# 暗号メールにおける個人情報不正送出チェックシステムの評価

安 健司[†1] 赤羽泰彦[†2] 尾崎将巳[†3]
瀬本浩治[†4] 佐々木良一[†1]

近年，顧客情報などの個人情報が漏洩する事件が起き，その保護対策が重要になってきている．個人情報漏洩の防止対策として，メール監査ソフトを導入する企業が増えつつある．しかし，メールが暗号化されていると，内容をチェックできないという問題がある．著者らは，この問題を解決するために，メールサーバでチェック可能な方式を考案した．その方式を実装し，個人情報を検出する実験を行い基本的な有効性の確認を行った．本稿では，その方式について説明し，実験結果について述べる．

# Evaluation of Check System for Improper Sending of Personal Information in Encrypted Mail System

Kenji Yasu,[†1] Yasuhiko Akahane,[†2] Masami Ozaki,[†3]
Koji Semoto[†4] and Ryoichi Sasaki[†1]

There have been cases, in recent years, where customer information or other personal information has been leaked, and protective measures for personal information have become important. Corporations and other organizations have increasingly adopted software with e-mail monitoring capability to prevent leakage of personal information to the outside through e-mail. However, if the e-mail is encrypted, it is completely impossible to check whether personal information is being improperly sent. The authors have designed and implemented a system for solving such problems. Experiments to detect personal information were conducted using the implemented system, and we were able to confirm the basic effectiveness of the system. This paper reports on those results.

## 1. はじめに

インターネットの普及により，e-コマースなどの様々なオンラインサービスが，提供され利用されている．一方で，顧客情報や社員情報などの漏洩問題が深刻化し，個人情報の保護対策が重要になってきている．NPO 日本ネットワークセキュリティ協会の調査[1)] によると，2003 年に起きた個人情報漏洩事件は，報道されたものだけでも 57 件にのぼり，漏洩した個人情報には「氏名」，「住所」，「電話番号」が高い確率で含まれていた．また，漏洩経路についても「E-mail 経由」，「Web 経由」による漏洩も多いと報告している．

一方，メールの機密を第三者から守るため S/MIME などを使った暗号化メールも普及しつつある．しかし，暗号化メールを許すと個人情報の漏洩が，管理者にチェックできないという問題も生じる．それにもかかわらず従来は，暗号化メールにおける個人情報のチェックの検討は行われてこなかった．

そこで著者らは，暗号化メールにおける個人情報のチェック手段の検討を行い，次の 2 つのケースに対応できる方式の開発を行った[2)~4)]．

**(1) 暗号化メールとして広く用いられている S/MIME 方式に対応**

この相反する要求を解決するために，暗号化メールとして広く用いられている S/MIME 方式を改良することで解決を図った．

従来の S/MIME 方式では，Alice から Bob へ暗号化メールを送信した場合，Bob のみが暗号化メールを復号化できるが，途中のメールサーバでは復号化できない．そこで，メールサーバ上に搭載したチェックシステムで，復号化できるように拡張した S/MIME 方式の考案を行った．

なお，拡張した S/MIME 方式で作成したデータの

†1 東京電機大学
Tokyo Denki University
†2 株式会社日本システムデベロップメント
Nippon System Development Co., Ltd.
†3 日立インフォネット株式会社
Hitachi Infonet Co., Ltd.
†4 ダイヤモンドコンピュータサービス株式会社
Diamond Computer Service Co., Ltd.

拡張部分をメールサーバから送信先に発信する前に削除することで，従来の S/MIME 方式の形式に戻すことができる．したがって，暗号化メールの受信側では，拡張した S/MIME に対応した特別なメールソフトが必要なく，従来の S/MIME に対応したメールソフトで受信することができる特長を持つ．

**(2) 個人情報のチェックを回避する不正対策**

個人情報の不正送出チェックシステムでは，メールサーバ上で平文に戻された後，パターンマッチを用いて個人情報のチェックを行う．しかし，個人情報のチェックは，平文に対してのみ有効で，個人情報のチェックを回避する不正者によって，メール本文や添付ファイルを S/MIME による暗号化以外にさらに何らかの方式で暗号化し，チェックを回避可能にするという問題が考えられる．

