ＩＣカードを用いた重要情報の配送方式

保母　雅敏†　渡邊　晃‡

†‡名城大学大学院理工学研究科　〒468-8502　愛知県名古屋市天白区塩釜口 1-501
E-mail: †m0432037@ccmailg.meijo-u.ac.jp, ‡wtnbakr@ccmfs.meijo-u.ac.jp,

あらまし　ユーザが自由に端末を選んで利用する環境でも安全な通信を行いたいという要求がある．このような環境においてもクライアント端末には，必要に応じてサーバから重要な情報を配送したい場合がある．この重要情報を配送するために，クライアントとサーバの間で確実な認証を行う必要があるが，クライアント端末はユーザ認証を行うための初期情報を所持していない．本論文では，非接触 IC カードを利用して初期情報を持たないクライアント端末に重要情報を配送するための方法を検討した．
キーワード　個人認証，IC カード，耐タンパ性

Important Data Distribution Method Using IC Card

Masatoshi HOBO†　Akira Watanabe‡

†‡Graduate School of Science and Technology, Meijo University
1-501 Shiogamaguchi, Tenpaku-ku, Nagoya-shi, Aichi, 468-8502, Japan
E-mail: †m0432037@ccmailg.meijo-u.ac.jp, ‡wtnbakr@ccmfs.meijo-u.ac.jp,

Abstract Even in the environment as the user can choose any client terminals, secure communication between a server and a client is essential for the system. However, in this case, the client has no data for identity verification. In this paper, assuming a non-contact IC card for identity verification, we have studied an authentication method between the client terminal and the server terminal.
Keywords Identity Verification, IC Card, Tamper Resistant

1.　はじめに

インターネットの普及に伴い，今後 P2P 通信を行うアプリケーションが一般的になってくると考えられる．しかし，従来からのクライアント/サーバ間通信がなくなることはない．P2P 中心のシステムであっても，管理装置によりシステムを集中的に管理することがあり，管理装置から P2P 端末へ通信グループの情報や暗号鍵などの重要な情報の配布を必要とする場合がある．この時の P2P 端末と管理装置の関係はクライアント/サーバの関係にある．

クライアント/サーバ間での認証と暗号化による情報配送は，従来から様々な方式が検討されてきた[1]-[4]．その中でもユーザが IC カードを所持する方式が注目されている．この方式では，IC カードの持ち主を確認するためのユーザ認証も併せて検討する必要がある．ユーザ認証は，IC カード内にパスワードなどのユーザ認証情報を格納し，クライアントで取得したユーザ認証情報を IC カード内で検証する方法が主流である[5]-[8].

しかし，従来のシステムでは IC カードはクライアントに挿入して一体となることを前提としているものがほとんどであり，IC カード/クライアント間の通信の安全性については十分に検討がなされていない．今後は使い勝手の良さから非接触 IC カードが主流になると考えられるが[9]-[11]，次のような課題について考察する必要がある．即ち，IC カード/クライアント間の情報交換が無線通信で行われるため，両者を一体とみなすことができず，暗号化が必要である．また，ユーザ認証を行うための情報は IC カードが所持し，クライアントには認証に必要となる情報は所持させないことが望ま

しい．しかし，実際に重要情報が必要となるのはクライアントであるため，何の情報を持たないクライアントとサーバとの間の認証方法を検討する必要がある．

本論文では，非接触 IC カードを利用することを前提とし，初期情報を持たないクライアントに重要情報を配送するためのプロトコル SPAIC(Secure Protocol for Authentication with IC card)を検討した．SPAIC では，ユーザの公開鍵を IC カード内に保存させ，この公開鍵を用いて IC カード/クライアント間の暗号通信を実現する．また，IC カードを経由してクライアント/サーバ間で乱数を共有する．この乱数を共通鍵として用いる事でクライアント/サーバ間の認証と暗号通信を実現する．

以降，２章でシステムの要件，３章で提案方式，４章で実装，５章でまとめを述べる．

2. システム要件

本章では想定するシステムのモデルを示し，IC カードを用いたユーザ認証モデルの検討，想定システムにおける課題について述べる．

2.1. 想定するシステムモデル

本研究で想定するシステムモデルを図 1 に示す．本システムはサーバからクライアントへ暗号鍵などの重要情報を配送することを目的とする．クライアントには個人の認証に必要となる初期情報を一切所持させない．これにより，ユーザは特定の端末に縛られることがない．また，個人の認証情報が端末から漏れる心配がなくなる．

