非接触ＩＣカードを利用した重要情報の配送手段に関する提案

保母　雅敏† 前羽　理克‡ 渡邊　晃†

†名城大学大学院理工学研究科　〒468-8502　愛知県名古屋市天白区塩釜口 1-501

‡NEC テレネットワークス(株) NTT グループシステム本部

〒108-0023　東京都港区芝浦 4 丁目 9-25 (芝浦スクエアビル)

E-mail:　†m0432037@ccmailg.meijo-u.ac.jp, wtnbakr@ccmfs.meijo-u.ac.jp,

‡maebam@mail.ntwx.nec.co.jp

あらまし　個人認証を行うために IC カードを利用する方法が有力視されている．個人を特定する情報は IC カード内に記録されているため，利用者は自由にクライアント端末を選んで利用できるという利点がある．このためクライアントは初期情報を持たないことが望ましいが，実際にクライアントを利用して暗号通信を行うためには，クライアント自身に暗号鍵などの重要情報が配送される必要がある．本論文では，非接触ＩＣカードを用いてクライアントに重要情報を配送する手段と，クライアントとサーバの間に第三の装置が介在する場合においてもパケットの確実な認証を行える方式を提案する．

Proposal of Important Data Distribution Method Using non-Contact IC Card

Masatoshi HOBO† Masakatsu MAEBA‡ Akira Watanabe†

†Graduate School of Science and Technology, Meijo University

1-501 Shiogamaguchi, Tenpaku-ku, Nagoya-shi, Aichi, 468-8502, Japan

‡NEC Telenetworx, Ltd. NTT Group System Center

Shibaura Square Building 4-9-25 Shibaura, Minato-ku, Tokyo, 108-0023, Japan

E-mail:　†m0432037@ccmailg.meijo-u.ac.jp, wtnbakr@ccmfs.meijo-u.ac.jp,

‡maebam@mail.ntwx.nec.co.jp

Abstract　IC Card authentication has become promising technology these days. Since all of user specific information is in IC Card, user can use any clients in the system, however, authentication between a server and clients is not clearly defied when non-contact IC card is used.　In this paper, we propose an authentication method among non-contact IC card, clients, and the server. We also propose a packet authentication method in mid-way devices on the way of communication.

1. はじめに

個人認証を行う手段として，パスワードや生体認証など様々なものが存在するが，その中で IC カードを利用した認証が有力な手段の一つとして注目されている[1]-[9]．IC カードは内部に CPU を有しており，カード内で暗号・認証といった処理を行うことが可能である．また，外部からの不正アクセスを防止する耐タンパ性を有しているため，高いセキュリティと携帯性を実現している．さらに，非接触 IC カードの登場により，IC カードをカードリーダに挿入する必要がなくなり，より手軽に利用できるようになった[10]．

IC カード内には個人を特定するための秘密情報が全て記録されているため，クライアント端末に初期情報を持つ必要がない．このため，ユーザは自由に端末を選んで利用することが可能である．しかし，暗号通信に使用する暗号鍵といった重要情報が必要なのは IC カードではなくクライアントであるため，クライアントとサーバ間で安全な配送手段を実現する必要がある．接触型 IC カードを用いる場合では, IC カードとクライアントを

一体のものとみなすことができるため，安全な配送手段の実現は比較的容易であった．しかし，非接触 IC カードでは IC カード/クライアント間が無線通信となるため，両者間の通信が盗聴されるという課題がある．

非接触 IC カードとして暗号化を考慮したものがあるが，利用するシステムであらかじめ共通鍵を共有しておくことが前提となっており，共通鍵が流出するとシステム全体に影響が及ぶ可能性がある．

これらの課題を解決するため, 本稿ではＩＣカードの初期情報を工夫することにより，IC カード/クライアント，IC カード/サーバ，クライアント/サーバの各間で暗号通信を行うことを可能とし, 暗号鍵などの重要情報をサーバからクライアントに安全に配送する方式を提案する．同時に, 従来検討が不十分であった, 通信経路上に第三の装置が介在する場合においてもパケットの確実な認証を行うことを可能にする．

以降，2 章で従来方式とその課題，3 章で提案方式， 4 章で実装，5 章でその評価を行い，6 章でまとめを述べる．

2. 従来方式と課題

本章では非接触 IC カードを用いたシステムのモデルを示し，従来の接触型 IC カードを用いた方法を適用した場合の処理シーケンスとその課題について述べる．

2.1 想定するシステムモデル

本研究で想定するシステムモデルを図 1 に示す. 本システムはサーバからクライアントへ暗号鍵などの重要情報を配送することを目的とする．各クライアントには非接触 IC カードリーダが搭載されている. 生体情報読み取り装置を組み合わせることによって, より高いセキュリティを実現することが可能となる．非接触 IC カード内には生体情報テンプレートや公開鍵暗号方式の秘密鍵といった個人を特定する情報が納められている. 生体情報をサーバ側に格納してユーザ認証に利用する方法も考えられるが，IC カードとサーバ間の認証は初期情報として保持する公開鍵を用いて確実に実現できるため，本システムでは IC カード内に格納することによって，ユーザが IC カードの持ち主であるかどうかのチェックに利用する．カード内で照合を行うため，テンプレートデータの漏洩や照合結果の改竄を防ぐことが出来る．これにより，システムを適用したクライアントであれば, どこからでもシステムを利用することが可能である[11].

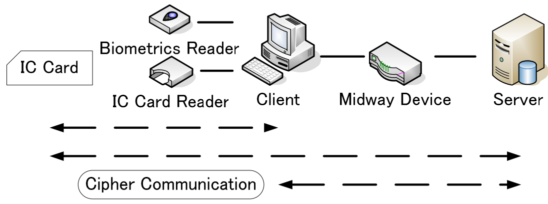


図 1　想定するシステムモデル
Fig.1 Assumed System Model

また, クライアントと重要情報を管理するサーバの通信経路上には第三の装置となる中間装置が介在する場合があるため, システムモデルに含めて考える. ここでいう中間装置とは配下のネットワークを保護する役割を持つ装置であり, 不要なパケットの侵入を遮断する役割を持つ[12]-[16].

