インターネットでの不正行為その傾向と対策

今回は電子メールのお話です。あなたは普段どんな意識で電子メールを使っていますか？ 瞬時に世界の裏側まで届くこの便利な道具は、その裏にいくつかの危険性をはらんでいます。これだけ普及した今となっては、危険を恐がって使わないというわけにはいきません。電子メールとはどのようなものかを知ることが、安全に使うためのファーストステップです。

第4回
電子メールの安全性に関する基本的な知識を身に付ける

JPCERT/CC（コンピュータ緊急対応センター）
URL http://www.jpcert.or.jp/

電子メールのメカニズム

今回は、電子メールのしくみに関して、基本から考えることによって、インターネット上での電子メールのセキュリティーに関して見直してみましょう。利用者が電子メールに対して求めるセキュリティーは、電子メールを何に利用するかで違ってきます。たとえば、友人に対する伝言を送る、ビジネスで利用する文書を送る、あるいは、商品購入のためにクレジットカードの番号を添えての購入申込書を送る、という目的を考えてみましょう。各々求められるセキュリティーのレベルが違います。電子メールが確保できるセキュリティーを知らなければ、その使用目的に対して電子メールを利用することが適当であるか否かを自分で判断することが難しいと思います。

多くの方が、電子メールを日常の情報交換ツールとして利用されていることと思います。しかし、利用者の大半は、電子メールを出す場合、あるいは電子メールを受け取る場合、ユーザーアプリケーション部分には目を向けますが、その背後にあるメカニズム自体はブラックボックスとして取り扱っているのではないでしょうか。どのように電子メールが送られているか、また、電子メールを送っているシステム環境とはどのようなものかを、まずは知ることから始めましょう。

利用者の環境

最初に利用者の電子メール環境を想定をしましょう。まず、大学や企業などで共用ホスト（UNIXワークステーションなど）を電子メールサーバーとして使っている利用者と、自宅などからパーソナルコンピュータを商用プロバイダーにネットワーク接続している利用者の2つに大別して話を進めたいと思います。

まず、共用ホストにログインした状態で利用している環境について考えましょう。1台のワークステーションを複数人で利用する環境にいる場合、一番最初に個々の利用者が注意を払うべき点は、電子メールを保存するファイルのアクセス権限の設定です。電子メー

ルを保存するファイルのアクセス権限が、他の利用者が読み書きできない状態に設定してあるかどうか確認してください。UNIXを用いた共用ホストでは、利用者宛に到着した電子メールは、利用者が電子メールソフトによって読み出すまで、/usr/spool/mail 以下（システムの設定によって異なる場合があります）に保存されています。電子メールを読むソフトを使って電子メールを読み出すことにより、自分宛の電子メールが自分のホームディレクトリー以下のいずれかに保存されます。このときに、正しいアクセス権限が設定されていない場合、他人に見られてしまう危険性があります（図-1）。

次に、パーソナルコンピュータを商用プロバイダーにネットワーク接続してインターネットを使用している場合です。電話回線などから商用プロバイダーに接続し、電子メールソフトを用いて、商用プロバイダーが用意している電子メールサーバーから電子メールを取り出します（図-2）。

さて、まだ読み出していない電子メールを含めて、電子メールサーバー上のどのファイルであってもシステム管理者は、アクセスすることが可能だということを注意しなければなりません。電子メールサーバーを共用ホストとして利用している場合、不正なシステム管理者が、電子メールを自分で保存したファイルも含めてアクセスする可能性があります。

また、電子メールの宛先などを間違えてエラーになったり、電子メールサーバーが障害を起こしたときなどは、エラーを起こした電子メールを自動的にポストマスターと呼ばれるメールシステム管理者に送る場合があります。あるいは電子メールサーバー上に残ってしまったエラーの電子メールをシステム管理者が手動で除去する場合もあるでしょう。その際に、システム管理者が何ら不正な意図を持たなかったとしても、電子メールの内容が目に触れてしまう可能性があります。

