1. Microsoft Azure 管理ポータル画面で、[ACTIVE DIRECTORY] をクリックし、[Contoso corporation] をクリックします。



2. [Contoso corporation] 画面で、[構成] をクリックします。

contoso corporation

ユーザー グループ アプリケーション ドメイン ディレクトリ統合 構成 レポート ライセンス

ディレクトリを使用する準備ができました。

作業開始するためのオプションは次のとおりです。

次回アクセス時はクリックスタートをスキップする

行う操作 ディレクトリのセットアップ アクセスの管理 アプリケーションの削除

作業を開始する

1 ユーザー サインイン エクスペリエンスの向上

ユーザーが使い慣れたユーザー名でサインインできるように、カスタムドメインを追加します。たとえば、組織のドメインが 'contoso.com' である場合、ユーザーは Azure AD に 'joe@contoso.com' のようなユーザー名でサインインできます。

3. [構成] 画面で、[ユーザー パスワードのリセット ポリシー] - [パスワードのリセットが有効になっているユーザー] - [はい] をクリックします。

Microsoft Azure | プロジェクトの状態 サブスクリプション ヘルプ

Contoso Corporat...

ユーザー パスワードのリセット ポリシー

パスワードのリセットが有効になっているユーザー はい いいえ

パスワード リセットへのアクセスの制限 はい いいえ プレビュー

ユーザーがパスワードをリセットするには、そのユーザーが事前に少なくとも 1 つの認証方法を定義していることが必要です。'Contoso Corporation' のユーザーを今すぐ編集します。

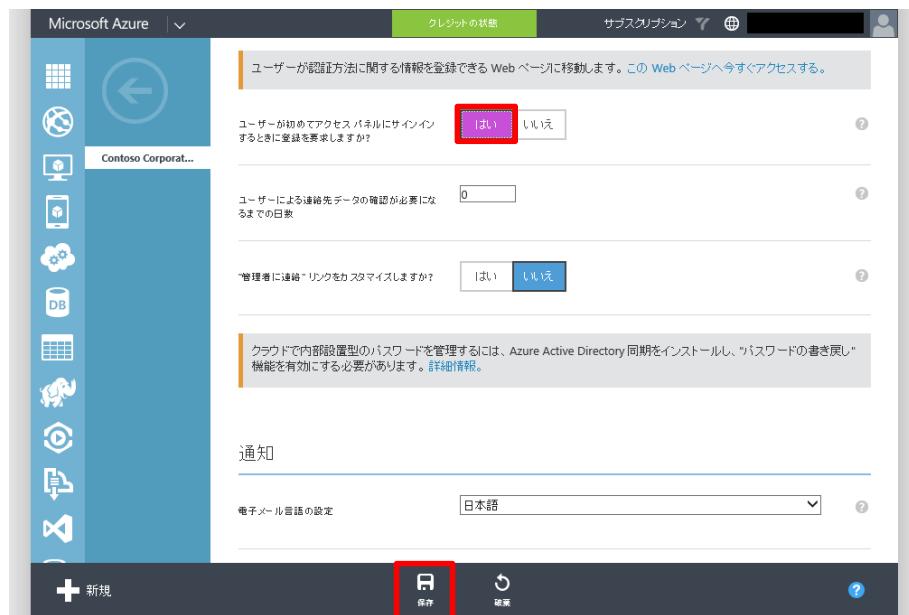
ユーザーが使用できる認証方法 会社電話 携帯電話 連絡用電子メール アドレス 秘密の質問 プレビュー

必要な認証方法の数 1

ユーザーが認証方法に関する情報を登録できる Web ページに移動します。この Web ページへ今すぐアクセスする。

Microsoft Azure Active Directory の活用

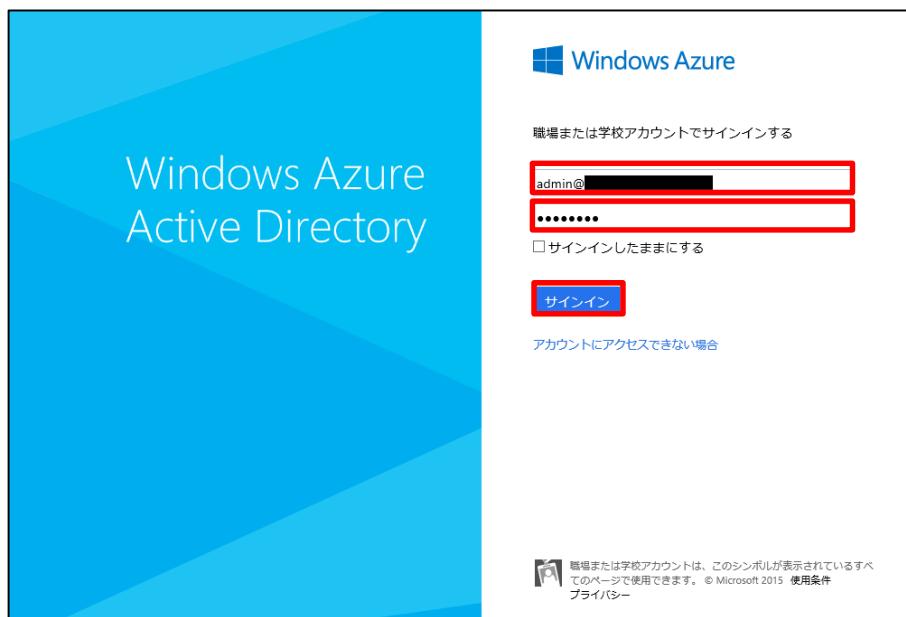
4. [構成] 画面で、[ユーザーが初めてアクセスパネルにサインインするときに登録を要求しますか?] - [はい] をクリックし、[保存] をクリックします。



◆ Azure AD ユーザーのパスワード リセット

Microsoft Azure 管理ポータルから直接作成されたユーザー（Azure AD ユーザー）のパスワードをリセットする場合、アクセス パネルからパスワードのリセットを行います。パスワードのリセットを行うには事前に本人確認の方法を設定しておく必要があるため、本手順ではアクセスパネルで本人確認の設定として電話番号を設定したのち、パスワードのリセットを行います。

1. InPrivate ブラウズで Internet Explorer を起動し、アクセス パネルの URL である <http://myapps.microsoft.com/> にアクセスします。
アクセス パネルの Web サイトで、aaduser1@<Microsoft Azure に登録されたドメイン名>ユーザーでサインインします。

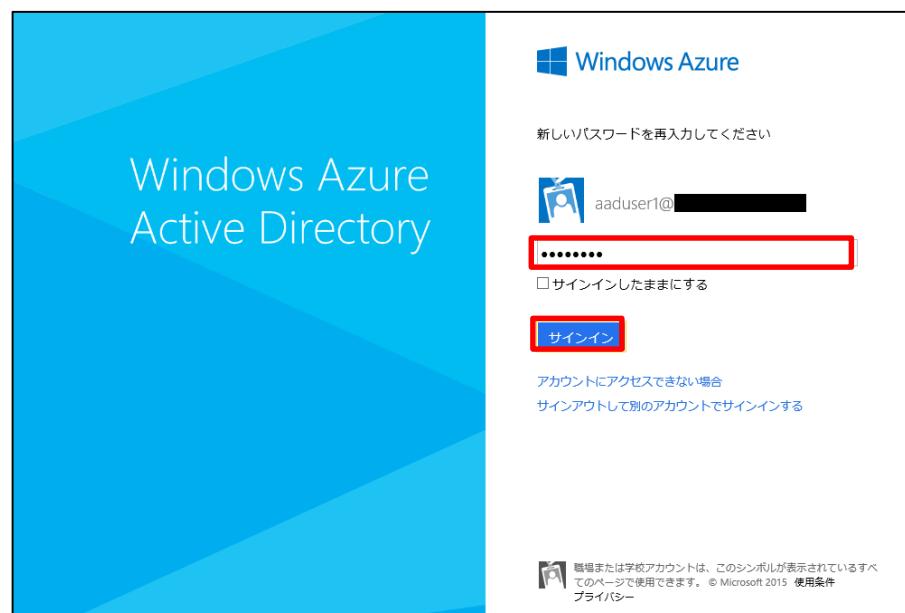


Microsoft Azure Active Directory の活用

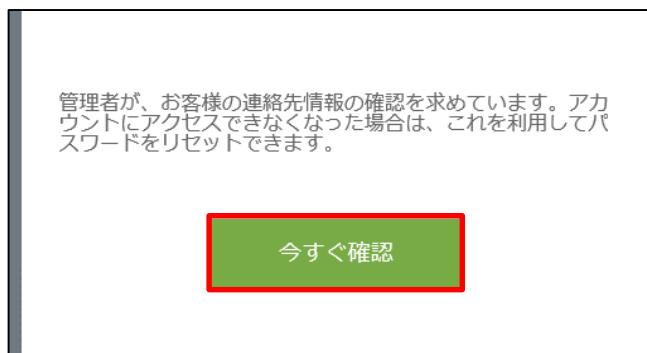
2. aaduser1 ユーザーで初めてサインインした場合、パスワードの変更を要求されます。[パスワードの変更] 画面で、[古いパスワード] には、サインインに使用したパスワードを入力し、[新しいパスワードの作成] と [新しいパスワードの確認入力] には新しいパスワードを入力して、[送信] をクリックします。



3. アクセス パネルの Web サイトのサインイン画面で、新しいパスワードを入力し、サインインをクリックします。



4. アクセス パネル画面で、[今すぐ確認] をクリックします。



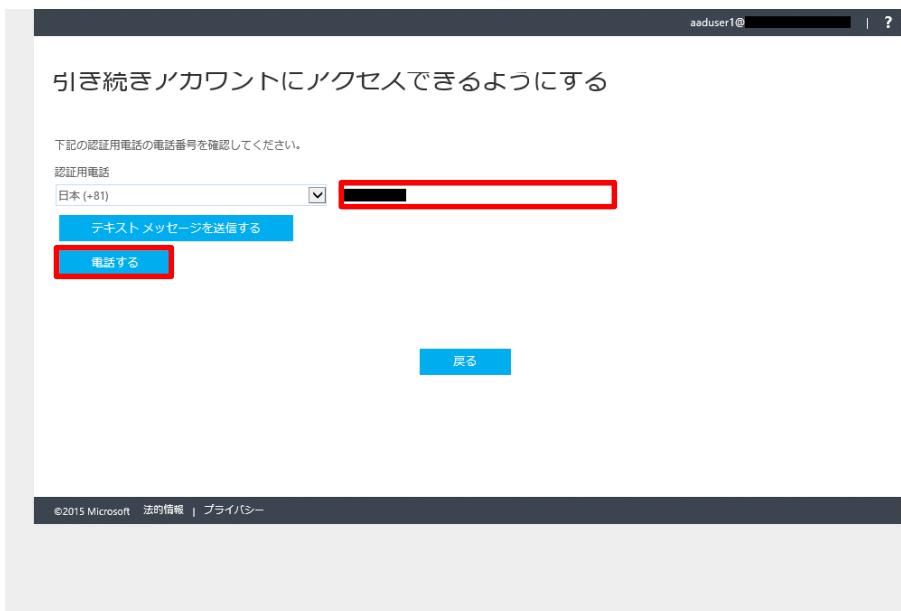
【Note:】

[今すぐ確認] メニューが表示されない場合、時間を置いてから再度アクセス パネルにサインインして下さい。

5. [引き続きアカウントにアクセスできるようにする] 画面で、パスワード リセットの本人確認で使用する電話番号またはメール アドレスを登録します。本手順では、電話を使用するため、[認証用電話が構成されていません。] の [今すぐセットアップ] をクリックします。



6. [引き続きアカウントにアクセスできるようにする] 画面で、[認証用電話] 欄に電話番号（電話番号の先頭の 0 を除いた番号）を入力し、[電話する] をクリックします。



【Note:】

[電話する] ボタンをクリックすると、設定した電話番号に着信があります。音声ガイダンスに従って本人確認を行うことになります。

一方、[電話する] ボタンの代わりに、[テキストメッセージを送信する] ボタンをクリックした場合、携帯電話の SMS メッセージによって確認コード番号が送信されます。受信した確認コード番号を画面に入力することで本人確認を行います。

7. 前の手順で登録した電話番号に着信があります。音声ガイダンスに従って、電話の # ボタンを押すと、サインイン（本人確認）が完了します。この時点で、認証用電話番号の設定が完了したことになります。[完了] をクリックします。



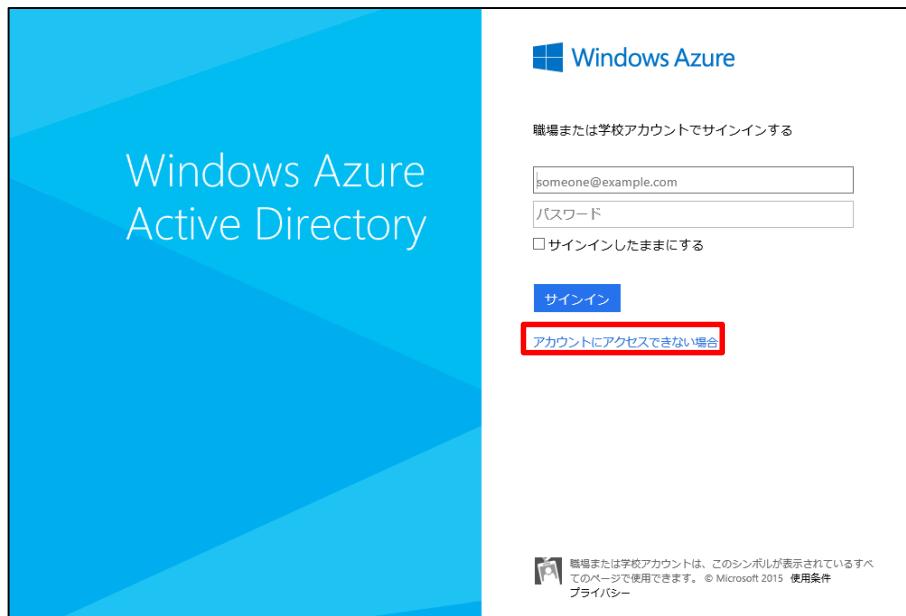
【Note:】

認証用電子メールを同時にセットアップすることも可能です。認証用電子メールでは、確認コードが電子メールで送信されるので、メールに記載された確認コードを入力することで本人確認を行います。

8. アクセス パネル画面で、画面上部のユーザー名をクリックし、[Sign out] をクリックします。



9. アクセス パネルのサインイン画面で、[アカウントにアクセスできない場合] をクリックします。



10. [パスワードのリセット] 画面で、[ユーザー ID] と表示されている画像文字を入力し、[次へ] をクリックします。



11. [パスワードのリセット] 画面で、確認に使用する連絡方法を選択します。本手順では、[携帯電話に発信] をクリックし、電話番号（電話番号の先頭の 0 を除いた番号）を入力して、[発信] をクリックします。



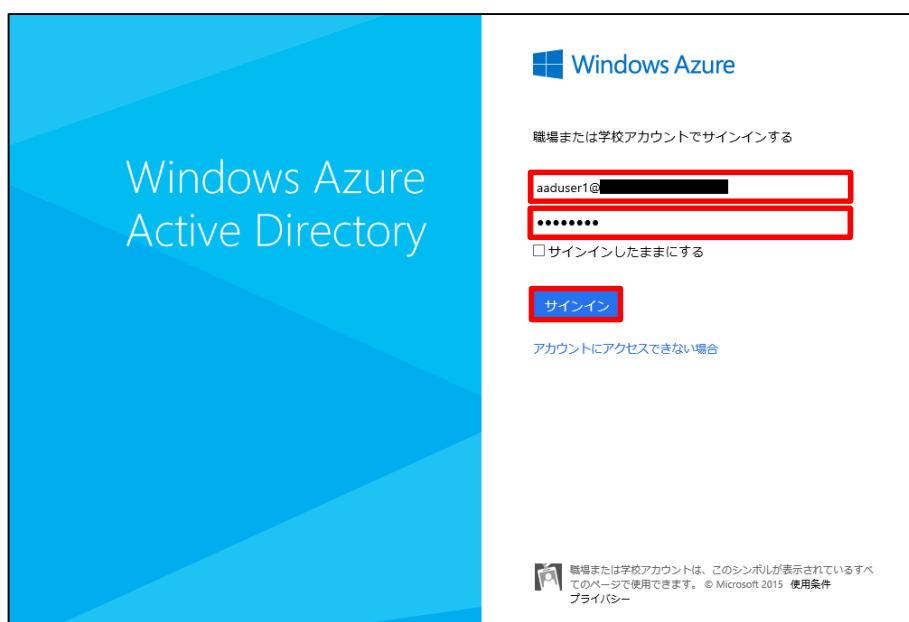
12. 前の手順で入力した電話番号に着信があります。着信した電話に応答したら、音声ガイダンスに従って、電話の # ボタンを押します。すると、[パスワードのリセット] 画面が自動的に表示されます。[新しいパスワードの入力] と [新しいパスワードの確認入力] に新しいパスワードをそれぞれ入力し、[完了] をクリックします。



13. [パスワードのリセット] 画面で、パスワードがリセットされたことが確認できます。そのまま新しいパスワードでサインインする場合は、[ここをクリック] をクリックします。



14. アクセス パネルのサインイン画面で、ユーザー名と新しいパスワードをそれぞれ入力し、[サインイン] をクリックします。



15. 新しいパスワードでサインインできたことを確認します。



◆ ディレクトリ同期ユーザーのパスワード リセット (AADSync の場合)

ディレクトリ同期ツールを利用して登録されたユーザー（ディレクトリ同期ユーザー）のパスワードをリセットする場合、Azure AD 上のユーザー パスワードだけでなく、オンプレミス Active Directory ユーザーのパスワードもリセットしなければなりません。そのため、事前設定としてディレクトリ同期ツールで Azure AD 側で設定したパスワードがオンプレミス Active Directory に同期されるように構成してからパスワード リセットの機能を利用開始します。

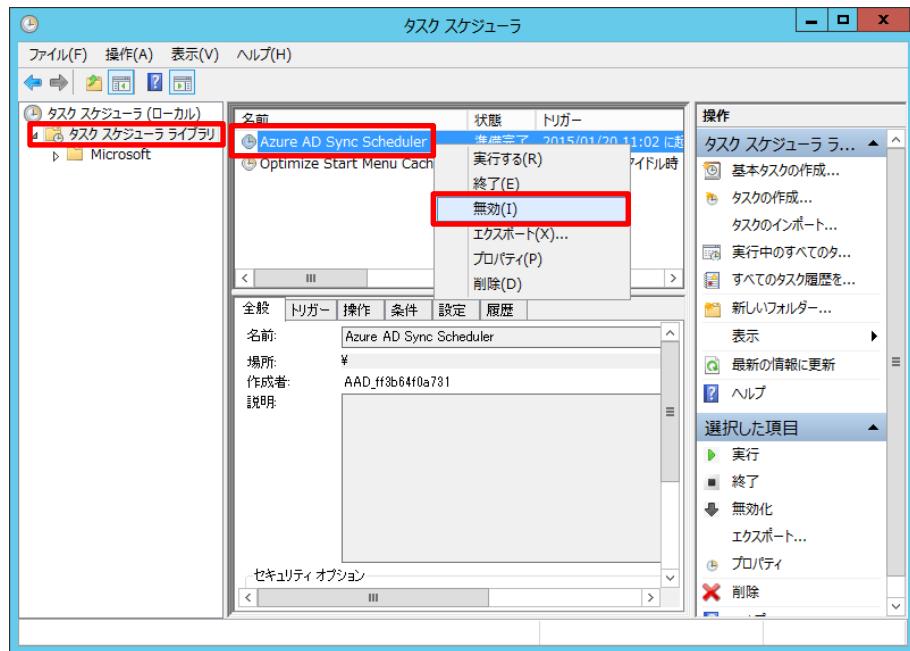
本手順では、AADSync を利用してディレクトリ同期ツールを実装している場合の手順を確認します。

1. WS2012-DC01 コンピューターで操作します。

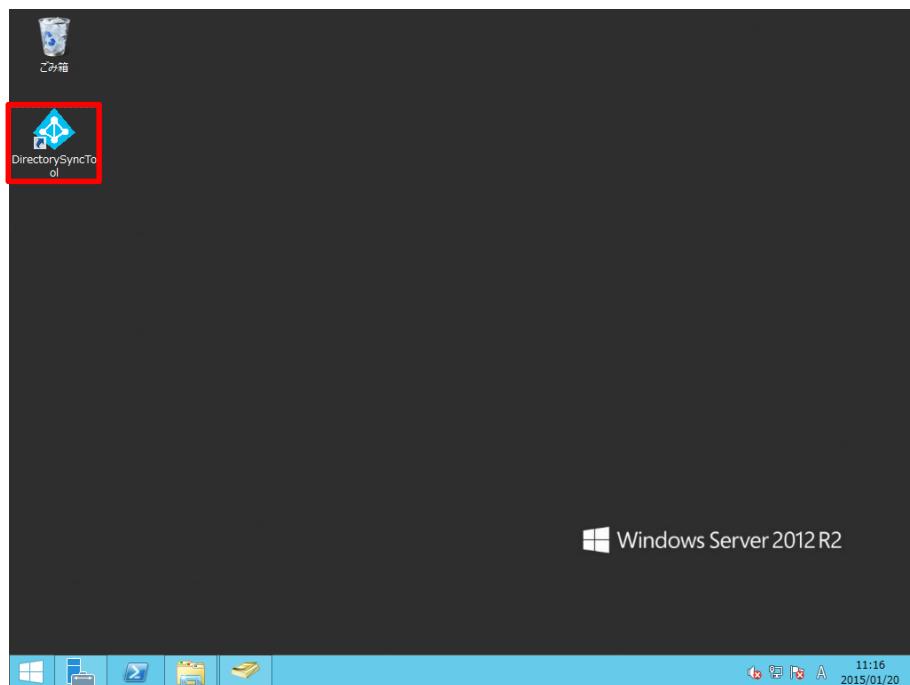
[サーバー マネージャー] 画面で、[ツール] - [タスク スケジューラ] をクリックします。



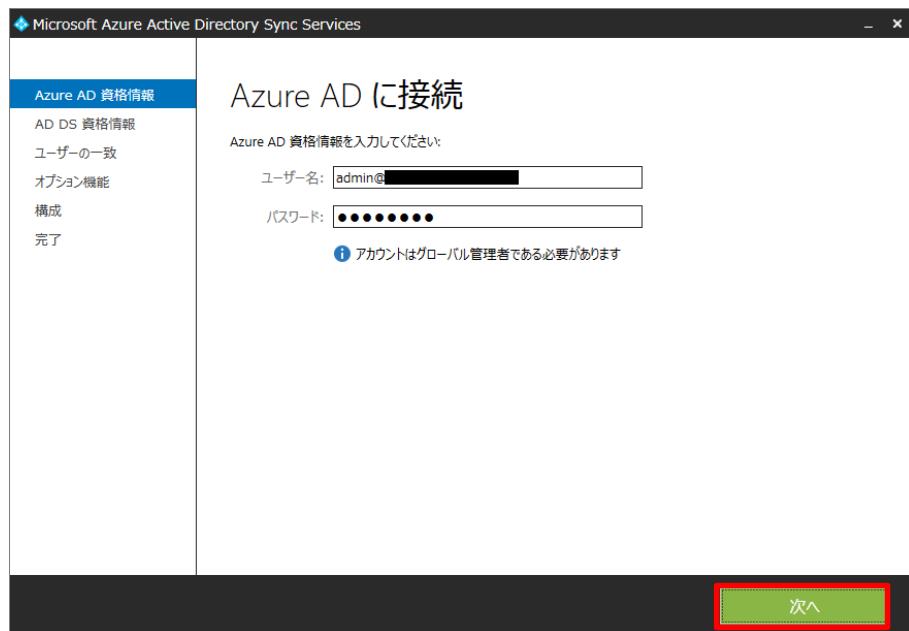
2. [タスク スケジューラ] 画面で、[タスク スケジューラ ライブラリ] をクリックし、中央上ペインの [Azure AD Sync Scheduler] を右クリックして [無効] をクリックします。画面を最小化します。(タスクスケジューラ画面を閉じないでください。)



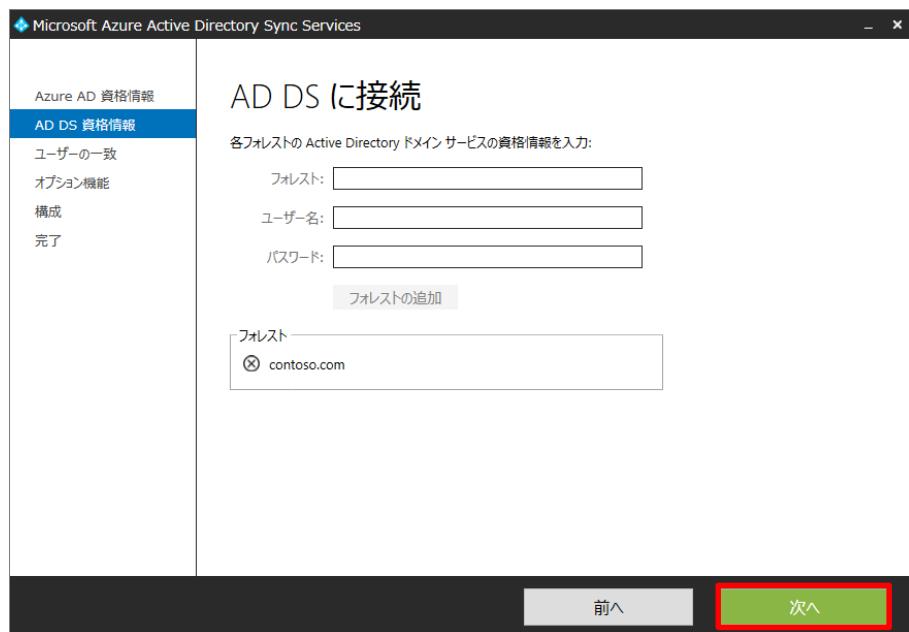
3. WS2012-DC01 コンピューターのデスクトップ画面で、[DirectorySyncTool] アイコンをダブルクリックします。



4. [Azure AD に接続] 画面で、[次へ] をクリックします。

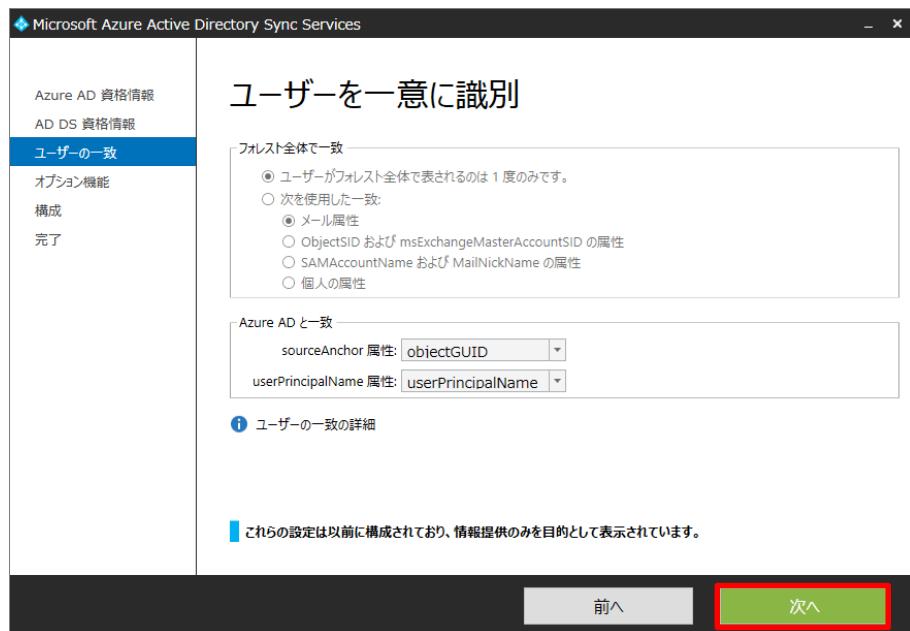


5. [AD DS に接続] 画面で、[次へ] をクリックします。

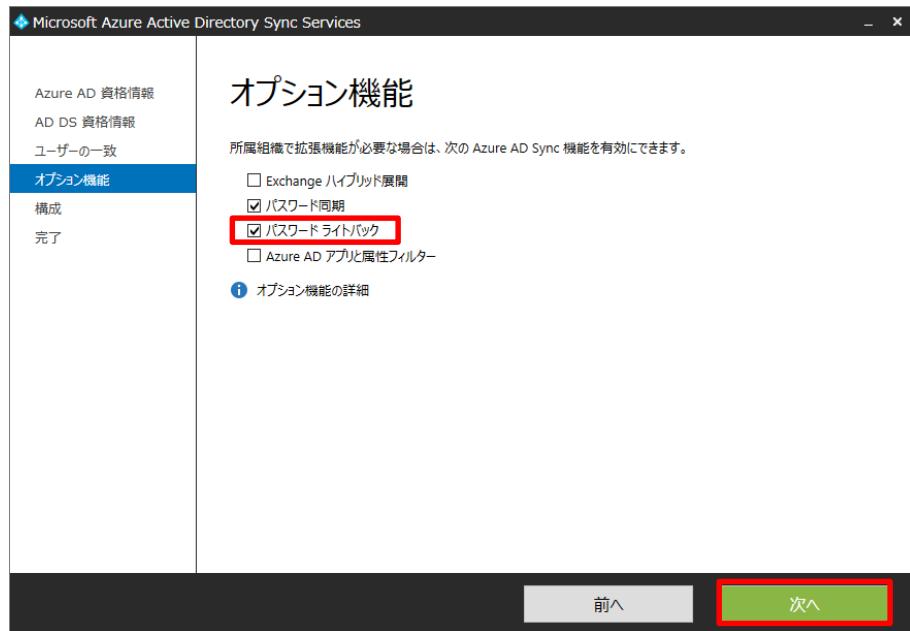


Microsoft Azure 自習書 No.18
Microsoft Azure Active Directory の活用

6. [ユーザーを一意に識別] 画面で、[次へ] をクリックします。

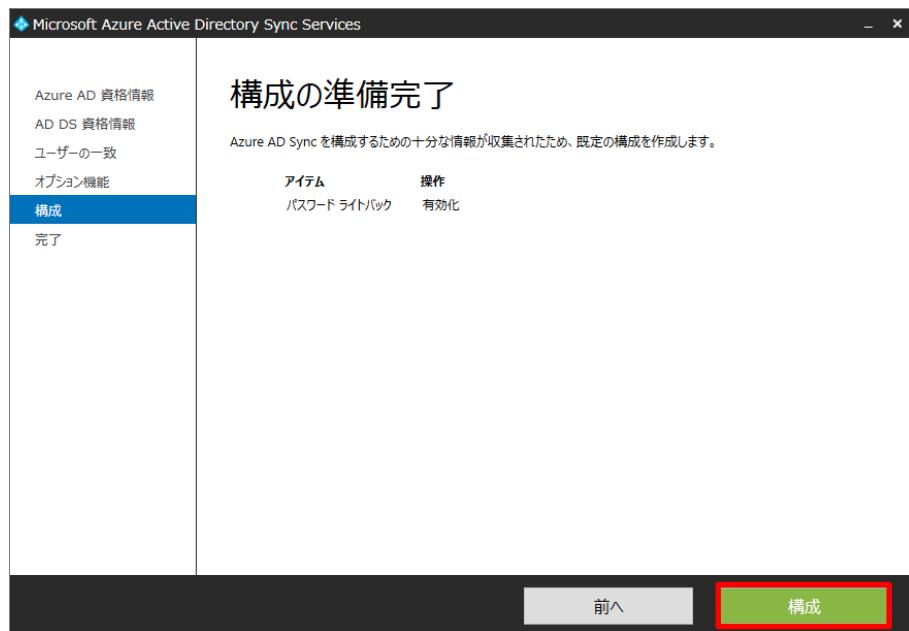


7. [オプション機能] 画面で、[パスワード ライトバック] にチェックをつけ、[次へ] をクリックします。

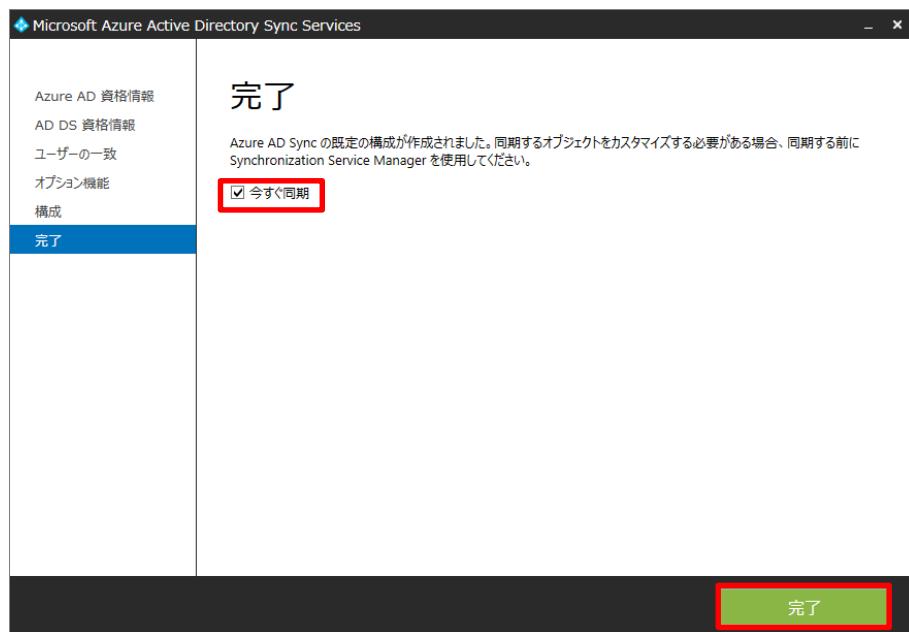


Microsoft Azure 自習書 No.18
Microsoft Azure Active Directory の活用

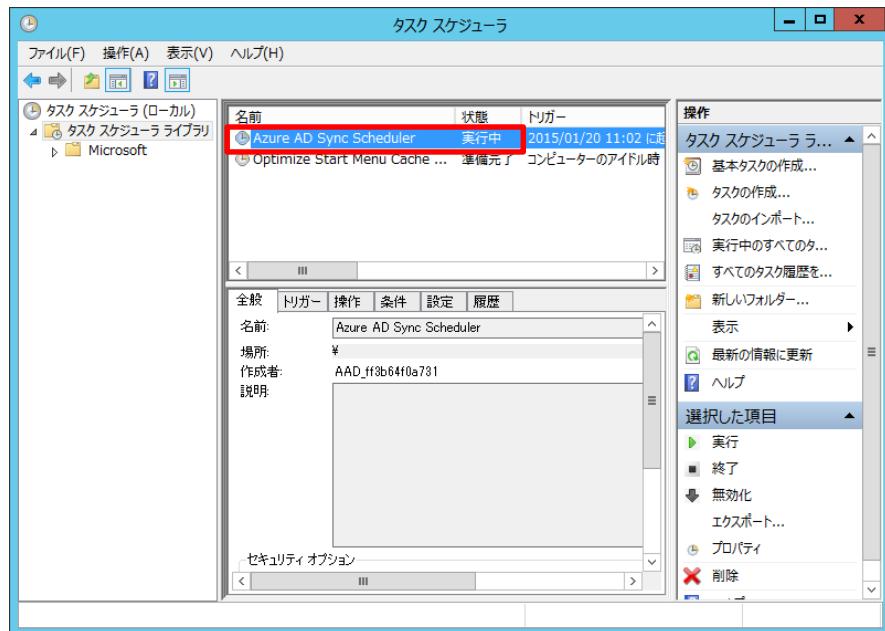
8. [構成の準備完了] 画面で、[構成] をクリックします。



9. [完了] 画面で、[今すぐ同期] にチェックが入っていることを確認し、[完了] をクリックします。



10. [タスク スケジューラ] 画面を最大化します。[タスク スケジューラ] 画面で、中央上ペインの [Azure AD Sync Scheduler] の状態が [実行中] または [準備完了] のいずれかの状態に変化していることを確認します。



