4U-06

携帯電話応用システムにおけるセキュリティ機能に関する考察

松田 規　　中野 初美　　中川路 哲男

三菱電機（株） 情報技術総合研究所

1. はじめに

従来、携帯電話は単なる音声通話を行う道具であったが、近年では Web ページの閲覧等、インターネットへ接続可能な携帯型情報端末へと成長している。そして、今後は Web ページ閲覧だけでなく、コンテンツ販売や、個人間のデータ交換なども盛んになると考えられる。コンテンツの不正流出・使用の防止などの観点から考慮すると、通信前に互いに通信相手を認証した後に、データを暗号化して送信することが望ましい。これを実現する技術として PKI (Public Key Infrastructure)が知られている。本技術では、電子署名や認証の実現に必要な証明書に関して、CA(Certification Authority)等の信頼おける機関による証明書発行・配布・失効管理等を実現するための方式が規定される。PKI は今後のモバイル EC に必要不可欠な技術だが、携帯電話は CPU 性能やメモリ量等のリソースが限られている点、証明書の発行・配布・失効管理などの運用面の検討が十分に行われていない点等により、携帯電話で PKI が完全に利用できる様に実装されるには至っていない。

本発表では、携帯電話にて電子署名等の PKI 機能が利用できない環境においても、携帯電話が契約しているネットワークオペレータ（以下オペレータと略す）を信頼できる機関として考える事により、携帯電話間で安全に通信を行う方式について検討した結果を報告する。

2. 携帯電話間通信に対する脅威

携帯電話間での通信時に発生しうる脅威を考えるにあたり、図１に示すようなモデルを想定する。このモデルは、異なるオペレータと契約する携帯電話間において、互いにコンテンツを交換するケースである。ここで、ネットワークは第三者によって盗聴・改竄がなされる危険性を持った安全でない通信回線と仮定する。

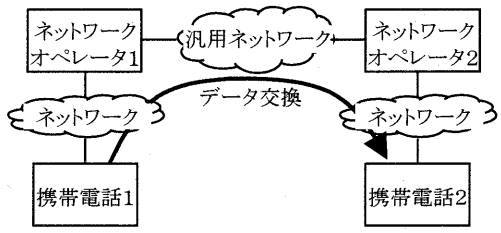

図１：検討モデル

この時、検討モデルに関して、次のような脅威が起こりうると考えられる。

- 第三者が携帯電話２に成りすまし、携帯電話１と不正に通信を行う
- 第三者が携帯電話１に成りすまし、携帯電話２に不正にコンテンツを送る
- 第三者が携帯電話１－携帯電話２間の通信を傍受し、コンテンツを不正に取得する

携帯電話間での通信を実現するためには、これらの脅威を防止・検出するセキュリティ技術を携帯電話に適用し、安全性を確保する必要がある。

3. 携帯電話での秘匿・認証通信

前章にて、携帯電話間での通信において考えられる脅威について述べた。これらの脅威への対策として、通信時に(1)携帯電話で相互認証を実施する事により正しい相手と通信している事を検証し、かつ(2)携帯電話間の通信を暗号化することにより秘匿する事が必要である。しかし、現状の携帯電話では、携帯電話の相互認証にて利用する電子署名に必要な、秘密鍵・証明書を扱うための機能や性能が十分には提供されていない。

そこで、携帯電話に PKI の全ての機能を実装することなく、安全な認証・秘匿通信を実現する方式として、次のような方式を提案する。

- オペレータが携帯電話加入者の身元を保証する事により携帯電話間の相互認証を行う
- CA が目的別に分割発行した証明書失効情報を扱え

Security functionality for mobile phone
N.Matsuda, H.Nakano,T.Nakakawaji
Information Technology R&D Center,
Mitsubishi Electric Corporation

るようにし、効率的な証明書失効確認を行う

3.1. 身元保証による携帯電話間認証

[前提条件]