各クライアントには非接触 IC カードリーダが搭載されており，各ユーザに発行された IC カードを用いてユーザ認証を行う．ここでは，生体情報読み取り装置と組み合わせることによって，より高いセキュリティを実現することを想定する．

2.2. IC カードを用いたユーザ認証モデル

IC カード内には公開鍵暗号の秘密鍵といった個人を特定する情報が格納されている．IC カード/サーバ間は PKI などの公開鍵暗号の仕組みを用いて確実な認証を行うことができる．しかし，IC カードの持ち主を確認するユーザ認証には別の手段が必要である．

ユーザ認証の方法として，一般的にはパスワードが用いられる．より高い安全性を必要とする場合には，パスワードと生体認証の組み合わせが必要となる．この際，認証情報の格納場所の違いにより，サーバに情報を格納して認証を行うサーバ認証モデル，IC カード内に情報を格納して認証を行うクライアント認証モデルに分けられる(図 2)．

サーバ認証モデルは，ユーザとサーバ間で直接認証を行うエンドエンドの認証である．クライアントで取得した認証情報を，IC カードを

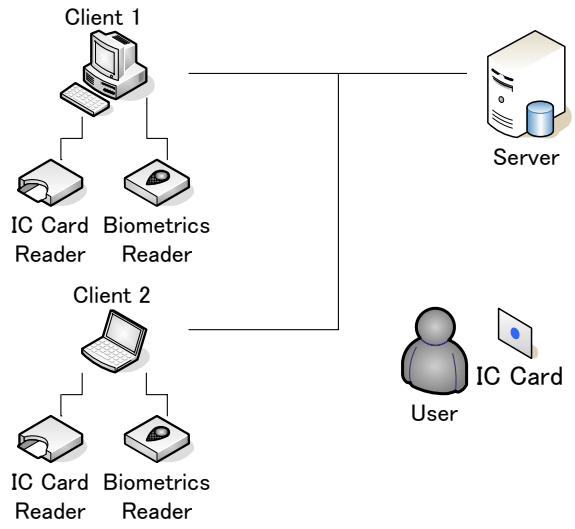

図 1 想定するシステムモデル
Fig.1Assumed System Model

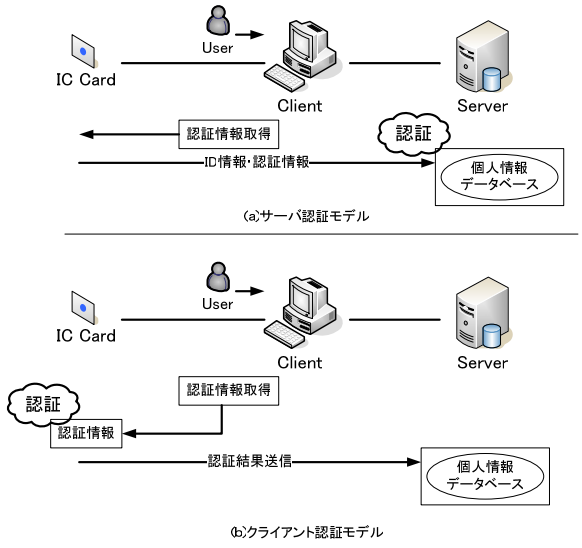

図 2 IC カードを用いた認証モデル
Fig.2 Authentication Model Using IC Card

経由してサーバへ送信して認証を行う．このモデルではサーバ側で集中して処理を行うため，IC カードの処理負荷の軽減できるというメリットがある．しかし，ユーザ全員の情報をサーバ側で一括して管理するため，管理体制が重要となる．このため，大規模な耐タンパハードウェアを用いる，厳重な設備を準備するなどの対策が必要となる可能性がある．

