Sophia Network

AD FS環境におけるAD RMSの利用

株式会社ソフィアネットワーク
国井　傑

自己紹介

国井 傑 (くにい すぐる)

- 株式会社ソフィアネットワーク取締役
- Microsoft MVP for Directory Services (Jul 2006-)

略歴

- 1997年　マイクロソフト認定トレーナーとしての仕事を開始
- 2000年　寝返りで脱臼 (元旦)
- 2001年　胸骨骨折して呼吸困難
- 2002年　脱臼して講習会でがんばるも、[ネタ]といわれる
- 2003年　ボールを投げたら肩もはずれた

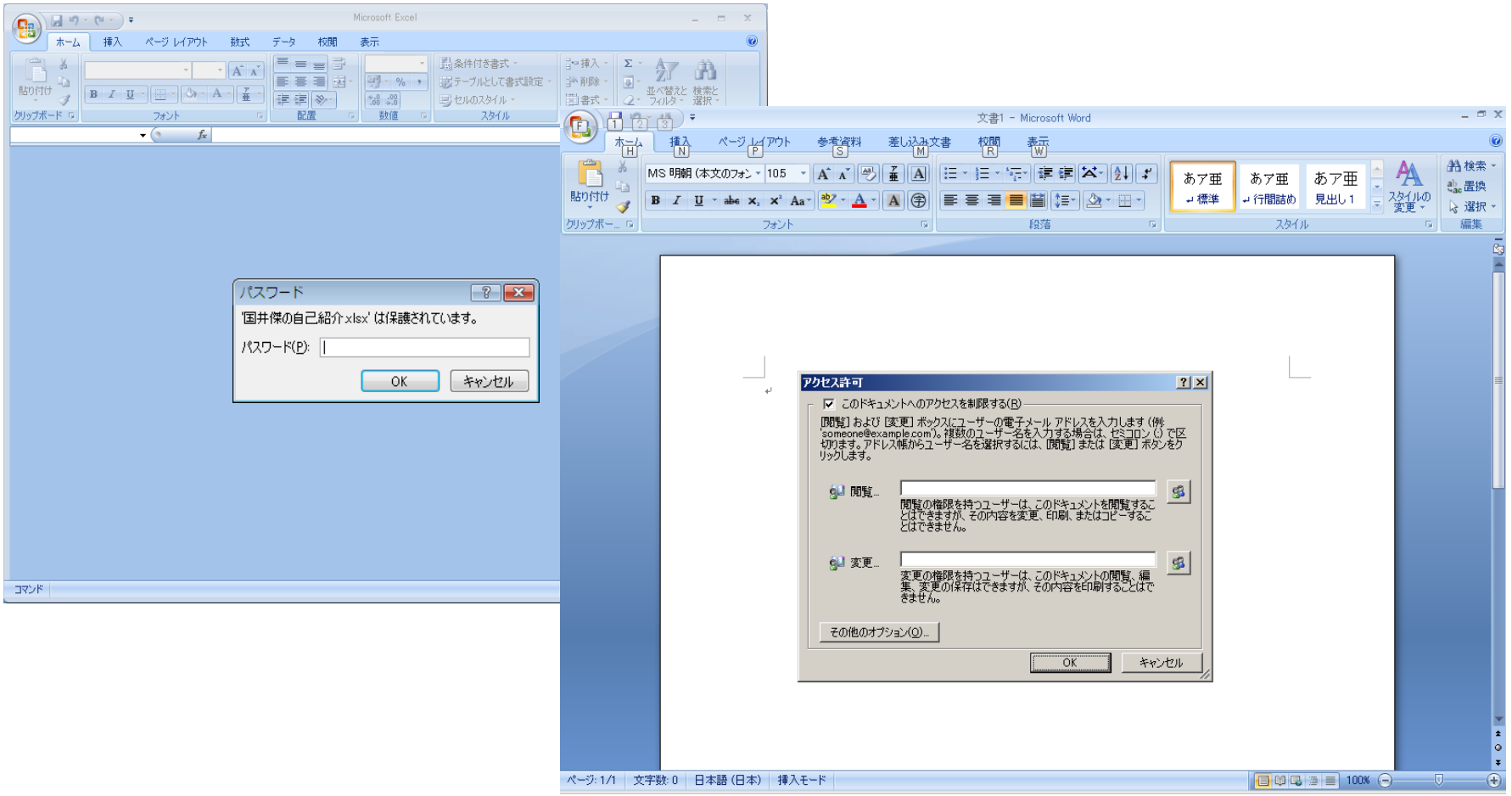
つまり...

