FUJITSU Server PRIMERGY
FUJITSU Server PRIMEQUEST

Windows Server 2016 Active Directory 設計指南書

第 1.0 版

2016 年　11 月

富士通株式会社

はじめに

本書は、Fujitsu Server PRIMERGY と Microsoft® Windows Server® 2016 を用いた Active Directory®構築を支援することを目的として、富士通での商談や検証で得たノウハウを指針としてまとめたものです。

本書の目的

本書を読むことで、Active Directory®導入の際のおおまかな考え方を理解していただけます。

本書を利用するにあたっての前提知識

以下の技術情報についての知識が必要となります。

- Active Directory®およびネットワークの基礎知識

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
http://jp.fujitsu.com/platform/server/primergy/technical/construct/

PRIMERGY については、以下のサイトを参照してください。

・PC サーバ FUJITSU Server PRIMERGY（プライマジー）
http://jp.fujitsu.com/platform/server/primergy/

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® 2003	Windows Server 2003
	Microsoft® Windows Server® 2008	Windows Server 2008
	Microsoft® Windows Server® 2008 R2	Windows Server 2008 R2
	Microsoft® Windows Server® 2012	Windows Server 2012
	Microsoft® Windows Server® 2012 R2	Windows Server 2012 R2
	Microsoft® Windows Server® 2016	Windows Server 2016
ドメイン	ドメインコントローラー	DC
	Active Directory®	AD
	Active Directory®ドメインサービス	ADDS
	グローバル カタログ	GC
その他	Windows PowerShell®	Windows PowerShell

改版履歴

改版日時	版数	改版内容
2016.11	1.0	・新規作成

目次

図表目次

1 Active Directory 設計の概要

1.1 設計の指針

Active Directory 導入に際しては通常、設計前に現状把握/分析および要件の整理を実施します。性能面・機能面で要件に適うシステムを構築する上で非常に重要なフェーズです。

- **構成は可能な限りシンプルに**

  Active Directory 設計において、まず念頭に置いておきたいのは、**可能な限りシンプルな構成にする**ということです。ドメイン構成を複雑にすると、トラブルの元になり得るとともにトラブルシューティングも困難になりかねません。まずは、シングルドメイン構成で要件が満たせるかを検討します。
  もちろんシングルドメインで要件を満たせない場合もありますので、本書で示す Active Directory 設計指針から適宜判断して設計してください。

- **基本構成設計は慎重に**

  Active Directory 設計では将来の拡張性も考慮して、構築後にドメイン構成を変更することがないよう設計時に十分な検討が必要になります。
  - Active Directory では、既存ドメインの上位へドメインを追加することができません（図 1.1）。
  - Windows Server 2003 以降の Active Directory ではフォレストルートドメインを除く、フォレストのドメインツリー階層内のドメインを再配置できます。しかし、その手順は複雑であり、変更後にコンピュータの再起動が必要である等の理由から、構築後の変更はできるだけ避けるに越したことはありません。

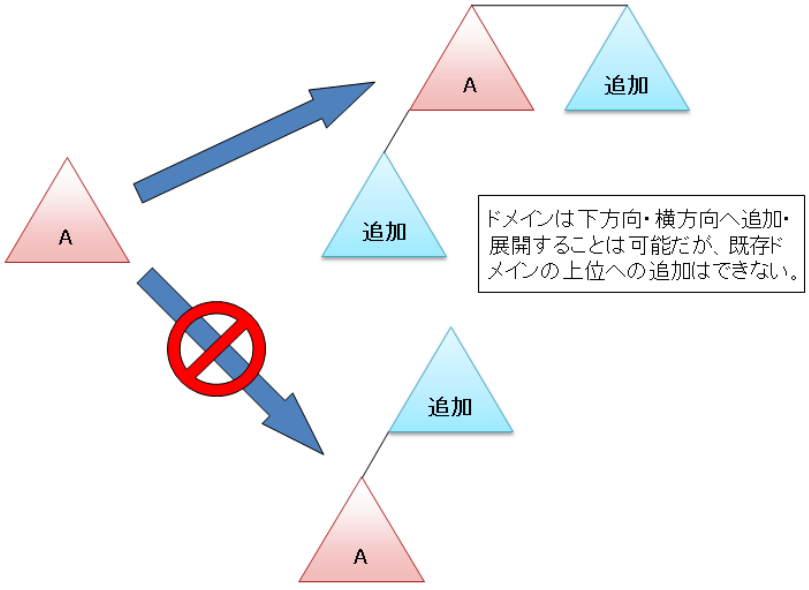


図 1.1 構成ドメインの拡張性

- **既存環境の考慮を忘れずに**

  Active Directory 導入時は既存環境を考慮した設計が必要になります。例えば、既存環境に DNS サーバ（BIND など）がある場合、Windows Server 2016 標準搭載の DNS サーバとの連携を考える必要があります。

1.2 Active Directory設計の流れ

本書では設計作業の流れを通常設計を考える順に記述していますが、実際の設計では、システム要件を満たすために複数の設計要素を絡めて検討しなければいけないケースがあります。最適なシステム設計を行うためには、設計に先立って行うヒアリングで必要な情報をどれだけ広く聞き出せるかが鍵となります。ヒアリングは必要に応じて設計中にも随時行っていきます。

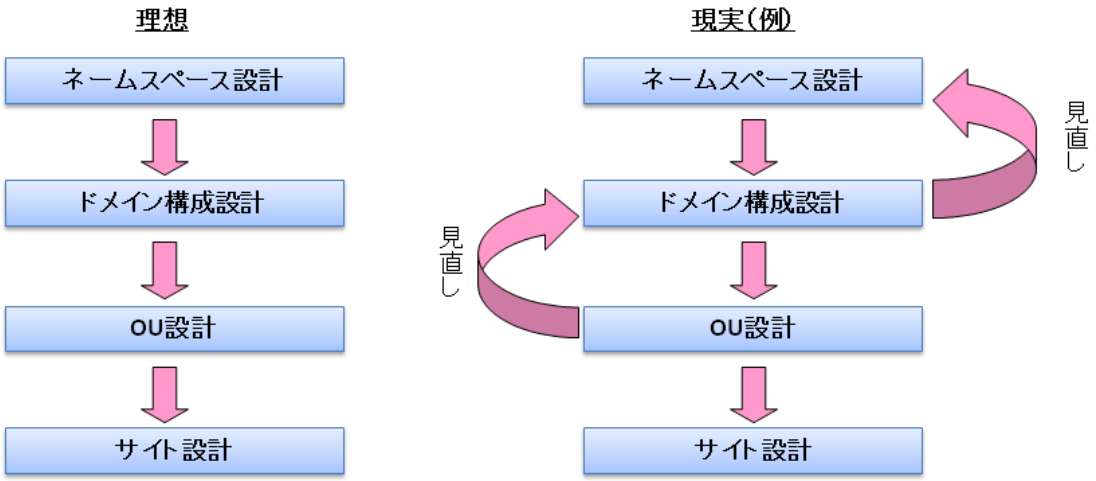


図 1.2 設計作業の流れ(イメージ)

本書では主要なヒアリング項目を示していますが、これが全てではないことに注意してください。設計に必要なヒアリング項目はお客様ごとに異なることを念頭に置き、十分にヒアリングを行うことが必要です。

以下に Active Directory 導入の流れを示します。
本書では、設計に必要なヒアリング、及び設計についての考え方を示します。実際の Active Directory 導入では、これ以外に疑似環境検証や導入作業などがありますが、本書では取り扱いません。

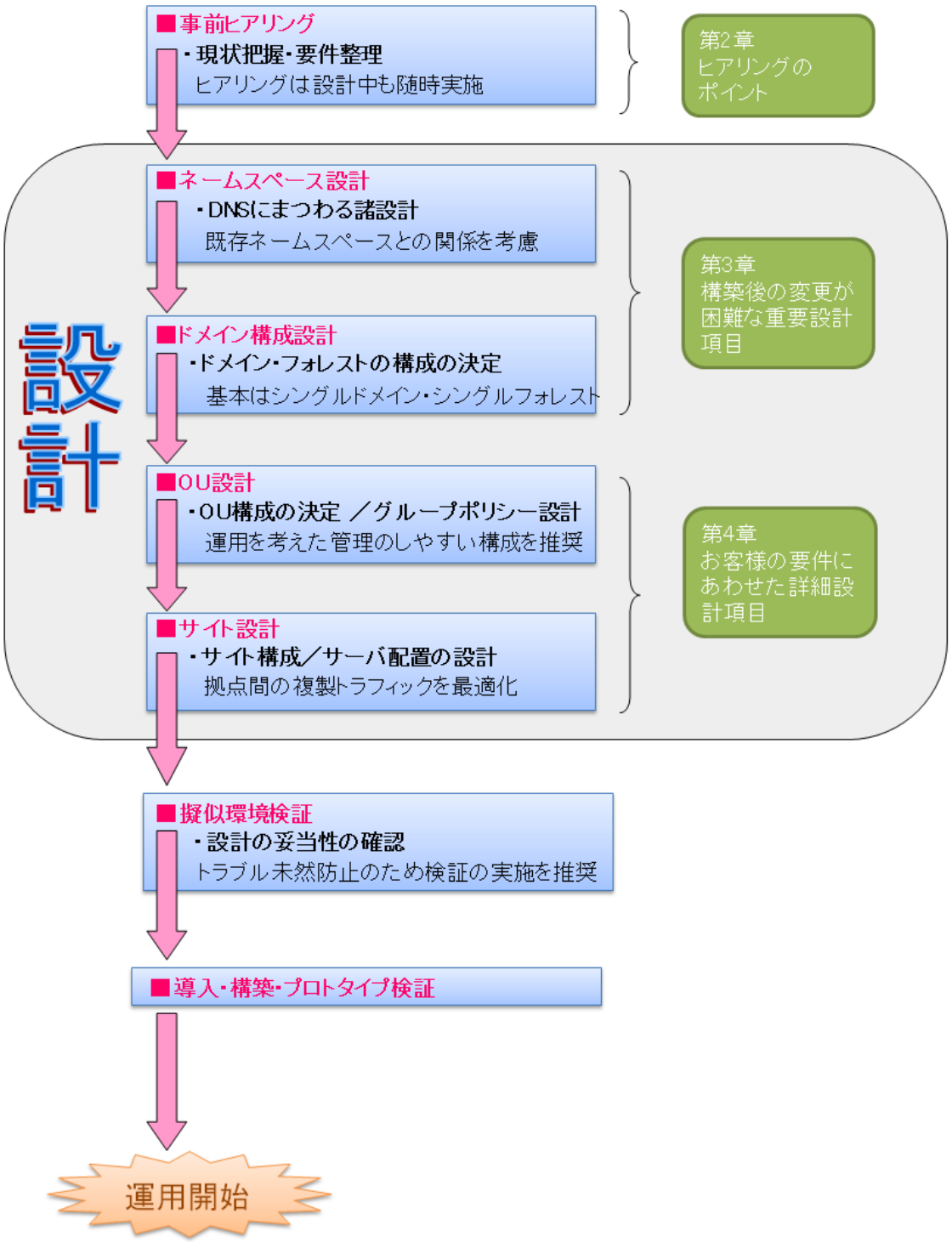


図 1.3 Active Directory 導入の流れ

2 ヒアリングのポイント

以下に Active Directory 設計を行う上で最低限必要なヒアリング項目をあげます。実際のヒアリングにおいては、運用イメージを含めて、お客様と十分なディスカッションを行う必要があります。またグループ ポリシー設計を行う場合は、セキュリティ要件やデスクトップ設計についてのヒアリングも必要となります。グループ ポリシーの詳細は 4.4.1 を参照してください。

