

インフラストラクチャの計画とデザイン

Windows Server® 2008

Active Directory® Domain Services

Version 1.0

Published: February 2008

For the latest information, please see [microsoft.com/technet/SolutionAccelerators](http://www.microsoft.com/technet/solutionaccelerators/default.mspx)

Copyright © 2008 Microsoft Corporation. All rights reserved. Complying with the applicable copyright laws is your responsibility. By using or providing feedback on this documentation, you agree to the license agreement below.

If you are using this documentation solely for non-commercial purposes internally within YOUR company or organization, then this documentation is licensed to you under the Creative Commons Attribution-NonCommercial License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/2.5/ or send a letter to Creative Commons, 543 Howard Street, 5th Floor, San Francisco, California, 94105, USA.

This documentation is provided to you for informational purposes only and is provided to you entirely “AS IS”. Your use of the documentation cannot be understood as substituting for customized service and information that might be developed by Microsoft Corporation for a particular user based upon that user’s particular environment. To the extent permitted by law, MICROSOFT MAKES NO WARRANTY OF ANY KIND, DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES, AND ASSUMES NO LIABILITY TO YOU FOR ANY DAMAGES OF ANY TYPE IN CONNECTION WITH THESE MATERIALS OR ANY INTELLECTUAL PROPERTY IN THEM.

Microsoft may have patents, patent applications, trademarks, or other intellectual property rights covering subject matter within this documentation. Except as provided in a separate agreement from Microsoft, your use of this document does not give you any license to these patents, trademarks or other intellectual property.

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious.

Microsoft, Active Directory, Outlook, SharePoint, Windows, Windows NT, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

You have no obligation to give Microsoft any suggestions, comments or other feedback (“Feedback”) relating to the documentation. However, if you do provide any Feedback to Microsoft then you provide to Microsoft, without charge, the right to use, share and commercialize your Feedback in any way and for any purpose. You also give to third parties, without charge, any patent rights needed for their products, technologies and services to use or interface with any specific parts of a Microsoft software or service that includes the Feedback. You will not give Feedback that is subject to a license that requires Microsoft to license its software or documentation to third parties because we include your Feedback in them.

目次

[Planning and Design シリーズのアプローチ 5](#_Toc229493155)

[Active Directoryのプランニングとデザインについて 7](#_Toc229493156)

[マイクロソフトのIO（Infrastructure Optimization）におけるActive Directory 8](#_Toc229493157)

[Active Directoryのデザイン･プロセス 10](#_Toc229493158)

[Step 1: フォレストの数を決定する 14](#_Toc229493159)

[Step 2: ドメインの数を決定する 18](#_Toc229493160)

[Step 3: ドメイン名を割り当てる 22](#_Toc229493161)

[Step 4: フォレスト･ルート･ドメインの選択 25](#_Toc229493162)

[Step A1: OU の構造をデザインする 27](#_Toc229493163)

[Step B1: ドメイン・コントローラの配置ついて決定する 29](#_Toc229493164)

[Step B2: ドメイン・コントローラの数を決める 33](#_Toc229493165)

[Step B3: グローバル・カタログの配置を決める 36](#_Toc229493166)

[Step B4: 操作マスタ役割の配置を決定する 41](#_Toc229493167)

[Step C1: サイト･デザインを実施する 45](#_Toc229493168)

[Step C2: サイト･リンクをデザインする 47](#_Toc229493169)

[Step C3: サイト･リンク･ブリッジをデザインする 51](#_Toc229493170)

[Step D1: ドメイン・コントローラのコンフィグレーションを決定する 54](#_Toc229493171)

[まとめ 59](#_Toc229493172)

[Appendix: 補足資料 60](#_Toc229493173)

[Acknowledgments 63](#_Toc229493174)

# Planning and Design **シリーズのアプローチ**

このガイドは IPD シリーズ一部であり、マイクロソフトの インフラストラクチャ･テクノロジーに関するデザイン･プロセスを明確にし、その合理的な運用を目指していくものです。このシリーズにおける個々のガイドでは、それぞれのインフラストラクチャに関するテクノロジーとシナリオに取り組んでいきます。 それらのガイドには、以下のテーマが含まれます：

* プランニング･プロセス全般におよぶ、技術面からの意思決定フローの定義。
* 実施すべき決定と、そのための判断時に考慮すべき各種の共通オプションに関する説明。
* コストや複雑さなどの、ビジネスに関連する判断と選択肢。
* ビジネスの視点からの、包括的で適切な理解を促進する、付加的な問題点を判断するのための枠組み。

このシリーズにおけるガイドは、製品ドキュメントを補完し補強していくという意図を持ちます。

## **このドキュメントにおけるアプローチ**

このガイドは、Windows Server® 2008 オペレーティング･システムにおける、Active Directory® ディレクトリ･サービスに関するインフラストラクチャの、適切な実装を促進するために作成されました。そして、そこで必要となる最も重要な取り組みと判断のための、一貫した構造を提供するようにデザインされています。

それぞれの取り組みと判断は、以下の４つの要素に細分されます：

* 取り組みと判断における背景のことであり、前後関係の設定と全体的な検討項目をを含む。
* 取り組みにおける、汎用的な Option と Task。
* それぞれのOption と Task におけるコストや複雑さといった項目を、評価するためのリファレンス･セクション。
* 実施されるべき決定事項に対して、重要な影響をおよぼすと思われるビジネス上の疑問点。

このドキュメントは Step 1 ～ Step 4 および、Step A1～D1 の意思決定フローで構成され、その中にいくつかの Option と Task が含まれます。Table 1 に列挙されるのは、各セクションの Optionで解説される特質の概要です。それらの項目にしたがって、各 Step の中では特定された Option に関する特質だけが説明されます。

Table 1. Option の特質

| 特質 | 内容 |
| --- | --- |
| 複雑さ | Option 間に干渉をもたらす、複雑さに関する特質です。 |
| コスト | Option の初期コストと継続的なコストに関する特質です。 |
| フォールト･トレランス | システムの可用性に大きな影響をおよぼす、インフラストラクチャにおける弾力性をサポートするための方式を示します。 |
| パフォーマンス | インフラストラクチャの性能に影響をおよぼす、Option に関する特質です。 |
| スケーラビリティ | インフラストラクチャのスケーラビリティに影響をおよぼす Option を示します。 |
| セキュリティ | この値は、全体的なインフラストラクチャに対して、プラスあるいはマイナスにはたらく Option を反映します。 |

それぞれのデザインにおける Option は、上記の表と同じ観点を持ち、また、特質に対する相対的な重み付けを提供するために主観的に評価されます。正確に Option を比較するとき、ビジネスの要素が増えるにつれて、その評価は不明瞭なものとなります。

そのときの等級は、以下の2つの形態を持ちます：

* 複雑さとコストは、High／Medium／Low で評価される。
* 他の特質は、以下のテーブルにおけるスケールで評価される。

Table 2. 付加的な特質

| Symbol | Definition |
| --- | --- |
| ↑ | 特質に対してプラスに作用します。 |
| → | 特質に影響を与えない状態、もしくは、比較の基準が無い状態を表します。 |
| ↓ | 特質に対してマイナスに作用します。 |

このセクションで説明している特質は、2カラムあるいは3カラムのテーブルとして提示されます。対象となる 特質が、すべての Option に適用可能なとき、あるいは利用可能な Option が存在しないときには、2カラムのテーブルが使用されます。例としては、タスクを実施するときなどが挙げられます。

3カラムのテーブルは、特質における、選択肢と、詳細、効果（Table 2）を記述するために、その順番で使用されます。

## **このガイドが想定する読み手**

このガイドは、Active Directoryインフラストラクチャにおける設計に責任を持つ、IT インフラストラクチャ専門家ぴょび、一般職、コンサルタント、付加価値リセーラーのために記述されています。

このドキュメントは、以下のタイミングで利用することができます：

* デザインを実施する上で重要になる判断について、理解を深めるためのデザイン･プロセスに着手するとき。
* 対象となるデザインに対して、一貫した見通しが適用されることを保証するための、デザイン･プロセスを実施しているとき。
* 取り組まれた全ての重要なデザイン領域を検証するために、そのデザイン･プロセスを完了するとき。

# Active Directory**のプランニングとデザインについて**

Active Directory は、Microsoft Windows ネットワーク環境において、セキュリティを制御する核となります。Active Directory インフラストラクチャを用いたディレクトリ･サービスは、ユーザーとコンピュータのアカウントに関する、認証について責任を持ちます。それに加えて、このディレクトリ･サービスは、フォレスト内のリソース管理について、集中化された委任のメカニズムを提供します。

Active Directory のデザインを、適切に開発し実装すていくためには、数多くの疑問を解く必要があり、また、数多くの決定と戦略について判断しなければなりません。このデザインが成功する背景においては、パフォーマンスおよび、セキュリティ、マネージャビリティ、スケーラビリティといった基準への取り組みが行われているはずです。

このガイドの目的は、意志決定プロセスにおいてデザイナーを支援することにあります。Active Directory インフラストラクチャのデザインについて、比較することが可能な背景や状況が提供され、さらに、明解で簡潔なパスが提供されることで目的は達成されます。その意味において、デザインにおける要点に対して検討と代案を提供する、ベストプラクティスと現実世界のエクスペリエンスが、このガイドを支えてくれます。

このガイドを、プロダクト･ドキュメントと組み合わせて利用するとき、Active Directory の実装計画を、自信を持って進められるようになるでしょう。なお、Appendix として提供される補足資料は、デザイン･プロセスにおいて決定された事柄を、記録するためのものです。

# マイクロソフトのIO（Infrastructure Optimization）におけるActive Directory

マイクロソフトのInfrastructure Optimization (IO) Model は、組織の成熟度を連続的にカバーするかたちで、IT のプロセスとテクノロジーを統合するためのものです（詳細については Microsoft.com/io を参照してください）。このモデルは、Massachusetts Institute of Technology (MIT) Center for Information Systems Research (CISR)の産業アナリストおよび、マイクロソフト自身と顧客の経験から作成されています。マイクロソフトが Infrastructure Optimization Model を作成する主な目的は、技術的な能力とビジネスを測定するためのベンチマークとして、柔軟で容易で成熟したフレームワークを利用する、シンプルな方式を開発することにあります。

このInfrastructure Optimization Modelは、核となるインフラストラクチャの最適化、および、アプリケーション･プラットフォームの最適化、そして、ビジネスの生産性のためのインフラストラクチャの最適化といった、3種類の IT を取り囲むかたちで構造化されています。核となるインフラストラクチャの最適化モデルにしたがい、物理的あるいは仮想的なアプリケーションの自動化された配布を、アドミニストレータが管理する組織は、合理化（Rationalized）の レベルへと移行するための要件を充たすことになります。Active Directory は、組織内のユーザーとマシンを認証するためのメカニズムを、アドミニストレータに提供します。Active Directory により、組織はStandardized レベルへ向けた移行を開始する一方で、Rationalized と Dynamic レベルの付加的なサービスが要求する、インフラストラクチャの提供を受けます。このガイドにより、Active Directory 実装に関するインフラストラクチャの、プランニングとデザインを支援します。



図1. 核となるインフラストラクチャ･モデルにActive Directory テクノロジーをマッピングする

## **インフラストラクチャとビジネスのアーキテクチャについて**

マイクロソフトが作成する、この意志決定のための構造化されたガイダンスは、ITインフラストラクチャとビジネス･アーキテクチャを対象としています。そして、Infrastructure Planning and Design シリーズが提供する構造化された手法と判断の形態は、IT のインフラストラクチャ･アーキテクチャに関するものとなっています。その一方で、マイクロソフトのビジネス･アーキテクチャ･テンプレートは、価格計算や、支払のプロセス、発注業務といった、ビジネスにおける詳細な項目にフォーカスしています。

IT インフラストラクチャはビジネスの可能性に貢献すべきであり、ビジネス･アーキテクチャの要件はインフラストラクチャの決定に寄与すべきです。しかし、Infrastructure Planning and Design シリーズは、特定のビジネス･アーキテクチャ･テンプレートを定義することなはく、また、そこに関連付けられることもありません。それに替えて、Infrastructure Planning and Design では判断のための重要なポイントを提供し、そこで、サービス･マネージメントやビジネス･プロセスなどの要素を取り込んでいきます。

# Active Directory**のデザイン･プロセス**

このガイドは、 Windows Server 2008 上に Active Directory を実装するときに、大半の組織が直面するクリティカルなデザイン上の決定や、取り組みについてフォーカスしていきます。

このガイドの目的は、大半の組織が遭遇することになる、最も一般的なシナリオおよび、決定、アクティビティ、Option、Task などの取り組むことです。ただし、すべてのシナリオを網羅するものではなく、また、既存のシナリオを置き換えるものでもありません。このガイドの視点が、ニーズに当てはまらないと考える読み手は、デザイン･コンサルタントの採用について検討してください。

