MC テックニュース No.05 2016 年 3 月

「外部からの脅威への対策」

企業情報に対するセキュリティとは、社内もしくは社外の権限のある利用者のみに情報を利用することを許し、許可されていない者には情報にアクセスできないようにすることです。しかし、インターネットやメール等の外部への接続の増加、社内のパソコンの増加などによって管理が行き届かず、セキュリティへの脅威は増しています。2015 年 5 月には日本年金機構で 110 万件にも及ぶ個人情報が流出しました。

このように、万が一お客様の情報や個人情報が漏れてしまった場合には非常に大きな問題となり、会社の信用失墜にもなりかねません。また、マイナンバー制度も始まり、ますますセキュリティに対して過敏になっています。今回は、不正アクセスなど基本的な脅威と、その最新情報に焦点を当てています。

不正アクセスとウィルス

不正アクセスには、データの改竄や破壊、データの盗難などの直接そのコンピュータを狙ったものと、そのコンピュータに侵入しウィルスを埋め込むなどして、他のコンピュータを攻撃するための踏み台に利用するものがあります。

その手段として、不正に入手した ID やパスワードによる侵入のほか、コンピュータの脆弱性を利用したり、ウィルスをメールで送り込むなどの方法が使われます。コンピュータの脆弱性を狙った不正なアクセスを防ぐには、Windows Update や更新プログラムを利用して、常にコンピュータやファイアウォール、その他のソフトウェアの状態を最新にしておくことです。

ウィルス（マルウェアとも呼ぶ）は、Web サイトからのダウンロードやメールの添付、USB メモリ等を介して、ウィルスにすでに感染したファイルを受取ることによって自身も感染します。

ウィルスの中には、データの破壊だけに留まらず、情報を外部へ送ることを目的とする悪質なものもあります。

また最近では、他のコンピュータの攻撃の踏み台にされる被害も増えています。攻撃者は、あらかじめ攻撃対象とは全く無関係のコンピュータにマルウェアを侵入させ、使用者が気づかない間に命令を実行して、標的に大量のデータを送るなどの不正行為を行うものです。このようにウィルス対策を十分に行っていない

(表 1)

	平成 24 年	平成 25 年	平成 26 年
国内からアクセス	987	2, 474	2, 469
海外からアクセス	122	289	298
アクセス元不明	142	188	778
認知件数　計	1, 251	2, 951	3, 545

(表 2)

	平成 24 年	平成 25 年	平成 26 年
一般企業	1, 163	2, 893	3, 468
大学･研究機関等	12	9	56
プロバイダ	22	9	16
行政機関等	54	40	5
計	1, 251	2, 951	3, 545

(上：表 1)「不正アクセスの件数推移」

※必ずしも、不正アクセスを行った者のアクセス元を示すものではなく、海外から国内のコンピュータを経由したような場合「国内からのアクセス」に分類しています。

(下：表 2)「被害を受けたコンピュータの管理者」

（国家公安委員会 HP：不正アクセス発生状況より）

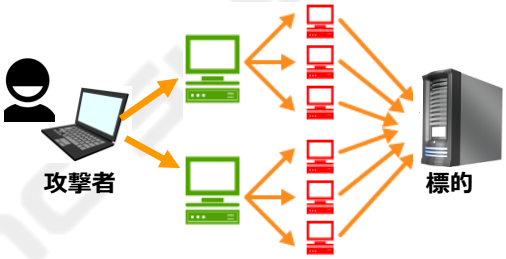
「複雑化する他のコンピュータへの攻撃」

「Dos 攻撃」：

標的に大量攻撃を仕掛けサービス不能な状態にする。

「DDos 攻撃」：

第三者のコンピュータに不正アクセスを使ってツールを忍ばせておき、時限爆弾のように、ある時刻になったら標的に大量攻撃を仕掛けサービス不能な状態にする。本人が攻撃をするわけでなく第三者を踏み台にするため、大元の攻撃者を特定できない。



