FUJITSU Server PRIMERGY
FUJITSU Server PRIMEQUEST

Windows Server 2016/2019/2022
DHCP、DNS 構築・運用ガイド

第 1.2 版

2022 年 3 月

富士通株式会社

はじめに

クライアントへ動的に IP アドレスを割り当てる「DHCP」と、コンピューター名と IP アドレスの名前解決を行う「DNS」は、Windows のネットワーク基盤を構築する上で重要な機能です。本書は、FUJITSU Server PRIMERGY および FUJITSU Server PRIMEQUEST において、Windows Server 2016/2019/2022 標準搭載の DHCP/DNS の概要と、構築手順を中心に紹介します。

Windows Server 2016 の新機能および削除された機能は以下のとおりです。

DHCP の新機能	説明
DHCP サブネットの選択オプション	新しい DHCP オプションとして「オプション 118」と「オプション 82(サブオプション 5)」がサポートされるようになりました。
DHCP サーバーによる DNS 登録エラーの新しいイベント	DHCP サーバーの DNS レコードの登録失敗イベントが含まれるようになりました。
削除された DHCP の機能	説明
DHCP NAP 機能	DHCP NAP 機能は、Windows Server 2016 で非サポートとなりました。
DNS の新機能	説明
DNS ポリシー	アプリケーションやクライアントロケーション、時間によって DNS クエリの応答を変更することができます。詳細は「2.1.5DNS ポリシー」を参照してください。
応答率の制限	DNS サーバーで応答率の制限を有効にすることができるようになりました。 詳細は「2.2.3 応答率の制限 (Response Rate Limiting)」を参照してください。
名前付きエンティティ（DANE）の DNS ベース認証	TLSA (トランスポート層セキュリティ認証) レコードを使用して、証明書の発行元の証明機関 (CA) がドメイン名に対して要求する情報を DNS クライアントに提供できるようになりました。
Unknown レコードのサポート	Windows DNS サーバーで Unknown レコードを追加できるようになりました。
IPv6 のルートヒント	IANA によって発行された IPv6 ルートヒントが Windows DNS サーバーで使用できるようになりました。

Windows PowerShell コマンドレット	DNS サーバーで新しい Windows PowerShell コマンドレットの使用が可能となりました。 詳細は「2.1.6Windows PowerShell のサポート」を参照してください。

Windows Server 2019 の新機能および削除された機能はありません。

Windows Server 2022 の新機能は以下のとおりです。

DNS の新機能	説明
セキュリティで保護された DNS	Windows Server 2022 の DNS クライアントで、DNS over HTTPS で暗号化された DNS 名前解決要求がサポートされます。 DNS over HTTPS に対応した DNS サーバーを指定することで、通信中の DNS データの暗号化ができるようになりました。詳細は「付録 9：DNS over HTTPS を使用する方法」を参照してください。 ※Windows Server の DNS サーバーは、DNS over HTTPS に未対応です。

本書に記載している内容

- DHCP/DNS は、IPv4/IPv6 両方のプロトコルに完全対応しています。本書では、IPv4/IPv6 の環境に該当する記載箇所に、以下のアイコンを表示しています。

：IPv4 環境に該当する記載

：IPv6 環境に該当する記載

- DHCP/DNS の構築について、PRIMERGY を使用して説明していますが、PRIMEQUEST シリーズでも共通です。

本書の目的

本書を読むことで、以下のことが理解できることを目的としています。

- Windows Server 2016/2019/2022 の DHCP/DNS の概要と構築手順
- Windows Server 2016/2019/2022 の IPv6 対応

本書を利用するにあたっての前提知識

本書は、DHCP/DNS の導入を行う予定の SE の方を対象としています。また、以下の技術情報についての知識が必要となります。

- Windows ネットワークに関する基本的な知識

参考資料

本書以外の Windows Server 技術情報は、以下のサイトで公開しています。

・Windows システム構築ガイド
https://jp.fujitsu.com/platform/server/primergy/technical/construct/

略称表記

本書では、以下の略称を使用しています。

	正式名称	略称
製品名	Microsoft® Windows Server® 2022	Windows Server 2022
	Microsoft® Windows Server® 2019	Windows Server 2019
	Microsoft® Windows Server® 2016	Windows Server 2016
機能名	Dynamic Host Configuration Protocol	DHCP
	Domain Name System	DNS

注意事項

本ドキュメントを輸出または第三者へ提供する場合は、お客様が居住する国及び米国輸出管理関連法規等の規制をご確認の上、必要な手続きをお取りください。

改版履歴

改版日時	版数	改版内容
2020.08	1.0	・新規作成
2022.02	1.1	・Windows Server 2022 に関する記述を追記
2022.03	1.2	・マルチホームコンピューターに関する記述を更新

目次

図表目次

1. DHCP サーバー

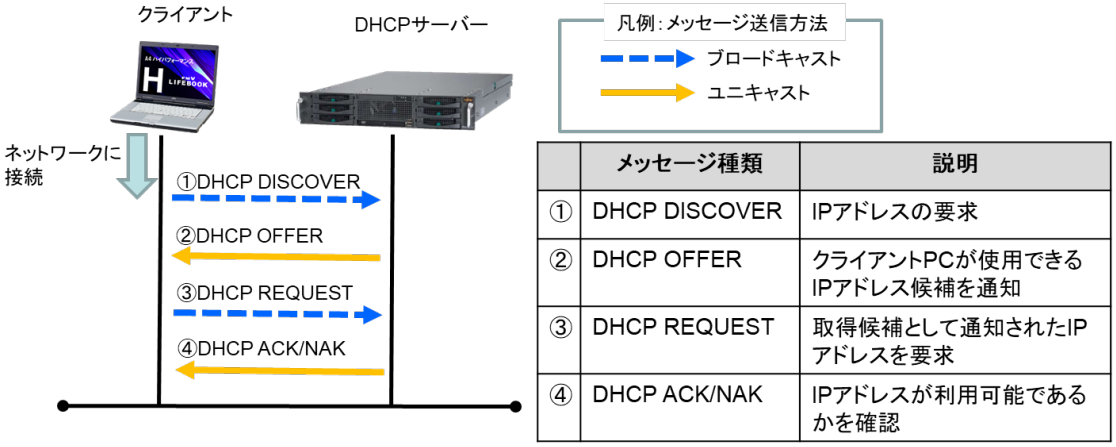
DHCP とは、ネットワーク上にあるコンピューターへ動的に IP アドレスを割り当てる機能です。コンピューターをネットワークに接続するだけで適切な IP アドレスが自動構成されるため、ネットワークの知識を持たないユーザーでも他のコンピューターと通信を開始できます。また、IP アドレス以外にも、ネットワーク情報をコンピューターに自動的に割り当てることができます。
コンピューターを持ち運び複数拠点で利用することが多いお客様や、IP アドレスの管理を最小限に抑えたい場合に特に有効な機能です。

1.1. DHCP の動作概要

DHCP サーバーから IP アドレスを自動取得するためには、DHCP サーバーや IP アドレスを取得するクライアントの設定が必要です。本節では、DHCP の基本的な機能や動作について紹介します。

1.1.1. DHCP の動作イメージ

DHCP サーバーから IP アドレスを自動取得するためには、クライアントのインターネットプロトコルのプロパティで「IP アドレスを自動的に取得する」が選択されている必要があります。このように設定されている場合、クライアントはネットワーク接続時に IP アドレスを要求します。DHCP サーバーがネットワーク上に存在する場合、この要求に応えて IP アドレスをクライアントに付与します（IP アドレス取得までの動作は図 1.1.1.1 IP アドレス取得までの動作を参照）。
DHCP サーバーによって付与された IP アドレスにはリース期限（既定では 8 日間）が設定されており、この期限内であれば DHCP サーバーから再度 IP アドレスを取得せずに同じ IP アドレスを使用できます。



	メッセージ種類	説明
①	DHCP DISCOVER	IPアドレスの要求
②	DHCP OFFER	クライアントPCが使用できるIPアドレス候補を通知
③	DHCP REQUEST	取得候補として通知されたIPアドレスを要求
④	DHCP ACK/NAK	IPアドレスが利用可能であるかを確認

図 1.1.1.1 IP アドレス取得までの動作

IP アドレスが利用可能な場合、DHCP サーバーは「DHCP ACK」メッセージをクライアントに返します。利用不可の場合「DHCP NAK」メッセージをクライアントに返します。この場合、クライアントは再度①の「DHCP DISCOVER」メッセージをブロードキャストで送信して IP アドレスの取得を再度試みます。

1.1.2. DHCP サーバーでの IP アドレス管理

DHCP サーバーでは、ネットワークセグメントごとに「スコープ」と呼ばれる IP アドレスの配布範囲を設定します。DHCP サーバーはスコープに設定された IP アドレスをクライアントへ順次リースします。また、スコープでは DNS サーバー、ルーターの IP アドレスやドメイン名など様々なネットワーク情報を「スコープオプション」として設定でき、IP アドレスと同時にクライアントへ配布できます。
クライアントでは、接続したセグメントに対応する DHCP サーバーのスコープ情報を基に各種ネットワーク情報が設定されます。IPv4 環境におけるスコープの設定例を図 1.1.2.1 に紹介します。

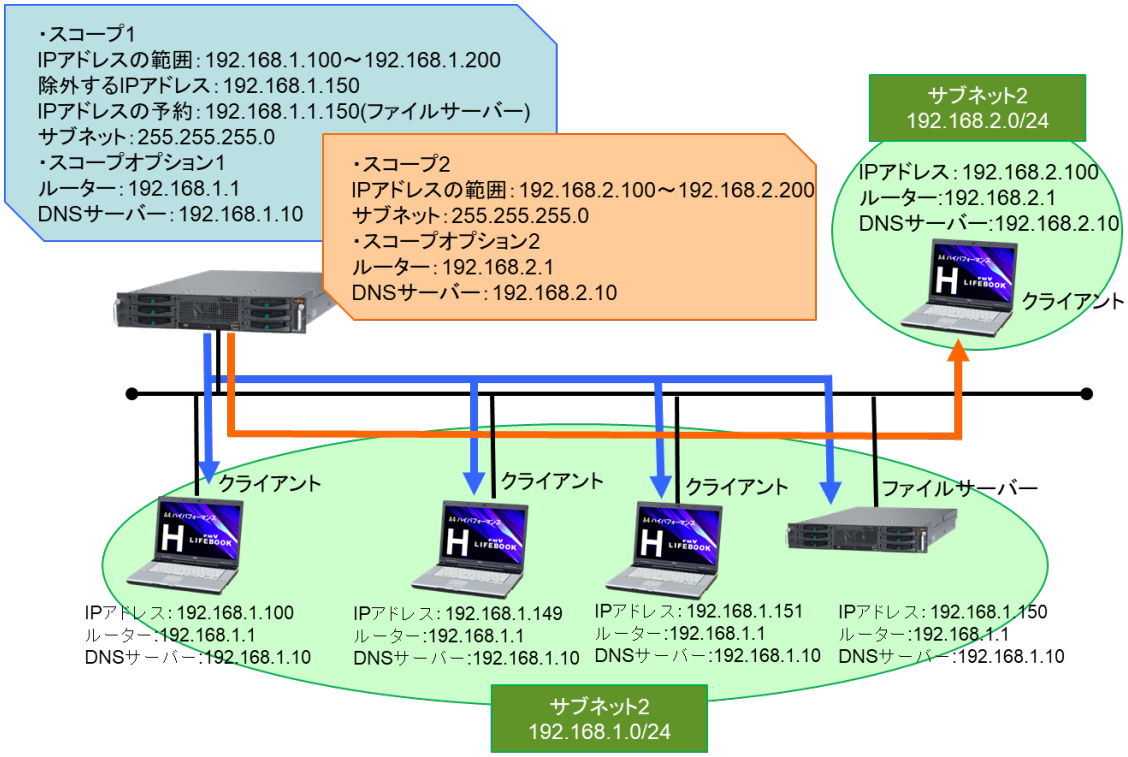


図 1.1.2.1 スコープの設定例

スコープでは、まず IP アドレスの配布対象とするサブネットの IP アドレス範囲を指定します。ここで設定した IP アドレスの一部を「除外する IP アドレス」として配布対象外に設定することも可能です。また、サーバー機（図 1.1.2.1 ではファイルサーバー）など固定で IP アドレスの付与が必要な場合は、IP アドレスをあらかじめ DHCP サーバーに登録（IP アドレスの予約(※)）することで、同じコンピューターに固定 IP アドレスを配布できます。スコープオプションとして「ルーターの IP アドレス」、「DNS サーバーの IP アドレス」を設定して、クライアントにネットワーク情報を設定しています。

（※）IPv6 環境における IP アドレス予約については、「付録 1：DHCPv6 におけるアドレス予約」を参照してください。

1.1.3. ポリシーベースの IP アドレス割り当て

ポリシーベースの IP アドレス割り当て機能を利用すると、DHCP サーバーは、ポリシーに定義された条件（MAC アドレスのプレフィックスなど）に一致するクライアントに対して、スコープで指定された範囲に含まれる IP アドレスと、DHCP オプション（DNS サーバーやルーターなどの IP アドレス）を割り当てます。
ポリシーには、DHCP サーバーに設定するポリシー（サーバーレベル）と、スコープに設定するポリシー（スコープレベル）の 2 種類あります。スコープレベルのポリシーは、設定したスコープに対してのみ適用されますが、サーバーレベルのポリシーは、サーバーが管理する全スコープに対して適用されます。
サーバーレベルとスコープレベルのどちらも設定されている場合、重複する DHCP オプションが設定されていると、スコープレベルの設定が有効になります。また、複数のポリシーを適用する場合は、サーバーレベル内およびスコープレベル内で優先順位を付けることもできます。

以下に、MAC アドレスのプレフィックスに基づいて定義したポリシーの適用例を示します。
例）MAC アドレスのプレフィックスが「4C:52:62:4D:31:*」であるクライアントのみ、DNS サーバーを「192.168.1.5」に設定する。

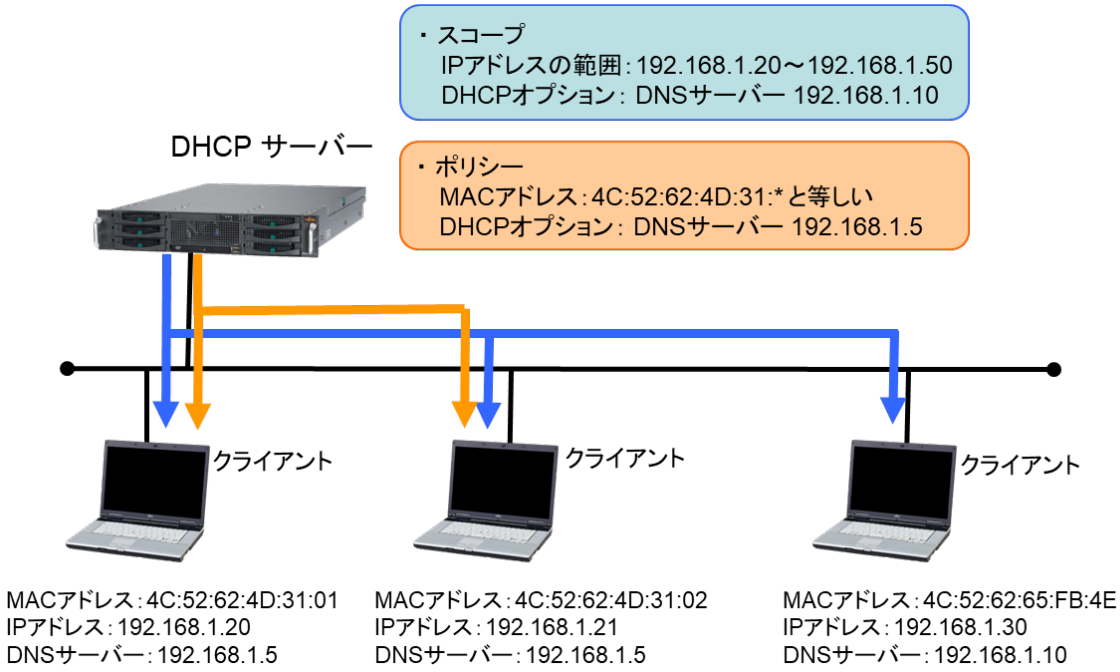


図 1.1.3.1 ポリシーベースの IP アドレス割り当て例

1.1.4. IP アドレス自動構成

IPv6 アドレスの自動構成には、以下の 2 つがあります。

- ステートレスアドレス自動構成
- ステートフルアドレス自動構成

ステートレスアドレス自動構成とステートフルアドレス自動構成の大きな違いは、IP アドレスの管理をどこで行うかです。ステートフルアドレス自動構成は、IPv4 環境と同様に DHCP サーバーで IP アドレス管理を行いますが、ステートレスアドレス自動構成では DHCP サーバーではなくルーターで管理を行います。なお、ルーター側でもステートレス/ステートフルの設定(ルーターアドバタイズの設定)が必要です。ルーターアドバタイズについては「付録 2：ルーターアドバタイズに関する補足」を参照してください。

(1) ステートレスアドレス自動構成

ルーターがステートレスアドレス自動構成を指示している場合、DHCP サーバーはアドレスをリースしません。つまり DHCP サーバーはアドレスの管理を行いません。

ステートレスアドレス自動構成ではアドレスプレフィックスをルーターが提供します。クライアントはアドレスプレフィックスと自身のインターフェイス識別子を組み合わせたアドレスを構成します。その際に、DHCP サーバーに設定されたサーバーオプションから、ネットワーク構成情報をクライアントに割り当て可能です。

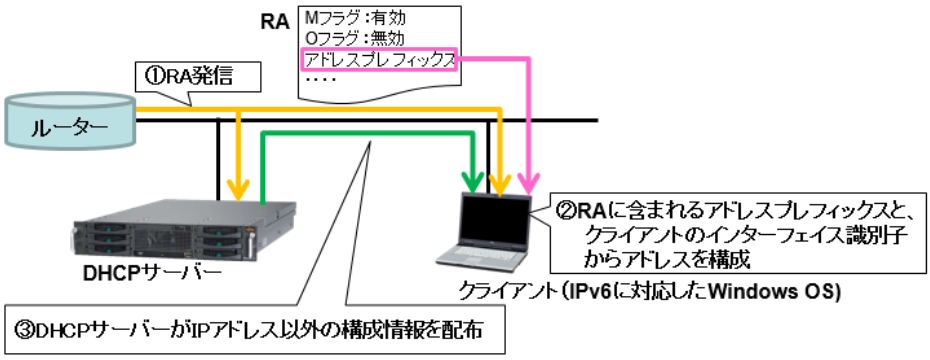


図 1.1.4.1 ステートレスアドレス自動構成のイメージ

(2) ステートフルアドレス自動構成

ルーターがステートフルアドレス自動構成を指示している場合、DHCP サーバーは従来の DHCP サーバー同様にスコープを使ってアドレスを管理します。また、その他のネットワーク構成情報も DHCP サーバーが管理します。ルーターはアドレスの構成には関与しません。

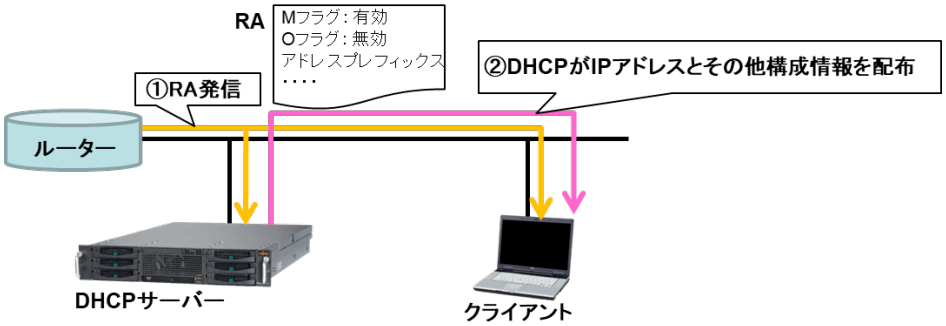


図 1.1.4.2 ステートフルアドレス自動構成のイメージ

1.2. その他の DHCP 機能

1.2.1. DHCP サーバーによる DNS 動的登録の代行

DHCP サーバーは IP アドレスを配布する際、クライアントの代わりに DNS サーバーへの動的登録が可能です。Windows 2000 以降のクライアントでは DNS サーバーへの動的登録機能が実装されているので、DHCP サーバーに DNS 動的登録を代行させる必要はありません。

DNS 動的登録機能を持たないクライアントは、DHCP サーバーによる DNS 動的登録の代行機能を利用することで DNS 動的登録を行うことができます。
DHCP サーバーによる DNS 動的登録は、以下の契機で行われます。

- クライアントにおける IP アドレスの追加・更新・削除
- リースの変更・更新による IP アドレス更新
- DNS サーバーへのレコードの登録依頼（ipconfig /registerdns コマンド）
- クライアント/サーバーの電源がオン
- メンバーサーバーがドメインコントローラに昇格

1.2.2. DHCP リレーエージェント機能

DHCP リレーエージェント機能を使用すると、別セグメントに存在する DHCP サーバーから IP アドレスのリースを受けることができます。各セグメントに DHCP サーバーを設置する必要がなく、アドレス配布の集中管理が可能なため、管理コストの削減が期待できます。

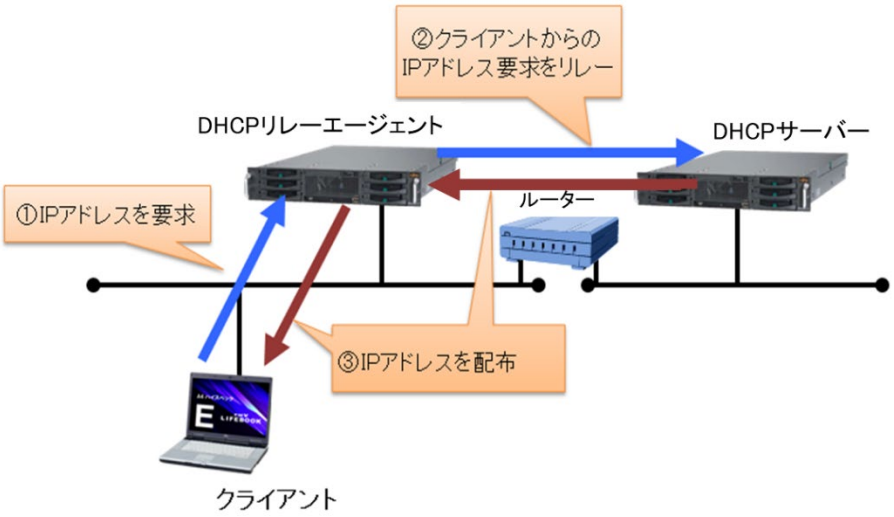


図 1.2.2.1 DHCP リレーエージェントのイメージ

1.2.3. DHCP サーバーの冗長化

DHCP サーバーを冗長化する方法は以下のとおりです。

(1) DHCP フェールオーバー

DHCP フェールオーバーは、プライマリサーバー/パートナーサーバーと呼ばれる 2 台の DHCP サーバーが、同じサブネットに対して DHCP サービスの継続的な可用性を実現する機能です。
DHCP フェールオーバーには、オプション設定として、以下の 2 つのモードがあります。

・ ホットスタンバイモード

ホットスタンバイモードを設定すると、2 台の DHCP サーバーはリース情報を同期します。プライマリサーバーが使用できなくなった場合、パートナーサーバーがサブネット内のクライアントに対するサービスを担います。
ホットスタンバイモードは、同じサブネット内で DHCP サーバーを冗長化するだけでなく、パートナーサーバーを共用することで、異なるサブネットに配置された DHCP サーバーを冗長化することもできます。すなわち、複数のサブネットに配置したそれぞれのプライマリサーバーに対して、ペアとなるパートナーサーバーを 1 台配置します(図 1.2.3.1)。

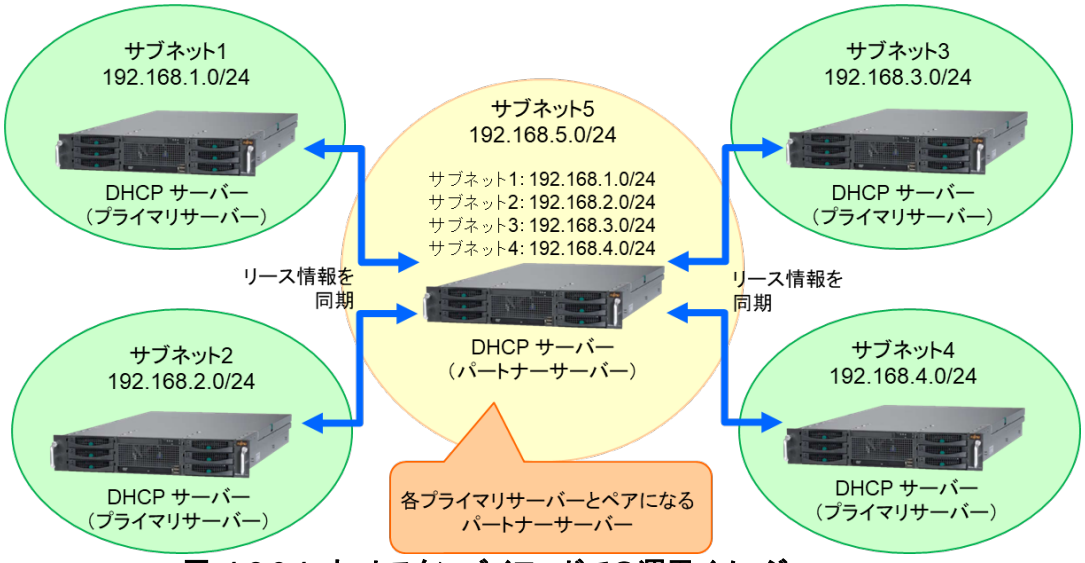


図 1.2.3.1 ホットスタンバイモードでの運用イメージ

従来は、クラスタ化した DHCP サーバーを設置する場合、サブネット毎に運用ノード、待機ノードが必要でしたが、ホットスタンバイモードを設定すれば、パートナーサーバー（従来の待機ノード）を1台だけ配置する構成になるため、より少ないサーバー台数で IP アドレスリース機能を冗長化できます。この構成は、パートナーサーバーを中心に複数サブネットの IP アドレスを取り扱えるため、IP アドレスの一括管理に適しています。
なお、複数台のプライマリサーバーが停止した場合、停止したプライマリサーバーの機能分をパートナーサーバーが担うことで、パートナーサーバーの負荷が高くなる可能性がありますが、全てのサブネットにおける DHCP サービスを継続できます。

・ 負荷分散モード

負荷分散モードを設定すると、2 台の DHCP サーバーは、ユーザーが設定した比率に基づきクライアントからの要求を分散して処理します。例えば、DHCP サーバーの性能が異なる場合、処理能力の比率を考慮して、一方の DHCP サーバーに 70%の処理を、もう一方の DHCP サーバーに 30%の処理を行うように設定します(図 1.2.3.2)。

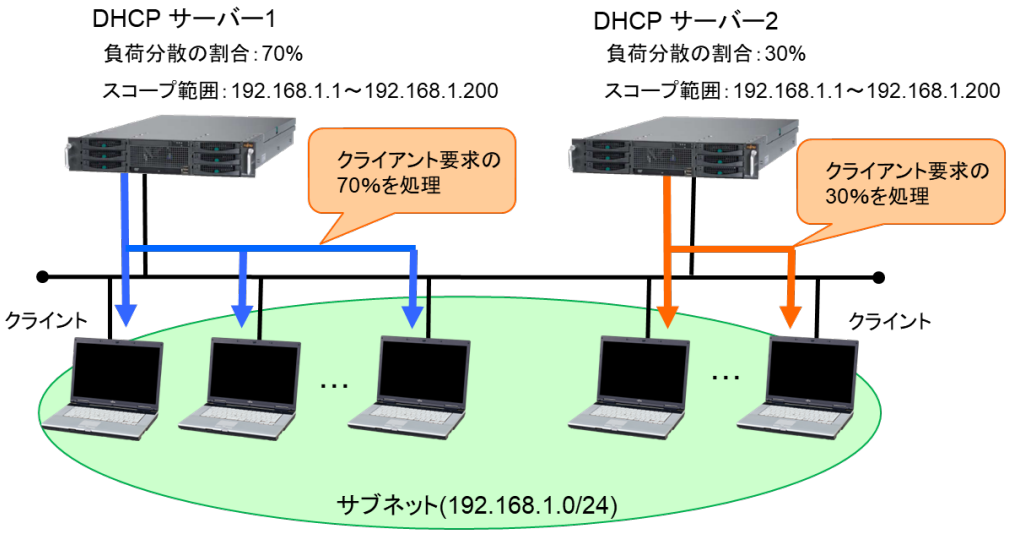


図 1.2.3.2 負荷分散モードでの運用イメージ

(2) 分割スコープ

2 台の DHCP サーバーで、同じサブネットを管理することで冗長化と負荷分散を実現する方法です。

2 台の DHCP サーバーで同じサブネットのアドレスのスコープ範囲を分散する場合、一般的にアドレスの 80%を一方の DHCP サーバーで配布して、残りの 20%をもう一方の DHCP サーバーで配布する手法がとられます。その際、リースする IP アドレスの重複を避けるため、アドレスプール範囲が被らないように各サーバーを構成します。

分割スコープは、同じサブネットのスコープ範囲を 2 台に分けて設定するため、一方の DHCP サーバーが停止して IP アドレスリースが切れると、もう一方の DHCP サーバーから異なる IP アドレスがリースされます。この際、例えば 100 個の IP アドレスを 80%, 20%で分割していた場合に、80%側の DHCP サーバーが停止すると、20%側の DHCP サーバーが配布する 20 個の IP アドレスのみが利用可能となります。このため、100 台のクライアントが存在すると、80 台のクライアントは IP アドレスが割り当たらないことになります。

同様な環境(100 個の IP アドレス、100 台のクライアント)において、負荷分散モードを設定した DHCP サーバーでは、2 台が同じスコープ範囲の IP アドレスをリースするため、一方が停止してもすべてのクライアントに IP アドレスが割り当たります。

IPv4 スコープに対応した分割スコープを簡単に設定するためのウィザード（DHCP 分割スコープ構成ウィザード）で設定が可能です。

(3) DHCP サーバーのクラスタ化

DHCP をホストするサーバーをクラスタ構成とすることで冗長化可能です。

1.3. DHCP サーバーの構築

DHCP サーバーは、DHCPv6 をサポートしており、IPv4/IPv6 クライアントに対して同時に動的なアドレスを配布するようサービスを展開できます。なお、DHCP 機能は、サーバーマネージャーの「役割と機能の追加」よりインストール可能です。

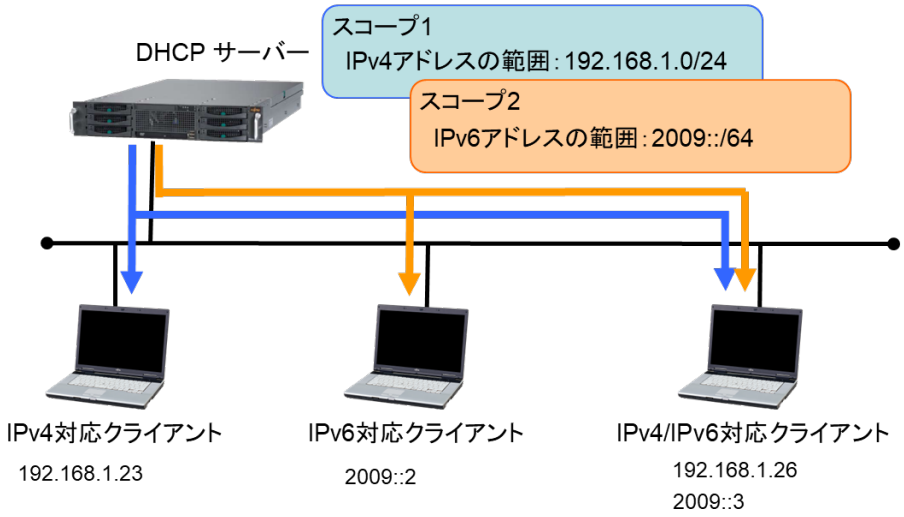


図 1.3.1 DHCP サーバーのサービス展開イメージ

DHCP サーバーを構成する場合の流れは、図 1.3.2 のとおりです。
IPv6 環境における DHCP サーバーの構成方法には、ステートレスアドレス自動構成とステートフルアドレス自動構成の 2 種類があります。構築手順の詳細は、各節を参照してください。
なお、DHCP サーバーの役割を追加するコンピューターは、静的な IP アドレスを使用する必要があります。

