中間者攻撃に対する SPAIC の安全性検討

宮崎　雄介*，鈴木　秀和，渡邊　晃(名城大学)

Studies on the safetiress of SPAIC agoliust the man-in-the-middle attack for SPAIC

Yusuke Miyazaki, Hidekazu Suzuki, Akira Watanabe (Meijo University)

１．はじめに

クライアント/サーバ間通信において重要な情報を交換する場合，確実な認証と暗号化が要求される．このような要求を満たす方式として，IC カードを用いた方式が注目されており，その一技術として，SPAIC（Secure Protocol for Authentication with IC card）[1]がある．しかし，クライアント/サーバ間での中間者攻撃に対する確認が十分に検証されていなかった．そこで，本稿では SPAIC に対する中間者攻撃の検討を行い，その安全性に問題がないことを示す．

２．SPAIC 概要

SPAIC は非接触 IC カードを利用して，秘密情報を一切持たないクライアントに対して重要情報を配送することを可能するプロトコルである．認証に必要となる初期情報はすべて IC カードに格納しているため，秘密情報が漏洩する心配がなく，特定の端末を使用する必要もない．

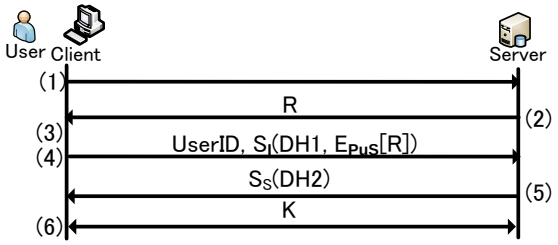


Fig.1. SPAIC sequence between a Client and a Sever

SPAIC でのサーバ/クライアント間のみを抜粋した動作を Fig.1 に示す．（1）クライアントは通信を開始することをサーバに知らせる．（2）サーバは乱数 R を生成しクライアントに送信する．(3) 乱数 R をサーバの公開鍵 PuS で暗号化（$E_{PuS}[R]$）する． Diffie-Hellman 鍵交換の交換値（DH１）を生成する．（4）クライアントは，IC カード経由で IC カードの秘密鍵を用いてディジタル署名した DH1 と $E_{PuS}[R]$を，ユーザの ID と一緒にサーバへ送信する．（5）サーバはユーザの ID に対応する IC カードの公開鍵を用いて，ディジタル署名を検証する．サーバの秘密鍵を用いて $E_{PuS}[R]$を復号し，R を検証する．DH2 を生成し，サーバの秘密鍵を用いてディジタル署名 S_S（DH2）を作成する．DH1 と DH2 を利用して共通暗号鍵 K を生成する．最後に，クライアントに S_S（DH2）を送信する．（6）クライアントは，あらかじめ IC カードから取得していたサーバの公開鍵 PuS を用いて，ディジタル署名を検証した後，DH1 と DH2 を利用して共通暗号鍵 K を生成する．以後，クライアント/サーバ間は共通暗号鍵 K を用いて暗号化通信を行う．

SPAIC では，非接触 IC カード/クライアント間は，近距離であるため中間者攻撃ができないという前提をおいている．本稿では，クライアント/サーバ間に攻撃者が存在すると仮定した場合の検討を行う．

３．中間者攻撃の検討

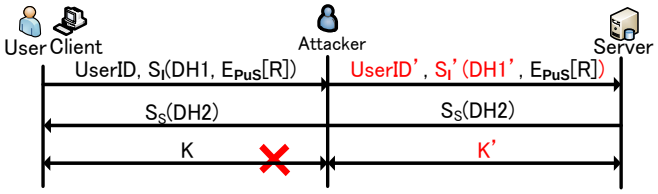


Fig.2. A man-in-the-middle attack in SPAIC sequence

Fig.2 に中間者攻撃が行われた場合のシーケンスを示す．始めに，攻撃者はクライアントが送信した UserID と DH1 を攻撃者の UserID'と DH1'に書き換える．さらに，新たに $E_{PuS}[R]$ を含むディジタル署名を作成し直す．これらの情報をサーバに送る．サーバは攻撃者の ID'に対応する IC カード公開鍵を用いて，ディジタル署名を検証する．ここで，攻撃者の ID'が存在しディジタル署名の検証にも成功したとすると，DH1'と DH2 を利用して共通暗号鍵 K'が生成される．共通暗号鍵 K'にサーバの秘密鍵を用いてディジタル署名を行い，クライアントに送信する．この際に，攻撃者は DH2 を盗聴することはできるが，改竄することはできない．なぜなら，サーバの秘密鍵を用いてディジタル署名されているからである．最後にクライアントはディジタル署名を検証した後，DH1 と DH2 を利用して共通暗号鍵 K を生成する．

