6.2 ブランチオフィス・ソリューションのActive Directory設計

ブランチオフィスといっても，ごく小規模なリモートオフィスからグローバルワイドな大規模展開まで，さまざまなケースが存在します．

前節で述べたBranch Office Infrastructure Solution（BOIS）をふまえた，Active Directory設計の基本的な項目について，記載します．なお，いくつかの項目をピックアップしたにとどめたため，すべての面に触れていない点はご了承ください．

6.2.1　ブランチオフィスでのActive Directoryフォレスト設計

ブランチオフィスでの認証ソリューションとしては，Active Directoryが前提となっています．これは，ドメインコントローラの展開や複製を上手に設計することで，高速から低速までのネットワーク環境にかんたんに対応できるためです．

Active Directoryのフォレスト構成を設計するには，主に組織間の管理要件を中心に確認します．BOISでは，基本的に単一フォレスト構成を推奨しています．

ブランチオフィスの管理組織の構成

一般にはセントラルサイトを管理する組織が，ブランチサイトもいっしょに管理することが望ましいでしょう．これは，セントラルサイトの管理組織が同一のサービスレベルで統一できること，管理が複雑とならず管理工程や経費を節約できる，などのメリットがあるためです．

しかし，会社の組織上，一つの組織による一括管理ではなく，各組織別あるいは特定組織だけ管理を完全に別にしたい，というような場合，管理組織別にフォレストを設定する必要があります．こうした場合，管理が別になることで管理工程が複雑となって，手間や経費がそれだけ増大するデメリットがあります．

上記をふまえ，Microsoft社では単一のフォレストで構成することを推奨しています．どうしても管理を別にしたいブランチサイトがあれば，そのブランチサイトは別フォレストで構成する必要があります．管理を分けたい管理組織の数だけフォレストを構成するので，数が増えると管理コストが高まります．

ブランチオフィス間のネットワーク環境

ブランチオフィス間は一般にWANで接続されていますが，WAN環境に安定した利用可能な帯域が十分にあれば，通常に単一フォレストを構成すれば問題ありません．

しかし，WAN環境が接続しにくい環境では，Active Directory複製が安定して行え

るかどうかを判断して，極力複製を必要としないよう，フォレストを分割することもあります．

なお，Active Directory複製のボリュームは，通常（アカウント情報が含まれる）ドメインパーティションの情報量が問題となります．そのため，これを理由にフォレストレベルで分割することはありません．ただし，きわめて大規模なサイト展開では，（フォレスト情報が含まれる）構成パーティションの情報も増えてしまうので，フォレスト分割を検討することもあります．

6.2.2　ブランチオフィスでのActive Directoryドメイン設計

ドメインの設計では，中間組織での管理要件と，パスワードポリシー要件などが問題になります．また，ドメインパーティションはアカウント情報を含む大量な情報となるため，複製時のトラフィックも考慮するケースがあります．

中間組織の管理構成

基本的に，一つの組織であれば単一ドメインでの運用をMicrosoft社は推奨しています．これは，複数のドメインを構成すると管理が複雑になってしまうためです．単純に管理上の委任を行いたいのであれば，組織単位（OU）を利用することで問題は解決します．

中間組織間で独立した形（ドメイン管理者を分けたい）で管理を行わせるなら，組織にひもづかせない形でフォレストルートドメインをトップに置き，各組織を子ドメインとしてフラットに配置することで，組織間の独立性とフォレスト管理の一貫性を両立できます．

ドメインパーティションとグローバルカタログの複製

同じドメインのドメインコントローラ間では，スキーマ/構成/ドメインと，（DNSサーバーがあれば）アプリケーションの四つのディレクトリパーティションがネットワーク間でActive Directory複製されます．

このうち，ドメインアカウント情報が含まれるドメインパーティションは，多数のアカウント情報を含むためサイズが大きくなります．アカウント情報が常に更新され，常時同期が必要な環境の場合，ドメインを分割することでドメインパーティションの複製はなくなるので，複製トラフィックを減らすことができます．

また，グローバルカタログサーバーの配置について，ドメインを分割した場合には，考慮が必要です．グローバルカタログは，フォレスト内すべてのアカウント情報の一部を複製したもののため，グローバルカタログサーバーと子ドメインコントローラとは，そのための追加複製が発生します．

単一ドメインであれば，こういった問題を単純化できるため，対応コストは下がります．

パスワードポリシーとドメイン

Windows Server 2003までは，同一ドメイン内でドメインアカウントのパスワードポリシーを使い分けることはできず，パスワードポリシーを別にする場合，ドメインを分割していました．

