IC カードを用いた重要情報の配送方式 SPAIC の検討

保母　雅敏　　渡邊　晃
名城大学大学院　理工学研究科

Researches on SPAIC: Secure Protocol for Authentication with IC Card

Masatoshi Hobo　　Akira Watanabe
Graduate School of Science and Technology, Meijo University

1.　はじめに

クライアント/サーバ間通信において安全に情報を交換するためには，確実な認証と暗号化が不可欠である．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いる[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. IC カード内に認証に必要な情報を格納するため，クライアント端末内にユーザの情報を保存することなく認証と情報配送を行うことが可能である．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行う必要がある．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，この間での認証と暗号化が必要となる．この際，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一切所持させないことが望ましい．これは，ユーザが端末を選べるという利便性だけでなく，端末から認証情報が盗まれるのを防止するという意味もある．しかし，実際にサーバからの重要情報が必要となるのはクライアントであるため，何の情報も持たないクライアントとサーバ間をどのように認証するかについて新たなモデルを定義し検証する必要がある．

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)を再検討した[12]．SPAIC では，IC カード公開鍵を IC カード自身に保存させる．この IC カード公開鍵を利用して，IC カードがクライアント(ユーザ)を認証するユーザ認証を行う．同様に IC カード秘密鍵を利用して，サーバが IC カードを認証する IC カード認証を行う．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し，この乱数を利用することでクライアント/サーバ間の認証を行う．以上の３つの経路の認証によって，クライアント/サーバ間の確実な認証を実現する．

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．

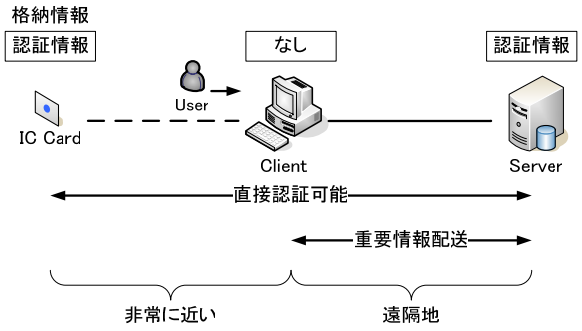

図 1 想定するシステムモデル
Fig.1Assumed System Model

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．従来の認証モデルとは異なり，クライアントには IC カード認証とユーザ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，ユーザは特定のクライアント端末に縛られず, 自由に選択することが可能となる．また，個人の認証情報がクライアント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．IC カード/クライアント間はユーザが確認できる程の近距離であるため，中間者攻撃(Man-in-the-middle Attack)は発生しないものとする．また，認証に生体情報読み取り装置などを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が可能である. 一方クライアント/サーバ間は遠隔地にあるため，中間者攻撃に耐えられる必要がある．

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ための認証には別の手段が必要である．以降, IC カードの持ち主を確認する認証をユーザ認証，正規の IC カードであることを確認する認証を IC カード認証と呼ぶ.

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，ユーザ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型認証モデルと IC カード内に情報を格納して認証を行うクライアント型認証モデルに分けられる(図 2).

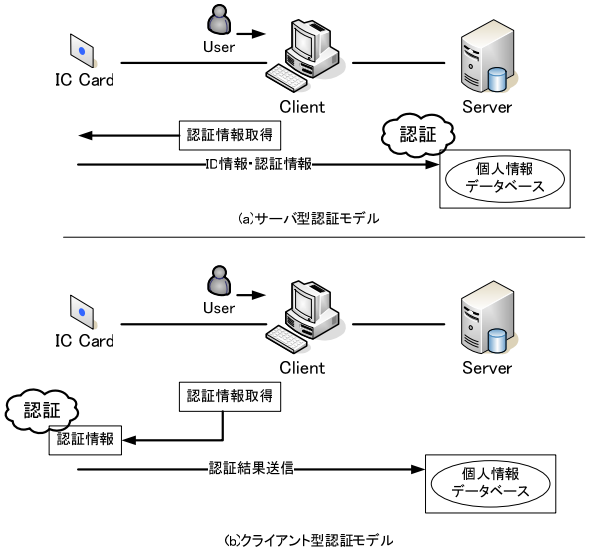

図 2　IC カードを用いたユーザ認証モデル
Fig.2 Authentication Model Using IC Card

サーバ型認証モデルは，ユーザとサーバ間で直接認証を行うエンドエンドのユーザ認証である．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ユーザ認証と IC カード認証を一括して行うため，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といった対策が必要となる可能性がある．

