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

2005－ＣＳＥＣ－30 (16)
2005／7／21

暗号メールにおける個人情報不正送出チェック機能の拡張と評価

安 健司[†1] 赤羽 泰彦[†2] 尾崎 将巳[†3] 瀬本 浩治[†4] 佐々木 良一[†5]

†1,5 東京電機大学 〒101-8457 東京都千代田区神田錦町 2-2
†2 株式会社日本システムデベロップメント 〒541-0043 大阪府大阪市中央区高麗橋 3-3-7
†3 日立インフォネット株式会社 〒101-0061 東京都千代田区三崎町 2-20-7
†4 ダイヤモンドコンピュータサービス株式会社 〒102-0076 東京都千代田区五番町 4-7

E-mail: †1 ykenji@isl.im.dendai.ac.jp, †2 cbh68880@yahoo.co.jp, †3,4 {ozaki, semoto}@isl.im.dendai.ac.jp, †5 sasaki@im.dendai.ac.jp

あらまし 著者らは，暗号メールを使っている場合にも，個人情報の不正送出をチェックする方式の研究を行ってきた．従来の方式では，弱い暗号での暗号化を S/MIME での暗号化の前に行うと，不正送出がチェックできない場合があった．そこで，ベイズ理論を応用し，高い精度でスパムメールを分類するソフトウェアである POPFile を用いて，弱い暗号化が行われていることを自動的に検知する方式を考案し，プロトプログラムの開発と，実験を行い基本的な有効性の確認を行った．本論文では，その方式について説明し，実験結果と今後の展開について述べる．

キーワード 個人情報，プライバシ，ネットワーク，暗号化メール

Extension and Evaluation of Check Function 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[†5]

†1,5 Tokyo Denki University 2-2, Kanda-Nishiki-Cho, Chiyoda-Ku, Tokyo, 101-8457 Japan
†2 Nippon System Development Co.,Ltd. 3-3-7, Koraibashi, Chuo-Ku, Osaka, 541-0043 Japan
†3 Hitachi Infonet Co., Ltd 2-20-7, Misaki-Cho, Chiyoda-Ku, Tokyo, 101-0061 Japan
†4 Diamond Computer Service Co.,Ltd., 4-7, Gobancho, Chiyoda-ku, Tokyo, 102-0076 Japan

E-mail: †1 ykenji@isl.im.dendai.ac.jp, †2 cbh68880@yahoo.co.jp, †3,4 {ozaki, semoto}@isl.im.dendai.ac.jp, †5 sasaki@im.dendai.ac.jp

Abstract We have been developing the system to check the improper sending of personal information in encrypted e-mail system. This system could not check improper sending of personal information, if mail was encrypted with weak cryptography before encrypting with S/MIME. We have designed and implemented a system for solving such problems using POPFile software which was based on Bayesian theory and developed to check the Spam mail. 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.

Keyword Personal Information, Privacy, Network, Mail

1. はじめに

近年，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[1]．第三者からメールの機密を保護するために S/MIME などを用いた暗号化メールが普及しつつある．

しかし，暗号化メールの使用を許可すると，暗号によって保護されたメールメッセージに個人情報が含まれるかをチェックすることができない問題がある．それにも関わらず従来は，暗号化メールを使用したケースでの個人情報のチェックの検討はされていなかった．

著者らは，暗号化メールとして広く用いられている S/MIME 方式を拡張し，企業内のメールサーバ上で個人情報のチェックを行うことで，相反する 2 つの要求を満たす解決策を考案してきた[2][3][4]．

この方式の概要は次の通りである．

（1）S/MIME 方式に対応したチェックが可能

従来の S/MIME 方式を使用して Alice が，暗号化したメールを Bob へ送信した場合，Bob はそのメールを

復号化できるが，途中のメールサーバは復号化することできない．そこで，メールサーバ上で復号化できるように拡張したS/MIME方式を考案し，この問題の解決を図った．

なお，拡張したS/MIME方式で作成した暗号化メールは，メールサーバから送信先に発信する前に，その拡張部分を削除することで，従来のS/MIME方式の形式に戻すことができる．従って，暗号化メールの受信側では，拡張したS/MIME方式に対応したメールソフトは必要なく，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徴を持つ．

（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，平文のメールだけに有効なチェックである．個人情報のチェックを回避する不正者が，平文のメールをS/MIMEによる暗号化以外に何かの方式で暗号化することで，個人情報のチェックを回避可能にする問題が考えられる．

