2014 年版　情報セキュリティ

10 大脅威

～複雑化する情報セキュリティ　あなたが直面しているのは？～

IPA 独立行政法人情報処理推進機構
セキュリティセンター

2014 年 3 月

目次

はじめに

本書は、情報セキュリティ専門家を中心とした 117 名で構成される「10 大脅威執筆者会」の投票により、その年に発生したセキュリティ事故や攻撃状況、IT 環境の変化等から、各セキュリティ脅威ついて順位づけし、解説したものである。脅威の順位については、毎年変動しているが、これには様々な要素が絡んできており、年々複雑な構造になってきている。

- 脅威の変遷

右の表は、2001 年から 2013 年までのタイムスパンで、攻撃傾向、IT 環境、政策等の変遷を表したものである。2001 年当時と比べると、脅威に関係する要素が増え、防御側が警戒すべき脅威が複雑化しているのが分かる。また、脅威の変化を追うようにして、新たな法整備や政策立案されており、安全保障や犯罪捜査等が新たな問題領域として認識されだしている。この様に、今日の“情報セキュリティ”は、従来のウイルスや不正アクセス問題、組織のセキュリティマネジメントの枠を超え、これまでとは異なる領域・分野においても異なる切り口で問題が定義されだしている。

- 2013 年の動き

2013 年は全体的に複数の領域で問題が顕在化した一年だったと言える。一つには、標的型攻撃に代表されるサイバー攻撃・犯罪が増大化していることが挙げられる。また、メガリークと呼ばれる大量の個人情報の漏えい、増え続けるウェブサイト改ざん、DDoS 攻撃におけるトラフィック量の増大等、サイバー攻撃に伴う脅威は相対的に増大している。

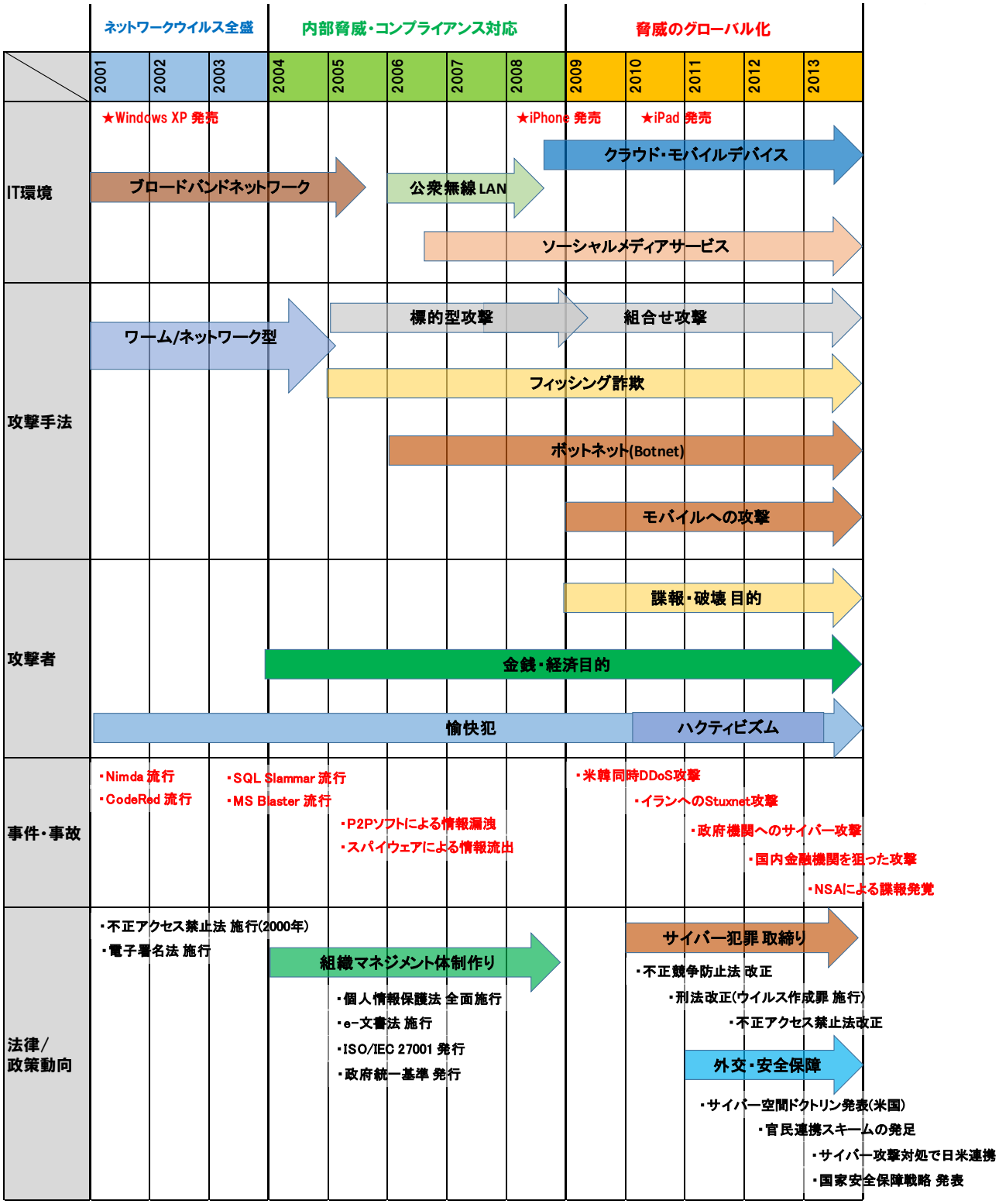
また、FaceBook や Twitter 等のソーシャルメディアへの不適切な投稿により、ネット上で炎上し、個人はもとより、組織の管理体制にまで影響が波及する等、個人ユーザーにおけるインターネットモラルも重要な課題として注視しなければならない。特に、未成年者が補導・逮捕されるケースも増えており、犯罪の低年齢化が社会的にも大きな問題になりつつある。

- 今後の懸念事項

IT 環境面の変化に目を向けると、インターネットに接続するオフィス機器や情報家電が増えている。それに伴い、不適切な設定による情報漏えいや不正アクセスが引き起こされている。守るべきものがパソコンやサーバーだけでなく、オフィス機器や情報家電まで広がりつつあり、セキュリティ対策の根本を見直す時期にきている。

このように IT 環境は、様々な形で変化しており、新たな問題を生み出している。重要なのは、脅威を自組織や自身に当てはめて、問題点や課題を認識し、適切な対応を講じることである。是非、本書に記載している脅威について、ご自身の目で、自組織や自身への脅威を見極めながら、読み進めていただきたい。

表１：脅威の変遷


ネットワークウイルス全盛
内部脅威・コンプライアンス対応
脅威のグローバル化
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
IT環境
★Windows XP 発売
★iPhone 発売
★iPad 発売
クラウド・モバイルデバイス
ブロードバンドネットワーク
公衆無線 LAN
ソーシャルメディアサービス
攻撃手法
ワーム/ネットワーク型
標的型攻撃
組合せ攻撃
フィッシング詐欺
ボットネット(Botnet)
モバイルへの攻撃
攻撃者
諜報・破壊 目的
金銭・経済目的
愉快犯
ハクティビズム
事件・事故
・Nimda 流行
・CodeRed 流行
・SQL Slammar 流行
・MS Blaster 流行
・P2Pソフトによる情報漏洩
・スパイウェアによる情報流出
・米韓同時DDoS攻撃
・イランへのStuxnet攻撃
・政府機関へのサイバー攻撃
・国内金融機関を狙った攻撃
・NSAによる諜報発覚
法律/
政策動向
・不正アクセス禁止法 施行(2000年)
・電子署名法 施行
組織マネジメント体制作り
・個人情報保護法 全面施行
・e-文書法 施行
・ISO/IEC 27001 発行
・政府統一基準 発行
サイバー犯罪 取締り
・不正競争防止法 改正
・刑法改正(ウイルス作成罪 施行)
・不正アクセス禁止法改正
外交・安全保障
・サイバー空間ドクトリン発表(米国)
・官民連携スキームの発足
・サイバー攻撃対処で日米連携
・国家安全保障戦略 発表

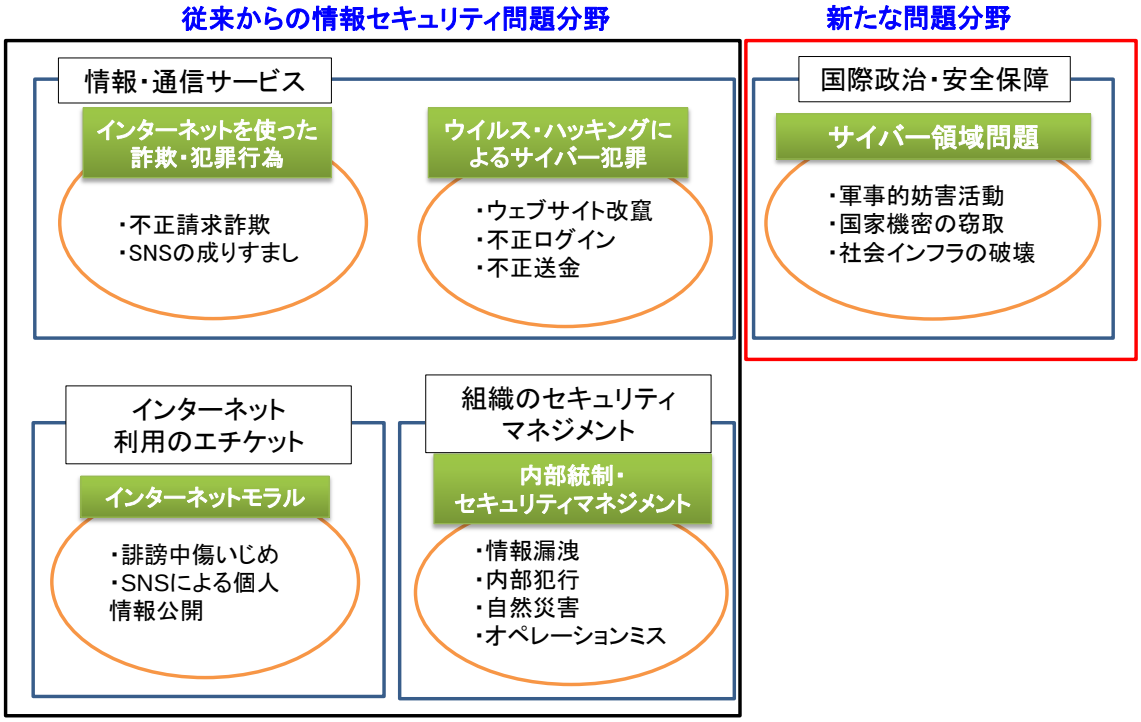
1章. セキュリティ脅威の分類と傾向

近年、「サイバー攻撃」「サイバー空間」「サイバー領域」等の言葉が飛び交うようになり、従来からの情報セキュリティとの関係に戸惑う読者の方も多いと思われる。事実、インターネットサービスの普及、SNS やスマートフォンに代表される人々のライフスタイルの変化、サイバー攻撃を主題とした国際問題等、情報セキュリティを取巻く問題と環境が多様化している。

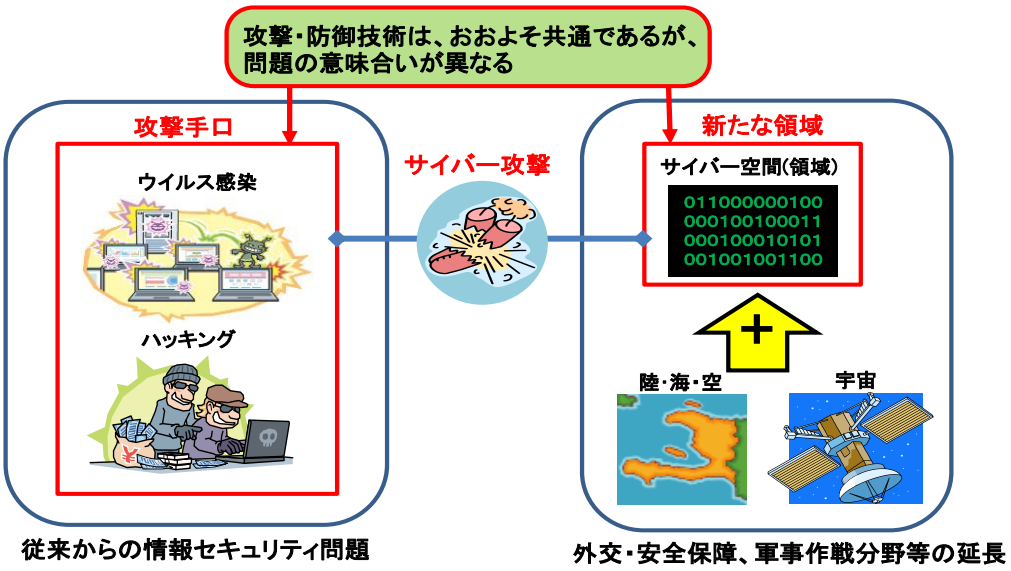
国際政治、外交・安全保障や軍事分野にまで多様化した問題と従来の情報セキュリティとの関係や全体像は、攻撃事象・事故のみに注目してしまうと一般的に解りにくく「複雑」に見えてしまうため、問題を整理することが困難になってきている。また、一言で「サイバー攻撃」と言っても、個人や企業・組織によって問題の意味合いも異なってきている。

どの脅威がどのような形で自組織や自身に影響するかを考えて対応を検討する事が大切である。脅威は、全ての組織やユーザーに一様に降りかかるものではなく、攻撃者の意図や自組織の環境、そして問題分野により受ける影響が異なるものである。この点を意識して、各脅威が自組織や自身にどのように影響するのか考えながら読み進めていただきたい。

本書では、各問題分野について、脅威が生じる背景、攻撃者の意図・特徴、対応側組織の特性等を基に、下図に示す 5 つに分類した。次項以降で、個々の問題分野について特徴と傾向について解説する。



1.1.サイバー領域問題



サイバー領域（5 番目のドメイン）という概念は、2011 年に米国政府により定義され、サイバー空間も他の領域（陸・海・空・宇宙空間）と同じく「国際政治、国際公共財」等で扱うとしている。サイバー空間は、「外交・安全保障、軍事作戦」等を目的とした領域として認識されるようになったため、サイバー攻撃が国際政治の問題として扱われるようになったと言える。即ち、従来の情報セキュリティとは別の問題として捉える必要がある。

- 国際公共財（グローバル・コモンズ）

サイバー空間が、他の領域と同様に国際公共財（グローバル・コモンズ）[1]として捉えられていることが国際的な背景にある。今日のサイバー空間は、社会、経済、軍事等のあらゆる活動が共存する場となっている。その為、サイバー空間における自由な活動やアクセスを妨げない為の規範作りが行われようとしている。

