



Microsoft Azure

Microsoft Azure 自習書シリーズ No.6

企業内システムと Microsoft Azure の VPN 接続、
ADFS、Office365 との連携

Published: 2014 年 5 月 30 日

Updated: 2015 年 1 月 31 日

Cloudlive, Inc.



Microsoft Azure 自習書シリーズ No.6
企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

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隨時更新されるため、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。

© Copyright 2014 Microsoft Corporation. All rights reserved.

本ドキュメントの更新について

バージョン	更新日	内容
v1.00	2014/6/30	・初版リリース
v1.10	2014/9/30	・2014年9月現在の情報に更新
v1.20	2015/1/31	・2015年1月現在の情報に更新

目次

STEP 1. Azure 仮想マシンを使用した Office 365 SSO の展開と 本書の目的について	7
1.1 Azure 仮想マシンを使用した Office 365 SSO の展開	8
1.2 シナリオ	13
1.3 ゴール	14
1.4 用語の説明	15
STEP 2. 実習の前提について	16
2.1 前提条件	17
2.2 今回構築するシステム構成	18
2.3 仮想マシンの冗長性・可用性とサイズ	20
2.4 各サーバーの役割／構成／前提条件	22
STEP 3. 認証フロー	29
3.1 Web ブラウザーからのアクセス (社内)	30
3.2 Web ブラウザーからのアクセス (社外)	31
3.3 その他のアクセス (Exchange Online)	32
3.4 フェデレーション ID 利用時のアクセス	33
STEP 4. 全体の構築手順	34
4.1 全体の構築手順	35
STEP 5. Office 365 ヘドメインの追加、およびドメインの確認	38
5.1 ドメインの追加	39
5.2 ドメイン登録情報の変更	42
5.3 ドメインの所在確認	43
5.4 ドメインの目的を設定	46
STEP 6. VPN 接続の設定	50
6.1 仮想ネットワークの作成	51
6.2 仮想ゲートウェイの作成	57
6.3 社内ネットワークの構成	61
STEP 7. ストレージ アカウントの作成	62
7.1 ストレージ アカウントの設定	63
STEP 8. 仮想マシンの作成	66
8.1 仮想ネットワークへの DNS サーバーの設定	67
8.2 仮想マシンの作成	72
8.3 仮想マシンへのリモートデスクトップ接続	77
8.4 日本語化	80

8.5 タイムゾーン	90
8.6 Windows Update の設定	92
8.7 ディスクの追加	95
8.8 ドメインへの参加	105
 STEP 9. AD DS サーバーのセットアップ、および動作確認	110
9.1 AD DS のインストール	111
9.2 ドメイン コントローラーへの昇格	119
9.3 サイトとサブネットの作成	128
9.4 初期レプリケートの完了	139
9.5 仮想ネットワークへの DNS サーバーの追加設定	141
9.6 NTP に関する注意点 (PDC エミュレーターとは同期しない)	147
9.7 2 台目以降の AD DS を構築する際のポイント	148
 STEP 10. ディレクトリ同期サーバーの セットアップ、および同期の確認	151
10.1 UPN サフィックスの追加	152
10.2 AD ユーザーの登録情報を確認	154
10.3 ディレクトリ同期の有効化	156
10.4 ディレクトリ同期ツール関連のインストール	159
10.5 ディレクトリ同期ツールのセットアップ (同期の実行)	171
10.6 ディレクトリ同期の確認	176
10.7 同期したユーザーのアクティビ化	180
 STEP 11. AD FS サーバーのセットアップ、およびフェデレーションの確認	184
11.1 AD FS 2.1 関連をインストール	185
11.2 サーバー証明書をインポートと設定	196
11.3 社内 DNS の設定	206
11.4 AD フェデレーション 用 サービス アカウントの作成	207
11.5 フェデレーション サーバーの設定	210
11.6 2 台目以降のフェデレーション サーバーの設定	216
11.7 IT プロフェッショナル 用 Microsoft Online Services サインイン アシスタントのインストール	221
11.8 Windows PowerShell 用 Windows Azure Active Directory モジュールのインストール	224
11.9 フェデレーション ドメインの有効化	229
11.10 ローカル イントラネット ゾーンへのサイトの登録	232
11.11 フェデレーション環境の動作確認	235
 STEP 12. AD FS Proxy サーバーの セットアップ、および動作確認	240
12.1 AD FS 2.1 関連をインストール	241
12.2 サーバー証明書をインポートと設定	251
12.3 エンドポイント HTTPS を作成	259
12.4 社外 DNS の設定	267
12.5 フェデレーション サーバー プロキシの設定	269
12.6 AD FS Proxy サーバーの動作確認	273

STEP 13. ファイアウォールの設定.....	277
13.1 ファイアウォールの設定.....	278
STEP 14. マルチドメインの設定	279
14.1 マルチドメインの設定	280
STEP 15. アクセス制御.....	285
15.1 要求記述の登録	286
15.2 要求規則の登録	289
15.3 規則のセット	294
STEP 16. 認証ログ.....	299
16.1 認証失敗ログ (AD FS によって制御されたログ)	300
16.2 認証成功ログ (AD FS によって認証されたログ)	303
16.3 AD FS トレース ログの設定.....	306
STEP 17. Appendix	312
17.1 SSO と仮想マシンを使用した AD DS または AD FS と Office 365 の展開	313
17.2 社内 VPN に関する要件	315
17.3 IP アドレス指定と名前解決	316
17.4 ディレクトリ同期するオブジェクトの要件.....	317
17.5 対応しているルート証明機関	318

STEP 1. Azure 仮想マシンを使用した Office 365 SSO の展開と 本書の目的について

この STEP では、Azure 仮想マシンを使用した Office 365 SSO の展開と本書の目的について説明します。

この STEP では、次のことを学習します。

- ✓ Azure 仮想マシンを使用した Office 365 SSO の展開
- ✓ シナリオ
- ✓ ゴール
- ✓ 用語の説明

1.1 Azure 仮想マシンを使用した Office 365 SSO の展開

◆ Office 365 の SSO のメリット

シングル サインオン (以下、SSO) をセットアップして有効にすると、組織のユーザーは会社の資格情報を使って Office 365 サービスにアクセスできるようになります。これにより、複数のログオン ID およびパスワードを管理する負担が軽減されます。SSO を使わない場合は、Office 365 ユーザーはユーザー名およびパスワードを個別に管理する必要があります。

エンド ユーザーのエクスペリエンスを向上させるために、スマート リンクを作成して展開することができます。スマート リンクを使うと、認証に必要なリダイレクト数を減らして、ユーザーのサインイン要求を高速に処理できます。 詳細については、「Office 365 でのスマート リンクまたは IdP 認証の使用 (<http://community.office365.com/en-us/w/sso/using-smart-links-or-idp-initiated-authentication-with-office-365.aspx?Sort=MostRecent&PageIndex=1>)」を参照してください。

ユーザーにとってのメリットだけでなく、管理者と組織にとっても非常に大きなメリットになります。たとえば、SSO を構成することで、社内ディレクトリと Office 365 ディレクトリの両方に組織のパスワード ポリシーとアカウントの制限を適用できます。

Office 365 では Active Directory フェデレーション サービス (以下、AD FS) を使って SSO を実現します。Office 365 サービスに SSO でアクセスできるように AD FS を計画、展開、および構成する方法の詳細については、「ディレクトリ同期を準備する (<http://technet.microsoft.com/ja-jp/library/jj151831.aspx>)」を参照してください。

この環境を構築するに当たり、Azure 仮想マシンを使うことで、社内インフラストラクチャ要件を最小限に抑えることができます。これらの仮想マシンを使って、Office 365 のディレクトリ同期と SSO を実装できます。

◆ 仮想マシン内で Office 365 インフラストラクチャ コンポーネントを実行するメリット

多くの場合、Office 365 を採用する企業のお客様の要望は、社内のインフラストラクチャ要件を最小化することです。

仮想マシンを導入すれば、AD フェデレーションが必要なお客様は、Microsoft がサポートする別の選択肢を利用してこれらのサービスをホストすることができます。

Azure でインフラストラクチャ コンポーネントを実行することには、次のようなメリットがあります。

クラウド戦略	クラウド戦略にいっそう良く適合しており、社内ハードウェアへの投資が削減されます。
ハードウェアとソフトウェアのコストが削減される可能性	Office 365 の展開をサポートするインフラストラクチャ サービスに関して、資本支出から運用支出への転換が広がる可能性もあります。追加のサーバーを購入して、それらをデータ センターで、または、リモートの場所から稼働させる必要がありません。
迅速な展開	インフラストラクチャ コンポーネントは比較的短期間で展開できるため、追加の社内ハードウェア リソースがほとんど、あるいはまったく必要ありません。
ビジネス継続性の向上	フェデレーション ユーザーは、社内環境が一時的に利用できなくなつても、引き続き、Office 365 にサインインすることができます。
オンデマンド拡張性	将来、ディレクトリ統合に対して拡張や変更が必要になつても、Azure なら柔軟な対応ができる、社内投資を増やすことなく、それらの変更を迅速に実現できます。
サイト回復性と災害復旧	考えられるシナリオには、Azure がインフラストラクチャに不可欠な冗長サービスをホストしている場合の災害復旧が含まれます。これにより、社内で障害が発生した場合のフェールオーバーが可能になります。
柔軟性	コンポーネントの再配置、負荷分散、複数の地理的領域に渡る分散が可能です。これにより、企業ネットワークに対する依存度が低減されます。

Office 365 と既存の社内プラットフォームを統合する場合は、それらを社内に実装するのか、Azure で実装するのかに關係なく、慎重な計画が必要です。クラウド内のこれらのインフラストラクチャ コンポーネントの実装と管理の計画は、社内のインフラストラクチャとほとんど同じです。

◆ SSO と仮想マシンを使用した Office 365 の概要

これまで、ディレクトリ同期と SSO を使用して Office 365 展開と既存のサービスを統合するために社内ハードウェアの投資が必要でした。このレベルの統合を含む展開には多くの時間とコストがかかります。

SSO のために、Office 365 には以下のコア コンポーネントが必要です。

- Active Directory ドメイン サービス (以下、AD DS)
- Active Directory フェデレーション サービス (AD FS)
- ディレクトリ同期サービス

これらのコア コンポーネントを総称して、「Office 365 ディレクトリ統合コンポーネント」と呼びます。これらのコンポーネントの詳細については、「シングル サインオンを準備する (<http://technet.microsoft.com/ja-jp/library/jj151786.aspx>)」を参照してください。

仮想マシンのリリースから、これらのコンポーネントの一部または全部をクラウドに展開するオプションが追加されました。この自習書は、Office 365 で SSO をサポートするために必要な Office 365 インフラストラクチャ コンポーネントの構築について説明しています。

なお、以下はこの自習書の範囲に含まれません。

Exchange ハイブリッド モードをサポートする Exchange Server の役割	Exchange ハイブリッド モードをサポートするために使用される Exchange Server の役割は 仮想コンピューター 上でサポートされません。これらの役割は意図的に除外されました。
仮想マシン上で Exchange サービスのホスティング	仮想マシン上の実稼働 Exchange サーバーの展開はサポートされません。
Shibboleth またはその他のサード パーティ SSO の実装	Azure AD と Office 365 は、AD FS、Shibboleth ID プロバイダー (*1)、その他のサード パーティ プロバイダー (*2) を含む、いくつかのセキュリティ トークン サービスをサポートします。仮想マシン上の Shibboleth またはその他のサード パーティ プロバイダーの展開が実現可能な場合もありますが、Microsoft ではこれらのプロバイダーをテストしていません。
要素認証または強力な認証	AD FS は多要素認証シナリオを可能にするように構成できます。実現可能な場合もありますが、サード パーティ ベンダーを通してサポート可能性を検証する必要があります。
マルチフォレスト トポロジ	ディレクトリ同期ツール はシングルフォレスト トポロジしかサポートしません。
複数の Azure データ センターにまたがる展開	Azure 障害ドメインの单一セットを越えたサービス展開ができます。これにより、複数の地理的地域にコンポーネントを展開できます。状況によっては、認証のパフォーマンスが改善されたり、ソリューション全体の可用性が向上したりします。Office 365 のほとんどのお客様には、単一の Azure データ センターへのディレクトリ統合サービスの展開で十分です。

Microsoft Azure 自習書シリーズ No.6
企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

- (*1) : 「Shibboleth ID プロバイダーによるシングル サインオンを実装して管理する
(<http://technet.microsoft.com/ja-jp/library/jj205456.aspx>)」
- (*2) : 「サードパーティ ID プロバイダーを使用してシングル サインオンを実装する
(<http://technet.microsoft.com/ja-jp/library/jj679342.aspx>)」

➔ SSO と Azure を使用した Office 365 の展開シナリオ

仮想マシン上にすべての Office 365 SSO 統合コンポーネントを展開すると、社内展開に勝るメリットを享受できます。これらのメリットには、迅速な導入、予測可能なコスト、社内サーバーの追加が不要であることなどが含まれます。あるいは、一部のコンポーネントを社内で展開しながら、フェデレーション コンポーネントのサブセットを Azure でホストすることができます。

他にも使用可能なオプションはありますが、最適な導入シナリオを 3 つ紹介します。

シナリオ①	すべての Office 365 SSO 統合コンポーネントを社内に展開する	これは、従来型のアプローチです。社内サーバーを使用して、ディレクトリ同期と AD FS を展開します。
シナリオ②	すべての Office 365 SSO 統合コンポーネントを Azure で展開する	これはクラウドのみを使用する新しいアプローチです。ディレクトリ同期と AD FS を Azure で展開します。この場合は、社内サーバーを展開する必要がありません。
シナリオ③	一部の Office 365 SSO 統合コンポーネントを災害復旧用として Azure で展開する	これは、社内展開コンポーネントとクラウド展開コンポーネントの組み合わせです。ディレクトリ同期と AD FS を主に社内に展開し、災害復旧用の冗長コンポーネントを Azure で追加します。

なお、この自習書では、上記の「シナリオ②」の構築手順を説明していきます。

1.2 シナリオ

この自習書では、すべての Office 365 SSO 統合コンポーネントを Azure で展開する環境を構築します。

◆ 仮想ネットワーク

サブネットを 1 つ作成

サイト間 VPN を構成

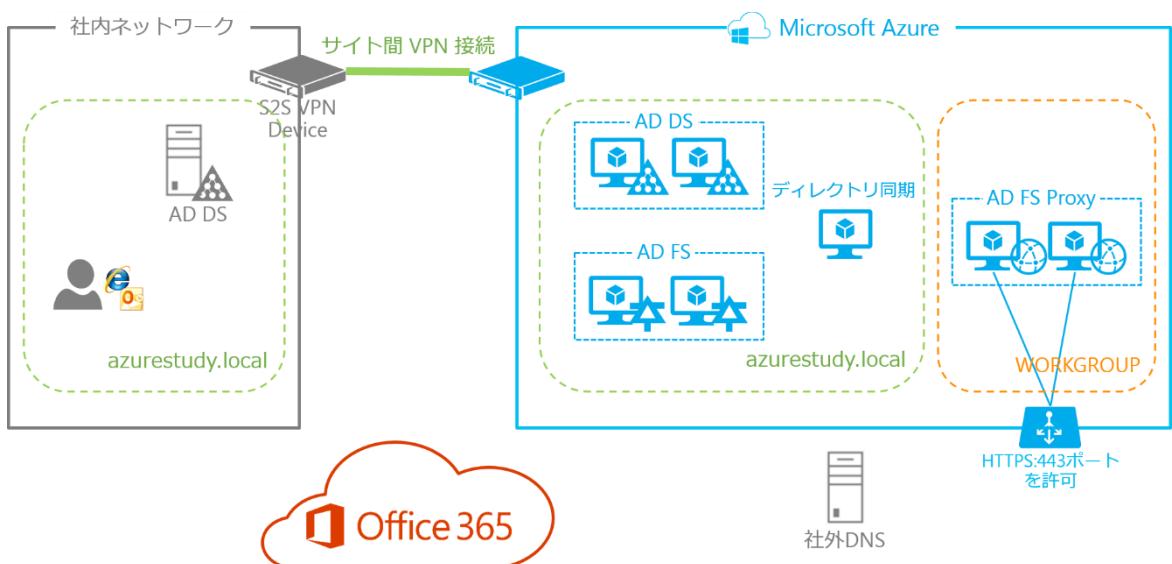
◆ 社内ネットワーク（オンプレミス）

ISP から払い出された固定グローバル IP アドレスを使用して接続

ISP の ONU と VPN デバイスを直接繋ぐ（FW などを間に挟まない）

オンプレミス内の既存セグメント 1 つを Azure 仮想ネットワークと VPN で接続

◆ システム構成図



1.3 ゴール

「1.2 シナリオ」の環境を構築し、以下ができたことをもってゴールとします。

- ・ 社内の AD 環境（この自習書では「azurestudy.local」ドメイン）にあるディレクトリ オブジェクト（ユーザー、グループ、および連絡先）が Office 365 に同期していること
- ・ 社内の AD 環境内にあるクライアント PC からブラウザー（Internet Explorer）で「Office 365 ポータル (<https://portal.office.com/Home>)」にアクセスし、SSO によって適切なユーザーでサインインできること
- ・ 社内の AD 環境外にあるクライアント PC からブラウザー（Internet Explorer）で「Office 365 ポータル」にアクセスし、適切なユーザーでサインインできること

1.4 用語の説明

この自習書で使用する用語については以下のとおりとなります。

用語	説明	補足
AD	Active Directory	
AD DS	Active Directory ドメイン サービス	
AD FS	Active Directory フェデレーション サービス	
CA	認証機関／認証局	
CN	Common Name (一般名)	SSL 接続するサイトの URL (FQDN) のこと
CSR	Certificate Signing Request	
EAC	Exchange 管理センター	Office 365 管理センターでは管理できない電子メールに関連するアイテムを管理する Web ベースの管理コンソール ※ Exchange コントロールパネル (ECP) に代わるもの
EOP	Exchange Online Protection	クラウドベースの電子メールフィルタリングサービス
EWS	Exchange Web Services	Exchange サーバーと通信するクライアント アプリケーションを有効にする機能。多くの Microsoft Office Outlook を通じて利用可能にする同じデータへのアクセスを提供する
FQDN	Fully Qualified Domain Name	完全修飾ドメイン名
IPsec	インターネット プロトコル セキュリティ	
MFG	Microsoft Federation Gateway	Microsoft が提供するクラウドベースの ID 認証サービス
ISP	Internet Services Provider	インターネット接続業者
NLB	ネットワーク負荷分散	
NTP	Network Time Protocol	
OWA	Outlook Web App	
SLA	Azure のサービス稼働保証。可用性に対する保証	
WID	Windows Internal Database	Windows 内部データベース (リレーショナル データストア) ※ 今回は、AD FS の構成を格納するデータベースとして使用

- (*1) : 「 Microsoft Azure のサポート サービス レベル アグリーメント (<http://azure.microsoft.com/ja-jp/support/legal/sla/>)」

STEP 2. 実習の前提について

この STEP では、この自習書で実習を行うために必要な前提について説明します。

この STEP では、次のことを学習します。

- ✓ 前提条件
- ✓ 今回構築するシステム構成
- ✓ 仮想マシンの冗長性・可用性とサイズ
- ✓ 各サーバーの役割／構成／前提条件

2.1 前提条件

- Azure 管理ポータルへサインインできるアカウントを持っていることを前提としています。
- VPN 接続用のインターネット回線があることを前提としています。 加えて、固定グローバル IP アドレスが必要となります。
- 仮想ネットワークとオンプレミスを VPN 接続するには、オンプレミス側に VPN デバイスを設置する必要があります。
- Azure 管理ポータルへのサインインの手順は省略しています。
- Office 365 Enterprise の契約が完了した状態を前提としています。 また、Office 365 上に管理者アカウント（全体管理者）が登録していることを前提とします。
- 既にオンプレミス環境に Active Directory ドメイン サービスが存在していることを前提とします。
- マルチフォレスト環境構成については、この自習書の対象外とさせていただきます。
- この自習書では、AD FS 環境を利用するに当たって必要なネットワーク設計、および設定（主に、オンプレミス側）については省略しています。 必要に応じて以下の設計を行ってください。
 - ✓ Office 365 向けファイアウォール
 - ✓ （必要に応じて）WAN アクセレーター
 - ✓ （必要に応じて）インターネットの帯域幅

2.2 今回構築するシステム構成

この項では、仮想ネットワーク上に、AD DS サーバー、ディレクトリ同期サーバー、AD FS サーバー、AD FS Proxy サーバーを導入するための各種情報を示します。

◆ システム構成図

「1.2 シナリオ」にあるシステム構成図をご覧ください。

◆ 仮想ネットワーク（サイト間 VPN）

仮想ネットワーク名	tokyo-nw			
アフィニティグループ	tokyo-ag			
DNS サーバー	AZSTADDS01	10.1.1.4	OPSTADDS01	192.168.118.160
	AZSTADDS02	10.1.1.5		
IP アドレス範囲	10.1.0.0/16			
サブネット	ゲートウェイ	10.1.0.0/29	tokyo-subnet1	10.1.1.0/24

◆ 仮想マシン

サイト	on-premise	on-azure		
サーバーの役割	AD DS	AD DS		ディレクトリ同期
マシン名	OPSTADDS01	AZSTADDS01	AZSTADDS02	AZSTDIRSYNC01
インスタンス	N/A	標準	標準	標準
サイズ	N/A	A1 (S)	A1 (S)	A2 (M)
クラウド サービス DNS 名 (*1)	N/A	AZSTADDS		AZSTDIRSYNC
可用性セット名	N/A	AZSTADDS-AS		(なし)
内部 IP アドレス	192.168.118.160	10.1.1.4	10.1.1.5	10.1.1.6
所属グループ	azurestudy.local			
ローカル管理者	ドメイン管理者と同 一	studyadmin / studyP@ss		
ドメイン管理者	administrator / studyP@ss			

サイト	on-azure			
サーバーの役割	AD FS		AD FS Proxy	
マシン名	AZSTADFS01	AZSTADFS02	AZSTPROXY01	AZSTPROXY02
インスタンス	標準	標準	標準	標準
サイズ	A1 (S)	A1 (S)	A1 (S)	A1 (S)
クラウド サービス DNS 名 (*1)	AZSTADFS			AZSTPROXY
可用性セット名	AZSTADFS-AS		AZSTPROXY-AS	
内部 IP アドレス	10.1.1.7	10.1.1.8	10.1.1.9	10.1.1.10
所属グループ	azurestudy.local		WORKGROUP	
ローカル管理者	studyadmin / studyP@ss			
ドメイン管理者	administrator / studyP@ss		N/A	

企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

- (*1) : クラウド サービス DNS 名の完全名は、「<xxxxx>.cloudapp.net」です。上の表の値は <xxxxx> の部分を示しています。

◆ Office 365 管理者アカウントと追加するドメイン

Office 365 管理者アカウント（全体管理者）は、これから構築する AD FS 環境に障害が発生して SSO できない場合でも Office 365 にアクセスできるようにするために、通常認証でサインインできるアカウント「<administrator user>@<tenant>.onmicrosoft.com」を用意してください。

また、この自習書では Office 365 に追加するドメインを「azurestudy.jp」として説明します。

◆ URL

この自習書で登場する以下のサイトの URL を紹介します。

- 「Office 365 管理センター (<https://portal.office.com/admin/default.aspx>)」
- 「Azure 管理ポータル (<https://manage.windowsazure.com>)」

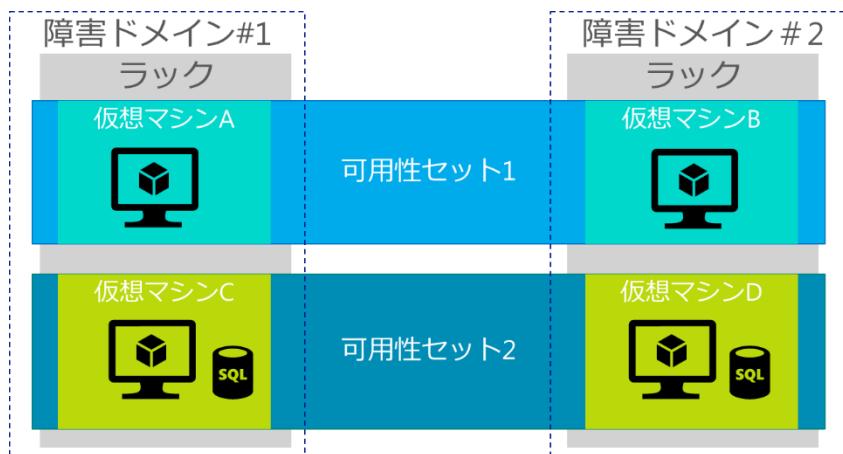
2.3 仮想マシンの冗長性・可用性とサイズ

◆ 仮想マシンの冗長化・可用性

仮想マシンの可用性を向上させるために、ほとんどのサーバーで 2 台以上の仮想マシンを用意します。複数の仮想マシンを使用すれば、ローカル ネットワークの障害、ローカル ディスク ハードウェアの故障、Azure のデータ センターに必要な予定ダウンタイムが発生してもサービスを利用し続けることができます。

複数の仮想マシンが 1 つのクラウド サービスで接続されている場合は、可用性セットを使用して、仮想マシンを確実に別々の障害ドメインに配置する必要があります。これは、2 つの冗長サーバーを社内のデータ センター内の物理的に異なるサーバー ラックに配置するのに似ています。

下の図は 2 つの可用性セットを表しており、各セットにはそれぞれ 2 つの仮想マシンがあります。



◆ 仮想マシンのサイズ

また、Office 365 で必要な仮想マシンのサイズは、組織内のユーザー数で決まります。下の表に、Office 365 ディレクトリ統合コンポーネントに関する仮想マシンのサイズとインスタンス数のガイドラインを示します。

サーバーの役割	AD DS (*1)	ディレクトリ同期 (*1) (*2)	AD FS	AD FS Proxy
インスタンス	基本または標準	基本または標準	基本または標準	標準 (*5)
5,000 ユーザー未満	A1 (S) × 2 台	A2 (M) × 1 台	A1 (S) × 2 台	A1 (S) × 2 台
5,001 ~ 15,000 ユーザー	A2 (M) × 2 台	A2 (M) × 1 台	A1 (S) × 2 台	A1 (S) × 2 台
15,001 ~ 50,000 ユーザー	A3 (L) × 2 台	A2 (M) × 1 台	A2 (M) × 2 台以上 (*4)	A2 (M) × 2 台以上 (*6)
50,001 ユーザー以上	A3 (L) × 2 台	A3 (L) × 1 台 (*3)	A3 (L) × 2 台以上 (*4)	A3 (L) × 2 台以上 (*4)

- (*1) : 各仮想マシンに、さらに 1 つのデータ ディスクを追加します。
- (*2) : 標準で冗長構成が組めない (サポートされていない) ため、シングル構成となります。

企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

- (*3) : さらに 1 つの SQL Server データベース用のデータ ディスクと、1 つの SQL Server ログ用のデータ ディスクを追加します。
- (*4) : 組織内のユーザー数が 15,000 を超過する場合は AD FS サーバーを 2 台以上用意します。
- (*5) : AD FS Proxy サーバーは、エンドポイント (HTTPS : 443 ポート) の負荷分散を設定する必要があるため、標準インスタンスで仮想マシンを作成します。
- (*6) : 組織内のユーザー数が 15,000 を超過する場合は AD FS Proxy サーバーを最低 2 台用意します。

展開計画の一部として、これらのガイドラインを最新の製品マニュアルや独自の要件と比較して、仮想マシンのサイズ選択が適切なことを確認する必要があります。以下のリソースは、容量計画を支援するために提供されています。

- 各 サ イ ズ の 仮 想 マ シ ン に 附 属 の リ ソ ー ス : 「仮想マシン (<http://msdn.microsoft.com/library/azure/jj156003.aspx>)」
- 仮想マシンの使用可能なサイズとオプション:「Azure の仮想マシンおよびクラウド サービスのサイズ (<http://msdn.microsoft.com/library/azure/dn197896.aspx>)」
- ディレクトリ同期:「ディレクトリ同期を準備する (<http://technet.microsoft.com/ja-jp/library/jj151831.aspx>)」
- AD FS:
 - ✓ 「フェデレーション サーバーの容量計画 (<http://technet.microsoft.com/ja-jp/library/gg749899.aspx>)」
 - ✓ 「AD FS 2.0 容量計画スプレッドシート (<http://www.microsoft.com/en-us/download/details.aspx?id=2278>)」
- SQL Server:「SQL Server 2012 のインストールに必要なハードウェアおよびソフトウェア ([http://technet.microsoft.com/ja-jp/library/ms143506\(v=sql.110\).aspx](http://technet.microsoft.com/ja-jp/library/ms143506(v=sql.110).aspx))」

2.4 各サーバーの役割／構成／前提条件

この項では、環境構築に必要な構成、および前提条件を記載します。

◆ 各サーバーの役割とシステム要件

この自習書では Windows Server 2012 を対象としています。

サーバー	役割	システム要件	
		OS	ソフトウェア、その他要件
AD DS	<ul style="list-style-type: none"> ユーザーの認証 AD FS サーバーへのユーザー情報の提供 	Windows Server 2012	<ul style="list-style-type: none"> ドメイン・フォレスト機能レベル 2003 以上 混合モード or ネイティブモードの機能レベル 読み取り/書き込みドメイン コントローラー (*1)
ディレクトリ同期	<ul style="list-style-type: none"> AD 上のオブジェクト（ユーザー、グループ、連絡先）を Office 365 上に片方向の同期・定期自動更新 	Windows Server 2012 ※ドメイン参加が必要	<ul style="list-style-type: none"> Windows PowerShell 3.0 .NET Framework 3.5/4.5 機能 ディレクトリ同期ツール SQL Server 2012 Express SP1 (*2) Forefront Identity Manager 2010 R2 (*2)
AD FS	<ul style="list-style-type: none"> Office 365 と信頼関係を結ぶためのトークンを生成し暗号化を行う Active Directory への認証を行う 	Windows Server 2012 ※ドメイン参加が必要	<ul style="list-style-type: none"> Windows PowerShell 3.0 AD FS 2.1 (フェデレーション サービス) Web サーバー (IIS 8.0) IT プロフェッショナル用 Microsoft Online Services サインイン アシスタント Windows PowerShell 用 Windows Azure Active Directory モジュール SSL 証明書 (*3)
AD FS Proxy	<ul style="list-style-type: none"> 社外からの Office 365 へ接続するために、AD FS サーバーに対して Office 365 と信頼関係を結ぶためのトークンを代理で発行依頼を行う AD FS サーバーから受け取ったトークンをクライアントへ受け渡す AD FS サーバーと連携して代理認証を行う 	Windows Server 2012 ※ドメイン参加は不要	<ul style="list-style-type: none"> AD FS 2.1 (フェデレーション サービス プロキシ) Web サーバー (IIS 8.0) SSL 証明書 (*3)

- (*1): 各サーバーから AD DS への常時アクセスを確保するために、仮想ネットワーク上にもドメイン コントローラーのレプリカを設置します。なお、読み取り専用ドメイン コントローラーをディレクトリ同期で使用することはサポートされていません。

企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

- (*2) : ディレクトリ同期ツールをインストールすると、自動でインストールされます。
- (*3) : SSL 証明書は自己署名入り証明書ではなく、外部証明機関 (Microsoft によって信頼されている CA) から正規に発行された証明書を利用しなければなりません。 (「17.5 対応しているルート証明機関」を参照。)

また、ドメイン名「<xxxxx>.cloudapp.net (クラウド サービス DNS 名)」で SSL 証明書を取得することができません (「cloudapp.net」は Microsoft 管理の CN) ので、注意してください。

(「付録 D: Windows Azure での DNS の使用 (<http://msdn.microsoft.com/ja-jp/library/ff803360.aspx>)」を参照。)

➔ AD DS の構成／前提条件

仮想マシン上に AD FS を展開して、ドメイン コントローラーを社内に残すことができますが、この方法はお勧めできません。 ドメイン コントローラーを AD FS から分離することによって、認証チェーンに遅延が生じる可能性があります。 これによって、この 2 つのサービスにネットワーク接続へのリアルタイム依存関係が生じます。 Azure 内部の仮想マシンにドメイン コントローラーを配置することによって、このようなリスクが軽減されます。

Azure 内のドメイン コントローラーは、別の AD サイトに配置する必要があります。 これにより、AD レプリケーションの遅延が若干増加します。 AD サイト間の既定のレプリケーション遅延は 3 時間です。 ディレクトリ同期ツールを使用した場合の AD と Office 365 間の既定の同期スケジュールも 3 時間です。

したがって、レプリケーション遅延が調整されない場合は、Office 365 にレプリケートするために社内で行われる変更に最大で 6 時間かかる可能性があります。

仮想マシン上の AD サービスの実行に関する一般的ガイダンスについては、「Azure の仮想マシン での Windows Server Active Directory のデプロイ ガイドライン (<http://msdn.microsoft.com/library/azure/jj156090.aspx>)」を参照してください。

◆ ディレクトリ同期の構成／前提条件

ディレクトリ同期ツールを展開するには、以下の最小要件を満たせなければなりません。

- ・ ディレクトリ同期ツールは Office 365 と統合するフォレスト内のドメインに参加しているコンピューター上にインストールする必要があります。
- ・ このコンピューターをドメイン コントローラーにすることはできません。
- ・ ディレクトリ同期ツールを構成するには、エンタープライズ管理者の資格情報が必要です。

以下の表では、ディレクトリ同期の構成は Office 365 にレプリケートするオブジェクト数によって異なることを示します。

社内 AD のオブジェクト数 (*4)	ディレクトリ同期の構成
50,000 個以下の場合	Microsoft SQL Server 2012 Express SP1 でディレクトリ同期を展開できます。 ※ディレクトリ同期ツールの既定のインストールには、 Microsoft SQL Server 2012 Express SP1 のバージョンが含まれます。
50,001 個以上の場合	SQL Server の完全なインスタンスを使用してディレクトリ同期を展開する必要があります。 SQL Server の必須の完全なインスタンスは、 Microsoft SQL Server 2012 SP1 です。 (*5)

- ・ (*4) : ディレクトリ同期ツールでレプリケートするオブジェクトは、以下のオブジェクトとなります。 ここでいうオブジェクト数とは、以下のオブジェクトの合計数となります。
 - ✓ ユーザー
 - ✓ 配布リスト
 - ✓ セキュリティ グループ
 - ✓ 連絡先
- ・ (*5) : スタンドアロン バージョンの SQL Server が必要な場合は、それをディレクトリ同期ツールと同じ仮想マシン上に展開する必要があります (ディレクトリ同期ツールを導入する前にインストールしてください)。これが仮想マシンのサイズを左右する場合があります。スタンドアロン バージョンの SQL Server に同期を展開する方法の詳細については、以下の記事を参照してください。

「SQL Server へのディレクトリ同期ツールのインストール (<http://technet.microsoft.com/ja-jp/library/dn441161.aspx>)」

また、以下の構成はサポートされていません。

- ✓ ディレクトリ同期ツールとは別のサーバー上に SQL Server を展開する
- ✓ ディレクトリ同期ツール用のデータベースとしての Azure SQL データベースを使用する
- ・ Azure AD サービスは、最大 50,000 個のオブジェクトの同期をサポートしています。 50,000 個を超えるオブジェクトをレプリケートするには、クラウド サービス のサポートに問い合わせてください。

企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

- Office 365 では最初の独自ドメイン登録によって、オブジェクト数の上限が 300,000 に自動拡張されます。オブジェクト数が 300,000 を超えるお客様は引き続きテクニカルサポートにお問い合わせください。
- インストールとセットアップが完了すると、完全な同期が直ちに開始されます。初回の同期後は、3 時間ごとに同期が行われます。なお、この同期頻度は変更することはできません。

ディレクトリ同期ツールを仮想マシン上に展開する場合にサポートされる構成を下の表に示します。

ディレクトリ同期ホスト	ドメイン コントローラー	サポート
仮想マシン	仮想マシン: 読み取り/書き込みドメイン コントローラー	○
仮想マシン	仮想マシン: 読み取り専用ドメイン コントローラー	×
仮想マシン	社内 (仮想ネットワーク 経由で接続) ディレクトリ同期の遅延許容範囲は広く設定されていますが、Azure と社内間の接続が不安定になると問題が発生すると、Office 365 でディレクトリ同期の機能停止や、期限切れのデータが発生する可能性があります。	○ 非推奨

ディレクトリ同期をセットアップして構成するときには、サーバーをドメインあたり 1 つ以上のドメイン コントローラーに接続できなければなりません。

ディレクトリ同期の要件と展開に関する詳細については、「ディレクトリ同期を準備する (<http://technet.microsoft.com/ja-jp/library/jj151831.aspx>)」を参照してください。

仮想マシン上の SQL Server の展開に関するガイドについては、「Azure の仮想マシンにおける SQL Server の概要 (<http://msdn.microsoft.com/library/azure/dn133151.aspx>)」を参照してください。

ディレクトリ同期は OS ディスク (C ドライブ) にインストールするのではなく、別途データディスク (*6) を追加して、そのディスクにインストールします。このディスクに必要な容量は Office 365 にレプリケートするオブジェクト数によって異なります。以下の表は、最小の推奨要件を示します。

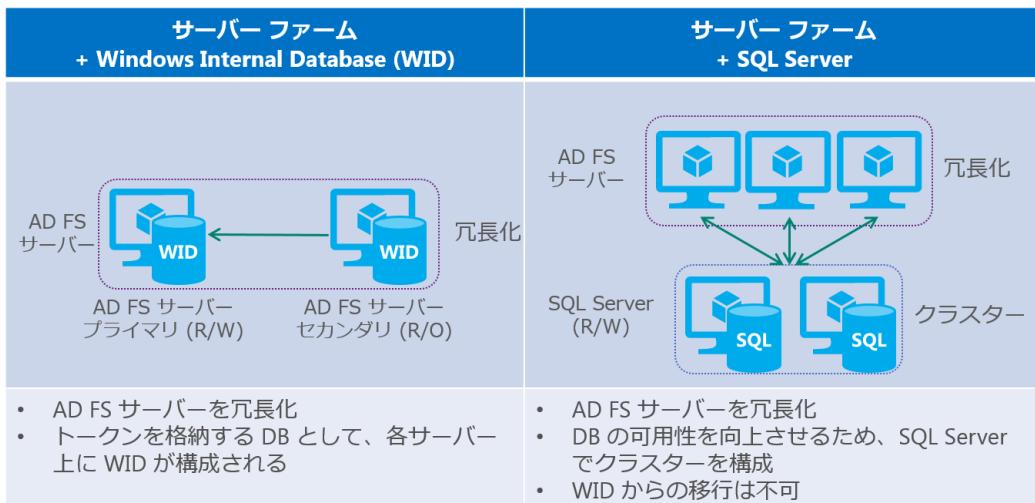
社内 AD のオブジェクト数 (*4)	データ ディスクの容量
10,000 個未満	70 GB
10,000 ~ 50,000 個	70 GB
50,001 ~ 100,000 個 (*7)	100 GB
100,001 ~ 300,000 個 (*7)	300 GB
300,001 ~ 600,000 個 (*7)	450 GB
600,001 個以上 (*7)	500 GB

- (*6): ディスクを追加する際に指定する [ホスト キャッシュ設定] は「なし」を指定します。
- (*7): SQL Server の完全なインスタンスを使用してディレクトリ同期を展開する必要があります。

なお、この自習書では、同梱されている SQL Server 2012 Express SP1 にて対応する手順を記載しています。

➔ AD FS, AD FS Proxy の構成／前提条件

AD FS サービスの最良の可用性を実現するために、AD FS サーバーと AD FS Proxy サーバーをそれぞれ 2 台以上で展開します。そのため、AD FS の構成は、サーバー ファームで構築します。



上の図では、AD FS 構成データベースとして、WID または SQL Server を用いた場合の AD FS の構成を示しています。AD FS 構成データベースとして WID を用いた場合は AD FS サーバー 5 台までをサポートします。AD FS サーバーが 6 台以上になる場合は、SQL Server (完全なインスタンス) に変更してください。（DB の可用性を向上させるため、クラスターを構成することを推奨）

仮想マシン上での SQL Server の展開に関するガイダンスについては、「Azure の仮想マシンにおける SQL Server の概要 (<http://msdn.microsoft.com/library/azure/dn133151.aspx>)」を参照してください。

ただし、AD FS サーバー構築後に構成データベースを WID から SQL Server に変更することができないため、その場合は AD FS サーバーを再構築する必要があります。

AD FS サーバーの冗長化は、Azure ではネットワーク負荷分散 (NLB) がサポートされていないため、社内 DNS サーバーのラウンドロビン機能によって実現します。

ただし、この機能で返される IP アドレスは、あくまでも DNS サーバーに登録されている情報であり、実際にその IP アドレスのサーバーがアクセスできるか否かは、DNS サーバーでは関知していません。

なお、この自習書では AD FS の構成データベースは同梱されている WID にて対応する手順を説明います。また、AD FS サーバーの冗長化は DNS のラウンドロビン機能を用いた手順を説明しています。

企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

以下の表では、組織内のユーザー数による AD FS、AD FS Proxy サーバーの構成を示します。

ユーザー数	推奨される構成
15,000 ユーザー 以下	<ul style="list-style-type: none"> 冗長化された専用 AD FS サーバー A1 (S) × 2 台を用意 <ul style="list-style-type: none"> ✓ AD FS 構成データベースは WID を利用 冗長化された専用 AD FS Proxy サーバー A1 (S) × 2 台を用意
15,001 ~ 50,000 ユーザー	<ul style="list-style-type: none"> 冗長化された専用 AD FS サーバー A2 (M) × 2 台以上を用意 <ul style="list-style-type: none"> ✓ AD FS 構成データベースは WID を利用 冗長化された専用 AD FS Proxy サーバー A2 (M) × 2 台を用意
50,001 ユーザー 以上	<ul style="list-style-type: none"> 冗長化された専用 AD FS サーバー A3 (L) × 2 台以上を用意 <ul style="list-style-type: none"> ✓ AD FS 構成データベースは WID を利用 冗長化された専用 AD FS Proxy サーバー A3 (L) × 2 台以上を用意

- 信頼できる証明機関から、ローカル AD ドメイン名前空間に対して発行された共通名を含む証明書を取得します。 この証明書によって、AD FS Proxy をセットアップできるようになります。
- AD は Windows Server 2003 以降で、混在モードまたはネイティブ モードの機能レベルで展開し実行します。
- クライアント PC (Windows 8.1 / 8 / 7 / Vista) にはオペレーティングシステムの最新の更新プログラムを実行してください。
- AD FS Proxy サーバーは、ユーザーが会社のネットワークの外部から接続している場合、または OWA 以外のメールクライアント (Outlook、POP/IMAP メーラーなど) から Exchange Online に接続する必要がある展開する必要があります。

STEP 3. 認証フロー

Web ブラウザーからのアクセスにて認証を行う際、アクセス元の環境（社内・社外）に応じて認証フローが異なります。

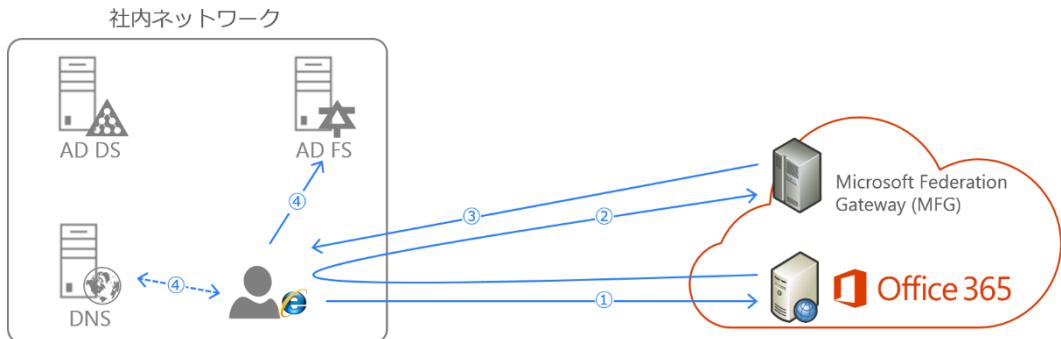
この STEP では、社内外で Web ブラウザーおよびメールクライアントからアクセスした時の認証フローについて説明します。

この STEP では、次のことを学習します。

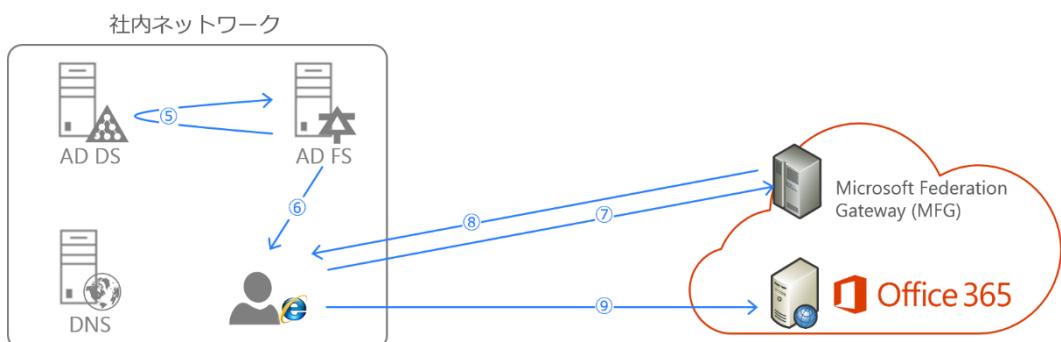
- ✓ Web ブラウザーからのアクセス（社内）
- ✓ Web ブラウザーからのアクセス（社外）
- ✓ その他のアクセス（Exchange Online）
- ✓ フェデレーション ID 利用時のアクセス

3.1 Web ブラウザからのアクセス（社内）

◆ Office 365 ポータル、Outlook Web App、SharePoint Online、Lync の場合



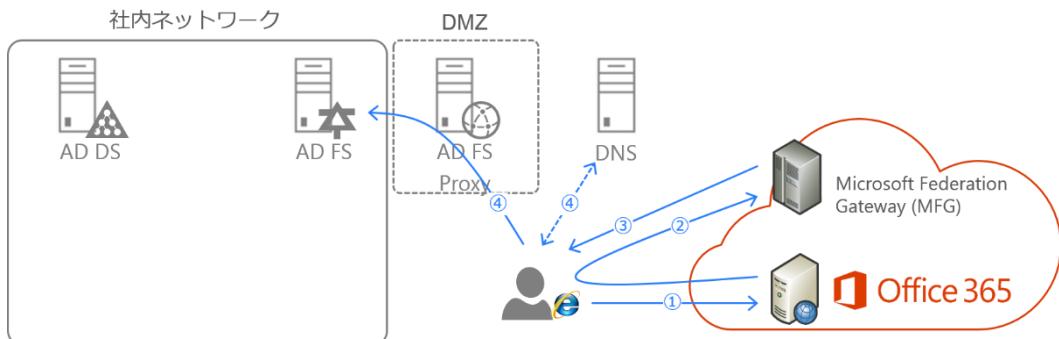
- ① ユーザーが Office 365 にアクセス
- ② 認証には MFG から発行されたサービス チケットが必要なため、ユーザーのアクセスを MFG にリダイレクト
- ③ サービス チケット発行には AD FS で署名されたログオン トークンが必要なため、AD FS の URL を送信
- ④ ユーザーは社内の DNS サーバーを参照し、AD FS に接続



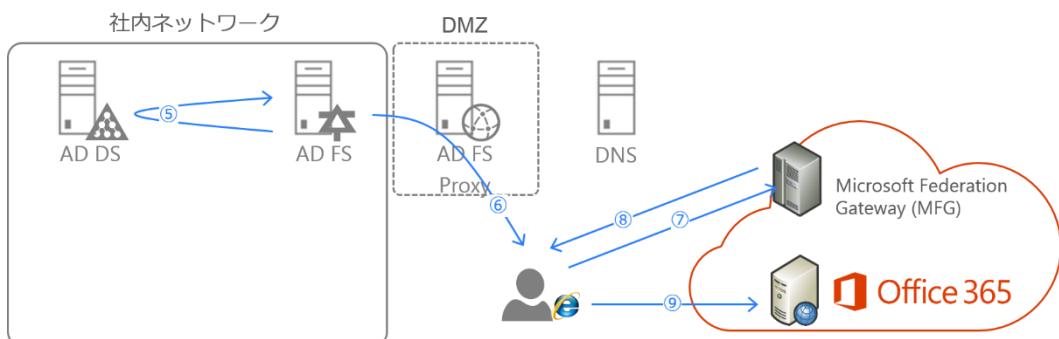
- ⑤ AD DS に接続し、ログオン トークン作成に必要なデータを収集
- ⑥ AD FS がログオン トークンを作成し、ユーザーに送信
- ⑦ ユーザーがログイン トークンを MFG に送信
- ⑧ 信頼している AD FS で署名されたログオン トークンであることを確認し、ユーザーにサービス チケットを返信
- ⑨ サービス チケットを Office 365 に送信し、認証が完了

3.2 Web ブラウザからのアクセス（社外）

◆ Office 365 ポータル、Outlook Web App、SharePoint Online、Lync の場合



- ① ユーザーが Office 365 にアクセス
- ② 認証には MFG から発行されたサービス チケットが必要なため、ユーザーのアクセスを MFG にリダイレクト
- ③ サービス チケット発行には AD FS で署名されたログオン トークンが必要なため、AD FS の URL を送信
- ④ ユーザーは社外の DNS サーバーを参照し、AD FS Proxy 経由で AD FS に接続



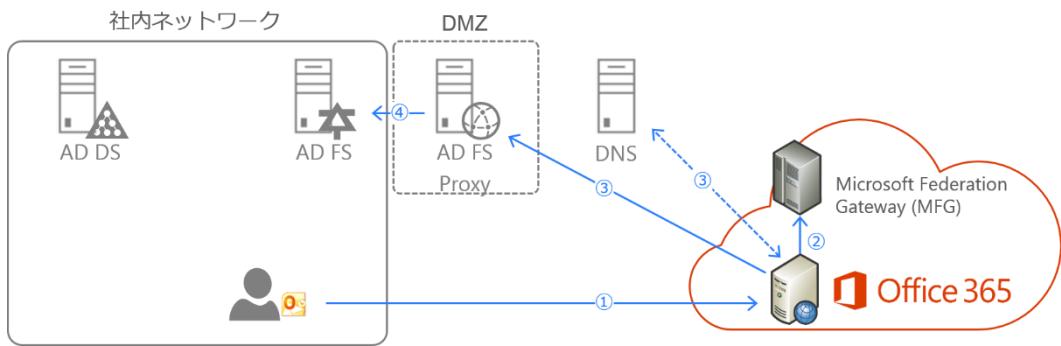
- ⑤ AD DS に接続し、ログオン トークン作成に必要なデータを収集
- ⑥ AD FS がログオン トークンを作成し、AD FS Proxy 経由でユーザーに送信
- ⑦ ユーザーがログイン トークンを MFG に送信
- ⑧ 信頼している AD FS で署名されたログオン トークンであることを確認し、ユーザーにサービス チケットを返信
- ⑨ サービス チケットを Office 365 に送信し、認証が完了

3.3 その他のアクセス (Exchange Online)

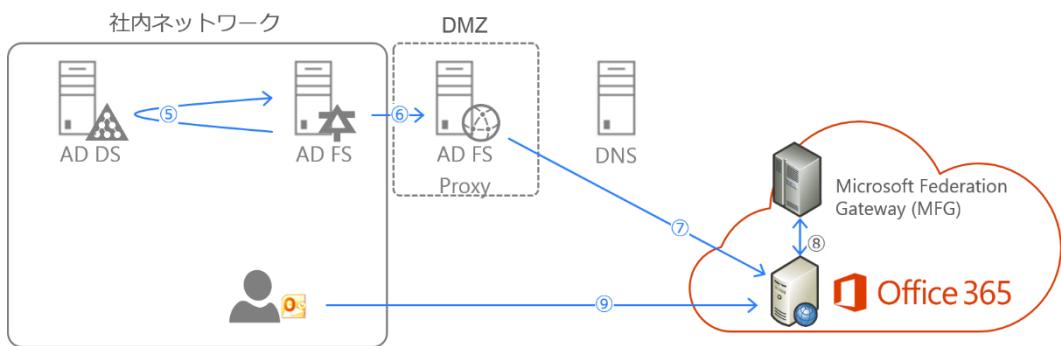
◆ POP, IMAP, ActiveSync, Outlook, EWS の場合

Note : この場合の認証フローについて

社内からのアクセス、社外からのアクセスとも同じフローとなります。



- ① ユーザーが Office 365 にアクセス (AD の認証情報が保存されていなければ認証画面が表示される)
- ② MFG にリダイレクト先の AD FS の URL を確認
- ③ 社外の DNS サーバーを参照して AD FS Proxy に接続し、AD の認証情報を送信
- ④ AD FS に接続してログイン トークンを要求



- ⑤ AD DS に接続し、ログオン トークン作成に必要なデータを収集
- ⑥ AD FS がログオン トークンを作成し、AD FS Proxy に返信
- ⑦ AD FS Proxy が Office 365 にログイン トークンを送信
- ⑧ MFG にログイン トークンを送信し、サービス チケットを取得
- ⑨ 認証が完了し、ユーザーにサービスの提供を開始

3.4 フェデレーション ID 利用時のアクセス

各サービス、およびアプリケーションを利用してアクセスする際の認証方法は、以下のとおりです。

	社内ネットワーク		社外ネットワーク	
	ドメイン参加 PC	ドメイン不参加 PC	ドメイン参加 PC	ドメイン不参加 PC
Outlook Web App	シングル サインオン	・ AD FS 接続時、認証情報を入力	・ AD FS Proxy 接続時、認証情報を入力	
Outlook	Outlook 起動時に認証情報を入力 (資格情報を保存することで次回以降の入力が不要)			
Office 365 ポータル	・ サインイン画面で ID を入力	・ サインイン画面で ID を入力	・ サインイン画面で ID を入力 ・ AD FS Proxy 接続時、認証情報を入力	
SharePoint Online		・ AD FS 接続時、認証情報を入力		
Lync Online	シングル サインオン	認証情報を入力	シングル サインオン	認証情報を入力

STEP 4. 全体の構築手順

この STEP では、これから導入する環境の構築の流れについて説明します。

この STEP では、次のことを学習します。

- ✓ 全体の構築手順

4.1 全体の構築手順

構築手順は以下のとおりです。上から順に作業を実施していきます。

STEP	大項目	項	中項目	作業場所			
				Office 365	Azure	社内	社外
5	Office 365 へ ドメインの追加、およびドメイ ンの確認	1	ドメインの追加	○			
		2	ドメイン登録情報の変更				○:DNS
		3	ドメインの所有確認	○			
		4	ドメインの目的を設定	○			○:DNS
6	VPN 接続、お よび接続状態 の確認	1	仮想ネットワークの作成		○:VNET		
		2	仮想ゲートウェイの作成		○:VNET		
		3	社内ネットワークの構成			○:DEV	
7	ストレージ ア カウントの作 成	1	ストレージ アカウントの設定		○:ST		
(8) 9	AD DS サーバーのセットアッ プ、および動作確認	1	AD DS のインストール		○:VM		
		2	ドメイン コントローラーへの昇 格		○:VM		
		3	サイトとサブネットの作成		○:VM		
		4	初期レプリケートの完了		○:VM		
		5	仮想ネットワークへの DNS サ ーバーの追加設定		○:VNET		
		6	NTP に関する注意点				
		7	2 台目以降の AD DS を構築す る際のポイント				
(8) 10	ディレクトリ 同期サーバー のセットアッ プ、および同期 の確認	1	UPN サフィックスの追加			○:AD	
		2	AD ユーザーの登録情報を確認			○:AD	
		3	ディレクトリ同期の有効化	○			
		4	ディレクトリ同期ツール関連の インストール		○:VM		
		5	ディレクトリ同期ツールのセッ トアップ(同期の実行)		○:VM		
		6	ディレクトリ同期の動作確認	○	○:VM		
		7	同期したユーザーのアクティブ 化	○			
(8) 11	AD FS サーバーのセットアッ プ、およびフェデレーシ ョンの確認	1	AD FS 2.1 関連をインストール		○:VM		
		2	サーバー証明書をインポートと 設定		○:VM		
		3	社内 DNS の設定			○:DNS	
		4	AD フェデレーション 用 サ ービス アカウントの作成			○:AD	
		5	フェデレーション サーバーの設 定		○:VM		
		6	2 台目以降のフェデレーション サーバーの設定		○:VM		

Microsoft Azure 自習書シリーズ No.6
企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

STEP	大項目	項	中項目	作業場所			
				Office 365	Azure	社内	社外
(8) 11	AD FS サーバーのセットアップ、およびフェデレーションの確認 ※前ページの続き	7	IT プロフェッショナル 用 Microsoft Online Services サインイン アシスタントをインストール		○:VM		
		9	Windows PowerShell 用 Windows Azure Active Directory モジュールのインストール	○	○:VM		
		10	フェデレーション ドメインの有効化		○:VM		
		11	ローカル インターネット ゾーンへのサイトの登録			○:PC	
		12	フェデレーション環境の動作確認		○:VM	○:PC	
(8) 12	AD FS Proxy サーバーのセットアップ、および動作確認	1	AD FS 2.1 関連をインストール		○:VM		
		2	サーバー証明書をインポートと設定		○:VM		
		3	エンドポイント HTTPS を作成		○:VM		
		4	社外 DNS の設定				○:DNS
		5	フェデレーション サーバー ポキシの設定		○:VM		
		6	AD FS Proxy サーバーの動作確認		○:VM		○:PC

【STEP.9 ~ 12 の事前作業】

STEP	大項目	項	中項目	作業場所			
				Office 365	Azure	社内	社外
8	仮想マシンの作成	1	仮想ネットワークへの DNS サーバーの設定		○:VNET		
		2	仮想マシンの作成		○:VM		
		3	仮想マシンへのリモートデスクトップ接続		○:VM		
		4	日本語化		○:VM		
		5	タイムゾーン		○:VM		
		6	Windows Update の設定		○:VM		
		7	ディスクの追加		○:VM		
		8	ドメインへの参加		○:VM		

Note : 凡例

- ・ DNS … DNS サーバー
- ・ VNET …仮想ネットワーク
- ・ DEV …VPN デバイス
- ・ ST …ストレージ アカウント
- ・ VM …仮想マシン
- ・ AD … AD DS サーバー
- ・ PC …クライアント PC

STEP 5. Office 365 ヘドメインの追加、 およびドメインの確認

この STEP では、Office 365 で利用するドメインを Office 365 の管理センターから追加する手順について説明します。

この手順を実施することで、ドメインの所有者の確認が行われ、以下のサービスが現在使用しているドメイン名で利用する準備が整います。

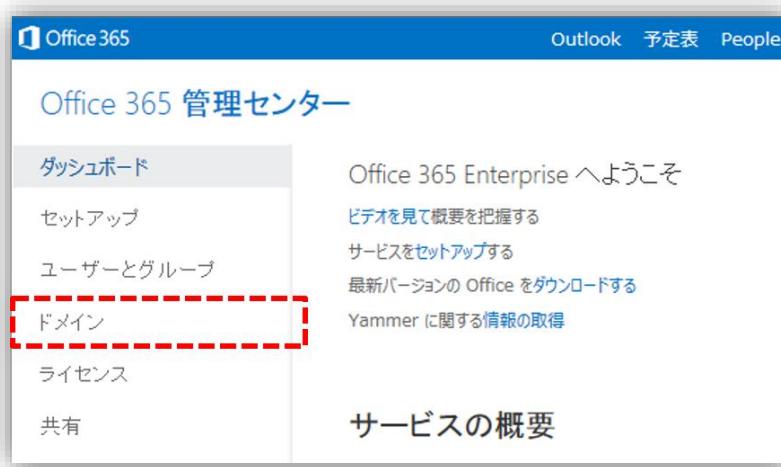
- Active Directory フェデレーション サービス
- ディレクトリ同期
- Microsoft Exchange Online
- Microsoft SharePoint Online
- Microsoft Lync Online

この STEP では、次のことを学習します。

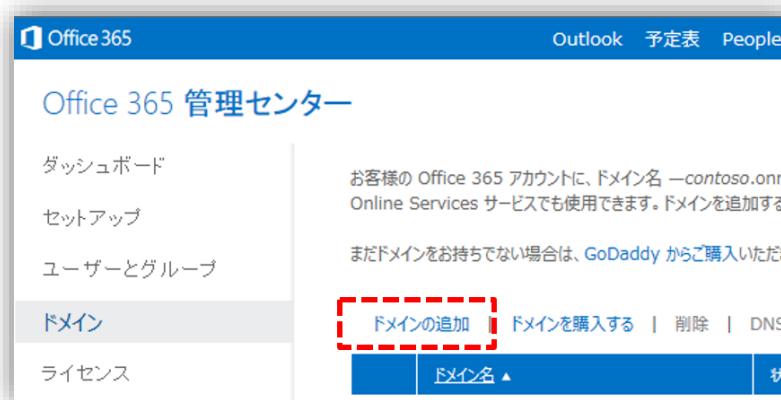
- ✓ ドメインの追加
- ✓ ドメイン登録情報の変更
- ✓ ドメインの所有確認
- ✓ ドメインの目的を設定

5.1 ドメインの追加

1. Office 365 管理者アカウントで「Office 365 管理センター」にサインインします。
2. [管理者の概要] ページの左側にある [ドメイン] をクリックします。

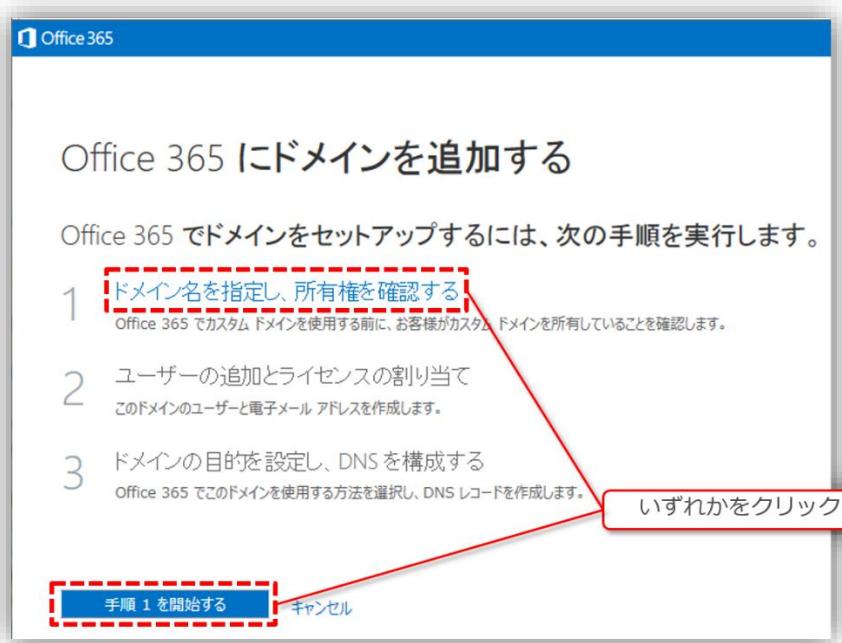


3. [ドメイン] ページが開きます。 ドメイン一覧にある [ドメインの追加] をクリックします。



企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

4. [ドメインのセットアップ] ページが開きます。[ドメイン名を指定し、所有権を確認する] または [手順 1 を開始する] をクリックします。



5. [1. ドメイン名の指定] ページが開きます。ドメイン名 (例 : azurestudy.jp) を入力し、[次へ] をクリックします。



企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

6. [2. 所有権の確認] ページが開きます。赤枠のドロップダウンリストからドメイン登録情報を管理している DNS ホスティング プロバイダーを選択する（無い場合は「一般的な手順」を選択）と、TXT レコードの情報（エイリアス、またはホスト名）が表示されます。

レコードタイプ (1つ選択)	エイリアス名またはホスト名	宛先またはポイント先のアドレス	TTL
TXT	@ または azurestudy.jp	MS=ms	1 時間
MX	@ または azurestudy.jp	ms	.outlook.com 1 時間

Note : 注意事項

この時点で [完了しました。今すぐ確認してください。] をクリックしても、TXT レコードの登録が済んでいないので、エラーが表示されます。ドメイン登録情報を管理している DNS にこのページで指定されている TXT レコードを追加して下さい。

5.2 ドメイン登録情報の変更

- ドメイン登録情報を管理している DNS に「5.1 ドメインの追加」の手順 6 で指定されている TXT レコードを追加してください。

Note : TXT レコードについて

今回のドメイン「azurestudy.jp」では、外部 DNS 上に以下の TXT レコードを追加しています。

azurestudy.jp MS=ms12345678

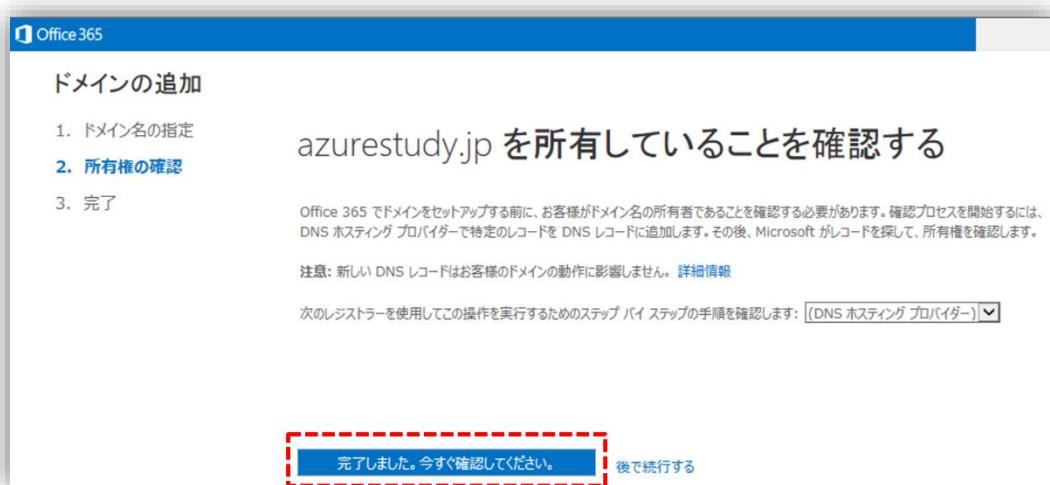
※ 数字部分 (12345678) はドメインによって異なります。

- 手順 1 の登録情報の変更が反映されるまで待ちます。

5.3 ドメインの所在確認

◆ ドメインの所在確認

- 「5.2 ドメイン登録情報の変更」で追加した TXT レコードが反映されたら、「5.1 ドメインの追加」の手順 6 の [2. 所有権の確認] ページで [完了しました。今すぐ確認してください。] をクリックします。

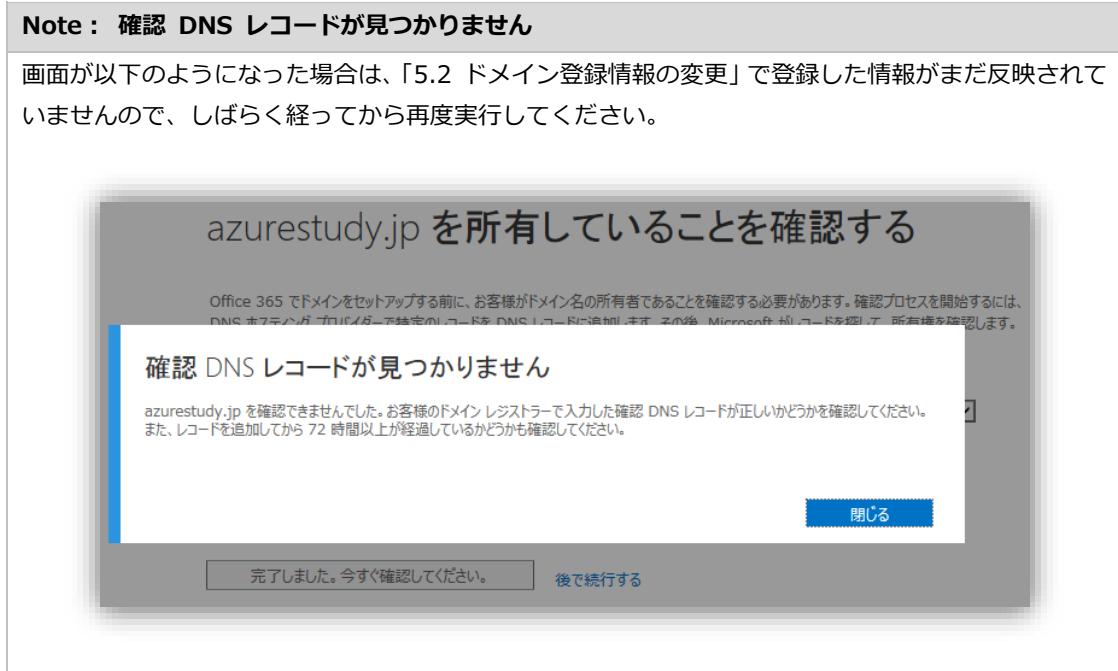


Note : サインアウトしてしまった場合

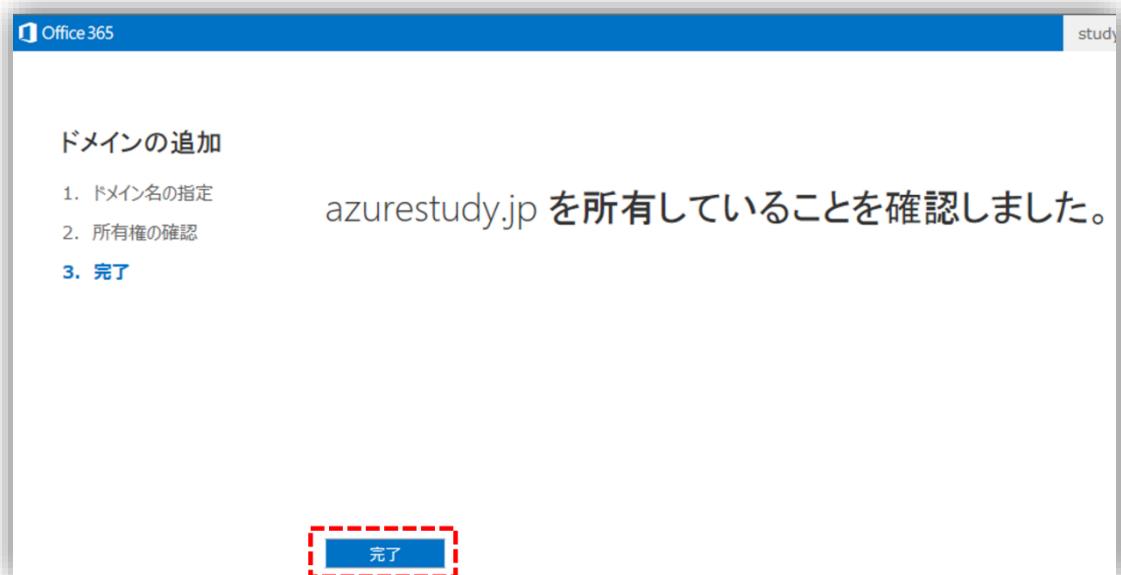
「Office 365 管理センター」からサインアウトしてしまった場合は、再び Office 365 管理者アカウントにて「Office 365 管理センター」にサインインして、当ページを開いてください。

- [ドメインの確認中] 画面が表示されます。



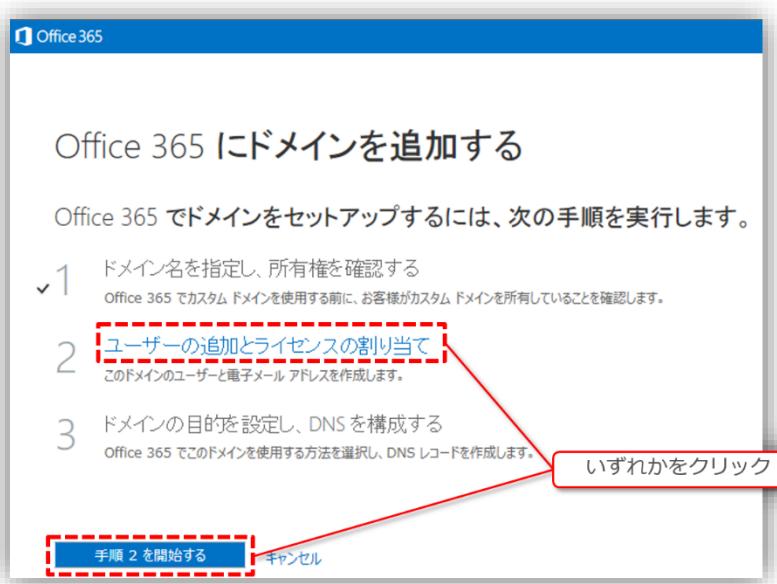


3. 「azurestudy.jp を所有していることを確認しました。」とメッセージが表示されます。 [完了] をクリックします。

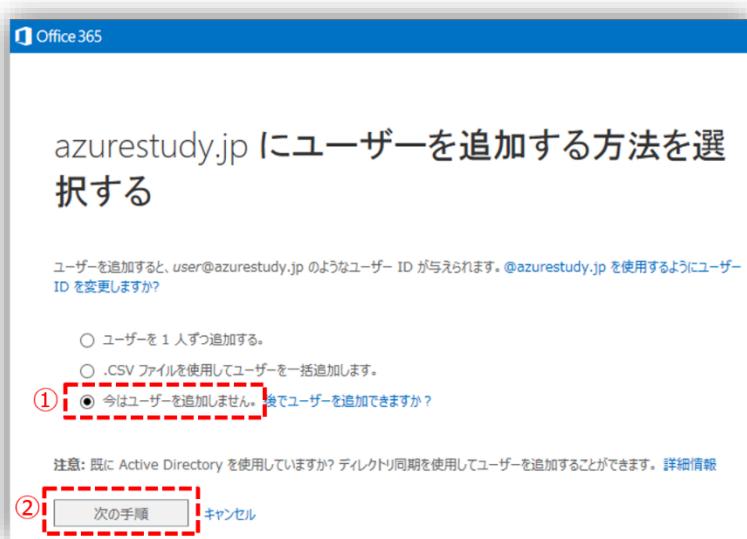


→ ユーザーの追加とライセンスの割り当て

4. 手順 3 後、[ドメインのセットアップ] ページに戻ります。 [ユーザーの追加とライセンスの割り当て] または [手順 2 を開始する] をクリックします。

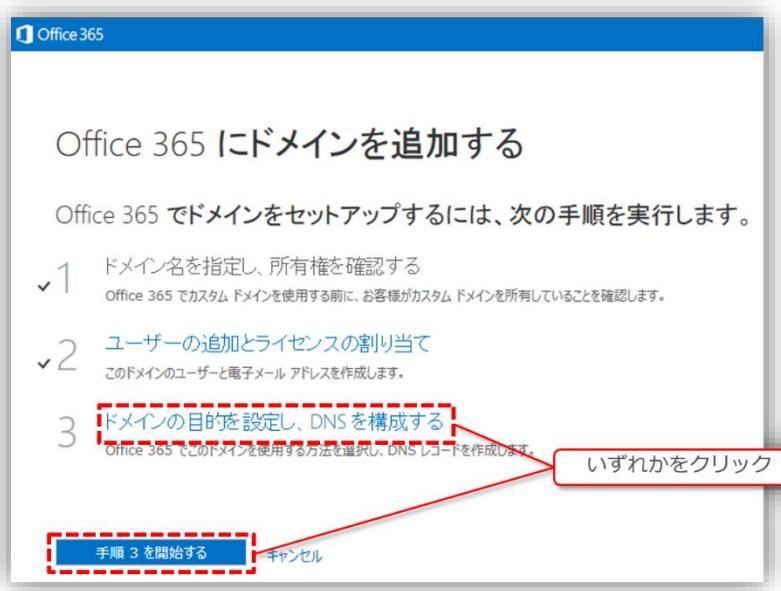


5. Office 365 のユーザーの追加は、後述する「STEP 10. ディレクトリ同期サーバーのセットアップ、および同期の確認」にて実施するので、[今はユーザーを追加しません。] を選択して [次の手順] をクリックします。

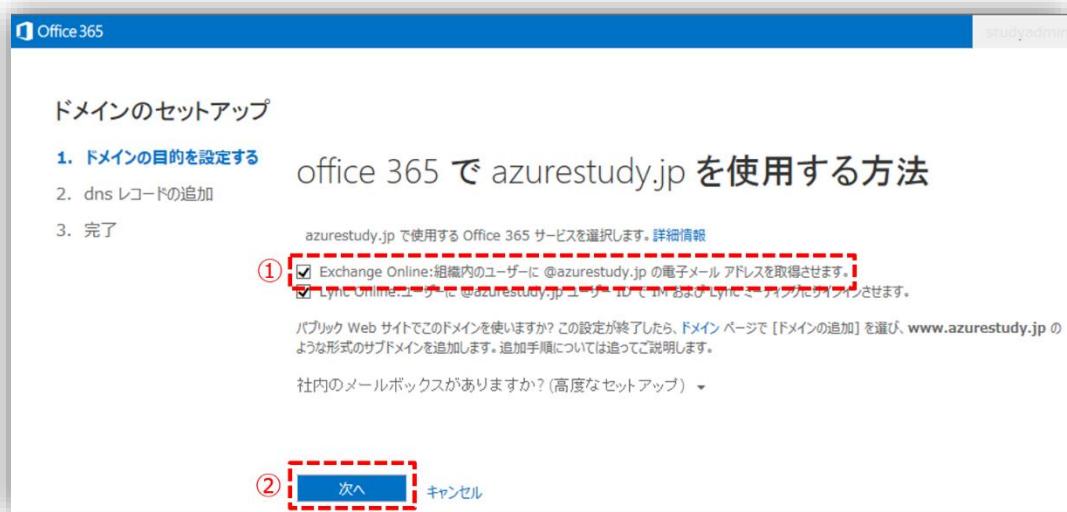


5.4 ドメインの目的を設定

- [ドメインのセットアップ] ページに戻り、[ドメインの目的を設定し、DNS を構成する] または [手順 3 を開始する] をクリックします。



- [ドメインの目的を設定する] ページが開きます。 [Exchange Online: 組織内のユーザーに @azurestudy.jp の電子メール アドレスを取得させます。] チェックボックスにチェックが付いていることを確認します。チェックが付いていない場合は、チェックを付けて [次へ] をクリックします。



Note : ドメインの目的を設定

AD FS でサインインできるかのみを確認する場合は、ドメインの目的をチェックしないで進ませることもできます。

- 必要な DNS レコードが表示されます。ドメイン登録情報を管理している DNS に必要なレコードを追加して下さい。

The screenshot shows the 'Domain setup' screen in the Office 365 portal. The main heading is 'Domain setup'. Below it, a note says: 'These DNS records will be added to the DNS provider for azurestudy.jp.' A table displays three DNS records:

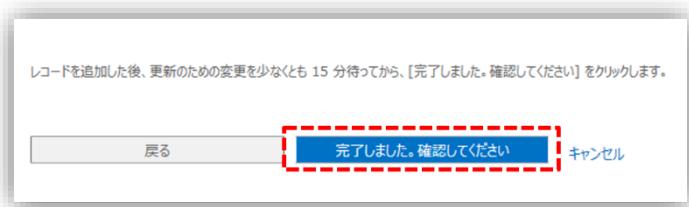
種類	優先度	ホスト名	ポイント先のアドレス	TTL
MX	0	@	[Redacted]	1 時間
CNAME	-	autodiscover	[Redacted]	1 時間

種類	TXT 名	TXT 値	TTL
TXT	@	[Redacted]	1 時間

Note : ドメインの目的を設定

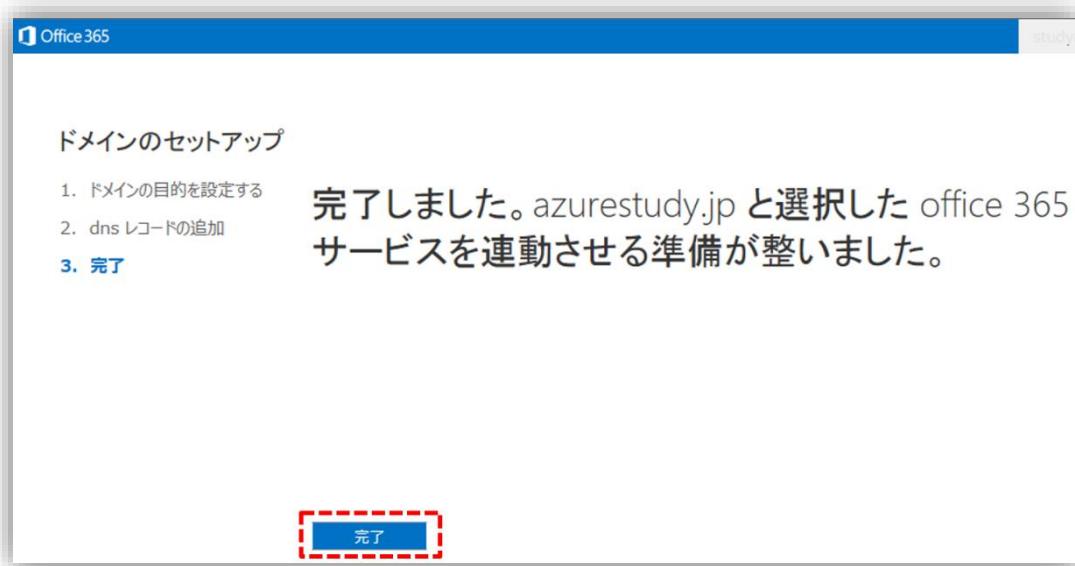
MX レコードなどの追加ができない場合でもドメインは利用できるので、AD FS の設定を進めることができます。

- 手順 3 の登録情報の変更が反映されるまで待ちます。
- 再び、手順 3 のレコードが表示されている画面に戻り、[完了しました。確認してください] をクリックします。



企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

6. 「完了しました。azurestudy.jp と選択した Office 365 サービスを連動させる準備が整いました。」とメッセージが表示されます。 [完了] をクリックします。



7. [ドメイン] ページに戻り、追加したドメインの状態が「アクティブ」になっていることを確認します。

Office 365 管理センター

お客様の Office 365 アカウントに、ドメイン名 —contoso.onmicrosoft.com— が付きます。既に独自のドメイン名をお持ちの場合 Online Services サービスでも使用できます。ドメインを追加するには、[ドメインの追加] をクリックします。

まだドメインをお持ちでない場合は、[GoDaddy](#) からご購入いただけますと、お客様の代わりに設定いたします。

	ドメイン名	状態
<input type="radio"/>	azurestudy.jp	アクティブ
<input type="radio"/>	.onmicrosoft.com	アクティブ

ドメインの追加 | ドメインを購入する | 削除 | DNS 設定の表示 | トラブルシューティング

ドメインの追加 | ドメインを購入する | 削除 | DNS 設定の表示 | トラブルシューティング

※ ドメインの状態について

状態	説明
セットアップが進行中です	ドメインがテナントに有効になりましたが、追加された手順を実行していません。作業を完了する場合、[ドメインの追加] ページの [手順 3 ドメインの目的を設定し、DNS を構成する] を行います。この状態は、DNS の構成工ラー、または DNS レコードの更新が終了していない場合にも表示されることがあります。
アクティブ	ドメインが正常に追加され、ドメインを所有していることが Office 365 により確認されました。ドメインが [アクティブ] 状態となっている場合、電子メールアドレスの作成を開始して、そのドメインを必要とする他の機能を使用できます。
削除待ち	Office 365 により、ドメインの削除が開始されましたが、削除処理が完了していないか、ドメインの削除中に問題がありました。この状態が解決されない場合は、ドメインをもう一度削除してみてください。

Note : 他のサービスとも連動する場合

この後、他のサービスとも連動するように Office 365 を構成する場合は、必要に応じてレコードを DNS に登録してください。

STEP 6. VPN 接続の設定

この STEP では、VPN 接続のために仮想ネットワーク、仮想ゲートウェイの作成について説明します。

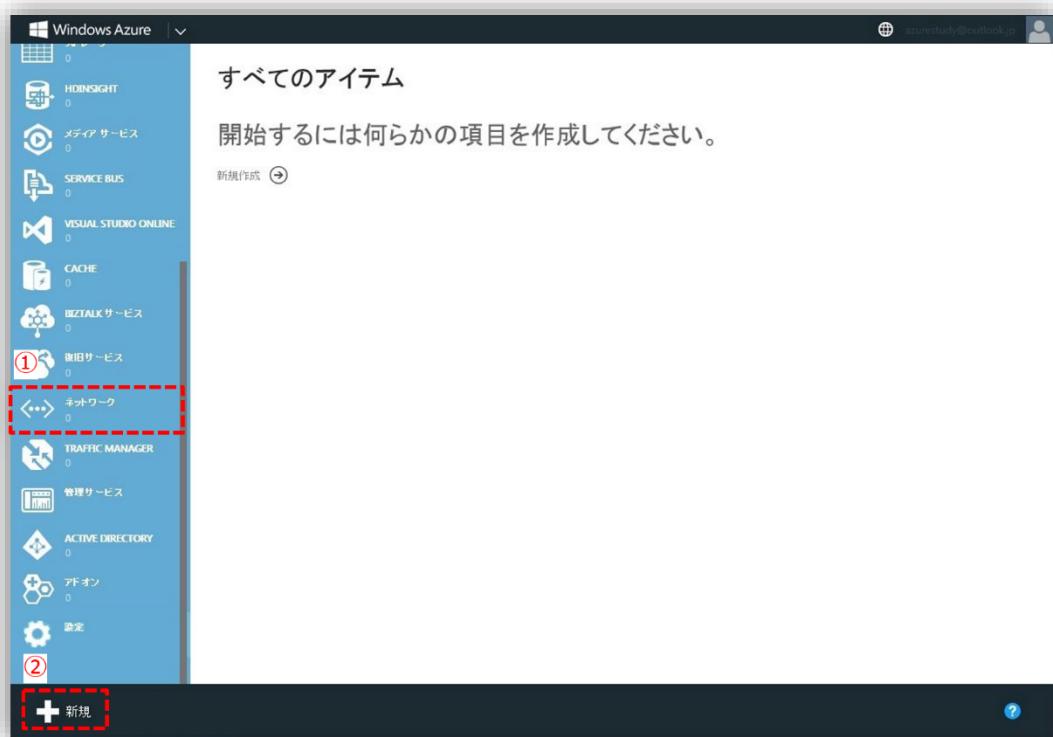
この STEP では、次のことを学習します。

- ✓ 仮想ネットワークの作成
- ✓ 仮想ゲートウェイの作成
- ✓ 社内ネットワークの構成

6.1 仮想ネットワークの作成

仮想ネットワークは、仮想マシンを社内ネットワークへ接続し、社内のコンピューターのように操作することができます。仮想ネットワークの接続形態には、「サイト間 VPN」と「ポイント対サイト VPN」があります。ここでは、サイトとサイトを接続する「サイト間 VPN」を作成します。

1. Azure 管理ポータルにサインインします。
2. 画面左側のメニューから [ネットワーク] をクリックして画面左下の [+新規] をクリックします。



3. [ネットワークサービス] > [仮想ネットワーク] > [カスタム作成] をクリックします。



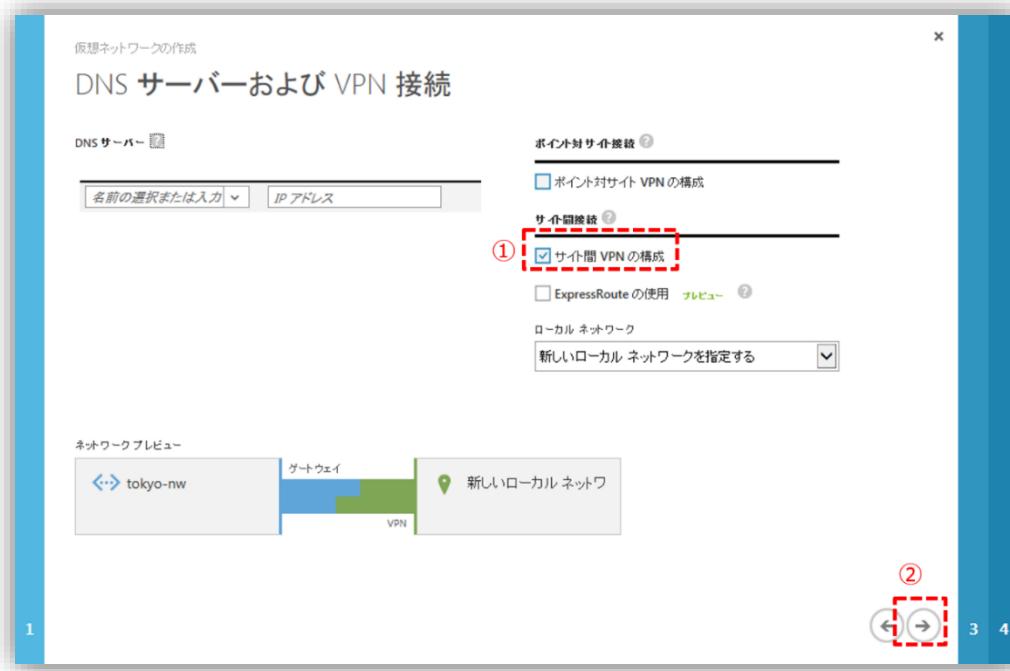
4. [仮想ネットワークの作成] ウィザードが表示されます。以下、ウィザードに従って操作していきます。

[仮想ネットワークの詳細] ページにて下の表のとおり指定して右下の [→] をクリックします。



項目	設定値
名前	「tokyo-nw」を入力
場所	「日本 (東)」を選択

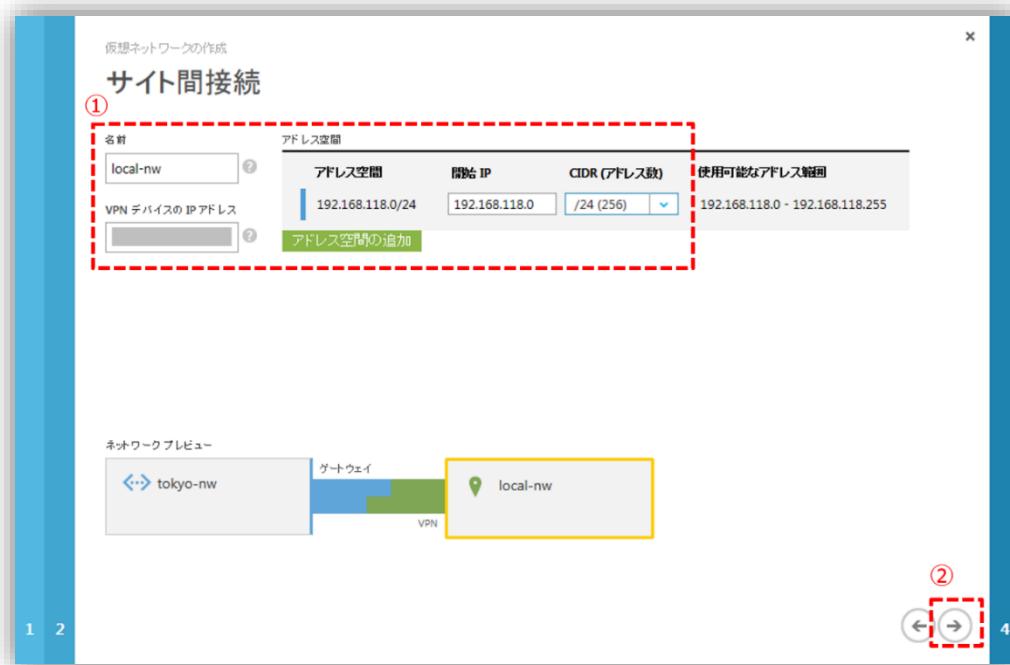
企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携
[DNS サーバーおよび VPN 接続] ページにて [サイト間 VPN の構成] チェックボックスにチェックを付けて右下の [→] をクリックします。



Note : DNS サーバーについて

DNS サーバーを設定することによって、Azure 上に構築した仮想マシンに DNS サーバーの設定が DHCP で払い出しされます。 DNS サーバーの IP アドレスが決まっていない場合は、後から設定することも可能です。