表 2.1 ヒヤリングのポイント

カテゴリ	ヒアリング項目	設計項目とのリンク
目的	・導入の目的、必須要件	全般
商談範囲	・Active Directory 導入の対象範囲（グループ会社/全社/部署） ・既存 Active Directory との連携の有無（信頼関係の必要可否）	ドメイン構成
導入計画	・稼動時期	スケジュール
	・将来の Active Directory 導入範囲拡張の可能性 ・ドメインの使用用途 ・利用したい機能、サービス	ドメイン構成
お客様環境（拠点情報）	・拠点毎のサーバ数/クライアント数/ユーザー数 ・現状の OS バージョン（移行の可否） ・海外拠点の有無と Active Directory 統合の可能性 ・物理ネットワーク構成、回線の帯域幅 ・ネットワーク増強の可能性（帯域が細い場合）	ドメイン構成 サイト構成 DC 配置
お客様環境（既存環境）	・既存のサーバ/ドメイン構成 ・移行の必要性（ユーザー/リソース/アクセス権等） ・既存ドメイン/システムの移行/連携の必要性	移行設計
	・既存 DNS 環境 ・社内からのインターネット接続について	ネームスペース
	・イントラネット内での NAT の使用 ・社内ファイアウォールやネットワークフィルタリングの存在	注意事項
	・Active Directory の管理体制（集中管理/分散管理） ・組織改定・人事異動の頻度（異動の範囲も含めて） ・拠点の増減の頻度	ドメイン構成
導入後の運用イメージ	・集中管理の場合、部分的な管理委任の必要性 ・ディレクトリで管理するオブジェクトについての要望 ・グループ ポリシーの適用可否	OU 構成
ビジネス環境	・将来の組織変更（M&A 等）の可能性	ドメイン構成
	・組織構造	OU 構成

その他	・ネットワークトラフィックに関する要望	サイト構成
	・DHCP サービスの利用の有無 ・クライアントの名前解決手段（Active Directory 導入後に NetBIOS 名前解決手段が必要かどうかの見極め） ・タイムサーバの利用の有無 ・ホスト名、IP アドレス、OS の決定	ネットワーク
	・OS 言語バージョンの確認（日本語版でよいことの確認）	全般
	・Active Directory 運用管理の検討 （1） 管理タスクの洗い出し（ルーチンタスク、イベントタスク） （2） 運用管理ツールの導入検討 （3） 管理体制の計画 （4） 運用管理の実施計画 （5） 利用者サポート、障害対策の計画	運用管理

3　構築後の変更が困難な重要設計項目

本章で述べる設計項目は構築後に変更することが困難なため、将来を見据えた十分な検討を行ってください。

3.1 ネームスペースの設計

Active Directory は DNS サーバが必須です。ここでは、Active Directory で使用するネームスペースの設計に関して記述します。

3.1.1 Active Directory で使用する DNS サーバ

Active Directory では、Windows Server 2016 標準搭載の DNS サーバ（以降、Windows DNS サーバ）を使用することを強く推奨します。Windows DNS サーバの Active Directory 統合ゾーンを用いることにより、セキュリティ的にも運用面でも大きなメリットを得ることができます。まれに BIND 等の既存 DNS サーバを用いて Active Directory 構築を検討するケースも見受けられますが、実績が少ない上にメリットも特に無いためお勧めしません。
既存の DNS サーバが存在する場合、Active Directory の DNS としては Windows DNS サーバを使用し、必要に応じて既存の DNS サーバと連携することを推奨します。

Windows DNS サーバ以外を Active Directory で使用するためには、SRV レコードのサポートなど、いくつかの要件を満たす必要があります。

推奨　：　Active Directory の DNS サーバには Windows DNS サーバを使用

3.1.2 DNS サーバのゾーン

Windows Server 2016 DNS サーバのゾーンには以下の 4 種類があります。Active Directory を構築するためには、標準プライマリゾーン、もしくは Active Directory 統合ゾーンの作成が必須となります。構築性・運用性に優れていることから、Active Directory 統合ゾーンを選択することを推奨します。

表 3.1 ゾーンの種類と特徴

ゾーンの種類	特徴
標準プライマリゾーン	DNS においてマスタ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。ゾーンの更新は標準プライマリゾーンから標準セカンダリゾーンへの一方向の複製で行われます。
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最新に保つ ・スタブゾーンのネームサーバー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 おすすめ	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 サーバでレコードの更新・参照が可能です。 ゾーンの更新は Active Directory の複製で行われます。 Windows DNS サーバ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 ゾーン」というゾーンを作成できます。

推奨 ： DNS ゾーンは【Active Directory 統合ゾーン】を使用

WINS（Windows インターネット ネーム サービス）サーバの利用をやめたい、または IPv6 だけのネットワーク構成にしたい（WINS と NetBT は IPv6 対応ではありません）という場合には、すべての名前解決を DNS サーバに移行する必要があります。この移行段階では GlobalNames ゾーンが役立ちます。GlobalNames ゾーンを使用すると、フォレスト全体において一意な単一ラベル名を保持することができるので、単一ラベル名をサポートするために NetBIOS ベースの WINS サーバを使用する必要がなくなります。

3.1.3 Active Directory の DNS 名の決定

DNS 名は運用開始後には変更しないことを念頭に、慎重に決定してください。
Windows Server 2003 以降では Active Directory の再構築をせずに DNS 名の変更が可能になりました。ただし、変更手順が複雑な上、変更後にクライアントの再起動が必要であるなど、あまり現実的ではありません。特にマルチドメイン構成の場合、最上位の DNS ドメイン名は影響が大きいため、Active Directory 構築後に DNS 名を変更することがないように設計を行ってください。

また、Active Directory 導入を考える際に、既存環境に DNS が存在している場合は、既存 DNS と Active Directory で使用する DNS との関係について考慮する必要があります。
大きく分けて表に示す 3 パターンが考えられますが、富士通の実績では、多くの場合②か③で設計を行っています。

表 3.2 既存 DNS を考慮した DNS 名の決定

既存 DNS 名前空間との関係			特徴
①	既存 DNS と連続した名前空間	既存の DNS ゾーンをそのまま使用	・既存環境への影響が大きい ⇒ 大規模環境の場合、社内調整が大変 ・既存 DNS が、Windows DNS サーバ以外（BIND 等）の場合、Active Directory と統合したゾーン管理ができない ⇒ 既存 DNS を Windows DNS サーバで置き換えが必要となる可能性があります
② おすすめ		既存 DNS ゾーンの下に Active Directory 用のゾーンを作成	・既存環境への影響が小さい ・ドメイン名が長くなるという短所有り
③ おすすめ	独立した名前空間	既存 DNS とはフォワーダ、ルートヒントを用いて連携	・既存環境への影響は最小 ・インターネット DNS からの参照を許さない設定にすることでセキュリティ確保が可能

既存の DNS ゾーンをそのまま使用することは、推奨しません。

3.1.4 既存 DNS 環境との連携

導入する環境によっては、既存 DNS サーバとの連携が必要になる場合があります。フォワーダやルートヒントを用いて連携を行うことにより、新規にルートドメインとして Windows Server 2016 の DNS サーバを導入した場合でも、既存の DNS ドメインやインターネットへの名前解決が可能になります。

- **フォワーダ**
  クライアントからの DNS クエリのうちローカルゾーンで解決できない場合に、フォワーダ先に設定されている DNS サーバに名前解決の依頼をする機能です。

- **ルートヒント**
  DNS ネームスペースにおいて、より上位レベルのドメインや他のサブツリーを管理する DNS サーバを、再帰クエリを利用して発見する機能です。

Windows Server 2016 の DNS サーバでルートゾーンを管理している場合、フォワーダおよびルートヒントは動作しません。これらの機能を使用する場合は、ルートゾーンを削除する必要があります。

3.1.5 NetBIOS の名前解決の設計

レガシークライアントおよび NetBIOS 依存アプリケーションが存在する場合は、NetBIOS の名前解決の設計が必要になります。NetBIOS の名前解決には以下の方法があります。管理コスト面などを考慮して、WINS による名前解決を行うように設計することを推奨します。

- **WINS による名前解決**
  WINS は NetBIOS 名と IP アドレスのマップを動的に更新するデータベースです。動的に更新するため、DHCP で IP アドレスを割当てられたクライアントに対する名前解決も容易に行えます。

- **LMHOSTS による名前解決**
  LMHOSTS は NetBIOS 名を IP アドレスにマップする情報ファイルです。NetBIOS 名と IP アドレスを LMHOSTS に登録することで、名前照会ブロードキャストを送信せずに名前解決が行えます。しかし、LMHOSTS は各ローカルコンピュータに保存するため、運用管理が大変になります。

- **ブロードキャストによる名前解決**
  ローカルネットワーク上に名前解決要求をブロードキャストし名前解決を試みます。ブロードキャストはルータを越えないため、ルータより先のネットワークに存在する NetBIOS 名の名前解決はできません。また、ブロードキャストはネットワークの帯域を圧迫する恐れがあります。

- **GlobalNames ゾーンによる名前解決**
  Windows Server 2008 以降の DNS では GlobalNames と呼ばれる特別なゾーンをサポートしています。この名前のゾーンを展開することで、WINS に依存することなく、単一ラベルの名前解決を行うことができます。ただし動的更新はサポートされません。

推奨　：　NetBIOS の名前解決は【WINS による名前解決】を使用

3.1.6 DNS 逆引き参照ゾーンの設計

DNS には DNS コンピュータ名（FQDN）から IP アドレスを取得するための前方参照ゾーンと、IP アドレスか

ら DNS コンピュータ名（FQDN）を取得するための逆引き参照ゾーンの 2 種類のゾーン体系があります。Active Directory では前方参照ゾーンは必須ですが、逆引き参照ゾーンは必須ではありません。逆引き参照ゾーンは、メールシステムなど IP アドレスからホスト名への名前解決を必要とするアプリケーションが存在する環境で必要になりますので、必要に応じて作成してください。

既存の DNS 環境に逆引き参照ゾーンが存在する場合は、Active Directory 側と二重管理にならないよう、どちらかで一元管理することを推奨します。

3.2 フォレスト/ドメイン構成の設計

3.2.1 フォレストの考え方

フォレストとはドメインツリーの集まりであり、簡単に言うとオブジェクト検索が行える範囲です。Active Directory を導入する場合、関連のある組織は一つのフォレストに構成します。
フォレストを分けるのは以下のようなケースです。

フォレスト分割が必要なケース

◎ スキーマ情報を共有したくない場合
スキーマはフォレストで一意です。組織間でそれぞれ独立したスキーマを持ちたい場合にフォレストを分割します。

別々に構築したフォレストは、後から統合することはできません。
なお、Windows Server 2003 以降ではフォレスト間で信頼関係を結ぶことが可能です。フォレスト間で信頼関係を結ぶと、フォレスト間で相互にリソースアクセスができるようになります。但し、その場合でも GC、スキーマ、サイトの統合はできません。

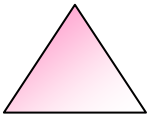
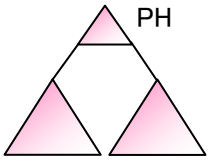
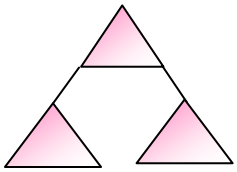
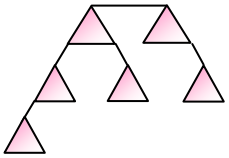
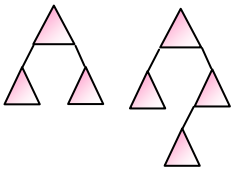
3.2.2 ドメイン分割の判断基準

Active Directory 設計全体に渡って言えることは、できるだけシンプルな構成にするのが望ましいということです。ドメイン構成について言えば、人事異動や組織変更の際の管理を考慮して可能な限りシングルドメイン構成にします。マルチドメイン構成をとる場合もできるだけドメイン数が少ない構成にすることを推奨します。なお部署単位でユーザー管理したいという場合は、ドメイン内で OU を作成することで対応できます。

