検印付き電子メールによる回覧システム

小林　信博 , 岡本　隆司 , 桜井　幸一, 冨樫　昌孝, 佐伯　保晴, 伊串　亮二

3N−5

三菱電機 (株)

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発展とともに、電子メールシステムが、その高速性や受信者の時間を拘束しない点などで、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、日本国内のビジネス文書には必須である印鑑が利用できず、現状では重要な文書には余り適用されていない。この問題を解決するため、我々は「零知識証明技術を利用した検印付き電子メールシステム」[1] を提案し、電子メールへの検印を開発したが、今回は更にビジネス文書の大半を占める複数名による検印と、コメント文章の追加が可能な回覧を、ＵＮＩＸ[1]システム上で「検印付き電子メールによる回覧システム」として開発したので報告する。

2　開発方針

検印付き電子メールによる回覧システムを開発するに当たって、以下の方針を設定した。

1. 多重検印
   既に検印の付いているメール文章に対して、更に検印することを可能にする。また、前の文章に対するコメント文章の追加も可能にする。そして、前の文書及び追加したコメント文章それぞれについて、検印の検証を可能にする。
2. 回覧
   回覧の開始者が指定した回覧経路にそって、電子メールが配送されるようにする。また、回覧中は次の回覧先の宛先が自動的に設定されて送信されるようにする。
3. 検印可変情報
   検印ごとに変化する検印日及び検印時刻などの情報をメール本文を変更することなく追加するとともに、検証及び参照を可能にする。

以上の方針のもとで、電子メールを回覧中に悪者が文章を改ざんした場合に受信者が判別できる回覧システムを開発した。

3　実現方法

3.1　デジタル署名

検印付き電子メールでは、デジタル署名 [2] により検印を実現しており、暗号方式には公開鍵暗号方式の一つである零知識証明 [3] を用いている。システムの実現手法を以下に示す。

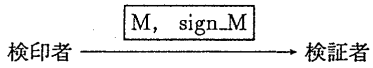
1. 検印者の公開鍵の作成
   検印者は、任意の秘密鍵 (sk_u) から公開鍵 (pk_u) を作成し、公開する。

$$f\_pk\ (\mathrm{sk\_u}) = \mathrm{pk\_u}$$

2. 検印者の検印情報の生成
   検印者は、秘密鍵 (sk_u) でメール文章 (M) から検印情報 (sign_M) を生成する。

$$f\_sign\ (\mathrm{sk\_u},\ \mathrm{M}) = \mathrm{sign\_M}$$

3. 検印付きメールの送信
   検印者は、メール文章 (M) と検印情報 (sign_M) を検証者に送る。



4. 検証者のメールの検証
   メール文章 (M) と検印情報 (sign_M) を受け取った検証者は、検印者の公開鍵 (pk_u) を用いて、メールの検証を行なう。

$$f\_verif\ (\mathrm{M},\ \mathrm{sign\_M},\ \mathrm{pk\_u}) = \mathrm{OK} / \mathrm{NG}$$

3.2　多重検印

多重検印を行なう場合、メールの文章と検印情報を各回覧者ごとに独立して保管すると、後から追加したコメント文章が、どの文章を参照して作成されたものなのか判断できない。従って、前の文章が変更されると、後から追加したコメント文章の意図した内容がすり替えられる恐れがある。そこで多重検印時は、参照した前の文章と追加したコメント文章を合成したものを検印対象文章とし、新たな検印情報を作成する。

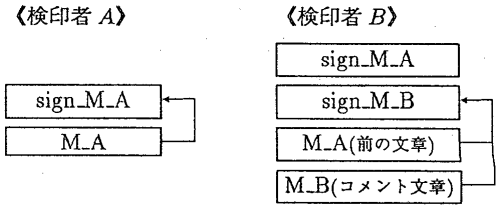


図 1 ：多重検印

A Circulation System using degital signed Electronic Mail
Nobuhiro KOBAYASHI, Takashi OKAMOTO, Kouichi SAKURAI, Masataka TOGASHI, Yasuharu SAEKI, Ryouzi IGUSHI
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。

また、検証時は検印時と同様に参照した前の文章と追加したコメント文章を合成したものを検証対象文章として改ざんの判別を行なう。以上の方式により、検印後に前の文章が変更されても判別可能な多重検印を実現した。

