電子メール認証技術

～迷惑メール撲滅に向けて～

瀬戸川 滋彰，折戸 俊彦
Shigeaki SETOGAWA，Toshihiko ORITO

1　はじめに

近年，インターネット上でやりとりされるメール内のスパムメールの割合が増え続けており，スパムメールの蔓延による業務効率の低下やインターネット資源の浪費が重大な社会問題となっている．特に最近流行しているフィッシングメールは現状の迷惑メール対策技術では対応ができず，被害が増加している．一方，IETF[1]ではこの問題の解決が期待されている送信者認証技術の標準化が進められており，現在注目を浴びている．本稿では，送信者認証技術とその展望について述べる．

2　迷惑メール対策技術と問題点

2.1　従来の迷惑メール対策技術

従来の迷惑メール対策技術にはメールサーバで受信拒否をする方法と，メールを受けとってからフィルタリングする方法がある．受信拒否はメールサーバで受信するメールに関するルールを定め，そのルールに沿わないメールは配送しない方法である．ルールはメールサーバによって異なり，既知のスパム業者が登録されているブラックリストを用いる方法や，IP アドレスから DNS の逆引きを行う方法などがある．フィルタリングはベイジアンフィルタと呼ばれる統計学的手法を基にしたフィルタを用いる方法である．ベイジアンフィルタは人間によるスパムメール，非スパムメールの判定を学習し，そのメール内容を解析してスパムメール，非スパムメールにそれぞれ良く用いられる言葉を抽出することで，届いたメールがスパムかどうかを判定する機能を持つ．

2.2　フィッシングメール

フィッシングメールはヘッダの詐称などによって社会的信用度の高い企業のメールになりすまし，巧妙な文章で偽の企業サイトに誘導して個人情報を盗み出すことを目的としたメールである．従来の迷惑メール対策技術はフィッシングメールに対しては有効ではない．フィッシングメールは送信者詐称をしているため受信拒否をすり抜けてしまう．また，社会的信用度の高い企業からのメールになりすましているという特性上，フィルタリングも困難である．送信者認証技術を用いると送信者名の詐称ができなくなるため，受信拒否によってフィッシングメールを防ぐなどの対策が可能になる．

[1]Internet Engineering Task Force

3　送信者認証技術

送信者認証技術は IETF で標準化が進められている電子メール向けのプロトコルであり，メールが記載されている送信元から確かに送信されたものであることを認証する仕組みを有している．送信者認証技術には，送信元の IP アドレスとドメイン名を元に認証する IP ベースの認証方式と，送信側メールサーバが付けたディジタル署名を元に正当な送信者から送信されているかを認証する署名ベースの認証方式がある．以下，各方式の代表的な技術である Sender ID と DomainKeys について述べる．

3.1　Sender ID

Sender ID は米 Microsoft 社の Caller ID for E-mail と SPF という 2 つの送信者認証技術を合わせた IP ベースの送信者認証技術である．Sender ID は送信元サーバの IP アドレスとドメイン名の関係をチェックし，メールを送信しているサーバを認証する．

3.1.1　手順

Sender ID は全ての電子メールに対して，送信元の SMTP サーバの IP アドレスを送信元のドメインが承認しているかどうか認証する方式である．Sender ID での認証手順を Fig.1 に示す．

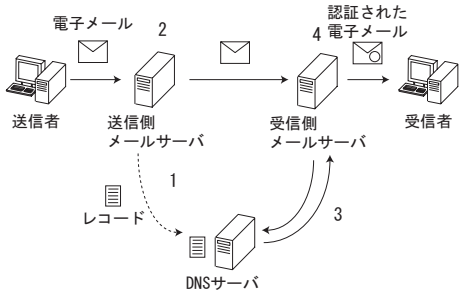

Fig. 1　Sender ID の手順

1. 送信者側は自分のドメイン名に対応するメールサーバの IP アドレス情報を DNS サーバに登録しておく．

2. 送信側サーバは普通に電子メールを送信する．

3. 受信側サーバは受信したメールの From ヘッダに書いてあるドメインの DNS サーバにそのドメインのレコードがあるかどうかを調べる．

4. 受信側サーバは送信側サーバの IP アドレスがレコードに公開されている IP アドレスのいずれかと一致するかどうかを認証する．

3.1.2 メリット

DomainKeys に比べて SMTP サーバへの負荷が小さく実装が簡単である．また，送信側は DNS に自ドメインのメールサーバのリスト情報を登録しておくだけで良く，暫定的な導入が可能である．

