情報処理学会論文誌 Vol.60 No.9 1565–1571 (Sep. 2019)

推薦論文

パスワード別送添付メールの問題点と受信側での対策について

乃村 能成[1,a)]

受付日 2018年12月3日, 採録日 2019年6月11日

概要：電子メールシステムは，歴史が長く枯れた技術であることから，相互運用性が高く，組織間の基本的な連絡手段として広く用いられている．電子メールで個人情報などの秘匿すべき情報を送信する際，暗号化された添付ファイルを送信し，共通鍵のパスワードを平文で別送することがよく行われている．本稿では，これをパスワード別送添付メールと呼び，パスワード別送添付メールの問題点を指摘する．また，問題点を受信側で解決する手法を提案する．提案手法は，暗号化されたメールに対応するパスワードメールとその中に含まれるパスワード文字列を効率良く発見し，パスワード解読を自動化する．さらに，提案手法を実装し，個人の電子メールシステムに組込み，運用した結果について評価する．評価では，多くのメールについて，数回のパスワード試行で解読が可能なことを示す．

キーワード：電子メール，セキュリティ，添付ファイル

Problems of e-mail Attachments Sent Separately for Passwords and Its Countermeasures at the Recipient Side

Yoshinari Nomura[1,a)]

Received: December 3, 2018, Accepted: June 11, 2019

Abstract: Since the e-mail system is a long-standing technology, it is highly interoperable and widely used as a basic communication tool between organizations. When transmitting confidential information such as personal information by e-mail, it is common in Japan to send an encrypted attachment-file and send the common key password separately in plaintext. In this paper, we name this as *eZIP mail* and point out the problem of e-mail attached with password. We also propose a method to solve the problem on the recipients side. Our proposed method efficiently finds the *password mail* corresponding to the encrypted mail and the password string contained therein and automates password decryption. Furthermore, we implemented the proposed method and evaluate the result of incorporating it into the personal e-mail system. In the evaluation, it shows that it is possible to decrypt many of mails with several password trials.

Keywords: e-mail, security, attachment-file

1. はじめに

電子メールシステムは，歴史が長く枯れた技術であることから，相互運用性が高く，組織間の基本的な連絡手段として広く用いられている．現状のメール配送系においては，end-to-end で通信が暗号化されている保証がないため，秘匿すべき情報を送信することは適切ではない．このため，何らかの暗号化手段が必要となることがある．メールの暗号化には，S/MIME [1] というメールの内容を暗号化して送受信する標準的な方式が存在する．しかし，S/MIME は，公開鍵暗号に基づくため，鍵交換の手間がかかり，広く普及するには至っていない．

[1] 岡山大学大学院自然科学研究科
Graduate School of Natural Science and Technology, Okayama University, Okayama 700–8530, Japan
[a)] nom@cs.okayama-u.ac.jp

本稿の内容は 2017 年 11 月のマルチメディア通信と分散処理研究発表会にて報告され，同研究会主査により情報処理学会論文誌ジャーナルへの掲載が推薦された論文である．

そこで，S/MIME の代替手段として，電子メールの添付ファイルを暗号化する手法が広くとられている．たとえば，個人情報を含む名簿などを送信したい場合，一連のファイルを zip アーカイブし，zip アーカイブに暗号化を施して送信する．ここで，アーカイブ形式として用いられる zip 形式も電子メールと同じく歴史が長く，相互運用性が高いと考えられている．つまり，電子メールを用いたコミュニケーションは，外部組織の不特定多数と交されるため，相互運用性が第一とされる傾向にある．

暗号化された zip ファイルは，共通鍵方式のため，電子メール送信側は，受信側に別途パスワードを知らせなければならない．日本においては，これを別の電子メールで送信することがよく行われている．これらのやりとりを含む暗号化メール，つまり，メールの添付ファイルを共通鍵暗号化し，別の平文メールでそのパスワードを知らせるような暗号化メールを本稿では，**パスワード別送添付メール**，もしくは，**eZIP メール**と呼ぶ．eZIP メールでは，送信側と受信側が暗号化に関して事前の合意をする必要がないため，近年広く用いられている．しかし，主に以下に示す問題がある．

(1) eZIP メール受信側のメールを開く手間が増大する．
(2) 受信側メールサーバ上でウィルススキャンができないため，セキュリティリスクが増大する．
(3) 送信側の望んでいると思われる効果が曖昧である．

