標的型攻撃への対策

－企業・組織における情報セキュリティ対策－

出典
総務省 安心してインターネットを使うために
国民のための情報セキュリティサイト

※アンケート（巻末参照）の提出をもって、受講終了となります。

株式会社アクト・テクニカルサポート

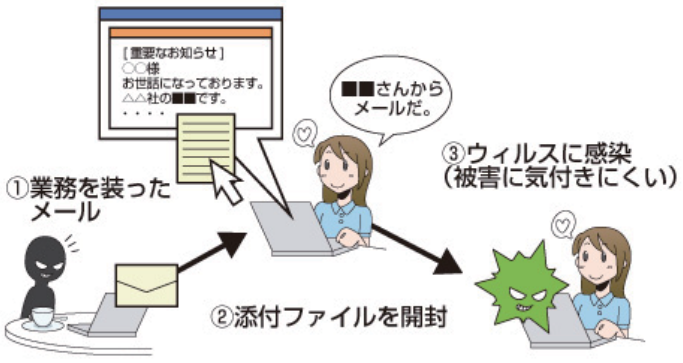
標的型攻撃への対策

最近、特定の企業や組織を狙った標的型攻撃メールにより、重要な情報が盗まれる事件が頻発しています。標的型攻撃メールとは、不特定多数の対象にばらまかれる通常の迷惑メールとは異なり、対象の組織から重要な情報を盗むことなどを目的として、組織の担当者が業務に関係するメールだと信じて開封してしまうように巧妙に作り込まれたウイルス付きのメールのことです。従来は府省庁や大手企業が中心に狙われてきましたが、最近では地方公共団体や中小企業もそのターゲットとなっています。

企業や組織の中のたった１人の社員や職員が、標的型攻撃メールの添付ファイルを開封したり、リンクをクリックしただけでも、情報を盗み出すウイルスに感染し、機密情報が漏洩（ろうえい）する事態に陥ることがあります。特に、標的型攻撃メールのウイルスは、ウイルス対策ソフトでは検出されないものが多いため感染に気づきにくく、知らぬ間に被害が拡大しているケースがあり、深刻な問題となっています。

標的型攻撃を一つの手段で防ぐことは困難ですが、社員・職員の対策としては、標的型攻撃メールの手口をよく知り、そのようなメールが届いても添付されたファイルを開封したり、リンクをクリックしたりしないようにすることが大切です。

標的型攻撃メールの文面は、業務でやりとりしているメールの送信者、よく使われているメールの件名やあて先、内容、添付ファイルの形式、署名などを真似て、受信側をだまそうとするものが主流です。一見して不審な点があまりなく、気がつきにくいのが特徴です。また、メールの件名や内容を、「緊急」や「重要」など、受信側の興味を引いたり、読まなければならないと思わせたりするような細工がされています。



このようなメールが標的型攻撃メールであることを見抜くためには、最近のメールのやりとりなどから判断をすることが重要です。たとえば、最近やりとりがなかったのに、突然メールが届いた、最近のやりとりの内容と全く脈絡のない内容のメールが届いた、などの場合は注意が必要です。このような疑わしいメールを受け取った場合は、情報管理者にすぐに報告・相談するようにしましょう。

その他、最近の標的型攻撃メールは、誰でも取得可能なフリーメールアドレスを利用して添付ファイルにマルウェアを仕込んで送信されることが増えていますので、フリーメールアドレスから送られてきたメールには特に注意が必要です。

また、送信者のメールアドレスを正規のドメインに詐称して攻撃メールが送られてくることもあります。この場合は、メールの送信者アドレスに注意し、送信ドメイン認証の機能を利用してメールが正しい送信元から送られてきているかどうかを確認することで、不審なメールを特定する手がかりになります。

また、一般的にウイルスに感染する危険性を小さくするために、ウイルス対策ソフトの利用とソフトウェアの更新を欠かさずにしておくことも最低限必要な対策となります。

ウイルスの感染経路と主な活動

ウイルスは、USB メモリなどの記憶媒体や電子メール、ホームページの閲覧など、そのウイルスのタイプによってさまざまな方法で感染します。また、ウイルスに感染すると、コンピュータシステムを破壊したり、他のコンピュータに感染したり、そのままコンピュータに残ってバックドアと呼ばれる不正な侵入口を用意したりするなど、さまざまな活動を行います。
ここでは、主なウイルスを感染経路と活動方法によって分類してみましょう。

ウイルスの感染経路

1. ホームページの閲覧

現在の Web ブラウザは、ホームページ上でさまざまな処理を実現できるように、各種のプログラムを実行できるようになっています。これらのプログラムの脆弱性を悪用するウイルスが埋め込まれたホームページを閲覧すると、それだけでコンピュータがウイルスに感染してしまう危険があります。最近では、Web ブラウザへ機能を追加するプラグインソフトの脆弱性（ぜいじゃくせい）を利用した感染方法が増加しています。

