目次

概要

ユーザが自由に移動する環境においても，認証と暗号化により確実な情報配送を行いたいという要求がある．このような環境では，ユーザ固有の情報を格納した IC カードを利用する方式が主流である．従来のシステムでは，接触型 IC カードを利用する場合がほとんどであり，IC カード/クライアント間通信の検討が不十分であった．しかし，今後は非接触型 IC カードの普及が見込まれ，IC カード/クライアント間でも暗号通信を行うことが必須になると考えられる．これを実現するためには,すべての IC カードとクライアントに同じ共通鍵を所持させるという方法があるが，クライアントからの情報流出の可能性があった．

本論文では，非接触型 IC カードを利用し，初期情報を一切持たないクライアントに重要情報を配送することを可能とするプロトコル SPAIC(Secure Protocol for Authentication with IC card)を提案する．

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]-[12]．近年ではユーザが自由に移動するケースが増えており，このような環境においても同様に認証と暗号化による情報配送を行えることが望ましい．

このような要求を満たす方式として，ユーザが IC カードを所持する方式が注目されている[13]-[19]．IC カード内には認証に必要な情報を安全に格納することが可能で，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，端末からユーザの情報が盗まれるのを防止するという利点もある．近年では，非接触型 IC カードの登場によって，IC カードの利便性が一層向上することが期待されている．

IC カードを利用した認証方式では，クライアント/サーバ間で行われる認証に加えて，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，クライアントから入力され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．これらの認証処理に必要な情報を安全にやりとりするためには，IC カードとクライアント間の暗号通信が必要である．従来のシステムでは，暗号通信を行うために，すべての IC カードおよびクライアントに共通鍵を所持させる方式がある[20]．しかし，この方式ではクライアント側から共通鍵が漏洩した場合，影響がシステム全体に波及する可能性がある．クライアントは IC カードのような耐タンパ性がないのが一般的であるため，秘密情報を一切所持させない方法が望ましい．そこで，IC カード，クライアント，サーバがあらかじめどのような初期情報を所持し，どのような手順で認証や暗号化を行うべきかについて検証を行った．

本論文では，非接触型 IC カードを利用し，初期情報を一切持たないクライアントに重要情報を配送することを可能とするプロトコル SPAIC(Secure Protocol for Authentication with IC card)を提案する．SPAIC では，IC カード公開鍵を IC カード自身に格納する．この IC カード公開鍵を利用して，クライアントから IC カードへの通信の暗号化を行う．また，IC カードに格納されているサーバ公開鍵を利用して IC カードからクライアントを経由し，サーバまで通信の暗号化を行う．更に，クライアント/サーバ間で Diffie-Hellman 鍵交換[21]を行うことにより，動的に暗号鍵を生成し，サーバから安全に重要情報を配送することを実現する．

以降，２章で想定システムの構成，３章で従来システムとその課題，４章で提案方式，５章で評価，６章でまとめを述べる．

2. 想定システムの構成

2.1. 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．このシステムはサーバからクライアントへ暗号鍵など第三者に見られたくない重要情報を安全かつ確実に配送するための通信経路を確立することを目的としている．ユーザは個人情報を格納した IC カードを所持していることを前提とする．

各クライアントには 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．ユーザ認証後，IC カードとサーバの間で相互認証を行い，クライアントへ重要情報を配送する．

IC カードと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．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．

