情報セキュリティ

10 大脅威 2024

～脅威に呑まれる前に十分なセキュリティ対策を～

IPA 独立行政法人情報処理推進機構
セキュリティセンター

2024 年 2 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 2024」
https://www.ipa.go.jp/security/10threats/10threats2024.html

目次

はじめに

本書「情報セキュリティ 10 大脅威 2024」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、2023 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 2024

個人の 10 大脅威では全ての脅威が 2023 年から 2 年連続で 10 大脅威に選抜されている。2023 年版まではこれらの脅威をランキング形式で紹介していたが、この順位が脅威の危険度であると誤解を招くおそれがあるため 2024 年版では五十音順の表記としている。いずれの脅威も危険度に差はないため等しく対策を講じることが望ましい。個人の脅威は攻撃の手口が古典的であり、本書で紹介している攻撃手口を知っておくだけでも対策になる脅威である。本書で最新の事例を確認し、攻撃手口を知ることが重要である。

一方、組織の 10 大脅威も、全ての脅威が 2 年連続で 10 大脅威に選抜されている。組織の脅威は 2024 年版でもランキング形式で紹介しているが、個人の脅威と同様に順位が危険度を表しているわけではない。昨年の被害事例等の状況から、「10 大脅威選考会」に参加している方々それぞれの観点で社会的に影響が大きかったと判断した脅威の順である。また、個人の脅威とは異なり、攻撃手口を知っているだけでは対策にならず、セキュリティ対策情報を継続的に収集し、使用している機器やサービスのセキュリティ対策をすることをはじめとした、状況に合わせた迅速な対応が求められている。各脅威の解説を読み、自組織の事業や体制にはどのようなリスクがあるのか洗い出すことが重要である。

本書では、2023 年の脅威の動向を 10 大脅威として解説する。

情報セキュリティ10 大脅威 2024

情報セキュリティ 10 大脅威 2024

■「情報セキュリティ 10 大脅威 2024」

2023 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 2024」では、「個人」と「組織」向け脅威として、それぞれ表 1.1、表 1.2 に掲載する。

表 1.1 情報セキュリティ 10 大脅威 2024 「個人」向けの脅威（五十音順）

「個人」向け脅威	初選出年	10 大脅威での取り扱い（2016 年以降）
インターネット上のサービスからの個人情報の窃取	2016 年	5 年連続 8 回目
インターネット上のサービスへの不正ログイン	2016 年	9 年連続 9 回目
クレジットカード情報の不正利用	2016 年	9 年連続 9 回目
スマホ決済の不正利用	2020 年	5 年連続 5 回目
偽警告によるインターネット詐欺	2020 年	5 年連続 5 回目
ネット上の誹謗・中傷・デマ	2016 年	9 年連続 9 回目
フィッシングによる個人情報等の詐取	2019 年	6 年連続 6 回目
不正アプリによるスマートフォン利用者への被害	2016 年	9 年連続 9 回目
メールや SMS 等を使った脅迫・詐欺の手口による金銭要求	2019 年	6 年連続 6 回目
ワンクリック請求等の不当請求による金銭被害	2016 年	2 年連続 4 回目

表 1.2 情報セキュリティ 10 大脅威 2024「組織」向けの脅威の順位

順位	「組織」向け脅威	初選出年	10 大脅威での取り扱い（2016 年以降）
1	ランサムウェアによる被害	2016 年	9 年連続 9 回目
2	サプライチェーンの弱点を悪用した攻撃	2019 年	6 年連続 6 回目
3	内部不正による情報漏えい等の被害	2016 年	9 年連続 9 回目
4	標的型攻撃による機密情報の窃取	2016 年	9 年連続 9 回目
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	2022 年	3 年連続 3 回目
6	不注意による情報漏えい等の被害	2016 年	6 年連続 7 回目
7	脆弱性対策情報の公開に伴う悪用増加	2016 年	4 年連続 7 回目
8	ビジネスメール詐欺による金銭被害	2018 年	7 年連続 7 回目
9	テレワーク等のニューノーマルな働き方を狙った攻撃	2021 年	4 年連続 4 回目
10	犯罪のビジネス化（アンダーグラウンドサービス）	2017 年	2 年連続 4 回目

