生体認証を利用した暗号鍵配送システム

Key delivery system using biometrics

前羽 理克　Masakatsu Maeba、渡邊　晃 Akira Watanabe（名城大学）

1. 研究背景

イントラネット内でのセキュリティ構築の手法として暗号技術を用いてセキュア閉域通信グループを構築する方式がある。そのグルーピングの手段として通信グループと共通鍵を 1 対 1 に対応させる方法が考えられている。このとき、ユーザ端末に対してグループ番号およびそれに対応した暗号鍵を安全・確実に配送しなければならない。本研究では、これらの情報の配信を実現するために生体認証技術を利用した個人認証システムを提案する。

2. 提案システムのポイント

・鍵管理サーバとユーザ端末間の認証は PKI に準拠するものとし、既存システムへの影響を最小限とする
・ユーザ側の認証に必要となる秘密情報はすべて IC カード内に保存させる。
・IC カードの使用者を認証するために、指紋とパスワードを用いる。
・従って、IC カード内に保持する秘密情報は、秘密鍵、指紋情報（テンプレート）、及びパスワードであり、あらかじめ登録しておく必要がある。
・指紋情報のマッチング処理、秘密鍵による署名生成は IC カード内部で行う。
・IC カードは耐タンパ性を有し、内部の秘密情報は外部に漏れないものとする。

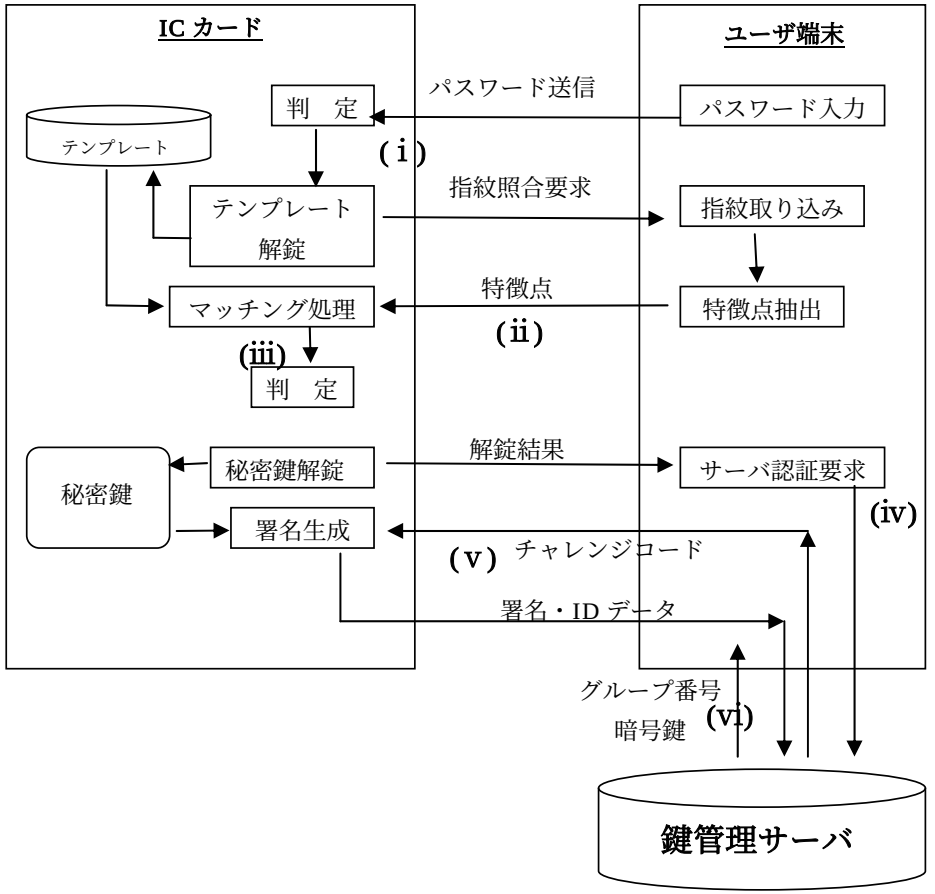
3. 提案システムの処理フロー

右に提案システムの構成を示す
本システムの処理フローを簡単に説明すると、
ⅰ)ユーザは端末を介してパスワードを入力する。判定結果が真ならばテンプレートが解錠され、同時にユーザ端末へ指紋照合要求を送信する。
ⅱ)ユーザ端末は指紋データを取り込み、特徴点データを IC カードに送信する
ⅲ)マッチングの判定が真ならば、秘密鍵が解錠される
ⅳ)ユーザ端末は鍵管理サーバに認証要求を送信し、チャレンジコードを獲得する
ⅴ)チャレンジを秘密鍵で暗号化し、ID データとともにサーバに送る
ⅵ)鍵管理サーバは認証を行い、認証が完了したら、グループ番号及びそれに対応する暗号鍵を送信する

