社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2008－DPS－134 (2)
2008－CSEC－ 40 (2)
2008／3／6

Sambaを利用した移動ユーザプロファイルの構築とICカード認証連携

葛生和人† 平野靖† 間瀬健二† 渡邉豊英†

† 名古屋大学情報連携基盤センター
〒464-8601 名古屋市千種区不老町
E-mail: † {kuzuu,hirano,mase,watanabe}@itc.nagoya-u.ac.jp

あらまし ドメイン構成を用いずに，いずれの共有端末からも個別のユーザ環境を再構築できるシステムを開発した．本システムでは，ドメインサーバを介さずにLDAP上で管理される既存のユーザディレクトリ情報にアクセスし，PKIアプリを搭載したICカードと連携して共有端末へのログオン認証が行われる．なお，ユーザ環境の再構築に必要なユーザプロファイル情報は，sshサーバを通して共有のデータストレージ上に格納される．また，共有端末からネットワークドライブとして接続したSambaファイルサーバ上に，ユーザプロファイル関連フォルダを置くことで，通常はドメイン構成上ではじめて成り立つ移動ユーザプロファイル機能を，ドメインサーバの導入の必要なく実現することができた．本システムは，管理運用面と経済性の両面において有利なソリューションであるといえよう．
キーワード ： PKI, ICカード認証，ユーザプロファイル，共有端末

Smart Card Authentication System accessing Roaming User Profile Folders on Samba File Server

Kazuto KUZUU†, Yasushi HIRANO†, Kenji MASE†, and Toyohide WATANABE†

† Information Technology Center, Nagoya University
Furo-cho, Chikusa-ku, Nagoya-shi, Aichi 464-8601, JAPAN
E-mail: † {kuzuu,hirano,mase,watanabe}@itc.nagoya-u.ac.jp

Abstract We developed newly the logon authentication system which can rebuild the individual environment on a shared terminal without depending on domain accounts. In this system, the logon authentication to the terminal is carried out using both a PKI application on smart card and the user directory information of LDAP, and the system does not need a domain control server. The user profile data, which is required for rebuilding of user environments, is stored on shared data storage through a ssh server. On the other hand, the concept of roaming user profile not belonging to a domain is realized through putting user profile folders on Samba file server connected to a shared terminal as a network drive. This system can be regarded as advantageous solution from the points of both user management and economical efficiency.
Keyword : PKI, smart card, authentication, user profile, shared terminal

1. はじめに

不特定多数の利用者を想定した共有端末は，図書館等の公共施設の端末に代表されるように，その多くがセキュリティの関係からゲストユーザ画面が開かれたままログオフできない状態となっており，そこでは利用可能なアプリケーションも蔵書検索用のソフトに制限されている．また，マウスや画面の操作制限が端末ごとに厳重に管理されていることも少なくない．

しかしながら，近年，ICカードの普及とそれに伴うセキュリティ技術の向上から，カードユーザを対象とした共有端末利用が企業を中心として増えつつある．すなわち，必要な情報リソースを特定のデータストレージ上に格納することで情報流出を防ぎたいというセキュリティ要求と，どの端末においてもユーザの作業環境を再構築できるようにしたいという利便性要求のいずれをも満たすことができるという点においては，ICカード認証は共有端末に欠かすことができないものと言えよう．

筆者らは，ICカード技術の標準化がいまだ不十分であるという現状をふまえつつ，共有端末利用法に関する大学独自のあり方を探るため，これまで共有端末用ICカードアプリとミドルウェアを独自に開発してきた．そして，Java Card™ Technology [1]を利用したPKI連携用ICカードアプリをJava Card VM上に搭載し，スマートカードログオン実現のための独自のミドルウェアをWindows上に実装した[2][3]．

一方，共有端末の利便性として求められるユーザ

環境の再構築機能に関しては，ユーザアカウント管理とプロファイルローミングがポイントとなる．

共有端末におけるユーザアカウント管理は，通常，ドメインコントロールサーバ上のユーザアカウント情報にもとづいて行われるが，このことはしばしば，ドメインサーバの新規導入やディレクトリ情報の2重管理など，システム管理者に対して余分な負担を強いることとなる．この問題を回避するために，筆者らは非ドメイン型移動ユーザプロファイルの考え方を導入して，ドメインコントロールサーバを設定することなく個別作業環境を再構築できるシステムを提案してきた[4]．

