メッセージングテクノロジー

1.1 はじめに

これまでIIRでは、迷惑メールの量的な傾向やその内容について報告してきましたが、前回のIIR Vol.39でも述べたとおり、今回からは迷惑メールの対策技術も含めた、メッセージングにおける技術の解説や普及状況についてよりフォーカスしていきます。

今回は、送信ドメイン認証技術、特にDMARCの普及状況についての調査結果と、昨年に仕様がRFCとなった、メールの配送経路の暗号化技術であるTLSの接続ポリシーに関するMTA-STS、更に、そのレポーティング機能であるSMTP TLS Reportingについて解説します。また、メッセージングに関連する情報として、昨年開催されたJPAAWG 1st General Meeting / 迷惑メール対策カンファレンスと、JPAAWGについても報告します。

1.2 なりすましメールと情報漏えい

メールの送信者になりすまして送られるメールは、フィッシングメールやBEC (Business Email compromise)など、事例として名称が付けられるほど、様々な問題を引き起こす要因となっています。これらなりすましメールによる被害は、金銭的な被害や各種IDやパスワードの搾取、マルウェア感染などによって生じる機密情報や個人情報の漏えいなど、被る被害も深刻かつ多岐に渡っています。

最近では、こうした事象に拍車をかけるような事案も発生しています。様々なWebサービスからの情報漏えいが立て続けに発生しており、これら漏えいする情報の中には、メールアドレスが含まれていることがほとんどで、多くの迷惑メールが的確に送信されるようになりました。昨年も大手ホテルチェーンから大量の個人データが漏えいしたとのニュースがあり、それ以降漏えいしたメールアドレス宛てに多くの迷惑メールが送られるようになりました。その中には、親切にもログイン時に設定したパスワードを教えてくれるものもあります。Web経由で利用できるサービスは便利な側面がありますが、それを提供している側のセキュリティについては、必ずしも信頼できるものばかりとは限りません。Webサービスで設定するパスワードなどの強度や共通で設定している利用サービスの種類については、利用する側でもきちんと把握しておくことが必要です。

1.3 送信ドメイン認証技術の普及状況

なりすましメール対策には、送信ドメイン認証技術が有効であることはこれまでも述べてきました。メール受信側としてなりすましメールを検知するための認証処理と、メール送信側としてなりすましメールと区別できるようにするためのいくつかの設定が、送受信双方で必要です。

送信ドメイン認証技術を普及させるには、まず現在の普及状況を認識することが必要です。ここで、メール受信側から見た流

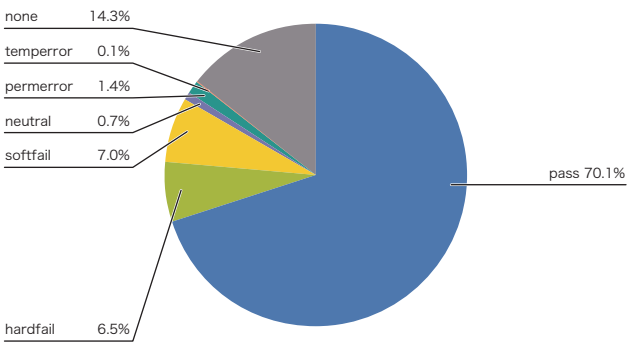

図-1 SPFの認証結果割合

量ベースでの送信側の普及状況と、登録ドメイン名に対する導入割合について、それぞれ調査結果を報告します。

1.3.1 流量ベースでの普及率

ここでは、メール受信側から見た送信側の設定の普及状況を、IIJのメールサービスで2019年4月に受信したメールの認証結果を示して解説します。

図-1は、SPFの認証結果の割合を示したグラフです。受信メール全体のうち、SPFでの認証結果が「none」であった割合は14.3%でした。「none」はSPF認証できなかったことを示す結果ですので、逆に言えば受信したメールの85.7%はSPFを導入した送信者からのメールだと言えます。昨年の同時期（2018年4月）の「none」の割合は16.0%でしたので、ほぼ同レベルで受信メールの大部分がSPF認証が可能なレベルまで普及してきた、と言えます。