## **判断と決定**

このガイドでは、 Active Directory のプランニングや準備で必ず生じる、判断と決定および、アクティビティに対して、以下のように取り組んでいきます。これらの Step 1 ～ Step D1は、適切にプランニングされた、 Active Directory 実装における最もクリティカルなデザイン要素を示します：

* Step 1: フォレストの数を決定する
* Step 2: ドメインの数を決定する
* Step 3: ドメイン名を割り当てる
* Step 4: フォレスト･ルート･ドメインの選択
* Step A1: ドメイン・コントローラの配置ついて決定する
* Step B1: ドメイン・コントローラの数を決める
* Step B2: ドメイン・コントローラの数を決める
* Step B3: グローバル・カタログの配置を決める
* Step B4: 操作マスタ･ロールの配置を決定する
* Step C1: サイト･デザインを実施する
* Step C2: サイト･リンクをデザインする
* Step C3: サイト･リンク･ブリッジをデザインする
* Step D1: ドメイン・コントローラのコンフィグレーションを決定する

いくつかの項目は、実施されなければならない決定を表します。そのようなケースにおいては、Option がリストアップされ、その中から一般的な回答が得られるでしょう。

同様に、インフラストラクチャ･デザインを完成させるために、実施しなくてはならない重要な Task も、これらの Step 内には含まれます。

## **決定フロー**

多くのデザイン･プロセスにおいて、決定のシーケンスと、タスク達成のシーケンスが、重要なものとなります。 このデザイン･プロセスにおけるクリティカル･パスは、連続した決定を指示するパスであり、他のタスクを開始する前に、対象となるタスクを完了しなければなりません。

Active Directory デザインのためのクリティカル･パスを、図 2のフローチャートに示します。この図のトップからボトムまで移行することで、対象となるステップの連続的なパスが実施され、このドキュメントの目的が達成されるはずです。なお、プロセス･フローは基本的に直列に実施されますが、並列で実施できるものもあります。たとえば、AとBの双方を完了する必要があっても、AとBが同時に実施されるケース、および、AがBの前に実施されるケース、その逆のケースなどがあります。



図2. Active Directoryに関する意思決定フロー

## **収集すべき情報**

この種のプランニング･プロセスにおいては、多様な情報が必要とされるでしょう。Active Directory インフラストラクチャのデザインにおいては、以下の情報が必要とされます。

* **それぞれのドメインにおける、OU 構造デザインの必要性 (A1)**
* 組織で用いられている、現行の管理モデルが必要です。それにより、環境内のリソース管理について、責任を持つ人がリストアップされます。もし、明確な規定が無い場合には、「誰が誰に何をするか？」と質問することで、責任者を探し出します。
* Group Policy の展開について、要件と戦略が必要です。
* **ドメイン・コントローラ配置の必要性 (B1)**
* 物理ロケーションごとのユーザー数が必要です。
* 物理ロケーションごとのコンピューター数が必要です。
* 双方について、コーポレートや、ブランチ、サテライトなどの、オフィスごとに調査します。
* **サイト･デザインに関する必要性 (C1)**
* 物理ロケーションのマップが必要です。
* ロケーション間のネットワーク･リンク速度と、利用可能な帯域幅の情報が必要です。
* 物理ロケーションごとに用いられる、TCP/IP サブネットの情報が必要です。
* 物理ロケーションごとの、ドメインに関する情報が必要です。
* 物理ロケーションごとの、それぞれのドメイン・コントローラの情報が必要です。
* **サイト･リンク・デザインの作成に関する必要性(C2):** 以下の項目について、複製の収束を目的とします：
* コンフィグレーションとスキーマ
* ドメイン
* グローバル･カタログ
* アプリケーション・パーテーション

## **適用可能なシナリオ**

このガイドで取り組んでいく検討項目は、適切なActive Directory インフラストラクチャにとって必要な、構成要素のプランニングとデザインにも関連するものとなります：

* イントラネットの実運用環境
* 集中化された設備（ハブ･リケーション）
* ブランチ･オフィス（サテライト･ロケーション）
* 国内のネットワーク
* 海外とのネットワーク

## スコープ外の領域について

このドキュメントは、Active Directory の中核を実装するためのデザイン･プロセスにおいて、アーキテクトを導くように構成されています。そのため、このドキュメントのスコープでは、以下の領域はカバーされません：

* Active Directoryの簡易版である Active Directory／Application Mode（AD/AM）は、個別のアプリケーションで使用するためにセットアップされるものであり、このスコープから除外されます。
* Microsoft 以外のディレクトリ･サービスに関連する、移行および、共存、相互依存は除外されます。
* Windows Server 2008 以前の実装からの移行については、除外されます。 ただし、Windows 2000 Server コンポーネントに関連する、いくつかのデザイン上の検討項目が提供されます。
* 多数の企業を統合するための、連携形式の実装は除外されます。
* シングル･フォレスト内に多数の企業をホストする、マルチ･テナント形式は検討されません。

このドキュメントの次のセクションからは、事前に定義する必要がある、判断とアクティビティに取り組んでいきます。

# 

# Step 1: **フォレストの数を決定する**

すべての Active Directory は、少なくとも 1つのフォレストを実装することになります。Active Directory デザインにおける Step 1 は、組織の目的を充たすために、1つのフォレストが必要なのか、あるいは、多数のフォレストが必要なのか、その点について判断することです。多数のフォレストが必要とされる場合には、フォレストの合計数を決定しなければなりません。

デザインに着手するときに、正しい判断を下すことが重要です。デザイン上の決定が駆り立てる仮定を用いて、コンフィグレーションを変更することは、計画が進捗するにつれて次第に難しくなるでしょう。フォレストを確立してしまうと、それらの追加よりも廃止の方が、難しくなると考えられます。

## Option 1: **シングル･フォレスト**

Active Directory の全体的なデザインを考えるとき、シングル･フォレストの実装がデフォルトになります。

ベスト･プラクティスな進め方は、シングル･フォレストから始めた後に、あらゆるフォレストの追加に関する正当性を、ビジネス要件により証明していきます。

きわめて大きなディレクトリにとっては、その複製が問題になり得ます。ドメインは、ディレクトリ情報を分割し、また、ドメインレベルの情報の複製を制御するために利用されます。その一方で、フォレスト規模での情報（コンフィグレーション･データ、スキーマ、グローバル･カタログ･データを含む）については、ドメイン間での複製が必須となります。

## Option 2: **マルチ･フォレスト**

マルチ･フォレストを用いたデザインにおいては、以下の要件が影響をおよぼすでしょう：

* **マルチ･スキーマ.** フォレスト内の全てのものが、一般的なスキーマを共有します。このスキーマの適用と運用が矛盾すると、フォレストを追加するという、必要性が生じる可能性があります。
* **リソース･フォレスト.** いくつかの組織では、アカウントとリソースの分離のために、マルチ･フォレストを必要とするかもしれません。この場合、Microsoft Exchange Server 2000 ～ 2007などでは、リソースの共有が必要になります。共有リソースをホストするために、分離されたフォレストの作成が可能であり、認証と認可のパスを提供するために、フォレスト・レベルの信頼関係を使用できます。リソース･フォレストを使用してテスト環境を作成することも可能です。
* **フォレスト管理の分離.** いくつかの組織は、複数のITチームを取り込んだ、内部構造を持っています。それぞれの IT チームが、他の IT スタッフによる制御を拒否し、かつフォレストの制御を望むとき、マルチ･フォレストの実装がそのような制御のための手段となります。この考え方は、企業や、行政、大学などで、合併が行われるときの共通シナリオとなります。
* **アプリケーションおよびデータへのアクセスに関する、法的な規制や地理的なポリシー.** シングル･フォレストにおける全てのドメインが、自動化された双方向のKerberosトラストを持つことで、データとアプリケーションへのアクセスが容易になります。いくつかの国や地域をまたいだ作業が行われるとき、法律上の要件が、データとアプリケーションの分離を規定するかもしれません。そのための分離を、マルチ･フォレストが提供します。

マルチ･フォレストの実装は、環境を管理するためのコストを増大します。マルチ･フォレストの維持とサポートのためのに、追加のハードウェアとソフトウェアが必要とされ、また、追加のスタッフも必要とされるかもしれません。

フォレスト間を横断する情報共有が要求とされる場合には、クロス･フォレスト･トラストが必要です。これらのトラストは、Windows Server 2003 と Windows Server 2008 による環境において、Kerberos をサポートします。

グローバル・カタログは、フォレスト境界をまたいで複製を行いません。マルチ･フォレストを網羅するための統一されたビューを得るには、[Identity Lifecycle Manager 2007](http://www.microsoft.com/miis/default.mspx)のような、ディレクトリ同期ソフトウェアを実装する必要があります。 このようなテクノロジーの実装が、マルチ･フォレストにおける管理上の負担を増やします。

### いくつのフォレストが？

マルチ･フォレストへの必要性が確認されるとき、要求されるフォレスト数の正確な値を決定しなくてはなりません。すべてのビジネス要件が取り上げられるまで、また、必要とされるフォレストの合計が確認されるまで、フォレスト決定のプロセスを反復します。

## **特性に関する評価**

|  |  |  |
| --- | --- | --- |
| 複雑さ | | |
| シングル･フォレスト | シングル･フォレストは、Active Directory 展開における入り口になります。つまり、複雑さの低減が可能になります。 | Low |
| マルチ･フォレスト | 2番目以降のフォレストは、対象となる環境における複雑さを増大します。 | High |

|  |  |  |
| --- | --- | --- |
| コスト | | |
| シングル･フォレスト | シングル･フォレストは、ハードウェアと、ソフトウェア、管理サポートへの要求が少ないため、最も費用のかからない選択となります。 | Low |
| マルチ･フォレスト | デザインに加えられる個々のフォレストにおいて、ハードウェアと、ソフトウェア、管理などの費用が増大します。 | High |

|  |  |  |
| --- | --- | --- |
| セキュリティ | | |
| シングル･フォレスト | フォレストはセキュリティ境界でもあり、管理者は、その中のすべてのリースにアクセスできます。 | － |
| マルチ･フォレスト | それぞれのフォレストにおける管理者は、セキュリティ責任者になります。マルチ･フォレストを用いて責任を分担することで、全体的なセキュリティ･レベルが向上するしょう。 | Up |

## **ビジネスの視点からの検証**

IT に関連する基準を背景として、この Step 1 における判断と決定を評価します。また、それらの決定がビジネスにおよぼす影響についても、同様に実証すべきです。フォレストのデザインを決定する上で、以下のような質問が影響をおよぼすとされています：

* **近い将来に、企業買収の可能性はあるのか?** 近い将来に企業買収の可能性があるなら、その後に廃棄されるかもしれないディレクトリをデザインするよりも、詳細なデザインについて相手の企業と検討する方が賢明かもしれません。その相手先が、新しいビジネスに進出している最中なら、それに関連する要件をデザイン･フェーズで検討すべきです。たとえば、そのための管理要件が、提起されるかもしれません。フォレストを分離することで、ビジネス･ユニットの売却において、より容易で単純な移行が実現されるかもしれません。
* **近い将来に、分離の要件が生じるのか?** 差し迫ったコンプライアンス規定などにより、分離の要件が生じるかもしれません。

## Task **と検討項目**

それぞれの環境内におけるフォレストに対して、時刻の同期について検討することは重要です。数分内に相互に同期する、ドメイン・コントローラおよび、サーバー、クライアントの時刻に、Kerberos は依存します。この条件が充たされない場合には、Kerberos 認証は失敗してしまうでしょう。時刻という要素は、ディレクトリのヘルス･ステートを算定するために用いられる、検討項目のひとつです。Active Directory が依存する相手は、ルート･ドメインで PDC（primary domain controller）エミュレータ･ロールを担うドメイン・コントローラとなります。そして、この依存関係により、フォレスト内の全てのドメイン･マスタ時刻が維持されます。ドメイン・コントローラの時刻を規定するための、2つの選択枝があります。

ここで言う、組織における時刻の同期には、内部ソースを利用する場合と、外部ソースを利用する場合の2通りがあります。内部ソースを使う場合には、インターネット上の Timeサーバー への同期が可能となります。さらに、信頼できる時刻を保証する認証メカニズムを、時刻ソースとドメイン・コントローラから活用できるようになります。外部ソースを用いる場合には、この認証メカニズムが提供されません。また、手作業による時刻の設定と更新は、推奨できません。Active Directory 環境は、時刻に大きく依存します。そして、時刻が適切に設定されていないと、深刻な問題を生じることがあります。

## **意思決定のサマリー**

シングル・フォレストが理想です。その管理が容易になるだけではなく、実装や、維持、サポートを低コストで行えます。その反対に、法令や、組織、運用、応用などの要件がある場合には、マルチ･フォレストが必要になります。

## **参考資料**

“Creating a Forest Design” ： <http://technet2.microsoft.com/windowsserver/en/library/fba18139-1168-4259-82b3-c3b4c81945981033.mspx?mfr=true>

