Windows DNS と Active Directory

マイクロソフト株式会社
システムテクノロジー本部
山本 明広

目次

- Windows DNS と Active Directory の関連性
- Windows DNS のセキュリティ
- UNIX 環境における Windows DNS の相互運用性

Windows DNS と Active Directory の関連性

DNSの役割

- Windows 環境におけるDNSの役割
  - ネットワークログオンのためのDNS
  - Windows クライアントはまずDNSを利用してActive Directory（ドメインコントローラ）を探しだし自身のドメインにログオンを行う
  - DNS サーバー上のレコード（SRV）としてドメインコントローラが登録されてなければならない

Windows DNS が必要な条件

- 必要用件を満たしていればWindows DNSである必要はない
- ただし、Active Directory を導入する場合は必ず必要

プライマリとして必要か？

- 必ずしもプライマリDNSとしてWindows DNSが必要なわけではない
- プライマリDNSに対する必要要件
  - ドメインコントローラの情報の登録が可能なこと
    - SRV リソースレコードが登録可能であること
  - プライマリ DNSサーバーにドメインコントローラ情報が存在すること
    - 権限のあるプライマリ DNSサーバーが、動的更新プロトコル (RFC 2136) で規定されているように動的更新をサポートしていること

実装可能な DNS サーバー

- Windows Server 2003 DNS Server
- Windows 2000 DNS server
- SRV レコード (RFC 2782) および動的更新プロトコル (RFC 2136) は、BIND version 8.2.2 patch 7 以降で完全にサポートされている

- 社内での利用であれば Windows DNS サーバーでの運用をお薦めします

DC（ドメインコントローラ）ロケータとしての DNS

- ドメインコントローラ上のNETLOGONサービスがSRV レコードの登録を行う
  - SRV レコード: RFC 2782
  - Locating LDAP servers using SRV: draft-ietf-ldapext-locate-*.txt
- SRV レコードフォーマット
  - <service>.<protocol>.<domain> IN SRV <priority> <weight> <port> <host>

（例）

```
_ldap._tcp.dc._msdcs.corp.example.com.
IN SRV  10 100 389 dc-01.corp.example.com.
```

DC ロケータとしての DNS

DNS Server

dns.corp.example.com

corp.example.com

追加登録

_ldap._tcp.dc._msdcs.corp.example.com. IN SRV 10 100 389 dc-01.corp.example.com.

dc-01.corp.example.com. IN A <IP address>

DC

dc-01.corp.example.com

DC ロケータとしての DNS

- Windows クライアントはドメインにログオンするためにSRVリソースレコードを要求するクエリを発行する

DC ロケータとしての DNS

DNS Server

dns.corp.example.com

corp.example.com

_ldap._tcp.dc._msdcs.corp.example.com. IN SRV 10 100 389 dc01.corp.example.com.

dc-01.corp.example.com. IN A <IP address>

クライアント

DC

dc-01.corp.example.com

DC ロケータとしての DNS

DNS Server

dns.corp.example.com

corp.example.com

_ldap._tcp.dc._msdcs.corp.example.com. IN SRV 10 100 389 dc-01.corp.example.com.

dc-01.corp.example.com. IN A <IP address>

クエリ:

_ldap._tcp.dc._msdcs.corp.example.com. IN SRV

クライアント

DC

dc-01.corp.example.com

DC ロケータとしての DNS

DNS Server

dns.corp.example.com

corp.example.com

_ldap._tcp.dc._msdcs.corp.example.com. IN SRV 10 100 389 dc-01.corp.example.com.

dc-01.corp.example.com. IN A <IP address>

レスポンス:

_ldap._tcp.dc._msdcs.corp.example.com. IN SRV 10 100 389 dc-01.corp.example.com.

dc-01.corp.example.com. IN A <IP address>

クライアント

DC

dc-01.corp.example.com

DC ロケータとしての DNS

DNS Server

dns.corp.example.com

corp.example.com

クライアント

ドメインコントローラへのアクセス

DC

dc-01.corp.example.com

DC ロケータとしての DNS

- ドメインログオンを要求するためのクエリの発行
  - 明示的なサイトへのクエリ
    - 例）redmond サイト

_ldap._tcp.*redmond*._sites.dc._msdcs.corp.example.com.
IN SRV 10 100 389 dc-02.corp.example.com.

DC ロケータとしての DNS

DNS Server

dns.corp.example.com

corp.example.com

DC2

dc-02.corp.example.com

Redmond

クライアント

Atlanta

DC

dc-01.corp.example.com

DC ロケータとしての DNS

DNS Server

dns.corp.example.com

corp.example.com

DC2

dc-02.corp.example.com

Redmond

Atlanta

DC

ドメインコントローラへのアクセス

クライアント

dc-01.corp.example.com

DC ロケータとしての DNS

DNS Server

dns.corp.example.com

corp.example.com

DC2

dc-02.corp.example.com

Redmond

クライアントは Redmond ドメイン上に存在
クライアントに近接しているドメインコントローラは
自身のドメインコントローラではない

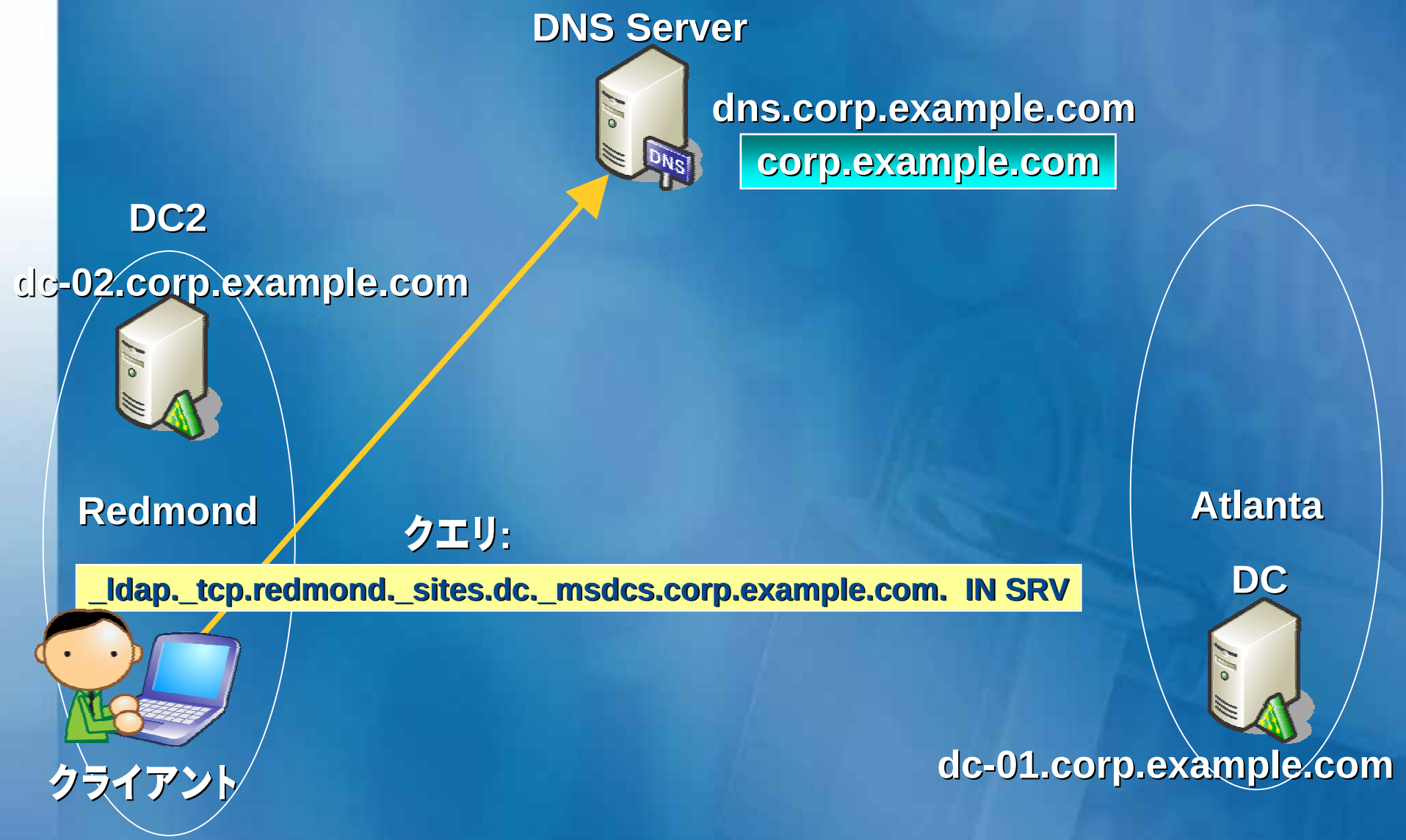
クライアント

Atlanta

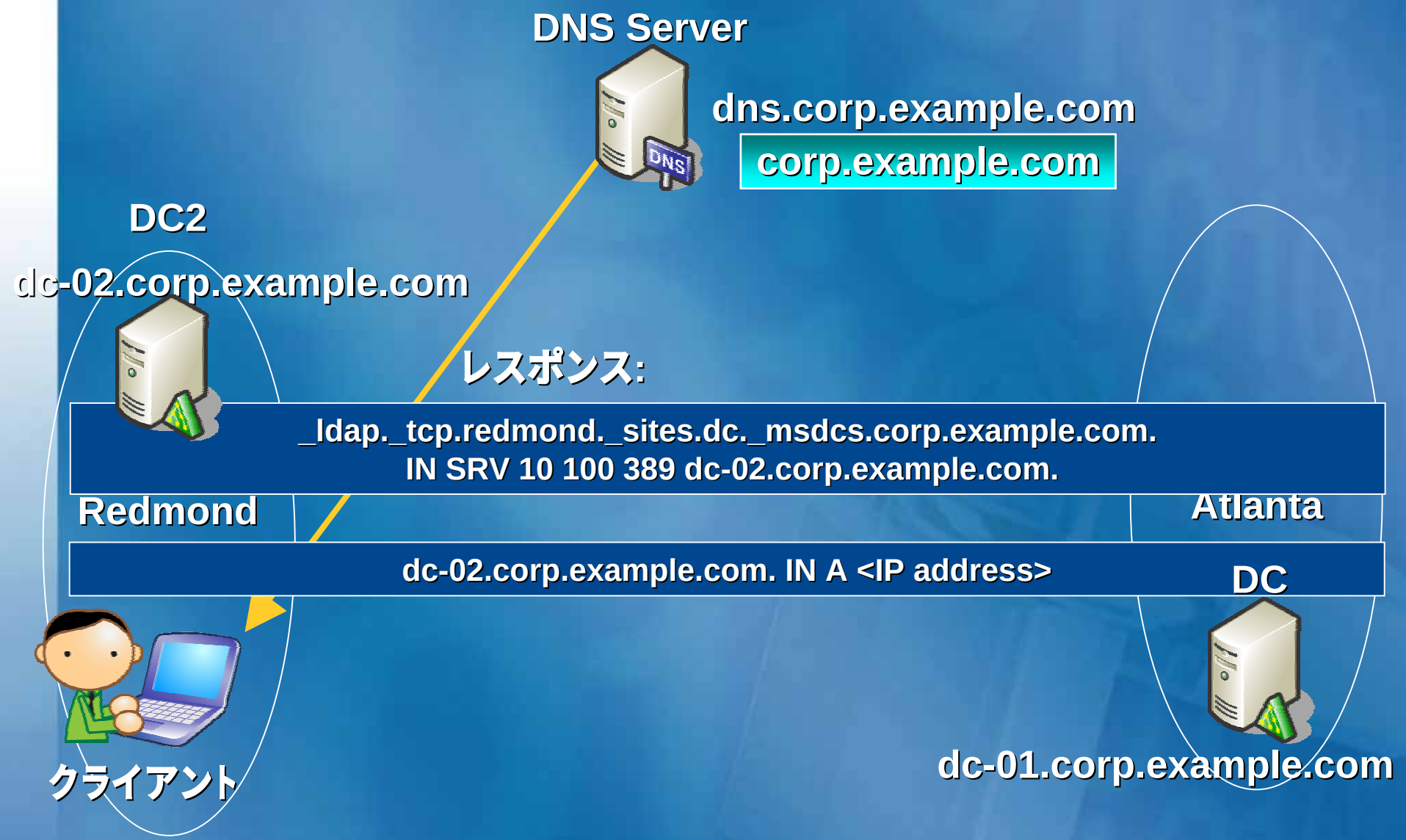
DC

dc-01.corp.example.com

DC ロケータとしての DNS



DC ロケータとしての DNS



DC ロケータとしての DNS

DNS Server

dns.corp.example.com

corp.example.com

DC2

dc-02.corp.example.com

Redmond

ドメインコントローラへのアクセス

クライアント

Atlanta

DC

dc-01.corp.example.com

DC ロケータとしての DNS

- ドメインログオンを要求するためのクエリ
  - 明示的なロールへのクエリ
    - 例）グローバルカタログ

```
_ldap._tcp.gc._msdcs.corp.example.com.
IN SRV  10 100 389 dc01.corp.example.com.
```