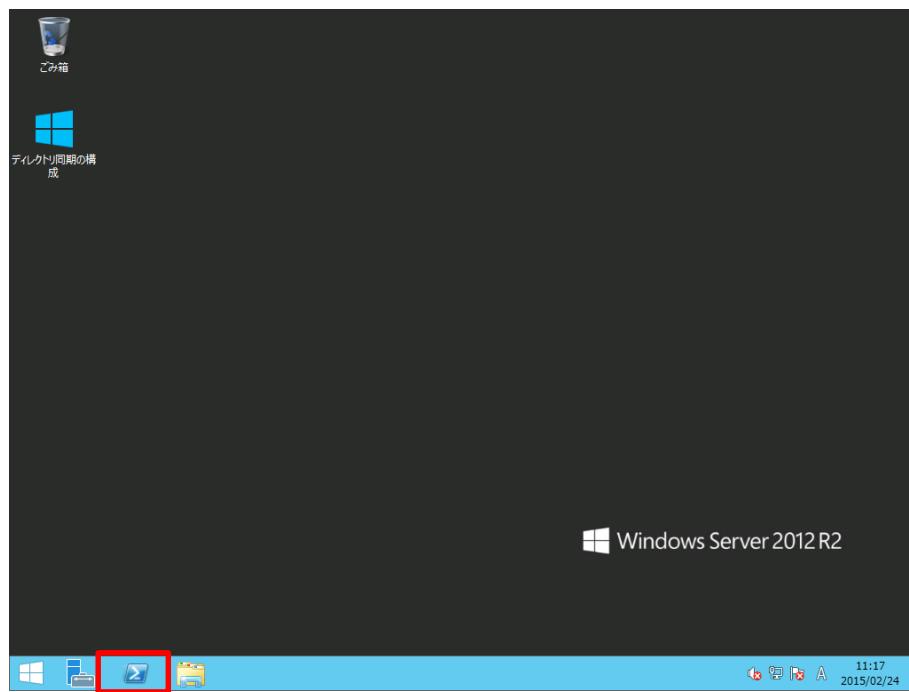
◆ ディレクトリ同期ユーザーのパスワード リセット (DirSync の場合)

ディレクトリ同期ツールを利用して登録されたユーザー（ディレクトリ同期ユーザー）のパスワードをリセットする場合、Azure AD 上のユーザー パスワードだけでなく、オンプレミス Active Directory ユーザーのパスワードもリセットしなければなりません。そのため、事前設定としてディレクトリ同期ツールで Azure AD 側で設定したパスワードがオンプレミス Active Directory に同期されるように構成してからパスワード リセットの機能を利用開始します。

本手順では、DirSync を利用してディレクトリ同期ツールを実装している場合の手順を確認します。

1. WS2012-DC01 コンピューターで操作します。

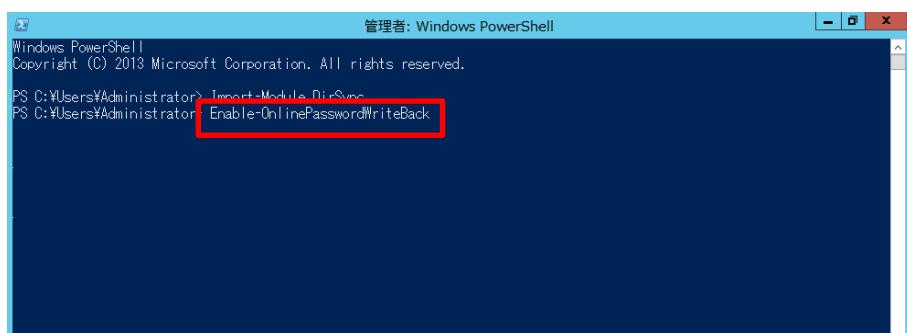
WS2012-DC01 コンピューターのデスクトップ画面で、Windows PowerShell アイコンをクリックします。



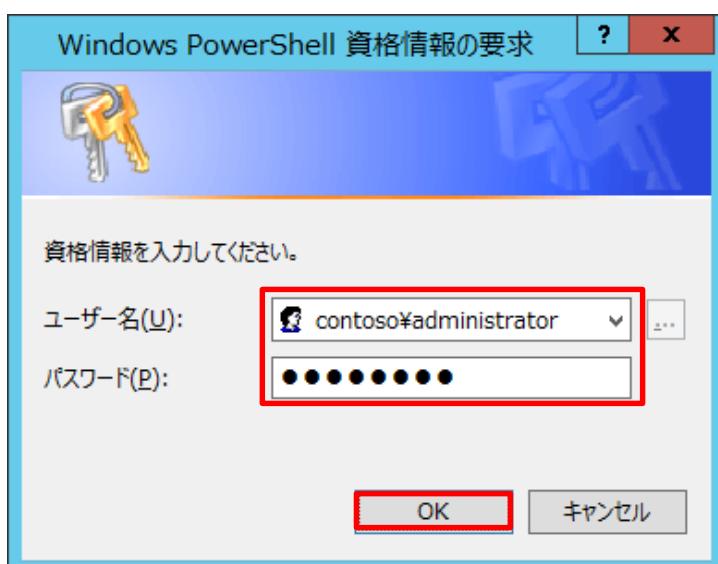
2. [管理者:Windows PowerShell] 画面で、「Import-Module DirSync」と入力し、Enter キーを押します。



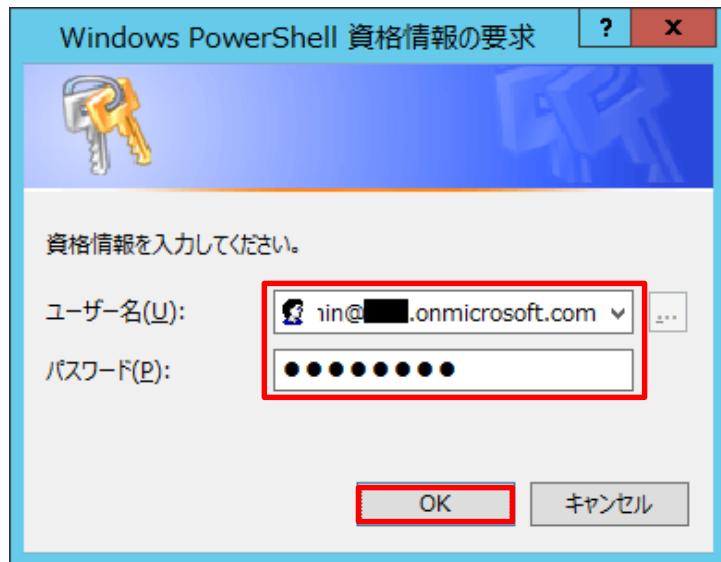
3. [管理者:Windows PowerShell] 画面で、「Enable-OnlinePasswordWriteBack」と入力し、Enter キーを押します。



4. [Windows PowerShell 資格情報の要求] 画面で、Active Directory 管理者のユーザー名とパスワードを入力し、[OK] をクリックします。



5. [Windows PowerShell 資格情報の要求] 画面で、Azure AD 全体管理者のユーザー名とパスワードを入力し、[OK] をクリックします。



6. [管理者:Windows PowerShell] 画面で、セルフサービス パスワード リセットが有効になったことを確認します。

```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\$Users\$Administrator> Import-Module DirSync
PS C:\$Users\$Administrator> Enable-OnlinePasswordWriteBack

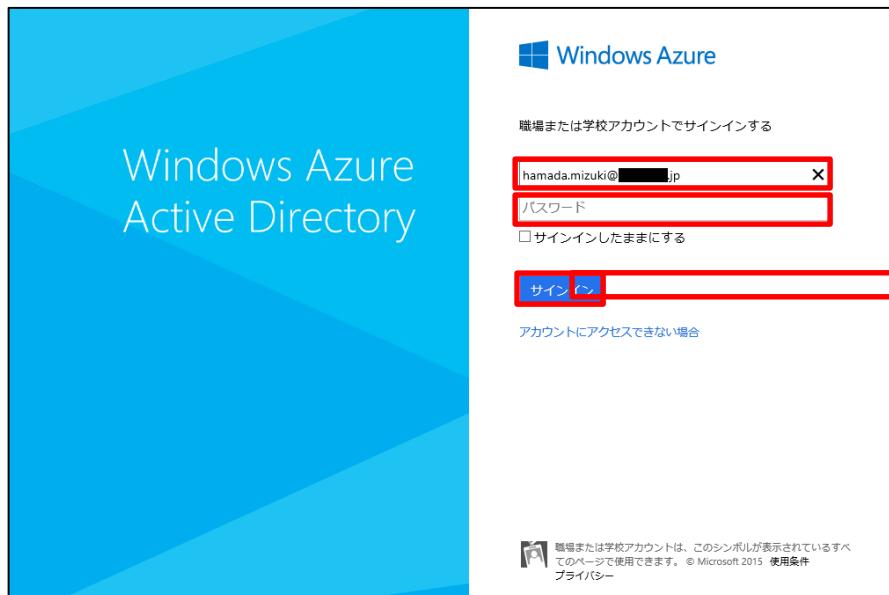
コマンド バイブライン位置 1 のコマンドレット Enable-OnlinePasswordWriteBack
次のパラメーターに値を指定してください:
LocalADCredential|
AzureADCredential|
パスワードのリセットのライトバックが有効になりました。

PS C:\$Users\$Administrator>
```

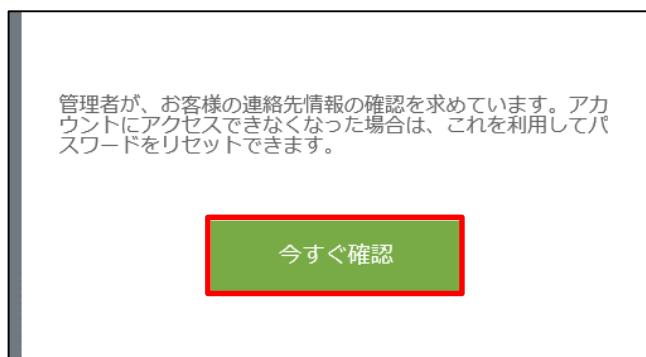
➔ パスワード リセットの実行

本手順では、AADSync または DirSync を利用してパスワード リセットの設定を行った結果を確認するため、パスワード リセットを実行できることを確認します。

1. InPrivate ブラウズで Internet Explorer を起動し、アクセス パネルの URL である <http://myapps.microsoft.com/> にアクセスします。
アクセス パネルの Web サイトで、Hamada.mizuki@<Microsoft Azure に登録されたドメイン名>ユーザーでサインインします。



2. アクセス パネル画面で、[今すぐ確認] をクリックします。



【Note:】

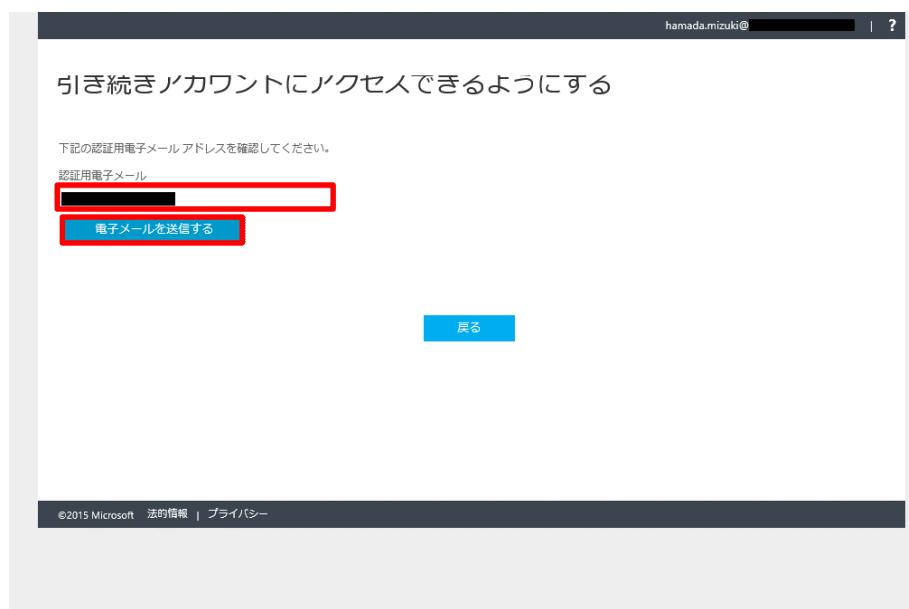
[今すぐ確認] メニューが表示されない場合、時間を置いてから再度アクセス パネルにサインインして下さい。

Microsoft Azure Active Directory の活用

3. [引き続きアカウントにアクセスできるようにする] 画面で、パスワード リセットの本人確認で使用する電話番号またはメール アドレスを登録します。本手順では、メール アドレスを使用するため、メール アドレスの [今すぐセットアップ] をクリックします。



4. [引き続きアカウントにアクセスできるようにする] 画面で、[認証用電子メール] を入力し、[電子メールを送信する] をクリックします。



5. しばらくすると、認証用電子メールで設定したメール アドレスにメールが送信されます。

受信したメールに記載された確認コードを入力し、[確認] をクリックします。



6. 認証用電子メールの設定が完了しました。[完了] をクリックします。

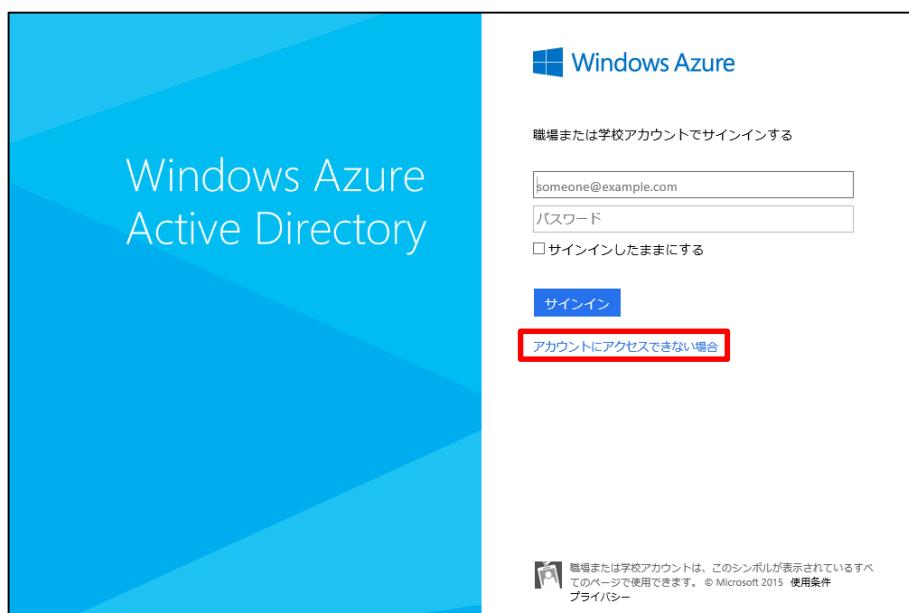
(必要に応じて、もうひとつの本人確認手段である、認証用電話の設定を行うことも可能です。)



7. アクセス パネル画面で、画面上部のユーザー名をクリックし、[Sign out] をクリックします。



8. アクセス パネルのサインイン画面で、[アカウントにアクセスできない場合] をクリックします。



9. [パスワードのリセット] 画面で、[ユーザー ID] と表示されている画像文字を入力し、[次へ] をクリックします。



10. [パスワードのリセット] 画面で、[電子メール] をクリックします。



11. 連絡用電子メール アドレスで受信したメールに記載された確認コードを入力し、[次へ] をクリックします。



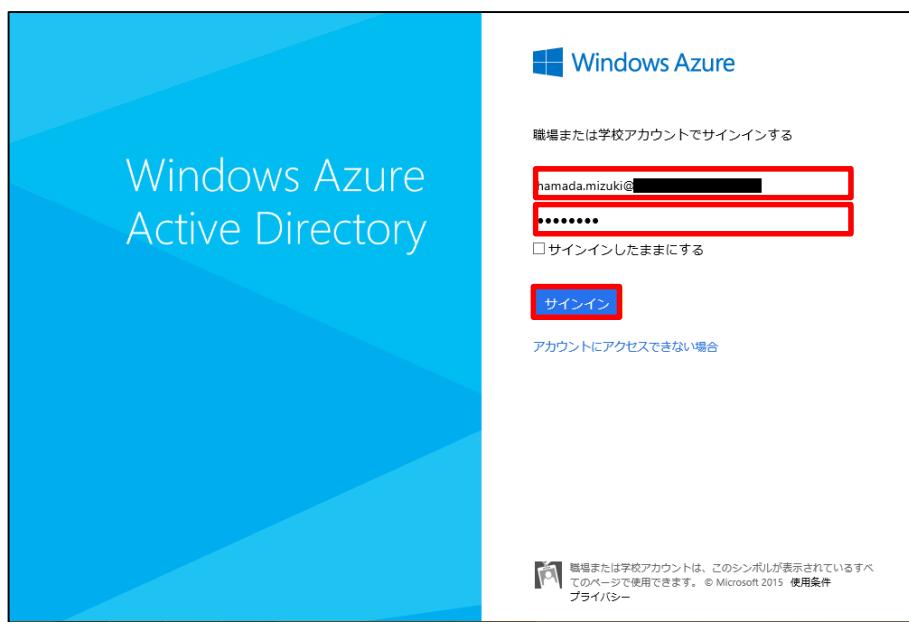
12. [パスワードのリセット] 画面で、[新しいパスワードの入力] と [新しいパスワードの確認入力] にそれぞれ新しいパスワードを入力し、[完了] をクリックします。



13. [パスワードのリセット] 画面で、パスワードがリセットされたことが確認できます。そのまま新しいパスワードでサインインする場合は、[ここをクリック] をクリックします。



14. アクセス パネルのサインイン画面で、ユーザー名と新しいパスワードを入力し、[サインイン] をクリックします。



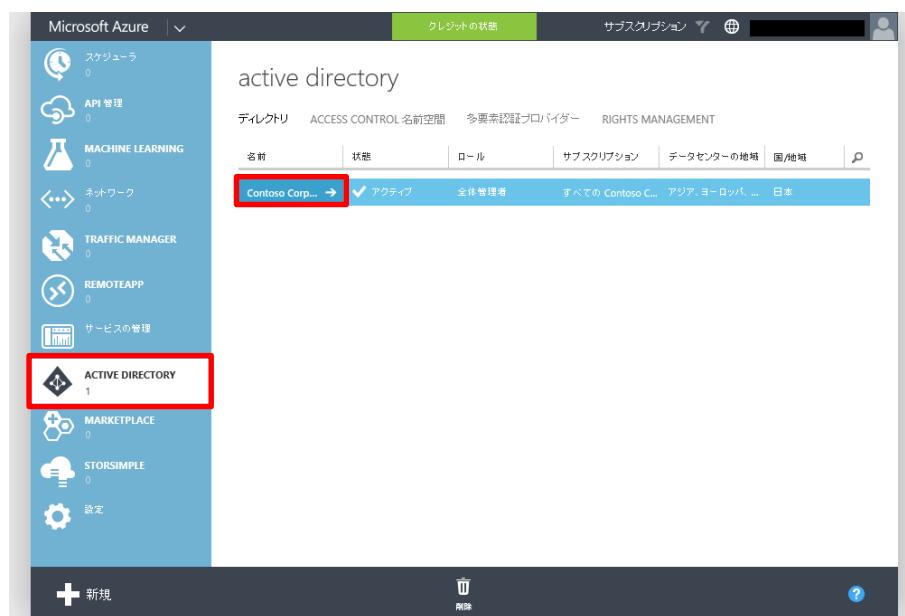
15. 新しいパスワードでサインインできたことを確認します。



4.10 ブランドのカスタマイズ

本手順では、Azure AD ユーザー向けポータル サイトである、アクセス パネルのサインイン画面をカスタマイズし、組織のために最適化されたサインイン画面とアクセス パネル画面を作成します。

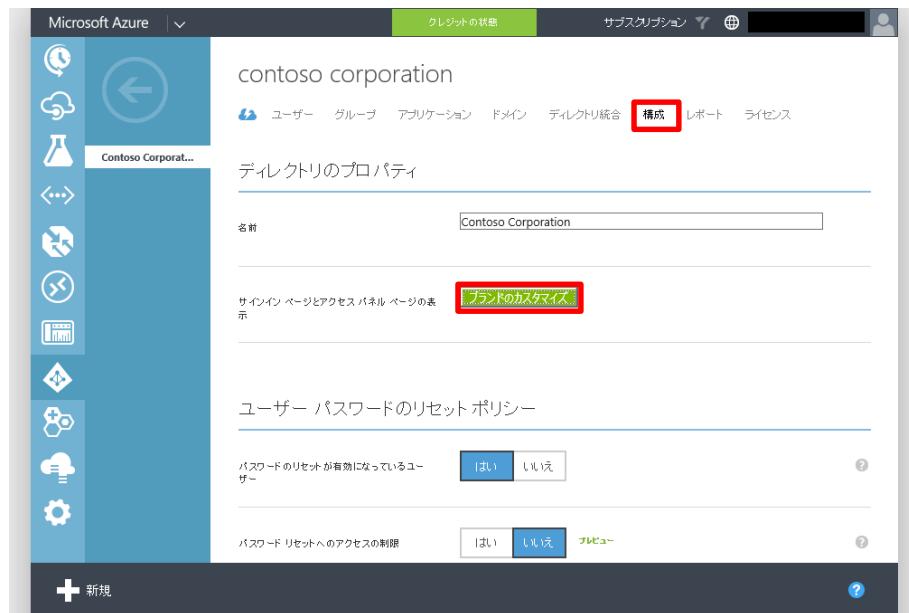
1. Microsoft Azure 管理ポータル画面で、[ACTIVE DIRECTORY] をクリックし、[Contoso corporation] をクリックします。



2. [Contoso corporation] 画面で、[構成] をクリックします。



3. [構成] 画面で、[ブランドのカスタマイズ] をクリックします。



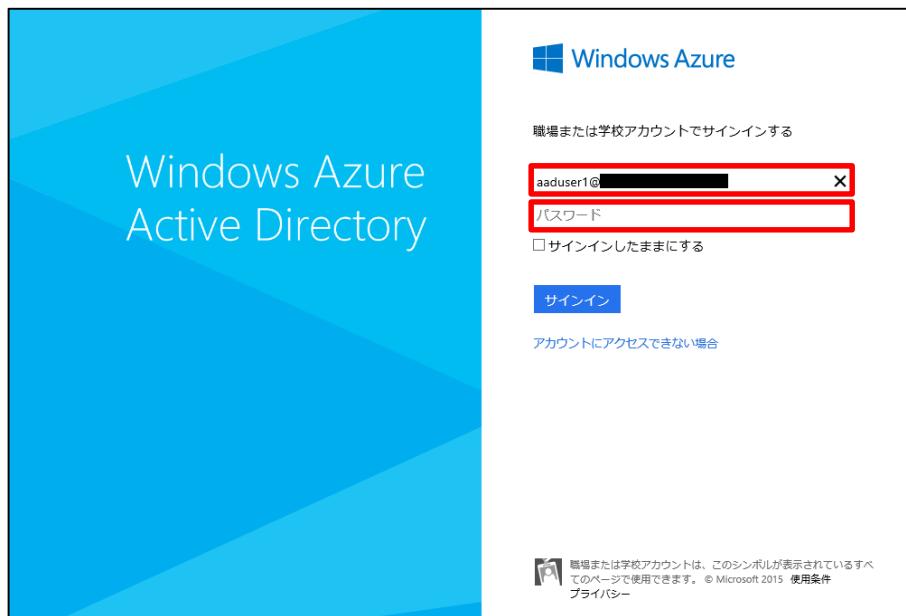
4. [既定ブランドのカスタマイズ] 画面で、[バナー ロゴ(60 × 280 ピクセル)]、[サインイン ページの図]にそれぞれ画像を選択します。[サインイン ページのテキスト] はサインイン ページ内に表示される文章を入力します。設定が完了したら、チェック マークをクリックして完了します。



5. InPrivate ブラウズで Internet Explorer を起動し、アクセス パネルの URL である

<http://myapps.microsoft.com/> にアクセスします。

アクセス パネルの Web サイトで、aaduser1@<Microsoft Azure に登録されたドメイン名>ユーザー名を入力し、パスワード欄をクリックします。



6. ロゴ、サインイン ページの図、サインインページのテキストが、カスタマイズを行った Web ページに切り替わります。パスワードを入力し、サインインします。



【Note:】

アクセスパネル Web ページにアクセスする際、URL を <http://myapps.microsoft.com/> の代わりに <http://myapps.microsoft.com/<Microsoft Azure に登録されたドメイン名>> と入力し、アクセスすると、最初からカスタマイズされた Web ページが表示されます。

7. サインイン後のアクセス パネル画面に、カスタマイズを行ったロゴが表示されます。



STEP 5. Microsoft Azure Active Directory を 利用したアプリケーションへのアクセス

本章では、Azure AD にサインインしたのちにアクセスするアプリケーションの構成方法について解説します。

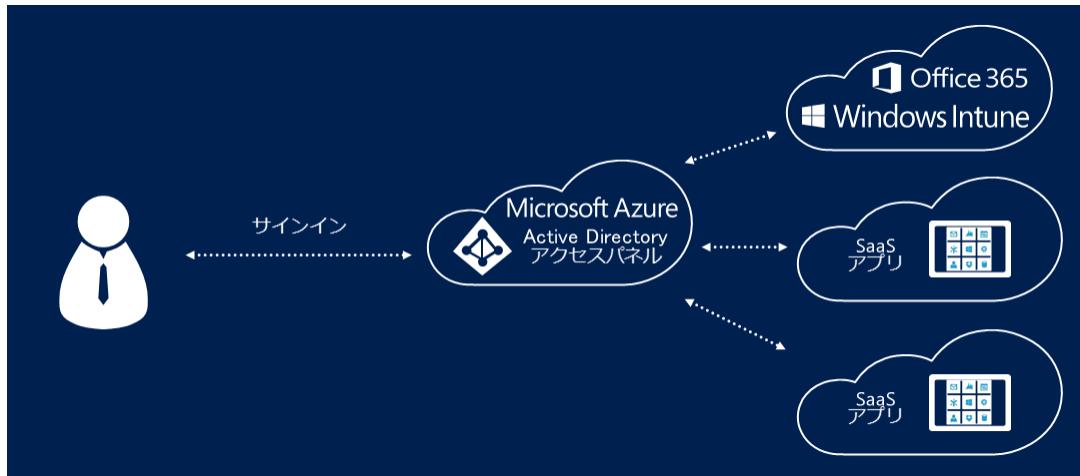
この STEP では、次のことを学習します。

- ✓ SaaS 型アプリケーションの登録
- ✓ 社内アプリケーションの登録
- ✓ レポートによるアプリケーションへのアクセス状況の確認

5.1 Azure AD ユーザーによる SaaS アプリへのアクセス

Azure AD ドメインのユーザーはアクセス パネルを経由して、様々なアプリケーションやサービスに再度サインイン情報を入力することなく（シングルサインオンで）、直接アクセスすることができます。

図 5.1-1 アクセスパネルを経由した SaaS アプリへのアクセス



ポータルサイトからシングルサインオンで各サービスにアクセスする場合、次の 2 つの方法でシングルサインオン アクセスを構成できます。

■ フェデレーション ベースのシングルサインオン

SAML プロトコル等を利用して、トークンの受け渡しによってシングルサインオンを実現する方法です。

■ パスワード ベースのシングルサインオン

シングルサインオンでアクセスするサービスのユーザー名とパスワードをあらかじめ Azure AD に記録させ、サービスへのアクセス時に自動的にユーザー名とパスワードを提示する方法です。この方法でシングルサインオンを行う場合、クライアントコンピューターに Access Panel Extension ツールをインストールしておき、ブラウザーから呼び出せるようにしておく必要があります。

これらのシングルサインオン方法は、アクセスするサービス種類によって利用可能な方法が異なるため、どちらでシングルサインオンを行うかはサービスに依存します。

以上を踏まえ、本節ではアクセス パネルを経由してアクセスさせる SaaS アプリの登録方法を確認します。本手順では、一例としてパスワード ベースのシングルサインオンを行うサービスである Microsoft OneDrive へのアクセスを登録する方法を確認します。

