情報セキュリティ

10大脅威 2018

～引き続き行われるサイバー攻撃、あなたは守りきれますか？～

独立行政法人情報処理推進機構
セキュリティセンター

2018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 2018」
https://www.ipa.go.jp/security/vuln/10threats2018.html

目次

はじめに

本書「情報セキュリティ 10 大脅威 2018」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、2017 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 IoT 機器（情報家電）編

昨今、IoT 機器が普及し、家庭での利用が進んでいる。一方、ネットワークに接続されている機器という意識が低く、セキュリティ対策は十分に行われていない。また、IoT 機器を狙ったウイルス等も存在しており、IoT 機器の利用者は感染に気づかず利用している。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、IoT 機器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、IoT 機器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 2018（10 大脅威）

2017 年はビジネスメール詐欺による被害が国内でも確認されだしている。ビジネスメール詐欺に遭うと高額な金銭的な被害を受け、企業にとって大きな痛手となる。また、公開されている脆弱性情報を悪用する攻撃が大きな問題となっている。昨今、脆弱性情報が公開されてから攻撃が開始するまでの期間が短くなっており、組織のシステム管理者は脆弱性情報公開後に早急な対応が求められている。

第 2 章では、2017 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

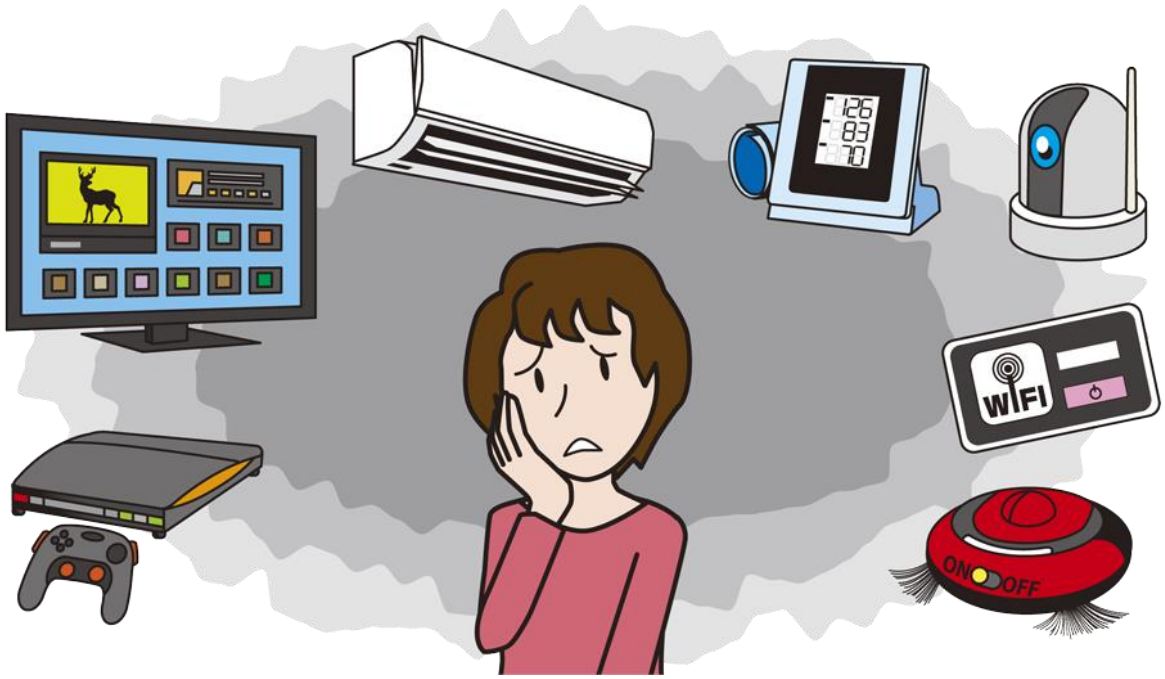
2017 年、仮想通貨の利用が普及し、商品の購入や投資等、様々な場面で活用されている。一方、仮想通貨に係わるサービスを提供するベンダーやその利用者において、セキュリティに関する知識が十分といえず仮想通貨に関連する被害が今後拡大する可能性がある。

広く使われているセキュリティプロトコルに脆弱性が発見されることがある。脆弱性が発見されると、影響を受ける製品やサービスも広範囲にわたり、開発ベンダーは対応に苦慮することになる。2017 年は無線 LAN の暗号化通信のプロトコル WPA2 に脆弱性が発見され、世界中で大きな騒ぎとなった。

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
IoT 機器（情報家電）編

1 章　情報セキュリティ対策の基本 IoT 機器（情報家電）編



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、制御システム等、多種多様な「モノ」がネットワークを介してつながることにより、新たなサービスを提供する IoT（Internet of Things）技術の各分野への適用が拡大している。特に、一般家庭においては、冷蔵庫・洗濯機・エアコン・電子レンジ・炊飯器・ロボット掃除機等の生活支援機器、スマートテレビ・DVD/Blu-ray/HDD レコーダー・ビデオカメラ・オーディオコンポ・ゲーム機等のエンターテイメント機器、体組成計・血圧計・活動量計等のヘルスケア機器、ホームルータ・モバイルルータ・ネットワークカメラ・スマートリモコン・スマートスピーカー等のネットワーク機器といった、様々なネットワーク接続機能を備えた IoT 機器の普及が進んでおり、「情報家電」や「スマート家電」と名付けられている。

このような IoT 機器（情報家電）は、我々に便利な生活をもたらしてくれる一方、誤った状態でネットワークに接続した利用を続けると、サイバー攻撃者による攻撃の対象となり、自らが被害者となるだけでなく、世界中に大きな影響を与えることがある。2016 年、Mirai と呼ばれるウイルスに感染した IoT 機器が遠隔操作され、第三者のサーバーへの攻撃に悪用された結果、Twitter や Amazon.com 等、世界中の多くの人が利用するサービスが一時利用不能となった。悪用された IoT 機器の中には、企業が導入した業務用機器に加えて、一般家庭に設置されたホームルータやネットワークカメラ等が含まれている。

この原因の 1 つとして、IoT 機器の利用者が購入した機器をほぼ初期設定のまま使っている等、セキュリティ対策が不十分なままで IoT 機器を利用していることが挙げられる。特に IoT 機器（情報家電）の場合、一般家庭の利用者にとっては、これまで使用してきた家庭用電化製品の 1 つであり、ネットワークにつながっているという認識が低いためと推察される。あるいは、「ネットワークにつながるメリット」を認識して IoT 機器を購入したものの、「ネットワークにつながることによって生じる脅威」の認識が不足しているため、サイバー攻撃者に対するセキュリティ対策が不十分な可能性がある。さらに、ネットワークにつなぐ課題を認識しているが、IT（情報技術）の専門家でない一般利用者にとっては設定が難しい機能もあり、適切な設定がされていないこともある。

2017 年に入ると IoT 機器を狙ったサイバー攻撃は進化し、特定の IoT 機器が有する脆弱性を突いて感染するウイルス（Mirai の亜種）が出現した。パスワード等の設定を適切に実施していてもウイルス感染するおそれがあり、脆弱性を放置したまま使い続けることが危険な状況となっている。また、第三者への攻撃でなく、家庭内に設置したネットワークカメラの覗き見の被害や、感染した IoT 機器の破壊を目的とするウイルス（BrickerBot）の出現といった、IoT 機器の利用者自身が攻撃対象となってきている。

現在、**IoT 機器（情報家電）の利用者には、IoT 機器はネットワークにつながる機器であり、ネットワークの外部にいる悪意を持った攻撃者から攻撃されるおそれがあるという認識を持って、IoT 機器を適切に利用することが求められる。**

そこで本章では、一般家庭での IoT 機器（情報家電）利用者向けに、IoT 機器を安全に利用する上で考慮しなければいけない点について解説する。なお、IoT 機器は利用時だけではなく、購入前および廃棄のタイミングでも考慮しなければいけない点があるため、それについても解説する。

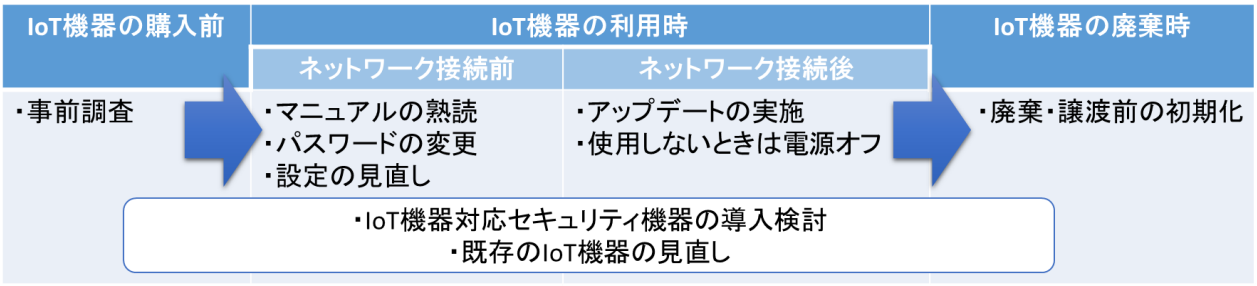
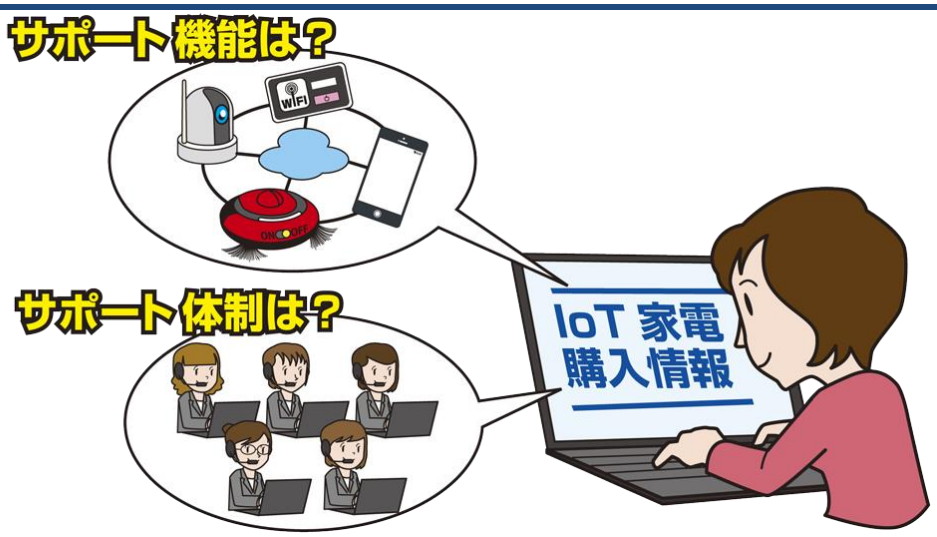


図 1.1 IoT 機器を安全に利用する上で考慮しなければいけない点

1.1. 事前調査



IoT 機器が提供するセキュリティ機能は、IoT 機器の種類や各々の製品により内容は様々である。また、IoT 機器のメーカーや販売店によってサポート体制も異なっており、問い合わせ窓口や不具合発生時のソフトウェアのアップデートの提供等の対応が異なる。そのため利用者は IoT 機器を購入する前に、どのセキュリティ機能を持っているか、メーカーサポートや販売店によるサポートはあるか等を確認することを推奨する。

◆ セキュリティ機能の確認

多くの IoT 機器はセキュリティ機能が提供されており、その機能を使うことで、ウイルス感染や不正な遠隔操作等のセキュリティ上の脅威に対して効果が期待できる。そのため、購入予定の IoT 機器が有するセキュリティ機能を事前に調査し、他の IoT 機器と比較することで、より安全性の高い IoT 機器を選定することができ、購入後の設定もスムーズに行える。選定にあたっては、以下のセキュリティ機能を持っている IoT 機器を推奨する。

- ✓ IoT 機器と通信可能な端末（PC やスマートフォン等）を制限する機能
- ✓ IoT 機器の利用時や IoT 機器との通信時の認証（ログイン）機能
- ✓ 認証の際に利用するパスワード等を変更する機能
- ✓ 自動アップデート機能
- ✓ 個人情報や設定の初期化機能

◆ サポート体制の確認

IoT 機器はメーカーや販売店の違いにより、サポート体制が異なり、脆弱性や不具合があった際のアップデートの有無や頻度が異なってくる。アップデートの提供が遅い、またはアップデートがまったく提供されない場合、攻撃者に脆弱性を悪用され、サイバー攻撃の被害に遭うおそれが高まる。

そのため、購入前に IoT 機器がどのようなサポート体制になっているかを確認する。最低限以下の観点で確認することを推奨する。

- ✓ アップデート頻度
- ✓ サポートの終了時期
- ✓ 日本語での問い合わせの可否

◆ 情報の収集手段

IoT 機器メーカーのウェブページやカタログ、オンラインマニュアル等から情報を収集する。これらの詳細については、メーカーの問い合わせ窓口や、IoT 機器を購入予定の販売店を経由して確認する。

1.2. マニュアルの熟読

IoT 機器には、マニュアル（取扱説明書）が付属されている。マニュアルの中には、操作方法に加えて、利用時の注意事項やセキュリティ機能の設定方法等も書かれている。IoT 機器を安全に利用するためには事前に熟読し、内容を理解した上で利用する必要がある。

◆ IoT 機器を箱から出したらマニュアルを読む

購入した IoT 機器を箱から出したら、IoT 機器にケーブルを接続したり、電源を入れる前に、マニュアルを読む。IoT 機器はネットワークにつないで使用するものであり、接続する前に知っておくべきことがある。まずはマニュアルを熟読してから使用開始する。

なお、紙のマニュアルが付属されていない場合は、購入した IoT 機器メーカーや販売代理店のウェブサイト（ホームページ）等で公開されているオンラインマニュアルを熟読する。

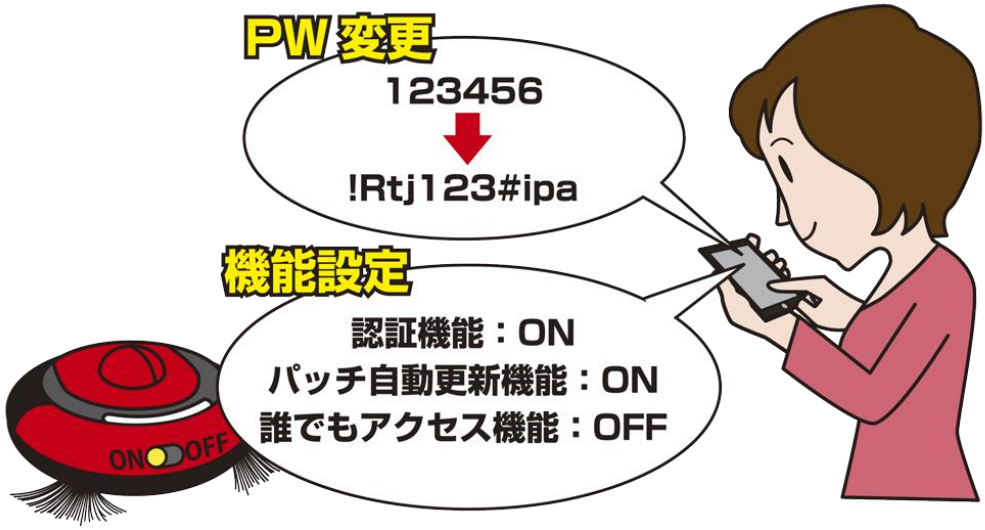
◆ マニュアルには大切なことが記載されている

マニュアルには、操作方法に加えて、利用時の注意事項やセキュリティ機能の設定方法等も書かれている。利用時の注意事項を守らないとサイバー攻撃の被害に遭うおそれがある。また、セキュリティ機能は工場出荷時に初期設定されているが、初期設定でセキュリティ機能が無効化されている場合もある。そのため、マニュアルを熟読し、セキュリティ機能の初期設定や設定の変更方法を確認しておく。

◆ 簡易なセットアップガイドだけを読んで満足するのは NG

購入した IoT 機器によっては、購入者がすぐに利用できるように 1～2 ページ程度の簡易なセットアップガイド等が付属している場合がある。セットアップガイドは、必要最低限の手順で IoT 機器を利用できるようになるため便利だが、IoT 機器をより安全に利用するためには、ひと手間かかるが、マニュアルも読むことが望ましい。

1.3. パスワードの変更 / 設定の見直し



購入直後の IoT 機器は、機器を利用するためのパスワードや各種機能の値がメーカー出荷時に設定された初期設定値となっている。そのままの状態で利用していると、ウイルス感染や不正な遠隔操作等の被害に遭うおそれがある。利用者は、IoT 機器をネットワークに接続する前に初期パスワードの変更や、各種セキュリティ機能の設定等を行った上で接続する。

◆ セキュアなパスワードに変更

IoT 機器によっては、IoT 機器の利用時や管理画面へのアクセス時等にパスワードを用いたログイン（認証）が必要なものもある。購入直後の IoT 機器のパスワードは初期設定値または未設定となっているため、セキュアなパスワードに変更する[1]。なお、パスワードと共にユーザー名や ID を入力する仕様となっており、設定可能であれば、それらも変更する。パスワードの変更を怠っていると、攻撃者に不正アクセスされるおそれがある。特に、同じ IoT 機器で共通の初期パスワードが設定されている場合、攻撃者はその情報を公開されているマニュアル等により容易に入手可能となり、遠隔からの不正ログイン・不正利用のおそれが高まるため、必ず変更する。

◆ 適切な設定への見直し

IoT 機器には、IoT 機器をより便利に利用するための機能や安全に利用するためのセキュリティ機能等、様々な機能がある。その機能の設定を変更できる場合は、初期設定値が適切であるかどうかを確認し、適切でない場合は見直しを行う。また、攻撃者に悪用されるおそれがあるため必要でない機能や使用しない機能は無効化しておく。

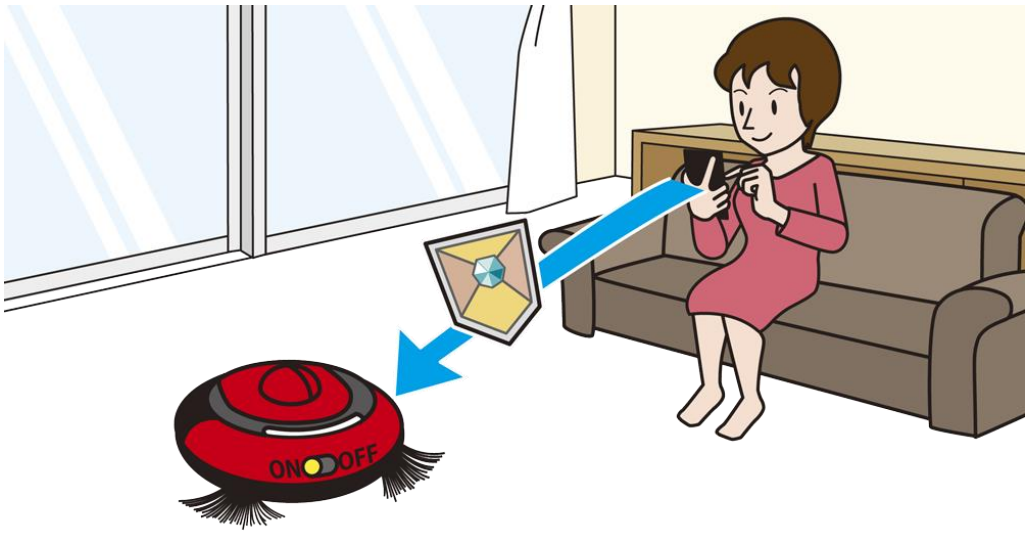
なお、設定項目の意味が不明な場合は、放置せず、マニュアルを読んだり、サポート窓口に問い合わせたり、インターネットで調べたりし、理解した上で適切な設定を行う。

◆ セキュリティ機能の設定

セキュリティ関連の設定は有効にしておくことが望ましい。特に以下の設定を用いることで、自分や家族以外からの不正アクセスによる遠隔操作を防ぐことができる。また、タイムリーにアップデートされるようになり、脆弱性の解消に役立つ。

- ✓ IoT 機器と通信可能な端末を制限する機能
- ✓ IoT 機器の利用時や IoT 機器との通信時にログイン（認証）を要求する機能
- ✓ 自動アップデート機能

1.4. アップデートの実施



IoT 機器によっては、PC やスマートフォンと同様に、そのソフトウェアのバージョンアップ機能を持っている場合がある。ただし、新品を購入したとしても、その IoT 機器のソフトウェアは最新バージョンとは限らない。古いバージョンのソフトウェアには脆弱性が存在するおそれがあり、ネットワークに接続した後は、すぐにアップデートする必要がある。

◆ IoT 機器のアップデート

通常、IoT 機器は、工場出荷時点の最新バージョンもしくはそれに準ずるバージョンのソフトウェアがインストールされている。販売店で IoT 機器を購入した場合、工場出荷後に新しいバージョンが公開されていることがある。古いバージョンには脆弱性が存在するおそれがあり、それを放置したまま IoT 機器を利用することは危険である。そのため、最初にアップデートを実施する必要がある。

また、今後も新しいバージョンが公開される可能性があるため、IoT 機器の利用開始時に限らず、新しいバージョンが公開されたらすぐにアップデートを実施する。

◆ 自動更新機能の利用

IoT 機器にソフトウェアを自動更新する機能があれば、その設定を有効にしておくと、アップデートの手間を低減でき、セキュアな状態を保てる。自動更新機能がない場合は、製品のウェブサイト等から最新バージョン情報を定期的に確認して、新しいバージョンが公開されていたら手動で更新する。最新バージョン情報が不明であれば問い合わせ窓口に確認する。

◆ 管理用アプリもアップデート

IoT 機器の種類によっては、スマートフォン等に IoT 機器を管理または操作するアプリをインストールする場合がある。その場合、そのアプリも最新バージョンの有無を確認し、定期的にアップデートを実施する。

◆ サポート終了機器の利用停止

IoT 機器発売後、一定期間を経過すると、新しいバージョンのソフトウェアが提供されなくなる。このようにサポートが修了した状態では、脆弱性が発見されても解消できなくなるため、継続の利用は危険であり、利用は停止する。また、サポート終了前に、サポートが続いている他機種の購入を検討する。

なお、サポートが継続しているか不明な場合は、メーカーの問い合わせ窓口や、販売店経由で確認する。

1.5. 使用しないときは電源オフ

常時使用しない IoT 機器は、使用終了後、ネットワーク経由でのサイバー攻撃を防ぐために、電源オフしておくと良い。例えば、夜間使用しない機器は、毎晩電源オフして、翌日に電源オンすることで、ウイルスに感染してしまった場合、駆除（IoT 機器から消去）できる場合もある。

◆ 使用しなくなった IoT 機器は電源オフ

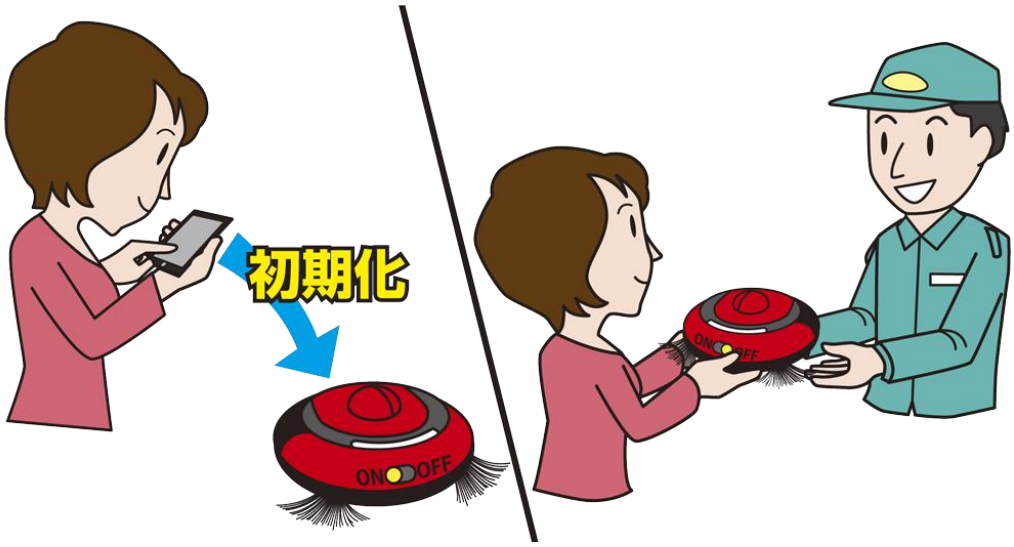
IoT 機器はネットワークにつながっているため、IoT 機器に設定不備や脆弱性が残っていると、サイバー攻撃を受けてウイルス感染や不正な遠隔操作のおそれがある。使用しなくなった IoT 機器や不具合がある IoT 機器はネットワークに接続したままにせず、電源オフにしておくとよい。また、長期間使わないときも電源オフにしておいた方が安全である。

◆ 電源オフによる IoT 機器の安定稼動

ウイルスの中には電源オフにすることで駆除できるものもある。例えば 2016 年に猛威を振るった「Mirai[2]」と呼ばれるウイルスは揮発性メモリ（電源オンのときのみ存在する保存領域）に感染するため電源オフにすることで駆除できる。そのため、常時使用しない IoT 機器や一時的に電源を落としても支障のない IoT 機器は、ときどき電源オフすることも有効である。

なお、電源オフによりウイルスを駆除した後は、再度感染しないようにアップデート等の対策を速やかに実施する。また、対策が取れない場合は、利用を停止する。

1.6.廃棄・譲渡前の初期化



IoT 機器にも、通常の IT 機器と同様に重要な情報が保存されている可能性がある。そのため、IoT 機器を使わなくなった、IoT 機器のサポートが終了した等により、IoT 機器を廃棄・譲渡する場合、初期化による情報の消去等の適切な対応を行う必要がある。

◆ IoT 機器内には重要情報が存在

IoT 機器内には様々な情報が保存されており、その中には悪用されると様々な被害に至る重要情報もある。例えば、機器自体や機器が通信するインターネット上のサービスにログインするためのユーザー名（ID）やパスワードがある。GPS 機能を搭載している場合は、IoT 機器の位置情報、つまり、自宅や個人の行動履歴の情報がある。さらに、クレジットカード等による決済機能がある場合は、クレジットカード情報等が含まれている可能性もある。

