クライアントを自由に選択できる認証プロトコル TSSAP の提案

五島　秀典　　鈴木　秀和　　旭　健作　　渡邊　晃

名城大学大学院理工学研究科

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

Hidenori Goshima　Akira Watanabe　Hidekazu Suzuki　Kensaku Asahi

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る．また，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．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，クライアントから共有鍵が漏洩する可能性がある[2-5].

また，別の方法として SSL-VPN を使用した認証方式がある．認証方式にはパスワードを用いた方法やクライアントや記憶媒体に電子証明書を保持させる方法がある．パスワードによる方式はパスワードが漏洩する可能性があり，セキュリティレベルは低いといわれている．そのため企業ネットワークでは電子証明書による方式が用いられる．しかし，SSL-VPN を使用しているために使用できるプロトコルに制限があり，自由度が失われるという課題がある.

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

2.　1　IC カードを利用した認証手法

図 1 に非接触 IC カードを利用した認証方式を示す[6].
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方式が定義されている．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.

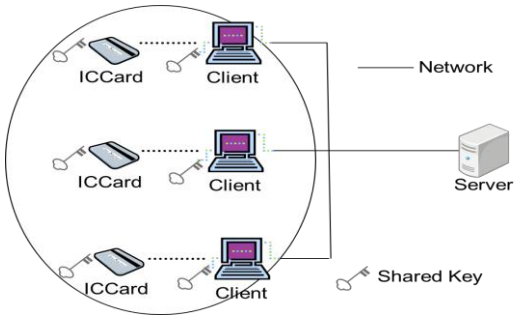


図 1　IC カードを利用した認証方式

2.　2　SSL-VPN を利用した認証方式

SSL-VPN は SSL（Secure Socket Layer）技術を使用した VPN(Virtual Private Network)ソリューションである．SSL の暗号化技術を用いてクライアントとサーバの間にトンネルを構築することによりサーバとクライアントで重要な情報を交換することができる.この方式ではユーザを認証する場合，パスワードを使用した認証方式が一般的である．しかし，パスワードのみを使用した場合パスワードが漏洩する危険があり，ひとたび漏洩すると簡単に成りすましが可能となってしまうためセキュリティレベルは低いといわれている．セキュリティレベルを上げるために企業ネットワークではパスワードと電子証明書を組み合わせた認証方法がある[7]. 具体的には電子証明書を耐タンパ性のある Keymobile[9]という microSD 型の記憶媒体に格納し，スマートフォンに装着する.

2.　3　Keymobile による認証

Keymobile は IC カード，フラッシュメモリ，コントローラから構成され，コントローラがフラッシュメモリと IC カードへのアクセスをコントロールする．フラッシュメモリへは制約なしにアクセスすることができるが, IC カード領域にはユーザがあらかじめ設定しておいた PIN コードと呼ばれる文字列の入力が必要である．Keymobile ではこの IC カード領域において PIN コードが流出しない限り IC カード内に格納された情報が不正に読みだされることがないため耐タンパ性を有している.

図 2 に Keymobile を利用した認証方式の概要を示す.

ユーザはサーバと SSL で鍵共有をするためクライアントからパスワードを入力する．また，スマートフォンの IC カード領域にある電子証明書を取得するため PIN コードを入力する.

クライアントは Keymobile から電子証明書を受け取り, 受け

取った電子証明書をサーバへ送る．これがサーバ側で正しいと判定されると認証が完了する．ユーザは普段からスマートフォンを持ち歩き，認証したい時にスマートフォンを取り出して認証する．スマートフォン-クライアントの間はBluetooth の標準搭載されている鍵共有アルゴリズムを使用するため安全に暗号化通信が行える[9，10]．しかし，この認証方式では，ユーザの覚えておくパスワードが 2 つ必要となる上，Keymobile という特殊な記憶媒体が必要となる．また，SSL を使用しているため，サーバへのアクセスにプロトコルの制限があり，社内システムすべてにアクセスできず，自由度が失われているという課題がある．

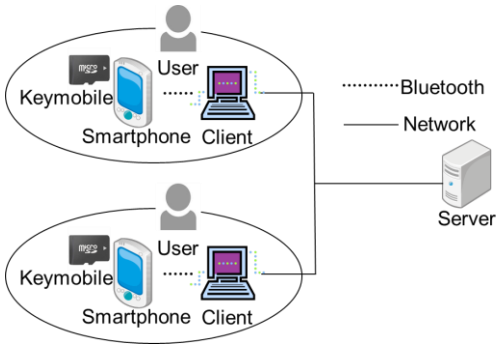


図 2 Keymobile を用いた認証方式の概要

3. TSSAP の提案

TSSAP(Terminal Selectable and Secure Authentication Protocol)はスマートフォンだけに秘密情報を持たせた認証プロトコルである．クライアントに秘密情報を一切所持させないためユーザが自由にクライアントを選択できることに加え，クライアントから秘密情報が漏洩する心配がないという利点がある．また，パスワードは 1 つだけでよく，普段持ち歩いているスマートフォンを認証用デバイスとして使用できる．

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 3 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．

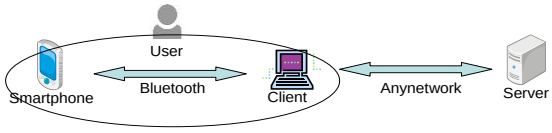


図 3 TSSAP のシステムモデル

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
Nr	サーバが生成する乱数
Ci	クライアントが生成するクッキー
Cr	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，スマートフォン公開鍵で暗号化したパスワード，サーバ公開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．

表 1 TSSAP の初期情報

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

3. 4 認証関係

TSSAP 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．図 3 に認証関係を示す．

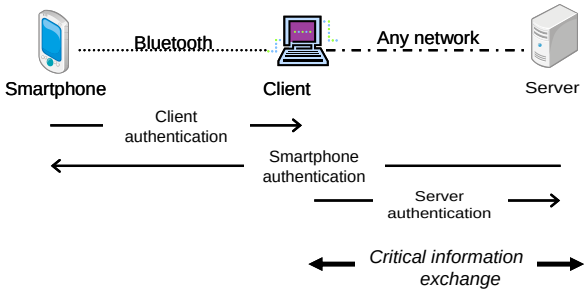


図 4 TSSAP の認証関係

矢印の方向は認証の方向を示している．ユーザはクライアントを操作しているため，両者は一体とみなすことができる．スマートフォンはユーザがクライアントから入力したパスワードを利用して，クライアントを認証する．サーバはスマートフォン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．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．

