Windows Server 2008 Active Directoryの強化点と新機能

グローバルナレッジネットワーク株式会社
横山 哲也
Microsoft MVP for Windows Server – Directory Services

自己紹介

- 1994年～ ITプロ向けWindows関連教育
- マイクロソフトMVP、MCSE(2003)
- 最近の著書・雑誌記事
  - ひと目でわかるMicrosoft Windows Server 2003ネットワーク設定・管理術 (日経BP出版センター)
  - 実践Active Directory逆引きリファレンス (毎日コミュニケーションズ)
  - 月刊 Windows Server World(IDGジャパン)
    - IT嫌いはまだ早い(連載)

Agenda

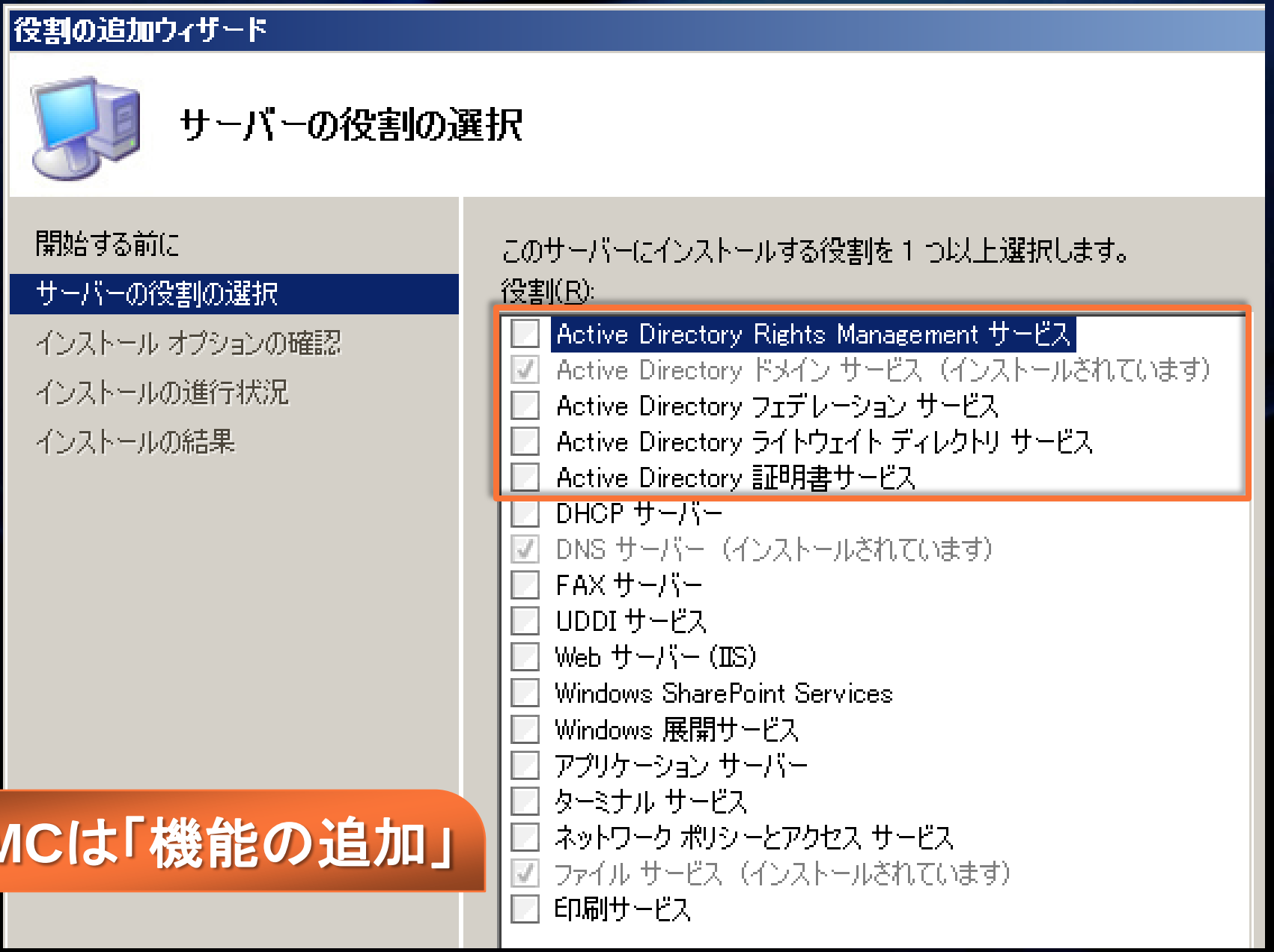
- Windows Server 2008 の Active Directory
- Active Directoryドメインサービス新機能
- きめ細かなパスワード ポリシー
- 読取専用ドメインコントローラ(RODC)
- その他の新機能
- まとめ

Windows Server 2008の Active Directory

Active Directory

- ドメインサービス
- ライトウェイトディレクトリサービス
- Rights Management Services
- 証明書サービス
- フェデレーションサービス

