インターネット 10min 分 講座

おさえておきたい基本や、最新動向を解説するコーナーです。

電子メールにおけるセキュリティ技術とセキュリティ・ニーズ

1 はじめに

電子メールは、職場や個人同士の連絡に使われる、日常的なコミュニケーションの手段ではないでしょうか。SNSやオンラインのメッセージングのサービスが増えていますが、電子メールは多くの人に告知するために便利で、また、以前にやり取りされた文章の内容や添付ファイルを取り出しやすいといった、他のものでは代替しきれない特徴を備えています。電子メールが別のものに変わることなく使われ続けているため、迷惑メールへの対策が重要であり続けるとともに、企業などの組織の間で送受信されるファイルのセキュリティが議論されているとも言えます。

ユーザーの視点で考えた時に従来の電子メールのセキュリティ技術は、リスクや不安になる要素に対して、どのような役割を果たしているのでしょうか。そして、ユーザーの安全や安心につなげていくためには、今後どのような課題があるのでしょうか。本稿では、前半で従来の電子メールのセキュリティ技術を概観し、後半で課題と今後について考察します。

2 電子メールにおけるセキュリティ技術

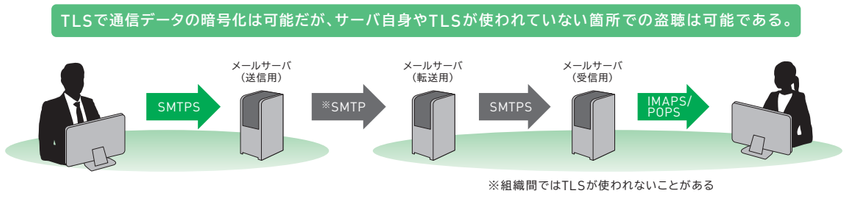
電子メールにおけるセキュリティのために、さまざまな技術が複合的に使われています。

表1：大きく三つに分類される電子メールのセキュリティ技術

分類	電子メールのセキュリティ技術
メールメッセージ	S/MIME・PGP/MIME
ドメイン名とメールサーバ	SPF・DKIM・DMARC
送受信プロトコル	SMTPS・IMAPS・POPS

一つ目の送受信プロトコルのセキュリティとは、送信者のメールクライアントとメールサーバ間の通信、配送に使われるメールサーバ間の通信、受信者のメールサーバと受信者のメールクライアント間のセキュリティです。二つ目の送信者のドメイン名に関するセキュリティ技術とは、送信メールアドレスのドメイン名を騙り、他のメールサーバからスパムメールが送られることに対するものです。三つ目のメッセージにおけるセキュリティ技術とは、メール本文の書き換え（改ざん）を検出したり、送信者が本人であるかどうかを確認したりする認証の技術です。これら三つの分類について説明していきます。

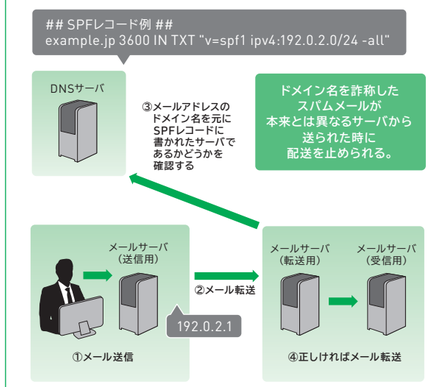
図1：送受信プロトコルにおけるセキュリティ技術



○送受信プロトコルに関するセキュリティ

メールクライアントから送信用メールサーバへ、そしてメールを転送するサーバとサーバ間の転送には、プロトコルとしてSMTP（Simple Mail Transfer Protocol）が使われます。このSMTPをTLS（Transport Layer Security）を使って行う方式はSMTPSと呼ばれます。このSMTPSには、TLSセッション確立後にSMTPを使う方式と、SMTPの途中でTLSに切り替えるSTARTTLS※1の2種類があります。また、受信用のメールサーバとメールクライアントの間でTLSを使う方式には、POPS※2、IMAPS※2があります。いずれも、TLSを使うことで通信データを暗号化し、メールが送受信される時のメールクライアントとメールサーバ間の通信を、盗聴から守る仕組みです。しかし、偽のメールサーバと暗号通信をしてしまうと、そのメールサーバで内容が傍受できてしまうため、TLSのサーバ認証を適切に行う必要があります。ただ、社外や組織をまたいだメールサーバの間では、TLSのサーバ認証が必ずできるわけではないため、SMTPSではなく、SMTPが使われることが多いようです。

