リスクマネジメント最前線
2012-13

東京海上日動火災保険株式会社
企業営業開発部
〒100-8050
東京都千代田区丸の内 1-2-1
TEL　03-5288-6589
FAX　03-5288-6590
http://www.tokiomarine-nichido.co.jp/
東京海上日動リスクコンサルティング株式会社
http://www.tokiorisk.co.jp/

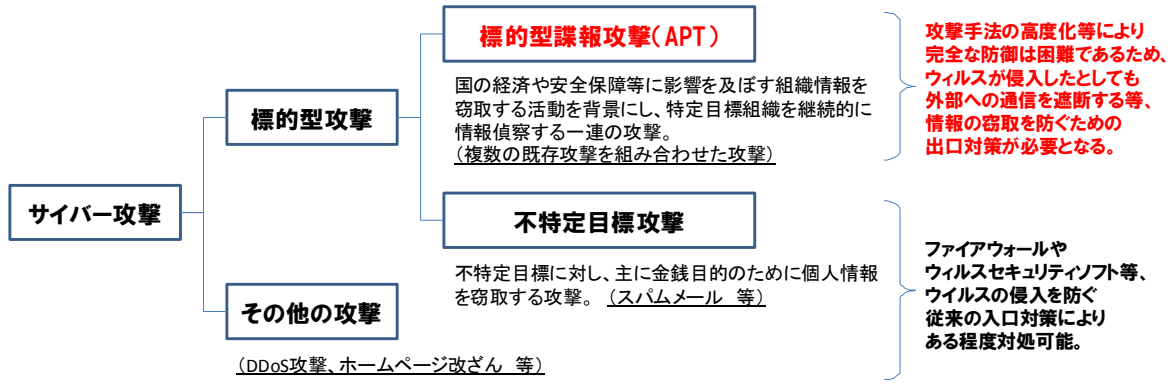
サイバー攻撃の脅威と企業における対策

昨年 4 月以降、日本の大手企業や政府関係機関に対して様々なサイバー攻撃が仕掛けられ、一部では大きな被害が発生している。近年のサイバー攻撃においては、特定の目的のもと、特定の組織に狙いを定めた攻撃が行われる動きが見られる。高度な技術を持ったハッカーに狙われた際は、その侵入を完全に防ぐのは難しい。本稿では、サイバー攻撃の脅威と、企業に求められる対策についてまとめる。

1．サイバー攻撃の分類と脅威

サイバー攻撃は、その攻撃対象が不特定多数か否か等によって、いくつかの種類に分けることができる。図 1 に、独立行政法人情報処理推進機構（IPA）によるサイバー攻撃の分類を示す。

図 1　サイバー攻撃の分類と対策概要



出典：IPA「『新しいタイプの攻撃』の対策に向けた設計・運用ガイド」を参考に弊社作成

図 1 の分類では、まず情報窃取を目的とする「標的型攻撃」か否かに分かれる。「標的型攻撃」に分類されないサイバー攻撃としては、DDoS 攻撃[1]やホームページ改ざんなど、情報窃取以外の方法で企業活動に影響を及ぼす攻撃が該当する。

「標的型攻撃」の中でも、特定の目標（企業・政府関係機関といった標的）を狙った攻撃か否かで分かれる。スパムメールなど不特定多数に対して行われる攻撃は「不特定目標攻撃」に該当する。一方、特定の目標に対し継続的に情報偵察等を行う一連の攻撃は「標的型諜報攻撃」に該当する。なお、「標的型諜報攻撃」は海外では「APT（Advanced Persistent Threat）」などと呼

[1] 特定のサイトに対して、大量のコンピュータから同時にアクセスを集中させることで、特定サイトの通常サービス提供を阻害する攻撃

ばれ、日本においては「新しいタイプの攻撃」と呼ばれることもある。この「標的型諜報攻撃」については近年、組織の機密情報流出等につながるような深刻な被害事例が世界中で発生しており、セキュリティ上の大きな課題となっている。