特に著者が問題と考えるのは，この方式は，受信側には，主に不利益しかないことである．一方で，送信側にとって重要と思われるセキュリティ向上にあまり貢献していない．本稿では，まず，eZIP メールの問題点をより具体的に指摘する．次に，eZIP メールに対する受信側での対策について提案する．提案手法は，単純にいえば，eZIP メールから対応するパスワードを含む平文メールを推定し，その中に含まれるパスワードらしき文字列群を使うことで辞書攻撃によって eZIP メールの暗号を解く方式である．さらに，提案手法を実装し，個人の電子メールシステムに組込み運用した結果について，オーバヘッドや解読成功率を報告する．

2. eZIP メールとその問題点

2.1 eZIP メール増加の背景

1 章では，eZIP メールをメールの添付ファイルを共通鍵暗号化し，別の平文メールでそのパスワードを知らせるような暗号化メールと述べた．**図 1**，**図 2** にその具体例を示す．図 1 は，eZIP メールの例で，図 2 は，そのパスワードを平文で別送している例である．

多くの場合，パスワードメールは，eZIP メールの直後に送られていることから，多くの送信側は，何らかの自動化システムによって eZIP メールとパスワードメールを送信していると思われる．実際，eZIP メールを送信するための

図 1 暗号化された添付ファイルを持つメールの例
Fig. 1 Example of e-mail with encrypted attachment-file.

図 2 パスワードを別の平文メールで通知する例
Fig. 2 Example of another e-mail sending the password string separately in plaintext.

商用システムが多数存在する [2], [3], [4]．本稿で指摘したいのは，このシステムの普及による受信側の著しい手間の増大である．これまでも送信側が手動で eZIP メールを送信することはあったが，その際には送信側も手間がかかるため，よほどの重要で意味のある場合にしか行われなかった．したがって，受信側の手間も相応のものであったといえる．

暗号化の本来の目的からすると脆弱といわざるを得ない手法が商用システムとして成立しているのは，プライバシ

マーク [5] 取得のためであると思われる．たとえば，プライバシマーク実施のためのガイドライン [6], [7] では，個人情報を含む添付ファイルを取り扱う際にセキュリティ対策（データの暗号化，パスワード設定など）の措置を講じることを要件としている．また，上記の商用システムでは，eZIP メールの送信自動化は，プライバシマーク取得審査の対策として有用であるともうたっている．さらに，eZIP メールは，日本のみの習慣であるともいわれており [8]，日本固有の制度に立脚していると推察される．

もちろん，これらシステムには，メールの誤送信防止といった目的もあるとされているため，存在を否定するべきではないが，システム導入によって，すべての添付ファイルを無差別に暗号化してしまうことが，eZIP メール増加の一因であることは否めない．以降，本稿は，受信側での対策を扱うが，送信側の eZIP メール送信システムの運用基準を見直すことで，受信側の手間は減少するのではないかと思われる．

2.2 eZIP メールの問題点

eZIP メールには，以下の問題がある．

(1) 暗号化の意義が薄い
パスワードを平文で同一通信路で送信することから，暗号化の意味はきわめて薄いといわざるを得ない．

(2) 標的型メールを送りやすい土壌を作る
IPA の報告によると，標的型メールが増加しており，暗号化した zip ファイルを開かせる攻撃手法が示されている [9]．
また，メール添付されてくる不審ファイルの割合いで最も高いのは，zip アーカイブで 69%，次いで rar アーカイブとなっている [10]．eZIP メールの受信が常態化すると，添付文書にマルウェアを付けて暗号化する攻撃が成功しやすい土壌を作ることになる．

(3) ウィルススキャンの妨げになる
受信側メールサーバ上でウィルススキャンができないため，eZIP メールの添付ファイル内に何らかのマルウェアが含まれていた場合，セキュリティリスクが増大する．図 1 でも，「このメールにはウィルススキャンを実行できない暗号化された添付ファイルが含まれています」との警告が表示されているのが分かる．

(4) 受信側の添付ファイル展開の手間が大きい
受信側の手間を増大させるだけでなく，昔のメールを開こうとして，対応するパスワードメールを見付けられず，eZIP メールを開けない事態が発生する．

