2013 年版

10 大脅威

～身近に忍び寄る脅威～

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

2013 年 3 月

本書は、以下の URL からダウンロードできます。

「2013 年版 10 大脅威　身近に忍び寄る脅威」

http://www.ipa.go.jp/security/vuln/10threats2013.html

目次

はじめに

本資料は、情報セキュリティ分野の研究者、企業などの実務担当者など 117 名から構成される「10 大脅威執筆者会」メンバーの知見や意見を集めながら、近年の情報システムを取り巻く脅威について解説したものである。2012 年は、政府機関や宇宙航空産業へのサイバー攻撃、遠隔操作ウイルス事件などの様々なセキュリティ事故や事件がメディアで取上げられ、社会へ大きなインパクトを与えた。また、金銭窃取を目的としたフィッシング詐欺、スマートデバイスを狙った攻撃の横行など、個人ユーザーにおいても看過できない脅威が迫っている。企業・組織や個人ユーザーにおいては、自身に関連する脅威を十分に認識し、対策を講じることが重要である。本資料が、その一助となれば幸いである。

以下、本資料のサマリーとなる。

1 章：情報セキュリティの変遷

1 章では、情報セキュリティの変遷として、情報セキュリティが定着してきた 2001 年から 2012 年までのセキュリティの変化を振り返っている。近年の IT 環境や攻撃意図の変化として下記の点が挙げられる。

- インターネットへの依存度の増大

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、我々の生活においてインターネットが深く浸透しており、経済活動や社会活動を行う上で必要不可欠なものとなっている。一方で、インターネットに接続しているために、攻撃者から狙われやすく、攻撃を受けた際の被害も大きくなっている。

- 抗議や諜報目的の攻撃の顕在化

2008 年頃までは、金銭を目的にした攻撃が主流であったが、2010 年あたりから更に異なる二つの攻撃が国内外の報道等により顕在化し、攻撃の意図性が明らかになってきた。

一つは、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挙げられる。

二つ目は、政府機関や特定の組織の情報を盗み出す諜報活動を意図した攻撃の広がりが挙げられる。日本国内でも 2011 年に政府機関や大手重要インフラ事業者が狙われたことで大きな注目を集めた。

- 国家を巻き込んだ大規模な攻撃

攻撃の規模が企業・組織をターゲットにしたものから国家を巻き込んだ大規模なものが出現してきた。米国防総省では「サイバー空間」を陸・海・空・宇宙空間に次ぐ「第五の戦場」であると定義しているように、サイバー攻撃が国際情勢や安全保障に関わる問題として扱われ、関係分野が拡大している。

- 官民が連携したプロジェクトの推進

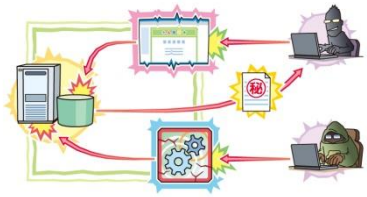
企業・組織が単独でセキュリティ対策を講じることが困難な状況になっている。国内では官民が連携した様々なプロジェクトが発足してきている。また、近年の巧妙化した攻撃に対処するためのスキルを持ったエンジニアが必要とされており、人材育成を主眼とした政策にも力が注がれている。

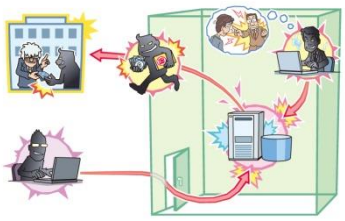
２章： 2013 年版 10 大脅威一覧

10 大脅威執筆者会メンバーの投票により選んだ 2013 年版の 10 大脅威の順位と概要は下記になる。下記表では、脅威を、外部的な要因により発生する脅威と、内部から発生する脅威に分類している。

【凡例】 :外部からの攻撃による脅威 :組織内部の管理に起因する脅威

1 位:クライアントソフトの脆弱性を突いた攻撃		
	クライアントソフトの脆弱性を悪用されることにより、ウイルスに感染したり、システム内の情報が窃取されるなどの被害の可能性がある。ユーザーにおいては、クライアントソフトを最新に保つ対応が求められる。	 個人ユーザーへの脅威  企業/組織への脅威
2 位:標的型諜報攻撃の脅威		
	2011 年に続き、2012 年も政府機関や宇宙航空産業への攻撃が報道され、機密として扱われている政府関連情報や特殊技術情報の流出が疑われている。わが国の政策会議でも、この問題が取上げられるなど、国益にまで影響する問題になっている。	 企業/組織への脅威  国家への脅威
3 位:スマートデバイスを狙った悪意あるアプリの横行		
	個人情報を収集する手口がより巧妙化している。近年、加速的に普及しているスマートデバイス（スマートフォンやタブレット）ユーザーをターゲットに、魅力的な機能を持っていると見せかけた不正アプリが電話帳等の情報を窃取する被害が増加している。	 個人ユーザーへの脅威  企業/組織への脅威
4位:ウイルスを使った遠隔操作		
	ウイルスに感染した PC は、これまでもスパムの送信や DDoS 攻撃のために悪用されてきた。2012 年、PC に感染したウイルスを経由して、悪意ある第三者が掲示板に脅迫文を書きこむとともに、当該ウイルスに感染した PC の所有者が誤認逮捕される事件が発生し、大きな話題となった。	 個人ユーザーへの脅威  企業/組織への脅威個

5 位：金銭窃取を目的としたウイルスの横行		
	2011 年頃より海外のインターネットバンキングで、ウイルスにより認証情報が窃取され、金銭被害に発展する事件が報告されはじめた。2012 年からは国内のインターネットバンキングでも同様の手口による被害が確認されだしている。	 個人ユーザーへの脅威
6 位：予期せぬ業務停止		
	システムのクラウド化が進む中、2012 年は、レンタルサーバー企業において人為的ミスによる大規模障害が発生した。東日本大震災によって、自然災害が原因となりシステムが停止するリスクが浮き彫りとなったように、不測の事態に備える必要性が組織に求められる。	 企業/組織への脅威
7 位：ウェブサイトを狙った攻撃		
	ウェブサイトを狙った攻撃は、旧来から認識されている脅威であるが、残念ながら被害が後を絶たない。ウェブサイト内の個人情報窃取や、ウェブサイトの改ざんによるウイルス配布など、組織や個人ユーザーに影響を及ぼす脅威である。	 個人ユーザーへの脅威  企業/組織への脅威
8 位：パスワード流出の脅威		
	オンラインサービスの増加に伴い、ユーザーが複数のパスワードを管理する必要が生じている。その結果、同一の ID/パスワードを使い回すユーザーが多くなり、一つのウェブサイトでパスワードが漏えいすることで、複数のウェブサイトで成りすましの被害に遭ってしまう。	 個人ユーザーへの脅威  企業/組織への脅威

9 位:内部犯行		
	内部の人間による故意の情報漏えいや不正操作による被害が報告されている。正当に権限を有したユーザーによる犯行であるため、防止が難しく、被害も大きくなる傾向にある。	 企業/組織への脅威
10 位:フィッシング詐欺		
	2012 年は大手銀行を騙ったフィッシング詐欺が広く行われ、銀行やセキュリティベンダーから注意が呼び掛けられた。フィッシング詐欺によってインターネットバンキングのパスワードを奪われると、知らないうちに口座から預金を引き出されてしまう恐れがある。	 個人ユーザーへの脅威

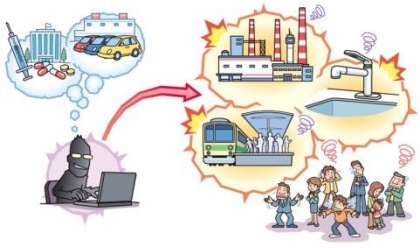
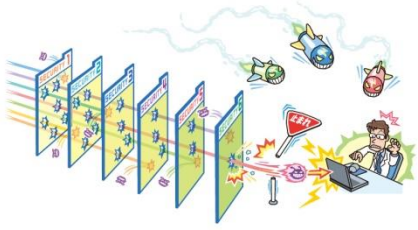
以下の表は、過去 6 年間の 10 大脅威の順位の変遷を表したものである。脅威として、継続的に上位にランキングされている脅威もあれば、スマートデバイスやクラウドに代表される、新たなデバイスやサービスの出現により、顕在化した脅威が見て取れる。

表 1:10 大脅威 順位の変遷

2008 年	2009 年	2010 年	2011 年	2012 年	2013 年	10 大脅威
8 位	―	2 位	3 位	4 位	**1 位**	クライアントソフトの脆弱性を突いた攻撃
4 位	3 位	6 位	8 位	1 位	**2 位**	標的型諜報攻撃
―	―	―	4 位	6 位	**3 位**	スマートデバイスを狙った悪意あるアプリの横行
―	―	―	―	―	**4 位**	ウイルスを使った遠隔操作
―	―	3 位	―	―	**5 位**	金銭窃取を目的としたウイルスの横行
―	―	―	―	2 位	**6 位**	予期せぬ業務停止
2 位	2 位	1 位	2 位	5 位	**7 位**	ウェブサイトを狙った攻撃
―	―	8 位	―	9 位	**8 位**	パスワード流出の脅威
3 位	5 位	5 位	1 位	8 位	**9 位**	内部犯行
7 位	―	―	―	―	**10 位**	フィッシング詐欺

３章： 今後注目すべき脅威

近年の IT 技術の発展に伴い、我々の生活スタイルや業務の在り方が変わってきており、新たな脅威や課題も見えてきている。3 章では、今後顕在化することが予想される脅威について、「10 大脅威執筆者会」のメンバーの投票により下記 3 つを選定した。

1.クラウド利用における課題	
	クラウドサービスは、業務システム、個人向けストレージ、災害時の代替システムなど様々な用途で活用されている。一方で、個人によるクラウド利用の拡大に伴い、内部データをクラウド上の無料ストレージへ複製されるなど、システム管理者にとって新たな課題が出てきている。システム管理の責任者は、情報システムを自身の完全な管理下に置けないことを前提に、インシデント発生時の対応を検討しておく必要がある。
2.重要インフラを狙った攻撃	
	これまでサイバー攻撃とは縁の薄かった、制御システム(とりわけ重要インフラシステム)への攻撃が懸念されており、国内外で対策が急がれている。また、自動車やメディカルデバイスといった機器の脆弱性も公表され、対策に向けた活動が行われている。
3.既存対策をすり抜ける攻撃の広がり	
	2010 年頃より特定のミッションに特化した高度な作りのウイルスが発見されており、セキュリティ関係者の間で話題となっている。また、高度なウイルスに限らず、既存のセキュリティ対策では、検知できない手法やウイルスが攻撃の主流になりつつあり、攻撃の全体像が掴みにくい傾向にある。攻撃の入口で検知・遮断に頼る対策から、攻撃の全体像を把握したセキュリティ対策が重要となる。

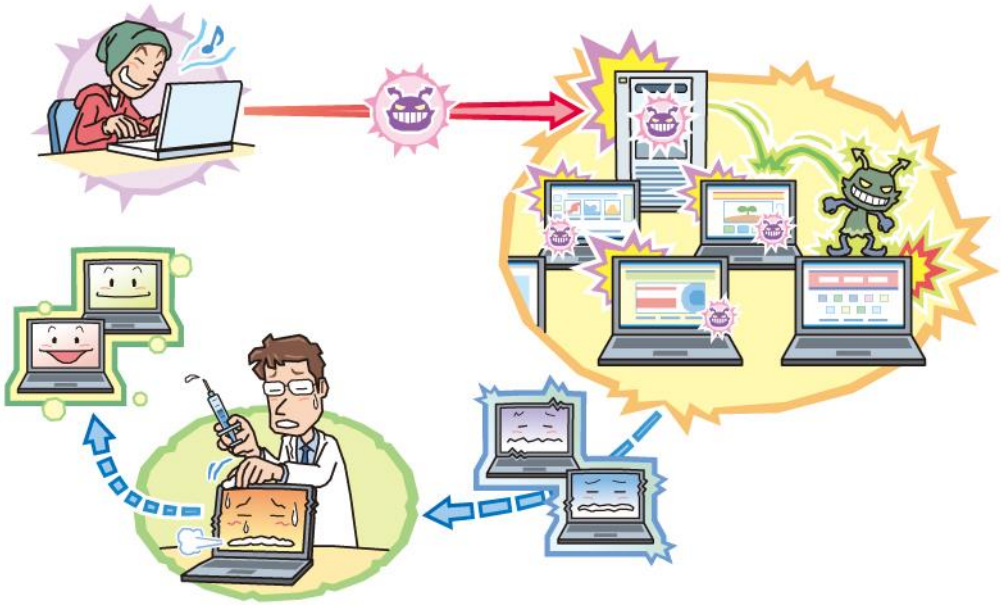
1章. 情報セキュリティの変遷

脅威とは「意図×能力(技術)」、「意図×能力(技術)×周辺環境」などと表現される。脅威というと攻撃する能力(技術)が注目されがちだが、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くる。約 10 年間で攻撃者の意図および IT インフラ環境も大きく変化し、情報セキュリティの意味合いも変わってきた。本章では、2001 年から今日までの情報システムを取巻く環境の変化や時代背景を振り返り、現在のセキュリティの実情を紹介する。

下の表は 2001 年から 2012 年までの国内における攻撃傾向や情報セキュリティに関する政策・制度面の動き、組織のセキュリティ対策の意味合いなどを 3 つの時期で分類したものである。次項以降で、3つの時期について、特徴と傾向について解説する。

	2001～2003 年	2004 年～2008 年	2009 年～2012 年
時代背景	ネットワークウイルスの全盛	内部脅威・コンプライアンス対応	脅威のグローバル化
IT 環境	コミュニケーション手段の確立	e-コマースの加速	経済・生活基盤に成長
セキュリティの意味合い	サーバーや PC の保護	企業・組織の社会的責任	危機管理・国家安全保障
攻撃者	・攻撃者 1 人	・金銭を目的とした攻撃者の出現	・ハクティビストの顕在化 ・諜報的集団(国家)の顕在化
攻撃の意図	・いたずら目的	・いたずら目的 ・金銭目的	・いたずら目的 ・金銭目的 ・抗議目的 ・諜報目的
攻撃傾向	ネットワーク上の攻撃	人を騙す攻撃の登場	攻撃対象の拡大
攻撃対象	PC、サーバー	人、情報サービス	スマートデバイス、重要インフラ
対策の方向	・セキュリティ製品中心の対策	・マネジメント体制の確立	・官民・国際連携の強化 ・セキュリティ人材育成強化
法律	・不正アクセス禁止法施行(2000) ・電子署名法施行(2001)	・個人情報保護法 全面施行 (2005) ・e-文書法施行(2005) ・日本版 SOX 法施行(2008)	・不正競争防止法改正(強化された営業秘密侵害罪施行)(2010) ・刑法改正(ウィルス作成罪施行)(2011) ・不正アクセス禁止法改正(2012)
政策・制度	・「情報セキュリティアドミニストレータ」試験新設(2001)	・ISO/IEC 27001 発行(2005) ・政府統一基準 発行(2005)	・制御システムセキュリティセンター(CSSC)設立(2012) ・官民連携プロジェクトの発足(2012)
主なセキュリティ事件	・Nimda 流行(2001) ・Code Red 流行(2001) ・SQL Slammer 流行(2003)	・P2P ソフトによる情報漏えい(2005～) ・不正アクセスによる情報流出(2005～) ・スパイウェアによる不正送金(2005～)	・米韓に DDoS 攻撃(2009) ・イランを狙った Stuxnet(2010) ・政府機関を狙ったサイバー攻撃(2011) ・金融機関を狙った攻撃(2012)

1.1.ネットワークウイルスの全盛期(2001～2003)



2001 年から 2003 年の期間は、個人ユーザーがコミュニケーション手段として日常的にインターネットに接続できるインフラを利用できる時代となった。また、情報処理技術者試験に「情報セキュリティアドミニストレータ」が新設されるなど、情報セキュリティの重要性が認知され始めた時期でもある。