個人情報のチェックシステム自体は，すでに発売されている[5] が，従来このような問題に対する検討は行われてこなかった．

著者らの方式は，このような場合についても対応可能な方式の実現を目指すものである．

2 章で考案したチェックシステムとチェックの考え方を述べるとともに，各チェック方式の説明を行う．3 章では，2 章で考案したチェックシステムの実装について述べ，4 章で実装したチェックシステムを使用し，各チェック方式の有効性を検証する検証実験を行った結果について述べる．5 章では，本稿をまとめるとともに，今後の課題と展開について述べる．

## 2. システムの構成と機能

### 2.1 システムの構成

本稿で想定しているネットワーク構成は，**図 1** に示すとおりである．企業内において社員 Alice およびその他複数の社員とその上長がいると想定している．

ここで，Alice はメールサーバ T を経由して Bob にメールを送信するものとする．

メールサーバに搭載されたチェックシステムは，**図 2** に示すとおり個人情報の不正送出が疑われるメールを発見した場合，上長に送り判断を仰ぐ．上長はそのメール内容が個人情報の不正送出にあたるかを確認し，外部送信の可否を決定する．ここで，上長は部下を監督する立場にあるとし，不正をしないものとする．

加えて，後述するチェックシステムにより，不正送出の疑いが持たれるメールだけを選び出し，最終判断のみを上長に委任することで上長への負担を軽減することができる．

ここで，Alice と Bob の間は，暗号化メールのやりとりができるものとし，一般的に普及しつつある S/MIME に対応したチェック方式を使っているものとする．従来の S/MIME の暗号化メール形式は，**表 1** の上部に示した従来方式である．

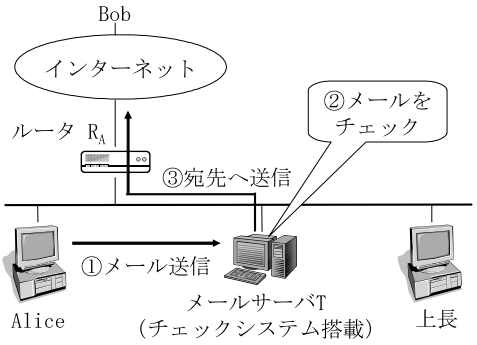



**図 1** ネットワーク構成
Fig. 1 Network composition.

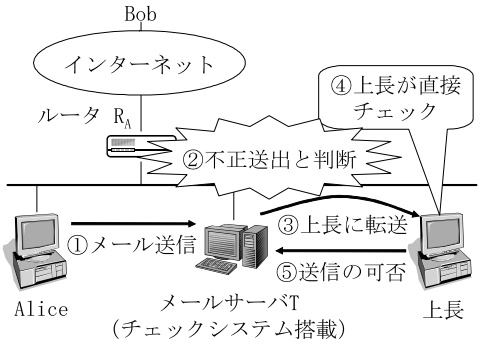



**図 2** 不正送出発見時の流れ
Fig. 2 Flow at time of unjust sending discovery.

**表 1** 暗号化メール形式
Table 1 Encrypted mail form.

| | |
|---|---|
| 従来方式 | $P_B(K)$, $K(M)$ |
| 考案方式 | $P_B(K)$, $K(M)$, $P_T(K)$ |

ここで，

$P_B$ ： Bob の公開鍵
$P_T$ ： メールサーバ T の公開鍵
$K$ ： 共通鍵
$M$ ： メールメッセージ

とする．この暗号化メール形式では，基本的に受信者しか復号化することができないため，メールサーバでメールをチェックすることが困難である．そこで，著者らは，従来の暗号化メール形式にメールサーバの公開鍵 $P_T$ で，データ暗号用の共通鍵 $K$ を暗号化したものを追加し，表 1 の考案方式にすることで問題の解決を図った．

すなわち，流れは以下のとおりである．

(1) Alice が暗号化メールを送る．
(2) メールサーバ上で秘密鍵 $S_T$ を用いて $P_T(K)$ を復号する．
(3) 得られた共通鍵 $K$ を用いて $K(M)$ を復号化し，メッセージ $M$ を求める．