図-2は、DKIMの認証結果の割合を示したグラフです。こちらも同様に認証結果「none」の割合は62.2%でしたので、受信メールのうち送信側がDKIMを導入している割合は4割未満ということになります。昨年同時期の認証結果「none」の割合は64.2%でしたので、DKIMの導入割合もそれほど大きな変化はなかったと言えます。

図-3は、DMARCの認証結果の割合を示したグラフです。同様に認証結果「none」の割合は76.9%でしたので、受信メールのうち送信側がDMARCを導入しているドメイン名の割合は、2割程度ということになります。DMARCはSPFあるいはDKIMの認証結果を利用して認証する技術ですので、SPFやDKIMより認証割合が低くなることは予想できます。しかしながら、メール再配送の課題はありますが、SPFだけでもDMARC認証はできますので、SPFの普及率が8割強だったのと比べれば、あまりにも低い割合です。

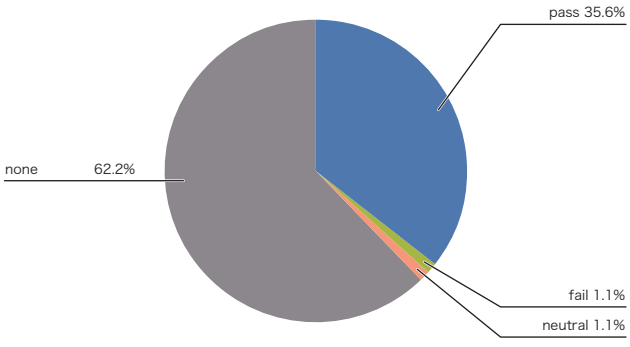

図-2 DKIMの認証結果割合

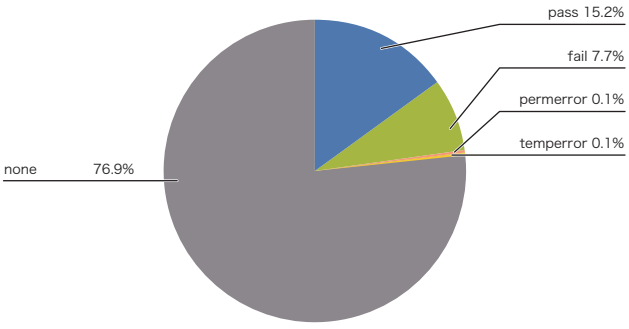

図-3 DMARCの認証結果割合

このDMARCの調査結果について、2016年1月からの推移を図-4に示します。調査当初は、DMARCの認証結果「none」の割合は87.5%でしたので、ほぼ3年間で流量ベースでの導入割合が1割程度増えたことになります。比率ではおおむね倍増しました。グラフ上でも、認証失敗を示す「fail」の割合の変化は時期によって変わりますが、認証失敗も含め全体として認証できているメールの割合は少しずつ増えていることが分かります。

1.3.2 登録ドメイン名ベースでの普及率

次に、登録されているjpドメイン名の中で、SPFあるいはDMARCを導入しているドメイン名の調査結果を示します。前回(Vol.39)でも述べたとおり、jpドメイン名を管理する日本レジストリサービス(JPRS)と(一財)日本データ通信協会は、送信ドメイン認証技術の普及状況調査を目的として共同研究契約を結んでおり、筆者は日本データ通信協会の客員研究員の立場で普及状況を調査しています。

2018年3月からの調査結果の推移を図-5に示します。調査結果は、jpドメイン名の登録種別ごとに、メールに利用しているドメイン名であることを示すMXレコードが設定されているドメイン名に対して、DMARCレコードが設定されている割合の推移を示しています。jpドメイン名全体では、5月の最新調査では、0.95%という結果となりました。登録種別では、ad.jpドメインが最も高い割合となっていますが、それでも3.4%です。次に割合が高いのが、種別ごととしては登録数が少ないため、段階的に増加しているgo.jpドメインで2.1%でした。

