O-015

パスワード保護付き添付ファイルにおけるウイルス検知方法の一検討
A Study of Virus Detection Method in Attached File with Password Protection

佐々木 昌樹† 横坂 直克† 明石 貴靖†
Masaki Sasaki Naoyoshi Yokosaka Takayasu Akashi

1. はじめに

近年，特定の企業を狙った情報セキュリティに対して標的型攻撃による被害が顕著である．標的型攻撃の代表的な手段として，標的型攻撃メールがある[1]．標的型攻撃メールの主なパターンは，攻撃者が実在する企業・団体名を名乗り，あたかも正当な業務や依頼に見せかけた件名・本文でメールを送りつけ，受信者にウイルスを含む添付ファイルを開かせたり，悪意のあるサイトへ誘導したりして，ウイルスに感染させる．特に，標的型攻撃メールの被害において，添付ファイルによる攻撃が中心になっている．添付ファイルとして，実行可能形式のファイルや悪意のあるマクロが仕込まれたドキュメントファイルが使われる．これらのファイルは，パスワードで保護されていなければ，ウイルスチェックが可能であるが，添付ファイルがパスワードで保護されている場合，一般的なウイルスチェックでは，パスワードが不明なため，パスワードの保護解除をすることができなく，ウイルスチェックもできない．例えば，ウイルス感染していることに気づいていない取引先から，パスワード保護を付けたファイルをメールで受信した場合，安心してファイルを開いてしまいウイルスに感染することがある．これに伴い，企業では，メール受信者がパスワード保護付き添付ファイルを受信する前に，パスワード保護付き添付ファイルのウイルスチェックを行うことが求められている．

2. 先行技術

上述したメール受信者がパスワード保護付き添付ファイルを含むメールを受信する前に，パスワード保護付き添付ファイルのウイルスチェックを行うためには，パスワード保護付き添付ファイルの保護解除をする必要があり，解決するための技術が公開されている（以降，先行技術と称する）．例えば，パスワード保護付き添付ファイルのメールを受信した際に，添付ファイルのパスワードは別のメールで受信する場合がある．先行技術では，メールサーバでこのパスワードが記載されたメールからパスワードを読み取り，パスワード保護付き添付ファイルのパスワード保護を解除する．これにより，添付ファイルのウイルスチェックを行うことができる[2].

3. 課題

しかしながら先行技術において，メールサーバによるパスワード保護付き添付ファイルのパスワード保護解除は，パスワード保護付き添付ファイルのメールとは別のパスワードを記載したメールを受信することが前提であり，このパスワードを記載したメールを受信できなかった場合は，パスワード保護付き添付ファイルのパスワード保護を解除できないため，ウイルスチェックを行うことができない．また，メールサーバは，メール受信者から受信要求があると，パスワード保護付き添付ファイルを含むメールを通知後，さらにメール受信者から，通知したパスワード保護付き添付ファイルを含むメールの削除要求があると，通知したパスワード保護付き添付ファイルを含むメールを削除する．これにより，パスワード保護付き添付ファイルを含むメールがメールサーバ上から削除されてしまうという課題も生じる．

このような課題を解決するため，本研究ではパスワード保護付き添付ファイルを含むメールを受信したが，添付ファイルのパスワード記載メールを受信していない場合において，添付ファイルのパスワード記載メールが送信されるまで，メールサーバ上にパスワード保護付き添付ファイルを含むメールを保管し，かつ，パスワード記載メールが送信された場合，パスワード保護付き添付ファイルのウイルスチェックを行うことを提案する．

4. 提案手法

4.1 方針

そこで，本提案では，メール受信者がメールサーバから自分のメールを取り出す時に使用するメール受信用プロトコルである Post Office Protocol - Version 3（以降，POP3 と称する）に着目し，POP3 において指定されたメッセージ番号のメッセージを削除する DELE コマンドを用いた提案を行う．以下，提案手法のシステム構成と動作手順について述べる．

4.2 システム構成

提案システムの構成図を図 1 に示す．提案システムは，既存のシステムに対して以下の要素を追加している．

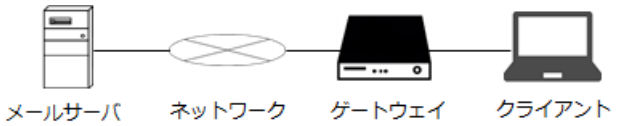

図 1　システム構成図

・ゲートウェイ

クライアントからパスワード保護付き添付ファイルを含むメールの DELE コマンドを受けた場合，DELE コマンドをメールサーバに通知せず，DELE コマンドに対する応答メッセージを作成し，クライアントに送信する．

4.3 動作手順

動作手順を図 2 に示す．ここでは，メールサーバには，パスワード保護付き添付ファイルを含むメールのみがあるとし，クライアントがメールサーバ上にある自宛のメールを受信するものとする．

† 株式会社ナカヨ 事業戦略本部 情報技術研究所,
Information Technology Laboratory, Business Strategy Division, NAKAYO, INC.