以上により，クライアント，攻撃者，サーバそれぞれの共通暗号鍵の生成が完了したとする．クライアントは共通暗号鍵 K を生成しており，攻撃者とサーバは K'を生成している。従って，クライアント/攻撃者間において鍵共有を行うことが出来ておらず，中間者攻撃は成立しないため SPAIC は安全であると言える。

４．むすび

SPAIC における中間者攻撃は成立しないことを証明した．今後は，SPAIC の実装と性能評価を行う．

文　献

[1] 束，他：Proposal of an authentication Method “SPAIC” using a non-contact type IC card, ISCIT2007, pp.1470-147, 2007

中間者攻撃に対するSPAICの安全性検討

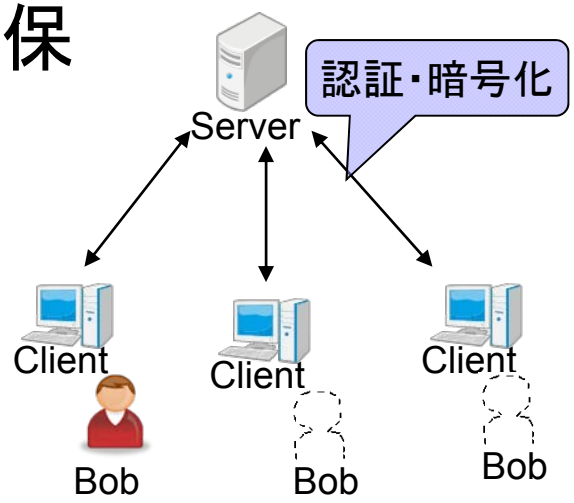
名城大学理工学部
宮崎 雄介，鈴木 秀和，渡邊 晃

研究背景

- 異なるクライアントからサーバへアクセス
- クライアント/サーバ間通信の安全確保
  - 重要情報の漏洩を防ぐ

確実な認証と暗号化が必要

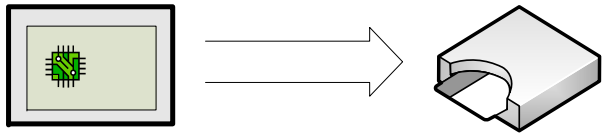
ICカードを利用した認証方式に注目



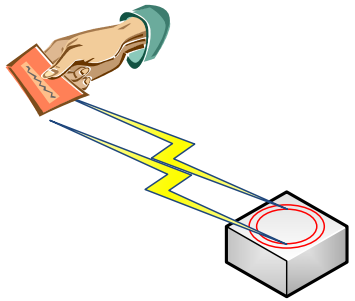
  - カード内で認証や暗号化などの処理が可能 ⇒演算能力
  - 外部からの不正読み取りを防ぐことができる ⇒耐タンパ性
  - 一人一人が持って移動できる ⇒携帯性

ICカードの分類

- 接触型ICカード
  - 数年前まで主流
  - ICカードとクライアントを一体と見なせる
  - 一般的に、ICカード/クライアント間は暗号化を行わない
- 非接触型ICカード
  - 近年普及しつつある
  - ICカード/クライアント間は無線通信
  - ICカード/クライアント間で暗号化が必要