このうち，受信側にとっての問題として大きいのは，(1) を除くすべてである．

3. 受信側での eZIP メール対策手法

3.1 目的

eZIP メール受信側は，望むと望まざるとにかかわらず，以下の一連の操作を強いられる．

(1) 対応するパスワードメールを探す．
(2) パスワードメールからパスワード文字列を探す．
(3) 添付ファイル展開時にパスワードを入力する．

ここでは，メール受信時における上記操作を自動化し，受信側の手間を軽減することを第一の目的とする．本稿では，この自動化を**パスワード自動解読**と呼ぶ．パスワード自動解読が実現できれば，受信側の手間が軽減できるだけでなく，eZIP メールに対するウィルスチェックも自動化できるため，受信側組織全体のセキュリティレベル向上が期待できる．

3.2 パスワード自動解読の考え方

eZIP メール（z とする）送信側は，対応するパスワードメール（p とする）を同じ宛先に時間差で送ってくるので，ある時点において受信側のメールサーバ（アーカイブ）上に z，p 2 通のメールが含まれている．そこで，z に対応する p をメールサーバから検索して発見することを試みる．検索の結果，絞り込んだメール（以下，**パスワード候補メール**）$c_1, c_2, \ldots, c_n$ の中に p が含まれていれば，c_1 から c_n すべての本文からパスワードらしい単語を切り出すことで，いわゆる辞書攻撃の要領で z のパスワード自動解読が可能となる．

3.3 提案手法の処理流れ

パスワード自動解読の考え方に基づいた提案手法の処理流れを**図 3** に示し，以下で説明する．

(1) 受信側メールサーバに eZIP メール，パスワードメールが到着する．
(2) 提案システムの `Fetcher` は，受信側メールサーバを監

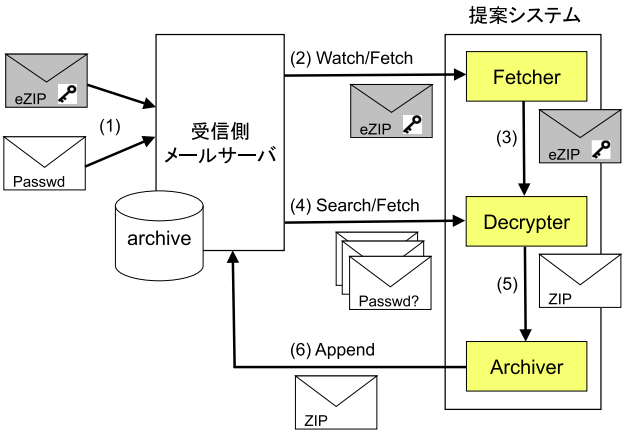

図 3 提案手法の処理流れ
Fig. 3 Control flow of our proposed method.

視しており，未処理の eZIP メールを 1 通取得する．
(3) `Fetcher` は，eZIP メールを `Decrypter` にわたす．
(4) `Decrypter` は，受信側メールサーバの検索機能を使い，eZIP メールに対応すると思われるパスワード候補メール群を取得する．
(5) `Decrypter` は，すべてのパスワード候補メールから単語を切り出すことでパスワード候補の辞書を作成し，以下を実行する．
  (a) 作成した辞書を用いて，eZIP メールのパスワード自動解読を試みる．
  (b) 解読に成功した場合，eZIP メールの添付ファイルをパスワードなしの zip に置き換える．
  得られたパスワード自動解読済みのメールを `Archiver` にわたす．
(6) `Archiver` は，受信側メールサーバに eZIP メールとは別のメールとして配送する．

上記処理流れにおいて，以下の 3 点が明らかではない．

- パスワード候補メールを取得する際の検索条件
- パスワード候補メールから切り出す単語の基準
- 作成した辞書からのパスワード適用順

以降では，それぞれについて検討する．

3.4 パスワード候補メールを取得する際の検索条件

事前調査の結果，eZIP メールに対応するパスワードメールは，以下の特徴を持っていることが分かった．

(1) パスワードメールは，eZIP メールに対してほぼ同時刻（配送遅延を考慮しても前後 1 日程度のブレ）で送られてくる．
(2) パスワードメールは，eZIP メールと同じ送信者から送られてくる．

