

# WS-FederationとPKI

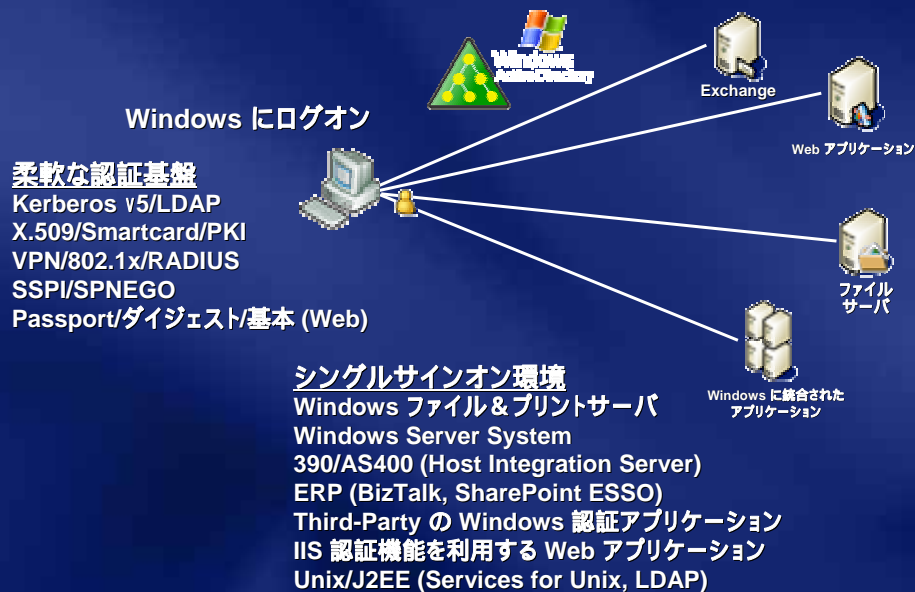
マイクロソフト株式会社  
公共インダストリー統括本部  
テクノロジーソリューション部  
テクニカルアーキテクト  
鈴木 章太郎  
shosuz@microsoft.com

## Agenda

- 現在のシステムが抱える課題
- WS-Federationの内容
- Active Directory フェデレーションサービス (ADFS)
  - コンポーネント
  - アーキテクチャ
  - 利用シナリオ
- 事例紹介: CWID2005-同盟国間インターオペラビリティ実証実験
- まとめ

## 現在のシステムが抱える課題

## 現在の Windows ベースの認証基盤





## PKIと認証基盤のお客様の声

- PKIに対するネガティブな声
  - ID、パスワードで十分だよ
  - PKIは運用が大変だ、コストに見合わない、等
- PKIに対するポジティブな声
  - 強固なセキュリティ対策が必要と考えおり、PKIを選択したい
  - 2 Factor Authenticationとして、PKIを利用したスマートカード認証を社内に取り入れる、等
- 認証基盤に対するお客様の期待
  - 今選択している認証方法はどこまで使えるの？
  - 違った認証基盤との運用性はあるの？
  - 簡単に導入/運用できるのかな？

## これから何が必要になるか？

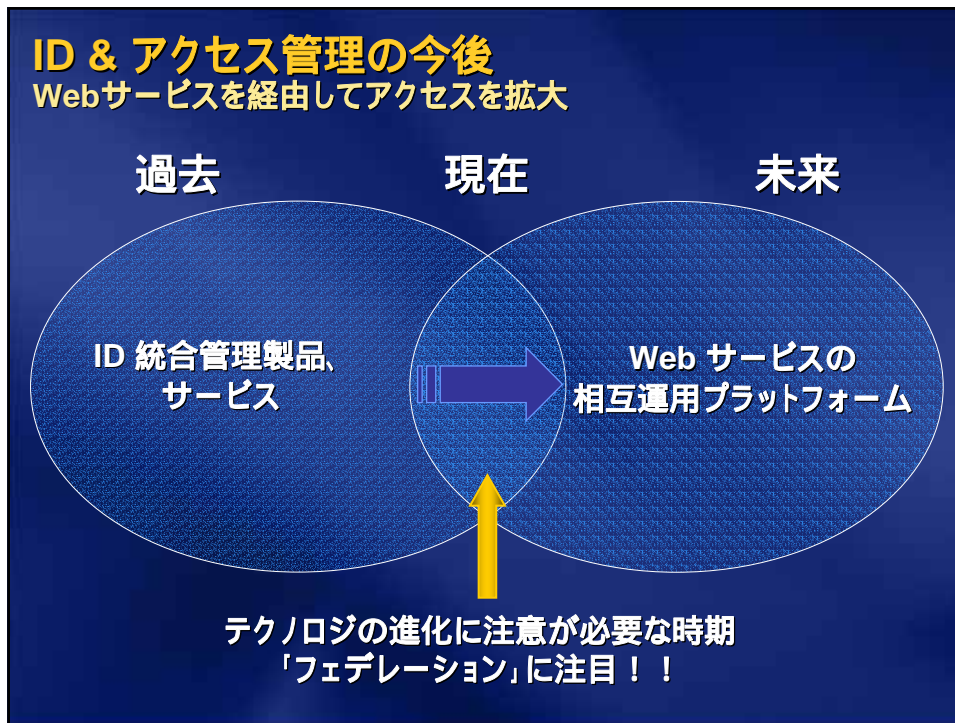
- 分散ID環境における認証や承認の基盤
  - セキュリティ、部門、組織、プラットフォーム等  
多種多様な境界を越えられるもの
  - Internet を経由した認証の技術
- インターオペラビリティ (相互接続性)
- 標準的な技術やプロセス
  
- マイクロソフト的に言うと
  - いつでもどこでもどんなデバイスでも・・・に加えて
  - 1度のログオンでどこにでもセキュアにアクセス
  - 低い導入コストとシンプルな運用、高いバリュー

これからは フェデレーション

## ID & アクセス管理の今後

Webサービスを経由してアクセスを拡大



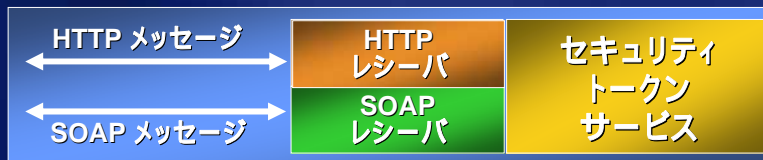


## WS-Federationの内容

## WS-Federation

Cross-organization, multi-vendor interoperability

- BEA, IBM, Microsoft, RSA, VeriSign が提唱
  - Web サービス フェデレーション言語
    - セキュリティで隔てられた領域間の連合とセキュリティトークンの交換を可能にするためのメッセージを定義
- パッシブ (Browser) リクエストプロファイル ADFS v1
  - Web ブラウザをサポート - https
- アクティブ (Smart) リクエスト プロファイル ADFS v2
  - SOAP 対応クライアント、Web サービス - SOAP