そのような重要情報が漏えいすると様々な被害に遭うおそれがある。例えば、ID やパスワードが漏えいした場合、他のサービスで同じものを使い回していると、そのサービスに不正にログインされるおそれがある。また、自宅や行動履歴が漏えいすると、ストーカー等の被害に遭うおそれがある。さらに、クレジットカードの情報が漏えいした場合は、不正に利用されるおそれがある。

◆ IoT 機器を廃棄する前に初期化

IoT 機器の使用終了や、メーカーのサポート終了等により IoT 機器を廃棄せざるをえない場合がある。IoT 機器に保存されている情報の漏えいを防止するため、廃棄前に必ず機器を初期化する。通常、初期化方法はマニュアルに記載されているが、記載がない場合や不明点がある場合には販売元やメーカーの問い合わせ窓口に相談する。

IoT 機器に初期化機能がない場合は、機器を破壊することも検討する。機器内の情報を消去し、適切に廃棄してくれる専門の廃棄業者も存在する。

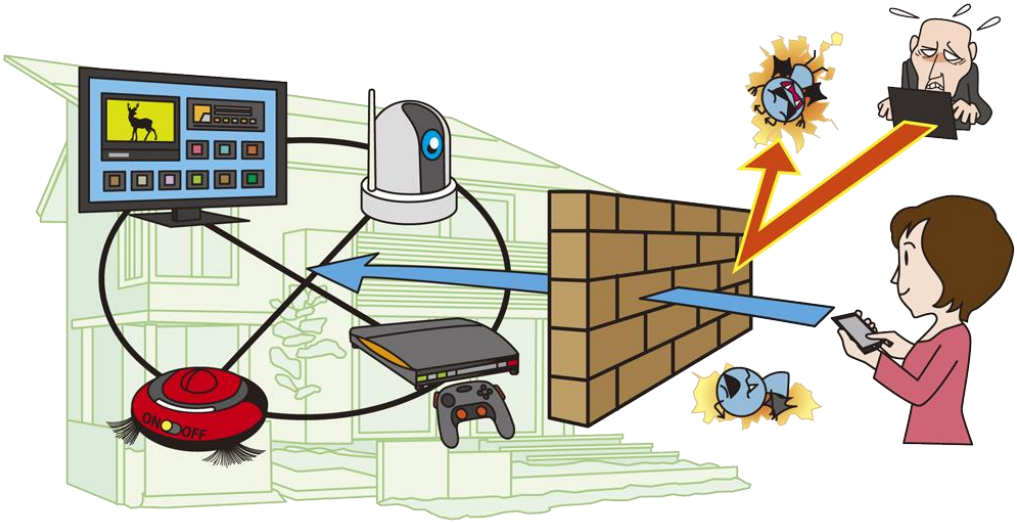
◆ IoT 機器の転売・譲渡時も初期化

使わなくなった IoT 機器を転売・譲渡する際も、廃棄時と同様に初期化を行い、自身に関連する情報は消去しておくこと。

◆ アプリもアンインストール

IoT 機器を管理するためにスマートフォン等にインストールしたアプリがある場合は、アプリをアンインストールしておく。これによりアプリが保存している情報も消去できる。

1.7. その他の対策



本節では IoT 機器を利用する上で実施すべきその他の対策について解説する。

◆ IoT 機器対応セキュリティ機器の導入検討

IoT 機器に対応したセキュリティ機器が存在する。例えば、家庭内に設置されているルーターにセキュリティ機器を接続して通信内容から攻撃を検知・防御する。そのようなセキュリティ機器を導入することで、IoT 機器のウイルス感染、不正遠隔操作や情報漏えいを防止する。

◆ セキュリティ機器の継続利用

セキュリティ機器には契約期間があるものがある。契約期間が過ぎると機能が制限されたり、そもそもすべての機能が使えなくなるおそれがある。IoT 機器のセキュリティを確保するためには、契約期間が終了する前に継続利用や他製品への移行を検討する。その際、利用する機能やランニングコスト（月単位や年単位での費用）を考慮すること。

◆ 既存の IoT 機器の見直し

IoT 機器がウイルスに感染した場合、周辺にある他の IoT 機器にも感染が拡大するおそれがある。例えば、Mirai と呼ばれるウイルスは周辺に感染できる脆弱な IoT 機器がないかを探索する機能を持っている。自宅のネットワーク内に脆弱な設定または脆弱性を放置した IoT 機器がある場合、その IoT 機器はウイルスに感染するおそれが高い。そのため、新規購入した IoT 機器のみならず、既に利用している IoT 機器についても本書の 1.2 節、1.3 節、1.4 節、1.5 節の観点で見直しを行う。

また、見直しを行うためにどの機器がネットワークにつながっているかを把握、管理する（見える化する）ことも重要である。

◆ ウイルスに感染してしまったら

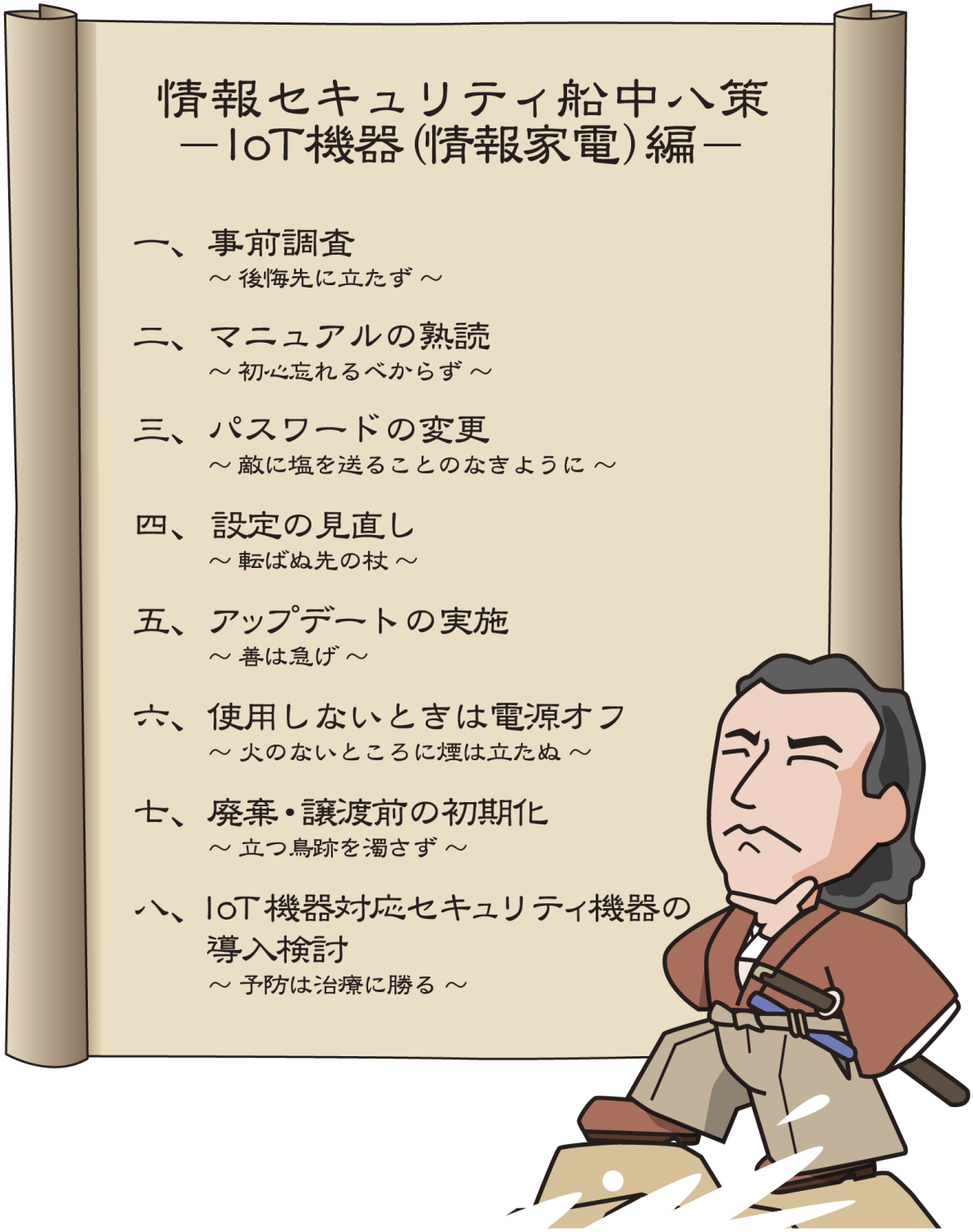
万が一、ウイルスに感染した場合は、IoT 機器を初期化する。初期化ができない場合や初期化しても解決できない場合は、メーカーのサポート期間内であればメーカーのサポート窓口に相談する。サポート期間外であれば、IoT 機器を廃棄し、最新の IoT 機器を購入する。

1章.情報セキュリティ対策の基本：参考資料

1. IPA：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
2. 「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

付録：情報セキュリティ船中八策 IoT 機器（情報家電）編

江戸時代に坂本龍馬がまとめたと言われている「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からさらに 8 つを厳選し、解説的にことわざと併記した「情報セキュリティ船中八策 IoT 機器（情報家電）編」を以下に示す。



このページは空白です。

2章. 情報セキュリティ10 大脅威 2018

2 章　情報セキュリティ 10 大脅威　2018

2017 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 2018」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 2018」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 2018「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等の不正利用	1	標的型攻撃による被害
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
ネット上の誹謗・中傷	3	ビジネスメール詐欺による被害
スマートフォンやスマートフォンアプリを 狙った攻撃	4	脆弱性対策情報の公開に伴う 悪用増加
ウェブサービスへの不正ログイン	5	脅威に対応するための セキュリティ人材の不足
ウェブサービスからの個人情報の窃取	6	ウェブサービスからの個人情報の窃取
情報モラル欠如に伴う犯罪の低年齢化	7	IoT 機器の脆弱性の顕在化
ワンクリック請求等の不当請求	8	内部不正による情報漏えい
IoT 機器の不適切な管理	9	サービス妨害攻撃によるサービスの停止
偽警告による インターネット詐欺	10	犯罪のビジネス化 （アンダーグラウンドサービス）

組織における脅威は、経営層やシステム管理者、開発者、一般従業員等様々な立場存在します。立場が変わると注意すべき脅威も変わります。**表 2.2** は、立場毎に注意すべき脅威を記載しています。立場毎の注意すべき脅威の参考にしてください。

表 2.2 10 大脅威 2018（組織）立場毎の注意するべき脅威

順位	脅威名（組織）	組織の立場	組織内の立場				
			経営層	セキュリティ管理者	システム管理者	製品開発者	一般従業員
1	標的型攻撃による被害	被害者	○	○	○	○	○
2	ランサムウェアによる被害	被害者	○	○	○	○	○
3	ビジネスメール詐欺による被害	被害者	○	○			○
4	脆弱性対策情報の公開に伴う悪用増加	ソフトウェアの開発者	○			○	
		ソフトウェアの利用者	○	○	○		○
5	脅威に対応するためのセキュリティ人材の不足	被害者	○	○	○	○	
6	ウェブサービスからの個人情報の窃取	ウェブサービスの開発者	○			○	
		ウェブサービスの提供者	○	○	○		
7	IoT機器の脆弱性の顕在化	IoT機器の開発者	○			○	
		IoT機器の利用者	○	○	○		
8	内部不正による情報漏えい	被害者	○	○	○	○	○
9	サービス妨害攻撃によるサービスの停止	被害者	○	○	○		
10	犯罪のビジネス化（アンダーグラウンドサービス）	被害者	○	○	○	○	○

経営層: 代表取締役社長や理事等の組織のトップ層
セキュリティ管理者: 組織におけるセキュリティの管理者
システム管理者: 組織で運用しているシステムの管理者
製品開発者: 製品の開発者
一般従業員: 営業や総務、財務等の組織におけるIT利用者

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 2018 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。

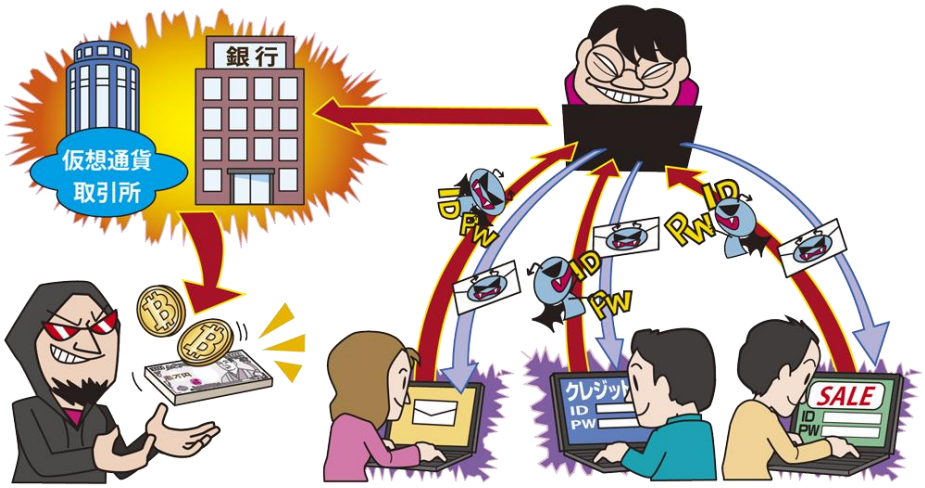
このページは空白です。

2.1. 情報セキュリティ10大脅威（個人）

組織ランク外

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等の不正利用

～被害は継続して発生、仮想通貨に関する被害も～



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、不正送金や不正利用が行われている。2017 年は、インターネットバンキングの被害件数と被害額は減少傾向だが、新たに仮想通貨利用者を狙った攻撃が確認されている。

＜攻撃者＞

- 犯罪グループ・犯罪者

＜被害者＞

- 個人（インターネットバンキング、クレジットカード、仮想通貨等の利用者）
- 組織（インターネットバンキング利用者）
- 組織（金融機関、仮想通貨交換業者）

＜脅威と影響＞

端末をウイルスに感染させたり、フィッシング詐欺等により窃取したインターネットバンキングやクレジットカードの情報を悪用した攻撃が行われている。それにより、インターネットバンキングやクレジットカードの利用者は、不正送金やクレジットカード悪用等により、金銭的な被害を受ける。

昨今、被害は PC に加えスマートフォン等のモバイル端末も攻撃対象となっているほか、2017 年には仮想通貨利用者を標的とした攻撃も確認されている。

＜攻撃手口＞

◆ ウイルス感染

攻撃者が、悪意あるファイルを添付したり、悪意あるウェブサイトのリンクを記載したメール等を送信し、添付ファイルを開かせたり、リンクをクリックさせることで、端末をウイルスに感染させる。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、仮想通貨交換所等にログインすると、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クレジットカードの不正利用、仮想通貨交換所から仮想通貨の窃取等を行う。

◆ フィッシング詐欺

攻撃者は、実在するインターネットバンキングのウェブサイトを模した偽のウェブサイト（フィッシングサイト）を作成する。その後、フィッシングサイトのリンクが記載されたメールを送信し、フィッシングサイトにアクセスさせ、フィッシングサイト上で入力したログイン情報等を窃取する。メール内では、実在する企業や組織を騙り、記載されているリンクも正規の URL を模倣しているものもある。

また、実在するショッピングサイトを騙り、メール件名に「請求書」、メール本文に「キャンセルはこちら」というリンクを記載してフィッシングサイトに誘導する手口も確認されている。メールの受信者はキャンセルしようとしてフィッシングサイトに誘導される。

＜事例または傾向＞

◆ **インターネットバンキング不正送金件数は減少するも、仮想通貨交換所が攻撃対象に**

警察庁によると、2017 年は、インターネットバンキング不正送金発生件数は 425 件、被害額は約 10 億 8,100 万円となり、2016 年の 1,291 件、約 16 億 8,700 万円と比較して発生件数、被害額共に減少している。ただし、1 件当たりの被害額は増加している。また、電子決済サービスを使用して仮想通貨交換所に対して送金を行う新たな手口も確認されている。[1]

◆ **情報窃取を目的としたウイルス「URSNIF」の被害拡大**

実在する企業やサービスを騙り、メールの本文中に記載されているリンクをクリックさせ、ウイルス「DreamBot」に感染させる被害が拡大した。[2,3] このウイルスは情報窃取を目的としたウイルス「URSNIF」の亜種で 2016 年末頃から感染被害が発生していたが、2017 年に入り感染被害が拡大した。感染すると、インターネットバンキング用認証情報やクレジットカード情報等を窃取されるほか、犯人に PC を乗っ取られ、不正操作されるおそれがある。さらに、このウイルスは仮想通貨も標的としている。感染した状態で仮想通貨交換所のウェブサイトにログインすると、入力した ID やパスワードが窃取されるおそれがある。

◆ **クレジットカード不正使用の被害額は増加**

一般社団法人日本クレジット協会によると、2017 年第 1 四半期から第 3 四半期までのクレジットカードの番号盗用被害額は 130.3 億円となり、前年同期間の 67.8 億円の 2 倍近くに増加している。また、不正被害の内、番号盗用被害が 7 割以上を占めており、ウイルス感染やフィッシング詐欺への警戒が必要である。[4]

＜対策/対応＞

個人（利用者）

- 被害の予防
  - ・受信メールや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（普段は表示されない）ポップアップに個人情報等は入力しない
  - ・事例・手口の情報収集

    銀行や公的機関から公開される注意喚起等を確認する。
  - ・OS・ソフトウェアの更新
  - ・セキュリティソフトの導入
  - ・ファイルの拡張子を表示させる設定
  - ・パスワードの適切な管理と運用

    パスワードの管理方法については本書の個人 5 位の対策を参考にして欲しい。
  - ・多要素認証等、銀行が推奨する認証方式の利用
  - ・仮想通貨の安全な利用

    利用端末のセキュリティ対策やウォレットの適切な管理を心がける。
- 被害の早期検知
  - ・不審なログイン履歴の確認
  - ・口座やクレジットカードの利用履歴の確認
  - ・利用時のメール連絡機能等の利用
- 被害を受けた後の対応
  - ・該当サービスのコールセンターへの連絡

    金融機関やクレジットカード会社によっては、全額または一部補償してくれる場合がある。
  - ・クレジットカードの停止
  - ・システムの復元・初期化
  - ・パスワードの再設定

参考資料

1. 平成29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/publications/statistics/cybersecurity/data/H29_cyber_jousei.pdf
2. インターネットバンキングの不正送金の被害に注意
https://www.jc3.or.jp/topics/dreambot.html
3. 国内ネットバンキングを狙う新たな脅威「DreamBot」を解析
http://blog.trendmicro.co.jp/archives/14588
4. クレジットカード不正使用被害の集計結果
https://www.j-credit.or.jp/information/statistics/download/toukei_03_f_171228.pdf

組織 2 位

2位 ランサムウェアによる被害

～ランサムウェアの感染経路拡大～

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ロック等を行い、金銭を支払えば復旧させると脅迫する犯罪行為の手口に使われるウイルスである。そのランサムウェアに感染する被害が引き続き発生している。さらに、ランサムウェアに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や外付け HDD に保存されているファイルも暗号化されるおそれがある。2017 年には、OS の脆弱性を悪用し、ネットワークを介して感染台数を増やすランサムウェアも登場した。

＜攻撃者＞

- 犯罪グループ・犯罪者

＜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させ、PC やスマートフォンに保存されているファイルの暗号化や PC やスマートフォンの操作ができないように画面ロック等し、復旧を名目に金銭を要求される被害が発生している。また、暗号化や画面ロック以外にも、ファイルを破壊したり、データを外部に流出させたり、OS を起動できないようにし、金銭を要求されるケースも確認されている。

一般家庭で利用する PC やスマートフォンには、旅行や結婚式等の思い出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等され、閲覧できなくなる。なお、復旧のため金銭の要求に応じても、確実に復旧される保証はなく、支払った金銭は犯罪グループの活動資金となり、犯罪を助長させる。

＜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付きのファイルやランサムウェアをダウンロードするファイルを添付し、添付ファイルを開かせることで感染させる。

◆ **ウェブサイトから感染（脆弱性を悪用）**

メール本文のリンクをクリックさせる等で攻撃者が用意した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させる。また、不正広告をクリックさせることで感染させる（ウェブサイトを表示させただけで感染するケースもある）。[1]

◆ **OS の脆弱性を悪用**

OS の脆弱性を悪用することにより、パッチを当てていない端末をインターネットに接続しているだけで感染させる。

◆ **スマートフォンアプリのインストール**

公式マーケット等に不正アプリを公開し、そのアプリをインストールさせることで、スマートフォンをランサムウェアに感染させる。

＜事例または傾向＞

◆　自己増殖型のランサムウェアの登場

ランサムウェアに感染する経路として、これまではメールの添付やウェブサイトの閲覧経由だったが、2017 年は、OS の脆弱性を悪用して、ネットワークに接続している PC 間で感染を拡大するタイプが登場した。代表的なものとして、「WannaCry」や「NotPetya」等がある。[2] 特に、WannaCry は、世界的に感染が拡大し、国内の大手企業や地方公共団体等でも被害が確認されており、大きくメディアで報道された。

◆　対策されない機器、依然として感染が継続

2017 年 11 月になっても「WannaCry」の感染被害が確認されている。2017 年 3 月にマイクロソフト社よりパッチが公開されていたが、対策を実施していない端末が狙われている。[3]

◆　セキュリティ対策が日々進化する一方、攻撃も進化

不正なファイルの振る舞いを予測して検出する等の機能を持つ機械学習を利用したセキュリティソフトも存在しており、セキュリティ対策は日々進化している。一方、ランサムウェアの中には、この機械学習を利用したセキュリティ対策を回避する手法を採用しているものが確認されており、攻撃も進化し続けている。[4]

＜対策/対応＞

個人（PC、スマートフォン利用者）

- 被害の予防（被害に備えた対策含む）
  - ・ 受信メールや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
  - ・ サポートの切れた OS の利用停止・移行
  - ・ アプリのアクセス権限の確認

  その他のスマートフォン関連の対策は本書の個人 4 位の対策を参考にして欲しい。
  - ・ バックアップの取得

  光学メディア（DVD-R、BD-R 等）、外付け HDD、USB メモリー等、外部記憶媒体へ定期的にバックアップを行う。なお、バックアップに使用する記録媒体は、暗号化等されないように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。

  バックアップから復旧できることを事前に確認しておくことも重要である。
- 被害を受けた後の対応

  ・バックアップから復旧

  ・復号ツールの活用

  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」にて、複数の復号ツールを提供している。[5] 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、これらの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、Microsoft OneDrive 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。

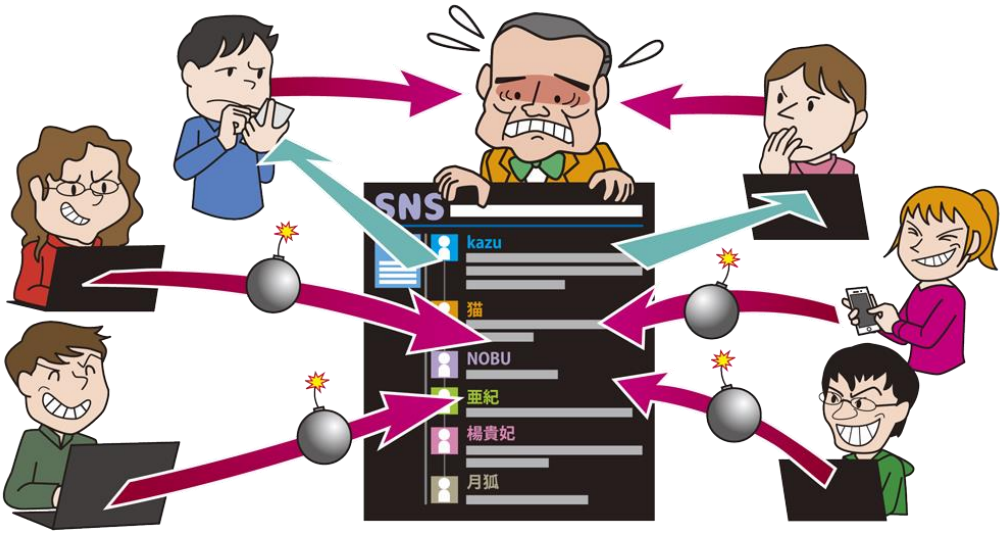
参考資料

1. 「見ただけで感染」する脆弱性攻撃サイトの国内状況
http://blog.trendmicro.co.jp/archives/14420
2. 安心相談窓口だより:WannaCryptorの相談事例から学ぶ一般利用者が注意すべきセキュリティ環境
https://www.ipa.go.jp/security/anshin/mgdayori20170713.html
3. トレンドマイクロ、「2017年国内サイバー犯罪動向」速報を発表
https://www.trendmicro.com/ja_jp/about/press-release/2018/pr-20180110-01.html
4. ランサムウェア「CERBER」、機械学習を利用したセキュリティ対策を回避
http://blog.trendmicro.co.jp/archives/14661
5. The No More Ransom Project
https://www.nomoreransom.org/

組織ランク外

3位 ネット上の誹謗・中傷

～匿名性を悪用した心無い投稿が横行、情報モラルを身に着けよう～



コミュニティサイト（ブログ、SNS、掲示板等）上で、個人や組織に対して誹謗・中傷や犯罪予告をする書き込みが行われている。コミュニティサイトへの書き込みは、匿名性や手軽さから安易に投稿されてしまう傾向にある。また、SNS を使った犯罪は社会的な問題となっており、2017 年は殺人事件にまで発展した事例もあった。

＜攻撃者＞

- 情報モラル・リテラシーが低い人
- 悪意・違法性の意識を持っている人

＜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の普及と共に、コミュニティサイトが広く利用され、不特定多数の人と容易にコミュニケーションを行うようになった。その反面、自分の氏名を明かさずに、自分の意見を発信できる点から、特定の個人や組織に対し誹謗・中傷や犯罪予告をする行為が後を絶たない。さらに関係のない第三者も誹謗・中傷に同調することでエスカレートしてしまう場合がある。

誹謗・中傷や差別的発言を受けた被害者は心理的に苦しむことになる。また、組織が誹謗・中傷を受けた場合には、風評被害等で社会的な信頼が低下し、結果的に組織に大きな不利益を及ぼすおそれがある。

＜要因＞

◆ 情報モラルや自己抑制力の欠如

自分の発言が他人を心理的に追い詰めるおそれがあることを理解しておらず、安易にネット上へ投稿してしまう。また、自身が持つ不満やストレスの捌け口として、過激な発言や個人・組織等の評判を落とすような不適切な発言を意図的に行っている。