役割の追加と機能の追加



GPMCは「機能の追加」

Active Directoryドメインサービス

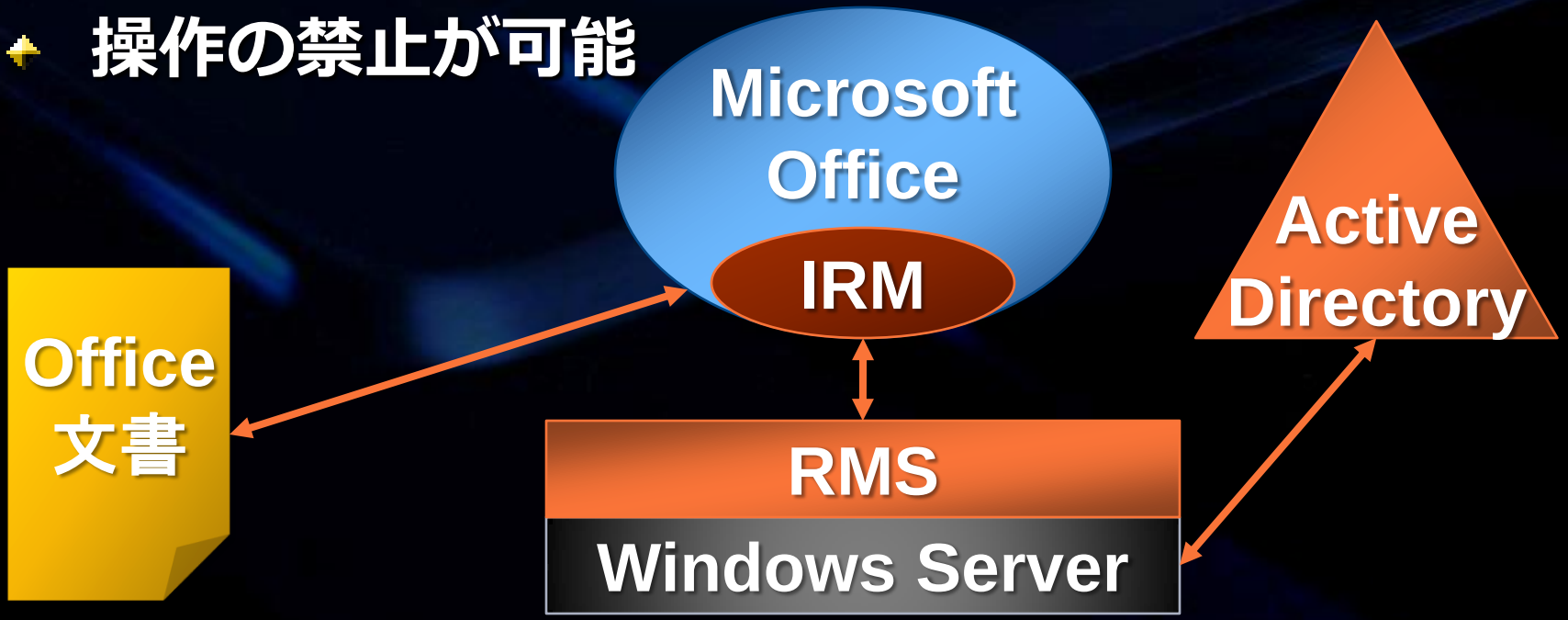
- いわゆる「Active Directory」
- 機能レベル…「Windows 2000混在」不可

Active Directory ライトウェイトディレクトリサービス

- 従来のADAM = LDAP サーバー
  - Active Directory Application Mode
- 認証のないActive Directory

Active Directory Rights Management Services

- 従来はオプション製品(サーバーは無償)
  - Windows Server 2008 に統合
  - クライアントライセンスについては不明
- Microsoft Office ドキュメントの暗号化
  - 操作の禁止が可能