既に，強い暗号を用いる場合は，乱数性のチェックを行うことにより，怪しいメールをチェックして，送出しないことで問題の解決を図ってきた．

しかし，この方式では，乱数性のない弱い暗号などを用いた場合には適用できなかった．そこで，今回，POPFileを用いて，弱い暗号化が行われていることを自動的に検知する方式を考案し，プロトプログラムの開発と，実験を行い基本的な有効性の確認を行った．

本論文では，その方式について説明し，実験結果と今後の展開について述べる．

2. 従来のシステムの概要

2.1. 従来のシステムの構成

本稿では，図1に示す小規模な企業内のネットワーク構成を考えている．最低限のユーザとして，社員Aliceとその上長がいると想定している．ここで，チェックシステムの説明を行う前に必要な前提条件について述べる．

(a) AliceとBobは暗号化メールの送受信ができる．
(b) Aliceは，メールサーバTを経由してメールをBobに送信する．
(c) メールサーバTには，著者らが開発した個人情報の不正送出チェックシステムを導入し，通過するすべてのメールをチェックする．
(d) 上司は，部下を監督する立場にあるとして，不正を行わない．

これらの前提条件を満たしているものとして説明を進めていく．また，本稿では，この後の暗号化メールの説明で次の記号を使用する．

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

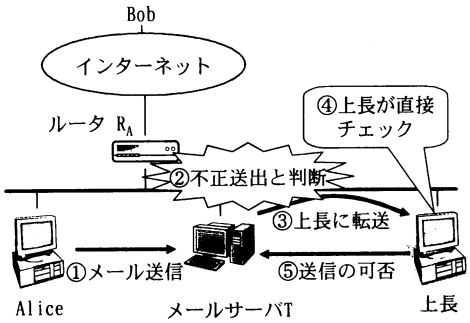


図1 不正送出発見時の流れ

チェックシステムが，個人情報の不正送出と疑われるメールを検出した場合，そのメールの送信を止めた上で，上司に転送する．上司は，個人情報であるかの確認と企業のポリシーなどを考慮した判断と対処を行う．また，検出されたメールに問題がなければ，チェックシステムに対して送信許可を与えられる．

チェックシステムで暗号化メールをチェックするには，暗号化メールを復号化する必要がある．しかし，表1に示す従来方式では，受信者のBob以外は復号化できないため，チェックができない．そこで，著者らは，従来方式にメールサーバTの公開鍵P_Tで，メールの暗号用の共通鍵Kを暗号化したものを追加することで問題の解決を図った．

表1 暗号化メール形式

従来方式	$P_B(K)$, K(M)
提案方式	$P_B(K)$, K(M), $P_T(K)$

2.2. メールサーバでの処理フロー

1章でも述べたが，著者らは，メールのチェックにおいてチェックを不正な暗号手法を用いることで，回避できる問題があると考えている．その対策についての考え方とチェックの流れについて述べていく．

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，不正者が，メールをすべてチェックされていることを知っていた上で，メールで個人情報を不正に持ち出す場合，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暗号をかけた上で，外部へ持出そうとする可能性があると考えられる．

そこで，そのような不正をチェックするため，

S/MIME 方式で復号化後のメールが，暗号文であるか個人情報チェックの前にチェックする．著者らは，幾つかの暗号方式について検討を行い，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，それぞれの特性に適したチェック方法を適用することでチェックの精度を高められると考えた．

また，これらの事前処理として，あて先のチェックを行うことで，チェックすべきメールを減らす．

以上の考え方に基づいて考え，個人情報不正送出チェックシステムの処理の流れを図 2 に示す．

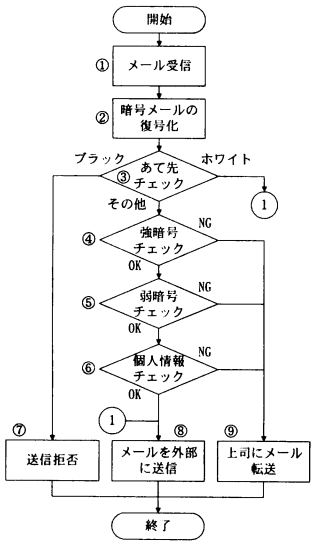


図 2 メールサーバでの処理フロー

2.3. 各チェック方式

1) あて先チェック

送信禁止のブラックリスト，チェック不要のホワイトリストと照合することで，チェックを行う．

2) 強暗号チェック

AES や Triple DES などの乱数性を持つ暗号を強い暗号と定義し，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使用する[6][7]．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

置換暗号や換字暗号など乱数性を持たない暗号を弱い暗号と定義し，文字や単語の出現頻度を基に暗号文の判定を行う．

著者らは，検出方式として，精度の高さから注目されているスパムメールフィルタリングの POPFile 方式に注目し，弱い暗号を効率よく検出する新しい方式を検討した．その方式を 3 章で説明する．