NISC(内閣サイバーセキュリティセンター)が公表している資料[*1]では、政府機関などの情報セキュリティ対策のための対策事項の中で、メールのなりすましの防止策として、SPF、DKIM、DMARCの送信側及び受信側の対策を行うこと、と示されています。よって、今後go.jpドメイン名でのDMARCレコードの設定割合が増えていくことが期待されます。なお、

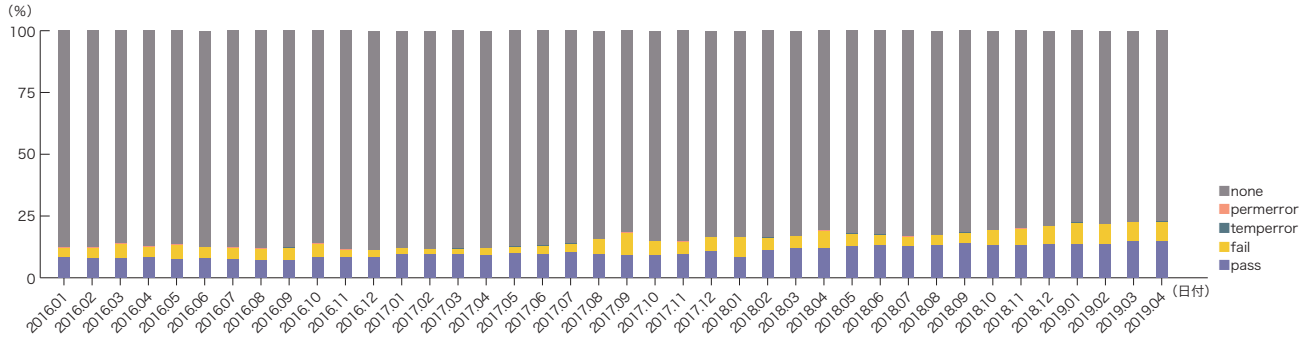

図-4 DMARCの認証結果割合の推移

*1 「政府機関等の対策基準策定のためのガイドライン(平成30年度版)」(https://www.nisc.go.jp/active/general/pdf/guide30.pdf)。

SPFレコードの設定割合では、go.jpは登録種別の中では最も高く、92.7%でした(図-6)。

同様に、jpドメイン名全体でのSPFレコードの設定割合は59.7%でした。前回(Vol.39)報告した、2018年1月時点の56.9%から2.8%増加したことになります。SPFの設定割合が未だ増加しているということは、SPFの認知度がかなり高くなっているものと考えられます。残念ながらDMARCの増加率はSPFよりかなり低い数値です。DMARCの認知度をより高める工夫が必要です。

1.3.3 海外の普及率について

米国に本社があるValimail社の調査[*2]によれば、米国連邦政府のドメインの80%がDMARCレコードを設定しているとのことです。これは、調査している各業界の中でも最も高い割合でした。前回も報告したとおり、米国国土安全保障省による法的拘束力のある命令[*3]により増加したものと考えられます。また、DMARC技術を推進する団体dmarc.orgによれば[*4]、DNSにDMARCレコードを設定しているドメイン名が、2018年で2.5倍以上に増えたことが報告されています。

1.4 メールの配送経路の暗号化

今やメールは単なるメッセージ交換だけではなく、添付ファイルの機能(MIME)により様々なデータの転送の手段にも用いられています。その一方で、データを含むメールがどのような配送経路で送られるのか、またデータが漏えいする危険性がどの程度あるのかなど、利用者側からはあまり考慮されていないようにも思えます。メール配送のプロトコル、SMTPでは拡張機能としてTLS(STARTTLS)が利用できます。ここでは、こうした従来のSTARTTLSの課題と、それを解決するための手段として規格が設けられたMTA-STS、SMTP TLS Reportingについて解説します。