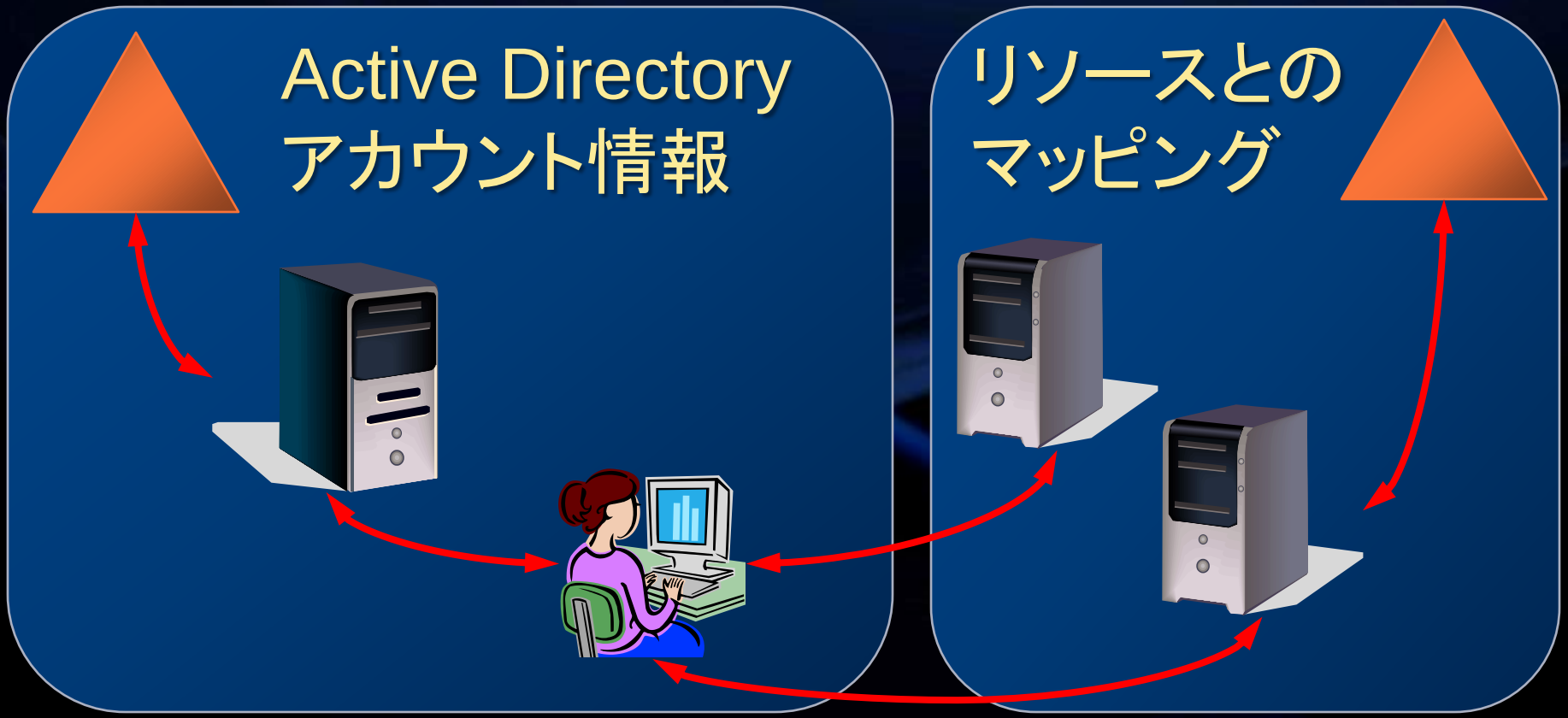


Active Directory証明書サービス

- 従来の「エンタープライズ証明機関」
  - Active Directoryと連動
  - ルート証明機関推奨
    - ドメインコントローラ以上の高セキュリティは無意味
- 従来以上にさまざまな場面で利用可能

Active Directory フェデレーションサービス (ADFS)

- 異なる組織間でアカウント情報を連係させる
  - アカウント情報の複製ではない



Active Directory ドメインサービス新機能概要

監査
きめ細かなパスワードポリシー
読取専用ドメインコントローラ
再起動可能なActive Directory
スナップショット表示
ユーザーインターフェイス強化
デモ

監査: 記録項目

- Windows Server 2003
  - 属性名のみ
- Windows Server 2008
  - 属性名
  - 旧属性値
  - 新属性値
- 実際にやってみると…
  - 更新ではなく、削除と作成が記録
    (GUIツールでもdsmodコマンドでも同じ)

監査: 詳細な監査の設定

- オブジェクトの監査を有効化
- オブジェクトの操作
- 監査ログを表示

監査ログの例(抜粋)

ディレクトリ サービス オブジェクトが変更されました。

オブジェクト:
DN: CN=YOKOYAMA Tetsuya,OU=Branch,DC=example,DC=com
クラス: user
属性:
LDAP 表示名: physicalDeliveryOfficeName
構文 (OID): 2.5.5.12
値: 新宿
操作:
種類: 値が削除されました

監査: 詳細な監査

- Windows Server 2003
  - ディレクトリ サービスのアクセスの監査
  - AUDITPOLコマンドでも可能
- Windows Server 2008
  - ディレクトリ サービスのアクセス
  - ディレクトリ サービスの変更
  - ディレクトリ サービスのレプリケーション
  - 詳細なディレクトリサービスレプリケーション

きめ細かなパスワードポリシー

- Windows Server 2003
  - パスワードポリシーはドメイン単位
- Windows Server 2008
  - グローバルセキュリティグループまたは
    ユーザー単位で異なるポリシーを設定可能

詳細は後述

読取専用ドメインコントローラ

- ディレクトリの(ほぼ)完全なコピー
  - ただし読み取り専用(単一方向の複製)
  - パスワードは限定的にコピー
- ブランチオフィスからの
  アカウント漏洩リスクを減らす
- BDCではない
  - BDC: Backup Domain Controller