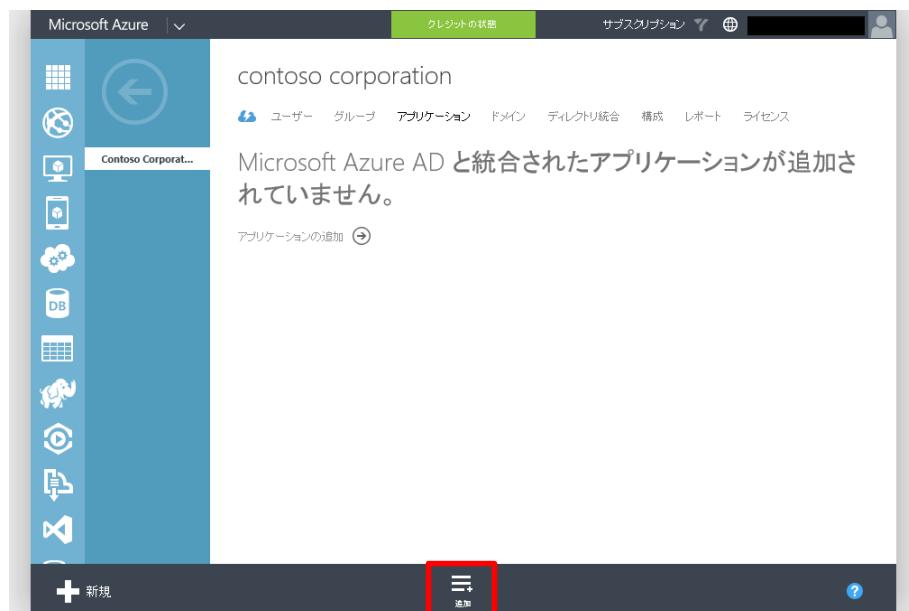
◆ Microsoft Azure 管理ポータルによる SaaS アプリの登録

本手順では、Admins グループのメンバーだけが Microsoft OneDrive にアクセスできるよう、アプリの登録を行います。また、aaduser1 ユーザーでアクセスパネルにアクセスした際には自動的にサインインを行い、Microsoft OneDrive にアクセスできるよう、構成します。

1. Microsoft Azure 管理ポータル画面で、[ACTIVE DIRECTORY] をクリックし、[Contoso corporation] をクリックします。

2. [Contoso corporation] 画面で、[アプリケーション] をクリックします。

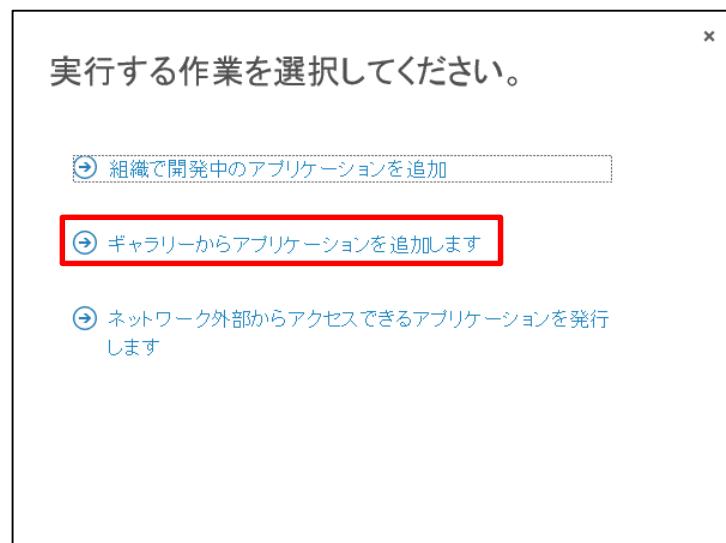
3. [アプリケーション] 画面で、[追加] をクリックします。



【Note:】

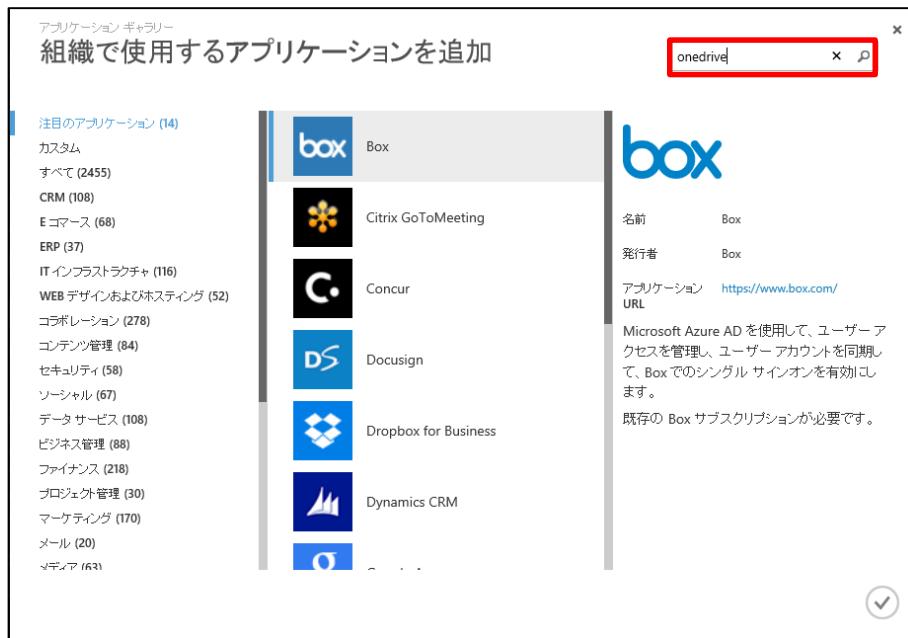
SaaS アプリケーションの登録を行う Azure AD ドメインで既に Office 365 の契約を行っている場合、アプリケーションの一覧に Exchange Online と SharePoint Online が既定で登録されています。

4. [実行する作業を選択してください。] 画面で、[ギャラリーからアプリケーションを追加します] をクリックします。

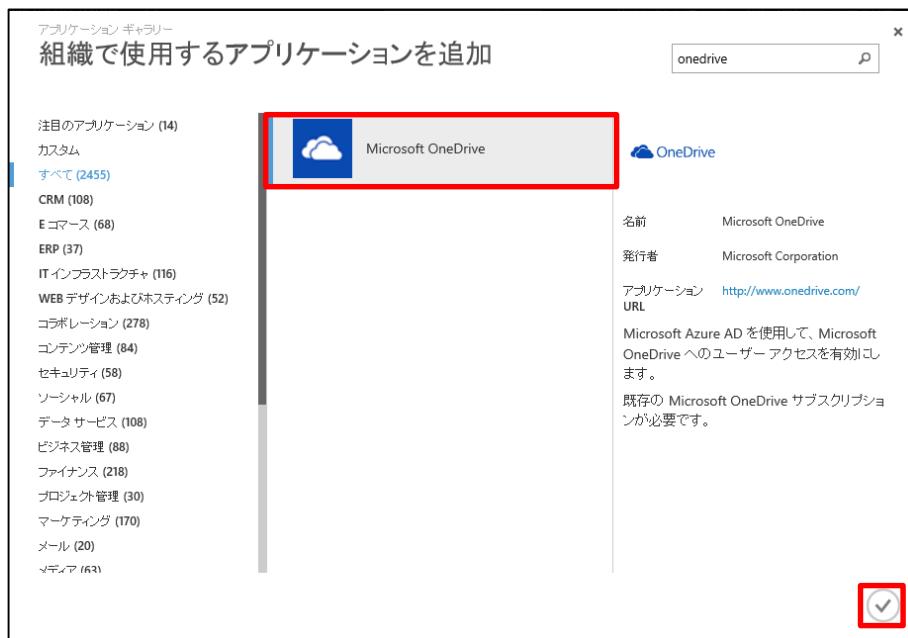


Microsoft Azure Active Directory の活用

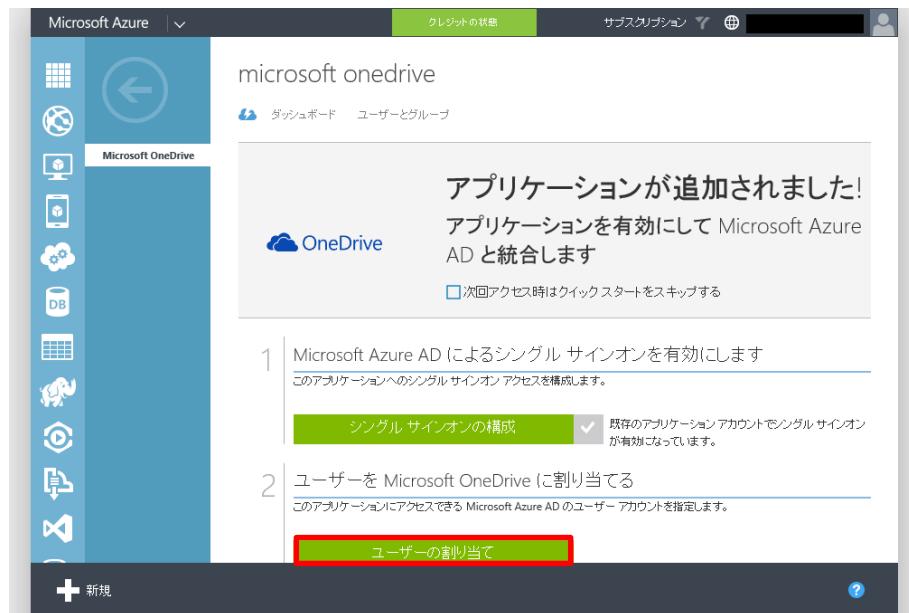
5. [組織で使用するアプリケーションを追加] 画面で、右上の検索窓に「OneDrive」と入力し、Enter キーを押します。



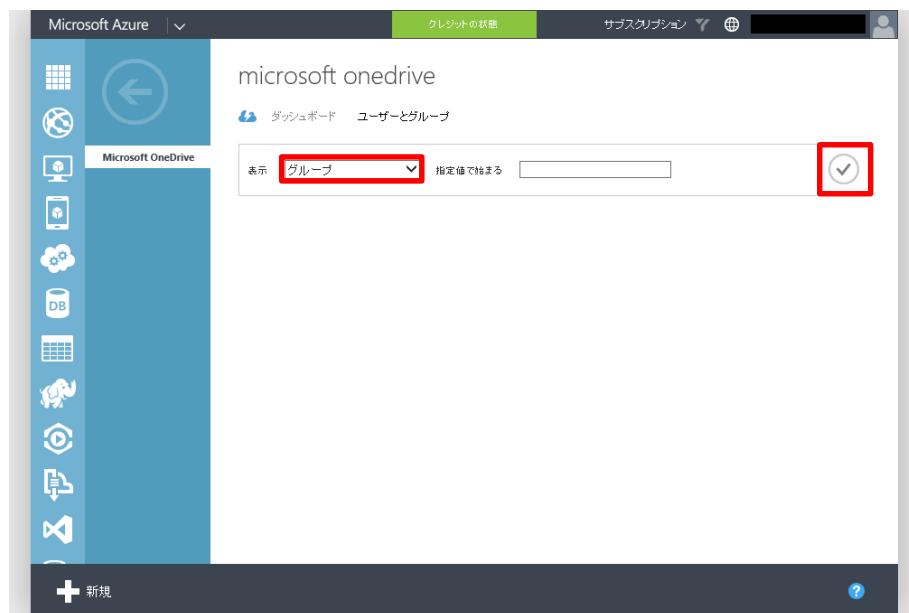
6. [組織で使用するアプリケーションを追加] 画面で、検索結果に Microsoft OneDrive が表示されたことを確認し、チェックマークをクリックします。



7. [microsoft onedrive] 画面で、[ユーザーの割り当て] をクリックします。



8. [microsoft onedrive] 画面で、[表示] 欄でグループが選択されていることを確認し、チェックマークをクリックします。



9. [microsoft onedrive] 画面で、Microsoft OneDrive にアクセスするグループとして Admins グループを選択し、[割り当て] をクリックします。

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various icons. The main area is titled "microsoft onedrive". At the top, there are navigation links: "ダッシュボード" and "ユーザーとグループ". Below that is a search bar with "表示: グループ" and a checkmark icon. The main content area displays a table of groups:

名前	電子メール アドレス	所有者	割り当て
Admins		Contoso 管理者	いいえ
ADSyncAdministrators			いいえ
ADSyncAdministrators			いいえ
ADSyncBrowse			いいえ
ADSyncBrowse			いいえ
ADSyncOperators			いいえ
ADSyncOperators			いいえ
ADSyncPasswordSet			いいえ
ADSyncPasswordSet			いいえ
DnsAdministrators			いいえ

At the bottom of the list, there are buttons: "+ 新規", "新しい割り当て" (highlighted with a red box), "アカウントの選択", and "削除".

【Note:】

Contoso Corporation ドメインでは、Azure AD Premium のライセンスを割り当てているため、SaaS アプリケーションへのアクセス許可としてグループを選択することができます。

10. [グループの割り当て] 画面で、[すべてのグループメンバー間で共有する Microsoft OneDrive 資格情報を入力する] のチェックはつけずに、画面右下のチェック マークをクリックします。



[Note:]

[すべてのグループメンバー間で共有する Microsoft OneDrive 資格情報を入力する] のチッ
クをつけた場合、Azure 管理ポータルで Microsoft OneDrive にアクセスするための資格
情報を設定するため、アクセスパネルから Microsoft OneDrive にアクセスする際、資格情報
を入力する必要がありません。

11. [microsoft onedrive] 画面で、グループにアプリケーションが割り当てられたことが確認で
きます。[表示] 欄から [すべてのユーザー] を選択し、チェックマークをクリックします。

名前	電子メール アドレス	所有者	割り当て
Admins	Contoso 管理者	はい	
ADSyncAdmins		いいえ	
ADSyncAdmins		いいえ	
ADSyncBrowse		いいえ	
ADSyncBrowse		いいえ	
ADSyncOperators		いいえ	
ADSyncOperators		いいえ	
ADSyncPasswordSet		いいえ	
ADSyncPasswordSet		いいえ	
DnsAdmins		いいえ	

Microsoft Azure Active Directory の活用

12. [ユーザーとグループ] 画面で、Admins グループのメンバーに対して、[アクセス] 欄が [はい] に設定されていることが確認できます。[アクセス] 欄が [はい] に設定されているユーザーをクリックし、[割り当て] をクリックします。(ここでは、aaduser1 ユーザーを選択して [割り当て] をクリックします)

表示名	ユーザー名	権限	アクセス	方法
aaduser1	aaduser1@[REDACTED].onmicrosoft.com	管理者	はい	継承 (Admins)
Azure 全体管理者	[REDACTED]	管理者	いいえ	割り当てなし
Contoso 管理者	admin@[REDACTED].onmicrosoft.com	管理者	はい	継承 (Admins)

13. [ユーザーの割り当て] 画面で、[ユーザーの代わりに Microsoft OneDrive 資格情報を入力する] にチェックをつけ、[電子メール アドレス] 欄に Microsoft OneDrive にサインインするためのメールアドレス、[パスワード] 欄にメールアドレスに対応するパスワードをそれぞれ入力し、チェックマークをクリックします。

ユーザーの割り当て

この操作を実行すると、選択されたユーザーを Microsoft OneDrive アプリケーションに対してアクセス パネルから認証できます。ユーザーはアクセス パネルでいつでも Microsoft OneDrive 資格情報を入力および更新できます。

ユーザーの代わりに Microsoft OneDrive 資格情報を入力する

電子メール アドレス
[REDACTED]@outlook.com

パスワード

Microsoft Azure Active Directory の活用

14. ここまで手順により、aaduser1 ユーザーに Microsoft OneDrive に接続するためのアカウント情報が関連付けられました。

The screenshot shows the Microsoft Azure portal interface. On the left, there's a vertical sidebar with various icons. The 'Microsoft OneDrive' icon is highlighted. The main content area has a title 'microsoft onedrive' and a subtitle 'ダッシュボード ユーザーとグループ'. A dropdown menu '表示' is set to 'すべてのユーザー'. Below this is a table with columns: 表示名, ユーザー名, 徒職, 部門, アクセス, 方法. The table contains three rows:

表示名	ユーザー名	徒職	部門	アクセス	方法
aaduser1	aaduser1@[REDACTED].onmicrosoft.com			はい	直接、権限 (Admins)
Azure 全体管理者	[REDACTED]			いいえ	割り当てなし
Contoso 管理者	admin@contoso.onmicrosoft.com			はい	権限 (Admins)

At the bottom of the page, there are buttons for '+ 新規', '戻る', 'アカウントの編集', and '削除'.

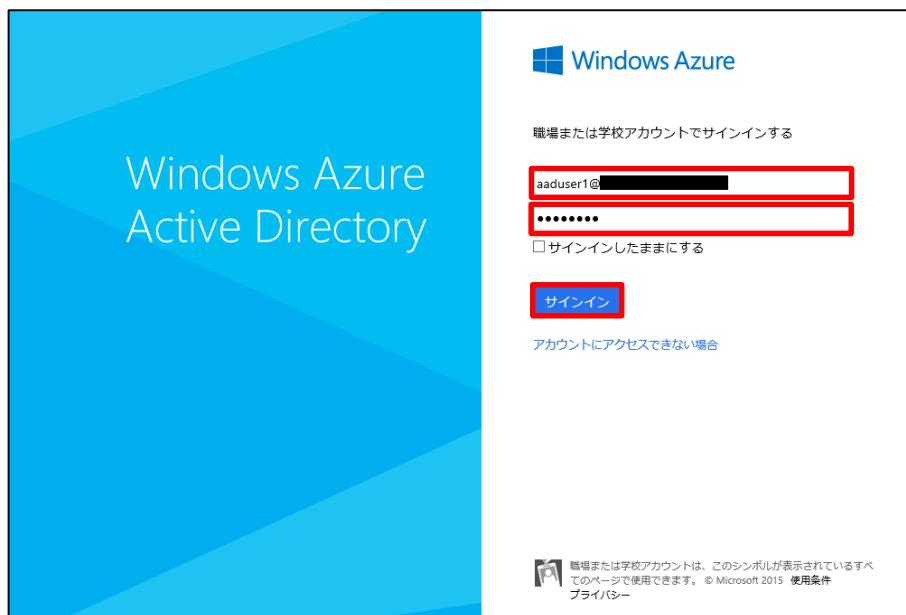
◆ アクセス パネル経由での SaaS アプリへのアクセス

- W81CL01 コンピューターで操作します。

Internet Explorer を起動し、アクセス パネルの URL である

<http://myapps.microsoft.com/> にアクセスします。

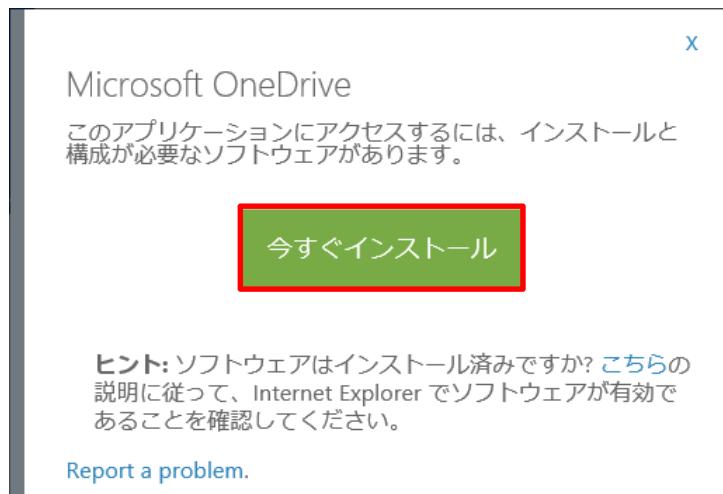
アクセス パネルの Web サイトで、aaduser1@<Microsoft Azure に登録されたドメイン名>ユーザーでサインインします。



- アクセス パネル画面で、[Microsoft OneDrive] をクリックします。



3. [Microsoft OneDrive] 画面で、[今すぐインストール] をクリックします。



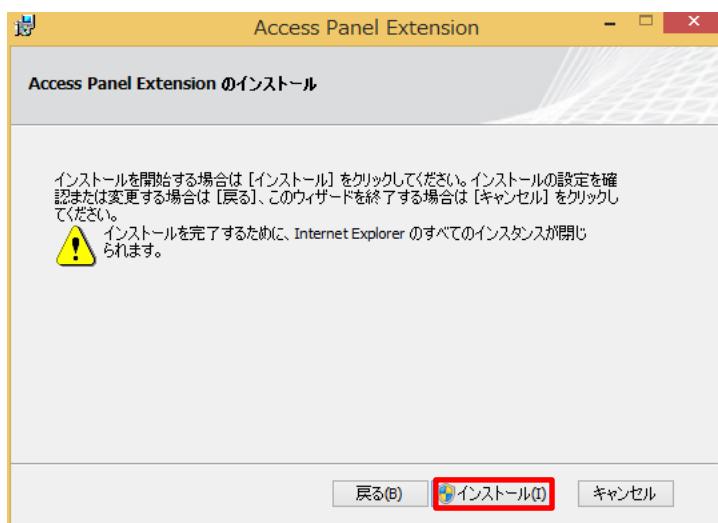
4. ブラウザー画面下部で、Access Panel Extension-jp.msi の実行または保存を問う画面が表示されるので、[実行] をクリックします。



5. [Access Panel Extension] 画面で、[次へ] をクリックします。



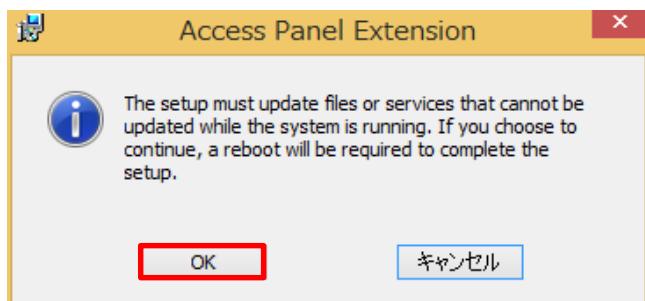
6. [Access Panel Extension のインストール] 画面で、[インストール] をクリックします。



7. [ユーザー アカウント制御] 画面で、[はい] をクリックします。



8. [Access Panel Extension] 画面の警告が表示される場合、[OK] をクリックします。



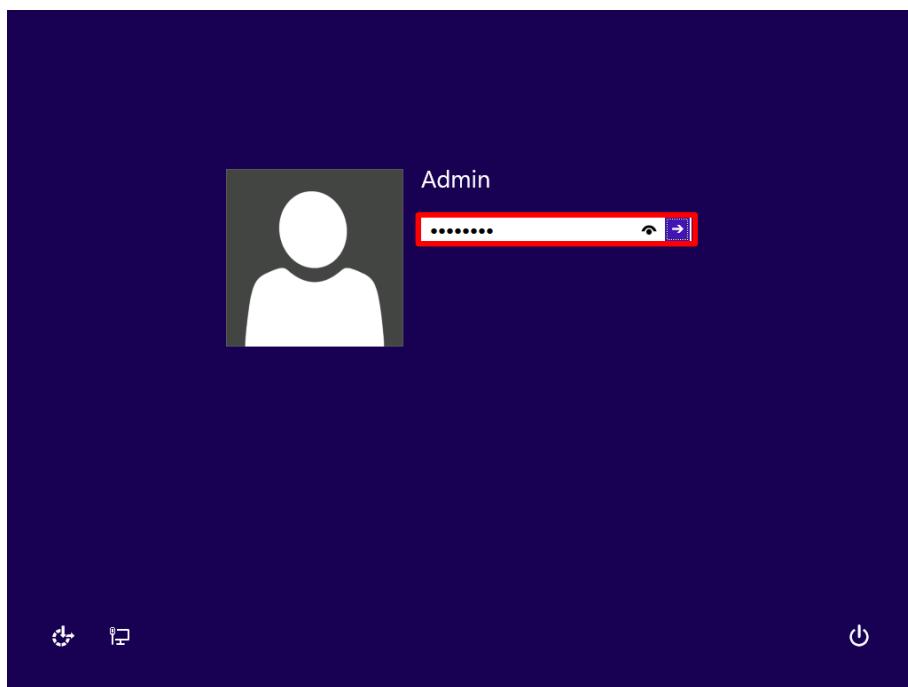
9. [Access Panel Extension セットアップ ウィザードの完了] 画面で、[完了] をクリックします。



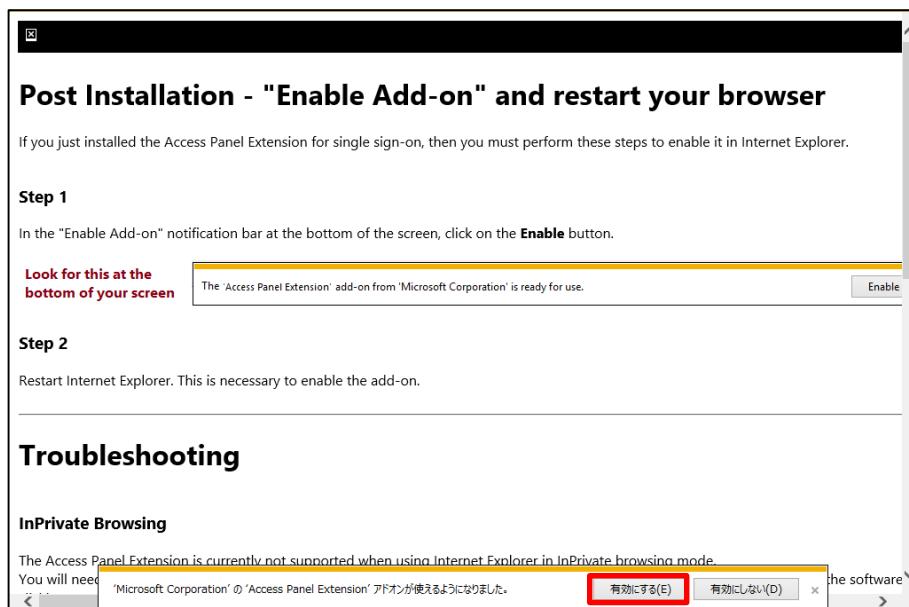
10. [Access Panel Extension] 画面が表示される場合、[はい] をクリックし、再起動します。



11. 再起動した場合は、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。

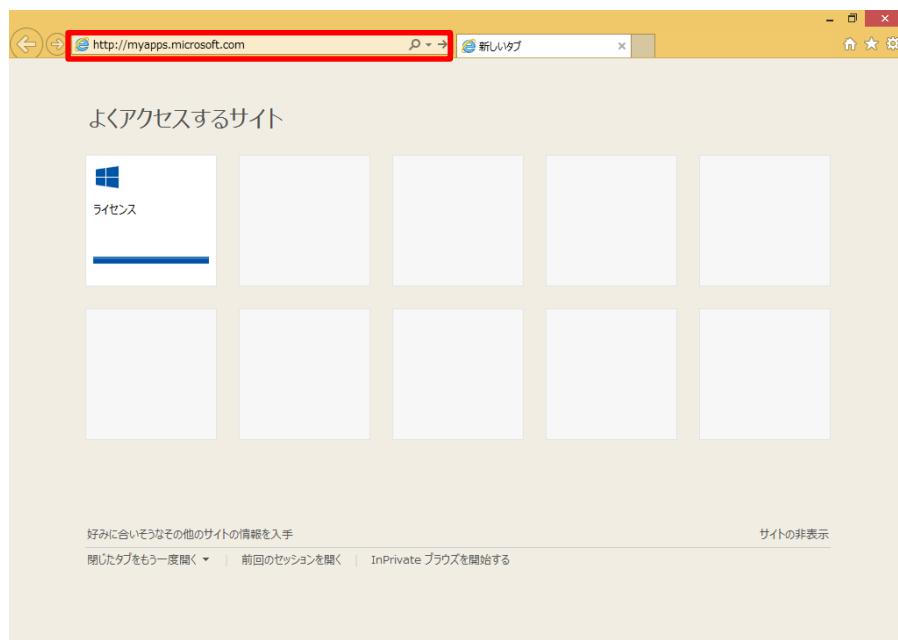


12. 自動的にブラウザーが起動します。ブラウザー画面下部の [‘Microsoft Corporation’ の ‘Access Panel Extension’ が使えるようになりました] 欄で [有効にする] をクリックします。

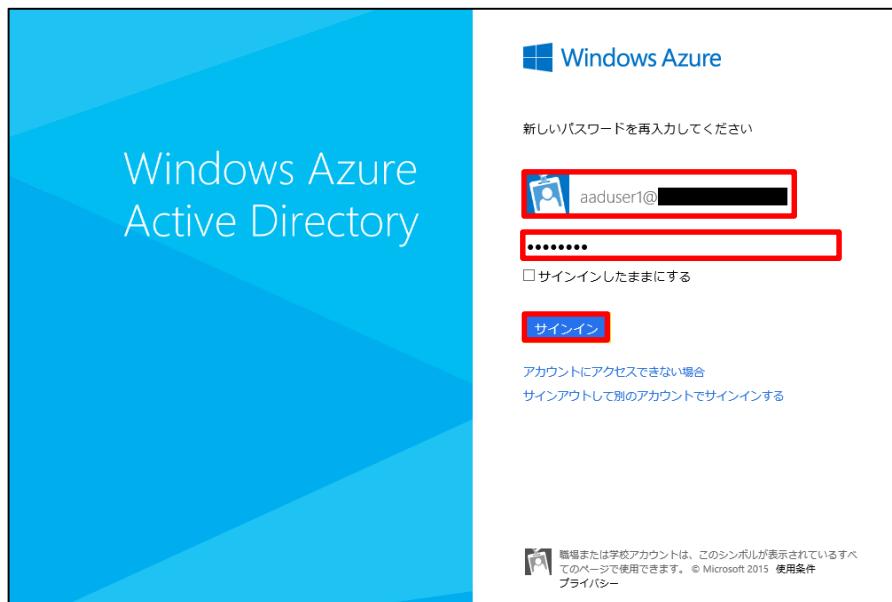


13. Internet Explorer を一度終了し、再び起動します。

14. ブラウザー画面で、アクセス パネルの URL として「<http://myapps.microsoft.com>」と入力し、アクセスします。



15. アクセス パネルの Web サイトで、aaduser1@<Microsoft Azure に登録されたドメイン名>ユーザーでサインインします。サインイン画面で、ユーザー名として前の手順で作成した aaduser1@<AAD ドメイン名> を入力し、パスワードに aaduser1 ユーザーのパスワードをそれぞれ入力し、[サインイン] をクリックします。



16. アクセス パネル画面で、[Microsoft OneDrive] をクリックします。



17. ブラウザー画面で、新しいタブが開き、Microsoft OneDrive へのサインイン操作を自動的に行い、Microsoft OneDrive にアクセスできるようになります。



5.2 アプリケーション プロキシによるオンプレミス アプリケーションの公開

本手順では、社内設置の Web サーバーを Azure AD Premium のアプリケーション プロキシ機能を利用して公開する方法について確認します。

手順の前半では WS2012-DC01 コンピューターに外部に公開する Web サーバーとして、IIS をインストールします。評価環境のコンピューターに Web サーバーがインストールされている場合、[IIS のインストール] 手順を割愛して構いません。