- ブロードバンド時代の幕開け

2001 年は、情報セキュリティにおいて、一つのターニングポイントとなる年であった。”ブロードバンド元年”と言われるように家庭やオフィスにおいて高速通信を行える環境が普及してきた。また、電子署名法が施行されるなど、インターネット上での公的サービスやビジネスが本格的にスタートした年でもある。

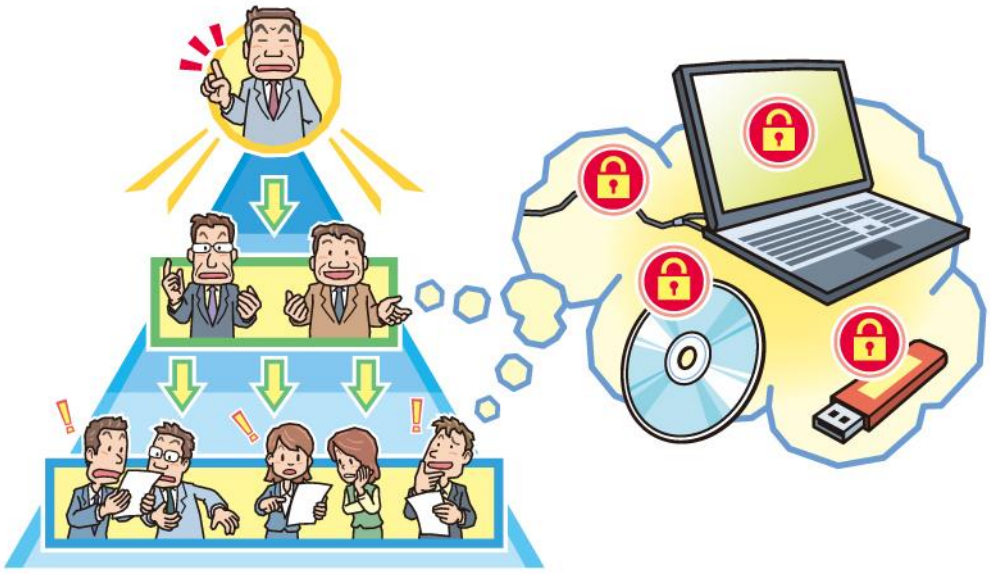
- インターネットを介した攻撃の全盛

その一方で、インターネットを介した攻撃が広く行われるようにもなった。2001 年に大流行したワーム（Nimda や CodeRed）は、インターネットを介して感染が拡大し、情報システムへ被害をもたらした。また、2003 年に発生したワーム型ウイルス SQL Slammer は、わずか 10 分で感染端末が 7 万 5000 台に達し、ワームの増殖に伴うネットワーク帯域の圧迫により、世界的にネットワーク障害が発生した。この頃の攻撃は、強力な感染力を有するワームや、システムへの不正アクセスが主流であった。また、攻撃の意図もいたずらや愉快犯的な意味合いが強かった。

- セキュリティ製品中心の対策

このような攻撃に対し、ワームの感染を防止するためのウイルス対策ソフトを導入したり、インターネットとイントラネットの境界にファイアウォールや IDS を設置して、外部からの不正侵入を検知・遮断する対策が採用されていった。この当時のセキュリティ対策は、「サーバーや PC を外部の脅威から保護する」意味合いが強く、セキュリティ製品の導入が積極的に行われた時期でもあった。

1.2.内部脅威・コンプライアンス対応 (2004～2008)



2005 年の「個人情報保護法」の全面施行、「e-文書法」の施行、ISO/IEC27001 の発行に伴い、2004 年から 2008 年は、組織・企業においてセキュリティ体制の整備が急速に行われた時期である。また、攻撃手法においても、人を騙す手口が主流となり、企業ユーザーの IT 利用や情報の取り扱いについて、内部ルールが設けられるようになった。

- セキュリティ制度・法制化の流れ

まず、企業が保有する情報の漏洩対策の一環として、2003 年の不正競争防止法改正時に、それまで不可罰であった営業秘密の侵害に対して刑事罰が導入され、2004 年に施行された。

2005 年は情報セキュリティの法制化、制度化が大きく動き出した年でもある。国内では、個人情報保護法が全面施行され、一定規模以上の個人情報を取り扱う事業者に対して、適切な運用体制の整備が義務付けられた。

同時期に情報システムの計画、実施・運用など継続的に情報システムを安全に運用していくための枠組みである ISMS 認証基準の国際規格が「ISO/IEC 27001:2005」として発行された。

また、金融商品取引法（日本版 SOX 法）が 2008 年に施行されるにあたり、企業には内部統制の強化が求められた。

このような社会的背景もあり、2004 年頃から組織・企業において情報セキュリティポリシーの策定を含めた包括的なセキュリティ対策が行われだした。トップダウンで計画から運用までをマネジメントすることが、情報セキュリティに求められるようになった。

- 相次ぐ情報漏えい事故

セキュリティ体制の整備が進む一方で、個人情報の漏えい事故が相次ぎ、組織・企業が謝罪を行うケースが散見され始めた。情報漏えいの原因としては、鞄や PC 等の紛失によるものや、「Winny」、「Share」 などのファイル交換ソフトを介したものがあった。このような状況

のもと、ファイルやハードディスクの暗号化やファイルの持ち出しを制限する「情報漏えい対策」が広く組織・企業に導入された。また、情報を漏えいさせないための社員教育やファイル交換ソフトの使用禁止等のルール化もこの時期に実施された。

その他にも、情報漏えい対策だけでなく、ウェブフィルタリング、ID 管理、持出し管理ソリューションといったような、コンプライアンスや内部統制に特化したシステム的なセキュリティ対策のソリューションも、この頃から導入された。

- e-コマースの加速

この時期、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きたことで、情報の発信や収集、相互コミュニケーションが主要な役割であったインターネットが、物品の売買を行うビジネスの場として急速に発達した。また、インターネットバンキングやネット証券などの金融資産・商品を取り扱う企業が相次いでオンラインビジネスに参画したことで、個人がインターネットで容易にオンライン取引を行える時代となった。

- 金銭を目的とした攻撃へ

このような時代背景もあり、攻撃者も個人のいたずらや顕示欲目的だったものが、徐々に組織化され金銭目的の犯行に変化してきた。海外ではブラックマーケットといわれる、攻撃ツールや個人情報等を売買するウェブサイトや、攻撃を請け負う闇業者が現れるなど、組織化された攻撃が始まった時期でもある。企業ユーザーだけでなく、一般ユーザーにおいても、知らないうちにアカウント情報が盗まれ、金銭が騙し取られる被害が散見され始めた。

- 人を騙す攻撃へ

不正アクセスやワーム感染に代表される、サーバーや PC 等のマシンに対する攻撃に加えて、フィッシング詐欺や標的型メール攻撃に代表される、人の心理面につけこみ、罠にはめて情報を窃取する攻撃が出始めた。システムやソフトウェアの脆弱性だけでなく、「人」や「組織」の脆弱性をも悪用する攻撃の傾向は、年々巧妙化しながら現在でも続いており、残念ながら、被害も継続的に報告されている。

- 企業・組織の社会的責任へ

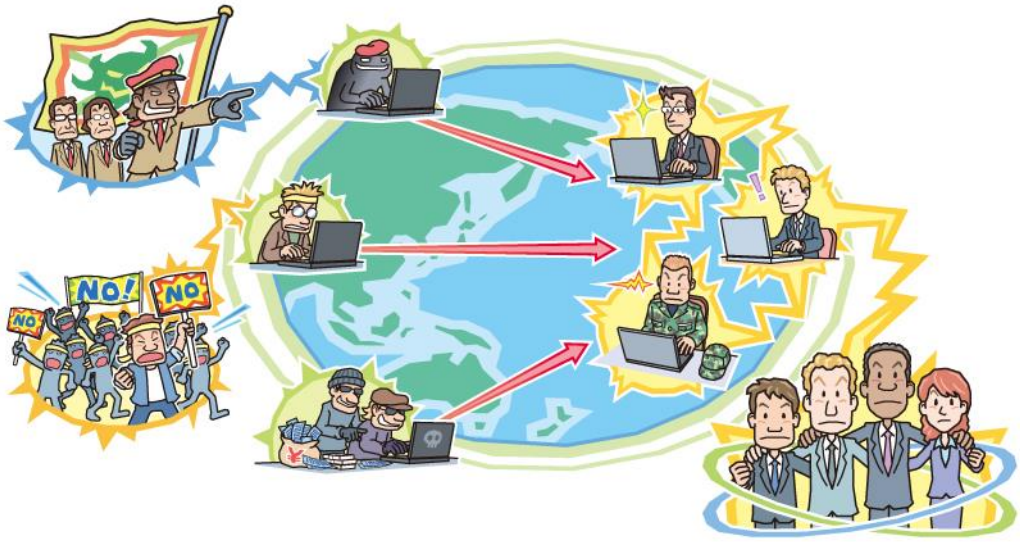
システム的な対策で対応できていた時代から、組織・企業が経営リスク・社会的責任として、組織一体となり情報セキュリティに取り組むマネジメント体制が確立されていったのがこの時期である。

また、ウェブサイトの改ざん、ウェブサイトからの個人情報流出などの外部からの攻撃によるインシデントも多数発生しており、企業・組織は、その顧客に対する社会的な責任として、十分なセキュリティ対策を取ることが求められるようになった。 その一環としてウェブサイトに対する脆弱性対策やセキュリティ診断／ペネトレーションテストなどの対応もウェブサイト運営者に求められてきた。

- ビジネスリスクとして

2007 年に発生した新潟中越沖地震をきっかけに、企業・組織が災害や事故などの予期せぬ出来事に遭遇しても、事業を継続させるように事前に計画・指針を立てておく事業継続計画(Business Continuity Plan)の重要性が考えられ始めた。災害などの不測の事態が、組織・企業におけるビジネスリスクの一つとして考えられるようになってきた。

1.3.脅威のグローバル化(2009～2012)



組織・企業のセキュリティマネジメント体制整備がひと段落した 2009 年頃から、再び外部からの攻撃へ注目が集まり、「サイバー攻撃」という言葉が一般化してきた。また、情報セキュリティをあまり考慮してこなかった分野についても、脅威が懸念されるようになり、複数の技術分野がネットワーク上で融合され、一つのシステムとしてセキュリティを考えなければならない状況となった。

- 生活基盤の一部となったインターネット

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、我々の生活においてオンラインサービスへの依存度が急激に増している。

また、運用の容易さを背景に交通システム、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も、徐々に汎用的なネットワークに接続されてきており、情報システムと同様の脅威に晒されるようになっている。

環境の変化に加えて、Facebook や Twitter 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いる。

- サイバー空間、サイバー攻撃

このように経済活動や社会活動を行う上でインターネットは無くてはならないものとなっている。一方で、インターネットに接続しているために、攻撃者から狙われやすく、攻撃を受けた際の被害も大きくなっている。

2009 年頃より、「サイバー空間(サイバースペース)」、「サイバー攻撃」という言葉が一般に使われるようになった。「サイバー空間」は、米国務省や国防総省が教書の中で使いだした言葉であり、「サイバー空間は特定の個人や組織のみが利益を得るものでなく、共同で消費または利用される国際公共財である」としている。言葉の使い方からも分かるように、サイバー空間は、国際情勢や安全保障、経済権

益確保の視点でサイバー攻撃問題を捉えている。

- 国家を巻き込んだ大規模な攻撃

2009 年に、アメリカ・韓国を標的とした大規模な DDoS 攻撃が発生し、政府機関の複数のウェブサイトが停止するに至り、国家におけるセキュリティ対策の重要性を認識させた。

また、2010 年には、イランの原子力施設を狙った攻撃（Stuxnet）が行われ、制御システムや重要施設が攻撃のターゲットになったことで大きな話題を集めた。また、攻撃の背景にはイランの核開発を阻止し、中東地域における軍事的脅威を排除しようとする米国とイスラエルの仕業であると報道されるなど、サイバー攻撃にも安全保障上の思惑が見え隠れし始めた。ウイルスを使ってイランの核施設にある遠心分離機を秘密裏に誤動作させるといった「秘密工作」「特殊工作」がサイバー攻撃により実施されたことに世間の注目が集まった。

- 政府の関与

米国防総省は「サイバー空間」を陸・海・空・宇宙空間に次ぐ「第五の戦場」であると定義し、サイバー攻撃に対して武力で反撃すると宣言している。このようにサイバー攻撃が国際情勢や安全保障に関わる問題として扱われ、関係分野が拡大している。

また、政府がインターネットの閲覧を制限する動きが複数の国で報告されている。2010 年から 2012 年にかけて、アラブ地域で起こった「アラブの春」では、Facebook や Twitter などのソーシャルメディアを通じて、政府への抗議メッセージが拡散し、反政府運動の高まりや大規模なデモに繋がったと言われている。このような状況下で、エジプト政府は、同国のインターネットを遮断する措置を取ったと言われている。また、中国では政府の都合の悪い情報に国民がアクセスできないように通信をブロックしていると言われている。このように、インターネット上の自由な情報交換が、政権を転覆させかねない事態と考えられ、政府がインターネット上の情報を統制する国も複数存在するようになった。

- 攻撃意図の変化

2008 年頃までは、金銭を目的にした攻撃が主流であったが、2010 年あたりから更に異なる二つの攻撃が、国内外の報道等により顕在化し、攻撃の意図が明らかになってきた。

一つは、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ハクティビスト[1]による攻撃が挙げられる。攻撃は、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呼び掛けられ、社会的・宗教的に対立する国や組織に対して一斉に行われる。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る。また、イランとイスラエル、イスラエルとパレスチナといった国家間の対立を背景に、ハッカー同士が相手の国を攻撃するケースも確認されている。

二つ目は、政府機関や特定の組織の情報を盗み出す諜報活動を意図した攻撃の広がりが挙げられる。日本国内でも 2011 年に政府機関や大手重要インフラ事業者が狙われたことで大きな注目を集めた。これらの攻撃は、現実世界におけるスパイ活動、

[1] 自分たちの主張を声明として発表したり、政治的に敵対する政府や企業へ攻撃したりする攻撃者の集まり。

諜報活動がサイバー空間でも行われてきた事象とも言える。政府内の機密情報や軍事関連情報が狙われるなど、国家の根幹や国益に影響を及ぼす事態となりつつある。

- グローバル、官民連携した対策

攻撃の巧妙化や攻撃意図の変化、更には守るべきプラットフォームの多様化に伴い、一つの組織・企業だけでセキュリティ対策を講じることが困難な状況になっている。このような背景の下、官民が連携したプロジェクトが発足している。重工、重電等、重要インフラで利用される機器の製造業者間で攻撃情報を共有し迅速に対応することを目的としたクローズドなサイバー情報共有イニシアティブ（J-CSIP）が2011年10月に発足した。また、サイバー攻撃からの防御に必要な高度解析を実施することを目的とした「サイバー攻撃解析協議会」が発足している[2]。

- 人材育成への取り組み

サイバー攻撃の対処に当たっては、マネジメント体制の整備だけでは防御が困難であり、攻撃者に対抗できるスキルを持ったエンジニアが必要とされる。サイバー攻撃に立ち向かうためのエンジニアの育成を目的にした強化合宿「セキュリティ・キャンプ」や実践的な経験を積める場として「CTF チャレンジジャパン[3]大会」が政府主導で開催されるなど、政策面でも人材育成に力が注がれている。

- 国内の法制度の状況

サイバー犯罪を取り締まる法律の整備も進められている。

一つには、刑法改正（ウィルス作成罪施行）が挙げられる。正当な理由がないのに、無断で他人のコンピュータ上でプログラムを実行させる目的で、ウイルスを「作成」したり「提供」したりする行為が犯罪として罰せられるようになった。

二つ目は、デンソー事件[4]などの度重なる産業スパイ事件の教訓から、2009 年には不正競争防止法の営業秘密侵害に関する刑事罰が強化され、営業秘密の領得自体への罰則が導入され、2010 年 7 月に施行された。これによって、たとえ競合関係になくとも、不正の利益を得たり保有者に損害を加えたりする目的で企業の営業秘密を持ち出すことが犯罪として罰せられるようになった。