再起動可能なActive Directory

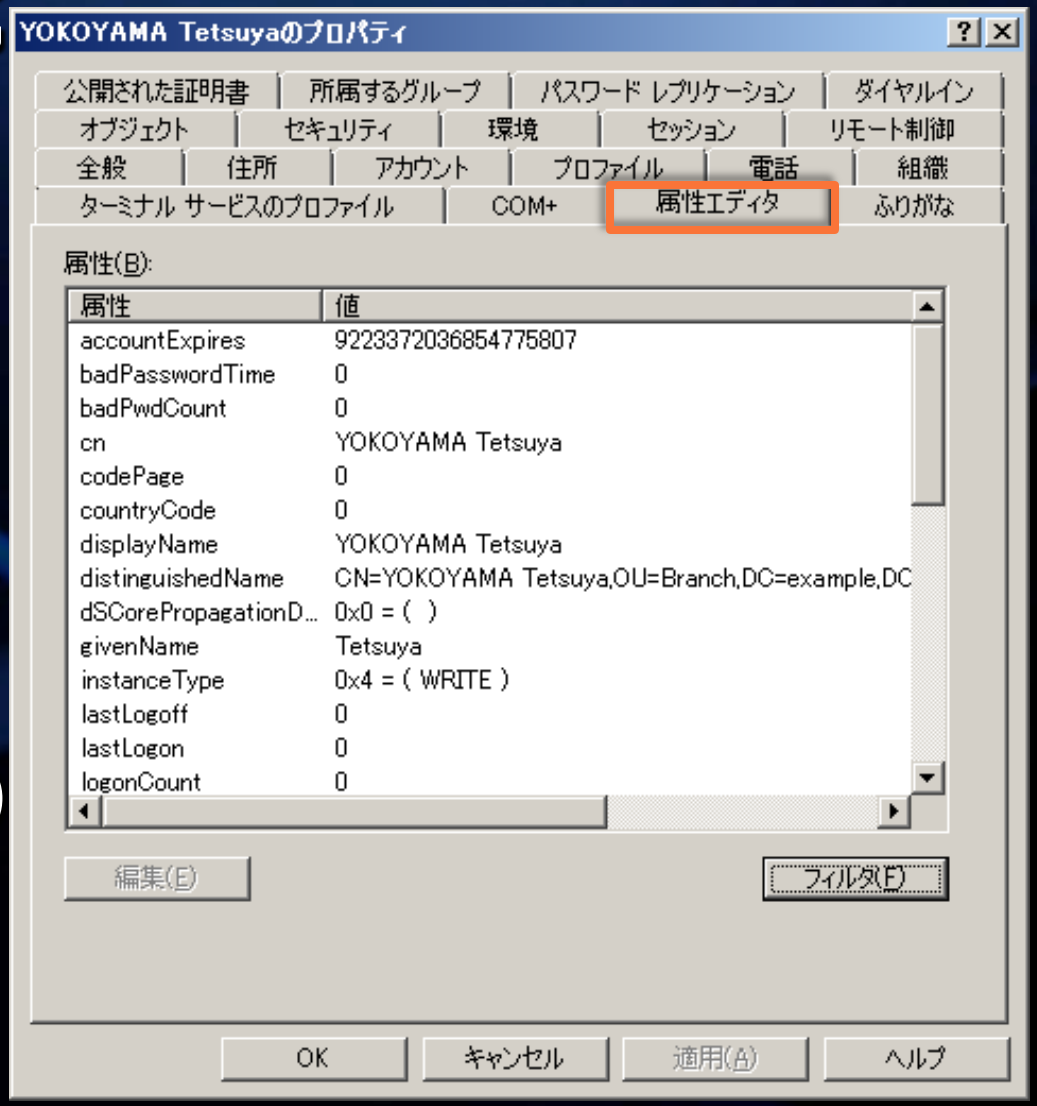
- 従来はディレクトリサービス復元モードのみ
  - セーフモードの一種
  - 全サービスが停止
- OS稼働中にActive Directoryの停止可能
  - メンバーサーバーとして動作
  - 複数の役割をインストールした場合
DC停止中でも他の役割は利用可能
  - 利用例: オフラインデフラグ

スナップショット表示

- 意味: ディレクトリのスナップショット保存
- 目的: 誤削除の復旧を容易にする
- 手順:

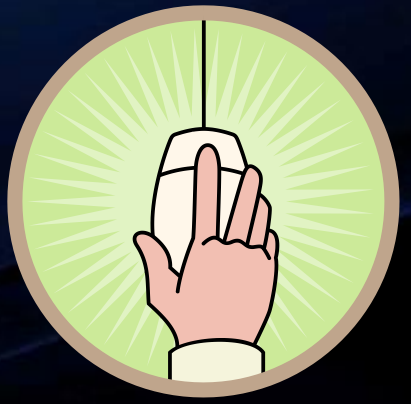
ユーザーインターフェイス強化

- DC昇格機能の強化
  - DCPROMOの設定を保存して再利用可能
- 管理ツールの強化
  - 属性エディタADSIEDITと同等
  - NTDSSettingsの構成(GC設定等)



Active Directory ユーザーとコンピュータ

デモ



1. オブジェクト属性
2. ドメインコントローラ属性の表示

きめ細かなパスワードポリシー

従来の問題点
Windows Server 2008の回答
Granular Password
デモ

従来の問題点

- パスワードポリシーはドメイン単位
- すべてのユーザーのパスワード強度が同じである必要はない
- すべてのユーザーが(システムにとって)同じように重要なわけではない
  - 一般ユーザーと管理者の重みは違う

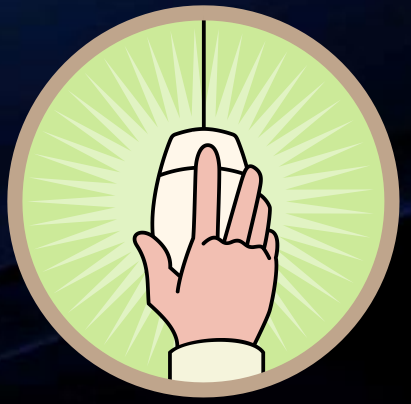
Windows Server 2008の回答

- 適切な単位でのパスワードポリシー設定
- グローバルセキュリティグループ
  またはユーザー単位
- 競合解決
  - グループよりもユーザー優先
  - グループ同士またはユーザー同士の競合は
    ポリシーに設定された優先順位を利用
  - 同じ優先順位の場合は不定(読み込み順)
- 問題点
  - 管理インターフェイスが貧弱

Granular Password
設定手順: 全てADSIEDITを利用

1. System/Password Settings ContainerにmsDS-PasswordSettingsオブジェクト追加(名前は任意)
2. パスワードポリシーの優先順位を指定 msDS-PasswordSettingsPrecedence
3. 設定したいポリシー値を指定
   - パスワードポリシー(6項目)
   - ロックアウトポリシー(3項目)
4. 適用先グループまたはユーザーを指定 msDS-PSOAppliesTo(DN形式)

Granular Password
デモ



1. ドメインのパスワードポリシーの確認
2. Password Settings Containerの設定
3. パスワードポリシー変更の確認

読取専用ドメインコントローラ (RODC)

