クライアントを自由に選択可能な認証プロトコル TSSAP

五島 秀典，旭 健作，鈴木 秀和，渡邊 晃

名城大学大学院 理工学研究科 情報工学専攻

Proposal of an authentication protocol TSSAP that can freely select terminals.

Hidenori Goshima and Kensaku Asahi and Hidekazu Suzuki and Akira Watanabe

Graduate School of Science and Technology, Meijo University

1 はじめに

インターネットの普及に伴い，ユーザがクライアント端末を利用して遠隔地のサーバと情報交換したいという要求が増えている．また，企業においては情報漏洩の防止，情報管理の徹底が重要となっている．情報漏洩する場合の事例として，PC ごと盗難されるケースや，社内データの入ったノート PC や USB メモリなどの記憶媒体を置き忘れ悪用されるなどの事例がある．これらの事例は情報を社外に持ち出している点が共通している．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 [1]．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安全にアクセスするリモートアクセスが注目されている．社内システムにアクセスするにはクライアントとサーバ間で正しい認証と暗号鍵の共有が必須であり，セキュリティの強度を上げるために，2 要素以上の認証が好ましい．2 要素以上の認証とは，ID, パスワードだけの認証ではなく，ID, パスワード認証と一緒に，生体認証や，複製不可能，もしくはしづらいユーザが持っているものをキーとして認証する認証方法である．

2 要素以上の認証では ID, パスワードだけの認証と違い，パスワードの問題点である，パスワードの流出，推測された場合でも認証を否定できる．そして，このようなシステムにはユーザの視点から考えるとホテルのパソコン，自宅のパソコン等，異なるクライアントからでもサーバへアクセスできることが望ましい．

このような認証システムの既存技術の例として，非接触型の IC カードをユーザが所持する方式がある [2-8]．この方式は IC カード，クライアントに共有鍵を持たせることによりクライアント，IC カード間の暗号通信が行える．しかし，この方式はクライアントが共有鍵を保持する必要があり，クライアント共有鍵が漏洩する可能性がある [2-5]．本論文ではスマートフォンに認証情報を持つデバイスとして利用し，初期情報を一切持たないクライアントに対し、サーバから重要な情報を配送することを可能とするプロトコル TSSAP(Terminal Selectable and Secure Authentication Protocol) を提案する．

2 既存の認証方式

図 1 に非接触 IC カードを利用した認証方式を示す．この方式では IC カード-クライアント間は無線通信で行われるため両者に共有鍵を埋め込む事前共有鍵を利用する方式が JICSAP により定義されている [9]．クライアントと IC カードの間は上記の共有鍵を使って認証と暗号通信を行う．ユーザは IC カードを所有しており，IC カード内の認証情報をクライアントから入力する認証情報で確認することにより認証する．しかし，この方式はクライアントに共有鍵を保持させているためクライアントから秘密情報が漏洩する可能性がある．また，漏洩した場合システム全体に影響を与える可能性がある．さらにセキュリティ面を考えると共有鍵を定期的に更新する必要があり，鍵の管理が煩雑になるという課題がある．

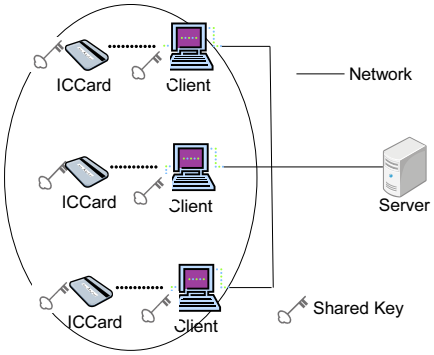


図 1: IC カードを利用した認証方式

3 TSSAP の提案

3.1 想定するシステムモデル

TSSAP で想定するシステムモデルを図 2 に示す．本システムの構成要素はスマートフォン，クライアント，サーバである．スマートフォンとクライアントは Bluetooth で接続する．ユーザは秘密情報を格納したスマートフォンを所持し，クライアントを操作する．クライアント-サーバ間は任意のネットワークで接続できる．また，前提条件としてユーザとクライアントの通信距離が近いため，スマートフォン-クライアント間の中間者攻撃はできないものとする．

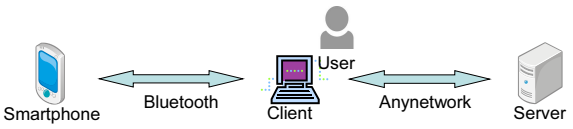


図 2: TSSAP のシステムモデル

3.2 記号の定義

TSSAP で使用する記号を以下のように定義する．

記号	説明
uID	ユーザ ID
PuSP	スマートフォン公開鍵
PrSP	スマートフォンの秘密鍵
PuS	サーバ公開鍵
PrS	サーバ秘密鍵
PW	パスワード
Kc	クライアントが生成する共有鍵
Rs	サーバが生成する乱数
Cc	クライアントが生成するクッキー
Cs	サーバが生成するクッキー
Ex[y]	x で y を暗号化
Sx[y]	x で y にディジタル署名
Key_REQ	配送要求パケット
Key_REP	配送応答パケット
Cookie_REQ	クッキー配送要求パケット
Cookie_REP	クッキー配送応答パケット
CertUser_DIST	ユーザ認証パケット
SignSP_DIST	スマートフォン署名情報配送パケット
Info_DIST	情報配送パケット
SignS_DIST	サーバ署名情報配送パケット

3.3 TSSAP の初期情報

各機器が所有する初期情報を表 1 に示す．スマートフォンにはユーザ ID，ユーザの登録したパスワードで暗号化したスマートフォン秘密鍵が格納されている．次にサーバはサーバ秘密鍵，スマートフォン公開鍵，ユーザ ID が登録されている．そして，クライアントには初期情報が一切ない．

Table 1: TSSAP の初期情報

機器名	初期情報
Smartphone	uID E_{PW}[PrSP] PuS
Client	-
Server	PrS PuSP uID

3.4 ユーザ認証について

一般的にユーザ認証の方法として，パスワードが用いられる．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記憶媒体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．本稿では記憶媒体の例としてスマートフォンとする．図 3 にサーバ型認証，図 4 にクライアント型認証の例を示す．

サーバ型認証は，クライアントで取得した認証情報を，スマートフォンを経由してサーバへ送信し，サーバで確認することで認証を行う．この認証方式では，サーバ側でユーザ認証とスマートフォン認証を一括して行う方法である．また，ユーザ全員の情報をサーバ側で一括管理できるため，データの管理がしやすいが，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たり，厳重な設備を準備するといった対策が必要となる．

クライアント型認証は，クライアントで取得した認証情報をスマートフォンに送信してスマートフォン内でユーザ認証を行い，その後スマートフォン-サーバ間でスマートフォン認証を行う．この認証方式ではサーバにおけるスマートフォン認証がユーザ認証を兼ねることとなる．その理由はクライアントをユーザが操作するためサーバがスマートフォン認証を行うとユーザ認証と同意となるためである．しかしこの方式の場合，スマートフォンにユーザの認証情報を安全に格納する必要があるため，記憶媒体に耐タンパー性を必要とする．

TSSAP では，スマートフォンを記憶媒体として使用しており，スマートフォンに耐タンパ性を持たせることは難しい．仮にクライアント型認証に耐タンパ性を有しない記憶媒体を使用した際は記憶媒体からユーザ認証情報が流出してしまう危険がある．これらより，TSSAP ではサーバ型認証を採用する．

