# 情報セキュリティ

# 10 大脅威 2016

## ～個人と組織で異なる脅威、立場ごとに適切な対応を～


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

2016 年 3 月

本書は、以下の URL からダウンロードできます。

「情報セキュリティ 10 大脅威 2016」
https://www.ipa.go.jp/security/vuln/10threats2016.html

# 目次

# はじめに

本書「情報セキュリティ 10 大脅威 2016」は、情報セキュリティ専門家を中心に構成する「10 大脅威選考会」約 100 名の協力により、2015 年に発生したセキュリティ事故や攻撃の状況等から脅威を選出し、投票により順位付けして解説した資料である。例年、総合的な見地から順位を決定しているが、今回は「個人」と「組織」という異なる視点で、それぞれにおける脅威を順位付けし、それを基に 10 大脅威を決定した。

各脅威が自分自身や自組織にどう影響するか確認しながら本書を読み進めることで、様々な脅威と対策を網羅的に把握できる。

本書が、読者自身のセキュリティ対策への取り組みと、各組織の研修やセキュリティ教育等に活用されることによるセキュリティ対策の普及の一助となることを期待する。

**【本書の概要】**

- 「10 大脅威」の 10 年史

「10 大脅威」という名称で解説資料を公開して丸 10 年が経過し、今回が 11 年目にあたる。
第 1 章では、過去 10 年の「10 大脅威」について振り返る。

- 情報セキュリティ 10 大脅威 2016（10 大脅威）

2015 年は日本年金機構に端を発した標的型攻撃の報道が相次いだ。また、相変わらず金銭に絡んだ内部不正も発生している。個人にとっての脅威に目を向ければ、インターネットバンキングの総被害額は過去最悪だった 2014 年を上回り、日本語対応したランサムウェアの被害も急増している。攻撃者の手口は巧妙かつ悪質になってきている。
第 2 章では、2015 年の脅威の動向を 10 大脅威として解説する。

- 注目すべき脅威や懸念

サポートが終了してパッチが提供されなくなったソフトウェアを使い続けている PC が残存している。また、本来は盗聴や改ざん、なりすましといった脅威を防止するための公開鍵証明書にかかわる脆弱性によって、新たな攻撃のきっかけが生まれている。さらに、2016 年 1 月からマイナンバーの利用が開始されたが、個人が自身のマイナンバーを適切に管理すると共に、他者のマイナンバーを預かる関係者が厳重に管理・運用する必要がある。
第 3 章では、これらの課題や脅威について解説する。

# 1章. 10 大脅威の 10 年史

# 1 章 10 大脅威の 10 年史

2005 年 3 月、IPA のコンピュータ・セキュリティ検討会が「コンピュータ・セキュリティ ～2004 年の傾向と今後の対策～」という名称で前年の脅威についての解説資料を公開した。翌 2006 年からは、情報セキュリティ専門家を中心に構成する「10 大脅威選考会（当初は、情報セキュリティ検討会）」の投票により、前年の脅威を順位付けした「10 大脅威」として年度末に公開してきた。

「10 大脅威」は 10 大脅威 2006 から 10 大脅威 2015 までで丸 10 年となり、今回の 10 大脅威 2016 から新たな 10 年に突入した。これを機に過去 10 年の「10 大脅威」を振り返り、社会的背景、脅威や攻撃手法の移り変わりとの関係を見ていく。

## 1.1. 情報セキュリティの変遷

10 大脅威 2006 から 10 大脅威 2015 の「10 大脅威」がその対象とした期間は、2005 年から 2014 年である。この間、国内外で様々な情報セキュリティに関する事件があった。また、これらに対抗するため、様々な対処方法が生み出されてきた。図 1.1 は IT 環境の進歩やそれに伴う脅威、攻撃傾向、を表したものである。10 年前の 2005 年から 2014 年までの流れを見てみると、IT 技術の発展とともに、脅威の種類が増え続けていることがわかる。

10 年前は、まだスマートフォンもなく、携帯電話（ガラケー）が全盛であった。その後、ユビキタスという言葉が使われだし、公衆無線 LAN の環境が整備され始めてきた。そして、スマートフォンやタブレットといったモバイル端末が登場した。モバイルネットワーク基盤が整備され、SNS やクラウド等のサービスが提供され、便利な世の中になっていくのに伴い、情報セキュリティにおける脅威は増えていった。

一昔前は、自身の IT スキルを誇示することが目的の愉快犯が主流であったが、2004 年頃からは、そのスキルを悪用して不正に金銭を得る者も出てきた。また、より高度な手法で組織の重要情報を窃取する標的型攻撃は、手口の巧妙化を図りながら、ここ 10 年継続・進化しており、国や組織にとって大きな脅威となっている。さらには社会的・政治的な主張を目的としたハクティビストと呼ばれるハッカー集団も現れてきた。近年は、これらの犯罪行為を安易に模倣する人物が現れており、逮捕された事例もある。また、内部不正・犯行も、大きな脅威となっている。権限を持っている人がその権限を使って情報を持ち出すため、対策が難しく、組織のセキュリティ管理者を悩ませた。

攻撃者はシステム内から情報を窃取したり、ウェブサイトを改ざんしたりする。そのためにソフトウェアの脆弱性を突いたり、ウイルスを使ったり、ソーシャルエンジニアリングを駆使したり、内部不正をする。攻撃者の罠にはまらないためにも過去の事例や動向を知ることは重要である。次の 1.2 節では、過去 10 年の「情報セキュリティ 10 大脅威」にランクインした計 100 個の脅威を基に 10 年間の脅威の特徴や傾向を見ていく。

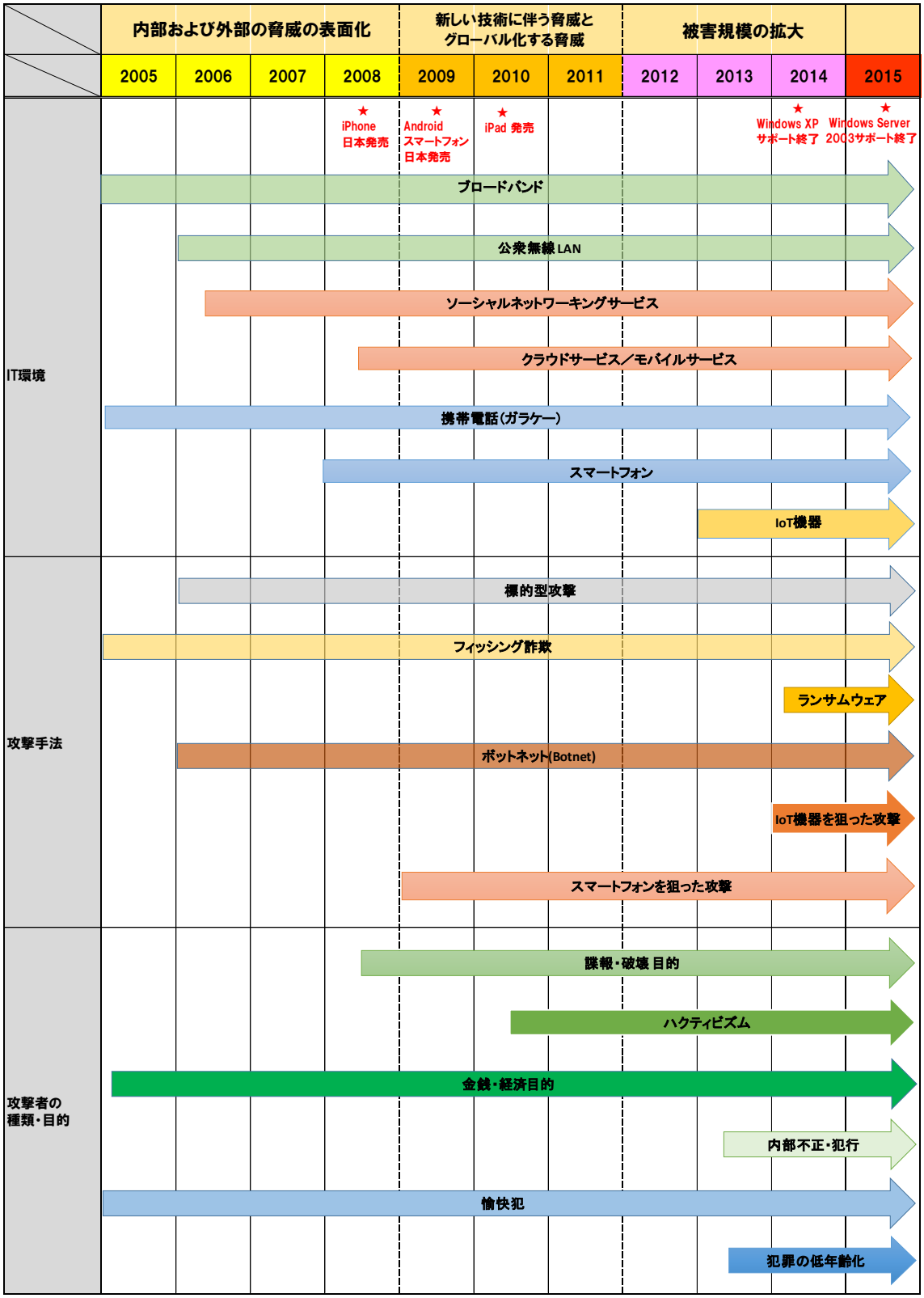



図 1.1:情報セキュリティの変遷

## 1.2. 10 大脅威の 10 年の変遷

過去 10 年の 10 大脅威について振り返ってみる。前節では情報セキュリティの変遷について記載したが、10 大脅威の変遷とあわせて見ることで、その年の脅威をより深く理解することができる。

今回は、以下 3 つの期間に分けてその期間ごとの特徴的な脅威について見ていく。

(1) 2005 年～2008 年の 4 年間（10 大脅威 2006～2009）
(2) 2009 年～2011 年の 3 年間（10 大脅威 2010～2012）
(3) 2012 年～2014 年の 3 年間（10 大脅威 2013～2015）

## （1） 2005 年～2008 年の 10 大脅威の振り返り

この時期には、家庭用ゲーム機にオンライン機能が標準搭載され、YouTube やニコニコ動画が始まり、iPhone が発売された。リーマンショックが起こったのもこの頃である。

表 1.1:2005 年～2008 年の 10 大脅威

| 順位 | 2005年 | 2006年 | 2007年 | 2008年 |
|---|---|---|---|---|
| 1位 | 事件化するSQLインジェクション | 漏えい情報のWinnyによる止らない流通 | 高まる「誘導型」攻撃の脅威 | DNSキャッシュポイズニングの脅威 |
| 2位 | Winnyを通じたウイルス感染による情報漏えいの多発 | 表面化しづらい標的型（スピア型）攻撃 | ウェブサイトを狙った攻撃の広まり | 正規ウェブサイトを経由した攻撃の猛威 |
| 3位 | 音楽CDに格納された「ルートキットに類似した機能」の事件化 | 悪質化・潜在化するボット | 恒常化する情報漏えい | 巧妙化する標的型攻撃 |
| 4位 | 悪質化するフィッシング詐欺 | 深刻化するゼロデイ攻撃 | 巧妙化する標的型攻撃 | 検知されにくいボット、潜在化するコンピュータウイルス |
| 5位 | 巧妙化するスパイウェア | ますます多様化するフィッシング詐欺 | 信用できなくなった正規サイト | 恒常化する情報漏えい |
| 6位 | 流行が続くボット | 増え続けるスパムメール | 検知されにくいボット、潜在化するコンピュータウイルス | 脆弱な無線LAN暗号方式における脅威 |
| 7位 | ウェブサイトを狙うCSRFの流行 | 減らない情報漏えい | 検索エンジンからマルウェア配信サイトに誘導 | 誘導型攻撃の顕在化 |
| 8位 | 情報家電、携帯機器などの組込みソフトウェアにひそむ脆弱性 | 狙われ続ける安易なパスワード | 国内製品の脆弱性が頻発 | 減らないスパムメール |
| 9位 | セキュリティ製品の持つ脆弱性 | 攻撃が急増するSQLインジェクション | 減らないスパムメール | 組込み製品に潜む脆弱性 |
| 10位 | ゼロデイ攻撃 | 不適切な設定のDNSサーバを狙う攻撃の発生 | 組み込み製品の脆弱性の増加 | ユーザIDとパスワードの使いまわしによる危険性 |
| 10大脅威名 | 10大脅威2006 | 10大脅威2007 | 10大脅威2008 | 10大脅威2009 |

凡例：

| | | | | | |
|---|---|---|---|---|---|
| 脆弱性関連 | ウェブサイト関連<br>不正ログイン関連<br>パスワード関連 | 標的型攻撃関連 | インターネット<br>バンキング関連 | 情報漏えい関連<br>内部不正、Winny | スマートフォン<br>関連 |

### ■Winny による情報漏えい被害拡大

2005 年から 2008 年の特徴的な脅威の 1 つに「情報漏えい」がある。特にファイル交換ソフトである Winny の機能を悪用した Antinny ウイルスによる情報漏えいは、個人と組織の双方で被害が続出した。「情報漏えい」は、2005 年に 2 位、2006 年に 1 位、2007 年に 3 位、2008 年に 5 位となり、常にトップ 5 にランクインしている。

Antinny は Winny がインストールされている PC 内のファイルを故意に Winny ネットワークへ流出させてしまうウイルスである。Winny 利用者の多さから、Antinny による被害は大きな問題となった。Winny ネットワーク上に流出した情報は次々に拡散されていくため、削除することは現実的には不可能である。Antinny による情報漏えいは、金銭目的や諜報目的というよりは愉快犯的なものであったといえる。

**■狙われる組織の情報、標的型攻撃の登場**

この時期の特徴的な傾向として「標的型攻撃」の登場がある。10 大脅威では、2006 年に 2 位で初登場して以来、常にトップ 10 にランクインしている。2015 年に起きた日本年金機構の事件をきっかけに、情報セキュリティに馴染みがない人たちにも知れ渡ることとなった「標的型攻撃」だが、10 年前から危険視されていたことがわかる。この頃の標的型攻撃は、攻撃者が送ったメールに添付されているファイルを実行することでウイルスに感染させ、機密情報を窃取するものであり、現在の標的型攻撃メールと同じ狙いである。添付されているファイルは、exe ファイル等の実行ファイルが多かったが、文書ファイルの脆弱性を悪用したものも出始めてきた。この頃はまだメール本文中の URL をクリックさせて、不正なサイトに誘導する手口は確認されていない。

**■10 年以上前から存在する、根深い脆弱性にかかわる脅威**

「脆弱性」という言葉はまだ世の中に浸透していなかったが、ウェブサイトやソフトウェアの「脆弱性」に関する脅威が数多くランクインしている。PC の普及やインターネット環境の整備が進んだことで、ウェブサイトが組織活動やサービス事業に不可欠な IT 基盤となってきた。これに伴い、ウェブサイトやソフトウェアに関する脆弱性を悪用した攻撃が増えている。10 大脅威では、脆弱性関連の脅威を今よりも細かく分けており、毎年、複数の脅威がランクインしている。攻撃者は脆弱性を突いて攻撃することが多く、いまだに大きな脅威となっている。

**■総括**

昨今、何かと耳にする「標的型攻撃」や「脆弱性」にかかわる脅威は、既に 10 年以上前から存在していて、その後 10 年以上変わらない大きな脅威となっている。一方、Winny の事例からわかるように、情報漏えい事件等によりインパクトあるニュースが報道されたことで、人目につかないところに存在していた脅威が顕在化し、組織や個人はその対策に追われていた。このように、技術の発展・普及に伴い、内部および外部の情報セキュリティに関する脅威が表面化し、それに対して組織側で対応が求められてきた期間といえるだろう。

## （2） 2009 年～2011 年の 10 大脅威の振り返り

この時期には、3D 映画「アバター」の大ヒットをきっかけに 3D ブームが起こり、デジタルカメラ、テレビ、携帯用ゲーム機等で 3D モデルが登場した。また、iPad の発売が開始した。

表 1.2:2009 年～2011 年の 10 大脅威

| 順位 | 2009年 | 2010年 | 2011年 |
|---|---|---|---|
| 1位 | 変化を続けるウェブサイト改ざんの手口 | 「人」が起こしてしまう情報漏えい | 機密情報が盗まれる！？新しいタイプの攻撃 |
| 2位 | アップデートしていないクライアントソフト | 止らない！ウェブサイトを経由した攻撃 | 予測不能の災害発生！引き起こされた業務停止 |
| 3位 | 悪質なウイルスやボットの多目的化 | 定番ソフトウェアの脆弱性を狙った攻撃 | 特定できぬ、共通思想集団による攻撃 |
| 4位 | 対策をしていないサーバ製品の脆弱性 | 狙われだしたスマートフォン | 今もどこかで・・・更新忘れのクライアントソフトを狙った攻撃 |
| 5位 | あわせて事後対応を！情報漏えい事件 | 複数の攻撃を組み合わせた新しいタイプの攻撃 | 止らない！ウェブサイトを狙った攻撃 |
| 6位 | 被害に気づけない標的型攻撃 | セキュリティ対策不備がもたらすトラブル | 続々発覚、スマートフォンやタブレットを狙った攻撃 |
| 7位 | 深刻なDDoS攻撃 | 携帯電話向けウェブサイトのセキュリティ | 大丈夫！？電子証明書に思わぬ落とし穴 |
| 8位 | 正規のアカウントを悪用される攻撃 | 攻撃に気づけない標的型攻撃 | 身近に潜む魔の手・・・あなたの職場は大丈夫？ |
| 9位 | クラウド･コンピューティングのセキュリティ問題 | クラウド･コンピューティングのセキュリティ | 危ない！アカウントの使いまわしが被害を拡大！ |
| 10位 | インターネットインフラを支えるプロトコルの脆弱性 | ミニブログサービスやSNSの利用者を狙った攻撃 | 使用者情報の不適切な取扱いによる信用失墜 |
| 10大脅威名 | 10大脅威2010 | 10大脅威2011 | 10大脅威2012 |

凡例：

| | | | | | |
|---|---|---|---|---|---|
| 脆弱性関連 | ウェブサイト関連<br>不正ログイン関連<br>パスワード関連 | 標的型攻撃関連 | インターネット<br>バンキング関連 | 情報漏えい関連<br>内部不正、Winny | スマートフォン<br>関連 |

### ■猛威を振るうガンブラー被害、それに伴い懸念される脆弱性の脅威

2009 年から 2011 年の間の特徴的な脅威の 1 つとして、ガンブラーに関する脅威が挙げられる。10 大脅威では「ウェブ改ざん」の攻撃の主因として、2009 年の 1 位、2010 年の 2 位に含まれている。しかし、2011 年の 5 位には含まれておらず、その攻撃は 2010 年でほぼ収束している。また、ガンブラーは PC にインストールされているクライアントソフトウェアの脆弱性を悪用するため、ガンブラーの脅威と同調する形でクライアントソフトウェアの脆弱性に関する脅威が、2009 年には 2 位、2010 年には 3 位と上位にランクインしている。

**■新しい IT 技術の普及に伴う新たな脅威**

新しい IT 技術の普及に伴う特徴的な脅威として、クラウドサービスやスマートフォンに関する脅威が挙げられる。2009 年から 2011 年はクラウドサービスの利用の促進や携帯電話（ガラケー）からスマートフォンへの転換等、より便利で多機能な技術の活用が進んだ時期である。それに伴い、クラウドサービスの脆弱性に関する脅威は、2009 年と 2010 年に 9 位にランクインし、スマートフォンの脆弱性に関する脅威は 2010 年に 4 位、2011 年に 6 位にランクインしている。このように世の中で活用され始めた技術に関する脅威が徐々にランクインし始めてきた。

**■現実化した事業継続の必要性**

2011 年に発生した東日本大震災は地域社会に多大な被害を与えた。この地震で被災した企業の中には事業継続に支障をきたす等の大きな影響を受けた企業もあった。これを受けて、BCP（Business Continuity Plan、事業継続計画）という災害、事故、テロ等不測の事態を想定して、事業継続の視点から対策を取り決めておく考え方が注目を集めた。10 大脅威でも、2011 年の 2 位にランクインしている。