ICカードをリーダライタに挿入



ICカードを挿入する必要がない

既存技術と課題

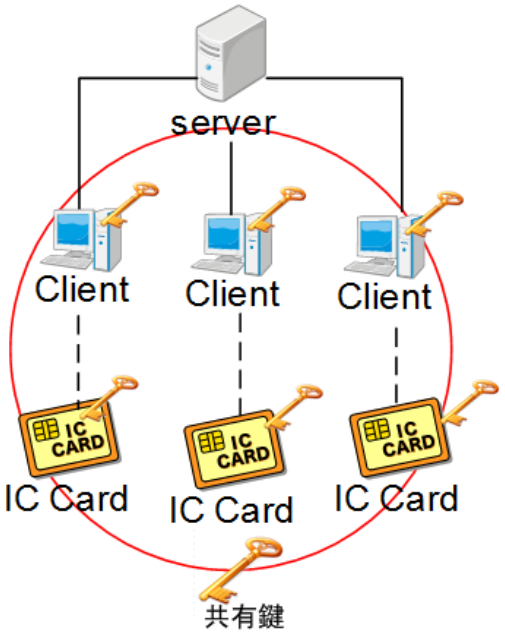
- ICカード/クライアント間の暗号化技術
  - 事前共有鍵方式→JICSAPで定義
  - 事前に共有鍵を全てのIC CardとClientで共有する
  - 共有鍵を用いて暗号化キーを生成する

課題

- クライアントから共有鍵が漏洩
  - 影響が全体に及ぶ
- 共有鍵を定期的に更新が必要となる
  - 鍵の管理が煩雑

解決

SPAIC



JICSAP:日本ICカードシステム利用促進協議会

SPAICについて

目的

- 非接触ICカードを利用し、ServerからClientへ重要情報を安全に配送するための通信路を確立する

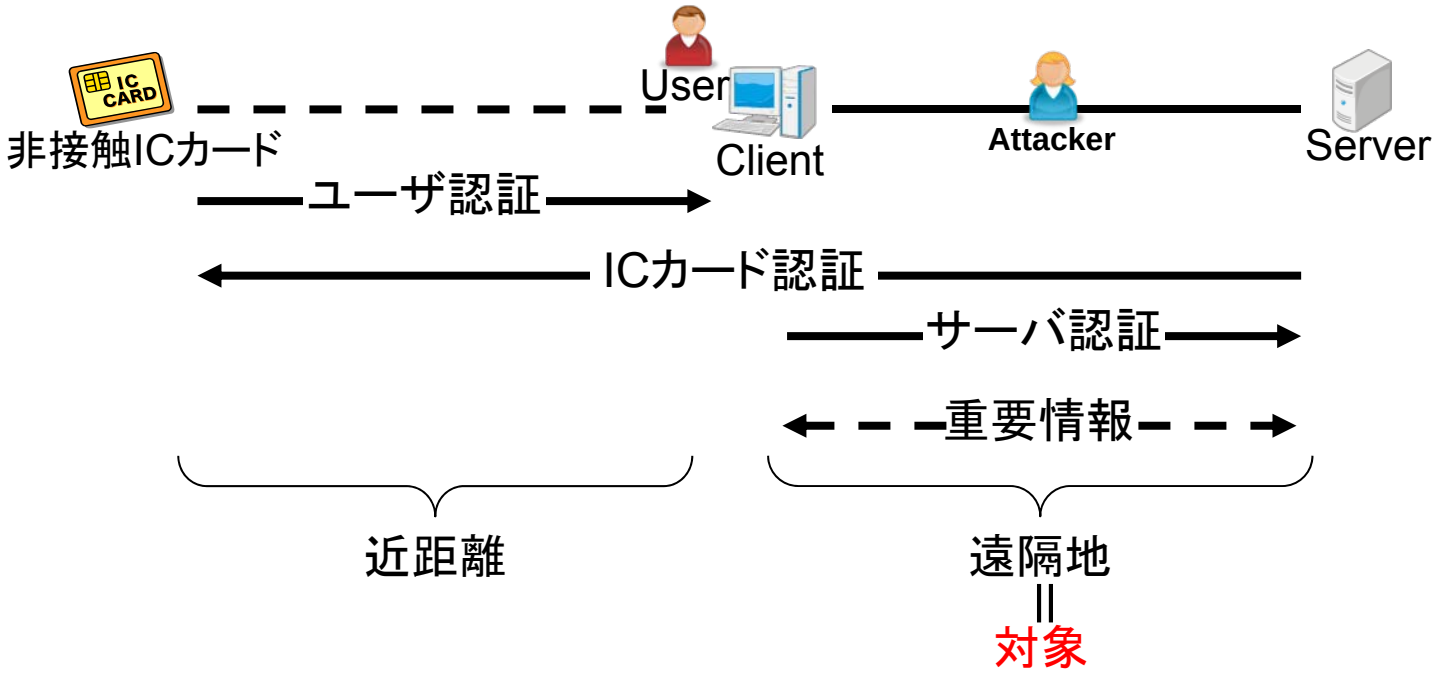
概要

- SPAIC:Secure Protocol for Authentication with IC Card
- クライアントに初期情報を一切所持しない
  - 情報漏えい防止
- ICカード/クライアント間の認証には
  - ICカードの公開鍵を利用
- クライアント/サーバ間の重要情報の配送には
  - Diffie - Hellman鍵交換によって生成した暗号鍵を利用