◆ 個人が発信できる公共の場が増加

様々なコミュニティサイトが存在し、ブログや Twitter、動画配信等多種多様な情報の発信方法がある。それにより、個人が自由に情報を発信することができる場が増加しており、匿名での発信が可能である。一方、その弊害として、発信者の詐称や誹謗・中傷、犯罪予告の発信もできる。

＜事例または傾向＞

◆ 個人を中傷するブログを投稿

2017 年 7 月、芸能人を中傷するデマをブログに投稿し、所属事務所の業務を妨害した疑いで、男女数名が書類送検された。男女は「興味を引く記事を掲載してブログの閲覧数を伸ばし、広告収入を増やしたかった」と容疑を認めている。[1]

◆ **掲示板やウェブサイト等を使った脅迫行為**

2017 年 10 月に男性が、教育事務所のウェブサイトに女学生を襲撃する旨の犯行予告をしたとして、市内の小中学校に対する業務妨害の疑いで逮捕された。男性は家電量販店に設置された PC を使って犯罪予告を投稿していた。[2]

◆ **教諭が生徒を装い中傷**

私立中学校の教諭が同校の男子生徒になりすまして、特定の女子生徒を中傷する内容の書き込みを行った。一部の生徒からの指摘で発覚した。この問題を受けて、市教育委員会では、若手教職員を対象に SNS の使用や教職員の服務規定等の研修を行っている。なお、県教育委員会では、中傷を行った教諭に対する処分を検討している。[3]

◆ **容疑者の父親というデマ拡散により、誹謗・中傷、業務妨害**

交通事故を引き起こして、逮捕された容疑者の父親とその勤務先としてインターネット上に誤って掲載され、嫌がらせや中傷を含む電話が多数かけられた。その後もその情報が拡散し、業務へも支障が出た。[4]

＜対策/対応＞

個人（投稿者）

● 情報モラルや情報リテラシーの向上、法令順守の意識の向上

・誹謗・中傷や公序良俗に反する投稿をしない

・投稿前に内容を再確認

SNS 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、一見匿名で投稿したように見えても、プロバイダーに情報開示を依頼できる場合があるため、発信者は特定されるという認識を持つ。

個人（家庭）、組織（教育機関）

・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る。また、トラブルの事例を知り、悪質な行為は犯罪になりうることを理解する。[5]

個人（投稿を閲覧した側）

● 情報モラルや情報リテラシーの向上、法令遵守の意識の向上

・情報の信頼性の確認

発信されている情報が正しいとはかぎらないため、不用意に拡散せず、一次情報やその他複数の情報元を確認し、信頼できる情報かを総合的に判断する。また、不確定情報の発信は、犯罪になりうることを理解する。

・誹謗・中傷された人を支える

誹謗・中傷された人の相談に乗ってあげたり、誹謗・中傷しないよう注意を促す。

個人（誹謗・中傷された側）

● 被害を受けた後の対応

・冷静な対応と支援者への相談

一人で抱え込まず、周囲の人や公的相談機関へ相談する。[6]

・犯罪と思われる誹謗・中傷の投稿は、警察へ被害届を提出

・管理者やプロバイダーへ削除依頼

問題ある書き込みを削除したいときは、本人または関係者がウェブサイトの管理者やプロバイダーに削除を要請する。なお、削除により炎上の火種になるおそれもあるため、関係者等に相談して慎重に行う。

参考資料

1. 西田敏行さん中傷のブログで書類送検…芸能フェイクニュースにだまされるな
http://www.yomiuri.co.jp/science/goshinjyutsu/20170725-OYT8T50097.html
2. 女子生徒襲撃予告容疑の無職男逮捕　埼玉
http://www.sankei.com/region/news/171027/rgn1710270031-n1.html
3. 男性生徒なりすましツイートで市教委がSNS研修　埼玉県北本市
http://www.sankei.com/affairs/news/171225/afr1712250052-n1.html
4. 東名事故「容疑者の父」とデマ拡散容疑　福岡県警が捜索
https://www.asahi.com/articles/ASKDQ43Q4KDQTIPE00F.html
5. インターネットトラブル事例集（平成29年度版）
http://www.soumu.go.jp/main_content/000506392.pdf
6. インターネット人権相談受付窓口（法務省人権擁護局）
http://www.moj.go.jp/JINKEN/jinken113.html

組織ランク外

4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

～依然として公式アプリストアにも不正アプリが存在、ウイルス感染に注意～

公式マーケット等に公開されている不正アプリをスマートフォン利用者がインストールしてしまうことで、スマートフォン内の重要な情報を窃取されたり、不正に操作される被害が確認されている。また、データの暗号化等を行うランサムウェアの機能を持つアプリに加えて、2017 年は個人情報を公開すると脅すランサムウェアの機能を持つアプリも確認されている。

＜攻撃者＞

- 犯罪グループ・犯罪者

＜被害者＞

- 個人（スマートフォン利用者）

＜脅威と影響＞

公式マーケット等に不正アプリが紛れ込んでいることがある。不正アプリには、端末内の重要な情報を窃取する機能、端末を不正に利用する機能、ランサムウェアの機能等を持っている。そのような不正アプリをインストールしてしまうと、端末内の連絡先や通話記録等の重要な情報を窃取されたり、録画・写真撮影・通話録音機能を不正に利用されたり、端末内のデータが暗号化される等により金銭を要求される被害に遭うおそれがある。また、端末を不正に利用されることで、別の攻撃の踏み台にされ、攻撃者に悪用され利用者以外にも影響を与えることもある。

＜攻撃手口＞

◆ **公式マーケットに不正アプリを紛れ込ませる**

不正アプリを正常なアプリと見せかけて公式マーケットに公開する。利用者は公式マーケットのアプリは安全だと思い込んでしまい、安易にインストールしてしまう。

◆ **人気アプリに偽装**

ダウンロード件数等が多い人気アプリに偽装して、不正アプリを公式マーケット等に公開する。

＜不正アプリインストール後の悪用例＞

- 連絡先等の端末内の重要な情報を窃取
- 録画・写真・通話録音機能を不正に利用
- ランサムウェアへの感染
- DDoS 攻撃等の踏み台

＜事例または傾向＞

◆　人気アプリに便乗した不正アプリ

Android の公式マーケットである「Google Play」のアプリに「FalseGuide」と呼ばれるウイルスが仕込まれていた。このウイルスは「Pokémon GO」や「FIFA Mobile」等の人気アプリを含む、40 種類以上の有名ゲームの攻略法を解説するガイドアプリの中に仕込まれており、アプリによっては 5 万回以上ダウンロードされ、感染した利用者は 200 万人近くに及ぶとされている。[1]

◆　ルートキットを組み込んだ「ZNIU」ウイルス

2017 年 9 月に、Linux の脆弱性「Dirty COW」を悪用した「ZNIU」と呼ばれるウイルスが確認されている。「ZNIU」に感染すると管理者権限を持つバックドアを仕込まれ、リモートの攻撃者にシステムを乗っ取られるおそれがある。また「ZNIU」が仕込まれた不正アプリは、ポルノアプリやゲームアプリとしか見えないよう偽装されており、日本を含む 40 カ国ほどで感染が確認されている。[2]

◆　モバイル端末向けランサムウェア

2017 年 7 月に Android 端末向けランサムウェア「LeakerLocker」が確認されている。LeakerLocker が仕込まれた不正アプリをインストールすると、遠隔サーバーに個人情報を送出し、スマートフォンの連絡先に登録されているすべての宛先に転送すると脅迫し、金銭を要求する。[3]

◆　Android 端末を攻撃の踏み台にする不正アプリ

2017 年 8 月に分散型サービス妨害（DDoS）による大規模な攻撃が確認されている。攻撃を行ったのは Android 端末上で動作するアプリで、利用者が誤ってインストールした不正アプリを実行することにより、ボットネットが形成され、DDoS トラフィックを発生させる仕掛けになっていた。[4]

＜対策/対応＞

個人（利用者）

- 被害の予防（被害に備えた対策含む）

・アプリは公式マーケットから入手

Android アプリの場合、公式マーケット以外からも入手可能だが、極力公式マーケットから入手する。ただし、公式マーケットでも不正アプリが紛れていることがあるため、レビューの評価に加え、アプリ開発者等の情報を確認し、信頼できるアプリなのか判断する。

・アクセス権限の確認

アクセス権限の確認の際に、アプリの機能に対して適切かどうか確認を行い、関係のない権限が要求されていればインストールしないことが望ましい。特にデバイス管理者になるための要求をしている場合は注意が必要である。

・OS・アプリの更新

・セキュリティソフトの導入

セキュリティソフトを利用する。なお、偽のセキュリティソフトが公式マーケットに紛れ込んでいるおそれもあるため、インストール前に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しない。

・利用しないアプリのアンインストール

・バックアップの取得

写真等の大切なデータをバックアップする。

- 被害を受けた後の対応

・不正アプリのアンインストール

不正アプリをアンインストールする。できない場合は、端末を初期化する。

・バックアップから復旧

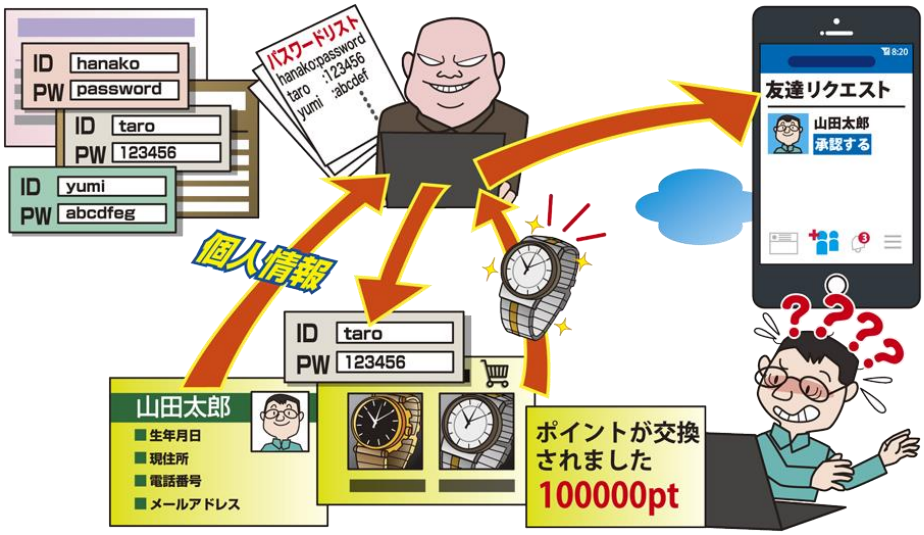
参考資料

1. 人気ゲームのガイドアプリにマルウェア、多数のAndroidデバイスが感染--Check Point
https://japan.zdnet.com/article/35100328/
2. 「Dirty COW」の脆弱性を突くAndroidマルウェア出現、日本でも感染
http://www.itmedia.co.jp/enterprise/articles/1709/27/news050.html
3. モバイル端末向けランサムウェア「LeakerLocker」、ユーザ情報の流出と引き換えに身代金を要求
http://blog.trendmicro.co.jp/archives/15624
4. Android端末を踏み台にしたDDoS攻撃発生　Google Playに300本の不正アプリ
http://www.itmedia.co.jp/news/articles/1708/29/news052.html

組織ランク外

5位 ウェブサービスへの不正ログイン

～パスワードの使いまわしに注意～



ウェブサービスに不正ログインされ、金銭的な被害や個人情報が窃取される等の被害が確認されている。2017 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り行われている。インターネットには多数のウェブサービスが存在しており、ウェブサービスの利用者が推測されやすいパスワードの使用やパスワードの使いまわしをしている場合、不正ログインが行われてしまう。

＜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＞

ID とパスワードが窃取または推測され、ウェブサービスへ不正ログインされる被害が引き続き確認されている。

ウェブサービスへの不正ログインによる影響は、利用しているウェブサービスの機能によって変わる。例えば、ショッピングサイトであれば、氏名や住所、電話番号が窃取されたり、不正な購買やポイント等が盗用される。また、SNS であればプライベートな写真やメッセージのやりとり等が覗き見される。さらに、その SNS を使って不正な広告やリンク等を知人へ配信された場合、自分以外も被害を受けてしまうおそれがある。

＜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する攻撃手法である。

複数のウェブサイトで同じ ID とパスワードを使いまわしている場合、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不正ログインをされて被害が拡大する。

◆ 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手法である。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を使用している場合、攻撃者にパスワードを推測されるおそれがある。SNS で公開している名前や誕生日等の情報を組み合わせたパスワードも危険である。[1] また、「qwerty」といった一見ランダムな文字列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。

◆ **ウイルス感染**

利用者が、攻撃者が用意した悪意のあるウェブサイトにアクセスしたり、メールに添付されている悪意あるファイルを開くことで使用している端末がウイルスに感染し、その端末で SNS やウェブサービスにログインすると、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利用者になりすまし、ウェブサービスを不正利用する。

＜事例または傾向＞

◆ **不正ログインによる個人情報流出とポイントの不正使用**

ガス・電気料金情報 Web 照会サービス「myTOKYOGAS」において、2017 年 9 月に不正ログインが行われ、106 件の個人情報が流出したおそれがあり、そのうち 24 件についてはポイントが他社のポイントに交換された形跡があった。[2] また、同社は、同年 8 月にも不正ログインが行われ、17 件の個人情報が流出していた。[3]

◆ **自分や自分の周りでアカウントの乗っ取り被害経験者がいるのは全体の約 4 割**

LINE が 2017 年に実施した「セキュリティ実態把握調査」によると、「自分や家族、恋人や友だち、知人等自分の周りの人で、アカウントを乗っ取られたことがある人がいる」と回答した人は全体の約 4 割であり、サービス別では「LINE」が多く、次いで「Twitter」「Facebook メッセンジャー」の順であった。また、インターネットや端末のセキュリティを「あまり意識していない」または「まったく意識していない」と回答した人も全体の約 3 割を占めており、情報リテラシーの向上が必要な状況である。[4]

◆ **面識のない女性のアカウントに不正アクセス**

面識のない女性 3 人の「Yahoo!」のアカウント等に計 12 回にわたり不正にアクセスしたとして、男性が逮捕された。ネットワーク上にデータを保存できるクラウドサービスに不正アクセスし、画像を盗み見していた。なお、アクセス時に必要な ID やパスワードは SNS に公開されている名前や誕生日から推測していた。[5]

＜対策/対応＞

個人（ウェブサービス利用者）

- 被害の予防
  - パスワードは長く、複雑にする
  - パスワードの使い回しをしない

    パスワードの基となるコアパスワードを作成し、その前や後ろにサービス毎に異なる識別子を付加することでユニークなパスワードを作成し、パスワードの使い回しを回避する。なお、コアパスワードは記憶し、識別子は電子ファイルや紙に記載しておくことでも良い。[6]
  - パスワード管理ソフトの利用

    パスワード管理ソフトのマスターパスワードを覚えておくだけですべてのウェブサービスのパスワードを一括管理できる。
  - 多要素認証等、ウェブサービスが推奨する認証方式の利用

    ワンタイムパスワード等の多要素認証を利用することで、仮に固定パスワードが知られたとしても、不正ログインや、その後の金銭被害等につながる重要な操作を阻止できる。
  - 利用をやめたサービスの退会
- 被害を受けた後の対応
  - パスワードを変更する
  - クレジットカードの停止

参考資料

1. 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
2. 不正アクセスによるお客さま情報の流出ならびにポイントの不正使用について
http://www.tokyo-gas.co.jp/important/20170922-01.html
3. 不正アクセスによるお客さま情報の流出について
http://www.tokyo-gas.co.jp/important/20170901-08.html
4. LINE「セキュリティリテラシー実態把握調査」
https://linecorp.com/ja/pr/news/ja/2017/1756
5. 面識のない女性のアカウントに不正アクセス
http://www.sanspo.com/geino/news/20170614/tro17061419020010-n1.html
6. 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

6位 ウェブサービスからの個人情報の窃取

～ウェブサービスの利用者は登録する個人情報を必要最小限に～

2017 年も引き続き、ウェブサービスの脆弱性が悪用され、ウェブサービスに登録した個人情報やクレジットカード情報を窃取される事件が多発している。窃取した情報を悪用されると不審メールを送信されたり、クレジットカード情報を不正利用されるおそれがある。

＜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者）

＜脅威と影響＞

近年、多くの企業がウェブサービスを提供する事業を行っている。それに伴い、利用者はウェブサービスを利用するためにメールアドレスやクレジットカード情報等、多くの重要な情報を登録している。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いる。それらのソフトウェアをウェブサービス提供者が適切に管理していない場合、セキュリティパッチ等が公開されていても適用されておらず、脆弱性を内在したままサービスを提供している状態となる。

ウェブサービス利用者がこのようなウェブサービスを利用している場合、攻撃者にソフトウェアの脆弱性を悪用されて、登録してある個人情報等の重要な情報を窃取されるおそれがある。また、窃取された情報を不正利用されると、クレジットカード情報の不正利用等の二次被害につながるおそれがある。

＜攻撃手口＞

◆ **ウェブサービスで利用されるソフトウェアの脆弱性を悪用**

ウェブサービスに存在する脆弱性を悪用され個人情報等の重要な情報を窃取される。特に、ウェブサービスで広く使用されているソフトウェアの場合、脆弱性への攻撃手法が判明すると、多くのウェブサービスで同様の攻撃や被害がすぐに発生するおそれがある。

＜事例または傾向＞

◆ **都税クレジットカード支払サイトに不正アクセス、合計 72 万件近くの情報が流出した可能性**

2017 年 3 月、GMO ペイメントゲートウェイ株式会社は、運営受託している東京都税クレジットカード支払いサイトや団体信用生命保険特約料のクレジットカード支払いサイトに不正アクセスが行われ、クレジットカード番号・有効期限等合計 72 万件近くの情報が流出した可能性があると発表した。不正アクセスはウェブサービスで利用されているソフトウェア「Apache Struts2」の脆弱性を悪用されたことが原因として公表されている。[1]

◆ **通販サイトへ不正アクセス、クレジットカード等の個人情報が流出した可能性**

日本文化センターは公式通販サイトのウェブアプリケーションの脆弱性を突く不正アクセスを受け、クレジットカード情報等が外部へ流出した可能性があることを公表した。漏えいしたのは、4 月 19 日から 5 月 12 日までに同サイトでクレジットカード決済を新規で利用した顧客の個人情報最大 189 件で、氏名、住所、クレジットカード番号、クレジットカード有効期限、セキュリティコードを窃取された可能性がある。[2]

◆ **テレビ局への不正アクセスで視聴者情報 37 万件が流出した可能性**

東京メトロポリタンテレビジョン（TOKYO MX）のウェブサイトが不正アクセスを受け、個人情報が流出した可能性があることが判明した。氏名とメールアドレスが約 1,270 件、ニックネームとメールアドレスが 37 万件流出した可能性がある。サーバーに脆弱性が存在し、その脆弱性を悪用して、不正アクセスされたと見られている。[3]

＜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
  - ・不要な情報を登録しない

    ウェブサイトからの情報漏えいに備えて、ウェブサービスを利用するための必須項目以外は、極力情報を登録しない。例えば、クレジットカード情報の登録は慎重にする。
  - ・利用しないウェブサービスの退会

    個人情報を登録したウェブサービスを使用しないと判断した場合は、退会することで、ウェブサービスから個人情報が削除される可能性がある。それにより、ウェブサービスから情報が漏えいするリスクを減らすことができる。なお、個人情報の取り扱いについては、そのサービスの規約に依存するため、ウェブサービスの入会時にしっかり確認しておく。
- 被害の早期検知
  - ・クレジットカードの利用明細の定期的な確認

    クレジットカード情報が窃取され、不正利用された場合、被害に気づける可能性がある。
- 被害を受けた後の対応
  - ・クレジットカードの停止
  - ・パスワードの変更

    パスワードが漏えいした場合、その情報を不正利用されるおそれがあるため、ウェブサービスを継続して利用する場合は、パスワードを変更する。

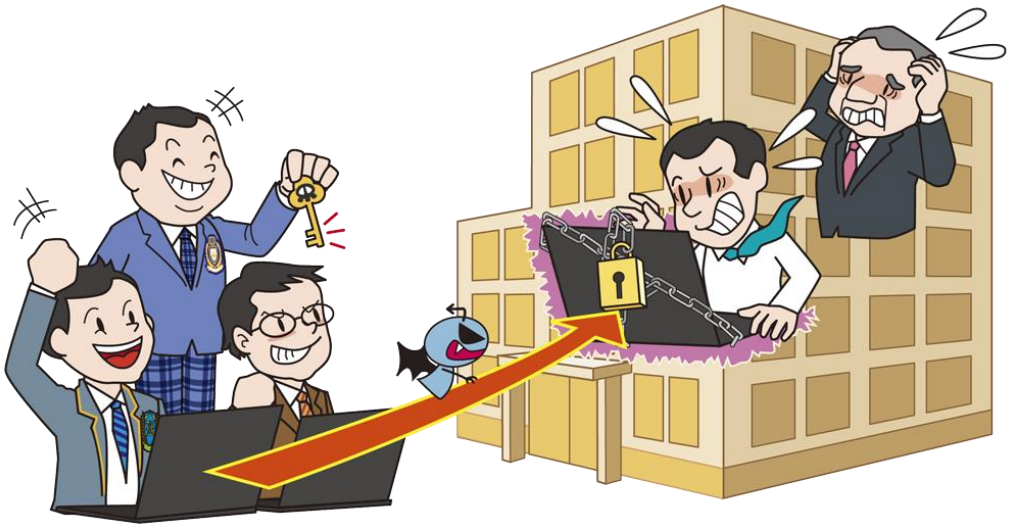
参考資料

1. Apache Struts 2の脆弱性を突かれて不正アクセス、都税支払いサイトなどからクレジットカード情報72万件が流出した可能性
https://internet.watch.impress.co.jp/docs/news/1049261.html
2. 5月に通販サイトへ不正アクセス、クレカなど個人情報が流出か - 日本文化センター
http://www.security-next.com/083999
3. 不正アクセスで視聴者情報37万件が流出か - TOKYO MX
http://www.security-next.com/086397

組織ランク外

7位 情報モラル欠如に伴う犯罪の低年齢化

～未来ある若者に情報モラル教育を～



2017 年も未成年者がサイバー犯罪の加害者として逮捕、補導される事件が確認されている。サイバー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・利用できるようになったことで、情報モラルの欠如した未成年者が、サイバー犯罪に手を染めやすくなっている。また、未成年者の PC やスマートフォンの所持も当たり前となってきているが、教員や親の監視が行き届きにくい。

＜攻撃者＞

- 情報モラル・リテラシーの低い若者
- 法令遵守の意識が欠けている若者

＜被害者＞

- 個人
- 組織（教育機関、ゲーム運営会社等）

＜脅威と影響＞

未成年者によるサイバー犯罪が多数確認され、逮捕・補導される事件が起きている。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り、未成年者はこれらの情報も悪用しているおそれがある。

未成年者による犯罪には、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場合もあるが、情報モラルの欠如により、自分の行為が犯罪と認識した上で私利私欲のために行っている場合もある。特に後者の場合、成人が行う犯罪と違いがなくなってきている。

教育機関やゲーム運営会社等、未成年者と関連が深い組織が攻撃対象なることが多い。例えば、DDoS 攻撃により、オンラインゲームのサービスを妨害したり、不正アクセスにより、他人のアカウントを不正利用する。また、攻撃対象は組織だけではなく、インターネット上でトラブルになった個人が狙われる場合もある。

＜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サイバー犯罪を行う。自己顕示欲や社会騒乱を目的に行うものもあり、SNS 等で犯行声明を出したり、標的を募集したりする場合がある。

◆ 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、面白半分に行ってしまう。

◆ 攻撃ツールや攻撃サービスの流通

近年、攻撃に悪用できるツールやサービス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ある。未成年者がそれらに興味を持ち、悪用して攻撃を行う。

＜事例または傾向＞

◆ **未成年者がランサムウェアを作成し逮捕**

2017 年 6 月に、大阪府の 14 歳の少年がランサムウェアを作成した容疑で警察に逮捕された。[1] 作成されたランサムウェアは、オープンソースのソフトウェア等を組み合わせて作られたものであり、ランサムウェアとしての機能を備えているものの、比較的簡易なものであった。少年は、ランサムウェアを作成した動機を、自分の知名度を上げるため等としていた。

また、同少年は、「iXintpwn（アイシントポウン）」等と呼ばれる、iOS 上で大量のアイコンを作成するウイルスも拡散していた。[2]

◆ **フリーマーケットアプリ「メルカリ」で少年らがウイルスを売買**

ウイルスの入手方法等の情報を、フリーマーケットアプリ「メルカリ」に出品したとして大阪府の 13 歳の少年が児童相談所に通告された。[3]

また、出品された情報の購入意思を示したとして 14 歳から 19 歳の少年 4 名が書類送検された。

動機について、出品した少年は金銭目的、購入の意思を示した少年らはいたずらに悪用する目的だった。

◆ **ゲームサーバーに不正アクセスした容疑で高校生 3 名を書類送検**

高校生 3 人が、人気のゲームで知り合った熊本県の中学生の ID とパスワードを使って当該ゲームのサーバーに不正アクセスし、勝手に 467 万円分の有料契約を結んだ疑いで書類送検された。[4]

被害者の中学生は、加害者の高校生らに有料契約の代行を頼んでおり、その際にトラブルがあったことが動機とされている。

◆ **中学生が警察をも欺く偽装工作を行い、誤認逮捕まで発展**

中学生が、Twitter で人気アイドルグループのコンサートチケットを売っていた女性に購入すると話を持ちかけ、女性の氏名や口座番号等を入手、その後、入手した情報を悪用した詐欺被害が確認された。中学生は、入手した情報を使い女性になりすまし、高校生ら 2 名が合計 8 万円の被害を受けた。また、警察は 2017 年 5 月になりすまされた女性を誤認逮捕し、19 日間拘留した。[5]

＜対策/対応＞

個人（家庭）、組織（教育機関）

- 情報モラルや情報リテラシーの向上
  - 情報モラルや情報リテラシーの教育、法教育の徹底

    未成年者へのモラル教育は、親や教師等、身近な大人が大きな影響力を持つため、幼い頃から家庭や学校でモラルを教える機会を作る等、責任を持った対応が求められる。また、悪質な行為は犯罪として、司法手続の中で重く処罰され得ること等の法教育も重要である。
- 被害の予防
  - インターネットの利用に年齢制限をかけるサービスやアプリを利用
  - 不要な機器を持たせない