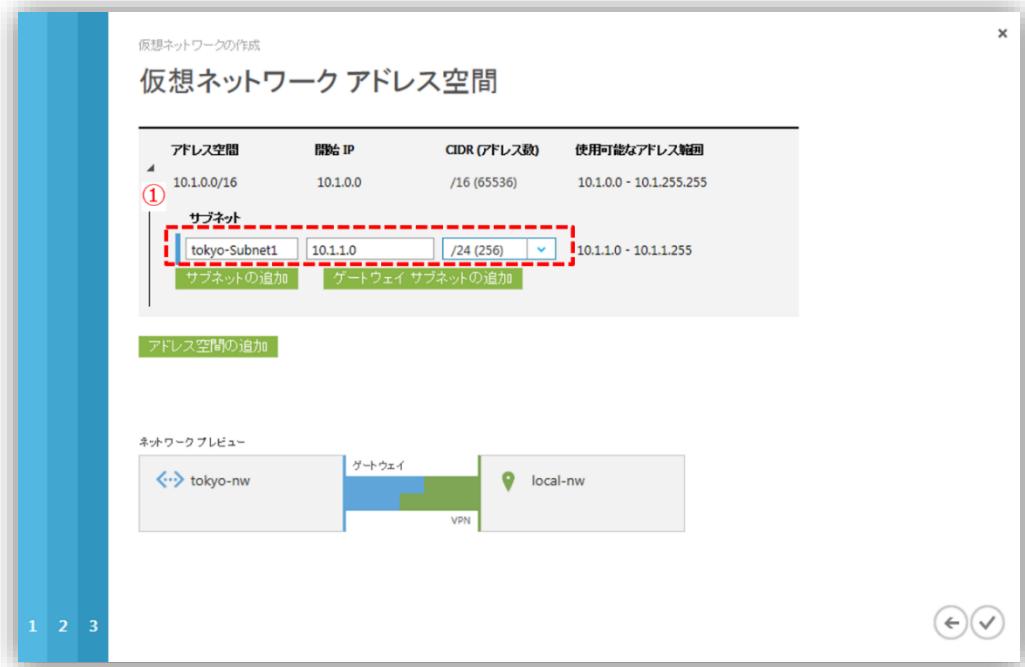
[サイト間接続] ページにて下の表のとおり指定して右下の [→] をクリックします。



企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

項目	設定値				
名前	「local-nw」を入力				
VPN デバイスの IP アドレス	<プロバイダーから割り当てられた WAN 側の IP アドレス>を入力				
アドレス空間	<table border="1"> <tr> <td>開始 IP</td> <td>「192.168.118.0」を入力</td> </tr> <tr> <td>CIDR (アドレス数)</td> <td>「/24 (256)」を選択</td> </tr> </table>	開始 IP	「192.168.118.0」を入力	CIDR (アドレス数)	「/24 (256)」を選択
開始 IP	「192.168.118.0」を入力				
CIDR (アドレス数)	「/24 (256)」を選択				

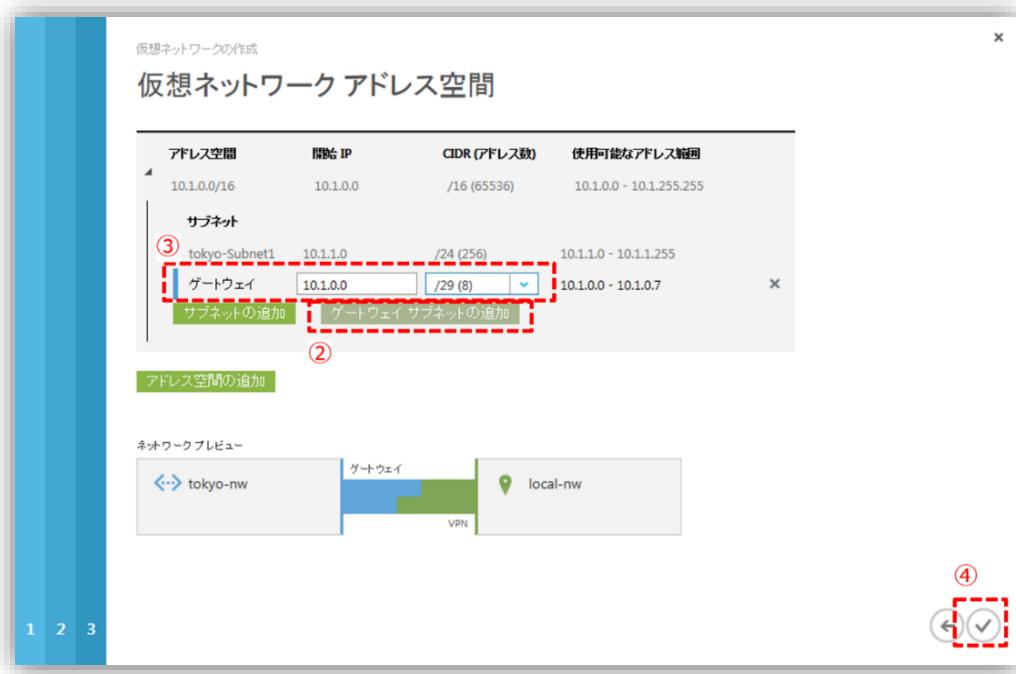
[仮想ネットワークアドレス空間] ページにて下の表とおり指定します。



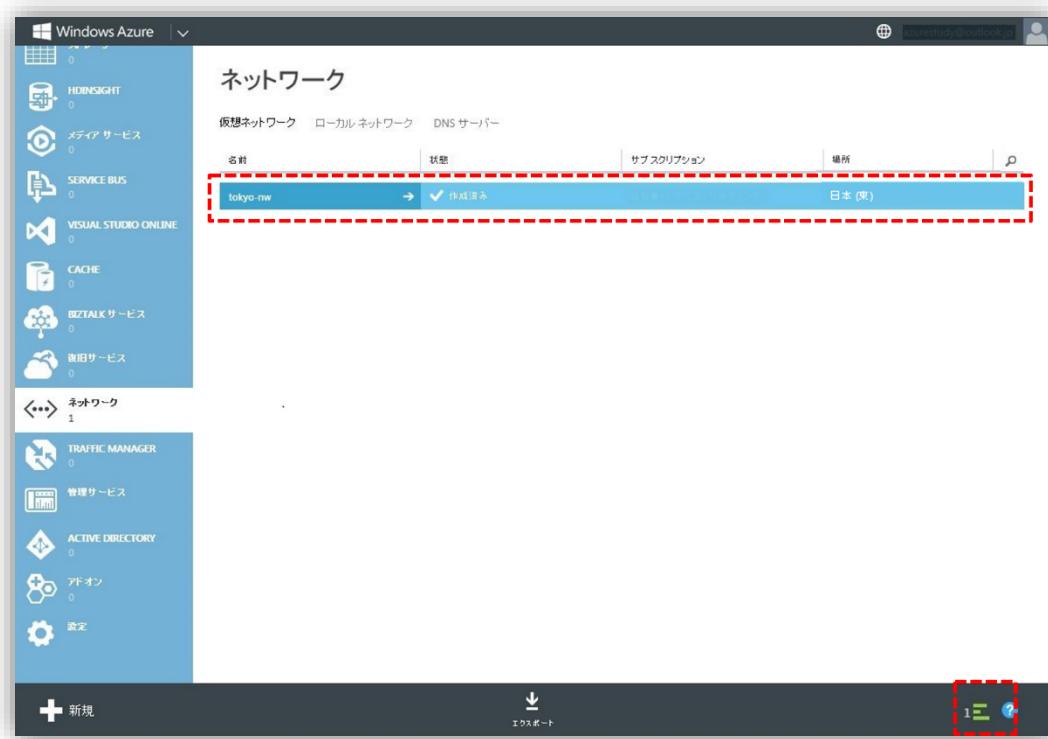
項目	設定値
名前	「tokyo-Subnet1」を入力
サブネットの開始 IP	「10.1.1.0」を入力
CIDR (アドレス数)	「/24 (256)」を選択

引き続き、[ゲートウェイサブネットの追加] をクリックします。サブネットの行に [ゲートウェイ] が追加されますので、[ゲートウェイの開始 IP] を入力し、[ゲートウェイの CIDR (アドレス数)] を選択します。（今回はデフォルト値を使用します。）入力および選択が終わったら、右下の [チェック] をクリックします。

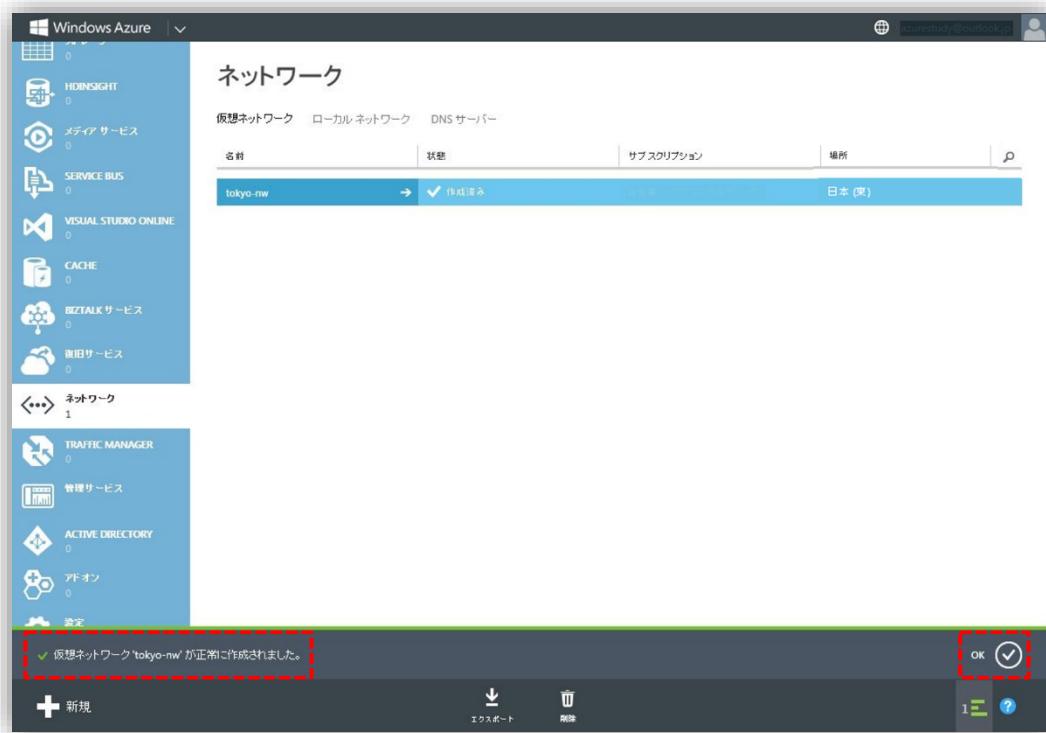
Microsoft Azure 自習書シリーズ No.6
企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携



5. [仮想ネットワーク] ページに戻ります。 作成中の仮想ネットワークがリストに表示されます。
右下に作成中であることを示すアイコンが表示されます。

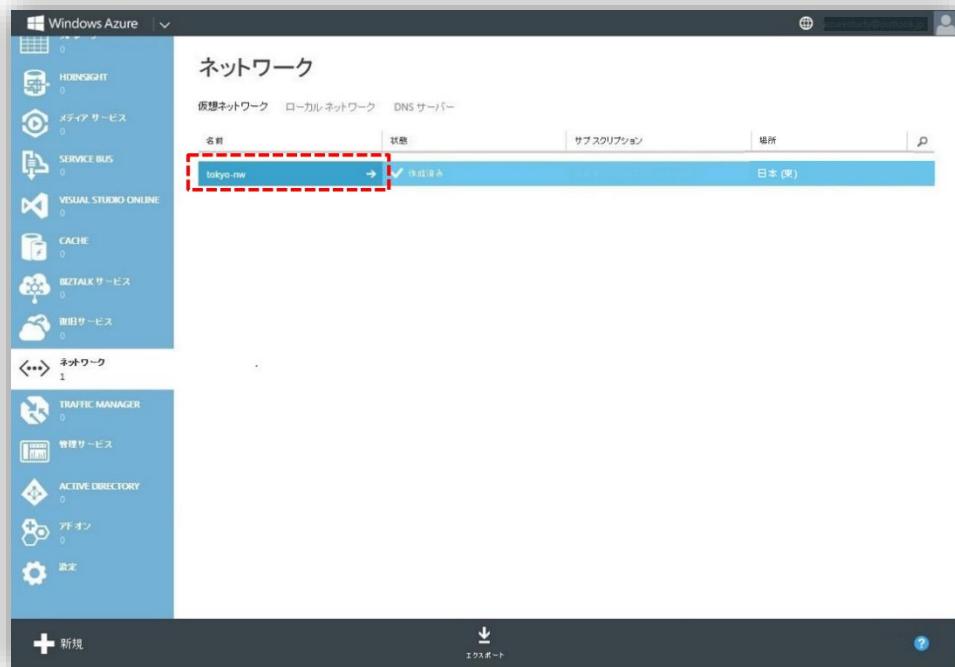


6. 「仮想ネットワーク “tokyo-nw” が正常に作成されました。」とメッセージが表示されたら、[OK] チェックをクリックしてメッセージを閉じます。

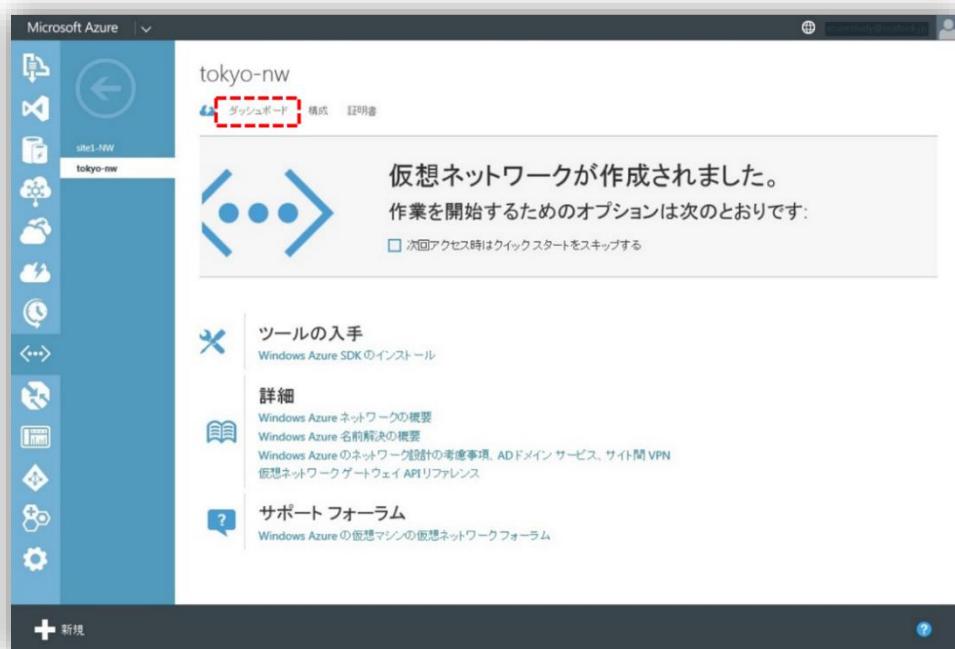


6.2 仮想ゲートウェイの作成

- 作成した仮想ネットワーク [tokyo-nw] をクリックします。

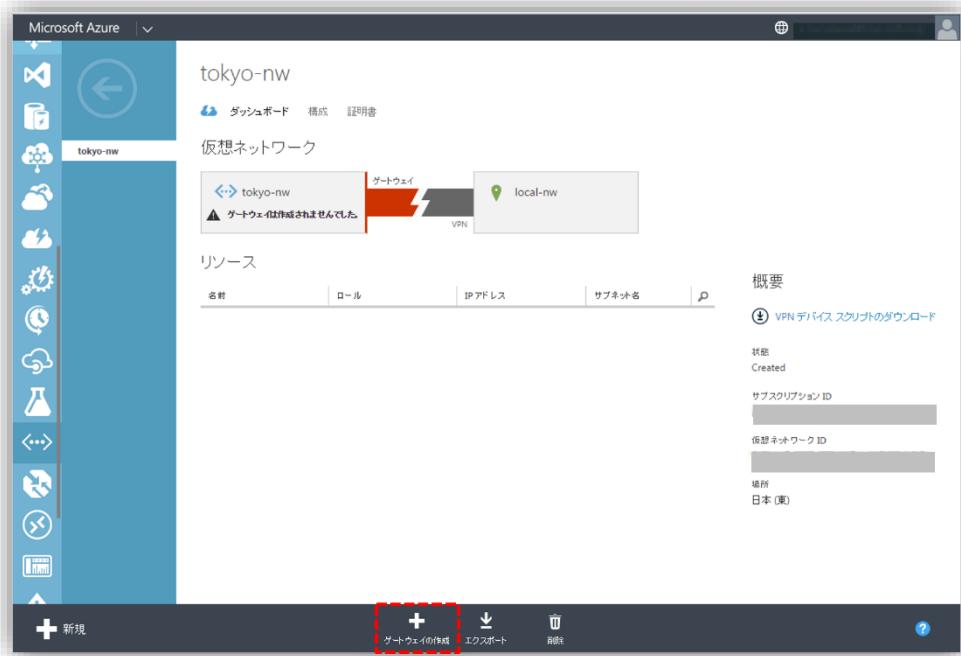


- [ダッシュボード] タブをクリックします。

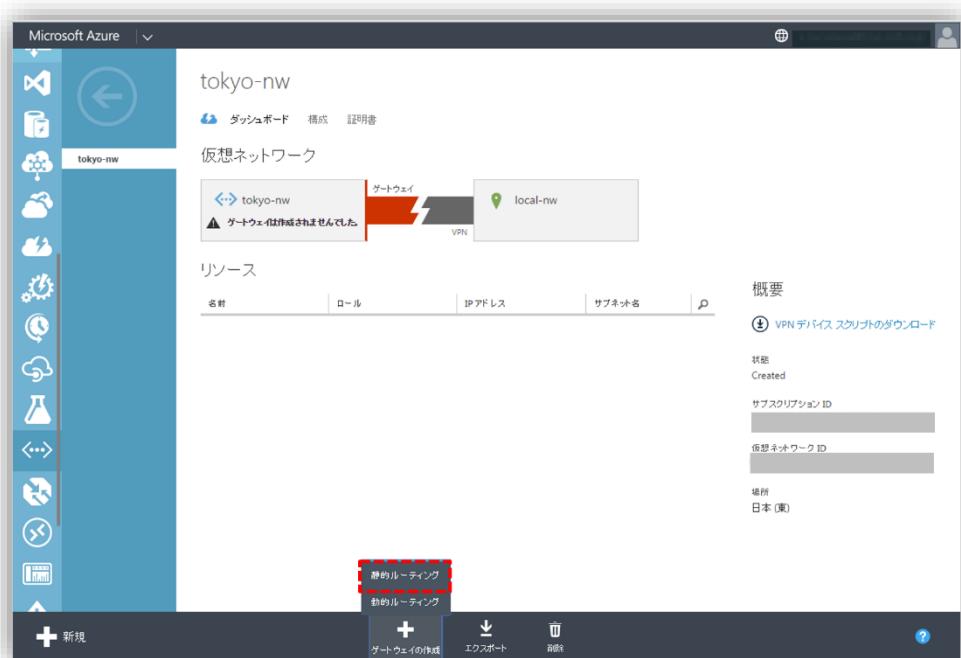


企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

3. [ダッシュボード] ページにて画面下部の [+ ゲートウェイの作成] をクリックします。

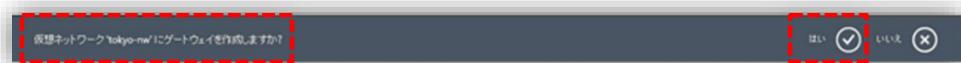


4. [静的ルーティング/動的ルーティング] のリストが表示されます。 今回は [静的ルーティング] をクリックします。

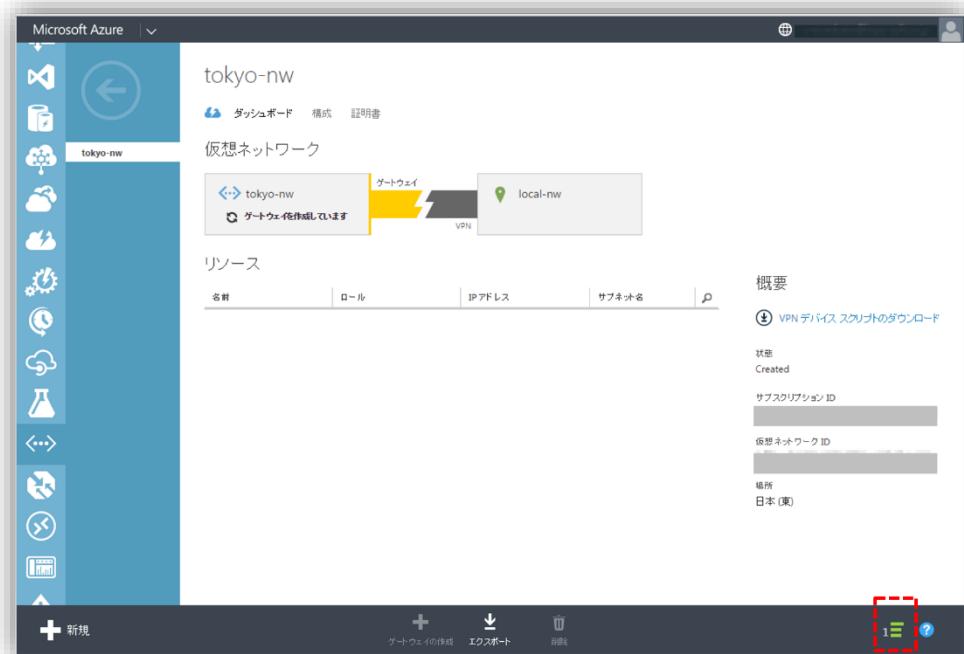


企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

5. 画面下部に「仮想ネットワーク "tokyo-nw" にゲートウェイを作成しますか？」のメッセージが表示されるので、[はい] をクリックします。

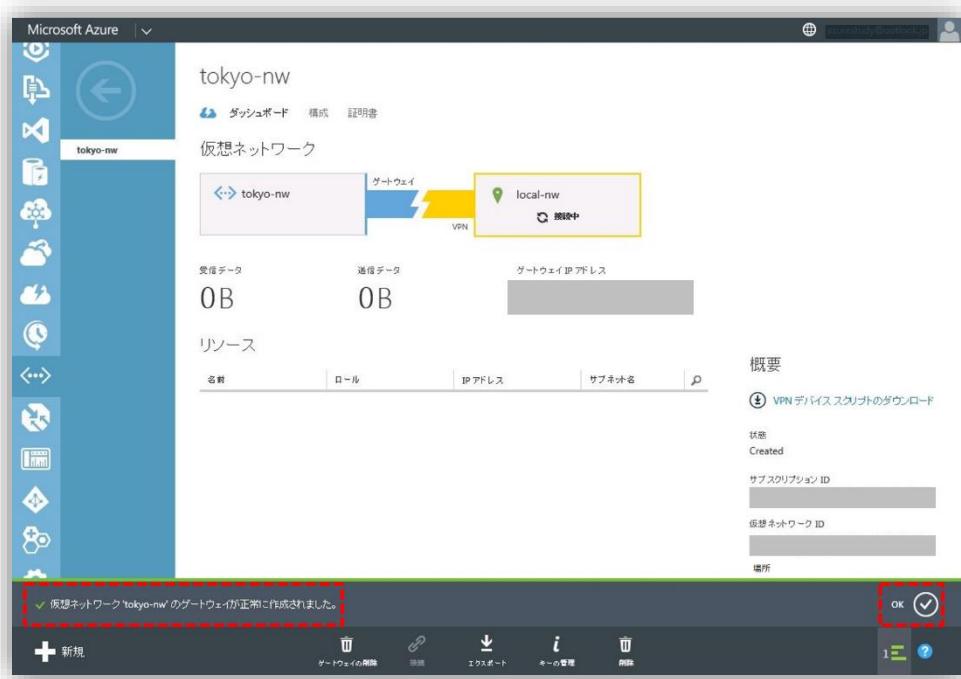


6. [ダッシュボード] ページに戻ります。右下に作成中であることを示すアイコンが表示されます。



企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

7. 「仮想ネットワーク “tokyo-nw” のゲートウェイが正常に作成されました。」とメッセージが表示されたら、[OK] をクリックしてメッセージを閉じます。



6.3 社内ネットワークの構成

◆ 社内ネットワークの構成

Azure と接続するための VPN 機器の設定を行います。

Note : VPN 機器関連の参考先

- VPN 接続検証済み ルーター一覧
<http://msdn.microsoft.com/ja-jp/windowsazure/dn132612.aspx>
- 一般的な VPN 機器の必須要件と Cisco 社と Juniper 社のルーターについては、こちらをご確認ください
<http://msdn.microsoft.com/en-us/library/windowsazure/jj156075.aspx>

◆ 社内ネットワークの構成手順

社内ネットワークの作成手順については、別途自習書「企業内システムと Microsoft Azure の VPN 接続」の「STEP 8 . ASA の設定」をご参照ください。

STEP 7. ストレージ アカウントの作成

この STEP では、仮想マシンを作成するために必要なストレージアカウントの作成について説明します。

この STEP では、次のことを学習します。

- ✓ ストレージ アカウントの設定

7.1 ストレージ アカウントの設定

ストレージアカウントは Azure のストレージを使用するために必要なアカウントです。事前にストレージアカウントを作成せずに仮想マシンを作成することも可能ですが、その場合、ランダムな名称が用いられます。

今後の管理の面なども考慮してこの自習書では、仮想マシンを作成する前に明示的にストレージアカウントを作成します。

1. Azure 管理ポータルにサインインします。
2. 画面左側のメニューから [ストレージ] をクリックし、画面左下の [+新規] をクリックします。

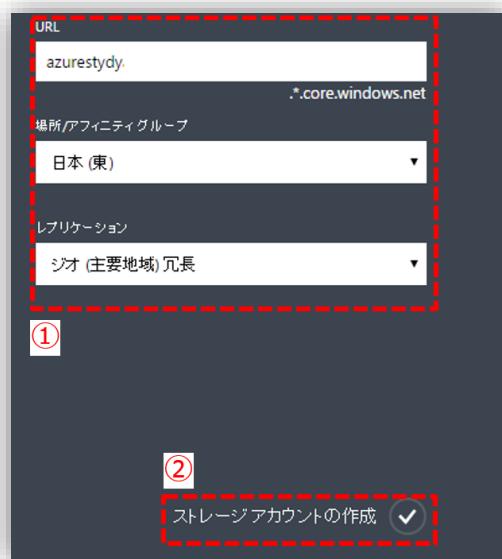


企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

3. [データサービス] > [ストレージ] > [簡易作成] の順にクリックします。

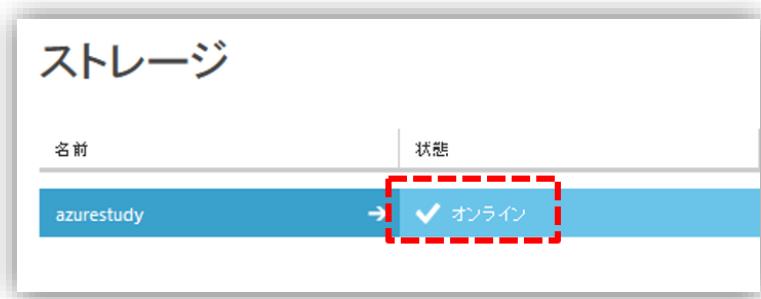


さらに、上記画面の右側の入力項目に下の表のとおり指定して右下の [ストレージアカウントの作成] をクリックします。



項目	設定値
URL	「azurestudy」を入力
場所/アフィニティ グループ	「日本 (東)」を入力
レプリケーション	「ジオ (主要地域) 冗長」を選択

4. ストレージアカウントが作成されると [状態] が [オンライン] になります。



STEP 8. 仮想マシンの作成

この STEP では、仮想マシンを作成するための手順について説明します。

この STEP では、次のことを学習します。

- ✓ 仮想ネットワークへの DNS サーバーの設定
- ✓ 仮想マシンの作成
- ✓ 仮想マシンへのリモートデスクトップ接続
- ✓ 日本語化
- ✓ タイムゾーン
- ✓ Windows Update の設定
- ✓ ディスクの追加
- ✓ ドメインへの参加

8.1 仮想ネットワークへの DNS サーバーの設定

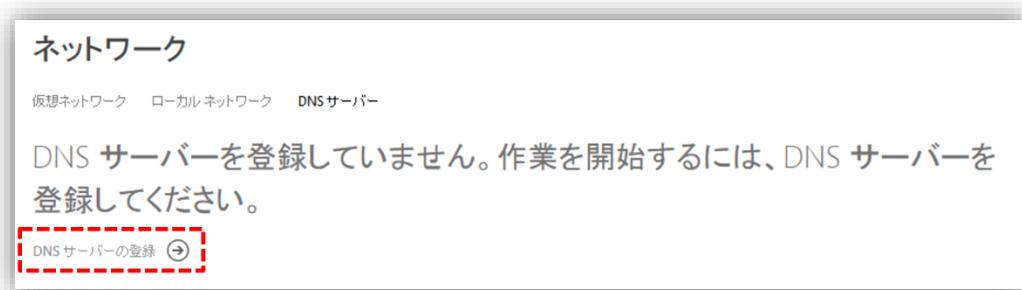
Azure 上に構築した仮想マシンへの IP の払い出しと DNS サーバーの払い出しも DHCP によって行われます。DNS サーバーの IP 設定は手動でも設定することは可能ですが、特別な理由がない限り DHCP で DNS サーバー (AD DS) の IP を払い出せるようにしておくことをお勧めします。

◆ DNS サーバーの登録

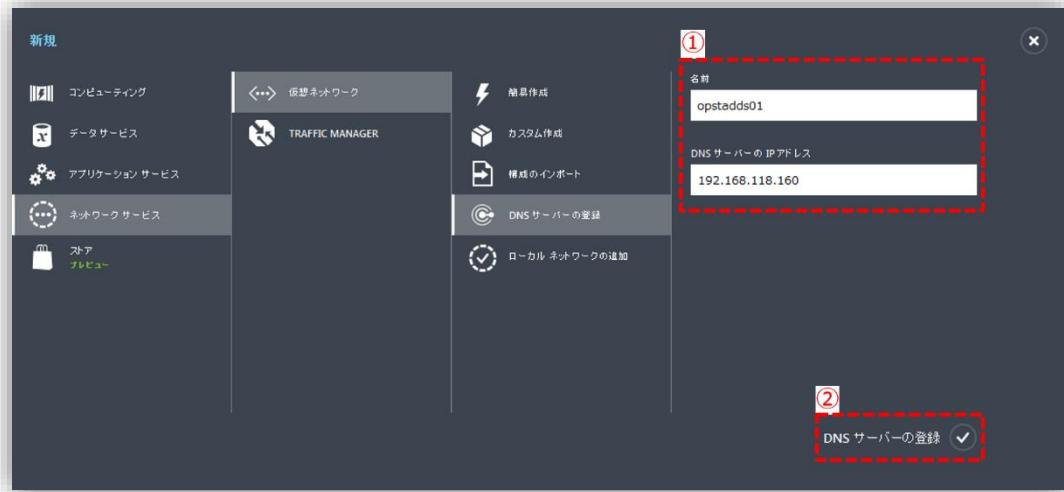
1. Azure 管理ポータルにサインインします。
2. 画面左側のメニューから [ネットワーク] をクリックします。 [ネットワーク] ページが表示したら、[DNS サーバー] タブをクリックします。



3. [DNS サーバーの登録] をクリックします。



4. ページが下図のようになります。下の表とおり指定して右下の [DNS サーバーの登録] をクリックします。



項目	設定値
名前	「OPSTADDS01」を入力
DNS サーバーの IP アドレス	「192.168.118.160」を入力

5. 登録処理後、手順 3 のページに戻り、DNS サーバーが登録されたことが確認できます。



➔ DNS サーバーの追加

6. [ネットワーク] ページの [仮想ネットワーク] タブをクリックします。

The screenshot shows the Microsoft Azure Network blade. At the top, there are three tabs: '仮想ネットワーク' (Virtual Network), 'ローカル ネットワーク' (Local Network), and 'DNS サーバー' (DNS Server). The '仮想ネットワーク' tab is highlighted with a red dashed box. Below the tabs, there are two rows of network configurations. The first row has a '名前' (Name) field containing 'opstadds01' and an 'アドレス' (Address) field containing '192.168.118.160'. The second row is partially visible.

7. 「tokyo-nw」をクリックします。

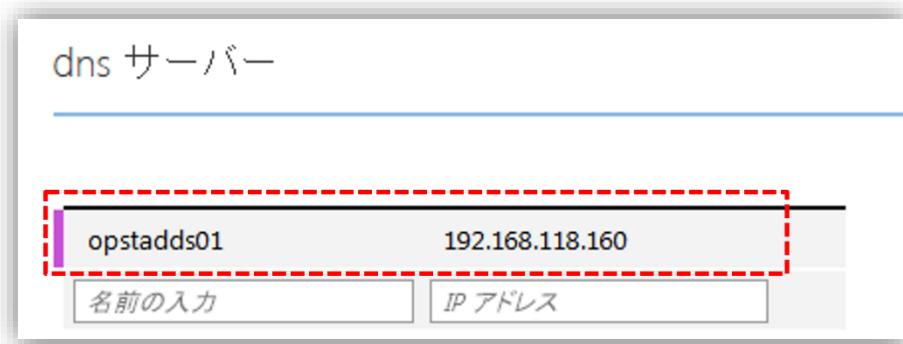
The screenshot shows the Microsoft Azure Network blade with the 'Virtual Network' tab selected. A list of existing virtual networks is displayed. One item, 'tokyo-nw', is highlighted with a red dashed box. To the right of 'tokyo-nw', there is a blue button with a white checkmark and the text '作成済み' (Created).

8. [構成] タブをクリックします。

The screenshot shows the Microsoft Azure Virtual Network configuration blade for the 'tokyo-nw' network. At the top, there are four tabs: 'ダッシュボード' (Dashboard), '構成' (Configuration), '証明書' (Certificates), and 'オプション' (Options). The '構成' tab is highlighted with a red dashed box. Below the tabs, there is a large blue arrow icon pointing from left to right. To the right of the icon, the text '仮想ネットワークが作成されました。作業を開始するためのオプションが表示されます。' (The virtual network has been created. Options for starting work will be displayed.) is shown. At the bottom right, there 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' (Skip quick start next time I access).

9. 手順 5 で登録された DNS サーバーをプルダウンから選択します。

変更等が入った箇所の DNS サーバー (AD DS) 名の左に紫のバーが表示されます。 今回は 1 つ新規に追加したため、下図のように表示されています。

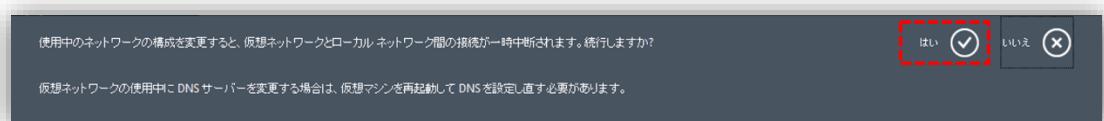


10. 画面下部の [保存] をクリックします。

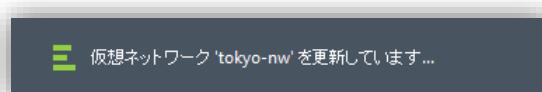


※ 手順 9 を実施すると表示されます。

11. DNS サーバーの設定を変更する際、一時的にネットワークが切断されることがあるため、その警告が表示されます。 [はい] をクリックします。



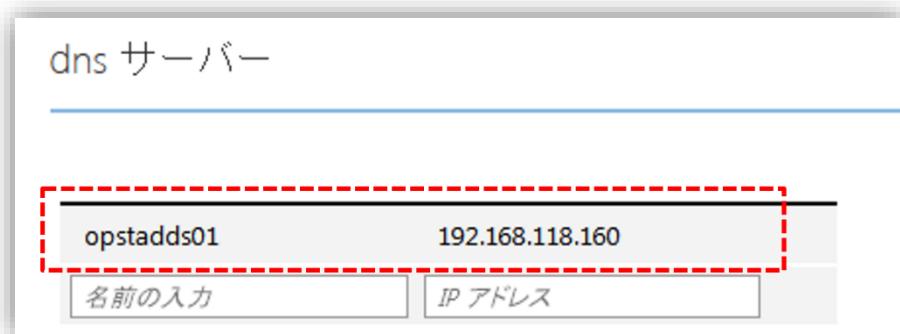
[はい] をクリック後、以下のように更新中のメッセージが表示されます。 更新が完了するまで待ちます。



12. 更新が完了すると、以下のようなメッセージが表示されます。



13. 設定が確定すると、DNS サーバー (AD DS) 名の左に表示されていた紫のバーが消えます。



8.2 仮想マシンの作成

各サーバーのベースとなる仮想マシンを作成します。

なお、この項の説明で出てくる項目の設定値は、「2.2 今回構築するシステム構成」の「仮想マシン」も併せてご参照ください。

1. Azure 管理ポータルにサインインします。
2. 画面左側のメニューから [仮想マシン] をクリックし、画面左下の [+新規] をクリックします。

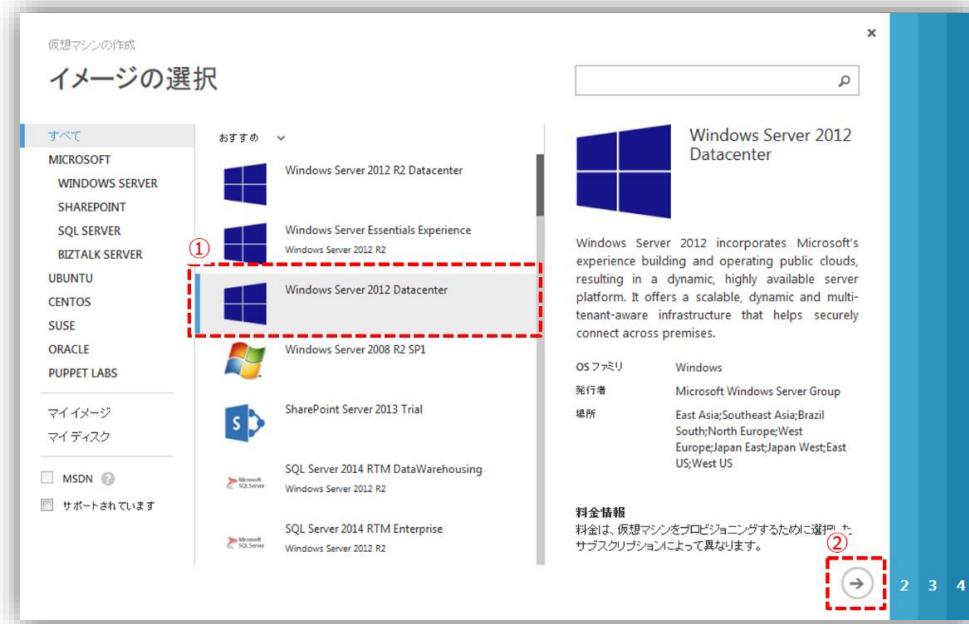


3. [コンピューティング] > [仮想マシン] > [ギャラリーから] の順にクリックします。

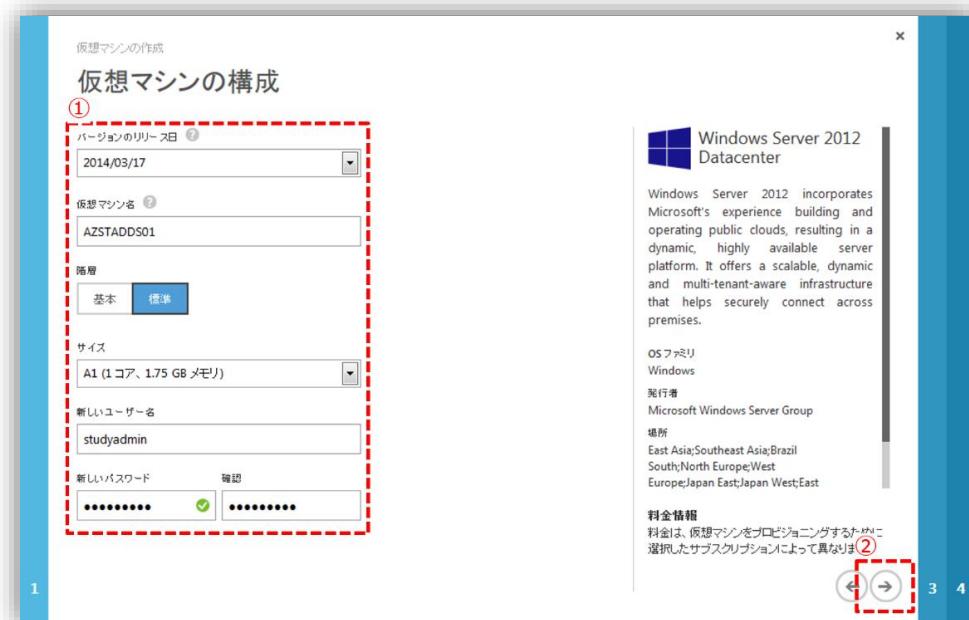


4. [仮想マシンの作成] ウィザードが表示されます。以下、ウィザードに従って操作していきます。

[イメージの選択] ページにてインストールする OS を選択します。今回は [Windows Server 2012 Datacenter] を選択します。そして、右下の [→] をクリックします。



[仮想マシンの構成 (2 ページ目)] ページにて下の表のとおり指定して右下の [→] をクリックします。

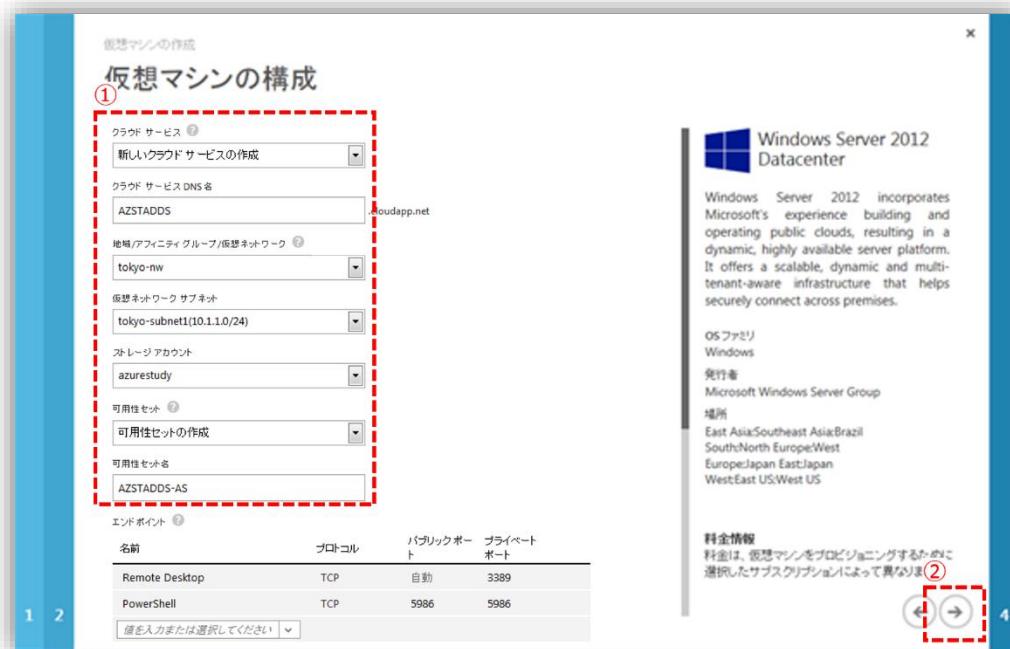


企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

項目	AD DS		ディレクトリ同期		
バージョンのリリース日	特に要件が無ければ、最新のリリース日を選択				
仮想マシン名	AZSTADDS01	AZSTADDS02	AZSTDIRSYNC01		
階層	「標準」を選択				
サイズ	A1 (1 コア、1.75 GB メモリ)	A2 (2 コア、3.5 GB メモリ)			
新しいユーザー名	studyadmin				
新しいパスワード / 確認	studyP@ss				

項目	AD FS		AD FS Proxy	
バージョンのリリース日	特に要件が無ければ、最新のリリース日を選択			
仮想マシン名	AZSTADFS01	AZSTADFS02	AZSTPROXY01	AZSTPROXY02
階層	「標準」を選択			
サイズ	A1 (1 コア、1.75 GB メモリ)			
新しいユーザー名	studyadmin			
新しいパスワード / 確認	studyP@ss			

[仮想マシンの構成 (3 ページ目)] ページにて下の表のとおり指定して右下の [→] をクリックします。



Microsoft Azure 自習書シリーズ No.6
企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

項目	AD DS		ディレクトリ同期
(仮想マシン名)	(AZSTADDS01)	(AZSTADDS02)	(AZSTDIRSYNC01)
クラウド サービス	「新しいクラウド サービスの作成」を選択	「AZSTADDS」を選択	「新しいクラウド サービスの作成」を選択
クラウド サービス DNS	「AZSTADDS」を入力	N/A	「AZSTDIRSYNC」を入力
地域/アフィニティ グループ/仮想ネットワーク	「tokyo-nw」を選択 ※「STEP 6. VPN 接続の設定」で作成した仮想ネットワーク		
仮想ネットワーク サブネット	「tokyo-Subnet1」を入力 ※「STEP 6. VPN 接続の設定」で作成したサブネット		
ストレージ アカウント	「azurestudy」を選択 ※「STEP 7. ストレージ アカウントの作成」で作成したストレージ アカウント		
可用性セット	「可用性セットの作成」を選択	「AZSTADDS-AS」を選択	「(なし)」を選択
可用性セット名	「AZSTADDS-AS」を入力	N/A	N/A

項目	AD FS		AD FS Proxy	
(仮想マシン名)	(AZSTADFS01)	(AZSTADFS02)	(AZSTPROXY01)	(AZSTPROXY02)
クラウド サービス	「新しいクラウド サービスの作成」を選択	「AZSTADFS」を選択	「新しいクラウド サービスの作成」を選択	「AZSTPROXY」を選択
クラウド サービス DNS 名	「AZSTADFS」を入力	N/A	「AZSTPROXY」を入力	N/A
地域/アフィニティ グループ/仮想ネットワーク	「tokyo-nw」を選択 ※「STEP 6. VPN 接続の設定」で作成した仮想ネットワーク			
仮想ネットワーク サブネット	「tokyo-Subnet1」を入力 ※「STEP 6. VPN 接続の設定」で作成したサブネット			
ストレージ アカウント	「azurestudy」を選択 ※「STEP 7. ストレージ アカウントの作成」で作成したストレージ アカウント			
可用性セット	「可用性セットの作成」を選択	「AZSTADFS-AS」を選択	「可用性セットの作成」を選択	「AZSTPROXY-AS」を選択
可用性セット名	「AZSTADFS-AS」を入力	N/A	「AZSTPROXY-AS」を入力	N/A

Note : エンドポイント

エンドポイントは、インターネットに対して公開するサービス（ポート）と仮想マシンのサービス（ポート）の紐付けを設定することができます。仮想マシンを作成した後でも追加、編集、削除することができます。

なお、リモートデスクトップと PowerShell のエンドポイントについてはセキュリティ対策の一環として、不要な場合はこれらを削除しておくことをお勧めします。

企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

[仮想マシンの構成 (4 ページ目)] ページにて [VM エージェントのインストール] チェックボックスにチェックを付けて右下の [チェック] をクリックします。



5. 仮想マシンが作成されると [状態] が [実行中] になります。

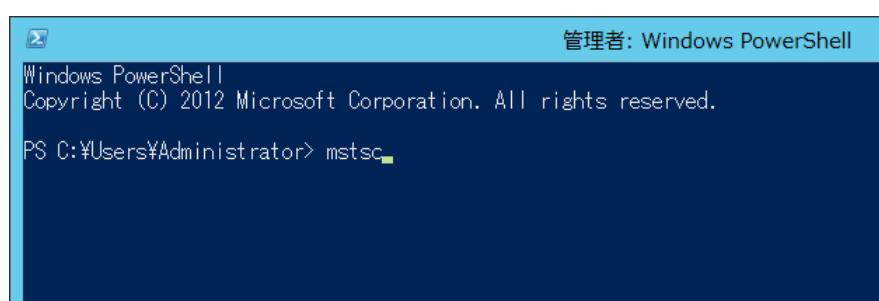


8.3 仮想マシンへのリモートデスクトップ接続

オンプレミス上の端末から作成した仮想マシンにリモートデスクトップを使って接続します。Azure で作成した仮想マシンはデフォルトでリモートデスクトップ接続が有効になっています。

- [PowerShell] もしくは [コマンド プロンプト] を起動し、以下のコマンドを入力し、[Enter] キーを押下します。

```
mstsc
```



- [リモート デスクトップ接続] 画面が開きます。[コンピューター] に対象の仮想マシンの内部 IP アドレスを入力して [接続] ボタンをクリックします。



Note : 仮想マシンの IP アドレスは DHCP で払い出される

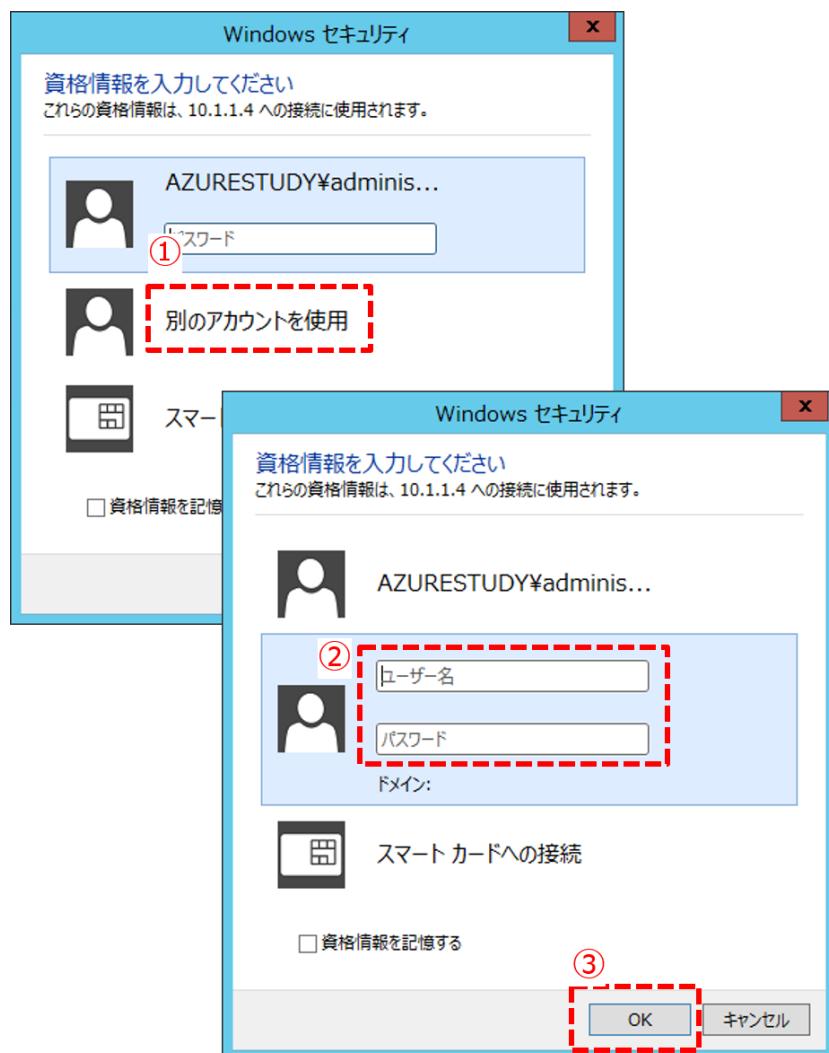
Azure 上の仮想マシンには基本的に DHCP で払い出されます。

```
IPv4 Address . . . . . : 10.1.1.4 (Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained . . . . . : 2014-04-02 22:10:56:05
Lease Expires . . . . . : 2150-05-02 17:34:03
Default Gateway . . . . . : 10.1.1.1
DHCP Server . . . . . : 168.63.129.16
DHCPv6 IAID . . . . . : 251663709
DHCPv6 Client DUID . . . . . : 00-01-00-01-1A-E6-85-B8-00-15-5D-90-40-C8
DNS Server's . . . . . : 10.1.1.4
```

また、IP アドレスが分からなくなつた場合には、Azure 管理ポータルから [仮想マシン] > 「対象の仮想マシン名」をクリック > [ダッシュボード] の右側にある [概要] でも確認できます。

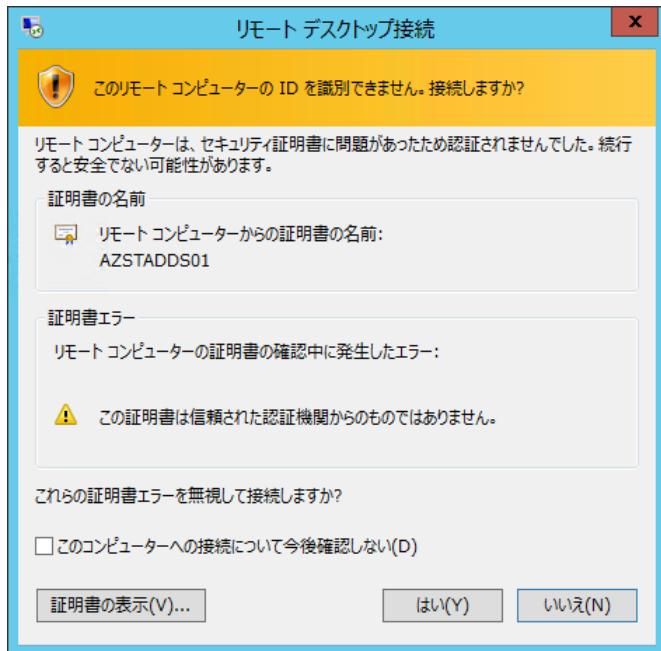
内部 IP アドレス
10.1.1.4

- [別のアカウントを使用] をクリックし、[ユーザー名] に「studyadmin」を入力、[パスワード] に「studyP@ss」を入力し、[OK] ボタンをクリックします。

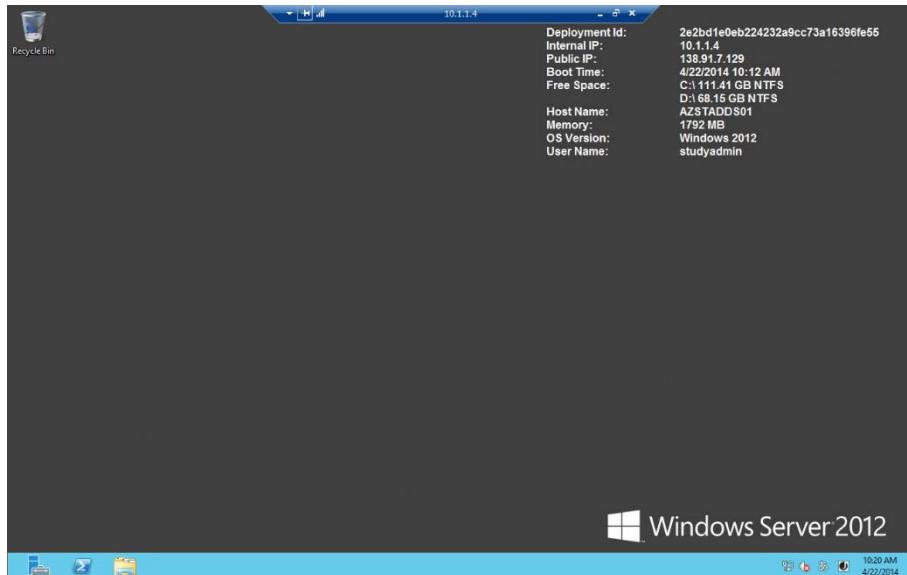


Microsoft Azure 自習書シリーズ No.6
企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

4. セキュリティ証明書の確認エラーが表示される場合は [はい] ボタンをクリックします。



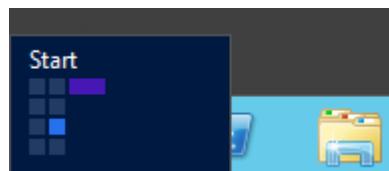
5. 仮想マシンに接続されます。



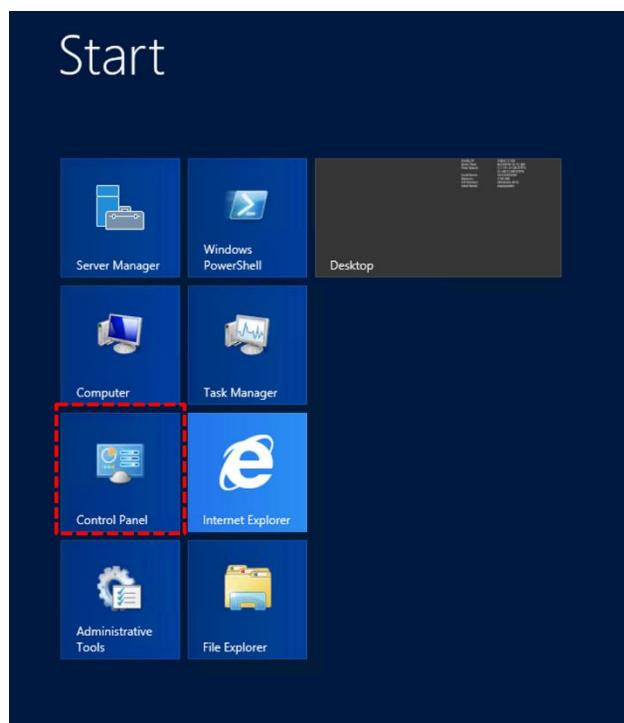
8.4 日本語化

Azure で作成される仮想マシンの言語は既定で英語になっているため日本語化を行います。以下の手順は各仮想マシンで実施します。

1. デスクトップ画面左下にマウスカーソルを移動し、[Start] を表示させてそれをクリックします（[Windows] キー押下でも可）。

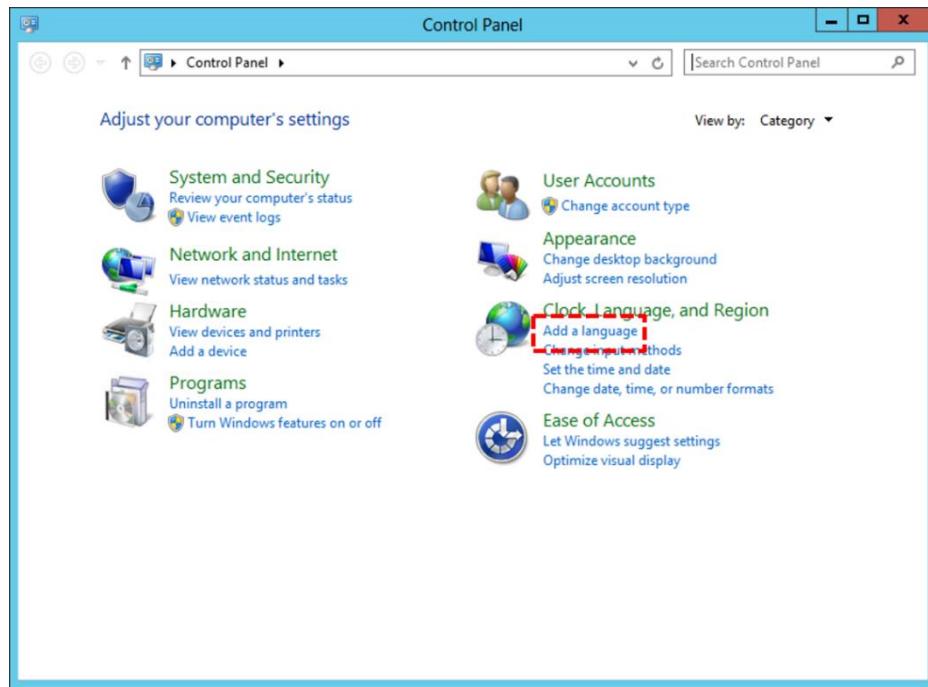


2. スタート画面にて [Control Panel] タイルをクリックします。

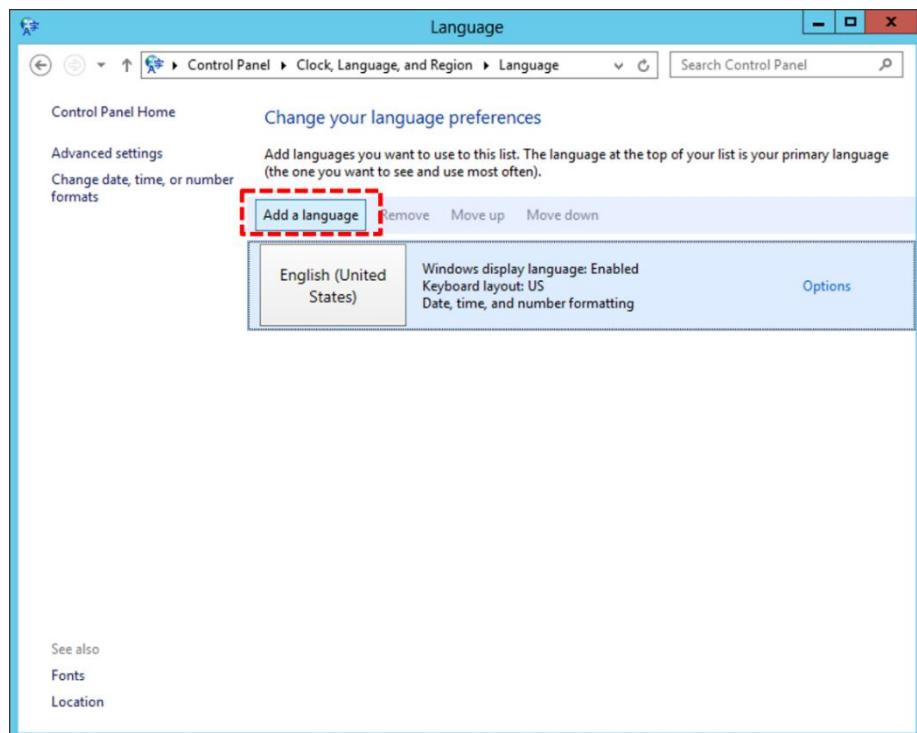


企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

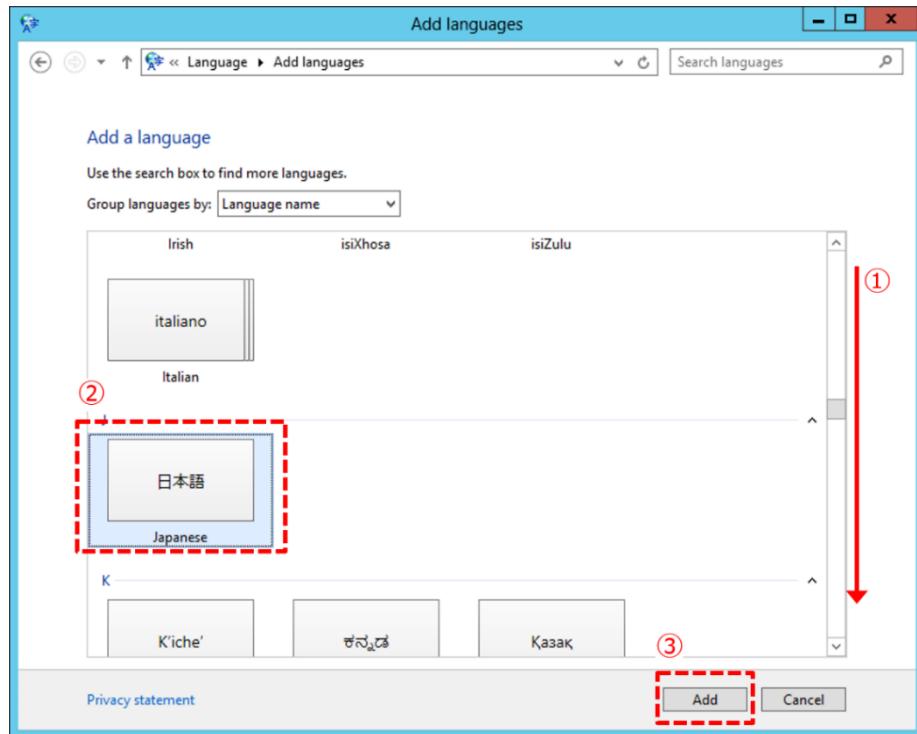
3. [Control Panel] 画面が開きます。[Clock, Language, and Region] にある [Add a language] をクリックします。



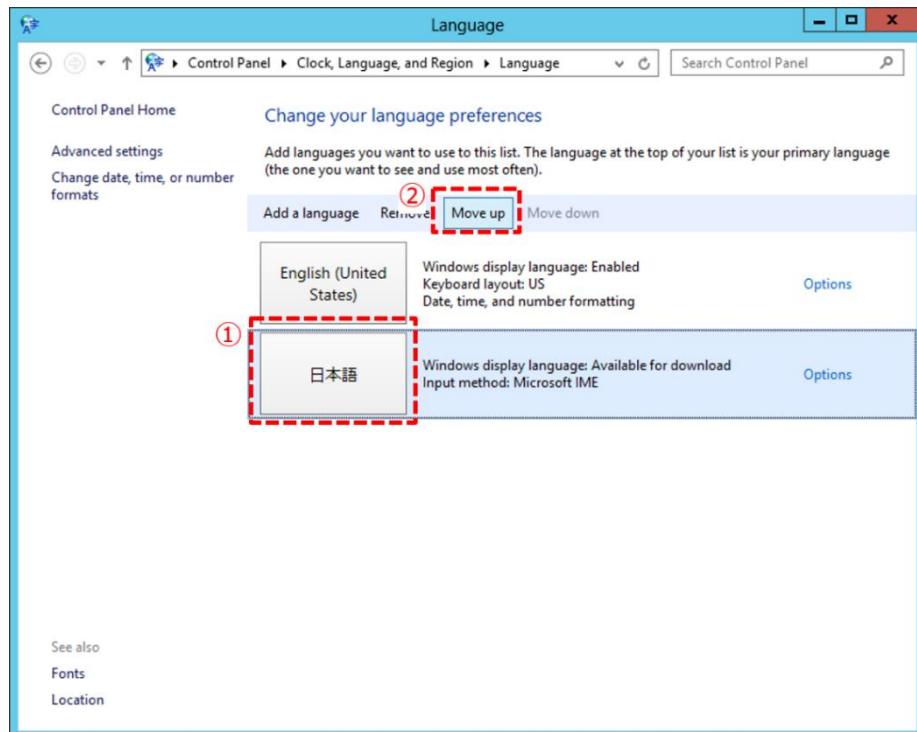
4. [Language] 画面が開きます。[Add a language] をクリックします。



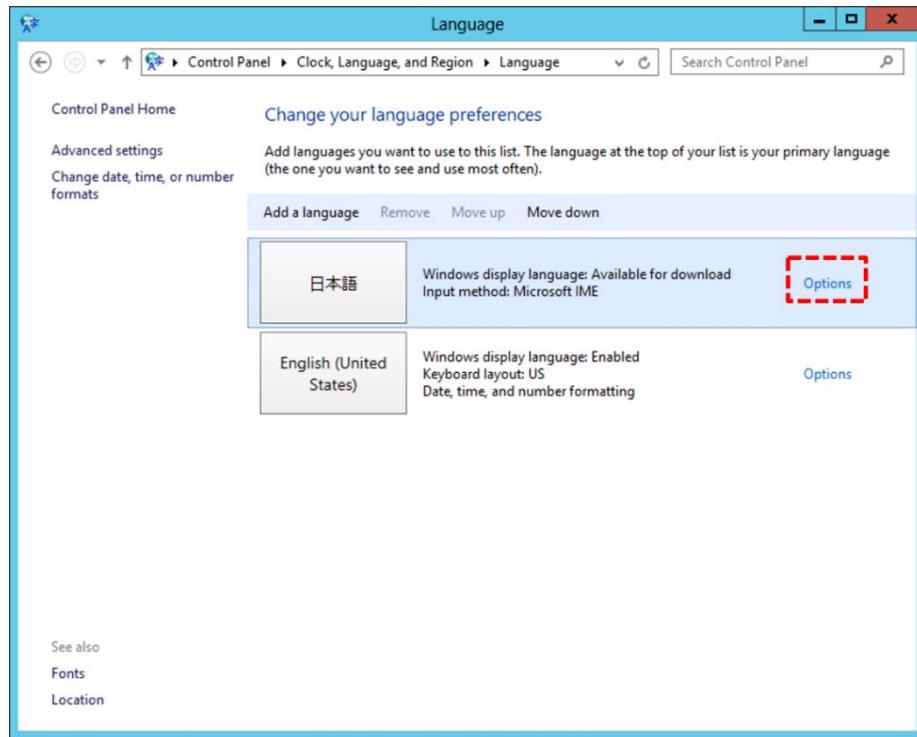
5. [Add language] 画面の右のスクロールバーを下にスクロールし、[日本語] を選択して [Add] をクリックします。



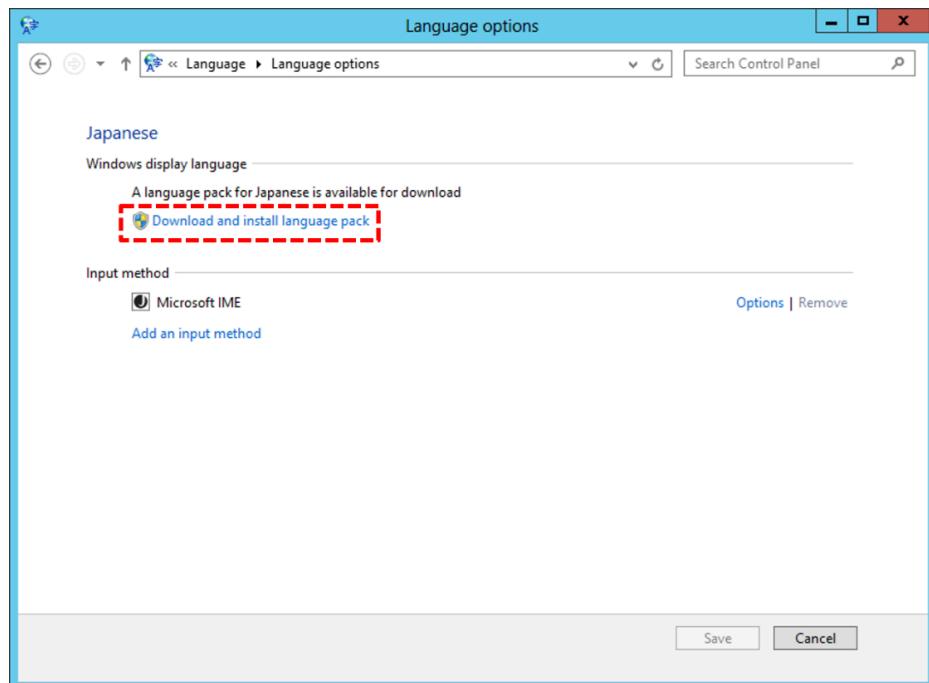
6. [Language] 画面に戻り、[日本語] を選択して [Move up] をクリックします。



7. [日本語] の [Options] をクリックします。

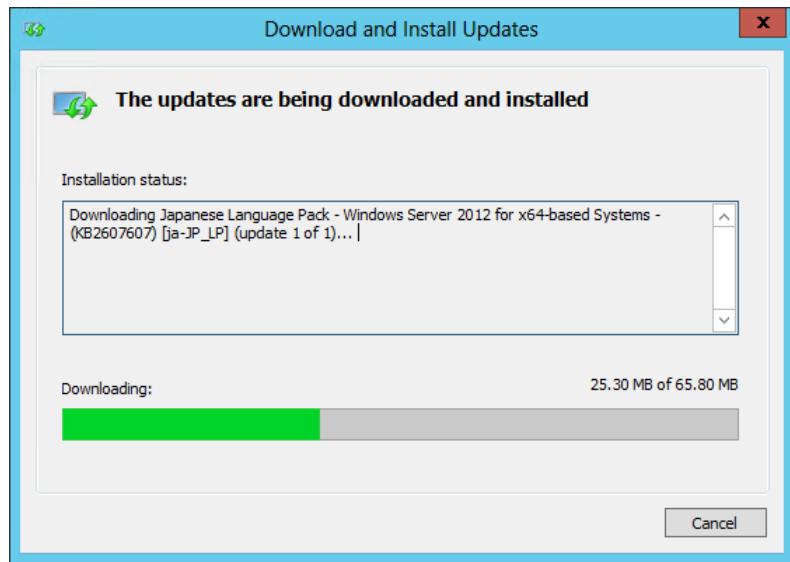


8. [Language options] 画面が開きます。[Download and install language pack] をクリックします。

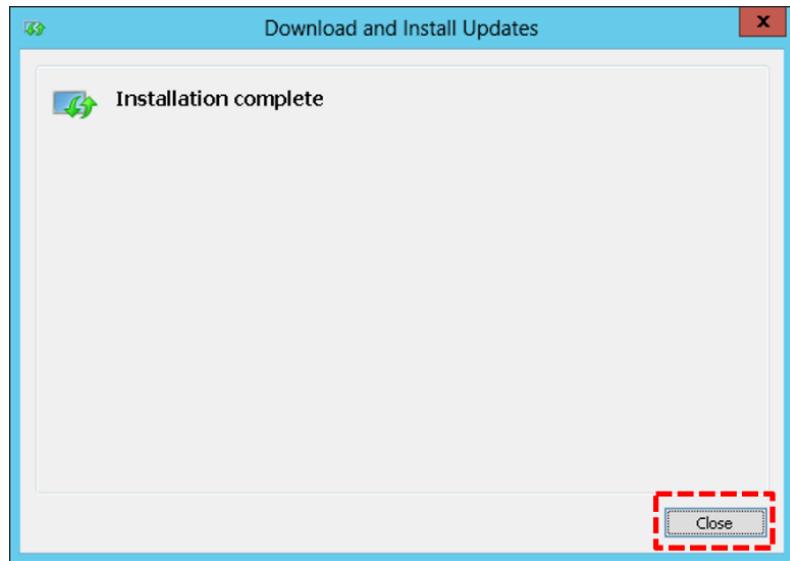


企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

9. [Download and Install Updates] 画面が開いてインストールが介します。 インストールが完了するまで待ちます。 環境にもよりますが、30 分程度かかります。



10. [Installation complete] 画面が表示されたら、[Close] ボタンをクリックします。



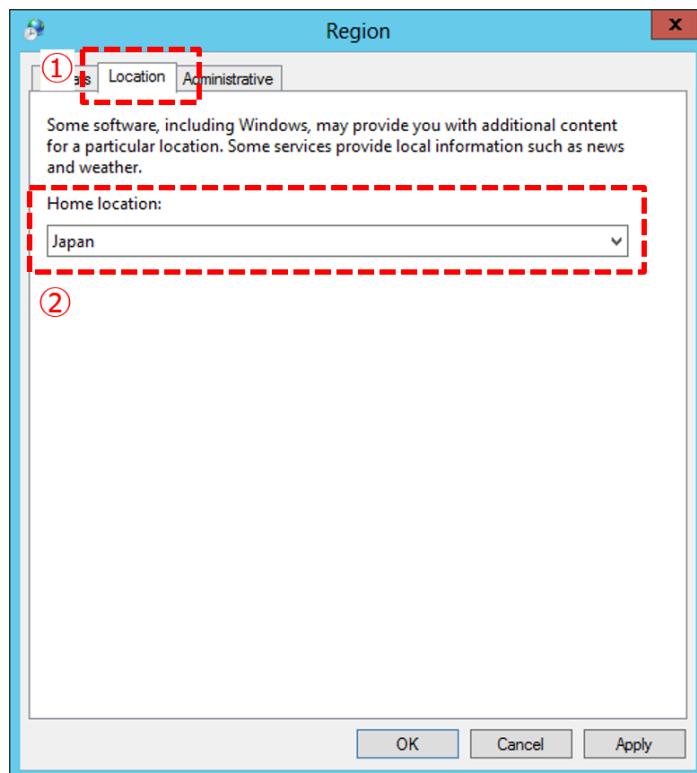
企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

11. 次に、場所 (Location) を変更し、サインイン画面の日本語化や PowerShell やコマンド プロンプトで日本語が使えるように設定を変更します。

[Language] 画面に戻り左下の [Location] をクリックします。

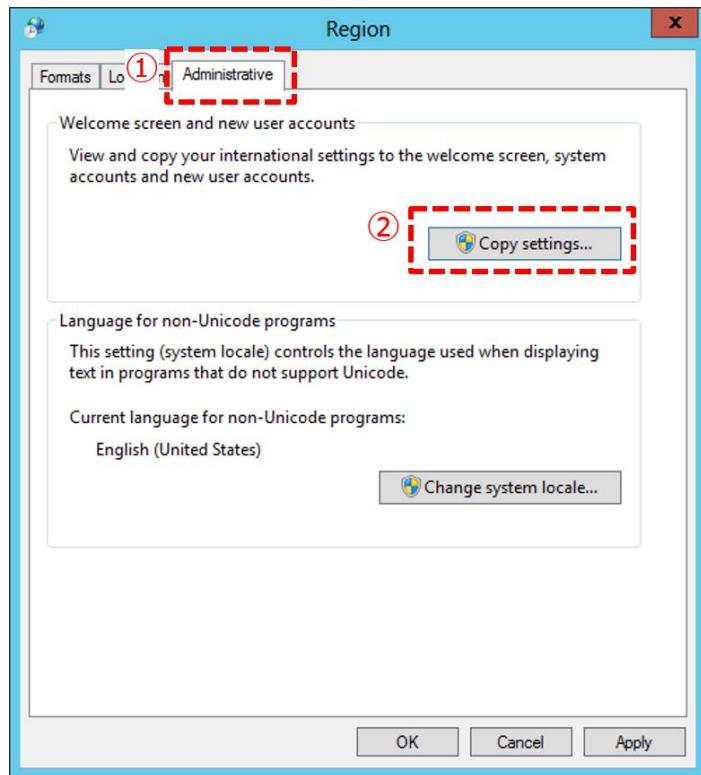


12. [Region] 画面が開きます。[Location] タブを開き、[Home location] で「Japan」を選択します。

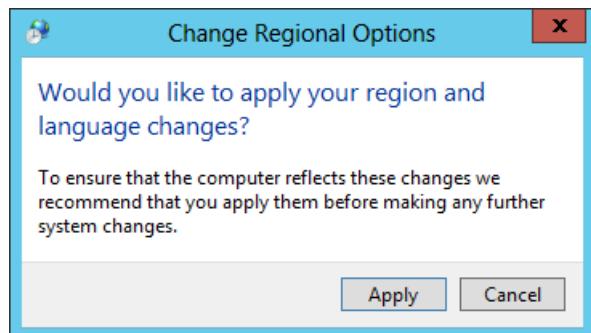


企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

13. [Region] 画面にて [Administrative] タブを開き、[Copy settings] ボタンをクリックします。

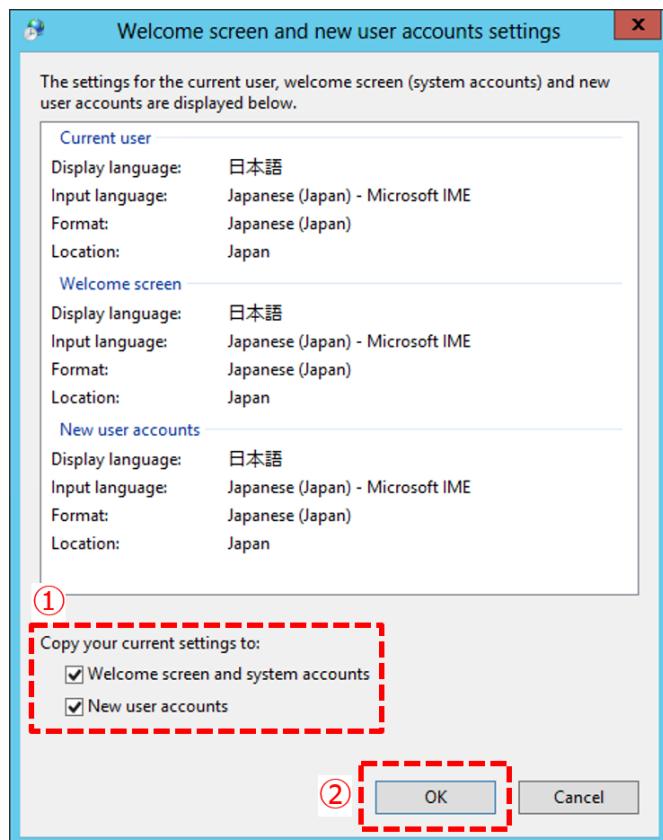
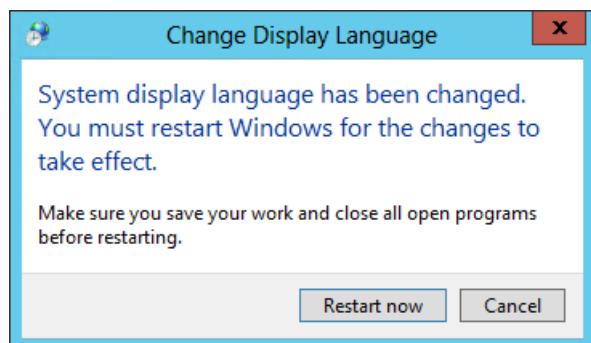


14. 場所と言語の変更を適用するか確認のウィンドウが開きます。 [Apply] ボタンをクリックします。

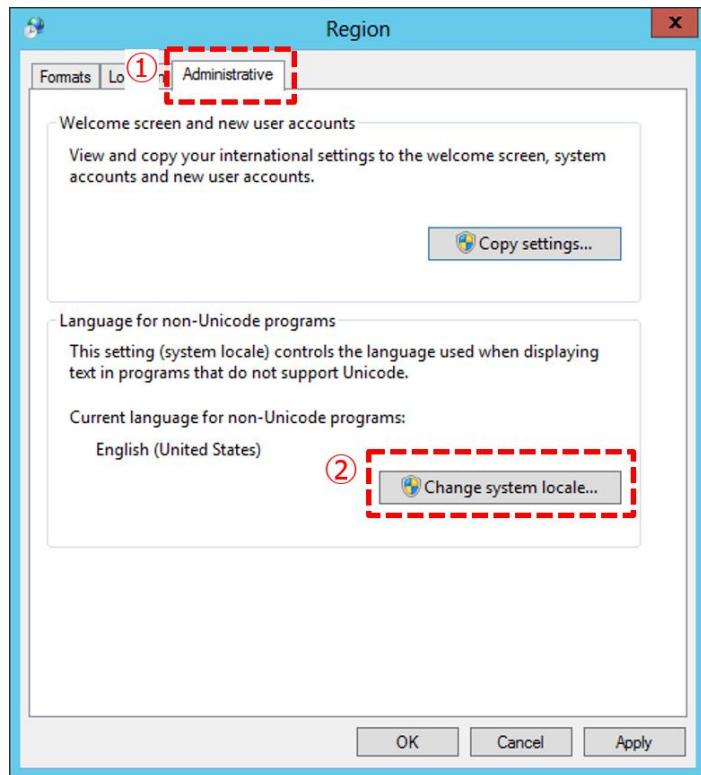


15. [Welcome screen and new user accounts settings] 画面が開きます。

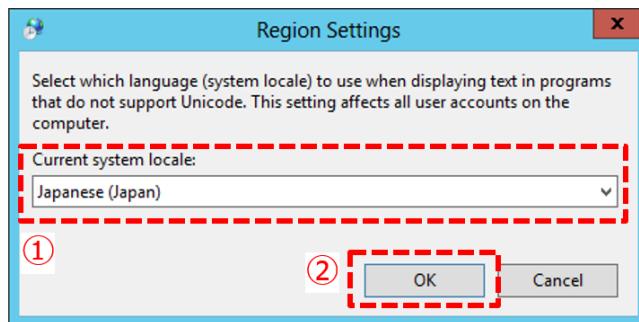
画面下部の [Welcome screen and system accounts (「ようこそ画面」の日本語化)]、[New user accounts (ユーザー追加時のデフォルト言語 (および場所) の日本語化)] チェックボックスにチェックを付けて [OK] ボタンをクリックします。

**16.** OS 再起動を薦めるウィンドウが開きますが、続けて作業を行うため [Cancel] ボタンをクリックします。

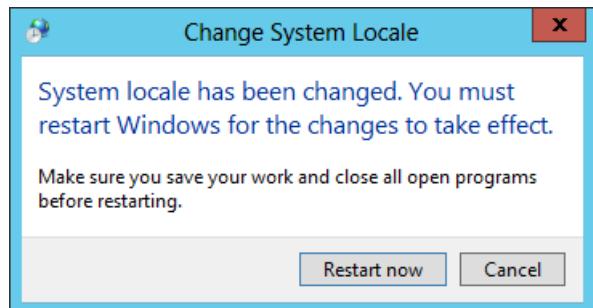
17. [Region] 画面に戻って [Administrative] タブを開き、[Change system locate] ボタンをクリックします。



18. [Region Settings] 画面が開きます。 [Current system locale] で「Japanese (Japan)」を選択して [OK] ボタンをクリックします。



19. OS 再起動を薦めるウィンドウが開きます。[Restart now] ボタンをクリックして OS を再起動します。



20. 再起動後、対象の仮想マシンにサインインしなおすと、日本語が適用されます。



8.5 タイムゾーン

既定では世界標準時 (UTC) となっているためこれを日本標準時に変更します。

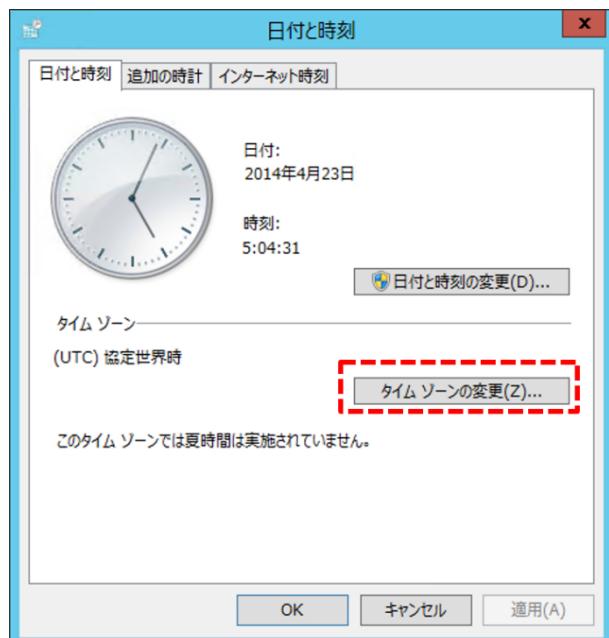
1. デスクトップ画面右下の時計をクリックします。



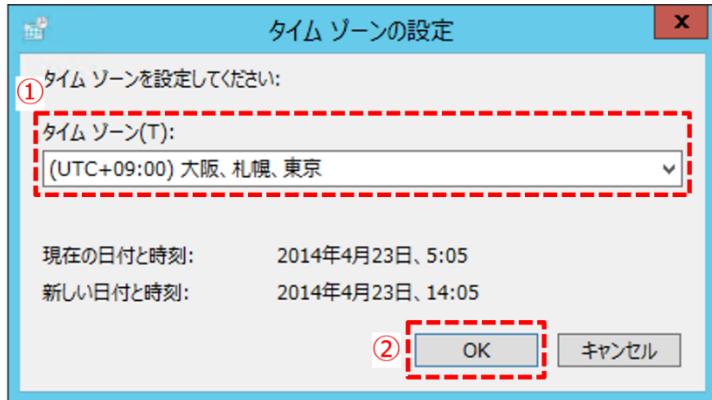
2. [日付と時刻の設定の変更] をクリックします。



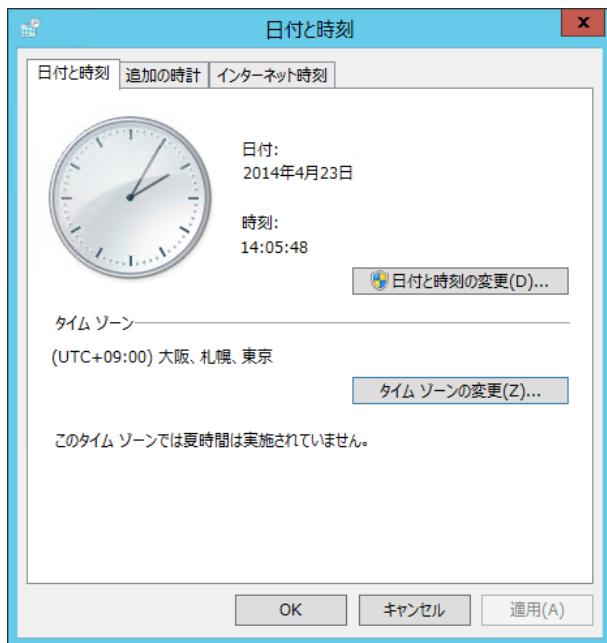
3. [日付と時刻] 画面にて [タイムゾーンの変更] ボタンをクリックします。



4. [タイム ゾーンの設定] 画面にて [タイム ゾーン] から「(UTC+09:00) 大阪、札幌、東京」を選択して [OK] ボタンをクリックします。



5. [日付と時刻] 画面に戻り、タイムゾーンが変更されたことを確認して [OK] ボタンをクリックして閉じます。



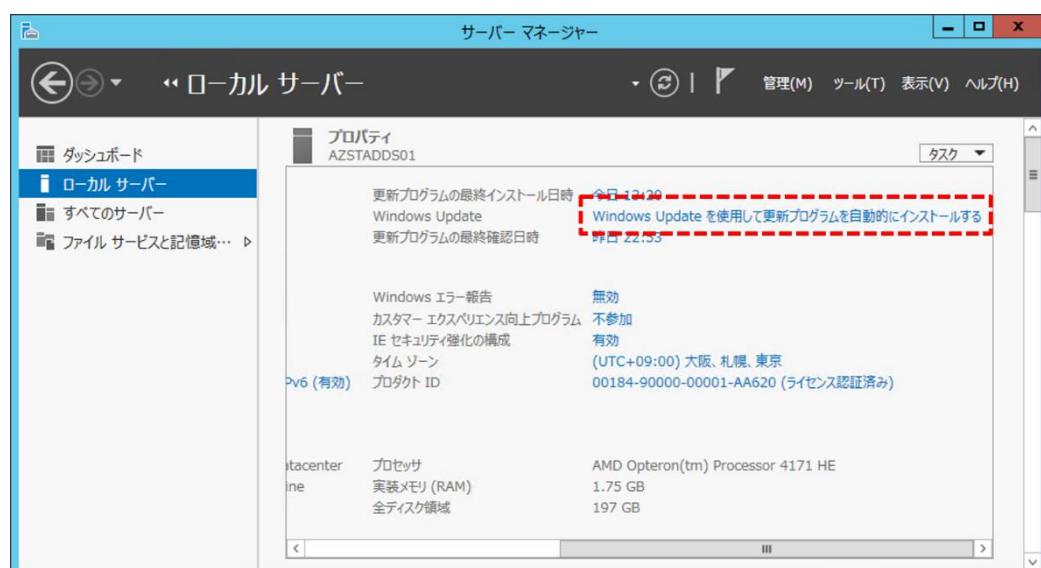
8.6 Windows Update の設定

Windows Update を行い、サーバーを最新の状態にします。また、Windows Update が自動で実行されないように設定します。これは、Windows Update 後の自動再起動を抑止するとともに、アップデート適用の管理を管理者にて意識的に行うようにするためとなります。