**■サイバー犯罪のグローバル化、集団によるサイバー攻撃の被害の表面化**

ハクティビスト（hacktivist）と呼ばれる、社会的・政治的な主張を目的とした集団によるサイバー攻撃の被害が表面化してきた。ハクティビストは、サーバーに多大な負荷をかける DDoS 攻撃によりウェブサイトを機能不全にしたり、自分たちの主張を掲載するようにウェブサイトを改ざんしたりと、様々な攻撃を行った。また、この集団は、複数の国や組織の人間で構成されており、地球上の様々なところから攻撃を行う。標的とされた組織は対策に苦慮することになった。これを受け、ハクティビストに関する脅威が、2011 年の 3 位にランクインしている。

**■引き続き行われる標的型攻撃**

この期間も引き続き標的型攻撃は行われている。特に 2011 年は、大手重機メーカーや衆議院への攻撃等立て続けに行われ大きく報道された。情報が国外に流出した可能性もあり、標的型攻撃が非常に大きな脅威であることが広く認識された。これを受け、10 大脅威において、2011 年に 1 位となった。

**■総括**

ガンブラーや東日本大震災等、突発的な被害の発生は、組織や個人を大きく混乱させた。それにより、脆弱性対策や BCP 等継続的な対策の必要性が再認識させられた。また、スマートフォンやクラウドサービス等新しい技術が普及しだし、それに関する脅威が表面化してきている。一方、ハクティビストや標的型攻撃に見られるように国外からの脅威が大きな懸案となっている。このように、突発的な脅威に加え、新しい技術の登場に伴う脅威のさらなる表面化や、国外からの攻撃といったサイバー犯罪のグローバル化がこの期間の特徴といえるだろう。

### （3） 2012 年～2014 年の 10 大脅威の振り返り

この時期には、東京スカイツリーが開業し、富士山が世界文化遺産に登録された。また、2020 年のオリンピック／パラリンピックの開催都市が東京に決定した。

表 1.3:2012 年～2014 年の 10 大脅威

| 順位 | 2012年 | 2013年 | 2014年 |
|---|---|---|---|
| 1位 | クライアントソフトの脆弱性を突いた攻撃 | 標的型メールを用いた組織へのスパイ・諜報活動 | インターネットバンキングやクレジットカード情報の不正利用 |
| 2位 | 標的型諜報攻撃の脅威 | 不正ログイン・不正利用 | 内部不正による情報漏えい |
| 3位 | スマートデバイスを狙った悪意あるアプリの横行 | ウェブサイトの改ざん | 標的型攻撃による諜報活動 |
| 4位 | ウイルスを使った遠隔操作 | ウェブサービスからの利用者情報の漏えい | ウェブサービスへの不正ログイン |
| 5位 | 金銭窃取を目的としたウイルスの横行 | オンラインバンキングからの不正送金 | ウェブサービスからの顧客情報の窃取 |
| 6位 | 予期せぬ業務停止 | 悪意あるスマートフォンアプリ | ハッカー集団によるサイバーテロ |
| 7位 | ウェブサイトを狙った攻撃 | SNSへの不適切な情報公開 | ウェブサイトの改ざん |
| 8位 | パスワード流出の脅威 | 紛失や設定不備による情報漏えい | インターネット基盤技術を悪用した攻撃 |
| 9位 | 内部犯行 | ウイルスを使った詐欺・恐喝 | 脆弱性公表に伴う攻撃 |
| 10位 | フィッシング詐欺 | サービス妨害 | 悪意のあるスマートフォンアプリ |
| 10大脅威名 | 10大脅威2013 | 10大脅威2014 | 10大脅威2015 |

凡例：

| 脆弱性関連 | ウェブサイト関連<br>不正ログイン関連<br>パスワード関連 | 標的型攻撃関連 | インターネット<br>バンキング関連 | 情報漏えい関連<br>内部不正、Winny | スマートフォン<br>関連 |
|---|---|---|---|---|---|

**■金銭被害拡大、狙われるインターネットバンキング・クレジットカード**

2012 年から 2014 年の間の特徴的な脅威の 1 つとして、インターネットバンキングやクレジットカード情報の不正利用に関する脅威が挙げられる。警察庁によると、不正送金による総被害額は 2012 年が約 4,800 万円、2013 年が約 14 億 600 万円、2014 年が約 29 億 1,000 万円となっており、年を追うごとに総被害額が大きく増加している。10 大脅威においても、被害金額の上昇に伴い、2012 年に 10 位、2013 年に 5 位、2014 年に 1 位と脅威の順位が上がっている。

**■パスワードの使いまわしによる被害拡大、求められる利用者のリテラシー**

オンラインショッピング等、ログインして利用するサービスが個人においても広く普及してきた。それに伴う脅威の 1 つとして、パスワードの使いまわし等による不正ログインに関する脅威が挙げられる。2012 年に 8 位、2013 年に 2 位、2014 年に 4 位と常に 10 大脅威にランクインしている。不正ログインをされると、例えばオンラインショッピングで勝手に商品を購入されたり、自身になりすまして SNS（Social Networking Service、Facebook や LINE 等のサービス）を使われたり等の被害を受ける。

**■内部犯行により持ち出される個人情報、問われる企業の管理体制**

2014 年には大手通信教育会社の委託先社員が内部不正を働き、約 3,504 万件もの名簿情報が漏えいする事件が起こった。漏えいした名簿情報は名簿会社に渡り、ダイレクトメールの宛先に使われた。これに対して情報漏えい元の企業では、情報が漏えいした顧客への補償として総額 200 億円を準備した。情報を漏えいした組織にとっては賠償金による損失以外に信頼の失墜という損失もあった。これを受け、10 大脅威において、2014 年に 2 位となっている。

**■引き続き狙われるスマートフォン**

2010 年から登場したスマートフォン関連の脅威が、10 大脅威として、2012 年に 3 位、2013 年に 6 位、2014 年に 10 位とこの期間でも引き続き 10 大脅威にランクインしている。昨今、スマートフォンは生活する上で必需品となってきており、それにかかわる脅威も顕在化している。特に、2012 年には、偽アプリにより約 1,000 万件の個人情報が窃取されるという、大規模な漏えい被害もあった。

**■軽率な情報配信行為による脅威の顕在化**

新たな脅威の 1 つとして、2013 年 7 位の SNS に関する脅威がある。主に 10 代～20 代の若者が Twitter を使って自身の反社会的行動の写真を公開する行為が横行し、「バカッター」と呼ばれた。スマートフォン等の操作が容易で便利なツールを、自己顕示欲が強く、倫理観が欠落した一部の若者が稚拙な使用をしたことで騒動が大きくなった。ちょっとしたいたずらのつもりでも、被害を受けた企業側の損害は大きく、当人たちは逮捕や補導されて、事の重大さに気づくこととなった。また、個人だけではなく、組織においても、立場上不適切な発言を配信してしまうことで降格や停職等の処分を受けるケースもあった。

**■総括**

億を超える金銭被害や千万単位の漏えい等、被害規模が非常に大きくなっていることがわかる。また、軽率な情報配信を行う一部の若者が大きくニュースで報道される等、若者を中心とした軽率な行動に起因する犯罪もこの期間の特徴といえるだろう。

## 1.3. 10 大脅威を振り返っての情報セキュリティ対策の考え方

ここまで過去の「10 大脅威」を振り返ってきた。この 10 年、様々な脅威が現れ、攻撃者の手口は年々巧妙になってきている。しかし、攻撃の糸口はあまり変わっておらず、脆弱性を突く、ウイルスを使う、ソーシャルエンジニアリングを使う、等の基本的な手口が使われている。

昨年公開した 10 大脅威 2015 では表 1.2 に示す「情報セキュリティ対策の基本」を紹介した。ここでは攻撃の糸口を 5 つに分類している。攻撃の糸口に変化がない間は、これら対策による効果は大いに期待できる。10 大脅威に対するリスク低減の効果を 2 章の「付録 3:10 大脅威 2016 と情報セキュリティ対策の基本との対応」の表 2.1 に示す。これらの対策は、ウイルス対策ソフトを購入すること以外は、基本的に費用が掛からない。まずはこれら対策を行い、その上で組織や個人の事情にあわせて多層防御を図ることをお薦めする。

なお、これらの対策についての詳しい解説は 10 大脅威 2015 の 1 章をご確認頂きたい。

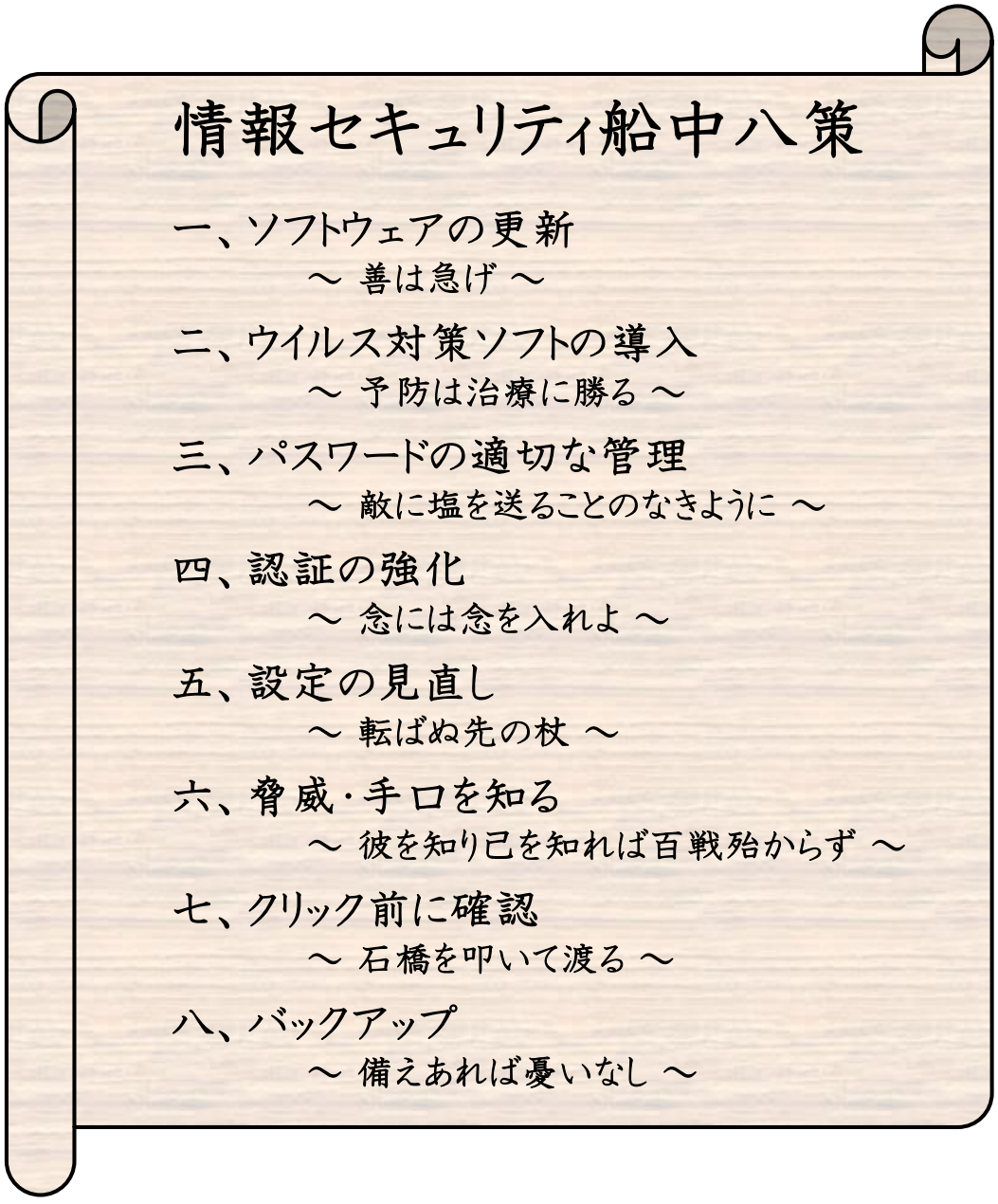
表 1.4 情報セキュリティ対策の基本

| 攻撃の糸口 | 情報セキュリティ対策の基本 |
|---|---|
| ソフトウェアの脆弱性 | ソフトウェアの更新 |
| ウイルス感染 | ウイルス対策ソフトの導入 |
| パスワード窃取 | パスワード管理・認証の強化 |
| 設定不備 | 設定の見直し |
| 誘導（罠にはめる） | 脅威・手口を知る |

IPA:情報セキュリティ 10 大脅威 2015
https://www.ipa.go.jp/files/000044680.pdf

## 付録 1:情報セキュリティ船中八策

「10 大脅威 2015」で紹介した「情報セキュリティ船中八策」を本書でも掲載する。江戸時代に坂本龍馬がまとめたといわれる「船中八策」にあやかり、情報セキュリティの 8 つの対策を示している。



# 2章. 情報セキュリティ10 大脅威 2016

# 2 章　情報セキュリティ 10 大脅威　2016

2015 年において社会的に影響が大きかったセキュリティ上の脅威について「10 大脅威選考会」の投票結果に基づき、表 2.1 の通り順位付けした。また、「情報セキュリティ 10 大脅威 2016」では、「個人」と「組織」向けの脅威を分けて表 2.2 の通り順位付けした。

本章では、総合順位で 1 位～10 位となった脅威を「情報セキュリティ 10 大脅威 2016」として、2.1 節で解説する。また、11 位以降となった脅威については、その他の脅威として 2.2 節で簡単に解説する。

**表 2.1　情報セキュリティ 10 大脅威 2016　総合順位**

| 順位 | タイトル |
|---|---|
| 1 | **インターネットバンキングやクレジットカード情報の不正利用**<br>～拡大する攻撃対象、様々な手段で金銭取引の重要な情報を収集～ |
| 2 | **標的型攻撃による情報流出**<br>～多くの組織や企業が標的型攻撃のターゲットに！～ |
| 3 | **ランサムウェアを使った詐欺・恐喝**<br>～日本人を標的にしたランサムウェアが日本上陸～ |
| 4 | **ウェブサービスからの個人情報の窃取**<br>～ハッカー集団による甚大な被害～ |
| 5 | **ウェブサービスへの不正ログイン**<br>～パスワードの適切な設定、管理を～ |
| 6 | **ウェブサイトの改ざん**<br>～引き続き狙われるCMSの脆弱性～ |
| 7 | **審査をすり抜け公式マーケットに紛れ込んだスマートフォンアプリ**<br>～蔓延する悪意あるスマートフォンアプリ、公式マーケットのアプリにも注意を～ |
| 8 | **内部不正による情報漏えいとそれに伴う業務停止**<br>～内部不正が事業に多大な悪影響を及ぼす～ |
| 9 | **巧妙・悪質化するワンクリック請求**<br>～被害者を欺く手口はますます悪質に～ |
| 10 | **脆弱性対策情報の公開に伴い公知となる脆弱性の悪用増加**<br>～求められる迅速な対策の実施～ |

表 2.2 情報セキュリティ 10 大脅威 2016 個人・組織別順位

| タイトル(個人) | 順位 | タイトル(組織) |
|---|---|---|
| インターネットバンキングや<br>クレジットカード情報の不正利用<br>総合:1位 | 1 | 標的型攻撃による情報流出<br>総合:2位 |
| ランサムウェアを使った詐欺・恐喝<br>総合:3位 | 2 | 内部不正による情報漏えいと<br>それに伴う業務停止<br>総合:8位 |
| 審査をすり抜け公式マーケットに<br>紛れ込んだスマートフォンアプリ<br>総合:7位 | 3 | ウェブサービスからの個人情報の<br>窃取<br>総合:4位 |
| 巧妙・悪質化するワンクリック請求<br>総合:9位 | 4 | サービス妨害攻撃による<br>サービスの停止<br>総合:11位 |
| ウェブサービスへの不正ログイン<br>総合:5位 | 5 | ウェブサイトの改ざん<br>総合:6位 |
| 匿名によるネット上の誹謗・中傷<br>総合:13位 | 6 | 脆弱性対策情報の公開に伴い<br>公知となる脆弱性の悪用増加<br>総合:10位 |
| ウェブサービスからの個人情報の<br>窃取<br>総合:4位 | 7 | ランサムウェアを使った詐欺・恐喝<br>総合:3位 |
| 情報モラル不足に伴う<br>犯罪の低年齢化<br>総合:18位 | 8 | インターネットバンキングや<br>クレジットカード情報の不正利用<br>総合:1位 |
| 職業倫理欠如による<br>不適切な情報公開<br>総合:14位 | 9 | ウェブサービスへの不正ログイン<br>総合:5位 |
| インターネットの広告機能を<br>悪用した攻撃<br>総合:12位 | 10 | 過失による情報漏えい<br>総合:16位 |

本章で共通的に使われる用語について表 2.3 に定義を記載する。

表 2.3 情報セキュリティ 10 大脅威 2016 用語定義

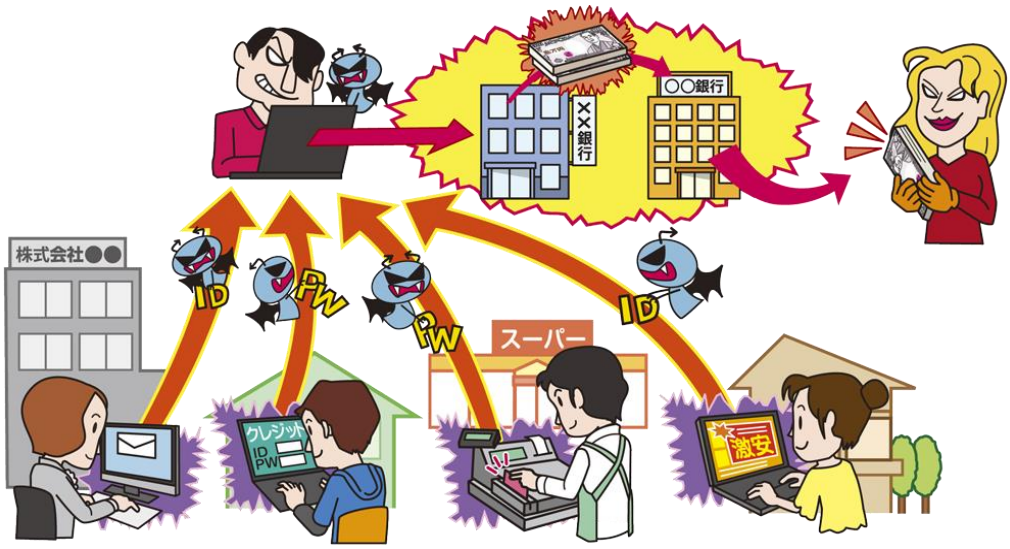
| 用語 | 意味 |
|---|---|
| 個人 | スマートフォンやパソコンでインターネットを利用する一般ユーザ |
| 組織 | 企業、政府機関・公共団体などの組織、およびその組織内のユーザ |
| 犯罪グループ | 金銭目的の攻撃(犯罪)集団 |
| 犯罪者 | 金銭目的の攻撃(犯罪)者 |
| 諜報員、産業スパイ | 機密情報窃取目的の攻撃(犯罪)集団<br>国家組織の支援を受けた攻撃(犯罪)集団 |
| ハッカー集団 | 思想・イデオロギーを背景とする攻撃(犯罪)集団(ハクティビスト) |

## 2.1. 情報セキュリティ10大脅威

個人 1 位　組織 8 位

# 1位 インターネットバンキングやクレジットカード情報の不正利用

## ～拡大する攻撃対象、様々な手段で金銭取引の重要な情報を収集～




ウイルス感染やフィッシング詐欺により、個人および組織から情報を窃取し、本人になりすました不正送金や利用が行われた。2015 年は攻撃対象が拡大し、地域の金融機関も標的となった。

### ＜攻撃者＞

- 犯罪グループ

### ＜被害者＞

- 個人、組織
  （インターネットバンキング利用者）
- 個人（クレジットカード利用者）
- 組織（銀行/カード発行会社）

### ＜脅威と影響＞

インターネットバンキングやインターネットを介したクレジットカードの利用が広く普及している。一方で、金銭を取り扱っているにもかかわらずサイトが十分なセキュリティ機能を提供していなかったり、利用者がセキュリティ対策を怠ったりしている。攻撃者はウイルス感染やフィッシング詐欺等の攻撃により、利用者から情報を窃取し、利用者になりすまして不正送金等を行っている。

