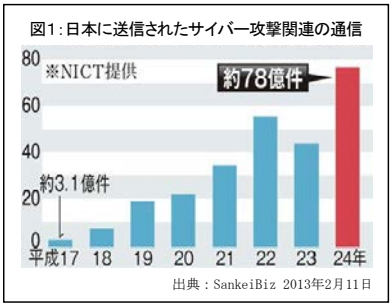
2013.4.1

情報セキュリティニュース ＜2013 No.1＞

2012 年における標的型メール攻撃事例の分析

2011 年以降、国内外では次々とサイバー攻撃が起こっており、これに関する報道をテレビや紙面で目にする機会が増えている。

たとえば、独立行政法人情報通信研究機構（NICT）の調査では、2012 年一年間で、日本の政府機関や企業へのサイバー攻撃関連の通信は約 78 億件に上ったとされている(図 1)。また、2012 年には、ウイルスにより感染し外部からのっとられたパソコンが、脅迫メールを送信するよう遠隔操作され、脅迫メール送信の犯人として、パソコンの持ち主が誤認逮捕されるという、いわゆる「遠隔操作ウイルス事件」が発生、社会的に大きな波紋を呼んだ。



さらに、海外に目を転じると、米国では、フェイスブック、アップル、マイクロソフトなどの IT 関連企業のほか、ニューヨークタイムズ、ニューズウィークなどのメディア企業に対してもサイバー攻撃が激化している。2013 年 2 月には、米国のインターネットセキュリティー会社が、米国の政府機関や企業に対するサイバー攻撃に、中国人民解放軍の関与が疑われると発表した。これに対し、中国政府は「根拠のない非難である」と反論している。つづいて 3 月には、韓国の複数の主要テレビ局および銀行等のコンピューターネットワークを一斉に停止させるサイバー攻撃が発生し、韓国国防省がサイバー防衛の警戒レベルを引き上げるなどの措置をとったことが我が国でも大きく報じられた。まさに「サイバー戦争」という言葉が頭をよぎった人も少なくないのではないだろうか。

特に、このようなサイバー攻撃の中でも、特定の組織やサービス、個人をターゲットとした「標的型サイバー攻撃」(注 1)と呼ばれる攻撃においては、ターゲットに確実に侵入するための「だましの手法」を日々進化させており、2012 年下期においても新たな手法が次々と発見され、企業や組織にとって重大な脅威となっている。

本稿ではかかる標的型サイバー攻撃の中から、2012 年に新たな手法が発見された「標的型メール攻撃」や、誰もが容疑者になり得る「遠隔操作ウイルス事件」に焦点を当て、それぞれのポイントと対策を紹介する。

(注 1)標的型サイバー攻撃には、「標的型メール攻撃」「Web 改ざん」「Advanced Persistent Threat（APT）（高度で執拗なサイバー攻撃)」などのタイプがある。

1. 標的型メール攻撃

1.1　標的型攻撃メールとは

標的型攻撃メールとは、添付ファイルを開かせたり、本文中に記載したリンク先の URL をクリックさせることで、特定の事業者や個人のパソコンをコンピュータウイルスに感染させることを目的としたメールである。送信者名に取引先の企業や組織内の関係者など、信頼性のあるものを記載したり、受信者が関心をもつようなメールの表題や本文を記載するなど、年々、より巧妙な偽装が施されるようになってきている。

1.2　2012 年 1 年間に確認された攻撃メール件数と接続先

警察庁の調べによると、2012 年中に国内の先端技術を持つ企業や電力・鉄道などのインフラ事業者、地方自治体などに送付された標的型攻撃メールは 1,009 件に上っている(図 2)。標的型攻

撃メールにより不正プログラムに感染した場合、そのパソコン等の端末は不審な外部接続先に接続しようとするが、接続先は、米国が約 26%、中国が約 21%、日本が約 20%となっている(図 3)。