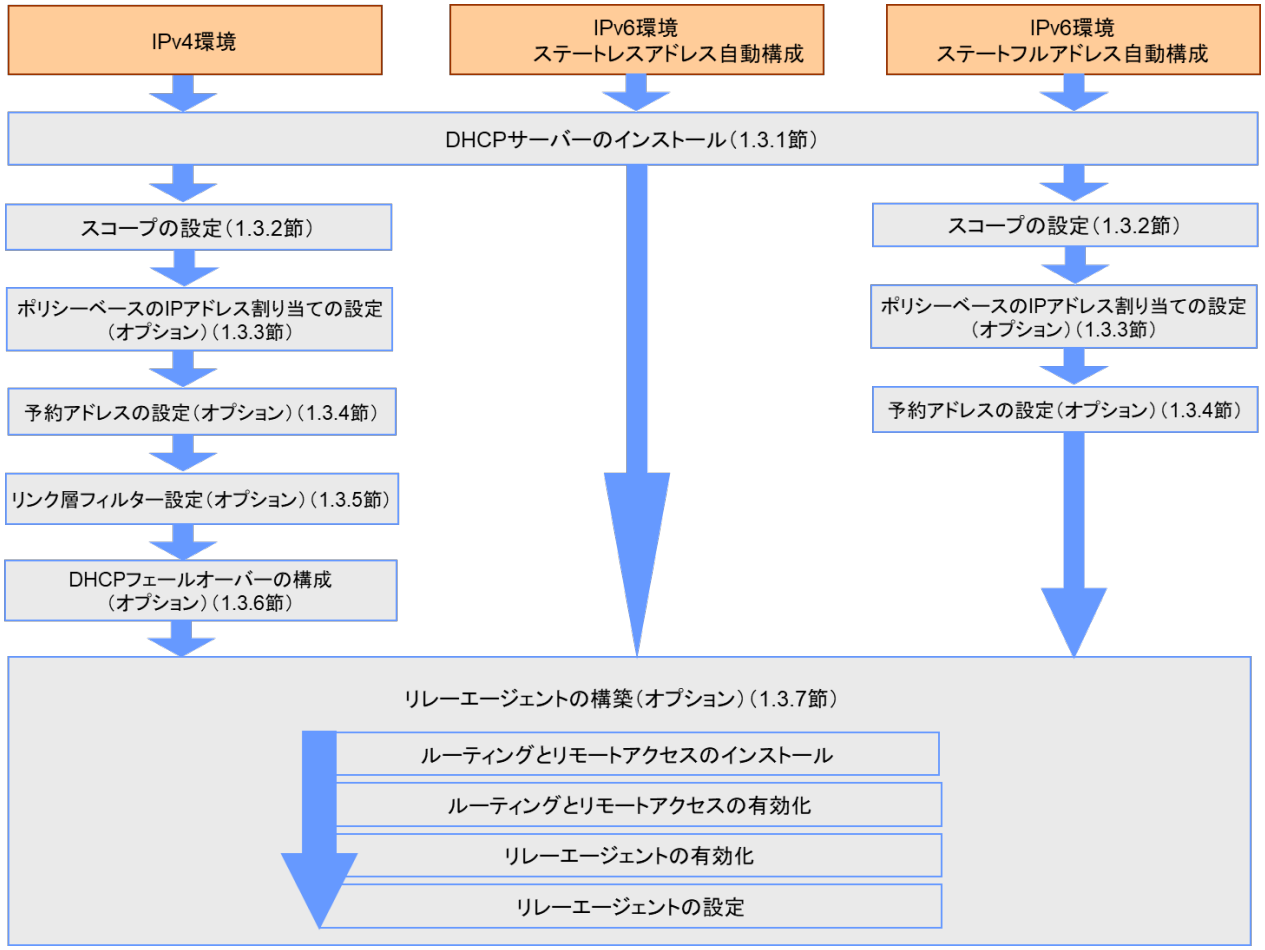
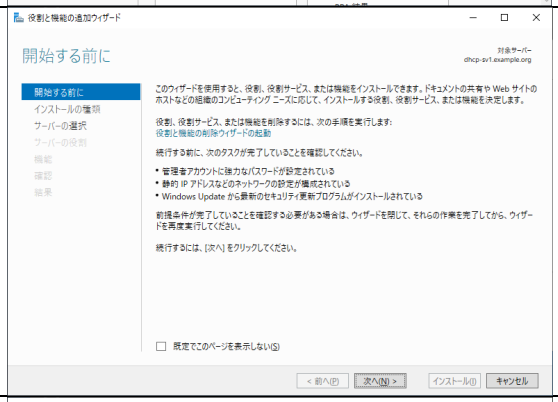
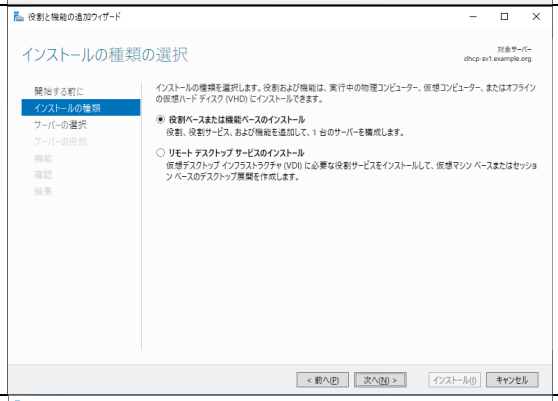
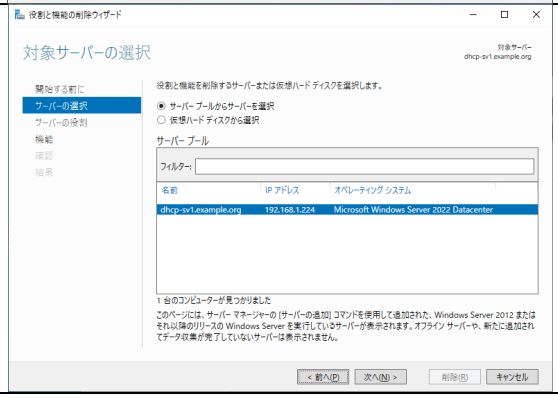
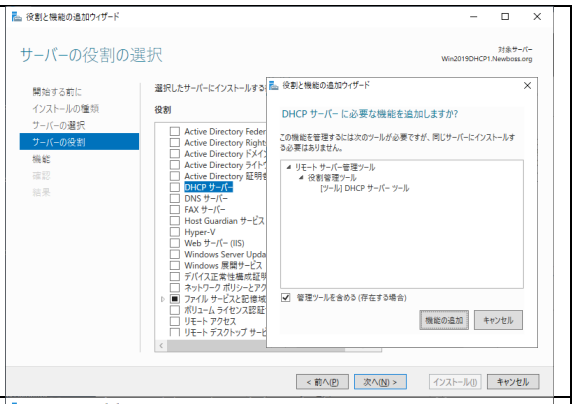
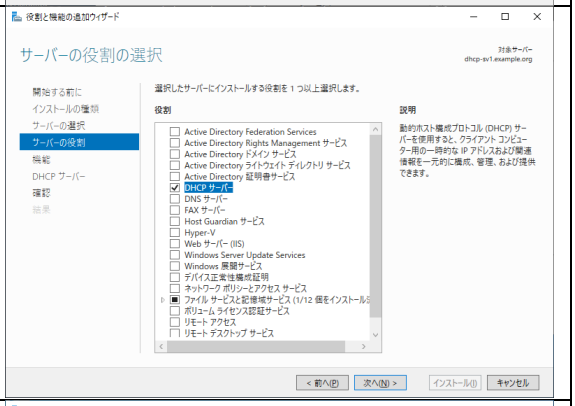
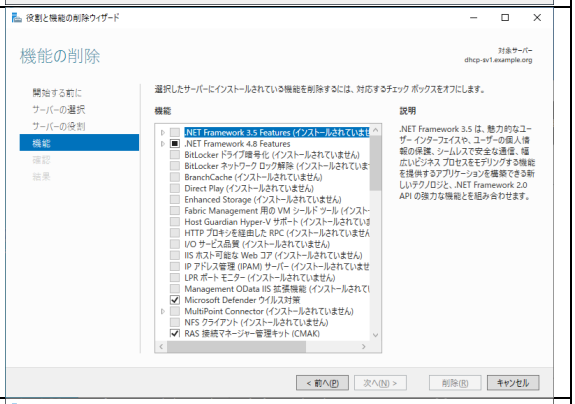
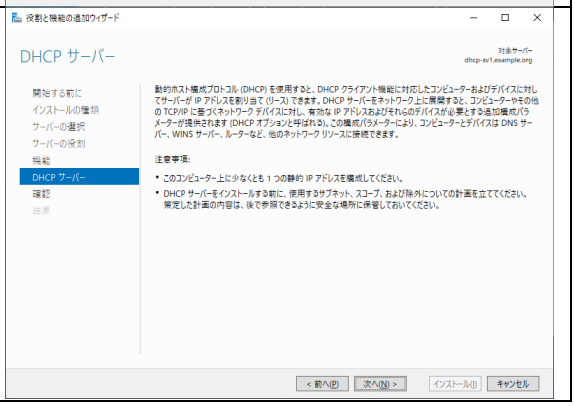


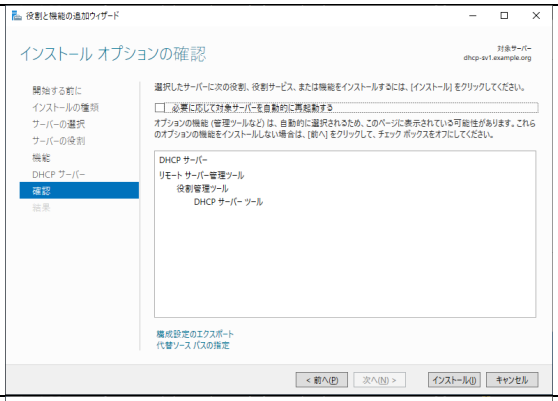
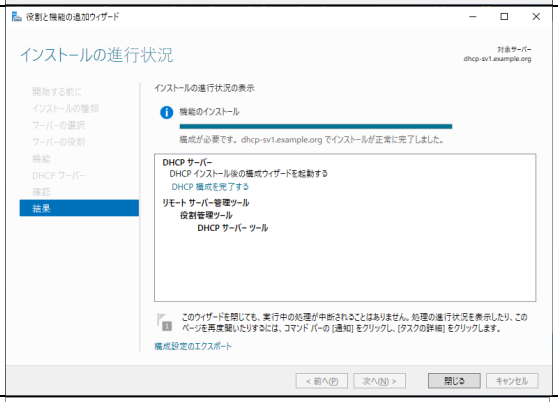
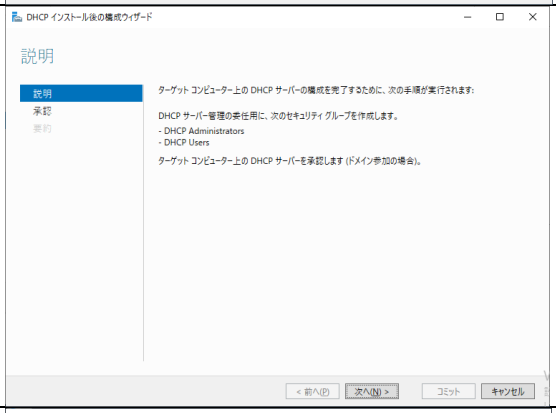
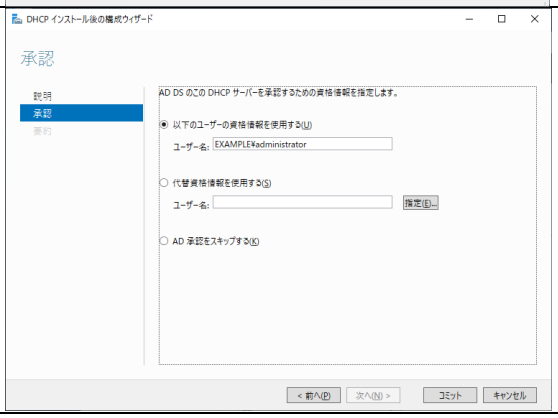
図 1.3.2 DHCP サーバー構築の流れ

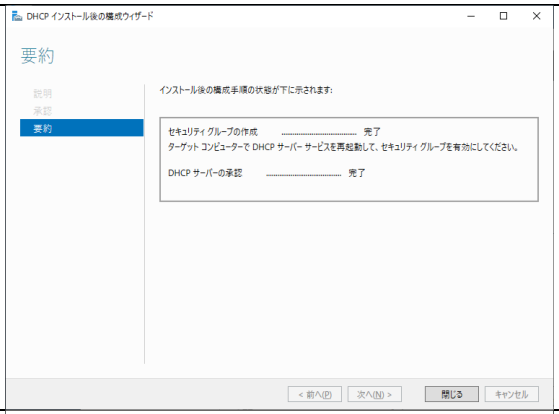
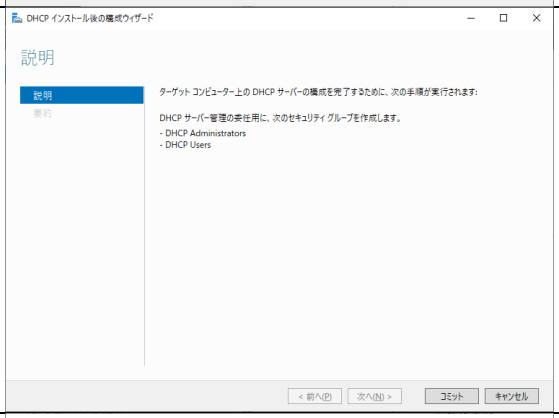
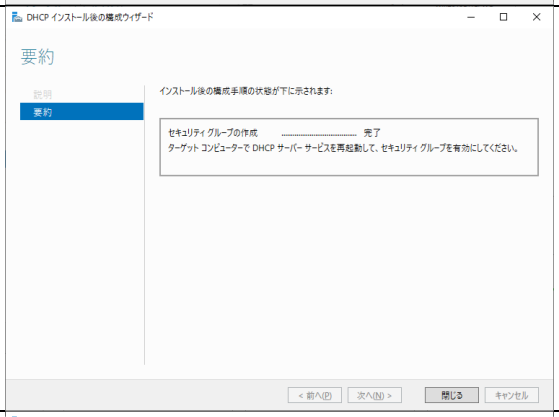
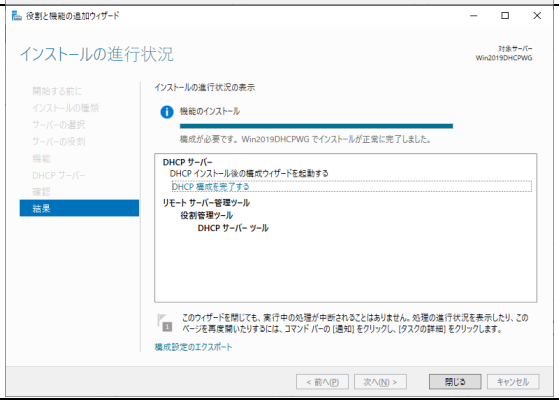
1.3.1. DHCP サーバーのインストール 

以下の手順に従い、DHCP サーバーをインストールします。

1	[サーバーマネージャー]の[役割と機能の追加]をクリックします。	
2	[役割と機能の追加ウィザード]が起動して、[開始する前に]が表示されます。 [次へ]をクリックします。	
3	[インストールの種類の選択]が表示されます。 [役割ベースまたは機能ベースのインストール]を選択します。 [次へ]をクリックします。	
4	[対象サーバーの選択]が表示されます。 必要に応じてインストール先を選択します。 [次へ]をクリックします。	

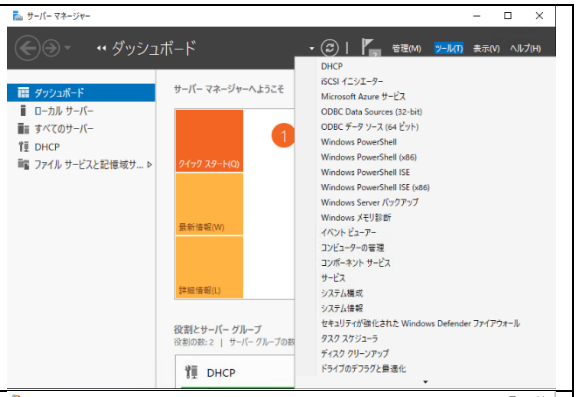
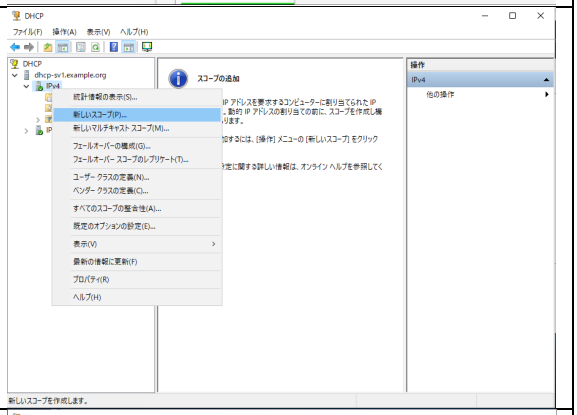
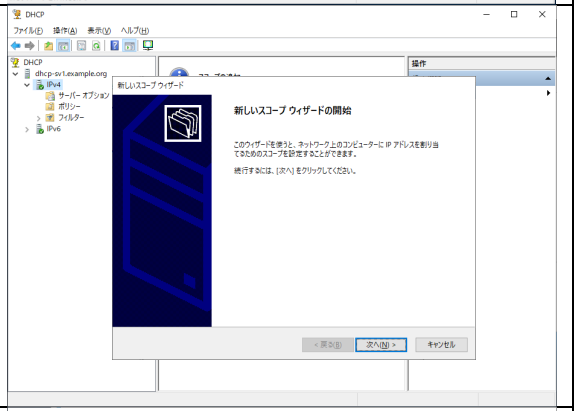
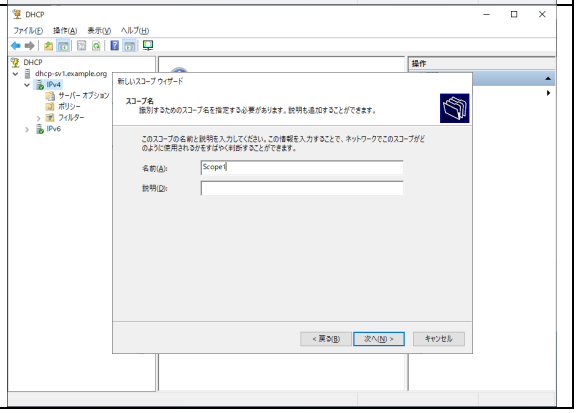
5	[サーバーの役割の選択]が表示されます。 [DHCP サーバー]をチェックすると確認画面が開きます。 [機能の追加]をクリックします。	
6	[サーバーの役割の選択]に戻ります。 [次へ]をクリックします。	
7	[機能の選択]が表示されます。 [次へ]をクリックします	
8	[DHCP サーバー]が表示されます。 [次へ]をクリックします。	

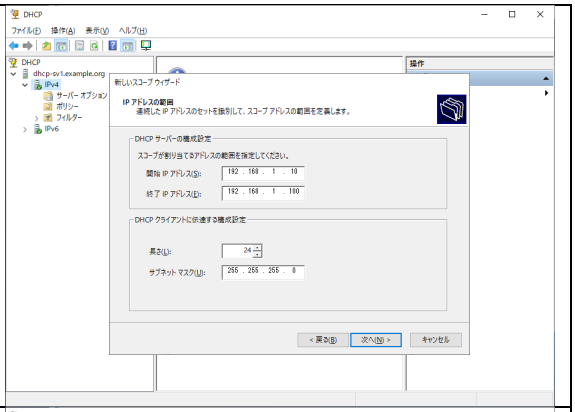
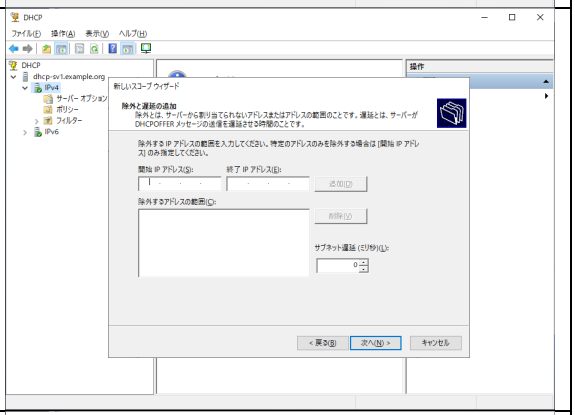
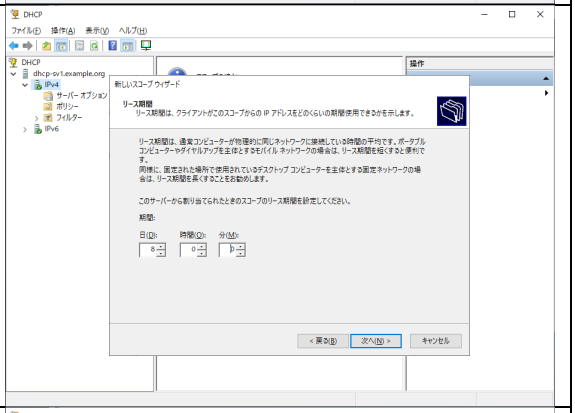
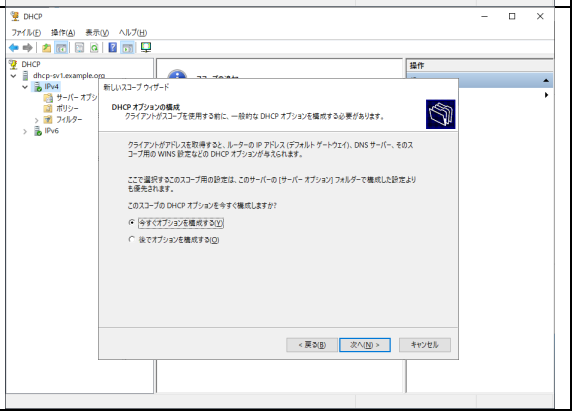
9	[インストール オプションの確認]が表示されます。 [インストール]をクリックします。	
10	[インストールの進行状況]が表示されます。 インストールが完了したら、中央の囲みの中に表示される[DHCP 構成を完了する]をクリックします。 このあとの手順は、ドメインメンバーの場合とスタンドアローンの場合とで異なります。先にドメインメンバーの場合を説明します。	
11	ドメインメンバーの場合(1/3) [DHCP インストール後の構成ウィザード]が起動して、[説明]が表示されます。 [次へ]をクリックします。	
12	ドメインメンバーの場合(2/3) [承認]が表示されます。 DHCP サーバーの承認に使用する資格情報を確認します。 [コミット] をクリックします。	

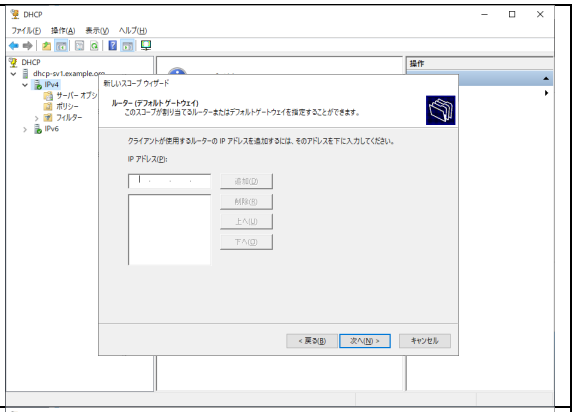
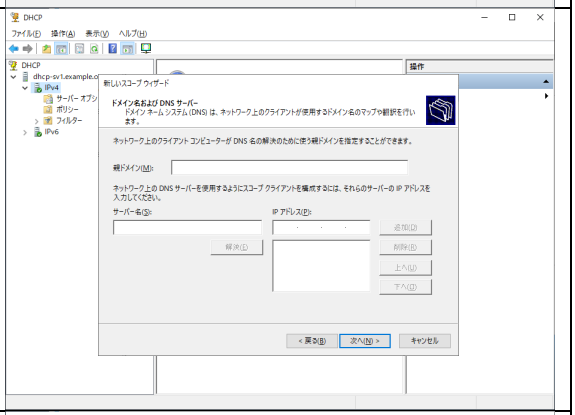
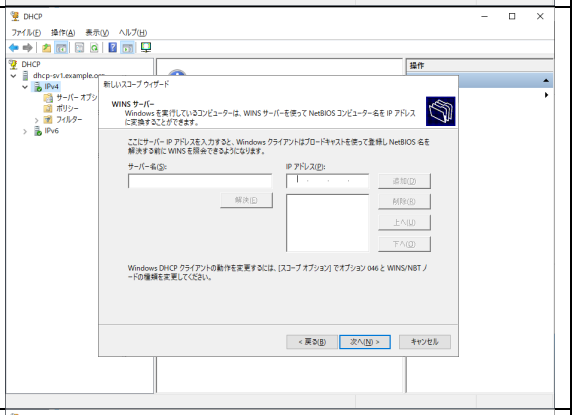
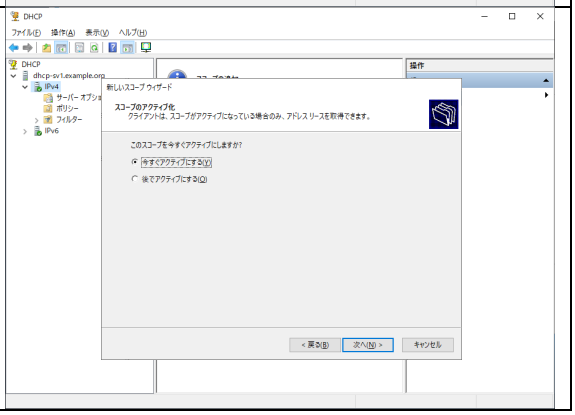
13	ドメインメンバーの場合(3/3) [要約]が表示されます。 [閉じる]をクリックします。	
14	スタンドアローンの場合(1/2) [DHCP インストール後の構成ウィザード]が起動して、[説明]が表示されます。 [コミット]をクリックします。	
15	スタンドアローンの場合(2/2) [要約]が表示されます。 [閉じる]をクリックします。	
16	[インストールの進行状況]に戻ります。 [閉じる]をクリックします。 構成したセキュリティグループを有効にするため、DHCP サーバー サービスを再起動してください。	

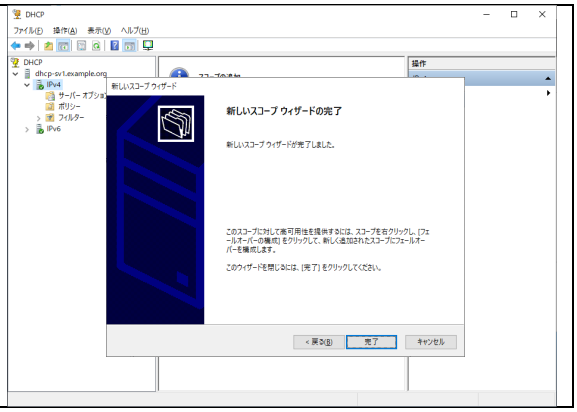
1.3.2. スコープの設定 

スコープの設定は、IPv4 環境、または IPv6 環境のステートフルアドレス自動構成の場合に設定してください。以下は IPv4 のスコープ設定手順です。IPv6 のスコープ設定については、手順の最後に記載している補足を参照してください。
スコープの設定は DHCP コンソールから行います。

1	[サーバー マネージャー]の[ツール]メニューから[DHCP]をクリックします。	
2	DHCP コンソールが起動します。 [DHCP]-[(サーバー名)]-[IPv4]を右クリックして、[新しいスコープ]をクリックします。	
3	[新しいスコープウィザード]が起動して、[新しいスコープウィザードの開始]が表示されます。 [次へ] をクリックします。	
4	[スコープ名]が表示されます。 [名前]にスコープ名を入力します。 [次へ]をクリックします。	

5	[IP アドレスの範囲]が表示されます。 [開始 IP アドレス]と[終了 IP アドレス]に、スコープに設定する IP アドレスを入力します。 [次へ]をクリックします。	
6	[除外と遅延の追加]が表示されます。 スコープに設定した IP アドレスの配布範囲から、一部の IP アドレスの配布を除外する場合は[開始 IP アドレス]と[終了 IP アドレス]を設定します。 [次へ]をクリックします。	
7	[リース期間]が表示されます。 必要に応じて IP アドレスのリース期間を設定します。 [次へ]をクリックします。	
8	[DHCP オプションの構成]が表示されます。 [今すぐオプションを構成する]を選択します。 [次へ]をクリックします。	

9	[ルーター(デフォルトゲートウェイ)]が表示されます。 ルーター(デフォルトゲートウェイ)の情報を DHCP サーバーで配布する場合は設定します。 [次へ]をクリックします。	
10	[ドメイン名および DNS サーバー]が表示されます。 DNS サーバーの情報を DHCP サーバーで配布する場合は設定します。 [次へ]をクリックします。	
11	[WINS サーバー]が表示されます。 WINS サーバーの情報を DHCP サーバーで配布する場合は設定します。 [次へ]をクリックします。	
12	[スコープのアクティブ化]が表示されます。 [今すぐアクティブにする]を選択します。 [次へ]をクリックします。	

13	[新しいスコープ ウィザードの完了]が表示されます。 [完了]をクリックします。	

補足：IPv6 のスコープ設定

IPv6 のスコープ設定は、手順 2 の[IPv4]を[IPv6]に置き換えた手順で開始する「新しいスコープウィザード」から行います。「新しいスコープウィザード」では以下の情報を入力します。