クライアント認証モデルは，ユーザ/IC カード，IC カード/サーバ間でそれぞれ認証を行うリンクバイリンク認証である．クライアントで取得した認証情報を IC カードへ送信して IC カード内で認証を行い，その後 IC カード/サーバ間で認証を行う．この方法では IC カードの認証がユーザ認証を兼ねることになる．IC カードは耐タンパ性を有しているため，パスワードや生体情報を安全に格納することができるというメリットがある．しかし，IC カードに掛かる負担が大きくなる．

どちらの認証モデルにおいても，安全に個人認証を行うことが可能であるが，ここではより簡単に安全性が達成できるクライアント認証モデルを採用する．ただし，SPAIC の原理はどちらのモデルでも適用可能である．

2.3. システムにおける課題

想定するシステムには IC カード/クライアント，IC カード/サーバ，クライアント/サーバの３つの通信経路が存在する．ここで，IC カード/クライアント，クライアント/サーバ間の通信には次のような課題がある．

IC カード/クライアント間の通信には，クライアントで取得した認証情報を IC カードへ送信する場合が含まれる．接触型 IC カードを利用する場合は，IC カードが物理的にクライアントと接続されているため，IC カード/クライアント間の情報交換が外部へ漏れる心配はなかった．しかし，非接触 IC カードを利用する場合，情報漏洩の危険性を考慮しなければならない．

また，クライアント/サーバ間の通信は，クライアントが認証情報を所持していないため，そのままではサーバから直接重要情報を受け取ることができない．

以上の課題を解決し，クライアントに安全に重要情報を配送するプロトコル SPAIC の検討を行った．

3. SPAIC

本章では非接触 IC カードを用いて安全に重要情報を配送するためのプロトコル SPAIC について述べる．SPAIC では，IC カード/クライアント，IC カード/サーバ，クライアント/サーバの各間での認証と暗号化を実現する．

3.1. SPAIC の概要

SPAIC の概要を図 3 に示す．IC カードにはユーザの秘密鍵とともに秘密鍵とペアになる公開鍵を格納しておく．この公開鍵は情報交換に先立ち，クライアントへ送信する．クライアントは乱数を生成し，ユーザから入力されたパスワードや生体情報とともに上記公開鍵で暗号化を行い，IC カードに送信する．

IC カードで上記情報を復号してユーザ認証を行う．次に IC カード/サーバ間で公開鍵暗号を用いた認証を行う．このときにクライアントが生成した乱数を暗号化しサーバへ送信する．

サーバは IC カードの認証を行う．クライアント認証モデルであるため，同時にユーザ認証も完了する．サーバは認証と同時にクライアントが生成した乱数を取得する．これにより，クライアント/サーバ間で乱数を共有することができる．この乱数を用いて，以降はクライアント/サーバ間の認証および重要情報の暗号通信が可能となる．

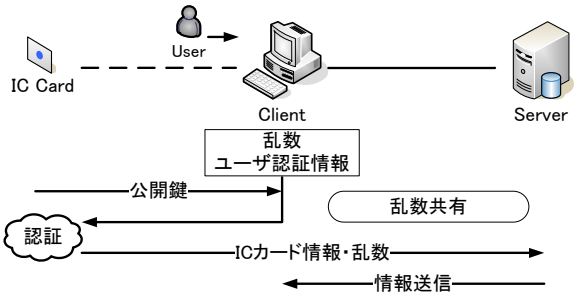

図 3　SPAIC の概要
Fig.3 Outline of SPAIC

3.2. 各端末の初期情報

SPAIC において，各端末が所持する初期情報を表 1 に示す．以降の説明は，ユーザ認証にパスワードと生体認証を用いて行うものとする．各ユーザは IC カード内に固有の ID，秘密鍵/

表 1　提案方式の初期情報
Table.1 Initial Information of Proposal Method

IC カード	IDx1 : IC カード ID Prx : IC カード秘密鍵 Pux : IC カード公開鍵 PuS : サーバ公開鍵 PW : パスワード情報 T : 生体情報テンプレート
クライアント	なし
サーバ	PrS : サーバ秘密鍵 IDx : IC カード ID Pux : IC カード公開鍵

公開鍵，サーバ公開鍵，ユーザパスワード，生体情報テンプレートを所持している. サーバでは，サーバ秘密鍵，各 IC カードの ID と公開鍵を所持する. これらの情報はサーバ側で一括して作成し，IC カードの発行はあらかじめオフラインで実施しておく.