- 国際政治における動き

サイバー攻撃を国際政治の主題とする動きが既に始まっている。2013 年 6 月に行われた米中首脳会談において、サイバー攻撃が主要議題に取り上げられた。国際政治を舞台では、領土、領海と同じく、サイバー空間が安全に利用されることを模索する動きが行われている。

- 安全保障問題

2013 年 12 月に発表された我が国の「国家安全保障戦略」において、サイバー空間への防護が国家戦略に盛り込まれた。ここで想定されている事象は、「国家の秘密情報の窃取」、「基幹的な社会インフラシステムの破壊」、「軍事システムの妨害を意図したサイバー攻撃」である。サイバー攻撃によって、機密情報や知的財産情報が他国へ流出するといった国益を損なう事態や、社会の混乱に繋がる危険を想定している。このように、社会、経済、軍事等の活動を脅かす事象として、サイバー攻撃が安全保障の枠組みの中で捉えられるようになった。

今後、国内外の様々な方面で環境整備が進められることが予想される。

[1]国際社会における共通の財産に位置づけられ、アクセスの阻害や、特定の国や地域が独占してはならないもの

1.2.ウイルス・ハッキングを用いたサイバー犯罪

ウイルスを使ったパソコン上の情報窃取や認証を回避してサーバーに不正アクセスを行うハッキング行為は、サイバー攻撃の代表的な手法である。これらの攻撃が行われる背景には、金銭・経済的な狙いがあると言われており、年々被害規模も増大している。

2013 年の統計[2]では、全世界で年間 3 億 7,800 万人が被害に遭っており、国内においても、年間 400 万人がサイバー攻撃の被害に遭っていると言われており、10 秒に 1 人の割合で被害者を生み出している。攻撃者は、インターネット上でグローバルに活動しており、企業・組織から一般個人まで攻撃のターゲットとなっている。

攻撃者は、高度なコンピューター技術を駆使した手法やインターネット上に公開されているツールを使い、金銭・経済的な価値を有する情報を窃取している。

- スマートフォン・タブレットにも拡大

近年は、攻撃対象となる機器も、パソコンやサーバーに限らず、スマートフォンやタブレット端末等に拡大しており、セキュリティ対策を行う対象範囲が広がっている。

- 金融サービスの普及

金銭に絡むサイバー犯罪が増加する要因として、金融関連のサービスがインターネット上で普及してきたことが挙げられる。2013 年は、オンラインバンキングにおける不正送金事件が話題となった。認証情報が窃取され、本人に成りすまされて不正送金されてしまい、金銭が盗み取られてしまう犯罪が増えている。

ウイルス・ハッキングを駆使したサイバー犯罪では、攻撃者によってソフトウェアの脆弱性やシステムの設定不備が狙われる。パソコンやサーバーだけでなくインターネットに接続するすべての機器でセキュリティ対策を行い、セキュアにシステムを運用していくことが重要である。

[2]http://www.symantec.com/content/ja/jp/about/presskits/2013_Norton_Report.pdf

1.3.インターネットを使った詐欺・犯罪行為

他人を騙して、金銭的な損害を与える詐欺行為は、古来より行われてきた犯罪手口であり、今日でも振り込め詐欺、悪徳商法等が横行する。この様な詐欺師による詐欺行為が、インターネット上でも繰り広げられている。

- 不正（架空）請求詐欺

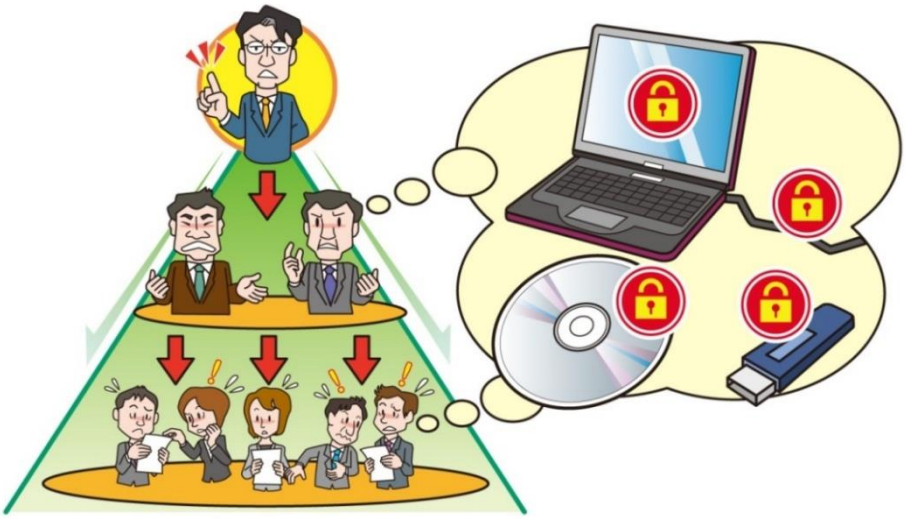
10 年ほど前より、郵送によって「サービス料が未払いです。至急連絡を下さい」「裁判所に訴状を提出した」といった内容のサービス利用料を請求する詐欺が横行している。これらの流れを汲む形で、アダルト・出会い系サイト上や、電子メールに記載されている URL を 1 回クリックすると、「ご入会ありがとうございました。」等の画面が表示され、一方的に契約したと偽って多額の料金支払いを求める「ワンクリック契約（請求）」と呼ばれる詐欺手口が存在する。実際には、契約は成立しておらず、ユーザーの無知や弱みに付け込んで、不正に請求する手口である。

- SNS による成りすまし

詐欺師による金銭目的の犯行だけでなく、近年では SNS を使った愉快犯的な行為も散見される。代表的なのが、Twitter 等のソーシャルメディアを使った、有名人や実在企業の成りすまし行為である。特に 2013 年は、インターネット選挙活動解禁の年であり、候補者がブログや SNS に投稿する等して、選挙活動を行った。一方で、候補者に成りすました偽アカウントも複数確認され、本人に成りすまして発言されるケースが散見された。また、同様に有名人に成りすました事例も確認されており、偽情報の流布に繋がる危険性が指摘されている。

インターネット詐欺は、現実世界同様に騙されないことが重要である。発信される情報に対して、ユーザー側が十分に用心して利用することが必要である。

1.4.内部統制・セキュリティマネジメント



2000 年代前半に発生した企業不祥事をきっかけに日本国内でも内部統制・コンプライアンスの考えが注目され始めた。情報システムにおいても同様に、2000 年代半ばから、企業・組織内における情報セキュリティマネジメント体制の確立が浸透している。内部統制・セキュリティマネジメントの基本は、セキュリティコントロールを確立し、組織が保有している情報資産（データやシステム）を故意または偶発的な事故によって、漏えい、改ざん、消失、システム停止させないことである。

- ルールとシステム対策

内部統制・セキュリティマネジメント体制が確立され、内部のルール化、それに伴う教育、システムによる対策が行われる。例えば、2000 年代半ばには、Winny やパソコン紛失による情報漏えいが多発した際は、「Winny の使用禁止」「暗号ツールの導入」等の対策が広く採られてきた。

- 形を変えてきた情報漏えい

従来までの情報漏えいは、パソコンや USB メモリの紛失、メールの誤送信といった人の不注意による偶発的な事故が主であった。しかし、最近では、複合機やウェブカメラ、クラウドサービスといったインターネットに接続する機器やサービスが増えており、公開設定ミスによって、情報が外部に筒抜けになる事故が報告されている。情報家電や事務機器の高度化に対して、機器とインターネットとの連動を意識した安全な運用が求められる。

- 自然災害・オペレーションミス

自然災害やオペレーションミスによるシステム障害が、組織のセキュリティの話題として取り上げられる機会は少ない。しかし、組織における事故の中で、これらの発生頻度が最も高く、場合によっては壊滅的な被害にも繋がる。偶発的な事故の発生に備えて、体制や代替運用策、復旧手順等を確立することも重要なセキュリティ対策の一つである。

企業・組織において、内部統制・セキュリティマネジメントは情報セキュリティの確保のために重要な役割を果たしている。IT 環境の変化に伴い、脅威やリスクも変化する。マネジメントもそれに追随していく必要がある。

1.5.インターネットモラル

我々の日常生活でインターネットは必要不可欠な存在となってきており、子供から高齢者に至るまでインターネットを使ったサービスを利用している。一方で、インターネット人口の増大やサービスが多様化する中で、インターネットを使う側のモラル（エチケットやリテラシー）についても問題視されるようになってきた。

- 未成年者に求められる教育

スマートフォンやオンラインゲームの普及に伴い、小中学生でも普通にインターネットを利用する機会が増えた。一方で、「学校裏サイト」と呼ばれる特定の学校の話題について匿名で書き込む掲示板において、他人を誹謗・中傷する等の新しいタイプのいじめが発生し、新たな社会問題を生み出している。また、オンラインゲームへ過度に熱中する中高生が、他人のアイテムを窃取する目的で不正ログインを試みて「不正アクセス禁止法」で検挙されたり、フィッシングサイトを立ち上げる等、犯罪行為の低年齢化も問題になっている。

- SNS による情報の暴露

インターネットモラルは、中高生だけでなく、若者世代においても深刻な問題である。SNS の普及により、他人の興味を引く為にプライベートな情報や職場での出来事を気軽に投稿し易い環境になったと言える。しかし、社会で生活していく上では、最低限の節度は持たなければならない。2013 年には、複数の若者が、コンビニのアイスケースに入って寝そべっている写真等、SNS 上で悪ふざけ写真を公開して社会的な問題に発展した。これらの結末は、個人に留まらず、店側の管理責任（使用者責任）が問われる問題となり、店舗閉鎖に至ったケースもある。

インターネットの利用に関しては、全ての責任は個人に跳ね返ってくる。他人の ID/パスワードの不正利用は不正アクセス禁止法に抵触し、他人の誹謗中傷は名誉毀損罪にて告訴される場合がある。現実社会と同様に、法律遵守やモラルを十分に意識して、インターネットを利用しなければならない。


秘
請求額

2章. 2014 年 10 大脅威

2013 年において社会的影響が大きかったセキュリティ上の脅威について、「10 大脅威執筆者会」の投票結果に基づき、表 2 のように順位付けをした。また、脅威を受ける対象は、攻撃者の意図や狙い、情報システムの形態やユーザーの立場によって異なってくる。

本章では、順位付けと共に脅威を受ける対象を＜一次被害者＞＜二次被害者＞として明記し、それぞれの脅威について解説する。

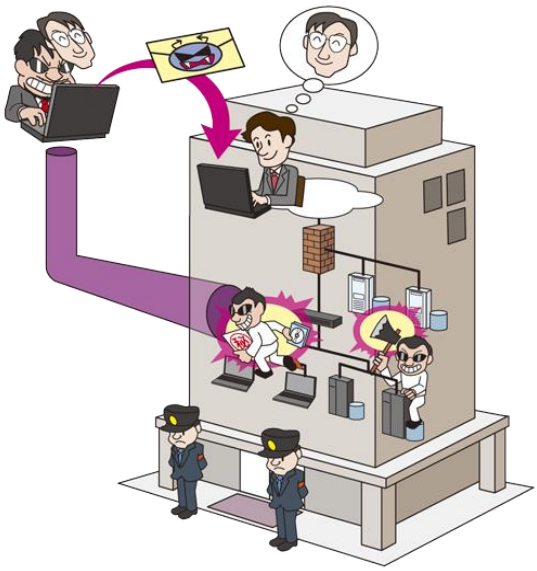
表 2：2014 年版 10 大脅威の順位

順位	タイトル	分類
1	標的型メールを用いた組織への スパイ・諜報活動	サイバー空間(領域)問題
2	不正ログイン・不正利用	ウイルス・ハッキングによるサイバー攻撃
3	ウェブサイトの改ざん	ウイルス・ハッキングによるサイバー攻撃
4	ウェブサービスからのユーザー情報の漏えい	ウイルス・ハッキングによるサイバー攻撃
5	オンラインバンキングからの不正送金	ウイルス・ハッキングによるサイバー攻撃
6	悪意あるスマートフォンアプリ	ウイルス・ハッキングによるサイバー攻撃
7	SNS への軽率な情報公開	インターネットモラル
8	紛失や設定不備による情報漏えい	内部統制・セキュリティマネジメント
9	ウイルスを使った詐欺・恐喝	ウイルス・ハッキングによるサイバー攻撃
10	サービス妨害	ウイルス・ハッキングによるサイバー攻撃

1 位　標的型メールを用いた組織へのスパイ・諜報活動

サイバー領域問題

～政府機関だけでない！民間企業も狙われている～



インターネットを介して組織の機密情報を盗み取る、諜報・スパイ型の攻撃が続いている。本攻撃は、政府機関から民間企業に至るまで幅広く狙われており、国益や企業経営を揺るがす懸念事項となっている。

＜一次被害者＞

政府機関

民間企業

＜脅威と影響＞

気付かない間にスパイに潜入され、機密情報が外部に持ち出されていた。この様な事件がサイバー空間でも行われている。

メールをシステムへの侵入手段とした標的型の攻撃は、最近の攻撃傾向として取り上げられることが多いが、実は 10 年以上前から存在する攻撃である。言い換えれば、攻撃による被害が顕在化し、騒がれ始めたのが、ここ 3、4 年と言うのが正しい。本攻撃の怖さは、「攻撃を受けていることに気付けない」、「攻撃が見えにくい」ところにある。また、影響は、情報システムの枠だけに留まらず、国家間の外交問題に発展している。

- 外交問題に発展

2013 年 7 月にワシントンで開催された「米中戦略経済対話」において、米国の副大統領から中国政府に対して「サイバー攻撃による窃盗行為を止めるように」強い要請がなされたと報じられた。この発言からも、米国政府が、サイバー空間における機密情報の窃盗に頭を悩ませている様子が窺える。

＜攻撃手口＞

攻撃は、多様なテクニックを駆使して「計画的」かつ「戦略的」に行われる。多くの場合、下記のステップで攻撃が実行される。

(1)　計画立案

攻撃対象とする組織を選定し、ウイルスを感染させるユーザーを調査する等の攻撃計画を立案する。

(2) 攻撃準備

ウイルス作成・標的型メールを準備する。

(3) 初期潜入

標的型メールをターゲットユーザーに対して送付し、パソコンをウイルスに感染させる。中には、ウェブサイトや VPN サービス経由による侵入手段も確認されている。

(4) 基盤構築

感染パソコンにバックドアを開設し、攻撃者との通信路を確保する。

(5) 内部侵入・調査

リモートからバックドア経由でシステム内部を調査し、侵入範囲を拡大する。

(6) 目的遂行

目的の情報を窃取する。場合によっては、データを改ざん、削除する。

(7) 再侵入

開設してあるバックドアを通じて、執拗に再侵入が行われる。

- バックドアを通じたリモートハッキング

攻撃手口でポイントとなるのは、バックドアを通じて内部のシステムがハッキングされ、情報が持ち出されることである。また、攻撃者は、一度開設されたバックドアを使い、執拗に情報を盗み取っていくことが多い。一度、攻撃者の餌食になると、長期間にわたって侵害されてしまう。