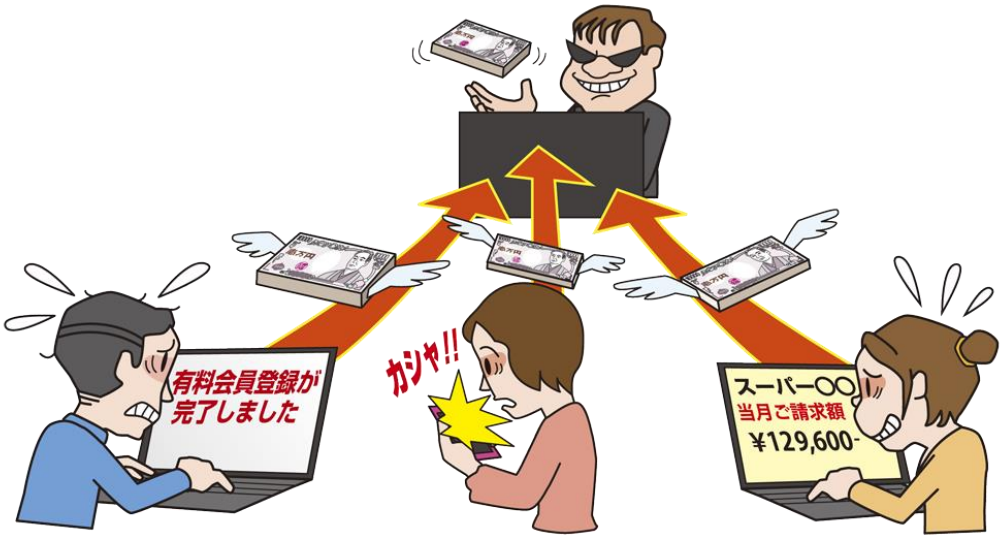
参考資料

1. 未成年者がランサムウェアを作る時代、日本初の逮捕事例を読み解く
http://blog.trendmicro.co.jp/archives/15133
2. OS 上で大量のアイコンを作成する不正プロファイル「YJSNPI ウイルス」こと「iXintpwn」を解説
http://blog.trendmicro.co.jp/archives/16007
3. メルカリで少年らがウイルス売買 「隠語」で出品、監視の目をかいくぐる
http://www.itmedia.co.jp/news/articles/1709/15/news052.html
4. サーバーに不正アクセスした容疑 高校生3人を書類送検
https://www.asahi.com/articles/ASK325H60K32TLVB00H.html
5. 成り済まし女子中生、匿名性悪用 徳島・チケット詐欺
http://www.topics.or.jp/localNews/news/2017/09/2017_15052653456481.html

組織ランク外

8位 ワンクリック請求等の不当請求

～複数回のクリックにより不当請求されるケースも～



PC やスマートフォンを利用中にアダルトサイトの請求画面が表示され、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。1 度のクリックによる請求だけでなく、複数回のクリックをさせることで、請求の正当性を主張されて不当請求されてしまう被害も確認されている。

＜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＞

PC やスマートフォンの利用者が悪意のあるアダルトサイト等へアクセスしたり、メールや SNS に記載されたリンクをクリックすることで、会員登録料や利用料といった名目で金銭の請求画面を表示するワンクリック請求が依然として発生している。

請求画面では、早急に支払わなければ訴訟をするといった脅しにより、被害者の不安な心理を煽ってくる。被害者は焦って料金を支払ってしまっている。支払った後も、再度支払いを要求される場合もある。

また、そういった被害者を狙って、ワンクリック請求の対処法を検索サイト等で検索する中で消費者救済を装う怪しい業者に金銭を騙し取られる二次被害も発生している。

＜攻撃手口＞

◆ 悪意あるウェブサイトの閲覧

アダルトサイト内に表示されている「18 歳以上」の画像等をクリックすることにより、会員登録完了の請求画面が表示される。誤って登録してしまったと閲覧者に勘違いさせ、不当に金銭を請求する。

◆ メールに記載されたリンクのクリック

届いたメールに記載されているリンクをクリックすることにより、ウェブサイトで入会完了の画面が表示され、高額な入会金を請求される。

◆ 不正プログラム・アプリをインストールさせる

無料動画ダウンロード等と偽り、不正プログラムやアプリをインストールさせる。請求画面の閉じても数分おきに請求画面が表示され、PC やスマートフォンを再起動しても再び画面が表示されることもある。[1]

◆ 電話をかけるように誘導

請求画面にお問い合わせ先の電話番号を表示し、退会を焦る被害者に電話をかけさせるように誘導する。電話をかけると相手に電話番号が知られ、さらに、「再生 OK ボタンを押したから契約は成立しているため解約はできない」等と支払いを迫られることもある。また、電話中に退会や支払いを免除するためと称し

て個人情報を聞きだそうとする場合がある。個人情報を伝えてしまうと、その情報を悪用されるおそれがある。

◆ **スマートフォン機能の悪用**

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 ボタンをタップするだけで犯罪者へ電話発信させる手口もある。

＜事例または傾向＞

◆ **依然として多いワンクリック請求サイト**

ワンクリック請求の被害は継続して発生している。2017 年 10 月には 160 万件以上の詐欺サイトが検知されており、PC だけでなくスマートフォンを対象にした詐欺サイトも検知されている。[2]

◆ **複数回クリックさせる詐欺の登場**

これまでは、1 回クリックしただけで不当請求を受けるワンクリック請求が主流だった。しかし、「再生」や「年齢確認」、「サイト入室に同意」等といった項目を数回クリックさせた上で、不当請求される事例もある。キャンセルするために業者に電話をかけたとしても、複数回クリックしたため入会の意思はあったと言われ、被害者は不当請求に応じてしまうおそれが高まる。[3]

◆ **ワンクリック請求の被害者を狙った詐欺**

ワンクリック請求の対処法を求めて相談した業者から不当請求される被害が発生している。ワンクリック請求画面が表示された被害者が、「消費生活センター」とインターネットで検索し、検索結果の上位に表示された公的機関以外の団体に相談したところ、依頼料として 5 万 4,000 円を請求された。[4]

◆ **ワンクリック請求によりギフト券を騙し取る**

ワンクリック請求に引っかかった被害者にアダルトサイトの退会料という名目でアマゾンのギフト券を 15 万円分騙し取る被害が発生している。アマゾンギフト券の利用番号を電話で聞き取り、騙し取った。[5]

＜対策/対応＞

個人（ウェブサービス利用者）

- 被害の予防
  - 不当請求には応じない

    不当な料金の請求画面が表示されても応じない。個人情報を取得したように見せかけていても、電話やメールをしたり、個人情報の入力を行っていない場合、攻撃者に情報は渡っていない。
  - 受信したメール内容の確認
  - アクセスするウェブサイトの確認
  - SNS（Twitter、Facebook 等）のメッセージのリンクは不用意にクリックしない
  - アプリのアクセス権限の確認

    その他のスマートフォン関連の対策は本書の個人 4 位の対策を参考にして欲しい。
  - 事例・手口の情報収集と学習

    日頃からニュースやセキュリティ機関のウェブサイト等から事例や手口等の情報を収集し、学習しておくことも有効である。
- 被害を受けた後の対応
  - 相談する際には信頼できる機関を利用する

    国民生活センターや地域の消費生活センター等、正しい対処法を紹介してくれる機関に相談する。[6]
  - システムの復元・初期化 [7]

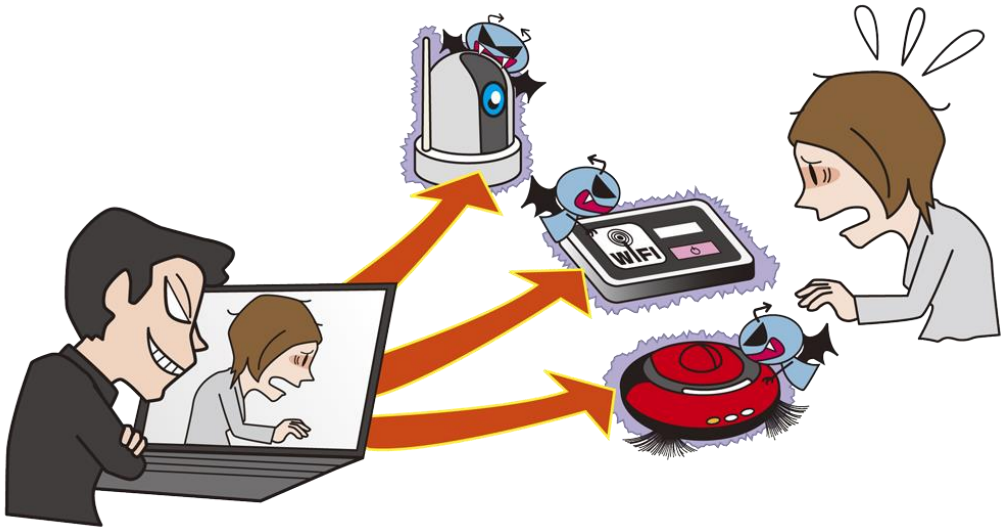
参考資料

1. 国民生活センター アダルト情報サイト
http://www.kokusen.go.jp/soudan_topics/data/adultsite.html
2. インターネット詐欺リポート（2017年9月度）
https://www.onlinesecurity.jp/reports/2017/201710.html
3. ワンクリック詐欺ならぬ「4クリック詐欺」が急増
https://www.moneypost.jp/131605
4. ワンクリック詐欺 解決装い… 相談で二次被害 ご用心 広告を悪用、依頼料請求
https://www.nikkei.com/article/DGXMZO18383050020720 17AC8Z00/
5. 被害額6億円超かクリック詐欺 容疑で男6人逮捕、京都府警
http://www.sankei.com/west/news/170224/wst1702240017-n1.html
6. 独立行政法人国民生活センター
http://www.kokusen.go.jp/ncac_index.html
7. ワンクリック請求被害への対策
https://www.ipa.go.jp/security/anshin/1click.html

組織ランク外

9位 IoT 機器の不適切な管理

～普及する IoT 製品、利用の前にセキュリティ対策を～



昨今、インターネットに接続されている機器である IoT 機器の利用が進んでいる。一方、利用者は IoT 機器がインターネットに接続されていることを意識せずに利用しており、セキュリティ対策等の適切な管理が行われていないことがある。管理を怠っている IoT 機器が狙われ、室内の覗き見や攻撃の踏み台にされるといった被害が出ている。

＜攻撃者＞

- 犯罪グループ

＜被害者＞

- 個人（IoT 機器利用者）
- 組織（企業、IoT 機器利用者）

＜脅威と影響＞

IoT 機器が世間に浸透したことによって、様々な情報家電、オフィス機器、医療機器、産業用設備・機器、制御システム等がネットワークを通じて利用できるようになってきた。一方、IoT 機器の利用者は IoT 機器がネットワークにつながっているという意識が低く、セキュリティ対策を行っていないケースがある。例えば、初期設定のまま利用していたり、脆弱性が公開されたとしても適切な対策を取らずに利用しているといった危険な状況にある。攻撃者はそのような IoT 機器に攻撃を行い、機器を乗っ取り、様々な攻撃を行う。

＜攻撃手口＞

◆ 初期設定の IoT 機器にウイルス感染

新規購入した IoT 機器には初期パスワードが設定済みの場合がある。初期パスワードは取扱説明書に記載されているため、攻撃者は初期設定のまま利用している IoT 機器に不正アクセスして、ウイルスに感染させ、IoT 機器を乗っ取る。

◆ 脆弱性を悪用した攻撃

公開された IoT 機器の脆弱性を悪用し、パッチ適用をせずに利用している IoT 機器を乗っ取る。

◆ 感染を拡大させる

攻撃者は、ウイルス感染させた IoT 機器を使って、その周辺に設定不備や脆弱性を放置した IoT 機器が存在しないか探索する。存在すれば、その IoT 機器もウイルスに感染させ、次々と感染範囲を拡大させる。

＜乗っ取られた後の攻撃や悪用の例＞

- 覗き見や盗撮

ネットワークカメラやカメラ機能がある IoT 機器を乗っ取り、遠隔からカメラを操作したり、覗き見したり、盗撮される。

- DDoS 攻撃等の踏み台

IoT 機器を乗っ取り、DDoS 攻撃の踏み台にする。

IoT 機器の利用者は乗っ取られた被害者でありながら、「悪意のない加害者」として攻撃に加担させられることになる。また、踏み台にされていても、IoT 機器の CPU やトラフィックへの負荷が小さければ、踏み台にされていると気づけず、長期感染となるおそれがある。

＜事例または傾向＞

◆ シャープの掃除ロボでセキュリティ上の脆弱性を確認、映像を覗き見されるおそれも

シャープ製のロボット掃除機「COCOROBO（ココロボ）」の一部機種に脆弱性があり、第三者から不正に操作されるおそれがあった。この掃除機はスマートフォンから操作可能であり、操作に利用する無線 LAN に攻撃者がアクセス可能であると、この脆弱性を悪用して掃除機を乗っ取られる。さらにカメラ搭載モデルの場合、室内を覗き見され、プライバシー侵害となるおそれがある。シャープは本脆弱性に対応するパッチを提供しており、適用を呼びかけている。[1]

◆ IoT ウイルス「Mirai」の亜種が活発化

2017 年 11 月頃より、IoT 機器等に感染するウイルス「Mirai」の亜種による感染活動が活発化しているとして JPCERT コーディネーションセンター（JPCERT/CC）[2]、情報通信研究機構（NICT）および警察庁は 12 月 19 日、注意喚起を行った。国内ではロジテック製 Wi-Fi ルーターの 11 機種が該当しており、同社は 2013 年 6 月から 2014 年 10 月に公開したパッチを適用するよう、改めて注意喚起を行った。[3]

IoT 機器の利用者は、公開されている脆弱性対策を適用しないこともあり、被害拡大のおそれがある。

◆ IoT 機器を破壊するウイルス「BrickerBot」

IoT 機器のファイルを破壊して、完全に使用不能にする「BrickerBot」と呼ばれるウイルスの感染が広がった。このウイルスはログイン情報をデフォルトのままにして、変更していない IoT 機器を狙って感染する。感染した場合、機器を再起動すると使用不能となり、工場出荷時の状態に戻すボタンを押しても復旧できなくなる。BrickerBot の作者を名乗る人物は Mirai 等のウイルスに対抗するため、対策や管理が不十分な IoT 機器を使用不能状態にしたと主張している。[4]

＜対策/対応＞

個人（利用者）

- 情報リテラシーの向上
  - ・使用前に取扱説明書を確認
- 被害の予防
  - ・初期パスワードから長く複雑なものへ変更 [5]
  - ・外部からの不要なアクセスを制限
    アクセス端末を制限できる機能を活用する。
  - ・不要な機能やポートは無効化 [6]
  - ・パッチが公開されたら迅速に更新（自動更新機能を有効にする）
    パッチ情報をメール等で配信するサービスが提供されていれば、そのサービスを利用する。
  - ・使用していないとき、IoT 機器の電源を切る
  - ・廃棄前や下取りに出す前に初期化
    IoT 機器には様々な情報が設定されているため、廃棄前や下取りに出す前に初期化する。また、中古品購入時は、ウイルス感染や改ざんのおそれを考慮し、初期化してから使用する。
- 被害を受けた後の対応
  - ・IoT 機器の電源を切る
  - ・IoT 機器の初期化後、「被害の予防」を実施
    ウイルス感染により初期化できない場合は、メーカーのサポート窓口に相談する。
  - ・パッチが公開されていない場合は使用中止

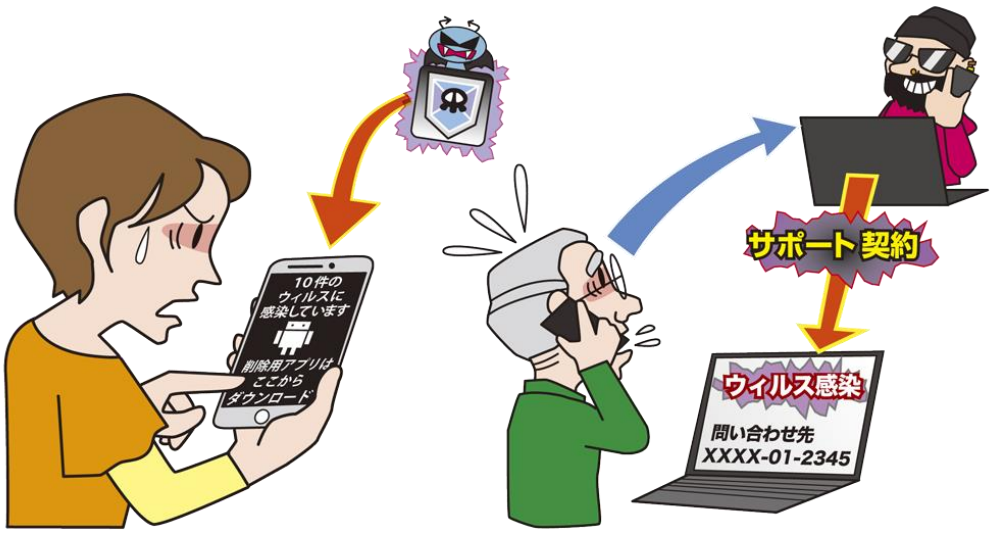
参考資料

1. ロボット掃除機 COCOROBO におけるセッション管理不備の脆弱性（JVN#76382932）
https://www.lac.co.jp/lacwatch/alert/20171117_001427.html
2. Mirai 亜種の感染活動に関する注意喚起
https://www.jpcert.or.jp/at/2017/at170049.html
3. ロジテック製300Mbps無線LANブロードバンドルータおよびセットモデル（全11モデル）に関する重要なお知らせとお願い
http://www.logitec.co.jp/info/2017/1219.html
4. IoT機器を破壊するマルウェア「BrickerBot」拡散中 「Mirai」に対抗か
http://www.itmedia.co.jp/enterprise/articles/1704/25/news056.html
5. 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
6. 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

組織ランク外

10位 偽警告によるインターネット詐欺

～その警告メッセージ、信じて大丈夫？～



PC やスマートフォンでウェブサイトを閲覧中に、突然「ウイルスに感染している」等の偽警告を表示し、利用者の不安を煽り、偽警告に記載された操作を行わせ、金銭的な被害や個人情報等を窃取される被害が発生している。偽警告は本物の警告と誤認されるように巧妙な細工が施されており、被害者は信じて指示に従ってしまう。

＜攻撃者＞

- 犯罪グループ

＜被害者＞

- 個人（インターネットサービス利用者）

＜脅威と影響＞

PC やスマートフォンでウェブサイトを閲覧中に、偽警告を表示し、利用者の不安を煽り、偽警告に記載された操作を行わせ、金銭被害や個人情報等を窃取される被害が引き続き発生している。

攻撃者はウェブサイト上の広告掲載の仕組みを悪用し、偽警告を表示させている。表示される偽警告は、有名な企業等を装っている場合があり、偽警告の内容を信用して指示に従ってしまう。攻撃者の指示に従うと、ソフトウェアの購入やサポート契約を結ばされたり、PC やスマートフォンへ不正なソフトウェアをインストールされる。また、企業のウェブサイトを模した偽のウェブサイトに誘導され、氏名、メールアドレス、クレジットカード情報を入力してしまうと、それらを攻撃者に窃取、悪用される等の被害に遭うおそれがある。

＜攻撃手口＞

◆ 偽警告を表示し、不安を煽り、誘導する

ウェブサイト上の広告掲載の仕組みを悪用し、「ウイルスに感染している」等の偽警告を表示する。閲覧者の不安を煽り、偽警告の指示に従わせる。偽警告を信じさせるために、有名な企業のロゴ等が使われる場合がある。

◆ 音声を流して、さらに不安を煽る

偽警告の表示に併せて警告音や警告アナウンスを流し、さらに不安を煽り、焦らせ、指示に従わせようとする。また、スマートフォンの場合、振動させて不安を煽る場合もある。

◆ サポート窓口を装い、電話をかけさせる

偽警告に表示されている連絡先に電話をかけるように誘導する。電話をかけるとオペレーターが「PC の状況を遠隔操作で確認する」等と説明し、遠隔操作ソフトをインストールさせる。遠隔操作により様々な画面を表示させてウイルスに感染しているかのように見せかける。その後、問題解決のために実施した作業の対価や今後の PC サポートの契約に誘導してクレジットカードやプリペイドカードでの支払いを不当に請求する。

◆ **偽セキュリティソフトを購入させる**

偽警告を表示し、警告の解決のために無償版の偽セキュリティソフトをインストールするように誘導する。セキュリティスキャンを行うと問題を検出したとのスキャン結果を表示し、修復するために有償版偽セキュリティソフトの購入を要求する。

◆ **アプリやソフトウェアをインストールさせる**

偽警告を表示し、警告の解決のためにスマートフォンであればアプリを、PC であればソフトウェアをインストールさせるよう誘導する。インストールしてしまうと、端末を操作されたり、個人情報等を窃取されるおそれがある。

＜事例または傾向＞

◆ **アニメーション等を利用した巧妙な騙しの手口**

2017 年 3 月にマウスのポインターが勝手に動いているアニメーションやマイクロソフト社の URL にアクセスしているようなアドレスバーの画像を表示させる偽警告の手口を確認している。この手口では、ウイルスに感染して PC が正常に操作できなくなったかのように閲覧者を錯覚させる。さらに、「5 分以内」等の時間制限を表示して、誰かに相談する時間を与えないように急かす。[1]

◆ **Google 社を騙る偽警告**

スマートフォンでウェブサイトの閲覧時に、「ウイルスに感染」と偽警告が表示される。偽警告には「Virus」等のウイルス検出を思わせる文字列を含んだサイト名や使用しているスマートフォンの機種名を表示して利用者の情報が相手に伝わっているかのように思わせる。偽警告の指示に従い、画面を進むと Google 社を偽装した画面が表示され、「Google Play」上の特定のアプリの入手と実行を促される。2017 年 11 月に確認した事例では、そのアプリはアフィリエイトプログラム（成功報酬型広告）により、アプリをインストールさせることで金銭的利益を得ようとすることが目的であるものと考えられている。[2]

＜対策/対応＞

個人（インターネット利用者）

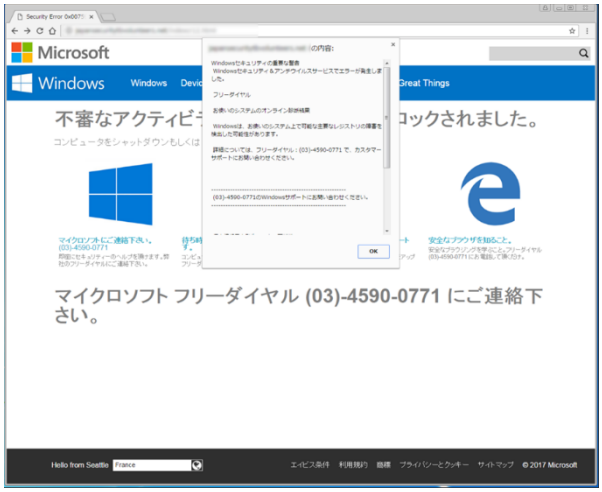
- 被害の予防
  - 事例・手口の情報収集

    日頃からニュースやセキュリティ機関のウェブサイト等から事例や手口等の情報を収集する。[3,4]
  - 偽警告が表示されても安易に従わない

    偽警告の指示に従いアプリやソフトウェアはインストールしない。また、電話をかけない、遠隔操作は許可しない、契約には応じない。
  - 偽警告が表示されたらブラウザを終了
- 被害を受けた後の対応
  - 遠隔操作ソフトをアンインストール[5]

    不安がある場合は、端末を初期化する。
  - サポート契約の解消

    近くの消費生活センター[6]に相談する。



図：マイクロソフト社を騙った偽警告の画面

参考資料

1. 独立行政法人情報処理推進機　安心相談窓口だより「偽警告で、また新たな手口が出現」
https://www.ipa.go.jp/security/anshin/mgdayori20170329.html
2. スマホの「ウイルス感染」偽警告に、ご注意を
http://blog.trendmicro.co.jp/archives/16382
3. フィッシング対策協議会
https://www.antiphishing.jp/
4. 独立行政法人情報処理推進機　安心相談窓口だより　被害低減のための偽警告の手口と対策を紹介する映像コンテンツを公開
https://www.ipa.go.jp/security/anshin/mgdayori20170411.html
5. 意図せずにインストールしてしまったプログラムをアンインストールする際の手順
https://www.ipa.go.jp/files/000054281.pdf
6. 独立行政法人国民生活センター　全国の消費生活センター等
http://www.kokusen.go.jp/map/

コラム：子供をめぐる状況というのは

SNS 等に起因して、未成年者が犯罪に巻き込まれる被害が後を絶ちません。警察庁の統計によれば、「平成 29 年度上半期におけるコミュニティサイト等に起因する事犯の被害児童数」は 919 人と過去最多となりました。[1]

犯罪者は、SNS 等で被害児童のプロフィールや投稿情報を確認し、その人となりや、悩んでいる事項等について知ることができます。その上で、金銭をエサに、援助交際を迫ったり、裸体画像を送信させる等し、未成年者の性を搾取しています。また、覚せい剤等の違法薬物が、掲示板やツイッター等で販売されている実態 [2] もあります。未成年者の性的自由、身体の安全に対する危険性が現に存在しています。

そんな中、2017 年 10 月、神奈川県座間市内において、複数の女性を殺害した疑いがあるとして、男が逮捕されました。容疑者は、Twitter を介し、自殺願望があった被害者らと知り合い、被害者の中には未成年者もいたとされています。[3]

この事件の真相は、司法の場において明らかにされることですが、インターネット社会に大きな衝撃を与えました。コミュニティサイト運営事業者等で構成される「青少年ネット利用環境整備協議会」は、2017 年 12 月、自殺等を紹介する等の投稿を確認した場合、積極的に対処する等の事項を盛り込んだガイドライン [4] を策定しました。全国 SNS カウンセリング協議会とも連携するとしています。ほかにも、「サイバー防犯ボランティア」と呼ばれる民間の方々の協力によるネット上の有害情報の発見・通報体制が強化されました。