クライアント型認証モデルは，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 カード内でユーザ認証を行い，その後 IC カード/サーバ間で IC カード認証を行う．この方法ではサーバにおける IC カード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などのユーザ認証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.　システムモデルにおける課題

想定するシステムモデルには 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パスワードなどの情報を 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，クライアントが情報を一切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．

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

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．SPAIC で特徴的なのは，IC カード公開鍵を IC カードに初期情報として格納することである．

3.1.　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(IDx)，秘密鍵 Prx/公開鍵 Pux，サーバ公開鍵 PuS，ユーザパスワード情報 P，生体情報テンプレート T を所持している．サーバでは，サーバ秘密鍵 PrS，各 IC カードの ID と公開鍵 Pux 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．

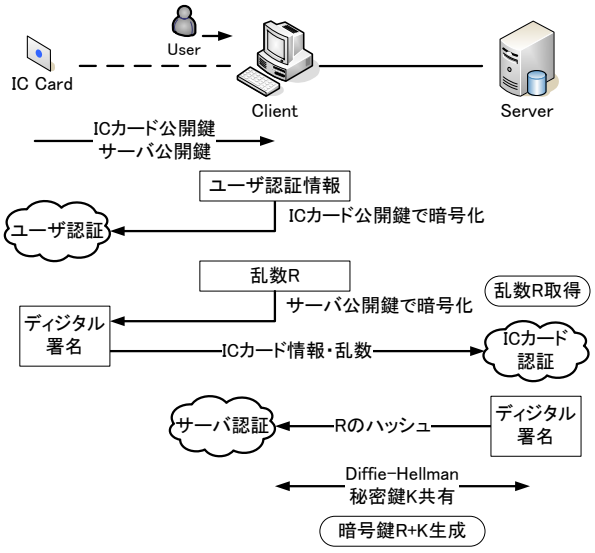

図 3　SPAIC の概要
Fig.3 Outline of SPAIC

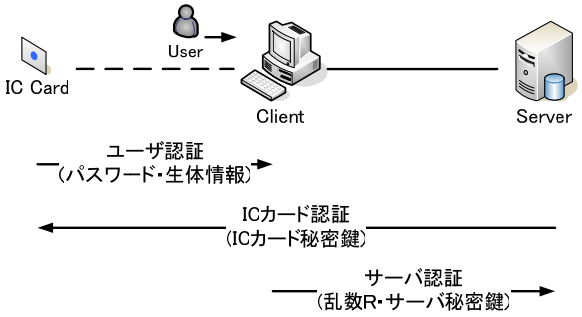

図 4　認証の関係
Fig.4 Relation of Authentication

3.2.　SPAIC の概要

SPAIC の概要を図 3 に示す．まず 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．次に，クライアントにユーザパスワード PW を入力し，同時に生体情報を入力して特徴点 S を得る．クライアントではパスワード PW と特徴点 S をユーザ認証情報として IC カード公開鍵 Pux で暗号化する．更に乱数 R を生成しサーバ公開鍵 PuS で暗号化し，これらの情報を IC カードへ送信する．

IC カードでは IC カード秘密鍵 Prx を用いてユーザ認証情報を取り出し，ユーザ認証を行う．その後，暗号化された乱数 R とユーザ ID にディジタル署名を付加し，サーバに送信する．

サーバでは保存された IC カード ID から対応する公開鍵 Pux を読み出し，ディジタル署名の検証を行い，IC カードを認証する．次に，サーバ秘密鍵 PrS を用いて乱数 R を取得する．そして取得した乱数 R のハッシュを取り，ディジタル署名を付加してクライアントへ送信する．

クライアントでは，事前に取得したサーバ公開鍵 PuS を利用してディジタル署名の検証を行う．更に自身が生成した乱数 R のハッシュを取り比較を行い，サーバを認証する．その後，クライアント/サーバ間で Diffie-Hellman 鍵交換を行い，秘密鍵 K を共有する．以上によって共有された R と K から暗号鍵 R+K を生成する．