本論文では，これまで開発してきたシステムをさらに発展させて，個別ユーザプロファイルに関連付けられるユーザごとの履歴データ，ドキュメントデータなどを，ドメイン構成によらずに共有端末上で保持できるシステムを提案する．

2. 共有端末システムの構築

本システムは，共有端末における個別ユーザの作業環境がドメイン構成によらずに IC カードユーザごとに再構築できるという機能を特徴としている．まず，このようなシステムの開発にあたって中心的な役割を果たす要素を以下に示す．

- IC カード認証によるセキュリティの確保
- 移動ユーザプロファイルデータの共有ストレージへの格納
- 共有ファイルシステム上に置かれたユーザ作業フォルダとユーザプロファイルの連携

先に述べた共有端末としての機能を満たすための要件は，上に掲げた構成内容それぞれが最終的に連携しあって実現されるものであるが，本節では，まず，それぞれの項目を実現するための具体的なシステム構築の内容について説明する．

2.1. IC カード認証システムの構築

共有端末のセキュリティに関して重要な役割を果たす IC カードによるログオン認証，いわゆるスマートカードログオンは多くの PC 端末で実装されつつある．本研究では Java Card™ Technology [1]を用いて，電子証明書格納可能な Java Card™ アプリを IC カード上に搭載するとともに，IC カードおよび LDAP サーバと連携したログオン認証用プログラムをミドルウェアとして Windows 上に実装し，PKI によるスマートカードログオン機能を実現してきた[2][3]．

なお，ログオン認証プログラムの開発にあたっては，Windows XP（および Windows 2000）において標準装備されている GINA（Graphical Identification aNd Authentication）[5]の拡張 API を利用した．また，認証システムに PKI を組み込むために，NAREGI-CA[6]を導入してプライベート認証局を構築し，さらに，CA 証明書や失効リスト（CRL）を管理するデータベースにとして，ディレクトリサーバ OpenLDAP2.3[7]を導入している．

なお，PKI を利用したログオン認証プロセスにおける IC カードおよび LDAP との連携プロトコルの概要は図 1 に示すとおりである．

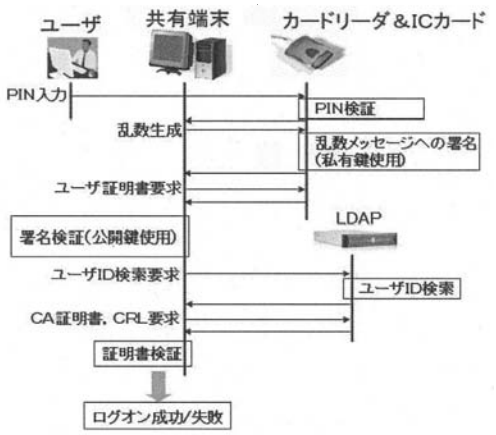

図 1 スマートカードログオン認証プロトコル

2.2. 移動ユーザプロファイルのストレージ格納

Windows 系システムのユーザ作業環境は，ログオン時にユーザプロファイルデータがレジストリ情報としてシステムにロードされることにより再構築されるが，このプロファイルデータは，その利用形態によってローカルユーザプロファイル，移動ユーザプロファイル，固定ユーザプロファイルに分類される[8]．これらプロファイルのうち，ローカルユーザプロファイルがスタンドアロンマシンに保存されるのに対して，移動ユーザプロファイルや固定ユーザプロファイルはドメイン管理を受け持つサーバマシンに保存される．特に，図 2 に示したように，移動ユーザプロファイルに関しては，個々のユーザによるプロファイル変更が可能なため，クライアントマシンが異なってもユーザごとに作業環境が再構築されることとなる．すなわち，共有端末における個別作業環境の再構築には，このような移動ユーザプロファイルの考え方が必要となる．

図 2 ユーザプロファイルの種類

しかしながら，移動ユーザプロファイルや固定ユーザプロファイルの設定は，Windows ドメインサーバでのユーザアカウントの登録が前提となる．このことは，LDAP など他のディレクトリサーバによってユーザ情報管理が行われている場合，ディレクトリ情報の2重管理，さらにはそれらの同期システムの必要性が生じるということを意味している．

筆者らは，ドメインサーバの新規導入により生ずるこのような非効率的な問題を回避し，なおかつプロファイルローミングの要件を満足させたいという観点から，ログオン認証に関しては LDAP と連携した IC カード認証システムでその機能を受け持たせ，プロファイルデータに関してはユーザごとにデータストレージに格納させるというシステムを提案した[4]．