従来の問題点
Windows Server 2003の回答
Windows Server 2008の回答
RODCの利点
RODCの注意事項
RODCの構成手順
RODCの利用シナリオ
デモ

従来の問題点
ブランチオフィスの実態

- 専任の管理者が不在
  - システム全体の管理者権限を与えたくない
- 管理体制が不十分
  - サーバー室に鍵がない→盗難リスクがある
- 低速なネットワーク
  - ログオンに時間がかかる
  - DCを配置すると複製に時間がかかる

Windows Server 2003の回答
GCレスログオン

- ログオンの高速化と複製トラフィックの削減
  - ドメイン分割して、DCをローカル配置
  - GCレスログオンを併用
    ユニバーサルグループメンバシップキャッシュ
  - セキュリティ問題の局所化

問題点
ドメイン分割の場合にのみ効果あり
複数ドメインの管理負荷大

Windows Server 2008の回答
読み取り専用ドメインコントローラ(RODC)

- シングルドメインでの対応
  - 複製の問題は解決しつつある
  - むしろ管理者の負担の方が問題
- 支社にRODCを配置
- RODC = ディレクトリの完全複製
  - シングルドメインで運用可能
  - GCにしても負荷は変わらない

問題点
複製の問題が残る場合は
Windows Server 2003
スタイルで対応

RODCの利点

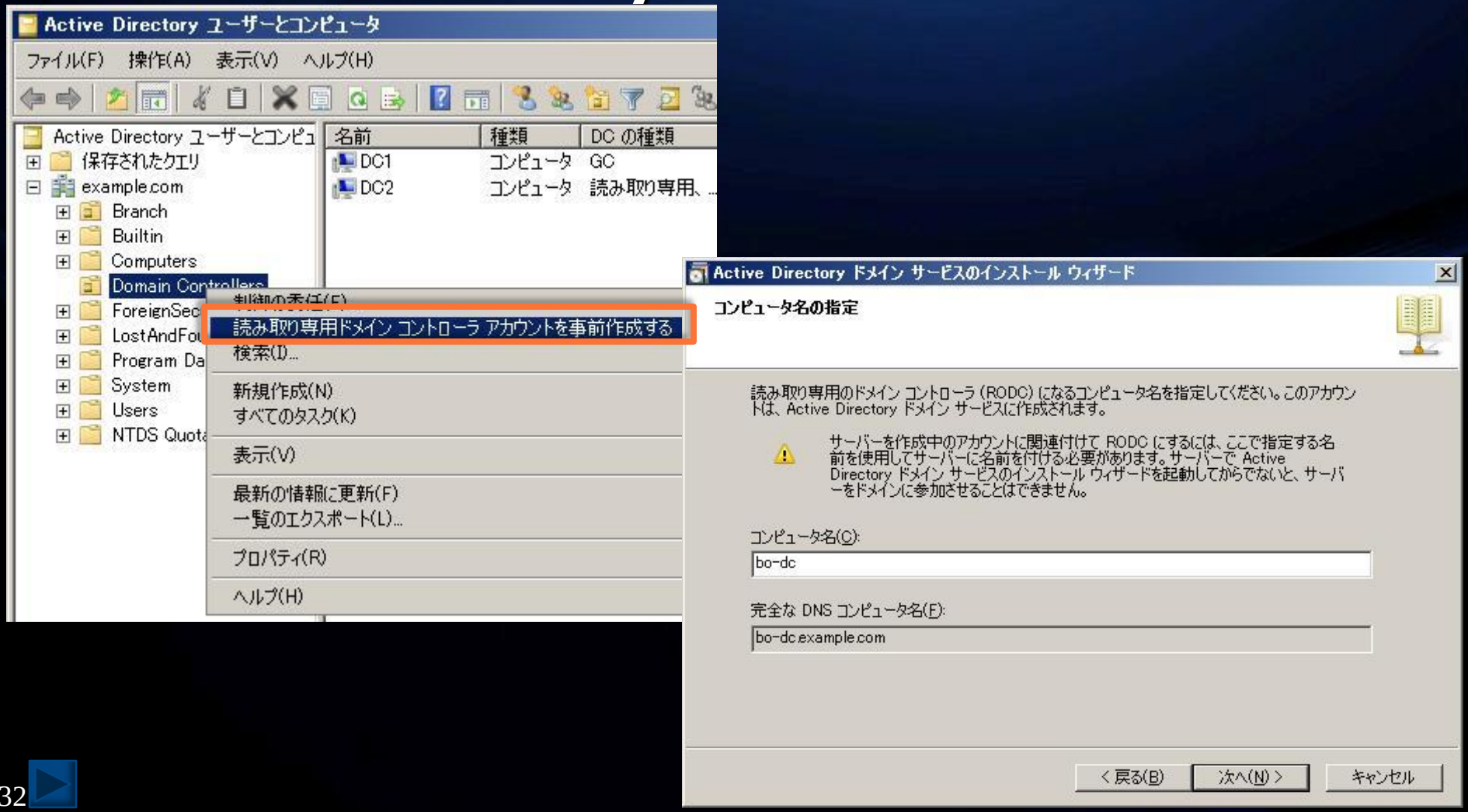
- ログオン時間の短縮
  - 同一サイトにドメインコントローラを配置
- セキュリティの向上
  - ログオンしないアカウントのパスワードは複製されない
  - ドメイン管理者とサーバー管理者の分離 Domain AdminsでなくてもRODC管理可能
- サイト設計が単純になる
  - 単一方向の複製のみ考えれば良い

