メール認証技術の背景と特徴

**今回は、2012年第40週から第52週までの迷惑メールの推移を報告します。
迷惑メールの割合は、前回のレポートから5.6%の減少、前年同時期からも6.3%の減少となり、
しばらく変化が少なかった最近の傾向から、更に減少に転じましたが、今回とりあげたように、
日本のユーザを狙ったフィッシングなど、迷惑メールに起因するセキュリティ的な脅威については、
より深刻さを増してきています。**

2.1 はじめに

このレポートでは、迷惑メールの最新動向やメールに関連する技術解説、IIJが関わる様々な活動についてまとめています。今回は、日本の多くの企業の第3四半期にあたる2012年第40週(2012年10月1日～10月7日)から第52週(2012年12月24日～12月30日)までの13週間分のデータを調査対象として分析結果を報告します。

迷惑メールの動向については、迷惑メール割合の推移と送信元地域の割合の分析、金融機関を騙ったフィッシングの事例について報告します。技術動向では、メールの認証技術の概要と送信ドメイン認証技術との関連について解説します。

2.2 迷惑メールの動向

ここでは、迷惑メールの動向として、IIJのメールサービスで提供している迷惑メールフィルタが検知した割合の推移と、迷惑メールの送信元に関する分析結果を中心に報告します。

2.2.1 迷惑メール割合は減少傾向だが脅威は深刻に

今回の調査期間(2012年10月1日～12月30日)での迷惑メール割合の平均値は、40.5%でした。前回のレポート(Vol.17)から5.6%の減少となりました。迷惑メールの割合は、前年同時期(Vol.14)からも6.3%減少しており、しばらく変化が少なかった最近の傾向から、更に減少に転じたような印象です。しかしながら、後でも詳しく述べますが、迷惑メールに起因するセキュリティ的な脅威については、より深刻さを増していると思います。迷惑メールは、これまでの届くかどうかに関わらない大量送信的なものから、対象を絞った、より巧妙な手法に変化してきているように見受けられます。前年の同時期(Vol.14)から今回の調査期間での迷惑メールの割合の推移を図-1に示します。

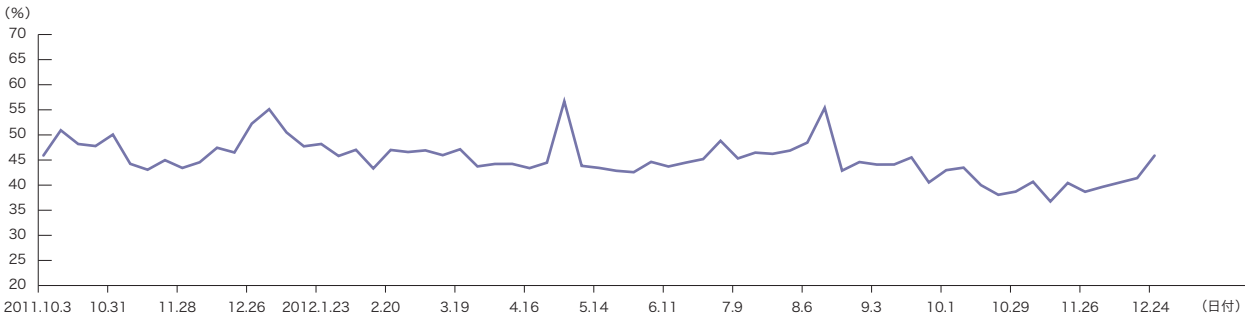


図-1 迷惑メール割合の推移

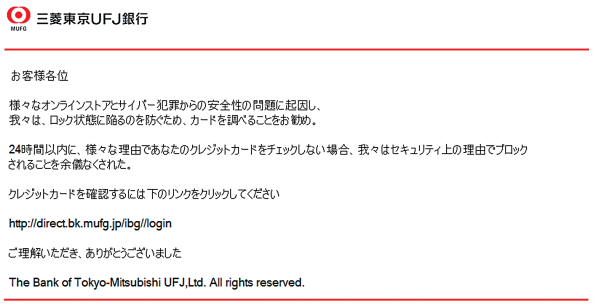
2.2.2 銀行を騙ったフィッシング

これまでも、銀行のウェブサイトを騙ったフィッシングサイトや、実在するオンラインバンキングへのアクセス時に出現する不正なポップアップ画面によるセキュリティ情報の搾取[*1]など、金融機関に関連する不正行為について触れてきました。今回は、2013年1月に大量送信された三菱東京UFJ銀行を騙った不正メールの事例について報告します。