- 複雑化する初期潜入の手口

数年前まで、初期潜入に関してはパソコン上の脆弱性対策をタイムリーに行っていれば、100%に近い確率で防げるというのが通説であった。しかし、最近では、メールで実行ファイルを送りつける等の脆弱性を使わない手口やゼロデイの脆弱性が悪用されるケースが増えており、初期潜入で食い止めるのが困難になってきている。

＜事例と傾向＞

- 民間企業もターゲットに

攻撃対象は、政府機関に限らず、民間企業に対しても行われていることが観測されている。「IBM Tokyo SOC Report」[I]によると、標的型メールの宛先の業種別では、「官公庁・地方自治体等」が 37.7%と最も多く、続いて「金融機関」: 16.4%、「マスコミ関連」: 13.1%、「IT・通信」: 8.2%となっている。あくまでメールの観測結果であり、攻撃の全体を俯瞰したものではないが、幅広く狙われているのが見て取れる。

＜対策/対応＞

- システム設計策
- ウイルス対策

本脅威への対策は、システム内部に侵入させない為のウイルス対策に加え、侵入後にシステム内部を探索させない、システム設計を合せて実施することが重要である。攻撃は、一連のシナリオに沿って行われる為、各段階における脅威を認識し、攻撃の発見・遮断に努めることが重要である。詳細は「標的型メール攻撃に向けたシステム設計ガイド」[II]を参照していただきたい。

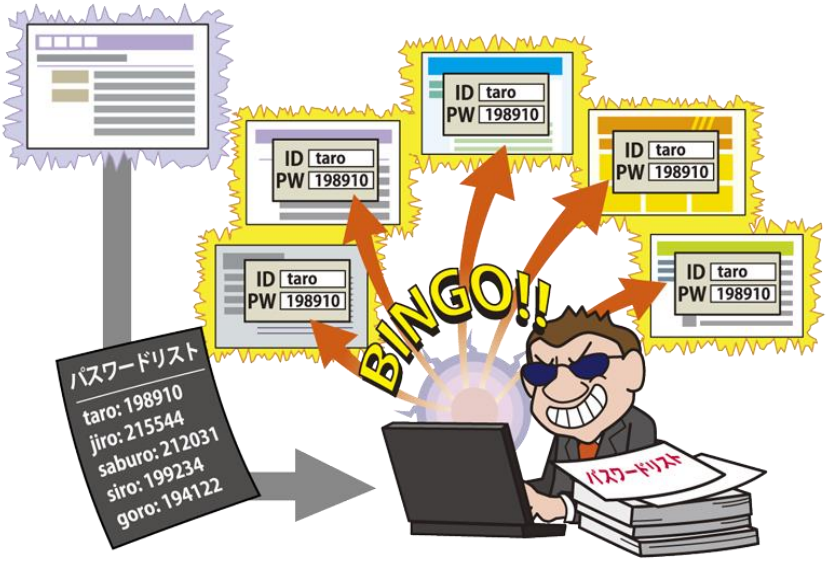
参考資料

I. 日本IBM:「2013年上半期 Tokyo SOC 情報分析レポート」
http://www-935.ibm.com/services/jp/its/pdf/tokyo_soc_report2013_h1.pdf
II. IPA:「標的型メール攻撃に向けたシステム設計ガイド」
http://www.ipajaea.go.jp/security/vuln/newattack.html

2 位 不正ログイン・不正利用

ウイルス・ハッキング
サイバー攻撃

～ユーザーの安全なパスワード管理が重要！～



2013 年は、攻撃者による不正なログインや、それに伴いサービスの不正利用や情報漏えい等の事件が頻発した。不正ログインを誘発する要因の一つに、複数のサイトでパスワードを使い回していることが挙げられ、ユーザーはサイト毎に異なるパスワードを設定することが求められる。

＜一次被害者＞

ウェブサービス利用者

＜脅威と影響＞

- 常に攻撃者が狙っているパスワード

ID/パスワードによる認証方式を採用した会員制のウェブサービスは、多方面で提供されている。ID/パスワードによるユーザー認証は、標準的な認証手段であり、パスワードを本人以外が知らない”秘匿性”を確保することで初めて機能するものである。一方で、パスワードは、本人に成りすますことができる情報でもあるため、常に攻撃者に狙われている。

- 不正ログインによる影響

2013 年は、攻撃者に盗まれたパスワードが複数のサイトで悪用され、不正ログインによる被害が相次いだ。不正ログインによる影響は、サービスの不正使用、情報漏えいに繋がる。また、システム管理者のパスワードが漏えいすると、稼動システムの不正操作だけでなく、データベースに保存されているユーザーのパスワードが窃取される等、二次・三次的な被害に発展してしまう。

- 意外に難しいパスワード管理

パスワードは、他人に知られないように管理しなければならない。近年では一人のユーザーが多数のサービスを利用する。そのために複数のパスワードを管理することはユーザーには大きな負担になっている。また、記憶できる ID/パスワードの組み合わせは 3 種類以下が 70%を占めるアンケート結果が出ている。この状況を狙い、あるサービスから漏れた ID/パスワードを別のサービスで

悪用する攻撃が横行しており、使い回しが原因で多くの不正アクセスが発生している。

＜攻撃手口＞

- パスワードリスト攻撃

パスワードリスト攻撃とは、攻撃者がウェブサイト等から不正に取得した ID/パスワードのリストを使い、複数のウェブサイトで同一の ID/パスワードを利用しているユーザーに対して不正アクセスを仕掛ける方法である。複数のサイトで ID/パスワードを使い回しているユーザーは、攻撃者にパスワードリストを使われると、知らない間に本人に成りすまされ、サービスが不正に利用されてしまう。

＜事例と傾向＞

- 成りすましによる不正アクセス [II]

国内クレジットカード会社は、2013 年 11 月に会員専用ウェブサービスへの不正アクセスが確認されたことを公表した。調査の結果から、第三者が外部インターネットサービス等から不正に取得した可能性の高い ID/パスワードを使用し、会員に成りすまして不正ログインしていたことが判明している。

- パスワード使い回しの危険性 [III]

IPA では、2013 年 8 月の呼びかけでパスワード管理についての注意喚起を行った。あるサービスサイトにおいては、不正ログインの試行件数 15,457,485 件に対して、0.15%にあたる 23,926 件の不正ログインが成立した統計情報となっている。0.15%という数字は一見小さいように思えるが、パスワード総当たり攻撃等と比較すると成功率が高いため、パスワードリスト攻撃は有効な攻撃手法であることが確認されている。

＜対策/対応＞

- パスワードを使い回さない
- ワンタイムパスワード／二要素認証方式の利用

サービス提供側ではパスワード窃取による不正ログイン対策として、パスワードのソルト付きハッシュ化や同一ホストからの連続ログイン拒否等の対策を講じることで、被害を緩和することができる。

ユーザー側も、パスワードを適切に管理することが求められる。推測できない複雑なパスワードをサイト毎に設定して、使いまわさないことが必要である。パスワードを覚えられない場合は、自分だけが見ることができる紙や電子ファイルに書き写し、“他人に知られないように“管理するのも一案である。パスワード管理ツールやメモサービス等を使ってオンライン上でパスワードを管理することは便利であるが、ハッキングされる可能性を認識した上で利用する必要がある。

オンラインバンキング等の重要性の高いサービスやシステムにおいては、ワンタイムパスワードや認証トークン等の認証方式が提供されている場合が多い。極力、認証強度の高い方式を利用することで、不正ログインやサービス不正利用のリスクを低減させることが重要である。

参考資料

I. 「個人・企業のパスワード管理」に関する意識調査結果のご報告
https://www.verisign.co.jp/welcome/pdf/password_management_survey.pdf

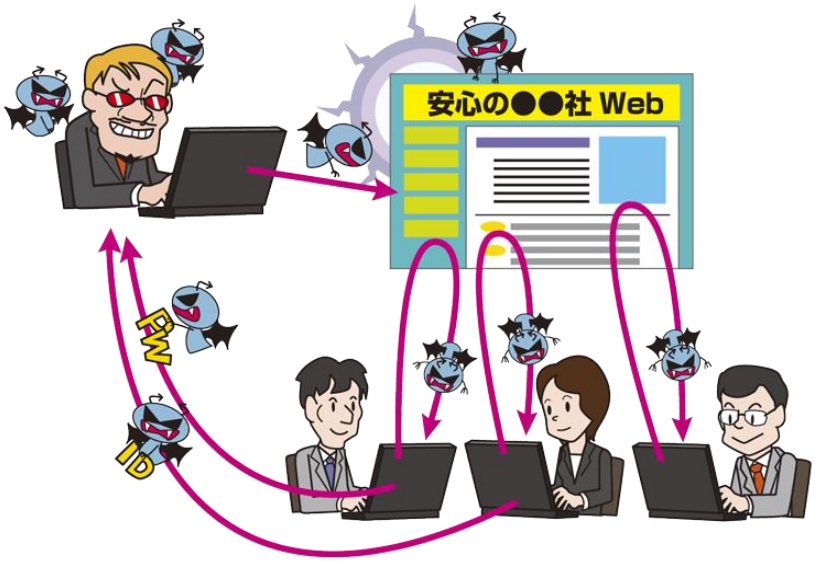
II. 【eオリコサービス】不正アクセスについて（続報）
http://www.orico.co.jp/information/20131115.html

III. 2013年8月の呼びかけ
http://www.ipa.go.jp/security/txt/2013/08outline.html#5

ウイルス・ハッキング
サイバー攻撃

3 位 ウェブサイトの改ざん

～気づかぬうちにウイルス感染～



2013 年は、ウェブサイトの改ざん被害が増加した。ウェブサイト改ざんは、ウイルス感染の踏み台にも悪用される手口であり、ウェブサイト運営側は、改ざんによる最終的な被害者がウェブサイト閲覧者になる点を認識して、十分な対策を実施しておかなければならない。

＜一次被害者＞　**＜二次被害者＞**

ウェブサイト運営者　ウェブサイト閲覧者

＜脅威と影響＞

2013 年は、政府・民間企業のウェブサイト改ざんの被害が飛躍的に増えた年である。ウェブサイト改ざんというと、目に見える画像や情報をページに挿入するイメージを持たれるが、改ざんの大半は、見た目の変化は無く、ウイルスをダウンロードする攻撃コードが埋め込まれている状態である。改ざんされたウェブサイトを閲覧したユーザーは、知らぬ間にウイルスをダウンロードしており、パソコンの情報が抜き取られたり、ネットワークへの不正侵入等の被害に発展する。

- 気付けない改ざん

改ざんされていてもウェブサイトの見た目は全く変化が無く、尚且つ正規のウェブサイトである為、サイトを閲覧したユーザーが不審に思うケースは少ないと言える。その為、他のウイルス感染手口に比べて罠に引っ掛る可能性が高い。

- 水飲み場攻撃

攻撃対象組織の職員が閲覧しそうなウェブサイト（水飲み場）を改ざんし、そのサイトを閲覧させることで、ウイルス感染させる手口を「水飲み場攻撃」と呼ぶ。名前の由来は、砂漠等の乾燥地域にあるオアシスに寄ってくる動物を待ち伏せて仕留める攻撃になぞらえたものである。攻撃成功確率が高いことから、今後ウイルス感染の主流手口となることが危惧される。

＜攻撃手口＞

ウェブサイト改ざんは、ウェブサーバーの

設定不備やソフトウェアの脆弱性、管理アカウントが悪用されて行われる。代表的な攻撃の手口としては、下記の 4 つが挙げられる。

- 管理端末からログイン情報窃取

ウェブサイト運営者の管理用端末がウイルスに感染し、ウェブサイト管理用のパスワードが窃取される。攻撃者は、盗んだパスワードを元に不正ログインを行い、コンテンツを書き換える。

- FTP、SSH 等のアカウントハッキング

世の中の多くのウェブサイトは、メンテナンス用 FTP、SSH のサービスを使用している。しかし、ID/パスワードによる認証方式を採用している場合、パスワード推測、辞書攻撃等に弱く、不正ログインが行われ、コンテンツが書き換えられてしまう。

- CMS の脆弱性悪用

コンテンツ管理システム（CMS）の脆弱性が悪用されると、その管理下にあるウェブサイトが改ざんされてしまう。特に WordPress や Joomla!等、世間のウェブサイトで広く使われている製品に脆弱性がある場合、共通の攻撃手法が多数のウェブサイトで適用できる為、大規模な攻撃に発展しやすい[I]。

- ウェブアプリケーションの脆弱性悪用

CMS 製品以外のウェブアプリケーションでも、脆弱性が悪用されることがある。例えば、「SQL インジェクション」の脆弱性が悪用されると、データベースを利用しているコンテンツが改ざんされてしまう。

＜事例と傾向＞

- ウェブサイト改ざん被害急増[II]

JPCERT/CC によると、ウェブサイト改ざんの月別被害件数が、2013 年 6 月および 7 月は 4,000 件を越える等、2013 年 1 月から 4 月までと比較して、2 倍以上に増加した。

- レンタルサーバーにおける改ざん被害[III]

2013 年 9 月、国内レンタルサーバー会社において、8,438 件のユーザーサイトが改ざんされる被害が発生した。改ざんの手法については、WordPress のプラグイン等の脆弱性を利用したものである。攻撃者により不正にアップロードされたファイルを利用され、設定情報が抜き出されることで、データベースの書き換えが行われ、サイトが改ざんされたと報告している。

＜対策/対応＞

- セキュアなサーバーの設定
- アカウント・パスワードの管理
- ソフトウェアの定期的な更新
- ウェブアプリケーションの脆弱性対策

ウェブサイトを狙った攻撃は、システムの設定不備やソフトウェアの脆弱性が悪用される。開発・構築時においてソフトウェアの脆弱性を作り込まないための対応や脆弱性診断を行い、セキュアな設定を施したサーバー構築を心掛けることが重要である。また、運用フェーズにおいても、定期的なソフトウェアの更新やアクセス権の管理や改ざん検知等、運用・監視を怠らない事が大切である。