かつては怪しい Web サイトを訪問しなければ大丈夫と思われていましたが、最近では正規の Web サイトが不正侵入を受けて書き換えられ、ウイルスが仕込まれてしまうケースも急増しています。この場合は、正規の Web サイトを閲覧しても、ウイルスに感染してしまうことになります。

2. 信頼できないサイトで配布されたプログラムのインストール

あたかも無料のウイルス対策ソフトのように見せかけて、悪意のあるプログラムをインストールさせようとする「偽セキュリティソフト」の被害が増えています。その代表的な手口は、ホームページなどで「あなたのコンピュータはウイルスに感染しています」のようなメッセージを表示し、利用者を偽のウイルス対策ソフトを配布する Web サイトに誘導する方法です。

3. 電子メールの添付ファイル

電子メールの添付ファイルもウイルスの感染経路として一般的です。電子メールに添付されてきたファイルをよく確認せずに開くと、それが悪意のあるプログラムであった場合はウイルスに感染してしまいます。

かつては、電子メールで実行形式のファイル（ファイルの拡張子が .exe　のファイル）が送られてきたときには特に注意するように言われていましたが、最近はファイル名を巧妙に偽装し、文書形式のファイルに見せかけて悪意のあるプログラムを実行させ、ウイルスに感染させる事例もあります。

また、文書形式のファイルであっても、文書を閲覧するソフトウェアの脆弱性を狙った攻撃も増加していることから、メールに添付されてきたファイルを安易に開くのは危険な行為です。

4. USB メモリからの感染

多くのコンピュータでは、USB メモリをコンピュータに差し込んだだけで自動的にプログラムが実行される仕組みが用意されています。この仕組みを悪用して､コンピュータに感染するウイルスがあります。このようなウイルスの中には、感染したコンピュータに後から差し込まれた別の USB メモリに感染するなどの方法で、被害を拡大させるものもあります。

5. ファイル共有ソフトによる感染

ファイル共有ソフトとは、インターネットを利用して他人とファイルをやり取りするソフトウェアのことです。自分が持っているファイルの情報と、相手が持っているファイルの情報を交換し、お互いに欲しいファイルを送り合ったりすることから、ファイル交換ソフトとも呼ばれています。

ファイル共有ソフトでは、不特定多数の利用者が自由にファイルを公開することができるため、別のファイルに偽装するなどの方法で、いつの間にかウイルスを実行させられてしまうことがあります。

6. 電子メールの HTML スクリプト

添付ファイルが付いていなくても、HTML 形式で書かれているメールの場合、ウイルスに感染することがあります。HTML メールはホームページと同様に、メッセージの中にスクリプトと呼ばれるプログラムを挿入することが可能なため、スクリプトの形でウイルスを侵入させておくことができるのです。電子メールソフトによっては、HTML メールのスクリプトを自動的に実行する設定になっているものがあり、その場合には電子メールをプレビューしただけでウイルスに感染してしまいます。

7. ネットワークのファイル共有

ウイルスによっては、感染したコンピュータに接続されているファイル共有ディスクを見つけ出し、特定のファイル形式など、ある条件で探し出したファイルに感染していくタイプのものがあります。このようなウイルスは組織内のネットワークを通じて、他のコンピュータやサーバにも侵入して感染を拡げる可能性があります。とても危険度が高く、完全に駆除することが難しいのが特徴です。

8. マクロプログラムの実行

マイクロソフト社の Office アプリケーション（Word、Excel、PowerPoint、Access など）には、特定の操作手順をプログラムとして登録できるマクロという機能があります。このマクロ機能を利用して感染するタイプのウイルスが知られており、マクロウイルスと呼ばれています。Office アプリケーションでは、マクロを作成する際に、高度なプログラム開発言語である VBA（Visual Basic for Applications）を使用できるため、ファイルの書き換えや削除など、コンピュータを自在に操ることが可能です。そのため、マクロウイルスに感染した文書ファイルを開いただけで、VBA で記述されたウイルスが実行されて、自己増殖などの活動が開始されることになります。

ウイルスの主な活動

1. 自己増殖

ウイルスの中には、インターネットや LAN を使用して、他の多くのコンピュータに感染することを目的としているものがあります。特にワーム型と呼ばれるウイルスは、自分自身の複製を電子メールの添付ファイルとして送信したり、ネットワークドライブに保存されているファイルに感染したりするなど、利用者の操作を介さずに自動的に増殖していきます。

