秘密情報を一切保持しないクライアントを利用できる認証プロトコル MSAP の提案

080425126　五島秀典
渡邊研究室

1. はじめに

企業においては情報漏洩の防止が重要な課題である.情報漏洩の原因の 4 割はノート PC 等のモバイル機器の盗難,紛失によるものと言われている.そこで社外に情報を持ち出さずに,必要に応じてクライアント PC から社内システムにリモートアクセスする方法が注目されている.このときクライアントは固定されることなく選べることが望ましい.このようなシステムには確実な認証と暗号化が要求される. 本稿では近年普及が著しいスマートフォンに認証情報を保持させ,初期情報を一切所持しないクライアントを利用可能とするプロトコル MSAP(Mobility-based Secure Authentication Protocol)を提案する.

2. 既存の方式

既存方式として非接触ＩＣカードに認証情報を保持させる事前鍵共有方式がある.(1)この方式ではセキュリティを確保するため,ＩＣカードとクライアントＰＣに共有鍵を埋め込んでおく必要がある.そのため,クライアントが固定されてしまうだけでなく,クライアントから共有鍵が漏洩する危険性がある.漏洩した場合システム全体に影響が及ぶという課題がある.

3. テンプレートおよびスタイルファイル

提案方式ではクライアントに認証に必要となる秘密情報を一切保持させないでよい.その代りにスマートフォンが自らの公開鍵を保持するものとする.表 1.に従来方式と提案方式の初期情報の違いを示す.ハッチング部分が異なるだけで,その他の初期情報は同じである.

表 1　MSAP と既存技術の初期情報

	事前鍵共有方式	提案方式
スマートフォン	ユーザ ID パスワード サーバ公開鍵 SP 秘密鍵 事前共有鍵	ユーザ ID パスワード サーバ公開鍵 SP 秘密鍵 SP 公開鍵
クライアント	事前共有鍵	なし
サーバ	サーバ秘密鍵 SP 公開鍵 ユーザ ID	サーバ秘密鍵 SP 公開鍵 ユーザ ID

MSAP で想定するシステムモデルと認証の関係を図 1 に示す.ユーザは秘密情報を格納したスマートフォンを所持している.クライアントは Bluetooth 接続ができ,MSAP 対応するアプリケーションが搭載されていればどのようなものでもよい.スマートフォン-クライアント間の Bluetooth のプロファイルは 1 対 1 通信を前提とするＳＰＰ(Serial Port Profile)とする.そのため,この間での中間者攻撃は成り立たない.

MSAP ではスマートフォン/クライアント/サーバを独立したものとして環状の認証を行う.矢印を方向は認証の方向を示している.ユーザの持っているスマートフォンからパスワードを入力することによりサーバにてクライアントの認証を行う. スマートフォン内スマートフォンの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スマートフォンを認証する.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クライアントはサーバを認証する.
以上の３つの経路の認証を実現することによりクライアント/サーバ間の認証が実現する.

図 1　想定するシステムモデルと認証の関係

4. まとめ

秘密情報を一切保持しないクライアントを利用できる認証プロトコルを提案した.今後は実装,評価を行っていく予定である.

参考文献

[1] 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 (2001).
[2] 山宮崎 雄介”中間者攻撃に対する安全性の検討” 平成 21 年度電気関係学会東海支部連合大会論文集, Sep.2009.
[3] 東 長俊”非接触型 IC カードを用いた認証方式 SPAIC の提案” マルチメディア，分散，協調とモバイル（DICOMO2007）シンポジウム論文集，情報処理学会シンポジウム， Vol.2007， No.1，pp.1332-1337，Jun.2007.