上記の事実を利用することで，以下の方法で eZIP メールに対応するパスワード候補メールを検索する．

(1) eZIP メールの `From:` と `Date:` を取得する．
(2) 受信側メールサーバから，`From:` が同一で `Date:` が前後 1 日のメールを検索し，結果をパスワード候補メール群とする．

3.5 パスワード候補メールから切り出す単語の基準

パスワード候補の単語として，メール中のすべての文字列とその部分文字列を対象とすれば，候補として漏れがないといえるが，代わりにパスワード自動解読の効率が低下する．そこで，パスワードとして妥当な文字列のみを切り出す必要がある．

提案手法では，妥当なパスワード文字列として，以下の仮定をおいた．

(1) プレーンテキスト部分（Content-Type: Text/Plain）に存在する．
(2) ASCII-printable（ASCII のうち，改行などを含まない）のみからなる．
(3) 4 文字以上 16 文字以下である．

これらを満たす文字列をパスワード候補メールから切り出す単語の基準とした．

ここで，文字列長 4 文字から 16 文字という条件は，これまで著者が観測した eZIP メールのパスワード長から得た値である．

3.6 作成した辞書からのパスワード適用順

パスワード候補メールから切り出したパスワード候補を辞書として eZIP メール解読に利用する場合，どの候補から適用するかで，解読の効率が変わる．ここで，提案手法では，1 つの仮定を置く：

送信側は，**良い**パスワードを設定している．

つまり，得られたパスワード候補を「パスワードとして見たときに強固な順」にソートすることで，解読の効率を高められると考える．

良いとされているパスワードは，以下の性質を持つ [11]．

- 文字列が長い．
- 多数の文字種が使われている．
- 英単語の辞書に含まれない．

つまり，これらの基準をスコア化し，その値によってパスワード候補をソートすればよい．そのために，これに対応するスコア「文字列エントロピー」を以下のとおり定義する．

(1) $\log_2$（文字列長 + 1）を計算する（例：abc → 2）．
(2) ASCII-printable を `A-Z`，`a-z`，`0-9`，「それ以外」の文字種に分け，文字列中で文字種が変化する点を数える（例：`Abc` → 1，`A?3z` → 3）．
(3) 上記 2 つの値の和を文字列エントロピーとする．

ここでは，英単語の辞書に含まれているかどうかを直接エントロピーの計算に反映させていない．なぜなら，「多数の文字種が使われている」が条件をほぼ包含しているといえるためである．

ここで，必ずしも送信側がエントロピーの高い文字列をパスワードとして設定するとは限らない．しかし，eZIP メールを多数送信するユーザは，自身の組織内に 2.1 節で述べた自動送信のシステムを設置していることが予想できる．これら自動化システムは，パスワード文字列の選定にも高い基準を持っていることが想像されるため，高い文字列エントロピーを持つパスワードを発行すると予想される．したがって，eZIP メールの多くは，高い文字列エントロピーのパスワードを持つと仮定できる．

4. 実装

提案手法を著者が開発中のメールクライアントである glima に実装した [12]．glima は，Gmail を受信側メールサーバとして動作し，図 3 の処理流れを実現している．

IMAP IDLE [13] でユーザの Gmail の到着を監視（Watch）し，Gmail API [14] で Search，Fetch，Append の処理を実現している．また，図 3 の動作に加えて，解読の結果得られた zip ファイルを手元に保存する機能も持つ．

なお，Append の結果，提案手法によってパスワードが解除されたメールと元の eZIP メールの 2 通がアーカイブに残ることになるが，これは，本実装のバグによるメールの消失を防ぐためである．また，アーカイブは，Gmail のアーカイブを対象としているが，過去のメールを検索可能な IMAP サーバであれば，同様の実装が可能であると思われる．

以降，glima を用いて提案手法の評価実験を行った結果を示す．

5. 評価実験

5.1 目的

本評価実験の目的は，提案手法の実装である glima の性能を評価することで，提案手法が実際の環境で利用可能かを検討する際の基本的なデータを得ることである．具体的には，個人のユーザが数年間の間に受信した eZIP メール 200 通余りを対象とし，パスワード解読の精度，解読にかかる時間を評価する．また，パスワード候補メールの平均的な数や解読できなかったメールについて，具体的な事例を収集することである．