Windows DNS サーバーの要点

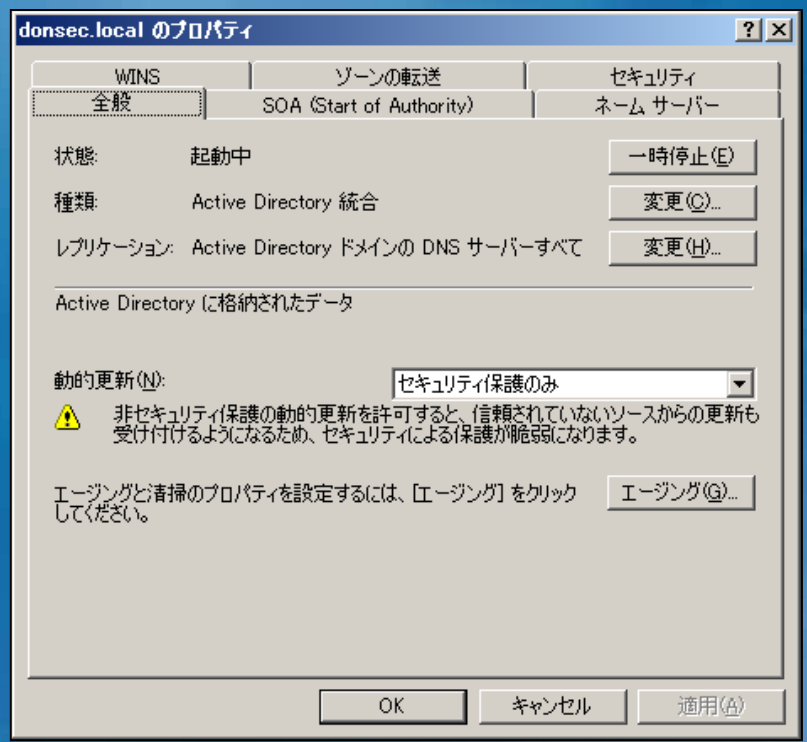
- 動的更新
- Active Directory との統合

動的更新の構成

- なぜ動的更新が必要なのか？
  - IPアドレスの管理負荷
    - 登録
    - 抹消
  - ホスト名でのロギング
  - DHCP環境
- DHCP サーバーとクライアントのどちらが動的更新の登録を実行する必要があるのか?

動的更新の考慮点

- クライアントからの要求によりDNSレコードが自動的に登録されてしまう
- 安全な動的更新のメカニズムが必要
  - “セキュリティで保護された更新”