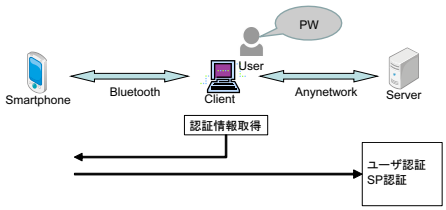


図 3: サーバ型認証モデル

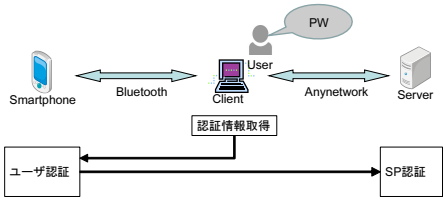


図 4: クライアント型認証モデル

3.5 Bleutooth のペアリング

TSSAP の認証処理を実行するにあたってスマートフォンとクライアント間で Bluetooth のペアリングを行う必要がある [10,11]．プロファイルは SPP(Serial Port Profile) を使用する．スマートフォン側では Bluetooth を ON にし，端末を他の機器が検出できるように設定する (ペアリングモード)．次にクライアント側で Bluetooth 端末のスキャンを行い，ペア設定を開始する．Bluetooth のバージョンによりペアリングの動作は異なるが，セキュアシンプルペアリング対応のバージョンではクライアントとスマートフォンの画面に乱数が表示される．ユーザの目で両者を確認し，一致すれば両画面の OK をクリックすることによりペアリングが完了となる．Bluetooth ではペアリングを確立すると Diff-Hellman 鍵交換が実行され，自動的にスマートフォン-クライアント間で鍵が共有される．以後の通信は Bluetooth の標準搭載の暗号化で実現する [12]．

3.6 TSSAP の動作

図 5 に TSSAP のシーケンスを示す．図中の記号はパケット名を示しており，パケット名後の ( ) の内容はパケットの情報を示している．スマートフォン-クライアント間の Bluetooth のペアリングは完了しているものとする．即ち，この間の通信は Bluetooth の共通鍵で暗号化される．

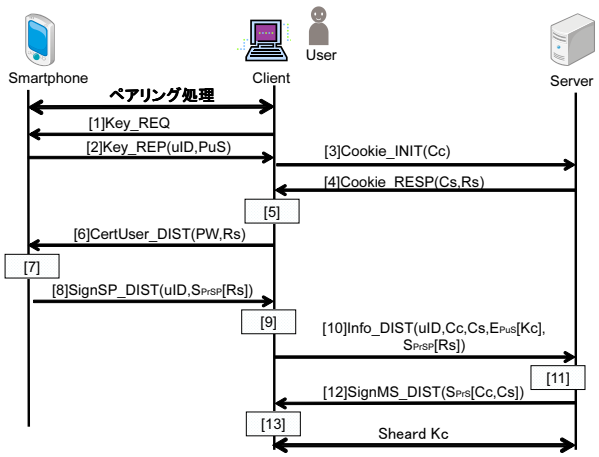


図 5: TSSAP シーケンス

1. スマートフォンへ Key_REQ を送信
   ユーザがクライアント画面上に示される，開始のボタンをクリックすることでクライアントはスマートフォンへサーバ公開鍵 PuS，ユーザ ID の情報配送を要求する．

2. Key_REP を送信
   スマートフォンはユーザ ID，サーバ公開鍵 PuS を送信する．

3. Cookie_REQ を送信
   クライアントは DoS 攻撃を防止するためのクッキー Cc を生成して，サーバへ送信する．

4. Cookie_REP の送信
   サーバはリプレイアタックに対応するための乱数 Rs と DoS 攻撃防止のクッキー Cs を生成する．この時接続してきたクライアントの IP アドレスと生成したクッキーとを対応づけて記憶させておく．また，クッキー Cs と共に乱数 Rs をクライアントへ送信する．

5. ユーザ情報 (PW) の入力
   クライアント PC の画面に PW 入力画面が表示される．ユーザはこの画面に PW を入力する．

6. CertUser_DIST の送信
   5. で入力された PW とサーバから受け取った乱数 Rs をスマートフォンへ送る．

7. スマートフォン秘密鍵の取得
   スマートフォンは受け取った PW で E_{PW}[PrSP] を復号する．

8. SignSP_DIST の送信
   スマートフォンはクライアントから受け取った乱数 Rs,PW にスマートフォン秘密鍵 PrSP でディジタル署名をし，クライアントへ送信する．

9. 共有鍵 Kc の生成
   クライアント自身が共有鍵 Kc を生成する．Kc をサーバ公開鍵 PuS で暗号化する．

10. Info_DIST の送信
    8. で生成した E_{PuS}[Kc] と.7. で生成した S_{PrSP}[Rs,PW] と共に uID，Cc，Cs をサーバへ送信する．

11. ユーザ，スマートフォン認証と署名の作成
    受信した Rs とサーバが 4. で生成した Rs を比較する．S_{PrSP}[Rs,PW] のディジタル署名をスマートフォン公開鍵 PuSP を用いて確認する．ここでディジタル署名が正しいと確認されれば，7. で復号したスマートフォン秘密鍵 PrSP が正しく復号されたことになるため，ユーザの入力した PW が正しいといえる．これより，ユーザ認証が完了する．また，クッキー Cc，Cs についても比較を行うことでスマートフォン認証が完了する．次に Cc，Cs にサーバ秘密鍵 PrS を用いてディジタル署名を行う．最後に，暗号化された Kc をサーバ秘密鍵 PrS で復号する．

12. SignS_DIST の送信
    シーケンス中の 10. で生成された S_{PrS}[Cc，Cs] をクライアントへ送信する．

13. サーバ認証
    S_{PrS}[Cc，Cs] のディジタル署名をサーバ公開鍵 PuS で確認することによりサーバ認証を行う．

以上の認証処理を行うことにより認証が完了し，クライアント-サーバ間で共有鍵を安全に共有できる．

4 TSSAP の安全対策

TSSAP では DoS 攻撃，リプレイアタック，中間者攻撃，紛失，盗難に対する対策, として以下の手段を取っている．以下はこれらの攻撃について考察する．

4.1 DoS 攻撃

DoS 攻撃はサーバに対して高負荷の処理，大量のパケットを送りつけることによりサーバをサービス不能状態にする．クライアント-サーバ間の認証処理に先だってお互いにクッキーを交換することによって対応する．クッキーの中身は送信元 IP アドレス，送信先 IP アドレス，時間情報を基に生成される．サーバはクライアントの IP アドレスと生成したクッキーとの対応をテーブルで管理する．クッキーは通信ごとに異なる値となるため，スマートフォン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により，無関係な端末からの DoS 攻撃を防止することができる．DoS 攻撃者は身元が特定されないように IP アドレスを偽造するため，サーバが事前に作成したクッキーの対応テーブルに攻撃者の IP アドレスが該当しない．サーバがクッキーの対応テーブルを確認することにより防ぐことができる．TSSAP のシーケンスでは 11. の処理がディジタル署名の検証，復号化の公開鍵は処理が入るため事前にクッキーのチェックによりこの処理が不用意に実行されないようにすることにより，DoS 攻撃を防いでいる．

4.2 リプレイアタック

リプレイアタックはパスワードや暗号鍵を盗聴しそのまま再利用することでユーザに成り済ます方法である．TSSAP では乱数 Rs を使用することによってリプレイアタックを防いでいる．乱数 Rs は，ユーザを認証するためのパスワードが認証時に入力された

ものであるかどうかを確認するために利用する．攻撃者が認証に成功したパケットを用いてリプレイアタックを試みても，乱数を比較した際に乱数が同じであると拒否する．TSSAP のシーケンスでは 10. のパケットをもう一度送られてしまうとクライアント認証なしでシーケンスが進んでしまう危険があるため，乱数を用いて防いでいる．

4.3 中間者攻撃

中間者攻撃とは通信を行う 2 者の間に割り込んで両者が交換する公開情報を自分のものとすりかえることにより，気づかれることなく盗聴，通信内容に介入する方法である．・スマートフォン-クライアント間 Bluetooth が使用するプロファイル SPP は 1 対 1 の通信を前提としているため，1 対 1 でしか通信できない．このため攻撃者がスマートフォン-クライアント間に入り込むことはできない．従って中間者攻撃は成り立たない．・クライアント-サーバ間 TSSAP ではクライアント-サーバ間に対してディジタル署名を用いている．従って中間者攻撃は成り立たない．