“How to configure an authoritative time server in Windows Server 2003” ： <http://support.microsoft.com/kb/816042/>

# 

# Step 2: **ドメインの数を決定する**

この Step 2 では、組織の目的を充たすために必要な、Active Directory デザインにおけるドメイン数を決定していきます。それぞれのフォレストは固有のものであり、また、他のフォレストから分離されるため、フォレストごとのドメイン数については、他のフォレストとは別個に考えなければなりません。

すでに、最初のデザインが実装された後に、ドメインを追加および削除する作業は、常にシンプルというわけではありません。コンピュータおよび、ユーザー、データ、アプリケーションの移行は複雑なタスクであり、また、ドメイン数への修正が生じるでしょう。

## Option 1: **シングル･ドメイン**

この Option 1 のデザインでは、少なくとも 1つのドメインを持つ必要性が生じるでしょう。そして、マルチ･フォレストの場合には、少なくともフォレストごとに1つのドメインが必要になるでしょう。シングル･ドメイン･モデルは、以下のアドバンテージとメリットを持ちます：

* シングル･ドメインは、安価な選択肢となります。ドメインの追加は、ハードウェアや、ソフトウェア、管理におけるコストを増大させます。
* シングル･ドメインの管理は、比較的に容易です。 ドメインの追加により、マネージメント･オーバーヘッドと間接コストが増大していきます。
* シングル･ドメインは、災害時の回復などが比較的に容易となります。

## Option 2: **マルチ･ドメイン**

以下にリストアップする、どれかの要件により、マルチ･ドメインを用いるデザインへと導かれるでしょう：

* 10万人のユーザーあるいは、10万台のコンピュータ･オブジェクトの結合により構成される環境では、ドメインにおける複製トポロジーの負荷が、限界を上回らないことをラボでのテストで検証すべきです。マルチ･ドメインでは、全体的なドメイン複製の負荷を減らすように要求されるでしょう。
* Active Directory 内に、変更頻度の高い大量の属性が含まれる場合には、ドメイン内の複製を制御するために、その環境をマルチ･ドメインに分割する方式が有用かもしれません。複製のためのトラフィックの削減が、有効な方式で実現できるかどうかを判断するために、マルチ･ドメインについてはラボでのテストを行うべきです。
* 低速のリンクを介してディレクトリ･サービス全体の変更をリプリケートするときには、適切な圧縮アルゴリズムの利用が、きわめて効率的なソリューションになります。しかし、低速のリンクが要因となり、複製における問題が改善されない場合には、別個のドメインが必要になるかもしれません。このシナリオの効果を試すには、通常に運用されているディレクトリ･サービス･オブジェクトに、多数の変更が生じる状況が必要になります。
* 従来のオペレーティング･システムにおいて運用されている、既存の Microsoft ディレクトリを維持していく必要があります。それを実現するために、対象となる環境を、それぞれのドメインに分割することが可能です。

Note   Windows Server 2008 は、きめ細かいパスワード･ポリシーをサポートされます。この新技術は、同一ドメイン上で、マルチ･パスワード･ポリシーをサポートします。Windows 2000 あるいは Windows Server 2003 のドメインは、ひとつパスワード･ポリシーだけを、ドメインごとにサポートします。

マルチ･ドメインを選択することで、環境を管理するためのコストに対して、以下のように影響がおよぶでしょう：

* ドメインを維持するために、スタッフの追加が必要になるでしょう。そして、ドメインごとに管理者グループが作られていくでしょう。
* マルチ･ドメインを管理するために、より多くのスタッフが必要になるでしょう。それにより、さらに複雑な、マネージメント要件のセットが生じます。
* ドメインのインスタンスを作成するために、追加のハードウェアとソフトウェアを取得しなければはなりません。
* ドメインあるいは OU に適用すべきグループ･ポリシーの 設定を、フォレスト内のドメインごとに適用させる必要性が生じるでしょう。

### いくつのドメインが？

マルチ･ドメインの必要性が認識されてはじめて、フォレストごとの正確なドメイン数が決定されます。確認された個々の検討項目を解決するために、複数ドメインの構築を検討します。

## **特性に関する評価**

|  |  |  |
| --- | --- | --- |
| 複雑さ | | |
| シングル･ドメイン | シングル･ドメインのディレクトリは、複雑になりません。 | Low |
| マルチ･ドメイン | それぞれのドメインを追加することで、複雑さが増大します。ただし、別のドメインを追加するだけの場合は、コストとマネージャビリティの増大ほどには、複雑さを加えることはありません。 | High |

|  |  |  |
| --- | --- | --- |
| コスト | | |
| シングル･ドメイン | シングル･ドメインにおけるセットアップと運用では、そのコストが最小になり得ます。 | Low |
| マルチ･ドメイン | それぞれのドメイン・コントローラのためのハードウェアとソフトウェアのコストは別にして、そのためのインストールやコンフィグレーションの要件により、追加されるドメインごとにセットアップ･コストが増大します。 | High |

## **ビジネスの視点からの検証**

IT に関連する基準を背景として、この Step 2 における判断と決定を評価します。また、それらの決定がビジネスにおよぼす影響についても、同様に実証すべきです。フォレストのデザインを決定する上で、以下のような質問が影響をおよぼすとされています：

* **法的要件のために、ビジネス･ユニットを分離する必要性はあるのか?** いくつかの企業や、多くの政府や、大学、軍事機関における環境では、一部のユーザーやコンピュータが、分離されたドメインに存在することが要求されます。こうしたポリシーが存在する場合には、Windows NT 4.0 以降のバージョンで確立されたドメインが、セキュリティの境界線ではないことを再評価すべきです。このようなポリシーが、分離の要件に関わってくる場合には、フォレストの分離が必要とされるでしょう。
* **Are there different administrative units that need to be autonomous?** 大半のケースにおいて、管理部門に自立性を提供するために、シングル･ドメイン内の OU レベルで委任を用いることが可能です。ただし、ポリシーおよび、組織構造、運用管理などの要因により、ドメインの追加が必要になるかもしれません。

## **意思決定の概要**

それぞれのフォレスト にとって、シングル･ドメインがデフォルトのコンフィグレーションとなります。シングル･ドメインでは解決できない、テクニカルおよびビジネスの関心事を解決することで、必要なドメインだけを追加します。それぞれのドメインでコントローラーを実行する必要があるため、ハードウェアとソフトウェアのインストールなどが増大し、ドメインを追加するためのコストが生じます。

決定された事柄を、このガイドの Appendix における補足資料に記録してください。

**Important!**   ドメイン数は、それぞれのフォレストごとに決定する必要があります。

## Additional Reading

## **参考資料**

“Creating a Domain Design” ： <http://technet2.microsoft.com/windowsserver/en/library/60b6817e-4123-4bb0-8646-964c83b2e3281033.mspx?mfr=true>

“AD DS: Fine-Grained Password Policies” ： <http://technet2.microsoft.com/windowsserver2008/en/library/056a73ef-5c9e-44d7-acc1-4f0bade6cd751033.mspx?mfr=true>

# Step 3: **ドメイン名を割り当てる**

Active Directory デザインにおける Step 3 は、それぞれのドメインに名前を割り当てることです。割り当てるべき名前としては、DNS名と NetBIOS名の 2つがあます。 Windows Server 2008 は名前解決のために、Windows Internet Name Service (WINS) NetBIOS に替えてDNS を使用します。しかし NetBIOS は、Microsoft Windows NT 4.0 ベースのネットワークにおける名前解決の手段であり、それが必要なアプリケーションを利用する、大半の組織において要求されています。

## Task 1: NetBIOS **名の割り当て**

Windows でドメイン名の入力を促されるとき、最も頻繁にユーザーが目にするのが NetBIOS 名です。そして、それぞれのドメインは、NetBIOS 名の割り当てを要求します。NetBIOS 名はネットワーク上でユニークでなければならず、同じものが使用されると、名前解決の競合が生じます。

同じエンティティを表すために、同じ NetBIOS 名が、複数の企業で使われる可能性があります。たとえば、「CORP」という NetBIOS 名は、企業内のネットワーク名として多くの組織で使用されます。この場合、もし2つの企業合併し、それぞれが NetBIOS 名 CORP を使用していると、2つのネットワークが統合されるときに競合が生じるでしょう。

名前解決の競合を避けるためには、たとえば Contoso という社名の場合には CONTOSOCORP といったような、他の企業では使われない固有の NetBIOS 名を使うべきです。つまり、既存の地域や組織の名称とは、重複しないような名前を使うべきです。

## Task 2: DNS **名の割り当て**

NetBIOS と同様に、さまざまな規則が、DNS ネーミングにも適用されます。この Step 3 の最後にある “参考資料”で は、それらの規則に関する情報へのリンクを提供します。

Active Directory ドメインの DNS 名は、2つのパートであるホスト名とネットワーク名を含みます。これらの名前が連結されるとき、リソースに対する曖昧性を排除した名前が作成されます。そして、このホスト名が、Active Directory ドメイン名となります。

最初に、ネットワーク名を決定します。この場合のベスト･プラクティスは、登録されるインターネット･ドメイン名を、企業名と一致させることです。そのような名前は、インターネットの至るところでユニークであり、名称に関する他の企業のオーナーシップと競合しません。それにより、合併や買収の際に、名前の競合に関するリスクが低減されるでしょう。

第二に、ドメインに対するホスト名を選択します。デフォルトのネーミング･スキームは、CONTOSOCORP のような NetBIOS 名や、contosocorp.com のような DNS を 作成することです。DNS 名とNetBIOS 名を結び付ける容易なトラッキングのために、また、ネットワークや Active Directoryに関するトラブル･シューティングのために、それらの名前を共通にしておくことは良い考えですが、必要とされるわけではありません。

他社との重複を防ぐために、既存の企業が登録している Internet DNS ドメイン名をリプリケートしてはいけません。ベスト･プラクティスは、 社内と社外で使用されている、すべてのトップレベル･ドメイン名（ネットワーク名として認識されている）を登録することです。インターネットにおける固有のグローバルDNS 名を保証するために、Internet Network Information Center (InterNIC) を使用します。

## **ビジネスの視点からの検証**

IT に関連する基準を背景として、この Step 3 における判断と決定を評価します。また、それらの決定がビジネスにおよぼす影響についても、同様に実証すべきです。フォレストのデザインを決定する上で、以下のような質問が影響をおよぼすとされています：

* **現時点のインターネット･ドメイン名の、利用について計画する。別の DNS 名前空間や、識別の方式を要求する、グループおよびアプリケーションは存在しないか?** 対象となるフォレスト内で、分離されたドメインをサポートする場合には、それぞれの DNS 名が必要とされるでしょう。
* **合併や買収の計画はないか?** 組織構造の変更が、ネーミング構成に影響を与えるでしょう。

## **意思決定の概要**

ドメイン名は、簡潔性を維持すべきであり、また、インターネット DNS 名前空間との一貫性を持つべきです。NetBIOS 名と DNS 名の双方に対して、一貫性および、マネージャビリティ、複雑さを検討する必要があります。

実装後の名称の変更は、すべてのコンピュータおよび、アプリケーション、スクリプトにおいて、新しい名前への更新が必要になるため、きわめて困難な作業となります。さらに、ユーザーはログオン時において、また、ドメインに関連するアプリケーションの利用において、ドメイン名を取り扱います。そのため、ドメイン名の変更は、紛らわしく、破壊的なものになるでしょう。

**Important!**   すべてのフォレスト内の、すべてのドメイン名を決定するための判断のプロセスを実施し、その結果を Appendix の補足資料に記録します。

## **参考資料**

“Naming conventions in Active Directory for computers, domains, sites, and OUs”：<http://support.microsoft.com/kb/909264>.

“Namespace planning for DNS” ：<http://www.microsoft.com/windows/windows2000/en/advanced/help/sag_DNS_imp_NamespacePlanning.htm>.