図2：送信者のドメイン名に関するセキュリティ技術



○ドメイン名に関するセキュリティ

電子メールのドメイン名と送信サーバに関するセキュリティで、送信ドメイン認証と呼ばれるものです。スパムメールや送信者になりすましたメールは、正しい送信者のドメイン名を騙って送られることがあります。ドメイン名を騙ることで、受信者が開いてしまう可能性が上がったり、送信元を制限しているメーリングリストの制限に引っかからなくなったりします。

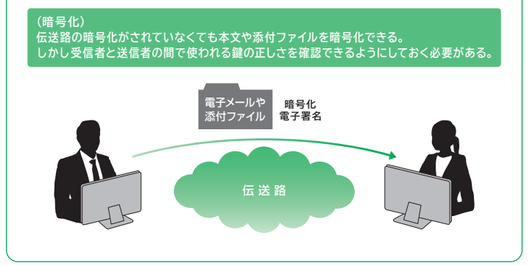
送信ドメイン認証の仕組みとして知られるSPF※3は、メールアドレスのドメイン名とDNSの検索結果を使って、送信したメールサーバが正しいものかどうかを確認する仕組みです。

DNSのゾーンに登録されたサーバ以外がドメイン名を騙ってメールを送信した場合、受信側のメールサーバで受信を拒否できます。Sender ID※4も、DNSに送信サーバのIPアドレスを登録して使う仕組みです。

DKIM※5は、送信メールサーバが署名を行い、DNSに登録しておいた鍵を使って、受信メールサーバが検証する仕組みです。署名検証に成功しなければ、本来のサーバから送られたメールではないと判定でき、拒否できます。

DMARC（Domain-based Message Authentication, Reporting and Conformance）は、SPFやDKIMと併用し、配送の判断を行うための仕組みです※6。DNSに登録された情報を使って、送信元メールアドレスのドメイン名とメールサーバの正しさを確認する点は、SPFなどと共通しています。

図3：電子メールのメッセージにおけるセキュリティ技術



○メッセージにおけるセキュリティ

本人が出したものなのか、内容が途中で改ざんされていないか、盗聴されても内容がわからないようになっているかという観点で、異常を発見できます。S/MIME※7や、OpenPGPを使った電子メール（以下、PGP/MIMEと呼ぶ）がこの分類に入ります。S/MIMEとPGP/MIMEは、電子署名とメール本文の暗号化を行うことができる点は共通しています。近年、スマートフォンやさまざまなWebサービスでも対応し始めました。

S/MIMEとPGP/MIMEで大きく異なる点は、電子署名や暗号化で使われた鍵が、本人のものであるかどうかを確認する方法です。S/MIMEは、認証局から発行されたX.509形式の電子証明書を使います。受信者が電子署名の検証を行うためには、認証局の証明書をあらかじめ確かな手段で入手し、その認証局証明書を証明書の検証に使うように設定する必要があります。この設定は、証明書の正しさを確認するために、その認証局を信頼し依存して有効性を判断する意味を持つた

※1 SMTP Service Extension for Secure SMTP over Transport Layer Security, https://tools.ietf.org/html/rfc3207
※2 Using TLS with IMAP, POP3 and ACAP, https://tools.ietf.org/html/rfc2595
※3 Sender Policy Framework（SPF）for Authorizing Use of Domains in Email, Version 1 https://tools.ietf.org/html/rfc7208
※4 Sender ID: Authenticating E-Mail, https://tools.ietf.org/html/rfc4406
※5 DomainKeys Identified Mail（DKIM）Signatures, https://tools.ietf.org/html/rfc6376
※6 dmarc.org - Domain Message Authentication Reporting &Conformance https://dmarc.org/
※7 Secure/Multipurpose Internet Mail Extensions（S/MIME）Version 3.2 Message Specification, https://tools.ietf.org/html/rfc5751
※8 社員・職員全般の情報セキュリティ対策，総務省，http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/staff/index.html
※9 電子メール利用時の危険対策のしおり，独立行政法人情報処理推進機構，https://www.ipa.go.jp/security/antivirus/documents/07_mail.pdf
※10 悪質メールトレンド情報，一般財団法人日本産業協会，http://www.nissankyo.or.jp/mail/trend/trend.html