このような施策は、SNS 等に起因した犯罪から未成年者を守る効果があるほか、悪質サイト運営者等に対する注意喚起にもなり得ます。

未成年者の性的自由を害する行為は厳しく処罰されます。2017 年 6 月、刑法が改正され、13 歳未満の者と性交等した場合、5 年以上の有期懲役に処せられる可能性があります。業として覚せい剤を売買した場合、無期懲役に処せられる可能性もあります。悪質な内容の投稿を積極的に放置するサイトは、これらの犯罪を助長した者として、行為者と同等の法的責任を負うという意識が社会で芽生えれば、上記施策がより実効的になるものと思われます。

「子供をめぐる状況というのは、学校と家庭と友人、この３つに平等に培われ、平等に責任がある。」という言葉があります（漫画家：手塚治虫氏）。現在の社会では、子供をめぐる問題は、インターネット利用者と事業者全体にも、平等に責任があると思われます。

参考資料

1. 警察庁「平成 29 年上半期におけるコミュニティサイト等に起因する事犯の現状と対策について」
http://www.npa.go.jp/cyber/statics/h29/H29_siryou.pdf
2. 警視庁「危険ドラッグ撲滅！！」
http://www.keishicho.metro.tokyo.jp/kurashi/drug/drug/bokumetsu_drag.html
3. 朝日新聞 DIGITAL：座間9遺体、1都4県の15～26歳と確認　警視庁発表
https://www.asahi.com/articles/ASKC97RCRKC9UTIL070.html
4.「LINEやTwitterなど参加の協議会、座間市事件を受け緊急提言」
http://itpro.nikkeibp.co.jp/atcl/news/17/120702817/

2.2. 情報セキュリティ10大脅威（組織）

個人ランク外

1位 標的型攻撃による被害

～組織全体でセキュリティ意識の向上を～

企業や民間団体や官公庁等、特定の組織を狙う、標的型攻撃が引き続き発生している。メールの添付ファイルを開かせたり、悪意あるウェブサイトにアクセスさせて、PC をウイルスに感染させる。その後、組織内の別の PC やサーバーに感染を拡大され、最終的に業務上の重要情報や個人情報が窃取される。さらに、金銭目的な場合は、入手した情報を転売等されるおそれもある。

＜攻撃者＞

- 諜報員、産業スパイ
- 犯罪グループ・犯罪者

＜被害者＞

- 組織（官公庁、民間団体、企業、研究機関、教育機関　等）

＜脅威と影響＞

メールの添付ファイルやウェブサイト、外部記憶媒体等によって標的の組織の PC をウイルスに感染させ、組織内部に潜入する標的型攻撃が確認されている。ウイルスに感染すると、感染した PC を攻撃者に遠隔で操作され、組織内部の情報を探索されたり、重要情報を窃取される。さらに、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おそれがある。また、システム破壊や業務妨害等を狙った標的型攻撃も確認されている。なお、標的の組織の取引先やグループ子会社等を攻撃の踏み台（ウイルスでメールアカウントを乗っ取る等）にすることもあり、業種や会社規模に関係なく狙われるおそれがある。

＜攻撃手口＞

◆　メールを使った手口

添付ファイルやメール本文のリンク先にウイルスを仕込み、開かせることでウイルスに感染させる。実在する組織のメールアドレスを模したメールアドレスを使用して偽装する場合もある。

◆　ウェブを使った手口

標的の組織が利用するウェブサイトを調査し、そのウェブサイトからウイルスをダウンロードするように改ざんする。組織の従業員がそこにアクセスすることでウイルスに感染する。また、DMZ 上に存在するウェブサイト等のサーバーの脆弱性（ミドルウェアの脆弱性等）を悪用して内部に侵入する場合もある。

＜事例または傾向＞

◆　様々な方法で行われる標的型攻撃

サイバー情報共有イニシアティブ（J-CSIP）によると、2017 年 1 月から 12 月までの間に J-CSIP 参加組織宛に届いた標的型攻撃メールの件数は 173 件となっている。本期間の標的型攻撃として、メールにパスワード付き圧縮ファイルを 1 つ添付し、開くと 2 つの

ウイルス付きファイルが格納されている攻撃を観測している。2 つのファイルは実行形式のファイルと Word 文書ファイルであり、後者は Microsoft Office およびワードパッドの脆弱性である CVE-2017-0199 の脆弱性を悪用してウイルスの感染を狙っていた。また、海外の関連企業の従業員のアカウントを乗っ取り、国内企業へ不審メールを送り付けるという攻撃を観測している。これは、攻撃者が防御の弱いところから侵入し、そこから侵入範囲の拡大を試みたおそれがある。[1]

＜対策/対応＞

標的型攻撃に対抗するには、侵入抑止、早期検知、被害拡大防止、最終被害回避等の対策に加え、経営者層、システム管理者、従業員が一体となった対策が重要である。

組織（経営者層）[2]

- 組織としての体制の確立
  - ・迅速かつ継続的に対応できる体制（CSIRT 等）の構築
  - ・対策の予算の確保と継続的な対策の実施
  - ・セキュリティポリシーの策定

組織（セキュリティ担当者）

- 被害の予防／対応力の向上
  - ・情報の管理とルール策定
  - ・サイバー攻撃に関する継続的な情報収集と情報共有
  - ・セキュリティ教育
  - ・インシデント発生時の訓練の実施
  - ・統合運用管理ツール等によりセキュリティ対策状況の把握

    統合運用管理ツールを使い従業員や職員が利用する PC のソフトウェア更新状況を管理し、リスクの可視化を行う。
- 被害を受けた後の対応
  - ・組織内の体制（CSIRT 等）の運用
  - ・影響調査および原因の追究

組織（システム管理者）[3]

- 被害の予防（BCP 対策含む）
  - ・セキュアなシステム設計
  - ・重要サーバーの要塞化（アクセス制御、暗号化等）
  - ・OS・ソフトウェアの更新
  - ・ネットワーク分離
  - ・バックアップの取得

    バックアップから復旧できることを事前に確認しておくことも重要である。
- 被害の早期検知
  - ・ネットワーク監視・防御
  - ・エンドポイントの監視・防御
- 被害を受けた後の対応
  - ・バックアップから復旧

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
  - ・取引先のセキュリティ対策実施状況の確認
- 被害を受けた後の対応
  - ・CSIRT への連絡

＜標的型攻撃メール訓練における留意事項＞

標的型攻撃の訓練を実施する際に、リアリティ追求の観点から実在する組織名を使い訓練を実施した場合、送信元となっている組織や個人にメール送信の有無を確認することがあるため、第三者の業務に影響を与えてしまう懸念がある。場合によっては訴訟問題に発展するおそれもあるため実在または酷似する組織名を使ったメールでの訓練は実施しないことが賢明である。[4]

参考資料

1. サイバー情報共有イニシアティブ（J-CSIP（ジェイシップ））
https://www.ipa.go.jp/security/J-CSIP/
2. 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
3.「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
4. 組織における標的型攻撃メール訓練は実施目的を明確に
https://www.ipa.go.jp/security/anshin/mgdayori20170731.html

2位 ランサムウェアによる被害

～ランサムウェアの感染経路拡大～

ランサムウェアとは、PC やスマートフォンに保存されているファイルの暗号化や画面ロック等を行い、金銭を支払えば復旧させると脅迫する犯罪行為の手口に使われるウイルスである。そのランサムウェアに感染する被害が引き続き発生している。さらに、ランサムウェアに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や外付け HDD に保存されているファイルも暗号化されるおそれがある。組織内のファイルが広範囲で暗号化された場合、事業継続にも大きな支障が生じる。また、2017 年は、OS の脆弱性を悪用し、ランサムウェアに感染した端末が接続しているネットワークを介して感染台数を増やすランサムウェアも登場した。

＜攻撃者＞

- 犯罪グループ・犯罪者

＜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させ、PC やスマートフォンに保存されているファイルの暗号化や PC やスマートフォンの操作ができないように画面ロック等し、復旧を名目に金銭を要求される被害が発生している。また、暗号化や画面ロック以外にも、ファイルを破壊したり、データを外部に流出させたり、OS を起動できないようにし、金銭を要求されるケースも確認されている。

組織のサーバーや PC 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おそれがある。特に経営に関する情報や顧客情報といった機密情報が暗号化された場合の影響度は大きい。また、重要なシステムのファイルが暗号化し、システムが動作しなくなるおそれもある。なお、金銭の要求に応じても、確実に復旧される保証はないが、事業継続や人命保護のために金銭を払ってしまった事例もある。

＜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させる。

◆ ウェブサイトから感染（脆弱性を悪用）

メール本文のリンクをクリックさせる等で攻撃者が用意した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させる。また、不正広告をクリックさせることで感染させる（ウェブサイトを表示させただけで感染するケースもある）。[1]

◆ OS の脆弱性を悪用

OS の脆弱性を悪用することにより、パッチを当てずにインターネットへ接続している端末を感染させる。

＜事例または傾向＞

◆　自己増殖型のランサムウェアの登場

ランサムウェアに感染する経路として、これまではメールの添付やウェブサイトの閲覧経由だったが、2017 年は、OS の脆弱性を悪用して、ネットワークに接続している PC 間で感染を拡大するタイプが登場した。代表的なものとして、「WannaCry」や「NotPetya」等がある。[2] 特に、WannaCry は、世界的に感染が拡大し、国内の大手企業や地方公共団体等でも被害が確認されており、大きくメディアで報道された。

◆　対策されない機器、依然として感染が継続

2017 年 11 月になっても「WannaCry」の感染被害が確認されている。2017 年 3 月にマイクロソフト社よりパッチが公開されていたが、対策を実施していない端末が狙われている。[3]

◆　対策が日々進化する一方、攻撃も進化

不正なファイルの振る舞いを予測して検出する等の機能を持つ機械学習を利用したセキュリティソフトも存在しており、セキュリティ対策は日々進化している。一方、ランサムウェアの中には、この機械学習を利用したセキュリティ対策を回避する手法を採用しているものが確認されており、攻撃も進化し続けている。[4]

＜対策/対応＞

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対応方針を決定しておく必要がある。

組織（経営者層）

- 組織としての体制の確立
  - 迅速かつ継続的に対応できる体制（CSIRT 等）の構築
  - 対策の予算の確保と継続的な対策の実施

組織（システム管理者/PC・スマートフォン利用者）

- 被害の予防（BCP 対策含む）
  - 受信メールや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
  - サポートの切れた OS の利用停止・移行
  - フィルタリングツール（メール、ウェブ）の活用
  - ネットワーク分離
  - 共有サーバー等へのアクセス権の最小化
  - バックアップの取得

    光学メディア（DVD-R、BD-R 等）、外付け HDD、USB メモリー等、外部記憶媒体へ定期的にバックアップを行う。なお、バックアップに使用する記録媒体は、暗号化等されないように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。また、バックアップするデータ量が膨大な場合は、大規模バックアップに対応した外部サービス等を活用する。

    バックアップから復旧できることを事前に確認しておくことも重要である。
- 被害を受けた後の対応
  - CSIRT への連絡
  - バックアップから復旧
  - 復号ツールの活用

    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」にて、複数の復号ツールを提供している。[5] 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、これらの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。
  - 影響調査および原因の追究

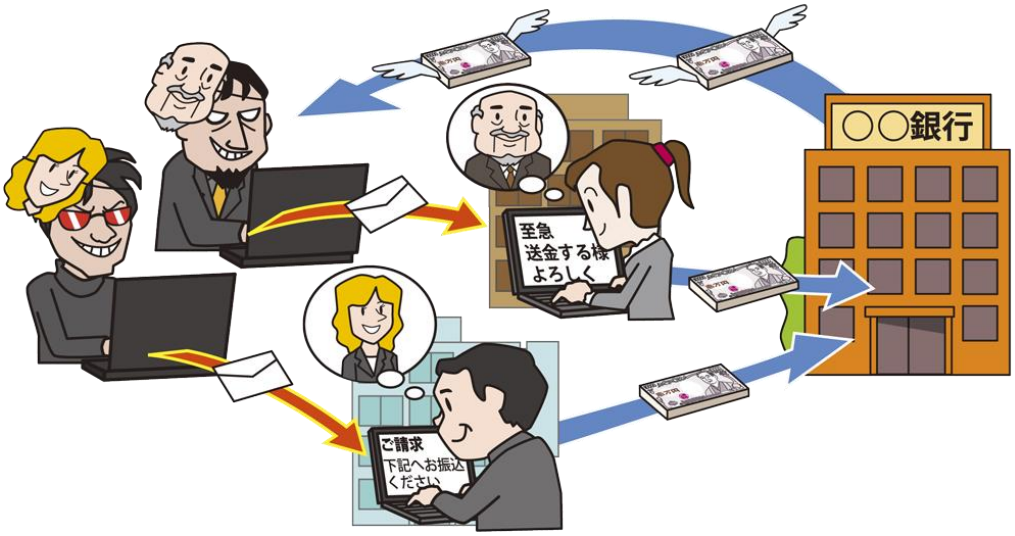
参考資料

1. 「見ただけで感染」する脆弱性攻撃サイトの国内状況
http://blog.trendmicro.co.jp/archives/14420
2. 安心相談窓口だより:WannaCryptorの相談事例から学ぶ一般利用者が注意すべきセキュリティ環境
https://www.ipa.go.jp/security/anshin/mgdayori20170713.html
3. トレンドマイクロ、「2017年国内サイバー犯罪動向」速報を発表
https://www.trendmicro.com/ja_jp/about/press-release/2018/pr-20180110-01.html
4. ランサムウェア「CERBER」、機械学習を利用したセキュリティ対策を回避
http://blog.trendmicro.co.jp/archives/14661
5. The No More Ransom Project
https://www.nomoreransom.org/

個人ランク外

3位 ビジネスメール詐欺による被害

～偽の振込・送金依頼に注意～



「ビジネスメール詐欺」（Business E-mail Compromise：BEC）は巧妙に細工したメールのやりとりにより、企業の担当者を騙し、攻撃者の用意した口座へ送金させる詐欺の手口である。詐欺行為の準備としてウイルス等を悪用し、企業内の従業員の情報が窃取されることもある。以前は主に海外の組織が被害に遭ってきたが、2016 年以降、国内企業でも被害が確認されている。

＜攻撃者＞

- 犯罪グループ

＜被害者＞

- 組織（企業、金銭の決裁権限を持つ責任者、金銭を取り扱う担当者）

＜脅威と影響＞

組織においてメールの利用がビジネスツールとして定着している中、海外の取引先や経営者等を装い企業の財務担当者等を騙して送金させる、ビジネスメール詐欺による被害が確認されている。

ビジネスメール詐欺で使用されるメールは、巧妙な騙しの手口が使われており、通常の取引のメールと見分けづらいように作成されている。また、取引先のメールアドレスを模したメールアドレスや本物のメールアドレスを使っている場合もあり、受信者は攻撃者からの偽のメールを本物のメールとして取り扱ってしまう。その結果、攻撃者に重要な情報を渡したり、攻撃者が用意した口座へ送金してしまう。ビジネスメール詐欺は組織間での取引のため金銭被害が高額になる傾向があり、組織にとって被害に遭った際の影響が大きい。

＜攻撃手口＞

◆ 取引先との請求書の偽装

取引先と請求に係わるやりとりをメール等で行っている際に、攻撃者が取引先になりすまし、攻撃者の用意した口座を記入した偽の請求書等を送りつけ、振り込ませる。なお、攻撃者は取引のやりとりをなんらかの方法により盗み見し、取引や請求に関する情報や、関係している従業員の情報を入手した上で攻撃を行なっている。

◆ 経営者等へのなりすし

企業の経営者等になりすまし、従業員に攻撃者の用意した口座へ振り込ませる。このとき、攻撃者は事前に入手した経営者や関係している従業員等の情報を利用している。

◆ 窃取メールアカウントの悪用

従業員のメールアカウントを窃取し、アカウントを乗っ取った上で、その従業員の取引実績のある別の企業の担当者へ、攻撃者の用意した口座を記入した偽の請求書等を送りつけ、振り込ませる。メール本文は

巧妙に擬装され、送信元が本物のアカウントであるため、受信したメールが攻撃であることに気づきにくい。

◆ **社外の権威ある第三者へのなりすまし**

弁護士や法律事務所といった社外の権威ある第三者へなりすまし、企業の財務担当者等に対して、攻撃者の用意した口座へ振り込ませる。

◆ **詐欺の準備行為と思われる情報の窃取**

詐欺を実行する前の準備行為として、標的組織の情報を窃取する場合がある。例えば、攻撃者が詐欺の標的とする企業の経営者や経営幹部、または人事担当等の特定任務を担う従業員になりすまし、企業内の他の従業員の個人情報等を窃取する。

＜事例または傾向＞

◆ **日本航空にてビジネスメール詐欺被害**

2017 年 12 月、日本航空は、偽の請求書メールにより、航空機リース料等の支払い要求に応じてしまい、約 3 億 8,000 万円の詐欺被害に遭ったと発表した。送信元のメールアドレスは取引先のメールアドレスを模したものが使われていた。取引先とのメールのやりとりはウイルスまたはメールアカウントの乗っ取りにより盗み見られたおそれがある。[1]

◆ **経営幹部を装ったビジネスメール詐欺では、ウェブメールサービスを利用した偽装メールが悪用される**

トレンドマイクロ社によると、2017 年 1 月から 9 月の間に確認された約 27,000 件の経営幹部を装ったビジネスメール詐欺を調査したところ、メールドメインを選択できる無料のウェブメールサービスを利用した偽装メールの手口が増加していることがわかった。この手口は全体の約 65%を占めていた。なお、この手口以外にもメールの返信先（Reply-To）を偽装する手口や模倣ドメインを利用する手口が確認されていた。

また、業務日ではない土日に行われたビジネスメール詐欺は全体の約 9%しかなく、業務日を狙って攻撃を行っていることも判明している。[2]

＜対策/対応＞

組織

ビジネスメール詐欺は、セキュリティ担当者やシステム管理者だけではなく、調達や経理担当者等が連携して対応を行う必要がある。

- 被害の予防 [3]

＜メールの真正性の確認＞

・ メール以外の方法で事実確認

振込先の口座変更等がある場合、電話や FAX 等メール以外の方法で取引先に確認する。

・ 普段とは異なるメールに注意

普段とは異なる言い回しや表現の誤り、送信元のメールドメインに注意する。

・ 電子署名の付与

取引先との間で請求書等の重要情報をメールで取り扱う場合は電子署名を付ける等のなりすまし防止の対策も有効である。

・ 専用のサービスの利用等のメールを使わない取引方法の採用

＜基本的な対策＞

・ OS・ソフトウェアの更新

・ セキュリティソフトの導入

・ メールアカウントの適切な管理

ビジネスメール詐欺では、攻撃や被害に遭う前に、何らかの方法でメールが盗み見られている場合があるため、これら基本的なセキュリティ対策を実施する。

- 被害を受けた後の対応

・ CSIRT への連絡

・ 警察に相談

・ 踏み台や詐称されている組織への連絡

・ 影響調査および原因の追究

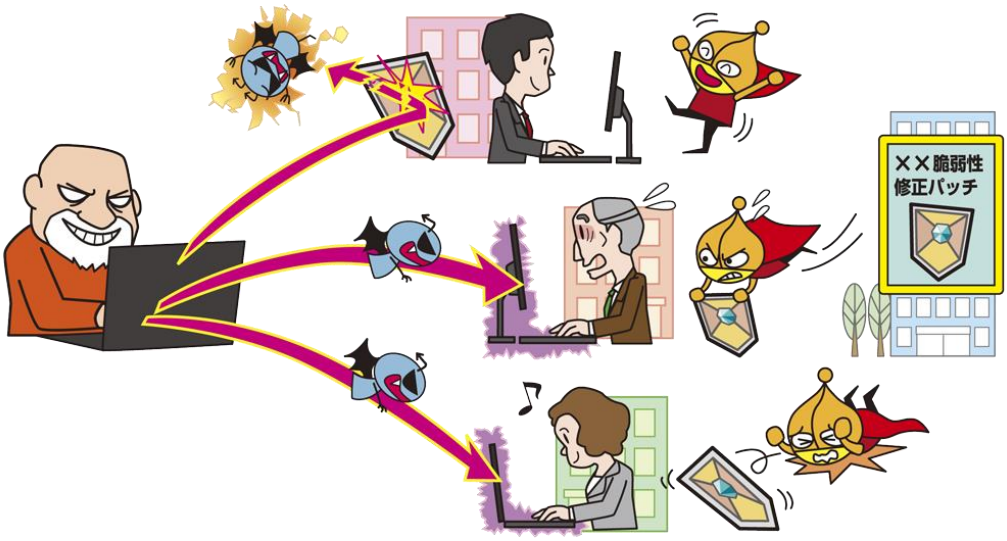
参考資料

1. 日本航空が被害を受けたビジネスメール詐欺をまとめてみた
http://d.hatena.ne.jp/Kango/20171220/1513795615
2. フィッシング攻撃に注意、「ビジネスメール詐欺」の攻撃手口を分析
http://blog.trendmicro.co.jp/archives/17003
3. 独立行政法人情報処理推進機構 【注意喚起】偽口座への送金を促す“ビジネスメール詐欺”の手口
https://www.ipa.go.jp/security/announce/20170403-bec.html

個人ランク外

4位 脆弱性対策情報の公開に伴う悪用増加

～未対策の脆弱性が狙われる！迅速な対応を～



ソフトウェア製品の脆弱性対策情報の公開は、脆弱性の脅威や対策情報を広く呼び掛けられるメリットがある。一方、その情報を攻撃者に悪用され、当該ソフトウェア製品を利用した対策前のシステムを狙う攻撃が行われている。また、近年では脆弱性情報の公開後、その脆弱性を悪用した攻撃が本格化するまでの時間が一層短くなっている傾向がある。なお、脆弱性対策情報の公開前に攻撃が行われる場合もある。

＜攻撃者＞

- 犯罪グループ

＜被害者＞

- 組織（開発ベンダー）
- 組織、個人（ソフトウェア利用者）

＜脅威と影響＞

一般的に、ソフトウェア製品に脆弱性が発見された場合、当該ソフトウェア製品の開発ベンダー等が脆弱性を修正するためのプログラム（パッチ）を作成する。その後、ベンダーはセキュリティ対応機関等と連携するか、または自身で脆弱性対策情報として脆弱性の内容とパッチまたは対策方法を公開し、当該ソフトウェア製品の利用者へ対策を促す。

一方、攻撃者が公開された脆弱性対策情報を元に攻撃コード等を作成し、パッチを適用していない利用者に対して脆弱性を悪用した攻撃を行う被害が確認されている。特に、Apache Struts や WordPress（プラグイン含む）といった広く利用されているソフトウェアの脆弱性対策情報が公開された場合は、攻撃コード等が公開されると被害が拡大するおそれがある。

また、脆弱性が発見されてから、脆弱性対策情報やパッチが公開されるまでの期間に発生するゼロデイ攻撃と呼ばれる攻撃も行われている。

昨今、脆弱性が発見されてからそれを悪用した攻撃が発生するまでの期間が一層短くなっている傾向があるため、より迅速な対応が求められる。

＜攻撃手口＞

◆ 対策適用前の脆弱性を悪用

ソフトウェア製品の利用者がそのパッチを適用する前に脆弱性を悪用し攻撃する。利用者が多いソフトウェアの場合、攻撃が拡大するおそれがある。

◆ 脆弱性対策情報が公開される前の脆弱性を悪用（ゼロデイ攻撃）

開発ベンダー等が認識していない、またはパッチが公開されていない脆弱性を悪用して攻撃する。パッチが存在しないため、利用者での事前の対策は困難となる。

＜事例または傾向＞

◆ **WordPress で構築された複数のサイトが改ざん被害**

2017 年 2 月 3 日頃より、多数のウェブサイトの改ざんされる被害が確認された。この改ざん被害では、同月 1 日に脆弱性情報が公開された、WordPress のコンテンツインジェクションの脆弱性が悪用されていた。WordPress のベンダーは、この脆弱性の影響範囲の広さや悪用の容易性を考慮して、脆弱性情報の公開に先行してパッチをリリースしていた。しかし、パッチを適用していない利用者も多く、多数のウェブサイトが改ざん被害を受けた。[1]

◆ **Apache Struts の脆弱性により情報流出**

2017 年 9 月に、米国の消費者信用情報会社「Equifax」が、攻撃者による不正アクセスを受け、約 1 億 4,000 万人の情報が流出する被害を受けた。攻撃者の侵入を許した原因としては、2017 年 3 月に公開された Apache Struts の脆弱性の対策を行っていなかったことが指摘されている。[2]

◆ **Microsoft Office の脆弱性の攻撃コードの公開に伴う攻撃の増加**

2017 年 11 月 15 日（日本時間）に脆弱性対策情報が公表された Microsoft Office のバッファオーバーフローの脆弱性（CVE-2017-11882）は、当初は技術的に悪用が難しいとされていた。しかし、11 月下旬にはこの脆弱性を悪用する攻撃コードが公開され、この脆弱性を悪用した攻撃が多発した。[3]

＜対策/対応＞

個人、組織（システム管理者／ソフトウェア利用者）

- 被害の予防
  - 資産の把握・体制の整備

    パッチを適用する場合、サービスが正常に動作することを検証する必要があるため、検証するための体制も含めて整備する。
  - 脆弱性関連情報の収集
  - OS・ソフトウェアの更新
  - セキュリティソフトの導入
  - WAF・IPS の導入

    導入後も対策情報（設定等）を定期的に更新する作業があることを想定し、予算や体制を確保しておくこと。
  - ネットワークの監視および攻撃通信の遮断

    ネットワーク越しに脆弱性の攻撃が可能な場合、ネットワークを監視し、攻撃の疑いのある通信をファイアウォール等により遮断することで、攻撃が成功するおそれを低減できる。
  - セキュリティサポートが充実している製品やバージョンを使う

    利用するソフトウェア製品やアプリケーションについては、パッチの提供が早い等のセキュリティサポートが充実しているものを選択する。
  - ベンダーの指示に従い対策（ゼロデイ攻撃確認時）
  - サーバーの停止等回避策

    すぐにパッチが適用できない場合、サーバーの停止等の回避策を実施する。回避策の実施に伴うサービス停止等の影響は関係者間で同意を事前に取っておく。
- 被害を受けた後の対応
  - CSIRT への連絡
  - 影響調査および原因の追究

組織（開発ベンダー）

- 製品セキュリティの管理、対応体制の整備
  - 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
  - 脆弱性関連情報の収集
  - 脆弱性発見時の対応手順の作成
  - 情報を迅速に発信できる仕組みの整備
- 被害を受けた後の対応
  - パッチの迅速な提供（ゼロデイ攻撃時）