# Step 4: **フォレスト･ルート･ドメインの選択**

Active Directory フォレストに最初に配置されるドメインを、フォレスト･ルート･ドメインと呼びます。このドメインは、Active Directory を展開するライフサイクルにおいて、フォレスト･ルートとしてのドメインを保持します。したがって、あとでそれを変更する際には、フォレスト全体を再展開する必要が生じてしまいます。

フォレスト･ルート･ドメインには、Enterprise Admins と Schema Admins のグループが含まれます。これらの管理者グループは、ドメインの増減や、スキーマの変更といった、フォレスト･レベルでの運用管理のために用いられます。

このデザインの中心に位置づけるドメインを、フォレスト･ルートとして選択すること、もしくは、専用のフォレスト・ルートを選択することが可能です。フォレスト･ルート･ドメインが確立された後には、フォレスト自体を再構築しなければ、その変更は行えなくなります。

## Option 1: **計画されたドメインの使用**

シングル･ドメインを指定するフォレストのデザインにおいては、そのシングル･ドメインがフォレスト･ルート･ドメインになります。このドメインは、すべてのユーザーおよび、グループ、コンピュータ、フォレスト･ルート･グループに対して、単体のホストとして機能するでしょう。

そのデザインにマルチ･ドメインが含まれる場合には、それらのドメインの1つを、ユーザーとリソースを管理するフォレスト･ルート･ドメインとして選択できます。そこで選択されたドメインは、対象となる環境で最初のドメインとして展開される必要があり、また、フォレストの名前空間を定義するものになるでしょう。 そのドメインは、ユーザーとリソースの管理を行いますが、Enterprise Admins と Schema Admins を取り込んだドメインとして、特別なステータスを常に維持するでしょう。

## Option 2:**フォレスト･ルート専用のドメイン**

フォレスト･レベルの機能を管理するだけのために、中身が空のフォレスト･ルート専用のドメインを、既存のドメイン構造に加えるケースがあるかもしれません。このドメインが選択されるとき、フォレスト･ルート･ドメインのためのサービス管理者アカウント以外の、ユーザー・アカウントやリソースは組み込みません。また、そのドメインは、いかなる領域も表現しません。 すべてのドメインは、このドメインの子供となります。

一般的に、専用のフォレスト･ルートが選ばれるときには、以下のような理由があります：

* フォレスト管理者を、ドメイン･サービス管理者から、運用上の理由のために分離する。
* 他のドメインにおける運用上の変更から、影響されないようにする。
* 領域間に従属関係が生じないように、ニュートラル･ルートとして振舞う。

ただし、注意しなければならないのは、ディレクトリの完全性とセキュリティを危うくするような不適切な方式で、Active Directory データベースを操作する管理者からは、フォレスト･レベル機能が保護されないことです。中身が空のフォレスト･ルートにより、管理者グループが機能面で分離されても、適正を欠く管理者からは、フォレストに対するセキュリティは提供さません。

## **特性に関する評価**

|  |  |  |
| --- | --- | --- |
| Cost | | |
| 計画されたドメイン | 計画されたドメインとして使用される場合には、フォレスト･ルートとしての追加コストは発生しません。 | Low |
| 中身が空のルート･ドメイン | フォレスト･ルートをホストするだけの中身が空のルート･ドメインは、そのドメインを実行し、その機能を保持するための、ハードウェアとソフトウェアのコストを生じます。 | High |

## **ビジネスの視点からの検証**

IT に関連する基準を背景として、この Step 4 における判断と決定を評価します。また、それらの決定がビジネスにおよぼす影響についても、同様に実証すべきです。フォレストのデザインを決定する上で、以下のような質問が影響をおよぼすとされています：

* **合併や買収の計画はないか?** 組織構造の変更は、フォレスト･ルートの配置に影響を与えるでしょう。

## **意思決定の概要**

この段階で、フォレスト･ルート･ドメインの独自性が決定されます。計画されたドメインが選択されるケースと、新しいドメインがフォレスト･ルートとして追加されるケースがあります。

# Step A1: OU **の構造をデザインする**

OU（organizational units）を使用することで、ディレクトリ内のオブジェクトが整理されます。 OU のためのデザインは、ディレクトリ･オブジェクトにおける管理の委任と、Group Policy Object（GPO）の適用という、2つの主な役割を担うでしょう。基本的に、OU デザインは、ドメイン内のオブジェクトの管理方式を反映すべきです。

OU デザインの変更は難しくはありませんが、アクセス･コントロール･リストの慎重な取り扱いが必要があるため、複雑なものにもなり得えます。委任と Group Policy が確立された後の、コンフィグレーションにおける OU デザインの変更は、時間を要するものになるでしょう。

OU は、管理の委任とGroup Policy の適用という2つの役割を担うため、OU のデザイン･プロセスを双方に対して実施する必要が生じるでしょう。一度目は委任の視点から、そして、二度目は、Group Policy 用法の視点からとなります。

## Task 1: **管理と委任のための OUをデザインする**

ユーザーやコンピュータなどのオブジェクト管理を、指名されたグループに委任することも、OU の用途には含まれます。 個人に許可を付与することも可能ですが、組織内の人員が変更されるにつれて、グループの利用がベスト･プラクティスになっていきます。

ディレクトリ内のオブジェクトに対して許可を更新することよりも、委任グループ内のメンバーシップを更新するほうが容易です。OU を用いる委任は、以下のタスクに関連します：

* 権限を委任される管理者グループを作成する。
* OU 内に委任される権限に対して、個人あるいはグループを割り当てる。 権限を持つ管理者グループに対して、OU を作成する。
* それぞれの OU 内の管理者グループに委任されるべき、オブジェクト権限を割り当てる。
* 制御されるべきオブジェクトを、OU内に作成し、配置する。

管理者タスクが委任されるグループを識別するとき、必要とされる最小限の制御について、可能な限り具体的に指定すべきです。たとえば、対象となるグループにとって、ユーザーの電話を更新することだけが必要な場合には、そのグループに全体的な制御を与えるべきではありません。

## Task 2: **グループ･ポリシーのためのOUをデザインする**

OU は Group Policy 設定を、コンピュータやユーザーの特定サブ･グループに、適用するために作成できる。

デフォルトでは、 適用されたGroup Policy Object（GPO）に含まれる設定を、OU 内の全オブジェクトが取得します。

委任（あるいは運用）の見通しに基づき、OU デザインを完成させます。続いて、Group Policy 設定が取り入れるかもしれない固有の状況であっても、それに対応するための OU デザインの修正に取り組みます。 たとえば、すべてのワークステーションを管理する権限を委任するために、“Workstations” と呼ばれる OU が確立されるかもしれません。また、Group Policy について検討するときも、デスクトップとノートブックというポリシーへの要求を反映するために、Desktop OU と Mobile OU が必要になるかもしれません。このケースにおいて、Desktop OU や Mobile OUは、Workstations OUの中の sub-OU として作成されるかもしれません。また、Desktop OU もしくは Mobile OUにより、Workstations OU が置き換えられるかもしれません。

GPO を適用しなければならない、ユーザーとマシンのグループを識別します。そのときに、ドメインにとって最新の OU デザインを調べ、 可能であれば既存の OU を再利用します。また、必要に応じて、新しい OU を作成します。GPO をサポートするために新しい OU を作成する場合には、オブジェクト管理と運用が最新であることを保証するために、Task 1 におけるオブジェクト管理の委任を確実に再検証します。

Group Policy の応用については、フィルタリングとターゲティングに関する、数多くのオプションが提供されています。GPO を取得するオブジェクトを対象に定めるために、Security フィルタリングおよび、Windows Management Instrumentation（WMI）フィルタリング、そして Group Policy プリファレンス・ターゲティングの全てを使用できます。これらのテクニックは、Group Policy の適用性と優先性に代えて、最終手段として使用するためのものです。その欠点として、フィルタリングされたGroup Policy セキュリティは、そのトラブルシュートと管理がきわめて困難になる点があげられます。また、クライアント･ログオンおいても、多少のパフォーマンス低下が引き起こされる可能性があります。

## **意思決定の概要**

このデザインにおける個々のドメインに対して、ここで説明した OU の構造を定義する必要があります。以下の項目を認識しながらOU をデザインし、最終的な判断を下すべきです：

* 管理の委任あるいはGroup Policy の応用という、2つの基準のいずれかに基づいて、OU は作成されます。
* それぞれの OU 内に配置すべきオブジェクトを決めます。
* 管理（委任）グループを作成し、OUに対してマップすべきです。
* OU ごとの各グループに対して、オブジェクトの権限を与えます。
* 作成が必要な GPO を決定し、リンクすべき OU を決定します。

## **参考資料**

*Best Practice Active Directory Design for Managing Windows Networks* ： <http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/activedirectory/plan/bpaddsgn.mspx>.

# Step B1: **ドメイン・コントローラの配置ついて決定する**

一般的に、ネットワーク･トポロジーは、コンピュータおよび、ネットワーク接続、ユーザーの集合を取り込むハブとして捉えることができる、数ヶ所の物理ロケーション（大規模キャンパス／オフィスビル／データセンター）を持ちます。そして、それらのハブは、たとえば支社やホーム･オフィスのような、数多くの小規模サテライト･ロケーションに対して、ネットワークやコンピュータのリソースを提供するために接続されるでしょう。一般的に、サテライト･ロケーションから、他のサテライト･オフィスに対して、サービスが提供されることはありません。

この Step B1 では、フォレストごとの各ドメインにおいて、ドメイン・コントローラのリソースを配置する場所を決めていきます。次の Step B2 では、いくつのドメイン・コントローラを、それらのフォレストやロケーションに配置すべきかという点に取り組んでいきます。

コストを低減し、複雑さを排除し、さらにマネージャビリティを向上させるためには、ドメイン・コントローラの配置箇所を、可能な限り絞り込むことが重要になります。そして、組織にとって、最も有益な利用を実現し、また、最も高い価値を与える場所に配置します。

もうひとつの検討ポイントとして、少なくとも地理的に分散された2つのロケーションに、それぞれのドメインのためのドメイン・コントローラが配置されるように考えるべきです。それにより、一方のロケーションに災害が発生した場合においても、ビジネスは停止することなく、その連続性が維持されます。

すべてのドメイン・コントローラに対して、物理的な面で安全性を維持する必要があります。物理的なセキュリティが確保できないロケーションには、フル･ドメイン・コントローラを配置すべきではありません。ただし、Read-Only Domain Controller であれば、物理的なセキュリティに不安があるロケーションにも配置できます。 それについては、次の Step B2：ドメイン・コントローラの数を決める”の“ドメイン・コントローラのタイプを、配置するロケーションに応じて決定する” を参照してください。

ドメイン・コントローラの配置については、いつでも容易に変更することが可能です。

## Task 1: **ハブ･ロケーション**

ハブ･ロケーションは、組織内の数多くのユーザーに対して、コンピュータとネットワークのサービスを提供します。また、それらのリソースは、ハブ内のユーザーに提供されるだけではなく、複数のサテライト･ロケーションにも提供される可能性があります。

ハブは中心的なポイントになるため、理想的には、最も効率の良いロケーションに配置すべきです。つまり、ハブには、いくつかのサテライト･ロケーションを集約するポイントになる可能性があります。したがって、それぞれのロケーションが、独自のドメイン・コントローラをホストする状況と比べて、ハブがドメイン・コントローラをホストする状況の方が、コストを低減できます。

どのハブ･ロケーションが、どのドメインのためのコントローラーのホストとして機能するのか、それらの点について判断を下し、その結果を補足資料に記録します。

## Task 2: **サテライト･ロケーション**

サテライト･ロケーションは、ハブを介してネットワーク全体と接続します。 大半のケースにおいて、ハブよりは少ないユーザーとコンピュータが、サテライト･ロケーションに含まれます。サテライト･ロケーションでは、クライアントおよび、ローカル･リソース、ハブ･リソースの使用が可能であり、また、ハブを介してネットワーク･リソースへアクセスすることも可能です。サテライト･サイトへのドメイン・コントローラの配ついては、いくつかの視点から、その必要性を示すことができます。

ドメイン・コントローラについては、その管理が重要になります。ドメイン・コントローラを特定ロケーションに配置する際には、そのドメイン・コントローラがセキュアに接続され、さらに、ローカルあるいはリモートで管理できることが条件となります。

ネットワーク･リソースへのアクセスでは認証が要求されるため、ドメイン・コントローラにおける通信は、欠かすことのできない要素となります。したがって、サテライト･オフィスからハブまでのWANリンクが信頼できない場合や、コストの問題で遅延が予測される場合には、サテライト･オフィスにドメイン・コントローラを配置し、クライアント認証を受け入れる方式を検討すべきです。

ドメイン・コントローラをサテライト･オフィスに配置する際の、認証以外の検討すべき要素として、通常のネットワーク･トラフィック利用に耐え得る、WAN リンクにおける帯域幅の確保があげられます。いくつかのケースにおいては、一般的なアプリケーションやサービスで用いられる帯域幅が、サテライト･オフィスの WAN ネットワーク･トラフィックでも要求される可能性があります。このような場合には、サテライト･オフィス内に、ローカルなドメイン・コントローラが必要になるかもしれません。

ドメイン・コントローラをサテライト･オフィスに配置する際の、もうひとつの検討ポイントは、サテライト･オフィスに存在すると思われる、サービスやリソースを受け入れることです。DNS や DFS (Distributed File System) のようなサービスだけではなく、メールやデータベースのようなリソースの利用も、 ディレクトリの認証と管理のために WAN リンクを横断することなく、同一のネットワーク上にドメイン・コントローラを持つことで利益を受けます。

サイトの自立性により、特定のロケーションにメイン･コントローラーが配置されるケースもあります。たとえば、ある企業において、リモート･ロケーションに製造施設があり、さらに、製造ラインが適切な認証を必要とする場合には、このサテライト･ロケーションにドメイン・コントローラを配置することが、 WAN が利用状況にかかわらず継続的な生産を実現します。

