モバイル端末の安全性向上のための モバイル端末とセキュアデバイスの連携方式に関する研究

内山　宏樹　　梅澤　克之　　洲崎　誠一

(株)日立製作所　システム開発研究所

1　はじめに

モバイル端末の普及とネットワーク環境の整備により、いつでもどこでも様々なサービスを享受可能なユビキタス社会が広がりつつある。今後、サービスの拡大によりモバイル端末内部に決済情報や生体情報などの重要なデータが格納されていくことが考えられる。これらのデータの盗み見や改ざんを防止するためには、モバイル端末全体の安全性を向上させることが必要となる。

モバイル端末の安全性向上には、ＩＣチップ等で利用されているハードウェア耐タンパ技術が有効である。しかし、モバイル端末はＩＣチップとは異なり、デバイス構成が複雑であるため、全体的な耐タンパ性の確保は困難であり、実現には多大なコストを要する。そこで、本研究では、耐タンパな領域をＩＣチップ等のセキュアデバイスに集約し、モバイル端末と組み合わせることにより、モバイル端末の安全性を向上させる方式を開発した。

本稿では、まず、２章でモバイル端末の安全性向上の際の要件について説明し、３章では本研究で開発した方式について、システム構成や前提条件を含めて述べる。４章では開発した方式の評価結果を示し、最後に５章でまとめと今後の方針を記述する。

2　要件

以下にモバイル端末の安全性を向上させる際の要件を列挙する。

①安価に実現可能な方式
②頻繁な端末の更新が発生する
③性能が低く、メモリ容量に制限がある

本研究では、これらの要件を満たすような方式を開発した。以下では提案方式に関して詳細に記述する。

3　実現方式の検討

3．1　システム構成

本研究で提案するシステム構成を図１に示す。

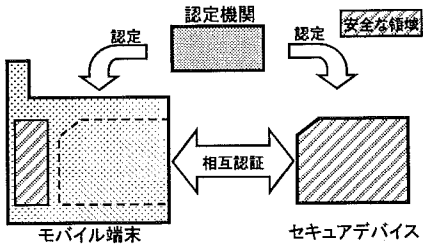

図１　システム構成

本研究で提案するシステムは、モバイル端末、セキュアデバイス、認定機関の三者から構成される。要件②を満たすために、モバイル端末には着脱可能なセキュアデバイスを組み合わせた。このような構成の場合には、不正なモバイル端末やセキュアデバイスの利用を防ぐために、モバイル端末とセキュアデバイス間で相互認証を実施し、互いの正当性を検証する必要がある。図中の安全な領域には、相互認証時に利用するデータを格納する。また、図中の認定機関とは、モバイル端末、及び、セキュアデバイスを事前に認定する第三者機関である。

3．2　前提条件

提案方式には以下の前提条件を設定した*。

① モバイル端末内に小容量の安全な領域が存在する
② モバイル端末及びセキュアデバイス自身が認定機関に認定されている

3．3　提案方式

相互認証方式を開発するにあたり、モバイル端末とセキュアデバイスの組み合わせ変更を容易にするために、安全な鍵配送が容易な公開鍵方式を利用することを検討した。しかし、公開鍵方式は共通鍵方式に比べ、多くの処理時間とメモリ容量を必要とするため、要件③から、従来方式をそのまま適用することは適切ではない。そこで、多くの処理時間が必要となる部分の実施回数を最小化するように、処理全体を分割し、全体の処理時間を低減させる方式を開発した。

Research on the method of combining a mobile terminal and a secure device for the improvement in the security of mobile terminals
Hiroki Uchiyama, Katsuyuki Umezawa, Seiichi Susaki
Hitachi, Ltd., Systems Development Laboratory

*これらの前提条件は、「現状の携帯電話にはＳＩＭカード等のＩＣチップが搭載されつつあること」、「現状の携帯電話はキャリア、ＩＣカードは発行者によって既に認定が行われていること」から現状と大きくかけ離れているものではないと考えられる。

