NPO ISEF
Not-for-Profit Organization of Information Security Forum

特定非営利活動法人
NPO情報セキュリティフォーラム

NPO-ISEF 情報セキュリティレポート：2011-No.06

企業におけるサイバー攻撃への対策

株式会社ディアイティ　セキュリティサービス事業部
部長　山田 英史（Yamada Eiji）

【著者経歴】
1997 年より情報セキュリティ製品の市場開拓に従事するかたわら、各種雑誌記事の執筆や各種セミナーの講師を務めている。2002 年からは企業や自治体の情報セキュリティ構築支援を主な業務としている。2006 年度 経済産業省商務情報政策局長表彰。

昨年以来 Anonymous の活動や標的型攻撃等のサイバー攻撃が繰り返しニュースに流れ一般の関心事となり、また実際に国内大手企業や政府機関が攻撃を受けていることを公表するに至り国も対策に動き始めた。実際にはずっと以前からサイバー攻撃の脅威にさらされていたのに、ことの深刻さにやっと気付いたようにも見えるが、それはさておき、サイバー攻撃、特に標的型攻撃について弊社が関わった事案の経験も踏まえその対策について整理してみよう。

1. サイバー攻撃の分類

サイバー攻撃は、以下のように２パターンに分類することができる。

表１： サイバー攻撃のパターン

目的	攻撃者	攻撃対象	特徴
情報の窃取	某国、競合	国家、防衛・原子力産業等	・徹底した偽装行動 ・成果不明
制裁	Anonymous 等	自分たちの権利を奪おうとする者	・宣言して行動 ・成果公表

上記の２パターンとも「明確な目的を持って、目的達成のために日々の研究を怠らず、根気強く、失敗してもトライし続ける」という共通の特徴を持つ。手口についても、様々な攻撃を複合的に用いるという点で似ている。標的型攻撃の方が事前の調査・準備が周到なところがあるが、それ以外は２パターンとも同様の対策が適用できるため、ここから先は標的型攻撃を題材に対策を解説して行こうと思う。

2. 標的型攻撃の手口

標的型攻撃は図 1 のように段階的に進行する。

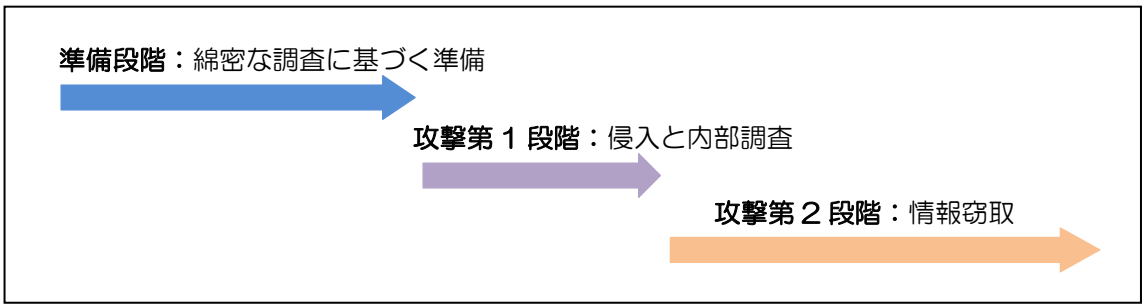

図 1： 標的型攻撃の進行

準備段階では、公開情報やソーシャルエンジニアリングにより侵入に使える情報を集め、その情報を参考にして偽装したメールやそれに添付する不正プログラムを用意する。次の攻撃第 1 段階ではまだターゲットを絞り込まず広範囲に不正プログラムを感染させ、端末等からできるだけ多くの情報を収集しそれを調査・分析して内部環境を把握する。その後の攻撃第 2 段階では、第 1 段階で調査・分析した結果を利用し攻撃対象に合わせカスタマイズした不正プログラムを用意してそれを送り込み、特定のサーバ上の情報を時間をかけて少しずつ気付かれないように外部に送出する。