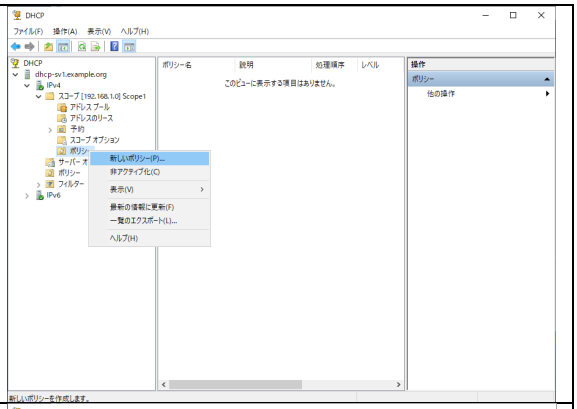
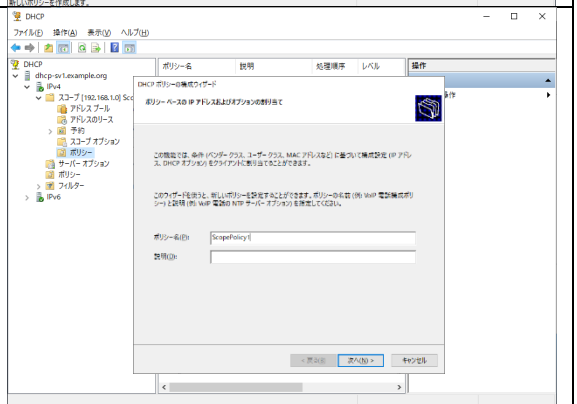
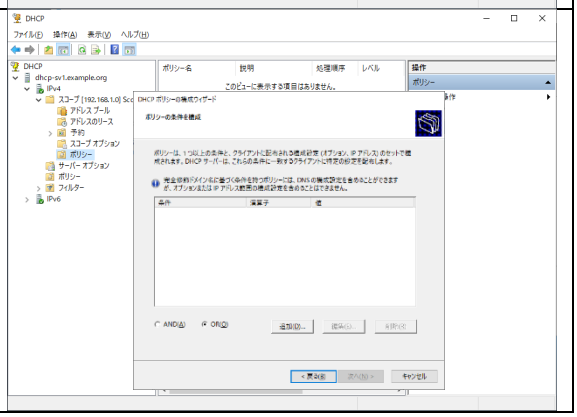
- スコーププレフィックス
- 除外の追加
- スコープリース

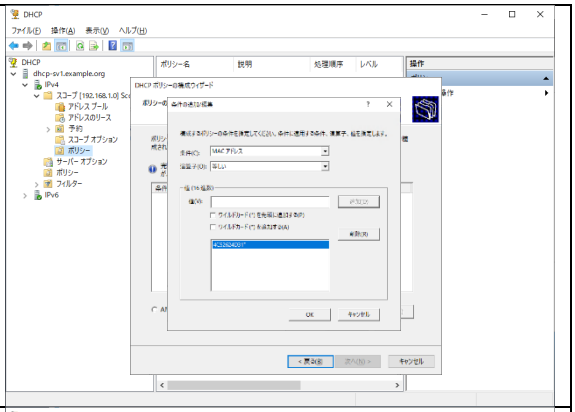
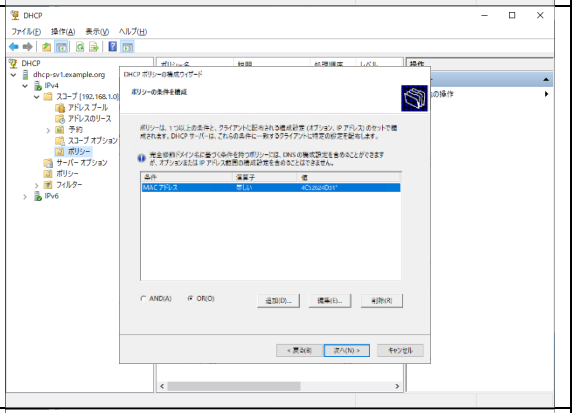
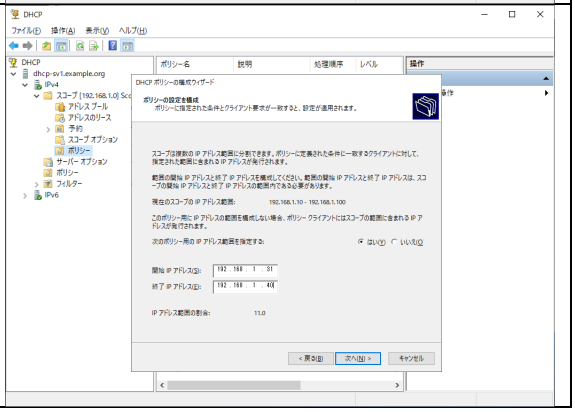
1.3.3. ポリシーベースの IP アドレス割り当ての設定

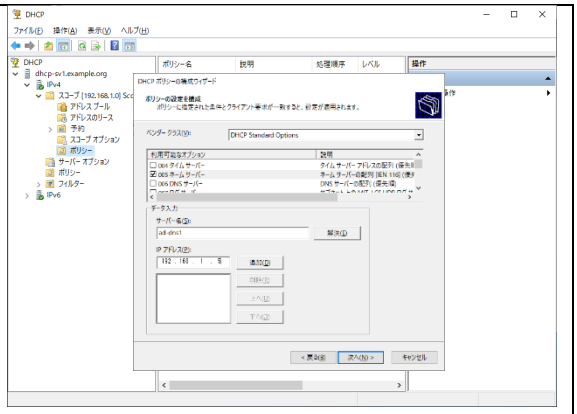
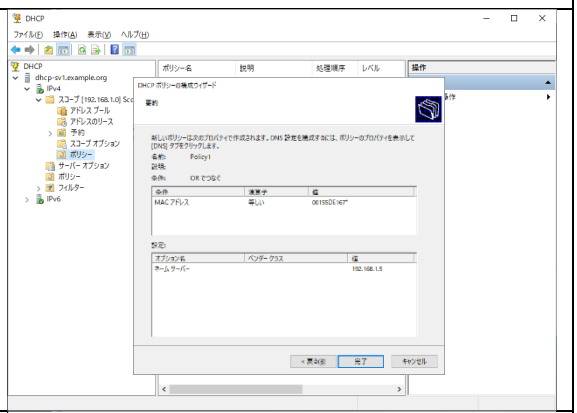
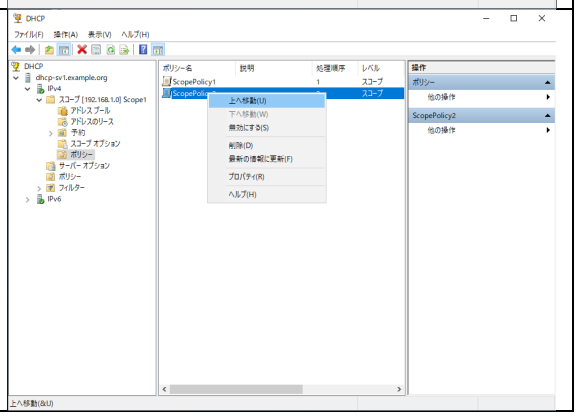
ポリシーベースの IP アドレス割り当ては、IPv4 環境、または IPv6 環境のステートフルアドレス自動構成時のオプション設定です。IP アドレスの割り当て条件は、DHCP サーバーレベルまたはスコープレベルで設定できます。

※本手順では、IPv4 環境でスコープレベルのポリシーを設定する手順を説明します。
ポリシーの条件の例は以下のとおりです。
・ MAC アドレスのプレフィックスが「4C:52:62:4D:31:*」と等しい

また本手順では、利用可能なオプションとして DNS サーバーを設定します。本手順と同様に利用可能なオプションを設定する場合は、あらかじめ DNS サーバーを起動しておく必要があります。
なお、本手順では DNS サーバーの IP アドレス例として 192.168.1.5 を設定しています。

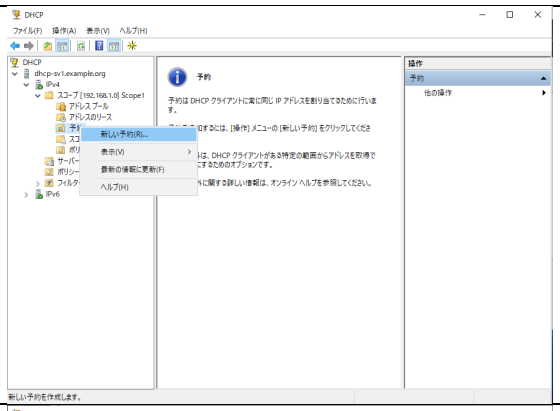
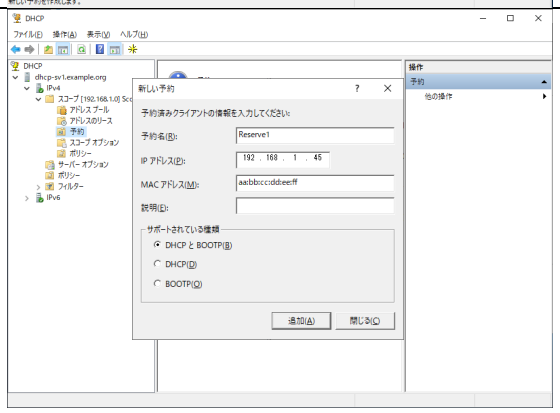
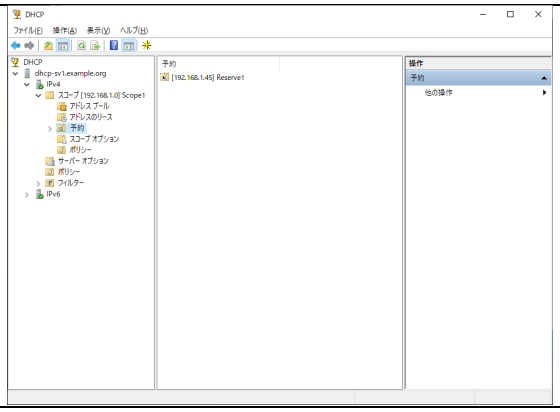
1	DHCP コンソールを起動します。 [DHCP]-[(サーバー名)]-[IPv4]-[(スコープ名)]-[ポリシー]を右クリックして[新しいポリシー]をクリックします。 (※)サーバーレベルのポリシーを設定する場合は、[DHCP]-[(サーバー名)]-[IPv4]-[ポリシー]を右クリックして[新しいポリシー]をクリックします。	
2	[DHCP ポリシーの構成ウィザード]が起動して、[ポリシーベースの IP アドレスおよびオプションの割り当て]が表示されます。 [ポリシー名]を入力します。 [次へ]をクリックします。	
3	[ポリシーの条件を構成]が表示されます。 [追加]をクリックします。 (※)複数の条件を組み合わせる場合には、2 つ目以降の条件の作成時に AND か OR を選択します。	

4	[条件の追加/編集]が開きます。 [条件]、[演算子]、[値]を入力します。 [OK]をクリックします。 (※)MAC アドレスのプレフィックスが「4C:52:62:4D:31:*」と等しいを条件にするため、[条件]は「MAC アドレス」、[演算子]は「等しい」、[値]は「4C52624D31」、「ワイルド カード(*)を追加する」をチェックします。	
5	[ポリシーの条件を構成] に設定した条件、演算子、値が表示されます。 [次へ]をクリックします。	
6	[ポリシーの設定を構成]画面が表示されます。配布する IP アドレスの範囲を指定する場合は、[はい]をチェックして、[開始 IP アドレス]と[終了 IP アドレス]を設定します。 [次へ]をクリックします。 (※)サーバーレベルのポリシーを設定する場合、本画面は表示されません。 手順 7 へ進んでください。	

7	[ポリシーの設定を構成]画面が表示されます。 オプションとして、DNS サーバーやルーター（デフォルトゲートウェイ）などの情報を DHCP サーバーで配布する場合は、[利用可能なオプション]を設定します。 サーバー名、IP アドレスを入力して、[次へ]をクリックします。 （※）利用可能なオプションの設定として DNS サーバーを設定する手順は以下の通りです。 ① 「006 DNS サーバー」をチェックします。 ② [サーバー名]に DNS サーバー名を入力して[解決]をクリックするか、[IP アドレス]に DNS サーバーの IP アドレス（例では「192.168.1.5」）を直接入力します。 ③ [追加]をクリックします。 指定したサーバーで DNS サーバーサービスが実行中であるかが自動で確認され、問題がなければ設定されます。	
8	[要約]画面に設定したポリシーの内容が表示されます。[完了]をクリックします。 ポリシーが追加されました。	
9	ポリシーが複数ある場合、ポリシーに処理順序を指定できます。 ポリシーを右クリックして[上へ移動]または[下へ移動]をクリックします。 指定した処理順序で、ポリシーが適用されます。	

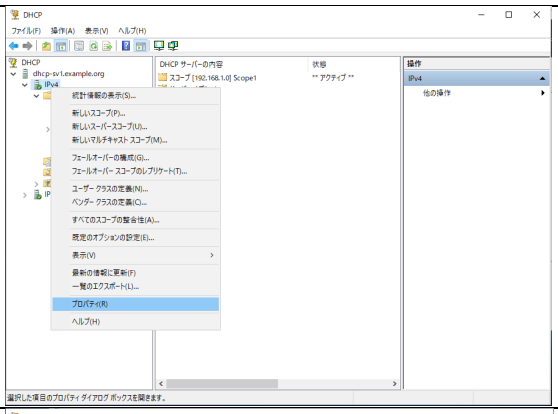
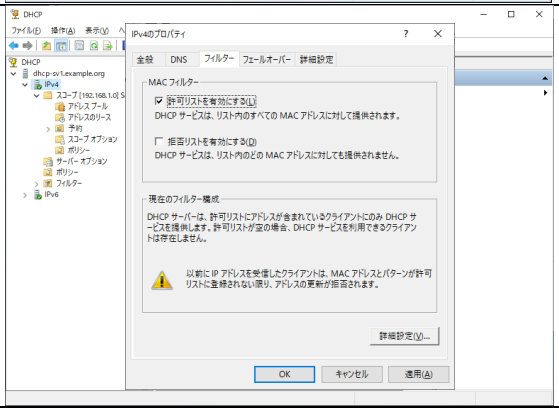
1.3.4. 予約アドレスの設定 

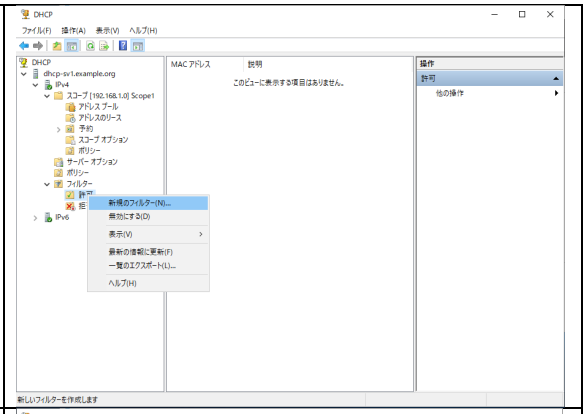
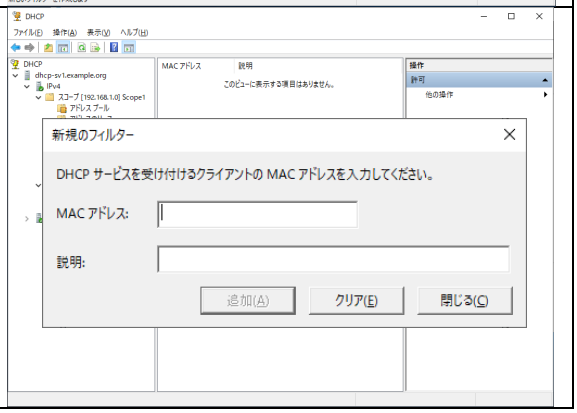
予約アドレスの設定は、IPv4 環境、または IPv6 環境のステートフルアドレス自動構成時のオプション設定です。

1	DHCP コンソールを起動します。 [DHCP]-[(サーバー名)]-[IPv4]-[(スコープ名)](※)-[予約]を右クリックして[新しい予約]をクリックします。 (※)予約アドレスの設定を行う対象のスコープ名をポイントします。ここでは、IPv4 のスコープで予約アドレス設定を行います。	
2	[新しい予約]ダイアログが表示されます。 [予約名]、[IP アドレス]、[MAC アドレス]を入力します。 [追加]をクリックします。 (補足：IPv6 における予約アドレス) IPv6 では MAC アドレスに代わり DUID、IAID(※)を入力します。 (※)DUID、IAID については「付録 1：DHCPv6 におけるアドレス予約」を参照してください	
3	予約が完了すると中央ペインに作成した予約アドレスが表示されます。	

1.3.5. リンク層フィルターの設定

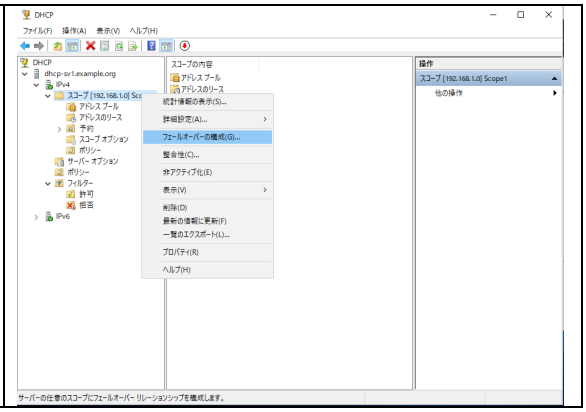
リンク層フィルターの設定は、MAC アドレスに基づいて IP アドレスの DHCP リースの発行または拒否を行うための、IPv4 環境のオプション設定です。
MAC アドレスは、完全なアドレスまたは MAC アドレスパターン（ワイルドカード）を指定できます。

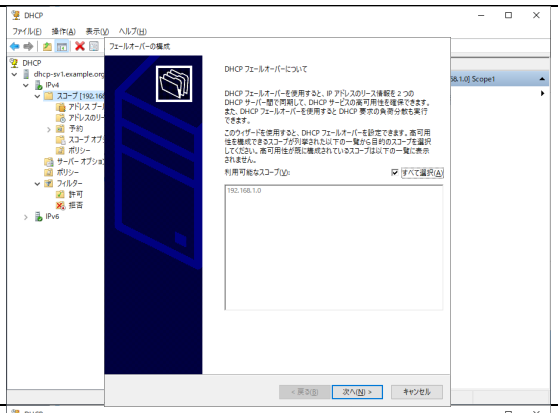
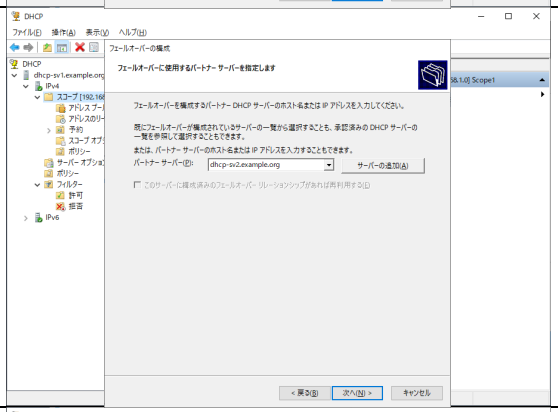
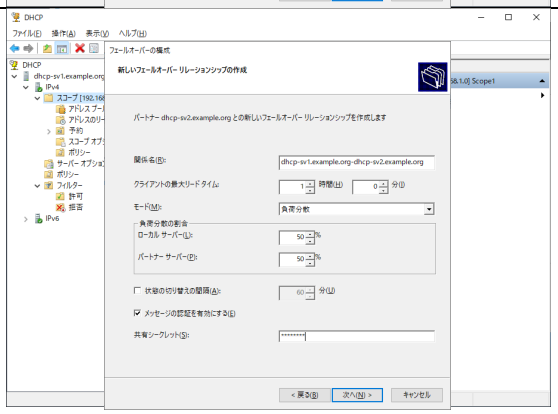
1	DHCP コンソールを起動します。 [DHCP]-[(サーバー名)]-[IPv4]を右クリックして[プロパティ]をクリックします。	
2	[フィルター]タブをクリックして、[許可リストを有効にする]と[拒否リストを有効にする]それぞれに、必要に応じてチェックを入れます。 [OK]をクリックします。	

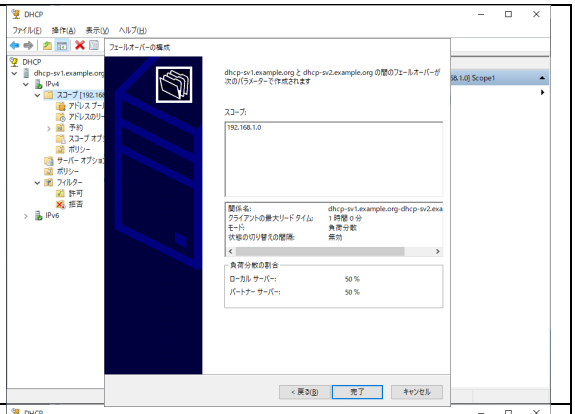
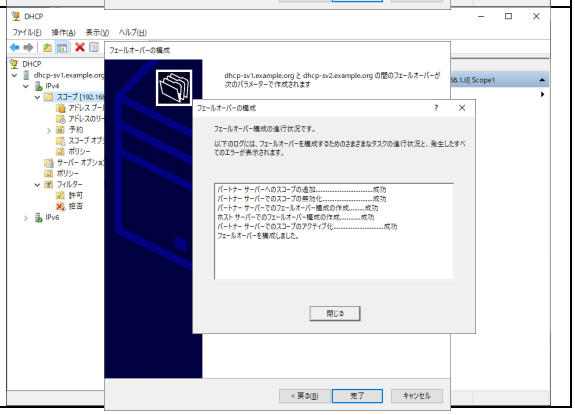
3	[DHCP]-[(サーバー名)]-[IPv4]-[フィルター]配下の[許可]または[拒否]を右クリックして[新規のフィルター]をクリックします。 (※)許可リストを有効にする場合は[許可]のフィルターを、拒否リストを有効にする場合は[拒否]のフィルターを、それぞれ作成する必要があります。どちらも有効にする場合は、[許可]と[拒否]の両方のフィルターを作成してください。	
4	[MAC アドレス]に MAC アドレスを入力します。 登録する MAC アドレスを追加する場合には[追加]をクリックして、登録を終える場合には[閉じる]をクリックします。 (※)MAC アドレスの入力例 ・ 4C-53-62-*-*-* ・ 4C526265FB4E ・ 4C52*	

1.3.6. DHCP フェールオーバーの構成

DHCP フェールオーバーの構成は、IPv4 環境時のオプション設定です。
2 台の DHCP サーバーに DHCP フェールオーバー関係を作成します。
ここでは、DHCP フェールオーバーの構成を行うサーバー(プライマリーサーバー)を DHCP1、パートナーサーバーを DHCP2 として説明します。以下の手順はあらかじめ DHCP2 が起動されていることを前提としています。

1	DHCP1 で、DHCP コンソールを起動します。 [DHCP]-[(サーバー名)]-[IPv4]-[(スコープ名)] を右クリックして[フェールオーバーの構成]をクリックします。	

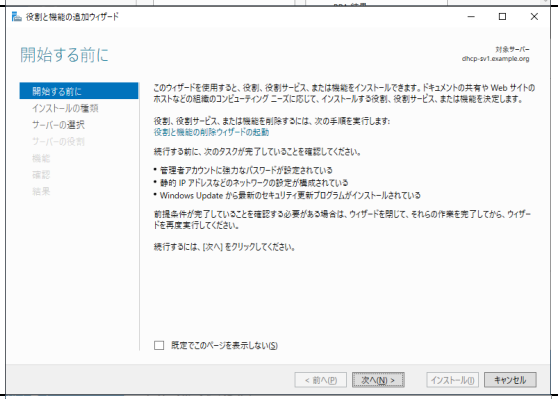
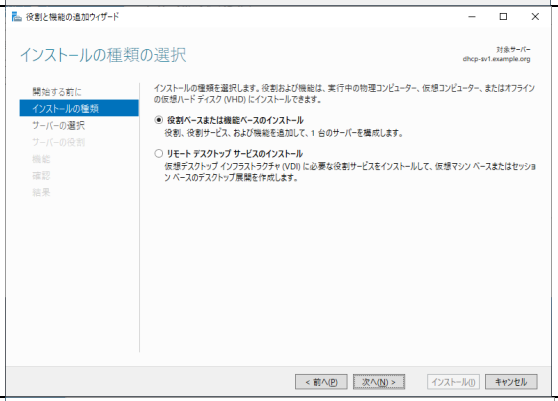
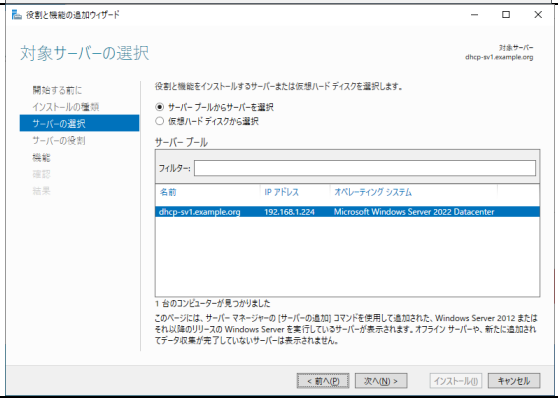
2	[フェールオーバーの構成]画面が表示されます。 [次へ]をクリックします。	
3	[フェールオーバーに使用するパートナーサーバーを指定します]画面が表示されます。 [パートナーサーバー]に DHCP2 のホスト名または IP アドレスを入力します。 [次へ]をクリックします。	
4	[新しいフェールオーバーリレーションシップの作成] 画面が表示されます。 [関係名]には、フェールオーバー関係を説明する任意の文字列を入力します。 [クライアントの最大リードタイム]には、プライマリサーバーがダウンした場合に、パートナーサーバーに切り替わるまでの時間を設定します。 [モード]には、「負荷分散」または「ホットスタンバイ」を指定します。 [共有シークレット]には、2 台の DHCP サーバー間でフェールオーバーを構成するために必要な共有シークレット（文字列）を入力します。 [次へ]をクリックします。 （※）画面は、[モード]に「負荷分散」を指定した場合の例です。	

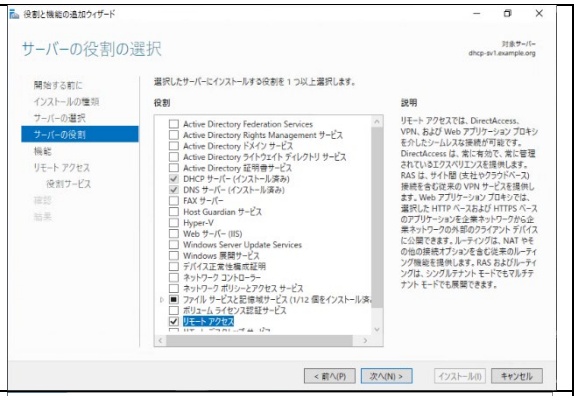
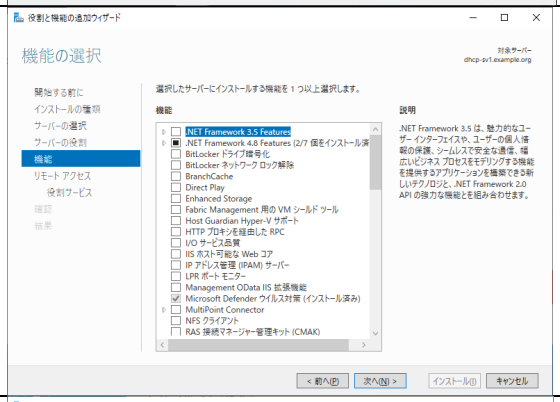
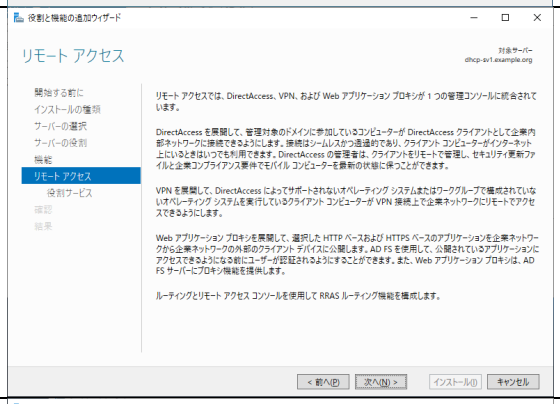
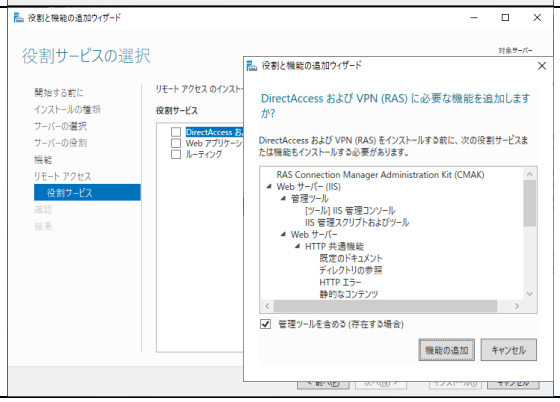
5	設定内容が表示されます。 [完了]をクリックします。	
6	フェールオーバー構成の進行状況が表示されます。フェールオーバーの構成が正常に完了したことを確認して、[閉じる]をクリックします。 DHCP2 の DHCP コンソールで、スコープの設定が DHCP1 と同じであることを確認してください。	

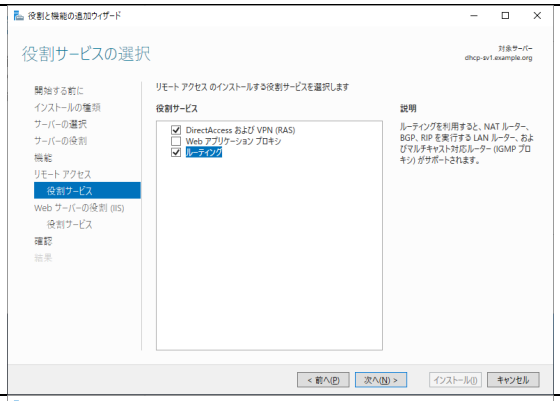
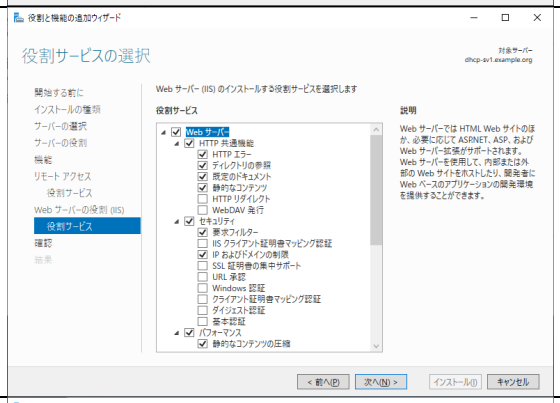
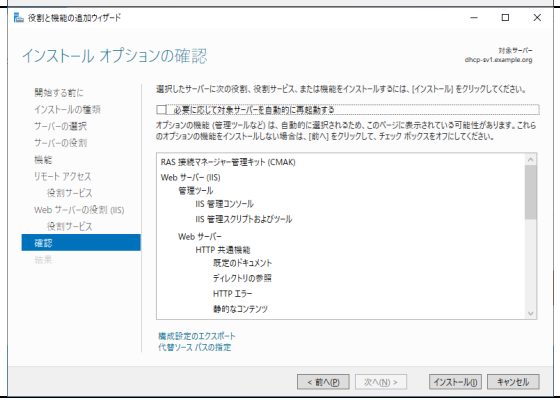
1.3.7. リレーエージェントの構築

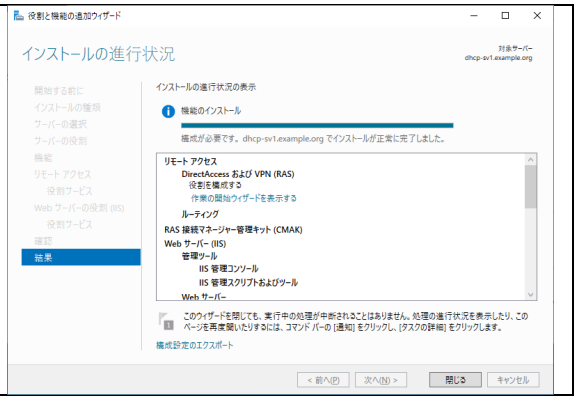
この手順は、リレーエージェント機能を利用して、他のセグメントのクライアントに対して IP アドレスを割り当てる場合のオプション設定です。