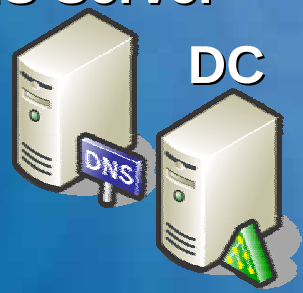


動的更新による登録
セキュリティで保護された更新

DHCP Server

DNS Server

DC



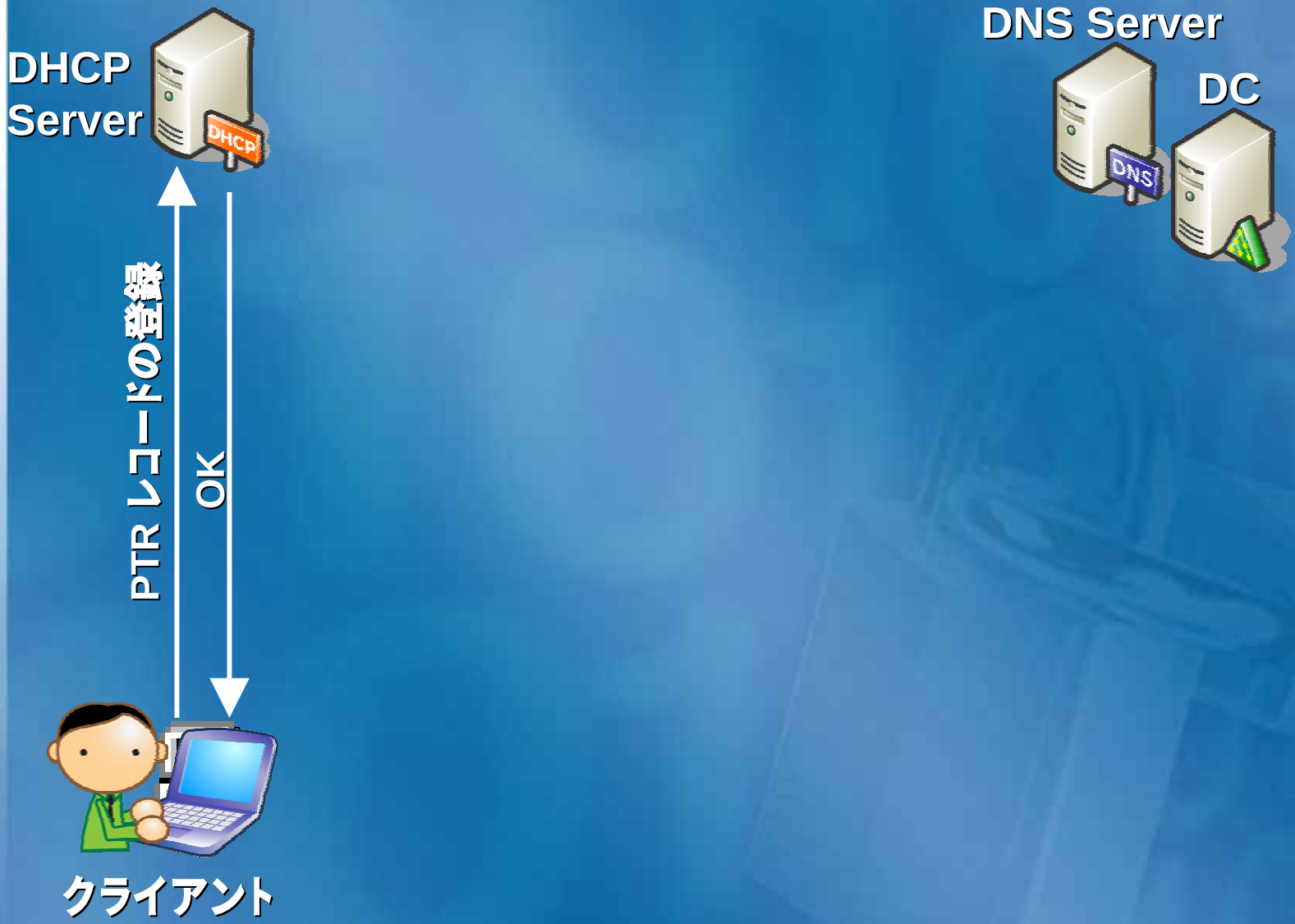
クライアント

動的更新による登録
セキュリティで保護された更新

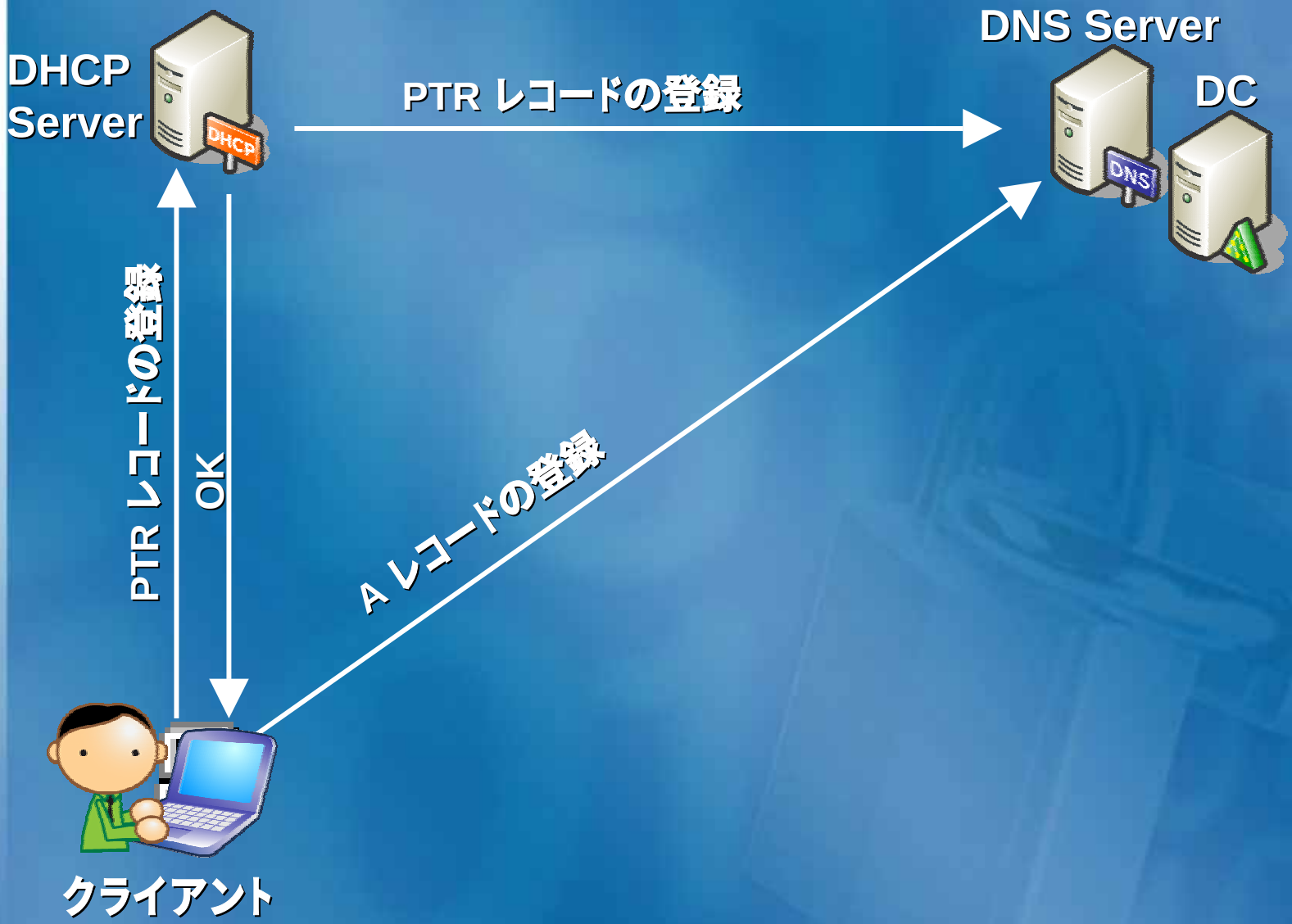
PTR レコードの登録

クライアント

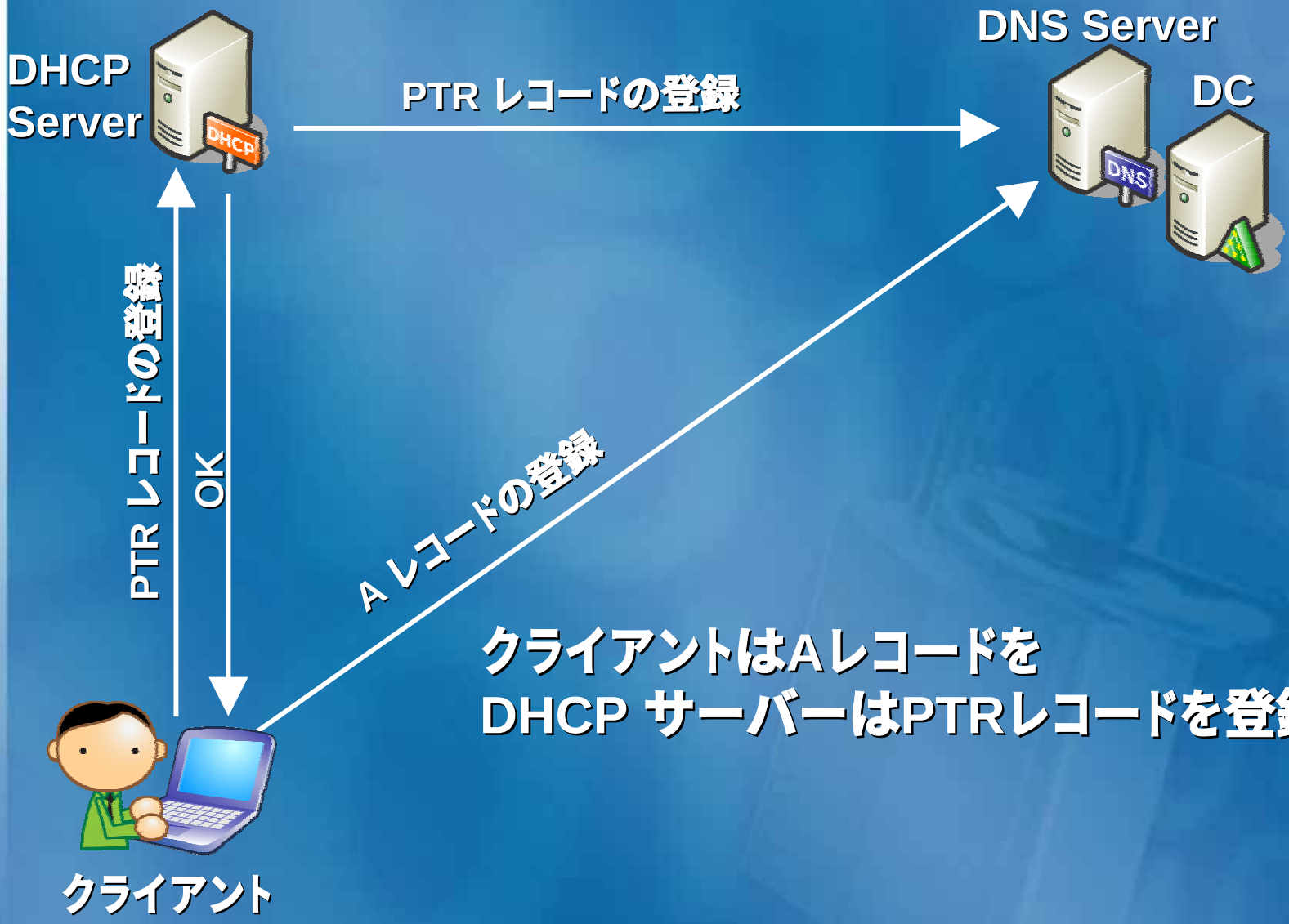
動的更新による登録
セキュリティで保護された更新



動的更新による登録
セキュリティで保護された更新



動的更新による登録
セキュリティで保護された更新



動的更新による登録
セキュリティで保護された更新

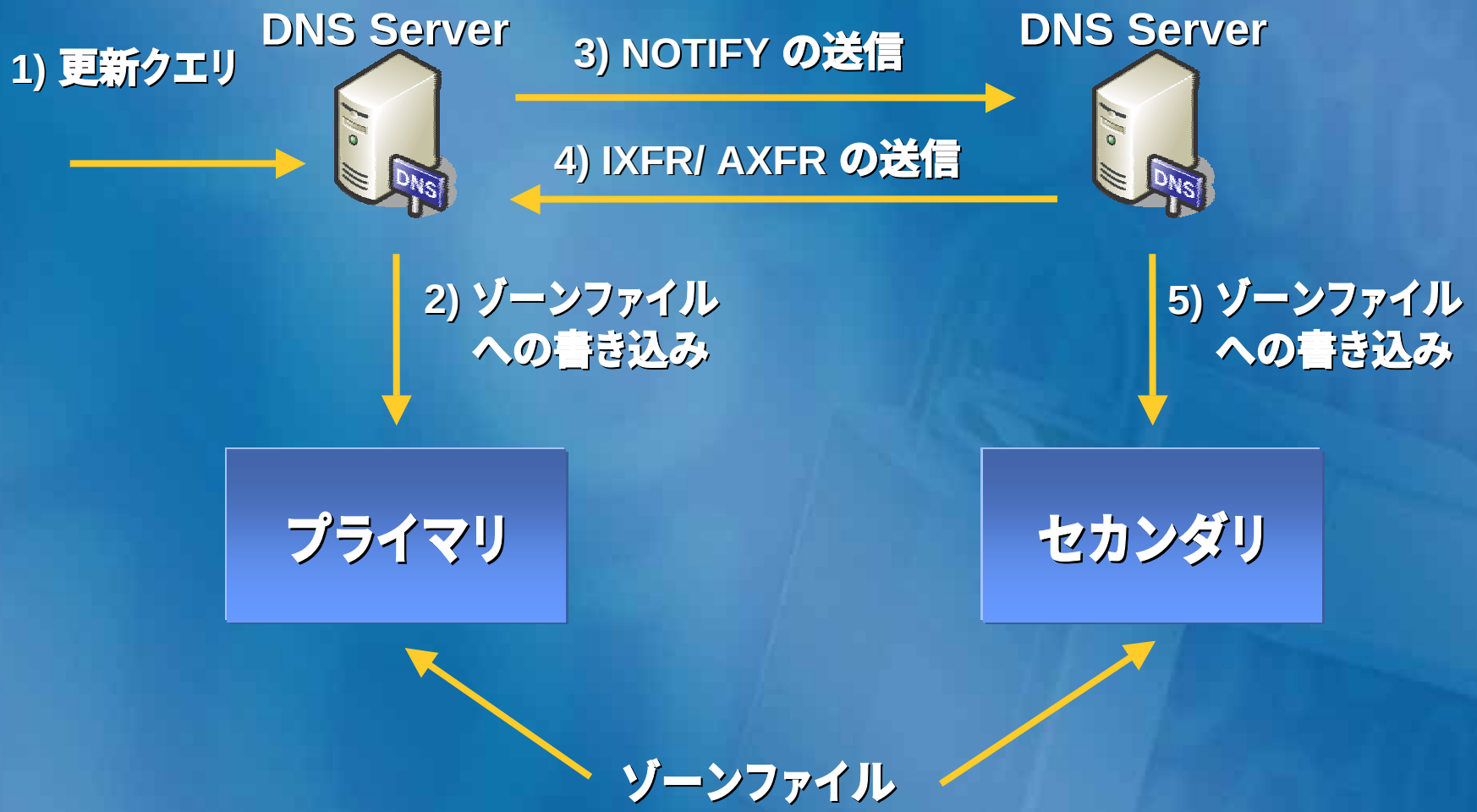
Recommended

クライアントはAレコードを
DHCP サーバーはPTRレコードを登録する

標準的なDNSでの考慮点
Active Directory 非統合

- 標準的な DNS ゾーンはシングルマスタ
  - 更新時の単一障害ポイントになる
    - プライマリDNSサーバーのダウン
    - ネットワークの障害