Diffie - Hellman鍵交換：公開鍵暗号方式の1種

SPAICの認証システム

- IC Card/Client/Serverを独立したものとして環状の認証
- 前提条件
  - IC Card/Clientは近距離なため、中間者攻撃は成立しない



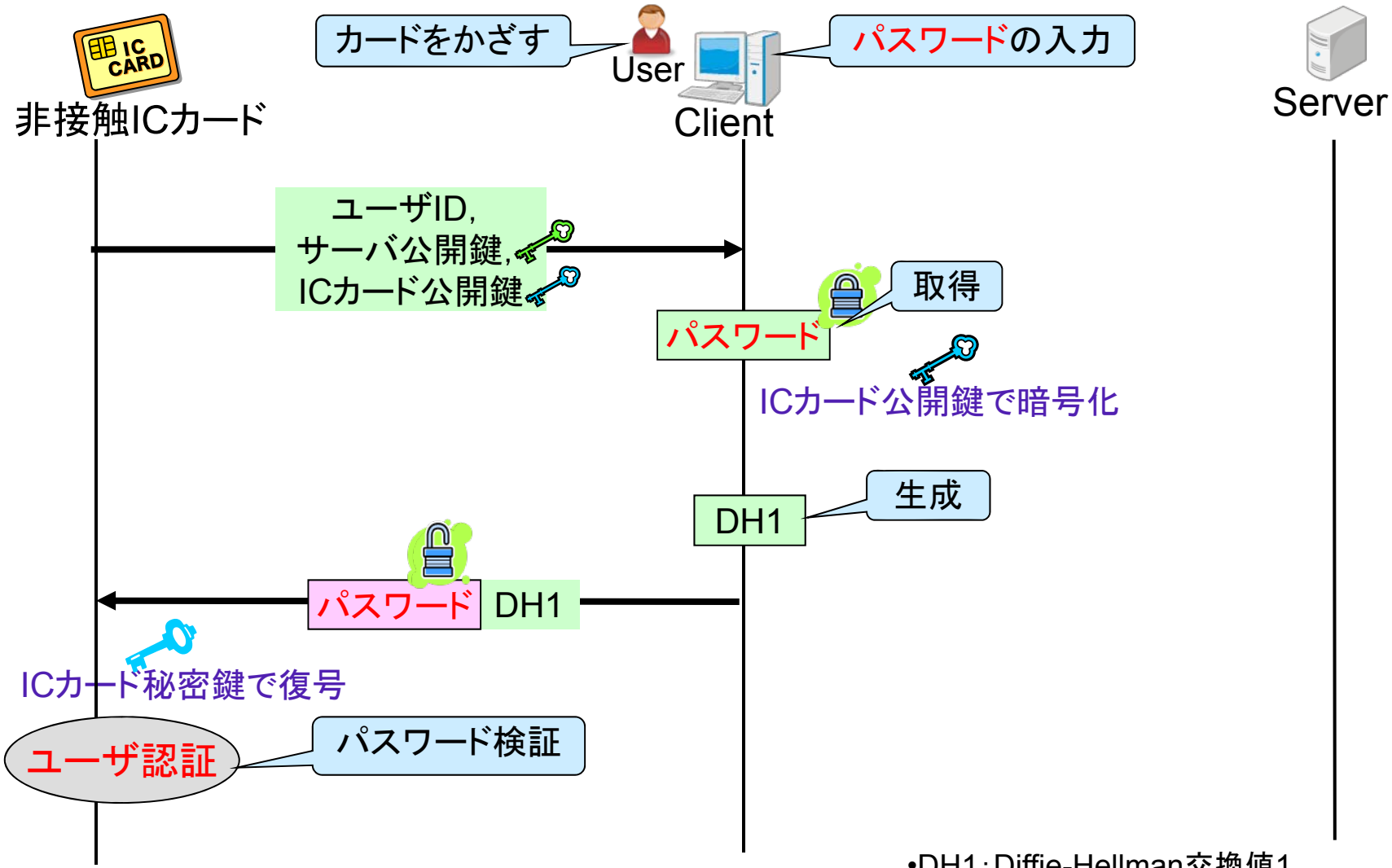
※クライアントは間接的に認証

