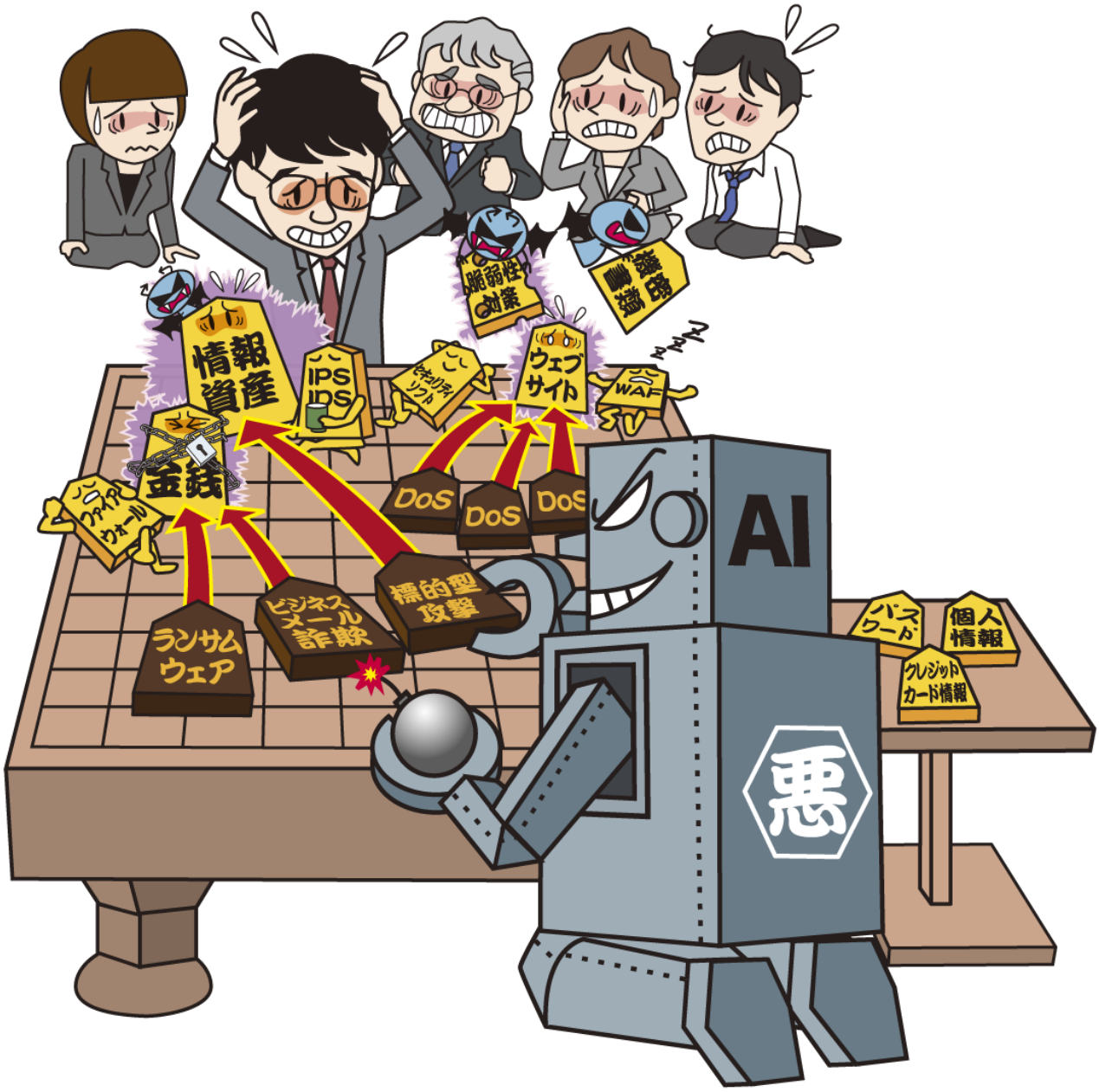
情報セキュリティ

10大脅威 2019

～局面ごとにセキュリティ対策の最善手を～



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

2019年7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 2019」
https://www.ipa.go.jp/security/vuln/10threats2019.html

目次

はじめに

本書「情報セキュリティ 10 大脅威 2019」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、2018 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。「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 10 大脅威 2019 概要

例年、第 2 章の最初に掲載していた「情報セキュリティ 10 大脅威」の順位表を本年は第 1 章に掲載する。その上で、「情報セキュリティ 10 大脅威 2019」の脅威候補の変更点と「情報セキュリティ 10 大脅威 2019」にランクインした脅威の特徴を記載する。

- 情報セキュリティ 10 大脅威 2019（10 大脅威）

個人の 10 大脅威では利用者を騙して金銭や情報を詐取する（必ずしもウイルスを必要としない）手口が多くランクインしている。騙しの手口への対策には具体的に手口を知ることが重要である。また、組織の 10 大脅威ではサプライチェーンに潜む脅威がランクインした。攻撃者はサプライチェーン内のセキュリティ対策が不十分な組織、箇所を攻撃の糸口に侵入し、最終目的である標的への攻撃を試みる。業務を委託する組織は自組織のみならず、子会社や委託先のセキュリティ対策にも目を光らせる必要がある。

第 2 章では、2019 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

近年、情報技術を含む様々な産業分野において、AI（人工知能）技術の活用が注目を集めている。サイバーセキュリティの分野においても、AI 技術を用いた新たなサイバー攻撃対策技術が開発・提供されている。一方で、AI 技術やそれを利用しているシステムに対するサイバー攻撃や、AI 技術を用いた新たなサイバー攻撃手法が出現する等、AI 技術はサイバー攻撃者にとっての攻撃対象や悪用可能な技術となっている。

また、2020 年東京五輪（オリンピック・パラリンピック）の開催まで約 1 年となり、関係団体・組織・企業は、サイバー攻撃対策の強化を進めている。五輪を機に規模が拡大されると予想される既知のサイバー攻撃、新しい手法による攻撃の備え等、東京五輪の開催国の組織や個人として考えるべき点について、おさらいする。

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10 大脅威 2019 概要

1 章 情報セキュリティ 10 大脅威 2019 概要

■「情報セキュリティ 10 大脅威 2019」

2018 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 2019」では、「個人」と「組織」向け脅威として、それぞれ表 1.1 の通り順位付けした。

表 1.1 情報セキュリティ 10 大脅威 2019 「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
クレジットカード情報の不正利用	1	標的型攻撃による被害
フィッシングによる個人情報等の詐取	2	ビジネスメール詐欺による被害
不正アプリによる スマートフォン利用者への被害	3	ランサムウェアによる被害
メール等を使った 脅迫・詐欺の手口による金銭要求	4	サプライチェーンの弱点を悪用した 攻撃の高まり
ネット上の誹謗・中傷・デマ	5	内部不正による情報漏えい
偽警告によるインターネット詐欺	6	サービス妨害攻撃によるサービスの停止
インターネットバンキングの不正利用	7	インターネットサービスからの 個人情報の窃取
インターネットサービスへの不正ログイン	8	IoT 機器の脆弱性の顕在化
ランサムウェアによる被害	9	脆弱性対策情報の公開に伴う悪用増加
IoT 機器の不適切な管理	10	不注意による情報漏えい

IPA から「10 大脅威選考会」に 2019 年版の投票を依頼するにあたり、2018 年版の脅威候補に対して見直しを行った。

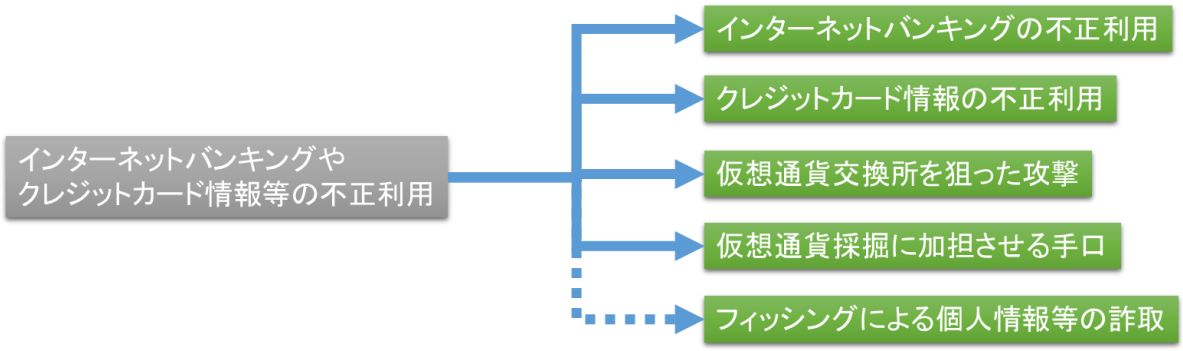
本章では、「情報セキュリティ 10 大脅威 2019」の脅威候補の変更点と「情報セキュリティ 10 大脅威 2019」にランクインした脅威の特徴を記載する。なお、各脅威の詳細については 2 章にて解説する。

■「情報セキュリティ 10 大脅威 2019」の脅威候補の変更点

「情報セキュリティ10大脅威 2019」では「情報セキュリティ10大脅威2018」の脅威候補の見直しを行い、以下の変更を行った。

① 「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」を 5 個の脅威に分割し分類

「情報セキュリティ 10 大脅威 2018」で個人 1 位となった「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」について、昨今のインターネットバンキング被害の減少、クレジットカード被害の増加、仮想通貨関連事件の発生に鑑み、1 つの項目にまとめることが難しい状況となっている。そこで 2019 年版では「インターネットバンキングの不正利用」、「クレジットカード情報の不正利用」、「仮想通貨交換所を狙った攻撃」、「仮想通貨採掘に加担させる手口」、に分割している。また、フィッシング手口の多様化を考慮して、金銭の窃取を目的とせず、個人情報の窃取を目的とする脅威を「フィッシングによる個人情報等の詐取」、に分割している。



なお、「仮想通貨交換所を狙った攻撃」、「仮想通貨採掘に加担させる手口」、は「情報セキュリティ 10 大脅威 2019」においては上位 10 位に入らず、ランク外となっている。

参考:

「仮想通貨交換所を狙った攻撃」

仮想通貨交換所に保有している他人の仮想通貨の窃取を目的とする攻撃全般

「仮想通貨採掘に加担させる手口」

他人の所有する PC リソース等を無断で使用して仮想通貨の採掘を目的とする手口全般

② 「脅威に対応するためのセキュリティ人材の不足」を脅威候補から除外

「脅威に対応するためのセキュリティ人材の不足」は「情報セキュリティ 10 大脅威 2018」では「10 大脅威選考会」のコメントを受け脅威候補とし、結果として組織 5 位となった。しかし、「10 大脅威選考会」内でも、「社会としての脆弱性ではあるが、脅威とは言えないのでは？」というコメントも多く受けており、「10 大脅威選考会」での検討結果を基に「情報セキュリティ 10 大脅威 2019」では脅威候補から除外している。

なお、社会的に影響度が高い問題であることから、「情報セキュリティ 10 大脅威 2019」ではコラムとして解説する。

■「情報セキュリティ 10 大脅威 2019」にランクインした脅威の特徴

「情報セキュリティ 10 大脅威 2019」にランクインした脅威の特徴を記載する。

① 新しく 2 つの脅威がランクイン

「情報セキュリティ 10 大脅威 2019」では、個人 4 位に「メール等を使った脅迫・詐欺の手口による金銭要求」、組織 4 位に「サプライチェーンの弱点を悪用した攻撃の高まり」が新たにランクインしている。

個人を狙った攻撃として、ワンクリック請求に代表されるようなアダルトサイトで利用者を待ち伏せして金銭を要求する手口が広く行われていた。昨今はそれに加えて、メール等を使って不特定多数に脅迫・詐欺メールを送り金銭を要求する手口が増えている。そのため、「情報セキュリティ 10 大脅威 2019」では「メール等を使った脅迫・詐欺の手口による金銭要求」を新しい脅威候補とし、投票の結果、個人 4 位にランクインした。

企業や組織では、サービスやソフトウェアを提供するための調達、開発、運用等の一連の流れ（サプライチェーン）の中で、一部の工程や業務を別企業や子会社等に委託しているケースがある。組織を狙った攻撃では、セキュリティ対策が弱いところを狙うのが常套手段であり、昨今は、サプライチェーン内でセキュリティ対策が弱く、委託元からのガバナンスを効かせにくい委託先の企業が狙われている。そのため、「情報セキュリティ 10 大脅威 2019」では「サプライチェーンの弱点を悪用した攻撃の高まり」を新しい脅威候補とし、投票の結果、組織 4 位にランクインした。

② 個人の脅威は金銭を目的とするものが多くを占める

「情報セキュリティ 10 大脅威 2019」の個人の脅威を主な目的別に分類すると表 1.2 のようになる。個人における脅威は、個人が所有する金銭の窃取や詐取を目的とするものが 10 個中 6 個を占めていることがわかる。個人の立場においては、特に金銭被害につながる脅威に晒されているということを理解し、適切な対応が求められる。

表 1.2「情報セキュリティ 10 大脅威 2019」の個人の脅威を目的別に分類

順位	「個人」向け脅威	金銭	個人情報	不正操作	その他（嫌がらせ等）
1	クレジットカード情報の不正利用	○			
2	フィッシングによる個人情報等の詐取		○		
3	不正アプリによるスマートフォン利用者への被害		○	○	
4	メール等を使った脅迫・詐欺の手口による金銭要求	○			
5	ネット上の誹謗・中傷・デマ				○
6	偽警告によるインターネット詐欺	○			
7	インターネットバンキングの不正利用	○			
8	インターネットサービスへの不正ログイン	○	○	○	○
9	ランサムウェアによる被害	○			
10	IoT 機器の不適切な管理		○	○	

③　組織の脅威は外部からの脅威だけでなく組織内部（関連会社含む）に潜む脅威にも注意

「情報セキュリティ 10 大脅威 2019」の組織の脅威を組織外部からの脅威または組織内部（関連会社含む）に存在する脅威で分類すると表 1.3 のようになる。組織外部からの脅威が多い状況ではあるが、組織内部に起因する脅威も 2 個ランクインしている。組織の立場においては、外部からの脅威だけに目を向けず内部に存在する脅威にもしっかりと注目し、適切な管理と対策が求められる。

表 1.3「情報セキュリティ 10 大脅威 2019」の組織の外部または内部に存在する脅威に分類

順位	「組織」向け脅威	組織外部	組織内部
1	標的型攻撃による被害	○	
2	ビジネスメール詐欺による被害	○	
3	ランサムウェアによる被害	○	
4	サプライチェーンの弱点を悪用した攻撃の高まり	○	
5	内部不正による情報漏えい		○
6	サービス妨害攻撃によるサービスの停止	○	
7	インターネットサービスからの個人情報の窃取	○	
8	IoT 機器の脆弱性の顕在化	○	
9	脆弱性対策情報の公開に伴う悪用増加	○	
10	不注意による情報漏えい		○

■「情報セキュリティ 10 大脅威 2019」をお読みになる上での留意事項

① 順位に捉われず、立場や環境を考慮する

「情報セキュリティ10大脅威 2019」は、「10大脅威選考会」の投票結果に基づき順位付けして「個人」「組織」それぞれ 10 個の脅威を選定している。投票により重要度が高いと考えられるものをより上位の順位としているが、上位の脅威だけ、または上位の脅威から優先して対策を行えばよいということではない。例えば、フィーチャーフォン(ガラケー)を利用している方であれば、個人 3 位「不正アプリによるスマートフォン利用者の被害」の対策の必要性は低くなるし、オンラインショッピング等の個人情報をメインで取り扱っている組織であれば、組織 7 位の「インターネットサービスからの個人情報の窃取」を優先的に対策しなければならないだろう。そのため、**順位が高いか低いかに関わらず、自身または組織が置かれている立場や環境を考慮して優先度を付け、適切な対応を取る必要がある。**

② ランクインした脅威が全てではない

「情報セキュリティ 10 大脅威 2019」で新しくランクインした脅威もあるが、それに伴いランク外となった脅威もある。しかし、ランク外になったとしてもその脅威が無くなったわけではない。かつてランクインしていた、「ワンクリック請求等の不当請求」や「ウェブサイトの改ざん」等は、依然として攻撃が行われている状況である。そのため、**ランク外の脅威だから対策を行わなくて良いということではなく、継続しての対策が必要となる。**ランク外となった脅威の詳細や対策方法等については、過去の「情報セキュリティ 10 大脅威」を参考にしてほしい。

③ 「情報セキュリティ対策の基本」が重要

世の中には「情報セキュリティ 10 大脅威」へランクインした脅威以外にも多数の脅威が存在する。とは言え、これらが利用する「攻撃の糸口」は似通っており、脆弱性を突く、ウイルスを使う、ソーシャルエンジニアリングを使う、等の古くからある基本的な手口が使われている。

詳しくは「情報セキュリティ 10 大脅威 2015」の1章で解説しているが、表 1.4 に示すように「攻撃の糸口」を 5 つに分類し、それぞれに該当する対策を「情報セキュリティ対策の基本」としている。「攻撃の糸口」に変化がない限り、「情報セキュリティ対策の基本」による効果が期待できるので、これを意識して継続的に対策を行うことで、被害に遭う可能性を低減できると考える。

表 1.4 情報セキュリティ対策の基本

攻撃の糸口	情報セキュリティ対策の基本	目的
ソフトウェアの脆弱性	ソフトウェアの更新	脆弱性を解消し攻撃によるリスクを低減する
ウイルス感染	セキュリティソフトの利用	攻撃をブロックする
パスワード窃取	パスワードの管理・認証の強化	パスワード窃取によるリスクを低減する
設定不備	設定の見直し	誤った設定を攻撃に利用されないようにする
誘導(罠にはめる)	脅威・手口を知る	手口から重要視するべき対策を理解する

コラム 1：情報セキュリティの人材不足を考える

2016 年 6 月、経済産業省は「IT 人材の最新動向と将来推計に関する調査結果」[1] を公開した。これによると、今後の市場の伸びを考えると、2020 年には情報セキュリティに対応できる人材が 19.3 万人不足すると試算されている。サイバー攻撃が巧妙化している中、情報セキュリティ人材または、その候補となるような IT 人材を中長期的に育成し、不足をカバーしていくことが求められている。とは言え、人材不足というのは今に始まった話ではない。高度成長期の頃から社会的な問題となっており、その頃は企業を発展させる攻めの人材が不足していた。しかし、今はそれに加えて、サイバー攻撃に備えた守りの人材が不足している。

日本は 2000 年代に入ってから少子高齢化の傾向が続いており、内閣府が 2018 年 6 月に公開した「平成 30 年版高齢社会白書」[2] を見ると、この傾向が加速していることが分かる。つまり、労働者の絶対数が徐々に減少しているのだ。「IT 人材白書 2018」[3] の調査結果によると、情報セキュリティ専門技術者を「確保できていない」または「やや確保できていない」と回答した IT 企業は 5 割近くあった。また、不足している人材の育成・確保については「既存人材を社内で育成」を挙げる企業が、従業員規模によらず 6 割以上であった。これは限られた人的リソースの中で何とかやりくりしなければならない昨今の企業事情の表れではなかろうか。

自組織だけでやりきれないことは、他組織の力を活用していくことも一案である。情報セキュリティを得意とする組織のサービスを活用することで、組織内の人的リソースを別のことに使えるようになる。ここで気をつけるべきことは、情報セキュリティに関する業務を全て外部に任せきってしまわないことである。少なくとも委託先の組織と情報セキュリティに関する会話ができる人材やインシデントが発生した際に自組織の方針や状況を的確に伝えられ、自組織を統率できる人材が必要である。このような人材がいること（できれば部署 [4] があること）で、インシデント発生時に情報を集約でき、委託先と連携したスピーディな対処が期待できる。

セキュリティ人材の育成・確保には、既存人材の活用と並行して、若手の育成が重要である。情報セキュリティを学んだ学生やセキュリティに興味を持っている学生を積極的に採用し、組織内のプログラム（技術的な部分は外部の教育サービスの利用も可）で育成していく。そのためには教育プログラムの策定、資格取得（情報処理安全確保支援士等）の奨励、等で後押しするのがよいだろう。

さらに定期的に情報セキュリティ教育を実施することで、組織全体の情報リテラシーの底上げを図り、情報セキュリティに強い組織作りをしていくことも重要である。その際、「情報セキュリティ 10 大脅威」を始めとする IPA コンテンツを活用いただければ幸甚である。

参考資料

1. IT 人材の最新動向と将来推計に関する調査結果
http://www.meti.go.jp/policy/it_policy/jinzai/27FY/ITjinzai_report_summary.pdf
2. 平成 30 年版高齢社会白書
https://www8.cao.go.jp/kourei/whitepaper/w-2018/zenbun/30pdf_index.html
3. IT 人材白書 2018
https://www.ipa.go.jp/jinzai/jigyou/about.html
4. CSIRT マテリアル
http://www.jpcert.or.jp/csirt_material/

2章. 情報セキュリティ10 大脅威 2019

2 章　情報セキュリティ 10 大脅威　2019

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　2019」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。

