

もうひとつの

IDENTITY LIFECYCLE MANAGER

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、お手柔らかかにお願いします

今日のおはなし

8月21-24日に開催された
“Microsoft Tech・Ed 2007”で
国井が担当したテクニカルセッションのうち

- T2-307
Active Directory と Microsoft Identity Lifecycle
Manager 2007 による ID 管理
についてサイドストーリーを紹介します。

ILM 2007 のコンポーネント

Microsoft Identity Integration Server 2003 (SP2)

- ディレクトリの同期
- ユーザープロビジョニング
- パスワード同期



Certificate Lifecycle Manager

- 証明書のライフサイクル管理
- スマートカードのライフサイクル管理



MIIS : 管理エージェントが標準で用意されているシステム

- ディレクトリ
 - Active Directory / NT4 ドメイン
 - ADAM
 - Sun Directory Server(Netscape / iPlanet / SunONE) 4.12 / 4.13 / 5.0 / 5.1 / 5.2
 - Netscape Directory Server 4.1 / 6.11
 - Novell e Directory 8.6.2 / 8.7 / 8.7.3
 - IBM Tivoli Directory Server 4.1 / 5.1 / 5.2
on Windows Server 2003 or Windows 2000 Server
- メインフレーム
 - IBM Resource Access Control Facility
 - Computer Associates eTrust ACF2
 - Computer Associates eTrust Top Secret
- グループウェア & 業務システム
 - Exchange 2000 / 2003 GAL (※ 2007 GAL は 2007 年末対応予定)
 - Exchange 5.5
 - Lotus Notes 5.0 / 6.x / 7.x
 - SAP R/3 4.7 / mySAP 2004
- データベース
 - SQL Server 7.0 / 2000 / 2005
 - Oracle 8i / 9i / 10g
 - IBM DB2 7 / 8.1 on Windows Server 2003 , 8.1 on Linux, 5.1.5 on OS /400
- ファイル
 - DSML (Directory Services Markup Language) 2.0
 - LDAP Directory Interchange Format (LDIF)
 - カンマ区切りテキストファイル (CSV)
 - 固定長テキスト ファイル
 - 属性と値の組 (Attribute-Value Pair) のテキストファイル
- その他
 - MA SDK で任意のシステムとの同期を実装可能
 - OpenLDAP 2.x 用 MA が サード パーティにより無償提供

今までの証明書管理

証明書サービス + Active Directory で運用

証明書テンプレートによる発行ポリシーの定義

- 有効期間
- アクセス許可 (エンタープライズ CA の場合) etc...

