情報セキュリティ

10大脅威 2017

～職場に迫る脅威！ 家庭に迫る脅威！？

急がば回れの心構えでセキュリティ対策を～

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

2017年5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 2017」
https://www.ipa.go.jp/security/vuln/10threats2017.html

目次

はじめに

本書「情報セキュリティ 10 大脅威 2017」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」の協力により、2016 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。昨年に引き続き、「個人」と「組織」という異なる立場で、それぞれの脅威を順位付けし、立場毎に 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】

- 情報セキュリティ対策の基本 スマートフォン編

昨今、スマートフォンが普及し、老若男女問わず利用されている。一方、セキュリティ対策は十分に行われているとはいえず、金銭を騙し取られる等の被害に遭うケースがある。10 大脅威 2015 にてパソコン（以降、PC と記載）利用者向けに情報セキュリティ対策の基本を解説したが、スマートフォンのセキュリティ対策も必須となってきている。

第 1 章では、スマートフォン向けの情報セキュリティ対策の基本について解説する。

- 情報セキュリティ 10 大脅威 2017（10 大脅威）

2016 年はランサムウェアによる被害が拡大している。ランサムウェアに感染すると、自分の PC だけではなく、組織内の別のサーバーのファイルも暗号化されるため、組織にとっては、警戒すべき脅威である。また、2016 年の後半には、設定が十分でない IoT 機器を狙い、IoT 機器をボット化し、DDoS 攻撃に悪用する、「Mirai」と呼ばれるウイルスが猛威を振るった。DDoS 攻撃によりサービスが停止する組織が多数確認された。

第 2 章では、2016 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

2016 年、ウイルスに感染した IoT 機器を踏み台とした大規模 DDoS 攻撃が発生し、セキュリティ設定・対策が不十分なままネットワークに接続された多数の IoT 機器の存在やセキュリティ対策の重要性を再認識することとなった。

インターネット通信における盗聴・改ざん・成りすましといった脅威の対策に用いられている暗号技術の一つ、ハッシュ関数が SHA-1 から SHA-2 へ世代交代の時期を迎えた。移行を怠ると、安全な通信を保証することが困難となる。

第 3 章では、これらの課題や脅威について解説する。

1章. 情報セキュリティ対策の基本
スマートフォン編

1 章 情報セキュリティ対策の基本 スマートフォン編

1999 年、世界初の携帯電話向けインターネット接続サービスの提供が日本で開始されると共に、電子メールやウェブサイト閲覧といった通話以外の目的での携帯電話の利用が始まり、その普及が加速した。2000 年代後半には、プログラミング可能な OS を搭載し、自分が使いたいアプリケーション（以下、アプリと記載）を自分で選びインストールしたり、自由に機能拡張やカスタマイズができたりするスマートフォンと呼ばれる新しい携帯電話が出現した。日本においては、2008 年の iPhone 国内販売開始を機に、スマートフォンの本格的な普及が始まった。2012 年に初心者及び高齢者層を主対象として操作性を容易化したスマートフォン、2013 年に年少者層向けに保護者が設定する制限機能を有するスマートフォンの発売も開始されたこと等により、現在の日本国内では、年少者層から高齢者層まで幅広く、多くの人がスマートフォンを利用している[1]。また、利用者の中には、PC と同等に活用している利用者もいる。

一方、スマートフォンが普及していく中で、不正アプリをインストールして電話帳データが漏えいしたり、ワンクリック請求に遭ったり等、スマートフォン利用者が被害に遭うケースも増えてきている。

このようなトラブルに巻き込まれる原因はいくつかあるが、例えば、以下の 4 つの考慮点を認識していないことが挙げられる。

- **セキュリティ対策の必要性**
- **スマートフォンの利用方法に応じたセキュリティ対策強化の必要性**
- **スマートフォン固有のセキュリティ対策の存在**
- **スマートフォンの OS や提供形態によって異なるセキュリティ方針**

【考慮点 1】セキュリティ対策の必要性

スマートフォンは、従来の携帯電話の機能に加えて、先進的な OS と高度な情報処理機能（PC と同等機能の一部）を取り込んだ携帯端末である。従来の携帯電話端末（通称、ガラケー、または、フィーチャーフォン）と比較して高度な情報処理機能を持つ反面、十分なセキュリティ対策を実施していないと、情報漏えい等の様々な脅威の被害に遭遇する恐れがある。携帯電話向けインターネット接続サービス機能を有する従来型の携帯電話とスマートフォンを比較した結果は以下の通りである。

- 通話機能
  - 従来型携帯電話と大きな違いはない。（LINE 等の通話アプリは、後述の「アプリのインストール・実行機能」の項目に従う）

- メール機能
  - メール本文に関しては従来型携帯電話と大きな違いはない。ウェブサイトの閲覧やアプリの

インストール・実行を促すリンクが埋め込まれていることがある。この場合、後述する「ウェブサイト閲覧機能」や「アプリのインストール・実行機能」に関するセキュリティ脅威を生じる恐れがある。

- ウェブサイトの閲覧機能
  - 従来型携帯電話では、主に携帯電話専用のブラウザ（コンパクトブラウザ）が実装されており、専用に用意されたサイトを閲覧していた。
  - スマートフォンでは、PC とほぼ同等の機能を有するブラウザ（フルブラウザ）が実装されており、PC と同じウェブサイトを閲覧することが可能となっている。このため、悪意のあるサイトや改ざんされたサイトへアクセスした場合、スマートフォンを攻撃対象とするウイルスに感染させられる等の被害に遭う恐れがある。

- アプリのインストール・実行機能
  - 従来型携帯電話では、端末の性能に制約があり、実行可能な機能にも制限が課せられていた。
  - スマートフォンでは、高機能・高性能のアプリを利用可能となっている。例えば、スマートフォン内部に保存されている利用者の様々なデータのみならず、スマートフォンが連携して動作するクラウドサービス上に保存された膨大なデータにアクセスすることも可能となっており、深刻な情報漏えいにつながる恐れがある。

- 更新用プログラムの提供方法
  - 従来型携帯電話では、安定利用する際に問題となる機能障害（通称：バグ）が検出された時に提供されることが多かった。
  - スマートフォンでは、これに加えて、セキュリティ上問題を生じ得る脆弱性が検出された時に脆弱性の解消のための更新用プログラムが提供されることがあり、速やかに適用すべき重要性が高まっている。また、機種によっては、OS の更新用プログラムが提供されて、機能が大幅に向上することがある。この場合、機能向上に伴う新たな脅威を生じることがあり、それに対応した対策が必要となることがある。

このように、従来型の携帯電話端末と比較して、スマートフォンはセキュリティ対策の必要性が大幅に増大しているが、一部の利用者はこの認識が不足しており、対策が不十分なままスマートフォンを使用している。

ポイント

・スマートフォンにはセキュリティ対策が必要である

【考慮点2】スマートフォンの利用方法に応じたセキュリティ対策強化の必要性

利用者によってスマートフォンの使い方が異なることが想定される。従来型携帯電話と同等の機能の範囲内で使用する利用者と、様々なアプリをインストールして PC と同等に活用している利用者では、セキュリティの脅威も大きく異なり、それに応じた対策が必要となる。ここでは、3 種類に分類した利用方法と留意点を示す。

表 1.1 スマートフォンの利用方法と留意点

脅威	利用方法	留意点
低	スマートフォンの電話機能や予めインストールされたアプリのみを使用し、アプリを追加インストールしない利用者	● 電話機能やメール機能を利用している間は問題ないが、ウェブサイト閲覧時にはワンクリック請求等の被害に遭う恐れがあるため従来型携帯電話以上の注意が必要。 ● マイナーアップデート（スマートフォン固有の不具合対策、セキュリティ対策等）が提供された場合、速やかに適用する。 ● メジャーアップデート（OS の機能追加等）が提供された場合、新バージョンにて提供される機能を必要としているか否か、旧バージョンのサポートが継続するか否か等をもとに、総合的に判断して適用を決定する。
中	公式マーケットや公式ストアで配布されているアプリをインストールして、スマートフォンの特徴的機能を積極的に使用している利用者	脅威「低」の留意点に加えて、 ● アプリの機能やアクセスする権限を十分に確認した上で行う。 ● アプリの更新用プログラムが提供された場合、内容を確認の上で適宜適用する。 ● セキュリティ対策アプリの導入を検討。
高	公式マーケットや公式ストア以外で配布されているアプリまでインストールして、PC とほぼ同等のレベルで使用している利用者（Android 搭載スマートフォン）	脅威「低」「中」の留意点に加えて、 ● 不正アプリをインストールする危険があるため、アプリのインストール・実行・更新には細心の注意を払う。

このように、スマートフォンの利用方法によって脅威レベルが異なるため、それに応じたセキュリティ対策が必要となるが、一部の利用者はそれに見合った対策を行わずスマートフォンを使用している。

ポイント

・利用方法に応じたセキュリティ対策が必要である

【考慮点3】スマートフォン固有のセキュリティ対策の存在

スマートフォン固有のサービス提供・利用形態やスマートフォン固有の機能に依り、PC のセキュリティ対策とは異なる対応が求められることがある。

スマートフォンは、インターネットを利用して提供されるサービスに関して、インターネットバンキング・オンラインショッピング・ナビゲーションサービス等、PC と同様のサービスを利用可能である。PC の場合、サービス提供者が用意したウェブサイトにアクセスし、サイト上の Web サービスを使用することによってサービスを利用している。一方、スマートフォンの場合、サービス提供者がスマートフォン専用アプリを開発・提供しており、利用者はこのアプリを介してサービスを利用していることが多い。このため、サービスのセキュリティは専用アプリの安全な利用に依るところが大きい。

また、スマートフォンは携帯電話通信事業者が提供する無線通信網を利用した通信機能や端末に搭載された GPS 機能を利用することによって、端末紛失・盗難時の遠隔ロック・データ消去や端末位置の検索が可能である等、スマートフォン故に可能なセキュリティ対策が存在する。

さらに、PC とは異なりスマートフォンは身に着けて持ち歩くことが多い。そのため、紛失、盗難、置き忘れ等が発生しやすく、他人に使用される潜在リスクも大きい。また、パスワードロック、指紋、顔認証等のセキュリティ対策も PC に比べて多用されている。

このように、スマートフォンのセキュリティを高めるためには、固有のセキュリティ対策を考慮・活用することが重要となる。

ポイント

・スマートフォンならではのセキュリティ対策もある

【考慮点4】スマートフォンの OS や提供形態によって異なるセキュリティ方針

日本で個人向けに販売されているスマートフォンは、主に二つに分けられる。一つは、Google 社が開発したオペレーティングシステム Android を組み込んで、各携帯電話端末メーカーにて開発された Android 搭載スマートフォン（以下、Android 端末と略す）である。もう一つは、Apple 社がオペレーティングシステム iOS および端末を開発している iPhone である。

さらに、Android 端末は、その提供形態によって、①携帯電話通信事業者を通じて販売されている端末（原則として SIM ロック（※1）がかかっているため、「SIM ロック版」と呼ばれることもある）、②携帯電話端末メーカーが直接販売している端末（SIM ロックがかかっていないため、「SIM フリー版」と呼ばれる）、③Google が開発した Android OS をカスタマイズせずにそのまま搭載した Android One 仕様の端末（販売経路によって「SIM ロック版」と「SIM フリー版」のいずれかに分かれる）の三種類がある。

スマートフォンは、**表 1.2** に示すように、搭載される OS や提供形態によって、セキュリティ方針（OS の更新用プログラムの提供者、アプリやその更新用プログラムの配布場所、審査方法等）が異なっており、それぞれの方針の違いを考慮したセキュリティ対策が必要となる。

表 1.2 OS や提供形態によるスマートフォンの違い

<table>
<tr><th rowspan="2"></th><th colspan="3">Android 端末</th><th colspan="2">iPhone</th></tr>
<tr><th>SIM
ロック版</th><th>SIM
フリー版</th><th>Android One</th><th>SIM
ロック版</th><th>SIM
フリー版</th></tr>
<tr><td>OS 開発元</td><td colspan="2">Google 製 Android を
端末メーカーでカスタマイズ</td><td>Google</td><td colspan="2" rowspan="2">Apple</td></tr>
<tr><td>OS の
更新用プログラム
の提供者</td><td>携帯電話
通信事業者</td><td>端末メーカー</td><td>販売経路
に依存</td></tr>
<tr><td>アプリや
その更新用プログラム
の配布場所、
審査方法</td><td colspan="3">・Google Play（Google）
比較的緩やかな審査
・各携帯電話通信事業者の公式マーケット
Google Play の審査に加え、各携帯電話通信事業者の観点で選定
・その他の配布場所
配布場所に依存</td><td colspan="2">・App Store（Apple）
厳格な審査</td></tr>
</table>

ポイント

・OS や提供形態によって、セキュリティ対策が異なる場合もある

また、スマートフォンでは、更新の目的（内容）によって、更新の種類が大きく二つある。一つが機能・操作性の大幅な向上を目的とするもの、もう一つが機能・操作性のマイナーな向上、動作安定性の向上、セキュリティ機能の改善を目的とするものである。OS や機種等の違いにより、それぞれの呼び方や更新方法が異なる可能性があるため、機種毎のマニュアル等を参考にしてほしい。なお、本書では、前者を「メジャーアップデート」、後者を「マイナーアップデート」として記載する。

スマートフォンの利用者は、上記、考慮点を理解した上で、適切なスマートフォンのセキュリティ対策が求められる。そこで、本章では、スマートフォンを利用していく上で必要な情報セキュリティ対策について解説する。**表 1.3** はスマートフォンの情報セキュリティ対策の 8 つの基本をまとめたものである。詳細については、次ページ以降で解説する。

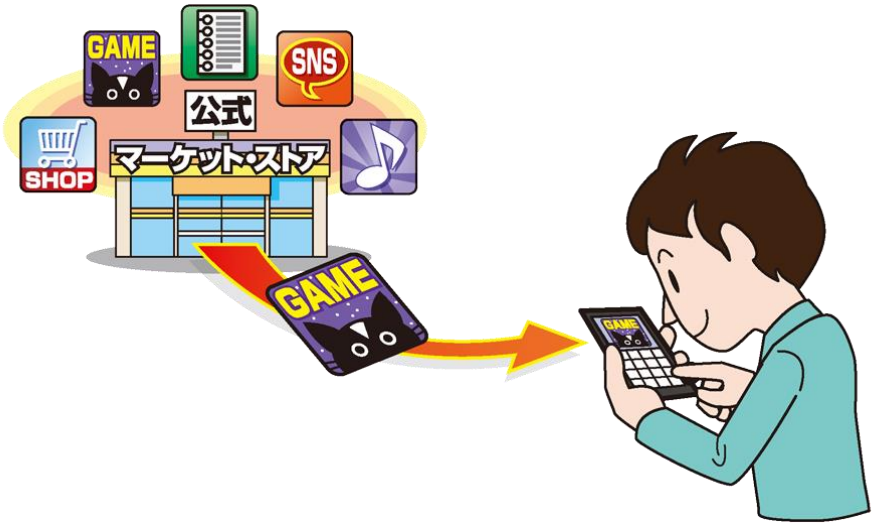
表 1.3 スマートフォンの情報セキュリティ対策の基本

攻撃の手口	情報セキュリティ対策の基本	解説
不正アプリ	信頼できるサイトからインストール	1.1 節
	アプリに許可する権限の確認	1.2 節
誘導（罠にはめる）	脅威や手口を知る	1.3 節
盗難・紛失	認証の強化・データの暗号化・バックアップ	1.4 節
盗聴	公衆無線 LAN の利用はリスクを理解	1.5 節
不正ログイン	パスワードを使い回さない	1.6 節
OS・アプリの脆弱性	OS・アプリの更新	1.7 節
ウイルス感染	セキュリティソフトの導入	1.8 節

※1　スマートフォンや携帯電話には、電話番号を特定するための固有の ID 番号が記録された IC カード（SIM カード）が入っている。携帯電話通信事業者から購入した端末は、通常、その事業者から提供された SIM カードしか使用できないようにロックされている。

2015 年 5 月以降に販売が開始された機種では、携帯電話通信事業者は必要な手続きを行った後、SIM ロック解除が義務付けられている。SIM ロック解除後は、任意の SIM カードを利用可能となるが、OS の更新プログラム提供者は SIM ロックされていた状態から変更されることはない。即ち、Android の場合、OS の更新プログラム提供者は、携帯電話通信事業者のままである。

1.1. 信頼できるサイトからインストール



スマートフォンはアプリを自由にインストールして様々な機能を利用することができる。一方、アプリの中には故意にウイルス機能を組み込んだ不正アプリ、またはウイルス機能を含んだツールキットで開発された不正アプリ等も存在しており、気づかずインストールしてしまうと、ウイルスに感染し、個人情報の窃取等をされる恐れがある。このようなアプリをインストールしないために、極力、アプリは公式マーケットや公式ストア（以降、公式マーケットと記載）からインストールすることが望ましい

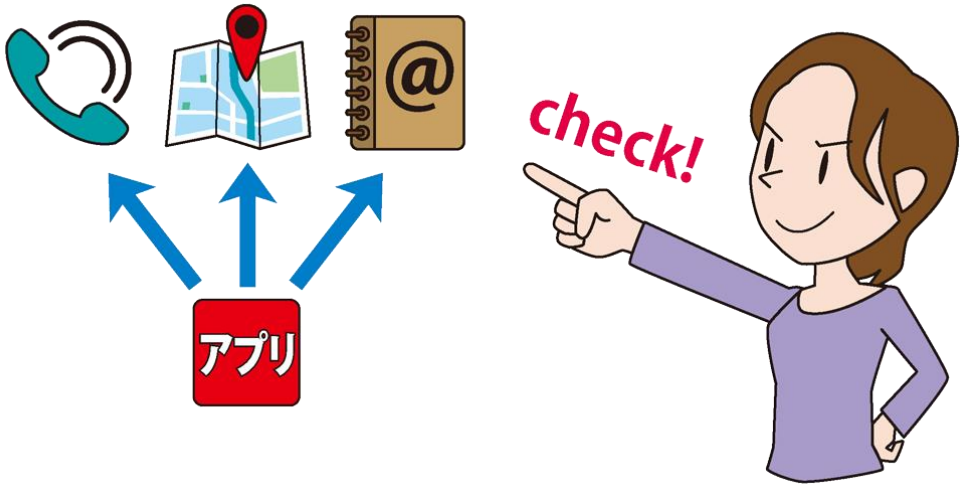
◆　アプリの入手は公式マーケットから

公式マーケットには、例えば OS 提供元が運営するもの（Google Play、App Store）や携帯電話通信事業者が運営するもの（d マーケット、au Market、ソフトバンク ピックアップ）等がある。公式マーケットではアプリの登録時に審査を行っているため、不正アプリが登録・公開されにくくなっている。公式マーケットを利用することで、比較的安全にアプリを入手できる。なお、厳格な審査が行われている iPhone 用の App Store や各携帯電話通信事業者の観点でアプリが選定されている携帯電話通信事業者が運営する Android 端末用のマーケットはより安全である。

◆　信頼できるサイト以外からのインストールは注意【Android 端末】

iPhone 用アプリとは異なり、Android 端末用アプリには公式マーケット以外にもサードパーティーのマーケットや個人のウェブサイトに公開されているものがある。ウェブサイトへのアプリ登録には公式マーケットのような審査が必須ではないため、利用者にとっては、様々なアプリを利用できるというメリットがある反面、不正アプリが混入するリスクは高いというデメリットがあることを認識する必要がある。このため、公式マーケット以外からのアプリの入手は避けることが望ましい。どうしても必要なアプリは、アプリ公開者の信頼性やアプリの評判等を十分に確認し、安全であると判断できた場合に入手し、判断できない場合はインストールしないことが望ましい。

1.2. アプリに許可する権限の確認



不正アプリをインストールしないために、1.1 節で解説した対策に加え、アプリを利用するときは、たとえ公式マーケット等の信頼できるサイトからダウンロードしたアプリでも、アプリインストール時に必要以上なアクセス権限を要求しないか、利用者側で注意する必要がある。インストールしたアプリに期待している機能を越えるアクセス権限を許可した場合、情報の窃取等の被害に遭う恐れがある。

◆　アプリ起動時のアクセス権限の確認

iPhone や Android 端末（バージョン 6.0 以降）では、アプリをインストール後、アクセス許可がされていない機能にアプリがアクセスする場合、アクセス権限確認画面が表示される。確認画面に表示されるアクセス権限が、そのアプリの利用目的を超えるアクセス権限を要求している場合は、注意が必要である（例えば、電卓のアプリで、電話帳にアクセスする等）。利用目的を超えるアクセス権限を許可してアプリを起動してしまうとスマートフォン内の情報を窃取される恐れがある。アプリを起動する際にはアクセス権限を確認し、怪しい場合はアクセス権限を不許可にすべきである。なお、後から機能拡張によりアクセス権限が追加される可能性があるため、その際も注意する。

また、既にアクセス権限を許可してしまった場合は、インストールされているアプリの管理画面からアクセス権限を変更することができる。

なお、インストールしているアプリがどの機能へのアクセス権限を持っているかを一度確認することが望ましい。権限の確認とあわせて、使っていないアプリがあれば削除してもよい。

◆　インストール時に表示される場合も【Android 端末】

古いバージョンの Android 端末（バージョン 6.0 未満）の場合、インストール時にアクセス権限が確認される。インストール時も同様に許可するアクセス権限は注意して確認する必要がある。

◆　アプリ連携時のアクセス権限の確認も

Twitter 等の一部のアプリは、他のアプリと連携する機能を持っている。アプリ連携時に利用目的を超える権限を要求している場合は注意が必要である。連携して問題ないかを確認し、怪しい場合はアクセス権限を不許可にすべきである。なお、後から連携を解除することも可能なため、既に連携してしまった場合は解除する。

1.3. 脅威や手口を知る

スマートフォンの利用者をターゲットにした詐欺行為による被害が確認されている。詐欺の方法はスマートフォンの特性を利用した巧妙な手口が使われており、突然被害に遭うと、焦ってしまい適切な対応が取れないケースがある。予め脅威や手口を把握しておくことで、適切な対応を取り、被害を予防できる。

◆ **スマートフォンの機能特性を悪用** [II]

スマートフォンのカメラや電話の機能等を悪用して、詐欺に引っ掛けようとする。例えば、カメラのシャッター音を BGM で鳴らして、あたかもカメラで撮影されたかのように見せかける場合や、電話を強制的に掛けさせようとする場合がある。

◆ **スマートフォンでもワンクリック請求**

PC 同様ワンクリック請求が確認されている。ウェブサイトやメールのリンクをタップすると突然「入会しました」といった画面が表示され、不当に料金を請求される。

◆ **性的な欲求を悪用した手口** [III]

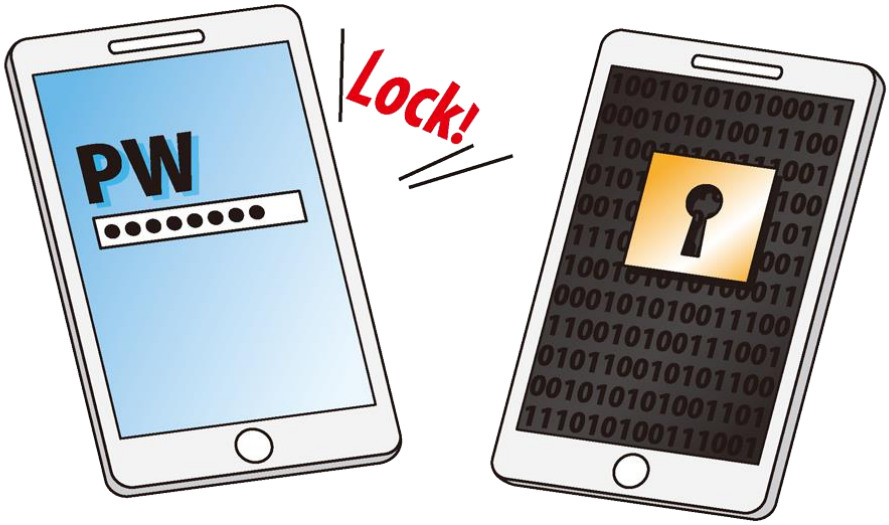
性的な欲求を悪用した脅迫（セクストーション）が確認されている。これは、まずは SNS 等で知り合ったことをきっかけに、言葉巧みにプライベートな写真をやり取りしようと持ちかけたり、個人情報を抜き取る不正アプリをインストールさせたりする。うっかり、プライベートな写真を送ってしまったり、不正アプリをインストールして情報が窃取されたりすると、その情報を元に脅迫が行われる。プライベートな写真の場合、他人に知られたくない情報であるため、誰にも相談できず、やむをえず脅迫に応じてしまう。

◆ **自発的な情報収集を**

報道やセキュリティ関連機関の注意喚起等の情報源から、セキュリティに関する脅威や犯罪の手口を知ることができる。IPA が公開している「安心相談窓口だより」[IV] や、官公庁やセキュリティ企業が公表しているレポートが参考になる。定期的に情報を収集し、被害に遭わないように備えておくことが有効である。なお、手口を知らない人もいるため、家族や知人、同僚等で情報共有を行うことも重要である。

また、被害に遭ってしまっても焦らず、早めに IPA[V] (技術面の相談)、消費者庁 [VI] (契約に関する相談)、警察庁 [VII] [VIII] (犯罪行為の取り締まり)等の支援機関に相談することをお奨めする。

1.4. 認証の強化・データ暗号化・バックアップ



スマートフォン内には様々な情報が保存されている。知り合いの氏名や電話番号等の個人情報も含まれる。一方、スマートフォンは手軽に持ち運べる半面、紛失や盗難等の被害に遭う恐れがある。万が一、紛失や盗難に遭った場合に備え、認証強化等の対策を行っておく必要がある。

◆　スマートフォンは個人情報の塊

スマートフォン内には、様々な個人情報が保存されている。家族・友人・知人の氏名や電話番号、メールアドレス、さらには、顔写真等 PC 内に保存されている情報と比べて自分以外の情報が登録されている可能性が高い。紛失や盗難により、その情報が第三者に渡ってしまう恐れがある。

◆　スマートフォン利用時の認証強化

スマートフォンは、利用する前に認証を求める機能を持っている。事前に登録した PIN コードや指を動かしたパターン、指紋等で認証し、正しい場合、ホーム画面が表示され、自由に操作できるようになる。認証強化により、紛失や盗難に遭った際に、すぐに情報を悪用されるといった被害を回避することができる。