本章で共通的に使われる用語について**表 2.1** に定義を記載する。

表 2.1 情報セキュリティ 10 大脅威　2019　用語定義

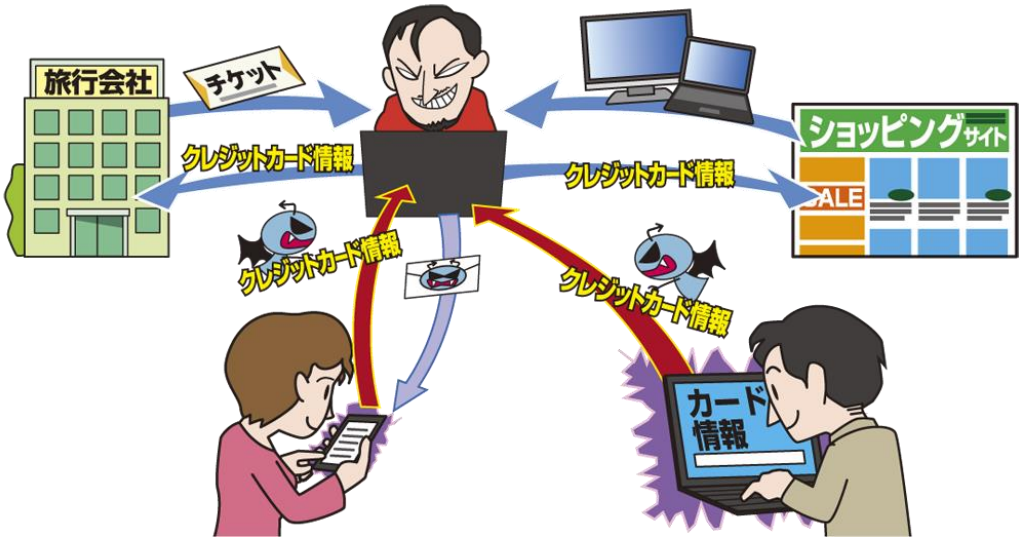
用語	意味
個人	家庭等でスマートフォンや PC を利用する人
組織	企業、政府機関、公共団体等の組織およびその組織に所属している人
犯罪者	金銭や情報窃取（ストーカー行為を含む）を目的とした攻撃（犯罪）者
犯罪グループ	金銭を目的とした攻撃（犯罪）者集団
諜報員、産業スパイ	機密情報窃取を目的とした攻撃（犯罪）集団 国家組織の支援を受けた攻撃（犯罪）集団
ハクティビスト	社会的・政治的な主義主張を目的としたハッキング活動（ハクティビズム）を目的とした攻撃（犯罪）者集団
IoT	モノのインターネット（Internet of Things）。ネットワークカメラや情報家電、医療機器といった様々な機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。
マイニング	PC 等を使って仮想通貨の取引に関連する情報を計算し、取引を承認する行為。計算の報酬として仮想通貨を得られる。
セクストーション	被害者のプライベートな写真や動画を入手したとして、それをばらまく等と脅迫する行為

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）

1位 クレジットカード情報の不正利用

～継続する悪用の被害、被害が拡大するおそれ～



ウイルス感染やフィッシング詐欺等により、クレジットカード情報が攻撃者に窃取され、不正利用が行われている。2018 年も、非常に多くの被害が発生しており、窃取されたクレジットカード情報と旅行サービスを組み合わせた悪用の手口（不正トラベル）による被害の増加も確認されている。

＜攻撃者＞

- 犯罪グループ
- 犯罪者

＜被害者＞

- 個人（クレジットカードの利用者）
- 組織（サービス事業者、クレジットカード会社）

＜脅威と影響＞

近年、キャッシュレス決済が普及してきたことで、電子マネーやモバイル決済等において、様々なサービスが次々と登場している。クレジットカードは、これらの多くのサービスに対して登録が可能となっており、広く活用されている。そういったクレジットカードの情報を攻撃者は狙っている。具体的には、クレジットカード利用者の端末をウイルス感染させたり、フィッシング詐欺等を行うことで、クレジットカード情報を窃取する。

クレジットカード情報が攻撃者に窃取されると、クレジットカード利用者の知らない間に不正に利用され、金銭的な被害を受ける。

＜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、メール受信者に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、クレジットカード情報を入力すると、入力した情報を攻撃者に窃取される。攻撃者は窃取したクレジットカード情報を使用して、正規の利用者になりすまし、不正に決済を行う。

◆ フィッシング詐欺

攻撃者は、実在するショッピングサイト等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、メール受信者を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クレジットカード情報を窃取する。メール内では、実在する企業や組織をかたり、記載されているリンクも正規の URL を模しているものもある。

◆ **漏えいした情報の悪用**

利用しているインターネットサービスから漏えいしたクレジットカード情報が悪用される。

＜窃取したクレジットカード情報の悪用例＞

- 不正トラベル

攻撃者はまず旅行代理店になりすまし、旅行者からの申し込みを募る。旅行者からの申し込みを受け付けると、攻撃者は別途不正に入手しておいたクレジットカード情報を用いて、正規の旅行事業者が提供する旅行サービスに旅行の手配を行う。カードの名義人やクレジットカード会社がクレジットカード情報の漏えいに気づいていなければ、通常通りに決済が完了する。その後、攻撃者が旅行に関する情報を旅行者に伝達することで、旅行者は通常通りの旅行が可能となり、攻撃者は旅行者から旅行サービスの支払金を詐取する。後日、不正利用されたクレジットカードに心当たりのない旅行サービスの請求があることで、クレジットカードが不正に利用されたことが発覚する。

＜事例または傾向＞

◆ **不正トラベルの手口が多発**

窃取されたクレジットカード情報が旅行サービスの不正購入に利用される不正トラベル被害の多発について、一般財団法人日本サイバー犯罪対策センター（JC3）から注意喚起が行われた。[1]

◆ **モバイル決済におけるクレジットカードの不正利用**

2018 年 12 月、QR コードを使用したモバイル決済サービス「PayPay」において、クレジットカードの不正利用が発生した。当該サービスでは、サービス提供元が提供するアプリにクレジットカードを登録して決済できる機能があり、本機能の本人認証に不備があったことで、窃取されたクレジットカードを悪用された可能性が高いとされている。悪用されたクレジットカード情報がどのような経緯で窃取されたのかについては明らかになっていない。[2,3]

◆ **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、2018 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 131.8 億円となり、一昨年から約 2 倍に増加した前年同期間の 130.3 億円よりもさらに増加している。また、不正利用被害の内、番号盗用被害が約 8 割を占めており、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
  - ・表 1.4「情報セキュリティ対策の基本」を実施
  - ・クレジットカード会社が提供している本人認証サービス（3D セキュア）の利用
  - ・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開かない
  - ・信頼できるインターネットサービスの利用
  - ・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
- 被害の早期検知
  - ・クレジットカードの利用履歴の確認
  - ・利用時のメール通知機能等の利用
- 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

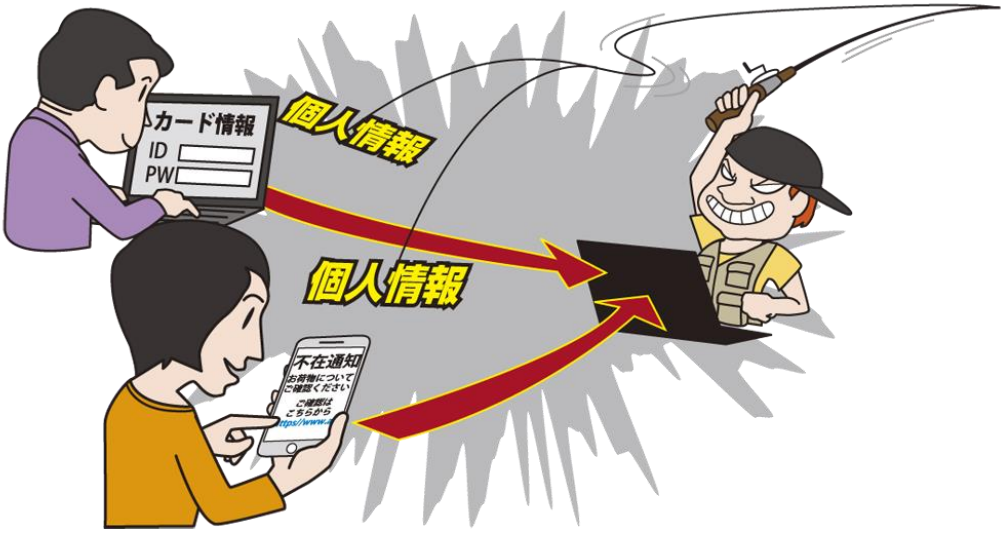
    クレジットカード会社によっては、全額または一部補償してくれる場合がある。
  - ・クレジットカードの再発行
  - ・端末の初期化
  - ・パスワードの再設定

参考資料

1. 不正トラベル対策の実施
https://www.jc3.or.jp/topics/travel_fraud.html
2. 3Dセキュア（本人認証サービス）の対応と、クレジットカード不正利用への補償について
https://paypay.ne.jp/notice-static/20181227/01/
3. ペイペイ不正利用「ダークウェブ」でカード情報入手か
https://www.nikkei.com/article/DGXMZO39071890Y8A211C1CC1000/
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_g_181228.pdf

2位 フィッシングによる個人情報等の詐取

～有名企業を装い偽サイトへ誘導、横行するフィッシングメールに注意！～



有名企業をかたったメールを送信して偽のウェブサイトへ誘導し、ID やパスワード等を詐取するフィッシング詐欺が行われている。Apple ID、Microsoft アカウント等、複数のサービスを利用できる認証情報が狙われる傾向にあり、詐取された情報を悪用され金銭的な被害が発生している。

＜攻撃者＞

- 犯罪グループ
- 犯罪者

＜被害者＞

- 個人（インターネット利用者）
- 組織（クラウドサービス利用者）

＜脅威と影響＞

PC やスマートフォンの利用者に、金融機関や有名企業を装った電子メールが届く。メールの本文には、攻撃者が用意した偽のウェブサイト（フィッシングサイト）へのリンクが記載されており、巧みな言葉で誘導し、リンクをクリックさせる。リンク先は正規のウェブサイトを装ったフィッシングサイトになっており、そこで入力した ID やパスワード等の個人情報を窃取される。それにより、窃取された情報を悪用され、金銭的な被害が発生する。

2018 年は、特定の組織で利用するクラウドメールサービスの認証情報を狙ったフィッシング詐欺による被害も確認されている。また、フィッシングサイトへ誘導された利用者も過去最大規模となっている。

＜攻撃手口＞

◆ **有名企業を装ったフィッシングメールを不特定多数に送信**

攻撃者は、実在する企業のウェブサイトを模したフィッシングサイトを作成する。その後、実在する企業を装い、フィッシングサイトのリンクが記載されたメールや SMS 等を送信し、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 ID やパスワード情報等を窃取する。

◆ **システム管理者等を装ったフィッシングメールを組織内の不特定多数に送信**

システム管理者等を装い、組織で利用するクラウドサービス等のログイン画面を模したフィッシングサイトへ誘導し、そこで入力したクラウドサービスの ID やパスワード情報を窃取する。

＜窃取した情報の悪用例＞

- 窃取した ID やパスワード情報等をリスト化し、ダークウェブ等で販売して金銭を得る。
- リスト化した ID、パスワード情報を悪用して複数のインターネットサービスに不正ログインを試みる。（パスワードリスト攻撃）

＜事例または傾向＞

◆ **過去最大規模に拡大したフィッシング詐欺**

2018 年は世界的にフィッシング詐欺による攻撃が過去最大規模で発生した。日本国内においてもフィッシングサイトへ誘導された利用者数は、10 月までの 10 か月間の統計であるにも関わらず、過去最大の 392 万件に達している。[1]

◆ **Amazon をかたったフィッシングサイト**

Amazon を装った不審なメールが出回っているとして、フィッシング対策協議会が注意を呼び掛けている。[2] メール内には「Amazon アカウントの有効期限が切れました」、「今すぐ更新」といった記載があり、「今すぐ更新」ボタンには正規の URL に似せた偽サイトのリンクが埋め込まれている。実際にクリックすると公式サイトに酷似したフィッシングサイトに遷移し、メールアドレス、パスワード、氏名、住所、郵便番号、クレジットカード情報等の個人情報の入力を求められる手口が確認されている。

◆ **大学を標的としたフィッシングが多発**

大学を標的としたフィッシングメールの被害が複数の大学で確認された。[3] メールの管理者を装ったフィッシングメールが大学内の不特定多数に送信され、その結果、大学で利用しているクラウドメールサービスの認証情報が詐取された。詐取した認証情報を用いてメールアカウントに不正ログインされることで複数のメールアカウントからメール情報が漏えいした。

＜対策/対応＞

個人（インターネット利用者）

- 被害の予防
  - ・表 1.4「情報セキュリティ対策の基本」を実施
  - ・受信メールやウェブサイトの十分な確認
    重要なお知らせや、身に覚えのない内容である場合は公式サイト等を確認する。
  - ・メール内のリンクを安易にクリックしない
    よく利用するウェブサイトはブラウザのお気に入り等からアクセスする。
- 被害の早期検知
  - ・利用するサービスのログイン履歴の確認
    不審な IP アドレスや端末からログインした形跡がないかを確認する。
  - ・口座、クレジットカード、キャリア決済の利用履歴の確認
- 被害を受けた後の対応
  - ・パスワードの再設定
  - ・クレジットカードの停止
  - ・信頼できる機関に相談する
    国民生活センターや地域の消費生活センター等に相談する。

組織（インターネット利用者）

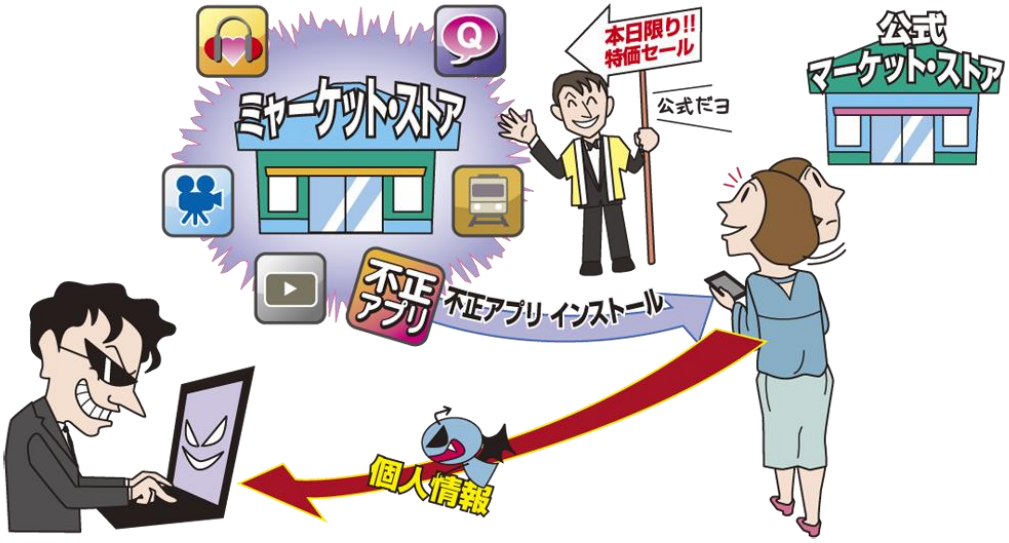
- 被害の予防
  - ・表 1.4「情報セキュリティ対策の基本」を実施
  - ・セキュリティ教育
- 被害を受けた後の対応
  - ・CSIRT やシステム管理者へ連絡

参考資料

1. 2018年「個人」を狙う三大脅威:「フィッシング詐欺」
https://blog.trendmicro.co.jp/archives/20138
2. Amazon をかたるフィッシング（2018/12/18）
https://www.antiphishing.jp/news/alert/_amazon_20181218.html
3. 横浜市立大学がフィッシングメール被害！個人情報5,794件が流出の可能性
https://cybersecurity-jp.com/news/25048

3位 不正アプリによるスマートフォン利用者への被害

～実在の企業をかたり不正アプリのインストールへ誘導、不正アプリによる被害に注意～



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、一部機能を不正に利用される被害が確認されている。不正アプリをインストールさせるための手口として、実在の企業をかたり誘導する等、手口が巧妙化している。

＜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＞

公式マーケットや攻撃者が用意したサイトに連絡先情報の窃取等を目的に不正アプリが公開されている。攻撃者は不正アプリを正規のアプリと誤認させ、インストールするように誘導してくる。

不正アプリをスマートフォンにインストールしてしまうことで、スマートフォン内の連絡先、通話記録、位置情報等の重要な情報を窃取されたり、録画、写真撮影、通話録音機能等を不正に利用される被害に遭うおそれがある。また、不正アプリをインストールしたスマートフォンを踏み台にして、第三者のスマートフォンや企業のサーバーへの攻撃に悪用されることで、利用者が意図せず加害者になってしまうおそれがある。

また、スマートフォン利用者が気づかないうちに仮想通貨のマイニングを実行する不正アプリも確認されている。このような不正アプリをインストールすることで、スマートフォンの発熱や意図しない不具合につながるおそれもある。

＜攻撃手口＞

◆ **不正アプリのダウンロードサイトへ誘導**

実在の企業をかたり、不正アプリのダウンロードサイトへ誘導する等、不正アプリを正規のアプリであると誤認させてインストールさせる。

◆ **公式マーケットに不正アプリを紛れ込ませる**

不正アプリを正規の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み、安易にインストールしてしまう。

＜不正アプリによるスマートフォンの悪用例＞

- 連絡先等の端末内の重要な情報を窃取
- 仮想通貨のマイニングに不正に利用
- 録画・カメラ・通話録音機能を不正に利用
- DDoS 攻撃や悪意のある SMS の拡散等の踏み台

＜事例または傾向＞

◆ **宅配便業者をかたった SMS による不正アプリインストールへの誘導**

宅配便業者をかたり荷物配達に関する偽の不在通知をスマートフォン利用者に対して SMS で送信し、宅配便業者の正規の Web サイトに偽装した Android スマートフォン用の不正アプリのダウンロードサイトに誘導されるという事例が確認された。[1]

この不正アプリをインストールすると、端末内の連絡先情報等が窃取されるおそれがある。また、当該不正アプリをインストールしたスマートフォンから、不特定多数のスマートフォンに対して宅配便業者をかたった SMS を送信するための踏み台に利用されたという被害も確認されている。

◆ **ルーターの DNS 設定を改ざんし不正アプリのインストールへ誘導**

ルーターの DNS 設定が改ざんされ、いつもアクセスしている正規の Web サイトへ接続しても、不正アプリのダウンロードサイトへ強制的に接続されるという事例が確認された。[2] 当該 Web サイトでは「facebook.apk」という名称の不正アプリがダウンロードされる。実在する有名なアプリの名をかたることによって正規のアプリであると誤認させ、不正アプリをインストールさせようとしたと考えられる手口である。

◆ **仮想通貨をマイニングする不正アプリ**

スマートフォン利用者が意図せずスマートフォンの処理能力を仮想通貨のマイニングに使用する Android スマートフォン用の不正アプリが確認された。[3] マイニングの機能以外にも、当該アプリのアイコンをホーム画面から隠ぺいしたり、画面をロックして当該アプリのアンインストールを妨害する機能も持っている。

＜対策/対応＞

個人（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）

  ・表 1.4「情報セキュリティ対策の基本」を実施

  ・アプリは公式マーケットから入手

  アプリは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。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を様々な情報から総合的に判断する。

  ・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、アプリの動作に関係がないと思われる権限が要求されている場合は、当該アプリを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権限を要求している場合は注意が必要である。

  ・アプリインストールに関する設定に注意

  Android スマートフォンの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。

- 被害を受けた後の対応

  ・不正アプリのアンインストール

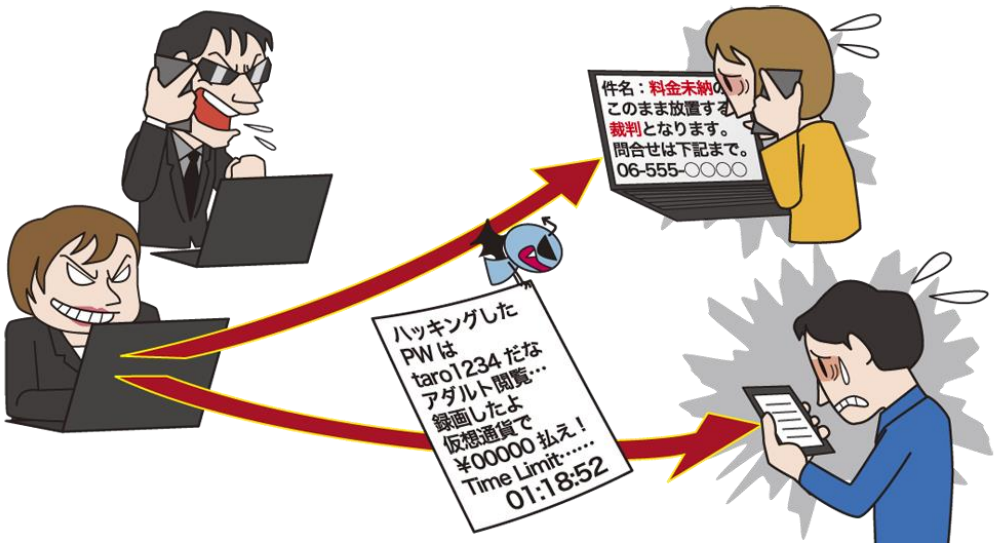
  不正アプリをアンインストールする。アンインストールできない場合は端末を初期化する。

