社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2006－CSEC－35 (7)
2006／12／8

携帯電話を用いた署名機能付メールシステム

田口 幸平 宇田 隆哉

東京工科大学コンピュータサイエンス学部

本論文では、携帯電話のアプリケーションを用いて電子署名を行うことで、携帯電話から安全なメールの送受信が行なうことを目的としたメールシステムを提案する。近年、連絡手段としてメールを利用する機会が増えているが、それに伴い、フィッシングメールなどのメールを利用した犯罪も増加している。解決策として、メールの正当性を証明する電子署名がある。しかし、現在利用されている一般的な署名メールでは、秘密鍵の管理に問題があり、不正アクセスされた場合、改竄やなりすまし鍵の不正利用などができてしまうといった問題がある。本システムでは、携帯端末内で安全に管理された秘密鍵を用いてメールに署名を施し、認証局に登録した公開鍵を利用して、メールを検証することで第三者に保障された本人認証を行なう。また、公開鍵暗号のアルゴリズムをアプリ系ション内で独自実装することで、携帯会社に依存しない署名メールの送受信が可能となる。

The digital signature function email system On A Cellular Phone

Kohei Taguchi, Ryuya Uda

Tokyo University of Technology School of Computer Science

I propose the e-mail system that can send and receive safe e-mail by using application of cellular phones to sign electronically. In recent years, the crimes which use e-mail such as fishing-e-mail have increased, so we need to prove justice of e-mail by using signature more than ever. However, there is a problem such as the falsification and the disguise key can be illegally used when there is a problem in the management of the private key, and it is accessed illegally in the general signature mail being used now.
In this system, we sign e-mail by using secret-keys that are managed safely in cellular phones' terminal and use public-keys that are registered at a certification office to certify the original person guaranteed by others by inspecting e-mail. In addition, the transmission of a message is enabled in e-mailing it the signature that does not depend on a cellular company by implementing public key encryption by software originally.

1． はじめに

近年、ネットワークの急速な普及や、携帯電話のメール機能の登場などに伴い、連絡をとる手段としてメールが使われる機会が増加している。しかし、インターネットを流れるメールは、テキストベースで伝送されており、盗聴や、改竄などが容易にできてしまうといった問題がある。また、金融機関などの正規のメールを装い、暗証番号や口座番号を搾取するフィッシングメールなどのオンライン詐欺など、メールを利用した犯罪も増加してきており、本当に本人が送ったものかどうかの確認の重要性が高まってきている。

現在、なりすまし・改竄対策として、電子署名を利用して、本人確認やメールの改ざんがあるかどうかの確認が行なわれている。しかし、署名生成や復号化などに用いられる秘密鍵を、ハードディスク上にファイルもしくはレジストリの形で保存している場合が多く、そのため、パソコンに不正アクセスされた場合、鍵の改竄や第三者による不正利用・暗号化メールの解読などができてしまうといった問題が生じる。

本論文では、秘密鍵の保護問題の解決策として、一般的に普及している携帯電話を用いることで秘密鍵を安全に管理し、署名を施したメールを送信することでなりすましや改竄、否認を防止できるシステムを提案する。

2. 関連研究

現在、提供されている電子署名付きメールシステムは、一般的に S/MIME[1]を用いたサービスが提供されている。S/MIME は、MIME を利用することにより電子メールに暗号化と電子署名のセキュリティ機能を提供している。既存技術の MIME を利用するため、既存のメールサーバーで動作可能なメールの暗号化方式である。S/MIME を利用した署名付加メールサービスとして、サーバー型のメールシステム[2]や IC カードを用いたメールシステム[3]が提供されている。

まず、サーバー型のメールシステムでは、メールサーバーを通過するメールに対して自動的に電子署名を付加するため、手作業の署名作業に比べ作業負担が少ない。しかし、導入時にかかるコストが高いといった問題がある。