昨年に続き法人口座も大きな被害が発生した。標的とされた金融機関は都市銀行や地方銀行から信用金庫や信用組合等、地域の金融機関へ及んでいる。

### ＜攻撃手口＞

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手口は、主なものとしてウイルス感染（金融情報の取得に特化したウイルスも存在）とフィッシング詐欺が挙げられる。

**◆　ウイルス感染**

利用者が悪意のあるウェブサイトにアクセスしたり、メールに添付された悪意あるファイルを開いたりすることでウイルスに感染してしまう。PC がウイルスに感染してしまうと、インターネットバンキングサイトにログインした際に利用者が入力した情報が窃取される。攻撃者は窃取した情報を使用して、正規の利用者になりすまして不正送金等を行う。

◆ **フィッシング詐欺**

例えばメールを使った手口の場合、攻撃者は銀行等の実在する組織を装い、「個人情報漏えい利用者の確認」といった内容でフィッシングサイトの URL を含むメールを利用者に送りつける。利用者は正規の組織からのメールであると誤認し、攻撃者の用意したフィッシングサイトにアクセスする。攻撃者による偽の情報を利用者が信じてしまい、そこで入力した情報が攻撃者に送られ、攻撃者はその情報を使用して、不正送金等を行う。

## ＜事例と傾向＞

◆ **不正送金被害が引き続き発生**

警察庁によると、2015 年のインターネットバンキングにかかわる不正送金の被害額は約 30 億 7,300 万円となり、2014 年の 29 億 1,000 万円を超え、被害額が過去最悪となったことが明らかとなった。特に信用金庫、信用組合、農業協同組合、労働金庫の利用者に被害が及んだ。[I] セキュリティ対策の遅れが原因と考えられる。

◆ **日本のインターネットバンキング利用者を標的としたウイルス**

日本のインターネットバンキング利用者を標的としたウイルスによる被害が発生している。被害者に気づかれにくくするため、注文連絡等を装ったメールにウイルスを添付しているものも確認された。[II]

また、このような日本を標的としているウイルスを撲滅する取り組みも実施された。[III]

◆ **金融庁を装ったフィッシング詐欺**

2015 年も多くのフィッシングサイトが観測された。金融庁を騙り、注意喚起やセキュリティ向上を謳ってフィッシングサイトに誘導し、アカウント情報を入力させる事例もあった。[IV]

## ＜対策/対応＞

**個人、組織（利用者）**

- OS・ソフトウェアの更新
- ウイルス対策ソフトの導入・更新
- 二要素認証等の強い認証方式の利用
- 事例・手口の情報収集

多くの銀行のホームページでは、犯罪手口や提供している対策を掲載している。利用者は被害にあった際に迅速に対応できるよう、対策情報を参照し、活用していくことが望ましい。

また、フィッシングサイトに誘導されないよう、ブックマーク経由等の信頼性が確認されている方法でアクセスしたり、被害にあった際に迅速に対応できるよう銀行の連絡先窓口の電話番号を確認したりしておくことも重要である。

**組織（銀行/カード発行会社）**

- 事例・手口の情報収集とその対策方法の公開および定期的な内容の見直し
- 二要素認証等の強い認証方式の提供

犯罪の手口や利用すべき暗号方式やブラウザの設定等は変化していく。公開した情報は定期的に見直していく必要がある。

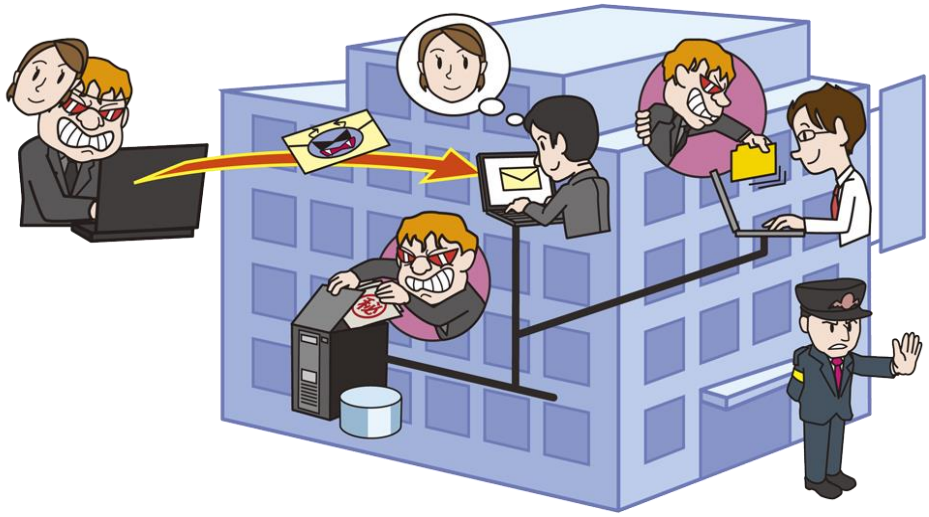
**参考資料**


I. 平成27年中のインターネットバンキングに係る不正送金事犯の発生状況等について
https://www.npa.go.jp/cyber/pdf/H280303_banking.pdf
II. 【注意喚起】特定の組織からの注文連絡等を装ったばらまき型メールに注意
https://www.ipa.go.jp/security/topics/alert271009.html
III. これぞ攻性防御!? 警視庁が国内初のボットネット無力化作戦決行！
http://ascii.jp/elem/000/001/006/1006696/
IV. 金融庁をかたるフィッシング
https://www.antiphishing.jp/news/alert/fsa_20151016.html

個人 15 位　組織 1 位

## 2位 標的型攻撃による情報流出

～多くの組織や企業が標的型攻撃のターゲットに！～



メールの添付ファイルやウェブサイトを利用して PC にウイルスを感染させ、その PC を遠隔操作して組織や企業の重要情報を窃取する標的型攻撃が後を絶たない。日本年金機構の事件報道以降、多くの組織や企業でも標的型攻撃を受けていたことがわかり、同様の事件報道が続いた。

### ＜攻撃者＞

- 諜報員、産業スパイ

### ＜被害者＞

- 組織
- 個人（顧客、サービス利用者）

### ＜脅威と影響＞

2015 年もソーシャルエンジニアリング（人の行動のミス等につけ込む手口）を駆使した標的型攻撃により、組織の企業秘密や顧客情報が漏えいする被害のニュースが度々報道された。これらの情報は企業の重要な情報であり、事業に多大な影響を及ぼす可能性がある。また、国家の機密情報が他国に渡れば、外交上や安全保障上の国際問題に発展する懸念がある。

標的型攻撃では、メールやウェブサイト、外部媒体等によって標的となる組織の PC にウイルスを感染させ、組織内部に潜入する。その後、ウイルス感染した PC を遠隔操作して組織内部の情報を探索し、重要情報を窃取する。また、関連組織への攻撃の踏み台にされる場合もあり、業種や会社規模に関係なく狙われる可能性がある。

### ＜攻撃手口＞

主に以下のシナリオに沿って遂行される。

(1) 計画立案
(2) 攻撃準備（標的組織の調査）
(3) 初期潜入（ウイルス感染）
(4) 基盤構築（感染拡大）
(5) 内部侵入・調査（文書や情報の探索）
(6) 目的遂行（外部へのデータ送信）
(7) 再侵入

「(3)初期潜入」では、ウイルスを標的組織の PC に感染させるための騙しの手口が

巧妙化している。標的型攻撃メールでは、実在する企業や官公庁から窃取したメール本文や差出人アドレスを使い、メール受信者の警戒を解く。その上で、ウイルスを仕込んだ添付ファイルを開かせたり、メール本文中に記載されたリンクをクリックさせたりする。添付ファイル名やリンク先の URL またはリンク先のファイル名は業務に関係がありそうなものや関心を持ちそうなもの等にしている。

## ＜事例と傾向＞

### ◆　日本年金機構から個人情報が流出

2015 年 5 月、日本年金機構への標的型攻撃により、「基礎年金番号」、「氏名」、「生年月日」、「住所」といった約 125 万件の個人情報が漏えいしたことが判明した。[I]

また、その後、厚生労働省や日本年金機構の職員を騙った「振り込め詐欺」や「個人情報の詐取」と思われる不審電話の事例もあり、関連組織から注意喚起が出された。[II]

### ◆　多数の組織で標的型攻撃の被害

日本年金機構の事件後、厚生労働省や政府が、全国に向けて再点検の呼びかけを行い、複数の組織で標的型攻撃の被害が見つかっている。[III] また、日本年金機構と同様の手口が、地方公共団体、大学、病院、報道機関等幅広い業界に対して行われている可能性があることを組織外の機関によって確認されている。[IV] 攻撃者が遠隔操作に使う指令サーバー（C&C サーバー）の設置場所の 93%は日本という調査結果もでており、日本の別の組織が踏み台となっている。

## ＜対策/対応＞

**組織（経営者層）**[V]

- 問題に迅速に対応できる体制の構築
- 対策予算の確保と継続的な対策実施

**組織（セキュリティ担当部署）**

- サイバー攻撃に関する情報共有
- セキュリティ教育の実施
- 情報の保管方法ルール策定

**組織（システム管理者）**

- システム設計対策・アクセス制限
- ネットワーク監視・分離
- 情報の取扱い・保管状態の確認

**組織（従業員・職員）**

- セキュリティ教育の受講
- OS・ソフトウェアの更新
- ウイルス対策ソフトの導入・更新

標的型攻撃は、組織の入口で見破り、排除できることが望ましい。しかし、100%防御することは不可能なため、組織内部に侵入されることを前提に、侵入されたことに早く気づく、情報資産を外部送信させない等の対策で「多層防御」することが重要である。対策の詳細は IPA の資料[VI・VII] が参考になる。

**参考資料**


I. 日本年金機構：「不正アクセスによる情報流出事案に関する調査結果報告について」
https://www.nenkin.go.jp/oshirase/press/2015/201508/20150820-02.html
II. 厚生労働省職員や機関を装った不審な電話・メールにご注意ください
http://www.mhlw.go.jp/kinkyu/0713-1.html
III. 読売新聞：「年金機構に続き10組織でウイルス感染・流出」
http://www.yomiuri.co.jp/it/security/goshinjyutsu/20150619-OYT8T50124.html
IV. 読売新聞：「34組織で年金機構と同じウイルス感染か」
http://www.yomiuri.co.jp/it/security/goshinjyutsu/20150626-OYT8T50138.html
V. サイバーセキュリティ経営ガイドライン
http://www.meti.go.jp/press/2015/12/20151228002/20151228002-2.pdf
VI. IPA：「高度標的型攻撃」対策に向けたシステム設計ガイド
https://www.ipa.go.jp/security/vuln/newattack.html
VII. IPAテクニカルウォッチ「標的型攻撃メールの例と見分け方」
https://www.ipa.go.jp/security/technicalwatch/20150109.html

個人 2 位　組織 7 位

## 3位 ランサムウェアを使った詐欺・恐喝

**～日本人を標的にしたランサムウェアが日本上陸～**


悪意あるプログラムによって PC 内のファイルが閲覧・編集できない形に暗号化され、ファイル復元の身代金として、利用者が金銭を要求される被害が増えている。このプログラムを「ランサムウェア」と呼ぶ。2015 年には、これまでの不自然な日本語から一転して流暢な日本語でメッセージが表示されるランサムウェアが登場し、多言語対応等の感染手口の巧妙化が見られた。

### ＜攻撃者＞

- 犯罪グループ

### ＜被害者＞

- 個人、組織
  （PC、スマートフォン利用者）

### ＜脅威と影響＞

メールの添付ファイルやウェブサイトの閲覧等を介して、利用できないよう PC 内のファイルを暗号化し、復号のために組織や個人に金銭を要求するランサムウェアによる被害が拡大した。2015 年に入り、流暢な日本語のランサムウェアが登場し、感染被害の報告が増加している。2015 年 12 月には、複数の OS に対応したランサムウェアも出現した。また、悪意あるアプリをインストールさせ、端末の暗号化や端末のロックをするスマートフォン向けのランサムウェアも確認されており被害の確認が懸念される。

組織の場合は、事業の根幹となる企業秘密や顧客情報等が、個人の場合は、プライベートな写真や文書等が閲覧できなくなる可能性がある。また、ランサムウェアは共有フォルダ内も暗号化されるため、組織においては組織内のデータがすべて使えなくなる等の大きな影響を及ぼす可能性がある。

なお、要求に従い金銭を支払うことで復号された事例はあるが、支払ったとしてもファイルが完全に復号される保証はない。

## ＜攻撃手口＞

◆ メール添付

- ランサムウェア（ダウンローダ含む）を添付したメールを送付し、添付を開かせ感染

◆ ウェブサイト

- ランサムウェアへのリンクを含んだメールを送り、クリックさせ感染
- ウェブサイトに不正広告を載せ、その広告をクリックまたは表示させ感染

## ＜事例と傾向＞

◆ **ランサムウェアの日本語化**

IPA では、2014 年 12 月に初めて日本語表示されるランサムウェア感染の相談を受けた。2015 年 4 月以降、日本語のランサムウェアについての相談が増加した。企業においても、2015 年 10 月以降、ランサムウェアの感染被害の相談が増加傾向にある。[I]

◆ **脆弱性を悪用したランサムウェア感染**

2015 年 11 月下旬以降、改ざんしたウェブサイトから、Adobe Flash Player の脆弱性を悪用し、ランサムウェアをダウンロードさせて、感染を試みる攻撃が連日確認されている。[II]

◆ **複数の OS に対応したランサムウェア**

海外のセキュリティ企業により、JavaScript で開発されたランサムウェアが出現したと報じられた。[III] このランサムウェアは、SaaS（Software as a Service）で提供され、簡単にダウンロードできる。OS 共通の言語で開発されており、Linux や Mac OS 等への被害拡大が懸念された。ランサムウェアによる攻撃が容易になる環境が整ってきており、今後は攻撃の増加が予測される。

◆ **スマートフォン向けランサムウェア**

2014 年にモバイル端末向けのランサムウェアが確認されていたが、2015 年には、端末のロックを行うスマートフォン向けのランサムウェアが登場した。[IV] 悪意あるアプリをインストールすることで感染する。

## ＜対策/対応＞

**個人、組織**

- 定期的なバックアップ（PC・共有サーバー等）と復元できるかの事前の確認
- OS・ソフトウェアの更新
- ウイルス対策ソフトの導入・更新
- メールの添付ファイル・リンクの URL を不用意に開かない

システム全体で、重要なファイルは定期的なバックアップを行い、また、元に戻せるかを事前に確認しておくことも重要である。なお、ネットワークが繋がったサーバーにも影響があるため、ネットワークに繋がっていない外部媒体にバックアップを保管することが重要となる。

また、スマートフォン向けの対策としてウイルス対策ソフトを導入することで悪意あるアプリのインストールを防げる可能性がある。

**参考資料**


I. 「ランサムウェア感染被害に備えて定期的なバックアップを」～組織における感染は組織全体に被害を及ぼす可能性も～
https://www.ipa.go.jp/security/txt/2016/01outline.html
II. ランサムウェア CryptoWall への感染を狙った攻撃を 11 月下旬から連日確認
https://www-304.ibm.com/connections/blogs/tokyo-soc/entry/ransomware_20151208?lang=ja
III. JavaScript のみで開発されたランサムウェア出現、SaaS 型の提供も
http://www.itmedia.co.jp/enterprise/articles/1601/06/news058.html
IV. 「Android」ランサムウェア「Lockerpin」が発見される--新しいPINで端末をロック
http://japan.cnet.com/news/service/35070480/

個人 7 位　組織 3 位

## 4位 ウェブサービスからの個人情報の窃取

～ハッカー集団による甚大な被害～


ウェブサイトの脆弱性を突き、ウェブサービスが保有する住所や氏名等の個人情報が窃取される事件が国内で発生した。また、海外では社会的・政治的主張を目的にサイバー攻撃を行うハッカー集団（ハクティビスト）が、窃取した個人情報や機密情報をインターネット上に公開する事件も発生した。

### ＜攻撃者＞

- ハッカー集団
- 犯罪グループ

### ＜被害者＞

- 組織（ウェブサービス提供ベンダー）
- 個人（ウェブサービス利用者）

### ＜脅威と影響＞

近年、ショッピングサイトやインターネットバンキング等生活を便利にするサービスが広く普及してきた。また、近年では SNS も広く使われており、多くの個人情報がウェブサービス上に登録されている。

一方、ウェブサービスは様々なソフトウェアで構成されており、セキュリティ上の問題を内包しやすい。また、インターネットに公開されているため、攻撃者の標的になりやすい。

ウェブサービスにセキュリティ上の問題が存在した場合、登録した個人情報（クレジットカード情報や顧客の住所、氏名、電話番号等）が窃取され、不正に使用される可能性がある。また、メールアドレスが漏えいした場合、スパムメール等を通じてフィッシングサイトに誘導され、さらには被害に繋がる可能性がある。

### ＜攻撃手口＞

◆ **独自に開発したウェブアプリケーションの脆弱性**

ウェブサービスを提供する際にセキュリティを十分に考慮していない場合、脆弱性を作りこんでしまう可能性がある。そうすると、

SQL インジェクションやディレクトリ・トラバーサル等情報漏えいに繋がる脆弱性を悪用され、個人情報を窃取される。

◆ **ソフトウェアの脆弱性**

広く使われているオープンソースや市販のソフトウェア製品は、攻撃手法が判明すれば、多くの対象を攻撃できるため、該当するソフトウェア製品を使用して構築されたウェブサイトは攻撃者の標的となりやすい。OS・ミドルウェア等のサーバーソフトウェアに存在する脆弱性を悪用された場合、サーバー内に保存していた情報を窃取される。

## ＜事例と傾向＞

◆ **アシュレイ・マディソンからの流出**

不倫専門の出会い系 SNS「アシュレイ・マディソン」を運営している Avid Life Media に同サービスの倫理性等を批判するハッカー集団による不正アクセスがあり、3,200 万人の会員のアカウント情報やログイン情報等が漏えいした。[I]

◆ **いまだに多い SQL インジェクション**

2014 年に引き続き、SQL インジェクションによる情報漏えいが相次いでいる。ハッカー集団による攻撃と思われる被害も発生した。[II] [III]

## ＜対策/対応＞

**組織（運営者）**

- セキュアなウェブサービスの構築

ウェブサービスを構築する際は、要件定義等の初期段階から、構成するソフトウェアのセキュリティ担保を考慮する必要がある。例えば、「安全なウェブサイトの作り方」[IV] や「Web システム/Web アプリケーションセキュリティ要件書」[V] が参考になる。また、必要以上に個人情報を持たない等漏えいリスクへの考慮も必要である。さらには、公開前にセキュリティ診断を行い、発見しづらい脆弱性の発見・対策を行うことも重要である。

- OS・ソフトウェアの更新

公開後も OS やミドルウェアのパッチが随時公開されるため、パッチを適用し、最新の状態に保つ必要がある。[VI]

- WAF・IPS の導入

WAF や IPS を導入することで、脆弱性が存在していても被害を防げる可能性がある。対策情報（設定やファイル）が提供されたら、管理者は適宜更新する必要がある。

**個人（ウェブサービス利用者）**

利用していたサイトで情報漏えいがあった場合、漏えいした情報や悪用される可能性の把握、金銭被害の防止を図る必要がある。また、不要な情報は極力サイトに登録しないことで漏えい時の被害を軽減できる。