参考資料

I. ウェブサイト改ざん等のインシデントに対する注意喚起～ウェブサイト改ざんが急激に増えています～
https://www.ipa.go.jp/security/topics/alert20130906.html

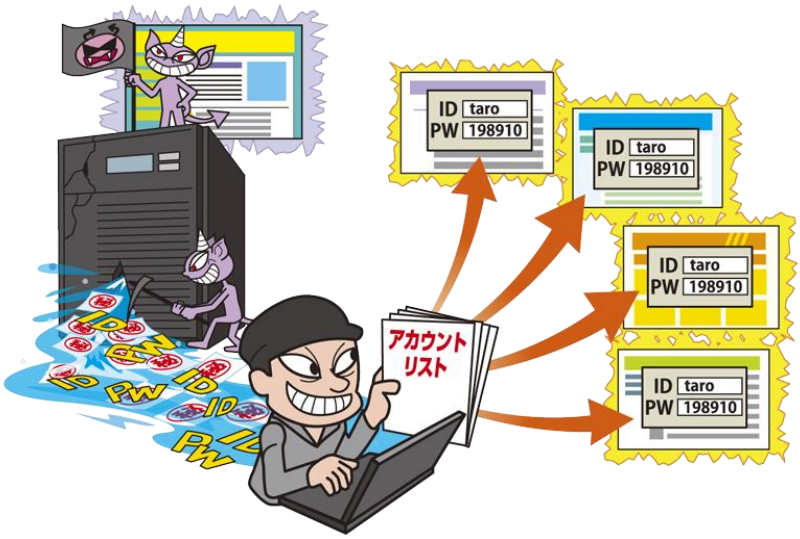
II. JPCERT/CC インシデント報告対応レポート［2013年10月1日～2013年12月31日］
http://www.jpcert.or.jp/pr/2014/IR_Report20140116.pdf

III. 第三者によるユーザーサイトの改ざん被害に関するご報告
http://lolipop.jp/info/news/4149/

ウイルス・ハッキング
サイバー攻撃

4 位 ウェブサービスからのユーザー情報の漏えい

～ハッキングによりユーザー情報がごっそり盗まれる～



2013 年前半、外部からの攻撃により大量のユーザー情報が流出する被害が、会員制のウェブサービスで多発した。クレジットカード情報等の個人情報を大量に保持しているサービスから情報が流出してしまうと、影響が広範囲に及ぶため、十分な対策が求められる。

＜一次被害者＞　**＜二次被害者＞**

ウェブサイト運営者　ウェブサービスユーザー

＜脅威と影響＞

インターネット上で提供されるウェブサービスは、生活に必要不可欠な存在となっている。一方、ウェブサイトにはサービスの対象となる膨大な数のユーザー情報が保管されており、攻撃者からみれば恰好のターゲットである。2011 年に PlayStation Network から 7 千万件以上の個人情報が漏えいし、大きく報道されたが、その後も大量の個人情報が外部に流出する“メガリーク”が相次いでいる。

- 影響は多方面に波及

メガリークによる影響は、一企業やサービスユーザーだけに留まらない。大量のパスワードが漏えいすれば、そのリストを悪用される可能性がある為、漏えいしたウェブサイトだけでなく、インターネット上でサービスを展開しているウェブサイトにも不正ログインのリスクが高まる。この様にメガリークによる影響は、漏えい元の一企業で収まる問題ではなく、社会的にも影響の大きい問題である。

- ウェブサービスユーザーへの影響

個人情報の漏えいにより、最も被害を受けるのは、当然のことながらウェブサービスユーザーである。ウェブサービスユーザーには、次の様な被害が及ぶ。

- スパムメール
- 悪徳セールス
- クレジットカード悪用による金銭被害
- 不正ログイン

＜攻撃の手口＞

攻撃には、先に挙げた「ウェブサイトの改ざん」と同様な手口が用いられることが多い。また、標的型攻撃のように、システム内部に潜入し、ウェブサイトの情報を窃取する手法も確認されている。

- 脆弱性の悪用

ウェブサービスは、単一のソフトウェアだけでなく複数のサービスレイヤーのソフトウェアで構成されている。サービス用に個別に開発したアプリケーションや、オープンソース等の汎用的なアプリケーションの脆弱性が狙われる。Apache Struts 2 等ウェブサイトを構築するためのフレームワークや、WordPress 等のコンテンツ管理システム（CMS）が狙われる傾向にある。

- 標的型攻撃

外部からの直接の攻撃だけでなく、ターゲット組織に標的型メールを仕掛け、バックドアを開設し、システム内部に侵入する手口も使われる。システム内部に侵入した攻撃者は、侵入範囲を拡大しウェブシステムを攻略し、情報を窃取する。

＜事例と傾向＞

- クレジットカード情報漏えい事故多発

2013 年前半、顧客のクレジットカード情報の漏えい事故が相次いだ。眼鏡の販売を手がける JINS は、利用しているミドルウェア Apache Struts 2 の脆弱性を悪用され、2,059 件のクレジットカード情報が漏えいしたと発表した。[I] また、ネットスーパーのセブンネットショッピングにおいては、成りすましによって、最大 15 万 165 件のクレジットカード情報が不正に閲覧された可能性があると発表した。[II] 2013 年後半には、アドビシステムズが 290 万件の認証情報と暗号化されたクレジットカード情報が漏えいしたと発表し、全世界で大きく報道された。[III]

- 標的型攻撃による情報漏えい

Yahoo! Japan が、最大 148.6 万の不可逆暗号化されたパスワード、パスワード再設定に必要な情報の一部が漏えいした可能性があると公表した [IV]。組織内部のパソコンが標的型攻撃を受け、そのパソコンを介してウェブシステム内部に情報収集用のプログラムが仕掛けられたことが原因とされている。

＜対策/対応＞

- ネットワークアクセス制御
- セキュアなサーバーの設定
- OS・ソフトウェアの更新
- 脆弱性対策

ウェブサイトを狙った攻撃に対処するには、ウェブシステムやウェブアプリケーションの脆弱性対策やセキュアな設定によって、ウェブサービスを適切に保護することが重要である。また、内部からウェブシステムに不正アクセスされないように、運用環境に対して標的型攻撃対策等を講じる。

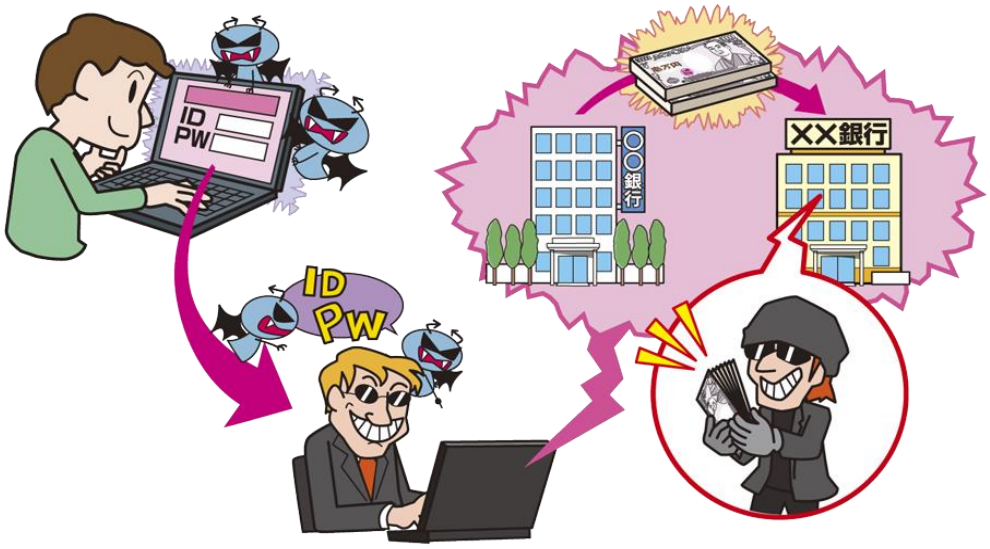
参考資料

I. 不正アクセスによるJINSオンラインショップのお客様情報流出に関するお知らせ
http://www.jins-jp.com/illegal-access/news.html
II. セブンネットショッピングでカード情報漏えいの可能性～最大15万件
http://internet.watch.impress.co.jp/docs/news/20131029_621296.html
III. お客様情報のセキュリティに関する重要なお知らせ（アドビハック）
http://helpx.adobe.com/jp/x-productkb/policy-pricing/customer-alert.html
IV.「当社サーバへの不正なアクセスについて」（5/17発表）の追加発表（ヤフー株式会社）
http://pr.yahoo.co.jp/release/2013/0523a.html

ウイルス・ハッキング
サイバー攻撃

5 位 オンラインバンキングからの不正送金

～攻撃者が銀行の認証情報を狙っている～



2013 年は、オンラインバンキングの不正送金の発生件数、被害額が過去最大となり、世間でも注目が集まった。フィッシング詐欺やウイルスにより、ユーザーのパスワードが盗まれ、本人に成りすまして、不正送金が行われる。

＜一次被害者＞　　**＜二次被害者＞**

オンラインバンキング　　銀行・クレジットカード会社

ユーザー

＜脅威と影響＞

オンラインバンキングの不正送金は、主に攻撃者がユーザーに成りすました不正ログイン・不正操作により実行される。攻撃者は、フィッシング詐欺やウイルスを使って盗んだパスワードを悪用して、本人に成りすまして攻撃者の口座に送金する。ユーザーは、預金残高を確認するまで、自身が被害に遭っているとは気付きにくく、事件の発覚が遅くなる傾向にある。

2012 年は大手銀行を狙ったフィッシング詐欺が広く行われ注目を浴びたが、2013 年は大手銀行だけでなく、地方銀行やネット銀行でも不正送金が行われ、被害の範囲が拡大している。

＜攻撃手口＞

オンラインバンキングから不正送金を行う為の ID/パスワードの窃取は、フィッシングサイトによるものとウイルス（不正プログラム）によるものの、2 つに分けられる。

- フィッシングサイトによる犯行

(1) 銀行やクレジットカード会社等の実在する組織を装ったメールをユーザーに送りつける。

(2) メールに添付された URL からフィッシングサイトに誘導し、ユーザーにオンラインバンキングの ID/パスワードを入力させる。

(3) 不正に取得した ID/パスワードを使ってオンラインバンキングにログインし、正規ユーザーに成りすまして、攻撃者の口座へ送金処理を行う。

- ウイルスによるパスワード漏えい

(1) OS やソフトウェアの脆弱性への対策を実施していないユーザーが、攻撃者が用意したウェブサイトに意図せずアクセスする。

(2) 攻撃者が用意したウイルスが自動的にダウンロードされ、自動的に感染する。

(3) ユーザーが標的となるオンラインバンキングにアクセスすると、ウイルスがマン・イン・ザ・ブラウザという手法を用いて偽の入力画面等をブラウザ上に表示し、ユーザーID、パスワード、第2暗証番号等を窃取する。

(4) 攻撃者は(3)で取得した情報を使用して不正送金を行う。

2013 年に起きた不正送金の事例において、ウイルス感染による犯行が全体の約98%を占めている。[I]

＜事例と傾向＞

- ウイルスによる不正送金被害の急増 [II]

インターネットバンキングの口座から預貯金が不正に送金される被害が、2013 年 1 月から 11 月末までに約 11 億 8,400 万円となったことが警察庁のまとめで明らかになった。この数字は、過去最悪だった 2011 年（年間約 3 億 800 万円）の 4 倍近い数字である。

- ワンタイムパスワードの盗取 [III]

不正送金被害への対策として、ワンタイムパスワードを利用し、取引の度にメールでパスワードを受け取る方法がある。このワンタイムパスワードを盗取する事件も発生している。ユーザーがフリーメールを利用してワンタイムパスワードを受け取る場合、フリーメール用の ID/パスワード等を第三者に不正に盗取され、メールの内容を覗き見られる事象が確認された。本件に起因すると思われる不正送金も実際に発生している。銀行のウェブページでは、「ワンタイムパスワードをメールで受けとる場合は、フリーメールではなく、携帯電話やスマートフォン等のパソコンとは別デバイスのメールで受け取るよう」に呼びかけている。

＜対策/対応＞

- OS・ソフトウェアの更新
- ウイルス対策ソフトの導入
- ワンタイムパスワードの利用
- 事例や手口を知る

ウイルス感染を阻止する為には、ウイルス対策ソフトと併せて JRE 、Adobe Reader,Adobe Flash Player 等のソフトウェアの更新をタイムリーに行うことが最も重要である。

銀行によっては、ワンタイムパスワード方式等、ID/パスワード以外の認証方式を提供しているので、極力、セキュリティ強度の高い認証方式を利用するのが良い。

また、ユーザー自身で「不用意に添付ファイルを開かない」「不用意にパスワードを入力しない」等の騙されない対応を心がけることが重要である。

参考資料

I. ネット不正送金11．8億円、最悪時の4倍＝25銀行、46都道府県の客ー警察庁
http://www.jiji.com/jc/zc?k=201312/2013121200517

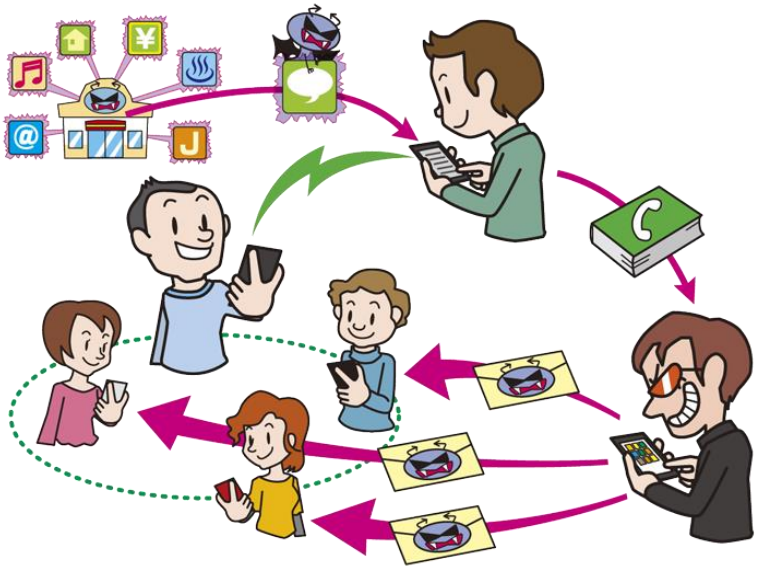
II. 不正送金及び不正アクセス等の被害について
https://www.antiphishing.jp/news/pdf/apcseminar2013npa.pdf

III. 不正送金の被害に関するご注意と対策について
http://www.rakuten-bank.co.jp/info/2013/130502.html

ウイルス・ハッキング
サイバー攻撃

6 位　悪意あるスマートフォンアプリ

～スマートフォンに保存されているデータが盗み取られています～



魅力的なコンテンツを含んでいると見せかけた悪意あるスマートフォンアプリにより、端末に保存されている電話帳等の情報が、知らぬ間に窃取される被害が続いている。また、収集された個人情報が、スパム送信や不正請求詐欺等に悪用される二次被害も確認されている。