RODCの注意事項

- RODC構成の条件
  - PDCエミュレータ = Windows Server 2008
  - フォレスト機能レベル = Windows 2003以上
- RODC上のDNS統合ゾーン
  - 動的更新不可
  - NSレコードにRODCホスト名が登録されない

RODCの構成手順: 第1ステップ
RODCアカウントの作成(省略可)

- Active Directoryユーザーとコンピュータ



RODCの構成手順: 第2ステップ
RODCに昇格(必須)

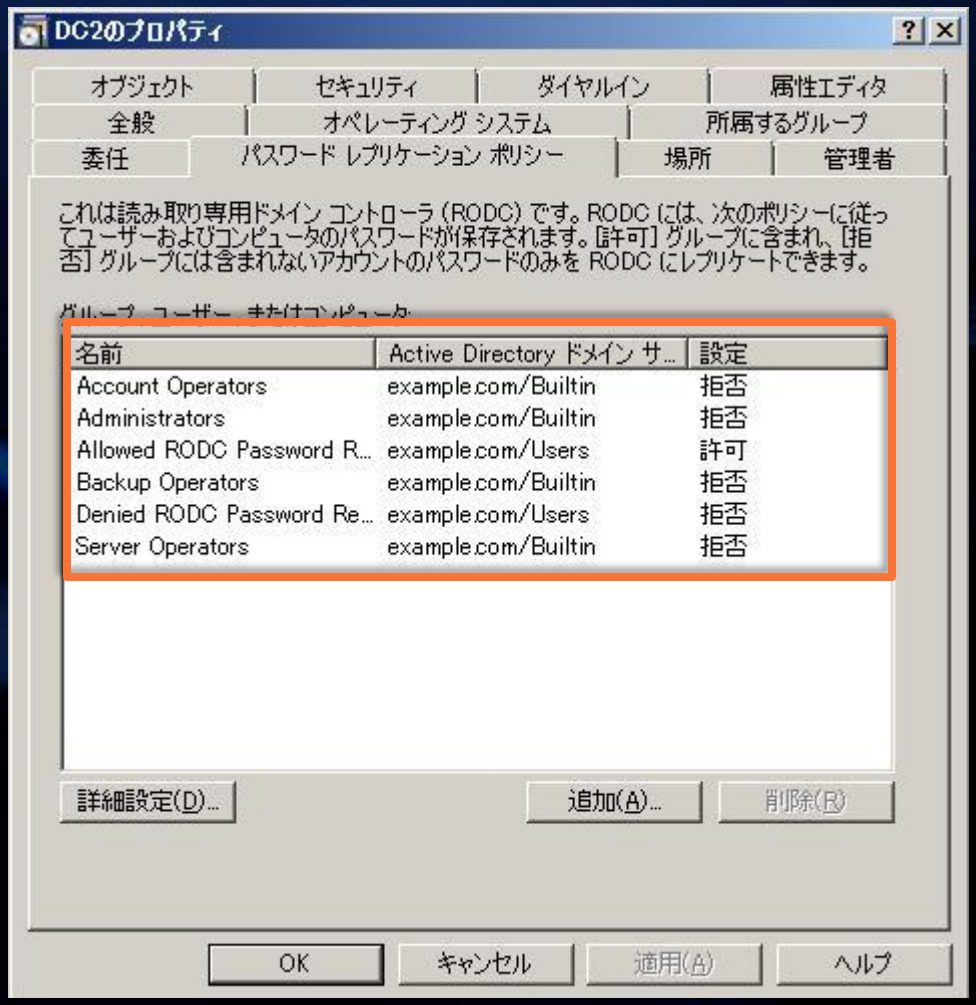
- 「DCPROMO」コマンド
  - 第1ステップを実行した場合

```
dcpromo /UseExistingAccount:Attach
```