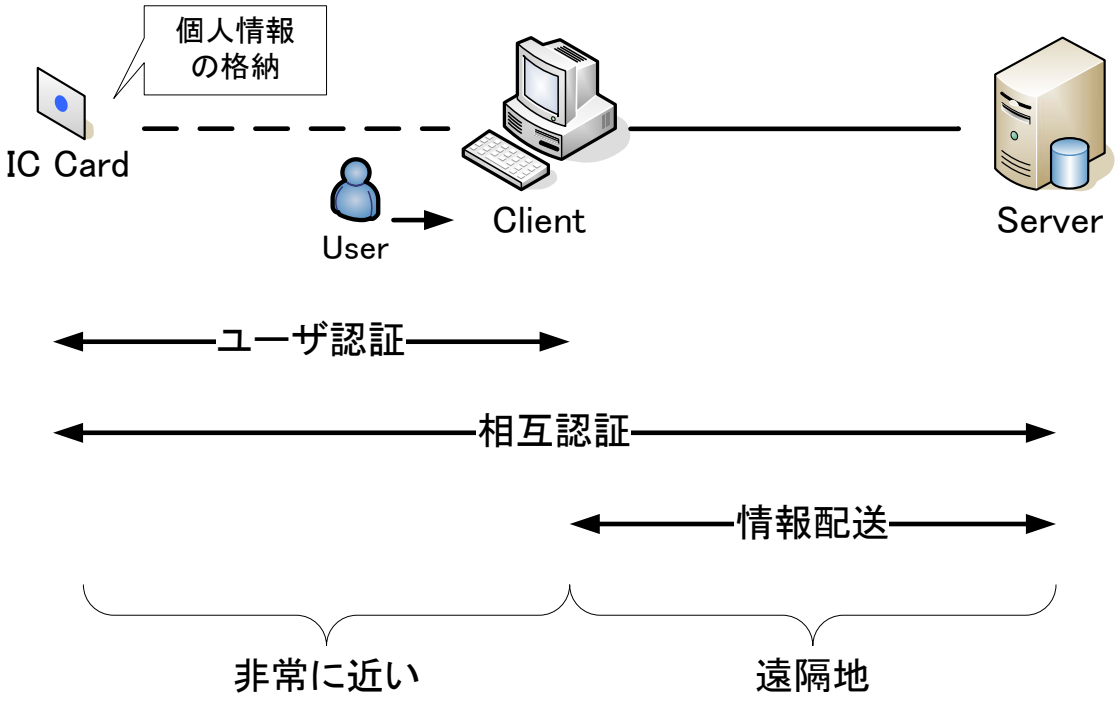


図 1　想定するシステムモデル

2.2. ユーザ認証方式

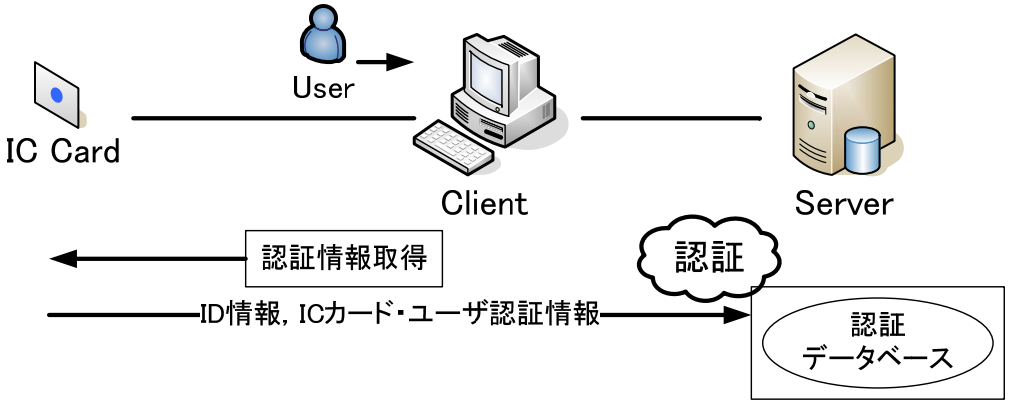
IC カード/サーバ間では PKI（Public Key Infrastructure：公開鍵認証基盤）などの仕組みを用いて確実な認証を行う．このため，IC カード内には公開鍵暗号方式における秘密鍵といった個人を特定するための情報が格納されている．この認証を「IC カード認証」と呼ぶ．しかし，IC カードの正当な持ち主を確認するためには上記とは別の手段が必要となる．この認証を「ユーザ認証」と呼ぶ．

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，生体認証などと組み合わせる．このとき，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に分けられる(図２)．

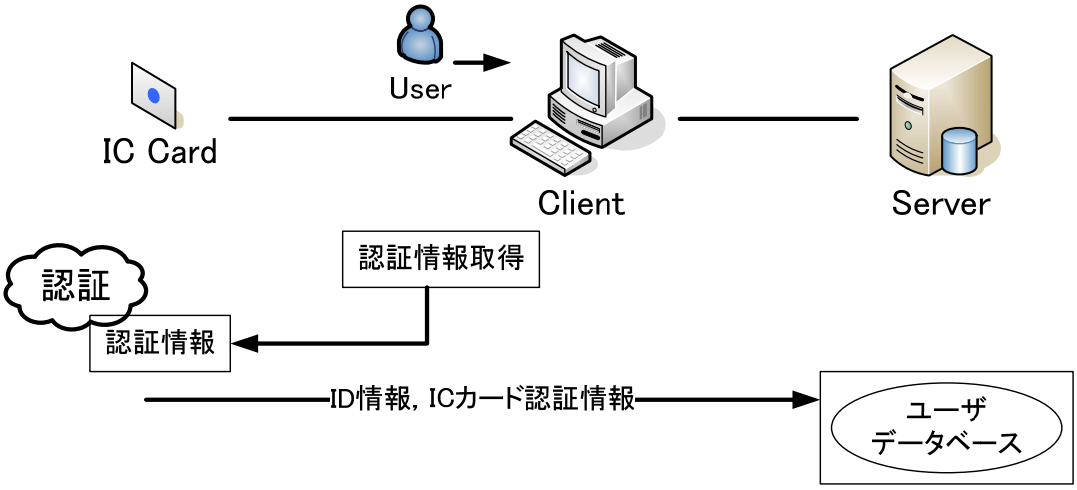
サーバ型認証は，ユーザとサーバ間で直接認証を行うエンドエンドのユーザ認証である．クライアントで取得した認証情報を，IC カードを経由してサーバへ送信して認証を行う．この認証方式ではサーバ側でユーザ認証と IC カード認証を一括して行うため，IC カードの処理負荷を軽減できるというメリットがある．しかし，ユーザ全員の情報をサーバ側で一括して管理するため，サーバの管理体制が重要となる．このため，大規模な耐タンパハードウェアを用いる，厳重な設備を準備するといった対策が必要となる可能性がある．