(1) ルーティングとリモートアクセスのインストール

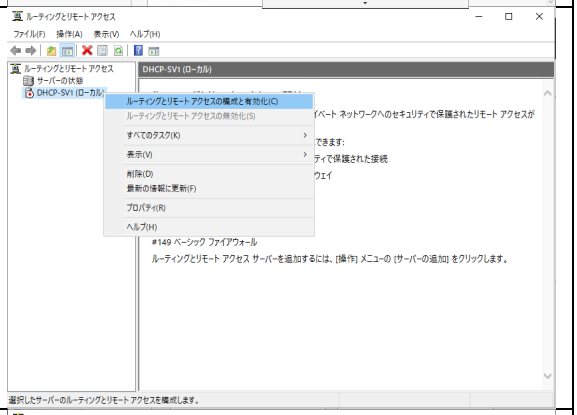
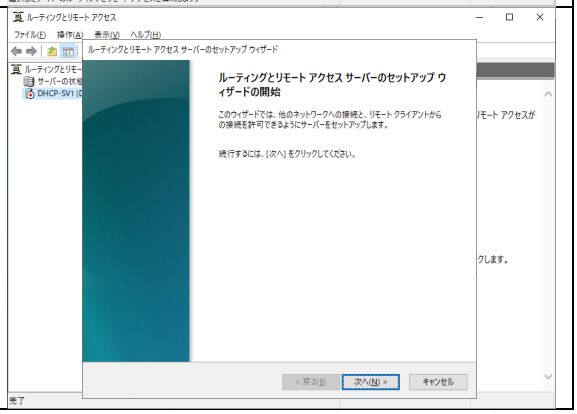
1	[サーバーマネージャー]の[役割と機能の追加]をクリックします。	
2	役割と機能の追加ウィザードの[開始する前に]が表示されます。 [次へ]をクリックします。	
3	[インストールの種類の選択]が表示されます。 [役割ベースまたは機能ベースのインストール]をチェックして、[次へ]をクリックします。	
4	[対象サーバーの選択]が表示されます。 必要に応じてインストール先を選択します。 [次へ]をクリックします。	

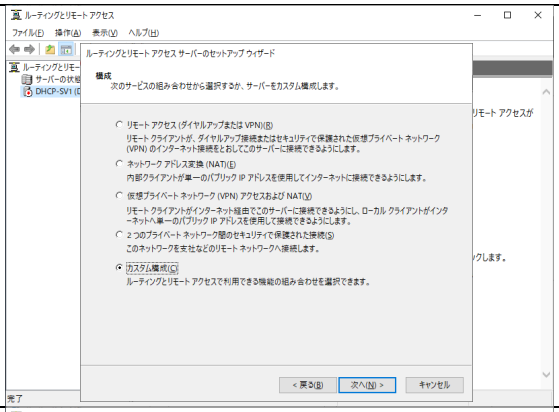
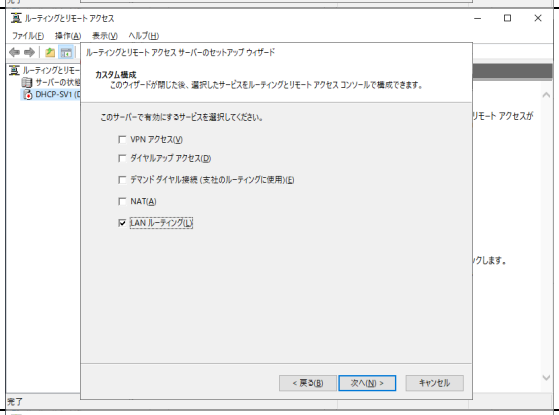
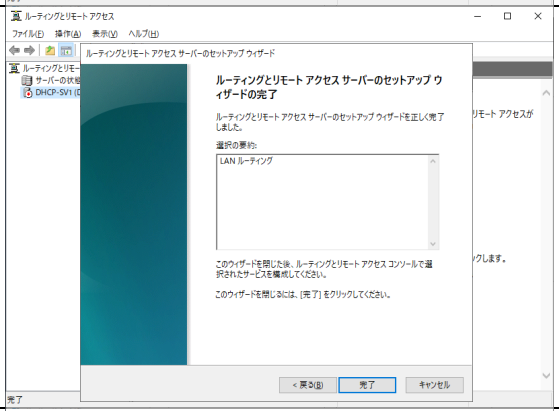
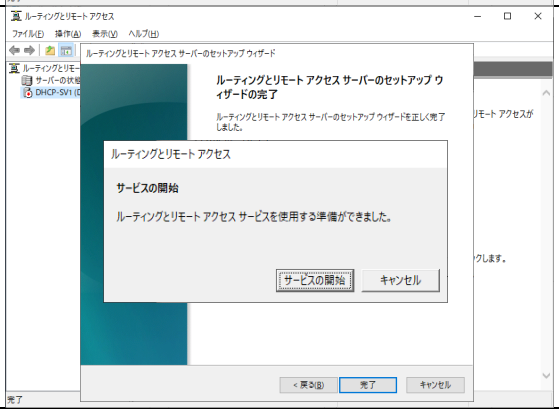
5	[サーバーの役割の選択]が表示されます。 [リモートアクセス]をチェックします。 [次へ]をクリックします。	
6	[機能の選択]が表示されます。 [次へ]をクリックします。	
7	[リモートアクセス]が表示されます。 [次へ]をクリックします。	
8	[役割サービスの選択]が表示されます。 [DirectAccess および VPN (RAS)]をチェックします。 チェックすると必要な機能追加の確認画面が表示されるので、[機能の追加]をクリックします。	

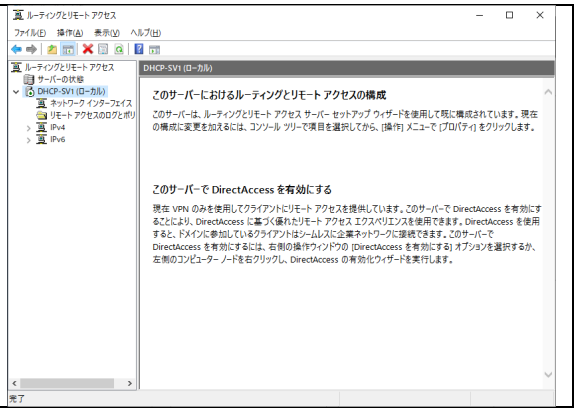
9	[ルーティング]をチェックして、[次へ]をクリックします。	
10	[Web サーバーの役割(IIS)]が表示されます。 [次へ]をクリックします。	
11	[役割サービスの選択]が表示されます。 [次へ]をクリックします。	
12	[インストールオプションの確認]が表示されます。 [インストール]をクリックします。	

13	[インストールの進行状況]が表示されます。 インストールが完了したら、[閉じる]をクリックします。	

(2) ルーティングとリモートアクセスの有効化

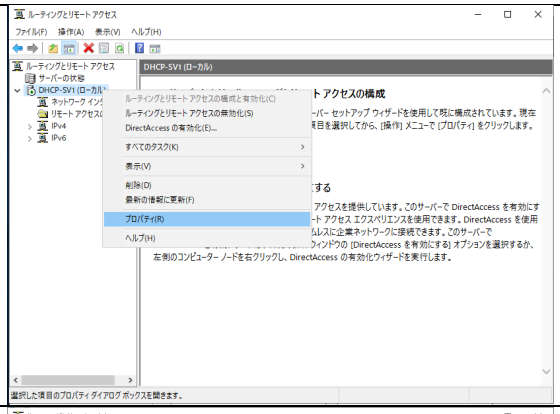
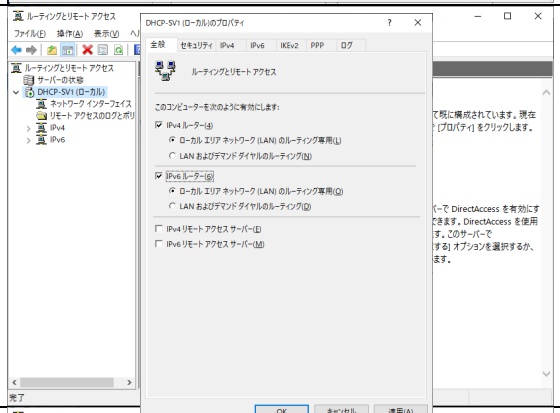
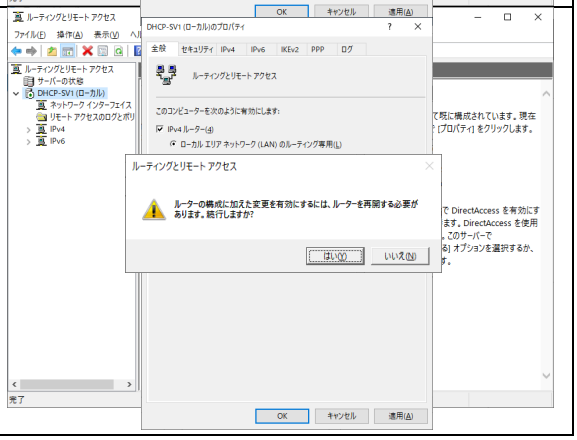
1	[サーバー マネージャー]の[ツール]メニューから[ルーティングとリモート アクセス]をクリックします。	
2	[ルーティングとリモートアクセス]ツール上で[(サーバー名)]を右クリックして、[ルーティングとリモート アクセスの構成と有効化]をクリックします。	
3	ルーティングとリモート アクセス サーバーのセットアップ ウィザードが開始されます。 [次へ]をクリックします。	

4	[構成]が表示されます。 [カスタム構成] にチェックを入れます。 [次へ]をクリックします。	
5	[カスタム構成]が表示されます。 [LAN ルーティング]にチェックを入れます。 [次へ]をクリックします。	
6	[ルーティングとリモート アクセス サーバーのセット アップ ウィザードの完了]が表示されます。 [完了]をクリックします。	
7	[ルーティングとリモート アクセス]ダイアログが表示されます。 [サービスの開始] をクリックします。	

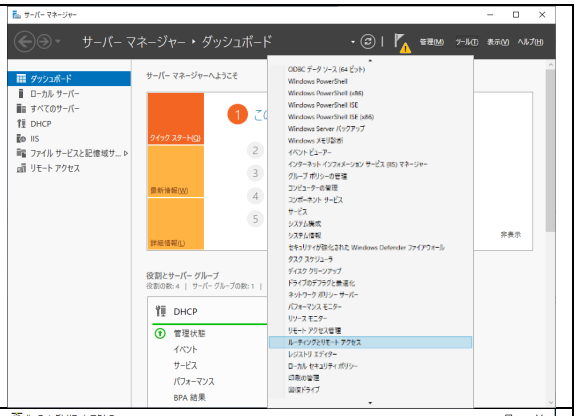
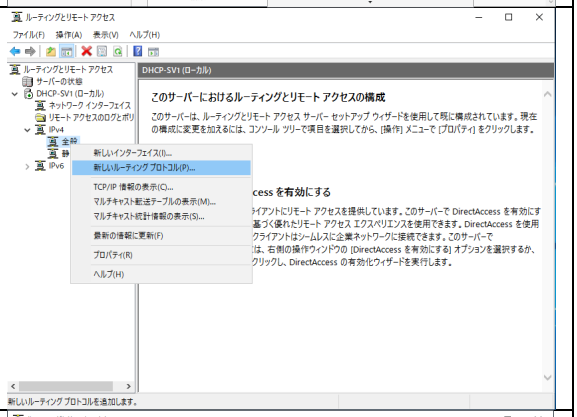
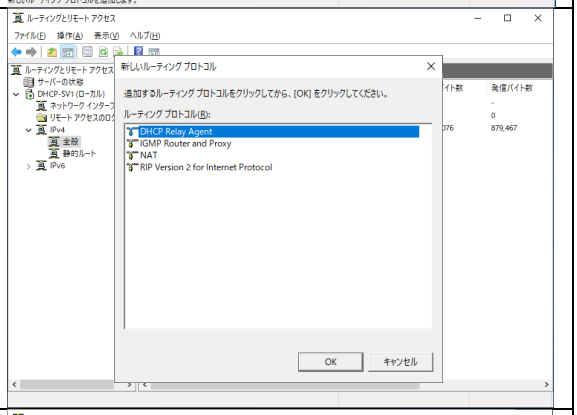
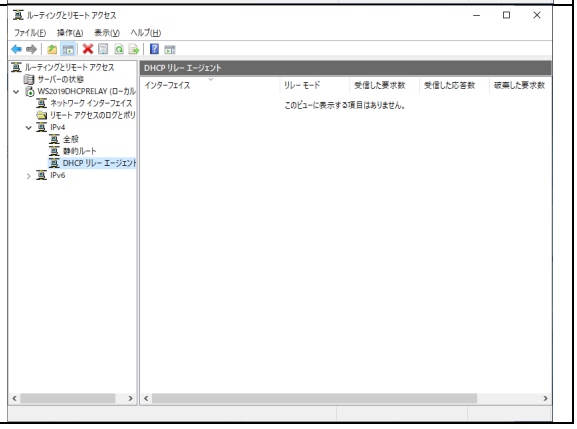
8	[サーバー名(ローカル)] アイコンにある[⇧]が、赤色から緑色に変わったことを確認します。	

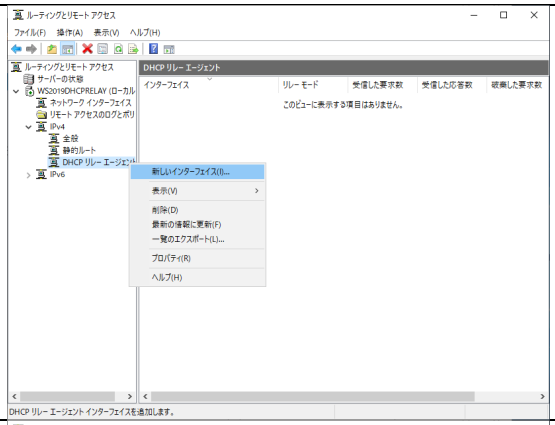
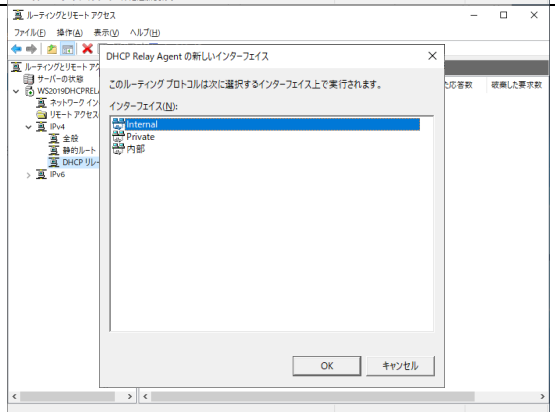
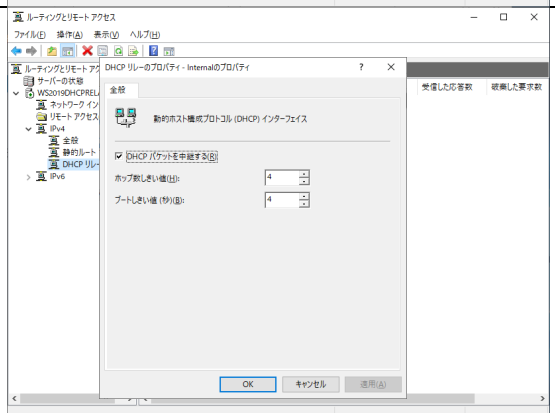
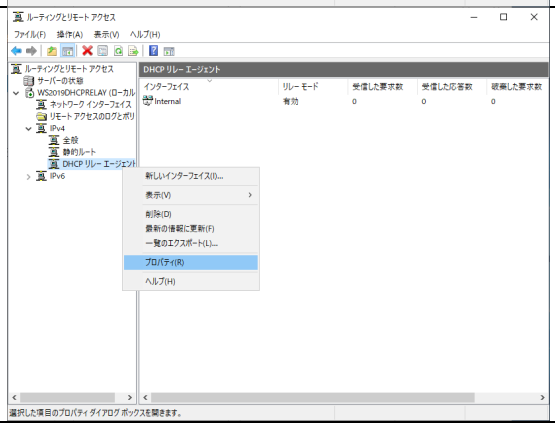
補足：IPv6 ルーターの有効化

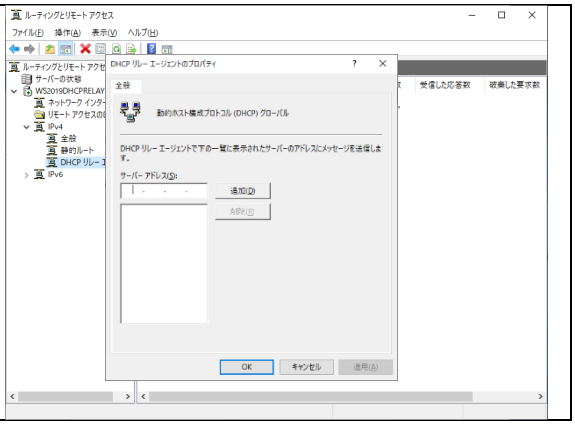
IPv6 環境では、引き続き以下の手順を行ってください。

1	[ルーティングとリモートアクセス]–[サーバー名(ローカル)]を右クリックして[プロパティ]をクリックします。	
2	[ルーティングとリモート アクセスのプロパティ]画面が表示されます。[全般]タブ内の[IPv6 ルーター]にチェックを入れます。 [OK]をクリックします。	
3	[ルーティングとリモートアクセス]のポップアップが表示されます。 [はい]をクリックします。	

(3) リレーエージェントの有効化

1	[サーバー マネージャー]の[ツール]メニューから[ルーティングとリモートアクセス]をクリックします。	
2	[ルーティングとリモートアクセス]–[サーバー名(ローカル)]-[IPv4]-[全般]を右クリックして、[新しいルーティングプロトコル]をクリックします。	
3	[新しいルーティング プロトコル]画面が表示されます。 [DHCP Relay Agent]をポイントします。 [OK]をクリックします。 (※)IPv6 環境の場合は[DHCPv6Relay Agent]をポイントします。	
4	[IPv4]配下に[DHCP リレー エージェント]が追加されたことを確認します。	

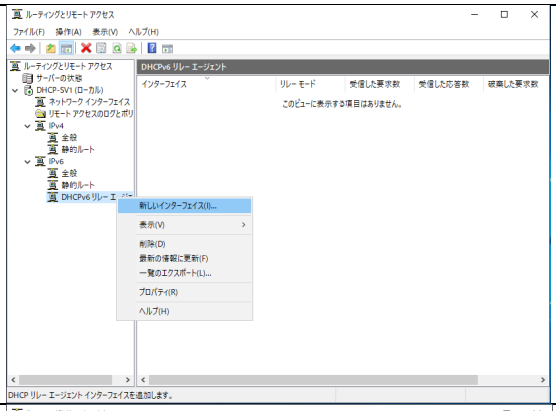
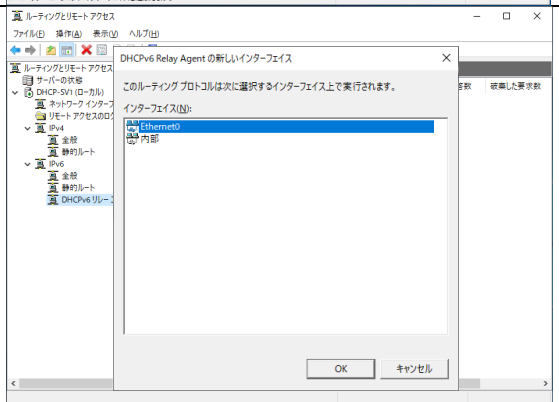
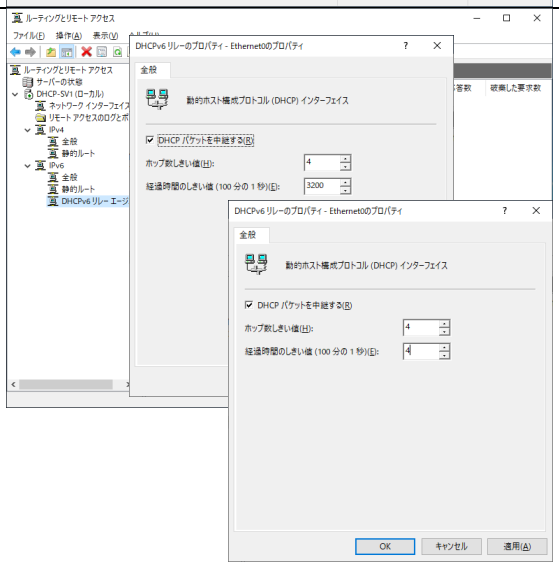
5	追加された[DHCP リレー エージェント]を右クリックして、[新しいインターフェイス]を選択します。	
6	[DHCP Relay Agent の新しいインターフェイス]が表示されます。 DHCP ルーティングプロトコルを実行するインターフェイスを選択して[OK]をクリックします。	
7	[DHCP リレーのプロパティ -<インターフェイス名> のプロパティ]が表示されます。 [OK]をクリックします。 インターフェイスが追加されたことを確認します。	
8	もう一度[DHCP リレー エージェント]を右クリックして、[プロパティ]をクリックします。	

9	[DHCP リレー エージェントのプロパティ]が表示されます。 [全般タブ]の[サーバー アドレス]に DHCP リクエストを転送する DHCP サーバーの IP アドレスを入力して、[追加]をクリックします。 [OK]をクリックします。	

(4) リレーエージェントの設定

DHCPv6 リレーエージェント機能を利用する際は、「経過時間のしきい値」の設定が必要になります。「経過時間のしきい値」は、ローカルネットワークの DHCP サーバーの応答を優先させるために、DHCPv6 リレーエージェントが DHCPv6 メッセージを転送せずに待機する時間です。
ローカルネットワークに DHCP サーバーが存在しない場合には、速やかにリレーエージェントから DHCP サーバーへの要求が行われるように、待機時間を短く設定してください。

待機時間の設定方法は以下のとおりです。

1	[ルーティングとリモートアクセス]–[サーバー名(ローカル)]-[IPv6]-[DHCPv6 リレーエージェント]を右クリックして、[新しいインターフェイス]をクリックします。	
2	[DHCPv6Relay Agent の新しいインターフェイス]画面が表示されます。 DHCP ルーティングプロトコルを実行するインターフェイスを選択して[OK]をクリックします。	
3	[DHCPv6 リレーのプロパティ - イーサネットのプロパティ]画面が表示されます。 [経過時間のしきい値(100 分の 1 秒)]を既定の 3200 から短い値に変更します。 [OK]をクリックします。 (※)[経過時間のしきい値]のここでは設定例として、値を"4"に変更します。	

1.4. DHCP サーバーの運用

1.4.1. DHCP データベースのバックアップと復元

DHCP サーバーに障害が発生した場合は、IP アドレスのリースができずクライアントがネットワークを利用できなくなります。IP アドレスをリースするために必要な情報は DHCP データベースに保存されています。スコープや予約アドレスなどの設定を変更した後は、DHCP データベースをバックアップしてください。ここでは DHCP データベースのバックアップと復元について紹介します。

(1) DHCP データベースのバックアップ

DHCP データベースのバックアップ方法は、以下の 2 通りがあります。

(a) 自動バックアップ

DHCP データベースの自動バックアップは既定では 60 分間隔で行われます。リース期間が長いなど自動バックアップを頻繁に行う必要がない場合は、以下の PowerShell コマンドを使用して自動バックアップの間隔を変更できます。

→ Set-DhcpServerDatabase -BackupInterval “間隔(分)”

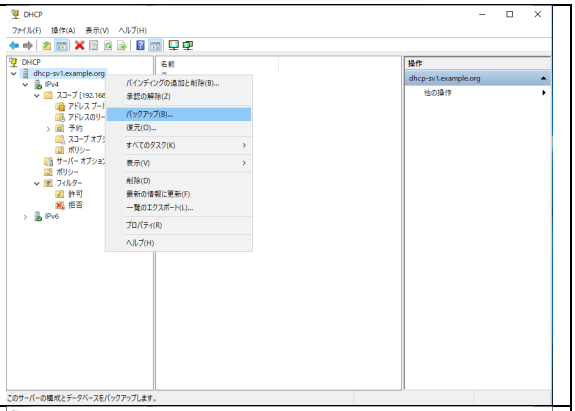
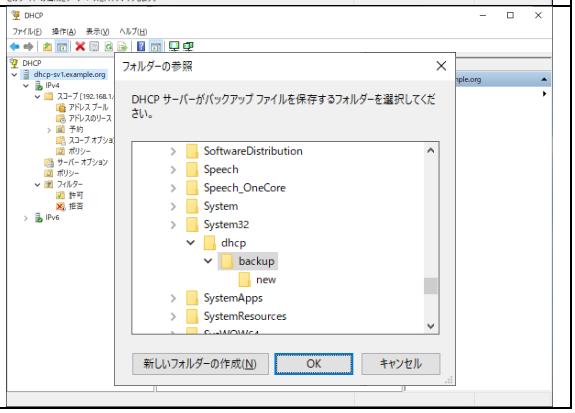
詳細は以下 URL を参照してください。

参考：Set-DhcpServerDatabase

https://docs.microsoft.com/en-us/powershell/module/dhcpserver/set-dhcpserverdatabase?view=win10-ps

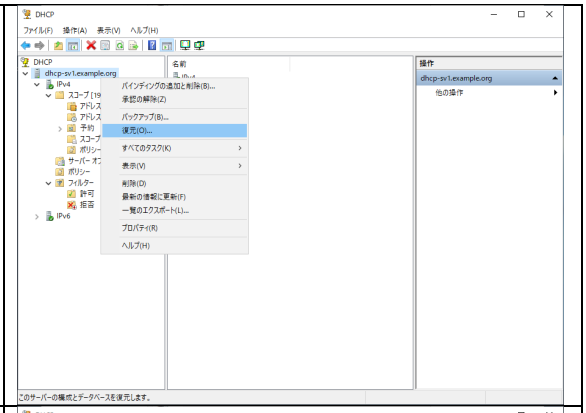
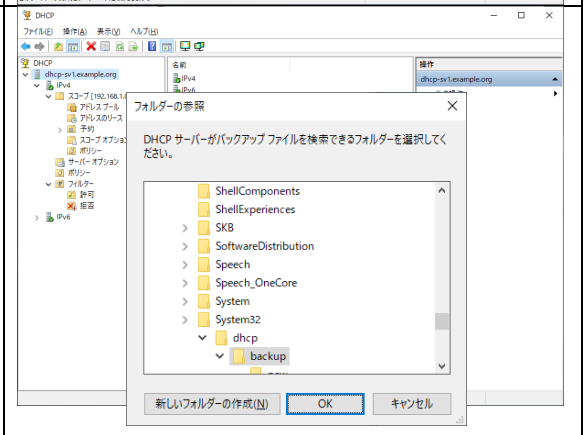
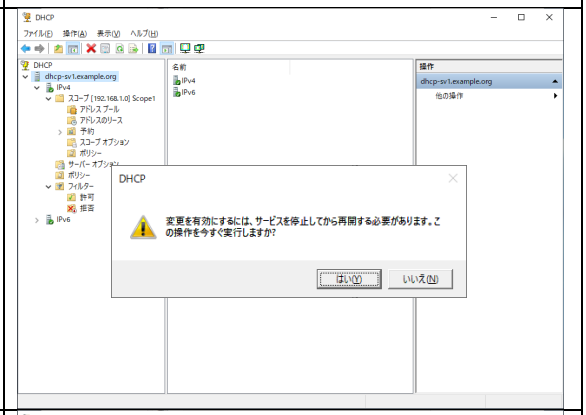
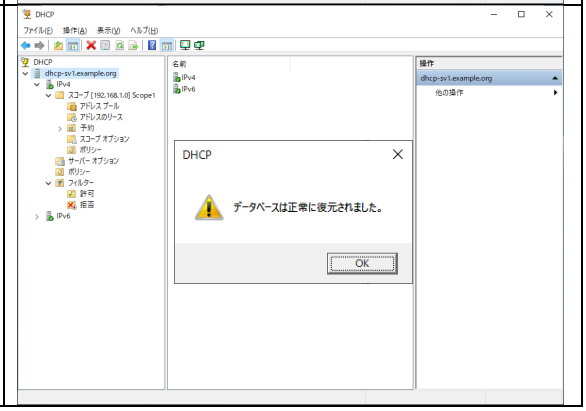
(b) 手動バックアップ

DHCP コンソールを利用して DHCP サーバーのデータベースのバックアップを取得します。

1	DHCP コンソールを起動します。 [DHCP]-[(サーバー名)]を右クリックして、[バックアップ]をクリックします。	
2	バックアップファイルを保存するフォルダーを選択します。 [OK]をクリックします。 (※)ローカルディスクのみ指定できます。 万一のトラブルに備えて、バックアップデータは別途、外部媒体などへ保存してください。	

(2) DHCP データベースの復元

DHCP コンソールを使用して DHCP データベースを復元します。

1	DHCP コンソールを起動します。 [DHCP]-[(サーバー名)]を右クリックして、[復元]をクリックします。	
2	バックアップファイルが保存されているフォルダーを選択します。 [OK]をクリックします。 (※)手動バックアップ時に保存先フォルダーを変更していた場合は、手動バックアップ時に選択したフォルダーを指定します。	
3	[はい]をクリックします。 DHCP Server サービスを再起動するメッセージが表示される間、しばらく待ちます。	
4	データベースが正常に復元されたことを示すポップアップが表示されます。 [OK]をクリックします。	

1.4.2. コマンドによる DHCP サーバーの設定 

ネットワーク構成の表示、更新のための Netsh コマンドは、DHCP サーバーの管理にも使用できます。スクリプトを組むことで一括設定できるため、スコープに設定した IP アドレスを複数操作したり、複数の DHCP サーバーを管理したりする場合には便利なコマンドです。

[例] スコープ 192.168.1.0 において、現在予約されているすべての IP アドレスを表示します。
netsh dhcp server scope 192.168.1.0 show reservedip

[例] スコープ 192.168.1.0 において、MAC アドレスに関連づけた IP アドレスを予約します。
netsh dhcp server scope 192.168.1.0 add reservedip 192.168.1.83 07002a20258c

参考：Netsh commands for DHCP
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc787375(v=ws.10)

DHCP サーバーの管理／構成を行う Common Information Model（CIM）ベースの DHCP サーバー用 Windows PowerShell コマンドレットが用意されています。
コマンドレット一覧については、以下のマイクロソフト社の Web サイトの情報を参照してください。
以下にコマンドレットの使用例を示します。

［例］スコープ名：Scope1、IP アドレスの範囲：192.168.1.100～192.168.1.200、サブネット：255.255.255.0 の IPv4 のスコープを追加します。
Add-DHCPServerv4Scope -Name "Scope1" -StartRange 192.168.1.100 -EndRange 192.168.1.200 -SubnetMask 255.255.255.0

参考：「Windows PowerShell を使用した DHCP の展開」内の「DHCP 用の Windows PowerShell コマンド」
https://docs.microsoft.com/ja-jp/windows-server/networking/technologies/dhcp/dhcp-deploy-wps#windows-powershell-commands-for-dhcp

1.4.3. リースの管理 

IP アドレスのリースは DHCP サーバーにより管理されるため、通常、システム管理者による管理は不要となりますが、システム管理者によるリースの管理が必要な場合があります。
例えば、IP アドレスの除外やクライアントの IP アドレス予約を行う際には、競合するリースを削除する必要があります。ただし、リースの削除を行っても、リースの再取得を禁止したわけではありません。すでにリースされていた IP アドレスは、そのクライアントから同じ IP アドレスの再取得が行われる可能性があるので、その要求に応える前に IP アドレスを再リースしないように、IP アドレスの除外や IP アドレス予約を完了しておく必要があります。

参考：Managing leases
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc780476(v=ws.10)

DHCP サーバーと DNS サーバーとは別に、IPAM サーバーを構築することで、IPAM 機能を使用したリース管理も可能です。
IPAM の主な機能は、以下です。

