IC カードを用いた重要情報の配送方式 SPAIC の検討

043432037　保母雅敏
渡邊研究室

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．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．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も暗号化されることが望ましい．特に，非接触 IC カードでは，暗号化が必須となる．このような要望を満たす方法として，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．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．

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，本来サーバ側だけが保持していれば良かった IC カード公開鍵を IC カード自身にも格納する．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可能とする．SPAIC では非接触 IC カードを用いていても，サーバから安全に重要情報を配送することが可能である．

2. 想定システム

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する．ユーザは個人情報を格納した非接触 IC カードを所持していることを前提とする．

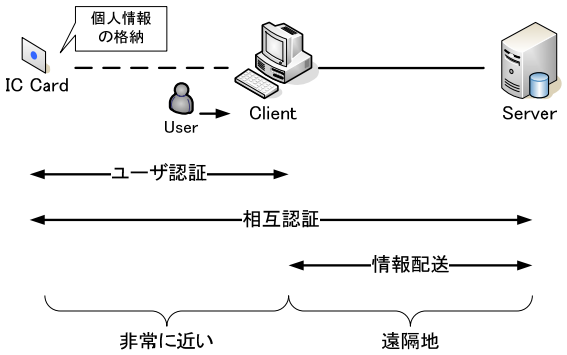


図 1　想定するシステムモデル

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．

3. 従来システムの課題

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可能性がある．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．

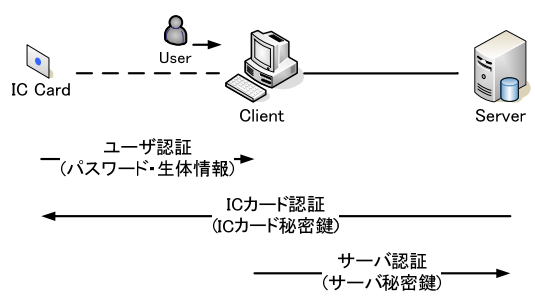


図２　認証の関係

4. SPAIC

4.1 SPAIC の概要

SPAIC では非接触型 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．

SPAIC で行う認証の関係を図２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できる．これを実現するために，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．

4.2 SPAIC の動作

SPAIC の動作概要を図３に示す．ユーザは，ユーザ認証情報となるユーザパスワードや生体情報を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．公開鍵はもともと公開されるべき情報であるため，これらが盗聴されても何ら問題とはならない．クライアントではユーザ認証情報を 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い，クライアントを認証する．次に，サーバ秘密鍵を用いて

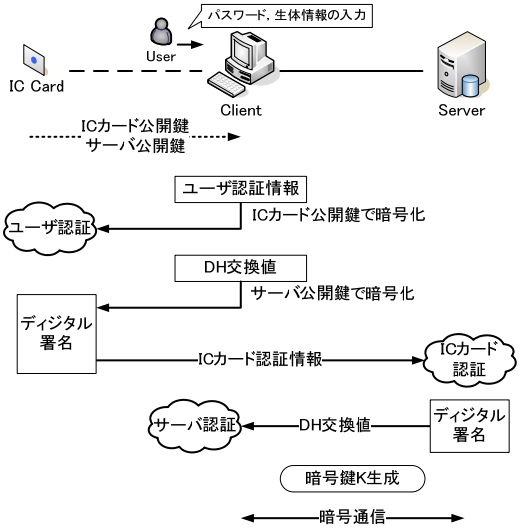


図３　SPAIC の概要

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，事前に所持しているサーバ公開鍵を利用してディジタル署名の検証を行い，サーバを認証する．その後 DH 交換値を取得する．

クライアント，サーバは上記手順で得られた 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．

5. まとめ

本論文では，事前共有鍵方式においてクライアント端末からの情報漏洩の問題を解決するために，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 の提案を行った．

IC カード公開鍵を新たに IC カードに所持させることにより，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，IC カード/クライアント/サーバ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により，安全に重要情報を配送するための通信経路を確立した．

SPAIC は，非接触 IC カードを利用したシステムにおける有効な手段である．

今後は実装を行い，詳細な評価を行う予定である．

参考文献

[1] 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

[2] 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

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

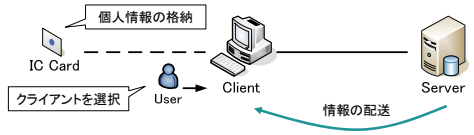
ICカードを用いた重要情報の配送方式 SPAICの検討

名城大学大学院理工学研究科
情報科学専攻
渡邊研究室
043432037　保母雅敏

はじめに

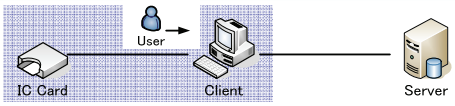
- クライアント/サーバ間の情報配送
  - 安全な通信の要求
  - 認証と暗号化による情報配送
  - ユーザが自由に端末を選択する環境
- ICカードを利用した認証
  - カード内で暗号・認証処理が可能
  - 外部からの不正読み取りを防ぐ耐タンパ性
  - 非接触ICカードの登場による利便性の向上

ICカードを利用した情報配送



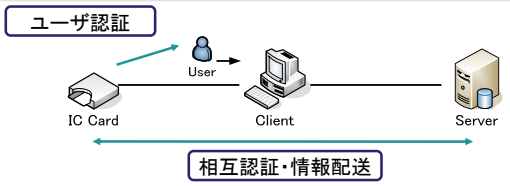
- ICカード内に個人を特定する情報を格納
  - 公開鍵暗号の秘密鍵などの情報
  - クライアントからの情報漏洩を防ぐ
  - ユーザはクライアントを自由に選択
- クライアントへの安全な情報配送
  - 他端末との通信に必要な暗号鍵など