3. 5 Bluetooth 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．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．

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．

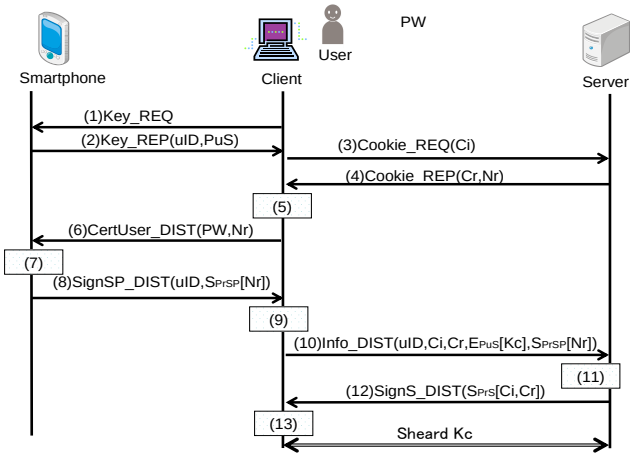


図 5 TSSAP シーケンス

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．

(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Ci 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 Nr と DoS 攻撃防止のクッキーCr 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Cr と共に乱数 Nr 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 Nr をスマートフォンへ送る．

(7) クライアント認証
スマートフォンは E_{PW}[PrSP]を受け取った PW で復号する．復号された PrSP を使って E_{PuSP}[PW]，を復号する．復号した PW と受け取った PW を比較することによりクライアント認証する．

(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 Nr 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}[Nr]と共に uID，Ci，Cr をサーバへ送信する．

(11) スマートフォン認証と署名の作成
暗号化された Kc をサーバ秘密鍵 PrS で復号する．受信した Nr とサーバが(4)で生成した Nr を比較する．S_{PrSP}[Nr]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．また，クッキーCi，Cr 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 Ci，Cr にサーバ秘密鍵 PrS を用いてディジタル署名を行う．

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

(13) サーバ認証
S_{PrS}[Ci, Cr]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環状の認証が完了し，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，中間者攻撃に対する対策として以下の手段を取っている．また，スマートフォンに秘密情報を保持させることの安全性についても考察する．

(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．

(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 Nr 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 Nr 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．

(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)スマートフォンからの秘密情報漏洩

TSSAP では安全を考慮して秘密情報であるスマートフォン秘密鍵を PW で暗号化している．また，PW をスマートフォン公開鍵 PuSP で暗号化している．秘密情報をすべて暗号化することによって外部にスマートフォンから情報が漏れた場合でも秘密情報が守られる．

5. 実装方式

TSSAP のモジュールの構成図を図 6 に示す．

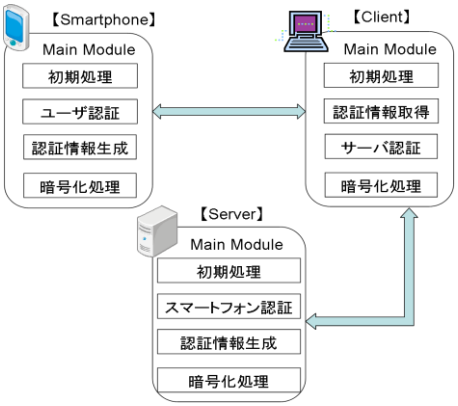


図 6 TSSAP モジュール構成

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スマートフォン認証と認証情報生成がある．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ユーザ認証と認証情報生成がある．ユーザ認証モジュールはクライアントから受信したパスワードを照合することでユーザ認証処理を行う．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(2011)

[2] 伊藤 雅彦 非接触 IC カード技術とその応用，情報処理学会，(1)IC カードシステム利用促進協議会:JICSAP ID カード仕様書 V2．0(2001)

[3] 渡邊晃，厚井裕司，井手口哲夫，横山幸夫，妹尾尚一郎，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，pp．904-914，(1997)

[4] 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 (2001)．

[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，(2002)．

[6] 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，(1999)

[7] 梅澤 克之，手塚 悟， スマートホンをセキュアデバイスとして用いるリモート接続システムの開発と評価，電子情報通信学会論文誌，J94-B No．4 (2011)

[8] 岡崎 司，畠山 誠基，佐藤 隆一，”KeyMobile を用いた安全なデータ持ち出し”，日立 TO 技報第 15 号(2009)

[9] Specification of the Bluetooth System―Version 2．0 + EDR， Volume 0， N (2004)

[10] Bluetooth Test Specification―RF， Part A，For Specification 2．0， Revision 2．0， (2005)