4. まとめ

提案システムは、生体認証とパスワードを複合使用することにより、生体認証の脆弱性をフォローして、高いセキュリティを確保できていると考えられる。今後は、システムの実現及び既存システムとの定量的比較を行っていく。

＜提案システム処理フロー＞



＜参考資料＞[Ⅰ]渡邊、厚井、井手口、横山、妹尾：“ 暗号鍵を用いたセキュア通信グループの構築方法とその実現 ” 情報処理学会論文誌 **Vol.38 No.04－025**
[Ⅱ]ユビキタス時代のバイオメトリクスセキュリティ
著：瀬戸　洋一　出版：日本工業出版

生体認証を利用した暗号鍵配送システム

Key delivery system using biometrics

名城大学理工学部情報科学科
前羽　理克　Masakatsu Maeba
渡邊　晃　Akira Watanabe

研究背景

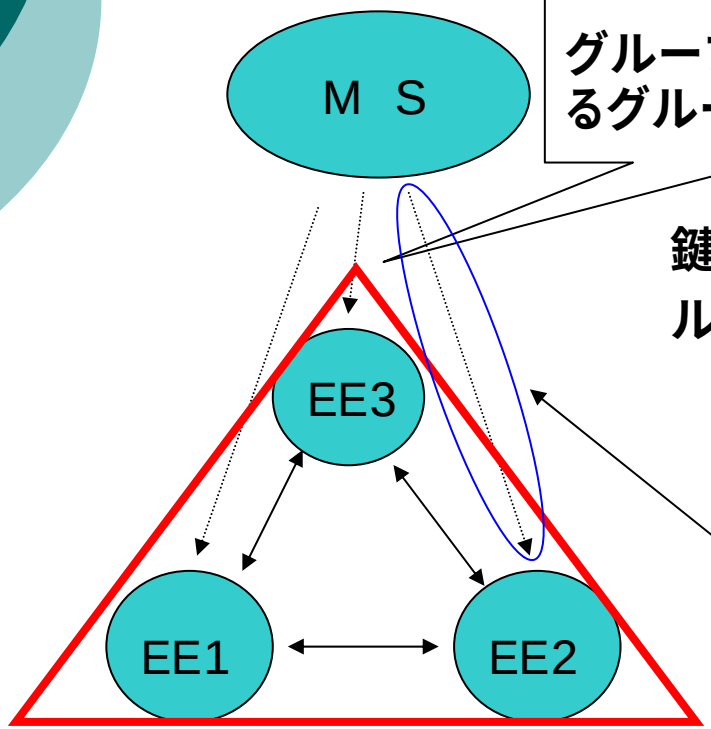
- インターネット･イントラネットの普及に呼応して、ネットワークセキュリティの研究が進んでいる
  --＞実際には、インターネットとイントラネットでは要求仕様が異なるため、個々に対応したセキュリティ構築が必要である

- インターネットのセキュリティ構築手段
  --＞インターネットVPN (Ipsec)

- イントラネット内のセキュリティ構築手段
  --＞ 暗号技術を用いてセキュア閉域通信グループを構築。そのグルーピング手段として通信グループと共通鍵を1対1対応させる方法が考えられている