- DHCP サーバー/DNS サーバー/ドメインコントローラの自動検出および遠隔操作
- IP アドレス利用率の予測や DHCP/DNS 処理能力のプランニングおよび利用率のトレース
- レポート作成機能（コンプライアンス要件として法的に利用可能な報告書を作成）

なお、Windows Server 2016 の IPAM では、以下の機能が追加または強化されました（表 1）。

表 1 Windows Server 2016 で追加または強化された IPAM の機能

機能	新機能/強化	説明
強化された IP アドレス管理	強化	IPv4/32 および IPv6/128 サブネットの処理や、IP アドレスブロック内の空き IP アドレスのサブネットと範囲の検索などのシナリオでは、IPAM 機能が強化されています。
強化された DNS サービス管理	新規	ドメインに参加している Active Directory 統合 DNS サーバーとファイルベースの DNS サーバーの両方について、DNS リソースレコード、条件付きフォワーダー、および DNS ゾーン管理がサポートされています。
統合 DNS、DHCP、IP アドレス（DDI）管理	強化	いくつかの新しいエクスペリエンスと統合ライフサイクル管理操作が可能になりました。たとえば、IP アドレスに関連するすべての DNS リソースレコードの視覚化、DNS リソースレコードに基づく IP アドレスの自動インベントリ、IP アドレスのライフサイクル管理などです。DNS と DHCP の両方の操作に使用します。
複数の Active Directory フォレストのサポート	新規	IPAM がインストールされているフォレストと各リモートフォレストの間に双方向の信頼関係がある場合は、IPAM を使用して複数の Active Directory フォレストの DNS および DHCP サーバーを管理できます。
使用率データの消去	新規	指定した日付よりも古い IP アドレス使用率データを削除することで、IPAM データベースのサイズを減らすことができるようになりました。
Windows PowerShell によるロールベースの Access Control のサポート	新規	IPAM オブジェクトのアクセススコープを設定できます。

出典：IPAM の新機能（マイクロソフト社）
https://docs.microsoft.com/ja-jp/windows-server/networking/technologies/ipam/what-s-new-in-ipam

2. DNS サーバー

DNS とは、IP アドレスとホスト名のマッピングを行うサービス(名前解決)を提供する機能です。名前解決によってユーザーは、数字を羅列した IP アドレスではなく、覚えやすい文字列でネットワークコンピューターを参照できます。
小規模環境における名前解決であれば hosts ファイルを用いた個別管理も可能ですが、大規模環境においては管理を容易に行うために、DNS サーバーを導入するのが一般的です。また、DNS は Windows の認証基盤「Active Directory」を構築する際の必須機能であり、Active Directory と連携して運用するケースが多くあります。
なお、Windows Server が提供する DNS サーバーは、コンピューター名と IPv6 アドレスのマッピングを行う AAAA レコードをサポートしており、IPv4/IPv6 クライアント共に名前解決が可能です。
詳細は「付録 4：DNS サーバー、クライアント間の名前解決」を参照してください。

2.1. DNS の動作概要

DNS サーバーでは名前解決を行う範囲を設定して、IP アドレスとコンピューター名とのマッピング情報を管理します。本節では、DNS サーバーの基本的な機能や動作について紹介します。

2.1.1. DNS の動作イメージ

DNS サーバーが構成されている環境でクライアントからファイルサーバーのファイルにアクセスする場合、利用者は IP アドレスではなくファイルサーバー名を指定してアクセスできます。
以下の図 2.1.1.1 は、DNS の動作イメージです。

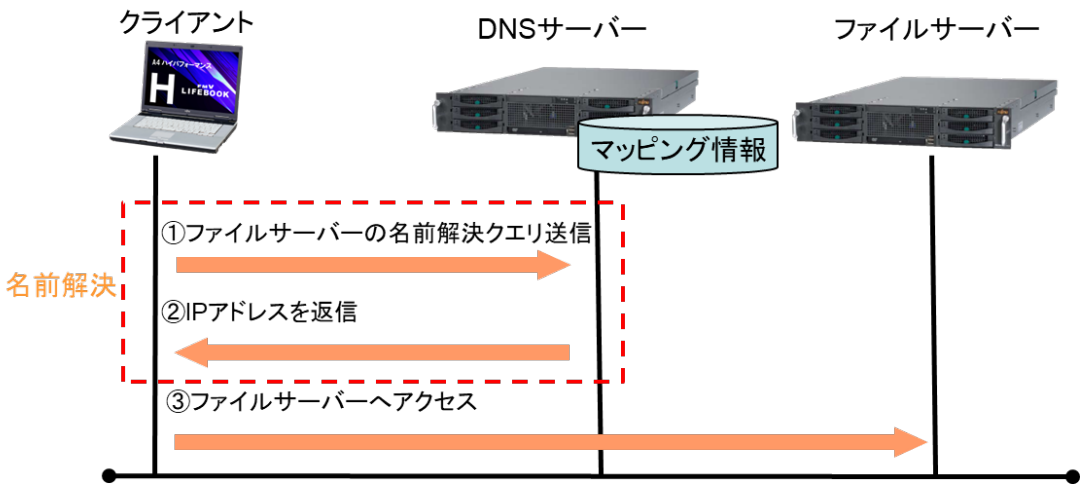


図 2.1.1.1 DNS の動作イメージ

クライアントは、ファイルサーバー名でファイルサーバーの IP アドレスを DNS サーバーへ問い合わせます(図 2.1.1.1 ①)。DNS サーバーがファイルサーバーのサーバー名と IP アドレスのマッピング情報を持っている場合、クライアントへサーバーの IP アドレスを返信します(図 2.1.1.1 ②)。サーバーの IP アドレスを取得したクライアントは、この IP アドレスを使用してファイルサーバーにアクセスします(図 2.1.1.1 ③)。図 2.1.1.1 ①と②が DNS の名前解決に当たります。

名前解決に必要な IP アドレスとコンピューター名のマッピング情報は手動で登録できますが、クライアントから自動登録する機能(動的更新)があります。新規にコンピューターをネットワークに接続したときや、IP アドレス、コンピューター名を変更した場合、これらの情報がクライアントから DNS サーバーに通知され DNS サーバーのマッピング情報に登録されます。

2.1.2. DNS サーバーにおけるレコード管理

DNS サーバーでは、DNS 名前空間を「ゾーン」と呼ばれる単位で管理します。各ゾーンでは IP アドレスとホスト名のマッピングを「レコード」で管理しており、このレコードの情報を元に名前解決を行います。
DNS のゾーンは、大きく「前方参照ゾーン」と「逆引き参照ゾーン」の 2 種類に分けられます。

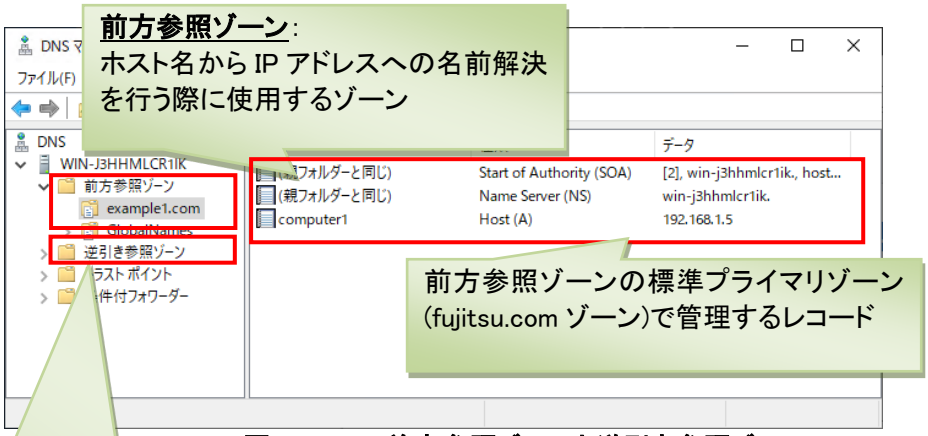


図 2.1.2.1 前方参照ゾーンと逆引き参照ゾーン

DNS サーバーでは、この「前方参照ゾーン」と「逆引き参照ゾーン」の中に目的に適うゾーン(表 2 参照)を作成して、レコードを管理します。
DNS サーバーは、主に表 2 のレコードを使用できます。レコードは種類によって名前解決以外にも様々な役割を担っています。

表 2 ゾーンの種類

ゾーンの種類	説明
標準プライマリゾーン	DNS においてマスターとなる書き込み可能なゾーンであり、DNS サービスを提供する上で必要な主要レコードを保持します。
標準セカンダリゾーン	負荷分散・可用性向上のために配置される読み取り専用のゾーンです。標準プライマリゾーンから DNS ゾーンの情報を複製することで最新状態を保ちます。
スタブゾーン	DNS の管理を簡略化するために使用します。 ・委任されたゾーン情報を自動的に最新に保つ ・スタブゾーンのネームサーバー一覧を使用して再帰を実行できるため、効率的に名前解決が可能
Active Directory 統合ゾーン	標準プライマリゾーンやスタブゾーンの情報を Active Directory のデータベースに保存します。プライマリ/セカンダリといった区別がなく、全ての DNS サーバーでレコードの更新・参照が可能です。 DNS ゾーンの更新情報は、Active Directory の複製により他のサーバーへ複製されます。 Windows Server 標準の DNS でのみ使用可能なゾーンです。

標準プライマリゾーンでは、単一ラベルの名前解決を行うために「GlobalNames」というゾーンを作成できます。GlobalNames ゾーンの詳細は「付録 5：GlobalNames ゾーン」を参照してください。

表 3 主要な DNS レコード

DNS レコード	説明
A レコード	ホスト名から IPv4 アドレスへマッピングする DNS レコード
AAAA レコード	ホスト名から IPv6 アドレスへマッピングする DNS レコード
PTR レコード	IPv4/IPv6 アドレスからホスト名へマッピングする DNS レコード
CNAME レコード	複数の名前から単一のホストを指定する際に使用するレコード
SRV レコード	ドメインコントローラなど特別なサービスを識別する際に使用するレコード
MX レコード	メールの転送先を格納したレコード

DNS サーバーは、ホスト名から IPv6 アドレスへマッピングする AAAA（クアッド A）レコードをサポートしています。IPv4/IPv6 の両方が有効に設定されているホストがある場合、DNS サーバー上にはそのホストに対して A レコードと AAAA レコードの両方が存在することになります。

2.1.3. ゾーン転送

ゾーン転送は、DNS 機能の負荷分散と冗長性を確保のために、プライマリ DNS サーバーのゾーン情報をセカンダリ DNS サーバーへ複製する機能です。プライマリ DNS サーバーの SOA レコードが更新(シリアル値の増加)されるとセカンダリ DNS サーバーはゾーン情報の複製を開始します。

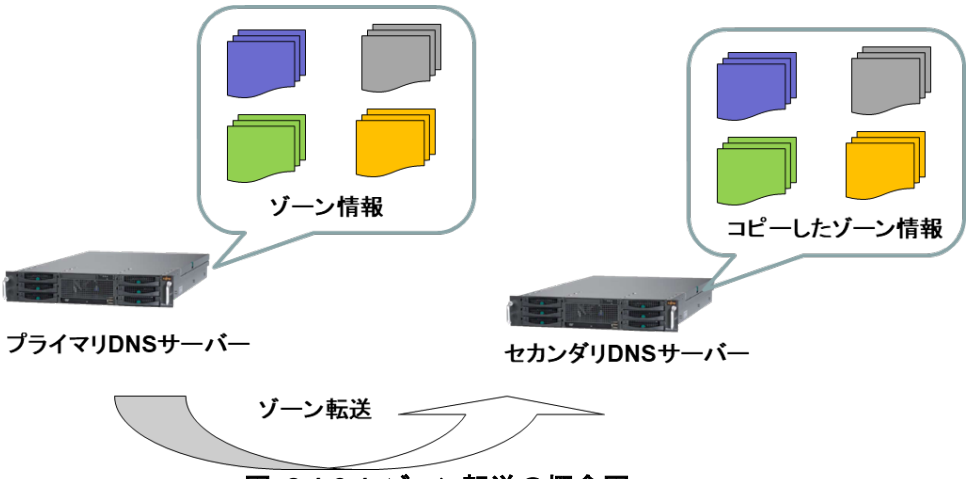


図 2.1.3.1 ゾーン転送の概念図

ゾーン転送の設定方法は「2.3.4 ゾーン転送の設定」を参照してください。
なお、セカンダリ DNS サーバーは DNS サーバーの冗長性を確保するために構築されますが、ゾーン情報の複製だけであり、DNS サーバー自体のバックアップにはなり得ません。DNS サーバーのバックアップについては「2.4.2 DNS サーバーのゾーンのバックアップ/リストア」を参照してください。

2.1.4. 他 DNS サーバーとの連携

DNS サーバーはルートヒント、フォワーダーといった他 DNS サーバーとの連携機能を持っています。これらの機能は、自分自身が管理していないゾーンに対するクエリ要求に応えるためのものです。例えば、イントラネットからインターネットへ接続する場合は、一般的にはイントラネット内の DNS サーバーとインターネット上の DNS サーバーが連携して名前解決を行います。また、管理負荷の分散のために、特定ゾーンの管理を「委任」することもできます。

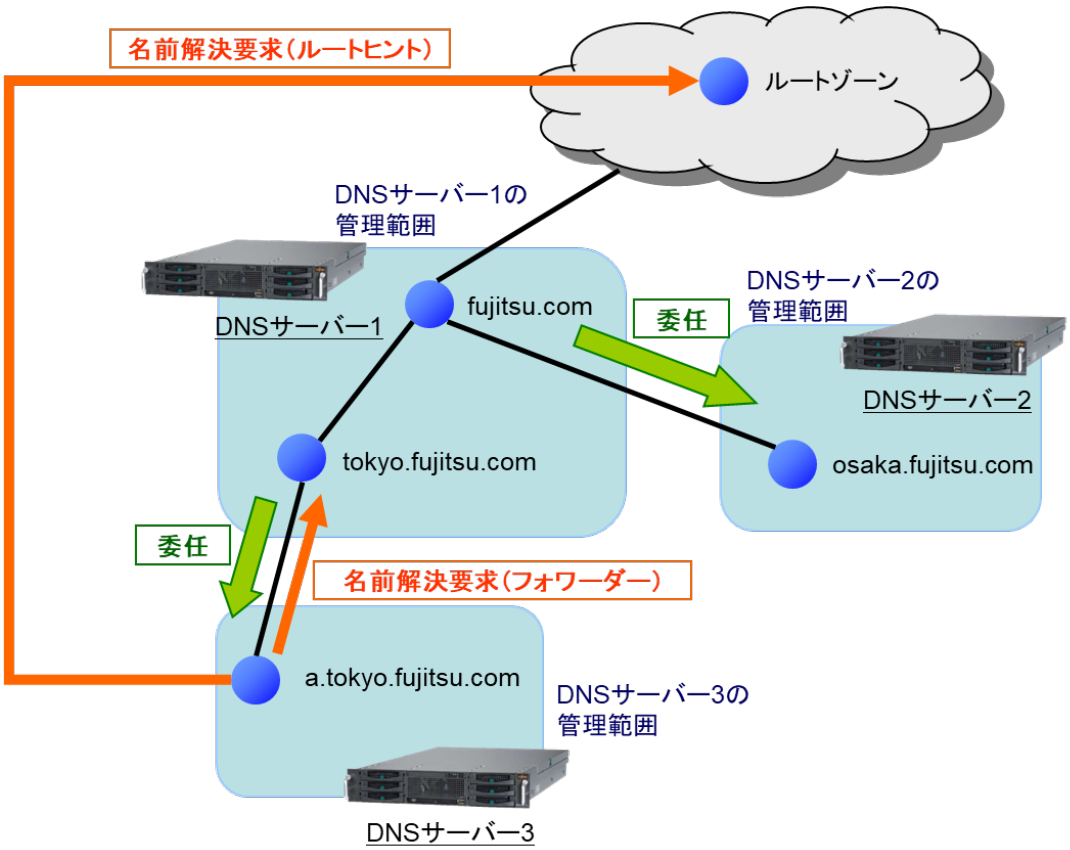


図 2.1.4.1 他 DNS サーバーとの連携

- ルートヒント
  ネットワーク内の DNS サーバーが自分自身で名前解決ができない場合、ネットワーク外部の DNS サーバーにクエリ要求を転送します。ルートヒントは、ルート(.)となる DNS サーバーからサブゾーンを管理している DNS サーバーの IP アドレスを取得して、サブゾーンを管理している DNS サーバーから、さらにその下位のサブゾーンを管理している DNS サーバーの IP アドレスを取得ということを繰り返し、クエリ要求を行ったゾーンの名前解決を行います。
  Windows Server 2016 で、IANA によって発行された IPv6 ルートヒントが Windows DNS サーバーに追加されました。 IPv6 ルートサーバーを使用した名前解決が可能です。

- フォワーダー
  フォワーダーとは、ネットワーク上の DNS サーバーの一種です。ネットワーク内の DNS サーバーが自分自身で名前解決ができない場合に、フォワーダーに名前解決させるために設定されます。フォワーダーは、ネットワーク外部の DNS サーバーにクエリ要求を転送して、他のフォレストや他のドメインに対するクエリ要求を解決します。
  フォワーダーの設定方法は「2.3.5 フォワーダーの設定」を参照してください。

- 委任
  上位の DNS サーバーで、下位の DNS サーバーに対する委任を構成することで、サブゾーンを下位の DNS サーバーで管理することができます。これにより、DNS サーバーの負荷を分散させることができます。委任したサブゾーンに対してクエリ要求された場合、DNS サーバーはサブゾーンを管理している DNS サーバーにクエリ要求を転送して、サブゾーンのホスト名を解決してもらいます。
  委任の設定方法は「2.3.6 委任の設定」を参照してください。

2.1.5. DNS ポリシー 

Windows Server 2016 で「DNS ポリシー」という新しい機能が実装されました。
DNS ポリシーは、クライアントからの名前解決要求(DNS クエリ)に対する DNS サーバーの応答を定義して、制御する機能です。
DNS ポリシーでは以下を制御することが可能です。

- アプリケーションの負荷分散
- 場所ベースのトラフィック管理
- スプリットブレイン DNS
- 時間ベースのリダイレクト
- DNS クエリのフィルタリング

参考情報
DNS ポリシーの概要
https://docs.microsoft.com/ja-jp/windows-server/networking/dns/deploy/dns-policies-overview

DNS ポリシーシナリオガイド
https://docs.microsoft.com/ja-jp/windows-server/networking/dns/deploy/dns-policy-scenario-guide

DNS ポリシーは、PowerShell を使用して設定できます。具体的な設定方法については、以下の説明内で記載しているマイクロソフト社の Web サイトの情報を参照してください。

- アプリケーションの負荷分散
  アプリケーションを複数のサーバーにインストールして分散稼働している環境で、クライアントが接続するアプリケーションサーバーの比率を制御することができます。例えば、処理能力に違いがあるアプリケーションサーバーが複数稼働している環境で、処理能力が高いアプリケーションサーバーへの接続割合を 50%に設定して、処理能力が低いアプリケーションサーバーへの接続割合を 25%に設定することができます。

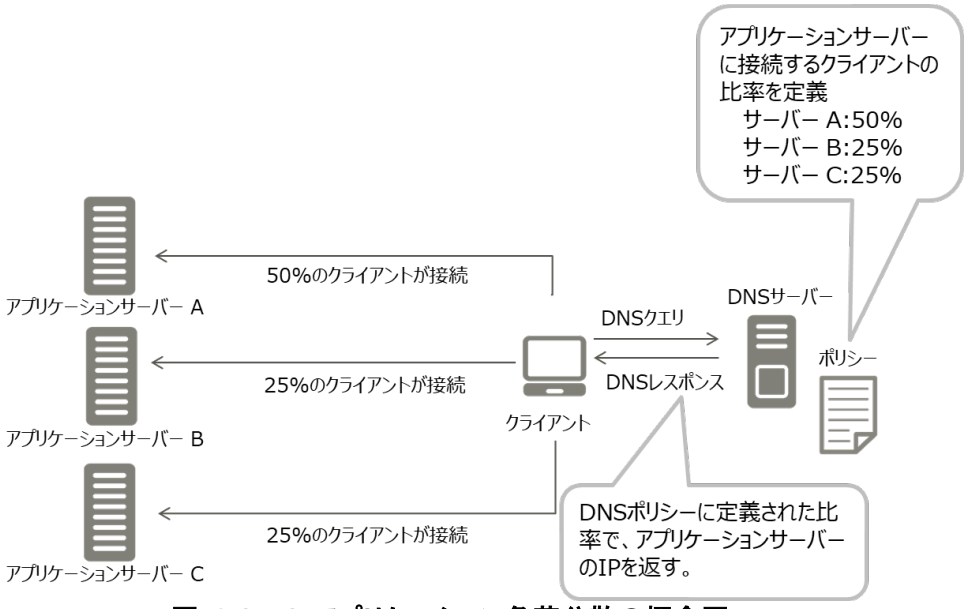


図 2.1.5.1 アプリケーション負荷分散の概念図

参考:アプリケーションの負荷分散に DNS ポリシーを使用する
https://docs.microsoft.com/ja-jp/windows-server/networking/dns/deploy/app-lb

- 場所ベースのトラフィック管理
  Web サーバーが複数の拠点で稼働している環境で、クライアントからの接続要求に対して、クライアントの場所に応じた Web サーバーの IP アドレスを返すように制御できます。

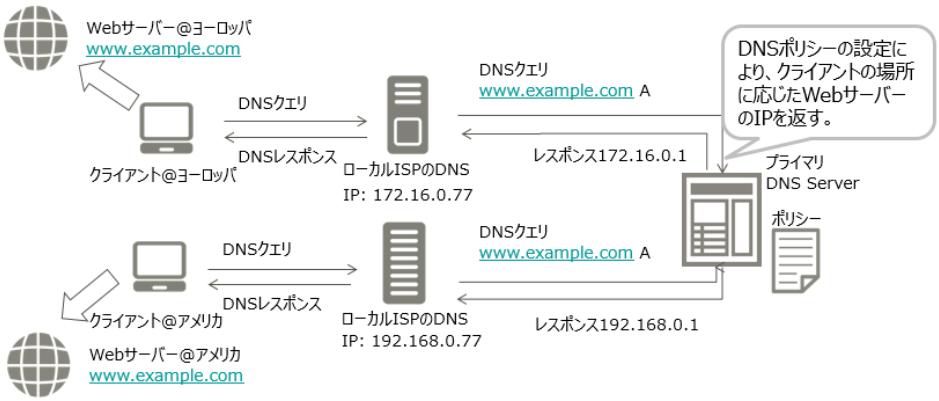


図 2.1.5.2 場所ベースのトラフィック管理の概念図

参考:地理的な場所を認識するアプリケーションの負荷分散に DNS ポリシーを使用する
https://docs.microsoft.com/ja-jp/windows-server/networking/dns/deploy/app-lb-geo

参考:プライマリ-セカンダリの展開での地理的な場所ベースのトラフィック管理に DNS ポリシーを使用する
https://docs.microsoft.com/ja-jp/windows-server/networking/dns/deploy/primary-secondary-geo-location

- スプリットブレイン DNS
  社内、社外のクライアントから接続要求があった場合、社内からの接続要求には社内向けサーバーの IP アドレスを、社外からの接続要求には社外向けサーバーの IP アドレスを返すように制御できます。

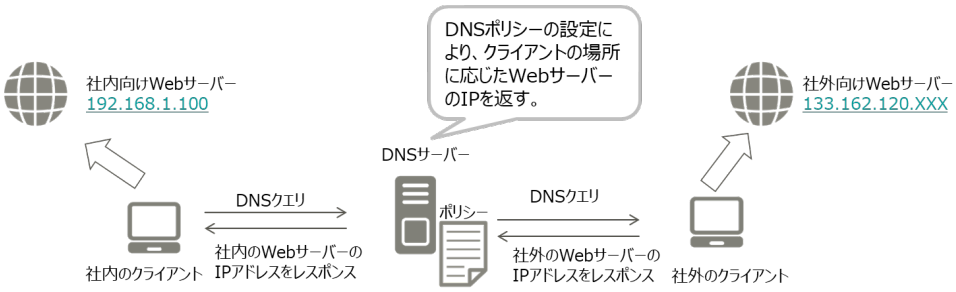


図 2.1.5.3 スプリットブレイン DNS の概念図

参考：Split ブレイン DNS 展開に DNS ポリシーを使用する -
https://docs.microsoft.com/ja-jp/windows-server/networking/dns/deploy/split-brain-dns-deployment

- 時間ベースのリダイレクト
  DNS ポリシーでは、クライアントから接続要求された時間に応じて、接続先のサーバーの IP アドレスを変更するよう定義できます。

  参考： 1 日の時間に基づくインテリジェントな DNS 応答に DNS ポリシーを使用する
  https://docs.microsoft.com/ja-jp/windows-server/networking/dns/deploy/dns-tod-intelligent

- DNS クエリのフィルタリング
  DNS ポリシーでは、指定した条件に基づいて DNS クエリをフィルタリングする「クエリフィルター」を作成して、クライアントからの DNS クエリへの応答を制御できます。
  たとえば、既知の悪意のあるドメインからの DNS クエリをブロックするクエリフィルターを使用して DNS ポリシーを構成できます。

  作成できるクエリフィルターの種類と内容については、以下の Web サイトを参照ください。

  参考：DNS クエリへのフィルターの適用に DNS ポリシーを使用する
  https://docs.microsoft.com/ja-jp/windows-server/networking/dns/deploy/apply-filters-on-dns-queries

2.1.6. Windows PowerShell のサポート

DNS は、PowerShell コマンドレットで管理できます。
各コマンドの詳細については、以下のサイトをご参照ください。

参考：DnsServer
https://docs.microsoft.com/en-us/powershell/module/dnsserver/?view=win10-ps&viewFallbackFrom=winserver2019-ps

2.2. その他の DNS 機能

DNS サーバーの運用において管理者の運用性・管理性を向上させる機能を紹介します。

2.2.1. Best Practices Analyzer(BPA)

BPA は、サーバーマネージャーまたは Windows PowerShell で利用できる機能です。DNS の構成情報をスキャンして、マイクロソフトの推奨構成であるかをチェックできます。
BPA は、DNS の他に Active Directory、リモートデスクトップサービスの構成をチェックできます。

2.2.2. Domain Name System Security Extensions (DNSSEC)

Windows Server の DNS は、DNSSEC に対応しています。
DNSSEC を使用すると、ゾーンやレコードにデジタル署名を施すことができ、なりすましや改ざんといったセキュリティ被害を防ぐことができます。インターネットに置かれる DNS サーバーなどで、高度なセキュリティレベルを必要とする場合に有効な機能です。

Windows Server 2016 で DNSSEC の新しいレコードである Unknown レコード（RFC 3597）がサポートされました。
Unknown レコードを DNS サーバーゾーンに追加することができます

2.2.3. 応答率の制限 (Response Rate Limiting)

本機能は、Windows Server 2016 以降でサポートされています。
DNS サーバーが同じクライアントから複数の要求を受け取った時の応答方法を制御する機能です。これにより、DNS サーバーへのサービス拒否（Dos）攻撃の送信を防ぐことができます。
具体的には以下の構成が可能です。

表 4 応答率の設定項目

項目	説明
1 秒あたりの応答数	1 秒以内にクライアントに同じ応答が与えられる最大回数です
1 秒あたりのエラー数	1 秒以内にエラー応答が同じクライアントに送信される最大回数です
ウィンドウ	要求が多すぎる場合にクライアントへの応答が中断される秒数です
リーク率	応答が中断されたときに、DNS サーバーがクエリに応答する頻度です
TC レート	クライアントへの応答が中断されたときに TCP との接続を試行するようにクライアントに指示するために使用されます
最大応答数	応答が中断されている間に、サーバーがクライアントに対して発行する応答の最大数です
ホワイトリストドメイン	RRL 設定から除外するドメインの一覧です
ホワイトリストサブネット	RRL 設定から除外するサブネットの一覧です
ホワイトリストサーバーインターフェイス	RRL 設定から除外する DNS サーバーインターフェイスの一覧です

応答率の制限の設定は PowerShell を使用します。PowerShell の設定方法については以下 URL を参照してください。

参考：Set-DnsServerResponseRateLimiting
https://docs.microsoft.com/en-us/powershell/module/dnsserver/set-dnsserverresponseratelimiting?view=win10-ps

2.2.4. DANE(DNS-Based Authentication of Named Entities)のサポート

Windows Server 2016 で DANE※がサポートされました。
DNS サーバーでホストされているドメイン名に対して証明書の発行元となる CA を DNS クライアントに指定できます。 これにより、だれかが DNS キャッシュを破壊して、DNS 名を自身の IP アドレスにポイントする man-in-the-middle 攻撃の形態を防ぐことができます。

※認証に関する情報を、DNS を用いて通信するための仕組み（RFC 6394、6698）

2.3. DNS サーバーの構築 

DNS サーバーは、以下の流れで構築します。

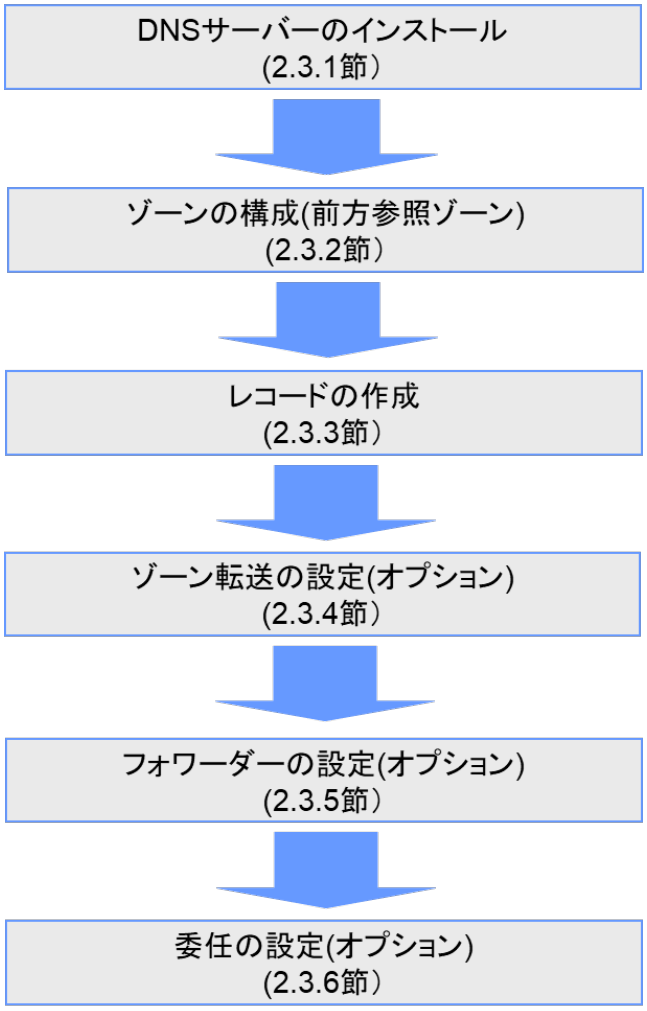
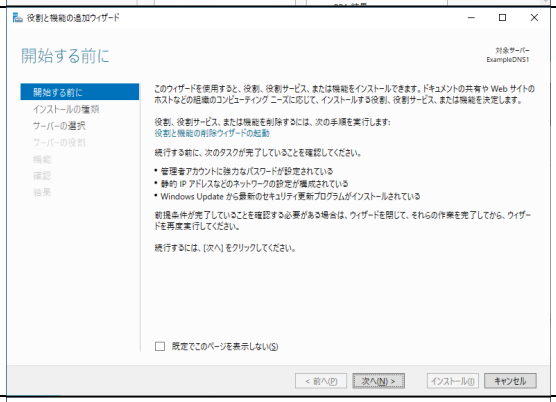
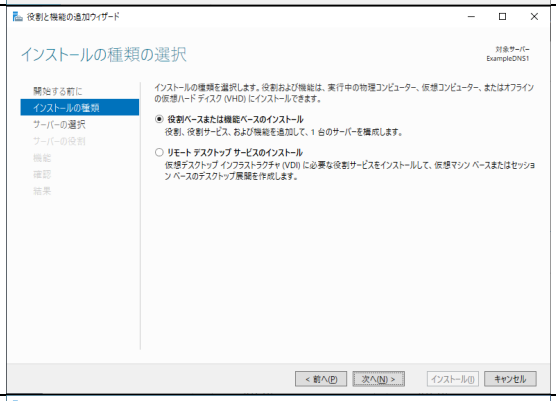
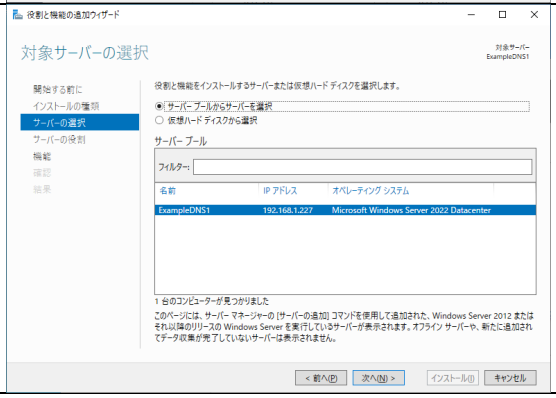


