最近の情報セキュリティ事情について

電気電子・情報系技術班　宮田 晃

1. はじめに

ネットワークを利用した情報システムが社会の細部にまで浸透してきた昨今，システムの停止や情報の盗み出しをねらった悪意あるアクセス（サイバー攻撃）も増加の一途をたどっている．平成 27 年 5 月，日本年金機構のシステムがサイバー攻撃を受け，約 125 万件の個人情報が外部に流失した事件は記憶に新しいが，同年 7 月にはついに愛媛大学内のサーバから個人のメールアドレス 366 件が流出する事態に至った．本稿ではこれらのサイバー攻撃の現状と，それに対する対策につき述べる．

2. サイバー攻撃の現状

2.1 標的型攻撃

最近，攻撃を仕掛ける組織の公開メールアドレスに，直接ウイルス等を添付したメールを送りつける「標的型攻撃」が増加している．メールの表題や内容も，その組織の業務に関連性を持たせるなど巧妙に偽装されている場合がある．

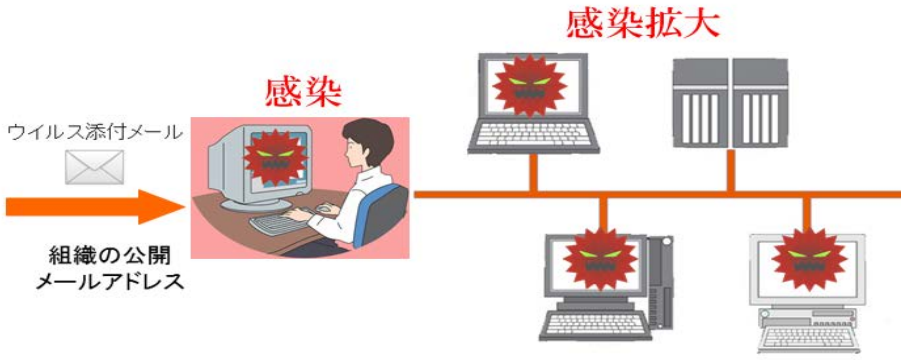
一例として，日本年金機構に送りつけられた不審メールの概要を表－１に示す．送り先に関連のある内容に装い，担当者にウイルス付き添付ファイルを開かせるために，ファイル名等にも工夫が凝らされていることがわかる．

表－１　日本年金機構に送りつけられた不審メールの概要 [1)]

不審メールの番号	受信日	不審メールの概要
Ⅰ	5月8日（金）	件名：「厚生年金基金制度の見直しについて（試案）に関する意見」 宛先：公開メールアドレス（2） リンク：商用オンラインストレージ
Ⅱ	5月18日（月）	件名：給付研究委員会オープンセミナーのご案内 宛先：非公開の個人メールアドレス（98） 添付ファイル：給付研究委員会オープンセミナーのご案内.lzh
Ⅲ	5月18日（月） ～ 5月19日（火）	件名：厚生年金徴収関係研修資料 宛先：非公開の個人メールアドレス（20） 添付ファイル：厚生年金徴収関係研修資料（150331厚生年金徴収支援G）.lzh（16） リンク：商用オンラインストレージ（4）
Ⅳ	5月20日（水）	件名：【医療費通知】 宛先：公開メールアドレス（3） 添付ファイル：医療費通知のお知らせ.lzh

※　表中の括弧内の数字はメールの件数を表す。

受信者が添付ファイルを開くと，その時点でウイルスが動作を始め，当該パソコンを乗っ取って内部データを収集し，その情報（メールソフトのアドレス帳など）をもとに更なる感染の拡大をはかる．その概念図を図－１に示す．