3.3. SPAIC のシーケンス

SPAIC の配送シーケンスを図 4 に示す．以下のシーケンスの説明は図中の番号に対応する.

① クライアントにパスワード PW を入力する．同時に生体情報を入力し，特徴点 S を取得する.
② IC カードからクライアントに IC カード公開鍵 Pux とサーバ公開鍵 PuS を送信する.

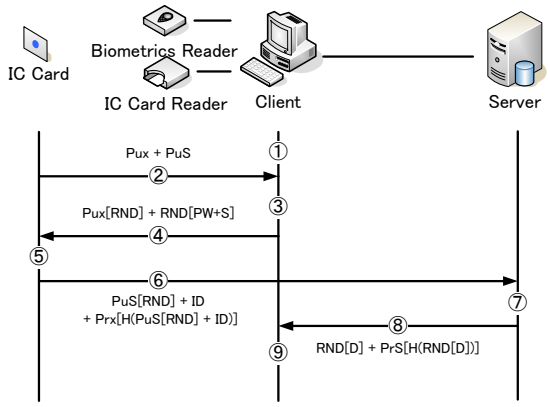

図 4　SPAIC の配送シーケンス
Fig.4 Distribution Method of SPAIC

③ クライアントは乱数 RND を生成し，パスワード PW と特徴点 S を乱数 RND で暗号化する. 乱数 RND を IC カード公開鍵 Pux で暗号化する.
④ 暗号化した乱数 RND，パスワード PW，特徴点 S を IC カードへ送信する.
⑤ IC カードでは IC カード秘密鍵 Prx を用いて乱数 RND を取得し，取り出した乱数 RND を用いてパスワード PW，特徴点 S を取得する. IC カード内のパスワード PW，生体情報テンプレート T を用いてユーザ認証を行う.
⑥ 乱数 RND をサーバ公開鍵 PuS で暗号化し，IC カードの ID を追加する．このデータにディジタル署名を付加しサーバに送信する.
⑦ パケットを受信したサーバは，IC カードの ID からサーバに保存された IC カード公開鍵 Pux を読み出しディジタル署名の検証を行う．その後サーバ秘密鍵 PrS を用いて乱数 RND を取得する.
⑧ 重要情報 D を乱数 RND で暗号化し，このデータのディジタル署名を付加しクライアントへ送信する.
⑨ パケットを受信したクライアントは，サーバ公開鍵 PuS を用いてディジタル署名の検証を行い，その後乱数 RND を用いて復号し重要情報 D を取得する.

以後の通信は配送された重要情報 D に含まれる暗号鍵を用いて暗号通信などを行うことが可能となる.

以上より，IC カード/クライアント，IC カード/サーバ，クライアント/サーバの各間での認証と暗号化を行うことが可能となる.

4. 実装

図 5 にサーバおよびクライアントにおける試作の実装の概要を示す. 今回は動作確認のため，IC カードはクライアント内の仮想プログラムとして動作させ，生体情報の代わりにパスワードによるマッチング処理を行うこととする. 表 2 に各モジュールの機能を示す. 暗号化および認証動作には，OpenSSL ライブラリを利用する[12].