1. [サーバー マネージャー] を開きます。
2. 画面左側の [ローカル サーバー] をクリックします。

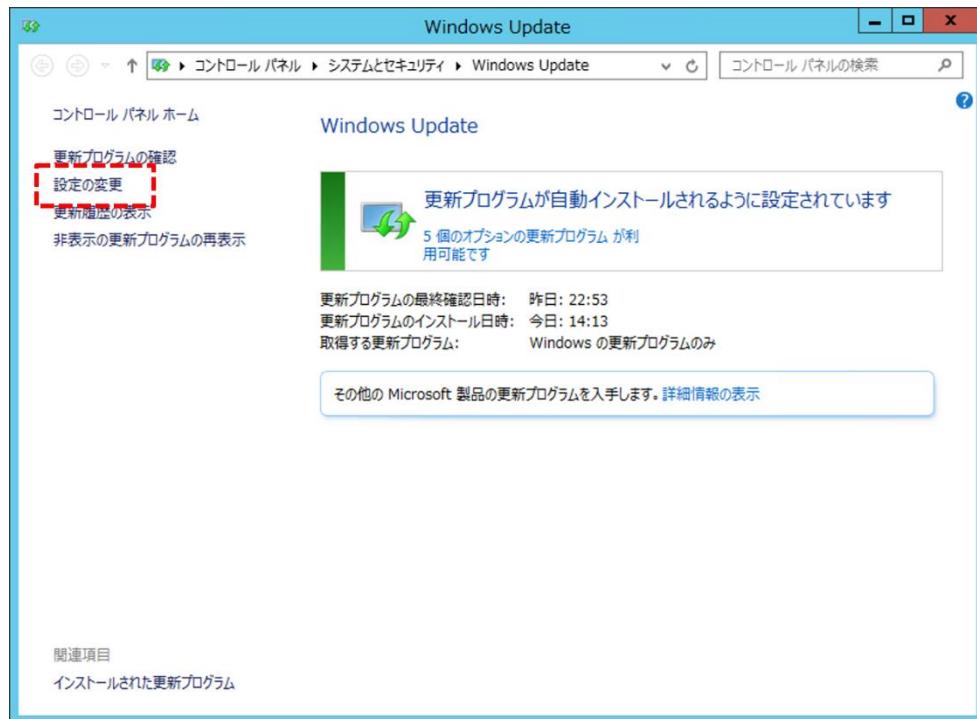


3. 画面をスクロールし、[Windows Update を使用して更新プログラムを自動的にインストールする] をクリックします。

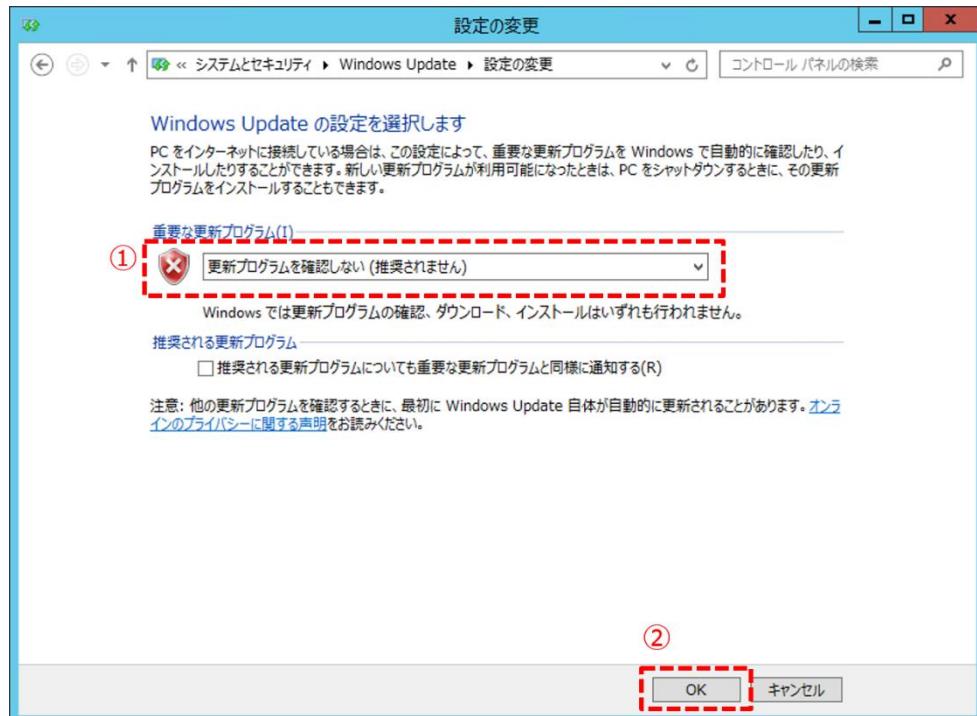


企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

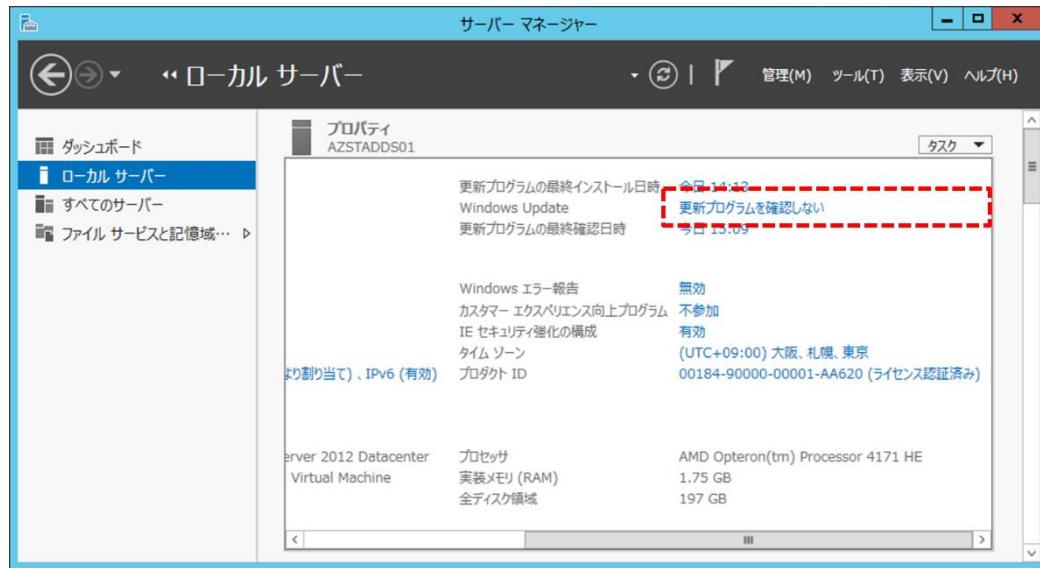
4. 更新プログラムがある場合にはインストールおよび OS 再起動後に、更新プログラムが特にない場合には [設定の変更] をクリックします。



5. [重要な更新プログラム] から「更新プログラムを確認しない (推奨されません)」を選択し、[OK] ボタンをクリックします。



6. [更新プログラムを確認しない] になっていることを確認します。



Note : Windows Update について

なお、章の始めにも記載したとおり、この設定は Windows Update を行わないことを推奨するものではなく、意図しない再起動を抑止するための設定となります。サービスとして本運用を行う際には適宜アップデートを行うよう運用設計を行ってください。

8.7 ディスクの追加

Note : ディスクを追加する仮想マシン

この作業を行う仮想マシンは以下のとおりです。

- AD DS サーバー ([AZSTADDS01]、[AZSTADDS02])
- ディレクトリ同期サーバー ([AZSTDIRSYNC01])

◆ Azure 管理ポータルでの作業

1. Azure 管理ポータルにサインインします。
2. 画面左側のメニューから [仮想マシン] をクリックして対象の仮想マシンを選択します。



3. 画面下部の [ディスクの接続] をクリックして [空のディスクの接続] をクリックします。



4. [サイズ (GB)] に「1023」を入力し、[ホスト キャッシュ機能] が「なし」になっていることを確認して右下の [チェック] をクリックします。



Note : ディスクのサイズについて

AD DS サーバーに追加するディスクのサイズは、1023 GB とします。

ディレクトリ同期サーバーに追加するディスクのサイズは、「2.4 各サーバーの役割／構成／前提条件」の「ディレクトリ同期の構成／前提条件」を参考に指定します。

5. ディスクの作成と追加が始まると対象の仮想マシンの状態が [実行中 (更新中)] になります。

追加が完了すると [実行中] になります。



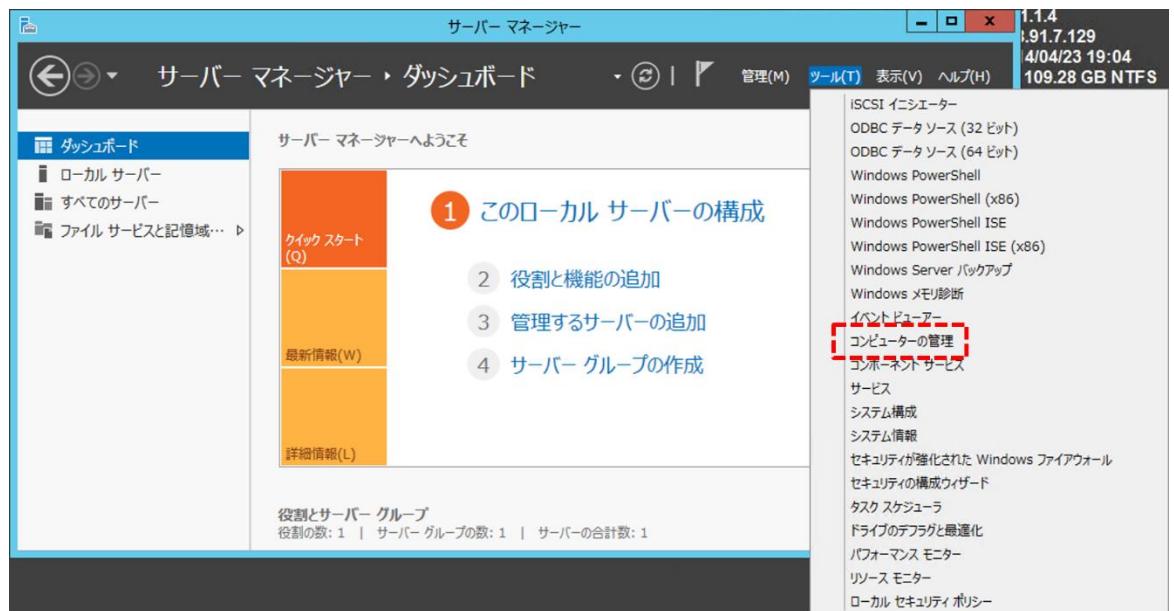
◆ 仮想マシンで追加したディスクのフォーマット

Azure 管理ポータルで追加しただけでは使用できません。 追加したディスクを仮想マシン上でフォーマットし、仮想マシンで利用できるようにします。

6. ローカル管理者アカウントで対象の仮想マシンにサインインします。

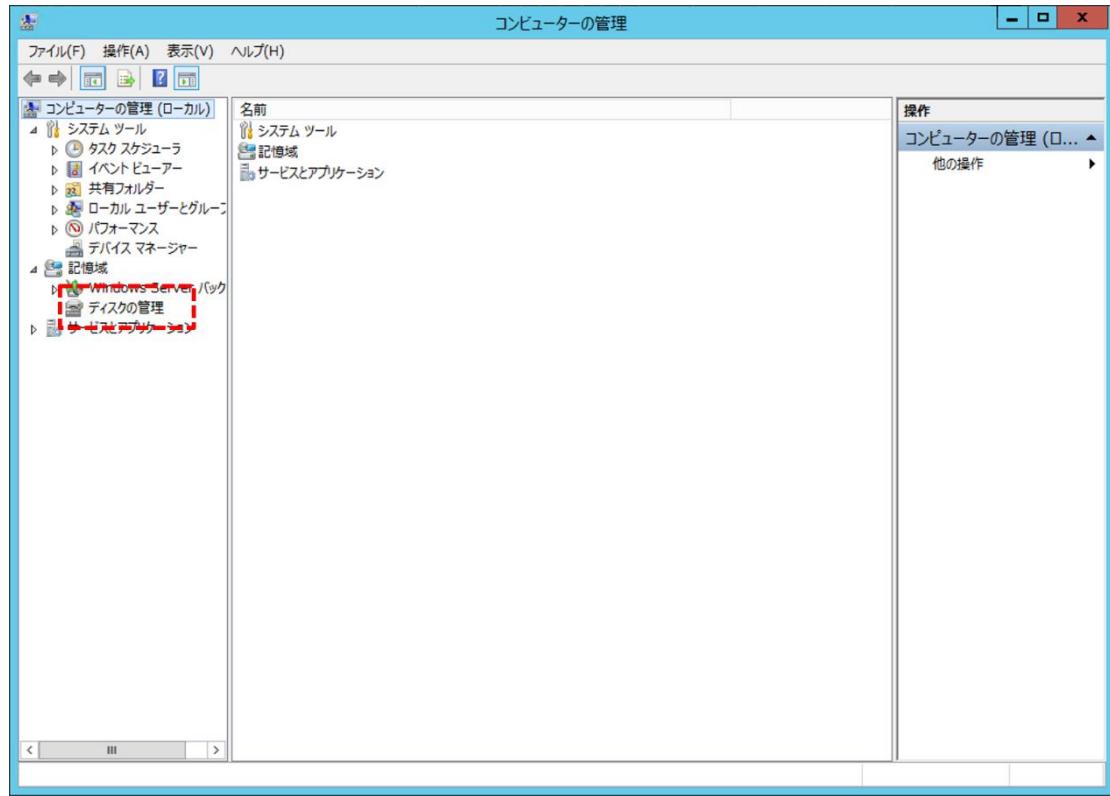
7. [サーバー マネージャー] を開きます。

8. [ツール] メニュー > [コンピューターの管理] をクリックします。



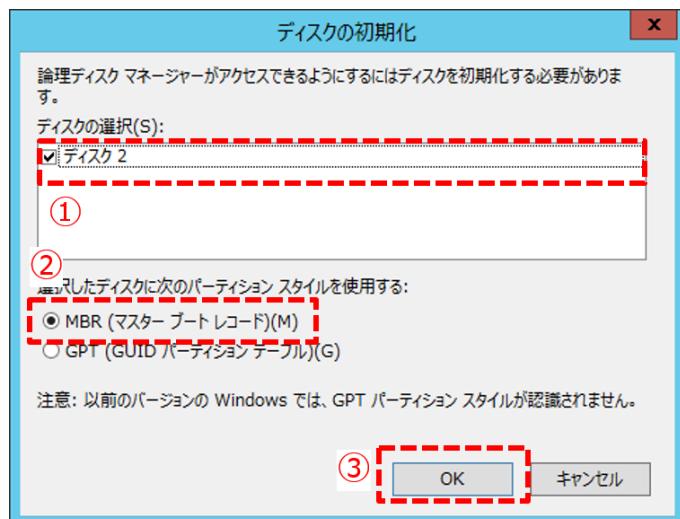
企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

9. 左ペインから [コンピューターの管理 (ローカル)] > [記憶域] > [ディスクの管理] をクリックします。

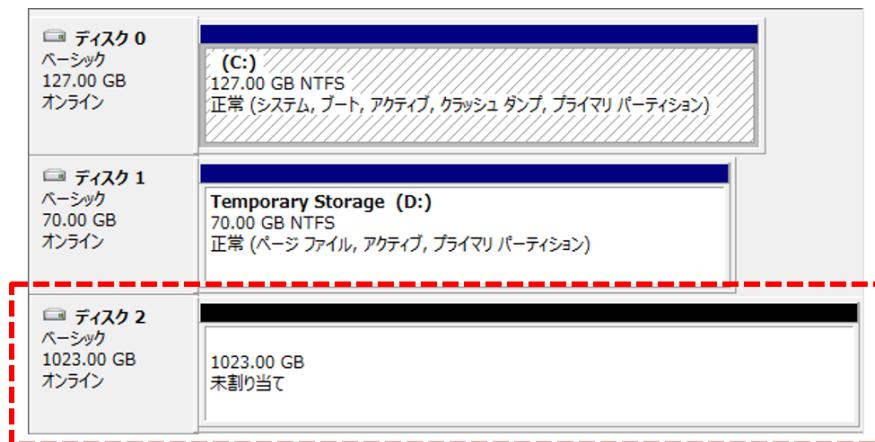


10. [ディスクの初期化] 画面が開きます。[ディスク 2] にチェックが付いていることを確認します。

[MBR] (任意のスタイル) を選択して [OK] ボタンをクリックします。



11. 追加したディスクが認識されていることを確認します。



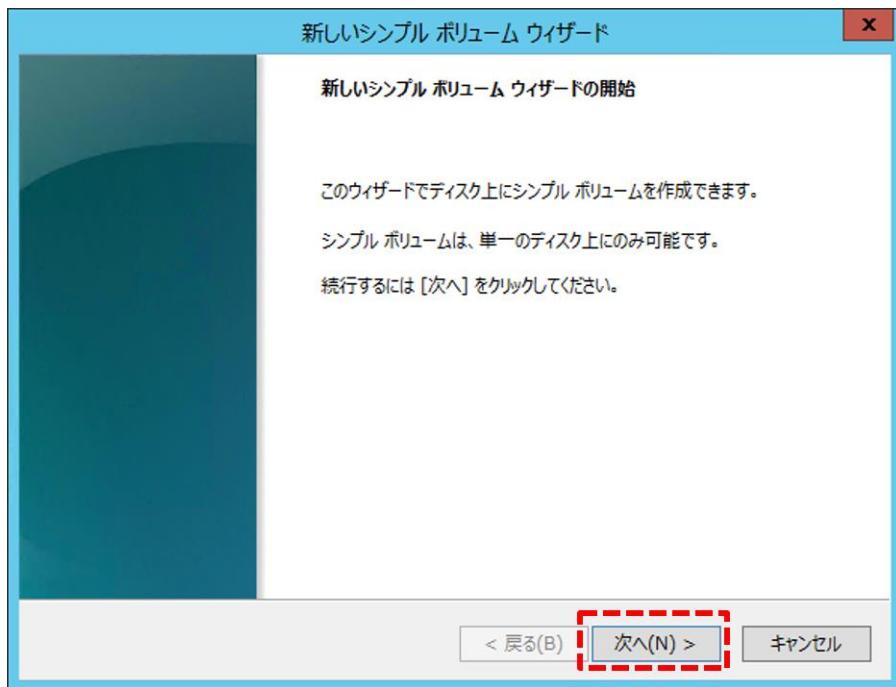
12. [未割り当て] を右クリックして [新しいシンプル ボリューム] をクリックします。



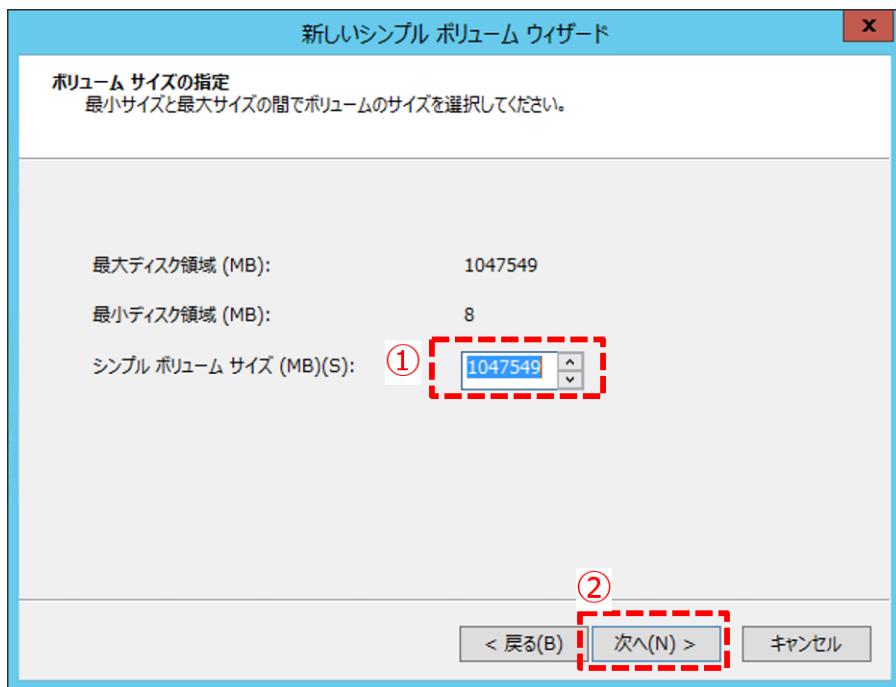
13. [新しいシンプル ボリューム ウィザード] が表示されます。以下、ウィザードに従って操作していきます。

企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

[開始] 画面にて [次へ] ボタンをクリックします。



[ボリューム サイズの指定] 画面にて [シンプル ボリューム サイズ (MB)] に最大値を入力して [次へ] ボタンをクリックします。

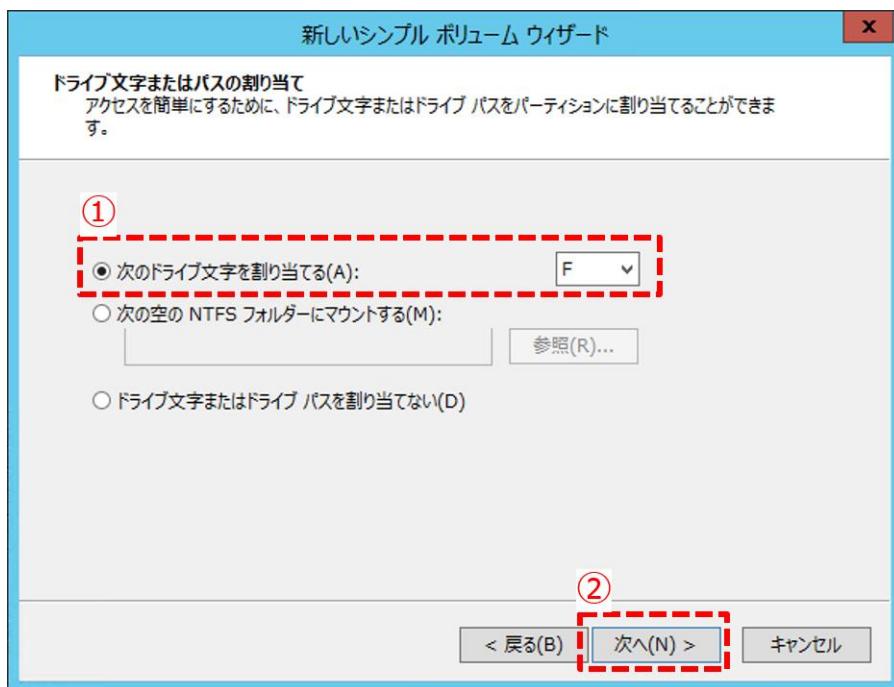


Note : ディスクのサイジング

今回は自習書ということですべての容量を割り当てています。

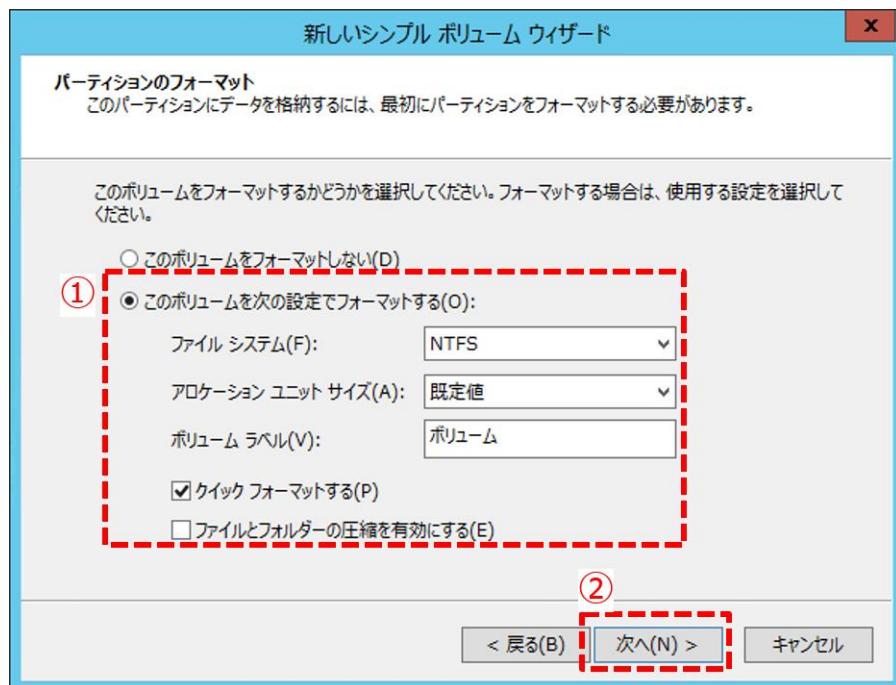
実際には AD DS のオブジェクト数などから環境に合わせた適切なサイズを割り当てるをお勧めします。

[ドライブ文字またはパスの割り当て] 画面にて [次のドライブ文字を割り当てる] チェックボックスにチェックを付け、プルダウンで [F] (任意のドライブ文字) を選択して [次へ] ボタンをクリックします。



[パーティションのフォーマット] 画面にて [このボリュームを次の設定でフォーマットする] チェックボックスにチェックを付け、[ファイル システム] に「NTFS」を選択、[アロケーション ユニット サイズ] に「既定値」を選択、[ボリューム ラベル] に「ボリューム (任意の文字列)」入力、[クイック フォーマットする] チェックボックスにチェックを付けて [次へ] ボタンをクリックします。

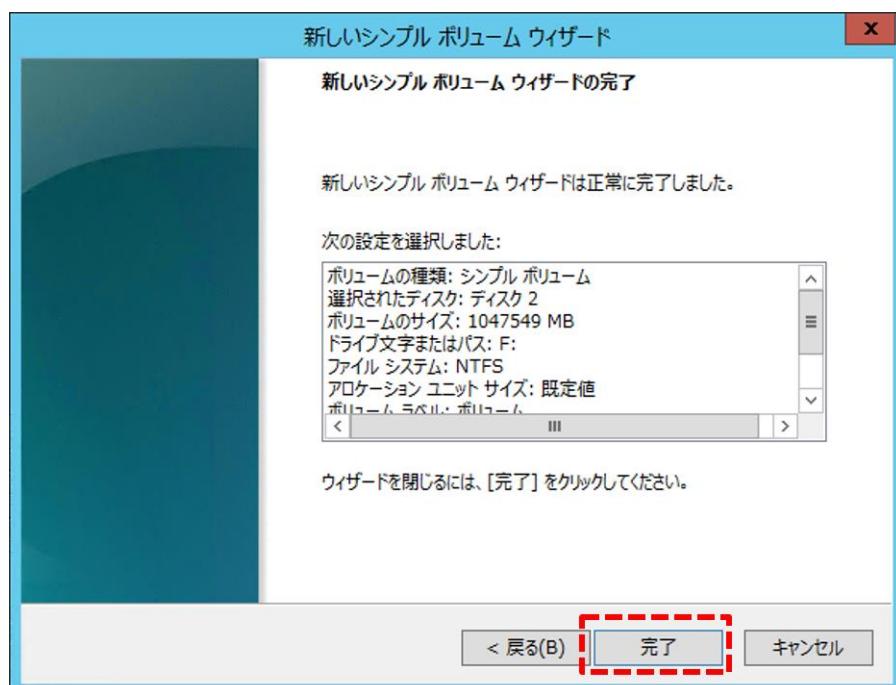
企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

**Note : クイックフォーマットする**

Azure のストレージは使用容量に応じて課金されます。

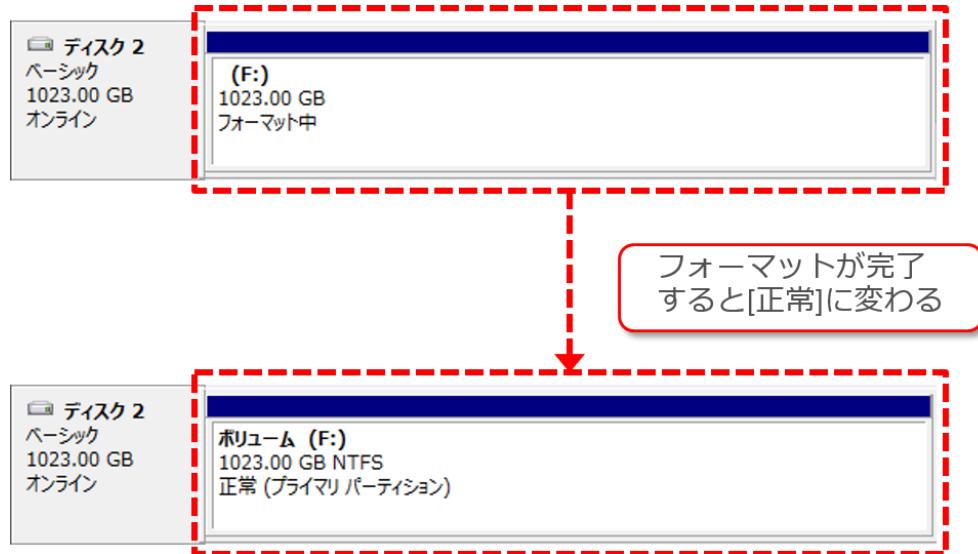
ディスクを通常フォーマットしてしまうと、ディスクのすべての領域を使用しているとみなされ、全容量（本自習書では約 1TB）分が課金対象となってしまいます。しかしながら、クイックフォーマットでフォーマットした場合は、実際のデータ量に比例した容量分のみが課金対象となります。

[完了] 画面にて [完了] ボタンをクリックします。

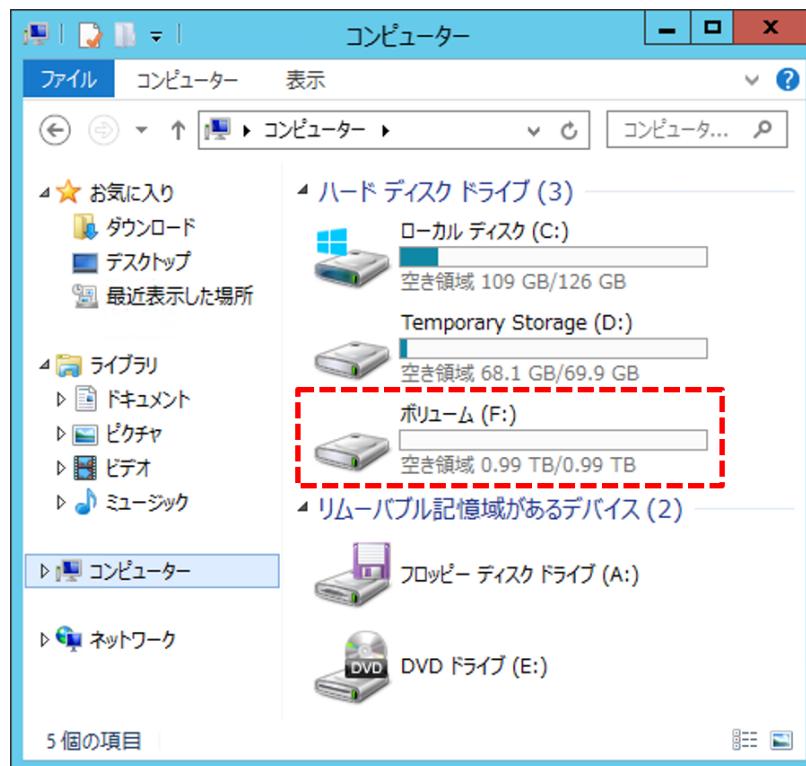


14. ディスクのフォーマットが始まると対象のディスクの状態が [フォーマット中] になります。

フォーマットが完了すると [正常] になります。



15. [コンピューター] 画面で確認すると、ディスクが追加されているのが分かります。



8.8 ドメインへの参加

各仮想マシンに該当する機能をインストールする前に、ドメインに参加させる必要があります。

Note : ドメインに参加する仮想マシン

この作業を行う仮想マシンは以下のとおりです。

- AD DS サーバー ([AZSTADDS01]、[AZSTADDS02])
- ディレクトリ同期サーバー ([AZSTDIRSYNC01])
- AD FS サーバー ([AZSTADFS01]、[AZSTADFS02])

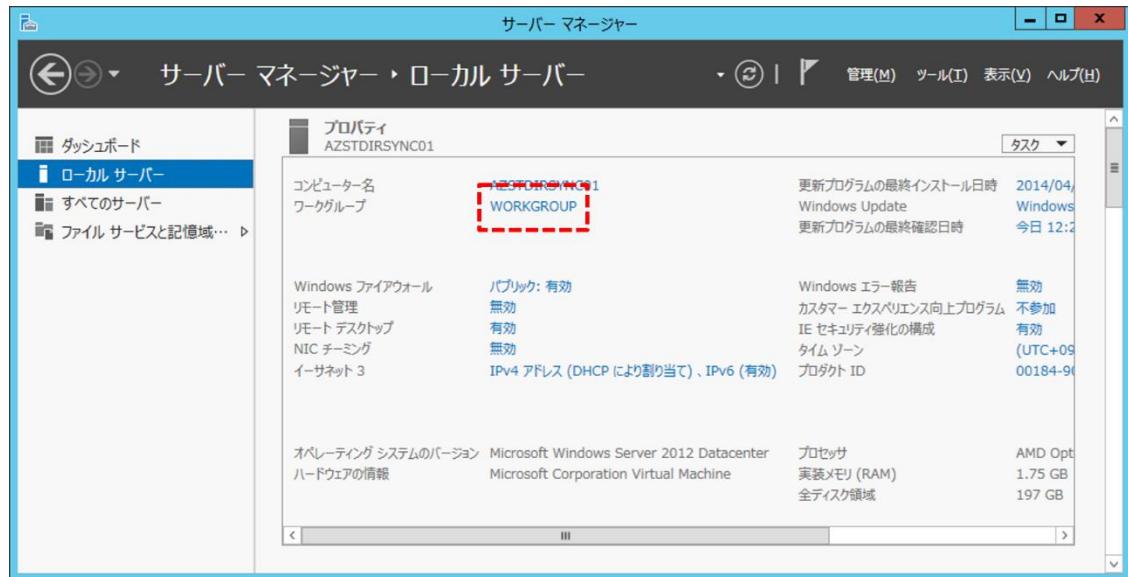
1. ローカル管理者アカウントで対象の仮想マシンにサインインし、[サーバー マネージャー] を開きます。

2. [ローカル サーバー] のプロパティを開きます。

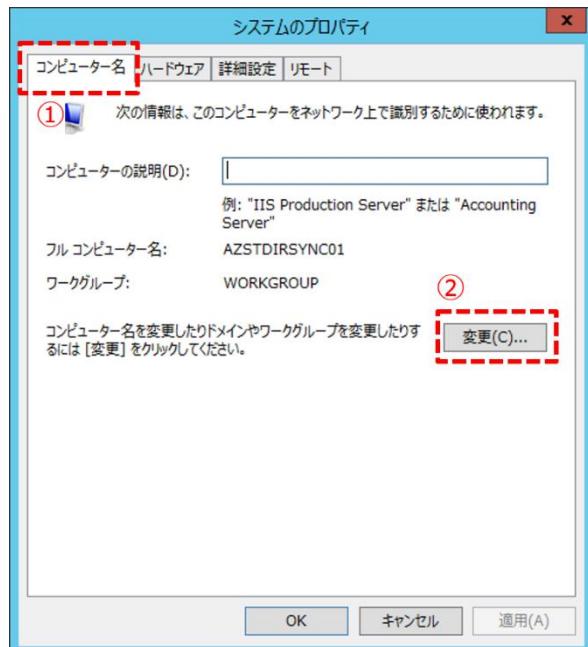


企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

3. [ワークグループ (WORKGROUP)] をクリックします。



4. [システムのプロパティ] 画面が開きます。[コンピューター名] タブの [変更] ボタンをクリックします。

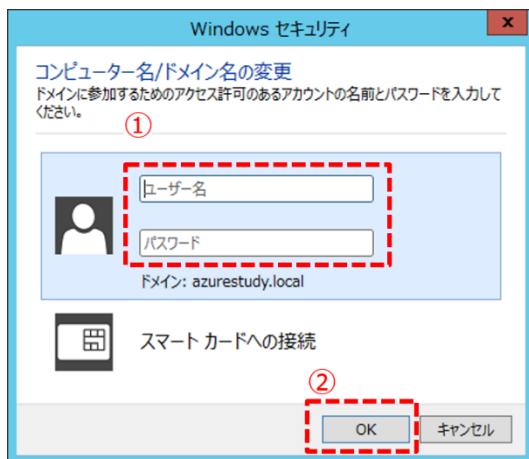


企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

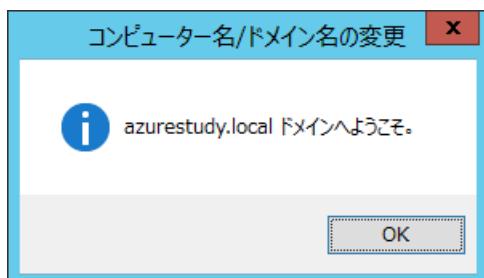
5. [コンピューター名/ドメイン名の変更] 画面が開きます。[所属するグループ] で [ドメイン] を選択して「azurestudy.local」を入力し、[OK] ボタンをクリックします。



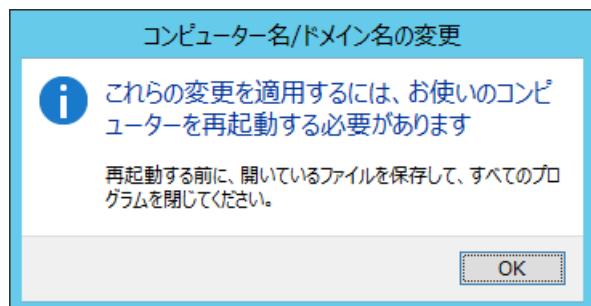
6. [Windows セキュリティ] 画面が開きます。ドメイン管理者のユーザー名、パスワードを入力して [OK] ボタンをクリックします。



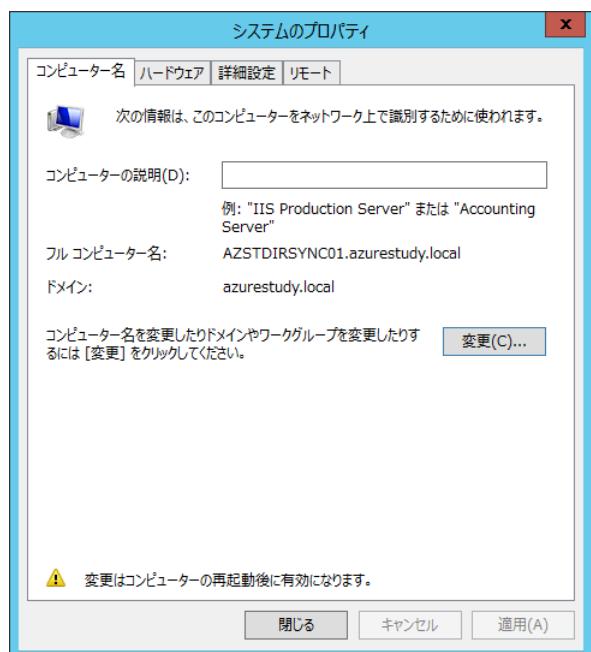
7. 手順 6 の認証が正常に終了すると、以下のメッセージ ボックスが順に表示されるので、[OK] ボタンをクリックして閉じます。



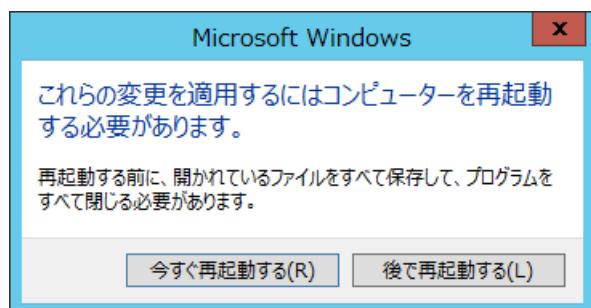
企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携



8. 手順 4 の [システムのプロパティ] 画面に戻ります。 [閉じる] ボタンをクリックして閉じます。



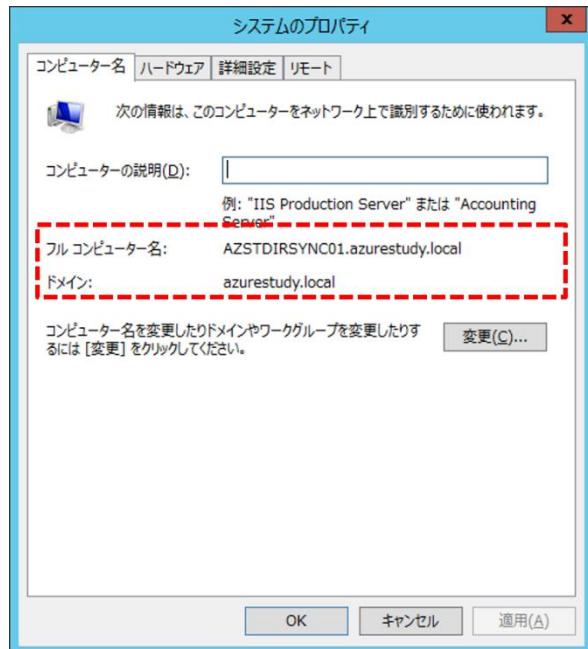
9. 以下の画面が表示されます。[今すぐ再起動する] ボタンをクリックし、OS を再起動します。



企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

10. OS 再起動後、ドメイン管理者アカウントで対象の仮想マシンにサインインし、[システムのプロパティ] を開きます。

社内ドメインに参加できていることを確認します。



STEP 9. AD DS サーバーのセットアップ、 および動作確認

この STEP では、仮想マシン上に AD DS を構築するための手順と構築が正常に完了していることを確認する方法について説明します。

Note : 2 台目以降の AD DS サーバーを構築する際の注意事項

2 台目以降の AD DS サーバーを構築する（特に以下の項の作業）は、1 台目の AD DS サーバーの構築が完了してから実施してください。

- 9.2 ドメイン コントローラへの昇格
- 9.3 サイトとサブネットの作成
- 9.4 初期レプリケートの完了

なお、「9.7 2 台目以降の AD DS を構築する際のポイント」に構築する際のポイントをまとめましたのでご覧ください。

2 台の AD DS サーバーを構築後、「9.5 仮想ネットワークへの DNS サーバーの追加設定」を実施します。

この STEP では、次のことを学習します。

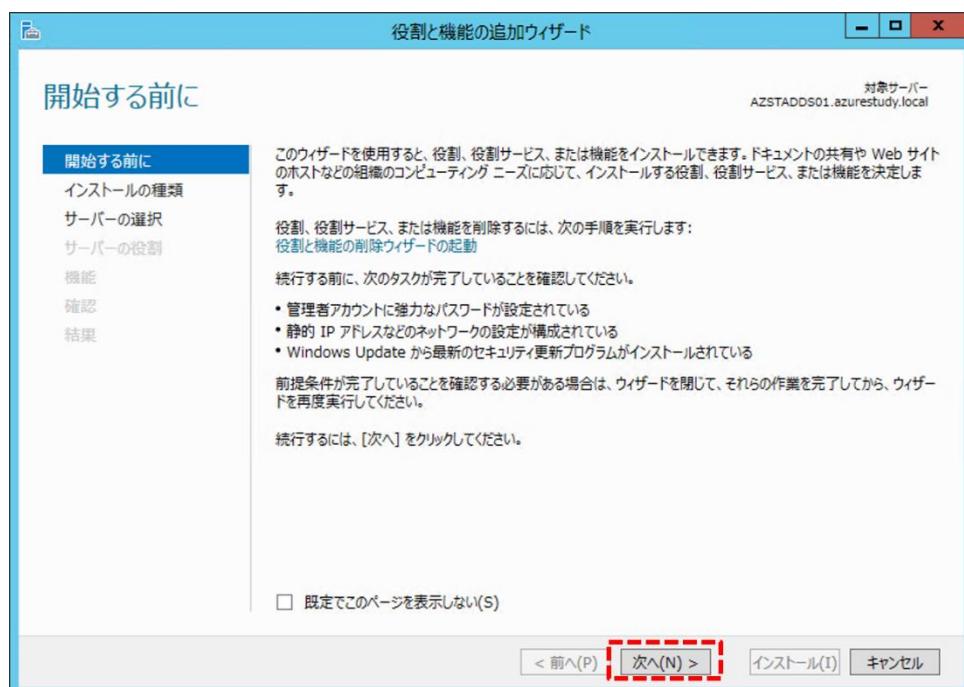
- ✓ AD DS のインストール
- ✓ ドメイン コントローラへの昇格
- ✓ サイトとサブネットの作成
- ✓ 初期レプリケートの完了
- ✓ 仮想ネットワークへの DNS サーバーの追加設定
- ✓ NTP に関する注意点（PDC エミュレーターとは同期しない）
- ✓ 2 台目以降の AD DS を構築する際のポイント

9.1 AD DS のインストール

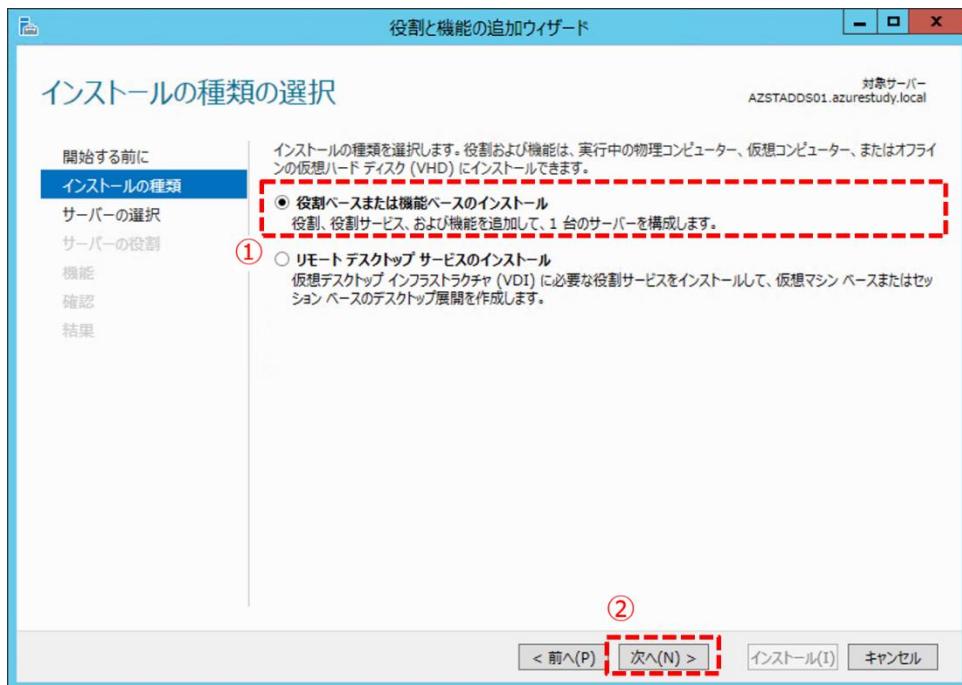
- ドメイン管理者アカウントで AD DS サーバー [AZSTADDS01] にサインインし、[サーバーマネージャー] を開きます。
- [管理] メニュー > [役割と機能の追加] をクリックします。



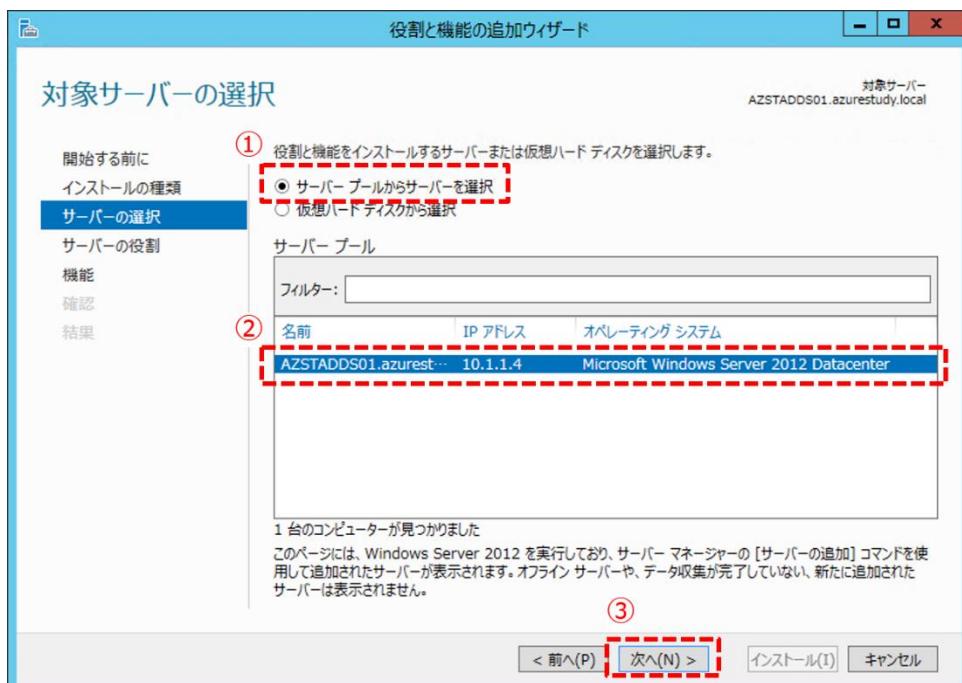
- [役割と機能の追加ウィザード] 画面が開きます。[開始する前に] ページにて [次へ] ボタンをクリックします。



4. [インストールの種類の選択] ページにて [役割ベースまたは機能ベースのインストール] を選択して [次へ] ボタンをクリックします。

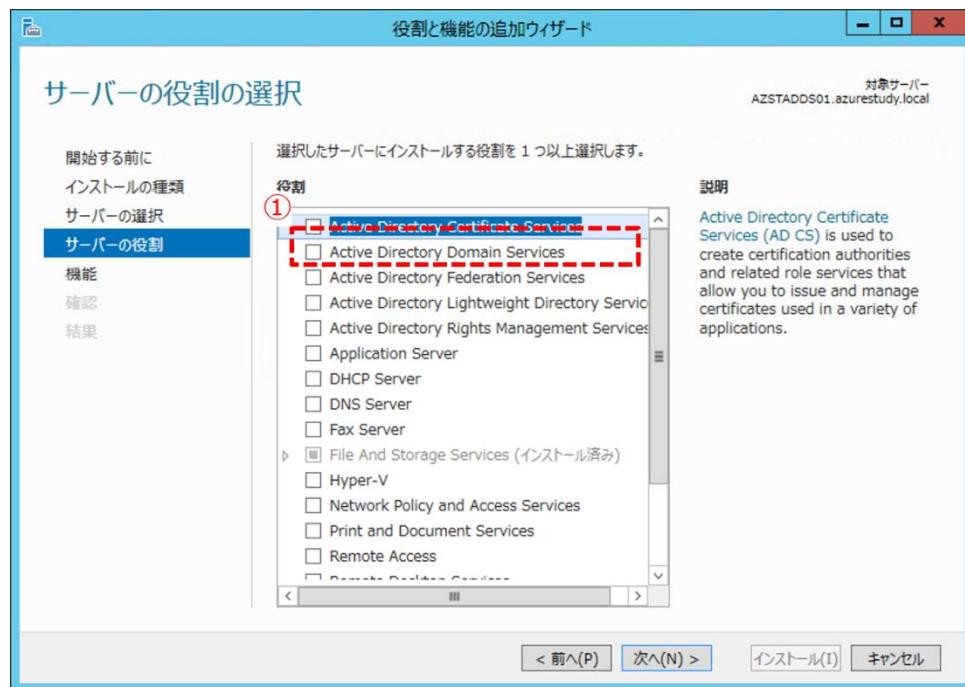


5. [対象サーバーの選択] ページにて [サーバー プールからサーバーを選択] を選択し、[サーバー プール] から AD DS サーバー [AZSTADDS01] を選択して [次へ] ボタンをクリックします。



企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

6. [サーバーの役割の選択] ページにて [役割] 一覧から [Active Directory ドメイン サービス] のチェックボックスにチェックを付けます。



以下の画面が開きます。[Active Directory ドメイン サービス] が依存するサービス、および機能も追加する必要があるので内容を確認し、[管理ツールを含める (存在する場合)] チェックボックスにチェックを付けて [機能の追加] ボタンをクリックして閉じます。

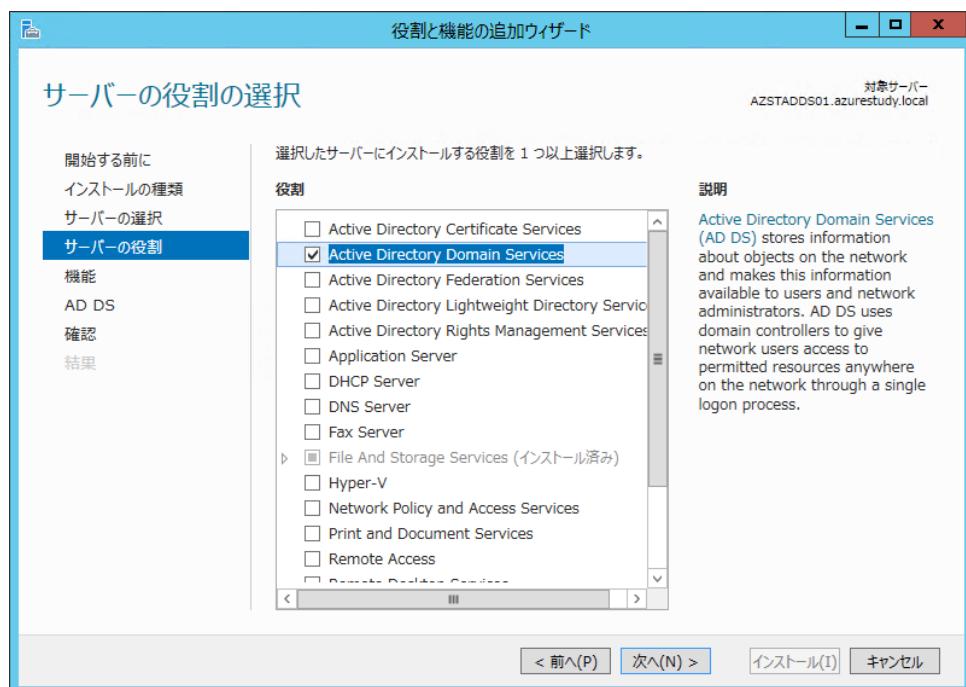


企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

【表：[Active Directory ドメイン サービス] が依存するサービスと機能】

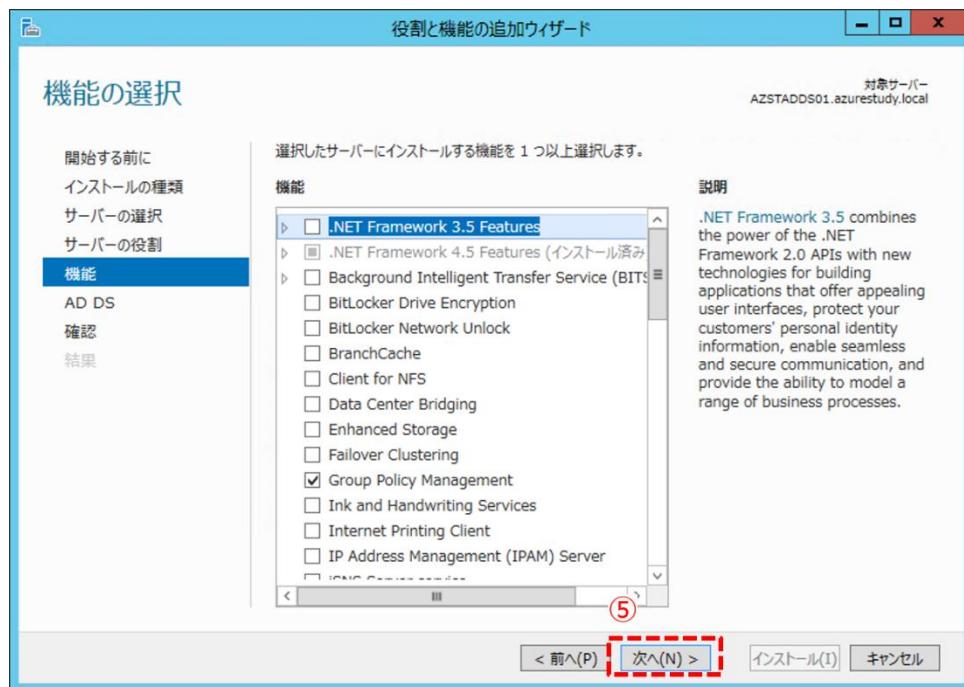
[ツール] グループ ポリシーの管理			
リモート サーバー 管理ツール	役割管理ツール	AD DS および AD LDS ツール	Windows PowerShell の Active Directory モジュール
		AD DS ツール	[ツール] Active Directory 管理センター [ツール] AD DS スナップインおよびコマンドライン ツール

[サーバーの役割の選択] ページに戻ると、[Active Directory ドメイン サービス] のチェックボックスにチェックが付きます。 [次へ] ボタンをクリックします。

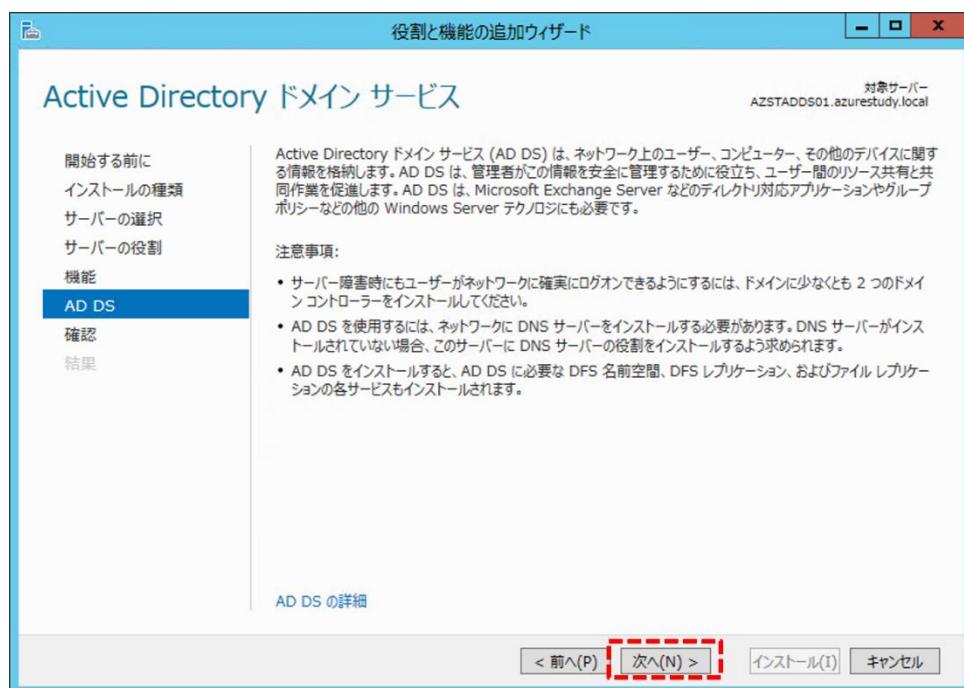


企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

7. [機能の選択] ページにて [機能] 一覧で [グループ ポリシーの管理] と [リモート サーバー管理ツール] チェックボックスにチェックが付いていることを確認して [次へ] ボタンをクリックします。

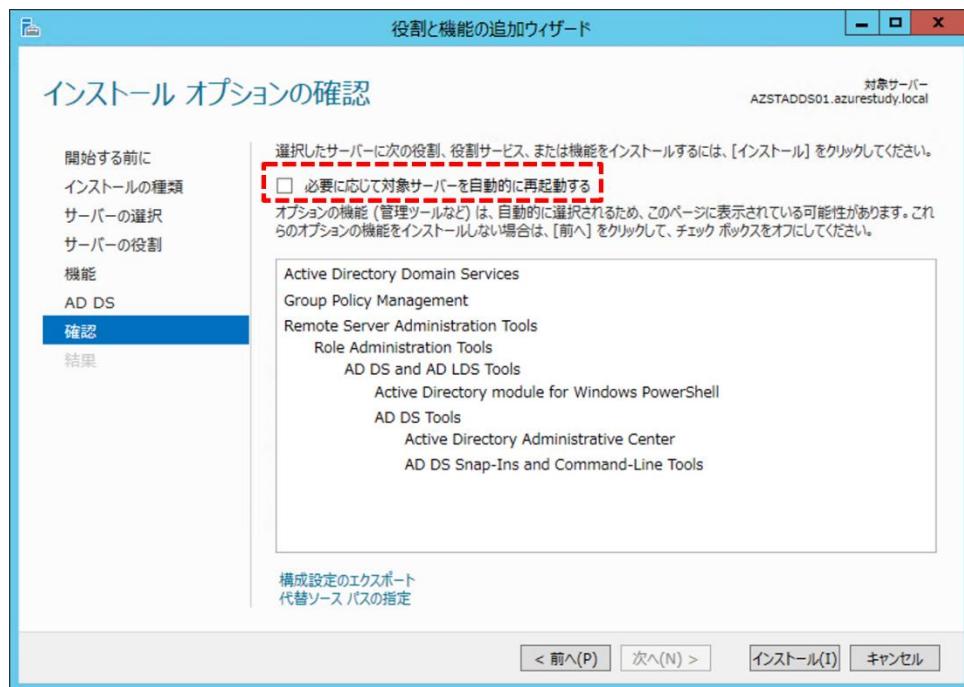


8. [Active Directory ドメイン サービス] ページにて [次へ] ボタンをクリックします。

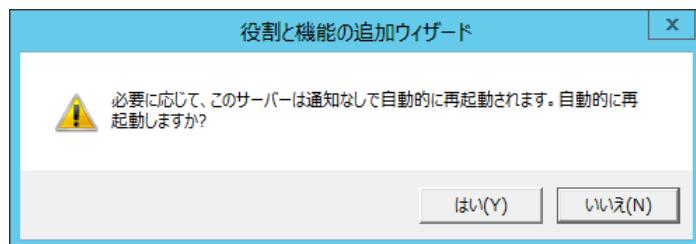


企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

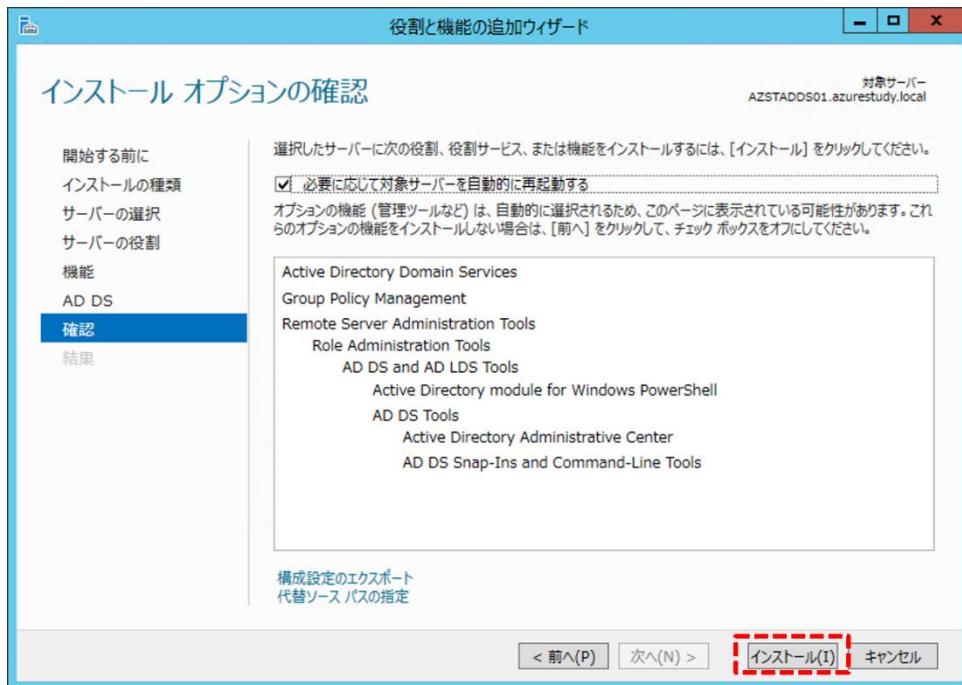
9. [インストール オプションの確認] ページにて [必要に応じて対象サーバーを自動的に再起動する] チェックボックスにチェックを付けます。



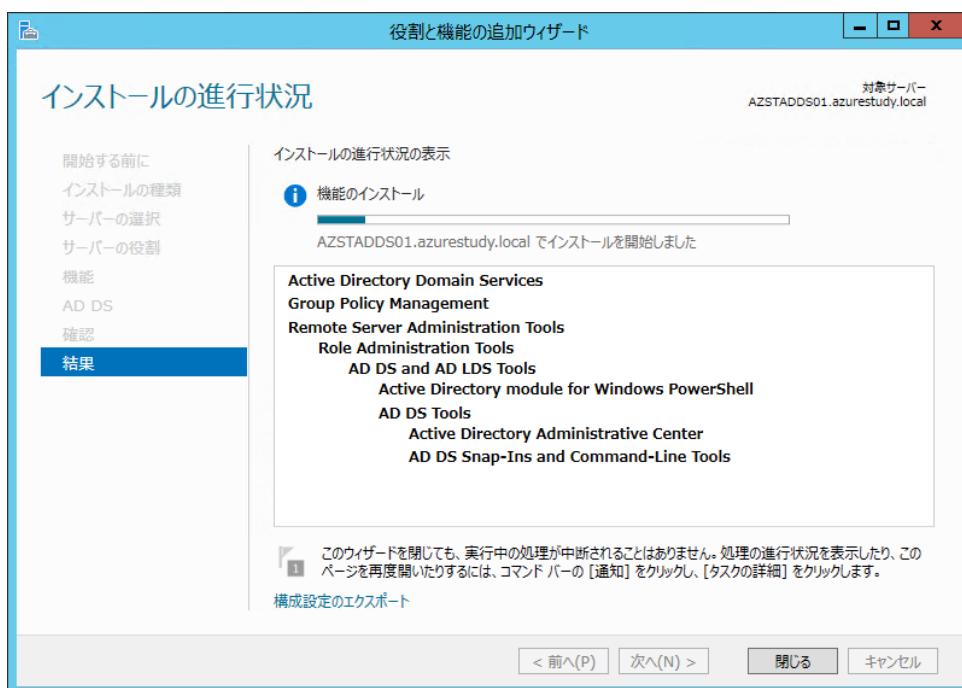
以下のメッセージ ボックスが開くので、[はい] ボタンをクリックして閉じます。



企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携
[インストール オプションの確認] ページに戻り、[必要に応じて対象サーバーを自動的に再起動する] チェックボックスにチェックが付いていることを確認して [インストール] ボタンをクリックします。

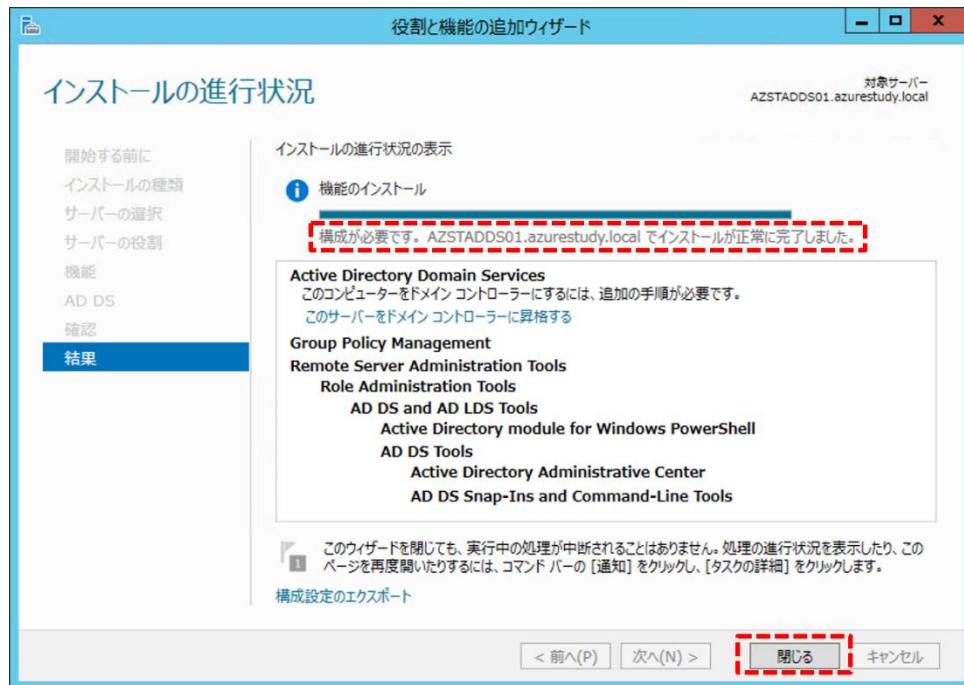


10. インストールが完了するまで待ちます。



企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

11. 「構成が必要です。AZSTADDS01.azurestudy.local でインストールが正常に完了しました。」とメッセージが表示されたら [閉じる] ボタンをクリックして閉じます。

**Note : 2 台目以降の AD DS サーバーでの作業**

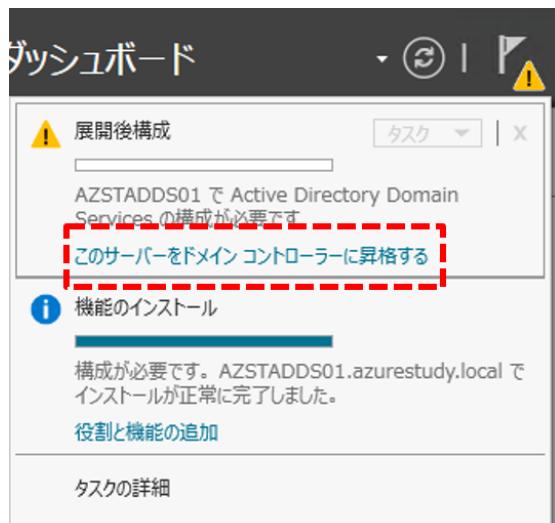
2 台目以降の AD DS サーバー [AZSTADDS02] についてもこの項の作業を実施します。

9.2 ドメイン コントローラーへの昇格

- ドメイン管理者アカウントで AD DS サーバー [AZSTADDS01] にサインインし、[サーバー マネージャー] を開きます。
- [サーバー マネージャー] 画面上部にタスクの通知（下図の赤枠部分）が表示されるので、これをクリックして展開します。

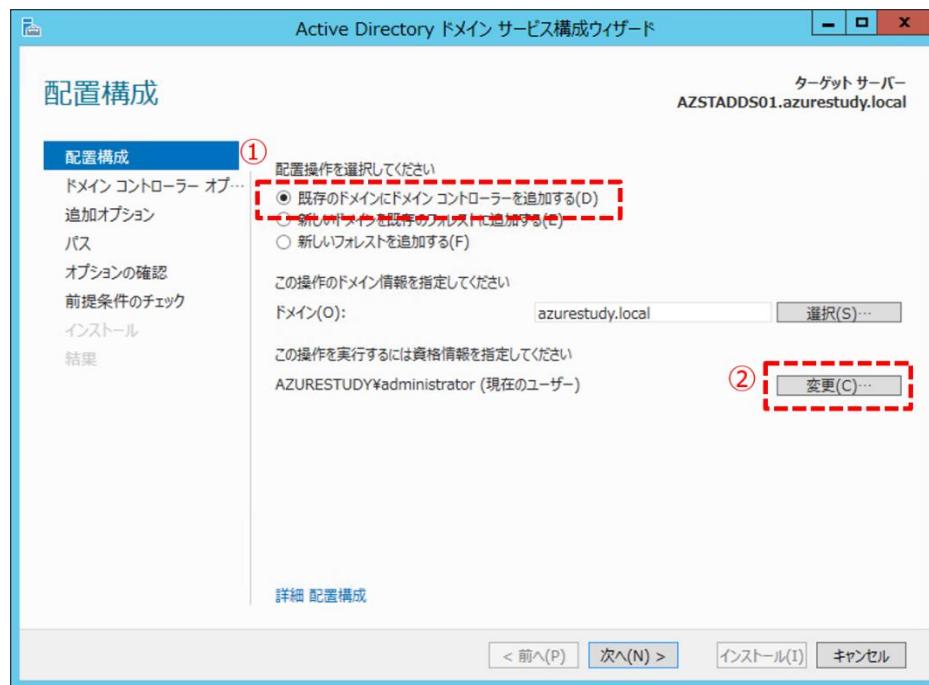


展開すると、下図のように表示されます。 [このサーバーをドメイン コントローラーに昇格する] をクリックします。



企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

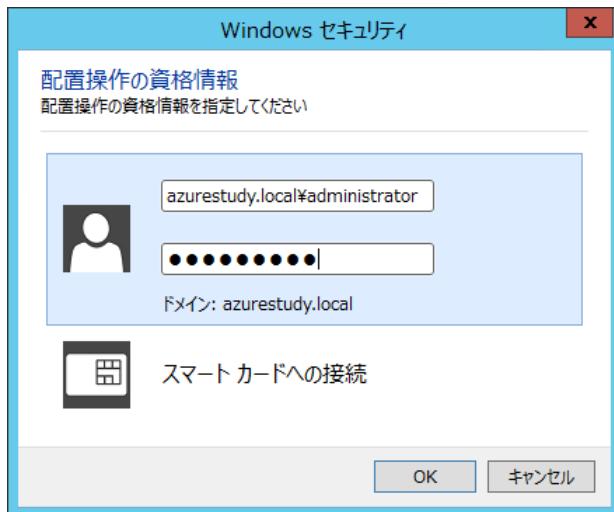
3. [Active Directory ドメイン サービス構成ウィザード] 画面が開きます。[配置構成] ページにて [既存のドメイン コントローラーを追加する] を選択し、「資格情報の指定」の [変更] ボタンをクリックします。

**Note : 資格情報の入力**

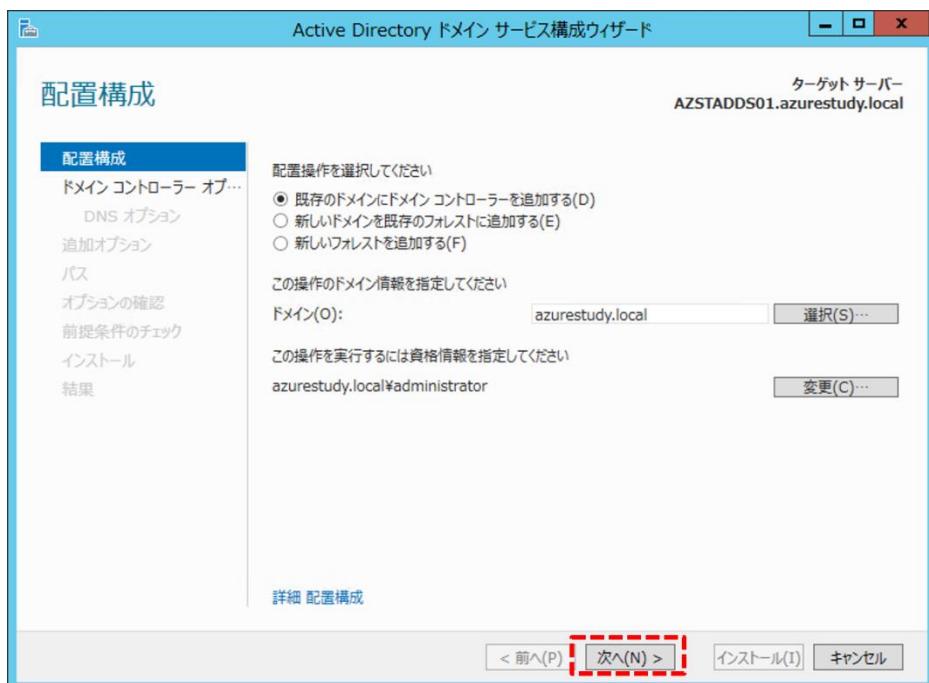
「技術情報の文書番号 2737935」の問題により、ローカル管理者とドメイン管理者のパスワードが同じ場合、昇格に失敗することがあります。そのため、自動で入力された資格情報のまま進めず手動で入力し直す必要があります。

「Active Directory installation stalls at the "Creating the NTDS settings object" stage (<http://support.microsoft.com/kb/2737935/ja>)」

企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携 [Windows セキュリティ] 画面が開きます。[ユーザー名] に「azurestudy.local\administrator」と入力し [パスワード] に「studyP@ss」と入力して [OK] ボタンをクリックします。

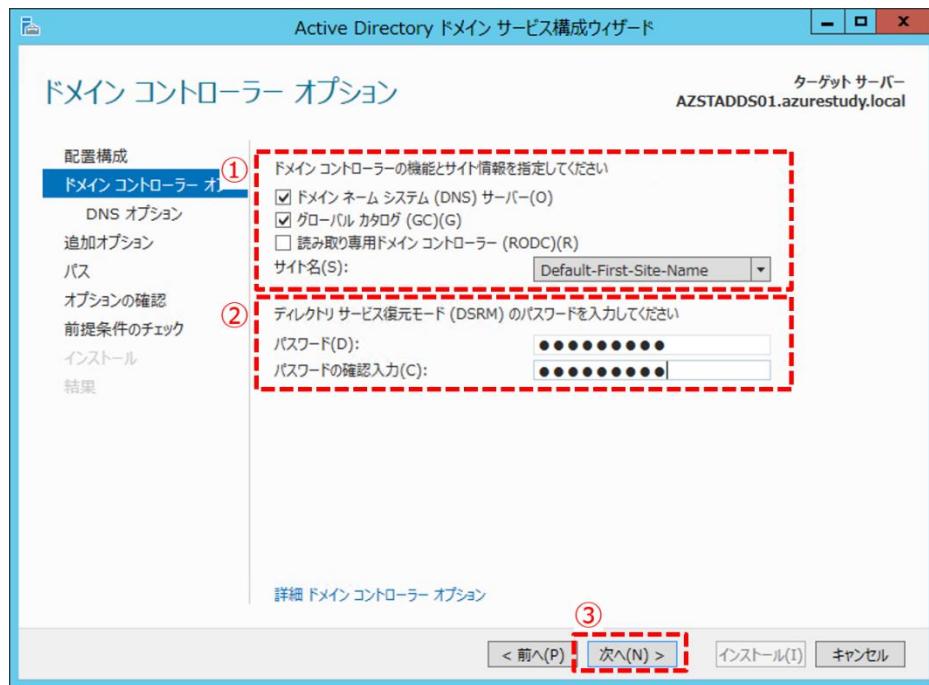


[配置構成] ページに戻り、[次へ] ボタンをクリックします。



企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

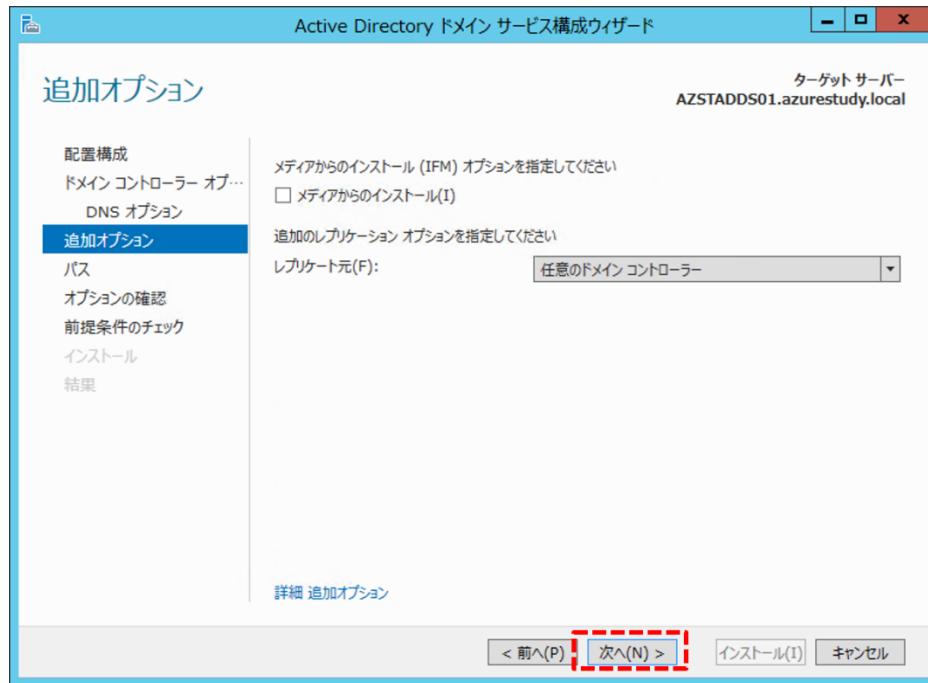
4. [ドメイン コントローラー オプション] ページにて [ドメイン ネーム システム (DNS) サーバー] と [グローバル カタログ (GC)] チェックボックスにチェックを付けて [サイト名] に「Default-First-Site-Name」が選択されていることを確認し、「ディレクトリ サービス復元モード (DSRM)」の [パスワード] 及び [パスワードの確認入力] に「studyP@ss」と入力して [次へ] ボタンをクリックします。



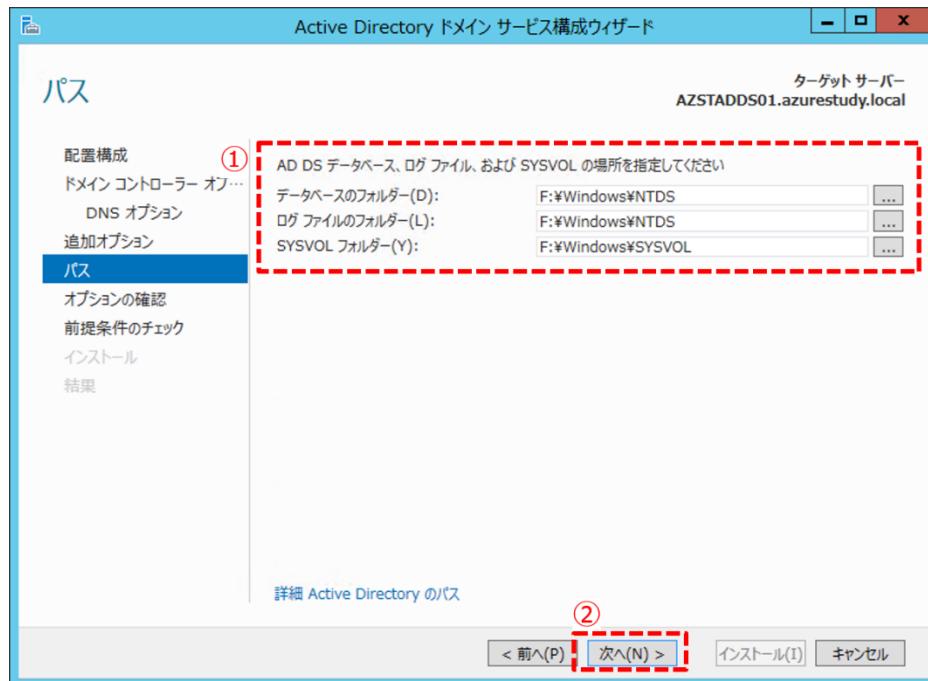
5. [DNS オプション] ページにて [次へ] ボタンをクリックします。



6. [追加オプション] ページにて [次へ] ボタンをクリックします。

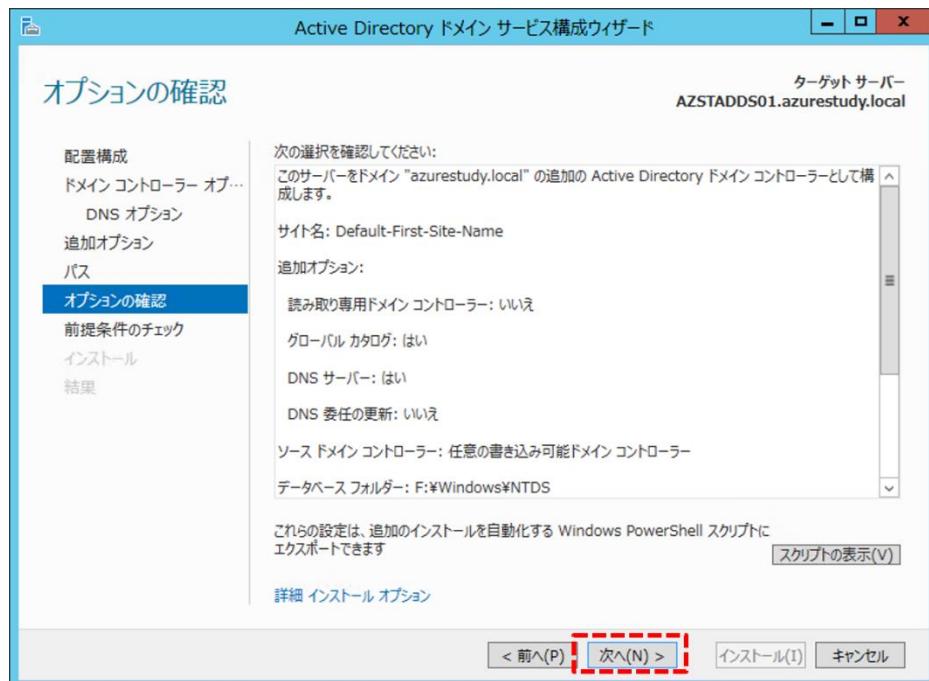


7. [パス] ページにて各情報の格納場所を、追加したディスク (今回は F ドライブ) に変更して [次へ] ボタンをクリックします。



企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

8. [オプションの確認] ページにて内容を確認して [次へ] ボタンをクリックします。



9. [前提条件のチェック] ページにて警告が 3 件表示されますが、そのまま [インストール] ボタンをクリックします。



Note : 前提条件チェックの警告について

これら 3 つの警告は基本的に無視して構いません。

以下は、Windows NT 4.0 で使用されている暗号化アルゴリズムとの互換性がないために表示されるメッセージとなります。

今回の環境では Windows Server 2012 のみの環境であるため、無視します。

! Windows Server 2012 ドメインコントローラーには、セキュリティ設定 "Windows NT 4.0 と互換性のある暗号化アルゴリズムを許可する" の既定値が設定されています。これにより、セキュリティチャネルセッションを確立するときに、セキュリティの弱い暗号化アルゴリズムの使用は許可されなくなります。

この設定の詳細については、サポート技術情報 (KB) の記事 942564 (<http://go.microsoft.com/fwlink/?LinkId=104751>) を参照してください。

以下は、動的 IP (DHCP) が設定されているために表示されるメッセージとなります。

AD DS で動的 IP を用いることは不可ですが、Azure の制限として静的 IP が指定できないため、無視します。

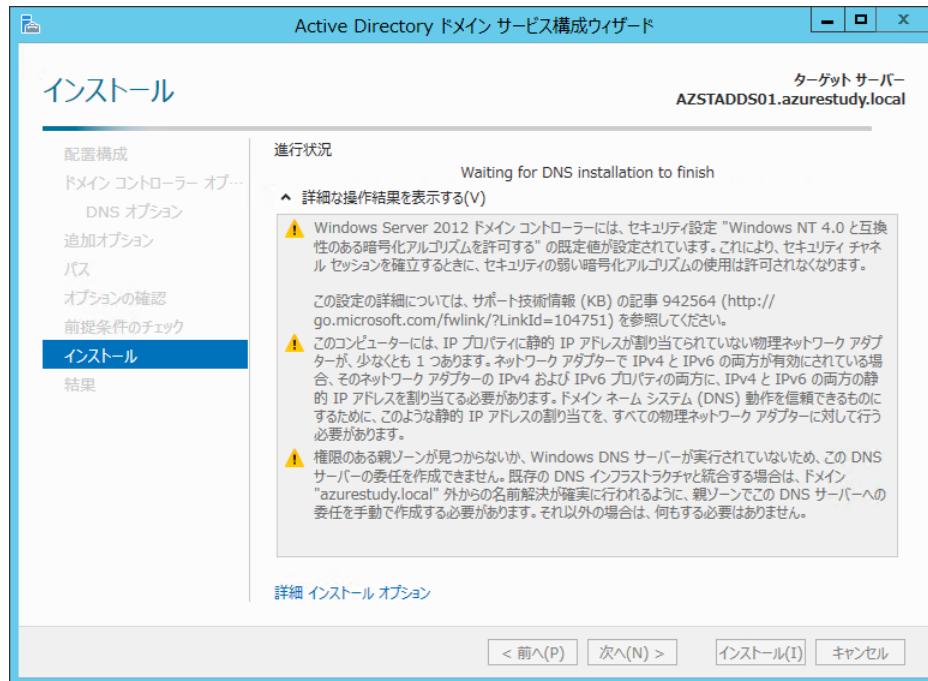
! このコンピューターには、IP プロパティに静的 IP アドレスが割り当てられていない物理ネットワークアダプターが、少なくとも 1 つあります。ネットワークアダプターで IPv4 と IPv6 の両方が有効にされている場合、そのネットワークアダプターの IPv4 および IPv6 プロパティの両方に、IPv4 と IPv6 の両方の静的 IP アドレスを割り当てる必要があります。ドメインネームシステム (DNS) 動作を信頼できるものにするために、このような静的 IP アドレスの割り当てを、すべての物理ネットワークアダプターに対して行う必要があります。

以下は、DNS サーバーが存在していないために表示されるメッセージとなります。

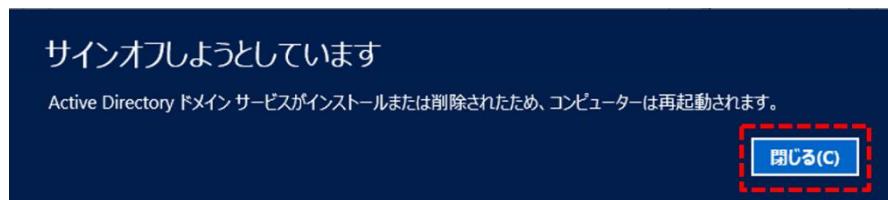
AD DS インストール時に合わせてインストールされるため、無視します。

! 権限のある親ゾーンが見つからないか、Windows DNS サーバーが実行されていないため、この DNS サーバーの委任を作成できません。既存の DNS インフラストラクチャと統合する場合は、ドメイン "azurestudy.local" 外からの名前解決が確実に行われるよう、親ゾーンでこの DNS サーバーへの委任を手動で作成する必要があります。それ以外の場合は、何もする必要はありません。

10. インストールが完了するまで待ちます。

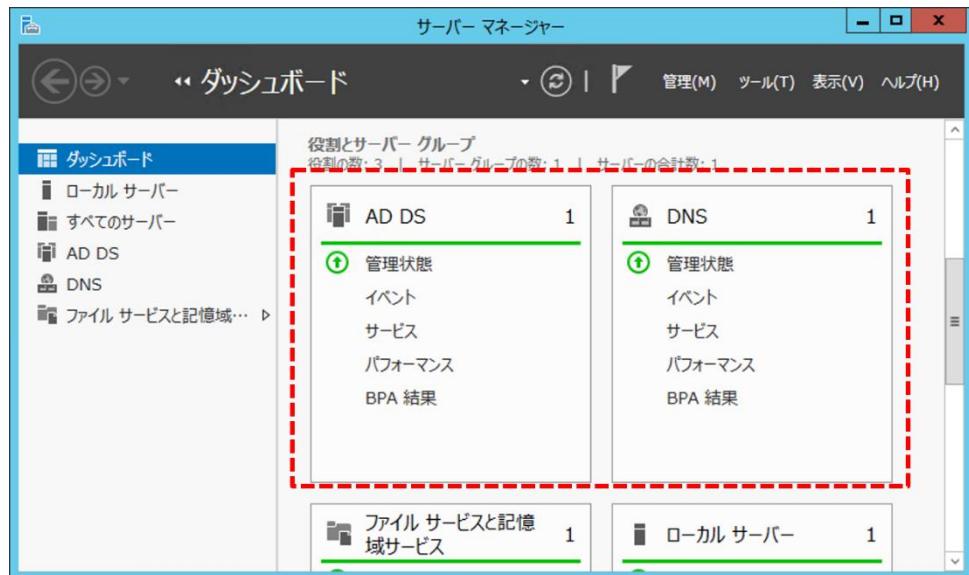


11. インストールが完了すると自動的に OS 再起動が開始されます。[閉じる] をクリックします。



企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

12. OS 再起動後、[サーバー マネージャー] を起動すると、「AD DS」と「DNS」が追加されています。



9.3 サイトとサブネットの作成

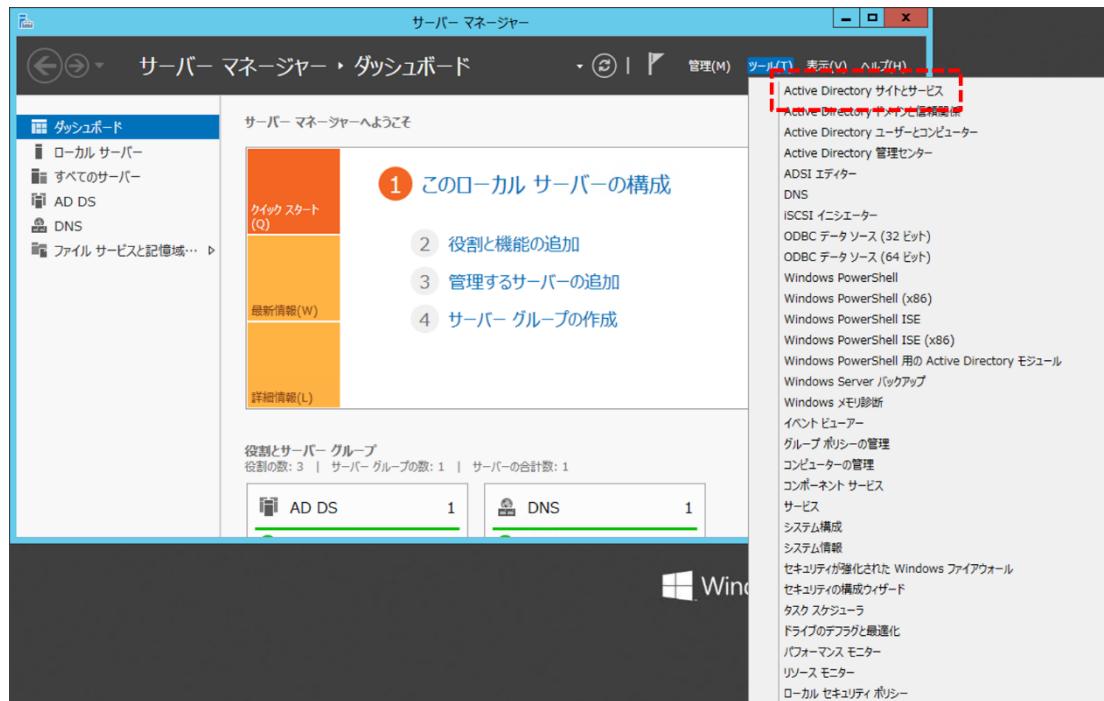
サイトとサブネットを適正に設定することにより Azure 側に AD DS の認証を必要とするサーバーを構築した際に適切な AD DS サーバー (Azure 上に構築した AD DS サーバー) にて認証が行われるようになります。通信コストが低減できます。