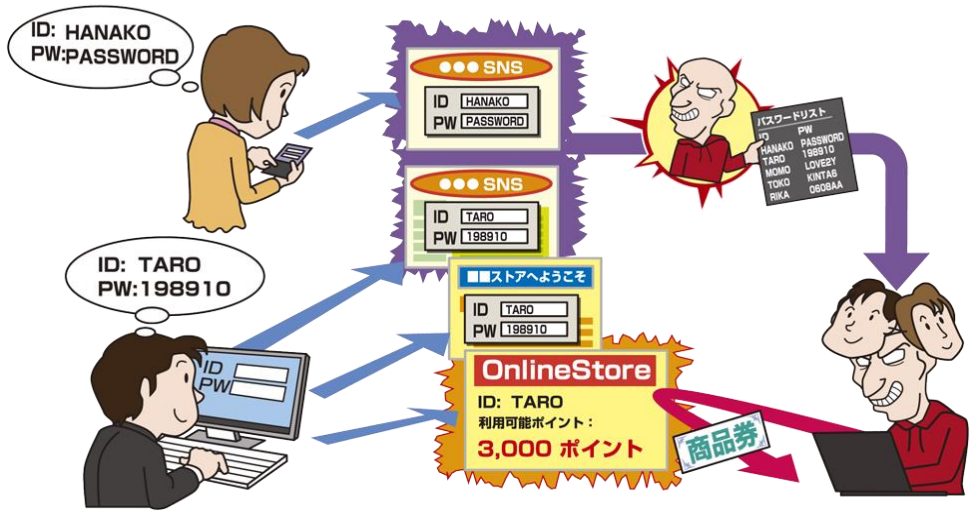
**参考資料**


I. アシュレイ・マディソンにおける個人情報の流出は何をもたらしたのか
http://canon-its.jp/eset/malware_info/special/151020/
II. シャトレーゼにSQLインジェクション攻撃、Web会員情報約21万人分流出の可能性
http://itpro.nikkeibp.co.jp/atcl/news/15/073002537/
III. 日本動物園水族館協会からの情報漏洩、AnonymousによるSQLインジェクション攻撃か
http://itpro.nikkeibp.co.jp/atcl/news/15/052701757/
IV. 安全なウェブサイトの作り方 改訂第7版
https://www.ipa.go.jp/files/000017316.pdf
V. Web システム／Web アプリケーションセキュリティ要件書
https://www.owasp.org/images/8/88/Web_application_security_requirements.pdf
VI. サーバソフトウェアが最新版に更新されにくい現状および対策
http://www.ipa.go.jp/files/000038393.pdf

個人 5 位　組織 9 位

## 5位 ウェブサービスへの不正ログイン

～パスワードの適切な設定、管理を～




ウェブサービスから窃取した ID とパスワードを用いて、不正ログインされる被害が発生している。利用者が同じパスワードを複数のウェブサービスで使い回している場合、被害が拡大する。また、安易なパスワードを設定している場合も、推測されることにより、不正ログインを許してしまう。

### ＜攻撃者＞

- 犯罪グループ、犯罪者

### ＜被害者＞

- 個人（ウェブサービス利用者）
- 組織（ウェブサービス提供ベンダー）

### ＜脅威と影響＞

会員制のウェブサービスを利用する場合、ログインには ID とパスワードによる認証手段が採用されていることが多い。

利用者が複数のウェブサービスで同じ ID とパスワードの組合せを使い回している場合、ある 1 つの脆弱なウェブサービスから ID とパスワードが漏えいすると、他のウェブサービスでもその組合せを悪用して不正ログインが可能になってしまう。これには、利用者が「複数のパスワードを覚えておくことは困難」といった理由によって、同じパスワードを複数のウェブサービスで利用する傾向が背景にある。IPA が行った調査では、サービスごとに異なるパスワードを設定している利用者は 30%に満たなかった。[1] また、パスワードに、連続した英数字、password 等のよく使われる英単語、自分の名前等、安易な文字列を設定している場合、攻撃者に推測される可能性が高くなる。

ウェブサービスに不正ログインされることにより、個人情報の漏えいや金銭被害等、様々な被害が発生する可能性がある。例えば、ショッピングサイトに不正ログインされた場合、登録住所を見られたり、勝手に商品を購入されたり、貯まっているポイントを窃取されたりする可能性がある。

### ＜攻撃手口＞

**◆ パスワードリスト攻撃**

脆弱なウェブサイトから窃取した ID とパスワードの組合せを用い、他のウェブサイトに

不正ログインを試みる方法である。利用者が強固なパスワードを設定していても、複数のウェブサービスでパスワードを使い回している場合には被害が拡大する。

◆ **パスワードの推測**

名前や誕生日、ID と同一の文字列、連続した英数字等、安易で使われやすい文字列をパスワードとして攻撃者が入力し、不正ログインを試みる方法である。

## ＜事例と傾向＞

◆ **ディノス・セシールへの不正ログイン**

2015 年 7 月、オンラインショップのディノス・セシールがパスワードリスト攻撃を受け、およそ 160 万円の不正注文が発生した。また個人情報を閲覧されただけでなくメールアドレスを変更される被害もあった。[II]

◆ **パスワード推測による内閣府メールアカウント乗っ取り**

2015 年 8 月、NPO 団体からの問い合わせ先として利用されていた内閣府のメールアカウントが乗っ取られた。委託先の担当者が推測しやすいパスワードを設定していたことが原因とされる。これにより約 2 万件のメールが不正に送信された。[III]

## ＜対策/対応＞

**個人（ウェブサービス利用者）**

- パスワードを使い回さない
- 推測されにくいパスワードの設定
- 長いパスワードの設定
- 二要素認証等の強い認証方式の利用
- ログイン履歴の確認

利用者は、パスワードの適切な管理方法を知り、実践することが重要となる。普段利用しているパスワードの最後にサービスごとに個別の文字列を追加するだけでも有効な対策となる。[IV]

**組織（ウェブサービス提供ベンダー）**

- 複雑なパスワード設定を要求（安易なパスワードを拒否等）
- 可能な範囲で長い文字数を要求
- 初期パスワード変更を要求
- 二要素認証等の強い認証方式の提供
- セキュリティ対策の徹底

ウェブサービス提供ベンダーは、提供する認証ページにおいて同一ホストからの連続ログイン試行の拒否といったシステム的な対策を講じることでパスワードリスト攻撃の被害を低減できる。また、利用者にパスワードを発行した際には、初回ログイン時に複雑なパスワードを強制的に再設定させるといった制限も有効となる。なお、脆弱性を悪用されウイルスに感染する等によりパスワードが漏えいする可能性もあるため、脆弱性対策や利用者のパスワードのハッシュ化等のセキュリティ対策を実施しておくことも重要である。

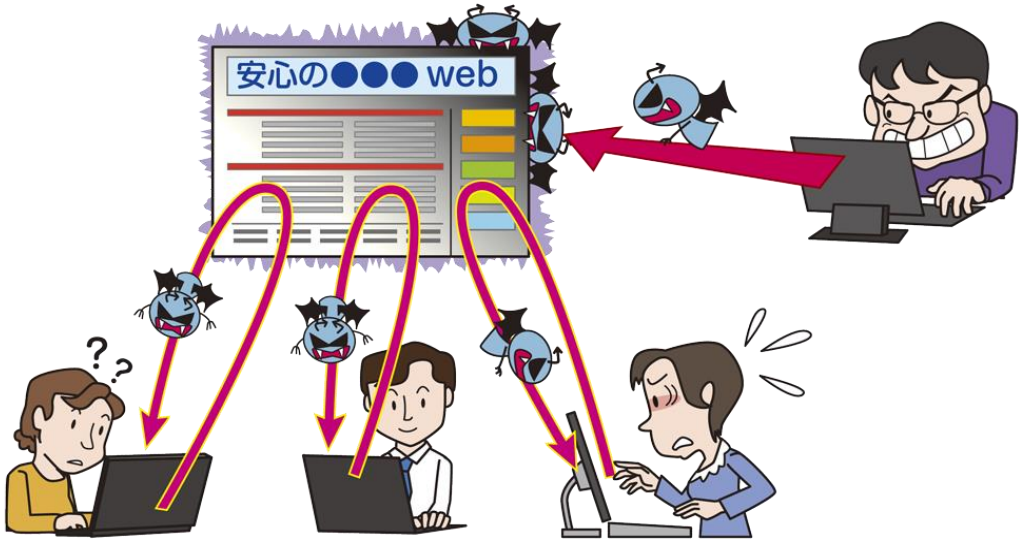
**参考資料**

I. IPA:「2015年度情報セキュリティの脅威に対する意識調査」P.62
https://www.ipa.go.jp/files/000050002.pdf
II. 株式会社ディノス・セシール：弊社オンラインショップへの不正アクセス並びに不正受注被害について
http://www.dinos-cecile.co.jp/pdf/topics_20150716.pdf
III. 内閣府　アカウント乗っ取られ、2万件のメールが…
http://news.tv-asahi.co.jp/news_economy/articles/000056053.html
IV. IPA:チョコっとプラスパスワード
https://www.ipa.go.jp/chocotto/pw.html

個人 12 位　組織 5 位

## 6位 ウェブサイトの改ざん

**～引き続き狙われる CMS の脆弱性～**




閲覧するだけでウイルスに感染するよう、CMS 等の脆弱性を悪用してウェブサイトが改ざんされる事例が多く発生した。改ざんされるとウェブサイトの一時停止を余儀なくされる等、経営上のダメージを被る被害者となる一方で、利用者にウイルスを拡散する加害者にもなってしまう。

### ＜攻撃者＞

- 犯罪グループ、犯罪者
- 諜報員、産業スパイ

### ＜被害者＞

- 組織（ウェブサイト提供ベンダー）
- 個人（ウェブサイト利用者）

### ＜脅威と影響＞

ウェブサイトを改ざんされると、ウイルスを配布する水飲み場型攻撃への悪用や政治的主張の掲載等をされ、結果ウェブサイト運営者が社会的信用を失う影響が懸念される。

また、改ざんされたウェブサイトにアクセスした閲覧者はウイルス感染により、端末をボット化されて DDoS 攻撃への加担や遠隔操作される等の被害が懸念される。

特に、ウェブサービスを作成、管理するためのコンテンツ管理システム（CMS）に脆弱性が存在した場合、その CMS で作られたウェブサイトすべてに影響を及ぼす可能性があり、影響範囲が広い。

### ＜攻撃手口＞

**◆ ソフトウェア製品の脆弱性**

広く一般に普及しているソフトウェア製品は、攻撃手法が判明すれば、広い対象を攻撃できるため、攻撃者の標的となりやすい。OS・ミドルウェア等のサーバーソフトウェアや、WordPress 等の CMS、および利用されるプラグインの脆弱性を悪用される。特に、ソフトウェアを構築時のままに放置しておくと、日々発見される脆弱性を悪用され、ウェブサイトを改ざんされてしまうリスクが高まる。

◆ **独自に作りこんだウェブアプリケーションの脆弱性**

ウェブアプリケーションの開発やパッケージソフトウェアのカスタマイズは、脆弱性対策を怠ると、そこを攻撃者に狙われ、ウェブサイトを改ざんされる。

◆ **外部から管理用サービスへの侵入**

ウェブサイト運用のために FTP、SSH、クラウドの管理コンソール等の管理用サービスを使用しているウェブサイトが存在する。攻撃者はウェブサイト管理者の管理端末をウイルスに感染させ、ウェブサイト管理用のアカウントを窃取する。窃取したアカウントを使用して外部から管理用サービスへ侵入し、ウェブサイトを改ざんする。また、CMS の場合は、意図せず公開していた管理画面を侵入口にされたケースも発生している。

◆ **設定不備による不適切な機能の公開**

外部からのファイルアップロード機能を公開する際、アップロード可能なファイルを制限する必要がある。不適切な設定を行っていた場合、悪意のあるプログラムをアップロードされ、ウェブサイトを改ざんされる。

## ＜事例と傾向＞

◆ **海外で利用される CMS が標的に**

脆弱性がある CMS は攻撃者からの標的となりやすい。2015 年は海外 EC サイトで高いシェアがある Magento に重大な脆弱性が発見され、大きな問題となった。[I]

◆ **WordPress を狙った攻撃が多発**

様々な組織で用いられている WordPress を狙った攻撃が相次いだ。WordPress のプラグインの脆弱性を悪用した攻撃コードも確認されており、構築したまま管理されていないウェブサイトには DDoS 攻撃の踏み台とされる脅威があった[II]。

## ＜対策/対応＞

**組織（ウェブサイト運営者）**

- OS・ソフトウェアの更新
- ウェブアプリケーションの脆弱性対策
- アカウント・パスワードの管理
- サーバーソフトウェアの設定
- 改ざん検知
- 二要素認証等の強い認証方式の利用
- 信頼できないサードパーティ製ソフトウェアの使用を控える

ウェブサイトで使用しているソフトウェアの製品名やバージョンを管理することで、脆弱性対策情報が公開された際、速やかに対策が行える。また、管理者やユーザの権限を適切に管理することも重要である。

開発・構築の際には脆弱性を作りこまないように IPA の資料[III]を参考にするとよい。

**個人（ウェブサイト利用者）**

- ウイルススキャンの実施
- OS・ソフトウェアの更新

改ざんされたウェブサイトにアクセスした可能性があれば、速やかにウイルススキャンを実施する。また、使用するソフトウェア製品を最新に更新しておくことでウイルス感染のリスクを低減できる。

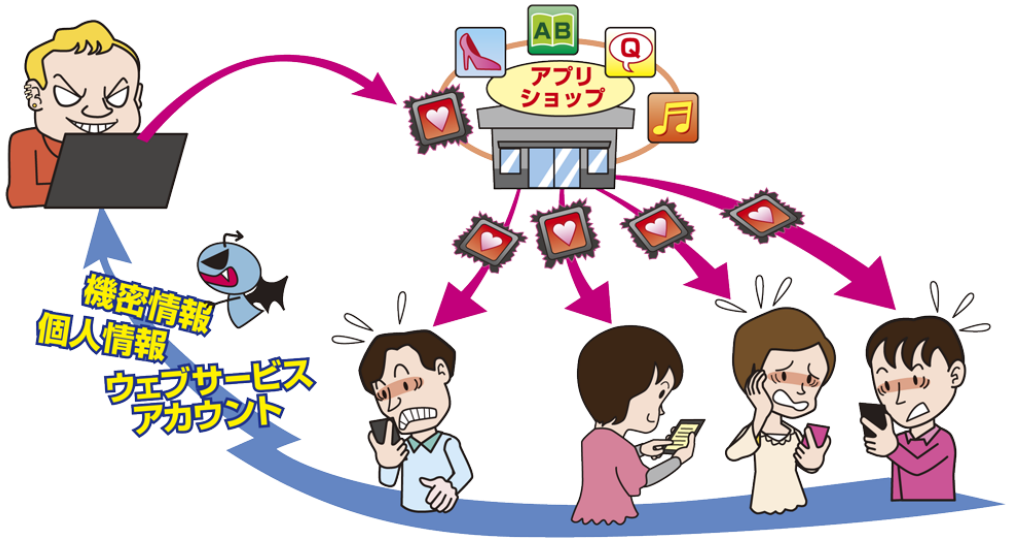
**参考資料**

I. eBayのプラットフォームに重大な脆弱性、約20万のネットショップが影響（チェック・ポイント）
http://scan.netsecurity.ne.jp/article/2015/04/30/36300.html
II. Monthly Research「WordPressの脆弱性を狙ったWeb改ざん攻撃」
http://www.ffri.jp/blog/2015/04/2015-04-28.htm
III. 安全なウェブサイトの作り方
https://www.ipa.go.jp/security/vuln/websecurity.html

個人 3 位　組織 15 位

## 7位 審査をすり抜け公式マーケットに紛れ込んだスマートフォンアプリ

～蔓延する悪意あるスマートフォンアプリ、公式マーケットのアプリにも注意を～




スマートフォンにインストールしてしまった悪意あるアプリにより、スマートフォン内の情報が窃取されてしまう。これまでは、悪意あるアプリの被害を回避する対策として、公式マーケットからアプリを入手することが有効であったが、公式マーケットに悪意あるアプリが紛れ込む事例もあり、利用者にはより一層の注意が求められる。

### ＜攻撃者＞

- 犯罪グループ

### ＜被害者＞

- 個人（スマートフォン利用者）

### ＜脅威と影響＞

スマートフォンアプリには利用者に被害をもたらす悪意あるアプリが依然として存在する。画面上にはアプリのアイコンを表示せず、スマートフォンに保存されているメール、写真、位置情報等を秘密裏に収集して攻撃者へ送信するアプリや、Android スマートフォンを乗っ取ることが可能なアプリが見つかっている。安全とされていた公式マーケットでさえも悪意あるアプリが紛れ込んでおり、アプリのインストールには注意を要する。

### ＜攻撃手口＞

◆ **公式マーケットに悪意あるアプリを公開**

悪意あるアプリを公式マーケットに公開する。公式マーケットは安全だと思い込んでいる利用者が安易にインストールしてしまう。

◆ **アップデート後に悪意あるアプリへ豹変**

アプリをインストールした時点では悪意ある機能を持っていないが、アップデート時に悪意ある機能が追加され、悪意あるアプリに変わる。

◆ **別のアプリを勝手にインストール**

利用者の同意なしに、別のアプリをインストールするアプリも存在する。本来ならばインストール時に表示される確認画面を出さずに、悪意あるアプリをインストールさせる。

## ＜事例と傾向＞

**◆　目に見えないところで動作するアプリ**

動画作成アプリの「Dubsmash」の最新版に見せかけた「Dubsmash2」という悪意あるアプリが、Android アプリ公式マーケットの Google Play に公開された。インストールした場合、画面にアイコンは表示されず、利用者の気づかないところでポルノサイトを次々とクリックする。攻撃者はクリック数に応じて利益を得られる仕組みだった。[I]

**◆　Android を乗っ取ってしまうアプリ**

ゲームの「テトリス」を装った「RetroTetris」という悪意あるアプリが Google Play やウェブサイトに公開されていた。このアプリには Android 端末を自由に操る不正な機能（root 化）が含まれており、スマートフォンを攻撃者に乗っ取られてしまう恐れがあった。[II]

**◆　開発環境の影響を受けた iOS アプリ**

iOS アプリの開発環境「Xcode」のコピー版に悪意あるコードが存在していた。この環境を用いて開発されたアプリには開発者も気づかず悪意あるコードが混入し、複数のアプリで悪意あるコードが含まれて配布されることになった。このコードは「XcodeGhost」と呼ばれ、ユーザに通知文を送信するといったことができるため、詐欺やフィッシング等の不正活動に利用される可能性があった。[III]

## ＜対策/対応＞

**個人（スマートフォン利用者）**

- 信頼できるアプリかどうかを確認

悪意あるアプリは公式ストアにも存在する可能性がある。アプリ名や開発者名等でインターネット検索した結果を確認することで信頼できるアプリかどうか確認する。

- アクセス権限の確認

Android アプリのインストールまたは実行時、アプリで使用する端末の機能や使用するデータへのアクセス権限の確認画面が表示される。確認画面の内容を確認し、アプリが要求する権限は本当に必要か考え、不安であれば承認せずインストールしない。

- ウイルス対策ソフトの導入と更新

悪意あるコードやウイルスを含んだアプリをインストールしようとした場合、既にウイルス対策ベンダーによってシグネチャが提供されていれば、警告画面の表示によって被害を防ぐことが期待できる。

- OS やアプリは最新版を利用

OS やアプリの脆弱性を、ウイルス等に悪用され、被害が発生する可能性があるため、OS やアプリは最新版に更新する。

**組織（スマートフォンアプリ開発者）**

- セキュアなアプリの開発

信頼できないサイトから開発環境等をダウンロードしない。組み込むライブラリ等にも信頼できるかを確認する。

また、自組織のアプリを装った偽のアプリが公開されている場合は、利用者にダウンロードしないよう注意喚起を行う必要がある。

**参考資料**


I. キヤノンITソリューションズ：Google Playにクリッカー型トロイの木馬「Dubsmash 2」が紛れ込む
http://canon-its.jp/eset/malware_info/news/150615/
II. トレンドマイクロ：Androidをルート化する不正アプリ2種をGoogle Playで確認
http://blog.trendmicro.co.jp/archives/12331
III. トレンドマイクロ：「XcodeGhost」：iOS正規アプリの汚染はどのように起きたか
http://blog.trendmicro.co.jp/archives/12251