このシステムでは，ユーザはドメイン環境の必要のないゲストユーザとして共有端末にログオンする一方で，認証は PKI と連携した IC カード認証を経るため，決して匿名ユーザではない共有端末ユーザとしてのセキュリティが確保されるようになる．なお，ログオンユーザのプロファイルデータは，各 IC カードのユーザ ID に紐付けされた個別ファイル名でデータストレージ上に保存される．図 3 は，共有端末に対して，PKI 連携認証で利用される LDAP サーバとユーザプロファイル格納用のデータストレージ，さらにそれぞれの間でのデータ通信の関係を示したものである．

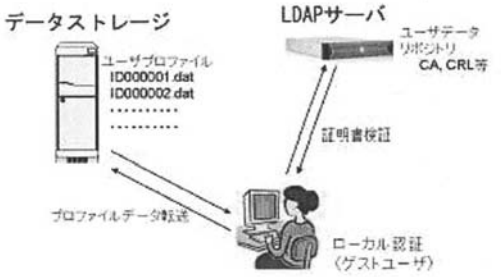

図 3 共有端末とデータストレージ，LDAP との関係

2.3. ユーザ作業フォルダの共有ファイルサーバ（Samba サーバ）への割り当て

2.2 で示したように，本システムにおけるプロファイルローミングは，ユーザ個々のプロファイルデータをデータストレージから端末に読み込むことにより実現される．このプロセスを通して，端末上は同じゲストユーザでありながら IC カードで識別されたユーザの作業環境が共有端末上で再構築されることとなる．しかしながら，本来のユーザ作業環境を実現するためには，さらに個別の作業環境に関連付けられたユーザデータ（各種ドキュメント，履歴データ，クッキー，ブックマーク，一時ファイルなど）もプロファイルデータとともに共有端末から参照されなくてはならない．ところが，そのようなデータの容量は大量であり，全ての個人データをさきのプロファイルデータとともにデータストレージ上に格納することは，データ転送時間の問題などから現実的ではない．

2.3.1. Samba による共有ファイルシステム構築

この問題を解決するために，本システムでは，個別ユーザ作業環境に関連付けられたユーザデータを，ユーザプロファイル用データストレージとは別の共有ファイルシステムに常に保存できるようにし，ログオン時にユーザ作業フォルダとして端末のファイルシステムに割り当てられるようにした．なお，ここではユーザデータの保存用に Samba ファイルサーバ[9]を用いて共有ファイルシステムを構築し，ユーザログオン時に作業環境構築プロセスの中でネットワーク接続できるようにした．ここで，ユーザ作業フォルダ保存用共有ファイルシステムとプロファイル用データストレージ，LDAP サーバとの関係を図 4 に示す．また，IC カードの読み込みからユーザプロファイルの読み込み，プロファイルデータのシステムへのロード，作業データフォルダーの割り当て，さらにはユーザ作業環境の構築までの一連のプロセスを図 5 に示す．