本章で共通的に使用する用語の定義を**表 1.3** に記載する。

表 1.3 情報セキュリティ 10 大脅威 2024 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
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
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
組織的犯罪グループ	金銭を目的とした攻撃（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
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。
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。
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。
SNS	ソーシャルネットワーキングサービスの略称
SMS	ショートメッセージサービスの略称
ダークウェブ	一般的な検索エンジンでは検出されない闇サイト

■「情報セキュリティ 10 大脅威 2024」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 2024」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。10 大脅威 2024 では、個人の 10 大脅威の順位は掲載せず、五十音順で並べている。これは、順位が高い脅威から優先的に対応し、下位の脅威への対策が疎かになることを懸念しているためである。組織向けの脅威については従来通り順位も掲載しているが、考え方は個人向けの脅威と同様である。

例えば、個人の立場では、スマホ決済を利用しているならば、「スマホ決済の不正利用」への対策の優先度が上がる。もし、スマホ決済の残額チャージにクレジットカードを利用しているならば「クレジットカード情報の不正利用」への対策の優先度も同様に上がる。

また、組織の立場では例えば、自組織で利用している製品の脆弱性対策情報が開発会社から公開された際に、「脆弱性対策情報の公開に伴う悪用増加」のリスクが高くなるため、優先的に対策しなければならないだろう。

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 2024」で「10 大脅威」とはならなかった脅威についても、「情報セキュリティ 10 大脅威 2022」では「10 大脅威」であった脅威もある。しかし、「10 大脅威」から外れたとしてもその脅威が無くなったわけではない。「情報セキュリティ 10 大脅威 2022」に登場していた、「インターネットバンキングの不正利用」、「予期せぬ IT 基盤の障害に伴う業務停止」等も、依然として攻撃が行われていたり、IT 基盤の障害に伴う長時間のサービス停止が発生したりしている状況である。

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。

なお、「10 大脅威」から外れ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知られている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」[1] 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 ※「共通対策」で詳細を解説	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	手口から重要視すべき対策を理解する

また、昨今はクラウドサービスの利用も一般的になってきている。クラウドサービスを利用する場合は、表 1.5 の対策を「情報セキュリティ対策の基本」+ α として行うことで、被害に遭う可能性を低減できると考えるので参考にしてほしい。

表 1.5 情報セキュリティ対策の基本+ α

備える対象	情報セキュリティ対策の基本 ＋ α	目的
インシデント全般	責任範囲の明確化（理解）	クラウドサービスを契約する際に、インシデント発生時は誰（どの組織）が対応する責任があるのかを明確化（理解）する
クラウドの停止	代替案の準備	業務が停止しないように代替策を準備する
クラウドの仕様変更	設定の見直し	更新情報を定期的に確認し、仕様変更により意図せず変更された設定を適切な設定に直す（設定不備による情報漏えいや攻撃への悪用を防止する。）