基本はシングルドメイン構成。ドメイン分割はお客様環境と要件から決定します。

以下はドメイン構成のパターンとその比較を示したものです。

表 3.3 ドメイン構成のパターン

ドメイン構成	シングルドメイン構成	マルチドメイン構成			
	シングルドメイン	プレースホルダドメイン（PH）	ドメインツリー	同一フォレスト	別フォレスト
構成例（図）					
説明	中央での一元管理が実現できる。 一部管理を分散したい場合は OU を用いて実現。	特定の部署が最上位の管理者権限を持たないように構成できる。 最上位にプレースホルダドメインという空のドメインを置く。	複数のドメインを連続したネームスペースで構成。 親会社-子会社のような関係。	複数のドメインを異なるネームスペースで構成。ドメインツリーとの相違点はネームスペースが不連続である点。	関連会社などでフォレストを分割して完全に別で構成。Windows Server 2003 以降ではフォレスト間の信頼関係の作成が可能。
メリット	フォレスト全体の検索 、 シングルサインオン				・独自のセキュリティや、必要に応じてスキーマ拡張が可能。 ・完全な分散管理
	・管理が容易 ・人事異動の際のオペレーションが楽	・管理が容易 ・将来の拡張がきれいに行える	―	―	
導入ケース	・新規導入で一元管理を行いたい場合、最も多い構成パターン	・新規導入時、将来の拡張性を持たせたい場合 ・複数の部署を対等な関係でドメイン分割したい場合	・既存ドメインツリーに追加する場合（ネームスペース上既存組織の子組織にしたい場合）	・既存ドメインツリーに追加する場合（ネームスペース上既存組織と並列にしたい場合）	・既存のドメインとは独立して管理を行いたい場合。
		・マルチドメイン構成を考えるケースについては次項参照。			
一般的な商談ケース	・全社的な導入時	・部門での先行導入時 ・M&A が見込まれる時	・親会社・子会社 ・海外拠点との連携 ・社内カンパニー制		・別会社

可能であればシングルドメイン構成で設計することを推奨します。ドメインの数が多くなると管理工数が増加するため、まずはシングルドメインで要件を満たせるか検討します。富士通の導入事例でもシングルドメインが大多数です。

以下にマルチドメイン構成にしなければならない主なケースを示します。

マルチドメイン構成を必要とするケース

◎ ネームスペース上、ドメインを分けたい場合
ドメインをまたぐ人事異動の際、管理者の作業が煩雑になることに留意。

◎ 分社制・カンパニー制を導入している場合
このような場合、ドメイン分割を検討する必要があるケースが多い。

◎ 海外拠点などで互いの通信がほとんど皆無の場合
シングルドメイン構成でもサイト設計でドメイン内の複製トラフィックの制御は可能だが、拠点間で互いに通信の必要がなく根本的にトラフィックを制限したい場合。
拠点間で言語バージョンの異なる DC を配置したい場合。

Windows Server 2008 以降の Active Directory では、一つのドメイン内で複数のパスワードポリシーを設定できます。
「細かい設定が可能なパスワードポリシー」では、一つのドメイン内のユーザやセキュリティグループに対してパスワードポリシーやアカウントのロックアウトポリシーを適用することができます。OU 単位では設定できないのでご注意ください。
また、この機能を使用するためにはドメインの機能レベルを Windows Sever 2008 以上にしなければなりません。
なお、Windows Server 2012 以降では、「細かい設定が可能なパスワードポリシー」を Active Directory 管理センターから設定できるようになり、操作性が向上しています。

3.2.3 ドメイン構成判断フロー

これまで説明してきたドメイン構成の決め方を、新規構築の場合と既存への追加の場合とで、それぞれフロー図で示します。
なお海外拠点を含む場合は、特に慎重に検討が必要であり単純に決定でないため、このフロー図には含めておりません。

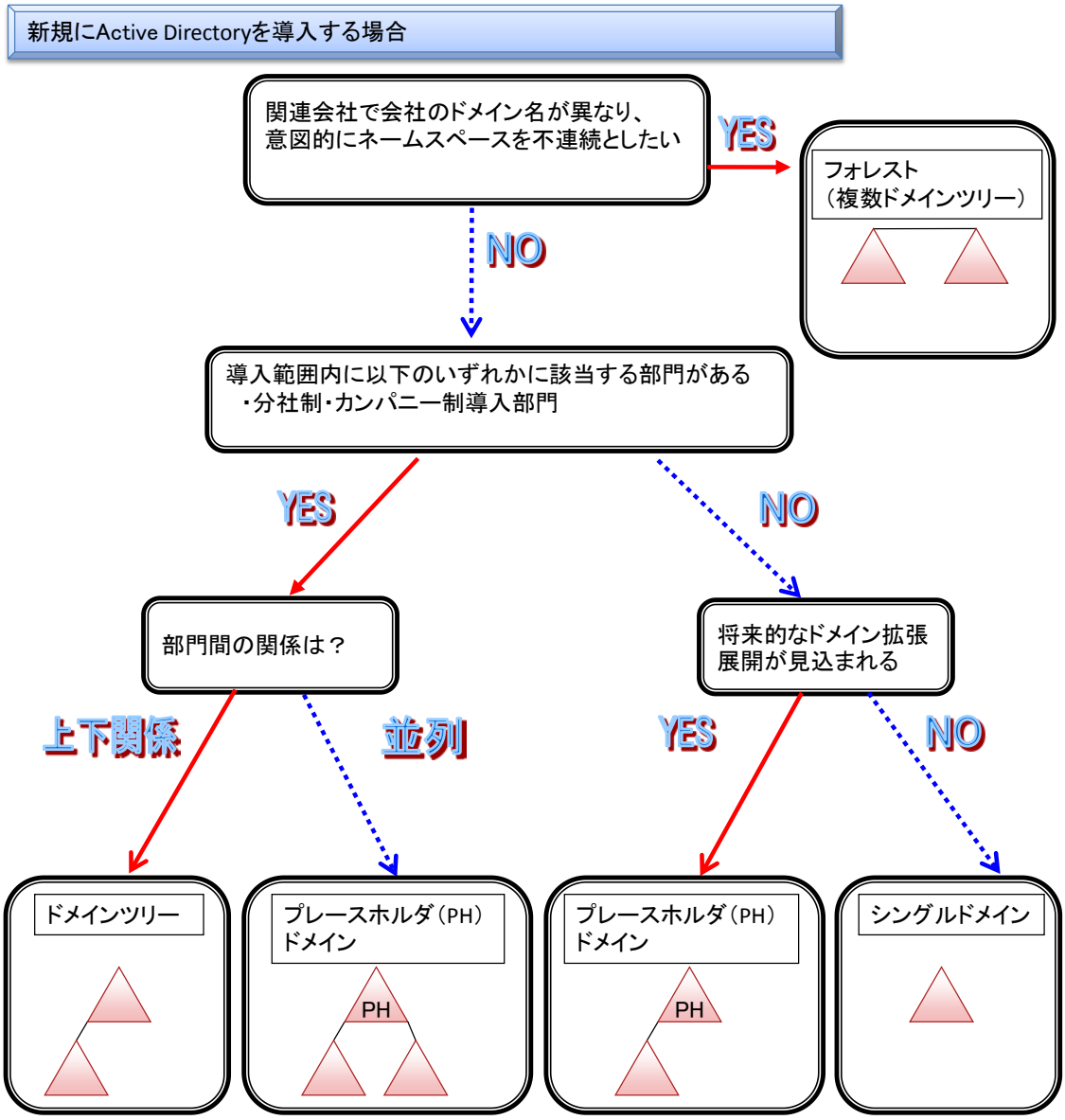


図 3.1 新規 Active Directory の導入

既存ドメインにドメインを追加する場合、既存ドメインの子ドメインにするか並列にドメインを作成するかのどちらかです。既存ドメインの上位にドメインを追加することはできません。

以下に既存の Active Directory にドメインを追加する場合の構成決定フローチャートを示します。以下のフローチャートはシングルドメイン構成の Active Directory に追加する場合です。既存環境がマルチドメイン構成の場合は、既存ドメインの設計方針やお客様の意向を踏まえて検討を行ってください。

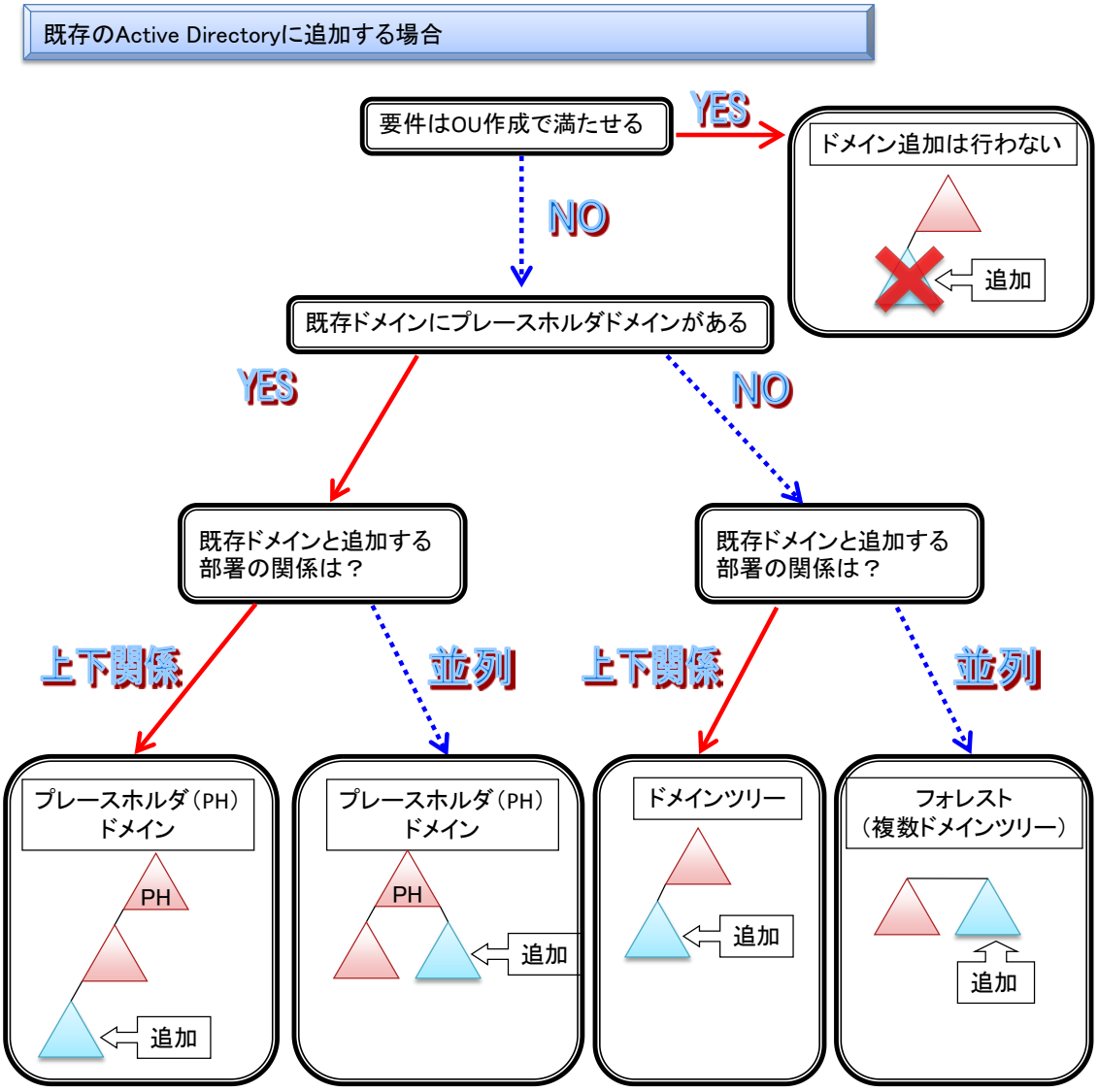


図 3.2 既存 Active Directory へのドメイン追加

3.2.4 Active Directory のフォレストとドメインの機能レベル

Active Directory ではドメインまたはフォレストの機能レベルを環境やニーズに合わせて決定します。ドメインまたはフォレストの機能レベルには以下の種類があります。

表 3.4 ドメイン機能レベル

ドメイン機能レベル	ドメイン内に存在できる DC のバージョン
Windows Server 2003	Windows Server 2003 Windows Server 2008 Windows Server 2008 R2 Windows Server 2012 Windows Server 2012 R2 **Windows Server 2016**
Windows Server 2008	Windows Server 2008 Windows Server 2008 R2 Windows Server 2012 Windows Server 2012 R2 **Windows Server 2016**
Windows Server 2008 R2	Windows Server 2008 R2 Windows Server 2012 Windows Server 2012 R2 **Windows Server 2016**
Windows Server 2012	Windows Server 2012 Windows Server 2012 R2 **Windows Server 2016**
Windows Server 2012 R2	Windows Server 2012 R2 **Windows Server 2016**
Windows Server 2016	**Windows Server 2016**