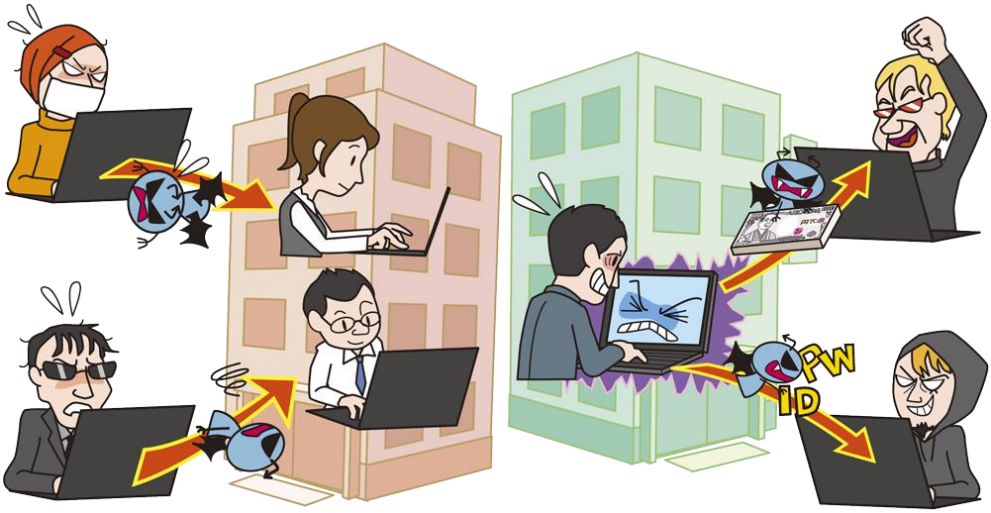
参考資料

1. WordPressのREST API脆弱性、国内サイトでもコンテンツ改ざん事例が発生、IPAとJPCERT/CCが注意喚起
https://internet.watch.impress.co.jp/docs/news/1042776.html
2. Equifaxの情報流出、「Apache Struts」の脆弱性に起因--パッチ適用怠る？
https://japan.cnet.com/article/35107320/
3. Microsoft Office の脆弱性(CVE-2017-11882)について
https://www.ipa.go.jp/security/ciadr/vul/20171129_ms.html

個人ランク外

5位 脅威に対応するためのセキュリティ人材の不足

～組織や国は積極的なセキュリティ人材の育成を～



情報セキュリティにおける脅威は増大の一途を辿っており、毎年のように新たな脅威が出てきている。これらの脅威に対応するためには情報セキュリティの知識や技術を有するセキュリティ人材が求められる。しかし、需要に対するセキュリティ人材の人数が不足しており、また、セキュリティ人材がいたとしても組織は確保するための十分な予算がなく、確保できていないケースもある。セキュリティ人材の不足により、様々な脅威への対応や対策が十分に行えず、被害を拡大してしまうおそれがある。

＜攻撃者＞

- すべての攻撃者（外部、内部）

＜被害者＞

- IT 社会全般（組織、個人）

＜脅威と影響＞

情報セキュリティ上の脅威に対応するに情報セキュリティの知識や技術（リスク評価や対策を検討する企画スキル、対策や修正を実装する技術スキル、監視や組織内教育等の運用管理スキル、事故発生時の調査や対応等の事案対処スキル等様々なスキル）を有するセキュリティ人材が求められている。しかし、組織がセキュリティ人材を確保しようとしても、十分な予算を確保できない等の理由により、必要な人材を確保できないケースがある。また、そもそもセキュリティ人材の絶対数が足りていないという問題もある。組織におけるセキュリティ人材の不足により、セキュリティ上の脅威に対応できる体制を整えられず、被害が深刻化するおそれがある。

＜事例または傾向＞

◆　セキュリティ人材の不足数に関する調査結果

経済産業省の調査によると、情報セキュリティ人材は 2016 年時点で既に約 13.2 万人が不足しており、情報セキュリティ市場の高い伸び率から 2020 年には約 19.3 万人が不足すると推計されている。また、「自社向け」の業務を担当する人材だけでなく、「社外向け」の業務を担当するセキュリティベンダーや IT ベンダーの人材も不足している。[1]

◆　国におけるセキュリティ人材の育成方針

内閣サイバーセキュリティセンター（NISC）は、組織におけるサイバーセキュリティ人材に係わる課題とそのあり方を検討し、「サイバーセキュリティ人材育成プログラム」を作成した。本プログラムでは、社会で活躍できるサイバーセキュリティに関連する人材育成の方向性を示すことにより、安全な経済社会の活動基盤としてのサイバー空間の形成に向けた環境整備を図っている。また、将来を視野に入れて、ビジネスにおけるイノベーションを実現するために必要なサイバーセキュリティ人材の育成や、若年層に必要な教育

のあり方についても示している。[2]

◆　**若年層のセキュリティ人材を発掘・育成**

既に就職している社会人だけでなく、後に就職する若者に対して、高度な情報セキュリティ技術の習得機会を提供する場もある。セキュリティ・キャンプは、セキュリティに対する専門家志向の強い若者に対し、技術面のみならず、倫理面、法制度面等の高い知識、実践能力の向上と、人的ネットワークの確立を図り、日本における将来の高度セキュリティ専門家となり得る優れた人材の発掘と育成を目的として開催している。2004 年度から毎年開催され、これまでに計 600 名以上の人材を輩出している。[3]

＜対策/対応＞

組織

- 組織としての対応体制の確立 [4]
  - セキュリティ人材を確保する戦略の決定

    セキュリティ人材に対する予算や確保していくための中長期的な戦略を決定していく。
  - セキュリティ人材（企画、技術、運用、管理、事案対処スキル等を保持する人材）の採用

    セキュリティに関する業務経験がない中途採用者や IT の基礎知識を有していない新卒採用者を入社後に育成しても良い。

    また、スムーズなセキュリティ対策の実施のために、組織の仕組みやシステムを理解し、ロジカルシンキングによるものの整理と伝え方等も学んでおく必要がある。
  - ジョブローテーション

    セキュリティ担当部門と開発担当部門等で、数年単位で希望者に対して要員交代を実施し、各部門にセキュリティの知識、技術を有する人材の層を拡げていく。交代要員は新しい部門に元の部門で得た情報を共有することで、部門双方にメリットが得られる。
  - 資格取得の推奨
  - 社内資格の整備
  - セキュリティ人材のキャリアパスの確立

    業務で必要となるスキルを定量的に測定することで、自社のセキュリティ人材の充足度を測ることが可能となる。また、従業員は求められるスキルを把握することができ、次に取得すべき資格が分かりやすくなる。
- 情報リテラシーの向上
  - セキュリティ教育

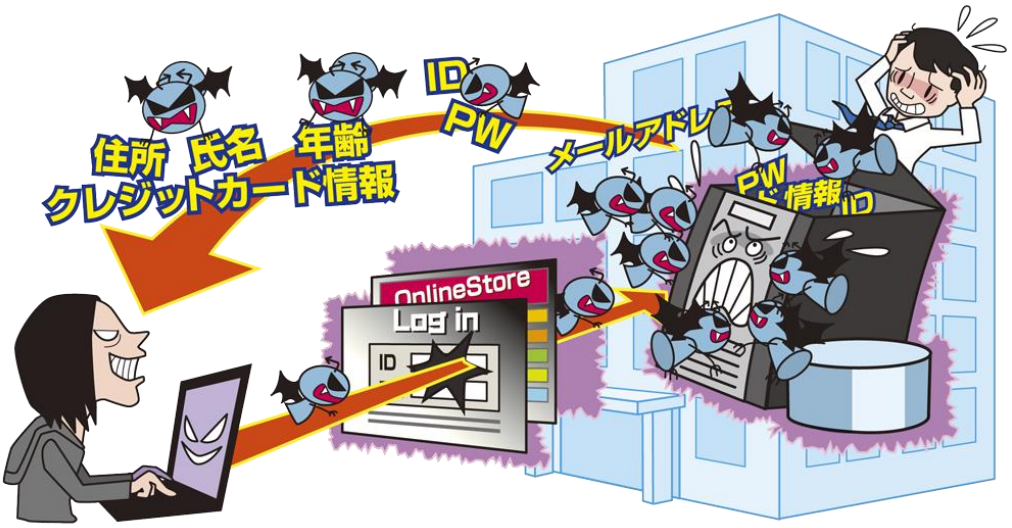
    セキュリティ部門だけでなく、全部門で定期的な研修を実施し、ウイルス感染時の対応手順といった、最低限必要となるセキュリティリテラシーを組織として高めることも重要である。
  - 外部の教育サービスを活用
  - 外部で開催される CTF（ハッキング技術コンテスト）や勉強会等への取り組みの促進

参考資料

1. IT人材の最新動向と将来推計に関する調査報告書
http://www.meti.go.jp/press/2016/06/20160610002/20160610002.html
2. サイバーセキュリティ人材育成プログラム
https://www.nisc.go.jp/active/kihon/pdf/jinzai2017.pdf
3. セキュリティ・キャンプ全国大会2017
https://www.ipa.go.jp/jinzai/camp/2017/zenkoku2017.html
4. 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

6位 ウェブサービスからの個人情報の窃取

～ウェブサービスの脆弱性対策は迅速に～



2017 年も引き続き、ウェブサービスの脆弱性が悪用され、ウェブサービス内に登録されている個人情報やクレジットカード情報等の重要な情報を窃取される被害が発生している。それらの情報を窃取されると、攻撃者により顧客や利用者の個人情報を悪用した不審なメールを送信されたり、クレジットカードを不正利用されるおそれがある。

＜攻撃者＞

- 犯罪グループ・犯罪者

＜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、住所、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おそれがある。

このようなウェブサービスの脆弱性を攻撃され、登録してある重要な情報を窃取されたり、その情報を不正利用される被害が確認されている。ウェブサービスはインターネットで提供されるため、攻撃者の標的にされやすい。

＜攻撃手口＞

◆ **企業で開発した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と脆弱性を作り込むおそれがある。例えば、SQL 文を実行させてデータベースを不正に操作することが可能な 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作り込み、その脆弱性を悪用された場合、個人情報を含む重要な情報を窃取されることがある。

◆ **ソフトウェアの脆弱性の悪用**

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。それらのソフトウェアの脆弱性を悪用して攻撃を行う。特に、ウェブサービスで共通的に広く使われているソフトウェア（OpenSSL、Apache Struts、WordPress 等）の脆弱性の場合、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。

＜事例または傾向＞

◆ **チケット販売大手のウェブサイトにて、Apache Struts2 の脆弱性により情報漏えい**

2017 年 4 月、チケット販売大手ぴあが運営を受託しているウェブサイトにおいて、最大約 15 万 5,000 件の個人情報が漏えいした可能性があると発表した。本件は、Apache Struts2 の脆弱性を悪用されたことが原因であった。[1]

◆ **登山情報サイトにて、SQL インジェクションの脆弱性により情報漏えい**

登山情報サイト「ヤマケイオンライン」において、不正アクセスにより氏名やメールアドレス等、1,160 名分の情報が漏えいした。情報漏えいの原因は、ウェブサイトの構築・運用の委託先企業が開発したプログラムに SQL インジェクションの脆弱性が存在し、それを悪用されたためであった。[2]

＜対策/対応＞

組織（ウェブサービス運営者）

- 被害の予防
  - セキュリティ対策の予算・体制の確保

    システムの導入時や保守作業時の十分な予算と体制を確保する。
  - 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」[3]、「Web システム/Web アプリケーションセキュリティ要件書」[4] や「セキュア・プログラミング講座」[5] が参考になる。また、漏えいのリスクを最小限にするため、必要以上に個人情報等を持たないようにすることも検討する。また、クラウドサービス等を使ってサービスを構築している場合、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。
  - セキュリティ診断（ウェブアプリケーション診断、プラットフォーム診断等）

    システムの導入時やシステム改修時に実施する。また、改修がなくても、1 年に 1 回等定期的に診断を行う。
  - 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、迅速に対応することが重要である。IPA の「重要なセキュリティ情報」[6] 等、各組織から発信される注意喚起情報を日々確認する。
  - WAF・IPS の導入

    なお、導入後も、対策情報（設定等）を定期的に更新する作業があることを想定すること。
- 被害の早期検知
  - 適切なログの取得と継続的な監視
- 被害を受けた後の対応
  - CSIRT への連絡
  - 影響調査および原因の追究
  - 漏えいした情報に対する利用者への補償

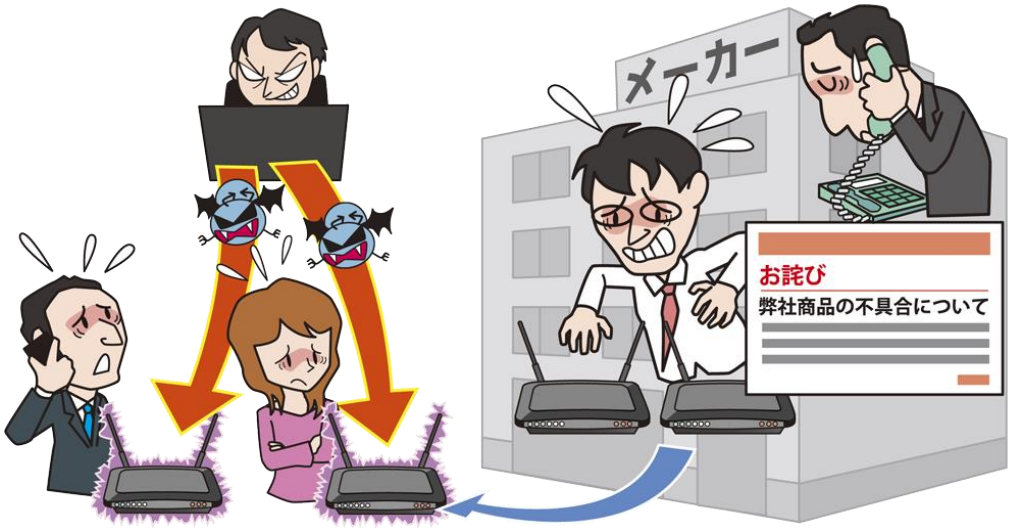
参考資料

1. またもStruts2で漏洩、ぴあ運営のB.LEAGUEサイトから流出したカード番号で被害
http://tech.nikkeibp.co.jp/it/atcl/news/17/042501271/
2. 「山と渓谷」サイトに不正アクセス、1160件の個人情報が流出
http://itpro.nikkeibp.co.jp/atcl/news/17/121902889/
3. 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
4. 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
5. セキュア・プログラミング講座
https://www.ipa.go.jp/files/000059838.pdf
6. 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

7位 IoT 機器の脆弱性の顕在化

～IoT 機器の脆弱性を突く攻撃が頻発、開発ベンダーは脆弱性に対する適切な対処を～



2016 年に引き続き、IoT 機器の脆弱性を悪用しウイルスに感染させることで、インターネット上のサービスやサーバーに対して、大規模な分散型サービス妨害（DDoS）攻撃が行われる等の被害が確認されている。また、国内で発売されている IoT 機器において脆弱性が発見されており、機器を乗っ取られる、または撮影機能等を悪用して個人情報を窃取されるといった危険性があることが公表されている。

＜攻撃者＞

- 犯罪グループ・犯罪者（愉快犯）

＜被害者＞

- 組織（企業、IoT 機器利用者）
- 個人（IoT 機器利用者）

＜脅威と影響＞

IoT 機器が世間に浸透したことによって、様々な情報家電、オフィス機器、医療機器、産業用設備・機器、制御システム等がネットワークを通じて利用できるようになってきた。一方、それらの IoT 機器にも開発者のリスク検討の不十分等により脆弱性を作り込んでしまっている。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分野の機器がインターネット上でつながることにより、攻撃者がネットワーク越しにその脆弱性を悪用することが可能となっている。悪用されると、DDoS 攻撃の踏み台にされたり、搭載されている機能を不正利用される等の被害に遭うおそれがある。

また、IoT 機器の利用者も「IoT 機器はネットワークにつながっている」という意識が薄く、また、感染時の被害についても軽視されており、脆弱性対策等のセキュリティ対策を行っていないケースがあり、被害を拡大してしまっている。

＜攻撃手口＞

◆ 脆弱性を悪用し、ウイルスを感染させる

IoT 機器の脆弱性を悪用してインターネットからウイルスに感染させる。ウイルスに感染することにより、インターネットに公開されているウェブサイト等に DDoS 攻撃を行ったり、IoT 機器に搭載されている機能を不正利用する。

◆ 感染を拡大させる

ウイルスに感染させた後、同じ脆弱性を持つ IoT 機器がないかを探索する。存在した場合、その IoT 機器もウイルスに感染させ、感染を拡大していく。

＜事例または傾向＞

◆ シャープの掃除ロボにセキュリティ上の脆弱性が存在、映像を覗き見される可能性も

シャープ製のロボット掃除機「COCOROBO（ココロボ）」の一部機種に脆弱性があり、第三者から不正に

操作されるおそれがあった。この掃除機はスマートフォンから操作が可能だが、利用する無線 LAN のセキュリティが不十分な設定の場合、掃除機の脆弱性を悪用され、攻撃者に掃除機を乗っ取られる。シャープは本脆弱性に対応する更新プログラムを提供しており、適用を呼びかけている。[1]

◆ IoT 機器を狙うウイルス「Mirai」亜種の発生

2017 年 11 月、ウイルスに感染した IoT 機器等による大規模な DDoS 攻撃が発生した。これは「Mirai」から派生したウイルスによる攻撃であることが判明しており、2017 年の 7 月から 9 月に掛けて、感染させたボットネットから 100Gbps を超える DDoS 攻撃を行ったとされている。また、攻撃のスキャン先ポートとして Mirai 同様 telnet 等に使われる 23/TCP のほか、2323/TCP、37215/TCP、52869/TCP 等が狙われている。特に 52869/TCP を対象とする攻撃の通信は、既知の脆弱性である「CVE-2014-8361」を悪用することが目的とみられる。[2]

◆ 脆弱性を悪用し、ボット化

「IoTroop」または「IoT_reaper」と呼ばれるウイルスが確認され、数百万台規模の IoT 機器が感染している。感染している主な IoT 機器は、インターネットに接続された監視カメラとされている。攻撃は、Mirai のように機器に設定されたデフォルトの ID、パスワード等を使わず、既知の脆弱性を悪用する。国内に設置されている監視カメラでも感染が確認されており、製品に存在する認証回避の脆弱性「CVE-2017-8225」が悪用されたとみられる。[3]

＜対策/対応＞

組織（IoT 機器の開発者）[4,5]

- 被害の予防
  - ・初期パスワード変更の強制化
  - ・脆弱性の解消（セキュア・プログラミング、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
  - ・分かりやすい取扱説明書の作成
  - ・迅速なセキュリティパッチの提供
  - ・利用者にとって不要な機能の無効化
  - ・アクセスできる範囲の制限
  - ・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。
  - ・ソフトウェアサポート期間の明確化

    ソフトウェアサポートの期間を明確化し、利用者に伝えることでサポート切れた状態での利用の注意を促す。

組織（システム管理者・利用者）、個人

- 情報リテラシーの向上
  - ・使用前に説明書を確認
- 被害の予防
  - ・パッチが公開されたら迅速に更新（自動更新機能を有効にする）
  - ・廃棄時は初期化

    IoT 機器には重要な情報が含まれる場合があるため廃棄時は初期化し、廃棄業者等に出す時はデータ消去や秘密保持に関する契約をする。

    その他の被害の予防については、本書の個人 9 位の対策を参考にして欲しい。
- 被害を受けた後の対応
  - ・CSIRT への連絡
  - ・IoT 機器の電源オフ
  - ・IoT 機器の初期化後、「被害の予防」を実施
  - ・影響調査および原因の追究

参考資料

1. シャープの掃除ロボ、情報セキュリティー上の脆弱性確認　カメラ映像のぞき見の可能性も
http://www.sankei.com/west/news/171116/wst1711160112-n1.html
2. IoTマルウェア「Mirai」の亜種が活発化--100Gbps級のDDoS攻撃も
https://japan.zdnet.com/article/35112184/
3. 新たなIoTボットネット出現、「Mirai」級のDDoS攻撃発生の懸念も
https://japan.zdnet.com/article/35109216/
4. 「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
5. 利用時の品質の観点を盛り込んだ「つながる世界の開発指針（第2版）」を発行
https://www.ipa.go.jp/sec/reports/20170630.html

個人ランク外

8位 内部不正による情報漏えい

～内部不正を許さない管理・監視体制を～

組織内部の従業員や元従業員により、私怨や金銭目的等の個人的な利益享受のため組織の情報が不正に持ち出されている。また、組織の情報持ち出しのルールを守らずに不正に情報を持ち出し、さらにその情報を紛失し、情報漏えいにつながることもある。内部不正が発覚した場合、組織は、被害把握や原因追求等の対応に追われ、また社会的信用の失墜等にもつながる。

＜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、悪意を持った組織内部の従業員や元従業員、業務委託先の作業者が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、従業員が自宅や外出先で仕事をするために内部情報を持ち出し、紛失してしまい、情報漏えいにつながることもある。

内部不正による情報漏えいの影響としては、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、株価下落等があり、場合によってはこれらが連鎖的に発生する。

＜攻撃手口＞

◆ アクセス権限の悪用

自身の持つ権限の範囲で、組織の情報を取得する。自身が高い権限を持っている場合や、必要以上に高いアクセス権限または当人に必要のないアクセス権限が付与されている場合、より多くの情報を窃取されるおそれがある。

◆ 退職前のアカウントの悪用

組織を退職した後に、自身が退職前に使っていたアカウントを使って、不正に組織の情報を取得する。組織で退職者のアカウントを削除していない場合に起こる。

◆ USB メモリーや電子メール等により外部持ち出し

組織の内部情報を USB メモリー、CD/DVD、PC 等に保存したり、電子メールで送付することで外部に持ち出す。また、紙媒体に印刷して持ち出すケースもある。

＜事例または傾向＞

◆ **元従業員が顧客情報を持出し、持ち込まれた業者の通報で発覚**

GMO メイクショップの元従業員が、顧客情報や営業関連データ等 3 万 2,800 件を外付けハードディスクへコピーして、自身が業務を請け負っていた会社に持ち込んでいた。

請負先の企業が、GMO メイクショップ側に「業務情報が持ち込まれた可能性がある」と通報したことで発覚した。[1]

◆ **日本年金機構職員が個人情報を不正に持ち出し売買したとして逮捕**

日本年金機構の職員が、年金加入者の個人情報を盗んだとして逮捕された。同職員は盗んだ個人情報を第三者に提供し、見返りに金銭を受け取る等をしていた。この事件は、同機構で定期的に実施している職員の持ち物点検をきっかけに発覚した。[2]

◆ **職員が無断で児童の個人情報を持ち出し**

大阪市の市立小学校の教員が、児童の個人情報が保存されたハードディスクを無断で外部へ持ち出した。さらに、外部での飲食後の帰宅途中に転倒して意識を失い、その間に何者かによって当該ハードディスクを鞄ごと持ち去られた。

個人情報の持ち出しは、同市教育委員会が禁止していたが、ルールが守られていなかった。[3]

＜対策/対応＞

組織

- 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、資産の管理体制の整備を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」[4] のチェックリストを用いることで、対策状況を確認することができる。
  - ・重要情報の管理・保護（アクセス制御、暗号化）

    不正競争防止法の営業秘密漏洩罪に問われないためには、「秘密管理性」が重要視される。
  - ・アカウント、権限の管理・定期監査

    不必要に高い権限を付与したり、アカウントを共有しない。
  - ・情報取り扱い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。
  - ・外部記憶媒体の利用制限

    USB メモリー等の外部記憶媒体の利用に制限をかける。
  - ・許可外の機器の接続の禁止
- 情報モラルの向上
  - ・情報の取り扱い教育の実施
- 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[5]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内部不正抑止に有効である。
- 被害を受けた後の対応
  - ・CSIRT への連絡
  - ・影響調査および原因の追究
  - ・警察への相談

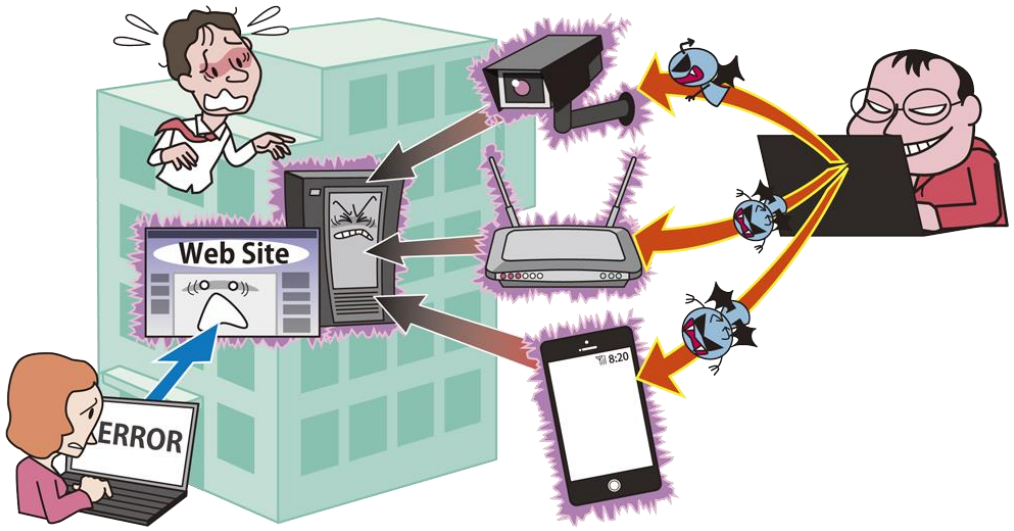
参考資料

1. 元従業員が顧客情報を持出、持ち込まれた業者の通報で発覚 - GMOメイクショップ
http://www.security-next.com/078598/
2. 日本年金機構職員が窃盗容疑で逮捕 - 個人情報を持ち出しで
http://www.security-next.com/083325/
3. 小学校4校の児童個人情報含むHDDを紛失 - 気を失った間に持ち去り
http://www.security-next.com/086000/
4. 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
5. 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
https://www.ipa.go.jp/files/000051140.pdf

個人ランク外

9位 サービス妨害攻撃によるサービスの停止

～ボットウイルスの感染拡大に伴う攻撃の大幅増～



ウイルスに感染し、ボット化した IoT 機器等から DDoS（分散型サービス妨害）攻撃が行われている。それにより、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確認されている。2017 年は公式のマーケットに公開されたスマートフォンアプリがボット化し、DDoS 攻撃が行われた被害が確認されている。