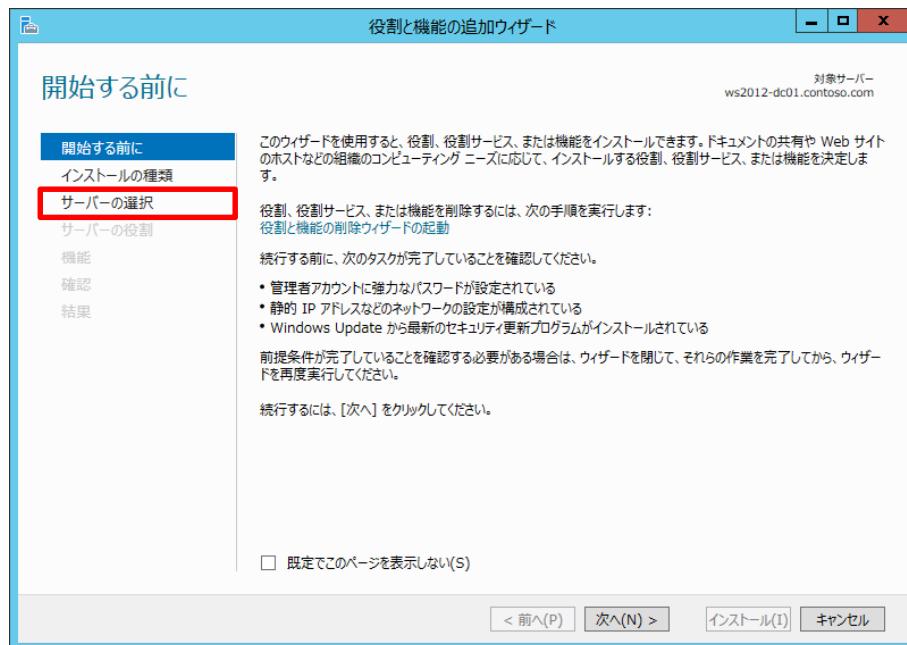
➡ IIS のインストール

1. WS2012-DC01 コンピューターで操作します。

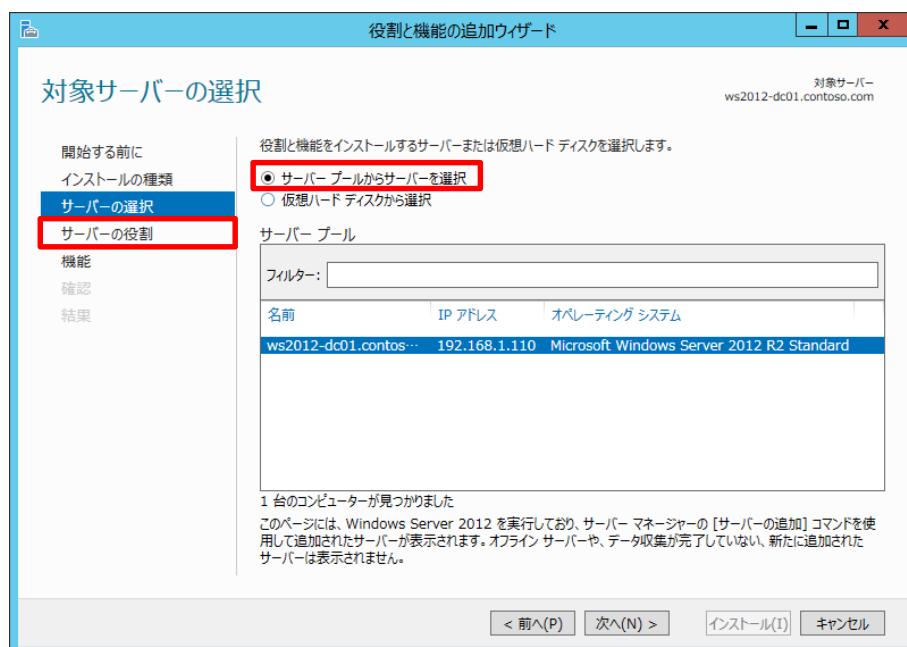
サーバー マネージャー画面で、[管理] - [役割と機能の追加] をクリックします。



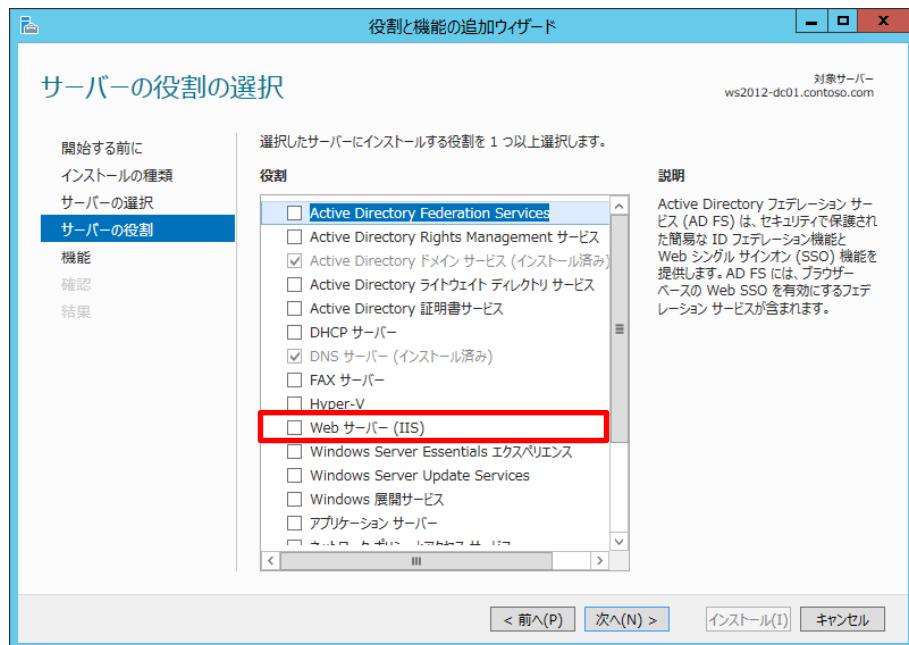
2. [役割と機能の追加ウィザード] 画面で、[サーバーの選択] をクリックします。



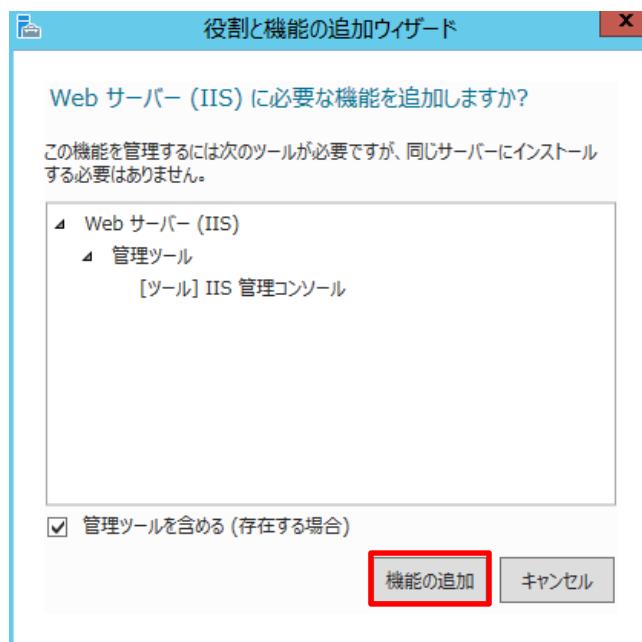
3. [対象サーバーの選択] 画面で、[サーバー プールからサーバーを選択] が選ばれていることを確認し、[サーバーの役割] をクリックします。



4. [サーバーの役割の選択] 画面で、[役割] の中から [Web サーバー (IIS)] をクリックします。

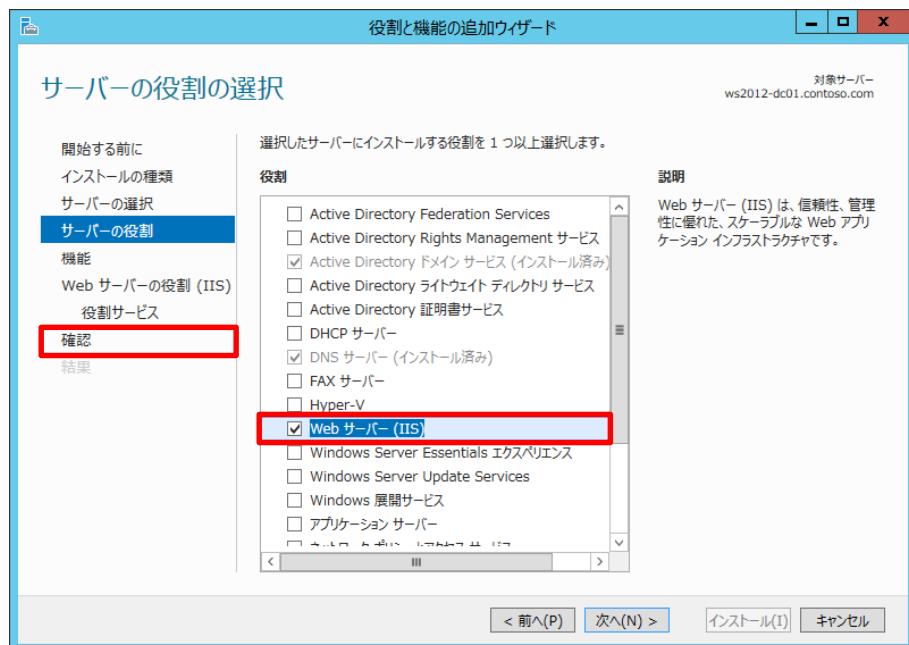


5. [役割と機能のウィザード] 画面で、[機能の追加] をクリックします。

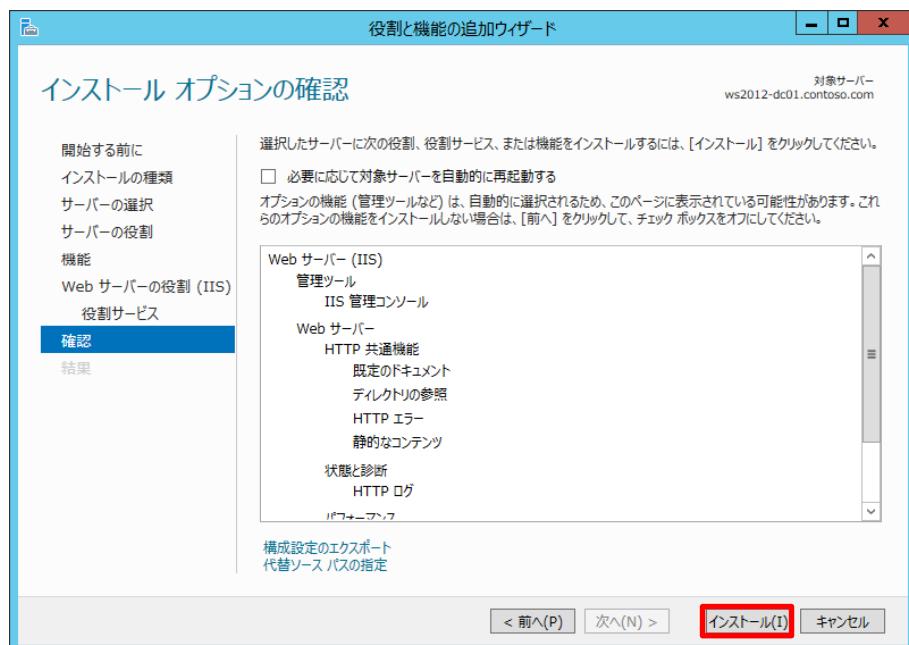


Microsoft Azure Active Directory の活用

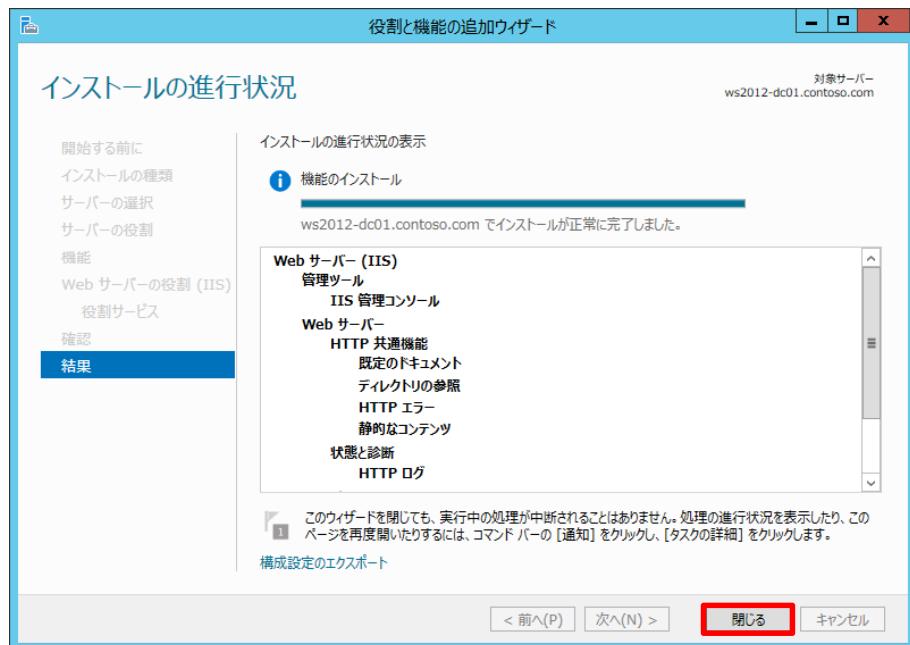
6. [サーバーの役割の選択] 画面で、[Web サーバー (IIS)] にチェックが入っていることを確認し、[確認] をクリックします。



7. [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。



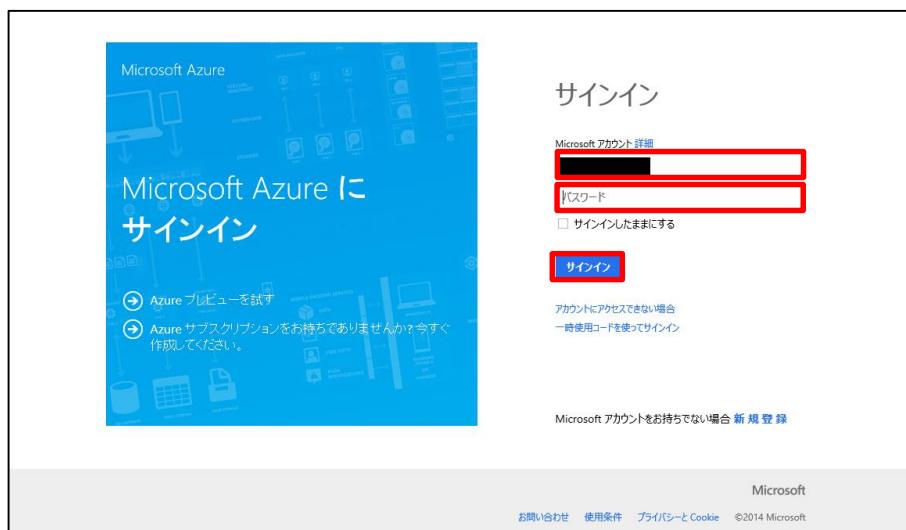
8. [インストール オプションの進行状況] 画面で、インストール完了後 [閉じる] をクリックします。



◆ アプリケーション プロキシの設定による Web サーバーの公開

本手順では、アプリケーション プロキシの設定を行い、Web サーバーを外部からアクセスできるように構成します。本手順を実行する場合、事前に [サーバーマネージャー] 画面の左ペイン [ローカル サーバー] で、[IE セキュリティ強化の構成] を無効に設定してから開始してください。

1. Internet Explorer を起動し、URL として「<https://manage.windowsazure.com>」と入力し、Microsoft Azure 管理ポータルにアクセスします。Microsoft Azure 管理ポータルのサインイン画面で、Microsoft アカウントのユーザー名とパスワードを入力し、[サインイン] をクリックします。



2. Microsoft Azure 管理ポータル画面で、[Contoso Corporation] をクリックします。



Microsoft Azure 自習書 No.18
Microsoft Azure Active Directory の活用

3. [Contoso corporation] 画面で、[構成] をクリックします。



4. [構成] 画面で、[アプリケーション プロキシ] - [有効] をクリックし、[保存] をクリックします。

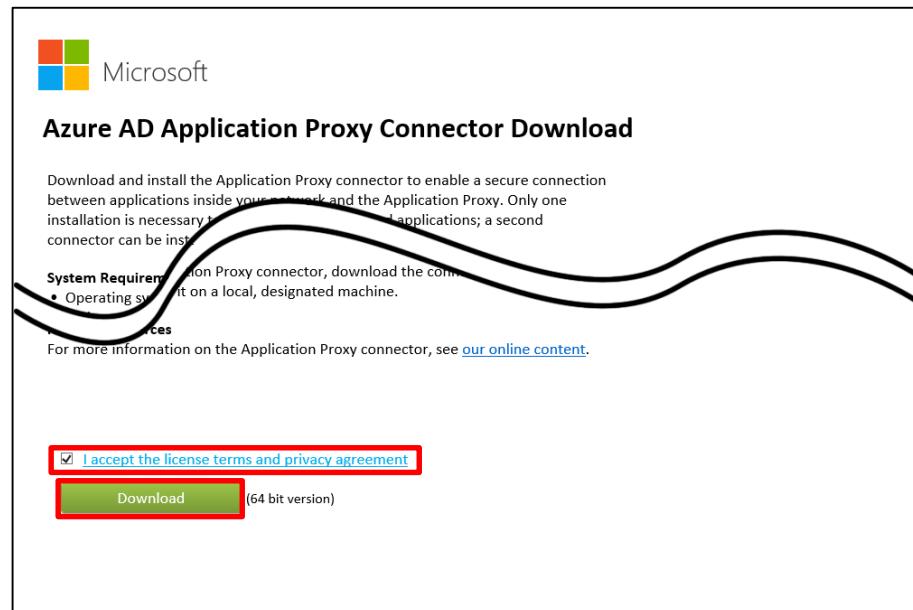


Microsoft Azure Active Directory の活用

5. [構成] 画面で、[アプリケーション プロキシ] - [ネットワークにアプリケーションプロキシコネクタをダウンロードしてインストールしてください。] メニューの [今すぐダウンロードする。] をクリックします。

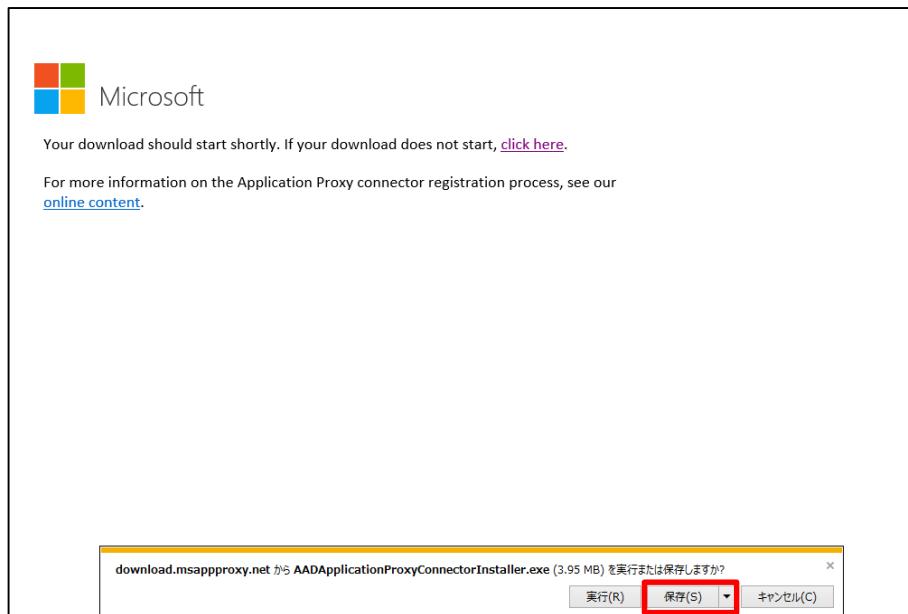


6. ブラウザー画面で Microsoft Azure AD Application Proxy Connentor Download が表示されます。下にスクロールし、[I accept the license terms and privacy agreement] にチェックを入れ、[Download] をクリックします。

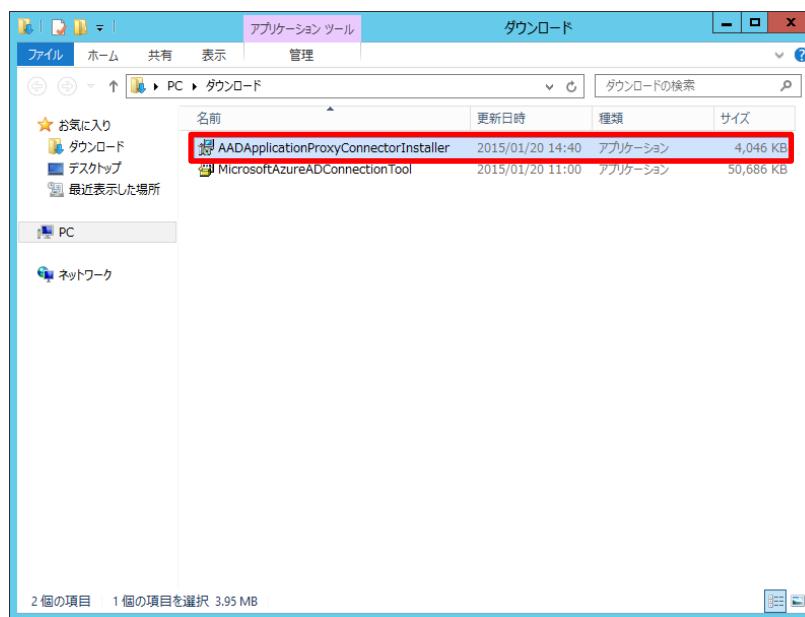


Microsoft Azure 自習書 No.18
Microsoft Azure Active Directory の活用

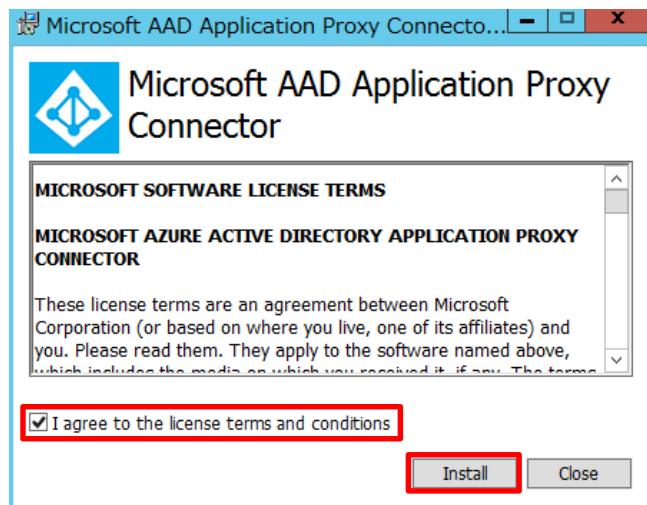
7. [保存] をクリックします。



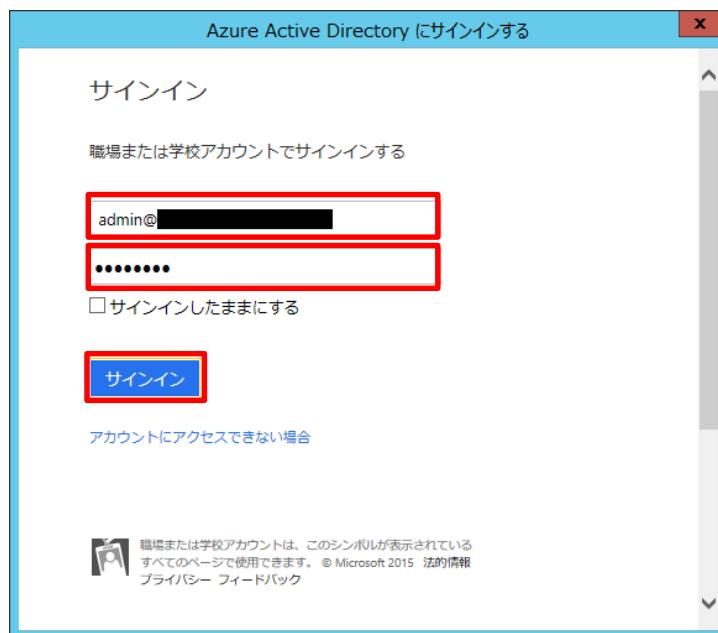
8. ダウンロードした保存先のフォルダーを開き、ダウンロードしたファイル [AADApplicationProxyConnectorInstaller] をダブルクリックします。



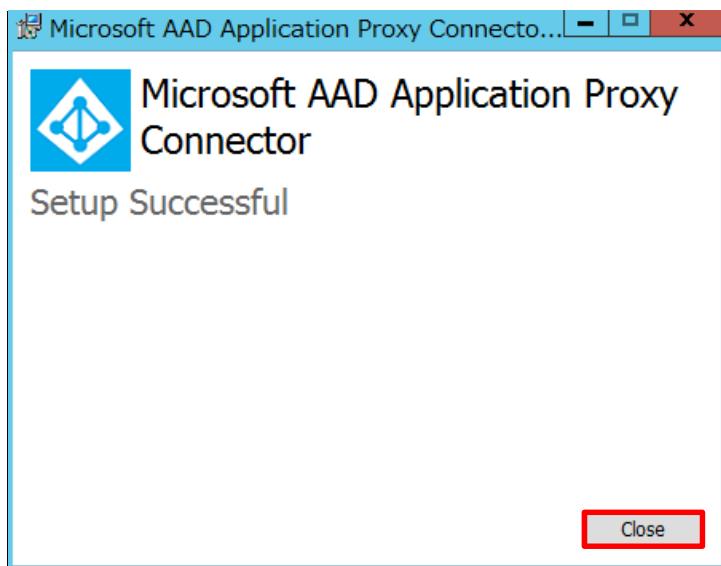
9. [Microsoft AAD Application Proxy Connector] 画面で、[I agree to the license terms and conditions] にチェックし、[Install] をクリックします。



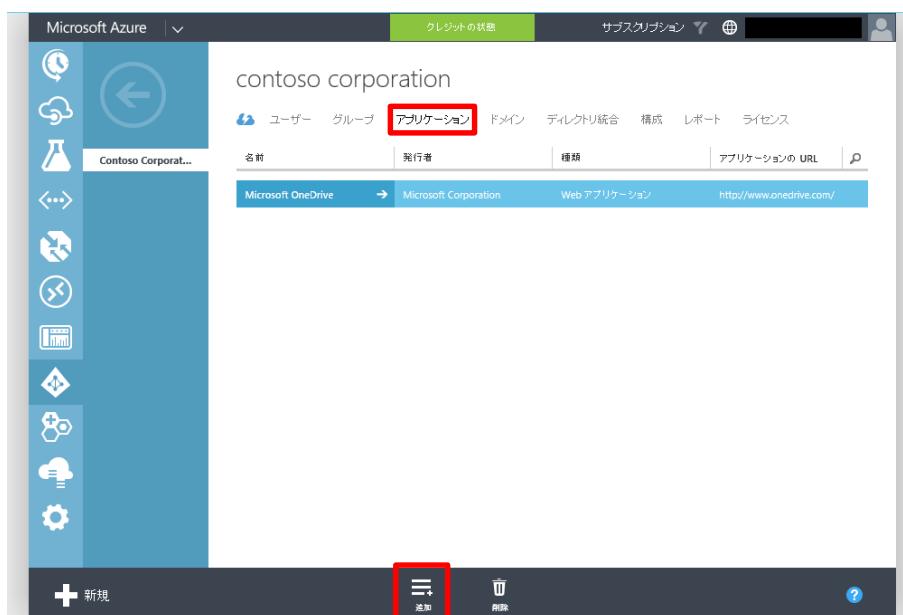
10. [Azure Active Directory にサインインする] 画面で、Contoso corporation の全体管理者のユーザー名とパスワードを入力し、[サインイン] をクリックします。



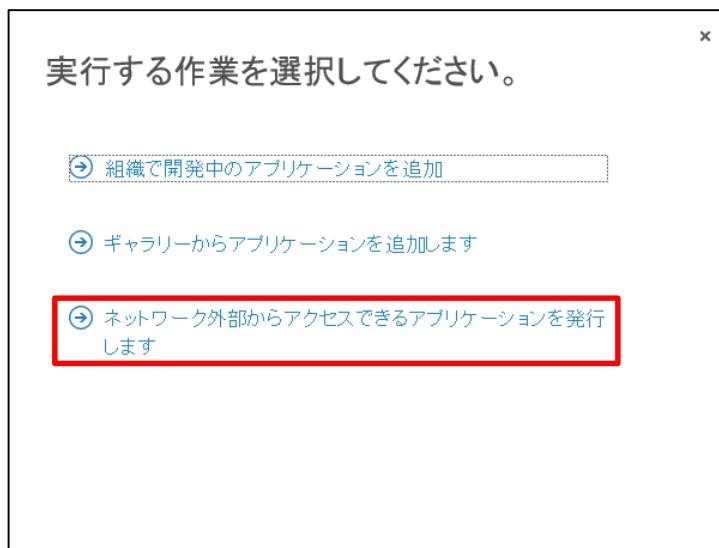
11. [Microsoft AAD Application Proxy Connector] 画面で、[close] をクリックします。



12. Microsoft Azure 管理ポータル画面に戻ります。[contoso corporation] 画面で、[アプリケーション] をクリックし、[追加] をクリックします。



13. [実行する作業を選択してください] 画面で、[ネットワーク外部からアクセスできるアプリケーションを発行します] をクリックします。



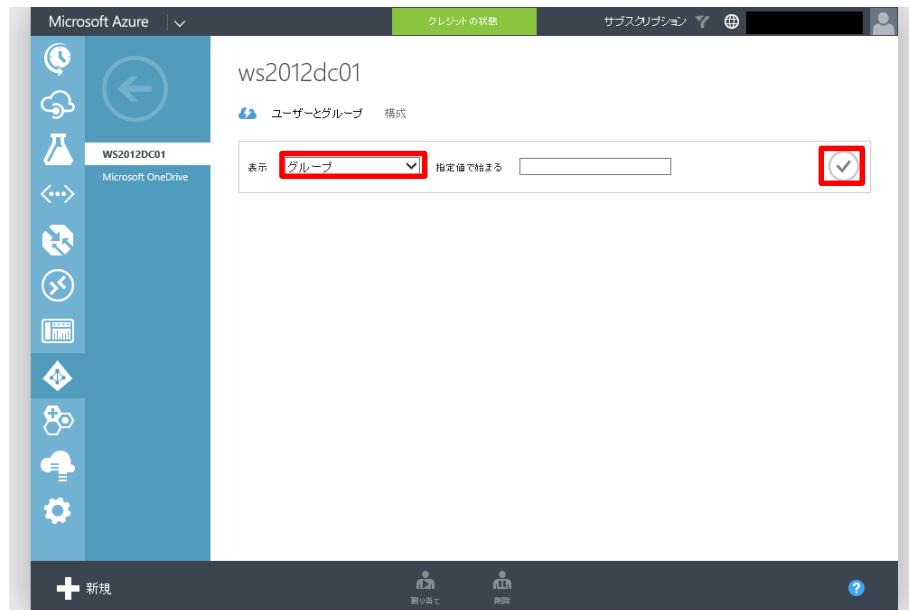
14. [アプリケーション情報の指定] 画面で、[名前] 欄に「WS2012DC01」、[内部 URL] 欄に「http://ws2012-dc01/」とそれぞれ入力し、チェックマークをクリックします。



15. [ws2012dc01] 画面で、アプリケーションが追加されたことが確認できます。アクセス権を割り当てるため、[ユーザーとグループ] をクリックします。



16. [ws2012dc01] 画面で、[グループ] を選択し、チェック マークをクリックします。



Microsoft Azure Active Directory の活用

17. [ws2012dc01] 画面で、グループの一覧が表示されます。アクセス権を割り当てるグループ [sales] をクリックし、[割り当て] をクリックします。

The screenshot shows the Microsoft Azure Active Directory Groups page for the 'ws2012dc01' tenant. On the left, there's a sidebar with various icons. The main area displays a list of groups. The 'Sales' group is highlighted with a red box. At the bottom right of the list, there are two buttons: 'Assign' (highlighted with a red box) and 'Delete'.