## ADFS による ID フェデレーションの仕組み

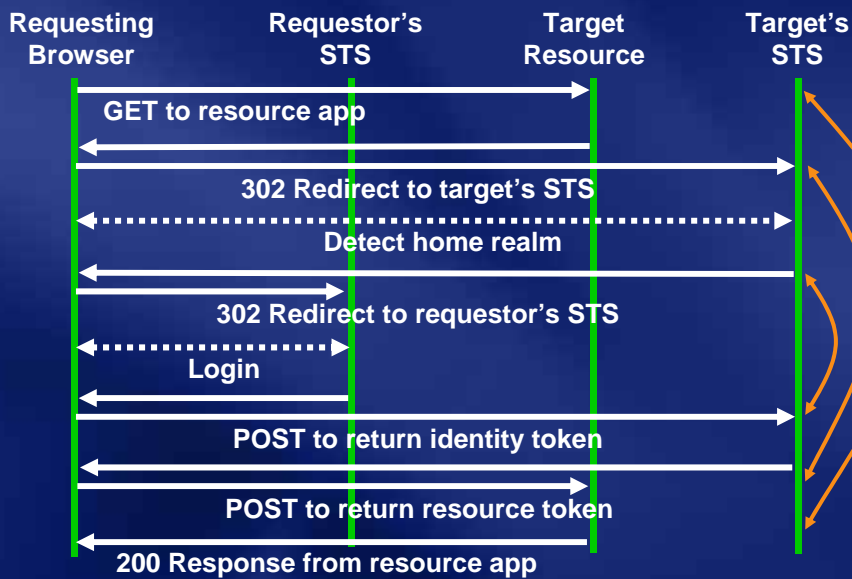


## パッシブリクエストプロファイルとは？

ADFSv1 in W2K03 R2でサポート

- ブラウザ(Passive)クライアントのための WS-FederationとWS-Trustの結合
  - 暗黙のうちにリダイレクションに従ってポリシーに惹きつけられる
  - 暗黙のうちにHTTPメッセージによりトークンを取得
- 認証にはHTTPSを要求
  - クライアントは“proof of possession”を提供できない
  - トークンは再試行を試みる
- 限定された (時間ベースの) トークンキャッシング

## サンプルフロー: パッシブクライアント



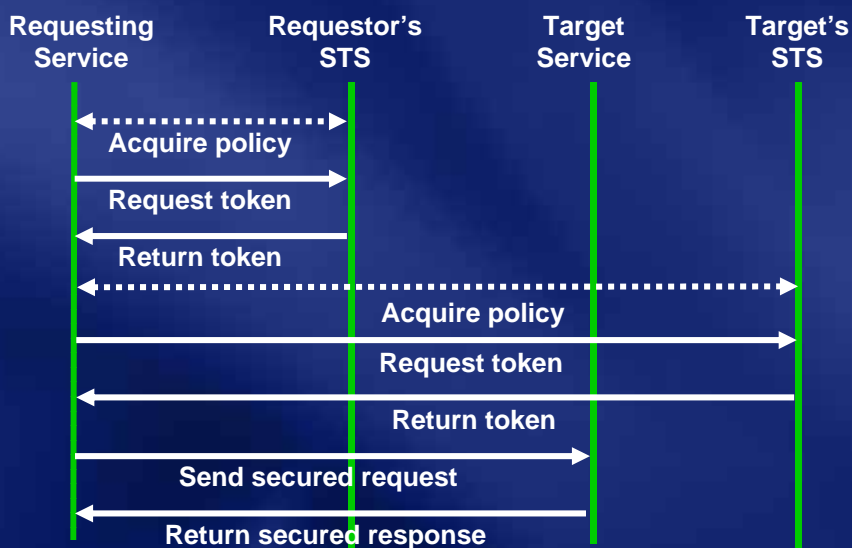
## アクティブリクエストプロファイル

将来のADFSにてリリース予定

- SOAP/XML (Active)クライアントのためのWS-FederationとWS-Trustの結合
  - 明示的にポリシーに従いトークンの要求を決定
  - 明示的にSOAPメッセージによりトークンを要求
- 全てのリクエストに対する強い認証
  - クライアントは“proof of possession”を提供可能
- デリゲーションをサポート
  - クライアントは自分が使用するためトークンを提供可能
- クライアント側でリッチなトークンキャッシングを可能にする
  - セキュリティリスクなしで向上されたパフォーマンス

