2011年版

10大脅威

「進化する攻撃…
その対策で十分ですか?」

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

2011年3月

目次

本書は、次の URL からダウンロードできます。

2011 年版

10 大脅威『進化する攻撃…その対策で十分ですか？』

http://www.ipa.go.jp/security/vuln/10threats2011.html

2011 年版　10 大脅威

『進化する攻撃…その対策で十分ですか？』

はじめに

本資料は、「情報セキュリティ早期警戒パートナーシップ」に参画する関係者のほか、情報セキュリティ分野の研究者、実務担当者等 127 名から構成される「10 大脅威執筆者会」により 2010 年の 10 大脅威をまとめたものである。

本資料における「脅威」とは、自組織へ何らかの損害を与える情報セキュリティにおける事象である。「リスク」とは、その「脅威」によって自組織にもたらされる損害や危険に遭う可能性である。「ビジネスインパクト」とは、「リスク」が自組織のビジネスやサービス継続に及ぼす影響の度合いである。

組織は対策を進める際に、事業の継続管理の考えに従って、脅威が自組織に及ぼすビジネスインパクトを分析・評価し、適切な対策をしていく必要がある。本資料を活用することで、近年の情報セキュリティを取り巻く状況の理解や、今後の対策の参考になることを期待する。

本資料の構成

本資料は、3つの章から構成されている。

第1章では、2010 年に実際に発生した被害事例を基に、組織にとってのビジネスインパクトを考察している。

第2章では、2010 年に「社会的影響が大きいもの」「印象が強かったもの」等の観点からまとめた10大脅威についてそれぞれ解説と影響を説明している。10 大脅威については、「10 大脅威執筆者会」の投票結果に基づき、表 1 のように順位付けした。

第3章では、セキュリティ対策の考え方や方向性について述べている。

2011 年版 10 大脅威の総括

2010 年には、複数の攻撃手法を組み合わせた新しいタイプの攻撃の出現、情報資産管理の不備による情報漏えい、スマートフォンを対象にしたウイルスの発生、ミニブログサービスの利用者を狙った攻撃等、様々なセキュリティ事件・事故が発生した。

特に、Stuxnet（スタックスネット）を代表とする複数の攻撃を組み合わせた新しいタイプの攻撃は、制御システム等の今まで不可能と考えられていた領域に対しての攻撃が現実のものとなってきている。

また、不正な情報持ち出しやノート PC 紛失等の「人」が起こしてしまう情報漏えいに関しては、個人が手軽に情報を発信できるウェブサービスが発達したことにより、資産管理の重要性が再認識された。参考までに、2010 年上半期に起きた情報漏えいの発生件数および想定損害賠償総額等を表 2に、事件・事故 1 件あたりの個人情報が漏えいした人数を表 3 に示す。

その他、普及が加速しているスマートフォンを対象にしたウイルスが確認された点や、ミニブログサービスにおいてクロスサイト・スクリプティングの脆弱性を悪用した問題や短縮 URL を悪用したウイルス感染サイトへの誘導が確認された点が特徴的であった。

情報資産を狙った攻撃はより複雑・高度に進

化している。そのため、これまでの対策では不十分な場合が出てきた。現実に存在する「脅威」が自組織に対してどのような「リスク」を生じさせ、どのような「ビジネスインパクト」を及ぼすかを考慮したうえで、自組織に適した対策をしていただきたい。

表 1：2011 年版 10 大脅威

順位	10 大脅威
1 位	「人」が起こしてしまう情報漏えい
2 位	止まらない！ウェブサイトを経由した攻撃
3 位	定番ソフトウェアの脆弱性を狙った攻撃
4 位	狙われだしたスマートフォン
5 位	複数の攻撃を組み合わせた新しいタイプの攻撃
6 位	セキュリティ対策不備がもたらすトラブル
7 位	携帯電話向けウェブサイトのセキュリティ
8 位	攻撃に気づけない標的型攻撃
9 位	クラウド・コンピューティングのセキュリティ
10 位	ミニブログサービスや SNS の利用者を狙った攻撃

表 2：2010 年上半期 個人情報漏えいに関するデータ

漏えい人数	127 万 383 人
インシデント件数	684 件
想定損害賠償総額	364 億 3705 万円
一件当たりの平均漏えい人数	1951 人
一件当たり平均損害賠償額	5597 万円
一人当たり平均損害賠償額	4 万 823 円

（出典）JNSA：2010年情報セキュリティインシデントに関する調査報告書【上半期 速報版】

表 3：2010 年上半期 個人情報漏えい人数

No.	漏えい人数	業種	原因
1	20 万 1414 人	学術研究，専門・技術サービス業	管理ミス
2	19 万 7907 人	情報通信業	盗難
3	17 万　325 人	金融業，保険業	管理ミス
4	10 万　　人	情報通信業	紛失・置忘れ
5	9 万　700 人	金融業，保険業	管理ミス
6	6 万 3805 人	サービス業	盗難
7	5 万 1300 人	金融業，保険業	管理ミス
8	3 万 3600 人	金融業，保険業	管理ミス
9	2 万 7998 人	金融業，保険業	管理ミス
10	1 万 5521 人	金融業，保険業	管理ミス

（出典）JNSA：2010年情報セキュリティインシデントに関する調査報告書【上半期 速報版】

10 大脅威分類図

2011 年版 10 大脅威を下記のように3つのカテゴリに分類した。分類した結果を図 1 に示す。

(1)「外部から攻撃される脅威」
(2)「情報漏えいの脅威」
(3)「情報システムの設計・実装や運用に起因する脅威」

外部ネットワークや電子媒体を経由した情報システムを脅かす攻撃に該当するものを(1)に分類した。組織で保持している情報(機密情報、個人情報等)を紛失や盗難等で漏えいする脅威を(2)に分類した。また、開発したアプリケーションのセキュリティ対策や対応の不備に起因する脅威を(3)に分類した。

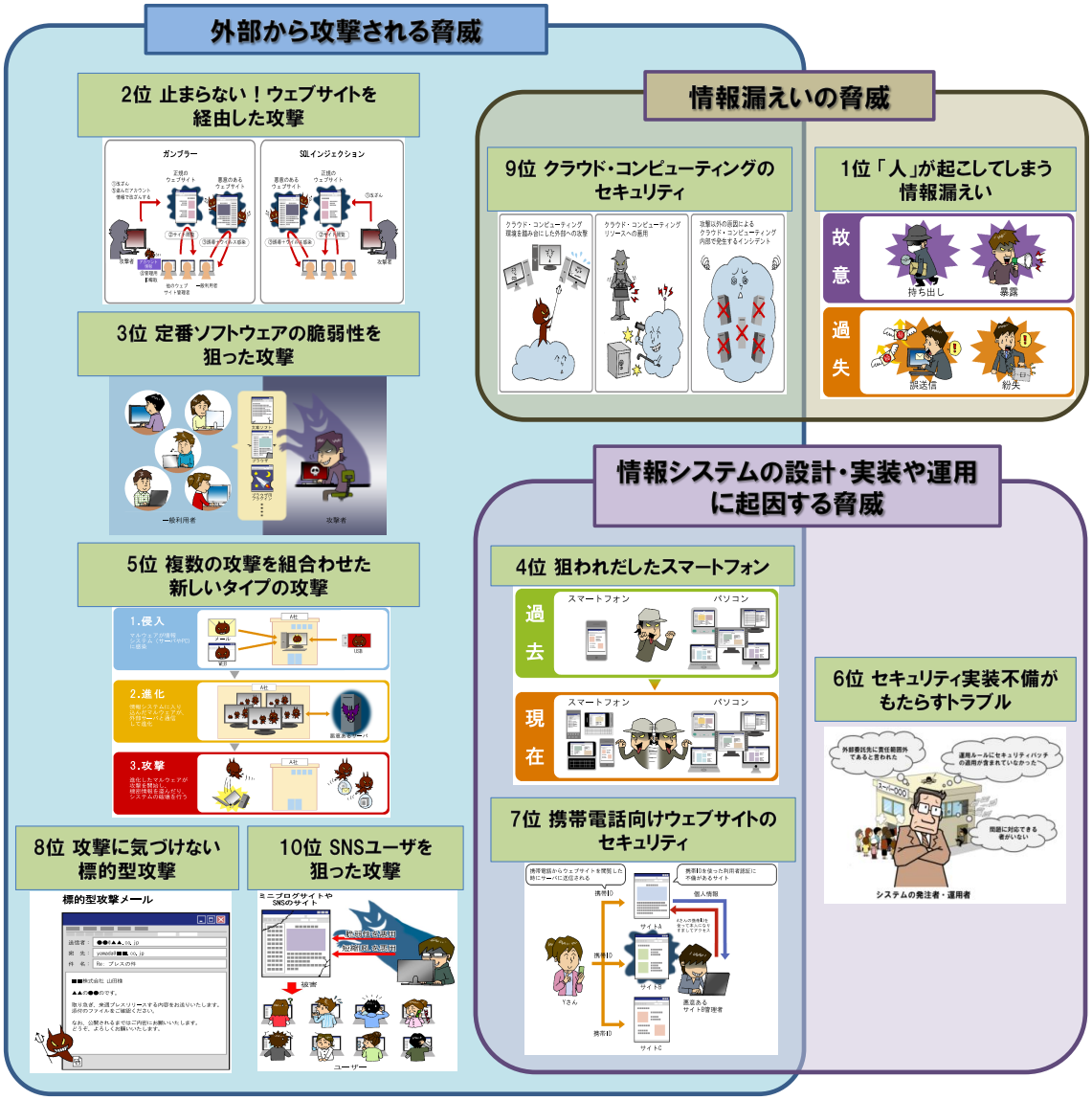


図 1：10 大脅威分類図

本ページは白紙です

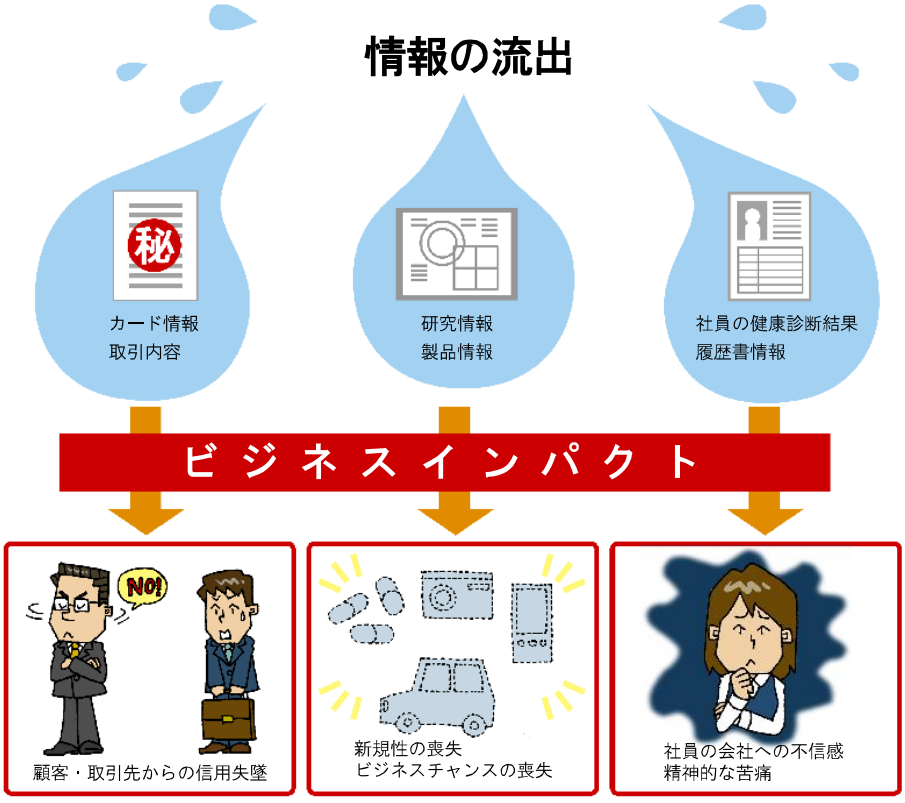
第 1 章 2010 年における組織へのビジネスインパクト

2010 年は、企業の営業活動に直接影響を与えるような情報窃取事件やシステム停止等のセキュリティ事件・事故が国内外で発生した。セキュリティの事件・事故が発生した場合、売上等の財務上の損失、社会的な信用失墜、利用者への影響、従業員のモチベーション低下等、企業の事業運営に大きく響いてくる。また、昨今では企業の知的財産や研究開発情報が窃取される事件まで発生しており、製造業者等において、死活問題になりかねない事態である。

本章では、代表的なセキュリティ事故である「情報流出」「システム停止」「ウェブサイト改ざん」について、実際に発生した事例を交えながら、企業活動に及ぼす影響や問題点を考察する。

1.1 情報が流出することによるビジネスインパクト

～複数企業に対して知的財産を窃取する攻撃が発生した～



1.1.1 情報流出の脅威とリスク

情報の流出に係る脅威は、大きく分けて、組織内部の情報管理の不備や不注意、あるいは故意に起因する「情報漏えい」と、外部の攻撃者が明確な意図を持って組織内の情報資産を窃取する「情報窃取」に分類することができる。本章では、この 2 つを併せて「情報流出」と定義する。

「情報漏えい」は、2011 年版 10 大脅威でも第 1 位に順位付けられており、年々社会的影響が大きくなる傾向にある。昨今は、内部の人間が故意に情報を持ち出すケースや、故意に情報

を公開するケースが散見されており、企業にとって大きなリスクになりつつある。また、攻撃者が外部から金銭的な見返りがある組織内部の情報資産を窃取する「情報窃取」も大きな脅威となっている。

情報流出することによる影響は、流出した情報の重要度により異なる。例えば、流出した情報によっては、当該情報関係者が経済的な被害を受ける可能性があり、個人情報であれば、それに伴い企業の社会的な責任にまで発展してしまい、事業の運営に影響を及ぼしてしまう。また、本人のみに通知される「成績結果」等のプライバシーに係る情報が流出した場合は、流出された個人が「精神的な苦痛」を受け、損害賠償に発展するリスクがある。

企業としては、情報流出が起こった場合は、流出した情報を突き止め、被害が拡大するのを一刻も早く食い止める必要がある。

1.1.2 ビジネスインパクト

・クレジットカード情報の流出

クレジット加盟店に不備があり、クレジットカード情報が漏えい・窃取された場合、情報を流出させた企業の信用失墜は勿論のこと、被害者へ謝罪金等の補償で、対策に係る費用、信頼回復に係る費用に加え今後の経営戦略にまで大きな影響を及ぼしてしまう。