名前	電子メール アドレス	所有者	割り当て
ADSyncAdmins			いいえ
ADSyncBrowse			いいえ
ADSyncOperators			いいえ
ADSyncPasswordSet			いいえ
DnsAdmins			いいえ
DnsUpdateProxy			いいえ
Sales			いいえ
SSPR セキュリティグループ ユー...			いいえ
WinRMRemoteWMIUsers...			いいえ

18. [選択したグループのアクセスを有効にしますか？] 画面で、[はい] をクリックします。

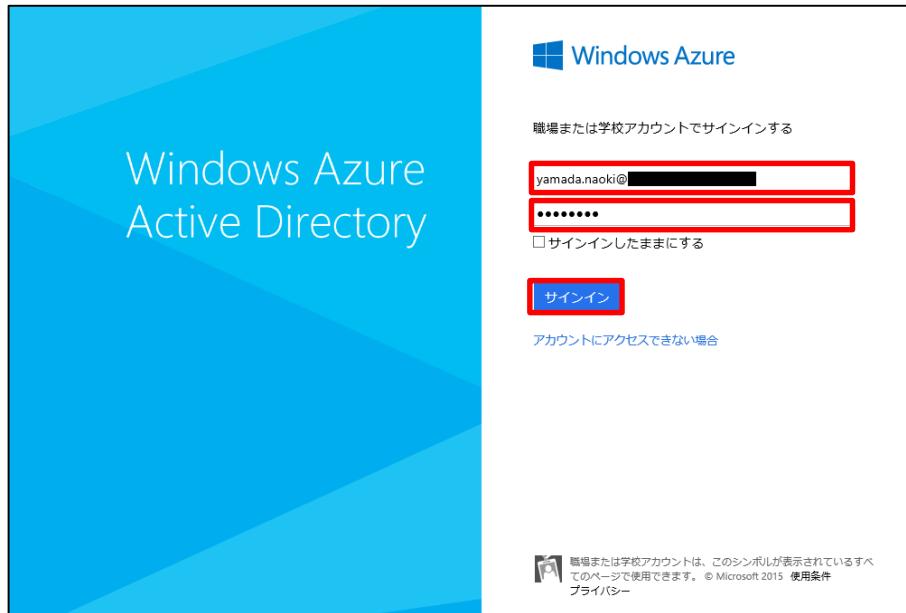


19. InPrivate ブラウズで Internet Explorer を起動し、アクセス パネルの URL である

<http://myapps.microsoft.com/> にアクセスします。

アクセス パネルの Web サイトで、Sales グループのメンバーである

Yamada.Naoki@<Microsoft Azure に登録されたドメイン名>ユーザーでサインインします。



【Note:】

Yamada.Naoki ユーザーで初めてサインインする場合、「4.9 セルフサービス パスワード リセット」の設定により、サインイン後に連絡先の登録を求められます。連絡先登録に関する手順は「4.9 セルフサービス パスワード リセット」の「パスワード リセットの実行」の手順を参照してください。

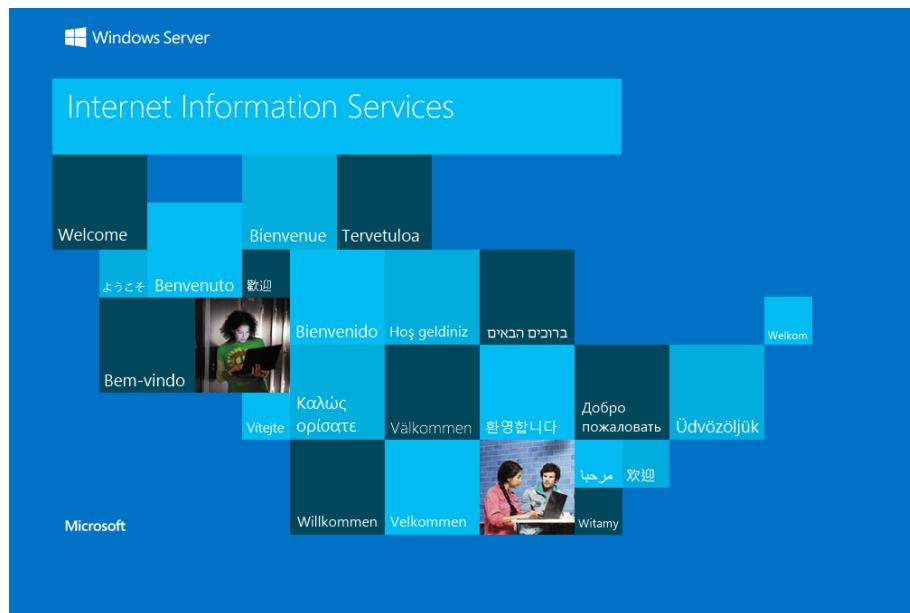
20. アクセス パネルの Web サイトで、登録したアプリケーションが表示されない場合は、[アプリがアップデートされました。更新するにはここをクリックしてください。] をクリックします。



21. アクセス パネル画面で、[WS2012DC01] をクリックします。



22. 社内設置の Web サーバーでホストされている Web ページが表示されたことを確認します。



5.3 レポートによるアプリケーション アクセスの確認

Azure AD では Azure AD の認証・認可に関わる様々なログを収集し、管理ポータルから参照することができます。本手順では、一例として Azure AD に登録されたアプリケーションの利用状況に関するレポートを参照します。

1. Microsoft Azure 管理ポータル画面で、[ACTIVE DIRECTORY] をクリックし、[Contoso corporation] をクリックします。

The screenshot shows the Microsoft Azure Management Portal. On the left, there's a sidebar with various service icons. The 'ACTIVE DIRECTORY' icon is highlighted with a red box. The main area is titled 'active directory' and shows a list of applications under 'Contoso Corp...'. One application, 'Contoso Corp...' itself, is selected and shown in detail. It has a status of 'アクティブ' (Active) and is managed by '全社管理者'. There are filters for 'すべての Contoso C...' and 'アジア、ヨーロッパ、... 日本'. The top navigation bar includes tabs for 'ディレクトリ', 'ACCESS CONTROL', '名前空間', '多要素認証プロバイダー', and 'RIGHTS MANAGEMENT'. The bottom navigation bar has buttons for '+ 新規', '削除', and a help icon.

2. [Contoso corporation] 画面で、[レポート] をクリックします。

The screenshot shows the Microsoft Azure Management Portal for 'contoso corporation'. The 'Reports' tab is highlighted with a red box. A large blue diamond icon with three white circles is displayed, accompanied by the text 'ディレクトリを使用する準備ができました。' (The directory is ready for use.) and '作業開始するためのオプションは次のとおりです。' (The options for starting work are as follows.) Below this, there's a checkbox for '次回アクセス時はクイックスタートをスキップする' (Skip quick start next time I access). At the bottom, there's a section titled '1 ユーザー サインイン エクスペリエンスの向上' (1 User sign-in experience improvement) with a note about adding custom domain names. The bottom navigation bar has buttons for '+ 新規', '?', and a help icon.

3. [レポート] 画面で、[アプリケーションの使用状況] をクリックします。

The screenshot shows the Microsoft Azure portal interface. On the left, there's a vertical sidebar with various icons representing different services like storage, databases, and monitoring. The main area is titled 'Report' and contains several sections:

- 異常なアクティビティ**: A list of activity types such as '不明なソースからのサインイン' (Sign-in from unknown source), '複数のエラー発生後のサインイン' (Sign-in after multiple errors occur), etc.
- アクティビティログ**: A list of log types such as '監査レポート' (Audit Report), 'パスワードリセットアクティビティ' (Password reset activity), etc.
- 統合アプリケーション**: This section is highlighted with a red box. It includes a sub-section 'アプリケーションの使用状況' (Application usage status) which provides a summary of SaaS application usage.

4. [アプリケーションの使用状況] 画面で、前の手順で追加した SaaS アプリケーションである Microsoft OneDrive へのサインインユーザー数と回数が確認できます。

This screenshot shows the 'Application usage status' report for Microsoft OneDrive. The report title is 'アプリケーションの使用状況'. It displays a summary of SaaS application usage over a specified time period. The table in the center shows the following data:

アプリケーション	一意なユーザー数	合計サインイン回数
Microsoft OneDrive	2	4

The table row for Microsoft OneDrive is highlighted with a red box. The report also includes a summary message: 'ディレクトリと統合されたすべての SaaS アプリケーションの利用状況の概要を提供します。' (Provides an overview of the usage status of all SaaS applications integrated into the directory.)

STEP 6. セキュアな Microsoft Azure Active Directory の利用

この STEP では、より安全に Azure AD にサインインするために利用可能な機能について説明します。

この STEP では、次のことを学習します。

- ✓ 多要素認証の実装
- ✓ デバイスの登録

6.1 多要素認証の管理

「2.9 多要素認証」では、Azure AD の多要素認証には、多要素認証サービスと、AD FS サーバーと組み合わせて利用する多要素認証プロバイダーがあることを解説しました。

それぞれの多要素認証を実装するにあたり、手順が異なるため、「6.2 多要素認証サービスの実装」にて Azure AD の多要素認証サービスについて、「6.3 多要素認証プロバイダーの実装」にて AD FS サーバーと組み合わせて利用する多要素認証プロバイダーについて、それぞれ手順を確認します。

Azure AD の多要素認証サービスと多要素認証プロバイダーでは、それぞれ次の認証要素を利用することができます。

- 通話

あらかじめ設定された電話番号に着信があります。着信に応答し、音声ガイダンスに従って # を押して認証を行います。

- 携帯電話に SMS を送信

携帯電話の SMS に確認コードを含むメッセージを送信します。携帯電話で受信したら、メッセージに含まれる確認コードを入力して認証を行います。

- モバイル デバイス アプリケーションに通知

iOS または Android のアプリとして提供されている Multi-Factor Authentication を使用します。多要素認証を行うことになると、メッセージが通知され、通知内容に従って [許可] をタップすることで認証を行います。

- モバイル デバイス アプリケーションの確認コード

iOS または Android のアプリとして提供されている Multi-Factor Authentication を使用します。Multi-Factor Authentication アプリに表示されている確認コード番号を入力して認証を行います。

6.2 多要素認証サービスの実装

本手順では、Azure の多要素認証サービスを利用してaaduser1 ユーザーでサインインするときに多要素認証が利用できる様子を確認します。

1. Microsoft Azure 管理ポータル画面で、[ACTIVE DIRECTORY] をクリックし、[Contoso corporation] をクリックします。



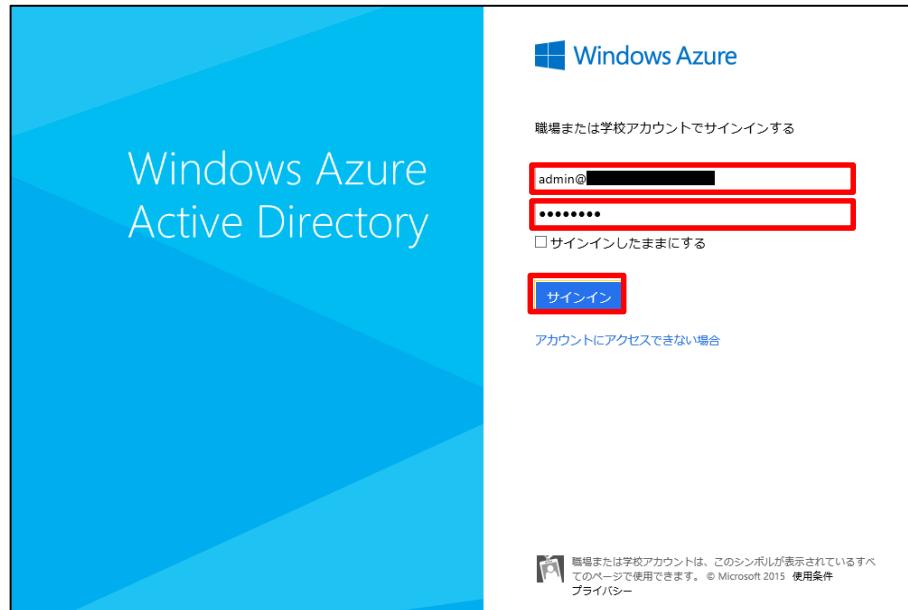
2. [Contoso corporation] 画面で、[ユーザー] をクリックします。



3. ユーザー画面で、aaduser1 ユーザーをクリックし、[多要素認証の管理] をクリックします。

The screenshot shows the Microsoft Azure Active Directory user list. A user named 'AADUser1' is selected, indicated by a red box around the row. In the bottom navigation bar, the 'Multi-factor authentication management' button (represented by a lock icon) is also highlighted with a red box.

4. サインイン画面が表示される場合、admin@<Microsoft Azure に登録されたドメイン名>ユーザーでサインインします。



5. ブラウザー画面で、新しいタブが開き、[多要素認証] 画面が表示されます。[多要素認証] 画面で、aaduser1 にチェックをし、[有効にする] をクリックします。

表示名	ユーザー名	MULTI-FACTOR AUTHENTICATION の状態	
<input checked="" type="checkbox"/> aaduser1	aaduser1@[REDACTED]	無効	aaduser1 quick steps <input checked="" type="button"/> 有効にする ユーザー設定の管理
<input type="checkbox"/> Azure 全体管理者	[REDACTED]	無効	
<input type="checkbox"/> Contoso 管理者	admin@[REDACTED]	無効	
<input type="checkbox"/> Hamada Mizuki	Hamada.Mizuki@[REDACTED]	無効	
<input type="checkbox"/> Yamada Naoki	Yamada.Naoki@[REDACTED]	無効	

6. [Multi-factor authentication を有効にする方法の概要] 画面で、[Multi-factor authentication を有効にする] をクリックします。



7. [更新が正常に完了しました] 画面で、[閉じる] をクリックします。



8. [多要素認証] 画面で表示されているタブを終了します。(Microsoft Azure 管理ポータル サイトは終了しないでください)

9. InPrivate ブラウズで Internet Explorer を起動し、アクセス パネルの URL である

<http://myapps.microsoft.com/> にアクセスします。

アクセス パネルの Web サイトで、aaduser1@<Microsoft Azure に登録されたドメイン名>ユーザーでサインインします。



10. [アカウントの保護にご協力ください] 画面で、[今すぐセットアップ] をクリックします。



11. [追加のセキュリティ確認] 画面で、多要素認証を設定する方法を選択します。

[認証用電話] で、[日本(+81)] を選択し、携帯電話の番号として、先頭の 0 を省いた番号を入力します（例 8012345678）。

[方法] 欄で、[テキスト メッセージでコードを送信する] を選択し、[連絡してください] をクリックします。

**【Note:】**

[方法] 欄で [電話する] を選択すると、通話による操作で多要素認証を実行します。

【Note:】

[認証用番号] 欄に入力する電話番号は Azure 管理ポータルから Azure AD ユーザーの [作業情報] から [認証の連絡先情報] 欄を使用して管理者が事前に登録することも可能です。

12. しばらくすると 6 行のコード番号が携帯電話に送信されます。

[追加のセキュリティ確認] 画面で、携帯電話に送信されたコード番号を入力し、[確認] をクリックします。



13. [追加のセキュリティ確認] 画面で、[このアプリ パスワードで今すぐ開始] 欄に表示されているアプリケーション パスワードを控え、[完了] をクリックします。



【Note:】

多要素認証はブラウザーからサインインする場合でのみ利用可能です。Outlook などの Microsoft Office アプリケーションからサインインする場合は自動生成されるアプリ パスワードをサインイン パスワードとして使用する必要があります。アプリ パスワードは一度しか表示されないため、忘れないように記憶しておいてください。

14. サインイン画面に移動します。

[アカウントの保護にご協力ください] 画面で、携帯電話にコード番号が送信されるので、受信した 6 桁のコード番号を入力し、[サインイン] をクリックします。



15. サインインに成功すると、[アプリケーション プロファイル] 画面が表示されます。ここまで手順で、AAD で作成したユーザーによるサインインには多要素認証が必要になっていることが確認できました。



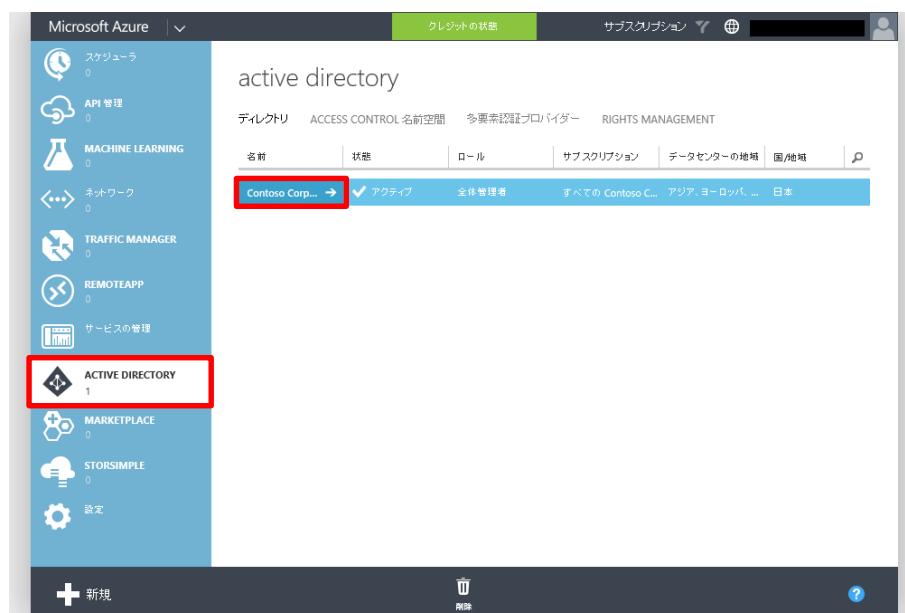
6.3 多要素認証プロバイダーの実装

本手順では、多要素認証プロバイダーを利用してオンプレミスの AD FS サーバーで Azure AD Premium で提供される多要素認証が利用できる様子を確認します。

◆ 多要素認証プロバイダーのインストール

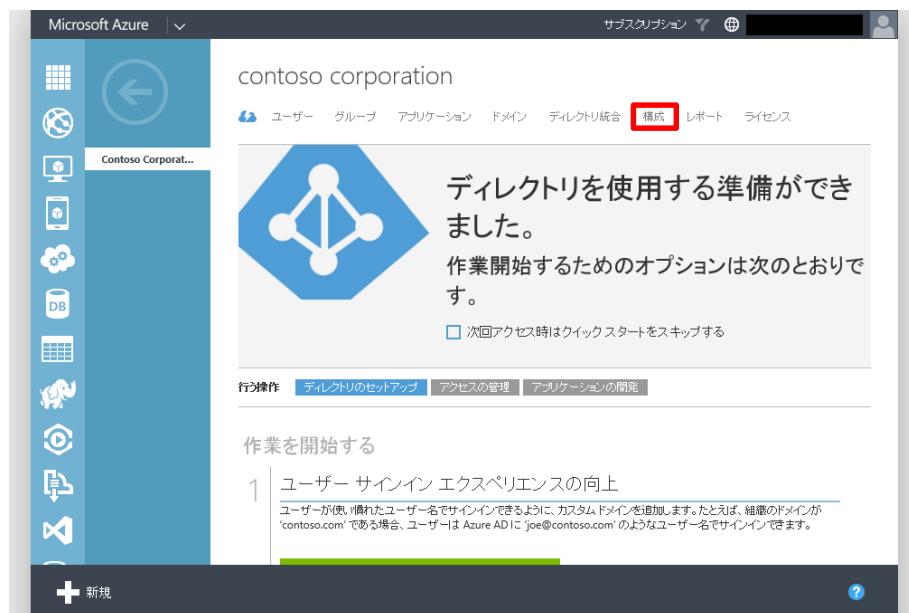
1. WS2012-DC01 コンピューターで操作します。

Microsoft Azure 管理ポータル画面で、[ACTIVE DIRECTORY] をクリックし、[Contoso corporation] をクリックします。



The screenshot shows the Microsoft Azure Management Portal interface. On the left, there's a sidebar with various service icons: Security, API Management, Machine Learning, Network, Traffic Manager, RemoteApp, and Service Management. Below these, the 'ACTIVE DIRECTORY' icon is highlighted with a red box. The main content area is titled 'active directory' and contains tabs for DIRECTORY, ACCESS CONTROL, NAME SPACES, MULTI-FACTOR AUTH PROVIDER, and RIGHTS MANAGEMENT. Under the 'MULTI-FACTOR AUTH PROVIDER' tab, a list shows 'Contoso Corp...' with a status of 'Active'. Other items in the list include 'すべての Contoso C...', 'アジア・ヨーロッパ、...', and '日本'. At the bottom of the page, there are 'New' and 'Delete' buttons.

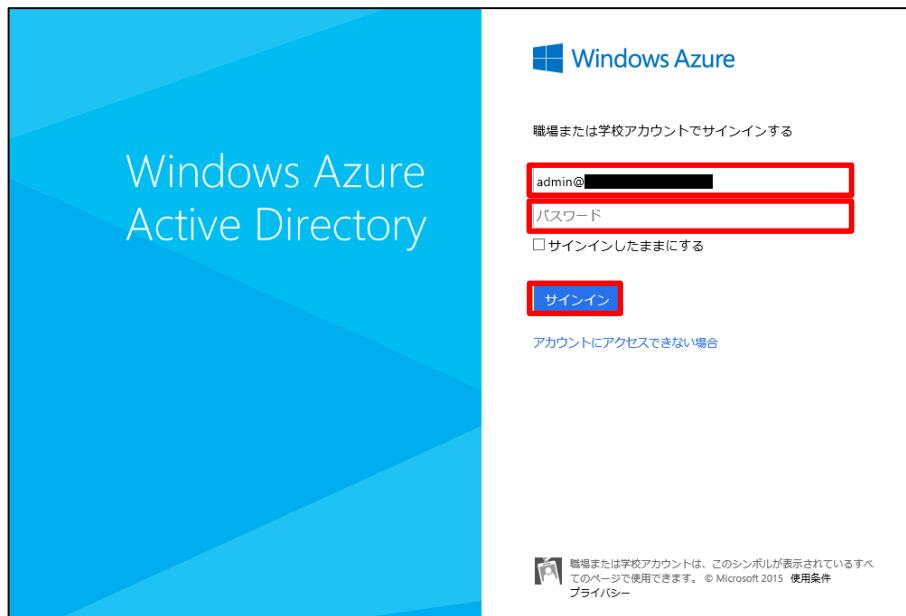
2. [Contoso corporation] 画面で、[構成] をクリックします。



3. [構成] 画面で、[多要素認証] - [サービス設定の管理] をクリックします。



4. サインイン画面が表示される場合、[ユーザー ID] に Windows Azure の全体管理者である admin@<Microsoft Azure に登録されたドメイン名>ユーザーでサインインします。



5. [多要素認証] 画面で、下にスクロールし、[ポータルに移動する] をクリックします。



6. [Azure Multi-Factor Authentication] 画面で、[DOWNLOADS] をクリックします。

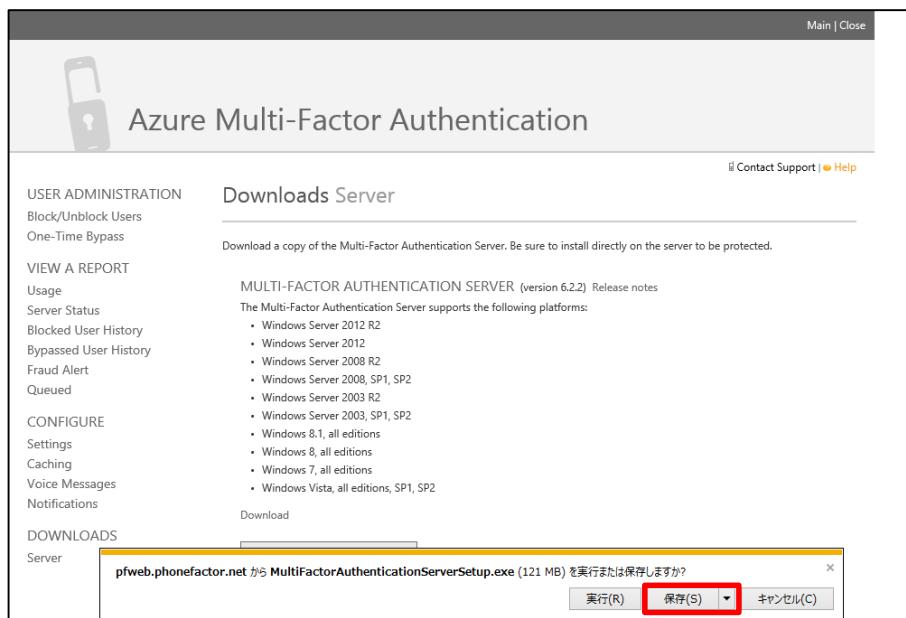
The screenshot shows the 'Welcome' screen of the Azure Multi-Factor Authentication interface. On the left, there's a sidebar with navigation links: 'VIEW A REPORT' (Usage, Server Status, Blocked User History, Bypassed User History, Fraud Alert, Queued), 'CONFIGURE' (Settings, Caching, Voice Messages, Notifications), and 'DOWNLOADS' (Server). The 'DOWNLOADS' section is highlighted with a red box around the 'Server' link. The main content area displays a 'Welcome' message and two buttons: 'VIEW A REPORT' and 'CONFIGURE'. Below these are sections for 'Tokenless multi-factor authentication' and 'Multi-Factor Authentication settings'. The 'DOWNLOADS' section contains a blue download icon and the text 'Download the Multi-Factor Authentication Server'.

7. [Azure Multi-Factor Authentication] 画面で、[MULTI-FACTOR AUTHENTICATION SERVER] の [Downloads] をクリックします。

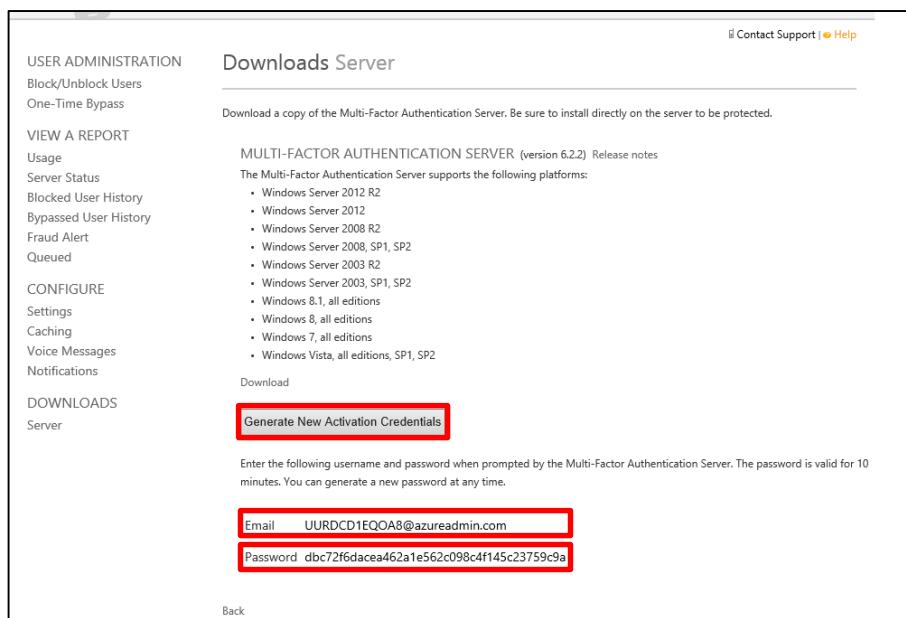
The screenshot shows the 'Downloads Server' page within the 'MULTI-FACTOR AUTHENTICATION SERVER' section. The left sidebar includes 'USER ADMINISTRATION' (Block/Unblock Users, One-Time Bypass) and 'VIEW A REPORT' (Usage, Server Status, Blocked User History, Bypassed User History, Fraud Alert, Queued). The 'CONFIGURE' and 'DOWNLOADS' sections are also present. The main content area has a heading 'Downloads Server' and a sub-section 'MULTI-FACTOR AUTHENTICATION SERVER (version 6.2.2) Release notes'. It lists supported platforms: Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, SP1, SP2, Windows Server 2003 R2, Windows Server 2003, SP1, SP2, Windows 8.1, all editions, Windows 8, all editions, Windows 7, all editions, and Windows Vista, all editions, SP1, SP2. A large red box highlights the 'Download' button, which is located below the platform list. There is also a 'Generate Activation Credentials' button.

Microsoft Azure Active Directory の活用

8. [Azure Multi-Factor Authentication] 画面で、[保存] をクリックし、ダウンロードを実行します。ファイルのダウンロードにはしばらく時間がかかる場合があります。

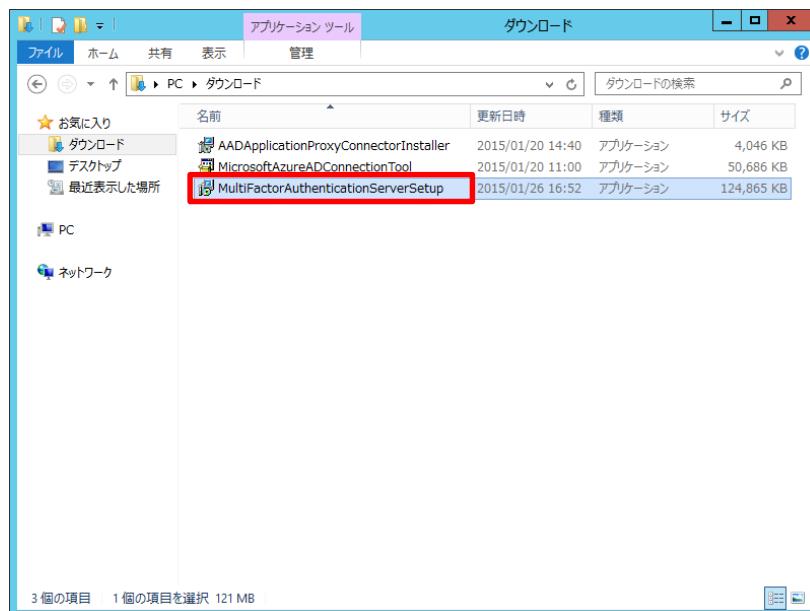


9. [Azure Multi-Factor Authentication] 画面で、[Generate New Activation Credentials] をクリックすると、[Email] と [Password] が表示されますので、メモ帳などに控えておきます。

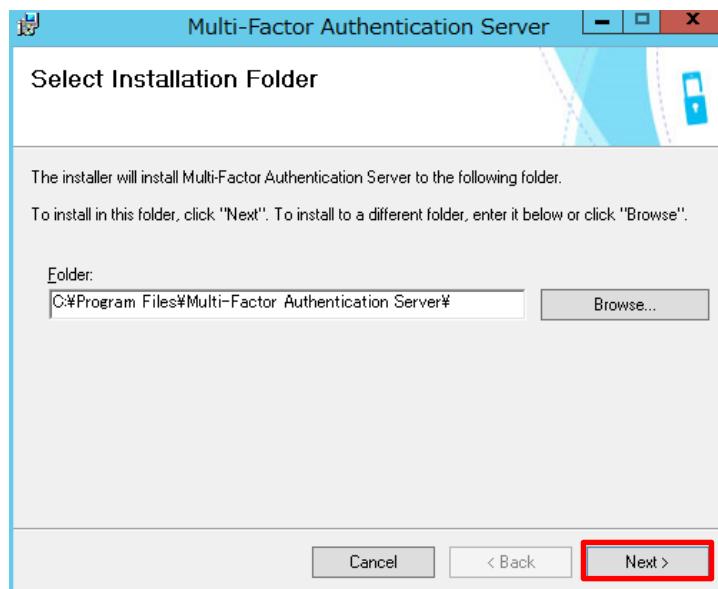


10. ダウンロードした保存先のフォルダーを開き、ダウンロードしたファイル

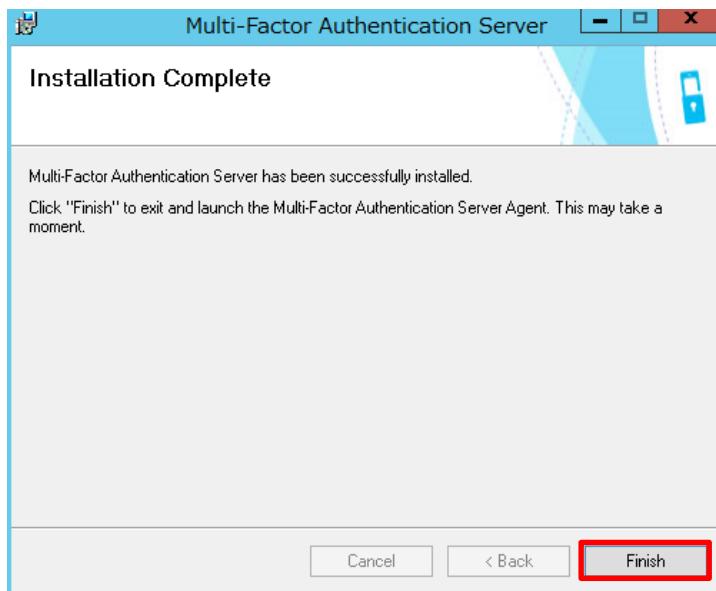
[MultiFactorAuthenticationServerSetup] をダブルクリックします。

**【Note:】**

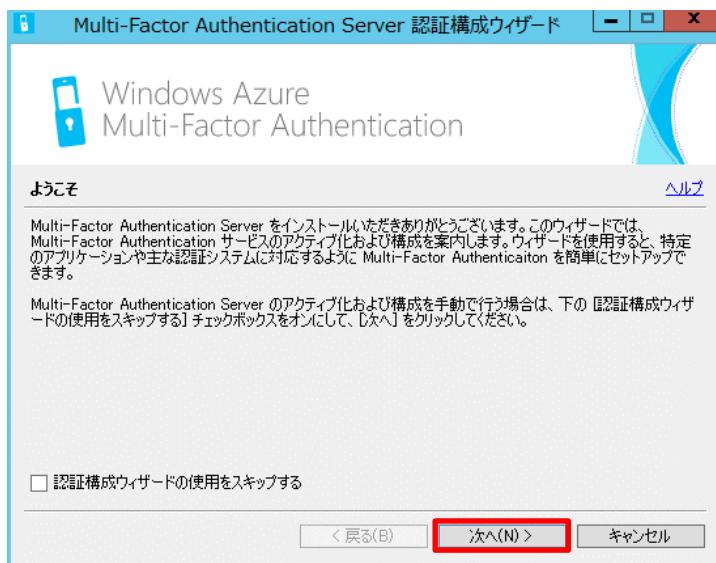
Multi-Factor Authentication Server のインストールには、.NET Framework Version 2.0.50727 が必要です。マイクロソフトの Web サイトより事前に .NET Framework を入手し、インストールしてください。