各端末の初期情報

ICカード 	クライアント 	サーバ 
ユーザID パスワード サーバ公開鍵 ICカード秘密鍵 ICカード公開鍵	なし	ユーザID サーバ秘密鍵 ICカード公開鍵

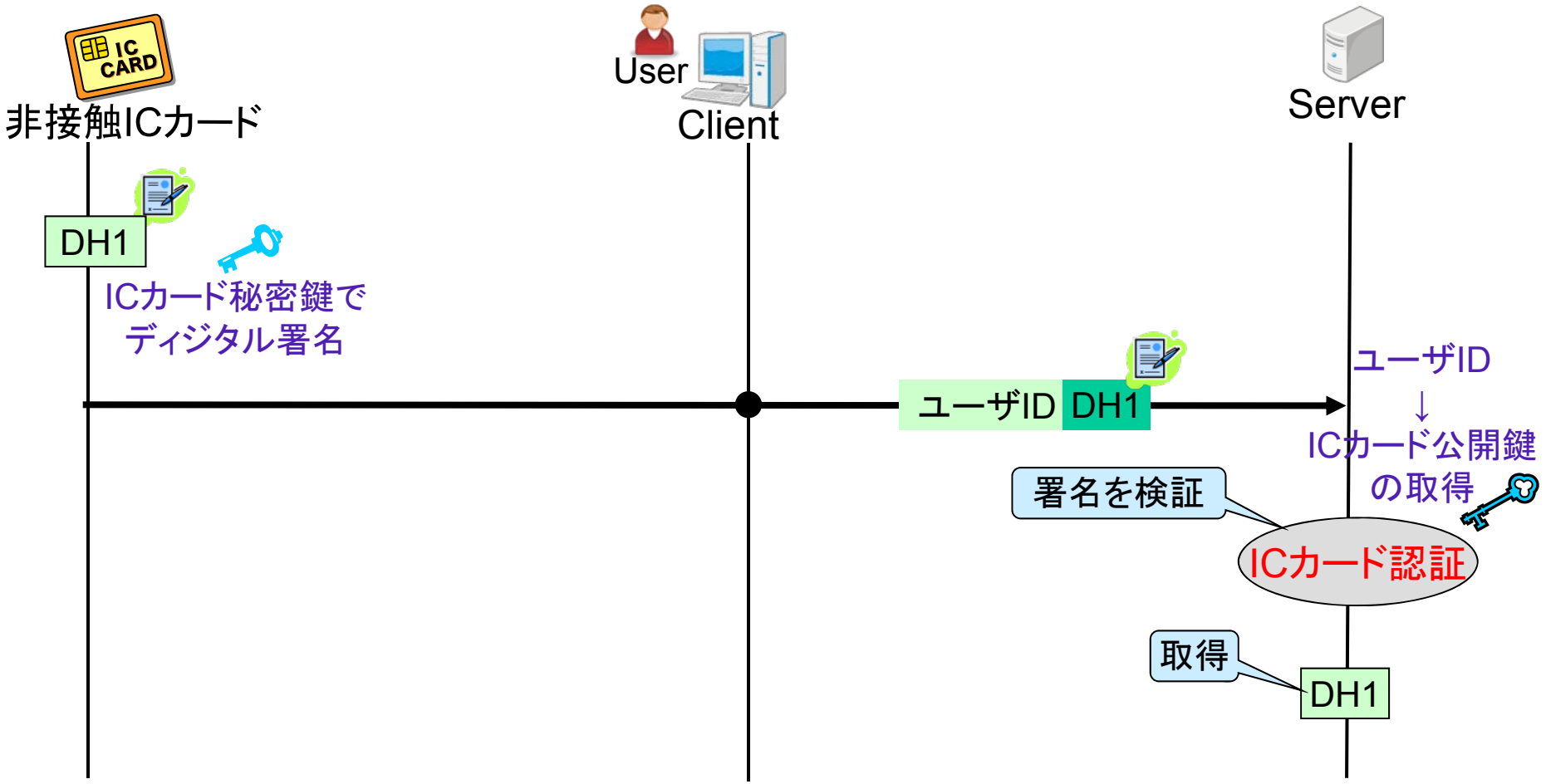
- 初期情報は事前にオフラインで設定する
- クライアントには初期情報が必要ない