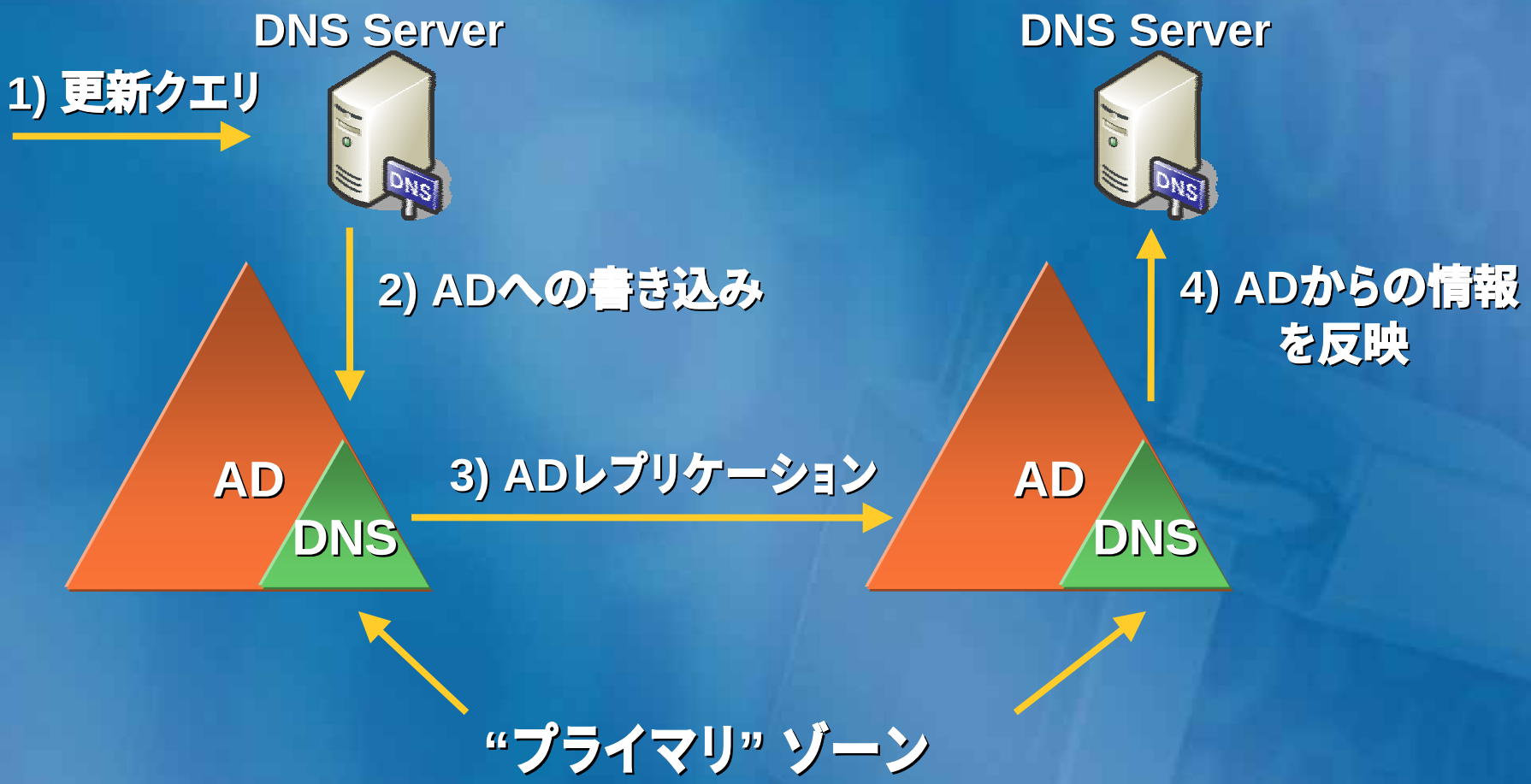
標準的なDNSでの考慮点
Active Directory 非統合



Active Directory との統合

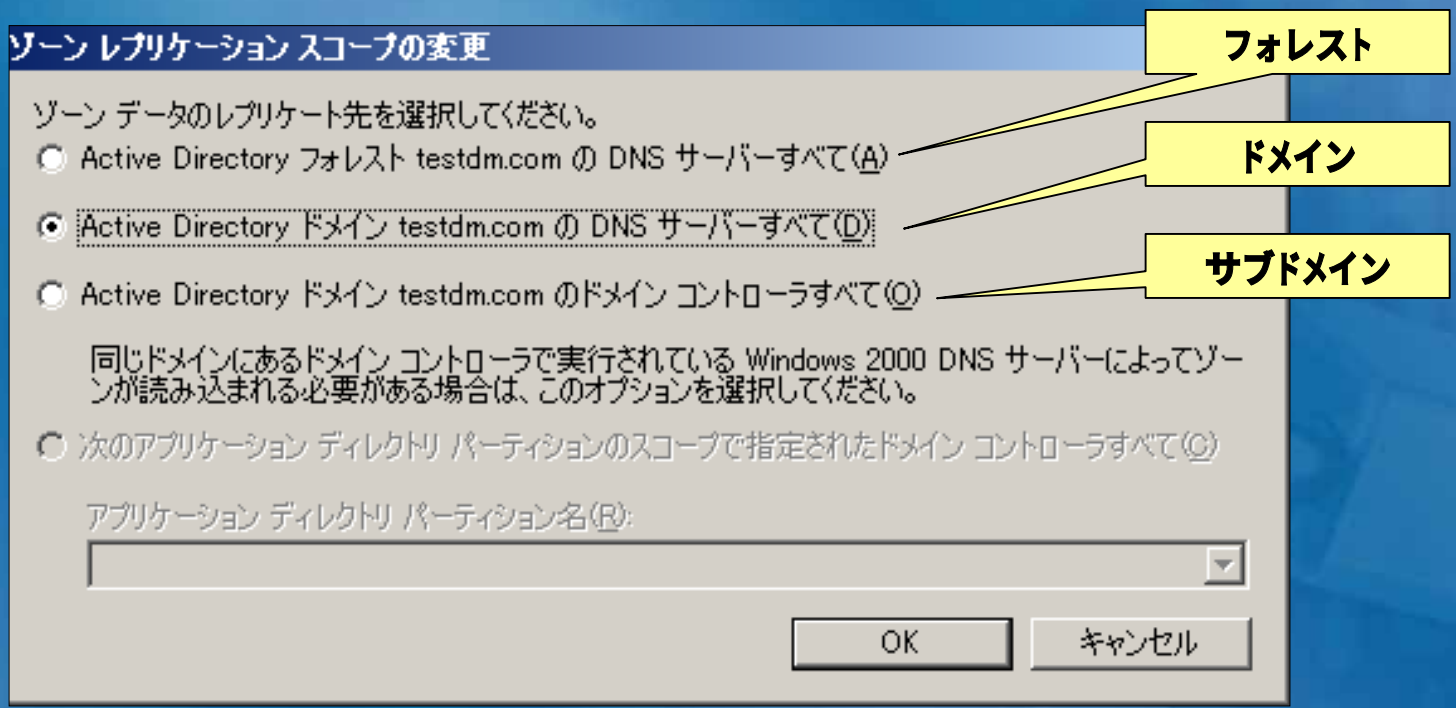
- AD統合されたDNSサーバーはマルチマスタ
  - 読み取りおよび更新における可用性の向上
  - ADレプリケーションと連動したゾーンファイルの同期

Active Directory との統合



Active Directory との統合

- ゾーン レプリケーションスコープの設定
  - DNS アプリケーション ディレクトリパーティションの利用

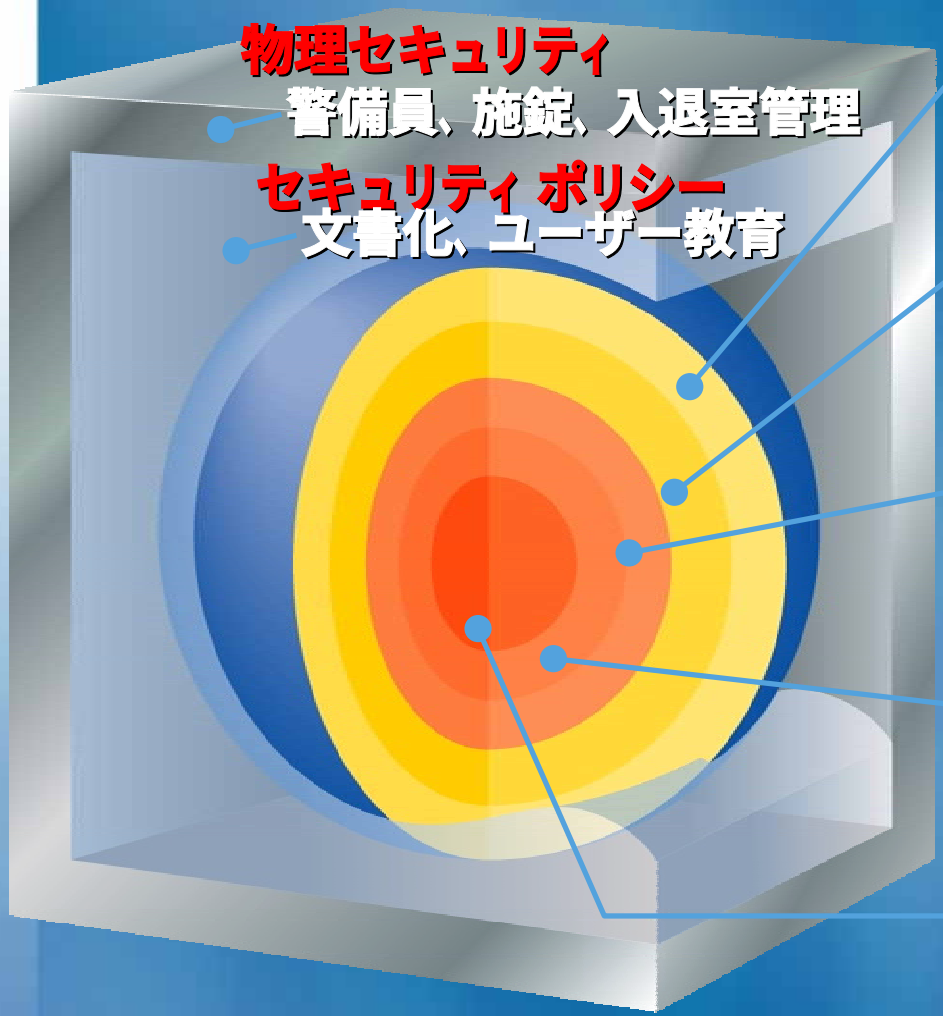


Windows DNS セキュリティ

DNS のセキュリティの考慮点

- 多層防御
  - ネットワークセキュリティの強化
  - インフラストラクチャ サーバーの強化
- DNS サーバーセキュリティ対策
  - 構成
  - サービス
  - リソースレコード
  - ゾーン
  - 監査ログ

多層防御 (Defense-in-depth)



物理セキュリティ
警備員、施錠、入退室管理

セキュリティ ポリシー
文書化、ユーザー教育

ネットワーク境界部
ファイアウォール、VPN、 侵入検知

内部ネットワーク
ネットワーク ポート、IPSec、
無線/有線LANセキュリティ、検疫

ホスト
OS の設定、パッチ管理
ネットワーク認証、侵入検知

アプリケーション
セキュアなコーディング、
ウイルス対策、ユーザー認証

データ
ACL、暗号化

内部ネットワーク

- Network Segmentation
  - セキュリティとネットワークスループットの向上を提供
    - IPサブネットの分離
    - L2スイッチ/ブリッジ
      - VLAN構成
    - L3スイッチ/ルータ
      - ルーティング、パケットフィルタリング
    - 内部ファイアウォールの導入

内部ネットワーク

- IPSec
  - IPレベルのセキュリティを提供
    - パケットフィルタリング
    - ホスト/ネットワーク単位での認証 (IKE)
    - IPパケット単位での暗号化 (ESP)
    - IPパケット単位での整合性確認 (AH)
    - ホスト-ホスト
    - トンネリング (ネットワーク間)
  - 構成ガイド:
    - Windows Server 2003 Deployment Kits 「Deploying Deploying Network Services」
    - Server and Domain Isolation Using IPsec and Group Policy

Host Defenses

- セキュリティと利便性 (使い勝手) とのバランス
- 構成要素
  - OSのハードニング (要塞化)
    - クライアント と サーバー
  - パッチ管理
  - アンチウィルス
  - ホスト型ファイアウォール
  - 効果的な監査

Host Defenses

- クライアント ハードニング
  - グループポリシーによるセキュリティ設定の展開と管理
    - 認証、承認、監査などのOS機能の有効化
    - ソフトウェア制限のポリシー

脅威とその対策ガイド
クライアントも含めたセキュリティ設定ガイド

Windows Server 2003 と
Windows XP を利用し、
高いセキュアなネットワーク
構成を実現するための手引書

- **グループポリシー構成の手引き**
  - セキュリティポリシー、監査ポリシー 、イベントログ、システムサービス 構成
- **その他のセキュリティ構成**
  - アカウント構成、IPSec フィルタリング、NTFS、ネットワーク構成
- **ツールとテンプレート**
  - 「Windows Default Security and Services Configuration.xls」
    デフォルトのポリシー、
    サービス構成を記載

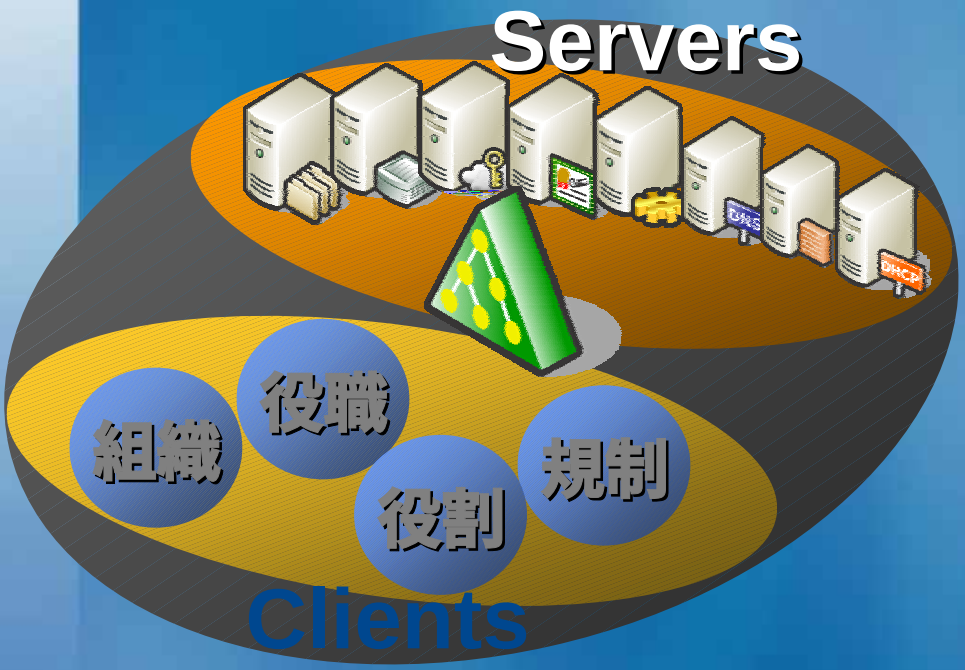
www.microsoft.com/japan/technet/security/prodtech/winclnt/secwinxp/default.asp

Host Defenses

- サーバー ハードニング
  - サーバーの役割別に不要なモジュールや機能を、無効化し、不要な機能を削除、無効化し、脆弱性の発生源を減らし、セキュリティを確保する
  - 既定のインストール状態からのロール別の環境を構築する
  - サーバーの役割別にハードニングを行う