次に、IC カードを用いたシステムでは、PKI 対応の IC カードを用いることで、秘密鍵を安全に管理できる。また、盗難対策として、カード使用時に PIN（Personal Identification Number）と呼ばれる:暗証番号を入力させ、一定回数間違えると IC カードがロックして使えなくなるといったカードを利用し、電子署名を行なうことでよりセキュアなメールを送信することができる。しかし、このシステムでは、IC カードの他にパソコンと接続する為の IC カードリーダも必要であるため、サーバー型のメールシステムと同様に導入時にコストが高いという問題点が挙げられる。

本システムでは、市販で販売されている携帯電話のアプリケーション（以下、アプリ）を利用することで、IC カードを用いたメールシステムと同じように秘密鍵の安全な管理を行なう。

現在、携帯電話を用いた認証方式として NTTDocomo の Firstpass [4] や KDDI の SecurityPass [5]などが実現されている。これらは、携帯電話会社に依存した認証サービスであるため、利用制限があり、独自に証明書の格納や、署名を発行したりできず、利用事業者が限定されている。

また、その他の携帯電話を用いた関連研究として、公開鍵暗号をソフトウェア実装した携帯電話の IC チップを用いた相互認証システム [6]や、携帯電話を利用して代返を防止し出席率の向上を図る出席確認システム[7]などがある。これらの研究では、公開鍵暗号をソフトウェア上で独自実装することで、携帯電話会社に依存することなく、電子署名の発行などが行なえるシステムである。本システムでも、公開鍵暗号をソフトウェア上で実装することで携帯電話会社に依存しない電子署名の発行を行ない、S/MIME を用いてメールに署名を付加できるようにする。

3. システム概要

3．1 概要

本システムは、図 1 に示すように秘密鍵の管理、署名付きメールの送信を行なう携帯電話、送信者の正当性を証明する認証局、メールの受信を行なう S/MIME 対応のメーラを導入したパソコン、もしくは本システムの携帯電話から構成される。

本システムでは、認証局を利用し、証明書を発行することで第三者から保障されたメールの送信を行うことができる。

送信者は、あらかじめ公開鍵と秘密鍵の鍵ペアを生成し、認証局に公開鍵とユーザーIDを登録しておく。送信者は、携帯電話のアプリを起動し、アプリ内でメールを作成し、秘密鍵を利用して署名の生成を行い、メールに署名を付加することで受信者に対してメールの送信を行う。

受信者は、認証局に登録されている送信者の証明書を取得し、署名の検証を行う。本システムでは、公開鍵の登録、取得の途中に鍵の改竄を行なえないように SSL 通信を用いて暗号化を施している。登録時とメール送信時の流れについて次項で説明する。

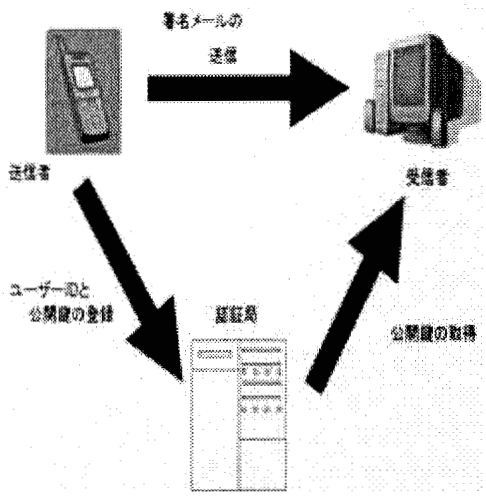

図１　システム概要

３．２　　登録時の流れ

図２に登録時の流れを示す。利用者は、サイトから本システムのアプリをダウンロードし、初回のアプリ起動時のみ、公開鍵と秘密鍵の鍵ペアの生成を行う。利用者は、携帯端末内で鍵ペアの生成後、ユーザーID と公開鍵を認証局に登録する。また、秘密鍵を携帯端末内のスクラッチパッド領域に格納する。スクラッチパッド領域は、他のアプリケーションからはアクセスできない為、スクラッチパッド領域に格納することで、安全な秘密鍵の管理方法を実現することができる。