表 3.5 フォレスト機能レベル

フォレスト機能レベル	フォレスト内に存在できるDC のバージョン
Windows Server 2003	Windows Server 2003 Windows Server 2008 Windows Server 2008 R2 Windows Server 2012 Windows Server 2012 R2 **Windows Server 2016**
Windows Server 2008	Windows Server 2008 Windows Server 2008 R2 Windows Server 2012 Windows Server 2012 R2 **Windows Server 2016**
Windows Server 2008 R2	Windows Server 2008 R2 Windows Server 2012 Windows Server 2012 R2 **Windows Server 2016**
Windows Server 2012	Windows Server 2012 Windows Server 2012 R2 **Windows Server 2016**
Windows Server 2012 R2	Windows Server 2012 R2 **Windows Server 2016**
Windows Server 2016	**Windows Server 2016**

※表 3.4、表 3.5 の太字下線部分は Windows Server 2016 で追加された部分です。
※Windows Server 2012 R2とWindows Server 2016で新規にフォレストおよびドメインを作成する場合には、Windows Server 2008 以上の機能レベルを選択する必要があります。

ドメインまたはフォレストの機能レベルは一度上げると、元の機能レベルに戻すことはできません。 しかし、下位の機能レベルは移行期間中に使用するものであり、ドメインまたはフォレスト内の古い DC が撤去された時点で機能レベルを上げることを推奨します。

4 お客様の要件にあわせた詳細設計項目

本章で述べる設計項目は、お客様環境で快適な運用を考える上で必要な項目です。前章の設計項目とは異なり、後からでも設定の変更が可能なため、必要に応じて運用後も見直しをかけることができますが、運用していく上で影響が非常に大きい重要な設計項目です。

4.1 OUの設計

OU（組織単位）は、オブジェクト（ドメインコントローラー、コンピュータ、ユーザー、グループ、連絡先、共有フォルダ、プリンター）を格納できるコンテナオブジェクトです。OU は管理（管理の委任、グループ ポリシーの適用可否など）を目的として作成します。リソースに対するアクセス権を与えるためのものではないことに注意してください。本章では OU の設計について記述します。

4.1.1 OU 設計における検討事項

以下に OU 設計の考え方について説明します。

(1) Active Directory で管理するオブジェクトの決定

まず、Active Directory で管理するオブジェクトを決定します。Active Directory に登録できるオブジェクトには以下のものがあります。

表 4.1 オブジェクト一覧

オブジェクト	登録	主な用途	グループ ポリシーの適用可否
ドメインコントローラー	必須	ドメインコントローラーの管理	適用可
コンピュータ	必須	コンピュータの管理	適用可
ユーザー	必須	ユーザーの管理、共有フォルダ、グループ ポリシーなどのアクセス制御	適用可
グループ	必須	ユーザーの管理、共有フォルダ、グループ ポリシーなどのアクセス制御	適用不可
連絡先	任意	Exchange Server 等で利用	適用不可
共有フォルダ	任意	共有フォルダの検索で利用	適用不可
プリンター	任意	プリンターの検索で利用	適用不可

Active Directory での管理が任意であるものについては、お客様の運用に応じて検討します。中でもプリンターオブジェクトは、プリンターの検索および設定が容易になるため、オブジェクトを作成する事例が多くあります。

(2) OU 構成の決定

Active Directory で管理するオブジェクトが決定したら、オブジェクトを格納する OU の構成を決定します。OU 構成の設計は管理の委任やグループ ポリシーの適用を視野に入れて行うことで、後戻りが少なくなります。

OU は階層化が可能です。上位 OU に適用したグループ ポリシーは下位 OU にも適用されるため、下位 OU ほど多数のグループ ポリシーが適用されることになります。結果、ログオンの性能劣化が起きるため、階層は深くても 5 階層までにすることを推奨します。

OU の分け方には以下のようなパターンがあります。Active Directory で管理するオブジェクト毎の管理体制に従い、パターンを適宜組み合わせて OU 構成を設計します。

表 4.2 OUの分け方

OU の分け方	説明
業務の組織構造	組織構造をそのままOU構造とする。注意点として組織変更による影響が大きいことが挙げられる。
地理的構造	地理的な構造を OU 構造とする方法。管理体制も拠点毎に分かれる場合などに適する。
管理単位	部署 A と部署 B を一箇所で管理している場合など、業務上の組織でなく管理単位で OU を分割する。
オブジェクト種別単位	ユーザーオブジェクト、コンピュータオブジェクト、といったオブジェクト単位にOU分割する方法。人事異動による管理工数削減のため、ユーザーオブジェクトについてよく使用されるパターン。

以下に OU の構成例を紹介します。この例は基本的に中央で集中管理のお客様で、クライアントについてのみ購入・管理が部署単位のケースでの OU 設計の一例です。

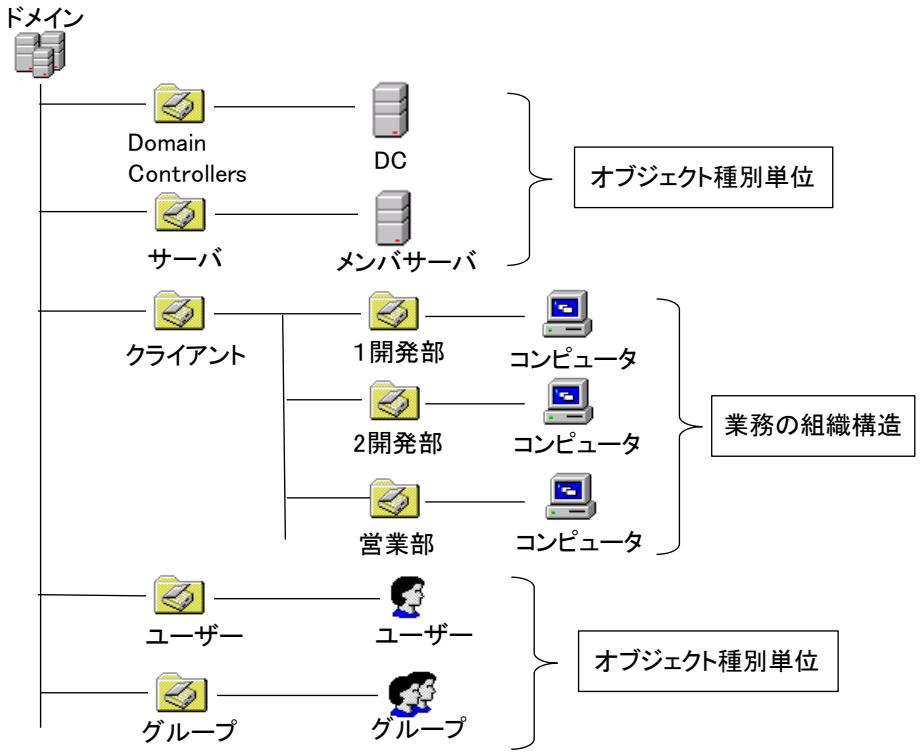


図 4.1 OU の構成例

(3) OU 管理の委任

委任は OU 配下の全権限を委任することだけでなく、一部の権限だけを委任することも可能です。お客様の管理体制、運用体系に合わせて設計を行ってください。
管理の委任は、オブジェクト制御の委任ウィザードで設定可能です。委任ウィザードを使用すると、対話形式で簡単に委任設定が可能です。ただし、設定した委任内容を変更する場合や詳細な委任を行う場合には、OU のアクセス許可で設定を行います。

OU の設計を行う際は、以下の事項を考慮して設計を行ってください。

－管理の委任はグループに対して設定することを推奨
管理を委任する場合は、ユーザではなくグループオブジェクトに対して設定することを推奨します。管理者が変更になった場合、管理者グループのメンバシップの変更のみで済むため、委任の解除忘れを防ぐことができます。

－管理の委任はドメイン/サイト単位も可能
本章では OU 単位での管理の委任について説明しましたが、この他にもドメインやサイト単位での委任設定が可能です。

4.2 サイトの設計

サイトの設計は、ディレクトリ複製のためのトラフィック制御や、ログオン認証を受ける DC を明示的に指定することを目的とします。

4.2.1 サイト構成の考え方

Active Directoryドメイン内では DC 間の情報同期のため定期的にディレクトリ情報の複製を行います。LAN など高速な回線で繋がれている DC 同士であれば問題ありませんが、回線速度の遅い拠点間で頻繁に複製が行われると問題となる可能性があります。
このような場合、サイトという物理的な境界線を定義することで対応します。サイト間では複製トラフィックのスケジュールが細かく定義でき、例えば毎日深夜の時間帯のみ複製を行うといった制御が可能です。加えてサイト間複製ではデータの圧縮が可能なため、回線への負荷も抑えられます。
また、サイト分割して各拠点に DC を配置することによって、コンピュータは同一サイトにある DC にログオン要求を行います。その結果、効率的なログオン認証処理が実現できます。

サイトの分割と各サイトへのサーバの配置計画はシステム全体としてのサーバ台数を見積もる上で必要なものです。以下にサイト構成の考え方の指針を示します。

サイト構成の考え方

基本的には DC を配置した拠点を、それぞれ 1 サイトとして構成します。結果として WAN を介さず接続されるネットワーク範囲を 1 サイトとして定義することが多いです。
DC が配置されていない拠点は、ネットワーク的に最も近い DC が配置されたサイトに含めます。

サイト構成の例

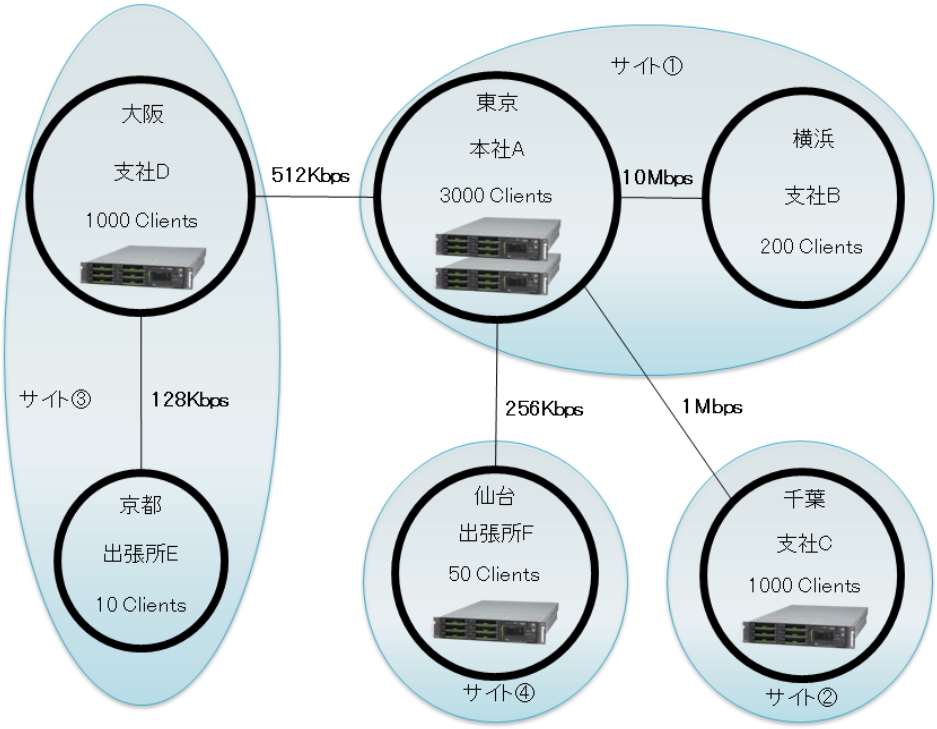


図 4.2 サイト分割の例

上の例では、東京本社 A と横浜支社 B は拠点間の回線速度が 10Mbps あり、横浜支社 B のクライアント数が 200 台と比較的少ないため、東京本社 A と横浜支社 B を合わせてサイト①として定義します。認証処理能力の意味では、サイト①はクライアント数 3200 台であり、DC1 台で処理可能な範囲です。しかしサイト①は本社サイトであることから、冗長性を考慮して 2 台構成にします。

千葉支社 C は東京本社 A との回線速度が 1Mbps ありますが、クライアント数 1000 台と比較的多いため、サイトを分割してサイト②として定義し DC を 1 台設置します。仮に千葉支社 C の DC にアクセスできなくなった場合でも、回線に問題がなければ東京本社 A の DC で認証ができるため、千葉支社 C に冗長化のための DC を設置する必要はありません。これはサイト③、サイト④についても同様です。