Windows Server 2003 セキュリティガイド
サーバー ハードニングのためのガイド

サーバーの役割に応じて
最適なセキュリティを
設定するための手引書

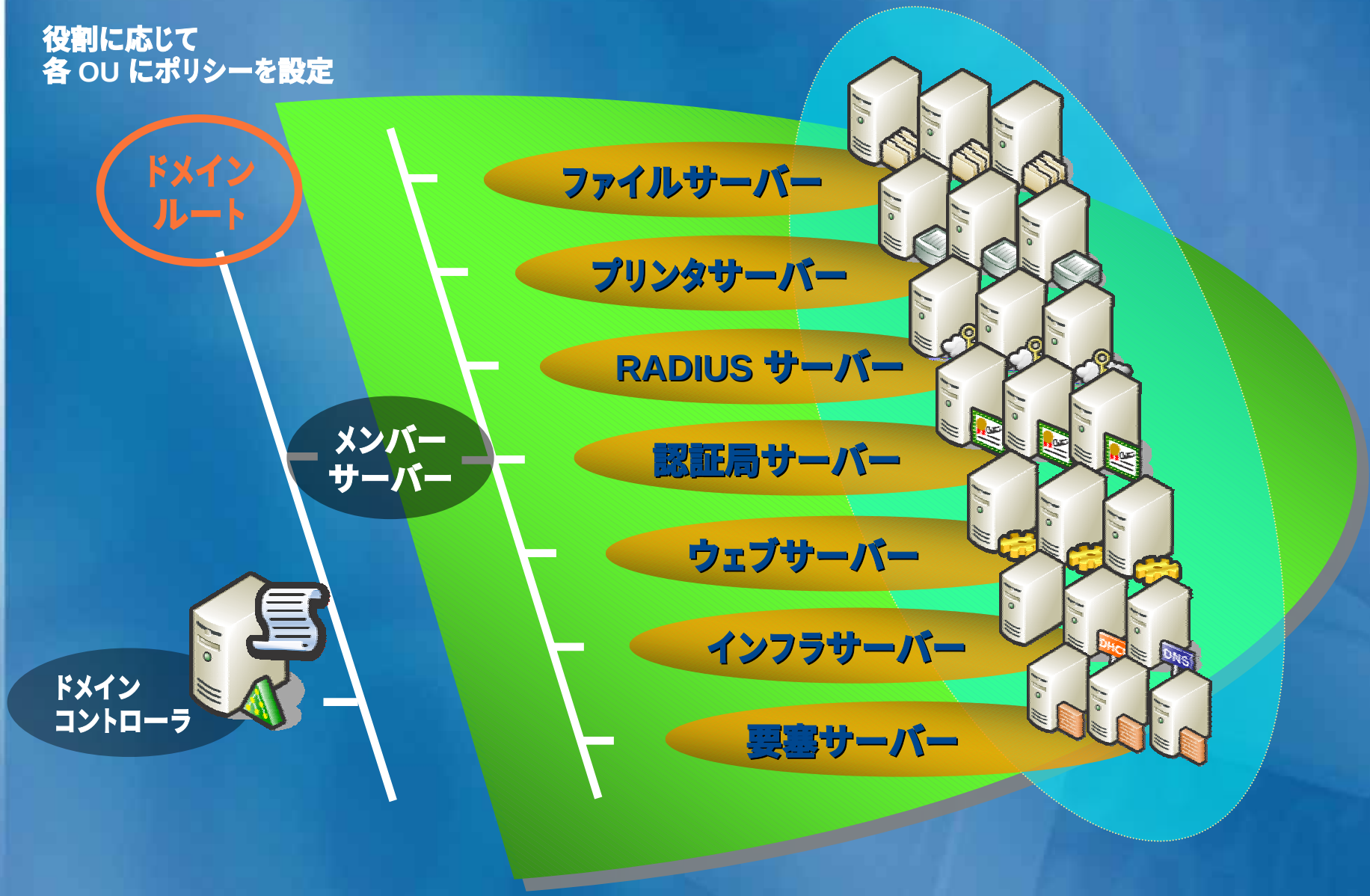


- Active Directory構成の手引き
  - well known アカウントの名前変更手順
  - IPSec Filterによるポートブロッキング手順
- グループポリシー構成の手引き
  - セキュリティポリシー、監査ポリシー、イベントログ、システムサービス構成
- ツールとテンプレート
  - セキュリティテンプレート
  - Netsh コマンドテンプレート

www.microsoft.com/japan/technet/security/prodtech/win2003/w2003hg/sgch00.asp

セキュリティガイド OU＆GPO 構成

役割に応じて
各 OU にポリシーを設定



インフラストラクチャ サーバーの強化

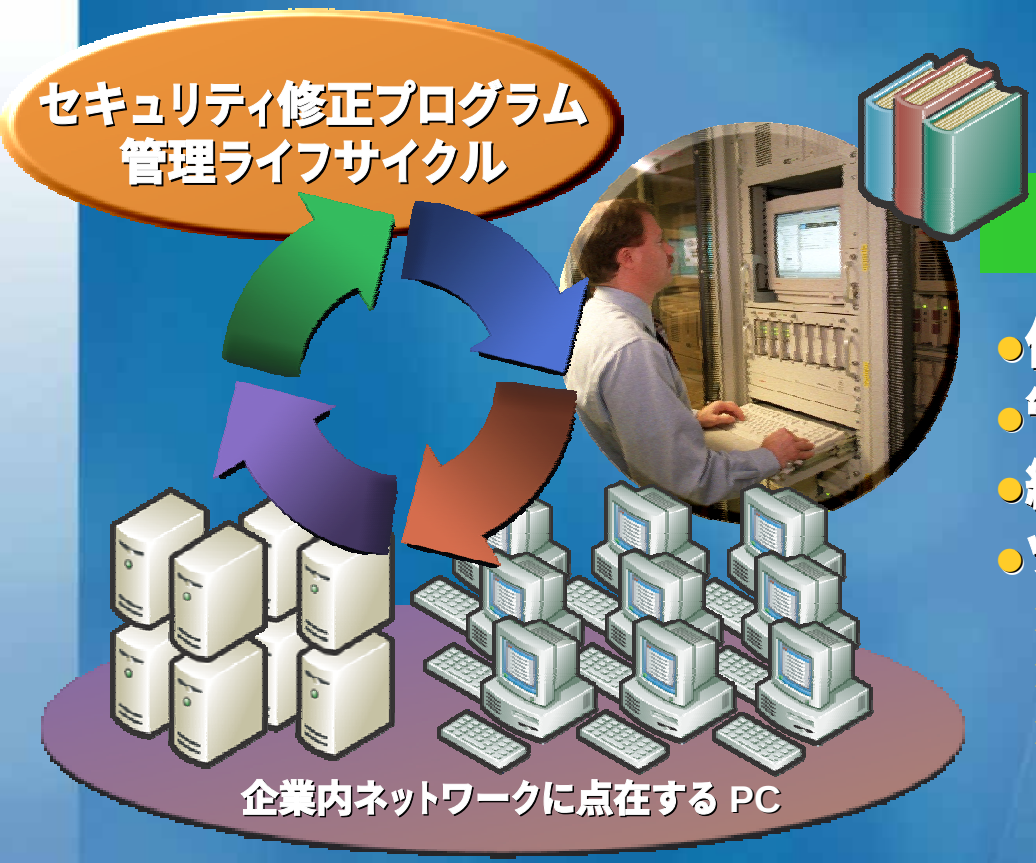
- Infrastructure Server セキュリティ テンプレートのセキュリティ設定を適用する
- 個々のインフラストラクチャ サーバーに対し手動で追加設定を構成する
  - DHCP ログ出力を構成する
  - DHCP サーバーを DoS 攻撃から保護する
  - Active Directory 統合 DNS ゾーンを使用する
  - サービスアカウントを保護する
  - IPSec フィルタを使用し、サーバーアプリケーションに必要なポートだけを許可する

Host Defenses

- Patch Management
  - 脆弱性を修正するための修正モジュールの適用方法と適用のためのポリシーなどを整備をおこなう

セキュリティ修正プログラム管理ガイド

セキュリティ修正プログラム管理に対するアプローチと管理ライフサイクルを解説



セキュリティ修正プログラムガイド

- 修正プログラムの管理の手順と理解
- 管理ライフサイクルの概要と技法
- 継続的な保守・管理技法
- ツールおよびテクノロジの利用方法
  - Systems Management Server
  - Software Update Services
  - Microsoft Baseline Security Analyzer

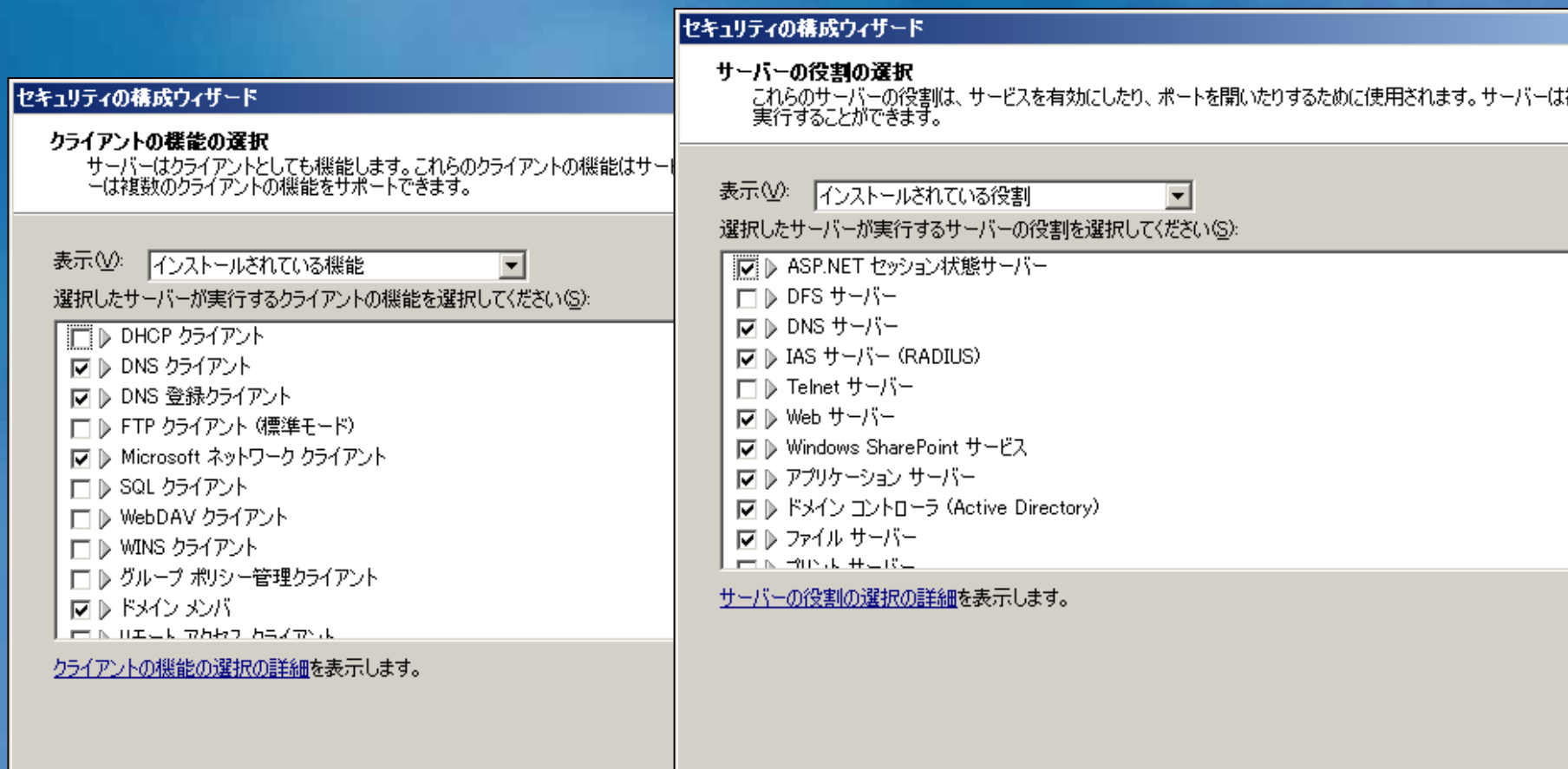
※www.microsoft.com/japan/technet/security/topics/patch/secpatch/default.asp

Host Defenses

- Antivirus
  - アンチウィルス ソフトウェアにより、悪意のあるコード (ワーム、ウィルス、トロイの木馬) から守る
  - パターンファイルの更新とメンテナンスが必要
- Distributed Firewall
  - 各ホストにインストールされるホストベースのソフトウェア ファイアウォール
  - トロイの木馬やスパイウェア、ワーム、ウィルスに対して効果的に攻撃をブロックすることが可能
  - Windows XP/2003のICF (インターネット接続ファイアウォール) /Windows Firewall

Host Defenses
セキュリティ構成ウィザード

- Windows Server 2003 SP1 に付属
  - サーバーのセキュリティ強化用ツール



アプリケーション
Active Directory への統合

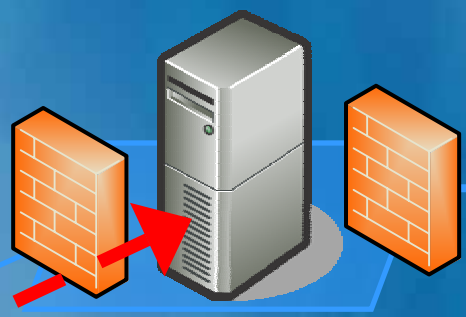
- Active Directoryを使用した統合DNSの使用を強くお勧めします
  - 安全なダイナミックなアップデートを実装
  - Windows セキュリティ保護に統合
    - アクセス権の設定
    - DACLの設定

