KPMG
cutting through complexity

2014年8月

新たなITリスクに立ち向かう 連載シリーズ 第7回

サイバー攻撃のトレンド

ウェブサイトの改ざんやID・パスワードの窃盗、インターネットバンキングを利用した不正送金等、インターネットを通じたさまざまな攻撃が新聞紙上をにぎわせることが多くなっている。

サイバー攻撃の定義について、警視庁のウェブサイト[1]では「サイバーテロとは、重要インフラの基幹システムに対する電子的攻撃又は重要インフラの基幹システムにおける重大な障害で電子的攻撃による可能性が高いものとされており、一般的にはコンピュータ・システムに侵入し、データを破壊、改ざんするなどの手段により、国家又は社会の重要な基盤を機能不全に陥れる行為」と定義されており、本稿もこちらに統一する。サイバー攻撃の定義にある重要インフラとは、「情報通信」「金融」「航空」「鉄道」「電力」「ガス」等を指しており、いずれも我々の日常生活に欠かせないものである。これらの生活インフラは、インターネットというオープンなネットワークを利用することにより国民にとって多大な利便性を享受することができる一方、そのオープン性の故に悪意ある第三者から攻撃を受けるリスクが急速に増大しているのが現状である。

本稿では、近年多く発生している代表的なサイバー攻撃を「機密情報漏えい」「フィッシング・ウイルス感染による不正送金」「ウェブサイト改ざん」「サービス停止」の4つに分類し、その概要と国内外の代表的な発生事例を紹介する。

1. 機密情報漏えい

(1)概要

特定組織／企業を標的とした攻撃により機密情報や顧客情報を搾取し、その販売またはクレジットカード情報を用いた不正利用を行う攻撃を指す。個人情報やクレジットカード情報を取り扱うウェブサイトが標的となりやすい。

[1] 警視庁 サイバーテロ対策協議会
http://www.keishicho.metro.tokyo.jp/haiteku/cyber/cyber.htm

(2)発生事例

国内で発生した代表例について、攻撃を受けた組織、攻撃の概要、原因、対策をまとめると、
以下の通りである。

【図表1】機密情報漏えい代表事例

攻撃を受けた組織 (タイプ)	攻撃の概要	原因	対策
政府関連[2] (標的型攻撃)	職員のパソコンがコンピュータウイルスに感染。職員は開発中の次世代固定燃料ロケット「イプシロンロケット」の関連業務に就いており、最先端技術漏えいの懸念があったが、当組織の事業の円滑な遂行に支障がないと結論づけた。調査の結果、ウイルスに感染したパソコン(端末)は1台で、それ以外への感染はないことを確認。	東日本大震災発生直後の2011年3月17日に、震災関連をかたった「なりすましメール」が原因。その後、同日から2012年11月21日に発覚するまでの約20ヵ月間にわたって、外部の不正サイトへの通信が継続。通信量と通信内容は不明だが、「当該端末内の情報が外部に漏えいした可能性は否定できない」としている。	非公表
検索大手[3] (不正アクセス)	最大2200万のIDのうち、約148万6000件については、IDに加えて暗号化されたパスワード等の情報も漏れていた可能性が高いと発表。漏えいした可能性があるものは、不可逆暗号化したパスワードと、パスワードを忘れた場合の再設定に必要な情報の一部。	外部攻撃の可能性が高い。	強制的にパスワードと秘密の質問のリセットを実施。リセットされたのは、パスワード等の情報が流出した可能性のある約148万6000件。各ユーザーに、自分のIDが漏えい対象になっているか否かを判定するためのツールを提供。
通信会社[4] (不正アクセス)	ウェブサイトから、10万9112件のクレジットカード情報が漏えい。	社外からの不正アクセス(SQLインジェクション攻撃)。	非公表

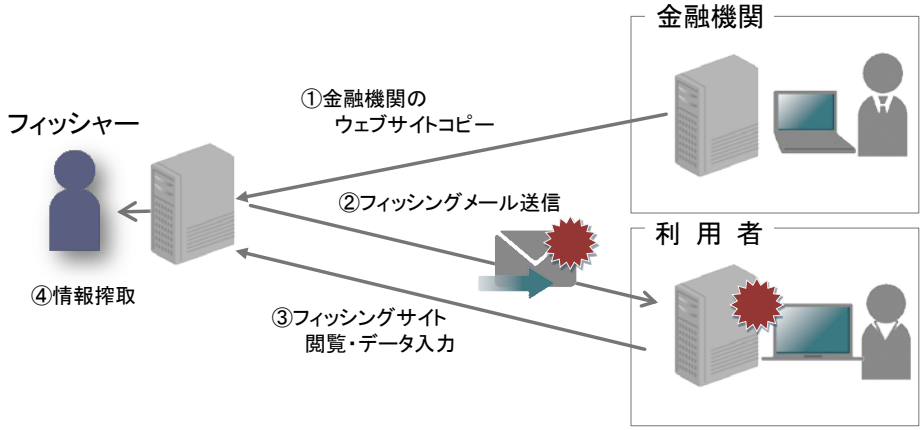
2. フィッシング・ウイルス感染による不正送金

(1)概要

フィッシング攻撃は
① フィッシャーが金融機関のウェブサイトコピー
② フィッシングメール送信
③ 利用者がフィッシングサイト閲覧・データ入力
④ フィッシャーが情報搾取
の手順で行われる。

