平成24年度　卒 業 論 文

邦文題目

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

英文題目

Proposal of an authentication protocol MSAP available to client that do not have any scret imformation

情報工学科

(学籍番号: 080425126)

五島　秀典

提出日: 平成 24 年 2 月 10 日

名城大学理工学部

内容要旨

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. 本論文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.

Abstract

The company is an important issue to prevent information leakage.40 % of the causes of information leaks are said to be due to loss and theft of mobile devices such as notebook PC. Outside the company without taking out the information we have been focused on how to access internal systems remotely from the client PC as needed.At this time, the client should be free to choose. In such a system is required to ensure the authentication and encryption. This paper proposes a protocol MSAP(Mobility-based Secure Authentication Protocol) that the client does not possess any available information on the initial authentication information is held remarkably popular smartphones in recent years.

目 次

第1章　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, 自宅に空き巣が入り家の PC ごと盗難されたり, 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どこかに忘れ悪用されるなどの事例がある. これらの最大の原因は情報を社外に持ち出している点が共通している. また情報漏洩の原因の 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安全にアクセスする方法が注目されている. 今までこれの実現のため, 事前鍵共有方式を使った方法が考察されている [1]-[5]. この事前鍵共有方式を採用した方法は非接触 IC カード, クライアントの中に共有鍵を埋め込んでおく必要がある. この技術の欠点としてクライアントから共有鍵が漏洩する恐れがあり, 漏洩してしまうとシステム全体に及んでしまう. また, セキュリティ面でも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上, すべての端末, カードの情報を書る必要があるため大規模のシステムへ実装できない. そして共有鍵を所持しているクライアントしか使用できないため, 使用するクライアントは固定されてしまう. ユーザ視点から考えるとクライアントはホテルのパソコン, 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. この方式の欠点を解消する１つの方法として非接触型の IC カードをユーザが所持する方式がある.[6]-[7] この方式は IC カード, クライアントに共有鍵を持たせるのではなく, 暗号化処理には公開鍵方式を採用することでクライアント,IC カード両方に鍵を持たせる必要がなくなる. 従ってクライアント端末にユーザ情報を保持する必要がなくなる. それに伴い, ユーザがクライアントを選ぶことができると同時にクライアントから情報が流出することも防ぐことができる利点がある. 本論文では IC カードと同じような動作を行え, 近年発展の著しいスマートフォンに認証情報を持たせることによりユーザの利便性を向上させ, 初期情報を一切必要と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.

第2章　既存の技術

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] 図 2.1 に例を示す. この方式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間の通信を暗号化するために IC カード, クライアント PC 両方に共有鍵を埋め込んでおく必要がある. そのため, ユーザが利用する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で同じ共有鍵を使用しているため, その影響がシステム全体に及んでしまう可能性がある. このため, 安全性を確保するにはすべての IC カード, クライアントの事前共有鍵を定期的に変更することが必要とされる. このことから事前共有鍵方式を採用している既存技術は鍵の管理が煩雑になり, 大規模システムへの適用が困難になるという課題が挙げられる.