個人 19 位　組織 2 位

## 8位 内部不正による情報漏えいとそれに伴う業務停止

～内部不正が事業に多大な悪影響を及ぼす～


企業や組織の職員が、内部の情報を窃取し、インターネット上に公開され、誰でも見られる状態だった事件が社会的な問題となった。内部の人間が悪意を持つと、正当な権限を用いて情報を窃取できるため、情報の重要度に応じたアクセス権限の設定や離職者のアクセス権の抹消等、厳格な管理と監視を継続的に行う必要がある。

### ＜攻撃者＞

- 組織の職員(在職者、離職者)

### ＜被害者＞

- 組織
- 個人(顧客、サービス利用者)

### ＜脅威と影響＞

組織内部の権限を持つ職員や離職者が悪意を持ち、内部情報を外部に持ち出し、販売したり、私的に利用したりする事件は度々発生している。

内部不正は、情報の取扱ポリシー等に基づいた倫理的制約だけの対策では、犯行を防ぐことが困難である。正当なアクセス権限を持つ職員であれば、その気になれば容易に内部情報を持ち出せるためである。

重要な内部情報にアクセスできる人間を制限しないということは、不正に情報を窃取されてしまう要因の 1 つとなる。利便性の観点から、1 つの管理者アカウントを複数のユーザで共有して使用する場合、共有する全員に必要以上の権限を付与してしまうほか、誰が操作を行ったのか特定できないという問題も起きる。

顧客情報や内部情報の漏えいを引き起こした企業・組織には、賠償や株価下落、信用失墜による競争力の低下等、事業に多大な悪影響が発生する。

### ＜発生要因＞

**◆　職場環境や処遇の不満**

内部不正を行う動機を高める要因は、当人にとって不当な解雇、業務多忙、給与や賞与、組織の人事評価の不満といった処遇

面に関することが多く、復讐や個人的な利益の享受を目的とすることもある。

◆　**アクセス権限の不適切な付与**

アクセス権限の管理が煩雑等により、必要以上の権限を付与されていると、権限を与える必要がない職員にまで情報資産へのアクセスを許すことになる。アクセス権の不適切な付与によって、データ操作や情報漏えいに関する内部不正が起こる。

◆　**システム操作記録と監視の未実施**

システム操作の記録と監視をしていない組織では内部不正のリスクが高まる。また、内部不正があっても不正に気づきにくいため、不正の発覚が遅れる。これにより内部不正発覚後の調査が困難になる。

## ＜事例と傾向＞

◆　**公的機関から膨大な個人情報漏えい**

大阪　堺市の元職員が不正に持ち帰った約 68 万人の有権者情報が漏えいした。[I] 漏えいした情報は、レンタルサーバー上で外部から閲覧可能な状態にあり、第三者にアクセスされた形跡も残っていた。本事例では、職員が自宅に持ち帰った選挙補助システムを改良して自作のシステムを開発し、複数の民間企業等に対して売り込みを行っていたことも判明した。

◆　**株主向けサービスから個人情報漏えい**

資産運用企業から約 12,000 件の個人情報の漏えいが発生した。また、その後漏えい元となったサービスを終了するに至った。漏えいした情報は、名簿化され業者に渡り、営業活動に使われていた。[II]

## ＜対策/対応＞

**組織**

- 情報取扱ポリシー作成および周知徹底・機密保護に関する誓約
- 資産の把握・体制の整備
- 情報の取扱教育の実施
- システム操作の記録・監視
- アカウント、権限の管理・定期監査
- 重要情報の管理・保護

「資産の把握と体制の整備」は、組織が保持する資産を重要度等で分類し、経営者層が責任を持ち、積極的に推進することが重要である。内部不正の対策は、多岐に渡って網羅的に行う必要がある。IPA の「組織における内部不正防止ガイドライン」のチェックリストを用いることで、対策を見直すことができる。[III]

**個人（顧客、サービス利用者）**

- 情報の管理が適切かを確認

利用するサービスの情報取扱ポリシーや規約等の有無等から情報が適切に管理されているかを確認。

また、内部不正等により個人情報が漏えいする可能性を考慮しておくことも重要である。早期に気づけるよう日頃から利用サービスの通知機能等を活用し、利用状況を把握すると良い。

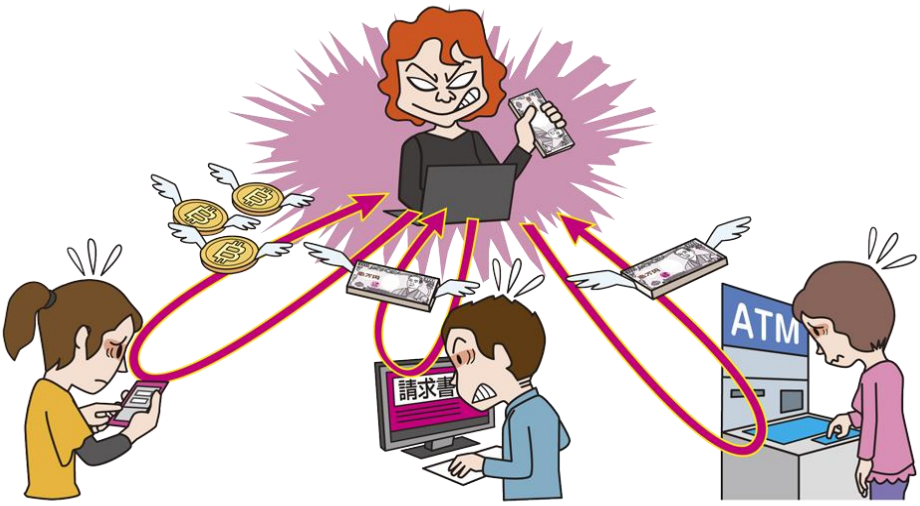
**参考資料**

I. 12月14日提供　職員の不祥事案について　堺市:
http://www.city.sakai.lg.jp/shisei/koho/hodo/hodoteikyoshiryo/kakohodo/teikyoshiryo_h27/teikyoshiryo_h2712/1214_02.html
II.「株主ポイント倶楽部」「株主倶楽部」個人情報データの漏えいの可能性に関する調査結果と再発防止策について
http://www.inv-net.co.jp/pdf/publicity/news/sr_release_20150529.pdf
III. IPA ： 組織における内部不正ガイドライン
https://www.ipa.go.jp/security/fy24/reports/insider/

個人 4 位　組織 18 位

## 9位 巧妙・悪質化するワンクリック請求

～被害者を欺く手口はますます悪質に～




アダルトサイトや出会い系サイトといった有料サイトや、セキュリティソフトの購入推奨等の金銭請求画面が表示され、金銭を不正に請求されるワンクリック請求の被害が発生している。スマートフォンのシャッター音を鳴らす、自動的に電話を発信させるといった、被害者の不安や焦燥感を煽り、支払いを誘発させる巧妙な手口も出現している。

### ＜攻撃者＞

- 犯罪グループ

### ＜被害者＞

- 個人（ウェブサービス利用者）

### ＜脅威と影響＞

悪意のあるアダルトサイトや出会い系サイトに誘導して閲覧させ、利用料といった名目で金銭を請求されるワンクリック請求が依然として発生している。

また、「あなたの PC に脅威が見つかりました」といったメッセージを表示して偽のウイルス対策ソフトを購入させたり、スマートフォンのシャッター音を鳴らして不安を煽って金銭を払い込ませたり、IT リテラシーの低い利用者を狙ったワンクリック請求が増えている。

金銭の支払い方法は、口座振り込み以外に、iTunes カード等のプリペイドカードといった電子マネーを指定される場合もある。[1]

### ＜攻撃手口＞

**◆　悪意あるウェブサイトの閲覧**

アダルトサイトを閲覧していると「再生しますか？」といった質問が表示され、「はい」を選択することによって利用料金の請求画面が表示される。

**◆　メールに記載された URL のクリック**

届いたメールに記載された URL をクリックしただけで「ご入会ありがとうございました」といった画面が表示され、入会金を請求される。

◆ **悪意あるソフトウェアのダウンロード**

悪意あるソフトウェアをダウンロードさせる手口が巧妙化している。例えば、サイトにアクセスした際に「あなたの PC に脅威が見つかりました」といった偽のメッセージが表示され音声が流れる。それに驚いた閲覧者がメッセージを信じてしまい指示に従っていくと有償ソフトウェアの購入を促される。[II]

◆ **悪意あるスマートフォンアプリ**

スマートフォンでインストールしたアプリを起動した際に、閲覧者の顔を撮影したと思わせるシャッター音を鳴らしたり、犯罪者への電話発信を誘導したりすることによって不安を煽った上で金銭を要求する。[III] また、動画の再生ボタンと見せかけてクリックを誘発し不正なアプリをインストールさせ金銭を要求する手口も確認された。[IV]

## ＜事例と傾向＞

◆ **アダルトサイト解約料として計 1,813 万円の不正請求**

スマートフォンでアダルトサイトを閲覧中に「会員登録されました」と表示された。サイトで連絡先等を書き込んだところ、電話で「解約には 32 万円必要」といわれ、電子マネーで支払った。さらには「他のアダルトサイトにも登録されていて解約料が必要」との電話が続き、計 1,813 万円を騙し取られた。[V]

◆ **世間の動向に便乗した詐欺**

マイナンバー制度が開始されるにあたり、この制度に便乗した詐欺が出現した。「利用したサイトの月額料金が未納になっており、放置するとマイナンバー制度に影響がある」といった内容のメールが届き、URL へのアクセスを要求された。[VI]

## ＜対策/対応＞

**個人（ウェブサービス利用者）**

● 怪しいソフトウェア・アプリは利用しない

ダウンロードする際に表示されるアクセス権限等の画面を確認し、怪しいソフトウェアやアプリはインストールしない。また、Twitter 等のメッセージについても注意が必要である。

● 怪しいサイト・メールは開かない

本当に利用する必要があるかどうかを確認した上でサイトにアクセスする。また、利用規約やメール文面をよく確認し、安全であると断定できない場合は利用しない。

また、金銭を要求されても、慌てず請求に応じない。必要に応じ、国民生活センターや最寄りの消費者センター等に相談する。

● 事例・手口の情報収集

事前にニュースやセキュリティ機関のホームページ等から事例や手口等を確認しておき、日頃から引っかからないように注意しておくことも有効である。

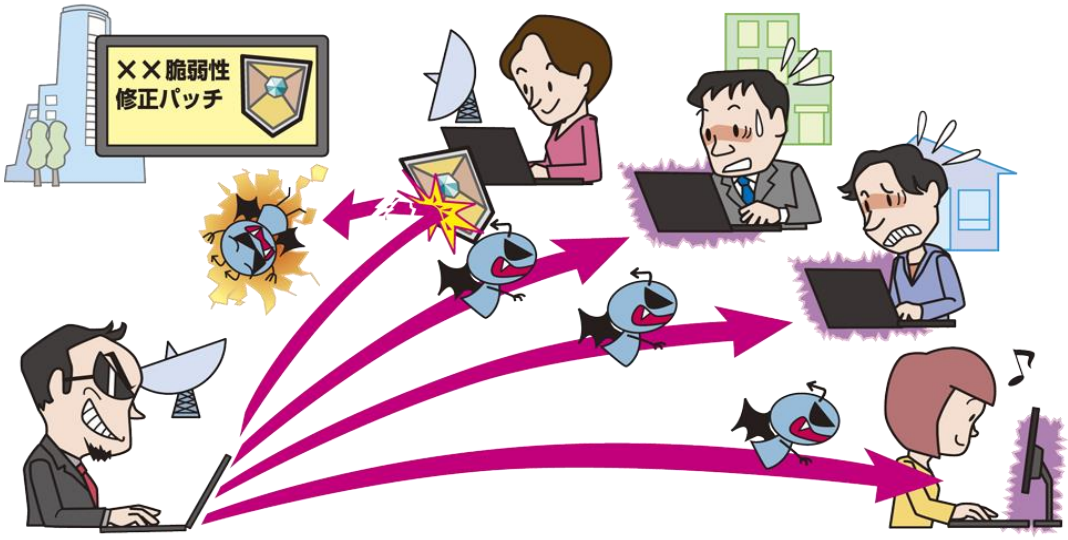
**参考資料**


I. 電子マネーの要求に注意！【暮らし安全おおいた】
http://www.oita-press.co.jp/1010000000/2015/07/14/131844223
II. IPA:「ウイルスを検出したと音声で警告してくるウェブサイトにご注意！」～ ウイルス検出の偽警告に騙されないで ～
https://www.ipa.go.jp/security/txt/2015/08outline.html
III. IPA:「スマートフォンでのワンクリック請求の新しい手口にご用心」～ 業者への電話、メールは絶対NG ～
https://www.ipa.go.jp/security/txt/2015/04outline.html
IV. 日本語によるワンクリック詐欺が、新しい手口で再登場
http://www.symantec.com/connect/ja/node/3428501
V . アダルトサイト解約で1800万円 巡査部長が詐欺被害
http://www.asahi.com/articles/ASH7Y5F1SH7YTLLS008.html
VI. 国民生活センター:マイナンバー制度に便乗した不審な電話等にご注意ください！（第2報）
http://www.kokusen.go.jp/news/data/n-20151112_1.html

個人 16 位　組織 6 位

## 10位 脆弱性対策情報の公開に伴い公知となる脆弱性の悪用増加

～求められる迅速な対策の実施～




2015 年も Adobe Flash Player 等の広く利用されているソフトウェアの脆弱性が公開されている。一方、セキュリティ情報に対して関心が低いシステム管理者や利用者も多く存在し、セキュリティ意識の格差が生じている。攻撃者は対策がなされていないシステムやソフトウェアを狙っており、近年、脆弱性対策情報の公開から攻撃までの期間が短くなっている傾向がある。システム管理者や利用者は日頃から情報収集や、対応方法の検討をしておく必要がある。

### ＜攻撃者＞

- 犯罪グループ
- 諜報員、産業スパイ

### ＜被害者＞

- 組織（ソフトウェア開発ベンダー）
- 個人、組織（ソフトウェア利用者）

### ＜脅威と影響＞

脆弱性の問題が顕在化するにつれ、脆弱性の報告を受け付ける窓口を設置するソフトウェア開発ベンダーが増加している。通常、脆弱性の情報は、修正プログラム（パッチ）とともに一般に公開される。

攻撃者は公開された脆弱性を悪用して、対策を実施していない利用者を攻撃する。近年は、脆弱性対策情報の公開から悪用までの期間が短くなる傾向があり、利用者は対策をできる限り早く実施する必要がある。

### ＜要因＞

**◆対策が実施されない要因**

脆弱性対策情報の公開から利用者が対策を実施するまでのタイムラグを利用し、攻撃者は脆弱性を悪用する攻撃を行う。

- **脆弱性対策情報を知らない**

セキュリティ意識の低い利用者は危険性自体を認識していない場合がある。

- **利用している製品が影響を受けることを知らない**

組織で利用している製品の管理ができておらず、必要な情報を収集できない場合がある。また、開発ベンダーにおいても開発し

た製品だけではなく、オープンソースソフトウェア等の組み込んだソフトウェアの情報を収集・公開しなければ、利用者は気づけない。

- **公開された対策をすぐに実施できない**

基幹システムのような重要システムでは、対策による影響について十分に検証した上で、関係者と調整する必要がある。このため、脆弱性対策情報を入手してもすぐには対策を実施できない場合がある。

**◆ 脆弱性対策情報が悪用される要因**

攻撃者は修正プログラム等を解析し、脆弱性の箇所を効率的に特定する。ソースコードが公開されている場合、修正前後の比較で問題箇所の特定が容易にできる。

## ＜事例と傾向＞

**◆ サーバーソフトウェアの脆弱性**

2015 年は Joomla！や WordPress 等の普及している CMS やそのプラグインで深刻な脆弱性が公開された。脆弱性公開後に探索行為と考えられるアクセスが確認され、ウェブサイト改ざん等の被害も発生した。[I] [II]

**◆ 制御システムの脆弱性**

産業制御システムで使用されているソフトウェアにおいても脆弱性は公開されている。実際に攻撃可能なことを実証するツールも公開され、そのツールを利用していると考えられるアクセスも観測されている。[III]

**◆クライアントソフトウェアの脆弱性**

広く利用されている Adobe Flash Player では、脆弱性の公開から数日で攻撃ツールに組み込まれ悪用可能となっていた。[IV]

また、脆弱性情報の流出により正式な公開前に攻撃が発生した事例もある。[V]

## ＜対策/対応＞

**個人、組織（ソフトウェア利用者）**

- 利用しているソフトウェアの把握
- ソフトウェアの更新、更新できない場合は緩和策
- 継続的な脆弱性対策情報の収集

**組織（システム管理者）**

- 担当するシステムの把握・管理の徹底
- 継続的な脆弱性対策情報の収集
- 脆弱性発見時の対応手順の作成
- ソフトウェアの更新、更新できない場合は緩和策
- ネットワークの適切なアクセス制限

**組織（ソフトウェア開発ベンダー）**

- 製品に組み込まれているソフトウェアの把握・管理の徹底
- 継続的な脆弱性対策情報の収集
- 脆弱性発見時の対応手順の作成
- 情報を迅速に展開できる仕組みの整備

**参考資料**


I. えのしま・ふじさわポータルサイトへのサイバー攻撃について
https://www.city.fujisawa.kanagawa.jp/joho006/press/enopo_syberattack.html
II. 「Islamic State（ISIS）」と称する者によるウェブサイト改ざんに係る注意喚起について
http://www.npa.go.jp/cyberpolice/detect/pdf/20150312.pdf
III. 産業制御システムで使用されるPLCの脆弱性を標的としたアクセスの観測について
http://www.npa.go.jp/cyberpolice/detect/pdf/20150526.pdf
IV. Flash Player悪用攻撃すぐに発生、修正版の早期適用を
http://www.itmedia.co.jp/enterprise/articles/1506/30/news046.html
V. Flash Playerの脆弱性を狙うWeb改ざん攻撃を多数確認
http://blog.trendmicro.co.jp/archives/11993

# 付録 2:脆弱性対策の方法

## ～迅速に対応できる体制や環境の整備～

10 位「脆弱性対策情報の公開に伴い公知となる脆弱性の悪用増加」の対策の推進には、IPA が公開しているツールやコンテンツを利用することも有効である。参考資料としてご活用頂きたい。

### ◆ 組織内システムの把握・管理の徹底

まず、組織内にあるシステムを把握することから始める。特に、メンテナンスがされなくなり、半ば放置状態のシステムには脆弱性が残存している可能性がある。担当しているシステムに加え、誰も担当しなくなったシステムの情報を把握することが対策の第一歩となる。

### ◆ 継続的な脆弱性対策情報の収集

システムを把握した後は、脆弱性対策が施されているか否かを確認する。これには IPA が公開している脆弱性対策情報データベース「JVN iPedia」を活用するとよい（図 2.1）。[I] また、最新のバージョンを使用していないかを効率的に確認するためには「MyJVN バージョンチェッカ」の利用を薦める。[II]

IPA では、危険度や緊急度が高いセキュリティ上の問題と対策を「重要なセキュリティ情報」として公開している。[III]IPA のウェブサイトにアクセスして、「重要なセキュリティ情報」を確認するやり方以外に、IPA からの情報発信を利用する方法もある。サイバーセキュリティ注意喚起サービス「icat for JSON」（図 2.2）や「Twitter(@ICATalerts)」を利用することでリアルタイムに「重要なセキュリティ情報」を入手できる。[IV]

また、ソフトウェア開発ベンダーが脆弱性対策の取り組みについて情報公開をしていないかウェブサイト等を確認することも重要となる。


図 2.1:JVN iPedia


図 2.2:icat for JSON 利用イメージ

◆　**脆弱性発見時の対応手順の作成**

可用性が重視される重要なシステムほど迅速な対策の実施が難しい。例えば、脆弱性が見つかったソフトウェアを最新バージョンに移行すると旧バージョンで作成したウェブアプリケーションが動かなくなる互換性の問題やシステム開発時の担当者が既に不在であるようなこともある。システム担当者はIPAで公開している資料等を活用し、対応手順を事前に整理しておく必要がある。[V]

脆弱性対策が後手に回り、万が一、ウェブサイトが被害にあった場合には、ウェブサイトの閲覧者への被害が拡大しないよう、利用者への適切なアナウンスやウェブサイトの閉鎖・修復を速やかに実施することが望まれる。