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．この認証方式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 カードに掛かる処理負荷が大きくなる．

どちらの認証方式においても，安全に個人認証を行うことが可能である．本論文ではユーザ認証と IC カード認証を独立して扱うことができ，簡単に安全性が達成できるクライアント型認証を採用する．



(a)サーバ型認証



(b)クライアント型認証

図２　ユーザ認証方式

3. 従来システムとその課題

従来システムで保持すべき初期情報を表１に示す.各ユーザが所持する IC カードには, IC カード固有の ID（IDx), IC カード秘密鍵（Prx), サーバ公開鍵（PuS), ユーザ認証に利用するパスワード（PW), 生体情報テンプレート（T）が格納されている．サーバには，サーバ秘密鍵（PrS)，各 IC カードの ID（IDx）と公開鍵（Pux）が格納されている．

IC カード/クライアント間の通信には，クライアントから入力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（図３）．このため，クライアントから IC カードへの通信は暗号化することが望まれる．特に，非接触型 IC カードを利用する場合には IC カード/クライアント間が無線通信となるため，暗号化による通信が一層重要になる．

従来システムでは,接触型 IC カードをクライアントに挿入して利用するような場合がほとんどであるため, IC カードとクライアントが一体のものであるとみなし，IC カード/クライアント間の暗号通信を行っていないものが殆どである．暗号化が必要な場合には，暗号通信の種となる共有鍵 K をすべての IC カード，クライアント端末に所持させる事前共有鍵方式が考えられている．この方式では，共有鍵 K を用いて IC カード/クライアント間で暗号通信を行うための暗号鍵をダイナミックに生成する．

事前共有鍵方式では，クライアントに秘密情報を所持させる必要があるため，クライアントからの情報漏洩の危険性がある．更に，システム全体で同じ事前共有鍵 K を所持しているため，この共有鍵が漏洩した場合，その影響がシステム全体に波及するおそれがある．このため，システムの安全性を確保するためにはすべての IC カード,クライアント事前共有鍵を定期的に変更する作業が必要となると考えられ，管理が煩雑となる．

表１　事前共有鍵方式の初期情報

IC カード	IDx：IC カード ID Prx：IC カード秘密鍵 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 ***K：事前共有鍵***
クライアント	***K：事前共有鍵***
サーバ	PrS：サーバ秘密鍵 IDx：IC カード ID Pux：IC カード公開鍵

