2Z-1

メール送信者認証技術における検証機能の改善について

増渕 篤† 土井 洋†
情報セキュリティ大学院大学†

1. はじめに

メールアドレスを偽って送信されてくるSPAMメールやフィッシングメール，マルウェア等による被害やメール本文から誘導されたフィッシングサイトによる被害は未だ続いている[1]．これらのいくつかは認証が正しく行われていれば被害は低減できることから，メール送信者認証技術に着目した．メール送信者認証には，送信者を認証するものやドメインを認証するものがある．メール送信者認証を実現する方法として，メールに署名を付与するもの（DKIM, S/MIME等）とそうでないもの（SPF等）に分けられる[2]が，転送やメーリングリストを経由することによる課題があると言われている．

本研究では，メール送信者認証技術の１つであるDKIMに着目し，DKIMの検証機能の改善を検討し，改善結果を仮想環境上で評価した．

2. メール送信者認証技術の現状

SPFは, SMTPを利用した電子メールの送受信において送信者のドメインの偽称を防ぎ，正当性を検証する仕組みのひとつとして元Pobox社のMeng Wong氏により提唱された（RFC4408[3]）．SPFは現在もっとも多く利用されている送信ドメイン認証技術であり[4]，送信元メールサーバのIPアドレス及びDNS情報をベースに認証する．

送信者を認証するS/MIMEは，米国のRSA Security 社によってS/MIME v2が1995年に提唱され標準化された（RFC2311[5]，RFC2312[6]）．更にIETFによってより汎用性を持たせたS/MIME v3が策定された（RFC2632[7], RFC2633[8]）．これは，PKI（公開鍵暗号基盤）を利用している．

DKIMは，電子署名を利用したメールの送信ドメイン認証技術である．DKIMでは，送信側（例えば送信側サーバ）で電子署名を施し，受信側（例えば受信側サーバ）で検証を行う. DKIMはIIMとDomainKeysを統合したものであるが，DomainKeysの影響をより大きく受けている．

A Study of the Verifier Side Improvement on Email Authentication Technique

Atsushi Masubuchi†, Hiroshi Doi†
†INSTITUTE of INFORMATION SECURITY

本研究では，メール送信者認証技術の中でも信頼性の高いDKIMに着目し，メーリングリストを経由する場合の課題解決に向けた改善手法を示す．

3. DKIMとその課題

3.1. DKIM(DomainKeys Identified Mail)

2章で紹介したDKIMは電子署名を利用した，メールの送信ドメイン認証技術の一つであり，Yahoo!社，Cisco Systems社，Sendmail社，PGP社の4社により共同開発された．DKIMの仕様はRFC6376[9]として公開されている．DKIMの普及を通して，迷惑メール対策を推進することを目的として設立された団体dkim.jpがある[10].

また，RFC6376[9]に準拠したOpenDKIMというフリーソフトが利用可能であり，RHELやCentOS用のパッケージ化もされている．

3.2. DKIMの課題

メールに対して電子署名を付与する場合，メーリングリストを経由すると検証が失敗する場合がある．これはメーリングリストマネージャーが，電子署名の対象となる本文やヘッダ（件名等）を再配送する際に変更する場合が多く，送信時に作成した署名対象を変更してしまうからである．

3.3. メーリングリストを経由する場合の問題

実験環境を構築し, 現状を確認した. 実験環境は, Windows 7をホストOSとし，VMWare 9.0.0をインストールした．ゲストOSはCentOS6.4で構築し，メーリングリストは，Mailman，Majordomo，FMLを調査対象とした．ゲストOSで稼動させたソフトを表1に示す．

Mailmanの場合は, デフォルトで件名と本文が変更される．一方、MajordomoやFMLは，デフォルトの場合，件名および本文は変更されない．ただし，メーリングリストを利用する上では件名に対して，ML名＋通番 を加えることが少なくなく，MajordomoとFMLについては，その設定も容易である. 実際, 件名にML名＋通番を加える設定とすると，

```
Authentication-Results: masu14.iisec.com; dkim=fail
reason="verification failed"
header.d=masu8.iisec.com header.i=@masu8.iisec.com
header.b=VjL75vhQ; dkim-adsp=unknown
```