例えば、国内では、オンラインのショッピングサイトで、外部からの攻撃により 7 万件に上るクレジットカード情報が流出したと報道される事件が発生した。また、2009 年には、大手の保険会社で、外部からの攻撃により 3 万件のクレジットカード情報が流出し、このうちの約 5,000 件において、カードの不正使用の試みが行われた事件がおこっている。

・研究開発情報の漏えい

2010 年 1 月に、Google をはじめ、Adobe Systems、Symantec、Yahoo!等、30 に及ぶ企業において、知的財産を窃取する攻撃が行われ、実際に被害が発生した。

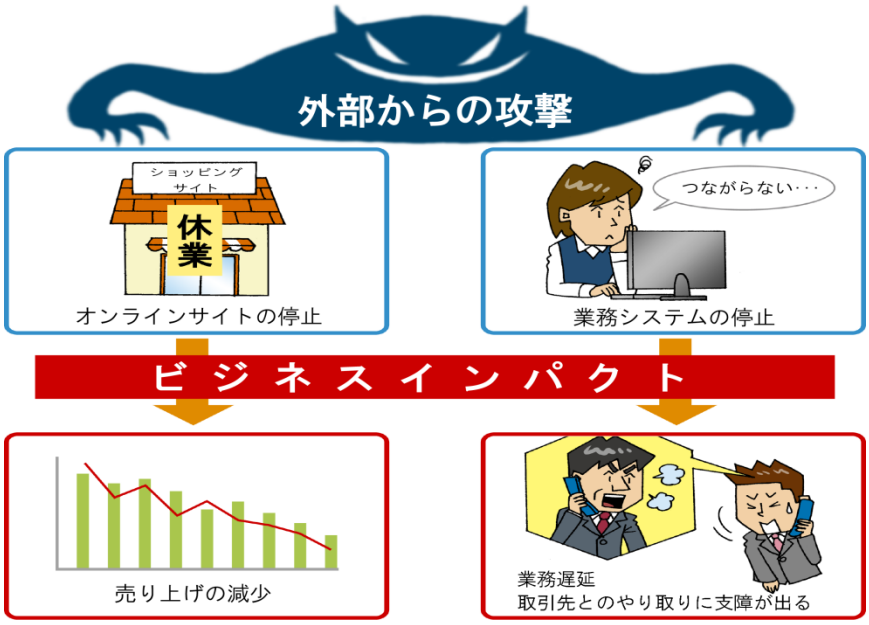
製品を開発している企業の場合、研究情報や製品の設計情報が窃取され、他組織に転売されてしまい、悪用される危険性がある。このような場合、発売前の製品が競合他社に先を越されて発売され、ビジネスチャンスを逸する可能性が考えられる。また、先に特許を取得され、販売できない事態となった場合、企業が今まで投資してきた研究開発費が無駄となり、今後の経営戦略に大きな影響を与えてしまう。その他、設計情報等の企業で機密にしているノウハウが流出すると、他社との優位性が薄れる等、競争力の低下につながってしまう。

・健康診断結果や履歴書情報の漏えい

企業には、ビジネス文書の他に社員の個人情報も保管されている。個人情報の中には、他人には知られたくない「健康診断結果」や「経歴」「成績表」も含まれている。このようなプライバシーに係る情報が外部に流出した際は、個人情報保護法に抵触するだけでなく、個人に対しても大きな精神的苦痛を与える可能性がある。さらに、社員の会社への不信感、仕事に対するモチベーションの低下等、間接的な影響も考えられる。社員のモチベーションは企業の成長に欠かせない要素であり、事業継続の観点からも大きな影響となり得る。

1.2 システム停止によるビジネスインパクト

～DDoS 攻撃やウイルスにより、複数の企業が一時的にサービス提供不能に陥った～



1.2.1 システム停止の脅威とリスク

外部からの攻撃によるシステム停止は、世界中の至る所で問題になっている。国内では、オンラインゲームやホスティングサービスを提供するサーバにおいて、DDoS 攻撃により通信障害を引き起こしてしまい、一時的にサービス提供ができない状況に陥った事例がある。さらに海外では、外部から持込まれたコンピュータウイルスによって原子力設備が一定期間停止したと言われている事例もある。

システム停止の脅威は、停止されるサービスの重要度によりビジネスへのインパクトが異なってくる。ウェブサイト上でビジネスを展開している企業の場合、「システムの停止」=「営業活動の停止」になりかねない。企業においては、各システムが停止した際のインパクトを把握しておき、その上で外部から攻撃されるリスクを低減する対応が重要である。

1.2.2 ビジネスインパクト

・サービス提供サイトの場合

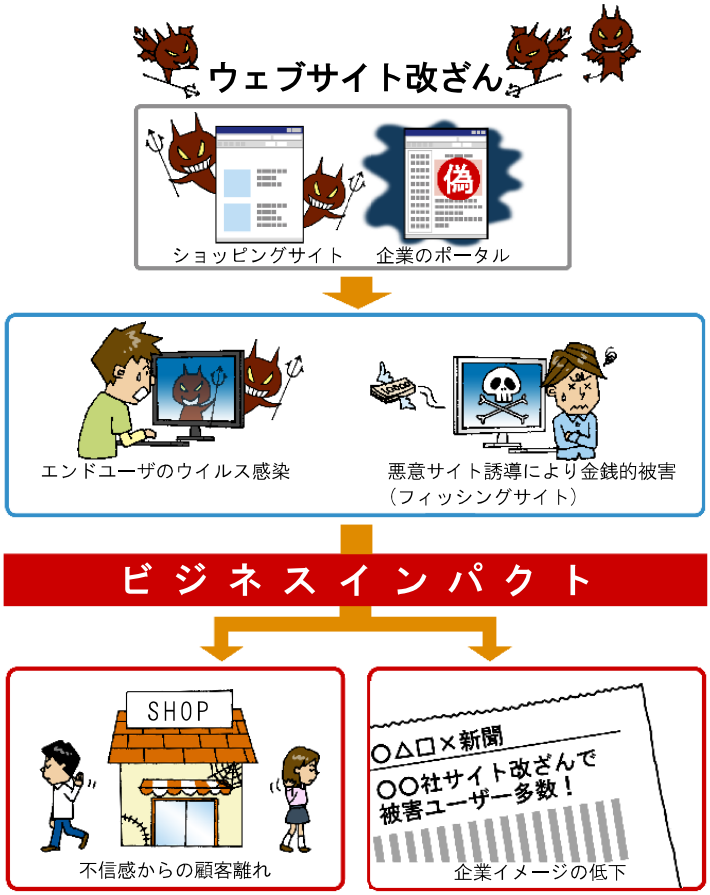
オンラインでショッピングサイトを運営している企業の場合、直接的な影響として、ウェブサイトが停止してしまうと営業活動が停止してしまうこととなり、停止期間中はオンラインでのビジネスが行えない状態に陥ってしまう。また、二次的な被害として、サービス停止による顧客や世間からの信用低下が懸念される。

・業務システムの場合

職場の情報インフラシステムがウイルスに感染し、メールや社内システムが使用できない事例は、身近でよく聞く話である。現状のオフィス環境が情報システムで構築されているため、社内の業務システムが停止した場合、日々の業務に影響を与えてしまう。例えば、取引先とのメールによるコミュニケーションが図れなかったり、発注管理システム等が停止してしまったりすると、納期遅延を引き起こす等のトラブルに発展し、結果的に取引先からのクレームや取引停止に発展する可能性がある。

1.3 ウェブサイト改ざんによるビジネスインパクト

～大手を含む複数企業のウェブサイトが改ざんされ、各々の企業イメージが低下した～



1.3.1 ウェブサイト改ざんの脅威とリスク

2009 年以降、ガンブラーの流行に伴った、ウェブサイトの改ざん事例が相次いでいる。2011 年版の 10 大脅威の中でも第2位に順位付けられており、相変わらず猛威を奮っている問題である。例えば、インターネットの広告配信サービスで使用しているサーバが改ざんされ、そのサービスを利用していたウェブサイトを訪れた利用者が、悪意あるサイトへ誘導され、ウイルスに感染してしまう事件が発生した。

ウェブサイトの改ざんというと、過去はいたずら目的の改ざんが多かったが、昨今は金銭目的の改ざんに移行してきている。攻撃者は、ウェブサイトの改ざんによって、ウェブサイトを訪れた利用者をフィッシングサイトに誘導したり、PC をウイルスに感染させたりすることで、利用者の個人情報やクレジットカード情報等を窃取しようとする。即ち、ウェブサイトは管理者の関知しないところで攻撃者の踏み台になり、結果として犯罪に加担してしまっている。このような事態により企業イメージが低下し、営業活動へ影響することが考えられる。

1.3.2 ビジネスインパクト

・ショッピングサイトの場合

ショッピングサイトが改ざんされた場合のビジネスインパクトとして、顧客離れが懸念される。利用者の心情として、自身が被害に遭うかもしれないという不安を感じると、そのウェブサイトの利用を躊躇ってしまう。また、被害にあった利

用者が、逆恨みによる理由からショッピングサイトを誹謗中傷する情報を掲示板サイトへ書込むことも考えられる。この場合、そのショッピングサイトのイメージが低下し、結果として顧客離れにつながる可能性がある。

・企業のウェブサイトの場合

インターネット社会となった今では、企業のウェブサイトはいわば「企業の顔」である。ウェブサイトが改ざんされた場合は、当該企業に興味を持った利用者がウイルス感染やフィッシングサイトへ誘導させられ、金銭的な被害を受ける可能性がある。この場合、利用者からの信用失墜や企業のイメージダウンは勿論のこと、攻撃サイトに加担したことで、世間や取引先からの印象は悪くなり、営業活動に影響を及ぼすことが考えられる。

本ページは白紙です

第 2 章 10 大脅威

【1 位】「人」が起こしてしまう情報漏えい

情報漏えいは、昔から存在している脅威であるが、PC やインターネットの普及に伴い、情報を気軽に発信、収集することができるようになった昨今、以前よりも大きな脅威となっている。

＜脅威＞

情報漏えいの脅威は、事故を引き起こすことにより企業経営に致命的なダメージを与えかねないため、予防的な対応に加え、事件・事故の発生後の対応も重要になってくる。

情報漏えいの特徴の一つとして、「人」の行動によって引き起こされる点が挙げられる。現代社会において情報漏えい事件・事故が減少しない要因の一つに、「人」が情報を取り扱う上で、システムで制御できない部分があるため、最終的な判断を「人」に任せなければならない点が挙げられる。

人による情報漏えいの原因は、「故意」、「過失」の大きく 2 つに分類される。原因ごとに、主だった情報漏えいのケースについて以降に記載する。

［故意による情報漏えい］

① データの持ち出し

従業員や元従業員が顧客の名簿リストの情報を USB メモリや CD-R 等の外部記憶装置で故意に持ち出し、情報を名簿業者に売却する等の行動が挙げられる。この問題の原因としては、クビになった会社への腹いせや、データを名簿業者へ売却することによる金銭的な見返り等が考えられる。

② 暴露・組織外部への情報流布

暴露の例として、組織内部で知り得た情報を外部の情報発信サイトに故意に掲載することで、情報を流布する行動が挙げられる。特に 2010 年は海外の暴露サイトにおいて、政府が秘匿していた情報が公開されたことで注目を集めた。国内においても、個人の軽い気持ちで、組織の秘匿としている情報が情報発信サイトに暴露される等の問題が発生している。背景には、個人で手軽に情報を発信できるウェブサービスが発達したことが挙げられる。

［過失による情報漏えい］

① 誤送信

過失による漏えいの代表的な問題として、メールの誤送信が一番に挙げられる。メールの誤送信を防ぐのが難しい背景として、送信先の正しさは送信者本人しか判断できない点がある。また、ミスを減らすための教育や啓発は、一定の効果はあるが、「人」が起こすミスをすべて無くすことは困難である。

② 紛失・盗難

紛失による情報漏えいとは、機密情報が格納されたUSBメモリやCD-R等の外部記憶装置やPCの紛失により情報が漏えいする問題である。データ記憶装置の小型化や大容量化に伴い、大量のデータが手軽に持ち出せるようになったことも、紛失のリスクを高める要因となっている。なお、盗難により情報が漏えいする場合もある。

＜影響＞

情報漏えいがもたらす組織への影響は、業種や漏えいした情報の種別によって異なる。

例えば、一般小売店やインターネット通販サイトのような直接的に消費者とビジネスを行っている企業の場合、顧客情報が流出すると、顧客からの信用を失うだけでなく、被害者から訴えられる可能性もある。この場合、売上への影響や信頼回復等の事後対応に多額の費用が掛かり、場合によっては企業の存続にまで影響する。また、新規性を売りにしている開発企業の場合、製品設計情報や研究情報等の営業秘密が漏えいすると、企業の経営戦略に大きな影響を及ぼす。

情報漏えいが起きてしまった場合、漏えい原因の究明、謝罪公告、監督官庁への報告、被害者への補償、信用の回復等、様々な対応が必要となる。そのため、問題が起った際にいかに早く通常業務に戻すかが事後対応の鍵となる。企業等の組織においては、情報漏えいを起こさない為の予防的な対策を講ずることはもちろんのこと、情報漏えいを起こした際の事後対応も事前に想定しておく必要がある。

＜2010年の事例・統計＞

JNSA（日本ネットワークセキュリティ協会）が公開している「情報セキュリティインシデントに関する調査報告書」によると、2010年1月から6月に漏えいした個人情報は、127万人分となり、インシデント件数では684件となる。その漏えい原因は、メール等の誤送信に伴う「誤操作」が約37%を占めており、次いで内部ルールの整備不良に伴う「管理ミス」が30%を占めている。

具体的な事例としては、ショッピングサイトの顧客情報46万人分を派遣社員が持ち出し、名簿業者に売却する事件が挙げられる。また、情報システム会社においては、顧客情報10万人分を保存したPCを社員が帰宅途中に紛失し、漏えいした事例がある。