電子メールはハガキと同じ

今度は、電子メールサーバーからインターネットを介して他の電子メールサーバーと電子メールのやり取りすることを考えてみましょう。この部分は、利用者に直接的に見えない処理であり、電子メールサーバー間で自動的に処理が行なわれるため、利用者にはブラックボックス的な部分でもあります。

なお、ここでは、最大公約数的に、ごく一般的な送られ方を仮定して説明しますが、必ずしも具体的なシステムがこのとおり動いているという意味ではありませんので注意してください。

電子メールがインターネットを介して送られるとき、電子メールは、いくつもの電子メールサーバーを経由していきます。まず利用者が電子メールを送付するとき、送り主が直接利用しているような電子メールサーバー、あるいはパーソナルンピューター上の電子メールソフトからローカルなネットワークにある電子メールサーバーへ電子メールが送られます。

ローカルな電子メールサーバーは、さらにインターネットへ接続されている（外部とやり取りしている）電子メールサーバーへ電子メールを転送します。大きな組織では、複数のローカルな電子メールサーバーを経由する場合もあります。

図-1
共有ホストを使って電子メールを使う場合

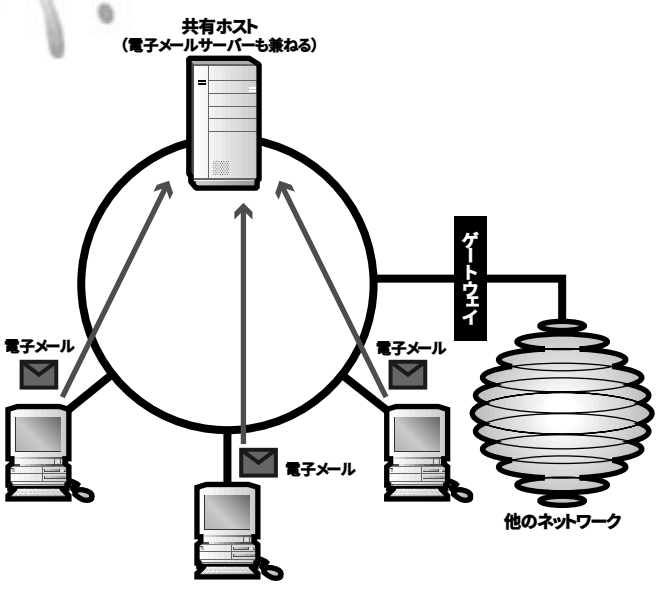
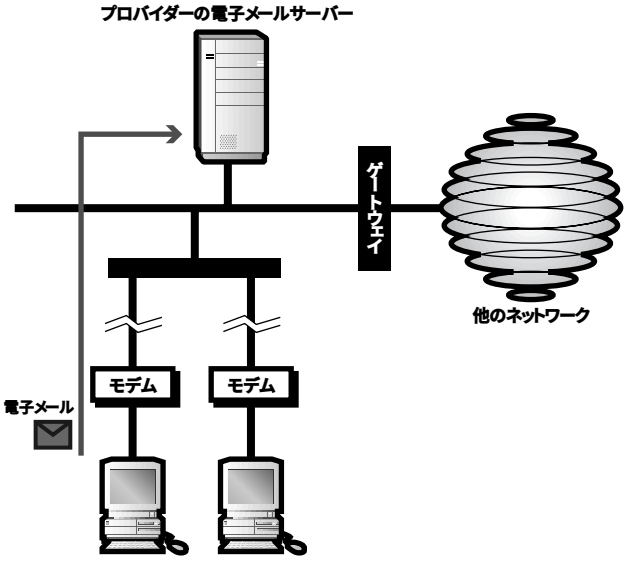


図-2
プロバイダーに接続して電子メールを使う場合



外部と接続している電子メールサーバーは、インターネットを介して、受け取り相手の組織にあって（ドメイン内にある）インターネットから送られる電子メールの窓口となる電子メールサーバーとネットワーク接続し、電子メールを転送します。その電子メールは、送るときと同様にローカルな電子メールサーバーを経由して、受取り人の利用している電子メールサーバーに送られます。