[11] 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，(2009)．

[12] 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，(2007)．

クライアントを自由に選択できる認証プロトコルTSSAPの提案

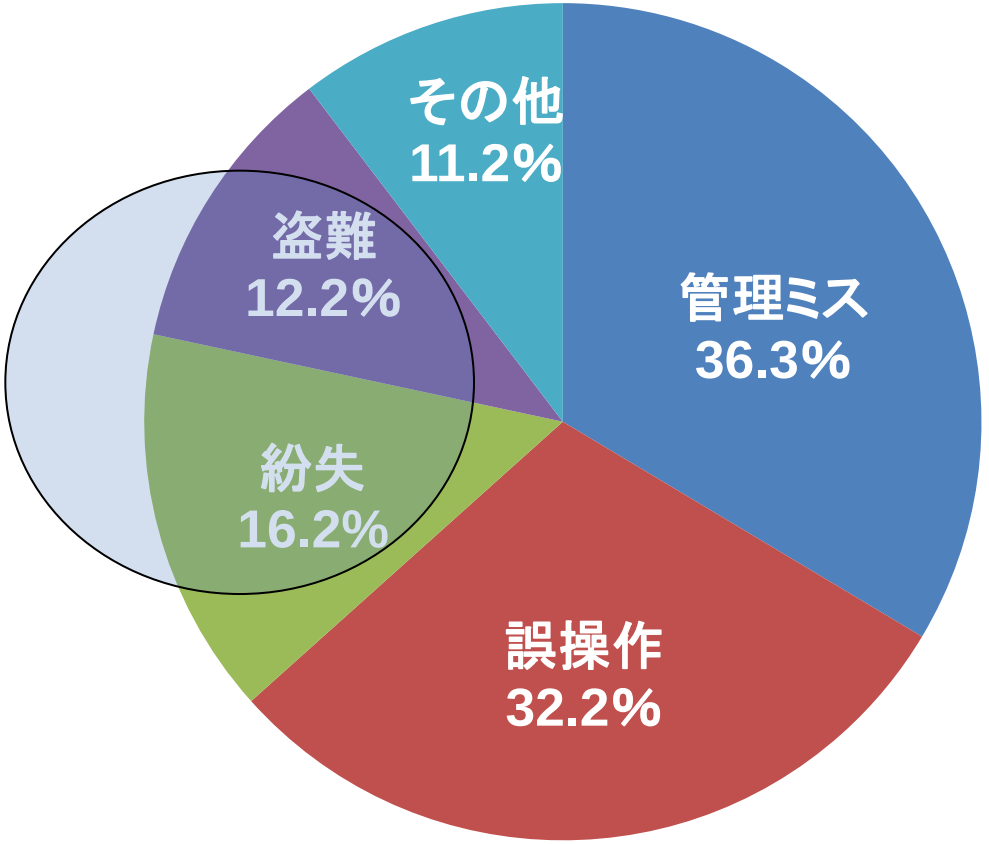
名城大学大学院 理工学研究科
五島 秀典　鈴木 秀和　旭 健作　渡邊 晃

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



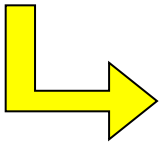
システムでカバーできる

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

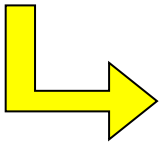
自宅に空き巣が入りPCごと盗難,電車内に置き忘れ
USBメモリなど記憶媒体の置き忘れ,紛失　etc・・・

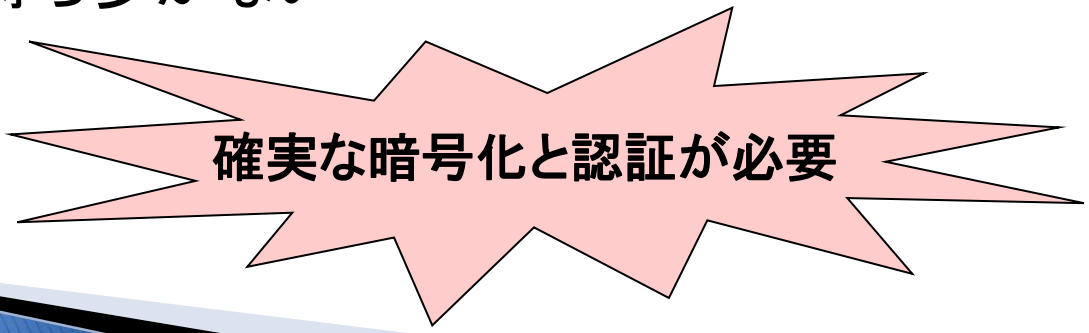


情報を社外へ持ち出すことが共通点

- 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



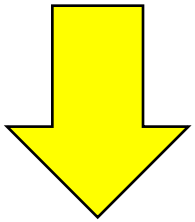


確実な認証と暗号化

- 情報を暗号化
- 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の例

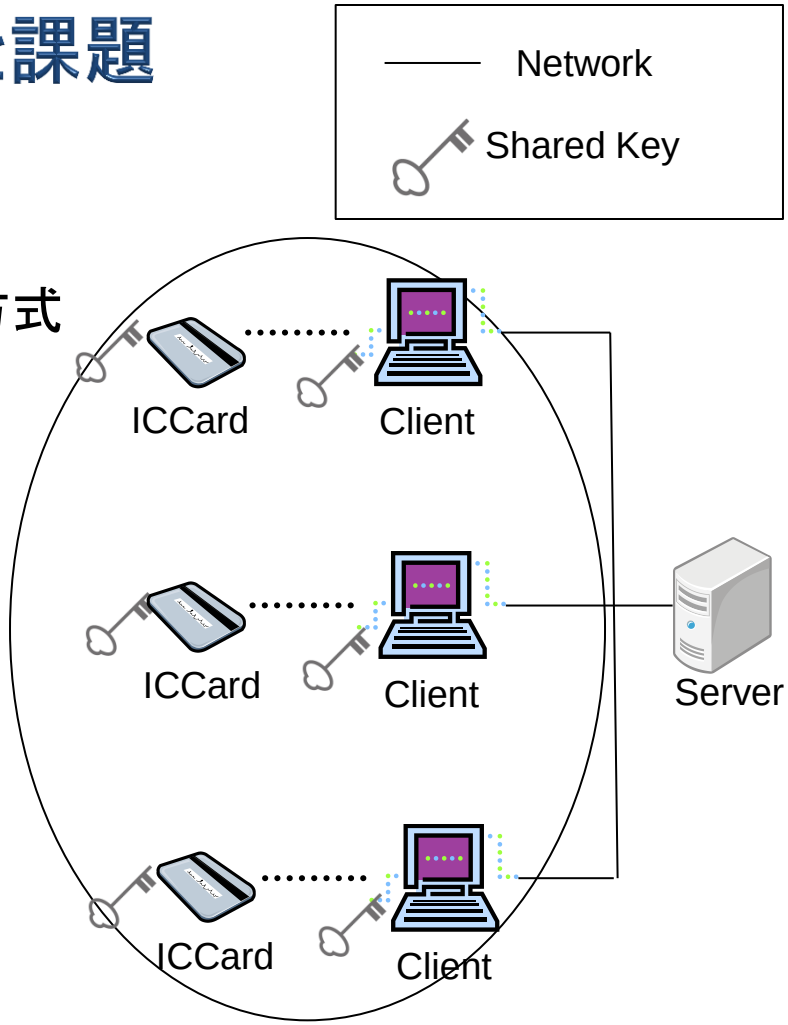
- ユーザのみが知っているパスワードでの認証
- ユーザにカード，USBなどの記憶媒体での認証
  - ユーザが所有する記憶媒体に電子証明書，暗号鍵などを記憶