関連資料

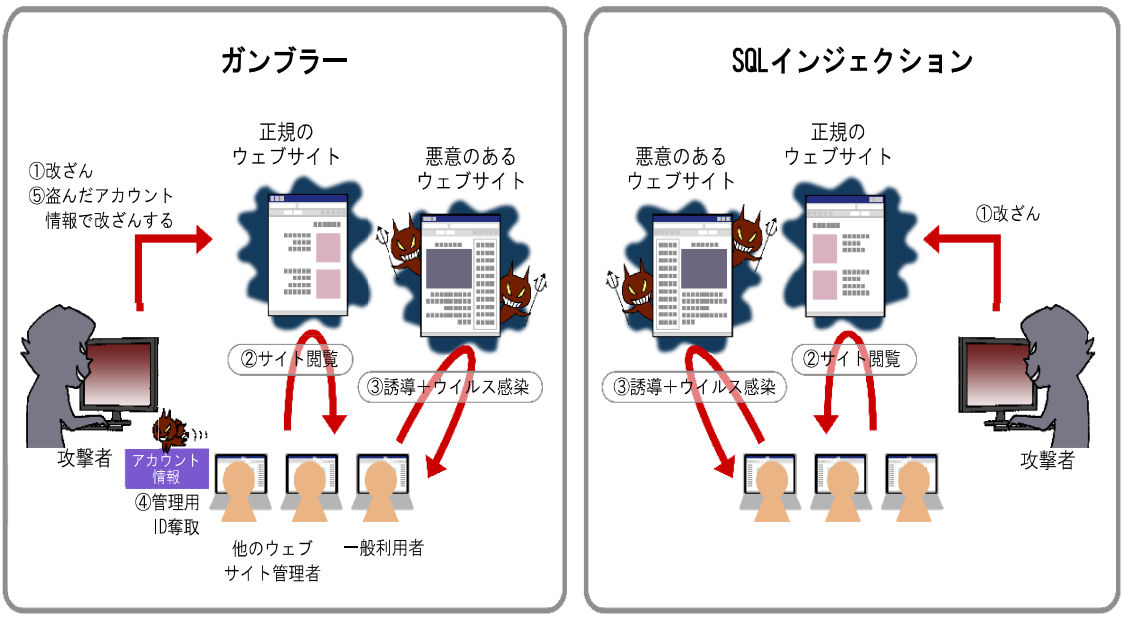
JNSA: 2010年 情報セキュリティインシデントに関する調査報告書【上半期 速報版】

http://www.jnsa.org/result/incident/data/2010fp_incident_survey_sokuhou_v1.0.pdf

SecurityNext： 個人情報漏洩事件一覧

http://www.security-next.com/cat_cat25.html

【2 位】止まらない！ウェブサイトを経由した攻撃



2010 年も、ウェブサイトを経由した攻撃は引き続き発生している。ウェブサイトを経由した攻撃は組織に対しても、一般の利用者に対しても影響を与える攻撃である。

＜脅威＞

ウェブサイトを経由した攻撃により、一般に知られた信用できると思われているウェブサイトが踏み台にされる可能性がある。その結果、ウェブサイトの閲覧者が知らぬ間にウイルスに感染し、情報窃取されてしまう等の恐れがある。

ウェブサイトを経由した攻撃としては、ガンブラーウイルスに代表される攻撃手法や、SQL インジェクションの脆弱性を悪用した攻撃手法が典型的である。それぞれの脅威や特徴について、下記に記載する。

[ガンブラーウイルスによるウェブサイト改ざん]

ガンブラーウイルスに代表される攻撃手法は次のステップとなる。

(1) 攻撃者により、ウイルスをダウンロードするサイトへリダイレクトするように、正規のウェブサイトが改ざんされる。

(2) 利用者が正規のウェブサイトを閲覧する。

(3) 利用者はリダイレクトされた先で、ウイルスに感染する。

(4) 利用者の PC に感染したウイルスは、アカウント情報（ID、パスワード）等の窃取や外部の攻撃者への送付の活動、および組織内の他 PC への感染拡大を行う。

(5) 感染した PC 利用者の中に、別のウェブサイトの管理用のアカウント情報を持つ者が含まれていた場合、攻撃者はそのアカウント情報を使い、ウェブサイトを改ざんする。

このように、改ざんされたウェブサイトをネズミ算式に増やしていくことも、この攻撃の大きな脅威となっている。

なお、(5)の攻撃が成功する条件は、下記が挙げられる。

- ウェブサイト管理者が使用する PC で脆弱性対策が行われていない。
- 個人宅やインターネットカフェ等、インターネット上の任意の場所からウェブサイトの更新が可能である。

[SQL インジェクションによるウェブサイト改ざん]

SQL インジェクション攻撃によるウェブサイト改ざんは、ウェブサイトで使われるデータベースを不正に操作して行われる。

SQL インジェクション攻撃によって改ざんを成立させるためには、次の2つの前提が必要である。

- ウェブサイトにSQL インジェクションの脆弱性が存在する。
- データベースに格納したデータを用いて、ウェブページを動的に生成するウェブサイトである。

これらの条件を満たすウェブサイトの場合、SQL インジェクション攻撃により、ウェブサイトが改ざんされ、ウイルスを仕掛けられる可能性がある。その結果、改ざんされたウェブサイトを閲覧した利用者がウイルスに感染してしまう。また、SQL インジェクションの攻撃では、ウェブサイトを改ざんする以外にも、データベースに格納された情報を窃取される脅威も存在する。

＜影響＞

ウェブサイトが改ざんされた場合、利用者がウイルスに感染したり、ウェブサイト上のサービスが一時的に停止する等の被害が発生する可能性がある。その結果、ウェブサイトを運営している組織の信用の低下につながる可能性がある。特によく利用されるサイトであればある程、その社会的な影響力は大きくなり、利用者が被害を受ける可能性は高まる。

なお、ウイルスによっては、セキュリティソフトのように振る舞い、ウイルスを削除するために有償版の製品が必要であるとして、クレジットカード情報の入力等を要求するものがある。利用者がこのようなウイルスに感染した場合、金銭を騙し取られる可能性がある。

これらの被害を回避するためにも、ウェブサイト運営者と利用者それぞれがセキュリティ対策を実施することが必要である。

＜2010 年の事例・統計＞

2009 年と比較すると、2010 年は一般紙やニュースサイトでウェブサイトを経由した攻撃の報道が取り上げられることは少なくなった。しかし、2010 年になっても、引き続き被害の報告が挙がってきている。

2010 年に発表されたウイルス対策ソフトウェアベンダのレポートによると、2010 年の 10 月だけで国内の 100 社以上で感染被害が報告されている。また別のレポートによると、2010 年に当該ベンダに寄せられたウイルス感染被害の上位 10 件の内、4 件がガンブラー等ウェブサイト関連のウイルスだったとある。これらのレポートからも、ガンブラー等による被害が沈静化しているわけではないことが分かる。

関連資料

JPCERT/CC: Web サイト改ざん及びいわゆる Gumblar ウイルス感染拡大に関する注意喚起

http://www.jpcert.or.jp/at/2010/at100001.txt

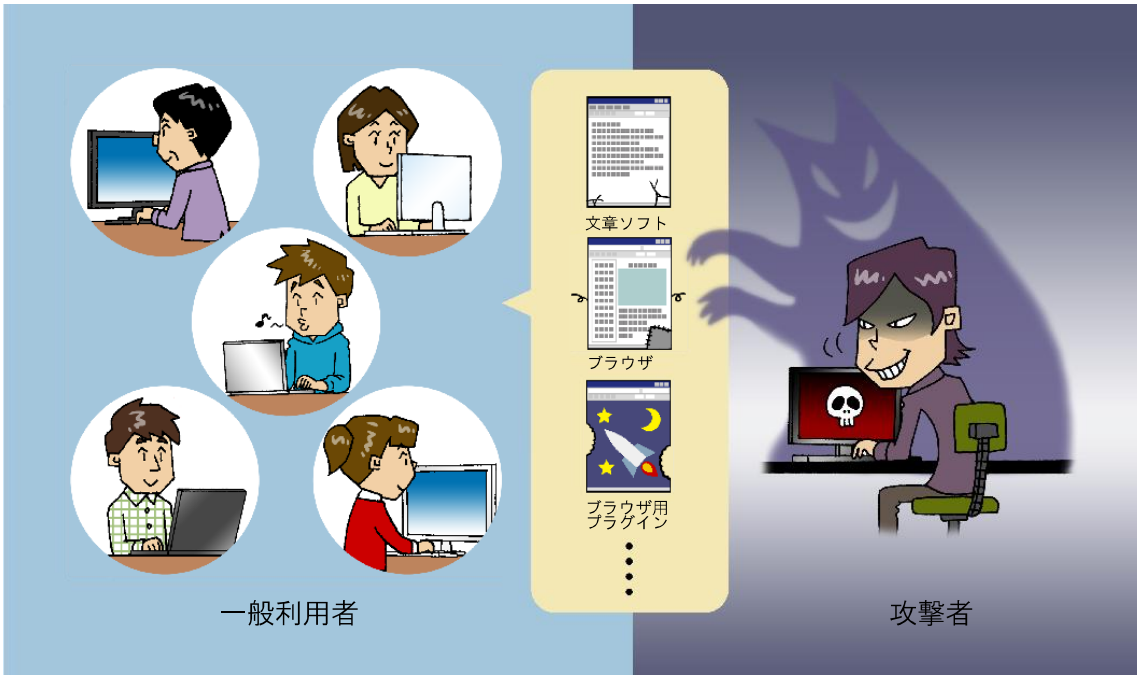
マイコムジャーナル: 国内100社以上の感染被害をもたらしたWebサイト改ざんの仕組みなど ―トレンドマイクロレポート

http://journal.mycom.co.jp/articles/2010/11/05/trendmicro/index.html

トレンドマイクロ: インターネット脅威年間レポート － 2010年度（速報）

http://jp.trendmicro.com/jp/threat/security_news/monthlyreport/article/20101217082311.html

【3 位】定番ソフトウェアの脆弱性を狙った攻撃



ソフトウェアには、多くの人が使用している、いわゆる定番ソフトウェアがある。このようなソフトウェアに存在する脆弱性を狙った攻撃が後を絶たない。

＜脅威＞

コンピュータ上では様々なソフトウェアが動作している。これらのソフトウェアに脆弱性が存在する場合、その脆弱性を悪用した攻撃が行われることがある。特に、脆弱性を悪用されるソフトウェアは多くの人が使用している定番ソフトウェアである場合が多い。

定番ソフトウェアが狙われる要因の一つとして、利用者が多いだけでなく、脆弱性が修正されたバージョンにアップデートしない利用者も多いことが考えられる。つまり、定番ソフトウェアに脆弱性が存在すると、多くの利用者が攻撃の影響を受けてしまう状態になると言える。

2010 年も定番ソフトウェアの脆弱性を狙った攻撃が多かった。IPA では、広く普及しているソフトウェアにおいて、脆弱性を狙った攻撃事例が確認されており、かつその脆弱性を修正するプログラムがリリースされている場合、緊急対策情報を発信している。2010 年は、この緊急対策情報を 15 件発信した。

緊急対策情報の対象となったソフトウェアは次のとおりである。

- Internet Explorer
- Adobe Reader, Adobe Acrobat
- Java Runtime Environment(JRE)
- Java Development Kit(JDK)
- 一太郎シリーズ
- Adobe Flash Player
- Windows シェル

＜影響＞

攻撃者が定番ソフトウェアの脆弱性を狙う場合、ウェブサイト経由、メール経由等様々な手段を用いる。2011 年版 10 大脅威の 2 位「止まらない！ウェブサイトを経由した攻撃」や 8 位「攻撃に気づけない標的型攻撃」にも定番ソフ

トウェアの脆弱性が悪用されている。

攻撃によって、PC 内の情報の窃取や、他のサーバを攻撃するための踏み台にされる等の被害が発生してしまう可能性がある。

これらの攻撃を回避するためには、定番ソフトウェアを脆弱性が修正されたバージョンにアップデートすることが有効な対策の一つである。多くの OS や OS に付属するソフトウェアは、定期的に自動でアップデートする機能を備えている。その他のソフトウェアにおいても、自動でアップデートする機能や、新しいバージョンが存在することを利用者に通知する機能が備わっていることがある。

攻撃者は、ウェブサイトやメール経由等様々な手段で利用者を攻撃しようとする。そのため、各ソフトウェアの自動アップデート機能や定期的に自身の PC の定番ソフトウェアが最新バージョンであるかどうかを確認する習慣を身につけていただきたい。なお、いくつかの定番ソフトウェアのバージョンチェックは、IPA が提供している MyJVN バージョンチェッカで確認することができる。

＜2010 年の事例・統計＞

IPA で実施した「2010 年度 情報セキュリティの脅威に対する意識調査」報告書における調査によると、「Windows Update 等によるセキュリティパッチの更新」をしていると回答した方は 69.4%であり、「Adobe Reader のバージョンアップ」をしていると回答した方は 55.6%だった。それ以外の回答者はアップデートしていないという結果であった。

Windows Update によって、利用者の多いウェブブラウザである Internet Explorer のセキュリティパッチも配布される。このことから、定番ソフトウェアである Internet Explorer や Adobe Reader をアップデートする習慣が身についていない利用者が多いと言える。

また、米国のセキュリティ企業が発表した 2010 年上半期に行われた攻撃で悪用された上位 15 件の脆弱性のうち、5 件が Microsoft Internet Explorer 関連、4 件が Adobe Reader 関連のものである。これらの脆弱性は、発見時期が 2006 年と古い時期に発見されたものもある。それでもなお、攻撃に利用されているということは、アップデートしていない利用者が多く、古い脆弱性であっても攻撃が成立するということを示している。