▼ サイトの作成

サイトの作成はオンプレミス側にて実施します。(なお、Azure 上で行っても構いませんがこの自習書ではオンプレミス側で作成し、Azure 側でレプリケートの確認を行います。)

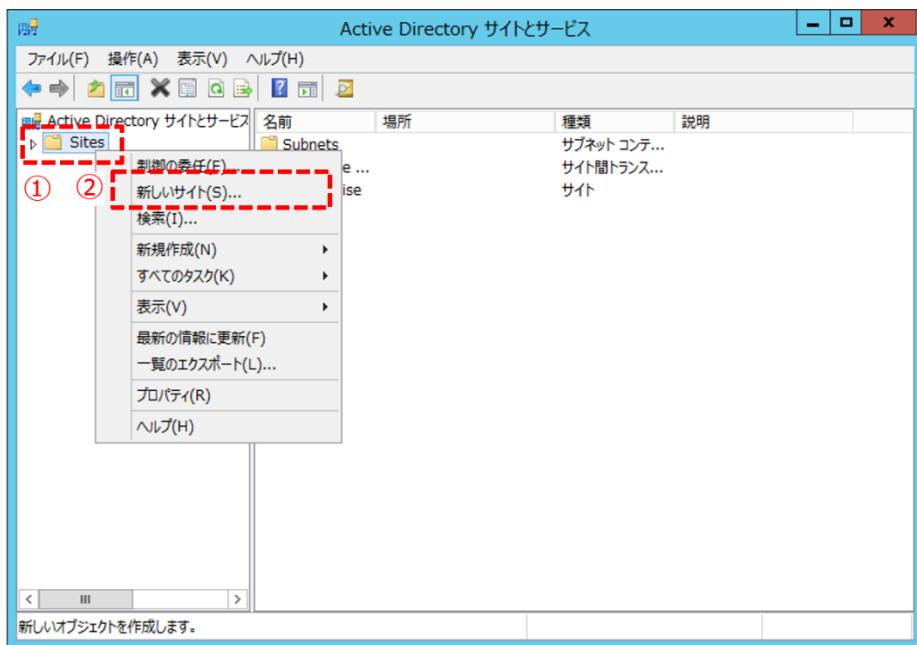
1. ドメイン管理者アカウントで AD DS サーバー [OPSTADDS01] にサインインし、[サーバーマネージャー] を開きます。

2. [ツール] メニュー > [Active Directory サイトとサービス] をクリックします。

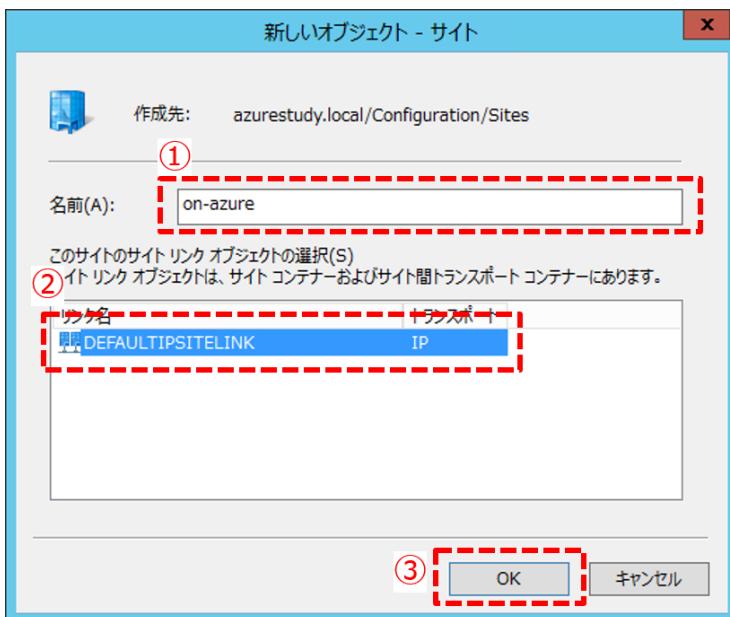


企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

3. [Active Directory サイトとサービス] 画面が開きます。左ペインから [Active Directory サイトとサービス] > [Sites] を右クリックして [新しいサイト] をクリックします。

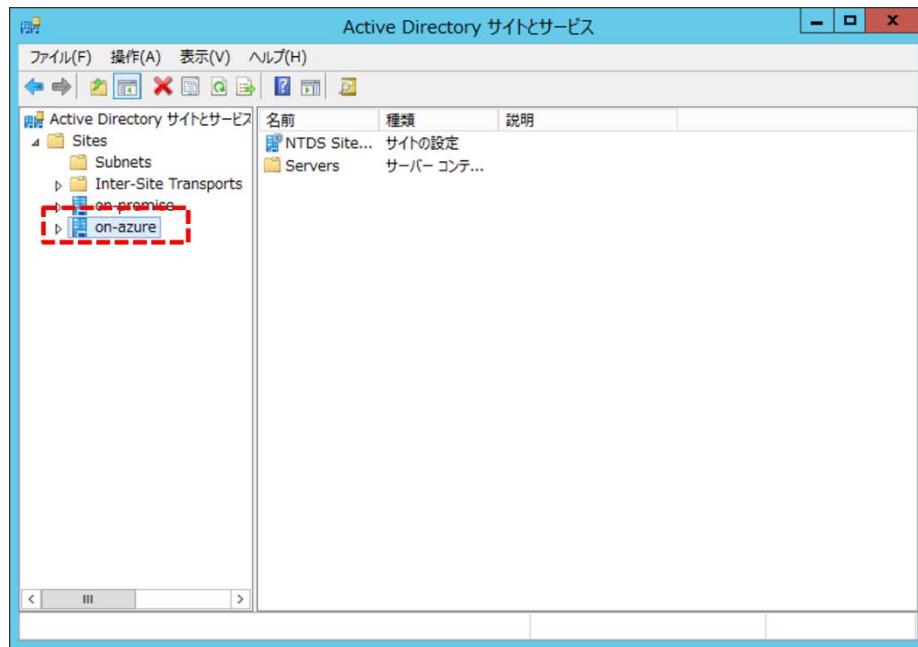


4. [新しいオブジェクト - サイト] 画面が開きます。[名前] に「on-azure」と入力し [このサイトのサイト リンク オブジェクトの選択] から「DEFAULTIPSITELINK」を選択して [OK] ボタンをクリックします。



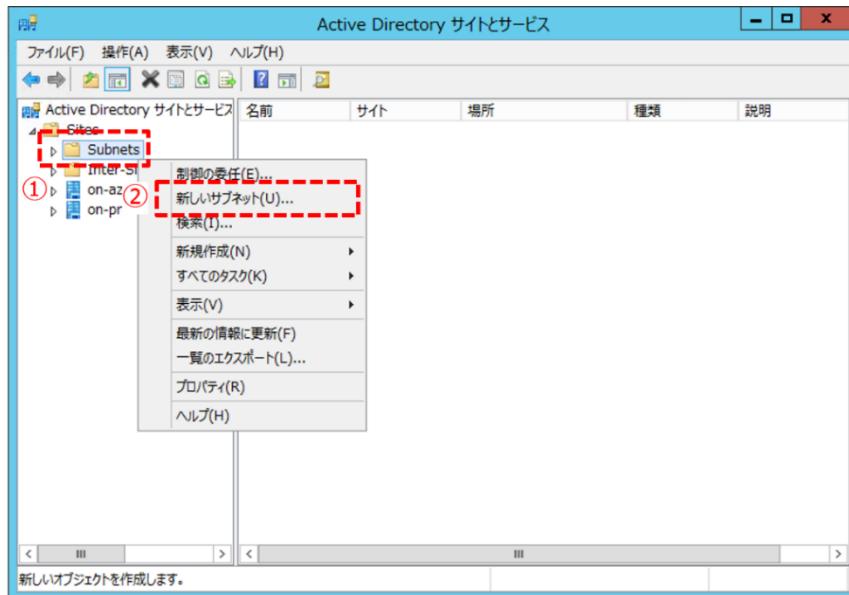
企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

5. [Active Directory サイトとサービス] 画面に戻り、[Sites] 配下に「on-azure」が作成されていることを確認します。

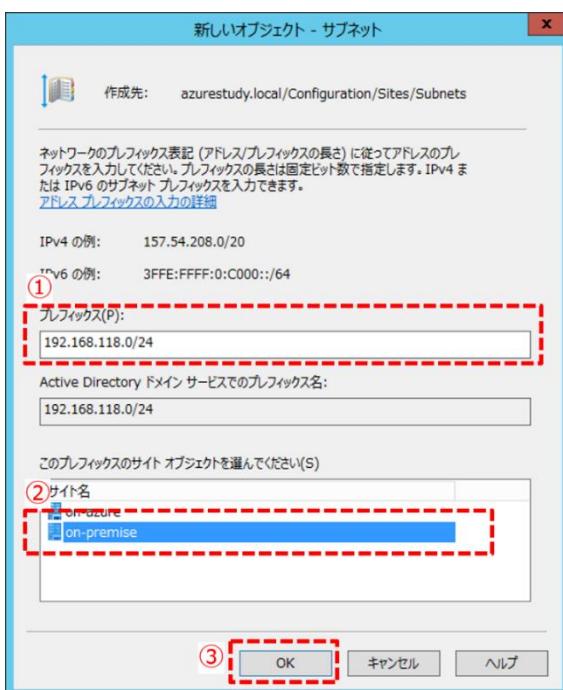


▼ サブネットの作成（オンプレミス環境用）

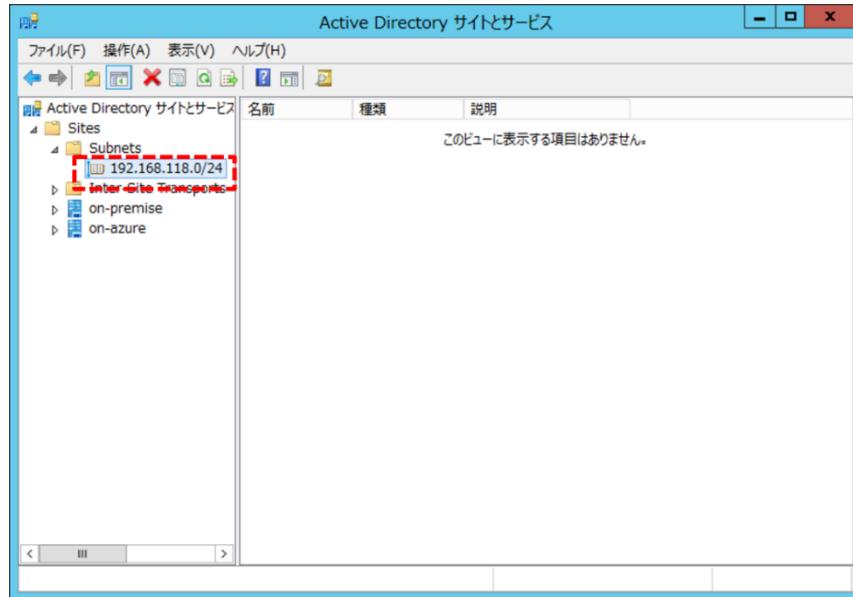
6. [Active Directory サイトとサービス] 画面にて左ペインから [Active Directory サイトとサービス] > [Subnets] を右クリックして [新しいサブネット] をクリックします。



7. [新しいオブジェクト - サブネット] 画面が開きます。[プレフィックス] にオンプレミス側のサブネットである「192.168.118.0/24」を入力し [このプレフィックスのサイト オブジェクトを選んでください] から「サイトの作成」で作成した「on-premise」を選択して [OK] ボタンをクリックします。

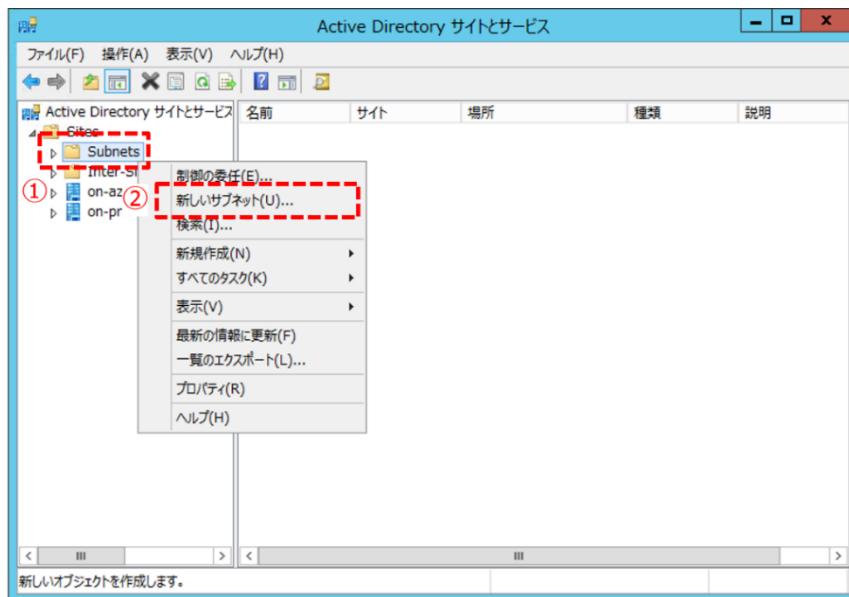


8. [Active Directory サイトとサービス] 画面に戻り、[Subnets] 配下にオンプレミス用のサブネットが作成されていることを確認します。

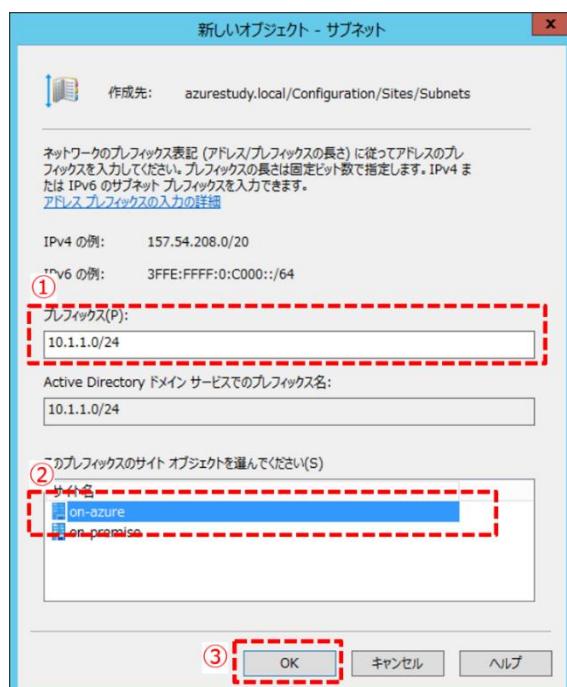


▼ サブネットの作成 (Azure 環境用)

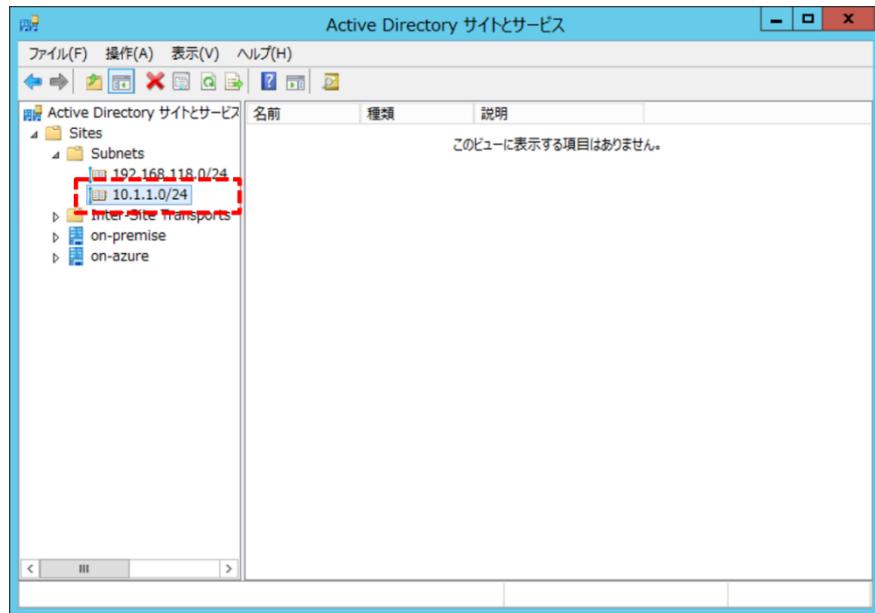
9. [Active Directory サイトとサービス] 画面にて左ペインから [Active Directory サイトとサービス] > [Subnets] を右クリックして [新しいサブネット] をクリックします。



10. [新しいオブジェクト - サブネット] 画面が開きます。[プレフィックス] に Azure 側のサブネットである「10.1.1.0/24」を入力し [このプレフィックスのサイト オブジェクトを選んでください] から「サイトの作成」で作成した「on-azure」を選択して [OK] ボタンをクリックします。



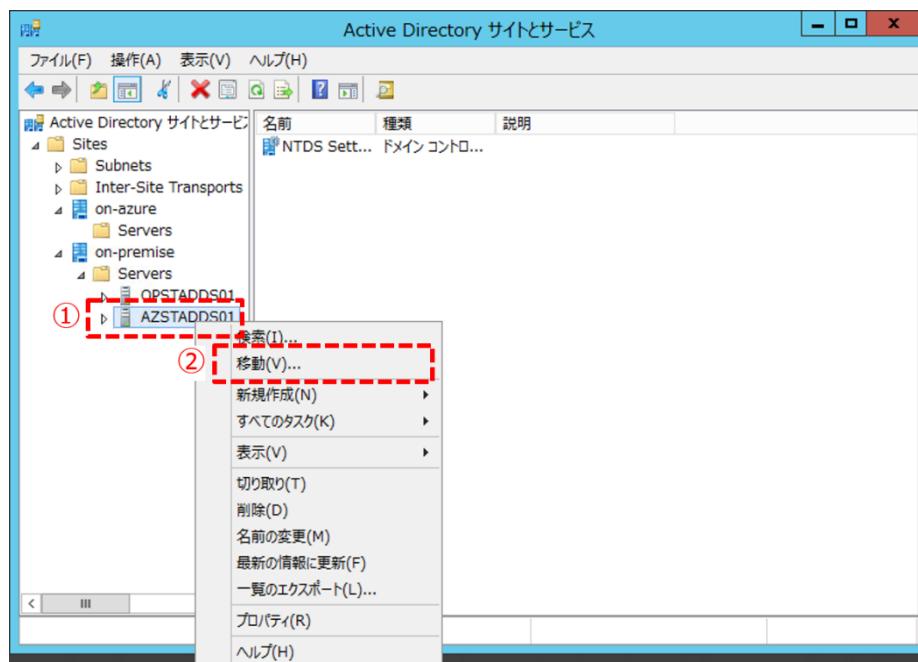
11. [Active Directory サイトとサービス] 画面に戻り、[Subnets] 配下に Azure 用のサブネットが作成されていることを確認します。



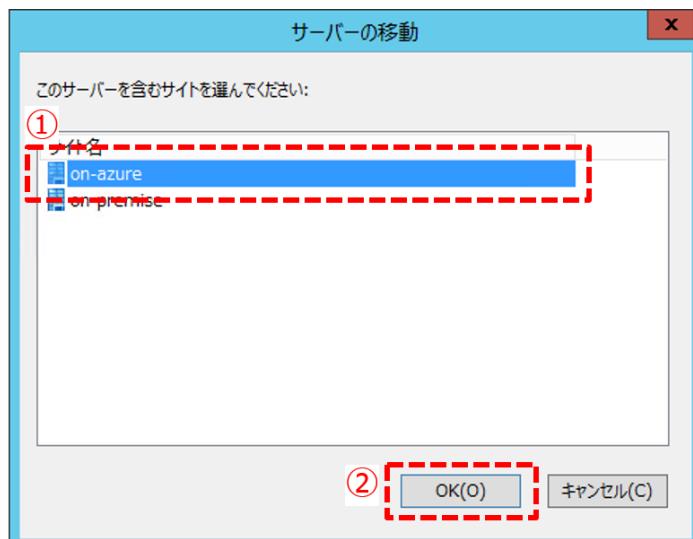
▼ オブジェクトの移動

Azure 上の AD DS サーバーを作成したサイトに移動します。

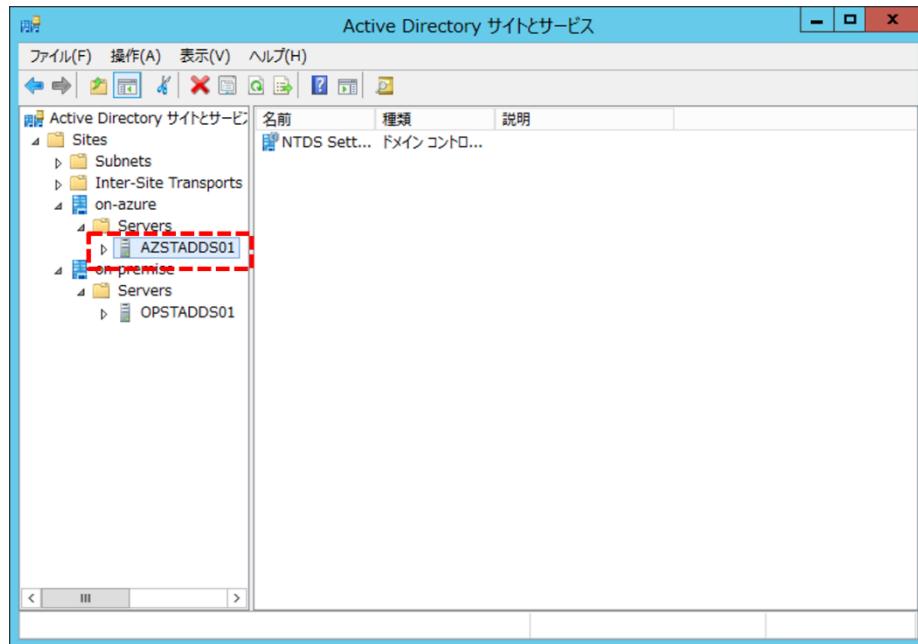
12. [Active Directory サイトとサービス] 画面にて左ペインから [Active Directory サイトとサービス] > [Sites] > [on-premise] > [Servers] > [AZSTADDSS01] を右クリックして [移動] をクリックします。



13. [サーバーの移動] 画面が開きます。 [このサーバーを含むサイトを選んでください] から「on-azure」を選択して [OK] ボタンをクリックします。

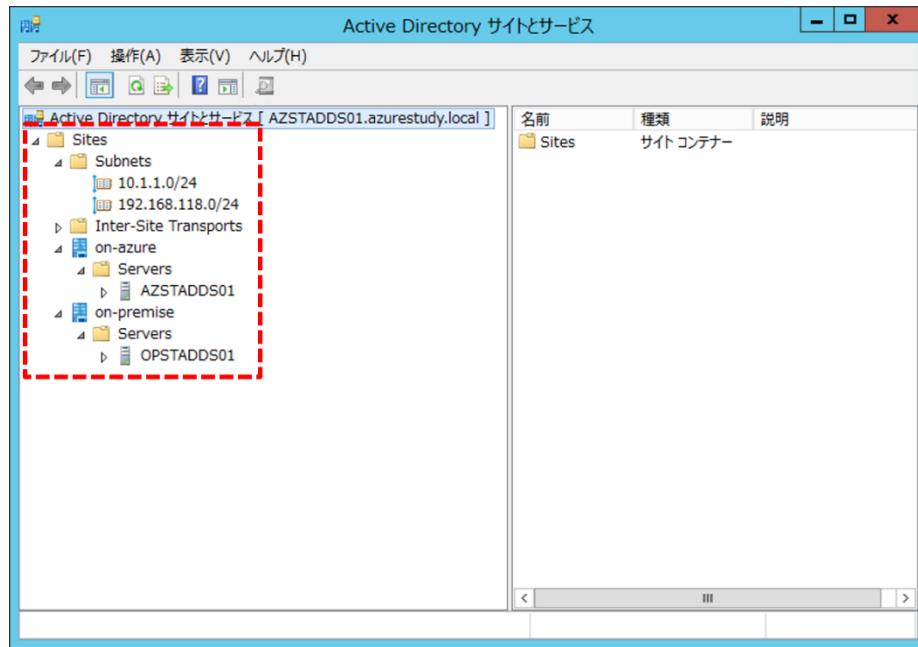


14. [Active Directory サイトとサービス] 画面に戻り、[AZSTADDS01] が [Sites] > [on-premise] > [Servers] 配下から [Sites] > [on-azure] > [Servers] 配下に移動されていることを確認します。



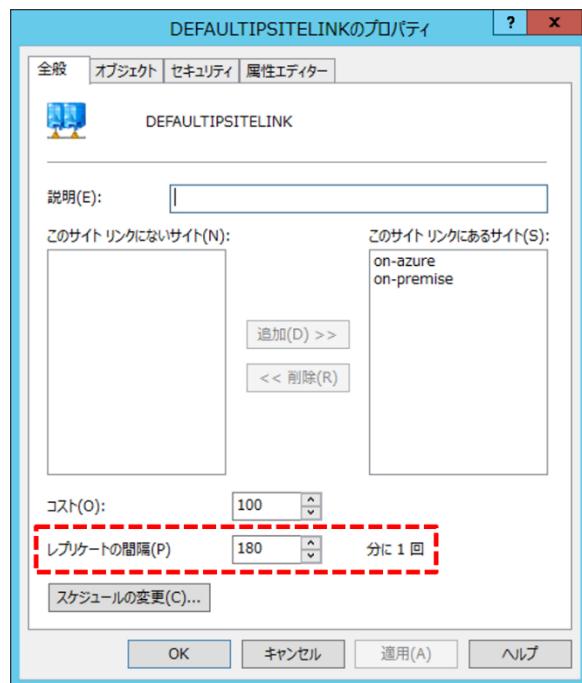
➔ **Azure 上での確認**

15. [Active Directory サイトとサービス] 画面にてサイトとサブネットが作成されていることを確認します。

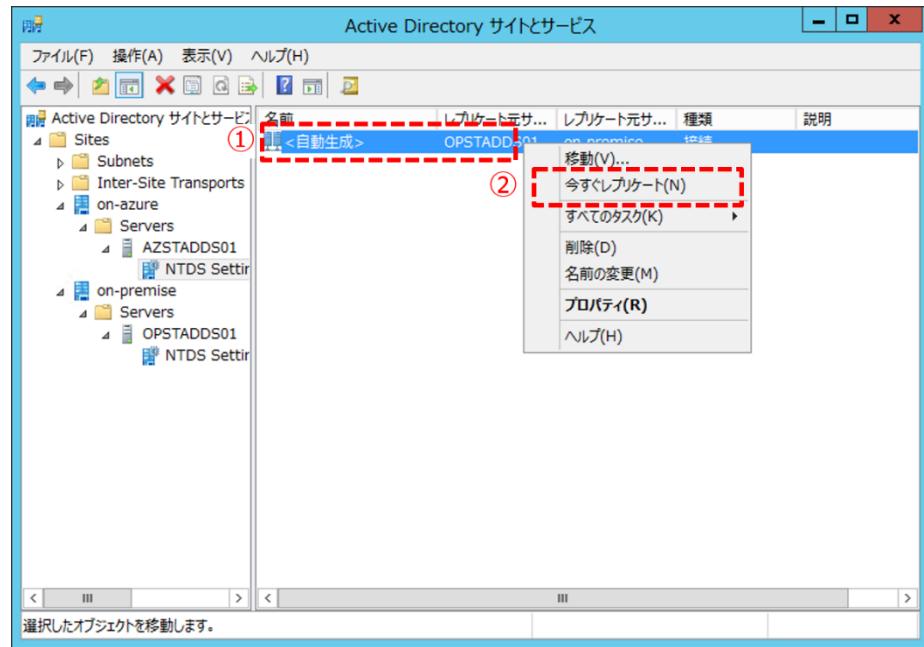


Note : サイト間 AD DS のレプリケートについて

同じサイトに配置されている場合にはリアルタイムでレプリケートされますが、サイトを分けている場合、既定では 180 分となっています。



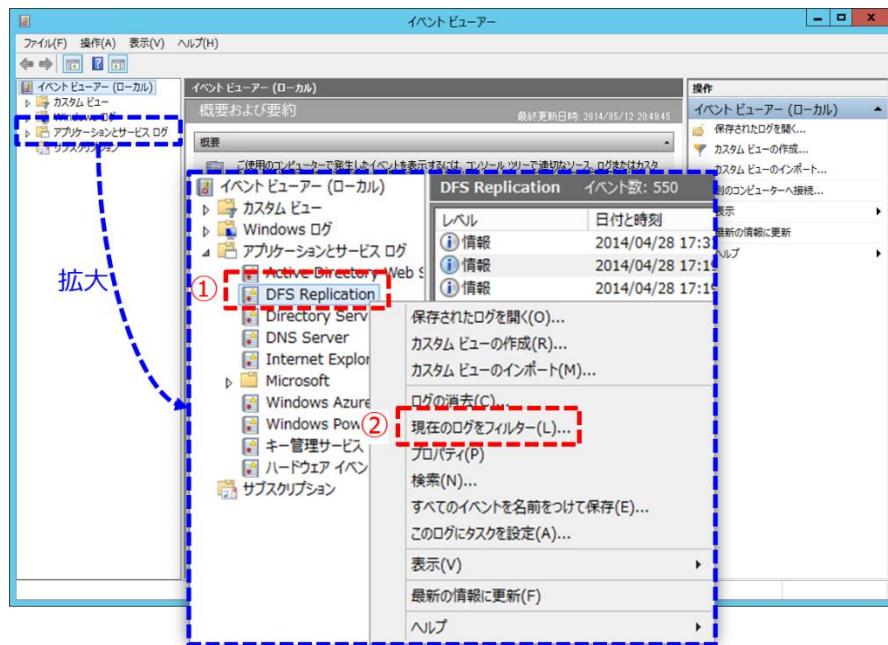
すぐにレプリケートをさせたい場合には [ADSTADDS01] の [NTDS Settings] を選択し [<自動生成>] を右クリックして [今すぐレプリケート] をクリックします。



9.4 初期レプリケートの完了

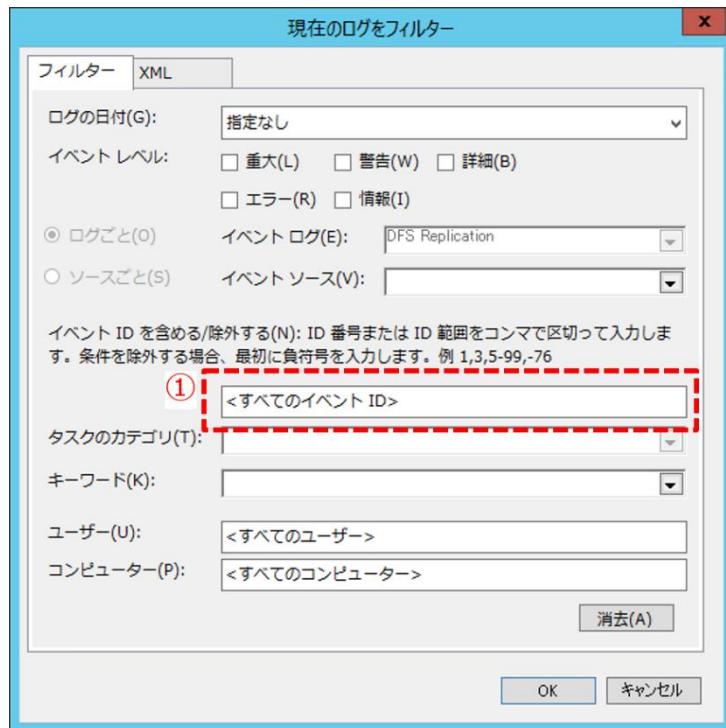
AD DS サーバーの初期レプリケートが正常に完了したことを確認します。

1. ドメイン管理者アカウントで AD DS サーバー [AZSTADDS01] にサインインし、[イベント ビューアー] を開きます。
2. 左ペインから [イベント ビューアー] > [アプリケーションとサービス ログ] > [DFS Replication] を右クリックして [現在のログをフィルター] をクリックします。

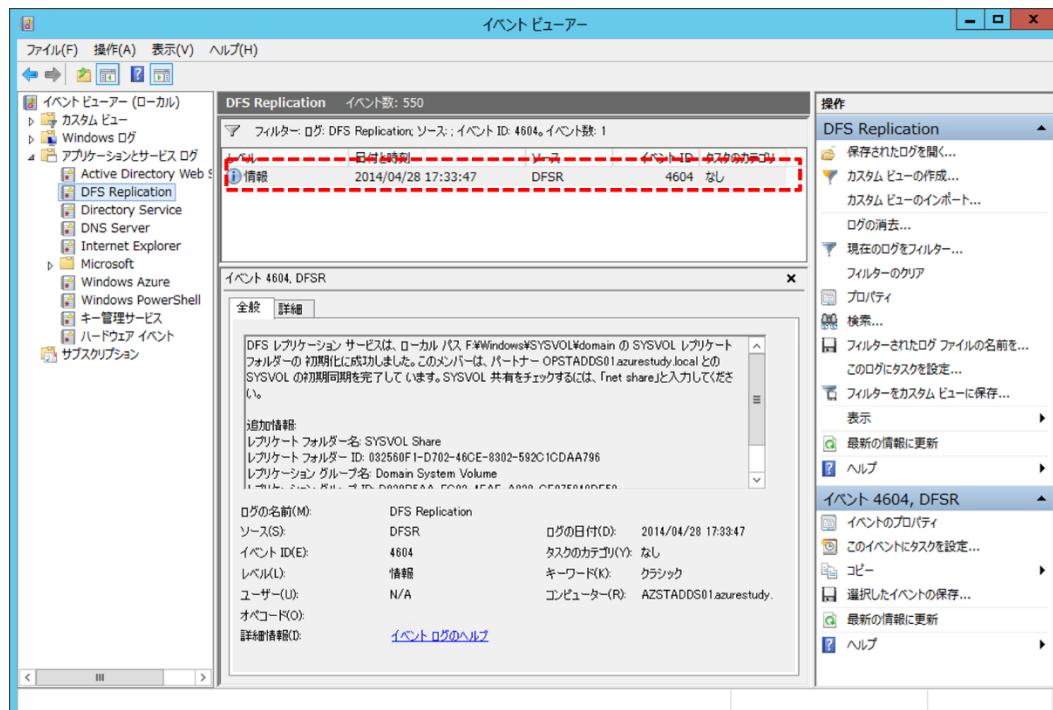


企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

3. [現在のログをフィルター] 画面が開きます。[フィルター] タブを開き [<すべてのイベント ID>] に「4604」と入力して [OK] ボタンをクリックします。



4. [イベントビューアー] 画面に戻り、フィルターの結果「4604」のイベントが表示されれば初期レプリケートが完了したことを示します。



9.5 仮想ネットワークへの DNS サーバーの追加設定

Azure 上に構築した AD DS サーバーも DNS として登録します。また、優先順位を変更し、Azure 上のサービスは優先的に Azure 上の AD DS サーバーに名前解決の問い合わせを行うよう、設定を行います。

➔ DNS サーバーの登録

1. Azure 管理ポータルにサインインします。
2. 画面左側のメニューから [ネットワーク] をクリックします。 [ネットワーク] ページが表示したら、[DNS サーバー] タブをクリックします。



3. 画面左下の [+新規] をクリックします。

4. ページが下図のように表示されます。画面右側の入力項目に下の表とおり指定して右下の [DNS サーバーの登録] をクリックします。

※ 1 台ずつ作業を実施します。

項目	設定値	
	1 台目	2 台目
名前	「AZSTADDS01」を入力	「AZSTADDS02」を入力
DNS サーバーの IP アドレス	「10.1.1.4」を入力	「10.1.1.5」を入力

5. 登録処理後、手順 3 のページに戻り DNS サーバーが登録されます。

ネットワーク	
名前	アドレス
azstadds01	10.1.1.4
azstadds02	10.1.1.5
opstadds01	192.168.118.160

◆ DNS サーバーの追加設定

6. 手順 5 を確認後、[仮想ネットワーク] タブをクリックします。

ネットワーク	
名前	アドレス
azstadds01	10.1.1.4
azstadds02	10.1.1.5
opstadds01	192.168.118.160

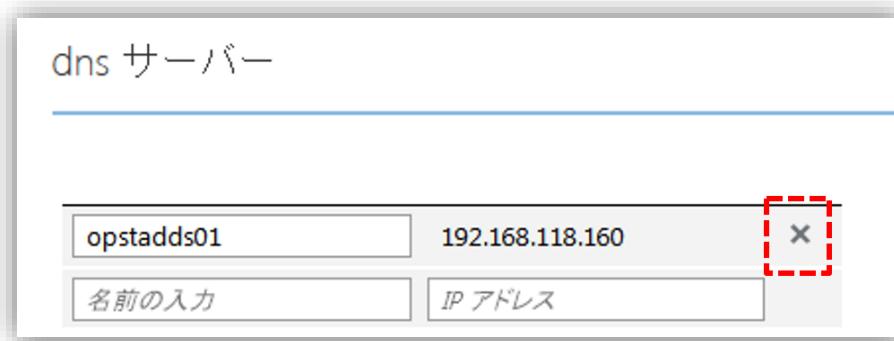
7. 「tokyo-nw」をクリックします。

ネットワーク	
名前	状態
tokyo-nw	→ ✓ 作成済み

8. [構成] タブをクリックします。



9. 「8.1 仮想ネットワークへの DNS サーバーの追加」にて追加した DNS サーバー [OPSTADDS01] の右端にある [×] をクリックしていったん削除します。

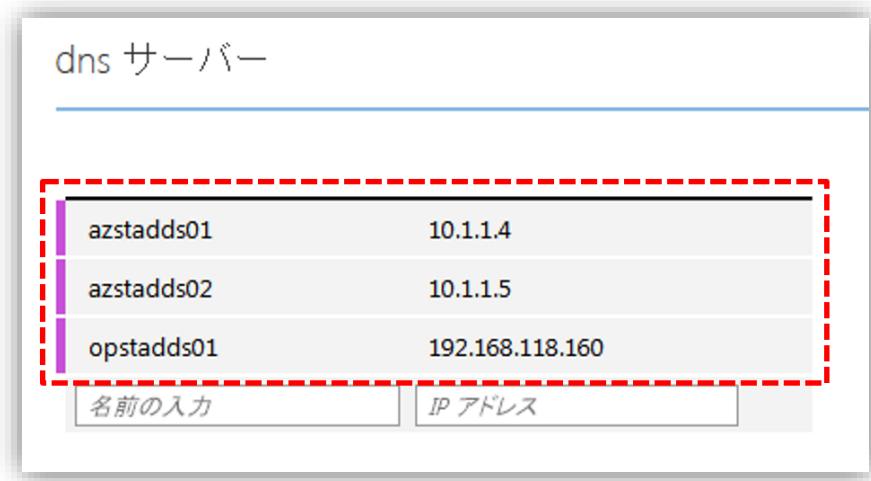


Note : 仮想ネットワーク DNS サーバーの優先順位

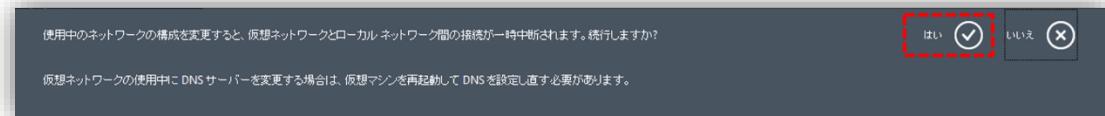
仮想ネットワークの DNS サーバーは上位ほど優先順位が高くなります。そのため、このままの状態で手順 3 ~ 5 で追加した Azure 上の DNS (AD DS) サーバーを追加して登録してしまうと、オンプレミス側の DNS (AD DS) サーバーが最優先となってしまいます。よって、これを削除した後に追加し直します。

10. 再度以下の順に追加していきます。

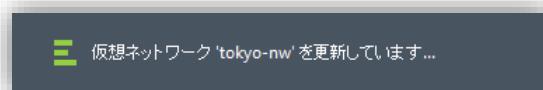
- AZSTADDS01
- AZSTADDS02
- OPSTADDS01

**11.** 画面下部の [保存] をクリックします。

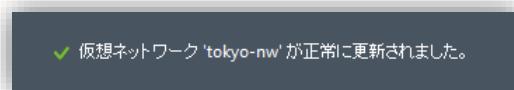
※ 手順 10 を実施すると表示されます。

12. DNS サーバーの設定を変更する際、一時的にネットワークが切断されることがあるため、その警告が表示されます。 [はい] をクリックします。

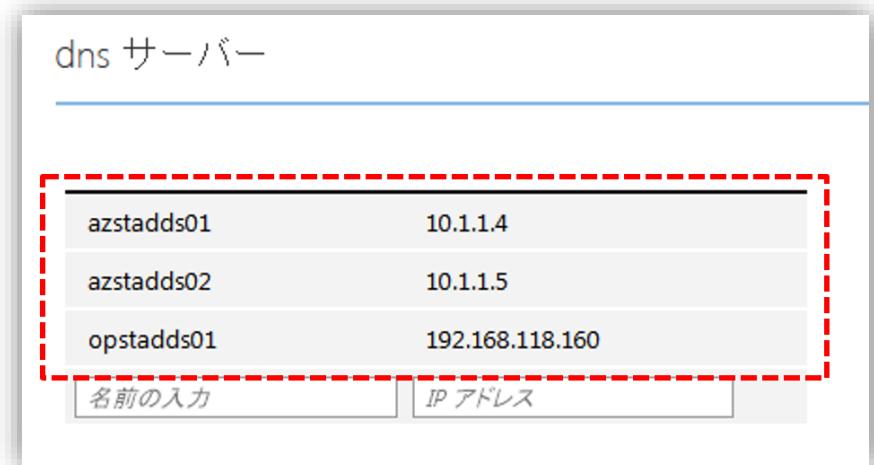
企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携
[はい] をクリック後、以下のように更新中のメッセージが表示されます。 更新が完了するまで待ちます。



13. 更新が完了すると、以下のようなメッセージが表示されます。



14. 設定が確定すると、各 DNS サーバー (AD DS) 名の左に表示されていた紫のバーが消えます。



azstadds01	10.1.1.4
azstadds02	10.1.1.5
opstadds01	192.168.118.160

Note : 仮想マシンの DNS の更新

仮想マシンの DNS を更新するためには、各仮想マシンの OS を再起動する必要があります。

9.6 NTP に関する注意点 (PDC エミュレーターとは同期しない)

通常ドメイン コントローラーに昇格すると、PDC エミュレーターの役割を持ったドメイン コントローラーと時刻同期を行います。

しかしながら、Azure 上に構築した AD DS サーバーは Hyper-V の仕様により PDC エミュレーターと同期を行いません。(イベント ログ上には PDC エミュレーターとも同期を試みているログが出力されます。)

以下は「w32tm /query /status」を実行した結果となります。

ソースには「VM IC Time Synchronization Provider」と表示されています。

なお、これは Hyper-V の機能でホストマシンと時刻同期されていることを示します。



```
管理者: Windows PowerShell
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.

PS C:\$Users\$administrator> w32tm /query /status
閲インジケーター: 0 (警告なし)
階層: 2 (二次参照 - (S)NTP で同期)
精度: -6 (ティックごとに 15.625ms)
ルート遅延: 0.0000000s
ルート分散: 0.0100000s
参照 ID: 0x564D5450 (ソース IP: 86.77.84.80)
最終正常同期時刻: 2014/05/12 15:42:42
ソース: VM IC Time Synchronization Provider
ホーリング間隔: 6 (64s)

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

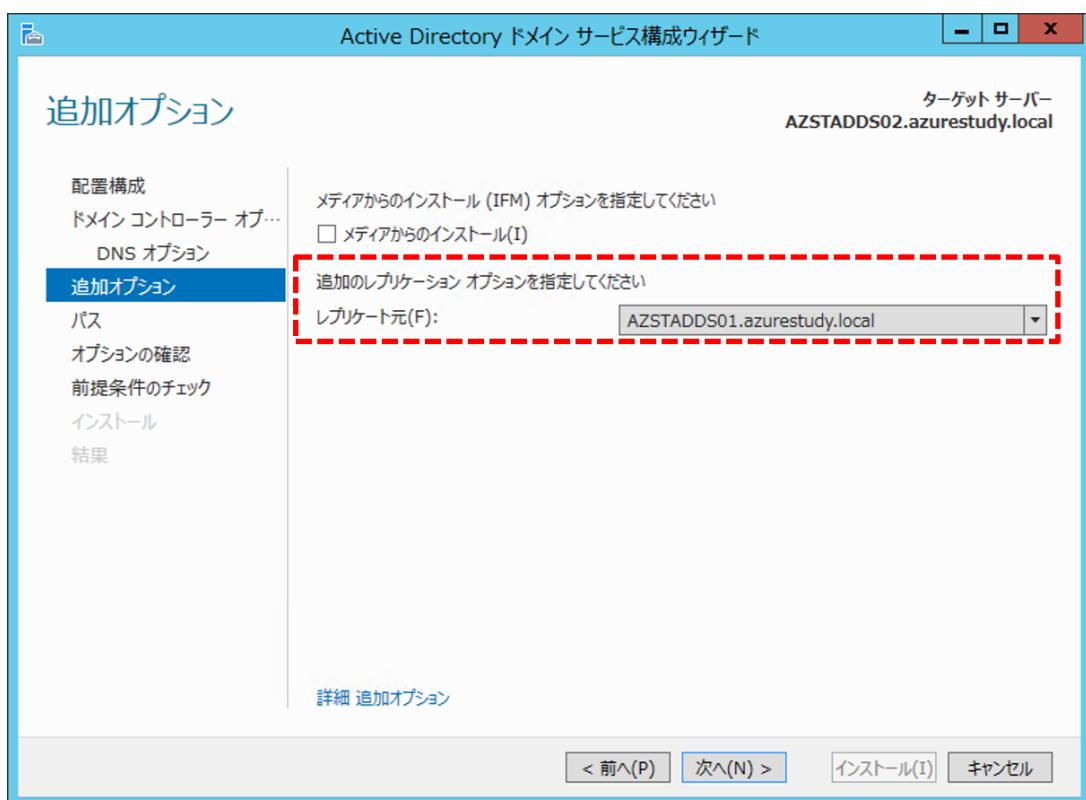
9.7 2 台目以降の AD DS を構築する際のポイント

この項では、2 台目以降の AD DS サーバー（今回は [AZSTADDS02]）を構築するためのポイントについて説明します。

➔ AD DS のレプリケート元の選択

ドメイン コントローラに昇格させる際のレプリケート元（「9.2 ドメイン コントローラへの昇格」の手順 6 にて）を Azure 上に構築した AD DS サーバー（今回は [AZSTADDS01]）とします。

レプリケーションの効率化から先に構築した AD DS サーバー [AZSTADDS01] を明示的に選択します。

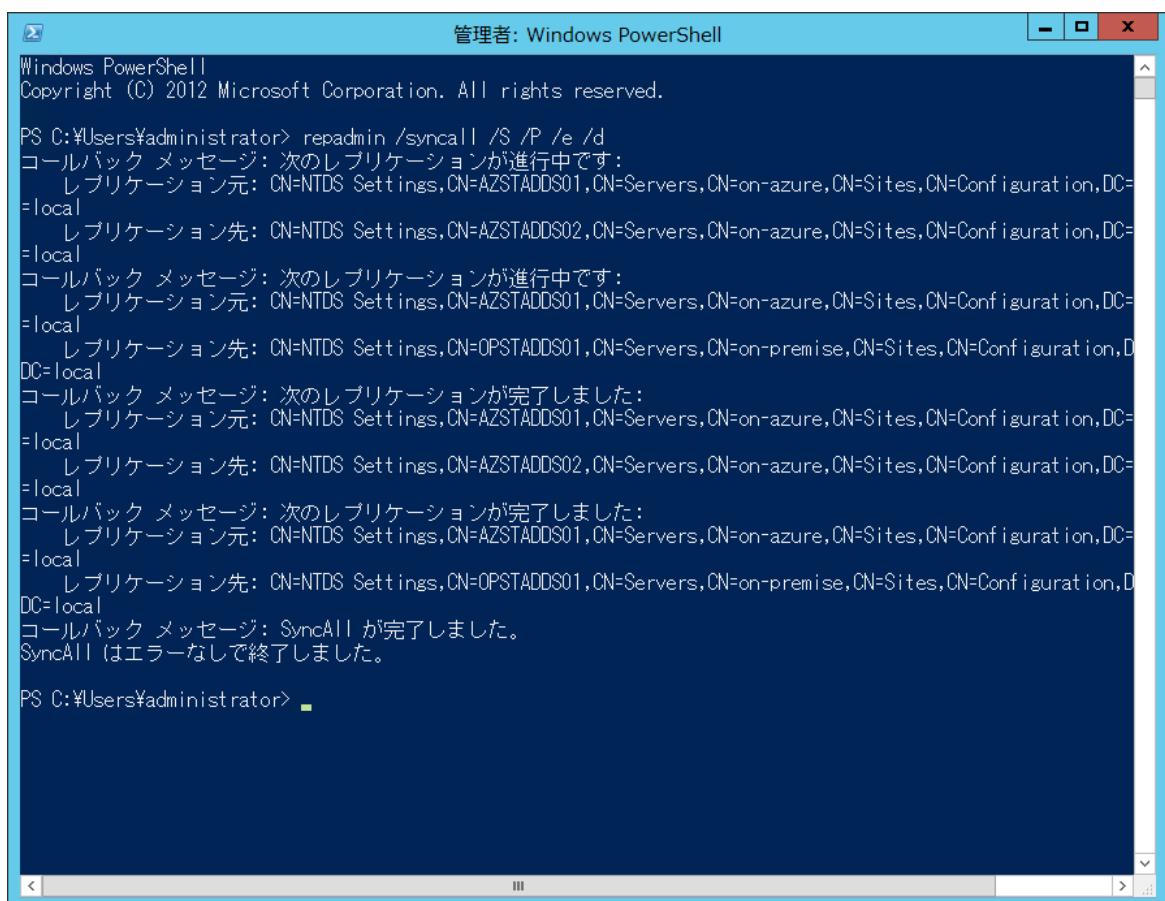


▼ 複数台の AD DS とのレプリケート確認

Azure 上に 2 台目の AD DS サーバーを構築した際には、インストール時に選択したレプリケート元とのレプリケートを確認するだけでなく、他の AD DS サーバー（オンプレミス）とのレプリケートが可能かも確認します。

[PowerShell] もしくは [コマンド プロンプト] を起動し、以下のコマンドを入力して [Enter] キーを押下します。コマンド実行結果に失敗が無いことを確認します。なお、オプションの「/S」はテストであるため、実際のレプリケーションは行われませんが、各 AD DS サーバーとレプリケーションが可能であるかの確認は可能です。

```
repadmin /syncall /S /P /e /d
```



The screenshot shows a Windows PowerShell window titled "管理者: Windows PowerShell". The command entered is "repadmin /syncall /S /P /e /d". The output displays multiple replication messages between two Active Directory Domain Services (AZSTADDS01 and AZSTADDS02) located on-premises (on-azure). The messages indicate that synchronization is in progress, has completed, and that SyncAll has finished successfully.

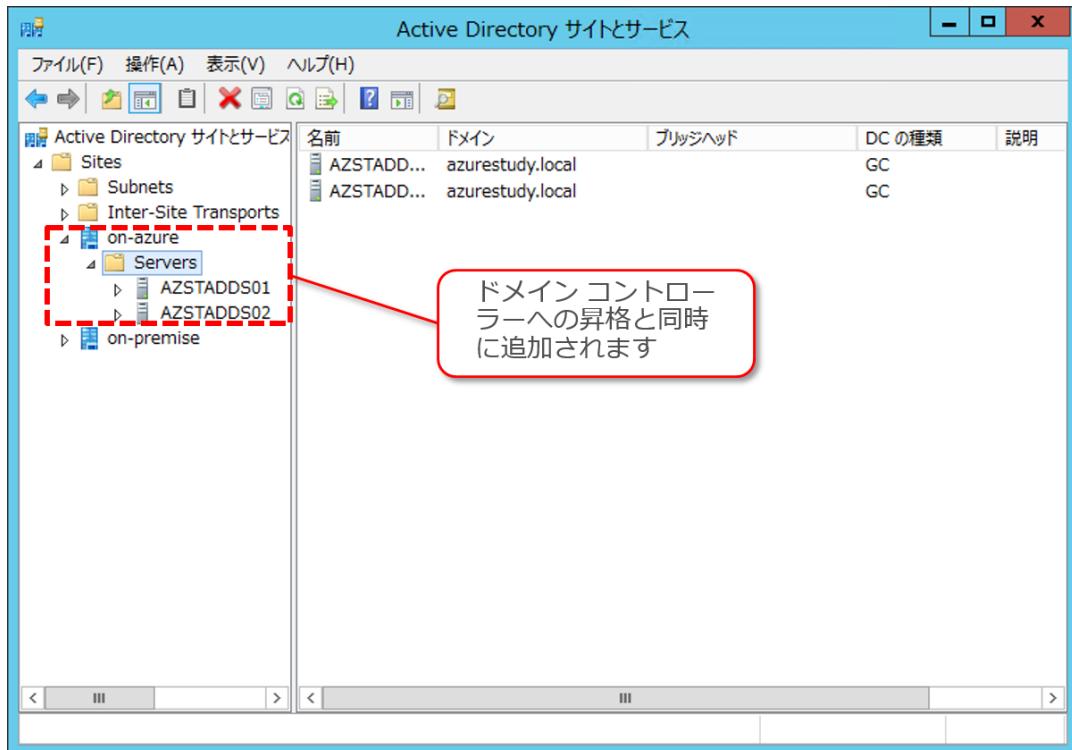
```
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.

PS C:\$Users\$administrator> repadmin /syncall /S /P /e /d
コールバック メッセージ: 次のレプリケーションが進行中です:
    レプリケーション元: CN=NTDS Settings,CN=AZSTADDS01,CN=Servers,CN=on-azure,CN=Sites,CN=Configuration,DC=local
    レプリケーション先: CN=NTDS Settings,CN=AZSTADDS02,CN=Servers,CN=on-azure,CN=Sites,CN=Configuration,DC=local
コールバック メッセージ: 次のレプリケーションが進行中です:
    レプリケーション元: CN=NTDS Settings,CN=AZSTADDS01,CN=Servers,CN=on-azure,CN=Sites,CN=Configuration,DC=local
    レプリケーション先: CN=NTDS Settings,CN=OPSTADDS01,CN=Servers,CN=on-premise,CN=Sites,CN=Configuration,DC=local
コールバック メッセージ: 次のレプリケーションが完了しました:
    レプリケーション元: CN=NTDS Settings,CN=AZSTADDS01,CN=Servers,CN=on-azure,CN=Sites,CN=Configuration,DC=local
    レプリケーション先: CN=NTDS Settings,CN=AZSTADDS02,CN=Servers,CN=on-azure,CN=Sites,CN=Configuration,DC=local
コールバック メッセージ: 次のレプリケーションが完了しました:
    レプリケーション元: CN=NTDS Settings,CN=AZSTADDS01,CN=Servers,CN=on-azure,CN=Sites,CN=Configuration,DC=local
    レプリケーション先: CN=NTDS Settings,CN=OPSTADDS01,CN=Servers,CN=on-premise,CN=Sites,CN=Configuration,DC=local
コールバック メッセージ: SyncAll が完了しました。
SyncAll はエラーなしで終了しました。