秘密情報を一切保持しない クライアントを利用できる認証 プロトコルMSAPの提案

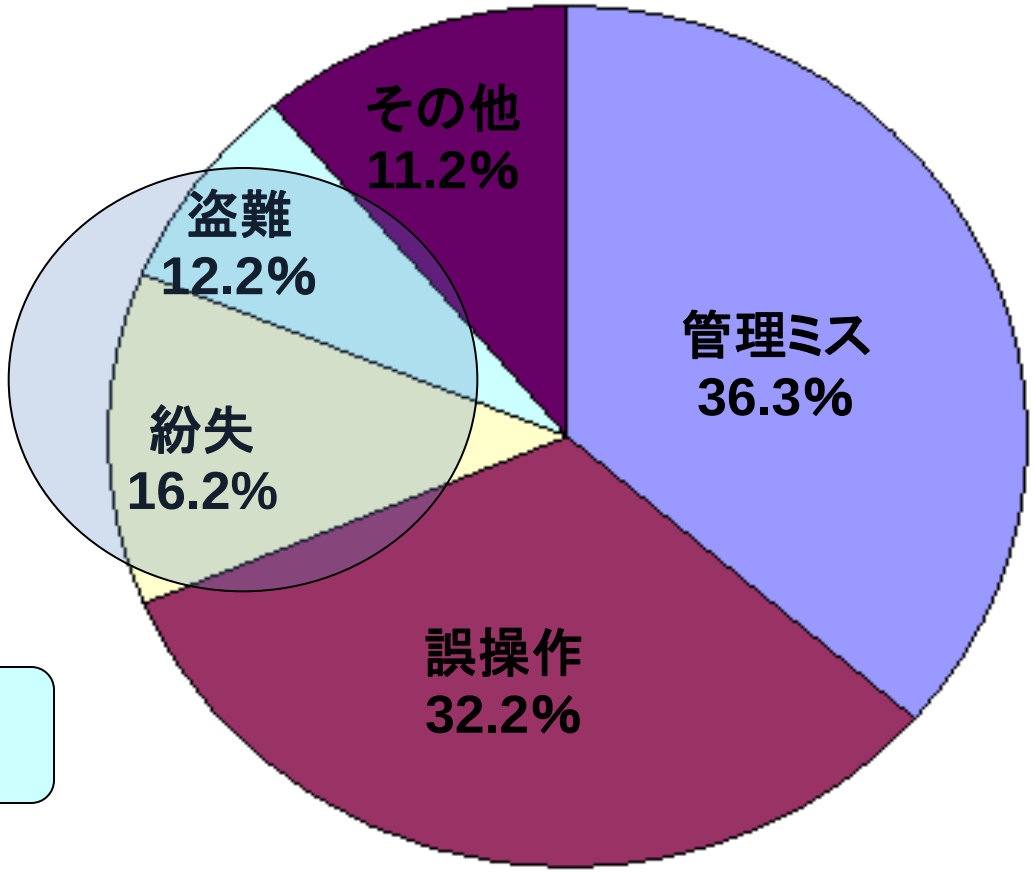
名城大学理工学部　渡邊研究室　080425126
五島 秀典, 鈴木 秀和, 渡邊 晃

Watanabe Lab.