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

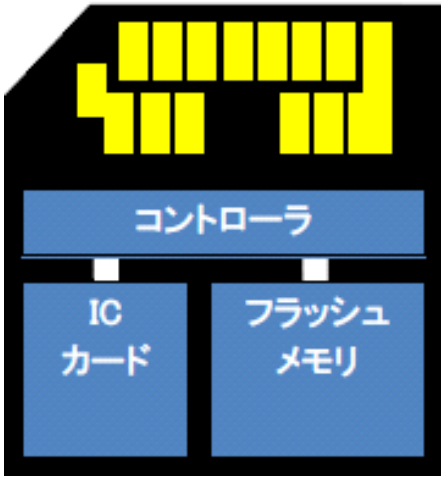


出典：日本ICカードシステム利用促進協議会(JISAP)

Keymobileを用いた認証方式と課題(1)

- 特徴
  - クライアント/サーバ間はSSL
  - どんなクライアントでも使用可能
  - スマートフォンにKeymobileを装着し，スマートフォンを認証デバイスとして用いる

- Keymobileとは
  - ICカード領域,フラッシュメモリ，コントローラで構成
  - ユーザがPINコードを設定
  - PINコードの入力でICカード領域へアクセス
  - PINコード流出しない限り耐タンパ性を有する



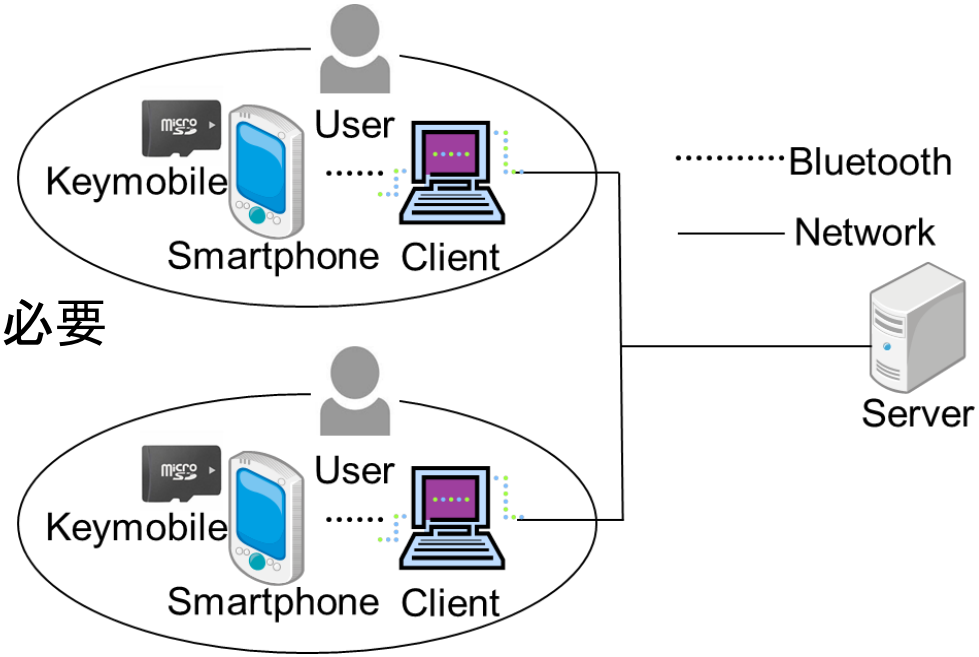
Keymobileの構造

出典：スマートホンをセキュアデバイスとして用いるリモート接続システムの開発

Keymobileを用いた認証と課題(2)

- 認証方法
  ①microSD型Keymobileをスマートフォン(SP)へ装着
  ②ユーザはSSL鍵共有のためPWを入力する
  ③PINコードを入力し，ICカード領域内の電子証明書を取出し，サーバへ送信
  ④サーバで電子証明書を確認

- 課題
  - Keymobileという記憶媒体が必要



Keymobile　初期情報

ICカード領域	電子証明書
フラッシュメモリ	なし

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
  - クライアントを自由に選択できる

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
- 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初期情報