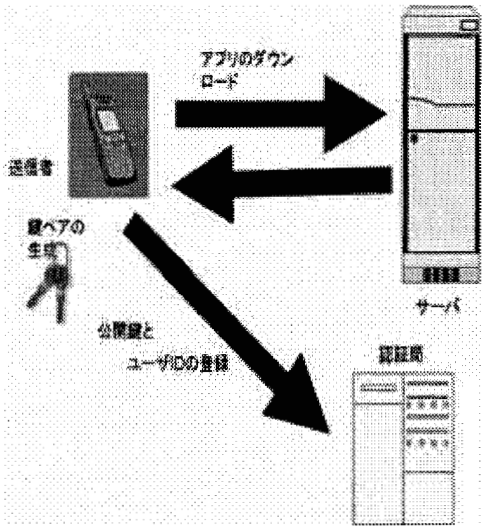

図２　登録時の流れ

３．３　　メールの送信

メール送信の流れについて以下に示す。

１．利用者は、アプリを起動してアプリ内でメールの作成を行う。

２．携帯端末内の秘密鍵を用いて署名を生成する。

３．生成した署名・本文をサーバーに送信する。

４．サーバー側で S/MIME フォーマットを作成

５．SMTP を用いて署名メールを送信する。

４．　　実装

４．１　登録

電子署名には、RSA1024 ビットを用いる。電子署名には、ECDSA（楕円曲線暗号）や RSA といった方式があるが、本システムでは、パソコンを利用した既存のメーラでも受信・検証が行なえるように S/MIME を用いて電子署名を付加してメールの送信を行う。S/MIME では、電子署名に利用できるアルゴリズムが限られており、ECDSA はサポートされていないため、RSA を用いる。

RSA 暗号方式は大きな整数の素因数分解が困難であるという仮定に基づいていたアルゴリズムであり、現在、一般的な暗号化方式である。

鍵ペアの生成後、ユーザーID と公開鍵を認証局に登録する。ユーザーID には、携帯電話の UIM カードの ID を用いる。UIM カードは、ユーザーの識別に利用する着脱可能な小さな IC カード（FOMA）カードのことであり、すべて異なる番号が割り振られている。また、この UIM カードは個人で改竄することが困難であり、なりすましの防止につながると考えられる。

認証局に登録する際、公開鍵の漏洩を防ぐために、128 ビット SSL で暗号化された通信路を利用して登録を行う。また、秘密鍵は、携帯端末内のスクラッチパッド領域に格納する。スクラッチパッド領域に格納することで、

秘密鍵を安全に管理することができる。また、初回起動以降は、携帯端末内に秘密鍵を格納してあるので、鍵ペアの生成を行なう必要がない。

4．2　メール送信

送信者は、アプリを起動しアプリ内でメールの作成を行い、署名の生成を行なう。クリアテキスト署名を用いる。署名メールの本文は、署名と一緒に CMS (Cryptographic Message Syntax) でエンコードされている。そのため、S/MIME に対応していないメーラ（MUA）では、署名の検証だけでなくメール本文を読むことすらできない。そこで、クリアテキスト署名を用いることにより、S/MIME に対応していないメーラ（MUA）であっても、メール本文を読むことができる。

メールの作成後、メールの本文に対してハッシュ関数 SHA-1 を用いて 160 ビットのハッシュ値に変換し、携帯端末内に格納している送信者の秘密鍵を用いて、暗号化したものを署名とし、メール本文と署名をメールに添付する。その様子を図３に示す。