関連資料

ITMedia: 1年間の新種マルウェア、史上最大数160万へ

http://www.itmedia.co.jp/enterprise/articles/1007/16/news013.html

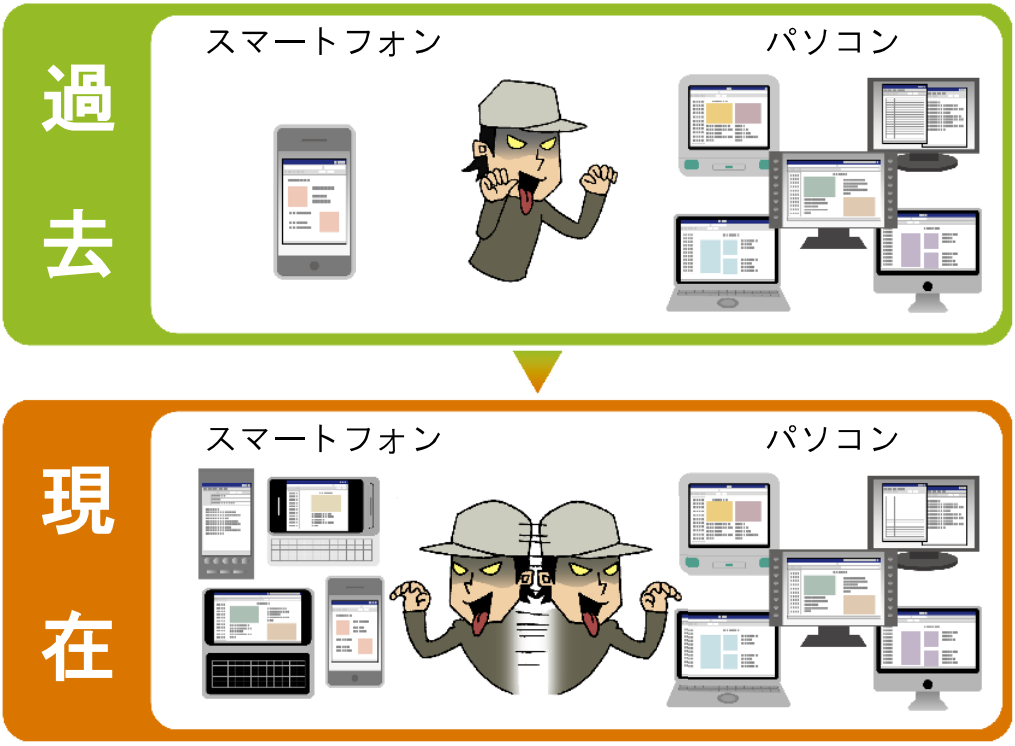
IPA: 緊急対策情報・注意喚起 一覧

http://www.ipa.go.jp/security/announce/alert.html

IPA: 「2010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/fy22/reports/ishiki/index.html

【4 位】狙われだしたスマートフォン



近年スマートフォンの普及が加速している。スマートフォンの普及により、セキュリティ上の問題が実際の脅威として顕在化してきた。

＜脅威＞

スマートフォンは、携帯電話と携帯情報端末(PDA)の機能を持った携帯端末である。電話帳等の個人情報を含み、かつアプリケーションをインストールすることで柔軟に機能拡張できる。従来の携帯電話ではできないことも機能拡張することで可能になる。年々普及は進み、スマートフォンを狙った攻撃も確認されるようになった。攻撃は次のようなものがある。

(A) スマートフォンに付属しているソフトウェアの脆弱性を悪用する攻撃

(B) 正規のアプリケーションを装ったウイルスをインストールさせる攻撃

（A）は、ソフトウェアに脆弱性が存在するスマートフォンで、ウェブサイトを閲覧させる、またはファイルを開かせることで攻撃が成功する。

（B）は、アプリケーションを装ったウイルスをスマートフォンにインストールさせることで攻撃が成功する。（B）の攻撃は、スマートフォンに付属するソフトウェアの脆弱性の有無には関係なく、利用者がウイルスのインストールを許可してしまった場合に成功する。

PC に近い機能をもったスマートフォンだが、現時点では PC と同様のセキュリティ対策を実施することが難しい。脆弱性を修正しようにも、スマートフォン開発事業者によるセキュリティパッチの提供までに時間がかかっていることや、アプリケーションが正規のものであるか判断する基準等が確立していないのが現状である。

利用者数の増加、柔軟な拡張性、不十分なセキュリティ対策等、悪意ある者が攻撃しやすい状況が揃いつつあるため、今後はさらに攻撃を受ける可能性が高まっていくと予想される。

＜影響＞

スマートフォンが狙われだしたことで、利用者はPCだけでなくスマートフォンのセキュリティも考慮する必要性が高まった。スマートフォンに格納されたメールや電話帳の個人情報の漏えいや、GPS によるスマートフォン保持者の位置情報のトラッキング、第三者を攻撃する踏み台になる等の脅威の可能性がある。なお、スマートフォンで使われる OS によっては、ウイルス対策ソフトウェアが存在する場合もある。

スマートフォンの利用者は、まずは、これらのセキュリティ上の問題やリスクの低減策の存在を十分に認識することが重要である。

また、組織内でスマートフォンを利用する場合、運用管理ルールの策定はもちろんのこと、スマートフォンの更なる高機能化や利用者数の増加、想定される脅威等のスマートフォンを取り巻く状況を加味した運用が重要になる。

＜2010 年の事例・統計＞

市場調査会社のレポートによると、2010 年度の国内におけるスマートフォンの出荷台数は 675 万台になる見通しである。前年度（234 万台）から約 2.9 倍の伸びとなり、スマートフォンが急速に普及し始めている。

2010 年には、iPhone/iPod touch/iPad で採用されているiOSにおいて脆弱性を利用したスマートフォンの制限解除行為や Android OS を狙ったウイルスが確認された。

具体的には、iOS に付属するウェブブラウザである Safari の脆弱性を利用して、スマートフォンの端末に設けられた制限を取り外す行為（Jailbreak）が確認された。ここで注目したいのは、脆弱性を利用して端末の制限を解除している行為である。

また、制限が解除されることにより、攻撃による被害を受けやすくなる。制限が解除されたスマートフォンを狙ったウイルスにより、学術機関でウイルスに感染した事例がある。

Android OS におけるウイルスは、トロイの木馬、スパイウェア、ボットの3種類のウイルスが確認されている。Android アプリは、Google 社が運営しているAndroid Market だけでなく、第三者が運営しているアプリ配布サイトや個人サイトでも配布することができる。IPA の「Android OS を標的としたウイルスに関する注意喚起」を参考に、配布元が信頼できるかどうか、インストール時に表示される「アクセス許可」の一覧に当該アプリに不自然なアクセス許可が含まれていないかどうかを確認し、インストール可否の判断をすることを推奨する。

関連資料

株式会社 MM総研: スマートフォンの市場規模の推移・予測

http://www.m2ri.jp/newsreleases/main.php?id=010120101216500

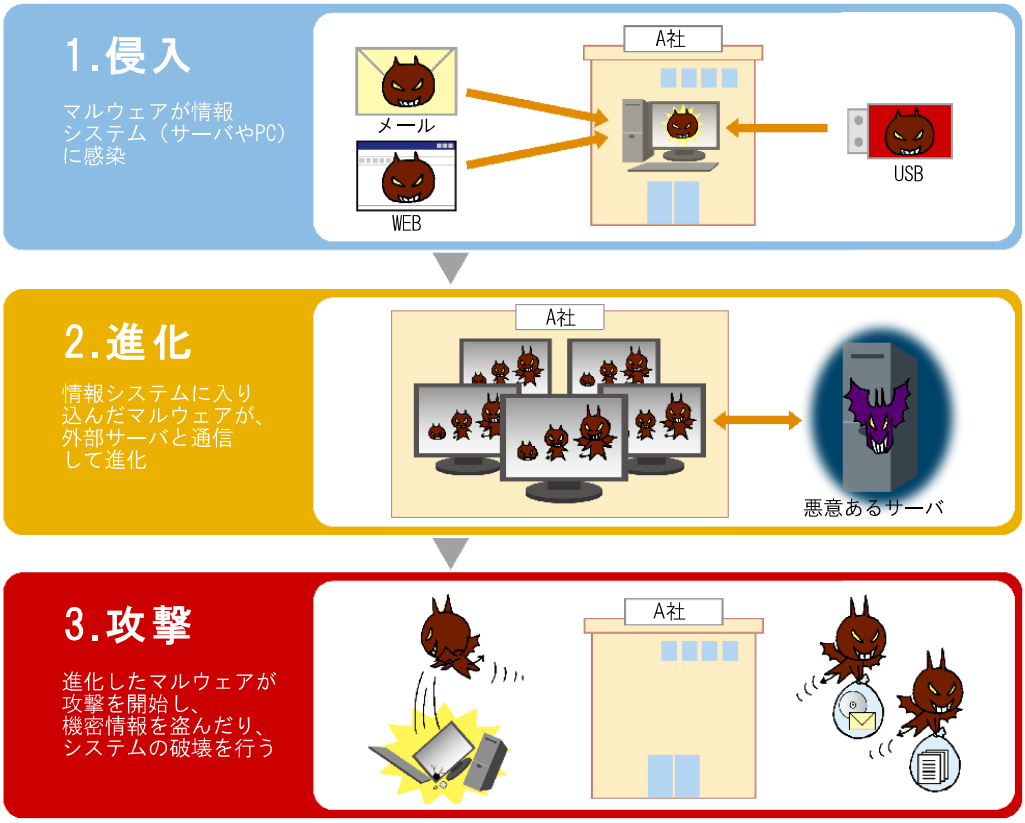
慶應義塾ITC: ″JailbreakされたiPhoneのウイルス感染に関する注意喚起 ″

http://www.hq.itc.keio.ac.jp/topics/topics61.html

IPA： Android OSを標的としたウイルスに関する注意喚起

http://www.ipa.go.jp/security/topics/alert20110121.html

【5 位】複数の攻撃を組み合わせた「新しいタイプの攻撃」



2010 年に、特定の組織を標的とした攻撃に対して、欧米を中心に「APT（Advanced Persistent Threats）」という用語が頻繁に使われるようになった。APT とは、ソフトウェアの脆弱性を悪用し、複数の既存攻撃を組み合わせ、ソーシャル・エンジニアリングにより特定企業や個人を狙った攻撃の総称である。IPA では、APT を「新しいタイプの攻撃」と名称付けをし、以降より「新しいタイプの攻撃」と称す。

＜脅威＞

「新しいタイプの攻撃」には、下記の特徴が挙げられる。

（1）ソーシャル・エンジニアリングの活用
（2）ゼロデイの脆弱性の利用
（3）ネットワーク/USB デバイスによる拡散
（4）外部の指令サーバとの通信
（5）個別システムに特化した攻撃

これらは新規の攻撃手法ではなく、既に存在する手法が大部分である。既存の攻撃と言うと、既に企業等で行われている一般的な対策さえ実施していれば、防げるように思われがちであるが、事はそう単純ではない。個々の攻撃が防御システムを回避するように巧みに組合わさり、攻撃目標に合わせて設計されている。そのため、従来は攻撃が不可能であると考えられていたシステムにまで攻撃の手が及んできている。

攻撃は、「1. 侵入」、「2. 進化」、「3. 攻撃」の 3 つのステップで構成されており、各ステップで複数の攻撃手法が織り交ぜられている。

[1.侵入]

攻撃者は、ソーシャル・エンジニアリングを活用した標的型メールや USB メモリ等の外部メディアを経由してシステムに侵入する。その際、ゼロデイを含めた複数の脆弱性を利用しており、

従来のウイルス対策で防御し辛いのが特徴である。

[2.進化]

ウイルスは、潜入した PC 内にバックドアを仕掛け、外部の指令サーバとの通信を行い、新たなウイルスを呼び込んだり、拡散、機能強化を行う。また、最終攻撃の前段として、特定システムに特化した攻撃に必要なプログラムをダウンロードする。

[3.攻撃]

攻撃対象システムに対して攻撃を実施し、情報窃取や情報システムの破壊活動を行う。

＜影響＞

海外の事例では、制御システムへの影響や、重要性の高い情報の窃取等の深刻な実害がでてきている。本攻撃は、報道されている内容が海外の事例が多いこともあり、国内システムでは縁遠いと思われがちである。しかし、攻撃者のターゲットになっていないだけとも考えられ、国内の多くの企業で起こり得る問題である。

なお、本攻撃が成功してしまう背景には、内部からの通信を安全と見なしている、従来のネットワーク設計を逆手に取っていることが考えられる。システムに入り込んだウイルスに情報を外部に抜かれないようなネットワークの設計を考慮していく必要がある。

＜2010 年の事例・統計＞

「新しいタイプの攻撃」の主な事例としては、「Operation Aurora」と呼ばれる攻撃と、「Stuxnet」ウイルスによる攻撃が挙げられる。

「Operation Aurora」は、Google などの複数の情報システム企業が被害にあった攻撃である。この攻撃では、セキュリティパッチが提供される前の Internet Explorer の脆弱性が悪用され、利用者の情報が窃取された。

「Stuxnet」は、イランの原子力設備を狙ったと言われるウイルスで、原子力設備の制御システムを操作するようなコードが埋め込まれていた。コードが実行されることで、制御システムが停止してしまう可能性があった。複数の脆弱性を悪用して感染を広げようとしており、悪用する脆弱性の中にはセキュリティパッチが提供される前の脆弱性も含まれていた。

いずれの場合でも、ゼロデイ攻撃が使われており、侵入の段階では防ぎにくいことを示している。そして、最終的には攻撃者の目的である情報窃取や重要システムの停止まで行われる。このような攻撃は、組織にとって大きな脅威となる。

関連資料

IPA: IPA テクニカルウォッチ『新しいタイプの攻撃』に関するレポート

http://www.ipa.go.jp/about/technicalwatch/20101217.html

マカフィー: Operation Aurora など、標的型サイバー攻撃からの防護方法を詳述

http://www.mcafee.com/japan/about/prelease/pr_10a.asp?pr=10/06/18-1

issa-sac: Advanced Persistent Threat

http://www.issa-sac.org/info_resources/ISSA_20100219_HBGary_Advanced_Persistent_Threat.pdf

【6 位】セキュリティ対策不備がもたらすトラブル

システムの発注者・運用者

ウェブシステムやアプリケーションのセキュリティ対策に不備が発生した場合、それに対応する手順や体制を充分に考慮しておくことが重要である。それを怠ると事業継続に大きな影響をおよぼすことになる。

＜脅威＞

ウェブアプリケーション等の情報システムは一般的に、開発時のセキュリティ対策、テスト等を経て、公開、運用される。開発時や運用時のセキュリティ対策の考慮が不足していたり、外部からの新しい攻撃等の脅威によってリスクが高まる。

その結果、不正アクセスにより情報漏えいが発生したり、ウェブサイト閲覧者のウイルス感染を媒介したり、あるいは可用性を維持できず、利用者がシステムにアクセスできない事態が発生したりといった問題へとつながる。

従って、長期間に渡って利用される情報システムのセキュリティ対策は、設計・開発時だけでなく、セキュリティレベルを維持、管理できる運用体制を含め、企画段階から考慮しておくことが重要である。

＜影響＞

公開しているシステムや、事業に活用しているシステムにセキュリティ上の問題が発生した場合、それに適切に対応ができないと、次のような影響が発生する。

- ◆ サービスの中断や風評等により、組織活動に支障をきたしたり、更には事業継続が困難な状況になる。
- ◆ 対策に不備があるシステムを公開し続けた結果、攻撃の踏み台に悪用され、ネット社会に多大な迷惑や被害をおよぼす。