＜一次被害者＞　　**＜二次被害者＞**

スマートフォンユーザー　　電話帳登録者

＜脅威と影響＞

スマートフォンユーザーは、従来の携帯電話よりも便利な機能を利用できるようになった。従来の携帯電話と比べたスマートフォン最大の特徴は、ユーザーが好きなアプリを自由にインストールできる点である。アプリには実用的なもの、趣味や娯楽に関するもの等、様々なものがあり、子供から高齢者に至るまで、様々なユーザーに利用されている。一方で、電話帳の情報を盗み取るアプリによる被害が増加している。

- 個人情報が狙われる

スマートフォンの電話帳には、膨大な数の個人情報が格納されている。電話帳には、個人の氏名、電話番号、メールアドレス、場合によっては会社の所属先まで記録されている。言い換えると、電話帳は“他人”の個人情報の集合体と言える。また、スマートフォンには、電話帳に限らず通話記録、メール情報、位置情報等プライバシー情報も多く含んでいる。攻撃者は、悪意あるアプリをばら撒き、スマートフォン上の情報を盗み出そうと試みる。

- 二次被害の怖さ

個人情報が漏えいした影響は、スマートフォンの所有者だけでなく、電話帳に登録されている知人にまで及んでしまう。電話帳に登録されている知人が、勧誘電話、スパムメールの標的になってしまう等、被害は後からジワリと忍び寄ってくる。スマートフォン所有者は、他人の個人情報を預かっていることを忘

れず、セキュリティ対策を行わなければならない。

＜攻撃手口＞

- 悪意あるアプリの配布

攻撃の大半は、ユーザーが悪意あるアプリをインストールすることで開始される。アプリの配布手法は、正規のアプリマーケットに有益な機能を持ったアプリと見せかけて登録し、被害者にインストールさせる手口が多い。また、パソコン同様にメール経由でアプリをインストールさせるもの等が存在する。端末上で電話帳へのアクセスを要求するアプリ等の悪意のあるアプリは、ユーザーは見た目では危険度を確認できず、有益なアプリと思い込んでしまう。

- 個人情報窃取以外の脅威

スマートフォンアプリに関する脅威は、個人情報の窃取だけではなく、「ボットネット」、「SMS トロイの木馬」等も存在する。Wi-Fi や Bluetooth を通じて近隣のスマートフォンに感染範囲を拡大し、ボットネットを形成するウイルスが登場している。また、海外において、SMS トロイの木馬が、プレミアム SMS の番号にメッセージを送信して、ユーザーに追加費用を支払わせ、攻撃者が金銭を得ている。

＜事例と傾向＞

- モバイルマルウェアの爆発的な増加[I]

Juniper Networks の発表した資料によると、2012 年 3 月から 2013 年 3 月にかけてスマートフォンをターゲットにしたマルウェアが 614%増加したと発表した。これは、27 万 6,259 件の悪意のあるアプリが世の中に出回っていることを示している。また、悪意あるアプリの 92%は Android OS をターゲットにしたものであると報告している。

- 81 万人のデータ抜き取り[I]

延べ約 81 万人が「ウイルス対策」等と騙った偽のアプリをダウンロードし、約 3,700 万人分の電話帳データが抜き取られる事件が発生した。逮捕された犯人は、抜き取った電話帳のデータを使い、不特定多数に勧誘メールを計 3 回送り付ける等し、自身が運営するサイトに誘導し、約 3 億 8,900 万円を売り上げたと言われている。

＜対策/対応＞

スマートフォンユーザーは、下記を実施し、危険を回避することが重要である。[II]

- スマートフォンの OS は常に最新の状態に更新する
- アプリは信頼できる場所からインストールする。ユーザーレビュー/評価を確認し、怪しいアプリをインストールしない
- Android 端末では、「提供元不明のアプリ」はインストールしない設定にしておく
- Android 端末では、アプリをインストールする際にアクセス許可を確認する
- アプリは常に最新の状態で利用する
- セキュリティ対策ソフトを利用する

参考資料

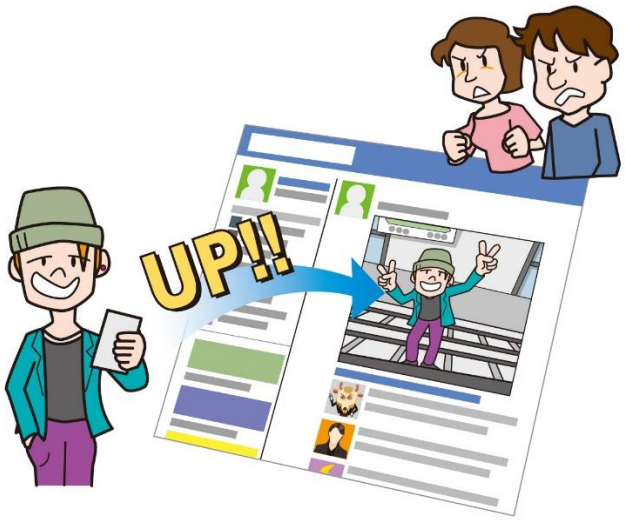
I. 不正アプリ使い勧誘容疑 80万人のデータ抜き取り正アプリ使い勧誘 80万人のデータ抜き取り IT企業社長ら逮捕
hhttp://www.sponichi.co.jp/society/news/2013/07/24/kiji/K20130724006284570.html

II. スマートフォンのセキュリティ<危険回避>対策のしおり
http://www.ipa.go.jp/files/000011456.pdf

インターネット
モラル

7 位 SNS への軽率な情報公開

～悪乗りや失言が社会問題に～



SNS の普及に伴い個人がプライベートな情報を気楽に発信できる時代となった。その一方で、従業員や職員が、職務に関係する情報を軽率に SNS へ投稿したことが原因で、企業・組織が損害を受ける事例が散見されている。

＜一次被害者＞

企業・組織

＜脅威と影響＞

携帯やスマートフォンの普及に伴い、ブログや SNS（ソーシャルネットワーキングサービス）が増大し、自己表現やコミュニケーションのツールとして定着してきた。Facebook や Twitter の登場は、コミュニケーションのあり方に変革をもたらしたと言われており、グローバルに情報を発信でき、様々なテーマでネットワークを構築することができる。

- 業務とプライベートの境界の崩壊

一方で、職務に関係する情報を軽率に SNS へ投稿したことが原因で、企業・組織に悪影響を及ぼす事例も見られる様になった。私的に行った投稿が反社会的でありモラルに欠ける行為であった為に、企業・組織の監督能力が疑われ、所属する企業・組織の信頼低下や営業停止等の被害が発生している。

- 組織は私人の集合体

当然のことながら、組織は私人の集合体であり、各個人のモラルやプライベートな事柄まで組織で把握・管理することは難しい。ただ、個人の私的な行為で組織運営に影響を及ぼす点は、事業継続上の脅威として認識しておかなければならない。また、個人においては、社会通念上のモラルを意識して行動することが求められる。

＜発生要因＞

不適切な画像や投稿を行う要因として、一部の SNS やブログのユーザーが、誤った認識を持っていることが挙げられる。

- 自己顕示欲の増長

SNS は、自身の情報を対外的に発信でき

るツールであり、いわば自身の存在感を友人・知人に伝えることができる。しかし、自分の行為がどういう意味を持つか、どう評価されるのか、という点の認識が誤っていると、外部から大きく批判されることになってしまう。また、インターネットに一度投稿した情報は、簡単に消すことができず、半永久的に残ってしまう。投稿や発言をする前に、冷静になって物事を考える必要がある。

- 予想外の情報拡散

Twitter 等の SNS は、投稿者本人の想定以上に情報が拡散する可能性がある。しかし、投稿者本人は、自身の投稿がどの様に社会に影響を及ぼすか理解していないケースが多い。投稿者は、SNS の特性と発言による影響を理解することが大切である。

- 公開範囲の誤認識

投稿内容の公開範囲の設定が、誰でも閲覧できる一般公開になっていることに気づかないユーザーも存在する。また、投稿に対して友人等、特定の人しか反応が無い状態が続くことで、友人しか閲覧していないという誤認識を持ってしまい、軽率な投稿を行ってしまうケースも存在する。

＜事例と傾向＞

- バカッターが社会問題に

バカッターとは、Twitter で馬鹿げた写真を公開することを指し示した造語である。2013 年 7 月、コンビニエンスストアを展開する企業のアルバイト店員が冷凍ケースに入っている写真を Twitter に投稿した。[I] その写真を見た人から不衛生である等の指摘を受ける事象が発生した。[II] その後、同様の事例が続き、店舗の閉鎖や従業員への訴訟、損害賠償請求に発展した事例も存在する。

- 官僚による不適切な発言

2013 年 6 月、市民団体へ立場上不適切な発言等を Twitter に投稿した官僚に対し 30 日間の停職処分が下された。処分を受けた官僚は、過去に Twitter のプロフィールに本名や経歴を掲載しており、本人の写真や動画等がインターネット上で明らかにされ、新聞等で報道されるまでに至った。[III]

また、2013 年 9 月、過去に個人のブログで不適切な暴言や批判を繰り返していた官僚に対し、停職 2 ヶ月の懲戒処分が下された。この官僚は、所属や実名等の個人情報を公開していなかったが、ブログの投稿内容から個人が特定された。

＜対策/対応＞

- 個人ユーザーのモラル向上
- 組織人の教育
- SNS 利用ポリシーの規定

企業・組織は、従業員や職員に対して不適切な写真や投稿が、社会的な問題を引き起こし、企業・組織に損害を招く可能性があることを周知することが必要である。また、従業員や職員に対して、SNS 利用に関するポリシーを定めることも抑止効果が見込まれる。更に、システム的にウェブ閲覧を制限することで、ポリシーに応じた運用も一つの緩和策である。

参考資料

I. アイスケースに入り→ツイッター投稿　19歳少年を書類送検　群馬県警
http://sankei.jp.msn.com/affairs/news/131018/crm13101813260004-n1.htm

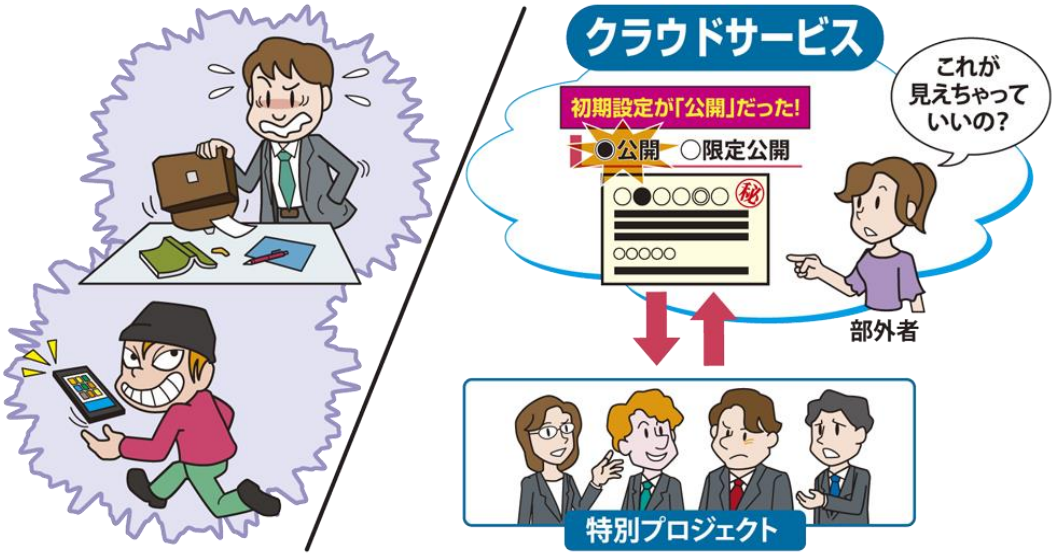
II. 非常識写真、相次ぐツイッター投稿　ウケ狙い過激化　稚拙な悪ふざけ
http://sankei.jp.msn.com/affairs/news/130825/crm13082509050001-n1.htm

III. 暴言ツイッター官僚、降格され大阪に異動　総務省「本省のままでは無理」
http://sankei.jp.msn.com/west/west_affairs/news/130724/waf13072413510015-n1.htm

8 位 紛失や設定不備による情報漏えい

内部統制・セキュリティマネジメント

～管理者によるコントロールが年々困難に～



ノートパソコンや USB メモリの紛失といった情報漏えい事故は後を絶たず、今日でも最も頻発するセキュリティ事故の 1 つである。一方、スマートフォンやクラウドサービスが普及し、情報を保管する手段、媒体・場所が多様になったことで、情報漏えいを引き起こすリスクが拡大した。

＜一次被害者＞　　**＜二次被害者＞**

企業・組織　　取引先の組織

＜脅威と影響＞

情報を蓄積したパソコンやデバイス等の紛失による情報漏えいは、旧来から存在するセキュリティ事故である。しかしながら、今日でも最も発生頻度の高いセキュリティ事故の 1 つである。

- デバイス増加に伴う流出経路の拡大

USB メモリやノートパソコン等の媒体を利用し、内部データを顧客先等の外部に持ち出すことが多くなっている。また、個人所有のスマートフォンやタブレットが急速に普及しており、内部データが個人所有のデバイスにコピーされ易い環境になってきている。記憶デバイスは、所有者が適切に管理できていれば、情報漏えいは起きない。しかし、記憶デバイスは物理的な“モノ”であるため、常に紛失・盗難のリスクを抱えており、情報漏えいは後を絶たない。

- 情報漏えいケースの変化

また、物理デバイスの紛失・盗難だけでなく、機器の設定不備によって外部から情報が閲覧されるタイプの情報漏えいも確認されている。背景には、インターネットを利用するオフィス機器やクラウドサービスが増えたことが挙げられる。このように、情報漏えいのリスクは年々拡大しており、システム管理者の負担の大きい環境が作られている。

この状況下において、不注意や設定不備によって機密情報が外部に漏えいすることにより、以下の影響を及ぼす。

- 第三者に機密情報を入手・悪用される

- 漏えい発覚により、顧客/サービスユーザーからの信頼やビジネス機会を損失する等、事業に悪影響を与える

＜発生要因＞

- 盗難・紛失による情報漏えい

従業員や職員の不注意や過失により、データ記憶媒体の紛失・盗難の被害に遭うことが考えられる。USB メモリ等の記憶媒体は小型であるため、持ち運びやすい反面、紛失しやすい。また、スマートフォンやノートパソコンは、高価であるため、盗難される危険性がある。