4.4 紛失，盗難

TSSAP ではクライアントに一切初期情報を持たないため，クライアントが盗難，紛失しても問題はない．また，スマートフォンの紛失，盗難に関してはスマートフォン内にある重要な秘密情報は暗号化されているため流出してしまっても問題ない情報である．

このためスマートフォンから情報を抜き取ったとしても成りすましすることはできず，また，盗んだスマートフォンを利用して認証を行う際にはパスワードが必要なため，TSSAP では紛失，盗難に関しても安全である．

5 実装方式

TSSAP のモジュールの構成図を図 6 に示す．

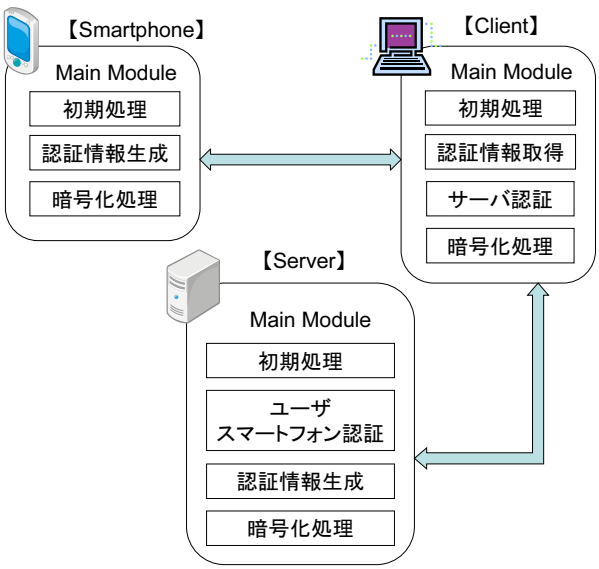


図 6: TSSAP モジュール構成

各端末には共通するモジュールと固有のモジュールで構成される．メインモジュールは処理状態を管理し，状態に対応したサブモジュールを呼び出す．暗号化処理はパケット通信における暗号/復号を行う．初期処理はシステムの初期化を行う．

クライアント固有のモジュールは認証情報取得とサーバ認証がある．認証情報取得モジュールはユーザが画面にパスワードを入力することでパスワードの取得を行う．サーバ認証モジュールはサーバ署名情報を検証する．

サーバ固有のモジュールはユーザ, スマートフォン認証，認証情報生成がある．ユーザ, スマートフォン認証モジュールはスマートフォンの署名情報を検証するための処理を行う．認証情報生成モジュールはサーバ認証に必要な情報を生成する．

スマートフォン固有のモジュールは認証情報生成がある．認証情報生成モジュールはスマートフォン認証に必要な情報を生成する．

6 むすび

本論文ではクライアントサーバ間で重要情報を安全に交換する方式 TSSAP を提案した．クライアントが秘密情報を持たないため， クライアントからの情報漏洩の心配がなく， クライアントを自由に選べるという利点を持つ．

参考文献

[1] NPO 日本ネットワークセキュリティ協会セキュリティ情報セキュリティ大学院大学，2011 年情報セキュリティインシデントに関する調査報告書

[2] 磯部義明，三村昌弘, 瀬戸洋一，菊地良知，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，Vol.99-CSEC-4，No.24，pp.55—60.

[3] 磯部義明，三村真一，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，99-CSEC-4,Vol.99,No.24,pp.55-60.

[4] 影井良貴，IC カードの動向，情報処理学会会誌，Vol.39，No.5，pp.429—433 .

[5] 吉田壱，平田真一，IC カード技術の現状と課題，情報処理学会会誌，Vol. 43，No. 3，pp. 296-303.

[6] 伊藤雅彦，非接触 IC カード技術とその応用，情報処理学会会誌，Vol.43，No.3，pp.304—307 .

[7] 渡邊晃，岡崎直宣，朴美娘，井手口哲夫，笹瀬巌，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，121-C，No. 9，pp. 1429-1438.

[8] 束長俊，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，No. 3，pp. 304-307.

[9] 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.

[10] Specification of the Bluetooth System—Version 2．0 + EDR.

[11] Bluetooth Test Specification—RF， Part A，For Specification 2．0， Revision 2．0.

[12] Diffie，W. and Hellman，New Directions in Cryptography，IEEE Transactions on Information Theory，Vol. IT-22，No. 6，pp.644-654.

クライアントを自由に選択可能な認証プロトコルTSSAPの提案

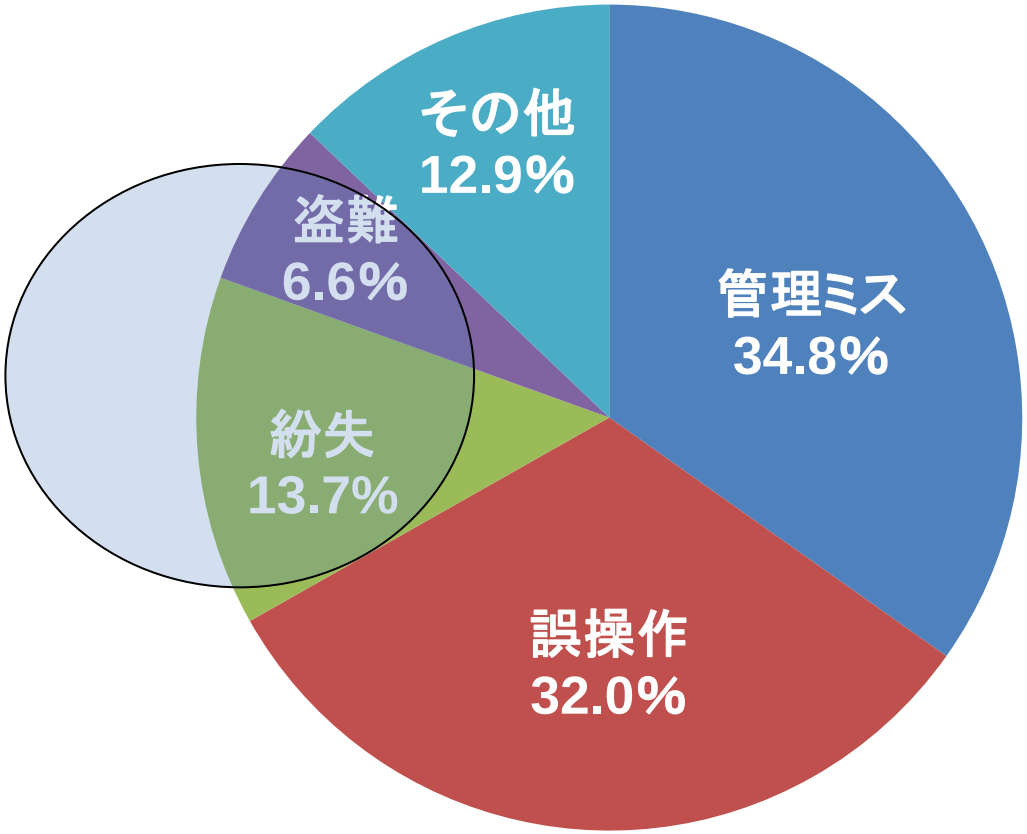
名城大学大学院 理工学研究科
五島 秀典　鈴木 秀和　旭 健作　渡邊 晃

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



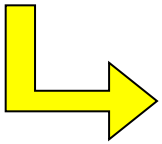
システムでカバーできる

出典：NPO 日本ネットワークセキュリティ協会

紛失/盗難

- 事例

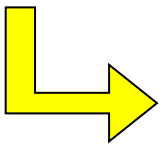
自宅に空き巣が入りPCごと盗難,電車内に置き忘れ
USBメモリなど記憶媒体の置き忘れ,紛失　etc・・・