- ドメインコントローラアカウントの確認

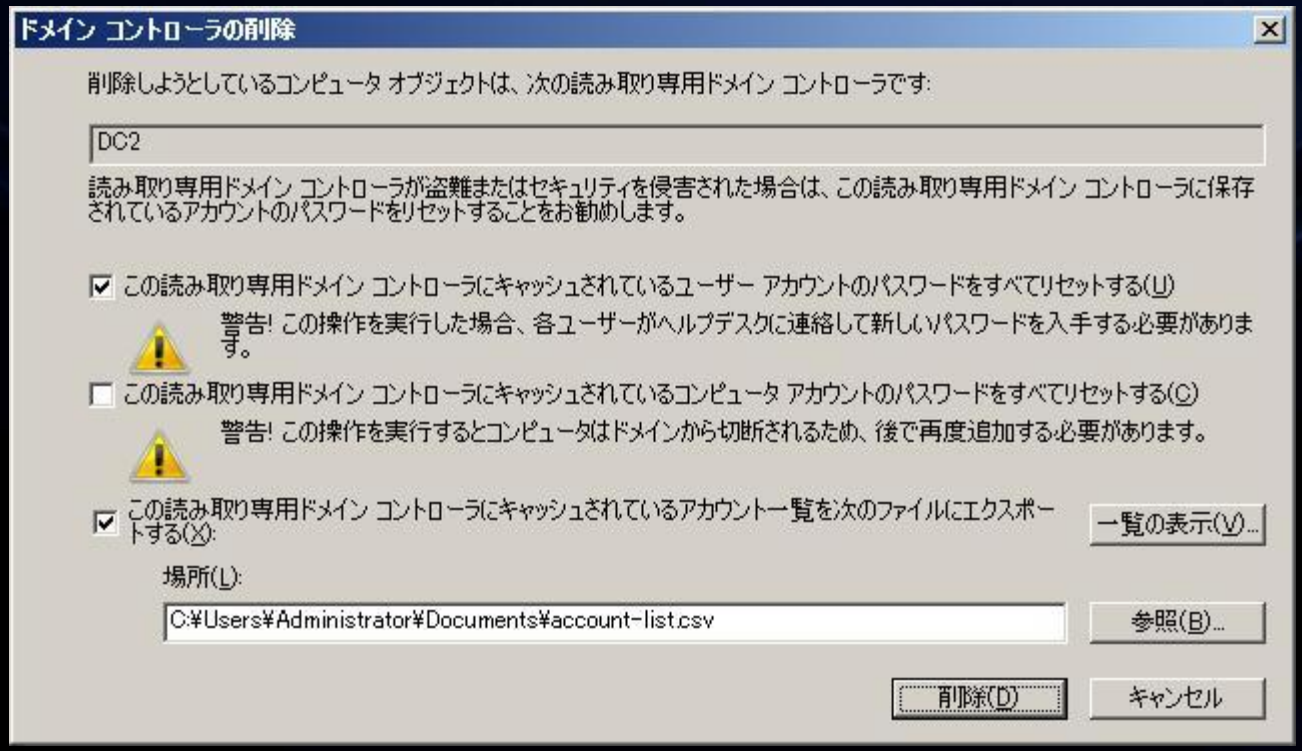
RODCの構成手順: 第3ステップ
パスワード複製ポリシーの設定

- Active Directoryユーザーとコンピュータ
- プリロードも可能

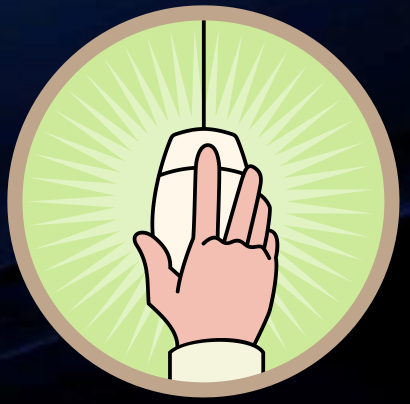


RODCの利用シナリオ
例: RODCが盗まれた!

- RODCアカウントの削除
- RODCにパスワードをキャッシュしている全アカウントのパスワード変更



読取専用ドメインコントローラ
デモ



1. パスワード複製可能なグループの設定
2. 通常のログオン
3. キャッシュを使ったログオン
4. RODCがセキュリティ侵害を受けた場合
5. パスワードを保護できることを確認

その他の新機能

時間の都合で説明できなかった機能
細かいけれど重要な機能

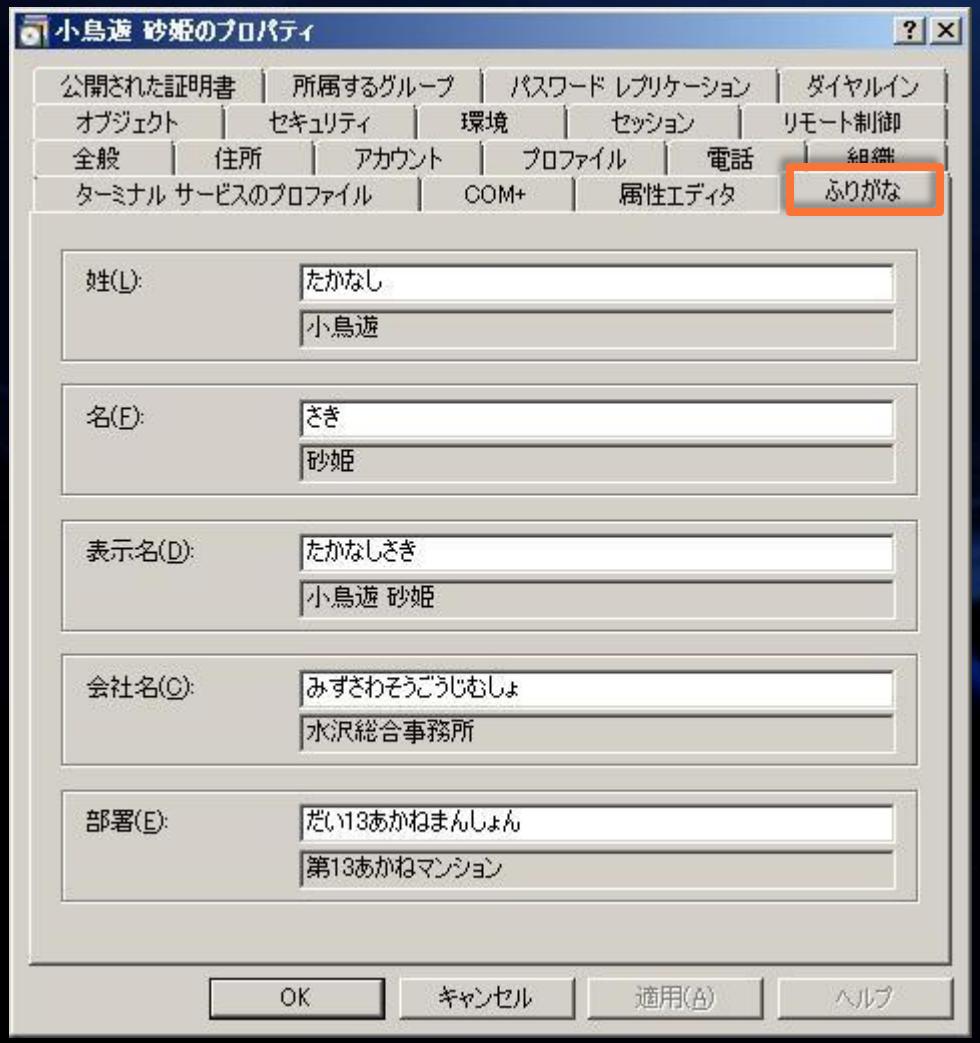
グループポリシー
ふりがな機能
削除禁止フラグ

グループポリシー

- Windows Vista 完全サポート
  - 新しいポリシーの設定が可能
- 中央ポリシーテンプレートのサポート
  - ADMXファイルの集中管理
  - 多言語対応