このように、電子メールは送信者から受信者までの間にいくつもの電子メールサーバーを経由します。このとき、不正なシステム管理者がいれば、送られている途中の電子メールに対し不正なアクセスを行うかもしれません。

電子メールは、郵便葉書にたとえると分かりやすいと思います。つまり、電子メールは、書かれている内容を隠していないので、送られている途中で、故意か偶然かにかかわらず、人の目に触れてしまう可能性は常にあるということです。

盗聴/改ざん/なりすまし

電子メールは、送信者から受信者に渡るまでに、いろいろな電子メールサーバーを経由します（図-3）。その通過する電子メールサーバー上で、不正なシステム管理者が電子メールを盗聴する（コピーする）というような事態もありえます。もし、不正なシステム管理者が途中で電子メールを盗聴している事態が発生しても、利用者がそれを発見することは非常に困難です。

送信者からの電子メールの転送途中で電子メールを盗んだうえ、さらに改ざんして、受信者に送るということも可能です。

共有ホストから利用するタイプの電子メールソフトを利用して電子メールを送った場合、システムに登録している利用者情報が自動的に電子メールのFrom:行（送信者情報）に付加される電子メールソフトが多いため、システム管理者が厳しい管理を行い、正しい利用者情報を用意している場合は、その信頼度は高いと言えるでしょう。

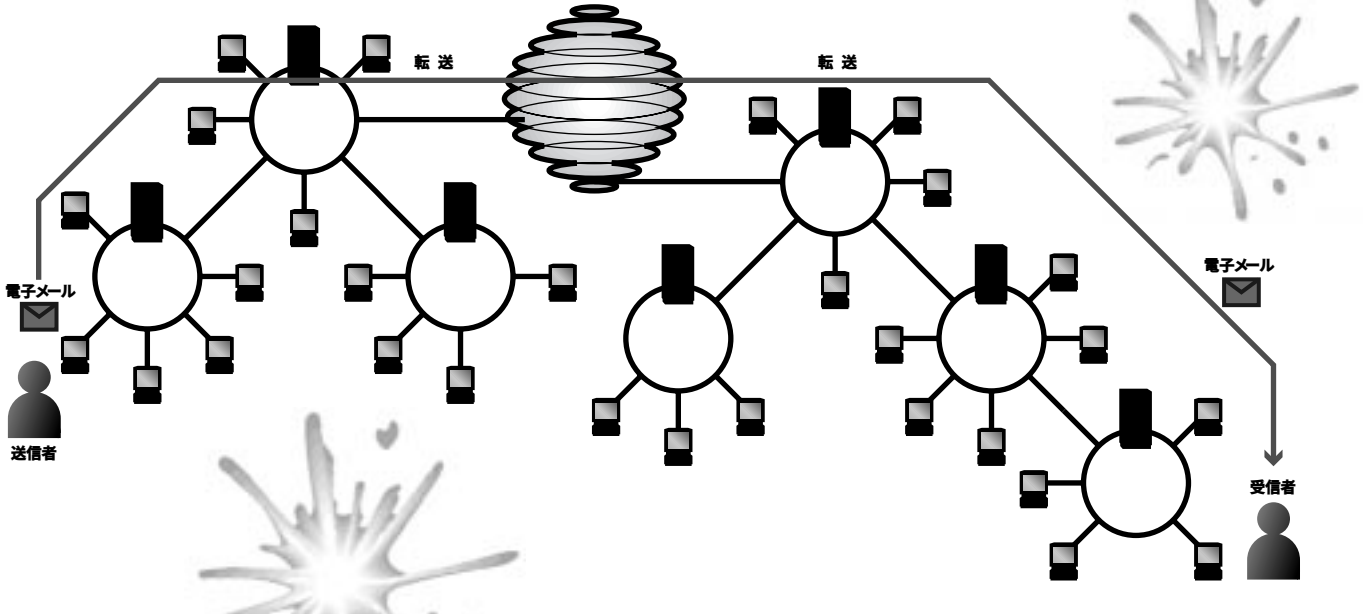
しかし、多くのダイアルアップユーザーが使うような電子メールサーバーにアクセスして電子メールを送るような電子メールソフトの多くは、電子メールのFrom:行（送信者情報）の発信者アドレスに、任意のアドレスや名前を記述することが可能になっているので、送信者の善意に頼るしかありません。また、共有ホストからと言えども、故意にFrom:行の情報を偽造することも可能です。