PS C:\$Users\$administrator> ■
```

▼ サイトの移動

2台目以降の AD DS サーバーのサイトの移動については、既にサブネット（「9.3 サイトとサブネットの作成」にて）を作成しているため、自動的に適切なサイトに移動されます。



STEP 10. ディレクトリ同期サーバーの セットアップ、および同期の確認

この STEP では、ディレクトリ同期ツールを使用して、社内の AD オブジェクトを Office 365 のディレクトリサービスへ同期する手順について説明します。

Note : ディレクトリ同期は社内 AD から Office 365 への片方向のみ

ディレクトリ同期は、社内 AD から Office 365 に対して一方向で行われます。

そのため、ディレクトリ同期後のオブジェクトの更新（作成や編集など）は、社内の AD 上で実施する必要があります。Office 365 上でオブジェクトを更新した場合は、社内の AD に反映されません。

この STEP では、次のことを学習します。

- ✓ UPN サフィックスの追加
- ✓ AD ユーザーの登録情報を確認
- ✓ ディレクトリ同期の有効化
- ✓ ディレクトリ同期ツール関連のインストール
- ✓ ディレクトリ同期ツールのセットアップ（同期の実行）
- ✓ ディレクトリ同期の確認
- ✓ 同期したユーザーのアクティブ化

10.1 UPN サフィックスの追加

Note : UPN サフィックスの追加が必要なケース

AD と SMTP のドメイン名が異なる場合、UPN の設定が必要となります。

この自習書の例

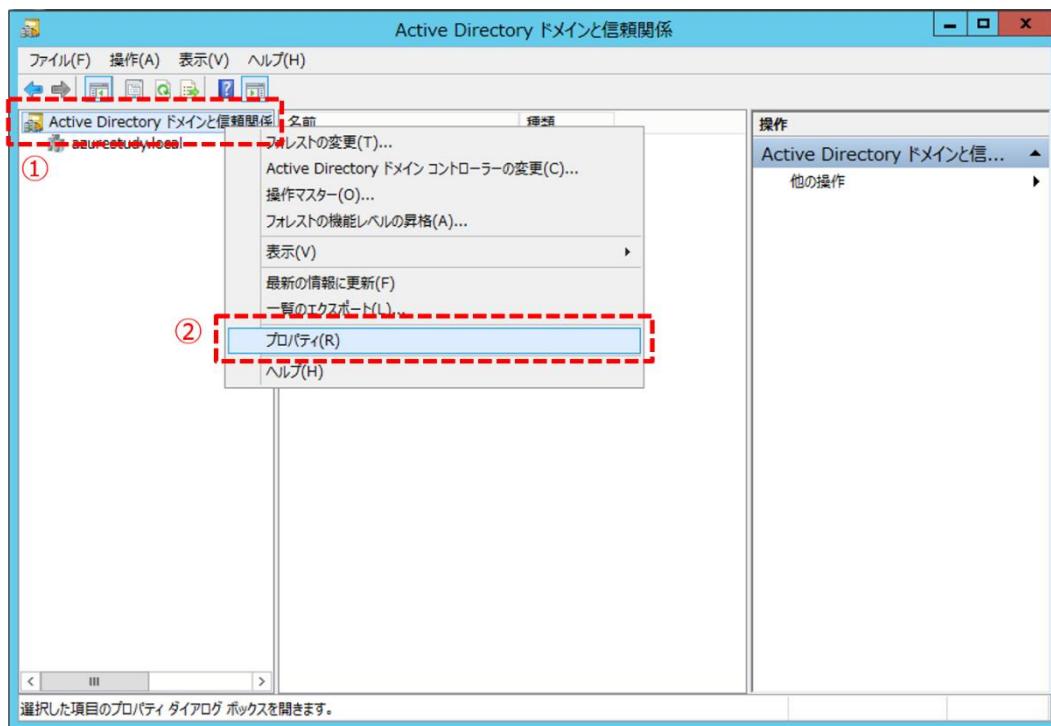
- [AD ドメイン] . . . azurestudy.local
- [SMTP ドメイン] . . . azurestudy.jp

上記の例の場合、以下の操作が必要となります。

- UPN サフィックス “azurestudy.jp” を追加
- ユーザー ログオン名を “user01@azurestudy.jp” に変更

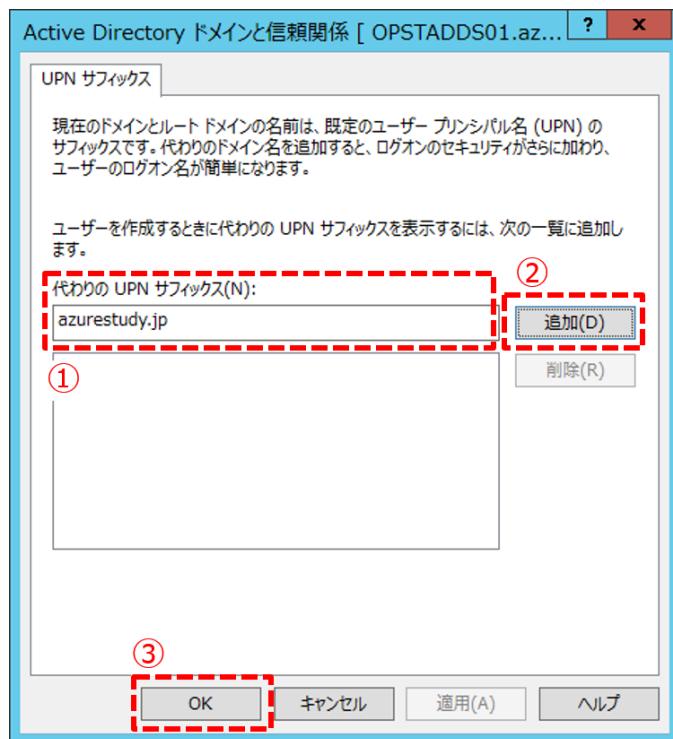
▼ UPN サフィックスの追加

1. ドメイン管理者アカウントで AD DS サーバー [AZSTADDS01] にサインインし、[Active Directory ドメインと信頼関係] を開きます。
2. 左ペインにて [Active Directory ドメインと信頼関係] を右クリックして [プロパティ] をクリックします。



企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

3. [UPN サフィックス] タブで、UPN サフィックス [azurestudy.jp] を入力して [追加] ボタンをクリックします。そして [OK] ボタンをクリックして画面を閉じます。



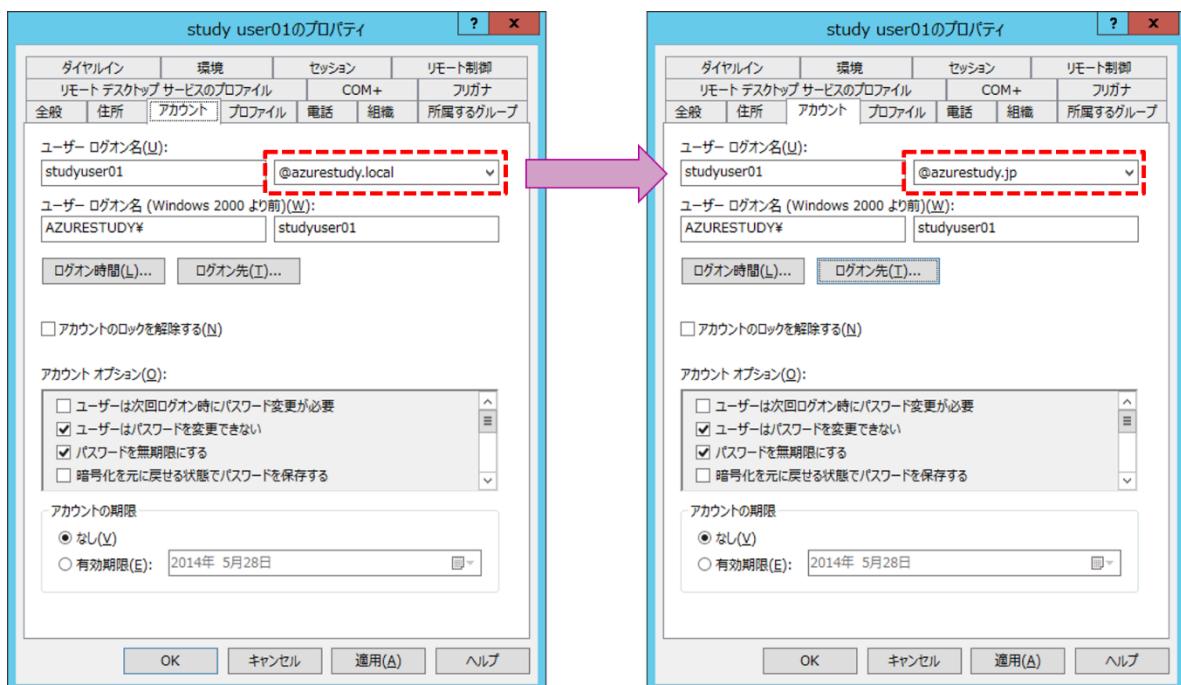
10.2 AD ユーザーの登録情報を確認

1. ドメイン管理者アカウントで AD DS サーバー [AZSTADDS01] にサインインし、[Active Directory ユーザーとコンピューター] を開きます。
2. 同期対象ユーザーのプロパティを開きます。

→ ユーザー ログオン名の確認

3. [ユーザー ログオン名] を確認します。

[アカウント] タブを開き、下図の赤枠の値を「@azurestudy.local」から「@azurestudy.jp」に変更します。



Note : Office 365 での [ユーザー ログオン名] の取り扱い

この [ユーザー ログオン名] が「Office 365 ユーザー名」となります。

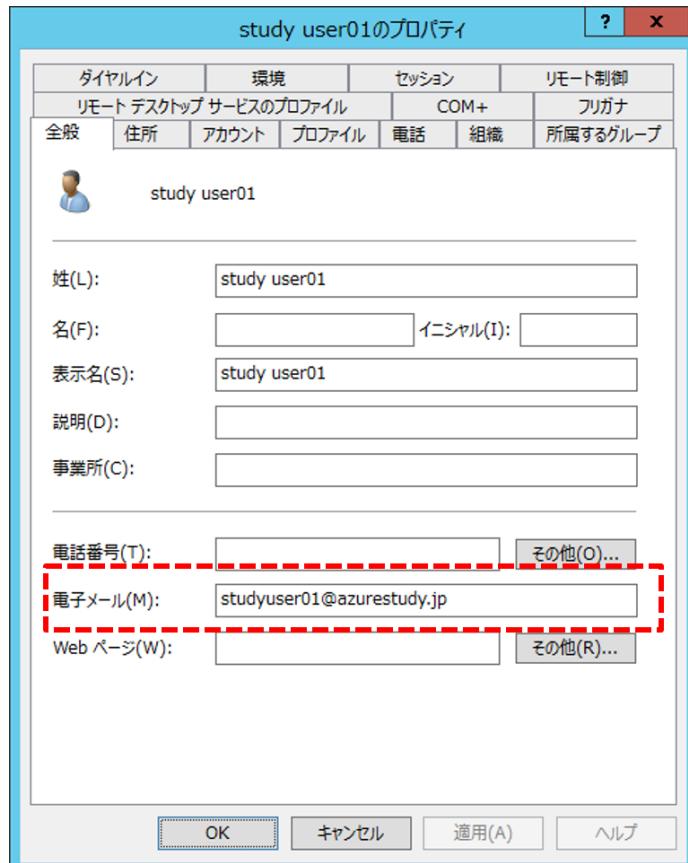
この作業は、すべての同期対象ユーザーに対して実施する必要があります。

- ・ [ユーザー ログオン名] のドメインが「STEP 5. Office 365 ヘドメインの追加、およびドメインの確認」で Office 365 に追加したドメインと異なるユーザーが同期されると、Office 365 に同期されたユーザー名は「<user01>@<tenant>.onmicrosoft.com」となってしまいます。

▼ 電子メール属性値の確認

4. [電子メール] を確認します。

[全般] タブを開き、[電子メール] 属性にそのユーザーが使用する電子メール アドレスが登録されていることを確認します。



Note : Office 365 での [電子メール] 属性値の取り扱い

この [電子メール] 属性が Exchange Online 上での「既定の (SMTP) メール アドレス」となります。

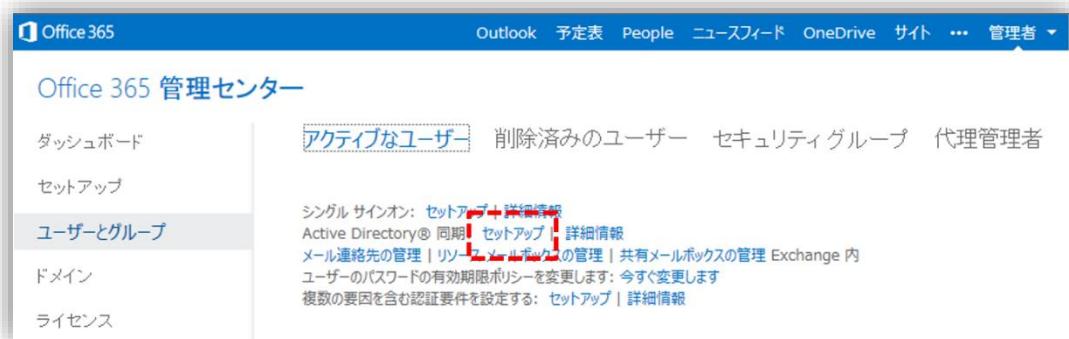
この作業は、すべての同期対象ユーザー（メールを利用するユーザー）に対して実施する必要があります。

10.3 ディレクトリ同期の有効化

1. Office 365 管理者アカウントで「Office 365 管理センター」にサインインします。
2. [管理者の概要] ページの左側にある [ユーザーとグループ] をクリックします。

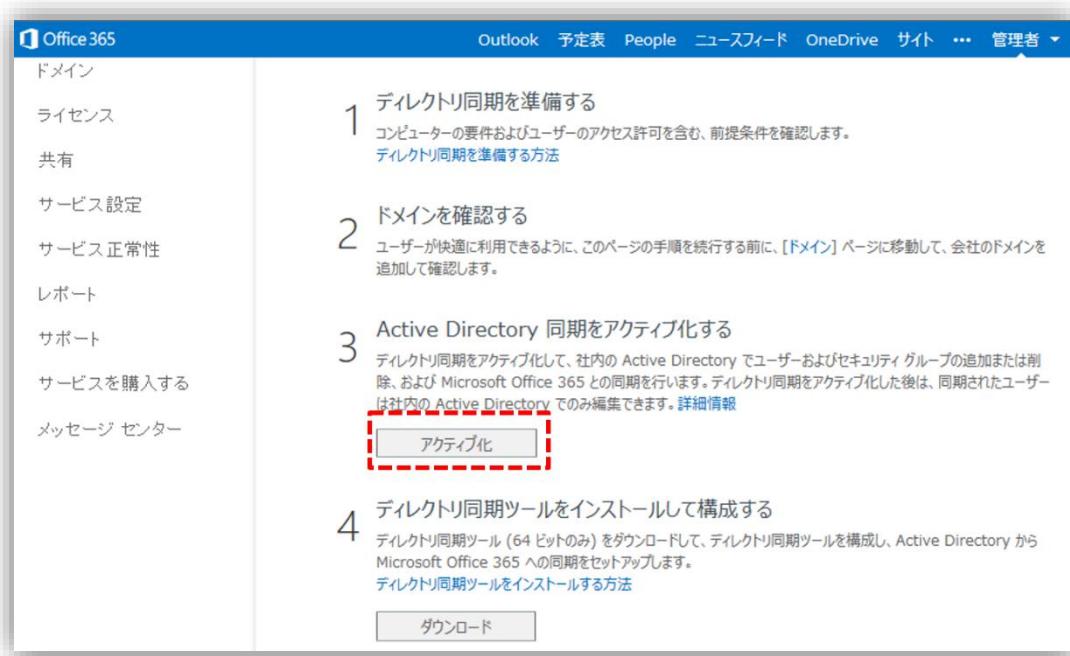


3. [アクティブなユーザー] ページにて [Active Directory® 同期] にある [セットアップ] をクリックします。



企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

4. [Active Directory 同期のセットアップと管理] ページにて [3 Active Directory 同期をアクティブ化する] にある [アクティブ化] をクリックします。



5. [Active Directory 同期をアクティブ化しますか?] という確認画面が表示されます。 [アクティブ化] をクリックします。



企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

6. [Active Directory 同期のセットアップと管理] ページに戻り、[3 Active Directory 同期をアクティブ化する] の下に「Active Directory 同期がアクティブ化されています。」とメッセージが表示されていることを確認します。

Office 365 Admin Center - Active Directory 同期

1 ディレクトリ同期を準備する
コンピューターの要件およびユーザーのアクセス許可を含む、前提条件を確認します。
[ディレクトリ同期を準備する方法](#)

2 ドメインを確認する
ユーザーが快適に利用できるように、このページの手順を続行する前に、[ドメイン] ページに移動して、会社のドメインを追加して確認します。

3 Active Directory 同期をアクティブ化する
ディレクトリ同期をアクティブ化して、社内の Active Directory でユーザーおよびセキュリティ グループの追加または削除、および Microsoft Office 365 との同期を行います。ディレクトリ同期をアクティブ化した後は、同期されたユーザーは社内の Active Directory でのみ編集できます。
[詳細情報](#)
Active Directory 同期がアクティブ化されています。

4 ディレクトリ同期ツールをインストールして構成する
ディレクトリ同期ツール (64 ビットのみ) をダウンロードして、ディレクトリ同期ツールを構成し、Active Directory から Microsoft Office 365 への同期をセットアップします。
[ディレクトリ同期ツールをインストールする方法](#)

[ダウンロード](#)

7. [アクティブなユーザー] ページに戻り、[Active Directory® 同期] にあるステータスが「セットアップ」から「管理」に変わっていることを確認します。

Office 365 管理センター - アクティブなユーザー

アクティブなユーザー 削除済みのユーザー セキュリティ グループ 代理管理者

シングル サインオン: [セットアップ](#) | [詳細情報](#)
Active Directory® 同期: 非アクティブ | [管理](#) | [詳細情報](#)

メール連絡先の管理 | リースメールボックスの管理 | 共有メールボックスの管理 Exchange 内
ユーザーのパスワードの有効期限ポリシーを変更します: 今すぐ変更します
複数の要因を含む認証要件を設定する: [セットアップ](#) | [詳細情報](#)

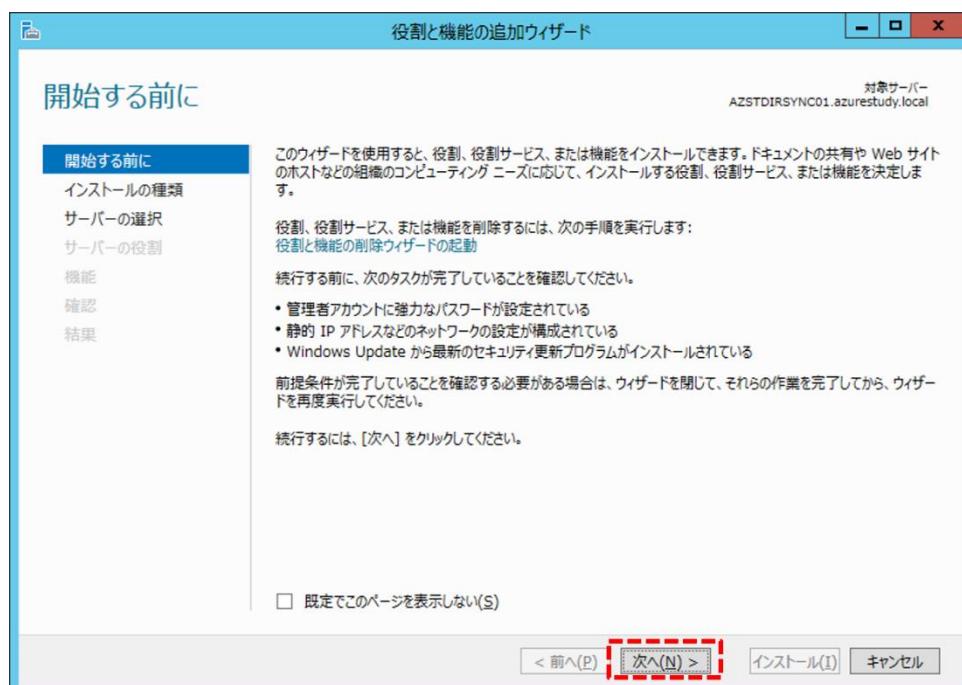
10.4 ディレクトリ同期ツール関連のインストール

◆ .NET Framework 3.5 Features のインストール

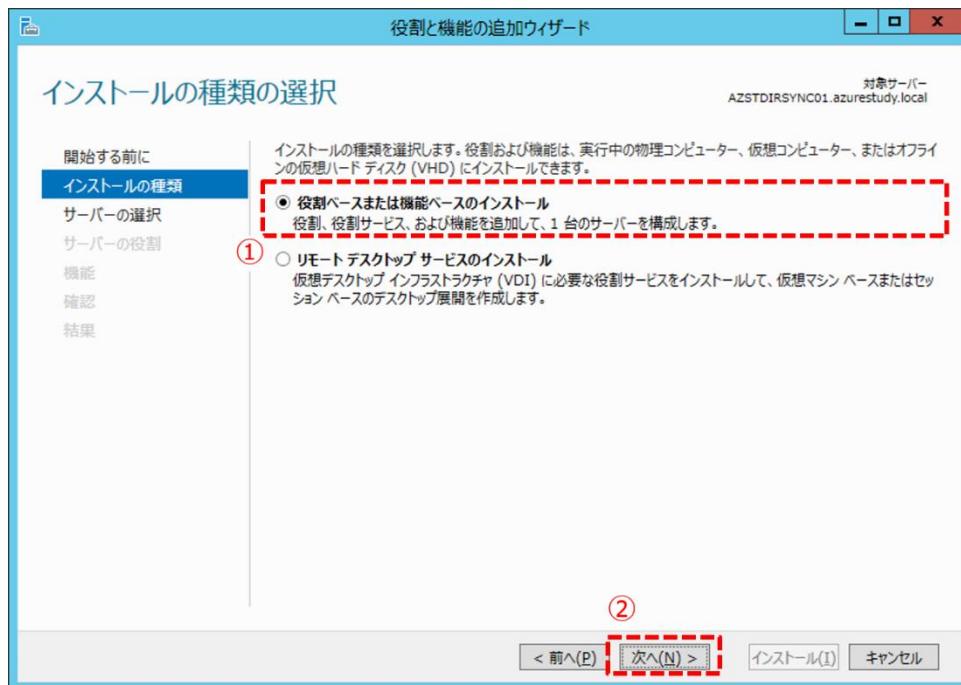
1. ドメイン管理者アカウントでディレクトリ同期サーバー [AZSTDIRSYNC01] にサインインし、[サーバー マネージャー] を開きます。
2. [管理] メニュー > [役割と機能の追加] をクリックします。



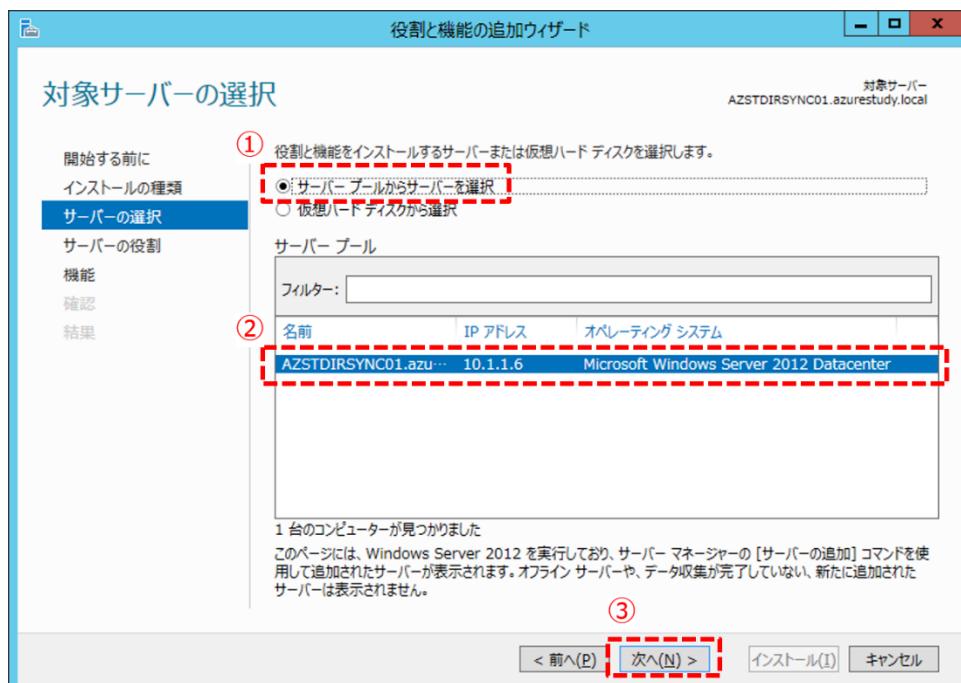
3. [役割と機能の追加ウィザード] 画面が開きます。[開始する前に] ページにて [次へ] ボタンをクリックします。



4. [インストールの種類の選択] ページにて [役割ベースまたは機能ベースのインストール] を選択して [次へ] ボタンをクリックします。

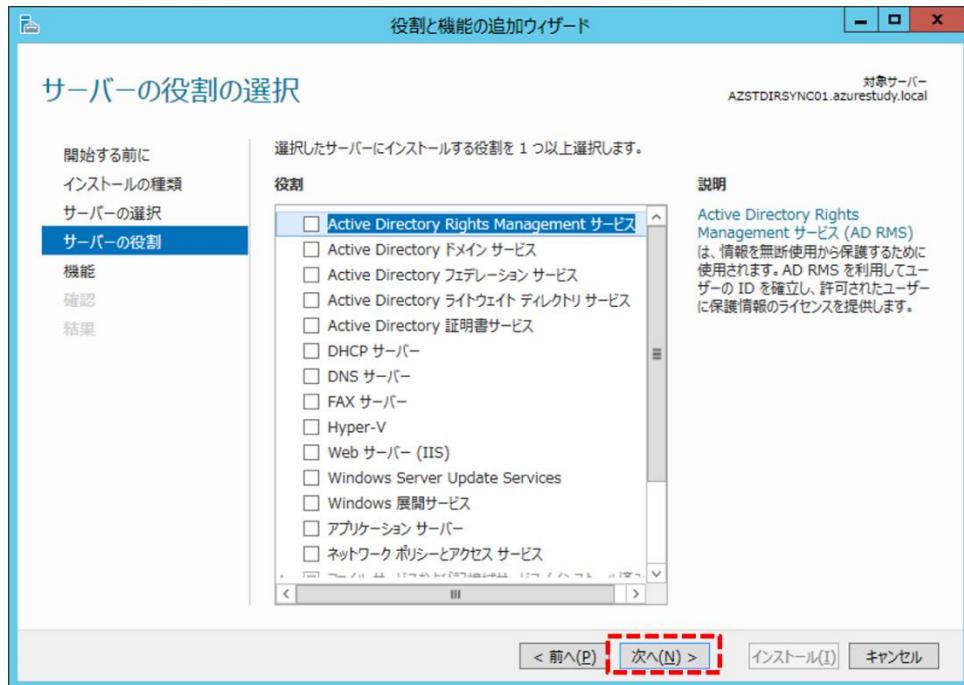


5. [対象サーバーの選択] ページにて [サーバー プールからサーバーを選択] を選択し、[サーバー プール] からディレクトリ同期サーバー [AZSTDIRSYNC01] を選択して [次へ] ボタンをクリックします。

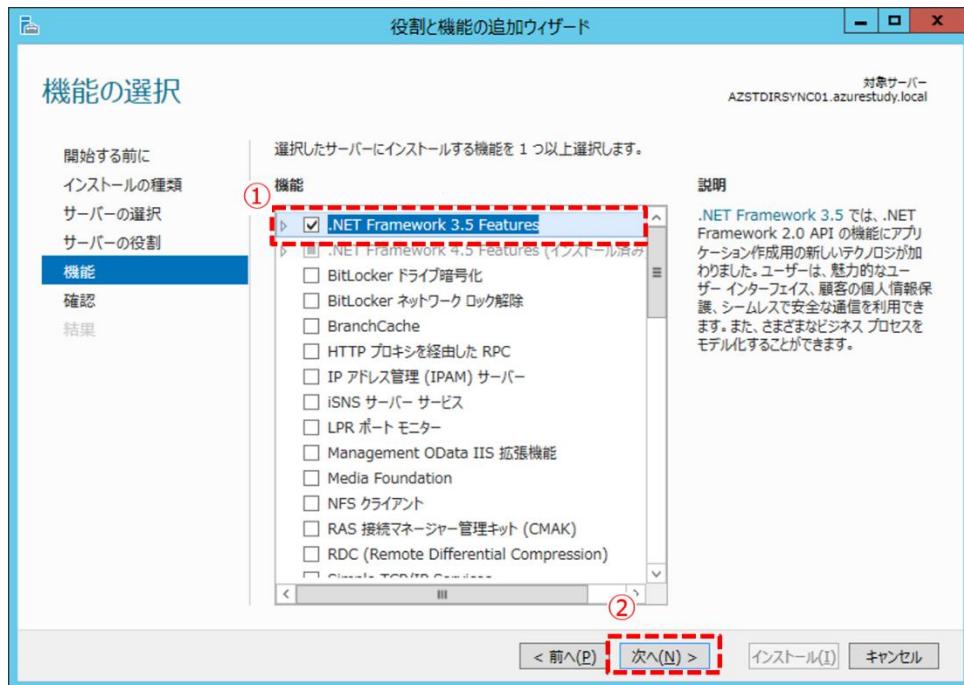


企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

6. [サーバーの役割の選択] ページにて [次へ] ボタンをクリックします。

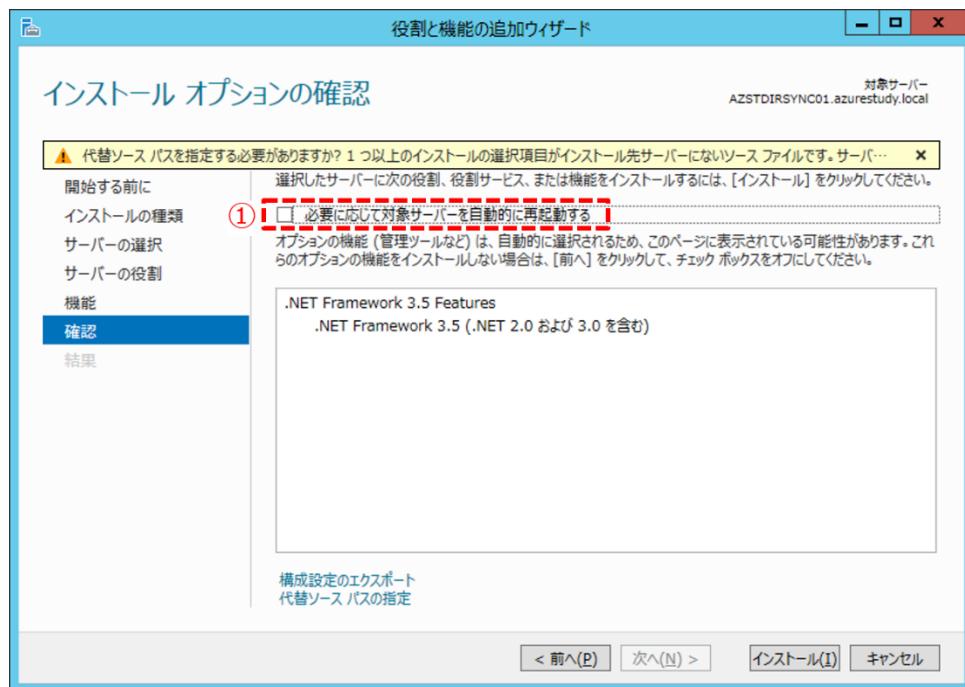


7. [機能の選択] ページにて [機能] 一覧から [.NET Framework 3.5 Features] チェックボックスにチェックを付けて [次へ] ボタンをクリックします。

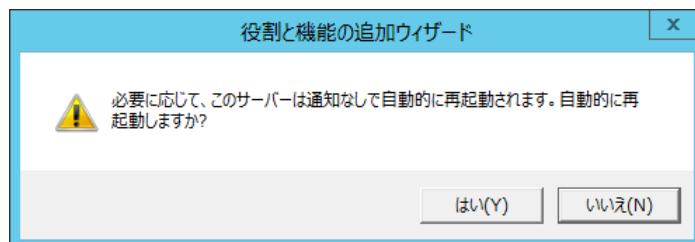


企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

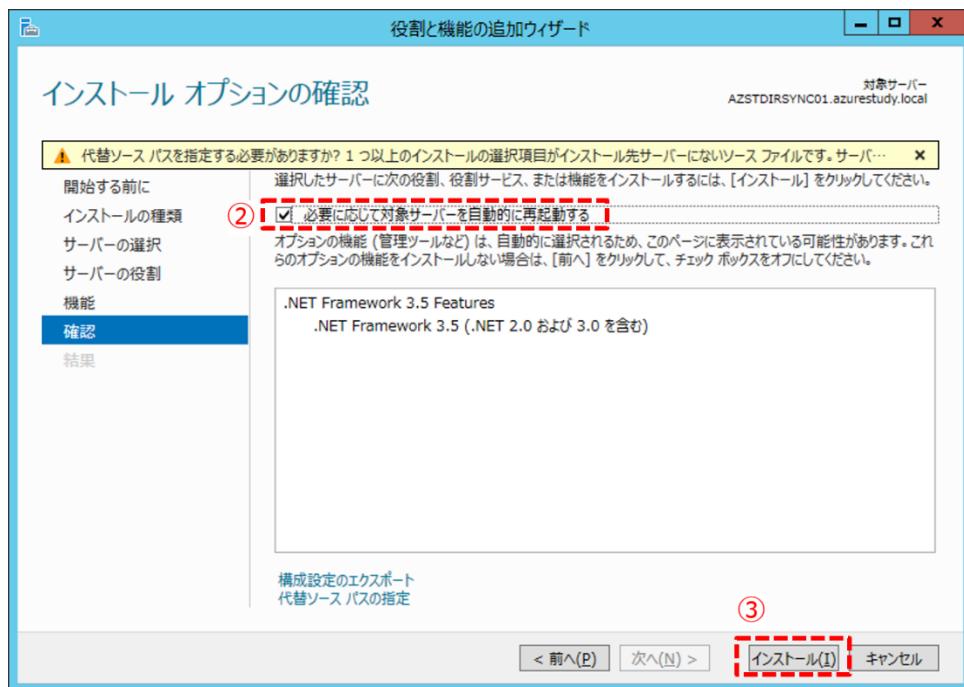
8. [インストール オプションの確認] ページにて [必要に応じて対象サーバーを自動的に再起動する] チェックボックスにチェックを付けます。



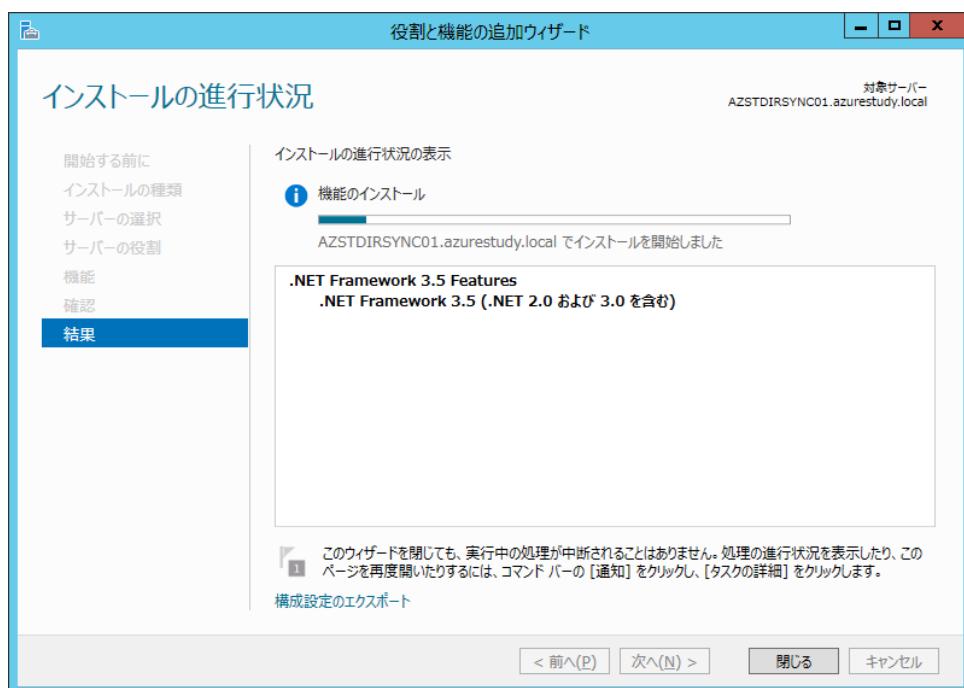
以下のメッセージ ボックスが開くので、[はい] ボタンをクリックして閉じます。



企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携 [インストール オプションの確認] ページに戻り、[必要に応じて対象サーバーを自動的に再起動する] チェックボックスにチェックが付いていることを確認して [インストール] ボタンをクリックします。

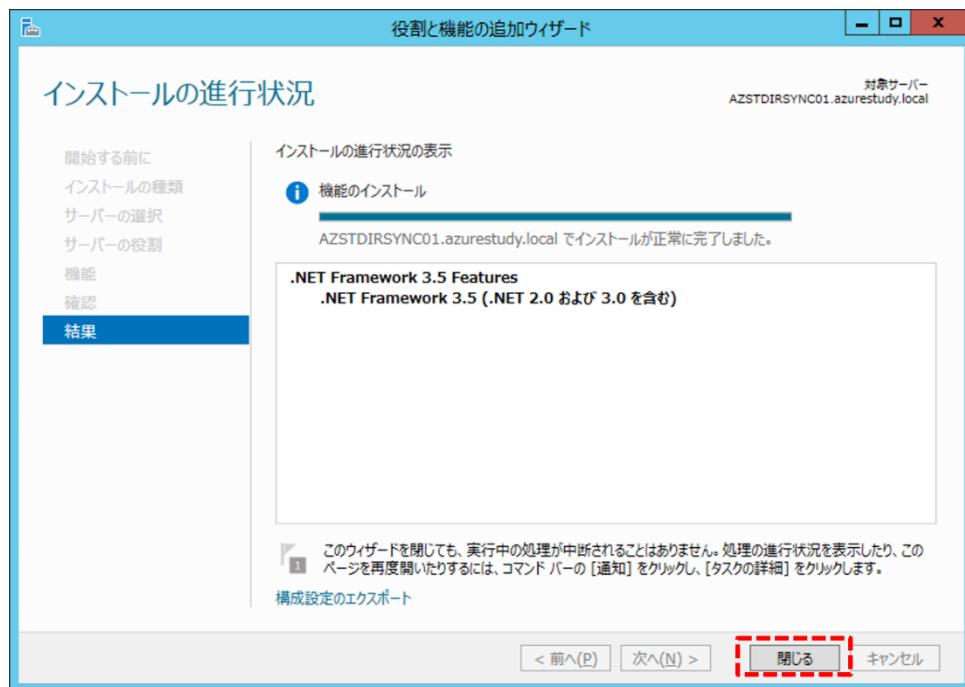


9. インストールが完了するまで待ちます。



企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

10. 「AZSTDIRSYNC01.azurestudy.local でインストールが正常に完了しました。」とメッセージが表示されたら [閉じる] ボタンをクリックして閉じます。



➔ ディレクトリ同期ツールをダウンロード

11. Office 365 管理者アカウントで「Office 365 管理センター」にサインインします。
12. [管理者の概要] ページの左側にある [ユーザーとグループ] をクリックします。



13. [アクティブなユーザー] ページにて [Active Directory® 同期] にある [管理] をクリックします。



企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

14. [Active Directory 同期のセットアップと管理] ページにて [4 ディレクトリ同期ツールをインストールして構成する] にある [ダウンロード] をクリックして「ディレクトリ同期ツール (64 ビット版)」をダウンロードします。



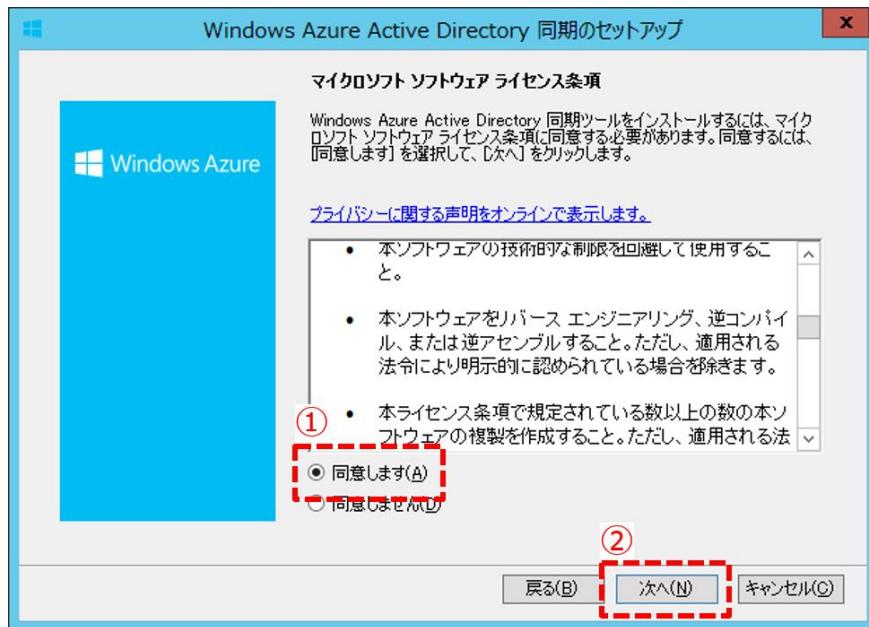
➔ ディレクトリ同期ツールをインストール

15. ドメイン管理者アカウントでディレクトリ同期サーバー [AZSTDIRSYNC01] にサインインし、手順 11 ~ 14 でダウンロードした「ディレクトリ同期ツール (64 ビット版)」を任意の場所にコピーします。
16. [dirsync-jc.exe] をダブルクリックして [Windows Azure Directory 同期のセットアップ] を起動します。
17. [ようこそ] 画面にて [次へ] ボタンをクリックします。

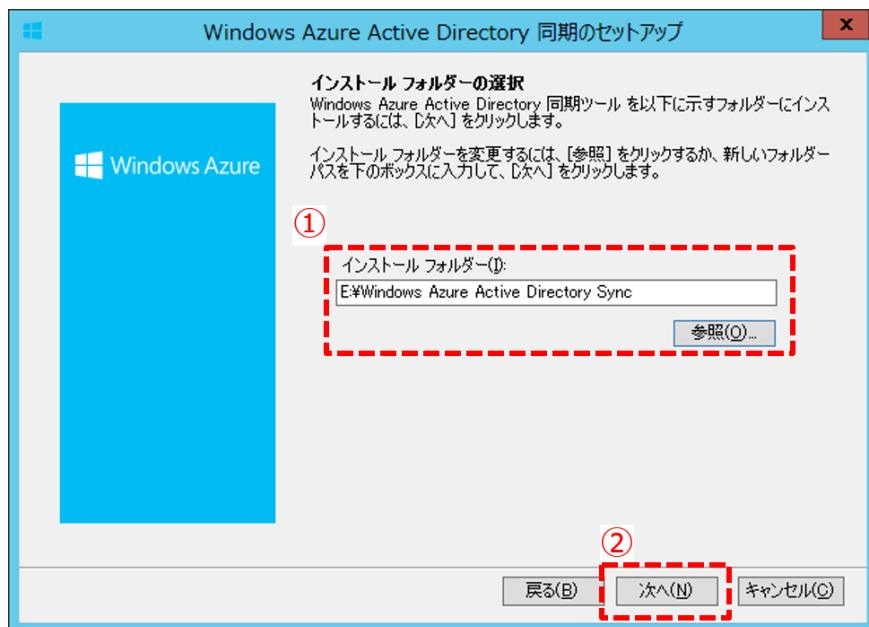


企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

18. [マイクロソフト ソフトウェア ライセンス条項] 画面にて [ソフトウェア ライセンス条項] をご確認いただき、同意される場合は [同意します] を選択して [次へ] ボタンをクリックします。

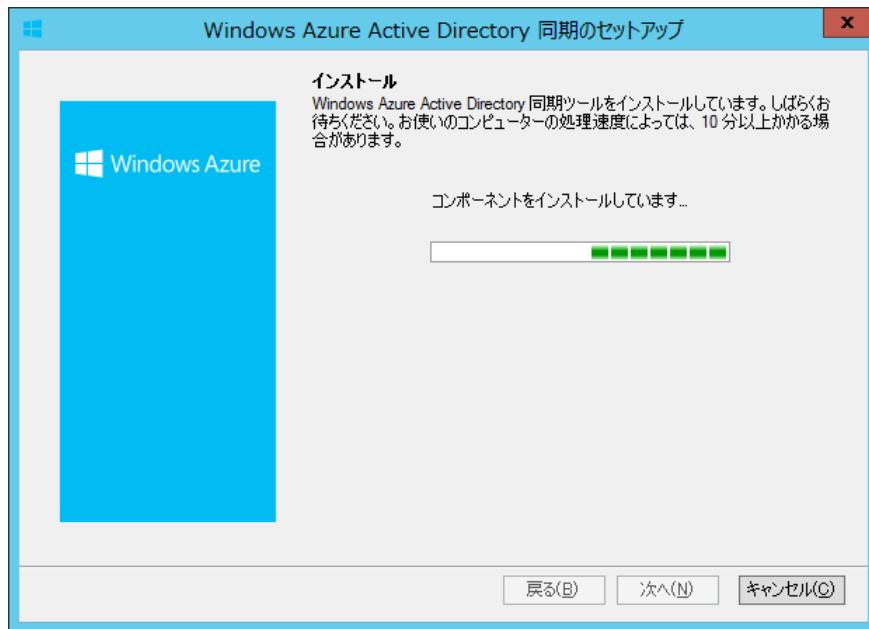
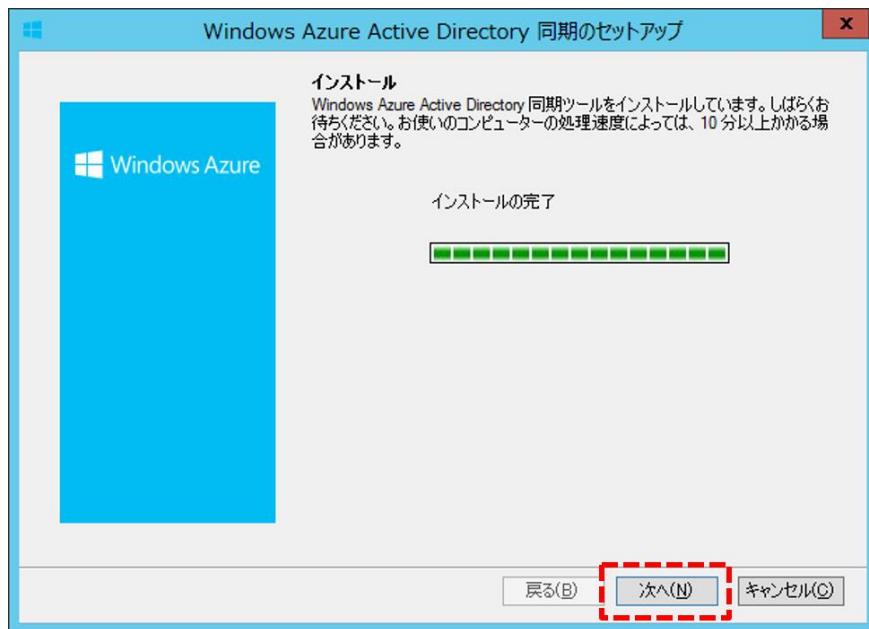


19. [インストール フォルダーの選択] 画面にてディレクトリ同期ツールのインストール先を、追加したディスク (今回は E ドライブ) に変更して [次へ] ボタンをクリックします。



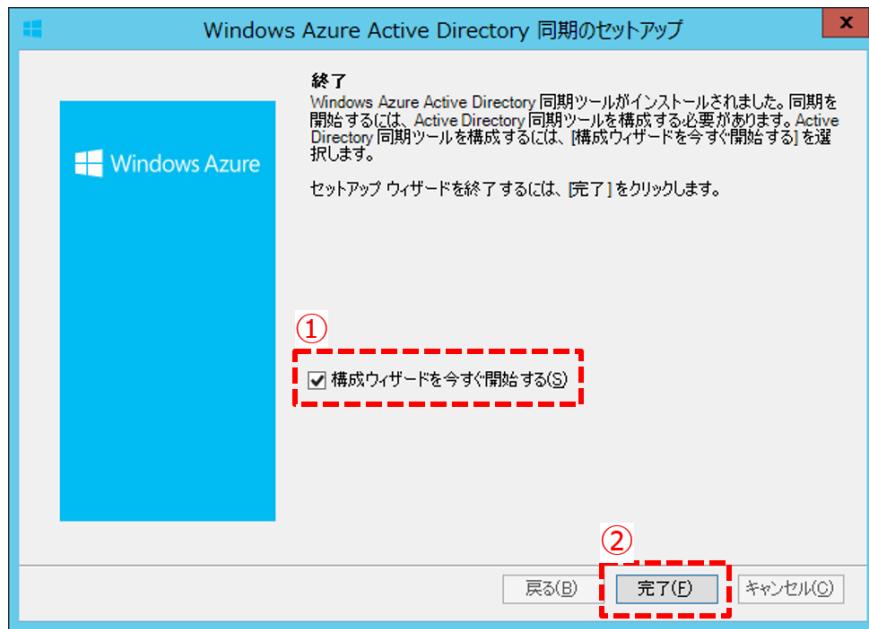
Note : インストール フォルダーについて

ディレクトリ同期は OS ディスク (C ドライブ) にインストールするのではなく、別途データ ディスクを追加して、そのディスクにインストールします。

20. インストールが完了するまで待ちます。**21. 「インストールの完了」とメッセージが表示されたら、 [次へ] ボタンをクリックします。**

企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

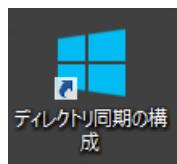
22. 続けてディレクトリ同期ツールのセットアップを行う場合は [構成ウィザードを今すぐ開始する] チェックボックスにチェックを付けます。 [完了] ボタンをクリックして閉じます。

**Note : ディレクトリ同期ツールのセットアップ**

ディレクトリ同期ツールのセットアップについては、「10.6 ディレクトリ同期ツールのセットアップ（同期の実行）」にて説明しています。

10.5 ディレクトリ同期ツールのセットアップ（同期の実行）

- ドメイン管理者アカウントでディレクトリ同期サーバー [AZSTDIRSYNC01] にサインインし、デスクトップにある [ディレクトリ同期の構成] ショートカットをダブルクリックして [Windows Azure Active Directory 同期ツールの構成ウィザード] 起動します。

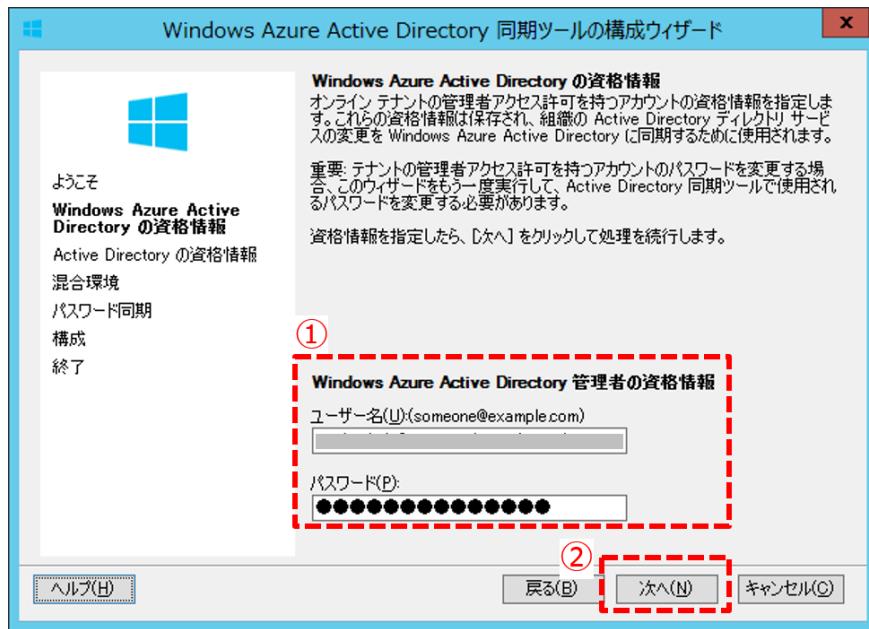


- [ようこそ] 画面にて [次へ] ボタンをクリックします。

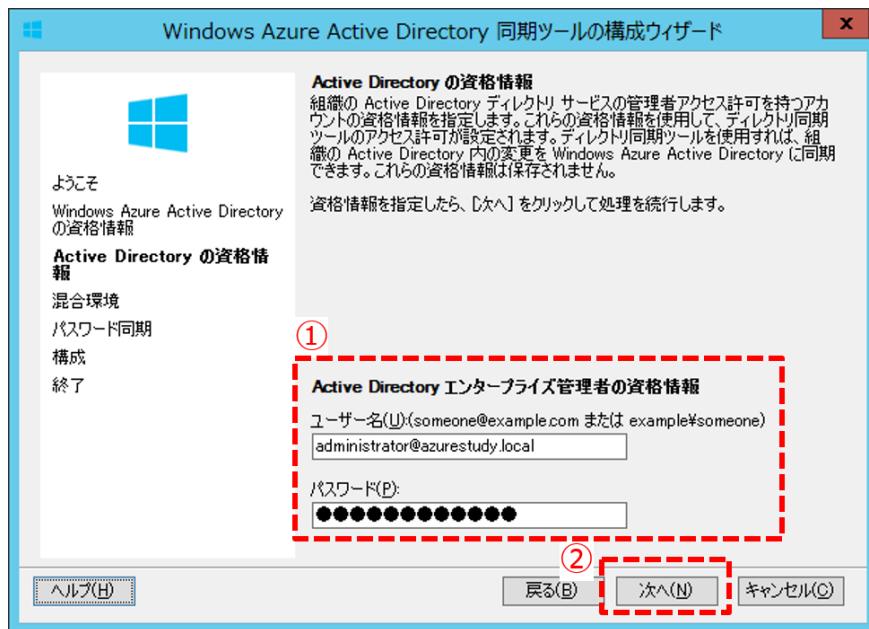


企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

3. [Windows Azure Active Directory の資格情報] 画面にて Office 365 管理者アカウントのユーザー名、パスワードを入力して [次へ] ボタンをクリックします。

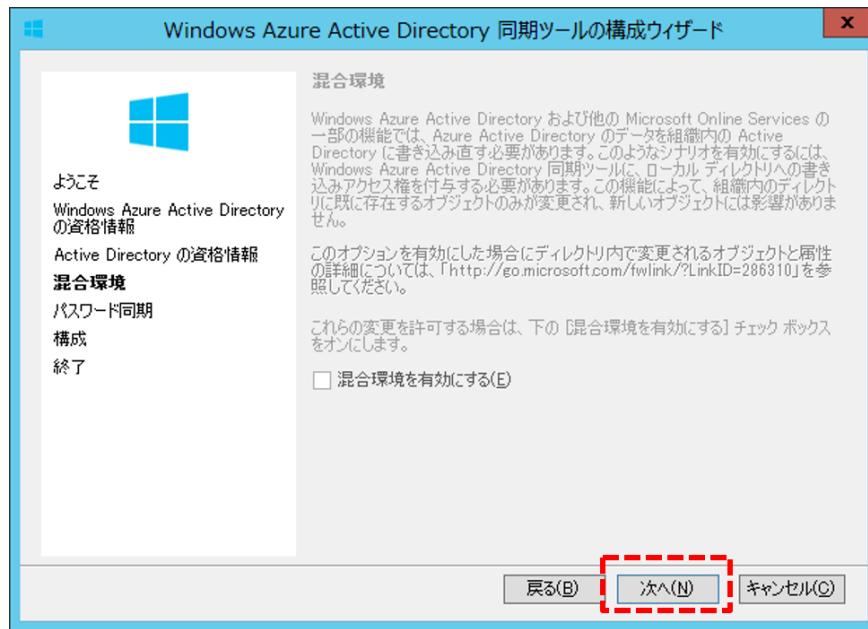


4. [Active Directory の資格情報] 画面にて ドメイン管理者アカウントのユーザー名、パスワードを入力して [次へ] ボタンをクリックします。



企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

5. [混合環境] 画面にて設定項目がグレーアウトしていることを確認して [次へ] ボタンをクリックします。

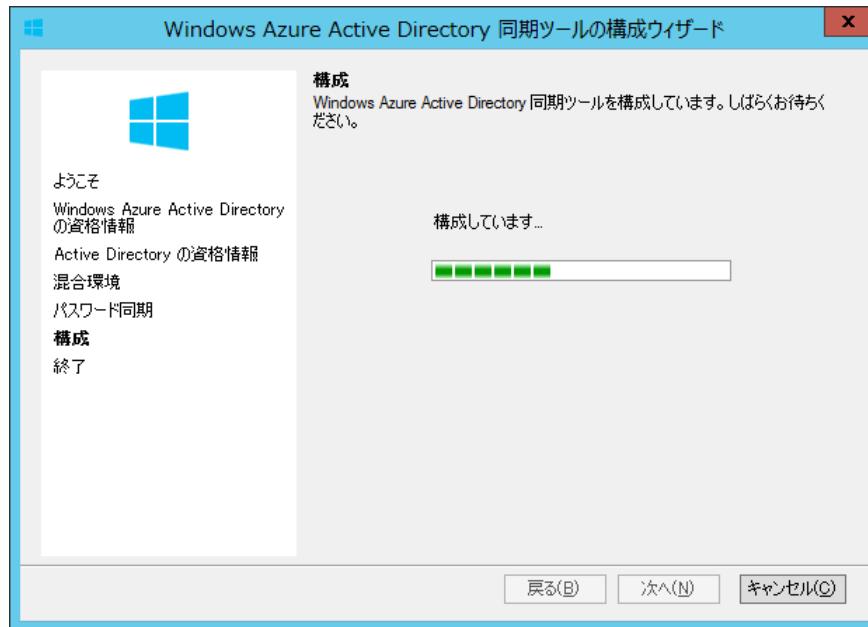


6. [パスワード同期] 画面にて [パスワード同期を有効にする] チェックボックスにチェックを外して [次へ] ボタンをクリックします。

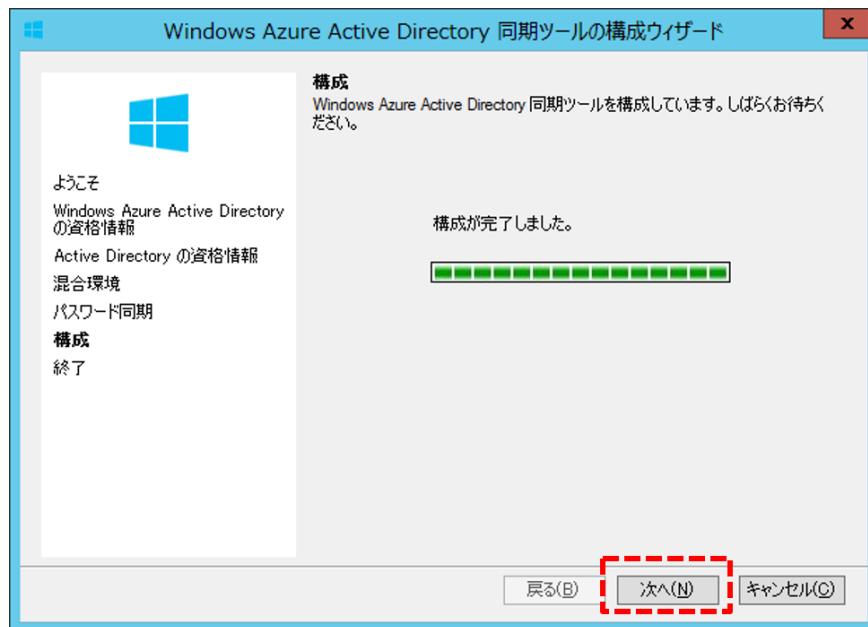


企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

7. ディレクトリ同期ツールの構成のセットアップが完了するまで待ちます。

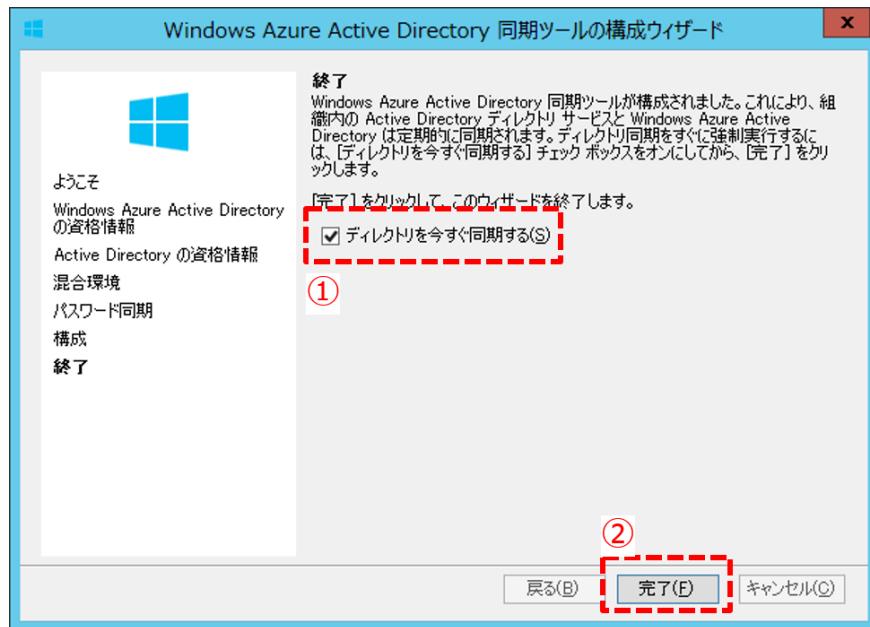


8. 「構成が完了しました。」とメッセージが表示されたら、[次へ] ボタンをクリックします。



企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

9. [終了] 画面にて [ディレクトリを今すぐ同期する] チェックボックスにチェックを付けて [完了] ボタンをクリックします。すると、社内 AD から Office 365 への同期が始まります。



以下のメッセージボックスが開きます。 [OK] ボタンをクリックして閉じます。



Note : 強制的に同期を行う場合

手動による強制的に同期を行いたい場合は、この項の手順を再度実施することで実行することができます。

Note : ディレクトリ同期ツールセットアップ後にいずれかの資格情報を変更した場合

ディレクトリ同期ツールセットアップ後に、Office 365 管理者アカウントまたはドメイン管理者のパスワードを変更してしまった場合、社内 AD から Office 365 への同期が失敗します。

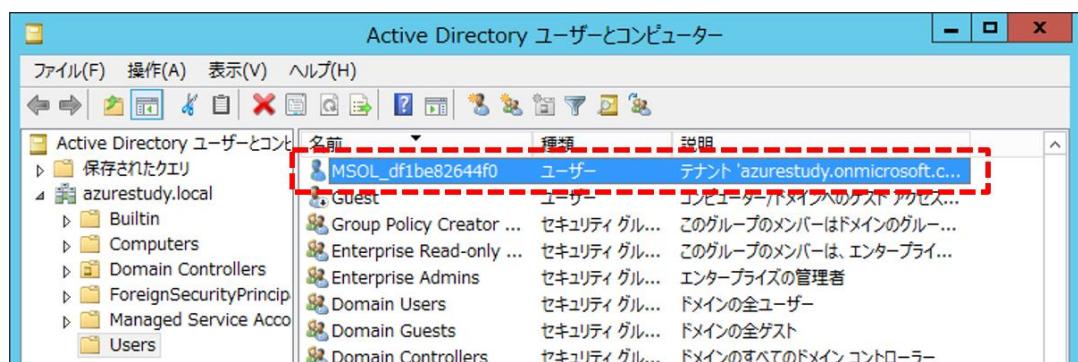
いずれかの資格情報を変更した場合は、再度この項の作業を実施してください。

10.6 ディレクトリ同期の確認

ディレクトリ同期サーバーのセットアップが完了したら、以下の内容を基にディレクトリ同期サービスが正常に稼動しているか確認を行います。

➔ AD DS サーバーでの確認

1. ドメイン管理者アカウントでドメイン コントローラー [OPSTADDS01] サインインし、[Active Directory ユーザーとコンピューター] を開きます。
2. OU [User] に ディレクトリ同期サービスのサービスアカウントである「MSOL_*****」というユーザー（ここでは「MSOL_df1be82644f0」）が存在することを確認します。



このサービス アカウントはディレクトリ同期後、AD 上で行われたオブジェクトの変更内容を読み取るために使用されます。

➔ ディレクトリ同期サーバーでの確認

3. ドメイン管理者アカウントでディレクトリ同期サーバー [AZSTDIRSYNC01] にサインインします。
4. [サービス] を開き、以下の表で挙げたサービスのプロパティを確認します。

	スタートアップの種類	サービスの状態	アカウント
Forefront Identity Manager Synchronization Service	自動	実行中(開始)	「.¥AAD_*****」 ※同期ツールにより設定されるアカウント
Windows Azure Active Directory Sync Service	自動	実行中(開始)	「.¥AAD_*****」 ※同期ツールにより設定されるアカウント
Microsoft Online Services Sign-in Assistant	自動	実行中(開始)	ローカル システム アカウント

5. [イベント ビューアー] を開き、以下のイベント ログが出力されていることを確認します。
 - ・ 3 時間毎の自動同期および手動による強制同期の際、イベント ログに以下のエントリーがあることを確認して下さい。

項目	内容
ログ保存場所	[Windows ログ] > [Application]
ソース	Directory Synchronization
イベント ID	114
ログの内容 (例)	Export cycle completed. Tracking id: 3a5514a2-dbb2-4e6c-86e7-6194d60a574b

6. 別途 SQL Server の完全なインスタンスをインストールした場合は、[SQL Server Management Studio] を起動して、[Microsoft Identity Integration Server] データベースがあることを確認します。
 - ・ この自習書では、SQL Server をインストールしていないため、確認は不要となります。

▼ Office 365 での確認

7. Office 365 管理者アカウントで「Office 365 管理センター」にサインインします。
8. [管理者の概要] ページの左側にある [ユーザーとグループ] をクリックします。



9. [Active Directory® 同期] のステータスに [最後の同期] と表示されていることを確認します。



企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

10. [アクティブなユーザー] ページに AD 上のユーザーが表示されていることを確認します。

The screenshot shows the Office 365 Management Center interface. On the left, there's a sidebar with various management options like Dashboard, Setup, User & Groups, Domain, License, Share, Service Settings, Service Health, Reports, Support, and Message Center. The 'User & Groups' option is selected. In the main content area, the title is 'Active Users'. Below it, there's a note about sing-in sources and synchronization status. The main part is a table listing users:

表示名	ユーザー名	状態
ADFS Service	adfssvc@azurestudy.onmicrosoft.com	Active Directory と同期済み
office001	office001@azurestudy.onmicrosoft.com	Active Directory と同期済み
office002	office002@azurestudy.onmicrosoft.com	Active Directory と同期済み
sales001	sales001@azurestudy.onmicrosoft.com	Active Directory と同期済み
sales002	sales002@azurestudy.onmicrosoft.com	Active Directory と同期済み
study user01	studyuser01@azurstudy.jp	Active Directory と同期済み
study user02	studyuser02@azurstudy.jp	Active Directory と同期済み
study user03	studyuser03@azurstudy.jp	Active Directory と同期済み
study user04	studyuser04@azurstudy.jp	Active Directory と同期済み
study user05	studyuser05@azurstudy.jp	Active Directory と同期済み
studyadmin	studyadmin@azurstudy.onmicrosoft.com	クラウド内

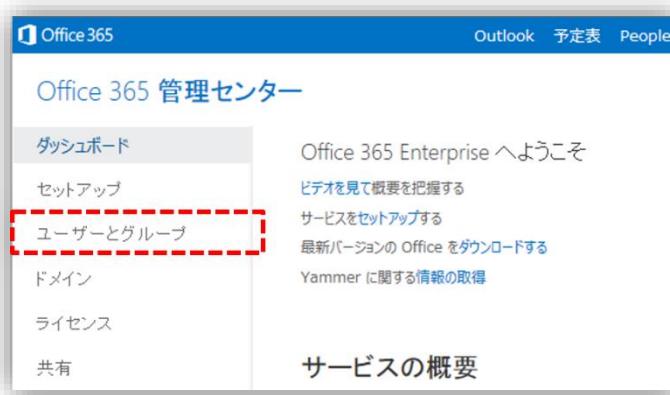
11. セキュリティグループまたは配布グループがある場合は、必要に応じて表示されていることを確認します。

The screenshot shows the Office 365 Management Center interface. The sidebar is identical to the previous screenshot. The main content area has a title 'Active Users' followed by 'Distribution Groups | Security Groups | Exchange' and a note about managing security and distribution groups. The main part is a table listing distribution groups:

表示名	型	ステータス
DnsAdmins	セキュリティ グループ	Active Directory と同期済み
DnsUpdateProxy	セキュリティ グループ	Active Directory と同期済み
WinRMRemoteWMIUsers__	セキュリティ グループ	Active Directory と同期済み
営業	セキュリティ グループ	Active Directory と同期済み
経理	セキュリティ グループ	Active Directory と同期済み

10.7 同期したユーザーのアクティビ化

1. Office 365 管理者アカウントで「Office 365 管理センター」にサインインします。
2. [管理者の概要] ページの左側にある [ユーザーとグループ] をクリックします。



3. [アクティブなユーザー] ページにて Office 365 のライセンスを与えるユーザーごとにチェックボックスにチェックを付け、右側にある [同期済みユーザーのアクティビ化] をクリックします。

The screenshot shows the 'Active Users' page in the 'Office 365 Management Center'. The left sidebar has links: 'ダッシュボード', 'セットアップ', 'ユーザーとグループ' (highlighted with a red box), 'ドメイン', 'ライセンス', '共有', 'サービス設定', 'サービス正常性', 'レポート', 'サポート', 'サービスを購入する', and 'メッセージセンター'. The main area has tabs: 'アクティブなユーザー' (selected), '削除済みのユーザー', 'セキュリティグループ', and '代理管理者'. Below the tabs, there's a message about single sign-on settings. The main content is a table of users:

表示名	ユーザー名	状態
<input type="checkbox"/> ADFS Service	adffsvc@azurstudy.onmicrosoft.com	Active Directory と同期
<input type="checkbox"/> office001	office001@azurstudy.onmicrosoft.com	Active Directory と同期
<input type="checkbox"/> office002	office002@azurstudy.onmicrosoft.com	Active Directory と同期
<input type="checkbox"/> sales001	sales001@azurstudy.onmicrosoft.com	Active Directory と同期
<input checked="" type="checkbox"/> sales002	sales002@azurstudy.onmicrosoft.com	Active Directory と同期
<input checked="" type="checkbox"/> study user01	studyuser01@azurstudy.jp	Active Directory と同期
<input checked="" type="checkbox"/> study user02	studyuser02@azurstudy.jp	Active Directory と同期
<input checked="" type="checkbox"/> study user03	studyuser03@azurstudy.jp	Active Directory と同期
<input checked="" type="checkbox"/> study user04	studyuser04@azurstudy.jp	Active Directory と同期
<input checked="" type="checkbox"/> study user05	studyuser05@azurstudy.jp	Active Directory と同期
<input type="checkbox"/> studyadmin	studyadmin@azurstudy.onmicrosoft.com	クラウド内

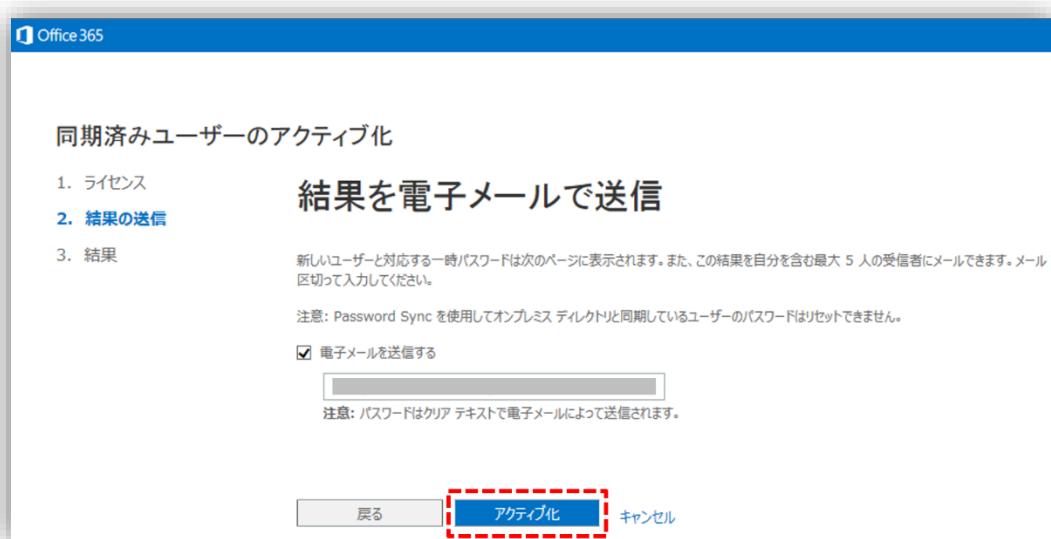
On the right side of the table, there are buttons for '選択済み' (highlighted with a red box) and '同期済みユーザーのアクティビ化' (highlighted with a red box). There are also other buttons like '編集' and '削除'.

企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

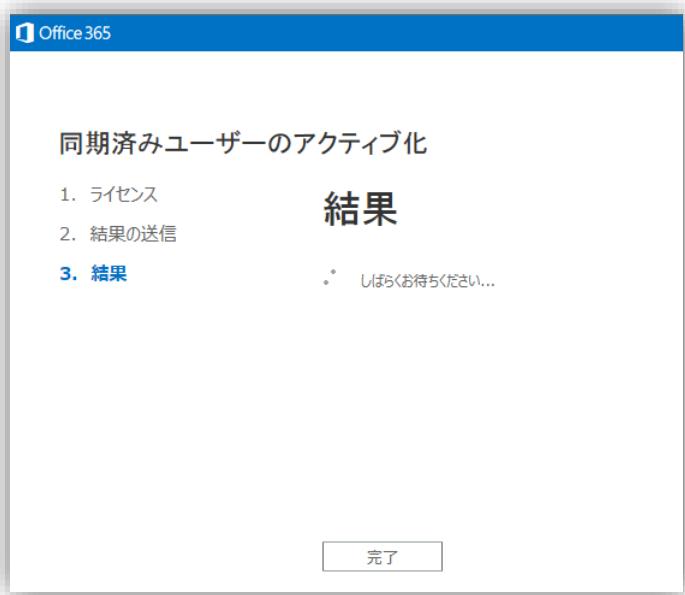
4. [ライセンスの割り当て] ページにて [ユーザーの所在地の設定] で「日本」を選択します。[ライセンスの割り当て] でユーザーにライセンスを割り当てるサービスを選択します。そして [次へ] をクリックします。



5. [結果を電子メールで送信] ページにて [アクティビ化] をクリックします。



6. 処理が完了するまで待ちます。



7. 同期済みユーザーのアクティビズ化が完了したら [完了] をクリックします。



8. [アクティブなユーザー] ページに戻り、左側にある [ライセンス] をクリックします。



9. ユーザーに付与したライセンス数分、[割り当て済み] のライセンス数が増えていることを確認します。

The screenshot shows the 'Licenses' page in the Office 365 Management Center. The left sidebar has 'Dashboard', 'Setup', 'Users & Groups', 'Domain', and 'Licenses'. The main area shows a table for a 'Microsoft Office 365 Plan E3' subscription. The columns are 'Name', 'Effective', 'Expiration', and 'Assigned'. The 'Assigned' column shows the value '6'. A red box highlights the 'Assigned' link in the table header, and another red box highlights the '6' in the table cell. A callout box with the text 'この項目の数を確認' (Check the number of items in this category) points to the 'Assigned' value.

名前	有効	期限切れ	割り当て済み
Microsoft Office 365 プラン E3	25	0	6

STEP 11. AD FS サーバーのセットアップ、 およびフェデレーションの確認

この STEP では、Azure 上に構築した仮想ネットワーク上に AD FS を実装する手順について説明します。

この手順を実施することで、社内 AD と Office 365 の間でフェデレーション信頼関係が結ばれ、ユーザーは会社の資格情報でサインインして、Office 365 の各種サービスにアクセスできる準備が整います。

この STEP では、次のことを学習します。

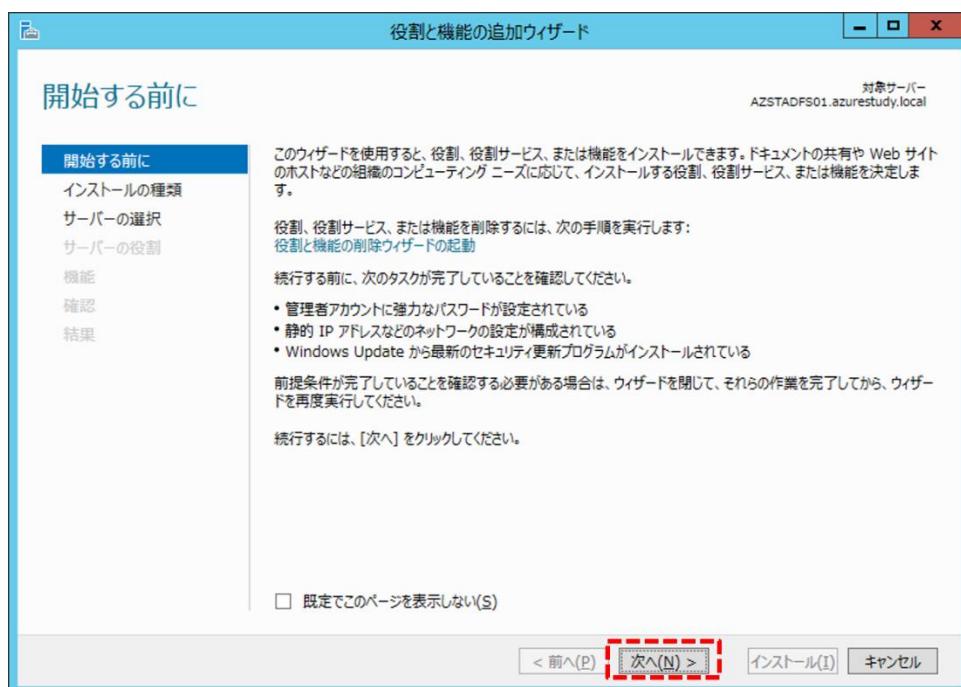
- ✓ AD FS 2.1 関連をインストール
- ✓ サーバー証明書をインポートと設定
- ✓ 社内 DNS の設定
- ✓ AD フェデレーション 用 サービス アカウントの作成
- ✓ フェデレーション サーバーの設定
- ✓ 2 台目以降のフェデレーション サーバーの設定
- ✓ IT プロフェッショナル 用 Microsoft Online Services サインイン アシスタン トのインストール
- ✓ Windows PowerShell 用 Windows Azure Active Directory モジュールのイン ストール
- ✓ フェデレーション ドメインの有効化
- ✓ ローカル イントラネット ゾーンへのサイトの登録
- ✓ フェデレーション環境の動作確認

11.1 AD FS 2.1 関連をインストール

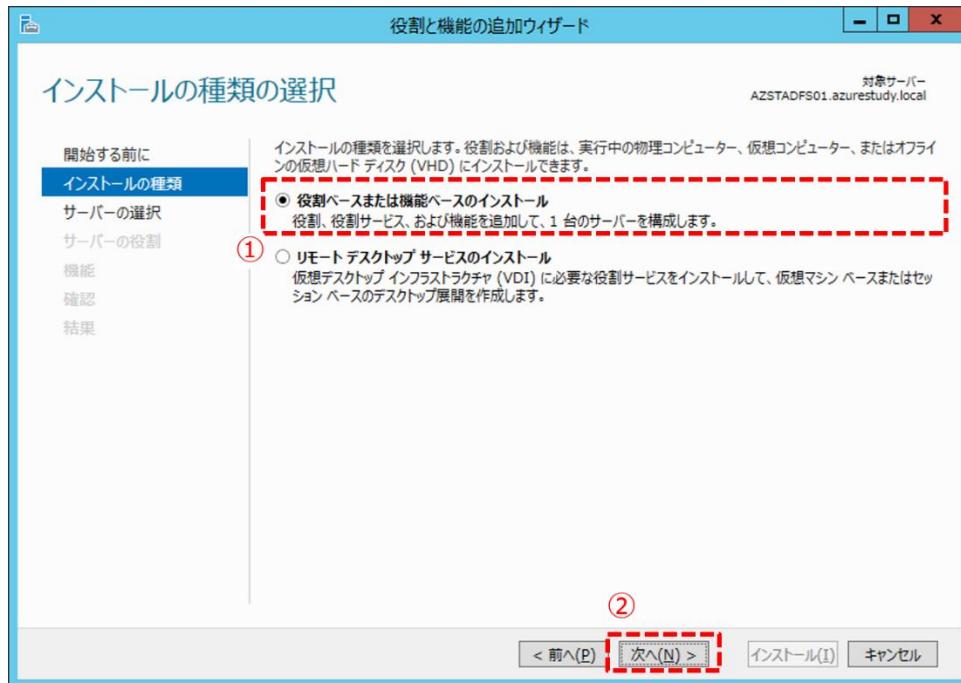
- ドメイン管理者アカウントで AD FS サーバー プライマリ [AZSTADFS01] にサインインし、[サーバー マネージャー] を開きます。
- [管理] メニュー > [役割と機能の追加] をクリックします。



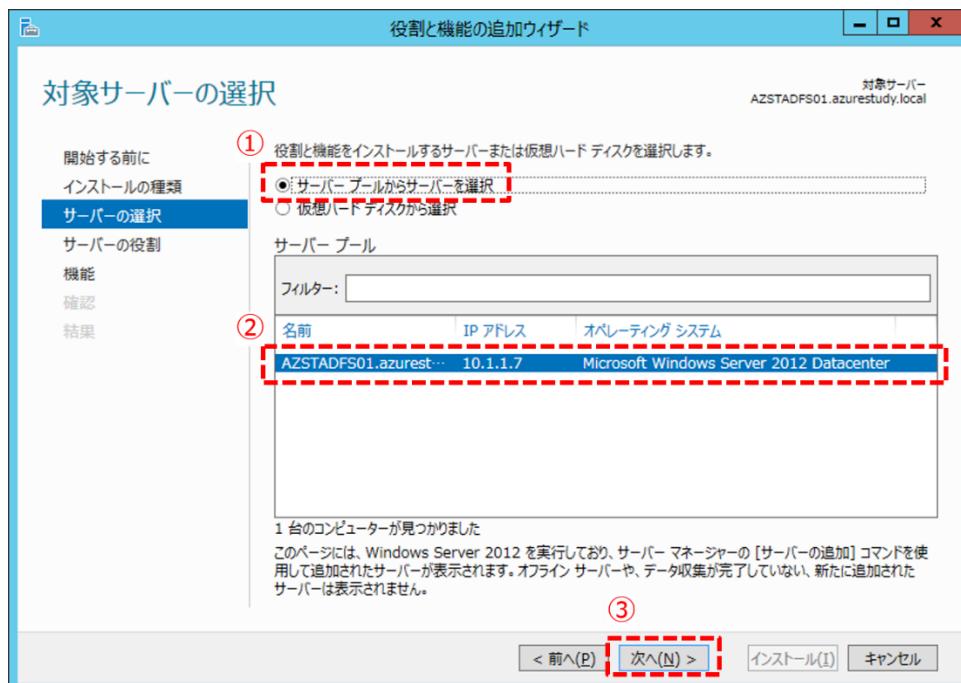
- [役割と機能の追加ウィザード] 画面が開きます。[開始する前に] ページにて [次へ] ボタンをクリックします。



4. [インストールの種類の選択] ページにて [役割ベースまたは機能ベースのインストール] を選択して [次へ] ボタンをクリックします。

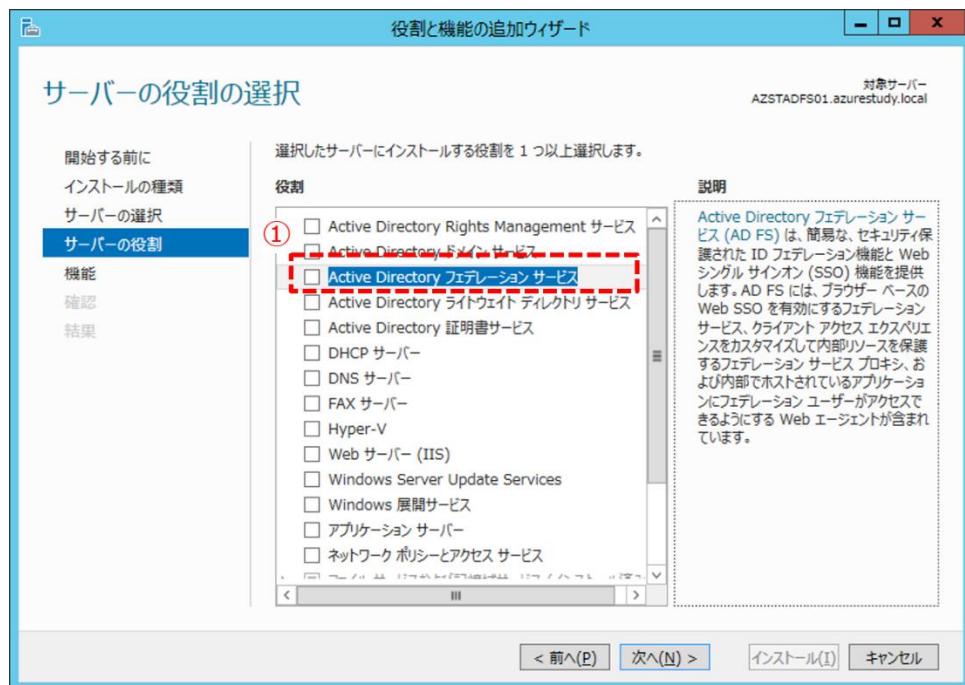


5. [対象サーバーの選択] ページにて [サーバー プールからサーバーを選択] を選択し、[サーバー プール] から AD FS サーバー プライマリ [AZSTPROXY01] を選択して [次へ] ボタンをクリックします。



企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

6. [「サーバーの役割の選択】ページにて [役割] 一覧から [Active Directory フェデレーションサービス] のチェックボックスにチェックを付けます。



以下の画面が開きます。[Active Directory フェデレーション サービス] が依存するサービス、および機能も追加する必要があるので内容を確認し、[管理ツールを含める (存在する場合)] チェックボックスにチェックを付けて [機能の追加] ボタンをクリックして閉じます。

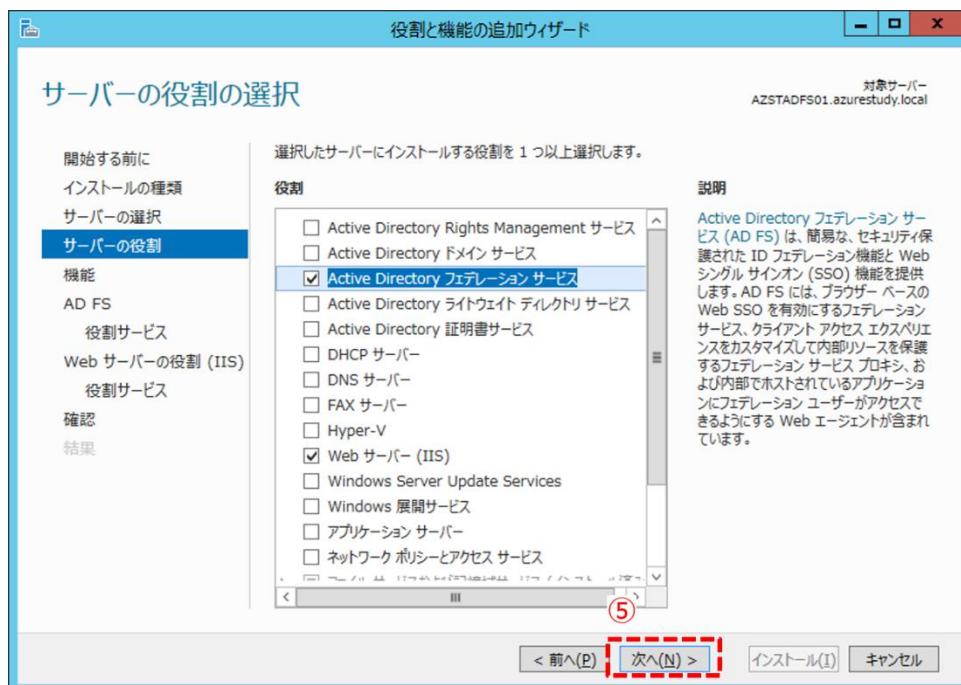


企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

【表：[Active Directory フェデレーション サービス] が依存するサービスと機能】

.NET Framework 4.5 Features	WCF サービス	HTTP アクティビティ化			
	ASP.NET 4.5				
Web サーバー (IIS)	管理ツール	[ツール] IIS 管理コンソール			
	Web サーバー	アプリケーション開発	ASP.NET 4.5		
			ISAPI 拡張		
			ISAPI フィルター		
			.NET 拡張機能 4.5		
		HTTP 共通機能	既存のドキュメント		
			ディレクトリの参照		
			HTTP エラー		
			HTTP リダイレクト		
			静的なコンテンツ		
		状態と診断	HTTP ログ		
		パフォーマンス	静的なコンテンツの圧縮		
		セキュリティ	クライアント証明書マッピング認証		
			要求フィルター		
			Windows 認証		
Windows プロセス	構成 API				
アクティビ化サービス	プロセス モデル				

[サーバーの役割の選択] ページに戻ると、[Active Directory フェデレーション サービス] と [Web サーバー (IIS)] のチェックボックスにチェックが付きます。[次へ] ボタンをクリックします。



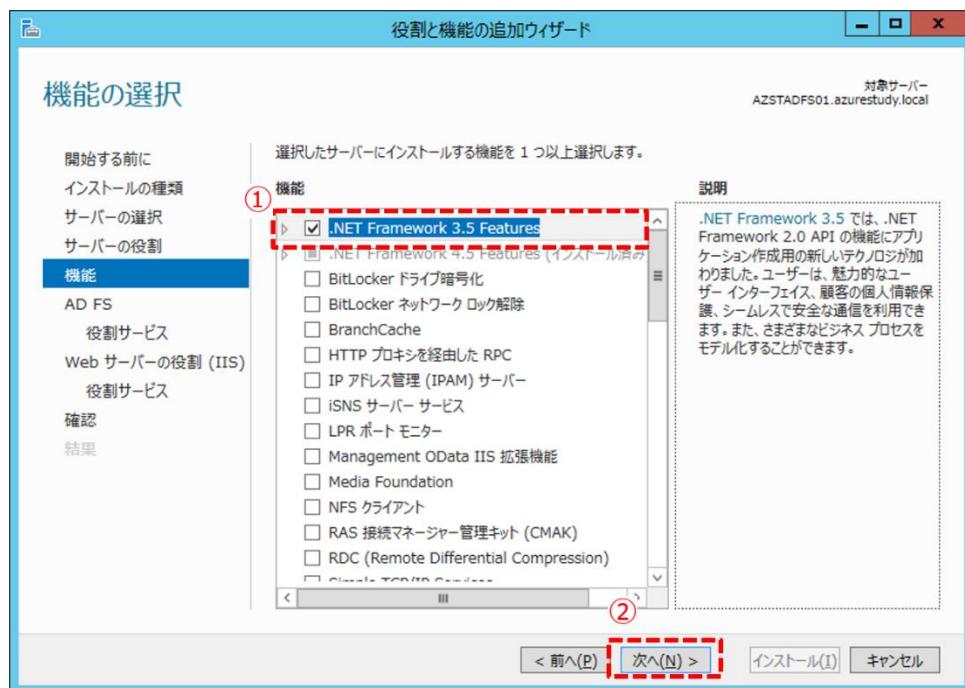
企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

7. [機能の選択] ページにて [機能] (*1) 一覧から [.NET Framework 3.5 Features] (*2) チェックボックスにチェックを付けて [次へ] ボタンをクリックします。

Note : 機能の確認と .NET Framework 3.5 Features の有効化について

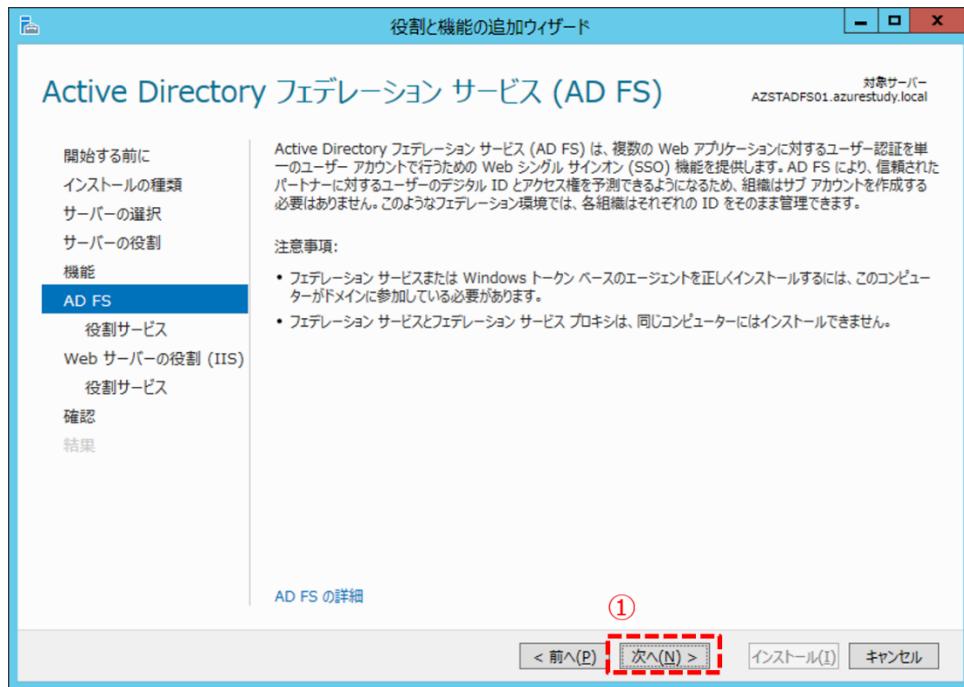
(*1) : 手順 6 の [Active Directory フェデレーション サービス] が依存するサービスと機能にある [.NET Framework 4.5 Features] (インストール済み) と [Windows プロセス アクティブ化サービス] チェックボックスにチェックが付いていることを確認します。

(*2) : 後述する「11.8 Windows PowerShell 用 Windows Azure Active Directory モジュールのインストール」にて必要なため、ここで併せてインストールします。

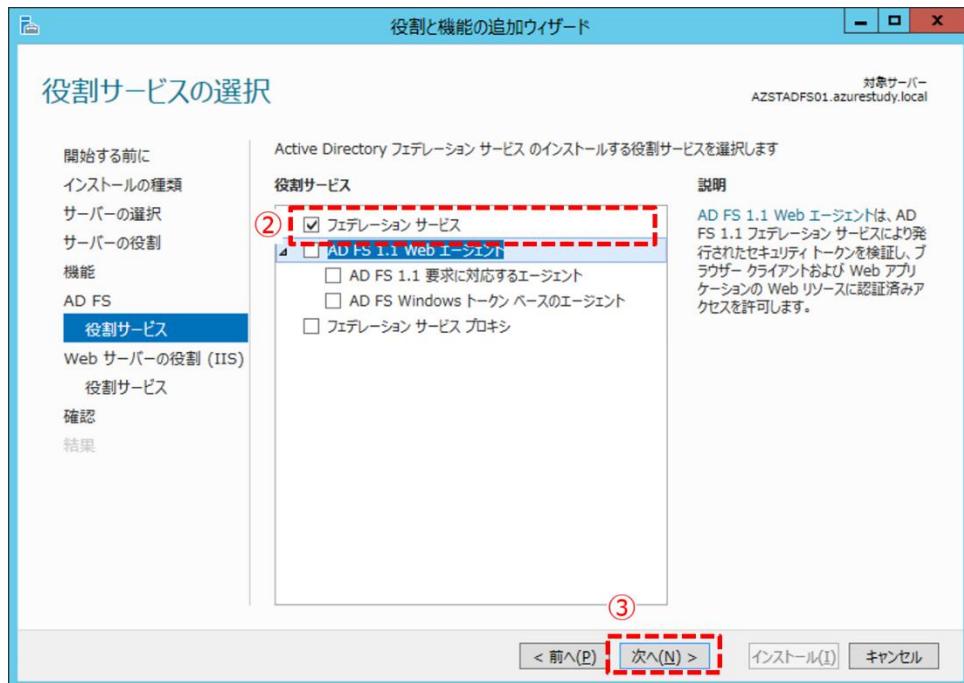


企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

8. [Active Directory フェデレーション サービス (AD FS)] ページにて [次へ] ボタンをクリックします。

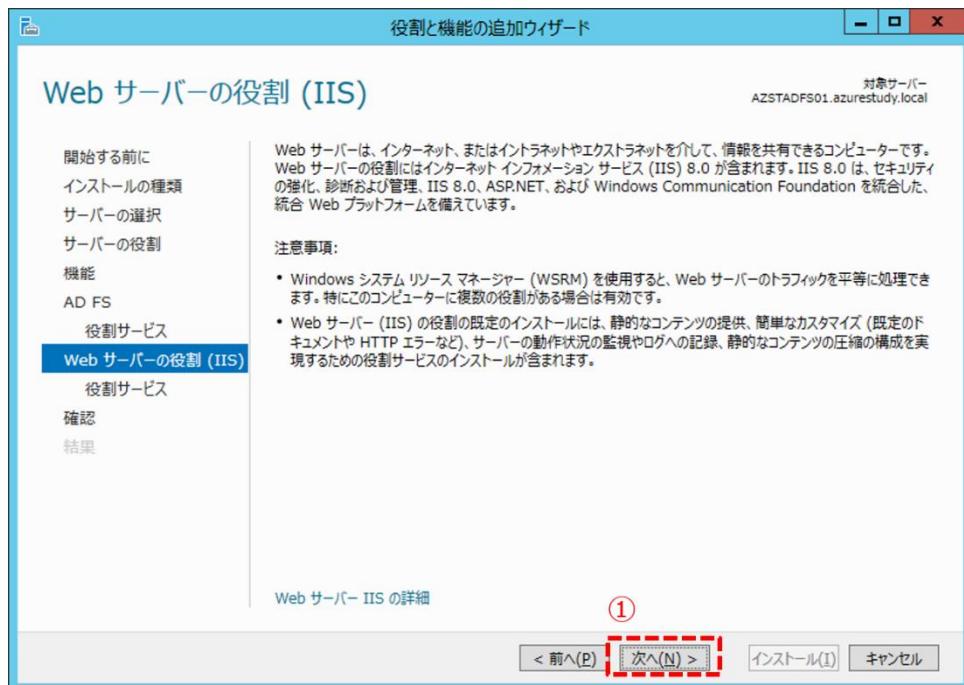


[AD FS の役割サービスの選択] ページにて、[役割サービス] から [フェデレーション サービス] チェックボックスのみにチェックを付けて [次へ] ボタンをクリックします。

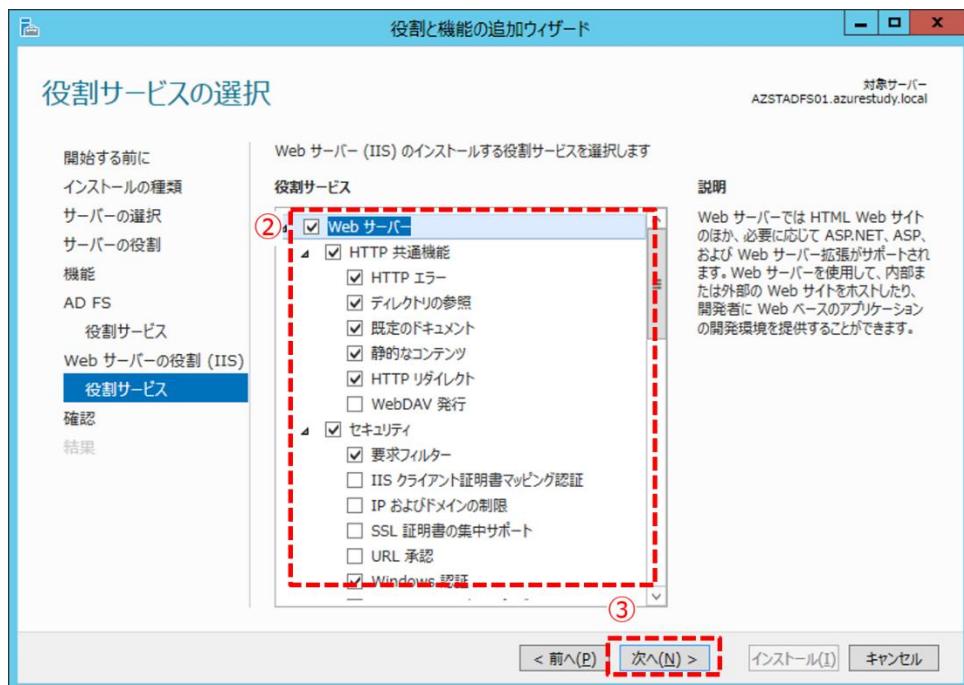


企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

9. [Web サーバーの役割 (IIS)] ページにて [次へ] ボタンをクリックします。



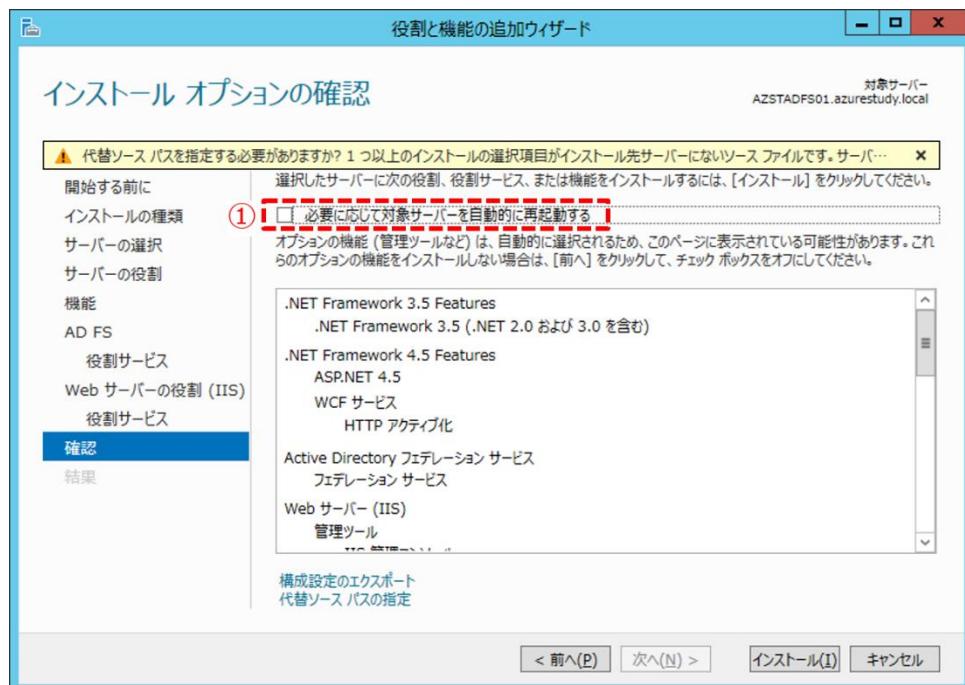
[Web サーバーの役割サービスの選択] ページにて、[役割サービス] から以下の表の項目にチェックが付いていることを確認して [次へ] ボタンをクリックします。



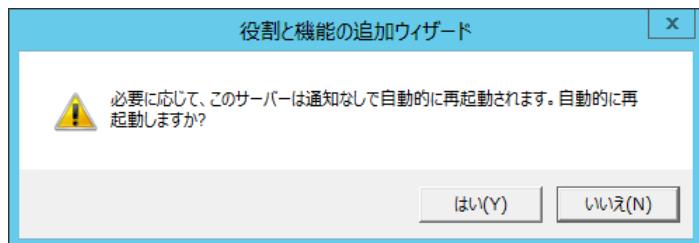
【表：Web サーバー デフォルト コンポーネント】

Web サーバー	HTTP 共通機能	HTTP エラー
		ディレクトリの参照
		既存のドキュメント
		静的なコンテンツ
		HTTP リダイレクト
	セキュリティ	要求フィルター
		Windows 認証
		クライアント証明書マッピング認証
	パフォーマンス	静的なコンテンツの圧縮
	状態と診断	HTTP ログ
	アプリケーション開発	.NET 拡張機能 4.5
		ASP.NET 4.5
		ISAPI フィルター
		ISAPI 拡張
管理ツール	IIS 管理コンソール	

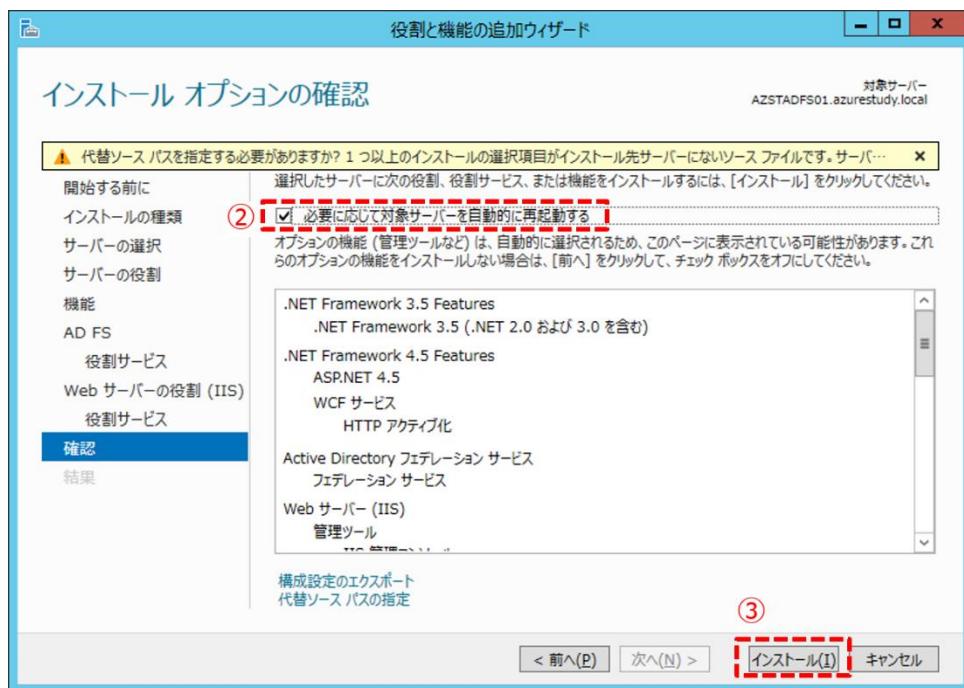
10. [インストール オプションの確認] ページにて [必要に応じて対象サーバーを自動的に再起動する] チェックボックスにチェックを付けます。



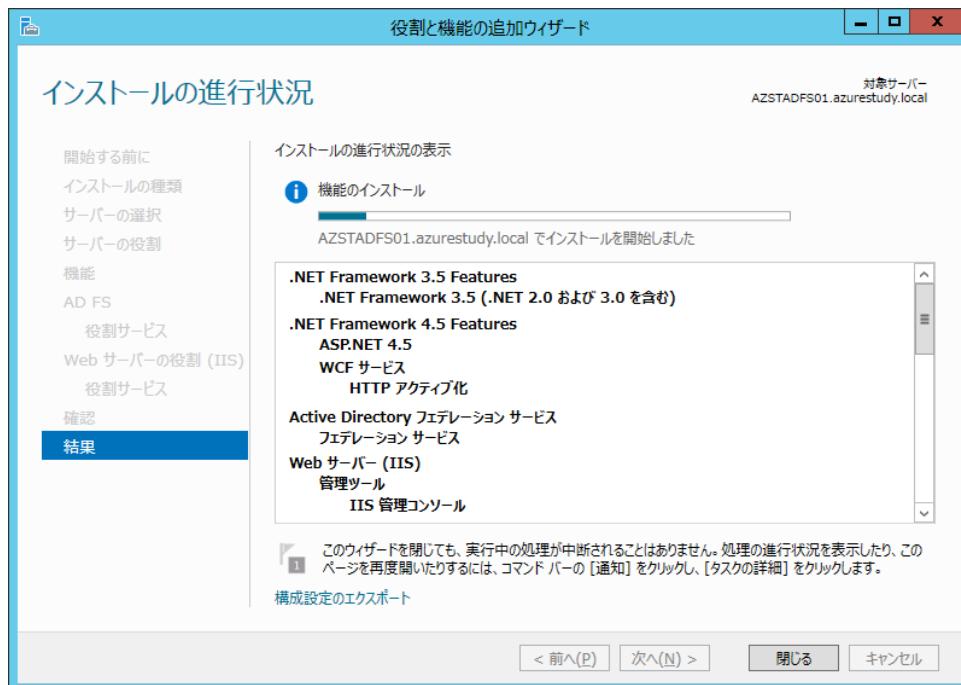
企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携
以下のメッセージ ボックスが開くので、[はい] ボタンをクリックして閉じます。



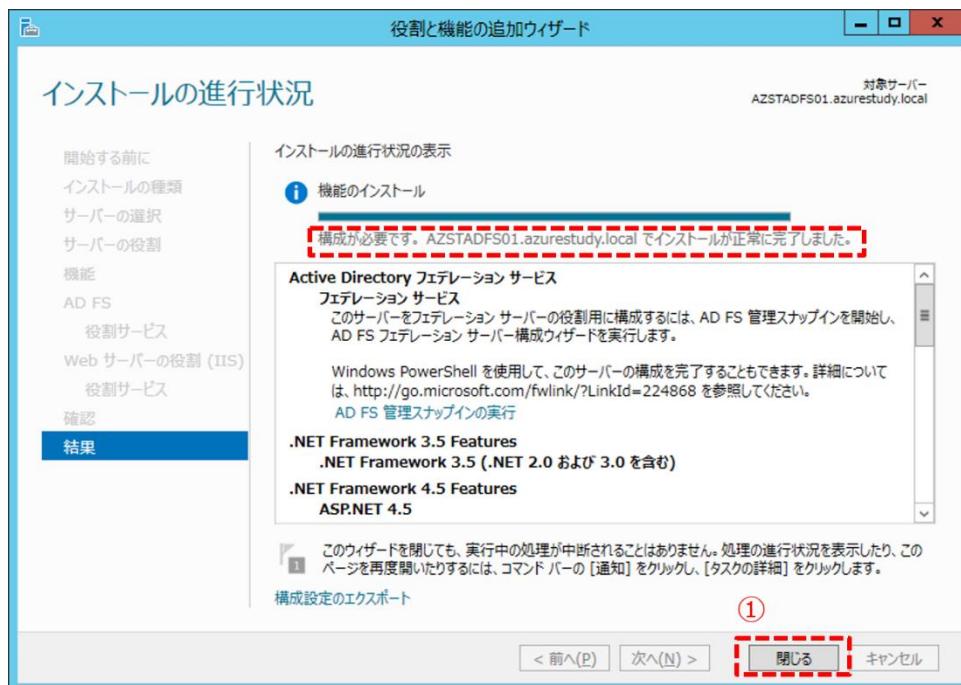
[インストール オプションの確認] ページに戻り、[必要に応じて対象サーバーを自動的に再起動する] チェックボックスにチェックが付いていることを確認して [インストール] ボタンをクリックします。



11. インストールが完了するまで待ちます。



12. 「構成が必要です。 AZSTADFS01.azurestudy.local でインストールが正常に完了しました。」とメッセージが表示されたら、[閉じる] ボタンをクリックして閉じます。



Note : AD FS サーバー セカンダリ (2 台目以降) での作業

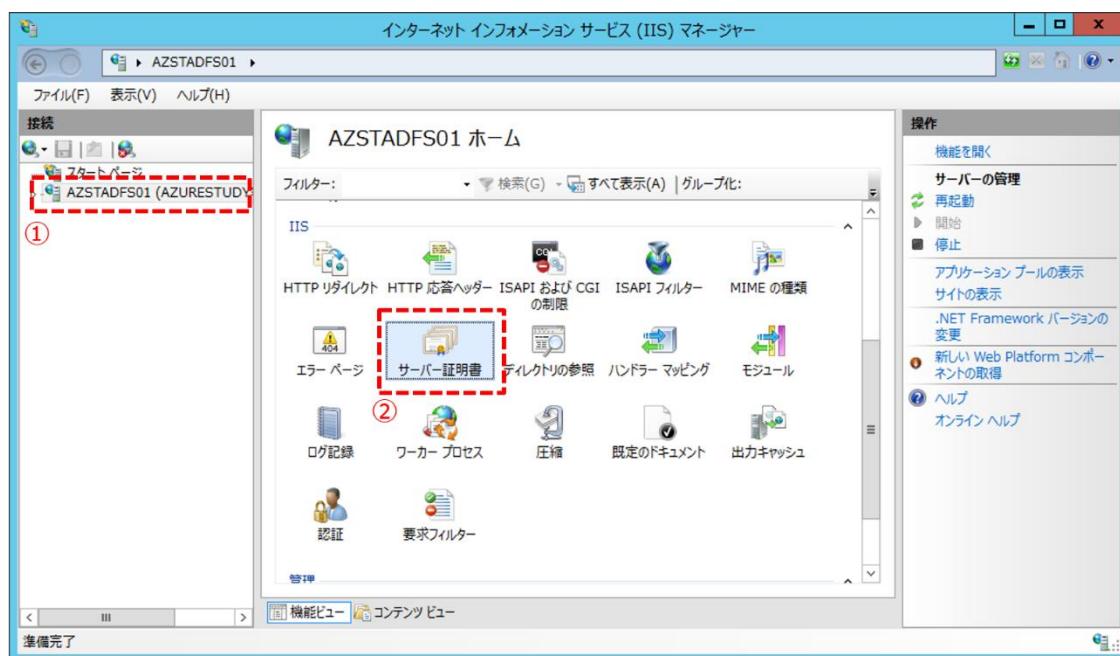
AD FS サーバー セカンダリ [AZSTADFS02] (2 台目以降) についてもこの項の作業を実施します。

なお、手順 7 の [機能の選択] ページにて選択した [.NET Framework 3.5 Features] は、AD FS サーバー セカンダリ (2 台目以降) では不要なのでインストールする必要はありません。

11.2 サーバー証明書をインポートと設定

◆ CSR の作成

1. ドメイン管理者アカウントで AD FS サーバー プライマリ [AZSTADFS01] にサインインし、[インターネット インフォメーション サービス (IIS) マネージャー] を開きます。
2. 左ペインにて IIS をインストールしたサーバーが表示されるので、そのサーバー名 ([AZSTADFS01 (AZURESTUDY\administrator)]) を選択します。
3. 中央ペインにて [サーバー証明書] をダブルクリックします。



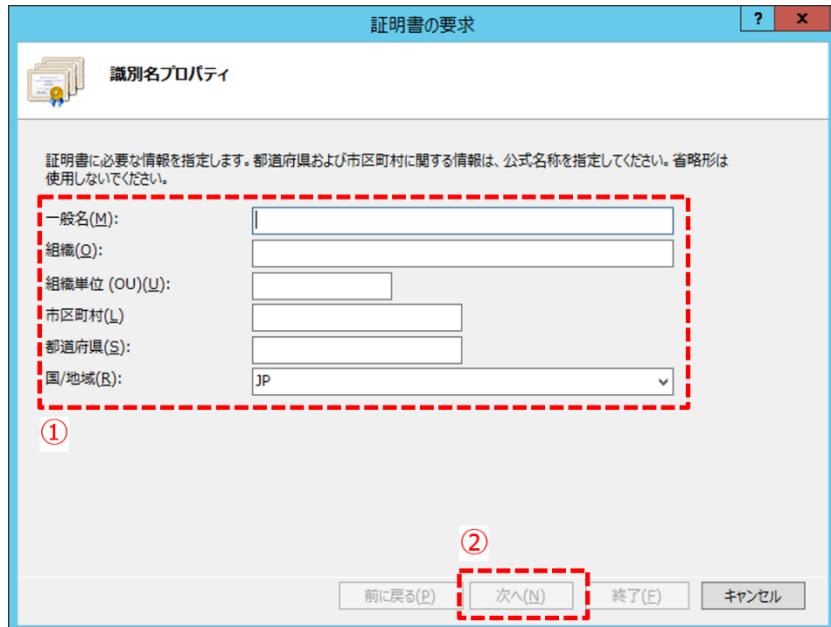
4. 右ペインにて [操作] の [証明書の要求の作成] をクリックします。



5. [識別名のプロパティ] 画面では証明書情報を入力します。入力できたら [次へ] ボタンをクリックします。

Note : [一般名] の取り扱いについて

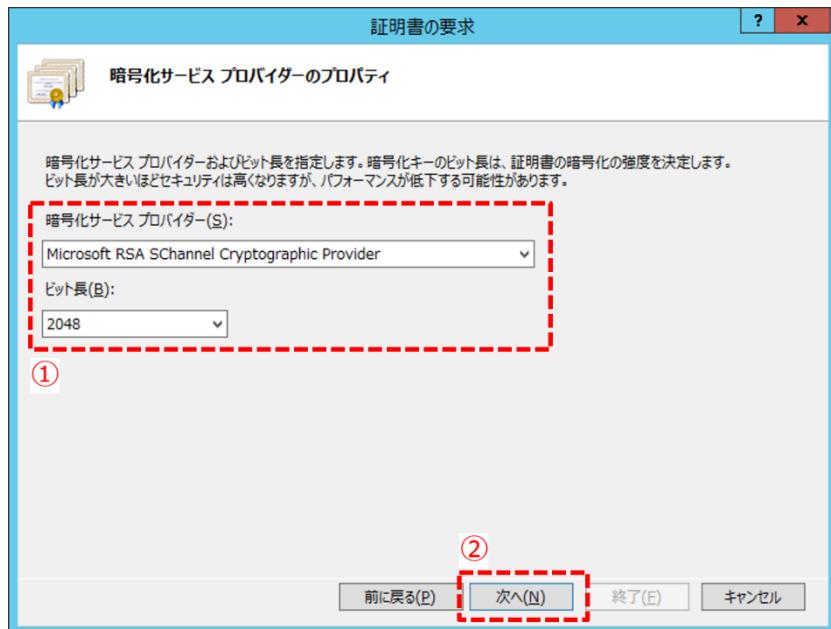
[一般名] に登録したものが ADFS、ADFS Proxy で使用されるフェデレーション サービス名 (FQDN) となります。



項目	設定値 (例)
一般名	sts.azurestudy.jp
組織	Cloudlive, Inc.
組織単位	Sales
市区町	Cyuo-ku
都道府県	Tokyo
国/地域	JP

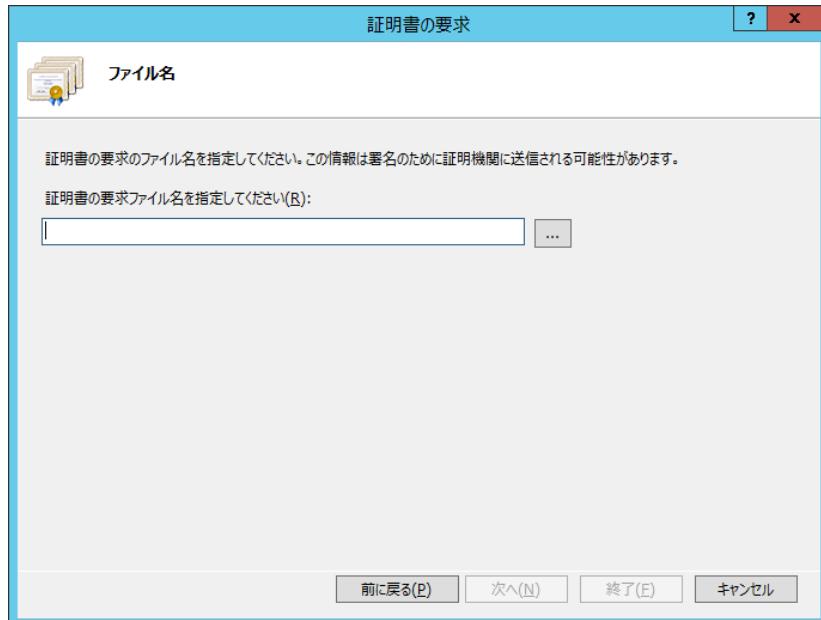
企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

6. [暗号化サービス プロバイダーのプロパティ] 画面にて、以下の表のとおり入力して [次へ] ボタンをクリックします。



項目	設定値
暗号化サービス プロバイダー	「Microsoft RSA SChannel Cryptographic Provider」を選択
ビット長	「2048」を選択

7. [ファイル名] 画面にて、任意のパスおよびファイル名を付け、[終了]をクリックします。



8. 作成した CSR を公的証明書機関（ベリサイン等）に提出し、SSL 証明書を発行してもらいます。

9. 取得した SSL 証明書を任意の場所に保存します。

Note : SSL 証明書の取り扱いについて注意事項

SSL 証明書は、信頼された認証局が発行する電子証明書であり、主に以下の 2 つの機能があります。

- ・ サイトの実在証明
サイトの運営組織が実在しドメイン名の使用権があることを第三者機関が証明する
- ・ SSL 暗号化通信
通信内容（例えば、クレジットカード番号等の個人情報）の盗聴・改ざん、サイトの運営者へのなりすましを防ぐ

上記機能により、SSL 証明書が流出した場合、第三者により暗号化された通信内容を解読されたり正当な証明書所有者に成りすまして悪用される危険性があります。

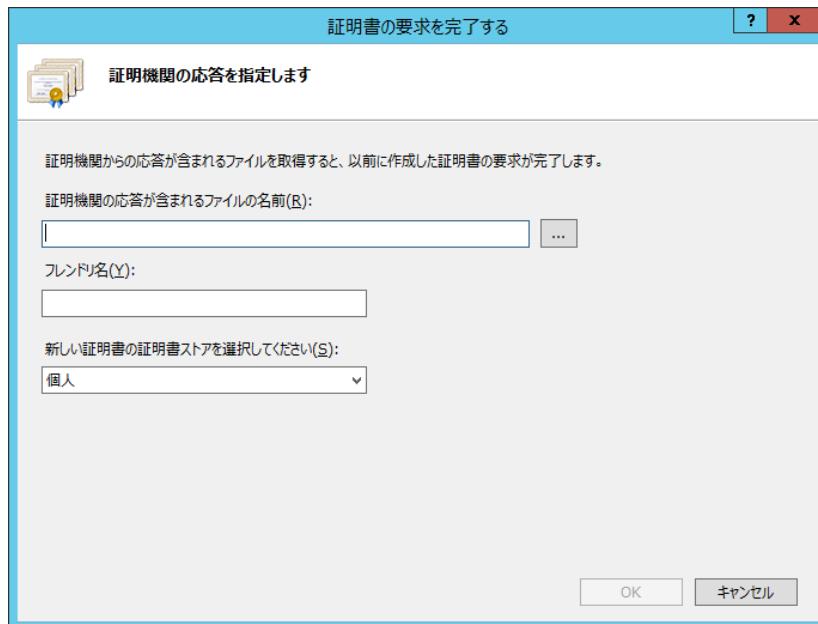
よって、取り扱いには十分注意してください。

▼ SSL 証明書のインポート

10. [インターネット インフォメーション サービス (IIS) マネージャー] の [サーバー証明書] を開き、右ペインにて [操作] の [証明書の要求の完了] をクリックします。



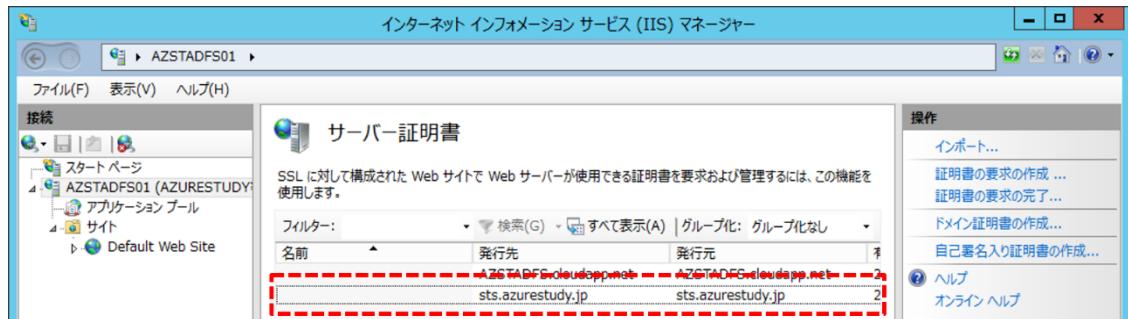
11. [証明書の要求を完了する] 画面が表示されます。以下の表のとおり入力して [OK] ボタンをクリックします。



項目	設定値
証明機関の応答が含まれるファイルの名前	手順 9 で保存した SSL 証明書のファイルパスを指定
フレンドリ名	「ADFSCertificate (分かりやすい任意の名前)」を入力
新しい証明書の証明書ストア	「個人」を選択

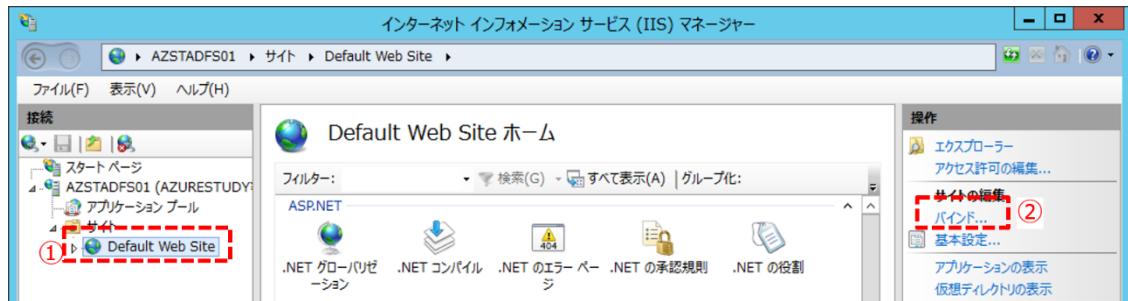
企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

12. [サーバー証明書] にインポートした証明書が表示されていることを確認します。



▼ SSL 証明書の設定

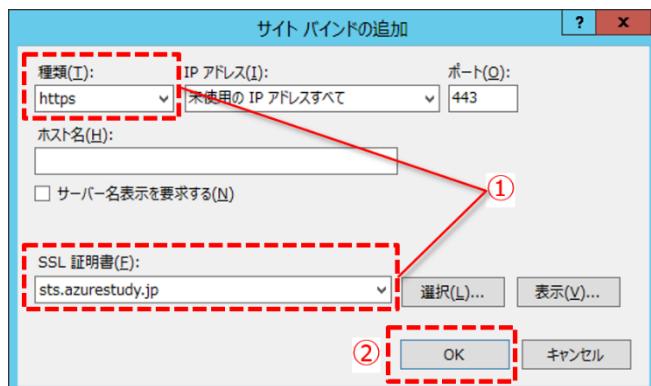
13. [インターネット インフォメーション サービス (IIS) マネージャー] を開き、左ペインにて IIS をインストールしたサーバーが表示されるので、そのサーバー名([AZSTADFS01 (AZURESTUDY\\$administrator)])を展開し、[サイト] > [Default Web Site] を選択します。そして、右ペインにて [操作] の [バインド] をクリックします。



14. [サイト バインド] 画面にて、[追加] ボタンをクリックします。



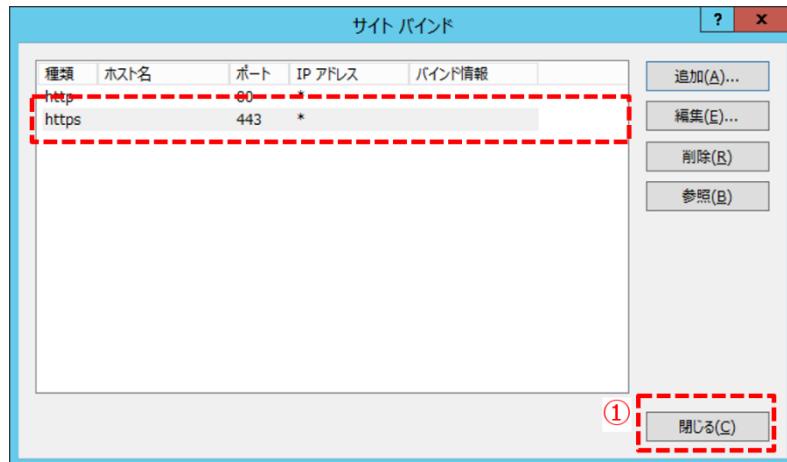
15. [サイト バインドの追加] 画面にて、以下の表のとおり入力して [OK] ボタンをクリックします。



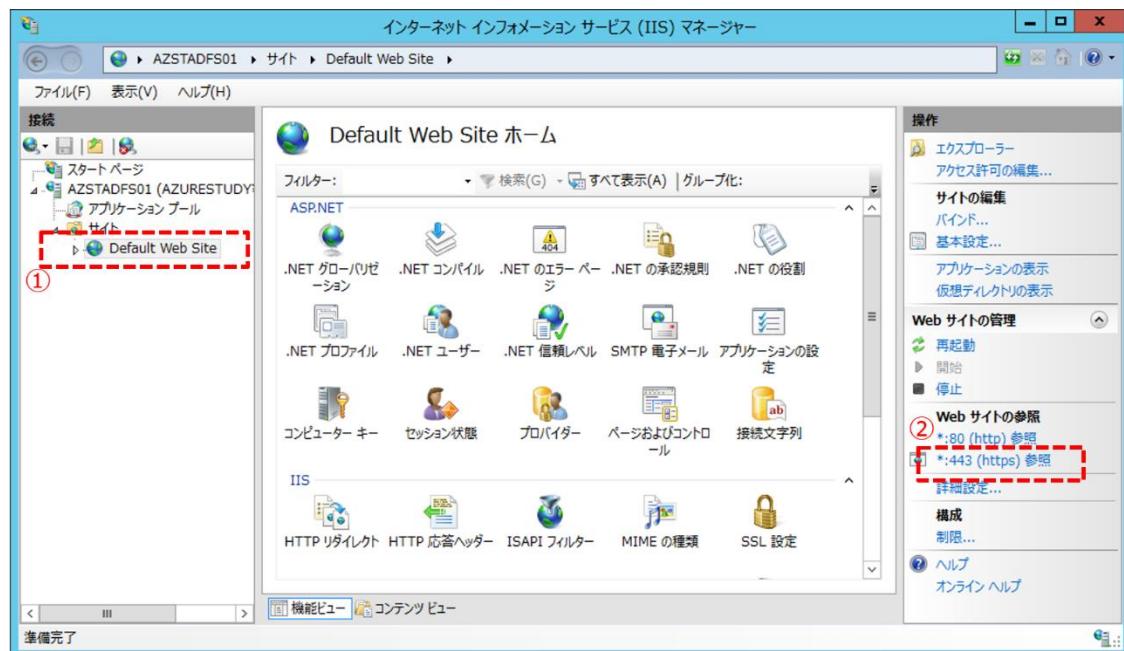
Microsoft Azure 自習書シリーズ No.6
企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

項目	設定値
種類	「https」を選択 ※ [IP アドレス]、[ポート] は自動的に選択されます。
SSL 証明書	手順 10 ~ 12 でインポートした SSL 証明書を選択

16. [サイト バインド] 画面に戻り、一覧に「https」が追加されていることを確認します。確認後、[閉じる] ボタンをクリックして閉じます。

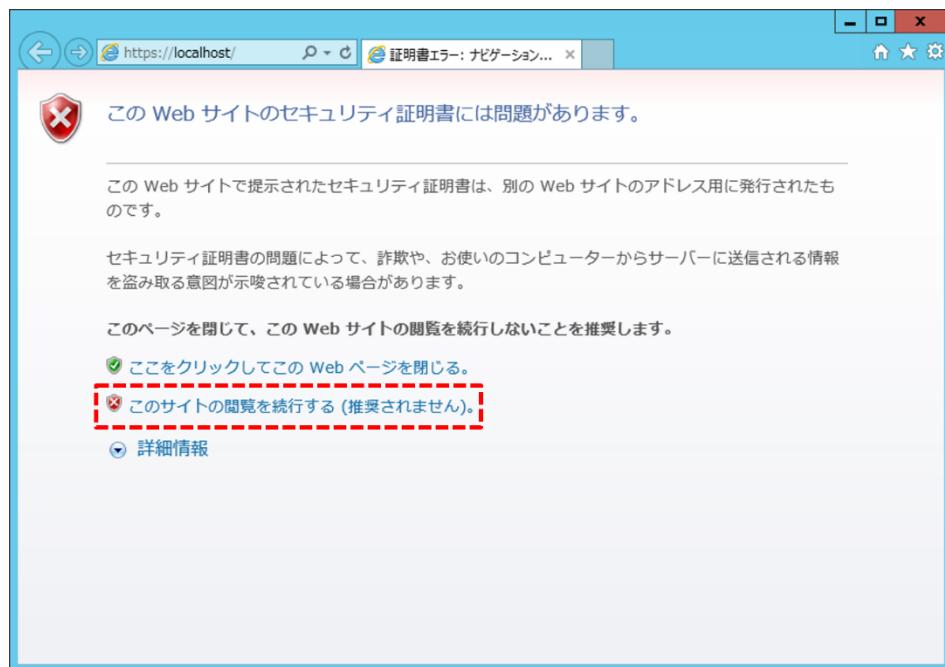


17. [インターネット インフォメーション サービス (IIS) マネージャー] を開き、左ペインにて IIS をインストールしたサーバーが表示されるので、そのサーバー名([AZSTADFS01 (AZURESTUDY\\$administrator)])を展開し、[サイト] > [Default Web Site] を選択します。そして、右ペインにて [Web サイトの管理] にある [*:443 (https) 参照] をクリックします。



企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

18. ブラウザーが開きます。 Web サイトに "証明書エラー" が表示されたら、[このサイトの閲覧を続行する] をクリックします。



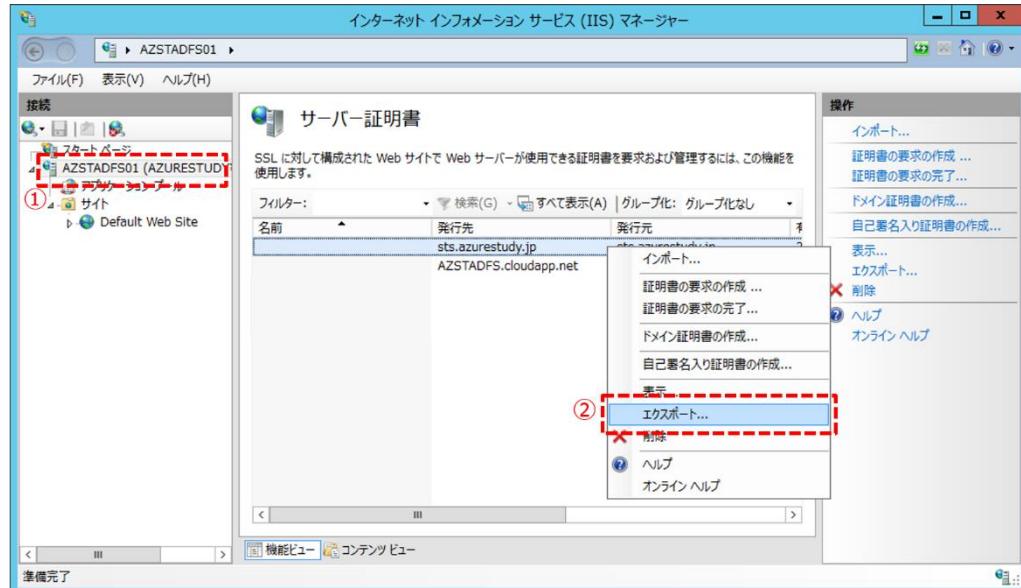
以下のページが表示されることを確認します。



Note : AD FS サーバー セカンダリ (2 台目以降) での作業

AD FS サーバー セカンダリ [AZSTADFS02] (2 台目以降) については、

AD FS サーバー プライマリ [AZSTADFS01] にインポートした SSL 証明書をエクスポートします。



エクスポートした SSL 証明書をインポートします。



その後、上記の手順 13 以降の作業を実施します。

11.3 社内 DNS の設定

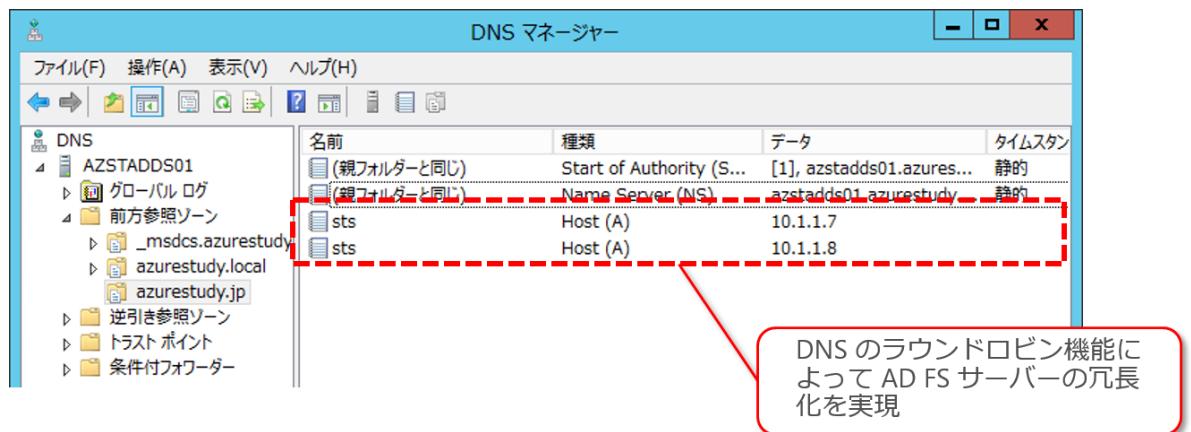
AD FS サーバーの冗長化は、DNS のラウンドロビン機能によって実現します。

※ Azure ではネットワーク負荷分散 (NLB) がサポートされていないため。

1. ドメイン管理者アカウントで AD DS サーバー [AZSTADDS01] にサインインし、[DNS マネージャー] を開きます。
2. Office 365 にて使用するフェデレーション ドメイン [azurestudy.jp] を登録します。

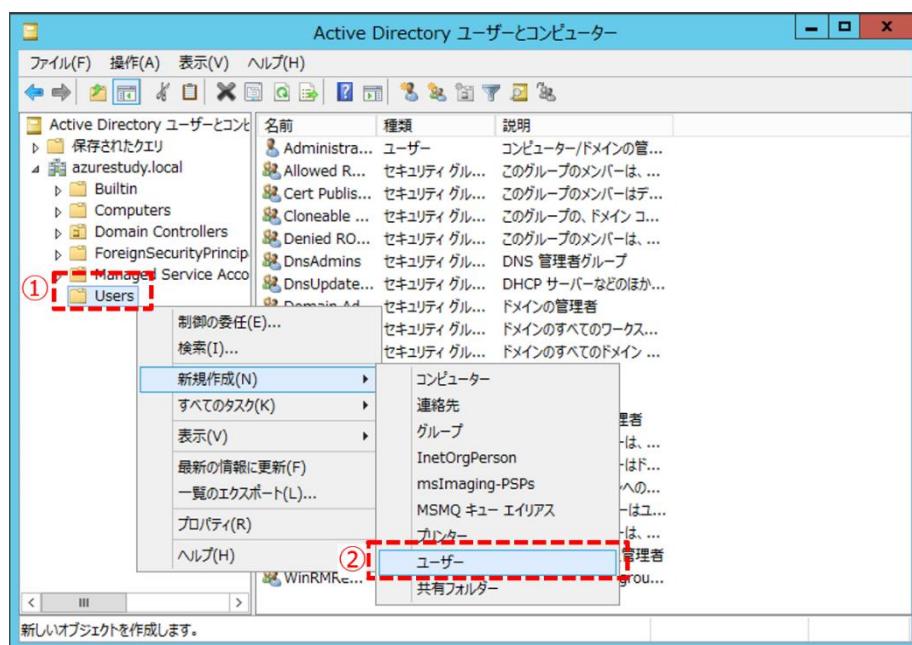


3. A レコードで AD FS サーバーに名前解決されるように [sts.azurestudy.jp] を追加します。



11.4 AD フェデレーション 用 サービス アカウントの作成

- ドメイン管理者アカウントで AD DS サーバー [AZSTADDS01] にサインインし、[Active Directory ユーザーとコンピューター] を開きます。
- サービス アカウントを作成する OU を選択します。
※ ここでは例として、OU を [Users] を選択します。
- OU [Users] を右クリックし、[新規作成] > [ユーザー] を選択します。

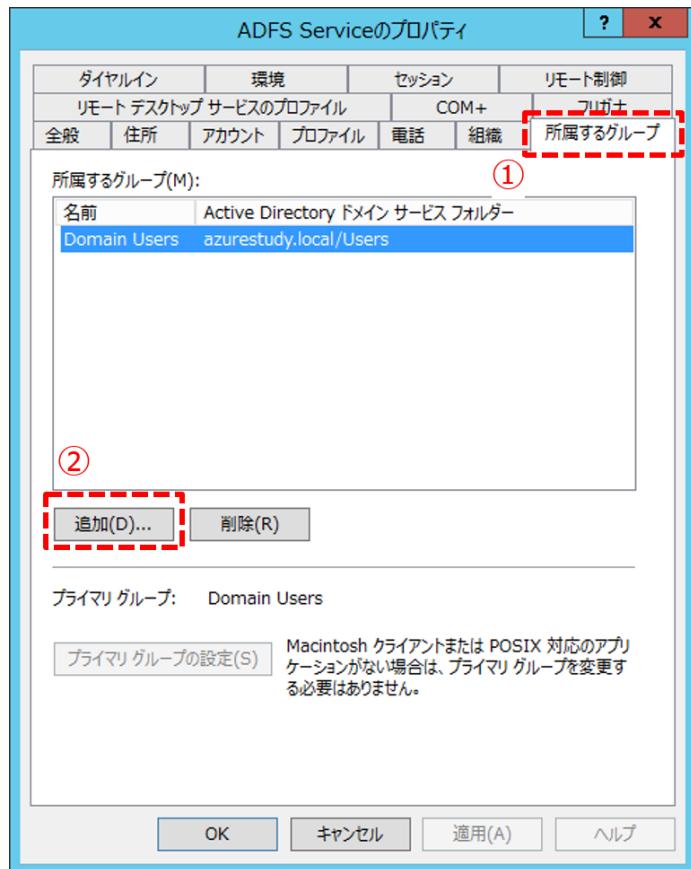


- 以下の内容でユーザーを作成します。

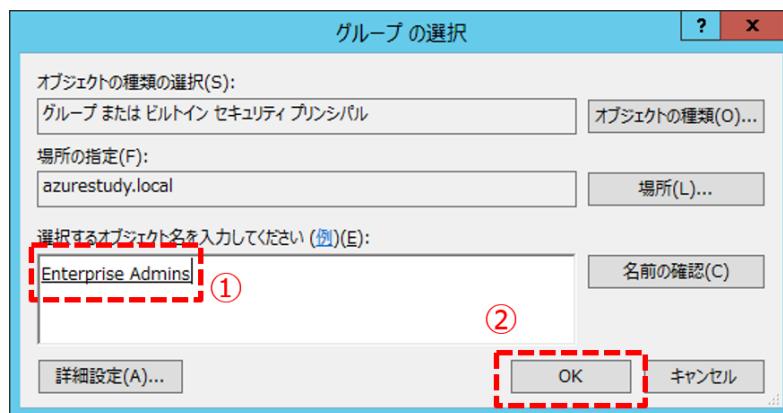
項目	設定値	
姓	ADFS Service	
名	(必要に応じて入力)	
フルネーム	ADFS Service	
ユーザー ログオン名	adfssvc@azurestudy.local	
ユーザー ログオン名 (Windows 2000 より前)	adfssvc	
パスワード	パスワード/パスワードの確認	(任意のパスワード)
	ユーザーは次回ログオン時にパスワード変更が必要	<input checked="" type="checkbox"/> OFF (無効)
	ユーザーはパスワードを変更できない	<input checked="" type="checkbox"/> ON (有効)
	パスワードを無制限にする	<input checked="" type="checkbox"/> ON (有効)
	アカウントは無効	<input checked="" type="checkbox"/> OFF (無効)

企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

5. 手順 4 で作成したサービス アカウントを [Enterprise Admins] セキュリティ グループに追加します。手順 4 で作成したユーザーのプロパティを開きます。[所属するグループ] タブを開き [追加] ボタンをクリックします。

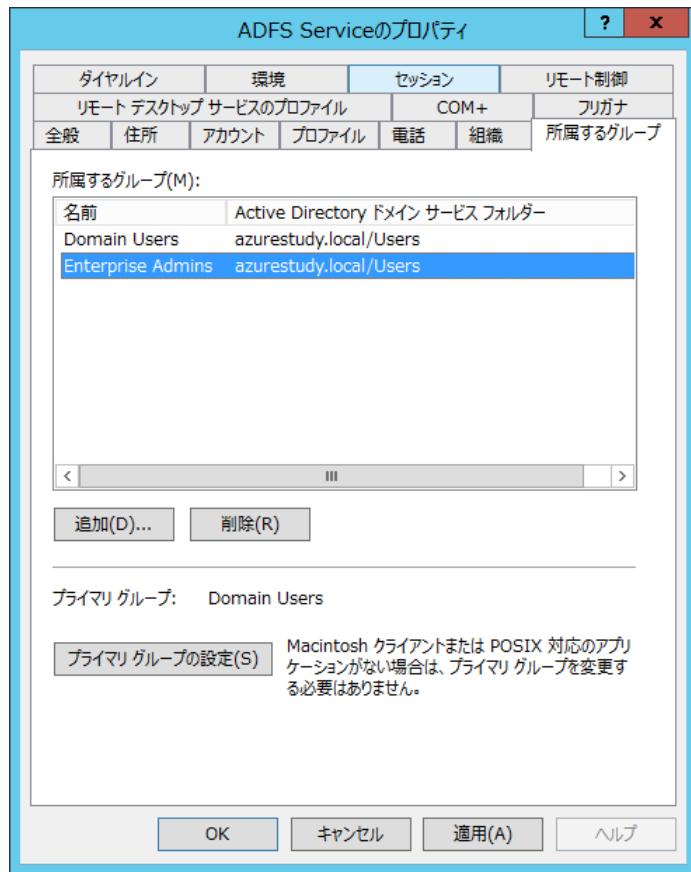


6. [グループの選択] 画面が開きます。[選択するオブジェクト名を入力してください] に [Enterprise Admins] セキュリティ グループを指定します。[OK] ボタンをクリックして閉じます。



企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

7. [ADFS Service のプロパティ] 画面に戻り、[所属するグループ] タブの [所属するグループ] に [Enterprise Admins] セキュリティ グループが追加されたことを確認して [OK] ボタンをクリックして閉じます。

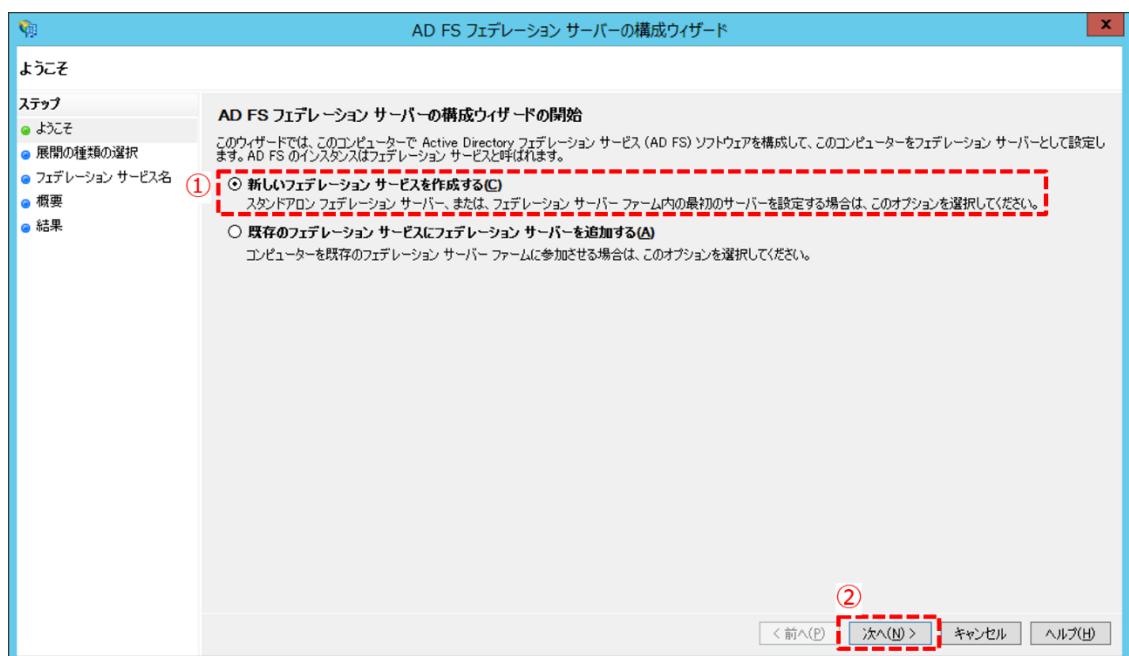


11.5 フェデレーション サーバーの設定

- ドメイン管理者アカウントで AD FS サーバー プライマリ [AZSTADFS01] にサインインし、[AD FS の管理] を開きます。
- 中央ペインにて [AD FS フェデレーション サーバーの構成ウィザード] をクリックします。

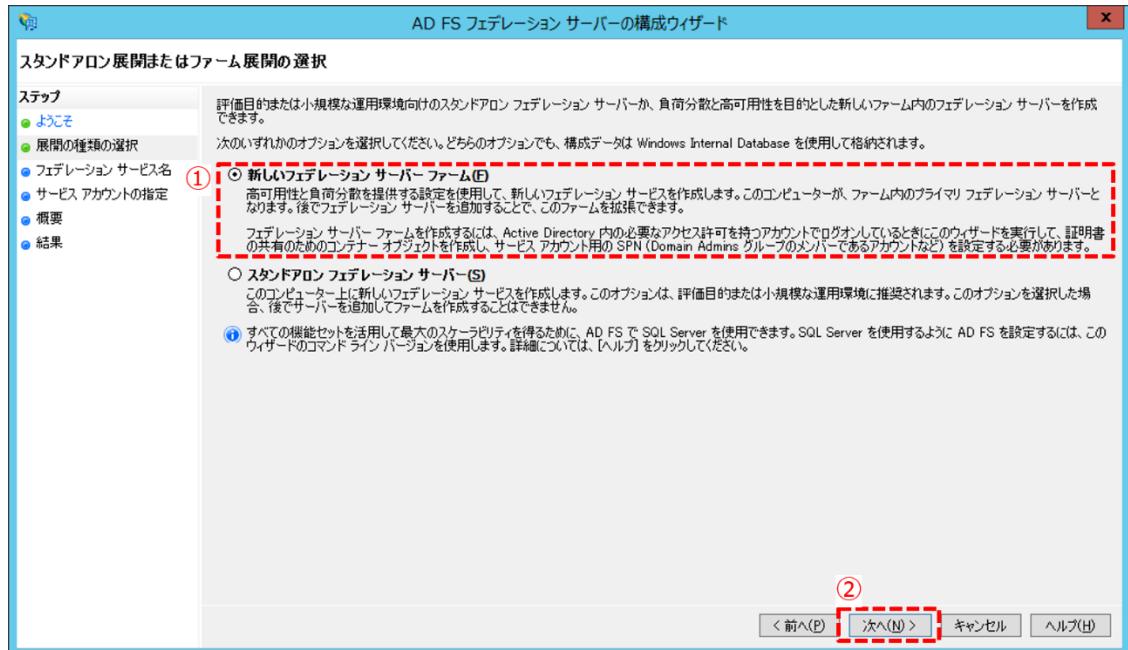


- [AD FS フェデレーション サーバーの構成ウィザード] 画面が開きます。[ようこそ] ページにて [新しいフェデレーションサービスを作成する] を選択して [次へ] ボタンをクリックします。

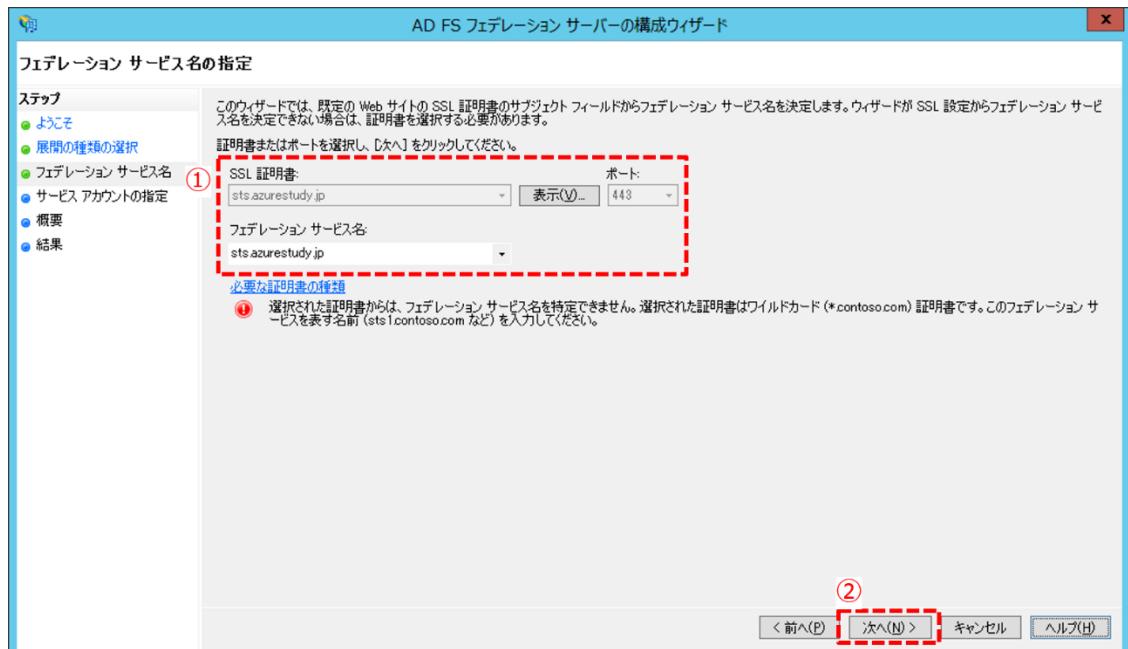


企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

4. [スタンダードアロン展開またはファーム展開の選択] ページにて [新しいフェデレーション サーバー ファーム] を選択して [次へ] ボタンをクリックします。



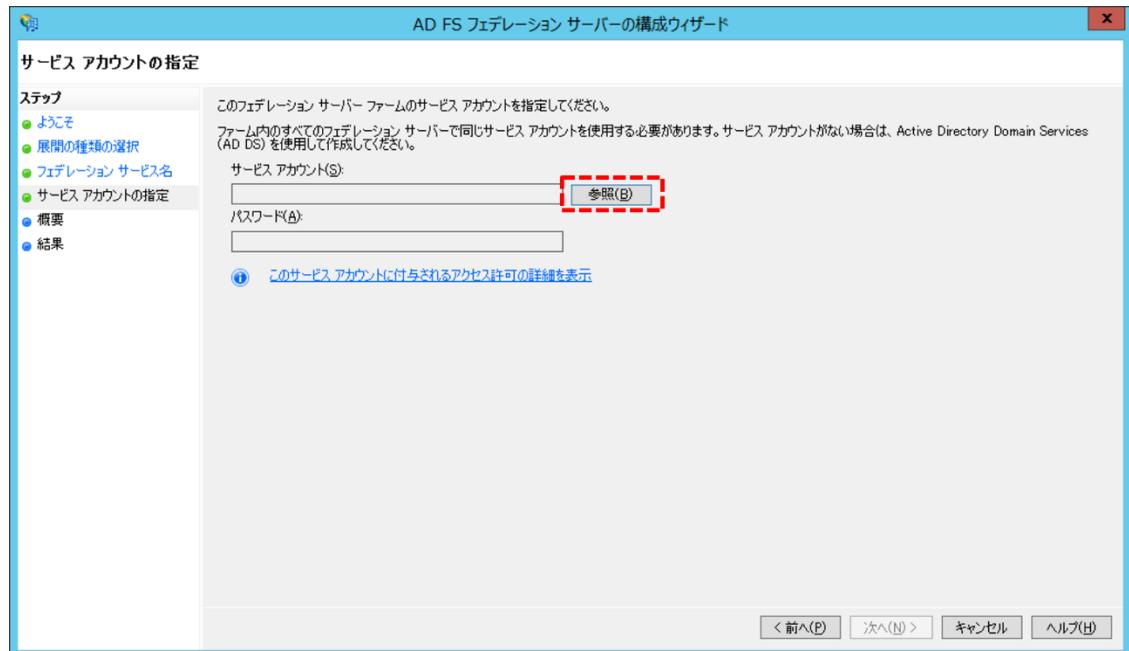
5. [フェデレーション サービス名の指定] ページにて [SSL 証明書] と [フェデレーション サービス名] に「sts.azurestudy.jp」が指定されていることを確認して [次へ] ボタンをクリックします。



企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

6. [サービス アカウントの指定] ページにて「11.4 AD フェデレーション 用 サービス アカウントの作成」で作成したアカウントを指定します。

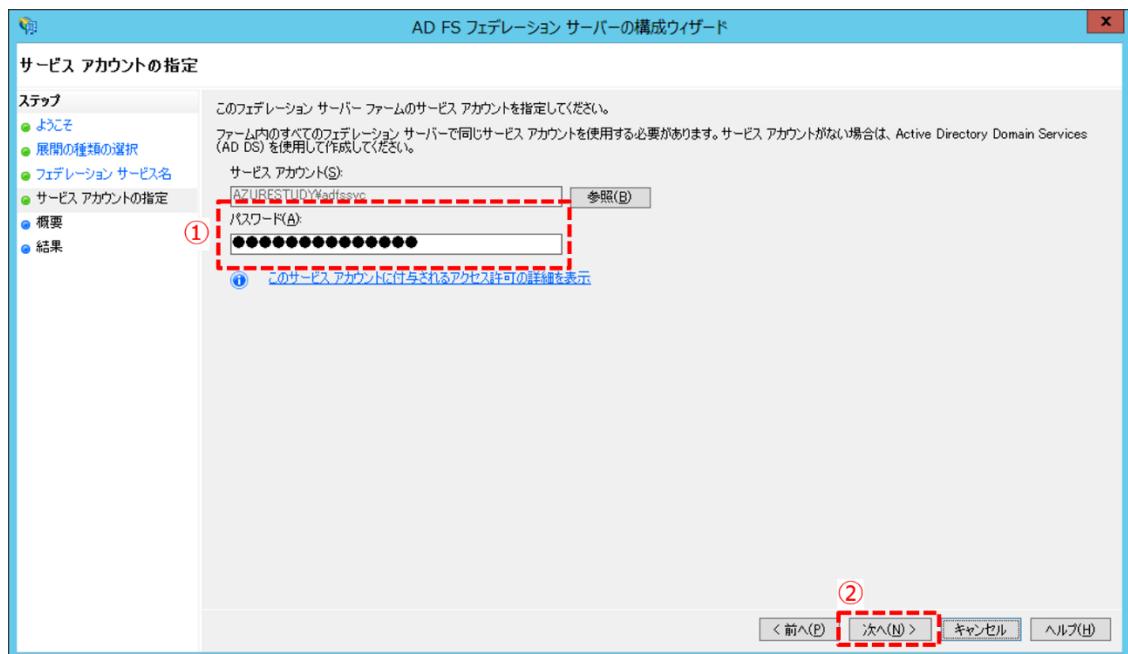
[サービス アカウント] の [参照] ボタンをクリックします。



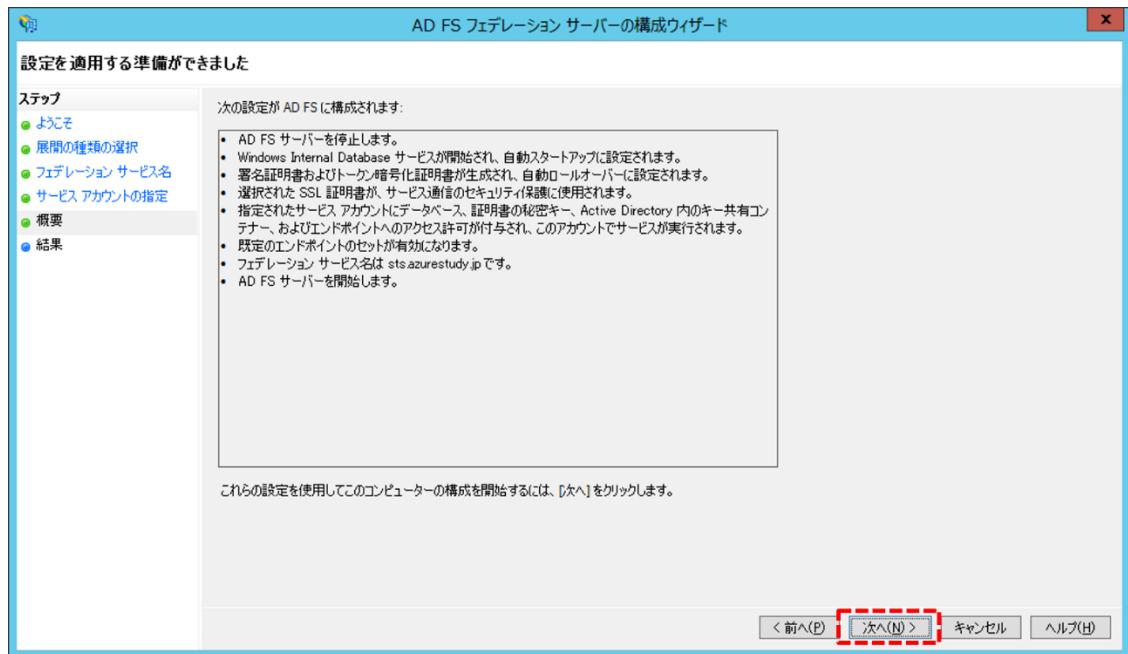
[ユーザー の選択] 画面が開きます。 「AD フェデレーション 用 サービス アカウント」を指定して [OK] ボタンをクリックして閉じます。



企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携
[サービス アカウントの指定] ページに戻り、[サービス アカウント] の [パスワード] を入力して [次へ] ボタンをクリックします。

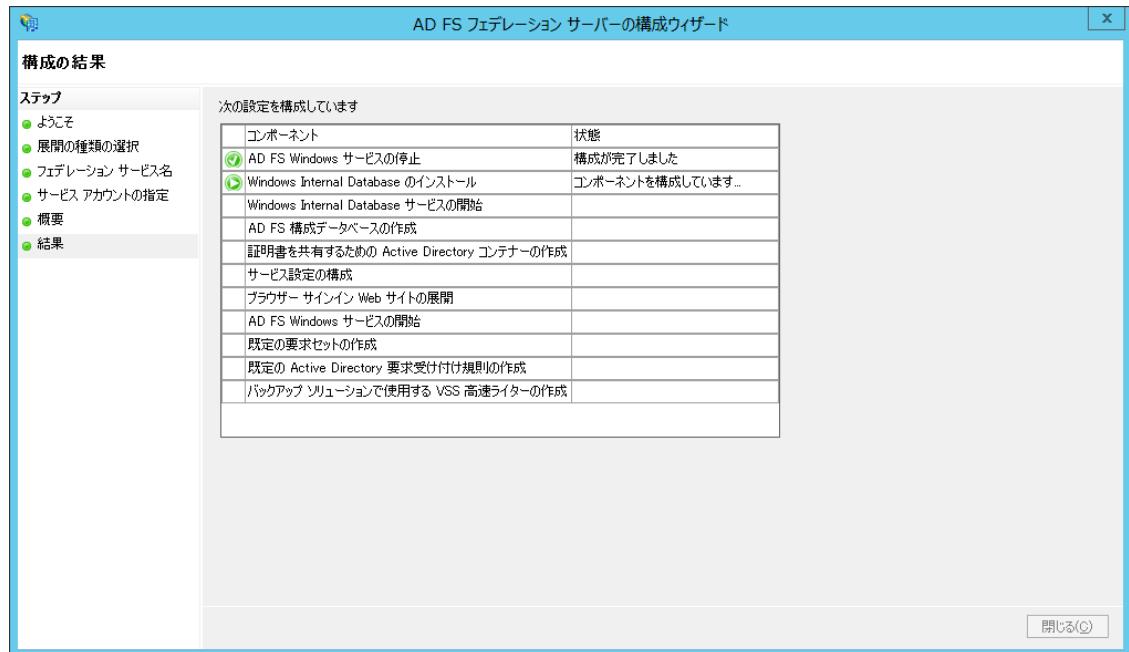


7. [設定を適用する準備ができました] ページにて [次へ] ボタンをクリックします。



企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

8. AD FS フェデレーション サーバーの構成のセットアップが完了するまで待ちます。



9. AD FS フェデレーション サーバーの構成のセットアップが完了したら、[閉じる] ボタンをクリックして閉じます。



企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

10. [AD FS の管理] 画面に戻り、下図の赤枠のように表示されていることを確認します。

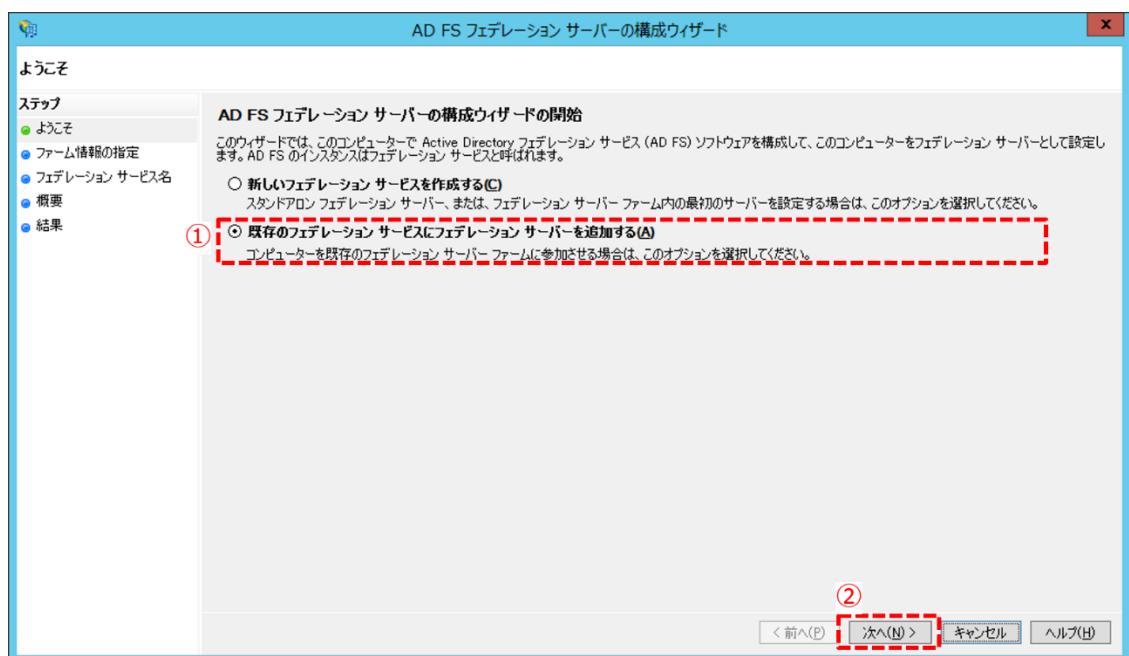


11.6 2 台目以降のフェデレーション サーバーの設定

- ドメイン管理者アカウントで AD FS サーバー セカンダリ [AZSTADFS02] にサインインし、[AD FS の管理] を開きます。
- 中央ペインにて [AD FS フェデレーション サーバーの構成ウィザード] をクリックします。

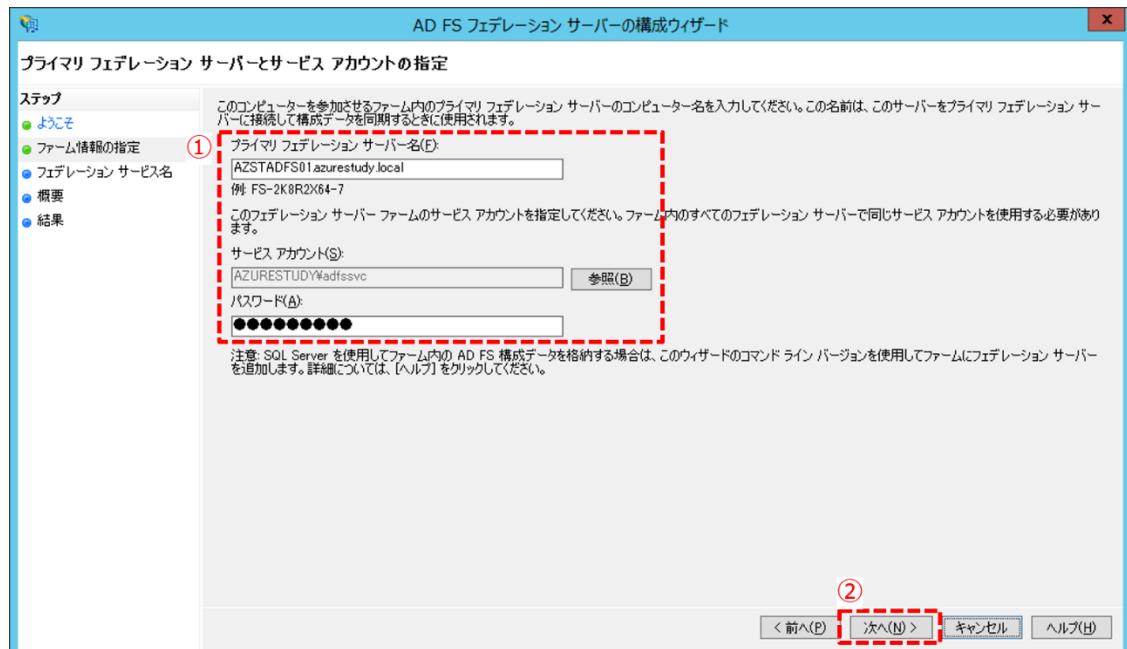


- [AD FS フェデレーション サーバーの構成ウィザード] 画面が開きます。[ようこそ] ページにて [既存のフェデレーション サービスにフェデレーション サーバーを追加する] を選択して [次へ] ボタンをクリックします。



企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

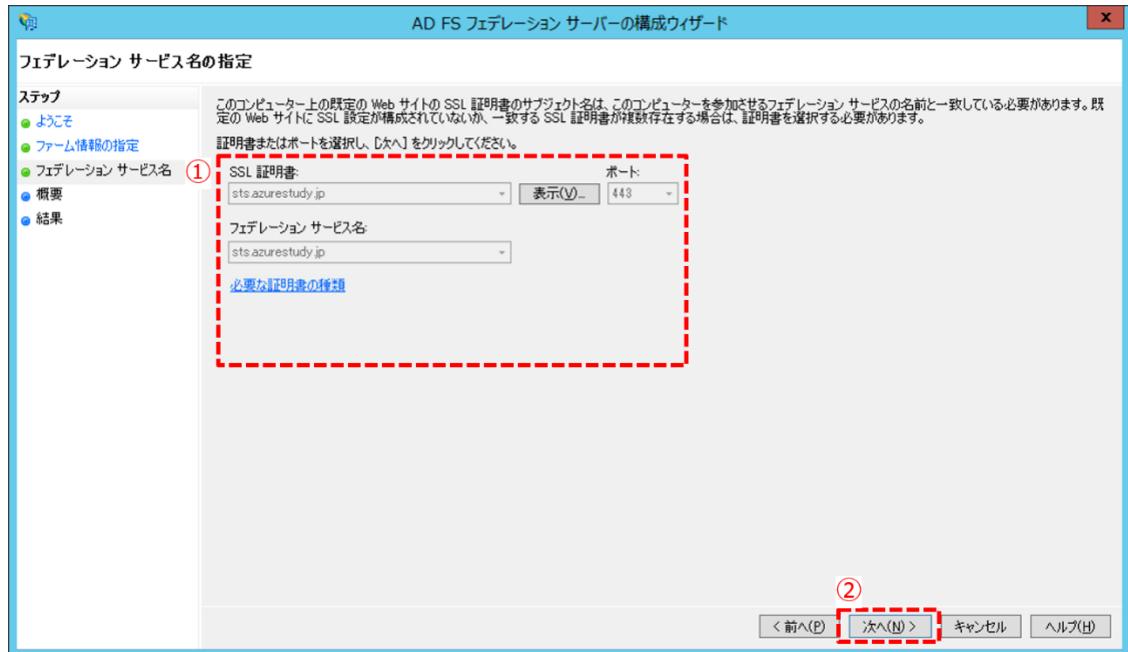
4. [プライマリ フェデレーション サーバーとサービス アカウントの指定] ページにて以下の表のとおり入力して [次へ] ボタンをクリックします。



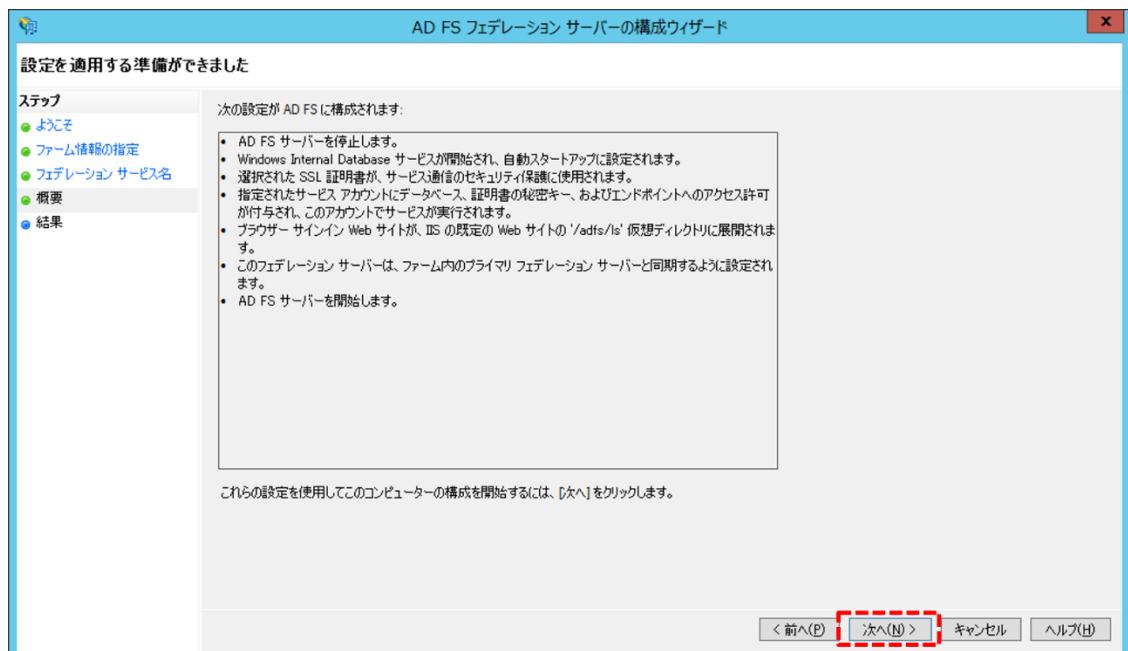
項目	設定値
プライマリ フェデレーション サーバー名	AZSTADFS01.azurestudy.local ※ AD FS サーバー プライマリ [AZSTADFS01]
サービス アカウント	AZURESTUDY\\$adfssvc ※ AD フェデレーション用サービスアカウント
パスワード	[サービスアカウント] のパスワード

企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

5. [フェデレーション サービス名の指定] ページにて [SSL 証明書] と [フェデレーション サービス名] に「sts.azurestudy.jp」が指定されていることを確認して [次へ] ボタンをクリックします。



6. [設定を適用する準備ができました] ページにて [次へ] ボタンをクリックします。



企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

7. AD FS フェデレーション サーバーの構成のセットアップが完了するまで待ちます。

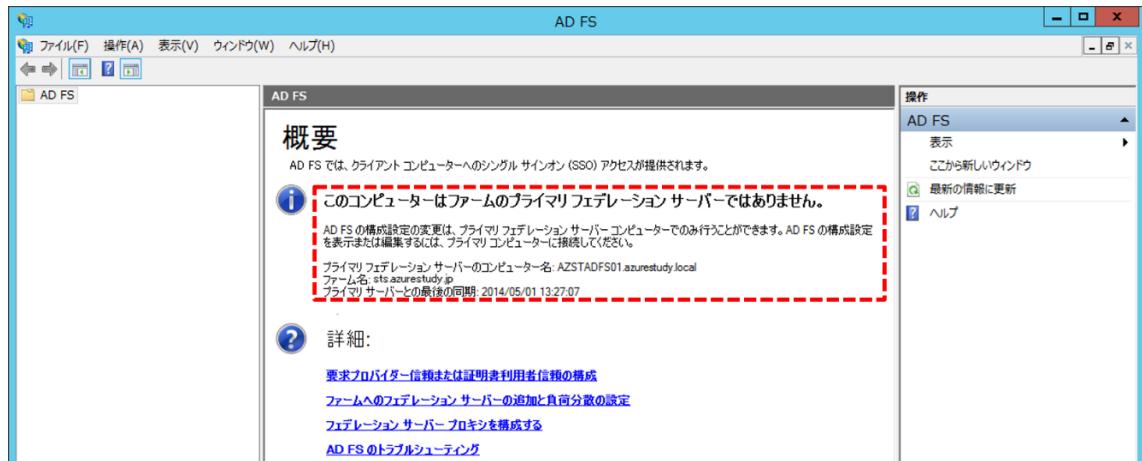


8. AD FS フェデレーション サーバーの構成のセットアップが完了したら、[閉じる] ボタンをクリックして閉じます。



企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

9. [AD FS の管理] 画面に戻り、下図の赤枠のように表示されていることを確認します。



Note : AD FS の構成設定の同期

AD FS の構成設定の変更は、AD FS サーバー プライマリ [AZSTADFS01] でのみ行うことができます。AD FS の構成設定を表示または編集するには、AD FS サーバー プライマリ にて作業します。

AD FS サーバー セカンダリ [AZSTADFS02] は、この「AD FS フェデレーション サーバーの構成のセットアップ」完了直後に、AD FS サーバー プライマリから構成設定が同期されます。その後、5 分間隔で構成設定が同期されます。

11.7 IT プロフェッショナル 用 Microsoft Online Services

サインイン アシスタントのインストール

Note : AD FS サーバー プライマリのみで実施

この項の作業は、AD FS サーバー プライマリ [AZSTADFS01] のみで実施します。

この項の作業は、後述の「11.9 フェデレーション ドメインの有効化 (= AD FS の構成設定の編集)」を行るために必要なものです。

また、AD FS の構成設定の編集は、AD FS サーバー プライマリで実施するので、AD FS サーバー セカンダリ [AZSTADFS02] には不要となります。

◆ IT プロフェッショナル 用 Microsoft Online Services サインイン アシスタント RTW をダウンロード

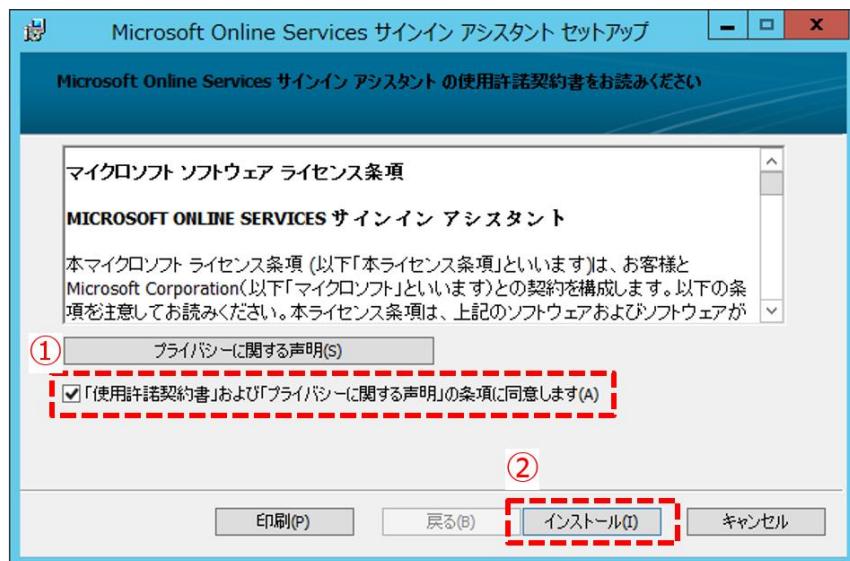
1. Microsoft ダウンロード センターより、「IT プロフェッショナル 用 Microsoft Online Services サインイン アシスタント RTW (64 ビット版)」をダウンロードします。

「IT プロフェッショナル 用 Microsoft Online Services サインイン アシスタント RTW (<http://www.microsoft.com/ja-jp/download/details.aspx?id=41950>)」

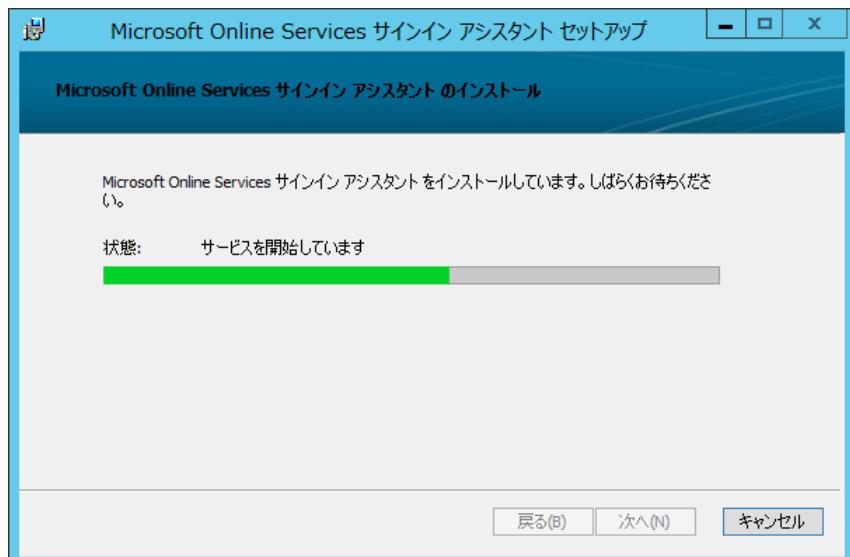
➔ IT プロフェッショナル 用 Microsoft Online Services サインイン アシスタント

RTW をインストール

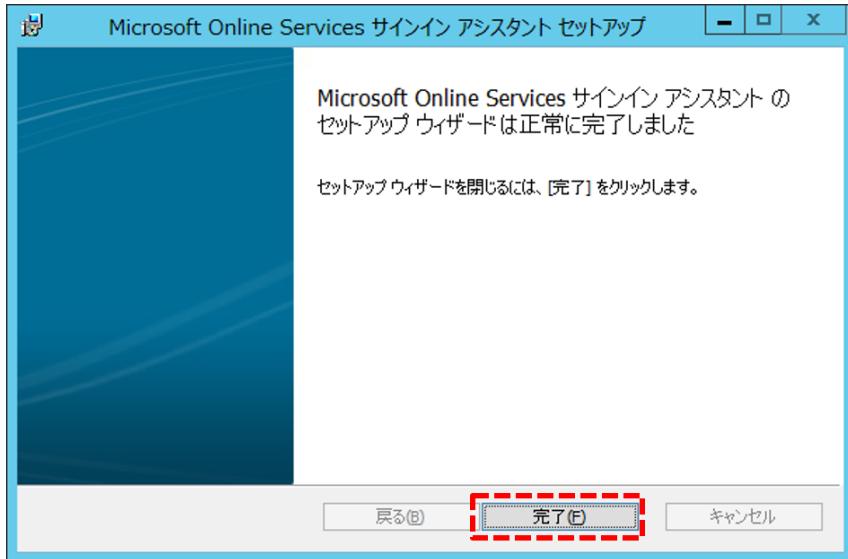
2. ドメイン管理者アカウントで AD FS サーバー プライマリ [AZSTADFS01] にサインインし、手順 1 でダウンロードした「IT プロフェッショナル 用 Microsoft Online Services サインイン アシスタント RTW (64 ビット版)」を任意の場所にコピーします。
3. [msoidcli_64.msi] をダブルクリックして [Microsoft Online Services サインイン アシスタント セットアップ] を起動します。
4. [Microsoft Online Services サインイン アシスタント の使用許諾契約書をお読みください] 画面にて [使用許諾契約書] をご確認いただき、同意される場合は [「使用許諾契約書」および「プライバシーに関する声明」に同意します] チェックボックスにチェックを付けて [インストール] ボタンをクリックします。



5. インストールが完了するまで待ちます。



6. 「Microsoft Online Services サインイン アシスタントのセットアップ ウィザードは正常に完了しました」とメッセージが表示されたら、[完了] ボタンをクリックして閉じます。



11.8 Windows PowerShell 用 Windows Azure Active Directory モジュールのインストール

Note : 事前に .NET Framework 3.5 Features を有効にしてください

Windows PowerShell 用 Windows Azure Active Directory モジュールの要件として .NET Framework 3.5 Features を有効にする必要があります。これについては「11.1 AD FS 2.1 関連をインストール」にてインストールしていますので、そちらをご確認ください。

Note : AD FS サーバー プライマリのみで実施

この項の作業は、AD FS サーバー プライマリ [AZSTADFS01] のみで実施します。

この項の作業は、後述の「11.9 フェデレーション ドメインの有効化 (= AD FS の構成設定の編集)」を行うために必要なものです。

また、AD FS の構成設定の編集は、AD FS サーバー プライマリで実施するので、AD FS サーバー セカンダリ [AZSTADFS02] には不要となります。

▼ Windows PowerShell 用 Windows Azure Active Directory モジュールをダウンロード

1. Office 365 管理者アカウントで「Office 365 管理センター」にサインインします。
2. [管理者の概要] ページの左側にある [ユーザーとグループ] をクリックします。



企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

3. [アクティブなユーザー] ページにて [シングル サインオン] にある [セットアップ] をクリックします。

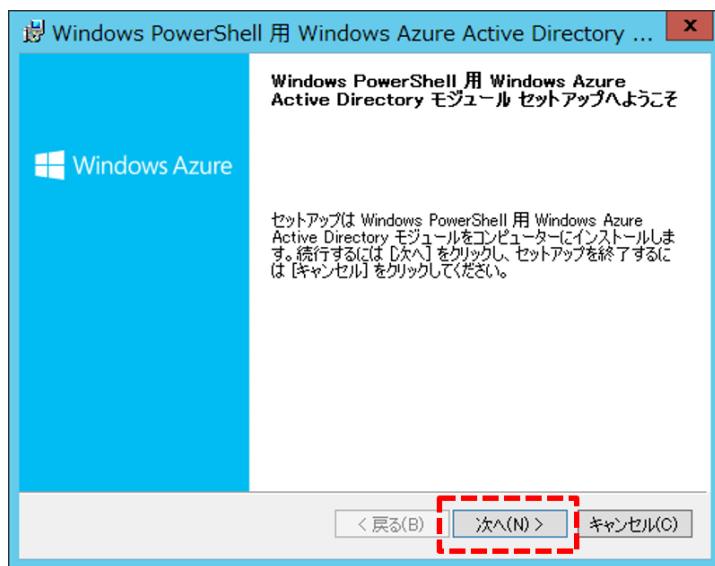


4. [シングル サインオンのセットアップと管理] ページにて [3 Windows PowerShell 用 Windows Azure Active Directory モジュールをインストールする] で [Windows 64 ビット版] を選択し、[ダウンロード] をクリックして「Windows PowerShell 用 Windows Azure Active Directory モジュール (64 ビット版)」をダウンロードします。

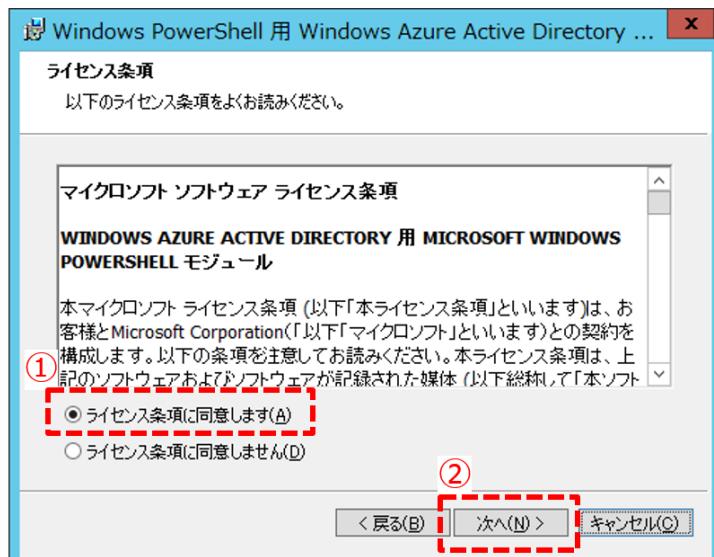


◆ Windows PowerShell 用 Windows Azure Active Directory モジュールをインストール

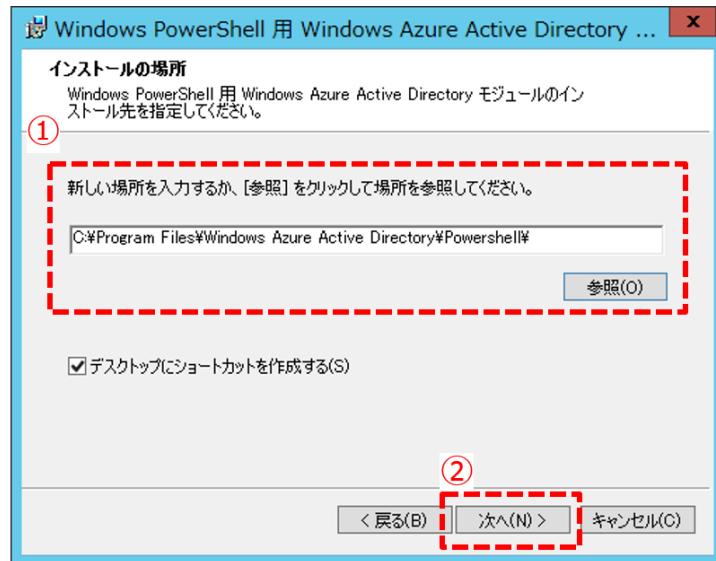
5. ドメイン管理者アカウントで AD FS サーバー プライマリ [AZSTADFS01] にサインインし、手順 1 ~ 4 でダウンロードした「Windows PowerShell 用 Windows Azure Active Directory モジュール (64 ビット版)」を任意の場所にコピーします。
6. [AdministrationConfig-JA.msi] をダブルクリックして [Windows PowerShell 用 Windows Azure Active Directory モジュール セットアップ] を起動します。
7. [ようこそ] 画面にて [次へ] ボタンをクリックします。



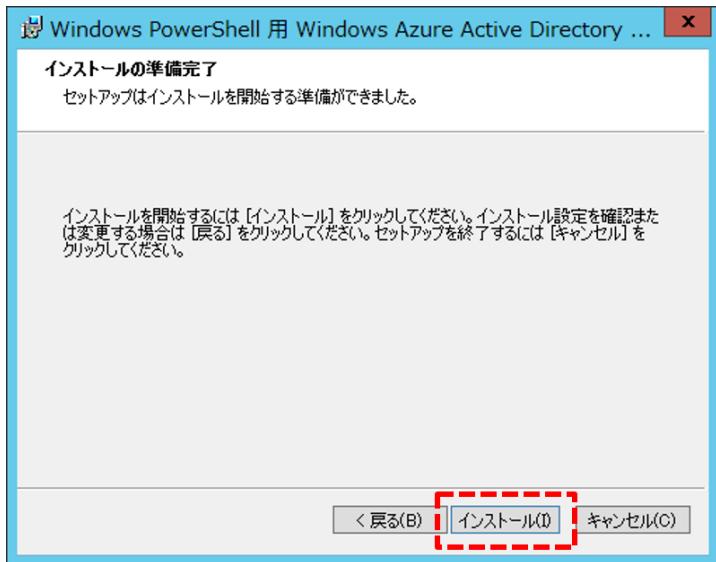
8. [ライセンス条項] 画面にて [マイクロソフト ソフトウェア ライセンス条項] をご確認いただき、同意される場合は [ライセンス条項に同意します] を選択して [次へ] ボタンをクリックします。

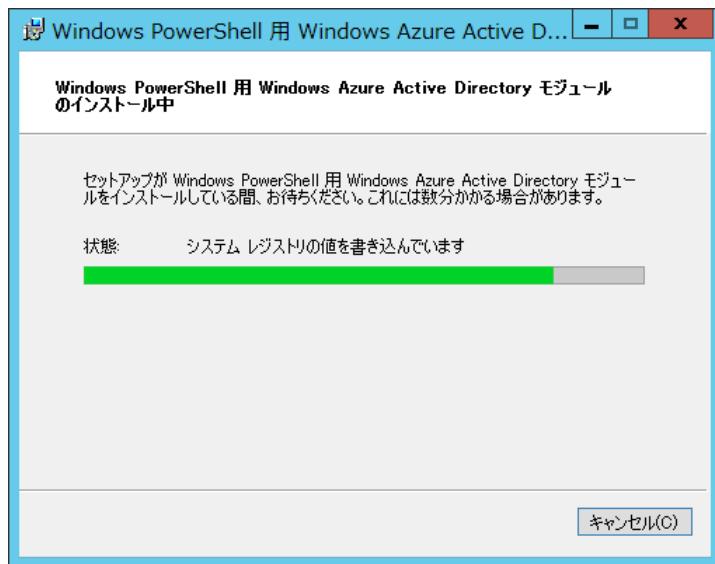
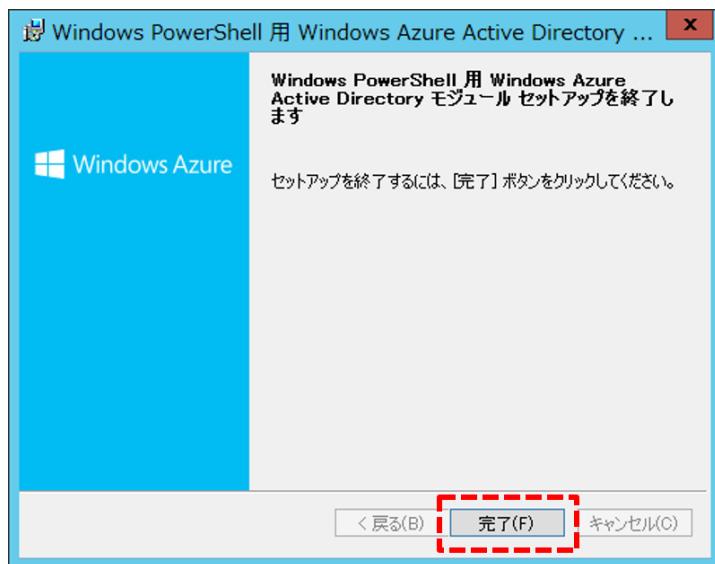


9. [インストールの場所] 画面にて Windows PowerShell 用 Windows Azure Active Directory モジュールのインストール先を指定して [次へ] ボタンをクリックします。



10. [インストールの準備完了] 画面にて [インストール] ボタンをクリックします。



11. インストールが完了するまで待ちます。**12.** 「Windows PowerShell 用 Windows Azure Active Directory モジュール セットアップを終了します」とメッセージが表示されたら、[完了] ボタンをクリックして閉じます。

11.9 フェデレーション ドメインの有効化

◆ “Microsoft Online Services User ID” から “フェデレーション ID” へ

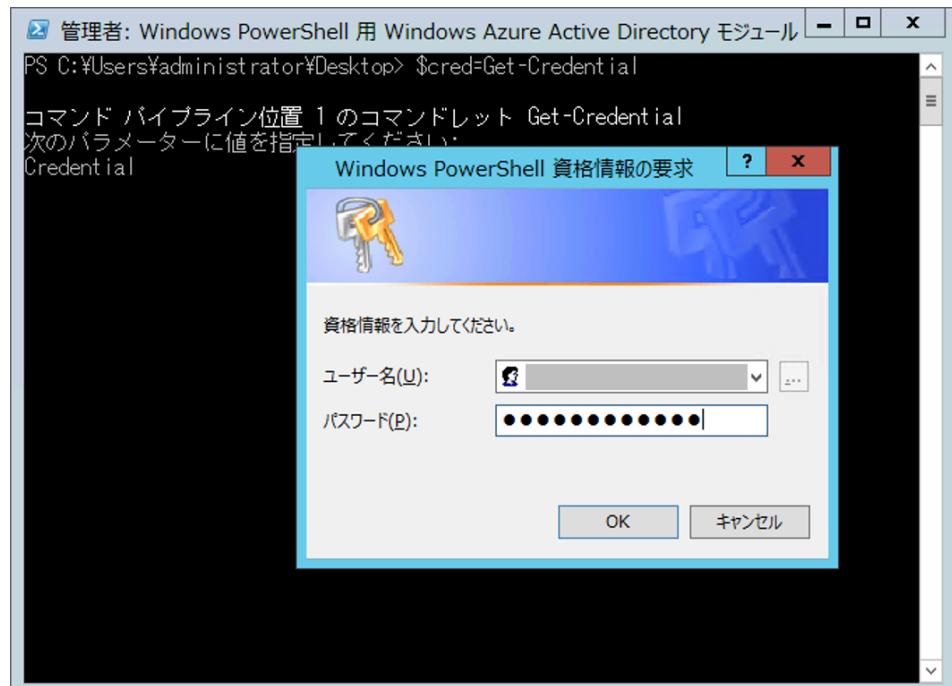
1. ドメイン管理者アカウントで AD FS サーバー プライマリ [AZSTADFS01] にサインインし、[AD FS の管理] を開きます。
2. 中央ペインにて [概要] に「必要な構成が未完了です」と表示されていることを確認します。



3. [Windows PowerShell 用 Windows Azure Active Directory モジュール] を「管理者として実行」で開き、以下のコマンドを実行します。