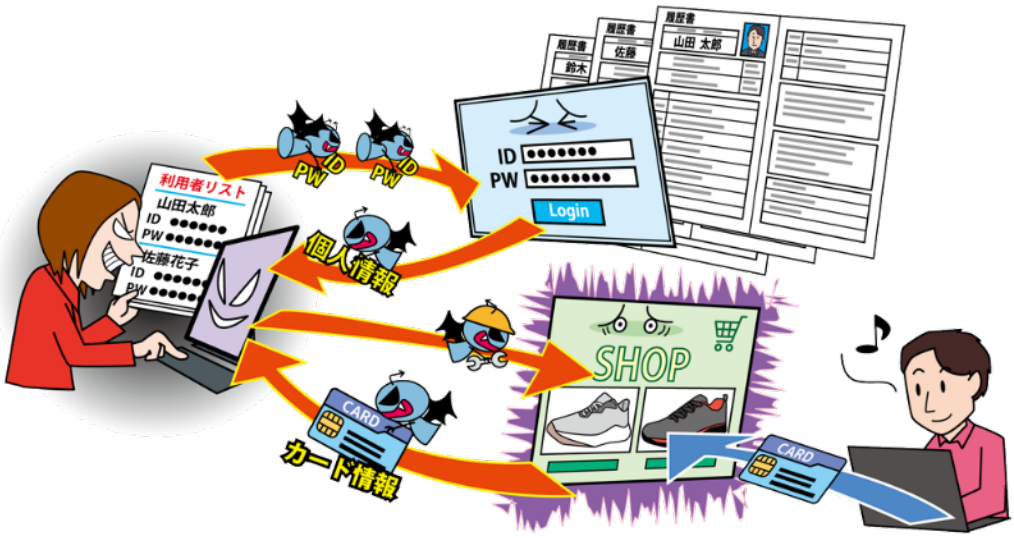
参考資料

1. 情報セキュリティ 10 大脅威 2015（IPA）
https://www.ipa.go.jp/security/10threats/2015/2015.html

1. 情報セキュリティ 10 大脅威（個人）

インターネット上のサービスからの個人情報の窃取

～情報が盗まれたことに気付いたら、即座に対応を～



ショッピングサイト（EC サイト）等、インターネット上のサービスへの不正アクセスや不正ログインが行われ、サービスに登録している個人情報等の重要情報を窃取される被害が継続して発生している。サービスの利用者は、窃取された情報を悪用されることにより、詐欺メールが送られてきたり、クレジットカードを不正利用されたりといった被害を受けるおそれがある。インターネットサービスの多様化や拡大は生活に大きな利便性をもたらしている一方で、インターネットサービスを狙った情報窃取も広がっている。

＜攻撃者＞

- 組織的犯罪グループ
- 犯罪者

＜被害者＞

- 個人（サービス利用者）
- 組織（サービス利用者、サービス運営者）

＜脅威と影響＞

昨今、多くの企業や組織によって、インターネット上で様々なサービスが運営されている。利用者は、そのサービスを利用するために個人情報等の重要情報（氏名、生年月日、メールアドレス、クレジットカード情報等）を入力して会員登録している。

しかし、サービスを運営している組織によって、サービスを構成しているソフトウェアの脆弱（ぜいじゃく）性対策や適切なセキュリティ対策が行われていない場合がある。また、利用者は、ログインに利用するアカウントのパスワード等を複数のサービスで使い回している場合がある。

これらのことに対して攻撃者は、ソフトウェアの脆弱性や他サービスから漏えいした認証情報を悪用して不正アクセスをすることで、サービスに登録されている重要情報を窃取する。そして、クレジットカードを不正利用したり、窃取した情報をダークウェブで売買したり、詐欺メールを送ったり等、さらなる被害につながるおそれがある。

＜攻撃手口＞

◆サービスの脆弱性や設定不備を悪用

攻撃者は、適切なセキュリティ対策が行われていないショッピングサイト等に対して、脆弱性や設定不備を悪用して、Web サイト内の個人情報等の重要情報を窃取する。

また、攻撃者は Web サイトの脆弱性を悪用して改ざんし、情報の送信先や保存先を変更する場合もある。例えば、サービスの利用者が改ざんに気付かず情報を入力してしまうと、その情報は攻撃者に窃取される。

◆他のサービス等から窃取した認証情報を悪用

他のサービスから窃取した認証情報（ID とパスワード）を悪用してサービスへ不正ログインし、個人情報等の重要情報を窃取する。詳細は個人の脅威「インターネット上のサービスへの不正ログイン」を参照すること。

＜事例または傾向＞

◆不正に入手された認証情報の悪用

2023 年 3 月、エン・ジャパンは同社が運営する総合転職情報サイト「エン転職」に登録されている個人情報が不正アクセスにより、情報漏えいしたことを公表した。調査によると 2023 年 3 月 20 日から 3 月 27 日の期間に、外部から不正に取得されたと思われる ID（メールアドレス）およびパスワードを使ったリスト型攻撃が行われ、「エン転職」に登録したユーザーのうち約 25 万 5,000 人の Web 履歴書にアクセスされたおそれがあるとしている。同社では「エン転職」の全ユーザーのアカウントについてパスワードをリセットし、パスワードの再設定方法および注意点等を「エン転職」を利用している全ユーザー向けにメールにて連絡している。[1]