2.2 配送シーケンスとその課題

接触型 IC カードを用いた認証シーケンスをシステムモデルに適用した場合の例を図 2 に示す．各端末は表 1 に示される初期情報を所持している．各ユーザは IC カード内に固有のユーザ ID，ユーザ秘密鍵，サーバ公開鍵，生体情報テンプレートを所持しており，中間装置では装置 ID，装置秘密鍵，サーバ公開鍵を装置内に所持している．そしてサーバではサーバ秘密鍵，各ユーザ/装置の ID と公開鍵を所持する．これらの情報はサーバ側で作成し，ユーザの IC カードの発行および中間装置への埋め込みをあらかじめオフラインで実施しておく必要がある．

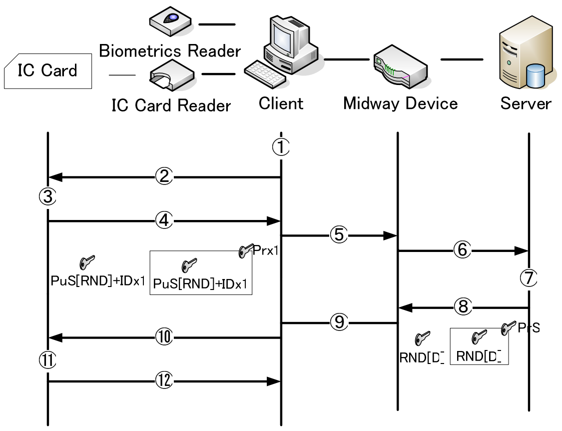


図 2　従来の配送シーケンス
Fig.2 Conventional Distribution Method

表１　初期情報
Table.1 Initial Information

IC カード	IDx1：ユーザ ID Prx1：ユーザ秘密鍵 PuS：サーバ公開鍵 T：生体情報テンプレート
クライアント	なし
中間装置	IDx2：装置 ID Prx2：装置秘密鍵 PuS：サーバ公開鍵
サーバ	PrS：サーバ秘密鍵 IDx1，IDx2：ユーザ/装置 ID Pux1,Pux2：ユーザ/装置公開鍵

以下のシーケンスの説明は図中の番号に対応する．

① 生体情報読み取り装置によって，特徴点 S を取得する．
② 取得した特徴点 S を IC カードに渡す．
③ IC カードはあらかじめ保持している生体情報テンプレート T を用い，特徴点の比較・照合を行う．
④ 照合結果が正しければ，乱数 RND を生成し，サーバ公開鍵 PuS で暗号化し，ユーザ ID を追加する．このデータにディジタル署名を付加しクライアントに渡す．
⑤ クライアントは IC カードが生成した情報をそのままサーバへ送信する．
⑥ 中間装置はこのパケットを透過的に中継する．
⑦ パケットを受信したサーバは，ユーザ ID からサーバに格納されたユーザ公開鍵 Pux1 を読み出しディジタル署名の検証を行う．その後サーバ秘密鍵 PrS を用いて乱数 RND を取得する．
⑧ 認証が成功した場合は，当該クライアントに対応する重要情報 D を乱数 RND で暗号化する．そして，このデータのディジタル署名を付加しクライアントへ送信する．
⑨ 中間装置はこのパケットを透過的に中継する．
⑩ クライアントは受信したデータをそのまま IC カードに渡す．
⑪ パケットを受けとった IC カードは，サーバ公開鍵 PuS を用いてディジタル署名の検証を行う．その後．乱数 RND を用いて復号し重要情報 D を取得する．
⑫ 重要情報 D をクライアントに渡す．

以後の通信は配送された重要情報 D に含まれる暗号鍵を用いて暗号通信などを行うことが可能となる．

接触型 IC カードを用いた場合は IC カードが物理的にクライアントと接続されているため，IC カード/クライアント間の情報交換が外部に漏れることはない．しかし，ここに非接触 IC カードを適用した場合，両者間の情報交換を無線通信で行う必要があるため，漏洩の危険性がある．また，従来の配送シーケンスでは中間装置において配送パケットを透過的に中継しており，配送を装った偽造パケットの通過を許してしまうという課題がある．

3. 提案方式

本章では非接触 IC カードを用いて安全に重要情報を配送する手段を述べる．提案方式では，IC カード/クライアント，IC カード/サーバ，クライアント/サーバの各間での確実な認証と暗号化，さらに中間装置におけるパケット認証を可能とする仕組みを実現する．

3.1 初期情報の追加

提案方式において，各端末が所持すべき初期情報を表 2 に示す．従来方式の初期情報に加え，IC

表２　提案方式の初期情報
Table.2 Initial Information of Proposal Method

IC カード	IDx1：ユーザ ID Prx1：ユーザ秘密鍵 PuS：サーバ公開鍵 T：生体情報テンプレート **※Pux1：ユーザ公開鍵** **※ACx1：認証情報**
クライアント	なし
中間装置	IDx2：装置 ID Prx2：装置秘密鍵 PuS：サーバ公開鍵 **※Pux2：ユーザ公開鍵** **※ACx2：認証情報**
サーバ	PrS：サーバ秘密鍵 IDx1，IDx2：ユーザ/装置 ID Pux1,Pux2：ユーザ/装置公開鍵

※　新たに追加した情報

カードと中間装置はユーザ公開鍵，認証情報をそれぞれ初期情報として所持する．認証情報とは，ユーザの公開鍵をサーバの秘密鍵で暗号化したものであり，サーバが認証した正規のユーザであることを証明するために利用する．これらの情報はICカードや中間装置の初期情報作成時に容易に追加することができ，全体の運用に大きな影響を与えることはない．

3.2　提案方式の配送シーケンス

提案方式の配送シーケンスを図 3 に示す．以下のシーケンス説明は図中の番号に対応する．

① クライアントからの情報送信に先立ち，IC カードからクライアントにユーザ公開鍵 Pux1 とサーバ公開鍵 PuS を送信する．

② クライアントは生体情報の特徴点 S を取得する．

③ クライアントは乱数 RND を生成しユーザ公開鍵 Pux1 暗号化する．同時に特徴点 S を乱数 RND で暗号化し IC カードへ送信する．

④ IC カードはユーザ秘密鍵 Prx1 を用いて乱数 RND を取得し，取り出した乱数 RND を用いて特徴点 S を取得する．IC カード内の生体情報テンプレート T を用いてユーザ認証を行う．

⑤ 乱数 RND をサーバ公開鍵 PuS で暗号化し，ユーザ ID を追加する．このデータとそのディジタル署名の組を Q とし，認証情報 ACx1 を付加しクライアントに送信する．

⑥ クライアントでは Q のハッシュを取り，乱数 RND で暗号化したものをパケットに追加する．

⑦ 宛先をサーバとして送信する．

⑧ 通信経路上に存在する中間装置では，サーバ公開鍵 PuS を用いて認証情報 ACx1 からユーザ公開鍵 Pux1 を取り出し，ディジタル署名の検証を行う．

⑨ ディジタル署名の検証によりパケットの整合性が確認された場合，データを中継する．

⑩ パケットを受信したサーバは，ユーザ ID からサーバに保存されたユーザ公開鍵 Pux1 を読み出しディジタル署名の検証を行う．その後 Q のハッシュを取り，サーバ秘密鍵 PrS を用いて乱数 RND を取得する．クライアントで追加された情報を乱数 RND で復号し，サーバ側でとったハッシュと比較を行う．