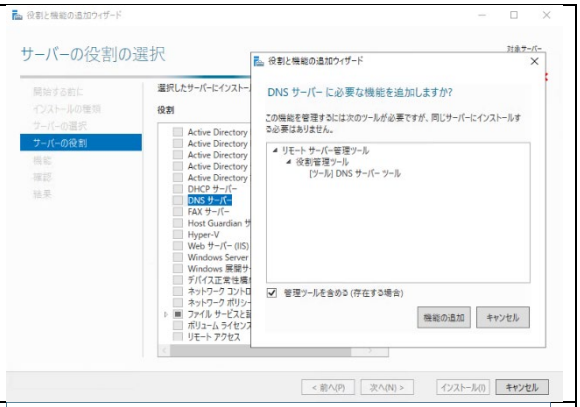
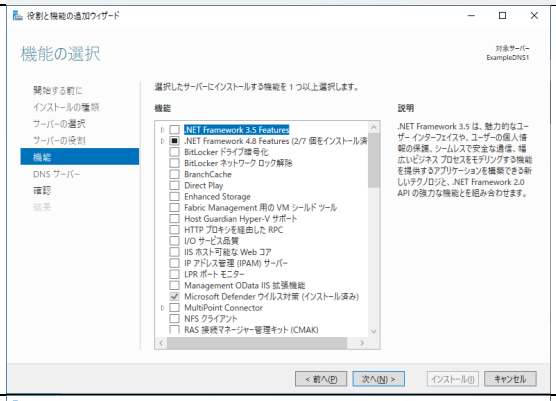
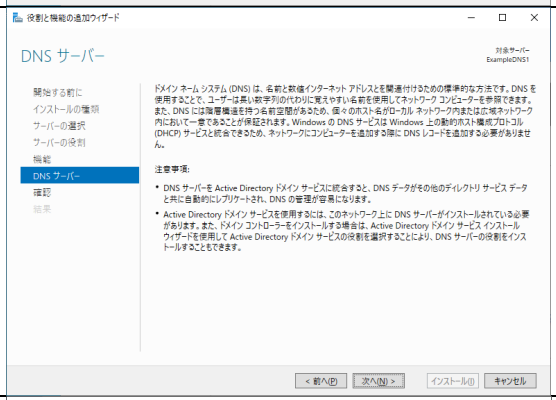
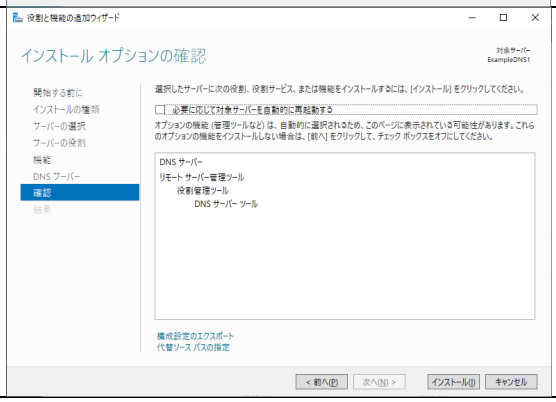
図 2.3.3.1 DNS サーバー構築の流れ

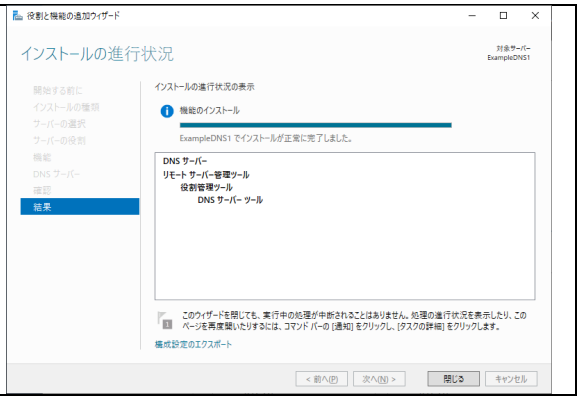
図 2.3.3.1 で紹介した項目以外にも、逆引きゾーン・PTR レコード、GlobalNames ゾーンなどを必要に応じて作成します。作成手順が特殊な GlobalNames ゾーンについては、「付録 5：GlobalNames ゾーン」を参照してください。
なお、DNS サーバーの役割を追加するコンピューターは、静的な IP アドレスを使用する必要があります。

2.3.1. DNS サーバーのインストール

以下の手順に従い、DNS サーバーをインストールします。

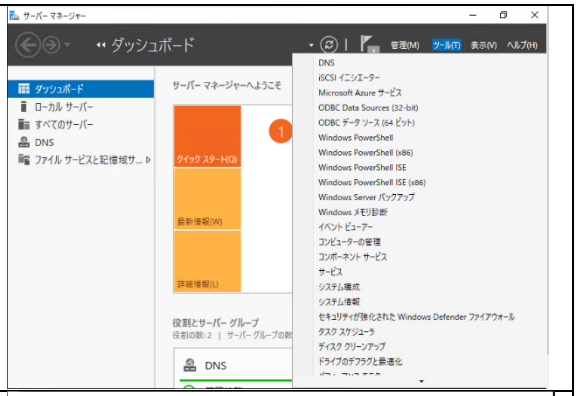
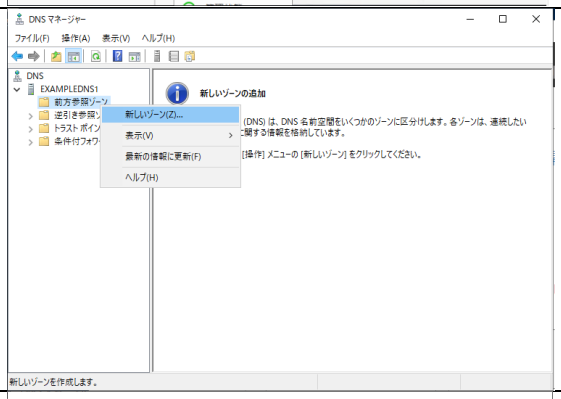
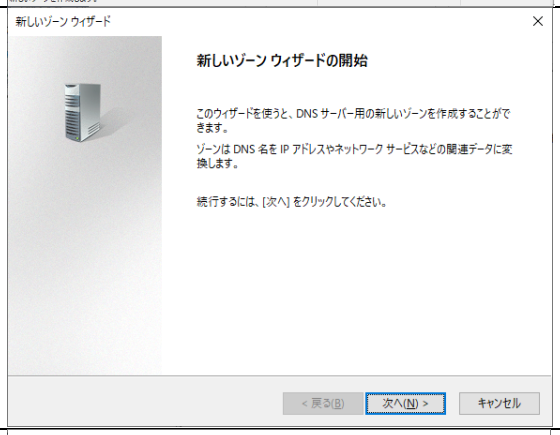
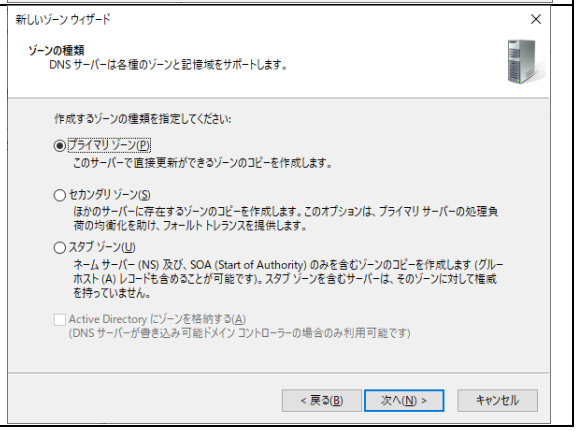
1	[サーバーマネージャー]の[役割と機能の追加]をクリックします。	
2	役割と機能の追加ウィザードが起動して、[開始する前に]が表示されます。 [次へ]をクリックします。	
3	[インストールの種類の選択]が表示されます。[役割ベースまたは機能ベースのインストール]をチェックして、[次へ]をクリックします。	
4	[対象サーバーの選択]が表示されます。 必要に応じてインストール先を選択します。 [次へ]をクリックします。	

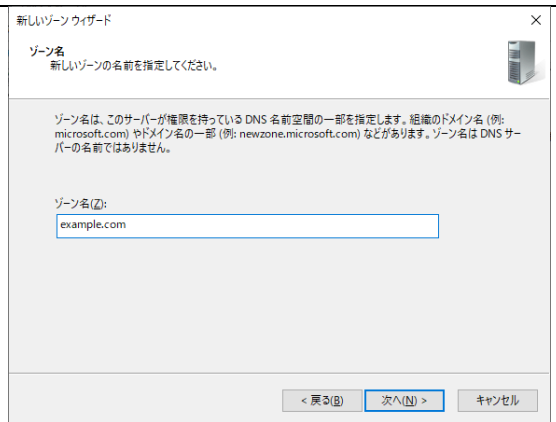
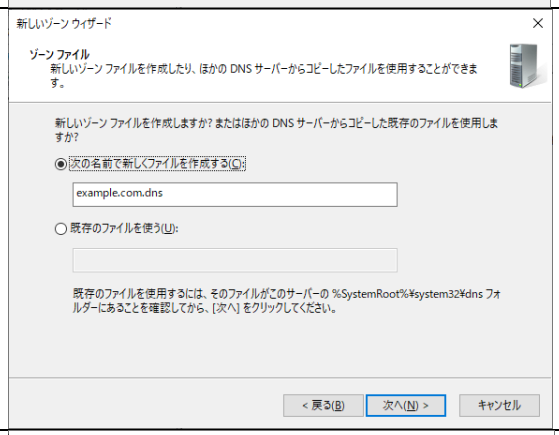
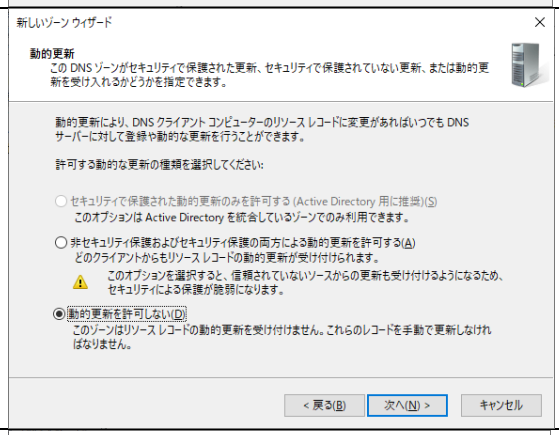
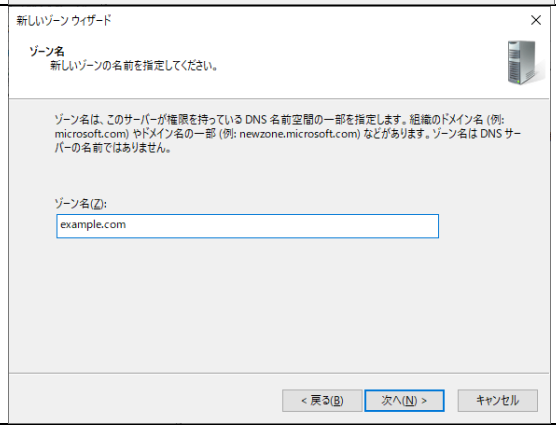
5	[サーバーの役割の選択]が表示されます。[DNS サーバー]をチェックすると、[役割と機能の追加ウィザード]が表示されるので、[機能の追加]をクリックします。 [次へ]をクリックします。	
6	[機能の選択]が表示されます。 [次へ]をクリックします。	
7	[DNS サーバー]が表示されます。 [次へ]をクリックします。	
8	[インストール オプションの確認]が表示されます。 [インストール]をクリックします。	

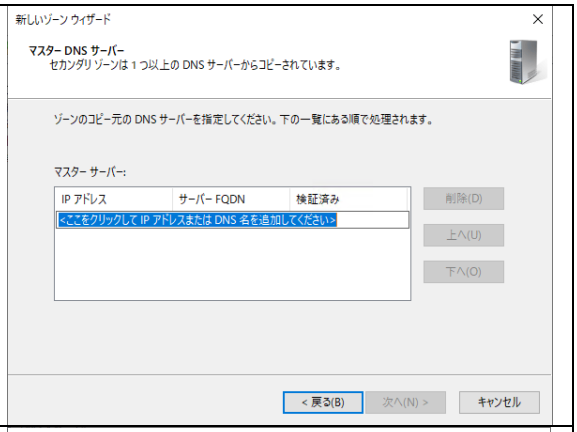
9	[インストールの進行状況]が表示されます。 インストールが完了したら、[閉じる]をクリックします。	

2.3.2. ゾーンの構成（前方参照ゾーン）

ゾーンの構成を DNS マネージャーから行います。

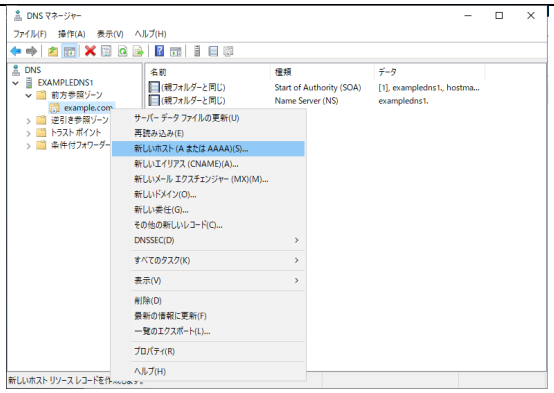
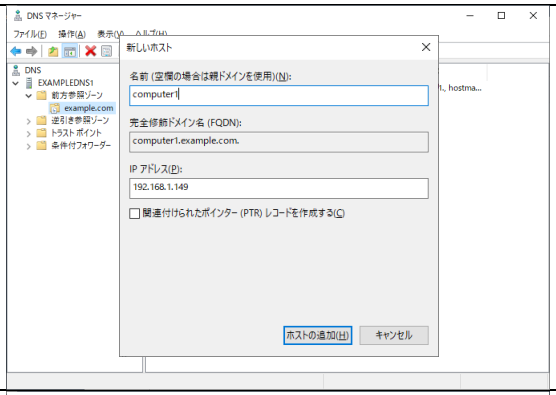
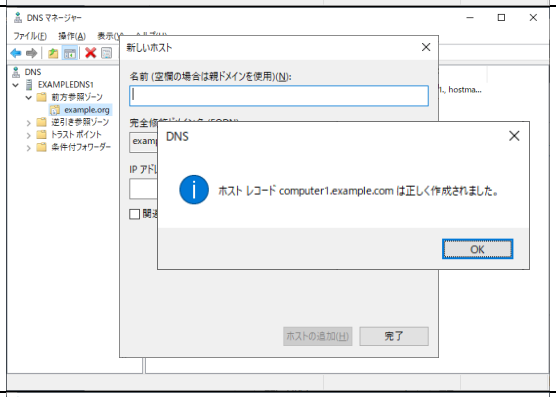
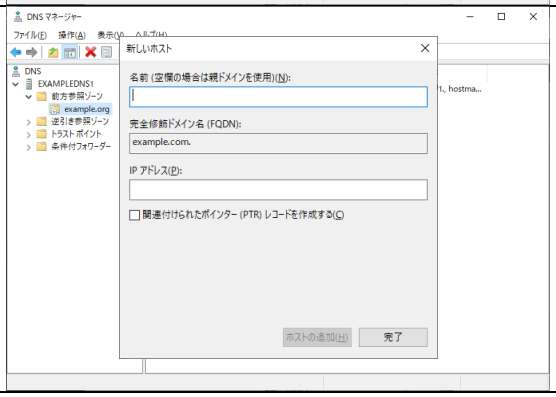
1	[サーバー マネージャー]の[ツール]メニューから[DNS]をクリックします。	
2	DNS マネージャーが起動します。[DNS]-[(サーバー名)]-[前方参照ゾーン]を右クリックして[新しいゾーン]をクリックします。	
3	[新しいゾーン ウィザード]が起動して[新しいゾーン ウィザードの開始]が表示されます。 [次へ]をクリックします。	
4	[ゾーンの種類]が表示されます。構成するゾーンの種類を選択します。 [次へ]をクリックします。 本手順例では、プライマリゾーンの場合と、セカンダリゾーンの場合を説明します。 先にプライマリゾーンの場合から説明します。	

5	プライマリゾーンの場合(1/3) [ゾーン名]が表示されます。[ゾーン名]にゾーン名を入力します。 [次へ]をクリックします。	
6	プライマリゾーンの場合(2/3) [ゾーン ファイル]が表示されます。 [次へ]をクリックします。	
7	プライマリゾーンの場合(3/3) [動的更新]が表示されます。動的更新を許可するかどうかを指定します。 [次へ]をクリックします。 (※)動的更新については、 「2.1.1DNS の動作イメージ」を 参照してください。	
8	セカンダリゾーンの場合(1/2) [ゾーン名]が表示されます。 [ゾーン名]に、他のサーバーに存在するコピー対象のゾーン名を入力します。 [次へ]をクリックします。	

9	セカンダリゾーンの場合(2/2) [マスター DNS サーバー]が表示されます。 [ここをクリックして IP アドレスまたは DNS 名を追加してください]をクリックして、コピー対象のゾーンが存在するサーバーの IP アドレスまたは DNS 名を入力します。 [次へ]をクリックします。	
10	[新しいゾーン ウィザードの完了]が表示されます。 [完了]をクリックします。	

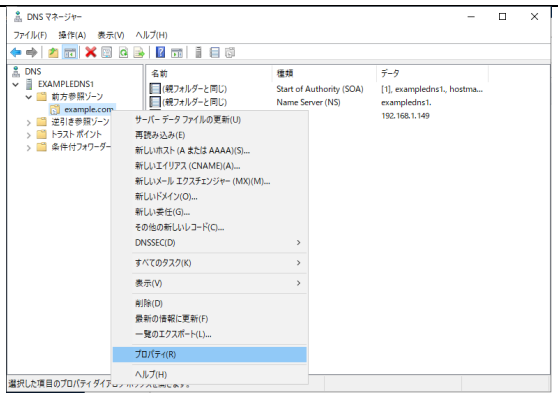
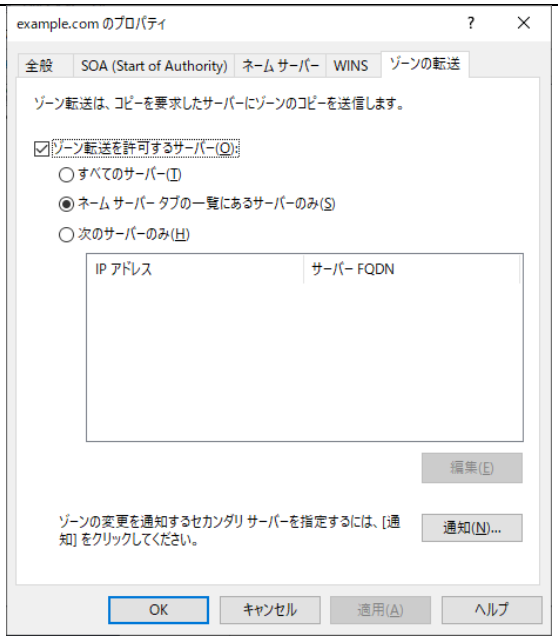
2.3.3. レコードの作成

ホスト名から IP アドレスへのマッピングを行う A レコード(または AAAA レコード)の静的登録や、特殊なレコードを必要に応じて作成します。以下では A レコードの作成手順を紹介していますが、その他のレコードも同等の手順で作成可能です。

1	DNS マネージャーを起動します。 [DNS]-[(サーバー名)]-[前方参照ゾーン]-[(ゾーン名)]を右クリックして[新しいホスト(A または AAAA)]をクリックします。	
2	[新しいホスト]が表示されます。[名前]にコンピューター名、[IP アドレス]に IP アドレスを入力します。 [ホストの追加]をクリックします。	
3	[ホスト レコード (完全修飾ドメイン名) は正しく作成されました。] と表示されます。 [OK]をクリックします。	
4	[新しいホスト]に戻ります。 [完了]をクリックします。	

2.3.4. ゾーン転送の設定 

セカンダリ DNS サーバーを構築後にプライマリ DNS サーバー側からゾーン転送の設定を行います。
セカンダリ DNS サーバーの作成方法は「2.3.2 ゾーンの構成（前方参照ゾーン）」を参照してください。

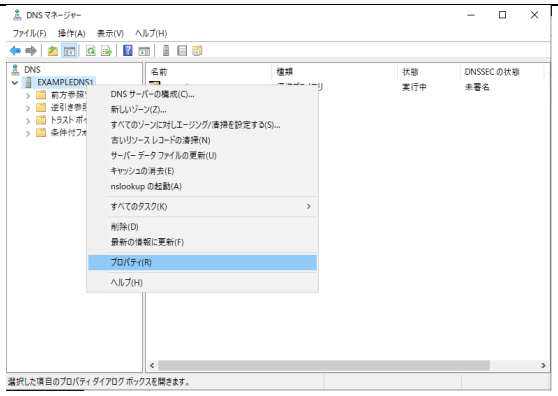
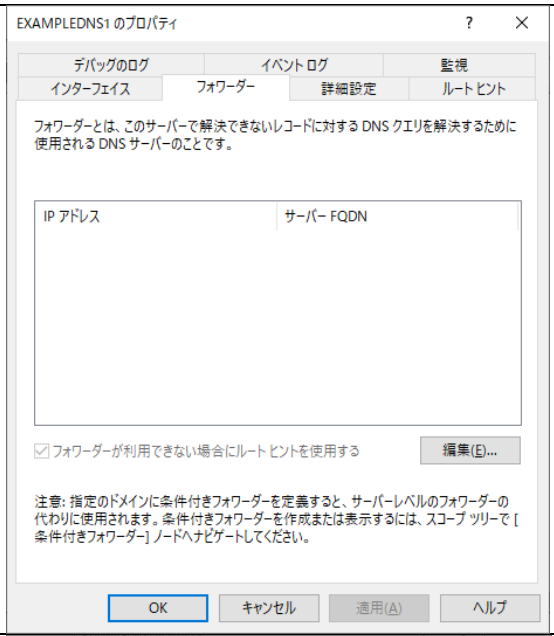
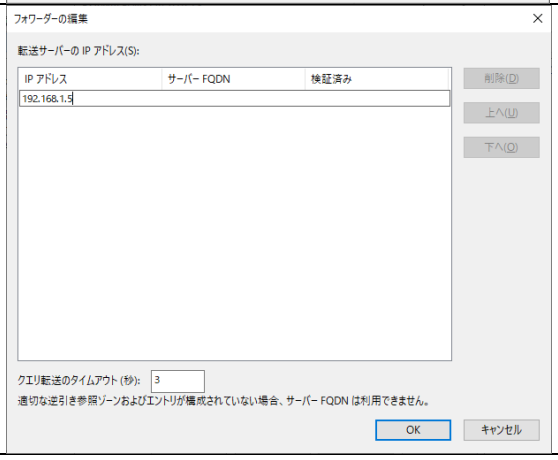
1	プライマリ DNS サーバーの DNS マネージャーを起動します。 [DNS]-[(サーバー名)]-[前方参照ゾーン]-[(転送するゾーン名)]を右クリックして[プロパティ]をクリックします。	
2	ゾーンのプロパティが表示されます。 [ゾーンの転送]タブをクリックして[ゾーン転送を許可するサーバー]チェックボックスをオンにします。 次のいずれかの操作を行います。 ・ すべてのサーバーにゾーンの転送を許可するには、[すべてのサーバー] をクリックします。 ・ [ネーム サーバー] タブに表示された DNS サーバーのみにゾーンの転送を許可するには、[ネーム サーバー タブの一覧にあるサーバーのみ] をクリックします。 ・ 特定の DNS サーバーのみにゾーンの転送を許可するには、[次のサーバーのみ]をクリックして、DNS サーバーの IP アドレスを 1 つ以上追加します。 [OK]をクリックします。	

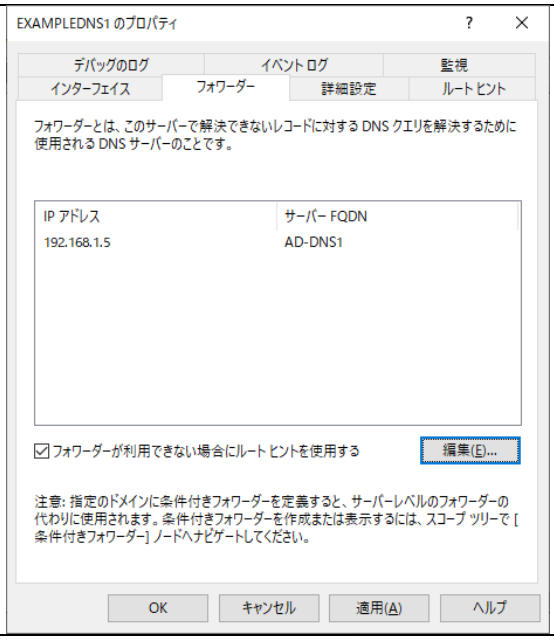
2.3.5. フォワーダーの設定

ネットワーク内部の DNS サーバーで解決できない DNS クエリを転送するために、ネットワーク外部の DNS サーバーをフォワーダーとして設定します。

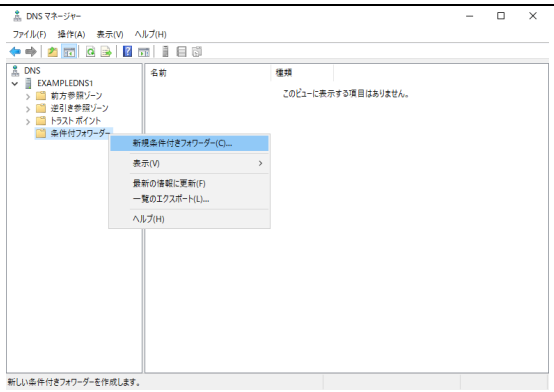
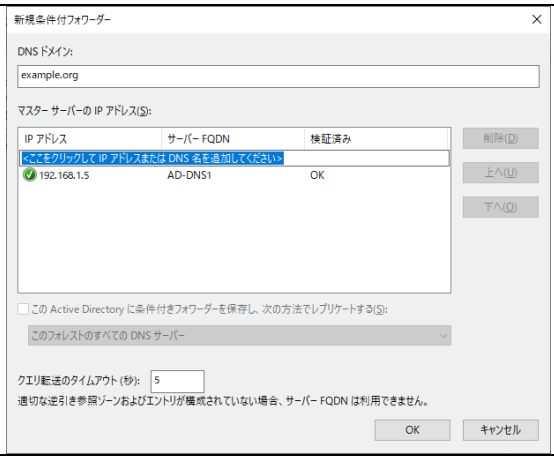
特定のドメインの名前解決のみ DNS クエリを転送する条件付きフォワーダーも構成可能です。

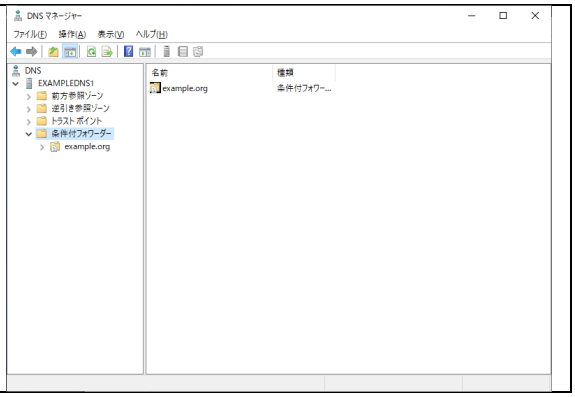
1) フォワーダーの設定

1	DNS マネージャーを起動します。 [DNS]-[(サーバー名)]を右クリックして[プロパティ]をクリックします。	
2	[(サーバー名)のプロパティ]が開きます。 [フォワーダー]タブの[編集]をクリックします。	
3	[フォワーダーの編集]が開きます。 [ここをクリックして IP アドレスまたは DNS 名を追加してください]をクリックして、DNS クエリを転送する DNS サーバー の IP アドレスまたは DNS 名を入力します。 [OK]をクリックします。	

4	[(サーバー名)のプロパティ]に戻ります。 [OK]をクリックします。	

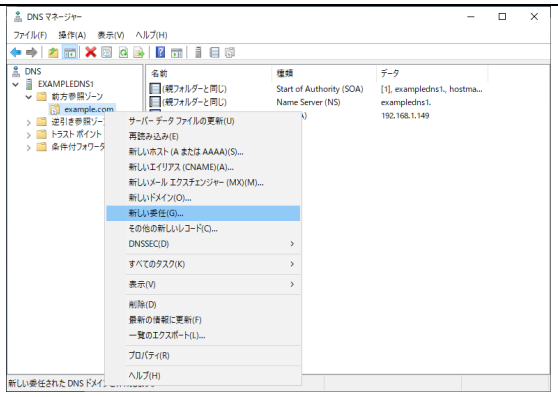
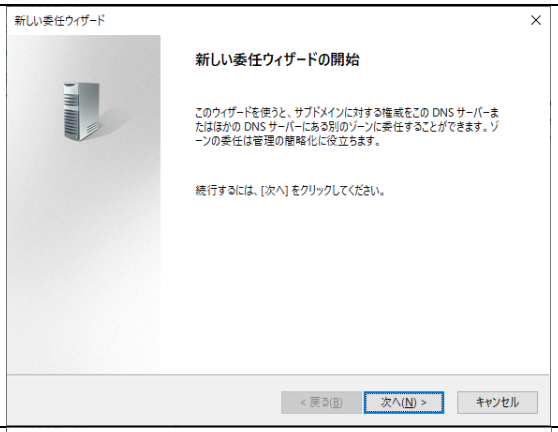
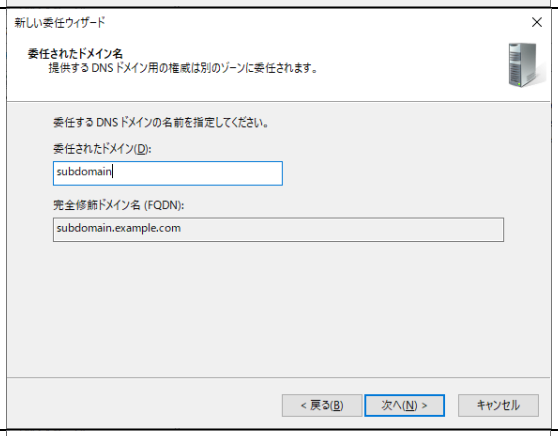
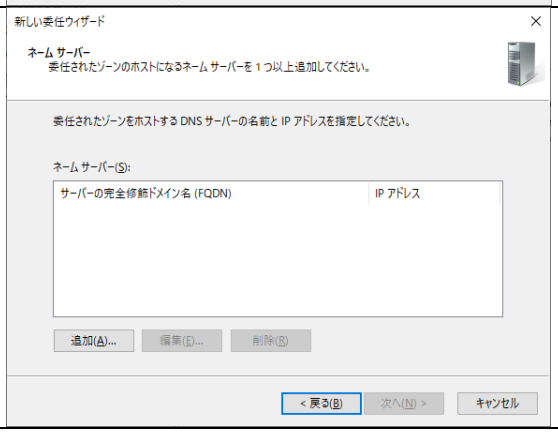
2) 条件付きフォワーダーの設定

