傾向と対策

最新動向と事例で考察する対策の最前線

2012年は国家間の緊張が高まったこともあり、企業や政府機関のWebサイトの改ざんなどサイバー攻撃に関する報道が相次いだ。標的型攻撃といった新たな脅威が出現する一方で、クライアントの脆弱性を狙った攻撃など従来型の脅威にも変わらぬ注意が必要である。脅威が多様化、複雑化する中、どのような情報セキュリティ対策が有効なのだろうか。対策への第一歩は敵を知り、現状を把握することから始まる。本特集では情報セキュリティに対する脅威の最新動向と、事例に見る対策の最前線を紹介する。

情報セキュリティに対する脅威の変化

インターネットがグローバル社会に欠かせない基盤となる中で、情報セキュリティに関する脅威はますます大規模化、高度化し、政府機関や企業へのサイバー攻撃の脅威も現実化してきている。

次々と新たなタイプのサイバー攻撃が生まれてくる状況は、総務省の資料による「ウイルス種類の増加状況」からも窺い知ることができる（図1）。ウイルスは重要情報を入手するための入り口として用いられる場合もあり、国内の大手重工業に対するサイバー攻撃もウイルスを突破口にしていた。

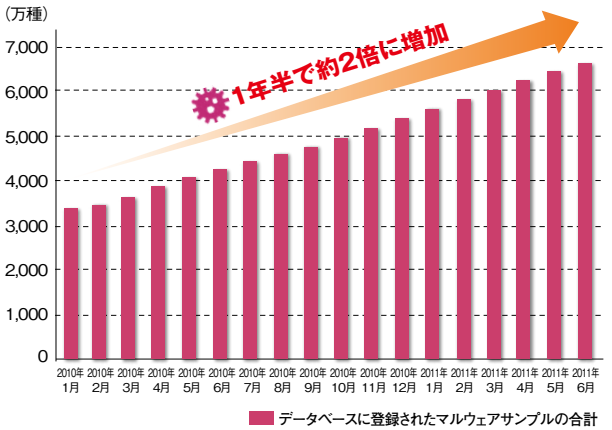


図1 ウイルス種類の増加状況

従来と現在のサイバー攻撃の違いについて、以下に2つのポイントを挙げる。

・攻撃目的の多様化

従来の攻撃は、攻撃者の自己顕示欲やいたずら目的が多かったが、近年では、経済的利益やハクティビズム（抗議活動）、サイバーテロ、機密情報の詐取など目的が多様化している。また、攻撃者も個人から集団、組織、国家機関までさまざまだ（図2）。一般社団法人JPCERTコーディネイションセンター（JPCERT/CC）に報告されたセキュリティインシデントにおいて、2012年7月から9月の報告件数5,430件は前年同期比で216%も増加。その背景には国家間の緊張の高まりなどが影響していると考えられる。

・攻撃手法の変化

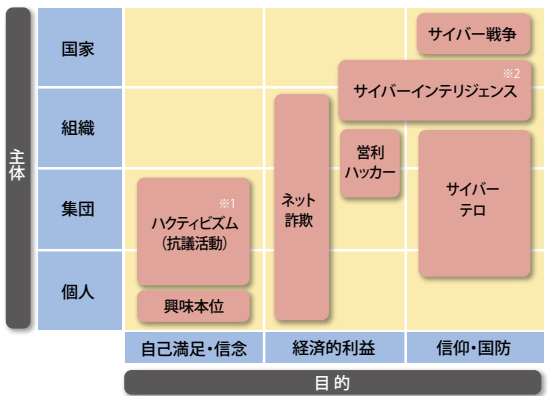
これまでは、1つの脆弱性に対して単発の攻撃が行われるケースがほとんどだったが、近年ではシステムに不正アクセスし、管理者権限を奪い、攻撃ツールを送り込むなど攻撃が段階的に行われるのが特徴だ。またシステム内部に潜入したウイルスが外部の攻撃者と通信を行いながら、既存のセキュリティ対策をすり抜ける戦略的な攻撃手法も出現。さらに、標的型メールに代表されるように、特定のユーザーを標的として心理的に相手をだますといった手法も巧妙化している。特定ユーザーを狙った攻撃は、攻撃対象となった企業が詳細を公