ライフサイクルに関する考慮がない

- 登録→更新→取消
- 取消・回復

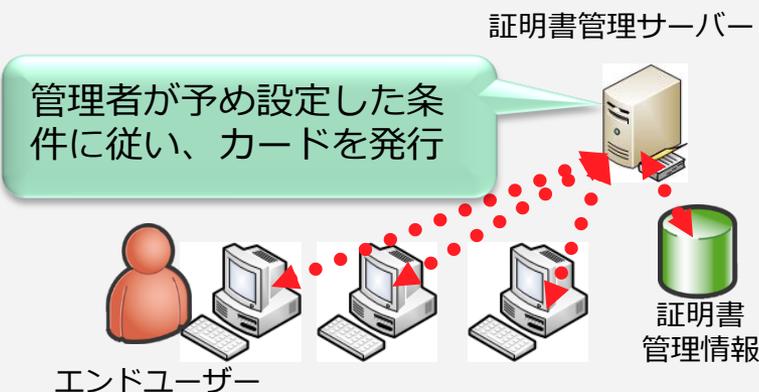
登録方法に関する柔軟性

- Web ページから手動
- グループポリシーから自動

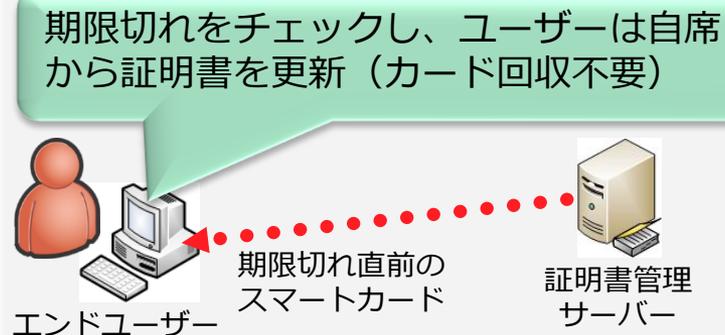
証明書管理のあるべき姿

- 確実な証明書 / スマートカードのライフサイクル管理
- 証明書管理システムに統合され、設定が容易な申請ベースの証明書 / スマートカード発行
 - カード発行に必要な一連の事務作業を自動化
 - 発行状況は、発行システムよりリアルタイムに集計・管理
- スマートカードの一括発行機能
 - 数百～数千（場合によってはそれ以上）の一括発行にかかる、管理者の負担を軽減
- IT 基盤との統合による、優れた運用管理性
 - カード発行や申請者・承認者のロール管理を認証基盤に統合

カード発行



セルフサービスによる更新



CLM の証明書・スマートカード管理機能

証明書とスマートカードの統一された管理機能を提供

- プロファイルテンプレートと呼ばれる定義情報を元に動作

以下のタスクに対して、ポリシーで定義可能なワークフローを提供

- 登録 / 更新 / アップデート
- 回復 / カードの交換
- 取り消し
- 退職 / スマートカードの無効化
- テンポラリ / 複製スマートカードの発行
- スマートカードのカスタマイズ (印刷機能)

監査と詳細なレポート機能

- CSV 形式での出力、グラフ及び表形式での印刷が可能

センター集中型のシナリオとセルフサービスシナリオのサポート

- スマートカードの一括発行
- クライアントサイドでの PIN 変更

既存のインフラストラクチャへの統合

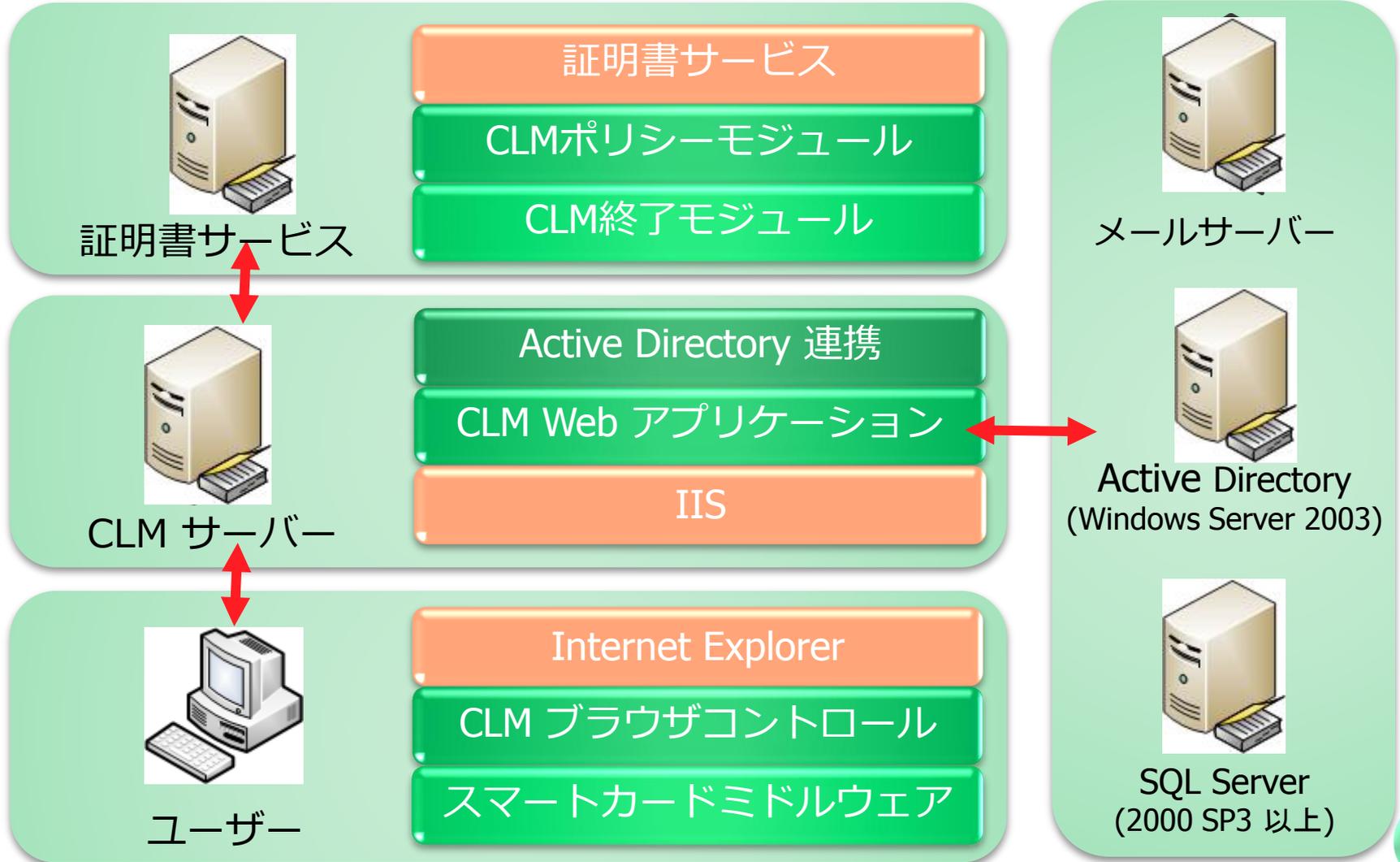
- Active Directory と Windows Certificate Services