⑪ 認証が成功した場合は，重要情報 D を乱数 RND で暗号化する．そして，このデータのディジタル署名を付加しクライアントへ送信する．

⑫ 通信経路上に存在する中間装置では，サーバ公開鍵 PuS を用いてディジタル署名の検証を行う．

⑬ ディジタル署名の検証によりパケットの整合性が確認された場合，データを中継する．

⑭ パケットを受信したクライアントは，サーバ公開鍵 PuS を用いてディジタル署名の検証を行い，その後乱数 RND を用いて復号し重要情報 D を取得する．

以後の通信は配送された重要情報 D に含まれる暗号鍵を用いて暗号通信などを行うことが可能となる．

新たに IC カードの初期情報として保持させたユーザ公開鍵を事前にクライアントに送付することで，IC カード/クライアント間での暗号通信が可能となる．クライアントが発生した乱数を IC カード経由でサーバに渡すことにより，サーバとクライアントが乱数を共有でき，相互認証と暗号化が可能となる．データが暗号化されているため，中間装置ではパケットの情報を読み取ることはできないが，データが改竄されていないこと，データは検証に使用した公開鍵と対になる秘密鍵によって署名されたことが確認できる．さらに認証情報から取り出したものをディジタル署名の検証に利用することで，検証するパケットはサーバが認証した正規のユーザが作成したものであることを確認することが可能である．

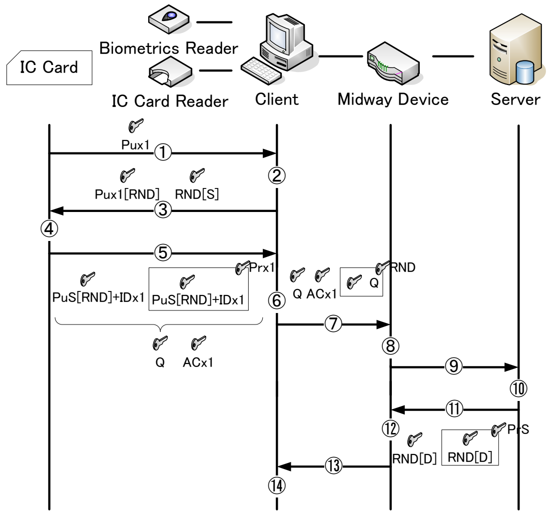


図 3　提案方式の配送シーケンス

Fig.3 Proposed Distribution Method

4. 実装

図 4 にサーバおよびクライアントにおける試作の実装概要図を示す. IC カードはクライアント内の仮想プログラムとして動作させた. 表 3 にモジュールの機能を示す. 暗号化および認証動作には, OpenSSL ライブラリを利用した[17].

クライアントおよびサーバではアプリケーション層でのプログラムとして実装するが, 中間装置では中継判定の機能を高速に実現するために, カーネルの改造が必要となる. そこで開発環境を揃えるため, IP 層に関する情報や処理内容の資料が多い FreeBSD での実装を進めている.

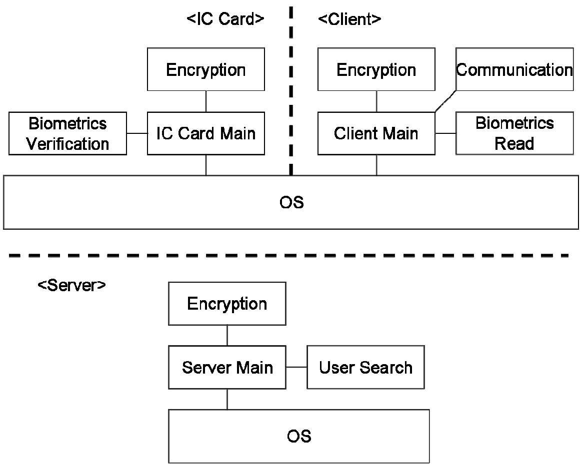


図 4 実装概要図
Fig.4 Outline Figure of Implementation

表 3 試作システムのモジュールと主な機能
Table.3 Function of the trial system

モジュール	機能
IC Card Main Client Main Server Main	状態を管理し，一連の処理を組み立てる．必要に応じてサブモジュールを呼び出す.
Encryption	OpenSSL を利用して暗号/復号，ディジタル署名の生成/検証，ハッシュ生成の処理を行う.
Biometrics Read	生体情報の読み取りを行う.
Biometrics Verification	生体認証のマッチング処理を行う.
User Search	ユーザ ID からユーザ公開鍵を取得する.

表 4 従来方式との比較
Table.4 Compression with Conventional Method

比較項目	従来	提案方式
IC カード/クライアント間の暗号化	不可	可
IC カードの処理負荷	高い	低い
中間装置での認証	不可	可
中間装置への負荷	低い	高い

5. 評価

従来の配送シーケンスと提案方式の配送シーケンスの比較を表 4 に示す. 提案方式では非接触 IC カードを利用してサーバによる認証を行う際に利用する全ての通信路の暗号化・認証を実現している．このため認証までの処理動作が従来に比べ多いが，サーバからのパケットをクライアントで直接処理できるため, IC カードの処理が軽減できる.

また，従来は検討が不十分であった中間装置が存在する場合においても，ディジタル署名を検証することによって中継の判定を行うことが可能である.

提案方式では，全ての端末においてディジタル署名の検証を行うため，サーバ・中間装置にかかる負荷が懸念される．パケットはサーバへ送信されるため，サーバに近づくに従って負荷が高くなると予想されるが，重要情報の配送は基本的にクライアントの立ち上げ時のみであるため，実際の通信に大きな影響を与えるものではないと考えられる．ただし，現状のままでは正常なパケットを大量に送信するような DoS 攻撃に対する脆弱性が存在する．今後，前処理によって事前にパケットを破棄できるような仕組みの検討が必要である.

6. まとめ

本稿では，非接触ＩＣカードを用いてサーバからクライアントに重要情報を配送する手段についての提案を行った．非接触 IC カードを用いて IC カード/クライアント，IC カード/サーバ，クライアント/サーバの各間で暗号通信を行うことにより，クライアントが初期情報を持たなくとも安全に重要情報を配送することを可能にした．公開鍵暗号方式を利用しているので継続的な通信には向かないが，初期の重要情報の配送において十分に利用できることを示した.

今後の課題としては，DoS 攻撃への対策を検討していく予定である.

文　献

[1] 瀬戸，“ユビキタス時代のバイオメトリクスセキュリティ”，日本工業出版

[2] Richard E. Smith (著)，稲村(訳)，“認証技術ーパスワードから公開鍵までー”，オーム社

[3] 坂倉，長嶋，辻井，“DNA バイオメトリックス本人認証システム”，情報処理学会コンピュータセキュリティ研究報告　Vol.2002, No.12 2002-CSEC-16(17)

[4] 妹尾，厚井，貞包，中谷，馬場，鹿間，“生体認証によるネットワーク個人認証システム”情報処理学会論文誌　Vol.44　No.4 Apr.2003

[5] 影井，“IC カードの動向”，情報処理学会会誌 Vol.39 No.5　May. 1998

[6] 吉田，平田，“IC カードの現状と課題”，情報処理学会会誌 Vol.43 No.3　Mar. 2002

[7] 飯野，岩瀬，坂野，中嶋，“指紋照合機能搭載 IC カードによる本人認証方式”，情報処理学会コンピュータセキュリティ研究報告 Vol.2000 No.68 2000-CSEC-10(22)

[8] 石田，三村，瀬戸，“IC カード実装型指紋照合装置の開発”，コンピュータセキュリティ研究報告 Vol.2000 No.68 2000-CSEC-10(21)