また、この 1,009 件のうちの数件では、実際に外部への情報流出が発生したとみられている。

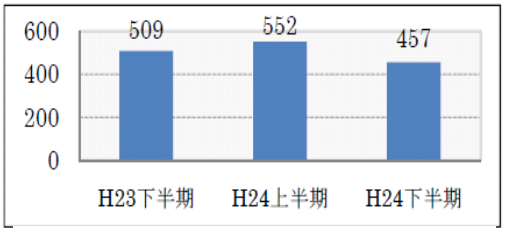


図 2：警察が把握した標的型メール攻撃の件数

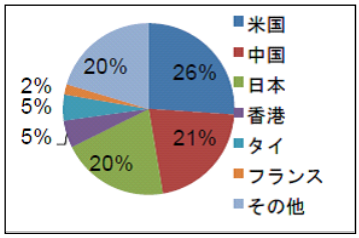


図 3：2012 年における標的型メール攻撃に使用された不正プログラム等の接続先

出典：警察庁広報資料(平成 25 年 2 月 28 日)「平成 24 年中のサイバー攻撃情勢について」

1.3　2012 年に発生した標的型メール攻撃の主な事例と特徴

1.3.1　主な事例

2012 年に発生した標的型メール攻撃の主な事例をご紹介する。

事例	発生年月	概　　要	特徴
1	2012 年 11 月	架空の日本人名を名乗った攻撃者が、不正行為の告発を装い、企業がウェブサイト上で公開しているメールアドレスに「問い合わせメール」を送信した。このメールに回答した企業の担当者に対し、不正プログラムを埋め込んだ『告発書』と題する「添付ファイル付メール」を送付した。	特徴 2 特徴 3
2	2012 年 11 月	攻撃者が就職希望者を装い、企業のウェブサイトに問い合わせメールを送り、これに返信した採用担当者に対し、『履歴書』と偽って「不正プログラム付メール」を送付した。このケースでは、不正プログラムを含むファイルにパスワードがかけられていたため、採用担当者がパスワードを尋ねるメールを送信し、攻撃者がパスワードを知らせるメールを返信するなど、複数回のやりとりがなされていた。	特徴 2 特徴 3
3	2012 年 10 月以降	政府機関職員を装った攻撃者から、「尖閣諸島の領有権についての基本見解」や「(政権交代に伴う) 内閣総理大臣就任記者会見への参加について議題速報」などと題するメールが、複数の企業に送付された。	特徴 1 特徴 3
4	2012 年 2 月、3 月	A社の職員が取引先に対して送付したメールの本文を引用し、A社と業務上の関係がある 2 協会・4 社あてに標的型攻撃メールが送付された。 また、3 月には、B社の職員がA社の職員に対して送付したメールを搾取され、このメールを利用し、A社と業務上関係する 7 社に標的型攻撃メールが送付された。	特徴 1 特徴 3
5	2012 年 7 月	C法人の複数の職員あてに、実在するC法人の職員(組織幹部)の名前で「連絡網の送付」という案件のメールが送付された。このメールは、3 分の間に、19 件送信されている。なお、送信元のメールアドレスはフリーメールで、添付ファイルは「事務系連絡網」という圧縮ファイルであった。	特徴 1 特徴 3

1.3.2　特徴

情報セキュリティの重要性に対する社会一般の認識が広がり、不審なメール等に対する警戒心が高まる中、単に不正プログラムを送信しても、攻撃対象者は容易に開こうとしない。このため、標的型メール攻撃では、攻撃対象者を安心・油断させるためのさまざま工夫がなされている点に大きな特徴がある。

特徴 1：関係の深い送信者へのなりすまし

見ず知らずの人物から送信されたメールに対しては多分に警戒を払うものの、面識のある人物や自分と関係のある人物から送信されたメールに対しては、警戒心が緩みがちである。また、たとえ警戒していても、添付ファイルを開かないと必要な情報を入手できず、自己の業務に支障が生じるのでは、と懸念して開いてしまう場合もある。

事例 3・4 では政府機関や取引先といった、攻撃対象と業務上の関係が深い組織・法人に所属する人物を装うことで、また事例 5 では攻撃対象の所属する組織の幹部を装うことで、添付ファイルを開くよう誘導している。また、この事例では、短時間に一斉にメールを送信することで、組織内で「怪しいメールが届いている」などの情報が共有される前に、攻撃対象が添付ファイルを開く可能性を高めようとしているものと考えられる。

特徴 2：攻撃対象とのやりとり

見ず知らずの人物から受信したメールであっても、それが自然な方法でなされ、かつ複数回のやりとりがなされると、いつの間にか警戒心が緩んでしまうこともある。事例 1・2 では、企業のウェブサイトに掲載しているメールアドレスにて受信しており、企業側からすると、見ず知らずの人物からメールが送られてきても不審な点はない。さらに、不正告発や採用希望といった企業の担当者が何らか対応すべき事項に関する「問い合わせ」を行い、これに対する企業からの返信に、「告発書」「履歴書」のように、極めて自然な方法で不正プログラムを送信している。担当者の心理を巧妙に突いた手口であるといえる。