参考資料

1. 「佐川急便」をかたる偽SMSが横行　不正アプリを導入しないで！
https://www.yomiuri.co.jp/science/goshinjyutsu/20180730-OYT8T50119.html
2. ルーターのDNS改竄によりダウンロードされる「facebook.apk」の内部構造を読み解く
https://blog.kaspersky.co.jp/malicious-facebook-apk/19968/
3. 仮想通貨「Monero」を採掘する不正アプリに注意　スマホのリソースを消費し尽くす
https://www.itmedia.co.jp/news/articles/1804/05/news104.html

4位 メール等を使った脅迫・詐欺の手口による金銭要求

～仮想通貨などを要求する詐欺メールには冷静な対処を～



アダルトサイトを閲覧している姿を撮影した映像をばらまくと脅迫するメールや有料サイトの未納料金を請求するメールを受信し、その内容を信じてしまい仮想通貨等を騙し取られる被害が発生している。昨今、PC をハッキングしているように見せかける等、信じさせる手口が巧妙化している。

＜攻撃者＞

- 犯罪グループ

＜被害者＞

- 個人（インターネット利用者）

＜脅威と影響＞

PC やスマートフォン利用者に、「アダルトサイトを閲覧している姿を撮影した」、「アダルトサイトの利用料金が未納である」等の内容が記載されたメール等を送りつけ、金銭を詐取しようと脅迫する攻撃が確認されている。しかし、実際には撮影や未納の事実はなく、単なる脅し文句である。

メールの受信者は脅迫を受けて不安になり、脅迫に従って金銭を支払ってしまう。

また、一度金銭を支払ってしまうと、同様の脅迫や詐欺行為が何度も繰り返され、さらに被害が拡大するおそれがある。

＜攻撃手口＞

◆ メール等に金銭を要求する脅迫

不特定多数のメール等に金銭を要求する脅迫を含めた内容を送信する。金銭の支払い方法として仮想通貨が使われる場合もある。[1]

◆ 周囲に相談しにくい「セクストーション（性的脅迫）」

「アダルトサイトを閲覧している姿を撮影した」、「アダルト動画を見られる有料サイトを使用した料金が未納である。」等、被害者が周囲に相談しにくい内容で脅迫することで、被害者の羞恥心につけこむ。[2]

◆ 受信者の情報を記載

メール受信者のメールアカウントのパスワード（過去に漏えいしてダークウェブなどで出回ったものを別途入手）を記載し、本当に攻撃者が被害者の PC をハッキングしているかのように装って、メールの内容を信じさせようとする。

◆ 電話でさらに追い込む

詐欺メールを受信して不安になり電話をかけてきた受信者に対し、「裁判沙汰になる。」等、脅迫してさらなる不安を煽る。

＜事例または傾向＞

◆ **性的脅迫を伴うメール**

2017 年 7 月以降、性的脅迫を伴うメールが確認されている。2018 年 8 月まではメールの文面は英語であったが、同年 9 月以降はメールの文面が日本語化されている。使用されている日本語は不自然であり、英語版のメールを機械的に日本語訳したものとみられる。[3]

また、メールの送信元として「情報セキュリティ大学院大学」を名乗る手口も確認されており、被害者を信じこませる手口が巧妙化している。[4]

2018 年 10 月末までに、性的脅迫を伴うメールに記載されたビットコインアドレスに合計 1,240 万円相当のビットコインが送金されたことが確認された。[5]

◆ **有料サイトの料金未納であるなどと偽り電子マネーを詐取**

被害者に対し、有料サイトの料金が未納である旨のメールを送信した上、電話をかけてきた被害者に対し、「未納料金を払わなければ裁判沙汰になる。」等、脅迫し、合計約 20 万円分の電子マネーを騙し取ったとして詐欺の容疑で、2018 年 12 月、福岡市内の男性ら 5 人が警察に逮捕された。犯人グループによる被害総額は全国で、合計約 1 億 4,000 万円に上るとみられている。[6]

＜対策/対応＞

個人（インターネット利用者）

- 被害の予防（被害に備えた対策含む）
  - ・表 1.4「情報セキュリティ対策の基本」を実施
  - ・受信した脅迫・詐欺メールは無視する

    詐欺メールに、被害者のパスワード等が記載されていても、実際にハッキングされているわけではない。被害者のパスワード等は、別のところから漏えいしたものであると思われる。
- 被害を受けた後の対応
  - ・パスワードを変更する

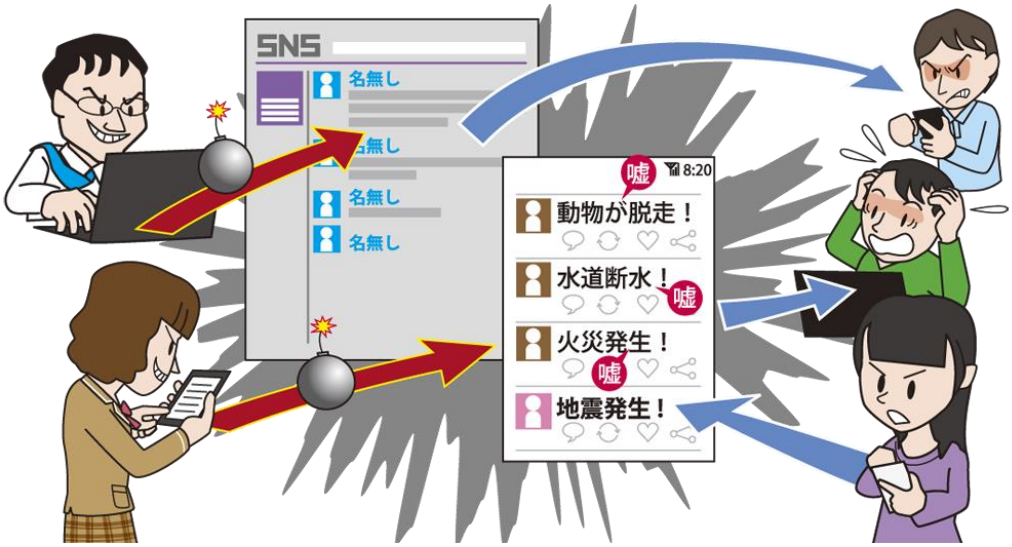
    脅迫・詐欺メールに記載されたパスワードが自分のパスワードと一致しているのであれば、どこかからパスワードが漏えいしたおそれがあるので、早急にパスワードを変更する。
  - ・警察に相談する

参考資料

1. 仮想通貨を要求する日本語の脅迫メールについて
https://www.jpcert.or.jp/newsflash/2018091901.html
2. 「架空請求詐欺」の被害、県内で急増
https://www.asahi.com/articles/ASLBB45X0LBBUOOB004.html
3. 性的な映像をばらまくと恐喝し、仮想通貨で金銭を要求する迷惑メールに注意
https://www.ipa.go.jp/security/anshin/mgdayori20181010.html
4. 恥ずかし画像で不安煽る詐欺メール、送信元を情セ大に偽装
http://www.security-next.com/101226
5. 10月も継続した「セクストーション」スパム、総被害額は1,000万円を突破か
https://blog.trendmicro.co.jp/archives/19824
6. 全国35都道府県で被害　1億4000万円詐取容疑で男5人を再逮捕
https://headlines.yahoo.co.jp/hl?a=20181204-03310151-saga-l41

5位 ネット上の誹謗・中傷・デマ

～投稿前に内容を再確認、軽い冗談のつもりが社会問題になることも～



インターネットの匿名性を利用して、特定の個人や組織に誹謗・中傷や犯罪予告をする事件が依然として発生している。また、2018 年に起きた震災では、SNS サービス上で嘘情報を発信し、人々を混乱させる事件も発生する等、情報モラルや情報リテラシーを欠いた行為が度々問題となっている。

＜攻撃者＞

- 情報モラル、情報リテラシーが低い人
- 悪意を持っている人

＜被害者＞

- 個人
- 組織（教育機関、公共機関、企業）

＜脅威と影響＞

SNS サービス等の普及に伴い、匿名での情報発信が容易に行えるようになっている。一方、そのサービスを利用する中で、意図的に他人を誹謗・中傷したり、脅迫・犯罪予告を書き込む事件が確認されている。また、嘘情報（フェイクニュース等）をいたずらに発信し、その情報が拡散されることで、大きな問題になるケースもある。

攻撃の対象にされた人は、追い詰められて精神的苦痛に苛まされることもある。組織であれば、風評被害による経済的な損失を受ける等、様々な影響が出る。また、災害発生時に嘘情報が拡散されると、非日常的な状況下では情報の真偽が確認できないため、社会的に大きな混乱を引き起こすおそれがある。

＜要因＞

◆ 情報モラルや自己抑制力の欠如

自分の発言が他人に及ぼす影響を気にすることなく、安易にネット上へ投稿してしまう。特に、自身が持つ不満やストレスの捌け口として投稿する場合、過激な発言や、特定の個人や組織等の評判を落とすような発言をすることがある。

◆ 個人が匿名で発信できる場の増加

様々なコミュニティサイトが存在し、ブログや SNS、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、個人が匿名で自由に情報を発信することができる場が増加している。匿名であるがゆえ、真偽が不明な情報の発信もしくは拡散や、他者に対する誹謗・中傷等を、起きうる影響を深く考慮せずに行ってしまう。なお、実際には警察等が正式に調査すれば容易に身元を特定できる場合が多い。

◆ 情報の真偽を確認せずに拡散

インターネット上には嘘情報や真偽不明な情報が出回ることがある。そうした情報の真偽を確かめることなく、拡散してしまう。有用な情報を拡散して

あげたいという親切心や正義感によって拡散されているケースも多いと考えられる。

＜事例または傾向＞

◆　ネット上のトラブルによる刺殺事件が発生

あるブログ運営者がネット上のトラブルによって刺殺される事件が発生した。犯人は他人の誹謗・中傷を繰り返すことで迷惑がられており、あるブログ運営者が関連した内容をブログで取り上げたところ、犯人が過剰反応して犯行に及んだのではないかとされている。[1]

◆　学術機関に対する爆破予告の書き込み

インターネット上の掲示板に爆破予告が書き込まれ、対象となった大学が構内への立ち入り禁止を発表した。[2]

◆　震災発生時における嘘情報の拡散

震災が発生した際に SNS 上で、「大地震が数時間後に発生する」との嘘情報が出回り、被災者が不安を募らせる事例が発生した。嘘情報の発信源には、自衛隊の名称が使われており、市の危機管理室は市民からの事実確認の問い合わせ対応に追われることとなった。[3]

＜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、法令遵守の意識の向上

  ・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、匿名で投稿していても、権利侵害があった場合は被害者がプロバイダーに発信情報の開示を請求できるため、発信者の特定は可能という認識を持つ。

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

自宅や学校で子供たちに情報モラルや情報リテラシーの教育を行う。さらに、トラブルの事例を伝え、悪質な行為は犯罪になりうることを理解させる。[4]

個人（閲覧者）

- 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

  インターネット上に流通している情報が必ずしも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、不確定情報の拡散は、犯罪になりうることを理解する。

個人（被害者）

- 被害を受けた後の適切な対応

  ・冷静な対応と支援者への相談

  一人で抱え込まず、信頼できる周囲の人や公的相談機関へ相談する。[5]

  ・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

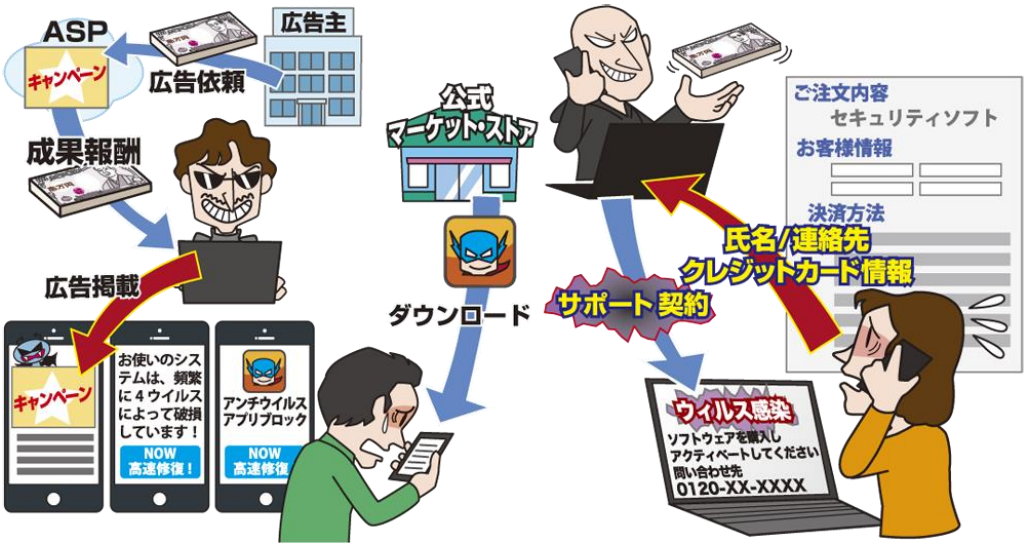
  問題ある書き込みを削除したいときは、本人または関係者がウェブサイトの管理者やプロバイダーに削除を要請する。なお、削除により炎上の火種になるおそれもあるため、関係者等に相談して慎重に行う。

参考資料

1. Hagexさん刺殺、殺人罪で容疑者起訴へ　福岡地検
https://www.asahi.com/articles/ASLB35W79LB3TIPE024.html
2. 青学大に爆破予告　7日休校、キャンパス立ち入り禁止
https://www.asahi.com/articles/ASL5671VTL56UTIL00F.html?iref=pc_ss_date
3. 北海道地震、SNSでデマ拡散　専門家「発信元確認を」
https://www.nikkei.com/article/DGXMZO35227790R10C18A9CC1000/
4. インターネットトラブル事例集（2018年度版）
http://www.soumu.go.jp/main_content/000590558.pdf
5. 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

6位 偽警告によるインターネット詐欺

～落ち着いて！あの手この手の騙しの警告画面～



PC やスマートフォンの利用者に対してインターネット閲覧中に、突然「ウイルスに感染しています」等の偽の警告画面（偽警告）を表示し、不要なソフトウェアをインストールおよび購入するように誘導したり、サポート窓口を装って電話を掛けさせ、サポート契約を結ばせる等で金銭を騙し取る被害が発生している。偽警告は利用者の不安につけこむ金銭詐欺であり、表示されても慌てず冷静に対応する必要がある。

＜攻撃者＞

- 犯罪グループ

＜被害者＞

- 個人（インターネット利用者等）

＜脅威と影響＞

インターネット閲覧中に、突然「ウイルスに感染しています」、「Windows のシステムが破損しています」等の偽の警告画面（偽警告）が表示されることがある。PC やスマートフォンの利用者は表示された偽警告を信じてしまい、警告の指示に従ってしまう。PC 利用者であれば、不要なソフトウェアをインストールしたり、サポート契約を結ばされる。スマートフォン利用者であれば、不要なアプリをインストールするように誘導される事例が多い。また、購入に使用された氏名、メールアドレス、クレジットカード情報は別の詐欺等に悪用される二次被害のおそれもある。

＜攻撃手口＞

◆ 巧妙に細工が施された偽の警告画面

偽警告は様々な警告メッセージを使い、偽警告を信じさせるために実在の企業ロゴを使う場合もある。また、警告音や警告メッセージを音声で流したり、警告画面を繰り返しポップアップで表示させる（偽警告を閉じさせない）ことでさらに不安を煽る。

◆ 偽対策ソフト（偽セキュリティソフト）

偽警告を表示し、PC 利用者に対して偽のセキュリティソフトをインストールさせる。そして最終的に有償ソフトウェアの購入へ誘導する。

◆ サポート契約詐欺

偽警告の画面に記載されている連絡先に電話をかけさせ、オペレーターによる遠隔操作により対策をしたように見せかけ、そして有償のサポート契約へ誘導する。サポート契約の支払い方法はクレジットカード決済やコンビニ決済等が確認されている。

◆　**スマホアプリのインストールへ誘導**

偽警告をスマートフォンの画面に表示し、警告画面に表示された警告の解決方法として、スマホアプリの公式マーケットからスマホアプリをインストールするように誘導する。[1]アプリのインストールへ誘導したことに対してのアフィリエイト収益が目的と考えられる。

＜事例または傾向＞

◆　**偽警告の相談が 5 月に急増、過去の手口が複合化した手口も**

IPA 安心相談窓口には多数の偽警告に関する相談が寄せられている。相談の状況から、2016 年 5 月に偽のエラー警告からソフトウェアの購入へ誘導する「偽セキュリティソフト」の手口、そして 2016 年 6 月には偽の警告画面に記載されている連絡先に電話をかけさせ、有償のサポート契約に誘導する「偽警告」の手口について注意を呼び掛けている。その 2 つの手口に関する相談が 2018 年 5 月に急増している。また、2017 年の年末頃より、これらの 2 つの手口が複合化された「パソコンがウイルスに感染している」、偽の警告画面から有償ソフトウェアの購入へ誘導し、さらに電話をかけさせたうえで、遠隔操作を行い有償サポート契約の誘導する手口が継続して確認されている。[2]

◆　**偽警告による被害が急増**

独立行政法人国民生活センターでは警告画面や警告音をきっかけとしたセキュリティソフト等に関する相談件数が 2018 年 9 月 30 日までに 2,135 件と前年度同時期の相談件数 1,601 件を大きく上回った。インターネットを使用中に突然「ウイルスに感染している」等の警告画面が表示され、不安になり慌ててセキュリティソフトやサポートの契約をしてしまったという相談や、契約を解除しようとしても解約手続きが進まない等の相談が多く寄せられ、2018 年 11 月にトラブル防止のために消費者へ注意喚起を行った。[3]

＜対策/対応＞

個人（インターネット利用者）

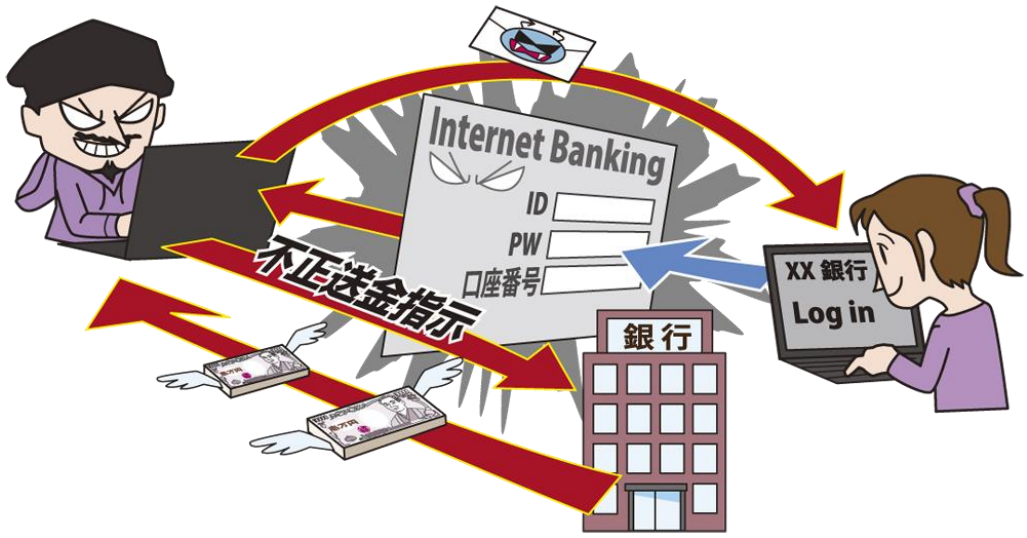
- 被害の予防（被害に備えた対策含む）
  - ・表 1.4「情報セキュリティ対策の基本」を実施
  - ・正規の警告を知る
    警告が本物か偽物かを判断するため、OS やセキュリティソフトの仕様を把握する。
  - ・偽警告が表示されても従わない
    偽警告の指示に従いアプリやソフトウェアはインストールしない。また、電話は掛けない、遠隔操作は許可しない、契約には応じない。
  - ・偽警告が表示されたらブラウザを終了
- 被害を受けた後の対応
  - ・端末を初期化
  - ・サポート契約の解消
    近くの消費生活センター[4]に相談する。
  - ・クレジットカード会社へ連絡

参考資料

1. ウイルス感染したという警告でアプリのインストールを誘導する手口が急増
https://www.ipa.go.jp/security/anshin/mgdayori20160711.html
2. IPA 安心相談窓口だより「偽のセキュリティ警告によって有償の「ソフトウエア購入」や「サポート契約」をしてしまう相談が増加中」
https://www.ipa.go.jp/security/anshin/mgdayori20180718.html
3. 独立行政法人国民生活センター「インターネット使用中に突然表示される偽セキュリティ警告画面にご注意！」
http://www.kokusen.go.jp/news/data/n-20181107_1.html
4. 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/

7位 インターネットバンキングの不正利用

～被害は継続して発生、しかし減少傾向に～



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ログイン情報を攻撃者が窃取し、本人になりすまして、不正送金や不正利用が行われている。インターネットバンキングを狙った攻撃は継続して確認されているが、被害件数や被害額は年々減少傾向となっている。

＜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）

＜脅威と影響＞

ウイルス感染やフィッシング詐欺等により、インターネットバンキングのログイン情報を窃取し、悪用する攻撃が行われている。情報を窃取された利用者は、インターネットバンキングから不正送金されることで、金銭的な被害を受ける。