なりすましの電子メールの発信元電子メールサーバーが、なりすました相手の電子メールサーバーと異なる場合、もし単純にFrom:行の発信者アドレスを偽造しているだけならば、電子メールのヘッダー情報部分にある電子メールの転送履歴（Received:行）やメッセージID（Message-Id:行）とFrom:行を照らしあわせることによって、違うことが確認できます。

しかし、転送履歴と発信者アドレスに注意を払うことは少ないので、うっかり見逃してしまい、そんな単純ななりすましでも通用する危険性がある点は注意しなければなりません。ただし、このようなごく単純なものでも、なりすました相手と同じ電子メールサーバーを使用している場合は、電子メールだけの情報から見つけ出すのは難しいことがあります。

しかし、通常の運用を行っていれば、電子メールサーバーおよび関連のシステムには、なりすました利用者を特定できるのに必要な情報が記録されています。関係するシステム管理者が協力して調査を行えば、ほとんどの場合、なりすました利用者を特定することが可能です。

図-3
送信者から受信者までいくつもの電子メールサーバーを中継してメールは届く



システムとしての信頼性

先程お話ししたシステム不調による事故のことも考えてみましょう。電子メールを転送途中に、中継している電子メールサーバーが不調になり、その拍子にそのまま電子メールが行方不明になってしまう可能性もあります。機械ですから、調子が悪くなって、回復できないような障害が発生することもありえるのです。

分かりやすいように極端な例を出して考えてみます。もし、ある電子メールサーバーが100通に1通の割合で配送エラーを起こして電子メールが正しく送れないとしましょう。途中で中継する電子メールサーバーが同じ信頼性を持つ電子メールサーバーであると仮定をして、その電子メールサーバーの台数が増えると、どうなるかを見てみましょう（図-4）。

このグラフを見て分かるように、100通に1通の割合で配送エラーが出ても、中継する電子メールサーバーが11台を超えると、10通に1通の割合という確率になります。

もちろん、電子メールが通過している最中に、電子メールサーバーが不調になり障害が発生してしまう実際の確率は、ここで仮定した数字よりも、もっとわずかなものです。しかし、いくつもの電子メールサーバーを経由すればするほど、電子メールが無事に届く確率が下ってしまうということを知っておいてください。

暗号を使う

電子メールの内容を暗号を使って保護することを考えてみましょう。ただし、今回の話題は、電子メールの安全性に関する話題なので、ここでは暗号技術を使ってどのように安全性が上がるかを議論するまでにとどめます。

さて、暗号技術を使って保証できるのは次の3つです。

- 秘匿性
- 整合性
- 認証性

秘匿性というのは、暗号を使えば内容を他人に見られないということを意味します。整合性というのは、誰かが途中で内容を改ざんした場合、整合性が崩れるので、改ざんしたことが分かるという意味です。認証性とは、誰が書いたものかが分かる技術です。

電子メールのようにネットワークを介して送信者と受信者が存在している場合は、公開鍵暗号という暗号化を行う鍵と、復号を行う鍵が別々に分かれているタイプの暗号方式を使うほうが安全です。

暗号技術を使うと、途中での盗聴やなりすましといった、途中で電子メールに不正にアクセスされることに関しての問題は、利用者レベルの段階で解決されます。

まとめ

暗号技術を用いるように、利用者レベルで解決できる問題もあります。一方、電子メールの配送自体の安全性といったものは、電子メールサーバーのシステムの安全性はもとより、インターネットを支える各種システムの安全性といった、多種多様なインターネットを運用していくうえでの大きなテーマと関係しています。

ここまで述べたような電子メールの安全性に関する問題点を踏まえたうえで、いかに電子メールを適切に利用するべきかは、利用者1人1人が考える必要があります。

図-4
メールが届かない可能性