- システム環境変化に伴う漏えい

(1)個人のモバイル環境の充実

個人向けの Wi-Fi ルーターが急速に普及している。Wi-Fi ルーターを組織内に持ち込み、業務用パソコンからインターネットへ接続することで、新たな情報流出ルートを設けてしまい、情報漏えいのリスクを高めている。管理者の知らない間に行われてしまうことが問題視されている。

(2)設定不備に伴う情報漏えい

近年、クラウドサービスやインターネットに接続する機器を利用する機会が増えている。しかし、アクセス制限や認証の無い設定で機器やサービスを利用すると、第三者がアクセス可能な状況を生み出し、情報漏えいの原因となってしまう。

＜事例と傾向＞

- Google グループを一般公開[I]

2013 年 7 月、クラウドサービス Google グループを使用して情報共有や意見交換を行っていた複数の組織の情報が一般公開設定になっていたため、誰でも閲覧できる状態であった。Google グループの初期設定が「一般公開」であることを、ユーザーが理解していなかったことが原因と考えられている。

- インターネットから閲覧可能な複合機[II]

2013 年 11 月、インターネットからアクセス可能な状態で設置されている複合機の存在を報道機関によって指摘された。公開状態にある複合機内のファックスで受信した文書やスキャナーでスキャンされた文書の多くには個人情報が含まれており、その文書に誰でもアクセスできる状態であった。

＜対策/対応＞

- 情報持ち出しルールの設定
- BYOD の組織ポリシーの徹底
- ユーザー教育
- 利用するサービスの仕様の理解
- アカウント・アクセス権限の管理
- 暗号化対策

ユーザー教育により、記録媒体の持ち出しルールの徹底や安全なクラウドサービスの利用を理解させることが必要である。

クラウドサービスの利用においては、必要以上に情報を開示しない様に、適切にアカウント・アクセス権を管理することが重要である。

記録媒体の持ち出しに関しては、ノートパソコンのハードディスクや USB メモリのデータを暗号化する製品を利用し、情報漏えいが発生しても被害を軽減することも重要である。

参考資料

I. 省庁でメール公開状態に グーグルG閲覧制限せず
http://www.nikkei.com/article/DGXNASDG10016_Q3A710C1CC0000/

II. 複合機をお使いのお客様へ ： 複合機のセキュリティーに関する報道について
http://www.jbmia.or.jp/whatsnew/detail.php?id=294

ウイルス・ハッキング
サイバー攻撃

9 位 ウイルスを使った詐欺・恐喝

～偽ウイルス対策ソフトや恐喝ソフトによる金銭要求～

ランサムウェアというパソコンをロックして身代金を要求するウイルスによる被害が増加している。感染するとデータにアクセスできなく場合があり、業務への支障や個人への心理的なダメージが大きい。

＜一次被害者＞

インターネットユーザー

＜脅威と影響＞

ある日突然、ウイルスに感染したパソコンにロックが掛けられてしまい、ファイルを取り出すことが出来ない。更には、画面上に「あなたのコンピューターはロックされています。支払いを行うまでアクセスできません」とメッセージが表示される。この様な、パソコンが利用できない状態を作り出し、金銭的な要求を行う「ランサムウェア」と呼ばれるタイプのウイルスが確認されている。[1]

- データを人質に金銭が要求される

「ransom」は英語で「身代金」を意味する。即ちランサムウェアは、ユーザーのパソコンのデータを人質に取り、犯人によって金銭的な要求が行われる仕組みである。

- 支払いかデータ破棄かのジレンマ

ランサムウェアに感染したパソコンは、犯人の要求に従って金銭を支払うか、データを断念するかの判断を強いられる。また、金銭の支払いを行ってもロック解除されないこともあり、最悪の場合、データを断念しなければならない。だが、ユーザーにしてみると、パソコンに保存されているデータは貴重な情報資産である。

- 思い出写真が消失

個人が使用するパソコンの場合、自分がダウンロードした趣味の動画や音楽ファイル等が含まれる。また、家族や友人と過ごした思い出の写真が含まれていることもあり、データが消去したことによる心理的ダメージが大きい。また、業務パソコンの場合は、メー

ルデータや取引先との関連資料が含まれており、ビジネス的な被害が大きい。

＜攻撃の手口＞

- ランサムウェアのタイプ

ランサムウェアは主に２つのタイプが存在する。パソコンの画面をロックして使用できない状態にするタイプと、感染先パソコンやUSB メモリ等の媒体や共有ドライブのファイルを暗号化してアクセス不可能な状態にするタイプである。どちらも、ロックや暗号化の解除と引き替えに身代金を要求し、クレジットカード情報を入力させる。ランサムウェアの多くが、金銭の要求時に司法機関や警察機関であると騙った偽りの画面を表示するのも特徴である。

- 感染経路

ランサムウェアは、通常のウイルス感染同様に、改ざんされたウェブサイト、悪意のある広告、メール等の複数の感染経路が存在する。ウイルス感染の手口についても、ユーザーが騙されてインストールしてしまうケースや、ソフトウェアの脆弱性を悪用したものが存在する。また、ウイルス感染してしまうと、パソコンのハードディスクを初期化せざるおえないケースも存在し、復旧を含めて大きな損失が発生することになってしまう。

＜事例と傾向＞

- ランサムウェア CryptoLocker[II]

2013 年後半、ファイルを暗号化するタイプのランサムウェア CryptoLocker の感染が拡大した。トレンドマイクロによると、CryptoLocker は急激に感染数が増加し、2013 年 10 月には前月比の 3 倍を記録した。

CryptoLocker は、ファイルをランダムに暗号化してロックし、ファイルを復号する鍵とツールを高額（日本円で約 300 万円）で売りつける。感染すると高度な技術でファイルが暗号化されてしまうため、復号のための鍵がなければ解読は不可能となる。重要なファイルのバックアップを取っておく等の、事前の対策が必要である。

＜対策/対応＞

- ウイルス対策ソフトの導入
- OS・ソフトウェアの更新
- データのバックアップ

ウイルス感染しなければ、被害に遭うことはない。その為、ウイルス対策ソフトの導入と OS やソフトウェアのセキュリティアップデートによる脆弱性対策をタイムリーに行っておくことが、必要不可欠な対策となる。

また、怪しいウェブサイトへのアクセスややメールやウェブサイトにおいて、不用意にリンクをクリックしないように、日頃から心がけることも重要である。

さらに、重要なデータがあれば、定期的にバックアップを取得しておくと良い。特に、職場で共有しているネットワークドライブは、業務上必要なファイルが存在するため、適切に保護する必要がある。

参考資料

I. 身代金要求型ウイルス、国内で160件以上確認
http://www.sankeibiz.jp/business/news/131105/bsj1311050608002-n1.htm

II. ランサムウェア「CryptoLocker」に感染しないためにすべきこと
http://blog.trendmicro.co.jp/archives/8074

ウイルス・ハッキング
サイバー攻撃

10 位 サービス妨害

～妨害手口はさまざま、気づかず加担することもある～

2013 年には、韓国の複数企業や政府機関のシステムがウイルスによってデータ破壊され、サービス停止状態に陥った。また、オープンリゾルバ設定になっている DNS サーバーを踏み台にした DDoS 攻撃が問題となっている。

＜一次被害者＞

企業・組織

＜脅威と影響＞

IT への依存度が高まった今日の情報社会において、安定的なサービス提供は、最も重要な課題の 1 つである。しかし、サービス提供者の意図に反して、サービス停止、データ破壊等の被害を受ける妨害型の攻撃が行われるケースが散見される。

攻撃者側のモチベーションは、様々である。金銭的な要求による攻撃から、プロパガンダ・ナショナリズムに乗じた攻撃、敵対する国家・組織への妨害工作として行われるケースも存在する。

- 増大する攻撃規模

攻撃の規模や被害も年々大きくなっている。2012 年には、米国の複数の大手銀行が断続的に大規模な DDoS 攻撃を受け、数時間に渡りサービスを中断する事態に発展している。また、2013 年には、同じ米国で 100 Gbps のトラフィックによる攻撃が、絶え間なく 9 時間にも渡って継続される史上最大の DDoS 攻撃が観測された。

サービス妨害による影響は、我々の生活にも影響を与える事態になってきている。また、EC サイトが事業基盤となっている企業においては、事業存続の危機に立たされる可能性がある。

＜攻撃の手口＞

代表的な攻撃手口として、以下の 3 つが挙げられる。

- DDoS

ウイルスに感染したパソコンが、ボットネットと呼ばれる攻撃者に乗っ取られたコンピューター群を構成する。攻撃者は、定期的に

ボットネットに攻撃指令を出し、集中的に特定のサーバーへのアクセスを発生させることで、標的組織のネットワーク帯域を逼迫し麻痺状態にする。今日では、ボットネットは裏社会のビジネスとして存在しており、妨害攻撃の請負や、ボットネットのレンタルを行うグループの存在が確認されている。

- データ破壊

パソコンに感染したウイルスが、パソコンを起動できなくしたり、パソコンに保存されているデータを削除してしまう。このようなデータ破壊を行うことで、サービスの継続を妨害する手法がある。

- メールボム

大量にメールを送りつけることでメールボックスをパンクさせる。メールは不特定多数から届くものであり、日常的に利用するため、簡単にブロックすることが難しい。

＜事例と傾向＞

- 韓国で発生したサイバー攻撃[I]

2013 年 3 月 20 日、韓国の複数の銀行および放送企業において、マルウェアの攻撃により数万台のパソコンが突如停止し、起動できない事態が発生した。被害を受けた農協銀行では ATM の約半数である約 4,500 台が影響を受け、復旧までの数日間に渡り銀行業務が混乱した。また、被害を受けた複数の放送企業では、報道番組の制作に影響が出た。マルウェアは、ソフトウェア資産管理システムを介して拡散し、特定の時間にデータを破壊するように仕込まれていた。

- DNS オープンリゾルバ[II]

オープンリゾルバとは、外部の不特定の IP アドレスからの再帰的な問い合わせを許可しているDNS サーバーである。2013 年は、オープンリゾルバ状態の DNS を悪用して、大量の応答パケットを送りつける攻撃が発生した。管理者は、ネットワーク機器がオープンリゾルバになっていないか確認し、適切な設定での運用を行う必要がある。また、時刻同期サービス NTP の設定不備を狙った攻撃に対しても対策が求められている。

- お問合せフォームの悪用[III]

2013 年、複数の脱原発を掲げる市民団体のメールアドレスを登録アドレスとして、メールマガジン等の申し込みフォームに申し込みがあり、数千から数万の登録完了メールが脱原発団体に送りつけられた。

＜対策/対応＞

- セキュアなサーバーの設定
- 通信制御
- ウイルス対策ソフトの導入
- OS・ソフトウェアの更新

DDoS 攻撃の通信に特徴があれば、特定の通信をネットワーク機器等でブロックする。また、システムの重要度によってはシステムを冗長化構成にする。更に、ウイルス対策ソフトの導入やセキュリティアップデートの適用を行い、ウイルス感染を防止することも重要である。

参考資料

I. 北のサイバー攻撃？韓国放送局や銀行に一斉障害
http://www.yomiuri.co.jp/net/news1/world/20130320-OYT1T00480.htm

II. DNS の再帰的な問い合わせを使った DDoS 攻撃に関する注意喚起
https://www.jpcert.or.jp/at/2013/at130022.html

III. 各地の反原発団体に大量メール　サイバー攻撃の可能性も
http://www.asahi.com/special/news/articles/SEB201309190046.html

その他 10 大脅威候補

ここでは、2014 年版 10 大脅威には選出されなかったものの、2013 年に社会へのインパクトを与えた脅威として、10 大脅威候補に挙がった脅威を簡単に説明する。

11位.　内部犯行・ルール違反

内部統制・セキュリティマネジメント

悪意を持つ従業員や元従業員によって、業務を妨害する問題が度々発生している。また、第三者に内部情報を販売したり、私的に情報を利用したりする事例が多く発生している。悪意を持つ内部の人間は、高度な攻撃手法を用いずとも、広範囲に影響を与えることができる。職務権限の分離やアクセス制限等を適切に行うことが、企業の内部統制における一つの課題となっている。

- 元上司のID使って不正アクセス、大阪市職員を懲戒免職　税証明書偽造も
  http://sankei.jp.msn.com/affairs/news/131031/crm13103113550008-n1.htm

12位.　オンラインゲームの仮想アイテムの窃取

インターネットモラル

近年、スマートフォンの普及を背景に、オンラインゲームの普及が拡大している。オンラインゲームの仮想通貨や仮想アイテムの窃取を目的とした不正ログインの被害が増加している。2013 年は、中高生が書類送検されるケースが増加し、不正ログインを行う者の低年齢化が問題となった。

- 不正アクセス:容疑で高1を書類送検--県警など　／岐阜
  http://mainichi.jp/area/gifu/news/m20131114ddlk21040034000c.html
- 不正アクセス、被疑者の4割が10代青少年
  http://www.yomiuri.co.jp/net/security/goshinjyutsu/20130412-OYT8T00917.htm

13位.　SNS アカウントの成りすまし・デマ

インターネット詐欺

SNS 上で有名人や有名企業のアカウントを名乗り、広告や出会い系サイト等、特定のサイトに誘導する事例が報告されている。被害者または被害企業は、対応コストの発生や風評被害により金銭的な損失を受けることになる。また、米国では報道機関のアカウントが乗っ取られて偽のテロ情報が伝えられ株価の下落が発生した事例も発生した。

- 「ディズニー公式」名乗り広告サイトへ誘導　偽Twitterアカウントに注意呼びかけ
  http://nlab.itmedia.co.jp/nl/articles/1310/29/news116.html
- AP通信のツイッター乗っ取り　偽情報で株乱高下
  http://www.nikkei.com/article/DGXNASGM2402U_U3A420C1EB1000/

14位.　インターネット上の誹謗・中傷・いじめ

インターネットモラル

インターネットの匿名性を悪用して、掲示板や SNS 等に誹謗・中傷を掲載される事例が継続的に発生している。また掲示板や SNS を使用したいじめも社会的な問題となっている。狙われた個人は、精神的ダメージや信頼損失等の被害を受ける。

- 悪い人間と思い込む…ネット掲示板に「殺す」と書き込み　容疑の男逮捕／狭山署
  http://www.saitama-np.co.jp/news/2013/12/04/07.html
- 2ちゃんで弁護士殺害予告　大分の高校生を書類送検　「恨みないけど注目されて…」
  http://sankei.jp.msn.com/affairs/news/131209/crm13120913190003-n1.htm

15位.　無線 LAN の不正利用・盗聴

ウイルス・ハッキング
サイバー攻撃

パスワードのかかっていない無線 LAN アクセスポイントに接続され、犯行予告等犯罪に悪用される事例が深刻な問題となっている。ネットワークに接続された後、ネットワーク内の端末が攻撃される可能性もある。また、セキュリティの弱い無線 LAN には、通信を盗聴される危険性も存在する。盗聴によって、機密情報の漏えいやアカウント認証情報の窃取等の影響を及ぼす可能性がある。