コンピュータは、他の利用者や企業に被害を及ぼしてしまうことがあります。(外部からの攻撃については後のページでもう少し詳しく触れています)

ウィルス対策で最も効果的なのはセキュリティソフトを導入することです。複数のポイントで行うことが重要です。

用語解説１：「コンピュータの脆弱性」

脆弱性とは、コンピュータの OS やソフトウェアにおいて、プログラムの不具合や設計上のミスが原因となって発生するセキュリティ上の欠陥のことを言います。セキュリティホールとも呼ばれ、そのままの状態でコンピュータを使用していると、悪意を持った者にその脆弱性をつかれて不正アクセスに利用されたり、ウィルスに感染する危険を持っています。

「Adobe」や「Java」、「Office」など広く普及しているソフトにも脆弱性は見つかっており、その危険性がニュースになったこともあります。開発メーカーは、脆弱性が発見されると迅速に更新プログラムを提供していますので、使用者も忘れずにアップデートを行わなければいけません。

有効対策のひとつ、ファイアウォール

不正アクセスを防ぐコンピュータのセキュリティ機能といえば、ファイアウォールです。

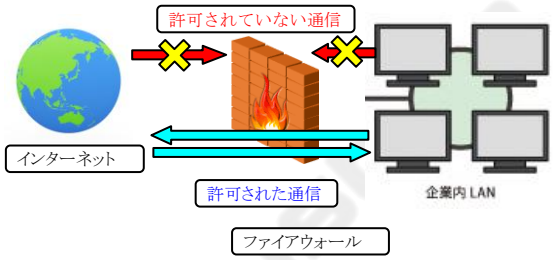
ファイアウォールとは、外部(インターネット側)からの攻撃や不正アクセスの侵入を防ぐだけでなく内部(コンピュータ側)からの意図しない通信をしないように制御するものです。内部から外部への通信にも目を光らせているのは、もしウィルスに侵入されてしまった場合でも、そのウィルスが不正にデータを外部に送れないようにするためです。

ファイアウォールの仕組みのひとつを簡単に説明すると、送られてきたデータの送信元や送信先の IP アドレスなどによって、そのデータを通過させるかどうかを判断して、不正アクセスと判断すると直通させないようにしています。

インターネットの接続部分やサーバー等より不正アクセスの攻撃を受ける可能性は低いとはいえ、各クライアントにもファイアウォール機能を有効化しておくことで、リスクを減らすことができます。

しかし、ファイアウォールでもメールに添付された形で送りつけられるウィルス等は防ぐことができません。セキュリティソフトで定期的にウィルススキャンを実行して、ウィルスの侵入を検知し直ちに隔離や駆除を行います。

「ファイアウォールの働き」



内部から外部への不正な通信も防ぐ

「スマートフォン(Android OS)のセキュリティ対策」

スマートフォンで用いられている OS のアンドロイド(Android)は、オープンソースといって開発環境やアプリケーションのソース(中味)がオープンに提供されているため、侵入のリスクが高く不正プログラムについても高度なものを組み込むことが可能な、危険な OS だと言えます。

コンピュータの場合の対策と同じように「ウィルス対策ソフト」を導入し、アプリケーションのインストール時にはアクセス許可を必ず確認することです。また、アンドロイド OS はテザリング機能を有効にした場合、「オープンリゾルバ」(後述)として機能してしまう問題が発覚しています。携帯各社のサイトに対策が掲載されています。

外部から攻撃される理由

社内のパソコンからインターネットを使用する時、パソコンはサーバやルータに見たいサイトの IP アドレスを問い合わせ、探索した答えを返してもらって、見たいサイトにつないでいます。

サーバやルータが、社内ネットワークからの問い合わせに応答するのは当然ですが、本来制限すべき外部の不特定者からの問い合わせにも反射的に応答を返してしまうサーバやルータが多数存在していることが、問題視されています。