2013年の1月から「Mitsubishi UFJ Financial Group」を騙ったメールの大量受信がありました。メールの内容は、いずれもHTML形式となっており、別のウェブサイトへのリンク先がついた外部にある画像ファイル(図-2)の情報を含んだものでした。画像上では、実在するドメイン名が示されていますが、画像全体がリンク先と関連付けられているため、どこの部分をクリックしても銀行とは関係のないサイトに移動するようになっていました(現在はサイト自体が存在していない)。また、三菱東京UFJ銀行[*2]を含んだ複数の銀行から、こうした電子メールについても警告されています。

今回の不正メールは、画像で示された文章の日本語の表現も不自然ですし、送信元情報も不正確でした。送信元情報には、次のドメイン名を使ったものがこの期間に多く受信されていました。

- mitsubishiufj.com
- financeufj.com
- ufjnet.jp
- ufjtokyo.com
- ufj.jp


三菱東京UFJ銀行

お客様各位

様々なオンラインストアとサイバー犯罪からの安全性の問題に起因し、
我々は、ロック状態に陥るのを防ぐため、カードを調べることをお勧め。

24時間以内に、様々な理由であなたのクレジットカードをチェックしない場合、我々はセキュリティ上の理由でブロックされることを余儀なくされた。

クレジットカードを確認するには 下のリンクをクリックしてください

http://direct.bk.mufg.jp/ibg//login

ご理解いただき、ありがとうございました

The Bank of Tokyo-Mitsubishi UFJ,Ltd. All rights reserved.

図-2 三菱東京UFJ銀行を騙ったメール内容

このうち、「ufj.jp」ドメイン名以外は実在していません。そのため、存在しないドメインからのメール受信を拒否する設定にしているメールサーバでは、メールそのものが届いていないはずです。実際、最近の標準的なメールサーバでは、受信しないように設定されているはずですが、メールサーバの管理者は、再度確認してみては如何でしょうか。また、実在するドメイン名を利用された場合でも、そのドメイン名を認証することによって不正に利用されているかどうかを確認することができます。認証方法やその意味についての詳細は、「2.3 メールの技術動向」で解説します。

2.2.3 迷惑メール送信元の動向

今回の調査期間での迷惑メール送信元地域の分析結果を図-3に示します。今回の調査では、迷惑メール送信元地域の1位は引き続いて中国(CN)となり、迷惑メール全体の26.6%を占めていました。割合も更に前回から2.6%増加しています。2位も前回と同様で日本(JP)となり、18.6%で割合も増加しています。3位は香港(HK)で7.9%で、前回の6位から増加しています。4位は韓国(KR、7.4%)、5位は米国(US、4.6%)、6位はバングラディッシュ(BD、3.2%)という結果でした。

前回(Vol.17)で3位だったサウジアラビア(SA)は、今回の調査では31位となり、前回は一時的な増加だったことになります。その一方で、今回の調査ではバングラディッシュが大幅に増加しました。これら、上位6地域(CN、JP、HK、

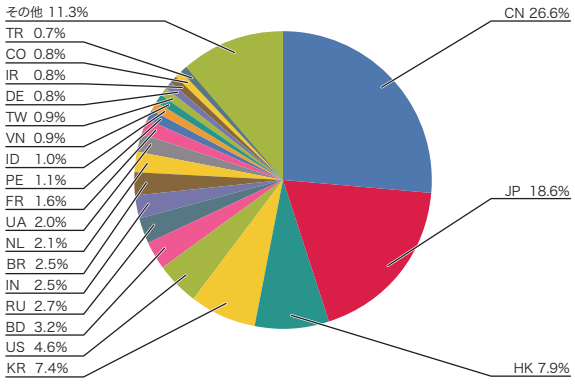


図-3 迷惑メール送信元地域の割合

＊1　警察庁:インターネットバンキング利用者の金融情報を狙った新たな犯行手口の発生について(http://www.npa.go.jp/cyber/warning/h24/121026.pdf)。
＊2　インターネットバンキングのパスワード等を騙し取る不審な電子メールにご注意ください(http://www.bk.mufg.jp/info/phishing/notice.html)。