SmartPhone

- ユーザID
- Eパスワード[SP秘密鍵]
- サーバ公開鍵
- E SP公開鍵[パスワード]
- SP公開鍵

Client

なし

Server

- サーバ秘密鍵
- ユーザID
- SP公開鍵

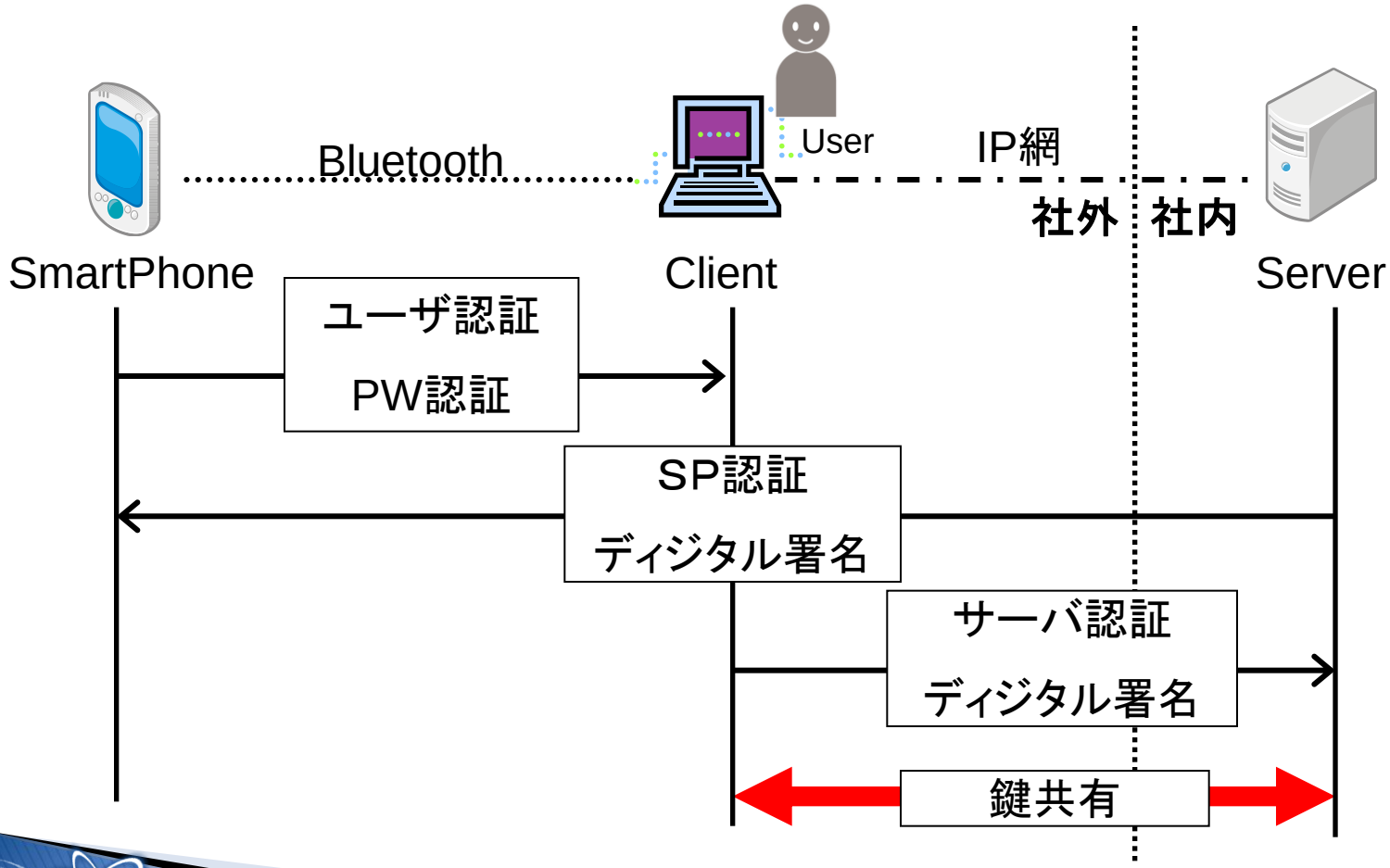
※パスワードはパスワードのハッシュ値をとった値
※EA[B]　BをAで暗号化

既存技術とTSSAPの初期情報の比較

	TSSAP	Keymobile	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] $E_{SP公開鍵}$[パスワード] サーバ公開鍵	電子証明書 PIN	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 PW	ユーザID IC公開鍵 サーバ秘密鍵

TSSAPの構成と認証

- 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



動作

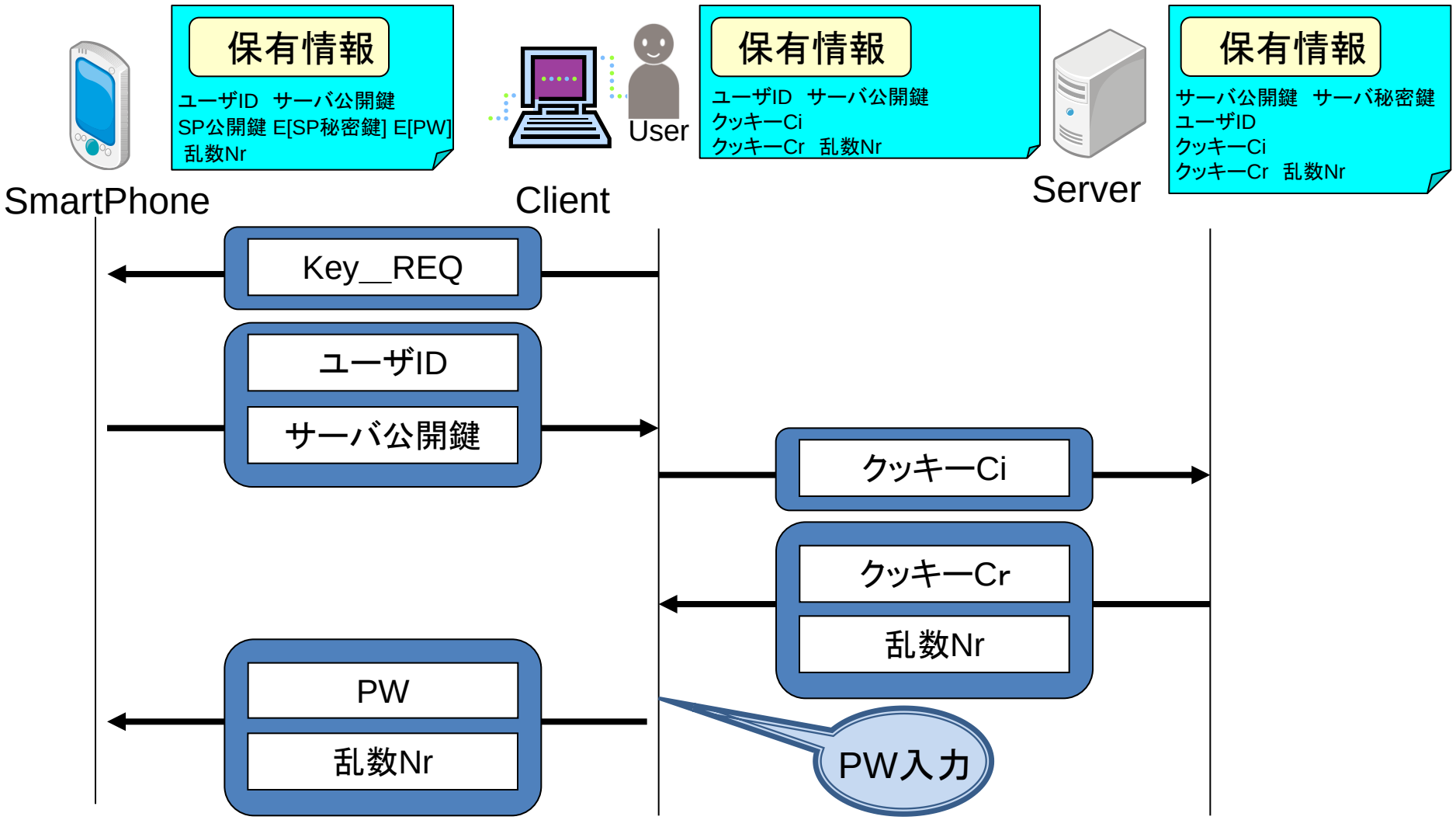
TSSAP前準備

- 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
  - PINを使ったペアリング
  - セキュアシンプルペアリング(Bluetooth2.1＋EDR以上)