「硝子」のトレーナー

すぐに壊れる(凹む)ので、お手柔らかにお願いします

今日のおはなし

- 企業間でのOfficeドキュメントの保護方法



今日のテクノロジ

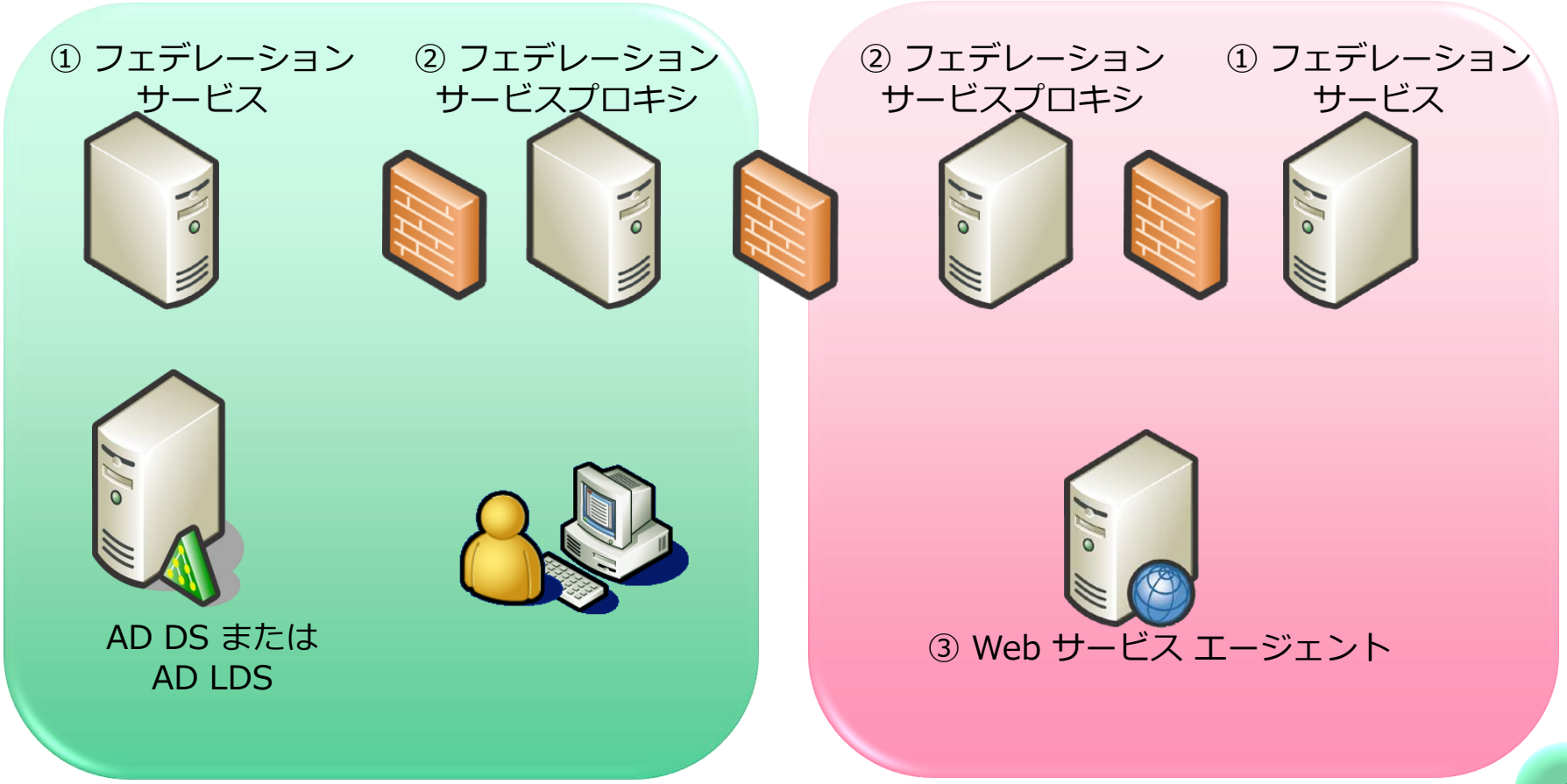
マイクロソフト の ID & アクセス管理ソリューション

ソリューション エリア	製品	
ID ライフサイクル管理	Microsoft Identity Lifecycle Manager 2007	IDA 管理
情報保護	Windows Rights Management Services	プラットフォーム
ID フェデレーション	Active Directory Federation Services	
強力な認証	Windows Certificate Services	
ディレクトリ サービス	Active Directory Directory Services Active Directory Lightweight Directory Services	
API ・ コネクタ ・ スタンダード		拡張性

色々ありますが…

AD FSに絞って説明します

AD FSのコンポーネント



WEBサービスエージェントでサポートするアプリケーションの種類

Sophia Network

NT トークン ベース	• Windows ベースの承認機構を利用 • 認証コンテキストを生成するためのセキュリティ プリンシパルが必要 • AD FS 認証トークンから Windows 認証トークンへ透過的な変換をサポート
要求に対応	• NT トークンは不要 • 受け取ったトークンの内容から承認を行う • 要求は定義が可能 • UPN、共通名、電子メール、カスタム要求

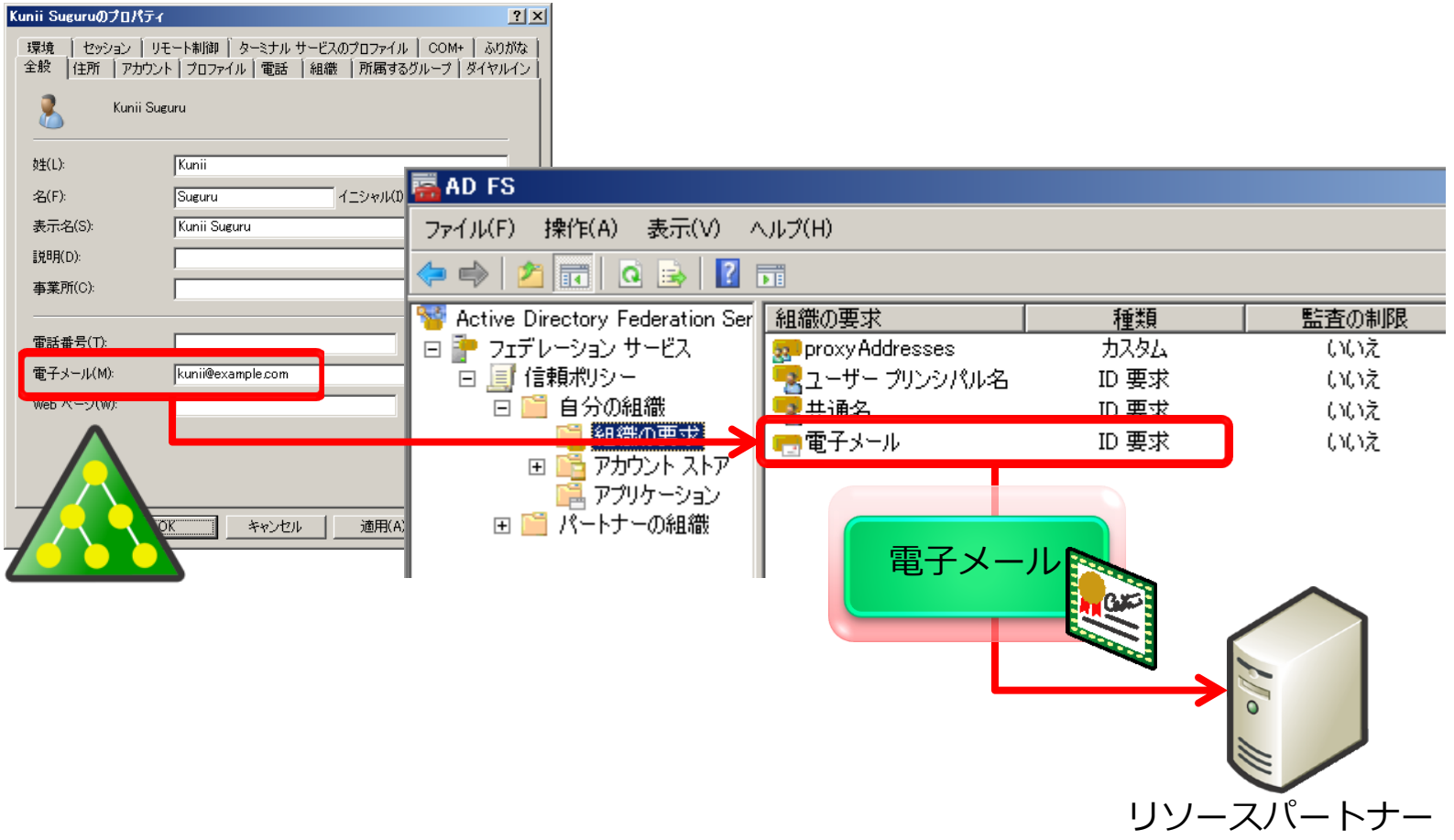
要求、セキュリティトークン、STS

- 要求 (クレーム)
  - ユーザーについての情報
- セキュリティトークン
  - 1つ以上の要求に対して、アカウントパートナーのフェデレーションサービスがデジタル署名したもの
- STS (セキュリティ トークン サービス)
  - セキュリティトークンの生成と送受信など、セキュリティトークンに関する管理を担当