[2] http://www.meti.go.jp/committee/kenkyukai/shoujo/cyber_attack/001_haifu.html

[3] セキュリティに関する問題を解いたり、旗を取り合ったりして、得点を取得し合う競技。

[4] http://www.47news.jp/CN/200704/CN2007040601000574.html

2章. 2013 年版 10 大脅威

2012 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明記し、それぞれの脅威について解説する。

表 2：2013 年版 10 大脅威の順位

順位	タイトル	脅威の対象		
1	クライアントソフトの脆弱性を突いた攻撃			
2	標的型諜報攻撃の脅威			
3	スマートデバイスを狙った悪意あるアプリの横行			
4	ウイルスを使った遠隔操作			
5	金銭窃取を目的としたウイルスの横行			
6	予期せぬ業務停止			
7	ウェブサイトを狙った攻撃			
8	パスワード流出の脅威			
9	内部犯行			
10	フィッシング詐欺			

【脅威の対象】

個人ユーザー

家庭等でのインターネットを利用するユーザー

企業/組織

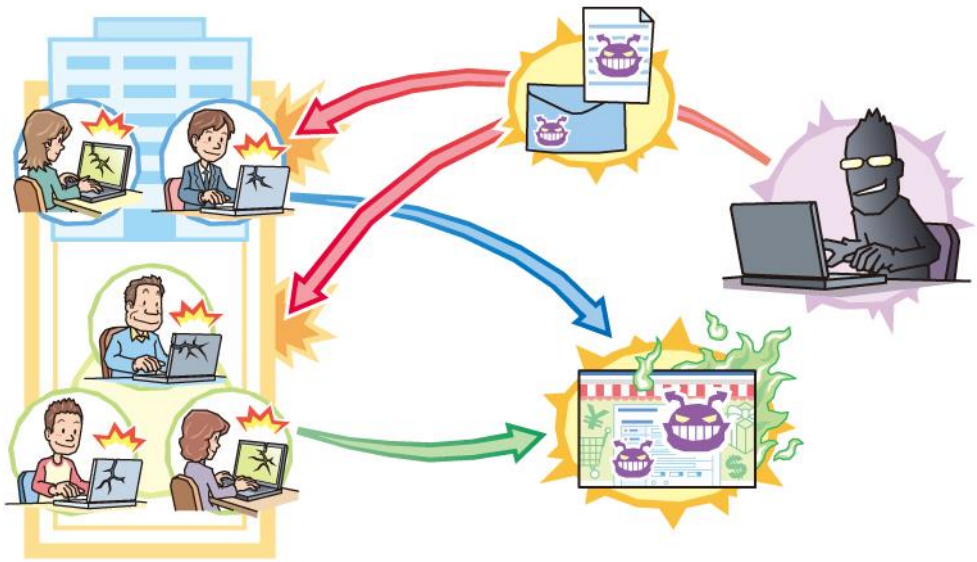
民間会社、および公共団体などの組織全体に影響する脅威

国家

国益、国民生活に影響する脅威全般

1位 クライアントソフトの脆弱性を突いた攻撃

～更新忘れのクライアントソフトが狙われている～



クライアントソフトの脆弱性を悪用されることにより、ウイルスに感染したり、システム内の情報が窃取されるなどの被害の可能性がある。ユーザーにおいては、クライアントソフトを最新に保つ対応が求められる。

＜脅威の対象＞

- 個人ユーザー
- 企業/組織

＜脅威と影響＞

近年発生しているウイルスを用いた攻撃の大半は、クライアントソフトの脆弱性が悪用されており、攻撃の常套手段となっている。しかし、昨今のインターネットバンキングを狙ったウイルスや政府機関を狙った攻撃を見ても分かるように、ユーザーに対策が浸透しておらず被害を食い止められていないのが実情である。このような実情もあり、2013 年版の 10 大脅威のランキングでは、1 位に選ばれた。

Adobe Reader、Adobe Flash Player、Oracle Java（JRE）、Microsoft Office といったクライアントソフトの脆弱性が悪用されやすい傾向にある。クライアントソフトの脆弱性が攻撃に悪用される背景としては、攻撃のターゲットになるユーザーが多いことや、ファイルやウェブサイトを閲覧するといった操作が、ユーザーが PC を利用する上で欠かせない操作であるため、攻撃の成功率が高くなる点が挙げられる。ウェブブラウザのプラグインの脆弱性が悪用されると、悪意あるサイトを閲覧しただけでウイルスに感染してしまう場合がある。

攻撃に悪用されるソフトウェアは、インターネットを利用する上で必要となる場面が多く、企業や個人で利用を控えるのは難しく、ユーザーにおいては安全に利用することが求めら

れる。

- ウイルス感染のリスクが高まる

クライアントソフトの脆弱性を放置しておくことの最大の脅威は、ウイルス感染のリスクが高くなることである。しかし、ソフトウェアの更新を行うことの必要性を認識していないユーザーや、更新の方法が分からず脆弱性を放置したままのユーザーが多く存在している。感染したウイルスによっては、個人情報が窃取されたり、金銭的な損失、PC を遠隔から操作されるなどの様々な被害が考えられる。

＜攻撃の状況＞

- 攻撃の 99.8%が既知の脆弱性を悪用[I]

2012 年上半期 Tokyo SOC 情報分析レポートによると、メールに添付される不正な文書ファイルに悪用された脆弱性の 99.8%が既知の脆弱性である。このことは、クライアントソフトが最新のバージョンであれば、多くの攻撃を防げることを意味しており、クライアントソフトを更新することの重要性が数値からも見て取れる。

＜2012 年の事例/統計＞

- Mac OS を狙う Flashback マルウェア[II]

2012 年 4 月、ロシアのコンピュータセキュリティ会社は、Mac OS X を狙ったトロイの木馬「Flashback」の被害が広がっているとして警戒を呼び掛けた。Flashback は、Adobe Flash Player のアップデートを装う Java アプレットとして不正ウェブサイトを介して拡散する。分析では、感染マシンは 60 万台以上で、98%以上が Mac OS X を稼働させている。日本では 3800 台以上の感染が見つかった。

- Adobe Reader 更新実施は半数以下[III]

IPA で実施した「2012 年度 情報セキュリティの脅威に対する意識調査」によると、Adobe Reader のバージョンアップを実施している利用者は 45%で、半数以上がバージョンアップを実施していないことが分かった。この数値は 2011 年と比較して 10%以上減少しており、ユーザーの、クライアントソフトを更新する必要性の認識の低さを示している。

＜対策/対応＞

クライアントソフトの脆弱性を狙った攻撃では、問題の根源であるソフトウェアの脆弱性を解消することが最も効果的な対策である。ソフトウェアの自動更新の設定を有効にし、更新された場合は、直ちに更新を適用することで、更新忘れを防止することができる。

一方で、アプリケーションの互換性問題やゼロデイ攻撃への対応など、対策が困難なケースも存在する。そのため、解消できない場合にも被害を防ぐためのシステム的な対策を実施することが重要となる。

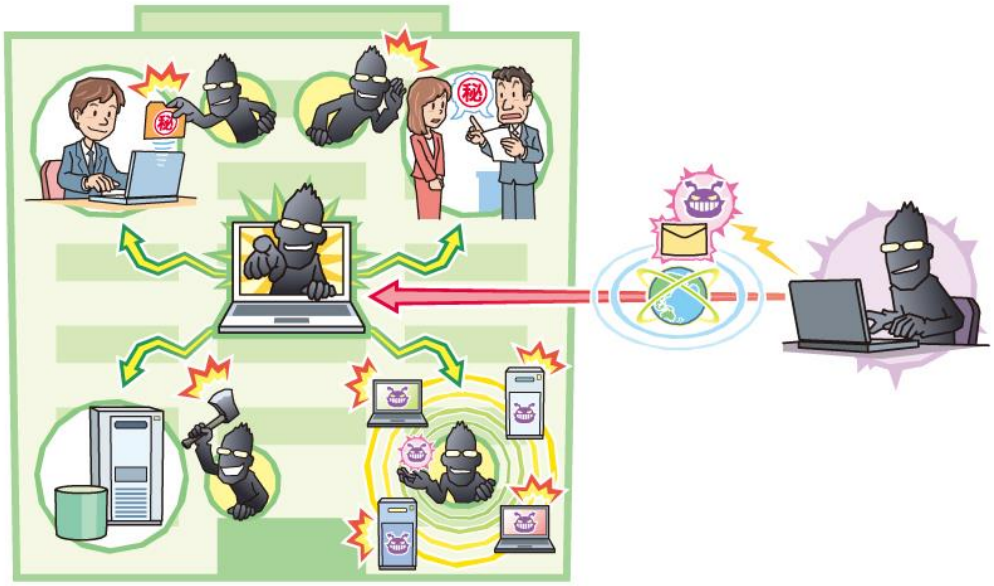
- 脆弱性対策
- システム設計

参考資料

I. 2012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_report2012_h1.pdf
II. 「Mac OS X」を狙う「Flashback」マルウエア、感染マシンは60万台以上
http://itpro.nikkeibp.co.jp/article/NEWS/20120409/390205/
III. 「2012年度 情報セキュリティの脅威に対する意識調査」報告書について
http://www.ipa.go.jp/security/fy24/reports/ishiki/index.html

2位 標的型諜報攻撃の脅威

～知らない間にスパイがあなたの情報を盗んでいる～



2011 年に続き、2012 年も政府機関や宇宙航空産業への攻撃が報道され、機密として扱われている政府関連情報や特殊技術情報の流出が疑われている。わが国の政策会議でも、この問題が取上げられるなど、国益にまで影響する問題になっている。

＜脅威の対象＞

- 国家
- 企業/組織

＜脅威と影響＞

諜報活動は、政治、軍事、経済活動に関する情報を、競争相手や敵対する組織、国家から収集することである。サイバー空間における諜報活動が、本攻撃の新しい流れである。

標的型諜報攻撃では、政府機関や特殊技術を持った組織が狙われ、知らぬ間に組織の機密情報が持ち去られてしまう。また、単に情報を持ち去るだけでなく、PC 内に侵入し、画面キャプチャー、職場での会話、PC の操作情報なども抜き取られている。いわば現実世界における産業スパイ、国家スパイが組織の PC 内部に潜入し、有益と思われる情報を盗みだしているようなものである。

なお、標的型攻撃は、単純にメールにウイルスを添付したものから、巧妙に攻撃シナリオが練られたものまで様々なレベルのものが存在する。本資料では、諜報的な意図で用いられている標的型攻撃について標的型諜報攻撃と称して紹介する。

- 国益に影響

情報が流出した組織の影響は、非常に大きい。企業の特殊技術が漏えいしたケースを想定すると、長年に渡り、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、競争力の低下になりかねない。また、政府機関の情報が流出した場合、行政の遂行に支障を及ぼすこと

が考えられる。標的型諜報攻撃における本当の怖さは、単に情報が流出したといった事象の話でなく、我々が未来に手にできるはずの利益が奪われることかもしれない。

＜攻撃の手口＞

標的型諜報攻撃が出現してから 10 年近く経過するが、残念ながら被害が後を絶たない。他の攻撃との大きな違いは、攻撃の「戦術性」にある。攻撃者は、執拗に標的となる組織を調査し、ウイルスを使ってシステム内部に潜入し、情報を収集する。攻撃に用いられるウイルスは、標的毎に作られているため、ウイルス対策ソフトでの検出が難しい。攻撃は、以下のステップで行われる。

(1)攻撃準備

攻撃者は、標的となる組織周辺の情報を収集し、攻撃の準備を行う。

(2)初期潜入

(1)で収集した情報を基にメール等でシステムに潜入する。

(3)バックドア開設

システムに侵入したウイルスがバックドアを開設する。

(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する。

攻撃では、「メールの巧妙さ」や「ウイルスの挙動」に注目が集まりがちであるが、メールやウイルスはシステムへの侵入手段にすぎず、真の脅威は、実際に情報が盗まれる(4)ハッキング・情報収集プロセスにある。これは、攻撃者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イメージである。内部からのハッキングを想定していないシステムは、このような攻撃に対して脆弱である。

＜2012 年の事例＞

- 農林水産省を狙った攻撃[I]

農林水産省が、サイバー攻撃を受け、少なくとも 1 回は意味のある情報の流出が疑われる通信があったことを確認した、と発表した。

- JAXA への攻撃[II]

宇宙航空研究開発機構（略称：JAXA）が攻撃を受け、国産ロケット「イプシロン」の仕様や運用、開発に関する情報が盗まれた可能性が報告された。また、同様に共同でイプシロンロケットを開発している、三菱重工にも同時期に「ウイルス感染事案」があった。

＜対策/対応＞

標的型諜報攻撃の対策については、完全な対策が難しい。以下のような対策を行い、外部からの攻撃だけでなく、ウイルスがシステム内部に潜入した後の、内部からの攻撃を想定した対策を講じることが重要である。

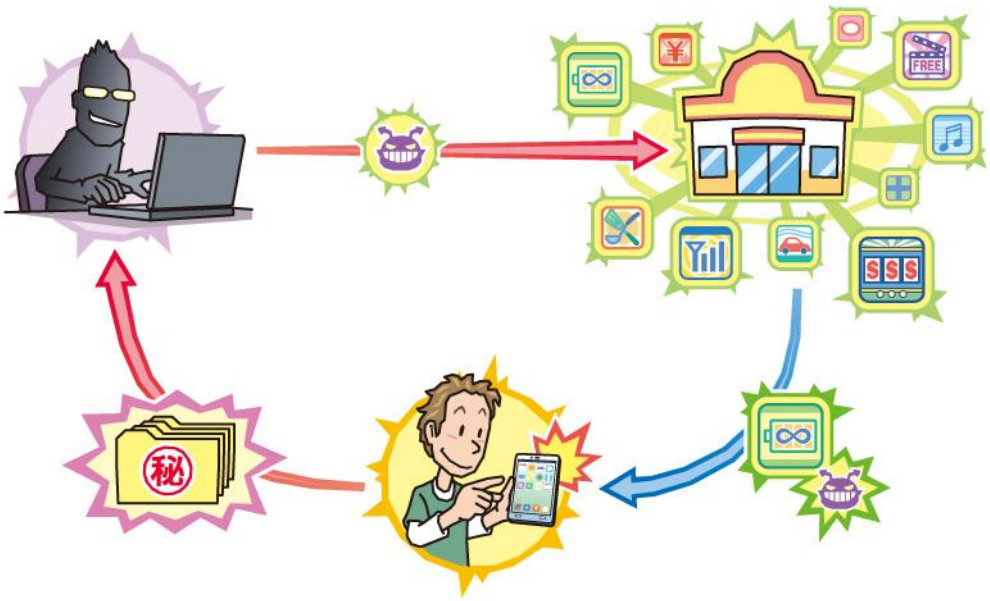
- 脆弱性対策
- システム設計
- システム監視
- アカウント/権限管理

参考資料

I. 農林水産省へのサイバー攻撃に関する調査委員会の設置及び第1回委員会の開催について
http://www.maff.go.jp/j/press/kanbo/hisyo/130111.html
II. JAXAにおけるコンピュータウイルス感染の発生及び情報漏洩の可能性について
http://www.jaxa.jp/press/2012/11/20121130_security_j.html

3位 スマートデバイスを狙った悪意あるアプリの横行

～あなたの個人情報が狙われている～



個人情報を収集する手口がより巧妙化している。近年、加速的に普及しているスマートデバイス（スマートフォンやタブレット）ユーザーをターゲットに、魅力的な機能を持っていると見せかけた不正アプリが電話帳等の情報を窃取する被害が増加している。

＜脅威の対象＞

- 個人ユーザー
- 企業/組織

＜脅威と影響＞

スマートフォン向けのアプリを中心に、ユーザーの知らない間に個人情報を窃取するアプリが問題となっている。スマートフォンは、見た目は携帯電話に似ているが、その中身はパソコンに近いものである。端末内には、電話帳、カメラで撮影した写真や動画のデータなどが格納されているため、悪意のある人間にとって魅力的なターゲットである。スマートフォンの電話帳情報を窃取されると、自分の情報だけでなく、知人や取引先企業など、保存されている全ての情報が窃取されてしまう。