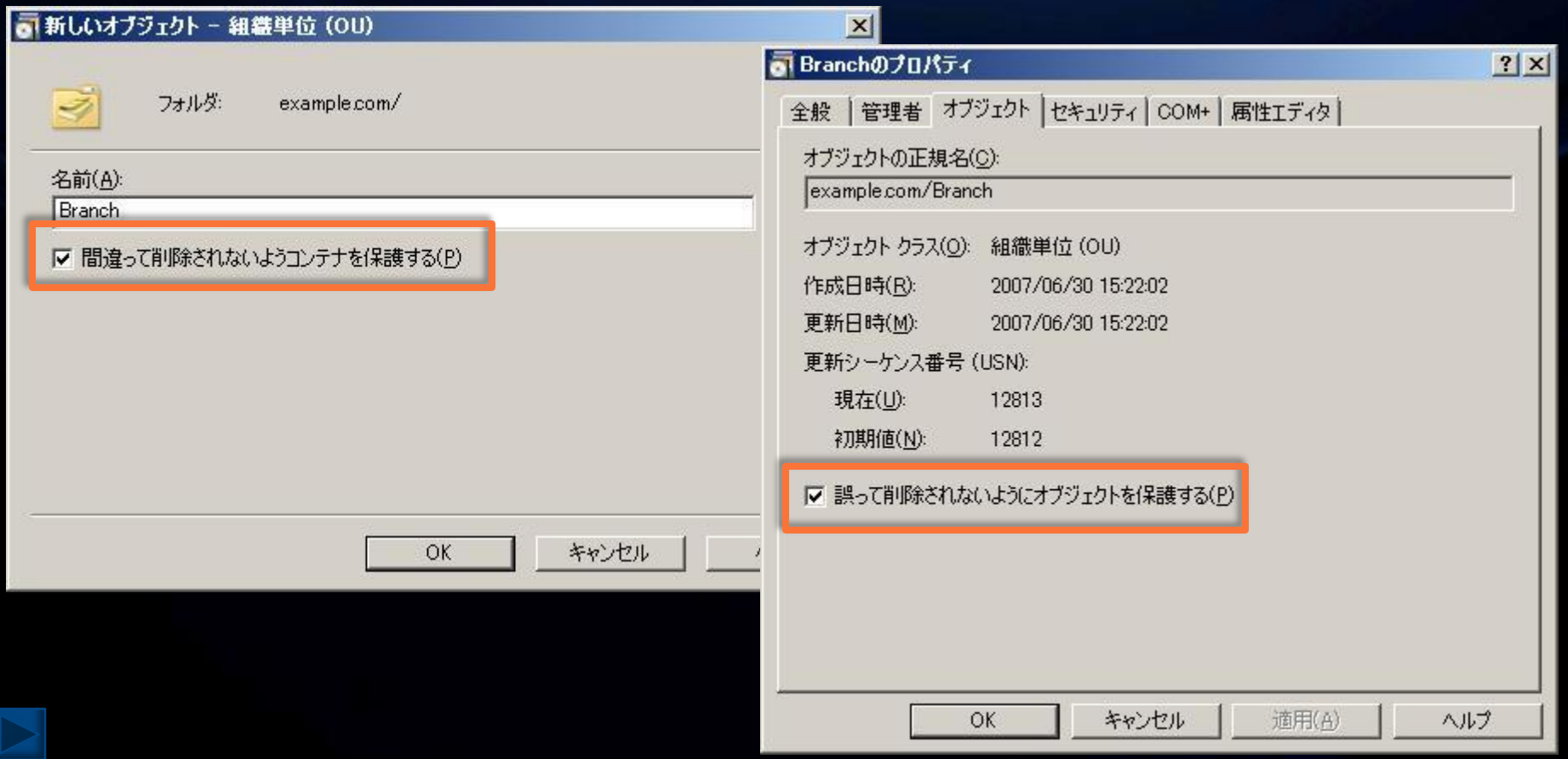
ふりがな(Phonetics)

- ソート順序のために重要



削除禁止フラグ

- 操作ミスを予防するために重要
- 既定ではOUに自動的に設定



まとめ

まとめ

- Windows Server 2008 の Active Directory
- Active Directoryドメインサービス新機能
- きめ細かなパスワード ポリシー
- 読取専用ドメインコントローラ(RODC)
- その他の新機能
- まとめ

参考資料

- Windows Server 2008 公式日本語サイト
  http://www.microsoft.com/japan/windowsserver2008
- Windows Server 2008 公式英語サイト
  http://www.microsoft.com/windowsserver2008
- Windows製品開発部ブログ
  - http://www.exconn.net/Blogs/windows
- 高添はここにいます
  - http://blogs.technet.com/osamut/
- 千年Windows
  - http://www.g20k.jp/