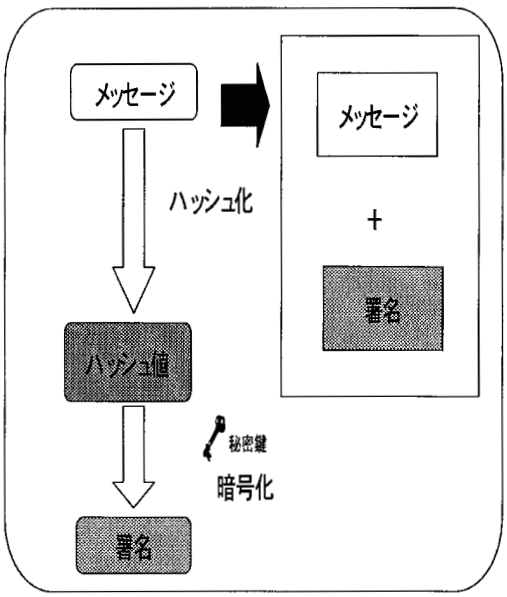

図３　署名の生成

署名の生成後、携帯電話の通信機能を用いてサーバーとの通信を行う。携帯電話とサーバー間の通信は HTTP による POST 形式で宛先、件名、メールの本文、アプリ内で生成した署名データを受け渡す。

受け取ったサーバーは、S/MIME のメールのフォーマットに整形を行なう。携帯電話による署名はＣＭＳの signed-data 型でエンコードし、CMS署名メッセージとメール本文をマルチパート形式で MIME エンコードする。CMS は PKCS#7 を拡張して作られた暗号と署名を扱うデータフォーマットである。CMS データ内には、CMS のバージョン、ダイジェストアルゴリズムの識別子、署名の対象データ（署名の対象となるデータの型とデータそのもの）、署名者の情報（署名に使用するダイジェストアルゴリズムの識別子、署名に使用するアルゴリズム、署名）、証明書のリストなどの情報が含まれ、Base64 変換されメールに添付される。図４に CMS データフォーマットについて示す。

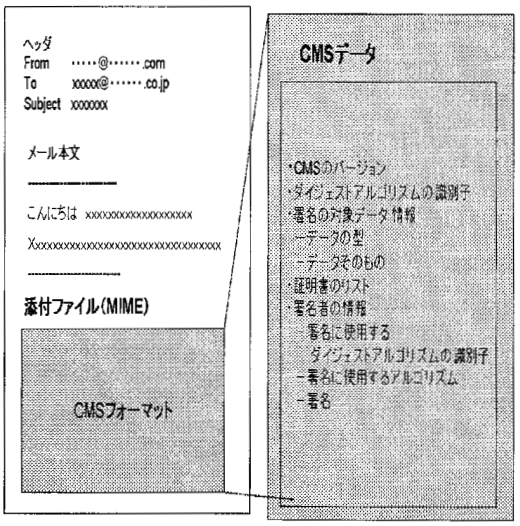

図４　CMS フォーマットの情報

S/MIME のメールフォーマットに整形後、CGI を用いて、SMTP コマンドを用いて SMTP サーバー（ポート２５）からメールを受信者に送信する。

4．3　メール受信

本システムでは、IMAP[8]を用いてメールの受信を行なう。IMAP は、IMAP サーバー上でメールの管理を行なうことができる。また、メールの MIME 構造を解析して、特定のパートだけを取得することもでき、テキスト部分

だけを取得するといったことが可能であり、情報量を削減することができるため、メモリの少ない携帯電話でも利用することができる。
本システムの実装では、メールのメニューにメール受信ボタンを用意しておき、ボタンが押された時、携帯電話とサーバー間を HTTP により通信を行なう。その後、CGI を用いて、IMAP コマンドを用いて IMAP サーバー（ポート１４３）から受信しているメール情報を取得する。

受信者は、メール受信後、CGI を用いて署名検証プログラムに受け渡す。署名検証プログラムでは、BASE64 に変換されて送られてきた署名を Base64 逆変換により署名の復元を行ない、送られてきたメッセージからハッシュ関数 SHA-1 を用いて 160 ビットハッシュ値に変換したものと、認証局に登録されている送信者の証明書を取得し、送信者の公開鍵を用いて署名を復号化して求めたハッシュ値とを比較して検証を行なう。その様子を図５に示す。