また、経済産業省が実施した調査[2] によると、標的型攻撃を受けた経験がある日本企業は、2007年に 5.4%であったのに対して 2011 年には 33.0%と急増している。

2. 近年のサイバー攻撃に見られる傾向

近年のサイバー攻撃においては、これまでのサイバー攻撃と異なる様々な傾向が見られる。ここでは、攻撃目的の特定化、攻撃主体の組織化、侵入防御の難度向上という観点から解説する。

（1） 攻撃目的の特定化

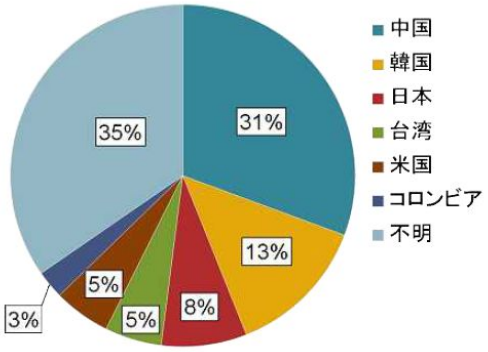
近年報道されたサイバー攻撃の事例を振り返ると、何らかの社会的な背景、意図等（例えば、企業の機密情報を盗み出す など）を持って特定の対象に攻撃が行われている点が特徴として挙げられる。

（2） 攻撃主体の組織化

近年のサイバー攻撃においては、攻撃する側（攻撃主体）の組織化が見られる。ハッカー集団の 1 つであるアノニマス（Anonymous）は、昨年から今年にかけて日本においても積極的に活動し、その犯行は度々報道されてきたところである。

また図 2 のグラフは、日本において標的型攻撃に使われたメールの IP アドレスを、国別に集計したものである。同集計では、中国で管理する IP アドレスからのメールが多いという結果になっている。同国では、複数のグループで形成された大規模なハッカー集団「中国紅客連盟」が活動しており、各国はサイバーテロへの警戒を強めている。

図 2　標的型攻撃メール発信 IP アドレスの国別内訳



引用 : IPA「標的型攻撃メールの分析に関するレポート」

[2] 経済産業省「最近の動向を踏まえた情報セキュリティ対策の提示と徹底」（平成 23 年 5 月）

（３）　侵入防御の難度向上

「標的型諜報攻撃」は、ソーシャルエンジニアリング[3]、ゼロデイアタック[4]等、複数の高度な既存攻撃を組み合わせて行われる等の理由から、攻撃によるウィルス侵入を完全に防ぐことは難しい。そのため、ウィルスの侵入を防ぐ入口対策に加え、ウィルスが侵入したとしても外部への通信を遮断する等、情報が出て行くことを防止する出口対策の必要性が新たに生じてきたことがポイントとして挙げられる。