11. [Multi-Factor Authentication Server] 画面で、[Next] をクリックします。

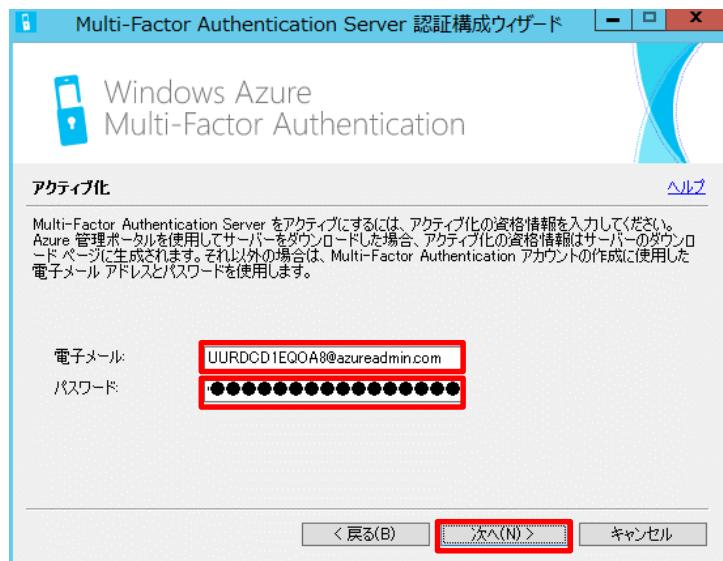
12. [Multi-Factor Authentication Server] 画面で、インストールが完了すると [Installation Complete] が表示されます。[Finish] をクリックします。



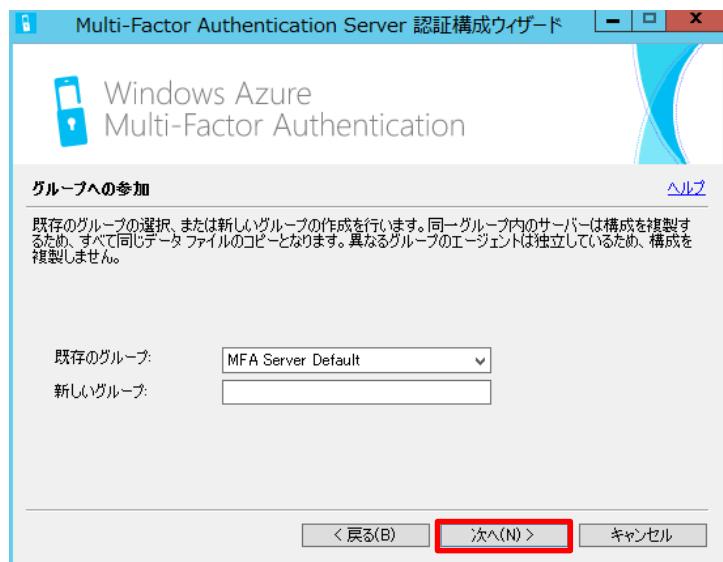
13. [Multi-Factor Authentication Server 認証構成ウィザード] 画面で、[次へ] をクリックします。



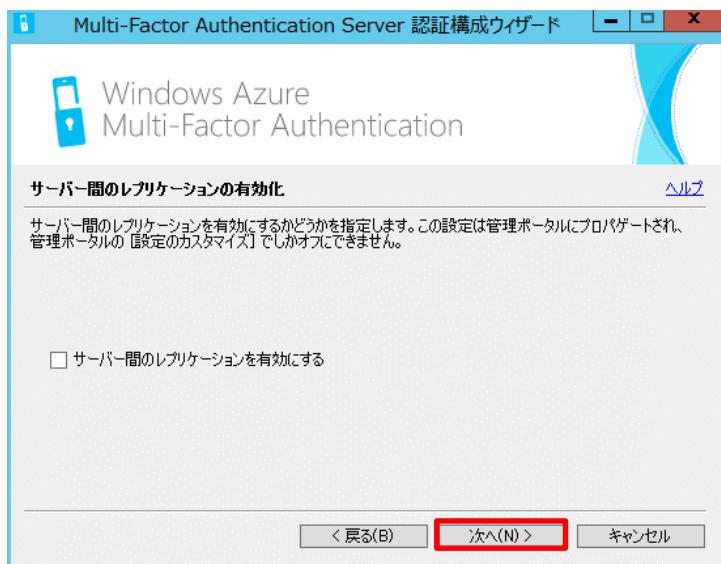
14. [アクティブ化] 画面で、手順 9 で控えておいた [Email] と [Password] を [電子メール]、[パスワード] にそれぞれ入力し、[次へ] をクリックします。



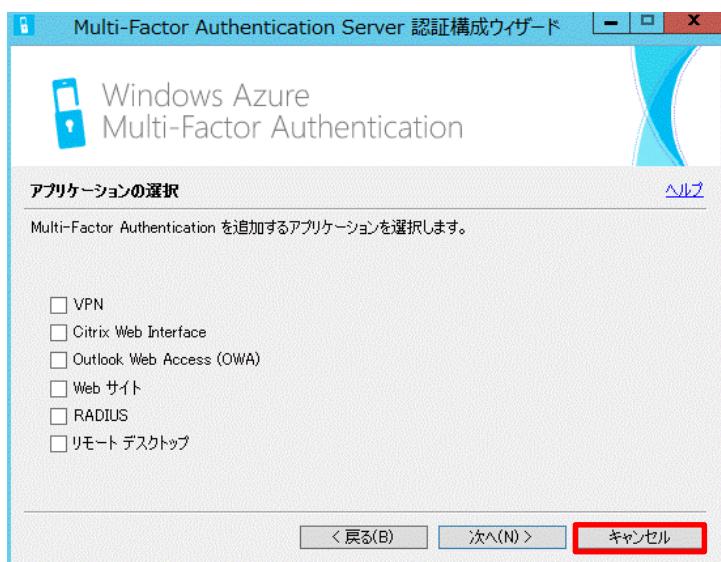
15. [グループへの参加] 画面で、[次へ] をクリックします。



16. [サーバー間のレプリケーションの有効化] 画面で、[次へ] をクリックします。



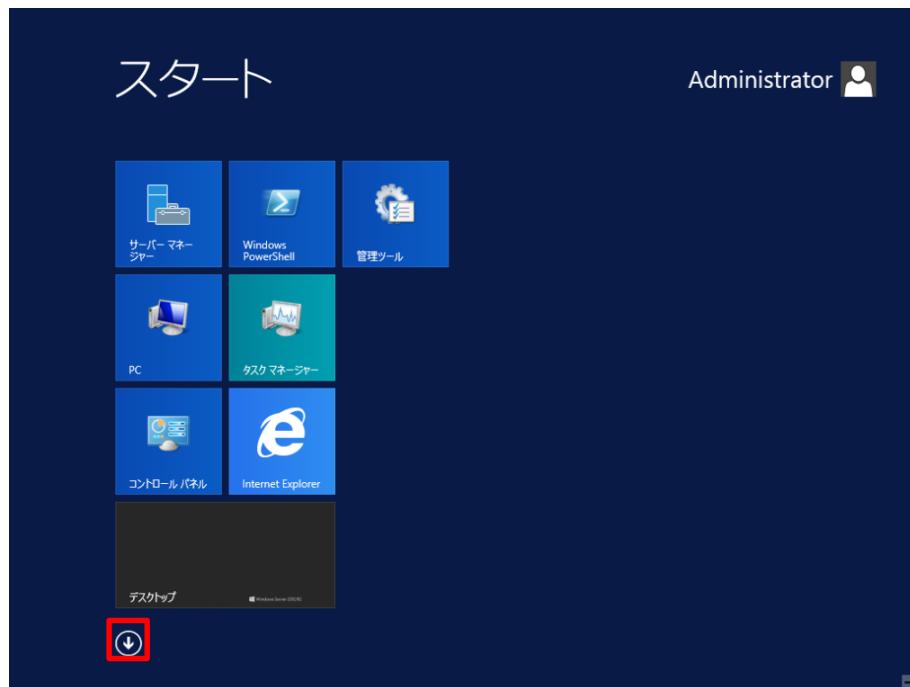
17. [アプリケーションの選択] 画面で、アプリケーションの選択を行わないため、[キャンセル] をクリックします。



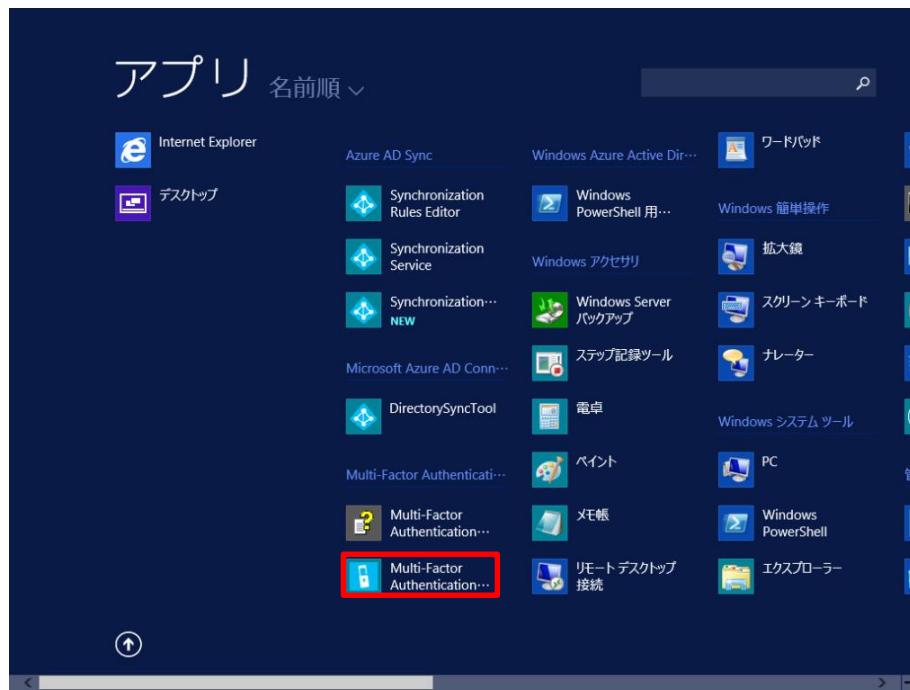
18. [Multi-Factor Authentication Server 認証構成ウィザード] 画面で、[はい] をクリックします。



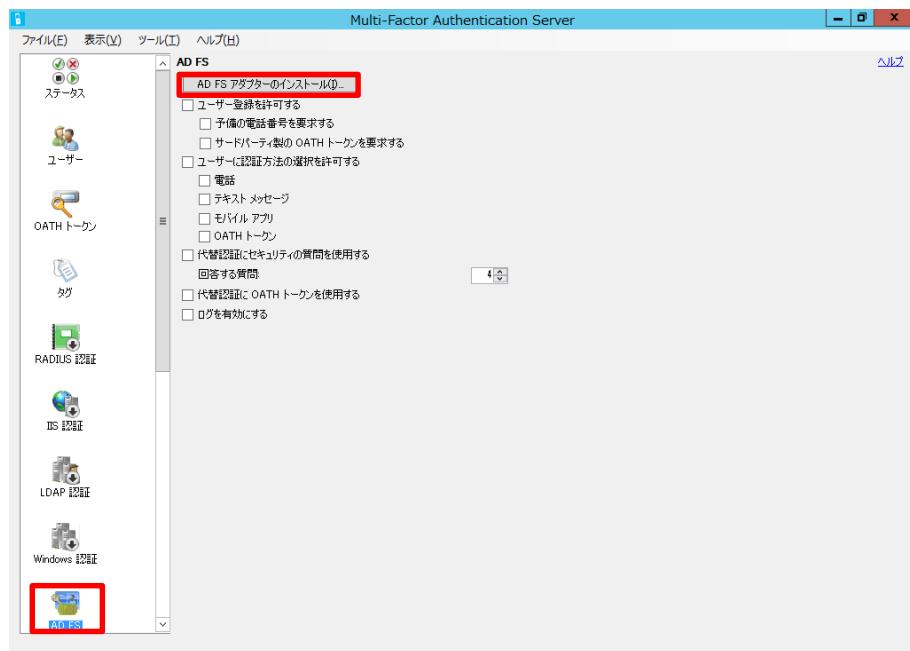
19. スタート画面で、[↓] をクリックします。



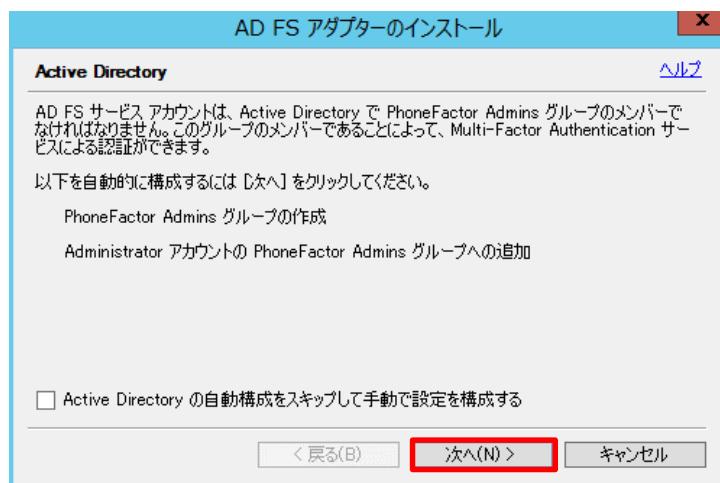
20. アプリ画面で、[Multi-Factor Authentication Server] アイコンをダブルクリックします。



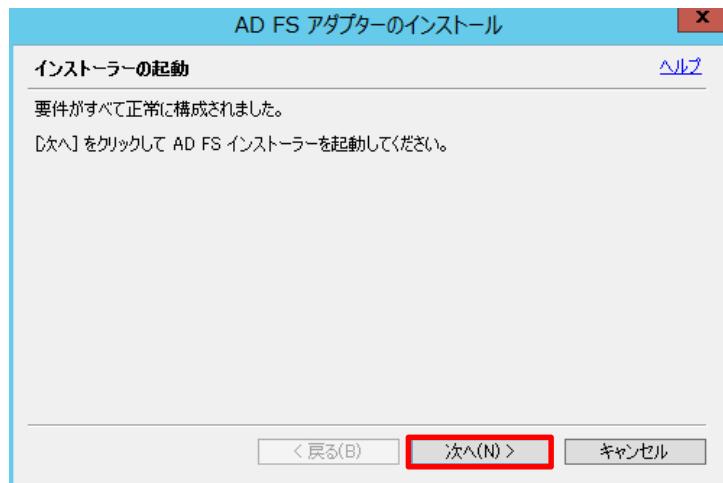
21. [Multi-Factor Authentication Server] 画面で、左ペインの [AD FS] をクリックし、[AD FS アダプターのインストール] をクリックします。



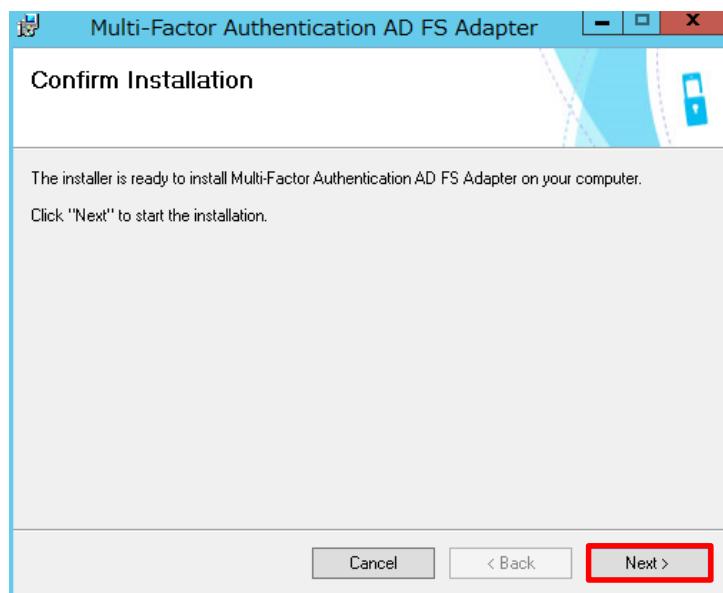
22. [AD FS アダプターのインストール] 画面で、[次へ] をクリックします。



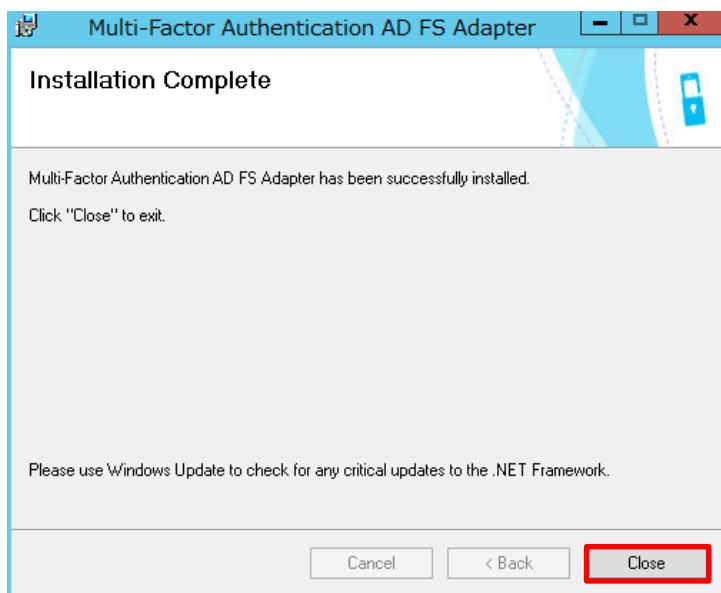
23. [インストラーの起動] 画面で、[次へ] をクリックします。



24. [Multi-Factor Authentication Server AD FS Adapter] 画面で、[Next] をクリックします。



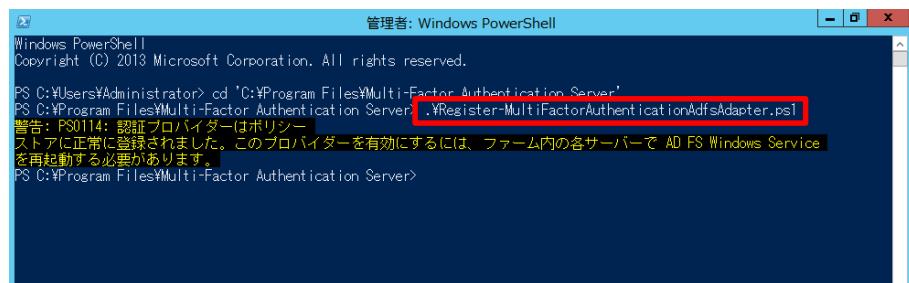
25. [Multi-Factor Authentication Server AD FS Adapter] 画面で、インストールが完了し、[Installation Complete] と表示されたら、[Close] をクリックします。



26. Windows Power Shell を起動します。「'cd C:\Program Files\Multi-Factor Authentication Server」と入力し、実行します。



27. Windows PowerShell 画面で、「.\\$Register-MultiFactorAuthenticationAdfsAdapter.ps1」と入力し、実行します。

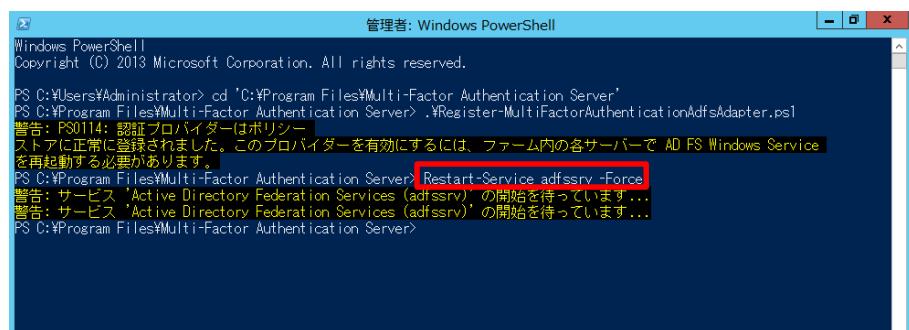


Windows PowerShell 管理者: Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.
PS C:\\$Users\\$Administrator> cd 'C:\Program Files\Multi-Factor Authentication Server'
PS C:\Program Files\Multi-Factor Authentication Server> .\\$Register-MultiFactorAuthenticationAdfsAdapter.ps1
警告: PS0114: 認証プロバイダーはポリシー
ストアに正常に登録されました。このプロバイダーを有効にするには、ファーム内の各サーバーで AD FS Windows Service
を再起動する必要があります。
PS C:\Program Files\Multi-Factor Authentication Server>

【Note:】

本手順によって、AD FS アダプターの登録が完了します。しかし、AD FS サーバーのユーザーインターフェイスに反映されるようにするには、AD FS サーバーを再起動する必要があります。

28. Windows PowerShell 画面で、「Restart-Service adfssrv -Force」と入力し、実行します。表示されるまで、しばらく時間がかかる場合があります。



Windows PowerShell 管理者: Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.
PS C:\\$Users\\$Administrator> cd 'C:\Program Files\Multi-Factor Authentication Server'
PS C:\Program Files\Multi-Factor Authentication Server> .\\$Register-MultiFactorAuthenticationAdfsAdapter.ps1
警告: PS0114: 認証プロバイダーはポリシー
ストアに正常に登録されました。このプロバイダーを有効にするには、ファーム内の各サーバーで AD FS Windows Service
を再起動する必要があります。
PS C:\Program Files\Multi-Factor Authentication Server> Restart-Service adfssrv -Force
警告: サービス 'Active Directory Federation Services (adfssrv)' の開始を待っています...
警告: サービス 'Active Directory Federation Services (adfssrv)' の開始を待っています...
PS C:\Program Files\Multi-Factor Authentication Server>

【Note:】

サービスの再起動に失敗する場合は、コンピューターを再起動して対処してください。

【Note:】

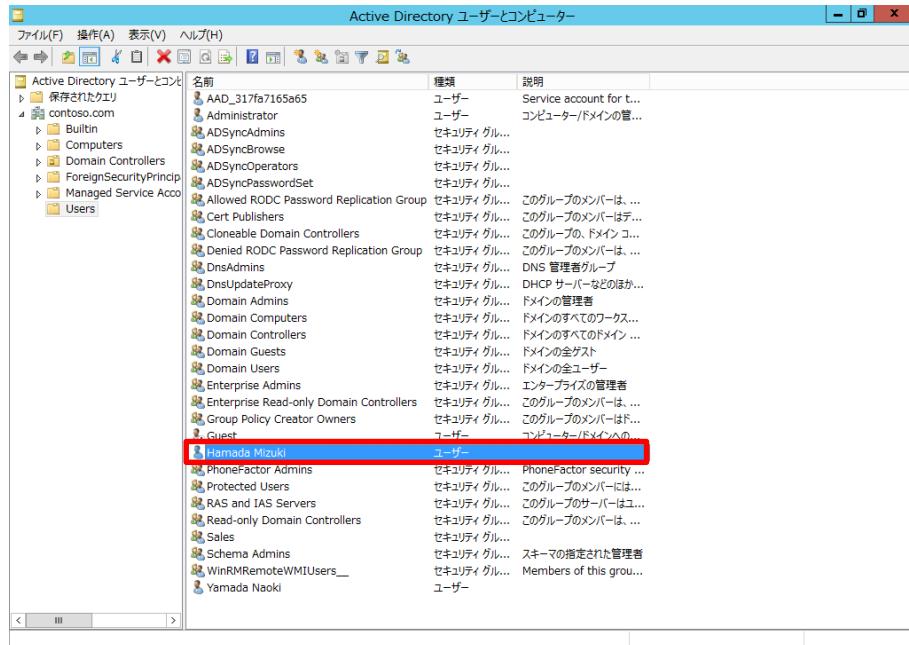
AD FS サーバーが複数台で構成される、ファーム構成の場合には、すべての AD FS サーバーで、本手順を実行してください。

➡ 電話番号の登録と多要素認証の実行

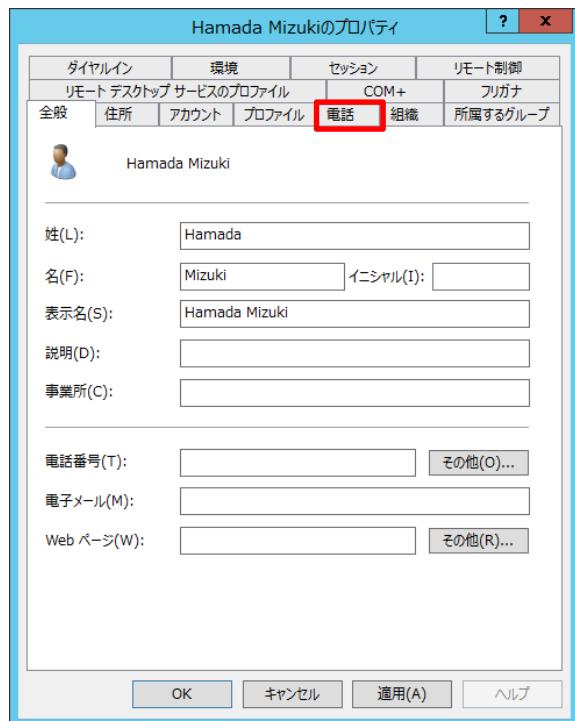
- [サーバー マネージャー] 画面で、[ツール] - [Active Directory ユーザーとコンピューター] をクリックします。



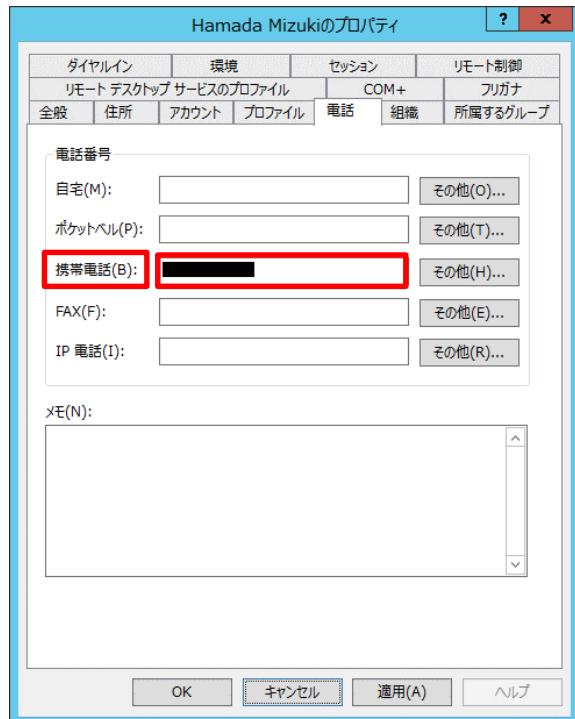
- [Active Directory ユーザーとコンピューター] 画面で、[Hamada Mizuki] ユーザーをダブルクリックします。



3. [プロパティ] 画面で、[電話] タブをクリックします。



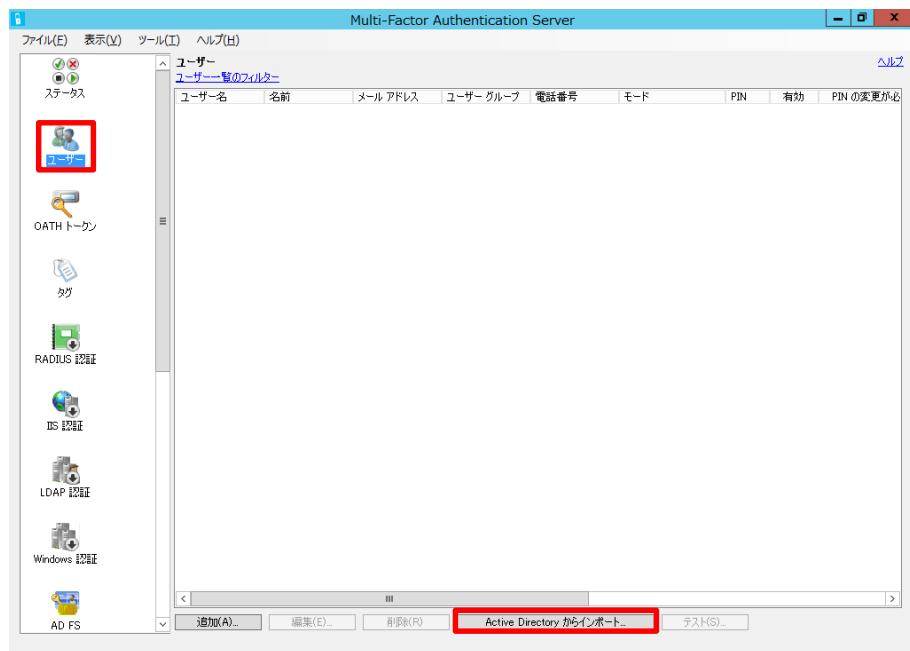
4. [電話] タブの画面で、[携帯電話] に携帯電話番号を入力し、[OK] をクリックします。



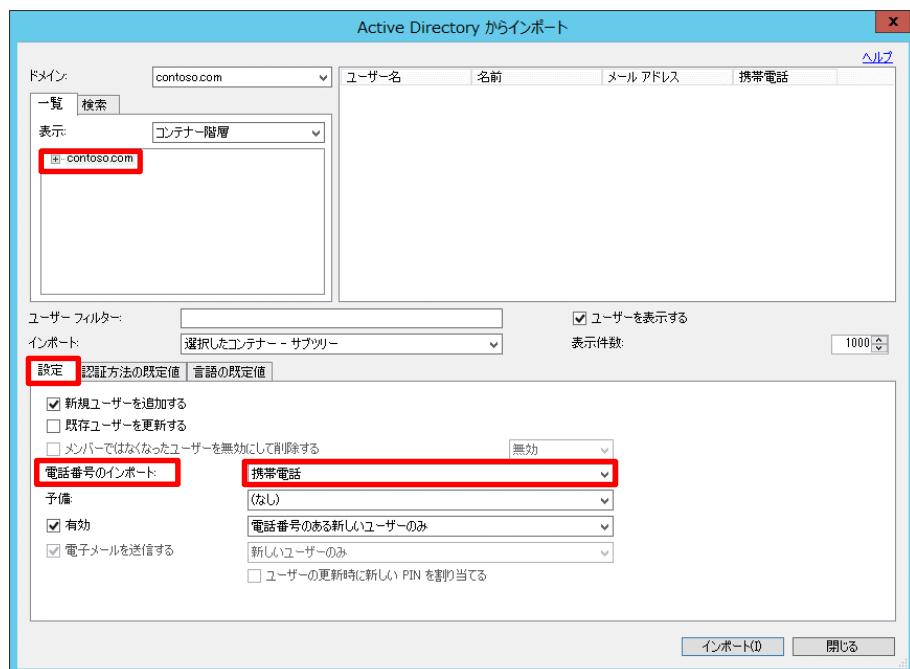
【Note:】

Active Directory ユーザーに登録する携帯電話番号には先頭の 0 をつける必要はありません。また、ハイフンの入力も不要です。(たとえば、090-1111-1111 の電話番号の場合、9011111111 と登録します。)

5. [Multi-Factor Authentication Server] 画面に戻ります。[ユーザー] をクリックし、[Active Directory からインポート] をクリックします。