◆　データの暗号化を忘れずに

スマートフォンには、保存しているデータを暗号化する機能がある。暗号化しておくと、スマートフォンを分解して直接解析されても、意味のある情報として取得できないため、紛失や盗難時のリスクを低減できる。ただし、スマートフォンのデータの保存先として外部 SD カードを利用している場合は注意が必要である。SD カードの暗号化はサポートされていないケースがあるため、個人情報等を保存する場合は、スマートフォンに内蔵されているストレージを利用すると良い。

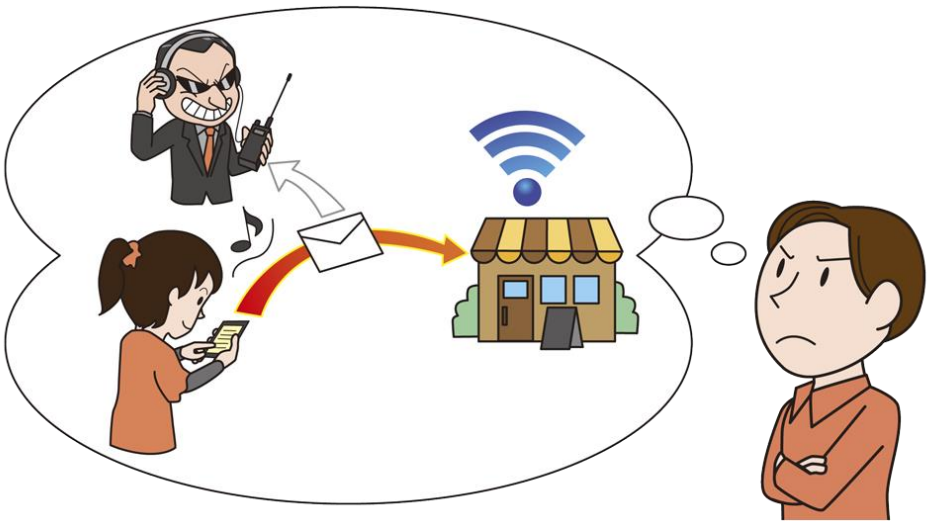
◆　万が一の場合は、遠隔ロック等の活用

携帯電話通信事業者や OS 開発元より GPS 機能を使ったスマートフォンの遠隔ロック・データ消去・探索を行うサービスが提供されている。紛失や盗難に遭った場合は、それらのサービスを利用することで不正操作を防いだり、紛失したスマートフォンを探したりすることができる。

◆　念のためのバックアップ

事前に重要なデータのバックアップをクラウド等に取得しておくことで、データだけでも復旧できる。また、ウイルスへの感染等によるデータ破壊への対策にもなる。

1.5. 公衆無線 LAN の利用はリスクを理解



無料で使える公衆無線 LAN がコンビニや飲食店等、様々なところに設置されている。スマートフォンは契約によって月のデータ通信量に何らかの制限があるため、通信量を気にしている利用者にとって公衆無線 LAN は非常に便利である。一方、公衆無線 LAN は盗聴のリスクがあり、通信に含まれる機微な情報が窃取される恐れがある。利用者は公衆無線 LAN のリスクを認識しておく必要がある。

◆ **公衆無線 LAN は盗聴のリスクがある**

公衆無線 LAN を利用している際に、盗聴されると通信内容が窃取される恐れがある[IX]。

◆ **通信を暗号化する仕組みを活用**

ウェブサービス自身の暗号化の仕組み（HTTPS 等）を使っての通信や VPN（通信を暗号化する仕組み）を使っての通信は、盗聴の危険性は低い。そのため、そのような通信の仕組みを活用することは有効である。ただし、同じ暗号化の仕組みでも無線 LAN 自身が提供するアクセスポイントとスマートフォン間の暗号化通信には注意が必要である。暗号化されているため、一見安全に見えるが、接続用の ID（SSID）や暗号化キーは公開されており、解読される恐れがある。

◆ **アプリの通信の仕組みに注意**

公衆無線 LAN で、アプリを利用している場合も注意が必要である。アプリが外部と通信する際に、暗号化しているかどうかはアプリの仕様に依存する。暗号化されていない場合、アプリ利用中の通信が盗聴される恐れがある。暗号化の有無については見た目ではわからないため、不安な場合は公衆無線 LAN ではアプリを使用しないか、あるいは、開発元に暗号化の有無を確認する。

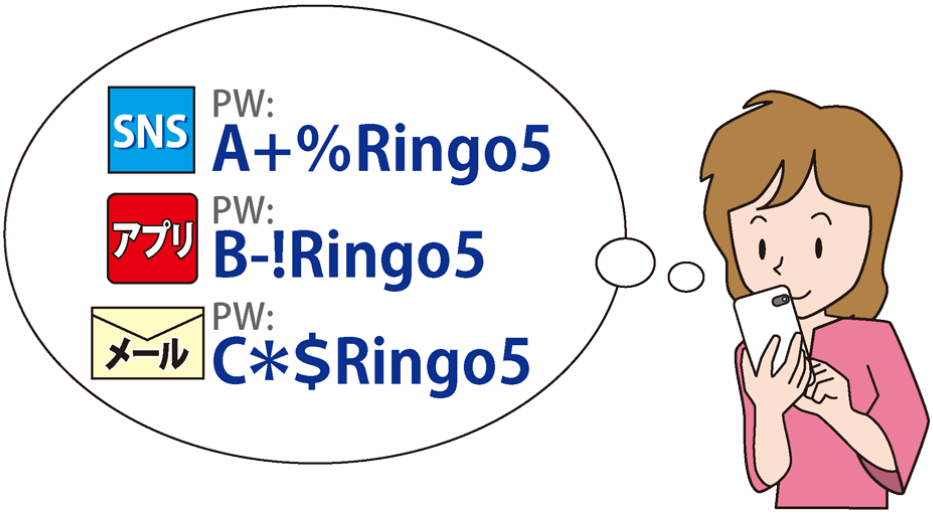
◆ **悪意のあるアクセスポイントに注意**

公開されている公式な公衆無線 LAN を装って、悪意あるアクセスポイントが設置されている恐れがある。SSID や暗号化キーを同じものにすることで、利用者に公式な公衆無線 LAN だと勘違いさせる。また、過去に一度接続したことがある無線 LAN と同じ SSID、暗号化キーであった場合、その情報を保存していると、自動的に接続される。知らずに接続すると盗聴される恐れがある。

◆ **通信する情報を限定**

公衆無線 LAN は盗聴の危険性があるため利用する場合は第三者に知られて困る情報を入力したり表示したりしないようにする。

1.6. パスワードを使い回さない



スマートフォンでは、オンラインショッピングで買い物したり、Twitter 等の SNS サービスやアプリを利用し、情報の発信を行ったりすることができる。サービスを利用する場合、ログインを行う必要があるが、各サービスでパスワードを使い回している場合、一つのパスワードが漏えいするだけで複数のサービスに不正ログインされてしまう恐れがある。複数のサービスを利用する場合、パスワードを使い回さないようにすることが重要である。

◆ パスワードは使い回さない

複数のオンラインサービスを利用していると利便性の観点から、同じパスワードを使い回してしまう場合がある。使い回していると一つのサービスでパスワードが漏えいした場合、そのパスワードを悪用して他のサービスに不正ログインされてしまう恐れがある。サービス毎に別のパスワードを利用することで不正ログインを回避することができる。

◆ 推測されやすいパスワードは使わない

推測されやすいパスワードを設定していると、パスワードを推測され、不正にログインされてしまう恐れがある。例えば、ID とパスワードが同一、パスワードに単純な単語や、「123456」や「abcdef」のような連続した英数字は使わない。

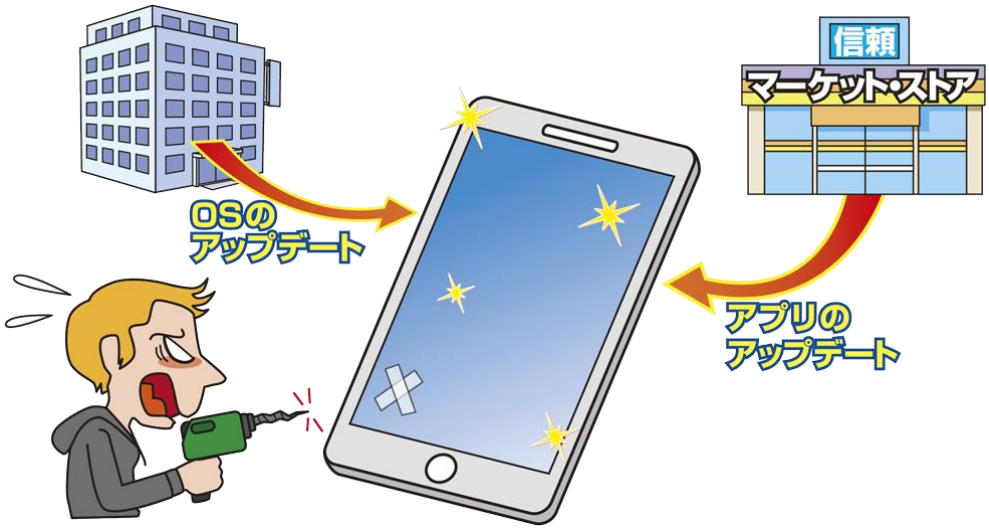
◆ ちょっとした工夫でパスワード管理

複数のパスワードを使い分けると管理が難しく、忘れてしまうこともある。パスワードの管理方法として例えば、覚えやすいコアパスワードを 1 つ決めて、サービス毎に異なるキーワードをコアパスワードの前または後ろにつける、といった方法がある [X]。コアパスワードは暗記し、サービス毎のキーワードは紙や電子ファイルで保存する。これにより、複数パスワードが容易に、かつ、安全に管理できる。

◆ 多要素認証の活用

サービスによってはワンタイムパスワードを発行して、ID、パスワードに加えてワンタイムパスワードを入力して認証する機能が提供されている。本機能を有効にしておくことで万が一パスワードが漏えいしても実被害を回避できる。

1.7. OS･アプリの更新



PC 同様、スマートフォンの OS やアプリにはセキュリティ上の欠陥である脆弱性が発見されることがある。脆弱性が存在するスマートフォンは悪意ある攻撃者にコントロールされるリスクがあることを認識すべきである。脆弱性を悪用され、情報窃取等の被害に遭わないために、更新用プログラムが提供されたらスマートフォンの OS（OS の一部として提供されるアプリを含む）を更新（マイナーアップデート･メジャーアップデート）することが基本である。また、個別にインストールしているサードパーティー製アプリも同様に更新する。

◆ 速やかなマイナーアップデートを実施

スマートフォンの OS の脆弱性を解決する更新プログラムが提供されたら、速やかにマイナーアップデートを実施する。脆弱性を悪用され、ウイルスに感染した場合、スマートフォン内の情報の窃取や盗聴等をされる恐れがある。マイナーアップデートには、脆弱性対策以外にも機能･操作性の向上や動作安定性の向上等も含まれる場合もあるため、可能な限り行うことが望ましい。

ただし、Android 端末の場合、更新プログラムの提供は、利用しているスマートフォンの種類や SIM の利用方法（ロックまたはフリー）によって提供者が異なる（上述の**表 1.2** を参照）。同じバージョンの OS でも提供されるタイミングが異なる場合があるため注意が必要である。

◆ 更新用プログラムが提供されない場合も

端末メーカーや通信事業者から更新用プログラムが提供されない場合がある。[xi] また、明確なサポートライフサイクルが提示されておらず、利用者が気づきづらい現状がある。セキュリティに関するアップデートを提供されない古い機種は、新しい機種への移行を検討することが望ましい。

◆ メジャーアップデートは慎重に

メジャーアップデートにより、機能や操作性が大幅に向上される。しかし、メジャーアップデート後にアプリが正常に動作しなくなる場合もある。また、端末設定の一部または全てが初期化される。メジャーアップデートは利用者の責任で実施するものであるため、予め更新内容をよく確認して、慎重に更新する必要がある。

◆　**アプリは自動更新を有効にして更新**

個別にインストールしているサードパーティー製アプリも同様に更新プログラムが提供されたら、速やかに更新する。スマートフォンにはアプリの自動更新機能があるため、その機能を有効にしておくことで、自動的にアプリが最新のバージョンとなり、より安全に利用することができる。なお、自動更新時にモバイルのデータ通信を使う場合があるため、データ通信量を気にする場合は適宜 Wi-Fi 環境で更新する。

◆　**更新する前に十分な充電とストレージの容量確保**

更新をする前には十分な充電とストレージの容量を確保しておく必要がある。更新中に電源が切れたり、ストレージの容量が不足したりすると更新が正常に終了できず、端末を起動できない等の別のトラブルにつながる恐れがある。特に OS のマイナーアップデートやメジャーアップデートでは、アプリの更新とは違い、更新プログラムの容量が大きい場合があり、注意が必要である。

◆　**安定したネットワーク環境の確保**

更新は安定したネットワーク環境で行う必要がある。車や電車で移動中のトンネルや、ビルの地下など、不安的な通信環境ではアップデート中に回線が途切れ、正常に完了出来ないケースもある。

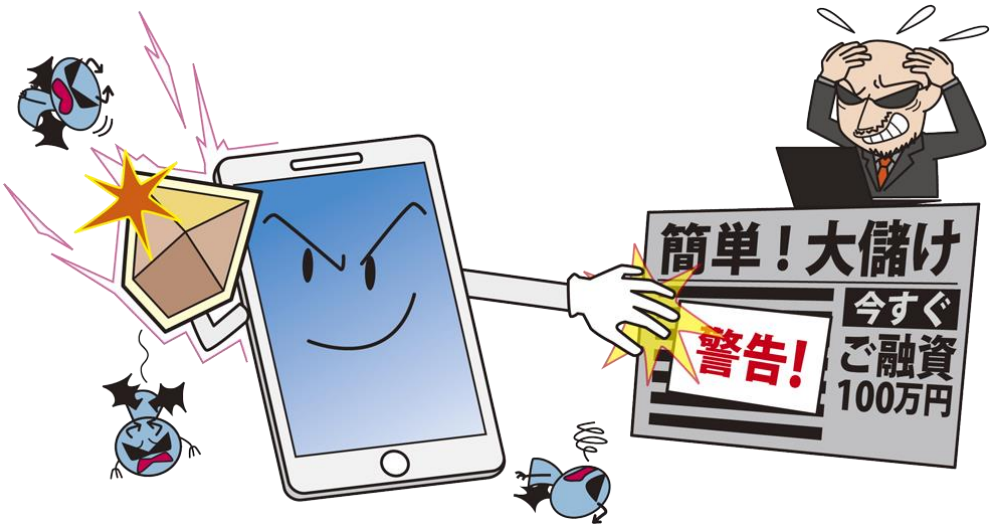
◆　**念のためのバックアップ**

更新に失敗しても復旧できるように、事前にデータのバックアップを取っておくと良い。特に OS のメジャーアップデートの場合、スマートフォンへの影響が大きいため、事前にバックアップをしておくことが望ましい。

◆　**最新 OS へのアプリのサポート状況確認**

OS を更新することで、アプリが動作しなくなる場合がある。どうしても使う必要があるアプリの場合は、インストールしているアプリが最新の OS に対応しているかをアプリのサイト等で確認する。

1.8. セキュリティソフトの導入



不正アプリのインストール等により、ウイルスに感染する恐れがある。ウイルスによる被害に遭わないために、予めセキュリティソフトを導入しておくと有効である。また、セキュリティソフトには詐欺行為等を行う不正サイトへのアクセスを抑止する機能があるため、より安全にウェブサイトを閲覧できる。

◆ **セキュリティソフトの導入【Android 端末】**

便利なアプリや有名なアプリに見せかけて不正アプリをインストールさせ、ウイルスに感染させられる恐れがある。ウイルスに感染するとスマートフォン内の個人情報が窃取されたり、スマートフォン自身を遠隔操作されたりする恐れがある。Android 端末を利用している場合は、ウイルスへの感染を防ぐために、セキュリティソフトを導入しておくと良い。なお、ウイルス検知精度や機能面で優れる有料のセキュリティソフトを使うのが望ましいが、無料のセキュリティソフトを使うという選択肢もある。ただし、偽のセキュリティソフトも公式マーケットに公開されている場合があるため、インストール時はアプリの信頼性を確認する必要がある。

◆ **不正サイトへのアクセスを抑止**

セキュリティソフトには不正サイトへのアクセスを抑止する機能もあるため、安全にウェブサイトを閲覧することができる。そのため、iPhone を利用している場合も、セキュリティソフトをインストールすることで安全に利用できる。

◆ **携帯電話通信事業者からセキュリティ対策サービスが提供されている場合も**

携帯電話通信事業者では、ウイルスチェック等のセキュリティ対策の機能を持つサービスを有償で提供している場合がある。各携帯電話通信事業者の窓口で手軽に相談でき、導入も容易なため、携帯電話通信事業者のサービスを利用することも対策の選択肢として挙げられる。

◆ **セキュリティソフトの限界**

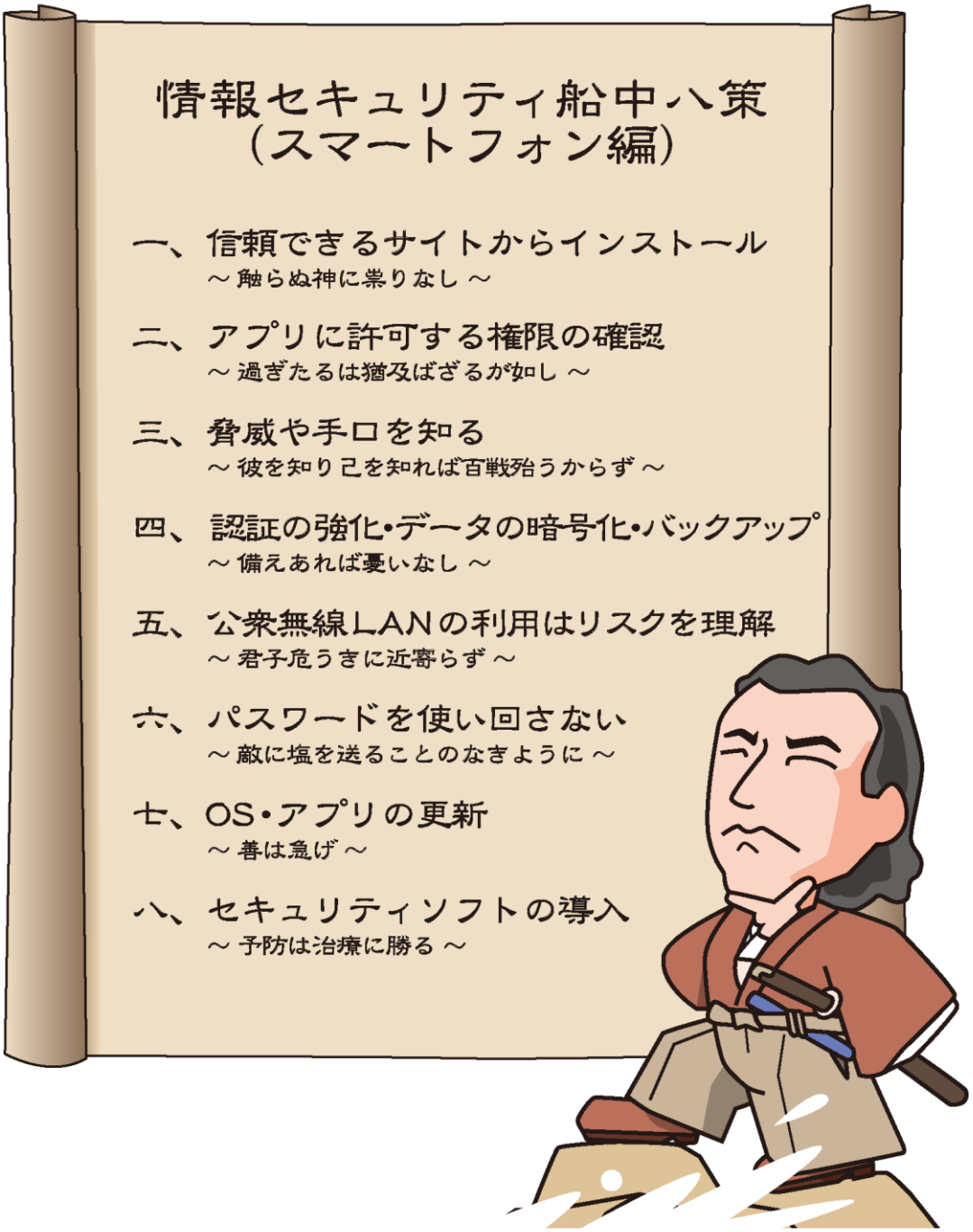
セキュリティソフトを導入したからといって100%ウイルスに感染しないわけではない。例えば、最近作成されたウイルスの場合、セキュリティソフトで検知の対象に入っておらず、ウイルスとして検知できない恐れがある。スマートフォンの利用者は、セキュリティソフトを導入しているから安全だと油断せず、怪しいアプリはインストールしない等、日頃からの注意が必要である。

1章.情報セキュリティ対策の基本　スマートフォン編：参考資料

I. 平成27年通信利用動向調査の結果
http://www.soumu.go.jp/johotsusintokei/statistics/data/160722_1.pdf
II. 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
https://www.ipa.go.jp/security/txt/2015/04outline.html
III. iPhoneユーザを狙った不正アプリによるセクストーション被害が発生
https://www.ipa.go.jp/security/anshin/mgdayori20161110.html
IV. 安心相談窓口だより
https://www.ipa.go.jp/security/anshin/mgdayoriindex.html
V. 情報セキュリティ安心相談窓口
https://www.ipa.go.jp/security/anshin/
VI. 全国の消費生活センター等
http://www.kokusen.go.jp/map/index.html
VII. 申請・届出等
http://www.npa.go.jp/policies/application/index.html
VIII. 都道府県警察本部のサイバー犯罪相談窓口等一覧
http://www.npa.go.jp/cyber/soudan.htm
XI. IPAテクニカルウォッチ「公衆無線LAN利用に係る脅威と対策」
https://www.ipa.go.jp/security/technicalwatch/201600330.html
X. 不正ログイン被害の原因となるパスワードの使い回しはNG
https://www.ipa.go.jp/security/anshin/mgdayori20160803.html
XI. Android端末の約半数、2016年中に更新されず
http://www.itmedia.co.jp/enterprise/articles/1703/24/news059.html

付録:情報セキュリティ船中八策

江戸時代に坂本龍馬がまとめたと言われる「船中八策」にあやかり、1 章で解説した情報セキュリティの基本的な対策の 8 つに解説的にことわざや故事を併記した「情報セキュリティ船中八策 スマートフォン編」を以下に示す。



2章. 情報セキュリティ10 大脅威 2017

2 章　情報セキュリティ 10 大脅威　2017

2016 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、「情報セキュリティ 10 大脅威 2017」では、「個人」と「組織」向けの脅威として、それぞれ**表 2.1** の通り順位付けした。

本章では、「個人」と「組織」向けの脅威で 1 位～10 位となった脅威を「情報セキュリティ 10 大脅威 2017」として、「個人」向けの脅威は 2.1 節、「組織」向けの脅威は 2.2 節で解説する。

表 2.1 情報セキュリティ 10 大脅威 2017 「個人」および「組織」向けの脅威の順位

「個人」向け脅威	順位	「組織」向け脅威
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	1	標的型攻撃による情報流出
ランサムウェアによる被害	2	ランサムウェアによる被害
スマートフォンやスマートフォンアプリを 狙った攻撃	3	ウェブサービスからの個人情報の窃取
ウェブサービスへの不正ログイン	4	サービス妨害攻撃によるサービスの停止
ワンクリック請求等の不当請求	5	内部不正による情報漏えいと それに伴う業務停止
ウェブサービスからの個人情報の窃取	6	ウェブサイトの改ざん
ネット上の誹謗・中傷	7	ウェブサービスへの不正ログイン
情報モラル欠如に伴う犯罪の低年齢化	8	IoT 機器の脆弱性の顕在化
インターネット上のサービスを悪用した攻撃	9	攻撃のビジネス化 （アンダーグラウンドサービス）
IoT 機器の不適切な管理	10	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

本章で共通的に使われる用語について**表 2.2** に定義を記載する。

表 2.2 情報セキュリティ 10 大脅威 2017 用語定義

用語	意味
個人	家庭等でスマートフォンや PC を利用する人
組織	企業、政府機関、公共団体等の組織およびその組織に所属している人
犯罪グループ	金銭や主義主張（ハクティビズム）を目的とした攻撃（犯罪）者集団
犯罪者	金銭や情報窃取（ストーカー行為を含む）を目的とした攻撃（犯罪）者
諜報員、産業スパイ	機密情報窃取を目的とした攻撃（犯罪）集団 国家組織の支援を受けた攻撃（犯罪）集団
IoT	モノのインターネット（Internet of Things）。ネットワークカメラや情報家電、医療機器といった様々な機器がインターネットにつながり、通信を行う仕組み。機器自体を指す場合は、IoT 機器と呼ぶ。
CSIRT	セキュリティインシデント等の問題が発生した際に原因究明や影響範囲の調査等を行う組織。自組織に関する問題に対応する場合は、自組織 CSIRT と呼ぶ。

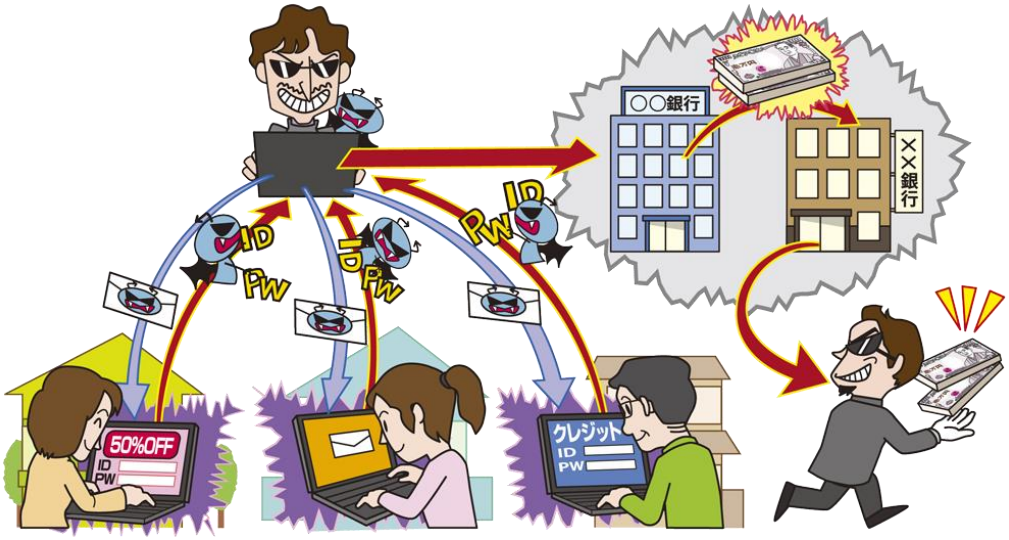
このページは空白です。

2.1. 情報セキュリティ10大脅威（個人）

組織 10 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

～攻撃件数および被害額は減少しているが、引き続き警戒が必要～



ウイルス感染やフィッシング詐欺により、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が攻撃者に窃取され、正規の利用者になりすまし、不正送金や不正利用が行われた。2016 年は 2015 年と比べインターネットバンキングの被害件数が減少し、さらに、個人口座の被害額も減少している。被害は減少傾向になってはいるが、個人口座の被害額は引き続き大きいため、個人のインターネットバンキングやクレジットカード利用者においては警戒が必要である。