Windows Server 2008では，一つのドメイン内で，セキュリティグループ単位でドメインパスワードポリシーとは別のパスワードポリシーを割り当てる機能（細かい設定が可能なパスワードおよびアカウントロックアウトのポリシー）があります．Windows Server 2008の環境であれば，パスワードポリシーを別にするためにドメインを分割する必要はありません．

6.2.3　ブランチオフィスでのドメインコントローラの配置

ブランチオフィス環境では，一般にブランチオフィス側にドメインコントローラを配置するかどうか，という形で検討されるでしょう．

ブランチオフィスにドメインコントローラを配置しない

これは，基本的に，サテライトブランチオフィスのモデルを想定していると考えられ，次のメリットとデメリットがあります．

メリットとしては，管理コストが下がる，サービスの品質が均一化，ドメインコントローラへのセキュリティ保護が高まる，といったものになります．

一方デメリットとしては，ログオンがWANの接続性に依存する，ピーク時のWAN間トラフィックやパフォーマンスの劣化，ログオンやグループポリシー適用に時間がかかる，などがあります．

ブランチオフィスにドメインコントローラを配置する

これは，基本的に，高速ブランチオフィスや独立ブランチオフィスのモデルを想定していると考えられ，次のメリットとデメリットがあります．

メリットとしては，WAN接続が切断しても確実にログオンを行えること，ログオントラフィックについてWANの影響を受けない，といったものになります．

デメリットとしては，管理コストが上がること，ドメインコントローラ間のWAN通信の影響や，設置の際のソリューションを考慮する場合がある，となります．

設置の際のソリューションとは，通常単体の専用サーバーを利用するところ，ハードウェアの有効利用のため，別の方法を検討するケースがある，ということです．例えば，仮想サーバーとしてドメインコントローラを展開したり，物理的なドメインコントローラ上にほかのサービス（あるいは仮想マシン）を利用したい場合，リスクの算出が必要になります．

また，大きな問題点として，ドメインコントローラの物理的な配置を含むセキュリ

ティを確保できない，という点があります．ドメインコントローラに侵入されたり，ハードディスクが盗難された場合，情報を解析されて悪用されることが考えられます．

この問題に対応したのが，Windows Server 2008のRODC（Read Only Domain Controller；読み取り専用ドメインコントローラ）になります．

Active Directoryサイトとサブネットの構成を検討する

ブランチオフィスはWAN接続でネットワークが構成されているため，クライアントがログオン時に適切なドメインコントローラを選択できるよう，適切な範囲でサイト構成を設計することが，強く推奨されます．

まず，ブランチオフィスごとにサイトを構成し，必要なサブネットを登録します．その上で，サイトリンクやコスト値，Active Directory複製トポロジーについて，物理的なIPレベルのネットワーク構成やリンクスピードを十分考慮の上，設計します．複雑になりすぎると，管理コストが高くなることに注意します．

なお，ドメインコントローラを配置しないブランチオフィスに対しても，サイトを設定することが推奨されています．これは，ドメインコントローラが配置されないサイトに対して，最もコストが少ない（ネットワーク的に近い）他サイトのドメインコントローラが認証を肩代わりする，自動サイトカバレージ機能が利用できるためです．

6.2.4　ブランチオフィスでのサーバーサービスの展開

ブランチオフィスで展開するサーバーサービスには，インフラまわりで必要となるものから業務に利用するサービスまでさまざまなものがあります．サービスの展開にあたっては，管理性，パフォーマンス，可用性を考えながら，展開を考えます．

DNSサーバーの展開

ドメインコントローラや各種サーバーへの名前解決のため，Active Directoryで必須のサーバーサービスです．

DNSサーバーは，ドメインコントローラ上で「Active Directory統合モード 」ゾーンを利用することで，セキュアなDNSサーバーとして構成されることと，Active Directory複製によりDNSゾーンの複製を制御することができます．

またドメインコントローラと同様に，DNSサーバーがダウンした場合ドメイン認証ができなくなるため，DNSサーバーの可用性は重要です．

これをふまえて，通常は複数のドメインコントローラ上にActive Directory統合モードでDNSゾーンを展開することが推奨されています．

Active Directory複製を少しでも少なくしたい，あるいはDNSゾーンの管理をドメインコントローラでないサーバーで行いたい，といった場合，標準的なプライマリ＝セカンダリ形式のDNSサーバーを配置することができます．