図 4 個別ユーザ作業フォルダの
共有ファイルシステムへの割り当て

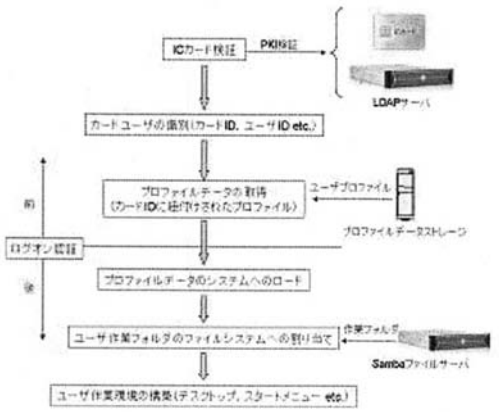

図 5 共有端末ユーザログオンプロセス

2.3.2. 共有ファイルシステムのドライブ割り当て

Windows システムにおけるユーザ作業フォルダ(Application Data, Cookies, My Documents, etc.)は通常はCドライブ Documents and Settings フォルダ内のユーザフォルダに置かれており，個別ユーザの所有するデータはその用途に応じてそれぞれのフォルダ内で読み書きされる．本システムでは端末上のゲストは同一アカウントであるため，この作業フォルダは同じフォルダ名で同じ場所に置かれることとなる．しかし，実際には異なるカードユーザとしてログオンしているため，各ユーザは他人の残した作業フォルダを参照することになってしまう．このような作業フォルダの共有化を避けるため，それらフォルダを Samba ファイルサーバ上に登録された個別ユーザ領域に置くこととした．そのため，まず，ユーザログオン時に IC カードによって識別された個別ユーザとして，Samba ファイルサーバへの自動接続を行い，必要なドライブ割り当てができるようにする．ここでは，GINA 実行シーケンス中のログオン認証後に，CreateProcess 関数を用いて外部プロセスとして net use コマンドを実行し，カードユーザ名義で Samba ファイルサーバに接続できるようにしている．また，それと同時に必要なドライブ割り当ても行っている．なお，ユーザごとにデータを保存するための Samba ユーザ登録は，必然的に共有端末利用者分が必要となるが，接続プロセス自体は GINA からの実行プロセスとして行っているため，個々のユーザがパスワード入力を行う必要は無く，パスワード管理もシステムの管理者が一括して行うこととなる．このことは，共有端末ユーザは，自身が Samba ユーザとして登録されているにもかかわらず，本システム(共有端末)以外からは Samba サーバに接続することはできないことを意味しており，その点で共有ファイルシステムに対するセキュリティは高められている．

2.3.3. ユーザ作業フォルダパスのレジストリ登録

前項で述べたように，本システムでは，作業データの共有化を避けるため，ユーザ作業フォルダを Samba ファイルサーバの共有ファイルシステム上に割り当てるようにした．しかし，この時点ではシステムはユーザプロファイルデータから構築された作業環境が Samba 上のユーザ作業フォルダを自動的に参照するようには設定されていない．Windows 上の通常の設定方法では，デスクトップ上のマイドキュメントフォルダに関しては，対応するターゲットフォルダを指定することができるものの，それ以外の作業フォルダに対する設定ツールは用意されていない．

そこで，本システムではレジストリ領域に登録されている作業フォルダパスを変更することにより上の問題に対処している．実際には，レジストリキー設定画面から，¥HKEY _USERS¥S-1-5-*¥Software¥Microsoft¥Windows¥CurrentVersion¥Explorer¥User Shell Folders の中の設定値としてフォルダパスを指定することにより実現できる(図 6)．なお，ここで設定したキーの値はユーザプロファイルデータ(NTUSER.DAT)としてプロファイルデータストレージ上に格納される．

図 6 作業フォルダパスの
ユーザプロファイルレジストリ登録

3. システム構成と実装

本システムの実装に当たって，その構成内容とソフトウェア，ハードウェアの仕様について述べる．

3.1. ICカード，カードリーダおよびカードアプリ

IC カードは，接触，非接触のいずれにも対応したデュアル・インタフェース型，1MB メモリを有するもので IC プラットフォーム上に Java Card VM を組み込んでいる．カード内でのセキュリティ API は RSA，DES，T-DES の複数の暗号処理が可能である．Java Card VM 上に搭載する認証用アプリケーションは，Java Card Technology を使って既に開発したもので[2][3]，カード内には PIN コード，ユーザ証明書，ユーザの私有鍵が格納されている．なお，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されたもの，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．

4.1. 共有端末，データストレージおよび Samba サーバ仕様

本実装では，仮想共有端末としてデスクトップマシン ThinkCentreA52T & WindowsXP Professional SP4 を割り当て，また，ユーザプロファイル格納用データストレージマシンに，DELL Power Edge 2850 3.8GHz Xeon & Cent OS5 を使用した．一方，同マシンには，認証局として NAREGI-CA[6]，ディレクトリサーバとして OpenLDAP2.3[7]も実装している．さらに，作業フォルダ保存用ファイルシステム構築のため，Samba 3.0.10 を用いてファイルシステムを ThinkCentreA52T & Cent OS5 上に実装した．

4. 実証実験

仮想共有端末を用いて，異なる 2 ユーザ(2 枚の IC カードに対して個別のユーザ証明書，私有鍵を格納)に対する実証実験行った．検証内容は，

- 異なるユーザが同一の共有端末からログオンした場合のユーザ作業フォルダ割り当ての確認
- ログオン時ユーザごとのアプリケーション作業環境の独立性の確認

である．

4.1. ユーザ作業フォルダの割り当て

まず，本システムを実装した共有端末上で，2 枚の IC カードを使ってログオン認証を試みる．ログオン時に，各々のカードユーザに対するデスクトップ作業環境が再構築されていることが確認できた．特に，図 7 に示すように，ファイルシステム内の構成を確認すると，ログオン時の作業フォルダが Samba の共有ファイルシステム上に割り当てられ，各カードユーザがそれぞれの ID に相当する Samba ユーザとして接続していることが確認できる．