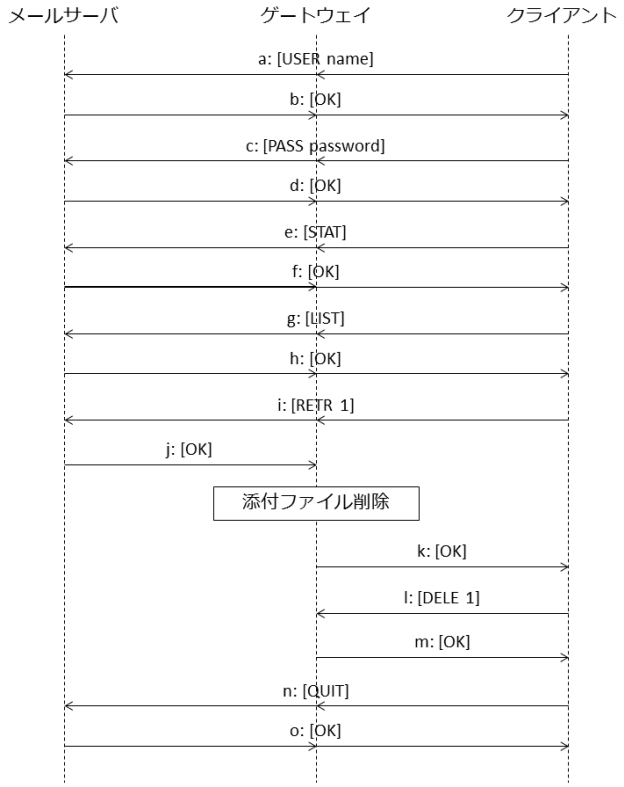

図 2　動作手順

1. クライアントはメールサーバにユーザ名とパスワードを送り認証を行う(a,b,c,d).
2. クライアントはメールサーバに自宛のメール数と全体データ量の問い合わせを行い，応答を得る(e,f).
3. クライアントはメールサーバにメール番号とメール番号に対するサイズの問い合わせを行い，応答を得る(g,h).
4. クライアントはメールサーバに読み出すメール番号を指定してメール読み出しを行う(i)．この時に，ゲートウェイは，メール番号を一時保持する.
5. メールサーバはクライアントにメールを通知する(j)．この時，ゲートウェイはメール内の添付ファイルを削除してクライアントに通知する(k).
6. クライアントはメールサーバに削除するメール番号を指定してメールの削除を行う(l)．ここでは，指定するメール番号はパスワード保護付き添付ファイルを含むメールのものとする.
7. ゲートウェイはクライアントから受信したメール削除メッセージに対して，メッセージにおけるメール番号と(i)で保持したメール番号が一致するか否かを判断し，一致の場合応答メッセージを作成し，クライアントへ通知する(m)．これにより，ゲートウェイにおいて，クライアントがメールサーバに対して送信するパスワード保護付き添付ファイルを含むメールの削除をメールサーバに通知しない仕組みとメール受信者のメールの削除に対して応答を行い，メール削除をメールサーバに通知したとする仕組みを実現できる.
8. クライアントはメールサーバと認証解除を行う(n,o).

尚，このあとに，メール送信者がパスワード保護付き添付ファイルのパスワード保護の解除を行うためのパスワードが示されたパスワード記載メールを送信して，メールサーバにパスワード記載メールとパスワード保護付き添付ファイルを含むメールがある場合において，クライアントから上述同様にメールの読み出しがあると，ゲートウェイはパスワード記載メールからパスワードを抽出し，抽出したパスワードを使い添付ファイルのパスワード保護解除を行い，ウイルスチェック後，ウイルスを含まない場合は，パスワード記載メールに添付ファイルを添付してクライアントに送信する.

5. まとめ

本研究では，パスワード保護付き添付ファイルにおけるウイルス検知方法について検討した.

提案手法では，POP3 の DELE コマンド用い，クライアントがメールサーバに対して送信するパスワード保護付き添付ファイルを含むメールの削除をメールサーバに通知せず，メール受信者のメールの削除に対して応答を行い，メール削除をメールサーバに通知するため，添付ファイルのパスワード保護の解除を行うためのパスワードが示されたパスワード記載メールがメールサーバに送信されるまで，メールサーバ上にパスワード保護付き添付ファイルを含むメールを保管することが可能である.

今後の課題として，パスワードが示されたパスワード記載メールを受信しない場合やパスワード保護付き添付ファイルを含むメールより先にパスワードが示されたパスワード記載メールを受信する場合の検討が必要である.

参考文献

[1] 独立行政法人情報処理推進機構“情報セキュリティ 10 大脅威 2017,” https://www.ipa.go.jp/security/vuln/10threats2017.html,May.2017
[2] 大谷洋，“電子メールの暗号化ファイルのパスワード決定装置および電子メール・サーバならびにそれらの動作制御方法,” 特開 2011-71615.