＜攻撃手口＞

◆　ウイルス感染

攻撃者が、悪意あるファイルを正規のものであるように偽装してメールに添付し、安全なファイルと誤認させてファイルを開くように誘導し、ウイルスに感染させる。または、メールや SNS 等を利用し、悪意あるウェブサイトのリンクをクリックさせるように誘導し、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することにより、入力した認証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、利用者の口座から別の口座への不正送金を行う。また、情報を窃取するだけではなく、自動的に不正な送金処理まで行うウイルスも確認されている。

◆　フィッシング詐欺

実在する銀行等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不特定多数に向けて送信し、フィッシングサイトにアクセスさせる。そして、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。メールでは、実在する企業や組織をかたり、正規のメールであると利用者に誤認させる。また、メール件名に「請求書」、メール本文に「キャンセルはこちら」等、リンクのクリックを誘導する内容を記載し、フィッシングサイトにアクセスさせる手口も確認されている。

＜事例または傾向＞

◆　インターネットバンキングの不正送金は減少

警察庁によると、2018 年上半期のインターネットバンキング不正送金件数は 211 件、被害額は約 3 億 7,200 万円となり、2017 年上半期の 217 件、約 5 億 6,700 万円と比較して、件数は横ばい、被害額は減少している。これは「法人」の被害が減少したことの影響が大きく、「個人」の被害について見ると、2018 年上半期の被害額は約 3 億 3,000 万円となり、2017 年下半期までの減少傾向から増加に転じている。[1]

また、不正送金ウイルス「DreamBot」に感染する被害が続いていることから、一般財団法人日本サイバー犯罪対策センター（JC3）は、インターネット利用者に対して注意喚起を実施している。[2]

◆　ウイルス感染を狙う新たなばらまき型メール

2018 年も 2017 年に引き続き、インターネットバンキング等の認証情報の窃取を目的とした「URSNIF」を感染させるばらまき型メールが多数確認されている。これまでは悪意のある Word ファイルや Excel ファイルがメールに添付されているばらまき型メールが多かったが、2018 年 7 月以降で、VBScript ファイルや PDF ファイル等が添付された新しいばらまき型メールも確認されている。[3]

◆　バンキングマルウェア Emotet を国内で確認

インターネットバンキング等のインターネットサービスにおける認証情報を窃取することを目的とした「Emotet」を感染させるばらまき型メールが多数確認された。[4] 当該メールの国内での検出数が特に多かったのは 2018 年 11 月ごろで、実在の企業をかたったメールに PDF ファイルや Word ファイルが添付されており、PDF ファイルに記載された URL からダウンロードしたファイルを実行したり、Word ファイルのマクロを実行することで Emotet に感染するおそれがある。

＜対策/対応＞

個人（利用者）

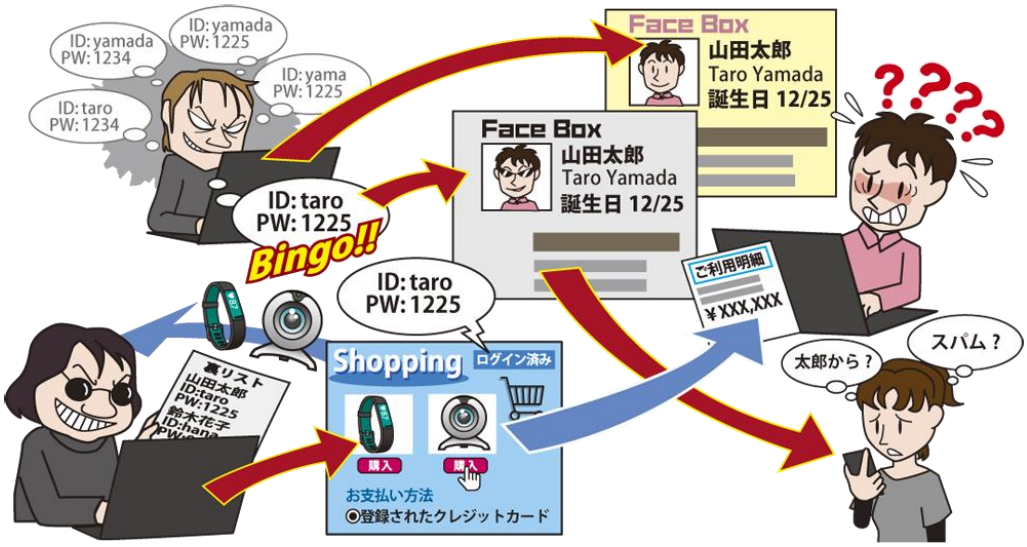
- 被害の予防（被害に備えた対策含む）
  - ・表 1.4「情報セキュリティ対策の基本」を実施
  - ・受信メールやウェブサイトの十分な確認
  - ・添付ファイルやリンクを安易にクリックしない
  - ・ファイルの拡張子を表示させる設定
  - ・怪しい（普段は表示されない）ポップアップに個人情報等は入力しない
  - ・銀行や公的機関から公開される注意喚起等の確認
  - ・多要素認証等、銀行が推奨する認証方式の利用
- 被害の早期検知
  - ・不審なログイン履歴の確認
  - ・口座の利用履歴の確認
  - ・利用時のメール連絡機能等の利用
- 被害を受けた後の対応
  - ・該当サービスのコールセンターへの連絡
    金融機関によっては、全額または一部補償してくれる場合がある
  - ・警察への被害届の提出
  - ・端末の初期化
  - ・パスワードの再設定

参考資料

1. 平成30年上半期におけるサイバー空間の脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/H30_kami_cyber_jousei.pdf
2. 不正送金等の犯罪被害につながるメールに注意
https://www.jc3.or.jp/topics/virusmail.html
3. 2018年7月 マルウェアレポート
https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1807.html
4. 2018年11月 マルウェアレポート
https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1811.html

8位 インターネットサービスへの不正ログイン

～多要素認証や多段階認証等を利用して攻撃に備えを～



インターネット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を受ける事例が確認されている。インターネット利用者が複数のサービスを利用する際に同じ ID とパスワードを使いまわしてしまう場合がある。その ID やパスワードを狙ったパスワードリスト攻撃による不正ログインが多く見られる。

＜攻撃者＞

- 犯罪グループ
- 犯罪者（ストーカー等）

＜被害者＞

- 個人（インターネットサービス利用者）
- 組織（インターネットサービス運営者）

＜脅威と影響＞

ID とパスワードが窃取または推測され、インターネットサービスへ不正ログインされる被害が 2018 年も多数確認されている。

インターネットサービスへの不正ログインによる影響は、利用しているインターネットサービスの機能によって様々である。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、サイトに登録しているクレジットカード情報やポイントを利用して不正に商品を購入される。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を覗き見される。さらに、その SNS を攻撃者に操作されて不正な広告やリンク等が知人に配信されてしまった場合、知人にも被害が及ぶおそれがある。

＜攻撃手口＞

◆ パスワードリスト攻撃

何らかの方法で入手した ID とパスワードを利用してログインを試みる攻撃手法である。

複数のインターネットサービスで同じ ID とパスワードを使いまわしている場合、1 つのインターネットサービスの ID とパスワードが漏えいすると、他のインターネットサービスにも不正ログインされ、被害が拡大するおそれがある。

◆ 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、パスワードに ID と同一の文字列や単純な単語、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やすい。SNS で公開している情報を使用することもある。[1]

◆ ウイルス感染

利用者が悪意あるウェブサイトやメールの添付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する。攻撃者はその端末で入力されたインターネットサービスの ID やパスワード等の情報を窃取し、不正ログインに利用する。

＜事例または傾向＞

◆ **不正ログインによるオンラインストアにおけるなりすまし購入**

NTTドコモが運営する「ドコモオンラインショップ」において、2018 年 7 月にパスワードリスト攻撃による約 1,800 件の不正ログインが行われたことが確認された。また、そのうち約 1,000 件で「iPhone X」が不正に購入される被害が発生していた。ドコモオンラインショップで商品購入する仕組みを悪用することにより、ログインさえできれば、商品を不正購入できる状態であった。

同社は本事例への対策として、オンラインショップの仕様を変更した。また、不正ログイン対策として、利用者に 2 段階認証の利用と適切なパスワードの設定を呼びかけた。[2,3]

◆ **不正ログインによるポイントの窃取と個人情報流出**

イオンマーケティングが電子マネーのポイントサービスを提供する「smartWAON ウェブサイト」において、2018 年 9 月にパスワードリスト攻撃による不正ログインが確認された。この不正ログインによって、52 名のポイントが第三者のカードに不正に移行されていた。また、一部の利用者の個人情報も閲覧されたおそれがある。[4,5]

◆ **不正ログインによる SNS スパムが再活性化**

2015 年頃から、Facebook や Twitter の不正ログインされたアカウントから、有名ブランド「レイバン」をかたったスパムが投稿される被害が多数確認されていたが、2018 年には mixi や Instagram でも同様のスパムが多数確認された。

攻撃者が不正ログイン時にスパムの投稿のみを行う場合、利用者は通常通りアクセスできるためスパムの投稿を見逃すと不正ログインされたことに気付かず、対策を放置してしまうおそれがある。[6]

＜対策/対応＞

個人（インターネットサービス利用者）

- 被害の予防
  - ・表 1.4「情報セキュリティ対策の基本」を実施
  - ・パスワードは長く、複雑にする
  - ・パスワードの使いまわしをしない

    例えばパスワードの基となるコアパスワードを作成し、その前後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することができる。[7]
  - ・パスワード管理ソフトの利用
  - ・サービスが推奨する認証方式の利用

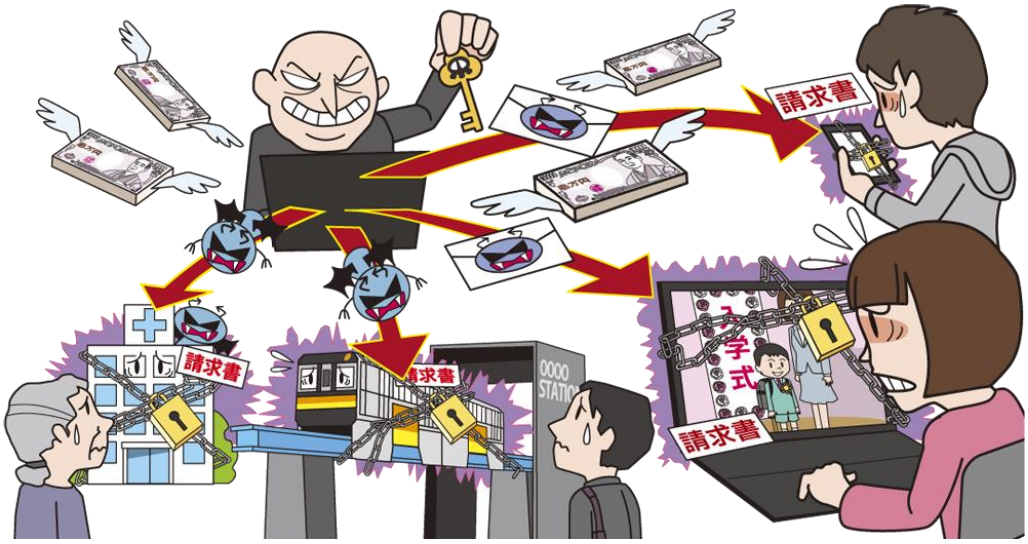
    ワンタイムパスワード等の多要素認証や多段階認証を利用することで、仮にパスワードが攻撃者に漏えいしたとしても、不正ログインや、その後の金銭被害等につながる重要な操作を阻止できる。[8]
  - ・不審なウェブサイトで安易に認証情報を入力しない（フィッシングに注意）
  - ・利用頻度が低いサービスや不要なサービスのアカウント削除
- 被害を受けた後の対応
  - ・パスワードを変更する
  - ・クレジットカードの停止
  - ・インターネットサービス運営者への連絡

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. 「iPhone X」不正購入被害1000件 「ドコモオンラインショップ」に不正ログイン、リスト型攻撃で
http://www.itmedia.co.jp/news/articles/1808/13/news084.html
3. 不正なアクセス対策としての「2段階認証」ご利用のお願い
https://www.nttdocomo.co.jp/info/notice/page/180814_00_m.html
4. WAONのポイント不正移行、被害者数を上方修正 - 個人情報流出の可能性も
http://www.security-next.com/098231
5. 「smartWAON ウェブサイト」における不正ログインについてお詫びと調査結果のお知らせ
http://www.aeonmarketing.co.jp/pdf/news_20180915.pdf
6. 「SNSスパム」が再び活発化？--原因と対策をチェック
https://japan.zdnet.com/article/35120490/
7. 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
8. 不正ログイン対策特集ページ
https://www.ipa.go.jp/security/anshin/account_security.html

9位 ランサムウェアによる被害

～ランサムウェアに感染し、思い出の写真や知人の連絡先情報等が閲覧不可に～



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、復旧に金銭を支払うよう脅迫するランサムウェアと呼ばれるウイルスへの感染が確認されている。感染すると PC やスマートフォン内に保存された家族や友人との思い出の写真や知人の連絡先情報等が閲覧できなくなる。また、2018 年は、個人に直接的な影響は少なかったが病院や鉄道会社といった日常生活でよく利用する組織においても被害が確認されている。

＜攻撃者＞

- 犯罪グループ
- 犯罪者

＜被害者＞

- 個人
- 組織

＜脅威と影響＞

PC やスマートフォンの利用に制限を掛け、制限を解除するために金銭を支払え等の脅迫文を表示するランサムウェアと呼ばれるウイルスの感染が広がっている。メールの添付ファイルを開いたり、ソフトウェアの脆弱性等を悪用した攻撃を受けることでランサムウェアに感染している。

ランサムウェアに感染すると、PC やスマートフォンのファイルを暗号化されたり、画面ロック等され、ファイルを開けなくなったり、PC やスマートフォンの利用を制限される。例えば、家族や友人との思い出の写真、お気に入りの音楽データ、年賀状用等に保存している知人の連絡先情報が閲覧できなくなる。また、個人が直接ランサムウェアの影響を受けなくても、病院や鉄道会社等の日常的に利用する組織が感染し、業務停止となった場合、日常生活に支障をきたすおそれがある。

＜攻撃手口＞

◆ メールからの感染

メールの添付ファイルやメール本文中のリンクを開かせることでランサムウェアに感染させる。

◆ ウェブサイトからの感染

脆弱性等を悪用しランサムウェアをダウンロードさせるよう改ざんした正規のウェブサイトや攻撃者が用意したウェブサイトを閲覧させることで、ランサムウェアに感染させる。そのようなウェブサイトに誘導するためにメール等が利用される場合もある。

◆ 脆弱性を悪用したネットワーク越しの感染

OS の脆弱性を悪用し、パッチを当てずにインターネットへ接続している PC をランサムウェアに感染させる。

＜事例または傾向＞

◆ **鉄道組織でランサムウェア感染、列車の運行には影響無し**

2018 年 7 月、多摩都市モノレールは、業務用ファイルサーバがランサムウェアに感染させられる被害を受けた。ファイルサーバには個人情報を含む情報が保存されていたが、情報漏洩の被害は確認されなかった。また、列車の運行に関わるシステムや定期購入に関わるシステムは別系統で管理されており、列車の安全運行等には支障はなかった。[1]

◆ **奈良県の病院で電子カルテシステムがランサムウェアに感染、身代金は支払わず**

2018 年 10 月、奈良県宇陀市立病院は、ランサムウェアに感染し、電子カルテシステムが約 2 日間にわたり使用できない被害を受けた。攻撃者より身代金の支払い要求があったが、金銭は支払わず、システムの復旧までは紙カルテおよび伝票運用による診療を行った。なお、感染した原因は、システム会社の不備により、最新のセキュリティソフトがインストールされていなかったことであった。また、バックアップ装置が適切に設定されておらず、データが一部復元できなかった。[2]

◆ **脅迫してランサムウェアに感染させる攻撃を確認**

盗撮した画像や動画を公開すると嘘の脅しを行い、金銭を騙し取る詐欺と組み合わせて、さらにランサムウェアにも感染させる攻撃が米国を中心に確認された。2018 年 12 月に観測された攻撃メールでは、盗撮を行い、証拠を示すプレゼンテーション動画を用意したと脅してくる。そして、本文内のリンク等からランサムウェアに感染させていた。JPCERT/CC によると、類似した文章を用いる詐欺メールはこれまでも流通していたが、ランサムウェアへの感染を狙うケースは、今回はじめて報告されたと指摘している。[3]

＜対策/対応＞

個人

- 被害の予防
  - ・表 1.4「情報セキュリティ対策の基本」を実施
  - ・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
  - ・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 3 位「不正アプリによるスマートフォン利用者の被害」の対策を参照。
  - ・バックアップの取得

  バックアップに使用する記録媒体は、ランサムウェアによって暗号化されないように、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。なお、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 [4]
  - ・復元機能の活用

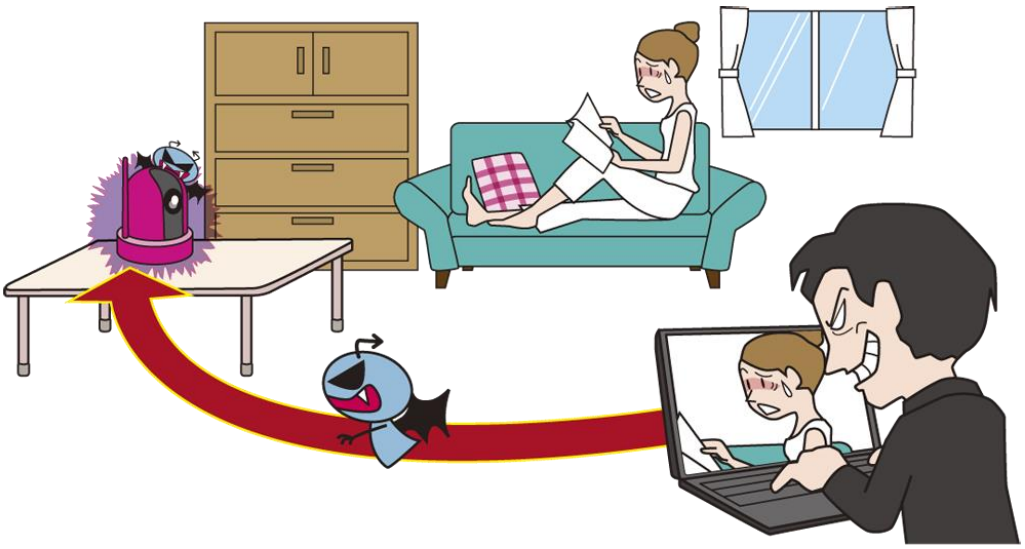
  DropBox や Google ドライブ、Microsoft OneDrive 等のクラウドサービスの中には復元機能を持っているものもあり、その機能を活用する。

参考資料

1. サイバーセキュリティ被害について
https://www.tama-monorail.co.jp/info/list/mt_img/180713%20press.pdf
2. 電子カルテシステムの障害発生について
https://www.city.uda.nara.jp/udacity-hp/oshirase/change-info/documents/press-release.pdf
3. 恥ずかし画像詐欺とランサム攻撃が融合 -「証拠動画」のリンクにワナ
http://www.security-next.com/100906
4. The No More Ransom Project
https://www.nomoreransom.org/ja/index.html

10位 IoT 機器の不適切な管理

～増え続ける IoT 機器を悪用する攻撃～



企業だけでなく一般家庭でもインターネット経由で操作を行うことができる IoT 機器の利用が増えている。しかし、パスワードの設定や管理が不十分なケースも多い。そのような IoT 機器に不正アクセスされ、情報の盗み見等の被害が発生している。

＜攻撃者＞

- 犯罪グループ

＜被害者＞

- 個人（IoT 機器利用者等）
- 組織（企業、IoT 機器利用者）

＜脅威と影響＞

昨今では様々な IoT 機器が普及しており、様々な製品をネットワーク経由で遠隔地から操作することができるようになった。しかし、IoT 機器利用者の情報リテラシーが十分ではなく、初期設定のパスワードのまま使用したり、アクセス制限を設けていない状態となっている IoT 機器は多数存在している。このような状態の IoT 機器には、乗っ取りの被害に遭うおそれがある。また、IoT 機器に脆弱性が見つかる場合もあり、IoT 機器の利用者がファームウェアの更新を怠ると、攻撃者に脆弱性を悪用されるおそれもある。

例えばネットワークカメラが乗っ取られた場合、IoT 機器の利用者が気付かないうちに盗撮される等、プライバシーの侵害を受けることもある。また、IoT 機器がウイルスに感染させられた場合、感染した IoT 機器を踏み台として、別の機器への攻撃や、さらなる感染活動に悪用される。

＜攻撃手口＞

◆ 初期設定のままの IoT 機器へ不正アクセス

工場出荷状態の IoT 機器には初期パスワードが設定されているが、IoT 機器の仕様によっては使用開始時にその変更を求められないものもある。攻撃者は IoT 機器に対して IoT 機器の説明書に記載された初期パスワードでログインを試行し、初期パスワードのまま使用している IoT 機器に不正アクセスを行う。[1]

◆ 脆弱性を悪用した攻撃

IoT 機器の公開された脆弱性を悪用し、パッチ適用が行われていない IoT 機器を乗っ取る。

◆ ウイルスを用いた攻撃

攻撃者は、IoT 機器にウイルスを感染させ、ネットワーク上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。また、ウイルスに感染した IoT 機器を利用して、DDoS 攻撃を行う。