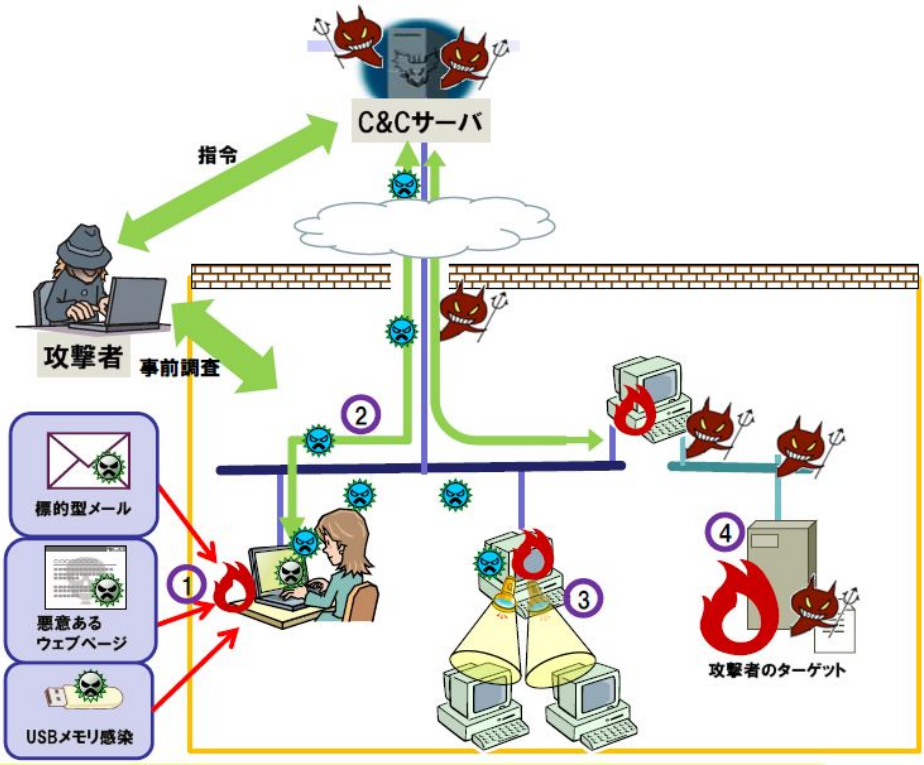
３.「標的型諜報攻撃」の手口

「標的型諜報攻撃」の流れと、その攻撃による侵入を防ぐことが難しい背景について、概要をまとめる。

（１）　「標的型諜報攻撃」の流れ

「標的型諜報攻撃」の流れを以下に示す（図 3)。

図３　「標的型諜報攻撃」の流れ



引用：IPA「『新しいタイプの攻撃』の対策に向けた設計・運用ガイド 簡易説明資料」

[3] 話術や盗み聞き・盗み見等の手法により、人間の心理・行動の隙を突くことで情報を不正に取得する手段の総称

[4] あるソフトウェアの脆弱性が判明した後、ソフトウェアの修正プログラムがベンダーから提供される前に、その脆弱性を悪用して行われる攻撃

＜事前調査段階＞

標的の組織に関係のある組織へ攻撃を行い、初期潜入の基となる組織間でやり取りをしたメールなどの情報を収集。

① 初期潜入段階

標的型メール、USB メモリ、ウェブサイト閲覧などの経路からウィルスに感染させる。

② 攻撃基盤構築段階

侵入した PC 内でバックドア通信経路を確保し、外部の C&C[5]サーバと通信を行って、新たなウィルス等をダウンロードする。

③ システム調査段階

情報の特定・取得を行い、収集した情報を基にさらなる攻撃を仕掛ける。

④ 攻撃最終目的の遂行段階

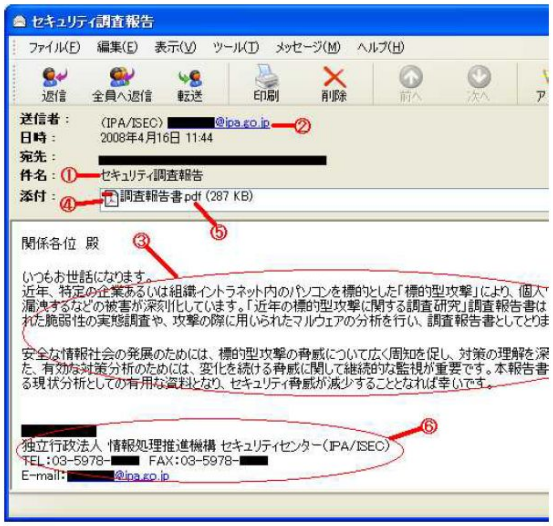
攻撃専用のウィルスをダウンロードして、目的の攻撃を遂行する。

（２） 標的型攻撃メールによる被害を防ぐ難しさ

「標的型諜報攻撃」の起点となる標的型攻撃メールについて、近年、注目が集まっている。一般的な手口としては、ID とパスワードを窃取するウィルスを添付したメールを送りつけ、その添付ファイルを開かせることで、利用者のパソコンにウィルスを感染させるという基本的なものである。しかしながら近年、メール送付の方法が巧妙化しており、何気なく開いた結果感染し、かつ、感染したことに気づかないといったケースが増加している。