ここで，パスワードを自動で解析するという観点から類似の手法として，単純なブルートフォースや辞書攻撃が考えられる．たとえば，“John the Ripper” [15] は，パスワードクラックを高速で行うツールであり，同様の既存ツールがいくつか存在する．これらの既存ツールを用いることで，提案手法と同様の受信側での対策が可能であると考えるが，本提案手法の特徴は，その辞書の用意の仕方である．具体的には，eZIP メールの特徴を利用してパスワード候補リストに優先順位を付けることである．つまり，いかに計算機に負荷をかけずに目的のパスワードが得られたかといったことが興味となる．したがって，解読にかかる時間の評価は，実時間も有用であるが，解読の際のパスワード試行回数がより重要になる．この観点は，本稿が取り扱う特殊な問題設定によるものであり，既存ツールや研究の観点としてよくある，計算速度を競ったり，暗号化方式そのものの強度を議論したりすることとは，やや異なる．

5.2 評価環境

実験環境と実験対象メールの内訳について**表 1** に示し，説明する．図 3 における受信側メールサーバとして，岡山大学の Gmail サーバを利用した．提案手法の実装として，glima version 0.3.0 を岡山大学内に設置した計算機（MacBook Pro）に導入して利用した．

実験対象の eZIP メールとして，著者の岡山大学 Gmail アカウントが保有する 2015 年 1 月から 2017 年 10 月までのメールのうち，eZIP メール 212 通を対象とした．

表 1 実験環境と対象メール
Table 1 Test Environment and mails.

受信側メールサーバ	岡山大学 Gmail
提案手法の実装	glima ver 0.3.0
対象としたメールの受信期間	2015 年 1 月–2017 年 10 月
受信 eZIP メール	212 通

表 2 パスワード解読の成功率
Table 2 Hit-rate of password decryption.

eZIP メール	解読成功	解読失敗	エラー停止
212 通	178 通（84%）	27 通（13%）	7（3%）

表 3 パスワード解読失敗 27 通の原因内訳
Table 3 Reasons for failure of decryption.

通番	原因	メール数
1	先日のメールと同一パスワードのため別送省略	12 通
2	添付として再転送したメール	5 通
3	同一メールにパスワードが含まれる	4 通
4	パスワード前後に全角の空白	2 通
5	パスワードが別送されていない	1 通
6	パスワード不明で困ったという転送メール	1 通
7	パスワードが間違っていた（システムは正常）	2 通

受信側メールサーバは，期間中に受信した全メールを保有している．つまり，eZIP メール以外にもパスワードメールや本実験とは無関係なメールも受信側メールサーバ中に存在する．

5.3 評価項目

eZIP メール 212 通について，以下の項目を評価する．

(1) 提案手法による，パスワード解読の成功率
(2) 解読成功時のパスワード試行回数
(3) eZIP メールあたりのパスワード候補メール数
(4) eZIP メールあたりの解読時間

5.4 評価結果

5.4.1 パスワード解読の成功率

パスワード解読の成功率について，**表 2** に示し，説明する．

対象となる 212 通のうち，178 通（84%）の解読が成功した．

ここで，解読に失敗した 27 通について，原因を分析した．その結果を**表 3** に示し，説明する．

- 通番 1 の「先日のメールと同一パスワードのため別送省略」は，添付ファイルを互いに編集して送り合う場合に発生していた．これは，過去に解読に成功したパスワードを一定期間保存しておき，それらをパスワード試行リストに含めることで対応可能である．

- 通番 2 の「添付として再転送したメール」は，受信した eZIP メールとパスワードメールを 1 通のメールに 2 つのファイルとして添付して転送した例である．ほぼ同様の形として，通番 3「同一メールにパスワードが含まれる」は，eZIP メールを転送する際に，本文に平文でパスワードを記載した例である．これら eZIP メールと同一メール内にパスワードが含まれる場合を想定していなかったが，これは容易に対応可能な例である．
- 通番 4 の「パスワード前後に全角の空白」は，パスワード候補メールからパスワード候補を切り出す際のデリミタを調整することで対応可能である．
- 通番 5 以降は，提案手法では対応できないが，どれも対応する必要はないケースである．

以上のことから，提案手法に実装上のいくつかの改良を加えることで，今回の実験の範囲内では，すべての eZIP メールについてパスワード解読を成功可能であるといえる．