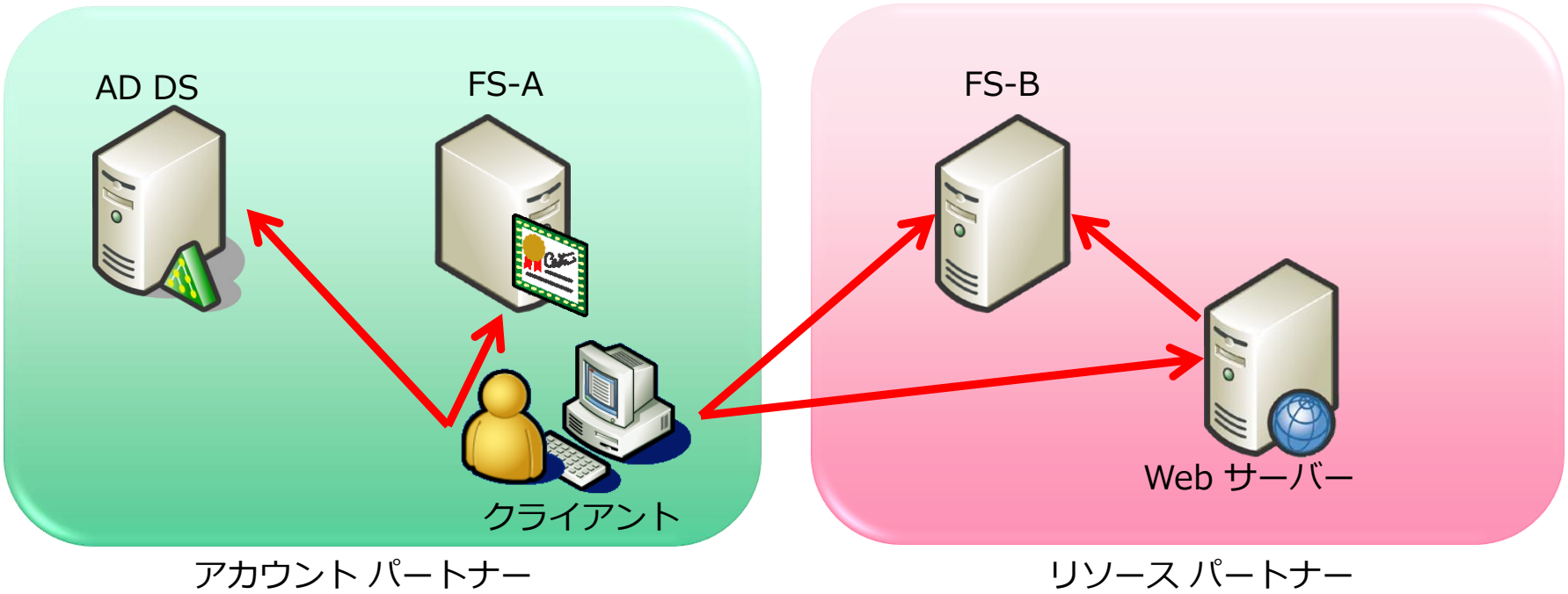
セキュリティ トークン

要求のながれ

- AD ユーザーの属性 mail を ”電子メール” という要求としてリソースパートナーに送信



ここまでのまとめ：フェデレーション動作概要



1. クライアントは Web サーバーにアクセス
2. Web サーバーは FS-B の URL を通知し、クライアントは FS-B にアクセス
3. FS-B は FS-A の URL を通知 (ホーム領域の解決) し、クライアントは FS-A にアクセス
4. FS-A はユーザー認証し、成功すると要求を含むセキュリティトークンを発行
5. クライアントはセキュリティトークンを Web サーバーに提示
6. Web サーバーが受信したトークンは FS-B でその内容を検査され、要求を Web サーバーが受信する

AD FSをAD RMSと共に実装します

AD FS 環境での AD RMS の実装手順

① リソースパートナーの準備

② アカウントパートナーの準備

③ 両方のパートナーで AD FS の実装

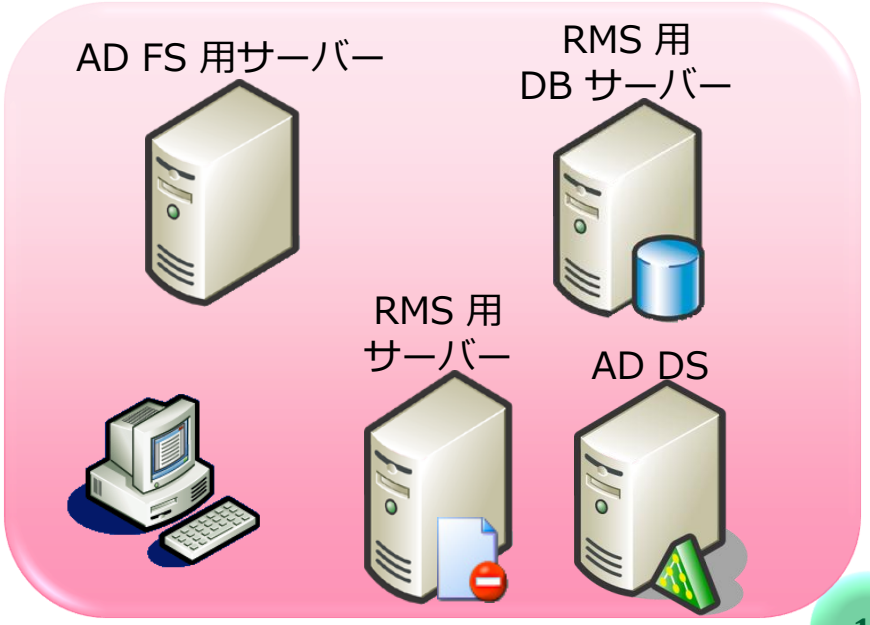
④ AD RMS の実装と AD FS と連携させるための設定

⑤ クライアントの設定

① リソースパートナーの準備

- アカウントストア (AD DS/AD LDS) をインストール
- そのほか、AD FS、AD RMS、AD RMS 用データベースの各サービスを提供するサーバーを用意
- すべてのコンピュータはリソースパートナーのドメインに参加

アカウント パートナー



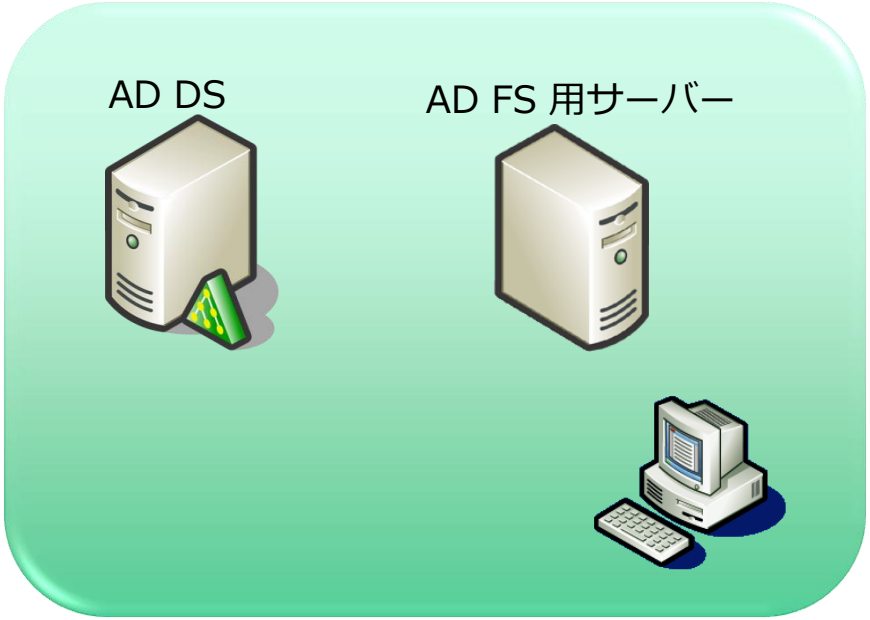
リソース パートナー

① リソースパートナーの準備(詳細手順)