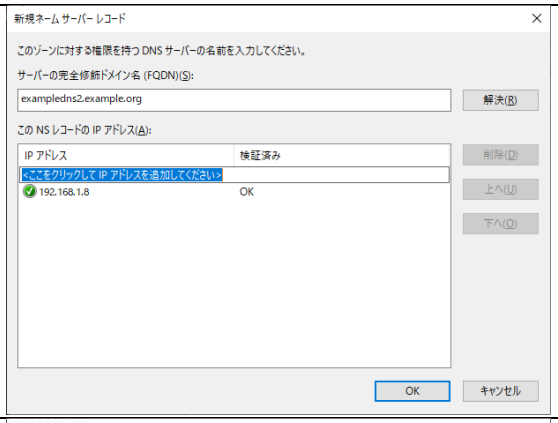
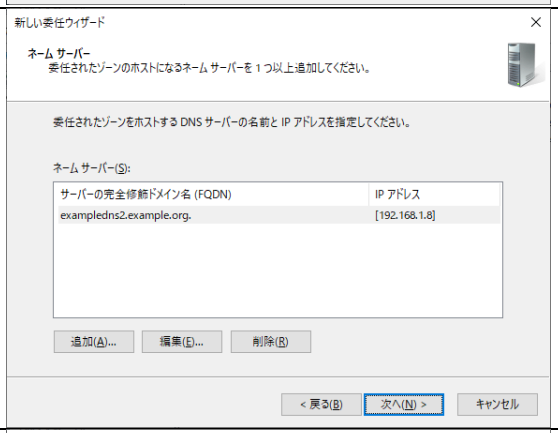
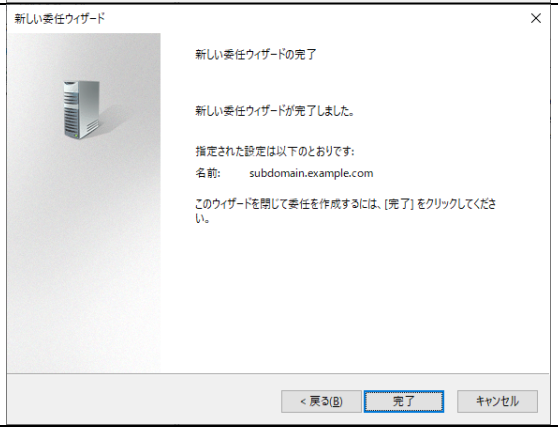
1	DNS マネージャーを起動します。 [DNS]-[(サーバー名)]-[条件付きフォワーダー]を右クリックして[新規条件付きフォワーダー]をクリックします。	
2	[新規条件付フォワーダー]が開きます。 [DNS ドメイン名]に転送したいドメイン名、[マスターサーバーの IP アドレス]に転送したいドメイン名をホストする DNS サーバーの IP アドレスを入力して、[Enter]を押下します。 [OK]をクリックします。	

3	[DNS マネージャー]に戻ります。 [条件付きフォワーダー]配下にドメイン名が作成されたことを確認します。	

2.3.6. 委任の設定 

クエリ要求に対する DNS サーバーの負荷を分散するために、サブゾーンを下位の DNS サーバーで管理するように委任できます。

1	DNS マネージャーを起動します。 [DNS]-[(サーバー名)]-[前方参照ゾーン]-[(委任を作成するゾーン名)]を右クリックして[新しい委任]をクリックします。	
2	[新しい委任ウィザード]が開きます。 [次へ]をクリックします。	
3	[委任されたドメイン名]が表示されます。 [委任されたドメイン]に委任するドメインを入力します。 [次へ]をクリックします。	
4	[ネーム サーバー]が表示されます。 [追加]をクリックします。	

5	[新規ネーム サーバー レコード]が開きます。 [サーバーの完全修飾ドメイン名]に委任するゾーンを管理する DNS サーバーを FQDN で入力します。 その後[解決]をクリックするか、[この NS レコードの IP アドレス]に委任するゾーンを管理する DNS サーバーの IP アドレスを直接入力します。 [OK]をクリックします。	
6	[次へ]をクリックします。	
7	[完了]をクリックします。 委任の設定は完了です。	

2.4. DNS サーバーの運用

2.4.1. エージングと清掃

DNS サーバーを長く運用していると、動的更新で自動登録されたまま削除されずに不要なレコードが大量に蓄積されるケースがあります。そのような場合、データベース容量の肥大化に伴う性能劣化などの問題が起こる可能性があります。長期間残っている不要レコードを削除するために、DNS サーバーはエージングと清掃のしくみを搭載しています。
DNS へレコードを登録した時間またはレコードが更新された時間から、レコードの使用状態を判断(エージング)して、指定された期間使用されていないレコードを DNS から自動的に削除(清掃)します。なお、エージングと清掃は既定で無効となっており、使用する場合は有効化する必要があります。詳細は以下 URL を参照してください。

参考:
How DNS Aging and Scavenging Works
https://social.technet.microsoft.com/wiki/contents/articles/21724.how-dns-aging-and-scavenging-works.aspx

Use Aging and Scavenging
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc754345(v%3dws.10)

2.4.2. DNS サーバーのゾーンのバックアップ/リストア

DNS サーバーのゾーンのバックアップ/リストア方法は、使用しているゾーンの種類によって異なります。

・ Active Directory 統合ゾーンの場合

Active Directory データベース内に DNS ゾーン情報も含まれています。
Windows Server Backup でドメインコントローラのシステムドライブと、システム状態のバックアップを行います。バックアップについての詳細は以下 URL を参照してください。

参考:
Active Directory フォレストの回復ガイド
https://docs.microsoft.com/ja-jp/windows-server/identity/ad-ds/manage/ad-forest-recovery-guide

AD フォレストの回復-完全なサーバーのバックアップ
https://docs.microsoft.com/ja-jp/windows-server/identity/ad-ds/manage/ad-forest-recovery-backing-up-a-full-server

AD フォレストの回復-システム状態データのバックアップ
https://docs.microsoft.com/ja-jp/windows-server/identity/ad-ds/manage/ad-forest-recovery-backing-up-system-state

Backing Up Your Server
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc753528(v=ws.11)

Create Backups of the System State Using a Command Line
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc753201(v=ws.11)

Windows Server 2016 Active Directory 運用管理の考え方
https://jp.fujitsu.com/platform/server/primergy/technical/construct/pdf/win2016-active-directory04.pdf

・ Active Directory 統合ゾーン以外の場合
DNS サーバーに DNS ゾーン情報があります。
Windows Server Backup で DNS サーバーのバックアップを行ってください。

3. 留意事項

3.1. DNS サーバー、DHCP サーバーの役割の追加

DNS サーバー、DHCP サーバーの役割を追加する場合には、コンピューターの IP アドレスを静的に構成しておく必要があります。
静的な IPv4 アドレスを構成していない場合には、"静的な IP アドレスが見つからない"旨の警告メッセージが表示されることがあります。このとき、静的な IPv6 アドレスが正しく構成されていれば問題はありませんので、そのまま継続して役割の追加を行ってください。

3.2. Active Directory 環境での DHCP サーバー承認

Active Directory 環境で IP アドレスを DHCP サーバーから配布する場合、DHCP サーバーはドメインコントローラの承認を受ける必要があります。 Active Directory を展開するネットワークに承認されていない DHCP サーバーが存在している場合、そのサーバーは DHCP サービスを停止します。詳細は以下 URL を参照してください。

参考：More about authorizing DHCP servers in AD DS
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc754493(v=ws.10)

3.3. リレーエージェントのルーター対応について

DHCP のリレーエージェント機能を利用する際は、経由するルーターがリレーエージェント(DHCP/BOOTP プロトコル)に対応していることを確認してください。

3.4. ルートゾーンにおけるフォワーダー設定について

DNS サーバーがルートサーバーとして構成されている(「.」という名前のゾーンを持つ)場合、ルートヒントやフォワーダーを構成することはできません。

3.5. マルチホームコンピューターにおける DNS 動的登録に関する留意事項

マルチホーム（複数 NIC を搭載したコンピューター）の DNS 動的登録について、以下の留意事項があります。

3.5.1. ドメインコントローラの場合

考え方

ドメインコントローラは自分自身が DNS サーバーでもあるため、マルチホームで構成すると、複数の NIC 情報（A レコード）が DNS サーバーに登録されてしまい、名前解決やドメインコントローラの機能に支障が生じます。したがって、基本的にドメインコントローラをマルチホームで構成することは、推奨されていません。

対処

止むを得ずマルチホームでドメインコントローラを構成する場合は、以下の Microsoft 技術情報を参照して、複数の NIC 情報が DNS 動的登録されないように構成してください。必要な対処は以下の 2 点です。

- 特定の NIC 以外は、NIC の設定で動的登録を無効にする
- Netlogon サービスが特定の NIC 情報のみ DNS に登録するように、DNS サービスを構成する

参考：Steps to avoid registering unwanted NICs in DNS on a multihomed domain controller
https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/unwanted-nic-registered-dns-mulithomed-dc

3.5.2. スタンドアロンサーバー、ドメインメンバサーバーの場合

業務ネットワークと管理ネットワークのような、分離された複数のネットワークに接続するサーバーにおいては、それぞれの NIC に適切なネットワーク設定を行ってください。構築中の人為ミスなどで誤って双方の NIC の情報（A レコード）が同じ DNS サーバーに登録されると、名前解決に問題が生じる可能性があります。念のため運用開始前に、関連する DNS 上に当該コンピューターの A レコードが複数登録されていないか確認することをお薦めします。

3.6. マルチホームコンピューターで DHCP サーバーを構築する場合の留意事項

複数 NIC を搭載した DHCP サーバーを利用する場合は、それぞれの NIC に異なるセグメントの IP アドレスを設定して、別の物理ネットワークまたは VLAN に接続してください。
なお、マルチホーム環境に DHCP サーバー機能を持たせることを富士通としては推奨しておりません。

参考： Windows Server におけるマルチホーム構成
https://docs.microsoft.com/ja-jp/archive/blogs/jpntsblog/windows-server-におけるマルチホーム構成

付録1：DHCPv6 におけるアドレス予約

DHCP サーバーで IP アドレスを予約することで、特定のクライアントに同じ IP アドレスを配布できます。
これまで DHCP サーバーで IPv4 アドレスを予約する場合は、MAC アドレスの登録が必要でした。
DHCPv6 において IPv6 アドレスを予約する場合、MAC アドレスの代わりに DUID と IAID という 2 つの ID を登録する必要があります。

(1) DUID(DHCP Unique Identifier)
DUID は、DHCP サーバーとクライアントを一意に識別するための識別子です。DHCPv6 サーバーによる IP アドレスの動的構成後に ipconfig /all コマンドからも確認できます。(図 付録 1.1 参照)
上記コマンドで DUID を確認した場合 00-01-…と表示されますが、DHCPv6 サーバーに登録する際には"-(ハイフン)"抜きで登録します。

(2) IAID(Identity Association Identifier)
IAID は、サーバーとクライアントが関連した IPv6 アドレス群を識別・管理する役割を持ちます。
IAID は IPv6 アドレスの自動構成後に ipconfig /all コマンドで確認できます。(図 付録 1.1 参照)

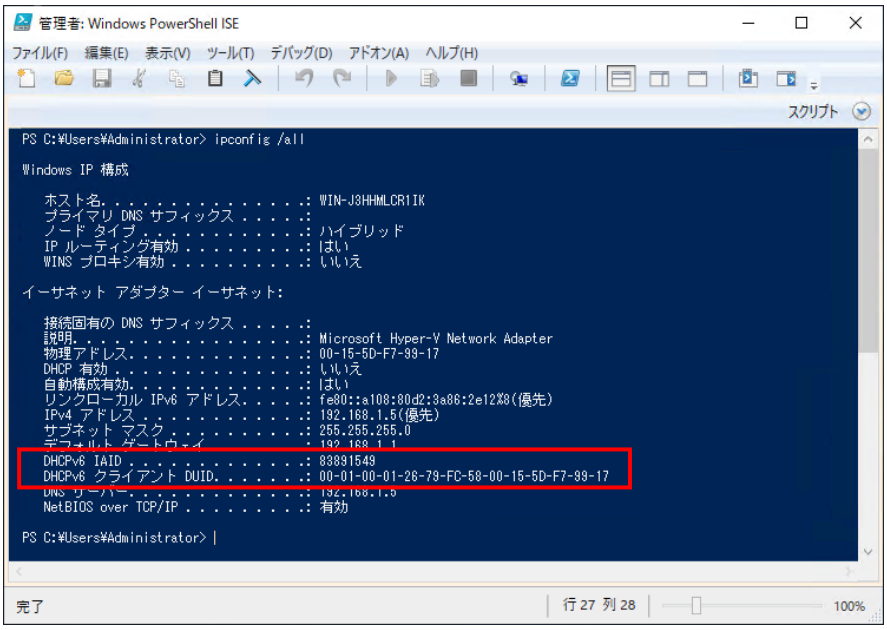


図 付録 1.1 DUID と IAID の確認

参考：その他の DUID、IAID 確認方法
DUID、IAID は、レジストリ エディターを使用して確認できます。各値は以下のレジストリに含まれます。
HKLM¥SYSTEM¥CurrentControlSet¥Services¥Tcpip6¥Parameters

付録2：ルーターアドバタイズに関する補足

ルーターアドバタイズとは、ルーターが定期的に、あるいは要請のあったときに発信する ICMPv6 情報メッセージです。
この情報メッセージには 2 種類のコントロールフラグが設定されており、それぞれのフラグを有効/無効にすることで、クライアントに対して 4 種類のアドレス構成を制御できます。そしてクライアントはこのコントロールフラグに沿った IP アドレスの自動構成を行います。

コントロールフラグは以下の 2 種類あり、組み合わせによって 表5 のようなアドレス構成が行われます。

- M フラグ：管理されたアドレス構成
- O フラグ：その他のステートフル構成（DNS サーバー、NTPサーバーの設定など）

表 5 M フラグ、O フラグの組み合わせと IP アドレス自動構成方法

O フラグ / M フラグ	有効	無効
有効	ステートフルアドレス自動構成	DHCPv6 を利用してアドレスの構成/管理を行うが、その他のネットワーク情報の構成/管理は行わない設定。 ※使用することはほとんどありません。
無効	ステートレスアドレス自動構成	クライアントはグローバルアドレスを自動構成するが、その他の構成は手動構成する場合の設定。 ※非 DHCPv6 環境で使用します。

(1) ルーターの無い環境でのルーターアドバタイズの出し方
一般的に、ルーターアドバタイズは IPv6 対応したルーターが発信します。しかし、ルーターがない環境ではルーターアドバタイズが発信されないため、クライアントがグローバルアドレスを自動構成できません。
このような環境で DHCPv6 サーバーを運用する場合は、インターフェイスの設定を変更してプレフィックス情報を含んだルーターアドバタイズを発信するように設定します。クライアントは DHCPv6 サーバーからのルーターアドバタイズを受けて IPv6 アドレスをステートレス/フルで構成できます。

プレフィックス情報を含んだルーターアドバタイズを発信する設定は以下になります。
→ netsh interface ipv6 set route "*プレフィックス*" interface "*インターフェイス番号*" publish=yes
→ netsh interface ipv6 set interface "*インターフェイス番号*" advertise=enabled

また、ルーターアドバタイズを発信する際には同時にコントロールフラグの設定も行います。
→ netsh interface ipv6 set interface "*インターフェイス番号*" managedaddress=enabled/disabled
→ netsh interface ipv6 set interface "*インターフェイス番号*" otherstateful=enabled/disabled
managedaddress は M フラグを制御して、otherstateful は O フラグを制御します。

(2) ルーターの設定
ルーターアドバタイズの設定は、ルーターの製造元によって異なります。設定方法については各機器の取り扱い説明書を参照、またはサポート窓口にお問い合わせください。

(3) サーバーのインターフェイス構成について
IP アドレスを一意の静的な構成にする場合は、ルーターアドバタイズを受信しないようにインターフェイス設定を変更する必要があります。

以下のコマンドでルーターアドバタイズを受信しなくなります。
→ netsh interface ipv6 set interface "*インターフェイス番号*" router=disabled

(※)上記のコマンドは同様に他のインターフェイスにも適用できますので、IP アドレスの一意性を求められるコンピューターには必ず適用してください。

付録3：IPv6 に関する補足

(1) 128bit のアドレス空間
現在主流の IPv4 は 32bit のアドレス空間で構成され、約 4.3×10^9 個のアドレスを提供できますが、インターネット利用の拡大に伴い、全ての IP アドレスが割り当てられ、新規に IP アドレスを配布できなくなる「IP アドレスの枯渇問題」が発生しています。その問題に対応するために生まれたのが IPv6 です。IPv6 は 128bit のアドレス空間で構成され、約 3.4×10^{38} 個という莫大な数の IP アドレスを提供できます。

以下に IPv6 アドレスの表記ルールを紹介します。

IPv6 アドレス表記ルール

IPv6 で使用される 128bit のアドレスは以下のように表現されます。

- 16bit ずつ":(コロン)"で区切って 16 進数で表記します。
  0001001000110100 0101・・・・・・・・・・・・・・・1011 1100110111101111
  ↓
  1234:5678:90ab:cdef：1234:5678:90ab:cdef

- コロンで区切られたブロック内の先頭に"0"がある場合は、0 を省略できます。ブロック内のアドレスが全て 0 の場合は、"0"と表記します。
  1234:0111:0022:0003:0040:0000:0000:abcd → 1234:111:22:3:40:0:0:abcd

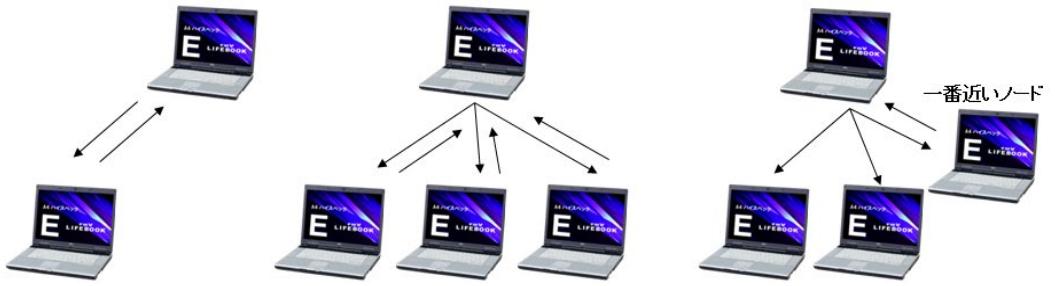
- 0 が連続する場合、1 回に限り"::(ダブルコロン)"で簡略表記できます。
  1234:0111:0022:0003:0000:0000:0000:abcd → 1234:111:22:3::abcd

(2) IPv6 アドレスの種類

IPv6 が使用するアドレスは、ユニキャスト、マルチキャスト、エニーキャストの 3 種類のアドレスがあります。それぞれの違いについては、下記を参照してください。

表 6 IPv6 アドレスの種類

アドレスの種類	説明	
ユニキャストアドレス	ユニキャストアドレスは、NIC に割り当てられる個別のアドレスになります。ユニキャストアドレスの種類は以下になります。	
	①リンクローカルアドレス	FE80::/64 で始まるプレフィックスを使用した IP アドレスで表記されます。このアドレスを用いた通信は、ルーターを越えない同一ネットワーク内でのみ有効です。 また、通常このアドレスはネットワークに接続することで自動的に構成されます。
	②グローバルアドレス	グローバルネットワークで使用可能なアドレスです。ルーターを越えた通信を行うことが可能です。
	③サイトローカルアドレス	サイトローカルアドレスは、企業内など特定の範囲（サイト）で有効なアドレスです。サイト外部からこのアドレスにアクセスはできず、またルーターが外部転送することもありません。(RFC3879 で廃止が決定していますが、代案が採用されるまで使用可能です。)
マルチキャストアドレス	マルチキャストアドレスは、該当するすべてのアドレスに対して送信する送信専用のアドレスです。マルチキャストアドレスを受信したホストは、送信元にユニキャストアドレスで返信します。	
エニーキャストアドレス	複数のホストに同一のユニキャストアドレスを割り当てた場合、このアドレスをエニーキャストアドレスと呼びます。エニーキャストアドレスは、該当するすべてのアドレスに対して送信されますが、マルチキャストアドレスと違い、該当するすべてのアドレスホストの中で最も近くのホストが返信します。	



ユニキャスト
特定のノードを指定したら通信を行う

マルチキャスト
該当するノード全てに発信して、パケットを受信すると個別にユニキャスト返信する

エニーキャスト
該当するノード全ての中で一番近い相手に届きユニキャストで返信される

図 付録 3.1 アドレスの種類による通信の違い

(3) IP アドレスの構成に関する用語

➢ **プレフィックス**

プレフィックスは IP アドレスの一部分を示すものであり、IP アドレスの固定ビットやサブネットを示す際に用いられます。

IPv6 アドレスを入力する際に一緒に入力するプレフィックスの値は既定で 64bit が入力されますが、任意に設定が可能です。任意に値を変更した場合、使用できるインターフェイス識別子の範囲も増減します。

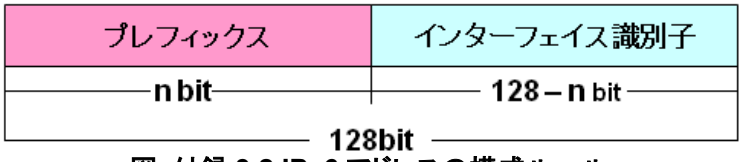


図 付録 3.2 IPv6 アドレスの構成ルール

プレフィックスは、IP アドレスの後に"/(プレフィックスの値)"を加えて表記します。

(例)リンクローカルアドレスのプレフィックス

リンクローカルアドレスは上位 64bit が"FE80:0:0:0"のプレフィックスを持つアドレスです。この場合、リンクローカルアドレスのプレフィックスは、以下のように表記します。

FE80::/64

➢ **グローバルアドレス**

グローバルアドレスは、グローバルルーティングプレフィックスによってサイトを指定します。次にサブネット識別子の部分でサイト内のサブネットを指定します。インターフェイス識別子は個別のインターフェイスを指定します。このように IPv6 のグローバルアドレスは経路集約可能な構造になっています。

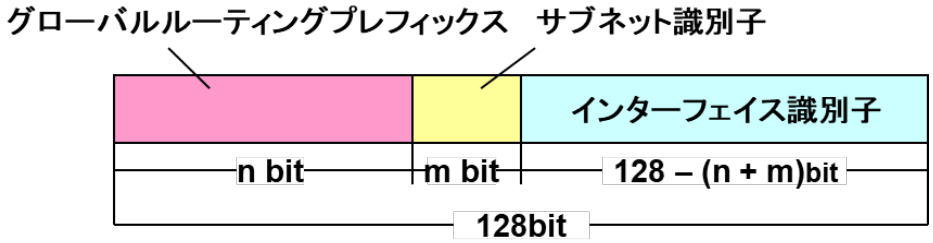


図 付録 3.3 グローバルアドレスの構成ルール

➢ **メトリック値**

コンピューターに複数のネットワーク接続がある場合、メトリック値を設定することで、接続の優先順位を設定できます。メトリック値を手動入力する場合、入力する値が小さいほど優先度が高くなります。メトリック値は既定で"5"に設定されています。

(4) IPv6 アドレスの割り当てについて

以下のアドレスは特別な用途のため、すでに割り当てられています。

- FE80::/64 (自動構成リンクローカルアドレス)
- 2001::/64 (Teredo アドレス)
- 2002::/16 (6to4 アドレス)

付録4：DNS サーバー、クライアント間の名前解決

Windows Server 2016/2019/2022 の DNS サーバーでは、IPv4 および IPv6 の名前解決ができます。

以下に DNS サーバーへの名前解決要求について、各コンピューターの IPv4/IPv6 の実装状況（有効/無効）による動作の違いを紹介します。

表 7 DNS サーバー、クライアント間の名前解決の結果

クライアント ＼ サーバー		IPv6	IPv4/IPv6	IPv4
IPv6	グローバルアドレス	IPv6 ①	IPv6 ①	- ②
	リンクローカルアドレス	- ③	- ③	- ②
IPv4 /IPv6	グローバルアドレス	IPv6 ④	IPv6 ④	IPv4 ④
	リンクローカルアドレス	- ⑤	IPv4 ⑥	IPv4 ⑥
IPv4	-	- ②	IPv4 ⑥	IPv4 ⑥

[凡例] IPv6：IPv6 で通信　　IPv4：IPv4 で通信　　－：DNS 名前解決の通信は行われない

①～⑥は表 7 へのリンクです。名前解決の動作に関する詳細は、番号に対応する「名前解決詳細」欄を参照してください。

表 8 DNS サーバー、クライアント間の名前解決動作の詳細

番号	名前解決詳細
①	名前解決は AAAA レコードのみ可能。A は解決できない(クエリが A レコード宛に出ない)。
②	DNS サーバーと DNS クライアントのプロトコルが異なるため通信できない。
③	DNS 名前解決は失敗。LLMNR、NetBIOS の順で近隣コンピューターの名前解決を試行。
④	A レコード後に AAAA レコードへの問い合わせ、両方のレコードの解決可能。
⑤	DNS パケットは出ない。
⑥	A レコードの解決可能。AAAA レコードは発信されない。

付録5：GlobalNames ゾーン

GlobalNames ゾーンは、DNS で使用できるゾーンの一つであり、WINS(NetBIOS ベースの名前解決)を使用せずに単一ラベルでの名前解決が可能です。GlobalNames ゾーンは IPv4/IPv6 の両環境で利用できます。
以下に GlobalNames ゾーンを使った名前解決の仕組みを紹介します。

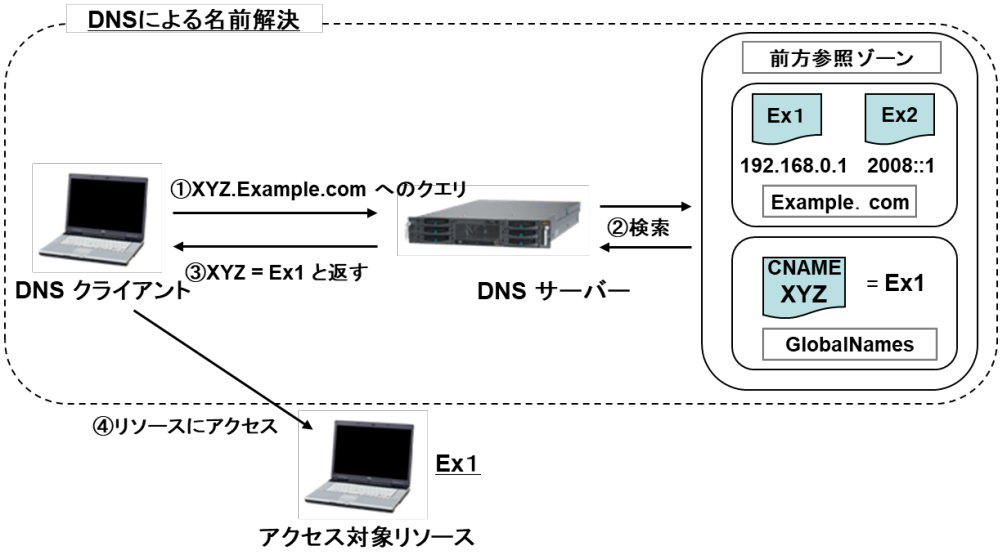


図 付録 5.1 GlobalNames ゾーンを使った名前解決の仕組み

- DNS による名前解決
  ① クライアントは単一名にサフィックスを付け足した FQDN のクエリを DNS サーバーに出す
  ② DNS サーバーは前方参照ゾーンのドメイン(例：Example.com、GlobalNames)を検索
  ③ CNAME レコード、A レコード、IP アドレスを含む応答を返す

- リソースへのアクセス
  ④ アクセス対象リソースにアクセスする

GlobalNames ゾーンには、以下の制限事項があります。
- GlobalNames ゾーンへの動的登録はできない
- 動的な IP アドレスの解決はできない

➢ GlobalNames ゾーンの作成手順
GlobalNames ゾーンは、既定の設定のままでは利用できません。下記手順で GlobalNames ゾーンを作成することで利用可能になります。なお、クライアントの設定は特に必要ありません。

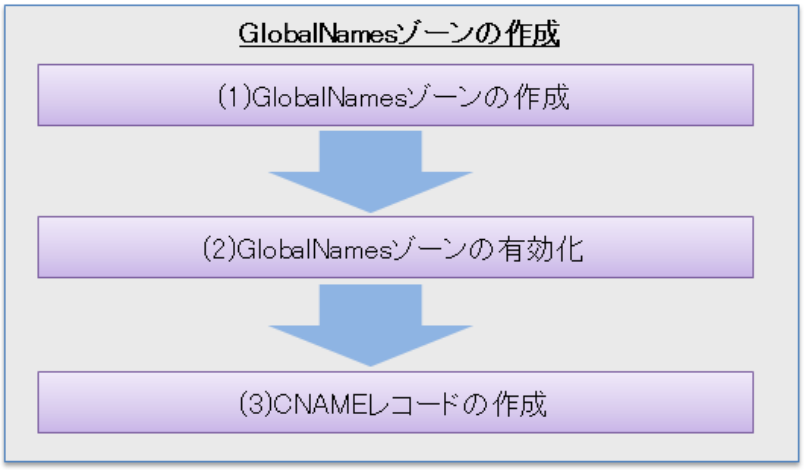
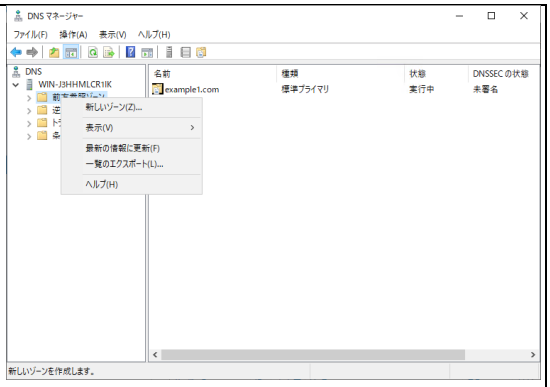
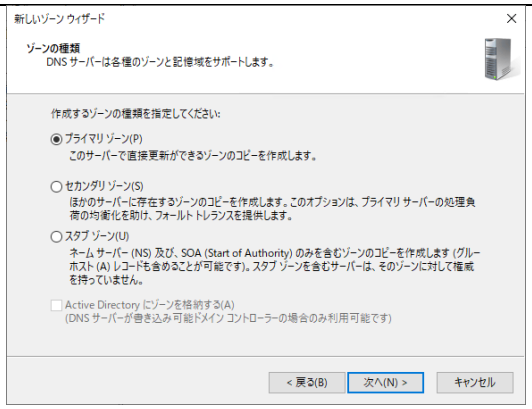
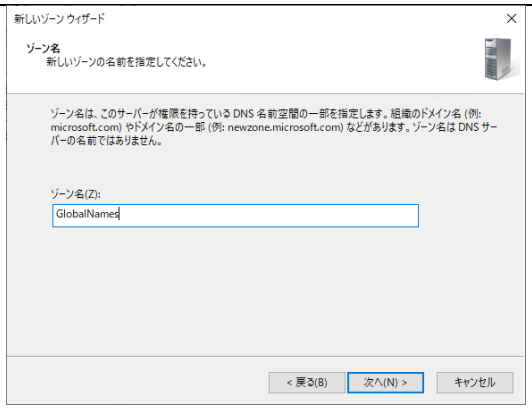
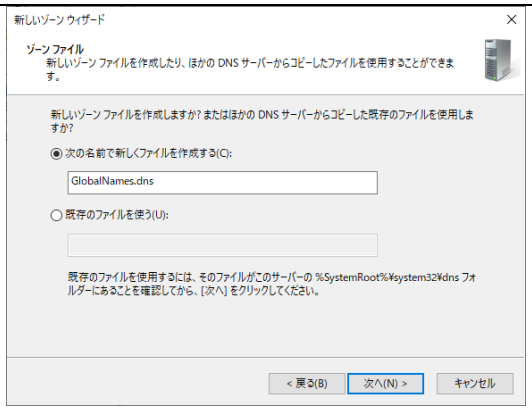
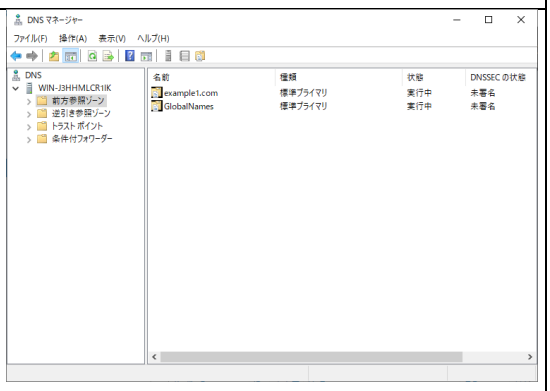