3.1.3 デメリット

Sender ID は直前の相手しか認証できないため，経由するサーバが全て Sender ID を導入しない限り転送メールに対応できない．

3.2 DomainKeys

DomainKeys は米 Yahoo!社と米 sendmail 社が開発した署名ベースの送信者認証技術である．DomainKeys は送信側メールサーバでメールに付加されたディジタル署名を用いて，オリジナルの送信者を認証する．

3.2.1 手順

DomainKeys は送信元の SMTP サーバで埋め込まれたディジタル署名を元に，ヘッダ及び本文が改ざんされていないかを認証する方式である．送信者詐称をしていると受信側が正しい公開鍵を受け取ることができず認証に失敗する．DomainKeys での認証手順を Fig.2 に示す．

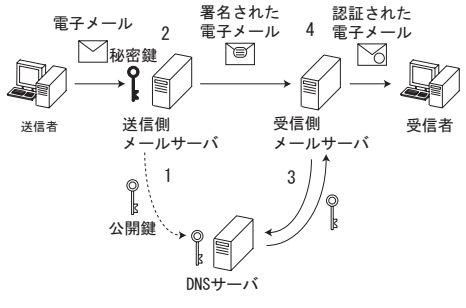

Fig. 2 DomainKeys の手順

1. 送信者側は認証に用いる公開鍵を DNS サーバに登録し，秘密鍵は送信側メールサーバに保管しておく．

2. 送信側サーバはメールを送信する際にディジタル署名をメールヘッダに埋め込む．

3. 受信側サーバは受信したメールの From ヘッダに書いてあるドメインの DNS サーバから公開鍵を受け取る．

4. 受信側サーバは公開鍵を用いて署名を認証する．

3.2.2 メリット

最初の送信サーバがメールにディジタル署名を付けるため，転送されても元の送信者を認証可能である．

3.3 デメリット

DomainKeys はメールのヘッダと本文から署名を作成しているため，メーリングリストなどこれらが変更されてしまう場合は認証できない．また，Sender ID よりもサーバに与える負荷が大きく，導入に関しても送信側と受信側が共に DomainKeys に対応する必要がある．

4 今後の展望

送信者認証技術は一つ導入すれば他の物は導入できないということは無く，むしろ組み合わせて使用することでお互いの欠点を補い合いより効果を高めることができるため，送信側は複数の方式に対応し，受信側は自分のポリシーにあわせてそれを選択し組み合わせて認証するといった普及の仕方をすると考えられる．

送信者認証技術はスパムメールやフィッシングメールを直接防ぐものではない．しかし，送信者認証技術の導入によって嘘をつけなくなった送信者情報は，迷惑メールか否かを判断する際の新たな根拠となる．今後は送信者詐称がされていないという前提に，それを利用して従来のものを発展させたより判断精度の高い迷惑メール対策技術の登場が期待できる．

5 一年後の予想

現在，hotmail や Yahoo などの大手フリーメールが送信者認証技術に対応し始めている．送信者認証技術では対応していないドメインから送信されたメールは未認証になってしまうため，送信者認証技術を導入したドメインに確実にメールを届けるためには送信側も対応する必要がある．そのため，多くのユーザを抱える大手フリーメールが送信者認証技術を導入すれば，他のドメインも送信者認証技術を導入せざるを得なくなる．フリーメールの中でも特に利用者の多い hotmail が今年の 10 月 1 日までに Sender ID に対応するとの発表がされているため，その前後から送信者認証技術の普及が進み，1 年後には送信者認証技術は広く利用されているだろう．

参考文献

1) Sender ID ホーム ページ
http://www.microsoft.com/japan/mscorp/safety/technologies/senderid/default.mspx.

2) どうなる？ メールの送信者認証
http://itpro.nikkeibp.co.jp/free/ITPro/OPINION/20041115/152576/.