個人情報を窃取されると、以下の被害が発生する可能性がある。

- スパムメールや詐欺メールの受信
- 迷惑電話（セールス、詐欺）
- プライバシーの侵害

＜攻撃の手口＞

2012 年において主流の窃取手段は、攻撃者が作成した有用に見せかけた偽アプリを、ユーザーにインストールさせ、知らぬ間に端末から個人情報を収集するものである。

＜2012 **年の事例/統計**＞

- 偽アプリによる情報窃取が大問題に[I]

2012 年 4 月、名前に「the Movie」という文字を含むスマートフォン向けアプリが、電話帳データを収集していると大きく報道された。ユーザーに魅力的な動画コンテンツが閲覧できると謳ったアプリが配布され、この一連のアプリによって約 1000 万件の個人情報が窃取されたと言われている。これらのアプリは、Google が運営する公式マーケットで流通していたため、ユーザーが気楽にインストールできる状態となっていた。

- 明示的に情報収集するアプリ登場！[II]

2012 年 10 月には「全国電話帳」というアプリが登場、このアプリの説明には、ユーザーの電話帳データや GPS の位置情報も利用すると明記されていたにも関わらず、約 3300 台の端末から約 76 万人分の個人情報がサーバーに送信されたとみられている。電話帳は他人の個人情報の集合であるため、ユーザーは他人の個人情報を扱っていることを意識しなければならない。

- サービス提供企業に求められる対応

スマートフォンアプリに限らず、利用規約に記載している場合でも、利用者に理解しやすい表現にしていないと、個人情報の収集をユーザーが気付かない可能性がある点や、サービス提供者が過剰に情報を収集しているケースが問題となっている。

2012 年は、PC のブラウザツールバーソフトウェアが、ポイントと引き換えにウェブ閲覧履歴を取得していることが話題となった。

サービスを提供する企業は、個人情報を収集する場合、利用規約に記載している場合でも、曖昧な表現や、目立たない表現を使ったならば、適切にユーザーから同意をとっていないとみなされる可能性がある。

総務省は 2012 年 1 月に「スマートフォン プライバシー イニシアティブ －利用者情報の適正な取り扱いとリテラシー向上による新時代イノベーション－」[III] を公表するなど、政府による指導的な取り組みも行われている。これを受けて、業界側としてガイドラインを作る動きが出てきている。

＜**対策/対応**＞

ユーザーがアプリを利用するにあたり、以下の対策を実施することが望ましい。

- 教育/啓発（信頼できるアプリの利用）
- ウイルス対策

特に、信頼できると判断したアプリやサービスだけを利用することは、現状において重要な対策となる。以下の情報も、ユーザー自身が信用できるアプリかどうか判断するための参考となる。

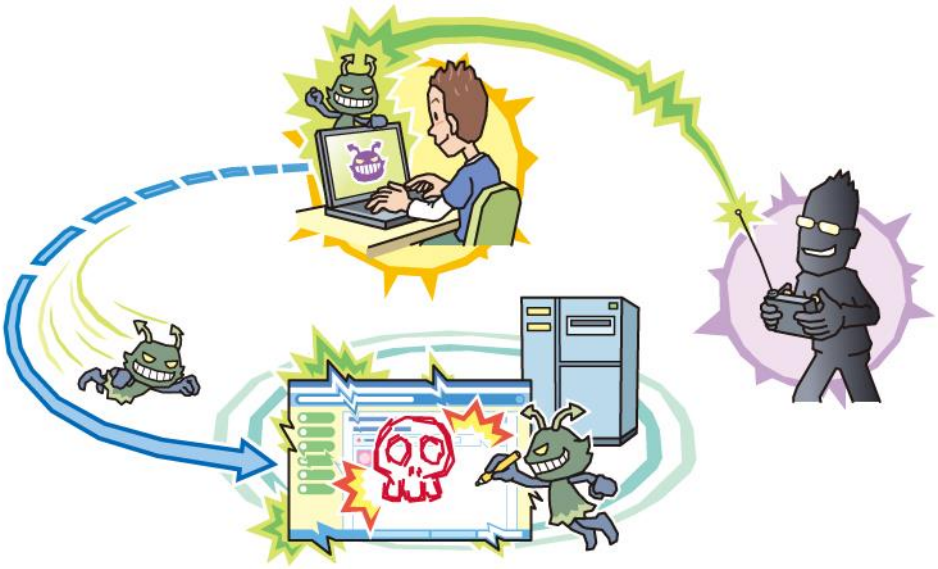
- ダウンロード数/利用者数
- ユーザーレビュー/評価
- 利用規約

参考資料

I.「情報を抜き取るスマートフォンアプリに注意！」
http://www.ipa.go.jp/security/txt/2012/09outline.html#5
II. スマホアプリで76万人分の個人情報流出か 「全国電話帳」インストールに注意
http://sankei.jp.msn.com/affairs/news/121006/crm12100617380008-n1.htm
III.「スマートフォン プライバシー イニシアティブ －利用者情報の適正な取扱いとリテラシー向上による新時代イノベーション－」の公表
http://www.soumu.go.jp/menu_news/s-news/01kiban08_02000087.html

4位 ウイルスを使った遠隔操作

～知らない間に濡れ衣を着せられることに！！～



ウイルスに感染した PC は、これまでもスパムの送信や DDoS 攻撃のために悪用されてきた。2012 年、PC に感染したウイルスを経由して、悪意ある第三者が掲示板に脅迫文を書きこむとともに、当該ウイルスに感染した PC の所有者が誤認逮捕される事件が発生し、大きな話題となった。

＜脅威の対象＞

- 個人ユーザー
- 企業/組織

＜脅威と影響＞

遠隔操作ウイルスに感染した PC は、攻撃者によって遠隔操作され、特定のサーバーを攻撃したり、内部の情報を外部に送出したりする。場合によっては、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る。

これまでも、ウイルスに感染した PC は、ボットネットと呼ばれる感染 PC で構成されるネットワークに組入れられ、攻撃者によって遠隔コントロールされ、ユーザーの知らないうちに次のような攻撃に加担させられていた。

- 設定情報や個人情報の送信
- スパムメールの送信
- DDoS 攻撃への加担
- ウイルス自身のアップデート
- ウイルスの拡散

特定の目的のために個別に作成されたウイルスは、ウイルス対策ソフトに検知されにくい。そのため、ユーザーはウイルス感染したことに気付けず、被害の発覚が遅れる可能性が高い。

＜攻撃の手口＞

攻撃者は、主に以下の手段によって、ユーザーをウイルスに感染させる。

- メールに添付されたファイルを開かせる
- 悪意あるウェブサイトを閲覧させる
- ウイルス混入したソフトウェアを利用させる

＜2012 年の事例/統計＞

- 遠隔操作ウイルス事件

2012 年 6 月から 9 月にかけて、攻撃者が、PC に感染させたウイルスを介して PC を遠隔操作し、掲示板などへ脅迫文の送信が行われ、4 人が誤認逮捕される「遠隔操作ウイルス」事件が発生し、大きな社会問題となった。

誤認逮捕された人物が所有する PC からは、掲示板を経由して誘導されたウェブサイトからダウンロードしたソフトウェアが保存されていた。保存されていたソフトウェアのファイルの中から攻撃者の命令を受けて動作するトロイの木馬型のウイルスが発見された。

また、犯行声明のメールが Tor(トーア)というソフトウェアを用いてアクセス元が巧妙に隠ぺいされるなど、真犯人の特定の難しさも大きな話題となった[I]

犯人とされる人物から送られた犯行声明によると、警察への恨みに基づいた、私的な目的のために、犯行に及んだとされている。この犯人とされる人物が用いた攻撃手法は、新しいものではなく、ある程度のコンピュータの知識があればウイルス作成が行えるため、今後模倣される可能性が懸念されている。

＜対策/対応＞

ユーザーにおいては、ウイルスに感染しないように日頃から下記の対策を怠らず、PC を安全な状態にしておくことが重要である。

- 教育/啓発
- 脆弱性対策
- ウイルス対策

遠隔操作ウイルス事件の事例では、ユーザーにとって便利なソフトウェアとして配布されたファイルの中にウイルスが混入していた。同様のウイルスに感染しないためには、信頼のおけない見知らぬウェブサイトからのソフトウェアのダウンロードは控えることも対策として必要である。

また、遠隔操作ウイルス事件は、社会的に反響が大きく、インターネットでこの事件に関する解説[II]などを閲覧できる。これらを読み理解しておくことは、自衛につながる。

参考資料

I. 犯行予告事件、身元隠す「Tor(トーア)」の悪用と犯人像
http://www.yomiuri.co.jp/net/security/goshinjyutsu/20121019-OYT8T01021.htm
II. 「濡れ衣を着せられないよう自己防衛を！」
http://www.ipa.go.jp/security/txt/2012/11outline.html#5

5位 金銭窃取を目的としたウイルスの横行

～日本でもインターネットバンキングが狙われている～

2011 年頃より海外のインターネットバンキングで、ウイルスにより認証情報が窃取され、金銭被害に発展する事件が報告されはじめた。2012 年からは国内のインターネットバンキングでも同様の手口による被害が確認されだしている。

＜脅威の対象＞

- 個人ユーザー

＜脅威と影響＞

インターネットバンキングは、銀行に行かずとも、残高照会や送金ができ、時間が無い人などには利便性が高い。その反面、悪意のある第三者に認証情報を知られた場合、金銭的な被害を受ける可能性がある。また、クレジットカード情報も同様に、金銭的な被害を受ける可能性がある。

従来の攻撃は、フィッシング詐欺等で偽のサイトに誘導し、口座番号や認証情報を入力させるものが主流だった。そのため、正規のサイトであることを確認してからパスワードを入力することにより、被害を避けることができた。しかし、ウイルスによる攻撃では正規サイトへのアクセスを監視された上で窃取されるため、注意しても攻撃に気づくことは難しい。

これらのインターネットバンキングの認証情報やクレジットカード情報を窃取するウイルスは、数年前までは日本のユーザーをターゲットとしていなかったが、現在は海外のみならず、日本でも流行し始めており、日本での金銭的な被害が拡大している。

＜攻撃の手口＞

ウイルスは次のような機能を有しており、ユーザーの認証情報を窃取する。

- 盗聴

SpyEye などのウイルスに感染後、ユーザーはインターネットバンキングの利用を監視され、キーロガーと呼ばれるタイプのウイルスにより ID/パスワードを盗聴される。

- ポップアップ画面

PC がウイルスに感染することにより、ユーザーが正規サイトにログインした直後に「合言葉」「第2暗証番号」などの入力を促すポップアップが画面に出力され、ユーザーに認証情報を入力させる。正規のサイトにアクセスしている途中に表示されるポップアップであるため、攻撃者からの罠だと気づくのが難しい。

＜2012 年の事例/統計＞

- ポップアップ表示するウイルスの登場

2012 年 10 月、日本の銀行をターゲットとした巧妙なポップアップ画面を表示するバンキングウイルスが確認された。[I] 三井住友銀行の口座から約 200 万円が送金される事例をはじめ、日本の複数の銀行口座から不正送金される被害が発生した。[II]

このウイルスに感染した PC において、日本の特定の銀行のインターネットバンキングを利用した際、偽のポップアップが表示され、通常の操作にはない多くの認証情報を入力させられる。攻撃者はこの認証情報を利用してログインし、不正送金を行った。

- 日本をターゲットにしたウイルスの増加

日本の銀行の偽認証画面をポップアップ表示させるウイルスの登場や、数年前までは海外のみで流行していた SpyEye が日本の銀行をターゲットとしはじめたことは [III]、金融業界に衝撃を与えている。この他に、ウイルススキャンしているように見せかけ、PC の情報を外部サイトに送信する偽ウイルス対策ソフトも、日本語対応されたものが確認されている。国内ユーザーが騙され易い状況が拡大している。

＜対策/対応＞

金銭窃取の被害に遭わないためには、PC を安全な状態に保つことに加え、罠に引っ掛らないように注意することである。

- 脆弱性対策
- ウイルス対策
- 教育/啓発

さらに、偽の認証画面が表示されたことに気付くためには、普段利用するインターネットバンキングの通常の認証プロセスを事前に確認しておくことも必要になる。また、金融機関は、注意喚起を行い、正しい画面遷移をユーザーに示すことが求められる。

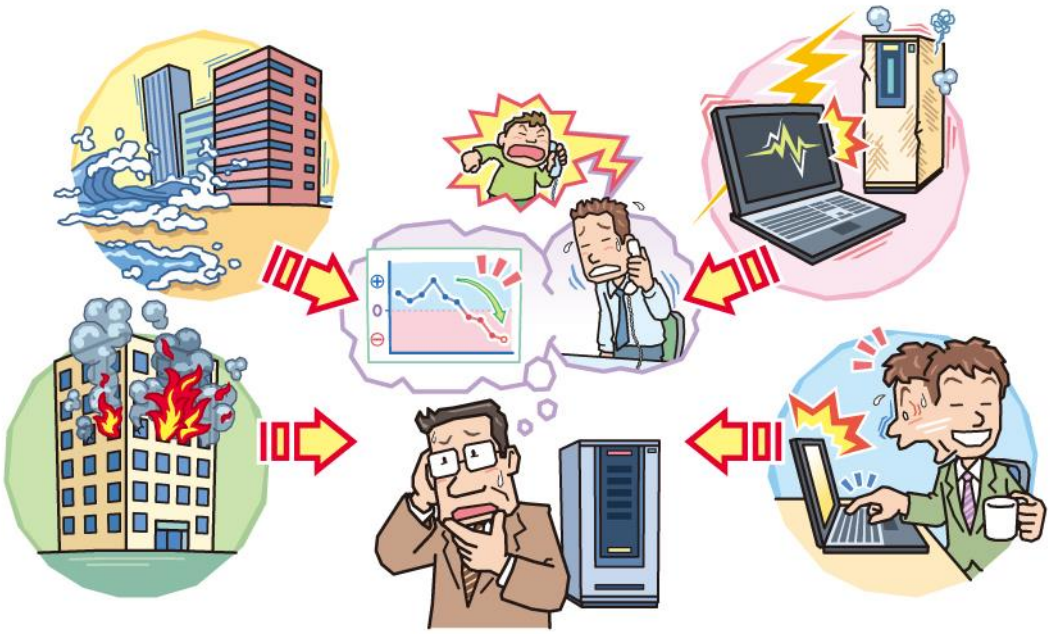
もし偽画面が表示されたことに気付いた場合、既にウイルスに感染している可能性が高いため、ウイルス対策ソフトによる駆除の実施や、必要に応じて PC の初期化を行う。

参考資料

I. 大手3銀行のネットバンクで偽の情報入力画面、原因はウイルス
http://itpro.nikkeibp.co.jp/article/NEWS/20121030/433523/
II. 送金先に「中国人名義」の口座　ネットバンク不正事件、背後に中国人犯行グループ？
http://sankei.jp.msn.com/affairs/news/121031/crm12103114170010-n1.htm
III.「あなたの銀行口座も狙われている！？」
http://www.ipa.go.jp/security/txt/2011/09outline.html#5

6位 予期せぬ業務停止

～自然災害やハードウェア障害、人的ミスが思わぬ事態を引き起こす～



システムのクラウド化が進む中、2012 年は、レンタルサーバー企業において人為的ミスによる大規模障害が発生した。東日本大震災によって、自然災害が原因となりシステムが停止するリスクが浮き彫りとなったように、不測の事態に備える必要性が組織に求められる。

＜脅威の対象＞

- 企業/組織

＜脅威と影響＞

情報セキュリティの基本は、情報システムやデータを外部要因により侵害させず、安全な状態が保たれることである。情報セキュリティと言えば外部からの攻撃に注目が集まりがちだが、自然災害やオペレーションミスなど悪意の無い要因によるシステム停止、データ破壊なども無視できない存在である。

近年、業務の IT 化やデータの肥大化が益々進んでおり、システムが停止した場合、システムへの依存度や停止期間によっては、企業/組織の事業に次のような影響を与える。

- 停止期間分の利益を失う
- 顧客/サービス利用者の事業に悪影響を与える
- 顧客/サービス利用者からの信用を失い、ビジネス機会を損失する

また、製造業においては、自身は被災していなくても、提携先や部品の調達先が被災することで、生産に影響がでることが想定されており、複数の企業間で物流システムを構築する、サプライチェーン・マネジメントが注目されるようになってきた。