昨年 9 月に公表された防衛産業をターゲットにした標的型メール攻撃の例でもう少し詳しく攻撃手法を見てみよう。

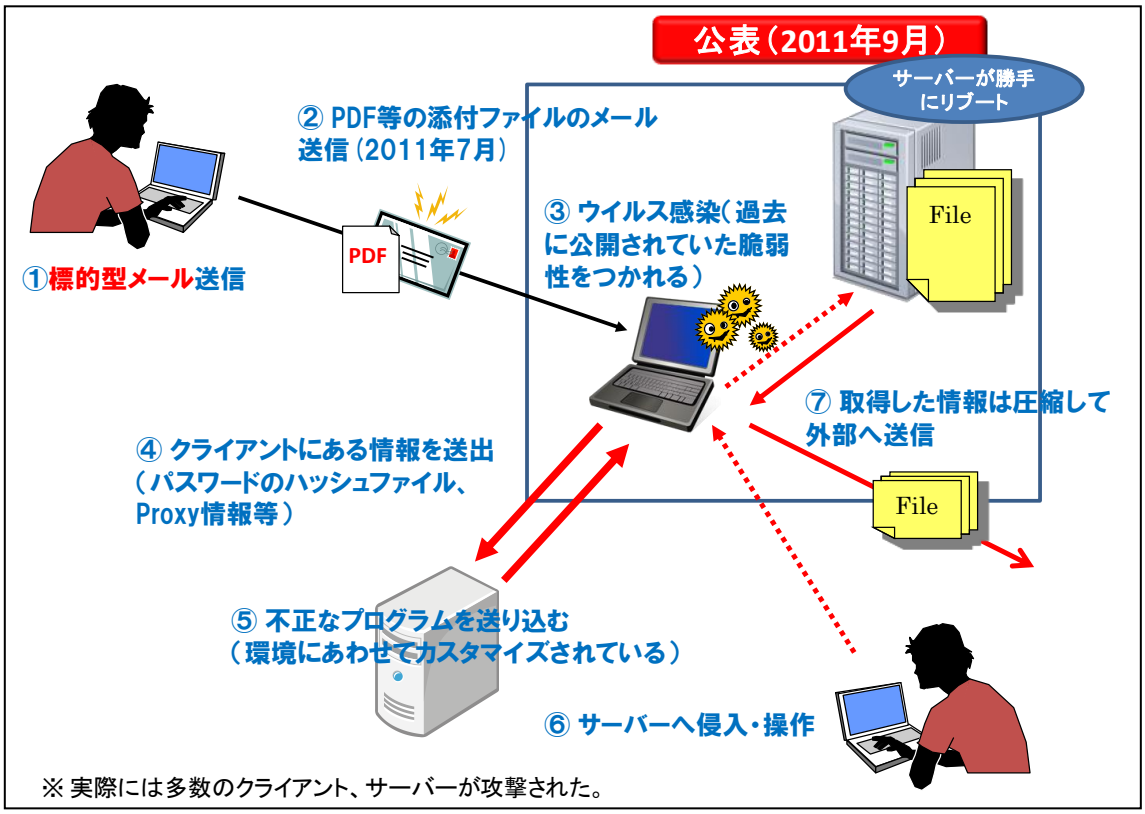

図 2： 標的型メール攻撃

図２の事例では標的型メールの送信から始まっているが、そのメールは、事前の綿密な調査に基づき送信元は同僚や取引先に詐称され、本文は実際の業務で使用されたメールから流用するなど巧妙な偽装をほどこし、受信者がうっかりメールを開封して添付ファイルをクリックするように工夫されている。添付ファイルを実行してしまうと外部のサイトへアクセスして不正プログラム（ウイルス）をダウンロードし、それが社内 LAN を通じて広範囲に感染する。この時点では防衛に関係ない部署も含めとにかく感染を広げ集められるだけ情報を集める。集めた情報の中にサーバ管理者の認証情報やプロキシ情報等の有用な情報が含まれていれば、それを足がかりに次の段階に進む。ここまでが攻撃の第一段階にあたる。（図の①～④）

図の⑤以降が攻撃の第 2 段階になるが、第 1 段階で集めた情報を利用して、社内のサーバへ侵入するためにカスタマイズした不正プログラムを送り込み、少しずつ時間をかけてサーバ内データを外部のサイトに送出する。この時、目立たないようにデータ送出は 80 番ポートを使って Web アクセスに偽装したり、社員が操作している間だけ送出するなど監視から逃れる工夫がされている。さらに、送出されるデータは rar や zip 形式あるいは独自の方式で圧縮または暗号化されているため、データ流出に気付いても何が窃取されたか把握できないことが多い。

3. 標的型攻撃への対策

前述したように、攻撃の手口は複合的で攻撃対象となる組織に合わせた手法が用いられ、かつそれが継続的に行われる。それに対抗するためには、守る側も複合的で状況に合わせた柔軟な対策を継続して行わなければならない。