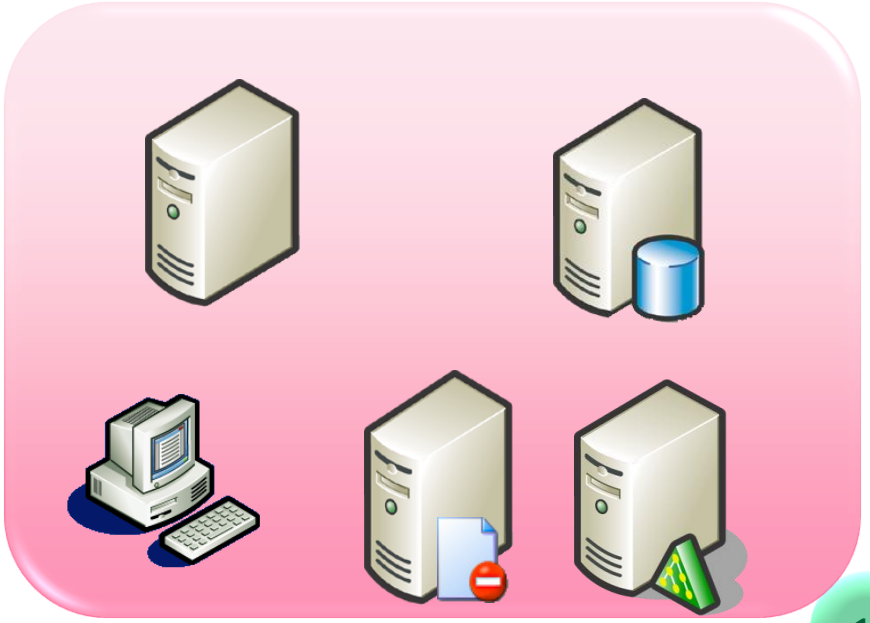
項番	作業内容
1	Active Directory と DNS サーバーのインストール
2	リソースパートナードメインのすべてのコンピュータをドメイン参加
3	AD RMS をインストールするサーバーで、ファイル共有を許可する Windows ファイアウォールの例外を設定
4	AD FS 管理者アカウントの作成と Domain Admins グループへ追加

② アカウントパートナーの準備

- アカウントストア (AD DS/AD LDS) をインストール
- 別途 AD FS を提供するサーバーを用意
- すべてのコンピュータはアカウントパートナーのドメインに参加
- DNS サーバーはフォワーダを使ってリソースパートナーの DNS サーバーを参照できるようにしておく



アカウント パートナー



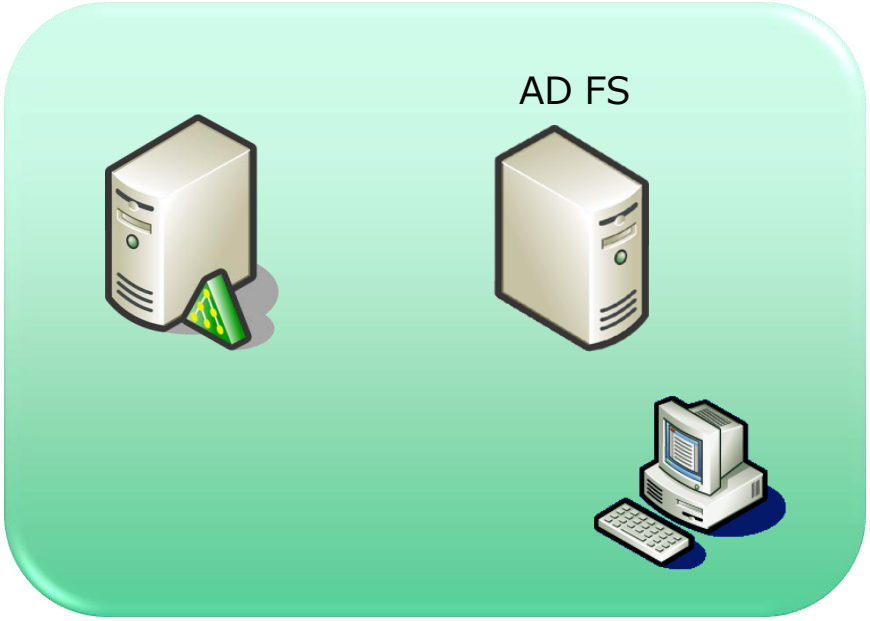
リソース パートナー

② アカウントパートナーの準備(詳細手順)

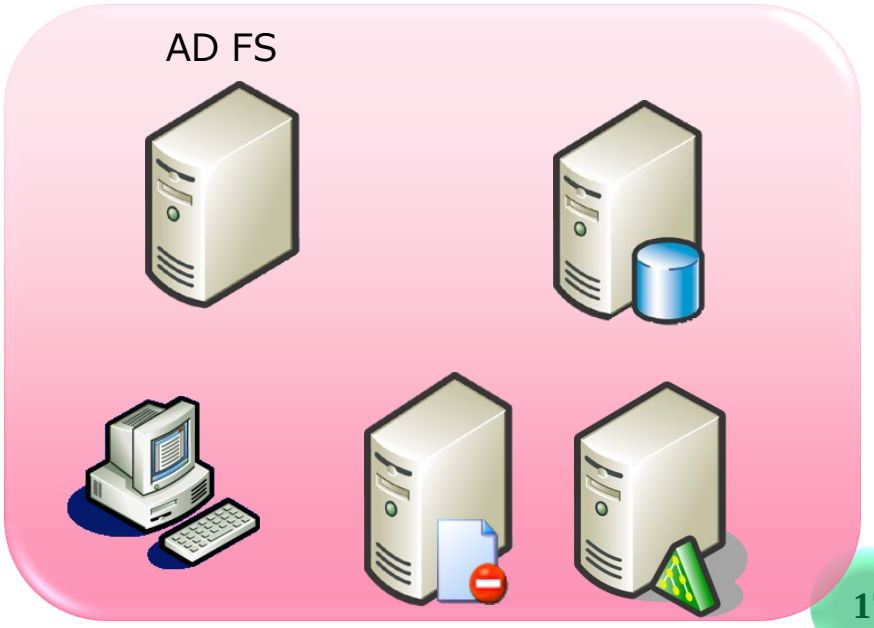
項番	作業内容
1	Active Directory と DNS サーバーのインストール
2	アカウントパートナードメインのすべてのコンピュータをドメイン参加
3	DNS フォワーダを設定 (フォワーダ先にリソースパートナーのDNSサーバーを指定)
4	ユーザーの作成 (メールアドレスの設定)
5	クライアントコンピュータでホーム領域の設定

③ 両方のパートナーで AD FS を実装

- アカウントパートナー / リソースパートナーで AD FS の役割を追加
- サーバー証明書の実装
- カスタム要求 (proxyaddresses) の作成
- AD FS でアカウントパートナー / リソースパートナーの指定
- 要求に対応するアプリケーションの作成



アカウント パートナー



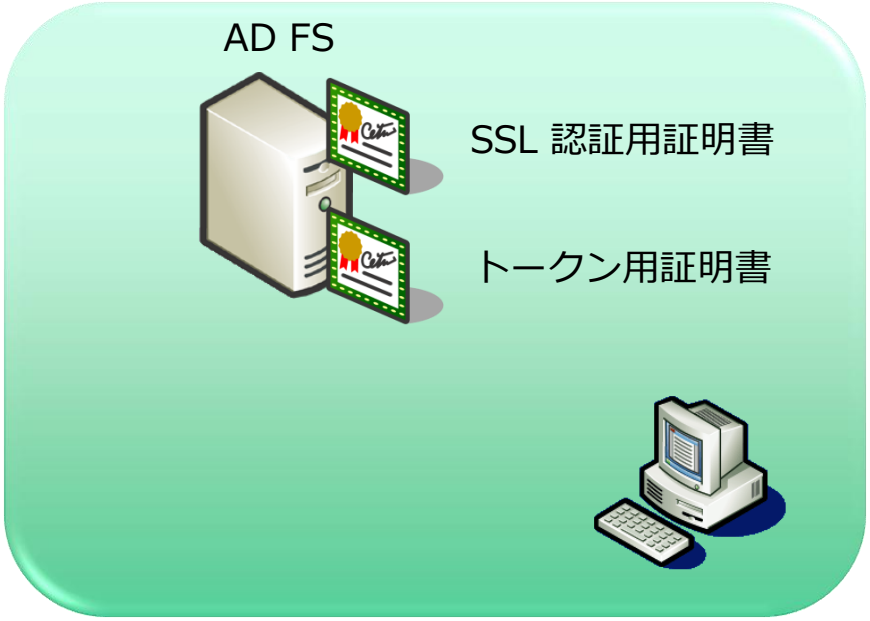
リソース パートナー

③ 両方のパートナーで AD FS を実装(詳細手順)