＜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て覗き見したり、盗撮する。

- 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＞

◆ 監視カメラへの不正アクセス

2018 年には、複数の組織において、組織が管理するウェブカメラへの不正アクセスが行われた。被害にあったウェブカメラはいずれも、初期設定のままのパスワードを使用していた。攻撃者により、不正アクセスを受けた結果、ウェブカメラの映像に攻撃者が設定したメッセージが表示されるようになっていた。[1]

本事例では組織が設置した監視カメラが狙われたが、個人の設置する監視カメラが同様の被害に遭うおそれもある。

◆ IoT マルウェア「サトリ」の攻撃が激化、新手のワームも出現

2018 年 6 月、IoT 機器を狙うウイルスである「サトリ」が形成するボットネットを通じて、特定のルーターの脆弱性を悪用する新たなウイルスに感染させようとする攻撃が世界各地で確認された。このウイルスに感染した IoT 機器からの DDoS 攻撃も報告されている。[2]

＜対策/対応＞

個人（利用者）

- 情報リテラシーの向上
  - ・信頼できるメーカーの製品を使用。
  - ・使用前に取扱説明書で適切な使用方法を確認する。
- 被害の予防
  - ・表 1.4「情報セキュリティ対策の基本」を実施
  - ・初期パスワードから長く複雑なものへ変更[3]
  - ・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[4]
  - ・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。
  - ・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. 監視カメラへの不正アクセスについて調べてみた
https://piyolog.hatenadiary.jp/entry/20180428/1524936297
2. IoTマルウェア「サトリ」の攻撃が激化、新手のワームも出現
http://www.itmedia.co.jp/enterprise/articles/1806/21/news055.html
3. 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
4. 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/security/technicalwatch/20160531.html

コラム 2：セキュリティ技術者の法的リスク　～刑事法上の責任～

高度化するサイバー攻撃から重要な情報を守るため、攻撃手法の対策を講じる必要がありますが、その際、セキュリティ技術者らが留意すべき刑事法上の規定を紹介します。

1　コンピュータ・ウイルスに関する罪（「不正指令電磁的記録作成罪等」 刑法 168 条の 2、同条の 3）

コンピュータ・ウイルス（以下「ウイルス」）の作成、提供、供用、取得、保管行為を処罰する規定です。

⑴ ウイルス作成・提供罪は、①正当な理由がないのに、②無断で他人のコンピュータにおいて実行させる目的で、③ウイルスを、④「作成」又は「提供」した場合に成立し、3 年以下の懲役又は 50 万円以下の罰金に処せられます。また、ウイルス供用罪は、①正当な理由がないのに、②ウイルスを、③人の電子計算機における実行の用に供した場合に成立し、3 年以下の懲役又は 50 万円以下の罰金に処せられます。

例えば、セキュリティソフトの開発等の目的でウイルスを作成する行為等については、そのウイルスを、自分のコンピュータのみで実行する目的か、あるいは、他人のコンピュータでその同意を得て実行する目的である場合には、①、②いずれの要件も欠き、ウイルス作成・提供罪は成立しないとされています。[1,2]

⑵ ウイルス取得・保管罪は、①正当な理由がないのに、②無断で他人のコンピュータにおいて実行させる目的で、③ウイルスを、④「取得」又は「保管」した場合に成立し、2 年以下の懲役又は 30 万円以下の罰金に処せられます。

仮想通貨をマイニング（採掘）するプログラム「Coinhive（コインハイブ）」をウェブサイトに埋め込み、同サイト閲覧者の CPU を使用してマイニングを行った事例が発生し、議論が起きています。（2019 年 2 月時点で、一部の事例につき刑事裁判が係属中です）。[3]

2　不正アクセス行為の禁止等に関する法律（以下「不正アクセス禁止法」）

⑴ 不正アクセス禁止法では、①不正アクセス行為、②他人の識別符号を不正に取得、保管する行為、③不正アクセスを助長する行為、④フィッシング行為を禁止しています。

⑵ 「不正アクセス行為」とは、ⓘ「他人の識別符号を悪用する行為」つまり、他人の識別符号を利用して、本来アクセス権限のないコンピュータを利用する行為や、ⓘⓘ「コンピュータプログラムの不備を衝く行為」つまり、セキュリティ・ホールがあるシステムに対して、ネットワーク経由で、特殊な情報又は指令を入力することで、本来は識別符号を入力しなければ行うことができない特定利用をできる状態にする行為を言います [4]。

大学の研究員が、コンピュータソフトウェア著作権協会のウェブサイトの脆弱性を悪用し、サーバー内ファイルに不正にアクセスした行為が不正アクセス禁止法違反とされた事例があります [5]。

参考資料

1. 法務省「いわゆるコンピュータ・ウイルスに関する罪について」
http://www.moj.go.jp/content/000076666.pdf
2. 法務省「いわゆるサイバー刑法に関するQ＆A」
http://www.moj.go.jp/content/000073750.htm
3. 仮想通貨「無断採掘」の疑い　県警、容疑者 2 人を逮捕
http://www.kanaloco.jp/article/338916
4. 不正アクセス行為の禁止等に関する法律の解説
https://www.npa.go.jp/cyber/legislation/pdf/1_kaisetsu.pdf
5. 「不正アクセス」の司法判断とは－ACCS 裁判
http://www.itmedia.co.jp/news/articles/0503/28/news008.html

このページは空白です。

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）

1位 標的型攻撃による被害

～標的型攻撃メールの多くは Office 文書ファイルを悪用～

企業や民間団体そして官公庁等、特定の組織から重要情報を窃取することを目的とした標的型攻撃が発生している。攻撃者はメールの添付ファイルや悪意のあるウェブサイトを利用し、組織の PC をウイルスに感染させる。その後、組織内部へ潜入し、組織内部の侵害範囲を拡大しながら重要情報や個人情報を窃取する。

＜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＞

組織の機密情報や知的財産情報等の重要情報の窃取を目的とし、組織内部へ潜入する標的型攻撃が確認されている。メールの添付ファイルやウェブサイト等から組織の PC をウイルスに感染させられ、そこを起点に組織内部へ潜入される。組織の情報システム内部が探索され、侵害範囲を拡大し長期に渡り、組織の重要情報の窃取や偵察が繰り返し行われる。重要情報が流出し悪用されると、組織、企業の事業継続に大きな影響を与えるおそれがある。また組織の活動を妨害するデータ削除やシステム破壊が行われる場合もある。標的組織の関連組織が攻撃の踏み台にされることもあり、業種や組織の規模に関係なく狙われるおそれがある。

＜攻撃手口＞

◆ メールの添付ファイルやリンク

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、開かせることで組織の PC をウイルスに感染させる。本文や件名、添付ファイル名は業務に関連するような内容に偽装され、実在する組織の差出人名が使われる場合もある。また複数回のメールのやりとりで油断させ、添付ファイルを開かせる等、不審を抱かないような巧妙な騙しのテクニックが使われる。

◆ ウェブサイトの閲覧

標的の組織が閲覧するウェブサイトを調査し、ウェブサイトからウイルスに感染させるように改ざんする。標的となる組織の従業員が改ざんされたウェブサイトを閲覧することでウイルスに感染する。

◆ 不正アクセス

組織が利用するメールのクラウドサービスやウェブサーバーへ不正アクセスし、認証情報等を窃取する。そして窃取した情報を利用し、社内システムの利用等に用いる正規のアクセス経路で組織内部へ潜入し、組織内部の PC やサーバーをウイルスに感染させる。

＜事例または傾向＞

◆　CSV ファイルを悪用した標的型攻撃メール

サイバー情報共有イニシアティブ（J-CSIP）によると J-CSIP 参加組織宛に届いた国内組織を狙う標的型攻撃メールのうち、悪意のある CSV ファイル（拡張子「.csv」）が使用されているものを観測した。CSV ファイルはカンマ記号で区切られているテキスト形式のファイルであり、Microsoft Excel に関連付けされていることが多い。この場合、CSV ファイルを開くと Microsoft Excel が起動され、コンテンツに関する警告が表示される。ここでコンテンツを有効にすると、ファイルに埋め込まれた命令が実行される。なお、メモ帳やテキストエディタでファイルを開くと命令は実行されない。[1]

J-CSIP では、Microsoft Office の文書ファイルを悪用した手口についても注意を促している。拡張子が「.wiz」[2]、「.iqy」、「.slk」等、Microsoft Excel や Word に関連づけされたファイルを開くと警告画面が表示される。「～を有効にする」等、何らかの命令を許可する操作を選択するとウイルスに感染するおそれがある。

＜対策/対応＞

組織（経営者層）[3]

- 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
  - ・セキュリティ教育の実施
  - ・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る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。
  - ・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
  - ・組織内の体制（CSIRT 等）の運用
  - ・影響調査および原因の追究、対策の強化

組織（システム管理者）[4]

- 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）
  - ・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）
  - ・表 1.4「情報セキュリティ対策の基本」を実施
- 被害を受けた後の対応
  - ・CSIRT への連絡

参考資料

1. サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2018年1月～3月]
https://www.ipa.go.jp/files/000066063.pdf
2. WIZファイルを悪用する攻撃手口に関する注意点
https://www.ipa.go.jp/files/000069663.pdf
3. 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
4. 「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

2位 ビジネスメール詐欺による被害

～日本語のメールが使用されたビジネスメール詐欺の事例も～

ビジネスメール詐欺（Business E-mail Compromise：BEC）は、取引先や経営者とやりとりするようなビジネスメールを装い、巧妙に細工されたメールのやりとりで企業の金銭を取り扱う担当者を騙し、攻撃者の用意した口座へ送金させる詐欺の手口である。当初は主に海外の組織が被害に遭ってきたが、ここ数年で国内企業でも被害が確認されはじめ、2018 年には日本語のビジネスメール詐欺の事例も確認された。

＜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、取引に伴う金銭の支払いのやりとりもメールで行われている。昨今、そのメールのやりとりを狙ったビジネスメール詐欺と呼ばれる攻撃が国内外で行われている。攻撃者は、通常の取引のメールと見分けづらいように作成したメールや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い、取引先や経営者等を装い企業の財務担当者を騙そうとする。

メールを受信した財務担当者が、そのメールを信じてしまうと、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たりしてしまう。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

取引先と請求に係るやりとりをメールで行っている際に、攻撃者が取引先になりすまし、攻撃者の用意した口座に差し替え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や関係している従業員の情報をなんらかの方法により入手した上で攻撃を行なっている。

◆　経営者等へのなりすまし

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の情報を利用し、通常の社内メールであるかのように偽装する。

◆　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

ル本文は巧妙に偽装され、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＞

◆　**ビジネスメール詐欺で日本人の逮捕者**

2018 年 7 月、ビジネスメール詐欺にて米国の農業関連会社が約 7,800 万円の詐欺被害にあったことが報じられた。[1] 本件において国内の会社役員ら男女 4 名が逮捕された。

◆　**日本語が使用されたビジネスメール詐欺**

2018 年 8 月、IPA で情報提供を受けた日本語のビジネスメール詐欺の事例と手口についての注意喚起を行った。[2] この事例では、メールの送信元として実際の CEO をかたり、偽の弁護士をメール本文に登場させながら、機密扱いでお願いしたいという旨のメールが従業員に送信されてきた。その後、本メールに返信したところ約 5 分後には、国際送金の必要があるという旨のメールが送信されてきた。日本語のビジネスメール詐欺の手口が確認された初めての事例であり、海外との取引や英語のメールのやりとりがない国内の企業・組織もビジネスメール詐欺の被害に遭う可能性が高まっているといえる。

＜対策/対応＞

組織

- 被害の予防（被害に備えた対策含む）

・表 1.4「情報セキュリティ対策の基本」を実施

＜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。

・過剰に判断を急がせるメールに注意

至急の対応を要求するなど、担当者が真偽を確認する時間を与えないようにする手口も考えられる。真偽を確認するフローを事前に策定するなど準備をしておく。

・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によるなりすまし防止の対策も有効である。

＜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、パスワードの適切な管理やログイン通知機能等で不正ログイン対策を行う。

- 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

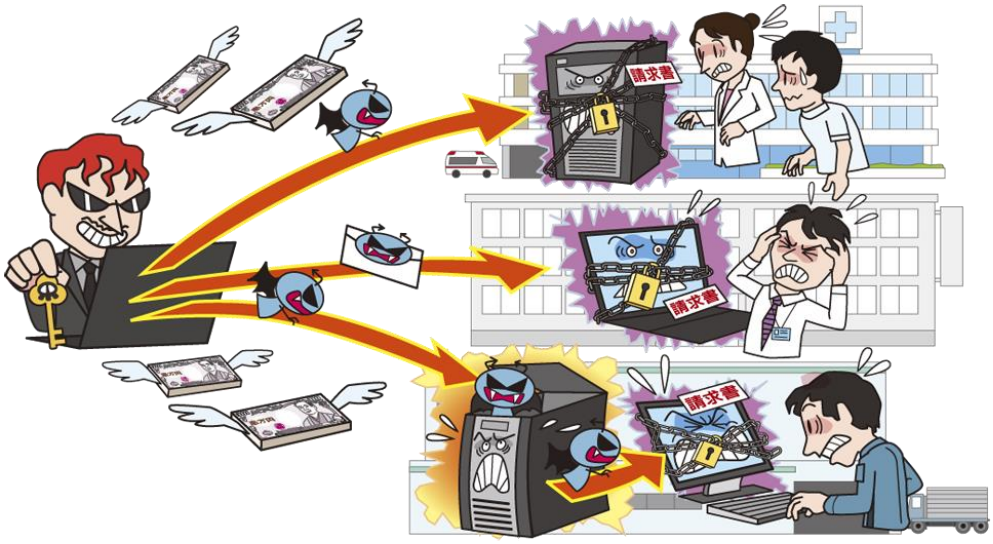
・影響調査および原因の追究、対策の強化

参考資料

1. 7千万円送金させた疑い　ビジネスメール詐欺で逮捕
https://www.nikkei.com/article/DGXMZO32602020U8A700C1CC1000/
2. 【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（続報）
https://www.ipa.go.jp/security/announce/201808-bec.html

3位 ランサムウェアによる被害

～ランサムウェアに感染し、不当に金銭を要求されたり、業務を妨害される～



PC（サーバー含む）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、復旧に金銭を支払うよう脅迫するランサムウェアと呼ばれるウイルスへの感染が確認されている。組織においては、業務を遂行する上で必要な情報を暗号化された場合、事業継続にも支障がでるおそれがある。また、脅迫に従った場合、金銭的な被害も発生する。

＜攻撃者＞

- 犯罪グループ
- 犯罪者

＜被害者＞

- 組織（経営者、システム管理者、従業員等）

＜脅威と影響＞

PC やスマートフォンの利用に制限を掛け、制限を解除するために金銭を支払え等の脅迫文を表示するランサムウェアと呼ばれるウイルスの感染が広がっている。メールの添付ファイルを開いたり、ソフトウェアの脆弱性等を悪用されることでランサムウェアに感染している。

ランサムウェアに感染すると、PC やスマートフォンのファイルを暗号化されたり、画面ロック等され、ファイルを開けなくなったり、PC やスマートフォンを利用できなくなる。暗号化されたファイルが顧客情報や基幹システムのファイル等、組織にとって重要な情報であった場合は、業務の遂行に大きな支障がでる。また、組織は事業継続のために、バックアップや復号ツール等により復旧するか、復旧する保証はないが、攻撃者の脅迫に従い金銭を支払うかの決断が求められる。

＜攻撃手口＞

◆ メールの添付ファイルやリンク

メールの添付ファイルやメール本文中のリンクを開かせることでランサムウェアに感染させる。

◆ ウェブサイトの閲覧

脆弱性等を悪用しランサムウェアをダウンロードさせるよう改ざんした正規のウェブサイトや攻撃者が用意したウェブサイトを閲覧させることで、ランサムウェアに感染させる。そのようなウェブサイトに誘導するためにメール等が利用される場合もある。

◆ 脆弱性の悪用

OS の脆弱性を悪用し、パッチを当てないままインターネットに接続している PC をランサムウェアに感染させる。

◆ その他の手口

リモートデスクトッププロトコル（RDP）等で遠隔からシステムに侵入しランサムウェアに感染させる。

＜事例または傾向＞

◆ **奈良県の病院で電子カルテシステムがランサムウェアに感染、身代金は支払わず**

2018 年 10 月、奈良県宇陀市立病院は、ランサムウェアに感染し、電子カルテシステムが約 2 日間にわたり使用できない被害を受けた。攻撃者より身代金の支払い要求があったが、金銭は支払わず、システムの復旧までは紙カルテおよび伝票運用による診療を行った。なお、感染した原因は、システム会社の不備により、最新のセキュリティソフトがインストールされていなかったことであると報告されている。また、バックアップ装置が適切に設定されておらず、データが一部復元できなかった。[1]

◆ **国内の組織の 35%がランサムウェアの被害経験有り**

2018 年 7 月に JPCERT/CC より公開されたレポートより、国内の重要インフラ組織を含む全 184 組織にとったアンケートの結果、35%の組織でランサムウェアの感染があったことが報告されている。感染原因として最も多いのは、メールの添付ファイル経由で、次にウェブサイトまたはウェブアプリケーション経由が続いている。[2]

◆ **ランサムウェア「SamSam」の被害総額が約 6 億 7,000 万円に**

2018 年 8 月にソフォスより公開されたレポートによると、ランサムウェア「SamSam」の被害額が 2018 年 7 月時点で約 600 万ドル（約 6 億 7,000 万円）になったことが報告されている。被害を受けているのは主に米国の組織であった。「SamSam」は 2015 年から確認されているランサムウェアで、リモートデスクトッププロトコル（RDP）を使って組織内部に潜入し、その後、ランサムウェアを感染させていく。最初の発見から複数回のバージョンアップを行っており、攻撃が年々巧妙化している。[3]

＜対策/対応＞

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
  - ・対策予算の確保と継続的な対策の実施

組織（システム管理者、従業員）

- 被害の予防（BCP 対策含む）
  - ・表 1.4「情報セキュリティ対策の基本」を実施
  - ・迅速かつ継続的に対応できる体制（CSIRT 等）の構築
  - ・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
  - ・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

    バックアップに使用する記録媒体は、ランサムウェアによって暗号化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。なお、バックアップから復旧できることの確認も重要である。
- 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 [4]
  - ・影響調査および原因の追究、対策の強化

＜例外措置＞

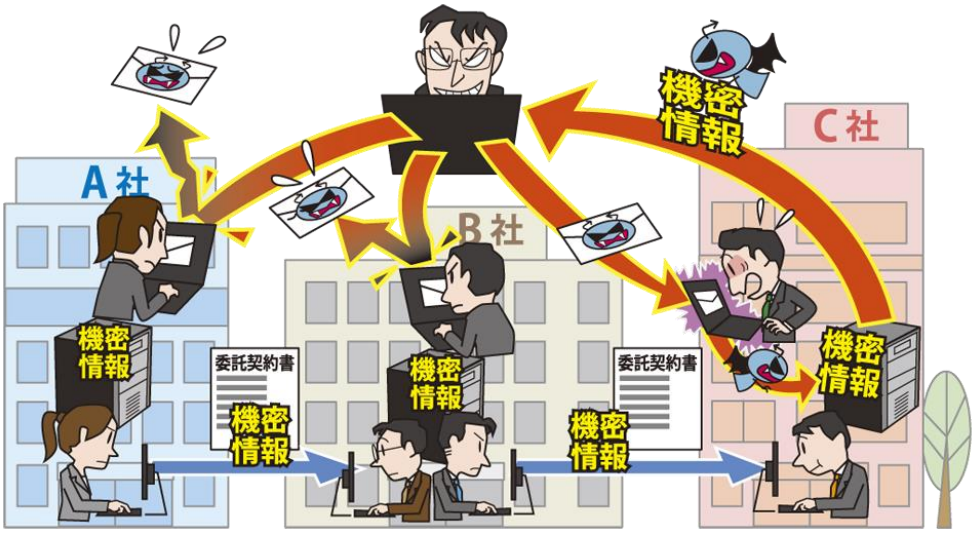
推奨されないが、暗号化されたファイルが人命に関わると、金銭を支払ったケースもある。

参考資料

1. 電子カルテシステムの障害発生について
https://www.city.uda.nara.jp/udacity-hp/oshirase/change-info/documents/press-release.pdf
2. ランサムウエアの脅威動向および被害実態調査報告書
https://www.jpcert.or.jp/research/Ransom-survey.html
3. SamSam: 600 万ドル（約6億7000万円）近くの身代金を手にしたランサムウェア
https://www.sophos.com/ja-jp/press-office/press-releases/2018/08/samsam-the-almost-6-million-ransomware.aspx
4. The No More Ransom Project
https://www.nomoreransom.org/ja/index.html

4位 サプライチェーンの弱点を悪用した攻撃の高まり

～業務委託先にも適切なセキュリティ管理を要求～



原材料や部品の調達、製造、在庫管理、物流、販売までの一連の商流、およびこの商流に関わる複数の組織群をサプライチェーンと呼ぶ。また、組織が特定の業務を外部組織に委託している場合、この外部組織もサプライチェーンの一環となる。業務委託先組織がセキュリティ対策を適切に実施していないと、業務委託元組織への攻撃の足がかりとして狙われる。昨今、業務委託先組織が攻撃され、預けていた個人情報が漏えいする等の被害が発生している。