なお，7 通の eZIP メールに対する処理がエラー停止した原因は，メールに含まれる文字コードが不正のため，プログラムが処理を中断したためであった．文字コードの対応については，プログラム実装上の問題として解決可能であり，本稿では議論しない．

5.4.2 解読成功時のパスワード試行回数

パスワード解読成功時におけるパスワード試行回数の分布について，**表 4** に示し，説明する．

表から，6 回以内の試行で 90%以上の eZIP メールを解読可能であることが分かる．このことから，3.6 節で示した文字列エントロピーに基づくパスワード適用順が有効に機能していると分かる．また，最悪ケースである 125 回の試行を要した eZIP メールのパスワードは，4 文字の単純な文字列であり，送信者が手動で付与したものであった．

表 4 パスワード解読成功時におけるパスワード試行回数の分布
Table 4 Distribution of number of password trials at successful password decryption.

試行回数	成功数	成功数（累積）（%）
1	57 通	57 通（32%）
2	63 通	120 通（67%）
3	11 通	131 通（74%）
4	19 通	150 通（84%）
5	8 通	158 通（89%）
6	5 通	163 通（92%）
7	3 通	166 通（93%）
8	3 通	169 通（95%）
9	1 通	170 通（96%）
10	1 通	171 通（96%）
21	1 通	172 通（97%）
24	2 通	174 通（98%）
36	1 通	175 通（98%）
40	1 通	176 通（99%）
53	1 通	177 通（99%）
125	1 通	178 通（100%）

5.4.3 eZIP メールあたりのパスワード候補メール数

解読成功/失敗を問わず eZIP メール 212 通に対して，平均 3.1 通のパスワード候補メールが対応することが分かった．最大は，19 通で，これは，送信元が受信者であるようなメールである．つまり，その日のうちに送信した自身のメールがすべてパスワード候補メールとして対象となっていた．この数は，ユーザが 1 日に何通メールを送信するかによって左右される．この数を抑えたい場合，3.4 節の条件を見直し，自身が送信元の eZIP メールの場合，パスワード候補メールは，送信先が同一のものに限定すればよい．これにより，解読精度を保ったまま，効率を向上できる．

5.4.4 eZIP メールあたりの解読時間

解読時間は，パスワード試行回数が最も多かった 125 回の eZIP メールにおいて，約 4 秒であった．

また，解読失敗をした例を含めた場合は，345 回の試行をして，11 秒を要している．これは，受信側メールサーバから eZIP メールやパスワード候補メールを取得する際の時間も含むため，ネットワークの状態や eZIP メール，パスワード候補メールの大きさにも依存する．したがって，より詳細な分析が必要である．

6. 終わりに

本稿では，暗号化された添付ファイルを送信し，共通鍵のパスワードを平文で送信する方式をパスワード別送添付メール，あるいは eZIP メールとして定義した．さらに，eZIP メール普及の要因と問題点を指摘し，これらの問題点に対する受信側での解決策を提案した．

これまで，eZIP メールの弊害や危険性，海外から見た特異性 [8] は，断片的に指摘，報道されてきたものの，この問題に定まった名前が与えられておらず，学術論文の題材としても特に取りあげられたことはない．したがって，本稿の貢献は，問題のメールに eZIP メールという名前を与えて，これまで議論がなされなかったことに対して，議論の先鞭をつけ，注目を促すということにあると考える．

受信側での対策の結果，少なくとも著者個人の eZIP メールに対応する手間は著しく減少した．評価で示されているように，80%以上の eZIP メールが自動で解読され，メーラを問わずそれを開くことができる．受信側メールサーバ上でのウィルスチェックも行われるようになるため，メールを開く際の心理的負担もかなり軽減される．

このように，提案手法は，受信側での操作の手間を主な動機として発案されている．しかし，組織のメールサーバ上に設置することも可能であり，メールサーバ上でウィルスチェックの自動化を実現したり，別のパスワードで暗号化したりすることで，目的に応じたメールアーカイブのセキュリティ向上にもつながる．これらをふまえて，残され

た課題として，提案手法のメールサーバ上での評価がある．今回の実験では，glima は，eZIP メール解読を 1 通 4 秒以内で終えられることを示したが，解読が失敗した際には，最大で 1 通のメールに 11 秒の処理時間を要している．これらの値が，メールサーバの処理性能とユーザ数との関係でどう変化するかを明らかにする必要がある．

なお，glima は，オープンソースとして公開している [12]．本稿を借りて広く利用をお願いするとともに，実装改善のためのフィードバックをお願いしたい．

参考文献

[1] Ramsdell, B. and Turner, S.: RFC 5751: S/MIME 3.2 Message Specification (2010) (online), available from ⟨https://tools.ietf.org/html/rfc5751⟩.