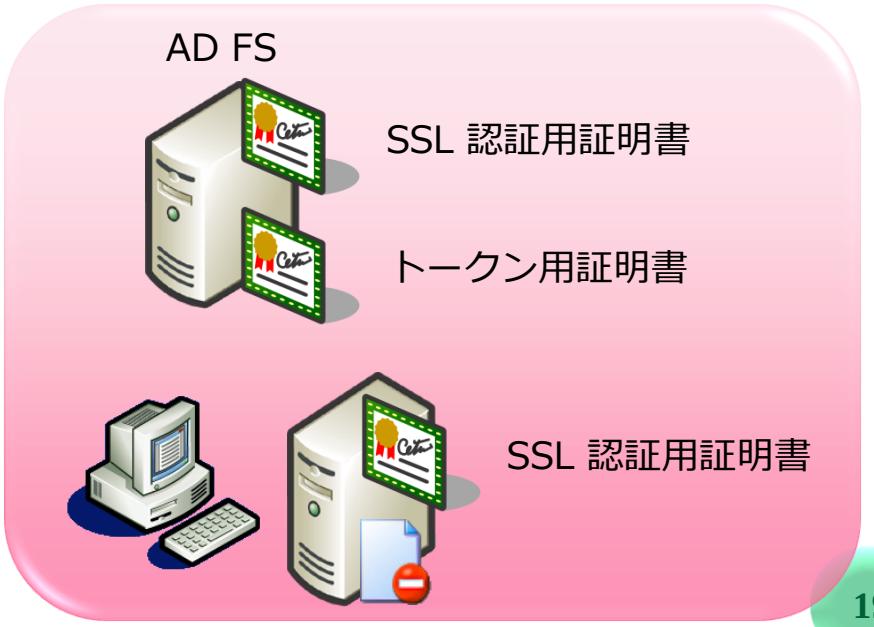
項番	作業内容
1	両方のパートナーで AD FS の役割を追加
2	ADFS 用 Web サイトの SSL 設定
3	SSL 用証明書のエクスポート
4	アカウントパートナーの AD FS で信頼ポリシーの設定
5	リソースパートナーの AD FS で信頼ポリシーの設定

証明書の実装詳細

- 証明書を信頼されたルート証明機関に登録 (CA/自己署名)
- AD FS が使用する証明書
  - SSL サーバー認証用証明書
  - セキュリティトークン用証明書
- AD RMS が使用する証明書
  - SSL サーバー認証用証明書

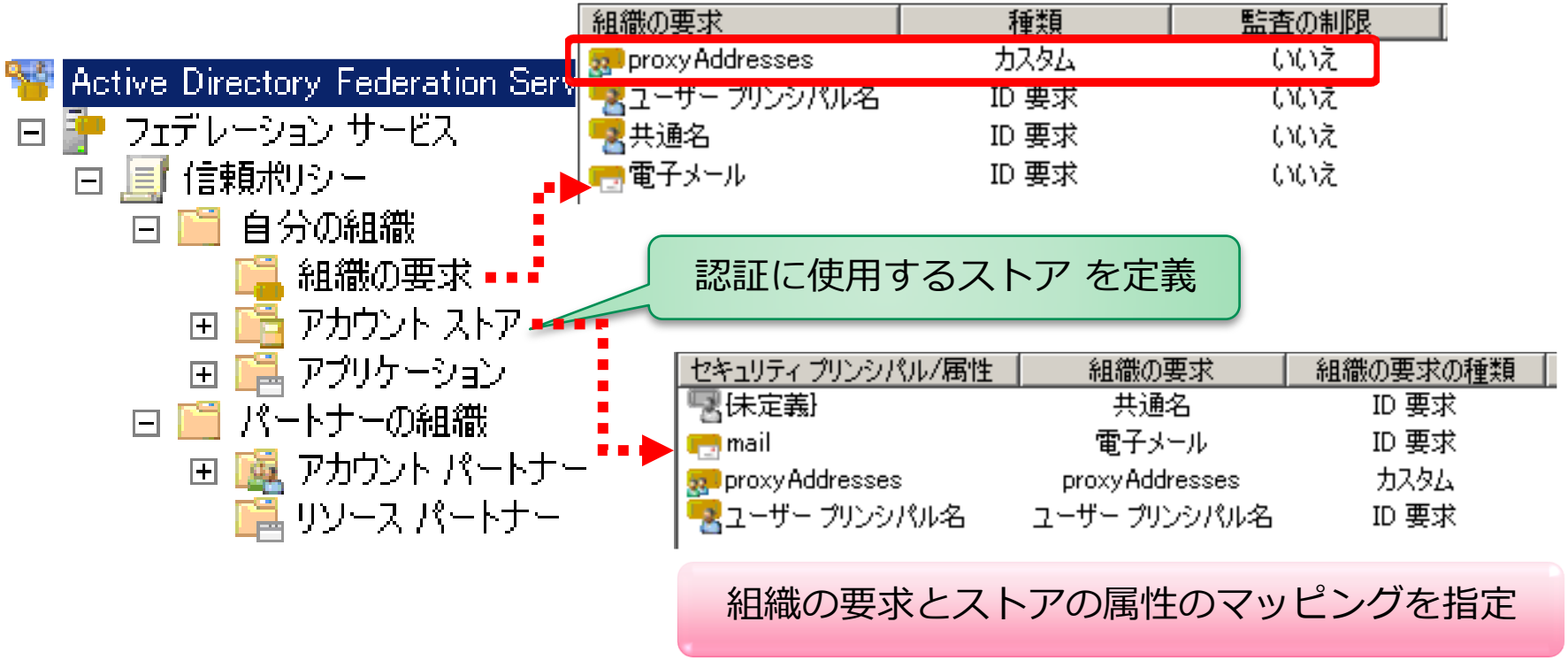


アカウント パートナー

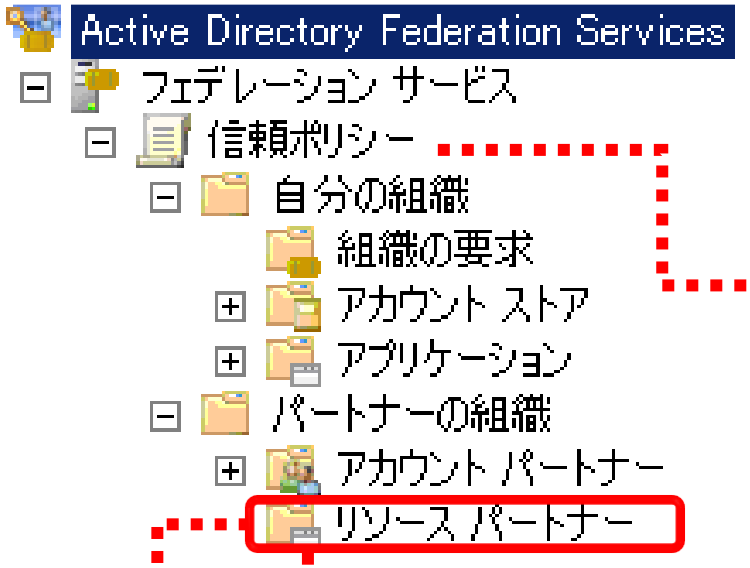


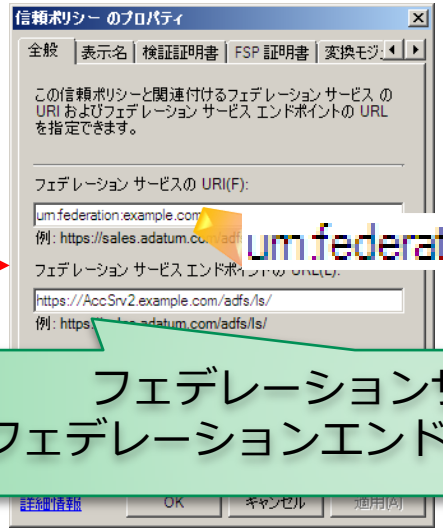
リソース パートナー

アカウントパートナーの AD FS 設定 (1)



アカウントパートナーの AD FS 設定 (2)





um:federation:example.com.