3.3 回覧

回覧の開始者は、回覧先のメールアドレスを回覧情報として列挙することにより回覧経路を指定する。この回覧情報と、回覧の開始者から数えて何人回覧したかを示す回覧済み人数はメールのヘッダ部分に格納する。回覧中は、このヘッダ情報から回覧状況を判断するとともに、次の回覧先のメールアドレスを自動的に宛先に設定して送信する。以上の方式により回覧機能を実現した。

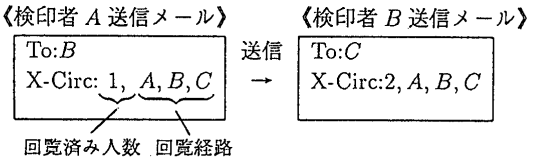


図2：回覧

3.4 検印可変情報

検印可変情報とは、検印時ごとに変化する情報のことで、検印日や検印時刻などである。この検印可変情報は、検印情報とともにメールのヘッダ部に格納する。また、この検印可変情報と本文を用いて検印情報を作成する。検証時はメールのヘッダ部より検印可変情報を取り出し、検印情報を用いて改ざんの判別を行なう。以上の方式により、本文を変更することなく検印可変情報を追加し、メール本文と同様な悪者による改ざんの判別を可能にした。

3.5 電子メールの構成

表1に示す通り、通常のヘッダに加え検印者名、検印可変情報及び検印情報を RFC822[4] に基づいた拡張ヘッダとしてメールヘッダ部に追加した。また、回覧情報も同様に追加した。

表1：メールの構成

To: masterpost@melco.co.jp	←宛先
X-Sign: root@melco.co.jp,1992.08.19, 15:30,MVD83H08+GY;k34!V4SDZ-S0S.C4P.	┐検印情報
X-Sign: manager@melco.co.jp,1992.08.20, 10:15,MAWI*:V>8A43934:V4HIZI00*@56.E	┐検印情報
X-Circ: 2,root@melco.co.jp, manager@melco.co.jp, masterpost@melco.co.jp	┐回覧情報
検印付き電子メールによる回覧システムのテストです。 root	┐メール文章
検印・回覧をしました。 manager	←コメント

4 システム構成

システム構成を図3に示す。本システムは、システム利用開始時に公開鍵を公開鍵データベースに登録する公開鍵登録システムの他、検印作成部、メール発信部、メール受信部、検証部、及び回覧処理部を含む検印回覧メールハンドラから構成される。

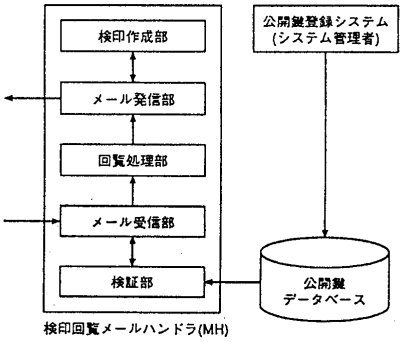


図3：システム構成

5 考察

本システムでは、複数名による検印と、コメント文章の追加が可能な回覧を提案しこれを開発した。この結果、電子メールの回覧中に悪者が改ざんを行なった場合に、その判別が可能である。また、最初の送信者が回覧先を指定することが可能であり、回覧中は自動的に次の宛先が設定されるので目的とした経路にそったスムーズな回覧処理が行なわれる。さらに、検印日や検印時刻などの検印可変情報を設定することが可能で、この検印情報についても改ざんの判別が可能である。以上のように本システムによって、安全性の高い検印付き電子メールによる回覧が可能となった。

6 おわりに

本稿では、検印付き電子メールによる回覧システムの実現と、そのシステム構成について述べた。現在のシステムでは、回覧機能として簡単な経路しかサポートしていないが、今後はより複雑な回覧経路への対応を考えていきたい。また、親展機能などを追加することにより更に機能を強化し、幅広い分野への展開をはかっていきたい。

参考文献

[1] 岡本，小林，桜井，”零知識証明を利用した検印付き電子メールシステム”，情報処理学会第44回（平成4年前期）全国大会

[2] 辻井，笠原，”暗号と情報セキュリティ”，昭晃堂，(1990)

[3] 太田，藤岡，”ゼロ知識証明の応用”，情報処理第32巻第6号，pp654-662，(1991)

[4] David H.Crocker，” RFC822「STANDARD FOR THE FORMAT OF ARPA INTERNET TEXT MESSAGES」”，(1982)