◆　**ソフトウェアの更新**

Windows、Adobe Flash Player、Acrobat Reader、Java 等のクライアントソフトウェアは広く利用されているため攻撃者に狙われやすい。このようなソフトウェアを利用している場合、自動更新の設定を有効にすることで、迅速にソフトウェアの更新ができる。[VI]

◆　**緩和策**

何らかの事情により迅速に対策を行えないような場合もある。このような場合は、緩和策を施すことで、いくらかでも被害にあいにくい環境にすることが重要である。

**(1) ネットワークのアクセス制限による緩和策**

ネットワークのアクセス制限を適切に実施することで、例えば外部の第三者からの攻撃を防ぎ、脆弱性の影響を緩和できる場合がある。

**(2) EMET による緩和策**

マイクロソフト社のWindowsを利用している場合、EMET（Enhanced Mitigation Experience Toolkit）を導入することで脆弱性の影響を緩和できる場合がある。[VII]EMETを導入する場合、導入することで問題が発生しないか事前に検証しておく必要がある。

**参考資料**


I. 活用ガイド　～攻撃状況や組織の環境を踏まえた脆弱性対策について～
http://jvndb.jvn.jp/nav/guide_sysadm.html
II. MyJVN バージョンチェッカ
http://jvndb.jvn.jp/apis/myjvn/personal.html
III. 重要なセキュリティ情報
https://www.ipa.go.jp/security/announce/alert.html
IV. サイバーセキュリティ注意喚起サービス「icat for JSON」
https://www.ipa.go.jp/security/vuln/icat.html
V.「サーバソフトウェアが最新版に更新されにくい現状および対策」
https://www.ipa.go.jp/security/technicalwatch/20140425.html
VI.「 ソフトウェアの自動更新を利用しましょう！
https://www.ipa.go.jp/security/txt/2012/06outline.html
VII.『クライアントソフトウェアの脆弱性対策』に関するレポート
https://www.ipa.go.jp/about/technicalwatch/20130322.html

## 付録 3:10 大脅威 2016 と情報セキュリティ対策の基本との対応

1.4 節で解説した通り、様々な手口・脅威は登場しているが、それに対する対策方法というのは基本的に同じである。ここでは、「情報セキュリティ 10 大脅威 2016」の脅威ごとにどの「情報セキュリティ対策の基本」が効果的なのかを記載する。セキュリティ対策の参考として活用頂きたい。

表 2.4 情報セキュリティ対策の基本と 10 大脅威 2016 との対応

| 順位 | 脅　威 | ソフトウェアの更新 | ウイルス対策ソフト | パスワードの強化 | 設定の見直し | 手口を知る |
|---|---|---|---|---|---|---|
| 1位 | インターネットバンキングやクレジットカード情報の不正利用 | ○ | ○ | ○ | | ○ |
| 2位 | 標的型攻撃による情報流出 | ○ | ○ | | ○ | ○ |
| 3位 | ランサムウェアを使った詐欺・恐喝 | ○ | ○ | | | ○ |
| 4位 | ウェブサービスからの個人情報の窃取 | ○ | ○ | ○ | ○ | ○ |
| 5位 | ウェブサービスへの不正ログイン | ○ | ○ | ○ | | ○ |
| 6位 | ウェブサイトの改ざん | ○ | ○ | ○ | ○ | ○ |
| 7位 | 審査をすり抜け公式マーケットに紛れ込んだスマートフォンアプリ | | ○ | | | ○ |
| 8位 | 内部不正による情報漏えい | | | | ○ | ○ |
| 9位 | 巧妙・悪質化するワンクリック請求 | | | | | ○ |
| 10位 | 対策情報の公開に伴い公知となる脆弱性の悪用増加 | ○ | ○ | | ○ | ○ |

凡例：○　対策効果あり、または部分的に効果あり

このページは空白です。

## 2.2. その他の脅威

個人 18 位　組織 4 位

## 11位 サービス妨害攻撃によるサービスの停止

**～主義主張の誇示や金銭を目的とした猛威を振るう DDoS 攻撃～**

ハッカー集団によるウェブサイトを狙ったサービス妨害攻撃により、ウェブサイトが高負荷状態となり、利用者がアクセスできなくなる被害が発生した。攻撃手口は攻撃者に乗っ取られた複数のマシン（ボットネット）等から大量に負荷をかける DDoS(分散型サービス妨害)攻撃が主流であった。

### ＜脅威と影響＞

企業や組織がウェブサイトを通じて情報発信することは、重要な業務の 1 つとなっている。近年、ウェブサイトに DoS/DDoS 攻撃を仕掛け、閲覧を不可能にする等、業務を妨害する行為が行われている。妨害の目的は主義主張の誇示や金銭目的等である。

### ＜攻撃手口＞

◆ **DDoS**

DDoS には、主に以下の手口が使われる。

- ボットネットの悪用
  ボットネットに攻撃命令を出し、標的組織のサーバーへ負荷をかける攻撃
- リフレクター攻撃
  送信元を標的組織のサーバーに詐称して、脆弱な多数のルータや DNS サーバー等に送り、応答結果を標的の組織に大量に送り付け負荷をかける攻撃
- DNS 水責め攻撃
  ボットネット等で、標的組織のランダムなサブドメインへ問い合わせ、ドメイン名の権威 DNS サーバーに負荷をかける攻撃

また、DDoS を代行するサービスを利用し、金銭を払うことで攻撃を行うこともある。

### ＜事例と傾向＞

◆ **厚労省のウェブサイトに DDoS 攻撃**

厚生労働省のウェブサイトが DDoS 攻撃を受け、安全確認の期間も含め約 3 日間ウェブサイトを停止した。その後、攻撃者から主義主張が表明された。[I]

◆ **金銭目的による DDoS 攻撃**

複数の金融系企業への DDoS 攻撃が確認された。インターネットの取引画面に接続できない状態となっていた。攻撃停止のため、ビットコインによる支払いを要求するメールが届いており、金銭目的と見られている。[II]

### ＜対策/対応＞

**個人・組織**

- OS・ソフトウェアの更新

踏み台にならないために、ルータ等の機器も含め脆弱性対策を行う必要がある。

**組織**

- DDoS 攻撃の影響を緩和する ISP 等によるサービスの利用
- 通信制御（DDoS 攻撃元をブロック等）
- システムの冗長化等の軽減策
- サイト停止時の代替サーバーの用意（告知手段）

**参考資料**

I. 厚労省のウェブサイトにDDoS攻撃 － 一時停止
http://www.security-next.com/064491
II. セブン銀などにDDoS攻撃　ネットバンク接続不良に　警視庁が捜査へ
http://www.sankei.com/affairs/news/150713/afr1507130049-n1.html

個人 10 位　組織 11 位

## 12位 インターネットの広告機能を悪用した攻撃

**～サービスの信頼を揺るがす攻撃～**

インターネット上では様々なサービスが提供されている。利用者の利便性を考慮し、容易に利用できるようにしていることが多い。一方で、どのようなサービスも使い方次第で悪用できる側面を持っている。2015 年はインターネットの広告機能を悪用した攻撃が確認された。対策を怠るとサービスの信頼を失うことに繋がるため、広告配信システムを提供する事業者は信頼できる環境を構築するよう、利用者と協力して対策に取り組む必要がある。

### ＜脅威と影響＞

広告配信機能を悪用し、正規のサービス内に掲載された悪意ある広告を閲覧またはクリックした利用者にウイルスを感染させる被害があった。正規のサービスの場合、広告の悪用有無について、利用者側が見分けることが困難であるため、利用者側での対策が難しく、サービス提供ベンダー側での対策が求められる。

### ＜要因＞

◆ **不正なコンテンツの情報に一致するサービス**

多くの利用者に攻撃をするためには事前に不正なコンテンツを配信するための環境を準備する必要がある。一般に提供しているサービスを用いることで、攻撃に必要な環境を簡易に用意できる場合がある。

◆ **隠匿効果**

正規のサービスに不正なコンテンツを潜ませている場合、一般の利用者が攻撃に気づくことが困難になる。

また、広告主が登録した内容について、確認が十分でないサービスでは、攻撃者を特定することが難しくなる。

### ＜事例と傾向＞

◆ **不正広告によるウイルス感染**

2015 年、ウェブサイト内に表示される広告を悪用して不正な情報を配信し、閲覧者をウイルスに感染させる事例が発生した。[I] 広告配信サービスの悪用を受け、広告配信システムのサービス事業者が、配信内容の確認を強化する取り組みもなされている。[II]

### ＜対策/対応＞

**組織（サービス提供ベンダー）**

- 運用やサービスの監視強化
- 登録情報の確認強化
- 悪用防止に向けたサービスの見直し

**個人（サービス利用者）**

- ソフトウェアの更新
- ウイルス対策ソフトの導入
- 広告ブロックソフトウェアの利用

**参考資料**

I. 不正広告に汚染された正規サイトが攻撃誘導経路に、トレンドマイクロが報告書公開
http://www.atmarkit.co.jp/ait/articles/1511/20/news052.html
II. グーグル、2015年に悪質広告7.8億件を削除--1000人以上を投入
http://japan.cnet.com/news/service/35076730/

個人 6 位　組織 16 位

## 13位 匿名によるネット上の誹謗・中傷

**～悪意のある投稿経験者が増加、投稿に負い目を感じない人も～**

インターネットの匿名性を悪用した、コミュニティサイト（ブログ、SNS、掲示板等）での誹謗中傷の書き込みが社会的な問題となっている。誹謗中傷された側は、精神的ダメージや社会的評判の下落、信頼損失等の被害を受ける。

### ＜脅威と影響＞

スマートフォンやインターネットの普及により、情報を発信することが容易になっている。そうした情報発信の容易さと匿名性により、ネット上で誹謗中傷する行為が相次いでいる。誹謗中傷された側は社会的評判の下落等の被害にあう危険がある。また投稿者側も、匿名で行ったつもりが身元を特定され、謝罪を要求されたり、名誉毀損で訴えられたりする場合があるため、誹謗中傷するような書き込みは控えるべきである。

### ＜要因＞

**◆ 不満の発散**

他者の投稿を見て不快になったり、いらいらしたりしている時等に、不満やストレスの発散を目的に悪意のある投稿が行われる。

**◆ 悪意のある投稿への同調**

他者に対する誹謗中傷の投稿を見て同調し、拡散目的で投稿が行われる。

### ＜事例と傾向＞

**◆ Twitter で中傷するツイートを投稿**

報道関係者が、匿名アカウントを使って弁護士に対し「人権侵害や差別に繋がるような内容を、著しく品位を欠いた表現」で繰り返し投稿していたことが発覚した。[I]

**◆ 悪意のある投稿経験者が増加傾向**

IPA が 2015 年に行った「情報セキュリティの倫理に対する意識調査」によると、PC 利用者およびスマートフォン利用者の悪意のある投稿経験者が 2014 年の調査時に比べ、約 3%増加した。投稿理由の「いらいらしたから」と「相手に仕返しするため」の割合は共に 5%以上増加している。特に 10 代では「いらいらしたから」の割合が 34.2%となり、悪意のある投稿をした理由のトップであった。[II]

### ＜対策/対応＞

**個人（投稿者）**

- モラルの向上（誹謗中傷や公序良俗に反する投稿を控える）
- 投稿前に内容の再確認

**個人（誹謗中傷された側）**

- 誹謗中傷の投稿は、運営側に削除を依頼

**組織**

- 対応ガイドラインの策定
- 迅速・適切な対応（情報提供等）

**参考資料**

I. 新潟日報、Twitterで弁護士中傷の元報道部長を無期限の懲戒休職に 「極めて不適切な行為」
http://www.itmedia.co.jp/news/articles/1511/27/news052.html
II.「2015年度情報セキュリティに対する意識調査」報告書について
https://www.ipa.go.jp/security/fy27/reports/ishiki/index.html

個人 9 位　組織 12 位

## 14位 職業倫理欠如による不適切な情報公開

**～社員の情報モラルの低下～**

個人情報を扱う立場にいる従業員の職業倫理が欠けている事に起因して、情報が漏えいしてしまう事件が発生した。業務上入手し得る情報や、悪ふざけや悪質な行動による不謹慎な内容を従業員が SNS 等に公開したり、個人情報を取り扱う立場でありながら晒し目的で公開したりすることで情報漏えいに繋がった。

### ＜脅威と影響＞

従業員の職業倫理の欠如により、個人情報や機密情報、企業のイメージにかかわる不謹慎な内容が無断で公開される。企業は信用失墜等に繋がるほか、顧客は個人情報をネット上に晒されることになる。

### ＜要因＞

**◆ 職業倫理欠如**

組織に属している・個人情報を取り扱っているという意識が低く、業務上知り得た個人情報や機密情報、または従業員による悪質な行動を、晒し目的等により故意にインターネット上に投稿・公開することで起こる。

### ＜事例と傾向＞

**◆ 晒し目的による情報漏えい**

個人情報の安全を守る立場にある企業の従業員が、独自に情報収集した個人情報を晒し目的で公開した。従業員が在籍していた企業は公開した情報を企業側が入手することは不可能であることを示し、一切関与していないことを強調した。[I]

**◆ 従業員が買い物客の画像を投稿**

コンビニの従業員が買物客を盗撮し、写真や身分証明証を公開する等、悪質な画像の投稿を行っていた。[II]

これらの事例から再発防止を徹底するよう、従業員 1 人 1 人に職業倫理を意識付ける必要があることが伺える。

### ＜対策/対応＞

**組織**

- 従業員の情報モラル教育を徹底
- 情報のアクセス権限の適正化
- 不適切な情報公開が発覚した際の対応をマニュアル化

情報を取り扱う立場としてその情報をどのように扱うべきなのか、適切に判断できるよう、従業員の教育が求められる。

また、従業員ごとにアクセスできる範囲や権限を設定することで、不適切な情報公開に伴う被害範囲を局所化できる。

また、不適切に情報を公開してしまった場合でも、対応フローをマニュアル化しておくことで初動対応を円滑に行い、事態の収束を早めることが期待できる。

**参考資料**

I.「個人情報晒し」騒動、セキュリティ会社が調査結果発表　渦中の人物は退職
http://www.j-cast.com/2015/11/09250055.html
II.「貧乏人は来るな」 セブンーイレブン店員が客を大量盗撮　個人情報や悪口もネット投稿（1/2）
http://www.itmedia.co.jp/news/articles/1511/25/news058.html

個人 11 位　組織 13 位

## 15位 インターネットサービス利用に伴う意図しない情報漏えい

**～そのサービスや機能は使って大丈夫？知らぬ間に情報漏えい～**

サーバー上でのデータ共有や他サービスとの連携等、便利な機能を持つサービスが提供されている。しかし、利用者がその機能を理解せずに利用していたため、意図せず個人情報や企業秘密等を漏えいしてしまうことがある。

### ＜脅威と影響＞

IT 利用の普及によりインターネットを利用したサービスが多数存在する。サーバー上でデータ共有するサービスや他サービスとの連携を提供するサービス等がある。利用者が機能を理解せずにサービスを利用すると、個人情報や企業秘密等を、意図せずサーバーへ保存したり、サービス連携を通して漏えいしたりする可能性がある。

### ＜要因＞

**◆　機能や危険性を理解せずに利用**

世の中で提供されているサービスは様々な機能を持っている。利用者がサービスの信頼性、機能や危険性を理解せずに利用すると情報漏えいする場合がある。

**◆　不用意なサービス・アプリ連携許可**

サービス・アプリによっては利用者にサービス・アプリ連携の許可やデータへのアクセス許可を求めるものがある。利用者が許可する内容を確認せずに、承認してしまうことで、情報漏えいに繋がる場合がある。

### ＜事例と傾向＞

**◆　翻訳サイトを利用して機密情報漏えい**

無料の翻訳サイトに入力した翻訳情報が翻訳例として誰でも閲覧可能な状態であった。中央省庁職員のメール内容や金融機関内でのやり取り内容が漏えいしている。外部サイトに企業秘密を送信することは自組織の情報セキュリティポリシーに違反する恐れがあるため、注意が必要である。[I]

**◆　SNS の友達申請で連絡先が漏えい**

SNS の友達申請を承認すると Google アカウントに登録されている連絡先が漏えいする被害が発生した。その連絡先を使って同様の友達申請が自動で行われ、被害が拡大した。友達申請のサービス連携の許可を確認せずに承認したことが原因である。[II]

### ＜対策/対応＞

**個人・組織**

- 機能・危険性の理解（自組織の情報セキュリティポリシーに違反しないか等）
- サービス・アプリ連携は不用意に許可しない

サービス提供元は、サービスのわかりやすい説明と、情報の取扱い方針等について示すことが求められる。

**参考資料**

I.「翻訳サイト入力の情報、閲覧状態に　中央省庁や大手メーカー」
http://www.nikkei.com/article/DGXLASDG20H2X_Q5A220C1CC0000/
II. IPA:「不用意なクリックによって自分名義の招待メールが友人に送信される可能性」
https://www.ipa.go.jp/security/txt/2015/11outline.html

個人 17 位　組織 10 位

## 16位 過失による情報漏えい

**～注意していれば防げた過失による情報漏えい～**

組織や企業では、情報に対する意識の低さや確認漏れ等により、従業員による個人情報や企業秘密の漏えいが後を絶たない。漏えいした情報が悪用される等の二次被害も懸念される。

### ＜脅威と影響＞

組織や企業がサービスを提供していく上で、サービスや立場によっては個人情報や企業秘密を取り扱うことがある。これら重要な情報を取り扱うことに対する意識の低さから、情報漏えい事件が発生している。漏えいした情報から二次被害が発生することもある。

### ＜発生要因＞

**◆　従業員のセキュリティ意識の低さ**

個人情報や企業秘密を取り扱う従業員が持つセキュリティ意識の低さから、これらの情報が入ったカバンを外出先で紛失したり、個人情報等を含むメールを誤送信したり、といった過失から情報漏えいする。

**◆　組織規定および確認プロセスの不備**

重要情報の定義、その取扱い規則、持ち出し許可手順の不備や、作業実行時の確認プロセス不備のまま重要情報を取り扱っていることが多く、情報漏えいを起こしやすい業務環境となっている。

### ＜事例と傾向＞

**◆　国交省職員が飲酒寝過ごしで置き引き**

国土交通省の航空局長が飲酒後の電車で寝過ごし、網棚に置いたカバンを置き引きされる事件が発生した。カバンの中には業務用タブレットや緊急連絡網を記した資料が含まれていた。[I]

**◆　リクルートキャリア社でケアレスミスによる情報漏えい**

人材採用広告事業等を行うリクルートキャリア社が、登録者のプロフィールや学歴等、本来は加工してすべき情報を加工しないまま業務委託先企業へメール送信してしまう事件が発生した。約 37,000 件の個人情報が含まれていた。[II]

### ＜対策/対応＞

**組織**

- 従業員のセキュリティ意識教育
- 組織規定および確認プロセスの確立
- 情報の暗号化

人的ミスを完全に防ぐことは困難である。人的ミスが起こることを前提に、組織内の規定を作成、システムおよび運用面での承認・管理体制の強化を行う必要がある。

**参考資料**

I.「国交省航空局長、電車内でカバン置き引き被害　飲酒で寝過ごし…職員連絡網など流出
http://www.sankei.com/affairs/news/150614/afr1506140012-n1.html
II. リクルートキャリアが約3万7000件の個人情報を誤送信
http://www.atmarkit.co.jp/ait/articles/1512/04/news096.html

個人 14 位　組織 14 位

# 17位 IoT に関連する機器の脆弱性の顕在化

## ～多種多様な機器が繋がる日常～

自動車、情報家電、医療機器、インフラ設備、流通用機器等、日常生活に関連する多種多様な機器がインターネットに繋がるようになってきた。従来インターネットに繋がることを想定していなかった機器が、インターネットに繋がることにより脆弱性への脅威が顕在化してきた。