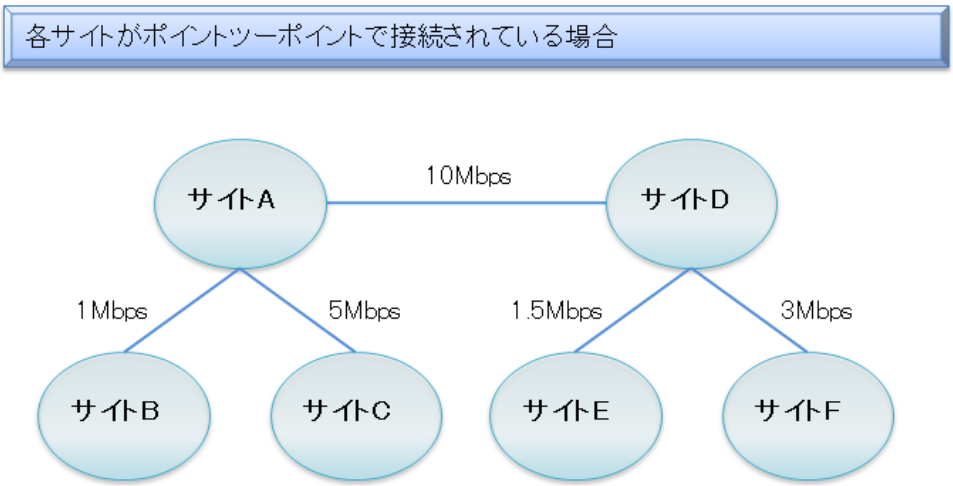
大阪支社 D では東京本社 A との回線速度が 512Kbps と同一サイトにするには低速なため、サイト③として定義して DC を 1 台設置します。京都出張所 E は、クライアント数も 10 台と極めて少ないため、DC を設置するよりも上位サイト③に含めてしまい、認証は大阪支社 D の DC で行うことにします。

仙台出張所 F ではクライアントが 50 台あるため、拠点内に DC を設置することにより効率良く認証が行えることと、上位サイト①との間の回線は比較的低速ですが、サイト分割してサイト間の複製を制御すれば耐えられると考えられるため、仙台出張所 F はサイト④として定義し DC を設置します。

このように Active Directory では、拠点間の回線速度と拠点内のクライアント数によって、サイトを分割するかどうかの判断をします。2 つ以上のドメインやフォレストでもサイト分割の考え方は同じなので参考にしてください。

4.2.2 サイトリンクオブジェクトの作成とリンクコストの定義

サイト間の論理的なネットワークパスをサイトリンクといいます。サイトリンクは Active Directory にサイトリンクオブジェクトとして保存され、指定のサイト間トランスポート(IP または SMTP)を使用して一様なコストで通信できるサイト群として表されます。サイトリンクオブジェクトは自動的に作成されませんので、管理者が手動で作成する必要があります。



サイトリンク	リンクするサイト
サイト A ― サイト D	サイト A、サイト D
サイト A ― サイト B	サイト A、サイト B
サイト A ― サイト C	サイト A、サイト C
サイト D ― サイト E	サイト D、サイト E
サイト D ― サイト F	サイト D、サイト F

図 4.3 サイトリンク例

2 つのサイトをサイトリンクで接続すると、それぞれのサイトにあるブリッジヘッドサーバと呼ばれる DC がサイト間の複製を実行します。ブリッジヘッドサーバの詳細は 4.2.5 章を参照してください。
サイトリンクオブジェクトでは指定したサイト間の複製に関する以下の設定を行うことができます。

- リンクに含まれるサイト
- リンクコスト
- 複製間隔
- 複製のスケジュール

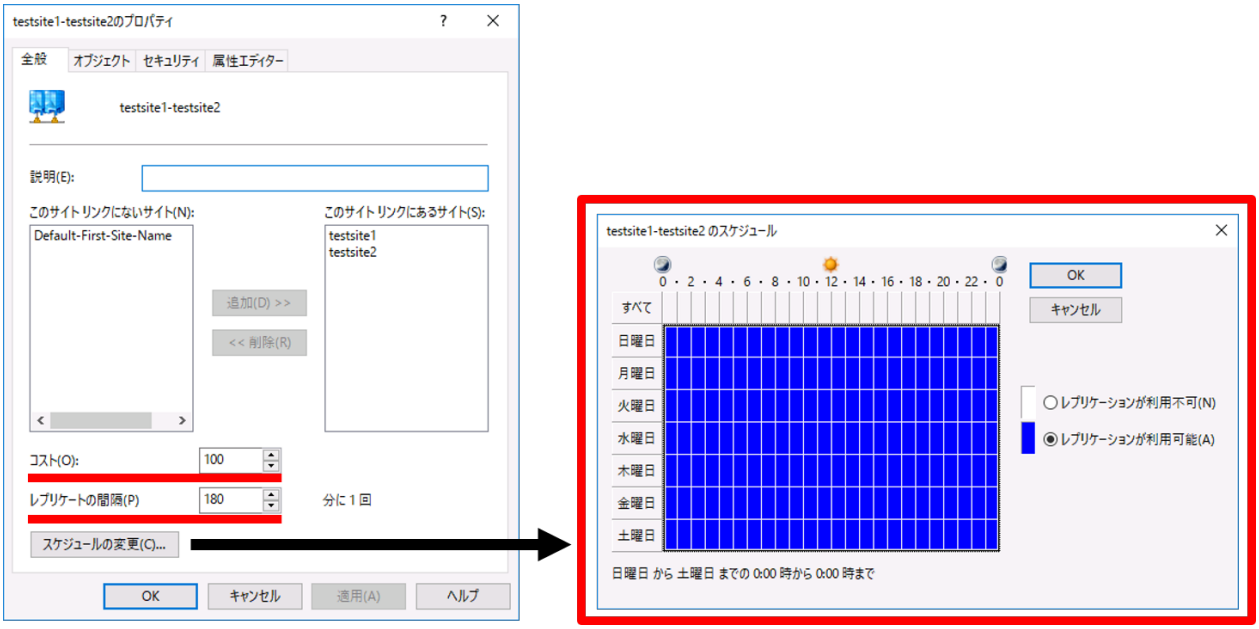


図 4.4 サイトリンクオブジェクトの設定

サイトリンクのコストを適切に構成することにより、より高速な接続経路を優先的に利用することができます。また、特定のアプリケーション（DFS など）やサービスでは、最も近くにあるリソースにアクセスするためにリンクコストを使用します。
リンクコストは、サイト間の回線の使用可能帯域、およびトラフィックの制御に関する個別の要件等から決定します。
リンクコストとして設定する値は下表に示す範囲で、値が小さいほど優先度が高くなります。

表 4.3 リンクコストの設定値

設定可能範囲	1～99999
デフォルト値	100

実際設定する値は、**相対的な値**として各回線の重みづけを定義します。例えば、以下の計算式よりリンクコスト値を算出する方法があります。

（計算式）リンクコスト = 1024/Log（利用可能な帯域幅（Kbps））　　注）Log は対数関数です。
主な帯域幅によるリンクコスト値の計算値例を下の表に示します。

表 4.4 リンクコスト値の計算値例

利用可能な帯域幅	リンクコスト
64Kbps	567
128Kbps	486
256Kbps	425
512Kbps	378
1Mbps	340
1.5Mbps	321
2Mbps	309
10Mbps	255
100Mbps	204
1Gbps	170
10Gbps	146

4.2.3 サイトの複製

サイトの複製にはサイト内複製とサイト間複製があります（4.2.4 章を参照）。同一サイトのドメイン間、サイト間には接続オブジェクトというレプリケーション接続を示すオブジェクトが作成されます（この接続オブジェクトによって構成される集まりを複製トポロジという）。接続オブジェクトは、KCC（知識整合性チェッカー）が自動的に生成します。なお、サイト間複製の場合は管理者が設定したサイトリンクコスト値に従って作成されます。

また、KCC は新しい DC、別サイトへ移動した DC、一時的に利用できなくなった DC、複製のスケジュールの変更などに対応するため、15 分ごとに複製トポロジをチェックし、動的に更新を行います。接続オブジェクトは手動で作成することも可能ですが、手動で作成された接続オブジェクトは動的に変更されることはありません。

4.2.4 サイトの複製種類

サイトの複製には、サイト内複製とサイト間複製の 2 種類があります。この 2 種類の複製について紹介します。

表 4.5 サイトの複製種類

項目	サイト内複製	サイト間複製	
プロトコル	IP	IP	SMTP
トポロジ	リング	スパニングツリー	
複製間隔	データベース更新から 5 分または 15 秒後 既定の複製間隔：60 分	管理者によるスケジュール設定 （複製実施時間帯、複製間隔） 既定の複製間隔： 3 時間	
複製モデル	更新通知とプル（同期）	プル（同期）	ストア＆フォワード（非同期）
複製可能情報	スキーマコンテキスト コンフィグレーションコンテキスト ドメインコンテキスト		スキーマコンテキスト コンフィグレーションコンテキスト
暗号化・電子署名	しない		可能（CA 認証局サービス要）
圧縮	不可能 （CPU 負荷の軽減）	可能（既定で圧縮） （ネットワーク負荷の軽減）	

・ **サイト内複製**

サイト内では、KCC により自動的にリング型の双方向の複製トポロジが作成されます。複製トポロジは 3 ホップ以内にすべての DC に複製が開始されるように形成されます。サイト内で DC の更新が発生した場合、フォレスト機能レベルが Windows Server 2003 以上の場合には 15 秒後に複製が実行されます。なお、サイト内複製ではデータは圧縮されません。

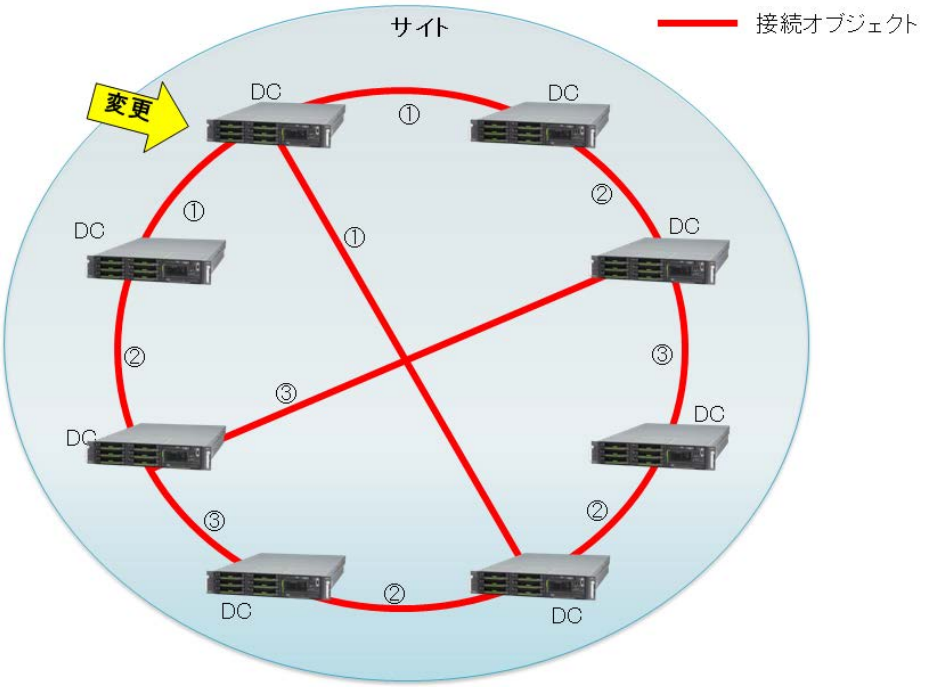


図 4.5 サイト内複製

基本的にサイト内の複製については KCC に一任し、ほとんどのケースでは特別なチューニングは必要としません。負荷や複製の遅延などが著しい場合は、接続オブジェクトや複製時間のチューニングを検討します。

・ **サイト間複製**

サイト間では、管理者が設計したサイトリンクおよびサイトリンクブリッジに従って、KCC によりサイト間接続の総コストが最小となるようなスパニングツリー状の複製トポロジが形成されます。サイト間では管理者が設定した複製スケジュールに従って複製が実行されます。サイト間複製は既定でデータは圧縮されます。