アプリケーション DNS サーバーの構成

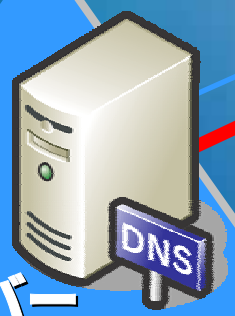
- 別々の内部と外部のDNS名前空間を分離して使用

公開 DNS サーバー

- Active Directory DNS ドメイン名
  - xxx.<*インターネット DNS 名*>
    - または -
  - xxx.local など



インターネット



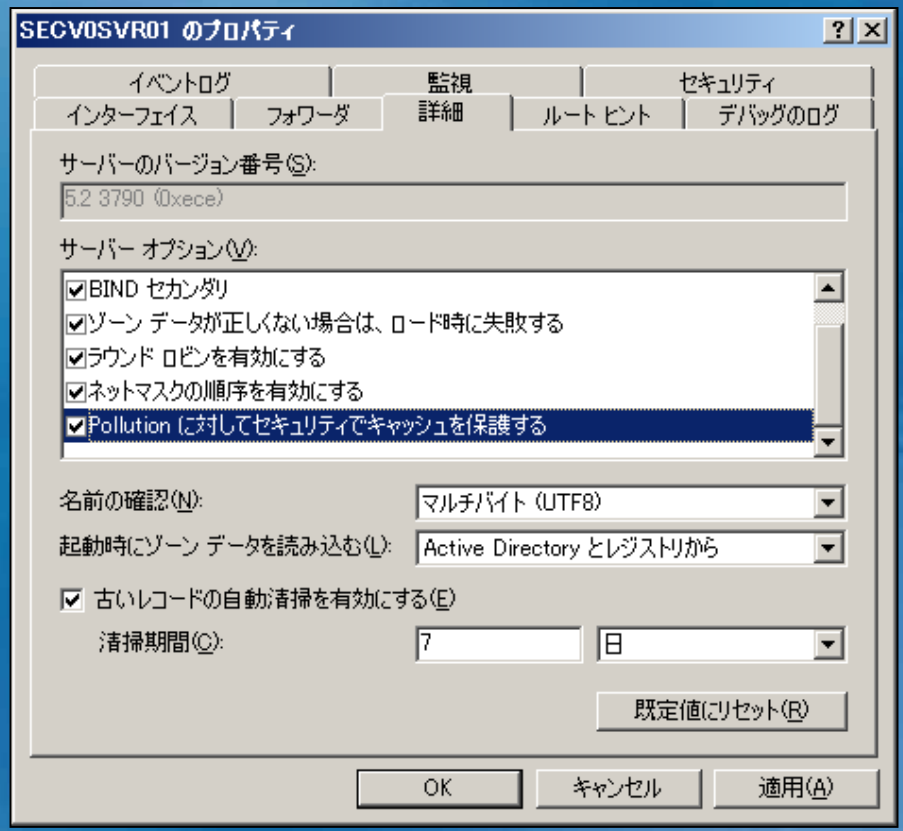
Windows DNS サーバー

- フォワーダ

- Windows Server 2003 ドメイン コントローラ
- 既定の “Active Directory 統合” ゾーン

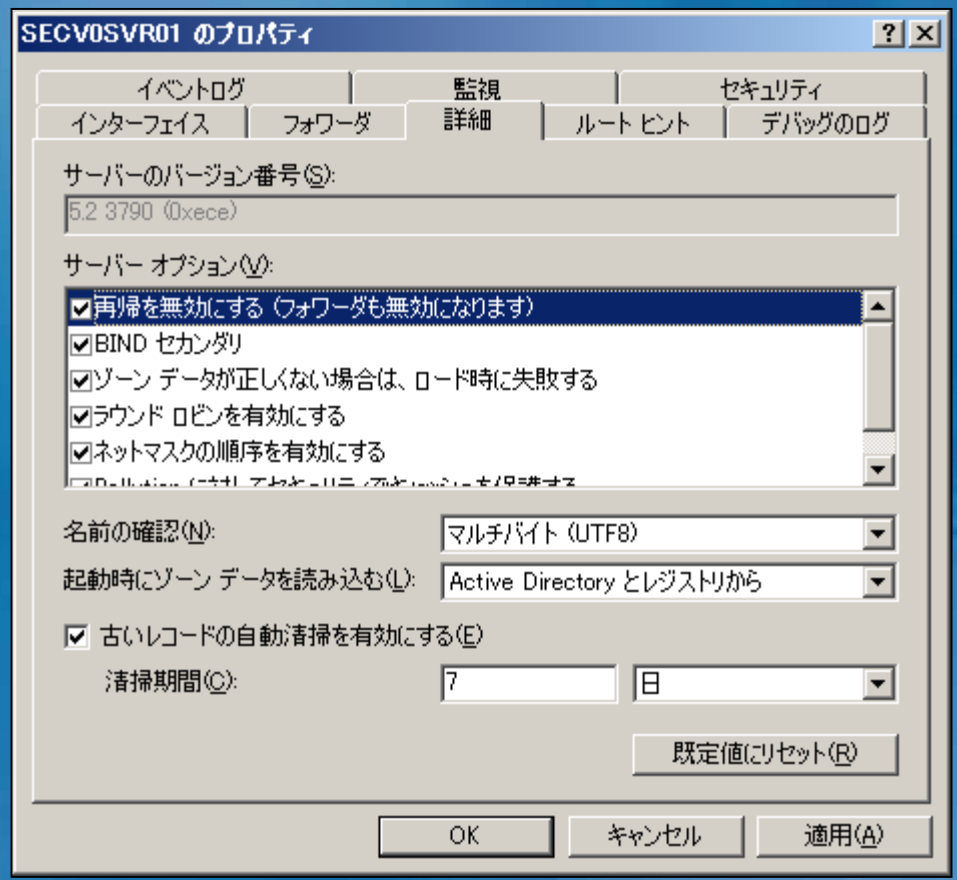
アプリケーション
DNS キャッシュ破壊の防止策

- DNSキャッシュ汚染の保護を有効にす
  - Pollution に対してセキュリティでキャッシュを保護する



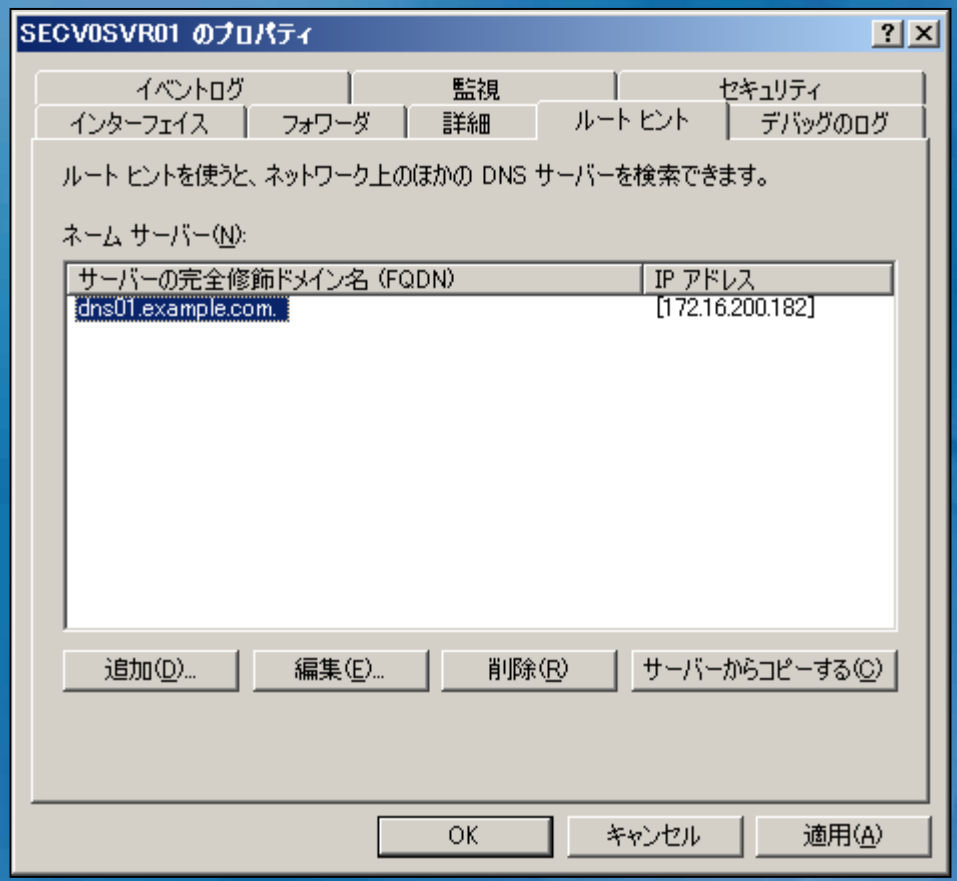
アプリケーション
再帰の無効化

- 必要であれば再帰クエリを受け取らないように設定することも可能



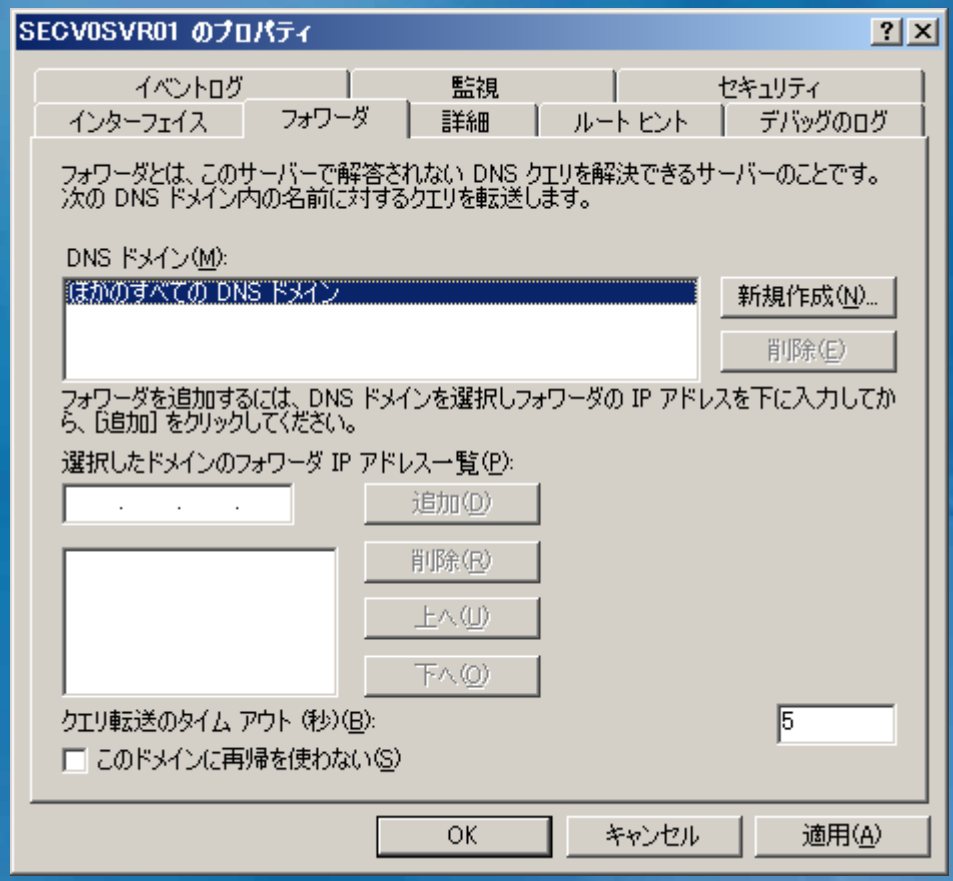
アプリケーション
ルートヒント

- 内部ルートの指定
  - 外部サーバーとの直接の通信を防止



アプリケーション
条件付きフォワーダ

- 内部のフォワーダの指定
  - 特定のドメインに対するフォワーダの指定



アプリケーション ゾーンの保護

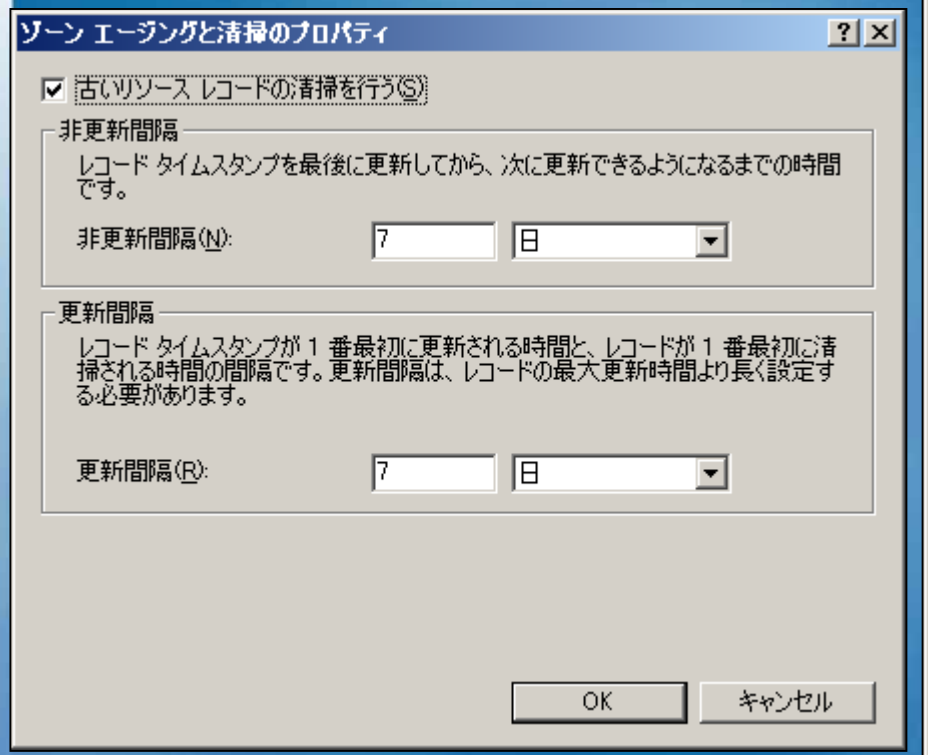