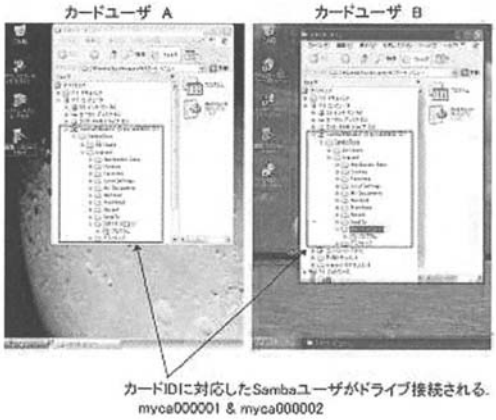

図 7 Samba 上の作業フォルダ割り当て

4.2. アプリケーション作業環境の独立性

次に，利用するアプリケーションごとに設定されるパラメータ(初期値設定，オプション設定，書式設定など)が，ユーザごとに独立して保持されているかを確認する．ここでは，共有端末上の一般的な利用を想定したアプリケーションとして Internet Explorer (IE6)と Office Word(Word 2003)を取り上げた．それぞれのアプリケーションを対象として，初期画面，閲

覧履歴，ブックマーク，デフォルト書式などいくつかの設定内容に対してユーザごとの独立性が確認できた．図 8 および図 9 にその代表例を示す．

図 8 IE6 ユーザ設定比較

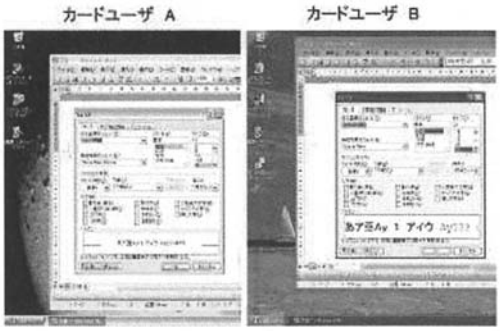

図 9 Word 2003 ユーザ設定比較

図 8 は IE6 の初期画面と登録しているブックマーク内容をユーザごとに比較したもので，個別ユーザごとの設定内容の違いが確認できる．また実験では，インターネット一時ファイル，クッキー情報，閲覧履歴などもユーザごとに独立して保存されていることを確認した．図 9 は，Word 2003 の新規データ作成時の書式設定画面で，ユーザごとに異なった入力書式が保持されていることが確認できる．

5. まとめ

ドメイン構成を用いずに，どの共有端末からも個別のユーザ環境を再構築できるシステムを開発し，それを仮想的な共有端末に実装した上で，実際の稼働状況や機能についての確認を行った．本システムでは，ユーザ作業フォルダをローカルマシンとは別の Samba ファイルシステム上に置くことにより，各端末利用者の作業データが個別に保持できるようにし，コスト面，運用面のいずれにおいても有利なユーザ環境再構築機能を実現することができた．なお，共有端末という特殊な利用形態を考えた場合，個別ユーザのアクセスログ管理を含め，十分なセキュリティ確保と情報管理に関する機能はさらに充実させる必要があり，今後の検討課題となるであろう．

謝辞

本研究は，国立情報学研究所の最先端学術情報基盤（CSI）事業の一環として行われたものである．ここに記して謝意をあらわす．

参考文献

[1] Zhiqun Chen, “Java Card™ Technology for Smart Cards”, Addison Wesley.

[2] 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（CSEC）研究発表会研究報告，No.2006-CSEC-035, pp.45-50.

[3] 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－共有端末における個人認証システムへの適用－*，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.

[4] 葛生和人，平野晴，間瀬健二，渡邊豊英，*IC カード認証と連携した非ドメイン型移動ユーザプロファイルの共有端末への実装*，インターネットコンファレンス 2007 論文集，日本ソフトウェア科学会研究会資料シリーズ No.51, pp.21-30.

[5] GINA, http://msdn.microsoft.com/msdnmag/issues/05/05/SecurityBriefs/

[6] T.Okuno,”New open source CA development as Grid research platform”, http://www.naregi.org/papers/data/ggf12-caops_pki.pdf, Global Grid Forum, 2004.

[7] OpenLDAP, http://www.openldap.org/

[8] ユーザプロファイルの概念，http://www.microsoft.com/technet/prodtechnol/windowsserver2003/ja/library/ServerHelp/20f61c10-0b87-41c9-a343-b4342c5562e8.mspx

[9] Samba, http://www.samba.gr.jp