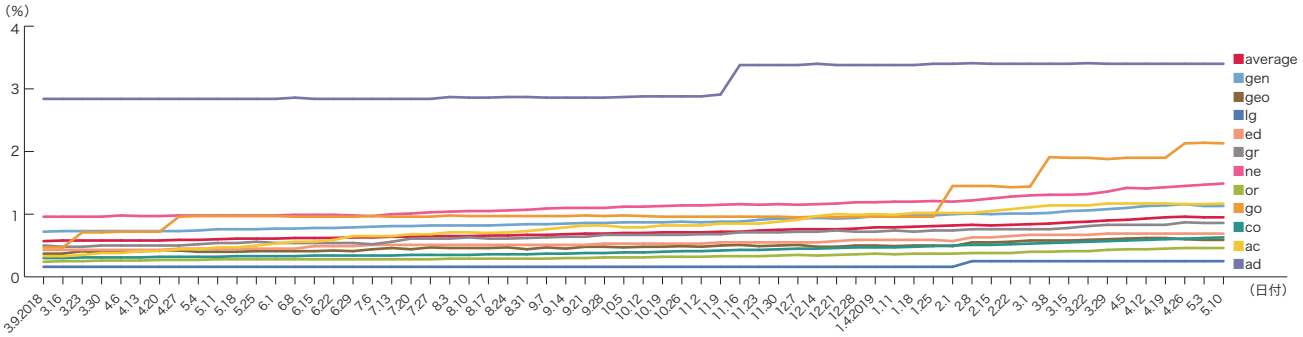

図-5 jpドメインのDMARCレコード設定割合の推移

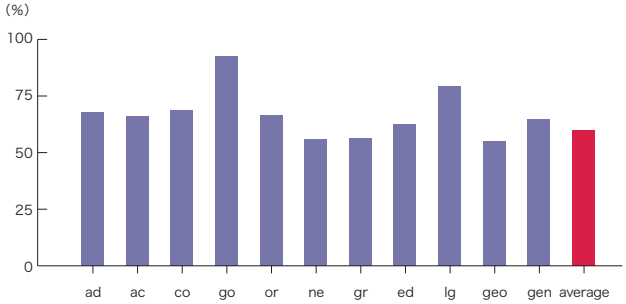

図-6 ドメインのSPFレコード宣言割合

*2 Email Fraud Landscape, Q4 2018 (https://www.valimail.com/resources/email-fraud-landscape-q4-2018/)。
*3 DHS, "Binding Operational Directive 18-01" (https://cyber.dhs.gov/bod/18-01/blank)。
*4 DMARC Policies Up 250% In 2018 (https://dmarc.org/2019/02/dmarc-policies-up-250-in-2018/)。

1.4.1 STARTTLSの課題

メール配送時の通信経路を暗号化するには、SMTPの拡張機能であるSTARTTLS（TLS）を利用します。手順としては、受信メールサーバ側がSTARTTLSに対応している場合（接続時の応答で判断できます）、送信側がSTARTTLSコマンドを送信することで、TLSセッションが開始されます。そのため、以下のような条件では、通信経路の暗号化ができなくなってしまいます。

- **受信メールサーバがSTARTTLSの機能を持っていない（STARTTLSに対応した応答メッセージを返さない）**
- **STARTTLSのコマンドを送信し、TLSセッションを開始しようとしたが、利用できるTLSのバージョンやCipher Suitesが合わなかった**

Cipher Suitesは、暗号化のためのアルゴリズムや鍵長などの組み合わせを示したもので、送受信側双方で同じものを利用できなければ暗号化通信は行えません。こうしたSTARTTLSコマンドが実行できない場合、多くの送信メールサーバは、暗号化せずに従来の平文によるメール送信の手順に移行します。このような仕組みでは、いわゆる中間者攻撃のように、SMTPセッションを仲立ちし、本来の受信サーバのSTARTTLSに関する応答を削除することで、平文による送信を行わせることで、メールの内容を搾取することが可能になります。こうした手法は、ダウングレード攻撃とも呼ばれます。

1.4.2 MTA-STSとTLSRPT

MTA-STS[*5]は、メール受信側のドメインが、DNSとHTTPSを利用して、受信側のポリシーを表明する仕組みです。この仕組みを利用することで、メール送信前にTLS認証をサポートしているか、TLS接続がうまくいかなった場合に送信側が取るべき動作を知ることができます。

