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.03

セキュリティー監視の現場から見た最近の脅威

日本アイ・ビー・エム セキュリティー・オペレーション・センター
朝長 秀誠（Tomonaga Shusei）

【著者経歴】

2007 年日本 IBM 入社。全世界 4,000 社以上のセキュリティー機器（IPS など）の監視を行うセンターにてセキュリティー監視、脅威動向調査に従事。日経 ITpro「今週の SecurityCheck」の連載や IBM ブログ「Tokyo SOC Report」からセキュリティー情報を発信中。

筆者は最近「攻撃が増えて忙しくないですか?」とよく聞かれる。2011 年９月頃から、連日のように大企業や政府機関がサイバー攻撃の被害にあったというニュースが報道されていたため、そのように感じている方も多いのではないだろうか。しかし、セキュリティー監視の現場から見ると攻撃が増えていると感じたことは全くない。むしろ３、４年前と比べると全体の攻撃総数は減っているような気さえする。

2011 年後半に報道された大企業や政府機関への「サイバー攻撃」の多くが、標的型メール攻撃による被害であったことが報告されている。標的型メール攻撃とは、ある特定の組織や個人に向けて不正なメールを送信する攻撃である。大企業や政府機関が標的となっている標的型メール攻撃は、最近始まったように思われがちだが、セキュリティー監視の現場では数年前から確認されている。最近になって攻撃による被害が表面化したため騒がれているが、知られていない被害は以前からあったのではないかと推測される。

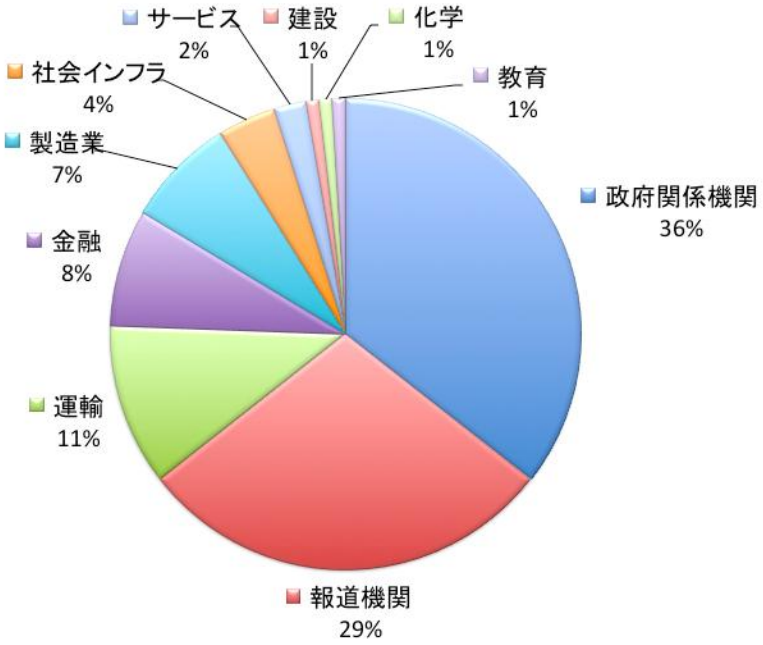
以降では、最近注目されている標的型メール攻撃について、世界に９カ所ある IBM セキュリティー・オペレーション・センターの一つで、主に日本国内の動向を監視している東京セキュリティー・オペレーション・センター（以下、東京 SOC）での検知状況について解説し、対策のポイントについて紹介する。

■東京 SOC での標的型メール攻撃検知状況

標的型メール攻撃は、メールを受信したターゲットが思わず開いてしまうような件名や文面になっている。例えば、最近の時事ニュースを題材にしたものや、行事などスケジュールの連絡に見せかけたもの、会議の議事録に見せかけるものなどがある。その中でも特に多いのが、時事ニュースを題材にしたタイプの標的型メール攻撃である。2011 年には、特に震災の情報に見せかけた不正なメールが多数確認された。また、2011 年 12 月には北朝鮮総書記死去のニュースに便乗したものも確認されている。

それ以上に悪質なものとして、すでに送信されたメールを引用するタイプがある。ターゲットの関係者が送受信したメールの一部を変更したり、そのメールの返信に見せかけたりすることでターゲットが受信した不正なメールを疑いなく開いてしまうようにするのである。このタイプのメールを受信することは、引用されたメールを送受信した関係者の誰かが、攻撃者によってメールを盗聴されている状態にあることを意味しており、すでに危険な状態であると言える。すぐに、どこから引用されたメールが漏洩しているのかの原因調査を始める必要がある。