研究背景

- 企業では情報漏洩の防止が重要となっている

情報漏洩の原因



システムでカバーできる

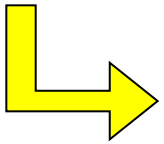
NPO　日本ネットワークセキュリティ協会

紛失/盗難

- 事例

自宅に空き巣が入りPCごと盗難

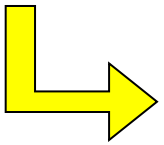
USBメモリなど記憶媒体の置き忘れ,紛失　　etc・・・

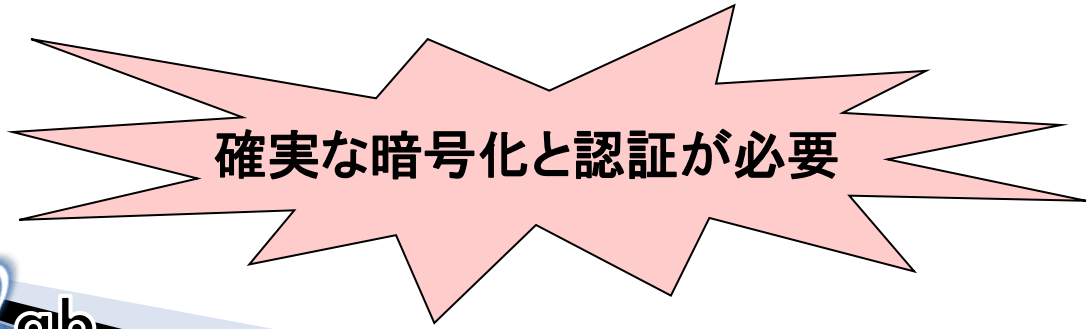


情報を社外へ持ち出すことが共通点

- 解決策

社内システムにリモートアクセスすることで社内情報を持ち歩かない





確実な暗号化と認証

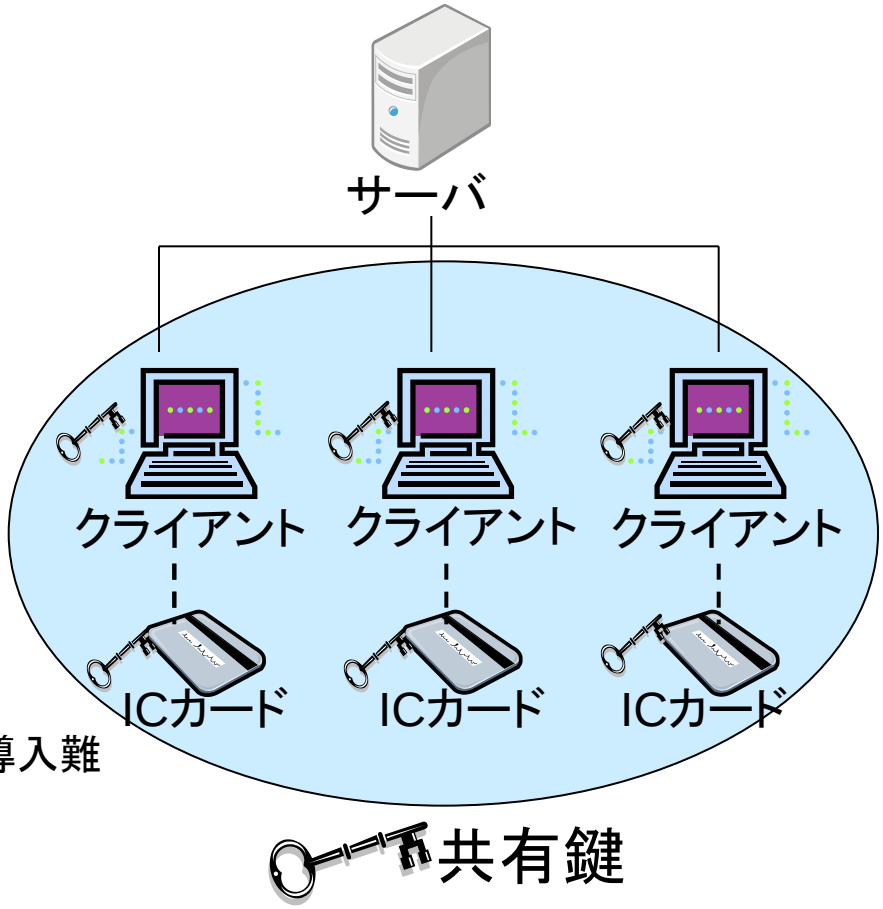
- 通信経路すべてに盗聴されも良いように暗号化
- 確実な認証のため各種攻撃に対応
  - 対応しなければならない攻撃
    - DoS攻撃:
    - サーバなどの機器にパケットを送るなど負荷をかけることでサービスの提供を不能にする手法
    - 中間者攻撃:
    - 通信を行う二者の間に割り込んで、両者が交換する情報を自分のものとすりかえることにより、気付かれることなく盗聴したり、通信内容に介入したりする手法。
    - リプレイアタック:
    - パスワードや暗号鍵などを盗聴し、そのまま再利用することでそのユーザになりすます手法