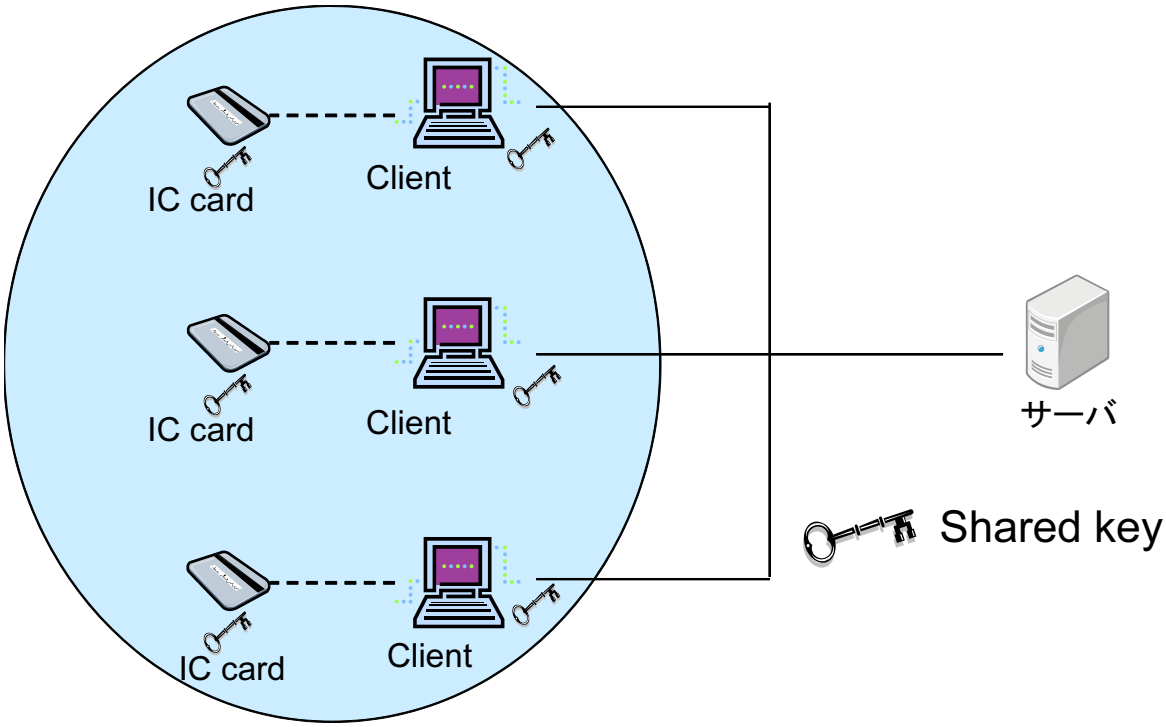

図 2.1　既存の方式

第3章　MSAPの提案

MSAP(Mobility-based Secure Authentication Protocol) はスマートフォンを利用し, 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となっている. クライアントに秘密情報を一切所持し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.

3.1　想定するシステムモデル

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. スマートフォンはBluetoothが接続でき,MSAP 対応アプリがインストールされているという条件, クライアントはBleutooth 接続ができ,MSAP 対応のソフトウェアがインストールされていることが条件となる. ユーザは秘密情報を格納したスマートフォンを所持している. スマートフォン/クライアント間の通信は Bluetooth としている. これ以外にも Wi-fi や ZigBee などの近距離通信が考えられるが Bluetooth は多くのモバイル機器に対応していることや通信距離が10m と比較的短いこのため MSAP では Bleutooth を採用している. また, 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. 次にクライアント/サーバ間は任意のネットワークで接続できる.

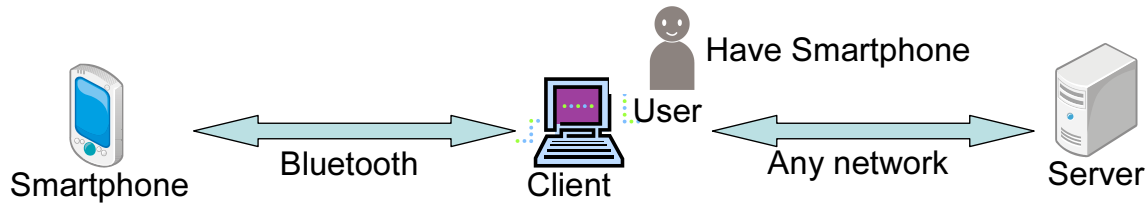

図 3.1　想定するシステムモデル

3.2　認証関係

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. 図 3.2 に認証関係を示す. 矢印を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. スマートフォンはユーザがクライアントか

らパスワードを入力し, スマートフォンで確認することでクライアントを認証する．ユーザ認証とクライアント認証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.

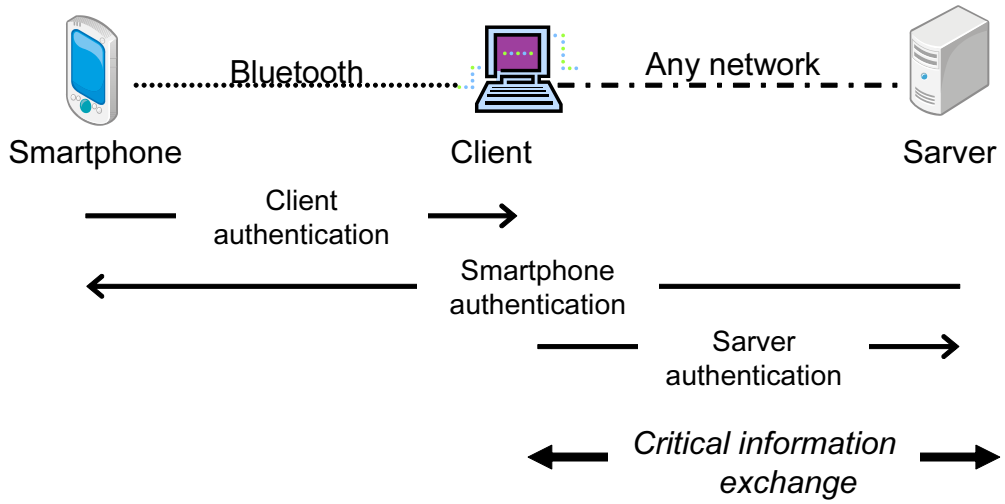

図 3.2　MSAP の認証関係

3.3　記号の定義

MSAP で使われる記号の定義を以下に示す.