SPAICの動作1＜ユーザ認証＞

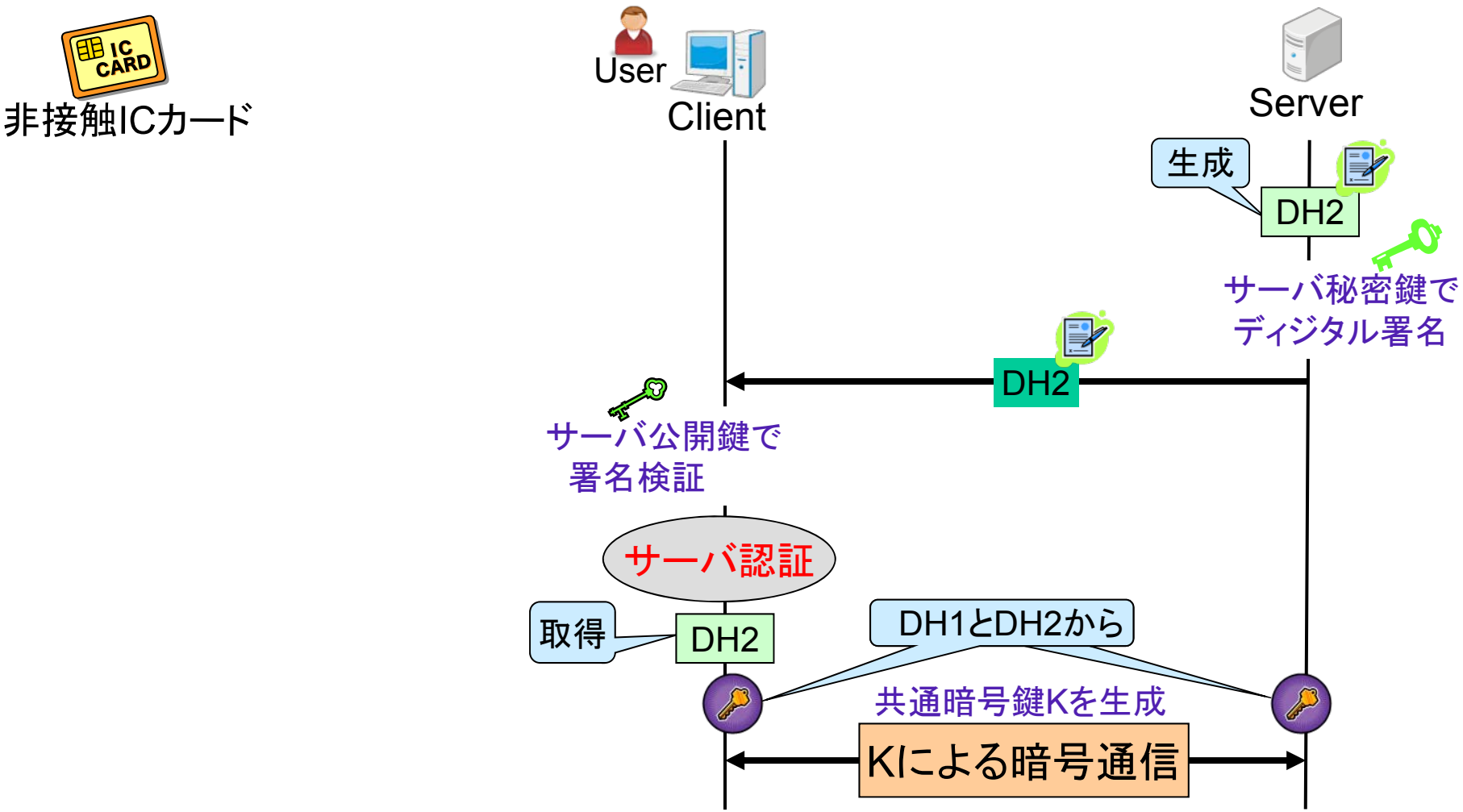


•DH1：Diffie-Hellman交換値1

SPAICの動作2＜ICカード認証＞

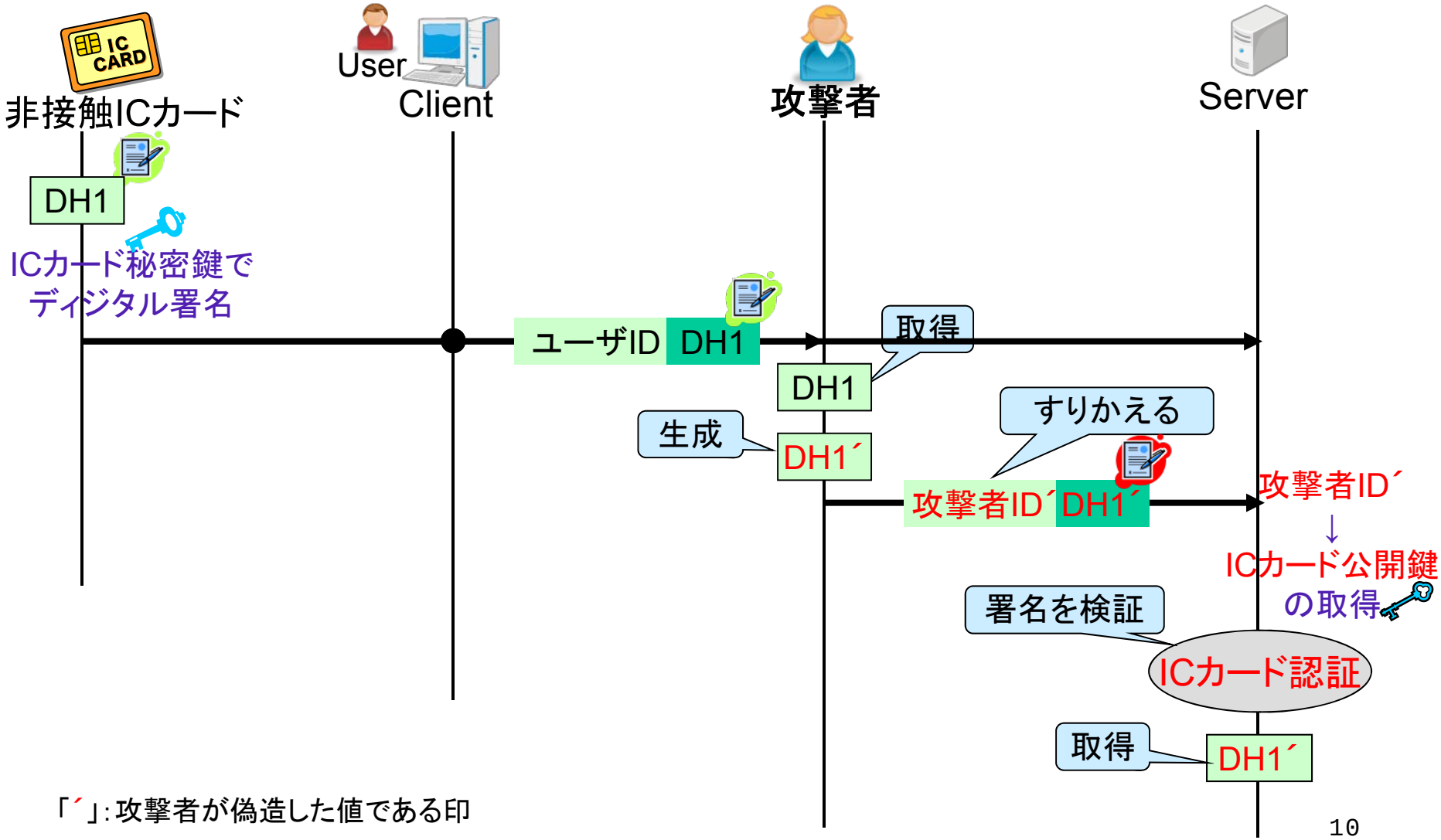