◆不正アクセスにより顧客情報の窃取のおそれ

2023 年 10 月、ビッグモーターは、同社の Web サイトが不正アクセスされ、お問い合わせページを利用したユーザーの個人情報が漏えいした可能性があることを公表した。漏えいした個人情報は 2016 年 11 月から 2023 年 8 月にお問い合わせページに入力された情報で、氏名、住所、電話番号、メールアドレスが含まれている。同社は該当のユーザーにメール等で連絡し、不審なメールや通知が届いた場合は、開封およびリンク先へアクセスしないよう注意を呼びかけている。なお、同社が取り扱う顧客情報は別システムで保管されているため、顧客情報の漏えいは無いとしている。[2]

◆不正アクセスで個人情報窃取

2023 年 10 月、カシオ計算機は、同社の運営する ICT 教育アプリ「ClassPad.net」のシステムへ不正アクセスがあり、国内外で契約している利用者の個人情報が漏えいしたことを公表した。漏えいした個人情報は国内では個人や教育機関等から約 9 万件、海外では 148 の国と地域から約 3 万 5,000 件で、合計約 12 万 5,000 件としている。氏名やメールアドレスのほか、学校名や購入に関する情報、サービスの利用履歴等の情報が含まれている。同社は「ClassPad.net」のアプリへの不正アクセスは無いとし、システムのネットワークセキュリティ設定の一部が解除状態になり、開発環境のデータベースへ不正アクセスが行われたことが原因として報じている。同社では個人情報の漏えいのおそれがある全ての利用者へ連絡するとし、また相談窓口を設けて利用者からの問い合わせに対応するとしている。[3]

＜対策と対応＞

個人（サービス利用者）

- 被害の予防
  - ・不必要なサービスであれば退会する
  - ・必須項目以外の情報は極力登録しない
    情報漏えいのリスクを考慮してサービスを利用するための必須項目以外の情報は登録を避ける。
  - ・利用しているサービスの多要素認証の設定を有効にする
  - ・利用していないサービスは退会する
  - ・パスワードを適切に運用する ※
- 被害の早期検知
  - ・クレジットカード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、被害に気付ける可能性がある。
  - ・漏洩したアドレスを検索できるサービス[4]を使って、自分の使用しているアカウント情報が窃取されていないか定期的に確認する。
- 被害を受けた後の対応
  - ・適切な報告/連絡/相談を行う ※
  - ・パスワードを適切に運用する ※

※巻末「共通対策」を参照

インターネット上のサービスへの不正ログイン

～そのパスワード、本当に安全？個人情報を含めないよう注意！～

インターネットでサービスを受ける際に個人を識別するためにアカウントを作成することがある。アカウントを作成したサービスに対し第三者が不正にログインを行い、アカウントの乗っ取りや、アカウントに紐づけた個人情報を窃取する事案が発生している。様々なサイトで導入されつつある二要素認証が突破されるケースも確認されているため、注意が必要である。

＜攻撃者＞

- 組織的犯罪グループ
- 犯罪者（愉快犯、ストーカー等）

＜被害者＞

- 個人（サービス利用者）
- 組織（サービス運営者）

＜脅威と影響＞

不正に入手したIDとパスワードを使い、インターネット上のサービスに対して不正ログインが行われている。攻撃に使用するIDとパスワードは、別のサービスから漏えいしたものや誰もが使いそうな文字列、SNSのプロフィール等から類推されたもの等である。

不正ログインされるとサービスに応じた被害を受ける。ショッピングサイトであれば、氏名、住所、電話番号等の個人情報やサイトに登録しているクレジットカード情報等を窃取されたり、商品の不正購入やサイト内のポイントを盗用されたりする。また、スマートフォンを利用したキャッシュレス決済サービスであれば、チャージした残高を不正に利用される。LINE等のSNSであれば、プライベートな写真やメッセージのやり取り等を覗き見されたり、投稿を削除されたり等、嫌がらせ行為や偽の投稿（フィッシング詐欺等）をされたりする。