KR、US、BD）の1年間（2012年1月2日～2012年12月30日）の割合の推移を図-4に示します。

この1年間で、中国（CN）は常に送信元地域で常に1位でした。その一方で米国（US）の割合は、段々と減少しています。今回急激に割合を増やしたバングラディッシュ（BD）は、今年の11月以降に急激に増加させていることが分かります。バングラディッシュを送信元とする迷惑メールを調べると、日本語で記述されたものが多かったので、日本向けの拠点がバングラディッシュに作られた可能性が高いといえます。米国や欧州など、以前は通信環境の整っている地域が送信元として主流でした。最近では、これら先進国地域での対策が進んで減少している一方で、前回のサウジアラビア（SA）の増加なども含め、通信環境がこれから発展していく地域からの迷惑メールが多くなってきています。迷惑メールを撲滅させるには、迷惑メール送信に対する対策を、グローバルで普及させていくことが今後も重要であると強く感じます。

2.3 メールの技術動向

ここでは、メールに関わる様々な技術的動向について解説します。今回は、メールの認証に関する複数の技術を解説します。

2.3.1 メールの認証技術

送られてくるメールを受信するべきかどうか、迷惑メールかどうかを判断する基準として、メール認証技術が利用されるようになってきました。これまでも、本レポートでは、送信ドメイン認証技術として、SPFやDKIM、その周辺技術としてDMARCの解説をしてきました。こうした送信ドメイン認証技術は、メールの送信者情報を認証するための技術ですが、メールに関連する技術には、それ以外の認証方法が送信ドメイン認証技術以前から提案されてきました。今回は、これらの認証技術の概要と、送信ドメイン認証技術との違いや背景などを解説します。

2.3.2 TLS（Transport Layer Security）プロトコル

TLS[*3]やそのベースとなった技術であるSSLは、HTTPの通信を暗号化したり、第三者認証機関を利用してそのドメインを認証するための技術として広く使われています。メールの配送プロトコルであるSMTPでも、通信路の暗号化や双方のメールサーバを認証するためにTLSを使うことができます[*4]。

SMTPでTLSを使うためには、SMTPのセッション冒頭で「STARTTLS」コマンドを送ります。これによりTLSのハンドシェークが開始され、以後は暗号化された通信路上で、通常のSMTPのやりとりが継続します。

米国を中心とした金融機関の集まりであるBITS[*5]では、メールのセキュリティ技術として、送信ドメイン認証技術のSPFやDKIMと共にTLSの利用を推奨しています[*6]。また、欧米の企業の一部では、取引先のメールサーバにTLSの利用を必須としているところもあります。

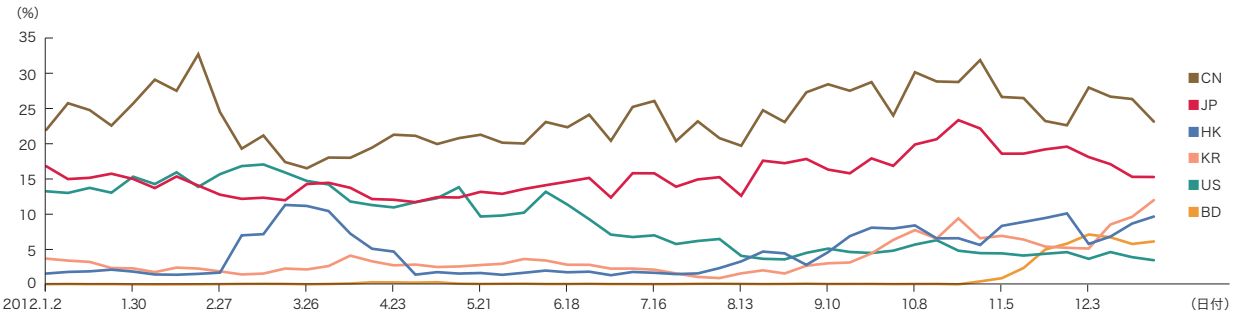


図-4 主要迷惑メール送信元地域の割合の推移

＊3　RFC2246、The TLS Protocol Version 1.0。
＊4　RFC3207、SMTP Service Extension for Secure SMTP over Transport Layer Security。
＊5　BITS（http://www.bits.org）。
＊6　BITS Email Security Toolkit: Protocols and Recommendations for Reducing the Risks（http://www.bits.org/publications/security/BITSSecureEmailApr2007.pdf）。