- 企業等が安心して 無線LANを導入・運用するために
  http://www.soumu.go.jp/main_content/000199320.pdf
- 2013年12月の呼びかけ「“ただ乗り”を するなさせるな 無線LAN 」
  http://www.ipa.go.jp/security/txt/2013/12outline.html

16位.　不正請求詐欺

インターネット詐欺

アダルトサイトや出会い系サイトの利用料を不正に請求されるワンクリック詐欺の被害が後を絶たない。古くは郵送によって行われていた不正請求は、インターネットの普及によりメールやウェブブラウザやスマートフォンアプリ等、IT を使用したものが主流になっていると言える。2013 年は、スマートフォンアプリを介して漏洩した個人情報宛への不正請求が拡大した。

- ワンクリック詐欺アプリ、Google Playで氾濫状態に
  http://www.itmedia.co.jp/enterprise/articles/1304/04/news089.html
- なぜ電話番号がわかったの？無料アプリのインストールで50万円請求！
  http://www.kokusen.go.jp/mimamori/kmj_mailmag/kmj-support69.html

17位.　自然災害・オペレーションミス

内部統制・セキュリティ
マネジメント

2011 年は東日本大震災よる被害が発生した。2012 年はレンタルサーバーつまりクラウド上で発生した事故による被害が浮き彫りになった。2013 年以降も不慮の事故や想定外の事件によるトラブルが後を絶たない。ITシステムには故障やバックアップデータの消失等に備えたBCP（事業継続計画）が求められている。

- GMOクラウドで障害、原因は台湾DCでの火災
  http://itpro.nikkeibp.co.jp/article/NEWS/20130225/458681/
- KDDIがauの2日半にわたるメール障害を謝罪--設備や人的ミスが原因
  http://japan.cnet.com/news/business/35031332/

このページは空白です。

3章. 注目すべき脅威や懸念

本章では、インターネット環境、ライフスタイルの変化に着目し、社会に影響を与えているまたは与えつつある、注目すべき脅威や懸念事項について解説する。

表 3：注目すべき脅威や懸念

番号	タイトル
1	ネットワーク対応機器の増加 ～サーバーやパソコン以外の機器も攻撃対象に～
2	エンドポイントセキュリティの重要性 ～最新のソフトウェアを使用することがセキュリティ対策の近道～
3	インターネット利用の低年齢化に伴う問題 ～未成年者がネット犯罪の加害者・被害者になってしまう～

3.1. ネットワーク対応機器の増加

～サーバーやパソコン以外の機器も攻撃対象に～

昨今、職場や家庭において、インターネットに接続できる機器が増加しており、リモートからメンテナンスが行える等の便利な機能を提供している。一方で、これらの機器の不適切な設定により、情報漏えいや機器が乗っ取られる等の被害が発生しており、新たな脅威となっている。

＜インターネット接続機器の増加＞

近年、ウェブサーバーを内蔵し、ウェブインタフェースにより設定・管理できる、下記のようなオフィス機器や家電機器が増えている。

（オフィス機器）

- 複合機/プリンター
- ウェブカメラ
- NAS（Network Attached Storage）
- ルーター

（家電製品）

- デジタル液晶テレビ
- ブルーレイディスクレコーダー
- ゲーム機

ユーザーは、ブラウザ経由でこれらの機器にアクセスし設定を変更したり、内部の情報を確認したりすることが出来る。また、インターネットに接続することで、リモートからの情報閲覧等に利用でき、家電製品であれば、外出先からの録画設定等も行える。

- 不正アクセスの脅威が迫る

しかし、ブラウザ経由でインターネット越しにアクセスできる環境は、攻撃者にとって絶好の攻撃機会でもある。即ち、攻撃者がインターネット越しに機器にアクセスし、不正操作が行えることを意味するからだ。これらの機器の本人確認には、ID/パスワードによる認証方式が用いられるのが一般的であり、常に不正アクセスの脅威に晒されている。

ウェブカメラが設置されているケースを考えると、オフィス内部の様子が筒抜けになり、攻撃者に常時監視されている状態になる。

複合機/プリンターやNASのケースでは、外部から印刷データやストレージ上のファイルが盗み見られる状態となってしまう。

更に、オフィス機器自体が攻撃の踏み台となり、内部への侵入を招くことも考えられる。

＜実際に起こった事例＞

実際に、家電製品やオフィス機器に関するセキュリティ事故が報告されている。

- ベビーモニターのハッキング[I]

2013 年に米国でベビーモニターがハッキングされ、外部にいる攻撃者が寝ている赤ん坊に罵声を浴びせる事件が起きた。ベビーモニターとは、赤ん坊の様子を音や映像等で確認できるモニター装置であり、ウェブインタフェースで視聴できるものが多い。通常は、インターネットに公開せず、内部ネットワークで接続し、別の部屋から赤ん坊の様子を確認する目的で使われる。しかし、インターネットからアクセスできるネットワーク環境に設置することで、この様な不正アクセスを受ける危険性がある。

- 複合機の情報が閲覧可能な状態に[II]

2013 年 11 月、一部の学術関係機関に設置されている複合機が、インターネットからアクセス可能な状態で設置されていることを、報道機関が指摘し、複合機メーカーや業界団体がユーザーへの注意喚起を行った。報道によるとファックスで受信した文書やスキャナーでスキャンされた文書の多くには個人情報が含まれており、その文書に誰でもアクセスできる状態であった。

＜ユーザー側の認識不足が要因＞

これらの問題を引き起こす要因の根底には、ユーザー側で脅威を十分に認識できていないことや、そもそもインターネットに公開される機器仕様に気づいていないことが挙げられる。また、オフィス機器の場合、通常の IT 機器と異なり、システム管理部門で管理されず、各部門や総務系の部門の管理下となるケースが多い。その為、ネットワーク管理部門と上手く調整が図られず、セキュリティ対策が疎かになりがちである。

＜安全に利用する為の注意点＞

インターネットに接続する機器を安全に利用する為には、機器に付属している説明書をよく読み、適切な設定を施すことが重要である。その上で、下記のような対策を施し、不正アクセスのリスクを低減することが重要である。

（ネットワークでの対策）

- 必要性がない場合には、機器をインターネットに接続しない。
- インターネットに接続する場合は、必ずファイアウォールを経由させ、適切な通信に限定する。家庭用機器は、ブロードバンドルータの内側に設置する。
- インターネットに接続する機器と内部ネットワーク用の機器を分け、機器へのアクセスも制限する。

（機器での対策）

- 機器の管理者パスワードを出荷時のもの（デフォルトパスワード）から変更する。
- アクセス制御機能を有効にし、アクセス時に ID/パスワード等の認証を求める。

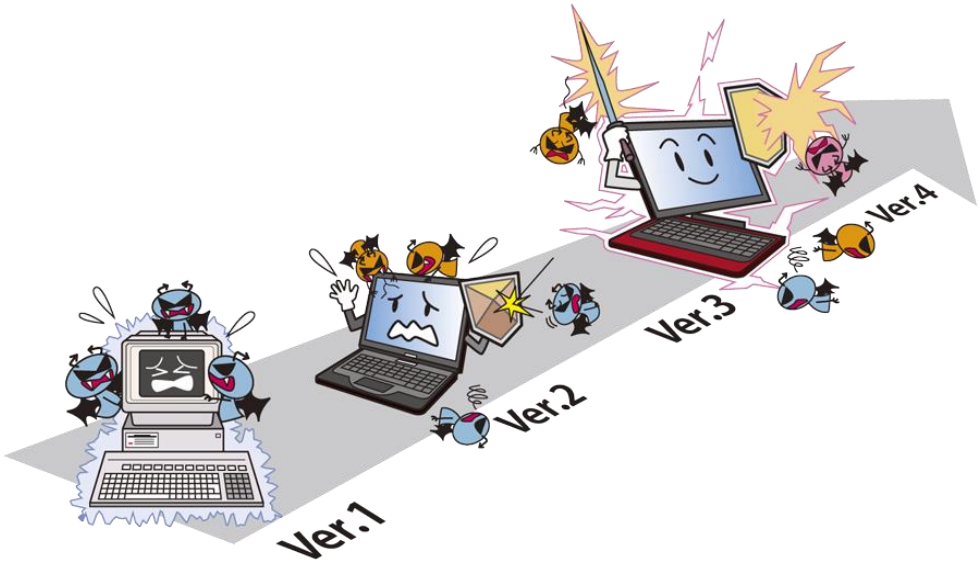
参考資料

I. 子ども部屋から不審な声、男がカメラ乗っ取り罵言　米
http://www.cnn.co.jp/tech/35036051.html

II. 一般社団法人 ビジネス機械･情報システム産業協会: 複合機のセキュリティーに関する報道について
http://www.jbmia.or.jp/whatsnew/detail.php?id=294

3.2. エンドポイントセキュリティの重要性

～最新のソフトウェアを使用することがセキュリティ対策の近道～



近年の攻撃は、エンドユーザーが使用するパソコン等のエンドポイントを狙ったものが主流となっている。OS やその上位で動作するソフトウェアは、顕在化したセキュリティの脅威に合わせて、順次セキュリティ機能が強化されており、最新バージョンを使用することが重要である。

＜境界防御の限界＞

境界防御（境界セキュリティ）の概念は、軍事に端を発した用語であり、攻撃者と防御する対象の間に障壁を設けることで、情報資産を守るセキュリティの考え方である。今日の情報システムの基本も、インターネットとイントラネットの間にファイアウォールを設置し、更にイントラネット内部にネットワーク機器を設置して、重要な資産を守るように作られている。この境界防御の概念は、一見作りの美しいセキュリティモデルに写るかもしれないが、既に限界が叫ばれている。近年の攻撃はメールやウェブと言ったオフィスワークで必須となる通信路を使い、障壁を掻い潜り、直接パソコン等のエンドポイントに対し攻撃を行ってくる。メールやウェブ等の通信は、オフィスワークの性質上、遮断することは難しく、エンドポイントのセキュリティ対策が重要になってくる。

＜狙われるソフトウェア＞

エンドポイントを狙った攻撃は、Oracle Java（ JRE ）、Adobe Acrobat/Adobe Reader、Adobe Flash Player、Microsoft Office 等の脆弱性が悪用されるケースが多い。これらのソフトウェアが悪用される背景には、ユーザー数が多いことや、ファイルやウェブサイトを閲覧するといった操作が、パソコンを利用する上で欠かせない操作であるため、罠にはめ易い点が挙げられる。

＜新しいソフトウェアほどセキュリティ機能が強固＞

エンドポイントを狙った攻撃に対して、OS やアプリケーションベンダーも、脅威の変化と共にセキュリティ機能を強化している。セキュリテ

ィ機能は、近年の攻撃手法や既存のソフトウェアのセキュリティ上の弱点を分析した上で、ソフトウェアに反映している。

例えば、Acrobat/Adobe Reader では、バージョン XI からサンドボックス[3]技術を用いて、悪意あるスクリプトの実行を限定的なものとし、システムへの影響を阻止している。この機能により、攻撃者は Acrobat/Adobe Reader に悪意あるスクリプトを埋め込みウイルスに感染させることが、急激に難しくなった。

また、Windows OS においても同様に、段階的にセキュリティ機能が強化されており、OS のバージョンによってセキュリティ強度に差異がある。Windows Vista 以降に ASLR[4]、SEHOP といった不正プログラムの実行を防止する機能が設けられ、ウイルス感染のリスクが低減している。マイクロソフトが公表した Windows OS 別のウイルス感染率で比較すると、Windows XP では 11.3%の感染率であるのに対し、Windows 7(32bit)では 4.8%に減少している。

ソフトウェアのバージョンアップを行うことは、これまで通用していた既知の攻撃手法が防御できることを意味する。当然ながら、新しいソフトウェアに更新しなくても、セキュリティ対策ソフト等で脅威を低減する事は可能である。ただ、新しいバージョンを使い、定期的にソフトウェアを更新することは、セキュリティ対策の第一歩として容易に脅威が低減できることを認識しておくことも重要である。

＜Windows XP のサポート終了＞

10 年以上の長きに渡り主力 OS として使われてきたWindows XP が 2014 年 4 月 9 日(日本時間)をもってサポートを終了する。サポート終了に伴う影響は、セキュリティパッチの提供の停止に留まらず、下記のような事項も連鎖する。

- アプリケーションの順次サポートの終了

攻撃に悪用されやすい文書ソフトやブラウザ、ウイルス対策ソフト等のソフトウェアについても順次サポートを終了することが想定される。サポート終了後も使い続ければ、パソコンのセキュリティレベルが段階的に低下する。

- 保守サービスの終了

修理等のパソコンのヘルプデスク、メンテナンスサポートも段階的に Windows XP をサポート対象外とすることが想定される。その為、パソコン故障時にデータを消失したり、業務が中断してしまうことが考えられる。

上記のようなリスクを回避する為にも、サポートが継続している後継または代替 OS に移行することが望ましい。

参考資料

I. Windows XP を 2014 年 4 月のサポート終了後も使い続けることのリスク
http://blogs.technet.com/b/jpsecurity/archive/2013/10/31/3607203.aspx

[3]外部から受け取ったプログラムを保護された領域で動作させることによってシステムが不正に操作されるのを防ぐセキュリティモデルのこと

[4]メモリ領域に格納するデータのアドレスをランダム化することで、攻撃者により不正な命令を実行させない為の技術

3.3. インターネット利用の低年齢化に伴う問題

～未成年者がネット犯罪の加害者・被害者になってしまう～

インターネット利用年齢の低下に伴い、未成年者が犯罪に巻き込まれるケースが散見されている。また、未成年者が IT 犯罪により逮捕・補導されるケースも続発しており、未成年者に対するセキュリティ教育の重要性が増している。

＜IT ユーザーの低年齢化＞

小学生の年齢から携帯電話・スマートフォンを使用する機会が増えてきている。オンラインゲームや学習教材、コミュニケーションツール等のコンテンツも充実しており、年々インターネットを利用し始める年齢が低下している。

＜インターネットのトラブルや犯罪＞

インターネットは、利便性が高い反面、偽名でも利用できるため犯罪への悪用が容易である。ここ数年で、未成年者が「出会い系サイト」に絡んだトラブルに巻き込まれるケースが増えている。警察庁発表「平成 25 年上半期の出会い系サイト等に起因する事犯の現状と対策について」によると、出会い系サイト経由での被害者は、2013 年上半期だけで 74 名に上る。また、驚くべきことに、被害者の大半は未成年である。