- ゾーン転送のためのDNSサーバを特定
  - ゾーンのネーム サーバー (NS) リソース レコードで指定されているサーバーへのみゾーン情報が転送
  - 指定した IP アドレスへの転送を許可するようにこの設定を変更

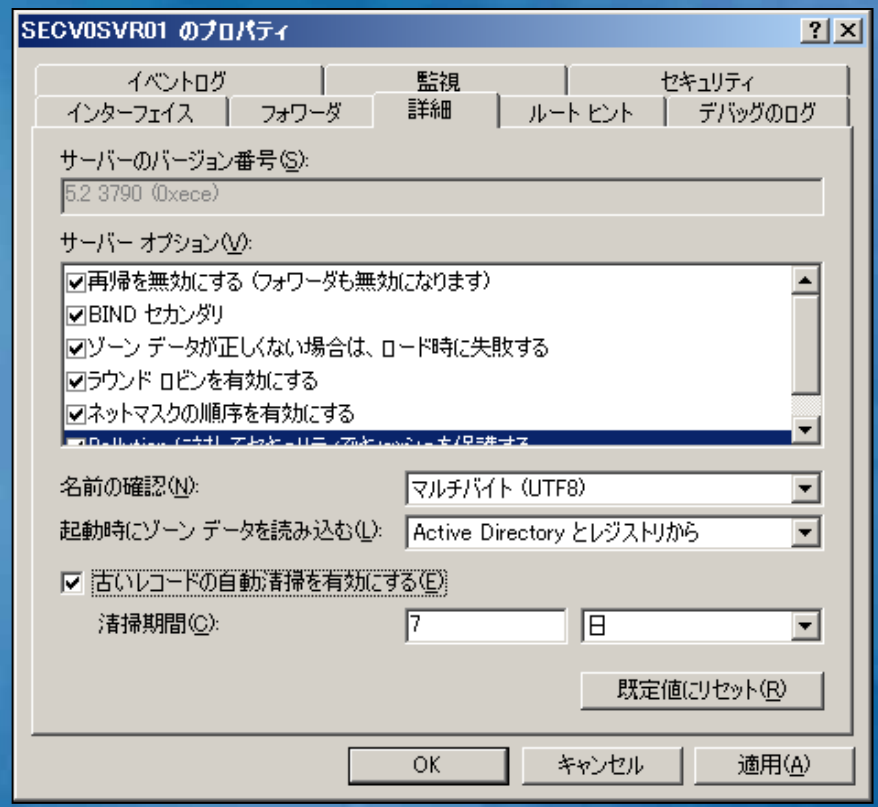
アプリケーション ゾーンの保護

- DNS ゾーン データの回復
  - バックアップファイルからの復旧
    - <システム ルート ディレクトリ>¥DNS¥Backup フォルダにあるバックアップ フォルダから DNS ゾーン ファイルを回復する
    - ゾーン作成時にバックアップ フォルダにコピーされる

アプリケーション

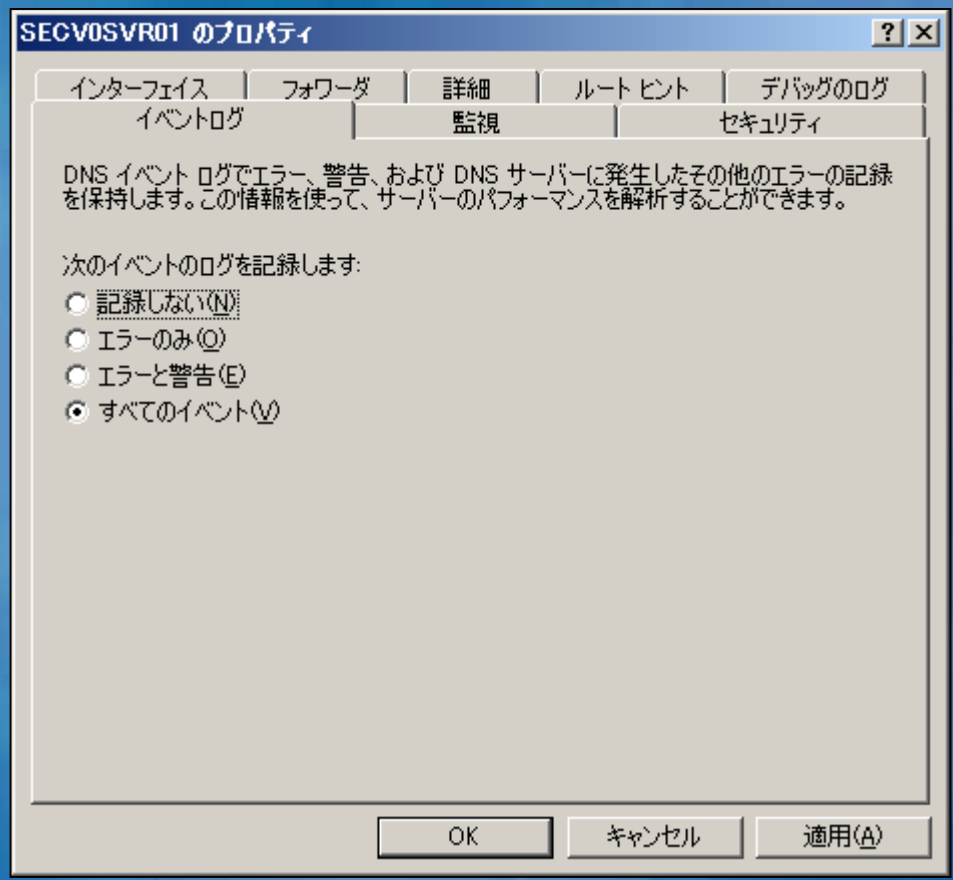
- 清掃サイクル (エイジング/スカビンジング)
  - データベース内の使用されていないレコードのリリースを行い古いデータの蓄積を防止





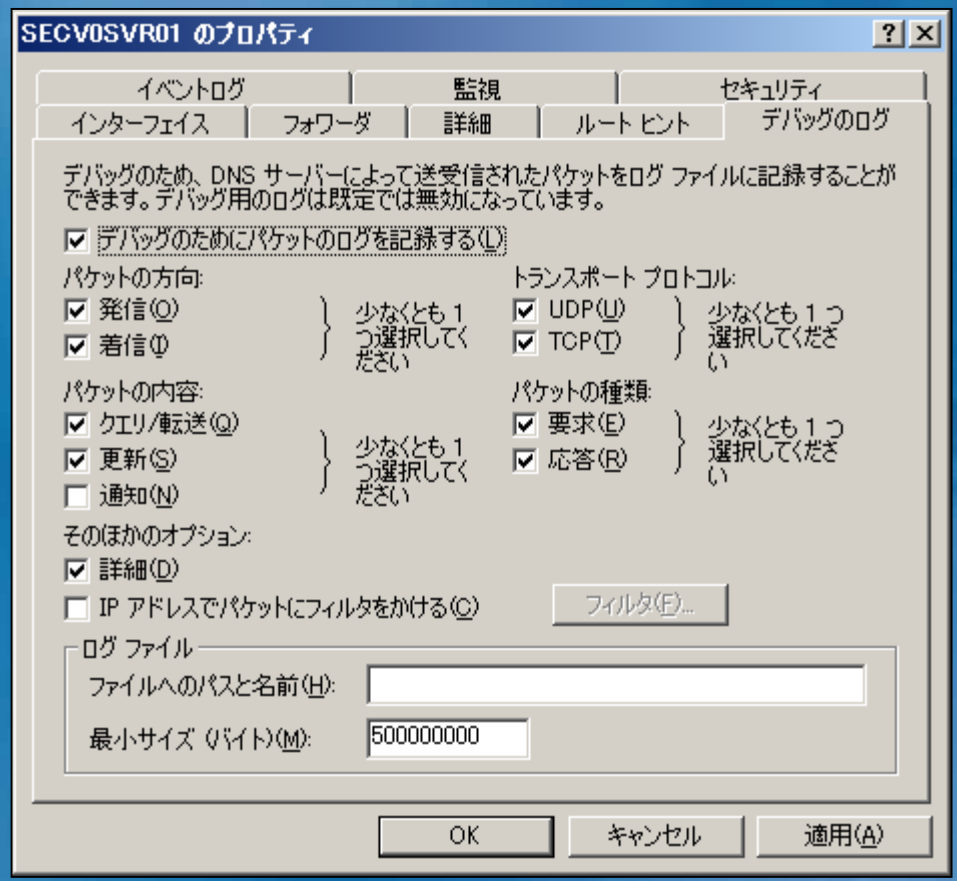
アプリケーション イベントログ

- すべてのイベントログを取得
  - 起動
  - シャットダウン
  - 構成エラー
  - ゾーン転送
  - etc



アプリケーション デバッグログ

- <システム ルート ディレクトリ>system32¥Dns¥Dns.log に書き込まれる
  - トラブルシュートなどに利用



その他

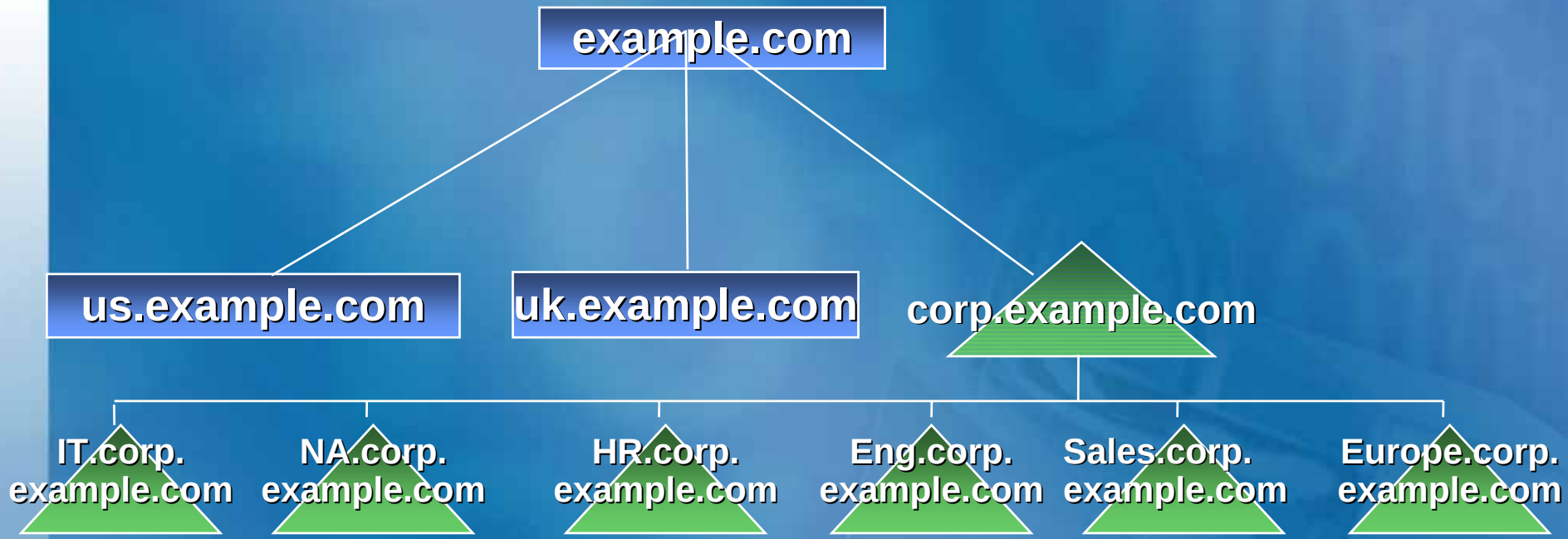
- 信頼できる人材だけへのDNS管理者特権を付与
- 更新不能な読み取り専用の DNS を使用