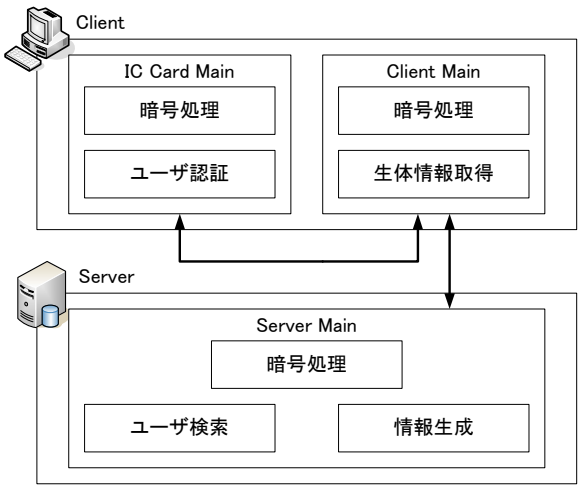

図 5　実装の概要
Fig.5 Outline Figure of Implementation

表 2　試作システムのモジュールと主な機能
Table.2 Function of the trial system

モジュール	機能
メイン	IC カード，クライアント，サーバにおいて状態を管理し，一連の処理を組み立てる．必要に応じてサブモジュールを呼び出す.
暗号処理	OpenSSL を利用して暗号/復号，ディジタル署名の生成/検証，ハッシュ生成の処理を行う.
認証情報取得	パスワードおよび生体情報の読み取りを行う.
ユーザ認証	パスワードおよび生体情報のマッチング処理を行う.
ユーザ検索	ユーザ ID からユーザ公開鍵を取得する.
情報生成	ユーザごとに適切な重要情報を生成する.

5.　まとめ

本論文では，非接触 IC カードを用いてサーバからクライアントに重要情報を配送するプロトコルである SPAIC の提案を行った.

非接触 IC カードを用いて IC カード/クライアント，IC カード/サーバ，クライアント/サーバの各間で暗号通信を行うことにより，クライアントが初期情報を持たなくとも安全に重要情報を配送することを可能にした.

本方式では公開鍵暗号方式を利用しているので継続的な通信には向かないが，初期の重要情報の配送において十分に利用できる.

今後は OS のログイン動作などと連携し，ユーザがより簡単に利用できる方法について検討していく予定である.

文　献

[1] Richard E. Smith (著)，稲村(訳)，“認証技術　ーパスワードから公開鍵までー”，オーム社

[2] 瀬戸，“ユビキタス時代のバイオメトリクスセキュリティ”，日本工業出版

[3] 渡邊，岡崎，朴，井手口，笹瀬“イントラネット閉域通信グループの構築に適した安全な鍵配送方式とその運用管理方式”電気学会論文誌 C　Vol.121-C，No.9 Sep.2001

[4] 妹尾，厚井，貞包，中谷，馬場，鹿間，“生体認証によるネットワーク個人認証システム”情報処理学会論文誌 Vol.44 No.4 Apr. 2003

[5] 磯部，三村，瀬戸，菊池，“本人認証 IC カードによる高セキュリティシステムの構築”，情報処理学会コンピュータセキュリティ研究報告 99-CSEC-4 Vol.99, No.24 pp.55-60 (1999)

[6] 石田，三村，瀬戸，“IC カード実装型指紋照合装置の開発”，コンピュータセキュリティ研究報告　2000-CSEC-10　Vol.2000 No.68 pp.145-152 (2000)

[7] 飯野，岩瀬，坂野，中嶋，“指紋照合機能搭載 IC カードによる本人認証方式”，情報処理学会コンピュータセキュリティ研究報告　2000-CSEC-10　Vol.2000　No.68 pp.153-158 (2000)

[8] 坂倉，長嶋，辻井，“DNA バイオメトリックス本人認証システム”，情報処理学会コンピュータセキュリティ研究報告 2002-CSEC-16, Vol.2002, No.12 pp.97-102 (2002)

[9] 影井，“IC カードの動向”，情報処理学会会誌 Vol.39 No.5　May. 1998

[10] 吉田，平田，“IC カードの現状と課題”，情報処理学会会誌 Vol.43 No.3 Mar. 2002
[11] 伊藤，“非接触 IC 技術とその応用”，情報処理学会会誌 Vol.43 No.3 Mar. 2002
[12] OpenSSL, http://www.infoscience.co.jp/technical/openssl/
[13] 保母，前羽，渡邊，“非接触 IC カードを利用した重要情報の配送手段に関する提案”，CSS2004 Vol.2004, No.11, pp.373-378, (2004)
[14] 渡邊，厚井，井手口，横山，妹尾，“暗号技術を用いたセキュア通信グループの構築方式とその実現” 情報処理学会論文誌，Vol.38，No.4 Apr. 1997
[15] 森川，青山，南，“ユビキタスネットワーキングへの道”，情報処理学会学会誌 Vol.43 No06 2002
[16] W. Polk，R. Housley，L. Bassham，” Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”，RFC3279 Apr. 2002
[17] D. Harkins，D. Carrel，” The Internet Key Exchange (IKE)”，RFC2409 Nov. 1998