適切なセキュリティ対応が困難となるケースには、システム開発、システム運用等が、外部委託されている場合が見受けられる。外部委託をする場合、問題発生時の責任範囲が不明確なために、トラブルが発生することがある。

また、システムに使用されているプラットフォ

ームやアプリケーションのバージョンが古く、セキュリティパッチがあてられていないまま使用されているケースも見受けられる。更に、昨今盛んになってきたクラウドの利用時にも、同様の課題が懸念される。

ここではそうした事態を回避するための重要なポイントを挙げる。

- 情報システムの開発を発注する場合、セキュリティ対策や可用性などの非機能要件について配慮する。
- 使用製品、開発システムの脆弱性対策が実施できることを確認する。
- システム運用を外部委託する場合、運用保守契約等で、委託先の対応範囲を明確化する。

＜2010 年の事例・統計＞

情報セキュリティ早期警戒パートナーシップガイドラインに基づき、IPA は脆弱性に関する情報を受け付ける業務を実施している。その業務の一環として、IPA は、一般の方から届け出られた脆弱性関連情報をウェブサイト運営者に通知し、修正を促している。

しかし、通知をしたにも関わらず、脆弱性の対策を完了していないウェブサイトが多数存在する。IPA が現在取り扱っている届出のうち、2010 年 12 月末までに 2 年以上対策されていないウェブサイトは 218 件ある。届け出られた脆弱性の内容は、クロスサイト・スクリプティングの届出が 111 件（51%）、SQL インジェクションの届出が 64 件（29%）、ファイルの誤った公開の届出が 22 件（10%）、その他の届出が21件（10%）である。深刻度が高い SQL インジェクションの脆弱性であっても長期間放置されている。対策していない運営者からは、開発工数の問題で対応できないという回答だけでなく、開発ベンダと連絡を取れずに対策ができないとの回答や、開発ベンダにメンテナンスできる人材が不在で対策できないとの回答が散見された。

その他、岡崎市立中央図書館において、ウェブサイトの実装に起因する事故が発生し、ウェブサイト利用者が一時的にアクセスできなくなった事例がある。本事例では、システムの運営者や開発ベンダの対応の不手際もあり、影響が多方面に波及し、結果として社会的な問題にまで発展した。

関連資料

IPA: 非機能要求の見える化と確認の手段を実現する「非機能要求グレード」の公開

http://sec.ipa.go.jp/reports/20100416.html

IPA： 中小企業の情報セキュリティ対策ガイドライン

http://www.ipa.go.jp/security/fy20/reports/sme-guide/index.html

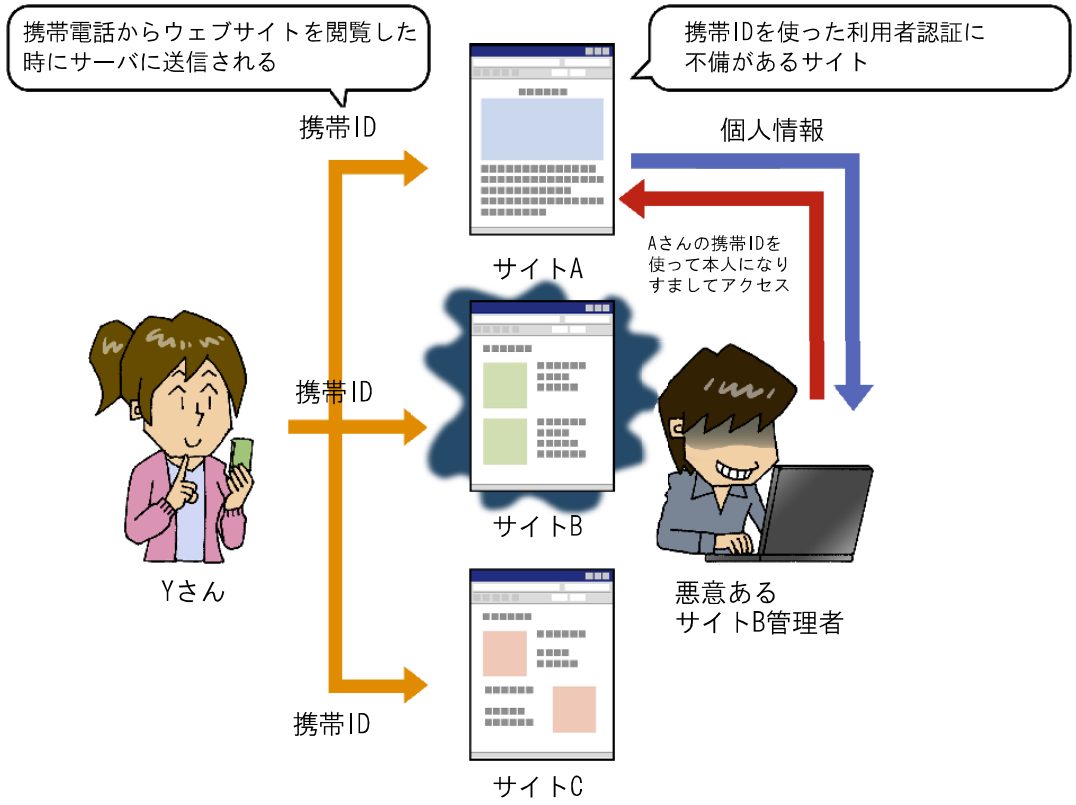
IPA： ソフトウェア等の脆弱性関連情報に関する届出状況[2010年第4四半期（10月～12月）]

http://www.ipa.go.jp/security/vuln/report/vuln2010q4.html

岡崎市立中央図書館： ホームページ閲覧障害に係る経過等について

http://www.library.okazaki.aichi.jp/tosho/about/files/20110225.html

【7 位】携帯電話向けウェブサイトのセキュリティ



携帯電話向けウェブサイトでは、携帯電話特有の情報を用いた実装をしている場合がある。携帯電話独自のノウハウで作られたウェブサイトの中には、安全でないものも見受けられる。

＜脅威＞

スマートフォンを除くこれまでの携帯電話は、PC に比べてブラウザ周りの機能が少ない。例えば、一部の機種では、ウェブブラウザで Cookie に対応していないことがある。このような機種を考慮した場合、特定の機能において、PC 向けウェブサイトと同じ実装方式を採用することができない場合がある。

このような状況において、携帯電話向けウェブサイトの利用者認証やセッション管理に、契約者や端末に関連付けられた携帯電話の識別子(以下、携帯 ID と呼ぶ)を使う実装が一部のウェブサイトで採用されている。ただし、この実装(以下、かんたんログインと呼ぶ)は、基本的に下記の条件を満たす場合において成り立ち、条件が満たされないとセキュリティ上の問題に発展する可能性がある。

(A) ウェブサイトへのアクセスは、携帯電話からのみ行われる。または、携帯電話以外からのアクセスをウェブサイト側で識別できる。

(B) 携帯電話からの HTTP リクエストに含まれる HTTP ヘッダは、利用者の操作では変更できない。

例えば、(A)の条件を満たすためにアクセス元 IP アドレスに基づく制限をする方法があるが、その IP アドレスによる制限に不備がある場合、下記の手順でなりすましの問題が発生する。なお、ここではサイト A に IP アドレスによる制限不備があるものとする。

(1) Yさんがサイト A およびサイト B にアクセスする。
(2) Y さんが、サイト A の「かんたんログイン」の設定をする。
(3) サイト B の管理者が Y さんの携帯 ID を利用して、PC からサイト A にアクセスする。

同じ携帯電話から複数のウェブサイトにアクセスした場合、それらウェブサイトすべてに同じ携帯 ID が送信される。そのため、携帯 ID は秘密情報とは言えない。携帯 ID のみを頼りに利用者を認証している場合、第三者になりすまされる可能性がある。このように、携帯電話独自のノウハウで作られたウェブサイトの中には安全ではないものがある。

新たに発売される機種は、基本的に Cookie に対応しており、さらに JavaScript に対応する機種も発売される等高機能化が進んでいる。そのため、携帯電話向けウェブサイトでも PC 向けウェブサイトと同様の実装が必要になってきた。携帯電話向けウェブサイトの構築事業者は、携帯電話の高機能化等の変化を考慮して、ノウハウを見直し、携帯電話向けのウェブサイトを構築する必要がある。

＜影響＞

なりすましにより、個人情報が漏えいしたり、情報が書き換えられたりする可能性がある。個人情報が漏えいした場合、直接の被害者はウェブサイト利用者だが、ウェブサイト運営側も信頼を失うことにより間接的に被害を受ける。

かんたんログインは、Cookie に対応していない携帯電話でも使える利用者認証の方式であるが、環境によって脆弱になりやすいものである。利用者認証の不備は個人情報に直結する問題になり得るため、採用する認証方式を慎重に検討する必要がある。パスワードや Cookie 等を使用した、PC 向けサイトと同様の認証方式を採用する、もしくは携帯電話キャリアが安全な認証方式を提供している場合、その認証方式を採用することが望まれる。

＜2010 年の事例・統計＞

2010 年には、かんたんログイン機能の実装不備に関する注意喚起や、実サービスで他の利用者としてログインが可能となる事例があった。

「OpenPNE」と呼ばれるソーシャル・ネットワーク・サービス構築ソフトウェアに、かんたんログインの実装不備があった。IP アドレスの制限機能に不備があったために、PC から他人になりすましてログインが可能であった。

その他、「クロネコメンバーズの Web サービス」にもかんたんログインの実装不備があった。特定の条件下で他の利用者のアカウントでログインが可能であった。

なお、どちらの問題も、適切に問題を公表し対策されている。

関連資料

IPA:「OpenPNE」におけるセキュリティ上の弱点（脆弱性）の注意喚起

http://www.ipa.go.jp/security/vuln/alert/201003_openpne.html

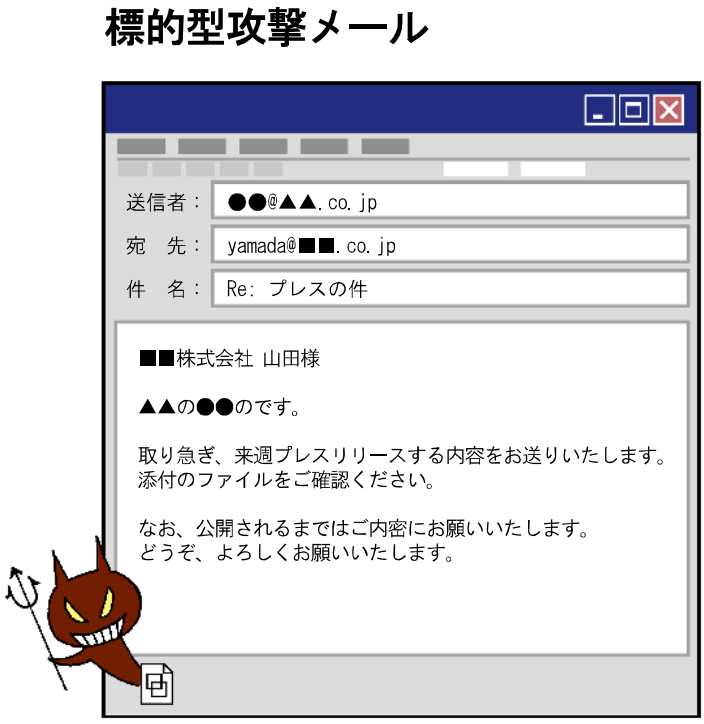
OpenPNE:【緊急リリース】携帯版かんたんログインの不備によりなりすましがおこなわれてしまう問題について

http://www.openpne.jp/archives/4612/

ヤマト運輸: 携帯版「クロネコメンバーズのWebサービス」クイックログイン機能の脆弱性への対応について

http://www.kuronekoyamato.co.jp/info/info_101025.html

【8 位】攻撃に気づけない標的型攻撃



標的型攻撃は、特定の個人や組織に向けて、知人や取引先企業になりすまして、ウイルスを添付したメールを送付したり、メール本文に記載されているリンクより悪意あるサイトへ誘導するなどして、情報窃取等の危害を加える手口である。

＜脅威＞

標的型攻撃の多くは、攻撃者が標的とする組織や人に対して、興味を引くような内容のメールを送付し、メール受信者がメール本文に記載されているリンクや添付ファイルを開かせることで、ウイルスに感染させる。PC に感染したウイルスは、PC 内の情報窃取やネットワークを通じた他システムへの破壊活動等を開始する。なお、メール経由で送り込まれたウイルスは、PC 内に潜伏しスパイ的な活動やネットワーク経由で別のウイルスを呼び込む等の活動をする。

標的型攻撃は、2005 年から確認され、既に数年経っているが、他の攻撃と違い有効な対策が取り辛いのが実情である。背景には、人間の心理面につけ込んだソーシャル・エンジニアリングが使用されていることが挙げられ、被害者が攻撃者によって騙されてしまうことがある。例えば、上図のようなメールが、取引先の実在する人物から送られて来た場合、標的型メールと通常メールとの見分けがつくだろうか。注意深い人は、メールの出所を疑うかもしれないが、大部分の人は、大事な取引先からの情報ということもあり、添付ファイルを開く可能性が高いだろう。このように標的型攻撃の特徴は、送られてきたメールが本物か偽物かの区別が困難で、結果として攻撃だと気づけない点にある。

また、標的型攻撃は特定の個人や組織のみが対象とされるため、ウイルスに関する情報が出回りづらい。そのため、当該ウイルスに対するパターンファイルの提供が遅れ、ウイルス対策ソフトウェアで検知が遅くなる傾向にある。

＜影響＞

標的型攻撃は、攻撃者の目的により攻撃のターゲットが変わる。そのため、影響においても、窃取される情報の種別や破壊されるシステムの種別により異なってくる。

石油会社の事例では、標的型攻撃により、石油の採掘場所の情報を盗まれたと言われている。組織内部で機密にしている情報が盗まれたことで、今後の企業活動に影響を及ぼす可能性が考えられる。

また、昨年話題となった、Google 社に対するサイバー攻撃においても、標的型攻撃が使用されている。Google 社からの発表によると、この攻撃は、中国の人権問題活動家の Gmail アカウントへのアクセス権を得ることが目的であったとのことである。言うまでもなく、アカウントのアクセス権が奪取されると、メールの内容が第三者により盗み見られ、機密情報の漏えいにつながってしまう。

＜2010 年の事例・統計＞

標的型攻撃に関するニュースは、中央省庁を狙った被害がクローズアップされていることもあり、一般の企業には縁遠いものと思われがちである。しかし、ウイルス対策ソフトウェアベンダの報告によると、同社がサービス提供している企業において、22.6 社に 1 社の割合で標的型攻撃のメールが確認されているという。実際の被害の有無は分からないが、一般企業が攻撃や被害を受けている状況に気づいていない可能性が考えられる。