[9] 磯部，三村，瀬戸，菊池，“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, No.24 99-CSEC-4(10)

[10] 伊藤，“非接触 IC 技術とその応用”，情報処理学会会誌 Vol.43 No.3　Mar. 2002

[11] 前羽，渡邊，“生体認証を利用したセキュアネットワーク通信”，情報処理学会第 66 回全国大会 講演論文集 3-503, Mar. 2004

[12] 渡邊，厚井，井手口，横山，妹尾，“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　Apr. 1997

[13] 鈴木，渡邊，“フレキシブルプライベートネットワークにおける動的処理解決プロトコル DPRP の仕組み”，情報処理学会コンピュータセキュリティ研究報告 Vol.2004，No.75 2004-CSEC-26(39)

[14] 増田，渡邊，“実用性を重視した暗号通信方式の提案”，情報処理学会コンピュータセキュリティ研究報告　Vol.2004，No.75 2004-CSEC-26(40)

[15] 竹尾，渡邊，“FPN における渡り歩きの検出方法の検討”，情報処理学会コンピュータセキュリティ研究報告　Vol.2004，No.75 2004-CSEC-26(41)

[16] 保母，渡邊，“多段構成ネットワークにおける鍵配送方式の一検討”，情報処理学会第 66 回全国大会 講演論文集 3-495, Mar. 2004

[17] OpenSSL, http://www.infoscience.co.jp/technical/openssl/

[18] 森川，青山，南，“ユビキタスネットワーキングへの道”，情報処理学会学会誌 Vol.43 No06 2002

[19] D. Harkins，D. Carrel，”The Internet Key Exchange (IKE)”，RFC2409 Nov. 1998

[20] W. Polk，R. Housley，L. Bassham, ”Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”，RFC3279 Apr. 2002

[21] S. Boeyen，T. Howes，P. Richard，”Internet X.509 Public Key Infrastructure Operational Protocols -LDAPv2”，RFC2559，April. 1999

[22] S. Boeyen，T. Howes，P. Richard，”Internet X.509 Public Key Infrastructure LDAPv2 Schema”，RFC2587，June. 1999

[23] R. Housley，P. Hoffman, ”Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP”，RFC2585，May. 1999

[24] D. Eastlake，O. Gudmundsson，”Storing Certificates in the Domain Name System (DNS)” RFC2538，March. 1999

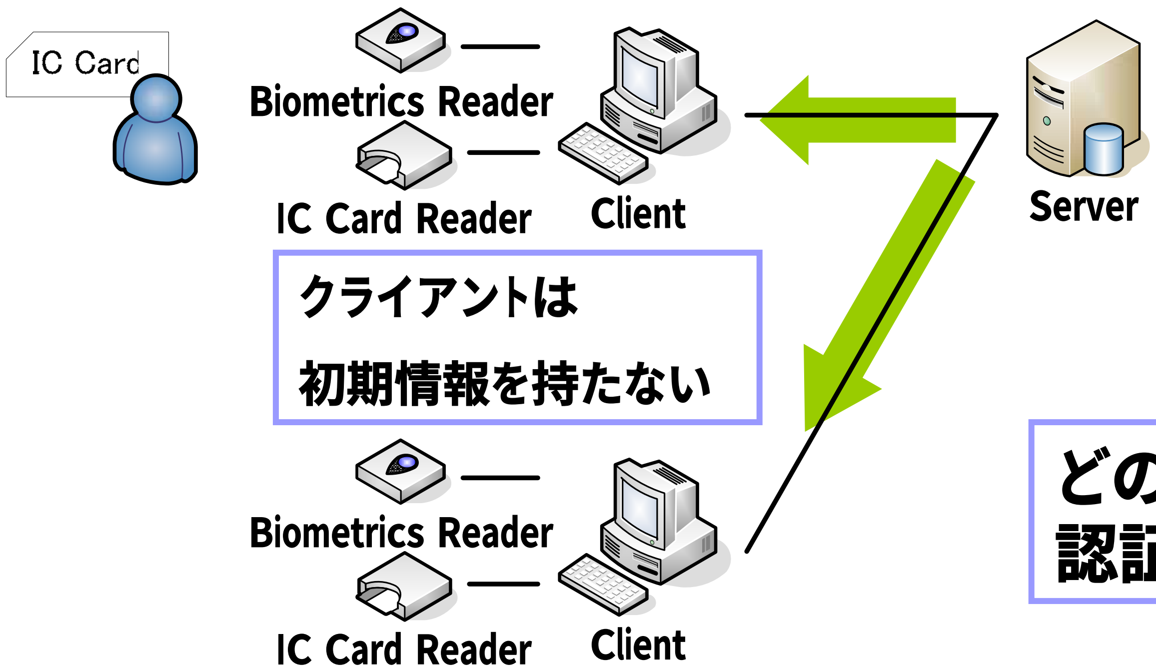
非接触ICカードを利用した重要情報の配送手段に関する提案

名城大学大学院　理工学研究科
保母雅敏　渡邊晃
NECテレネットワークス(株)
前羽理克

はじめに

- 「個人認証」要求の高まり
  - パスワード, 生体認証, ICカードなど
- ICカード
  - カード内で暗号･認証処理が可能
  - 外部からの不正読み取りを防ぐ耐タンパ性
  - 高い携帯性
- 非接触ICカードの登場による利便性の向上

ICカードを利用したユーザ認証

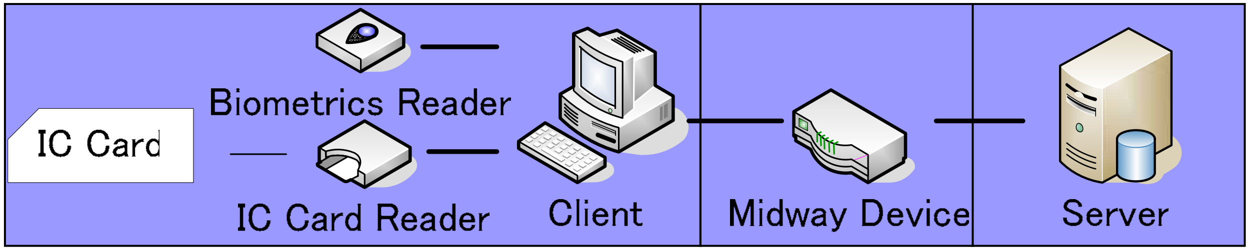


どの端末からでも
認証可能

- ICカードに個人を特定する情報を格納
  - パスワード, 生体情報, ユーザ情報など

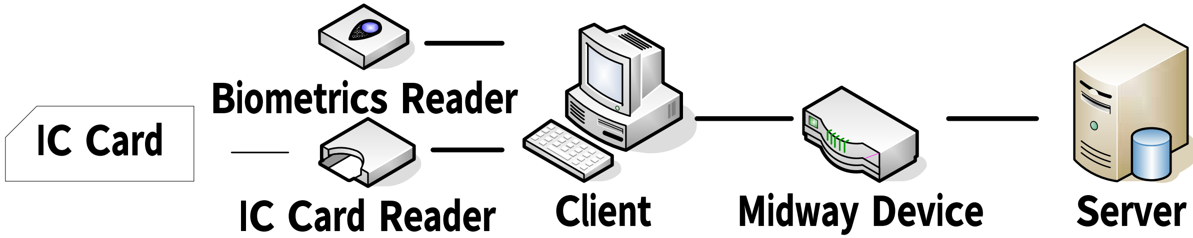
    カードの持ち主を確認するために利用
- ユーザ認証時に重要情報の配送
  - 暗号通信に利用する暗号鍵などの情報

