

共有端末における ICカード認証システムの適用

名古屋大学情報連携基盤センター
葛生和人

第4回東海地区CSI事業報告会
2007年10月5日(金) 名古屋大学情報連携基盤センター

これまでの経緯

- PKIと連携したスマートカード認証システムを独自に開発^{[1][2]}

[1] 葛生和人, 平野晴, 間瀬健二, 渡邊豊英, *ICカードによる共有端末認証システムの構築*, 第35回 コンピュータセキュリティ(GSEC) 研究発表会研究報告, No.2006-CSEC-035, pp.45-50.

[2] 葛生和人, *PKIと連携したスマートカードログオンについてー共有端末における個人認証システムへの適用ー*, 名古屋大学情報連携基盤センターニュース, Vol.6, No.1, 2007, pp.27-40.

- Java Card Technologyを用いることにより, カードベンダー独自OSの影響を受けにくい汎用性の高いシステムを構築

第4回東海地区CSI事業報告会
2007年10月5日(金) 名古屋大学情報連携基盤センター

目的

PKIと連携したスマートカード認証システムを共有端末に適用するにあたり、

「共有端末としての特徴を生かせる形」

で発展させる。

共有端末の利用形態

- ICカードの所有者が利用可能である。
- いずれの共有端末でもユーザの作業環境は保持される。
- 利用者は限定されたユーザ権限の範囲内で端末を利用できる。
- ユーザの作業ログ，作業環境は管理者により管理される。

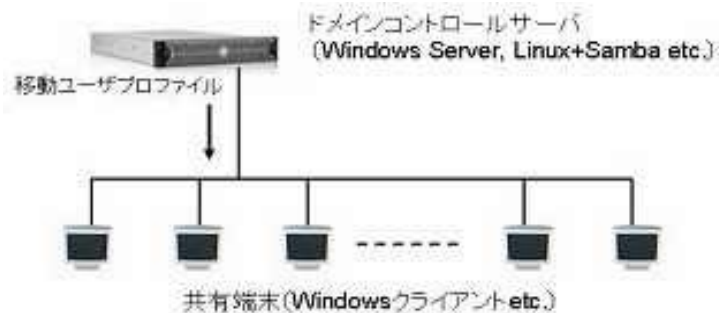
第4回東海地区CSI事業報告会
2007年10月5日(金) 名古屋大学情報連携基盤センター

共有端末利用システム

■ ドメインサーバを利用したシステム構築

Windows系サーバを使って共有端末用ドメインを構成。

個別ユーザの作業環境は**移動ユーザプロファイル**としてドメインコントロールサーバに保存。



第4回東海地区CSI事業報告会
2007年10月5日(金) 名古屋大学情報連携基盤センター

共有端末利用システム

■ ドメインサーバを利用したシステム構築

Windowsにおけるユーザプロファイルの形態



第4回東海地区CSI事業報告会
2007年10月5日(金) 名古屋大学情報連携基盤センター

共有端末利用システム

■ ドメインサーバを利用したシステム構築

考慮しなければならない問題

1. ドメインコントロールサーバ, クライアントアクセスライセンス導入コスト
2. LDAPなど従来のディレクトリーサーバを利用した認証システムとの統合



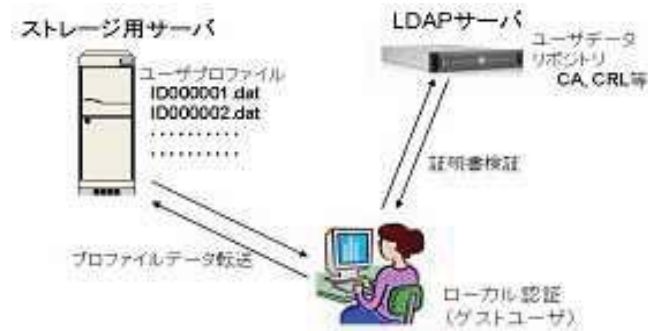
既存のシステムや共有端末の利用規模との関係が重要

第4回東海地区CSI事業報告会
2007年10月5日(金) 名古屋大学情報連携基盤センター

共有端末利用システム

■ 非ドメイン型移動ユーザプロファイルの導入

Shared PCの考え方を適用

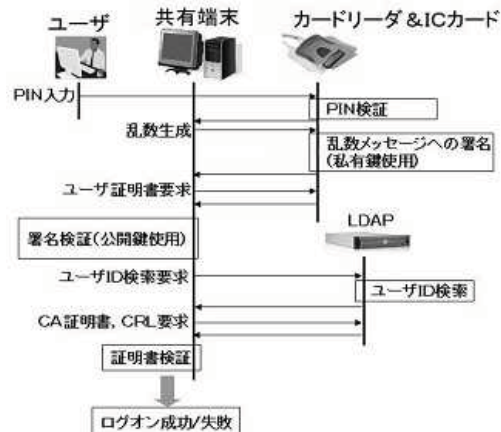


第4回東海地区CSI事業報告会
2007年10月5日(金) 名古屋大学情報連携基盤センター

共有端末利用システム

■ 非ドメイン型移動ユーザプロファイルの導入

PKIと連携したICカード認証(証明書検証, ユーザIDの確認など)