また、2010 年は国内外で標的型攻撃が確認されている。一般紙等でも報道された事例として、経済産業省を狙った標的型攻撃がある。報道によると、経済産業省の職員宛に一斉に標的型メールが送付され、その内の約 20 人がメールを開いてしまったとある。メールは、実際に行われた会談の内容に関するものであり、送信元のメールアドレスも会談を担当している職員に酷似していたとのことだ。この事象から、当事者間で共有されている情報が使用される等、偽メールと疑う余地が無い、手の込んだ攻撃だと分かる。

また、海外では、石油会社や Google 社の他にも、米軍事契約企業を狙った攻撃に標的型攻撃が観測されており、サイバー攻撃におけるシステムに侵入するための常套手段として使われだしている。

各組織においては、攻撃者の目的によって標的が変わり得ることを念頭におき、利用しているソフトウェアへのセキュリティパッチの適用やウイルス対策ソフトウェアの定期的なパターンファイルの更新、内部から外部への不要ポートの遮断などの対策を講じておきたい。

関連資料

CSMonitor.com: US oil industry hit by cyberattacks: Was China involved?

http://www.csmonitor.com/USA/2010/0125/US-oil-industry-hit-by-cyberattacks-Was-China-involved

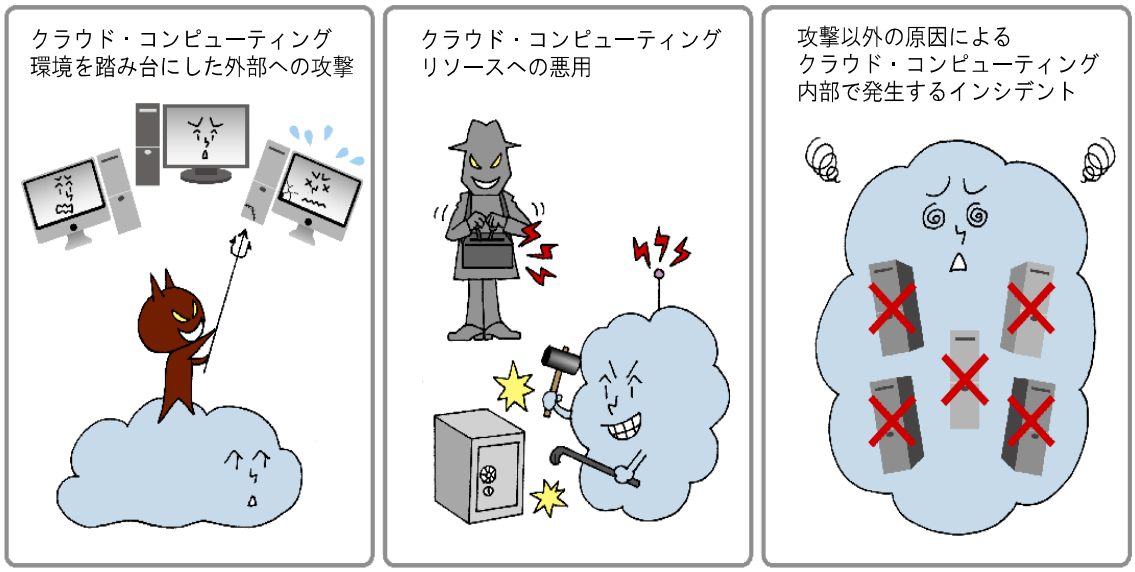
Itmedia Googleに対する標的型攻撃

http://www.itmedia.co.jp/enterprise/articles/1001/14/news085.html

PCOnline 日本の「迷惑メール率」は9割、「標的型攻撃」も増加中

http://pc.nikkeibp.co.jp/article/news/20101101/1028271/

【9 位】クラウド・コンピューティングのセキュリティ



クラウド・コンピューティング（以降、クラウド）を利用したサービスは、数年前より新しいビジネスモデルとして注目を集めており、企業への普及が進んでいる。一方、セキュリティ上の問題についても徐々に顕在化し始めており、事件・事故の発生やクラウド環境における、新たな脅威が公表されている。

＜脅威＞

IPA の「クラウド・コンピューティング社会の基盤に関する研究会」報告書では、クラウド環境における脅威として下記の 5 パターンを挙げられている。

（1）外部からクラウド環境への攻撃
（2）クラウド環境内部から他のクラウド利用者へ攻撃
（3）クラウドを踏み台とした攻撃
（4）コンピューティングパワーの悪用（パスワード解析や暗号解析等）
（5）攻撃以外の原因（停電、システム不具合等）

また、CSA(Cloud Security Alliance)の「Top Threats to Cloud Computing V1.0」では、クラウドの問題点として次の 7 つを挙げている。

（1）「クラウド・コンピューティングの不正および犯罪目的の利用（Abuse and Nefarious Use of Cloud Computing）」
（2）「安全ではないインターフェースおよび API（Insecure Interfaces and APIs）」
（3）「悪意ある内部者（Malicious Insiders）」
（4）「共有技術問題（Shared Technology Issues）」
（5）「データ消失または漏えい（Data Loss or Leakage）」
（6）「アカウントもしくはサービスのハイジャック（Account or Service Hijacking）」
（7）「未知のリスク（Unknown Risk Profile）」

クラウドの環境において、様々な脅威や問題点が指摘されており、事件・事故が発生したものもある。クラウドを利用する際は、組織の情報処理とデータ管理をどこまでクラウドで実施するか、事前に検討する必要がある。

＜影響＞

クラウドの脅威が具現化した場合、クラウド事業者と利用者双方が影響を受ける。

クラウド事業者にとっては、サービスの提供の中断がある。また、提供しているクラウド環境が不正に利用されていることによって、利用者からの評判が悪くなる可能性も考えられる。

クラウド利用者にとっては、クラウドシステム上の情報の漏えい、個人情報保護法等の法令遵守違反、事業継続性への影響等が挙げられる。また、利用者は、クラウドが自身のコントロールが完全に効かない環境であることを認識しなければならない。例えば、クラウドで情報漏えいが発生した場合、クラウドのサービス内容によっては、調査に必要なログや FW のポリシー情報等の提供が受けられない可能性がある。クラウドを利用する際は、事業者との間で SLA(Service Level Agreement) や OLA(Operation Level Agreement)を明確にしておくことが重要である。

＜2010 年の事例・統計＞

2010 年において、クラウドに関連する事件・事故が複数報告されている。

クラウド環境の不正利用（もしくは踏み台にされた）の事例として、2010 年 4 月頃、Amazon が提供する Amazon EC2 からインターネット通話で使用する SIP(Session Initiation Protocol)のサーバやクライアント等を狙ったパスワードの総当たり攻撃（ブルートフォース攻撃）が確認された。他にもスパムメールの送付元として、クラウド環境が利用されていることも観測されている。

停電等のクラウドにおける障害は、Amazon や Microsoft、Apple 等の様々なクラウド事業者で発生している。クラウド事業者は、各所に拠点を置くことでリスクの分散化を行う等の対応が進んでいる場合もあり、利用者への影響が少ない場合もある。

また、障害以外の事例では、Microsoft の BPOS(Business Productivity Online Suite)において、2 時間ほどメール情報が漏えいする事故があった。

関連資料

VoIP Tech Chat: Amazon EC2 SIP Brute Force Attacks on Rise

http://www.voiptechchat.com/voip/457/amazon-ec2-sip-brute-force-attacks-on-rise/

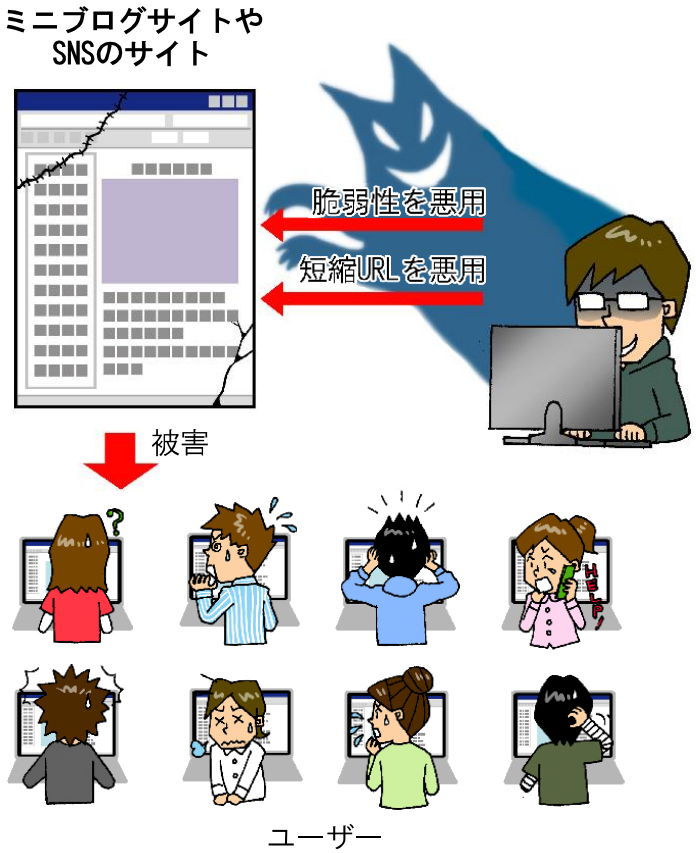
internet.com K.K.（Japan）クラウドを利用し Wi-Fi パスワード破り

http://japan.internet.com/webtech/20110113/11.html

Impress: SkyDriveで大量の個人情報を誤公開？ 保存先フォルダー・共有設定に注意！

http://internet.watch.impress.co.jp/docs/news/20101104_404541.html

【10 位】ミニブログサービスや SNS の利用者を狙った攻撃



ミニブログサービスや SNS(ソーシャルネットワーキングサービス)の利用者は爆発的に増えている。それに比例するように、それらの利用者を狙った攻撃も増えている。

＜脅威＞

世の中には、Twitter(ツイッター)、アメーバなう等のミニブログサービスや mixi(ミクシィ)、Facebook(フェイスブック)等の SNS が存在する。これらのウェブサイトで提供されるサービスは、今の自分の行動や考えを簡単にインターネット上に発信することや、同じ趣味や考えを持つ利用者同士の交流の場として利用できることが特徴となっており、利用者が数千万人規模のサイトもある。簡単に情報発信でき、面識のない人物とも交流を持て、利用者も多い環境であると言える。

このミニブログサービスや SNS の特徴を悪用し、利用者を騙したり、ウイルスに感染させようとしたりする攻撃が出現している。

例えば Twitter 上で、利用者が興味を持つような内容の発言をして、ウイルス感染を目的とした外部サイトに誘導しようとする。その際に、長い URL 文字列を短縮して利用する「短縮 URL」サービスが使われることがある。これはクリックするまでどのようなウェブサイトに誘導されるかわからない短縮 URL の性質を悪用したものだ。

また、攻撃者はウェブサイトの脆弱性を悪用して利用者に偽の情報を表示させたり、意図しない操作をさせたりする。実際に悪用された脆弱性としてクロスサイト・スクリプティングやクロスサイト・リクエスト・フォージェリがある。その他、

SQL インジェクションやディレクトリ・トラバーサル等の一般的なウェブアプリケーションの脆弱性も狙われる可能性がある。

ウェブサイト運営者は、ウェブアプリケーションの脆弱性への対策が必要である。

＜影響＞

直接の被害を受けるのはミニブログサービスやSNSの利用者である。利用者は、ウイルス感染により情報が漏えいしたり、自身が利用しているサイトにおいて他者を中傷するようなコメントを、意図せず投稿させられたりしてしまう可能性がある。これらの被害を受けないために、利用者は、使用しているPCのOSやソフトウェアを最新バージョンにアップデートする、短縮URLを本来のURLで表示するツールやサービスを使用し、URLの信頼性を確認する等の対策をする必要がある。しかし、ウェブサイトの脆弱性を悪用した問題については、基本的に利用者側で適切に対策できない。そのため、運営しているウェブサイトの利用者が被害を受けないよう、ミニブログやSNSのウェブサイト運営者がセキュリティ対策を行う必要がある。

ウェブサイト運営者には、脆弱性が作り込まれないように設計段階からセキュリティを考慮し、脆弱性が発見された場合にも速やかに対応できる運用体制を確立することが望まれる。

＜2010年の事例・統計＞

2010年には、pixivのクロスサイト・リクエスト・フォージェリの脆弱性を悪用した問題やTwitterのクロスサイト・スクリプティングの脆弱性を悪用した問題が発生した。

2010年2月、イラストの投稿・閲覧に特化したSNSサイトであるpixivにおいて、クロスサイト・リクエスト・フォージェリの脆弱性が発見され、悪用される騒動があった。この騒動では、脆弱性を悪用された結果、pixivの利用者が他者を中傷するようなコメントを、意図せず投稿してしまう被害があった。

2010年9月、ミニブログサービスの一つであるTwitterにおいて、クロスサイト・スクリプティングの脆弱性が発見され、悪用される騒動があった。この騒動では、Twitterの利用者に意図していない投稿を行わせたり、利用者のTwitterの表示を崩してしまう被害があった。

その他、2010年12月には、短縮URLを悪用してTwitterの利用者をウイルス感染サイトへ誘導する攻撃が発生した。

関連資料

IPA：ウイルス・不正アクセス届出状況について（4月分）

http://www.ipa.go.jp/security/txt/2010/05outline.html

Twitterブログ:「マウスオーバーの」問題についての全容

http://blog.twitter.jp/2010/09/blog-post_22.html

pixiv開発者ブログ:[不具合報告]意図しない作品へのコメントについて

http://dev.pixiv.net/archives/1026973.html

CNET Japan: Twitterユーザーをターゲットにしたウイルス出現--URL短縮サービスのgoo.glを利用

http://japan.cnet.com/news/sec/20423830/

第 3 章 対策

第 1 章で述べたように、ひとたびセキュリティ事故を起こしてしまうと、システムへの影響に限らず、組織のブランドイメージや経営に大きな打撃を与えてしまう。また、セキュリティ対策が不十分なことで、意図せず攻撃に加担してしまうことからもセキュリティを確保することは、いわば企業の社会的責任であると言える。本章では、第 2 章で示した 10 大脅威の内容をベースにセキュリティ対策の考え方や方向性について解説する。