どのサテライト･ロケーションが、どのドメイン・コントローラのホストとして機能するのか、その点について判断を下し、その結果を補足資料に記録します。

## **ビジネスの視点からの検証**

IT に関連する基準を背景として、この Step B1 における判断と決定を評価します。また、それらの決定がビジネスにおよぼす影響についても、同様に実証すべきです。フォレストのデザインを決定する上で、以下のような質問が影響をおよぼすとされています：

* **サテライトロケーション間を頻繁に移動し、それらの場所で迅速なログオンおよびディレクトリのサービスを要求するユーザーはいるのか?** 移動ユーザーに対してローカル･エクスペリエンスを提供するために、いくつかのサテライト･ロケーションでは、ドメインが必要とされるでしょう。

## Task **と検討項目**

ドメイン・コントローラをハブやサテライトに配置するとき、DNS 内にサイト･ロケーションを記録するドメイン・コントローラに対して、制御する必要性が生じるかもしれません。たとえば、サテライト･サイト内のドメイン・コントローラに障害が生じた場合には、クライアントがコンタクトすべき先は、別のサテライト･サイトに配置されたドメイン・コントローラではなく、近くにあるハブ内のドメイン・コントローラになります。この方式は、2つのポイント間の WAN リンクの信頼性が高くない場合に、とりわけ重要な解決策となります。計画の対象となる環境において、そのような懸念を明らかにしていきます。“参考資料” セクションの、追加情報を参照してください。

## **意思決定の概要**

ドメイン・コントローラのハブとサテライト･ロケーションへの配置は、その状況が適切な場合に実施します。大半のハブ･ロケーションが、1つもしくは複数のドメイン・コントローラを必要とします。WAN リンクの特性や、クライアントとリソースの量に応じて、サテライト･オフィスへのドメイン・コントローラの配置が必要とされるでしょう。すべてのフォレスト内の、すべてのドメインに対して、この決定のプロセスを繰り返して適用することを忘れてはなりません。

## **参考資料**

“Planning Domain Controller Placement” ：<http://technet2.microsoft.com/windowsserver/en/library/c0834916-4166-4f81-894a-acd1276f8c6d1033.mspx?mfr=true>.

“How Domain Controllers are Located in Windows” ： <http://support.microsoft.com/kb/247811/>

“How to optimize the location of a domain controller or global catalog that resides outside of a client’s site” ： <http://support.microsoft.com/?id=306602>

# Step B2: **ドメイン・コントローラの数を決める**

Step B1 では、ドメイン・コントローラの物理的な配置を決定する際に、必要となる事柄について取り組んできました。この Step B1 では、それに関連する事柄として、それぞれのロケーションにおけるドメイン・コントローラの数を決定していきます。

それぞれのドメインが持つべき、ドメイン・コントローラの数については、決定すべき数多くの要因があります。それらを 決定するときの基本的な判断材料は、認証のパフォーマンスおよび、リソースへのアクセス、複製、コストなどになります。

## Task 1: **ドメイン・コントローラの数を決める**

Step B1 で確認された、ロケーションごとの各ドメインにおいて、ドメイン・コントローラ数を最小にするための検討が必要になります。以下のテーブルに、ユーザー数に基づいて要求される、ドメイン・コントローラの最小数を示します。

Table 3. ドメイン・コントローラの最少数

|  |  |
| --- | --- |
| ドメインごとのユーザー数 | **ドメインごとの最小のドメイン・コントローラ数** |
| 1–499 | One – Single Processor |
| 500–999 | One – Dual Processor |
| 1,000–2,999 | Two – Dual Processor |
| 3,000–10,000 | Two – Quad Processor |

サイト内に 1万人以上のユーザーがいる場合には、追加ハードウェアの必要性を決定するために、そのユーザー負荷について追加のテストを実施すべきです。 以前のガイダンスでは、5千人のユーザーに対して必要以上の Quad プロセッサ･システムを規定しましたが、認証の負荷だけであれば、大半の環境において過剰となるでしょう。

1 つのドメイン・コントローラだけがロケーションごとに存在する場合には、ロケーションを超えた認証のためにドメイン・コントローラと通信することを想定して、WANを測定する必要があります。また、ローカルなドメイン・コントローラで障害が発生したときの、リソース･アクセスについて検討する必要性も生じるはずです。

ドメイン内のすべてのドメイン・コントローラは、ドメインに関係する、すべての情報を完全に検知しなければなりません。それはドメイン・コントローラ間での、Active Directory データベースの複製により処理されます。この複製は Active Directory サイト内で発生し、サイト境界線をまたぐものとなります。前提となるサイト内の複製パートナー数が 15個を超えようとする場合には、追加のドメイン・コントローラをサイトに加えるべきです。そのドメイン・コントローラは、これから追加される 15 個の複製パートナーのためのものになります。

Active Directory データに依存する、すべてのアプリケーションについて再確認してきます。 Exchange Server などの、いくつかのアプリケーションは、正確な動作を保証するために追加のドメイン・コントローラを必要とします。 それらのアプリケーションで予想される負荷と要件に基づき、ドメイン・コントローラを追加する必要性について評価してください。

## Task 2: **ドメイン・コントローラのタイプを、配置するロケーションに応じて決定する**

それぞれの確認されたドメイン・コントローラに対して、書き込み可能もしくは、読み出し専用の、いずれの設定をするのか、その点について判断していきます。フル･ドメイン・コントローラについては、物理的なセキュリティが保証されるロケーションだけに配置すべきです。

RODC（Read Only Domain Controller）を用いる主な理由は、脆弱な物理セキュリティを持つロケーションのためとなります。RODC はリード･オンリーであるため、書き換えが生じることはなく、また、書き込み可能なドメイン・コントローラにリプリケートされることもありません。認証を目的にする場合、RODC から フル･ドメイン・コントローラに対する、上流へと向けたアクセスが必要となります。デフォルトでは、パスワードのためのハッシュが、RODC にリプリケートされることはありません。 RODC はログオン･リクエストを、書き込み可能なドメイン・コントローラに転送します。必要とされるパスワードハッシュをRODC にキャッシュするようにコンフィグレーションすることも可能です。このような処理によってRODC が脆弱になるような場合には、RODC にリプリケートされたハッシュのみをリセットすることができることを把握しておきましょう。

RODC からのリクエストに対して、WANがダウンしている場合や、フル･ドメイン・コントローラが使用できない場合に、このようなRODC が提供する機能は影響を受けるでしょう。

書き込み可能なドメイン・コントローラと、リードオンリーのドメイン・コントローラ識別し、その結果を補足資料に記録します。

## **意思決定の概要**

ドメインにフォールト･トレランスを提供するためには、最小で2つのドメイン・コントローラが必要となります。 以前に記述されたビジネス要件に基づいて、ドメイン・コントローラを物理的なロケーションに配置し、ローカルな認証を提供することが可能です。ユーザー認証とアプリケーション要件に基づき、 追加のドメイン・コントローラが必要とされるかもしれません。RODC サーバーを使用することで、セキュリティとパフォーマンスを飛躍的に高めることが可能です。これらのサーバーを加えるためのコストは、シナリオが正しければ最小となります。そのため、検討すべき事柄となります。 ドメイン・コントローラの増減は、いつでも変更することが可能です。

## **参考資料**

*Windows 2000 Active Directory Sizer Tool* ： <http://www.microsoft.com/technet/prodtechnol/windows2000serv/downloads/w2kadst.mspx>

# Step B3: **グローバル・カタログの配置を決める**

グローバル･カタログ･サービスは、フォレスト内における全ドメインの情報参照を促進しますが、とりわけカレントのドメイン以外に対して有効に機能します。このカタログとは、フォレスト内のグローバル･カタログ･サーバーにリプリケートされた、それぞれのドメインに含まれる情報のサブ･セットのことです。Exchange Server のようなアプリケーションは、関連情報のためにのグローバル･カタログに大きく依存します。さらにグローバル･カタログは、ログオン･プロセスにおけるユニバーサル･グループ･メンバーシップを列挙するためにも使用されます。

すべてのグローバル･カタログ･サービスは、1つあるいは複数のドメイン・コントローラ上に物理的に存在します。また、グローバル･カタログ機能を、ドメイン・コントローラから分離する方法はありません。

The decision needs to be made as to which domain controllers in the forest will host global catalog services.

対象となるフォレスト内において、どのドメイン・コントローラがグローバル･カタログ･サービスをホストするのか、その点について決定する必要があります。

## Task 1: **グローバル･カタログの位置と数を決める**

1つのドメインだけでフォレストが構成される場合には、その中に含まれるすべてのドメイン・コントローラを、グローバル･カタログ･サーバーとしてコンフィグレーションすべきです。対象となるデータのサブ･セットは、通常のドメイン複製のプロセスを介して、すでにグローバル･カタログ上に存在しているはずです。そのため、ディスク･スペースの使用や、CPU の使用、そして、複製トラフィックなどについて、追加の要件は存在しないはずです。

フォレスト内に一般的なマルチ･ドメインが含まれる場合には、必要以上のドメイン・コントローラをグローバル･カタログ･サーバーにすべきではありません。その理由は、ストレージ要件の増大と追加の複製によるオーバーヘッドにあります。

マルチ･ドメインを取り込んだフォレストでは、それぞれのドメイン・コントローラのサブ･セットが、グローバル･カタログ･サーバーとして実行するようにコンフィグレーションされるでしょう。そして、すべてのグローバル･カタログが、それぞれのドメイン内の全オブジェクトのサブ･セットをリプリケートします。そのため、グローバル･カタログを配置する際には、追加トラフィックがもたらす帯域幅のオーバーヘッド について、慎重に検討する必要がでてきます。それに加えて、グローバル･カタログ･データをストアするための、ハードウェア要件の増大もあります。対象となる環境内において、グローバル･カタログを配置すべき位置を決定するための、意思決定フローを 図 3 に示します。



図3. 対象となる環境内に、グローバル･カタログ･サーバーを配置する際の意思決定フロー

### このロケーションで、グローバル･カタログ･サーバーを実行しなければならないアプリケーションはあるのか?

Exchange Server や、Microsoft Message Queuing、そして DCOM を使用する特定のアプリケーションなどが、グローバル･カタログ･サーバーに大きく依存します。それらのアプリケーションの特性として、クエリーに費やされる時間を短縮するために、アクセス可能なローカル･グローバル･カタログを持つときに、さらに高い性能を発揮するという傾向があります。

グローバル･カタログとして RODC を使用できる場合でも、使用できない場合で、それらのアプリケーションに制約が生じる可能性があります。Exchange Server は RODC 上で実行されるグローバル･カタログをサポートしませんが、メッセージとコラボレーションを利用する Microsoft Outlook クライアントは、アドレス帳を 参照するために RODC グローバル･カタログを使用します。

### このロケーションのユーザー数は、100人以上になるのか？

100ユーザー以上を持つロケーションの場合には、グローバル･カタログ･サーバーを配置すべきです。それにより、WAN トラフィックが低減され、WAN リンクに障害が発生した場合の損失が防止されます。

### WAN リンクは、100% 信頼できるのか？

WAN リンクの信頼性が充分ではないロケーションでは、ユーザー認証を保証するために、グローバル･カタログ･サーバーの配置を検討します。さもなければ、ユニバーサル･グループ･メンバーシップの、キャッシュをコンフィグレーションシします。

### このロケーションで、大勢の移動ユーザーが作業するのか？

あらゆるロケーションにおいて、移動ユーザーが初めてログオンするときに、グローバル･カタログ･サーバーにコンタクトする必要があります。そのため、数多くのローミング･ユーザーを含むロケーションには、グローバル･カタログ･サーバーを配置すべきです。多くのケースにおいて、WAN リンク上の多すぎるログオン数が、膨大な WAN トラフィックを引き起こし、パフォーマンスおよび生産性の低下を引き起こされます。

### ユニバーサル･グループ･メンバーシップのキャッシュは充分にあるのか？

ユニバーサル･グループ･メンバーシップのキャッシュが有効な選択肢となるのは、ユーザーが 100 人以下で、多くの移動ユーザーを含まず、さらに、グローバル･カタログ･サーバーが不要なロケーションという状況が重なった場合です。Windows Server 2003 および Windows Server 2008 上のドメイン・コントローラで、ユニバーサル･グループ･メンバーシップのキャッシュを利用することが可能です。

ユーザーがネットワークにログオンするときに、グローバル･カタログ･サーバーへの接続が行われ、そのユーザーのためのユニバーサル･グループ･メンバーシップが列挙されます。この操作を低速のリンク上で実施すると、プロセスにより膨大な時間が消費されるだけではなく、グローバル･カタログ･サーバーへの接続の失敗や、ログオン･プロセスの拒否などが起こり得ます。この問題を回避するために、ユニバーサル･グループ･メンバーシップのキャッシュを利用できます。 ユニバーサル･グループ･メンバーシップのキャッシュは、Windows Server 2003 および Windows Server 2008 で実行されるドメイン・コントローラ上で、デフォルトとして使用できます。なお、この機能は、サイトごとに実行しなければなりません。