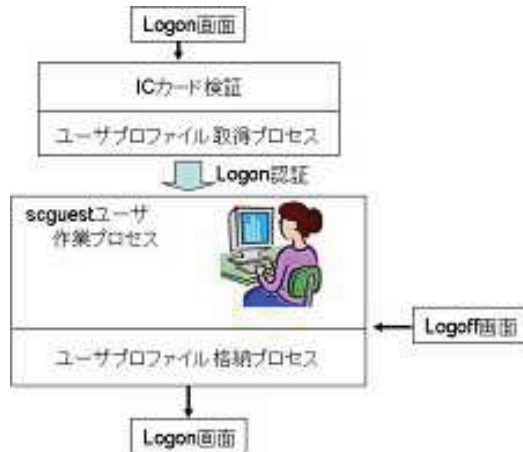
第4回東海地区CSI事業報告会
2007年10月5日(金) 名古屋大学情報連携基盤センター

共有端末利用システム

■ 非ドメイン型移動ユーザプロフィールの導入

プロフィールデータの取得(または格納)

ユーザのログオン, ログオフの直前に,
プロフィールの取得, 格納のための外部
プロセス(ssh通信)がそれぞれ呼ばれる.

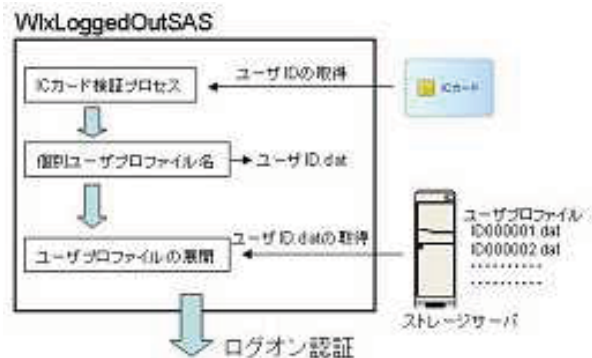


第4回東海地区CSI事業報告会
2007年10月5日(金) 名古屋大学情報連携基盤センター

共有端末利用システム

■ 非ドメイン型移動ユーザプロフィールの導入

プロフィールデータの取得(または格納)

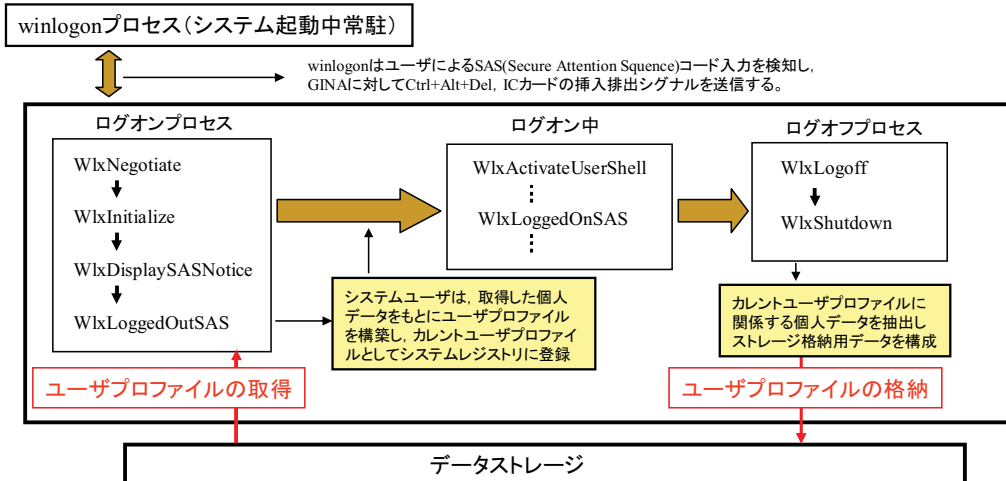


第4回東海地区CSI事業報告会
2007年10月5日(金) 名古屋大学情報連携基盤センター

共有端末利用システム

■ 非ドメイン型移動ユーザプロファイルの導入 プロファイルデータの取得(または格納)