＜攻撃手口＞

◆フィッシング詐欺

メールやSMS等を使い、受信者を騙してフィッシングサイトに誘導し、認証情報等を詐取する。詳細は個人の脅威「フィッシングによる個人情報等の詐取」を参照すること。

◆パスワードリスト攻撃

攻撃者がダークウェブで購入する等何らかの不正な方法で入手したIDとパスワードのリストと、これを自動的に入力するプログラム等を用いて、ログイン機能を持つインターネット上のサービスにログインを試みる。サービス利用者が複数のサービスでパスワードを使い回すと、それら全てのサービスでログインされるおそれがある。

◆パスワード類推攻撃

使われやすいパスワードを類推し、そのパスワードでログインを試みる。例えば、芸能人や知人の個人情報（氏名、誕生日等）からパスワードを類推して、ログインを試みる。

◆ウイルス感染

攻撃者の用意した悪意のある Web サイトにアクセスさせたり、メールに添付されている悪意のあるファイルを開かせたりすることで、利用者の端末をウイルスに感染させる。利用者がその端末でインターネット上のサービスにログインすると、入力した ID やパスワードを攻撃者に窃取され、不正ログインに使われる。

＜事例または傾向＞

◆乗っ取った著名人のアカウントを販売

2023 年 5 月、著名人のアカウントを乗っ取り、売買した男など 7 人が不正アクセス禁止法違反の容疑で書類送検された。著名人のアカウントのパスワードは、公開されたプロフィール情報内の氏名、生年月日等から推測していた。アカウントはゲームデータを中心に販売する Web サイトで売買され、更にアカウントを購入した人に転売されていた。また、アカウントを購入した人は、乗っ取ったことを自慢したりしていたとされる。[1]

◆二段階認証を突破し、不正ログインで買い物

2023 年 9 月、X（旧 Twitter）上で Amazon の不正利用を報告するポスト（旧ツイート）が次々投稿された。投稿したユーザーが Amazon に問い合わせを行い、Amazon は不正ログインが横行していることを明らかにした。不正ログインされたアカウントは購入履歴を非公開にされ不正利用に気付きにくくなっていた。

不正ログインされたアカウントの中には二段階認証を突破してログインされたパターンもあり、この手口について Amazon は調査中としている。[2]

◆不正に入手された情報で第三者がログイン

2023 年 9 月、オンライントレードサービスを提供する SMBC 日興証券は第三者によってシステムへの不正ログインが行われていることを明らかにした。悪意のある第三者が窃取したと思われる口座番号やパスワード等を用いて不正なログインが行われていた。公表時点では口座からの資産流出は確認されていないが、提供しているオンライントレードサービスで、不正に保有株式の売却を行ったと思われる取引が 1 件あったことが判明している。

同社は不正ログインが確認された利用者に対して電話、メール等の手段で連絡を取りパスワードの変更を依頼した。また、すべての利用者に対して注意喚起を行った。[3,4]

＜対策と対応＞

個人（サービス利用者）[5]

- 被害の予防
  - ・表 1.4「情報セキュリティ対策の基本」を実施
  - ・メールの添付ファイル開封や、メールや SMS のリンク、URL のクリックを安易にしない ※
  - ・パスワードを適切に運用する ※
  - ・利用しているサービスの多要素認証の設定を有効にする
  - ・不審な Web 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）
  - ・利用していないサービスから退会する
  - ・利用頻度が低いサービスではクレジットカード情報を都度入力する
- 被害の早期検知
  - ・利用しているサービスのログイン履歴を確認する
  - ・クレジットカードやポイント等の利用履歴の定期的な確認をする
- 被害を受けた後の対応
  - ・クレジットカードの利用停止手続きをする
  - ・パスワードを適切に運用する ※
  - ・適切な報告/連絡/相談を行う ※