3.1 脅威の分類

セキュリティ対策を実施するにあたっては、損害が発生した際のビジネスへのインパクトを理解したうえで、現状の対応状況(セキュリティコントロール)と照らし合わせて、実施内容を検討する必要がある。今回の 10 大脅威で取上げた脅威を分類すると、大きく下記の3つのカテゴリに分類することができる。

次節以降で、この3つのカテゴリについて「情報漏えいに対する脅威」、「外部から攻撃される脅威」、「情報システムの設計・実装や運用に起因する脅威」と題して、対策の考えや方向性を説明する。

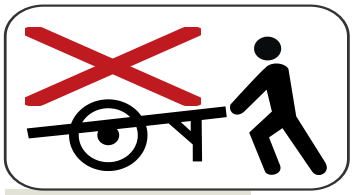
10大脅威		脅威の分類		
		情報漏えい	外部からの攻撃	システムの問題
1位	「人」が起こしてしまう情報漏えい	○		
2位	止まらない！ウェブサイトを経由した攻撃		○	
3位	定番ソフトウェアの脆弱性を狙った攻撃		○	
4位	狙われだしたスマートフォン		○	○
5位	複数の攻撃を組み合わせた新しいタイプの攻撃		○	
6位	セキュリティ対策不備がもたらすトラブル			○
7位	携帯電話向けウェブサイトのセキュリティ		○	○
8位	攻撃に気づけない標的型攻撃		○	
9位	クラウド・コンピューティングのセキュリティ	○	○	
10位	ミニブログサービスやSNSの利用者を狙った攻撃		○	

情報漏えいの脅威(情報漏えい)
組織で保持している情報(機密情報、個人情報など)を紛失や盗難などで漏えいする脅威

外部から攻撃される脅威(外部からの攻撃)
外部ネットワーク(主にインターネット)や電子媒体を経由した情報システムを脅かす攻撃。

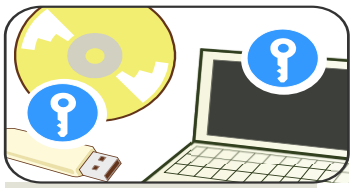
情報システムの設計や実装や運用に起因する脅威(システムの問題)
開発したアプリケーションのセキュリティ対策や対応の不備に起因する問題

3.2 情報漏えいに対する脅威への対策

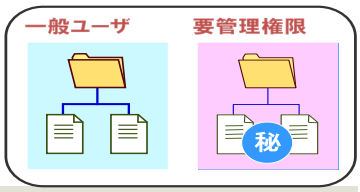


持出し禁止ルール

セキュリティ教育の実施



記録媒体等の暗号化



適切なアクセス権限付与

情報漏えいは、様々な漏えいルートがある為、考えられる情報漏えいのリスクに対応していく必要がある。

＜対策の考え方＞

情報漏えいは、内部の「人」による過失や故意、あるいは外部からの攻撃によって、引き起こされる。対策の基本的な考え方として、情報資産の明確化、管理ルールの策定とセキュリティ教育による運用管理に加えて、リスク低減と漏洩抑止効果を考慮したシステム的な対策を打つことが重要である。

以下に対策例を示す。

＜対策例＞

(1) セキュリティ運用対策

① 情報取扱いルール/罰則規定の制定

② アカウント・権限管理の実施

③ セキュリティ教育の実施

④ 情報漏えい時の対応体制・手順準備

(2) システム技術対策

① ネットワーク設計

② ユーザ認証・アクセス制御

③ 持出しデータ、重要データの暗号化

④ アクセスログの記録

＜クラウドにおける考慮点＞

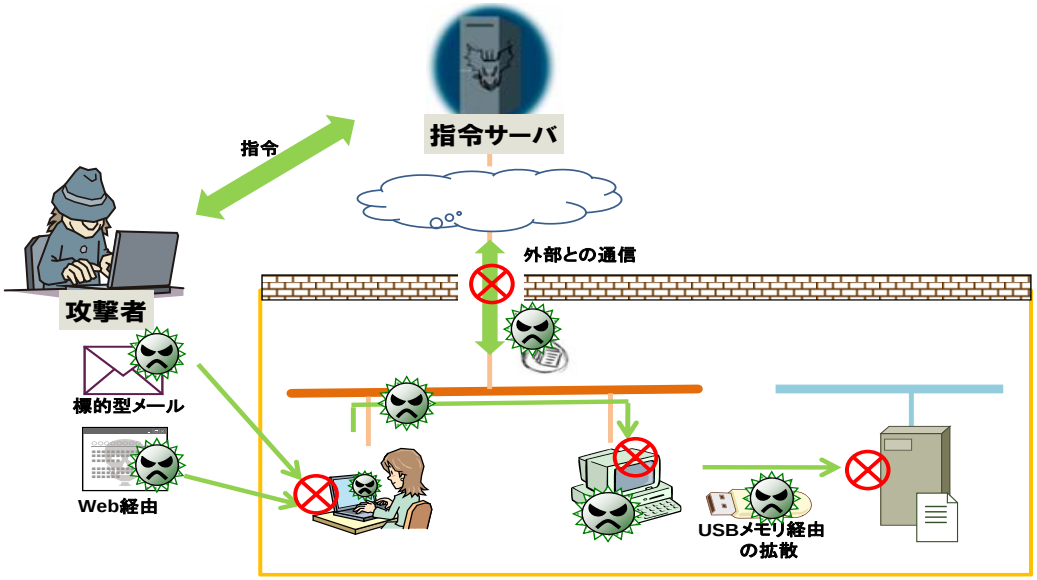
クラウド環境にデータを預ける場合、クラウド事業者によっては、データが海外に置かれることが考えられる。その際、利用者としてはデータの漏えいや消滅した場合の、法的対処やデータ保障等の内容が、事業継続性の観点からも重要となる。そのため、導入前にクラウド事業者との契約を明確にしておくことや、クラウド環境に預けるデータを識別してリスクを小さくして預ける等の考慮が必要である。

参考情報

IPA：情報漏えい対策のしおり

http://www.ipa.go.jp/security/antivirus/documents/5_roei_v3.pdf

3.3 外部から攻撃される脅威への対策



外部から攻撃される脅威の特徴は、第三者が悪意を持って他人の情報システムを攻撃してくることである。そのため、対策としては、攻撃者の手の内を理解した上で、攻撃を無効化する必要がある。ここでは、「5 位:新しいタイプの攻撃」について対策方法を説明する。

＜対策の考え方＞

新しいタイプの攻撃の特徴は、①脆弱性を突いてくることや巧みなソーシャル・エンジニアリングによってウイルスに感染。②そのウイルスが、外部の指令サーバと通信を行うことで、ウイルスが増強し、情報窃取やシステム破壊等の大きな被害をおよぼすことである。

従って、第二段の攻撃を抑止する最も効果的な対策として、ネットワーク設計に着眼し、外部からの不正アクセスの防御、および内部から外部の指令サーバとの不正な通信を遮断する対策を組込むことがポイントである。

また、本攻撃の特徴として、脆弱性を突いてくることや巧みなソーシャル・エンジニアリングが用いられる為、脆弱性対策や安易に添付ファイルを開かない等のセキュリティ教育も併せて実施しておくと良い。

＜対策例＞

(1) システム・ネットワーク設計対策

① ネットワーク設計

- 最重要部のネットワークの分離設計
- スイッチ等でのネットワーク分離設計
- 認証プロキシの導入
- システム外との P2P 通信の検知と遮断

② ウイルス対策製品の導入

(2) セキュリティ運用による対策

① クライアント／サーバの脆弱性対策

② セキュリティ教育の実施

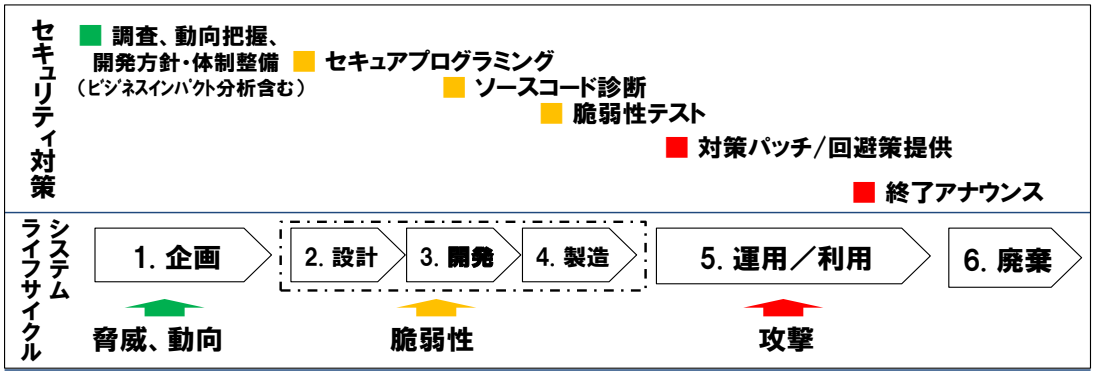
③ 通信の監視

参考情報

IPA:「IPAテクニカルレポート:『新しいタイプの攻撃』に関するレポート」

http://www.ipa.go.jp/about/technicalwatch/20101217.html

3.4 情報システムへの設計・実装や運用に起因する脅威への対策



開発されたシステムやソフトウェア製品は、一度公開されると長期間利用される。その間にセキュリティの面では、システムの脆弱性の露見や新たな脅威の出現に遭遇することになる。そのために、企画、設計・開発、運用フェーズに至るまで、「脆弱性を作り込まない開発」「対策を打てる体制」が求められる。以降に各開発フェーズにおける対策について、考え方と具体的な対策例を説明する。

＜対策の考え方＞

・企画・設計・開発・製造時の対応

企画・設計工程においては、当該アプリケーションに想定される脅威を洗い出し、防御機能として実装していく必要がある。また、開発・製造工程では、セキュアプログラミングや脆弱性テストを実施し、アプリケーションのセキュリティ実装の質を高めていく必要がある。

・運用利用時の対応

アプリケーションを狙った攻撃は、日進月歩で進化しており、新たな脆弱性や攻撃手法が発見されると昨日まで安全であったアプリケーションが脆弱なものになってしまう危険性がある。そのため、リリース後に脆弱性が発見された場合は、利用者がセキュリティ被害に遭うことがないように、対策パッチや回避策を提供し、広く利用者に周知することが重要である。また、公開しているシステムであれば、利用者に被害が及ばないように脆弱性の対策を実施することになるが、外部に開発委託したシステムなどでは、開発の契約時に開発業者が対応する範囲を明確にしておくことも重要となる。

・サポート終了時の対応

製品のサポートが終了する際は、事前に利用者にサポートが終了する旨のアナウンスを行い、サポート終了後は、セキュリティ対策が行われない旨を周知しておく必要がある。また、サポート終了後に推奨する使い方等あれば、併せて通知することが望ましい。

＜対策例＞

① 脅威の分析と対応方針の決定(企画時)
② セキュアプログラミングの実施
③ ソースコード診断の実施
④ 脆弱性テストの実施
⑤ 対策パッチ・回避策の提供
⑥ 終了アナウンス

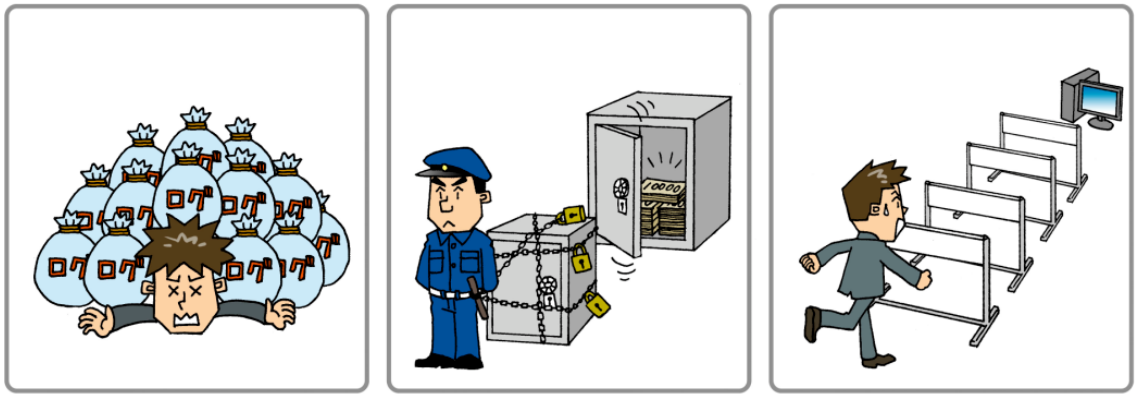
参考情報

IPA:「安全なウェブサイトの作り方」	http://www.ipa.go.jp/security/vuln/websecurity.html/
IPA:「脆弱性体験学習ツール AppGoat」	http://www.ipa.go.jp/security/vuln/appgoat/index.html

3.5 考慮事項

・有効に機能しないセキュリティ対策の一例

人手が足りない　　バランスが悪い運用　　業務に支障が出るルール



上記は、セキュリティ対策が有効に機能しないパターンの一例である。

セキュリティ対策は、いかに立派なルールや最新技術のセキュリティ製品を導入したとしても、それを運用する人的資源・運用体制に問題があれば、有効に機能しない。対策立案にあたっては、組織の特性や運用体制・体力を考慮し、効率かつ効果的な対策を立てる必要がある。

・効果的なセキュリティ対策の実施

効果的な対策の検討　　安全な設計・開発　　継続的な運用

セキュリティ対策は、情報システムのライフサイクルに合わせて、企画段階から運用を見越した対策を計画する必要がある。また、情報システムのライフサイクルは、企画、設計、開発、構築、運用を含めて、複数の事業者で構成されるケースが多く見られる。そのため、情報システムの構築・運営に携わる管理責任者と指示系統を明確化して、セキュリティ対策を実施する必要がある。

本ページは白紙です

【付録 1】10 大脅威関係表

付票 1 は、第 2 章で示した 10 大脅威の内容を理解していただきたい主な対象者を表す。

事業の情報技術依存度が高まり、情報システム関連の事故が、事業の存続すら脅かすリスクとなりつつある。実際、最近の情報流出事故やウェブサイトへの不正侵入事件より生じる損失は大きなものになっている。したがって、これらの事故や事件を未然に防止するためのセキュリティ対策が重要となる。

組織の経営者はセキュリティ対策において自組織がとるべき行動を内外に示し、システム管理者は組織のセキュリティ対策の方針のもと、適切にシステムやアカウントの管理を実施する必要がある。また、開発者はソフトウェアに作り込まれる脆弱性がどのようなものがあるのかを把握し、脆弱性を作り込まないように開発する必要がある。