表しない限りウイルス対策ソリューションのベンダーなどとの間でウイルスのパターンや攻撃の手口などの情報が共有されにくい。そのため新種の攻撃に対しては、ウイルス対策ソフトウェアでも検知が難しいことが課題となっている。

また、スマートフォンの業務活用やクラウドの普及、制御系システムのオープン化など企業におけるシステム環境の変化は、攻撃者に新たなターゲットや攻撃手法を与える背景にもなっている。

このように情報セキュリティを取り巻く環境は大きく変化し新たな脅威が生まれているが、その一方でクライアントソフトの脆弱性を狙った攻撃や情報漏えいのように定番となった攻撃も見逃せない。近年では OS の脆弱性よりもクライアントソフトの脆弱性が攻撃に利用されるケースも増えてきた。長期間、課題として挙げられながら解決に至っていないという事実は対策の難しさも物語っている。

他組織で発生した事件・事故をそのまま自組織に当てはめて対策をとることは適切でない場合もある。だが、企業が晒されているリスクを実感し対策を実践することの大切さを伝えるために、企業において関心の高いサイバー攻撃と情報漏えいに関する事例と対策を紹介する。



※1 **ハクティビズム**:ハッカーとアクティビズム（積極行動主義）をあわせた造語で、社会的・攻撃的な主張のもとに、ハッキング活動を行うこと
※2 **サイバーインテリジェンス**:サイバー空間で行われる諜報活動（intelligence）のこと

図 2 攻撃目的の多様化

事例で考察する対策の最前線

ケース 1　標的型サイバー攻撃

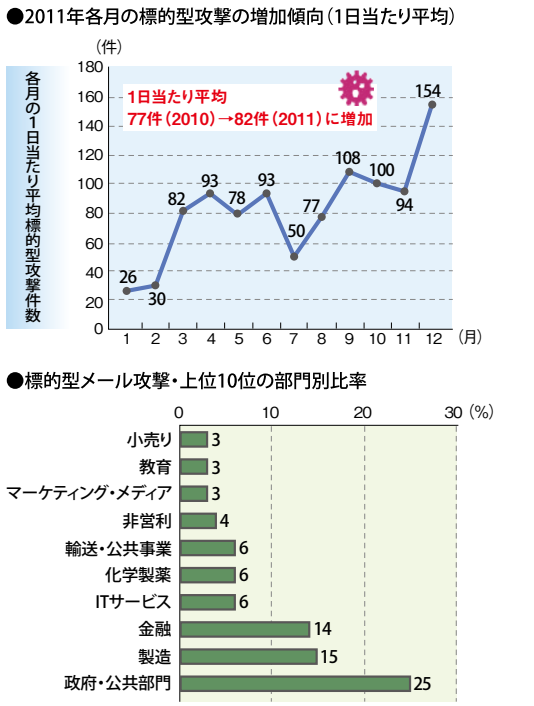
特定の企業にターゲットを絞って情報詐取

●特徴

攻撃者は、人事異動やミーティングの情報など標的企業の受信者が興味を惹き、なおかつ疑いの持ちにくい内容のメールを送信し、受信者が添付ファイルを開くとそのPCがマルウェアに感染する。攻撃者が事前に内部情報を収集するなど手口も巧妙である。またシステム内部に潜入したウイルスが外部のサーバと通信を行うことで、ネットワークやシステムの情報が攻撃者に筒抜けとなり、既存のセキュリティを回避しながら長期間にわたって攻撃が密かに続く。

●事例

衆議院をターゲットにした標的型メールにより、全議員の ID とパスワードが流出しメールが攻撃者に見られた可能性があるとする報告書が公表された。また国内大手重機メーカーでは、標的型メールによりクライアントソフトの脆弱性が悪用され、本社、工場、研究所などにあるサーバなどがウイルスに感染しシステム内部に潜入したとされている。総務省の資料によると標的型攻撃は増加傾向にあり、幅広い業種に及んでいることがわかる（図 3）。