特徴 3：添付ファイルの工夫

添付ファイルにも、攻撃対象の警戒を招かないよう、さまざまな工夫がなされている。
事例 1 では、添付された圧縮ファイルは、RLO 機能（注 2）を利用して exe 形式の実行ファイルを文書ファイルに偽装していた。また、事例 2 と同種のケースで、添付ファイルを開くと実際に「履歴書」を装った文書が開き、採用担当者が、不正プログラムであると気がつきにくくする工夫がなされたものもある。

さらに、これらをパスワード付きの圧縮ファイルで送信し、ウイルス対策ソフトで検知されないようにしており、ウイルス対策ソフトを使用しているからといって安心はできない。

（注 2）ファイル名を右読みから左読みに変える機能で、例えばファイル名「fdp.exe」は、RLO 機能により「exe.pdf」と表示されるため、実行ファイルを PDF ファイルに偽装することができる。

2. 遠隔操作ウイルス事件

2012 年から世間を騒がせていた「遠隔操作ウイルス事件」の容疑者が、2013 年 2 月に逮捕された。

この事件では、ネット掲示板のスレッドを経由し無料ソフトをダウンロードした個人のパソコンが遠隔操作され、脅迫メールの送信や自治体のウェブサイトに犯罪予告の書き込みをした疑いで、４人が誤認逮捕されている。

ここでは、警視庁が公表した資料を基に「遠隔操作ウイルス事件」を振り返り、どのような対策をとりうるかについて解説する。

2.1　事件の経緯

本事件の主な経緯は、以下のとおりである。

日時	書き込み・送付先	内容	パソコン使用者
6月29日	横浜市役所のウェブサイト	小学校に対する無差別殺人予告	A氏
7月29日	大阪市中央区役所のウェブサイト	繁華街の無差別殺人予告	B氏
8月 1日	航空会社のウェブサイト	航空機爆破予告	B氏
8月 9日	２ちゃんねる	イベントの無差別殺人予告	C氏
8月27日	子役タレントへのメール	殺害予告	D氏
8月27日	幼稚園へのメール	無差別殺人予告	D氏
8月29日	２ちゃんねる	アイドルグループ無差別殺人予告	D氏
9月10日	２ちゃんねる	伊勢神宮における無差別殺人予告	E氏

上記の事件において、警察は「ＩＰアドレス」(注 3) を追跡することで、事件に使われたパソコンの使用者を割り出し、4 名を逮捕した。

しかし、その後の捜査で、これらのパソコンは「遠隔操作ウイルス」と呼ばれる「IEsys. exe」というバックドア型不正プログラム(注 4)に感染しており、容疑者が外部から遠隔操作していたことが判明した。

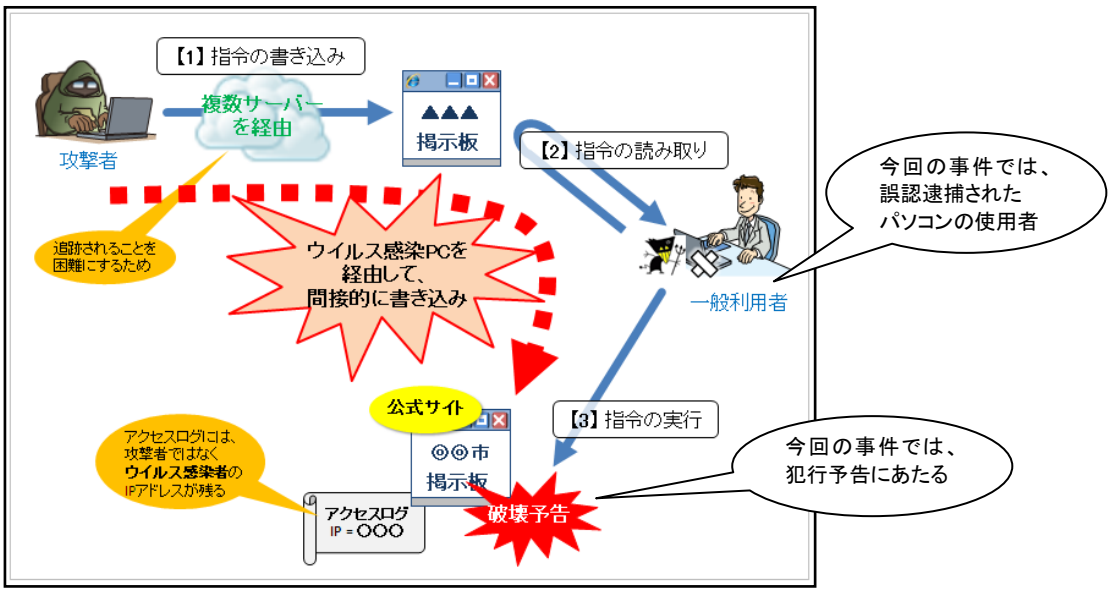
(注 3)インターネットなどのＩＰネットワークに接続されたコンピュータなどに割り振られる識別番号のこと。