フェデレーションサービスの URI と
フェデレーションエンドポイントの URL を定義

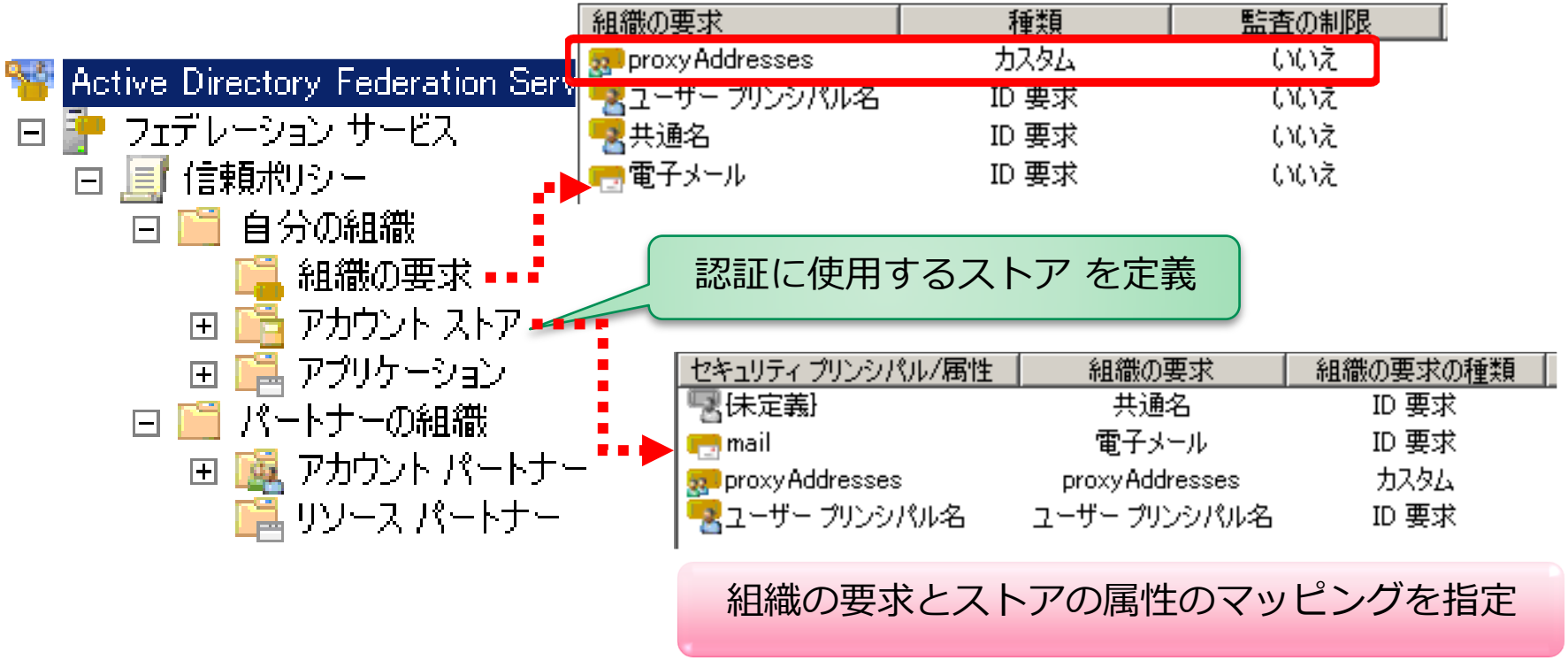
um:federation:rmsdom.com.

組織の要求	組織の要求の種類	出力方向の要求へのマップ	出力方向の要求の種類	監査の制限
{undefined}	{undefined}	共通名	ID 要求	いいえ
proxyAddresses	カスタム	proxyAddresses	カスタム	いいえ
ユーザー プリンシパル名	ID 要求	ユーザー プリンシパル名	ID 要求	いいえ
電子メール	ID 要求	電子メール	ID 要求	いいえ

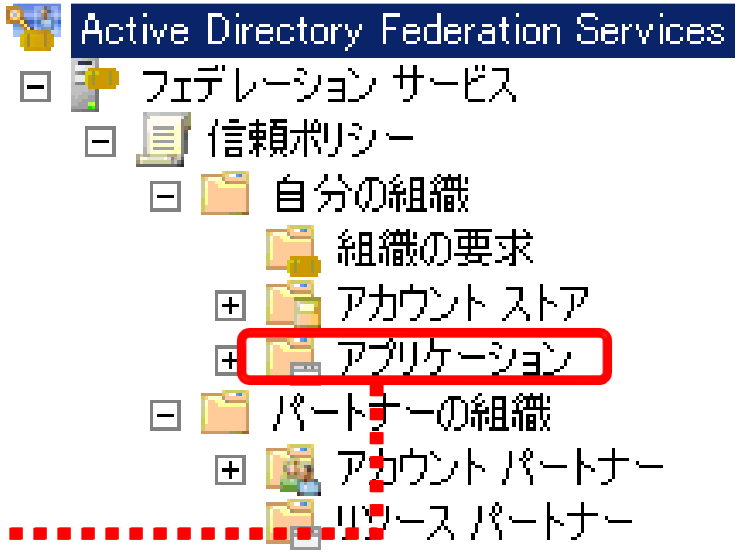
リソースパートナー組織 (ドメイン) の指定
と要求のマッピングを指定

フェデレーションサービスの URI と
フェデレーションエンドポイントの URL を定義

リソースパートナーの AD FS 設定 (1)



リソースパートナーの AD FS 設定 (2)



AD RMS と通信を行うために必要な
設定 (アプリケーション) を 2 つ作成

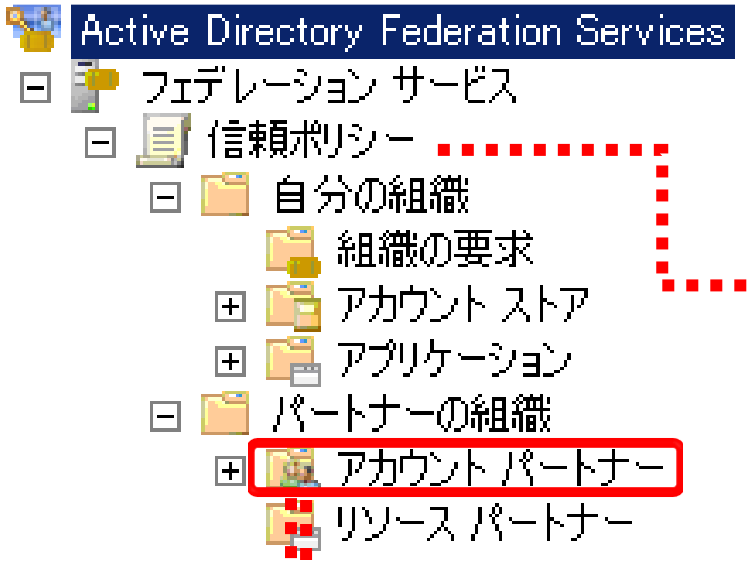
RMS 証明書

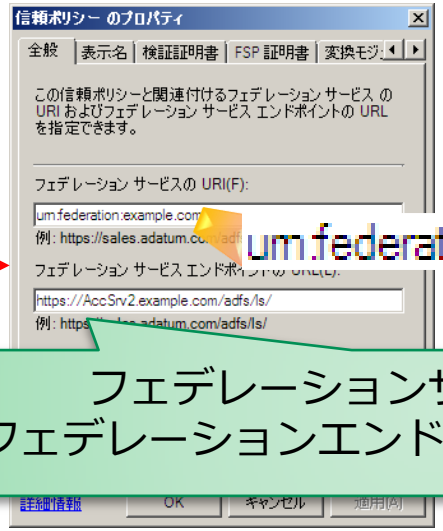
- UPN と電子メールの要求を使用する
  要求に対応するアプリケーション
- https://RMS/_wmcs/certificationexternal/