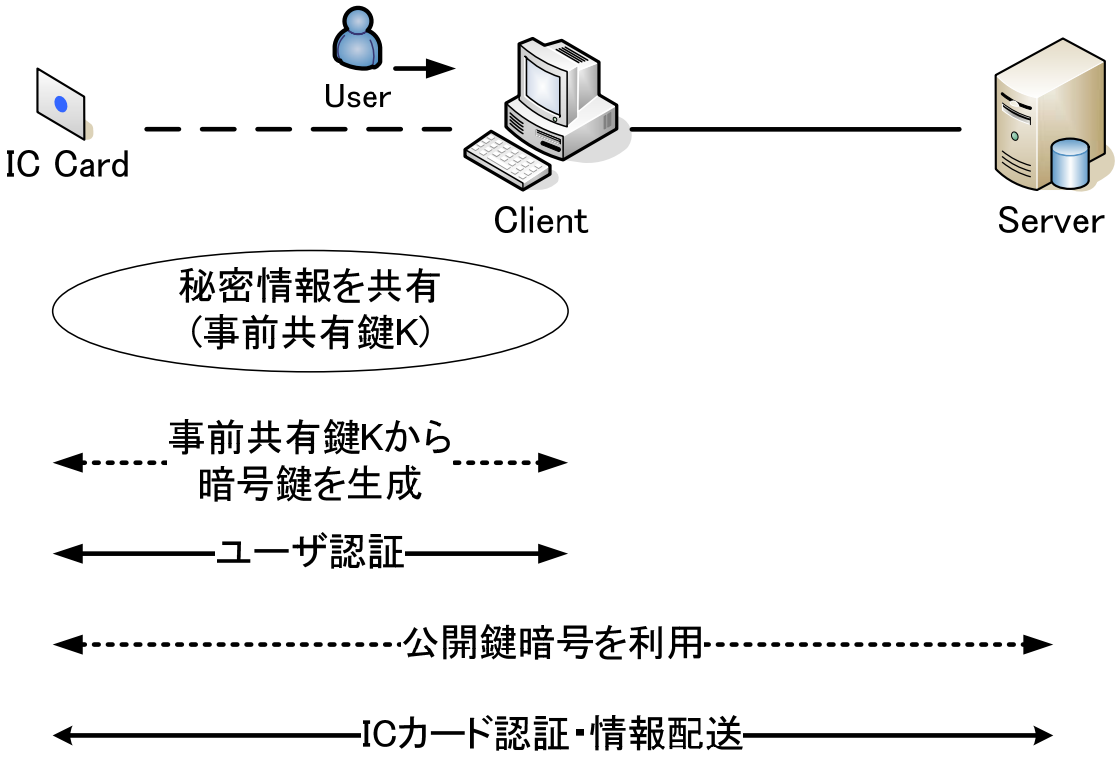


図３　事前共有鍵方式

4. SPAIC

本章では，事前共有鍵方式の課題を解決するために，クライアントに秘密情報を一切所持させないまま，サーバからクライアントへの重要情報の配送を可能とする SPAIC（Secure Protocol for Authentication with IC card）を提案する．

4.1. SPAIC の概要

SPAIC では今後の普及を考え，非接触型 IC カードを利用することを前提とする．また，クライアントには認証動作を行うプログラムだけを格納し，認証に必要となる初期情報は一切所持させない．このためクライアントからの情報漏洩の心配がない．IC カードに格納する初期情報として，事前共有鍵に代わり，新たに IC カード公開鍵を初期情報として格納する．

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によりクライアント(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と自身が生成した乱数 Nr を検証することにより 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秘密鍵から作成されたディジタル署名を検証することによりサーバを認証する．

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．

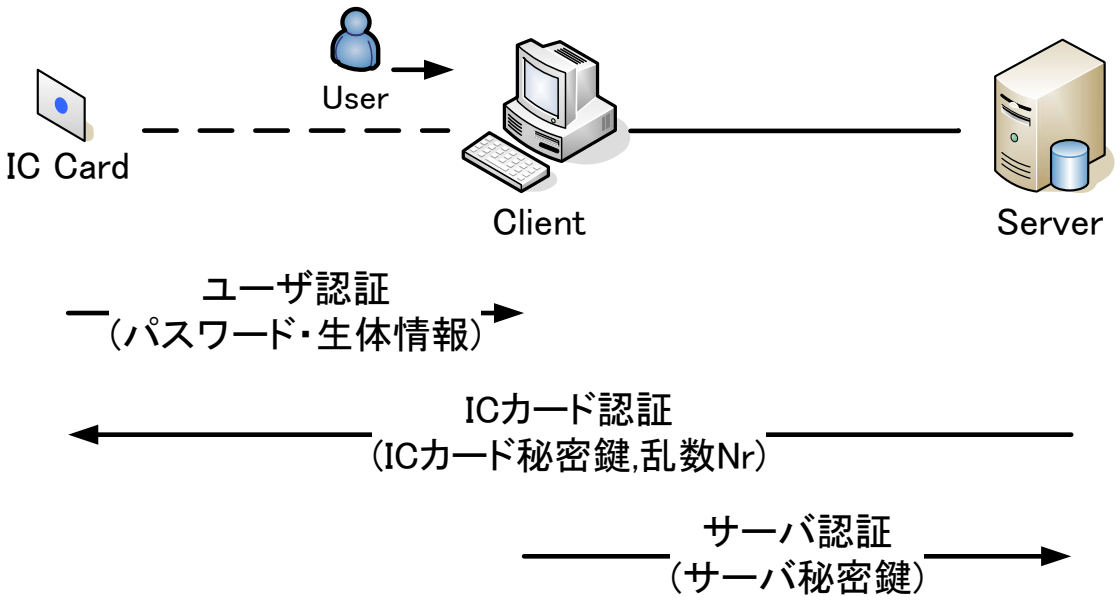


図 4　認証の関係

4.2. 各端末の初期情報

各端末が所持する初期情報を表２に示す．ユーザ認証にはパスワードと生体認証を用いる． 各ユーザが所持する IC カードには，IC カード固有の ID(IDx)，秘密鍵 Prx，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 に加え，新たに IC カード公開鍵 Pux を格納する．クライアントは初期情報を一切所持しない．サーバには，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．

表２　SPAIC の初期情報

IC カード	IDx：IC カード ID Prx：IC カード秘密鍵 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 ***Pux：IC カード公開鍵***
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

4.3. SPAIC の動作

SPAIC の動作概要を図５に示す．ユーザは，ユーザ認証に必要となるユーザパスワードや生体情報を入力クライアントに入力する．IC カードからクライアントへは IC カード公開鍵，サーバ公開鍵を送信する．これらの情報はもともと公開されるべき情報であるため，外部へ漏れても何ら問題とはならない．クライアントではパスワード等のユーザ認証情報を IC カード公開鍵で暗号化する．更に Diffie-Hellman 鍵交換の交換値（DH 交換値）を生成し，サーバ公開鍵で暗号化する．これらの情報を IC カードへ送信する．