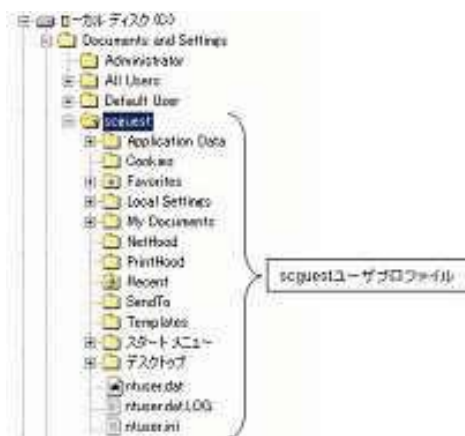
GINAの実行シーケンスとの関係



第4回東海地区CSI事業報告会
2007年10月5日(金) 名古屋大学情報連携基盤センター

共有端末利用システム

■ 非ドメイン型移動ユーザプロファイルの導入 ユーザプロファイル構成



プロファイルデータ分類

レジストリ登録データ(必須)

NTUSER.DAT

個人の作業環境フォルダA(容量小)

Cookies/最近使ったファイル/スタートメニュー/お気に入り

個人の作業環境フォルダB(容量大)

ApplionData/LocaSettings/MyDocument/デスクトップ

共有可能な作業環境フォルダ(容量小)

NetHood/PrintHood/SendTo/Templates

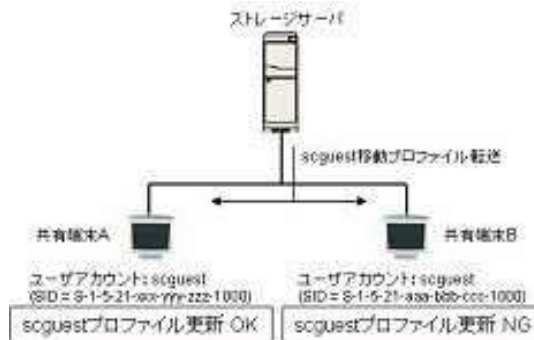
第4回東海地区CSI事業報告会
2007年10月5日(金) 名古屋大学情報連携基盤センター

共有端末利用システム

■ 非ドメイン型移動ユーザプロファイルの導入

ユーザプロファイルへのアクセス権限

共有端末のように異なる端末からログオンした場合、Windowsでは、同一ユーザ名であってもシステム上異なるSID(セキュリティ識別子)が割り当てられ、ユーザプロファイルへの変更権限が拒否される。



第4回東海地区CSI事業報告会
2007年10月5日(金) 名古屋大学情報連携基盤センター

共有端末利用システム

■ 非ドメイン型移動ユーザプロファイルの導入

ユーザプロファイルへのアクセス権限

ユーザプロファイルデータと登録用レジストリキーに対して共有のアクセス権限を与える。



第4回東海地区CSI事業報告会
2007年10月5日(金) 名古屋大学情報連携基盤センター

実証実験

■ カード関係仕様

表 1 ICカード仕様

タイプ	Java Card VM	
	接触型	非接触型
準拠規格	ISO/IEC7816	ISO/IEC 14442 Type B
通信プロトコル	T = 0, 1	ISO/IEC14443-4
通信速度(kbps) MAX	19.2	424.0
メモリ	1Mバイト(フラッシュメモリ)	
CPU	16ビット	
セキュリティ	RSA, DES, T-DES演算対応	

表 2 カードリーダ仕様

タイプ	接触型	非接触型
品名(品番)	GemPC TWIN	PD2992P
準拠規格	ISO/IEC7816	ISO/IEC 14442 Type B
インタフェース	USB 2.0	USB 1.1

■ その他カード関係環境

Java Card VM上に搭載されたJava Card認証用アプリケーション
カード内にはPINコード、ユーザ証明書、ユーザの私有鍵を格納
ユーザ証明書は、X.509標準規格に従い、ASN.1、DERフォーマットでエンコード
私有鍵に関しては1024ビット長のRSA暗号鍵を格納している。

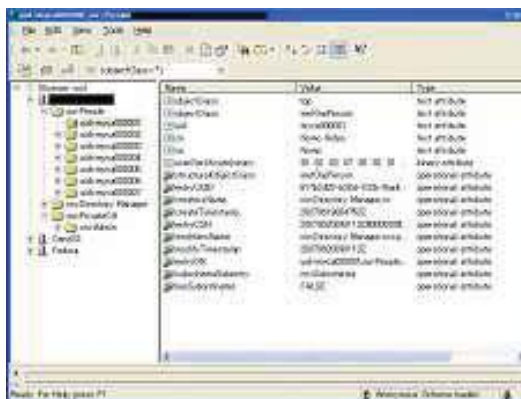
第4回東海地区CSI事業報告会
2007年10月5日(金) 名古屋大学情報連携基盤センター