＜攻撃者＞

- 犯罪グループ
- 犯罪者

＜被害者＞

- 組織（委託元組織、委託先組織）

＜脅威と影響＞

組織におけるウェブサイトの運営や情報システムの導入が当たり前になり、多くの組織で運用されている。しかし、ウェブサイトや情報システムの運用には設備や人材が必要であり、外部の業者に委託することもある。このような環境において、委託元組織からのガバナンスが効かない委託先組織がセキュリティ対策を適切に実施していないと、そこを攻撃者に狙われ、被害が発生する。

例えば、委託先組織に個人情報等の重要情報を扱うウェブサイトの運用管理を委託している場合、委託先が不正アクセスを受けることで、その情報が漏えいするおそれがある。また、ソフトウェア開発を委託している場合、セキュリティに配慮した開発が行われないと、脆弱性を内在したソフトウェアが納品され、ソフトウェア利用者が脆弱性を突いた攻撃を受ける。

これらの攻撃で被害を受けた場合、サービス利用者への賠償対応や、組織の信用の失墜により業務継続が困難になるおそれがある。

＜要因＞

◆　委託先組織のセキュリティ対策不足

サプライチェーン内にセキュリティ対策を適切に実施していない委託先組織がある。攻撃者はその弱点に対して攻撃を行い、そこから連鎖して委託元組織に被害がおよぶ。

◆　委託先組織を適切に選定、管理していない

委託元組織が委託先組織を選定するにあたり、セキュリティ対策の実施状況等の確認を怠ると、セキュリティ対策が不十分な組織に委託することがある。また、委託後も委託先の状況を管理せずにいると、委託先組織のセキュリティ対策が不十分なままとなり、攻撃者からの攻撃を受ける。

◆ **再委託先や再々委託先の管理が難しい**

委託先組織の先に再委託先組織や再々委託先組織がある場合、その管理は委託先組織が行うため、委託元にとってのセキュリティ対策管理は更に難しくなる。

＜事例または傾向＞

◆ **委託先への不正アクセスによる情報漏えい**

2018 年 2 月、ポルシェジャパン株式会社から、情報漏えいの被害が報告されている。[1] 本件では、業務委託を行っていた委託先の企業に対し不正アクセスが行われ、電子メールアドレスが漏えいした。また、委託先企業のウェブアプリケーションに何らかの問題があったことが原因とされた。

◆ **実施すべき情報セキュリティ対策を仕様書等で明示していない組織が多い**

2018 年 3 月に IPA が公開した「IT サプライチェーンの業務委託におけるセキュリティインシデント及びマネジメントに関する調査」によると、情報通信業以外の委託元企業の過半数で、実施すべきセキュリティ対策を仕様書等で委託先組織に明示していなかった。特に、製造業では 71%、卸売業・小売業では 74%が明示していなかった。

また、委託元組織、委託先組織ともに、契約におけるセキュリティ上の責任範囲や実施すべき具体的な情報セキュリティ対策が不明確な点を課題としており、両社の責任範囲と負担について契約上で明示することが望ましい。[2]

◆ **企業経営者を対象としたガイドラインの公開**

2017 年 11 月、経済産業省と IPA は、大企業及び中小企業（小規模事業者を除く）のうち、IT に関するシステムやサービス等を供給する企業及び経営戦略上 IT の利活用が不可欠である企業の経営者を対象に「サイバーセキュリティ経営ガイドライン V2.0」を公開した。

このガイドラインでは、経営者が認識する必要のある「3 原則」および経営者が情報セキュリティ対策を実施する上での責任者となる担当幹部に指示すべき「重要 10 項目」がまとめられている。[3]

＜対策/対応＞

組織（委託元組織）

- 被害の予防
  - ・業務委託や情報管理における規則の徹底
    製造においては原材料や部品の調達経路、物流経路等も考慮する。
  - ・信頼できる委託先組織の選定
    委託先組織の信頼性評価や委託先への品質基準を導入する。
  - ・委託先からの納品物の検証
  - ・契約内容の確認
    委託元組織と委託先組織の情報セキュリティ上の責任範囲を明確化し合意を得る。また、賠償に関する取り決めを契約に含める。
  - ・委託先組織の管理
    委託元組織が責任をもって委託先組織のセキュリティ対策状況の実態を定期的に確認することが重要である。
- 被害を受けた後の対応
  - ・影響調査および原因の追究、対策の強化
  - ・被害への補償

組織（委託先組織）

- 被害の予防
  - ・攻撃者の目的や攻撃手段は多岐に渡るため、他の脅威の対策を参考にすること。
- 被害を受けた後の対応
  - ・委託元への連絡

参考資料

1. 不正アクセスによるお客様情報の流出に関するお詫び
https://www.porsche.co.jp/news/201802-001.php
2. 「IT サプライチェーンの業務委託におけるセキュリティインシデント及びマネジメントに関する調査」報告書について
https://www.ipa.go.jp/security/fy29/reports/scrm/index.html
3. サイバーセキュリティ経営ガイドライン Ver 2.0
http://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf

5位 内部不正による情報漏えい

～不正を許さない管理・監視体制を～

組織の従業員や元従業員等、組織関係者による機密情報の漏えい、悪用等の不正行為が発生している。組織関係者による不正行為は、組織の社会的信用の失墜、損害賠償による経済的損失等により、組織に多大な損害を与える。

＜攻撃者＞

- 組織の従業員（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＞

悪意を持った従業員や元従業員が、組織の保管する顧客情報等の重要情報を閲覧することや持ち出すことがある。持ち出した重要情報は外部に公開されたり、競合関係にある同業他社に漏えいさせられることもある。これは組織に対する私怨や金銭目的等から行われている。

漏えいした情報の機密性や重要性、漏えい規模によっては、組織の社会的信用の失墜や、顧客等に対する損害賠償による経済的損失が発生し、組織の競争力の弱体化等につながり、結果、組織の根幹を揺るがすインシデントに発展するおそれがある。

＜攻撃手口＞

◆ **アクセス権限の悪用**

付与されたパスワードを悪用し、組織の重要情報を取得する。必要以上に高いアクセス権限を付与していると、権限悪用の被害が大きくなるおそれがある。

◆ **離職前のアカウントの悪用**

組織を離職した者が、離職前に使用していたアカウントを使って、組織の重要情報を不正に取得する。

◆ **USB メモリーや電子メール等による持ち出し**

組織の重要情報を USB メモリー等の外部記録媒体やメールを使用して、外部に持ち出す。

＜事例または傾向＞

◆ **市役所職員が、管理者パスワードを不正利用し、人事情報を閲覧**

岩手県八幡平市の職員が、一時的に付与された管理者用パスワードを業務外目的で使用し、業務用パソコンから人事に関する情報を不正に閲覧し、懲戒処分を受けた。[1]

◆ **元従業員が、営業管理ツールを悪用し、顧客情報を不正閲覧**

予約管理サービスの開発、販売を手掛けるリザーブリンクの元従業員が、同社の営業管理ツールに不正ログインして顧客情報を閲覧し、転職先の営業活動に不正利用していた。[2]

◆ **従業員が、社員情報を私物パソコンに転送した上、入手データを他団体に送付**

日本経済新聞社の従業員が、同社の業務用パソコンを分解してハードディスクを抜き取り、社員の賃金データ等を私用パソコンに転送した上、データを他団体に送付した。[3]

◆ **従業員が顧客のクレジットカード情報を盗み、不正利用**

セキ薬品の元アルバイト従業員が、勤務時に顧客のクレジットカード情報を盗み取り、同情報をインターネット通販で不正利用して商品を購入した。[4]

＜対策/対応＞[5]

組織

- 被害の予防

・基本方針の策定

組織全体において効率的な対策を推進するため、経営者の積極的な関与が重要である。経営者は、内部不正対策が経営者の責任であることを示すとともに、内部不正対策の総括責任者を定める等した基本方針を策定し、組織横断的な管理体制を構築する必要がある。

・情報資産の把握、体制の整備

重要な情報資産を把握し、重要度に応じた格付けをした上で重要情報の管理担当者を定める。

・重要情報の管理、保護

重要情報の利用者 ID・アクセス権の登録、変更、削除等の手順を定めて運用する。従業員の異動や離職時に伴い、不要となった利用者 ID およびアクセス権を直ちに削除する。

また、アカウントおよび権限の適切な管理、定期的な監査を実施する。

・物理的管理の実施

重要情報の格納場所等へ入退去を管理する。また、USB メモリー等外部記録媒体の利用の制限をする。

- 情報モラルの向上

・人的管理、コンプライアンス教育の徹底

情報取扱ポリシーの作成、不正行為を犯した者に対する懲戒処分等を規定した就業規則等の内部規程の整備を行い、従業員に対する教育を実施する。その際、従業員に秘密保持義務を課す誓約書を作成させることも重要である。

また、離職者と秘密保持契約等を締結し、離職後の重要情報の漏えいを防止する。

- 被害の早期検知

・システム操作履歴の監視

重要情報へのアクセス履歴や利用者の操作履歴等のログ、証跡（メールの内容等）を記録し、監視することで、内部不正の早期検知に努める。

- 被害を受けた後の対応

・CSIRT への連絡

・警察への連絡

・影響調査および原因の追究、対策の強化

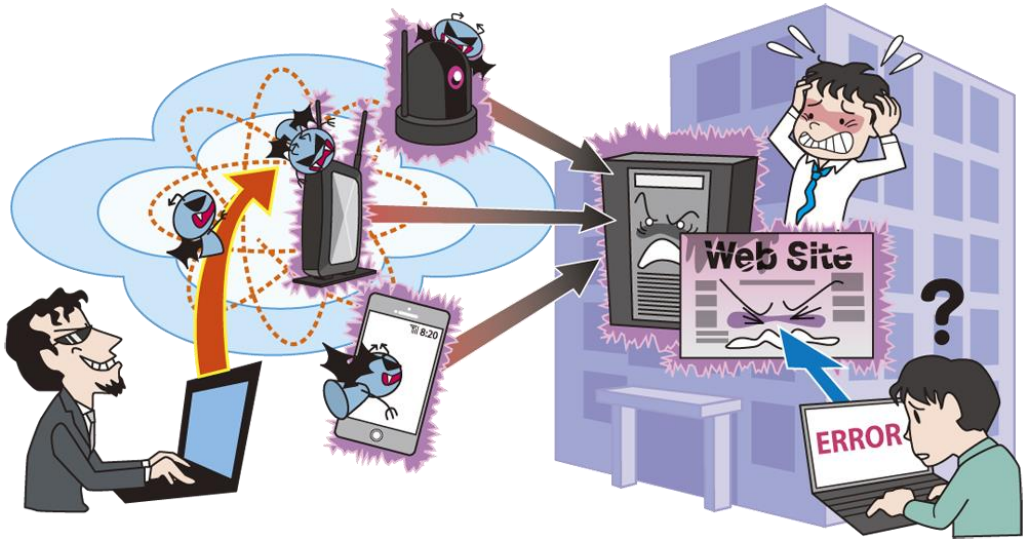
・内部不正者に対する適切な処罰実施

参考資料

1. 管理者パスワードを不正利用、人事資料閲覧で職員処分 - 八幡平市
http://www.security-next.com/092170
2. 元従業員が営業管理ツールで顧客情報を不正閲覧、営業利用 – システム開発会社
http://www.security-next.com/092510
3. 日経が元社員を告訴 社員3千人分の賃金データ漏洩容疑
https://www.asahi.com/articles/ASL735TGPL73UTIL047.html
4. 従業員がカード情報を盗み取りネット通販で不正利用（セキ薬品）
https://scan.netsecurity.ne.jp/article/2018/08/27/41320.html
5. 組織における不正防止ガイドライン
https://www.ipa.go.jp/security/fy24/reports/insider/

6位 サービス妨害攻撃によるサービスの停止

～国内外問わず大規模な DDoS 攻撃が発生～



攻撃者に乗っ取られた複数の機器から形成されるネットワーク（ボットネット）を踏み台とし、企業や組織が提供しているインターネットサービスに対して大量のアクセスを仕掛け高負荷状態にさせる DDoS（分散型サービス妨害）攻撃が確認されている。攻撃を受けた場合、自組織が管理するウェブサイト等からのレスポンスが遅延、または機能停止状態となり、サービス提供に支障が出るおそれがある。

＜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（インターネットサービスの運営者）
- 個人（インターネットサービスの利用者）

＜脅威と影響＞

多くの組織がインターネット上で、ウェブサイト等を運営し、情報の発信やサービスの提供を行っている。攻撃者はそうしたウェブサイトや組織で利用している DNS サーバーに対して、政治的な主張や金銭の恐喝等をするために大量の処理要求を送信している。

処理が追いつかなくなる程の処理要求を受けたウェブサイトや DNS サーバーは、閲覧ができなくなったり、レスポンスが遅延したりする等、サービスを正常に保つことができなくなるため、機会損失による損害が発生する。

＜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

  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標的組織が利用している DNS サーバーへ大量のアクセスを行い、高負荷をかける。

- リフレクター攻撃

  送信元の IP アドレスを標的組織のサーバーに偽装して、多数のルーターや DNS サーバー等に問い合わせを送り、応答結果を標的組織に送り付け、高負荷をかける。SNMP リフレクター攻撃や DNS リフレクター攻撃等がある。

- 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 サーバーに高負荷をかける。

- DDoS 代行サービスの利用

  ダークウェブ等にある DDoS 代行サービスを利用して DDoS 攻撃を行う。DDoS 攻撃のための専門的な技術や設備が無くても攻撃が行える。

＜事例または傾向＞

◆ **memcached による大規模な攻撃**

memcached と呼ばれるオープンソースのメモリキャッシュシステムが DDoS 攻撃の踏み台に利用され、最大 335 万 pps のパケットによる 33.08Gbps もの通信量が観測された。[1] この攻撃に関して、JPCERT/CC から注意喚起が公表されており、アクセスに用いる IP アドレスやポートを制限したり、memcached のバージョンをアップデートするよう勧告が行われた。[2]

◆ **DDoS 攻撃によるサービスの利用制限**

2018 年 10 月に、動画サイトである niconico において、サービスが利用できなくなったり、画面表示に時間が掛かる等の不具合が発生した。動画サイトの運営者は、システムに過剰な負荷を及ぼす異常な量の通信が観測されたことを受け、その通信を遮断すると、攻撃者は手段を変えて同事象を発生させる等して、執拗な DDoS 攻撃が行われていたことが分かっている。[3]

◆ **ルーターの脆弱性を突いたボットネット**

ルーターに存在する既知の脆弱性が悪用され、大規模なボットネットが構築されていたことが確認された。本件は Huawei のルーター「HG532」の脆弱性（CVE-2017-17215）を狙ったもので、2018 年 7 月 18 日に観測され、その日の内に 1 万 8 千台ものルーターがボットネットの一部として組み込まれたとされている。[4]

＜対策/対応＞

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 対策が提供されている場合はそれを利用する。
  - ・不要なサーバーやサービスへの外部からの適切なアクセス制限
  - ・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や告知手段の整備

    DDoS 攻撃を受けてサービスを停止させられることを想定して、サービス停止時の代替サーバーや、サービス停止によって利用者を混乱させないための告知用サーバーおよび SNS の公式アカウント等の連絡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（攻撃元 IP アドレスからの通信をブロック等）
  - ・利用者への状況の告知
  - ・影響調査および原因の追究、対策の強化

組織（IoT 機器ベンダー）

- 被害の予防
  - ・セキュリティ対策

    IoT 機器が不正アクセスやウイルス感染で乗っ取られ、ボットネットが形成される。ボットネットに組み込まれて攻撃の踏み台にされないために IoT 機器のセキュリティ対策を行う必要がある。[5]

参考資料

1. 2018年5月観測レポートサマリー
https://wizsafe.iij.ad.jp/2018/06/362/
2. memcached のアクセス制御に関する注意喚起
https://www.jpcert.or.jp/at/2018/at180009.html
3. 【解除済み】一部地域からの利用制限について
https://blog.nicovideo.jp/niconews/92066.html
4. ルーターの脆弱性を突くbotネットが相次ぐ、攻撃に加担させられる恐れも
http://www.itmedia.co.jp/enterprise/articles/1807/23/news054.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

7位 インターネットサービスからの個人情報の窃取

～インターネットサービスのセキュリティ対策の再確認を～

インターネットサービスの脆弱性が悪用され、インターネット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。攻撃者は窃取した情報を悪用して不審なメールを送信したり、クレジットカードを不正利用する。

＜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等）
- 組織（インターネットサービス運営者等）

＜脅威と影響＞

利用しているインターネットサービスには個人情報を含んだ情報が登録されている。例えば、ショッピングサイトであれば自身の個人情報やクレジットカード情報等の重要な情報が登録されている。

インターネット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脆弱性対策を適切に実施していない場合、脆弱性を内在したままサービス提供されている。

このようなインターネット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。

＜攻撃手口＞

◆ 開発時に作りこんだ Web アプリケーションの脆弱性を悪用

インターネットサービスを開発する際に Web アプリケーションのセキュリティ対策を十分に実施していない場合、脆弱性を作り込んでしまうことがある。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 SQL インジェクションの脆弱性を作り込んでしまうと、その脆弱性を悪用され、個人情報等の重要な情報を窃取される。

◆ ソフトウェアの脆弱性を悪用

インターネットサービスは 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、インターネット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多くのインターネットサービスを標的にされる。

＜事例または傾向＞

◆ **コンタクトレンズ会員サイトにて、OpenSSL の脆弱性により情報漏えい**

2018 年 5 月、コンタクトレンズ販売大手メニコンの子会社が運営するウェブサイトにおいて、最大 3,412 件のクレジットカード情報が漏えいし、不正利用による被害が生じたと発表した。

本件は、2014 年 4 月に公開された、「Heartbleed」と呼ばれる OpenSSL の脆弱性を悪用されたことが原因であった。[1]

◆ **がん治療認定医機構のサイトにて、SQL インジェクションの脆弱性により情報漏えい**

日本がん治療認定医機構において、がん治療認定医の変更届システムが不正アクセスを受け、認定医のメールアドレスやパスワード等、最大で 2 万名以上の情報が漏えいした。情報漏えいの原因は、委託先が運営する同システムに SQL インジェクションの脆弱性が存在し、それを悪用されたものと見られている。[2]

＜対策/対応＞

組織（インターネットサービス運営者等）

- 被害の予防
  - ・表 1.4「情報セキュリティ対策の基本」を実施
  - ・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。
  - ・セキュアなインターネットサービスの構築

    インターネット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（Web アプリケーション診断、プラットフォーム診断等）の実施

    システムの導入時やシステム改修時に実施する。また、改修がなくても定期的に診断の実施および改善を行う。
  - ・WAF、IPS の導入

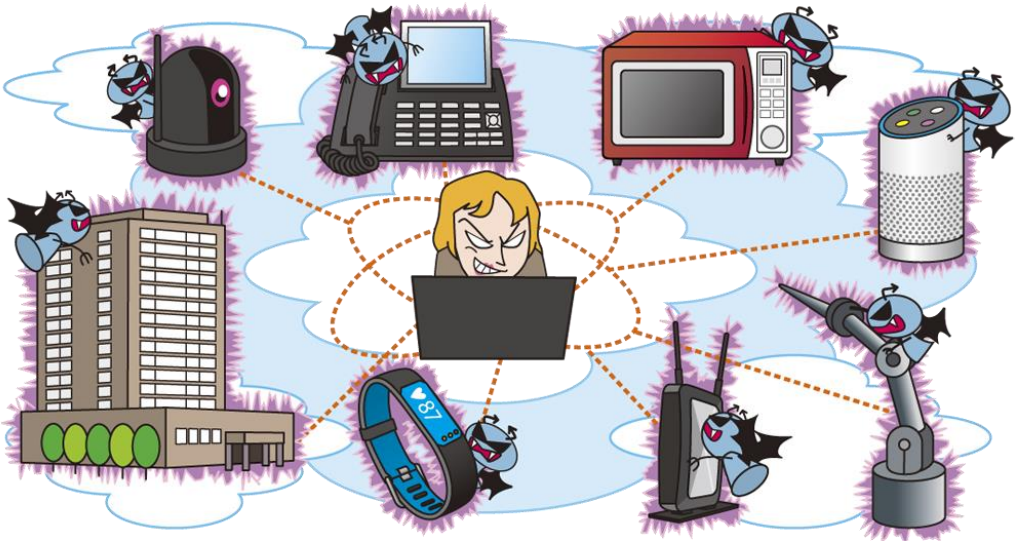
    導入後も、対策情報（設定等）を定期的に更新する保守作業があることを想定すること。また、ただ導入するだけではなく、アラートのハンドリングなど適切な運用が重要である。運用体制の構築や外部サービスの利用等も検討する。
- 被害の早期検知
  - ・適切なログの取得と継続的な監視
- 被害を受けた後の対応
  - ・CSIRT への連絡
  - ・影響調査および原因の追究、対策の強化
  - ・漏えいした情報に対する利用者への補償

参考資料

1. Webサイトの脆弱性を4年前から放置か、メニコン情報漏洩の原因
https://tech.nikkeibp.co.jp/atcl/nxt/column/18/00001/00561/
2. 不正アクセスで認定医情報が流出か - 日本がん治療認定医機構
http://www.security-next.com/091799
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/index.php/Pentester_Skillmap_Project_JP
5. セキュア・プログラミング講座
https://www.ipa.go.jp/files/000059838.pdf

