特集　サイバー攻撃の現状と防止策

標的型攻撃の脅威と新たな発想によるセキュリティ対策

独立行政法人情報処理推進機構（IPA）
技術本部セキュリティセンター
情報セキュリティ技術ラボラトリー研究員　大森　雅司

1．はじめに

2012年は、政府機関や宇宙産業などの我が国における政治や技術の中枢機関がサイバー攻撃を受けたことが、メディア等で大きく報道されました。政府機関の情報が外部に漏えいすると、外交・防衛上の不利益を被るなど、国家レベルで大きな影響を与えかねない問題です。今日ではインターネット空間のセキュリティ対策が個人や組織・企業の枠を超え、国家としても無視できない、守るべき領域となってきています。特に、多くのサイバー攻撃の中でも、組織・企業が最も警戒しなければならないのが、「標的型攻撃」です。

本稿では、近年の情報セキュリティを取巻く脅威の変化を踏まえて、標的型攻撃の特徴と対応策について紹介します。

2．変化・増大する脅威

（1）脅威とは

脅威とは「意図×能力（技術）」、「意図×能力（技術）×周辺環境」と表現されます。脅威というと、攻撃の能力面ばかりに注目されがちですが、攻撃者の意図や周辺環境も脅威を計る上で大きな要素になってきます。IT環境の変化もさることながら、ここ数年で攻撃者の意図に変化が見えてきました。システム管理者は、攻撃者の狙いや傾向を知ることで、注力する対策分野を見つけることが重要になります。

（2）システム環境の変化

「ビッグデータ」という言葉が生まれたように、スマートデバイスや公衆無線LANの普及により、「いつでも」「どこでも」インターネットに繋がりやすい環境が整備され、我々の生活におけるオンライン提供での依存度が急激に増しています。

また、運用面の向上を目的に交通システム、電力、水道、ガスといった我々の社会生活に欠かせないシステムにおいても徐々にインターネットに接続されてきており、情報システムとの差異が無くなってきています。環境の変化に加えて、FacebookやmixiにFacebookやmixiに代表されるソーシャルメディアの普及により、情報発信や相互のコミュニケーションのあり方もここ数年で大きく変わってきています。

このようにインターネット社会へのユーザの組込まれ方が、経済的（決済、買い物等）、社会的に依存度が高くなっています。一方で、オンラインに依存するが故に攻撃者から狙われやすく、攻撃を受けた際の影響が大きくなっており、攻撃者の意図も様々な点で変化しています。

（3）攻撃意図の変化

現在の攻撃は、どのような背景・意図で行われているでしょうか。現在の攻撃目的を大きく分類すると以下の四つになります（図１）。

１）愉快犯・社会の混乱を目的とした攻撃

個人の技術者やハッカーが顕示欲や社会混乱を目的に行う攻撃になります。攻撃内容も軽度のいたずらから社会を不安に陥れる行為まで様々あります。昨年、非常に大きな社会問題となった遠隔操作ウイルス事件のように社会を騒がせるケースもこの分類に当てはまります。場合によっては、個人ユーザが事件に巻き込まれたり、攻撃の加害者にされたりする可能性があります。

２）金銭窃取を目的とした攻撃

今日ではインターネット上で決済を行うオンライン決済が一般化しています。また、インターネッ

図１　攻撃者タイプ分類

トバンキングも広く一般に普及しており、インターネット上で当たり前のように金銭を扱えるようになりました。一方で、フィッシング詐欺に代表されるような他人のアカウントを盗み出し、不正に金銭を騙し取ろうとする攻撃が散見されています。シマンテック社の報告によると、ネット犯罪の被害に遭った成人は１秒間に 18 人、つまり、世界中で毎日 150 万人以上が被害に合っていると試算[1]しています。個人ユーザもセキュリティ対策を怠っていると、知らない間に金銭が盗まれている時代になっています。

2009年頃より上記１）２）に加えて、新たに二つのタイプの攻撃意図が顕在化してきました。

３）ハクティビストによる攻撃[1]