```
$cred=Get-Credential (*1)
Connect-MsolService -Credential $cred
Convert-MsolDomainToFederated -DomainName azurestudy.jp
```

- ✓ (*1) : 資格情報の入力画面が表示されるので、Office 365 管理者アカウントのユーザー名、パスワードを入力します。



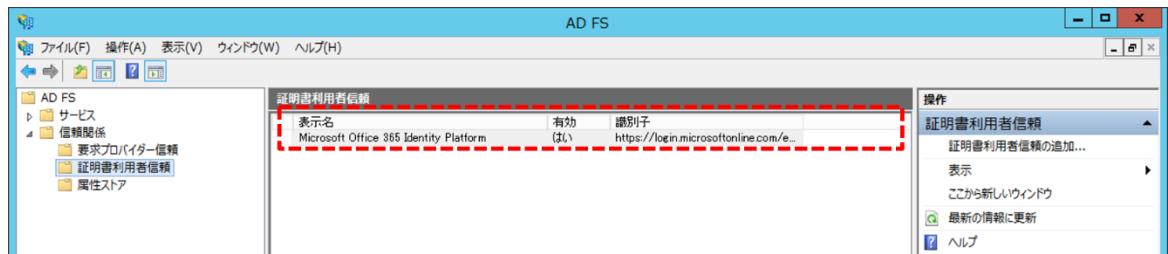
上記のコマンドを実行後、“Successfully updated 'azurestudy.jp' domain.” と表示されると、ドメインが標準のドメインからフェデレーション ドメインと変更されます。

4. [AD FS の管理] に戻り、[操作] メニュー > [最新の情報に更新] をクリックします。手順 2 のメッセージが消えていることを確認します。



企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

5. 左ペインにて [AD FS] > [信頼関係] > [証明書利用者信頼] と展開して、中央ペインに [Microsoft Office 365 Identity Platform] が登録されていることを確認します。

**Note : トークン署名証明書を更新された際の注意事項**

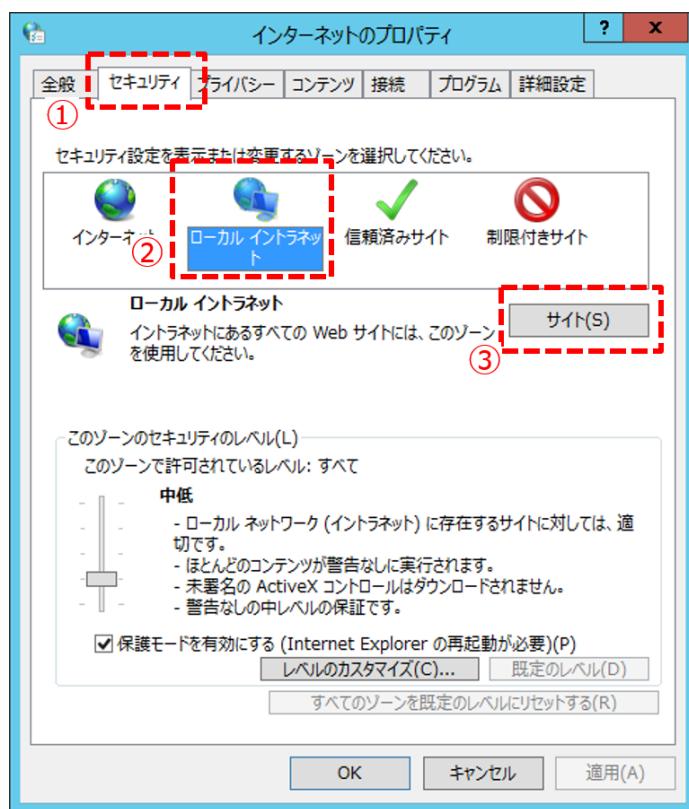
フェデレーション サーバーが発行し、Office 365 に登録されたトークン署名証明書は、期限が 1 年です。証明書自体は、フェデレーション サーバーによって自動で更新されます。ただし、その更新を Office 365 に反映する必要があります。 更新方法については、以下の記事を参照してください。

「AD FS 2.0 トークン署名証明書のロールオーバーにより、すべての Office 365 のサービスへのアクセスができなくなる - ディレクトリ統合サービス - Office 365 - 日本語 - Microsoft Office 365 Community (<http://community.office365.com/ja-jp/w/sso/3329.aspx>)」

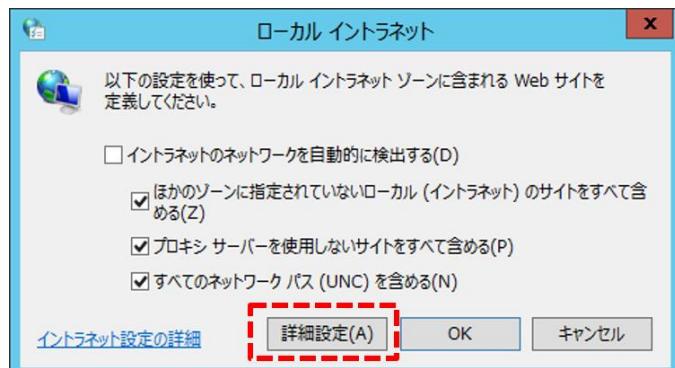
11.10 ローカル イントラネット ゾーンへのサイトの登録

社内の AD 環境内にて Office 365 SSO を実現させるため、AD FS フェデレーション サービス名 (FQDN) を [Internet Explorer] の「ローカル イントラネット」ゾーンとして追加します。

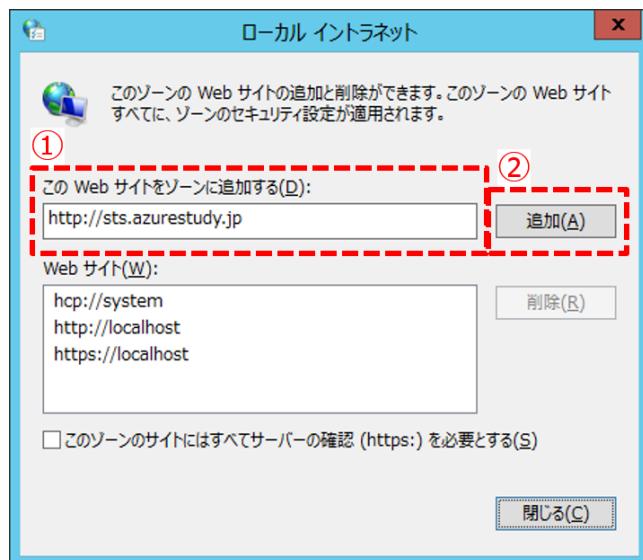
1. クライアント PC にサインインします。
2. [コントロール パネル] > [インターネット オプション] を開きます。
3. [セキュリティ] タブを開き、[ローカル イントラネット] を選択して [サイト] ボタンをクリックします。



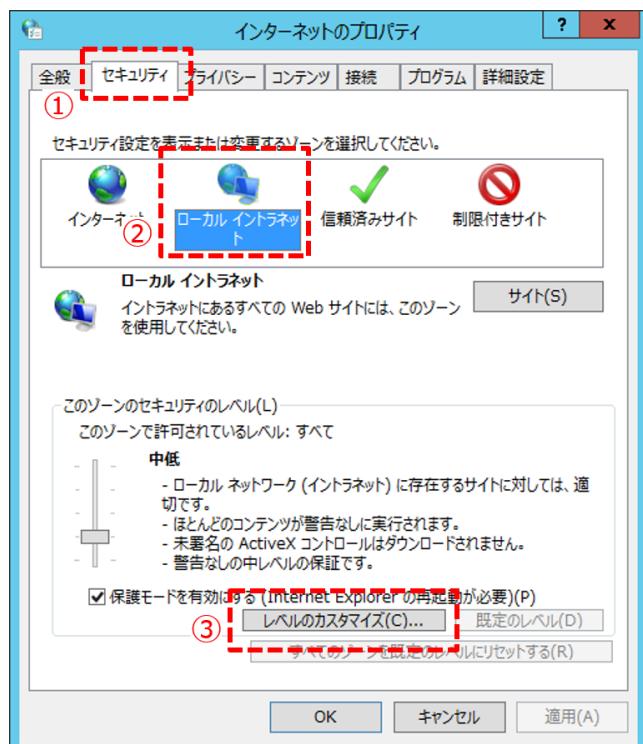
4. [ローカル イントラネット] 画面にて [詳細設定] ボタンをクリックします。



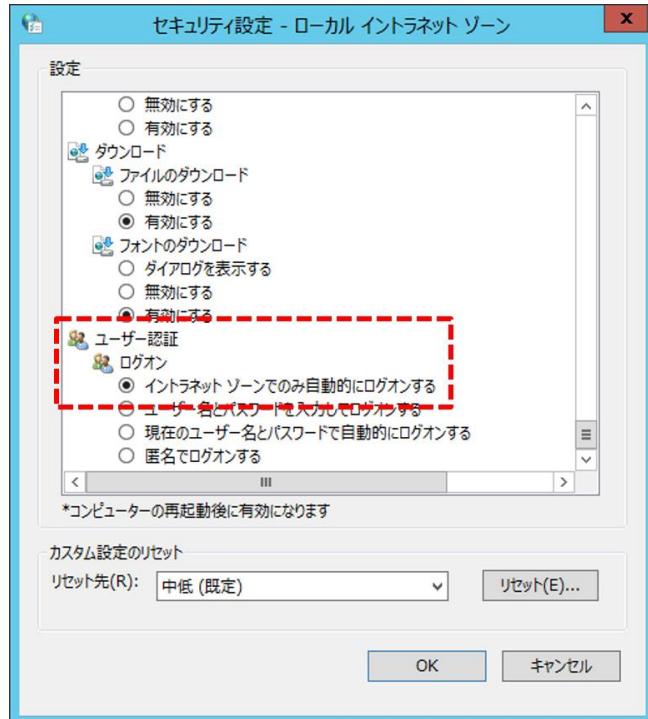
5. [ローカル イントラネット] 画面にて [この Web サイトをゾーンに追加する] に「<https://sts.azurestudy.jp>」と入力して [追加] ボタンをクリックします。追加したら、[閉じる] ボタンをクリックして閉じます。



6. [セキュリティ] タブを開き、[ローカル イントラネット] を選択して [レベルのカスタマイズ] ボタンをクリックします。



7. [ユーザー認証] > [ログオン] で [インターネット ゾーンのみ自動的にログオンする] が選択されていることを確認します。



11.11 フェデレーション環境の動作確認

AD FS サーバーのセットアップが完了したら、以下の内容を基にフェデレーション環境が正常に稼動しているか確認を行います。

➔ AD FS サーバーでの確認

1. ドメイン管理者アカウントで AD FS サーバー ([AZSTADFS01] および [AZSTADFS02]) にサインインします。
2. [サービス] を開き、以下の表で挙げたサービスのプロパティを確認します。

	スタートアップの種類	サービスの状態	アカウント
AD FS Windows Service	自動 (遅延実行)	実行中(開始)	「AZURESTUDY\\$adfssvc」
Microsoft Online Services Sign-in Assistant	自動	実行中(開始)	ローカル システム アカウント

3. [イベント ビューアー] を開き、以下のイベント ログが出力されていることを確認します。

項目	内容
ログ保存場所	[アプリケーションとサービス ログ] > [AD FS] > [Admin]
ソース	AD FS
イベント ID	349
ログの内容	フェデレーション サービスの管理サービスが正常に開始されました。AD FS の Windows Powershell コマンドを使用すると、フェデレーション サービスの構成を変更できます。次のサービス ホストが追加されました: ポリシー管理 ServiceHost net.tcp://localhost:1500/policy net.tcp://localhost:1500/policy net.tcp://localhost:1500/policy http://sts.azurestudy.jp:80/adfs/services/policystoretransfer net.tcp://localhost:1501/adfs/services/policystoretransfer

企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

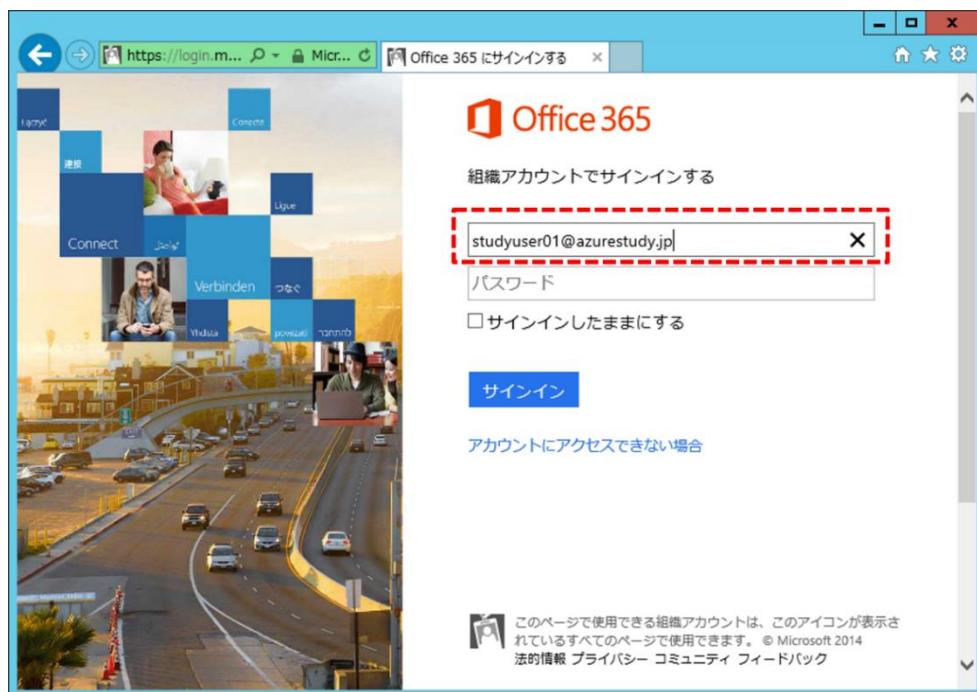
項目	内容
ログ保存場所	[アプリケーションとサービス ログ] > [AD FS] > [Admin]
ソース	AD FS
イベント ID	100
ログの内容	<p>フェデレーション サービスは正常に開始されました。次のサービス ホストが 追加されました:</p> <p>フェデレーション サーバー プロキシ ServiceHost https://sts.azurestudy.jp:443/adfs/services/proxytrustpolicystoretransfer</p> <p>AD FS 1.x 信頼情報サービス https://sts.azurestudy.jp/adfs/fs/federationserverservice.asmx</p> <p>SAML トークン発行 ServiceHost net.tcp://localhost:1501/samlprotocol https://sts.azurestudy.jp/adfs/services/trust/samlprotocol/proxytrust</p> <p>発行 ServiceHost http://localhost:80/adfs/services/trust/mexsoap https://sts.azurestudy.jp:443/adfs/services/trust/proxymexhttpget/</p> <p>発行 ServiceHost https://sts.azurestudy.jp/adfs/services/trust/proxymex https://sts.azurestudy.jp:443/adfs/services/trust/proxymexhttpget/</p> <p>発行 ServiceHost https://sts.azurestudy.jp/adfs/services/trust/2005/windowstransport https://sts.azurestudy.jp/adfs/services/trust/2005/certificatemixed https://sts.azurestudy.jp/adfs/services/trust/2005/certificatetransport https://sts.azurestudy.jp/adfs/services/trust/2005/usernamemixed https://sts.azurestudy.jp/adfs/services/trust/2005/kerberosmixed https://sts.azurestudy.jp/adfs/services/trust/2005/issuedtokennmixedasymmetricbasic256 https://sts.azurestudy.jp/adfs/services/trust/2005/issuedtokennmixedasymmetricbasic256 https://sts.azurestudy.jp/adfs/services/trust/13/kerberosmixed https://sts.azurestudy.jp/adfs/services/trust/13/certificatemixed https://sts.azurestudy.jp/adfs/services/trust/13/usernamemixed https://sts.azurestudy.jp/adfs/services/trust/13/issuedtokennmixedasymmetricbasic256 https://sts.azurestudy.jp/adfs/services/trust/13/issuedtokennmixedasymmetricbasic256 net.tcp://localhost:1501/adfs/services/trusttcp/windows https://sts.azurestudy.jp/adfs/services/trust/proxytrust https://sts.azurestudy.jp/adfs/services/trust/proxytrust13 https://sts.azurestudy.jp/adfs/services/trust/proxytrustprovisionusername https://sts.azurestudy.jp/adfs/services/trust/proxytrustprovisionissuedtoken</p> <p>SAML メタデータ https://sts.azurestudy.jp/FederationMetadata/2007-06/</p>

4. 別途 SQL Server の完全なインスタンスをインストールした (AD FS 構成データベースとして SQL Server を採用した) 場合は、[SQL Server Management Studio] を起動して、[AdfsArtifactStore] データベース、[AdfsConfiguration] データベースがあることを確認します。

※ この自習書では、SQL Server をインストールしていないため、確認は不要となります。

→ クライアント PC での確認

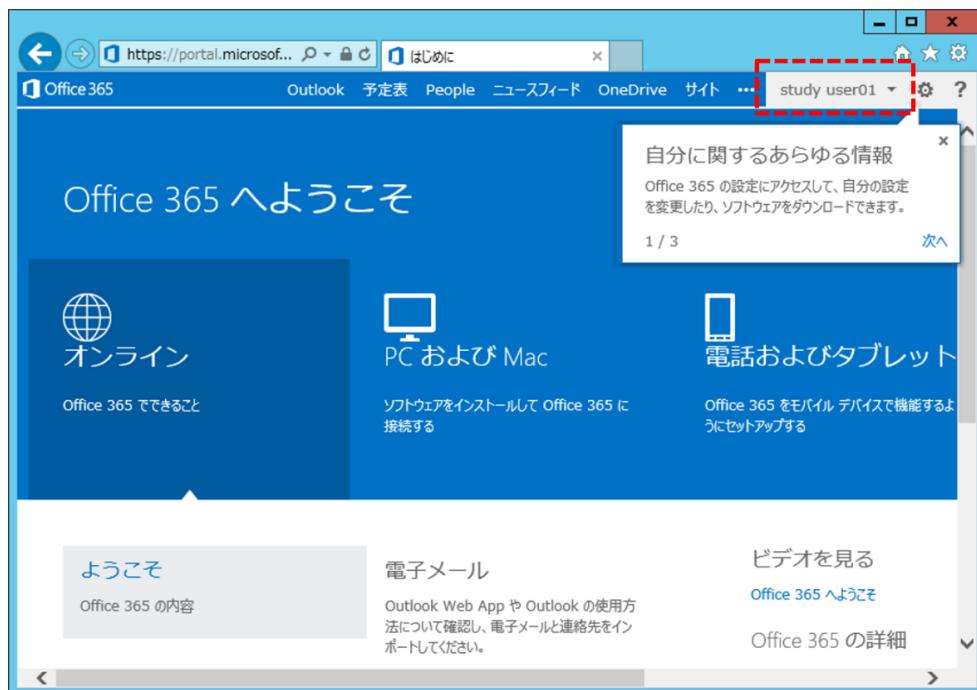
5. 「azurestudy.local」ドメイン内にあるクライアント PC にサインインします。
6. [Internet Explorer] を開きます。
7. アドレス欄に「<https://portal.office.com/Home> (Office 365 ポータル)」と入力してアクセスします。
8. 資格情報を求められるので、UPN [<user>@azurestudy.jp] を入力して、フォーカスを移動 ([TAB] キー押下) します。



9. 下図のように AD FS 用の認証処理が行われます。



10. [Office 365 ポータル] ページが表示されたら、下図（右上）のように適切なユーザーでサインインしていることを確認します。



STEP 12. AD FS Proxy サーバーの セットアップ、および動作確認

この STEP では、構築した AD FS 環境に AD FS Proxy サーバーを実装する手順について説明します。

この手順を実施することで、会社の外からでも Office 365 の各種サービスにアクセスできる環境が整います。

この STEP では、次のことを学習します。

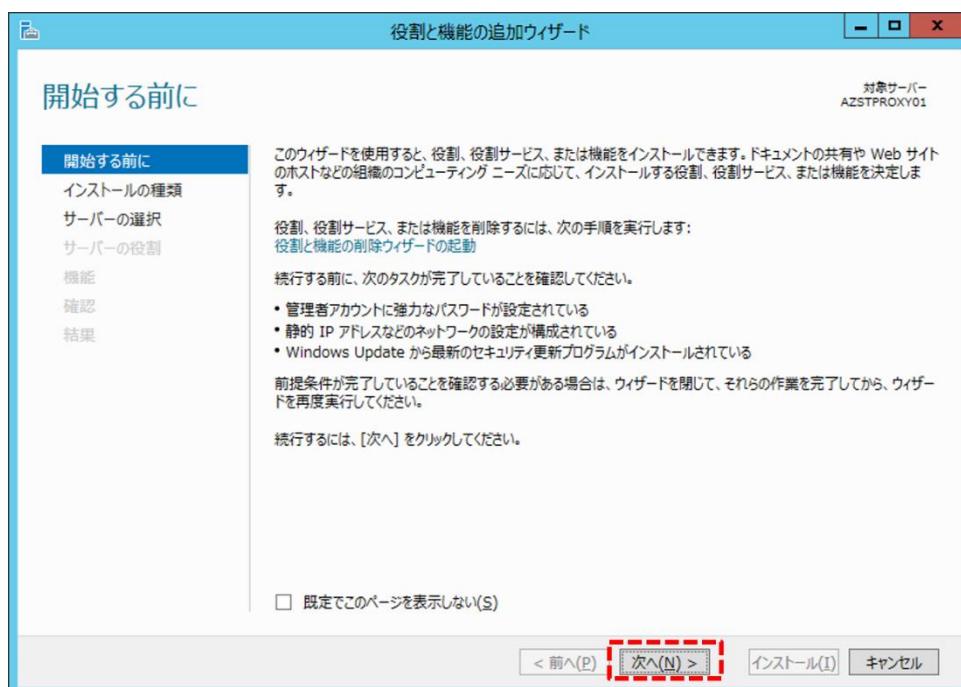
- ✓ AD FS 2.1 関連をインストール
- ✓ サーバー証明書をインポートと設定
- ✓ エンドポイント HTTPS を作成
- ✓ 社外 DNS の設定
- ✓ フェデレーション サーバー プロキシの設定
- ✓ AD FS Proxy サーバーの動作確認

12.1 AD FS 2.1 関連をインストール

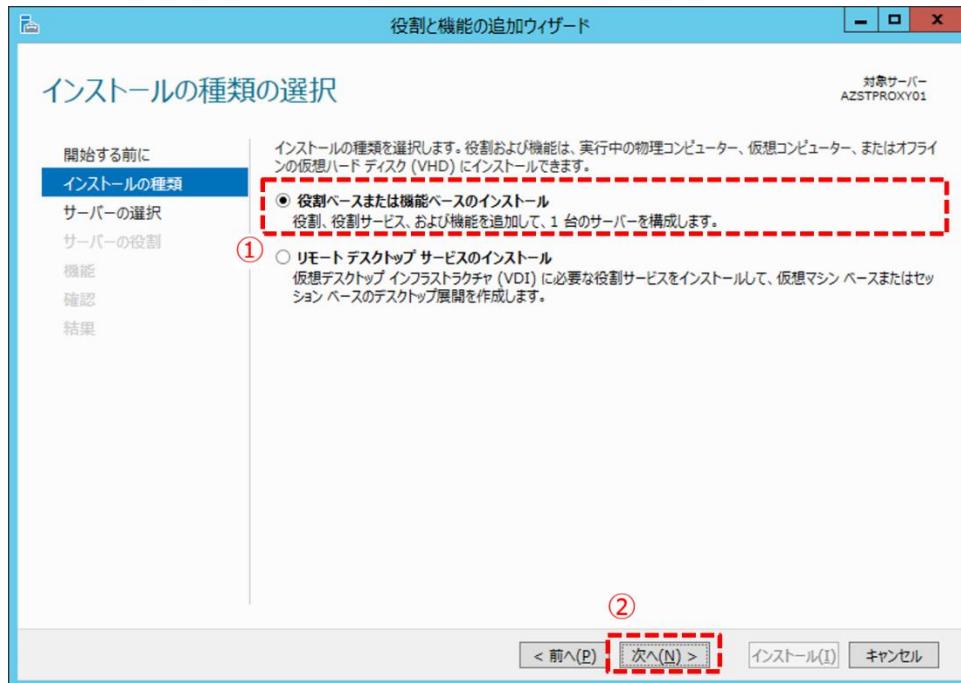
- ローカル管理者アカウントで AD FS Proxy サーバー [AZSTPROXY01] にサインインし、[サーバー マネージャー] を開きます。
- [管理] メニュー > [役割と機能の追加] をクリックします。



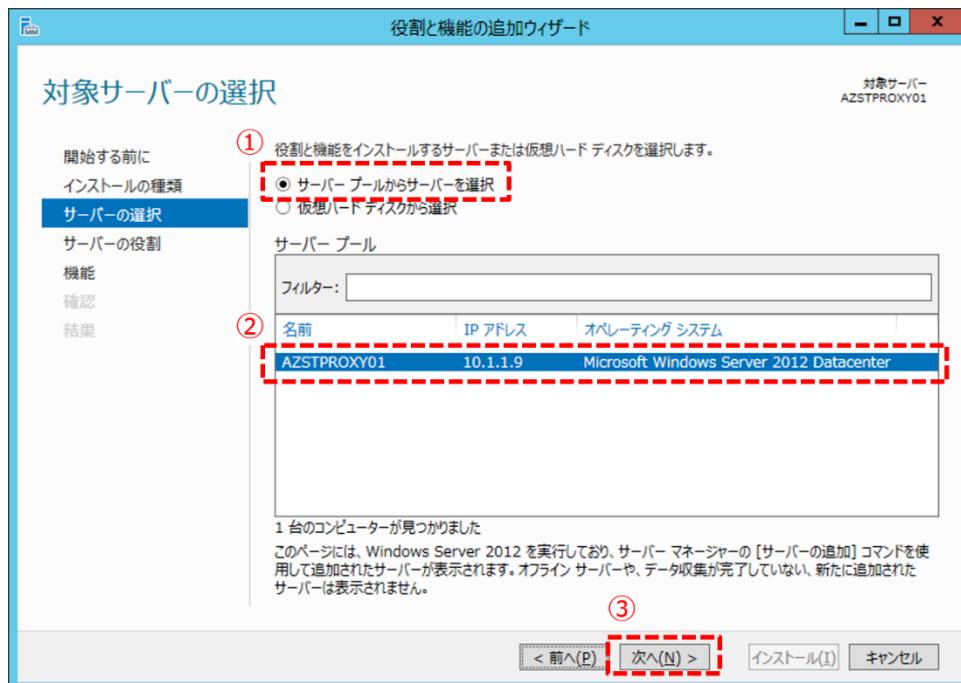
- [役割と機能の追加ウィザード] 画面が開きます。[開始する前に] ページにて [次へ] ボタンをクリックします。



4. [インストールの種類の選択] ページにて [役割ベースまたは機能ベースのインストール] を選択して [次へ] ボタンをクリックします。

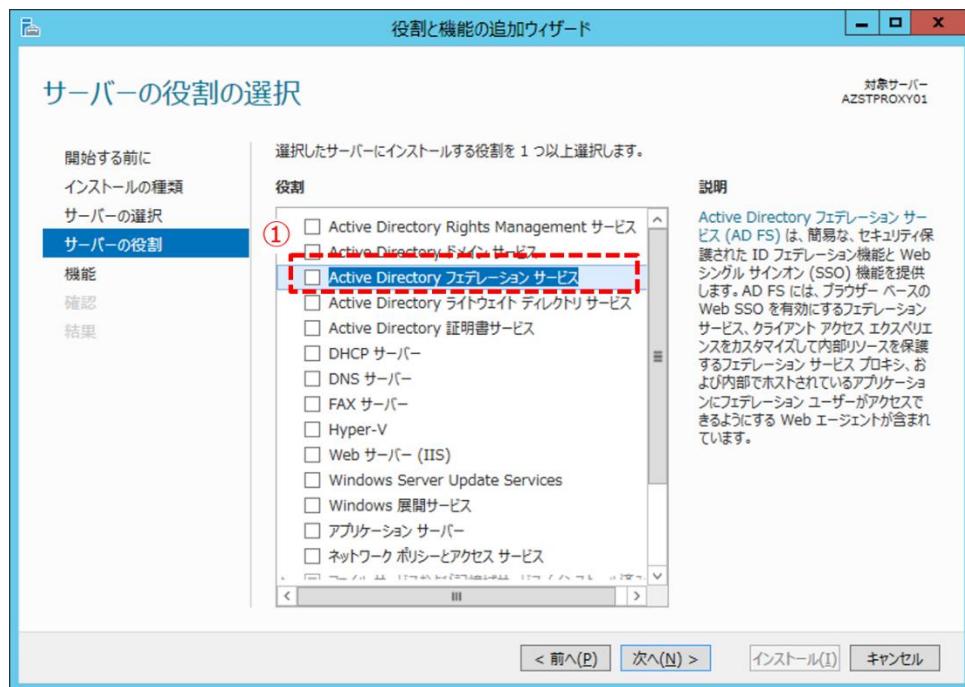


5. [対象サーバーの選択] ページにて [サーバー プールからサーバーを選択] を選択し、[サーバー プール] から AD FS サーバー プライマリ [AZSTADFS01] を選択して [次へ] ボタンをクリックします。

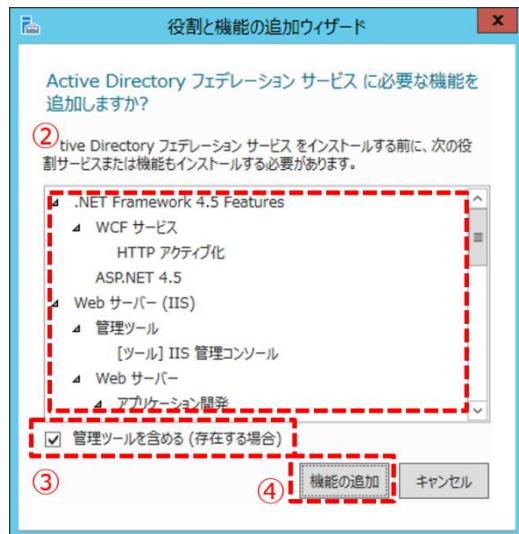


企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

6. [サーバーの役割の選択] ページにて [役割] 一覧から [Active Directory フェデレーション サービス] のチェックボックスにチェックを付けます。



以下の画面が開きます。[Active Directory フェデレーション サービス] が依存するサービス、および機能も追加する必要があるので内容を確認し、[管理ツールを含める (存在する場合)] チェックボックスにチェックを付けて [機能の追加] ボタンをクリックして閉じます。

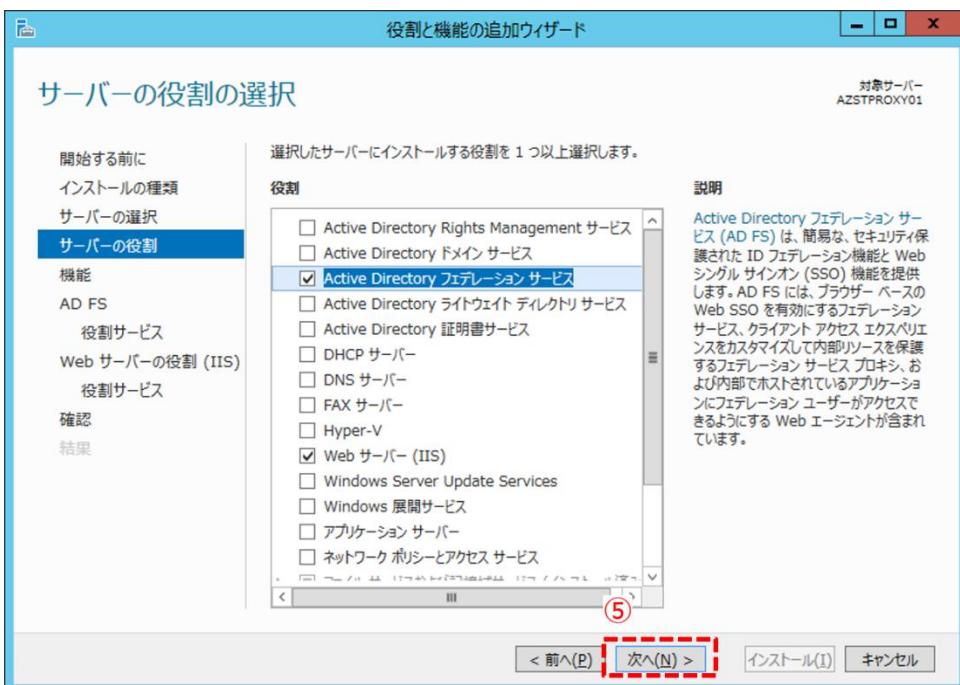


企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

【表：[Active Directory フェデレーション サービス] が依存するサービスと機能】

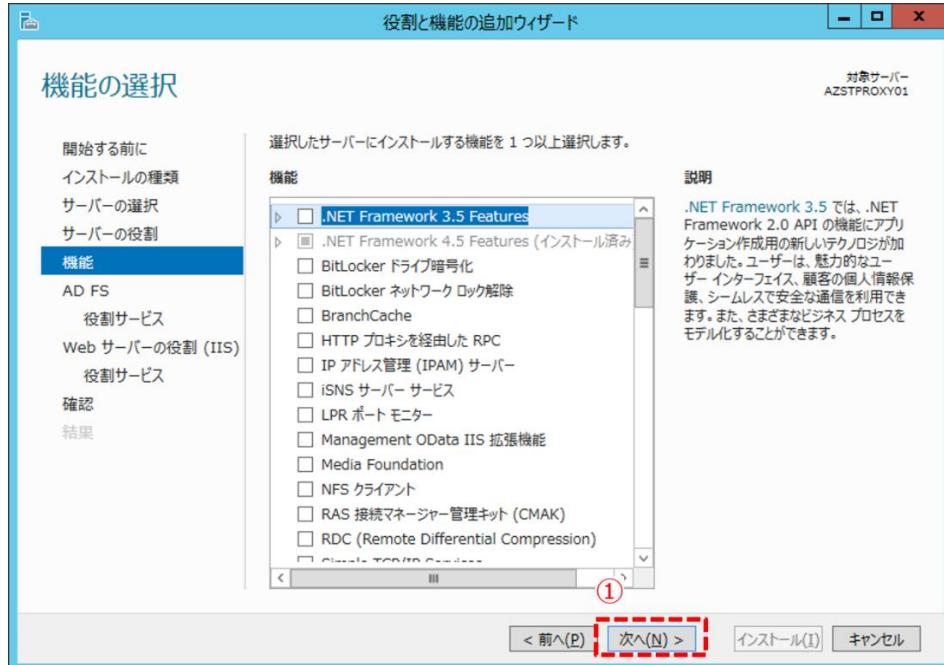
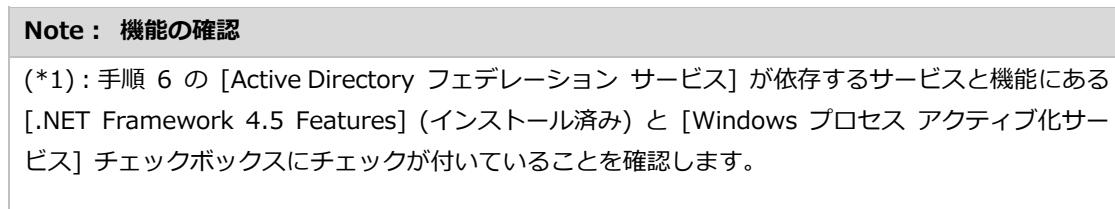
.NET Framework 4.5 Features	WCF サービス	HTTP アクティビ化		
	ASP.NET 4.5			
Web サーバー (IIS)	管理ツール	[ツール] IIS 管理コンソール		
	Web サーバー	アプリケーション開発	ASP.NET 4.5	
			ISAPI 拡張	
			ISAPI フィルター	
			.NET 拡張機能 4.5	
		HTTP 共通機能	既存のドキュメント	
			ディレクトリの参照	
			HTTP エラー	
			HTTP リダイレクト	
			静的なコンテンツ	
		状態と診断	HTTP ログ	
		パフォーマンス	静的なコンテンツの圧縮	
		セキュリティ	クライアント証明書マッピング認証	
			要求フィルター	
			Windows 認証	
Windows プロセス アクティビ化サービス	構成 API			
	プロセス モデル			

[サーバーの役割の選択] ページに戻ると、[Active Directory フェデレーション サービス] と [Web サーバー (IIS)] のチェックボックスにチェックが付きます。[次へ] ボタンをクリックします。

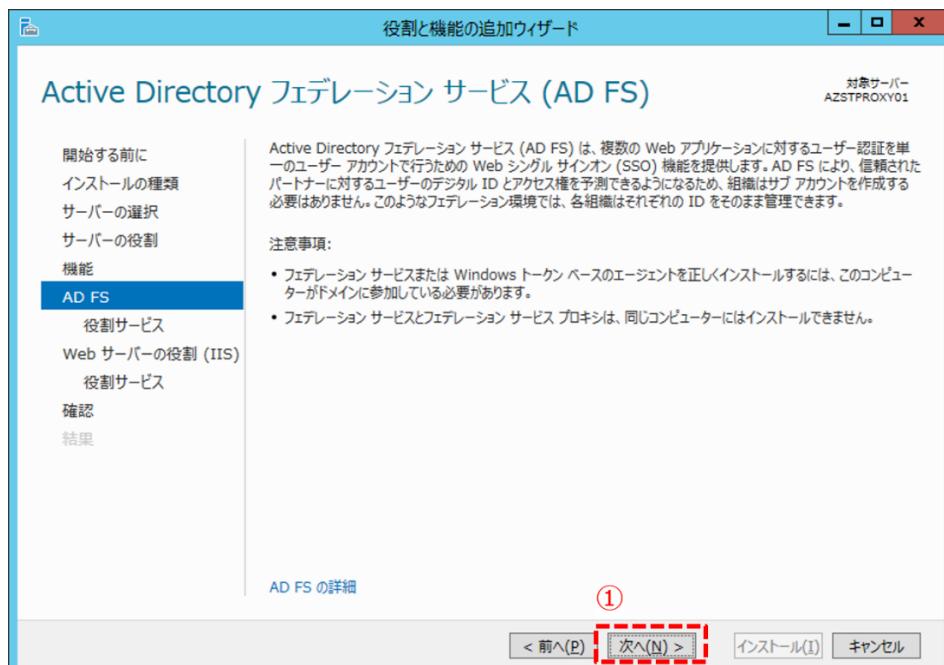


企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

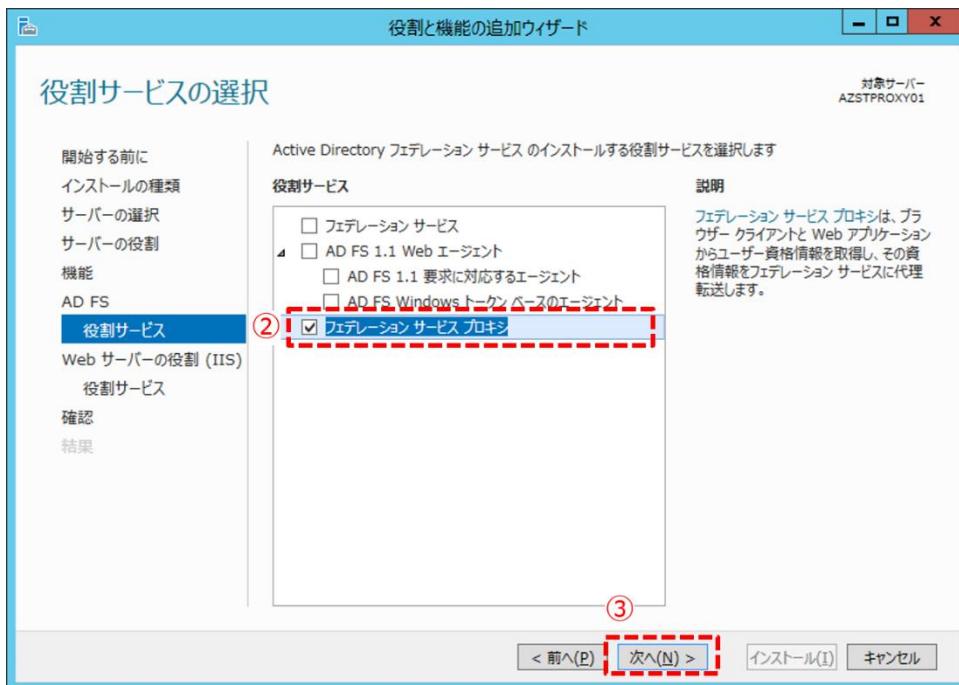
7. [機能の選択] ページにて [次へ] ボタンをクリックします。 (*1)



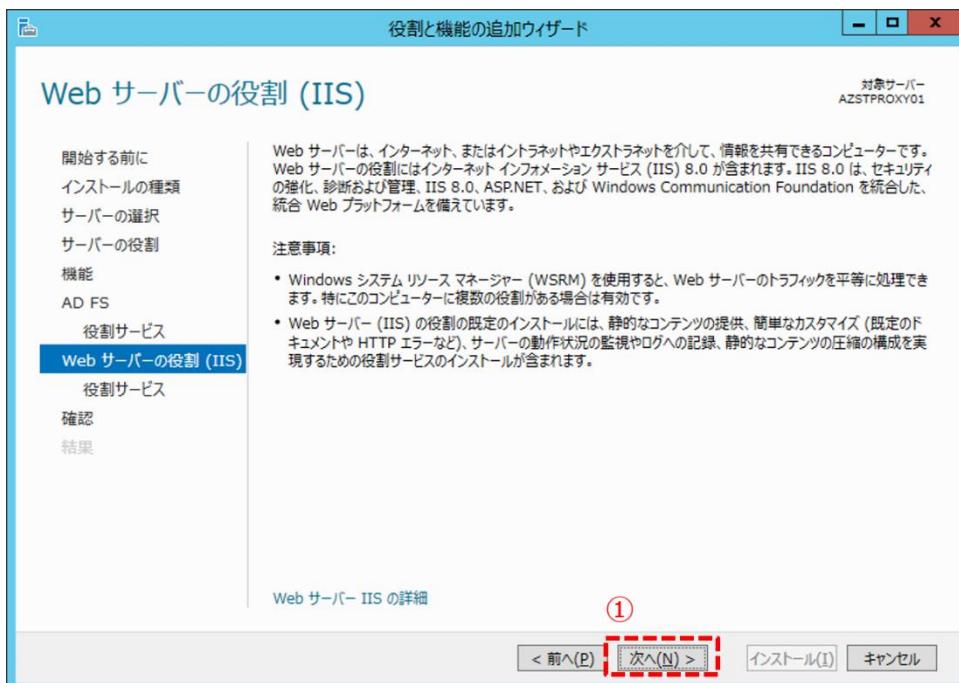
8. [Active Directory フェデレーション サービス (AD FS)] ページにて [次へ] ボタンをクリックします。



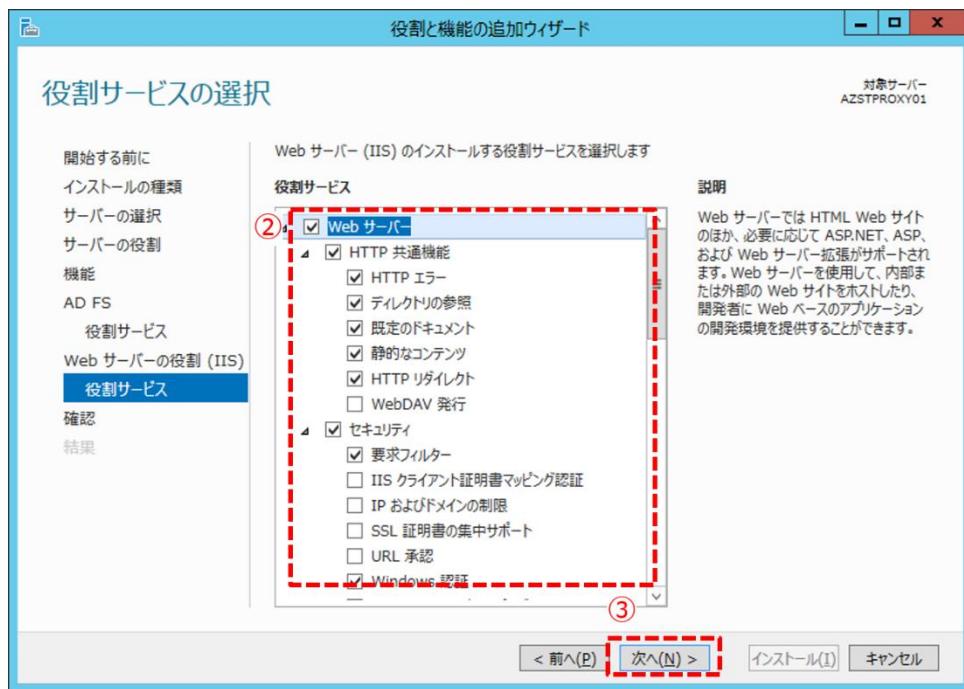
[AD FS の役割サービスの選択] ページにて、[役割サービス] から [フェデレーション サービス プロキシ] チェックボックスのみにチェックを付けて [次へ] ボタンをクリックします。



9. [Web サーバーの役割 (IIS)] ページにて [次へ] ボタンをクリックします。



企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携 [Web サーバーの役割サービスの選択] ページにて、[役割サービス] から以下の表の項目にチェックが付いていることを確認して [次へ] ボタンをクリックします。

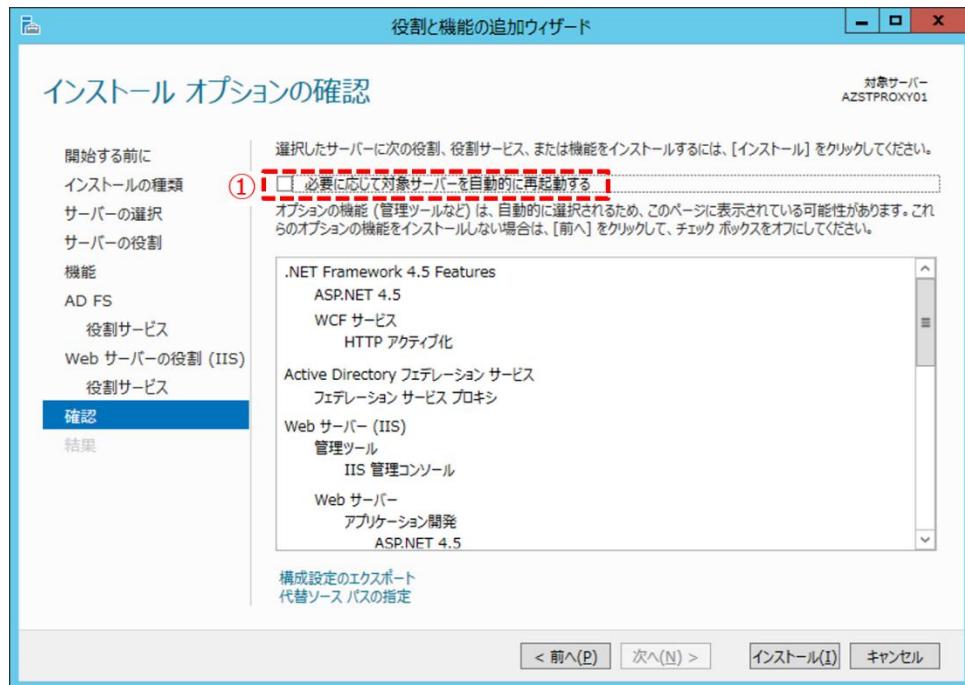


【表：Web サーバー デフォルト コンポーネント】

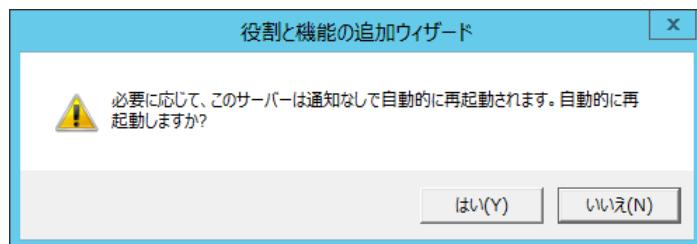
Web サーバー	HTTP 共通機能	HTTP エラー ディレクトリの参照 既存のドキュメント 静的なコンテンツ HTTP リダイレクト
	セキュリティ	要求フィルター Windows 認証 クライアント証明書マッピング認証
	パフォーマンス	静的なコンテンツの圧縮
	状態と診断	HTTP ログ
	アプリケーション開発	.NET 拡張機能 4.5 ASP.NET 4.5 ISAPI フィルター ISAPI 拡張
管理ツール	IIS 管理コンソール	

企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

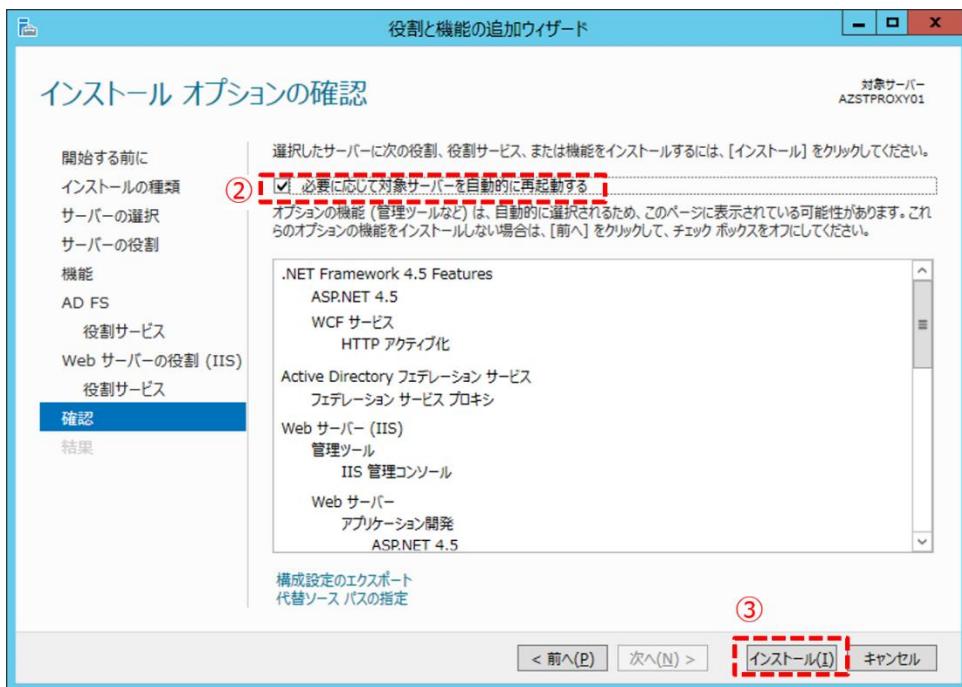
10. [インストール オプションの確認] ページにて [必要に応じて対象サーバーを自動的に再起動する] チェックボックスにチェックを付けます。



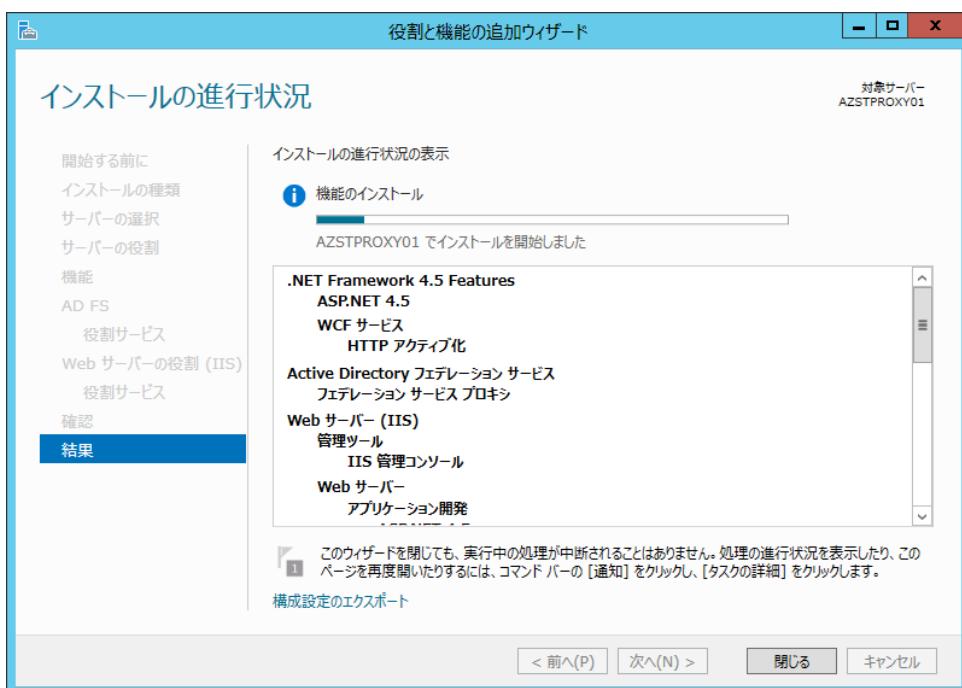
以下のメッセージ ボックスが開くので、[はい] ボタンをクリックして閉じます。



企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携
[インストール オプションの確認] ページに戻り、[必要に応じて対象サーバーを自動的に再起動する] チェックボックスにチェックが付いていることを確認して [インストール] ボタンをクリックします。

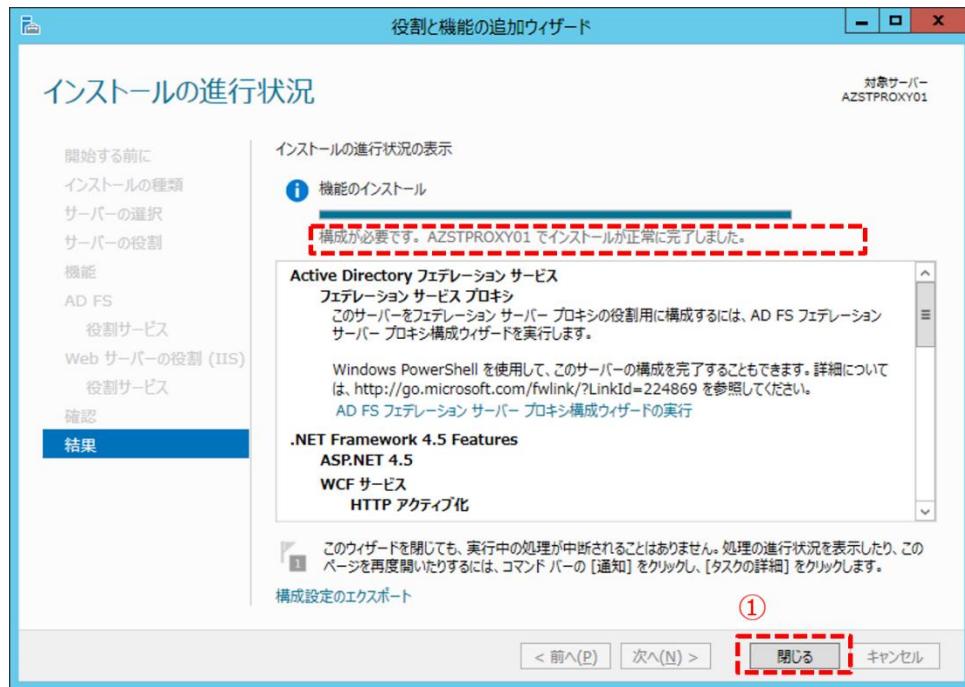


11. インストールが完了するまで待ちます。



企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

12. [構成が必要です。 AZSTPROXY01 でインストールが正常に完了しました。] とメッセージが表示されたら、[閉じる] ボタンをクリックして閉じます。



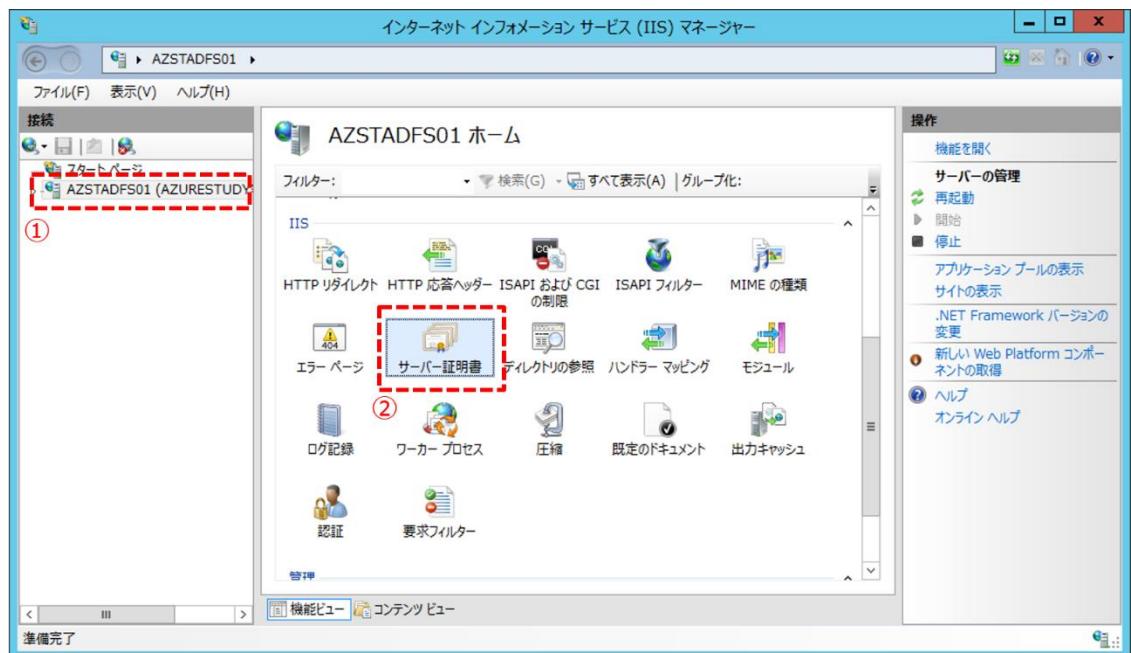
Note : 2 台目以降の AD FS Proxy サーバーでの作業

2 台目以降の AD FS PROXY サーバー ([AZSTPROXY02]) についてもこの項の作業を実施します。

12.2 サーバー証明書をインポートと設定

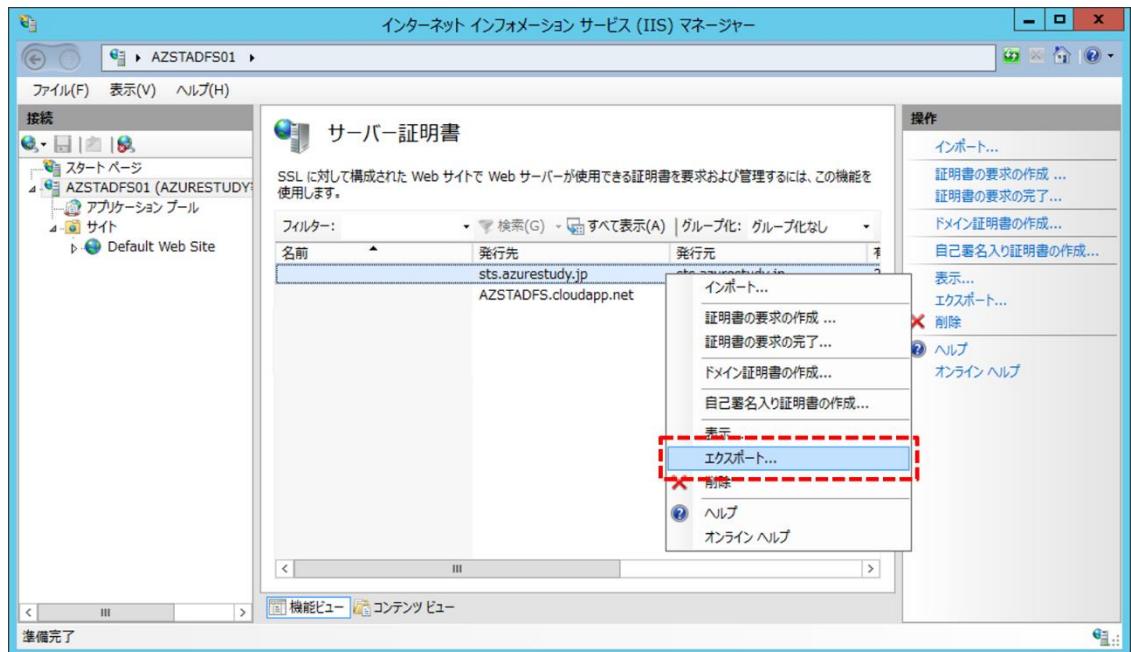
◆ AD FS サーバーから SSL 証明書をエクスポート

- ドメイン管理者アカウントで AD FS サーバー プライマリ [AZSTADFS01] にサインインし、[インターネット インフォメーション サービス (IIS) マネージャー] を開きます。
- 左ペインにて IIS をインストールしたサーバーが表示されるので、そのサーバー名 ([AZSTADFS01 (AZURESTUDY\\$administrator)]) を選択します。
- 中央ペインにて [サーバー証明書] をダブルクリックします。

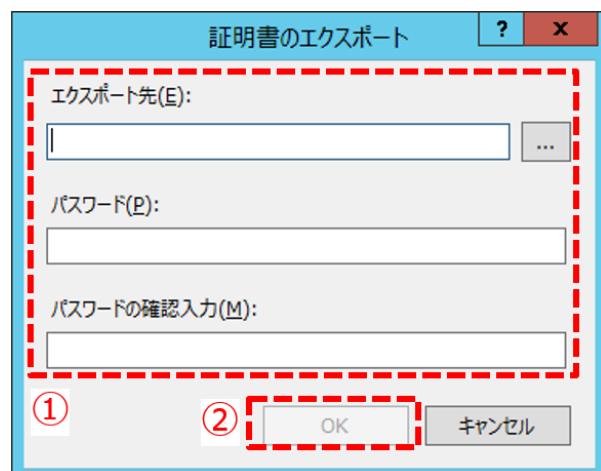


企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

4. 中央ペインにて「11.3 サーバー証明書をインポートと設定」でインポートした SSL 証明書を右クリックし、[エクスポート] をクリックします。



5. [証明書のエクスポート] 画面にて、以下の表のように入力して [OK] ボタンをクリックします。

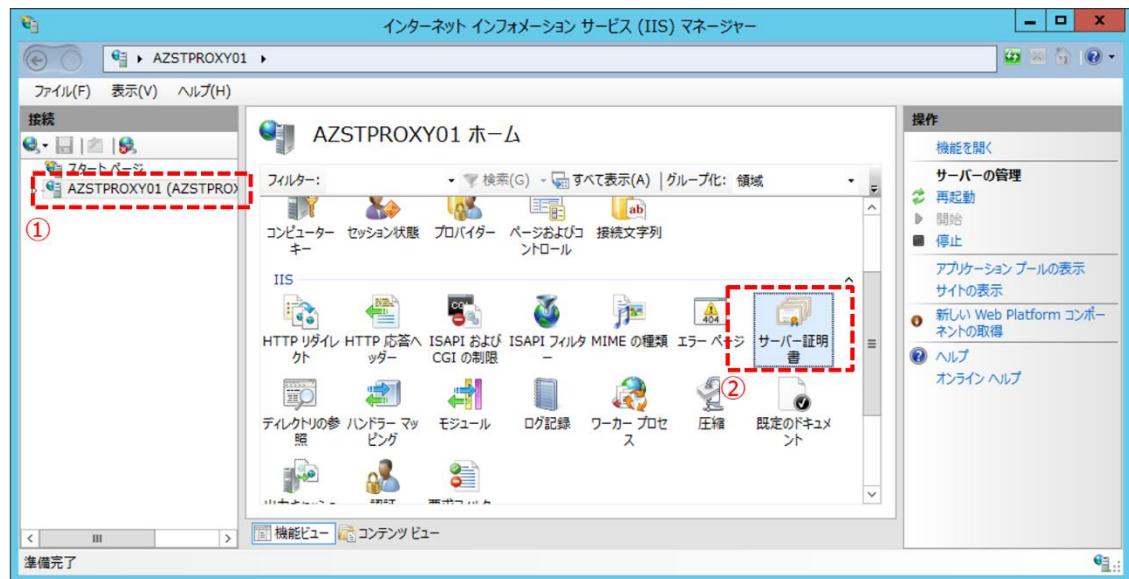


項目	設定値
エクスポート先	pfx ファイルの保存先 (任意のファイルパス) を指定
パスワード	任意のパスワードを入力
パスワードの確認	[パスワード] と同じ値を入力

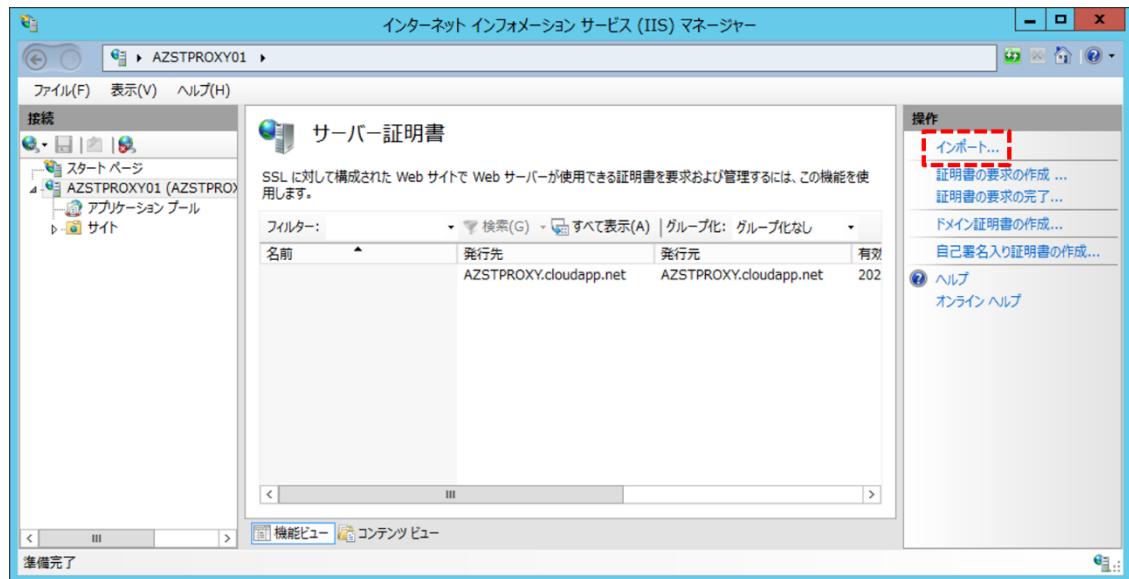
6. 手順 5 でエクスポートされた証明書を ADFS Proxy サーバー ([AZSTPROXY01]、および [AZSTPROXY02]) にコピーします。

▼ SSL 証明書のインポート

7. ローカル管理者で AD FS Proxy サーバー [AZSTPROXY01] にサインインし、[インターネット インフォメーション サービス (IIS) マネージャー] を開きます。
8. 左ペインにて IIS をインストールしたサーバーが表示されるので、そのサーバー名 ([AZSTPROXY01 (AZSTPROXY01\\$studyadmin)]) を選択します。
9. 中央ペインにて [サーバー証明書] をダブルクリックします。

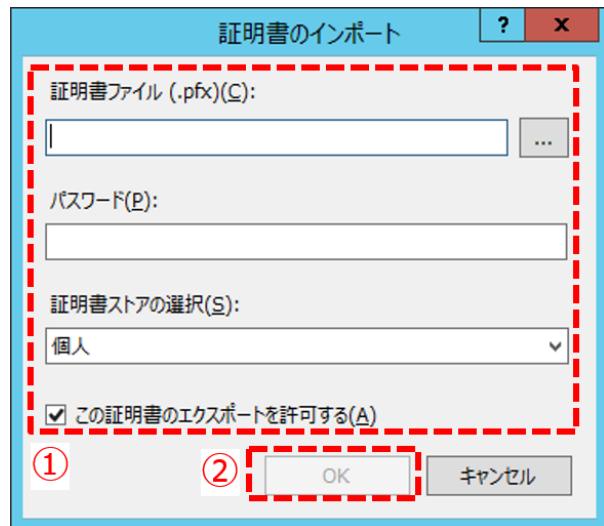


10. 右ペインにて [インポート] をクリックします。



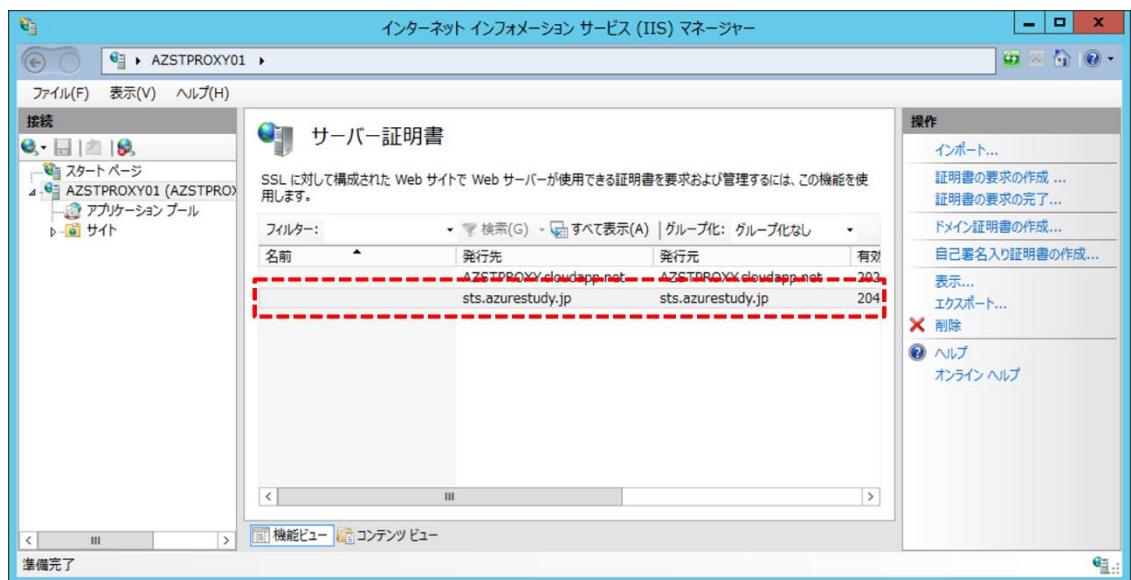
企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

11. [証明書のインポート] 画面が表示されます。以下の表のように入力して [OK] ボタンをクリックします。



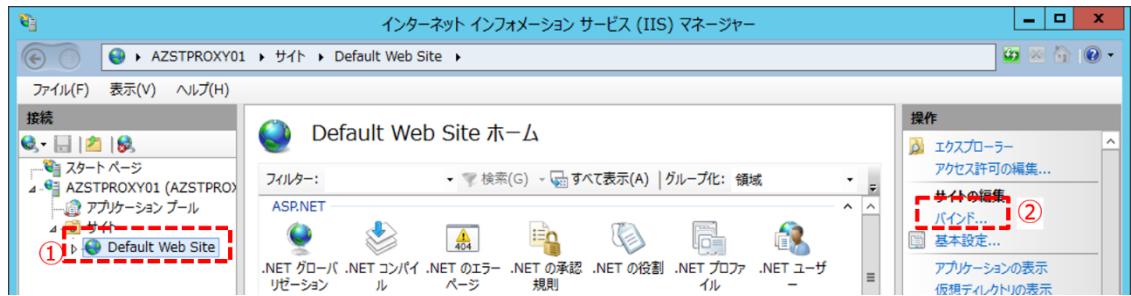
項目	設定値
証明書ファイル	手順 6 で AD FS サーバーよりコピーした SSL 証明書 (*.pfx) ファイルパスを指定
パスワード	手順 5 で入力した「パスワード」を入力
証明書ストアの選択	「個人」を選択
この証明書のエクスポートを許可する	デフォルト (チェック ON) のままで可

12. [サーバー証明書] にインポートした証明書が表示されていることを確認します。



▼ SSL 証明書の設定

13. [インターネット インフォメーション サービス (IIS) マネージャー] を開き、左ペインにて IIS をインストールしたサーバーが表示されるので、そのサーバー名([AZSTPROXY01 (AZSTPROXY01\\$studyadmin)])を展開し、[サイト] > [Default Web Site] を選択します。そして、右ペインにて [操作] の [バインド] をクリックします。

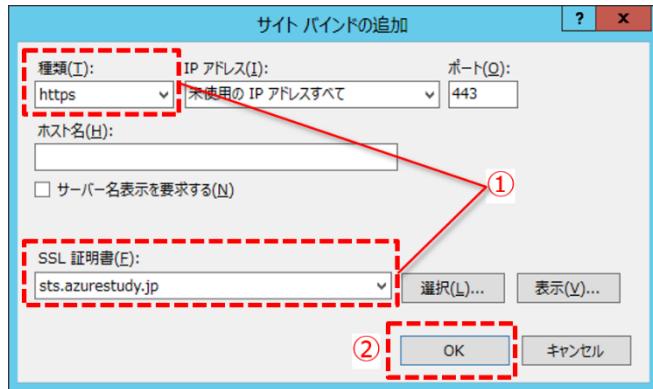


14. [サイト バインド] 画面にて、[追加] ボタンをクリックします。



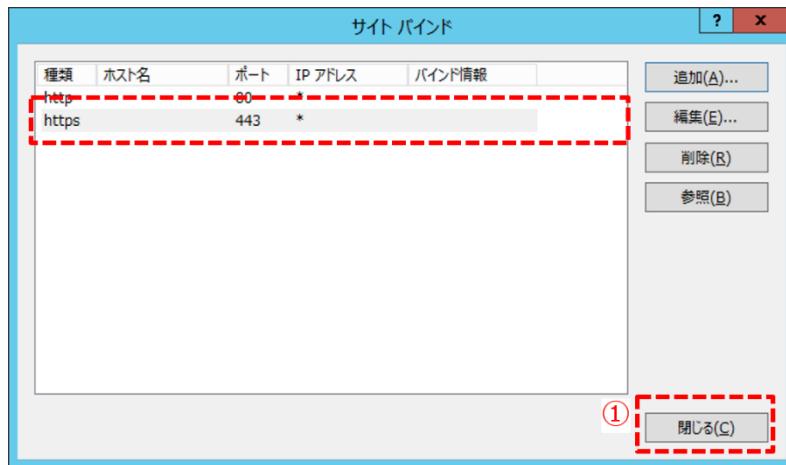
企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

15. [サイト バインドの追加] 画面にて、以下の表のとおり入力して [OK] ボタンをクリックします。



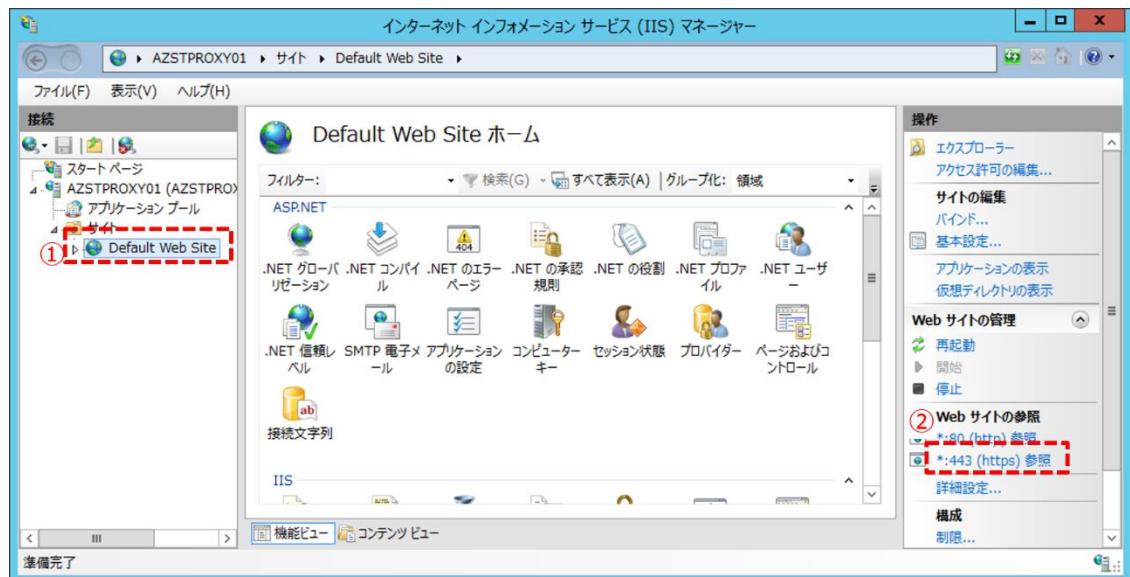
項目	設定値
種類	「https」を選択 ※ 「IP アドレス」、「ポート」は自動的に選択されます。
SSL 証明書	手順 7 ~ 12 でインポートした SSL 証明書を選択

16. [サイト バインド] 画面に戻り、一覧に「https」が追加されていることを確認します。 確認後、[閉じる] ボタンをクリックして画面を閉じます。

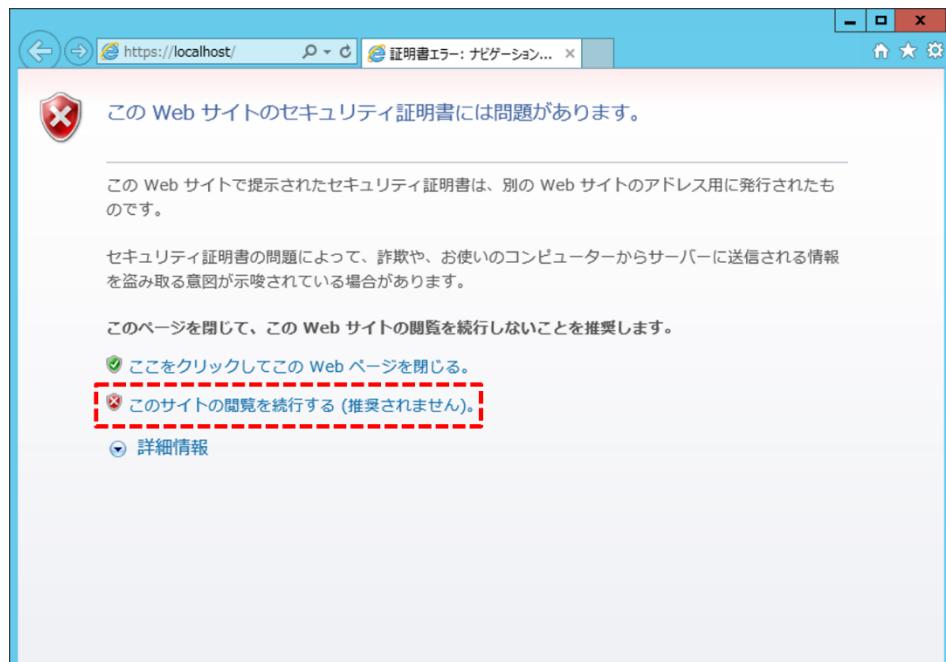


企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

17. [インターネット インフォメーション サービス (IIS) マネージャー] を開き、左ペインにて IIS をインストールしたサーバーが表示されるので、そのサーバー名([AZSTPROXY01 (AZSTPROXY01\\$studyadmin)])を展開し、[サイト] > [Default Web Site] を選択します。そして、右ペインにて [Web サイトの管理] にある [*:443 (https) 参照] をクリックします。



18. ブラウザーが開きます。Web サイトに “証明書エラー” が表示されたら、[このサイトの閲覧を続行する] をクリックします。



企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携
以下のページが表示されることを確認します。



Note : 2 台目以降の AD FS Proxy サーバーでの作業

2 台目以降の AD FS Proxy サーバー ([AZSTPROXY02]) についてもこの項の作業を実施します。

12.3 エンドポイント HTTPS を作成

AD FS Proxy サーバーの冗長化は、エンドポイントの負荷分散セットを作成することによって実現することができます。

◆ 1 台目の操作

1. Azure 管理ポータルにサインインします。
2. 画面左側のメニューから [仮想マシン] をクリックします。



名前	種類	状態	サブスクリプション	場所
azurestudy	ストレージアカウント	オンライン		tokyo-ag (日本 (東))
portalvhdsn3bqyvqyhk4kp	ストレージアカウント	オンライン	自習書(シグマコンサルテ)	日本 (東)
ss7020	ストレージアカウント	オンライン	自習書(シグマコンサルテ)	tokyo-ag (日本 (東))
AZSTADD01	仮想マシン	実行中	自習書(シグマコンサルテ)	tokyo-ag (日本 (東))
AZSTADD02	仮想マシン	実行中	自習書(シグマコンサルテ)	tokyo-ag (日本 (東))
AZSTADFS01	仮想マシン	実行中	自習書(シグマコンサルテ)	tokyo-ag (日本 (東))
AZSTADFS02	仮想マシン	実行中	自習書(シグマコンサルテ)	tokyo-ag (日本 (東))
AZSTDIRSYNC01	仮想マシン	実行中	自習書(シグマコンサルテ)	tokyo-ag (日本 (東))
AZSTFS01	仮想マシン	実行中	自習書(シグマコンサルテ)	tokyo-ag (日本 (東))
AZSTPROXY01	仮想マシン	実行中	自習書(シグマコンサルテ)	tokyo-ag (日本 (東))
AZSTPROXY02	仮想マシン	実行中	自習書(シグマコンサルテ)	tokyo-ag (日本 (東))
p2testserver	仮想マシン	停止済み (...)	自習書(シグマコンサルテ)	Site1 (日本 (東))

企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

3. AD FS Proxy サーバー [AZSTPROXY01] をクリックします。

名前	状態	サブスクリプション	場所	DNS 名
AZSTADDS01	実行中	自習書(シグマコンサルテ...)	tokyo-ag (日本 (東))	azstadds.cloudapp.net
AZSTADDS02	実行中	自習書(シグマコンサルテ...)	tokyo-ag (日本 (東))	azstadds.cloudapp.net
AZSTADFS01	実行中	自習書(シグマコンサルテ...)	tokyo-ag (日本 (東))	azstadfs.cloudapp.net
AZSTADFS02	実行中	自習書(シグマコンサルテ...)	tokyo-ag (日本 (東))	azstadfs.cloudapp.net
AZSTDIRSYNC01	実行中	自習書(シグマコンサルテ...)	tokyo-ag (日本 (東))	azstdirsync.cloudapp.net
AZSTPROXY01	実行中	自習書(シグマコンサルテ...)	tokyo-ag (日本 (東))	azstproxy.cloudapp.net
AZSTPROXY02	実行中	自習書(シグマコンサルテ...)	tokyo-ag (日本 (東))	azstproxy.cloudapp.net
p2testserver	停止済み (割り当て...)	自習書(シグマコンサルテ...)	Site1 (日本 (東))	p2testserver.cloudapp.net

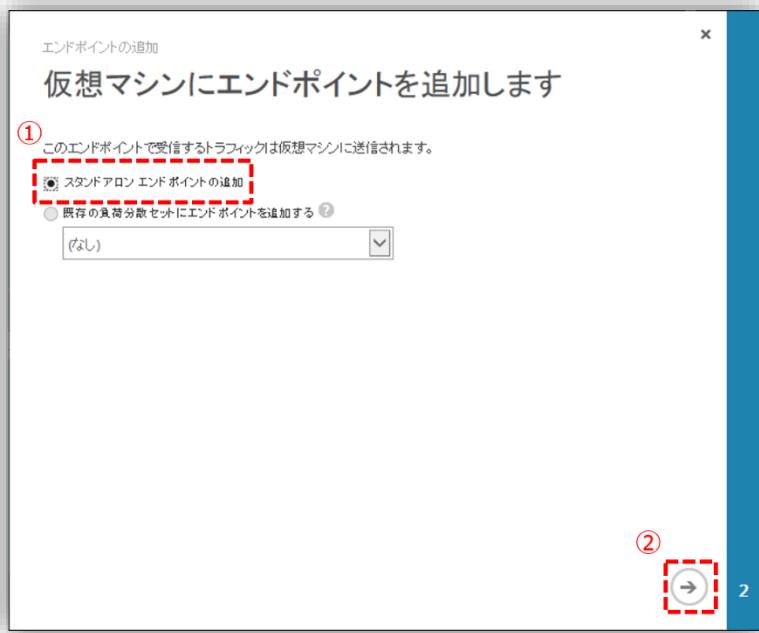
4. [エンドポイント] タブを開き、画面下部の [追加] をクリックします。

名前	プロトコル	パブリック ポート	プライベート ポート	負荷分散セット名
PowerShell	TCP	5986	5986	-
Remote Desktop	TCP	57937	3389	-

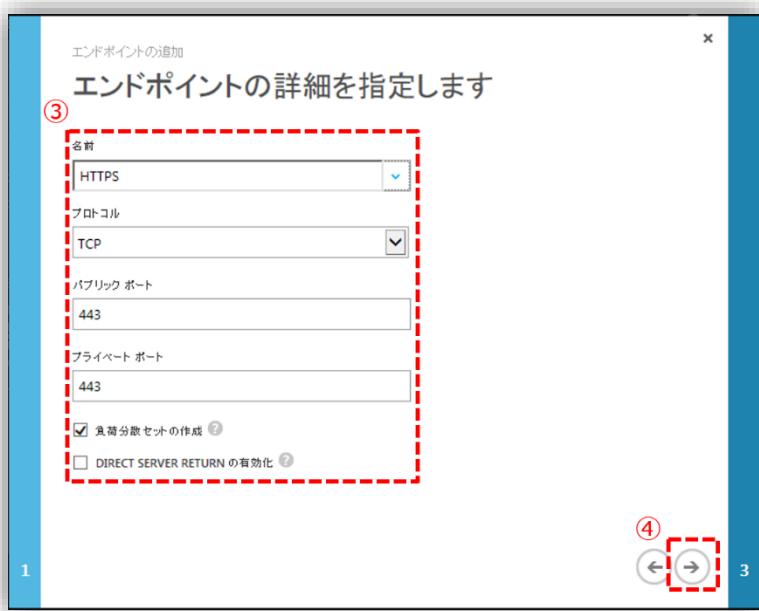
企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

5. [エンドポイントの追加] ウィザードが表示されます。以下、ウィザードに従って操作していきます。

[仮想マシンにエンドポイントを追加します] ページにて [スタンドアロン エンドポイントの追加] を選択して右下の [→] をクリックします。



[エンドポイントの詳細を指定します] ページにて以下の表のとおりに入力して右下の [→] をクリックします。



【表：[エンドポイントの詳細を指定します] ページの設定値】

項目	設定値
名前	「HTTPS」を選択
プロトコル	「TCP」を選択 (*1)
パブリック ポート	「443」を入力 (*1)
プライベート ポート	「443」を入力 (*1)
負荷分散セットの作成	チェック ON
DIRECT SERVER RETURN の有効化	チェック OFF

- ・ (*1) : [名前] 項目の設定値を選択することで自動的に設定されます。

[負荷分散セットの構成] ページにて以下の表のとおりに入力して右下の [チェック] をクリックします。



【表：[負荷分散セットの構成] ページの設定値】

項目	設定値
負荷分散セット名	「AZSTPROXY-LB (任意の名前)」を入力
プローブ プロトコル	「TCP」を選択 (*2)
プローブ ポート	「443」を入力 (*2)
プローブの間隔	「15 (秒)」を入力 (*3)
プローブの数	「2 (回)」を入力 (*3)

- ・ (*2) : 自動的に設定値が設定されます。
- ・ (*3) : 自動的に設定値が設定されます。 必要に応じて任意の値を設定することも可。

Microsoft Azure 自習書シリーズ No.6
企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

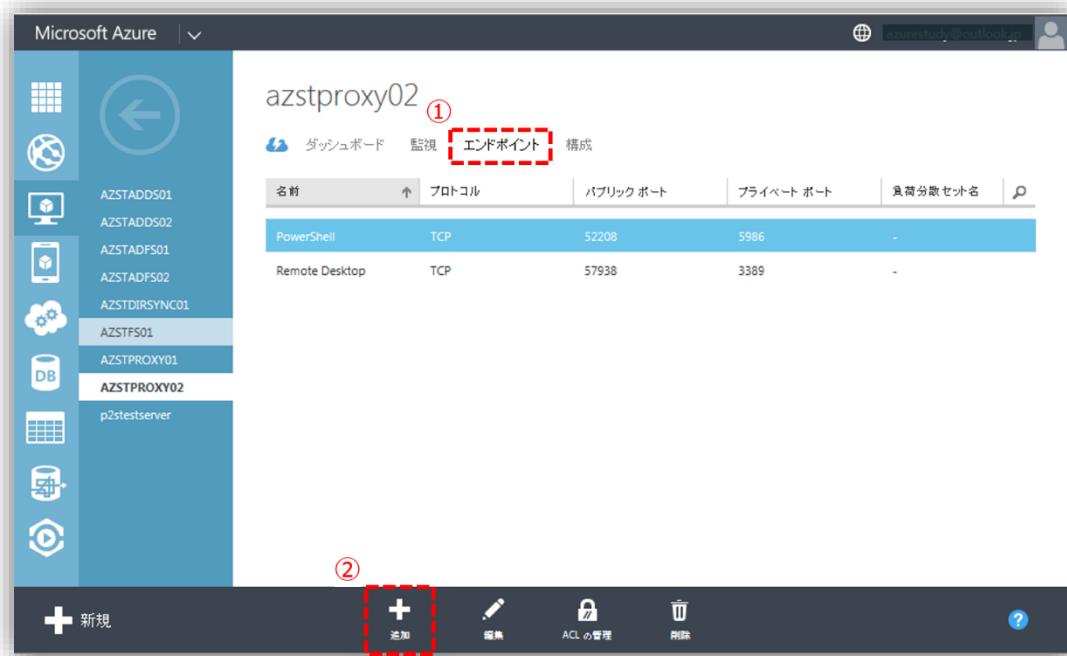
しばらくすると、[HTTPS] エンドポイントが追加されます。

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with icons for various services like Storage, Network, and Compute. A list of resources is on the left side of the main content area. In the center, a table lists endpoints for a VM named 'azstproxy01'. The table has columns for Name, Protocol, Public Port, Private Port, and Load Balancer. A new row for 'HTTPS' has just been added, showing Public Port 443 and Private Port 443, associated with the load balancer 'AZSTPRXY-LB'. At the bottom of the table, a success message says '✓ 仮想マシン AZSTPROXY01 にエンドポイント HTTPS が正常に追加されました。' (Virtual machine AZSTPROXY01 successfully added endpoint HTTPS). Below the table are buttons for 'New' (+), 'Edit' (pencil), 'ACL Management' (key icon), and 'Delete' (trash bin). There are also 'OK' and 'Close' buttons at the bottom right.

名前	プロトコル	パブリック ポート	プライベート ポート	負荷分散 セット名
HTTPS	TCP	443	443	AZSTPRXY-LB
PowerShell	TCP	5986	5986	-
Remote Desktop	TCP	57937	3389	-

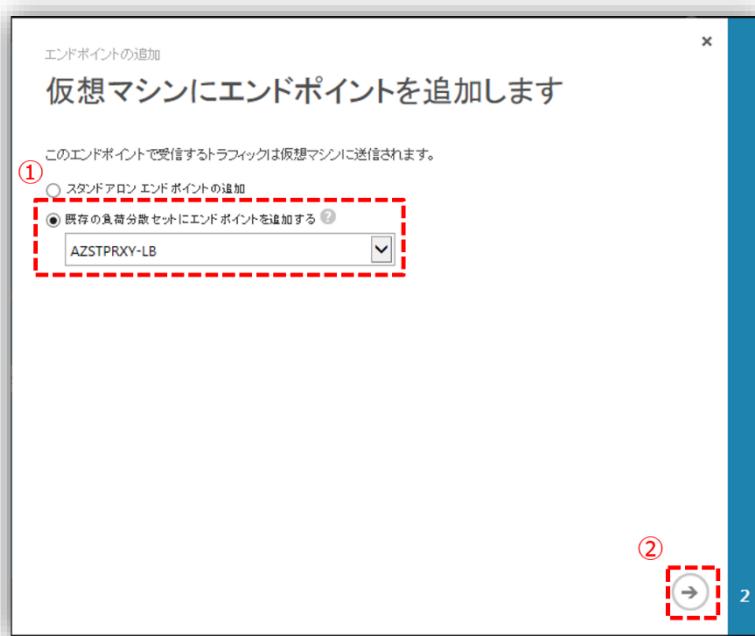
➔ 2 台目以降の操作

6. 手順 5 までで作成したエンドポイントの負荷分散セットに 2 台目以降の AD FS Proxy サーバーを紐付けます。AD FS Proxy サーバー [AZSTPROXY02] の [エンドポイント] タブを開き、画面下部の [追加] をクリックします。



7. [エンドポイントの追加] ウィザードが表示されます。以下、ウィザードに従って操作していきます。

企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携
 [仮想マシンにエンドポイントを追加します] ページにて [既存の負荷分散セットにエンドポイントを追加する] を選択し、その下にあるプルダウンから「AZSTPROXY-LB (手順 5 の [負荷分散セットの構成] ページにて [負荷分散セット名] に入力した名前)」を選択して右下の [→] をクリックします。



[エンドポイントの詳細を指定します] ページにて以下の表のとおりに入力して右下の [チェック] をクリックします。



【表：[エンドポイントの詳細を指定します] ページの設定値】

項目	設定値
名前	「HTTPS」を入力
プロトコル	使用不可（「TCP」）(*1)
パブリック ポート	使用不可（「443」）(*1)
プライベート ポート	使用不可（「443」）(*1)
負荷分散セットの再作成	チェック OFF
DIRECT SERVER RETURN の有効化	使用不可（チェック OFF）

- ・ (*1) : 自動的に設定されます。

しばらくすると、[HTTPS] エンドポイントが追加されます。

名前	プロトコル	パブリック ポート	プライベート ポート	負荷分散セット名
HTTPS	TCP	443	443	AZSTPRXY-LB
PowerShell	TCP	52208	5986	-
Remote Desktop	TCP	57938	3389	-

✓ 仮想マシン AZSTPROXY02 にエンドポイント HTTPS が正常に追加されました。 OK ✓

12.4 社外 DNS の設定

Note : ドメインとアドレスのマッピング

一般的にドメインとアドレスをマップするには、2通りの方法があります。

- ① A レコードを特定の IP アドレスにマップする
- ② CNAME レコードを使用して、サブドメインを別の DNS エントリーにマップする

Azure は、アプリケーションに割り当てられた IP アドレスを変更する権利を留保しているため、①の方法は Azure アプリケーションには適しません。

Azure では、②の方法が適しています。ドメイン登録業者が提供するツールを使用して、アプリケーション用に使用するサブドメインを、Azure から提供された名前に対応付ける必要があります。この自習書で取り扱っているドメイン名を題材として説明すると、Azure でのドメイン名 (AD FS Proxy サーバーのクラウド サービス DNS 名) が azstproxy.cloudapp.net で、ドメイン名 azurestudy.jp を登録している場合は、sts サブドメインを azstproxy.cloudapp.net にマップする CNAME エントリーを作成することで、sts.azurestudy.jp (=フェデレーション サービス名) という名前でアクセスできるようになります。

1. ドメイン登録情報を管理している DNS にフェデレーション サービス名「sts.azurestudy.jp」を「azstproxy.cloudapp.net」にマップする CNAME レコードを追加してください。
2. 登録情報の変更が反映されるまで待ちます。
3. クライアント PC で、コマンド プロンプトを開き、[nslookup] コマンドで「sts.azurestudy.jp」と入力して、設定した CNAME レコードが正常に登録できていることを確認します。

Note : インターネット経由で AD FS サーバーにアクセスする際の名前解決

インターネット経由で AD FS サーバーにアクセスする際、AD FS Proxy サーバーにて名前解決を行う必要があります。

オンプレミス環境の場合は Hosts ファイルなどで「フェデレーション サービス名」と「IP アドレス」を紐付けます。

仮想ネットワーク上の仮想マシンの場合は、仮想ネットワークで設定した DNS サーバーを参照するようになっているので、これらの DNS サーバーにて「フェデレーション サービス名」と「IP アドレス」を紐付けます。（この自習書では、「11.3 社内 DNS の設定」にて実施済みです。）



[ipconfig /all] コマンドで確認