### どれだけのグローバル･カタログ･サーバーが必要なのか？

対象となるロケーションにおいて、グローバル･カタログ･サーバーが必要だと決定されると、続いて検討すべきことは、そこで要求されるサーバー数となります。大半のケースにおいて、1～2台のグローバル･カタログ･サーバーを、それぞれのロケーションごとに配置すれば充分と思われます。 ただし、たとえば Exchange Server のようなアプリケーションの要件により、必要なグローバル･カタログ･サーバー数を増やす可能性もあります。

グローバル･カタログ･サーバーとして、コンフィグレーションするドメイン・コントローラ数を決定し、その結果を記録します。

## **ビジネスの視点からの検証**

IT に関連する基準を背景として、この Step B3 における判断と決定を評価します。また、それらの決定がビジネスにおよぼす影響についても、同様に実証すべきです。フォレストのデザインを決定する上で、以下のような質問が影響をおよぼすとされています：

* **サテライトロケーション間を頻繁に移動し、それらの場所で迅速なログオンおよびディレクトリのサービスを要求するユーザーはいるのか?** 移動ユーザーに対してローカル･エクスペリエンスを提供するために、いくつかのサテライト･ロケーションでは、ドメインが必要とされるでしょう。

## **意思決定の概要**

ドメイン・コントローラをグローバル･カタログ･サーバーとしてコンフィグレーションすることは、それを行う技術的な要因があるときにのみ実施するようにします。 高性能なグローバル･カタログ･サービスを必要とするユーザーが、対象となるサイト内の、別ユーザー･ドメインで移動するときに、例外が生じるかもしれません。

コンフィグレーションとメンテナンスにおける、費用と、管理、複雑さを低減するためには、グローバル･カタログ･サーバー数を最小限に保つようにします。

グローバル･カタログ･サーバーのデザインは、すべてのフォレストに対して、繰り返して実施する必要があります。

## **参考資料**

“Planning Domain Controller Placement” ： <http://technet2.microsoft.com/windowsserver/en/library/c0834916-4166-4f81-894a-acd1276f8c6d1033.mspx?mfr=true>

# Step B4: **操作マスタ役割の配置を決定する**

この Step B4 では、フォレスト内のドメインごとに、操作マスタ（FSMO とも言われる）の配置を決めていきます。

Active Directory 内のドメイン・コントローラは、アカウントを認証し、ディレクトリ･データベースへの書き込みを行いますが、いくつかの機能においては、シングル･ドメイン・コントローラが対象となっています。 FSMO ロールは、指名されたドメイン・コントローラ上に存在し、ドメインとフォレストにおける特定の機能を制御します。

それぞれのドメインに対して、3つのFSMOロールがあります：

* **PDC エミュレーション操作マスタ.** このロールは、Windows NT 4.0 の BDC（Backup Domain Controller）から、すべての複製を処理します。また、Active Directory クライアント･ソフトウェアを実行していないクライアントのために、すべてのパスワード更新を処理します。 さらに、このロールは、Group Policy を更新するために使われる、デフォルトのドメイン・コントローラにもなります。
* **RID操作マスタ.** このロールは、すべてのドメイン・コントローラに RID を割り当て、すべてのセキュリティ･プリンシパルが固有のセキュリティID（SID）を持つことを保証します。
* **インフラストラクチャ操作マスタ.** このロールは、操作マスタのドメインに含まれるグループ内で、メンバーシップを持つ別ドメインのセキュリティ･プリンシパル･リストを維持します。

さらに、それぞれのフォレストに対して、2つの操作マスタ･ロールがあります：

* **スキーマ操作マスタ.** このロールは、スキーマの変更を許可します。
* **ドメイン･ネーム操作マスタ.** このロールは、対象となるフォレストに関連する、ドメインおよび、サイト、ドメイン･ベース DFS コンフィグレーションについて、追加と削除に責任を持ちます。

ロールのロケーションの追跡を簡単にする、一般的なガイドラインとして、可能な限り少数のドメイン・コントローラ上に、操作ロールを保持することを推奨します。操作マスタ上へのロードについて、その移動が許可される場合には、同一サイト内の別のドメイン・コントローラ上に、RID と PDC のエミュレータ･ロールを配置します。それらのドメイン・コントローラは、直接的な複製パートナーになるべきです。

一般的には、インフラストラクチャ･マスタを、グローバル･カタログ･サーバー上に配置すべきではありません。インフラストラクチャ･マスタがグローバル･カタログ･サーバー上に配置されると、従来からのセキュリティ原則を、他のドメインから正確に識別できなくなります。例外は、すべてのドメイン・コントローラが、グローバル･カタログ･サーバーになっている場合、あるいは、シングル ･ドメインのフォレストに存在する場合となります。これらのケースにおいて、インフラストラクチャ･マスタは、それ自身が必要とする、すべての情報を持っています。

マスタに名前をつけるスキーマとドメインは、通常では使用されませんが、それらを使用するときには、厳格な制御が必要となります。グローバル･カタログをホストする、同一のドメイン・コントローラ上に、それらをまとめておくようにします。孫ドメインを作成するような特定の操作では、マスタに名前をつけるドメインを使用します。ただし、そのロールが、グローバル･カタログ･サーバー上に存在しない場合には、その処理は失敗します。

これらのドメイン・コントローラは、対象となるドメイン内で最も多くのユーザーを持ち、また、信頼性の高いネットワークを持つロケーションに配置されるものとなります。操作マスタ･ロールの配置は、容易に修正できます。

すべての FSMO ロールは、対象となる環境における、すべてドメイン・コントローラから直ちに利用可能な、ドメイン・コントローラに対して与えるべきです。FSMO をホストするドメイン・コントローラと、通信できないドメイン・コントローラは失敗するでしょう。

## Task 1: FSMO **の配置**

シングル･ドメイン･フォレストにおいては、5つのロールがシングル･サーバー上に配置さます。それらのロールを分離しても、メリットは生じません。

マルチ･ドメイン･フォレストのフォレスト･ルート･ドメインにおいて、すべてのドメイン・コントローラがグローバル･カタログ･サーバーであるなら、同一ドメイン・コントローラ上に、すべての操作マスタ･ロールを配置します。ロールを分離しても、メリットは生じません。

グローバル･カタログ･サーバーとして設定されていない、フォレスト･ルート･ドメイン・コントローラがある場合には、その設定が行われていないドメイン・コントローラに、インフラストラクチャ･マスタのロールを移動します。そして、グローバル･カタログ･サーバーとして、コンフィグレーションされないことを保証しなくてはなりません。ドメイン内の全てのドメイン・コントローラがグローバル･カタログ･サーバーでない限り、インフラストラクチャ･マスタ･ロールを、グローバル･カタログ･サーバー上に位置すべきではありません。

その他の、すべてのドメインにおいては、ドメイン固有の3つの操作マスタ･ロールを、そのドメインの最初ドメイン・コントローラ上に位置します。 また、グローバル･カタログ･サーバーでもあるドメイン・コントローラ上に、インフラストラクチャ･マスタ･ロールを配置してはなりません。

## **意思決定の概要**

すべてのディレクトリ･サービスにおける機能の完全性と正確性を、認証と管理の面から保証するという、戦略的な視点に基づいて FSMO を配置すべきです。FSMO サーバーの配置は、ルート･ドメインにおける5つのロールと、フォレスト内の別ドメインのための3つのロールを考えて、決定されなければなりません。このプロセスは、すべてのフォレストに対して完全なものでなければなりません。

## Task **と検討項目**

それぞれの操作マスタ･ロールに対して、そのロールをホストすることが可能な、ドメイン・コントローラを指定していきます。現実のロール･ホルダーに障害が生じ、スタンバイ･ロールが処理を引き受ける場合にも備えなければなりません。そのため、スタンバイしている操作マスタ･ドメイン・コントローラは、実際の操作マスタ･ホルダーの、直接の複製パートナーであるべきです。この役割を引き継ぐ、新しい FSMO ロール･ホルダーは、Active Directory に関する最新の情報を持つことになるでしょう。

## Additional Reading

## **参考資料**

“FSMO placement and optimization on Active Directory domain controllers” ：<http://support.microsoft.com/kb/223346>

“Windows 2000 Active Directory FSMO roles” ：

<http://support.microsoft.com/kb/197132>

“How to view and transfer FSMO roles in Windows Server 2003” ： <http://support.microsoft.com/kb/324801>

# Step C1: **サイト･デザインを実施する**

サイト･デザインとは 、Active Directory 内の論理的なサイト構造に対して、物理的なネットワークをマップすることです。Active Directory 内のサイトとは、1つあるいは複数の、適切に接続された TCP/IP サブネットの論理的なコレクションのことです。サイト間の複製にスケジュールを設定することで、ディレクトリの複製を制御できるようになります。Active Directory を検知するネットワーク･リソースへ向けて、クライアント･システムを誘導するために、それらのサイトを使用することも可能です。したがって、それらのサイトの論理的なロケーションは、リソースに最も近い場所になるでしょう。

以下の項目について、検討する必要があります：

* 物理的なロケーションは、サイトに対して直接的な相関性を持つべきか？
* 物理的なロケーションを、他のロケーションと共に、サイト内にグループ化できるか？

サイトが確認された後の最終的な Task は、特定のロケーションで確立している TCP/IP サブネットを、対応するサイトにマップすることになるでしょう。サイト･デザインは、必要に応じて、後に変更できます。

## Task 1: **対象となるロケーションのためのサイトを作成する**

ドメイン・コントローラが配置されている、あらゆる物理ロケーションに対して、サイトを定義していくべきです。それだけではなく、クライアントからのリクエストに応じて、最も近くにあるリソースに、それらのクライアントを誘導していかなければなりません。そのためには、サイト･トポロジー情報に依存する、リソースおよびサービスを含む物理ロケーションに対しても、サイトを定義していくべきです。

たとえば、ファイル･リソースへのアクセスを、多数の物理的なロケーションが必要とする場合には、それらのリソースを DFS（Distributed File System）環境内にコンフィグレーションできます。物理ロケーション内にリソースを含む DFS サーバーを配置した後に、それぞれのロケーションに対して、サイトのコンフィグレーションを実施していきます。そうすることで、クライアントが DFS ベースのリソースにアクセスするとき、ローカルな DFS リソースへのアクセスが実現されます。そして、WAN トラフィックの低減と、リソース･アクセスにおけるパフォーマンス向上が達成されます。

その結果として、きわめて高度な認証要件を持つアプリケーションに対して、その認証トラフィックを担うドメイン・コントローラを制御するサイトが作成されます。たとえば、大規模な Microsoft SharePoint ポータル環境では、ドメイン・コントローラ と グローバル･カタログによる相当量のトラフィックが生じるでしょう。そのような場合には、SharePoint サーバーのためのサイトを具体的に作成し、サイト固有のドメイン・コントローラとグローバル･カタログを割り当てることで、管理者によりポータル･ソリューションの認証トラフィックが制御されるようになります。

それぞれの確認されたサイトについて、そのサイトに割り当てられる、サイト名と IP サブネットを記録します。

## Task 2: 最も近いサイトとロケーションを組み合わせる

Active Directory 内のサイトと結び付けられなかった、その他の物理ロケーションについては、そのロケーションのサブネットを、既存のサイトに関連づけていきます。選択されたサイトには、最速のWAN スピードと帯域幅をコンフィグレーションされたロケーションに取り込むべきです。 このアプローチにより、対象となるロケーション内で生じるクライアント･トラフィックは、より大きなトラフィックを処理することが可能なサイトへと誘導されるでしょう。

選択されたサイトに追加される、サブネット情報の割り当てについて記録します。

## Decision Summary

## **意思決定の概要**

それぞれの物理的なロケーションを調査し、対象となるロケーションが、ディレクトリ内の新しいサイトになるべきか、それとも、他のサイトと提携すべきか、その点について判断すべきです。それぞれのロケーション内のサブネットは、それらが属するサイトに割り当てられるべきです。さらに、それぞれのドメイン・コントローラも、適切なサイトに割り当てられるべきです。

このサイト･デザインについては、それぞれのフォレストに対して適用し、また、完了する必要があります。

## **参考資料**

“Best Practices for Active Directory Design and Deployment” ：<http://www.microsoft.com/technet/community/columns/profwin/pw0302.mspx>

# Step C2: **サイト･リンクをデザインする**

Active Directory 内で定義されたサイトに接続するために、サイト･リンクを使用します。このサイト･リンクは、サイト間の接続性と、複製トラフィックで用いる方式を、反映したものになります。したがって、それぞれのサイト内のドメイン・コントローラがリプリケートされたものなら、すべてのサイトがサイト･リンクと接続しているはずです。デフォルトでは、すべてのサイトはdefault-first-site-link に属し、毎日 180分ごとに実行する複製スケジュールを持つことになります。