個人・組織の主義主張、もしくは政治・文化的に対立する組織への抗議や報復の意味を込めた攻撃が行われはじめました。インターネットの掲示板やソーシャルメディアを通じて攻撃が呼掛けられ、社会的・宗教的に対立する国や組織に対して一斉に攻撃を行うことが特徴として挙げられます。現実世界でいう抗議活動、デモ活動と似たようなことがインターネットの世界でも繰り広げられており、政府機関・金融機関などのシステム管理者にとって、大きな脅威となりつつあります。

４）諜報活動型攻撃

諜報活動は、政治、軍事、経済活動に関する情報について、競争相手や敵対する組織、国家から収集する活動になります。現実の世界においても、複数の国が諜報機関や偵察衛星を保有しているように、日常的に行われている行為です。数年前より、サイバー空間における諜報を目的とした攻撃が確認されはじめています。日本国内でも、組織内部の情報が攻撃者により収集され、外部に漏えいした事例が報告されており、国家の危機管理の問題に発展してきています。

上記四つの攻撃意図について、組織・企業にとって気を付けなければならないのが、諜報活動型攻撃になります。諜報活動型攻撃には、主として標的型攻撃が用いられます。

それでは、標的型攻撃について、攻撃の流れと対策について紹介します。

３．標的型攻撃の脅威

（１）標的型攻撃とは？

近年、「標的型攻撃」という言葉をニュースやメディアでよく耳にすると思います。この「標的型攻撃」の攻撃手法について明確な定義はありませんが、あえて他の攻撃との違いを挙げると、「戦術の巧妙さ」にあります。個人をターゲットにしたフィッシング詐欺やマルウェア感染といった脅威は、単独の手法で広く攻撃を仕掛けて、多くの情報を盗もうとします。一方で、標的型攻撃はターゲットとして定めた組織に対して、確実に攻撃が成功するように、組織ごとに緻密な偵察活動が行われ、攻撃がカスタマイズされています。

また、攻撃によって情報が外部に流出した場合の影響は、非常に大きいと言えます。組織の特殊技術情報が漏洩したケースを想定すると、長年に亘り企業が、費用と労力、知恵を出して開発してきたものが、一瞬にして他の組織に奪われることになり、競争力の低下に繋がりかねません。政府機関の政策に関する情報が、他国に渡ってしまうと、敵を利することとなり、国際社会における交渉力の減衰に繋がってしまいます。標的型攻撃の怖さは、単に情報が流出したといった事象の話でなく、我々の未来に手にする利益が奪われていると言えるかもしれません。

（2）攻撃の流れ

標的型攻撃は、概ね下記のステップで攻撃が実行されます。

1）攻撃準備（偵察）

標的となる組織周辺の情報を収集し、攻撃の準備を行います。

2）初期潜入

1）で収集した情報を基に標的型攻撃メール等でシステムに潜入します。

3）バックドア（通信経路）

設置システムに侵入したマルウェアがバックドアを設置します。

4）ハッキング・情報収集

攻撃者は、バックドアを通じて内部システムのハッキングや内部情報を収集します。

標的型攻撃では、「メール本文の巧妙さ」や「マルウェアの挙動」に注目が集まりがちですが、メールやマルウェアはシステムへの侵入手段と考えるべきであり、真の脅威は実際に情報が盗まれる「4）ハッキング・情報収集ステップ」にあります。図2のように、攻撃者が自身が仮想的にシステム内部に潜入して、ハッキングを行っているようなものです。イントラ内部からのハッキングを想定していない現在のシステムは、このような攻撃に対して脆弱なのが実情です。

（3）攻撃が成功する背景

標的型攻撃が登場してから約10年が経ちますが、残念ながら被害を食い止められていないのが実情です。では、なぜ攻撃が成功してしまうのでしょう？様々な理由が考えられますが、あえて三つ理由を挙げると下記が考えられます。

1）見えない攻撃

標的型攻撃に使われるマルウェアの通信は、通常のオフィス環境で使われている、HTTP、HTTPSといったノーマルな通信になります。そのため、Firewallからは、通常の通信と同じように見えてしまい、通信を遮断することができません。また、IDS・IPSにおいても同様に検知することが難しいです。防御側にとって、見えない攻撃と戦うほど、対策が難しいことはありません。