＜発生要因＞

これらの不測の事態の要因として、次のような事象が考えられる。

- ハードウェアの故障
- プログラムの不具合
- オペレーションミス
- 自然災害

2011 年に発生した東日本大震災では、数多くのシステムで、サーバー障害やデータの消失が発生し、システムの可用性の重要さを再確認する機会となった。また、自然災害に限らず、ハードウェア障害や人為的ミスによるデータ損失により大きなインパクトを残す事故も発生しており、システムの信頼性に大きな課題を投げかけている。

＜2012 年の事例/統計＞

- ファーストサーバのデータ消失事故[I]

2012 年 6 月 20 日、レンタルサーバー企業であるファーストサーバにおいて大規模障害が発生した。5 万顧客中、約 5700 の顧客のサーバー群に対し、不適切なファイル削除処理を含むプログラムを検証環境・本番環境・バックアップ環境で実行してしまった。その結果、大規模にデータが消失し、復旧不可能な状況となった。ファーストサーバの一部の広告で「お客様による作業（バックアップ）は不要」と記載されていたこともあり、ユーザーの多くが、バックアップを行っておらず、ユーザー組織のビジネスに大きな損害を与えた。

- 東京証券取引所の障害[II]

2012 年 2 月、東京証券取引所において、株価情報の配信システムの待機系への切り替え失敗が検知できず、情報が配信できない障害が発生した。3 時間半の間、約 300 銘柄で取引が停止し、投資家や投資会社に大きな影響を与えた。原因は、診断ソフトウェアへの過信、深夜の監視体制の弱さとされている。

＜対策/対応＞

様々なトラブルをあらかじめ想定しておき、それらへの対応策を準備しておくことが大切である。

- システム設計
- システム監視
- アカウント/権限管理

特に、手順書の作成や検証・実施・承認の手順遵守など運用を強化することで、人為的ミスを軽減することが重要である。

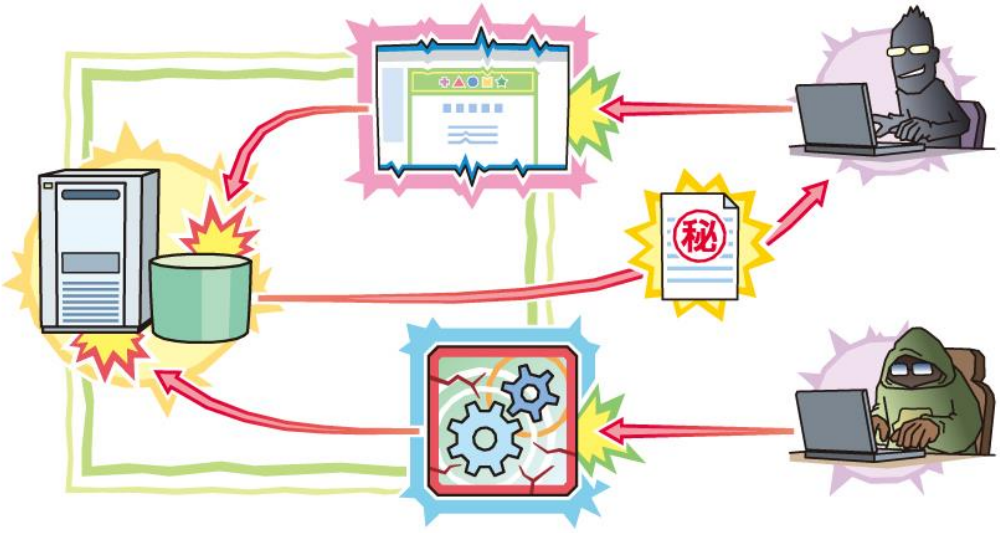
次に、上記の取り組みでは防ぐことができない自然災害などによる不測の事態の発生に備え、事業の継続あるいは早期復旧を可能にするための行動計画、事業継続計画（BCP）を選定し運用することが有効である。
経済産業省より、BCP 策定を支援する文書として、事業継続に関するガイドラインが公開されている。[III] [IV]

参考資料

I. 6/20に発生した大規模障害に関するお詫びとお知らせ
http://support.fsv.jp/urgent/
II. 株式売買システムの障害発生に関する再発防止措置等について
http://www.tse.or.jp/news/03/120216_a.html
III. 事業継続計画策定ガイドライン
http://www.meti.go.jp/policy/netsecurity/secgov-tools.html#bcp-model
IV. 高回復力システム基盤導入ガイド
http://sec.ipa.go.jp/reports/20120508.html

7位 ウェブサイトを狙った攻撃

～断続的に続くウェブサイトを狙った攻撃～



ウェブサイトを狙った攻撃は、旧来から認識されている脅威であるが、残念ながら被害が後を絶たない。ウェブサイト内の個人情報窃取や、ウェブサイトの改ざんによるウイルス配布など、組織や個人ユーザーに影響を及ぼす脅威である。

＜脅威の対象＞

- 個人ユーザー
- 企業/組織

＜脅威と影響＞

ウェブサイトを狙った攻撃は、10 年以上前から続いている脅威の一つであるが、被害が後を絶たない。攻撃者は、次のような意図を持ってウェブサイトへ攻撃を行う。

(1) 情報の窃取

ウェブサイトで保持している個人情報などの有益な情報を盗み出す。

(2) ウイルスの配布

ウェブサイトにウイルスを埋め込むことで、サイトを閲覧したユーザーの PC をウイルスに感染させる。

(3) ウェブサイト改ざんによる主義・主張

敵対する組織のウェブサイトを改ざんし、自分達の主張を誇示する。

ウェブサイトから顧客情報が流出したり、ウイルスの配布に悪用されることで、企業/組織の信頼喪失につながる可能性がある。また、権威あるサイトの内容が悪意ある内容に書き換えられた場合、当該機関の権威を損なう事態が考えられる。

＜攻撃の手口＞

ウェブサイトを狙った攻撃は、ウェブサイト上の設定不備やソフトウェアの脆弱性を悪用する。概ね以下の 3 点を狙った複合的な攻撃が行われる。

- ウェブアプリケーションの脆弱性

ウェブサイトの様々なサービスや機能を提供するウェブアプリケーションの脆弱性を悪用して攻撃が行われる。個別に開発したアプリケーションの脆弱性が発見されたり、オープンソースなどの汎用的なアプリケーションの脆弱性が狙われることもある。

- ウェブ実行環境の脆弱性

PHP や Apache など、ウェブサイトを構築するための実行環境やプログラミング言語の脆弱性を悪用された攻撃が行われる。

- システムの設定不備

サーバーの管理者アカウントに脆弱なパスワードが設定されていたり、ウェブサイトの管理機能が外部からアクセスできる状態で放置されることで、不正アクセスを受け、ウェブページの改ざんやデータ窃取が行われる。

＜2012 年の事例/統計＞

- 不正アクセスによる情報漏えい[I]

2012 年 3 月、国内ソフトウェアダウンロードサイトは、4 回にわたる不正アクセス、システム改ざんにより、PC オンラインゲームを利用している 463 件のユーザーのクレジットカード情報が窃取されたとして報告した。

対応策として、システム改修、不正アクセスの検知・遮断対策、個人情報の暗号化、パスワード強化などを行っている。

- PHP の脆弱性を悪用する攻撃[II]

2012 年 5 月、PHP の脆弱性を悪用する攻撃が検知された。この脆弱性は、ウェブサーバー上で PHP を CGI モードで動作させている場合に影響する。リモートからの操作により、PHP スクリプトのソースを閲覧されたり、任意のコードを実行されたりする。

- ウェブサイト改ざん件数が約 6 倍に[III]

JPCERT/CC インシデント報告対応レポートによると、2012 年のウェブサイト改ざん件数は 1814 件に上り、2011 年の 320 件と比較して約 6 倍となっている。ページに不正に挿入された JavaScript コードや iframe によりサイト閲覧者を攻撃サイトに誘導し、複数の脆弱性を使用した攻撃により PC をウイルスに感染させるものが多く確認されている。

＜対策/対応＞

ウェブサイトを狙った攻撃は、システムの設定不備やウェブアプリケーションの脆弱性が悪用されて引き起こされる。そのため、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、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、脆弱性対策やアクセス権の管理など、運用・監視を怠らない事が大切である。

- システム設計
- システム監視
- アカウント/権限管理
- 脆弱性対策

参考資料

I. 当社サーバーへの不正アクセスに対する調査結果（最終報告）
http://ir.vector.co.jp/corp/release/20120724_1/
II. CGI版PHPの脆弱性に注意喚起、国内でも攻撃を検出
http://www.atmarkit.co.jp/news/201205/10/php543.html
III. インシデント報告対応四半期レポート
http://www.jpcert.or.jp/ir/report.html#year2012

8位 パスワード流出の脅威

～知らぬ間にパスワードが盗まれていませんか？～

オンラインサービスの増加に伴い、ユーザーが複数のパスワードを管理する必要が生じている。その結果、同一の ID/パスワードを使い回すユーザーが多くなり、一つのウェブサイトでパスワードが漏えいすることで、複数のウェブサイトで成りすましの被害に遭ってしまう。

＜脅威の対象＞

- 個人ユーザー
- 企業/組織

＜脅威と影響＞

今日では、個人向けにフリーメールなどのオンラインサービスが数多く提供されており、ID/パスワードによるユーザー認証が定着している。また、ID にはメールアドレスが用いられることが多い。

パスワードを他人に知られてしまうと、他人が本人に成りすまして権限を行使し不正な操作が行えるため、パスワードは他人に知られてはならないものである。ID/パスワードに変わる認証方式は複数存在するが、事業者側のコスト負担やユーザー側の利便性の観点から、パスワードによる認証が未だに一般的である。

- 攻撃の影響

本攻撃の脅威は、本人に成りすまされ不正が行われることである。例えば、システム管理者であれば管理しているサーバーが乗っ取られることを意味する。また、インターネットバンキングを利用する個人ユーザーの場合だと、不正送金などの金銭的な被害に発展する可能性が考えられる。

- ID/パスワードの使い回しの問題

オンラインサービスの増加に伴い、ユーザーが複数のパスワードを管理する必要が生じている。その結果、同一の ID/パスワードを使い回すユーザーが多くなり、一つのサイトで使用している ID/パスワードが盗まれることで、

他サイトでも悪用されてしまうなどの二次被害が考えられる。

＜攻撃の手口＞

主なパスワード入手の手口として以下の三つが挙げられる。

(1) ソーシャルエンジニアリング

(2) パスワード推測

(3) パスワードリスト攻撃

(1)のソーシャルエンジニアリングは、入力の盗み見、廃棄物からの読み取り、ネットワーク管理者や顧客を装って聞き出すなどによりユーザーのパスワードを入手する方法である。

(2)のパスワード推測では、可能な限り全ての文字列の組み合わせを試してパスワードを推測する総当たり攻撃や、辞書に記載された単語からパスワードを推測する辞書攻撃などが挙げられる。

(3)のパスワードリスト攻撃では、ユーザーの多くが複数サイトで同一のID/パスワードを使い回ししている状況に目を付けた攻撃者が、脆弱なウェブサイトなどから不正に取得したパスワードのリストを使い、他のウェブサイトに不正アクセスを仕掛ける。この攻撃では、攻撃者に正規のパスワードを入手されているため、ユーザーによるパスワード強化やウェブサイトによる不正アクセス対策も効果が無い。

＜2012 年の事例/統計＞

- ユーザーのパスワード管理状況[I]

国内セキュリティシステム企業の調査によると、ユーザーの 7 割が 3 種類以下のパスワードを使い回しているという結果が出ている。

- オンラインゲームサイトへのパスワードリスト攻撃[II]

2012 年 8 月、国内オンラインゲームサービス会社のサーバーにおいて、第三者によりパスワードリスト攻撃が試みられていることが判明した。不特定の企業・サービスなどから不正に入手した ID/パスワードのリストを悪用して不正ログインをされることで、ID/パスワードや会員情報が流出する可能性がある。この影響により、他のオンラインゲームサービス会社でもパスワードの変更を促す注意喚起を出している。[III]

＜対策/対応＞

ユーザーはパスワードの使い回しを避けるなどの対策を実施する必要がある。

システム管理者は、パスワード推測攻撃に備えて、アカウントロックを設定することも大切である。

ウェブサイトにおいては、保存されているパスワードデータが漏えいしたとしても悪用されることがない様に、パスワードをソルト付きでハッシュ化するなどの対策を実施しておく。

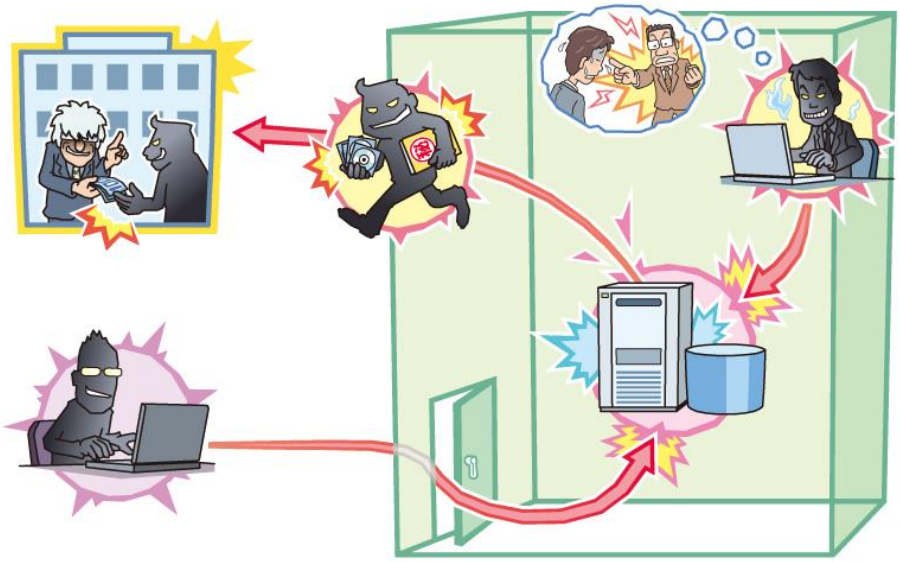
- アカウント/権限管理
- 教育/啓発
- システム設計（適切な認証方式の導入）

参考資料

I. パスワードの使い回しにご用心
http://www.yomiuri.co.jp/net/security/goshinjyutsu/20121228-OYT8T00771.htm
II. SEGA IDとパスワード管理に関するご注意
http://gw.sega.jp/gw/news/index.html?category=2&id=3
III. 【重要】アカウントハッキングにご注意ください。
http://www.gungho.jp/index.php?module=Page&action=NoticeDetailPage&notice_id=2291

9位 内部犯行

～あなたの職場は大丈夫？内部に潜む犯行者～



内部の人間による故意の情報漏えいや不正操作による被害が報告されている。正当に権限を有したユーザーによる犯行であるため、防止が難しく、被害も大きくなる傾向にある。

＜脅威の対象＞

- 企業/組織

＜脅威と影響＞

攻撃者は、外部だけに存在するのではない。もし、組織内部の権限を持つシステム管理者が悪意を持てば、攻撃を実行することは容易であるため、組織にとって大きな脅威であると言える。近年、従業員や元従業員による意図的な情報持出しやシステム停止などの犯行が発生している。

社内システムにアクセスできる権限を持つ従業員は、自らの権限を利用して内部システムにアクセスし、業務妨害、重要情報・顧客情報などの持ち出しによる情報漏えいを行うことが可能である。また、退職者や委託社員などによって仕掛けられたバックドアや、付与されたままのリモートアクセス権限を利用して、元従業員が内部情報を窃取する可能性がある。