従来のICカードモデル



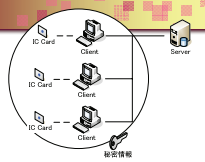
- 接触型ICカードの利用が多い
  - ICカードとクライアントを一体とみなす

従来のICカードモデル



- ICカードと持ち主（ユーザ）の認証
  - パスワードや生体情報による認証
- ICカードとシステム（サーバ）の認証
  - 公開鍵暗号方式を利用した相互認証・暗号通信

従来のICカードモデルの課題

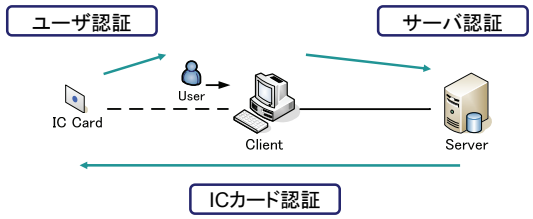


- ICカード/クライアント間通信
  - 非接触ICカード利用時は無線通信
    - 暗号化による通信が望ましい
- 暗号化が必要な場合
  - ICカード・クライアントで暗号通信の種となる秘密情報を共有
  - 秘密情報から暗号鍵を生成
    - クライアントから秘密情報が漏洩する可能性
      - 漏洩時の被害が全体に波及する
    - 秘密情報の定期的な更新
      - 非常に手間がかかり，煩雑
  - 実際の運用
    - 暗号通信を行わない
    - 暗号通信は行うが，秘密情報を更新しない

SPAIC (Secure Protocol for Authentication with IC card)

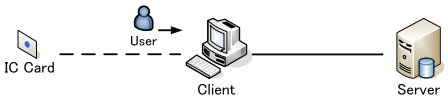
- 非接触ICカードの利用を前提
- クライアントが初期情報を一切所持しない
  - 情報漏洩の防止
- 安全な通信経路の確立
  - ICカード/クライアント間
    - ICカード公開鍵を利用
  - クライアント/クライアント間の重要情報の配送
    - Diffie-Hellman鍵交換による暗号鍵生成
- ICカード/クライアント/サーバを独立したものとして認証

SPAICの認証関係



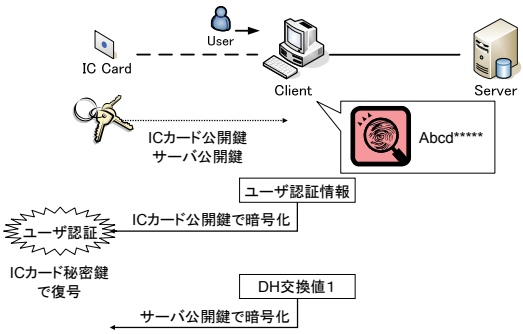
- ユーザ認証
  - ICカードがユーザを認証
- ICカード認証
  - サーバがICカードを認証
- サーバ認証
  - クライアントがサーバを認証

SPAIC　初期情報

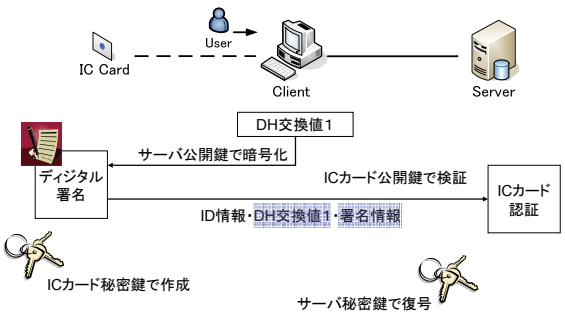


ICカード	ICカードID ICカード秘密鍵 サーバ公開鍵 ユーザ認証情報 ***ICカード公開鍵***
クライアント	なし
サーバ	サーバ秘密鍵 ICカードID ICカード公開鍵

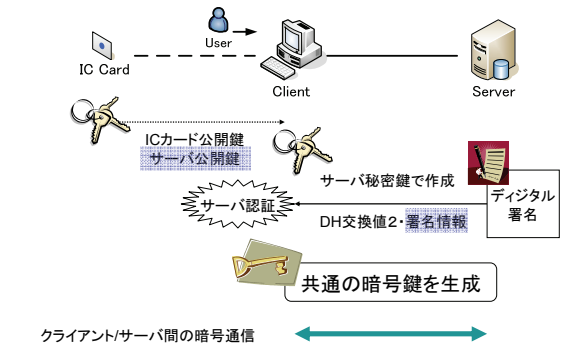
SPAICの動作①



SPAICの動作②



SPAICの動作③



従来方式との比較

	従来方式	SPAIC
クライアントに格納する情報	動作プログラム 秘密情報	動作プログラムのみ
ICカード/クライアント間の暗号	秘密情報より暗号鍵を生成	ICカード公開鍵による暗号化
ICカードへの負荷	中程度	高い
認証方法	ICカード/サーバ間の相互認証	ICカード/クライアント/サーバで環状の認証
運用時の管理負荷	秘密情報の更新が必要	ユーザの追加，削除程度

まとめ

- SPAICの提案
  - 非接触ICカードを利用した新しい情報配送モデル
  - 初期情報を持たないクライアントへの情報配送
    - 3つの認証経路による確実な認証
    - ICカード公開鍵をICカードに持たせる
    - Diffie-Hellman鍵交換の利用
      - 安全な通信経路の確立
- 今後の課題
  - 実装による詳細な評価