サーバは重要情報 D を暗号鍵 R+K で暗号化し，クライアントへ送信する．クライアントでは，暗号鍵 R+K を用いて重要情報 D を取得する．

以上より，クライアントへ安全に重要情報 D を配送することが可能となる．

3.3.　認証の関係

SPAIC で行う認証の関係を図 4 に示す．IC カードはパスワードや生体情報を用いてユーザ認証を行うことでクライアント(ユーザ)を認証する．サーバは IC カード秘密鍵から作成されたディジタル署名を利用することで IC カードを認証し，間接的にクライアントを認証する．クライアントはサーバと共有した乱数 R とサーバ秘密鍵から作成されたディジタル署名を利用することでサーバを認証する．

以上の 3 つの経路の認証により，クライアント/サーバ間で確実な認証を行うことが可能となる．

4.　実装

サーバおよびクライアントにおける実装の概要を図 5 に，各端末のモジュールと主な機能を表 2 に示す．今回は動作確認の試作であるため，IC カードの処理はクライアント内で仮想プログラムとして動作させる．ユーザ認証情報はパスワードのみを利用する．また，暗号および認証動作には，OpenSSL ライブラリを利用する[13].

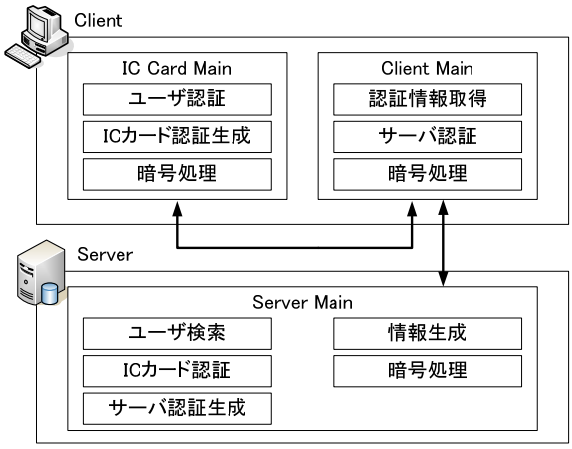

図 5　実装の概要
Fig.5 Outline Figure of Implementation

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
Client	メイン	クライアント処理の組立
	認証情報取得	ユーザ認証情報の取得
	サーバ認証	サーバ認証を行う
	暗号処理	暗号/復号処理
IC Card	メイン	IC カード処理の組立
	ユーザ認証	パスワードや生体情報の認証処理
	IC カード認証生成	IC カード認証の情報生成
	暗号処理	暗号/復号, ディジタル署名生成
Server	メイン	サーバ処理の組立
	ユーザ検索	IC カード公開鍵の取得
	IC カード認証	IC カード認証を行う
	サーバ認証生成	サーバ認証のための情報生成
	情報生成	重要情報の生成
	暗号処理	暗号/復号, ディジタル署名生成/検証

クライアントの処理は，状態を管理し一連の処理を組み立てるメインモジュール，パスワードや生体情報などの取得を行う認証情報取得モジュール，サーバを認証するためのサーバ認証処理，暗号/復号の処理を行う暗号処理モジュールより構成される．IC カードの処理は，状態を管理し一連の処理を組み立てるメインモジュール，ユーザ認証を行うユーザ認証処理，IC カード認証のための情報を生成する IC カード認証生成処理，暗号/復号やディジタル署名の生成を行う暗号処理より構成される．サーバの処理は，状態を管理し一連の処理を組み立てるメインモジュール，IC カード ID より IC カード公開鍵を取得するユーザ検索処理，IC カードを認証するための IC カード認証処理，サーバ認証のための情報を生成す

るサーバ認証生成処理，ユーザごとに適切な重要情報を生成するための情報生成処理，暗号/復号やディジタル署名の生成/検証処理を行う暗号処理モジュールより構成される．

5. まとめ

本論文では，クライアント端末が初期情報を所持しないというモデルを定義し，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 SPAIC の検討を行った．

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/サーバの各間で確実な認証と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　－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] 保母，渡邊，“ＩＣカードを用いた重要情報の配送方式”，2005-CSEC-28 Vol.2005, No.33, pp.229-234, (2005)

[13] OpenSSL, http://www.infoscience.co.jp/technical/openssl/

[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