＜攻撃者＞

- 犯罪グループ

＜被害者＞

- 個人（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）

＜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く中、これらの利用者の情報を窃取し不正利用することを目的とした攻撃が引き続き行われている。ウイルス感染やフィッシング詐欺等により窃取した利用者の情報を攻撃者が不正利用することで、正規の利用者に金銭的な被害が生じる。

2016 年は、請求書や宅配の伝票等を装った巧妙な日本語で書かれたメールにファイルを添付し、ファイルを開かせることでウイルスに感染させる攻撃が数多く確認された。

＜攻撃手口＞

◆ ウイルス感染

利用者が、攻撃者が用意した悪意あるウェブサイトにアクセスしたり、メールに添付されている悪意あるファイルを開いたりすることで、利用者の端末にウイルスを感染させる手口。利用者がウイルスに感染した端末でインターネットバンキングにログインしたり、クレジットカード情報を入力したりすると入力した情報を攻撃者に窃取される。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利用者の口座から

別の口座への不正送金や、利用者クレジットカードの不正利用等を行う。

◆ **フィッシング詐欺**

攻撃者が実在する銀行やクレジットカード会社等を装い、悪意あるウェブサイトの URL を含むメールを利用者に送り、利用者を当該ウェブサイトへアクセスさせ、不正にログイン情報等を窃取する手口。利用者が正規ウェブサイトであると信用して、ログイン情報やクレジットカード情報等を入力すると、その情報を攻撃者に窃取される。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利用者の口座から別の口座への不正送金や、利用者クレジットカードの不正利用等を行う。

＜事例と傾向＞

◆ **不正送金被害は減少傾向**

警察庁によると、2016 年中に発生したインターネットバンキングの不正送金事件は 1,291 件あり、2015 年と比べて 204 件減少している。また、被害額を同様に比較すると、全体では約 16 億 8,700 万円で、約 13 億 8,600 万円の減少となっている。さらに、個人口座の被害額は約 12 億 5,200 万円で、約 3 億 5,500 万円の減少となっている。[I]

◆ **巧妙な日本語で記載されたメールによるウイルスの拡散**

2016 年はウイルス拡散の手法としてメールによる攻撃が活発化した。例えば、1 回の攻撃で400通以上のウイルスを含むメールを送信する攻撃が 2016 年 11 月までに 33 回あったことが確認されている。なお、2015 年には 400 通以上の攻撃が 1 回も発生していなかった。[II]

＜対策/対応＞

個人（利用者）

- 情報リテラシーの向上
  - ・受信メール、ウェブサイトの十分な確認
  - ・添付ファイルやリンクを安易にクリックしない
  - ・怪しい（普段出ない）ポップアップが表示されたら個人情報等は入力しない
  - ・事例・手口の情報収集

  実在する組織からのメールだからと、安易に信用しないことが重要である。また、多くの金融機関やクレジットカード会社のホームページでは、犯罪手口の説明やセキュリティ対策の提供を行っているのでそれらを参考にする。[III]
- 被害の予防
  - ・OS・ソフトウェアの更新
  - ・セキュリティソフトの導入
  - ・多要素認証等、銀行が推奨する認証方式の利用

    トランザクション認証と組み合わせることでより安全に利用できる。
  - ・ファイルの拡張子を表示させる設定
- 被害の早期検知
  - ・不審なログイン履歴の確認
  - ・自身の口座やクレジットカードの利用履歴を確認する習慣をつける

参考資料

I. 平成28年中におけるサイバー空間をめぐる脅威の情勢等について
http://www.npa.go.jp/kanbou/cybersecurity/H28cyber_jousei.pdf
II. 2016年個人の三大脅威：ネットバンキングを狙う「オンライン銀行詐欺ツール」
http://blog.trendmicro.co.jp/archives/14247
III. フィッシング対策の心得
https://www.antiphishing.jp/consumer/attention.html

組織 2 位

2位 ランサムウェアによる被害

～ランサムウェアによる被害が急増～

ランサムウェアとは、PC やスマートフォンにあるファイルの暗号化や画面のロックを行い、復旧させることと引き換えに金銭を要求する手口に使われるウイルスである。2016 年は前年と比べるとランサムウェアの検知数が増大している。感染した端末だけではなく、共有サーバーや外付け HDD に保存されているファイルも暗号化されるため、ソフトウェアの更新等の感染を予防する対策に加え、定期的にファイルのバックアップを取得し、PC やサーバーから切り離して保管しておくことが望ましい。

＜攻撃者＞

- 犯罪グループ

＜被害者＞

- 個人（PC、スマートフォン利用者）

＜脅威と影響＞

ランサムウェアに感染し、PC やスマートフォンに保存されているファイルが暗号化されたり、PC やスマートフォンの操作ができないように画面をロックされたりし、金銭を要求される被害が発生している。

一般家庭で利用する PC やスマートフォンには、家族や友人の写真や動画が保存されていることが多い。ランサムウェアに感染すると、これらのファイルが暗号化され、閲覧できなくなる。なお、金銭を支払ったとしても、確実に復号される保証はないが、大切なファイルを取り戻すために、金銭を支払うケースもある。

また、ファイルの暗号化や画面のロック以外にも、ファイルの破壊やデータを外部に流出させると脅迫するケースも確認されている。

＜攻撃手口＞

◆ **メールの添付ファイルから感染**

- メールにランサムウェアやランサムウェアのダウンローダーを添付し、添付ファイルを開かせることで感染

◆ **ウェブサイトから感染(脆弱性を悪用)**

- メールのリンクをクリックさせる等で悪意あるウェブサイトや改ざんされたウェブサイトを閲覧させることで感染

- 不正広告をクリックさせることで感染（表示のみで感染するケースもある）

＜事例と傾向＞

◆ ランサムウェア被害の急増

2016 年は前年に比べるとランサムウェアの被害が急増している。[I]2016 年に日本国内で検出されたランサムウェアの件数は、前年比で約 9.8 倍になった。日本で確認されているランサムウェアの大半は英語表記だが、日本語表記で脅迫を行うランサムウェアも確認されている。

◆ 暗号化されたファイルの復号ツールを活用

ランサムウェアによって暗号化されたファイルを復号するツールがセキュリティベンダー等から公開されている。[II] [III] [IV] また、ランサムウェア対策情報を提供しているウェブサイト「The No More Ransom Project」でも、複数の復号ツールを提供している。[V]

これらのツールは全てのランサムウェアに対して有効ということではないが、暗号化されたファイルの復号に活用できる可能性がある。

＜対策/対応＞

個人（PC、スマートフォン利用者）

- 被害の予防
  - ・受信メール、ウェブサイトの十分な確認
  - ・添付ファイルやリンクを安易にクリックしない
  - ・OS・ソフトウェアの更新
  - ・セキュリティソフトの導入
- 被害を受けた後の対策
  - ・バックアップから復旧

    光学メディア（DVD-R、BD-R 等）、外付け HDD、USB メモリ等、外部記録媒体へ定期的にバックアップを行う。但し、バックアップに使用する記録媒体は、バックアップするときのみ、PC やスマートフォンに接続すること。常時接続していると、バックアップしたファイルもランサムウェアの感染対象となる。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。
  - ・復号ツールの活用

    ランサムウェアをセキュリティソフト等で駆除した上で、復号ツールを実行することで、暗号化されたファイルを復号できる可能性がある。
  - ・復元機能の活用

    Dropbox や Google ドライブ、Google フォト等のクラウドサービスの中には復元機能を持っているものもあるため、バックアップ先として利用している場合、その機能を使うのも有効である。

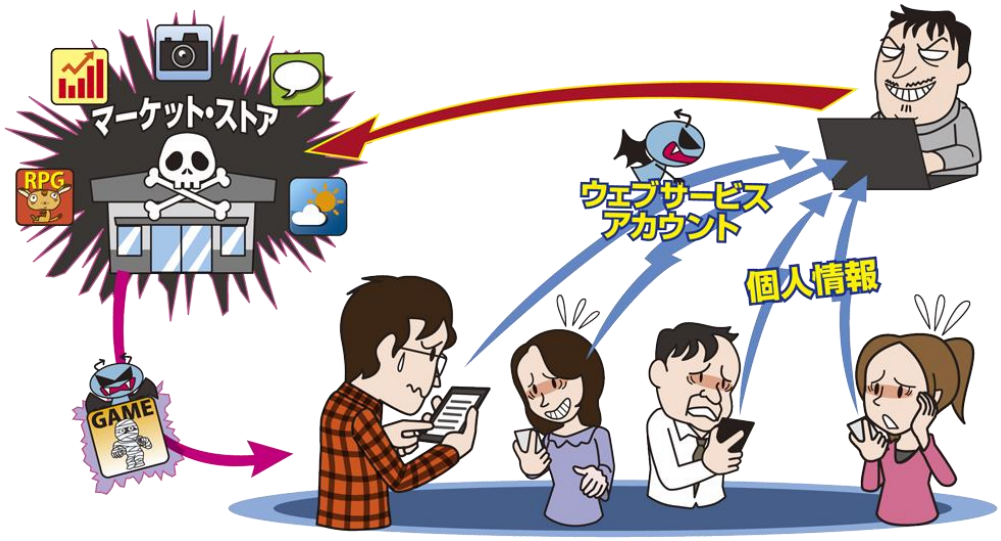
参考資料

I. 日本と海外の脅威動向を分析した「2016年年間セキュリティラウンドアップ」を公開
http://www.trendmicro.co.jp/jp/about-us/press-releases/articles/20170301015352.html
II. Trojan-Ransom.Win32.Rannoh の感染により影響を受けたファイルを復号化するユーティリティ
https://support.kaspersky.co.jp/viruses/disinfection/8547
III. ランサムウェア ファイル復号ツール
https://esupport.trendmicro.com/support/vb/solution/ja-jp/1114210.aspx
IV. ESET Releases Decryptor for Recent Variants of TeslaCrypt Ransomware
https://www.eset.com/us/about/newsroom/press-releases/eset-releases-decryptor-for-recent-variants-of-teslacrypt-ransomware/
V. The No More Ransom Project
https://www.nomoreransom.org/

組織ランク外

3位 スマートフォンやスマートフォンアプリを狙った攻撃

～人気アプリに酷似した不正アプリが暗躍～



人気アプリに偽装した不正アプリを利用者にインストールさせ、スマートフォン内の個人情報を窃取したり、遠隔操作を行える状態にしたりする事件が発生した。また、スマートフォン向けランサムウェアによって端末をロックして、復旧と引き替えに金銭を要求される被害も起きている。

＜攻撃者＞

- 犯罪グループ
- 犯罪者(ストーカー等)

＜被害者＞

- 個人（スマートフォン利用者）

＜脅威と影響＞

人気（注目度が高い）アプリに偽装することで、不正アプリと気づかせずにインストールさせる手口が確認されている。不正アプリをスマートフォンにインストールすると、連絡先や通話記録、位置情報等の個人情報を含む重要な情報を窃取されたり、録画・写真撮影・通話録音等を遠隔操作されたりする。

また、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、ランサムウェアに感染すると、スマートフォン内のファイルが暗号化されたり、画面をロックされたりし、復旧と引き換えに金銭を要求される。

＜攻撃手口＞

◆ **人気アプリに偽装した不正アプリ**

人気アプリに偽装した不正アプリをスマートフォンにインストールさせ、不正アプリを通して、個人情報を窃取する。さらに、録画・写真撮影・通話録音等を遠隔操作される恐れもある。

◆ **スマートフォン向けのランサムウェア**

不正アプリのインストール等によりランサムウェアに感染すると、スマートフォン内に保存されたファイルを暗号化して開けなくしたり、画面をロックして端末を操作不能にしたりして、復旧と引き替えに金銭を要求される（詳細は本書「10 大脅威 2017」の個人の第 2 位「ランサムウェアによる被害」を参照）。

◆ **騙してアプリをインストールさせる**

知人等の被害者と親しい攻撃者が、言葉巧みに遠隔操作や個人情報の窃取等をできるアプリをインストールする。その後、不正に操作や個人情報を窃取する。攻撃者が信頼できる人である場合、無条件にアプリをインストールさせてしまう恐れがある。

＜事例と傾向＞

◆ **人気アプリに偽装する不正アプリ**

人気アプリに偽装する手法としては、2016 年 7 月以降、「ポケモン GO」[I] や「スーパーマリオラン」[II] 等の人気ゲームアプリの偽装事例が複数確認された。人気ゲームに便乗し、不正アプリをインストールさせる手口は、スマートフォンを狙うサイバー犯罪者にとって常套手段の1つとなっている。

◆ **スマートフォン向けランサムウェア**

2016 年 3 月に日本語で脅迫するスマートフォン向けのランサムウェアが確認された。これは端末ロック型で日本の「MINISTRY OF JUSTICE（法務省）」をかたり、被害者に解除の対価として 10,000 円をギフトカードで支払うよう要求するタイプのものだった。[III]

＜対策/対応＞

個人（スマートフォンアプリ利用者）

● 情報リテラシーの向上

・アプリは公式マーケットから入手

iPhone アプリは公式マーケットである「App Store」からの入手に限られているが、Android アプリは色々なマーケットから入手可能であるため注意が必要である。

Android アプリを入手するときは、公式マーケットである「Google Play ストア」から入手する。また、サードパーティーマーケットから入手するときは、運営者がアプリ審査を実施してセキュリティ品質を確保しているマーケットを選択する。

・アクセス権限の確認

アプリのインストールまたは実行時に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。アプリの機能に対して妥当かどうかを判断し、関係のない権限の要求であればインストールせず、見合わせる。また、妥当性が判断できない場合もインストールや許可をしないことを推奨する。例えば、連絡先や位置情報等の重要な情報にアクセスする場合は注意が必要である。

● 被害の予防

・OS やアプリは最新版を利用

・セキュリティソフトの導入

偽のセキュリティソフトも公式マーケットに公開されている場合があるため、インストール時はアプリの信頼性を確認する。

・セキュリティ設定の実施

Android のセキュリティ設定で提供元不明のアプリのインストールを許可する設定を有効にしない。

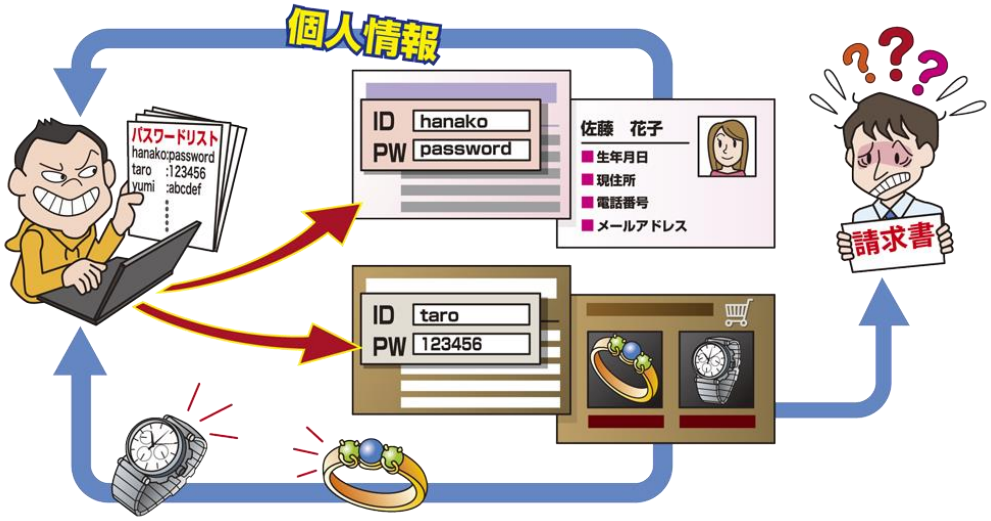
参考資料

I. 最新モバイル脅威事情号外：「Pokémon GO」の話題性を悪用する攻撃者
http://blog.trendmicro.co.jp/archives/13621
II. 人気の「スーパーマリオラン」偽アプリが問題に
http://www.yomiuri.co.jp/science/goshinjyutsu/20161216-OYT8T50040.html
III. ファイルや端末を人質に脅迫！？スマホを狙う不正アプリの最新事情
http://www.is702.jp/special/1938/#Content02

組織 7 位

4位 ウェブサービスへの不正ログイン

～多要素認証の活用を～



2016 年に確認されたウェブサービスへの不正ログインの多くが他のウェブサイトから漏えいした ID やパスワードを悪用している。ウェブサービス利用者は、パスワード管理ソフト等を使い、複雑なパスワードを設定した上でパスワードの使い回しを避ける必要がある。また、ウェブサービスの一部では、多要素認証等の不正ログイン対策を行っている場合があるので、ウェブサービスの利用者は、それらの対策を活用する。

＜攻撃者＞

- 犯罪グループ
- 犯罪者（ストーカー等）

＜被害者＞

- 個人（ウェブサービス利用者）
- 組織（ウェブサービス運営者）

＜脅威と影響＞

窃取や推測されたパスワードによりウェブサービスへ不正ログインされる被害が引き続き起きている。ウェブサービスへの不正ログインによる影響は、提供しているウェブサービスの機能によって変わる。例えば、インターネットバンキングの場合は、不正送金により金銭被害が発生する。ショッピングサイトであれば、氏名や住所、電話番号、クレジットカード情報等が窃取されたり、不正な購買やポイント等の盗用が行われたりする。また、オンラインゲームサイトであれば、勝手に支払いが行われたり、ゲーム内アイテムを窃取されたりする。

＜攻撃手口＞

◆ パスワードリスト攻撃

他のウェブサイトから漏えいした ID とパスワードの組み合わせを利用して攻撃する手法である。複数のウェブサイトで同じ ID とパスワードを使い回している場合、1 つのウェブサイトの ID とパスワードが漏えいしただけで、他のウェブサイトにも被害が拡大する。

◆ パスワードの推測攻撃

利用者が使いそうなパスワードを推測して不正ログインを試みる攻撃。例えば、ID とパスワ

ードが同一、パスワードに単純な単語や、「123456」や「abcdef」のような連続した英数字を使用している場合、攻撃者にパスワードを推測される恐れがある。SNS で公開している誕生日等の情報をパスワードにするのも危険だ。[I] また、「qwerty」といった一見ランダムな文字に見えるが実はキーボード上の隣接している文字も推測されやすい。

＜事例と傾向＞

◆ **ブログへの不正ログイン**

ブログサービス「Ameba」において、2016 年 5 月と 11 月に不正ログインが行われた。[II] 特に 11 月は、約 59 万件の不正ログインを確認している。[III] なお、ブログの登録情報の改ざんは確認されていない。他のウェブサイトで漏えいしたパスワードが使われた可能性がある。

◆ **オンラインショッピングへの不正ログインによるポイントの不正利用**

オンラインショッピングサイト「ビックカメラドットコム」において、不正ログインが行われ、ポイントを不正に利用される被害が発生した。[IV] また、氏名、住所等の利用者の情報も閲覧された可能性があった。他のウェブサイトで漏えいしたパスワードが使われた可能性がある。

◆ **SNS への不正ログイン**

イラストを投稿できる SNS「pixiv」において、2016 年 11 月 29 日から 12 月 2 日にかけて、パスワードリスト攻撃が行われた。これにより約 3,600 件のアカウントが不正ログインされ、登録しているメールアドレス、生年月日、性別が閲覧された可能性がある。[V]

＜対策/対応＞

個人（ウェブサービス利用者）

- 情報リテラシーの向上
  - ・パスワードは長く、複雑にする [VI]
  - ・パスワードの使い回しをしない
- 被害の予防
  - ・パスワード管理ソフトの利用

    信頼できるパスワード管理ソフトを利用し、ウェブサイトごとに異なるパスワードを設定する。また、パスワードには推測されにくい文字列を設定する。

    パスワード管理ソフトが利用できない場合は、普段使用しているパスワードの最後にウェブサイト毎に数字や記号を加えるだけでも対策として有効である。また、厳重に管理されたメモにパスワードを記載しておくことでも良い。
  - ・多要素認証の利用

    多要素認証が利用できる場合は、これを利用することで不正ログイン防止に効果がある。また、仮に ID やパスワードが窃取されても、金銭等の最終的被害を回避することもできる。
  - ・利用をやめたウェブサービスの退会

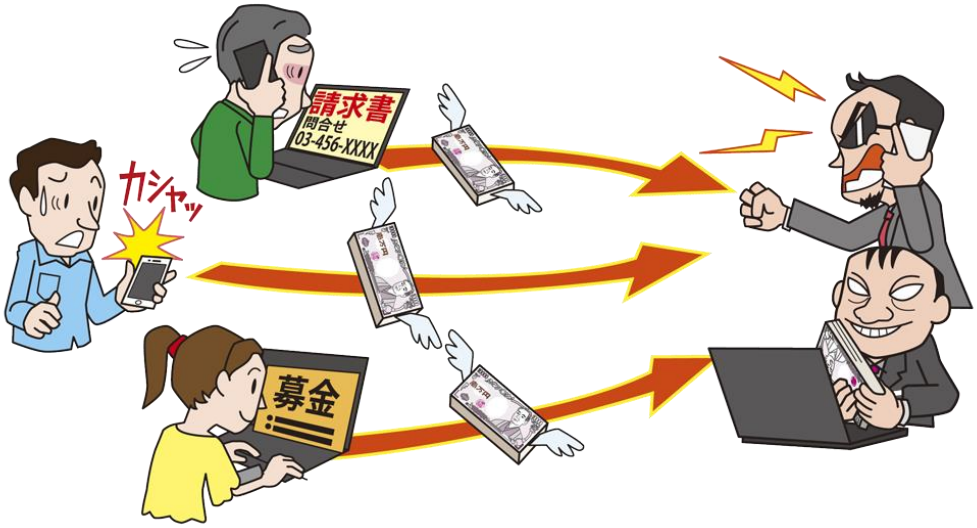
参考資料

I. SNSで公開している誕生日などの情報を使ったパスワード設定は推測されやすくNG
https://www.ipa.go.jp/security/anshin/mgdayori20161221.html
II. 「Ameba」への不正ログインに関するご報告とパスワード再設定のお願い
http://ameblo.jp/staff/entry-12159141397.html
http://ameblo.jp/staff/entry-12224046295.html
III. 「Ameba」で約59万件の不正ログイン--パスワードリスト型攻撃で
https://japan.cnet.com/article/35092962/
IV. 当社インターネットショッピングサイトでの会員ID、パスワード不正使用被害について
http://www.biccamera.com/bc/c/info/report/20160303.jsp?160303
V. 【重要】pixivの一部アカウントに対する「なりすましログイン」の報告とパスワード変更のお願い
http://www.pixiv.net/info.php?id=3897
VI. 不正ログイン被害の原因となるパスワードの使い回しはNG
https://www.ipa.go.jp/security/anshin/mgdayori20160803.html

組織ランク外

5位 ワンクリック請求等の不当請求

～「ゼロクリック詐欺」登場！サイトを見ただけで「登録完了」～



PC やスマートフォンを利用中にアダルトサイトや出会い系サイト等にアクセスすることで金銭を不当に請求されるワンクリック請求の被害が依然として発生している。これまでは利用者のクリックをきっかけにして請求画面が表示されるものだったが、2016 年はクリックすることなく請求画面が表示される「ゼロクリック詐欺」と呼ばれる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、利用者の安易なクリックで、会員登録料や利用料といった名目で金銭を請求するワンクリック請求が依然として発生している。

また、被害者の不安な心理を悪用して、高額な金銭要求がされる被害もある。例えば、サポートセンターへの連絡を促してくることで、慌てて電話を掛けてしまい電話番号が攻撃者に知られてしまう。

＜攻撃手口＞

◆ 悪意あるウェブサイトへの誘導

アダルトサイト内に表示されている動画再生ボタンをクリックすることにより、会員登録の完了画面の表示と利用料金の請求画面を表示させる。閲覧者に誤って登録してしまったと勘違いさせ、不当に金銭を請求する。

◆ 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ていた外部サイトの URL をクリックすると入会完了の画面が表示され、高額な入会金を請求する。また、サポートセンターへの電話番号が表示されたポップアップが表示され続け、退会のために電話を掛けてしまうと相手に自身の電話番号を知られることになる。さらに退会に必要な情報だとして個人情報を聞き出されることもある。

◆　**スマートフォンの仕組みを悪用した手口**

スマートフォンでアダルトサイト等を閲覧した際に、閲覧者の顔をカメラで撮影したと思わせるシャッター音を鳴らし、不安を煽り、金銭を要求する。また、ポップアップを表示し、ポップアップ内の画面に表示された OK ボタンをクリックさせることで勝手に犯罪者へ電話発信させる手口もある。

＜事例と傾向＞

◆　**閲覧するだけで登録完了**

従来の不当請求は、利用者にクリックさせた上で登録が完了したと告げる手口であったが、利用者のクリックを必要とせず、ウェブサイトを閲覧しただけで「登録完了」と表示して利用者を欺き利用料を請求する「ゼロクリック詐欺」が登場した。[I]

◆　**義援金を装った詐欺**

5 月、国民生活センターは熊本地震に便乗したワンクリック請求等が発生しているとして注意を呼びかけた。[II]

SNS の投稿の「募金」と書かれた文字をクリックしたところアダルトサイトの料金請求画面が表示されたケースや、義援金の募集を謳ったメールに URL のみ記載して送られてくる等の相談が寄せられている。

◆　**被害者をさらに騙すネット広告も**

アダルトサイトのワンクリック請求の被害者をさらに騙すネット広告が確認された。探偵業者や司法書士事務所の広告で、「無料相談」や「返金可能」と謳った上で「調査料」や「契約取り消しの交渉」等の名目で料金を請求する。調査を数万円で依頼したもののアダルトサイト業者からの返金もない、といった相談が国民生活センターで急増している。[III] また、正規のサポートを装って不必要なツールをインストールさせた上でサポート費用と称して金銭を要求するケースも確認されている。[IV]