uID:ユーザ ID

PuSP:スマートフォンの公開鍵

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通鍵

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]:鍵 x で y を暗号化

Sx[y]:x で y にデジタル署名

Key_REQ：鍵配送要求パケット

Key_REP：鍵配送応答パケット

Cookie_INIT：クッキー配送要求パケット

Cookie_RESP：クッキー配送応答パケット

CertUser_DIST：ユーザ認証情報配送パケット

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

SignMS_DIST：サーバ署名情報配送パケット

3.4 MSAP の初期情報

事前鍵共有方式と MSAP の初期情報を表 1 に示す. 事前鍵共有方式では各ユーザが所持しているスマートフォンにはユーザ ID の uID, スマートフォン秘密鍵 PrSP, サーバ公開鍵 PuS, パスワード PW が格納されている. クライアントには事前共有鍵方式で使うための共有鍵 Shared key が格納されている. サーバにはサーバ秘密鍵 PrS, ユーザ ID の uID とスマートフォン公開鍵 PuSP , 共有鍵 Shared Key が格納されている. 共有鍵はすべてのクライアント, スマートフォンが所持していることになる.MSAP では，IC カードには，事前共有鍵方式における共有鍵 Shared key の代わりにスマートフォン公開鍵 PuSP を格納している. クライアントは初期情報を一切所持しない．また，サーバには，サーバ秘密鍵 PrS，ユーザ ID uID と公開鍵 PuSP を所持する．従来方式と提案方式の初期情報の違いは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. また, 表 1 に示す初期情報はサーバ側で一括して作成し，IC カードの発行はあらかじめオフラインで実施しておく．スマートフォン公開鍵 PuSP はスマートフォン秘密鍵 PrSP と同時に生成するものであり，この情報をスマートフォンに格納することによって管理負荷が増えることはない.

表 3.1　事前共有鍵方式と MSAP の初期情報

	PSK Method	MSAP
Smartphone	uID PW PrSP PuS Sheard key	uID PW PrSP PuS PuSP
Client	Sheard key	-
Server	PrS PuSP uID	PrS PuSP uID