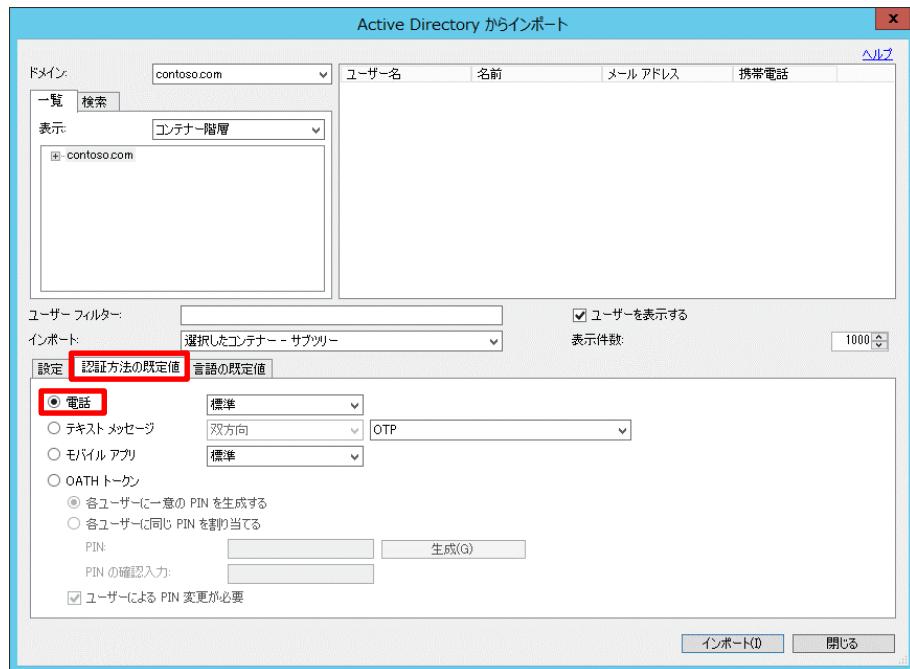
6. [Active Directory からインポート] 画面で、[ドメイン] が [contoso.com] になっていること、[設定] タブ内の [電話番号のインポート] が [携帯電話] になっていることを確認します。



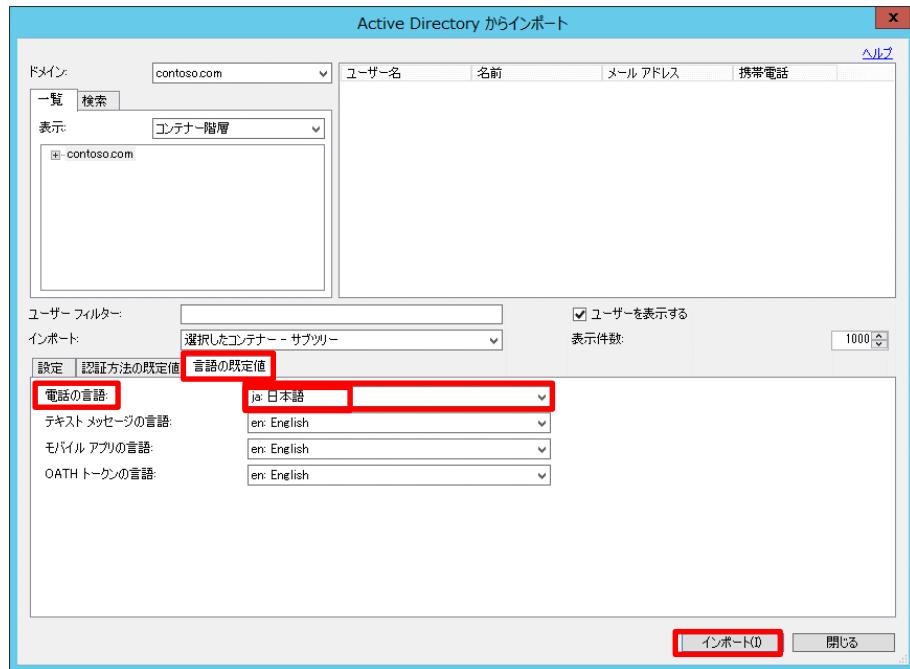
【Note:】

2回目以降のインポートで、Azure AD にインポートする電話番号が変わった場合は [既存ユーザーを更新する] チェックボックスにチェックをつけてインポートしてください。

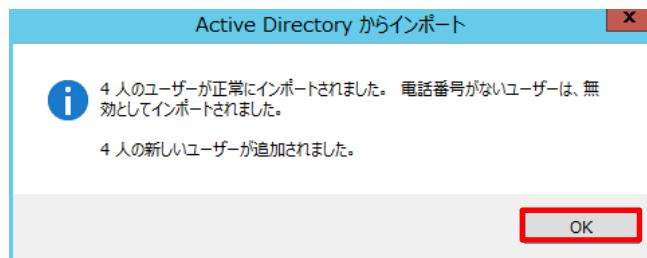
7. [Active Directory からインポート] 画面で、[認証方法の既定値] タブ内では [電話] が選択されていることを確認します。



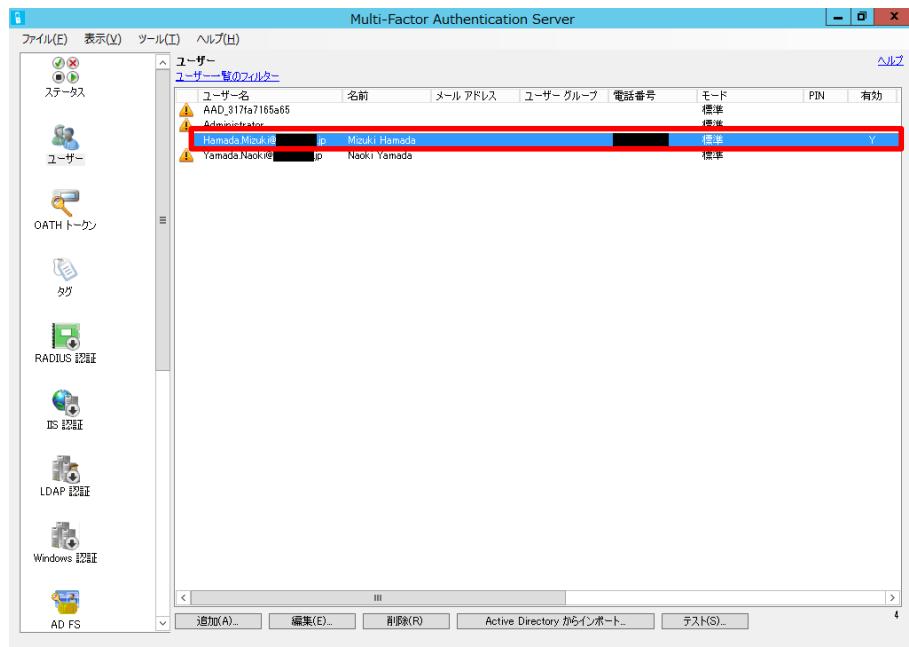
8. [Active Directory からインポート] 画面で、[言語の既定値] タブ内では [電話の言語] をプルダウンメニューより [ja:日本語] を選択します。選択が完了したら、[インポート] をクリックします。



9. [Active Directory からインポート] 画面で、[OK] をクリックします。[Active Directory からインポート] 画面は、[閉じる] をクリックします。

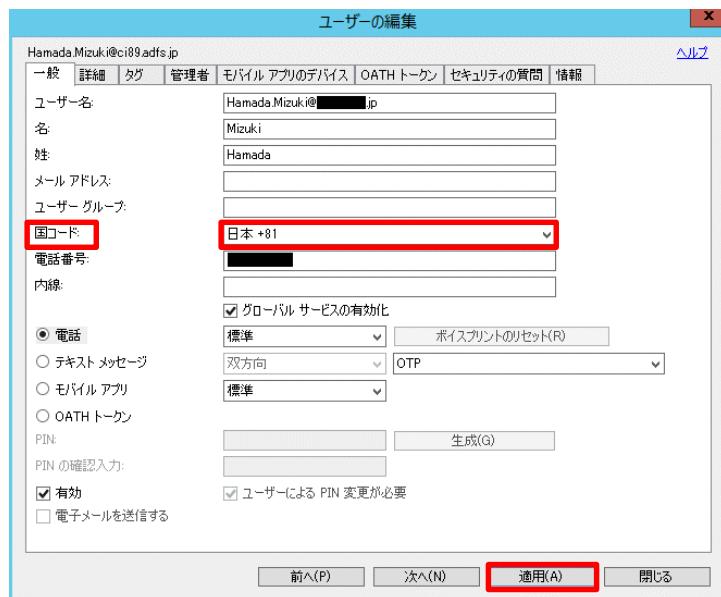


10. [Multi-Factor Authentication Server] 画面に戻ります。ユーザーの情報がインポートされたことが確認できます。インポートされた、Hamada Mizuki ユーザーをダブルクリックします。

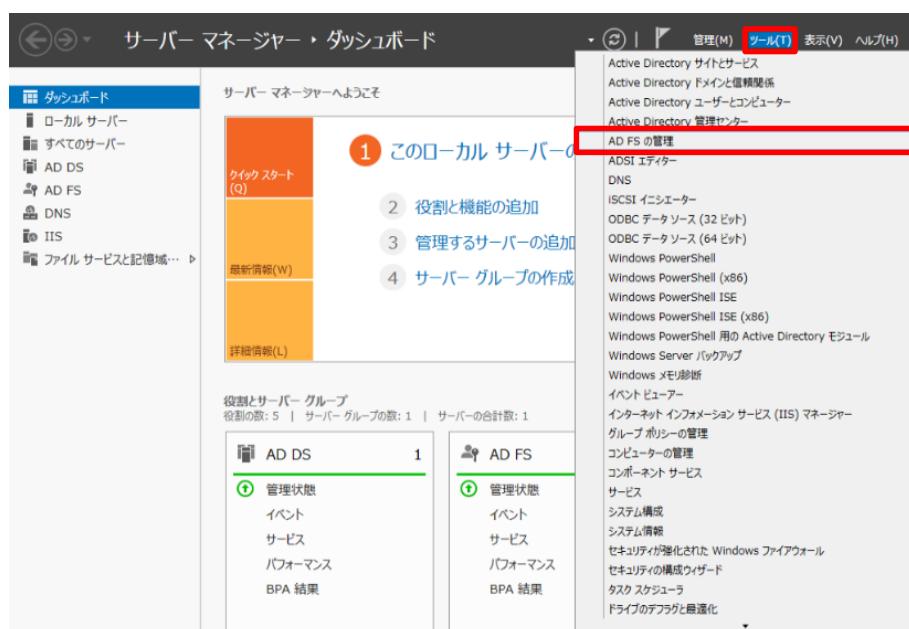


Microsoft Azure Active Directory の活用

11. [ユーザーの編集] で、[国コード] をプルダウンメニューから [日本] を選択します。[適用] をクリックし、[閉じる] で画面を閉じます。

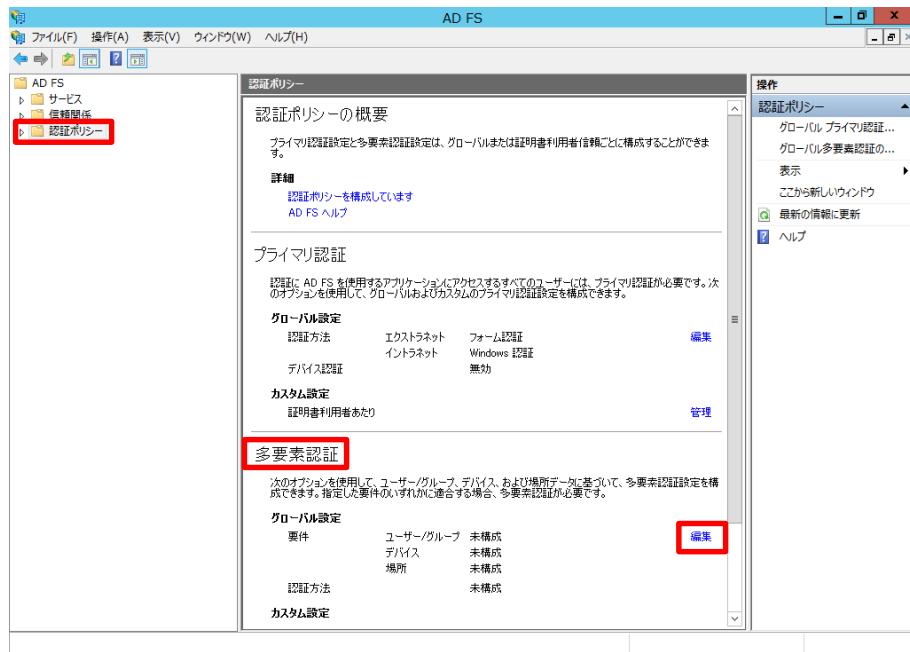


12. [サーバー マネージャー] 画面で、[ツール] - [AD FS の管理] をクリックします。

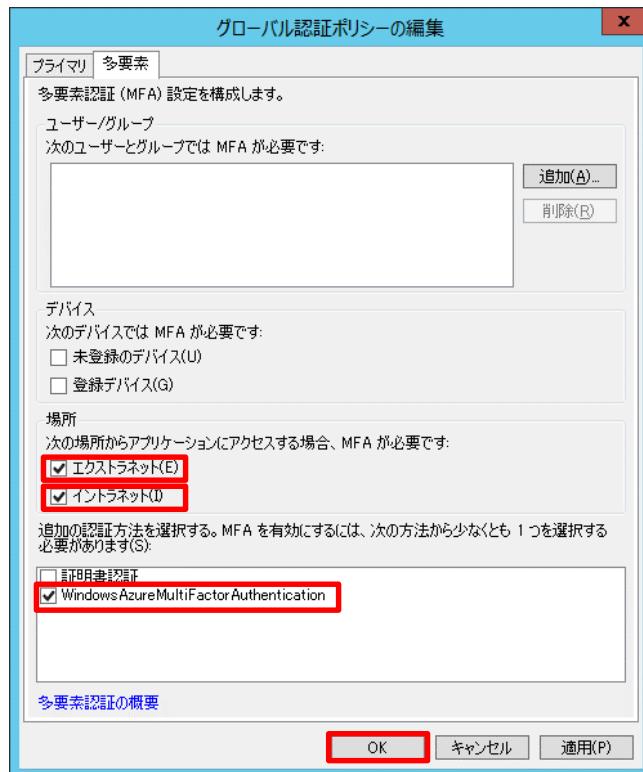


Microsoft Azure Active Directory の活用

13. [AD FS] の管理画面で、[認証ポリシー] をクリックし、中央ペイン下の [多要素認証] - [編集] をクリックします。



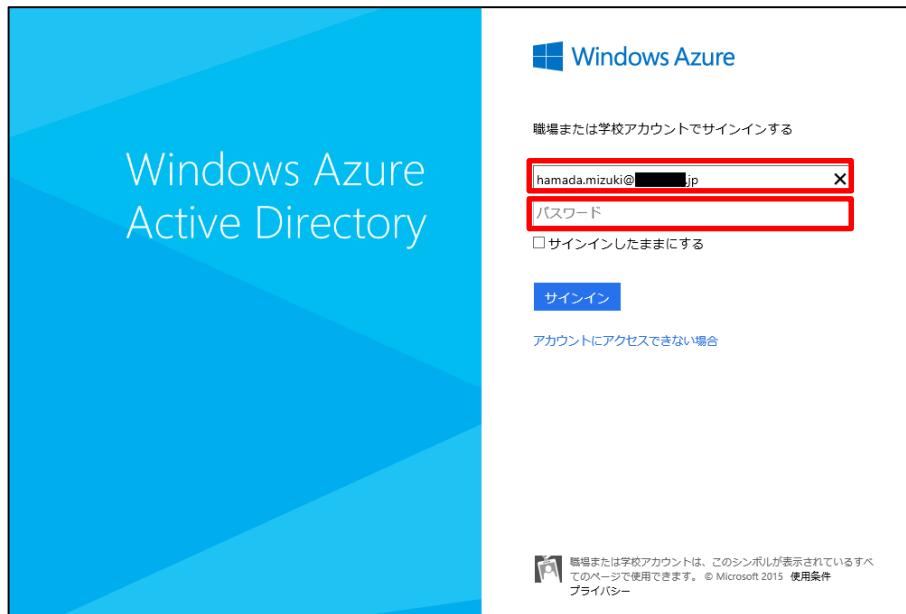
14. [グローバル認証ポリシーの編集] 画面で、[多要素] タブの [エクストラネット]、[インターネット] にチェックをします。さらに [WindowsAzureMultiFactorAuthentication] にチェックをし、[OK]をクリックします。



15. W81CL01 コンピューターで操作します。

Hamada Mizuki ユーザーでサインインし、ブラウザーを起動して、アクセス パネルの URL である <http://myapps.microsoft.com/> にアクセスします。

アクセス パネルの Web サイトで、Hamada Mizuki@<Microsoft Azure に登録された自己所有パブリック ドメイン名>ユーザーでサインインします。



16. Web ページがリダイレクトされ、[Multi-Factor Authentication] の Web ページが表示されます。[続行] をクリックします。



17. Hamada Mizuki ユーザーの登録された携帯電話番号に着信します。音声ガイダンスに従って、電話の # ボタンを押すとアクセス パネルの Web ページにアクセスすることができます。



6.4 デバイスの登録

Windows Server 2012 R2 の AD FS サーバーに実装されているデバイス認証機能を利用する場合、AD FS サーバー自身が提供するデバイス登録サービスではなく、Azure AD Premium で提供するデバイス登録サービスを代わりに利用することができます。Azure AD のデバイス登録サービスを利用するためには手順を本節では確認します。

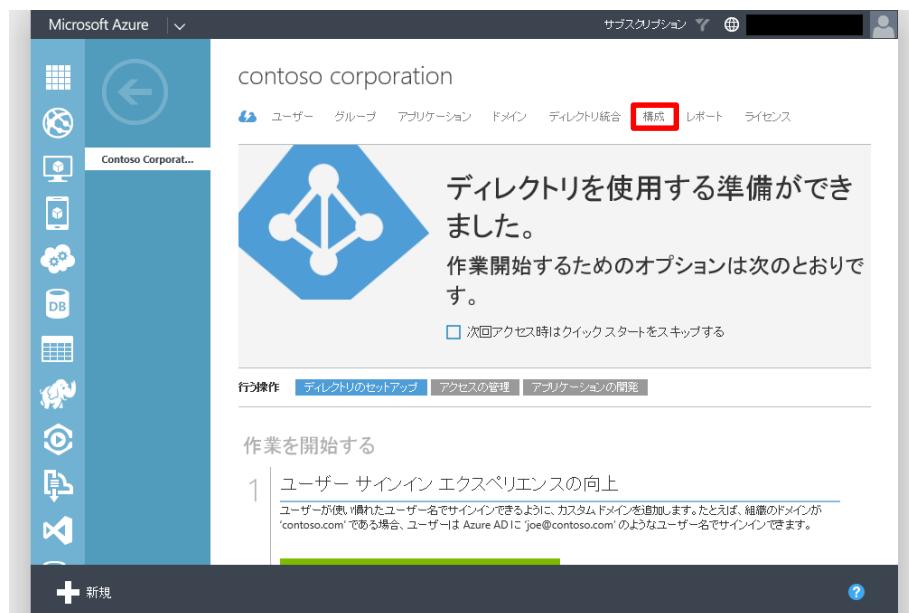
※ 「2.10 デバイス登録サービス」でも解説したように、デバイスの登録自体は AD FS サーバーがない状態でもできますが、デバイス認証には AD FS サーバーが必要です。

◆ クライアントによるデバイスの登録

1. Microsoft Azure 管理ポータル画面で、[ACTIVE DIRECTORY] をクリックし、[Contoso corporation] をクリックします。

名前	状態	ロール	サブスクリプション	データセンターの地域	国/地域
Contoso Corp...	✓ アクティブ	全体管理者	すべての Contoso C...	アジア、ヨーロッパ、...	日本

2. [Contoso corporation] 画面で、[構成] をクリックします。



3. [構成] 画面で、[デバイス] - [DEVICE REGISTRATION の有効化] - [はい] をクリックし、[保存] をクリックします。

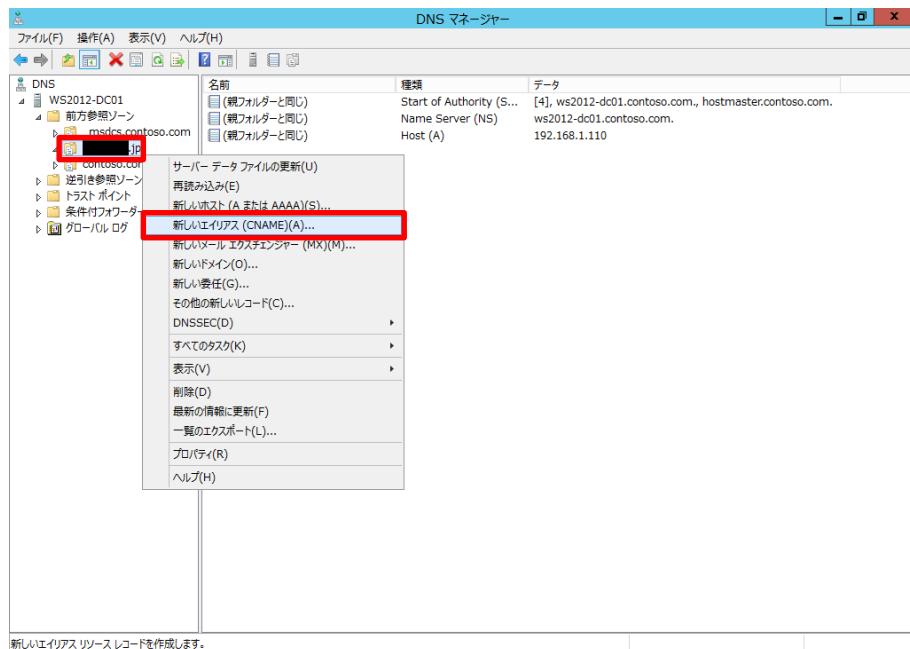


4. WS2012-DC01 コンピューターで操作します。

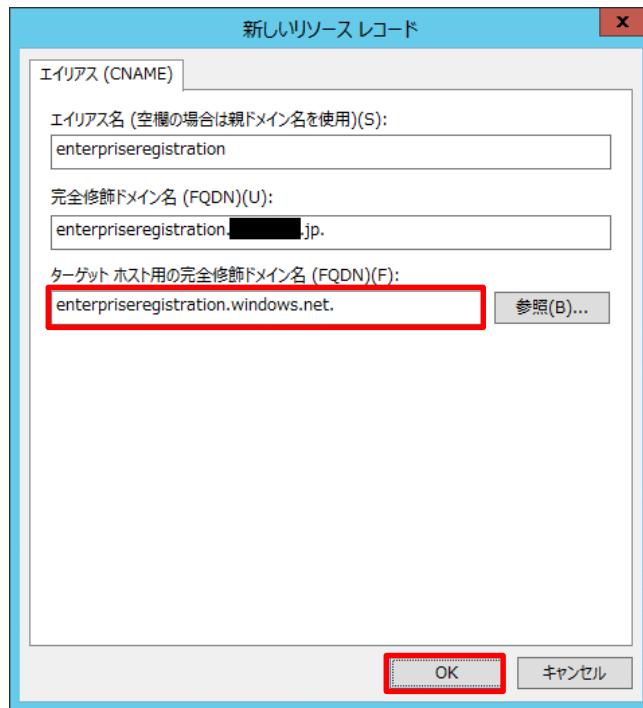
[サーバー マネージャー] 画面で、[ツール] - [DNS] をクリックします。



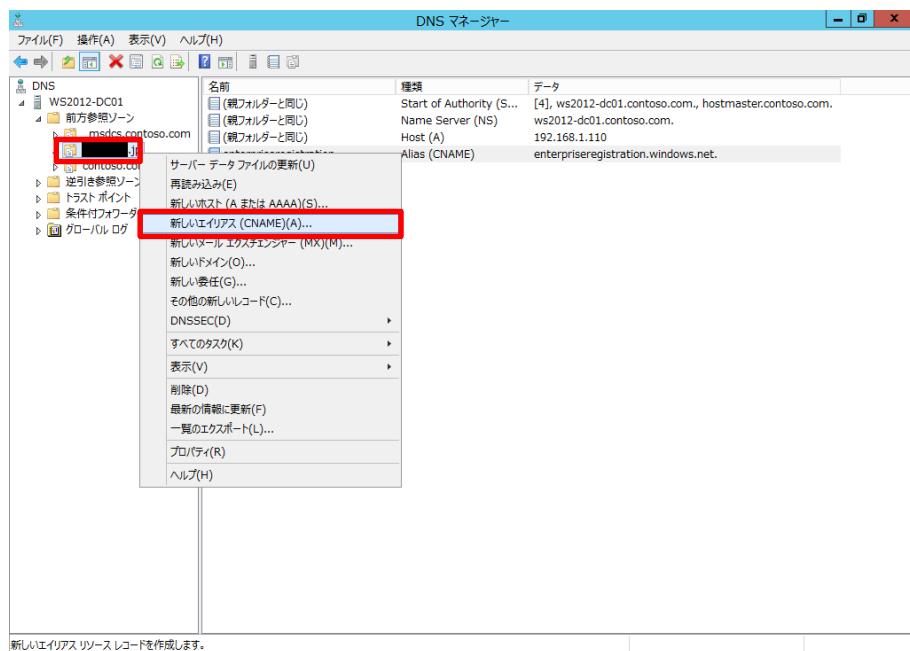
5. [DNS マネージャー] 画面で、左ペインの [WS2012-DC01] - [前方参照ゾーン] - [(自己所有パブリック ドメイン名)] の順に展開し、[(自己所有パブリック ドメイン名)] を右クリックして、[新しいエイリアス (CNAME)] をクリックします。



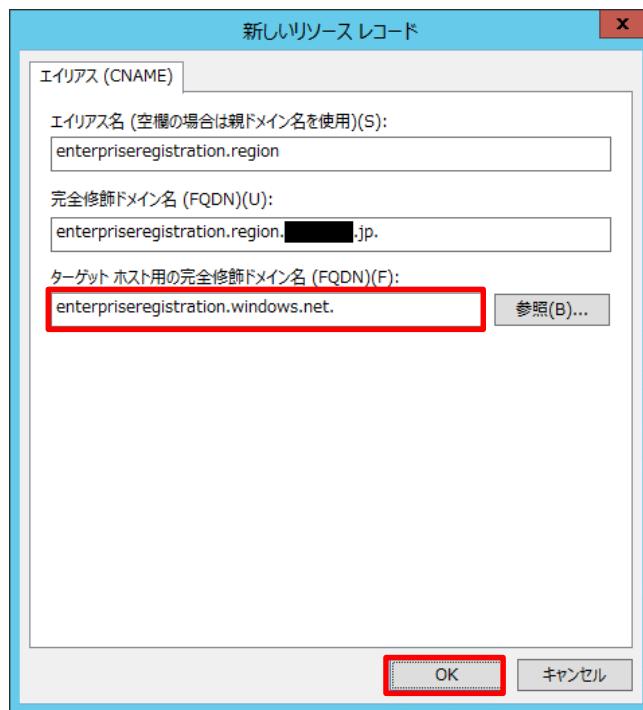
6. [新しいリソース レコード] 画面で、[エイリアス名] 欄に「enterpriseregistration」、[ターゲット ホスト用の完全修飾ドメイン名 (FQDN)] 欄に「enterpriseregistration.windows.net.」とそれぞれ入力し、[OK] をクリックします。



7. [DNS マネージャー] 画面で、左ペインの [WS2012-DC01] - [前方参照ゾーン] - [(自己所有パブリック ドメイン名)] の順に展開し、[(自己所有パブリック ドメイン名)] を右クリックして、[新しいエイリアス (CNAME)] をクリックします。



8. [新しいリソース レコード] 画面で、[エイリアス名] 欄に「enterpriseregistration.region」、[ターゲット ホスト用の完全修飾ドメイン名 (FQDN)] 欄に「enterpriseregistration.windows.net.」とそれぞれ入力し、[OK] をクリックします。

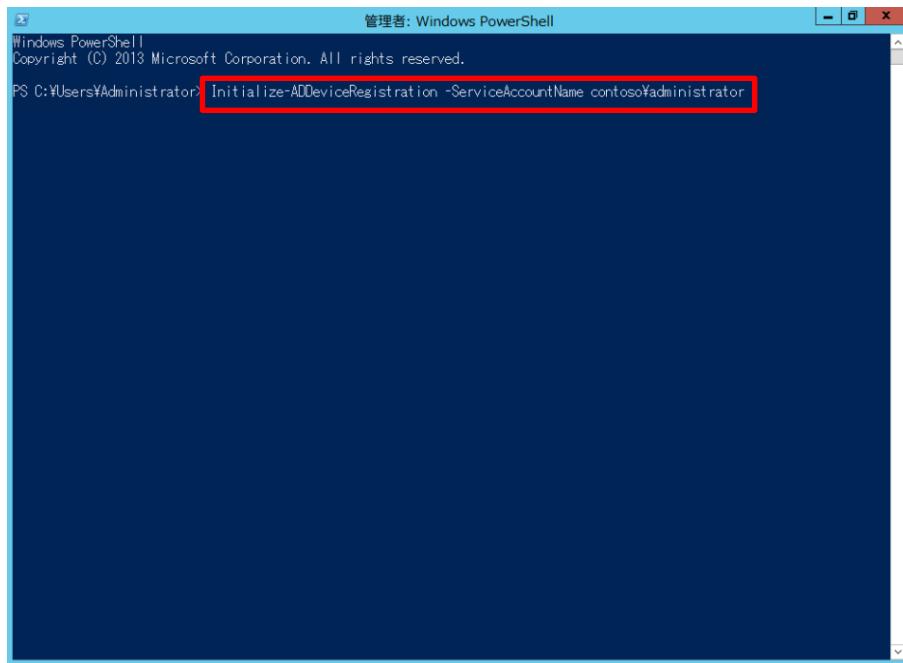


9. インターネット向け DNS サーバーに対して、以下の DNS レコードを登録します。

レコード種類	エイリアス名	FQDN
CNAME	enterpriseregistration.< 自己所有パブリック ドメイン名 >	enterpriseregistration.windows.net
CNAME	enterpriseregistration.region.< 自己所有パブリック ドメイン名 >	enterpriseregistration.windows.net

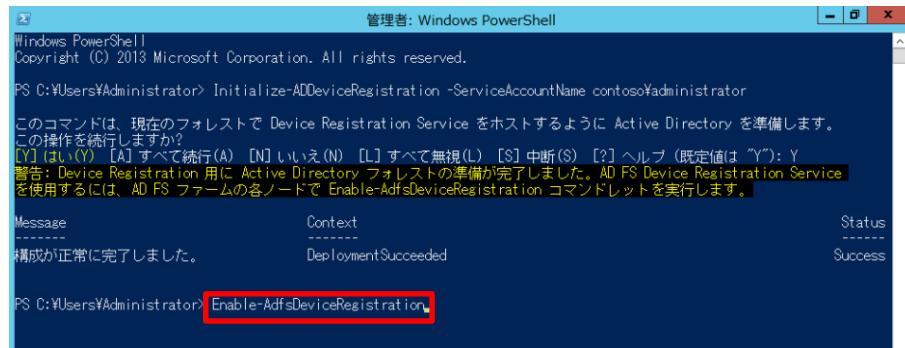
10. DNS サーバーにレコードを登録後、Windows PowerShell を起動します。

コマンド「Initialize-ADDeviceRegistration -ServiceAccountName contoso\\$administrator」を入力し、エンターキーを入力します。

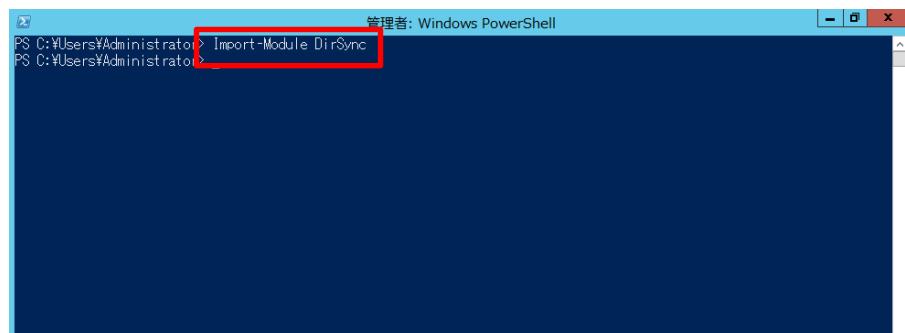
**【Note:】**

Initialize-ADDeviceRegistration -ServiceAccountName に続くアカウント名は AD FS サーバーのサービス アカウントを入力します。お使いの環境に合わせて書き換えてください。

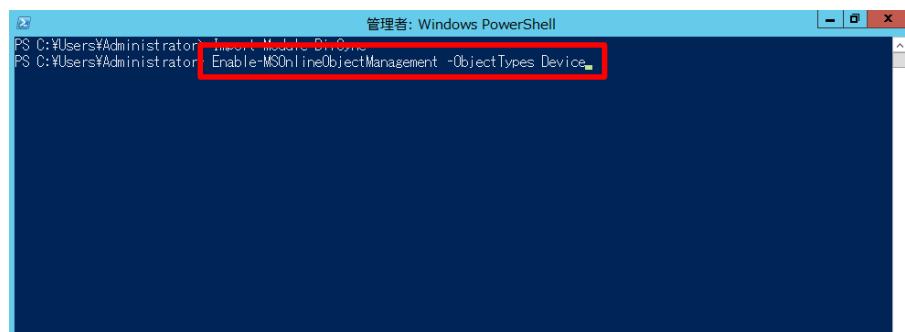
11. [Windows PowerShell] 画面で、「Y」を入力し、実行します。