以下に、標的型攻撃のためのセキュリティ対策を第 1 段階（侵入・調査）と第 2 段階（情報窃取）のそれぞれの攻撃段階に対応して整理し解説する。

表２： 各攻撃段階に対するセキュリティ対策

攻撃段階	セキュリティ対策
第１段階 （侵入・調査）	(1) 基本的な対策を徹底する
	(2) 検知能力を上げる
第２段階 （情報窃取）	(1) ターゲットを守る
	(2) 監視能力を上げる
	(3) 分析能力を上げる
	(4) 長期的な戦略に基づく取り組み

■ 第１段階（侵入・調査）への対策

日々進化し巧妙になる標的型攻撃に対しては、偽装された攻撃を完全に防ぐことは困難で、侵入されることを前提にした対策を考える必要がある。とは言え、侵入の可能性を減らし被害の拡大を低減する努力はすべきで、特に基本的な対策を徹底することはコスト負担も比較的小さく効果が期待できる対応である。

(1) 基本的な対策を徹底する

第１段階で用いられる攻撃は一部にゼロデイ攻撃も含まれるが、大半が既知の脆弱性を攻撃する。したがって、OS やアプリケーションを最新にする、ウイルス定義ファイルを最新にするといったセキュリティの基本を徹底することが対策として有効である。可能な限り OS やアプリケーションのアップデートやウイルス定義ファイルの更新は“自動”に設定することが望まれる。加えて、PDF Reader の JAVA Script の OFF や不要なプロセスの停止など不要なデフォルト設定を見直す。また、付属的な対策としてスパムメール対策も有効である。この段階では広く無差別に攻撃されるため、全社で徹底しなければ効果が薄い。

(2) 検知能力を上げる

図 2 のケースもそうだが、過去の事例では攻撃の発見に際し社員からの報告が重要な役割をはたしている。端末やサーバの動作が遅い、サーバがよくリブートする、疑わしいメールが届いた等、いつもと違うことに対し敏感になるように社員を教育し、気付いたことがあれば小さなことでも報告するよう周知する。そのために、社内に報告窓口も設置する。

また、自社には標的になるような情報は無いなどと無関心にならず、取引先等に防衛や原子力その他重要インフラに関わる企業や国の機関が含まれる場合は、その組織を攻撃するための足がかりとして自社が狙われるかもしれないと考え、少なくとも第 1 段階の攻撃に備えた対策は取っておくようにする。

■ 第 2 段階（情報窃取）への対策

第２段階の攻撃には、侵入されることを前提に、いかに社外に情報を出さないか、あるいは窃取されたとしても損失をいかに最小限にするかという発想で対策を考える。

(1) ターゲットを守る

標的型攻撃でターゲットになるのは、サーバ上の情報とそれを窃取するための管理特権の認証情報（ID/パスワード等）である。したがって、それらを保護することが損失を最小限にするための重要な対策になる。例えばサーバ内のデータを暗号化することによりそれが窃取された場合の被害を最小限にする。また、管理者のパスワードを短周期で変更するあるいはワンタイムパスワードにすることで、奪われた管理者権限を悪用できる可能性を最小限にするといった対策が考えられる。

(2) 監視能力を上げる

従来は社外から社内への不正アクセスを警戒し監視していたが、内部情報が社外に送出されることも監視対象に付け加える必要がある。最近よく言われる出口対策のひとつであるが、社内から社外への通信をファイアウォールや IDS、IPS で監視し、可能であればそれを止める。しかし、先に書いた通り Web アクセスに偽装するなど特殊な通信ではない上、通信量が急激に上がる等の顕著な現象が見られるわけではないので監視対象を限定することは簡単ではない。ICMP のデータグラムに窃取した情報を紛れ込ませたり、DNS 通信に偽装して送出する等の手法も確認されており益々監視が難しくなっている。そんな中で監視のポイントを挙げるとすると、“海外サイトとの間で短期間にデータ量の小さい通信が頻発している”や“特定サイトとの HTTP/HTTPS 通信で in より out が多い”

といった傾向をもつトラフィックの検知が考えられる。アメリカ、中国、韓国などが代表的な送出先であるが、まずは海外との通信はすべて注意する。

また、出口対策ではないが、社内の端末間通信も監視対象にすることで不正プログラムの感染を検知できることがある。さらに、送出前にファイルを圧縮して一時的に保持することも多いため、サーバ等のディスク空き容量が急激に減少していないかディスクの容量変化を監視することも一定の効果がある。