[2] http://www.jaxa.jp/press/2012/11/20121130_security_j.html
http://www.jaxa.jp/press/2013/02/20130219_security_j.html
[3] http://pr.yahoo.co.jp/release/2013/0517a.html
http://pr.yahoo.co.jp/release/2013/0523a.html
[4] http://www.xcomglobal.co.jp/info/

【図表2】フィッシング攻撃概要図



フィッシング攻撃でインターネットバンキングのログインおよび送金に必要な情報を搾取し、不正送金を実行するのが最も原始的な手口である。
近年では、利用者のパソコンをウイルスに感染させ、ログイン情報や送金に必要な情報を搾取する手法が多くなっており、攻撃手口が高度化している傾向にある。

(2)発生事例

警視庁の広報資料によると、平成23年の被害総額は約3億800万円にのぼり、平成24年は約4800万円まで減少したものの、平成25年は14億600万円と過去最大の被害が発生している[5]。
また、平成26年には法人向けインターネットバンキングでも被害発生が確認されており、不正送金の被害は全体的に増加傾向にある。

3. ウェブサイト改ざん

(1)概要

ウェブサイト改ざんとは文字通り、ウェブサイトを本来の表示内容と異なるものに第三者が書き換えることをいう。情報漏えいリスクと異なり、顧客に迷惑をかけないのであれば相対的にリスクは高くないという意見もあるものの、昨今の改ざん事例では単なるサイト改ざんのみならず、閲覧者にウイルスを拡散するタイプの攻撃もあり、影響確認や復旧作業を含め数日～数週間のサイト閉鎖を余儀なくされるケースも発生しているため、リスクが低いという認識は必ずしも正しくない。

2010年のガンブラーの流行や、毎年9月18日に近隣国より日本への攻撃が繰り返されていることに加え[6]、最近では企業のウェブサイト改ざん事例が新聞で報道される等、サイト改ざん攻撃は流行の兆しを見せつつある。

(2)発生事例

業界・業種を問わず、ウェブサイトが改ざんされたり、サイトにウイルスが埋め込まれた結果、閲覧者のPCがウイルス感染した事例が多数報告されている。

---

[5] 警視庁　広報資料「平成25年中のインターネットバンキングに係る不正送金事犯の発生状況等について」（平成26年1月30日） https://www.npa.go.jp/cyber/pdf/H260131_banking.pdf
[6] 警視庁 「中国を発信元とする再帰問い合わせ可能なDNSサーバの探索行為の増加について」（平成25年9月11日） http://www.npa.go.jp/cyberpolice/detect/pdf/20130911.pdf

4. サービス停止

(1)概要

サービス停止とは、Eコマース系サイトや検索サイト、インターネットバンキング等、正常に稼働し続けることがビジネス上重要なシステムに対し、何らかの攻撃を加えサービスの提供を不能にすることをいう。

「Distributed Denial of Service(DDoS)」が代表的な攻撃手法で、複数のネットワークに分散する大量のコンピュータが一斉に特定のサーバへパケットを送出して通信路をあふれさせ、機器のメモリ等システム資源を大量消費させる等してシステム機能を停止させてしまう。

DDoS攻撃によるアクセスは通常のアクセスと見分けがつきにくく、選択的に排除するのが難しい。このため、標的のサーバにセキュリティ上の弱点を放置する等の管理のミスがなくても被害が発生してしまうという特徴がある。

(2)発生事例

国内の有名なDDoS攻撃の事例として、中国国内での呼びかけにより、柳条湖事件が発生した日に合わせて、9月17日～18日にかけて断続的に人事院ウェブサイトや内閣府のストリーミング配信等のサイトへアクセスしづらくなる被害が発生している[7]。

また、海外の事例であるが、韓国の農協でサイバー攻撃によりATMが多数停止したほか、複数の銀行で支店での取引やインターネットバンキングが停止し、また業務用PCが動作不能になる被害が発生している[8]。

5. まとめ

サイバーセキュリティの攻撃技術は日進月歩で変化しており、どこまで対策を実施すれば安心なのかという水準が見えにくい。そのため日々世の中で発生している事象や最新のトレンドに着目し、情報収集の努力を怠らないことがリスクを低減するために非常に重要なポイントである。インターネットに接続するメリットを享受する企業はこの点に常に留意し、サイバー攻撃に立ち向かっていただきたい。

KPMGコンサルティング株式会社
ディレクター　原田　克樹

---

[7] 日本経済新聞(2011年9月19日)
http://www.nikkei.com/article/DGXNASFK1901A_Z10C11A9000000/
[8] 日本経済新聞(2013年3月20日)
http://www.nikkei.com/article/DGXNASGM2001P_Q3A320C1000000/

KPMGコンサルティング株式会社

東京本社
〒100-0004
東京都千代田区大手町1丁目9番5号
大手町フィナンシャルシティ ノースタワー
TEL ： 03-3548-5305
FAX ： 03-3548-5306

名古屋事務所
〒451-6031
名古屋市西区牛島町6番1号 名古屋ルーセントタワー
TEL ： 052-571-5485

kpmg.com/jp/kc