また、出会い系サイトだけではなく、無料通話アプリ「LINE」を通じて、他人に個人情報を教えてしまい、犯罪に巻き込まれる事例も増えている。

残念ながらインターネットを使う人は善良な人ばかりではなく、犯罪に悪用しようと考えている人も紛れている。「個人情報を教えない」「安易に見知らぬ人と会わない」ことを、若年層から教えていく必要がある。

＜保護者への高額請求＞

若年層からインターネットにのめり込む背景の一つにオンラインゲームの浸透が挙げられる。オンラインゲームは、インターネット上で複数人が参加できる対戦形式のものから、バーチャルな世界で生活するものまで多種多様に存在する。オンラインゲームでは、ゲーム内で使用するアイテムを販売している。近年、保護者の知らないうちに子供がアイテムを購入し、契約者である保護者に高額の請求が行われる事例が増えている。

国民生活センターは、オンラインゲームによる年間トラブルの相談件数が、2013 年 11 月

末時点で 3,000 件を超えていると公表している。相談の中には、「高校２年生の息子が、約 60 万円分のアイテムを購入していた」、「同居中の孫がクレジットカードを勝手に使い、オンラインゲーム会社から 20 万円弱の高額な請求が届いた」等の声が寄せられている。オンラインゲームには有料アイテム無しには楽しめないものがあり、ゲームに熱中するあまり、家族・身内に損害を与えてしまう事例が散見される。保護者は、オンラインゲームの仕組みをよく理解し、ゲーム利用について日頃から子どもとよく話し合っておくことが重要となる。

＜IT 犯罪の低年齢化＞

未成年者が IT 犯罪に巻き込まれる一方で、未成年者が犯罪の加害者になる事件も増えている。

- オンラインゲーム　不正アクセス

オンラインゲームへの熱中や好奇心によって、不正アクセスする行為が散見されている。最も多いのが、他人の ID/パスワードを使って不正ログインを試みるケースである。

「同級生のキャラクターやアイテムが見たかった」として、同級生の ID/パスワードを使って不正アクセスし、12 歳の児童が補導された事件も発生している。

また、他人のパスワードを使った不正アクセスだけでなく、フィッシングサイト構築やウイルス作成等の IT の専門知識を有した行為も確認されている。善悪の区別のつきにくい年頃なので、日頃からITリテラシ教育を徹底していかなければならない。

- 不適切な情報をインターネットに投稿

2 章で紹介したようにインターネット上に不適切な投稿を行ったことで未成年者が逮捕・補導される事例も目立ってきた。

特に深刻なのが、掲示板に他人の悪口を書き込む、他人を誹謗した写真を投稿する等の“いじめ”的な行為である。特筆すべきは、これらの行為に小学生も含まれており、小学生が補導される事件も発生している。また、高校生の例では、投稿された 18 歳男子が自殺するという、痛ましい事件も起こっている。

更に、いじめに限らず、爆破予告、殺害予告を掲示板に書き込んだことで、中高生が逮捕される事件も起きている。

犯行の形態や動機は様々であるが、いずれも逮捕・補導されて初めて、自身の行為が犯罪であると認識するケースが多い。また、インターネットは匿名で利用できるものの、ログに残された情報によっては本人を特定できてしまう。これを利用者が認識せずに、軽率な投稿をするケースも見られる。

幼少期から適切なインターネット利用を教えていくことが社会全体に求められている。また、サービスや機器のペアレンタルコントロール機能を活用することも有効的な対策となる。

参考資料

I. 平成25年上半期の出会い系サイト等に起因する事犯の現状と対策について
http://www.npa.go.jp/cyber/statics/h25/pdf02-1.pdf

II. 国民生活センター：オンラインゲーム
http://www.kokusen.go.jp/soudan_topics/data/game.html

III. IPA：小学生／中高生向け教材
http://www.ipa.go.jp/security/keihatsu/videos/

付録:2013 年　セキュリティ事件・ニュース

1月7日　三菱東京UFJ銀行、クレジットカード情報を窃取しようとする電子メールに注意喚起

2月10日　パソコン遠隔操作事件　容疑者逮捕
2月20日　トレンドマイクロ、「LINE」を悪用したサクラサイト商法などの手口に対して注意喚起

3月20日　韓国の数万台のパソコンがサイバーテロにより停止、複数の企業に影響

4月19日　インターネット選挙活動の全面解禁

5月23日　Yahoo! Japanが不正アクセスによるユーザー情報148.6万件の漏えいを公表
5月24日　警察庁、Webサイト改ざんの急増に対して注意喚起
6月5日　スノーデン氏が米NSAによる諜報活動について暴露

7月10日　「Googleグループ」で省庁内部情報が外部閲覧可能、報道で明らかに

7月25日　JR東日本がSuica履歴情報の社外提供ついて説明不足であったと謝罪
8月1日　多発するアカウントリスト型ハッキングに対して注意喚起（IPA）

8月29日　ロリポップでWeb改ざん、8,438件でデータ改ざんや不正ファイル設置

9月19日　日本を狙った高度な標的型ゼロデイ攻撃による被害を確認

10月2日　退職した契約社員の個人用PCがウイルス感染、顧客情報が流出
10月3日　日米安全保障協議委員会（「2＋2」）がサイバー空間における協力を発表

11月5日　複合機からの情報漏えい報道を受けて各メーカーが注意喚起

12月12日　インターネットバンキング不正送金の被害年間11.8億円で過去最大に（警察庁）
12月17日　国家安全保障戦略が閣議決定。サイバー領域が防護対象に

このページは空白です。

10 大脅威執筆者会構成メンバー

10 大脅威執筆者会

氏名	所属	氏名	所属
石田 淳一	(株)アールジェイ	林 薫	(株)シマンテック
高橋 潤哉	(株)イード	山内 正	(株)シマンテック
佐藤 直之	(株)イノベーションプラス	神薗 雅紀	(株)セキュアブレイン
加藤 雅彦	(株)インターネットイニシアティブ	星澤 裕二	(株)セキュアブレイン
齋藤 衛	(株)インターネットイニシアティブ	青谷 征夫	ソースネクスト(株)
高橋 康敏	(株)インターネットイニシアティブ	唐沢 勇輔	ソースネクスト(株)
梨和 久雄	(株)インターネットイニシアティブ	澤永 敏郎	ソースネクスト(株)
三輪 信雄	S&J コンサルティング(株)	百瀬 昌幸	(財)地方自治情報センター(LASDEC)
石川 朝久	NRI セキュアテクノロジーズ(株)	杉山 俊春	(株)ディー・エヌ・エー
大塚 淳平	NRI セキュアテクノロジーズ(株)	岩井 博樹	デロイト トーマツ リスクサービス(株)
小林 克巳	NRI セキュアテクノロジーズ(株)	相馬 基邦	デロイト トーマツ リスクサービス(株)
正木 健介	NRI セキュアテクノロジーズ(株)	桑原 和也	デジタルアーツ(株)
中西 克彦	NEC ネクサソリューションズ(株)	大浪 大介	(株)東芝
杉浦 芳樹	NTT-CERT	田岡 聡	(株)東芝
住本 順一	NTT-CERT	長尾 修一	(株)東芝
種茂 文之	NTT-CERT	吉松 健三	(株)東芝
井上 克至	(株)NTT データ	小島 健司	東芝ソリューション(株)
入宮 貞一	(株)NTT データ	小屋 晋吾	トレンドマイクロ(株)
西尾 秀一	(株)NTT データ	大塚 祥央	内閣官房情報セキュリティセンター
池田 和生	NTTDATA-CERT	恩賀 一	内閣官房情報セキュリティセンター
林 健一	NTTDATA-CERT	佐々木 勇也	内閣官房情報セキュリティセンター
宮本 久仁男	NTTDATA-CERT	須川 賢洋	新潟大学
やすだ なお	NPO 日本ネットワークセキュリティ協会	田中 修司	日揮(株)
	(JNSA)	井上 博文	日本アイ・ビー・エム(株)
前田 典彦	(株)Kaspersky Labs Japan	徳田 敏文	日本アイ・ビー・エム(株)
山崎 英人	カルチュア・コンビニエンス・クラブ(株)	守屋 英一	日本アイ・ビー・エム(株)
秋山 卓司	クロストラスト(株)	宇都宮 和顕	日本電気(株)
小熊 慶一郎	(株)KBIZ	谷川 哲司	日本電気(株)
鈴木 啓紹	(社)コンピュータソフトウェア協会(CSAJ)	榎本 司	日本ヒューレット・パッカード(株)
野渡 志浩	(株)サイバーエージェント	西垣 直美	日本ヒューレット・パッカード(株)
名和 利男	(株)サイバーディフェンス研究所	大村 友和	(株)ネクストジェン
福森 大喜	(株)サイバーディフェンス研究所	金 明寛	(株)ネクストジェン
高木 浩光	(独)産業技術総合研究所	杉岡 弘毅	(株)ネクストジェン
高橋 紀子	(社)JPCERT コーディネーションセンター	高橋 直人	(株)ネクストジェン
	(JPCERT/CC)	圓山 大介	(株)ネクストジェン
古田 洋久	(社)JPCERT コーディネーションセンター	山下 潤一	ネットエージェント(株)
	(JPCERT/CC)	徳丸 浩	HASH コンサルティング(株)
宮﨑 清隆	(社)JPCERT コーディネーションセンター	水越 一郎	東日本電信電話(株)
	(JPCERT/CC)	太田 良典	(株)ビジネス・アーキテクツ
宮地 利雄	(社)JPCERT コーディネーションセンター	寺田 真敏	Hitachi Incident Response Team
	(JPCERT/CC)	藤原 将志	Hitachi Incident Response Team

氏名	所属	氏名	所属
丹京 真一	(株)日立システムズ	志田 智	(株)ユビテック
本川 祐治	(株)日立システムズ	福本 佳成	楽天(株)
梅木 久志	(株)日立製作所	伊藤 耕介	(株)ラック
鵜飼 裕司	(株)FFRI	川口 洋	(株)ラック
金居 良治	(株)FFRI	長野 晋一	(株)ラック
村上 純一	(株)FFRI	石川 芳浩	(株)ラック
国部 博行	富士通(株)	山崎 圭吾	(株)ラック
望月 大光	富士通(株)	若居 和直	(株)ラック
森 玄理	富士通(株)	山梨 晃	ルネサスエレクトロニクス(株)
金谷 延幸	(株)富士通研究所	伊藤 毅志	(独)情報処理推進機構(IPA)
綿口 吉郎	(株)富士通研究所	町田 昇	(独)情報処理推進機構(IPA)
岡谷 貢	(株)富士通システム総合研究所	金野 千里	(独)情報処理推進機構(IPA)
高橋 正和	マイクロソフト(株)	栗栖 正典	(独)情報処理推進機構(IPA)
寺田 健	三井物産セキュアディレクション(株)	益子 るみ子	(独)情報処理推進機構(IPA)
川口 修司	(株)三菱総合研究所	花村 憲一	(独)情報処理推進機構(IPA)
村瀬 一郎	(株)三菱総合研究所	加賀谷 伸一郎	(独)情報処理推進機構(IPA)
村野 正泰	(株)三菱総合研究所	渡辺 貴仁	(独)情報処理推進機構(IPA)
日高 和夫	(株)ユービーセキュア	大森 雅司	(独)情報処理推進機構(IPA)
松浦 孝征	(株)ユービーセキュア	棚町 範子	(独)情報処理推進機構(IPA)
冨張 伸宏	(株)ユービーセキュア	中西 基裕	(独)情報処理推進機構(IPA)

著作・制作　　独立行政法人情報処理推進機構（IPA）

編集責任　　大森 雅司

イラスト制作　　株式会社 日立ドキュメントソリューションズ

執筆協力者　　10 大脅威執筆者会

執筆者　　大森 雅司　 中西 基裕　 棚町 範子

2014 年版　情報セキュリティ

10 大脅威

～複雑化する情報セキュリティ　あなたが直面しているのは？～

2014 年 3 月 17 日　　第 1 刷発行

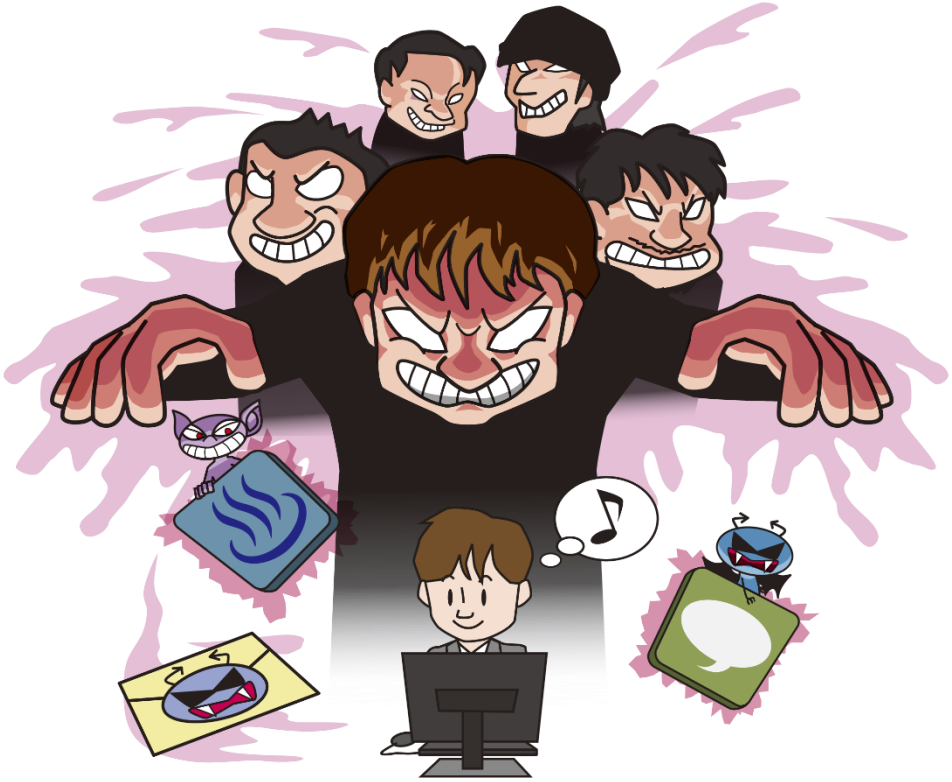
［事務局・発行］　　独立行政法人情報処理推進機構

〒113-6591

東京都文京区本駒込二丁目 28 番 8 号

文京グリーンコートセンターオフィス 16 階

http://www.ipa.go.jp/



IPA 独立行政法人**情報処理推進機構**
セキュリティセンター
〒113-6591
東京都文京区本駒込二丁目 28 番 8 号
文京グリーンコートセンターオフィス
TEL：03-5978-7527　FAX：03-5978-7518
http://www.ipa.go.jp/security/