想定システム



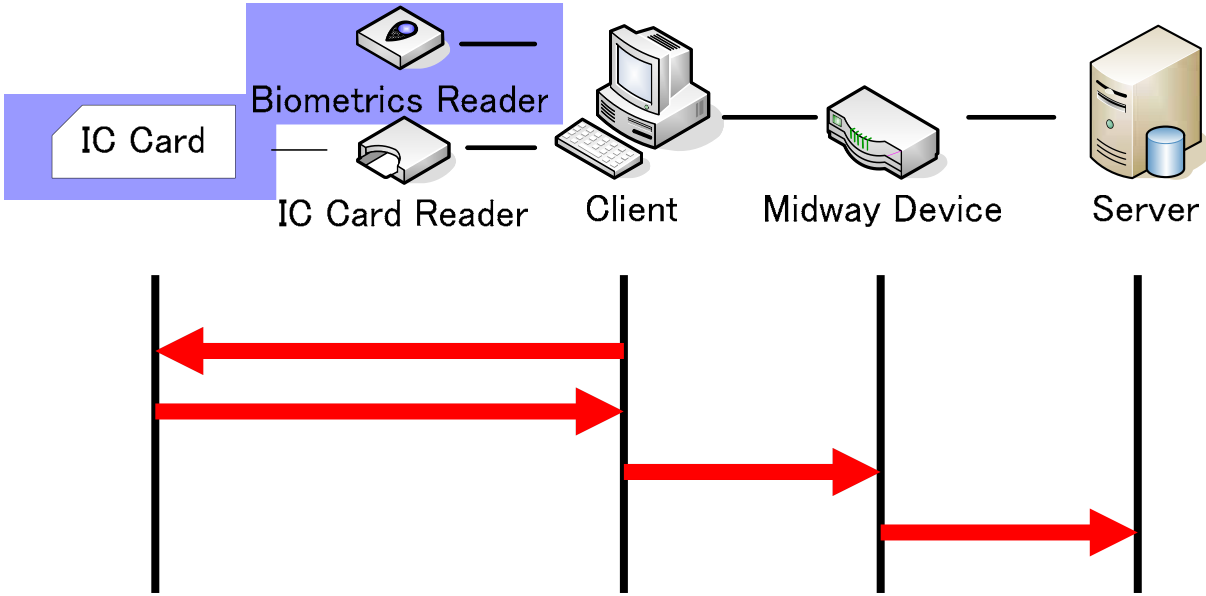
- 従来方式では接触型ICカードが前提
  - クライアントとICカードは一体のものとみなす
- サーバ
  - 重要情報の管理，配送
- 中間装置
  - 配下の端末を保護
  - 従来方式では想定されていない
    - 配送パケットは透過的に中継

従来方式の初期情報



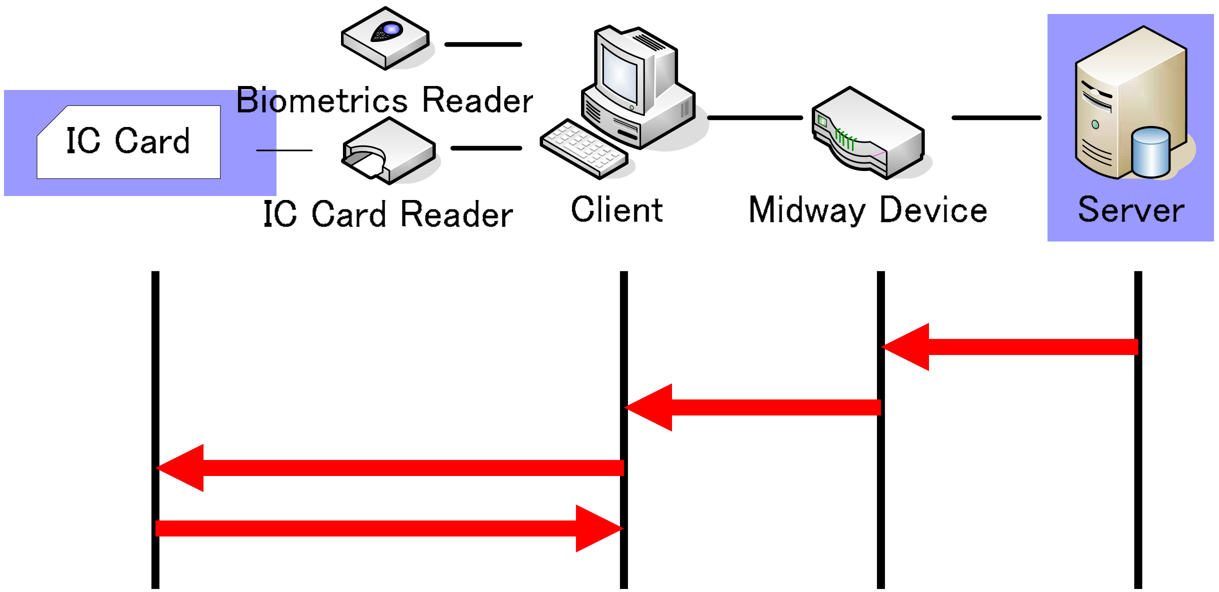
ICカード	IDx1：ユーザID Prx1：ユーザ秘密鍵 PuS：サーバ公開鍵 T：生体情報テンプレート
クライアント	なし
中間装置	IDx2：装置ID Prx2：装置秘密鍵 PuS：サーバ公開鍵
サーバ	IDx：ユーザ/装置ID Pux：ユーザ/装置公開鍵 PrS：サーバ秘密鍵

従来の配送シーケンス



①生体情報の特徴点Sを取得
②特徴点SをICカードへ送信
③特徴点Sを比較･照合
④乱数RNDを生成しサーバ公開鍵PuSで暗号化しユーザIDを追加
　ディジタル署名を付加しクライアントへ送信
⑤データをサーバ宛に送信
⑥中間装置はパケットを透過的に中継