2）攻撃者がシステムの状況に応じて攻撃方法を変える

攻撃者は、マルウェアを操りながら、情報を収集・分析し、新たな攻撃を仕掛けてきます。特にハッキング・情報収集ステップの標的は、アカウント情報になり、管理者パスワードやActive Directoryなどが狙われます。管理者パスワードが盗まれると、設計したセキュリティ機能も無効となり、攻撃者を自由にさせてしまいます。状況に応じて、攻撃者の打つ手が変わるため、防御側も対策が取りづらい傾向にあります。

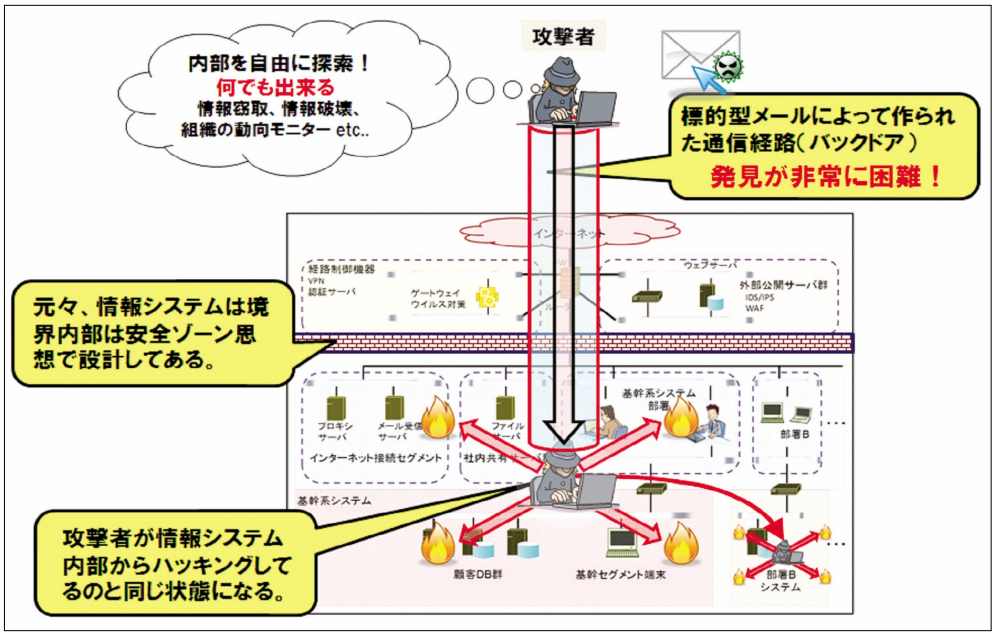

図2　攻撃イメージ

3）巧みなソーシャルエンジニアリング

標的型攻撃は、メールによってマルウェアを配送し、エンドユーザがメールに添付されて　いるファイルやプログラムを実行することで、システムに侵入します。攻撃者は、メール受信者が確実にファイルを開くように巧みなソーシャルエンジニアリングを用います。興味を持ちそうな時事ネタや内部に関連した

情報、実在メールの返信といった例もあります。受信者は、実在している人からのメールであるため、偽物とは気付けずファイルを開き、マルウェアに感染してしまいます。

４．新しい発想による対策

標的型攻撃の仕組みと対策の難しさを述べましたが、現状のセキュリティ対策は、標的型攻撃に対して、十分でないのが実情です。これまでのセキュリティ対策アプローチでは、限界が見えてきており、発想転換を迫る時期に来ています。

（1）実害を防ぐ対策へ

これまでのセキュリティ対策は、外部からの攻撃を内部に入れないために様々な対策が取られてきました。Firewallやアンチウイルスソフトなどは、ほとんどの企業で導入されていることと思います。それに加え、IDS/IPSなどを導入する企業も増えてきています。さらにシステム的な対策だけでなく、ソーシャルエンジニアリングの対策や脆弱性対策などの利用者への教育も行われてきました。しかし、残念ながら攻撃手法は日進月歩で進化しており、対策をすり抜ける攻撃が出てきています。このような背景もあり、IPAではセキュリティ対策の発想を転換することを検討しました。