```
Windows PowerShell 管理者: Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.

PS C:\Users\studyadmin> ipconfig /all

Windows IP 構成

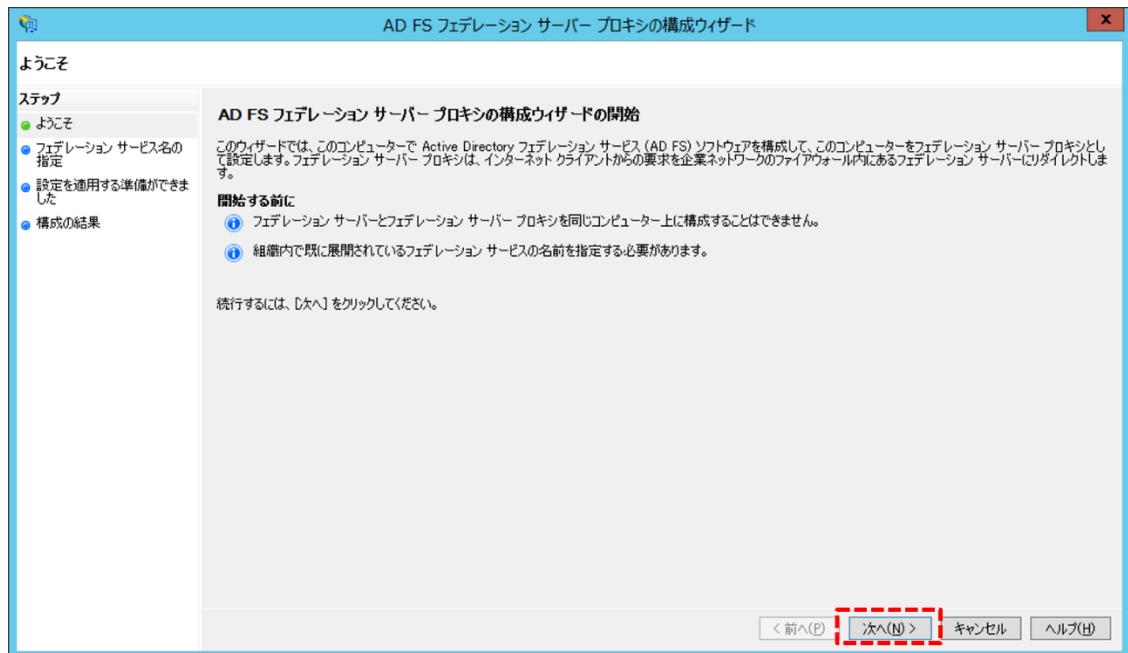
ホスト名 . . . . . : AZSTPROXY01
プライマリ DNS サフィックス . . . . . :
ノード タイプ . . . . . : ピア ツー ピア
IP ルーティング有効 . . . . . : いいえ
WINS プロキシ有効 . . . . . : いいえ
DNS サフィックス検索一覧 . . . . . : AZSTPROXY.13.internal.cloudapp.net

イーサネット アダプター イーサネット :

接続固有の DNS サフィックス . . . . . : AZSTPROXY.13.internal.cloudapp.net
説明 . . . . . : Microsoft Hyper-V Network Adapter
物理アドレス . . . . . : 00-15-5D-90-1A-E5
DHCP 有効 . . . . . : (はい)
自動構成有効 . . . . . : (はい)
リンクローカル IPv6 アドレス . . . . . : fe80::7cea:f038:f61d:ce09%12(優先)
IPv4 アドレス . . . . . : 10.1.1.9(優先)
サブネット マスク . . . . . : 255.255.255.0
リース取得 . . . . . : 2014年5月2日 20:10:22
リースの有効期限 . . . . . : 2150年6月21日 2:24:34
デフォルト ゲートウェイ . . . . . : 10.1.1.1
DHCP サーバー . . . . . : 168.63.129.16
DHCPv6 IAID . . . . . : 251663709
DHCPv6 クライアント ID . . . . . : 00-01-00-01-1A-E5-00-00-15-5D-00-1A-E5
DNS サーバー . . . . . : 10.1.1.4
10.1.1.5
192.168.118.160
NetBIOS over TCP/IP . . . . . : 有効
```

12.5 フェデレーション サーバー プロキシの設定

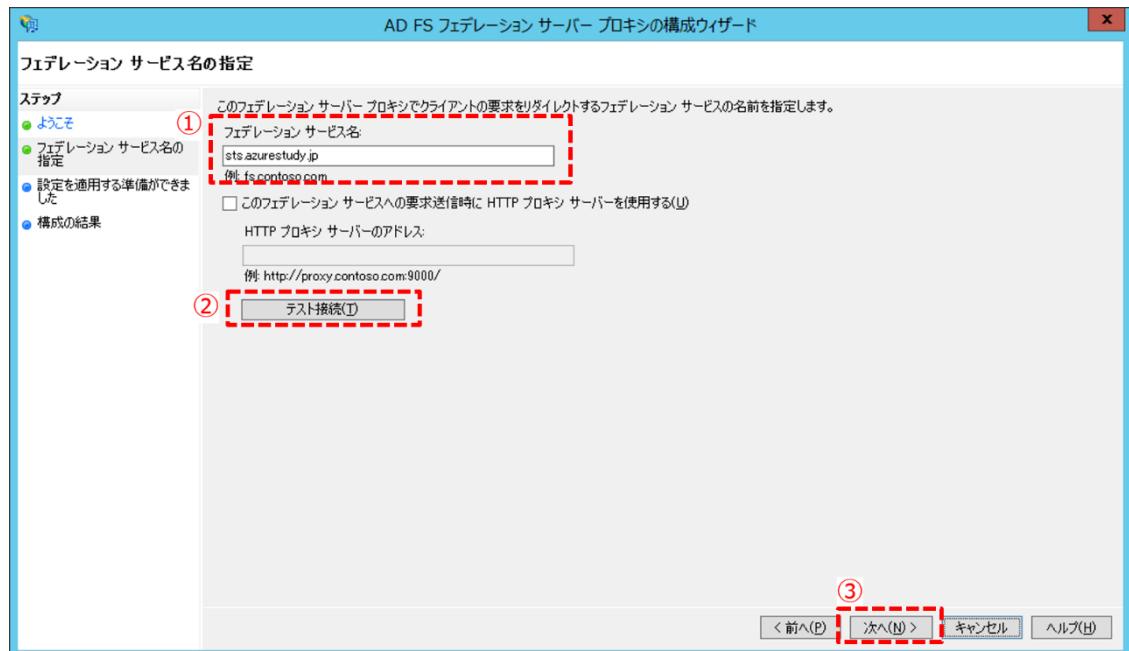
1. ローカル管理者で AD FS Proxy サーバー [AZSTPROXY01] にサインインし、[AD FS フェデレーション サーバー プロキシの構成ウィザード]を開きます。
2. [ようこそ] ページにて [次へ] ボタンをクリックします。



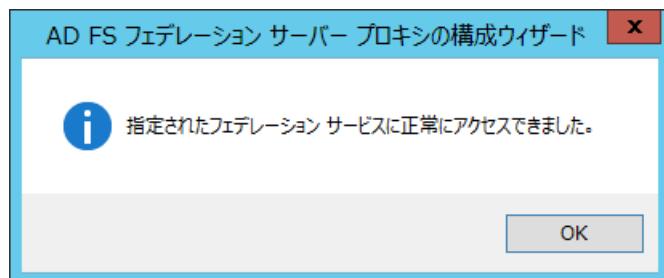
企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

3. [フェデレーション サービス名の指定] ページにて、[フェデレーション サービス名] に「sts.azurestudy.jp」を入力します。

※ 必要に応じて、[このフェデレーション サービスへの要求送信時に HTTP プロキシ サーバーを使用する] チェックボックスにチェックを付けて [HTTP プロキシ サーバーのアドレス] を指定してください。(この自習書では不要です。)



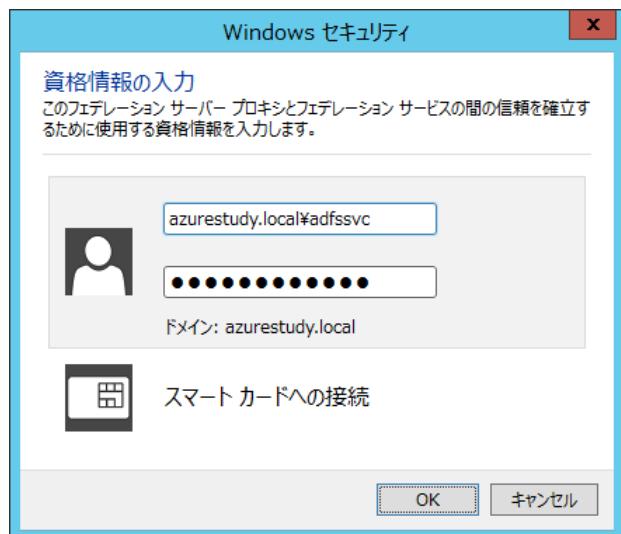
[フェデレーション サービス名] を入力したら、[テスト接続] をクリックします。 フェデレーション サービス名が正しい場合は、下図のメッセージ ボックスが開きます。



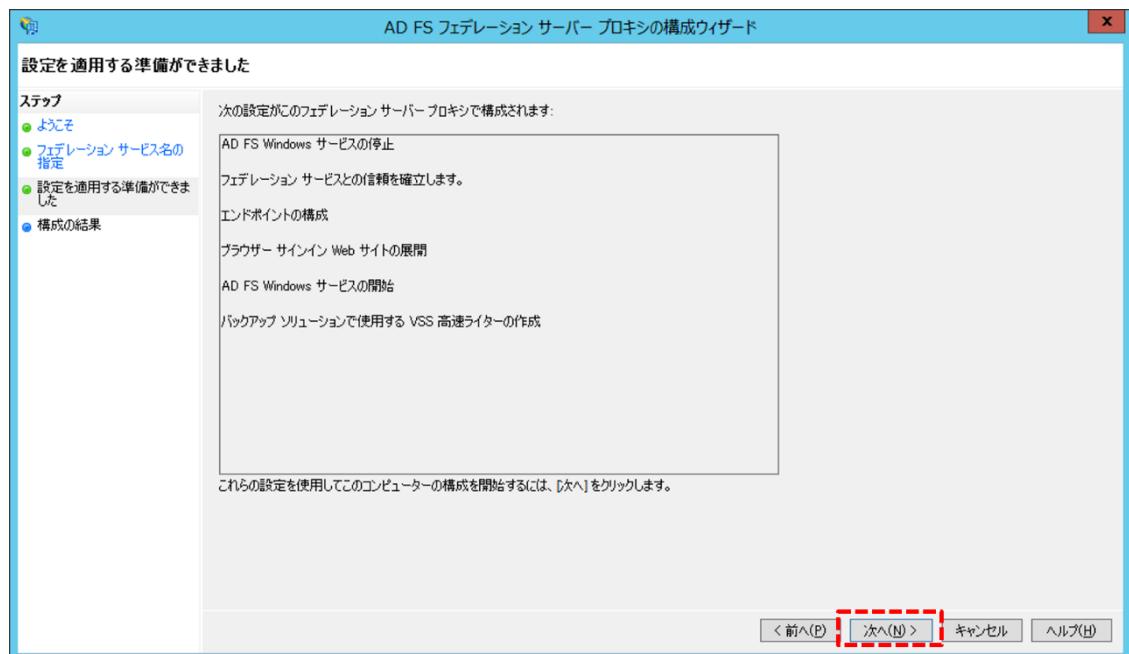
[次へ] ボタンをクリックします。

企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

4. [Windows セキュリティ] 画面が開きます。「11.4 AD フェデレーション 用 サービス アカウントの作成」で作成したアカウントのユーザー名とパスワードを入力します。



5. [設定を適用する準備ができました] ページにて [次へ] ボタンをクリックします。

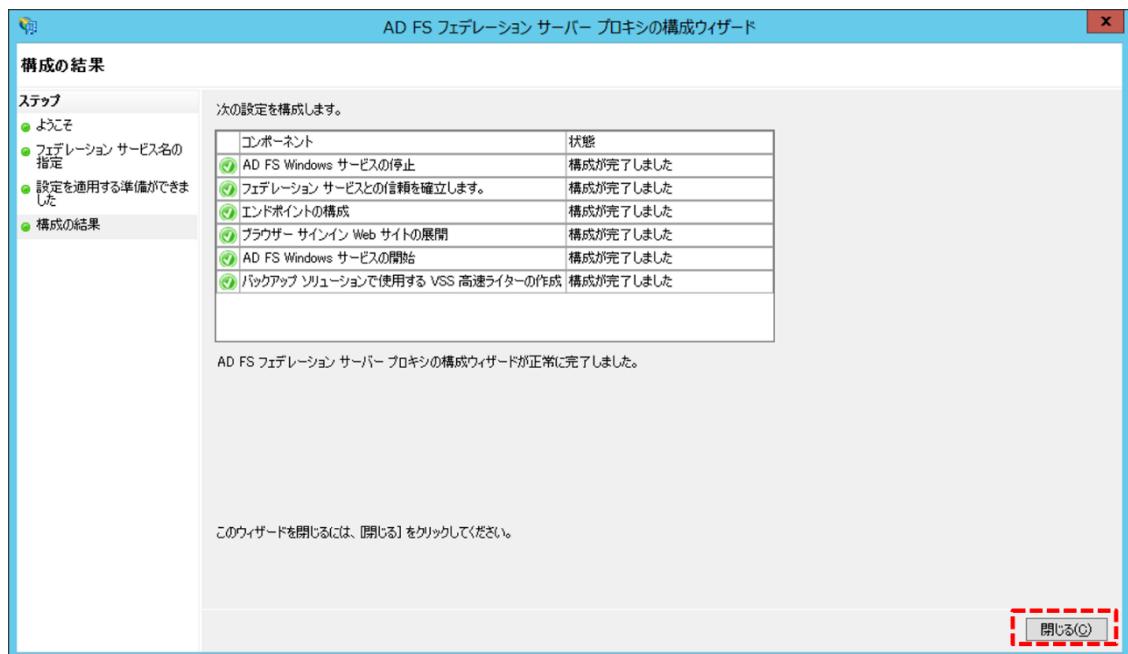


企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

6. AD FS フェデレーション サーバー プロキシの構成のセットアップが完了するまで待ちます。



7. AD FS フェデレーション サーバー プロキシの構成のセットアップが完了したら、[閉じる] ボタンをクリックして閉じます。

**Note : 2 台目以降の AD FS Proxy サーバーでの作業**

2 台目以降の AD FS PROXY サーバー ([AZSTPROXY02]) についてもこの項の作業を実施します。

12.6 AD FS Proxy サーバーの動作確認

AD FS Proxy サーバーのセットアップが完了したら、以下の内容を基にフェデレーション環境が正常に稼動しているか確認を行います。

➔ AD FS Proxy サーバーでの確認

1. ローカル管理者で AD FS Proxy サーバー ([AZSTPROXY01] および [AZSTPROXY02]) にサインインします。
2. [サービス] を開き、以下の表で挙げたサービスのプロパティを確認します。

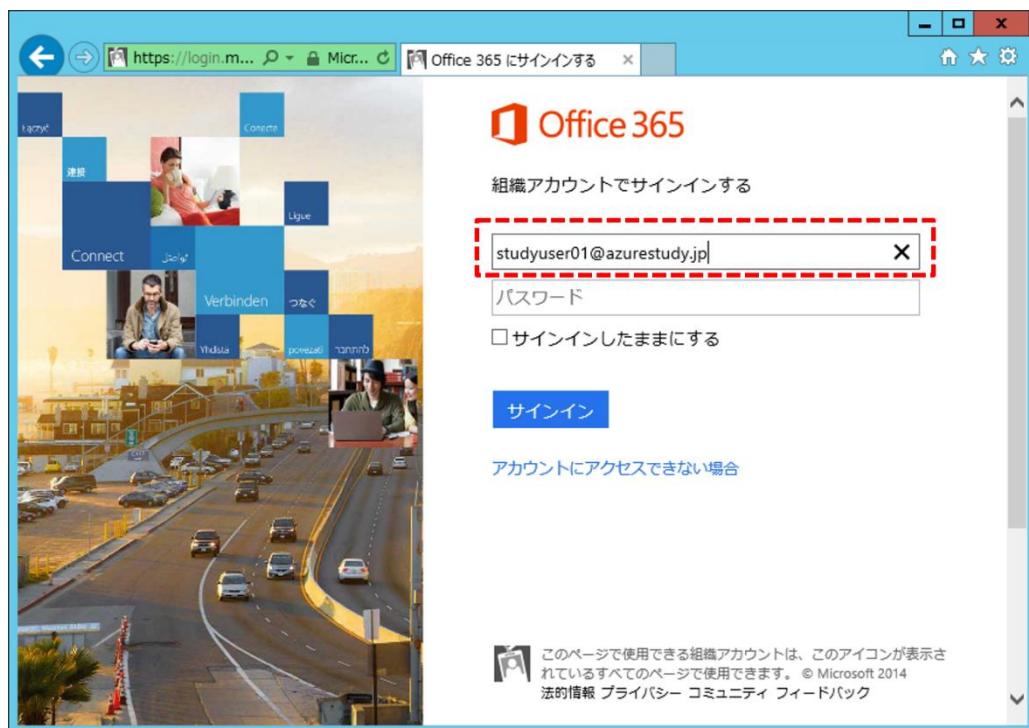
	スタートアップの種類	サービスの状態	アカウント
AD FS Windows Service	自動 (遅延実行)	実行中(開始)	「Network Service」

3. [イベント ビューアー] を開き、以下のイベント ログが出力されていることを確認します。

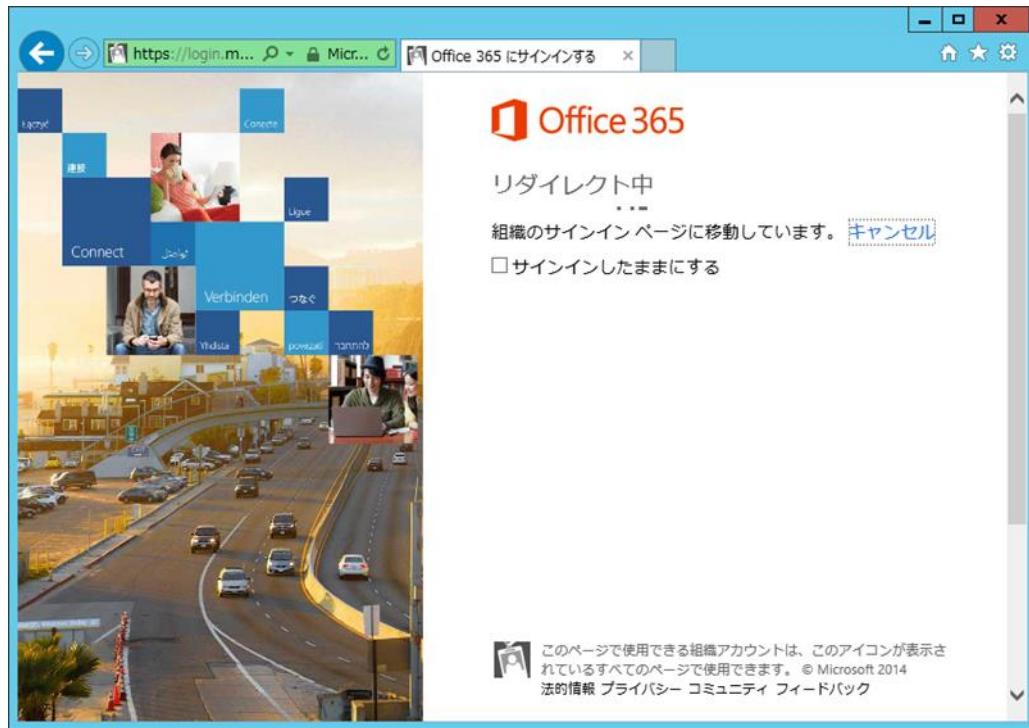
項目	内容
ログ保存場所	[アプリケーションとサービス ログ] > [AD FS] > [Admin]
ソース	AD FS
イベント ID	198
ログの内容	<p>フェデレーション サーバー プロキシは正常に開始しました。次のプロキシ リスナーが 追加されました:</p> <pre>http://+:80/adfs/services/trust/ https://+:443/adfs/services/trust/ https://+:443/FederationMetadata/2007-06/</pre>

➔ クライアント PC での確認

4. 「azurestudy.local」ドメイン外にあるクライアント PC にサインインします。
5. [Internet Explorer] を開きます。
6. アドレス欄に「<https://portal.office.com/Home> (Office 365 ポータル)」と入力してアクセスします。
7. 資格情報を求められるので、UPN [<user>@azurestudy.jp] を入力して、フォーカスを移動 ([TAB] キー押下) します。



8. 下図のように AD FS 用の認証処理が行われます。

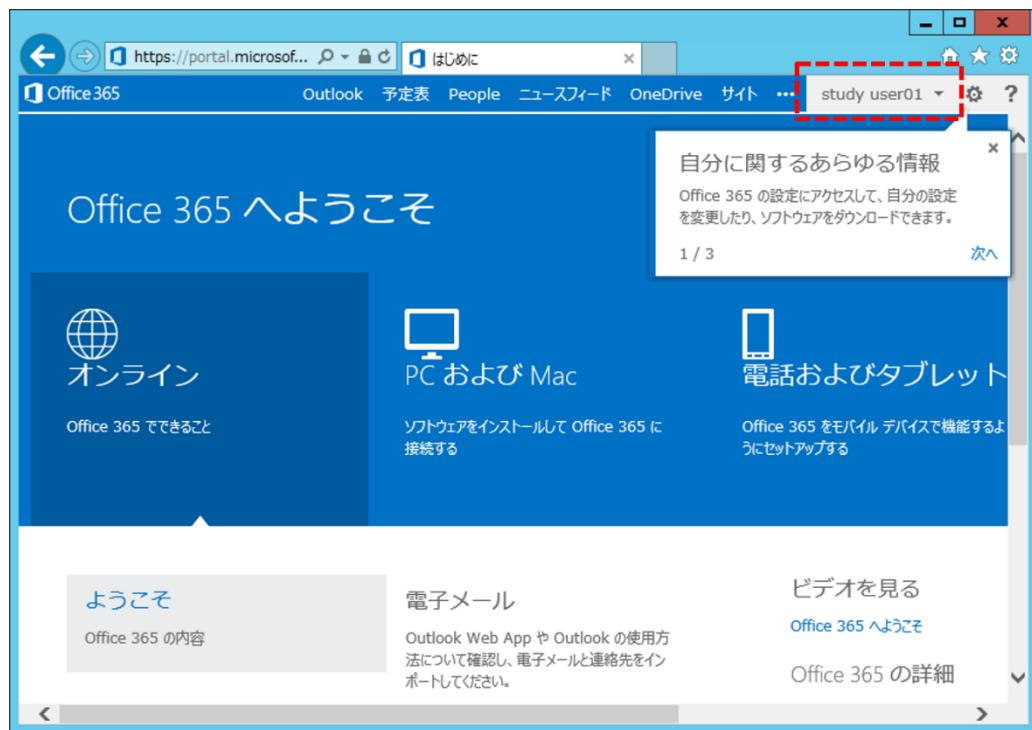


9. [サインイン] ページ (AD FS Proxy サーバー) では、AD の資格情報が求められますので、手順 7 のアカウントのユーザー名とパスワードを入力し、[サインイン] ボタンをクリックします。



企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

10. [Office 365 ポータル] ページが表示されたら、下図（右上）のように適切なユーザーでサイ
ンインしていることを確認します。



STEP 13. ファイアウォールの設定

この自習書では、AD FS 環境を利用するに当たって必要なネットワーク設計、および設定（主に、オンプレミス側）については省略しています。必要に応じて以下の設計を行うための参考資料を紹介します。

- Office 365 向けファイアウォール
- (必要に応じて) WAN アクセレーター
- (必要に応じて) インターネットの帯域幅

13.1 ファイアウォールの設定

以下の URL には、Office 365 利用時に使用する URL 、ポート、IP アドレスについて記載しております。

必要に応じてファイアウォールの設計を行ってください。

「 Office 365 URLs and IP address ranges (<http://technet.microsoft.com/en-us/library/hh373144.aspx>)」

※ 構築の際には、最新の情報をご確認ください。

以下の URL には Office 365 の必要なポートとプロトコルを記載しております。

「 Office 365 で使用されるポートとプロトコル (<http://technet.microsoft.com/ja-jp/library/hh852522.aspx>)」

※ 構築の際には、最新の情報をご確認ください。

STEP 14. マルチドメインの設定

この STEP では、Office 365 に複数のトップ レベル ドメインを追加し、それらのドメインに属するユーザーが AD FS サーバーで認証できるようにするための設定について説明します。

この STEP では、次のことを学習します。

- ✓ マルチドメインの設定

14.1 マルチドメインの設定

Note : 複数のトップ レベル ドメインのサポート

複数のトップ レベル ドメインのサポート - ディレクトリ統合サービス - Office 365 - 日本語 - Microsoft Office 365 Community

<http://community.office365.com/ja-jp/w/sso/1007.aspx>

以下、抜粋

単一のトップ レベル ドメインと複数のサブドメインを使用している場合、"SupportMultipleDomain" スイッチは必要ないことにご注意ください。たとえば、UPN サフィックスに使用されているドメインが @sales.contoso.com、@marketing.contoso.com、および @contoso.com で、トップ レベル ドメイン（この場合、contoso.com）が追加されてからフェデレーションが行われた場合、"SupportMultipleDomain" スイッチを使用する必要はありません。これは、これらのサブドメインが親の範囲内で効率的に管理されており、単一の AD FS サーバーを利用して既にこれを処理できているためです。

ただし、複数のトップ レベル ドメイン (@contoso.com および @fabrikam.com) を使用していて、これらのドメインにサブドメイン (@sales.contoso.com および @sales.fabrikam.com) も存在する場合、"SupportMultipleDomain" スイッチはサブドメインに対して機能しないため、これらのユーザーはログインできなくなります。マイクロソフトでは、この問題の解決に取り組んでおり、準備が整い次第、解決策を掲載する予定ですが、それまではこのソリューションをサポートすることができません。

「オンプレミス ユーザー アカウントの UPN を SSO が有効な異なるドメイン サフィックスに更新した後、Azure AD に変更が同期されない (<http://support.microsoft.com/kb/2669550>)」

「Office 365 で 2 つ目のフェデレーションドメインを構成しようとすると表示されるエラー：“AD FS 2.0 サーバーに指定するフェデレーションサービスの識別子は既に使用されています” (<http://support.microsoft.com/kb/2618887/ja>)」

この項では以下の例を用いて AD FS サーバーの設定方法について説明します。

現在のフェデレーション ドメイン	azurestudy.jp
新たに追加するフェデレーション ドメイン	contoso.jp

▼ Office 365 にドメインを追加

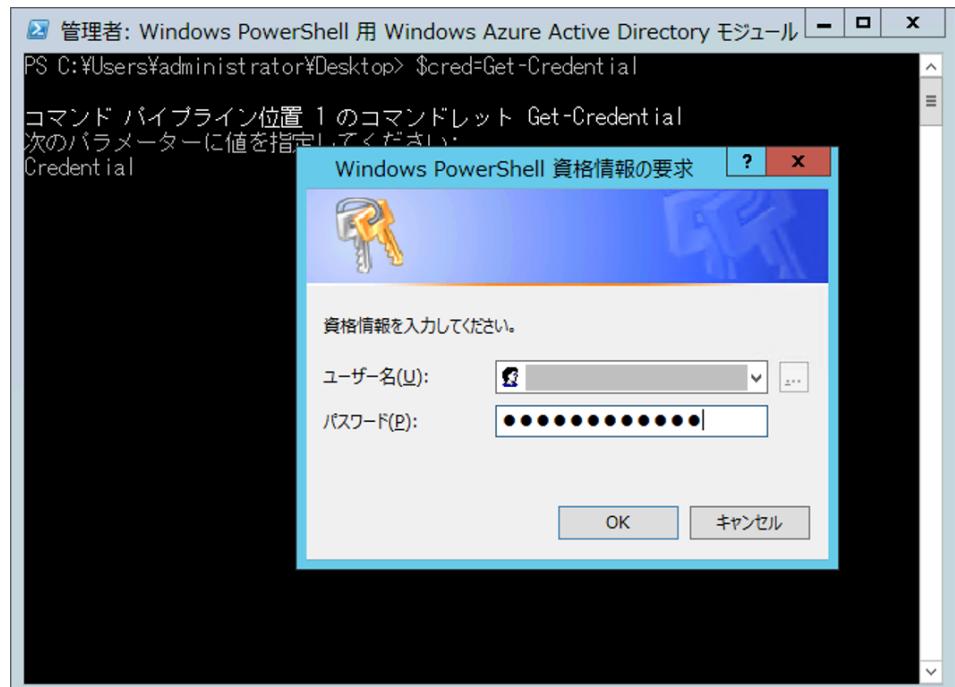
1. 「STEP 5. Office 365 ヘドメインの追加、およびドメインの確認」の手順に従って、新たなトップ レベル ドメインを追加してください。

▼ AD FS サーバーの設定

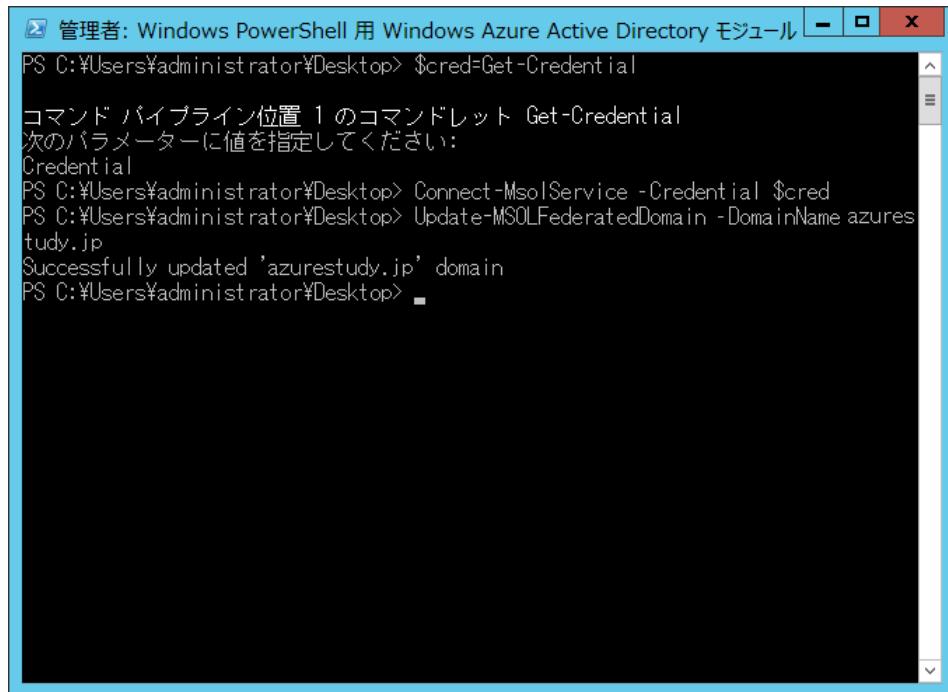
2. ドメイン管理者アカウントで AD FS サーバー プライマリ [AZSTADFS01] にサインインします。
3. [Windows PowerShell 用 モジュール] を「管理者として実行」で開きます。
4. 以下のコマンドを実行します。

