5T−3

零知識証明を利用した検印付き電子メールシステム

岡本 隆司, 小林 信博, 桜井 幸一

三菱電機 (株) 情報電子研究所

1 はじめに

近年、エンジニアリングワークステーションの急速な発展とともに、電子メールシステムの利用がますます盛んになってきている。特に、電子メールの高速性や、受信者の時間を拘束しない点などで、ビジネス社会での重要性が増すようになり、文書に替わる高速伝達手段として、企業内でも盛んに利用され始めている。しかしながら、従来の日本国内のビジネス書類では必ず利用されている印鑑が利用できないため、重要な意味をもつ文章などにはあまり適用されていないのが現状であった。そこで今回、暗号技術の 1 つである零知識証明技術を用いて、UNIX[1] ワークステーション上で、従来の印鑑の役目を果たす、検印 (署名) 付きの電子メールシステムを実現したので報告する。

2 開発方針

検印つき UNIX 電子メールを開発するに当たって、以下の開発方針を設定した。

(1) 社内で運用している従来の UNIX メール方式と互換性を保つこと。具体的には、受/発信マシンの検印システムのサポートの有無に係わらず、メール文章自体の配送には影響がないこと。

(2) メールに付随する、検印に関連する情報量を可能な限り減らし、ネットワークへの影響を及ぼさないこと。

(3) 暗号処理部の負荷を実運用できるレベルまで減少させるよう配慮すること。

(4) ワークステーション画面上に、実際の検印を表示できるユーザインタフェースを採用すること。

以上の方針のもとで、メールを配送中に悪者が文章を改ざんした場合、受信者が判別できるシステムを構築した。

3 実現方法

3.1 零知識証明の利用

今回は、Fiat-Shamir のデジタル署名を用いて、UNIX 電子メールにおける署名の作成、検証を実現し、電子メール文章の改ざんを防止している。システムの実現手法を以下に示す。

(1) システム管理者による、ユーザの秘密鍵の生成
公開情報であるユーザのメールアドレス (ID_A) から秘密鍵 (s_A) を作成する。

ID_A ——————→ s_A

(2) 秘密鍵のユーザへの配送

C ——s_A——→ A

(3) 電子メールによる署名

- 送信者の署名生成
  Sign(A,M) = f(M, s_A)
  署名計算量を削減するためハッシュ関数を用い、メール文章と秘密鍵から署名を作成する。

  A ——(M, Sign)——→ B

- 受信者の署名検証
  メール文章 (M) と署名 sign(M) を受け取った受信者は、送信者の公開情報 (ID_A) で署名の正当性を確認する。
  Verif(M, sign(M), ID_A) = Correct or False?

3.2 検印メールの構成

表 1 に示すとおり、通常のヘッダに加え、署名部分を X ヘッダとして、メールヘッダ部に追加している。

表 1: メールの構成

To: postmaster@ecs.isl.melco.co.jp cc: root@ecs.isl.melco.co.jp Subject: IPSJ'92	通常ヘッダ部分
X-Zkip: MMOIAJ2NLQHIH[8[2/N(WSO21 2l:wEyrDp*I—B1h)D)=ve+zbUpA'4J932;	署名部分
こんにちわ これはテスト文章です。 : : さようなら	メール文章

An Electric Mail System using Zero-Knowledge Interactive Proof Technologies
Takashi OKAMOTO,Nobuhiro KOBAYASHI,Kouichi SAKURAI
Mitsubishi Electric Corp.

[1] UNIX オペレーティングシステムは、UNIX システムラボラトリーズ社が開発し、ライセンスしています。

署名は、メール発信の際に uuencode を用いて ASCII コードにエンコードしており、受信の際に、ヘッダ部から署名を取り出し、uudecode でデコードして検証に用いている。署名のサイズは、約１５０ byte、エンコードしても約２００バイト程度で、通常メールに対し、３行程度の追加で収まっている。

4 システム構成

システム構成を、図１に示す。初期データ設定システムの他、メール受発信、到着メール表示機能を兼ねた検印表示システム、鍵データベースから構成される。

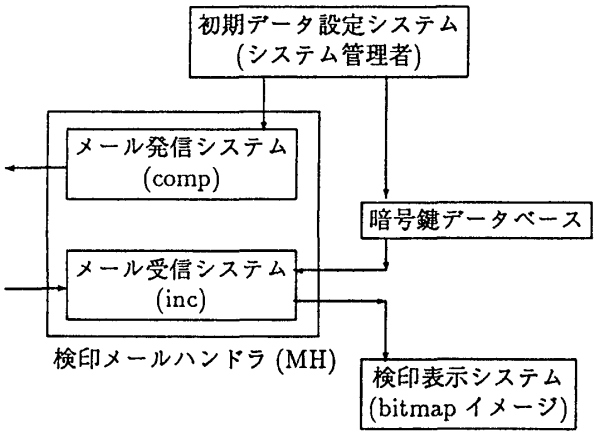

図 1: システム構成

4.1 メールシステム

従来との互換性を保つため、UNIX で一般的なメールハンドラである MH に対して改良を加えた。具体的には以下の MH コマンドに対して検印部分をインプリメントしている。

- comp：検印メールの作成・発信。
- inc ：検印メールの受信・検証。

4.2 検印表示システム

受信側で、メール到着と同時に、検印付きメールかどうかを調べ、検印付きメールの場合は、Xウインドウ上に印鑑を表示するシステムである。また、メール到着を通知する機能も兼ねている。実際には、印鑑の bitmap イメージを UNIX の xbm イメージファイルに納めて表示している。

4.3 データベース部

検印システムで利用する、ユーザ固有の情報を納めている部分である。システム管理者により生成される秘密情報、メール受信者が参照する発信者の公開情報からなる。公開情報は、メールアドレスから生成されており、メールを受信した際、発信者のメールアドレスを参照して、公開鍵サーバーマシンにデータアクセスされる。

5 考察

一般の UNIX 電子メールでは、メール配送マシンの特権ユーザならば、幾らでも文章の改ざんが容易であるが、本システムにおいては、メール配送途中で、悪者がメール文章を１字でも変更した場合、到着時にすぐに判別することが可能である。従って、経理文章や人事情報等のような重要の書類も電子メールで送付できる可能性を示した。また、ユーザインタフェースに従来と同等な視覚的な検印を表示することにより、使用者の心理的な配慮も行なっている。また、検印の必要のない一般ユーザも、検印システムを意識することなく、従来システムと同様な使用が可能である。

6 おわりに

本稿では、零知識証明技術の UNIX 電子メールシステムへの実現と、そのシステム構成について述べた。現システムでは、署名者は１人署名で多重署名には対応していないが、今後、多重署名や鍵配送や親展機能などを追加・改良することにより、全社メールへの展開をはかっていきたい。

参考文献

[1] Goldwasser, S.,Micali,S. and Rackoff,C."The Knowledge Complexity of Interactive Proof Systems", Proc. of STOC'85, pp.291-304(1985)

[2] 小山, " ゼロ知識対話証明の原理と課題 ", 情報処理, 1991.6, pp.643-653

[3] 太田, 藤岡 " ゼロ知識証明の応用 ", 情報処理, 1991.6, pp.654-662

[4] 辻井, 笠原, " 暗号と情報セキュリティ ", 昭晃堂

[5] RFC-822,STANDARD FOR THE FORMAT OF ARPA INTERNET TEXT MESSAGES