IC カードでは IC カード秘密鍵を用いてユーザ認証情報を取り出し，内部に保持している秘密情報と照合することによりユーザ認証を行う．その後，IC カード秘密鍵を用いて，サーバ公開鍵で暗号化されている情報にディジタル署名を付加し，クライアント経由でサーバへ送信する．

サーバでは IC カード認証を行うために，受信した IC カード ID から対応する IC カード公開鍵を読み出す．この公開鍵を用いてディジタル署名の検証を行う．次に，サーバ秘密鍵を用いて DH 交換値を取得する．その後，DH 交換値を生成し，サーバ秘密鍵を用いて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を利用してディジタル署名の検証を行う． その後 DH 交換値を取得する．

クライアント，サーバは Diffie-Hellman 鍵交換によって得られた DH 交換値を用いて共通の暗号鍵を生成する．

以降のクライアント/サーバ間の暗号通信はこの暗号鍵を用いて行う．

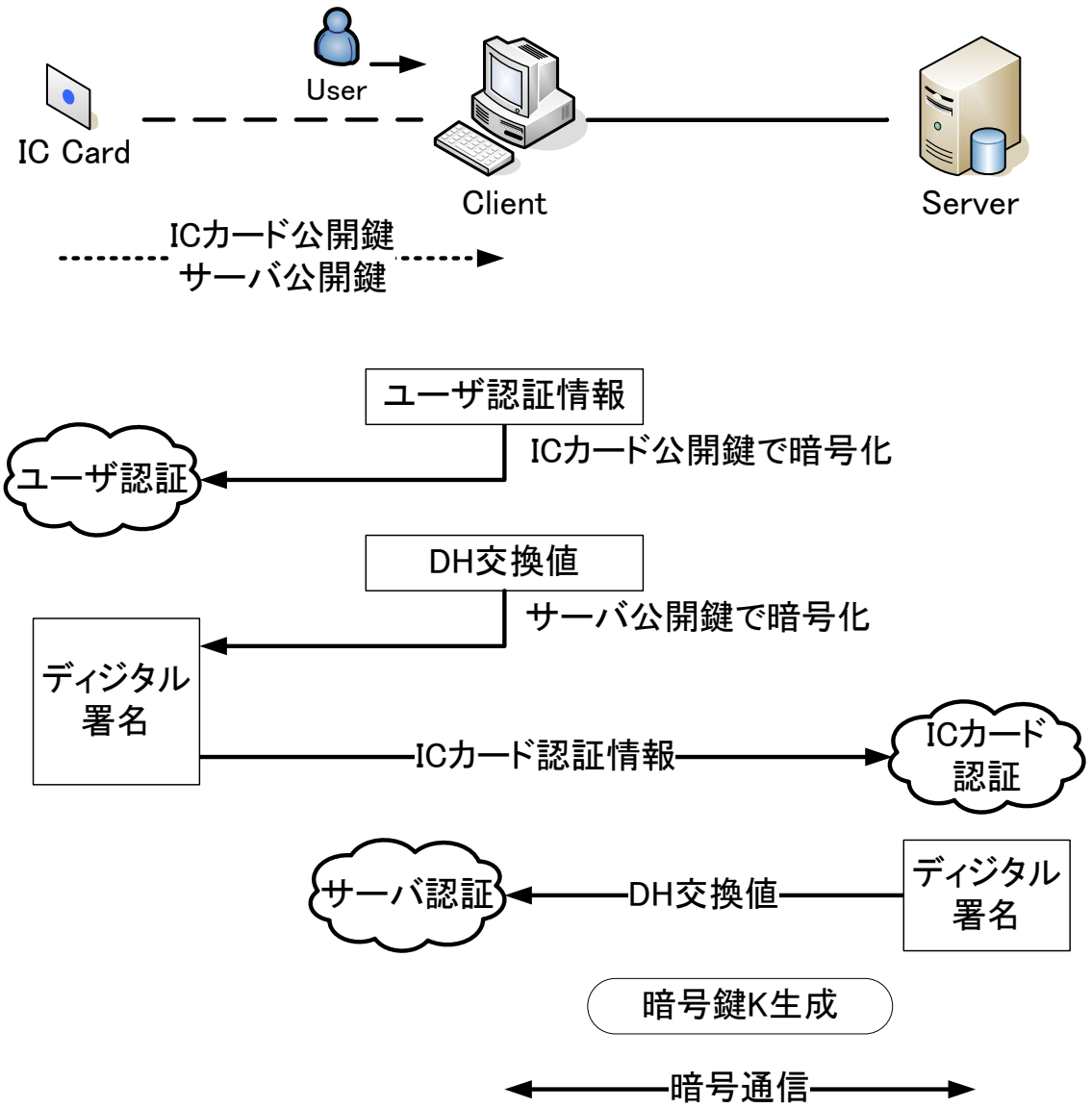

User
IC Card
Client
Server
ICカード公開鍵
サーバ公開鍵
ユーザ認証情報
ICカード公開鍵で暗号化
ユーザ認証
DH交換値
サーバ公開鍵で暗号化
ディジタル
署名
ICカード認証情報
ICカード
認証
サーバ認証
DH交換値
ディジタル
署名
暗号鍵K生成
暗号通信