標的型攻撃メールの一例として、以下に IPA が公開している資料から引用した例を示す（図 4）。

図 4　標的型攻撃メールの一例



① メールの受信者が興味を持つと思われる件名

② 送信者のメールアドレスが信頼できそうな組織のアドレス

③ 件名に関わる本文

④ 本文の内容に合った添付ファイル名

⑤ 添付ファイルがワープロ文書や PDF ファイルなど

⑥ ②に対応した組織名や個人名などを含む署名

引用：IPA「標的型攻撃メールの分析に関するレポート」

[5] Command and Control：攻撃者が用意している外部の指令サーバ

また、IPA による日本で発見された標的型攻撃メールの分析結果においては、官公庁・独立行政法人等、政府関係機関を騙(かた)るメールが約 2/3 を占めている（図 5)。また、送信されるメールのテーマについては、重要さをにじませる様々なテーマで作成されている（表 1)。

このように、攻撃対象の企業に合わせて、受信者が業務関連の連絡と錯覚するような標的型攻撃メールが作成され、送信されているのが現状である。なお、内閣官房情報セキュリティセンター（NISC）が内閣官房のほか 12 の政府機関を対象に 2011 年 10 月～12 月に実施した、仮の標的型攻撃メールを送付し開封されないかどうかを確認する訓練では、10.1%の職員が誤って開封しており、標的型攻撃メールの被害を防ぐ難しさがうかがえる。

図 5　標的型攻撃メール送信者の騙(かた)る主体の属性

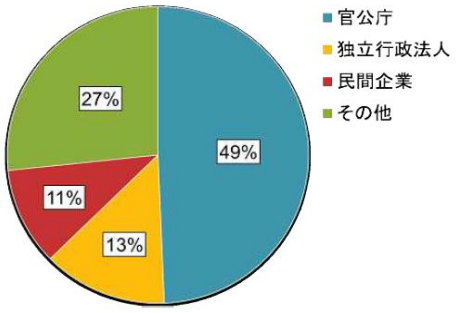


表 1　テーマによる分類

分類	割合	テーマ事例(抽象化済)
イベント	38%	国際会議、シンポジウム、研修会、選挙、法令改正、VIP会合日程、役員人事異動、来訪者情報、社内ウイルス調査
報告書	32%	外交機密文書、国際情勢、海外資源、政府部局報告書、情報セキュリティ調査、ウイルス・不正アクセス届出状況、会議資料
ニュース・注意喚起	30%	東日本震災、金融情勢、国際情勢、外交情報、政府予算、製品事故、情報セキュリティ注意喚起、新型インフルエンザ

引用：IPA「標的型攻撃メールの分析に関するレポート」

4．企業に求められる対策のポイント

上述の近年におけるサイバー攻撃の傾向や、対策に関する世の中の動向等を踏まえ、サイバー攻撃について企業に求められる対策のポイントを、以下にまとめた。

（1）　外部からの脅威をブロックする「入口対策」の見直し

従来から実施されてきた「外部から組織に入り込まれないような対策」の徹底を行う。ファイアウォールやウィルス対策ソフトの設定に関する対策はもちろんのこと、メールのフィルタリング（IP アドレス偽装、添付ファイル解析、スパムメール隔離等)、ウェブフィルタリング、USB やモバイルデバイスを含むエンドポイント管理等、攻撃者の潜入経路となるポイントについて、必要に応じてさらなる対策強化を図る。

（2）　情報が外部に持出されない為の「出口対策」追加検討

「標的型諜報攻撃」等のサイバー攻撃に対しては「外部にいる攻撃者に情報を窃取されないための対策」という観点から、バックドア通信、ウィルスのシステム内拡散、情報の流出を止める対策が重要となる。具体的には、ログ監視、不正通信検知・遮断、重要性の極めて高い情報をネットワークから分離、アカウント管理等の重要サーバに対する防護の強化等を、組織が