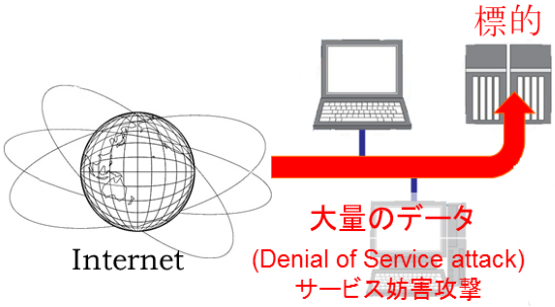
図－１　標的型攻撃の概念図

感染したウイルスは，パソコンに攻撃先からの指令を受け取る設定（バックドア）を施し，潜伏するため，外見からは感染を判断することはできない．組織内でネットワークトラフィックの監視を行っている場合，通常起こりえない不正な通信が検知されてウイルス感染が発見されるケースもある．

2.2 無差別攻撃

ネットワーク上にある数多くのサーバに対し，無差別に，大量のデータを送りつけてサービスの停止をねらう攻撃（DoS 攻撃）や，OS やサーバプログラムの脆弱性をついてシステムを乗っ取ろうとする攻撃，Web ページにウイルスを含むスクリプトをおき，閲覧に来た不特定のユーザに感染させる攻撃など，従前より存在し今なお猛威を振るっている様々なサイバー攻撃がある．

一例として，DoS 攻撃の概念図を図－２に，当技術部サーバに届いた DoS 攻撃と思われるアクセスログの一部を図－３に示す．この日（2015 年 9 月 7 日）に sshd に対して行われた不正アクセスは 22,820 回（およそ 3.8 秒に 1 回）に達し，IP アドレスから推測した発信元はほとんど中国ないし香港であった．この前後の日にも同程度の不正アクセスが引き続き行われている．



図－２　DoS 攻撃の概念図

```
[root@svr ml]# cat /var/log/secure | grep 'Sep  7.*sshd.*Failed' | head
Sep  7 00:00:00 svr sshd[4227]: Failed password for root from 182.100.67.59 port 35
111 ssh2
Sep  7 00:00:03 svr sshd[4225]: Failed password for root from 43.229.53.60 port 163
38 ssh2
Sep  7 00:00:04 svr sshd[4229]: Failed password for root from 182.100.67.59 port 41
565 ssh2
Sep  7 00:00:04 svr sshd[4225]: Failed password for root from 43.229.53.60 port 163
38 ssh2
Sep  7 00:00:06 svr sshd[4229]: Failed password for root from 182.100.67.59 port 41
565 ssh2
Sep  7 00:00:06 svr sshd[4225]: Failed password for root from 43.229.53.60 port 163
38 ssh2
Sep  7 00:00:08 svr sshd[4229]: Failed password for root from 182.100.67.59 port 41
565 ssh2
Sep  7 00:00:11 svr sshd[4234]: Failed password for root from 182.100.67.59 port 48
742 ssh2
Sep  7 00:00:13 svr sshd[4234]: Failed password for root from 182.100.67.59 port 48
742 ssh2
Sep  7 00:00:14 svr sshd[4232]: Failed password for root from 43.229.53.60 port 410
59 ssh2
```

図－３　技術部サーバに対する不正アクセス例

3. サイバー攻撃への対策

3.1 標的型攻撃への対策

標的型攻撃で送りつけられるウイルスは，攻撃対象の組織にあわせて細かな修正が加えられている場合が多く，一定のパターンでウイルスを検知するセキュリティソフトでは検出することができない．したがってこの種の攻撃に対する対策としては，以下のようなことがあげられる．