このように内部犯行は、人為的なものであり、技術的な対策だけでは犯行を防ぎにくいことが特徴である。

また、組織内部の人間の犯行であるため、外部からは監督不行き届きと映り、外部からの信頼低下が予想される。

＜犯行の手口＞

内部犯行の手口は以下３つに分類される。

(1) 管理者権限の悪用
(2) 情報・システム破壊
(3) 不正アクセス

(1)のシステム悪用は、金銭目的で行われることが多く、不正入金やメールの盗み見・転送などを行う。

(2)の情報破壊・システム破壊は、社内システム内のデータを削除したり、プログラムを消去・改ざんすることで業務妨害を行う。

(3)の不正アクセスは、金銭目的やビジネス目的で顧客情報を社外に持ち出して、内部情報の転売・流用を行う。

このように、内部犯行の目的や犯行の手口は様々である。

＜2012 年の事例/統計＞

- 委託社員によるキャッシュカード偽造 [I]

2012 年 11 月、国内システム会社の委託社員により、取引情報を不正に取得され、金融機関のキャッシュカードを偽造されて現金を不正に引き出される被害が発生した。

この委託社員は「システムの動作確認」を口実にホストコンピュータに 3 回アクセスをし、三百数十口座分の顧客データを抜き取っていたという。

- 退職した元社員による不正アクセス [II]

国内生命保険会社の退職した元社員および代理店の保険販売員計 19 名により顧客 422 人の氏名・生年月日、契約内容などの個人情報が漏えいした。退職した社員の ID/パスワードを無効化する処理が遅れ、退職後も最大 10 日間アクセス可能となっていたという。

- 内部不正の実態 [III]

『組織の内部不正防止への取り組み』に関するレポートによると、内部犯行の動機として最も多かったのが金銭目的であると報告されている。金銭目的は 32%、その次に組織への不満、転職目的がそれぞれ 26%であった。

また、不正行為の 7 割以上が、個別・単独で作業を行う、監視性の低い職場で起きている。犯行対象は、顧客情報が 53%、社内情報が 16%、ID/パスワードが 16%、開発情報が 10%で、顧客情報を対象とした犯行が半数以上を占めていた。さらに、不正行為者の内訳は一般社員が 58%、システム管理者が 21%、開発者が 16%となっており、一般社員の数が最も多いが、組織の人数構成を考慮すると、システム管理者の割合が高いと言える。

＜対策/対応＞

内部犯行の代表的な対策として、以下の対策が考えられる。不満の出にくい職場環境に加え、監視の目を光らせることや、アカウント権限を厳しくして、不正を起こしづらい状況を創出することが重要である。

- アカウント/権限管理
- ポリシー/ルール
- システム設計
- システム監視

参考資料

I. 地銀システム保守を口実、データ盗みカード偽造 NTTデータ委託社員を再逮捕
http://sankei.jp.msn.com/affairs/news/130117/crm13011710340003-n1.htm
II. 退職社員らが不正アクセス、情報漏えい ジブラルタ生命保険
http://www.nikkei.com/article/DGXNZO48189210Y2A101C1CC1000/
III. 『組織の内部不正防止への取り組み』に関するレポート
http://www.ipa.go.jp/about/technicalwatch/20120315.html

10位 フィッシング詐欺

～あなたの口座から預金が無くなっていませんか？～

2012 年は大手銀行を騙ったフィッシング詐欺が広く行われ、銀行やセキュリティベンダーから注意が呼び掛けられた。フィッシング詐欺によってインターネットバンキングのパスワードを奪われると、知らないうちに口座から預金を引き出されてしまう恐れがある。

＜脅威の対象＞

- 個人ユーザー

＜脅威と影響＞

フィッシング詐欺とは、ユーザーを騙すことにより、インターネットバンキングの ID/パスワードやクレジットカード番号などの情報を盗み取る犯罪である。最近では金銭情報だけでなくオンラインゲームやインターネットオークションのアカウントが盗まれるケースも存在する。

オンラインでの決済や送金が一般化した今日では、ID/パスワードやクレジットカード番号といった情報は、印鑑や通帳と同等の価値があると言っても過言ではない。攻撃者は、フィッシング詐欺により盗んだ認証情報を利用して、本人に成りすまして金銭を引き出す。ユーザーは、金銭の請求や残高を確認するまで、自身が被害にあっているとは気付きにくく、事件の発覚が遅くなる傾向がある。

- 不正アクセス禁止法の改正

フィッシング詐欺に対する法律面の改正も行われた。2012 年 5 月に施行された、いわゆる「改正 不正アクセス禁止法」では、新たに以下の行為が取り締まり対象となった。

(1) 他人の ID/パスワード等を不正に取得する行為
(2) 入手した ID/パスワード等を他人に提供する行為
(3) 他人の ID 等を入手するためフィッシングサイトを作成して公開する行為やID等の入力を求めるメールを送信して ID 等を入手しようとする行為
(4) 他人の ID 等を不正に保管する行為

＜攻撃の手口＞

代表的なフィッシング詐欺の手口は、メールとウェブサイト(以下、フィッシングサイト)を用いて、以下の流れで行われる。

(1) 銀行やクレジットカード会社など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) メールには、「利用情報確認」などとフィッシングサイトに誘導するためのリンクが貼られている。

(3) リンクをクリックすると、見た目は本物そっくりのフィッシングサイトに誘導され、ユーザーが ID/パスワードなどを入力することで、攻撃者に盗まれてしまう。

- 巧妙化する手口

フィッシング詐欺の手口は次第に巧妙化しており、数年前からウイルスを用いる例が増えてきている。一例として、ウイルスを使って PC の hosts ファイルの情報を書き換える手口が挙げられる。ウイルスにより hosts ファイルの情報が書き換えられた PC では、正規の URL を入力しても、攻撃者が用意したフィッシングサイトに誘導されてしまう。ユーザーは、ブラウザ上に正規の URL が表示されているためフィッシングサイトだと気付きにくい。

＜2012 年の事例＞

- フィシング詐欺の被害状況 [II]

フィッシング対策協議会の発表によると、2012 年 12 月の 1 ヶ月間に同協会に寄せられたフィッシング詐欺の件数は 52 件であった。また、フィッシングサイト数は 2012 年 12 月時点で 207 件となり、1 年前の 2011 年 12 月時点での 35 件に比べて約 6 倍に増加している。

- 大手銀行を装ったフィッシング詐欺 [III]

2012 年は、大手銀行を装ったフィッシング詐欺が広く行われた。三菱東京 UFJ 銀行を装った例では、電子メールで「三菱東京 UFJ 銀行より大切なおしらせです」といったタイトルでユーザーにメールが送付された。メール本文には、URL のリンクが貼られており、個人ユーザーがリンクをクリックすることでフィッシングサイトに誘導されてしまう。フィッシングサイトは、本物と同じような画面構成であり、ログインを要求する内容になっていた。この件で、当該銀行からユーザーに注意喚起が行われた。

＜対策/対応＞

フィッシング詐欺の対策は、ユーザーが騙されないための教育・啓発や、ワンタイムパスワードや二要素認証等の強い認証方式を利用するのが良い。

- 教育/啓発
- アカウント/権限管理

参考資料

I. 改正不正アクセス禁止法
http://www.ipa.go.jp/security/ciadr/law199908.html
II. 2012/12フィッシング報告状況
http://www.antiphishing.jp/report/monthly/201212.html
III. 当行を装った不審な電子メールにご注意ください。(平成24年6月6日)
http://www.bk.mufg.jp/info/phishing/20120606.html

求められる対策

第 2 章では、2012 年において影響が大きかったセキュリティ上の脅威について、2013 年版 10 大脅威として解説してきた。これらの脅威の解説に示している対策に視点を当てると、脅威は異なるが共通する対策が多く見られる。

以下に示す対策は、新しいものではなく、10 年以上前から必要とされているものが多い。組織において十分でない対策があれば、優先的に実施していくべき対策となる。対策を実施する場合、計画を立て予算を組み、可能であれば専門家に依頼や助言を求めて、対策を実現できる適切なソリューションを選定し、段階的に導入することが重要となる。

表 3：脅威と推奨対策（対策の目安）

順位	10 大脅威タイトル	(1) ポリシー/ルール	(2) 教育/啓発	(3) システム設計	(4) 脆弱性対策	(5) ウイルス対策	(6) システム監視	(7) アカウント/権限管理
1	クライアントソフトの脆弱性を突いた攻撃			○	◎			
2	標的型諜報攻撃の脅威			◎	○		○	○
3	スマートデバイスを狙った悪意あるアプリの横行		◎			○		
4	ウイルスを使った遠隔操作		◎		○	○		
5	金銭窃取を目的としたウイルスの横行		○		◎	○		
6	予期せぬ業務停止			◎			○	○
7	ウェブサイトを狙った攻撃			◎	○		○	○
8	パスワード流出の脅威		○	○				◎
9	内部犯行	○		○			○	◎
10	フィッシング詐欺		◎					○

【凡例】　◎：最も実施/強化しておくべき対策　　○：実施/強化しておくことが望ましい対策

（IPA 執筆者により選定）

対策一覧

導入時に検討する対策
(1) ポリシー/ルール
セキュリティポリシーなどの文書によって、不要なサイトの閲覧や不要なソフトの利用など、組織にとって望ましくない行動の禁止をユーザーに明示することは、企業/組織がセキュリティを維持するために必要な対策となる。 代表的な対策 ◆ ポリシー策定 ◆ ルール策定
(2) 教育/啓発
脅威について事前に知っておかなければ、攻撃や被害に気付くことや、適切に対応することが難しくなる。どの脅威に対しても、教育や啓発活動は一定の効果を得ることができる。 代表的な対策 ◆ セキュリティ教育実施 ◆ セキュリティ啓発資料の配布
(3) システム設計
システムの導入段階において、脅威や想定する攻撃を考慮した上で、セキュリティに考慮したシステムを検討する。ネットワーク設計とセキュリティソリューションの導入が重要であるが、ミスを起こさない手順の確立など実運用を見据えた運用設計も重要となる。 また、事業継続の観点に立ち、重要データのバックアップや復旧方式の検討など、データ消失のリスクに対しても検討しておく必要がある。 代表的な対策 ◆ ネットワーク機器やセキュリティソリューションの導入 ◆ 認証方式の検討 ◆ ログ設計（取得対象選定と容量計算） ◆ バックアップ設計 ◆ 事業継続計画策定 ◆ セキュリティ診断の実施

運用時に実施する対策

(4) 脆弱性対策

新しく公開されたセキュリティアップデート（パッチ）を日々適用していくことが、攻撃者やウイルスから PC やサーバーを乗っ取られないために重要な対策となる。パッチ管理（資産管理）ソリューションや検疫ソリューションを導入することにより、管理や適用の徹底を実現することが可能となる。

代表的な対策
- 自動アップデート
- パッチ管理
- 検疫（未対策端末の排除）

(5) ウイルス対策

ウイルス対策ソフトウェアを導入することが、ウイルスやマルウェアから PC やサーバーを守るために最も有効な対策となる。新種のウイルスにも対応できるパターンファイルだけに頼らない検出方式を採用しているウイルス対策ソフトウェアやアプライアンスもあり、今後の採用のポイントとなる。また、検疫ソリューションを導入することにより、ウイルスパターンファイルの古い端末をネットワークから隔離することが可能となる。

代表的な対策
- ウイルス対策ソフトウェアやアプライアンスによる端末の保護
- 検疫（未対策端末の排除）

(6) システム監視

外部からの攻撃やシステムの異常を監視し、有事発生時に迅速に対応することは重要となる。ログ監視などの監視ソリューションを導入することにより、攻撃を検知しブロックすることが可能となる。

代表的な対策
- 侵入検知/防御システム（IDS/IPS）による監視
- ログの監視

(7) アカウント/権限管理

ユーザーが、十分な長さを持ち容易に推測されないパスワードを使用する、サービスごとに別のパスワードを使用するといった自衛策を取ることが重要である。ユーザーに強度のあるパスワードを強要する設定や、ワンタイムパスワードなどの認証ソリューションを導入して、システム的に対策することも求められる。また、各ユーザーには、必要以上の権限を与えず、適切に権限を付与し、情報資産を継続的に保護する必要がある。

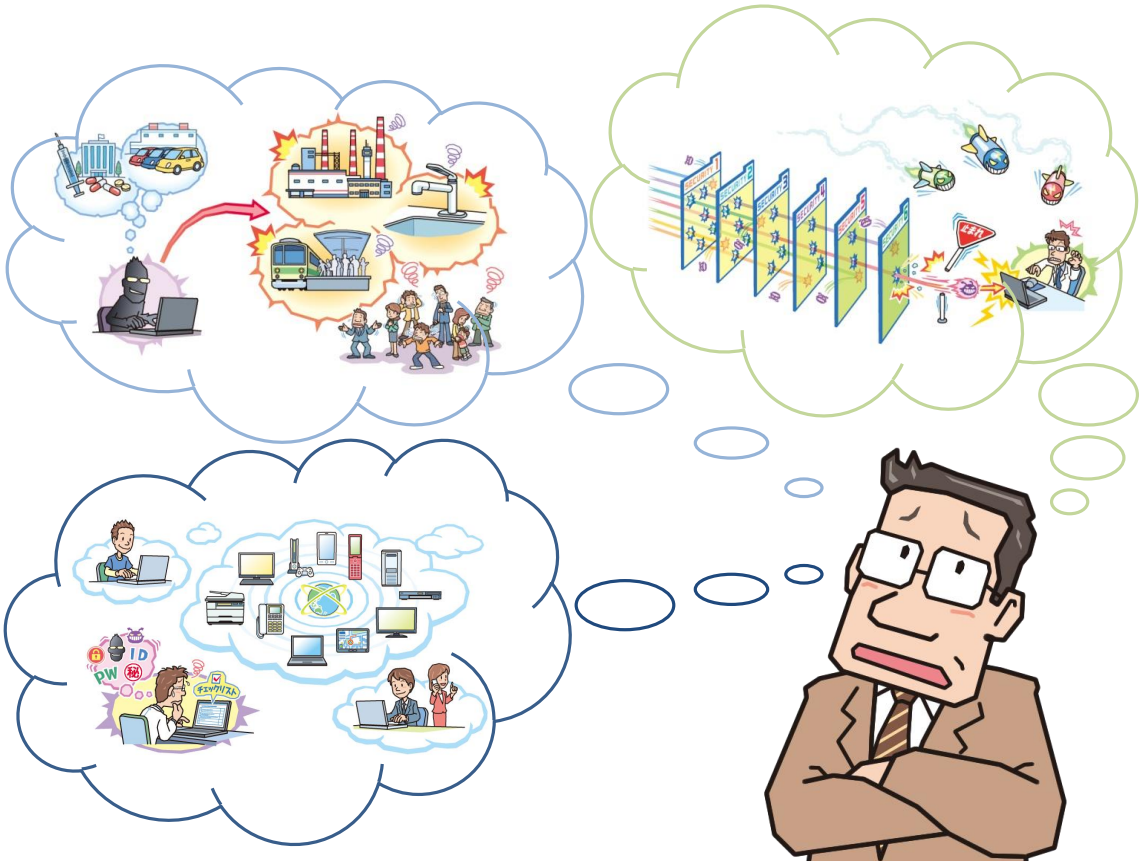
代表的な対策
- ワンタイムパスワードや二要素認証など強度が高い認証の利用
- 権限の管理（アクセス制限の実施）

3章. 今後注目すべき脅威

情報セキュリティを取り巻く環境は、情報技術の革新、新しいサービスモデルの出現などにより、利便性が向上した反面、新たな脅威が顕在化してくる。今後、社会的影響が大きくなると予想される脅威について、「10 大脅威執筆者会」の投票結果に基づき、表４のように順位付けした。本章では、下記３つのテーマについて解説する。

表４：今後注目すべき脅威

順位	タイトル
1	**クラウド利用における課題** ～クラウドサービスの拡大と新たな懸念～
2	**重要インフラを狙った攻撃** ～様々な技術分野へ広がる脅威～
3	**既存対策をすり抜ける攻撃の広がり** ～攻撃の全体像を把握したセキュリティ対策を～



3.1. クラウド利用における課題

～クラウドサービスの拡大と新たな懸念～

クラウドサービスは、業務システム、個人向けストレージ、災害時の代替システムなど様々な用途で活用されている。一方で、個人によるクラウド利用の拡大に伴い、内部データをクラウド上の無料ストレージへ複製されるなど、システム管理者にとって新たな課題が出てきている。