このようにして，復号化したメールメッセージは，2.2 節で述べるメールのチェックが完了後に問題がなければ消去し，復号化する前の暗号化メールから，$P_T(K)$ の部分を取り外したのち，表 1 の従来方式と同じようにして送信する．ただし，チェックシステムが，不正送出のメールを上長へ送る場合，上長の公開鍵で共通鍵 $K$ を暗号化したものを追加してから送る．

メールサーバ内でしか平文が現れないので，通常考えられる送信者のところでは暗号化せず平文のまま送り出し，サーバでチェック後，サーバから送り出すところではじめて暗号化する方式に比べ，安全性が高い．また，チェック済みのメールを外部に送り出すときに，$P_T(K)$ を削除することで従来の S/MIME の暗号化メール形式と同じになり，受信者は従来どおりの S/MIME に対応したメーラを使用することができる．

クライアント側については，メールソフトの機能を拡張するプラグインを導入する手間が必要である．しかし，暗号化メールを送信する場合については，メールソフト側で自動的にメールサーバ T の公開鍵 $P_T$ を付加して送信するため，負担はほとんどないといえる．

### 2.2 メールサーバでの処理フロー

メールサーバ上に搭載したチェックシステムで，個人情報の検出を行い不正送出にあたるかどうかを判断する．正当なユーザは，通常の S/MIME 方式で正当な暗号化メールを送信すると考えられる．しかし，メールが逐一チェックされていることを知っていて，しかも，メールで個人情報を不正に持ち出そうとしたとき，すべて平文のまま送るとは考えにくい．すなわち，通常の S/MIME 方式で暗号化する前に何らかの手法で，メール本文や添付ファイルに独自の暗号をかける不正な暗号化をしたうえで，外部へ持ち出そうとする可能性があると考えられる．

著者らは，暗号手法を大きく 2 つに分けられると考え，乱数性を持つ強い暗号と，乱数性を持たない弱い暗号に分けた．これら 2 つの暗号手法に対しては，それぞれの特性に適したチェック方法を適用すべきと考えた．したがって，個人情報のチェックを行う前に，不正な暗号化メールを検出する目的で，次のチェックを行う．

(1) 強暗号チェック
強い暗号で暗号化されたメールをチェックする．

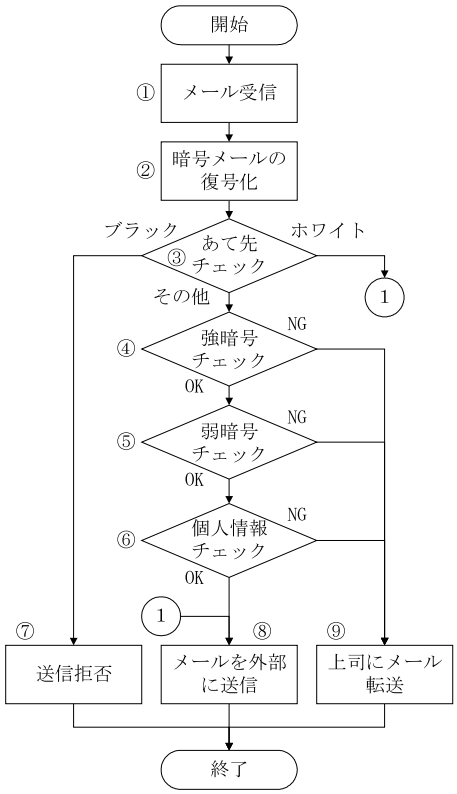



**図 3** メールサーバでの処理フロー
Fig. 3 Processing flow in mail server.

(2) 弱暗号チェック
弱い暗号で暗号化されたメールをチェックする．

この 2 つのチェックを導入することにより，大部分の不正な暗号化メールに対処することが可能と考えた．また，これら 2 つのチェックにおいて，暗号がかかっていると判断された場合は，外部に送信せずに上長に送り，上長の判断や社内のポリシに基づいて対処を行うものとする．