実証実験

■ 簡易認証局

DELL Power Edge 2850 3.8GHz Xeonプロセッサ
Cent OS5上でNAREGI-CAを使って、CA証明書、ユーザ
証明書、CRLを発行

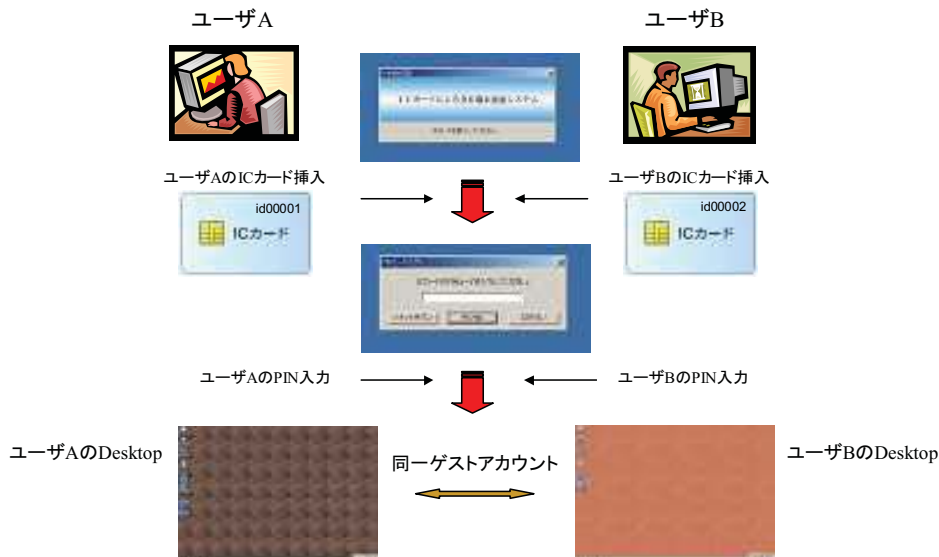
各証明書、CRLのリポジトリとして
同サーバにOpenLDAP2.3を実装、
CA証明書、CRLとともに仮想ユー
ザ情報も格納



第4回東海地区CSI事業報告会
2007年10月5日(金) 名古屋大学情報連携基盤センター

実証実験

- ユーザA,Bは**同一のゲストアカウント**でありながら個別の作業環境を保持

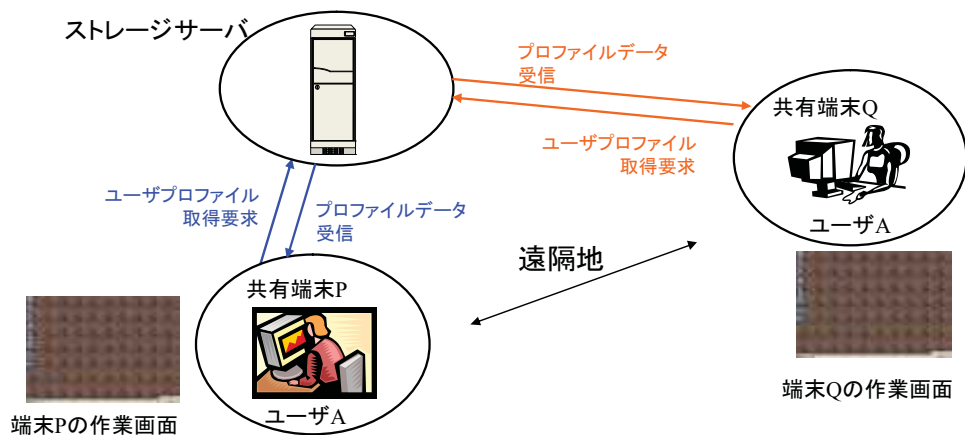


第4回東海地区CSI事業報告会
2007年10月5日(金) 名古屋大学情報連携基盤センター

実証実験

- 何処の共有端末であってもログオン時に同じ作業環境を構築

遠隔地の端末であっても同じICカードでのログオンならばデスクトップ等の作業環境は同じ。
(その他ブラウザ等の設定を保持することも可能:但しセキュリティポリシーによる)



第4回東海地区CSI事業報告会
2007年10月5日(金) 名古屋大学情報連携基盤センター

実証実験

デモンストレーション

第4回東海地区CSI事業報告会
2007年10月5日(金) 名古屋大学情報連携基盤センター

まとめ

- ICカードを用いた共有端末認証において、カードユーザごとの作業環境をストレージに保持するための機能を追加した。

今後

- ユーザ作業環境に加えてさらに個別ユーザのドキュメント等のデータストレージ保存について効率的な方法を考える。
- セキュリティを考慮してゲストユーザの作業状況をログとして監視できる仕組みも合わせて構築する。

第4回東海地区CSI事業報告会
2007年10月5日(金) 名古屋大学情報連携基盤センター