従来の配送シーケンス

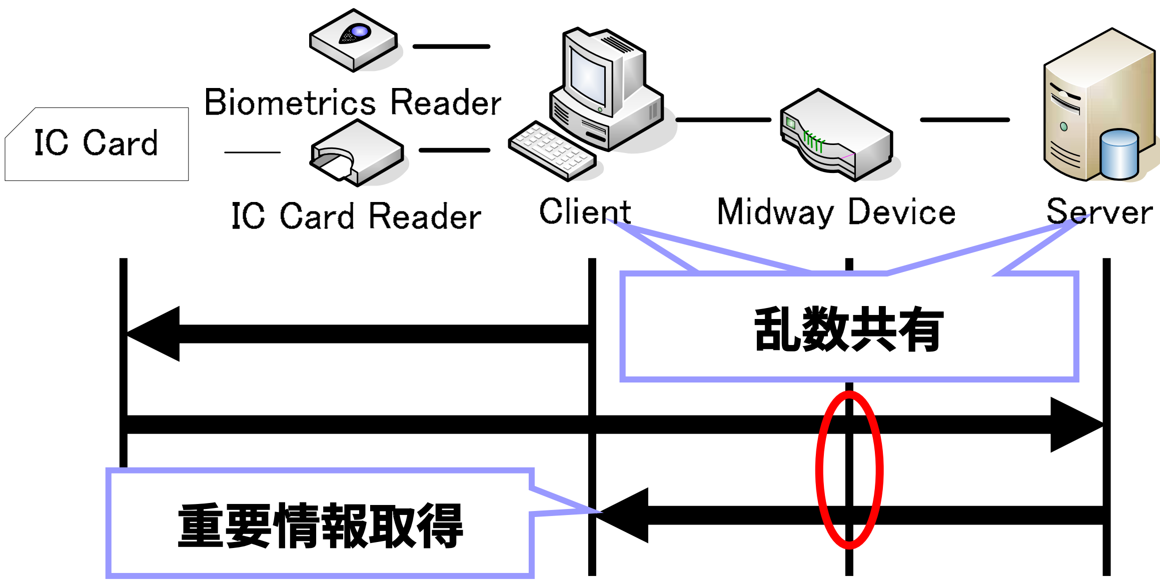


⑦サーバはユーザ認証を行い，乱数RNDを取得
⑧重要情報Dを乱数RNDで暗号化し，ディジタル署名を付加
　クライアントへ送信
⑨中間装置はパケットを透過的に中継
⑩受信したデータをICカードへ送信
⑪ICカードはサーバ認証を行い，重要情報Dを取得
⑫重要情報Dをクライアントに送信

従来方式の課題

- ICカード/クライアント間の通信
  - 接触型ICカードが前提
  - 非接触ICカードの場合
    - 重要情報がそのまま流れてしまう
- 中間装置での透過的な中継
  - 従来方式では想定されていない
  - 配送を装った偽造パケットの通過

提案方式の概要



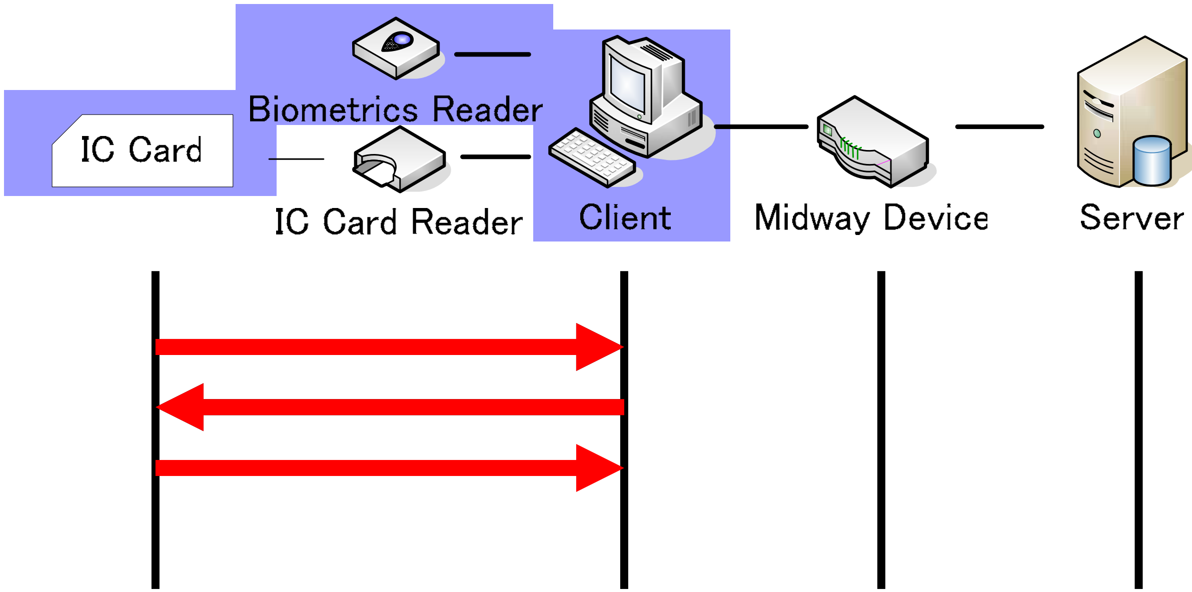
- クライアントで乱数を発生
  - ICカードを経由してサーバと乱数を共有
- 中間装置での中継判定
  - ディジタル署名の検証

提案方式

- ICカード/装置に情報を追加
  - Pux1/Pux2：ユーザ/装置公開鍵
    - ICカード/クライアント間の暗号通信に利用
  - ACx1/ACx2：認証情報
    - Pux1/Pux2をサーバが認証した情報
    - 中間装置での中継判定に利用

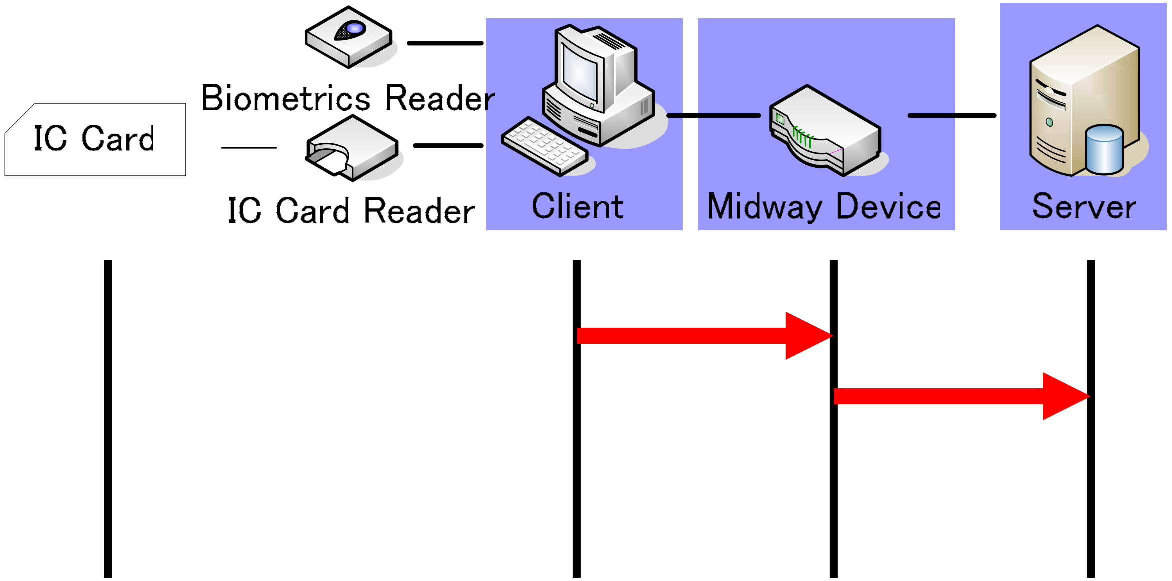
ICカード	IDx1：ユーザID Prx1：ユーザ秘密鍵 PuS：サーバ公開鍵 T：生体情報テンプレート Pux1：ユーザ公開鍵 ACx1：ユーザ認証情報
クライアント	なし
中間装置	IDx2：装置ID Prx2：装置秘密鍵 PuS：サーバ公開鍵 Pux2：装置公開鍵 ACx2：装置認証情報
サーバ	IDx：ユーザ/装置ID Pux：ユーザ/装置公開鍵 PrS：サーバ秘密鍵