また，これらの事前処理として，チェックすべきメールを減らすため，あて先チェックを行うことにした．あて先チェックでは，あて先を見て送信が禁止されているか（ブラック）チェックが不要なあて先か（ホワイト）をチェックする．これらに該当しないメールについて，個人情報チェックを行い OK の場合に正当なメールであると判断し外部へ送信する．

以上の考えに基づいたチェックシステムによるメールチェック処理の流れを**図 3** に示す．個人情報のチェックは，図 3 の「個人情報チェック」部で行う．「個人情報チェック」部を含む計 4 つのチェック部については，2.3 節で詳しく説明する．

### 2.3 各チェック方式

前節では，チェックシステムのチェックの考え方と，処理フローについて述べた．本節は，図 3 に示す ③〜⑥ のチェック方式について詳しく述べる．

**1) あて先チェック**

あらかじめメール送信を禁止したブラックリストと，メールのチェックが不要なホワイトリストを作成し，あて先チェック時にこれらのリストに該当するかを確認する．いずれかのリストに該当すれば「ホワイト」または「ブラック」，該当しなければ「その他」となる．その後の処理の流れは，図 3 に示すとおりである．

**2) 強暗号チェック**

先にも述べたように，電子メールは，通常 S/MIME によって暗号化されるが，意図的に S/MIME 以外の方式で事前にデータが暗号化されると，個人情報のチェックができない．ただし，強い暗号で平文を暗号化すると，その暗号文はランダム化され乱数性を持つようになる．そこで，その特性を利用し，乱数であるかどうかで暗号文の判定を行う．

乱数の判定法については，連の検定，線形複雑度検定，累積和検定の 3 つの乱数検定方式を利用する[6),7)]．また，暗号文の検出精度を向上させるため，これら 3 つの検定方式を併用した強暗号チェックを行うこととした．これらの検定を行うとその結果として $P$ 値が得られ，しきい値と比較して暗号文であるかを判定する．

**3) 弱暗号チェック**

強暗号チェックにより，AES や Triple DES などの強い暗号を用いた暗号手法について対策を行った．しかし，換字暗号などのような弱い暗号を用いた暗号手法に対しては，ランダムにならないので無力である．そこで，文字頻度を基に本来あまり出現しない文字が多く出現したり，多く出現する文字が少なかったりした場合，弱い暗号による暗号文ではないかと考えるチェック方式を考案した．ここでは，文字以外に，主な単語もチェックすることとした．これにより，強暗号チェックでは，検出できない弱い暗号を用いた暗号手法の検出が可能な見通しを得た．

ただし，その方式の開発と実験による有効性の確認は，今後の課題である．

**4) 個人情報チェック**

1 章で述べたが漏洩した個人情報には，住所，電話番号，メールアドレスが高い確率で含まれる．そこで，著者らは，これらの情報が含まれていないか検出することで個人情報のチェックを行う．

個人情報の検出には，パターンマッチ[8)] を用いてデータの中から個人情報を抽出し，それぞれの出現個数を求める．いずれか 1 つの出現個数が 10 個以上ならば，個人情報が含まれる可能があると判断する．個人情報の判定基準を 10 個以上とした理由は，自分が受信した過去メールのうち実験に使用していない返信メールを調査し決定した．

**表 2** 正規表現を用いたキーワード
Table 2 Keyword using regular expression.

| | |
|---|---|
| 住所 | (¥w+(市\|区\|町\|村\|郡))+(¥w\| \| )*?¥d |
| 電話 | [¥( (]{0,1}[0 0 ]¥d{1,5}[¥- - - -] (¥)¥(]¥d{1,4}[¥- - - -] ¥)])¥d{4} |
| メール | [0-9a-zA-Z_¥-¥.]+@[0-9a-zA-Z_¥-¥.]+ |

**表 2** に各個人情報を抽出するキーワードを示した．各個人情報は，次の特徴を持っていることが一般的にいえる．

イ） 住所
「都道府県」，「市区町村」の地域名と丁目などの数字で記述される．郵便番号の併記などで「都道府県」が，省略される場合があるが他は必ず含まれる．

ロ） 電話番号
国内電話であれば必ず「0」から始まる．一般的には，市内外局番や加入者番号などをハイフンの文字で区切って記述する．

ハ） メールアドレス
アカウント名とドメイン名を「@」で区切り半角文字で記述する．

上記の特徴を正規表現で記述し，各個人情報を検出するためのキーワードとした．

## 3. 実　　装

著者らは，(1) メールサーバ上に実装する個人情報の不正送出チェックを行うメールチェックプログラムと，(2) 従来のメーラで表 1 の考案方式の暗号化メールを送信可能にするプラグインの開発を行った．