RMS ライセンス

- UPN と電子メールの要求を使用する
  要求に対応するアプリケーション
- https://RMS/_wmcs/licensingexternal/

リソースパートナーの AD FS 設定 (3)





um:federation:example.com.

フェデレーションサービスの URI と
フェデレーションエンドポイントの URL を定義

um:federation:rmsdom.com.

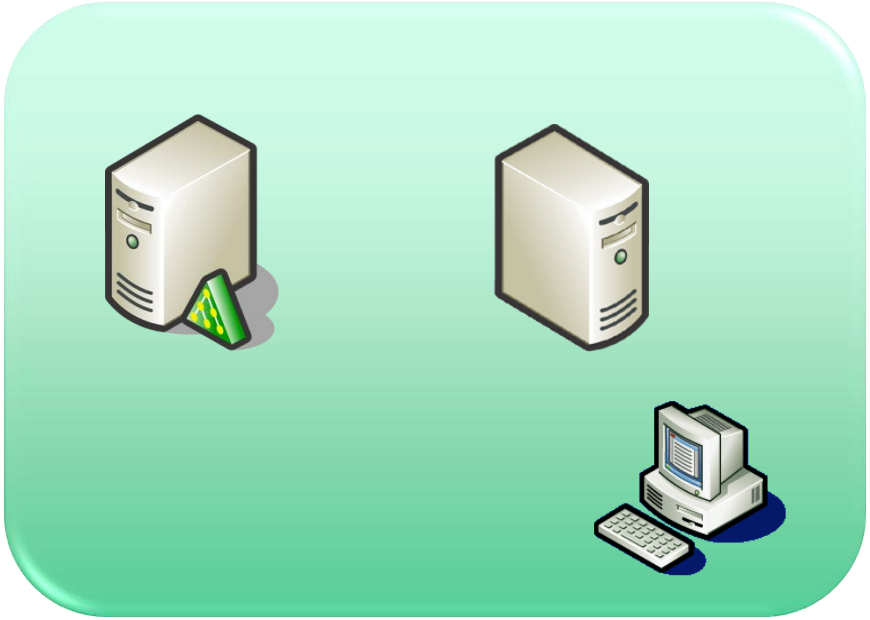
組織の要求	組織の要求の種類	出力方向の要求へのマップ	出力方向の要求の種類	監査の制限
{undefined}	{undefined}	共通名	ID 要求	いいえ
proxyAddresses	カスタム	proxyAddresses	カスタム	いいえ
ユーザー プリンシパル名	ID 要求	ユーザー プリンシパル名	ID 要求	いいえ
電子メール	ID 要求	電子メール	ID 要求	いいえ

リソースパートナー組織 (ドメイン) の指定
と要求のマッピングを指定

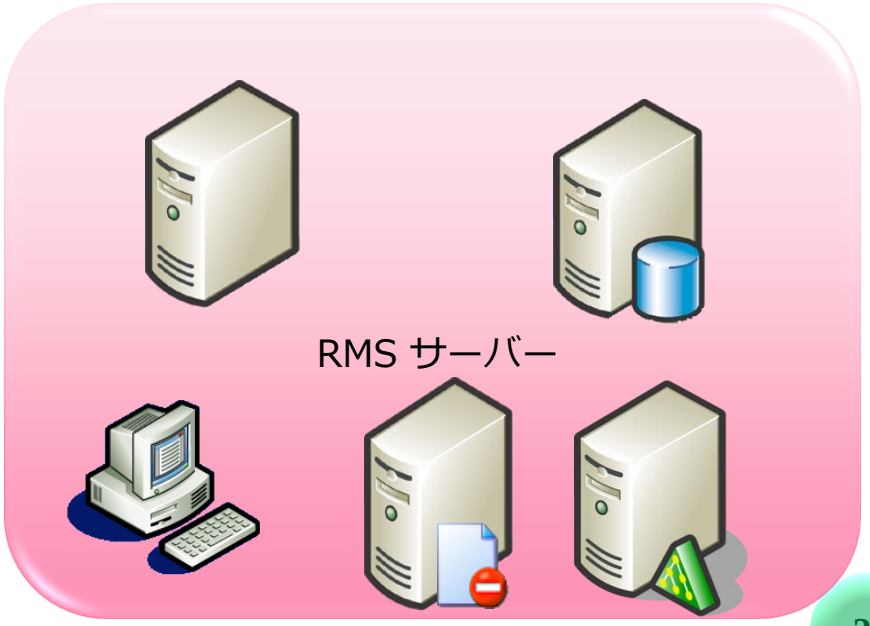
フェデレーションサービスの URI と
フェデレーションエンドポイントの URL を定義