スマートフォンの画面

クライアントの画面

TSSAP動作(ユーザ認証1/2)



TSSAP動作(ユーザ認証2/2)

保有情報

ユーザID　サーバ公開鍵
SP公開鍵 E[SP秘密鍵] E[PW]
乱数Nr

SmartPhone

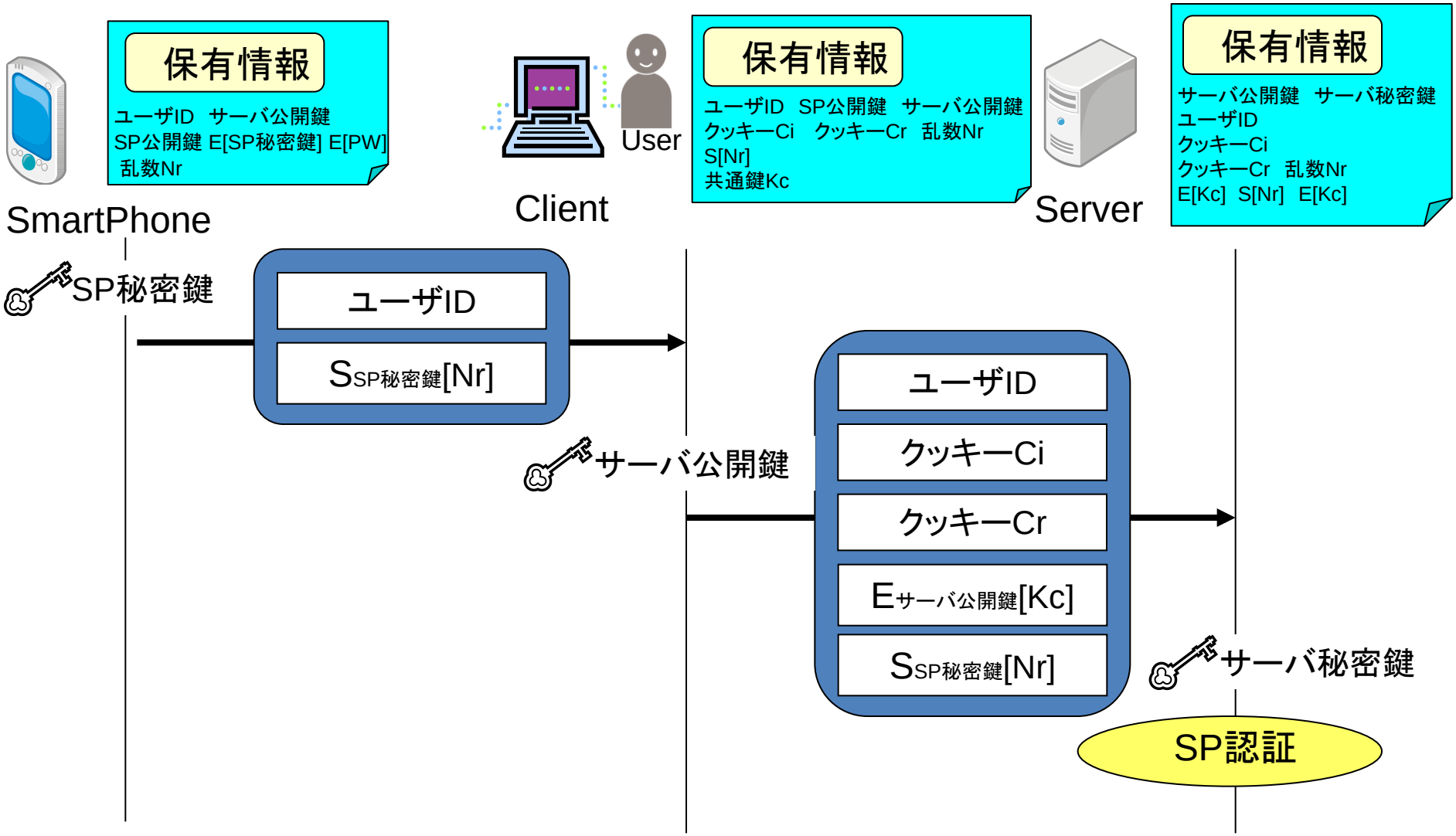
E_{PW}[SP秘密鍵] ← 受信したPW

$E_{SP公開鍵}$[PW] ← SP秘密鍵

PW ⟷ 受信したPW

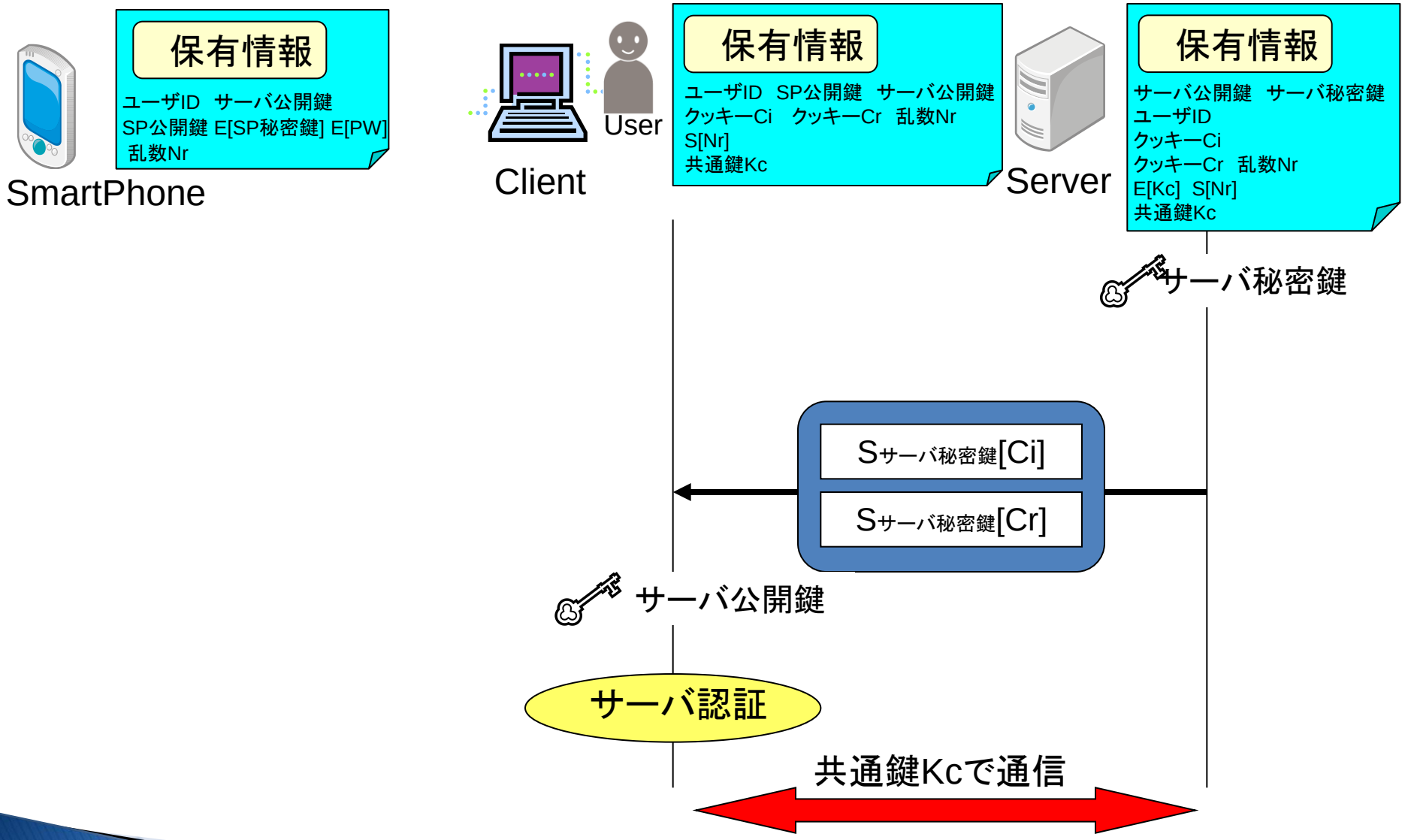
ユーザ認証

TSSAP動作(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CiをIPアドレス,時間情報,乱数をもとに生成