ただし，本来 S/MIME 対応のソフトの暗号化方式を $P_T(K)$ などが付け加えられるように修正すべきであるが，簡単に修正を行うことができる S/MIME 対応のソフトが手に入らなかったので，MIME 方式のソフトをベースに必要最低限の機能を追加することで，表 1 の考案方式に対応した実装を行っている．

2.3 節でも述べたが，弱暗号チェックについては現在方式の開発途上であるため，(1) のメールチェックプログラムの処理フローである図 3 の ⑤「弱暗号チェック」部の実装を行っていない．その他の処理機能はすべて実装している．

**表 3** 開発環境
Table 3 Development environment.

| | |
|---|---|
| OS | Windows XP |
| 開発言語 | Microsoft Visual C++ 6.0 |

メールサーバについては，Windows 上で動作する XMail を採用し，そのソフトが持つメールフィルタリング機能を利用して，メールチェックプログラムを実装した．プログラムのステップ数は，約 3,000 ステップである．開発環境を**表 3** に示す．

また，クライアントについては，プラグインで機能拡張ができる AL-Mail32 を採用した．しかし，標準では暗号化メールをサポートしていないため，メールサーバの公開鍵 $P_T$ を自動的に付加する機能を含む，暗号化メールの送受信を可能にするプラグインの開発を行い実装した．プログラムのステップ数は，約 2,800 ステップである．

## 4. 評　　価

### 4.1 強暗号チェック

考案した強暗号検査方式の有効性を検証するために実験を行った．2.3 節で述べたが，強暗号チェックでは，3 つの検定方式[6),7)] を併用して暗号文の検出を行うことにより，検出精度を向上させている．

各検定方式からは，分析結果として $P$ 値が得られ，あらかじめ設定してあるしきい値 (0.001) と比較して，その値が大きければ暗号文とする．しかし，複数の検定方式を使用するとどの $P$ 値を評価すべきかが問題となる．そこで，3 つの検定方式から得られる $P$ 値の評価方法を 2 つ考案した．

a) 最小値評価法
　各検定方式から得られる $P$ 値のうち，最小の値を用いて評価する方法．
b) 最大値評価法
　a) とは逆に最大値を評価する方法．

最小値評価法と最大値評価法の検出精度を適切に評価するため，式 (1) で定義される適合率，式 (2) で定義される再現率を用いて検出精度の比較を行う．適合率は，検出結果中に含まれる正解の割合を示し，再現率は，検出結果の正解がすべての正解に占める割合を示す指標である．

$$\text{適合率} = \frac{\text{正検出}}{\text{正検出+誤検出}} \quad (1)$$

$$\text{再現率} = \frac{\text{正検出}}{\text{正検出+検出漏れ}} \quad (2)$$

ここで，式 (1) と式 (2) で用いられている正検出，誤検出，検出漏れを次のとおりに定義する．

(1) 正検出
　暗号文を「暗号文である」と判定した場合
　平文を「暗号文ではない」と判定した場合
(2) 誤検出
　平文を「暗号文である」と判定した場合
(3) 検出漏れ
　暗号文を「暗号文ではない」と判定した場合

(1) に平文を「暗号文ではない」と判定した場合が含まれているのは，ある平文をチェックしたときに「暗号文ではない」と判定をしたとすると，暗号文ではない平文として検出したと考えることができる．よって，平文が「暗号文ではない」と判定された場合についても正検出と定義できる．

また，(3) は，暗号文を「暗号文ではない」と判定したために，検出すべき暗号文を見逃したと考えることで検出漏れと定義する．

評価指標を定義したところで，a)，b) の方式のうちどちらが最も良いかを評価するために実験を行った．実験に用いたデータは，著者が受信した過去のメールからランダムに選択した 60 件を用い，その本文を抽出して平文とした．また，暗号文は，平文を Triple DES で暗号化したものを用いた．**図 4** と**図 5** の太い点線は，しきい値を示す．