(注 4)バックドア型不正プログラムとは、トロイの木馬の一種。ネットワークを介して被害者のコンピュータなどを自由に操ったり、パスワードなど重要な情報を盗んだりすることを目的としているプログラム。なお、被害に遭ったコンピュータはバックドア（裏口）ができ、そのバックドアが盗んだ情報の出口となる。

2.2　ウイルス感染後の遠隔操作の仕組み

攻撃者が他人のパソコンを遠隔操作する仕組みは以下のとおりである（図 4)。

＜図 4：攻撃者が遠隔操作を行うイメージ図＞



出典：独立行政法人情報処理推進機構　第 12-30-265 号「今月の呼びかけ」

①【1】指令の書き込み：

攻撃者が別の掲示板に、ウイルス感染パソコンへの指令に相当する文字列を書き込む。

②【2】指令の読み込み、【3】指令の実行：

遠隔操作ウイルスが感染したパソコンから【1】の掲示板の特定のページを定期的にチェックし、自身への指令に相当する文字列を発見すると、その指令を実行する。今回の事件では、脅迫メールの送信や自治体のウェブサイトに犯行予告の書き込みの指令が実行された。

2.3　今回の事件の特徴

この事件により、パソコンの「遠隔操作ウイルス」が一躍有名になったが、実はパソコンを遠隔操作するウイルス自体は、2004 年ごろから発見されている。2011 年に国内で話題となった「標的型サイバー攻撃」で使われたウイルスも、同種のウイルスである。

今回の事件の特徴は２つある。ひとつは、攻撃者から IEsys.exe へ指令を出す際に、ある掲示板のスレッドを経由して行っていたことである（図 4 を参照）。この方法を行うことで、より証拠が残りにくくなり、アクセス元の攻撃者まで追跡していくことが困難になってしまう。

もうひとつの特徴は、IEsys.exe が攻撃者自作のプログラムであったことである。一般的なウイルスは、すでに流通している不正プログラム作成ツールキットを用いて作成されることが多いが、IEsys.exe は攻撃者が一からプログラミングしたとみられている。不正プログラム作成ツールキットを用いて作成された不正プログラムは、既存のウイルス対策ソフトに検知される可能性が高いが、今回のようなオリジナルのウイルスの場合、これを検知する対策ソフトが開発されていないため、パソコンは確実に感染してしまう。

3.標的型メール攻撃ならびに遠隔操作ウイルスへの感染防止対策

ここまで「標的型攻撃メール」と「遠隔操作ウイルス」の事例とその特徴を紹介してきたが、これらへの対策を別物として考える必要はない。これさえやれば完璧であるという対策はないが、ウイルスを「入れない」「早く見つける」「データにアクセスさせない」「出さない」という多層防御を実施するという考え方が重要である。個人レベルでは、このうちウイルスを「入れない」ことを徹底すべきである。具体的には、不審なメールやサイトにアクセスしない、パソコン等は常に最新のセキュリティ状態にする、自身の個人情報等をウェブサイト等に安易に入力せず、慎重に取り扱うなどである。

一方、組織レベルでは、多層防御を漏れなく行うことが望ましい。ここでは、組織レベルでとるべき対策について簡単に解説する。なお、標的型サイバー攻撃に対する具体的な対策については、「情報セキュリティニュース＜2011　No.4＞」も参照いただきたい。

(1)ウイルスを「入れない」対策(入口対策)

①使用しているＯＳやアプリケーションの脆弱性を解消する(注 5)