どのような脅威が存在するのかを知り、セキュリティ対策実施の参考となれば幸いである。

付票 1. 脅威を理解していただきたい対象者

10大脅威		脅威を理解していただきたい対象者		
		経営者	システム管理者	開発者
1位	「人」が起こしてしまう情報漏えい	◎	○	
2位	止まらない！ウェブサイトを経由した攻撃		◎	○
3位	定番ソフトウェアの脆弱性を狙った攻撃		◎	○
4位	狙われだしたスマートフォン		○	◎
5位	複数の攻撃を組み合わせた新しいタイプの攻撃	◎	○	
6位	セキュリティ対策不備がもたらすトラブル	○		◎
7位	携帯電話向けウェブサイトのセキュリティ		○	◎
8位	攻撃に気づけない標的型攻撃	◎	○	
9位	クラウド・コンピューティングのセキュリティ	◎	○	○
10位	ミニブログサービスやSNSの利用者を狙った攻撃			◎

◎：特に脅威を理解していただきたい対象者　○：脅威を理解していただきたい対象者

【付録 2】10 大脅威の変遷

付票 2 は、第 2 章で示した 10 大脅威と過去の 10 大脅威の順位を比較したものである。

2011 年版の 10 大脅威は、スマートフォンや SNS の利用者を狙った攻撃等、過去の 10 大脅威には含まれていない 5 つの脅威が登場した。情報漏えいや標的型攻撃等は、毎年 10 位内に登場する脅威である。

付票 2. 10 大脅威の変遷

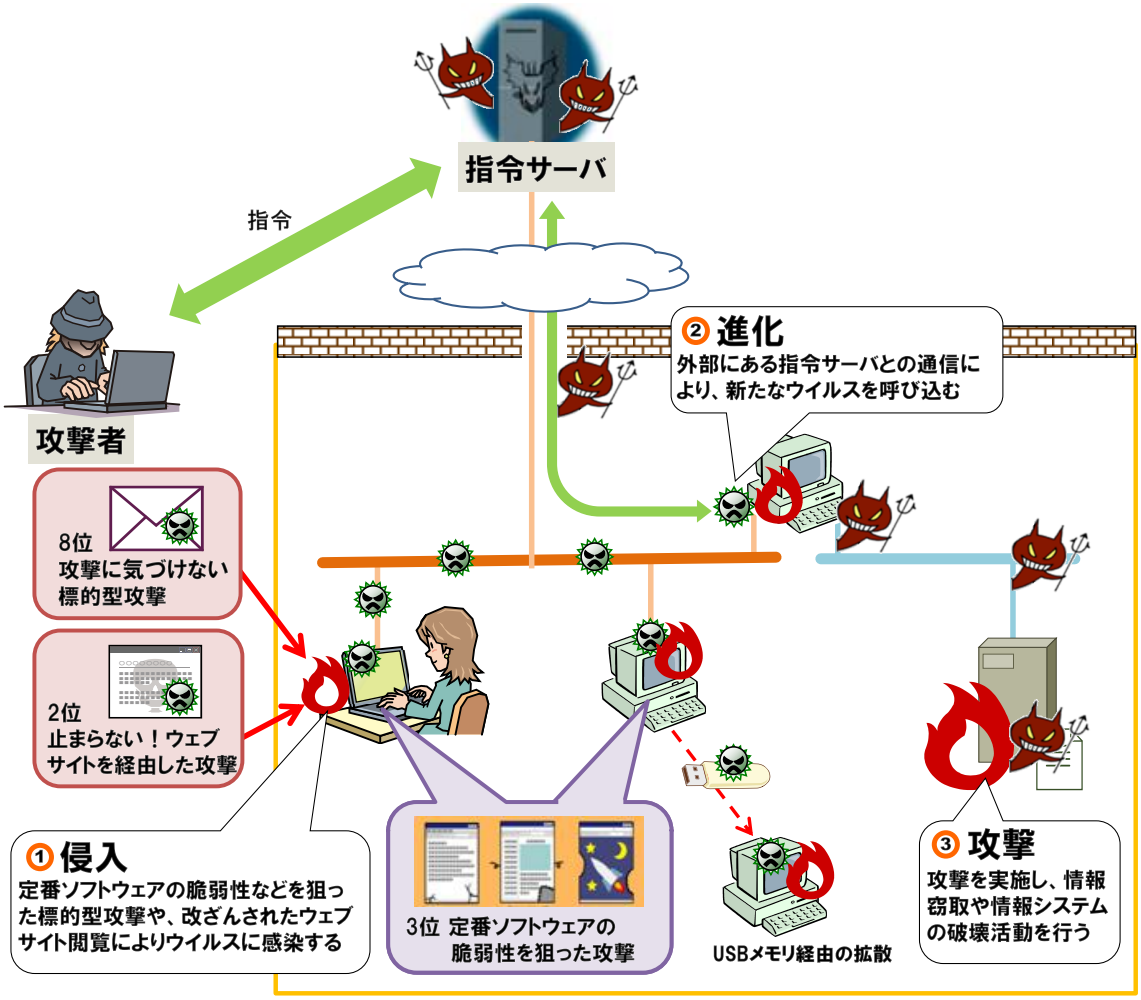
2010年10大脅威		2009年順位	2008年順位	2007年順位	2006年順位
1位	「人」が起こしてしまう情報漏えい	5位	5位	3位	7位
2位	止まらない！ウェブサイトを経由した攻撃	1位	2位	5位	9位
3位	定番ソフトウェアの脆弱性を狙った攻撃	2位	—	8位	—
4位★	狙われだしたスマートフォン	—	—	—	—
5位★	複数の攻撃を組み合わせた新しいタイプの攻撃	—	—	—	—
6位★	セキュリティ対策不備がもたらすトラブル	—	—	—	—
7位★	携帯電話向けウェブサイトのセキュリティ	—	—	—	—
8位	攻撃に気づけない標的型攻撃	6位	3位	4位	2位
9位	クラウド・コンピューティングのセキュリティ	9位	—	—	—
10位★	ミニブログサービスやSNSの利用者を狙った攻撃	—	—	—	—

★：IPA が公表している「10 大脅威」において、新しく登場した脅威

【付録 3】10 大脅威と「新しいタイプの攻撃」の関連図

次の図は、10 大脅威の『5 位 複数の攻撃を組み合わせた「新しいタイプの攻撃」』に関連する脅威を示したものである。第 2 章の 5 位を補足する図である。

「新しいタイプの攻撃」は、組織内の重要な情報の窃取やシステムの情報破壊を目的とした攻撃の総称である。特徴として、既存の攻撃方法を複雑・高度に組み合わせており、「2 位 止まらない！ウェブサイトを経由した攻撃」、「3 位 定番ソフトウェアの脆弱性を狙った攻撃」、「8 位 攻撃に気づけない標的型攻撃」等の攻撃が使われている点が挙げられる。



付図 1.『5 位 複数の攻撃を組み合わせた「新しいタイプの攻撃」』の関連図

執筆協力者

10 大脅威執筆者会 構成メンバー

氏名	所属	氏名	所属
渡部 章	(株)アークン	岡谷 貢	内閣官房情報セキュリティセンター
石田 淳一	(株)アールジェイ	鍋島 学	内閣官房情報セキュリティセンター
加藤 雅彦	(株)インターネットイニシアティブ	須川 賢洋	新潟大学
高橋 康敏	(株)インターネットイニシアティブ	徳田 敏文	日本アイ・ビー・エム(株)
齋藤 衛	(株)インターネットイニシアティブ	井上 博文	日本アイ・ビー・エム(株)
三輪 信雄	S&J コンサルティング(株)	守屋 英一	日本アイ・ビー・エム(株)
小林 克巳	NRI セキュアテクノロジーズ(株)	梨和 久雄	日本アイ・ビー・エム(株)
大塚 淳平	NRI セキュアテクノロジーズ(株)	谷川 哲司	日本電気(株)
石川 朝久	NRI セキュアテクノロジーズ(株)	宇都宮 和顕	日本電気(株)
西尾 秀一	(株)NTT データ	秋山 卓司	(社)日本電子認証協議会(JCAF)
池田 和生	(株)NTT データ	長島 雅夫	日本電信電話(株)
林 健一	(株)NTT データ	杉浦 芳樹	日本電信電話(株)
入宮 貞一	(株)NTT データ	住本 順一	日本電信電話(株)
井上 克至	(株)NTT データ	やすだ なお	NPO 法人 日本ネットワークセキュリティ協会(JNSA)
前田 典彦	(株)Kaspersky Labs Japan		
徳江 崇宏	京セラコミュニケーションシステム(株)	榎本 司	日本ヒューレット・パッカード(株)
		西垣 直美	日本ヒューレット・パッカード(株)
林 弘毅	経済産業省	佐藤 直之	日本ベリサイン(株)
枝川 慶彦	経済産業省	杉岡 弘毅	(株)ネクストジェン
島田 紀章	経済産業省	大村 友和	(株)ネクストジェン
鈴木 啓紹	(社)コンピュータソフトウェア協会(CSAJ)	圓山 大介	(株)ネクストジェン
		山田 陽介	ネットエージェント(株)
福森 大喜	(株)サイバーディフェンス研究所	高橋 潤哉	(株)ネットセキュリティ総合研究所
名和 利男	(株)サイバーディフェンス研究所	徳丸 浩	HASH コンサルティング(株)
高木 浩光	(独)産業技術総合研究所	水越 一郎	東日本電信電話(株)
大岩 寛	(独)産業技術総合研究所	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(JPCERT/CC)	吉野 友人	(株)ビジネス・アーキテクツ
		本川 祐治	(株)日立情報システムズ
伊藤 友里恵	(社)JPCERT コーディネーションセンター(JPCERT/CC)	丹京 真一	(株)日立情報システムズ
		寺田 真敏	(株)日立製作所
宮崎 清隆	(社)JPCERT コーディネーションセンター(JPCERT/CC)	梅木 久志	(株)日立製作所
		藤原 将志	(株)日立製作所
古田 洋久	(社)JPCERT コーディネーションセンター(JPCERT/CC)	鵜飼 裕司	(株)フォティーンフォティ技術研究所
		金居 良治	(株)フォティーンフォティ技術研究所
高橋 紀子	(社)JPCERT コーディネーションセンター(JPCERT/CC)	森 玄理	富士通(株)
		冨士原 裕文	富士通(株)
林 薫	(株)シマンテック	小林 浩治	富士通(株)
山内 正	(株)シマンテック総合研究所	金谷 延幸	(株)富士通研究所
大野 雅子	(株)スマートバリュー	望月 大光	(株)富士通ソフトウェアテクノロジーズ
星澤 裕二	(株)セキュアブレイン	木村 秀年	富士通 CIT(株)
神薗 雅紀	(株)セキュアブレイン	佐藤 友治	(株)ブロードバンドセキュリティ
正木 健介	セコムトラストシステムズ(株)	藤田 耕作	放送大学大学院
澤永 敏郎	ソースネクスト(株)	高橋 正和	マイクロソフト(株)
青谷 征夫	ソースネクスト(株)	加藤 義宏	マカフィー(株)
百瀬 昌幸	(財)地方自治情報センター(LASDEC)	国分 裕	三井物産セキュアディレクション(株)
		後藤 久	三井物産セキュアディレクション(株)
木村 道弘	(株)電子商取引安全技術研究所	寺田 健	三井物産セキュアディレクション(株)
渡辺 淳	(株)デンソーウェーブ	村瀬 一郎	(株)三菱総合研究所
山岸 正	東京大学	川口 修司	(株)三菱総合研究所
吉松 健三	(株)東芝	村野 正泰	(株)三菱総合研究所
小島 健司	東芝ソリューション(株)	青木 歩	(株)ユービーセキュア
小屋 晋吾	トレンドマイクロ(株)	松岡 秀和	(株)ユービーセキュア

氏名	所属	氏名	所属
杉山 俊春	(株)ユービーセキュア		
志田 智	(株)ユビテック		
福本 佳成	楽天(株)		
岩井 博樹	(株)ラック		
山崎 圭吾	(株)ラック		
柳澤 伸幸	(株)ラック		
川口 洋	(株)ラック		
伊藤 耕介	(株)ラック		
若居 和直	(株)ラック		
中田 邦彦	ルネサスエレクトロニクス（株）		
矢島 秀浩			
小森 聡			
小松 文子			
杉浦 昌			
島 成佳			
小門 寿明			
木邑 実			
加賀谷 伸一郎			
花村 憲一			
宮本 一弘			
小林 偉昭			
金野 千里			
中野 学			
渡辺 貴仁			
大森 雅司			
園田 道夫			
勝海 直人			
永安 佑希允			
相馬 基邦			
大谷 槙吾			
谷口 隼祐			
甲斐根 功			

※独立行政法人情報処理推進機構の職員については所属組織名を省略しました

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

執筆協力者　10 大脅威執筆者会

執筆者　谷口 隼祐　大森 雅司

2011 年版

10 大脅威『進化する攻撃...その対策で十分ですか？』

2011 年 3 月 24 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。

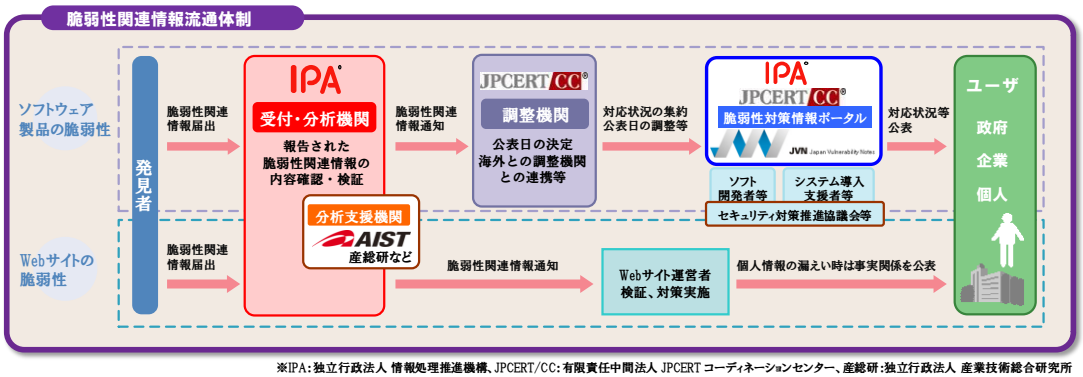
ソフトウエア製品脆弱性関連情報

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:有限責任中間法人 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/