図 4 の最小値評価法では，平文は「暗号文ではな

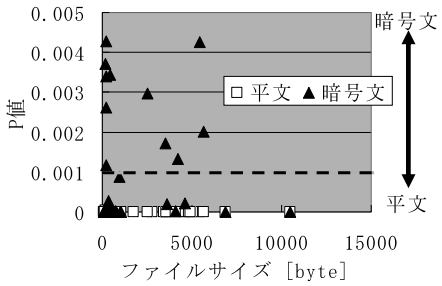



**図 4** 最小値評価法
Fig. 4 Minimum value appraisal method.

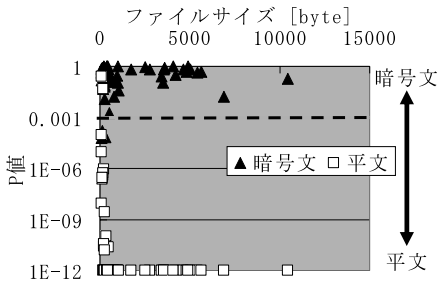



**図 5** 最大値評価法
Fig. 5 Maximum value appraisal method.

い」と正しく判定されているが，多くの暗号文が「暗号文ではない」として正しく検出できていないことが分かる．他方，図 5 の最大値評価法では，いくつか平文を「暗号文である」と判定する誤検出があるが，暗号文と平文を適切に判定できたことが読み取れる．

最大値評価法と最小値評価法の評価を行うために，それぞれの適合率と再現率を求め**表 4** に示す．本研究は，1 章で述べたように個人情報が，外部に不正に送信されるのを防止するのが目的である．よって，暗号化された個人情報が，外部へ不正に送信される最悪のケースの発生を最小限にするため，強暗号チェックでは，適合率が多少低くなってでも再現率を高め，検出漏れを最小にする必要がある．

表 4 から 2 つの評価法を比較すると，適合率がやや低くなるものの再現率が，97.5%と最も高い最大値評価法が優れているといえる．よって，最大値評価法を用いるのが最も良いと結論づけた．

また，最大値評価法において，2.5%の検出漏れがあるが，これらのデータサイズは 300 バイト以下の小さなもので，一度に持ち出せる個人情報は少量と考えられる．したがって，数値以上に安全性が高いといえる．

### 4.2 個人情報チェック

2.3 節で述べた検出方式で，住所，電話番号，メールアドレスをそれぞれ検出して，式 (1) と式 (2) に示した適合率と再現率を求めることで性能評価を行う．実験データには，個人情報が多く含まれている名簿形式のファイルデータ 4 件を用いた．また，本実験における正検出，誤検出，検出漏れを次のとおり定義する．

(1) 正検出
パターンマッチングにより，検出すべき正しい情報を検出した場合

(2) 誤検出
パターンマッチングにより，検出すべきではない誤った情報を検出した場合

(3) 検出漏れ
検出すべき正しい情報であるが，パターンマッチングで検出することができなかった場合

個人情報の検出では，誤検出が多すぎると無関係な正規の電子メールを誤って不正送出と判断してしまう．すると，上長がチェックすべき電子メールが増加し，負担を軽減するという目的に反する恐れがある．また，検出漏れが多すぎると，検出すべき不正送出の電子メールを検出できない見逃しが増加し，不正送出のチェックが適切にできなくなる恐れがある．

**表 5** の実験結果では，適合率と再現率の平均がそれぞれ 95%以上とかなり高い結果となった．ただし，電話番号が他の再現率の平均と比べ 10 ポイントほど低かった．特に低かった C と D のデータを分析したところ，ハイフン記号で区切らずに数字のみで記述されていたことが原因であった．この対策として，0 から始まる 10 桁と 11 桁の数字も検出できるようにキーワードを改良した．その結果，適合率の平均が 1 ポイント下がったが，再現率の平均を 97%まで高めることができた．