サイト･リンクの作成はいつでも可能であり、その追加と削除も容易に行えます。ただし、サイトおよびサイト･リンク再コンフィグレーションと、サイトリンクに関連するスケジューリングが行われるとき、遅延による複製への影響が生じます。

## Task 1: **サイト･リンクのデザインを決定する**

Active Directory は、自動的に default-first-site-link を作成します。ここで説明している デザインにおいて、すべてサイトが接続され、また、相互に接続性と可用性を持つとき、シングル･サイト･リンクを用いて、サイト間の関連を表現することが可能になります。このフル･メッシュ・デザインでは、すべてのサイトが適切に接続され、サイト間で特定リンクを設計する必要がない、という状況が想定されています。このアプローチは、サイト･リンクを設計する必要性を取り除くだけではなく、サイト･リンク構造を 自動的にコンフィグレーションすることで、そのデザインを単純化します。

このリンクの接続性と可用性は同質のものであるため、複製のスケジュールおよび、インターバル、コストも、同じようにコンフィグレーションされるでしょう。すべてのサイトが WAN で接続され、帯域幅と待ち時間を等しく共有するとき、この選択は有用なものになります。

使用コストや、可用性、スピード、帯域幅などが異なる物理ネットワークリンクと、サイトを接続する場合には、別の複製スケジュールが必要になるかもしれません。これらの相違点を緩和するために、新しいサイト･リンクを作成する必要性が生じるでしょう。

サイト･リンクが使用するコスト･アルゴリズムは、サイト間のフローで用いられるパス複製の、トラフィックの選択に影響を与えます。 望ましい接続は、望ましくない接続と比べて、より低いコストでコンフィグレーションされるでしょう。この複製システムは、最も低コストのリンクを使うように設定されます。もし、リンクの使用コストが高くなる場合には、そのような設定が、対象となるリンクに割り当てらている可能性があります。

トラフィックがリンクをまたぐ複製は、利用可能なスケジュールと、リンクに設定される複製の頻度により制御されます。たとえば、月曜日から金曜日までの、午前2時から午前4時の間に、30分ごとに複製を行うような、リンクの設定が可能です。

サイト･スケジューリングは、24時間の範囲の中で、また、週や日の各種組み合わせにおいて、たとえば15分間隔でというような、短いインターバルを指定できます。

複製に対してスケジュールやインターバルを割り当てるとき、組織が必要とする各種の複製の目的を、保証するよう注意すべきです。以下のように設定された時間内に、すべての変更が記録されるように、複製の目的を定義できます：

* **コンフィグレーションとスキーマの収束.** コンフィグレーションとスキーマに対する、いかなる変更であっても、フォレスト内のドメイン・コントローラごとにリプリケートされます。
* **ドメインの収束.** すべてのドメイン変更は、ドメイン内のドメイン・コントローラごとにリプリケートされます。
* **グローバル･カタログの収束.** すべてのグローバル･カタログ変更は、フォレスト内のグローバル･カタログごとにリプリケートされます。
* **アプリケーション･パーティションの収束.** すべてのアプリケーション･パーティション変更は、影響を受けるアプリケーション･パーティションをホストする、すべてのドメイン・コントローラにリプリケートされます。

複製に関するスケジュールとインターバルを定義するとき、すべての複製の目的が、最悪のシナリオにも対応できることを保証します。つまり、1つのサイトから開始された変更が、最大数のサイトを経由して、所定のタイムフレーム内でリプリケートできるでしょうか? この目的を達成できない場合には、インターバルとスケジュールの更新や、目的の再定義が必要になります。

4つのドメインを持つシングル･フォレストで構成され、6つのサイト（A－F）から成り立つ、トポロジーについて検討してみます。複製のスケジュールは24時間にコンフィグレーションされ、インターバルはデフォルトで3時間に設定されています。そして、サイト間は、ダイレクト･サイト･リンクで相互接続されています。この例には、目的として 2つの複製プロセスが含まれます。それらは、スキーマとコンフィグレーションの収束を6時間で完了し、グローバル･カタログの収束を4時間で完了することです。



**図4. コンフィグレーションとスキーマの収束**

連携するホップ数があるため、サイトE／F にで導入された変更を、6時間の内にサイト C に収束することは不可能です。それを実現するためには、最低限で9時間（3つのホップ）を要するでしょう。つまり、プリケーション目的の変更、もしくは、インターバルの再設定が必要になります。



図 5. グローバル･カタログの収束

この、グローバル･カタログ収束の例では、サイト A、B、D、E に、4つのグローバル･カタログ･サーバーがあります。サイト D で変更が生じる場合には、目標である 4時間での複製を、すべてのサイトで達成するでしょう。 ただし、変更がサイトA、B、E で生じた場合、すべてのサイトに到達するのに、最短でも 6時間（2つのホップ）が必要されるでしょう。そのため、4時間という目的を、達成することは不可能になるでしょう。再び、プリケーション目的の変更、もしくは、インターバルの再設定が必要になります。

すべての類似するリンクを持つサイトを、新しいリンクと結び付け、それらのサイトを default-first-site-link から削除します。

それぞれの確認されたサイト･リンクについて、サイト･リンク名、および、リンクと関係づけられるコスト、リンクの複製に関するスケジュールとインターバルを記録します。続いて、それぞれのサイトについて、他サイトとの接続で用いられるリンクを記録します。マルチ･サイト･リンクを持つ、サイトが生じる可能性があります。

## **意思決定の概要**

すべてのサイト間におけるリンクは、1つあるいは複数のサイト･リンクを用いて定義されるべきです。サイト間の接続が切れる場合には、エラー・メッセージである Knowledge Consistency Checker（KCC）が生成されるでしょう。これらのサイト･リンクは、分離されたサイトのドメイン・コントローラ間で、ディレクトリ･データベースの複製を制御します。さらに、マルチ･パスが利用可能な場合には、適切なパスの選択に関する制御を提供します。

サイト･リンクのデザインは、変更が可能です。しかし、サイト･リンクを変更すると、すべての更新が一点に収束されるまでの間に、ディレクトリ変更のパフォーマンスに影響が生じるかもしれません。

## **参考資料**

“Creating a Site Link Bridge Design” ： <http://technet2.microsoft.com/windowsserver/en/library/5d05f4ed-a9ec-4dac-b9a8-8527b6c8e0da1033.mspx?mfr=true>

# Step C3: サイト･リンク･ブリッジをデザインする

サイト･リンク･ブリッジにより、サイト･リンク間の推移性（transitivity）が実現されます。ブリッジされたサイト･リンクは、ブリッジをまたいだ正確な複製のフローを可能にするために、共通のサイトを持つ必要があります。サイト･リンク･ブリッジのデザイン変更は可能ですが、Active Directory の複製に脆弱性や停止が生じないことを保証するために、慎重に行われるべきです。

## Option 1: **デフォルトの振舞い**

ネットワークのルーティングが完全であり、さらに、Active Directory複製フローの制御も不要な場合には、**Bridge All Site Links**オプションを使用可能な状態にして、すべてのサイト･リンクに対して推移性（transitivity）を適用します。 それが、デフォルトのステートとなります。

すべてのサイトにまたがる推移性（transitivity）を許すことで、サイト内の各種ドメイン・コントローラから、多サイト内の別のドメイン・コントローラに対して、ダイレクトな複製パートナーの作成が可能になります。ドメイン・コントローラが複製パートナーを捜すために使う、サイトに対する制限あるいは定義が不要なるという点で、この方式は複製を簡単にします。

それは、ハブ･アンド･スポーク･モデルに基づいた、大規模な実装を伴う論点になるかもしれません。 すべてのサイト･リンクをブリッジすることで、複製が行われるときにハブ･サイトの一部だと考えられる、ドメイン・コントローラを制御する必要がなくなります。

## Option 2: **カスタムなサイト･リンク･ブリッジ**

ネットワークのルーティングが完全ではない場合には、IP 転送のための Bridge All Site Links オプションを OFF にし、サイト･リンク･ブリッジを物理ネットワーク接続にマップするようにコンフィグレーションします。それに加えて、IP ネットワークのルーティングが完全であっても、KCC （Knowledge Consistency Checker）が考慮していないはずの、多すぎるルートが存在する場合があります。そのようなときには、カスタムなサイト･リンク･ブリッジ･トポロジーを作成し、サイト･リンクの自動的な推移性（transitivity） を不能にすることで、混乱は回避されるでしょう。デフォルトの KCC では、すべての可能性のある接続とブリッジが、複製における検討の対象となります。

さらに、Active Directory における複製フローの制御に、サイト･リンク･ブリッジを使用することが可能です。サイト･リンク･ブリッジの作成は、2つの大きな理由により行われます。1つは、ハブ･アンド･スポークをを持つネットワークのフェイル･オーバーのために複製を制御すること、そして、もう1つは、ファイア･ウォールを介して複製を制御することです。 サイト･リンク･ブリッジのデザインを介して、Active Directory の複製フローが制御される場合には、IP 転送に対して **Bridge All Site Links** オプションを OFF にします。

2つのサイト間で Active Directoryの複製を実現するために、2つのサイト･リンク･ブリッジをコンフィグレーションすることが可能です。それにより、たとえ一方のリンクが失敗しても、複製は成功するようになるでしょう。こうした処理を施すことで、 対象となるトポロジーのあらゆる局面の失敗において、サイト･リンクのブリッジによる支援が行われ、**Bridge All Site Links** による KCC と Intersite Topology Generator（ISTG）の拒絶が排除されます。

ファイアウォールのコンフィグレーションにおいて、複製トラフィックの通過と、特定ドメイン・コントローラからの接続を許す場合には、その環境に適合するように、サイト･リンク･ブリッジを設定する必要があります。サイト･リンク･ブリッジは、ファイアウォールの両側で作成されます。そして、それぞれのサイトを接続するサイト･リンクは、ファイアウォールにおけるリンク側のサイト･リンク･ブリッジに関連づけられます。 ファイアウォールを介して2つのサイトを接続するサイト･リンクは、ブリッジ上には配置されません。ファイアウォールを介した通信が許可されているはずの、ドメイン・コントローラが失敗する場合もあります。そのときの複製パートナーは、対象となるブリッジの一部であるサイト内のドメイン・コントローラだけと、新しい複製パートナーを設定しようと試みるでしょう。

どのような選択をするかにより、Active Directoryにおける複製の堅牢性が、低減する可能性があることに注意すべきです。たとえば、ハブ･アンド･スポーク･ デザインの中枢において、すべてのドメイン・コントローラが失敗する場合には、すべての接続しているパートナーがネットワークから切断されるため、サテライト･サイトも複製トポロジーから切断されてしまうでしょう。

同様に、ファイアウォールをまたいで通信する、ドメイン・コントローラの機能が失敗する場合には、ファイアウォールの両側における変更だけが、複製により更新されるでしょう。このような状況は、たとえばファイアウォールの通過が、何らかの理由により遮断されたときなどに起こり得ます。その場合には、問題が解決した後に、ドメイン・コントローラによる修正が、ファイアウォールを通過していくことになります。

## **特性に関する評価**

|  |  |  |
| --- | --- | --- |
| 複雑さ | | |
| デフォルトのサイト･リンク･ブリッジ | 実装の複雑さが低減されます。 | Low |
| カスタムなサイト･リンク･ブリッジ | 実装の複雑さが増大します。 | High |

## **意思決定の概要**

サイト･リンク･ブリッジはコンフィグレーションされるべきであり、また、ネットワークがな修正を必要とするときにだけ、デフォルトのコンフィグレーションを変更すべきです。すべてのサイトの連結は、ダイレクトに、あるいは、ブリッジを介して、行われるべきです。

サイト･リンク･ブリッジの確立あるいは変更の決定自体を、変更することが可能です。

作成されるサイト･リンク･ブリッジと、そのブリッジに関連づけられるサイト･リンクを記録します。

## **参考資料**

“Creating a Site Link Bridge Design” at <http://technet2.microsoft.com/windowsserver/en/library/5d05f4ed-a9ec-4dac-b9a8-8527b6c8e0da1033.mspx?mfr=true>

# Step D1: **ドメイン・コントローラのコンフィグレーションを決定する**

ドメイン・コントローラの数が確認された後に、最終の Step D1 に取り組みます。 ここでは、それぞれのドメイン・コントローラのための、ディスク･スペースおよび、メモリ、CPU、ネットワークに関する要件を決定していきます。

## Task 1: **ドメイン・コントローラごとの、最小ディスク･スペース要件を確認する**

それぞれのドメイン・コントローラに対して、以下のように、最小限のスペース割当てを計画します：

* 500 MB ： Active Directory のトランザクション･ログ
* 500 MB ： SYSVOL 共有を取り込むドライブ
* 1.5 GB ～ 2GB ： Windows Server 2008 オペレーティング･システムのファイル
* 0.4 GB ： ディレクトリ内の1,000 ユーザーを前提とした、NTDS.dit のためのストレージ