＜クラウドの拡大＞

IDC[I] の予測によると、2012 年のパブリッククラウド市場は前年比 46.0%増の 941 億円になる見込みで、2016 年には 3027 億円に達すると試算されている。

クラウドとは、インターネット環境を利用したサービス全般を指し、業務システムを提供しているものからインフラ環境を提供しているサービスまで様々な形態が存在する。また、企業ユーザーにとどまらず、個人向けストレージや動画サービスなど、一般ユーザーにとって身近な存在になっている。また、今後ソーシャルクラウド[II]と言われるクラウド基盤を、医療、農業、行政といった分野へ提供することが検討されており、クラウドサービスによる IT 社会の構築が進められている。

＜クラウドを利用することの利点＞

クラウドサービスを利用することの主な利点として、以下のような点が挙げられる。

- システム導入・運用コストの低減

システムを自前で用意するのに比べ、システムの調達・構築の手間が省け、運用に係る諸費用も抑えることができる。

- 使いたい時にどこからでも利用可能

インターネットが繋がる環境であれば、職場だけでなく自宅や出先での操作を可能とし業務効率の向上が期待できる。

- 災害時の代替として最適

災害等でシステムに障害が起きた場合でも、クラウドサービスであれば、短期間での代替が可能となる。

また、企業ユーザーだけでなく個人ユーザ

ーにおいても、写真、動画、音楽等のコンテンツをオンラインストレージ上で一元的に保存できることで、自宅の PC やスマートフォンなどの複数デバイスでいつでも自由に利用することが可能になる。

＜クラウドにおけるセキュリティ事故＞

一方でクラウドサービスに関する事故も発生している。実際に発生している事故は大別して下記の3つである。

(1) ハードウェア障害
(2) オペレーションミス
(3) アクセス権の奪取

(1)(2)については、ハードウェア障害や事業者側のオペレーションミスによりデータを消失するケースがある。クラウド利用者としては、データの重要度に応じて、適切にバックアップを行うことが求められる。クラウド事業者から提示される約款を十分に理解した上で、自社の運用に即したクラウド事業者を選ぶことが重要である。

(3)については、クラウドサービスはインターネット環境越しに利用することが基本であるため、パスワードの漏えいにより、アカウントを乗っ取られるリスクがある。

対策としては、アカウントやパスワードを適切に管理することやデータや業務の重要度に応じて二要素認証などの認証オプションが豊富なサービスの利用を検討するのが良い。

＜システム管理者の留意点＞

クラウドの広がりと共にシステム管理者が留意しなければならない事項が見えてきた。

- インシデント対応

クラウドサービスを利用する上で留意しなければならないのは、サービスによってクラウド利用者が行える管理操作が制限されていることが想定される。例えば、自前システムであれば容易にできたログの収集や分析も、クラウドサービスでは実施できない場合がある。とりわけセキュリティ事故が発生した場合、ログの提供を受けられず被害状況が確認できない等の不都合が考えられる。このような点も踏まえて、セキュリティ事故発生時に情報が調査・追跡できるように、事前にクラウド事業者に確認しておくことが重要である。

- 個人向けサービスの利用

個人向けクラウドサービスの活況と共に組織・企業のシステム管理者にとって悩ましい問題も出てきた。近年、業務効率の向上を目的として、スマートフォンやタブレット PC などの個人が所有するデバイスを職場に持ち込んだり、個人が契約したサービスを業務に利用したりするケースが出てきた。その際に、業務データが個人所有のデバイスやストレージサービスに保管されることが想定され、不用意に業務データが外部に持ち出されてしまう危険性が考えられる。また、スマートフォンやタブレット PC に対応したクラウドサービスの普及に伴い、データの移動が活発化し、情報管理が難しくなってきている。

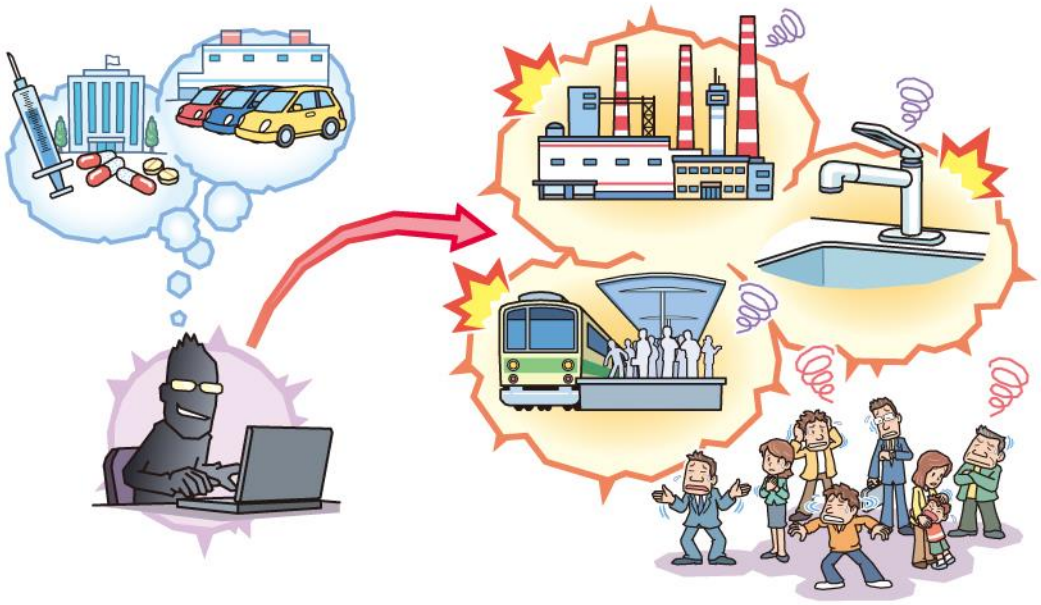
個人契約のデバイスの利用においても、情報の重要度に応じた一定のルール化やシステム的な制限の検討が必要となっている。

参考資料

I. IDC: 国内パブリッククラウド市場、2016年には3000億円超え
http://www.itmedia.co.jp/enterprise/articles/1211/05/news056.html
II. 平成23年度 次世代高信頼・省エネ型IT基盤技術開発・実証事業（ソーシャルクラウド基盤技術に関する調査研究）
http://www.meti.go.jp/policy/mono_info_service/joho/cloud/2011/10_01.pdf

3.2. 重要インフラを狙った攻撃

～様々な技術分野へ広がる脅威～



これまでサイバー攻撃とは縁の薄かった、制御システム(とりわけ重要インフラシステム)への攻撃が懸念されており、国内外で対策が急がれている。また、自動車やメディカルデバイスといった機器の脆弱性も公表され、対策に向けた活動が行われている。

＜重要インフラを狙った攻撃＞

我々の生活を支えている、エネルギー（電力、ガス、石油他）、生産ライン、化学プラント、輸送、通信などの重要インフラと呼ばれる設備も複数のコンピュータとネットワークで構成されている。これらのシステムは、中央コンピュータで産業機器・装置を制御しながら、システムを運用している。

近年、この重要インフラに対するサイバー攻撃が増加傾向にある。米国 DHS の公表によれば、2009 年から 2011 年の 3 年間の米国内の制御システムインシデントの報告件数[1]はそれぞれ 9 件、41 件、198 件となっている。このような状況下において、制御システムへのサイバーセキュリティ対策は国家の安全保障、危機管理上の重要な課題となりつつある。

＜制御システムの汎用化＞

重要インフラへの攻撃が懸念される背景の一つには制御システムの環境変化が挙げられる。制御システムを構築する際、従来は可用性を重視し、認証等行わずに、閉域ネットワーク前提で個々のシステムごとに閉じた設計が行われていたため、サイバー攻撃の危険性は低いと考えられていた。しかし、昨今は、国内外において汎用製品や標準プロトコルの活用が進んでおり、汎用的なネットワークとの接続により利便性が向上している反面、攻撃を受ける危険性も高まりつつある。

＜重要インフラが狙われることの影響＞

制御システムが攻撃を受けた場合、機器が故障、誤動作するなどの「物理的な被害」が考えらえる。

電気・ガス・水道・交通といった重要インフラが攻撃を受け物理的な被害が発生した場合、我々の社会生活に甚大な影響を及ぼしてしまう可能性がある。国内での重要インフラに対する攻撃の報道は表立っていないが、海外では既に攻撃が報道されている。

＜重要インフラセキュリティの取組み＞

重要インフラへのセキュリティ対策に関する取組みとして、国内外で以下の取組みが行われている。

- 制御システムセキュリティセンター設立

日本国内では、2012 年 3 月に重要インフラを含む制御システムのセキュリティを確保するため、研究開発、国際標準化活動、認証、人材育成、普及啓発を目的に「技術研究組合制御システムセキュリティセンター」が設立[II]された。

- 認証制度

海外では、制御システムセキュリティに関する国際規格の整備が進むとともに、規格に基づく認証制度が確立されてきており、制御システムの輸出の際の要件にも加わり始めている。

＜その他のシステムへの攻撃拡大の懸念＞

スマート家電やスマートフォンなど、常時インターネットに繋がり、インターネットを通じてさまざまな機能を利用できる機器が増えてきた。この傾向は、自動車やメディカルデバイスにも波及し応用されており、これによって新たな脅威が懸念されるようになった。

- 自動車のセキュリティ

近年、自動車の装備にカーナビゲーションや車載カメラなど情報通信技術が導入されており、スマートフォンやタブレットと連携できるようになるなど用途も多様化している。

2010 年には米国の研究者等により、自動車内外からの通信によって車載システムの脆弱性を攻撃することで、特定の自動車の制御等に影響を与えることが可能であることが明らかとなった。自動車におけるセキュリティの重要性も増してきている。[III]

- メディカルデバイスの脆弱性

2011 年に米国の研究者がインスリンを投与するメディカルデバイスをハッキングし、遠隔操作できることを実証した。また、アメリカ会計検査院のレポートが、インスリンポンプや ICD（植込み型除細動器）といった医療機器について、ハッキングによる遠隔操作が脅威になりうると警告している。[IV]

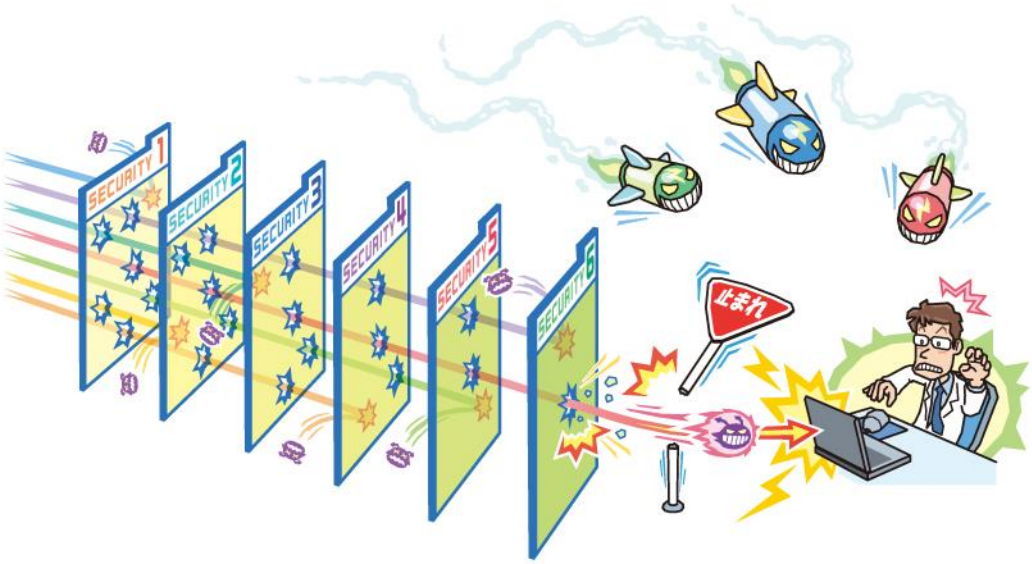
自動車やメディカルデバイスが攻撃を受けた場合、生命の安全性が脅かされかねない。自動車やメディカルデバイスへの攻撃は、現在のところ研究者による実証実験レベルであり、攻撃事例はないが、攻撃者の意図次第で脅威が高まることを忘れてはならない。

参考資料

I. DHS:ICS-CERT Incident Response Summary Report
http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Incident_Response_Summary_Report_09_11.pdf
II. 技術研究組合制御システムセキュリティセンター
http://www.css-center.or.jp/ja/aboutus/index.html
III.「2011年度 自動車の情報セキュリティ動向に関する調査」報告書の公開
http://www.ipa.go.jp/security/fy23/reports/emb_car/index.html
IV. MEDICAL DEVICES
http://www.gao.gov/assets/650/647767.pdf

3.3. 既存対策をすり抜ける攻撃の広がり

～攻撃の全体像を把握したセキュリティ対策を～



2010 年頃より特定のミッションに特化した高度な作りのウイルスが発見されており、セキュリティ関係者の間で話題となっている。また、高度なウイルスに限らず、既存のセキュリティ対策では、検知できない手法やウイルスが攻撃の主流になりつつあり、攻撃の全体像が掴みにくい傾向にある。攻撃の入口で検知・遮断に頼る対策から、攻撃の全体像を把握したセキュリティ対策が重要となる。

＜高度なウイルスの登場＞

2012 年は、2010 年のイランの原子力施設を狙ったとされる「Stuxnet」に続いて、「Flame[I]」「Gauss[II]」といった第二、第三の Stuxnet と呼ばれる高度な作りのウイルスが登場した。これらのウイルスは、通常のウイルスと異なり、プログラムサイズも大きく、攻撃内容も高度であることから、サイバー犯罪集団の仕業ではなく、政府が背後にある可能性が高いと見られている。

＜攻撃の背景＞

これらのウイルスは、特定の地域に感染が集中している。「Flame」は、イラン、イスラエル、スーダン、シリア、レバノンといった中東地域に集中している。また、「Flame」には、ネットワークトラフィックの傍受、スクリーンショットの保存、音声通話の記録といった機能を有しており、諜報・スパイ行為を行う目的で作られたと見られている。

また、「Gauss」に至っては、パスワードやインターネットバンキングのログイン情報、システム設定データ等を窃取する機能を備えている。これだけ読むと、通常のスパイウェアと変わらないと思われるかもしれないが、感染地域が中東のレバノンに集中していることから、

攻撃者はレバノンに対して何らかの攻撃の意図を持っていると言われている。

これら高度なウイルスは、ある特定のミッションの下に多くの労力と工数を掛けて開発されたと見られており、背景には国家などの大きな組織の関与が噂されている。日本がこのような高度なマルウェアに狙われたという事実は今のところないが、攻撃者の興味や目的が日本に向いた時、同様の脅威に晒される可能性が考えられる。

＜攻撃検知の限界＞

高度なウイルスに限らず、ウイルス対策ソフトによるウイルス検知をすり抜ける攻撃が主流になりつつある。ウイルス対策ソフトは、世界中に配置してあるウイルスの検知センサーで検知したウイルスを解析し、ウイルスのパターンを定義ファイルに格納している。しかし、これらの対応は、ウイルスの種類が少なければ対応できるが、種類が増え続ける状況では、解析が追い付かない。また、個別に作り込まれたウイルスについては、検知するのは極めて困難である。

また、近年の攻撃では、リモートメンテナンス用のソフトウェアが攻撃に悪用されるケースが見られる。これらのソフトウェアは便利である反面、攻撃により悪用された場合、管理のためのアクセスか攻撃によるアクセスかの区別が付かず、攻撃を検知することができない。例えば、遠隔操作ツールなどは、正しい使い方をすれば、PC やサーバーにリモートでアクセスでき、遠隔でのヘルプデスクや運用を行うことができる。しかし、悪意を持って使用すると、他人の PC を乗っ取り、その人に成りすまして様々な悪事を働くことができてしまう。

＜セキュリティ対策＞

このように、悪意あるプログラムと悪意のないプログラムの判別が難しくなっており、既存のセキュリティ対策をすり抜ける攻撃が増えてきている。そのため、全ての攻撃を社内ネットワークの入口で堰き止めるのは困難であり、ウイルスを内部に侵入させても被害を最小限にとどめる対策を考える必要がある。