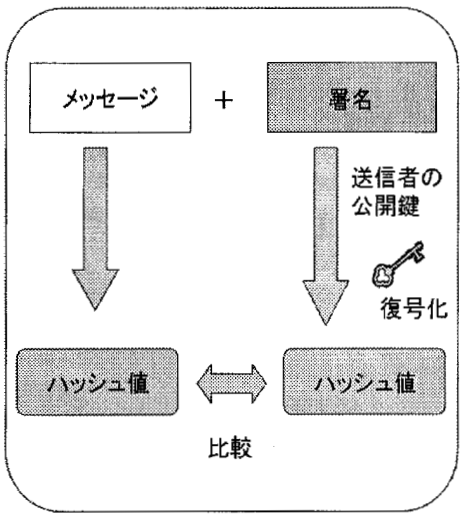

図５　署名検証

５．　おわりに

５．１　考察

本システムでは、公開鍵暗号をソフトウェアで独自実装することにより携帯会社に依存しない署名メールの送信が可能となる。また、本システムでは、携帯電話を用い、秘密鍵を携帯端末内で管理することで第三者からの不正アクセスを防止できる。また、その秘密鍵を利用してメールに署名をつけることでなりすましや、改竄、否認を防止することができ、パソコン内での鍵管理を行なったメールシステムより信頼性の高いメールの送受信が行なえると考えられる。

本システムでは、一般的に普及している S/MIME を用いてメールに署名を添付することで、S/MIME に対応しているメーラであればパソコン上でも署名の検証を行なうことができる。
また、クリアテキスト署名を用いることにより、署名の検証はできないが、S/MIME に対応していないメーラでもメールの本文の内容をみることができる。

また、一般的に普及している携帯電話を用いることで、新たに携帯電話を買い換える必要がほとんどないため、導入時のコストの低減も期待できる。また、使用時に発生するパケット料金についても、既存の携帯電話についているメールを利用したときに発生するパケット料金とさほど変わらないと考えており、利用者による負担がそこまで大きくはならないと考えられる。

携帯電話を利用することで、ネットワーク環境が整っている場所でなければメールサーバーとの通信ができないパソコンと違い、携帯電話に入っているアプリの通信機能を用いることで、電波の届く範囲であればどこでもメールサーバーとの通信が行なえるため利便性が高いと言える。

５．２　今後の展望

本システムでは、NTTDocomo の i アプリに対応している Doja-4.1 を用いて実装を行なっており、まだ実際に携帯電話を用いた評価をまだ行なっていない。今後、実際に携帯電話のアプリを９０２シリーズ全機種および１１月に発売された９０３シリーズにおいて、実装・評価を行なっていく予定である。

また、現状のシステムの実装は、NTTDocomo の携帯電話の実装であるため、Softbank や au などの他の携帯会社の携帯電話でも同様のシステムの実現が可能であり、今後、実装開発を行なっていくことも検討している。

６．　参考文献

[1]PKI 関連技術解説
http://www.ipa.go.jp/security/pki/index.html
[2] HDE Signed Mail Gateway
http://www.hde.co.jp/smgw/
[3]PKI 構築サービスと PKI カードシステム TARGUSYS
http://www.gigabeat.net/tech/review/2001/07/56_07pdf/a10.pdf
[4]ＮＴＴＤｏｃｏｍｏ
http://www.nttdocomo.co.jp/service/other/firstpass/index.html
[5]ＫＤＤＩ
http://www.kddi.com/corporate/news_release/2005/0713/besshi.html
[6]尾崎 啓、宇田 隆哉、棟上 昭男
“ 公開鍵暗号による携帯電話を用いた相互認証システム”
情報処理学会 コンピュータセキュリティシンポジウム 2005 p.535-540(2005)
[7]琴浦 崇　宇田 隆哉　星 徹 松下 温
“ 携帯電話を用いた出席率を向上させる出席管理システム”
情報処理学会 DICOMO2006　p.535-884(2006)
[8]Dianna Mullet , Kevin Mullet 著 株式会社オレンジソフト　監訳 木田　直子 訳 “IMAP”
オライリー・ジャパン発行