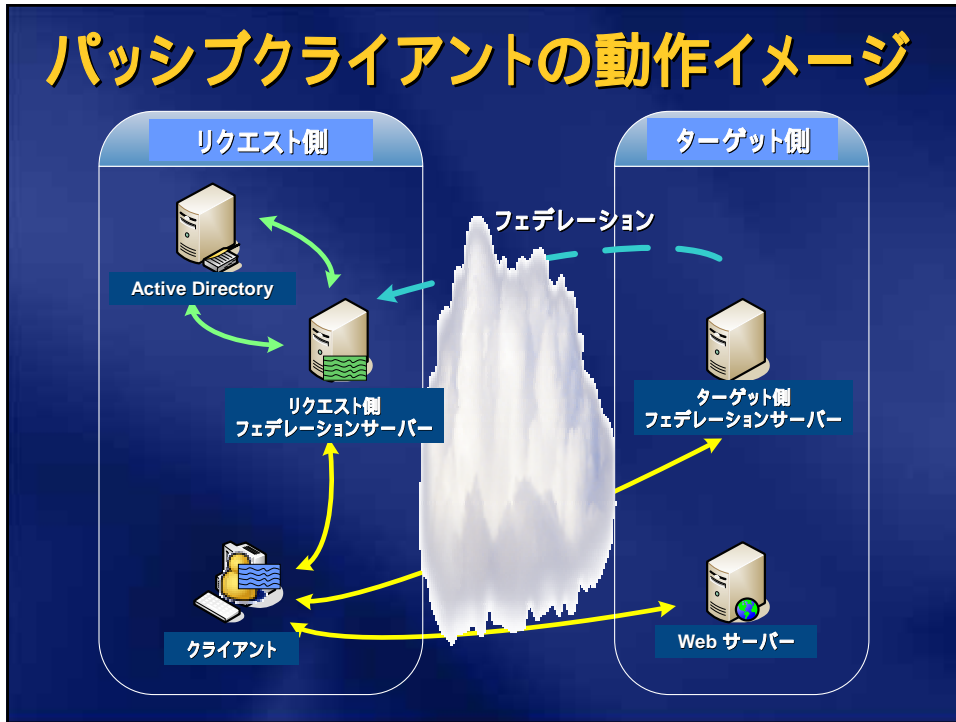
## サンプルフロー: アクティブクライアント

WS-Policy によってクライアントトークンのリクエストをルーティングする

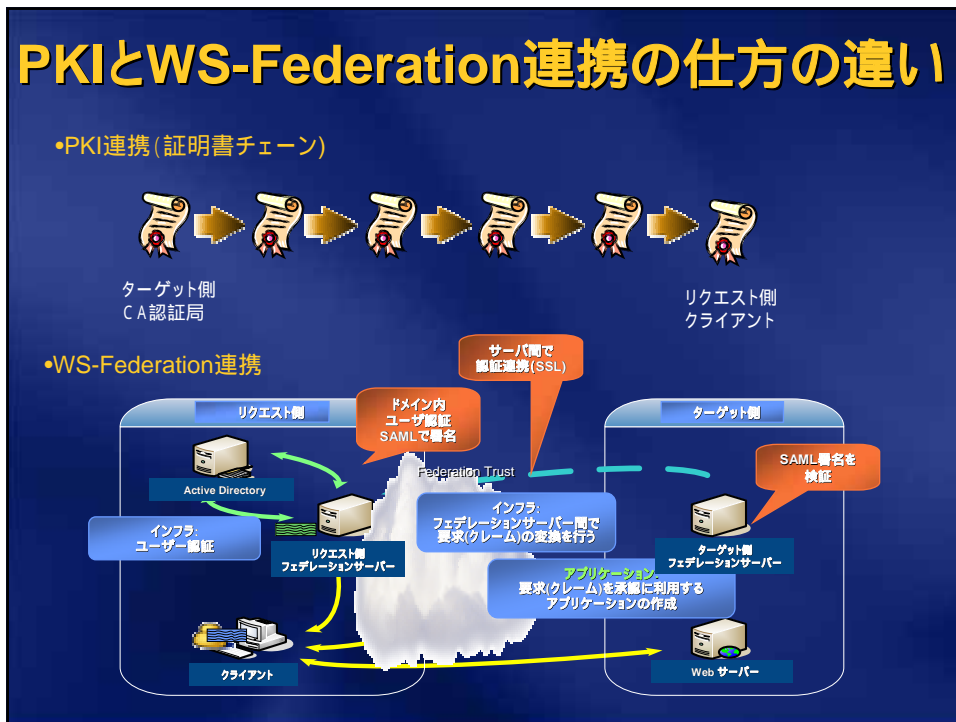




# パッシブクライアントの動作イメージ



# PKIとWS-Federation連携の仕方の違い



Ac

# マイクロソフトのWebサービスプロダクト ロードマップ

## WS-\* Web サービスアーキテクチャ

Webサービスとしての分散アプリケーションをデザイン  
するためのサービス指向アーキテクチャ

## Active Directory フェデレーションサービス

ID管理とアクセス管理のためのインフラストラクチャ

## Windows Communication Foundation

(WCF, 旧名: "Indigo")

ComposableなWebサービスから分散アプリケーションを構築するためのランタイム環境

## InfoCards

Windows用のID選択カード - ユーザのデジタルIDの  
安全な管理



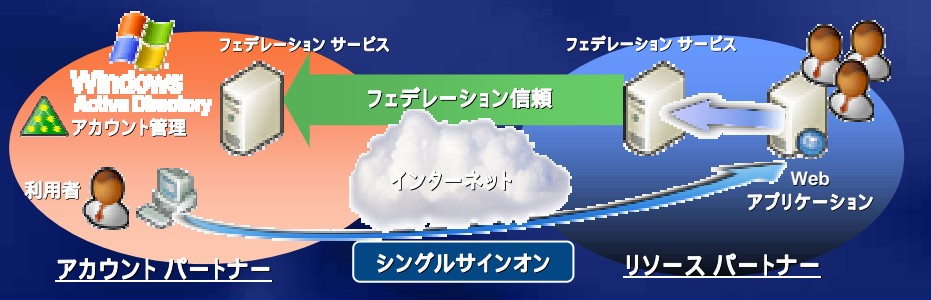
## Active Directory フェデレーション サービス (ADFS)

(Windows Server 2003 R2 にて提供開始)

(本セッションは Beta 2 相当をベースにしています)

## Active Directory フェデレーション サービス

- フォレストを越えたアクセス環境の提供
  - お客様/パートナー/サプライヤ/社員も認証可能・・・
- Web サービス フェデレーション (WS-\*) に準拠
- コスト削減とセキュリティ向上の両立
  - ユーザアカウントは所属する組織内でのみ管理
  - リソース提供者はフェデレーションサーバを呼び出し



## ADFS アーキテクチャ

### Active Directory (2K, 2K3, ADAM)

- ユーザーを認証
- 属性情報を管理

### フェデレーションサービス (FS)

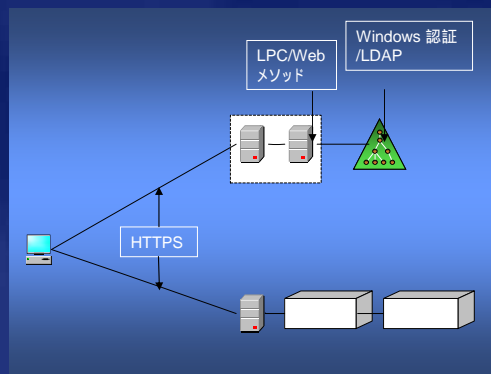
- STS (security token service)
- セキュリティトークンを発行
- クレームを生成
  - ユーザーアカウントの属性を記述
- フェデレーション信頼ポリシーを管理

### FS プロキシ (FS-P)

- クライアントのトークンリクエストをプロキシ
- ブラウザクライアントに UI を提供

### Web SSO エージェント

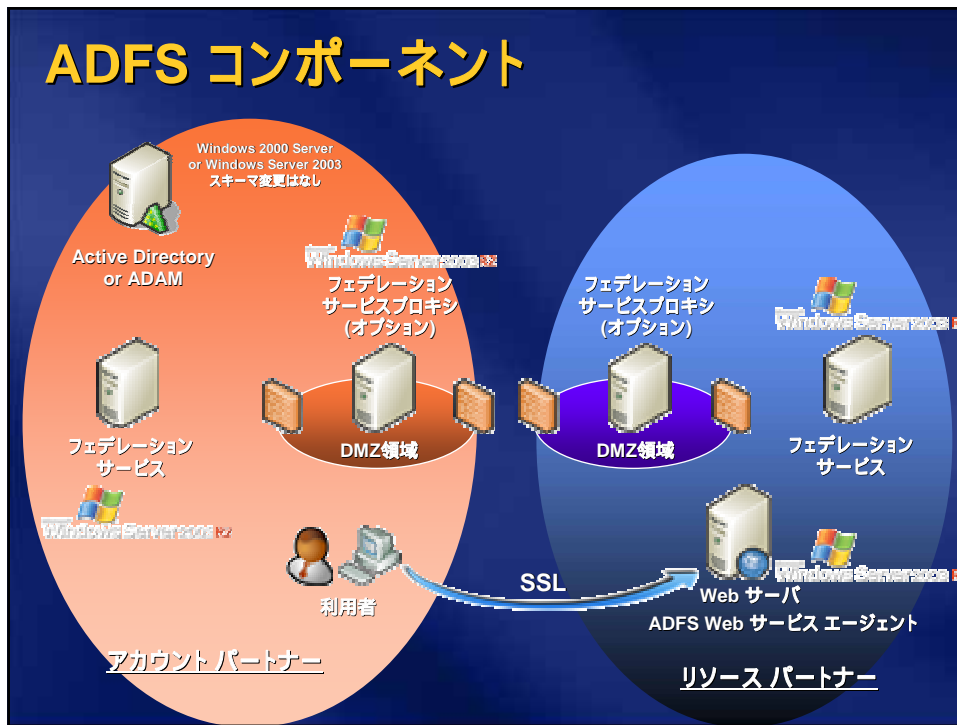
- ユーザー認証を施行
- ユーザーの認可用コンテキストを生成





### アプリケーション

- 認可方式
  - NT の偽装モデル & ACL
  - ASP.NET IsInRole()
  - 承認マネージャの RBAC と統合
    - ロールベースのアクセス制御
  - ASP.NET のクレーム対応 API