CLM アーキテクチャ

物理アーキテクチャ

論理アーキテクチャ

その他のサービス



プロフィール テンプレート

ポリシー テンプレート

証明書テンプレート (1つ以上)

管理ポリシー (1つ以上)

登録

- ワークフロー
- セルフサービス
- データコレクション

回復

- ワークフロー
- セルフサービス
- データコレクション

Etc. ,

- ワークフロー
- セルフサービス
- データコレクション

スマートカード 詳細情報 (オプション)

- 証明書のライフサイクルで必要な管理ポリシーを定義 (登録、回復、廃止など)
- 管理タスクを定義するコンポーネント (1つ以上存在)
- Active Directory に格納され、組織内の全 CLM サーバーで共有
- 構成情報
 - 1つ以上の証明書テンプレート
 - 複数の証明書の管理に必要な情報
 - ワークフロー ポリシー

証明書の発行

- セルフサービスによる発行

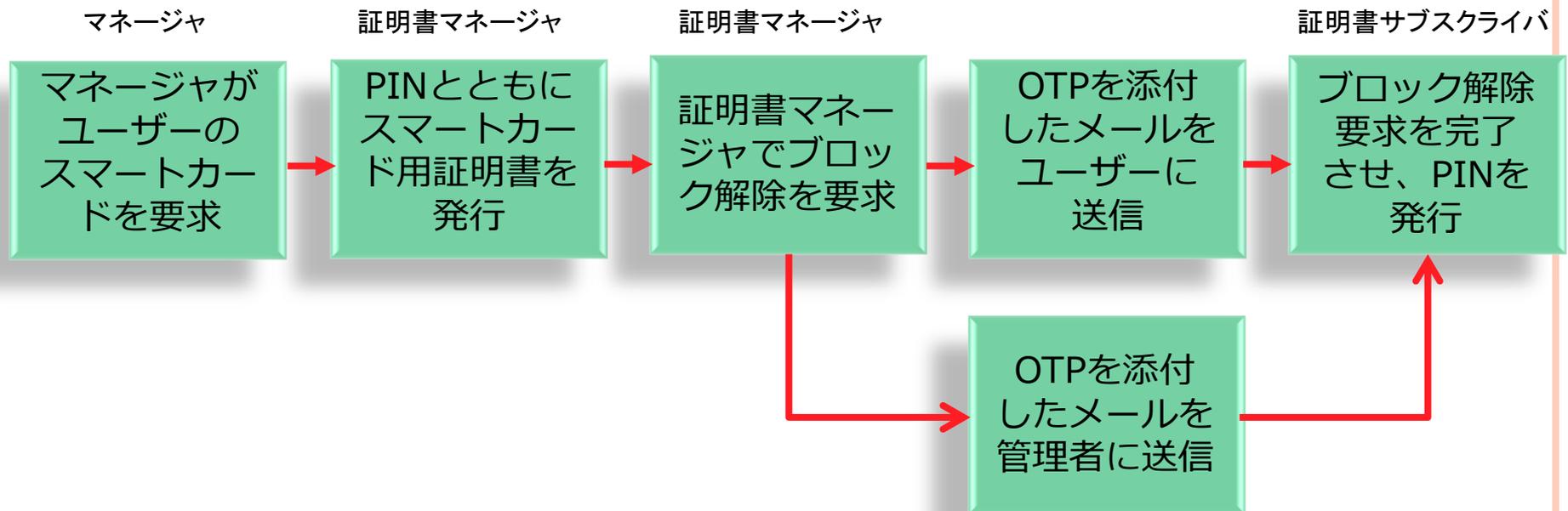


- 承認の必要なセルフサービス



スマートカードの発行

■ 発行エージェントによる発行



証明書の登録

マネージャポータル

スマートカードを
用意

外部または自動化されるプロセス

MIIS CLM MA が
要求を初期化

スマートカードの
PIN をセットして
PIN 番号を提示

スマートカードに
証明書とPINを
登録

証明書サブスクラ
イバにカードの
PINを送信

サブスクライバポータル

証明書サブスクラ
イバはカードを受
信

スマートカード紛失時