本攻撃の脅威の本質について考えた場合、組織にとって一番の脅威は、システム内部の機密情報が盗まれることです。一方で、今までの対策は、マルウェアや不正アクセスなどの脅威を内部に入れないことを重視した対策でした。当然、脅威をシステム内部に入れないことも対策として重要ですが、それ以上に情報を盗まれないことに着目した対策を行うことが重要です。

（2）攻撃を封じ込めるシステム設計による対策

標的型攻撃の動作を分析すると図３のように一連のシーケンシャルなステップで構成されています。ステップ２が成功しなければ、ステップ３に移れず、攻撃が成立しないシーケンシャルな攻撃になります。

1）攻撃準備（ステップ０）
2）初期潜入（ステップ１）
3）バックドア設置（ステップ２）
4）ハッキング・情報収集（ステップ３）

IPAでは、実際の攻撃事案を分析した上で、上記のステップ２と３に対策の焦点を当て、「外部通信の検知と遮断」、「マルウェアのシステム内拡散防止」の対策に焦点を当てた、下記の八つのシステム設計対策を導き出しました。

1）サービス通信経路設計
2）ブラウザ通信パターンを模倣するhttp通信検知機能
3）RATの内部Proxy通信の検知と遮断
4）最重要部のインターネット直接分離設計
5）重要攻撃目標サーバ(Directory Server)の防御
6）SW等でのVLANネットワーク分離設計
7）容量負荷監視による感染活動の検出
8）P2P到達範囲の限定設計

重要な点は、マルウェアが外部通信および内部拡散しづらいネットワーク環境を構築することです。また、重要な情報を保管しているサーバについては、ネットワークセグメントを分離し、イン

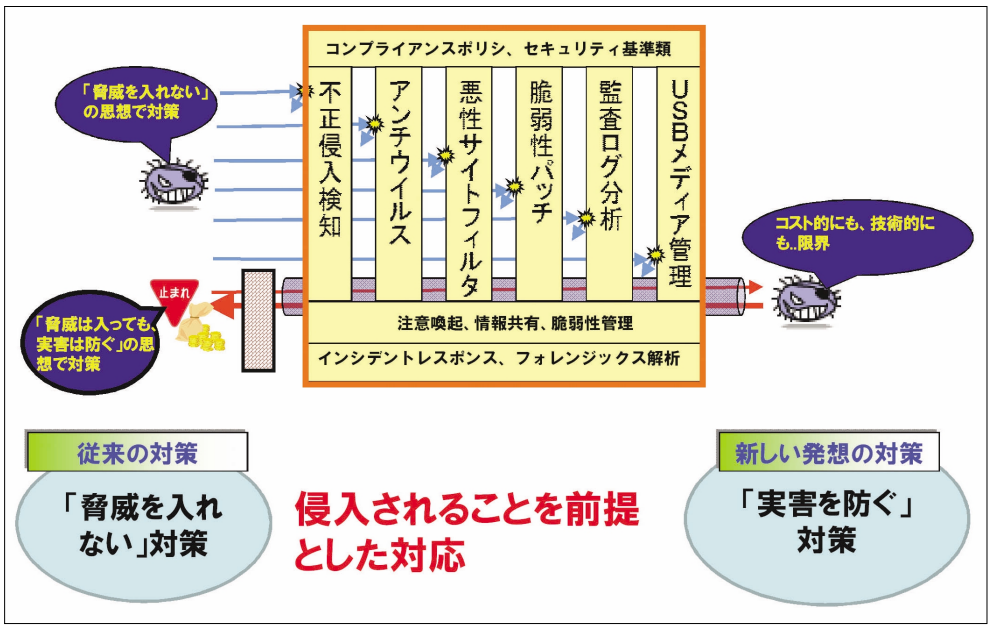

図３　従来の対策から新しい発想の対策へ

ターネットへの接続を制限するなどして、情報が持出されにくいネットワーク環境を構築することで、被害を極小化することができます。

これら対策の詳細については、「『新しいタイプの攻撃』の対策に向けた設計・運用ガイド」[2]で紹介をしています。詳細については同書を参考にしていただければと思います。