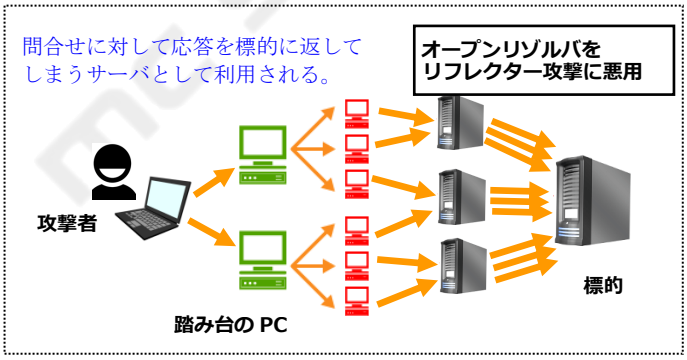
そのようなサーバやルータの特性を「リフレクター（反射板）」といいますが、悪意を持った攻撃者が「リフレクター」機能を使って、標的に大量の問い合わせ結果を送りつける「リフレクター攻撃」に意図せず利用されてしまうからです。

最近良く耳にする、オープンリゾルバとは

また、インターネット上のどこからでも問い合わせを受け付ける状態となっている、つまり「リフレクター攻撃」に利用できるサーバやルータなどのネットワーク機器のことを「オープンリゾルバ」と言います。つまり、攻撃者は「オープンリゾルバ」状態の機器を常にネット上で探しており、DDos 攻撃などの踏み台として利用しようと狙っています。

警察庁も「オープンリゾルバ」に対して、ホームページ等で盛んに注意を呼びかけています。

「オープンリゾルバ」



攻撃者は、あらかじめ標的者の IP アドレスを手に入れ、踏み台となるコンピュータやオープンリゾルバとなっているサーバを探しておいて、その上で、オープンリゾルバに問い合わせを送るため、マルウェアを踏み台となるコンピュータに侵入させておきます。

攻撃者がマルウェアに指令を出すと、踏み台となったコンピュータは同時刻一斉にオープンリゾルバに向かって問い合わせを実行します。オープンリゾルバのサーバは外部の問合せに対して、リフレクターとなり返答を返しますが、IP アドレスは偽装された IP アドレスのため、送信者(踏み台のコンピュータ)ではなく IP アドレス宛、すなわち標的者宛に送信してしまいます。

攻撃者がこのような問い合わせを多数のオープンリゾルバに対して行うことで、標的になったサーバは大量の回答が集中し、ダウンしてしまうわけです。

オープンリゾルバ対策

悪意の構造は複雑化しており、攻撃者を特定することは容易ではないようです。海外からの攻撃や海外を経由した攻撃もあるので尚更です。となれば自分たちで防衛しなければいけません。最も有効な対策と思われるのは、オープンリゾルバ状態をなくすことです。

具体的には、社内のサーバやルータがオープンリゾルバになっていないかどうか確認します。

一般社団法人「日本ネットワークインフォメーションセンター（JPNIC）」の「オープンリゾルバ確認サイト」を掲載しておきます。（ http：//www.openresolver.jp/ ）

問題があれば、応答機能を持つサーバやルータの設定を変更し、無視あるいは遮断にすることです。(設定方法は機器によって異なります)

用語解説２：「ドメイン名 と ＩＰアドレス」

ドメイン名は、インターネット上の住所に例えられます。具体的には、ドメイン名は HP アドレスやメールアドレスの一部として使われます。

例： HP アドレス　http://www.mcsystem.co.jp
　　Mail アドレス　nagoya@mcsystem.co.jp
　　※(mcsystem.co.jp) がドメイン名になります。

また、インターネット上のコンピュータにはすべて IP アドレスという数字が割り振られていて、場所の特定は IP アドレスで行われます。しかし、数字の羅列である IP アドレスはわかりにくいため、より理解しやすいドメイン名を IP アドレスに対応付けて使用しています。ドメイン名と IP アドレスの対応づけを行う仕組を、ドメインネームシステム(DNS)と呼び、DNS 機能を持ったサーバやルータが、問い合わせに答えてくれるため、インターネットにアクセスすることができます。