12. [Windows PowerShell] 画面で、コマンド「Enable-AdfsDeviceRegistration」を入力し、実行します。

管理者: Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.
PS C:\\$Users\\$Administrator> Initialize-ADDeviceRegistration -ServiceAccountName contoso\\$administrator
このコマンドは、現在のフォレストで Device Registration Service をホストするように Active Directory を準備します。
この操作を続行しますか?
[Y] (はい)(Y) [A] すべて続行(A) [N] いいえ(N) [L] すべて無視(L) [S] 中断(S) [?] ヘルプ (既定値は "Y"): Y
警告: Device Registration 用に Active Directory フォレストの準備が完了しました。AD FS Device Registration Service
を使用するには、AD FS ファームの各ノードで Enable-AdfsDeviceRegistration コマンドレットを実行します。
Message Context Status
----- -----
構成が正常に完了しました。 DeploymentSucceeded Success
PS C:\\$Users\\$Administrator> **Enable-AdfsDeviceRegistration**

13. [Windows PowerShell] 画面で、「Import-Module DirSync」と入力し、Enter キーを押します。

管理者: Windows PowerShell
PS C:\\$Users\\$Administrator> Import-Module DirSync
PS C:\\$Users\\$Administrator>

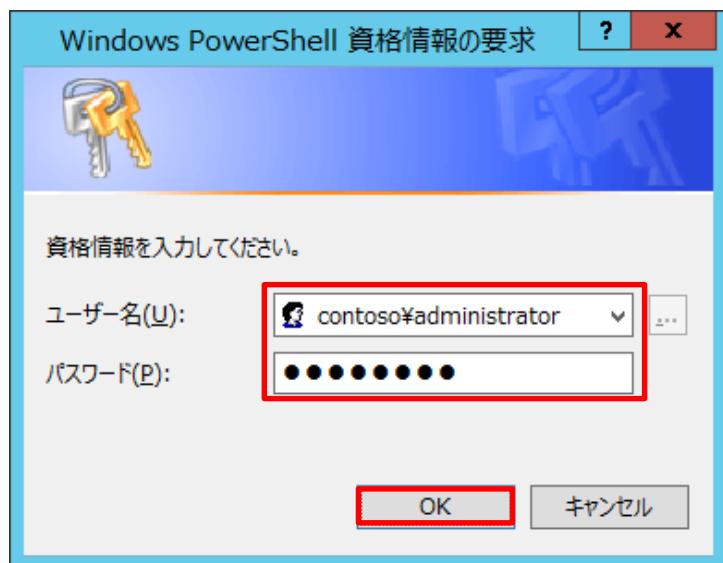
14. [Windows PowerShell] 画面で、「Enable-MSOnlineObjectManagement -ObjectTypes Device」と入力し、Enter キーを押します。

管理者: Windows PowerShell
PS C:\\$Users\\$Administrator> Import-Module CSOnline
PS C:\\$Users\\$Administrator> **Enable-MSOnlineObjectManagement -ObjectTypes Device**

15. [Windows PowerShell 資格情報の要求] 画面で、Azure AD 全体管理者のユーザー名とパスワードを入力し、[OK] をクリックします。

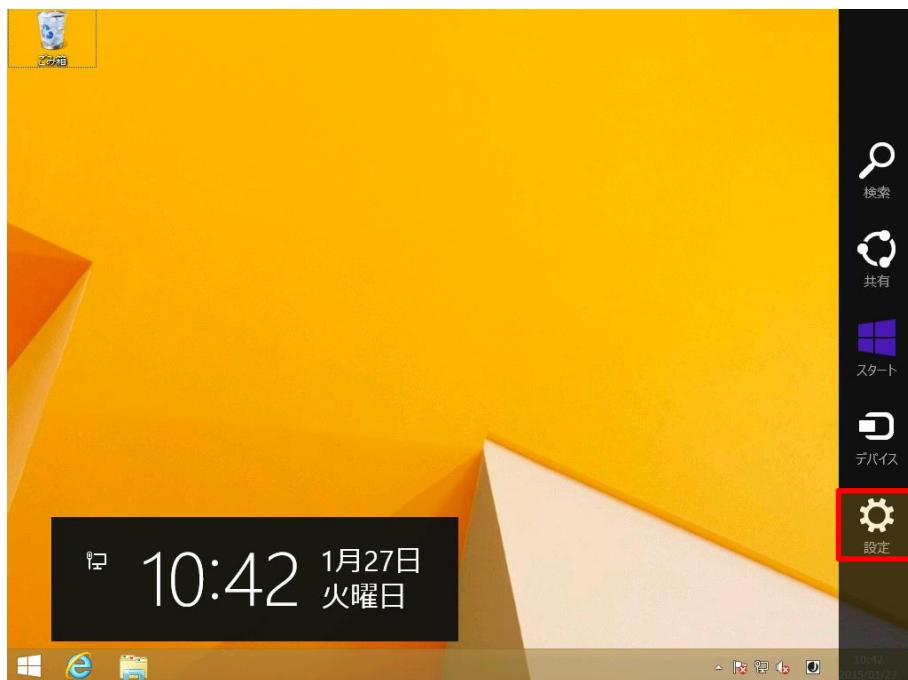


16. [Windows PowerShell 資格情報の要求] 画面で、Active Directory 管理者のユーザー名とパスワードを入力し、[OK] をクリックします。

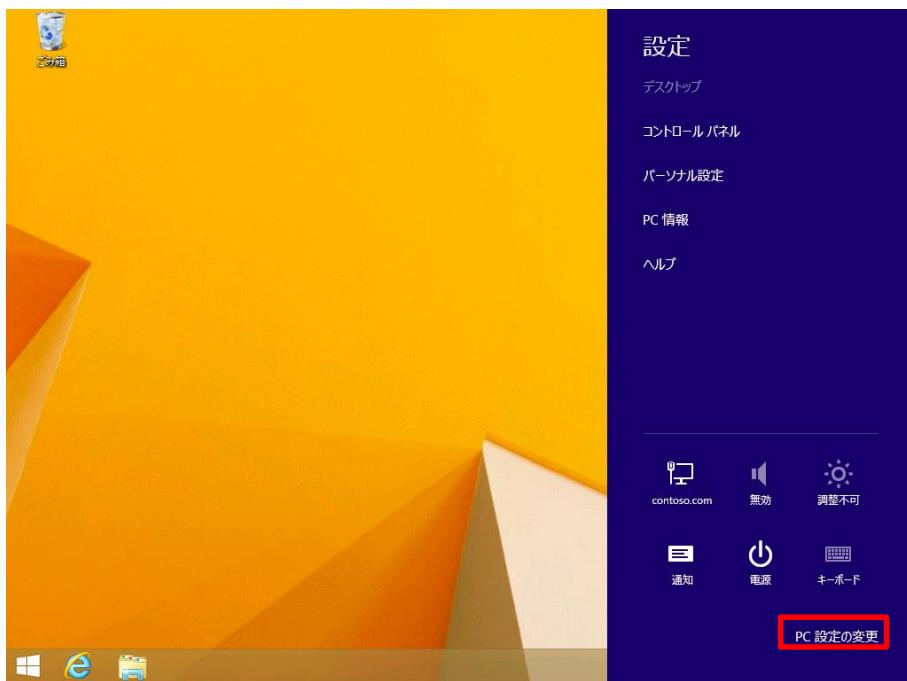


17. W81CL01 コンピューターで操作します。

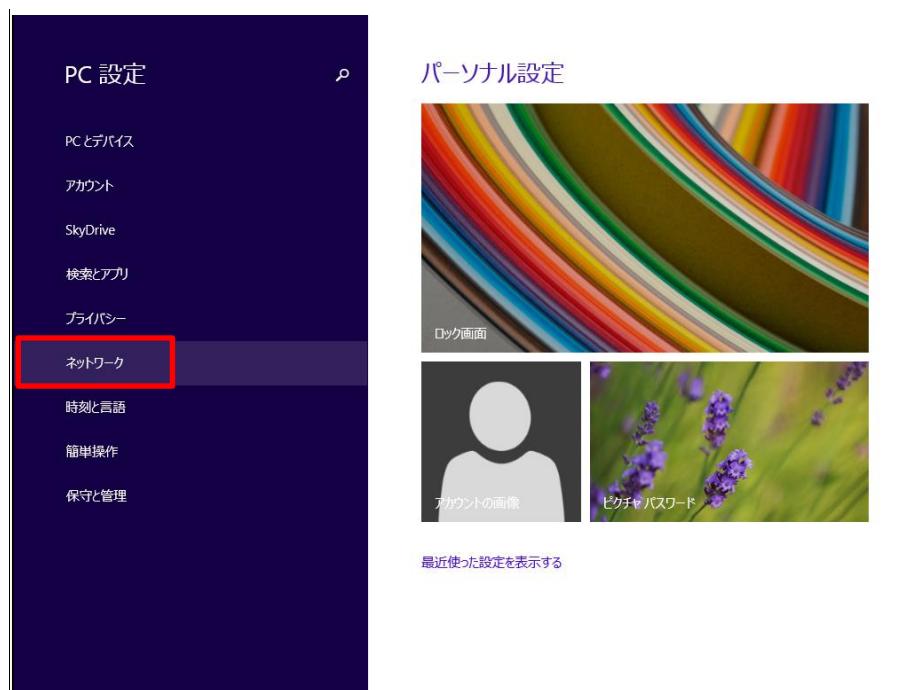
Hamada Mizuki ユーザーでサインインし、デスクトップ画面で Windows + C キーを押し、[設定] をクリックします。



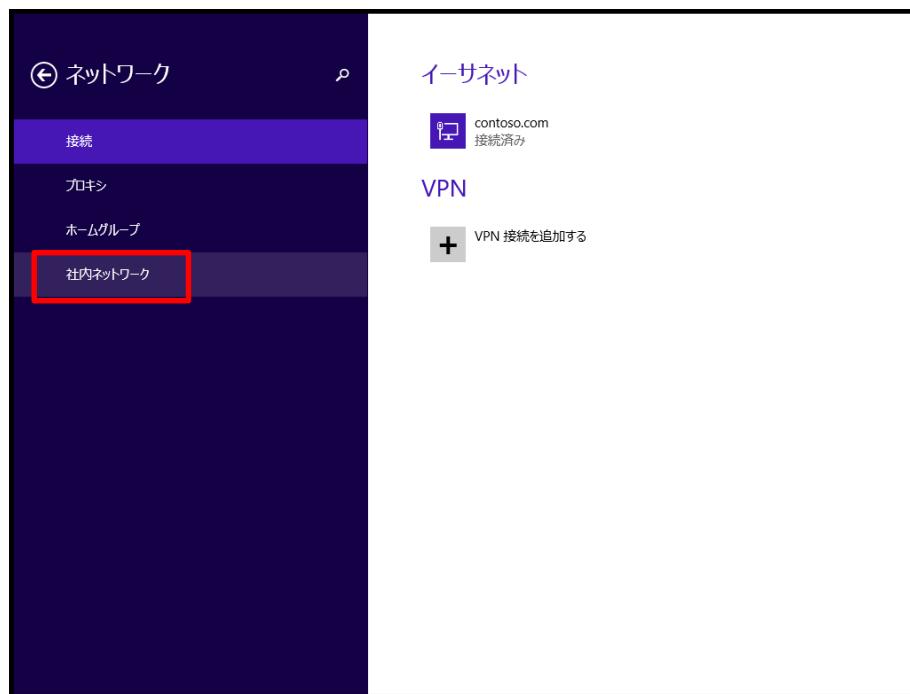
18. [設定] 画面で、[PC 設定の変更] をクリックします。



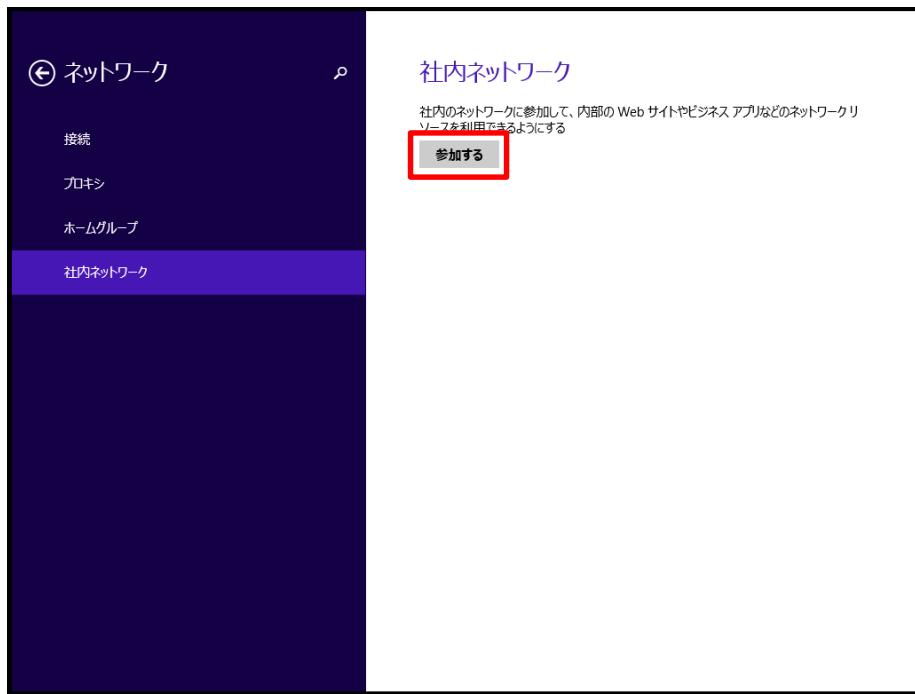
19. [PC 設定] 画面で、[ネットワーク] をクリックします。



20. [ネットワーク] 画面で [社内ネットワーク] をクリックします。



21. [社内ネットワーク] 画面で、[参加する] をクリックします。すると、W81CL01 コンピューターがデバイス登録サービスによって Hamada.Mizuki ユーザーのデバイスとして Azure AD に登録されます。



➡ 登録されたデバイスの確認

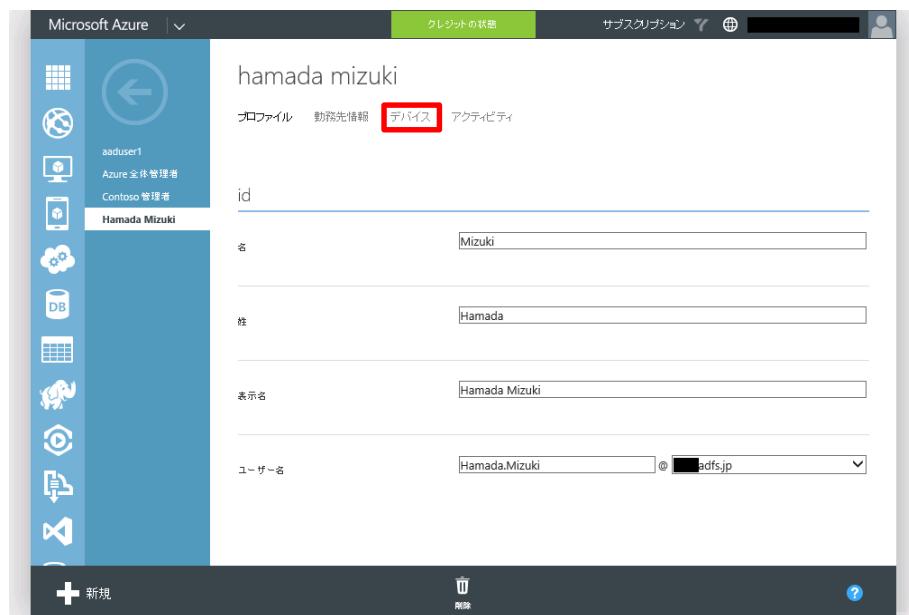
1. Azure 管理ポータル画面の [Contoso corporation] 画面で、[ユーザー] をクリックします。

The screenshot shows the Microsoft Azure Management Portal interface for the 'contoso corporation' tenant. The left sidebar contains various service icons. The top navigation bar has tabs for 'ユーザー' (User), 'グループ' (Group), 'アプリケーション' (Application), 'ドメイン' (Domain), 'ディレクトリ統合' (Directory Integration), '構成' (Configuration), 'レポート' (Report), and 'ライセンス' (Licenses). The 'ユーザー' tab is highlighted with a red box. The main content area features a blue diamond icon with three nodes connected by lines. Text reads: 'ディレクトリを使用する準備ができました。作業開始するためのオプションは次のとおりです。' Below this is a checkbox labeled '□ 次回アクセス時はクイックスタートをスキップする'. At the bottom, there's a task list with the first item being 'ユーザー サインイン エクスペリエンスの向上'. A note below it says: 'ユーザーが使用慣れたユーザー名でサインインできるように、カスタムドメインを追加しました。たとえば、組織のドメインが "contoso.com" である場合、ユーザーは Azure AD に "joe@contoso.com" のようなユーザー名でサインインできます。' A green progress bar is shown at the bottom of the task list.

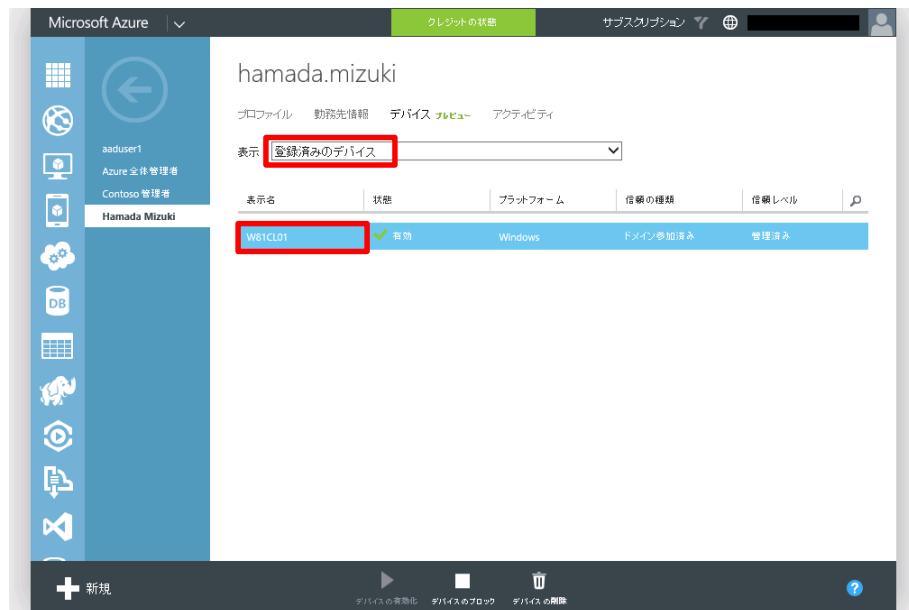
2. [Contoso corporation] 画面で、Hamada.Mizuki ユーザーをクリックします。

The screenshot shows the 'User' list in the Microsoft Azure Management Portal for the 'contoso corporation' tenant. The left sidebar is visible with its service icons. The top navigation bar has tabs for 'ユーザー' (User), 'グループ' (Group), 'アプリケーション' (Application), 'ドメイン' (Domain), 'ディレクトリ統合' (Directory Integration), '構成' (Configuration), 'レポート' (Report), and 'ライセンス' (Licenses). The 'ユーザー' tab is selected. The main content area displays a table with columns: '表示名' (Display Name), 'ユーザー名' (User Name), and 'ソース ディレクトリ' (Source Directory). The table rows are: 'aaduser1' (User Name: aaduser1@████████.onmicrosoft.com, Source: Microsoft Azure の Active Directory), 'Azure 全体管理者' (User Name: Azure AD administrator@████████.onmicrosoft.com, Source: Microsoft アカウント), 'Contoso 管理者' (User Name: admin@████████.onmicrosoft.com, Source: Microsoft Azure の Active Directory), 'Hamada Mizuki' (User Name: Hamada.Mizuki@████████.onmicrosoft.com, Source: ローカル Active Directory), and 'Yamada Naoki' (User Name: Yamada.Naoki@████████.onmicrosoft.com, Source: ローカル Active Directory). The row for 'Hamada Mizuki' is highlighted with a red box.

3. [Hamada.Mizuki] 画面で、[デバイス] をクリックします。



4. [Hamada.Mizuki] 画面で、[表示] 欄から [登録済みのデバイス] を選択すると、登録したデバイスの名前が表示されていることが確認できます。



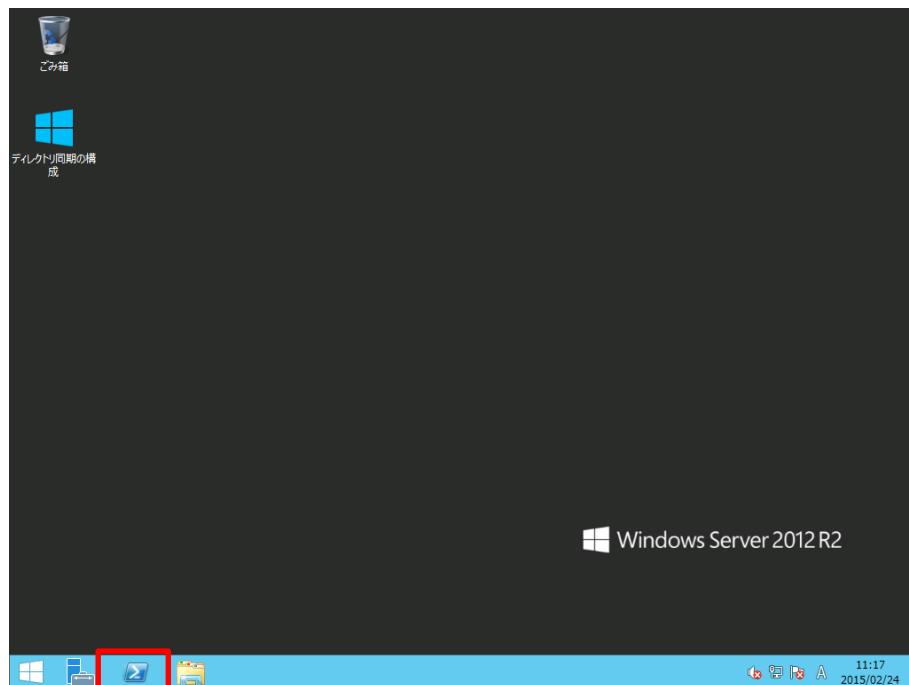
【Note:】

この画面により、ユーザーが所有するデバイスを確認できます。

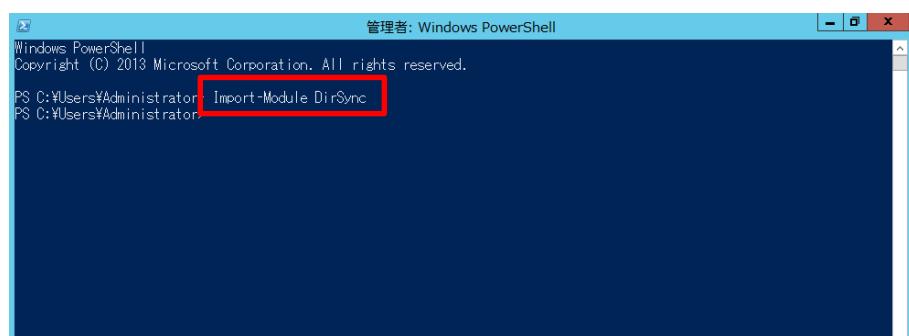
5. WS2012-DC0 1 コンピューターで操作します。

Azure AD に登録されたデバイスの情報は Active Directory ドメイン コントローラーにディレクトリ同期を実行することによって登録されます。既定では、ディレクトリ同期は 3 時間に一度実行されますが、ここでは今すぐ同期が実行されるように構成し、登録されたデバイスを確認します。

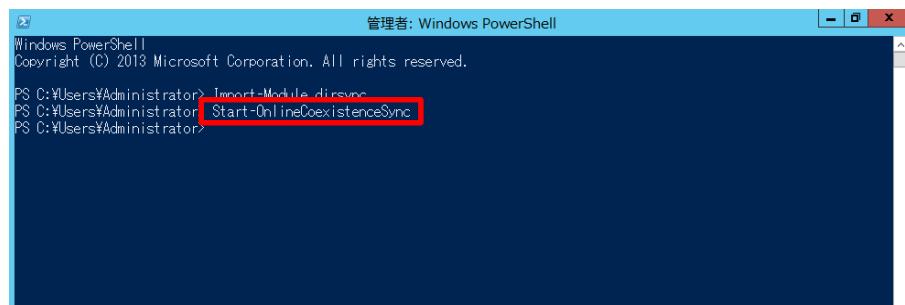
WS2012-DC01 コンピューターのデスクトップ画面で、Windows PowerShell アイコンをクリックします。



6. [管理者:Windows PowerShell] 画面で、「Import-Module DirSync」と入力し、Enter キーを押します。



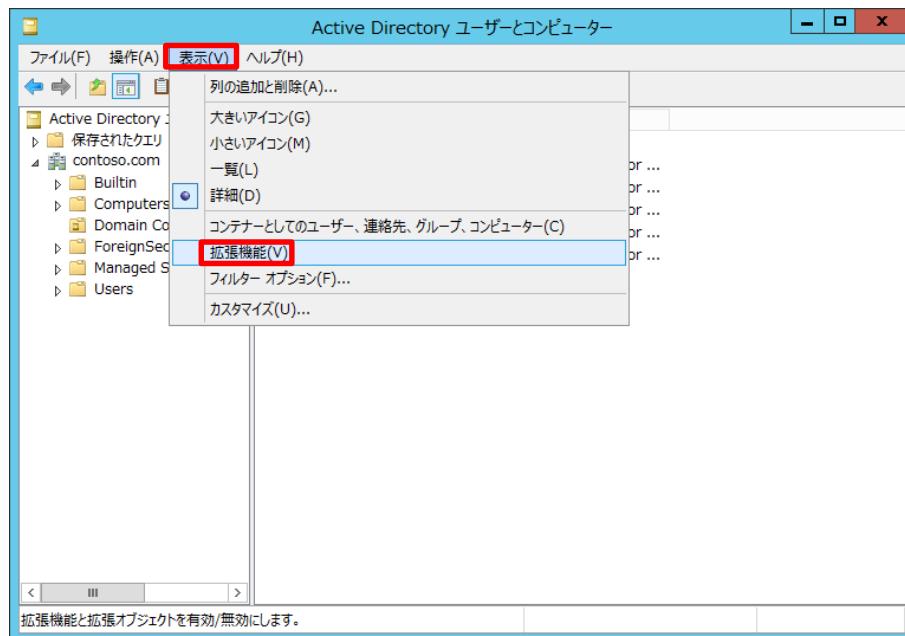
7. [管理者:Windows PowerShell] 画面で、「Start-OnlineCoexistenceSync」と入力し、Enter キーを押します。これにより、ディレクトリ同期が今すぐ実行します。



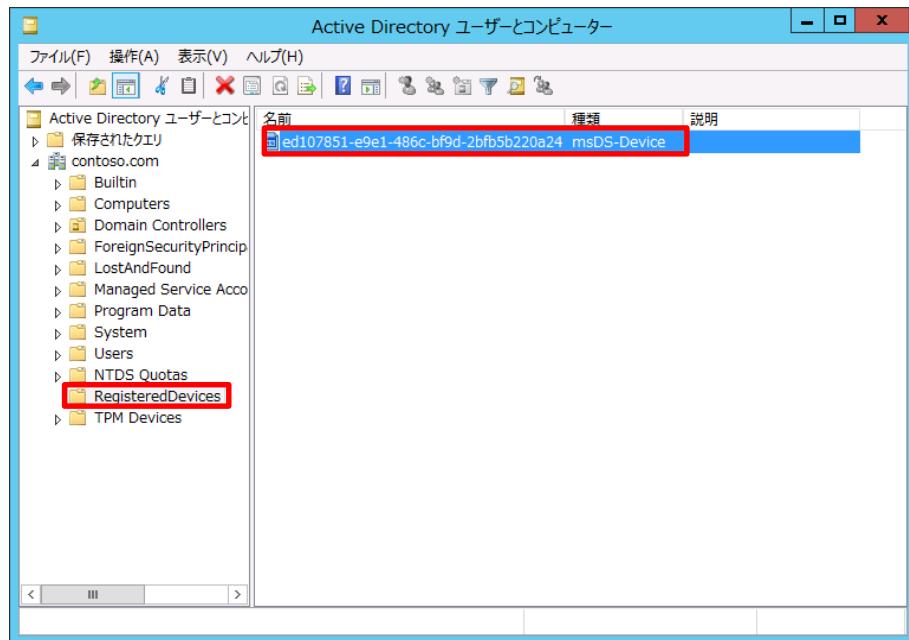
```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\$Users\$Administrator> Import-Module DirSync
PS C:\$Users\$Administrator> Start-OnlineCoexistenceSync
PS C:\$Users\$Administrator>
```

8. [Active Directory ユーザーとコンピューター] 画面を開き、[表示] - [拡張機能] をクリックします。



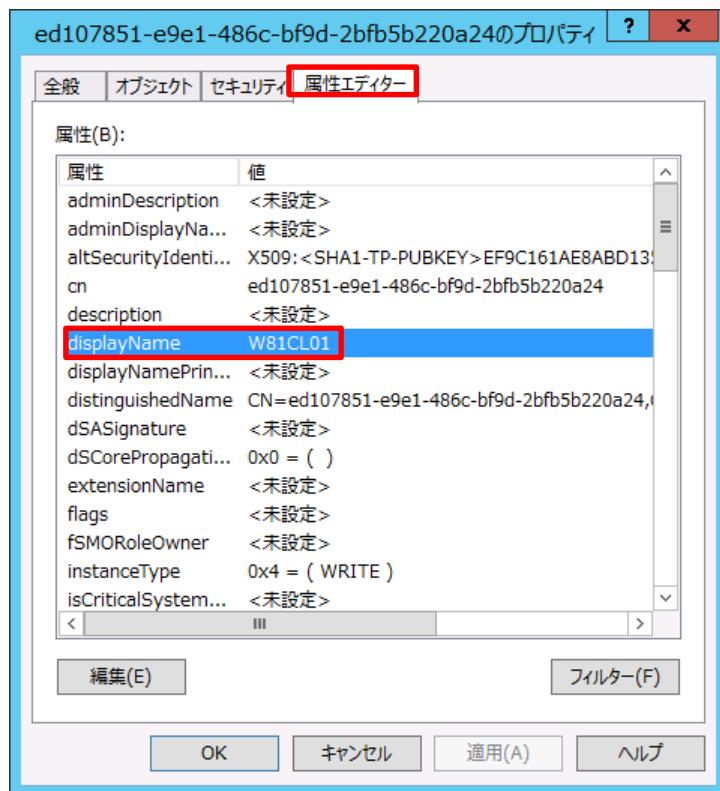
9. [Active Directory ユーザーとコンピューター] 画面で、[RegisteredDevices] コンテナーをクリックし、デバイス オブジェクトが作成されていることを確認します。確認したら、デバイス オブジェクトをダブルクリックします。



【Note:】

デバイス登録後、ディレクトリ同期を実行することにより、[RegisteredDevices] コンテナーにオブジェクトが登録されます。

10. デバイス オブジェクトのプロパティ画面で、[属性エディター] タブをクリックすると、登録したデバイスの名前などが確認できます。



【Note:】

AD FS サーバーによるデバイス認証を行う場合、Active Directory に登録されたデバイス オブジェクトの有無により、デバイスによるアクセス許可の判定を行います。

まとめ

この自習書では、Microsoft Azure Active Directory を利用してクラウド上に認証と認可を行うための基盤を構築する手順について学習しました。

クラウド/オンプレミスを問わず、様々なアプリケーションやサービスに安全かつ便利にアクセスできる環境を構築する上で Azure AD は欠かせないテクノロジーです。そして、これまで組織で実践してきたセキュリティポリシーや IT 統制（ガバナンス）に基づく運用を行う上で、Azure AD Premium は重要な役割を果たすことを確認しました。

本書が Microsoft Azure Active Directory ならびに Enterprise Mobility Suite の検証、環境構築を行う際の参考になれば幸いです。