＜対策/対応＞

個人（ネットサービス利用者）

- 情報リテラシーの向上
  - ・受信メール、ウェブサイトの十分な確認
  - ・Twitter や SNS 等のメッセージに注意

    Twitter や SNS 等のメッセージに記載している URL も安易にクリックしない。
  - ・怪しいアプリは利用しない

    ダウンロードやアプリを起動する際に表示されるアクセス権限等の画面を確認し、アプリの機能と関係がない権限を要求してくるアプリはインストールしない。
  - ・事例・手口の情報収集

    日頃から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の情報を収集しておくことも有効である。
  - ・不当請求には応じない

    「登録完了」と表示されても、不当請求には応じない。個人情報の入力を行っていない等により攻撃者は実際に請求するための情報を入手していないケースもある。不安な場合は、国民生活センターや消費者センター等に相談する。

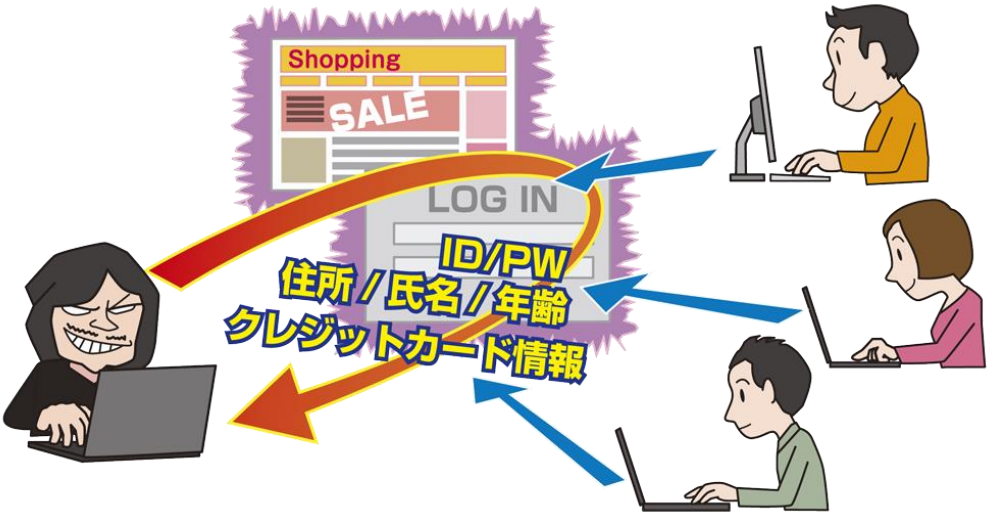
参考資料

I. 日本語のゼロクリック詐欺が登場
https://www.symantec.com/connect/ja/node/3563951
II. 熊本地震に便乗した不審なメールやSNSの投稿などにご注意ください！
http://www.kokusen.go.jp/pdf/n-20160527_1.pdf
III. 詐欺被害者を二重にだますネット広告に注意！
http://www.yomiuri.co.jp/science/goshinjyutsu/20161226-OYT8T50017.html
IV. 不安をあおって電話でだます「サポート詐欺」の手口を追う
http://blog.trendmicro.co.jp/archives/13970

組織 3 位

6位 ウェブサービスからの個人情報の窃取

～犯罪グループの攻撃による甚大な被害～



ウェブサービスの脆弱性を悪用し、ウェブサービス内に登録されている住所や氏名等の個人情報やクレジットカード情報が窃取される事件が 2016 年も前年に引き続き発生している。数 10 万件の個人情報等の重要な情報が漏えいする事件も発生しており、ウェブサービスを運営・管理する組織は適切な対応が求められる。また、ウェブサービス利用者は万が一の情報漏えいを考慮して、そのサービスの信頼性の確認やサービス利用に不必要な情報は登録しない等の対応が必要である。

＜攻撃者＞

- 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＞

ウェブサービスには多くの個人情報等が登録されている。例えば、ショッピングサイトであれば個人情報を含む重要な情報（氏名・性別・生年月日、クレジットカード情報等）が登録されている。また、SNS であれば自身の情報に加え、友人の個人情報が登録されていることもある。

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、利用しているソフトウェアのバージョン等を適切に管理していない場合、ソフトウェアのセキュリティ上の欠陥である脆弱性を内在したままサービス提供している可能性もある。

このようなウェブサービスは内在している脆弱性を攻撃され、登録してある重要な情報を窃取されたり、その情報を不正使用されたりする被害が確認されている。ウェブサービスはその性質上、インターネットで提供されるため、攻撃者のターゲットにされやすい。

＜攻撃手口＞

◆ ウェブサービスの脆弱性を悪用

ウェブサービスに存在する脆弱性を悪用され、個人情報が窃取される。ウェブサービス運営事業者にて、ウェブサービスを構成しているソフト

ウェアに対して適切な脆弱性対策を行っていない場合に起こる恐れがある。

＜事例と傾向＞

◆ **民間放送会社に不正アクセスされ、最大 43 万件の個人情報漏えいの可能性**

日本テレビのウェブサイトへの不正アクセスが発生した。ウェブサイトで利用しているソフトウェアの OS コマンドインジェクションの脆弱性を突かれ、最大 43 万件の個人情報が漏えいした可能性がある。[I] [II]

◆ **化粧品通販サイトに不正アクセスされ、個人情報約 42 万件が流出した可能性**

システムの脆弱性を突いたイプサの通販サイトへの不正アクセスにより、登録している顧客のクレジットカード情報や個人情報約 42 万件が漏えいした可能性がある。[III]

◆ **大手学習塾のウェブサイトにゼロデイ攻撃**

大手学習塾栄光ゼミナールのウェブサイトが CMS の「Movable Type」のプラグイン「ケータイキット for Movable Type」の脆弱性を狙ったゼロデイ攻撃（脆弱性の修正プログラムが開発ベンダーより提供される前に行われる攻撃）による不正アクセスを受けた。不正アクセスにより、ウェブサイトから説明会に申し込んだ生徒と保護者、2,761 人の個人情報が漏えいした。[IV]

＜対策/対応＞

個人（ウェブサービス利用者）

- 情報リテラシーの向上
  - ・必須項目以外の情報登録しない
    ウェブサイトからの情報漏えいの可能性を考慮して、サービス利用するための必須項目以外の情報は登録しない。
  - ・利用をやめたウェブサービスの退会

【参考】

組織（ウェブサービス運営事業者）

ウェブサービスの利用者が安心して利用できるように、以下のセキュリティ対策を実施する（詳細は本書「10 大脅威 2017」の組織の第 3 位「ウェブサービスからの個人情報の窃取」を参照）。

- ・脆弱性対策を含めたセキュリティ対策（システム構築時）
- ・ウェブサイトシステムを構成しているソフトウェアの継続的な脆弱性対応（事業運営時）[V]

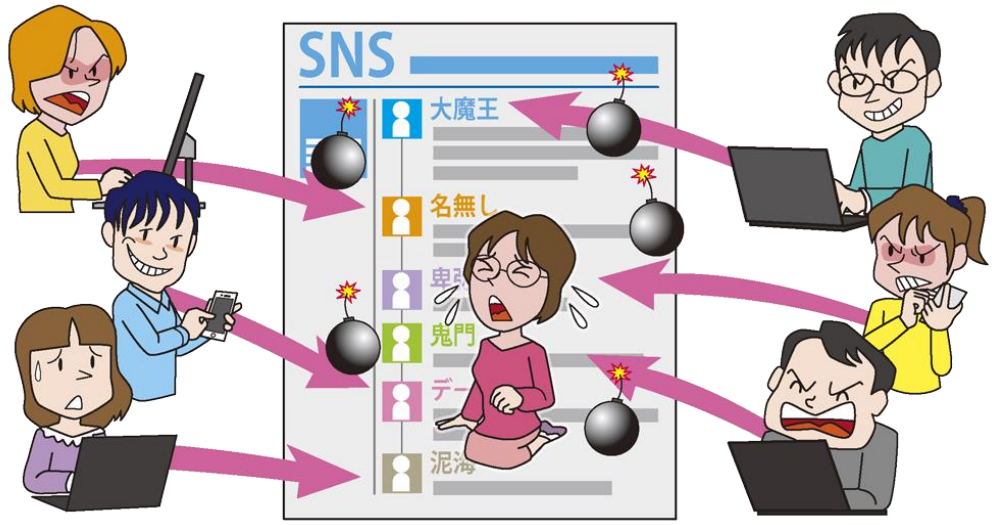
参考資料

I. 日テレに不正アクセス - 最大43万件の個人情報が漏洩した可能性
http://www.security-next.com/069154/
II. 個人情報不正アクセスに関する調査報告書
http://www.ntv.co.jp/oshirase/20160714.pdf
III. クレカ情報5.6万件含む個人情報42万件が流出した可能性 - イプサ
http://www.security-next.com/076305/
IV. 大手学習塾で個人情報が流出 - MT用プラグインにゼロデイ攻撃
http://www.security-next.com/069542
V. IPAテクニカルウォッチ「脆弱性対策の効果的な進め方（実践編）」
https://www.ipa.go.jp/security/technicalwatch/20150331.html

組織ランク外

7位 ネット上の誹謗・中傷

～不満やストレス発散を目的とした過激な投稿の増加～



コミュニティサイト（ブログ、SNS、掲示板等）での誹謗中傷や犯罪予告の書き込みが行われ問題となっている。不用意で過激な投稿により、一般人の心理的脅迫や名誉棄損、営業妨害や社会混乱等を招いている。

＜攻撃者＞

- 情報モラルの低い人
- 悪意ある攻撃者

＜被害者＞

- 個人
- 組織（教育機関、公共機関、企業）

＜脅威と影響＞

スマートフォンやインターネットサービスの普及により、誰でも不特定多数の人に情報を発信することが容易となっている。そうした情報発信の容易さや匿名性により、ネット上で誹謗中傷や犯罪予告する行為が相次いでいる。心ない誹謗中傷や差別的発言等によって、被害者は心理的脅迫に苦しんでいる。また、悪意ある暴言やデマは社会的混乱を招くこともある。一方、不用意な投稿を行っている人は、名誉棄損や、脅迫罪や業務妨害等に問われることもある。

＜要因＞

◆ **情報モラルの欠如**

自分の発言が他人を心理的に追い詰めることを理解しておらず、安易に誹謗中傷や差別的発言等の投稿が行われる。不満やストレスの発散が目的であったり、わざと過激で鋭利な発言を行い、知名度を上げることが目的だったりする。

＜事例と傾向＞

◆ **悪意ある投稿の理由「人の意見に反論したかったから」が前年より増加**

IPA が 2016 年に行った「情報セキュリティの倫理に対する意識調査」[1] によると、例えば、スマートデバイス利用者の悪意ある投稿経験者は 24.2%と 2015 年の 26.9%と比べ、若干減ってはいるが大きな変化はない。しかし、投稿理由として「人の意見に反論したかったから」が

35.2%と前年の 24.5%から 10.7%と大きく増加している。また、2014 年の 32.3%、2013 年の 27.9%と直近のアンケート結果の中では最大となっている。スマートフォン利用者は、対抗心や反発心が強くなっている傾向が伺える。容易に広く発信できるという仕掛けを手に入れた現代において、逆により高い情報モラルが今後求められてくるものと考える。

◆ **犯行予告の書き込み**

大学や自治体等を爆破する旨の犯行予告が投稿され、対象の組織は安全のため立ち入りを禁止する等の対応をとった。このようなインターネット上への犯罪予告の投稿が相次いでいる。投稿理由は「いたずらのつもりだった」や「目立ちたかった」等が挙げられている。単なる投稿は犯罪ではないと思っている情報リテラシーの低下や、ネットコミュニティ上で目立ちたいという自己顕示欲が原因と考えられる。[II]

◆ **軽率な発言で炎上**

某企業の従業員の過労自殺の事件を受けて、某大学の教授が「月当たりの残業時間が 100 時間超えたくらいで過労死するのは情けない」とコメントを投稿した。コメントはネット上で拡散し、批判が殺到した。その後、教授はそのコメントを削除し、謝罪のコメントを投稿した。[IV]

＜対策/対応＞

個人（投稿者）

- 情報モラル・情報リテラシーの向上
  - ・誹謗中傷や公序良俗に反する投稿を控える

    匿名だからばれないと思うのではなく、プロバイダーに依頼すると投稿者の情報が開示される可能性があるということを理解した上で投稿を行う必要がある。[III]
  - ・投稿前に内容を再確認

    Twitter やブログ等に投稿する内容は不特定多数の人に見られることを想定し、投稿して問題ない内容かをしっかりと確認する。また、閲覧範囲の設定ができる場合は、必要最小限に設定する。
  - ・情報モラル・情報リテラシーの教育

    インターネット利用の低年齢化が進む中で、早い段階で、情報モラルや情報リテラシーに対する教育を図っていく。

個人（誹謗中傷された側）

- 被害を受けた後の対策
  - ・冷静な対応と支援者への相談

    一人で抱え込まず、周囲への相談や公的相談機関を利用する。
  - ・SNS 運営会社に投稿の削除を依頼
  - ・犯罪と思われる誹謗中傷の投稿は、警察へ被害届を提出

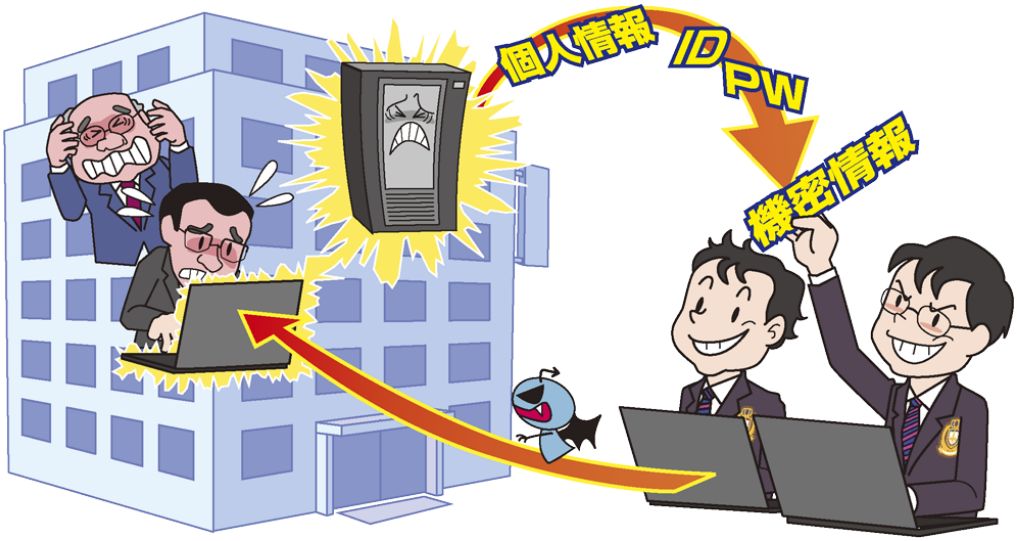
参考資料

I.「2016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
http://www.ipa.go.jp/security/fy28/reports/ishiki/
II. 中学生の犯行も！ネット犯罪予告が急増する理由
https://www.eltes-orm.com/column/id366/
III. 掲示板等での誹謗中傷
http://www.consumer.go.jp/seisaku/caa/kohyo/econsumer/tokumei/tokumeisei3-1.html
IV.「残業100時間で過労死は情けない」のか？ 電通女性社員自殺めぐり武蔵野大教授の投稿が炎上 大学は処分へ
http://www.sankei.com/affairs/news/161012/afr1610120015-n1.html

組織ランク外

8位 情報モラル欠如に伴う犯罪の低年齢化

～情報モラルを教育できる体制を構築しよう～



2016 年も未成年者が IT 犯罪の加害者として逮捕、補導される事件が多数確認されている。IT 犯罪に悪用できるツールや知識がインターネットを通じて誰でも入手できるようになり、情報モラルの欠如した未成年者が、IT 犯罪に手を染めてしまっている。

＜攻撃者＞

- 情報モラルの低い若者
- 悪意ある若者

＜被害者＞

- 個人（オンラインゲーム利用者）
- 組織（教育機関）
- 組織（オンラインゲーム会社等）

＜脅威と影響＞

未成年者による IT 犯罪が多数確認され、逮捕・補導される事件が起きている。

未成年者による犯罪には、未成年者自身の情報リテラシーの不足により自分の行為が犯罪であることを認識しないで行っているケースや情報モラルの欠如により犯罪と認識した上で私利私欲のために行っているケースがある。特に後者のケースでは、成人が犯す犯罪と同じ動機であり、未成年者の犯罪と成人の犯罪に違いがなくなってきている。

また、インターネットの普及に伴い、サイバー攻撃に悪用できるツールや知識が、誰でも入手できるようになった。このような環境が未成年者による犯罪を助長していることも、未成年者の IT 犯罪が増加している要因と考えられる。

一方、攻撃対象も、教育機関やオンラインゲーム会社等、未成年者と関連が深い組織が狙われる他、インターネット上でのトラブルに巻き込まれた個人が狙われる場合がある。

組織が被害者となったケースでは、DDoS 攻撃によるサービスの妨害や、不正アクセスによる情報漏えい等が確認された。これら被害の二次被害として、組織の社会的な信用の失墜やビジネス機会の損失等によって、結果的に金銭被害につながる場合がある。

また、個人が被害者となったケースでは、チート(不正・改変)行為をする人を懲らしめようと、

チートツールと偽って遠隔操作ができるウイルスを仕込み、チート行為をする人に感染させるといった被害が確認された。なお、オンラインゲームのチート行為は一見犯罪に見えないが、ゲームバランスを崩壊させて運営会社に損害を与えるデータを作り出す点で攻撃であり、私電磁的記録不正作出罪・供用罪に問われる可能性がある。

＜要因＞

◆ **情報モラルの欠如**

自分の行為が犯罪であることを理解した上で、金銭目的等の私利私欲のために犯罪を行う。

◆ **情報リテラシーの不足**

自分の行為が犯罪であることを理解せず、面白半分に犯罪を行う。

◆ **攻撃ツールの普及**

攻撃に悪用できるツールがインターネット上に公開され、未成年者を含め誰もが容易に入手できる環境が犯罪を助長している。

＜事例と傾向＞

◆ **佐賀県の教育情報システム「SEI-NET」と校内 LAN への不正アクセス**

2016 年 6 月に、佐賀県の教育情報システム（SEI-NET）および校内 LAN が、17 歳と 16 歳の少年らによる不正アクセスを受けた。少年らは、不正アクセスの手口や盗み出した情報をネット上で他の複数の未成年者らと共有していた。[I]

◆ **オンラインゲーム会社に対する DDoS 攻撃で高校生を書類送検**

DDoS 攻撃によりオンラインゲーム運営会社のサービスを妨害したとして、大阪府高槻市の男子高校生が書類送検された。男子高校生は攻撃対象の会社の反応等を見るのが面白かった、自己顕示欲を満たしたかったという主旨の供述をしている。[II]

◆ **PC 遠隔操作ウイルス供用容疑で高校生を逮捕**

横浜市の男性の PC を遠隔操作ウイルスに感染させたとして、和歌山県の 16 歳の男子高校生が逮捕された。高校生は、オンラインゲームを有利に進めるためのプログラムを装い、不特定多数にウイルスをダウンロードさせていたと見られる。[III]

＜対策/対応＞

個人

- 情報モラル・情報リテラシーの向上

  ・情報モラル・情報リテラシーの教育

  情報リテラシー向上の教育は随所で取り組まれるようになってきているが、今後は、併せて、情報モラルに関しての教育も行っていく必要がある。特に、情報分野に限らず、未成年者への情報モラルの教育は、親や教師等が大きな影響力を持つので、家庭内でしっかり教育を行う等、責任を持った対応が求められる。

参考資料

I. 佐賀県の教育情報システム「SEI-NET」と校内LANへの不正アクセス事案についてまとめてみた
http://d.hatena.ne.jp/Kango/20160627/1467041904
II. オンラインゲーム会社にDDoS攻撃　男子高校生を書類送検　滋賀
http://www.sankei.com/west/news/161119/wst1611190052-n1.html
III. 高1、遠隔操作ウイルス供用容疑　和歌山の少年逮捕
http://www.nikkei.com/article/DGXLASDG02H0B_S6A101C1CC0000/

組織ランク外

9位 インターネット上のサービスを悪用した攻撃

～怪しいサイトは見ないは通用しない。基本的な対策を確実に～

正規のサイトに表示される不正広告や、正規のサービスをコマンド＆コントロールサーバー（C&C：ウイルスに感染している PC に対して命令するサーバー）として動作させてウイルスとの通信に悪用する等、インターネット上でサービスとして提供されている機能や仕組みを隠れみのとする攻撃が問題となった。これらは、正規のサービスを利用していることから、利用者側の対策が難しく、サービス提供ベンダー側での対策が求められる。

＜攻撃者＞

- 犯罪グループ

＜被害者＞

- 個人（サービス利用者）
- 組織（サービス提供ベンダー）

＜脅威と影響＞

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。この正規のサービスやサイトが攻撃に悪用される被害が増えている。

例えば、2015 年から被害が顕著化した不正広告は、2016 年も引き続き被害が確認されている。まずは、ウェブサイト上の広告掲載の仕組みを悪用し、不正なコードを含んだ広告をウェブサイト上に掲載する。その後、ウェブサイトの利用者がそのウェブサイトを閲覧した際に不正なコードが実行される。

また、インターネット上の正規のサービスを C&C サーバーとして動作させて、正規の通信に見せかけてウイルスと通信させる攻撃は、以前から確認されていたが、2016 年には、画像共有サービスや文書・表計算・プレゼンテーション作成サービスを悪用するウイルスが確認された。

＜攻撃手口＞

◆ 不正広告による正規ウェブサイトの汚染

攻撃者が、ネット広告の配信システム内にウイルス等を含む不正広告を混入させ、一般のウェブサイト上に表示させる。ウェブサイトの利用者がアクセスした際に、不正広告をクリックしたり、閲覧したりするとウイルスに感染する。ウェ

ブサイトを閲覧した不特定多数の人を攻撃することが可能である。

正規のウェブページへの不正広告の挿入手口としては、広告会社に不正アクセス等を行い、正規の広告コンテンツに不正なコードを挿入する方法と、攻撃者が不正なコードを含む広告を作成し、正規の方法で出稿する方法が挙げられる。国内で確認された例は、ほとんどが後者である。

このような不正広告は、正規の広告の画像等を元に作成されるため、利用者が外見で判断をすることは困難である。

◆ **正規のサービスを悪用した C&C 通信**

ウイルスに感染した PC と C&C サーバーの機能を持たされた正規のサービスとで通信を行い、正規の通信と見せかけ、攻撃を隠匿する手口である。攻撃者にとっては、攻撃情報を正規のトラフィックやコンテンツ内に隠蔽でき、攻撃を検出されにくくできるというメリットがある。例えば、無料オンライン画像共有サービスや文書・表計算・プレゼンテーション作成サービス等に C&C サーバーの機能を持たせて悪用する。

＜事例と傾向＞

◆ **音楽配信サービスに不正広告**

音楽配信サービス「Spotify」の無料版に、不正広告が挿入され、一部の利用者から、ブラウザ上に不審なポップアップが表示される、トロイの木馬がダウンロードされる等の被害が報告された。[I] サービス提供ベンダーは、その広告を停止し、サービスのコミュニティサイト等で注意を呼びかけた。

◆ **窃取した情報を PNG ファイルとして正規画像共有サービスにアップロード**

暗号化型ランサムウェア「CryLocker」は、感染した PC から窃取したデータを PNG 形式の画像ファイルに加工し、無料オンライン画像共有サービス「Imgur」にアップロードした。[II] また、このランサムウェアを拡散させる手口として、不正広告が用いられていた。

◆ **ポップアップでクレジットカード番号の入力を要求する不正広告**

ウェブサイトを閲覧しているとアンケートに答えると動画サービスが無料になると称して、ポップアップが表示され、クレジットカード番号等の入力を求める手口が確認された。[III] 広告機能を使って、不正に表示させていた可能性があった。

＜対策/対応＞

組織（サービス提供ベンダー）

- 被害の予防
  - ・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
- 被害の早期検知
  - ・運用やサービスの監視強化

個人（サービス利用者）

- 情報リテラシーの向上
  - ・怪しい(普段出ない)ポップアップが表示されたら個人情報等は入力しない
- 被害の予防
  - ・OS・ソフトウェアの更新
  - ・セキュリティソフトの導入
  - ・広告ブロックソフトウェアの利用

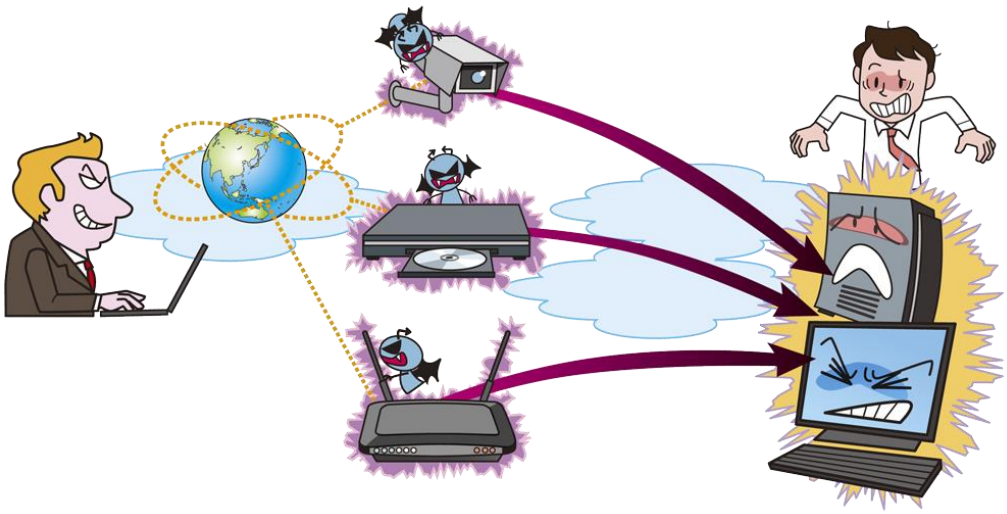
参考資料

I. 音楽配信サービス「Spotify」に不正広告 - マルウェア感染報告も
http://www.security-next.com/074579
II. 暗号化型ランサムウェア「CryLocker」、PNGファイルを利用して収集情報を正規画像共有サービスにアップロード
http://blog.trendmicro.co.jp/archives/13793
III. 「ユーザー調査」、実はカード番号収集の詐欺
http://www.yomiuri.co.jp/science/goshinjyutsu/20160902-OYT8T50028.html