4) 個人情報チェック

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，これらの情報を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．自分の受信メールから返信メールを調査したところ，出現個数が最高で 9 個であった．よって，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．

3. 弱い暗号への対応

本章では，弱い暗号に対するチェック方式について詳しく述べる．著者らは，スパムメールをフィルタリングするソフトウェアとして，ベイズ理論を応用し高い精度でスパムを分類する POPFile を用いて，弱い暗号を検出するチェック方式を考案した．

3.1. 弱い暗号方式

2.3 節で AES, Triple DES などのような乱数性を持つ暗号を強い暗号と定義し，置換暗号や換字暗号などの乱数性を持たない暗号を弱い暗号と定義した．著者らは，インターネットから暗号ツールを入手し，そのツールの具体的な弱い暗号方式について述べる．

1) ミックス

文字の位置を一定の規則にしたがって，ランダムに入れ換える．このツールの暗号方式は，MIX 暗号とする．

2) FileLock

使用されている暗号方式が公開されていないため，詳細は不明であるが何らかのアルゴリズムで，平文を暗号化している．このツールの暗号方式は，可逆暗号とする．

3) ゆなシークレット

平文を 2 進数値に変換し，各ビットを反転する．このツールの暗号方式は，ビット反転暗号とする．

4) DoXOR

平文と入力されたパスワードと XOR をとる．このツールの暗号方式は，XOR 暗号とする．

5) 換字暗号

換字暗号については，インターネットから入手したツールを用いずに，著者らが手動で文字の換え字を行った．暗号化の手法は，著者らが任意に選択した 4～5 文字について，別な文字に換え字する部分的な換字暗号とした．

1)～5)の暗号方式で作成した暗号文は，強暗号チェックで検出することができなかった．従って，乱数性を持たない弱い暗号と言える．著者らは，代表的な 5

つの弱い暗号方式を用いてこれらを検出するチェック方式の開発を行う．

3.2. POPFile

POPFile[9]は，単語の出現頻度を基にしたモデルにベイズ理論を応用し，高い精度でスパムメールを分類するソフトウェアである．この POPFile は，「バケツ」と呼ばれるメールを分類する入れ物があり，初期段階でユーザが分類してほしいメールをバケツに入れて学習させる．その後，POPFile が誤って分類したメールについて，ユーザが手動で正しく修正していく形で運用する．

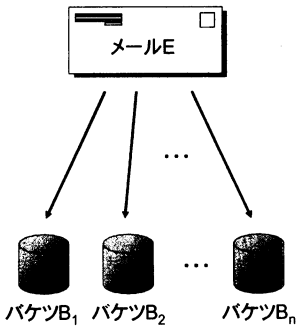


図 3 POPFile の概念図

POPFile は，単語の出現頻度を基に計算し，メールを適切なバケツに分類する．POPFile が行う処理は，次の通りである．

1) メール E の受信
2) KAKASI[10]で漢字を全て平仮名に変換し，単語に切り分ける．
3) メール E から単語 W_j を取り出し[1]，バケツ B_i に含まれる確率を式(1)と式(2)を用いて計算する．この計算を全てのバケツに対して行う．
4) 3)で求めたバケツ B_i に含まれる確率が，最も大きいバケツにメール E を分類する．

B_i ：i 番目のバケツ
E ：メールメッセージ
W ：メール E に含まれる単語
$P(B_i \mid E)$ ：メール E がバケツ B_i に含まれる確率
$P(E \mid B_i)$ ：メール E に含まれる単語が，バケツ B_i の中に現れる確率
$P(B_i)$ ：与えられたバケツが選ばれる確率

$$P(B_i \mid E) = P(E \mid B_i) \times P(B_i) \quad (1)$$

$$P(E \mid B_i) = P(w_1 \mid B_i) \times P(w_2 \mid B_i) \times \cdots \times P(w_m \mid B_i) \quad (2)$$