本研究分野

研究内容



グループ番号に対応するグループ鍵：EKj

鍵管理サーバからグループ番号に対応するグループ鍵を配送し、グルーピングを行う

-->端末によらない自由なグルーピングが可能

MS：鍵管理サーバ

EE：終端装置

＜－－研究内容－－＞

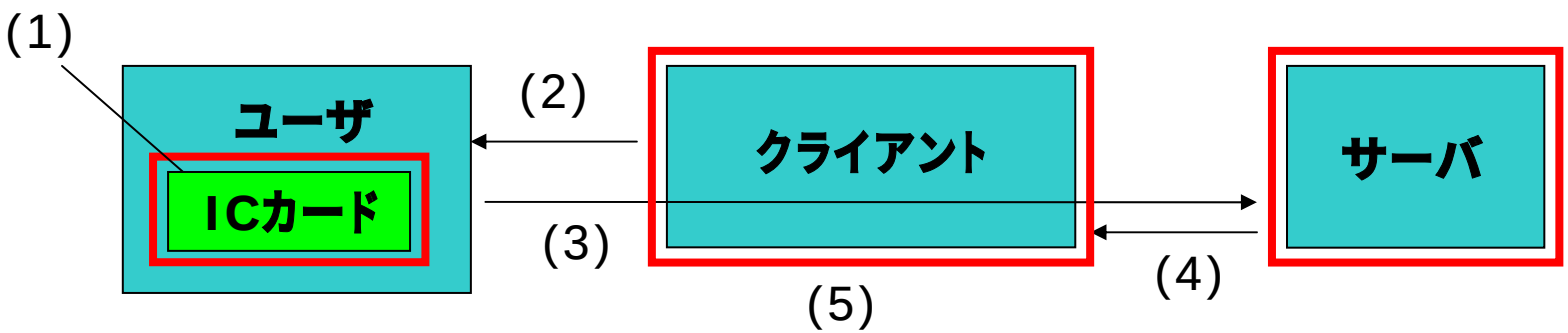
・正しいユーザにグループ番号・暗号鍵を送付するための、認証処理機能

・認証に生体情報を利用した安全なネットワーク認証

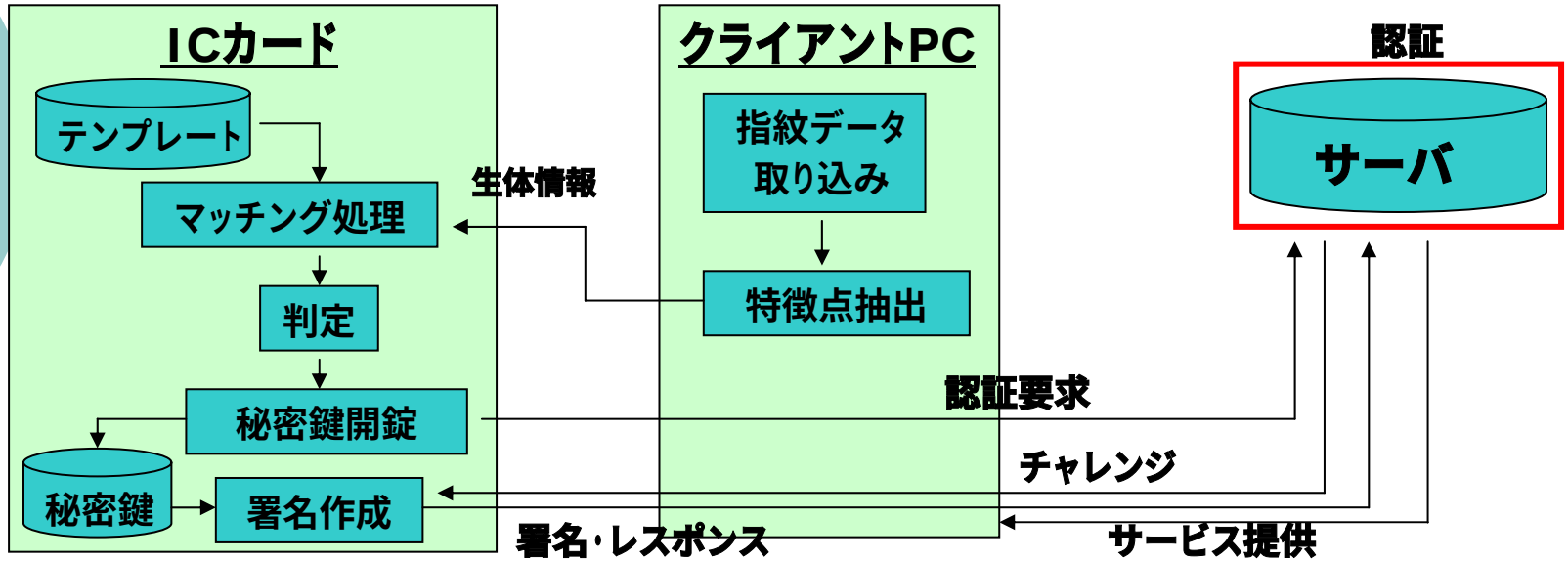
認証システムの機能要求

本システムに要求される主な機能を以下にあげる

1. ICカードの利用
2. 生体認証の利用
3. サーバによるユーザの認証
4. グループ番号＆暗号鍵配送時のセキュリティの確保
5. クライアントによるサーバの認証