SPAICの動作3＜サーバ認証＞



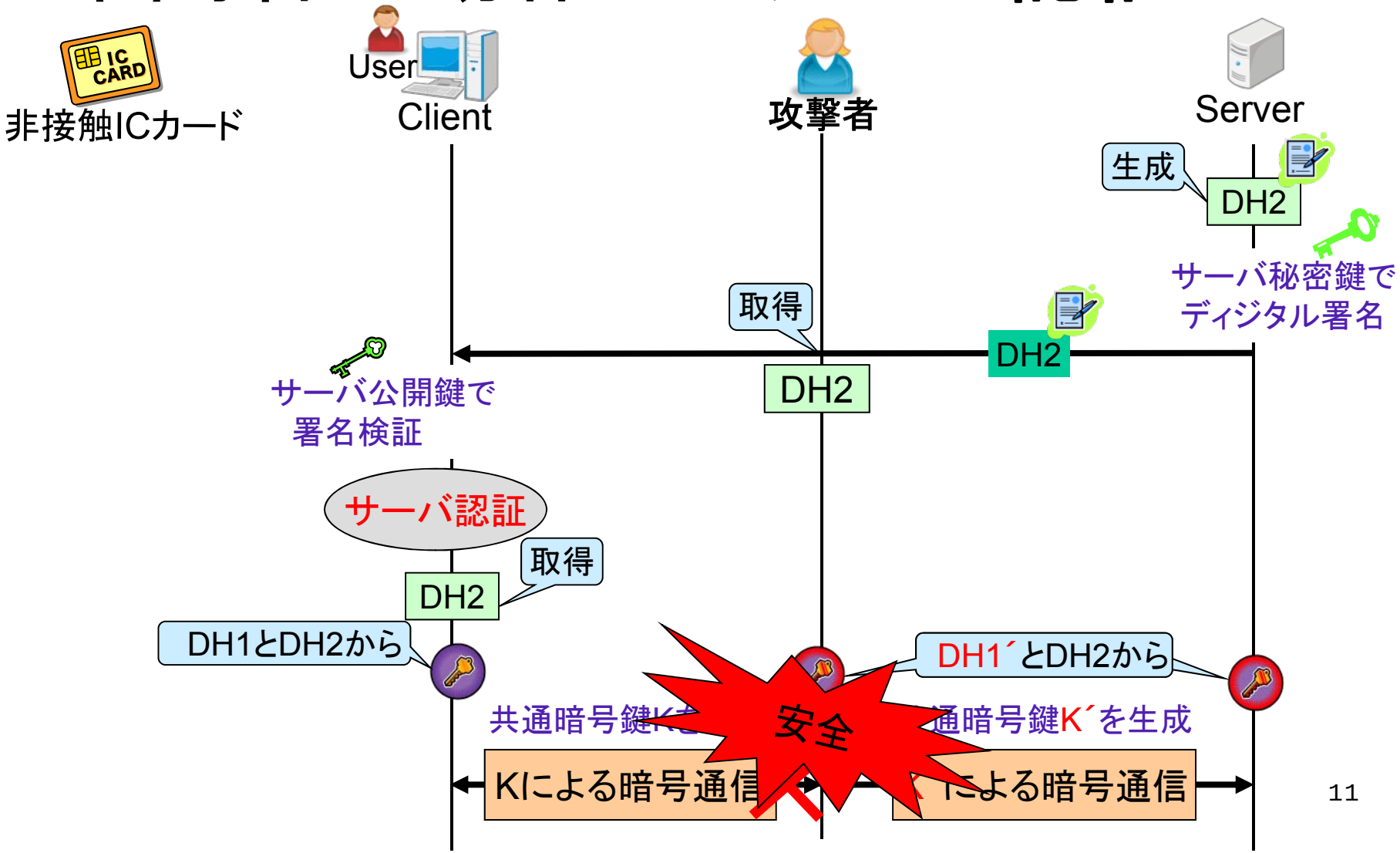
•DH2：Diffie-Hellman交換値2

中間者の動作1＜ICカード認証＞



「´」:攻撃者が偽造した値である印

中間者の動作2＜サーバ認証＞



まとめ

- SPAICは
  - 非接触ICカードを利用し、クライアント/サーバ間の安全な通信路を確立する
  - クライアントに初期情報が必要ない
- SPAICに対して中間者攻撃は成立しない
  - SPAICは安全なプロトコルである

今後

- 実装を行っている段階である
  - 実装を進め、性能評価を行う