例として、10,000人のユーザーを持つドメインA と、5,000人のユーザーを持つドメインB で構成される、1つのフォレストについて考えます。ドメインAをホストするドメイン・コントローラに、最小限のディスク・スペースとして4GBを割り当て、また、ドメインBをホストするドメイン・コントローラに、最小限のディスク・スペースとして2GBを割り当てます。

グローバル･カタログ･サーバーとして機能するドメイン・コントローラは、フォレストが複数のドメインを含むときに、追加のディスク･スペースを必要とするでしょう。 前提となるグローバル･カタログ･サーバーのための追加要件としては、グローバル･カタロ･グサーバー自身のドメイン部分に対して、その 50% を加えたディスク･スペースが適量となります。前述の例では、ドメインA では 4GBのディスク・スペースを必要とし、また、ドメインB では 2GBのディスク・スペースを必要としています。ドメインA では、グローバル･カタログ･サーバーのために1GB（ドメインBの 2GBの50%）を追加するため、全体で5GBのストレージになります。また、ドメインB では、グローバル･カタログ･サーバーのために2GB（ドメインAの 4GBの50%）を追加するため、全体で4GBのストレージになります。

最終的に、アプリケーション･パーティションにデータをストアするために、対象となるディレクトリが使用される場合には、それらのパーティションのストレージ要件を、ドメイン・コントローラのディスク要件に加える必要性が生じるでしょう。

キャパシティ要件の確認は、ディスク･コンフィグレーション計画における最初の要素です。そして、2番目の要素はパフォーマンスのための計画となります。ビジネス要件を充たすレベルで、ディスク･サブシステムにおけるデータの読み書きを実行するよう、コンフィグレーションをしなければなりません。また、データにフォールト･トレランスを提供するために、 何らかの形式による RAID を使用できます。

小規模なサイトにおいては、シングル･ディスクにより、キャパシティとパフォーマンスの要件が充たされるかもしれません。大規模なサイトにおいては、パフォーマンス要件を充たすために、ログおよび、OS、ータベースのファイルを、別ボリューム上に配置する必要があるかもしれません。予測される負荷に対して、ディスク･サブシステムがボトルネックにならいことを保証するために、コンフィグレーションについてテストを実施すべきです。 オリジナルの容量に基づくディスク･コンフィグレーションでは、パフォーマンスが不足するという場合には、追加のディスク･ドライブが必要になるかもしれません。

それぞれのサーバーについて、そのコンフィグレーション情報を記録します。

## Task 2: **ドメイン・コントローラごとの、メモリ要件を確認する**

ドメイン・コントローラのために必要とされる、最小限のメモリ割り当てについて、控えめな見積もりを以下のテーブルに提供します。このデータの前提となるのは、ドメイン・コントローラが Active Directory と DNS だけをホストするという状況です。

Table 4.必要とされる最小のメモリ割り当て

|  |  |
| --- | --- |
| サイトにおけるドメインごとのユーザー数 | ドメイン・コントローラごとの最小メモリ |
| 1–499 | 512 MB |
| 500–999 | 1 GB |
| > 1,000 | 2 GB |

上記のテーブルには、最小値をリストアップしていますが、メモリを追加することで、ディレクトリのパフォーマンスが改善される可能性があります。充分なメモリが提供されると、Active Directory はデータベースをメモリ上にキャッシュしようと試み、それによりディスク･アクセスが低減し、パフォーマンスが改善されます。サーバーにおける仮想アドレス空間と、物理的な RAM の量により、このキャッシュは制約を受けます。

既存のインフラストラクチャを利用する場合には、ドメイン・コントローラのパフォーマンスを測定することで、そのメモリ量と環境のバランスを判断していきます。また、新たな展開を実施する場合には 2GBの RAM から開始し、予想される負荷でコンフィグレーションをテストした後に、必要とされるメモリを加えていきます。

サーバーに RAM を追加する必然性を判断するために、Reliability と Performance のモニターを用いて、Active Directory 運用におけるキャッシュのパーセンテージを監視します。Active Directory Domain Services に関しては、lsass.exe インスタンスを調べます。また、Active Directory Lightweight Directory Services に関しては、Database\Database Cache % Hit パフォーマンス･カウンターの Directory インスタンスを調べます。操作と実行の結果が、あまりキャッシュされていない状況では、低い値が示されます。そのような場合には、RAM を追加することで、Active Directory のキャッシュ･ヒットレートと パフォーマンスが改善するかもしれません。なお、しばらくの間、Active Directory を実行して、標準的な負荷をかけた後に、カウンターを調べるべきです。 Active Directory サービスが再開されたとき、あるいは、マシンがリブートされたときには、キャッシュはエンプティで開始するため、最初のヒットレートは低くなりますので、注意が必要です。

サーバーが必要とする RAM の総量を算定するための望ましい方式として、Database Cache % Hit カウンターの使用を推奨します。なお、代替のガイドラインとして、データベース全体をメモリにキャッシュする充分な余地を確保するために、ディスク上の Active Directory データベースの物理サイズに対して、サーバー上のRAM を 2倍にするという方式もあります。しかし、最も頻繁に使われるデータベースのパートが、データベース全体の一部に過ぎないため、多くのシナリオにおいて、この代替案は過大な見積もりとなります。

## Task 3: CPU **要件を決定する**

Windows Server 2008 の Standard Edition を実行する32 bit サーバーの場合、そのアドレス空間は 4GB RAM に過ぎません。4GB 以上の RAM を持つサーバーが必要な場合には、64 bit アーキテクチャに移行してください。Windows Server 2008 の 64bit バージョンに移行することで、将来のシステムにおける拡張性が保持されるだけではなく、今後のマーケットが証明するハードウェアの将来性も手にすることができます。

500ユーザー以下のサイトであればシングルCPUでスタートし、また、10,000ユーザー以下のサイトであればデュアルCPUでスタートし、そこからスケールアップしていくことが、一般的な推奨モデルとなります。ただし、このモデルは、ディレクトリの主要な目的が、ユーザー認証だと想定した場合のものです。

たとえば、Exchange Server のようなサーバーが、付加的なリクエストを処理する場合には、システム･パフォーマンスをモニターし、CPU数を調整する必要性が生じます。 対象となる環境内に、既存のドメイン・コントローラが存在する場合には、パフォーマンス･モニターを用いて、要求されるハードウェアのベースラインを得るという方式が有益になります。

それぞれのドメイン・コントローラに対する、CPU数と、選択されたアーキテクチャを記録します。

## Task 4: **ドメイン・コントローラごとに、ネットワーク要件を確認する**

多くの社内ネットワークでは、100 Mbps もしくは 1G bps で、サーバーとの接続が構成されています。Active Directory のサーバーにおいても、一般的にはシングル･ネットワーク･アダプターで、すべてのネットワーク･トラフィックを処理することが可能です。

ドメイン・コントローラに、マルチ･ネットワーク･アダプターを配置すると、複製や認証の失敗といった問題を引き起こす可能性が生じます。そのため、一般には推奨されません。

## Task **と検討項目**

Active Directory は読込みの負荷が大きなシナリオに、つまり、データのアップデートよりも、クエリー操作が多くなるシナリオに最適化されています。パフォーマンスの調整において最も重要なことは、データベース内の最も頻繁に使用される部分をメモリにキャッシュするための、充分な RAM 領域をサーバーが持つことの保証です。パフォーマンス･モニターにより、サーバーの Database Cache % Hit を確認することで、メモリの追加に関する必然性が判断できます。ただし、ディレクトリ･サービスを開始したばかりの状態では、キャッシュ･ヒットのパーセンテージは低くなりますので、注意してください。

対象となるディレクトリに対して、書き込みの負荷が大きくなるシナリオでは、ディスク･サブシステムを最適化することでパフォーマンスを向上させます。ハードウェア RAID コントローラーおよび、高回転型のディスク、コントローラー上のバッテリー･バックアップ付き書き込みキャッシュなどを用いることで、パフォーマンスの改善を促進できます。負荷の大半が書き込みで構成されるため、読み込みで負荷が生じるシナリオほど、キャッシュがメリットを提供することはありません。

## **意思決定の概要**

Active Directory の適切な運用には、ドメイン・コントローラの正確な物理コンフィグレーションが欠かせません。 クリティカルな要素として、ディスク･サブシステムおよび、メモリ、CPU、ネットワーク･アダプターなどが、そこには含まれます。必要に応じて、ハードウェアの再コンフィグレーションが可能ですが、システムの運用停止がもたらされるでしょう。

## **参考資料**

“Performance Tuning Guidelines for Windows Server 2008” ：<http://www.microsoft.com/whdc/system/sysperf/Perf_tun_srv.mspx>

“Active Directory Performance for 64-bit Versions of Windows Server 2003” ： <http://www.microsoft.com/downloads/details.aspx?FamilyID=52e7c3bd-570a-475c-96e0-316dc821e3e7>

# **まとめ**

このガイドは、Windows Server 2008 Active Directory のデザインを実現するために必要な、

クリティカルなデザイン上の決定および、アクティビティ、タスクを要約することにフォーカスしています。 そして、意志決定プロセスの包括的なレビューを完了するために必要な、テクニカルな視点、および、サービスの特徴、ビジネス要件に取り組んできました。 このガイドを、プロダクトのドキュメントと組み合わせて利用するとき、Active Directory の実装を自信を持って 計画することが可能になるでしょう。

# Appendix: **補足資料**

This job aid summarizes the decision and task results. Additional job aids included with the *Windows Server 2008 Deployment Kit* can be found at <http://www.microsoft.com/downloads/details.aspx?familyid=6cde6ee7-5df1-4394-92ed-2147c3a9ebbe&displaylang=en>.

この補足資料は、決定および判断、そして Task の結果を要約するためのものです。なお、以下のURLの*Windows Server 2008 Deployment Kit* も、その一部として取り込んでいます：

<http://www.microsoft.com/downloads/details.aspx?familyid=6cde6ee7-5df1-4394-92ed-2147c3a9ebbe&displaylang=en>.

1. いくつのフォレストがありますか?

数 \_\_\_\_

名前 \_\_\_\_\_\_\_\_

1. フォレストごとに、いくつのドメインがありますか?

フォレスト 1\_\_\_\_

フォレスト N\_\_\_\_

1. それそれのドメイン名（DNSと NetBIOS）：必要に応じて表を拡張してください。

|  |  |  |
| --- | --- | --- |
| ドメイン | フォレスト1 | フォレスト N |
| 1 |  |  |
| 2 |  |  |
| 3 |  |  |
| N |  |  |

1. フォレストごとの、フォレスト･ルート･ドメイン

フォレスト1\_\_\_\_\_

フォレスト N\_\_\_\_\_\_

1. ドメインごとの OU 構造のデザイン

|  |  |  |  |
| --- | --- | --- | --- |
| OU 名 | ドメイン | 目的 | 制御 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. ドメインごとに配置される、ドメイン・コントローラ

（ドメイン・コントローラの配置に関する概要）

1. ドメインごとに決定された、ドメイン・コントローラの数

|  |  |
| --- | --- |
| ロケーション | ドメイン・コントローラの数 |
|  |  |
|  |  |
|  |  |

1. ドメインごとに配置する、カタログ･サーバーの計画

（カタログ･サーバーの配置に関する概要）

1. ドメインごとに配置する、FSMO ロールの計画

（FSMO ロールの配置に関する概要）

1. サイトのデザイン

（サイト･デザインに関する概要）

1. サイト･リンク･デザインの作成

（サイト･リンク･デザインに関する概要）

1. 設置する物理サーバー

|  |  |  |  |
| --- | --- | --- | --- |
| サーバー名 | CPU | ディスク（ 容量／コンフィグレーション） | メモリ |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Acknowledgments

The Solution Accelerators - Management and Infrastructure（SA-MI）チームは、この*Infrastructure Planning and Design* guide for Active Directory Domain Services 2008を作成したメンバーを承認し、また、感謝を述べます。このガイドの記述および、作成、そしてテストにおいて、彼らは重責を担い、また、多くの貢献をもたらしました。

Contributors:

* Charles Denny – *Microsoft*
* Michael Kaczmarek – *Microsoft*
* Robin Maher – *Microsoft*
* Derek Melber – *Studio B*
* Lee Oommen – *Microsoft*
* Fergus Stewart – *Microsoft*

Reviewers:

* Robert DeLuca – *Microsoft*
* Dave Field – *Studio B*
* Lex Liao – *Microsoft*
* Greg Myers – *Studio B*

Editors:

* Laurie Dunham – *Microsoft*
* Janet Majure – *Studio B*
* Lisa Pere – *Studio B*
* Ruth Preston – *Volt Technical Services*
* Patricia Rytkonen – *Volt Technical Services*