既存生体認証システム



利点：➢秘密鍵・テンプレートをICカード内に保管しているため、データの盗用に対して高いセキュリティを実現

欠点：➢生体情報が生で流れるため、盗聴の危険がある

1.ICカードの利用
2.生体認証の利用
3.サーバによるユーザの認証

→ 既存システムの欠点を改良して利用

4.グループ番号＆暗号鍵配送時のセキュリティの確保
5.クライアントによるサーバの認証

→ 新たに提案

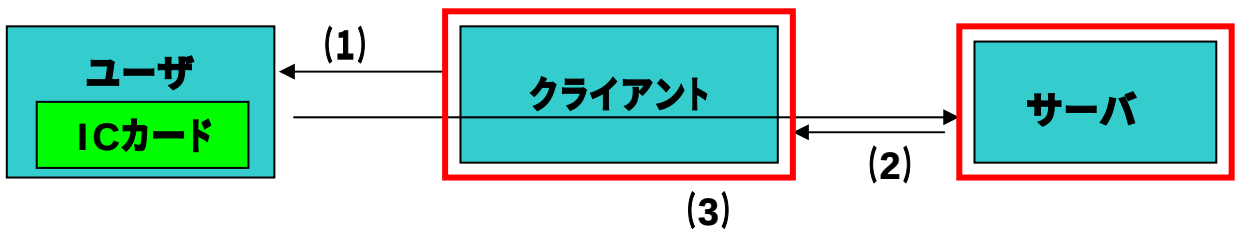
問題点の整理・構築時の留意点

問題点の整理

(1) 生体情報の暗号化通信

(2) グループ番号・暗号鍵の送信時のセキュリティの確保

(3) クライアントPCによるサーバの認証



システム構築時の留意点

ユーザ⇔クライアントPC

ユーザ⇔サーバ

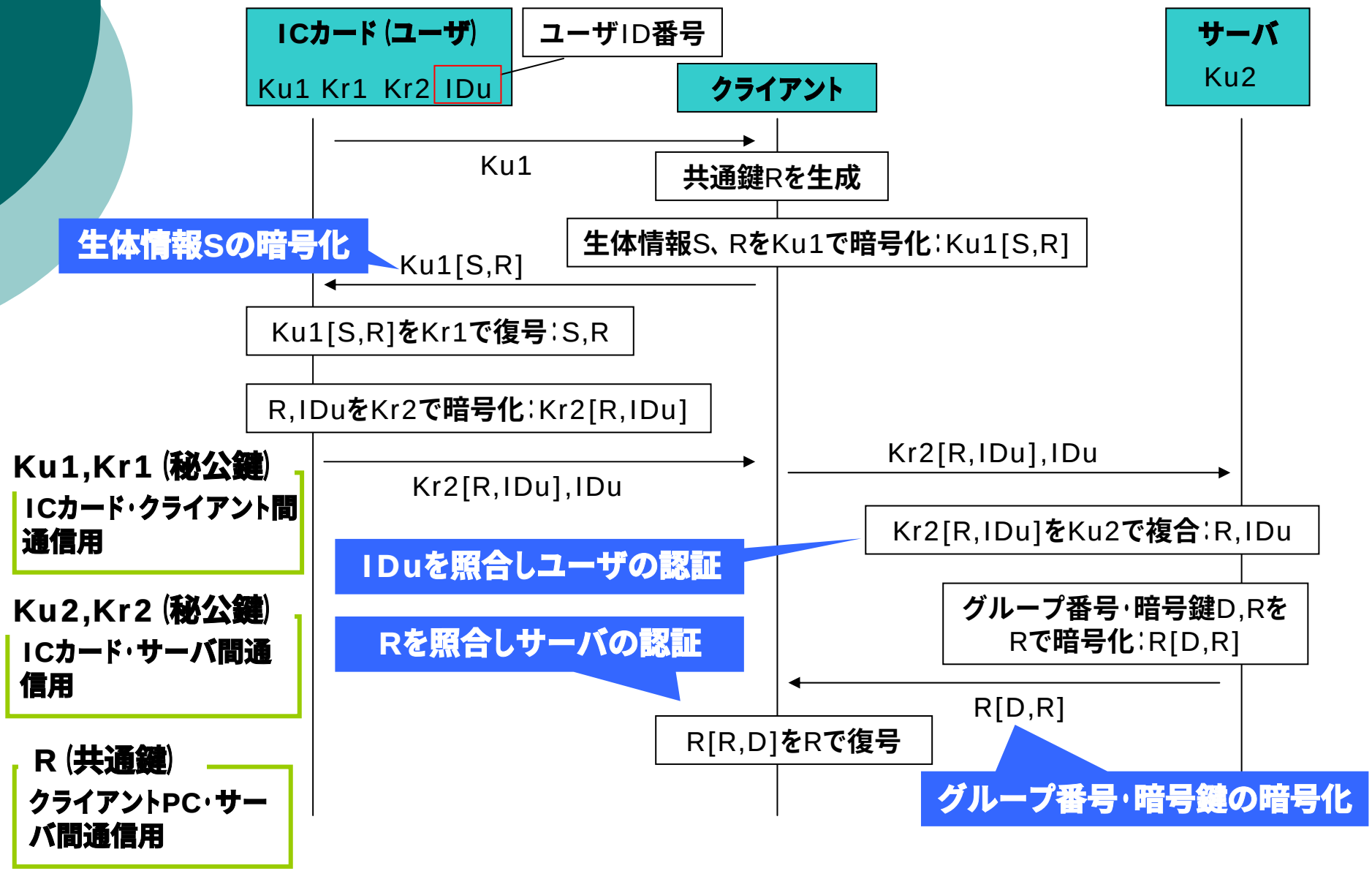
クライアント⇔サーバ

3種類の通信経路が存在 → 暗号化・認証のためには3種類の暗号鍵ペアが必要

システムの性質上、クライアントには依存しない → ICカードおよびサーバで鍵管理をする必要がある

以上の点をふまえた上で、提案システム認証処理を構築する

提案システム認証機能シーケンス



提案システムの利点

- 既存システムの利点･システム構成を損なわず、新しい機能を追加
  --＞既存システムから高い整合性でシステム移行が可能

- 通信路上を生で流れるデータは、公開鍵Ku1･ユーザIDのみ
  --＞盗聴に対して高いセキュリティを確保

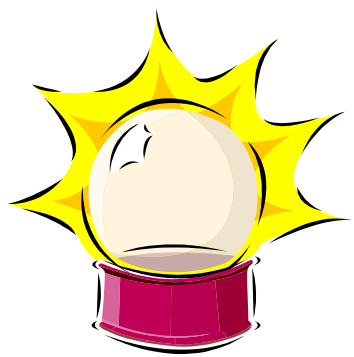
- 既存システムでは、明確に定義されていない“サービス提供”部分を提案
  --＞ICカード･生体認証を利用した、他のサービス提供システムに対して
  応用が可能