受信側のドメインが用意すべき設定は、以下のとおりです。

（1）MTA-STSレコードを設定
（2）MTA-STSポリシーを取得できるようwell-knownパスに設定

MTA-STSレコードは、通常はメールの宛先ドメインに"_mta-sts"をつけたドメインのTXTレコードであって、先頭が"v=STSv1"であるものです。例えば、メールの宛先ドメインが"example.com"である場合、以下のように設定されることになります。

```
_mta-sts.example.com.  IN TXT "v=STSv1; id=20160831085700Z;"
```

idパラメータは、ポリシーの変更時に把握できるよう設定する文字列です。送信側は、まずこのMTA-STSレコードを参照することで、受信側ドメインがMTA-STSに対応しているかどうかを確認することができます。

*5　SMTP MTA Strict Transport Security, RFC8461

次に、MTA-STSポリシーを取得する方法です。対象のドメインに"mta-sts"を付けたポリシードメインのwell-knownパスを参照します。well-knownパスは、RFC5785で示されていますが、MTA-STSの場合、以下のパスに対してHTTPSのGETメソッドで取得します。

```
https://mta-sts.example.com/.well-known/mta-sts.txt
```

MTA-STSポリシーは、key/valueペアを改行(CRLF)で区切った形式で、現在指定可能なパラメータを表-1に示します。

"max_age"は、ポリシー参照する側がキャッシュしておく期間を示します。"mx"は、MXレコードで設定されるホスト名のパターンを指定します。複数のホストあるいはパターンを設定可能です。動作モード("mode")で設定できる値を表-2に示します。これらのモードにより、送信側のMTAは送信を続けるべきかどうかを判断します。

MTA-STSポリシーの設定例を以下に示します。

```
version: STSv1
mode: enforce
mx: mail.example.com
mx: *.example.net
mx: backupmx.example.com
max_age: 604800
```

MTA-STSでのポリシー検証が失敗した場合や成功した場合、またそれ以外のDANE[*7]などの仕組みで、送信側にレポートを送るための仕様がTLSRPT[*6]です。送信側は、レポートを受け取るために、DNSを利用してTLSRPTポリシーを表明します。TLSRPTに対応したメール受信側は、まず送信側のドメインでこのTLSRPTポリシーが設定されているかどうかを判断し、取得できた場合でレポート先が指定されている場合にレポートを送信することになります。TLSRPTポリシーの設定は、対象のドメイン名に"_smtp._tls"を追加したドメイン名となります。設定するパラメータは、DMARC[*8]によく似ていますが、最初のバージョン情報が"v=TLSRPTv1"であること、レポート先を示す"rua="にメール("rua=mailto:")以外にHTTPS ("rua=https:")も利用できること、が異なります。以下にTLSRPTポリシーレコードの設定例を示します。

```
_smtp._tls.example.com. IN TXT "v=TLSRPTv1;rua=mailto:reports@example.com"
```

メールで、"rua=mailto:"で指定された宛先にレポートを送る場合は、送信側のドメインでDKIM署名されている必要があります。このDKIM署名する送信側のDKIMレコードには、サービスタイプを示す"s=tlsrpt"が設定されているべき(SHOULD)となっています。

表-1 MTA-STSポリシー

パラメータ	意味
version	バージョン(値はSTSv1)
mode	ポリシー検証が失敗した場合の送信側の動作
max_age	ポリシーの存続期間(秒)
mx	MXレコードのパターン

表-2 MTA-STSポリシーモード

動作モード	意味
enforce	ポリシー検証やTLSが失敗した場合に配送してはならない
testing	送信側のMTAがTLSRPT[*6]を実装している場合レポート送信し、メール送信を継続
none	明示的にMTA-STSポリシーを適用しないことを示す

*6 SMTP TLS Reporting, RFC8460
*7 The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA, RFC6698
*8 Domain-based Message Authentication, Reporting, and Conformance (DMARC), RFC7489

```
selector._domainkey.example.com  IN TXT
      "v=DKIM1; k=rsa; s=tlsrpt; p=MIf4qwSZfase4fa=="
```