②ウイルス対策ソフトの導入ならびに最新版へ確実に更新する（“振舞い（ヒューリスティック）検知”(注 6) 機能が実装されたウイルス対策ソフトであればなお可）

③標的型攻撃の発端となるメールを排除する（スパムフィルターなど）

(注 5)脆弱性を修正するパッチを、OS だけでなくアプリケーションも含めきちんと適用する。

(注 6)「ウイルスは、大体こういう動作をする」 という経験則から、ウイルスと同じような動作をするプログラム を「疑わしいファイル」として予測検知する。ただし、100%正確であるわけではない。

(2)侵入したウイルスを「早く見つける」対策(セキュリティマネジメント)

①ネットワークログ・サーバーログを定期的に分析する

②アクセスログを定期的に分析する

※ログの存在は、攻撃者にとっては都合が悪いため、ログを正常に採取されないように仕掛けを施されることがある。ログ自体のセキュリティに配慮が必要となる。

※膨大な量のログ情報を収集することはできても、その分析についてはシステム担当者に依存することになるため、システム管理部門の要員体制によっては、アウトソーシングすることも含めた検討が必要となる。

(3)重要なデータに「アクセスさせない」対策（データの保護対策）
①ユーザー認証によりアクセスを制限する
②重要データのファイルなどを暗号化し、暗号鍵(注 7)を安全に管理する
(注 7)暗号化したデータを安全に保つためには、唯一の秘密情報である鍵を安全に保つことが非常に重要となる。
(4)重要な情報を「出さない」対策（出口対策）
①端末間、部門間のネットワーク通信を制限する
②組織の端末から外部への直接通信を抑止する
③重要なデータが保管されたサーバをインターネットから隔離する

4. 今後増加すると考えられるスマートフォンへの標的型攻撃

さらに、急速に普及しているスマートフォンでも標的型サイバー攻撃が現実のものになろうとしていることに留意が必要である。

2012 年 9 月に、大手セキュリティベンダーが Android OS 向けに標的型攻撃を行う不正アプリを初めて発見したと公表している。これは、インドの軍事研究施設や、日本やチベットなどを狙った「Luckycat（ラッキーキャット）」(注 8)と呼ばれる標的型サイバー攻撃の調査を進める中で、発見されたものである。ただし、この時点では開発途中であり、完成していなかった。

現在、業務効率の向上を図るために、スマートフォンやタブレット端末を社員に配布し、自社のイントラネットと接続できるようにする企業が増えている。これは、見方を変えれば、スマートフォンを攻撃することにより、価値の高い情報を入手できる機会が増えているともいえる。上記のとおり、既にスマートフォンにおいても、利用者をだまして不正アプリをインストールさせるさまざまな手法が存在しており、これらをより巧妙に発展させた標的型攻撃がいつ本格的に行われてもおかしくない。

(注 8) 「Luckycat」は「標的型メール攻撃」の手口を利用している。

5. おわりに

報道によれば 2013 年 3 月中に、経済産業省において日本政府として初めて発電所やガスなど社会インフラの稼働停止や誤作動を狙うサイバー攻撃を防ぐための対策を講じる専門チームが立ち上げられる。サイバー攻撃が、我々の日常生活において放置できない脅威となりつつあると政府が認識していることの表れであると言える。

インターネットは、事業活動や日常生活の中でもはや欠くことのできないものとなっているが、これに伴う危険や脅威が日々増大していることについても、これを利用する企業や個人は十分認識しておく必要がある。

インターネットに潜むリスクについての情報を絶えず入手したうえで、必要な対策を迅速・適切に行ってリスクに備えていただきたい。

インターリスク総研 コンサルティング第二部　ＢＣＭ第二グループ
アソシエイト　沖　　歩（オキ　アユミ）

株式会社インターリスク総研は、ＭＳ＆ＡＤインシュアランスグループに属する、リスクマネジメントについての調査研究およびコンサルティングに関する専門会社です。
弊社では情報セキュリティに関するコンサルティング・セミナー等を実施しております。
コンサルティングに関するお問い合わせ・お申込み等は、下記の弊社お問い合わせ先、または、あいおいニッセイ同和損保、三井住友海上の各社営業担当までお気軽にお寄せ下さい。

お問い合せ先
㈱インターリスク総研 コンサルティング第二部
TEL.03-5296-8918　　http://www.irric.co.jp/

本誌は、マスコミ報道など公開されている情報に基づいて作成しております。
また、本誌は、読者の方々が企業の情報セキュリティへの取り組みを推進する際に、役立てていただくことを目的としたものであり、事案そのものに対する批評その他を意図しているものではありません。