※巻末「共通対策」を参照

クレジットカード情報の不正利用

～一度も使っていないクレジットカードが不正利用される！？～

オンラインショッピングやキャッシュレス決済の普及に伴い、クレジットカードを利用する機会が増えている。それに伴い、クレジットカード所有者を狙ったフィッシング詐欺や 脆弱(ぜいじゃく)性を悪用した Web サイトの改ざん等によりクレジットカード情報が詐取され、攻撃者にクレジットカードを不正利用される被害が発生している。

＜攻撃者＞

- 組織的犯罪グループ
- 犯罪者

＜被害者＞

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

＜脅威と影響＞

攻撃者はフィッシング詐欺や不正アクセス等の様々な攻撃手口を用いてクレジットカード情報の窃取を試みている。

クレジットカード情報が攻撃者に窃取されると、正規の利用者が知らない間に不正利用され、金銭的な被害を受けるおそれがある。

また、利用者が一度も使ったことがないクレジットカードであっても、クレジットカード番号を攻撃者に推測されて悪用されるおそれもある。

＜攻撃手口＞

以下の手口でクレジットカード情報を入手し、不正利用を行う。[1]

◆フィッシング詐欺

メールや SMS 等を使い、受信者を騙してフィッシングサイトに誘導し、クレジットカード情報等を詐取する。詳細は個人の脅威「フィッシングによる個人情報等の詐取」を参照すること。

◆正規の決済画面を改ざんし入力情報を詐取

EC サイト（ショッピングサイト）の脆弱性を悪用し、正規 Web サイトの決済画面を改ざんする。改ざんした決済画面に利用者を誘導し、クレジットカード情報を入力させる。入力されたクレジットカード情報を攻撃者が詐取する。

◆不正アクセス

決済代行会社のシステムの脆弱性等を悪用し、システムに不正アクセスを行い、保存されているクレジットカード情報を窃取する。

◆クレジットマスター攻撃

クレジットカード番号、有効期限、セキュリティコードはパターンが限られている。これらの組み合わせをツールにより総当たりで入力し、クレジットカード情報を特定、悪用する。

◆ウイルス感染

ウイルスをメールに添付して開かせたり、悪意ある Web サイトのリンクを記載したメール等を送信し、リンクをクリックさせたりすることで、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、利用者がクレジットカード情報を入力すると、入力した情報が攻撃者に窃取される。

◆漏えいした情報の悪用

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を悪用する。漏えいしたクレジットカード情報は、ダークウェブ等で売買されることもある。

＜事例または傾向＞

◆「NICO ONLINE SHOP」でクレジットカード情報 13,084 件流出

2023 年 10 月、FANSMILE は、運営している「NICO ONLINE SHOP」において 2021 年 3 月から 2022 年 12 月にかけて利用された 13,084 件のクレジットカード情報が流出したおそれがあることを公表した。同社が運営する Web サイトが攻撃者に不正アクセスされ、決済アプリケーションを改ざんされたことが原因であった。[2]

◆「志布志市ふるさと納税特設サイト」でクレジットカード情報 910 件流出

2023 年 6 月、鹿児島県志布志市は、運営している「志布志市ふるさと納税特設サイト」で 2021 年 3 月から 12 月にかけて利用された 910 件のクレジットカード情報が流出したおそれがあることを公表した。当該 Web サイトが改ざんされ、クレジットカード決済時に情報を窃取する不正なソフトウェアが実行されたことが原因であった。[3]

◆クレジットカード情報の不正利用被害額が昨年より増加

2023 年 12 月、日本クレジット協会はクレジットカード発行会社を対象としたクレジットカード不正利用被害実態調査の結果を公開した。

調査結果によると、2023 年 1 月～9 月の被害額は 401.9 億円となった。2022 年同期間の被害額 309 億円と比較して増加しており、過去最悪のペースで被害が発生している。[4]