従来の暗号化・認証方式と課題

- ICカードを利用した方法

  - 特徴
    - ICカード/クライアント間は事前鍵共有方式
    - 共有鍵を用いて暗号化

  - 課題
    - クライアントから共有鍵が漏えい
      - 漏洩時の影響が全体に及ぶ
    - 共有鍵を定期的に変更する必要がある
      - 管理が煩雑、ICカードの更新、大規模システムに導入難
    - ICカードリーダが必要
      - 端末にリーダがないとカードを読み取れない



*JICSAP：日本ICカードシステム利用促進協議会

提案方式MSAP

MSAP(Mobility-based Secure Authentication Protocol)

特徴

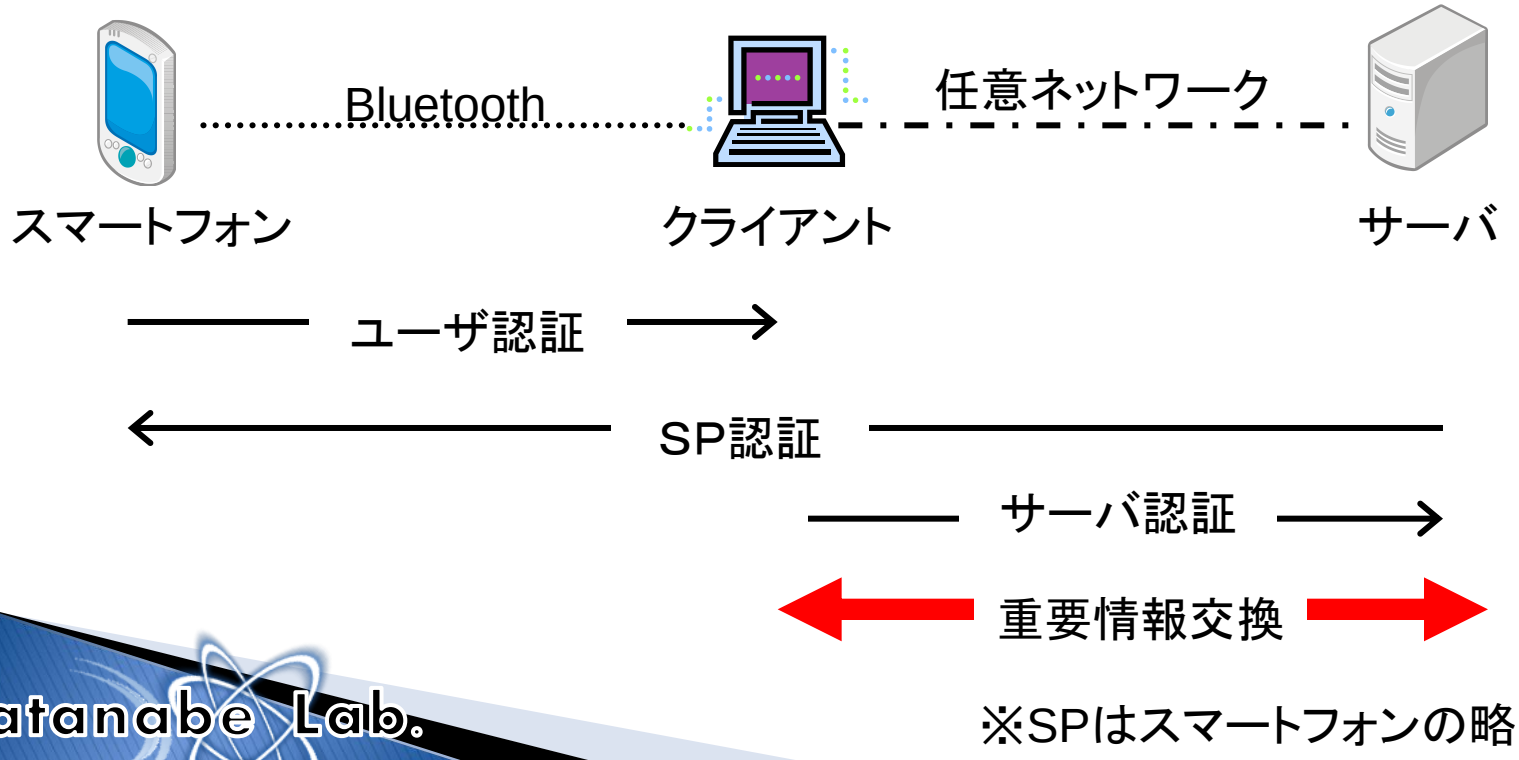
- スマートフォンを利用して認証
  スマートフォンがより普及し、スマートフォンが認証に使えれば有用
- クライアントに初期情報を保持させない
  - クライアントからの情報漏洩の防止