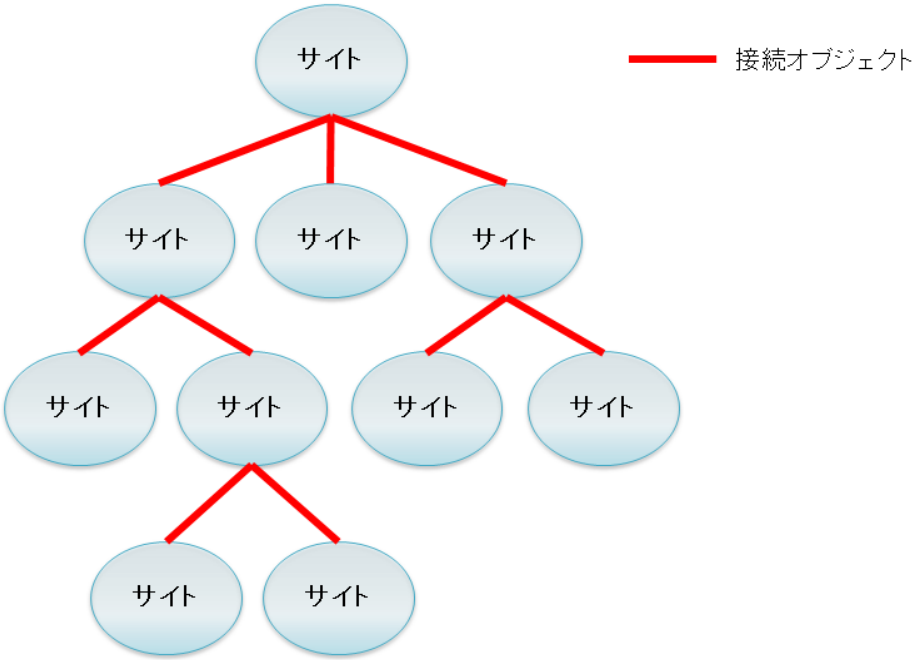


図 4.6 サイト間複製

サイト間の複製は業務時間を避け夜間のみ複製、或いは朝夕のログオン/ログオフトラフィックが集中する時間帯を避けるようなスケジューリングが一般的です。

サイト間複製でサイトリンクが使用するプロトコルには、IP と SMTP の 2 種類ありますが、通常は IP を使用して DC 間の複製を行います。SMTP を使用する形態は、マルチドメイン構成且つドメイン間が Firewall で遮断されている環境の場合のみです。また、プロトコルに SMTP を使用すると以下の注意が必要です。

- 同一ドメインのサイト間複製に利用できない（ドメインコンテキストの複製ができないため）
- それぞれの DC が証明書を持つ必要があり、認証局（CA）の導入が必要

4.2.5 ブリッジヘッドサーバの選定

ブリッジヘッドサーバとは、サイト間の複製時に使用されるDCのことで、サイト間の架け橋的役割を担うものです。ブリッジヘッドサーバは何も設定を行わなければ、KCC が自動的に指定するため**基本的には設定は必要ありません。**

より厳密なチューニングを行いたい場合などは、以下のような条件に最も適う DC を明示的に【優先ブリッジヘッドサーバ】として指定することで複製効率を向上させることも可能です。ただし明示的に指定を行うと、指定されたDCの間でしか障害時のフェールオーバーが行われなくなるため、複数指定するなど考慮が必要です。また、サイト内にドメインが異なるDCが存在する場合は、ドメインごとに優先ブリッジヘッドサーバを指定します。

優先ブリッジヘッドサーバの選定指針

- GC を実装しており、かつ FSMO でない DC
- サイト内で外部のサイトにネットワーク的に近い DC
- スペックの高い DC

4.3 DCと各種役割の配置の考え方

4.3.1 DC のサーバの選定基準

富士通PCサーバ PRIMERGYであれば全ラインナップがDCとして必要なスペック要件を満たしています。機種選定の際は、サーバ部品の冗長化、将来の拡張性の有無、設置要件を考慮の上、選定してください。
富士通 PC サーバ PRIMERGY については、以下 URL を参照してください。

> 「 PC サーバ FUJITSU Server PRIMERGY（プライマジー）」
> http://jp.fujitsu.com/platform/server/primergy/

（参考）クライアント認証処理能力の目安
マイクロソフト社では、クライアント認証処理能力として必要な DC 台数を以下と公開しています。
ユーザー数が 1～499 人の場合は、1CPU が搭載されたサーバ 1 台
ユーザー数が 500～999 人の場合は、2CPU が搭載されたサーバ 1 台
ユーザー数が 1000～2999 人の場合は、2CPU が搭載されたサーバ 2 台
ユーザー数が 3000～10000 人の場合は、4CPU が搭載されたサーバ 2 台

詳細については以下 URL を参照してください。

> 「Step B2: ドメイン コントローラの数を決める」
> http://technet.microsoft.com/ja-jp/library/cc268208.aspx

4.3.2 DC の配置の考え方

DC は可用性を考慮し、各ドメインに最低 2 台の DC を配置することを推奨します。DC のユーザー認証能力という意味では、大概のユーザーはこの 2 台だけで十分ですが、ユーザー数が多いサイトや回線速度に問題があるサイトがある場合は、各サイトにも DC を置くことを検討してください。
また、DC の中には操作マスタ（FSMO）と呼ばれる 5 つの特別な役割を持つサーバがあります（表 4.6 を参照）。

表 4.6 FSMO の役割

名称	役割	配置
スキーママスタ	ディレクトリスキーマへの変更処理を行う	フォレストに 1 台
ドメイン名前付けマスタ	ドメインの追加・削除を制御	
RID マスタ	セキュリティ ID を生成する際に必要な RID を割り当てる	ドメインに 1 台
PDC エミュレータ	時刻同期、パスワード複製、アカウントロック等のマスタ的役割、および Windows NT の PDC 相当の役割を担う。	
インフラストラクチャマスタ	ドメイン間のオブジェクト参照において、オブジェクトの SID、識別名（DN）の更新処理を行う	

フォレストまたはドメインに 1 台、各 FSMO の役割を持つ DC（FSMO サーバ）の配置が必要になります。これらの FSMO の役割は分散配置可能ですが、一般的に 1 台のサーバに集約します。運用管理面を考慮すると、FSMO サーバと、障害対策用にバックアップを取得している DC を、Active Directory 全体を管理する管理者のいる拠点に配置することが望ましい構成です。

さらに、ドメイン内で最低 1 台は GC の役割を持たせる必要があります。GC の配置については「4.3.3 節 GC の配置の考え方」を参照してください。

DC 配置の考え方

・各ドメインに最低 2 台の DC を配置。
・FSMO サーバと、障害対策用にバックアップを取得している DC は管理者のいるサイトに配置。
・各拠点に DC を配置するか否かはユーザ数と回線速度から検討してください。
DC 間の複製トラフィックから考えると、上位サイトー下位サイト間の回線速度が 256Kbps 未満の場合は下位サイトへの DC の設置は避けます。
但し、下位サイトのクライアント台数が多い場合は配置の要否を検討してください。

配置例

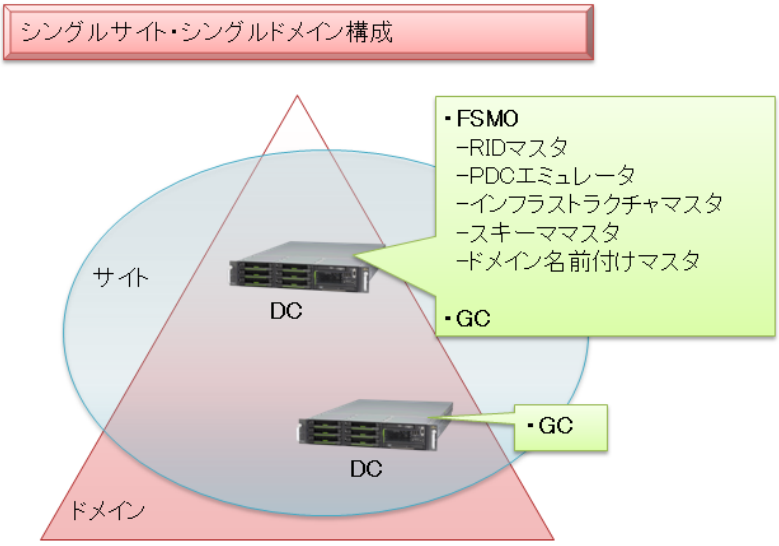


図 4.7 シングルサイト・シングルドメイン構成

DC 台数:**2 台**
FSMO の役割は 1 台に集約。最低 2 台の構成を推奨します。

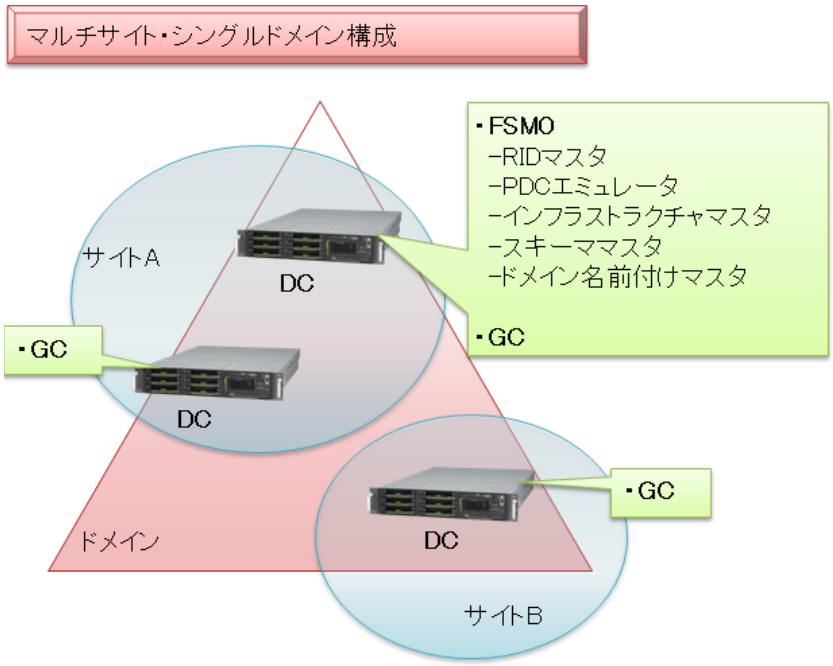


図 4.8 マルチサイト・シングルドメイン構成

DC 台数:**3 台**
ドメイン内に複数のサイトが存在し、サイト内のユーザー数が多い場合などはサイトごとに DC を配置します。

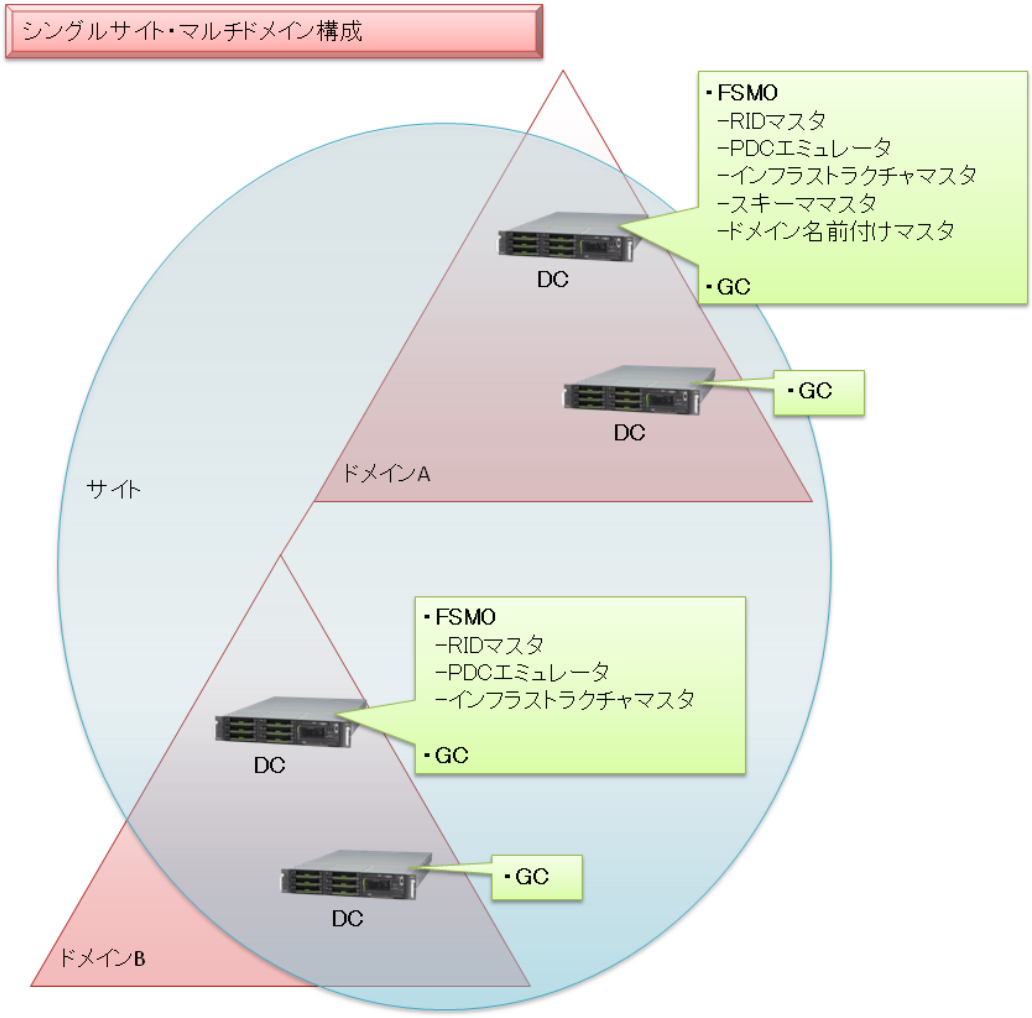


図 4.9 シングルサイト・マルチドメイン構成

DC 台数:**4 台**
各ドメインで FSMO の役割は 1 台に集約し全ての DC を GC とする、各ドメイン最低 2 台構成を推奨します。

POINT!