8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増加、開発ベンダーは対策が急務～



IoT 機器をウイルスに感染させ、その IoT 機器を踏み台として大規模な DDoS（分散型サービス妨害）攻撃を行い、サービスやネットワーク、サーバーに悪影響を与える被害が確認されている。IoT 機器は稼働台数が多く、脆弱性対策も浸透していないことからサイバー攻撃の対象になりやすい。IoT 機器を狙ったサイバー攻撃は年々増加傾向で深刻な被害も発生しており、早急なセキュリティ対策が必要となっている。

＜攻撃者＞

- 犯罪グループ
- 犯罪者（産業スパイ、愉快犯、離職者等）
- 他国家（諜報員等）

＜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＞

情報家電、オフィス機器、医療機器、産業用設備・機器、制御システム等の様々な分野の製品が、インターネットに接続して利用できるようになってきた。一方、IoT 機器のリスク検討が不十分のまま製品が開発され、脆弱性を作り込んでしまっている。かつてはインターネット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、攻撃者がインターネット越しにその脆弱性を悪用されている。

脆弱性を悪用されると、IoT 機器がウイルスに感染させられ、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、不正操作により、IoT 機器の設定を変更されると業務に影響が出る場合もある。

一方、IoT 機器の利用者も「IoT 機器はインターネットにつながっている」という意識が薄く、パッチの適用等の IoT 機器の脆弱性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＞

◆ 脆弱性を悪用した攻撃

脆弱性を悪用して、インターネット経由で IoT 機器に不正アクセスしたり、ウイルスに感染させる。IoT 機器が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、サーバー等に 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。

◆ ウイルスの感染を拡大させる

ウイルスに感染した IoT 機器は、同じ脆弱性を持つ IoT 機器がインターネット上にないかを探索する。存在した場合、その IoT 機器もウイルスに感染させ、次々と感染範囲を拡大させる。

＜事例または傾向＞

◆ **河川監視カメラへ不正アクセス**

芝川都市下水路鎌倉橋に河川監視カメラを 1 台設置し水位状況を河川課監視カメラホームページで公開していたが、このカメラへの不正アクセスが判明したと発表した。4 月 26 日 17 時頃、第三者がインターネット回線を通じて芝川都市下水路鎌倉橋に設置した河川監視カメラに不正アクセスし、画像に日付と「I'm hacked.bye2」の文字を表示するように不正に操作されていた。河川監視カメラへの外部からのアクセスにはパスワード等を設定していたが、さらに侵入者によりパスワード等が変更されたため、同局から河川監視カメラの制御ができなくなった。[1]

◆ **ルーターに侵入し DNS 設定を書き換え、不正サイトに誘導**

2018 年 3 月頃、インターネット上のルーターの DNS 設定を不正に書き換え、当該ルーター経由でウェブサイトに接続しようとする PC やスマートフォンを不正サイトへと誘導する攻撃が日本国内で相次いで発生した。[2] 誘導された不正サイトでは「Facebook 拡張ツールバックを取付て安全性及び使用流暢性を向上します」と、有名なアプリの機能向上を装ったメッセージが出る。メッセージに従うと不正アプリがダウンロードされる。情報通信研究機構（NICT）によれば、当該不正アプリをインストールすると、Google を装った警告が表示され、個人情報を入力させようとする。[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

    利用者へ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

    利用者にソフトウェアサポートの期間を伝え、サポートが切れた状態での利用について注意を促す。

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

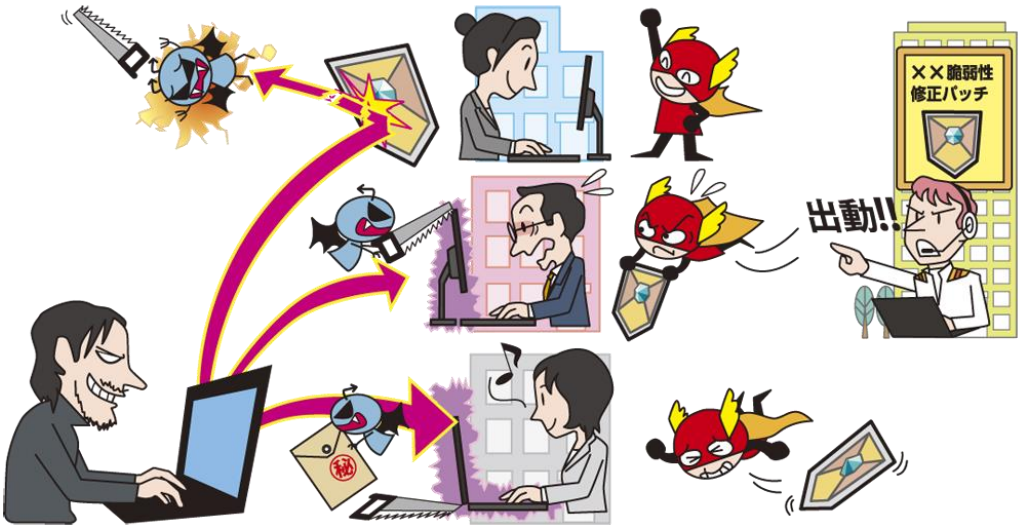
    廃棄時は初期化し廃棄業者等に出す場合、データ消去や秘密保持に関する契約をする。
  - ・機器の管理画面や管理ポートに対する適切なアクセス制限
- 被害を受けた後の対応
  - ・CSIRT への連絡
  - ・IoT 機器の電源オフ
  - ・IoT 機器の初期化後、「被害の予防」を実施
  - ・影響調査および原因の追究、対策の強化

参考資料

1. 河川監視カメラへ不正アクセス、「I'm hacked.bye2」のメッセージ残す
https://scan.netsecurity.ne.jp/article/2018/05/01/40886.html
2. ルーターの設定書き換え、不正アプリに感染させる攻撃　被害相次ぐ
http://www.itmedia.co.jp/news/articles/1803/30/news106.html
3. Wi-Fi ルータの DNS 情報の書換え後に発生する事象について
https://blog.nicter.jp/reports/2018-02/router-dns-hack/
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

9位 脆弱性対策情報の公開に伴う悪用増加

～脆弱性対策はスピード勝負、迅速かつ適切な対応を～



ソフトウェア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、当該ソフトウェアに対する脆弱性対策を行っていないシステムを狙った攻撃が行われている。近年では脆弱性情報の公開後、攻撃コードが流通し、攻撃が本格化するまでの時間が短くなっている。

＜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、ソフトウェアに脆弱性が発見された場合、当該ソフトウェア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ことで、情報漏えいや改ざん、ウイルス感染等の被害の発生が確認されている。特に、Apache Struts2 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の場合、攻撃コード等が公開されると被害が大きくなるおそれがある。

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短くなっており、より迅速な対応が求められる。

＜攻撃手口＞

◆ **対策前の脆弱性を悪用**

ソフトウェアの利用者が脆弱性対策のパッチを適用する前にその脆弱性を悪用する。利用者が多いソフトウェアの場合、同じ手口が使えるため攻撃が拡大するおそれがある。

＜事例または傾向＞

◆ **Apache Struts2 の脆弱性を悪用したコインマイナー**

2018 年 8 月 22 日に、Apache Struts2 のリモートでコードを実行されるおそれのある脆弱性（CVE-2018-11776）が公表された。この数日後に脆弱性を悪用する攻撃コードが公開されると、約 2 週間後には仮想通貨のマイニングを行うマルウェアに感染させようとする攻撃が観測された。また、

アンダーグラウンドでの攻撃キャンペーンの標的となり、この脆弱性を含むウェブサイトのリストが流通していたことも確認されている。[1,2]

◆ **Drupal の脆弱性の攻撃コードの公開に伴う攻撃の増加**

2018 年 3 月 28 日に公表された Drupal の脆弱性は、公表の直後には脆弱性を悪用しようとする動きは見られなかったが、4 月 12 日に攻撃コードが公開されると、この脆弱性を狙ったと見られるアクセスが国内だけでも数万件規模で観測された。攻撃の内容としては、コインマイナーのダウンロードや、バックドアの設置等が確認されている。[3,4]

＜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
  - ・表 1.4「情報セキュリティ対策の基本」を実施
  - ・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事前に検証する必要がある。そのため、検証するための体制や環境も準備する必要がある。
  - ・脆弱性関連情報の収集
  - ・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

    ネットワーク経由で脆弱性を悪用する攻撃がないか監視する。攻撃の疑いがある場合は、ファイアウォール等により通信を遮断する。
  - ・セキュリティのサポートが充実しているソフトウェア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たものを選択する。
  - ・一時的なサーバー停止等

    すぐにパッチが適用できない場合、一時的にサーバー停止等を実施して、攻撃を回避する対策を取ることも検討する。サーバー停止等に伴うサービス停止の影響については事前に検討をしておく。また、速やかにサービス利用者への通知を行う。
- 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、対策の強化

組織（開発ベンダー）

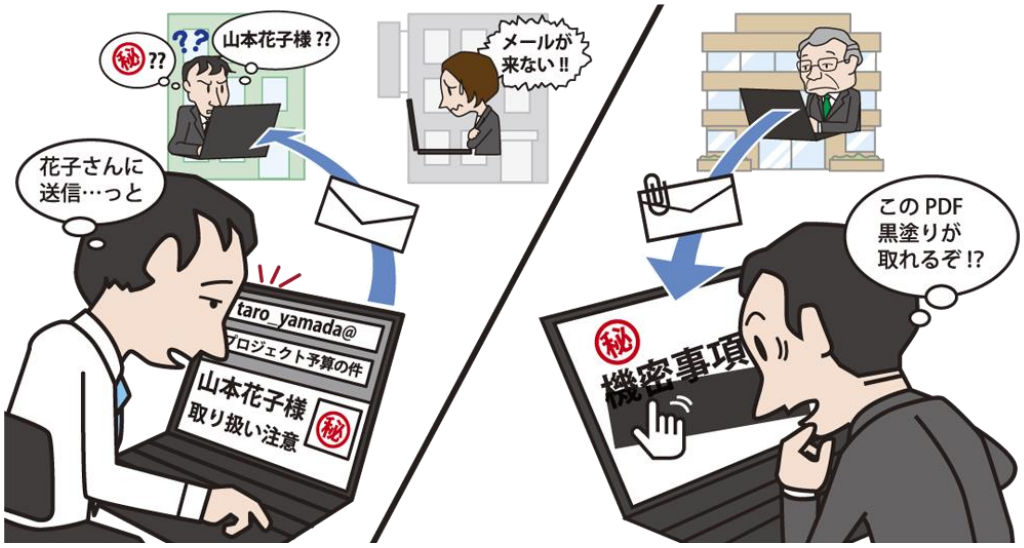
- 製品セキュリティの管理、対応体制の整備
  - ・製品に組み込まれているソフトウェアの把握、管理の徹底
  - ・脆弱性関連情報の収集
  - ・脆弱性発見時の対応手順の作成
  - ・情報を迅速に発信できる仕組みの整備

参考資料

1. 「Apache Struts 2」の脆弱性、仮想通貨採掘攻撃に悪用される
http://www.itmedia.co.jp/enterprise/articles/1809/06/news066.html
2. 「Struts 2」脆弱性を狙う攻撃キャンペーン「Bleeding Thunder」 - 国内企業のサイト含む標的リストも
http://www.security-next.com/097318
3. 「Drupal」脆弱性、国内で1日あたり数万件規模のアクセス - 70カ国以上から
http://www.security-next.com/092540
4. 国内でも「Drupalgeddon 2.0」を観測 - 「Drupal」利用者はアップデート状況の確認を
http://www.security-next.com/092467

10位 不注意による情報漏えい

～一度の過失が組織の信用を大きく脅かす～



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

＜当事者（情報を漏えいさせた側）＞

- 組織（従業員）

＜被害者（情報を漏えいされた側）＞

- 個人（当事者のサービス利用者等）
- 組織（当事者の取引先企業等）
- 組織（当事者自身）

＜脅威と影響＞

組織や企業がサービスを提供していく上で、サービス内容や担当業務によっては個人情報や機密情報を取り扱うことがある。これら重要情報を取り扱うことに対する意識の低さから、従業員の不注意等によって、意図せず機密情報を漏えいする事件が発生している。

情報漏えいによる影響は、社会的信用の失墜やそれに伴う経済的損失が発生するだけでなく、漏えいした情報が悪用され、二次被害が発生することもある。

＜要因＞

◆　取り扱う情報の重要性に対する認識不足

個人情報や機密情報を取り扱う際に、その情報に対する重要性の認識不足から不用意に取り扱って情報漏えいしてしまう。例えば、重要情報をカバンに入れて持ち出し、そのカバンを外出先で紛失したり、宛先等を十分に確認しないまま個人情報等を含むメールを誤送信する。

◆　情報を取り扱う際の本人の状況

重要情報を取り扱う際の本人を取り巻く状況から不用意な対応を取り、情報漏えいにつながる。例えば、体調不良や急ぎの用事がある等により、注意が散漫になり、メールの誤送信等をしてしまう。

◆　組織規程および確認プロセスの不備

重要情報の定義・取り扱い規程・持ち出し許可手順や、作業時の確認プロセスに不備がある環境で業務を行うことがある。このような環境で重要情報を取り扱うことにより、情報漏えいを起こす。

＜不注意による情報漏えい例＞

- メールの誤送信（宛先間違え、TO/CC/BCC の設定間違え、添付ファイル間違え等）
- 不適切なウェブ公開
  （重要情報への対処が不十分なまま公開）
- 重要情報を保存した情報端末（PC やスマートフォン等）・記録媒体（USB メモリー等）の紛失
- 重要書類（紙媒体）の紛失

＜事例または傾向＞

◆　**取材音声データ等の情報をメールで誤送信**

2018 年 11 月 1 日、NHK のディレクターが、宗教団体「アレフ」に関する住民インタビュー音声ファイルのダウンロード先情報を含むメールを、誤って宗教団体側に送信した。

また、同月 9 日から 10 日にかけて、業務委託先のディレクターが、放送素材を入手できる情報を含むメールを第三者に誤送信した。

これらメールの誤送信が立て続けに発生したことに対して、NHK は同月 21 日に謝罪文を掲載し、以下 3 点の再発防止策を掲げると共に、情報管理の厳格化に努めていくとしている。[1]

1.再発防止のためのルールの強化と徹底

2.誤送信を防ぐシステムの改修

3.放送倫理とITリテラシーの再教育等の徹底

◆　**「墨塗り」が不適切な PDF を公開**

財務省は 2018 年 5 月 23 日に公開した PDF ファイルの「墨塗り（マスキング処理）」が適切に行われておらず、一定の操作により情報を閲覧可能であったことを同月 24 日に公表した。また、問題のあった PDF ファイルは同月 23 日に適切な「墨消し」が行われたものに差し替えられた。

なお、同様の「墨塗り」の不備が大阪市や法務省等、複数の組織において発生しており、「墨塗り」の正しいやり方が各組織で徹底されておらず、誤ったやり方による同様の事案を招いていることが問題となっている。[2]

◆　**業務用端末等の紛失**

東京ガスは、2018 年 12 月 19 日に業務委託先企業の作業員が、住所や氏名など 421 世帯分の顧客情報を記録した業務用携帯端末と制服を紛失したことを同月 21 日に公表した。その後、同月 25 日に紛失物を無事発見したことを公表している。[3,4]

なお、紛失した業務用携帯端末には、セキュリティ対策を施しており、発見後の調査で端末に記録された情報の閲覧やダウンロードなど外部への流出が発生していないことを確認したとしている。

＜対策/対応＞

組織（当事者）

- 情報リテラシーや情報モラルの向上
  - ・従業員のセキュリティ意識教育
  - ・組織規程および確認プロセスの確立
    特定の担当者への業務集中が発生しないような体制の構築も重要である。
- 被害の予防（被害に備えた対策含む）
  - ・確認プロセスに基づく運用
  - ・情報の保護（暗号化、認証）
  - ・外部に持ち出す情報や端末の制限
  - ・業務用携帯端末の紛失対策機能の有効化
- 被害の早期検知
  - ・問題発生時の内部報告体制の整備
  - ・外部からの連絡窓口の設置
- 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、対策の強化
  - ・被害拡大や二次被害要因の排除
    ウェブサイトへの誤った情報公開の場合、非公開にする等。
  - ・漏えいした内容や発生原因の公表

個人/組織（被害者）

- 被害を受けた後の対応
  - ・漏えいが発生した組織からの情報に従う
    パスワードの変更
    クレジットカード情報の変更等

参考資料

1. 取材データの誤送信で職員8人を懲戒処分 - NHK
http://www.security-next.com/100289
2. 森友文書でも発生、墨塗りPDFから漏洩　間違った対策
https://www.nikkei.com/article/DGXMZO31095690Z20C18A5000000/
3. お客さま情報が入った業務用携帯端末および制服の紛失について
https://www.tokyo-gas.co.jp/important/20181221-02.pdf
4. 紛失したお客さま情報が入った業務用携帯端末および制服の発見について
https://www.tokyo-gas.co.jp/important/20181225-01.pdf

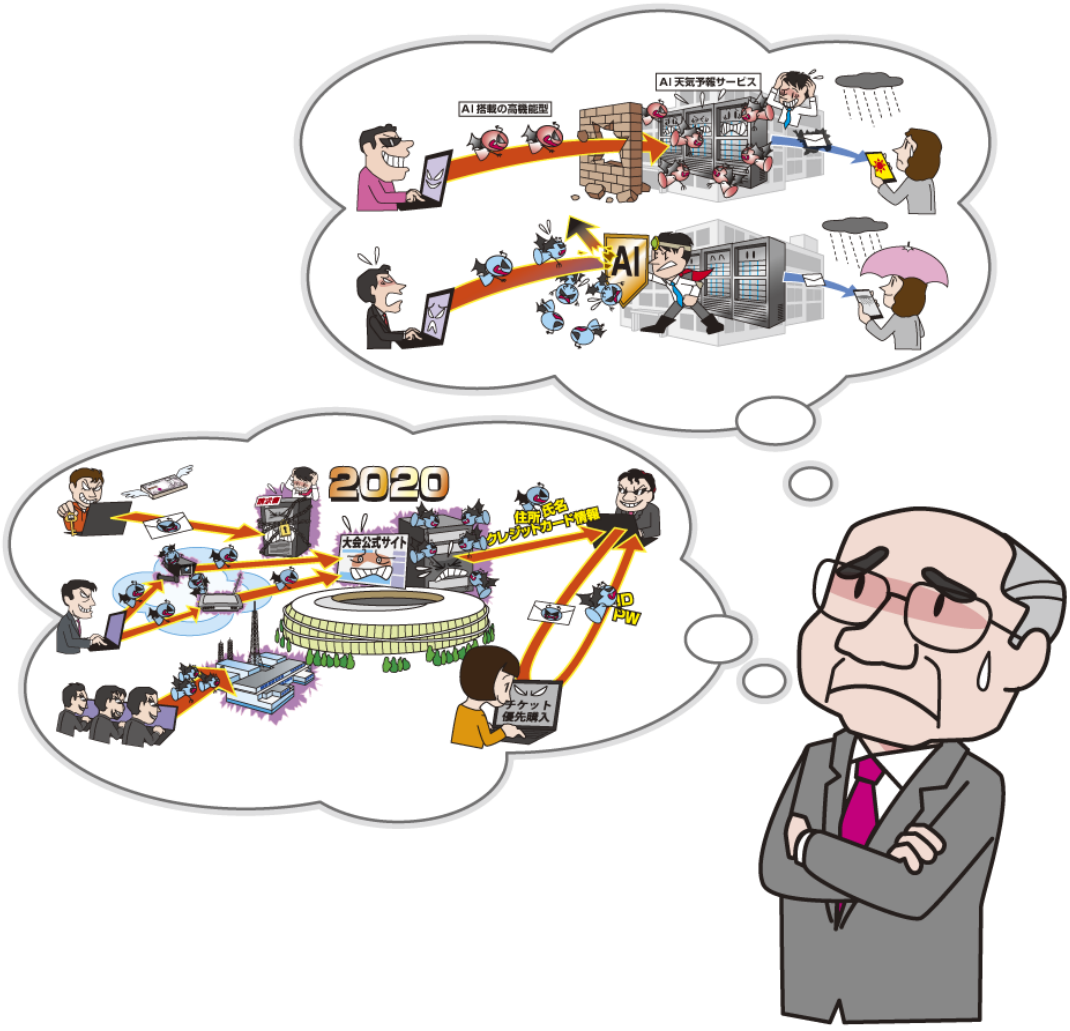
3章. 注目すべき脅威や懸念

3 章 注目すべき脅威や懸念

本章では、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。

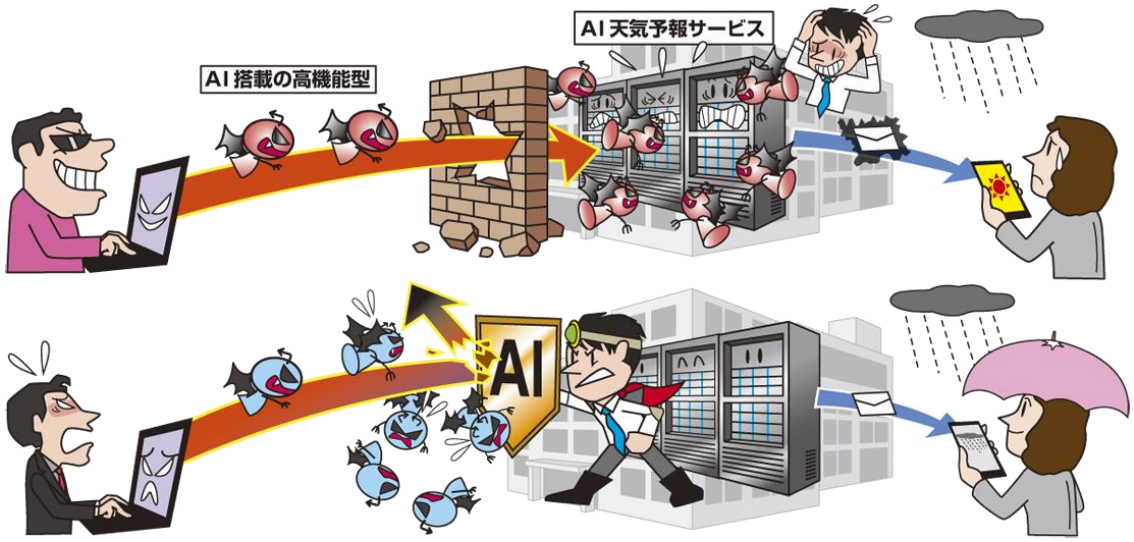
表 3.1：注目すべき脅威や懸念

番号	タイトル
1	**AI 技術を巡るサイバー攻撃の攻防 ～AI を用いたサイバー攻撃 vs AI を用いたサイバー攻撃対策～**
2	**東京五輪に向けたサイバー攻撃の備え ～過去の事例に学び、「10 大脅威」を読んで対策の再確認を～**