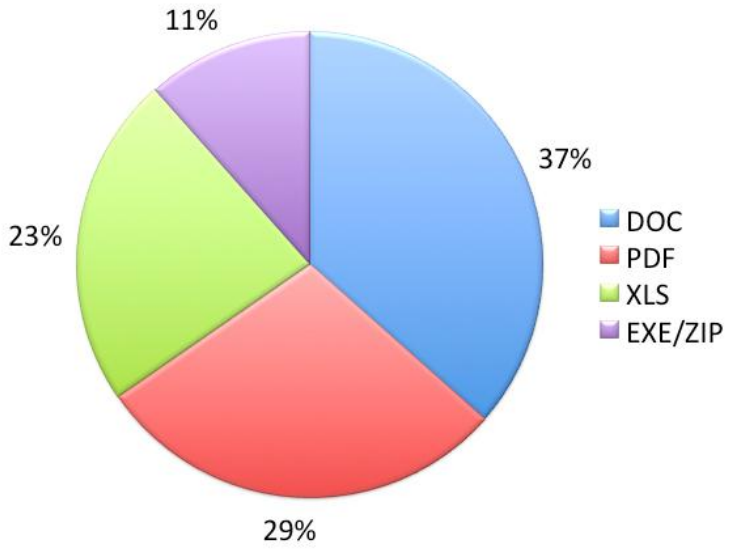
標的型メール攻撃のターゲットとなるのはどのような組織だろうか。以下は、東京 SOC で確認した 2011 年に標的型メール攻撃のターゲットになった組織の業種別割合を示している。



標的型メール攻撃のターゲットとなった組織の業種別割合
（東京 SOC 調べ： 2011 年 1 月～2011 年 12 月）

標的型メール攻撃は、政府機関や大手製造業がターゲットになっているイメージが強いが、現実には様々な組織がターゲットとなっており、報道機関や運輸業、金融、社会インフラに関連する企業までもが攻撃を受けている。自組織が政府機関や大企業でないため、攻撃のターゲットにならないのではないかと考えている方もいると思う。しかし、攻撃者は最終的なターゲットに向かうためにまず、その組織の子会社や関連する取引先から攻撃を進めている場合もある。そのため、政府機関や大企業でなくても攻撃者のターゲットになるという意識を持っていた方がよいだろう。

標的型メール攻撃には、不正なファイルが添付されていることが多い。攻撃者は、メールを受信したターゲットにこの添付ファイルを開かせることで、マルウェアに感染させようとする。以下は、東京 SOC で確認した標的型メール攻撃に添付されたファイルの識別子割合を示している。



標的型メール攻撃に添付されていた不正なファイルの拡張子
（東京 SOC 調べ： 2011 年 1 月～2011 年 12 月）

標的型メール攻撃には、DOC や PDF、XLS などのドキュメントファイルが添付されていることが多い。これらのファイルには、脆弱性があるドキュメント・ビューアーで表示した際に、マルウェアに感染させようとする攻撃コードが含まれている。例えば、PDF であれば Adobe Reader の脆弱性を悪用する攻撃コードが含まれている。そのため、脆弱性のある Microsoft Office Word や Excel、Adobe Reader/Acrobat を利用していると、標的型メール攻撃の添付ファイルを開いたことでマルウェアに感染してしまう。

また、不正なドキュメントファイルが狙う脆弱性の中には、パッチがリリースされていない脆弱性（ゼロデイ脆弱性）を攻撃するものも存在する。そのような場合は、最新バージョンのドキュメント・ビューアーを利用していてもマルウェアに感染してしまう。

標的型メール攻撃の添付ファイルを開いた場合、RAT（Remote Access Trojan）と呼ばれるプログラムがインストールされることが多い。RAT とは、インストールしたコンピュータをリモートから操作するツールである。RAT は高機能なものが無料で配布されていることが多いため、攻撃者は既存の RAT を攻撃で利用することが多々ある。

RAT を利用すれば、「アプリケーションの実行」「ファイルの転送」など簡単な操作から、「スクリーンショットの撮影」「キー入力の監視」「Webcam による盗撮」「内蔵マイクによる盗聴」など高度なスパイ活動をリモートから行うことができてしまう。攻撃者は、この RAT をインストールしたクライアント PC から情報を詐取したり、内部ネットワークへのさらなる侵入を試みる。