2. 情報漏洩（じょうほうろうえい）

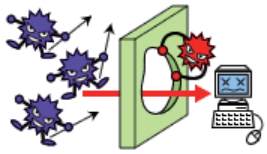
ウイルスによる情報漏洩は、大きく分類すると、コンピュータに保存されている情報が外部の特定のサイトに送信されて起こる場合と、インターネット上に情報が広く公開されて起こる場合があります。ウイルスによって漏洩する情報は、ユーザ ID やパスワード、コンピュータ内のファイル、メール、デスクトップの画像など､さまざまです。情報漏洩を引き起こすタイプのウイルスには､利用者がキーボードで入力した情報を記録するキーロガーや、コンピュータ内に記録されている情報を外部に送信するスパイウェアと呼ばれるものなどがあります。コンピュータがこのようなウイルスに感染していたとしても、コンピュータの画面上には何の変化も起こらないことが多いため、利用者はウイルスに感染していることに全く気が付きません。

なお、漏洩した情報がインターネットに掲載され、公開されてしまった場合は、その情報をネットワーク上から完全に消去することは非常に困難です。

3. バックドアの作成

感染したコンピュータの内部に潜伏するタイプのウイルスをトロイの木馬と呼びます。この中でも、コンピュータに外部から侵入しやすいように「バックドア」と呼ばれる裏口を作成するタイプのウイルスは極めて悪質なものです。この種のウイルスに感染すると、コンピュータを外部から自由に操作されてしまうこともあります。

外部からコンピュータを操作するタイプのウイルスは、RAT（Remote Administration Tool）とも呼ばれ、利用者に気が付かれることもなくコンピュータを遠隔操作します。多くの場合、コンピュータの画面上に何も表示されることなく、プログラムやデータファイルの実行・停止・削除、ファイルやプログラムのアップロード・ダウンロードなど、不正な活動を行います。



4. コンピュータシステムの破壊

ウイルスによっては、コンピュータシステムを破壊してしまうものがあります。その動作はウイルスによって異なりますが、特定の拡張子を持つファイルを探し出して自動的に削除するものから、コンピュータの動作を停止してしまうものまでさまざまです。

5. メッセージや画像の表示

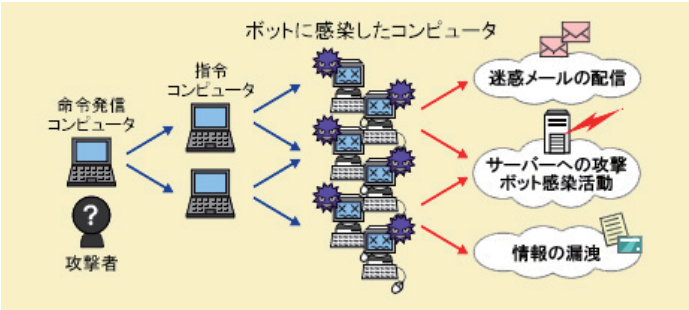
いたずらを目的としたウイルスは、一定期間コンピュータ内に潜伏して、ある日時に特定のメッセージや画像を表示することがあります。ただし、最近はこのようないたずらを目的としたウイルスは減ってきています。

【コラム】ボットとは？

ボット（BOT）とは、コンピュータを外部から踏み台にして遠隔操作するためのウイルスです。ボットに感染したコンピュータは、同様にボットに感染した他の多数のコンピュータとともにボットネットを形成し、その一員として動作するようになります。そして、インターネットを通じて、悪意のある攻撃者が、ボットに感染したコンピュータを遠隔操作します。外部から自由に操るという動作から、このような遠隔操作ソフトウェアのことを、ロボット（Robot）をもじってボット（BOT）と呼んでいます。

攻撃者は、ボットに感染したコンピュータを遠隔操作することで、インターネットに対して、「迷惑メールの配信」、「インターネット上のサーバへの攻撃」、「さらにボットを増やすための感染活動」など、迷惑行為や犯罪行為を行います。また、感染したコンピュータに含まれる情報や、コンピュータの利用者が入力した情報を盗み出す「スパイ活動」も行うことがあります。ボットは旧来のウイルスのように愉快犯的な行為で作られたものではなく、迷惑メールの送信者や個人情報を不正に利用しようとする犯罪者と取引するために作られているという点で、手口が巧妙化しています。このような目的から、旧来のウイルスと比べると、感染しているということに利用者が気付きにくいように作られているというのも特徴のひとつです。

もし、あなたのコンピュータがボットに感染した場合、あなたはもちろん被害者なのですが、あなたのコンピュータが迷惑メールを送信したり、別のサイトを攻撃したりするため、攻撃の標的となったコンピュータから見ると、あなたのコンピュータは加害者になってしまいます。あなた自身が加害者にならないようにするためにも、ボットへの対策はとても大切なことなのです。



アンケートの提出をもって受講完了となります。（必ずご提出をお願いいたします。）
下記のボタンをクリック、または QR コードを読み取り、アンケートにお答えください。

アンケートに回答する