また、IPA においてはクレジットマスター攻撃を複数確認しており、2023 年 9 月に「コンピュータウイルス・不正アクセスの届出事例」の中で攻撃手口を紹介した。この攻撃手口はクレジットマスター攻撃であるため、正規の利用者が騙されていなくてもクレジットカード情報を攻撃者に入手され、正規の利用者が被害に遭うおそれがある。利用者自身が定期的にクレジットカードの利用状況を確認したり、利用時に通知されるよう設定したりすることで早期検知することが重要である。[5,6]

＜対策と対応＞

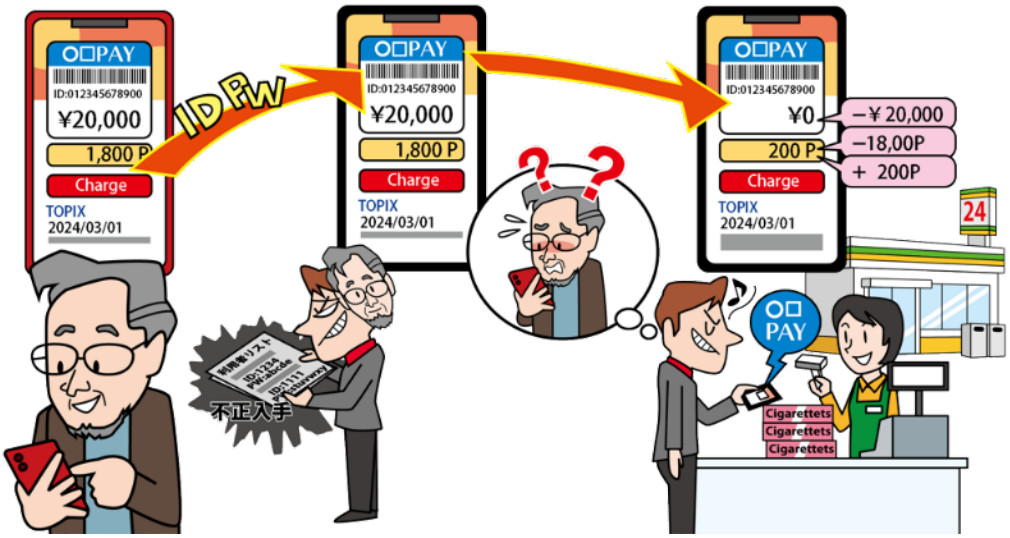
個人（利用者）

- 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 セキュア等）の利用
  - ・メールの添付ファイル開封や、メールや SMS のリンク、URL のクリックを安易にしない ※
  - ・普段は表示されないような画面やポップアップが表示された場合、情報を入力しない
  - ・プリペイドカード、デビットカードの利用を検討
  - ・不正利用被害額となる利用可能金額の範囲を限定する
  - ・利用頻度が低いサービスではクレジットカード情報を保存しない
    利用していないクレジットカードは契約解除や物理的破棄を検討する
- 被害の早期検知
  - ・クレジットカード利用明細の定期的な確認
  - ・サービス利用状況の通知機能の利用
- 被害を受けた後の対応
  - ・クレジットカードの利用停止手続きをする
  - ・ウイルス感染した端末を初期化する
  - ・適切な報告／連絡／相談を行う ※
  - ・パスワードを適切に運用する ※

※巻末「共通対策」を参照

スマホ決済の不正利用

～スマホで簡単決済。悪用されると攻撃者も簡単決済。～



スマートフォンの普及に伴い、2018 年頃よりキャッシュレス決済の 1 つであるスマートフォンを利用した決済（スマホ決済）が登場した。その後、スマホ決済を使った各社のサービスも登場しその手軽さから普及が進んだ。利便性が高い反面、第三者のなりすましによるサービスの不正利用や、連携する銀行口座からの不正な引き出しも確認されている。

＜攻撃者＞

- 組織的犯罪グループ
- 犯罪者

＜被害者＞

- 個人(スマホ決済サービス利用者)
- 個人(スマホ決済サービスと連携可能な銀行口座の所有者)
- 組織（サービス事業者・サービス利用店舗・クレジットカード会社）