[1] (1)～(3)で用いられる単語 W は，メール E に含まれる単語の内，バケツ B_i にも含まれる単語を使用する．

$$P(B_i) = \frac{B_i\text{に含まれる単語数}}{\text{全バケツの単語数}} \quad (3)$$

3.3. POPFile を利用したチェック方式

POPFile は，「バケツ」をいくつも用意することで分類するメールをいくつも設定できる．そこで，著者らは，POPFile を利用したチェック方式を考案した．

そのチェック方式は，「暗号文」と「平文」の二つのバケツを作成し，分類する方式である．この方式を「2 バケツ方式」と呼ぶことにする．

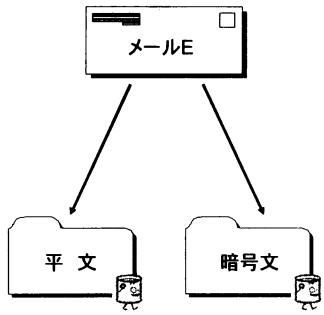


図 4 2 バケツ方式概念図

2 バケツ方式では，「平文バケツ」に平文を分類し，「暗号文バケツ」には 3.1 節で述べた 1)～5)の弱い暗号を分類する．本論文では，2 バケツ方式について幾つか実験を実施し，弱い暗号を検出するチェック方式としての有効性を確認する．

4. 評価

著者らは，3 章で考案した弱暗号チェック方式の性能評価実験を実施した．

4.1. 弱い暗号の種類別検出実験

3.3 節で述べたチェック方式で，どの程度 3.1 節に示した弱い暗号方式が検出できるか，弱い暗号方式ごとに確認する実験を行った．

予め平文バケツには，メール①②を 3 通ずつ学習しておく．そして，3.1 節に示した弱い暗号方式で，暗号化したメール③④を計 15 通送信する．これを 5 種類の暗号別に行い，その精度を確かめた．その実験結果を図 5，図 6 に示す．

表 2 使用したメールの種類

	個人情報なし	個人情報あり
暗号なし	①	②
暗号あり	③	④

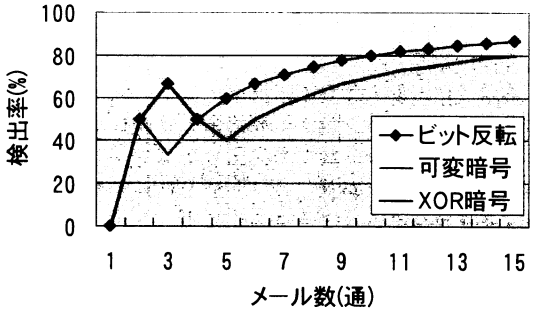


図 5 暗号別検出精度

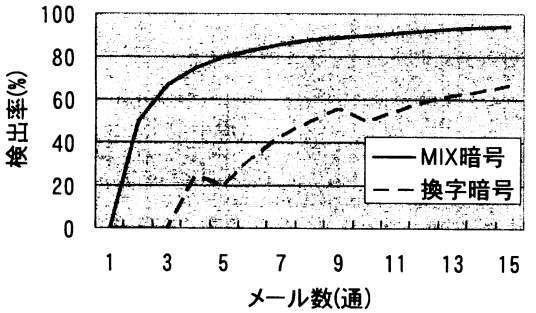


図 6 暗号別検出精度

図 5，図 6 に示す通り，各暗号方式を比較すると，ビット反転暗号などのビット列を細工する手法については，暗号化したデータが乱数に近い形になるため，検知することは容易である．また，MIX 暗号などの文章自体を細工する暗号についても，ランダム化された文章には，普段表れるような単語が存在しなくなるため，メールを 2,3 通学習させることでほぼ検出することができた．

ただし，換字暗号に関しては，暗号化するパターンが多いため，学習させるのに時間がかかりかつ検出率は，他の暗号方式比べ著しく低かった．

4.2. 弱い暗号の検出実験

前節では，3.3 節のチェック方式を用いて，弱い暗号方式を個別に実験を実施し，検出精度の確認を行った．しかし，実際には各種弱い暗号方式が，混在して送信されるケースが想定される．そこで，そのようなケースにおいても適切に検出できるかを確認する実験を実施した．

表 2 に示したメール①②③④を順番に送信し，平文 24 通，暗号文 36 通の計 60 通を弱暗号チェックで，チェックした時の検知精度を実験により求めた．

この時，メール①②は平文バケツに，メール③④は暗号バケツに分類されれば成功とし，未学習の状態からスタートした場合と，①②③④のメールをそれぞれ 3 通ずつ学習済みの場合の計 2 つの実験を行った．実験には，3.1 節に示す弱い暗号方式の計 5 方式を使用した．実験結果は，次に示す．

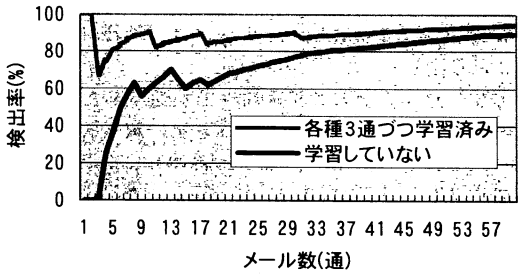


図 7 2 バケツ方式精度表

図 7 に示す通り，未学習からスタートした場合，数回学習させなければ検出することができない．しかし，ある程度学習させることで，安定して検出することができることが分かった．ただし，今回は実験データを 60 件で実験したため，今後は実験データをもっと増やし，その後の検出率の変化を見る必要があると考えている．