ま と め

今回の研究で機能要求を満たすシステムの提案ができた。

＜--今後の流れ--＞

- システムを実際に構築し、既存システムとの定量的比較
- 改ざん･成りすましに対するセキュリティレベルの確認及び改善案の提示

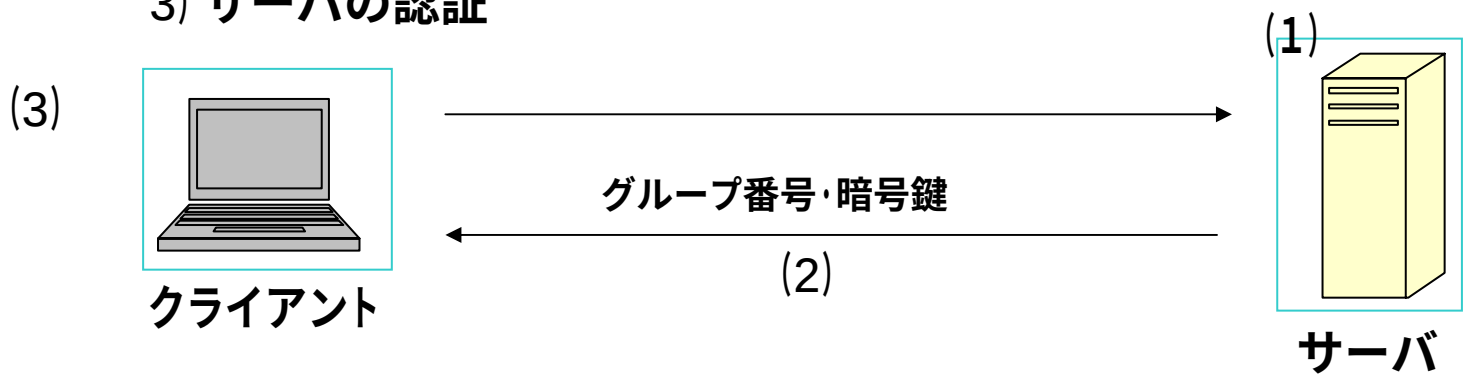


お　わ　り

改善案

提案システムでは、鍵管理サーバから“グループ番号・暗号鍵”を送信する。そのため、クライアント・サーバ間での通信のポイントは以下の3つあげられる

1) クライアントの認証
2) グループ番号・暗号鍵の送信時のセキュリティの確保
3) サーバの認証



改善案

(1) 生体情報の暗号化

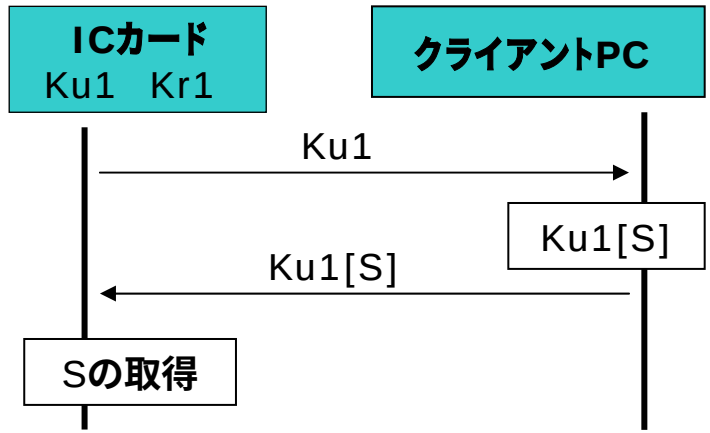
i. 秘密鍵Kr1・公開鍵Ku1ペアをICカード内に保持

ii. Ku1をクライアントPCに送信

iii. 生体情報SをKu1で暗号化

iv. Ku1[S]をICカードに送信

v. Kr1で複合、生体情報を取得



(2) UDP通信可能なサーバによるユーザ認証

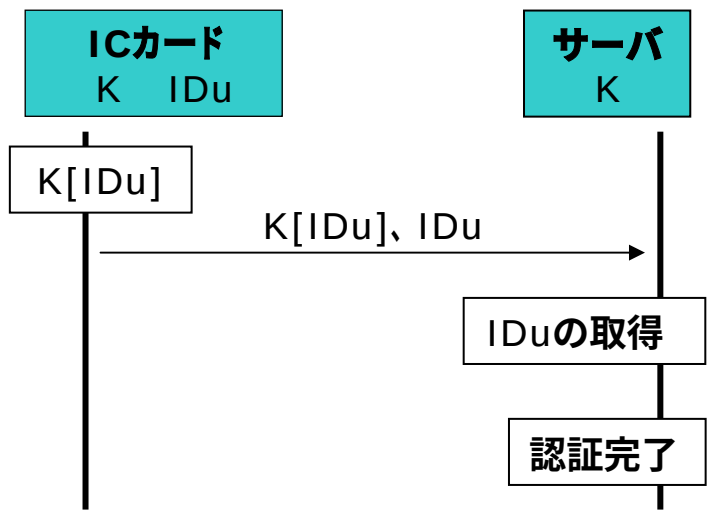
i. ICカード・サーバにユーザ毎に異なる共通鍵Kを保持。また、ICカード内にはユーザIDも保持

ii. IDuをKで暗号化

iii. K[IDu]、IDuをサーバに送信

iv. サーバはKでK[IDu]を複合し、IDuを取得

v. 照合結果が正しければ、認証完了



改善案

(3) グループ番号・暗号鍵送信時のセキュリティの確保

(4) クライアントPCによるサーバの認証

i. クライアント側で共通鍵Rを生成

ii. Rを暗号化しサーバに送信

iii. サーバはグループ番号・暗号鍵DをRで暗号化

iv. R[D]をクライアントPCに送信

v. クライアントPCはRで複合、Dを取得

鍵送信時のセキュリティの確保完了

クライアントPCによるサーバの認証完了