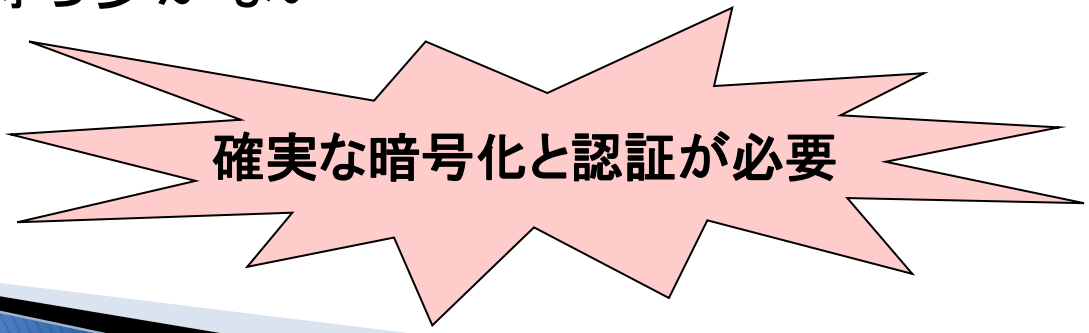


情報を社外へ持ち出すことが共通点

- 解決策

社内サーバとクライアント間で鍵を共有することで通信路を確立し
社内情報を持ち歩かない





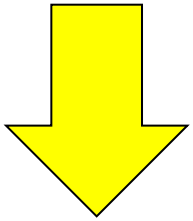
目的

- 異なるクライアントからサーバへアクセス
  - サーバ内の情報にどこからでもアクセス
- クライアント/サーバ間の安全確保
  - 確実な認証
    - 認証方式の組み合わせ
  - 各種攻撃に対応
    - DoS攻撃
    - 中間者攻撃
    - リプレイアタック

認証方式の組み合わせ

例

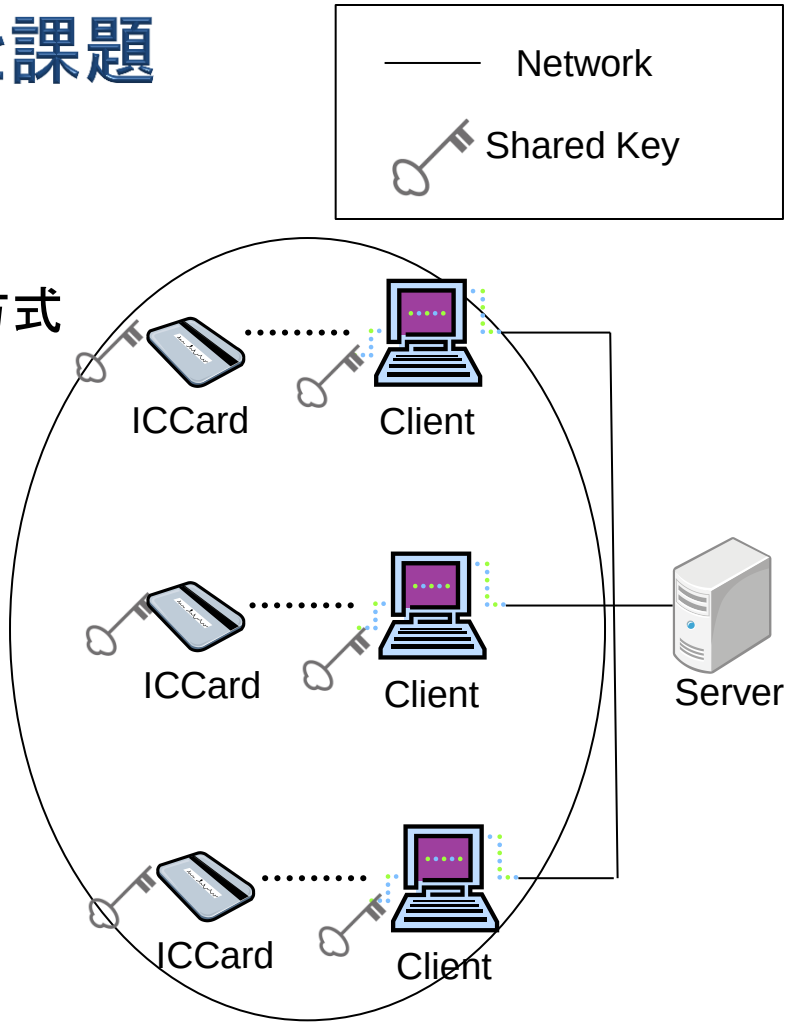
- パスワードでの認証
- カード，USBなどの記憶媒体での認証
  - ユーザが所有する記憶媒体に電子証明書，暗号鍵などを記憶



両者を組み合わせることでセキュリティ向上

ICカードを利用した認証方式と課題

- 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
  - クライアントとサーバ間は公開鍵で認証
- 課題
  - クライアントから共有鍵が漏洩
    - 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
    - 同じ鍵を使い続けることでセキュリティ低下
    - 管理が煩雑になる



出典：日本ICカードシステム利用促進協議会(JISAP)

TSSAPの提案

- TSSAP (Terminal Selectable and Secure Authentication Protocol)

- 特徴
  - スマートフォンを認証デバイスとして利用
    - スマートフォンを利用することにより利便性の向上
  - 特別なハードウェアが不要
  - クライアントに初期情報を持たせない
    - クライアントからの情報漏洩の防止
  - クライアントを選択できる

TSSAP初期情報

- ユーザID
- Eパスワード[SP秘密鍵]
- サーバ公開鍵

なし

- サーバ秘密鍵
- ユーザID
- SP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

※パスワードはパスワードのハッシュ値をとった値
※$E_A[B]$　BをAで暗号化

既存技術とTSSAPの初期情報の比較

	TSSAP	ICカード
ユーザの所持する媒体 （SmartPhone,ICCard)	ユーザID $E_{パスワード}$[SP秘密鍵] サーバ公開鍵	ユーザID IC秘密鍵 パスワード サーバ公開鍵 事前共有鍵
Client	-	事前共有鍵
Server	ユーザID SP公開鍵 サーバ秘密鍵	ユーザID IC公開鍵 サーバ秘密鍵