```
$cred=Get-Credential (*1)
Connect-MsolService -Credential $cred
Update-MSOLFederatedDomain -DomainName azurestudy.jp
```

- ✓ (*1) : 資格情報を求められるので、Office 365 管理者アカウントのユーザー名、パスワードを入力します。



5. 結果、以下の画面のようになります。



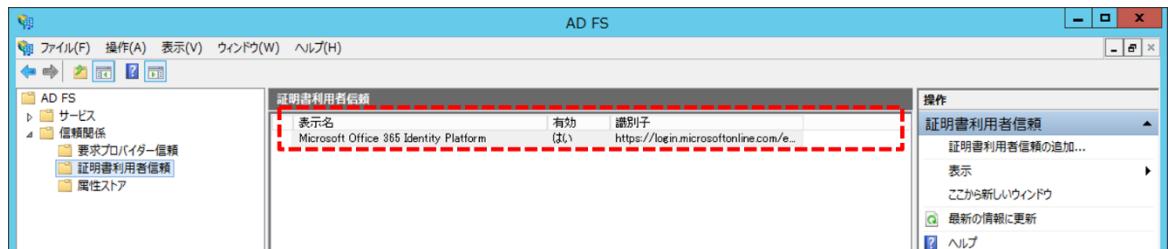
```

管理者: Windows PowerShell 用 Windows Azure Active Directory モジュール - ×
PS C:\$Users\$administrator\Desktop> $cred=Get-Credential
コマンド バイブルайн位置 1 のコマンドレット Get-Credential
次のパラメーターに値を指定してください:
Credential
PS C:\$Users\$administrator\Desktop> Connect-MsolService -Credential $cred
PS C:\$Users\$administrator\Desktop> Update-MSOLFederatedDomain -DomainName azurstudy.jp
Successfully updated 'azurstudy.jp' domain
PS C:\$Users\$administrator\Desktop>

```

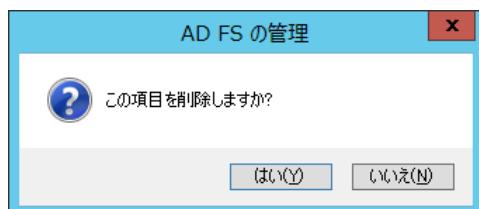
6. [PowerShell] 画面は開いたまま [AD FS の管理] を開きます。

7. 左ペインにて [AD FS] > [信頼関係] > [証明書利用者信頼] を展開し、[証明書利用者信頼] に登録されている「Microsoft Office 365 Identity Platform」を削除します。



Note : 注意事項

確認メッセージ ボックスが開くので、[はい] ボタンをクリックします。



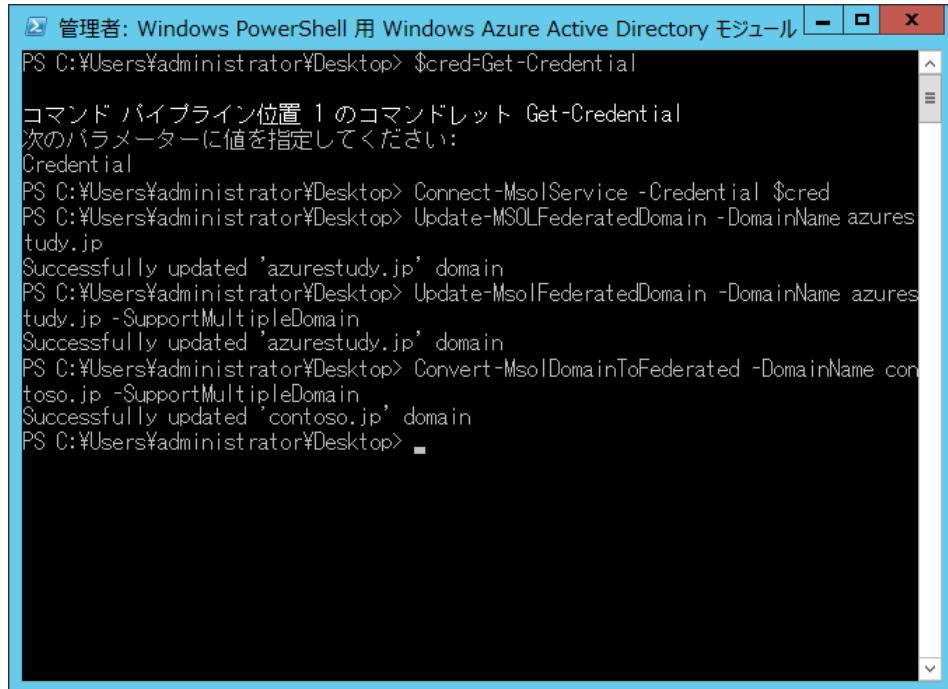
この手順を実行すると、手順 10 が完了するまで、ユーザーは Office 365 にログオンできなくなります。

企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

8. 再び [PowerShell] 画面に戻り、以下のコマンドを実行して 2 つ目のフェデレーション ドメインを追加、または変換します。

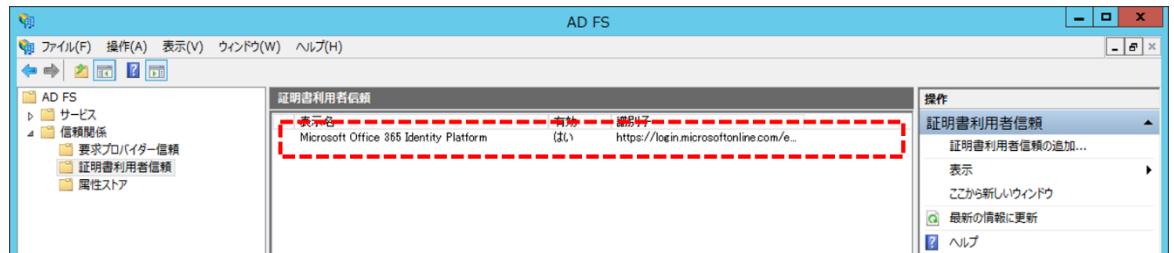
```
Update-MsolFederatedDomain -DomainName azurestudy.jp -SupportMultipleDomain
Convert-MsolDomainToFederated -DomainName contoso.jp -SupportMultipleDomain
```

9. 結果、以下の画面のようになります。



```
管理着: Windows PowerShell 用 Windows Azure Active Directory モジュール
PS C:\$Users\$administrator\Desktop> $cred=Get-Credential
コマンド バイブライン位置 1 のコマンドレット Get-Credential
次のパラメーターに値を指定してください:
Credential
PS C:\$Users\$administrator\Desktop> Connect-MsolService -Credential $cred
PS C:\$Users\$administrator\Desktop> Update-MsolFederatedDomain -DomainName azur
estudy.jp
Successfully updated 'azur
estudy.jp' domain
PS C:\$Users\$administrator\Desktop> Update-MsolFederatedDomain -DomainName azur
estudy.jp -SupportMultipleDomain
Successfully updated 'azur
estudy.jp' domain
PS C:\$Users\$administrator\Desktop> Convert-MsolDomainToFederated -DomainName con
toso.jp -SupportMultipleDomain
Successfully updated 'contoso.jp' domain
PS C:\$Users\$administrator\Desktop>
```

10. 再び [AD FS の管理] に戻って [操作] メニュー > [最新の情報に更新] をクリックし、[証明書利用者信頼] に新たに「Microsoft Office 365 Identity Platform」が登録されていることを確認します。



以上で UPN ドメインを複数登録するマルチドメイン対応手順は完了です。

ユーザーが OWA を利用する際の URL は以下どちらでも可能です。

<https://www.outlook.com/azurestudy.jp>

<https://www.outlook.com/contoso.jp>

STEP 15. アクセス制御

この STEP では、Office 365 を利用するユーザーのアクセスを制限するための設定方法について説明します。

この機能により、Office 365 を利用するユーザーのアクセスを制限することが可能です。

Note : 注意事項

Web ブラウザーによるアクセスの場合、要求元 IP アドレスを制限することはできません。こちらは、AD FS Proxy サーバーの IIS の設定（ファイアウォールの受信の規則）により制御することができます。

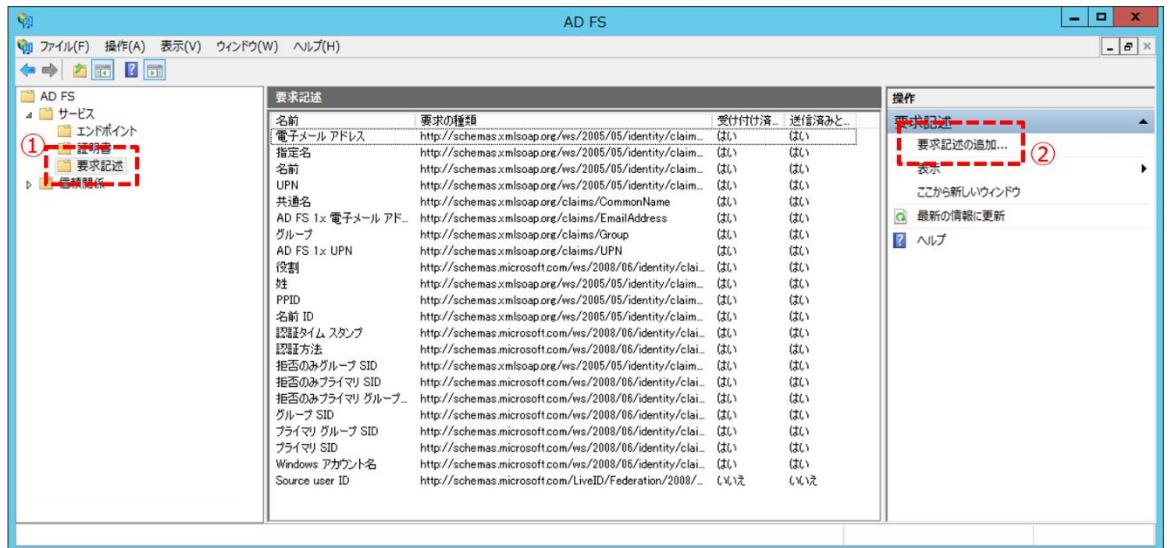
※この自習書では割愛します。

この STEP では、次のことを学習します。

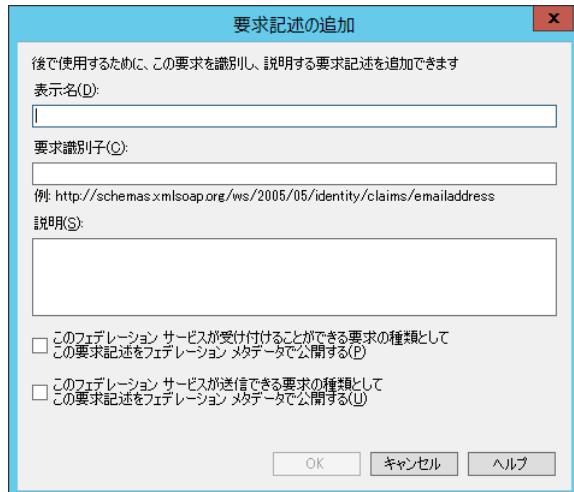
- ✓ 要求記述の登録
- ✓ 要求規則の登録
- ✓ 規則のセット

15.1 要求記述の登録

- ドメイン管理者アカウントで AD FS サーバー プライマリ [AZSTADFS01] にサインインし、[AD FS の管理] コンソールを開きます。
- 左ペインにて [AD FS] > [サービス] > [要求記述] を展開し、右ペインにて [操作] の [要求記述の追加] をクリックします。



- [要求記述の追加] 画面に必要な情報を登録します。



4. 手順 3 の画面で以下の内容を登録します。

表示名 (*1)	要求識別子 (*2)	説明 (*3)
要求元 IP アドレス	http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-forwarded-client-ip	要求元の IP アドレスを制御 (Office 365 を経由したデバイスに限る) (*4) → Web ブラウザーによるアクセスは Office 365 を経由せずに AD FS へ接続する為、OWA 利用の際にクライアント IP アドレスを制限することはできません
要求元アプ リケーショ ンの種類	http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-client-application	要求元のアプリケーションの種類を制御
使用デバイ スの種類	http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-client-user-agent	使用しているデバイスの種類を制御
AD FS Proxy 経由	http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-proxy	AD FS Proxy 経由か否かで制御
ブラウザ ベースアプ リケーショ ン	http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-endpoint-absolute-path	ブラウザベースのアプリケーションか 否かで制御

- (*1) : 表示名は任意の名前を付けてください。必須項目。
- (*2) : 要求識別子は必須項目。
- (*3) : 説明は省略可。
- (*4) : 社外からの Web ブラウザーによるアクセスは Office 365 を経由せずに AD FS Proxy サーバーへ直接アクセスするため、OWA を利用する要求元 IP アドレスを制御することはできません。 社外から OWA を利用する IP アドレスを制御する場合は、AD FS Proxy サーバーの IIS 設定 (ファイアウォールの受信の規則) により制御する必要があります。
- [このフェデレーション サービスが受け付けることができる要求の種類としてこの要求記述をフェデレーション メタデータで公開する] チェックボックスにチェックを付けます。
- [このフェデレーション サービスが送信できる要求の種類としてこの要求記述をフェデレーション メタデータで公開する] チェックボックスにチェックを付けます。

企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

The screenshot shows the Microsoft Active Directory Federation Services (AD FS) Management console. The left navigation pane shows 'AD FS' with categories like 'サービス' (Services), 'エンタープライズ' (Enterprise), '証明書' (Certificates), '要求記述' (Claim Rules), and '信頼関係' (Trust Relationships). The right pane displays a table titled '要求記述' (Claim Rules) with columns: '名前' (Name), '要求の種類' (Claim Type), '受け付け済' (Accepted), and '送信済み' (Sent). One specific rule, 'Source User ID', is highlighted with a red dashed box. The rule details are as follows:

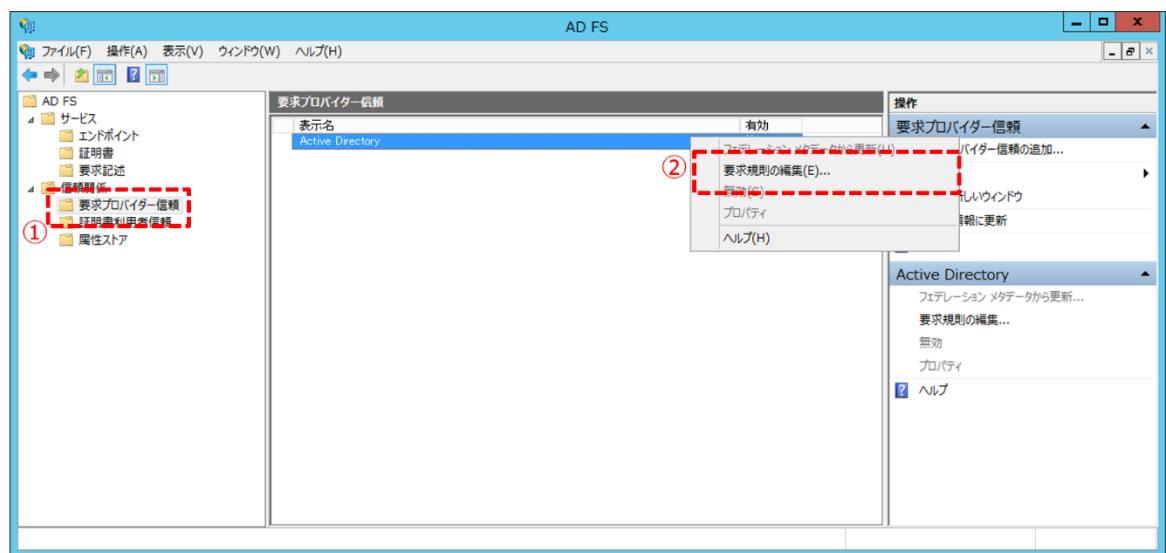
名前	要求の種類	受け付け済	送信済み
Source User ID	http://schemas.microsoft.com/ws/2008/06/identity/claims/sourceuserid	(はい)	(はい)

The '操作' (Operations) pane on the right includes options like '要求記述' (Claim Rule), '電子メール アドレス' (Email Address), and '削除' (Delete).

15.2 要求規則の登録

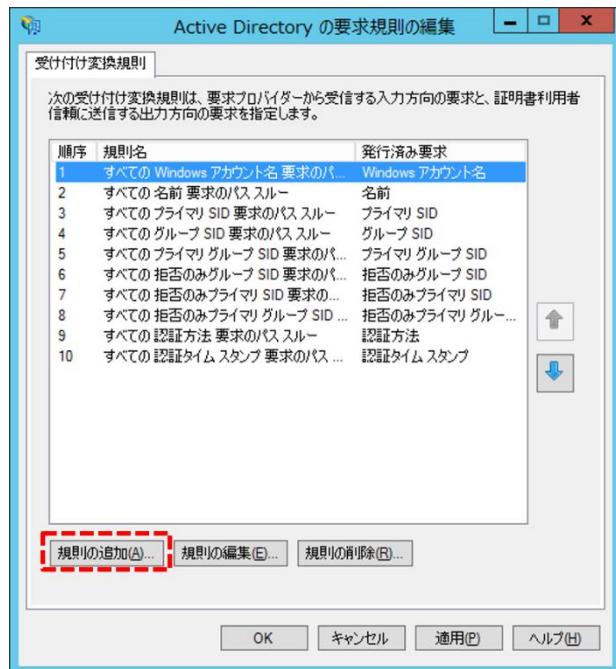
この項では、「15.1 要求記述の登録」にて作成した要求記述を要求プロバイダー信頼にセットする手順を説明します。

- ドメイン管理者アカウントで AD FS サーバー プライマリ [AZSTADFS01] にサインインし、[AD FS の管理] コンソールを開きます。
- 左ペインにて [AD FS] > [信頼関係] > [要求プロバイダー信頼] を展開し、中央ペインにて [Active Directory] を右クリックし、[要求規則の編集] をクリックします。

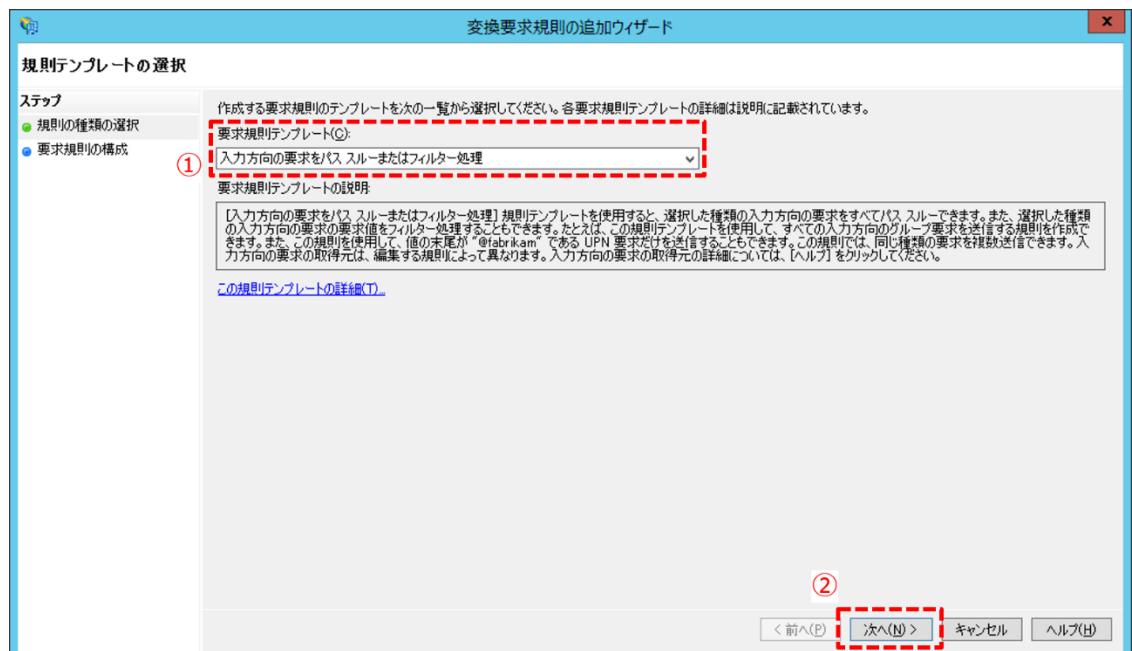


企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

3. [Active Directory の要求規則の編集] 画面の [受け付け変換規則] タブの [規則の追加] ボタンをクリックします。

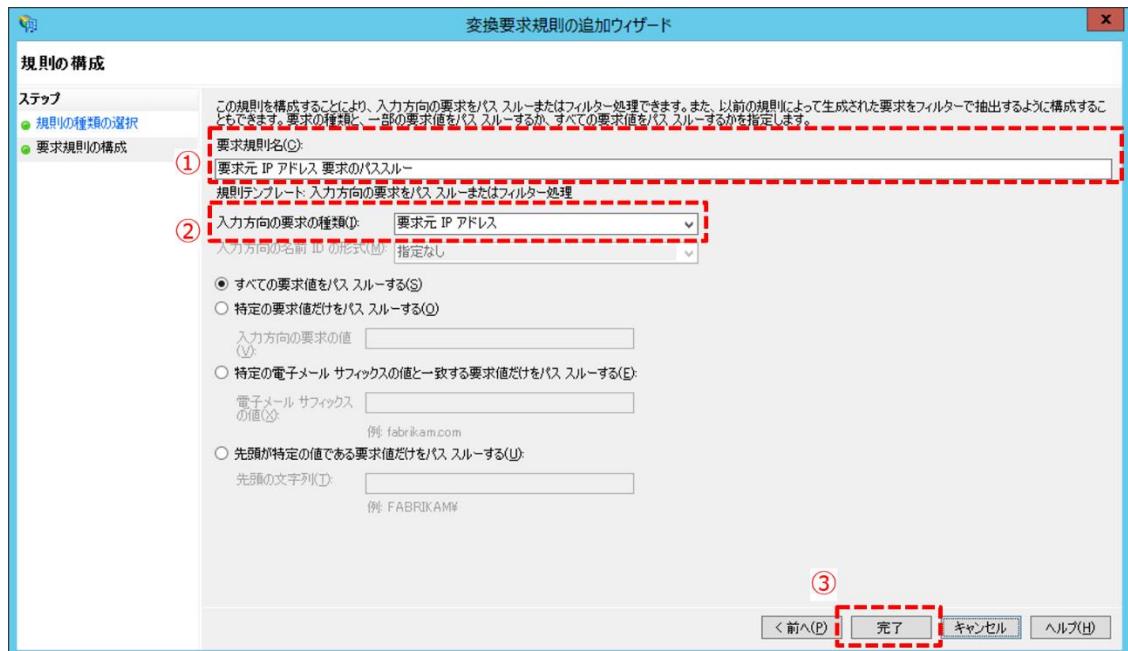


4. [変換規則の追加ウィザード] 画面の [規則テンプレートの選択] ページが表示されるので、[要求規則のテンプレート] 欄にて [入力方向の要求をパス スルーまたはフィルター処理] を選択し [次へ] ボタンをクリックします。

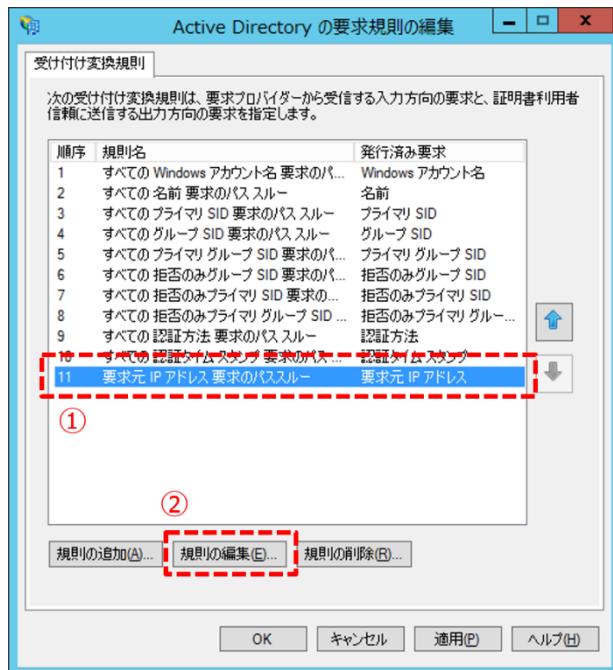


企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

5. [規則の構成] ページが表示されるので、[要求規則名] 欄に「要求元 IP アドレス 要求のバスルート (任意の名前)」を入力し、[入力方向の要求の種類] 欄に「要求元 IP アドレス」を選択して [完了] ボタンをクリックします。

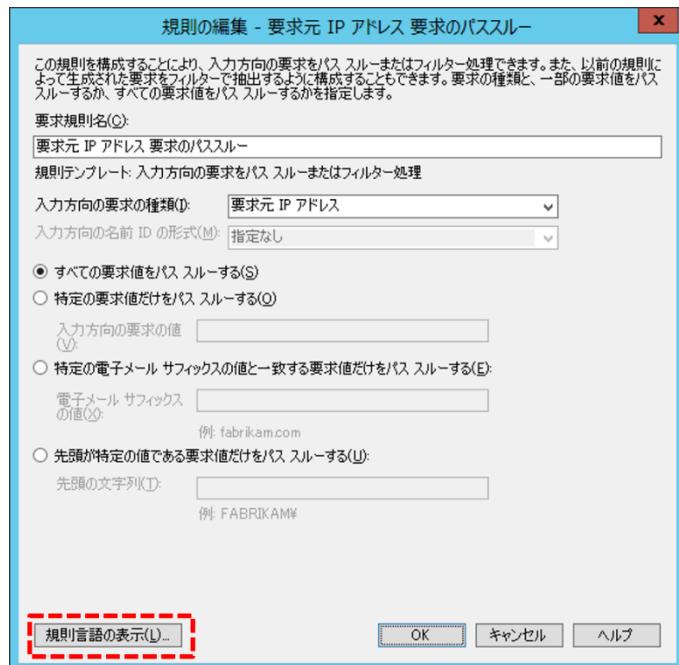


6. [Active Directory の要求規則の編集] 画面に戻り、[受け付け変換規則] タブで作成した規則を選択し [規則の編集] ボタンをクリックします。

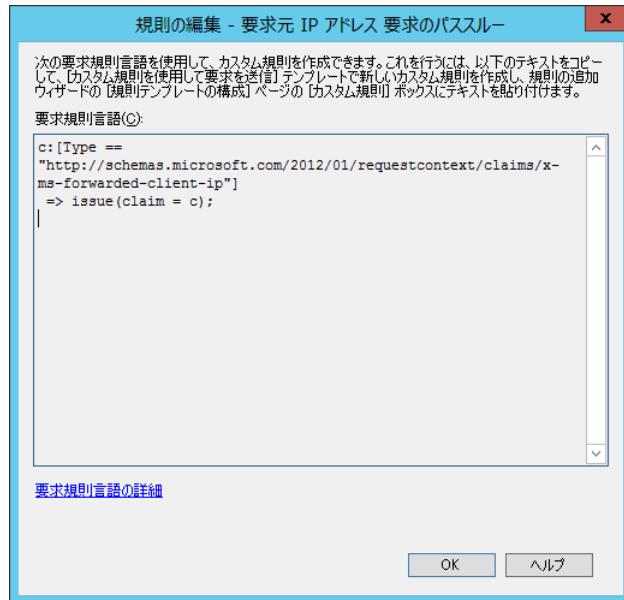


企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

7. [規則の編集 - 要求元 IP アドレス 要求のバスルート] 画面が表示されるので [規則言語の表示] ボタンをクリックします。

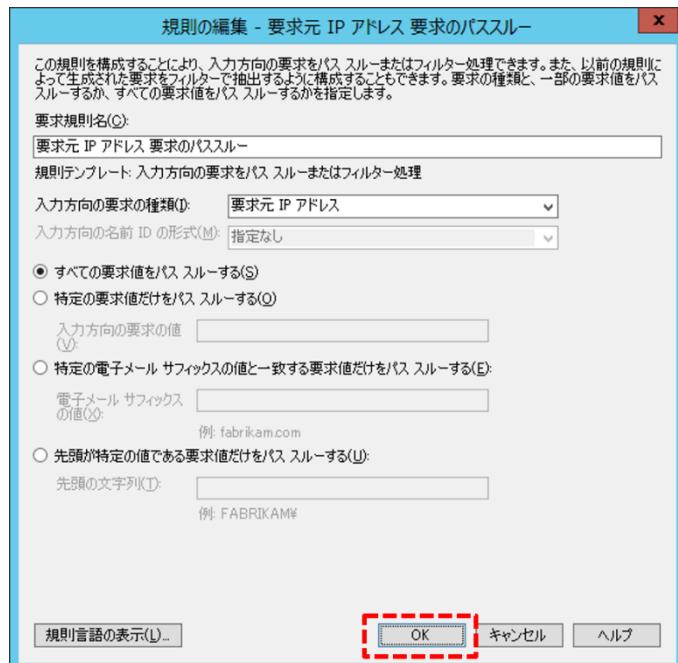


8. 表示画面にて下図のような表記になっていることを確認し [OK] ボタンをクリックします。



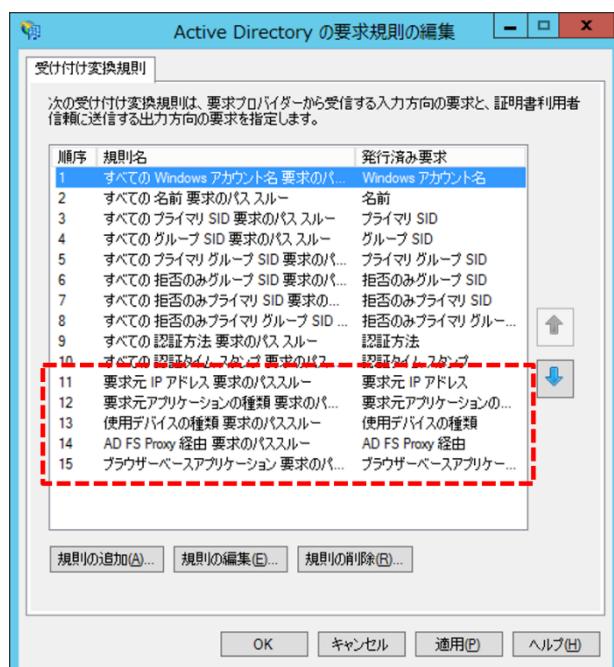
企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

9. [規則の編集 - 要求元 IP アドレス 要求のパススルー] 画面に戻るので、[OK] ボタンをクリックして閉じます。



10. 手順 3 ~ 9 を繰り返し、以下の残りの 4 つの要求規則を追加します。

- 要求元アプリケーションの種類 要求のパススルー
- 使用デバイスの種類 要求のパススルー
- AD FS Proxy 経由 要求のパススルー
- ブラウザベースアプリケーション 要求のパススルー



15.3 規則のセット

この項では、「15.2 要求規則の登録」にて作成した要求規則を証明書利用者信頼にセットする手順を説明します。

本手順により、AD FS にてアクセス制御が行われます。

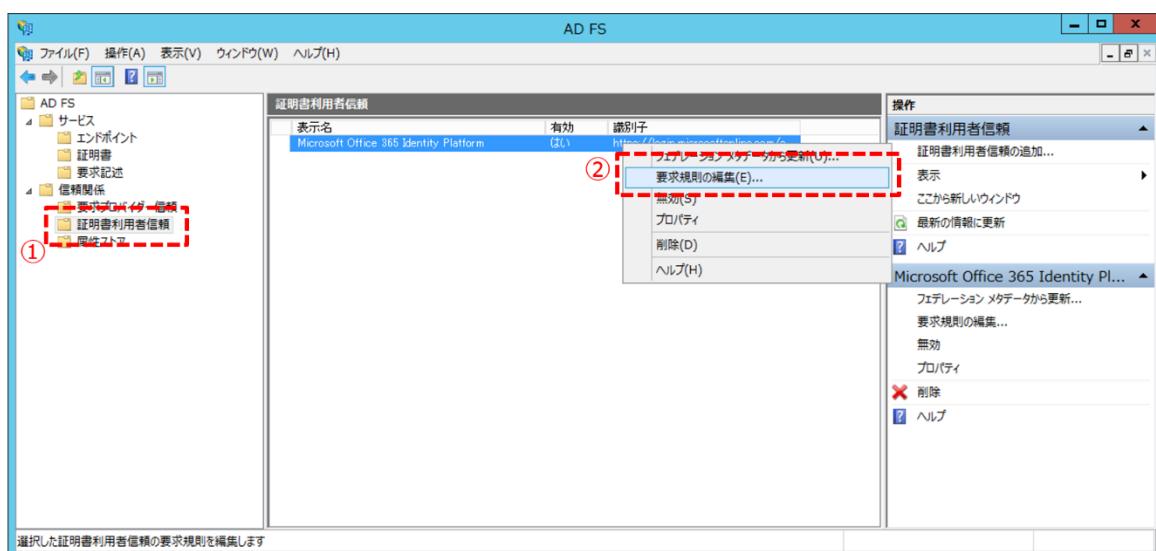
◆ 例 1) Office 365 へのアクセスは、社内からのアクセスに限定する

- ・ 社内からインターネットにアクセスする場合には Proxy を経由し、Proxy で使用するグローバル IP アドレスは、「111.111.111.111」または「222.222.222.222」とする。

本ルールは「社内や別拠点（海外拠点など）の利用は許可するが、それ以外の利用は拒否する」際に使用します。

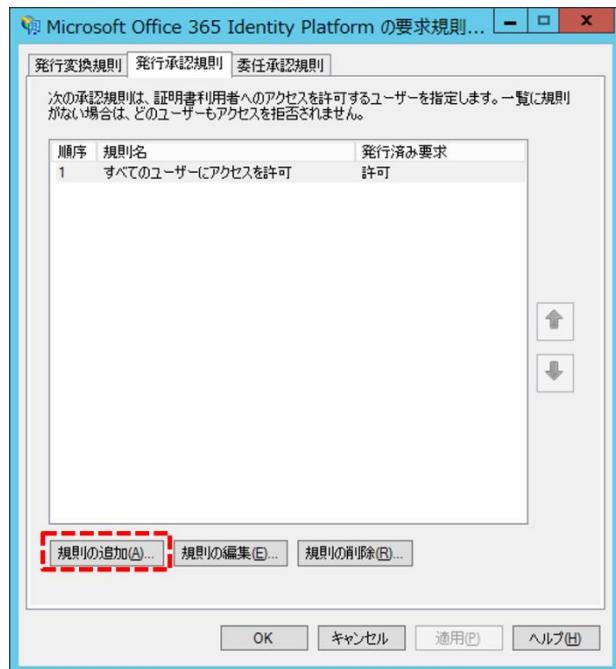
この場合、IP アドレスは拠点で利用しているプロキシサーバーの IP アドレスを指定します。

1. ドメイン管理者アカウントで AD FS サーバー プライマリ [AZSTADFS01] にサインインし、[AD FS の管理] コンソールを開きます。
2. 左ペインにて [AD FS] > [信頼関係] > [証明書利用者信頼] を展開し、中央ペインにて [Microsoft Office 365 Identity Platform] を右クリックし、[要求規則の編集] をクリックします。



企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

3. [要求規則の編集] 画面が表示されるので、[発行承認規則] タブの [規則の追加] ボタンをクリックします。



4. [規則テンプレートの選択] ページが表示されるので、[要求規則テンプレート] 欄にて [カスタム規則を使用した要求の送信] を選択し、[次へ] ボタンをクリックします。

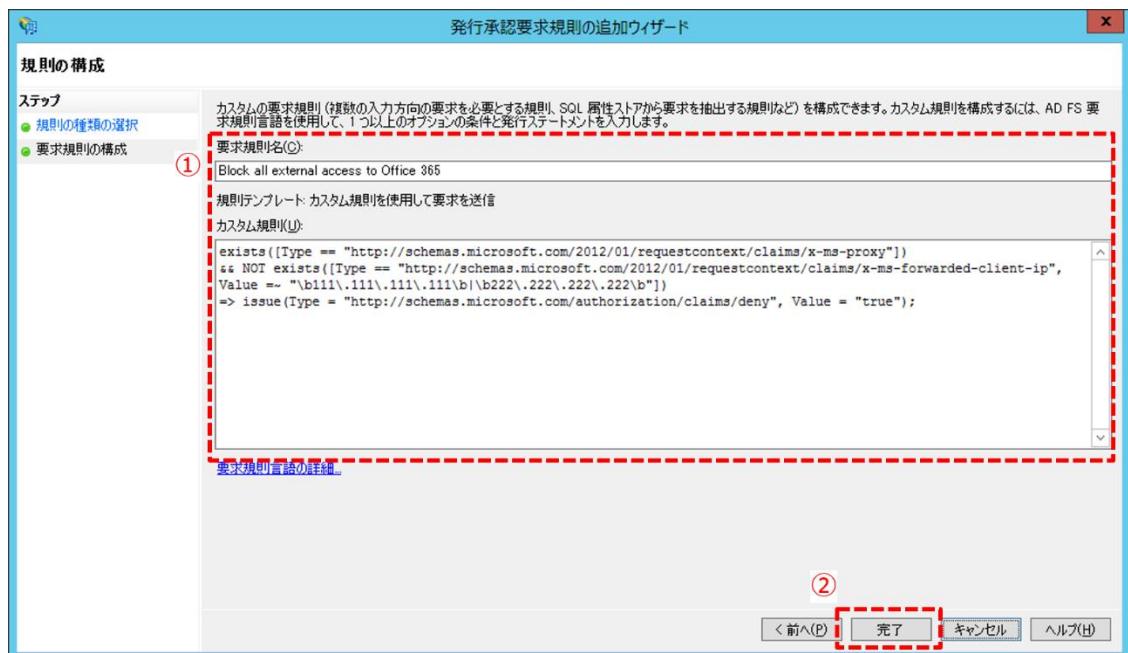


企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

5. [規則の構成] ページで、[要求規則名] 欄にてこの規則の名前を入力します。（任意の名前を入力します。）

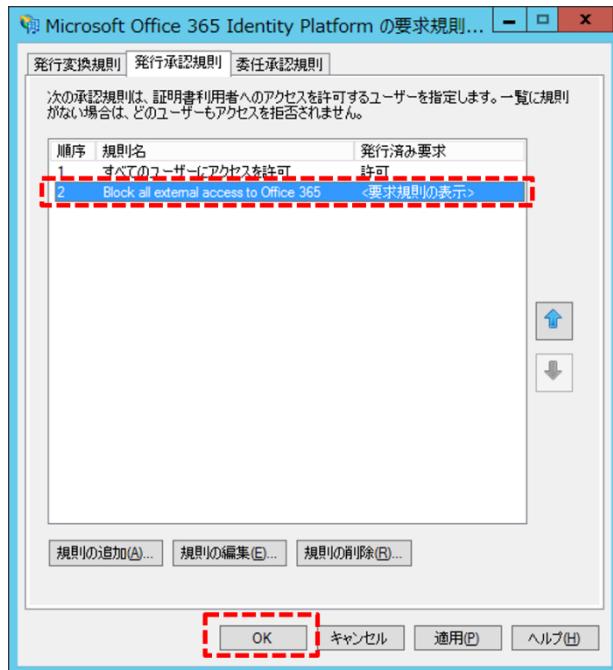
[カスタム規則] 欄にて、以下の要求規則の言語の構文を入力し、[完了] ボタンをクリックします。

```
exists([Type == "http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-proxy"])
&& NOT exists([Type ==
"http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-forwarded-client-ip",
Value =~ "\$b111\$.111\$.111\$.111\$b|\$b222\$.222\$.222\$.222\$b"])
=> issue(Type = "http://schemas.microsoft.com/authorization/claims/deny", Value =
"true");
```



企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

6. 発行承認規則が作成されたことを確認し [OK] ボタンをクリックします。



➔ 例 2) Office 365 へのアクセスは、社内からのアクセスに限定する。ただし、特定のセキュリティ グループに所属するユーザーの社外からの利用は許可する。

- ・ 社内からインターネットにアクセスする場合には Proxy を経由し、Proxy で使用するグローバル IP アドレスは、「111.111.111.111」または「222.222.222.222」とする。
- ・ セキュリティ グループの SID は、「S-1-5-21-397933417-626991126-188441444-512」とする。

例 1 の手順を参考にし、[カスタム規則] 欄にて、以下の要求規則の言語の構文を入力します。

```
exists([Type == "http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-proxy"]) &&
NOT exists([Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid", Value =~ "S-1-5-21-397933417-626991126-188441444-512"]) &&
NOT exists([Type == "http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-forwarded-client-ip",
Value=~"¥b111¥. 111¥. 111¥. 111¥b|¥b222¥. 222¥. 222¥. 222¥b"])
=> issue(Type = "http://schemas.microsoft.com/authorization/claims/deny", Value
="true");
```

参考情報 URL : 「クライアントの場所に基づいた Office 365 サービスに対するアクセスの制限 (<http://community.office365.com/ja-jp/w/sso/927.aspx>)」

STEP 16. 認証ログ

AD FS のサービスは AD の接続処理と Office 365 の信頼関係の処理結果を AD FS サーバーのイベント ビューアーのログから取得できます。

この STEP では、ログの保存場所、設定方法について説明します。

この STEP では、次のことを学習します。

- ✓ 認証失敗ログ（AD FS によって制御されたログ）
- ✓ 認証成功ログ（AD FS によって認証されたログ）
- ✓ AD FS トレース ログの設定

16.1 認証失敗ログ (AD FS によって制御されたログ)

➔ ログの内容

項目	内容
ログ保存場所	[アプリケーションとサービス] > [AD FS 2.1] > [Admin]
イベント ID	325 (付加情報のログのイベント ID:501)
ログの内容	Microsoft.IdentityServer.Service.IssuancePipeline.CallerAuthorizationException : MSIS5007: 証明書利用者信頼 urn:federation:MicrosoftOnline の発信者 ID azurestudy¥studyuser01 に対する発信者の承認が失敗しました。

➔ 付加情報のログに含まれる項目

付加情報のログに含まれる項目
<ul style="list-style-type: none">ユーザー ID所属グループの SID日付・時刻アクセス元の IP アドレスアクセス プロトコル (RPC/HTTPS, POP/IMAP, ActiveSync など)アクセス アプリケーション (Outlook であればバージョンやエディション)

▼ 認証失敗ログ（AD FS によって制御されたログ）の例

- 例①



- 例②



Microsoft Azure 自習書シリーズ No.6
企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

- 例③



16.2 認証成功ログ (AD FS によって認証されたログ)

「16.3 AD FS トレース ログの設定」後、すべてのログが表示されます。認証成功ログを参照する場合は、「16.3 AD FS トレース ログの設定」を行ってください。

◆ ログの内容

項目	内容
ログ保存場所	[Windows ログ] > [セキュリティ]
イベント ID	299 (付加情報のログのイベント ID: 500, 501)
ログの内容	トークンは証明書利用者 'urn:federation:MicrosoftOnline' に対して正常に発行されました。発行された要求については同じインスタンス ID を持つ監査 500 を参照してください。発信者 ID については同じインスタンス ID を持つ監査 501 を参照してください。OnBehalfOf ID (存在する場合) については、同じインスタンス ID を持つ監査 502 を参照してください。ActAs ID (存在する場合) については、同じインスタンス ID を持つ監査 503 を参照してください。

◆ 付加情報のログに含まれる項目

付加情報のログに含まれる項目
<ul style="list-style-type: none"> ユーザー ID 所属グループの SID 日付・時刻 アクセス元の IP アドレス アクセス プロトコル (RPC/HTTPS, POP/IMAP, ActiveSync など) アクセス アプリケーション (Outlook であればバージョンやエディション)

➔ 認証成功ログ (AD FS によって認証されたログ) の例

- 例①

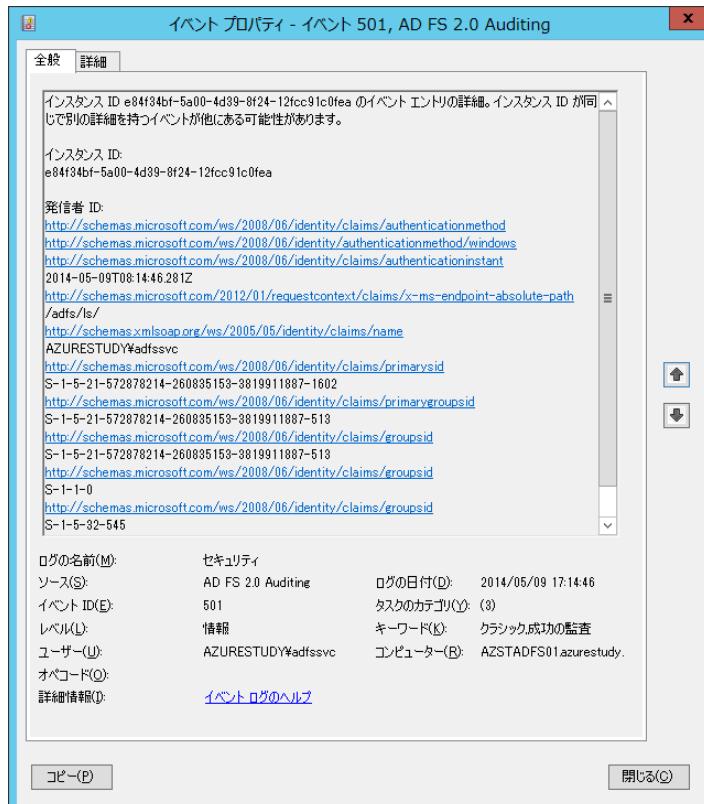


- 例②

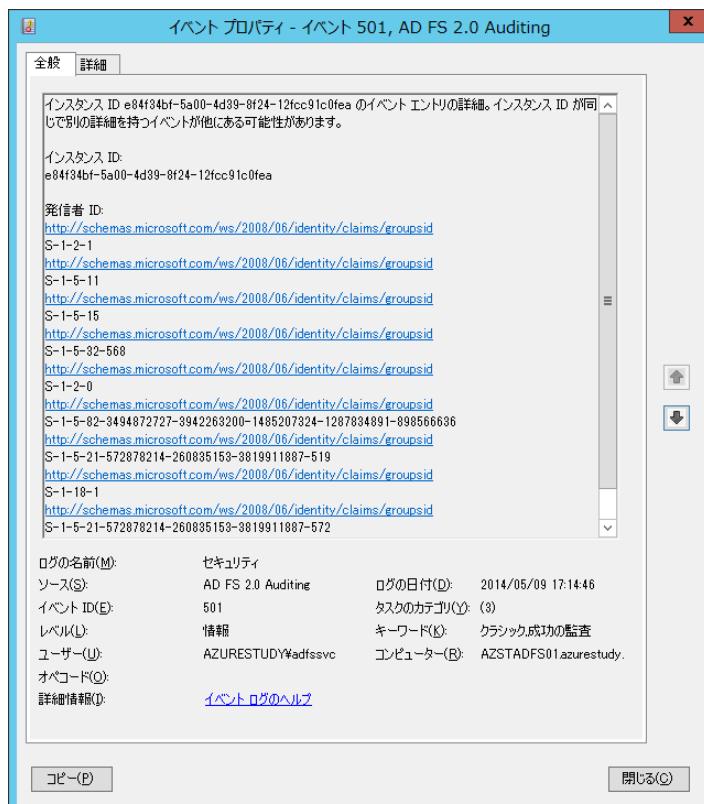


企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

• 例③

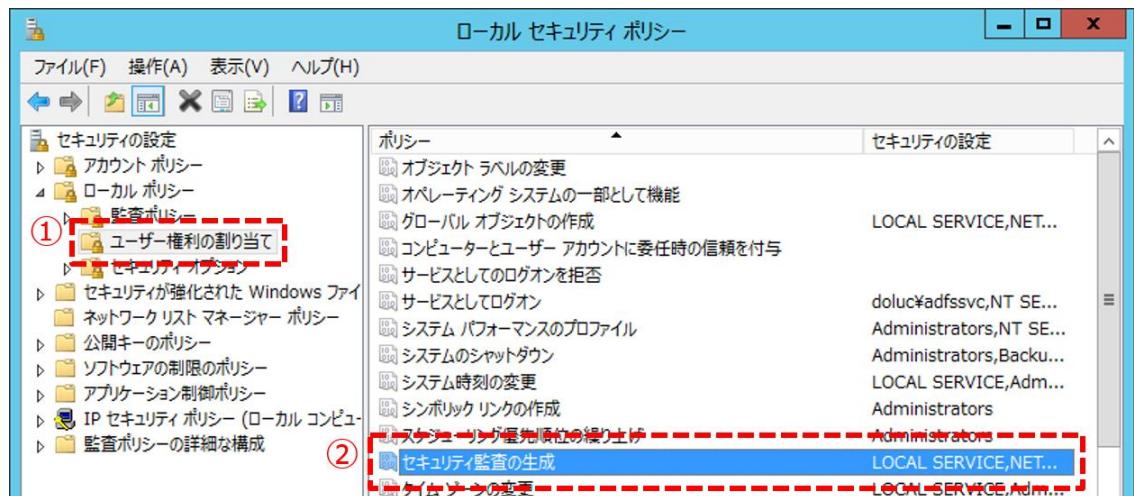


• 例④

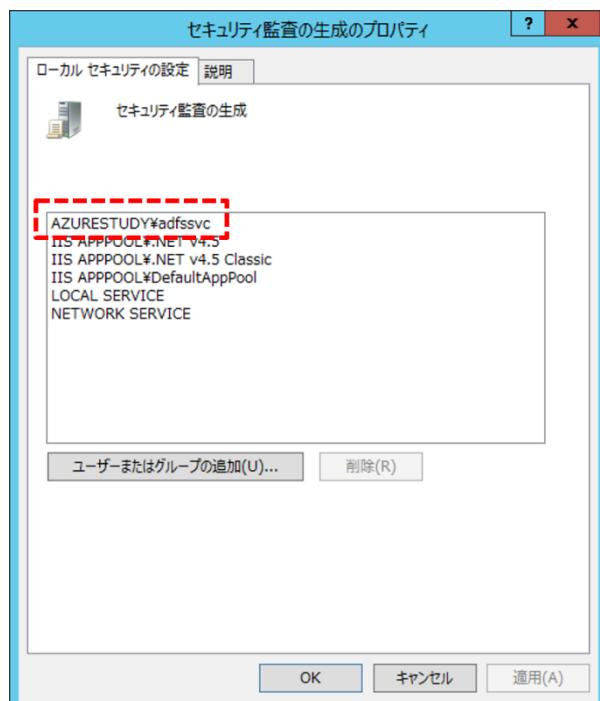


16.3 AD FS トレース ログの設定

- ドメイン管理者アカウントで AD FS サーバー プライマリ [AZSTADFS01] にサインインし、[ローカル セキュリティ ポリシー] を開きます。
- 左ペインにて [セキュリティの設定] > [ローカル ポリシー] > [ユーザー権利の割り当て] を展開し、右ペインの一覧から [セキュリティ監査の生成] のプロパティを開きます。



- [セキュリティ監査の生成] に AD フェデレーション 用 サービス アカウントが登録されていることを確認します。

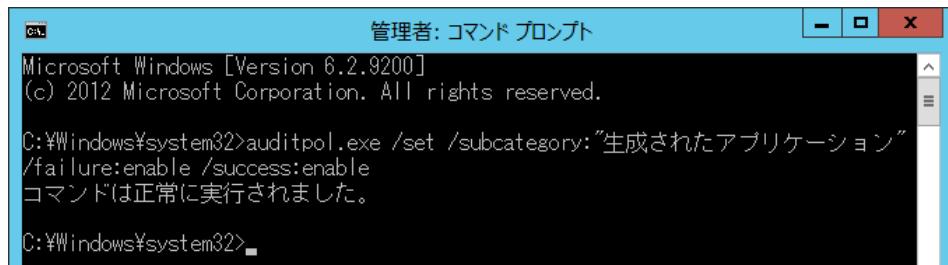


企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

4. [PowerShell] または [コマンド プロンプト] を「管理者として実行」で開き、以下のコマンドを実行します。

```
auditpol.exe /set /subcategory:"生成されたアプリケーション" /failure:enable
/success:enable
```

※ 実際は 1 行で入力します。



元に戻す場合のコマンドは以下のとおりです。

```
auditpol.exe /set /subcategory:"生成されたアプリケーション" /failure:disable
/success:disable
```

※ 実際は 1 行で入力します。

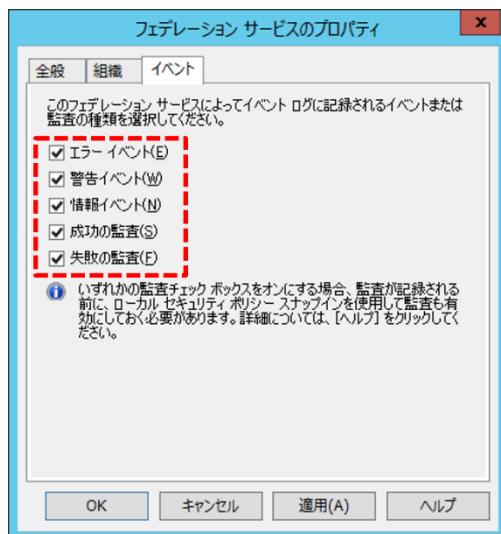
5. [AD FS の管理] を開きます。

6. 左ペインにて [AD FS] を選択し、右ペインにて [操作] の [フェデレーション サービスのプロパティの編集] をクリックします。



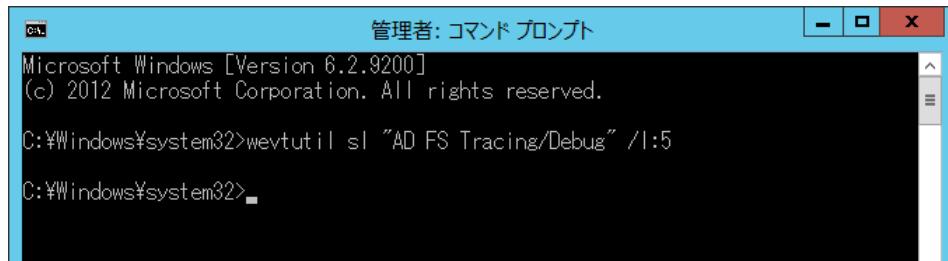
企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

7. [フェデレーション サービスのプロパティ] 画面が表示されます。[イベント] タブを開き、赤枠のすべてのチェックボックスにチェックを付けます。そして、[OK] ボタンをクリックし、画面を閉じます。



8. [PowerShell] または [コマンド プロンプト] を「管理者として実行」で開き、以下のコマンドを実行します。

```
wvtutil sl "AD FS Tracing/Debug" /l:5
```

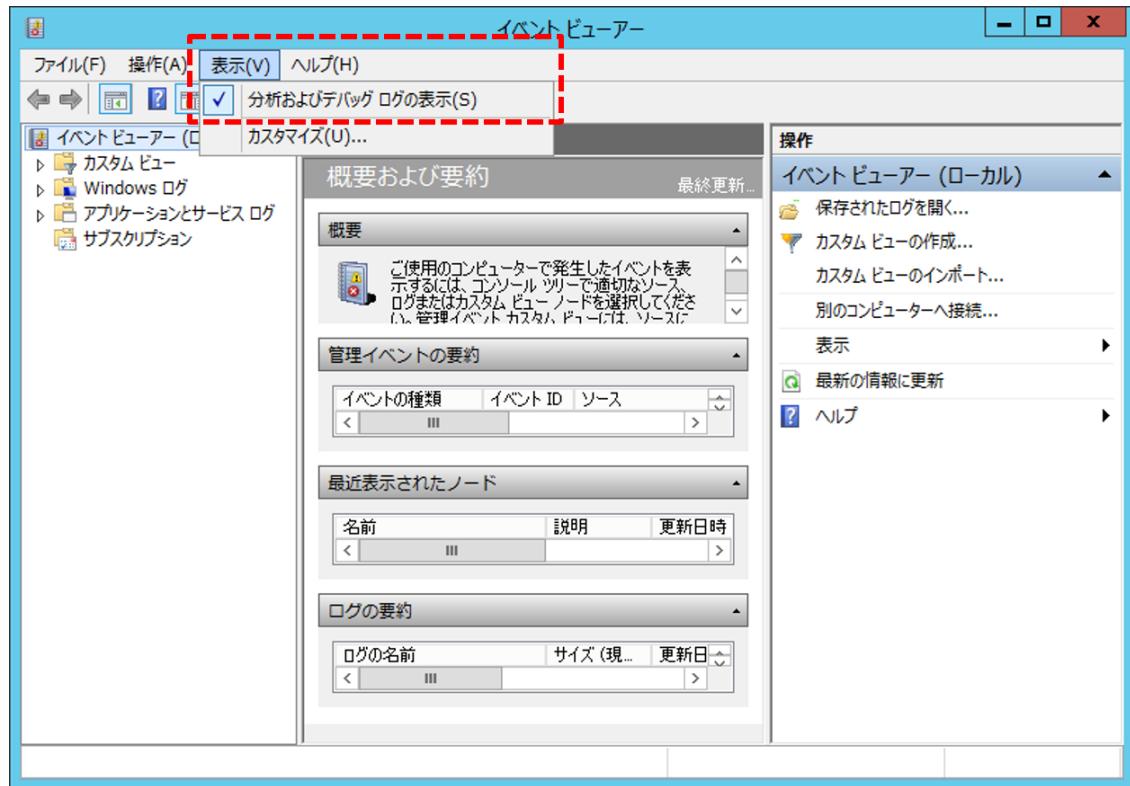


元に戻す場合のコマンドは以下のとおりです。

```
wvtutil sl "AD FS Tracing/Debug" /l:4
```

9. [イベント ビューアー] を開きます。

10. [表示] > [分析およびデバッグログの表示] をクリックします。

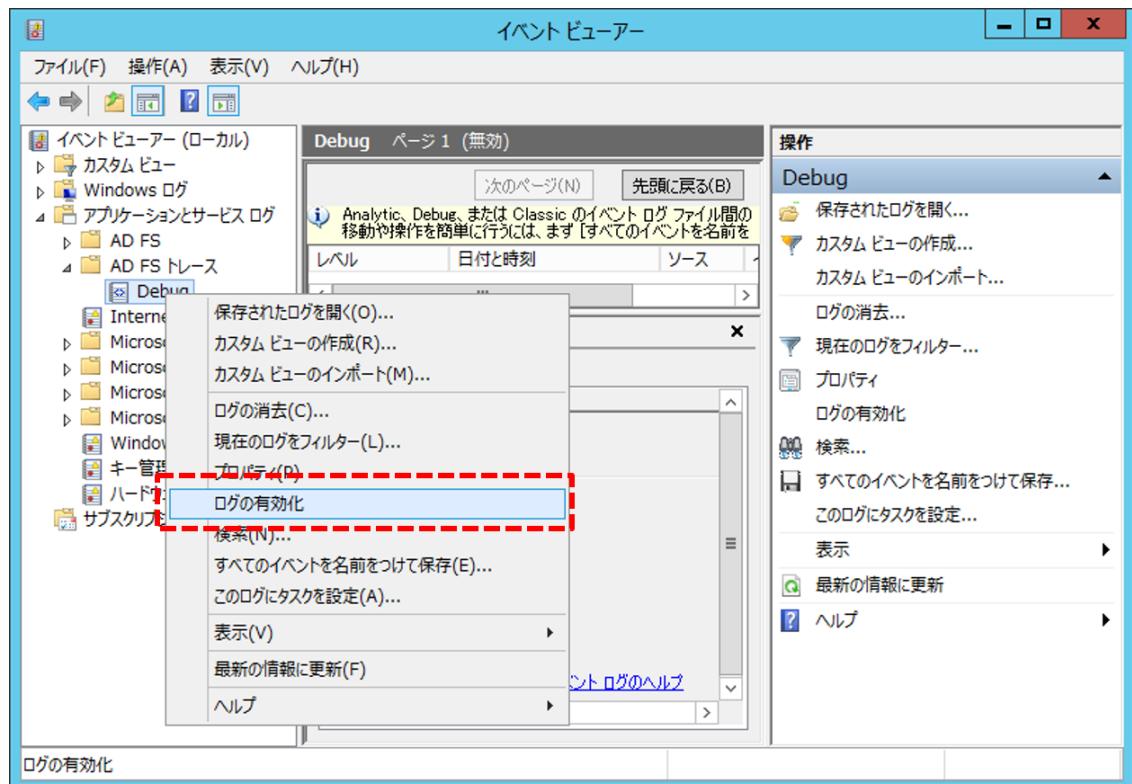


企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携

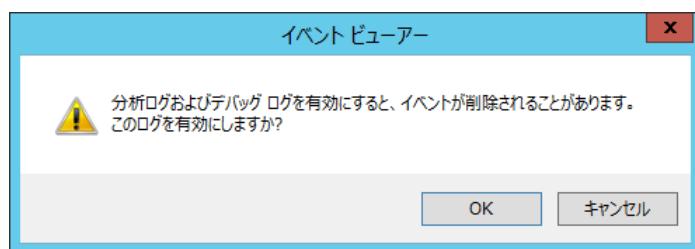
11. 左ペインにて [イベント ビューアー] > [アプリケーションとサービス ログ] > [AD FS トレース] > [Debug] と展開し、[Debug] を右クリックして [ログの有効化] をクリックします。

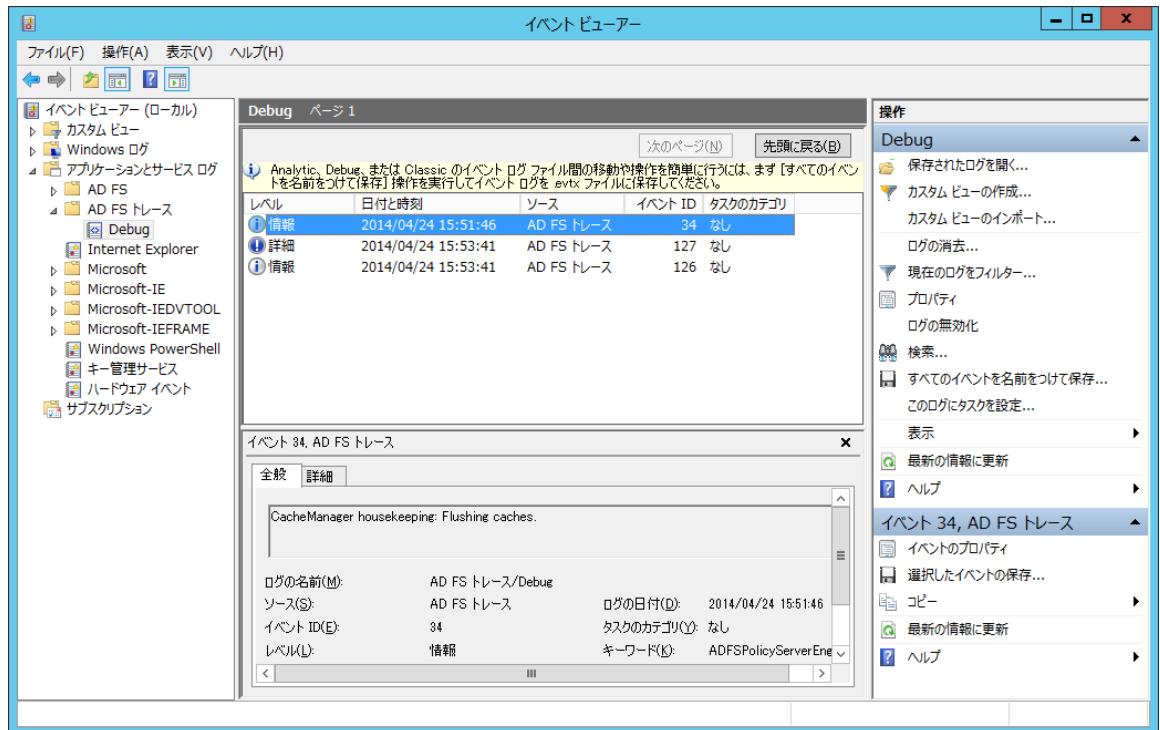
Note : 既に「ログの有効化」を行っている場合

既に有効な場合は手順 8 にてエラーが発生します（事前に無効にしてから手順 8 を実施することで解消します）



12. 確認メッセージボックスが開くので、[OK] ボタンをクリックします。



13. AD FS トレース ログが表示されます。

STEP 17. Appendix

- ✓ SSO と仮想マシンを使用した AD DS または AD FS と Office 365 の展開
- ✓ 社内 VPN に関する要件
- ✓ IP アドレス指定と名前解決
- ✓ ディレクトリ同期するオブジェクトの要件
- ✓ 対応しているルート証明機関

17.1 SSO と仮想マシンを使用した AD DS または AD FS と Office 365 の展開

◆ Azure の展開ガイドライン

Windows Server AD を仮想マシン上で展開する際のガイドラインは、社内で（仮想マシンで、あるいは多くの場合は物理コンピューターで）実行する場合と同じです。通常は、同じベスト プラクティスが Azure 内の仮想ドメイン コントローラーに適用されます。

Azure 上での AD DS と AD FS の仮想化と展開に関する詳しいガイドラインは、「Azure の仮想マシンでの Windows Server Active Directory のデプロイ ガイドライン (<http://msdn.microsoft.com/library/azure/jj156090.aspx>)」に記載されています。

これらのガイドラインは、仮想マシン上でのドメイン コントローラーの展開に関する一般的なガイダンスとして使用することをお勧めします。

また、以下の原則に従う必要があります。

- 読み取り/書き込みドメイン コントローラーを展開する必要があります。読み取り専用ドメイン コントローラーをディレクトリ同期で使用することはサポートされていません。
- AD フォレストに複数のユーザー ドメインが含まれている場合は、ドメインごとに 1 つ以上のドメイン コントローラーを Azure に展開する必要があります。これにより、サービスへの連絡アクセスが保証され、VPN トンネルを通過する認証トラフィックが削減されます。
- AD FS サービスの最良の可用性を実現するために、AD FS サーバーと AD FS Proxy サーバーを 2 台以上展開することをお勧めします。
- ドメイン コントローラーと AD FS サーバーは絶対に直接インターネットに公開しないで、VPN を経由した場合にのみ到達できるようにすることをお勧めします。
- AD FS サーバーをインターネットに公開する場合には AD FS Proxy を使用する必要があります。
- Office 365 ディレクトリ統合コンポーネント間の遅延を削減するために、ドメイン コントローラーと AD FS サーバーを単一のアフィニティ グループとして展開することをお勧めします。 詳細については、「地域 Vnet および仮想ネットワークのアフィニティ グループについて (<http://msdn.microsoft.com/library/azure/jj156085.aspx>)」を参照してください。

➔ AD サイト、サブネット、レプリケーション トラフィック

展開を最適化するには、ドメイン コントローラー ポケーター、サイト間トポロジ ジェネレーター (ISTG)、サイト間メッセージング サービス (ISM) のトラフィックの微調整を検討します。

- AD のサブネットとサイトを正しく定義して接続します。
- 社内サイトと Azure サイトとの間のリンク コストが社内サイトのリンク コストを上回るようになります。 リンク コストが大きければ大きいほど、社内のコンピューターが社内での操作のために VPN 接続を通過して Azure 内のドメイン コントローラーに接続する可能性が小さくなります。
- レプリケーションは、通知に従ってではなく、スケジュールに従って駆動されるようにします。
- レプリケーション トラフィックで適切な量の圧縮が使用されるようにします。 ドメイン コントローラーは、さまざまなレプリケーション トラフィック圧縮ツールを提供しています。 詳細については、「Active Directory レプリケーション ツールと設定 ([http://technet.microsoft.com/ja-jp/library/cc739941\(v=ws.10\).aspx](http://technet.microsoft.com/ja-jp/library/cc739941(v=ws.10).aspx))」を参照してください。
- レプリケーション スケジュールを遅延許容範囲に合わせて調整します。 ドメイン コントローラーは値の最後の状態しかレプリケートしません。 小規模なオブジェクトの変更が大量に発生した場合は、レプリケーションを遅らせることによって、コストが節約されます。

➔ AD FS の公開

クライアントにフェデレーション アプリケーションとフェデレーション サービスへのアクセスを提供するために、AD FS エンドポイントが使用されます。 クライアントの認証が成功すると、エンドポイントからクライアントに認証トークンが発行されます。 AD FS サーバー上でこれらのエンドポイントを管理し、それぞれを AD FS Proxy サーバーを介して安全に公開します。

基本認証クライアント (Outlook を含む) の接続を許可するには、AD FS インフラストラクチャが AD FS Proxy 経由でインターネットからアクセスできる必要があります。 そうでない場合は、どの Outlook クライアントも認証できなくなります (内部の組織のネットワークからでさえも)。

17.2 社内 VPN に関する要件

社内のネットワークを仮想マシンに接続するには、VPN を構成する必要があります。そのため、インターネットに直接公開されている VPN デバイスを構内に設置する必要があります。現時点では、ネットワーク アドレス変換 (NAT) はサポートされていません。

社内 VPN デバイスは、以下の機能をサポートする必要があります。

- インターネット キー交換バージョン 1 (IKEv1)。
- トンネル モードで IPsec アソシエーションを確立します。
- NAT トラバーサル (NAT-T)。
- AES 128 ビット暗号化関数、SHA-1 ハッシュ関数、グループ 2 モードの Diffie-hellman Perfect Forward Secrecy。
- VPN デバイスは、VPN ヘッダーを付けてデータをカプセル化する前に、パケットを分割する必要があります。

Note : VPN デバイスを NAT の背後に配置することはできません

VPN デバイスを NAT の背後に配置することはできません。VPN デバイスには、インターネットに接続するパブリック IPv4 アドレスを付与する必要があります。

仮想ネットワークでサポートされている VPN デバイスの一覧については、「仮想ネットワークに使用する VPN デバイスについて (<http://msdn.microsoft.com/ja-jp/library/windowsazure/jj156075.aspx>)」を参照してください。

17.3 IP アドレス指定と名前解決

基本的に仮想マシンの内部 IP アドレスは DHCP によって払い出される IP アドレスを使用することになります。 そうする場合、仮想ネットワークに接続される仮想マシンの IP アドレスは、そのマシンが使用停止になるまで変化しません。 つまり、ドメイン コントローラーと併置されている場合（推奨）、IP アドレスに関する Windows Server AD の要件は、DNS の要件と同様に満たされるということです。 加えて、仮想ネットワークでは、IP アドレス指定と DNS に対する高度な制御が行えます。

◆ IP アドレスの指定

仮想マシンは、DHCP リース アドレスを使用するように構成する必要があります。 Azure は、リースが期限切れになるとことや、仮想マシン間で移動することが起こらないようにします。 この非静的構成は、ほとんどの AD 管理者が使い慣れているものと正反対ですが、仮想マシンが VPN や社内サーバーとシームレスに連動するための要件になっています。

Note : 過去にリースされたアドレスの取り扱いについて

過去にリースされたアドレスを静的に定義することは考慮しないでください。 このアドレスはリース期間が残っている間は機能しますが、リース期間が切れると、仮想マシンがネットワークとのすべての通信を失い、ネットワークから切断されます。

◆ 名前の解決

ドメイン コントローラー上に Windows Server DNS を展開する必要があります。 Azure DNS は Windows Server AD DS の複雑な名前解決ニーズを満たしておらず、動的サービス レコード (SRV レコード) などもサポートしていません。 Windows Server の社内展開と同様に、Active Directory DNS はドメイン コントローラーとドメインに参加しているクライアントにとって極めて重要な構成項目の 1 つです。

フォールト トレランスとパフォーマンス上の理由から、Azure 上で動作しているドメイン コントローラーに Windows Server DNS サービスをインストールすることをお勧めします。

17.4 ディレクトリ同期するオブジェクトの要件

この項では、社内 AD と Office 365 との間のディレクトリ同期を成功させるために必要な要件について説明します。

ディレクトリ同期を行うに当たっては、社内 AD 上のオブジェクトが以下の要件に満たしている必要があります。

オブジェクト	説明
sAMAccountName	<ul style="list-style-type: none"> 利用できる最大文字数は 20 文字 以下の禁則文字は利用できません ✓ ` ~ ! @ # \$ % ^ & * + = { } [] ¥ : " ; ' < > ?, / 無効な "sAMAccountName" でも有効な "userPrincipalName" を持つていればユーザーは Office 365 に同期されます "sAMAccountName" および "userPrincipalName" が無効な場合、AD 上で "userPrincipalName" を有効なものに修正します
givenName	<ul style="list-style-type: none"> 利用できる最大文字数は 64 文字 以下の禁則文字は利用できません ✓ ?@¥+
sn (surname)	<ul style="list-style-type: none"> 利用できる最大文字数は 256 文字 以下の禁則文字は利用できません ✓ ?@¥+
displayName	<ul style="list-style-type: none"> 利用できる最大文字数は 256 文字 以下の禁則文字は利用できません ✓ ?@¥+
mail	<ul style="list-style-type: none"> 利用できる最大文字数は 256 文字 以下の禁則文字は利用できません ✓ ! # \$ % & * + / = ? ^ ` { } 一意の値 <p>※ 値が重複していた場合、ディレクトリ同期によって最初に同期されたユーザーが Office 365 へ反映され、それ以降のユーザーは同期されません</p>
mailNickname	<ul style="list-style-type: none"> 利用できる最大文字数は 64 文字 以下の禁則文字は利用できません ✓ " ¥ [] : > < ;
proxyAddresses	<ul style="list-style-type: none"> 利用できる最大文字数は 256 文字 以下の禁則文字は利用できません ✓) (; > <] [, ¥
userPrincipalName	<ul style="list-style-type: none"> ユーザー名で利用できる最大文字数は 64 文字 ドメイン名で利用できる最大文字数は 256 文字 以下の禁則文字は利用できません ✓ }{ # _ \$ % ~ * +) (> < ! / ¥ = ? ` 1 ディレクトリ同期の際、"&" は自動的に "_" に変換されます ディレクトリ同期の際、"^" は自動的に取り除かれます ディレクトリ同期の際、"_" はそのままです
Groups	<ul style="list-style-type: none"> ディレクトリ同期の際、"@" の有無でメールの有効性を確認します
Contacts	<ul style="list-style-type: none"> ディレクトリ同期の際、"@" の有無でメールの有効性を確認します

17.5 対応しているルート証明機関

次の表は、現在 Microsoft によって信頼されている CA の一覧です。

(2014 年 4 月現在)

CA のフレンドリ名	発行元	目的
Comodo	Comodo Certification Authority	サーバー認証、クライアント認証
Digicert	Digicert Global Root Certification Authority	サーバー認証、クライアント認証
Digicert High Assurance EV	Digicert Global Root Certification Authority	サーバー認証、クライアント認証
Entrust	Entrust.net Secure Server Certification Authority	サーバー認証、クライアント認証
Entrust (2048)	Entrust.net Secure Server Certification Authority	サーバー認証、クライアント認証
Equifax	Equifax Secure Certification Authority	サーバー認証、クライアント認証
GlobalSign	GlobalSign Certification Authority	サーバー認証、クライアント認証
Go Daddy	Go Daddy Class 2 Certification Authority	サーバー認証、クライアント認証
Network Solutions	Network Solutions Certification Authority	サーバー認証、クライアント認証
PositiveSSL	Comodo Certification Authority	サーバー認証、クライアント認証
SECOM	セコムトラストシステムズ証明機関	サーバー認証、クライアント認証
UTN-UserFirst-Hardware	Comodo Certification Authority	サーバー認証、クライアント認証
VeriSign	Class 3 Public Primary Certification Authority	サーバー認証、クライアント認証
VeriSign	VeriSign Trust Network	サーバー認証、クライアント認証

おわりに

この自習書では、すべての Office 365 SSO 統合コンポーネントを Azure で展開する環境の構築について学習しました。

Office 365 SSO 統合コンポーネントを Azure に展開することで、コスト削減、迅速な展開、ビジネス継続性の向上、災害対策、社内ネットワークに対する依存の低減などのメリットを得ることができます。

なお、この自習書で取り扱った環境を構築するために、以下の自習書についてもご参考ください。

- Microsoft Azure 自習書シリーズ「企業内システムと Microsoft Azure の VPN 接続」
- Microsoft Azure 自習書シリーズ「企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携」
- Microsoft Azure 自習書シリーズ「企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携」
- Microsoft Azure 自習書シリーズ「企業内システムと Microsoft Azure の VPN 接続、Active Directory、ファイルサーバー連携」

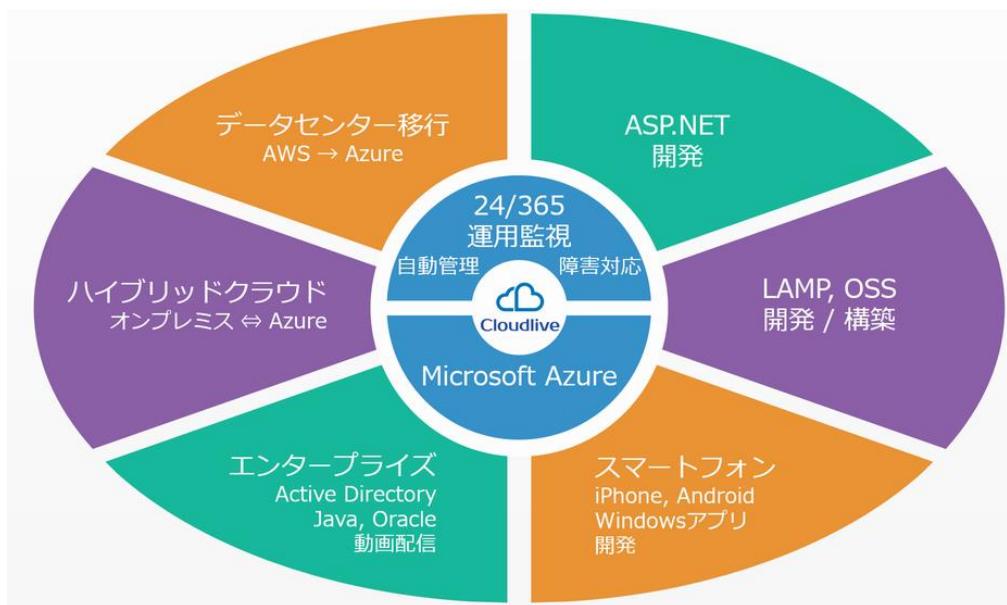
この自習書が仮想マシンを使用して Office 365 SSO 統合コンポーネントを構築する手助けになれば幸いです。

執筆者プロフィール

Cloudlive 株式会社 (<http://www.cloudlive.jp/>)

皆様が Microsoft Azure の恩恵を受け、最大限に活用できるよう、支援することをミッションとした企業です。24/365 の運用監視や、各種コンサルティング、開発支援を行っています。

Azure の 2008 年レビュー時から、Azure 事業に取り組んでおり、Windows, Linux ともに日本 TOP のノウハウと実績を持ちます。Microsoft Azure MVP 経験者が 4 名在籍しており、Microsoft 本社へフィードバックや情報交換も頻繁に行うとともに、変化の速いクラウド業界において最新のノウハウを提供します。お困りの点がありましたら、ぜひご相談ください。本書に対する感想や、ご意見もお待ちしています。



安心、安全の運用監視
24時間365日 Microsoft Azure を監視



ノウハウに基づく、最適なプラン、構成を提案
Microsoftテクノロジに限らず、Linux/OSSの実績も豊富



Microsoft Azureスペシャリストによるサービス提供
Microsoft Azure MVP経験者4名 + 経験豊富なメンバー



初回アセスメント無料
ちょっとしたわからないことも、まずはご相談ください