図 5　SPAIC の概要

4.4. SPAIC のシーケンス

SPAIC の処理シーケンスを図 6 に示す．プログラム起動時にパスワード等のユーザ認証情報をクライアントに入力する．その後認証処理を開始する．

① IC カード情報要求

ユーザ認証情報などの暗号化を行うために，IC カードへ公開鍵等の情報配送を要求する．

② IC カード情報送信

ユーザ ID，IC カード公開鍵 Pux，サーバ公開鍵 PuS，チャレンジコードとなる乱数 Ni を送信する

③ クッキー生成要求

DoS 攻撃防止に利用するクッキーを生成するための要求をサーバへ送信する

④ クッキー，乱数 Nr の送信

ユーザ ID，クライアントの IP アドレスなどの情報をもとにクッキーを生成する．チャレンジコードとなる乱数 Nr と共にクライアントへ送信する

⑤ 認証情報の生成

IC カードから受け取った乱数 Ni のハッシュ値とクライアントに入力されたユーザ認証情報を Pux で暗号化する．同時に Diffie-Hellman 交換値 KEi とサーバから受け取った乱数 Nr を PuS で暗号化する．

Pux[PW, S, Hash(Ni)], PuS[KEi, Nr]

⑥ ユーザ認証要求

③で作成した情報を IC カードへ送信する．

⑦ ユーザ認証，IC カード認証情報の生成

IC カード秘密鍵 Prx を利用して PW，S を取り出しユーザ認証を行う．ユーザ認証後，PuS で暗号化した情報 ***PuS[KEi, Nr]***にユーザ ID を付加して，これらの情報のディジタル署名を作成する．

IDx, PuS[KEi, Nr], Cert

⑧ IC カード認証情報の送信

⑦で作成した IC カード認証情報をクライアントへ送信する．

⑨ IC カード認証要求

⑧で受信した IC カード認証情報を④で受信したクッキーの値と共にサーバへ送信する．

Cookie, IDx, PuS[KEi, Nr], Cert

⑩ IC カード認証，サーバ認証情報の生成

IC カード認証を行うために，ユーザ ID から該当する 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 を利用して KEi, Nr を取り出し，生成した Nr と比較する．

更に，Diffie-Hellman 交換値 KEr を生成し，サーバ認証を行うためのディジタル署名を作成する．

KEr, Cert

⑪ サーバ認証情報の送信

⑩で作成した情報をクライアントへ送信する

⑫ サーバ認証

あらかじめ受信した PuS を利用しディジタル署名の検証を行う．その後 KEr を取得する．

⑬ 暗号鍵の生成

KEi, KEr を利用して暗号鍵 K を生成する

認証システムにおいては，大量のパケットを送信してサーバをダウンさせるサービス拒否攻撃（DoS 攻撃），以前の通信内容を入手して同じ内容を送信するリプレイ攻撃への対応が重要となる．

DoS 攻撃に対しては，クライアント/サーバ間でクッキーの交換で対応する．クッキーは通信ごとに異なる値が生成されるため，IC カード認証時にクライアントからサーバへのパケットに含むことで無関係な端末からの DoS 攻撃を防止することができる．

リプレイ攻撃に対しては，クッキー交換時に送信される乱数 Nr の利用と，シーケンスの推移を管理することによって対応することができる．また，この乱数 Nr は，IC カード認証情報が認証時に作成されたものであるかどうかを確認するためにも利用する．