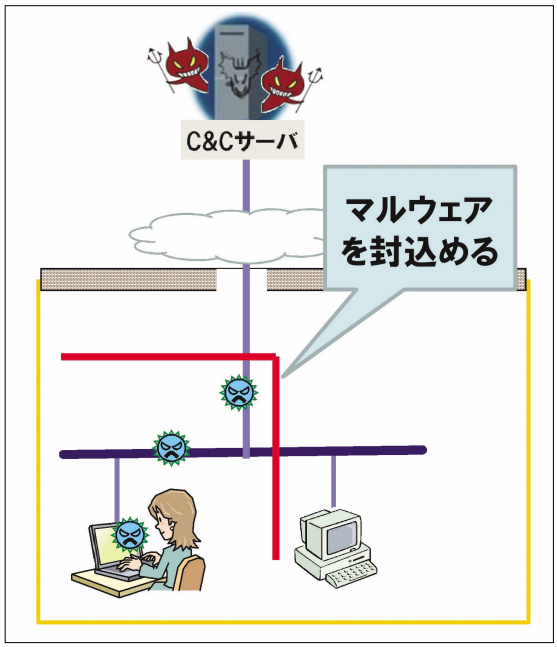

図４　対策イメージ

５．今後の課題

情報セキュリティを取巻く環境は、様々な側面で変化しており、変化に応じた対策を講じることが重要です。以下に、セキュリティ対策における今後の課題を三つ挙げます。

（１）システムトータルでの対策

一つの脆弱性に対して一つの攻撃が行われていた時代は、それに対応するセキュリティ製品を導入していれば事足りていました。しかし、近年ではシステムの設定不備、ソフトウェアの脆弱性、人の心理面に至るまで幅広く弱点を突いた攻撃が仕掛けられます。今後は、情報資産の管理、セキュリティ製品の適切な配置と設定、攻撃を受けても実害を防ぐためのネットワーク設計を含めて、システムトータルで対策することが重要となってきます。そのためにも、システム管理部門、ネットワーク管理部門、セキュリティ部門、さらには、企画部門や経営陣といった様々な立場の人の視点を取り入れて、システムトータルで対策検討を行うことが求められます。

（２）情報共有の仕組み

標的型攻撃は被害に気付きにくく、攻撃情報が表に出にくい傾向にあり、防御側も有効な対策が立てづらいのが実情です。一方、標的型攻撃の大半は、一組織だけが攻撃を受けるのではなく、業界・関連組織が攻撃を受けることが分かっています。そのため、業界・関連組織で攻撃情報や対策情報を共有することは、事前対策を進める上でも有効になってきます。一組織・機関だけの対応には限界が見えてきており、情報共有の枠組みが求められています。

（３）組織ごとのリスクの見極め

同じ攻撃手法であっても防御側の環境や保持している情報の重要度によって、組織ごとにリスクの大きさは変わるものです。各組織においては、攻撃を受けた際の損失を見極めた上で、組織の運用形態や現状の対策状況に合わせて対策を講じることが重要です。

６．おわりに

本稿では、標的型攻撃を中心に近年の脅威の傾向、攻撃分析、対策、課題について概説しました。学術機関においても、研究情報・学生の個人情報など攻撃者に狙われやすい情報が多数存在しています。本文中でも述べましたが、組織内のシステム管理部門、経営陣などが連携して、組織ごとに攻撃を受けた際のインパクトを分析した上で対策を立案することが重要になります。本稿が、そのような取り組みの推進の一助となれば幸いです。

注

(1)「Hacker」と「Activist(活動家)」を合わせた造語。

関連ＵＲＬ

[1]http://www.symantec.com/ja/jp/about/news/release/article.jsp?prid=20120919_01
[2]http://www.ipa.go.jp/security/vuln/newattack.html