3.1. AI 技術を巡るサイバー攻撃の攻防

～AI を用いたサイバー攻撃 vs AI を用いたサイバー攻撃対策～



近年、情報技術を含む様々な産業分野において、AI（人工知能）技術の活用が注目を集めている。サイバーセキュリティの分野においても、AI 技術を用いた新たなサイバー攻撃対策技術が開発・提供されている。一方で、AI 技術やそれを利用しているシステムに対するサイバー攻撃や、AI 技術を用いた新たなサイバー攻撃手法が出現する等、AI 技術はサイバー攻撃者にとっての攻撃対象や悪用可能な技術となっている。本節では、AI 技術を用いたサイバー攻撃の攻防や AI 技術に対する攻撃の動向、今後の予測について概説する。

＜AI 技術を用いたサイバー攻撃対策＞

高度化、巧妙化するサイバー攻撃に対する防衛手段の一つとして、未知の攻撃手法による脅威を検知するため、近年、AI 技術を用いたサイバー攻撃対策製品やサービスが開発・提供されている。これらの多くは、機械学習による、未知の攻撃を脅威として検出する能力を備えたものである。

機械学習は、AI の基盤技術の一つであり、人間の学習能力と同様に、経験からの学習による予測を可能とする。具体的には、一定量のデータを分析し、規則性や法則を抽出することによって、計算機やネットワーク機器に未知の経験に関する予測や判断能力を与えることである。これらの技術を用いて、以下に示す様に、未知の攻撃手法を含む様々な攻撃に対抗する機能を持つ製品やサービスが存在する。[1]

- 未知のウイルスの検知
- 未知の脅威・攻撃の検知・解析
- 悪意のあるファイルや URL の検知
- 迷惑メールのフィルタリング
- 脆弱性の網羅的な検知

上記以外にも、既知のウイルス検知を効率化するために、AI 技術を用いてパターンファイル（シグネチャ）の自動生成を行う製品等も存在している。[2]

企業においてサイバー攻撃対策を検討する上での選択肢が拡大しているだけでなく、個人向けのセキュリティソフト等においても、AI 技術が活用される様になってきている。

＜AI 技術を用いた攻撃対策の回避＞

これに対して、攻撃者は AI 技術を用いたサイバー攻撃対策の仕組みを解析し、防御側の検知を回避する攻撃方法を編み出している。具体的には、以下の様な方法が発見されている。[3]

- 一般的でない拡張子を持つファイルの利用
- ファイルレス攻撃（ウイルスの実ファイルを生成せず、スクリプトのリモート実行や攻撃コードのレジストリへの保存）
- 電子署名されたウイルスの利用
- 正規のメールアカウントやオンラインストレージサービス、アプリの悪用

＜AI 技術を用いたサイバー攻撃＞

AI 技術がサイバー攻撃からの防御に活用されている反面、攻撃者による AI 技術を悪用したサイバー攻撃（例えば、SNS のデータの自動収集と採取したデータからのフィッシング攻撃作成）も試みられている。[4] 今後は、ユーザーからの質問に AI 技術を用いて自動応答するサポート詐欺や、標的型攻撃の対象企業や対象者の挙動を AI 技術の活用によって予想した攻撃等、AI 技術を用いた新たなサイバー攻撃の発生も考えられる。

＜AI 技術に対するサイバー攻撃＞

サイバー攻撃の攻防とは無関係な領域で利用されている AI 技術についても、サイバー攻撃の対象となり得る。AI 技術を実装したサーバーやクライアント、それらを用いて実現しているサービスに対して、一般的な IT システムと同様のサイバー攻撃が想定される。加えて、収集したデータを分析して機械学習を行う AI 技術に特有の脅威として、以下に示す様な方法で規則性や法則を汚染して、AI を用いた予測や判断能力を低下させる攻撃が存在する。[5]

- 収集中のデータの汚染
  規則性や法則を抽出するため収集中のデータの中に、故意に誤った情報を混入させることで、誤った規則性や法則を抽出させる。
- 収集・分析済みデータの改ざん
  規則性や法則を抽出した収集・分析済みデータや得られた規則性や法則を改ざんする。

＜今後の教訓＞

AI 技術を巡るサイバー攻撃の攻防の動向から、以下の様な教訓が得られる。

「最新の動向把握の重要性」

AI 技術により、サイバー攻撃対策の技術が進化すると共に、攻撃者のサイバー攻撃技術も進化する。攻める側と守る側のいたちごっこは、今後も継続していくと考えられる。サイバー攻撃対策に従事する者は、最新の技術動向を常に収集・把握し続けることが重要である。

「多層防御の有効性」

最新技術を用いた新たなサイバー攻撃対策技術が開発されたとしても、その対策が攻撃の 100%を防御できるとは限らない。そこを突破された場合に大きな被害につながる箇所においては、複数の対策を実装した多層防御によってシステムを守ることが有効である。

「AI 技術におけるデータ防御の重要性」

AI 技術が取り扱うデータの正当性は、結果として得られる予測や判断の正しさに直結するので、一般的なサイバー攻撃により想定される脅威（改ざんや漏えい）のセキュリティ対策を実施すると共に、収集するデータの正当性を確認することが不可欠である。

「新規ビジネスに不可欠なセキュリティ対策」

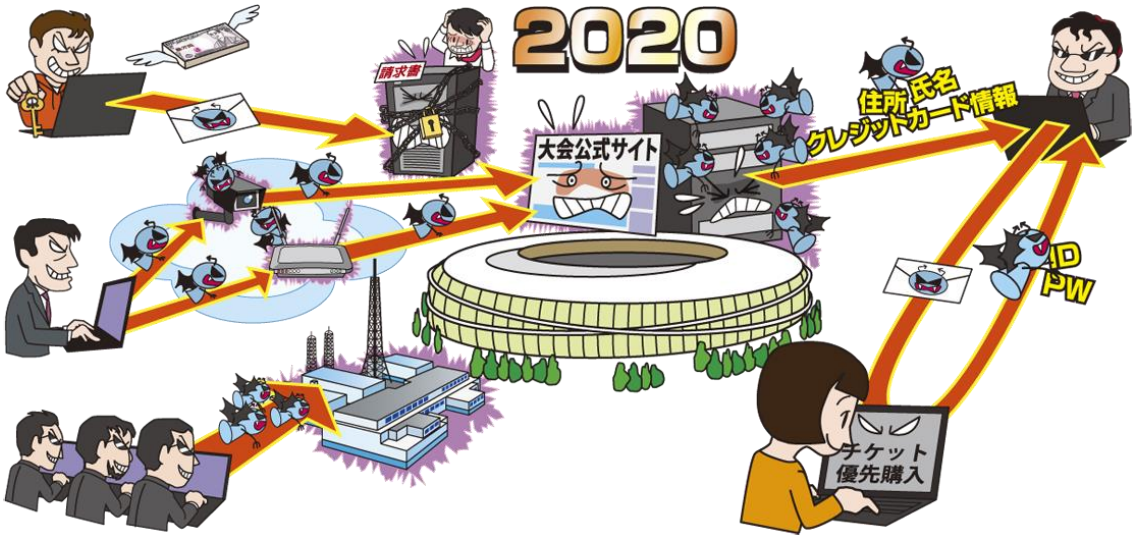
技術開発により提供される新しいビジネスは、注目が集まると共に、サイバー攻撃者によるターゲットとなる確率も高まっていく。AI 技術を用いた新規ビジネスを提供する際は、悪意を持った攻撃者が存在することを前提として、攻撃者の視点を考慮して脅威を分析・検討し、十分なセキュリティ対策を実施した上でサービス開始することが望ましい。

参考資料

1. AIで複雑化するサイバー攻撃、対抗できるのもまたAIか、それとも人か
https://www.atmarkit.co.jp/ait/articles/1708/16/news012.html
2. 自動化が進むサイバー攻撃とAIを使った防御側の対応--フォーティネットが説明
https://japan.zdnet.com/article/35116169/
3. 2019年はAI悪用のサイバー攻撃が登場--トレンドマイクロ予測
https://japan.zdnet.com/article/35130285/
4. AIを使ったサイバー攻撃はもう時間の問題――マカフィーが警告
https://www.itmedia.co.jp/enterprise/articles/1710/13/news042.html
5. 人工知能の敵とは？ SECCON実行委員の園田道夫教授らが人工知能のセキュリティについて議論
https://internet.watch.impress.co.jp/docs/event/1004668.html

3.2. 東京五輪に向けたサイバー攻撃の備え

～過去の事例に学び、「10 大脅威」を読んで対策の再確認を～



2020 年東京五輪（オリンピック・パラリンピック）の開催まで約 1 年となった。2012 年ロンドン、2016 年リオデジャネイロ等で開催された過去大会においても、五輪を狙ったサイバー攻撃が発生し、関係者は対策や対処に追われた。東京五輪に向けて、関係団体・組織・企業は、サイバー攻撃対策の強化を進めている。本節では、五輪を機に規模が拡大されると予想される既知のサイバー攻撃、新しい手法による攻撃の備え等、東京五輪の開催国の組織や個人として考えるべき点について、おさらいする。

＜過去の事例＞

2012 年ロンドン五輪 [1]、2016 年リオ五輪 [2]、2018 年平昌（冬季）五輪において、大会関係組織、開催国の政府機関や自治体、大会準備に携わった関係者、国民等に対して、例えば以下に示す様なサイバー攻撃が確認された。

- 公式及び関連ウェブサイトへの DDoS 攻撃
- 偽ウェブサイトの設置
- フィッシング詐欺メール
- ウェブサイトからの情報窃取
- 電力供給の監視制御システムへの攻撃
- メディアプレスセンター等への破壊攻撃

東京五輪に対しても、これまでと同等あるいはそれ以上のサイバー攻撃が予想される。

＜脅威の概要とその対策＞

予想されるサイバー攻撃の多くについては、「情報セキュリティ 10 大脅威 2019」の 2 章で解説している脅威とその対策に該当する。ここでは、脅威の概要と 2 章の解説の対応箇所への参照を示す。

◆ 公式及び関連ウェブサイトへの DDoS 攻撃

五輪に関連するウェブサイトを DDoS 攻撃によって利用不能とし、運営を妨害する。設定不備や脆弱性を放置した IoT 機器が乗っ取られ、攻撃の踏み台に悪用されることが考えられる。

【DDoS 攻撃を受ける側の対策】

☞ **組織 6 位「サービス妨害攻撃によるサービスの停止」**

【DDoS 攻撃の踏み台にされる側の対策】

☞ **個人 10 位「IoT 機器の不適切な管理」**

☞ **組織 8 位「IoT 機器の脆弱性の顕在化」**

◆ 偽ウェブサイトの設置

チケット販売詐欺やフィッシング等を目的とした、偽ウェブサイトを設置し、個人のクレジットカード情報等を窃取する。

☞ **個人 1 位「クレジットカード情報の不正利用」**

☞ **個人 2 位「フィッシングによる個人情報等の詐欺」**

◆ フィッシング詐欺メール

チケット、宿泊施設、関連商品等を餌にしたフィッシング詐欺メールを送信し、前述の偽ウェブサイトへの誘導やクレジットカード情報の窃取、個人の認証

情報の窃取、それらを悪用した次なる攻撃等を試みる。

- ☞ **個人 1 位「クレジットカード情報の不正利用」**
- ☞ **個人 2 位「フィッシングによる個人情報等の詐欺」**

◆ ウェブサイトからの情報窃取

ウェブサイトのサーバーやウェブアプリケーションを攻撃し、そこにある機密情報（大会出場選手や登録利用者の個人情報等）を窃取する。

- ☞ **組織 7 位「インターネットサービスからの個人情報の窃取」**

◆ 電力供給の監視制御システムへの攻撃
（重要インフラを担う制御システムへの攻撃）

ロンドン五輪では、電力供給を行うための監視制御システムへの攻撃によって停電を発生させて、大会の運営を妨害しようとする動きが見受けられた。電力に限らず、運営に関わる重要インフラの制御システムがサイバー攻撃を受けるおそれがある。

- ☞ **『制御システム利用者のための脆弱性対応ガイド 第 3 版』**[3] を参照

◆ メディアプレスセンター等への破壊攻撃

平昌（冬季）五輪では、開会式当日、メディアプレスセンターの IPTV システムや組織委員会内部のインターネットや Wi-Fi 等が使用不能になった。情報窃取に加えて、システム破壊機能を持ったウイルスが用いられたと報告されており、「破壊を目的としたウイルス感染」を想定脅威の一つとして捉える必要がある。

- ☞ **組織 1 位「標的型攻撃による被害」**

＜その他、考えられる脅威と対策＞

近年の攻撃傾向から、東京五輪を機会として、他のサイバー攻撃の増加も警戒する必要がある。

◆ ランサムウェア

大会の運営に関わるウェブサイトやサーバーをランサムウェアで使用不能とし、早期復旧せざるを得ない被害者から金銭を脅し取る。個人の PC やスマートフォンの感染も要警戒である。

- ☞ **個人 9 位「ランサムウェアによる被害」**
- ☞ **組織 3 位「ランサムウェアによる被害」**

◆ 関連組織への攻撃増加

リオ五輪では、大会開催後、攻撃対象ウェブサイトは、大会関連→政府関連→準備に携わった事業者関連と、徐々に周辺へと推移した。東京五輪では、先ずセキュリティ対策が不十分な周辺の関係者を攻撃して侵入し、そこから最終的な攻撃対象へと迫っていく攻撃が試みられるおそれがあり、サプライチェーンを含めた対策強化が必要である。

- ☞ **組織 4 位「サプライチェーンの弱点を悪用した攻撃の高まり」**

◆ 嘘情報の発信・拡散による混乱

何者かが発信した嘘情報（フェイクニュース等）が SNS 等のネットワーク上で拡散することで混乱が発生し、大きな被害を生じるおそれがある。ネットワーク上で流通している情報を取得した際は、落ち着いて情報源を確認し、不確定情報を拡散しないことが大切である。

- ☞ **個人 5 位「ネット上の誹謗・中傷・デマ」**

◆ 新しい手法による攻撃

これまで観測されていない、全く新しい攻撃が試みられるおそれがある。脆弱性を放置すると、容易に攻撃される。組織・個人のサーバー、PC、スマートフォン、IoT 機器等のソフトウェアを最新に保ち、脆弱性を狙った攻撃を回避する必要がある。

- ☞ **組織 9 位「脆弱性対策情報の公開に伴う悪用増加」**

＜まとめ＞

東京五輪を機会として、組織も個人も、自らのサイバーセキュリティ対策を見直す契機としたい。

参考資料

1. オリバー・ホーア氏 講演録「2012年ロンドンオリンピックのセキュリティ ～我々の経験をご紹介～」
https://www.ipa.go.jp/files/000039004.pdf
2. リオオリンピックから見たサイバー攻撃（IPAサイバーセキュリティシンポジウム2017：講演資料）
https://www.ipa.go.jp/files/000057712.pdf
3. 制御システム利用者のための脆弱性対応ガイド ～重要な経営課題となる制御システムのセキュリティリスク～
https://www.ipa.go.jp/files/000058489.pdf

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	田中 博和	(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	東 恵寿	(一社)セキュリティ対策推進協議会
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)
佐藤 直之	SCSK(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
鈴木 寛明	SCSK(株)	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
保村 啓太	SCSK(株)	辻 伸弘	ソフトバンク・テクノロジー(株)
大塚 淳平	NRI セキュアテクノロジーズ(株)	楢原 盛史	タニウム合同会社
小林 克巳	NRI セキュアテクノロジーズ(株)	金城 賀真	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)
小林 義徳	(株)NTT データ	前田 隆行	DXC テクノロジー・ジャパン(株)
宮本 久仁男	(株)NTT データ	森 槙悟	(株)ディー・エヌ・エー
池田 和生	NTTデータ先端技術(株)	松本 隆	(株)ディー・エヌ・エー
植草 祐則	NTTデータ先端技術(株)	桑原 和也	デジタルアーツ(株)
徳毛 博幸	エムオーテックス(株)	内山 巧	(株)電算
間嶋 英之	エムオーテックス(株)	田岡 聡	(株)東芝
楯 研人	エムオーテックス(株)	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	小島 健司	東芝デジタルソリューションズ(株)
岡村 浩成	京セラコミュニケーションシステム(株)	大山 水帆	戸田市役所
小関 直樹	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)
西井 晃	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)
遠藤 誠	(株)ケイテック	加藤 雅彦	長崎県立大学
岩城 尚志	KDDI デジタルセキュリティ(株)	須川 賢洋	新潟大学
村上 正太郎	KDDI デジタルセキュリティ(株)	猪股 秀樹	日本アイ・ビー・エム(株)
小熊 慶一郎	(株)KBIZ / (ISC)2	坂 明	(一財)日本サイバー犯罪対策センター
三木 剛	(株)神戸デジタル・ラボ	磯田 弘司	日本電気(株)
宮﨑 清隆	国際マネジメントシステム認証機構(株)	谷川 哲司	日本電気(株)
福森 大喜	(株)サイバーディフェンス研究所	淵上 真一	日本電気(株)
中嶋 美貴	サイバーリーズン・ジャパン(株)	住本 順一	日本電信電話(株)
岩井 博樹	(株)サイント	山本 築	日本マイクロソフト(株)
奥石 隆	(一社)JPCERT コーディネーションセンター	金 明寛	(株)ネクストジェン
福本 郁哉	(一社)JPCERT コーディネーションセンター	武田 智宏	(株)ネクストジェン
齊藤 和男	(株)ジェイピー・セキュア	渡辺 久晃	パナソニック(株)
古谷 尋	(株)シマンテック	林 薫	パロアルトネットワークス(株)
山内 正	(株)シマンテック	岩佐 功	東日本電信電話(株)
大久保 隆夫	情報セキュリティ大学院大学	水越 一郎	東日本電信電話(株)
阿部 実洋	(株)スプラウト	折田 彰	(株)日立システムズ

氏名	所属	氏名	所属
本川 祐治	(株)日立システムズ	小屋 晋吾	(株)豆蔵ホールディングス
寺田 真敏	(株)日立製作所	小河 哲之	三井物産セキュアディレクション(株)
藤原 将志	(株)日立製作所	高江洲 勲	三井物産セキュアディレクション(株)
古賀 洋一郎	ビッグローブ(株)	平田 真由美	みゅーらぼ
上村 理	ファイア・アイ(株)	東内 裕二	(株)メルカリ
會澤 篤志	(株)ファイブドライブ	白橋 朋弥	(株)ユービーセキュア
大高 利夫	藤沢市役所	関根 鉄平	(株)ユービーセキュア
原 和宏	富士通(株)	本間 知生	(株)ユービーセキュア
原田 弘和	富士通(株)	島田 理枝	(株)ユビテック
福田 有希	富士通(株)	松田 和宏	(株)ユビテック
坂本 拓也	(株)富士通研究所	福本 佳成	楽天(株)
神薗 雅紀	PwC サイバーサービス合同会社	山崎 圭吾	(株)ラック
近藤 隆雄	(株)ベリサーブ	若居 和直	(株)ラック
島田 敏宏	(株)ベリサーブ	柳川 俊一	(株)ラック / KDDI デジタルセキュリティ(株)
樅山 清	(株)ベリサーブ	猪野 裕司	(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)	六宮 智悟	(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	

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　天野 農
黒谷 欣史　亀山 友彦　渡邉 祥樹
大友 更紗　吉本 賢樹　熊谷 悠平
堀江 亘　佐々木 敬幸　木村 泰介

IPA 執筆協力者　瓜生 和久　桑名 利幸　渡辺 貴仁
加賀谷 伸一郎　板橋 博之　竹内 智子

情報セキュリティ 10 大脅威 2019

～局面ごとにセキュリティ対策の最善手を～

2019 年 2 月 28 日　初 版
2019 年 3 月 1 日　第二版
2019 年 3 月 20 日　第三版
2019 年 4 月 3 日　第四版
2019 年 7 月 3 日　第五版

［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/