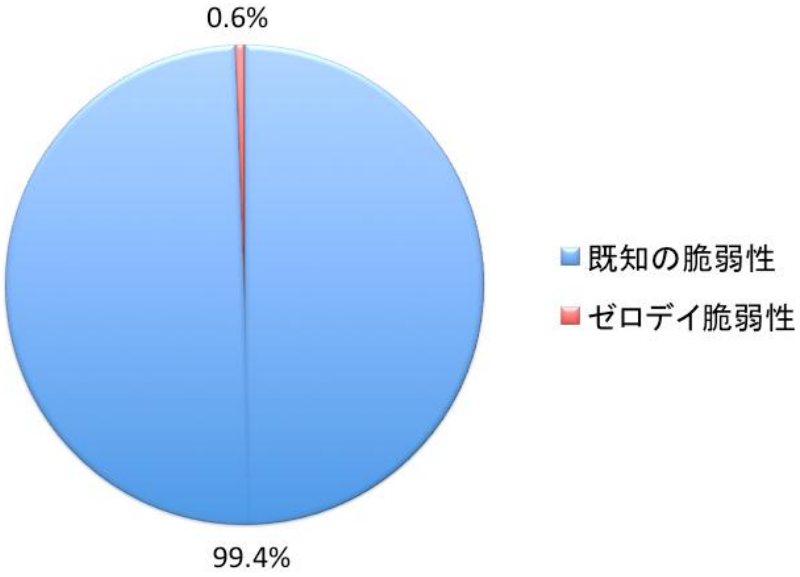
■標的型メール攻撃への対策のポイント

これまで紹介してきたように、標的型メール攻撃では「不正なドキュメントファイル」を送信して「RAT」に感染させようとする。このような攻撃への対策として最も一般的な対策はウイルス対策ソフトを利用することである。しかし、最近ではウイルス対策ソフトで検知できないマルウェアの存在が問題となっている。

ウイルス対策ベンダーでは、マルウェアを収集し、検知するためのルールを作成し、ウイルス対策ソフトに反映させる。そのため、未知のマルウェアであれば検知することができない（ヒューリスティック技術などを利用して、検知できる場合もある）。標的型メール攻撃は、ターゲットとなる範囲が限定されているため、ウイルス対策ベンダーにてマルウェアを収集することが難しく、対策が遅くなるという問題がある。そのため、ウイルス対策ソフトを過信しすぎるのはお勧めしない。

それよりも重要な対策は、OS およびアプリケーションのバージョンを最新の状態にしておくことである。先程、紹介したように標的型メール攻撃に添付されているドキュメントファイルは、Microsoft Office Word や Excel、Adobe Reader/Acrobat の脆弱性を悪用する。そのため、これらのアプリケーションに脆弱性がなければ、RAT に感染することはなくなる。

しかし、アプリケーションが最新の状態でも、ゼロデイ脆弱性を悪用された場合は防げないと思われるだろう。以下は、東京 SOC で確認した標的型メール攻撃がターゲットとする脆弱性の中で、ゼロデイ脆弱性が狙われた割合を示している。



標的型メール攻撃が狙う脆弱性の割合
（東京 SOC 調べ： 2011 年 1 月～2011 年 12 月）

これからも分かる通り、ゼロデイ脆弱性が狙われる割合は、1%未満なのである。そのため、アプリケーションを最新の状態にしておくことは、効果があるといえる。最近では、Microsoft セキュリティパッチの適用は徹底されているため、Microsoft Office に関しては最新の状態であることが多いと予想される。しかし、Adobe Reader などのサードパーティー・アプリケーションまで徹底できている組織は少ないだろう。このようなサードパーティー・アプリケーションに関してもパッチ管理を徹底させることが重要である。

また、組織の人間が標的型メール攻撃などの怪しいメールを受信しても開かないようにするための訓練を行うという方法もある。これは、組織内での標的型メール攻撃に対する耐性を上げることを目的として、不審なメールを模倣したものを訓練対象者に送信し、開いてしまった人物に教育を行うものである。

2010 年頃によく確認されていた標的型メール攻撃には、以下のような不審な点があったため、比較的簡単に不審なメールを見分けることができた。

・メールヘッダーから確認できるメールの送信元が中国などの海外
・メール内の文字コードが中国語（GB2313 など）
・本文や添付ファイルに不自然な日本語を使っている

しかし、昨今では、メールの送信元は国内で、メール内の文字コードも ISO-2022-JP などの日本語、本文や添付ファイルは関係者宛てに送信したメールの返信などを装うことで、自然なものになってきている。今後もさらに標的型メール攻撃は洗練されて疑いにくいものとなってくることが予想される。そのため、人間の注意力に頼る方法には限界があるだろう。訓練を行う際は、人間の注意力でカバーしきれない部分は、セキュリティー技術で補う必要があることを理解したうえで行ってほしい。

今回は、標的型メール攻撃についての紹介に終始したが、これは攻撃の全容から見ると一部に過ぎない。最近、標的型メール攻撃ばかりに注目が集まっているが、これは攻撃の初期段階であり、攻撃者の目的はその後の情報詐取である。標的型メール攻撃の対策ばかりに、気をとられていると、標的型メール攻撃を防げなかった際に、ネットワーク内部で自由に重要情報へのアクセスを許してしまう可能性がある。対策を考える際は、標的型メール攻撃への対策にとらわれず、侵入された後どのように侵入に気付くのか、また、侵入されても重要情報やサーバーにアクセスできないネットワーク設計など、様々な観点から考えていく必要がある。

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