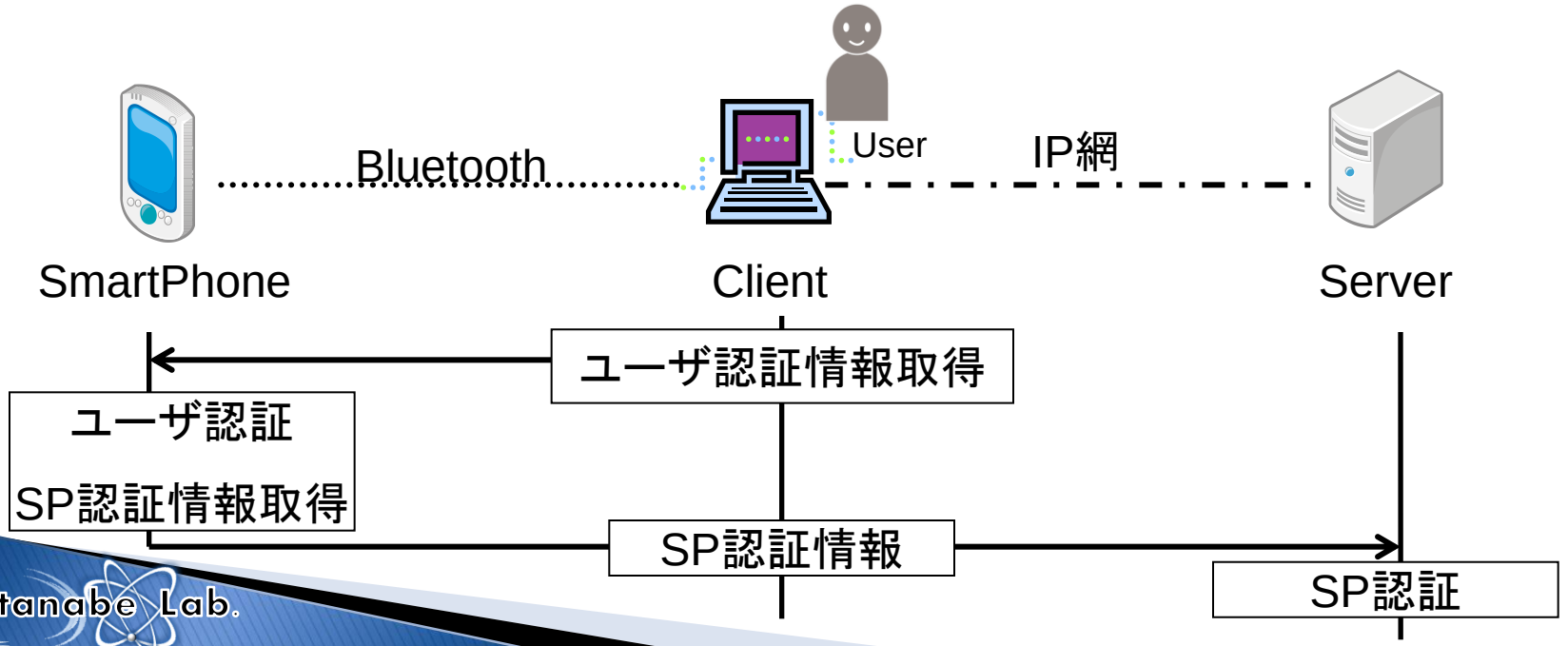
ユーザ認証

- クライアント型認証
  - スマートフォン内でユーザ認証を行う
  - スマートフォンの認証をサーバ側で行う

- サーバ型認証
  - サーバ側でユーザ，SP認証を行う

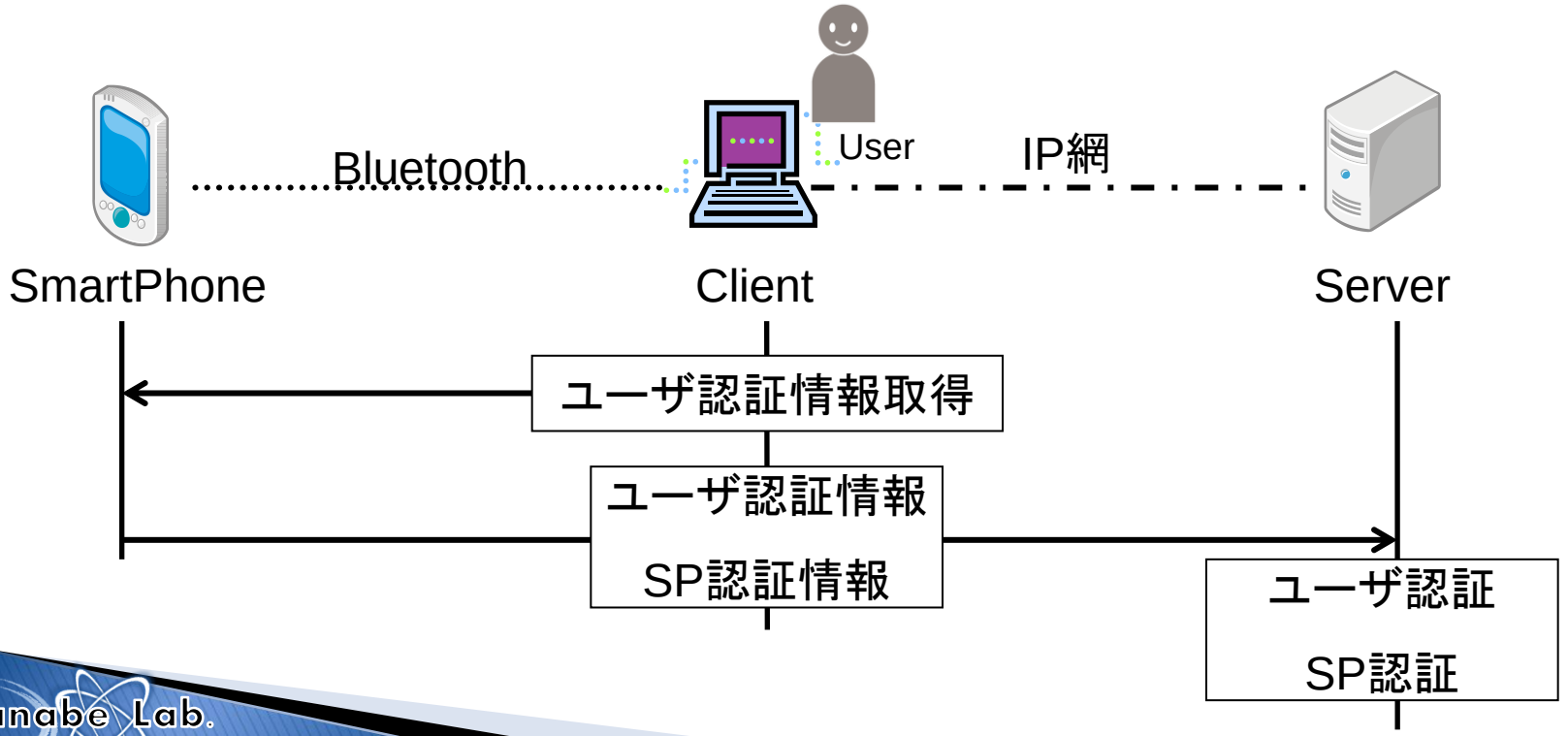
ユーザ認証(クライアント型認証)

- クライアント型認証
- 課題
  - スマートフォンにユーザ認証情報を保持させているため，スマートフォンの処理負荷が大きくなる
  - 耐タンパ性のあるデバイスが必要



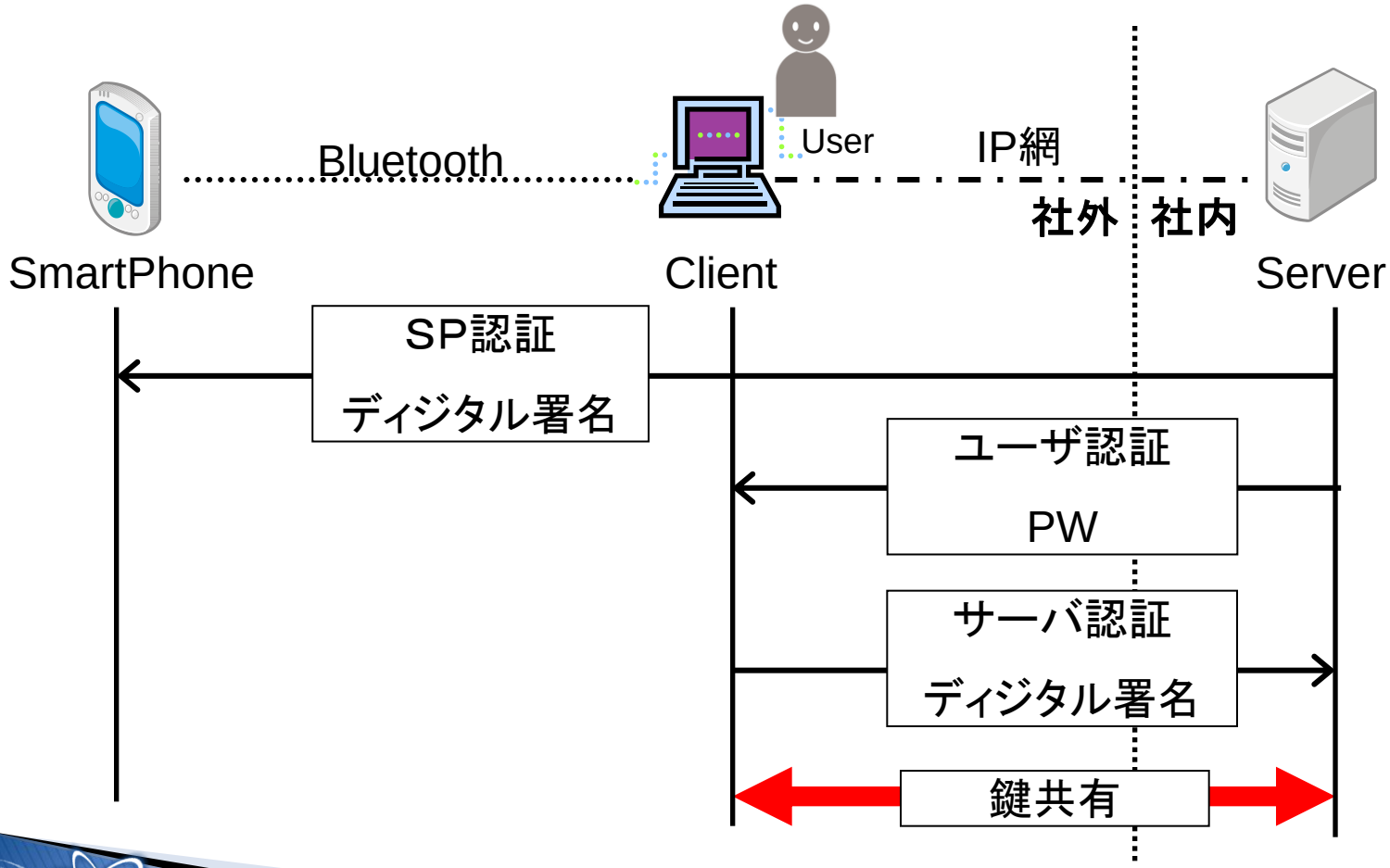
ユーザ認証(サーバ型認証)