マイナンバー制度の安全管理

マイナンバー制度が始まりました。特定個人情報の取扱いにおいて、その講ずべき安全管理措置がガイドラインに書かれています。

マイナンバーを取扱うために鍵のかかる部屋を用意するなど、無理な対策を取る必要は決してありません。万が一情報が漏洩した時に、会社として基本的な管理をしていたことを証明できればよいのです。ガイドラインにおいて重視されているのは、アクセス制御と記録を取ることです。

コンピュータで管理する場合、機器を取扱う事務取扱担当者を限定し、コンピュータが標準で持っているログインユーザーとパスワードの設定でアクセスを制御します。パスワードを記載した書面は、鍵のかかる引出しや鍵のかかるキャビネット等に保管します。

さらに、コンピュータの特定個人情報が入っているフォルダを他人から見られないようにしておくとよいでしょう。

フォルダを他人から見られないようにする方法

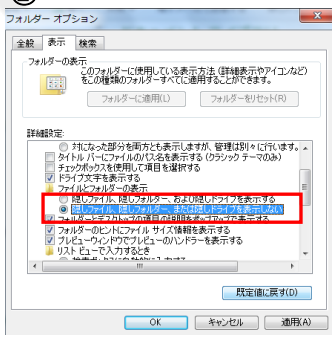
（1）隠しフォルダの設定

①「スタートメニュー」→「ドキュメント」→「整理」→「フォルダーと検索のオプション」をクリック

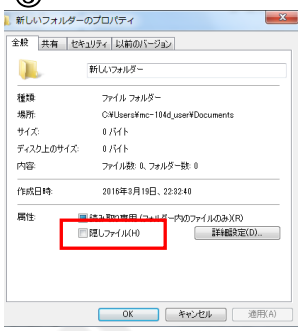
②「フォルダーオプション」→「表示」→「詳細設定ボックス」の「隠しファイル隠しフォルダーまたは隠しドライブを表示しない」にチェックを入れて「OK」を押す

③「特定個人情報」が入った隠したいフォルダーを右クリック→「プロパティ」→「全般」→「隠しファイル」にチェックを入れると、見えなくなる。

②



③



④作業をする時は、「隠しファイル隠しフォルダーおよび隠しドライブを表示する」にチェックを入れて、見えるようにしてから作業を行う。

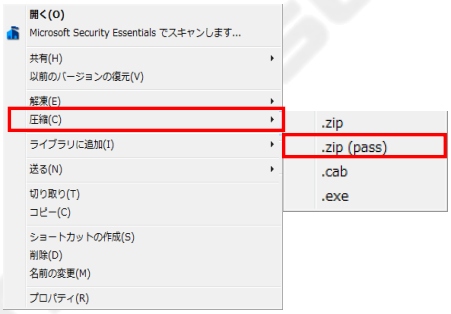
（2）圧縮ソフトの利用

7-Zip や Explzh などの圧縮ソフトには、圧縮をしたうえパスワードがかけられるものがあります。
作業が完了したら、圧縮しパスワードを設定しておけば他人に見られることはありません。

「Lhaplus」を例に、Zip ファイル作成時に、パスワード設定をする方法を紹介します。

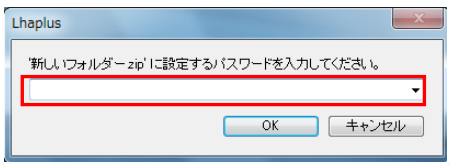
①パスワードを掛けて Zip 圧縮したいファイル(フォルダ)で右クリック。「圧縮」→「.zip(pass)」

①



②パスワードを入力するよう求められますので、パスワードを入力して下さい。入力したら「OK」

②



③作業をする時は、圧縮されたファイルをダブルクリックすると、パスワードを求める画面が開きますので、パスワードを入力すると解凍されます。

システム設計から情報分析まで
mc System
エムシー システム株式会社
〒450-0002
名古屋市中村区名駅五丁目 30 番 4 号　名駅 KD ビル 8F
TEL(052)571-7011　FAX(052)571-7013
URL　http://www.mcsystem.co.jp