＜攻撃者＞

- 犯罪グループ・犯罪者（愉快犯）
- ハクティビスト

＜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＞

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運営し、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 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。攻撃は、ウイルスに感染しボット化した IoT 機器等から行われているが、攻撃者がその環境を準備して攻撃を行っているのではなく、DDoS 攻撃を代行するサービスを利用していることもある。妨害の目的は主義主張の誇示や社会混乱、金銭要求等がある。

＜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サーバーへ想定外の大量アクセスを行い、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と騙って、脆弱な設定の多数のルーターや 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、負荷をかける攻撃。

- DNS 水責め攻撃

  標的組織のドメインにランダムなサブドメインを付けて問い合わせ、標的組織ドメイン名の権威 DNS サーバーに負荷をかける攻撃。

- DDoS 代行サービスの利用

  DDoS を代行する不法なサービスを利用する攻撃。専門的な技術がなくても攻撃ができる。

＜事例または傾向＞

◆ スマートフォンアプリのボット化

2017 年 8 月にスマートフォンから大規模な DDoS 攻撃が確認された。原因は、公式マーケットの Google Play にて Android 用アプリとして配信されていたアプリにスマートフォンを踏み台として特定のサービスへ DDoS 攻撃を仕掛けるウイルス「WireX」が仕込まれていたためである。そのアプリをインストールしたスマートフォンがボット化していた。そのアプリは、約 300 種存在し、同月末に対象のアプリの一斉削除が行われ、併せて、感染している端末からの対象のアプリを削除する処置を講じている。[1]

◆ IoT 機器のボット化

2016 年に大規模 DDoS 攻撃の原因となった IoT 機器を踏み台にボットネットを構築するウイルス「Mirai」の亜種がたびたび確認されている。2017 年 11 月頃より、その「Mirai」の亜種による感染活動が活発化している。[2] 感染の拡大のメカニズムに、既知の脆弱性（CVE-2014-8361）が悪用されている。

◆ DDoS 攻撃で金銭を要求

DDoS 攻撃を仕掛けた後に、さらなる攻撃を受けたくなければ金銭を支払えとメールで脅迫を行う事例が確認されている。DDoS 攻撃を行った組織に向けて脅迫した事例や広い範囲に向けて DDoS 攻撃を行うと脅迫した事例が確認されている。[3,4]

＜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、ボットとして悪用される。攻撃の踏み台にされないために IoT 機器の脆弱性対策や対応を強化する必要がある。[5]

組織（ウェブサイトの運営者）

- 被害の予防
  - DDoS 攻撃の影響を緩和する ISP や CDN 等のサービスの利用

    既にサービスを利用している場合は、サービスの価値とかける費用を考慮して、最大許容量の見直し等を行う。また、オプション等で 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
  - ネットワークの冗長化

    DDoS 攻撃の影響を受けない非常時用ネットワークを事前に準備する。
  - 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する。連絡手段として、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。
- 被害を受けた後の対応
  - CSIRT への連絡
  - 通信制御（DDoS 攻撃元をブロック等）
  - 利用者への状況の告知
  - 影響調査および原因の追究

参考資料

1. Android端末を踏み台にしたDDoS攻撃発生 Google Playに300本の不正アプリ
http://www.itmedia.co.jp/enterprise/articles/1708/29/news052.html
2. Mirai 亜種の感染活動に関する注意喚起
https://www.jpcert.or.jp/at/2017/at170049.html
3. Armada Collective を名乗る攻撃者からの DDoS 攻撃に関する情報
https://www.jpcert.or.jp/newsflash/2017062901.html
4. Phantom Squad を名乗る攻撃者からの DDoS 攻撃に関する情報
https://www.jpcert.or.jp/newsflash/2017092101.html
5. 「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

10位 犯罪のビジネス化（アンダーグラウンドサービス）

～様々な攻撃ツールがアンダーグラウンドで販売されている～

犯罪に使用するためのサービスやツール、ID やパスワードの情報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おそれがある。

＜攻撃者＞

- 犯罪グループ・犯罪者（愉快犯等）

＜被害者＞

- 組織
- 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引されている。攻撃者は、IT に関する高度な知識がなくても、これらを購入して、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で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やオンライン銀行詐欺ツール、DDoS（分散型サービス妨害）攻撃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、業務を妨害される。

なお、アンダーグラウンドで取引されているサービスやツールはダークウェブまたはディープウェブと呼ばれる、通常のブラウザでは検索できないウェブサイト上に存在する場合がある。攻撃者は、特殊なブラウザ等のツールを利用してそれらのウェブサイトにアクセスしている。

＜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。

◆ 認証情報を購入し攻撃

アンダーグラウンドで購入した ID やパスワード等の認証情報を利用して、ウェブサービス等に不正ログインする。

＜事例または傾向＞

◆ モバイル向けランサムウェアを作成できる Android アプリ

モバイル向けランサムウェアを容易に作成できる Android アプリが、アンダーグラウンドで公開され、さらに、中国の SNS で表示される広告からも入手可能となっている。攻撃者は購入後、脅迫メッセージやアイコン、ロック解除コード等を入力することで、モバイ

ル向けランサムウェアのファイル（APK ファイル）を作成することができる。なお、このランサムウェア作成アプリは、中国語のユーザーを対象にしているが、インターフェース等を変更すれば、簡単に多言語化できると言われている。[1]

◆ **ハッキングトレーニングがアンダーグラウンド上で売買**

アンダーグラウンドで悪意あるハッカーを育成するハッキングトレーニングがサービスとして提供されている。ハッキングトレーニングの利用者を犯罪グループのメンバーに募り、組織化してサイバー犯罪事業を行っている。犯罪グループは、組織化された指揮系統や師弟関係を築きながら事業を拡大している。[2]

◆ **Mac ユーザーを標的としたウイルスがアンダーグラウンドに存在**

Mac ユーザーを標的とした悪意あるプログラムが約 45 万種存在すると報告されている。約 2,300 万種存在するといわれる Windows ユーザーを標的とした悪意あるプログラムと比較して少なく、大きな影響がないように思える。しかし、Mac のマーケットシェアが小さいことが要因とも考えられ、Mac のシェアが大きくなるにつれ、ランサムウェアも増えていくおそれがある。さらに、2017 年 6 月、新たに Mac ユーザーをターゲットにした悪意あるプログラムが 2 つ確認されている。1 つはユーザーのデータを暗号化して金銭を要求するランサムウェアで、もう 1 つはユーザーの情報を収集するスパイウェアであった。研究者らによると、2 つのウイルスはダークウェブ上で、誰でも無料で使える状態になっていたという。[3]

＜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、以下には代表的な対策を記載している。より具体的な対策については、本書に記載されている他の脅威の項も合わせて確認してほしい。

組織（経営者層）

- 組織としての体制の確立
  - 迅速に対応できる体制（CSIRT 等）の構築
  - 予算の確保と継続的な対策の実施

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 や CDN 等のサービスの利用
  - システムの冗長化等の軽減策
- 被害を受けた後の対応
  - CSIRT への連絡
  - 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

影響調査および原因の追究

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
- 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
  - 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

参考資料

1. ランサムウェア作成アプリ出現、コード入力不要--中国語ユーザーが対象
https://japan.zdnet.com/article/35106406/
2. 中国のサイバー犯罪者が利益率の高いハッキング ビジネスを開発
https://blogs.mcafee.jp/chinese-cybercriminals-develop-lucrative-hacking-services
3. Macユーザーを標的にしたマルウェアがダークウェブに出回っている
https://gigazine.net/news/20170615-mac-computer-ransomware/

このページは空白です。

3章. 注目すべき脅威や懸念

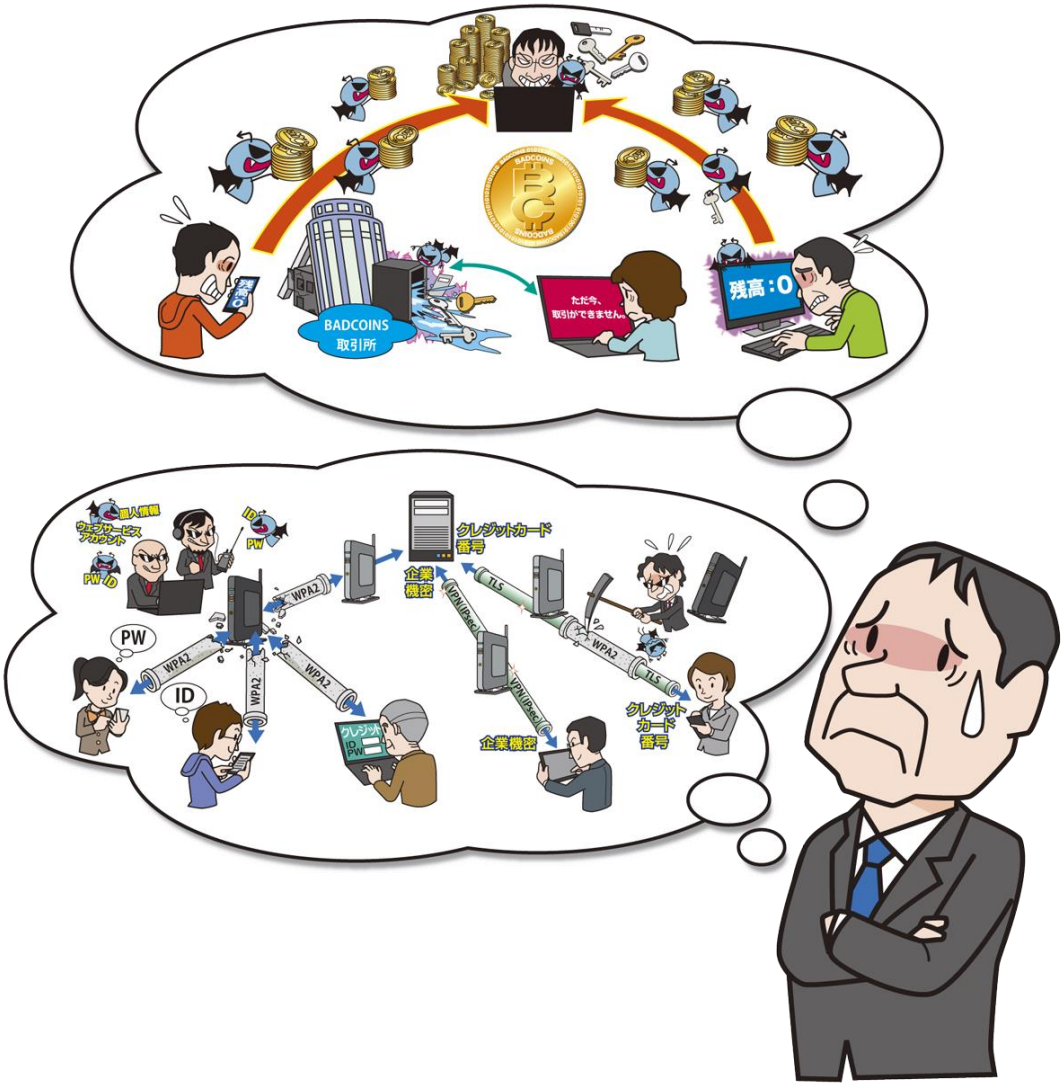
このページは空白です。

3 章 注目すべき脅威や懸念

本章では、10 大脅威には含まれていないが、問題視されている脅威や懸念、今後も継続的な脅威になると考えられる、**表 3.1** に記載している 2 つの脅威や懸念について解説する。

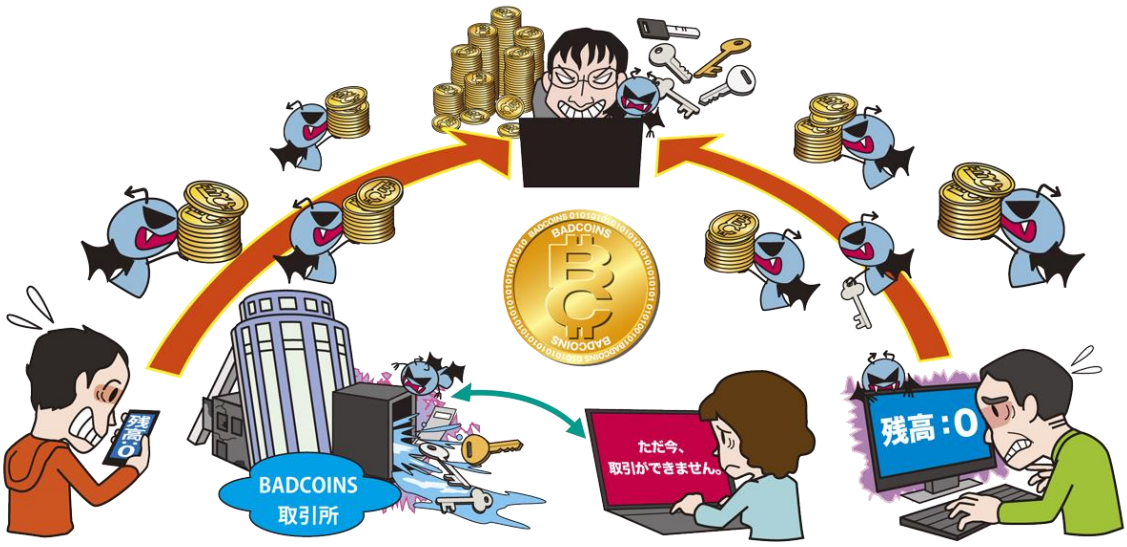
表 3.1：注目すべき脅威や懸念

番号	タイトル
1	仮想通貨の安全性と危険性 ～暗号技術に基づくブロックチェーン技術の応用における脅威～
2	セキュリティプロトコルとその実装に潜む脆弱性 ～必要不可欠な通信における未知の脆弱性への備え～



3.1. 仮想通貨の安全性と危険性

～暗号技術に基づくブロックチェーン技術の応用における脅威～



仮想通貨の一種であるビットコインを利用可能な店舗が急増し、国内家電量販店等でも利用可能となった。仮想通貨に対して肯定的な国と否定的な国とで世界が二分される一方、日本国内では改正資金決済法の施行等の法整備が行われつつある。個人投資家による投資の対象としても注目されてきた中、巨額の不正送金事件や仮想通貨購入に関する詐欺事件が発生した。仮想通貨の安全性や危険性、利用上注意すべきことについて解説する。

＜仮想通貨とは何か＞

2017 年 4 月、改正資金決済法が施行されて、**図 3.1** に示す様に「仮想通貨」が法律上定義された。これにより、金融庁・財務局の登録を受けた事業者（仮想通貨交換業者）以外による国内における仮想通貨の売買や他の仮想通貨との交換等が禁止された。法律上の明確な定義が与えられたことで、国内での注目はさらに高まっている。

> 5 この法律において「仮想通貨」とは、次に掲げるものをいう。
> 一 物品を購入し、若しくは借り受け、又は役務の提供を受ける場合に、これらの代価の弁済のために不特定の者に対して使用することができ、かつ、不特定の者を相手方として購入及び売却を行うことができる財産的価値（電子機器その他の物に電子的方法により記録されているものに限り、本邦通貨及び外国通貨並びに通貨建資産を除く。次号において同じ。）であって、電子情報処理組織を用いて移転することができるもの
> 二 不特定の者を相手方として前号に掲げるものと相互に交換を行うことができる財産的価値であって、電子情報処理組織を用いて移転することができるもの

図 3.1 仮想通貨の定義（法 2 条 5 項）

仮想通貨は、暗号技術を用いて発行の管理や取引の安全性の確保を実現しており、「暗号通貨」とも呼ばれる。仮想通貨には、ビットコインの様な非中央集権型と、リップルの様な中央集権型が存在する。

◆ 非中央集権型

発行者や管理者が存在しない。分散型とも呼ぶ。価値の保証はなく、価格安定性も低いが、仮想通貨の当初の特徴である高い匿名性を有する。

◆ 中央集権型

特定の発行者や管理者が存在する。発行者によっては一定の価値を保証し、価格安定性が高い反面、匿名性はシステムに依存する。

＜ブロックチェーン技術＞

ブロックチェーンは、仮想通貨ビットコインのために考案された分散型台帳管理技術の一種である。暗号技術を用いた改ざん検出機能を備えたデータを、P2P ネットワーク上に分散する複数のノードに保持する分散型データベースで、高可用性やデータ同一性等を実現する。[1] ブロックというデータ構造を、一定時間毎に新たに生成し、時系列で鎖状に接続していくことでデータを保管する。

表 3.2　ブロックチェーン技術の比較

	パブリック型	コンソーシアム型	プライベート型
管理者	存在しない	複数組織	単一組織
参加者	無制限	管理者による許可制	
合意形成	厳格であることが必要 （悪意のある参加者を前提）	厳格でないことが可能 （悪意のある参加者を前提としないことが可能）	
取引速度	低速	高速	

ブロックチェーン技術は、仮想通貨を実現するためのネットワーク、分散型データベースの中核技術として採用されており、その運用形態でパブリック型とコンソーシアム型、プライベート型に分類される（**表 3.2**）。[2]

◆　**パブリック型**

管理者が存在せず、参加は自由である。不特定多数のノードによって、Proof of Work（PoW）やProof of Stake（PoS）等のコンセンサスアルゴリズムに沿った合意形成が行われる。PoW では、ブロック生成とその対価を得るためのマイニングと呼ばれる膨大な計算を行うためのリソースや処理時間を必要とする。

◆　**コンソーシアム型**

複数の管理者が存在し、参加には管理者グループの許可が必要である。合意形成は、管理者が指定する特定のノード（通常は複数）により行われる。

◆　**プライベート型**

単一の管理者が存在し、参加には管理者の許可が必要である。合意形成は、特定のノードにより迅速に行われる。

ビットコイン等の非中央集権型の仮想通貨では、パブリック型ブロックチェーンが用いられており、管理者が不在で、嘘をつく可能性のある参加者や正常に動作していない参加者がいる環境においても、参加者の相互監視による合意形成で、不正な取引や取引事実の改ざんを現実的に不可能とする技術として活用されている。

なお、管理者がブロック（仮想通貨の取引）の承認者を選択する場合を「許可型」、不特定多数の誰もが取引の承認に参加可能な場合を「非許可型」とする分類法も存在する。[3]

ブロックチェーン技術の詳細な説明は本項では割愛するが、基本的には暗号技術によって強固に守られた技術である。仮想通貨ビットコインにおける利用に関しては、プロトコル設計や実装上の問題により脆弱性が指摘されている[4]が、対策も検討されており、採用している暗号技術の危殆化が発生しない限り、概ね安全と考えてよいだろう。

＜仮想通貨の入手方法＞

仮想通貨の入手には、複数の方法が存在する。

◆　**所有者との交換**

仮想通貨の所有者に法定通貨、他の仮想通貨、金銭的価値がある物等を譲渡して、その対価として受け取る。

◆　**取引所における購入**

仮想通貨交換業者（取引所）で購入する。

◆　**マイニング（採掘）**

仮想通貨のブロックチェーンを維持するマイナー（採掘者）として参加し、ブロック生成の成功報酬を仮想通貨建てで受け取る。膨大な計算能力が必要なため、現在は、個人所有の設備では多くの場合費用対効果に見合わず、現実的ではない。

＜仮想通貨の保管方法＞

仮想通貨は、貨幣に相当するデジタルデータとして P2P ネットワーク上で分散管理されており、個々の所有者がデータを保有している訳ではない。仮想通貨の所有権を表す、匿名化されたアドレスとその取引履歴が、巨大なブロックチェーンに記録されている。このブロックチェーンの内容（取引履歴）をたどることによって、仮想通貨の移転状況や二重支払いを監視できるため、個々の匿名化アドレスが保有している仮想通貨の総額を求めることができる。即ち、仮想通貨の所有者は、仮想通貨自体を保管する必要はない。

＜仮想通貨における暗号鍵＞

仮想通貨の所有者は、公開鍵暗号技術の秘密鍵と公開鍵を生成し、さらにその公開鍵からウォレットアドレスを生成する（**図 3.2**）。ウォレットアドレスは、仮想通貨の所有権を表す匿名化されたアドレスであり、送金受け取り時に利用するため、他のユーザーに公開する情報である。銀行口座における

「口座番号」に相当する。秘密鍵は、送金時に利用する秘密情報（暗号鍵）で、送金要求のトランザクションに対する電子署名に用いる。即ち、秘密鍵の所有者のみが対応するウォレットアドレスの保有する仮想通貨を送金可能である。銀行口座における「通帳と印鑑の組合せ」あるいは「キャッシュカードと暗証番号の組合せ」に相当する。

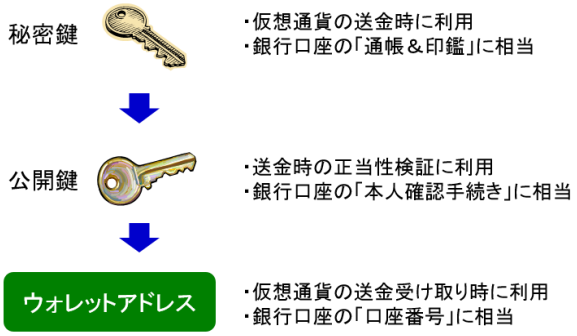


図 3.2　仮想通貨における暗号鍵

＜ウォレットを用いた秘密鍵の管理＞

仮想通貨において、「通帳と印鑑の組合せ」や「キャッシュカードと暗証番号の組合せ」に相当する秘密鍵を盗まれた場合、不正送金によって仮想通貨を失うおそれがある。従って、仮想通貨を利用する上では、**秘密鍵を安全に管理することが重要である。**一般に、仮想通貨では、「ウォレット」と呼ばれる、秘密鍵の保管場所を用いて秘密鍵を管理（保管および利用）する。ウォレットによる秘密鍵の管理には複数の方法がある（**表 3.3**）。

(1) 取引所のウォレットでの管理

契約した仮想通貨交換業者（取引所）のウォレットを利用する方法。ユーザーから見ると、自らの仮想通貨を取引所に預けているイメージであるが、実際には、**自ら秘密鍵を持たずに取引所がその秘密鍵で管理する仮想通貨の一部を自分専用に借用する**形態である。預金通帳を持たず、法人口座を所有する交換所との契約取引によって、所有権を間接的に持つ行為（仮想通貨の直接の所有権は取引所が保有）に相当する。安全性は、取引所が使用するウォレットの種類に依存するが、残高管理や秘密鍵の管理に関して取引所を全面的に信用する必要があり、サイバー攻撃を受けて取引所の秘密鍵が漏えいした場合、利用者の資産も失われるおそれがある。

(2) オンラインウォレットでの管理

◆　ウェブウォレット

Web ベースのウォレットサービスを利用する。暗号鍵を含むウォレットはサービス提供者に管理してもらい、Web ブラウザや専用スマートフォンアプリを介して、Web サービスにアクセスする形態である。**秘密鍵をサービス提供者に預ける**こととなり、デジタル化した通帳と印鑑を預ける行為に相当する。サービス提供者のセキュリティ対策が不十分な場合、サイバー攻撃を受けて利用者が預けた秘密鍵が漏えいした場合、不正送金によって仮想通貨を失うおそれがある。

取引所がウェブウォレットのサービスを提供している場合もある。また、秘密鍵のバックアップ目的でダウンロード可能な場合があるが、ダウンロード後、自分の PC に保存した秘密鍵の漏えいに注意が必要である。

(3) クライアントウォレットでの管理

◆　デスクトップ／モバイルウォレット

ウォレット機能を有する **PC やスマートフォン用のウォレットアプリを用いて秘密鍵を自己管理**し、（通常は仮想通貨交換事業者を介さずに）仮想通貨のブロックチェーンネットワークに直接アクセスする方法。ローカルウォレットとも呼ぶ。PC を用いる場合はデスクトップウォレット、スマートフォンを用いる場合はモバイルウォレットと呼ぶ。通帳と印鑑をデジ

表 3.3　ウォレットの比較

	取引所のウォレット	ホットウォレット			コールドウォレット	
		オンラインウォレット（サイトウォレット）	クライアントウォレット（ローカルウォレット）		ハードウェアウォレット	ペーパーウォレット
		ウェブウォレット	デスクトップウォレット	モバイルウォレット		
秘密鍵の保管場所	仮想通貨交換業者に依存	Web サイト（PC にバックアップ）	PC	モバイル端末	ハードウェアウォレット（専用端末）	紙面
秘密鍵の利用場所		Web サイト				利用不可

タル化して、自分の PC やスマートフォンで保管する行為に相当する。PC やスマートフォンがウイルスに感染すると、秘密鍵が漏えいし、不正送金されるおそれがある。クライアントウォレットで管理していた仮想通貨を失った場合、全て自己責任となる。

(4) コールドウォレットでの管理

ネットワークから切り離されたウォレットを用いて秘密鍵を自己管理する。以下に示す様な方法がある。

◆ **ハードウェアウォレット**

専用機器を用いて秘密鍵を保管し、取引の際に USB ポート経由等で PC に接続して使用する方法。普段は通帳と印鑑を自宅の金庫や貸金庫等の安全な場所で管理し、利用する際に持ち出す行為に相当する。秘密鍵を最も安全に管理する方法であるが、機器の購入費用がかかる。また、取引に使用していない間は、PC から外しておく必要がある。不正改造された物を入手しないため、公式サイトから正規品を購入すべきである。

◆ **ペーパーウォレット**

コード化した秘密鍵を印刷した紙面で保管する方法。通帳と印鑑を現金化して自宅の金庫や貸金庫等の安全な場所で保管する行為に相当する。サイバー攻撃による盗難の心配はないが、仮想通貨のネットワークに接続していないため、そのままでは送金することができず、他のウォレットと併用する必要がある。

＜マルチシグネチャ（マルチシグ）＞

仮想通貨によっては、一つのウォレットアドレスからの送金の際に、複数の秘密鍵による署名を必須とする「マルチシグネチャ」を利用することができる。秘密鍵の漏えいに対するセキュリティを高めたい場合は、マルチシグに対応した交換所やウォレットの利用を考慮すると良い。

＜仮想通貨交換事業者への攻撃＞

2018 年 1 月、ビットコイン取引所 Zaif が不正アクセスを受け、不正出金・不正取引が行われた。[5]

同月、取引所 Coincheck から時価換算で約 580 億円に相当する仮想通貨 NEM が不正送金される事件が発生し、本来は厳重に管理されるべき取引所のウォレットでコールドウォレットやマルチシグ等の安全策が採られないまま管理されていたことが判明した。[6]