MSAPの構成

●スマートフォン/クライアント/サーバを独立したものとして環状の認証

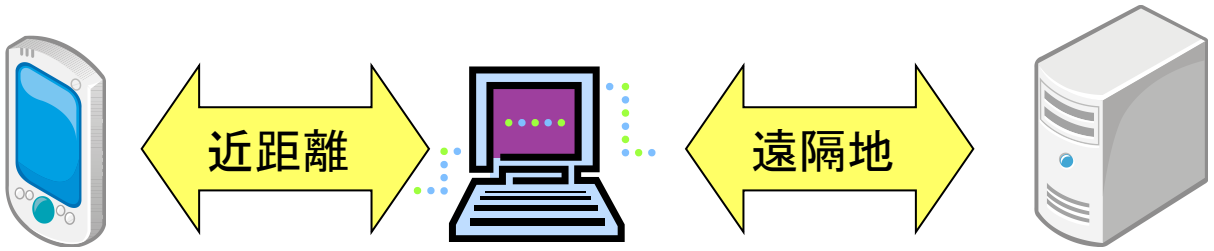
●Bluetooth

→プロファイルはSPP(Serial Port Profile)を使用するためこの間は中間者攻撃不可



※SPはスマートフォンの略

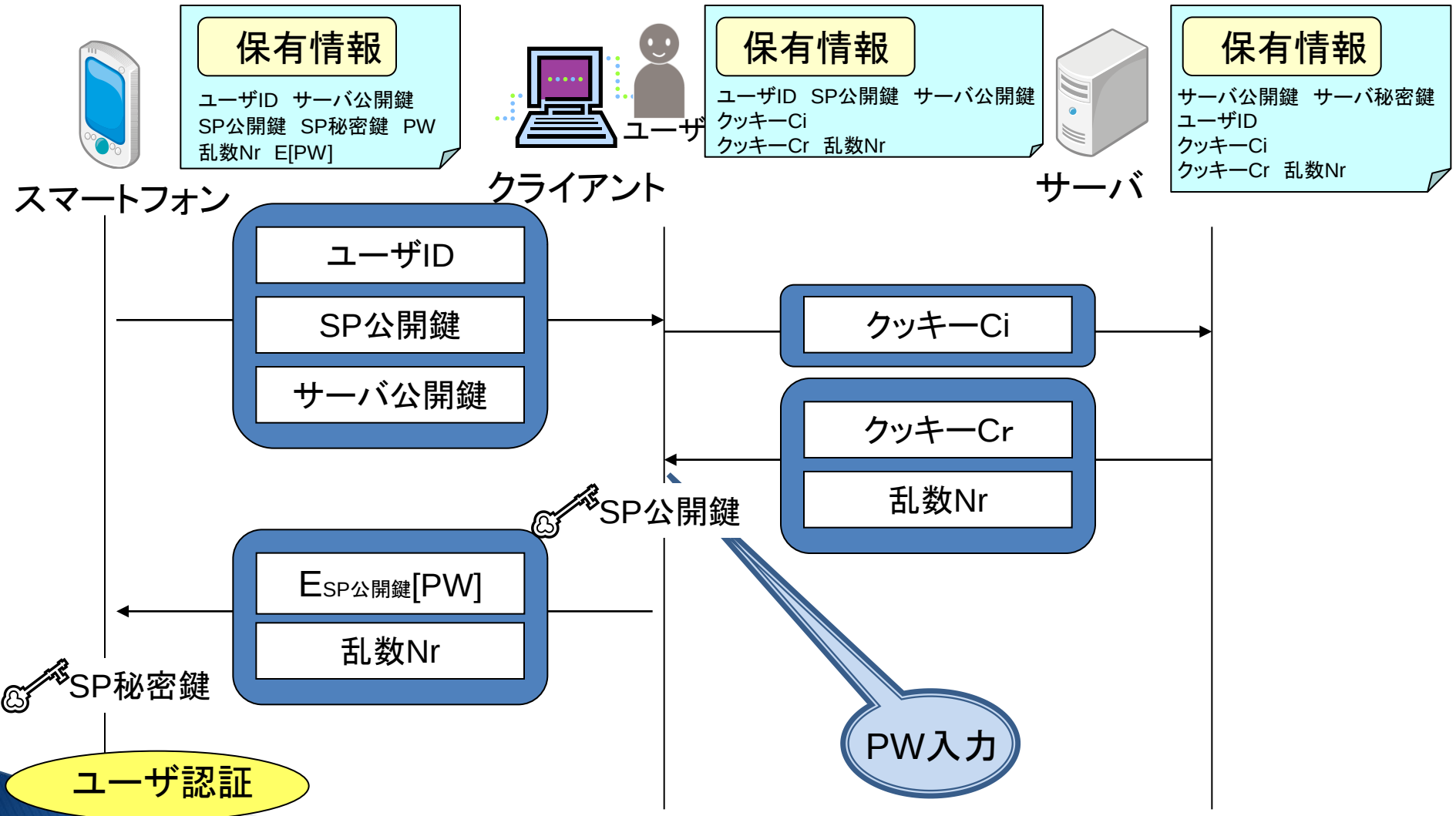
MSAPと事前共有鍵方式の初期情報



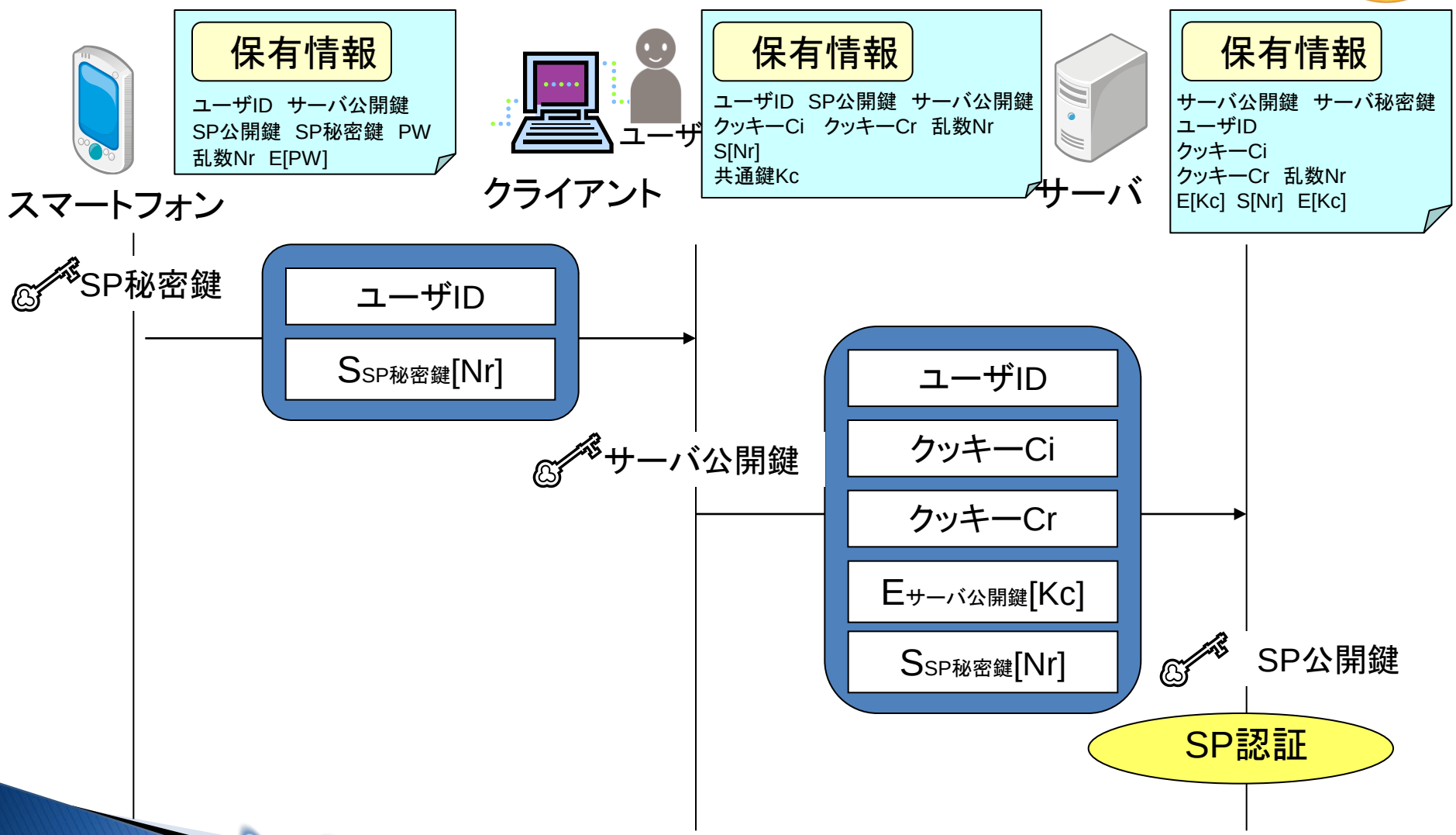
	事前共有鍵方式	MSAP
スマートフォン	ユーザID SP秘密鍵 サーバ公開鍵 パスワード 事前共有鍵	ユーザID SP秘密鍵 サーバ公開鍵 パスワード SP公開鍵
クライアント	事前共有鍵	なし
サーバ	サーバ秘密鍵 ユーザID SP公開鍵	サーバ秘密鍵 ユーザID SP公開鍵