- サーバ型認証
- 課題
  - サーバに全ユーザの情報を管理する必要がある
    - サーバの管理体制が重要となる



TSSAPの構成と認証

- TSSAPではサーバ型認証を採用する
  - スマートフォンに耐タンパ性がないため



ユーザの動作

- 前提
  - ユーザは常にスマートフォンを携帯
  - クライアントおよびスマートフォンにTSSAPのアプリケーションをインストール
  - クライアントおよびスマートフォンがBluetooth対応であること
- 動作

①両端末のアプリケーションを起動
②スマートフォン-クライアントをペアリングする
③クライアントからパスワード入力

TSSAP前準備

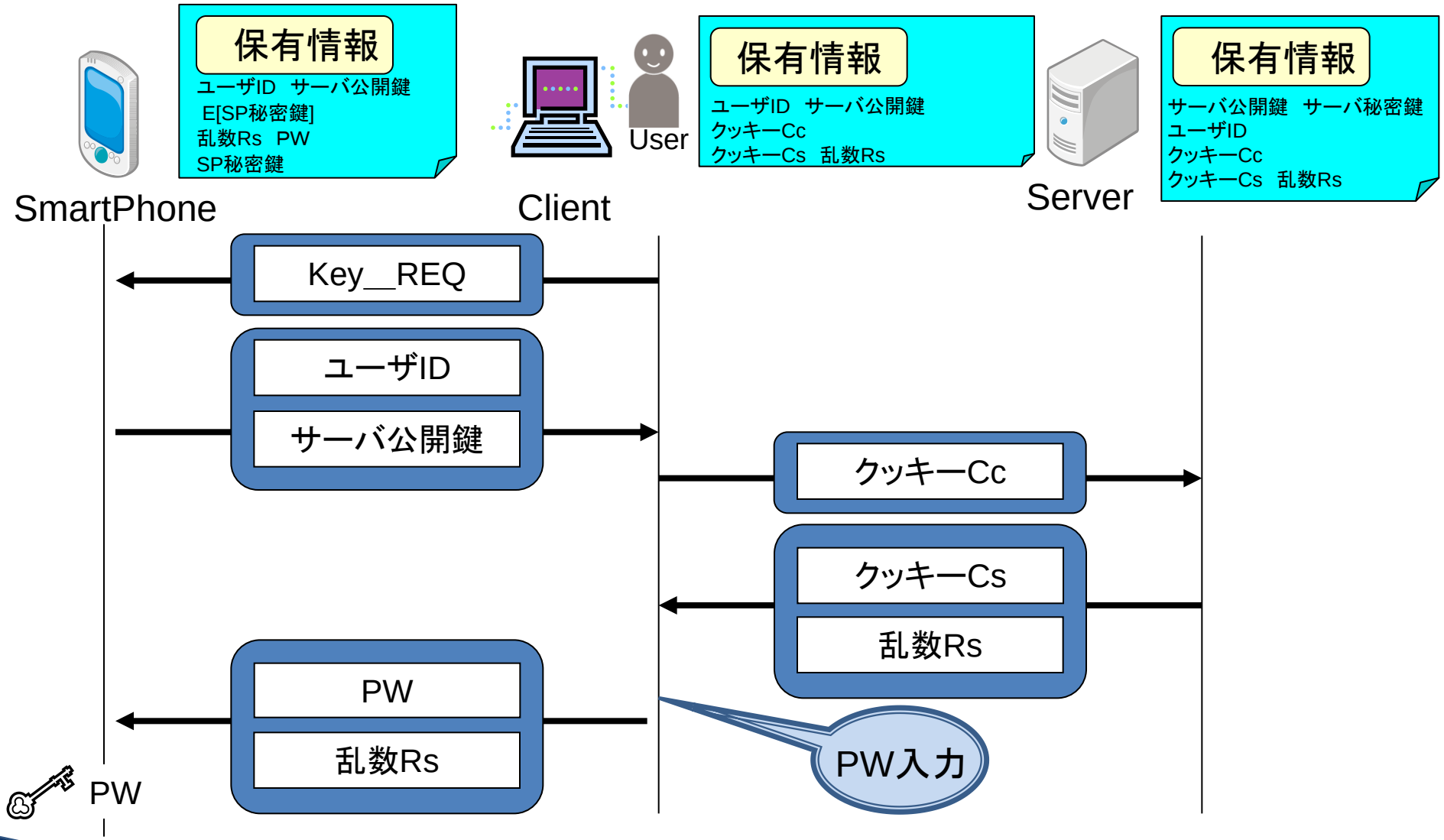
- 両端末でアプリ起動
- スマートフォン–クライアント間でBluetoothペアリング
  - セキュアシンプルペアリング