ここで，2 バケツ方式での誤検出について検討する．著者らは，「不正な暗号化メール」について，起こりうる最悪のケースについて検討した．すなわち，最悪のケースとは，次の 2 つが同時に起きることを考えている．

a) 弱暗号チェックで検出されない
b) 検出すべき個人情報が，含まれているにもかかわらず個人情報チェックで検出されない

a)と b)が，同時に起こる最悪のケースは，「学習なし」の場合で約 8.3%，「学習あり」の場合で約 6.7%となり，「学習なし」がやや高い結果となった．

また，これらの実験では，特に換字暗号の誤検出が目立った．この方式では，単語の出現頻度を基に確率計算を行うため，今回用いた部分的に置き換える換字暗号方式では，個人情報と暗号データの区別を付けるのが困難であると考えられる．

また，処理時間を計測してみると，表 3 の結果となった．

表 3 2 バケツ方式の処理時間 [秒]

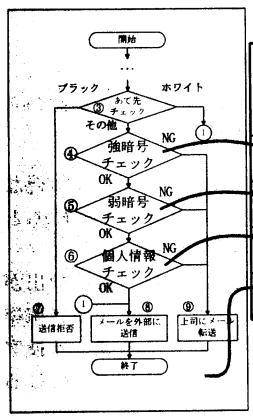
サイズ(KB)	平文メール		暗号化メール
	個人なし	個人あり	
10	0.66	1.76	0.98
1	0.11	0.33	0.18
平均	0.39	1.05	0.52

4.3. システム全体の処理時間の評価

システム全体の処理時間についての評価を行った．本章では，平文の電子メール，強暗号で暗号化した電子メール，弱暗号で暗号化した電子メールの3種類のデータを用いて実験し，各チェックの処理時間を計測して評価を行った．

実装したシステムの処理時間を測定するため，入力する電子メールのデータセットを次に示す3種類を用意し，それぞれのデータセットを入力した場合の処理時間を計測した．図8に示す1)から3)の平均処理時間の内，「全体」の平均処理時間には，各チェックの処理時間の他に初期化などの処理時間が含まれている．また3章で述べたように各チェックで発見された場合，その後のチェックは行われないため，「-」となっていることに留意する．

1) 平文データセット
   個人情報を含む電子メール10件，通常の電子メール10件の計20件の平文の電子メール
2) 強い暗号文のデータセット
   1)のデータセット 20 件を強い暗号方式であるAESで暗号化した電子メール
3) 弱い暗号文のデータセット
   1)のデータセット 20 件を弱い暗号方式であるYUNA暗号で暗号化した電子メール



チェック	データセット		
	平文	弱暗号	強暗号
強暗号	0.14	0.14	0.14
弱暗号	1.37	1.36	-
個人情報	0.10	-	-
全体	1.79	1.68	0.29

図8 各データセットの平均処理時間 [秒]

1)から3)のデータセットの内，1)は強暗号チェック，弱暗号チェック，個人情報チェックの3つのチェックを全て通過するため，最も平均処理時間が長かった．1)から3)の全体の処理時間を平均したメール1通当りの平均処理時間は，約1.8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，メール一通あたり約1.8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，個人情報不正流出チェックシステムのうち弱暗号チェックシステムの開発と評価を行った．

弱暗号実験では，図7を見て分かるように学習していく度に精度が上がり，ビット列を細工する暗号方式や文章をランダムにミックスする暗号方式については，ほぼチェックできることが証明できた．しかし，換字暗号などの文字の置き換えに対しては，まだ弱い部分がある．

今後の課題としては，換字暗号方式のチェックの精度を上げていくこと，全自動でのシステムの検討，チェックシステム全般としては，処理時間の短縮などが挙げられる．

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”, March 2004

[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, October 2004. 1

[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, October 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, July 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, "A Statistical Test Suite For Random and Pseudorandom Number Generators for Cryptographic Applications", Special Publication 800-22, May 2001.

[7] 情報処理振興事業協会 セキュリティセンター (IPA/ISEC), "擬似乱数検証ツールの調査開発　調査報告書", February 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, July 1998.

[9] POPFileDocumentationProject. http://popfile.sourceforge.net/cgi-bin/wiki.pl?JP_POPFileDocumentationProject

[10] KAKASI. http://kakasi.namazu.org/