# ADFS コンポーネント



# フェデレーション サービス (FS)

**フェデレーション サービス**

- ASP.NET v2 ホストサービス
  - Windows Server 2003 R2 の IIS v6 で稼動
- フェデレーション ポリシーの管理
  - FS 間の信頼関係を確立
  - 証明書のコピーで署名されたトークンを用いて信頼関係を確立
  - フェデレーション領域間のトークン/ クレームの種類、共有ネームスペースを定義
- セキュリティトークンの生成
  - 要求 (クレーム) へのマッピング
  - セキュリティトークン サービス (STS)
  - Kerberos や LDAP サーバから情報取得
    - Active Directory or ADAM
    - LDAP で AD/ADAM からユーザーの属性情報を取得し、クレームを生成
  - Security Assertion Markup Language (SAML) トークンを生成
  - アプリケーションの認可ロジックにあわせてクレームの内容を変換
  - 署名した SAML セキュリティトークンを生成し、FS-P へ送信
  - “ユーザー SSO” クッキーを生成し、FS-P へ送信
- ユーザ認証
  - フォーム認証の際、ID/パスワードを LDAP バインドで確認

## フェデレーション サービス プロキシ (FS-P)



フェデレーション  
サービスプロキシ

- ✦ ASP.NET v2 ホストサービス
  - Windows Server 2003 R2 の IIS v6 で稼動
- ✦ FS の機能の一部を代理
  - セキュリティトークン処理
    - クライアント用のセキュリティトークンを FS から要求
    - Web ブラウザに POST リクエストを送信し、トークンをフェデレーションサーバーヘルパーティング
  - フェデレーションサーバーへのフォワーディング
  - ブラウザに“ユーザ SSO”クッキーを提供
- ✦ ユーザー認証
  - ホームレルムの解決とフォーム認証用の UI を提供
  - 統合 Windows 認証、SSL クライアント認証によるユーザー認証
  - ブラウザに“ユーザ SSO”クッキーを提供
- ✦ 必須ではない
  - FS のみでフェデレーション環境を構築可能
  - ネットワークの都合に応じて配置
  - システム構築の柔軟性向上

## ADFS Webサーバー SSO エージェント

- ✦ Windows Server 2003 R2 の IIS v6 で稼動
  - IIS 管理画面にタブ追加
- ✦ 2つのコンポーネント
  - ADFS Web Agent ISAPI Extensions
  - ADFS Web Agent Authentication Service
- ✦ ISAPI エクステンション (Windows Server 2003 R2 の IISv6 用)
  - ユーザー認証
    - URL GET リクエストを取り出し、認証されていないクライアントをローカルシステムにリダイレクト
    - “Web サーバー SSO”クッキーをブラウザに提供
- ✦ Windows サービス
  - ユーザーを認可
    - 乗装用の NT トークンを生成 (AD ユーザーのみ)
- ✦ マネージド Web モジュール
  - セキュリティトークンの処理
    - セキュリティトークンをチェックし、トークン内のクレームを解読
  - ユーザーを認可
    - クレームから ASP.NET の GenericPrincipal コンテキストを生成し、IsInRole() をサポート
    - アプリケーションが解釈できるクレームを提供



ADFS  
Webサーバー  
SSO エージェント

## ADFS のメッセージフロー



1. 利用者は A-Corp のポータル経由で B-Corp の注文処理アプリケーションにアクセス
2. 利用者のアクセスをA-CorpのSTSにリダイレクト
  - 既に Active Directory で認証済みの場合、A-CorpのSTS は統合 Windows 認証 によって透過的にユーザーを認証
3. A-Corp のSTS はフェデレーションクレームを含む SAML セキュリティトークンを発行し、利用者はB-Corp のSTSに提示
4. B-Corp のSTSはアプリケーションクレームを含む SAML セキュリティトークンを発行し、利用者はB-Corpの注文処理アプリケーションにアクセス

## ADFS 対応アプリケーションの開発

- アセンブリを用いた容易な API 開発
  - 認証済みユーザー (署名済みトークン) の確認
    - System.Web.Security.SingleSignOn.Identity
  - クレームからユーザー情報を抽出
    - System.Web.Security.SingleSignOn.Authorization
- 認可ロジックの開発
  - 既存の ASP.NET アプリケーションを使用
    - クレームから GenericPrincipal 生成、IsInRole() でロールを決定
  - 承認マネージャ (AzMan)
    - クレームから AzMan コンテキストを生成し、AzMan API をコールしてロールを解決

## ADFS による生産性の向上

### 管理者



- 一つの ID で全ての Web へアクセス、エクストラネット用のディレクトリ管理は不要
- ポリシー管理の集中化
- AD、ADAM、承認マネージャ、IIS を統合
- 単一パスワード = ヘルプデスクコールの減少
- 標準技術に基づくクロスプラットフォームの相互運用性

### 開発者



- エクストラネット用の Web アプリケーションに強固な認証サービスを提供
- 承認マネージャ、ASP.NET ロールと統合し、アプリケーション開発からユーザー管理を分離
- 従来 of 認可方式 (NT トークンベース) を標準サポート

### 利用者



- Windows ログオンのみで、組織内および外部のリソースへシングルサインオン: 一つのパスワードを記憶するのみ
- 社内システムへ容易にリモートアクセス (VPN は不要)
- アカウント作成の待ち時間を解消

## ADFS によるセキュリティとコンプライアンスの向上

### セキュリティ



- フェデレーション経由のエクストラネットアクセスを自動的に停止: アカウントの残存を防止
- 証明書ベースでトークンを検証
- 必要なファイアウォール/ポートを制限 (HTTP 443)
- SSL/TLS で全てのコンポーネント間通信を防御

### 規制

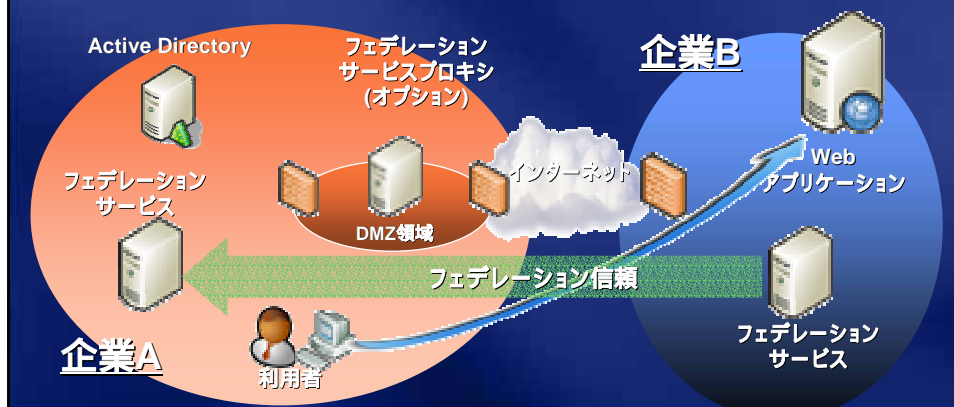


- 境界を挟んだデータ共有を木目細かく制御: アクセスに必要なデータのみを共有
- 全てのインバウンド/アウトバウンドアクセスリクエストをロギングし、否認防止の問題を解決
- WS-Federation によりフェデレーションのアクセス制御を正規化