組織ランク外

10位 IoT 機器の不適切な管理

～ウイルス「Mirai」による DDoS 攻撃の被害が深刻化～



ウイルス「Mirai」による DDoS 攻撃により、複数の大手ネットサービスが 5 時間にわたって接続しにくくなるトラブルが発生した。これは、初期パスワードのまま使用されているネットワークカメラ等の IoT 機器が、ウイルス「Mirai」に感染し、ネットサービスに DDoS 攻撃を行ったことが原因である。個人や組織の IoT 機器の所有者が知らないうちに攻撃に加担してしまっている。

＜攻撃者＞

- 犯罪グループ

＜被害者＞

- 組織（官公庁、企業）
- 個人（顧客、サービス利用者）

＜脅威と影響＞

昨今、ネットワークカメラ、ホームルーター、情報家電といった家庭に存在する IoT 機器もネットワークを介してつながるようになってきた。IoT 機器の利用者は IoT 機器がネットワークにつながっており、セキュリティ対策を行わなければいけないという認識が薄く、初期設定のまま利用しているケースがある。そのような初期設定のまま使用している IoT 機器を悪用するウイルス「Mirai」が登場し、「Mirai」に感染した IoT 機器で構成されたボットネットにより大規模な DDoS 攻撃が行われている。

「Mirai」に感染すると IoT 機器の利用者は、知らないうちに DDoS 攻撃に加担してしまい、企業のウェブサービス等を利用できなくしてしまっている恐れがある。また、もし攻撃されたウェブサービスが利用しているウェブサービスの場合、IoT 機器の利用者自身がそのサービスが使えないという被害も起こる恐れがある。

一方、DDoS 攻撃の被害だけではなく、設定不備を突いてネットワークカメラ越しに覗き見られる被害も起きている。

＜攻撃手口＞

- **初期設定に使用され易いユーザー名・パスワードを悪用して、設定が脆弱な IoT 機器をウイルスに感染させる**
- **ウイルス感染した IoT 機器をボットとして稼働させ、ウイルス感染した機器をインターネット上に増殖させる**
- **ボットに感染した IoT 機器群を攻撃者が遠隔から操作し、ウェブサイトの公開サービス等を DDoS 攻撃で麻痺させる**
- **初期設定のネットワークカメラにアクセスし、撮影情報を覗き見られる**

＜事例と傾向＞

- **Twitter や Amazon 等、5 時間にわたる接続困難になるトラブルが同時発生**

2016 年 10 月、Twitter、Amazon、Netflix 等の大手ネットサービスで 5 時間にわたって接続がしにくくなるトラブルが同時に発生した。[I] 今回のトラブルは、DNS サービスを提供している Dyn 社が、ウイルスの Mirai に感染した IoT 機器等で構成されたボットネットから DDoS 攻撃を受けたことが原因である。その結果、Dyn 社の DNS サービスを利用していた大手ネットサービスに影響が及んだ。

- **日本国内のネットワークカメラを覗き見**

世界各地の防犯カメラを覗き見できるサイトに日本国内のカメラと見られる約 4,300 台分の映像が公開されていた。原因は、パスワードが未設定のまま利用していたことであった。[II]

＜対策/対応＞

組織（システム管理者・利用者）、個人

- 情報リテラシーの向上
  - ・機器使用前に説明書を確認
- 被害の予防
  - ・初期設定されたパスワードを十分な長さを持つパスワードへ変更 [III]
  - ・外部からの不要なアクセスを制限 [IV]
  - ・不要な機能やポートの無効化（telnet、NAPT 設定等）
  - ・ソフトウェアの更新（自動化設定含む）

組織（IoT 機器の開発者） [V]

- 被害の予防
  - ・初期パスワード変更の強制化
  - ・セキュアプログラミング技術の適用
  - ・脆弱性の解消（脆弱性検査、ソースコード検査、ファジング等）
  - ・ソフトウェア更新手段の自動化
  - ・迅速なセキュリティパッチの提供
  - ・不要な機能の無効化（telnet 等）
  - ・安全なデフォルト設定
  - ・設計の見直し（セキュリティ設計含む）

    機器の中で複数のパスワードを管理する場合、パスワードの変更漏れがないように設計を見直す。
  - ・分かり易い取扱説明書の作成
  - ・利用者への適切な管理の呼びかけ

    IoT 機器の利用者は必ずしも情報リテラシーが高いとは限らない。マニュアルやウェブページ等で適切な管理を呼びかけることも重要である。

参考資料

I. 「IoT乗っ取り」攻撃でツイッターなどがダウン
http://www.yomiuri.co.jp/science/goshinjyutsu/20161028-OYT8T50051.html
II. のぞきサイトからウェブカメラ丸見え 飲食店・コンビニ・工場… パスワード管理徹底、メーカー呼びかけ
http://www.sankei.com/life/news/160131/lif1601310040-n1.html
III. ネットワークカメラや家庭用ルータ等のIoT機器は利用前に必ずパスワードの変更を
https://www.ipa.go.jp/security/anshin/mgdayori20161125.html
IV. IPAテクニカルウォッチ「増加するインターネット接続機器の不適切な情報公開とその対策」
https://www.ipa.go.jp/files/000052712.pdf
V. IoT開発におけるセキュリティ設計の手引き
https://www.ipa.go.jp/security/iot/iotguide.html

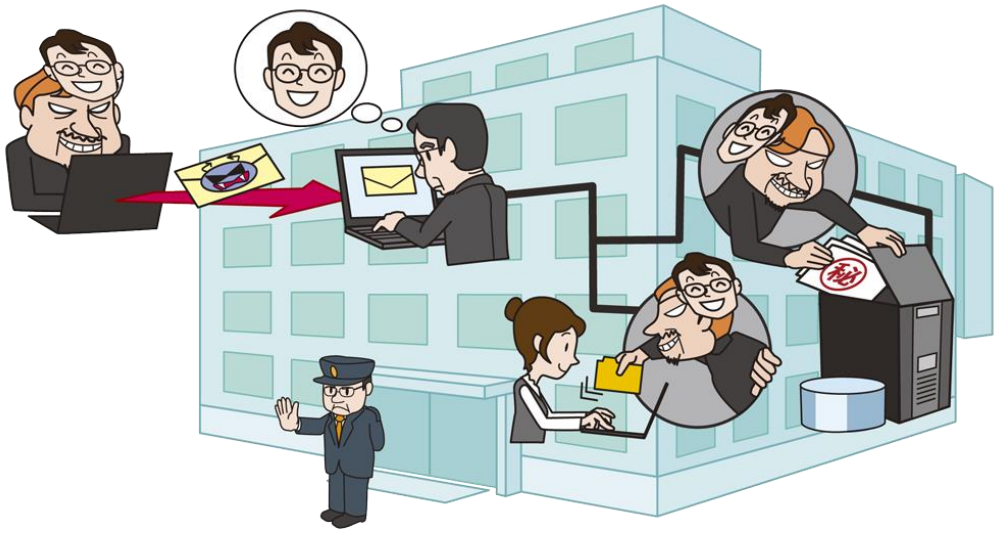
このページは空白です。

2.2. 情報セキュリティ10 大脅威（組織）

個人ランク外

1位 標的型攻撃による情報流出

～引き続き警戒、標的型攻撃による被害が増加～



企業や民間団体や官公庁等、特定の組織に対して、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、別の PC に感染を拡大し、最終的に個人情報や業務上の重要情報を窃取する標的型攻撃による被害が引き続き発生している。

＜攻撃者＞

- 諜報員、産業スパイ
- 犯罪グループ

＜被害者＞

- 組織（官公庁、民間団体、企業、研究機関）

＜脅威と影響＞

2016 年も標的型攻撃により組織の機密情報や顧客情報等が漏えいした事件の報道が続いている。標的型攻撃により情報漏えいが発生すると組織の信頼度低下や組織の基幹事業停止、といった大きな問題につながることがある。

標的型攻撃では、メールやウェブサイト、外部記録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、関連組織を攻撃の踏み台にすることもあり、業種や会社規模に関係なく狙われる恐れがある。

＜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）

特に、「(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狡猾になっている。例えば不正な署名が行われた同種のウイルスを複数観測している。署名とは、ソフトウェアが改ざんされていないこと、開発元組織が実在することを証明するための仕組みである。本来は、ソフトウェアの信頼性を担保し、

利用者を安心させるための仕組みが、長期間の感染のために悪用されている。[I]

＜事例と傾向＞

◆ **大手旅行会社から個人情報が流出**

2016 年 6 月、大手旅行会社 JTB への標的型攻撃により、氏名、生年月日、メールアドレス、住所、電話番号、パスポート番号といった約 678 万件の個人情報等が漏えいした可能性があると公表された。[II] 発端は 2016 年 3 月、社員が、取引先になりすましたメールの添付ファイルを開き、ウイルスに感染したことで、その後、外部からの遠隔操作により、個人情報を保管しているサーバーへと侵害が拡大していった。

◆ **経団連の PC が外部と不審な通信**

2016 年 10 月下旬から 11 月初めにかけて、23 台の事務局 PC が 10 台の外部サーバーとの間で不審な通信を行っていたことが判明した。[III] 不審な通信を行っていた事務局 PC からは標的型攻撃で悪用されることが多い PlugX と Elirks の検体が発見された。

◆ **富山大学に標的型攻撃**

富山大学の水素同位体科学研究センターへの標的型攻撃により、個人情報や原発の汚染水処理に関する研究成果等が外部流出した可能性があった。[IV] 非常勤の研究者の PC がウイルスに感染したことが原因であった。

＜対策/対応＞

組織（経営者層） [V]

- 組織としての対応体制の確立
  - ・問題に対応できる体制（CSIRT 等）構築
  - ・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） [I VI]

- 被害の予防／対応力の向上
  - ・セキュリティ教育の実施
  - ・情報の管理とルール策定
  - ・組織内 CSIRT の運用
  - ・サイバー攻撃に関する情報共有

組織（システム管理者） [I VII]

- 被害の予防
  - ・システム設計対策
  - ・重要サーバーの要塞化（アクセス制御、暗号化等）
- 被害を受けた後の対策
  - ・ネットワーク分離
- 被害の早期検知
  - ・ネットワーク監視

組織（従業員・職員）

- 情報リテラシーの向上
  - ・セキュリティ教育の受講
- 被害の予防（通常、組織全体で実施）
  - ・OS・ソフトウェアの更新
  - ・セキュリティソフトの導入・更新

組織内部に侵入されることを考慮して、早期検知、重要情報の保護、情報を外部送信させない等の多層防御が重要である。

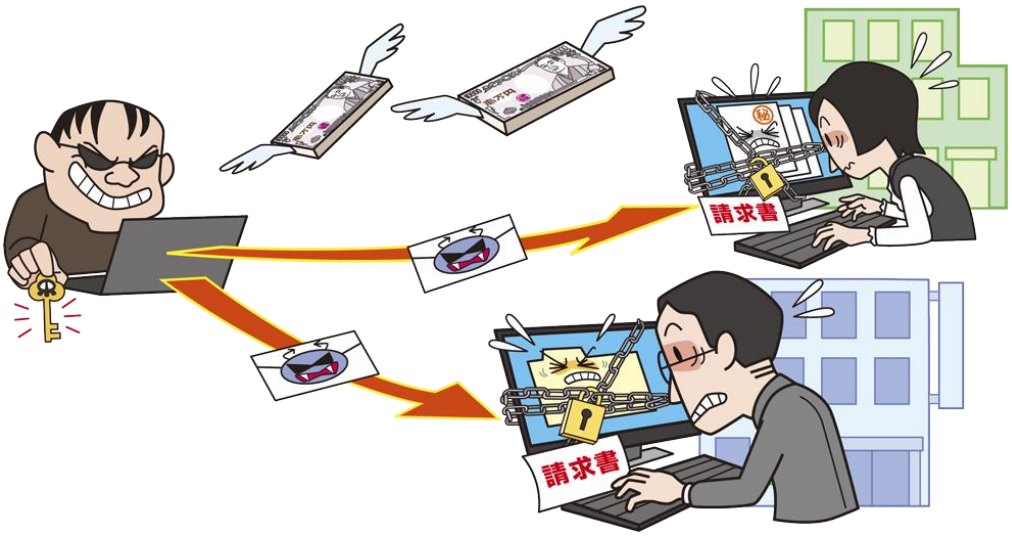
参考資料

I. J-CRAT分析レポート 長期感染の実態 ～1台の感染PCに残された攻撃痕跡の分析～
https://www.ipa.go.jp/security/J-CRAT/report/20170127.html
II. 不正アクセスによる個人情報流出の可能性について
http://www.jtbcorp.jp/jp/160824.html
III. 経団連事務局コンピュータのマルウェア感染
http://www.keidanren.or.jp/announce/2016/1115.html
IV. 富山大学水素同位体科学研究センターに対する標的型サイバー攻撃について（概要）
https://www.u-toyama.ac.jp/news/2016/doc/1011.pdf
V. サイバーセキュリティ経営ガイドライン
http://www.meti.go.jp/policy/netsecurity/mng_guide.html
VI. 標的型攻撃メールの例と見分け方
https://www.ipa.go.jp/security/technicalwatch/20150109.html
VII.「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

個人 2 位

2位 ランサムウェアによる被害

～ランサムウェアによる被害が急増～



ランサムウェアとは、PC やスマートフォンにあるファイルの暗号化や画面のロックを行い、復旧させることと引き換えに金銭を要求する手口に使われるウイルスである。2016 年は前年と比べるとランサムウェアの検知数が増大している。感染した端末だけではなく、その端末からアクセスできる共有サーバーに保存されているファイルも暗号化されるため、ソフトウェアの更新等の感染を予防する対策に加え、定期的にファイルのバックアップを取得し、PC やサーバーから切り離して保管しておくことが望ましい。

＜攻撃者＞

- 犯罪グループ

＜被害者＞

- 組織（サーバー、PC、スマートフォン利用者）

＜脅威と影響＞

ランサムウェアに感染し、PC やスマートフォンに保存されているファイルが暗号化されたり、PC やスマートフォンの操作ができないように画面をロックされたりし、金銭を要求される被害が発生している。

組織の PC やサーバーには、顧客情報や業務運営上の重要な情報が格納されており、それらが暗号化されると、事業継続に支障が出る恐れがある。特に機密情報が保管されているサーバーまで暗号化された場合の影響度は大きい。

なお、金銭を支払ったとしても、確実に復号される保証はないが、事業継続のために金銭を払うケースもある。

また、ファイルの暗号化や画面のロック以外にも、ファイルの破壊やデータを外部に流出させると脅迫するケースも確認されている。

＜攻撃手口＞

◆ **メールの添付ファイルから感染**

- メールにランサムウェアやランサムウェアのダウンローダーを添付し、添付ファイルを開かせることで感染

◆ **ウェブサイトから感染（脆弱性を悪用）**

- メールのリンクをクリックさせる等で悪意あるウェブサイトや改ざんされたウェブサイトを閲覧させることで感染

- 不正広告をクリックさせることで感染（表示のみで感染するケースもある）

＜事例と傾向＞

◆ ランサムウェア被害の急増

2016 年は前年に比べるとランサムウェアの被害が急増している。[I] 2016 年に日本国内で検出されたランサムウェアの件数は、前年比で約 9.8 倍になった。日本で確認されているランサムウェアの大半は英語表記だが、日本語表記で脅迫を行うランサムウェアも確認されている。

◆ 暗号化されたファイルの復号ツールを活用

ランサムウェアによって暗号化されたファイルを復号するツールがセキュリティベンダー等から公開されている。[II] [III] [IV] また、ランサムウェア対策情報を提供しているウェブサイト「The No More Ransom Project」でも、複数の復号ツールを提供している。[V]

これらのツールは全てのランサムウェアに対して有効ということではないが、暗号化されたファイルの復号に活用できる可能性がある。

＜対策/対応＞

ランサムウェアに感染した場合、業務に必要なデータが暗号化され、事業継続できなくなる恐れがある。ランサムウェアに感染しないための対策と感染した場合の手順を決定しておく必要がある。

組織（経営者）

- 組織としての対応体制の確立
  - ・問題に対応できる体制（CSIRT 等）構築
  - ・予算の確保
  - ・セキュリティ対策の指示

組織（システム管理者/PC・スマートフォン利用者）

- 情報リテラシーの向上
  - ・受信メール、ウェブサイトの十分な確認
  - ・添付ファイルやリンクを安易にクリックしない
- 被害の予防
  - ・OS・ソフトウェアの更新
  - ・セキュリティソフトの導入
  - ・フィルタリングツール（メール、ウェブ）の活用
- 被害を受けた後の対策
  - ・バックアップから復旧

    光学メディア（DVD-R、BD-R 等）、外付け HDD、USB メモリ等、外部記録媒体へ定期的にバックアップを行う。但し、バックアップに使用する記録媒体は、バックアップするときのみ、PC やスマートフォンに接続すること。常時接続していると、バックアップしたファイルもランサムウェアの感染対象となる。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。
  - ・復号ツールの活用

    ランサムウェアをセキュリティソフト等で駆除した上で、復号ツールを実行することで、暗号化されたファイルを復号できる可能性がある。

参考資料

I. 日本と海外の脅威動向を分析した「2016年年間セキュリティラウンドアップ」を公開
http://www.trendmicro.co.jp/jp/about-us/press-releases/articles/20170301015352.html
II. Trojan-Ransom.Win32.Rannoh の感染により影響を受けたファイルを復号化するユーティリティ
https://support.kaspersky.co.jp/viruses/disinfection/8547
III. ランサムウェア ファイル復号ツール
https://esupport.trendmicro.com/support/vb/solution/ja-jp/1114210.aspx
IV. ESET Releases Decryptor for Recent Variants of TeslaCrypt Ransomware
https://www.eset.com/us/about/newsroom/press-releases/eset-releases-decryptor-for-recent-variants-of-teslacrypt-ransomware/
V. The No More Ransom Project
https://www.nomoreransom.org/

個人 6 位

3位 ウェブサービスからの個人情報の窃取

～犯罪グループの攻撃による甚大な被害～

ウェブサービスの脆弱性を悪用し、ウェブサービス内に登録されている住所や氏名やクレジットカード情報が窃取される事件が 2016 年も引き続き発生している。数 10 万件の個人情報等の重要な情報が漏えいする事件も発生しており、ウェブサービスを運営・管理する組織は適切な対応が求められる。

＜攻撃者＞

- 犯罪グループ

＜被害者＞

- 組織（ウェブサービス運営者）
- 個人（ウェブサービス利用者）

＜脅威と影響＞

ウェブサービスには多くの個人情報等が登録されている。例えば、ショッピングサイトであれば個人情報を含む重要な情報（氏名・性別・生年月日、クレジットカード情報等）が登録されている。また、SNS であれば自身の情報に加え、友人の個人情報が登録されていることもある。

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、利用しているソフトウェアのバージョン等を適切に管理していない場合、ソフトウェアの脆弱性を内在したままサービス提供している可能性もある。

このようなウェブサービスは内在している脆弱性を攻撃され、登録してある重要な情報を窃取されたり、その情報を不正使用されたりする被害が確認されている。ウェブサービスはその性質上、インターネットで提供されるため、攻撃者のターゲットにされやすい。

＜攻撃手口＞

◆ 開発時に作りこんだウェブアプリケーションの脆弱性を悪用

ウェブサービスを開発する際にセキュリティを十分に考慮していない場合、脆弱性を作り込んでしまう可能性がある。例えば、SQL インジェクション等の情報漏えいにつながる脆弱性を悪用され、個人情報を含む重要な情報を窃取される。

◆ ソフトウェアの脆弱性を悪用

ウェブサービスは OS・ミドルウェア・CMS 等の複数のソフトウェアで構成されている。その中

には、機能を実現するためにウェブサービスで共通的に使われているソフトウェア（OpenSSL、Apache Struts、WordPress 等）もある。このようなソフトウェアの脆弱性を悪用し、個人情報を含む重要な情報を窃取される危険性が高くなる。これらのソフトウェアの脆弱性は攻撃手法が判明すると複数のウェブサービスを攻撃できるため、標的にされやすい。

＜事例と傾向＞

◆ **民間放送会社に不正アクセスされ、最大 43 万件の個人情報漏えいの可能性**

日本テレビのウェブサイトへの不正アクセスが発生した。ウェブサイトで利用しているソフトウェアの OS コマンドインジェクションの脆弱性を突かれ、最大 43 万件の個人情報が漏えいした可能性がある。[I]

◆ **化粧品通販サイトに不正アクセスされ、個人情報約 42 万件が流出した可能性**

システムの脆弱性を突いたイプサの通販サイトへの不正アクセスにより、登録している顧客のクレジットカード情報や個人情報約 42 万件が漏えいした可能性がある。[II]

＜対策/対応＞

組織（ウェブサービス運営者）

● 被害の予防

・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」[III] や「Web システム/Web アプリケーションセキュリティ要件書」[IV] 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。セキュリティ要件を満たすための予算確保も忘れてはならない。なお、クラウドサービス等をインフラ基盤として利用している場合、クラウドサービスのベンダーに対して、セキュリティ対策の内容を確認することも重要である。

・OS・ソフトウェアの更新

OS やミドルウェアの最新バージョンやパッチが公開されたら、パッチを適用し、最新の状態に保つ必要がある。[V]IPA の重要なセキュリティ情報 [VI] 等の各組織からの注意喚起情報を日々確認し、情報が発信されたら迅速に対応する。また、保守作業があることを想定し、保守作業の予算確保を事前に行っておくことも重要である。

・WAF・IPS の導入

仮に未対策の脆弱性が存在していても被害を防げる可能性がある。なお、管理者は対策情報（設定等）を定期的に更新する作業があることを予め想定し、予算や体制を確保しておくこと。

● 被害の早期検知

・適切なログの取得と継続的な監視

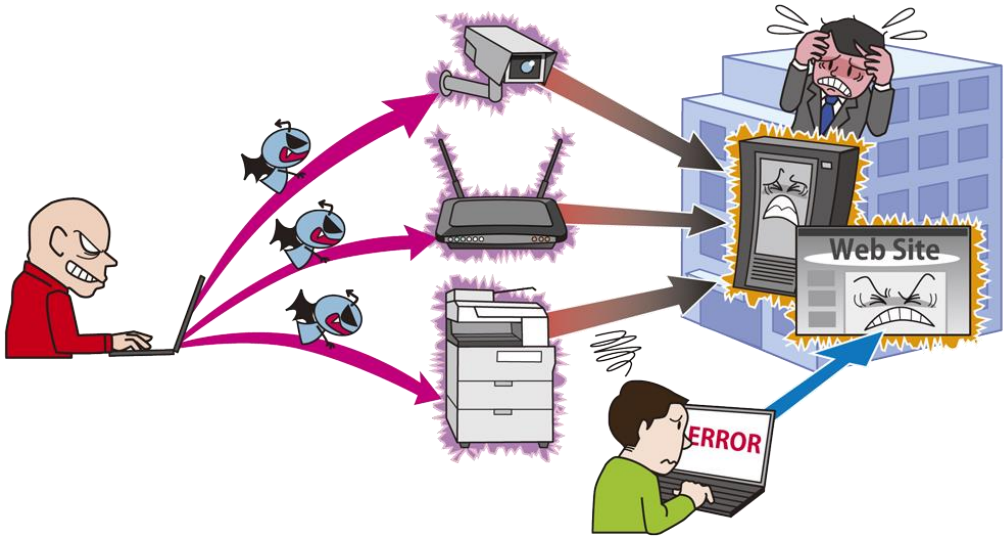
参考資料

I. 日テレに不正アクセス - 最大43万件の個人情報が漏洩した可能性
http://www.security-next.com/069154/
II. クレカ情報5.6万件含む個人情報42万件が流出した可能性 - イプサ
http://www.security-next.com/076305/
III. 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
IV. 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
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
http://www.ipa.go.jp/files/000038393.pdf
VI. 重要なセキュリティ情報とは
https://www.ipa.go.jp/security/announce/about.html

個人ランク外

4位 サービス妨害攻撃によるサービスの停止

～ボットネットウイルスの普及に伴う攻撃の大幅増加～



攻撃者に乗っ取られた IT 機器等から構成されたボットネットにより、企業や民間団体等、組織のウェブサイトや組織の利用している DNS サーバーに大量のアクセスを行う DDoS（分散型サービス妨害）攻撃が急増した。攻撃によりウェブサイトや DNS サーバー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、ウェブサイト運営者が対応に追われた。

＜攻撃者＞

- 犯罪グループ（ハクティビスト含む）
- 愉快犯

＜被害者＞

- 組織、個人

＜脅威と影響＞

インターネットの普及に伴い、官公庁や企業、民間団体等、多くの組織がウェブサイトを持ち、インターネットを使って情報の発信やサービスの提供を行っている。そのウェブサイトや組織の利用している DNS サーバーに DoS/DDoS 攻撃を仕掛け、閲覧を不可能にする等の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社会混乱や脅迫等である。攻撃には DDoS 攻撃を代行するサービスが利用されることがある。

＜攻撃手口＞

◆ **DDoS 攻撃**

DDoS 攻撃には、主に以下の手口が使われる。

- ボットネットの利用

  予め構築されたボットネットに攻撃命令を出し、標的組織のウェブサイトや組織の利用している DNS サーバーへの想定外の大量アクセスによる負荷をかける攻撃
- リフレクター攻撃

  送信元を標的組織のサーバーを騙って、脆弱な多数のルーターや DNS サーバー等に通信を送り、応答結果を標的組織に送り付け負担をかける攻撃
- 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、標的組織

ドメイン名の権威 DNS サーバーに大きな負荷をかける攻撃

また、DDoS を代行する不法なサービスを利用し、攻撃を行うこともある。

＜事例と傾向＞

◆ 主義主張のための DDoS 攻撃

JICA（国際協力機構）や JCR（日本格付研究所）等のウェブサイトが DDoS 攻撃を受けアクセスしづらい状態となった。攻撃者である犯罪グループ（ハクティビスト）は主義主張のため日本を対象とした攻撃を活発化させており、今回の攻撃もその一環と考えられる。[I]

◆ DDoS 攻撃で金銭を脅迫、攻撃者が逮捕されるケースも

DDoS 攻撃を仕掛ける前または仕掛けた後に脅迫してビットコイン等の仮想通貨を要求する事例が確認されている。犯罪が発覚し、実際に逮捕された攻撃者もいる。[II]

◆ ボットネットウイルスの拡散

2016 年 9 月に毎秒 1 テラビットという大規模な DDoS 攻撃が確認された。[III] 原因は、IoT 機器を踏み台にボットネットを構築するウイルス「Mirai」であった。同月末に、ハッカーが集まるフォーラムでその「Mirai」のソースコードが公開され、そのソースコードを流用したウイルスの拡散につながった。ボットネットによる攻撃件数は 2015 年の 1960 万件だったのに対し、6.4 倍の 1 億 2,600 万件まで急増した。[IV]「Mirai」のソースコードの公開が件数の増加につながっていると考えられる。