クッキーCi

クッキーCi

クッキーCr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

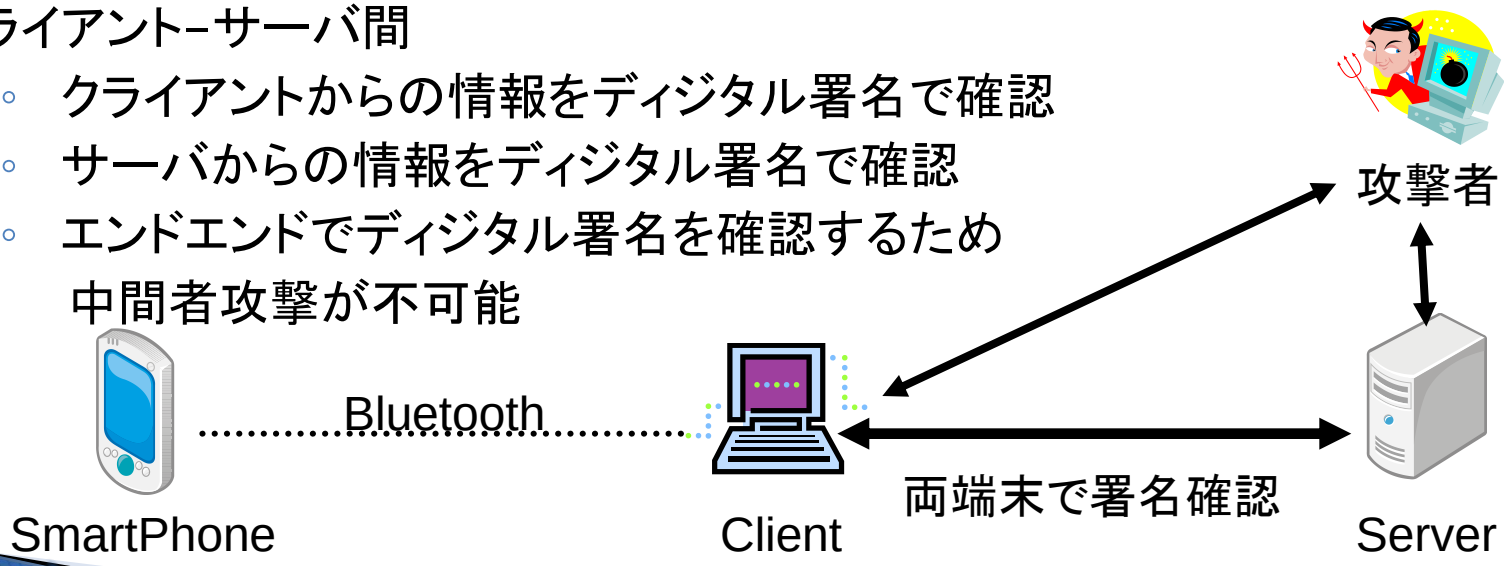
※偽装IPアドレス使用

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

IPアドレスとクッキーに関するテーブル

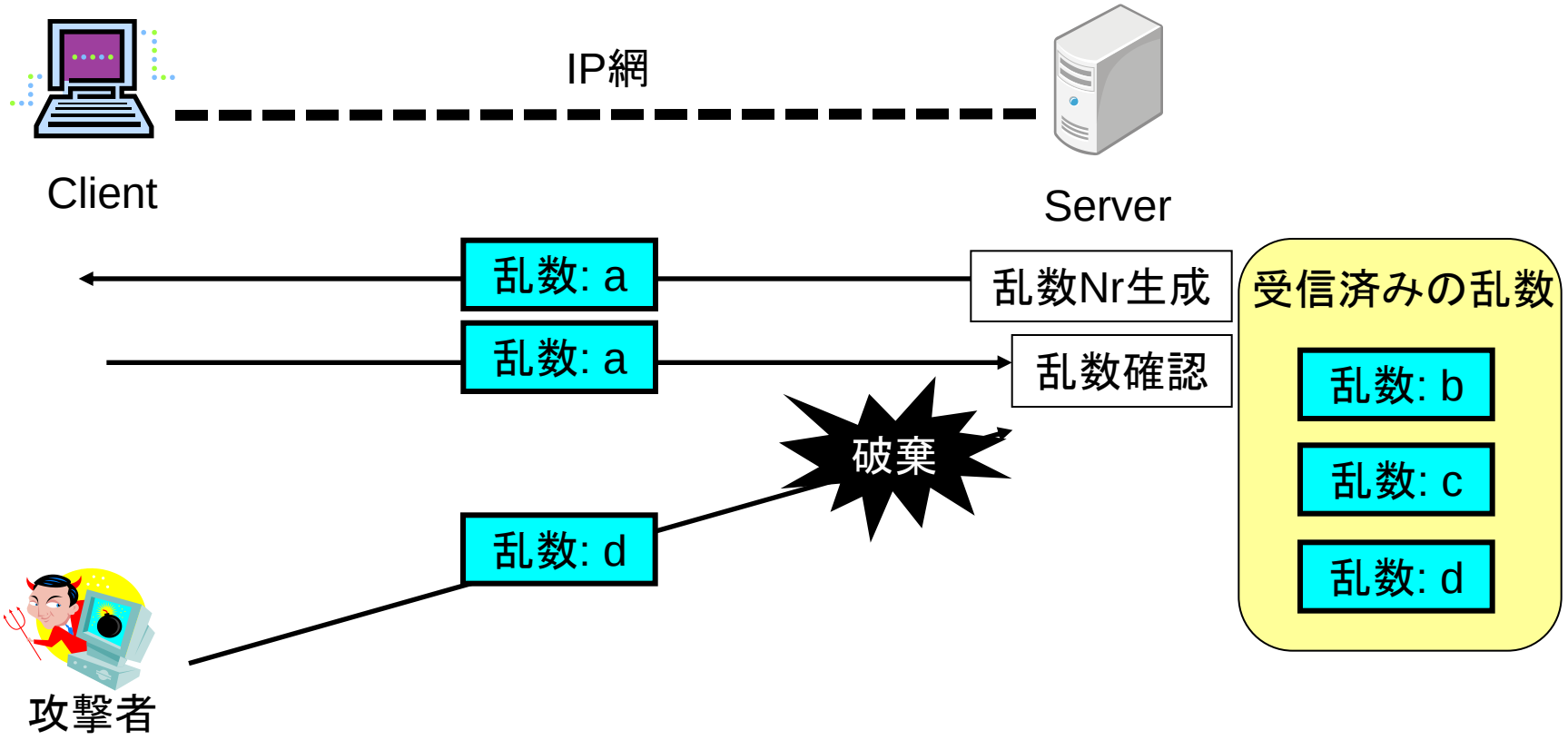
中間者攻撃による対策

- 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によって通信
  - プロファイルSPP (Serial Port Profile)
    - 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