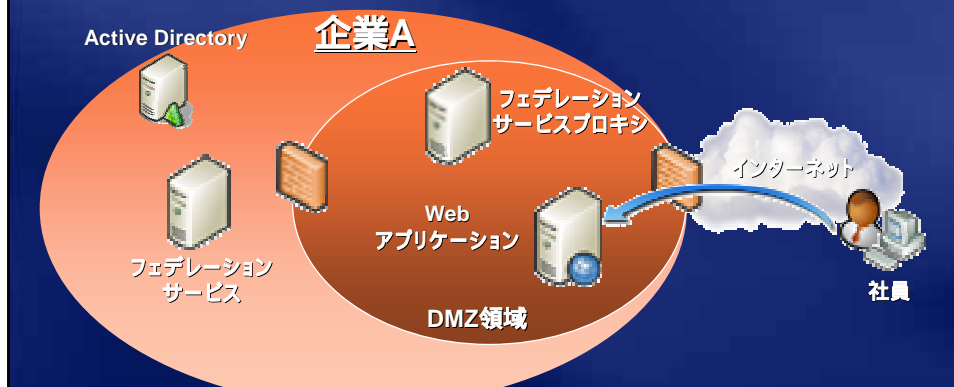
## シナリオ (1) ~ B2B:企業間での利用 ~

- (例) パートナー企業へのアプリケーション公開
  - トラベル、出店式社内購買、カタログ・・・
  - ASP, アウトソーシング, 業務提携後・・・



## シナリオ (2) ~ B2E:SSO ~

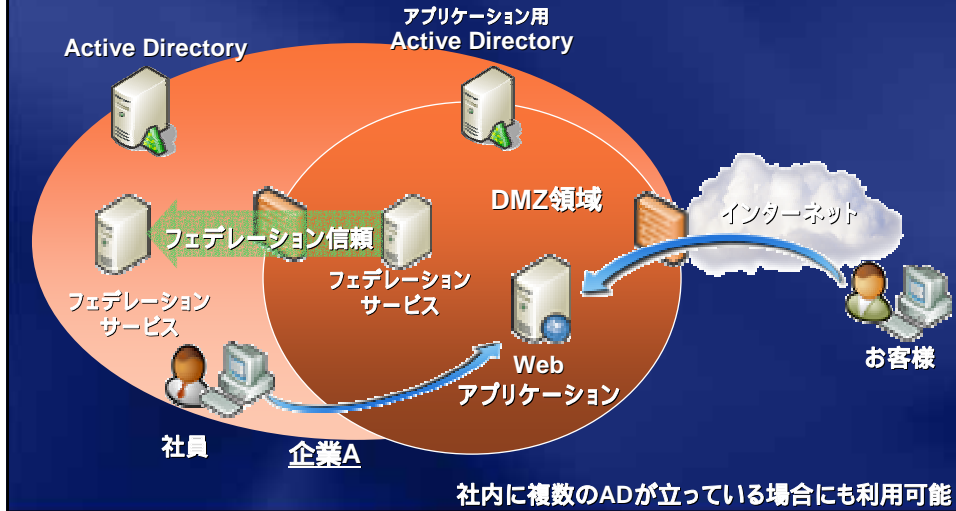
- インターネットに社員用アプリケーションを公開
  - VPN なしで 社内 Active Directory の有効活用
  - シングルサインオン環境の提供





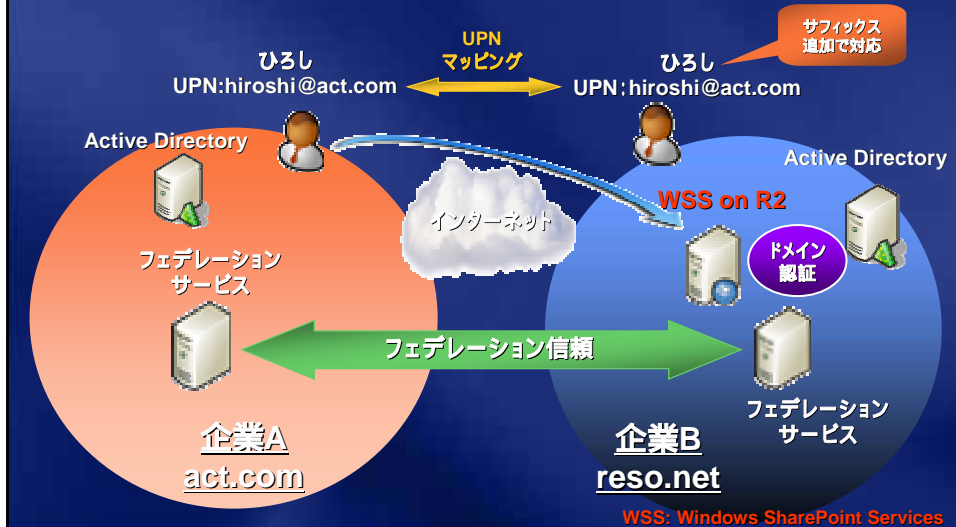
### シナリオ (3) ~ B2C & E + BU2BU ~

- (例) お客様用アプリケーションを社員も利用



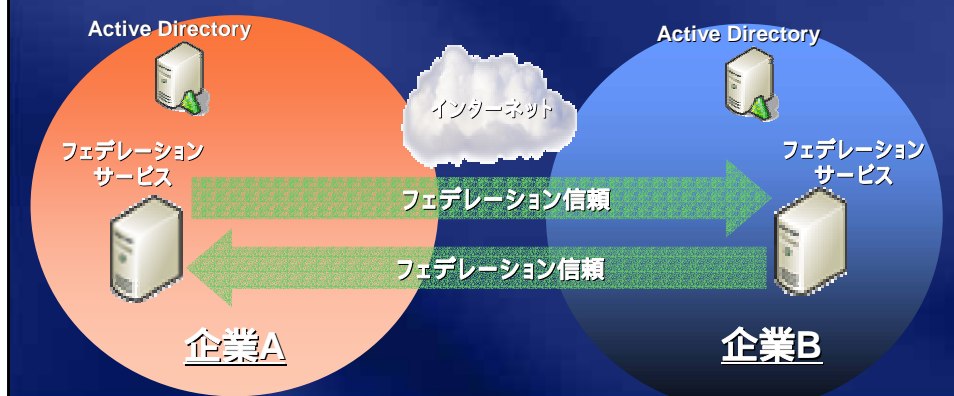
### シナリオ (4) ~ シャドーアカウント ~

- ドメイン認証 + フェデレーションで SSO



## シナリオ (5) ~ 双方向フェデレーション ~

- 企業A も 企業B もアカウントパートナーでありリソースパートナー でもある
- フェデレーション サービス プロキシ の利用も可



## ADFS 設計と設定のポイント

- 証明書 (Certificate)
  - 安全なフェデレーション環境を構築するために
  - パートナーとのフェデレーション信頼
  - 暗号化通信 (SSL)
  - サーバ認証用 (SSL)
  - FS-P によるクライアント認証用 (SSL)
  - FS トークン署名用 (FSが正しいことの証明)
- ツールと設定のポイント
  - [Active Directory フェデレーション サービス] ツール
  - フェデレーション環境の構成管理
    - ポリシー、要求 (クレーム) の定義、マッピング設定