- 全体像を把握したセキュリティ対策

ウイルスの共通的な特徴として、外部の攻撃者サーバーと通信を行い、新たな攻撃を仕掛けてくることがある。そのため、外部と通信させにくいシステム設計、ネットワーク構成を組むことや、ログなどから異常を検知するようシステムを設計で工夫することが重要である。

- セキュリティパッチの適用

世の中の攻撃の大半は、ソフトウェアの脆弱性を悪用して攻撃が行われる。ソフトウェアの脆弱性とは、防御側からすると弱点(ウィークポイント)となり、逆に攻撃者側から見るとアタックポイントになる。そのため、既知の脆弱性を放置しない様に、常に最新のセキュリティパッチを適用することが望ましい。

参考資料

I. 高度なターゲット型マルウエア「Flame」、政府主導の攻撃か
http://itpro.nikkeibp.co.jp/article/NEWS/20120529/399281/
II. Kaspersky Lab がオンラインバンキングアカウントを監視する高度なサイバー脅威「Gauss」を新たに発見
http://www.kaspersky.co.jp/news?id=207585649

[付録] その他 10 大脅威候補

ここでは、2013 年版 10 大脅威には選定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.　内部から発生する情報漏えい

ファイル共有ソフト（P2P）を介して、業務情報や個人情報が漏えいしてしまう事例が後を絶たない。USB メモリだけでなく、スマートフォンやタブレットなどのモバイル機器やクラウド上のストレージも、持ち出し媒体として利用可能な現状があり、多くの管理者が頭を悩ませている。

- NTT西日本、顧客情報3,140件および電話番号21万件がWinnyで流出
  http://internet.watch.impress.co.jp/cda/news/2006/12/05/14135.html
- 水道利用者4059人の個人情報流出　秋田市、「ウィニー」通じ
  http://www.nikkei.com/article/DGXNASDG22043_T20C12A8CC0000/

12位.　証明書を悪用した攻撃

2011 年に発生した、認証局が不正アクセスを受けて偽の証明書が発行されてしまった事件は、世間に大きなインパクトを与えた。2012 年、マルウェア Flame がプレフィックスの衝突により生成した偽のマイクロソフトの証明書を使用し Windows Update を悪用した。認証局の技術基盤は、信頼型の技術モデルであるため、偽の証明書は基盤そのものの信用を揺るがす問題になっている。

- 「Windows Update」をハッキングする「Flame」マルウェア、制作には世界トップクラスの暗号解析技術が必要と研究者
  http://www.computerworld.jp/topics/666/203423
- 偽装証明書が失効されているか確認を ？「Flame」の不正証明書問題
  http://www.security-next.com/31527

13位.　DNS を狙った攻撃

2011 年と 2012 年に話題になった DNS Changer をはじめとするマルウェアは DNS を悪用してターゲットを偽のサイトに誘導する。また、2012 年は、幽霊ドメイン名の問題や、DNS として普及している BIND の新しい脆弱性が数か月おきに公表され、世界中の DNS サーバーが攻撃の対象になりやすい状態となっている。レジストラが管理する DNS 情報が書き換えられる被害も発生している。

- DNSサーバーの実装に脆弱性、“幽霊ドメイン名”がキャッシュされ続ける
  http://internet.watch.impress.co.jp/docs/news/20120210_511317.html
- DNSサーバーの「BIND 9」に重大な脆弱性、企業などのキャッシュサーバーにも影響
  http://itpro.nikkeibp.co.jp/article/NEWS/20120605/400443/
- 「BIND 9」にDoS攻撃が可能な脆弱性、ISCが修正版をリリース
  http://cloud.watch.impress.co.jp/docs/news/20121011_565205.html

14位.　SNS 利用者を狙った攻撃(短縮 URL やソーシャルエンジニアリング等)

SNS は攻撃のインフラに利用されるようになっている。主に SNS に貼られた悪意のあるリンクを用いて、詐欺、マルウェアに感染させる攻撃や、スパムを拡散させる攻撃が発生している。また、SNS で公開されている個人情報が、攻撃の事前情報として利用されている。

- OAuthを悪用したアカウント乗っ取りに注意喚起、IPA
  http://www.atmarkit.co.jp/ait/articles/1210/01/news147.html
- 詐欺サイトへの誘導はメールからSNSへ
  http://is702.jp/special/1119/partner/101_g/

15位.　ハクティビストによる攻撃

日本の改正著作権法に反対した Anonymous による OpJapan、日本を含む世界各国の大学の情報を狙った攻撃、尖閣諸島問題を起因とした攻撃など、日本においてもハッカー（ハクティビスト）グループによるとされる攻撃があった。

- Anonymousが日本政府とレコード協会に“宣戦布告” 違法ダウンロード刑事罰化に抗議
  http://www.itmedia.co.jp/news/articles/1206/26/news064.html
- ハッカー集団、世界100大学の個人情報など12万件を暴露　日本の大学名も
  http://www.itmedia.co.jp/enterprise/articles/1210/03/news021.html
- 総務省や最高裁、銀行など国内19ウェブサイトにサイバー攻撃　中国で攻撃予告
  http://sankei.jp.msn.com/affairs/news/120919/crm12091915430030-n1.htm

16位.　ソフトウェアの不正コード挿入

オープンソースソフトウェアの公式サイトで公開されているソースコードに不正なコードが挿入された問題が度々発生する。そのソースコードを利用することで、気付かぬうちにマルウェアに感染してしまう危険性がある。

- phpMyAdmin における任意の PHP コードを実行される脆弱性
  http://jvndb.jvn.jp/ja/contents/2012/JVNDB-2012-004599.html
- FreeBSD の開発･配布マシン群への不正侵入発生について
  http://www.freebsd.org/ja/news/2012-compromise.html

17位.　無線 LAN の盗聴や不正利用

暗号化されていないホットスポットや WEP のアクセスポイントへの接続には、盗聴などの危険が潜んでいる。また、悪意のある第三者に企業や自宅のアクセスポイントに接続され、不正アクセスを受けたり、攻撃の踏み台に利用されたりする危険がある。また、2011 年 12 月に公表された無線 LAN の規格 WPS 脆弱性には、総当たり攻撃で PIN 情報を取得される可能性がある。

- 無料の無線LAN「connectFree」、ユーザーからTwitter IDや閲覧URLなど無断取得
  http://www.itmedia.co.jp/news/articles/1112/07/news053.html
- Wi-Fi Protected Setup (WPS) におけるブルートフォース攻撃に対する脆弱性
  http://jvn.jp/cert/JVNTA12-006A/

18位.　IP 電話の不正利用による損害

攻撃者が IP 電話のユーザーID/パスワードを盗み取り、国際電話を不正に発信することで、身に覚えの無い料金を請求される被害が続いている。個人や企業などの IP 電話利用者を狙った攻撃は今後も続くとみられている。

- 社団法人日本インターネットプロバイダー協会 IP電話の不正利用による国際通話に関する注意喚起について
  http://www.jaipa.or.jp/topics/?p=530
- アイ･ ティ･エックス株式会社【おしらせ】IP 電話の不正利用による国際通話について
  http://moranet.jp/biz-park/img/moraphone.pdf

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	古田 洋久	(社)JPCERT コーディネーションセンター
木村 道弘	(株)ECSEC Laboratory		(JPCERT/CC)
高橋 潤哉	(株)イード	宮崎 清隆	(社)JPCERT コーディネーションセンター
加藤 雅彦	(株)インターネットイニシアティブ		(JPCERT/CC)
齋藤 衛	(株)インターネットイニシアティブ	宮地 利雄	(社)JPCERT コーディネーションセンター
高橋 康敏	(株)インターネットイニシアティブ		(JPCERT/CC)
梨和 久雄	(株)インターネットイニシアティブ	林 薫	(株)シマンテック
三輪 信雄	S&J コンサルティング(株)	山内 正	(株)シマンテック総合研究所
石川 朝久	NRI セキュアテクノロジーズ(株)	徳田 敏文	(株)シンプレクス・コンサルティング
大塚 淳平	NRI セキュアテクノロジーズ(株)	神薗 雅紀	(株)セキュアブレイン
小林 克巳	NRI セキュアテクノロジーズ(株)	星澤 裕二	(株)セキュアブレイン
正木 健介	NRI セキュアテクノロジーズ(株)	青谷 征夫	ソースネクスト(株)
中西 克彦	NEC ネクサソリューションズ(株)	唐沢 勇輔	ソースネクスト(株)
杉浦 芳樹	NTT-CERT	澤永 敏郎	ソースネクスト(株)
住本 順一	NTT-CERT	百瀬 昌幸	(財)地方自治情報センター(LASDEC)
種茂 文之	NTT-CERT	杉山 俊春	(株)ディー・エヌ・エー
井上 克至	(株)NTT データ	大浪 大介	(株)東芝
入宮 貞一	(株)NTT データ	田岡 聡	(株)東芝
西尾 秀一	(株)NTT データ	長尾 修一	(株)東芝
池田 和生	NTTDATA-CERT	吉松 健三	(株)東芝
林 健一	NTTDATA-CERT	小島 健司	東芝ソリューション(株)
宮本 久仁男	NTTDATA-CERT	小屋 晋吾	トレンドマイクロ(株)
やすだ なお	NPO 日本ネットワークセキュリティ協会	大塚 祥央	内閣官房情報セキュリティセンター
	(JNSA)	恩賀 一	内閣官房情報セキュリティセンター
前田 典彦	(株)Kaspersky Labs Japan	佐藤 朝哉	内閣官房情報セキュリティセンター
山崎 英人	カルチュア・コンビニエンス・クラブ(株)	須川 賢洋	新潟大学
秋山 卓司	クロストラスト(株)	田中 修司	日揮(株)
加藤 耕三	経済産業省	井上 博文	日本アイ・ビー・エム(株)
小熊 慶一郎	(株)KBIZ	守屋 英一	日本アイ・ビー・エム(株)
鈴木 啓紹	(社)コンピュータソフトウェア協会(CSAJ)	宇都宮 和顕	日本電気(株)
野渡 志浩	(株)サイバーエージェント	谷川 哲司	日本電気(株)
名和 利男	(株)サイバーディフェンス研究所	榎本 司	日本ヒューレット・パッカード(株)
福森 大喜	(株)サイバーディフェンス研究所	西垣 直美	日本ヒューレット・パッカード(株)
大岩 寛	(独)産業技術総合研究所	佐藤 直之	日本ベリサイン(株)
高木 浩光	(独)産業技術総合研究所	大村 友和	(株)ネクストジェン
伊藤 友里恵	(社)JPCERT コーディネーションセンター	金 明寛	(株)ネクストジェン
	(JPCERT/CC)	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	圓山 大介	(株)ネクストジェン
	(JPCERT/CC)	山下 潤一	ネットエージェント(株)
		徳丸 浩	HASH コンサルティング(株)

氏名	所属	氏名	所属
水越 一郎	東日本電信電話(株)	青木 歩	(株)ユービーセキュア
太田 良典	(株)ビジネス・アーキテクツ	佐藤 健	(株)ユービーセキュア
吉野 友人	(株)ビジネス・アーキテクツ	松岡 秀和	(株)ユービーセキュア
寺田 真敏	Hitachi Incident Response Team	志田 智	(株)ユビテック
藤原 将志	Hitachi Incident Response Team	福本 佳成	楽天(株)
丹京 真一	(株)日立システムズ	伊藤 耕介	(株)ラック
本川 祐治	(株)日立システムズ	岩井 博樹	(株)ラック
梅木 久志	(株)日立製作所	川口 洋	(株)ラック
鵜飼 裕司	(株)フォティーンフォティ技術研究所	長野 晋一	(株)ラック
金居 良治	(株)フォティーンフォティ技術研究所	柳澤 伸幸	(株)ラック
国部 博行	富士通(株)	山崎 圭吾	(株)ラック
森 玄理	富士通(株)	若居 和直	(株)ラック
金谷 延幸	(株)富士通研究所	中田 邦彦	ルネサスエレクトロニクス(株)
岡谷 貢	(株)富士通システム総合研究所	笹岡 賢二郎	(独)情報処理推進機構(IPA)
望月 大光	(株)富士通ソフトウェアテクノロジーズ	小林 偉昭	(独)情報処理推進機構(IPA)
高橋 正和	マイクロソフト(株)	金野 千里	(独)情報処理推進機構(IPA)
国分 裕	三井物産セキュアディレクション(株)	島 成佳	(独)情報処理推進機構(IPA)
後藤 久	三井物産セキュアディレクション(株)	加賀谷 伸一	(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)	渡辺 貴仁	(独)情報処理推進機構(IPA)
川口 修司	(株)三菱総合研究所	大森 雅司	(独)情報処理推進機構(IPA)
村瀬 一郎	(株)三菱総合研究所	棚町 範子	(独)情報処理推進機構(IPA)
村野 正泰	(株)三菱総合研究所	中西 基裕	(独)情報処理推進機構(IPA)

IPA 協力者

松坂 志　　勝海 直人　　相馬 基邦　　木曽田 優　　田中 健司

著作・制作　　独立行政法人情報処理推進機構（IPA）

編集責任　　小林 偉昭　 金野 千里

イラスト制作　　日立インターメディックス株式会社

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

2013 年版

10 大脅威 『身近に忍び寄る脅威』

2013 年 3 月 12 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/

情報セキュリティに関する届出について

IPA セキュリティセンターでは、経済産業省の告示に基づき、コンピュータウイルス・不正アクセス・脆弱性関連情報に関する発見・被害の届出を受け付けています。

ウェブフォームやメールで届出ができます。詳しくは下記のサイトを御覧ください。
URL: http://www.ipa.go.jp/security/todoke/

コンピュータウイルス情報

コンピュータウイルスを発見、またはコンピュータウイルスに感染した場合に届け出てください。

不正アクセス情報

ネットワーク（インターネット、LAN、WAN、パソコン通信など）に接続されたコンピュータへの不正アクセスによる被害を受けた場合に届け出てください。

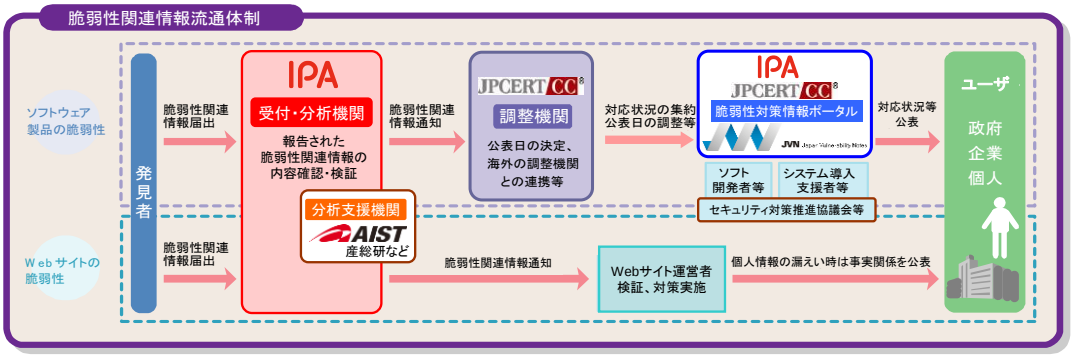
ソフトウエア製品脆弱性関連情報

OSやブラウザ等のクライアント上のソフトウエア、ウェブサーバ等のサーバ上のソフトウエア、プリンタやICカード等のソフトウエアを組み込んだハードウエア等に対する脆弱性を発見した場合に届け出てください。

ウェブアプリケーション脆弱性関連情報

インターネットのウェブサイトなどで、公衆に向けて提供するそのサイト固有のサービスを構成するシステムに対する脆弱性を発見した場合に届け出てください。

脆弱性関連情報流通の基本枠組み「情報セキュリティ早期警戒パートナーシップ」



※IPA：独立行政法人 情報処理推進機構、JPCERT/CC：一般社団法人 JPCERT コーディネーションセンター、産総研：独立行政法人 産業技術総合研究所

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/

セキュリティセンター
TEL: 03-5978-7527 FAX 03-5978-7518
http://www.ipa.go.jp/security/