- 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

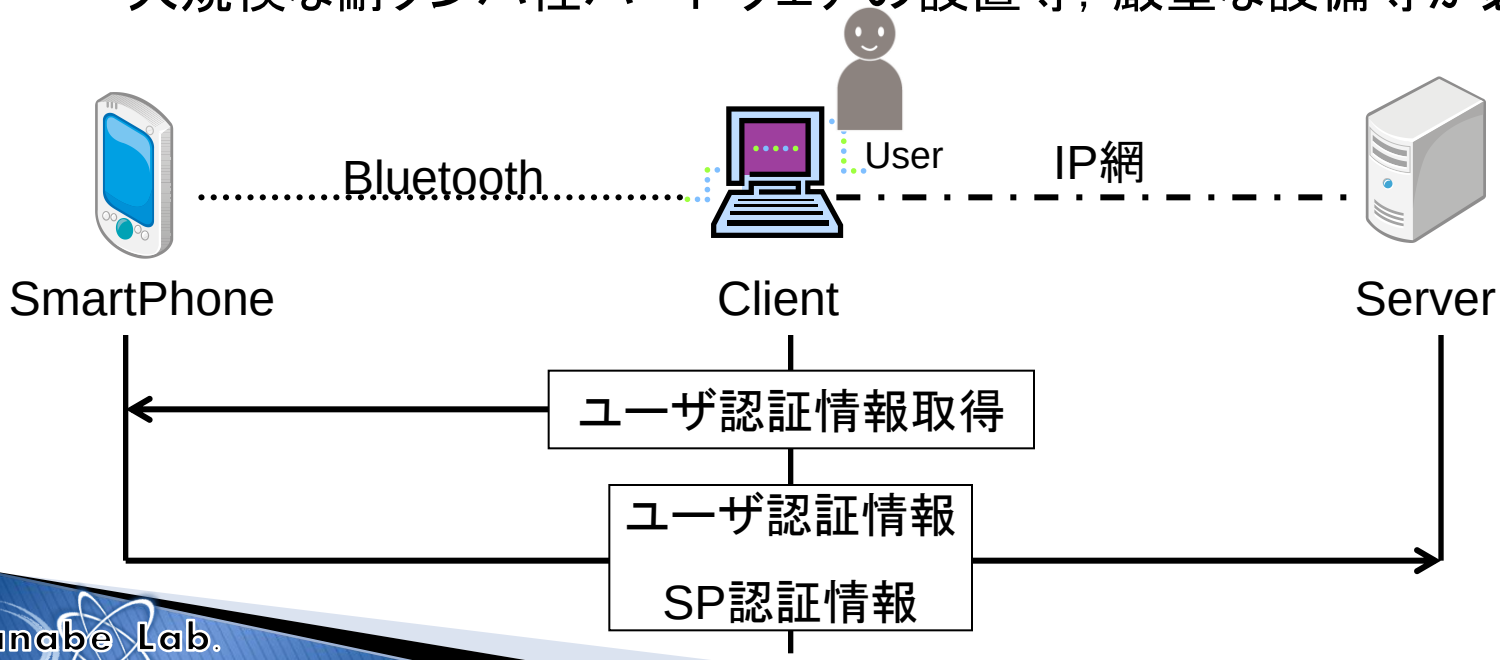
- 提案では
  - クライアントが初期情報を持たないモデルを定義
  - 重要情報を配送するための通信路の確立
  - 各種攻撃へ対応
- 今後
  - 現在実装中のTSSAPを完成させ，性能評価する

終

付録

ユーザ認証

- サーバ型認証
  - サーバ側でユーザ，SP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
    - 大規模な耐タンパ性ハードウェアの設置等，厳重な設備等が必要となる



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
- 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不可が大きくなる