[2] メール Zipper：メール添付ファイルの自動パスワード Zip 暗号化，LRM 株式会社（オンライン），入手先 ⟨https://www.lrm.jp/mailzipper/about/⟩（参照 2018-12-01）．

[3] GUARDIANWALL：添付ファイル ZIP 暗号化サービス，キヤノン IT ソリューションズ株式会社（オンライン），入手先 ⟨https://www.canon-its.co.jp/products/guardian_encryption/⟩（参照 2018-12-01）．

[4] WISE Audit：メールアーカイブソリューション ZIP 暗号化オプション，株式会社日立システムズエンジニアリングサービス（オンライン），入手先 ⟨http://www.hitachi-systems-es.co.jp/products/WISEAudit/spec/option/index.html⟩（参照 2018-12-01）．

[5] JIPDEC：プライバシーマーク制度，一般財団法人日本情報経済社会推進協会（オンライン），入手先 ⟨https://privacymark.jp/⟩（参照 2018-12-01）．

[6] 日本情報処理開発協会プライバシーマーク推進センター：JIS Q 15001:2006 をベースにした個人情報保護マネジメントシステム実施のためのガイドライン第二版，日本規格協会 (2010).

[7] JISA 審査業務部：JISA におけるプライバシーマーク審査項目の一部改訂について，一般財団法人情報サービス産業協会（オンライン），入手先 ⟨http://www.jisa.or.jp/service/privacy/tabid/831/Default.aspx?itemid=31⟩（参照 2018-12-01）．

[8] 小川大地：「ここが変だよ!?日本の IT インフラ」：第 27 回解凍パスワードは続けてメールします，ITmedia エンタープライズ（オンライン），入手先 ⟨http://www.itmedia.co.jp/enterprise/articles/1509/11/news019.html⟩（参照 2018-12-01）．

[9] 独立行政法人情報処理推進機：IPA 対策のシオリシリーズ (10) 標的型攻撃メール対策のしおり，IPA セキュリティセンター（オンライン），入手先 ⟨https://www.ipa.go.jp/security/antivirus/documents/10_apt.pdf⟩（参照 2018-12-01）．

[10] 独立行政法人情報処理推進機：標的型攻撃メールの傾向と見分け方，IPA セキュリティセンター（オンライン），入手先 ⟨https://www.ipa.go.jp/files/000052612.pdf⟩（参照 2018-12-01）．

[11] 独立行政法人情報処理推進機：IT 社会を，守る，育てる：ID とパスワード，IPA セキュリティセンター（オンライン），入手先 ⟨https://www.ipa.go.jp/security/keihatsu/pr2012/general/01_password.html⟩（参照 2018-12-01）．

[12] Nomura, Y.: Glima - Gmail CLI client (online), available from ⟨https://github.com/yoshinari-nomura/glima⟩ (accessed 2018-12-01).

[13] Leiba, B.: RFC 2177: IMAP4 IDLE command (online), available from ⟨https://tools.ietf.org/html/rfc2177⟩ (1997).

[14] Google Developers: Gmail API, Google (online), available from ⟨https://developers.google.com/gmail/api/⟩ (accessed 2018-12-01).

[15] Openwall Project: John the Ripper password cracker (online), available from ⟨https://www.openwall.com/john/⟩ (accessed 2019-04-10).

推薦文

本研究は，一般に広まっている，パスワードを平文で別のメールで送信する運用方法の問題点を指摘するだけでなく，それらにともなう作業を効率化する方法をオープンソースとして実装しており，大変有用な提案がなされております．様々な環境における事例を通し，技術的な発展が期待されることから，本稿を推薦いたします．

（マルチメディア通信と分散処理研究会主査　田上敦士）

乃村 能成　（正会員）

平成 5 年九州大学工学部電子工学科卒業．平成 7 年同大学院情報工学専攻修士課程修了．同年九州大学工学部助手を経て，現在，岡山大学工学部准教授．博士（情報科学）．本会シニア会員．