※SPはスマートフォンの略

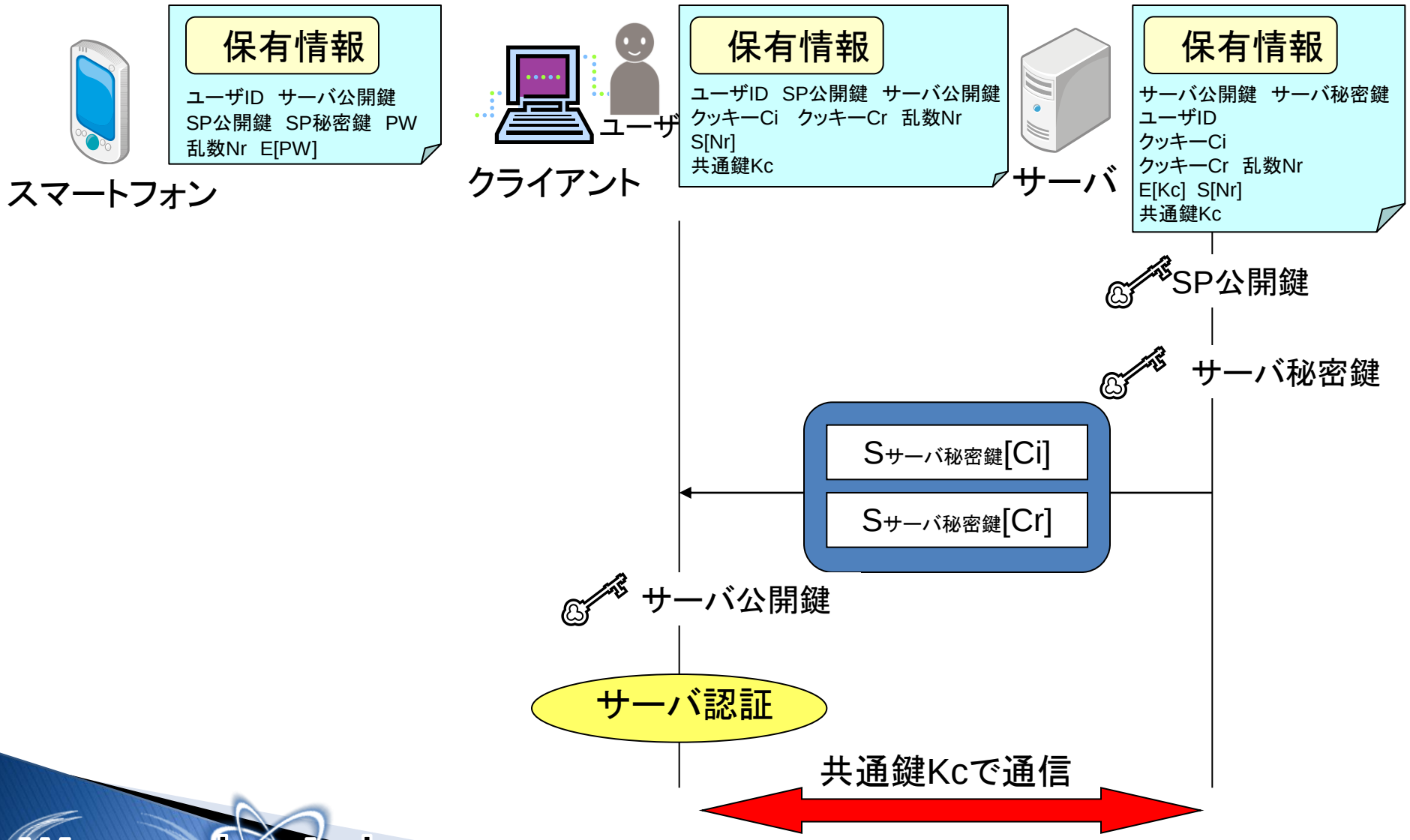
MSAP動作1(ユーザ認証)



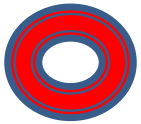
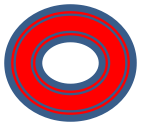
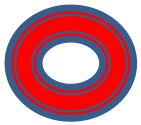
MSAP動作2(SP認証)



MSAP動作3(サーバ認証)



評価

	事前鍵共有方式	提案方式
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
管理負荷	共有鍵の管理が煩雑 	ユーザ追加、削除 
スマートフォンへの負荷	 低い	 高い

まとめ

- 提案では
  - クライアントが初期情報を持たないモデルを定義
  - 重要情報を配送するための通信経路を確立

- 今後
  - PC上で実装したのちにスマートフォンに移植して実装を行う