④ AD RMS の実装と AD FS と連携させるための設定

- リソースパートナーで AD RMS の役割を追加
- フェデレーション用 URL の設定
- サーバー証明書の実装と SSL の設定



アカウント パートナー

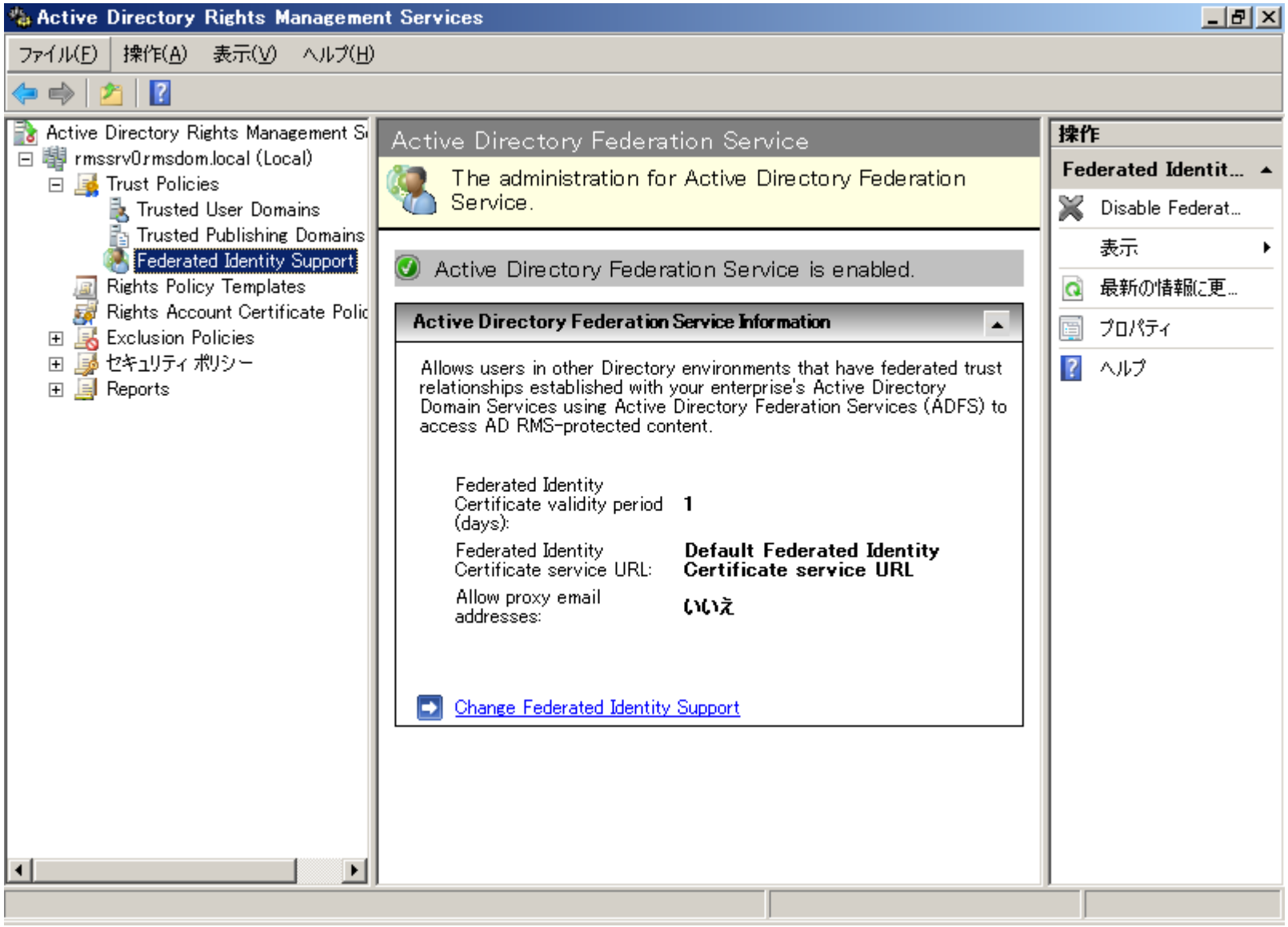


リソース パートナー

④ AD RMS の実装と AD FS と連携させるための設定(詳細設定)

項番	作業内容
1	サーバー証明書を AD RMS へインポート
2	AD RMS 管理者アカウントに監査権限を追加
3	AD RMS の役割を追加
4	AD RMS クラスタ URL の追加
5	AD RMS 用 Web サイトで web.config ファイルの編集
6	AD RMS サーバーで ID フェデレーションを有効

AD RMSサーバーの設定
ID フェデレーションの設定



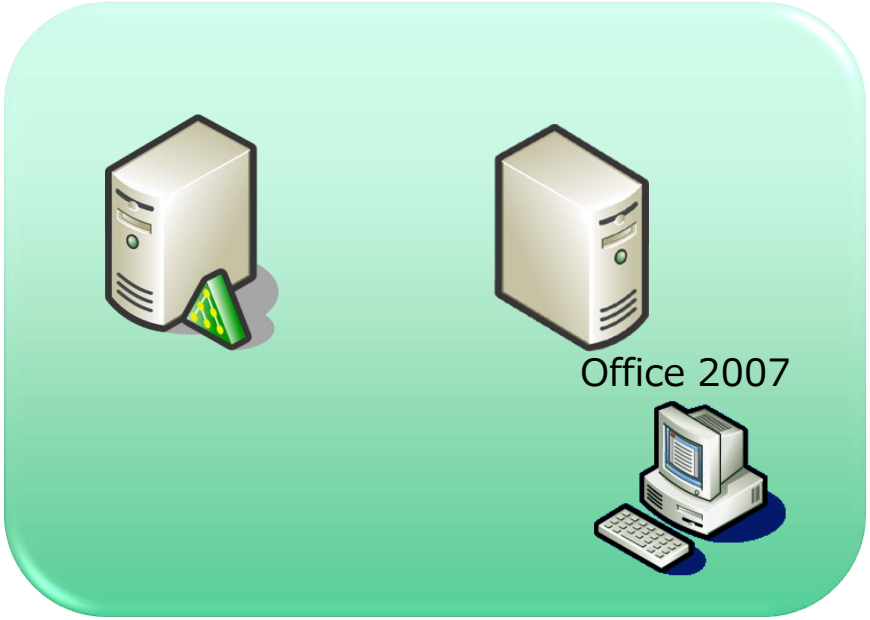
AD RMSサーバーの設定

WEB.CONFIGの設定

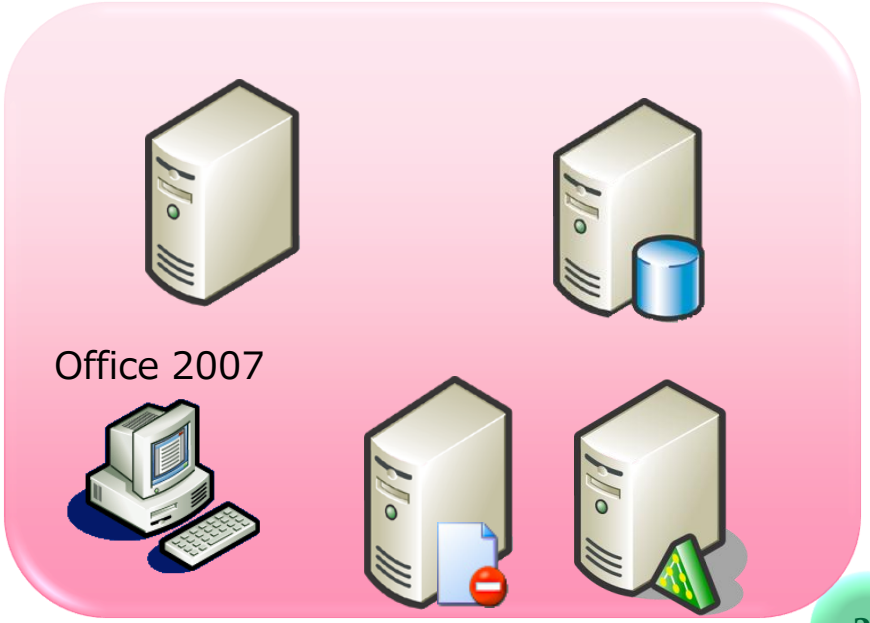
- 外部からのライセンス / 証明書用アクセスが可能になるよう、以下のディレクトリにあるファイルの <returnurl> タグ内の URL を書き換える
  - C:¥inetpub¥wwwroot¥_wmcs¥certificationexternal¥web.config
  - C:¥inetpub¥wwwroot¥_wmcs¥licensingexternal¥web.config
- <usettp/> タグの削除

⑤ クライアントの設定

- クライアントにサーバー証明書をルート証明機関に追加
- Office アプリケーションからアクセス



アカウント パートナー



リソース パートナー

⑤ クライアントの設定(詳細設定)

項番	作業内容
1	Microsoft Office Professional 2007 のインストール
2	RM クライアントのインストール (オプション)
3	サーバー証明書の追加
4	AD RMS サーバーのクラスタ URL を IE のイントラネットゾーンに追加

さらに…

WSS(MOSS)と組み合わせます

AD FS+AD RMS 環境での WSS の実装手順

① リソースパートナーにWSSを実装

② WSS サーバーに RMS クライアントをインストール

③ WSS サーバーで AD RMS を利用するための設定

④ WSS サーバーで AD FS を利用するための設定

まとめ

Windows Server 2008 の AD FS は
RMSやSharePointとの組み合わせが
可能になることで、ノンコーディングで
テクノロジが利用できる

Windows Server 2008 の AD FS は
RMSやSharePointとの組み合わせにより
組織間の利用が可能に