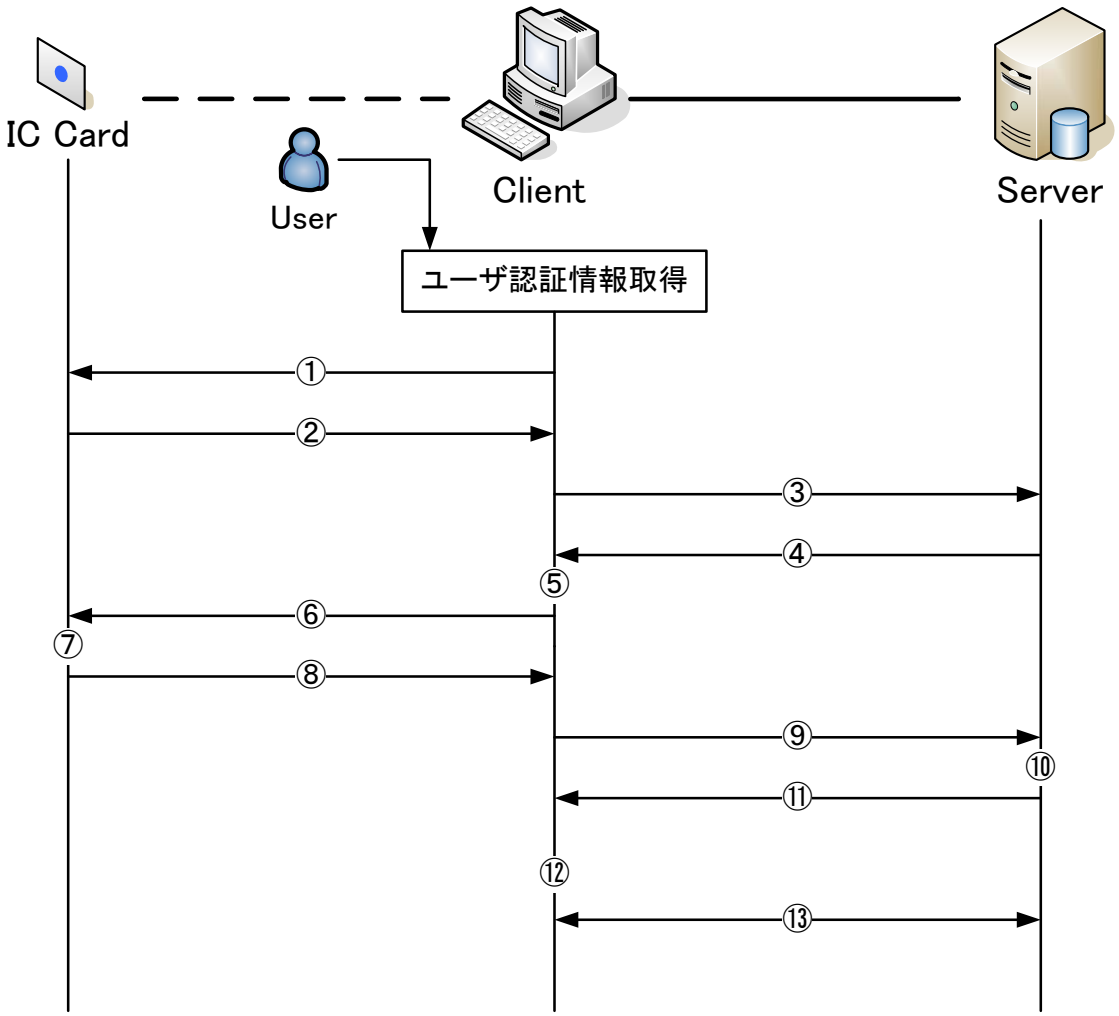


図 6　**SPAIC** の動作シーケンス

5. 評価

事前共有鍵方式と SPAIC との比較を表３に示す．SPAIC ではクライアント端末に格納する情報が動作プログラムのみであるため，クライアントからの情報漏洩の心配がないという利点がある．

ユーザ認証時の暗号化に公開鍵暗号方式を利用する SPAIC では，秘密情報を共有して暗号通信を行う事前共有鍵方式に比べ，IC カーヘドの処理負荷の増加が考えられる．しかし，SPAIC が動作するのは重要情報の配送を行うクライアントの立ち上げ時のみであるため，公開鍵暗号方式の利用は実用上大きな影響を与えるものではないと考えられる．

事前共有鍵方式では，システムの安全上事前共有鍵を頻繁に更新する必要があるため，運用時の管理が煩雑になる．一方 SPAIC ではユーザの追加，削除程度の作業で済むため，管理負荷の低減が見込まれる．

表３　従来システムとの比較

	事前共有鍵方式	SPAIC
クライアントに 格納する情報	動作プログラム 事前共有鍵 （×）	動作プログラムのみ （○）
IC カード/クライアント 間の暗号	事前共有鍵より 暗号鍵を生成 （○）	公開鍵暗号 （○）
IC カードへの負荷	中程度 （○）	高い （△）
運用時の管理負荷	共有鍵の交換が面倒 （×）	ユーザの追加，削除程度 （○）

6. まとめ

本論文では，事前共有鍵方式の課題であるクライアント端末からの情報漏洩を解決するために，クライアント端末が動作プログラム以外の初期情報を一切所持しないというモデルを定義し,非接触型 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ことを可能とするプロトコル SPAIC の検討を行った．

IC カード公開鍵を新たに IC カードに所持させることで，クライアントが初期情報を持たなくとも IC カード/クライアント間の暗号通信を行い，各間での確実な認証を可能にした．更に，クライアント/サーバ間で Diffie-Hellman 鍵交換で作成した暗号鍵を利用することで，安全に重要情報を配送するための通信経路を確立した．DoS 攻撃に対してはクッキー交換により，リプレイ攻撃には乱数 Nr の利用とシーケンスの推移を管理することによって対策をとった．