スマートフォンの画面

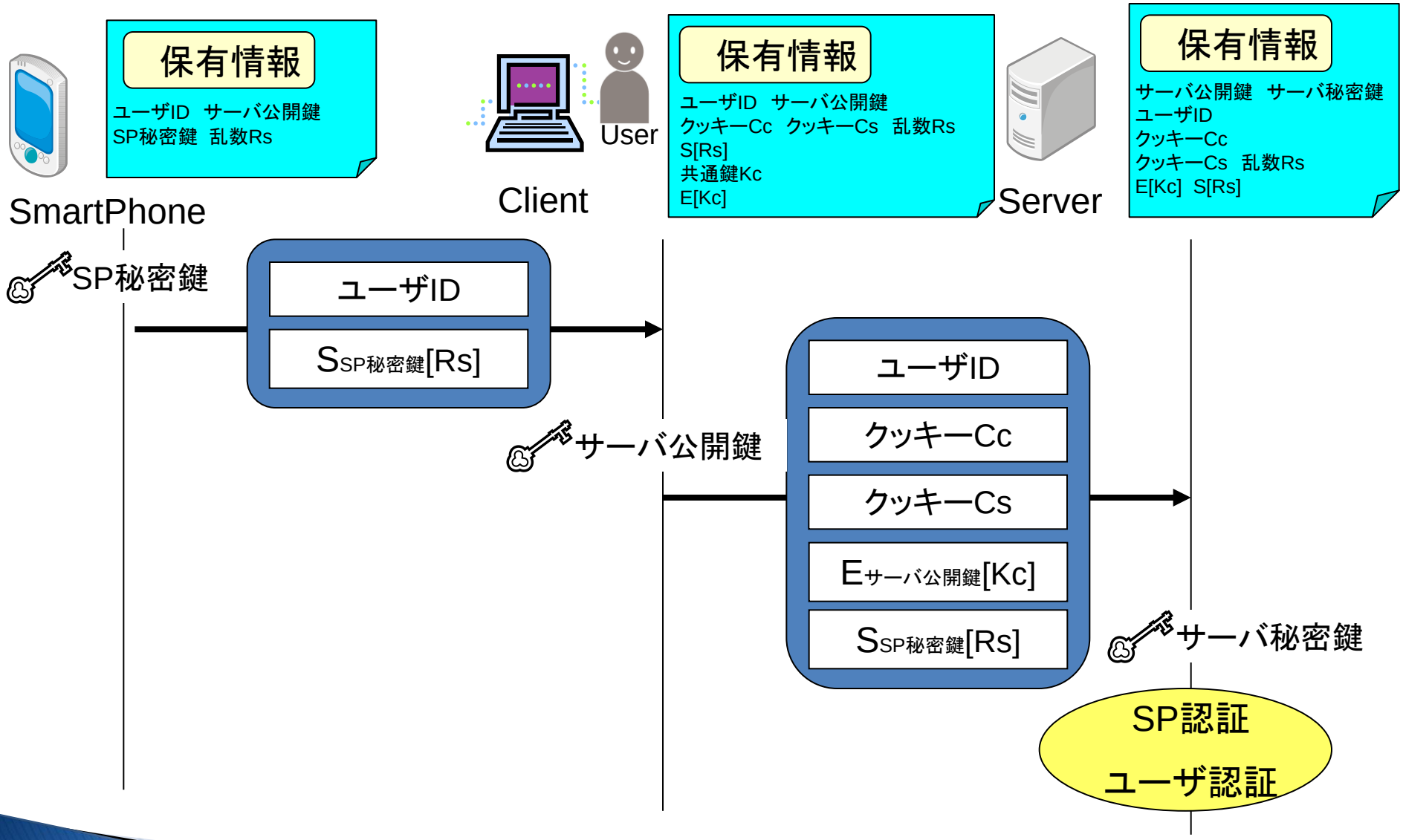
クライアントの画面

動作

TSSAP動作(ユーザ認証)

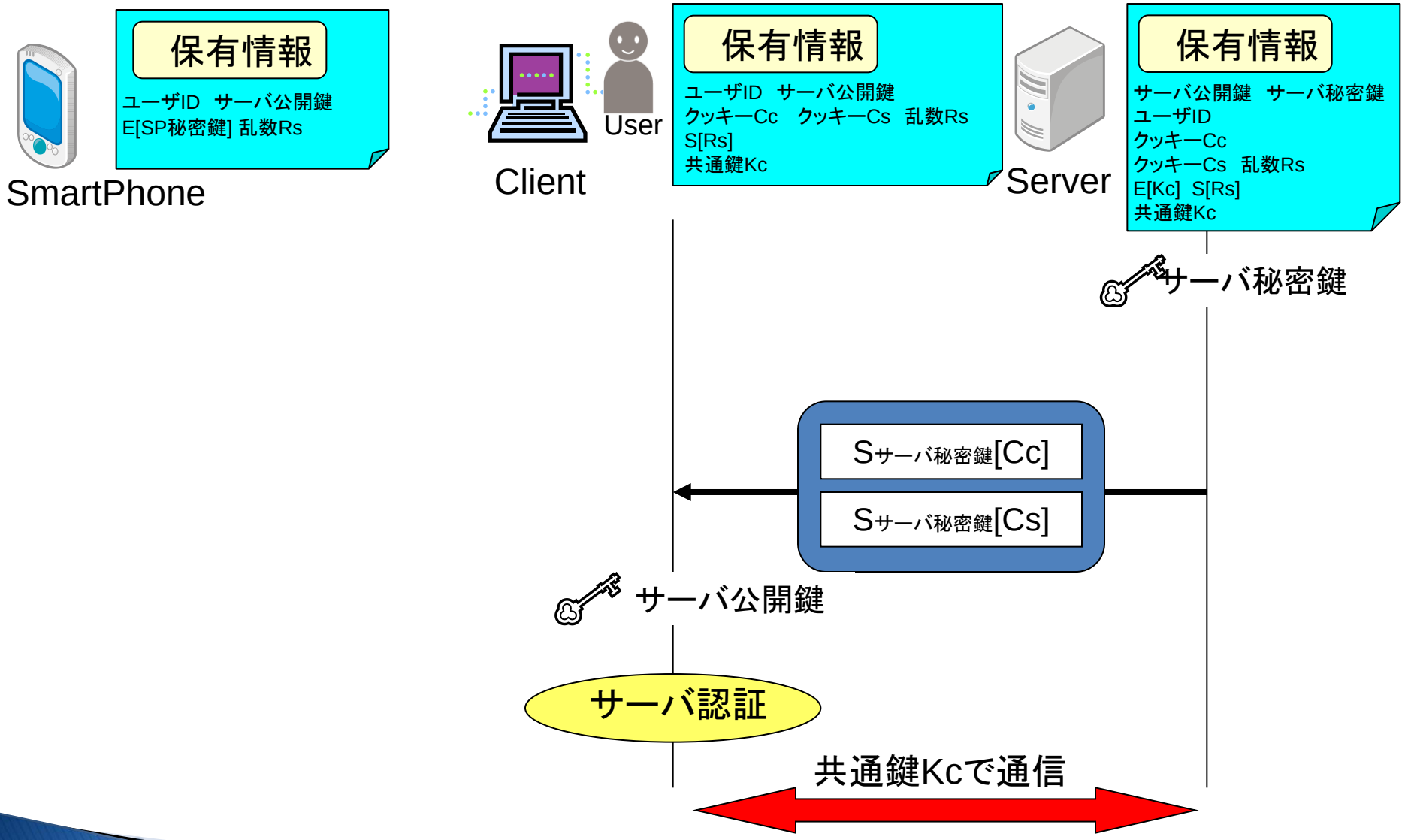


TSSAP動作(ユーザ,SP認証)



※$S_A[B]$　BをAでディジタル署名

TSSAP動作(サーバ認証)