## AD フェデレーションサービスの画面

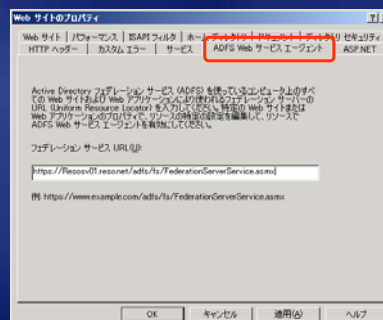
The screenshot displays the Active Directory Federation Services (ADFS) management console. Two dialog boxes are highlighted with callouts:

- フェデレーション管理画面** (Federation Management Screen): Shows the main configuration interface for the ADFS service.
- 信頼ポリシーファイルの指定 トークン署名用の証明書設定** (Specify Trust Policy File and Certificate Settings for Token Signing): A dialog box for selecting a trust policy file (e.g., C:\ADFS\TrustPolicy.xml) and a token signing certificate.
- フェデレーション サービス (& プロキシ) の URL 設定** (Federation Service (& Proxy) URL Settings): A dialog box for setting the federation service URL (e.g., urn:federation:HIMicheal) and the proxy URL (e.g., https://Acts01.act.com/adfs/ls/clientlogon.aspx).

UI は変更の可能性がありますので、ご注意ください。

## ADFS Web サービス エージェント

### ● IIS のプロパティを自動拡張



- 要求に対応するアプリケーション
  - (Claims aware application)
- 従来のアプリケーション
  - (Windows NT token application)

## SSOエージェントのパートナーソリューション Centrify: ADFSへのダイレクトコントロール

- **ダイレクトコントロールWebシングルサインオンエージェントにより、Apache, WebSphere, WebLogic, JBoss, またはTomcat. にホストされたアプリケーションに対して、ADFSを通じた認証が可能となる**



ダイレクトコントロールWeb SSO エージェントは、マイクロソフトの Webプラットフォームで無いプラットフォーム上で、IIS上でマイクロソフトのWeb SSOエージェントが動作するのと同様のタスクを実行する

- **利点:**
  - より古く、更に複雑なWeb SSO製品との連携等、ヘテロジニアスな環境での統合ID管理が可能となる
  - 実装が簡単: 単純にWeb SSOエージェントをインストールするだけ
  - ロールベースのアクセス手段の中央での集中的な管理、簡素化された運用、法的な要求事項に対して拡張された監査/レポート
  - シームレスなADFSとの統合: 今までどおりと同じ設定管理ツールを使用できる; Active Directoryには何の変更も無い; ユーザの使用感は今までどおりで何も変わらない
- **早期評価版:** <http://www.centrify.com/adfs>



## 事例紹介: 同盟国間のインターオペラビリティ実証実験 – CWID2005

The Coalition Warrior Interoperability Demonstration (CWID) is a US programme with participation by Australia, Canada, NATO (SHAPE), New Zealand, and the United Kingdom. Additional participants in 2005 included South Korea and some of the 'partners for peace' nations.

## 背景

### ラムズフェルド国防長官:

- 米国とオーストラリア軍隊が一体化した行動を行うことが重要。21世紀の脅威がどのようなものか私達はすでに経験している。“スピードと機敏さ、そしてコネクティビティ”が何よりも重要であることは明白である。

ラムズフェルド国防長官とオーストラリア国防相との会議内容:

2003年11月19日

[http://www.defenselink.mil/news/Nov2003/n11192003\\_200311198.html](http://www.defenselink.mil/news/Nov2003/n11192003_200311198.html)

### 国防総省のブリーフィング:

一時的に、または特殊な任務のために結成された同盟国に共通の目的を与えることは困難。

- 一部だけがネットワーク化されたシステムに慣れている軍隊を統合するには、不慣れな部分については機能を解除し、豊富な技術の代わりとして利用できるブリッジ機能を挿入する必要がある。

出典 - 国防総省のブリーフィング 2004年1月

<http://www.teammultimedia.com/catalog/pb.html#pb-order>

## 現場からの要求

- 堅牢な指揮統制ネットワークを構築するには、柔軟なデジタルマルチサービス通信機能が必要
- 隊員、戦略立案者、サポートスタッフのためにオンデマンドで情報を収集、処理、保存、配信、管理することができるような、グローバルな相互接続機能が必要



## パターン分析 イラクのケース

- イラク戦後の報告会では、同盟国間での情報共有に関する問題が明らかになった
- IEDのパターン分析がこの一例
- 第4歩兵師団 (ID) が、リンクパターン分析情報に基づき、サダムフセインを拘束
- コメント: 「SIPRNETアカウントを持っていなければ、情報入手に時間がかかり、問題が発生しただろう」



## CWID – 会長のコメント

**CWID は、米国の戦闘部隊と国際社会が同盟国間インタオペラビリティを迅速に、そしてタイムリーに強化するために、C4ISR ソリューションについて調査することを目的として各国共同により設立された。**

command, control, communications,  
computers, intelligence, surveillance,  
and reconnaissance





## JWID / CWIDの目的

以下の改善を実証

- 複数の情報ドメインでの情報共有
- 帯域幅の限られた運用環境での共同計画
- 情報の配信－諜報、監視、偵察 (ISR)
- 指揮任務の保証
- 状況把握機能

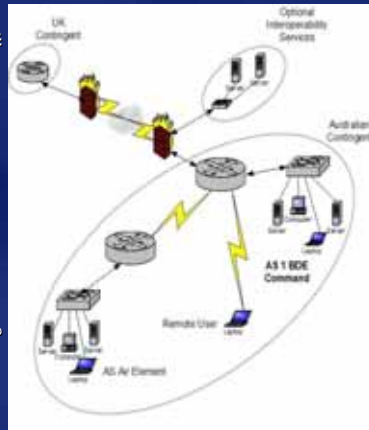


## JWID 2004 マイクロソフト担当分野

- 段階的なアプローチ – 最低でも2～3年を計画
- 第1段階の目標
  - メッセージングおよびコラボレーションサービス提供のためのマイクロソフト技術とサードパーティ製品を紹介
- 参加国
  - 米国、英国、カナダ、オーストラリア
- 第1段階の内容
  - メッセージング
    - Eメール(非公式)
    - ACP133、P772に準拠したミタリーメール(公式)
    - チャット(リアルタイム通信)
  - 以下を利用したドキュメント指向のコラボレーション環境 (Microsoft Office SharePoint Portal Server 2003)
    - 同盟国は同じ作業空間で共同文書を作成