＜安全性と危険性＞

仮想通貨の安全な点と危険な点を理解する。

安全性

- ブロックチェーン技術を用いた安全性
  （改ざん検知、高可用性、データ同一性）

危険性

- 非中央集権型の仮想通貨や一部の中央集権型の仮想通貨には、価値の保証が存在しない。
- 仮想通貨交換業者のセキュリティは、各業者が実施している対策に依存している。
- 秘密鍵の漏えいは、仮想通貨の盗難に直結。

＜仮想通貨の利用上、注意すべきこと＞

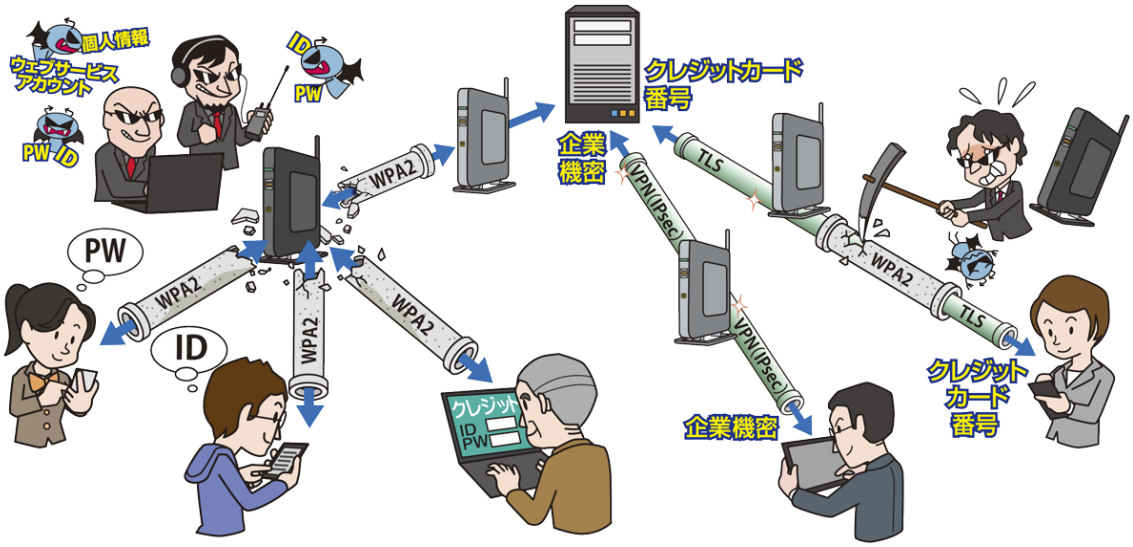
- 投資対象として注目されているが、元本保証がない。預貯金や債券とは異なる存在であることを理解する。
- 仮想通貨交換業者は、十分なセキュリティ対策を実施している業者を選択する。[7]
- ウォレットはセキュリティを考慮した選択・使い分けを行い、可能であればマルチシグの利用を検討する。
- 仮想通貨の購入に関する詐欺行為に注意する。国民生活センターに寄せられるトラブル相談件数が急増している。[7]

参考資料

1. 日本ブロックチェーン協会（Japan Blockchain Association）
http://jba-web.jp/
2. 中央銀行から見たブロックチェーン技術の可能性とリスク
https://www.boj.or.jp/announcements/release_2016/rel161128a.pdf
3. 許可型ブロックチェーンとプライベートブロックチェーン
https://jpbitcoin.com/bitcoin2/permissionedchain
4. ビットコインは本当に安全なのか、理論研究が示す意外な落とし穴 （会員登録要）
http://itpro.nikkeibp.co.jp/atcl/column/16/062400138/112400011/
4. 1月6日から7日未明にかけて発生したAPIキーの不正利用、および1月9日に報告された不正アクセスおよび不正出金に関するご報告
https://corp.zaif.jp/info/8265/
5. Coincheckサービスにおける一部機能の停止について
http://corporate.coincheck.com/2018/01/26/29.html
6. コインチェック事件でブロックチェーン推進協会が会見。「秘密鍵管理」の問題を指摘
https://enterprisezine.jp/article/detail/10343
7. 仮想通貨の勧誘セミナーに潜入して驚愕した （会員登録要）
http://tech.nikkeibp.co.jp/it/atcl/watcher/16/110700001/112100054/

3.2. セキュリティプロトコルとその実装に潜む脆弱性

～必要不可欠な通信における未知の脆弱性への備え～



世界中の多くの人が利用しているセキュリティプロトコルの仕様や実装に脆弱性が発見され、多くのユーザーやサービス提供者が対処を余儀なくされている。2017 年 10 月、無線 LAN の暗号化通信手段として、広く利用されているセキュリティプロトコル WPA2（Wi-Fi Protected Access II）の脆弱性が公開され、世界中で大きな騒ぎとなった。この様に、身近で広く使われているセキュリティプロトコルの仕様や、それらを実装した通信機器やソフトウェアにおいて、脆弱性が発見されることがある。今後同様の脆弱性が発見された場合に備えて、どの様に対処すればよいかを解説する。

＜WPA2 に対する攻撃「KRACKs」＞

2017 年 10 月 16 日（米国時間）、無線 LAN の暗号化通信手段として、広く利用されているセキュリティプロトコル WPA2 の脆弱性が公開され、世界中で大きな騒ぎとなった。[1]

セキュリティプロトコルとは、通信におけるなりすましや通信データの盗聴・改ざんといった脅威の対策として、暗号技術を用いた認証・電子署名・暗号化等を行う、セキュアな通信プロトコルである。WPA2 は、無線 LAN の業界団体 Wi-Fi Alliance が策定したセキュリティプロトコル及びその認証プログラムの一つである。1997 年に策定された WEP（Wired Equivalent Privacy）の暗号化が容易に解読可能と判明した後、2003 年に置き換えが開始された暫定的な対策 WPA（Wi-Fi Protected Access）を、2004 年に正式な仕様としたものである。2017 年の時点において、Wi-Fi 規格に基づく無線 LAN のほぼ全てで利用されている。

発見者により KRACKs（Key Reinstallation AttaCKs）と名付けられたこの攻撃は、WPA2 仕様の脆弱性（プロトコル設計上の曖昧性や誤り）、クライアント及びアクセスポイントの脆弱性（実装上の誤り）を悪用し、暗号技術の不適切な使い方を強制させることで、その効果を無効化し、第三者による暗号化されたパケットの復号や通信パケットの改ざんを可能とする攻撃であった。[2]

＜WPA/WPA2 における複数の脆弱性＞

発見者によると、WPA 及び WPA2 には、4-way Handshake、Group Key Handshake、PeerKey Handshake、Fast BBS Transition Handshake（FT Handshake）等の通信手順において、複数の脆弱性が存在する。

これらの手順におけるプロトコル設計上の曖昧性や誤りといった脆弱性を悪用し、通信メッセージの一部の伝達を遮断したり、遅延したりすることで、以前使用した暗号鍵を再インストール（Re-installation）させて、同じ鍵を再使用させる攻撃が可能である。この結果、WPA/WPA2 で保護された暗号化パケットの復号や改ざんのおそれがあることを明らかにした。

4-way Handshake において、Wi-Fi クライアントとアクセスポイントが通信の暗号化に用いる暗号

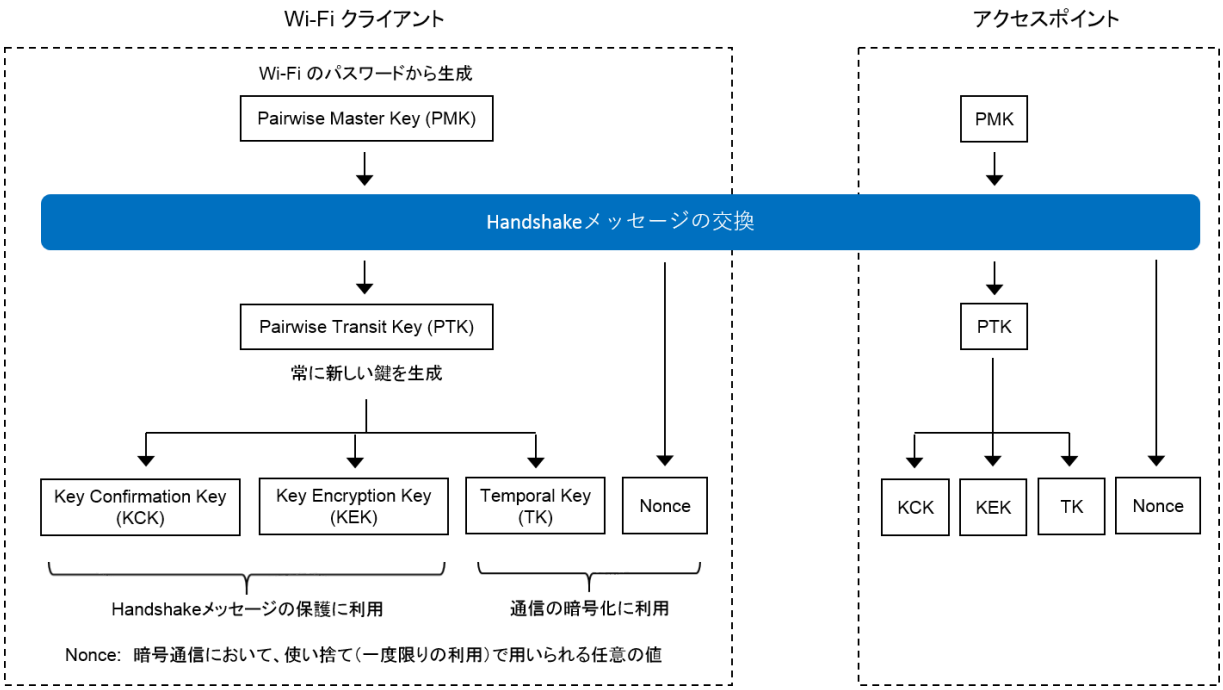


図 3.3 WPA/WPA2 の 4-way Handshake における暗号鍵の共有の仕組み

鍵（セッション鍵）を共有する仕組みを、**図 3.3** に示す。Wi-Fi クライアントとアクセスポイントは、事前に共有している Wi-Fi のパスワードから Pairwise Master Key（PMK）を生成する。そして、Handshake メッセージを交換することで、PMK から毎回異なる Pairwise Transit key（PTK）を生成する。PTK の一部は、Temporal Key（TK）となり、以後の Wi-Fi クライアントとアクセスポイントの間の暗号化に用いられる。また、Handshake メッセージの交換過程で、Wi-Fi クライアントとアクセスポイントは、毎回異なる値の Nonce を共有する。

今回発見された脆弱性の一例は、Handshake メッセージの一部を横取りし、伝達を遮断したり、遅延したりすることで、過去に使用した鍵と同じ鍵を PTK として再利用させ、所定の初期値を Nonce として繰り返し利用させることが可能であった。この結果、通信の暗号化に用いる TK 及び Nonce に同じ鍵、同じ値を使用することとなり、暗号化したパケットの復号や通信パケットの改ざんのおそれを生じた。[3] 発見者の報告をもとに、計 10 件の脆弱性対策情報が登録された（**表 3.4**）。

＜暗号鍵と Nonce の再利用の影響＞

WPA/WPA2 は、複数の暗号化方式（**表 3.5**）を利用可能となっているが、TKIP は安全性の理由によって利用が推奨されていない。CCMP は、WPA/WPA2 と組み合わせて広く利用されている方式である。GCMP は、60GHz 帯のミリ波を使用する近距離用次世代無線通信規格 IEEE 802.11ad で WPA2 を利用する際に追加された方式である。

今回の脆弱性を悪用され、同じ鍵の再利用と同じ Nonce の繰り返し利用を行うこととは、暗号化方式 CCMP では「AES の CCM モードで、同一の暗号鍵で同一の Nonce を使用すること」、暗号化方式 GCMP では「AES の GCM モードで、同一の暗号鍵で同一の初期化ベクタ（IV）を使用すること」に相当する。[4]

この様な使い方をしていると、ある一組の平文と暗号文の組合せが漏えいした場合、そこから暗号鍵を求めることができ（※）、同じ鍵で暗号化している他の通信パケットの復号や改ざんが発生するおそれがある。セキュリティプロトコルで使用する通信パケットは、一定の形式に従っているため、部分的に平文を推定され、結果として暗号鍵の特定からパケットの復号や改ざんへとつながる。

（※） AES の CCM モード及び GCM モードでは、
「暗号文＝平文 XOR 暗号鍵」であるため、
「暗号鍵＝平文 XOR 暗号文」で計算可能。

CCM モードを用いる際の「同一の暗号鍵で同一の Nonce の使用」、GCM モードを用いる際の「同一の暗号鍵で同一の初期化ベクタの使用」は行ってはならないとされているが、一連の脆弱性はこの要件を満たしていなかった。

表 3.4 KRACKs に関連する WPA/WPA2 の脆弱性

脆弱性情報の管理番号		脆弱性の概要
CVE	JVN iPedia	
CVE-2017-13077	JVNDB-2017-008412	WPA/WPA2 において、4-way Handshake 中に Pairwise Transient Key（PTK）を再インストールされ、フレームを再送、復号、または改ざんされる脆弱性
CVE-2017-13078	JVNDB-2017-009171	WPA/WPA2 において、4-way Handshake 中に Group Temporal Key（GTK）を再インストールされ、アクセスポイントからクライアントへのフレームを再送される脆弱性
CVE-2017-13079	JVNDB-2017-009172	IEEE 802.11w をサポートする WPA/WPA2 において、4-way Handshake 中に Integrity Group Temporal Key（IGTK）を再インストールされ、アクセスポイントからクライアントへのフレームを改ざんされる脆弱性
CVE-2017-13080	JVNDB-2017-009173	WPA/WPA2 において、Group Key Handshake 中に Group Temporal Key（GTK）を再インストールされ、アクセスポイントからクライアントへのフレームを再送される脆弱性
CVE-2017-13081	JVNDB-2017-009174	IEEE 802.11w をサポートする WPA/WPA2 において、Group Key Handshake 中に Integrity Group Temporal Key（IGTK）を再インストールされ、アクセスポイントからクライアントへのフレームを改ざんされる脆弱性
CVE-2017-13082	JVNDB-2017-009175	IEEE 802.11r をサポートする WPA/WPA2 において、Fast BSS Transition Handshake（FT Handshake）中に Pairwise Transient Key（PTK）を再インストールされ、フレームを再送、復号、または改ざんされる脆弱性
CVE-2017-13084	JVNDB-2017-009176	WPA/WPA2 において、PeerKey Handshake 中に STSL Transient Key（STK）を再インストールされ、フレームを再送、復号、または改ざんされる脆弱性　STSL: Station to Station Link
CVE-2017-13086	JVNDB-2017-009177	IEEE 802.11z をサポートする WPA/WPA2 において、TDLS Handshake 中に TDLS Peer Key（TPK）を再インストールされ、フレームを再送、復号、または改ざんされる脆弱性　TDLS: Tunneled Direct-Link Setup
CVE-2017-13087	JVNDB-2017-009178	IEEE 802.11v をサポートする WPA/WPA2 において、Wireless Network Management（WNM） Sleep Mode Response フレームの処理中に Group Temporal Key（GTK）を再インストールされ、アクセスポイントからクライアントへのフレームを再送される脆弱性
CVE-2017-13088	JVNDB-2017-009179	IEEE 802.11v をサポートする WPA/WPA2 において、Wireless Network Management（WNM） Sleep Mode Response フレームの処理中に Integrity Group Temporal Key（IGTK）を再インストールされ、アクセスポイントからクライアントへのフレームを再送される脆弱性

表 3.5　WPA/WPA2 の暗号化方式

暗号化方式	暗号アルゴリズム	
	アルゴリズム	モード
TKIP	RC4	ー
CCMP	AES	CCM
GCMP	AES	GCM

＜機種による異なる脆弱性の状況＞

今回の WPA/WPA2 の脆弱性の原因の一部となる仕様は、2004 年に制定された IEEE 802.11i では明確に規定がなく、曖昧性（実装依存性）のあった Handshake 仕様の一部を、2008 年に制定された IEEE 802.11r で追加規定した際に混入した、プロトコル設計上の誤りである。後付けで制定された仕様のため、市場に流通している全ての実装がこの仕様に従っているとは限らず、脆弱性が存在しない場合もあった。また、Handshake メッセージの遮断や遅延が発生した際の挙動の一部は、実装毎に異なるため、脆弱性の影響の度合いに違いがあった。さらに、一部の脆弱性は、全ての製品で実装されていない追加仕様の中に存在した。このため、製品毎に、今回公開された複数の脆弱性の

一つ一つに該当するか否か判断する必要があり、製造業者における確認作業や情報提供に時間を要し、利用者も大いに混乱することとなった。

＜一部の実装にある致命的な脆弱性＞

一連の脆弱性情報と共に、WPA/WPA2 の実装の一部に、極めて危険な実装上の誤りがあることが報告された。一部の製品では、wpa_supplicant というフリーのソフトウェアコンポーネントを用いて WPA/WPA2 を実装しているが、version 2.4 及び 2.5 の wpa_supplicant には、本脆弱性を突いた Handshake メッセージを受信すると、値が 0 の TK を暗号鍵として利用する脆弱性が存在する。これは、かつて暗号鍵を記録していたメモリーをゼロクリアした後、その内容をコピーするという実装上の誤りで、結果として平文＝暗号文となり、全く暗号化が行われない状態となる。例えば、大半の Android 6.0 スマートフォンがこの脆弱性を有しており、攻撃が成功すると全ての通信パケットの復号や改ざんが可能となり、致命的な脆弱性と言える。

＜環境に依存する攻撃成立条件＞

世界中の大半の WPA/WPA2 実装が影響を受けるため、当初は大騒ぎとなった KRACKs であったが、攻撃が成立するためには、クライアントとアクセスポイントの間に割り込み、パケットの送受信を制御する中間者攻撃（MITM: man-in-the-middle attack）が必要である。例えば、不正なアクセスポイントの設置が困難である企業内の無線 LAN 等では、実際に攻撃を行うのは容易ではない。従って、この条件が成り立たない環境では、脅威の度合いが低い。但し、偽のアクセスポイントを設置されるおそれがある、公共の場における無線 LAN 接続サービス等では注意が必要である。

＜TLS/SSL における様々な脆弱性＞

IoT の普及拡大に伴い、ネットワークにつながる様々な製品に実装されるセキュリティプロトコルの脆弱性への対応が重要となっている。世界中の多くの人が利用しているセキュリティプロトコルの仕様や実装に脆弱性が発見された問題としては、2014 年 4 月に発見された Heatbleed（TLS/SSL を実装したオープンソース OpenSSL における実装上の誤り）、2014 年 10 月に発見された POODLE（SSL 3.0 の設計上の脆弱性）、2015 年 3 月に話題となった FREAK（1990 年代の輸出仕様の暗号スイートが未だに SSL で利用可能な状態で運用されていた）等があり、多くのユーザーやサービス提供者が対処を余儀なくされている。

＜今後の備え：脆弱性対策と多層防御＞

WPA/WPA2 の脆弱性は、仕様が公開されてから約 10 年を経て発見された。多くの人が利用している、著名なセキュリティプロトコルであっても、完全に脆弱性をなくすことは不可能に近い。

従って、未知の脆弱性が発見された際の備えとして、事前の対策である多層防御、即ち複数の対策の組合せを実施しておくことが重要である。

例えば、WPA2 はクライアントとアクセスポイントの間の無線区間の暗号化であり、PC／スマートフォンとインターネット上のサーバーの間で通信を行う場合は、TLS や IPsec 等の別の対策で暗号化することも有効である。複数の対策を組み合せて実施しておくことで、一つの対策に脆弱性が見つかり、期待した効果が得られなくなった際の備えとなる。TLS や IPsec で通信路を暗号化するだけで不安があるならば、送るファイルを別の方法で事前に暗号化しておくことが考えられる。

また、事後の対策として、脆弱性の発見後、パッチが公開されたら速やかに適用することも忘れてはならない。

企業においては、脆弱性情報の監視とパッチ適用状況の確認を定期的に行うこと、パッチの適用手順や適用スケジュールを事前に整備しておくことが望ましい。購入時、パッチ提供を含むメーカーサポートが適切に受けられる製品を選定しておくことが望ましいが、利用している製品にパッチが提供されないことが判明した場合は、多層防御を行いつつ、当該機能や当該製品の利用停止、代替機能を有する機器への交換を検討することを推奨する。

参考資料

1. KRACK Attacks: Breaking WPA2
https://www.krackattacks.com/
2. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2
https://papers.mathyvanhoef.com/ccs2017.pdf
3. JVNVU#90609033 Wi-Fi Protected Access II (WPA2) ハンドシェイクにおいて Nonce およびセッション鍵が再利用される問題
https://jvn.jp/vu/JVNVU90609033/index.html
4. IoT開発におけるセキュリティ設計の手引き（2018年4月版） コラム（p.69）
https://www.ipa.go.jp/security/iot/iotguide.html

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)	斯波 彰	(一社)セキュリティ対策推進協議会
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
徳丸 浩	EG セキュアソリューションズ(株)	勝海 直人	(株)ソニー・インタラクティブエンタテインメント
高橋 康敏	(株)インターネットイニシアティブ	相馬 基邦	(株)ソニー・インタラクティブエンタテインメント
藤田 平	ヴイエムウェア(株)	松田 誠一	(株)ソニー・インタラクティブエンタテインメント
佐藤 直之	SCSK(株)	辻 伸弘	ソフトバンク・テクノロジー(株)
保村 啓太	SCSK(株)	楢原 盛史	Tanium 合同会社
松本 隆	SCSK(株)	幸地 佑	地方公共団体情報システム機構
大塚 淳平	NRI セキュアテクノロジーズ(株)	鈴木 一弘	地方公共団体情報システム機構
正木 健介	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
中西 克彦	NEC ネクサソリューションズ(株)	田中 卓朗	TIS(株)
杉井 俊也	NEC フィールディング(株)	三木 基司	TIS(株)
北河 拓士	NTT コミュニケーションズ(株)	山室 太平	TIS(株)
東内 裕二	NTT コミュニケーションズ(株)	森 槙悟	(株)ディー・エヌ・エー
大山 千尋	(株)NTT データ	桑原 和也	デジタルアーツ(株)
宮本 久仁男	(株)NTT データ	岩井 博樹	デロイトトーマツリスクサービス(株)
矢竹 清一郎	(株)NTT データ	内山 巧	(株)電算
池田 和生	NTT データ先端技術(株)	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
七條 麻衣子	大分県立芸術文化短期大学	大浪 大介	東芝インフォメーションシステムズ(株)
前田 典彦	(株)カスペルスキー	森 周	(株)Doctor Web Pacific
淵上 真一	学校法人 KBC 学園	原田 博久	(株)Doctor Web Pacific
岡村 浩成	京セラコミュニケーションシステム(株)	今 佑輔	トレンドマイクロ(株)
小関 直樹	京セラコミュニケーションシステム(株)	萩原 健太	トレンドマイクロ(株)
辻 駿介	京セラコミュニケーションシステム(株)	加藤 雅彦	長崎県立大学
小熊 慶一郎	(株)KBIZ / (ISC)2	須川 賢洋	新潟大学
山下 慶子	KPMG コンサルティング(株)	猪股 秀樹	日本アイ・ビー・エム(株)
吉岡 一真	(株)KPMG FAS	前田 隆行	(株)日本エンタープライズサービス
高倉 弘喜	国立情報学研究所	坂 明	(一財)日本サイバー犯罪対策センター JC3
福森 大喜	(株)サイバーディフェンス研究所	磯田 弘司	日本電気(株)
宮﨑 清隆	(社)JPCERT コーディネーションセンター	谷川 哲司	日本電気(株)
	(JPCERT/CC)	住本 順一	日本電信電話(株)
齊藤 和男	(株)ジェイピー・セキュア	山本 築	日本マイクロソフト(株)
菅原 修	(株)ジェイピー・セキュア	大村 友和	(株)ネクストジェン
矢次 弘志	(株)ジェイピー・セキュア	金 明寛	(株)ネクストジェン
髙岡 隆佳	(株)シマンテック	中野 学	パナソニック(株)
山内 正	(株)シマンテック	渡辺 久晃	パナソニック(株)
大久保 隆夫	情報セキュリティ大学院大学	林 薫	パロアルトネットワークス(株)
阿部 実洋	(株)スプラウト	岩佐 功	東日本電信電話(株)

氏名	所属	氏名	所属
小川 茂樹	東日本電信電話(株)	小屋 晋吾	(株)豆蔵ホールディングス
水越 一郎	東日本電信電話(株)	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)
本川 祐治	(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)
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	石井 崇喜	(株)ユービーセキュア
古賀 洋一郎	ビッグローブ(株)	関根 鉄平	(株)ユービーセキュア
上村 理	ファイア・アイ(株)	長田 啓史	(株)ユービーセキュア
大高 利夫	藤沢市	島田 理枝	(株)ユビテック
原 和宏	富士通(株)	松田 和宏	(株)ユビテック
原田 弘和	富士通(株)	福本 佳成	楽天(株)
福田 有希	富士通(株)	柳川 俊一	(株)ラック
藤本 真吾	(株)富士通研究所 セキュリティ研究センター	山崎 圭吾	(株)ラック
神薗 雅紀	PwC サイバーサービス合同会社	若居 和直	(株)ラック
鈴木 暁	(株)ベリサーブ	清水 亮輔	(株)リクルートテクノロジーズ
太田 良典	弁護士ドットコム(株)	杉山 俊春	(株)リクルートテクノロジーズ
花村 実	マイクロソフトコーポレーション	清水 秀一郎	
増田 博史	マイクロソフトコーポレーション	piyokango	

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　徳竹 敬一
亀山 友彦　渡邉 祥樹　竹村 純輝
田村 智和　菅原 尚志　小林 桂
吉本 賢樹

IPA 執筆協力者　江口 純一　金野 千里　桑名 利幸
加賀谷 伸一郎　松坂 志　吉川 誠司
中島 尚樹　野澤 裕一　黒谷 欣史
板橋 博之　田中 里実　須藤 直樹
堀江 亘　唐亀 侑久　木曽田 優
大塚 龍彦　小助川 重仁

情報セキュリティ 10 大脅威 2018

～引き続き行われるサイバー攻撃、あなたは守りきれますか？～

2018 年 3 月 30 日　初 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/

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