図 付録 5.2 GlobalNames ゾーンの作成手順

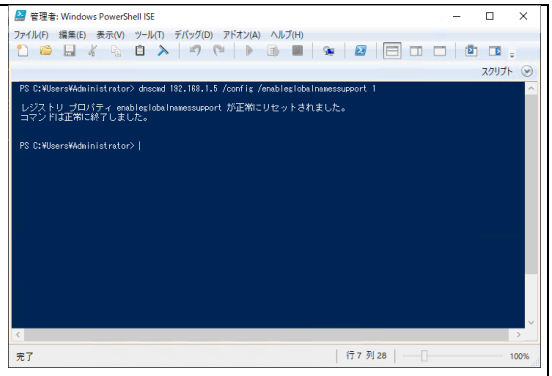
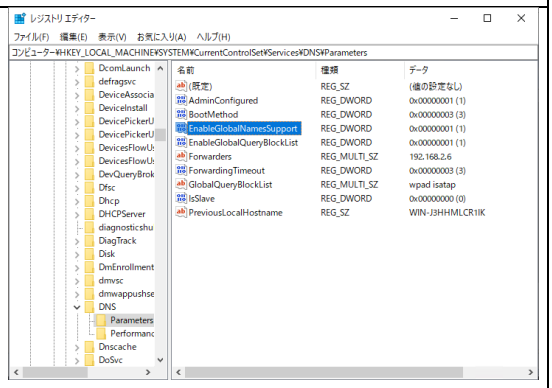
（1） GlobalNames ゾーンの作成

1	DNS マネージャーを起動します。 [DNS]-[(サーバー名)]-[前方参照ゾーン] を右クリックして、[新しいゾーン]をクリックします。	
2	[新しいゾーン ウィザード]が起動します。 [次へ]をクリックします。	

3	[ゾーンの種類]が表示されます。 [プライマリ ゾーン]を選択します。 [次へ]をクリックします。	
4	[ゾーン名]が表示されます。 [ゾーン名]に”GlobalNames”と入力します。 [次へ]をクリックします。	
5	[ゾーン ファイル]画面が表示されます。 [次へ]をクリックします。	
6	[動的更新]画面が表示されます。 [動的更新を許可しない]にチェックを入れます。 [次へ]をクリックします。	

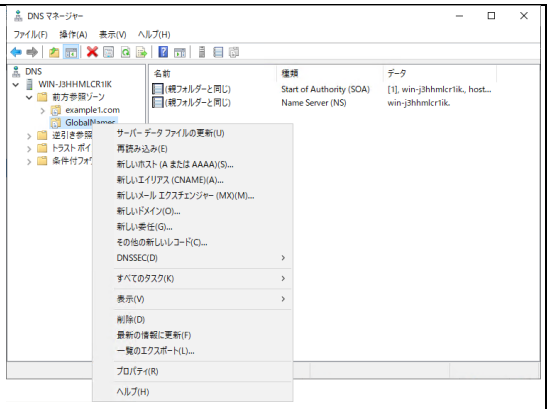
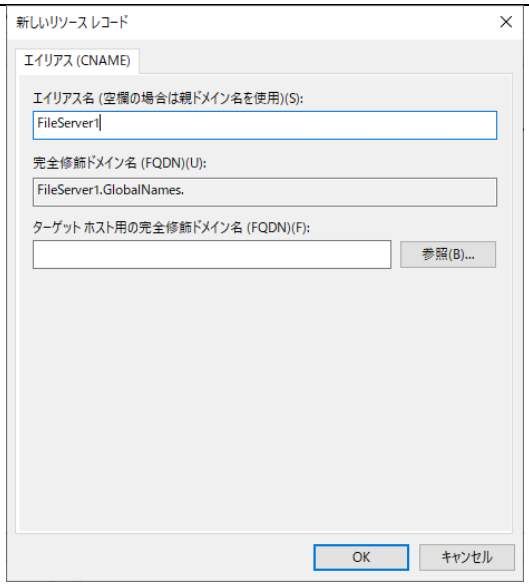
7	[新しいゾーン ウィザードの完了]が表示されます。 [完了]をクリックします。	
8	前方参照ゾーン内に GlobalNames ゾーンが作成されたことを確認します。	

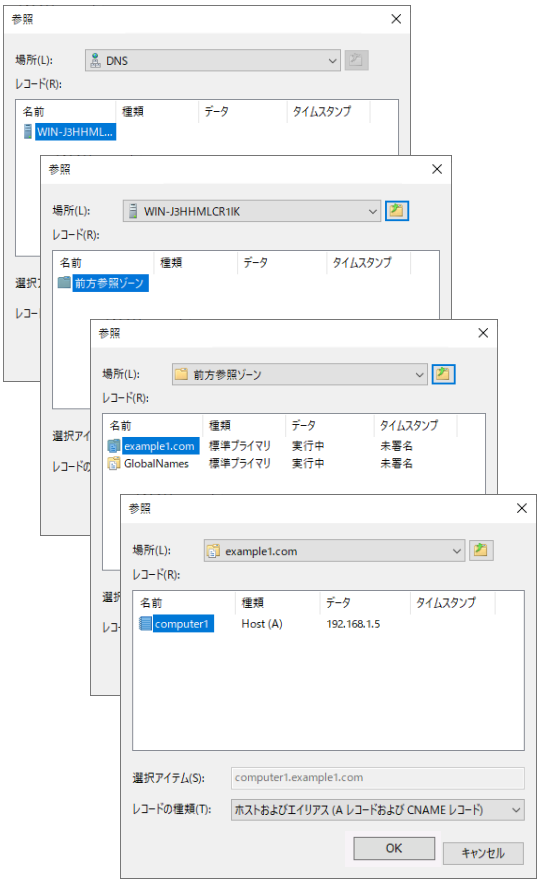
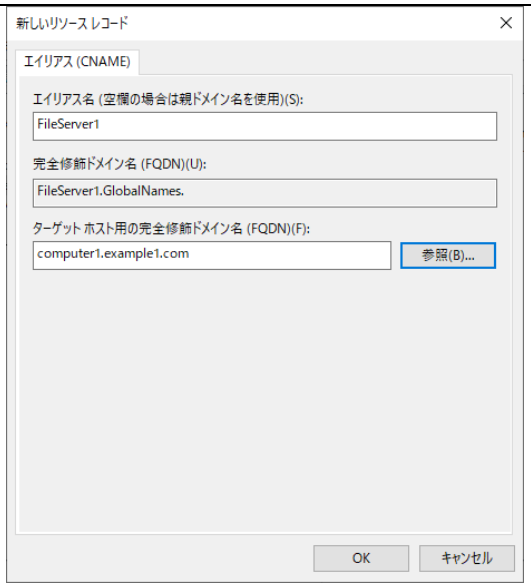
(2) GlobalNames ゾーンの有効化

1	PowerShell を起動して、以下のコマンドを実行します。 **dnscmd <*サーバー名*> /config /enableglobalnamessupport 1** (※) *サーバー名*の部分は IP アドレスでも入力可能です。 (※)以下の PowerShell コマンドレットでも有効化は可能です。 Set-DnsServerGlobalNameZone -Enable $true	
2	コマンドの入力が成功すると、以下のレジストリが追加され、GlobalNames ゾーンが有効になります。 **HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥DNS¥Parameters¥EnableGlobalNamesSupport**	

(3) CNAME レコードの作成

CNAME レコードを作成して、リソースレコード（A や AAAA）へのマッピングを定義することで、単一ラベル名の名前解決を行います。

1	DNS マネージャーを起動します。 [DNS]-[(サーバー名)]-[前方参照ゾーン]-[GlobalNames] を右クリックして[新しいエイリアス(CNAME)]をクリックします。	
2	[新しいリソース レコード]が表示されます。 [エイリアス名]に適当な名前を入力します。 [参照]をクリックします。	

3	[参照]が表示されます。 [サーバー名]-[前方参照ゾーン]-[(参照するゾーン)]-[(参照するレコード(A、AAAA レコードの参照が可能))]と進みます。 [OK]をクリックします。 (※)AAAA レコードを選択する際は[レコードの種類]を[すべてのレコード]に変更します。	
4	[OK]をクリックします。	

付録6：LLMNR(Link-Local Multicast Name Resolution)

DNS サーバーを利用して名前解決ができない場合、LLMNR を使用して、ルーターを越えない同一ネットワーク内に接続されているコンピューターの単一ラベル名で名前解決を行います(IPv4環境では NetBT を利用して名前解決することもできます)。

DNS サーバーからのエラーメッセージ受信後 2 回（IPv4 が有効な場合はさらに 2 回）LLMNR のクエリをマルチキャスト送信します。
LLMNR での名前解決は、DNS と類似した構造をしています。
LLMNR には以下の 5 つの特徴があります。

1.クエリはマルチキャストアドレス宛に発信される
LLMNR クエリはマルチキャストアドレス（IPv6/FF02::1:3、IPv4/224.0.0.252）宛に発信されます（DNS はユニキャストアドレス宛）。
応答はユニキャストで受信します。

2.コンピューター名を解決する
LLMNR は完全修飾ドメイン名(FQDN：Fully Qualified Domain Name)ではなく、単一ラベル名で名前解決します。
例)コンピューター名が"server"というコンピューターがあり、DNS サーバーに"ws2019.example.com"という名前でレコードが登録されていたとしても、LLMNR によって解決できるのは"server"コンピューター名です。

3.ルーターを越えた名前解決はできない
LLMNR パケットのホップ数（IPv4 の TTL に相当）は 1 に設定されているため、ルーターを超えることはできません。

4.使用するポートは UDP ポート 5355
LLMNR は UDP ポート 5355 を使用して通信を行います。

5.LLMNR 名前解決は対応ノード間でのみ有効
LLMNR で名前解決を行うには、通信を行う両ノードで LLMNR をサポートしている必要があります。

付録7：IPv4 ネットワークと IPv6 ネットワークの相互通信

Windows Server 2016/2019/2022 では、IPv6 がサポートされています。
しかし、社内ネットワークでは継続して IPv4 が使用されるケースが多く見られます。このような環境で IPv6 環境との相互通信を考える場合、IPv4 と IPv6 間の通信手段を確保する必要があります。
ここでは、既存の IPv4 ネットワークを利用した IPv6 通信や、IPv4 ホストと IPv6 ホストの通信を確保する以下のトンネリングプロトコルについて紹介します。

- 6to4
- ISATAP
- Teredo

(1) 6to4

6to4 は、IPv6 ネットワークが IPv4 ネットワークを介して他の IPv6 ネットワークに接続する技術です。
6to4 は、IPv6 ネットワークの境界に設置された 6to4 ルーターが、IPv6 パケットを IPv4 パケットにカプセル化することで IPv6 ネットワークの相互通信を提供します。
6to4 のアドレスには 2002::/16 というプレフィックスが割り当てられており、このプレフィックスに続いて IPv4 グローバルアドレスの 32bit を割り当てた合計 48bit のプレフィックスを使用します。そのため、6to4 ルーターのアドレスプレフィックスは IPv4 グローバルアドレスによって一意性が確保されます。
また、6to4 ネットワークからネイティブ IPv6 インターネットに接続する場合は、ネイティブ IPv6 インターネットの境界に設置された 6to4 リレーと呼ばれるルーターに 6to4 ルーターがトンネル接続します。これは IPv6 ホストにカプセル化されたパケットを直接送信しても、元に戻すことができないためです。そのため、一旦 6to4 リレーがカプセル化されたパケットを元に戻して、IPv6 ホストへ改めてパケットを送信します。

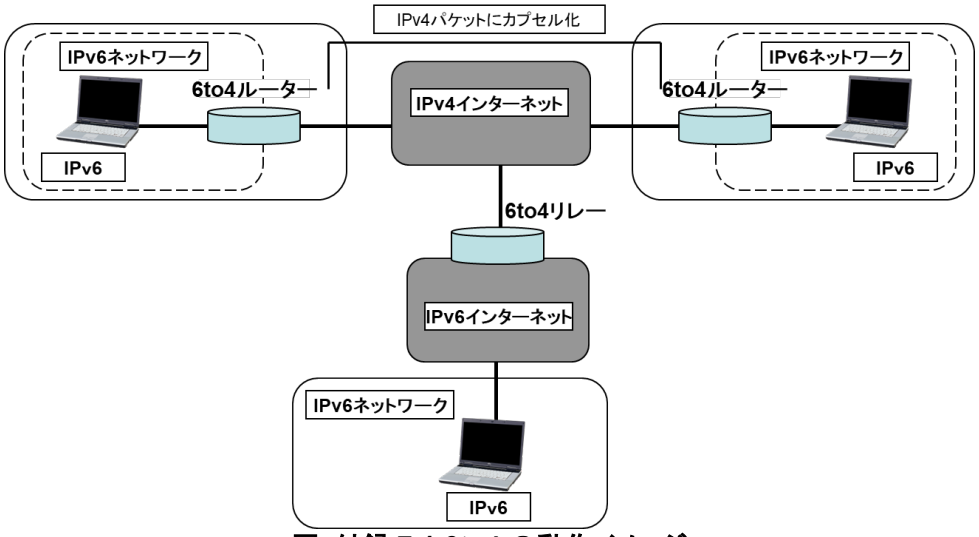


図 付録 7.1 6to4 の動作イメージ

6to4 は、IPv4 ネットワークの中に IPv6 ネットワークが点在するような環境で使用することを想定しています。このような環境では、IPv6 ネットワークの境界に 6to4 ルーターを設置することで、IPv4 ネットワークを介して IPv6 ノード同士が通信できます。
また、6to4 接続は 6to4 ルーターによって自動構成されるため、IPv6 ノードは特別な設定をする必要はありません。ただし、6to4 ルーターは IP アドレスの一意性を確保するために、IPv4 グローバル IP アドレスを保持する必要があります。

(2) ISATAP(Intra-Site Automatic Tunnel Addressing Protocol)

IPv4 ネットワーク内に存在するデュアルスタックホスト(※)は、ISATAP を使って IPv6 インターネットに接続できます。

ISATAP を利用する場合、IPv4 ネットワークに存在するデュアルスタックホストは、まず ISATAP ルーターに IPv4 で接続を行います。ISATAP ルーターから IPv6 アドレスを割り当てられます。その後、ISATAP ルーターとデュアルスタックホスト間は IPv6 over IPv4 トンネルで接続され、ISATAP ルーターから先は IPv6 で通信が行われます。

(※)IPv4/IPv6 を利用して通信可能なホストです。接続先に合わせて利用するプロトコルを選択して通信を行います。

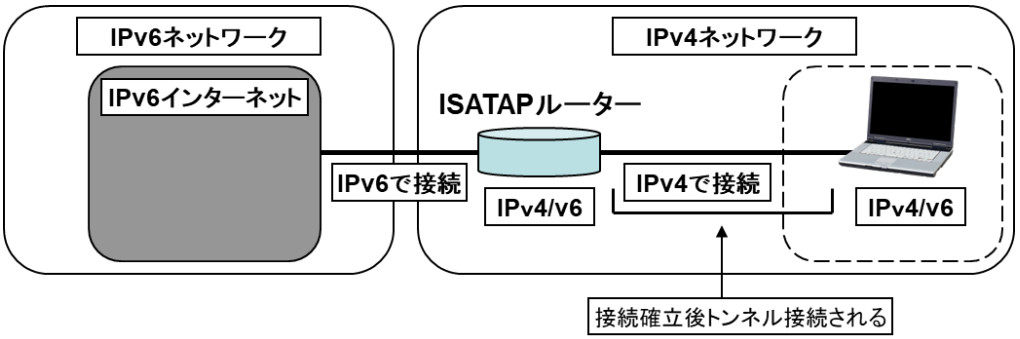


図 付録 7.2 ISATAP の動作イメージ

IPv4 ホストを徐々に IPv6 ホストへ置き換えて行くようなケースで ISATAP を利用すると、スムーズな移行を行うことができます。ISATAP ルーターを用意しておけば、デュアルスタックホストは IPv4 ネットワークの中にあっても IPv6 インターネットに接続できます。

また、ISATAP ルーターはイントラネットのアドレスを使用して構成可能です。

(3) Teredo

Teredo を使用した通信では、パケットが UDP にカプセル化されます。カプセル化されたパケットは、NAT を越えて他の Teredo ノードや IPv6 ホストと End-to-End 通信を行います。また、Teredo を利用する場合、前提条件として Teredo サーバーのアドレスをあらかじめクライアントに設定する必要があります。

Teredo クライアント同士が通信を行う場合、Teredo サーバーを利用してアドレスの構成を行います。このときクライアントは、IPv4/IPv6 のアドレスを相互にマッピングします。

クライアント同士は、マッピングされた情報を元に IPv4 を使用してトンネリング接続を確立して、以降は IPv6 で通信を行います。

また、この接続方法では、クライアント同士がトンネリング接続を行っているため、End-to-End 通信を行うことができます。

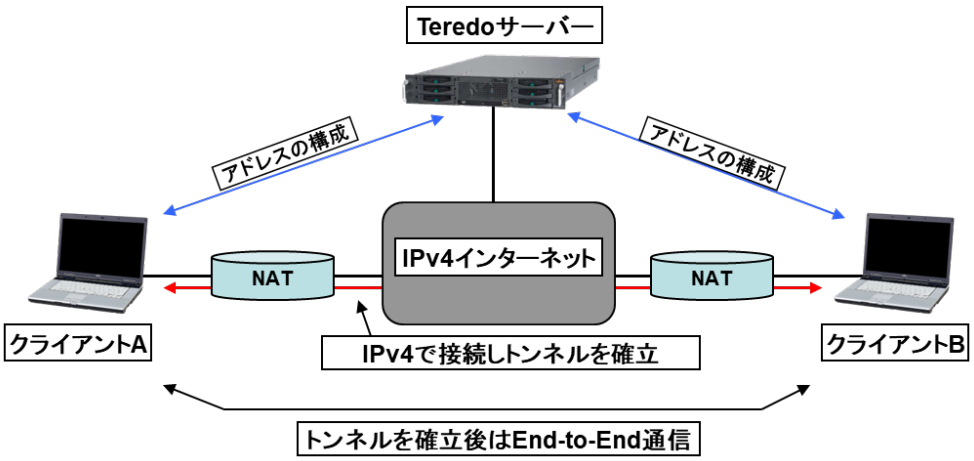


図 付録 7.3 Teredo の動作イメージ

Teredo サーバーの用意、およびクライアントに Teredo サーバーのアドレスを指定する必要がありますが、中継装置として 6to4 / ISATAP ルーターを用意する必要がないため、手軽に IPv6 を利用できます。

ただし、Teredo は IPv6 接続の最後の手段 (last resort) として規定されており、IPv6 グローバル接続、または 6to4 などほかのトンネルサービスが利用可能な場合、そちらを優先して利用するように提案されています。

付録8：IPv4 または IPv6 の使用を中止する方法

IPv4 または IPv6 の使用を中止する場合は、インターフェイスのプロパティで IPv4 または IPv6 のチェックボックスのチェックを外すだけで使用を中止できます。この場合、プロトコルをアンインストールしたわけではありませんので、いつでも再使用が可能です。
特定のプロトコルを利用不可能にしたい場合、IPv4 はアンインストールが可能ですが、IPv6 のアンインストールはできません。ただし、レジストリに値を追加することで利用不可能にできます。

・ IPv4 をアンインストールする方法
IPv4 をアンインストールする場合は、コマンドプロンプトで以下のコマンドを入力します。
C:¥>netsh interface ipv4 uninstall

補足：IPv4 をインストールする場合は、コマンドプロンプトで以下のコマンドを入力します。
C:¥>netsh interface ipv4 install

・ IPv6 を利用不可能にする方法
IPv6 を利用不可能にする場合は、以下のレジストリ値（DWORD）を追加します。値は 0xff です。
キー ：HKLM¥SYSTEM¥CurrentControlSet¥Services¥Tcpip6¥Parameters
名前 ：DisabledComponents
種類 ：REG_DWORD
値 ：0xff

(※)DHCP サーバー側に IPv6 の使用を中止する設定はありません。

参考 ：上級ユーザー向けに Windows で IPv6 を構成するためのガイダンス
https://support.microsoft.com/ja-jp/help/929852

注意：Windows Server 2016/2019/2022 環境で RRAS による VPN やダイヤルアップ接続を使用する場合は、上記方法による IPv6 の完全無効化ではなく、以下レジストリと GUI による無効化を行ってください。

無効化手順
1. トンネルインターフェイスを対象に IPv6 を無効化して、OS を再起動します。
1-1. 管理者権限でコマンド プロンプトを起動します。
1-2. regedit と入力して [Enter] キーを押します。
1-3. 以下のレジストリ設定を行います。

キー ：HKLM ¥SYSTEM¥CurrentControlSet¥Services¥Tcpip6¥Parameters
名前 ：DisabledComponents
種類 ：REG_DWORD
値 ：0x1

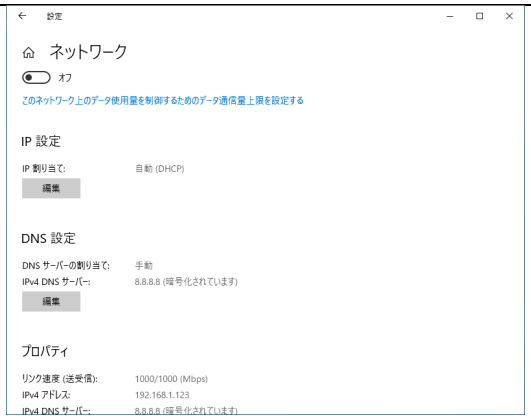
1-4. 設定を反映させるために OS を再起動します。

2. RRAS サーバーの個々の物理インターフェイスのプロパティにて、IPv6 を無効化します。
2-1. 管理者ユーザーでログオンして、コマンド プロンプトを起動します。
2-2. ncpa.cpl と入力して [Enter] キーを押します。
2-3. RRAS サーバーでご利用の NIC を右クリックして、[プロパティ] をクリックします。
2-4. [インターネット プロトコル バージョン (TCP/IPv6)] のチェックボックスを OFF にして [OK] をクリックします。

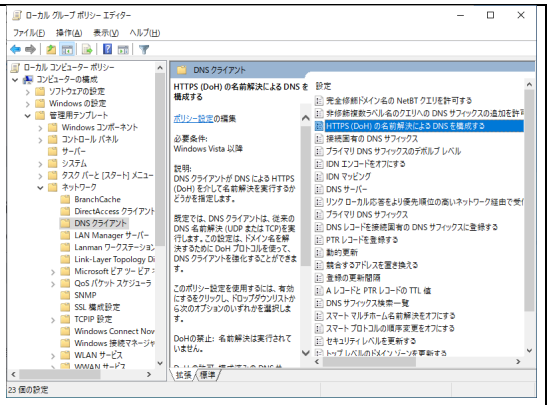
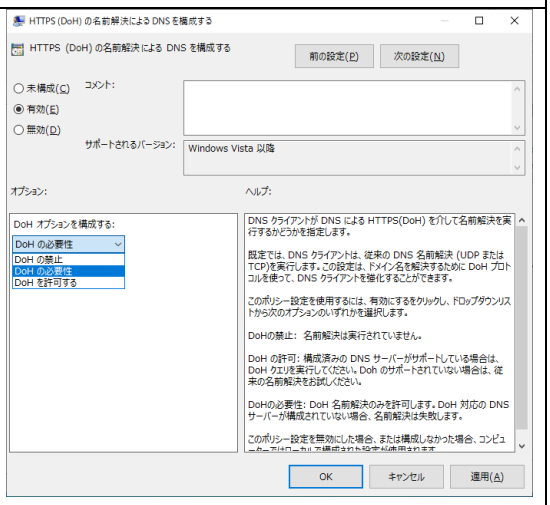
付録9：DNS over HTTPS を使用する方法

Windows Server 2022 の DNS クライアントで、HTTPS プロトコルを使用して DNS クエリを暗号化する DNS over HTTPS (DoH) がサポートされます。DNS データの暗号化により、中間者攻撃による盗聴から通信内容を保護できます。
DoH に対応した DNS サーバーで、かつ Windows Server に登録済みの DNS サーバーを指定している場合に使用可能です。設定の有効化は、GUI、またはグループポリシーを使用して行います。
※なお、Windows Server の DNS サーバーは DoH に対応しておりません。

(1) GUI での設定方法

1	スタートボタンから[設定]を起動します。[ネットワークとインターネット]-[イーサネット]をクリックして暗号化を有効化したい NIC をクリックします。 ※ GUI では NIC ごと、および優先 DNS /代替 DNS それぞれに設定可能です。	
2	[DNS 設定]の[編集]をクリックします。[優先 DNS]に DoH 対応の DNS サーバーの IP アドレスを入力したあと、[優先 DNS 暗号化]の設定を選択して[保存]します。 [優先 DNS 暗号化]の設定として選択できるものは、以下の通りです。 ・[非暗号化のみ] DNS クエリは暗号化されません。 ・[暗号化のみ(HTTPS 経由の DNS)] すべての DNS クエリが HTTPS 経由で暗号化されます。 ・[暗号化優先、非暗号化の許可] DNS クライアントは DoH 暗号化 を試み、失敗した場合は非暗号化 DNS クエリにフォールバックします。	
3	[DNS 設定] の内容が、2 で設定した内容となっていることを確認します。 ・[非暗号化のみ] IP アドレス (非暗号化) ・[暗号化のみ(HTTPS 経由の DNS)] IP アドレス (暗号化されています) ・[暗号化優先、非暗号化の許可] IP アドレス (暗号化優先)	

(2) グループポリシーでの設定方法

1	グループポリシーエディターを起動して、以下を展開します。 [コンピューターの構成] -[管理用テンプレート] -[ネットワーク] -[DNS クライアント] [HTTPS(DoH)の名前解決による DNS を構成する] ※ポリシーではコンピューター単位の設定となります。	
2	オプションとして、以下のいずれかを選択します。 ・[DoH の禁止] DoH を使用しません。 ・[DoH の必要性] DoH を使用してクエリを実行します。 ・[DoH を許可する] 指定した DNS サーバーが DoH をサポートしている場合、DoH クエリを使用します。サポートしていない場合は、暗号化されていないクエリを発行します。 なお、Windows Server の DNS Server サービスは DoH クエリに対応しておらず、「DoH の必要性」を設定すると名前解決に失敗します。このため、ドメインに参加しているコンピューターに対して上記ポリシーは設定しないでください。	

・ Windows Server に登録されている DoH 対応サーバーの確認方法
PowerShell で以下のコマンドを実行することで、Windows Server に登録されている DoH 対応サーバーを確認することができます。

PS C:¥> Get-DnsClientDohServerAddress

2022/1 時点では以下のサーバーが登録されています。

サーバー所有者	IP アドレス
Cloudflare	1.1.1.1 1.0.0.1 2606:4700:4700::1111 2606:4700:4700::1001
Google	8.8.8.8 8.8.4.4 2001:4860:4860::8888 2001:4860:4860::8844
Quad 9	9.9.9.9 149.112.112.112 2620:fe::fe 2620:fe::fe:9

・ Windows に DoH 対応サーバーを追加する方法
PowerShell で以下のコマンドを実行することで、Windows に DoH 対応サーバーを追加することができます。

PS C:¥> Add-DnsClientDohServerAddress -ServerAddress <DNS IP Address> -DohTemplate <URI Template>

参考：Add-DnsClientDohServerAddress
https://docs.microsoft.com/en-us/powershell/module/dnsclient/add-dnsclientdohserveraddress?view=windowsserver2022-ps

PC サーバーFUJITSU Server PRIMERGY につきましては、以下の技術情報を参照願います。

・PC サーバーFUJITSU Server PRIMERGY（プライマジー）
https://www.fujitsu.com/jp/products/computing/servers/primergy/
・FUJITSU Server PRIMERGY 機種比較表
https://jp.fujitsu.com/platform/server/primergy/products/lineup/select-spec/
・FUJITSU Server PRIMERGY サーバー選定ガイド
https://jp.fujitsu.com/platform/server/primergy/products/lineup/select-model/

PC サーバーFUJITSU Server PRIMERGY のお問い合わせ先。

・PC サーバーFUJITSU Server PRIMERGY お問い合わせ
https://www.fujitsu.com/jp/products/computing/servers/primergy/contact/

基幹 IA サーバーFUJITSU Server PRIMEQUEST につきましては、以下の技術情報を参照願います。

・基幹 IA サーバーFUJITSU Server PRIMEQUEST（プライムクエスト）
https://www.fujitsu.com/jp/products/computing/servers/primequest/
・FUJITSU Server PRIMEQUEST 3000 シリーズ　製品ラインナップ
https://www.fujitsu.com/jp/products/computing/servers/primequest/products/3000/
・FUJITSU Server PRIMEQUEST 2000 シリーズ　製品ラインナップ
https://www.fujitsu.com/jp/products/computing/servers/primequest/products/2000/

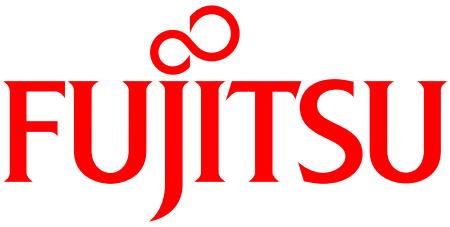
基幹 IA サーバーFUJITSU Server PRIMEQUEST のお問い合わせ先。

・本製品のお問い合わせ
https://www.fujitsu.com/jp/products/computing/servers/primequest/contact/

商標登記について

- Microsoft、Windows、Windows Server、Active Directory、Windows PowerShell は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

免責事項


FUJITSU