身元保証方式では、次の事項を仮定する。

- 現在の携帯電話には、通信料金の課金等の目的のために、携帯電話固有に割り当てられた加入者 ID が事前に埋め込まれており、オペレータは携帯電話を一意に認証可能である
- 携帯電話はオペレータとの契約を交わした後に利用可能となる。即ち、契約を交わした時点で、携帯電話にとってオペレータは信頼できる機関として考えることが出来る

この仮定により、オペレータは携帯電話加入者の身元を保証することが出来る。

[実現方式概要]

オペレータが携帯電話加入者の身元を保証する情報として加入者証明情報を作成し、これを用いた携帯電話間認証を行う事を考える。図２は、そのモデルである。

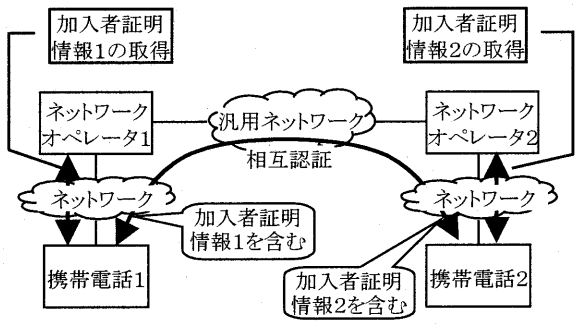

図２：身元保証による認証方式概要

図に示したように、携帯電話１はオペレータ１から加入者証明情報１を取得し、携帯電話２への通信データに添付、携帯電話２はオペレータ２から加入者証明情報２を取得し、携帯電話１への通信データに添付する事により、携帯電話間で相互認証を行う。これにより、携帯電話にて電子署名を行う機能が提供されていなくても、相互認証が実現される。

[実現方式詳細]

携帯電話からの要求にて作成した加入者証明情報が、他目的に不正に使用される事があってはならない。そのため、加入者証明情報は次の要件を満たす必要がある。

- 携帯電話をユニークに特定でき、かつ身元保証の要求を受けたデータ以外には転用困難である
- 加入者証明情報は専用の署名鍵にて作成される
- 加入者証明情報の失効管理を不要にするため有効期間が短期間である

そこで、加入者情報は次のようなデータを含んだ構成にする事が望ましいと考える。

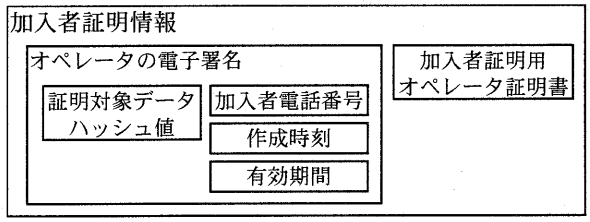

図３：加入者証明情報の構成

図のような構成にする事により、加入者証明情報は転用が困難、かつ失効管理が不要となる。

3.2. 分割発行された証明書失効情報のサポート

加入者証明情報の検証を行うためにはオペレータの署名を検証する必要がある。署名検証は、(1)署名正当性検証と(2)証明書失効検証に分けられる。ここで、(2)証明書失効検証には、CA が発行した CRL(Certificate Revocation List)を利用するが、これは CA の管理下にある全ての証明書を対象として発行されるため、データサイズが大きくなり易いという問題点がある。

本点に関しては、CA 証明書の失効情報のみ記述された ARL (Authority Revocation List)や、新しく X.509 で規定された CRL 拡張機能の利用が有効である。これにより携帯電話で頻繁に利用されるオペレータ証明書の失効管理情報を効率的に配布する事が可能である。

4. まとめ

本発表では、オペレータが信頼できる機関との仮定の下、携帯電話間で安全な認証を実現する方式について検討した。今後は、著作権管理が可能なコンテンツ配信方式等に対して本方式を適用する事を検討する。

参考文献

[1] D.R.Stinson (櫻井幸一監訳):"暗号理論の基礎", 共立出版

[2] C.Adams, S.Lloyd (鈴木優一訳) : "PKI", ピアソン・エデュケーション・ジャパン