各種攻撃への対策

DoS攻撃への対策

- 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
- クッキーを交換することで防ぐ

Client

Server

クッキーCcをIPアドレス,時間情報,乱数をもとに生成

クッキーCc

クッキーCs

クッキーCsをIPアドレス,乱数,時間情報をもとに生成

接続してきたクライアントのIPアドレスを対応させて記憶

攻撃者

関係のないパケット

テーブルを確認

一致しなければ破棄

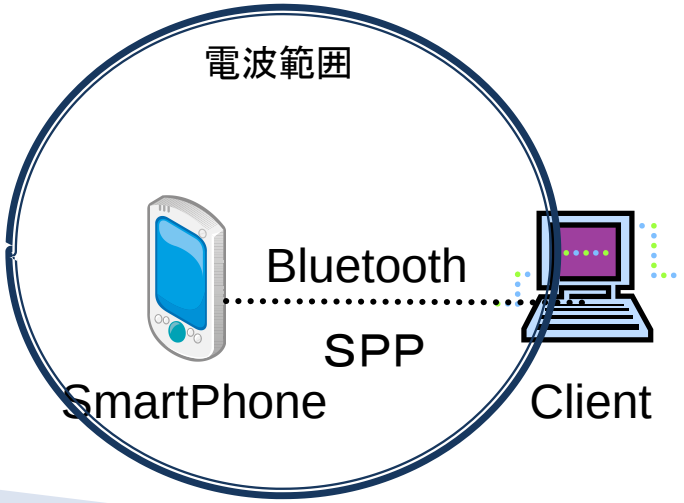
※偽装IPアドレス使用

クッキー	クライアントIPアドレス
Cc	192.168.111.111
Cc(a)	192.168.222.222

IPアドレスとクッキーに関するテーブル

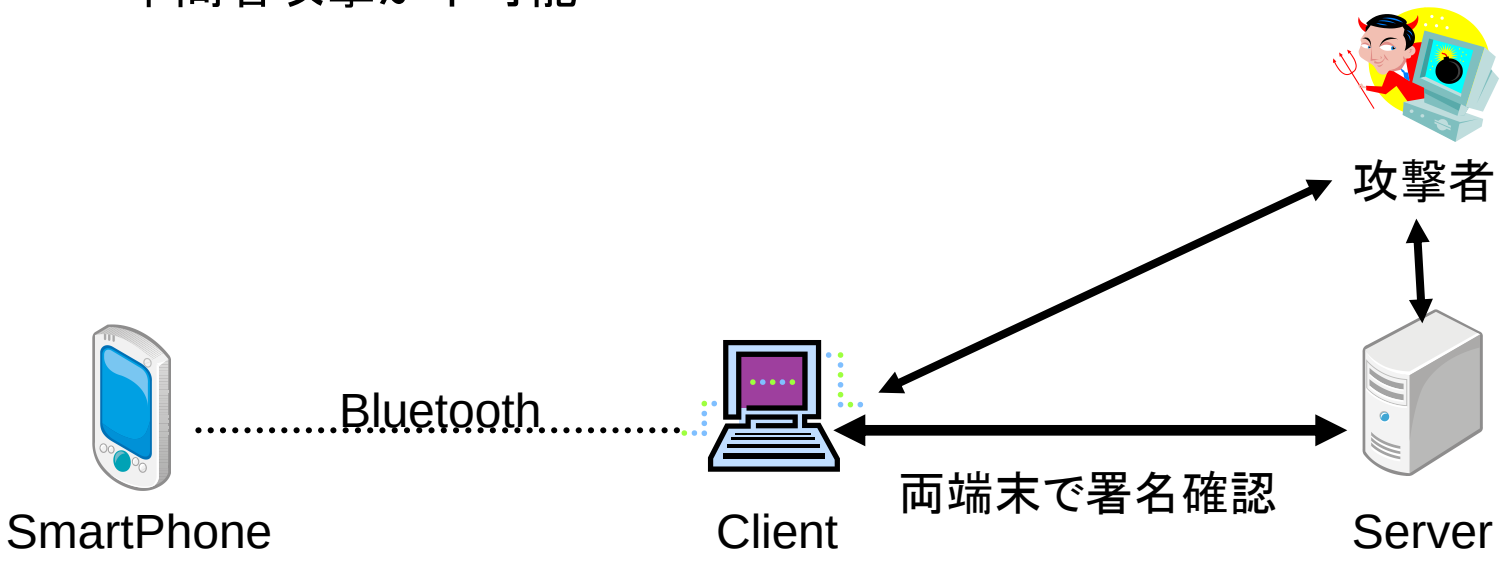
中間者攻撃による対策(1/2)

- 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または、通信内容に介入したりする手法
- スマートフォン-クライアント間(Bluetooth通信)
  - ペアリング時
    - Bluetoothの電波到達距離を制限することで介入を不可とする
  - ペアリング後
    - プロファイルSPP (Serial Port Profile)の利用
      - 1対1通信を前提としたプロファイルのため攻撃者が通信に介入不可
      - 中間者攻撃が成り立たない



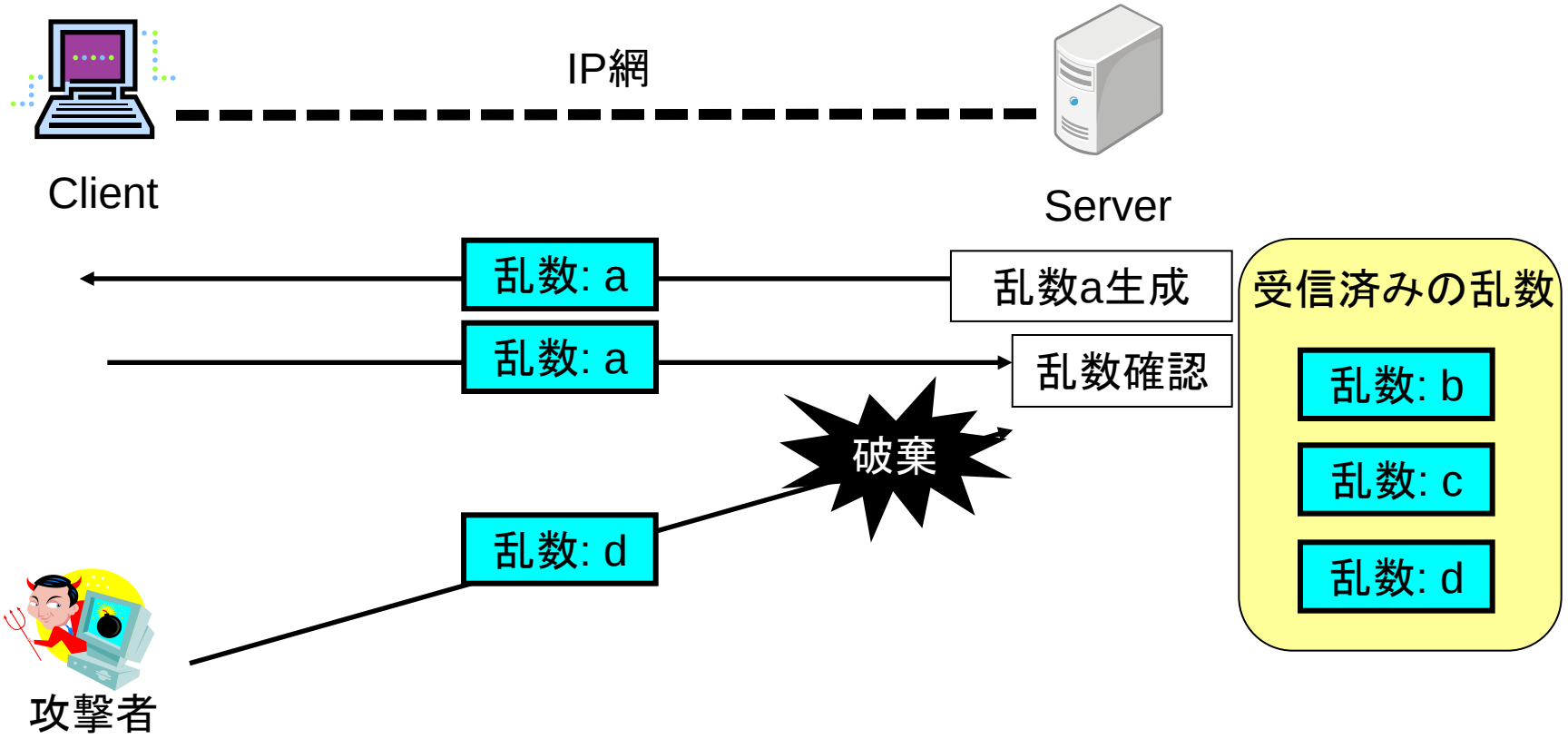
中間者攻撃による対策(2/2)

- クライアント–サーバ間
  - クライアントからの情報をディジタル署名で確認
  - サーバからの情報をディジタル署名で確認
  - エンドエンドでディジタル署名を確認するため
    中間者攻撃が不可能



リプレイアタックへの対策

- 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
- 乱数をメッセージに付加し,乱数を確認する



※乱数:d　攻撃者があらかじめ通信内容を記録したパケット

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路の確立
  - 各種攻撃へ対応
- 今後
  - 現在実装中のTSSAPを完成させ，性能評価する

終