マネージャポータル

フロントデスクが
証明書サブスクライバを選択

フロントデスクは証明書サブスクライバ用に一時利用できるスマートカードを用意

ヘルプデスクはブロック解除リクエストを作成

OTPを生成し、証明書サブスクライバに送信

外部または自動化されるプロセス

サブスクライバポータル

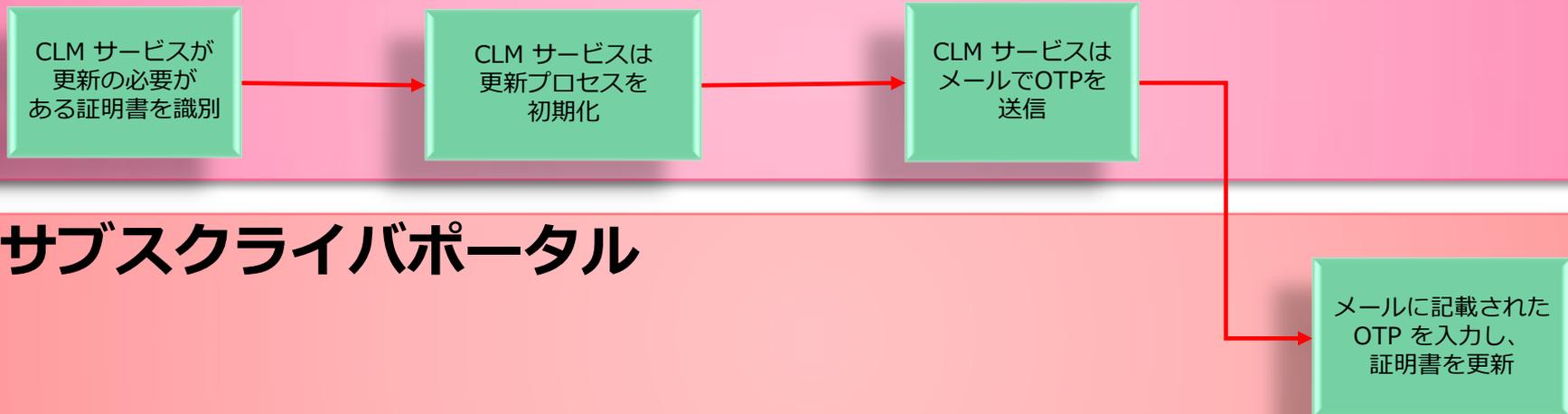
ヘルプデスクに連絡し、ブロック解除をリクエスト

証明書サブスクライバはKIOSKを使用してスマートカードのブロックを解除

証明書の更新

マネージャポータル

外部または自動化されるプロセス



サブスクライバポータル

自動登録

マネージャポータル

外部または自動化されるプロセス



サブスクライバポータル

WANTED

● ILM でサポートするスマートカード

PKCS 11 互換のスマートカードをサポート

- Axalto Client Software (ACS) v 5.2
- AET SafeSign v2.1
- Aladdin eToken RTE 3.6
- Gemplus GemSafe v4.2
- Siemens HiPath Scurity Card API v3.1.026

Base CSP

- CryptoAPI を採用するデフォルトのソフトウェアモジュール
- Windows Vista からオフラインによる証明書のブロック解除をサポート
- Microsoft Base Smart Card Cryptographic Service Provider パッケージによる実装可能 (KB909520)