出典:総務省「情報通信産業・サービスの動向・国際比較に関する調査研究」（平成24年）

図 3 標的型攻撃の増加状況

●対策

標的型サイバー攻撃に特効薬はなく、入口から出口、さらに万一発生した場合の早急な対応まで多層防御が必要である。

入口対策としては、多くの攻撃がクライアントソフトの既知の脆弱性を突破口とすることもあり、クライアントソフトのタイムリーなアップデートといった修正パッチのマネジメントがポイントとなる。

また、人的な対策では「不自然なメールを社員に送信しその対応の仕方を見る」といった標的型攻撃メールへの訓練が挙げられる。富士通の情報セキュリティ部門が所属従業員を対象に実施した訓練を例に説明しよう（図 4）。

メール A は通常、各従業員宛てに送られてきたことのない件名であり、メール B は部門長がよく出す件名となっている。メール A はほとんど添付ファイルを開封することがなかったのに対し、メール B は半数が開封する結果となった。ポイントはメールアドレスの @ マーク以下。「fjcert.jp」ではなく、「jp.fujitsu.com」が正しい。普段、氏名と件名で直観的に判断していると気づきにくい。

訓練では誰が開封したか、何割の人が開封したかは重要ではない。大切なのは訓練を通じ、社員が標的型攻撃を身近に認識できること。また情報セキュリティマネジメントの観点では標的型攻撃メールに対する自社のセキュリティ対策の状況把握が重要だ。

出口対策としては、外部との通信の遮断や内部での拡散を防止するネットワーク設計・設定といった技術的対策がポイントとなる。

メール A	メール B
・差出人： システム管理者 (admin@fjcert.jp) ・件　名： 【緊急】Windows Update による脆弱性の回避手順書	・差出人： 部門長名 (admin@fjcert.jp) ・件　名： [部門メーリングリストヘッダ：00311] 座席レイアウト変更について

＊部門長名には部門長の実名が入る

図 4 富士通の情報セキュリティ部門で実施された標的型攻撃メール訓練で使われた擬装メールの例

ケース 2　組織的サイバー攻撃

自らの主張を認めさせるための組織的な攻撃

●特徴

組織や企業の主張や行動に反発し、自らの主張を認めさせようとする一般の人たちが、インターネットを通じて組織化しサイバー攻撃を行う。組織的攻撃が活発化した背景には、ソーシャルメディアが一般的に利用されてきたことが挙げられる。

●事例

大手エンターテインメント会社のネットワークサービスとビデオ・オン・デマンドサービスがサーバの脆弱性を突いて不正侵入を受け、複数サイトが継続的にダウンしたうえ、多くの個人情報が漏えいした可能性があるという。

●対策

機密情報の取り扱いや公開 Web サーバなどの脆弱性の見直しを徹底的に行うとともに、日々のセキュリティ対策の取り組みを通じて情報セキュリティへの意識向上が必要となる。また、利用者の意見に真摯に耳を傾け、誤った行動をとっていた場合は誠実に謝罪するなど適切な対応をすることにより、問題の発生を未然に防止し影響を最小限に抑えることが可能になる。

ケース 3　内部関係者による情報漏えい

被害が拡大する組織内部や関係者の犯行による情報漏えい

●特徴

社員や元社員による情報漏えいは、誰もが重要な情報にアクセスできる権限を持っていたり、退職者や異動者といった関係者のアカウントが適切に管理されていないなど、情報を容易に詐取できる状態にあるケースが多い。2011 年には機密情報の詐取だけでなくデータの改ざんなどの事件も起きている。

●事例

国内通信会社では、業務委託先の元社員のデータ改ざんによる営業妨害でサービス利用者にも影響が出た。また国内クレジット会社では、関係者によって不正に持ち出された顧客情報が売却された可能性が高いことが判明した。

●対策

内部犯行の対策では、外部や他部門の人間が立ち入ることを防ぐ入室制限とシステムへのアクセス制限を組み合わせることが重要である。また機密情報を扱う場合、作業者と承認者を分け、承認されないと作業を実施できないなど職務権限分離もポイントとなる。