MSAP の動作概要

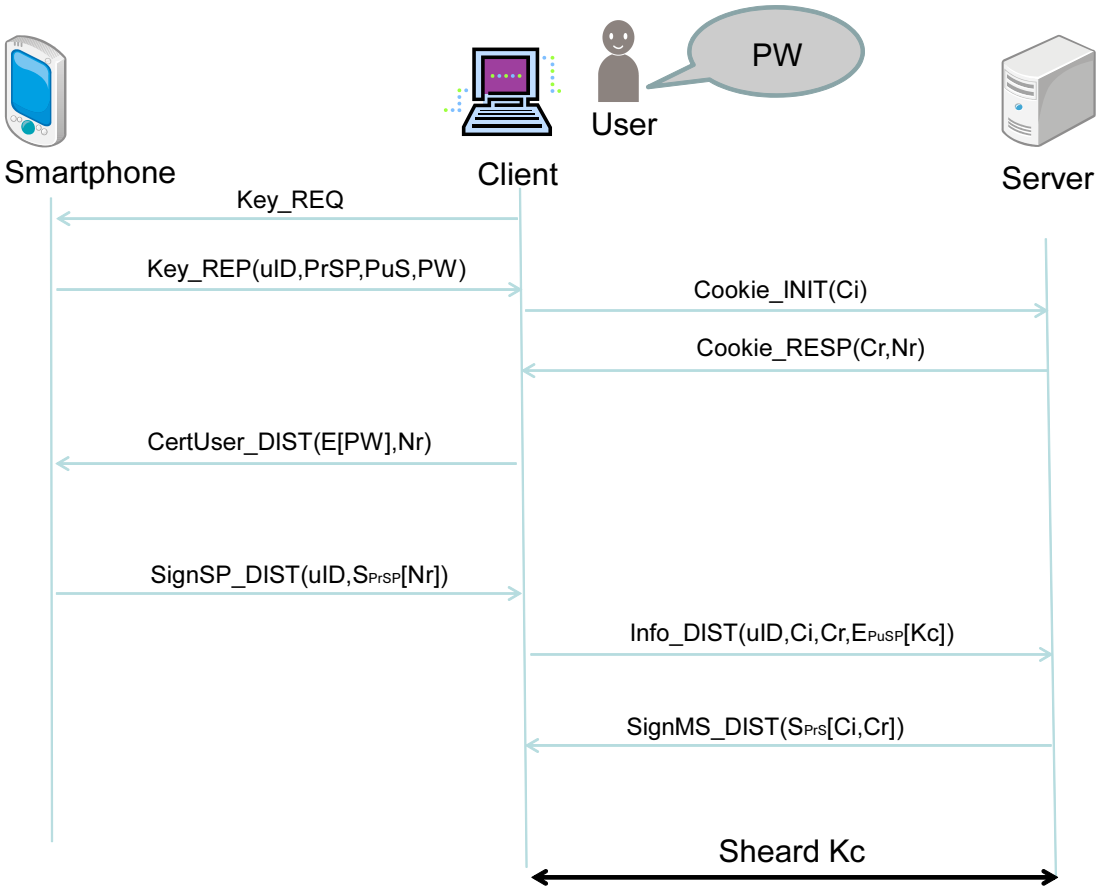

図 3.3　MSAP 動作概要

動作概要を図 3.2 に示す. スマートフォンを保持するユーザがクライアントに近づくと両者は bluetooth によるペアリングを実行する. 次にユーザがクライアント側の MSAP 用アプリケーションを起動する. クライアントからスマートフォンに配送要求が送信されることでスマートフォンから uID,PuSP,PuS をクライアントへ送信する. クライアントでは Ci を作成し, サーバへ送信する. サーバは Ci を受け取ると Cr,Nr を生成し, クライアントへ送信する. この時クライアントにログイン画面が表示されるのでユーザはパスワードをクライアント PC へ入力する. クライアントではユーザ情報をスマートフォン公開鍵で暗号化し, サーバから受け取った乱数 Nr を付加してスマートフォンへ送信する. スマートフォンではスマートフォン秘密鍵 PrSP を用いてパスワードを取り出し, 比較する. これでクライアント認証が終了する. 続いて Nr をスマートフォン公開鍵 PuSP を用いてディジタル署名を作成し, クライアントへ送信する. クライアントでは共通鍵 kc を生成し, サーバ公開鍵 PuS で暗号化し, スマートフォンから受け取った情報にこれを付加してサーバへ送信する. サーバではクッキーの正当性を検証し, ディジタル署名の検証,Nr の確認も行

う. ここでディジタル署名が正しいと判断されるとスマートフォン認証が終了する. 最後にサーバ秘密鍵 PrS でディジタル署名を作成し, クライアントへ送信する. クライアントではクッキーの検証, ディジタル署名の検証を行う. ディジタル署名が正しいと判断されるとサーバ認証が終了する.

3.5 安全性の考察

スマートフォン/クライアント/サーバ間の認証は動作概要に示す手順にて達成された. しかし, 冒頭に述べたようにこのようなシステムには確実な認証が必要である. これを守るためには各種の攻撃からも対処できることが必要である. 以下に DoS 攻撃, リプレイ攻撃, 中間者攻撃に対する安全性の考察を述べる.

3.5.1 DoS 攻撃

DoS 攻撃（SYN flood など）とは, 攻撃対象のサービス提供を妨害することが主目的である. このような攻撃がごく少数の IP アドレスから行なわれている場合, それらの IP アドレスからのアクセス制限を施すことが攻撃への有効な対策となる. しかし,IP スプーフィング (偽装) を用いて行う場合このような対策は無効となる. また, 攻撃元を詐称することで本当の攻撃元の特定が困難となり, 攻略対象システムの管理者からの追跡を逃れられる可能性が高まる. このような観点から DoS 攻撃における IP スプーフィングは有用であり, 現実にはほぼこの攻撃手法が併用されている.

対策

クライアント/サーバ間の認証処理と同時に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. ようするに, 攻撃者は IP アドレスを偽造して行っているため, 事前に作成したクッキーの対応テーブルに該当しないため防ぐことができる.

3.5.2　リプレイアタック

リプレイ攻撃とは，ユーザーがログインするときにネットワークを流れるデータを盗聴してコピーし，コピーしたデータを認証サーバーへ送ることでシステムへ不正にログインしようとする行為である. また, リプレイ攻撃への留意点としてネットワークに流す情報を暗号化するだけでは, 対策にならないことがあることに注意. 第三者がネットワークを流れるデータを盗聴しても，パスワードが暗号化されているため，パスワード自体は解読できない. しかし，暗号化されたデータそのものをコピーして認証サーバーへ送れば，ログインに成功してしまう. つまり，パスワードの暗号化だけでは，リプレイ攻撃に対しての対策にならない.