＜対策/対応＞

組織（IoT 機器ベンダー）

- 被害の予防
  - ・脆弱性対策

    IoT 機器への不正アクセスやウイルス感染でシステムを乗っ取られ、ボットネットとして悪用される。攻撃の踏み台にされないためにも、IoT 機器の脆弱性対策や対応を強化する必要がある。[V]

組織

- 被害の予防
  - ・DDoS 攻撃の影響を緩和する ISP によるサービスの利用

    既に ISP のサービスを利用している場合は、最大許容量の見直しを行う。また、ISP で DDoS 対策を行っている場合はそれを利用する。
  - ・システムの冗長化等の軽減策
- 被害を受けた後の対策
  - ・通信制御（DDoS 攻撃元をブロック等）
  - ・ウェブサイト停止時の代替サーバーの用意と告知手段の整備

    DDoS 攻撃を受けてサービス停止することを想定して、切り替えるため、またはサービスの利用者を混乱させないために状況を連絡できるよう代替サーバーまたは SNS の公式アカウント等の告知手段を用意しておくことも重要である。

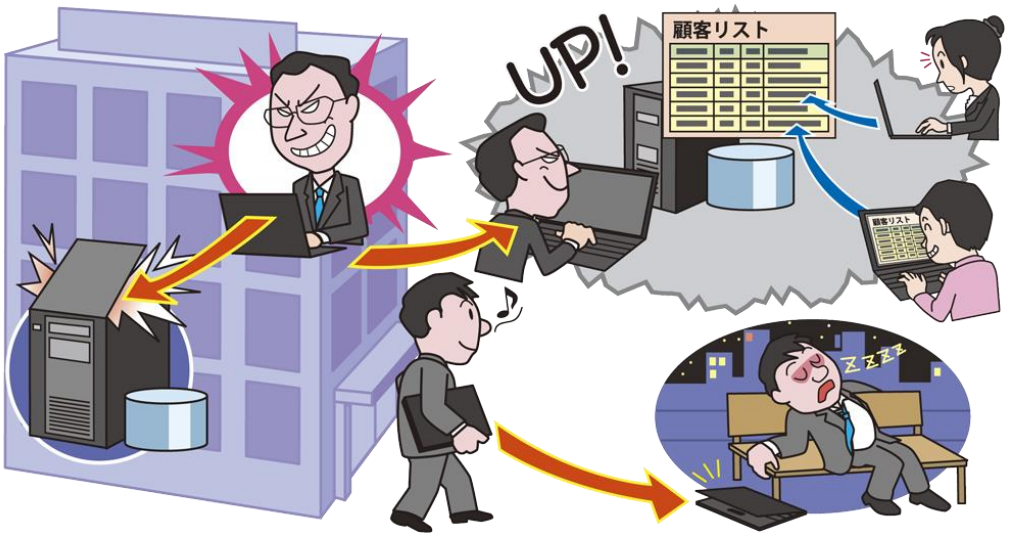
参考資料

I. JICAなどのサイトが閲覧しづらい状態――またアノニマスのDDoS攻撃か
http://www.atmarkit.co.jp/ait/articles/1602/19/news078.html
II. ユーロポール、セブン銀行など攻撃のDDoS攻撃グループ「DD4BC」を逮捕
http://news.mynavi.jp/news/2016/01/14/549/
III. 毎秒1テラビットという史上空前のDDoS攻撃が発生、攻撃元はハッキングされた14万5000台ものウェブカメラ
http://gigazine.net/news/20160929-record-breaking-ddos/
IV. IoT製品乗っ取りサイバー攻撃1億2600万件…家電や通信機器から発信　昨年、前年の6倍に
http://www.sankei.com/west/news/170120/wst1701200014-n1.html
V. 「IoT開発におけるセキュリティ設計の手引き」を公開
https://www.ipa.go.jp/security/iot/iotguide.html

個人ランク外

5位 内部不正による情報漏えいとそれに伴う業務停止

～内部不正を許さない管理・監視体制を～



組織内部の職員や元職員による、情報の不正な持ち出し等の不正行為が起きている。不正に持ち出した情報の紛失により情報漏えいにつながるケースがある。内部不正を防ぐには、制約や罰則を設けるといった管理的な対策に加えて、適切なアクセス権限の設定やログの収集・管理等の技術的な対策を取り、不正行為を防止すると共に、検知と追求が可能な環境であることを職員に周知する必要がある。

＜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＞

組織への私怨や金銭目的等から、悪意を持った元職員が離職前に内部情報を持ち出し、それを公開・売買することで組織に損害を与えることがある。また、職員が自宅で仕事をするために書類を持ち出し、その書類を紛失してしまい、情報漏えいにつながることもある。

内部不正による影響は、情報漏えい、社会的信用の失墜、ビジネス機会の損失、賠償等の金銭的ダメージ、株価下落等が連鎖的に発生する。

＜発生要因＞

◆　職場環境や処遇の不満

内部不正を犯す動機は、当人にとっての不当な解雇、業務多忙、給与や賞与、人事評価の不満といった処遇面に関することが多く、報復や不正な金銭取得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になり、必要以上の権限を付与してしまうと、本来はアクセスできないはずの人が情報資産にアクセスできるようになる。アクセス権限の過剰な付与が引き金となり、内部不正が起こる。

なお、正当なアクセス権限を持つ職員が悪意を持った場合には、アクセス権限の及ぶ範囲で不正行為が可能となる。

◆ **システム操作記録と監視の未実施**

ログ管理（システム操作の記録と監視）を行っていない組織では、内部不正があっても不正に気づきにくく、不正の発覚が遅れる。これにより被害が拡大したり、内部不正の発覚後の調査が困難になったりし、内部不正のリスクが高まる。

＜事例と傾向＞

◆ **YJFX!元従業員の持ち出しにより顧客情報 18 万件が流出**

元従業員によって不正に持ち出された顧客情報が、インターネット上に保存され、外部から第三者が閲覧可能な状態となっており、一部が実際に閲覧されていた。[I]

◆ **職員が持出データを酒に酔って紛失**

職員が、個人情報が含まれる業務用ファイルが保存されたハードディスクを、セキュリティポリシーで持ち出しが禁止されているにもかかわらず持ち出した。帰宅途中に泥酔し、居眠りしていたところ、ハードディスクの所在がわからなくなった。職員は自宅で作業を行うために持ち出していたという。[II]

＜対策/対応＞

組織

【運用管理的対策】

- 被害の予防
  - ・資産の把握・体制の整備

    組織が保持する資産を重要度等で分類し、経営層が責任を持ち、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]
  - ・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
  - ・罰則の周知と相互監視の強化

    紛失・漏えいを隠蔽した場合、より懲罰が重くなることを周知することも有効である。
  - ・情報の取扱教育の実施

【技術的対策】

- 被害の予防
  - ・アカウント、権限の管理・定期監査
  - ・重要情報の管理・保護（アクセス制御、暗号化）
- 被害の早期検知
  - ・システム操作の記録・監視

IPA で行った内部不正に関する実態調査[IV]では、効果的な内部不正対策として、アクセスログの監視が上位となっており、効果が期待できる。また、併せてアクセスログを取得していることを周知することも不正防止に有効である。

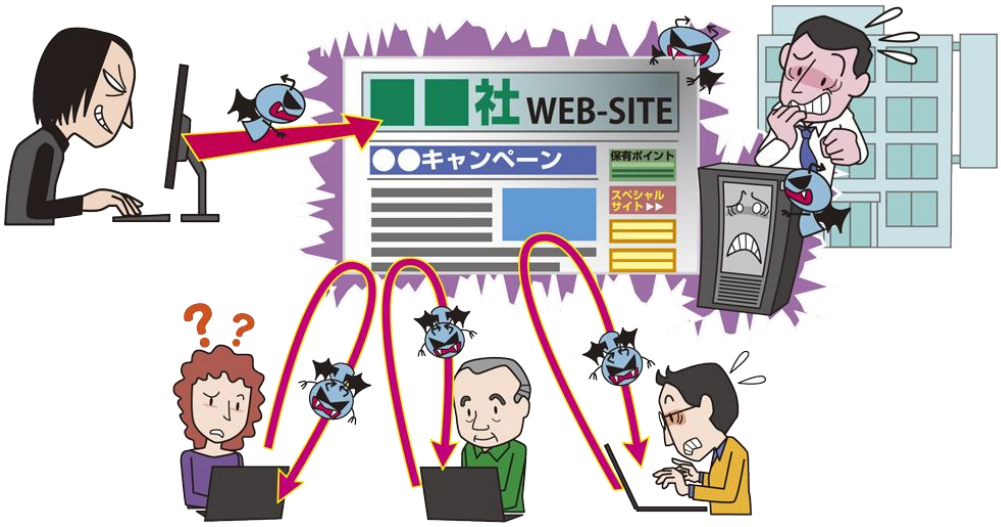
参考資料

I. 顧客情報持ち出しに関するご報告
http://www.yjfx.jp/20160202news/
II. 職員が持出データを酒に酔って紛失 - 川口市
http://www.security-next.com/074773
III. 組織における内部不正防止ガイドライン
https://www.ipa.go.jp/files/000057060.pdf
IV. 「内部不正による情報セキュリティインシデント実態調査」報告書について
https://www.ipa.go.jp/security/fy27/reports/insider/

個人ランク外

6位 ウェブサイトの改ざん

～気づかぬうちにウイルスをばら撒くウェブサイトに～



コンテンツ管理システム（CMS）等に存在する脆弱性を悪用し、ウェブサイトが改ざんされる事例が今年も発生している。復旧までウェブサイトを停止することになり、特にオンラインショッピング等を運営している場合、事業上の被害が大きい。また、閲覧者がウイルスに感染するように改ざんされた場合、社会的信用を失うことにつながる。

＜攻撃者＞

- 犯罪グループ(ハクティビスト含む)
- 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(ウェブサイトの利用者)

＜脅威と影響＞

脆弱性を悪用され、ウェブサイトを改ざんされる被害が引き続き発生している。改ざんされると、政治的主張等を掲載されたり、ウイルスを配布する水飲み場型攻撃に悪用されたりする。

特に、水飲み場型攻撃では、見た目では分からないようにウイルスやウイルス配布サイトへのリンクをウェブサイトに埋め込まれるため、ウェブサイトの管理者や利用者が気づくのが遅れ、長期間にわたって利用者がウイルスに感染する等の被害を与え続けることになる。

また、CMS の脆弱性が開発元等により公表された場合、その CMS で作られたウェブサイトは一律で攻撃を受け、改ざんの被害が急増する恐れがある。

＜攻撃手口＞

◆ **開発時に作りこんだウェブアプリケーションの脆弱性を悪用**

ウェブアプリケーションの開発時に脆弱性対策を怠り、脆弱性を作り込んでしまう可能性がある。その脆弱性を悪用され、ウェブサイトを改ざんされる。

◆ **ソフトウェアの脆弱性を悪用**

広く一般に普及しているソフトウェア製品の脆弱性が公開され、さらに攻撃手法が判明した場合、攻撃者は広範囲を攻撃することが可能とな

る。そのため、OS・ミドルウェア等のサーバーソフトウェアや WordPress 等の CMS 及びそのプラグインの脆弱性が狙われやすい。特に、それらの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恐れがある。

◆ **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。

＜事例と傾向＞

◆ **時刻表のページを改ざんし、外部ウェブサイトへ誘導**

高松空港のホームページが改ざんされた。時刻表のページのキャッシュを表示すると、特定の広告サイトに誘導する文字列が表示されていた。改ざんの原因として 2 つの可能性があり、1 つは、管理用 PC がウイルスに感染し、ID・パスワードが窃取された可能性、もう 1 つは、ホームページの管理用ツールに脆弱性があり、攻撃を受け、管理者権限を奪取された可能性がある。[I]

◆ **動物園の HP が改ざん**

動物園のホームページ上のイベント告知欄が英語で「ハッキングした」と書き換えられ、「動物を自由にしろ」等のメッセージが記載されていた。この被害により、運営側はホームページの公開を一時中止した。[II]

◆ **CMS の脆弱性を悪用した攻撃**

2016 年 10 月、CMS の「Joomla!」の深刻な脆弱性が修正されたバージョンを公開後、24 時間たたないうちに脆弱性を探る動きが見られ、36 時間程で悪用を試みる動きが急増したと報告された。修正バージョンを利用していない Joomla!を使用したウェブサイトが狙われ、修正バージョン公開後 3 日間で 2 万 7,000 件以上の脆弱性を悪用した攻撃が観測された。[III]

＜対策/対応＞

組織（ウェブサイト提供ベンダー）

- 情報リテラシーの向上
  - ・アカウント・パスワードの管理
- 被害の予防
  - ・サーバーソフトウェアの更新

    利用しているソフトウェアの製品名やバージョンを把握し、利用製品の脆弱性対策情報をタイムリーに収集する。
  - ・ウェブアプリケーションの脆弱性対策 [IV]
  - ・管理用端末の OS・ソフトウェアの更新
  - ・管理用サービスは多要素認証を利用
  - ・管理用サービスへのアクセス制限
  - ・利用者に多要素認証の仕組みを提供
  - ・セキュリティを考慮したインフラ基盤

    クラウドサービス等をインフラ基盤として利用している場合、クラウドサービスのベンダーに対して、セキュリティ対策の内容を確認することも重要である。
- 被害の早期検知
  - ・改ざん検知

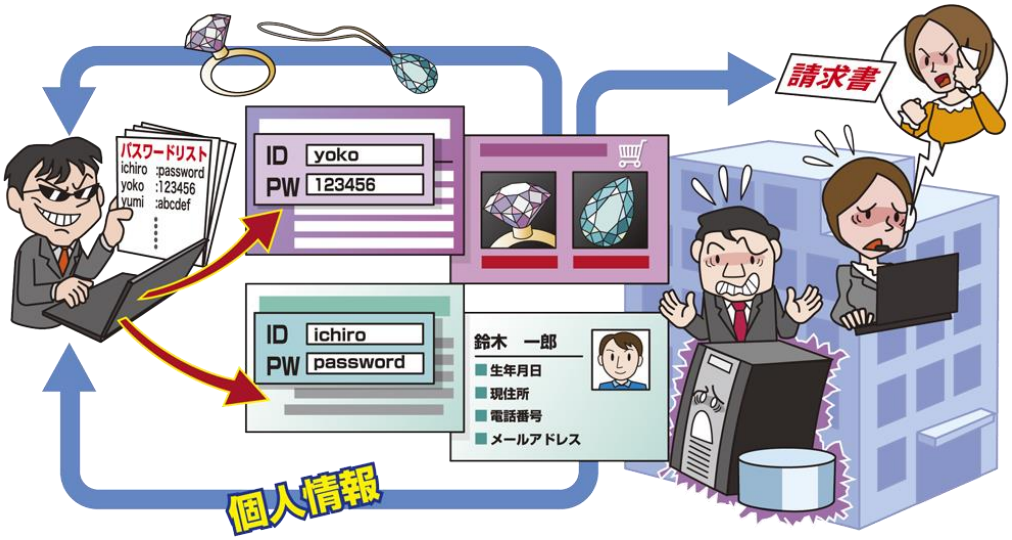
参考資料

I. 高松空港ホームページの改ざんについて（第2報）
http://www.pref.kagawa.lg.jp/content/dir5/dir5_2/dir5_2_1/w462cu160826182142.shtml
II. 都立動物園・水族園のホームページへの不正アクセスについて（続報）
http://www.metro.tokyo.jp/INET/OSHIRASE/2016/07/20q78600.htm
III. Joomla!の脆弱性突く攻撃、パッチ公開直後から発生　既にハッキングの恐れも
http://www.itmedia.co.jp/enterprise/articles/1611/02/news086.html
IV. 安全なウェブサイトの作り方
https://www.ipa.go.jp/security/vuln/websecurity.html

個人 4 位

7位 ウェブサービスへの不正ログイン

～多要素認証の活用を～



2016 年に確認されたウェブサービスへの不正ログインの多くがパスワードリスト攻撃によって行われている。ウェブサービスの利用者がパスワードを使い回している場合、不正ログインが行われる恐れがある。ウェブサービスの提供者は、不正ログインされないように多要素認証等のセキュリティ機能をウェブサービスの利用者に提供する必要がある。

＜攻撃者＞

- 犯罪グループ
- 犯罪者（ストーカー等）

＜被害者＞

- 組織（ウェブサービスの運営者）
- 個人（ウェブサービスの利用者）

＜脅威と影響＞

窃取や推測されたパスワードによりウェブサービスへ不正ログインされる被害が引き続き起きている。ウェブサービスへの不正ログインによる影響は、提供しているウェブサービスの機能によって変わる。例えば、インターネットバンキングの場合は、不正送金により、金銭被害が発生する。ショッピングサイトであれば、氏名や住所、電話番号、クレジットカード情報等が窃取されたり、不正な購買やポイント等の盗用が行われたりする。また、オンラインゲームサイトであれば、勝手に支払いが行われたり、ゲーム内アイテムを窃取されたりする。

＜攻撃手口＞

◆ パスワードリスト攻撃

他のウェブサイトから漏えいした ID とパスワードの組み合わせを利用して攻撃する手法である。複数のウェブサイトで同じ ID とパスワードを使い回している場合、1 つのウェブサイトの ID とパスワードが漏えいしただけで、他のウェブサイトにも被害が拡大する。

◆ パスワード推測攻撃

利用者が使いそうなパスワードを推測して不正ログインを試みる攻撃。例えば、ID とパスワードが同一、パスワードに単純な単語や、「123456」や「abcdef」のような連続した英数字

を使用している場合、攻撃者にパスワードを推測される可能性がある。SNS で公開している誕生日等の情報をパスワードにするのも危険だ。[I] また、「qwerty」といった一見ランダムな文字に見えるが実はキーボード上の隣接している文字も推測されやすい。

＜事例と傾向＞

◆ **ブログへの不正ログイン**

ブログサービス「Ameba」において、2016 年 5 月と 11 月に不正ログインが行われた。[II] 特に 11 月は、約 59 万件の不正ログインを確認している。[III] なお、ブログの登録情報の改ざんは確認されていない。他のウェブサイトで漏えいしたパスワードが使われた可能性がある。

◆ **オンラインショッピングへの不正ログインによるポイントの不正利用**

オンラインショッピングサイト「ビックカメラドットコム」において、不正ログインが行われ、ポイントを不正に利用される被害が発生した。[IV] また、氏名、住所等の利用者の情報も閲覧された可能性があった。他のウェブサイトで漏えいしたパスワードが使われた可能性がある。

◆ **SNS への不正ログイン**

イラストを投稿できる SNS「pixiv」において、2016 年 11 月 29 日から 12 月 2 日にかけて、パスワードリスト攻撃が行われた。これにより約 3,600 件のアカウントが不正ログインされ、登録しているメールアドレス、生年月日、性別が閲覧された可能性がある。[V]

＜対策/対応＞

組織（ウェブサービスの運営者）

- 被害の予防

・簡単なパスワードを許可しない

容易に推測できるパスワードは設定できないようにする。「password」「123456」「abcdef」等の単純な単語や連続した英数字は登録できないようにすることで、パスワードを推測されにくくすることができる。

・多要素認証の導入

パスワードによる認証に加え、サーバー側で追加認証用のワンタイムパスワードを生成して登録したメールアドレスに送信する、追加認証用のワンタイムパスワードをクライアント側で生成するスマートフォンアプリを使用する等、実装方法は複数存在する。また、仮に ID やパスワードが窃取されても、金銭等の最終的被害を回避することもできる。

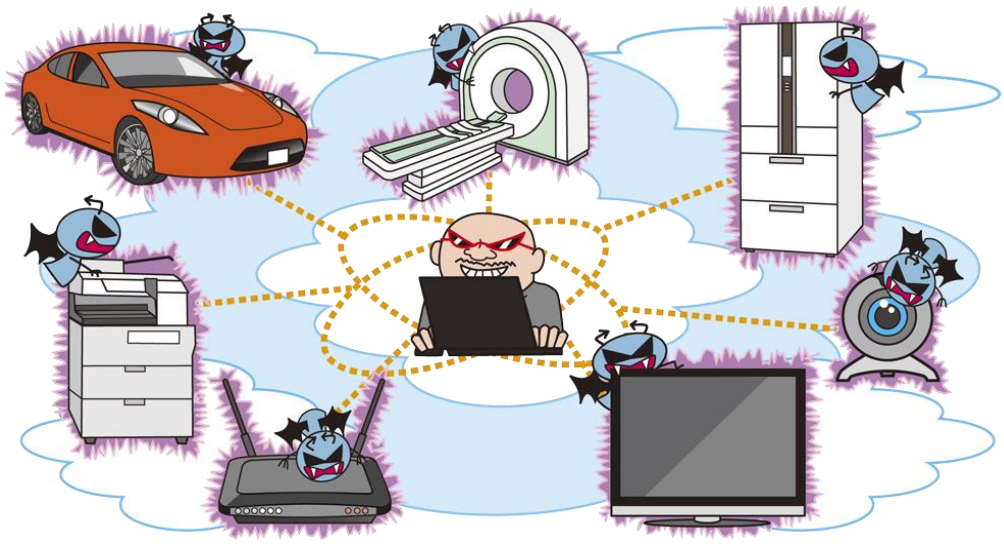
参考資料

I. SNSで公開している誕生日などの情報を使ったパスワード設定は推測されやすくNG
https://www.ipa.go.jp/security/anshin/mgdayori20161221.html
II. 「Ameba」への不正ログインに関するご報告とパスワード再設定のお願い
http://ameblo.jp/staff/entry-12159141397.html
http://ameblo.jp/staff/entry-12224046295.html
III. 「Ameba」で約59万件の不正ログイン--パスワードリスト型攻撃で
https://japan.cnet.com/article/35092962/
IV. 当社インターネットショッピングサイトでの会員ID、パスワード不正使用被害について
http://www.biccamera.com/bc/c/info/report/20160303.jsp?160303
V. 【重要】pixivの一部アカウントに対する「なりすましログイン」の報告とパスワード変更のお願い
http://www.pixiv.net/info.php?id=3897

個人ランク外

8位 IoT 機器の脆弱性の顕在化

～IoT 機器のボットネットを悪用した大規模な DDoS 攻撃を観測～



2016 年は、自動車や医療機器の脆弱性が昨年に続いて公表された。また IoT（Internet of Things）機器の脆弱性を悪用してボット化することで、インターネット上のサービスやサーバーに対して大規模な DDoS 攻撃が行われる等、IoT 機器の脆弱性に関する脅威が顕在化している。

＜攻撃者＞

- 犯罪グループ

＜被害者＞

- 組織（官公庁、企業）
- 個人（顧客、サービス利用者）

＜脅威と影響＞

昨今、情報家電、オフィス機器、医療機器、自動車、産業用設備・機器、制御システム等、多種多様な機器がネットワークを介してつながるようになってきた。これまではネットワークにつながることを想定していなかった機器がインターネット上でつながることにより、攻撃者は多数のインターネット上の IoT 機器の脆弱性を悪用することができる。そして、その IoT 機器を乗っ取り、DDoS 攻撃等をインターネット上のサービスやサーバーに対して仕掛け、公開サービスを利用不可にする、といった被害も報道されている。また、医療機器等の命に関わる IoT 機器にも脆弱性が確認されており、脆弱性を悪用された場合のリスクが大きい。

＜攻撃手口＞

- **IoT 機器の脆弱性を悪用してウイルスに感染させる**
- **ウイルス感染した IoT 機器をボットとして悪用して、インターネット上にウイルス感染した機器を増殖させる**
- **ボットに感染した IoT 機器群を攻撃者が遠隔から操作し、ウェブサイトの公開サービス等を DDoS 攻撃で麻痺させる**
- **IoT 機器からの機密情報を窃取する**

＜事例と傾向＞

◆ **電気自動車の専用アプリに遠隔操作が可能となる脆弱性**

2016 年 2 月、電気自動車の専用アプリにエアコン等を遠隔操作できてしまう脆弱性があることが公表された。[I]

アプリの API には認証の仕組みが実装されておらず、個々の車に割り当てられている車両識別番号（VIN）の下 5 ケタさえ分かれば、他の車両を制御できてしまうことが判明している。

◆ **医療機器にも脆弱性が存在、糖尿病患者が使うインスリンポンプで遠隔操作が可能となる脆弱性**

2016 年 10 月、糖尿病患者へのインスリン注入に使われるインスリンポンプに、患者の治療情報や機器のデータを取得されたり、機器を操作されたりする脆弱性が存在していることが公表された。[II]

製品開発元の情報によると、ファームウェアのアップデートをリリースする予定は無く、当該製品を使用している患者や医療関係者に通知を送付すること等の対応を実施した。

◆ **海外製ルーターの脆弱性を標的としたアクセスを観測**

2016 年 11 月、警察庁では、インターネット定点観測システムにおいて、海外製ルーターの脆弱性を標的としたアクセスを多数観測した。[III]

脆弱性を悪用した攻撃を受けたルーター等の機器がボット化し、DDoS 攻撃の踏み台となったり、感染拡大を狙ってさらなる探索を行ったりする恐れがある。

＜対策/対応＞

組織（IoT 機器の開発者） [IV]

- 被害の予防
  - ・セキュアプログラミング技術の適用
  - ・脆弱性の解消（脆弱性検査、ソースコード検査、ファジング等）
  - ・ソフトウェア更新手段の自動化
  - ・分り易い取扱説明書の作成
  - ・迅速なセキュリティパッチの提供
  - ・不要な機能の無効化（telnet 等）
  - ・安全なデフォルト設定
  - ・利用者への適切な管理の呼びかけ