め、「トラスト」と呼ばれます。S/MIMEに対応したメールソフトでは、インストール直後から、数多くの認証局証明書をトラストするようになっています。

PGP/MIMEは、OpenPGPをメールの拡張であるMIME（Multipurpose Internet Mail Extensions）に適用したもので、鍵が本人のものであるかどうかは、OpenPGPの仕組みや使い方の中で確認されます。基本的に「Web of Trust」と呼ばれる方法で、鍵の確からしさをユーザー同士の鍵の確認度合いと、鍵に対する署名を通じて確認できるようになっています。例えば、ある人の鍵が確かに本人に保有されていることがわかったときに、そのことを示す署名をつけておきます。直接会って確認した場合には、確認の度合いは高く設定されます。その鍵に複数の署名がついていると、本人が鍵を保有していることの確からしさが高いと判断できます。ユーザー本人が鍵を生成し、やり取りする相手の鍵を確認していくため、使い方をマスターしたユーザーにとってはチェックの結果が確実である一方、ユーザー自身が鍵をきちんと管理していく必要があります。S/MIMEの場合は、相手の鍵の確からしさをユーザー自身ではなく認証局が確認しておきます。一定の確認がなされた鍵を多くのユーザーが使う場合には認証局を使うS/MIMEが向いていると言えます。

3 電子メールにおけるセキュリティ・ニーズ

本節からは視点を変えてみます。電子メールを利用するユーザーの視点では、どのようなリスクや不安要素があるのでしょうか。そこに重大なものがあれば、優先して対策を取るべきであり、いわばセキュリティ・ニーズがあると言えます。 総務省のガイド※8や独立行政法人情報処理推進機構（IPA）のしおり※9などを元に、電子メールを使うにあたってのリスクや、ユーザーが不安になる状況を挙げてみます。

（ア）誤送信
本来とは異なるユーザーのメールアドレスを入力した状態で、メールを送信してしまったようなケースです。機密にすべき情報が入っていた場合には、情報が漏えいしてしまうということになります。

（イ）内容が不適切であったが送られてしまったメール
ユーザーの視点では、相手に迷惑をかけてしまうことや、送信者自身が恥ずかしい思いをすることも、リスクであると言えます。電子メールは、管理外のメールサーバに配送されてしまうと削除が難しくなりますので、配送後は根本的な対策を取ることができないと言えます。

（ウ）詐欺メール
架空請求や、不当に会費を請求するようなサイトに誘導するメールです。不当な請求は数多く報告されています※10。

（エ）標的型攻撃、ばらまき型マルウェア付きメール
マルウェアが入ったファイルが添付されたメールや、本文に書かれているURLにアクセスするとマルウェアをダウンロードしてしまうようなメールです。マルウェアに感染すると、機密にすべきファイルが漏洩してしまったり、不正アクセスの踏み台としてコンピューターが使われてしまったりします。メールは巧妙に書かれていることがあり、数多くのユーザーがいる場合にマルウェアにまったく感染しないとは考えにくいため、善後策が必要だと考えられます。

（オ）スパムメール
スパムメールとは、大量に届く宣伝メールなどです。ある統計によると、受信したメールの50%が、スパムメールであるという報告があります※11。スパムメールが増えすぎてしまうと、メールシステムそのものが使えないものになってしまう恐れがあります。

（カ）メールの内容や添付ファイルが第三者に見られてしまうリスク
暗号化を行う仕組みを利用していない場合、メールの本文は平文でやり取りされます。機密にしたい内容であっても、メールクライアント上、メールサーバ上、そして通信路のいずれにおいても第三者に見える状態であり、送信者にとっての不安要素であると言えます。

（キ）自組織になりすまされてしまうリスク
顧客関係のあるようなユーザーに対して、第三者によってなりすまされたメールが送信されてしまい、フィッシング詐欺が起きてしまうようなリスクです。銀行やWebサービスを行っている大手事業者の顧客に、よく起こり得るリスクです。

これらのリスクや不安要素に対して、2節で概説したセキュリティ技術は、どのような位置づけにあるのでしょうか。考察していきます。

4 リスクや不安要素に対してセキュリティ技術はどう位置づけられるのか

（ア）「誤送信」と（イ）「内容が不適切であったが送られてしまったメール」は、ユーザー自身が本文を作成し、送信先を指定しているため、送信ドメイン認証や暗号化を行ったとしても、起きてしまうリスクであると言えます。対策としては、第2節で述べたものではなく、送信前に宛先を再確認するメールソフトの機能や、送信までに時間がおかれて、それまでであれば送信を取りやめることができるサーバ製品・Webサービスを使うといったことが考えられます。

（ウ）「詐欺メール」に関しては、送信ドメイン認証とS/MIMEやPGP/MIMEが、対策技術に位置付けられます。しかし、ドメイン名が詐称されていないでたらめなメールアドレスが使われた詐欺メールで、しかもS/MIMEやPGP/MIMEの電子署名を確認する環境が整っていない場合には、これらの技術に頼ることができないため、ユーザー自身が詐欺への対策を取れるようになっておく必要があります。