個人情報の検出実験を行った結果，適合率，再現率がともに高い結果を得ることができ，考案した方式の有効性を示すことできた．

### 4.3 全体システムの機能評価

次に稼働しているシステムでメールにおける個人情報検出の評価実験を行った．

この実験には，前述の 2 つの実験で用いたデータとは別のテストデータを用いた．テストデータは，計 8 件で内 4 件が名簿データで，残り 4 件は著者が受信した過去のメールから返信メールであることを条件に

**表 4** 各評価法の誤検出率 [%]
Table 4 Rate of incorrect detection in each appraisal method.

| | 適合率 | 再現率 |
|---|---|---|
| 最小値評価法 | 100 | 70.0 |
| 最大値評価法 | 98.3 | 97.5 |

**表 5** 個人情報検出結果 [%]
Table 5 Personal information detection result.

| データ名 | 住所 | | 電話番号 | | メールアドレス | |
|---|---|---|---|---|---|---|
| | 適合率 | 再現率 | 適合率 | 再現率 | 適合率 | 再現率 |
| A | 99.5 | 99.6 | 100.0 | 95.3 | 100.0 | 99.4 |
| B | 100.0 | 100.0 | 100.0 | 100.0 | − | − |
| C | 100.0 | 99.2 | 100.0 | 80.1 | 100.0 | 98.3 |
| D | 99.0 | 99.5 | 100.0 | 79.7 | 100.0 | 98.6 |
| 平均 | 99.6 | 99.6 | 100.0 | 88.8 | 100.0 | 98.8 |

**表 6** メールの検査結果
Table 6 Inspection result of mail.

| データ名 | | 住所 | 電話 | メール | 判定 |
|---|---|---|---|---|---|
| 不正送出 | E | 41 | 44 | 6 | DENY |
| | F | 97 | 120 | 42 | DENY |
| | G | 204 | 143 | 0 | DENY |
| | H | 84 | 78 | 78 | DENY |
| 正規 | I | 0 | 0 | 8 | ALLOW |
| | J | 1 | 2 | 3 | ALLOW |
| | K | 0 | 0 | 6 | ALLOW |
| | L | 2 | 3 | 3 | ALLOW |

**表 7** 平均処理時間 [秒]
Table 7 Average processing time.

| 二重暗号検査 | 個人情報検査 | 全体 |
|---|---|---|
| 0.09 | 0.16 | 0.68 |

ランダムに選択したメールデータである．返信メールは，前の内容に追加する形で記述するため，署名などにより本文中に記述される住所やメールアドレスなどが増加する可能性があり，正規のメールと判断できるのかを確認するため実験データに用いた．

**表 6** に示す実験結果より，考案した検査方式で個人情報の不正送出の可能性があるメールと正規のメールのそれぞれの判定結果は，すべて正解であった．また，各メールの検査に要した処理時間を測定し，その平均処理時間を**表 7** に示す．

### 4.4 処理時間の評価

表 7 からメール 1 通あたりの検査の平均処理時間は，0.68 秒であった．本チェックシステムを導入していない場合と比較すると，メール 1 通あたり 0.68 秒の遅延が生じる．しかし，ある程度の遅延を許容できる電子メールの特性から考えると，大部分は問題ないと考えられる．ただし，今後，さらに高速にすることが望ましい．

## 5. おわりに

本稿では，(1) S/MIME を改良することにより，メールサーバ内で個人情報のチェックを可能にする方式を提案するとともに，(2) 具体的な個人情報流出チェック方式を提示した．あわせて，個人情報不正送出チェックシステムを完成させ，各チェック機能の評価実験を行った．個人情報チェック機能の実験では，パターンマッチを用いた個人情報の検出の有効性を示した．また，強暗号チェック機能の実験では，乱数検定法を用いた暗号文の検出の有効性を示すことができた．全体システムの機能評価では，個人情報の不正送出の可能性があるメールを適切に検出できた．処理時間の評価においては，電子メールの特性から考えて大部分は問題ないとの結果を得られた．

今後，強暗号チェックについては，Triple DES 以外の強い暗号方式を用いた検出実験を行い検出精度の評価を行う．また，弱暗号チェックに関して，次のような検討を実施していく必要がある．