という検証失敗のヘッダが追加され，DKIMの検証が失敗することが確認できる．

一方，本文への修正に関して，Mailmanにおいては，デフォルトで本文末尾に追加される．更に設定により本文先頭への追記も可能なことも分かったことから，DKIMのlタグでの対処は難しいと考えられる．

各メーリングリストマネージャーの件名および本文への修正について確認し，その設定がデフォルトなのか，オプションとして変更可能なのかを表2にまとめた．

表1　実験環境

サーバ	主な稼動ソフト
送信側メールサーバ	PostFix 2.6.6
	OpenDKIM 2.8.4
メーリングリストサーバ	PostFix 2.6.6
	Mailman 2.1.12
	Majordomo 1.94.5
	FML 4.0.3
受信側メールサーバ	PostFix 2.6.6
	OpenDKIM 2.8.4

表2　ML毎の機能

メーリングリスト	件名変更	本文変更
Mailman	デフォルト	デフォルト（末尾，設定により本文先頭も可）
Majordomo	可	不可
FML	可	可
Aliases	不可	不可

4.　提案手法

本研究では，まず，3章で示した通り，メーリングリスト経由の場合に検証が失敗することを確認した．これらは，メーリングリストマネージャーが件名や本文の修正を行うためである．しかし，変更内容を確認すると，メーリングリストの修正は限定的であると考えられる．実際，受信者にメールを読んでもらうという観点からも修正はそれほど大きく複雑になるとは考えにくい．そこで，検証の際に修正部分を元に戻すことができれば，メーリングリスト経由であっても，検証が成功するのではないかと考えた．

本研究では，OpenDKIM 2.8.4に修正を加えることとした．メーリングリスト経由の可能性が高い場合の条件を定め，その条件を満たした場合，メーリングリストマネージャーが修正した情報を元に戻した上で検証を行うことで，検証精度の向上を目指す．ただし，受信したメール自体はメーリングリストマネージャーが修正した形のまま，受信者に届くよう修正には配慮した．

5.　実験結果

OpenDKIM 2.8.4を修正し，各々のメーリングリストに対して実験を行った結果，どのメーリングリスト経由のメールにおいても，検証が成功することを確認した．

一方，受信者にはメーリングリストが修正したメールの情報を保持したまま，届いている．

ただし，今回の実験により，メール本文の先頭に追加された場合の対応が難しいことが分かった．また，件名や本文にメーリングリストマネージャーが行ったと思われるような記載があるメールは誤動作する場合があった．

6.　まとめと課題

本研究では，DKIMについて着目し，まずはDKIMの課題であるメーリングリスト経由の問題が現在でも未解決であることを確認した．DKIMの検証機能を改善することで，メーリングリスト経由でも検証が成功することを確認した．なお，本報告では対象外としているが，S/MIMEにおいても本文に追記するメーリングリストマネージャーにおいては検証が正常に動かないことを確認している．

今後は，誤動作を減らすような修正を検討するとともに，S/MIMEに関しても検討したい．また，検証結果を受信者へ伝える手段の検討や，パフォーマンス評価を行う必要がある．

参考文献

[1] フィッシング対策協議会, フィッシングレポート 2013, https://www.antiphishing.jp/report/pdf/phishing_report_2013.pdf, 2013.
[2] 日本データ通信協会, 迷惑メール相談センター, http://www.dekyo.or.jp/soudan/taisaku/4-2.html, accessed 2014-01.
[3] RFC 4408, Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail Version 1, http://www.ietf.org/rfc/rfc4408.txt, 2006.
[4] 日本データ通信協会, 送信ドメイン認証実施状況, http://www.dekyo.or.jp/soudan/auth/, accessed 2014-01.
[5] RFC 2311, S/MIME Version 2 Message Specification, http://www.ietf.org/rfc/rfc2311.txt, 1998.
[6] RFC 2312, S/MIME Version 2 Certificate Handling, http://www.ietf.org/rfc/rfc2312.txt, 1998.
[7] RFC 2632, S/MIME Version 3 Certificate Handling, http://www.ietf.org/rfc/rfc2632.txt, 1999.
[8] RFC 2633, S/MIME Version 3 Message Specification, http://www.ietf.org/rfc/rfc2633.txt, 1999.
[9] RFC 6376, DomainKeys Identified Mail (DKIM) Signatures, http://www.ietf.org/rfc/rfc6376.txt, 2011.
[10] Japan DKIM Working Group, http://www.dkim.jp/, accessed 2014-01.