(3) 分析能力を上げる

情報流出が疑われる場合、その原因や被害規模を分析するために各種ログを解析する必要があることから、それに備え、端末、サーバ、ドメインコントローラ等のイベントログ、アクセスログ等を保存しておくことが望まれる。市販されているログ管理ツールを導入できればなお良いが、とりあえず取っておくだけでも良いのでログを残すようにする。また、可能な限りログはシステム本体ではなくログサーバ等に転送して保存するようにする。多くの攻撃で、攻撃の痕跡となるシステム上のログを消去・改ざんすることが確認されているので、ログは別に保存して保護することが望ましいからだ。

ログを保存する場合、その保存期間が問題になることがあるが、過去の事例で情報流出から発覚まで半年以上かかったケースも見られるため、半年間は保存しておいた方が良いという意見もある。また、欧州連合（EU）のデータ保護法や米 Google のサーバログが 18 カ月保存としているためそれに倣う企業もある。おおよそ半年間～1 年間が目安というところか。

ところで肝心の分析だが、ログの中から何を見つけ出すのか評価基準が明確でないと実施は難しい。独力での分析が難しいと判断するなら、企業はログの保全にだけ努め、分析は専門業者に委託すると良いだろう。

なお、全てのシステムで時間を同期しておくことも重要である。数秒ずれるだけでシステム間のログの相関分析が困難になる。入室記録や監視カメラ記録の時間同期もお忘れなく。

(4) 長期的な戦略に基づく取り組み

ここまで列記した対策を実施するためには時間をかけていくつもの課題を解決していく必要がある。例えば、OS を常に最新にするとした場合、ベンダーから OS のアップデートによるアプリケーションの動作保証ができない、あるいは検証に費用が発生すると言われアップデートに踏み切れないでいるという話を効くことがある。しかし、PSN（ソニー）事件でも一度内部に侵入された後にサーバがことごとく被害を受けたことからわかる通り、サーバを最新状態にせず放置しておくことの弊害は大きいことは明白である。アプリケーションやハードのベンダーとはアップデートの責任範囲、実施条件を今一度調整し合意しておく必要がある。また、サーバにデータ暗号化機能を実装する場合も、既存のシステムに後付けで暗号化機能を追加するのは難しいため、次期改修に合わせて検討といったことになるだろう。監視やログ機能の向上についても機器の増設や設定変更が伴うはずだ。

投資効果も考えると、標的型攻撃のように高度な攻撃に対しては、長期的な戦略に基づく業務フロー見直しとシステム改修に本気で臨まなければならない。取り急ぎ検討しなければならないのは情報の分類と集中化である。暗号化するにしても全てのデータを暗号化するといった不効率で不経済なことはできない。同様に、データベースに重要な情報も一般情報も混在しているならクエリを記録するとした時に莫大な量を想定しなければならず現実的ではない。したがって、情報は重要度に応じ分類

し分割し保護対象を絞り込まなければならない。さらに、監視する対象が分散していると監視のための装置（ログ管理装置、パケット監視装置等）を大量に配置しなくてはならず大きな投資が必要となる。可能な限り保護対象のサーバ等は集中して管理できるように配置する。ただし、一方で集中することで一箇所の防御が破られると全てに被害がおよぶというリスクもあるため、効率化とリスクのバランスを考えて設計しなければならない。

また、監視能力の向上の項で述べたが、一般的な通信に紛れて情報が送出されることに象徴されるように異常を検知するのがきわめて難しい。基準となる“正常な状態”が決まっていなければ異常を発見することはできない。そこについては時間がかかるが業務のフローやプロセスを整備し、業務で利用するアプロケーションも標準化し、アクセスする海外サイトを限定するなどして正常な状態とは何かを明確に定義して、それから逸脱する処理や通信を異常として検知できるようにする。それを徹底すると柔軟性のない窮屈な業務環境になるというマイナス面もあるが、防衛や重要インフラの運用に関わる組織ではその可能性だけでも検討していただきたい。

現在のサイバー攻撃は攻撃者がプロであることから、防御する側も専門的な力量を要求される状況となっている。企業は最新の情報の収集につとめ、具体的な攻撃手法を研究し柔軟にそれに対応しなければならない。

今回提示した対策を実装するためには市販のツールやサービスも利用できるので、それらの情報収集も怠らずに行っていく必要がある。また、社内に専門家を置いている場合であっても、外部の専門家との接点を持ち支援を受けられる環境を整えておくことをセキュリティベンダーの立場から付け加えておきたい。

2012 年3月２８日発行

特定非営利活動法人　NPO 情報セキュリティフォーラム
〒221-0835
神奈川県横浜市神奈川区鶴屋町 2-17　相鉄岩崎学園ビル
TEL(045)311-8777　　FAX(045)311-8747
E-Mail: isef@isef.or.jp　　URL: http://www.isef.or.jp