  IoT 機器の利用者は必ずしも情報リテラシーが高いとは限らない。マニュアルやウェブページ等で適切な管理を呼びかけることも重要である。

組織（システム管理者・利用者）、個人

- 情報リテラシーの向上
  - ・機器使用前に取扱説明書を確認
- 被害の予防
  - ・不要な機能の無効化（telnet 等）

  利用上の注意や初期設定から変更が必要な設定等を把握し、適切に運用する。
  - ・外部からの不要アクセスを制限
  - ・ソフトウェアの更新（自動化設定を含む）

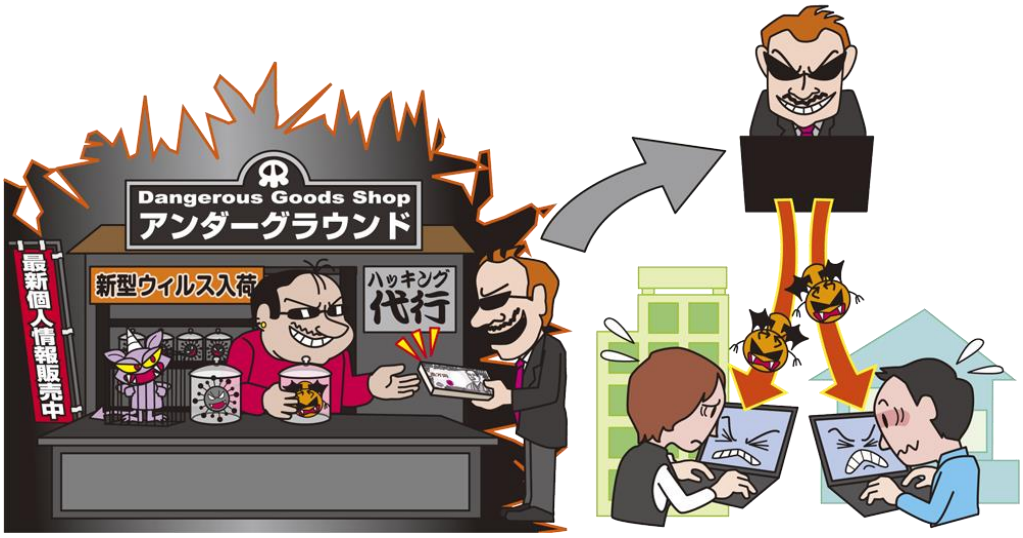
参考資料

I. 日産「リーフ」のアプリに脆弱性、他人の車を遠隔操作可能に
http://www.itmedia.co.jp/enterprise/articles/1602/25/news067.html
II. Animas OneTouch Ping に複数の脆弱性
https://jvn.jp/vu/JVNVU95089754/
III. 海外製ルータの脆弱性を標的としたアクセスの急増等について
https://www.npa.go.jp/cyberpolice/detect/pdf/20161221.pdf
IV. 「IoT開発におけるセキュリティ設計の手引き」の公開
https://www.ipa.go.jp/security/iot/iotguide.html

個人ランク外

9位 攻撃のビジネス化（アンダーグラウンドサービス）

～サイバー犯罪を目的としたサービスやツールの売買～



犯罪に使用するためのサービスやツールがアンダーグラウンド市場で取り引きされ、これらを悪用した攻撃が行われている。攻撃に対する専門知識に詳しくない者でもサービスやツールを利用することで、容易に攻撃を行えるため、サービスやツールが公開されると被害が広がる恐れがある。

＜攻撃者＞

- **犯罪グループ**

＜被害者＞

- **組織（PC 利用者、**システム管理者）
- **個人**

＜脅威と影響＞

サイバー攻撃を目的としたサービスやツールがアンダーグラウンドで取り引きされている。IT 技術を熟知していなくても、これらを利用して、容易にサイバー攻撃を行うことができる。アンダーグラウンドの商用化されたサービスやツールとして、例えば、エクスプロイトキット[I]やオンライン銀行詐欺ツール、DDoS 代行サービス等がある。

これらを利用した攻撃を受けた場合、ウイルスに感染し、金銭を窃取されたり、サーバーに DDoS 攻撃をされ、業務を妨害されたりする。

＜攻撃手口＞

◆ **ツールやサービスを購入し攻撃**

アンダーグラウンドで購入したサービスやツールを利用して攻撃を行う。脆弱性の悪用やボットネットの利用等、ツールやサービスの種類によって攻撃方法は異なる。

＜事例と傾向＞

◆ **エクスプロイトキットを使ったランサムウェア拡散**

エクスプロイトキットを利用して、ランサムウェアを拡散させる事例が確認された。[II] エクスプロイトキットとは、ソフトウェアや OS に内在する脆弱性を確認したり、その脆弱性を悪用したりするツールのことである。犯罪グループは、アンダーグラウンドでエクスプロイトキットを購入・レンタルし、ランサムウェアを拡散するために利用している。

◆ **インターネットバンキング詐欺ツールによる金融取引関連情報の窃取**

インターネットバンキング詐欺ツール「Gozi」等によって金融関連情報を窃取され、銀行口座から不正送金が行われてしまう事例が確認された。[III] [IV] この詐欺ツールは金融関連情報を窃取する等の機能があるウイルスである。利用者が感染した端末を使用し、インターネットバンキングを利用すると、ID やパスワード等の情報が窃取され、銀行口座から不正送金が行われてしまう恐れがある。

◆ **海外において DDoS 代行サービスの利用者が逮捕されるケースも**

欧州サイバー犯罪センターと 13 カ国の警察当局が国際的に連携し、DDoS 代行サービスの利用者に対して拘束や警告を行った。[V] 拘束や警告された人の多くは 20 歳以下の若者達であった。欧州刑事警察機構は、今回の逮捕に関して、サイバー攻撃者予備軍にとって教訓となることを期待している、と述べている。

＜対策/対応＞

攻撃に悪用するツールやサービスの目的・仕様によって対策は異なる。そのため、以下の対策は一部を記載している。詳しい対策方法については、本書「10 大脅威 2017」の他の脅威の対策等を参考にして欲しい。

組織（PC 利用者）

- 情報リテラシーの向上
  - ・セキュリティ教育の受講
  - ・受信メール、ウェブサイトの十分な確認
  - ・添付ファイルやリンクを安易にクリックしない
  - ・事例・手口の情報収集
- 被害の予防
  - ・OS・ソフトウェアの更新
  - ・セキュリティソフトの導入
  - ・多要素認証等の強い認証方式の利用
- 被害の早期検知
  - ・不審なログイン履歴の確認
- 被害を受けた後の対策
  - ・バックアップからの復旧

組織（システム管理者）

- 被害の予防
  - ・DDoS 攻撃の影響を緩和する ISP 等によるサービスの利用
  - ・システムの冗長化等の軽減策
- 被害を受けた後の対策
  - ・通信制御（DDoS 攻撃元をブロック等）
  - ・ウェブサイト停止時の代替サーバーの用意（告知手段）

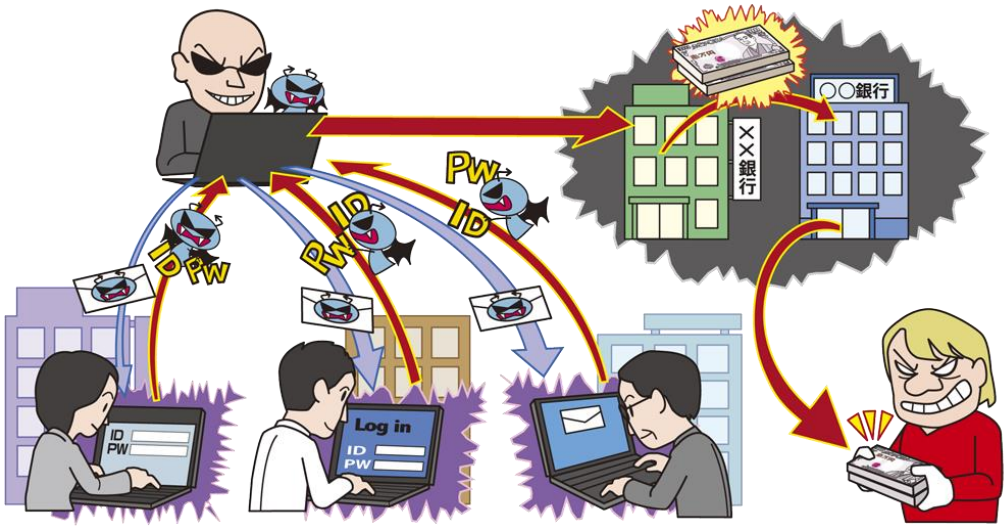
参考資料

I. エクスプロイトキットとは
http://about-threats.trendmicro.com/RelatedThreats.aspx?language=jp&name=Exploit+Kit
II. エクスプロイトキットとランサムウェアの密接な関係
http://blog.trendmicro.co.jp/archives/14030
III. アンダーグラウンドが加速させるランサムウェアの脅威
http://www.trendmicro.co.jp/cloud-content/jp/pdfs/security-intelligence/threat-report/pdf-sr2016q3-20161116-01.pdf?cm_sp=threat-_-sr2016q3-_-lp-img
IV. インターネットバンキングマルウェア「Gozi」による被害に注意
https://www.jc3.or.jp/topics/gozi.html
V. ユーロポールと13カ国の警察当局が連携、DDoS攻撃ツール利用容疑の若者ら拘束
https://japan.zdnet.com/article/35093605/

個人 1 位

10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

～攻撃件数および被害額は減少しているが、引き続き警戒が必要～



ウイルス感染やフィッシング詐欺により、インターネットバンキングの認証情報が攻撃者に窃取され、正規の利用者になりすまし、不正送金や不正利用が行われた。2016 年は 2015 年と比べインターネットバンキングの被害件数は減少し、さらに、銀行やカード発行会社の被害額は減少している。

＜攻撃者＞

- 犯罪者グループ

＜被害者＞

- 組織（インターネットバンキング利用者）
- 組織（銀行/カード発行会社）

＜脅威と影響＞

組織においてインターネットバンキングの利用が広く普及していく中、これらの利用者の情報を窃取し不正利用することを目的とした攻撃が引き続き行われている。ウイルス感染やフィッシング詐欺等により窃取した利用者の情報を攻撃者が不正利用することで、正規の利用者に金銭的な被害が生じる。

2016 年は、添付ファイルを開くと利用者の情報を窃取するウイルスに感染してしまう悪意あるメールを送付する攻撃が数多く確認された。

＜攻撃手口＞

◆ ウイルス感染

利用者が、攻撃者が用意した悪意あるウェブサイトにアクセスしたり、メールに添付されている悪意あるファイルを開いたりすることで、利用者の端末にウイルスを感染させる手口。利用者がウイルスに感染した端末でインターネットバンキングにログインすると情報が攻撃者に窃取される。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利用者の口座から攻撃者の口座への不正送金を行う。

また、ウイルスに感染した端末の利用者がインターネットバンキングを利用していなくても、端末のアドレス帳等から利用者の個人情報を窃取され、別の攻撃に悪用される恐れがある。

◆　**フィッシング詐欺**

攻撃者が取引先会社等、実在する組織を装い、フィッシングサイトの URL を含むメールを組織の担当者に送りつけ、組織の担当者を正規の組織からのメールであると誤認させ、攻撃者が用意したフィッシングサイトへアクセスさせる手口。組織の担当者は攻撃者による偽の情報を信用してしまい、そこで入力した情報が攻撃者に窃取される。攻撃者は窃取した情報を使用して、組織の担当者になりすまし組織の口座から別の口座への不正送金等を行う。

＜事例と傾向＞

◆　**不正送金被害は減少傾向**

警察庁によると、2016 年中に発生したインターネットバンキングの不正送金事件は 1,291 件あり、2015 年と比べて 204 件減少している。また、被害額を同様に比較すると、全体では約 16 億 8,700 万円で、約 13 億 8,600 万円の減少となっている。被害額の内訳は、組織が約 4 億 3,500 万円で、約 10 億 3,100 万円の減少、個人が約 12 億 5,200 万円で、約 3 億 5,500 万円の減少となっており、特に、組織の被害額が大幅に減少している。[I]

◆　**日本を狙ったウイルスメールの拡散**

2016 年はウイルス拡散の手法としてメールによる攻撃が活発化した。例えば、1 回の攻撃で400通以上のウイルスを含むメールを送信する攻撃が 2016 年 11 月までに 33 回あったことが確認されている。なお、2015 年には 400 通以上の攻撃が 1 回も発生していなかった。[II]

＜対策/対応＞

組織（利用者）

- 情報リテラシーの向上
  - ・受信メール、ウェブサイトの十分な確認
  - ・添付ファイルやリンクを安易にクリックしない
  - ・事例・手口の情報収集

  実在する組織からのメールだからと、安易に信用しないことが重要である。また、多くの金融機関やクレジットカード会社のホームページでは、犯罪手口の説明やセキュリティ対策の提供を行っているのでそれらを参考にする。[III]
- 被害の予防
  - ・OS・ソフトウェアの更新
  - ・セキュリティソフトの導入
  - ・多要素認証等、銀行が推奨する認証方式の利用
  - ・ファイルの拡張子を表示させる設定
- 被害の早期検知
  - ・不審なログイン履歴の確認
  - ・自身の口座やクレジットカードの利用履歴の確認

参考資料

I. 平成28年中におけるサイバー空間をめぐる脅威の情勢等について
http://www.npa.go.jp/kanbou/cybersecurity/H28cyber_jousei.pdf
II. 2016年個人の三大脅威：ネットバンキングを狙う「オンライン銀行詐欺ツール」
http://blog.trendmicro.co.jp/archives/14247
III. フィッシング対策の心得
https://www.antiphishing.jp/consumer/attention.html

このページは空白です。

3章. 注目すべき脅威や懸念

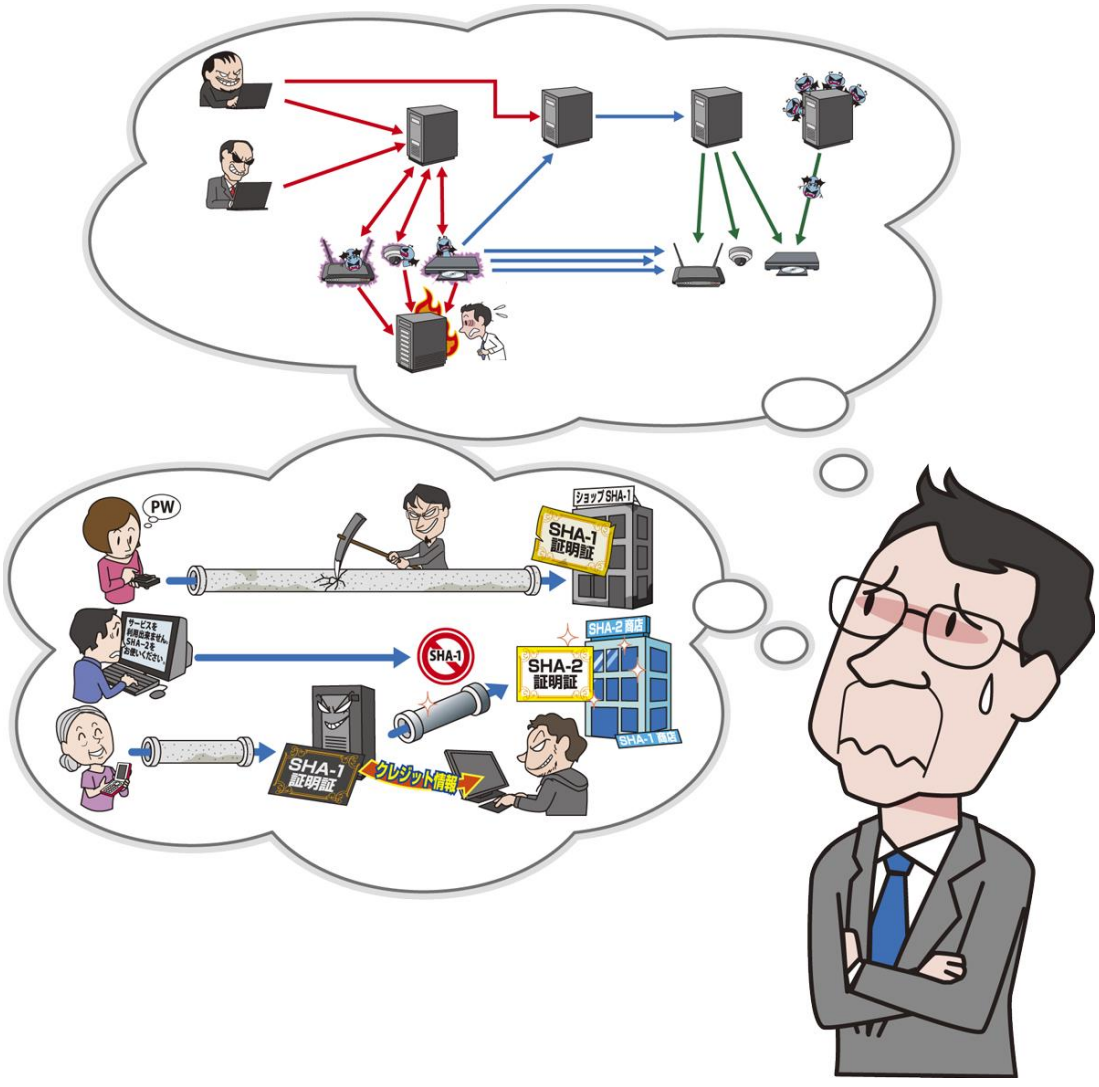
このページは空白です。

3 章 注目すべき脅威や懸念

本章では、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 2 つの懸念について解説する。

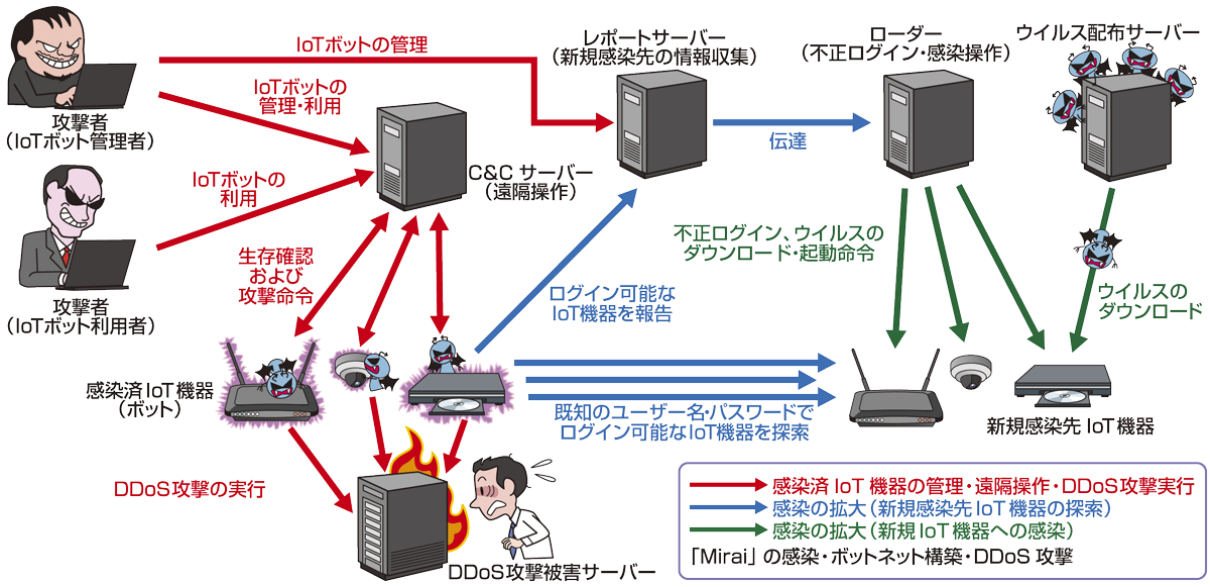
表 3.1 注目すべき脅威や懸念

番号	タイトル
1	IoT におけるセキュリティ脅威の顕在化 ～IoT 機器の大量乗っ取りと大規模 DDoS 攻撃への悪用～
2	TLS における SHA-1 の利用停止とその波紋 ～ハッシュ関数の SHA-2 への移行期に潜む脅威～



3.1. IoT におけるセキュリティ脅威の顕在化

～IoT 機器の大量乗っ取りと大規模 DDoS 攻撃への悪用～



情報家電、玩具、自動車、オフィス機器、医療機器、産業用設備・機器、制御システムなど多種多様な「モノ」がネットワークを介してつながる IoT（Internet of Things）に対するセキュリティ脅威は二年前に公開した「情報セキュリティ 10 大脅威 2015」の 3 章（注目すべき課題や懸念）でも取り上げたが、2016 年、ウイルスに感染した IoT 機器を踏み台とした大規模 DDoS（Distributed Denial of Service）攻撃が発生し、セキュリティ設定・対策が不十分なままネットワークに接続された多数の IoT 機器の存在やセキュリティ対策の重要性を再認識することとなった。

＜「Mirai」が与えた衝撃＞

2016 年 9 月 20 日（米国時間）、セキュリティ専門家 Brian Krebs 氏が運営するブログ Krebs on Security は、約 620Gbps の DDoS 攻撃を受けた。Krebs 氏は、この大規模 DDoS 攻撃が、ウイルス「Mirai」に感染したネットワークカメラやホームルーター等の IoT 機器群で構成されるボットネットによるものと報告した。同時期、フランスのホスティングサービス会社 OVH は 14 万 5 千台以上の IoT 機器から DDoS 攻撃を受け、ピーク時には 1Tbps を超えるトラフィックを観測した。[I]

9 月 30 日、「Anna-senpai」と名乗る人物が「Mirai」のソースコードをインターネット上の掲示板サイトで公開した。その後、「Mirai」に感染していると見られる IoT 機器（内 80%以上は DVR: デジタルビデオレコーダー）は 21 万 3 千台から 49 万 3 千台に倍増すると共に、「Mirai」の新たな亜種が次々に出現した。[II]

10 月 21 日には、DNS サービス提供会社 Dyn に対して DDoS 攻撃が行われ、同社のサービスを利用する Twitter、SoundCloud、Spotify、Reddit 等のサービスが一時利用不能となった。[III] さらに、11 月 28 日にはインターネット接続サービスを提供するドイツテレコム（Deutsche Telekom AG）の顧客の外部ルーターが「Mirai」の亜種と思われるウイルスを感染させようとする攻撃を受け、全ルーターの 4～

5%がクラッシュまたは制限状態となり、90 万人の顧客サービスに障害を生じた。[IV]

＜二つの被害者＞

近年、IoT におけるセキュリティ脅威として報告された事例は、医療機器や自動車等の IoT 機器の利用者が被害者となり、その人命に関わる攻撃が注目されていた。「Mirai」やその亜種による攻撃は、二つの異なる被害者グループを生じる点が異なっている。

◆ **被害者1（IoT 機器の利用者）**

ウイルスに感染し、DDoS 攻撃の踏み台に悪用された IoT 機器の利用者。

◆ **被害者 2（DDoS 攻撃の被害者）**

ウイルスに感染した**被害者1**の IoT 機器で構成されたボットネットからの DDoS 攻撃を受けたサーバーの所有者・運営者・利用者。

「Mirai」への対策を困難としている理由として、第一の被害者である IoT 機器の利用者は、機器の機能（ネットワークカメラであれば画像の閲覧、ホームルーターであればインターネット接続、DVR であればテレビ番組の録画等）は正常に動作し続けるため、感染して被害に遭っていること、第二の被害者である第三者への攻撃に悪用されていることに気付きにくい点が挙げられる。

＜「Mirai」とその亜種の挙動＞

「Mirai」は、以下に示す動きで感染・ボットネット構築・DDoS 攻撃を行う。[V]

- 組込み Linux および軽量 UNIX コマンドツール BusyBox の上に実装された IoT 機器を感染対象としている。
- 「Mirai」は、典型的なユーザー名とパスワードの初期値の組合せ（例：”admin”と”password”）や、著名な IoT 機器ベンダーの製品の初期ユーザー名・パスワードがハードコーディングされた一覧表を持ち、このユーザー名とパスワードを用いて、telnet（ポート番号 23 または 2323）で不正ログイン可能な機器に感染する。
- 「Mirai」に感染した IoT 機器は、60 秒毎に C&C サーバーと通信する。また、C&C サーバーからの攻撃命令を受けると、指定された攻撃対象に DDoS 攻撃を行う。
- また、「Mirai」に感染した IoT 機器は、不正ログイン可能な他の IoT 機器を探索し、攻撃者が管理するレポートサーバーに報告する。
- この情報は、攻撃者が管理するローダーに渡り、ローダーが新たに感染させようとする IoT 機器に不正ログインして不正プログラムを実行し、ウイルス配布サーバーから「Mirai」をダウンロードして感染を拡大させる。

公開されたソースコードをもとに派生した「Mirai」の亜種は、異なるポート番号、異なるプロトコル及びその脆弱性を利用して感染するものも存在するので、上記の攻撃のみ防止すれば十分ということではない。[VI]

＜感染が拡大した理由＞

上記の挙動を考慮すると、ユーザー名とパスワードを初期値から安全な値へ変更していれば、「Mirai」の感染を防ぐことが出来たはずである。しかしながら、IoT 機器の一部には、例えば以下に示すような問題が存在したため、感染は世界中に拡大することとなった。

【ポート／サービス管理の問題】

- 製品出荷後に IoT 機器を使用するために必ずしも必要のない telnet プロトコルが動作し、対応するポートがオープンの状態で出荷されていた。
- 機器によっては、telnet プロトコルを停止し、対応ポートをクローズするための管理機能

が提供されていなかった。

- 機器によっては、telnet プロトコルの動作や対応ポートのオープン状態が説明書等に記載されておらず、IoT 機器の利用者はその存在を知らない「バックドア」状態となっていた。

【ユーザー名／パスワード管理の問題】

- 利用者がユーザー名とパスワードを初期値から変更すべきであることを、説明書等において注意喚起していなかった。
- 機器によっては、パスワードがハードコーディングされており、利用者が変更できなかった。
- 機器によっては、「バックドア」状態であり、ユーザー名とパスワードの存在そのものが利用者に隠蔽されていた。

Flashpoint 社の調査によると、この条件を満たす IoT 機器が世界中に 51 万 5 千台以上発見されている。

＜「Mirai」や亜種に対する対策＞

「Mirai」とその亜種に対する対策として、IoT 機器の製造者・開発者および利用者、DDoS 攻撃の被害者が考慮すべき対策について示す。

【IoT 機器の製造者・開発者の対策】

- 不要な管理機能の無効化
  製品出荷後に不要な管理機能（プロトコルやポート開放）は無効化して出荷する。製品出荷後に一時的に必要となる管理機能については、不要な際に無効化するための手段を提供し、説明書等への記載で利用者に周知徹底する。
- 初期認証情報の変更の周知徹底
  ユーザー名・パスワードは変更可能とし、セキュアな値に変更することを、説明書等への記載で利用者に周知徹底する。可能であれば、初期値から変更しないと IoT 機器が動作しない設定とし、セキュアでないパスワードへの変更は不可とすることが望ましい。
- 更新ソフトウェアの提供
  既に出荷した製品に前述の問題点が見つかり、ソフトウェアを入れ替えないと対応できない場合は、更新ソフトウェアを作成し、利用者に配布する。製品出荷時に自動更新機能を組み込んでおくことも、選択肢の一つである。