内部犯行とは異なるが、社員のミスによる情報漏えいの要因としてメール誤送信や紙情報の紛失も多い。メール誤送信は対策ツールの導入が有効である。紙情報の紛失は社員の意識を高める啓発活動を積極的に行うとともに、クラウドサービスを活用し外出先では紙情報を持たないといった工夫も必要だろう。

ケース 4　スマートフォンやタブレットを狙った攻撃

スマートデバイスの業務利用へのニーズの高まりに伴いリスクも拡大

●特徴

スマートデバイスは、高機能かつ携帯性に優れた通信端末であるため、PC と同様にメールだけではなく業務アプリケーションを使って外出先や自宅でも業務を行うことが可能だ。しかし、そうした利便性はリスクの拡大を伴う。さらにスマートデバイスは PC と比べ市販アプリケーションの利用が容易であり、個人所有端末を利用する BYOD（Bring Your Own Device）の場合はさらにリスクが高まる。端末紛失、盗難リスクに加え、マルウェアによる情報漏えいや標的型攻撃の対象となる可能性もある。

●事例

2011 年、2012 年と特に Android 向けのマルウェアの脅威が急速に高まっている。米国の調査会社 ABI Research によると、Android を狙ったマルウェアの数はこの 1 年で約 23 倍に増えたという（図 5）。

Android に対するマルウェア攻撃のほとんどは不正アプリケーションをユーザーがダウンロードしてしまうことをトリガーに起きている。2012 年 4 月には Android アプリケーションの公式マーケットで公開された不正アプリケーションを利用し、約 100 万人分もの個人情報を不正に入手した犯罪が大きな問題となった。またバッテリーの消費量を抑えられるなどの便利ツールに見せかけて不正アプリケーションをインストールさせる手口も増えている。まだ企業における被害は顕在化していないが、Android 端末を対象とする標的型攻撃用の不正アプリケーションを日本国内で発見したとする報告もされている。

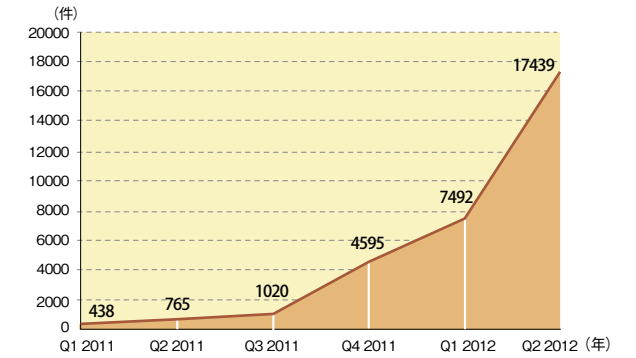


図5 Androidを中心にスマートフォン向けのマルウェアは急速に増加

●対策

今後 PC と同様に情報詐取などを目的に標的型攻撃の侵入口としてスマートデバイスを利用する手口も増えていくだろう。

スマートデバイスの業務活用における課題は、紛失・盗難時の情報漏えい対策、不正利用の防止、端末情報の収集と OS のアップデートの徹底、インストールできるアプリケーションの制限などがある。これらの課題に対し、ユーザーの意識向上とともに、企業側が統一したポリシーのもとに遠隔から複数端末を統合管理できる MDM（Mobile Device Management）やスマートデバイス向けのセキュリティソフトなど技術的対策をあわせて行うことが重要である。スマートデバイスを業務で使う場合は PC と同等のセキュリティを備えることが必要だろう。

ユーザー部門から経営陣までの連携が重要

標的型攻撃などの新しい脅威は、システムの設定不備、ソフトウェアの脆弱性、人の心理面までさまざまな角度から弱点を突いて攻撃を行ってくる。これからの情報セキュリティ対策では情報システム部門はもとより、ユーザー部門、企画部門、総務部門、経営陣まで含めた連携がポイントになる。

また、事業活動のリスクマネジメントという視点から情報の価値や意味を見直すとともに、アプリケーションへのパッチの適用や Active Directory 管理の徹底など基本対策を積み重ねていくことが必要だ。