### ＜脅威と影響＞

昨今、自動車や情報家電等 IoT に関連する機器が登場し、世の中に普及し始めている。一方、それらの機器は、今までインターネットに繋がることを想定しておらず、十分なセキュリティが考慮されていない状態でインターネットに繋がっているものもある。それにより、攻撃者がインターネット越しにその機器の脆弱性や設定不備等を突いて攻撃を行い、不正アクセスやウイルス感染等が行われる可能性がある。その後、データの改ざんや漏えい、機器操作をされる等が懸念される。

### ＜攻撃手口＞

- ◆ DoS/DDoS
- ◆ IoT に関連する機器の脆弱性を悪用
- ◆ 他機器からのウイルス感染

### ＜事例と傾向＞

**◆ 米国の自動車がハッキング対策で 140 万台リコール**

クライスラー製自動車の車載情報システムに脆弱性が存在し、外部からの攻撃により、車両を操作される可能性があった。[I]

**◆ IoT 機器を標的とした攻撃とアクセスを観測**

警察庁の発表によると、インターネットに接続された IoT 機器を標的とした攻撃を観測しており、この攻撃を受けた機器が、攻撃者の命令に基づいて動作する「ボット」になる事例を確認した。[II] また、産業制御システムで使用される PLC（Programmable Logic Controller）の脆弱性を標的としたアクセスも観測されている。[III]

### ＜対策/対応＞

**組織(製品開発者)**

- 脆弱性対策　等

詳細については、IPA が公開している SEC journal[IV] 参照して頂きたい。

**組織(利用者)、個人**

- 機器使用前に、説明書を確認
- 初期設定済みのパスワードの変更
- 不要な機能の無効化
- 機器のソフトウェアの更新
- 他の機器によるインターネットの接続制限（ルータ、ファイアウォール等）

**参考資料**

I. Chrysler、車の遠隔操作問題で140万台のリコール発表
http://www.itmedia.co.jp/enterprise/articles/1507/27/news038.html
II. IoT機器を標的とした攻撃の観測について 平成27年12月15日
https://www.npa.go.jp/cyberpolice/detect/pdf/20151215_1.pdf
III. 産業制御システムで使用されるPLCを標的としたアクセスの観測について（第2報）
https://www.npa.go.jp/cyberpolice/detect/pdf/20150605.pdf
IV. つながる世界における脅威と脆弱性対策のポイント（SEC Journal No.43）
https://www.ipa.go.jp/files/000049573.pdf

個人 8 位　組織 19 位

## 18位 情報モラル不足に伴う犯罪の低年齢化

**～情報社会におけるモラルとリテラシーを身につけよう～**

近年、未成年者が IT 犯罪の加害者として逮捕、補導されるケースが増加している。逮捕・補導されて初めて、自身の行為が犯罪であると認識するケースが多く、幼少期から情報社会におけるモラルとリテラシーを教えていくことが社会全体に求められる。

### ＜脅威と影響＞

近年、オンラインゲームや学習教材、コミュニケーションサービス等の若者向けのコンテンツが充実しており、未成年者のインターネット利用は当たり前となっている。しかし、未成年者は情報モラルや情報リテラシーが不十分である場合もあり、ちょっとした興味からウイルスを作成したり、友人のパスワードを聞きだしたりして不正アクセスを行うことがある。さらには、インターネット上で金銭目的の犯罪を行う事例も増加してきている。

### ＜発生要因＞

◆ **金銭目的**

未成年者が金銭を目的としてコンピュータウイルスを作成・販売する。

◆ **いたずらや能力の誇示**

情報モラルや情報リテラシーが欠如しているため、「犯罪」という認識がないまま、いたずらや能力の誇示をする。

### ＜事例と傾向＞

◆ **PC ウイルスの販売や購入**

札幌市の中学生が、不正送金に利用されるウイルスの保管容疑で逮捕された。[I]また、自身が作成したウイルスの提供容疑(販売)で再逮捕されたが、販売相手も中学生であった。[II]

◆ **ランサムウェアによるサイバー攻撃**

インターネット上で「ZeroChiaki」と名乗る少年がランサムウェアを作成し、サイバー攻撃を繰り返すという事件が発生した。[III] ランサムウェアは世界中で確認されているが、日本語対応版として初めて発覚したものはこの事件を起こした少年によるものだった。

### ＜対策/対応＞

**個人**

- 情報モラルの教育
- 情報リテラシーの教育


**参考資料**

I. 「ウイルス保管容疑で14歳逮捕＝海外サイトで販売か－警視庁
http://www.jiji.com/jc/zc?k=201511/2015110400238
II. 中2女子にPCウイルス販売容疑　中2男子を再逮捕
http://www.asahi.com/articles/ASHCS36H0HCSUTIL00C.html
III. ウイルス作成ツール初摘発　保管容疑で「ZeroChiaki」追送検
http://www.sankei.com/affairs/news/150814/afr1508140010-n1.html

個人 13 位　組織 17 位

## 19位 無線 LAN の無断使用・盗聴

**～一般家庭でも利用されている無線 LAN ルータが犯罪に悪用されることも～**

一般家庭でも利用されている無線 LAN ルータにおいて、アクセスポイントを「ただ乗り」される被害が後を絶たない。被害を防止するためには、無線 LAN を利用する上での脅威を理解した上で、不正な利用をさせない設定等を実施しておくことが重要である。

### ＜脅威と影響＞

適切なセキュリティ設定がされていない無線 LAN はアクセスポイントに不正に接続され、通信内容を傍受される、管理画面に不正アクセスされる、犯罪行為の踏み台に利用される等の被害を受ける可能性がある。また、公衆無線 LAN は誰でも容易に利用することができるため、強力な暗号技術を使っていてもパスワードが共有されている場合、通信を傍受される可能性がある。

### ＜攻撃手口＞

◆ **脆弱なアクセスポイントを突き、無断使用、盗聴される**

パスワード未設定のアクセスポイントやパスワード強度の弱いアクセスポイントに接続して無断使用したり、通信を盗聴したりする。

WEP(Wired Equivalent Privacy)等の暗号強度の低い暗号技術を使っている場合、パスワード解析ソフトを悪用することで簡単にパスワードが解読される。WEP の場合、解読に要する時間はわずか 10 秒という実証結果も公表されている。[I]

また、強固な暗号技術を使っている場合でも、同一の無線 LAN ネットワークを使用していると、パスワードが同一なため、通信を盗聴されることがある。

### ＜事例と傾向＞

◆ **狙われる自宅の無線LAN**

他人の無線 LAN 環境に無許可で接続を行い、インターネットバンキングの不正送金等を行っていた男性が逮捕される事件があった。[II] IPA でもこの事件を受けて、あらためて一般家庭における無線 LAN 利用に関する注意喚起を行っている。[III]

### ＜対策/対応＞

**個人**

- 強固な暗号技術（WPA2-PSK 等）・複雑なパスフレーズの使用

公衆用無線 LAN 利用時等は VPN サーバーを経由して接続することで盗聴を防ぐことができる。

**組織(公衆用無線 LAN 提供元)**

- WPA2-EAP 等の使用

**参考資料**


I. Internet Watch Corporation：「WEPは10秒で解読可能」、神戸大と広島大のグループが発表
http://internet.watch.impress.co.jp/cda/news/2008/10/14/21162.html
II. 産経新聞：狙われる自宅の無線LAN　ただ乗り簡単、犯罪に巻き込まれる可能性
http://www.sankei.com/premium/news/150630/prm1506300003-n1.html
III. IPA：【注意喚起】家庭内における無線LANのセキュリティ設定の確認を
https://www.ipa.go.jp/security/topics/alert270612.html

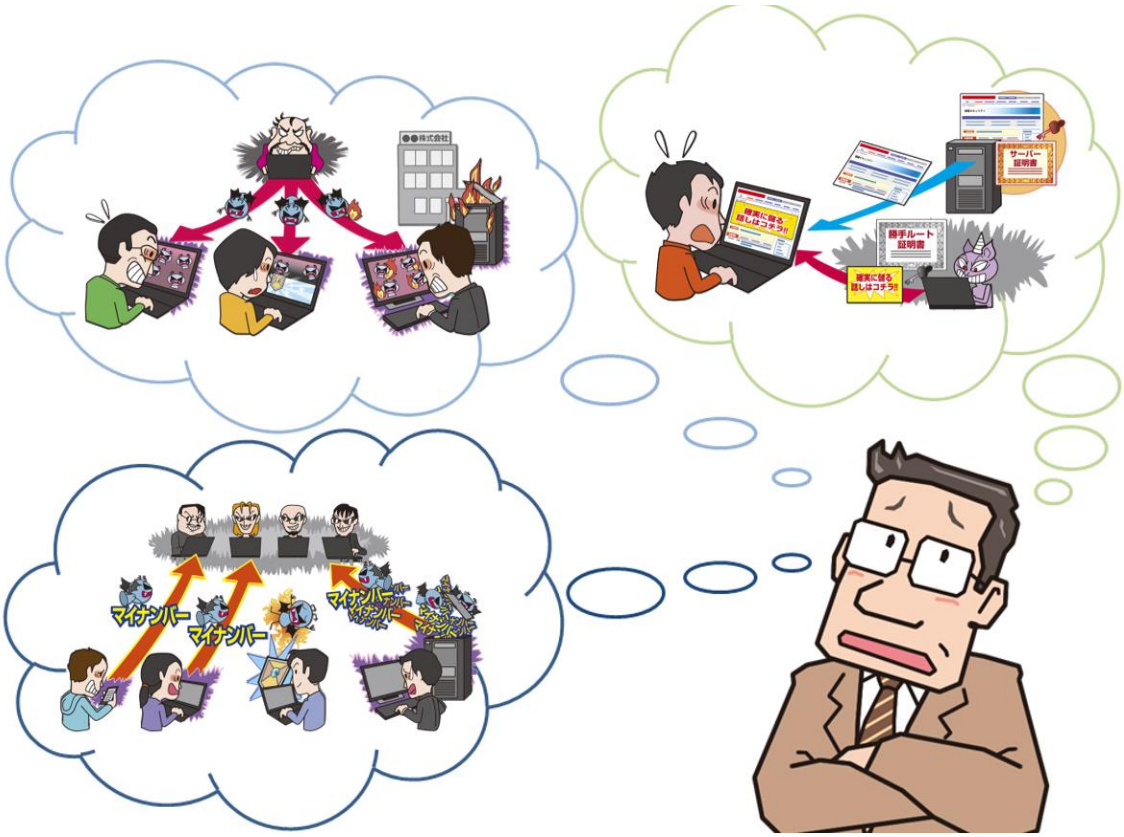
# 3章. 注目すべき脅威や懸念

# 3 章 注目すべき脅威や懸念

本章では、解決すべき課題や、問題視されている脅威や今後大きな脅威となると考えられる表 3.1 に記載している 3 つの懸念について解説する。

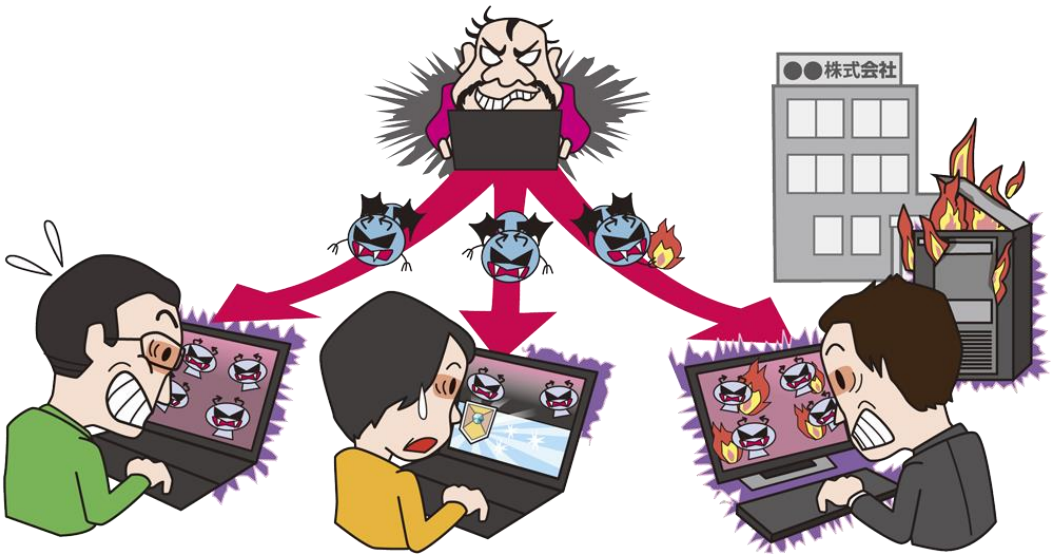
**表 3.1：注目すべき脅威や懸念**

| 番号 | タイトル |
|---|---|
| 1 | サポートの終了したソフトウェアを継続使用する危険性<br>～サーバーOS やブラウザも最新版の利用へ移行を～ |
| 2 | 証明書の導入・設定不備や検証不備に起因する脅威と対策<br>～ルート証明書の強制インストールに御用心～ |
| 3 | マイナンバーの管理・運用の重要性<br>～他者のマイナンバーを預かる事業者等は厳重な管理を～ |



## 3.1. サポートの終了したソフトウェアを継続使用する危険性

**～サーバーOS やブラウザも最新版の利用へ移行を～**




サポートが終了してパッチが提供されなくなったソフトウェアを使い続けている PC が残存しており、いまだに Windows XP を使い続けている個人や組織が存在すると報道されている。Windows Server 2003 が 2015 年 7 月にサポート終了となり、2016 年 1 月に Internet Explorer のサポート方針が変更となった。永続的にサポートされるソフトウェアは存在しないため、サポートの終了したソフトウェアの継続使用中止、最新版への移行は、常に忘れてならない課題である。

### ＜継続利用の危険性＞

サポートが終了したソフトウェアは、セキュリティ更新プログラムの提供が終了する。このことは、脆弱性が発見されたとしても、修正するためのアップデートが提供されないことを意味する。また、原則として、ソフトウェア提供ベンダーから脆弱性情報を含む技術情報の提供が終了する。即ち、サポート終了以降に発見された脆弱性を利用者は知ることができない。

この結果、例えばウイルス感染や不正アクセスの被害にあいやすくなる。個人情報や企業の機密情報が漏えいして本人・自社が被害を受けるだけでなく、不特定多数の第三者に攻撃するための「踏み台」に悪用された場合、加害者になってしまう危険性がある。特に企業の場合、社会的信用の失墜や対応へのコスト増大等、経営リスクにも繋がりかねない。脆弱性を利用した攻撃の脅威については、2 章にて詳しく説明しているので、参照のこと。

### ＜サーバーOS やブラウザも＞

2014 年 4 月 9 日（日本時間）、マイクロソフト社による Windows XP、Office 2003、Internet Explorer 6 のサポートが終了したが、2015 年から 2016 年にかけても、企業および個人において、広く使用されているソフトウェアのサポートが終了した。

◆ Windows Server 2003

2015 年 7 月 15 日（日本時間）に、マイクロソフト社が提供している Windows Server 2003 のサポートが終了した。[I][II]

◆ Internet Explorer

2016 年 1 月 12 日（米国時間）、マイクロソフト社が提供するウェブブラウザ Internet Explorer（以後、IE）のサポートポリシーが変更された。サポートが継続される IE は、各 Windows OS で利用可能な最新版のみとなった。[III] [IV]

## ＜最新版に移行できない利用者＞

◆ **いまだに使われている Windows XP**

サポートが終了してから約二年間が経過し、他の OS への移行が推奨されている Windows XP だが、いまだに国内外で利用されているようだ。

NetApplication 社の調査によれば、インターネットアクセスに使われている OS の内、10.93%が Windows XP であると報告されている（2015 年 12 月の値）。[V]

◆ **Windows Server 2003 も同様の状況**

2015 年 1 月の時点の調査であるが、サーバー運用管理者の約半数がサポート終了後に Windows Server 2003 を利用し続けると回答した、との報告がある。[VI]

## ＜最新版への移行＞

やむを得ない事情により早急に移行ができない場合は、ネットワークに繋がっていない環境で利用する等のリスク緩和策を実施すること。但し、リスク緩和策を行ったとしても、脆弱性が解消される訳ではないため、可能な限り早急な移行を進めることを推奨する。

## ＜今後のサポート終了予定＞

現在サポートが継続しているOS やアプリケーションであっても、その多くはメーカーからサポート終了予定が発表されている。例えば、マイクロソフト社の主要ソフトウェアの場合、以下のサポート終了予定日となっており、永続的に安全に使い続けられるソフトウェアは存在しないと考えるべきである。

- SQL Server 2005 : 2016 年 4 月 12 日
- Windows Vista : 2017 年 4 月 11 日
- Office 2007 : 2017 年 10 月 10 日
- Windows 7 : 2020 年 1 月 14 日
- Windows Server 2008 R2 : 2020 年 1 月 15 日

## ＜組織においては計画的な運用を＞

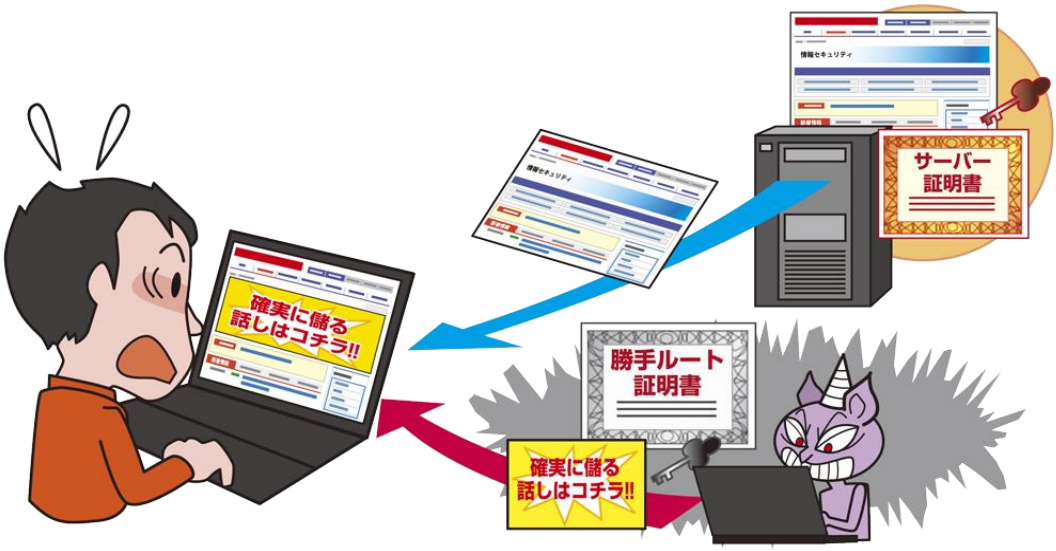
企業・組織においては、組合せて使用しているアプリケーションが動作しなくなる等の理由により、最新版への移行が困難な場合が考えられる。システム担当者は、システムの構築や更改、運用にあたり、(1)特定の製品やバージョンに依存しないこと、(2)ソフトウェア製品のライフサイクルを考慮すること、等の計画性が求められる。

**参考資料**


I. 日本マイクロソフト：Windows Server 2003 サポート終了
https://www.microsoft.com/ja-jp/server-cloud/products-Windows-Server-2012-r2-Support.aspx
II. IPA：Windows Server 2003のサポート終了に伴う注意喚起
https://www.ipa.go.jp/security/announce/win2003_eos.html
III. 日本マイクロソフト：Internet Explorer のサポートポリシーが変わりました。
https://www.microsoft.com/japan/msbc/Express/ie_support/
IV. IPA：【注意喚起】Internet Explorer のサポートポリシーが変更、バージョンアップが急務に
https://www.ipa.go.jp/security/ciadr/vul/20151215-IEsupport.html
V. マイナビニュース：Windows XPが2位に復活 - 12月OSシェア
http://news.mynavi.jp/news/2016/01/04/088/
VI. トレンドマイクロ：Windows Server 2003利用の企業ユーザのうち、約半数がサポート終了後も継続利用予定
http://www.trendmicro.co.jp/jp/about-us/press-releases/articles/20150108023429.html

## 3.2. 証明書の導入・設定不備や検証不備に起因する脅威と対策

～ルート証明書の強制インストールに御用心～




本来は盗聴や改ざん、なりすましといった脅威を防止するための公開鍵証明書にかかわる脆弱性（導入・設定不備や検証不備等）によって、新たな攻撃のきっかけが生まれている。