本方式では，IC カードで行う公開鍵暗号方式の処理のため，若干のパフォーマンスの低下が予想されるが，初期の重要情報の配送において十分に利用できる．

今後は実装を行い，より詳細な評価を行う予定である．

参 考 文 献

[1] J. Kohl, Digital Equipment Corporation, C. Neuman, “The Kerberos Network Authentication Service (V5)”, RFC1510 Sep. 1993

[2] T. Dierks, Certicom, C. Allen, Certicom, “The TLS Protocol Version 1.0”, RFC2246 Jan. 1999

[3] D. Maughan, National Security Agency, M. Schertler, Securify, Inc., M. Schneider, National Security Agency, J. Turner, RABA Technologies, Inc., “Internet Security Association and Key Management Protocol (ISAKMP)”, RFC2408 Nov. 1998

[4] D. Harkins, D. Carrel, “The Internet Key Exchange (IKE)”, RFC2409 Nov. 1998

[5] 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

[6] C. Kaufman, Ed., Microsoft, “Internet Key Exchange (IKEv2) Protocol”, RFC4306 Dec. 2005

[7] J. Schiller, Massachusetts Institute of Technology, “Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)”, RFC4307 Dec. 2005

[8] 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

[9] 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

[10] 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

[11] 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

[12] 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

[13] 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)

[14] 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)

[15] 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)

[16] 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)
[17] 影井，“IC カードの動向”，情報処理学会会誌 Vol.39 No.5　May. 1998
[18] 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
[19] 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
[20] IC カードシステム利用促進協議会，“JICSAP IC カード仕様書 V2.0”，Jul. 2001
[21] E. Rescorla，RTFM Inc.，“Diffie-Hellman Key Agreement Method”，RFC2631 June. 1999
[22] 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
[23] J. Myers，Netscape Communications，“Simple Authentication and Security Layer (SASL)”，RFC2222 Dec. 1997
[24] J. Schiller，Massachusetts Institute of Technology，“Strong Security Requirements for Internet Engineering Task Force Standard Protocols”，RFC3365 Aug. 2002
[25] S. Bellovin, Ed.，J. Schiller, Ed.，C. Kaufman, Ed.，Internet Architecture Board，“ Security Mechanisms for the Internet”，RFC3631 Dec. 2003

研　究　業　績

1) 保母雅敏，渡邊晃，“イントラネット閉域通信グループにおける鍵管理方式の提案”，電気関係学会東海支部連合大会，Oct. 2003
2) 保母雅敏，渡邊晃，“多段構成ネットワークにおける鍵配送方式の一検討”，情報処理学会全国大会，Mar. 2004
3) 保母雅敏，前羽理克，渡邊晃，“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”，コンピュータセキュリティシンポジウム（CSS2004），Oct. 2004
4) 保母雅敏，渡邊晃，“IC カードを用いた重要情報の配送方式”，情報処理学会コンピュータセキュリティ研究会，Mar. 2005
5) 保母雅敏，渡邊晃，“IC カードを用いた重要情報の配送方式 SPAIC の検討”，マルチメディア，分散，協調とモバイル（DICOMO2005）シンポジウム，Jul. 2005
6) 坂野文男，保母雅敏，渡邊晃，“企業ネットワークにおける認証基盤の構築に関する研究”，電気関係学会東海支部連合大会，Sep. 2004
7) 坂野文男，保母雅敏，渡邊晃，“企業ネットワークにおける認証基盤の構築に関する研究”，電気関係学会東海支部連合大会，情報処理学会全国大会，Mar. 2005
8) 坂野文男，保母雅敏，渡邊晃，“企業ネットワークにおける認証基盤構築の一方式”，マルチメディア，分散，協調とモバイル（DICOMO2005）シンポジウム，Jul. 2005
9) 坂野文男，保母雅敏，渡邊晃，“企業ネットワークにおける管理負荷の少ない認証システムＡＳＥの提案”，暗号と情報セキュリティシンポジウム（SCIS2006），Feb. 2006

謝　辞

本研究を進めるにあたり，多大なる御指導，御鞭撻を賜わりました名城大学大学院理工学研究科　渡邊晃教授に心より厚く御礼申し上げます．とりわけ，御多忙の中御時間の許す限り御相談に乗って頂きましたことに，深い感謝の念を表します．

本研究を進めるにあたり，研究内容に関して御熱心な御指導，御教示を賜わりました名城大学大学院理工学研究科　小川明教授，山本新教授，宇佐見庄五講師に心より厚く御礼申し上げます．

また，本研究を進めていく上で様々な御助言，御検討を頂きました名城大学大学院理工学研究科情報科学専攻　渡邊研究室の皆様に深く感謝いたします．

最後に，研究を進めていく中，いつも暖かく支えて頂いた御両親に心から感謝いたします．