【IoT 機器の利用者の対策】

- 説明書を熟読し、指示に従い使用する。
- 常時動作不要な管理機能が搭載されていた場合は、説明書等の指示に従って無効化する。
- 動作上問題なければ、ルーター経由でネットワークに接続し、ルーターにて不正通信をブロックする。
- ユーザー名（変更可能な場合）やパスワードは、セキュアな値に変更する。
- 更新ソフトウェアが提供された場合、速やかに適用する。

【DDoS 攻撃の被害者の対策】

- これまでの想定を超える大規模な DDoS 攻撃を受ける恐れがあることを認識し、重要なサーバー等における対策を見直す（詳細は **2 章**「組織 4 位」等を参照）。

＜「Mirai」だけでない脅威＞

IoT 機器に感染するウイルスは「Mirai」だけではない。[VII] 例えば、2014 年 9 月に発見された「Bashlite」は、2015 年初めにソースコードが公開された後に様々な亜種が作成され、2016 年 8 月の時点で台湾・ブラジル・コロンビアを中心に 100 万台の IoT 機器に感染し、依然としてボットネットを形成している。[VIII]

＜求められる対応の見直し＞

ウイルス「Mirai」は、初期設定のままで利用されている IoT 機器といった、初歩的なセキュリティ設定が不十分な機器をターゲットとしていた。世界中に悪用可能な IoT 機器が多数存在することを認識した攻撃者は、今後もっと高度な攻撃手法を用いて IoT 機器を乗っ取ったり、IoT 機器の利用者自身に対して攻撃を仕掛けたりしてくることが考えられる。IoT のセキュリティ対策を改めて見直すべき時期に来ている。IPA では、このような被害を防ぐため適切なセキュリティ対策が施された IoT 機器が供給されるよう、製造者・開発者向けに IoT のセキュリティ設計について解説した「IoT 開発におけるセキュリティ設計の手引き」を公開している。[IX]

＜「Anna-senpai」の正体とは＞

「Mirai」に感染した IoT 機器からの DDoS 攻撃を受けた初期の被害者である Krebs 氏は、2017 年 1 月にブログを更新し、数か月に渡る調査の結果、「Anna-senpai」と名乗りソースコードを公開した「Mirai」の開発者グループの一人を突き止めたと報告した。[X] 事の真偽を確かめることは困難であるが、Krebs 氏によると、DDoS 対策サービス提供会社のオーナーであるという。事実とすれば、かつては DDoS 攻撃を仕掛ける攻撃者と戦っていたセキュリティ技術者が、罪を犯す側に転向したことになる。「Mirai」による大規模 DDoS 攻撃は、IoT セキュリティの見直しだけでなく、セキュリティ技術者のモラルをも考えさせられる事件となった。

＜今後に向けた提言＞

上記では、IoT 機器への特定の攻撃に焦点を当て、脅威の具体的な事例と対策を説明した。今後の IoT 技術の適用分野の拡大と共に、個々の IoT 機器やシステムやサービスにおける脆弱性対策を始めとしたセキュリティへの考慮が重要となってくる。

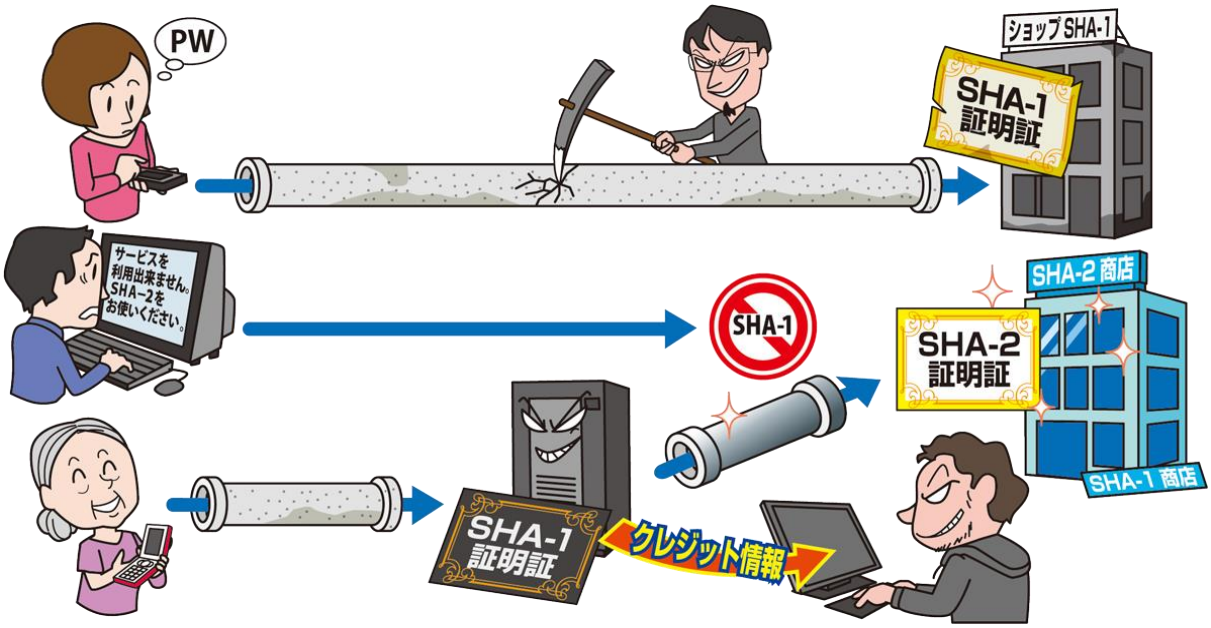
公開されている「IoT セキュリティガイドライン」[XI] や「IoT 開発におけるセキュリティ設計の手引き」、様々な業界での基準やガイド他を参照して、安心安全な IoT 社会の発展に向けて、機器開発者、システム事業者、サービス事業者が各々の立場で、また相互に連携して、対策に取り組むことが望まれる。

参考資料

I. セキュリティニュースサイトに史上最大規模のDDoS攻撃、1Tbpsのトラフィックも
http://www.itmedia.co.jp/enterprise/articles/1609/26/news047.html
II. マルウェア「Mirai」に感染したIoT機器が急増、亜種も相次ぎ出現
http://www.itmedia.co.jp/enterprise/articles/1610/20/news061.html
III. Dyn、大規模DDoS攻撃に関する報告を発表
https://japan.cnet.com/article/35091202/
IV. Deutsche Telekomのルータで大規模障害、マルウェア「Mirai」が関与か
http://www.itmedia.co.jp/enterprise/articles/1611/30/news064.html
V. Internet Infrastructure Review Vol.33
http://www.iij.ad.jp/company/development/report/iir/033.html
VI.「Mirai」ソースコード徹底解剖－その仕組みと対策を探る
http://www.atmarkit.co.jp/ait/articles/1611/08/news028.html
VII. DDoS攻撃が広がるIoTデバイス
https://www.symantec.com/connect/ja/blogs/ddos-iot
VIII.マルウェア「BASHLITE」、100万台のIoTデバイスに感染
http://news.mynavi.jp/news/2016/09/04/061/
IX. 「IoT開発におけるセキュリティ設計の手引き」を公開
https://www.ipa.go.jp/security/iot/iotguide.html
X. Who is Anna-Senpai, the Mirai Worm Author?
https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/
XI. IoTセキュリティガイドラインver1.0
http://www.meti.go.jp/press/2016/07/20160705002/20160705002.html

3.2. TLS における SHA-1 の利用停止とその波紋

～ハッシュ関数の SHA-2 への移行期に潜む脅威～



インターネット通信における盗聴・改ざん・成りすましといった脅威の対策として、広く採用されている暗号通信プロトコル TLS（Transport Layer Security）で用いられている暗号技術の一つ、ハッシュ関数が SHA-1 から SHA-2 へ世代交代の時期を迎えた。移行を怠ると、安全な通信を保証することが困難となる。また、SHA-2 がサポートされない OS や携帯電話端末は、ソフトウェアやハードウェアの更新を考慮しなければならない時期に来ている。

＜TLS における SHA-1 の役割＞

ブラウザを介したインターネット上の Web サイトの閲覧、スマートフォン用アプリとインターネット上のサーバーとの通信等において、盗聴・改ざん・成りすましといった脅威の対策として、暗号通信プロトコル TLS が広く採用されている。TLS においては、複数の暗号技術が組み合わされて用いられているが、その中の一つにハッシュ関数があり、SHA-1 は以下の処理において用いられている。

- **CA 証明書の署名検証**
  公開鍵証明書(※1)の発行機関である CA（Certification Authority）の公開鍵証明書（CA 証明書）に付与された電子署名が正しいか否かを確認する。

（※1）公開鍵暗号アルゴリズムの公開鍵とその所有者の結び付きを証明する証明書。

- **TLS サーバー証明書(※2)の署名検証**
  TLS を利用するサーバー（Web サーバーやアプリケーションサーバー）の公開鍵証明書（TLS サーバー証明書）に付与された電子署名が正しいか否かを確認する。

（※2）TLS の前身である SSL（Secure Socket Layer）から由来して、「SSL サーバー証明書」と呼ばれることもある。

- **通信データの署名生成・検証**
  TLS 通信の初期段階（ハンドシェークプロトコル）において、サーバーから送信するメッ

セージに電子署名を付与し、クライアント（Web ブラウザやスマートフォン用アプリ）において正しいものであるか否か確認する。

- **内部での秘密演算**
  TLS 通信の初期段階において、サーバー・クライアント双方の内部で行う秘密演算の一部で利用する。

＜SHA-1 の脆弱性とその影響度＞

ハッシュ関数としては、1995 年に公開された SHA-1 が長らく使用されてきた。2005 年、暗号研究者により SHA-1 の理論的な脆弱性が指摘され、一度は 2010 年までに後継の SHA-2（SHA-224、SHA-256、SHA-384、SHA-512 の総称であるが、TLS においては SHA-256 の採用を意味する）への移行が計画されたが、現実的な攻撃方法の確立にまで至らなかったため、移行は進展しなかった。2015 年、SHA-1 に対する実用的な攻撃方法の可能性を示す、新たな理論が発表された。

TLS における SHA-1 が破られた場合、公開鍵証明書や通信データの電子署名を改ざんし、サーバーに成りすましてクライアントとの通信路を確立可能となる。この結果、通信相手に成りすましによる機密情報の窃取等が発生する恐れがある。

現時点で即 SHA-1 が改ざん可能な訳ではないが、「いつ破られても不思議でない状態」となったため、TLS における電子署名の生成・検証で用いるハッシュ関数に関して、2016 年から 2017 年にかけて SHA-1 から SHA-2 への移行が進められることとなった。

＜影響を受ける関係者とその対応＞

◆ CA

CA は、CA および Web ブラウザ・ソフトウェアのベンダー等で構成された民間団体である CA/Browser Forum が定めた Baseline Requirements（**表 3.2**）に従い、原則として、有効期限が 2017 年 1 月 1 日以降となる公開鍵証明書における SHA-1 の使用を禁止し、SHA-2 へ移行した。

◆ サーバー管理者

TLS を利用するサーバーの管理者は、TLS サーバー証明書を SHA-2 使用のものに更新する必要がある。サーバー上で利用しているソフトウェアが SHA-2 に対応していない場合は、対応する版へアップデートする必要がある。

また、クライアント利用者に対して、SHA-1 は利用不可となること、SHA-2 対応ブラウザやアプリへの移行を促す必要がある。自社製アプリを提供している場合は、SHA-2 対応版を開発・

表 3.2 SHA-2 移行に関わる CA/Browser Forum の Baseline Requirements（抜粋）

	発効日	条件	内容
1	2015-01-16	推奨	CA は 2017 年 1 月 1 日以降の有効期限を持つ SHA-1 を用いた利用者証明書（TLS サーバー証明書を含む）を発行すべきでない。
2	2015-04-01	必須	CA は特定の条件を満たす場合を除き、39 ヶ月を超える有効期間を持つ証明書（CA 証明書、TLS サーバー証明書を含む）を発行してはならない。
3	2016-01-01	必須	CA は SHA-1 を用いた利用者証明書、中間 CA 証明書（他の CA に対して発行する CA 証明書）を発行してはならない。
4	2016-06-30	必須	CA は条件に依らず、39 ヶ月を超える有効期間を持つ利用者証明書を発行してはならない。

提供する必要がある。

開発時にオープンソースを利用する場合、ネット等に公開されているサンプルコードに SHA-1 を使用したものが残っていることがあるので、参照・流用する際は注意する必要がある。

◆ **Web ブラウザ・OS 開発・提供者**

各社が提供するブラウザや OS の最新版は、SHA-2 に対応している。2017 年以降、一部の SHA-2 対応ブラウザは、SHA-1 を利用するサーバーと接続した際、警告を発して接続拒否するようになっている（**表 3.3**）。

◆ **クライアント利用者**

SHA-2 に対応したブラウザやアプリ、OS に移行する必要がある。引き続き SHA-1 が利用可能なブラウザやアプリであっても、SHA-2 を優先的に使用するように設定可能であれば、そうすべきである。SHA-1 を用いて TLS 通信を行っている場合、盗聴・改ざん・成りすまし対策は保証されていないことを認識し、重要なデータのやり取りを行わないよう、注意する必要がある。

SHA-2 対応の OS・ブラウザ・アプリ等が動作しないハードウェア（製造年度の古い一部 PC および携帯電話端末）（**表 3.4**）の利用者は、機器自体の更新を検討する必要がある。一部のサーバーは、セキュリティ向上のため、TLS を用いない接続を拒否する「常時 SSL 化（AOSSL: Always On SSL）」を導入しているが、これに SHA-1 を用いた TLS 接続拒否を加えると、旧機種の利用者はサーバーにアクセス不可となる。従って、ハードウェアを更新しないと、これまで使用してきたサービスが全く利用出来なくなることがある。[VI]

表 3.3 主なブラウザにおける SHA-1 から SHA-2 への移行計画（抜粋）

開発元	ブラウザ	移行計画（抜粋）
Microsoft	Edge, IE	2017 年中旬（当初計画の 2/14 から延期）以降、Microsoft Edge および Internet Explorer 11 で SHA-1 のサーバー証明書を用いた Web サイトは安全とは見なさず、閲覧時に警告を表示する。[II] 開始時期未定だが、Internet Explorer 10 以前およびその他のアプリケーションでの SHA-1 のサーバー証明書を用いた Web サイトアクセス時の警告表示または利用不可措置を検討中である。
Google	Chrome	2017 年 1 月 25 日公開の Chrome 56 以降、SHA-1 のサーバー証明書を用いた Web サイトは安全とは見なさず、閲覧時に警告を表示する。また、2019 年 1 月 1 日以降公開の Chrome において、企業向けプライベート PKI においてのみ SHA-1 証明書を許容する例外オプションの提供を終了する予定である。[III]
Mozilla	Firefox	2017 年 1 月 24 日公開の Firefox 51 以降、SHA-1 のサーバー証明書を用いた Web サイトは安全とは見なさず、閲覧時に警告を表示する。[IV]
Apple	Safari	2017 年春公開予定のアップデートにおいて、OS の信頼されたルート証明書に対応する CA から発行された SHA-1 のサーバー証明書を用いた Web サイトは安全とは見なさず、閲覧時に警告を表示する。[V]

表 3.4 SHA-2 非サポート OS 例 [VII]

OS	バージョン
Windows	Windows XP SP2 以前
	Windows Server 2003 R2 以前
Android	Android 2.2 以前、Android 2.3.x の一部
iOS	iOS 2.2.1 以前
携帯電話独自 OS	主として 2010 年春以前に発売された機種

＜今後想定される懸念＞

◆ 2017 年以降も残る SHA-1 証明書

前述の通り、2017 年以降も有効となる、SHA-1 を用いた TLS サーバー証明書は原則として発行されていない。しかしながら、CA/Browser Forum の定めた要件（**表 3.2**）では、項番 2 が成立するまでは 60 ヶ月以下の有効期間を持つ証明書を任意発行することが出来たため、「2015 年 1 月 15 日発行、有効期間 5 年（2020 年 1 月 14 日まで有効）」の SHA-1 証明書が存在する。また、項番 1 が必須規定ではないため、これを無視すれば、項番 3 の発効までに「2015 年 3 月 31 日発行、有効期間 5 年（2020 年 3 月 30 日まで有効）」、「2015 年 12 月 31 日発行、有効期間 39 ヶ月（2019 年 3 月 30 日まで有効）」といった証明書も発行し得る。

このように 2017 年以降も有効な SHA-1 証明書が存在するため、警告機能を持たない旧バージョンのブラウザの利用者は、個人情報やクレジットカード番号等の機微な情報の入力の際に注意する必要がある。可能であれば、最新版のブラウザにアップデートすることが望ましい。

また、サーバー運営者は、クライアント利用者の対応可否を確認の上、速やかに SHA-2 へ移行することが望ましい。

◆ 中間者攻撃の脅威

SHA-2 に対応した OS やブラウザが提供されない旧機種の利用者を狙って、攻撃者が用意した TLS プロキシを中継すれば SHA-1 のまま接続可能と騙り、中継点で暗号化を一旦解除して利用者が入力した情報を窃取しようとする、中間者攻撃を行う者が現れる恐れがある。

◆ サポートと見せかけた攻撃に注意

現時点では存在は確認されていないが、「このサイトを経由するように設定すると、SHA-2 のサーバーに接続できます」「このルート証明書をインストールすると、SHA-2 のサーバーと通信できるようになります」といった、困っている利用者の弱みに付け込む甘い言葉には注意して頂きたい。

参考資料

I. BASELINE REQUIREMENTS
https://cabforum.org/baseline-requirements/
II. SHA-1ウェブサーバー証明書は警告！ウェブサイト管理者は影響の最終確認を
https://blogs.technet.microsoft.com/jpsecurity/2016/11/25/sha1countdown/
III. SHA-1 Certificates in Chrome
https://security.googleblog.com/2016/11/sha-1-certificates-in-chrome.html
IV. Phasing Out SHA-1 on the Public Web
https://blog.mozilla.org/security/2016/10/18/phasing-out-sha-1-on-the-public-web/
V. SafariおよびWebKitでのSHA-1証明書のサポート終了について
https://support.apple.com/ja-jp/HT207459
VI.【重要なお知らせ】「SHA-2」方式非対応の携帯情報端末およびパソコン、ならびにIE6.0以前等のブラウザをご利用のお客さまへ
https://www.jreast.co.jp/mobilesuica/new_s/sha220160307.html
VII. 証明書のSHA2署名への移行が本格化
http://itpro.nikkeibp.co.jp/atcl/column/14/277462/032600030/

SHA-1 が破られた？

3.2. TLS における SHA-1 の利用停止とその波紋では、SHA-1 の脆弱性を利用した電子署名の改ざんに関して、**「いつ破られても不思議でない状態」**と解説した。2017 年 2 月 23 日、オランダの国立研究機関 CWI（Centrum Wiskunde & Informatica）と Google は、2 年間の共同研究の末、衝突攻撃（同じハッシュ値を出力する異なる入力データを見つける攻撃）を用いて、実際に SHA-1 を破ることに成功した、と発表した。[I] [II] これは、SHA-1 に対する衝突攻撃の初めての実用的な技術であると述べ、同一のハッシュ値となる一対の PDF ファイルを公開した。

今回の発表では、2^{80} 回のハッシュ値計算（GPU 1,200 万年分の計算量）を行う全数探索より 10 万倍速い、2^{63} 回（922 京 3372 兆 368 億 5477 万 5808 回）の計算で衝突を発見し、Google の技術やクラウドインフラを用いて、CPU 6,500 年分および GPU 100 年分を合わせた計算を実施したとのこと。

ハッシュ値の衝突が見つけられるようになると、**3.2.**で述べた通り、電子署名の偽造が可能となる等の脅威が考えらえる。

Google は、90 日後、ある条件の下で、ハッシュ値が同一となるような異なる画像を示す、一対の PDF ファイルを生成するためのコードを公開するとしている。また、ファイルが衝突攻撃で作成されたか否かを確認する、無料のオンラインツールの提供を開始した。Gmail および Google Drive では、PDF ファイルの自動検査機能を追加した。[III] [IV]

今回の衝突攻撃には、誰もが利用不可能な高い計算機能力が必要であること、また攻撃を成立させるには一定の条件を満たす必要があること（任意のデータに対して同じハッシュ値となる別のデータを必ずしも見つけられるとは限らないこと）から、世の中に存在する SHA-1 を用いた電子署名の全てが即時に信用できない、という状況には当たらない。本当に SHA-1 が破られたか否かは、今後 Google が公開を予定しているコードを見て、判断することになるであろう。しかしながら、CRYPTREC の電子政府推奨暗号リストにおいて互換性維持以外の目的での利用を推奨していない、「いつ破られても不思議でない状態」であることに変わりはない。可能な限り、速やかに SHA-2 等の安全なハッシュ関数への移行に着手することが望ましい。[V] [VI]

参考資料

I. CWI and Google announce first collision for Industry Security Standard SHA-1
https://www.cwi.nl/news/2017/cwi-and-google-announce-first-collision-industry-security-standard-sha-1
II. Announcing the first SHA1 collision
https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html
III. SHATTERED
https://shattered.io/
IV. GoogleとCWI、SHA-1衝突に成功、ハッシュ値が同じ2つのPDFを公開
http://internet.watch.impress.co.jp/docs/news/1046144.html
V. SHA-1の安全性低下について
https://www.cryptrec.go.jp/topics/cryptrec_20170301_sha1_cryptanalysis.html
VI【注意喚起】ハッシュアルゴリズム「SHA-1」の衝突攻撃（SHAtterd）の Web サイトへの影響に関して（2017/03/07）
https://www.antiphishing.jp/news/info/sha1shatterd20170307.html

このページは空白です。

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	浜田 譲治	セキュアーワークス(株)
石井 彰	旭化成(株)	Piyokango	セキュリティインコ
岡田 良太郎	(株)アスタリスク・リサーチ	平田 真由美	(一社)セキュリティ対策推進協議会
齋藤 衛	(株)インターネットイニシアティブ		(SPREAD)
高橋 康敏	(株)インターネットイニシアティブ	唐沢 勇輔	ソースネクスト(株)
楢原 盛史	ヴイエムウェア(株)	辻 伸弘	ソフトバンク・テクノロジー(株)
佐藤 直之	SCSK(株)	有村 肇将	地方公共団体情報システム機構(J-LIS)
保村 啓太	SCSK(株)	鈴木 一弘	地方公共団体情報システム機構(J-LIS)
松本 隆	SCSK(株)	百瀬 昌幸	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)	杉山 俊春	(株)ディー・エヌ・エー
小林 克巳	NRI セキュアテクノロジーズ(株)	森 槙悟	(株)ディー・エヌ・エー
正木 健介	NRI セキュアテクノロジーズ(株)	田岡 聡	(株)東芝
中西 克彦	NEC ネクサソリューションズ(株)	小島 健司	(株)東芝
杉井 俊也	NEC フィールディング(株)	小屋 晋吾	トレンドマイクロ(株)
北河 拓士	NTT コミュニケーションズ(株)	加藤 雅彦	長崎県立大学
東内 裕二	NTT コミュニケーションズ(株)	須川 賢洋	新潟大学
大山 千尋	(株)NTT データ	猪股 秀樹	日本アイ・ビー・エム(株)
宮本 久仁男	(株)NTT データ	坂 明	日本サイバー犯罪対策センター(JC3)
矢竹 清一郎	(株)NTT データ	谷川 哲司	日本電気(株)
植草 祐則	NTTデータ先端技術(株)	住本 順一	日本電信電話(株)
佐久間 邦彦	NTTデータ先端技術(株)	大森 健史	(株)日本エンタープライズサービス
七條 麻衣子	大分県立芸術文化短期大学	前田 隆行	(株)日本エンタープライズサービス
前田 典彦	(株)カスペルスキー	金 明寛	(株)ネクストジェン
岡村 浩成	京セラコミュニケーションシステム(株)	徳丸 浩	HASH コンサルティング(株)
佐藤 宏昭	京セラコミュニケーションシステム(株)	出口 敬規	HASH コンサルティング(株)
山田 淳二	京セラコミュニケーションシステム(株)	渡辺 久晃	パナソニック(株)
小熊 慶一郎	(株)KBIZ / (ISC)2	林 薫	パロアルトネットワークス(株)
山下 慶子	KPMG コンサルティング(株)	岩佐 功	東日本電信電話(株)
増本 有希	(株)KPMG FAS	小川 茂樹	東日本電信電話(株)
淵上 真一	学校法人 KBC 学園	水越 一郎	東日本電信電話(株)
高倉 弘喜	国立情報学研究所	太田 良典	(株)ビジネス・アーキテクツ
清水 秀一郎	(株)コロプラ	折田 彰	(株)日立システムズ
鈴木 啓紹	(社)コンピュータソフトウェア協会(CSAJ)	本川 祐治	(株)日立システムズ
福森 大喜	(株)サイバーディフェンス研究所	藤原 将志	(株)日立製作所
宮地 利雄	(社)JPCERT コーディネーションセンター	古賀 洋一郎	ビッグローブ(株)
	(JPCERT/CC)	上村 理	ファイア・アイ(株)
宮﨑 清隆	(社)JPCERT コーディネーションセンター	大高 利夫	藤沢市
	(JPCERT/CC)	原 和宏	富士通(株)
金田 智史	(株)シマンテック	原田 弘和	富士通(株)
山内 正	(株)シマンテック	綿口 吉郎	(株)富士通研究所

氏名	所属	氏名	所属
神薗 雅紀	PwC サイバーサービス合同会社	吉岡 克成	横浜国立大学
鈴木 暁	(株)ベリサーブ	福本 佳成	楽天(株)
山室 太平	(株)ベリサーブ	柳川 俊一	(株)ラック
山谷 晶英	三井物産セキュアディレクション(株)	山崎 圭吾	(株)ラック
関根 鉄平	(株)ユービーセキュア	若居 和直	(株)ラック
松田 和宏	(株)ユビテック		

更新履歴

2017 年 3 月 30 日	初版
2017 年 5 月 30 日	個人 2 位の参考資料変更およびそれに伴う修正 誤字修正

このページは空白です。

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　辻 宏郷　亀山 友彦
竹村 純輝　扇沢 健也　鹿野 一人
小林 桂　斉藤 良彰　工藤 伊知郎

IPA 執筆協力者　江口　純一　金野 千里　桑名 利幸
加賀谷 伸一郎　野澤 裕一　黒谷 欣史
大道 晶平

情報セキュリティ 10 大脅威 2017

～職場に迫る脅威！ 家庭に迫る脅威！？
急がば回れの心構えでセキュリティ対策を～

2017 年 3 月 30 日　初　版　第 1 刷発行
2017 年 5 月 30 日　第 2 版　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/

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