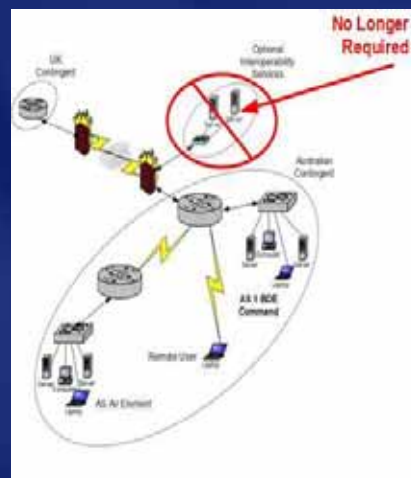
## JWID 2004のハイレベルアーキテクチャ

- 参加各国は独自のActive Directory ネットワークをホスティングした。これには標準のITインフラストラクチャ、アプリケーション、特定のC2ツールセットから成るJWIDコアサービスが含まれている。
- 主として以下のホスティングを行う同盟国間共有環境を作成した。
  - Microsoft Office Live Communications Server 2003 (LCS)
  - Windows SharePoint Services.
- 環境間の信頼関係は確立されていなかった。
- クライアントは共有リソースにアクセスする際、第2のセキュリティレイヤに直面した (意図的な設定)



## 第1段階 – 機能はするが最適ではない

- CWID 2005 – マイクロソフトのソフトウェア開発によって、Active Directory Federated Services (ADFS)などの新技术を用いたモデルを拡張
  - データの冗長性を回避
  - 全データは所有者が管理
  - 身元情報はローカルに管理し、同盟国間で信頼性を確保
  - ADFSは(必要に応じて)アクセス権を即座に無効化できる



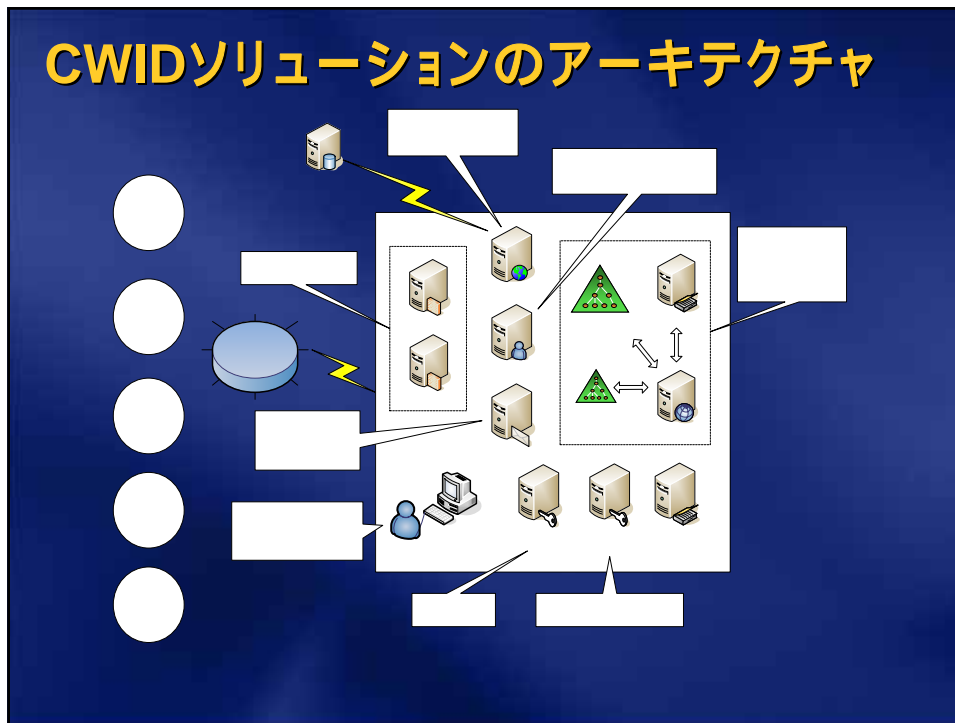


## CWID 2005 マイクロソフト担当分野

- 連合セキュリティアーキテクチャを使用した、統合コラボレーションおよびミリタリーメールの提供
- JWID 2004の試行を基に構築 (第2段階)
- マイクロソフトの新たな目標
  - 複数の情報ドメインでの情報共有
  - ミッションの再確認
  - コラボレイティブな計画(帯域幅が限られた状況下での)
  - 状況把握 – (追跡情報の開示)
- 参加国および機関
  - オーストラリア、カナダ、ニュージーランド、英国、米国、NATO加盟国(オブザーバ)
  - FBI、HLS、FEMA
  - PSEPC(カナダ)
  - 英国警視庁/ MACA

## ソリューションの概要

- Active Directory Federation Services
  - デジタル身元情報と権限情報を、セキュリティ境界を越えて共有
  - 簡略化されたシングルサインオンソリューション(標準ベース)に対応
- 統合コラボレーション
  - エンタープライズチャット、VoIP、ビデオ、アプリケーション共有およびポータルサービス
- エンタープライズドキュメント&レコード管理
  - 現行のデスクトップソリューションを英国国防省向けに導入
    - Office 2003、Sharepoint、レコード管理(Meridio)、ワークフロー(K2.NET)
- Windows権限管理サービス – 制限処理機能を強化
- ミリタリーメール
  - Microsoft Exchange Server 2003 - DMS
  - ACP133 & P772 - ACP145 Gatewayを含む



## 新しいアプローチ – 連携

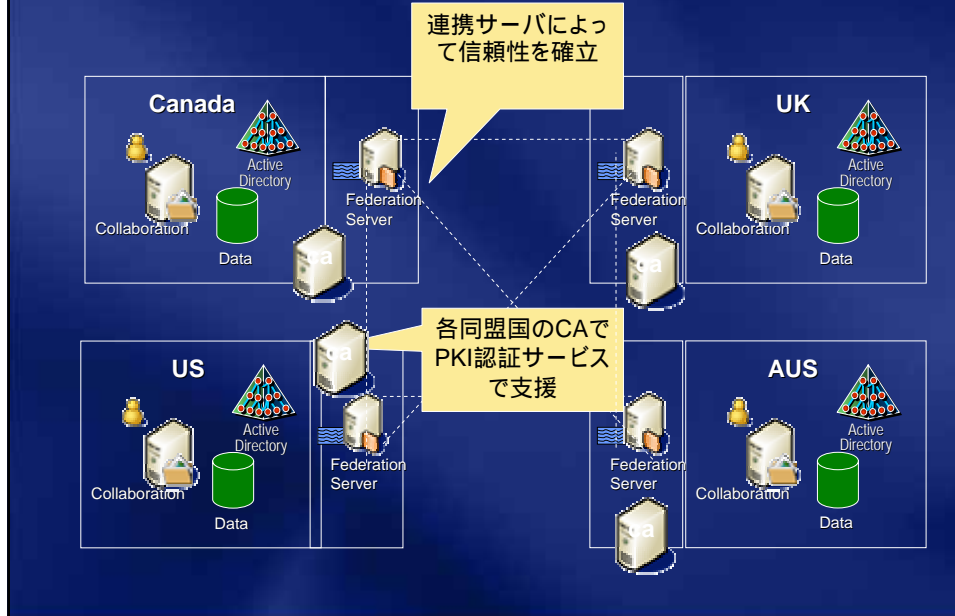
- **連携** – 同盟国間の信頼に基づく関係に対する、以下のような新しいアプローチ
  - 当初Active Directory証明書を使用して、クレーム概念を導入し、PKIを活用
  - クレーム: アクセス権限付与のための認証ステートメント
  - 安全性が向上 – 「証明書ではない」クレームをネットワーク上で安全にやり取りすることで、ユーザの身元情報のハイジャックのリスクを軽減することができる
- **利点**
  - 隊員
    - 同盟国間でのシングルサインオンに対する大きな前進
    - 外国のパートナーが提供するサービスに対する依存度を低くする
  - 組織
    - 管理オーバーヘッドの軽減
    - 連合体制の確立と解除に要する時間を短縮
- **参照**
  - Trans Atlantic Secure Gateway Initiative  
(大西洋横断セキュア ゲートウェイ イニシアチブ)  
<http://www.tscp.org/>