(1) 弱暗号チェック方式の検討
(2) 弱暗号方式を用いた検出実験による有効性の確認

(1) の一案として，ベイズ理論を応用したスパムメールフィルタリングソフトである POPFile[9] を用いたチェック方式の検討を行っている．この POPFile は，単語の出現頻度を元にスパムメールと通常のメールを分類する方式である．POPFile を用いるチェック方式以外についても検討するとともに，有効性の確認実験を行っていきたいと考えている．

また，各チェック方式の検討とともに，処理時間の短縮を図りたいと考えている．

## 参 考 文 献


1) NPO 日本ネットワークセキュリティ協会：2003 年度情報セキュリティインシデントに関する調査報告書 (2003).
2) 安 健司，赤羽泰彦，尾崎将巳，瀬本浩治，佐々木良一：暗号メールにおける個人情報不正送出チェックシステムの評価，コンピュータセキュリティシンポジウム 2004 論文集，pp.1–6 (2004).
3) 安 健司，赤羽泰彦，佐々木良一：個人情報不正送出チェック機能を持つ暗号メールの構想と基本部の開発，コンピュータセキュリティシンポジウム 2003 論文集，pp.193–198 (2003).
4) 赤羽泰彦，安 健司，佐々木良一：暗号メールにおける機密情報不正送出チェック方式の開発，マルチメディア，分散，協調とモバイル（DICOMO 2003）シンポジウム論文集，pp.257–260 (2003).
5) キヤノンシステムソリューションズ：GUARDIAN WALL. http://www.canon-sol.co.jp/guardian/product/gw/index.html
6) NIST Special Publication 800-22: A Statistical Test Suite For Random and Pseudorandom Number Generators for Cryptographic Applications (2001).
7) 情報処理振興事業協会セキュリティセンター（IPA/ISEC），電子政府情報セキュリティ技術開発事業：擬似乱数検証ツールの調査開発調査報告書 (2003).
8) 浅野久子，加藤恒明，高木伸一郎：Signature の局所的パターンマッチによる電子メールからの送信元住所録情報抽出とそれを用いた住所録管理

システム，情報処理学会論文誌，Vol.39，No.7，pp.2196–2206 (1998).
9) POPFileDocumentationProject. http://popfile.sourceforge.net/cgi-bin/wiki.pl?JP_POPFileDocumentationProject

(平成 16 年 11 月 29 日受付)
(平成 17 年 6 月 9 日採録)

**安　健司**（学生会員）

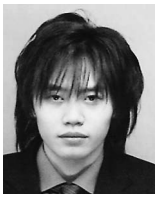
平成 15 年東京電機大学工学部二部情報通信工学科卒業．平成 17 年同大学大学院工学研究科情報通信工学専攻修士課程修了．現在，同大学院工学研究科情報メディア学専攻博士課程に在籍．情報セキュリティに関する研究に従事．

**赤羽　泰彦**

平成 14 年東京電機大学工学部一部情報通信工学科卒業．平成 16 年同大学大学院工学研究科情報通信工学専攻修士課程修了．同年日本システムデベロップメント入社．

**尾崎　将巳**

平成 17 年東京電機大学工学部一部情報通信工学科卒業．同年日立インフォネット入社．



**瀬本　浩治**

平成 17 年東京電機大学工学部一部情報通信工学科卒業．同年ダイヤモンドコンピュータサービス入社．

**佐々木良一**（フェロー）

昭和 46 年 3 月東京大学卒業．同年 4 月日立製作所入所．システム開発研究所にてシステム高信頼化技術，セキュリティ技術，ネットワーク管理システム等の研究開発に従事．同研究所第 4 部長，セキュリティシステム研究センタ長，主管研究長等を経て平成 13 年 4 月より東京電機大学工学部教授．工学博士（東京大学）．平成 10 年電気学会著作賞受賞．平成 14 年情報処理学会論文賞受賞．著書に，『インターネットセキュリティ』（オーム社，1996 年），『情報セキュリティ事典』（代表編，共立出版，2003 年）等．IEEE，電子情報通信学会等の会員．情報処理学会フェロー．日本セキュリティ・マネージメント学会常任理事，IFIP TC11 日本代表．