送信ドメイン認証と、S/MIME、PGP/MIMEの組み合わせにおける課題について、次の節で述べます。

（エ）「標的型攻撃、ばらまき型マルウェア付きメール」と（オ）「スパムメール」は、送信ドメイン認証を使って詐称されたメールアドレスのメールを防ぐとともに、メールサーバ上やメールクライアントで動作する、スパムフィルターやマルウェア対策ソフトを使うといった対策が考えられます。

（カ）「メールの内容や添付ファイルが第三者に見られてしまうリスク」と、（キ）「自組織になりすまされてしまうリスク」に対しては、送信ドメイン認証や、S/MIME、PGP/MIMEが対策として位置づけられます。しかし、対策技術として採用していく場合には、ユーザーの視点でのリスクや不安要素に対して、役立つ形を考えていかなければなりません。

5 送信ドメイン認証とS/MIMEとPGP/MIMEにある課題

送信ドメイン認証は、ドメイン名が詐称されたメールをサーバが受信しないという形で運用されていますが、認証されたかどうかは技術に詳しくないユーザーには分かりません。後述するS/MIMEで送信メールアドレスが確認されていても、ドメイン名が詐称され、加えてトラストされている認証局のうちのどれかが送信メールアドレスを含む証明書を発行してしまうと、ユーザーには有効な電子署名として表示されることになってしまいます。送信ドメイン認証が行われたドメイン名なのかどうかを含めて、ユーザーに表示していくことが考えられます。このような取り組みには、「なりすましメールに対するJIPDECの取り組み」※12があります。

S/MIMEが広く普及していない状況下でも確実な対策を取れるようになるためには、署名検証を行うユーザー環境における表示と、トラストの課題が考えられます。S/MIMEの証明書には、Webサーバ証明書におけるEV（Extended Validation）証明書のような仕組みがなく、ユーザーには電子署名の検証結果が一律に見えてしまいます。ユーザーが感知していない、数多くの認証局があらかじめインストールされているため、2011年に起きたDigiNotar事件※13やComodo事件※14のように、不正証明書発行が起きてしまう可能性もあります。一見、ユーザーには正しい署名がついているように見えて、実は詐欺メールだったという事態は避けたいところです。

現在、利用できる電子証明書という意味では、商用認証局発行局の証明書や、JCAN証明書※15の他、組織内で運用されているプライベート認証局の証明書をスマートフォンで使うことが可能であり、そのハードルは下がりつつあると言えます。S/MIMEやPGP/MIMEを電子メールの暗号化に使うためには、やり取りする相手と適切にトラストの設定を行う必要があります。例えば、ファイルの送受信を行う取引先とは、共通の認証局やPGPの署名鍵を用意しておき、業務ではそれらを使って認証したやり取りに限定する、署名や暗号化が行われていないメールは送信されないように設定する環境を設けてみる、といった方法も考えられます。現在の利用環境では実施できなくても、新たな環境を設けて試してみる、暗号メールの業務利用を検討してみるといった活動は、対策の選択肢を広げるという意味で意義のあることだと考えられます。

6 おわりに

本稿では、電子メールのセキュリティ技術について概説したあと、ユーザーの視点でリスクと不安要素への対策として、それらがどう位置づけられるのかを述べました。セキュリティ技術は導入や構築に目がいきがちですが、視点を変えて、ユーザーが何に困っていて、どのような対策が必要とされているのかという検討の、例になればと思います。今回は触れることはできませんでしたが、インシデント対応の業務が発生した時にも、その対応業務を減らすためにはどうすればいいのか、今回の例では、本来電子メールのセキュリティはどうあるべきなのかといった機会を考えるようなテーマにもつながればと思います。

（JPNIC 技術部／インターネット推進部 木村泰司）

※11 迷惑メールの統計，一般財団法人日本産業協会，
http://www.nissankyo.or.jp/mail/graph/graph.html
※12 なりすましメールに対する JIPDEC の取り組み，一般財団法人日本情報経済社会推進協会，
http://www.dekyo.or.jp/soudan/image/anti_spam/archive/2016/2016_d6.pdf

※13 DigiNotar事件
オランダの認証局DigiNotarが侵入され、Google社やFBIを含む、Webサーバの証明書が不正に発行された事件。2011年8月に明らかになりました。証明書を使った偽のサーバを用意してDNSなどに細工を行うと、ユーザーにはGoogle社やFBIのサーバに接続し、サーバ認証が成功しているように見えてしまいます。

※14 Comodo事件
2011 年 4 月に起きた、米国の大手認証局事業者 Comodo の認証局が侵入された事件。Google 社や Yahoo 社を含むサーバ証明書が、不正に発行されたとされています。

※15 JCAN 証明書，一般財団法人日本情報経済社会推進協会，
https://jcan.jipdec.or.jp/jcan/