FSMO とサイトについて
FSMO の役割を持っている DC は、ドメイン管理者のいる拠点に置くことを推奨します。これにより、FSMO の役割を持つサーバの障害発生時の復旧作業を迅速に行えます。

4.3.3 GC の配置の考え方

GC の配置はクライアントのログオンやディレクトリの検索など、クライアントの要求に対する応答性能に大きくかかわります。GC はフォレスト内で最初にセットアップした DC 上に自動的に作成されます。また、手動による構成で、任意の DC に GC の役割を持たせることが可能です。GC 配置の考え方は以下のとおりです。

- GC は各サイトに最低 1 台は配置
  同じサイトに GC がない場合、他サイトの GC に参照に行きます。サイトごとに DC を配置しても GC は他サイトへ参照が必要となるので、帯域幅によってはパフォーマンスに影響を与えることがあります。

- マルチドメインの場合インフラストラクチャマスタ以外の DC に GC を配置
  インフラストラクチャマスタを搭載している DC に GC を配置することはできません。ただし、全ての DC に GC が配置してある場合は、インフラストラクチャマスタを搭載している DC に GC を配置することが可能です。

- サイトの場合、ユニバーサル グループ メンバシップのキャッシュを有効にする
  Windows Server 2003 以降の Active Directory の機能に、ユニバーサル グループ メンバシップをキャッシュするという機能があります。これによりサイトの WAN がダウンした場合でも、DC に、以前にログオンしたユーザーのユニバーサル グループ メンバシップのキャッシュが存在するため、ネットワークへのログオンや拠点内のリソースへのアクセスが可能になります。

  GC を配置する DC では、GC のデータ分の追加データベース容量が必要です。また、その分の複製トラフィックも発生するため、オブジェクト更新が多く、ネットワーク帯域が著しく狭い環境においては考慮が必要です（クライアント応答性能と複製トラフィックとのトレードオフ）。

4.3.4 読み取り専用 DC の配置の考え方

読み取り専用 DC（RODC）は Windows Server 2008 で新たに追加された機能です。主にセキュリティに不安のある拠点サイトへの DC 設置を目的としています。ただし、セキュリティに不安のある拠点には DC は置かない、という選択肢もあるため、拠点サイトへ提供する認証のサービスレベルを考慮の上、RODC の配置を検討します。
要件上、DC 設置が必要な以下の拠点では、RODC の導入を検討する価値があります。

- AD に精通した管理者がいない
- 適切なセキュリティが確保されたサーバ設置場所がない

なお、RODC は、特定拠点への認証機能の提供に特化しており、ドメイン全体へのサービス提供を前提としていないため、DC の冗長化やバックアップを目的とした設置には向きません。

4.3.5 DC の役割配置に関する留意点

DC 配置の設計を行う際は、以下の事項を考慮して設計を行ってください。

- FSMO を持つ DC とアプリケーション/サービスの同居は避ける
  運用監視ソフトやウィルス対策ソフト等を除き、DC と業務アプリケーションなど他の機能を同居することは、運用上推奨しません。DC が FSMO の役割を持つ場合は特に注意してください。

- FSMO を持つ DC は管理者のいる拠点に配置
  障害時を考慮すると、FSMO を持つ DC と、障害対策用にバックアップを取得している DC は、管理者のいる拠点と物理的に近い場所にまとめて配置することを推奨します。

4.4 グループ ポリシーとローカル グループ ポリシー

Windows には、OS やユーザーの設定を統一する機能としてグループ ポリシーが提供されています。グループ ポリシーは、Active Directory 環境で利用するグループ ポリシーと個々のコンピュータで利用するローカル グループ ポリシーから構成されています。

一般にグループ ポリシーという言葉は、Active Directory 環境で利用するグループ ポリシーのみを示す場合と、Active Directory 環境で利用するグループ ポリシーとローカル グループ ポリシーの両方を含めて示す場合が混在して使われていますが、本書では前者を示す場合は「グループ ポリシー」、後者を示す場合は「グループ ポリシーとローカル グループ ポリシー」と記載します。

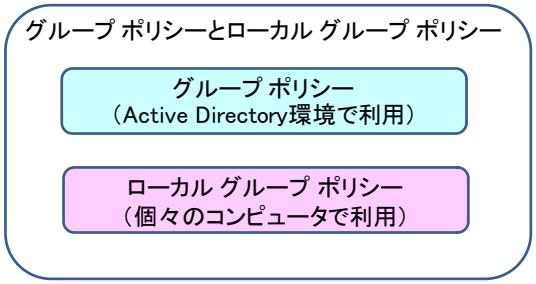


図 4.10 グループ ポリシーとローカル グループ ポリシー

4.4.1 グループ ポリシーについて

グループ ポリシーには、OS に関する設定を行う“コンピューターの構成”とユーザーに関する設定を行う“ユーザーの構成”という 2 つのカテゴリがあります。適用対象のコンピュータは DC 上に格納されたグループポリシーを参照し、設定内容を適用します。

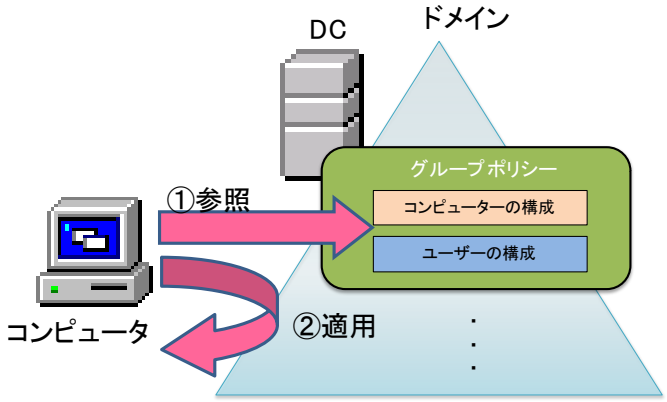


図 4.11 グループポリシーの適用

グループ ポリシーは、ドメイン、サイト、OU に紐づけることができ、その中に含まれる表 4.1 のオブジェクトに対して表 4.7 のタイミングで適用されます。

表 4.7 グループ ポリシーの適用タイミング

カテゴリ	設定項目	適用/実行タイミング
コンピューターの構成	OS に関する設定	OS 起動時および定期間隔(※)
	シャットダウンスクリプト	シャットダウン時
	スタートアップスクリプト	OS 起動時
ユーザーの構成	ユーザーに関する設定	ログオン時および定期間隔(ログオン中の場合)(※)
	ログオンスクリプト	ログオン時
	ログオフスクリプト	ログオフ時

(※)既定では、90 分±10 分間隔で適用されます。
詳細は、以下 URL を参照してください。

> デフォルトのグループ ポリシーの更新間隔を変更する方法
> http://support.microsoft.com/kb/203607/ja

複数のグループ ポリシーを使用する場合、サイト、ドメイン、OU の順に適用され、OU に階層が設けられている場合は、上位の OU から順に適用されるとともに、既定では上位の OU に適用されたグループ ポリシーは下位の OU にも適用されます。
オブジェクト間で重複する設定項目があった場合、より後に適用された設定が有効になります。

グループ ポリシーは DC に接続可能であれば、定期的に適用されますが、表 4.7 のようにスクリプトに限っては特定のタイミングで実行されます。そのため、24 時間運用やシャットダウンではなく休止機能を利用しているコンピュータでは、朝の出社時に適用するといった管理者が期待するタイミングにスクリプトが実行されないこともあります。グループ ポリシーを使用する場合、コンピュータの運用形態を考慮する必要もあります。

DC とクライアント/サーバが低速回線でつながれている場合は、一定の帯域が確保されないとグループ ポリシーで適用されない項目もあります。低速回線で適用されない項目については、以下 URL を参照してください。

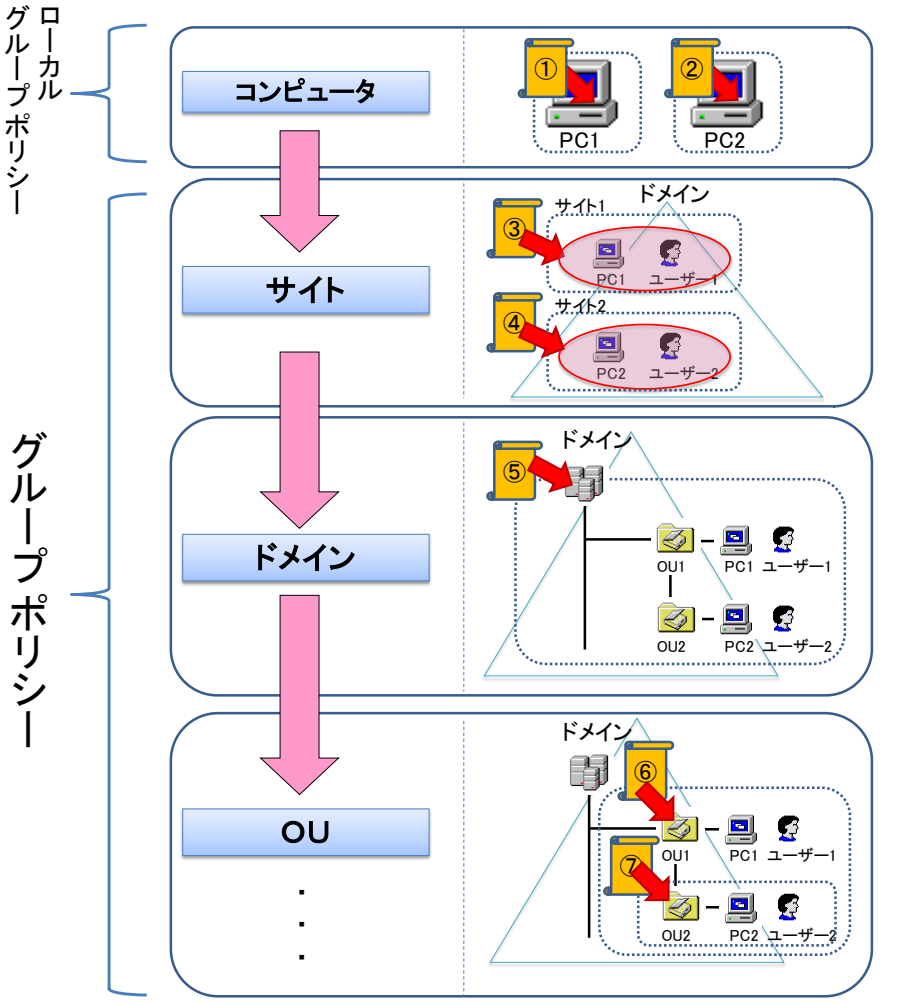
> 低速接続に関するグループ ポリシーの拡張機能のデフォルト動作
> http://support.microsoft.com/kb/227369/ja