### ＜公開鍵証明書の役割組織においては計画的な運用を＞

現在、PC やスマートフォンでオンラインショッピングやインターネットバンキングを利用する等、インターネット上のサーバーと通信する場合の多くは、TLS（Transport Layer Security）というプロトコルを用いて通信内容の盗聴や改ざんを防止している。TLS は、公開鍵暗号という暗号技術を用いており、公開鍵証明書（以下、「証明書」）が重要な役割を担っている。

証明書は、公開鍵とその所有者の結び付きを証明するもので、通信相手やデータの作成者を確認する認証や、盗聴されないように暗号化するための暗号鍵の交換を実現する。証明書は、通常は認証局（CA: Certification Authority）という信頼できる第三者機関によって発行され、特に認証局が自身の公開鍵に対して、公開鍵に対応する秘密鍵で署名発行した証明書（自己署名証明書）を「ルート証明書」と呼ぶ。ルート証明書は、PC やスマートフォン内の「信頼する証明書」として管理されており、セキュリティの基礎となっている。

### ＜勝手ルート証明書問題[1]＞

2015 年 2 月、レノボ社製の個人向けノート PC の一部に搭載されているサードパーティ製ソフトウェア Superfish に脆弱性が確認され、同社から削除ツールが提供された。

**◆ 問題点の本質**

Superfish には、以下の問題点があった。

- 認証局でないアプリケーション自身の自己署名証明書を、OS 内にルート証明書としてインストールしていた。
- 同時に、プログラムの一部として証明書内の公開鍵に対応する秘密鍵（本来は公開不可の鍵）をインストールしていた。

- この自己署名証明書と秘密鍵は、全世界で共通、即ち容易に入手可能であった。
- インストールされた証明書と秘密鍵を使用して、他のウェブサイト用に発行されたサーバー証明書の偽物を生成し、これらを用いて TLS で保護されたサイトの表示時に無理矢理広告を挿入していた。

**◆ それらによる影響**

Superfish が行っていた行為は、盗聴・改ざん防止されたウェブサイトのコンテンツを通信路上で書き換えて、許可なく広告を挿入するもので、不正行為にあたる。また、Superfish の証明書と秘密鍵を第三者が悪用した場合、(1)信頼できる他のサイトやサービスへのなりすまし、(2)ソフトウェアやメールへの署名偽造、(3)通信内容の解読、(4)悪意のあるソフトウェアの強制インストール等が可能となる危険性を秘めていた。本問題発覚後も、認証局以外が発行した自己署名証明書をルート証明書に強制インストールするソフトウェアが発見され、一部では「勝手ルート証明書」や「オレオレ認証局」問題といわれるようになった。

## ＜勝手ルート証明書問題、再び[II]＞

2015 年 11 月、デル社製クライアント PC とタブレットに、遠隔サポートサービス提供用としてプレインストールまたは更新インストールされた証明書（eDellRoot 証明書および DSDTestProvider 証明書）が問題となり、これらを削除するアップデートが配信された。

**◆ 問題点の本質**

レノボ社の件と同様、デル社の問題でも、認証局発行でない自己署名証明書をルート証明書にインストールし、本来秘密にすべき秘密鍵が含まれていた。今回、秘密鍵はパスワードで保護されていたが、誰もが容易に推測可能な文字列が使用されていたため、第三者が不正利用可能となっていた。

**◆ それらによる影響**

デル社自身はこれらの証明書や秘密鍵を用いた通信内容の盗聴・改ざんを行っていなかったが、第三者の悪用により、Superfish と同様の脅威が発生する危険性がある。このため、一部では「Superfish2.0」問題と呼ばれた。

## ＜証明書の検証不備の多発[III]＞

これらの問題に加えて、様々なアプリケーションにおいて、サーバー証明書の検証不備の脆弱性が発見されている。詳細は割愛するが、放置すると通信内容の盗聴や改ざんが行われる危険性を生じている。

## ＜事業者が注意すべきこと＞

認証局発行でない自己署名証明書をルート証明書にインストールするソフトウェア、秘密鍵を他者に配布することで動作するソフトウェア等を開発・配布すべきではない。証明書に関する問題が発見された場合、速やかに脆弱性情報を公開すると共に、更新プログラム等の解決策を提供することが必要である。

## ＜個人として注意すべきこと＞

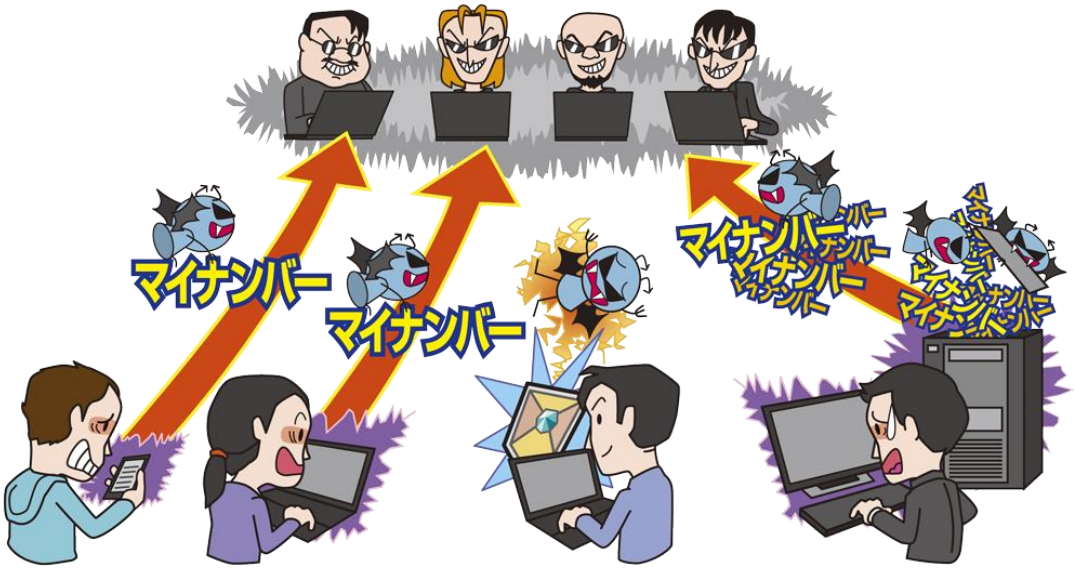
最新情報の収集に努め、更新プログラム等が提供された場合、早急に適用することが重要である。また、サードパーティ製のソフトウェアには「勝手ルート証明書」問題を含んでいる危険性があるので、不審なソフトウェアはインストールしないことを推奨する。

**参考資料**

I. レノボ： Superfishの脆弱性
https://support.lenovo.com/jp/ja/product_security/superfish
II. デル：弊社PC証明書脆弱性について（eDellRoot証明書ならびにDSDTestProvider証明書）
http://ja.community.dell.com/dell-blogs/direct2dell/b/direct2dell/archive/2015/11/26/pc-edellroot-dsdtestprovider
III. JVN iPedia：JVNDB-2015-000181 iOS アプリ「ぐるなび」における SSL サーバ証明書の検証不備の脆弱性
http://jvndb.jvn.jp/ja/contents/2015/JVNDB-2015-000181.html

## 3.3. マイナンバーの管理・運用の重要性

**～他者のマイナンバーを預かる事業者等は厳重な管理を～**




2016 年 1 月からマイナンバーの利用が開始されたが、利用開始前から人為的誤り等による漏えいが問題となっている。制度自体は危険なものではないが、個人が自身のマイナンバーを適切に管理すると共に、他者のマイナンバーを預かる関係者が厳重に管理・運用する必要がある。

### ＜マイナンバーの漏えい＞

マイナンバー[I・II・III]の利用開始前から、一部で漏えい（未遂を含む）が発生している。マイナンバー通知カードの誤配達、マイナンバーが印刷された公文書の誤交付・誤送付等、人為的かつ物理的誤りが原因である。自動交付機の設定不備により、記載不要の住民票にマイナンバーを印刷・交付してしまったという、IT（情報技術）上の誤りを原因とする事案も発生している。また、専用ネットワーク内で起きたため「外部への漏えい」は避けられたものの、マイナンバーを含む個人情報のデータファイルの誤送信も発生している。

### ＜便乗不審メールの流布＞

マイナンバーに便乗した詐欺行為は、電話や直接訪問のほか、電子メールを用いて行われている。[IV] マイナンバーを話題としたメールから不正なウェブサイトへのアクセスを誘導したり、個人情報を入力させたり、不正送金させたりと、様々な脅威が発生している。

### ＜大規模漏えいの危険性＞

現時点では大規模漏えいは発生していないが、今後、各企業が従業員のマイナンバーを収集・管理することから、他者のマイナンバーを預かった事業者が注意を怠ると、大規模漏えいに繋がる危険性がある。

### ＜漏えいが発生すると・・・＞

マイナンバーに相当する「社会保障番号（SSN: Social Security Number）」の導入で先行する米国では、漏えいした番号による「なりすまし」事件が大きな問題となっている。[V] 窃取した社会保障番号を用いて、銀行口座開設、クレジットカードの作成と利用、住所変更手続等が可能であるため、被害者になり

すまして還付金や年金の給付を横取りする、という金銭的被害が発生している。2015 年 7 月、ハッカー集団により合衆国政府のデータベースから 2150 万人の社会保障番号（内 560 万人は指紋データを含む）が盗まれるという事件も発生している。[VI]

一方、日本では、マイナンバーを使う手続において、原則、顔写真付き身分証明書等を用いた本人確認を必要としているため、マイナンバー単独の漏えいではなりすましは発生しない。したがって、漏えいしたマイナンバーを用いた不正な手続は出来ないため、個人情報等が窃取されることはない。

## ＜個人として注意すべきこと＞

### ◆ 趣旨と提示範囲の理解

マイナンバーは、法令に定められた社会保障・税・災害対策の行政手続のためのみに提示が求められるものである。また、勤務先事業主や金融機関が個人の手続を代行する場合、勤務先等に提示する必要がある。上記以外で提示が求められた場合は、拒否すべきである。なお、個人のブログ等における自身のマイナンバー公開は、法律違反となる恐れがあるため、行ってはならない。制度の趣旨と開示範囲を、個人が理解・把握しておくことが重要である。

### ◆ 電子化して保存する場合

記憶用等で PC やスマートフォンにマイナンバーを電子化して保存する場合は、不正アクセスや漏えいに備えて、情報自体を暗号化し、端末操作にパスワード入力や指紋認証等の本人確認を必須となるように設定すべきである。

### ◆ ネットワーク経由で提示する場合

勤務先等にマイナンバーを提示する際、メールやウェブサイトでの連絡、即ちネットワークを経由する場合は、注意が必要である。マンナンバーを電子化することになり、不正アクセスや漏えいの恐れがあるため、メールやウェブサイト経由の送信に対しても、暗号化や改ざん防止対策をすべきである。それが不可能であれば、ネットワーク経由の通知は行わない方がよい。

## ＜事業者が注意すべきこと＞

マイナンバーを含む特定個人情報に関する罰則は、不正行為に対して厳格に対処するために、個人情報保護法における類似規定より強化されている。事業者は、特定個人情報の取扱いに関するガイドラインを遵守し、法令に定められた利用制限、厳重な管理、提供・収集の制限を実施しなければならない。[VII]ガイドラインの規定を満たしたことで満足せず、継続的なセキュリティ対策の見直し・実施が求められる。

金融業務にかかわる事業者や行政機関・地方公共団体等は、個別のガイドラインが公開されているので、併せて従う必要がある。

**参考資料**


I. 総務省：マイナンバー制度とマイナンバーカード
http://www.soumu.go.jp/kojinbango_card/index.html
II. 内閣官房：マイナンバー 社会保障・税番号制度
http://www.cas.go.jp/jp/seisaku/bangoseido/
III. 政府広報オンライン：社会保障・税番号制度＜マイナンバー＞
http://www.gov-online.go.jp/tokusyu/mynumber/index.html
IV. 消費者庁：マイナンバー制度に便乗した不正な勧誘や個人情報の取得にご注意ください！
http://www.caa.go.jp/adjustments/pdf/151001adjustments_1.pdf
V. Yahoo!ニュース：マイナンバー、先行する米国「なりすまし」被害の実態
http://news.yahoo.co.jp/pickup/6178886
VI. ITmedia：米政府版マイナンバー情報漏えい、560万人の指紋データも流出していたことが判明
http://www.itmedia.co.jp/news/articles/1509/24/news101.html
VII. 個人情報保護委員会：特定個人情報の適正な取扱いに関するガイドライン
http://www.ppc.go.jp/legal/policy/

# 10 大脅威選考会

| 氏名 | 所属 | 氏名 | 所属 |
|---|---|---|---|
| 石田 淳一 | (株)アールジェイ | 宮崎 清隆 | (社)JPCERT コーディネーションセンター |
| 石井 彰 | 旭化成ケミカルズ(株) | | (JPCERT/CC) |
| 岡田 良太郎 | (株)アスタリスク・リサーチ | 金田 智史 | (株)シマンテック |
| 佐藤 直之 | (株)イノベーションプラス | 浜田 譲治 | (株)シマンテック |
| 齋藤 衛 | (株)インターネットイニシアティブ | 山内 正 | (株)シマンテック |
| 高橋 康敏 | (株)インターネットイニシアティブ | 平田 真由美 | (一社)セキュリティ対策推進協議会 |
| 梨和 久雄 | (株)インターネットイニシアティブ | | (SPREAD) |
| 楢原 盛史 | ヴイエムウェア | 唐沢 勇輔 | ソースネクスト(株) |
| 三輪 信雄 | S&J(株) | 辻 伸弘 | ソフトバンク・テクノロジー(株) |
| 松本 隆 | SCSK(株) | 鈴木 一弘 | 地方公共団体情報システム機構(J-LIS) |
| 大塚 淳平 | NRI セキュアテクノロジーズ(株) | 永野 恵寿 | 地方公共団体情報システム機構(J-LIS) |
| 小林 克巳 | NRI セキュアテクノロジーズ(株) | 百瀬 昌幸 | 地方公共団体情報システム機構(J-LIS) |
| 正木 健介 | NRI セキュアテクノロジーズ(株) | 杉山 俊春 | (株)ディー・エヌ・エー |
| 中西 克彦 | NEC ネクサソリューションズ(株) | 森 槙悟 | (株)ディー・エヌ・エー |
| 北河 拓士 | NTT コムセキュリティ(株) | 桑原 和也 | デジタルアーツ(株) |
| 東内 裕二 | NTT コムセキュリティ(株) | 岩井 博樹 | デロイト トーマツ リスクサービス(株) |
| 鴨田 浩明 | (株)NTT データ | 後藤 啓一 | 東京都 |
| 西尾 秀一 | (株)NTT データ | 大浪 大介 | (株)東芝 |
| 宮本 久仁男 | (株)NTT データ | 小島 健司 | (株)東芝 |
| 植草 祐則 | NTTデータ先端技術(株) | 田岡 聡 | (株)東芝 |
| 佐久間 邦彦 | NTTデータ先端技術(株) | 長尾 修一 | 東芝インフォメーションシステムズ(株) |
| 村上 純一 | (株)FFRI | 小屋 晋吾 | トレンドマイクロ(株) |
| 前田 典彦 | (株)カスペルスキー | 須川 賢洋 | 新潟大学 |
| 奥村 剛 | 技術研究組合制御システムセキュリティ | 井上 博文 | 日本アイ・ビー・エム(株) |
| | センター(CSSC) | 猪股 秀樹 | 日本アイ・ビー・エム(株) |
| 小林 偉昭 | 技術研究組合制御システムセキュリティ | 坂 明 | 日本サイバー犯罪対策センター(JC3) |
| | センター(CSSC) | 宇都宮 和顕 | 日本電気(株) |
| 岡村 浩成 | 京セラコミュニケーションシステム(株) | 谷川 哲司 | 日本電気(株) |
| 佐藤 宏昭 | 京セラコミュニケーションシステム(株) | 住本 順一 | 日本電信電話(株) |
| 古澤 健一 | 京セラコミュニケーションシステム(株) | 大森 雅司 | NPO 日本ネットワークセキュリティ協会 |
| 秋山 卓司 | クロストラスト(株) | | (JNSA) |
| 小熊 慶一郎 | (株)KBIZ / (ISC)2 | 加藤 雅彦 | NPO 日本ネットワークセキュリティ協会 |
| 淵上 真一 | 学校法人 KBC 学園 | | (JNSA) |
| | 国際電子ビジネス専門学校 | 阿部 実洋 | 日本ヒューレット・パッカード(株) |
| 清水 秀一郎 | (株)コロプラ | 大森 健史 | 日本ヒューレット・パッカード(株) |
| 鈴木 啓紹 | (社)コンピュータソフトウェア協会(CSAJ) | 大村 友和 | (株)ネクストジェン |
| 野渡 志浩 | (株)サイバーエージェント | 金 明寛 | (株)ネクストジェン |
| 福森 大喜 | (株)サイバーディフェンス研究所 | 高橋 直人 | (株)ネクストジェン |
| 宮地 利雄 | (社)JPCERT コーディネーションセンター | 七條 麻衣子 | (公財)ハイパーネットワーク社会研究所 |
| | (JPCERT/CC) | 徳丸 浩 | HASH コンサルティング(株) |

| 氏名 | 所属 | 氏名 | 所属 |
|---|---|---|---|
| 渡辺 久晃 | パナソニック(株) | 神薗 雅紀 | PwC サイバーサービス合同会社 |
| 林 薫 | パロアルトネットワークス(株) | 星澤 裕二 | PwC サイバーサービス合同会社 |
| 岩佐 功 | 東日本電信電話(株) | 山室 太平 | (株)ベリサーブ |
| 水越 一郎 | 東日本電信電話(株) | 鈴木 暁 | (株)ベリサーブ |
| 太田 良典 | (株)ビジネス・アーキテクツ | 小河 哲之 | 三井物産セキュアディレクション(株) |
| 折田 彰 | (株)日立システムズ | 高江洲 勲 | 三井物産セキュアディレクション(株) |
| 丹京 真一 | (株)日立システムズ | 山谷 晶英 | 三井物産セキュアディレクション(株) |
| 本川 祐治 | (株)日立システムズ | 川口 修司 | (株)三菱総合研究所 |
| 寺田 真敏 | (株)日立製作所 | 村野 正泰 | (株)三菱総合研究所 |
| 藤原 将志 | (株)日立製作所 | 関根 鉄平 | (株)ユービーセキュア |
| 脇坂 隆則 | (株)日立ソリューションズ西日本 | 近田 昇平 | (株)ユービーセキュア |
| 古賀 洋一郎 | ビッグローブ(株) | 酒井 宏 | (株)ユビテック |
| 上村 理 | ファイア・アイ(株) | 志田 智 | (株)ユビテック |
| 山下 慶子 | ファイア・アイ(株) | 吉岡 克成 | 横浜国立大学 |
| 大高 利夫 | 藤沢市 | 福本 佳成 | 楽天(株) |
| 原 和宏 | 富士通(株) | 柳川 俊一 | (株)ラック |
| 原田 弘和 | 富士通(株) | 山崎 圭吾 | (株)ラック |
| 綿口 吉郎 | (株)富士通研究所 | 若居 和直 | (株)ラック |

著作・制作　独立行政法人情報処理推進機構（IPA）

編集責任　土屋　正

イラスト製作　株式会社　創樹

執筆協力者　10 大脅威選考会

10 大脅威執筆者　土屋 正　亀山 友彦　竹村 純輝
辻 宏郷　大道 晶平　菅原 尚志
岡崎 圭輔　山下 勇太　斉藤 良彰

IPA 執筆協力者　頓宮 裕貴　石川 勝一郎　金野 千里
桑名 利幸　加賀谷 伸一郎　岡下 博子
板橋 博之　野澤 裕一　黒谷 欣史

# 情報セキュリティ 10 大脅威 2016

## ～ 個人と組織で異なる脅威、立場ごとに適切な対応を ～

2016 年 3 月 31 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

https://www.ipa.go.jp/

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