メールで送信する場合、DMARCレポートと同様に、添付ファイル形式(MIME)で送信します。同様にHTTPSでレポートを送信してもらうためのTLSRPTポリシーレコードの例を、以下に示します。

```
_smtp._tls.example.com.  IN  TXT  "v=TLSRPTv1;  rua=https://report-
ing.example.com/v1/tlsrpt"
```

レポートデータは、メールあるいはHTTPSの両方の場合で、圧縮形式で送るべき(SHOULD)となっています。圧縮あるいは圧縮しない場合でも、メディアタイプは実体に即した形で指定します("application/tlsrpt+gzip"あるいは"application/tlsrpt+json")レポートデータの形式は、DMARCレポートとは異なり、JSON形式となっています。データに含まれるパラメータについては、ここでは省略しますが、詳細はRFC8460を参照してください。

1.5 JPAAWG について

これまで、国際的な迷惑メール対策組織であるM^{3}AAWG[*9]について、IIRでも何度か触れてきました。最近ではメール以外にも、より関連するセキュリティ分野も含めて、様々な議論や検討を行う場となっています。また最近では、M^{3}AAWGメンバーの多い北米や欧州だけでなく、他の地域とも連携していくために、各地で地域的な組織の立ち上げも支援しています。最初に立ち上がったのが、南米及びカリブ地区によるLAC-AAWGです。同様にアフリカ地域でのAFR-AAWGについても検討及びサポートを行っています。となると、次に残された地域のアジアをどうするか、ということになります。

M^{3}AAWGでは、その設立時からIIJがメンバーとして長年活動してきましたが、日本からの参加メンバーが欧米に比べて

*9　Messaging, Malware and Mobile Anti-Abuse Working Group

なかなか増えない状況が続いてきました。我々も参加者をより増やすために、M³AAWGの活動を日本で紹介したり、時々M³AAWG General Meetingを日本あるいはアジア地域で開催できないかなどと打診してきました。そうした中、LAC-AAWGのように、M³AAWGと連携した各地域の活動をM³AAWGが支援する動きが出てきました。こうした動きの中で、M³AAWGと日本から参加しているメンバーとの間で、JPAAWGを設立しようと動き出すことになりました。

JPAAWG（Japan Anti-Abuse Working Group）は、あくまでM³AAWGとは独立した組織ですが、M³AAWG側から多くの支援を得ています。昨年2018年11月8日に開催されたJPAAWG 1st General Meetingは、これまで10年以上開催してきた（一財）インターネット協会の迷惑メール対策カンファレンスと併催する形で、多くの講演者及び参加者を集めました。講演者にはM³AAWGのチェア及び主要メンバーも加わりました。このイベントの成功もあり、JPAAWGは継続して活動できるための準備をいくつか行い、2019年5月30日にようやくJPAAWGとして設立することができました。今後のJPAAWGの活動に関心を持っていただければと考えています。

1.6 おわりに

今回は、メール配送の暗号化を確実に実施するための技術仕様MTA-STSと実施状況を把握するためのTLSRPTについて解説しました。これまでも、送信ドメイン認証技術DAMRC やARC、DANEなどについて紹介や技術解説してきましたが、メールに関連する技術仕様は、BIMI（Brand Indicators for Message Identification）やJMAP（JSON Meta Application Protocol）など、新たな仕様とともに進化しています。IIRでは、これからも新しい技術仕様や、そうした仕様が生まれる背景なども含めて解説していきます。

執筆者：
櫻庭 秀次（さくらば しゅうじ）
IIJ ネットワーク本部 アプリケーションサービス部 担当部長。コミュニケーション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、社外関連組織と協調した各種活動を行う。M³AAWGの設立時からのメンバー。Japan Anti-Abuse Working Group（JPAAWG）会長。迷惑メール対策推進協議会 座長代理、幹事会 構成員、技術WG 主査。一般財団法人インターネット協会 迷惑メール対策委員会 委員長。Email Security Conferenceプログラム委員。一般財団法人日本データ通信協会 客員研究員。一般財団法人日本情報経済社会推進協会（JIPDEC）客員研究員。