4.4.2 ローカル グループ ポリシーについて

グループ ポリシーと同様に、“コンピューターの構成”と“ユーザーの構成” の 2 つのカテゴリがあります。
コンピュータにローカル グループ ポリシーが設定されていると、コンピュータは自身に保存されているローカル グループ ポリシーの設定項目を表 4.7 のタイミングで適用します。

4.4.3 グループ ポリシーとローカル グループ ポリシーの適用例

図 4.12のグループ ポリシーとローカル グループ ポリシーがどのように適用されるのかを表 4.8に記載します。グループ ポリシーとローカル グループ ポリシーの適用は、PC1 とユーザー1 の組み合わせでドメインへログオンした場合と、PC2 とユーザー2 の組み合わせでドメインへログオンした場合を条件としています。



＜凡例＞ :グループ ポリシー または ローカル グループ ポリシー の適用範囲

:グループ ポリシー または ローカル グループ ポリシー

＜グループ ポリシー または ローカル グループ ポリシーで設定している内容＞
①:デスクトップからコンピュータアイコンの削除
②:デスクトップからコンピュータアイコンの削除
③:PROXYサーバをサーバAとする
④:PROXYサーバをサーバBとする
⑤:パスワードの長さを8文字以上とする
⑥:スクリーンセーバーまでの待ち時間を5分とする
⑦:スクリーンセーバーまでの待ち時間を10分とする、デスクトップからコンピュータアイコンの削除

図 4.12 グループ ポリシーとローカル グループ ポリシーの適用イメージ

表 4.8 グループ ポリシーとローカル グループ ポリシーの適用結果

コンピュータ	グループ ポリシー、ローカル グループ ポリシーの適用順および最終的な適用結果	適用結果			
		デスクトップからコンピュータアイコンの削除	パスワードの長さ	PROXY サーバ	スクリーンセーバーまでの待ち時間
PC1	ローカル グループ ポリシー①	有効	-	-	-
	グループ ポリシー③	-	-	サーバ A	-
	グループ ポリシー⑤	-	8 文字以上	-	-
	グループ ポリシー⑥	-	-	-	5 分
	最終的な適用結果	有効	8 文字以上	サーバ A	5 分
PC2	ローカル グループ ポリシー②	有効	-	-	-
	グループ ポリシー④	-	-	サーバ B	-
	グループ ポリシー⑤	-	8 文字以上	-	-
	グループ ポリシー⑥	-	-	-	5 分
	グループ ポリシー⑦	無効	-	-	10 分
	最終的な適用結果	無効	8 文字以上	サーバ B	10 分

（参考）ローカル グループ ポリシーを利用しないで、一部のコンピュータにのみグループ ポリシーを適用させる場合は、以下のグループ ポリシーの機能で制御することも可能です。

- セキュリティ フィルタを利用（ドメインコントローラー/コンピュータ/ユーザー/グループにグループポリシーを適用するアクセス許可を設定する機能）
- WMI フィルタを利用（WMI でクエリを実行し、条件に一致した場合のみコンピュータにグループポリシーを適用させる機能）

5 Active Directory 導入における留意事項

5.1 NATを使用する環境へのActive Directory展開について

お客様環境にNATが存在する場合は、慎重な調査・検証が必要となります。Active Directoryでは通信を行う際に Kerberos 認証を使用します。Kerberos 認証ではパケットのデータ部分にも IP アドレス情報を持っており、NAT によるアドレス変換時に併せて変換が必要です。お客様のネットワーク環境が、Active Directory および Kerberos 認証に対応しているかを確認した上で、十分な検証を行うことをお勧めします。

5.2 DCの冗長化について

Active Directory は DC の台数を増やすことで冗長化します。Active Directory 機能はフェールオーバークラスタ機能に対応していません。フェールオーバークラスタ構成にしても、Active Directory サービスはフェールオーバーしないため、意味がありません。

5.3 Active Directory展開とクライアントリプレイスの実施順序

Active Directory 展開とクライアントリプレイスが同時期に予定される場合、クライアントのドメイン参加設定の二度手間を避けられるため、Active Directory 展開を先に行ったほうが効率的です。

5.4 ドメイン内のDCの言語バージョンは統一する

ドメイン内の DC の言語バージョンは統一することを推奨します。主に海外拠点を含む Active Directory 展開時では、拠点毎に言語バージョンの異なる DC を使用したいという要望がありますが、その場合ドメイン分割を、お客様と検討してください。

5.5 信頼関係を利用した他ドメインへのアクセス

信頼関係を利用して他ドメインのファイルサーバなどの資源へアクセスする場合は、信頼関係先の全 DC の名前解決が必要になります。名前解決ができないと、NTFS セキュリティ許可の設定や、ユーザー認証に失敗します。
なお、DC の名前解決をする場合は、ドメインの DNS 名（SRV レコード）または、ドメインの NetBIOS 名（1b レコード/1c レコード）が必要になります。

5.6 コンピュータのドメイン参加について

ドメインユーザーを意味する Authenticated Users には、既定でドメインにコンピュータを参加させる権限が付与されています。そのため、ドメインユーザーが管理対象外のコンピュータをドメインに参加させるというセキュリティ上、問題のある操作を行うことができてしまいます。予期せぬ操作を行わせないために、ドメインにコンピュータを参加させる権限をドメインユーザーから剥奪することをお勧めします。
ドメインにコンピュータを参加させる権限を剥奪するには、DC に対して既定で適用されるグループポリシー（Default Domain Controllers Policy）から以下の項目を変更します。

[コンピューターの構成]-[ポリシー]-[Windows の設定]-[セキュリティの設定]-[ローカル ポリシー]-[ユーザー権利の割り当て]-[ドメインにワークステーションを追加]

6 最新 Active Directory でのドメイン設計

Windows Server 2016 の新機能を利用しなければ、以前の Windows Server バージョンでの設計方法と大きな変更点はありません。新機能を利用する場合、その特長を押さえて設計することがポイントになります。本章では、Windows Server 2012 以降で追加された、ドメイン設計に影響を与える可能性のある新機能についてご紹介します。

6.1 Windows Server 2016 の新機能

- 新しい認証方式「Microsoft Passport」への対応
  Microsoft Passport は、Windows 10 から採用されたパスワードレスのユーザー認証を可能にする新しいテクノロジーです。この新しい認証方法は、登録済みデバイスと、PIN あるいは生体認証の多要素認証から成り、従来のパスワード方式に比べてより強固なセキュリティ基盤を構築することができます。これまでは Microsoft アカウントと Azure AD アカウントでサポートされていましたが、Windows Server 2016 の登場によりオンプレミスの Active Directory に参加する Windows 10 でもサポートされるようになりました。

- クラウドとオンプレミスとのハイブリット統合
  Azure AD Connect ツールを使用して Azure AD のディレクトリとオンプレミスの Active Directory ドメインをディレクトリ統合することで、社内外のデバイスからオンプレミスの ID を用いて、クラウドアプリやオンプレミスのリソースにシングルサインオンでアクセスできる環境を実現できます。Windows Server 2016 の Active Directory フェデレーションサービスの機能強化により、社内外で Microsoft Passport を利用した認証が可能になります。

- 特権アクセス管理 (PAM)
  Windows Server 2016 の Active Directory ドメインでは、Microsoft Identity Manager (MIM) 2016 の特権アクセス管理 (Privileged Access Management, PAM) 機能がサポートされます。この機能により、ユーザーに対して永続的ではなく、必要なときに有効期限付きの特権アクセスの権限を付与し、有効期限が経過すると特権アクセスの権限をはく奪することできるため、セキュリティリスクを低減することができます。MIM 2016 の PAM は、Windows Server 2012 R2 以降の Active Directory ドメインをサポートしています。

6.2 Windows Server 2012/2012 R2の新機能

- 細かい設定が可能なパスワードポリシーの設定の GUI 化
  Windows Server 2008 で導入された「細かい設定が可能なパスワードポリシー」を使用すると、1 つのドメイン内で複数のパスワードポリシーを指定できるようになります。そのため、ドメイン内のさまざまなユーザーやセキュリティグループの単位に複数のパスワードポリシーとアカウントロックアウトのポリシーを適用できます（OU 単位には設定できません）。
  また、管理者には厳しい設定を適用し、他のユーザーにはそれほど厳しくしない設定を適用するなど、柔軟な設計を行うことができます。
  しかし、実際にこのポリシーを設定するには「ADSI エディタ」を使用して煩雑な操作を行う必要があり、大変面倒でした。
  Windows Server 2012 以降では、「Active Directory 管理センター」から GUI で設定を行うことができるようになり、操作性が向上しています。

- Active Directory ごみ箱の GUI 化
  Windows Server 2008 R2 で追加された「Active Directory ごみ箱」は、削除したオブジェクトを、簡単

かつ迅速に復旧できる機能です。Windows Server 2008 以前のドメインでオブジェクトを誤削除した場合、オブジェクトの属性値を完全に復旧するためには、バックアップデータから復元しなければなりませんでした。
Windows Server 2008 以前のドメインと比較すると削除したオブジェクトの復旧が、簡単にできるようにはなりましたが、実際に復旧を行うには、「LDAP ユーティリティ」または「Windows PowerShell」などを使用しなければなりませんでした。
Windows Server 2012 以降では、「Active Directory 管理センター」から、より簡単かつ迅速に削除したオブジェクトの復旧ができるようになり、操作性が大幅に向上しています。

・ 仮想化環境での DC のクローン作成
DC として動作する仮想マシンの仮想ハードディスクをコピーして別の仮想マシンに割り当てて DC を展開することができます。
また、仮想ハードディスクをコピーして利用する場合には、Sysprep で汎用化する必要がありますが、クローン作成では Sysprep を実施していない仮想ハードディスクのコピーを使用して DC を展開することができます。
そのため、仮想環境において、すばやく DC を展開することができるようになります。

・ USN ロールバックからの自動回復
仮想環境で DC の運用を行っている場合、スナップショットの適用時や仮想マシン（VHD）のコピーによるバックアップからの復元時に、USN（※）のロールバックが発生すると、DC 間における複製が停止してしまいます。
USN のロールバックから回復を行う場合には、「ディレクトリサービス復元モード」で起動し、「ADDS の権限のない復元」でシステム状態を復元する必要がありました。
Windows Server 2012 以降の Hyper-V の仮想環境で、Windows Server 2012 以降の DC を構築している場合には、スナップショットの適用などにより USN のロールバックを検出すると、自動的に回復処理が行われるため、回復のための追加の操作は必要ありません。

（※）オブジェクトの変更状態の管理に使用する一意の識別名を更新シーケンス番号（USN:Update Sequence Number）といいます。

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

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

・PC サーバ FUJITSU Server PRIMERGY お問い合わせ
http://jp.fujitsu.com/platform/server/primergy/contact/

基幹 IA サーバ 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 FUJITSU Server PRIMEQUEST（プライムクエスト）
http://jp.fujitsu.com/platform/server/primequest/
・FUJITSU Server PRIMEQUEST 2000 シリーズ　製品ラインナップ
http://jp.fujitsu.com/platform/server/primequest/products/

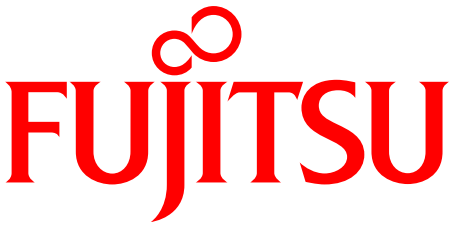
基幹 IA サーバ FUJITSU Server PRIMEQUEST のお問い合わせ先。

・本製品のお問い合わせ
http://jp.fujitsu.com/platform/server/primequest/contact/

商標登記について

- Microsoft、Windows、Windows Server、Active Directory、Hyper-V、Windows Powershell、Azure、Microsoft Passport 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。
- 記載されている会社名、製品名は各社の登録商標または商標です。
- 記載されている会社名、製品名等の固有名詞は各社の商号、登録商標または商標です。
- その他、本資料に記載されている会社名、システム名、製品名等には必ずしも商標表示を付記しておりません。

免責事項


FUJITSU