提案方式の配送シーケンス



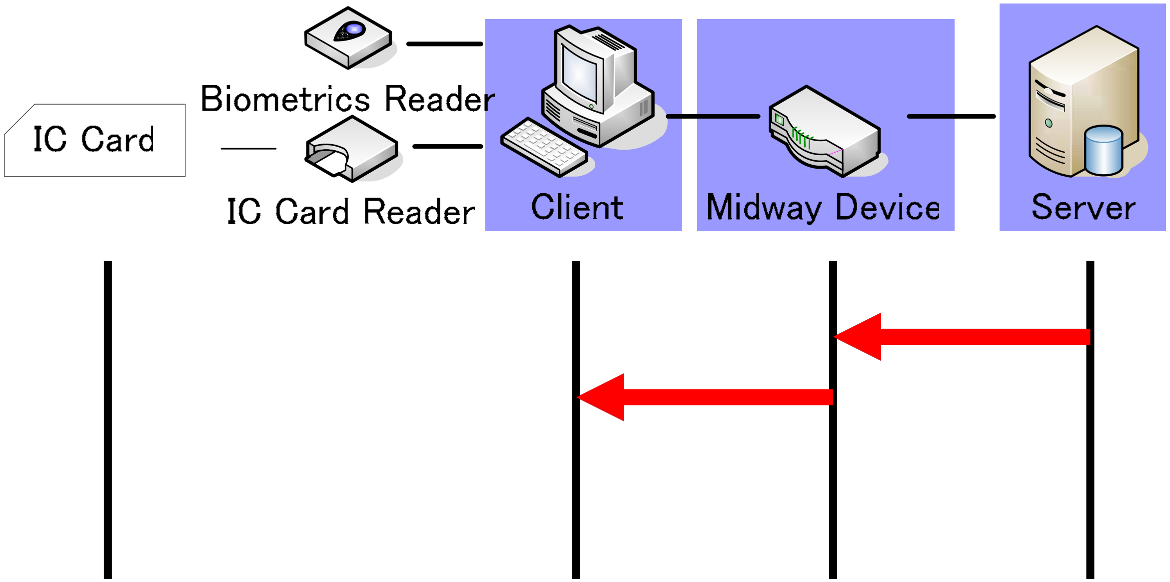
①ユーザ公開鍵Pux1，サーバ公開鍵PuSを送信
②生体情報の特徴点Sを取得
③乱数RNDを生成し，特徴点Sを暗号化
　乱数RNDをユーザ公開鍵PuSで暗号化し，ICカードへ送信
④特徴点Sを比較･照合
⑤乱数RNDをサーバ公開鍵PuSで暗号化しユーザIDを追加
　ディジタル署名と認証情報ACx1を付加しクライアントへ送信

提案方式の配送シーケンス



⑥受信したデータのハッシュを取り，乱数RNDで暗号化したものを追加
⑦サーバ宛に送信
⑧サーバ公開鍵PuSを用いて認証情報ACx1からユーザ公開鍵Pux1を取得
　ディジタル署名の検証を行う
⑨パケットの整合性が確認された場合，パケットを中継
⑩サーバはユーザ認証を行い，乱数RNDを取得

提案方式の配送シーケンス



⑪重要情報Dを乱数RNDで暗号化し，ディジタル署名を付加
　クライアントへ送信
⑫サーバ公開鍵PuSを用いてディジタル署名の検証を行う
⑬パケットの整合性が確認された場合，パケットを中継
⑭クライアントはサーバ認証を行い，重要情報Dを取得

提案方式の利点

- 非接触ICカードを利用した安全な情報配送
  - クライアント/サーバ間の乱数共有
  - クライアントが直接重要情報を取得
  - クライアントに初期情報が不要

- 中間装置での認証
  - 正規ユーザの配送パケットかどうかを判定
  - 配送を装った偽造パケットを遮断

まとめ

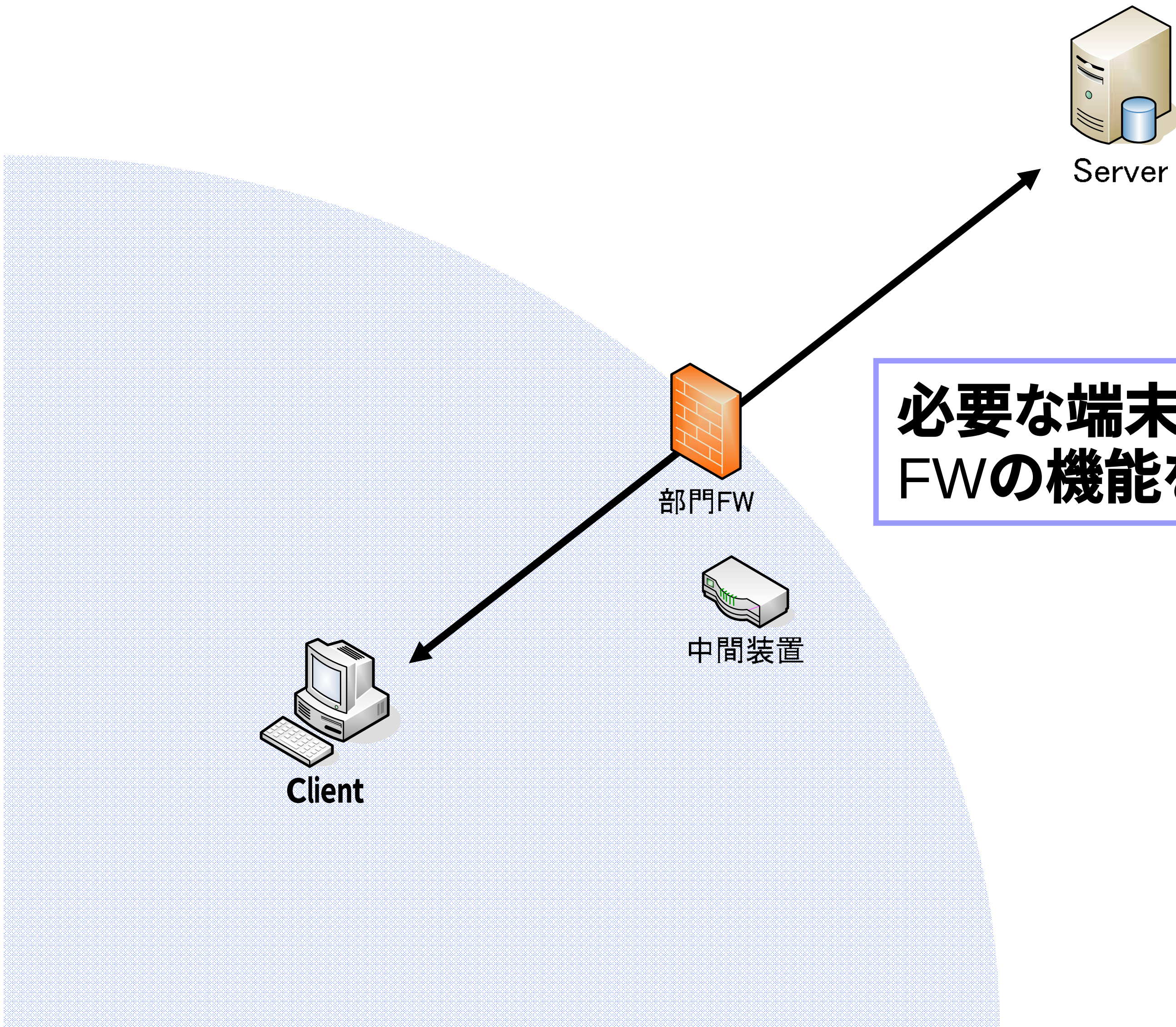
- 非接触ICカードを利用した重要情報の配送手段
  - 初期情報の追加
    - 初期情報を持たないクライアントへ安全に情報を配送
    - 中間装置での認証による通過
- 今後の課題
  - 提案方式の実装と性能評価
  - ネットワーク全体の負荷の増加
    - DoS攻撃等への対策
  - 端末へのログイン処理との連携