ア）添付ファイルつきのメール（特に外部組織からのもの）に関しては，送信者や宛先，本文に注意し，

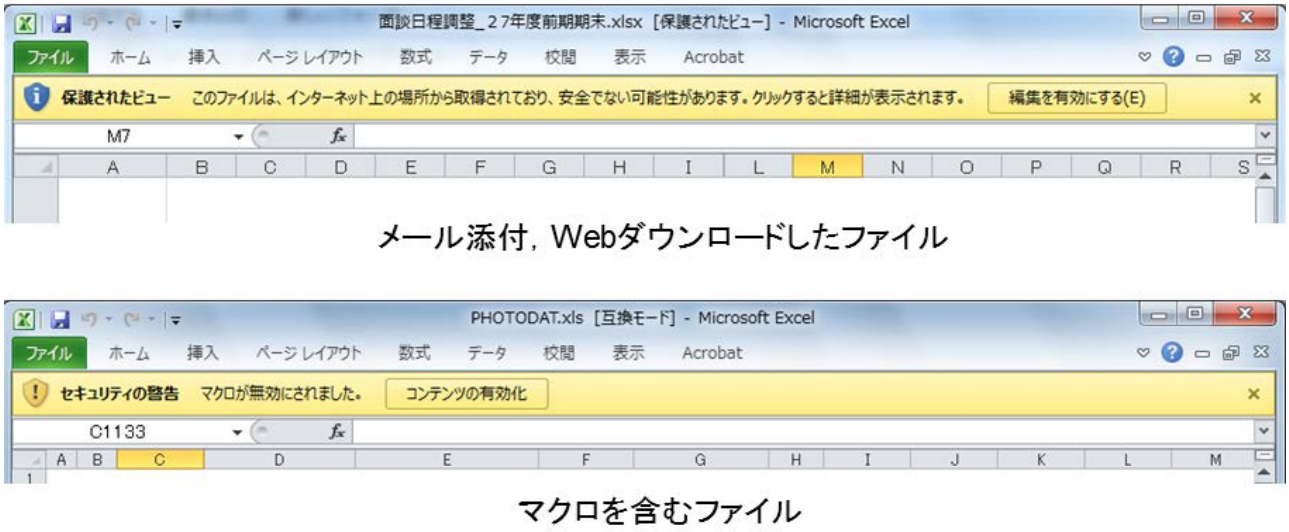
むやみに添付ファイルを展開しない.

イ) Word 文書等のマクロにウイルスが仕込まれている場合もあるので, アプリケーションの設定でマクロを自動実行しない設定にしておく.

ウ) 個人情報を各人が使用しているパソコン上におくことは必要最小限にとどめ，不要になった場合は直ちに削除する.

エ) ウイルスの発信する不正な通信を検出し，警報を発する仕組みを導入する.

上記イ)に関し，Microsoft Office の 2010 以降のバージョンでは，ネットワークからダウンロードしたりメールに添付されていた文書ファイルに対するアラートが強化され，アプリケーションで開いた直後には編集が無効にされている．また従来より，マクロを含む文書ファイルに対してもデフォルトではマクロが無効にされる．これらのアラート表示例を図－４に示す.



図－４ Microsoft Office 2010 のアラート表示例

3.2 その他攻撃への対策

標的型攻撃への対策にも当てはまることであるが，以下に示すような一般的な対策を施すことが必要といえる.

ア）OS やアプリケーション，サーバソフトウェア等を常に最新の状態にアップデートしておく.

イ）セキュリティソフトの定義ファイルを常に最新のものにしておく.

ウ）重要なデータは定期的にバックアップを取る.

エ）情報管理部門からの連絡等，常に最新のセキュリティ情報に注意する.

オ）組織により，インシデント（緊急事態）発生時の対応手順が定められていることがあるので，確認しておく.

4. まとめ

組織の情報システムをねらったサイバー攻撃は，今後増加を続け，手口もより巧妙化してくることは確実である．そのような状況においては，情報システムを使用するうえでの「違和感」にいちはやく気づき，直ちに対策をとることが何よりも重要である. 対応が早ければ早いほど, 有効な対策が打てる. つまるところ，職員一人一人が，自分もいつ攻撃の矢面に立たされるかわからないという危機感を共有する必要がある.

謝辞：本稿執筆にあたり，国立情報学研究所教授，高倉弘喜氏による講演や Web ページの記事を参考にさせていただいたことに対し謝意を表します.

参考文献

1）日本年金機構における個人情報流出事案に関する原因究明調査結果，内閣サイバーセキュリティセンター，2015.