保有している情報の内容等に応じて追加・強化していく対策が考えられる。

（３） パッチ適用等の脆弱性対策を徹底

ゼロデイアタックに代表されるように、パッチ適用等の脆弱性対策の遅れは攻撃者に狙われやすい点である。企業によっては膨大な量のサーバやソフトウェアを保有・管理しており、更新に多大な労力を要する場合もあるが、脆弱性に対処しきれていなかった弱点をつかれた攻撃による大規模な情報漏えいも起きていることから、脆弱性対策のスピードを速めていくことが必要であるといえる。

（４） サーバ集約

サイバー攻撃に対する防御力向上や、震災時における事業継続を図るため、プライベートクラウド等を活用したサーバ集約を図る例も増えている。ある製造業のメーカーにおいては昨年、全国で 4500 台のサーバを 3 か所のデータセンタに集約している。

サーバ集約によって一括で管理することにより、セキュリティ対策レベルの均一化を図ることができるため、企業にとっては防御を行いやすくなるメリットがある。しかしながら、集約することにより、ある拠点がサイバー攻撃によりダウンする等の事態が起きた際の影響は大きくなるため、高度なセキュリティ専門家の配置等、徹底した対策が必要となる。

（５） 積極的な情報収集の実施

IT の安全性・信頼性の向上等に取り組む IPA では、サイバー攻撃に関する各種調査・研究等を行っており、ホームページより様々なレポートや注意喚起の情報を得ることができる。ここでは昨年 4 月～9 月にかけて発生した各サイバー攻撃の事件の後に出された、本テーマに関連するレポートを 2 点、以下に示す。

- **『新しいタイプの攻撃』の対策に向けた設計・運用ガイド（2011 年 11 月 30 日）**[6]
- **『標的型攻撃メールの分析』に関するレポート（2011 年 10 月 3 日）**[7]

（６） 重要情報の区分・管理方法の再検討

一度「標的型諜報攻撃」の対象となると、ウィルスの侵入を完全に防御するのは難しい。そのため情報の重要度に応じ、パスワードの付加を行う、さらにセキュリティの高いファイル管理システムで管理を行う等、万が一のウィルス侵入に備えた防衛策を徹底しておく必要がある。

また、「絶対に」外に漏らしてはいけない機密情報については、外部のネットワークにつながっていない環境に保存する、もしくは、電子化を行わない（紙等で管理する）といった対策を検討することも一案である。

---

[6] http://www.ipa.go.jp/security/vuln/newattack.html
[7] http://www.ipa.go.jp/about/technicalwatch/20111003.html

（７）　教育実施による意識啓発

標的型攻撃メールに代表されるように、攻撃者は、従業員の意識低下や不注意等をついてウィルス侵入を画策する。そのため、ハードウェア対策やルール整備に加え、教育の実施による意識啓発も、サイバー攻撃による被害抑制のためには不可欠となる。

不審なメールへの警戒、USB を含めた外部媒体の利用制限等の理解浸透へ向け、集合教育、e ラーニング、確認テスト、掲示板やメールによる注意喚起等を継続して行うことが重要となる。また、標的型攻撃メールに関しては、NISC の事例に代表されるように、実際に仮の標的型攻撃メールを従業員等に送付し、適切な対応をとれるかどうか検証する実動訓練を行うことも効果的であると言える。

（８）　有事対応体制の強化

上記対策を講じてきたとしても、完璧な防御を図ることは困難であり、何らか不測の事態が発生してしまう可能性をゼロにはできない。また、DDoS 攻撃のような意図的なアクセス集中に対してコントロールを行うことも不可能である。そのため、万が一の際の情報集約、対応体制の構築、Web サイト閉鎖等の適切な初動対応を可能とするため、マニュアル整備及び訓練等の有事対応体制の強化を図ることも、重要な対策となる。

５．最後に

情報技術の発達により、電子化された情報は膨大な量に増え続けており、情報漏えいに関するリスクは高まり続けている。さらに今般のサイバー攻撃においては、一度標的にされると、防御がかなり難しいという現実がある。そのため企業においては、ステークホルダーに対して説明責任を果たせる範囲までの対策を講じておくことに加え、万一の際に適切な対応が行えるよう有事対応体制を構築しておくことが、より一層求められてくるものと考えられる。

（2012 年 8 月 13 日発行）