具体的な処理フローを図２に示す。

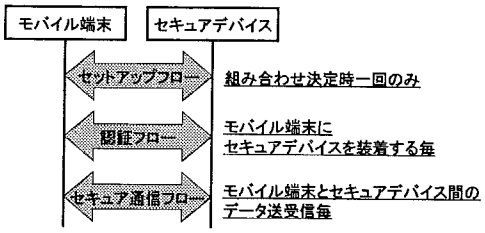

図２　処理フロー

処理フローはセットアップフロー、認証フロー、セキュア通信フローから構成される。セットアップフローは、モバイル端末やセキュアデバイスの更新時など両者の組み合わせを初めて決定する際に実行する。認証フローは、モバイル端末にセキュアデバイスを装着する度毎に実行する。セキュア通信フローは、モバイル端末とセキュアデバイス間でデータの送受信を行う毎に実行する。以降の節で各々のフローで行われる処理を詳細に説明する。

３．３．１セットアップフロー

セットアップフローでは、モバイル端末及び、セキュアデバイス内に認定機関の署名が格納されているか否かを確認し、共通鍵を生成する。図３に流れを示す。

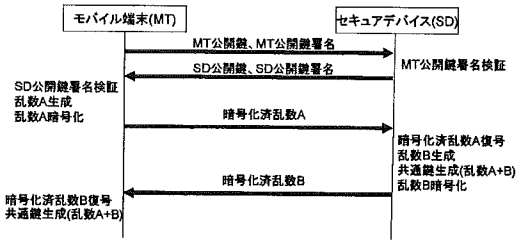

図３　セットアップフロー

３．３．２認証フロー

認証フローでは、セットアップフローで生成した共通鍵を用いてセッション鍵を生成する。図４に流れを示す。

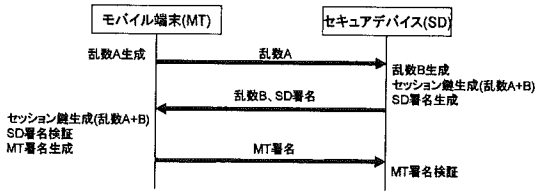

図４　認証フロー

３．３．３セキュア通信フロー

セキュア通信フローでは、認証フローで生成したセッション鍵を用いて送受信データに署名を付加し、データ自身を暗号化する。図５に流れを示す。

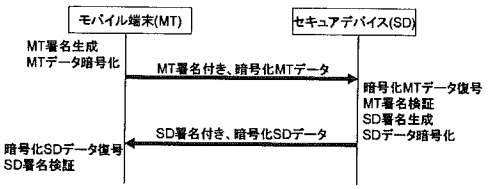

図５　セキュア通信フロー

４　評価

図６に提案方式と従来方式（公開鍵方式、共通鍵方式）の性能評価結果を示す。横軸は実行回数、縦軸は一回あたりの処理フローに要した時間の平均値を示す。提案方式は認証回数が増加すればするほど、一回あたりの処理時間の平均値が共通鍵方式と同等レベルまで減少していくことがわかる。

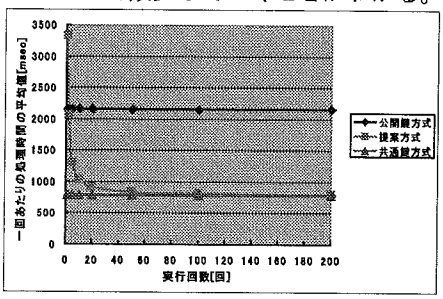

図６　性能評価結果

５　まとめと今後の方針

本研究では、モバイル端末の安全性を安価に向上させるために、モバイル端末にセキュアデバイスを組み合わせる方式を提案し、両者間の相互認証方式を開発した。提案方式は、公開鍵方式よりも高速で、安全な鍵配送も容易であるという特徴を持つ。

今後は提案方式を実際の携帯電話端末等及びＩＣカード等に実装し、使い勝手や処理時間等を検証していく予定である。

謝辞

本研究は、独立行政法人情報通信研究機構（ＮＩＣＴ）の委託研究「モバイル端末におけるセキュリティ保護技術に関する研究開発」の一環として実施された。

参考文献

[1] *GlobalPlatform Card Specification Version 2.1.1*, Global Platform Inc., March 2003.
[2] T. Dierks, C. Allen: *RFC2226 - The TLS Protocol Version 1.0*, IETF, January 1999.