Canada

US

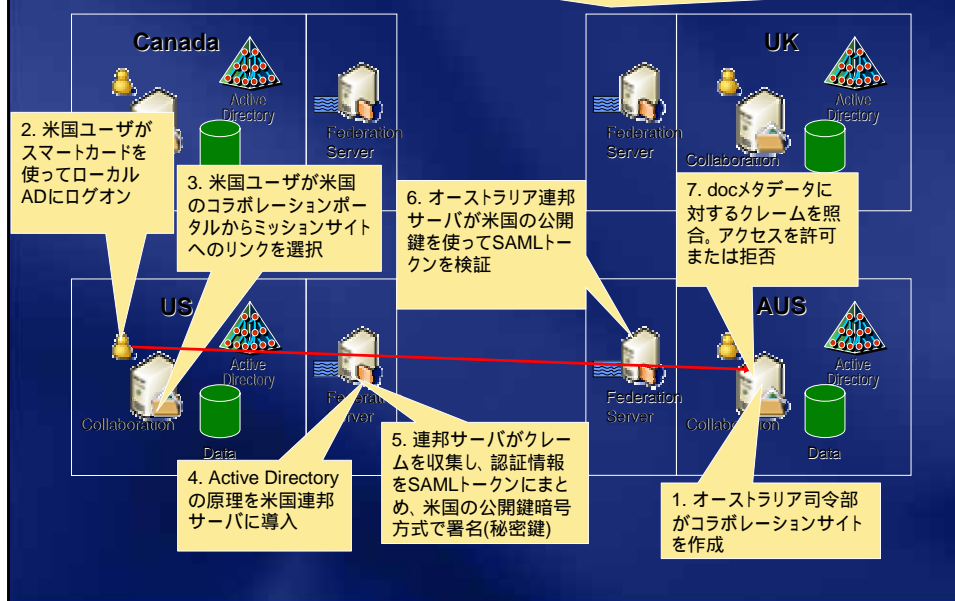
Australia

## CWID 2005連携セキュリティモデル

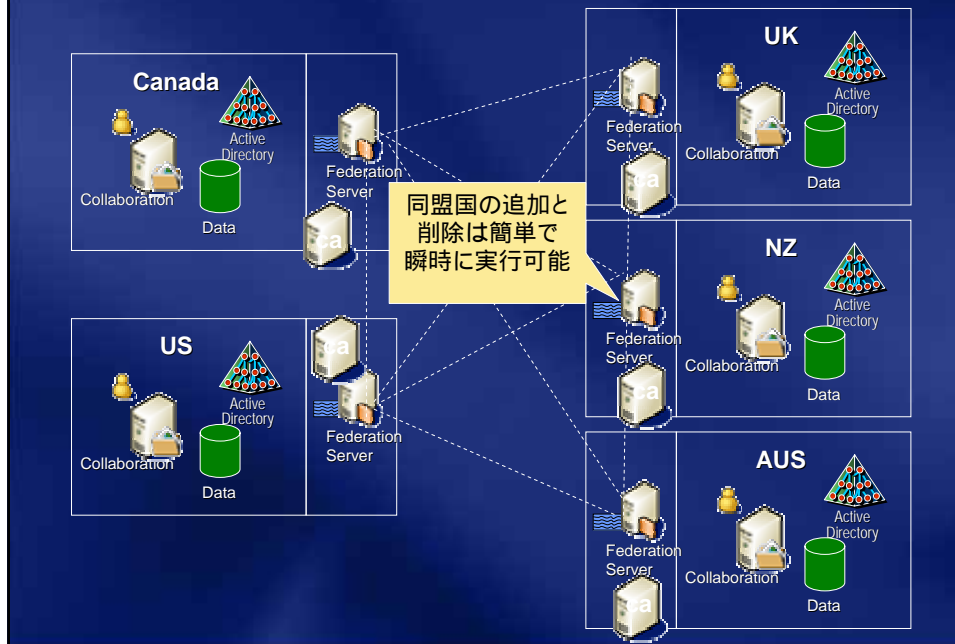


## CWID 2005連携セキュリティモデル

シナリオ: 米国司令部はオーストラリア司令部に安全性導入のミッションを委任



## CWID 2005による提案 – 連携セキュリティモデル



## 統合コラボレーション

- リアルタイムコミュニケーション
  - Microsoft Live Communications Server 2005 (チャット)
    - 連携アーキテクチャ
    - 高い可用性とスケーラビリティ (拡張性)
      - (15k ~ 100kのアクティブユーザ)
    - オプションのトランスポート暗号化 (チャット、データ、音声、ビデオ)
    - Microsoft SQL Server データベースに対するオプションのログと監査
    - Active Directoryに統合
  - 複数名による音声/ビデオ会議
    - ミッション計画
    - VoIP
  - ビデオストリーミング (未定)
    - CNNニュースの配信
    - 司令官のブリーフィング



## 統合コラボレーション(続き)

- Parlano – 継続的なチャット
  - 仮想会議室機能
- SharePointポータルサービス
  - ミッションに関する共有情報(司令官の意図説明)
  - 指令系統の分散化を支援(状況把握機能の向上)
  - OODA  
(Observe, Orient, Decide & Act: 観察、判断、決定、行動)  
の流れを加速
  - ユーザが使い慣れた一連のツールに完全に統合
  - Webサービスによってアプリケーションとデータを迅速に、そして簡単に公開 – (Webパーツ)
- DCTS  
(Defense Collaboration Tool Set:  
防衛コラボレーションツールセット)
  - 有効と思われる次世代技術



## まとめ

### まとめ = Key Takeaways

Active Directory フェデレーション サービス は  
ID の利用と管理の両方の課題を解決

組織のネットワークを超えて  
Windows で管理する ID を利用することが可能

既存Webアプリケーションとのインターオペラビリティも  
パートナーソリューション等を活用して確保可能

**Microsoft**  
*Your potential. Our passion.™*

© 2005 Microsoft Corporation. All rights reserved.  
This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.