UNIX 環境における Windows DNS の相互運用性

既存環境へのActive Directory の導入
2種類の導入方法

- 重複しない名前空間への Active Directory の導入
  - 例:
    - 既存DNS名前空間：example.com
    - 導入するAD名前空間：
      サブドメイン corp.example.com または
      新規の内部専用ドメイン example.local など
- 既存の名前空間へのActive Directory の導入
  - 例: 既存のDNS名前空間：example.com
  - 導入するAD名前空間：example.com

既存の名前空間と重複しないADの導入



既存の名前空間と重複しないADの導入

- Active Directory 名前空間を Windows DNS 名前空間へ委任する

既存の名前空間と重複しないADの導入

Windows DNS へのゾーンの委任

既存 DNS Server

example.com

委任するゾーン “corp.example.com”

corp.example.com

corp.example.com

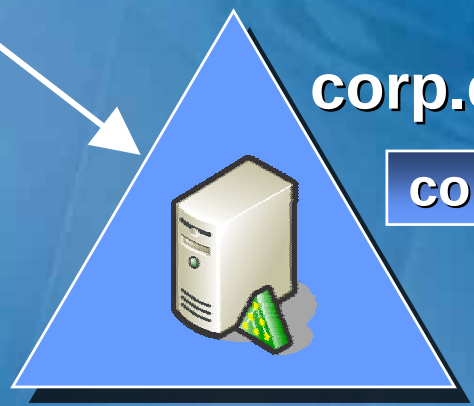
既存の名前空間と重複しないADの導入

Windows DNS へのゾーンの委任

既存 DNS Server

example.com

委任するゾーン “corp.example.com”



corp.example.com

corp.example.com

Recommended

既存の名前空間と重複しないADの導入

Windows DNS へのゾーンの委任

- 推奨するシナリオ:
  - 既存DNS管理者との管理（権限）の分離
  - セキュアな動的更新の適用
  - Active Directory 統合による単一障害ポイントの除去

既存の名前空間と重複しないADの導入

- Windows DNS サーバーへの委任
- 既存の権限のある DNSサーバーのSRV レコードのサポート
  - サポートしていない場合はアップグレードが必要

既存の名前空間と重複しないADの導入

Windows DNS へのゾーンの委任

既存 DNS Server

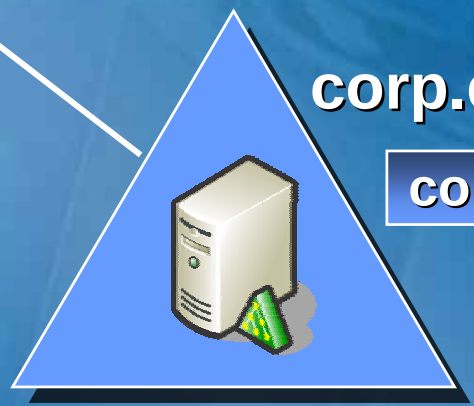
example.com

SRV レコードのサポート

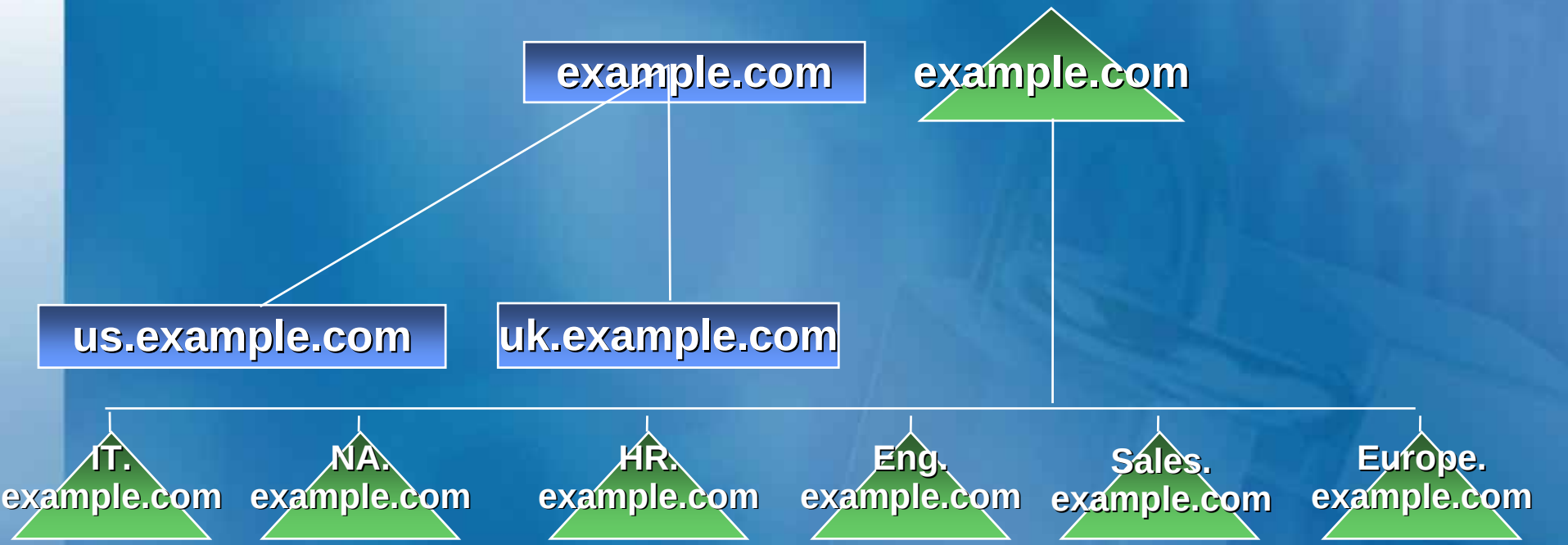
DNS レコードの登録

corp.example.com

corp.example.com



既存の名前空間への AD の導入
Windows DNS への移行



既存の名前空間への AD の導入

- 導入前の考慮点
  - 既存のDNSサーバーがSRVレコードをサポートしていない場合
    - サーバーのアップグレードが必要

既存の名前空間と重複しない AD の導入

既存 DNS Server のアップグレード

既存 DNS Server

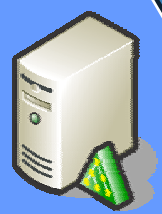
example.com

SRV レコードの
サポート

DNS レコードの登録

corp.example.com

corp.example.com



既存の名前空間へのADの導入
Windows DNS サーバーへの移行

既存 DNS Server

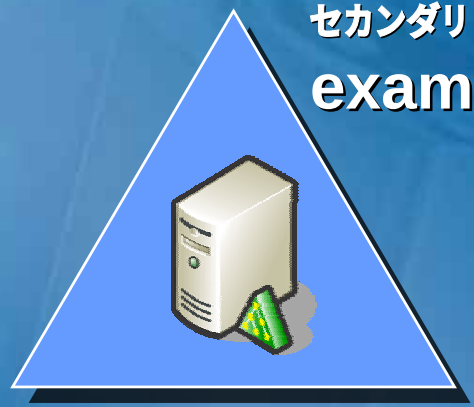
プライマリ

example.com

1. example.com の セカンダリ DNS サーバーとして Windows DNS サーバーを設置

セカンダリ

example.com



既存の名前空間へのADの導入
Windows DNS サーバーへの移行

既存 DNS Server

プライマリ

example.com

ゾーン転送

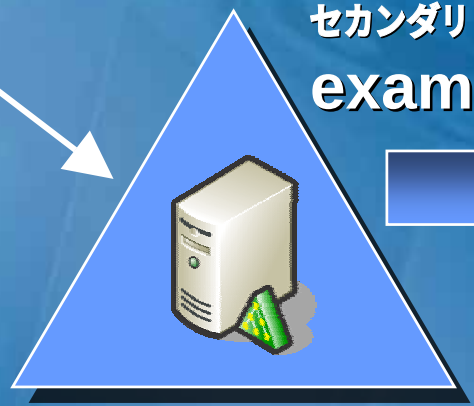
1. example.com の セカンダリ
   DNS サーバーとして
   Windows DNS サーバーを設置

2. ゾーン転送

セカンダリ

example.com

example.com



既存の名前空間へのADの導入
Windows DNS サーバーへの移行

既存 DNS Server

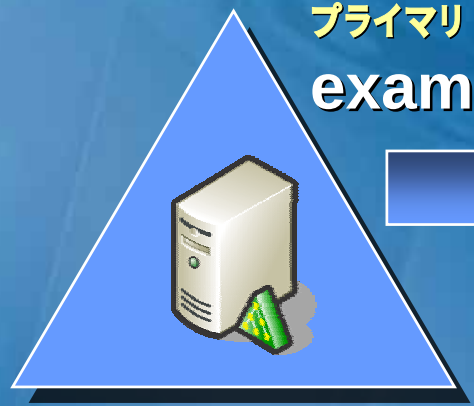
プライマリ

example.com

1. example.com の セカンダリ
   DNS サーバーとして
   Windows DNS サーバーを設置

2. ゾーン転送

3. Windows DNS サーバーを
   プライマリDNSサーバーへ
   昇格させる



プライマリ

example.com

example.com

既存の名前空間へのADの導入
Windows DNS サーバーへの移行

既存 DNS Server

セカンダリ または 削除

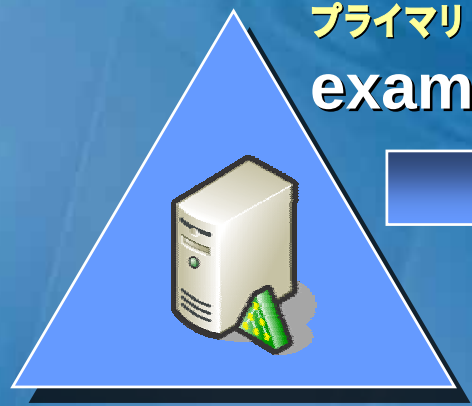
example.com

1. example.com の セカンダリ
   DNS サーバーとして
   Windows DNS サーバーを設置

2. ゾーン転送

3. Windows DNS サーバーを
   プライマリDNSサーバーへ
   昇格させる

4. 既存DNSサーバーの降格または削除



プライマリ

example.com

example.com

既存環境への AD の導入

- 既存の DNS サーバーが SRV レコードをサポートしていない場合は次の3つの方法のうちどれかを選択する
  - サーバーのアップグレード
    - SRV レコードをサポートさせる
  - Windows DNS サーバーへの移行
  - SRV リソースレコードを含む Windows DNS サーバーへのゾーンの委任を行う

管理用ツール

- コマンドラインツール
  - netdiag.exe (Update!)
  - nslookup.exe
  - dnscmd.exe
  - dnslint.exe (Update!)
  - ipconfig.exe
- WMI DNS プロバイダ
- DNS MMC コンソール

まとめ

- Windows 環境での DNSの役割
  - ドメインログオン時の利用
  - Windows DNS による動的更新の利点
- Windows DNS のセキュリティ
  - 多層防御によるサービスの保護
  - グループポリシー、サポートツールによる ハードニング (要塞化) 一括設定
  - Windows 統合環境でのアクセス制御
- 既存環境へのActive Directoryの導入
  - サブドメイン、内部ドメインによる導入
  - 既存環境からの移行

Microsoft®

Your potential. Our passion.™