対策

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. 乱数は通信ごとに値が異なるため, 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異なるため拒否する.

3.5.3　中間者攻撃

暗号通信を盗聴したり介入したりする手法の一つ. 通信を行う二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.

対策

MSAP 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対策している. クライアントからの送られてきた情報が本当にクライアントからなのかというのをサーバがディジタル署名を確認することで行っている. 反対にサーバからも情報も本当にサーバから送られた情報かを確認するためにクライアントがディジタル署名の確認を行う. 中間者攻撃が成立していしまう原因は, データの送信元が正しいかがわからないために起こるため両端末で確かめることによって防いでいる.

第4章　実装方式

本来ならスマートフォンを使って実装するのが望ましいが, 本論文ではすべて PC 上で実装をひとまず行う.

4.0.4　モジュール構成

各端末におけるモジュール構成を図 4.1 に示す. 各端末に共通するモジュールとしてメインモジュール, 初期処理, 暗号化処理モジュールがある. メインモジュールは処理状態を管理し, 各状態に対して対応した処理を行うサブモジュールを呼び出す. まず各端末共通のモジュールから説明する. 初期処理モジュールは初期化処理を行う. 暗号化モジュールは通信パケットの暗号化, 復号化, ディジタル署名の検証, 作成などを行う. スマートフォンのモジュールは認証情報生成, ユーザ認証である. ユーザ認証モジュールはユーザの入力した PW をクライアントから受信し, 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処理を行う. クライアントでは認証情報取得, サーバ認証モジュールがある. 認証情報取得モジュールはパスワードの取得を行う. サーバ認証モジュールではサーバ署名情報を検証することにより認証を行う. 最後にサーバ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ことにより認証処理を行う. 認証情報生成モジュールではサーバ認証に必要な情報を生成する.

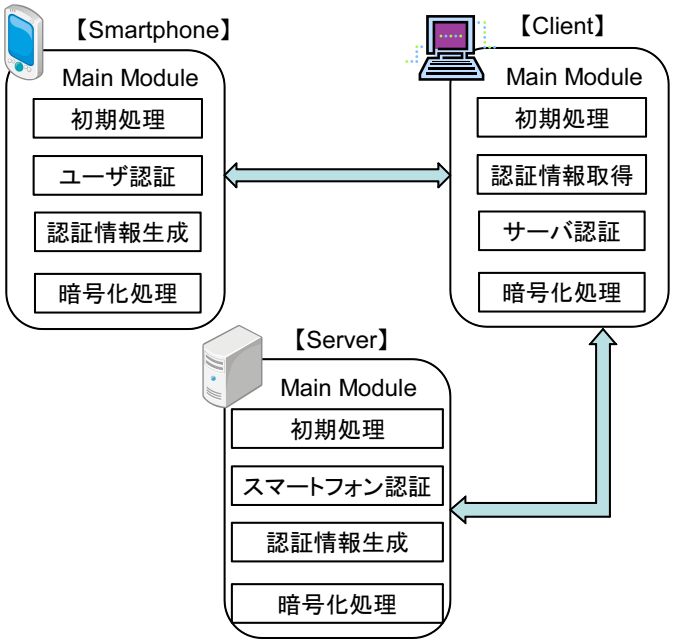

図 4.1　モジュール構成図

4.0.5　ネットワーク構成

ラップトップ PC を 2 台とデスクトップ PC を 1 台の合計 3 台の PC を用いて行う．各 PC はスイッチングハブで接続せれている．ラップトップ PC1 にはスマートフォンの処理プログラム, ラップトップ PC2 には，クライアントの処理プログラムを，デスクトップ PC3 にはサーバの処理プログラムを実行させる．

第5章　おわりに

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 MSAP を提案した. 従来の事前共有鍵方式に比べ, 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. 今後は PC 上で実装を行ったのち, スマートフォンに移植し, 実機にて性能評価を行う予定である.

謝辞

参考文献

[1] 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.(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] Richard E. Smith (著) , 稲村雄 (訳), “ 認証技術－パスワードから公開鍵まで－ ”, オーム社, 2003.

[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, Apr. 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, Vol.121-C, No.9, pp.1429-1438, Sep.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, Mar. 2002.

[6] 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.

[7] 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, Vol.2007, No.1, pp.1332-1337, Jun.2007. 43, No.3, pp.304-307, Mar. 2002.

研究業績

学術論文

なし

研究会・大会等

1. 五島 秀典，鈴木秀和，渡邊 晃秘密情報を保持しないクライアントを用いた 認証プロトコルの提案電気関係学会東海支部連合大会，Sep.2011.