非接触ICカードを利用した重要情報の配送手段に関する提案

終わり

補足資料

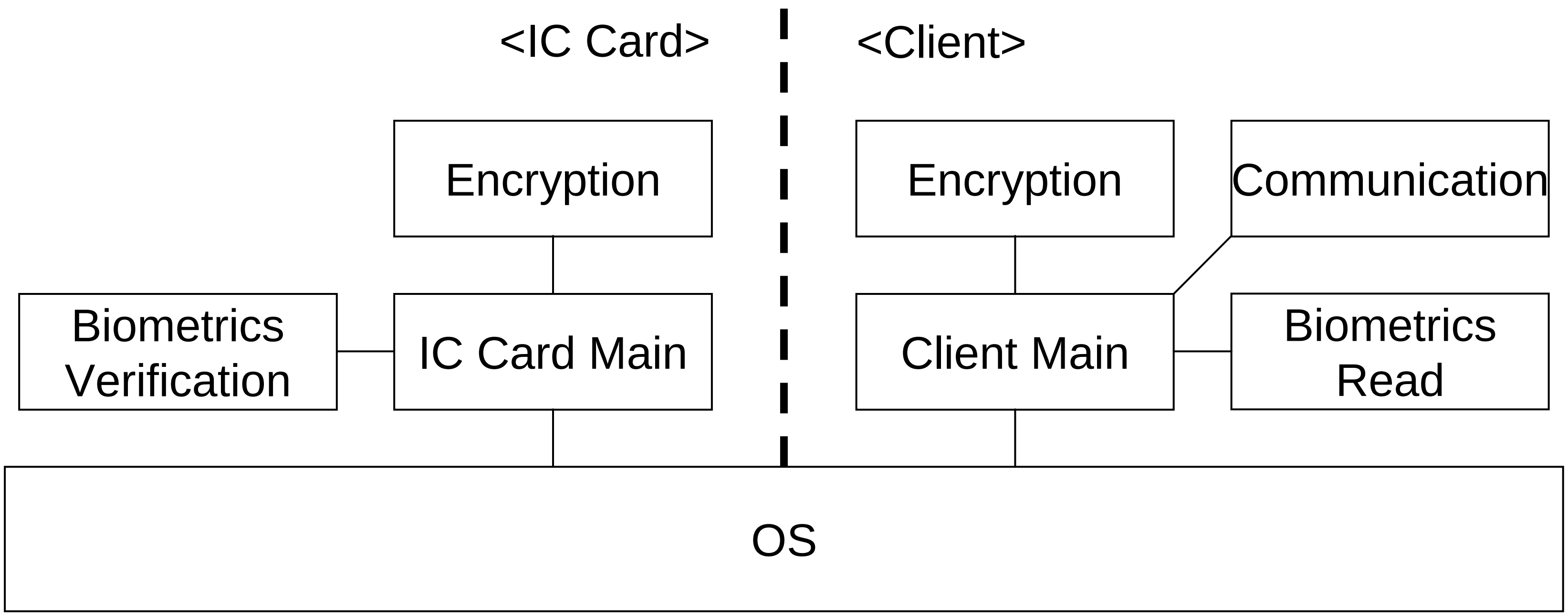
補足資料　–中間装置



必要な端末とアクセスするため
FWの機能を補助する役割

実装方法 –クライアント

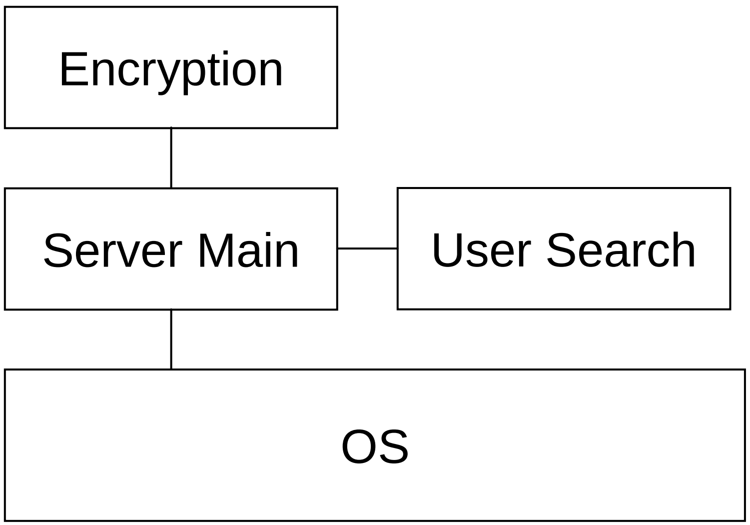
- 開発環境はFreeBSD 5.2.1
- ICカードの処理はクライアント内で仮想プログラムとして作成
- 生体認証はパスワード認証等の置き換えが可能



実装方法 –サーバ

- メインモジュール
- 暗号･復号モジュール
- ユーザ検索モジュール
  - ユーザIDから該当する公開鍵を取得

<Server>



実装方法 –中間装置

- 中間装置はIP層へ実装
- 配送パケットの転送時に呼び出し
- 不正パケットはその場で破棄

<Midway Device>