2.3.3 S/MIMEとDKIM

メールに画像やアプリケーションのデータファイルなどを一緒に送信する、いわゆる添付ファイルは、メールの本文部分を、MIME（Multipurpose Internet Mail Extensions）と呼ばれるパートごとに分割するフォーマットの規格によって実現されています。パートのデータタイプによって複数のRFCが追加されていますが、基本構造はRFC2045[*7]で示されています。

S/MIMEは、このMIMEの構造を利用して、メール本文を暗号化したりメールの署名情報を添付するため仕組みを定義しています[*8]。このうち、署名情報のパートを検証することで、メールを認証することもできます。

メールの認証に電子署名を利用するということで、S/MIMEはDKIM[*9]と仕組みがよく似ています。しかし、DKIMのRFCの中でも述べられているとおり、そのアプローチには以下のような違いがあります。

- メッセージの署名がヘッダ上に示されることにより、対応していないMUA（Mail User Agent）が本文に置かれる署名関連情報に困惑することがない
- 秘密鍵と公開鍵といった鍵管理に関して、信頼された認証局といった問題に関係しない
- 公開鍵の配布に関して新たなインターネットプロトコルを導入する必要がない

S/MIMEがIETFで最初にRFC化されたのは、1995年のRFC1847です。その後、DKIMの最初のRFCであるRFC4869が提案されたのが2007年ですので、12年ほどの時間が経過しているわけです。DKIMができた背景にもあるとおり、S/MIMEがその間普及して認証機能が有効に利用されていれば、DKIMが提案されることもなかったと思います。S/MIMEがあまり普及してこなかったのは、認証局の問題（主にコストなど）や、認証がメール受信者が利用するMUAで行われていることにより、結局のところ認証できないメールの削減に結びつかないこと、認証結果をどう利用すべきかの判断が受信者に任されてしまっていることなど、運用上の問題が大きかったでのはと考えています。

やはり、MUAの利用者など個々のメール受信者への利用を働きかけるよりは、メールを利用する事業者間で、信頼性を構築する枠組みを確立し、主要なメールの送受信を手軽に行えるような環境が必要だと考えています。そのためには、送信ドメイン認証技術の普及と、それを利用した信頼できるドメイン名の共有、ドメインの信頼性を維持する枠組みを確立が大事だと思います。DMARC[*10]は、これらの目標をうまく技術的に包含している期待の技術だと考えています。

2.4 おわりに

メールの受信側は、これまで送信されるメールについては基本的に受け取ることが前提となっていました。しかし、これまでも本レポートで報告してきたとおり、迷惑メールが受信するメールの大部分を占めるようになったり、メール利用者のセキュリティ的脅威が高まっている現在では、こうした前提をそのまま維持することが難しくなってきています。そのため、メールの利用者全体を信頼するモデルから、メールの利用ルールを設定し、その枠組みの中で信頼できる相手を選別あるいは優先するモデルを検討すべき時期がきているように感じます。そのための基盤として、送信相手を認証する送信ドメイン認証技術をまず普及させる必要があると考えています。

執筆者：

桜庭 秀次（さくらば しゅうじ）
IIJ プロダクト本部 アプリケーション開発部 戦略的開発室 シニアエンジニア。メッセージングシステムに関する研究開発に従事。特に快適なメッセージング環境実現のため、社外関連組織との協調した各種活動を行う。M^3AAWGメンバー及びJEAGボードメンバー。迷惑メール対策推進協議会及び幹事会構成員、送信ドメイン認証技術WG主査。（財）インターネット協会 迷惑メール対策委員。総務省 迷惑メールへの対応の在り方に関する検討WG構成員。

＊7　RFC2045、Multipurpose Internet Mail Extensions（MIME）Part One: Format of Internet Message Bodies。
＊8　RFC5751、Secure/Multipurpose Internet Mail Extensions（S/MIME）Version 3.2 Message Specification。
＊9　RFC6376、DomainKeys Identified Mail（DKIM）Signatures。
＊10　DMARCの詳細は、本レポートのVol.15で解説（http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol15_message.pdf）。