＜脅威と影響＞

スマホ決済には、決済サービス毎に専用のシステムやアプリがあり、以下のような決済方法がある。

① スマートフォンを IC カードリーダーにかざす（非接触型決済）方法
② QR コードやバーコードをアプリで生成して、店舗のバーコードリーダーに読み込ませる方法
③ 店舗に置いてある QR コードをスマホアプリで読み込んで決済金額を手動で入力する方法

これらの方法は決済サービスに事前にクレジットカード情報や銀行口座番号を登録して利用する。

攻撃者は決済サービスに登録された ID とパスワードを窃取して不正ログインしたり、決済サービスの仕組みの不備を悪用したりすることで不正利用をする。

決済サービスを不正利用されると、クレジットカード情報が窃取されたり、意図しない金銭取引をされたり等の被害に遭う。

＜攻撃手口＞

◆不正アクセスによるアカウントの乗っ取り

不正に入手した ID とパスワードを使い、不正アクセスし、アカウントを乗っ取る。

被害者が複数のサービスで同一のパスワードを使い回している場合、攻撃者は過去に漏えいした ID とパスワードをリスト化し、それを基にログインを試みる（パスワードリスト攻撃）。または、フィッシング攻撃等により詐取した ID とパスワードでログインを試みる。そして、ログインに成功すると、本人になりすまして不正利用する。ここで、不正ログインの手口については、個人の脅威「インターネット上のサービスへの不正ログイン」を参照すること。

◆スマホ決済サービスと連携している銀行口座間における口座振込手続きの不備の悪用

スマホ決済サービスは、開発時に当該サービスと関連サービスの連携も含めたセキュリティが十分に考慮されていないと、スマホ決済サービスを不正利用できる脆弱性が存在する状態で公開されるおそれがある。利用者がそのようなサービスを利用している場合、攻撃者に脆弱性を悪用され、不正利用される。

◆不正に入手したスマホで決済をする

スマホを拾う、盗む、eSIM で乗っ取る等、不正に入手したスマホで決済をする。

＜事例または傾向＞

◆「PayPay」を使用して知人のアカウントから自身のアカウントに不正送金

2023 年 4 月、兵庫県警が電子計算機使用詐欺の疑いで容疑者を逮捕した。容疑者は会社員女性の「PayPay」のアカウントから自身のアカウントに約 8 万円を不正送金していた。

同署によると容疑者と被害者の女性は飲食店で知り合ったとしており、被害者は自身のスマートフォンのロックが解除されていたことと「PayPay」の残高がなくなっていたことに気が付き、同署に相談した。その後、送金履歴等から容疑者が特定された。[1]

◆他人の「auPAY」アカウントで不正に決済

2023 年 1 月、佐賀県警サイバー犯罪対策課と蕨署等が不正アクセス禁止法違反と詐欺等の疑いで中国籍の男女を再逮捕（いずれも詐欺罪で起訴）した。容疑者はコンビニエンスストアで「auPAY」を使用し約 55,000 円の物品を購入していた。購入時に容疑者が提示していたバーコードは佐賀県の女性名義の決済用バーコードであり、被害者の女性が不正な決済に気が付き、佐賀県警に相談したことで事件が発覚した。その後、店舗の防犯カメラの映像等から容疑者が特定された。[2]

◆スマートフォンを乗っ取り、スマホ決済を不正に利用

2023 年 9 月、名古屋県警等がブラジル国籍の容疑者を詐欺容疑で逮捕した。容疑者は大阪府の女性名義の決済サービスを利用して約 8,000 円相当の物品を不正に購入した疑いがある。被害者の女性のスマートフォンの「eSIM」（スマホ等に内蔵されたデジタル SIM）を乗っ取って不正に決済したと見られている。[3]

＜対策と対応＞

個人（スマホ決済サービス利用者）

- 被害の予防
  - ・表 1.4「情報セキュリティ対策の基本」を実施
  - ・利用しているサービスの多要素認証の設定を有効にする
  - ・スマホ決済でクレジットカードを利用する場合は 3D セキュアを利用する

    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、その後の金銭被害につながる重要な操作を阻止できる確率を高める。
  - ・パスワードを適切に運用する ※
  - ・フィッシングに注意する

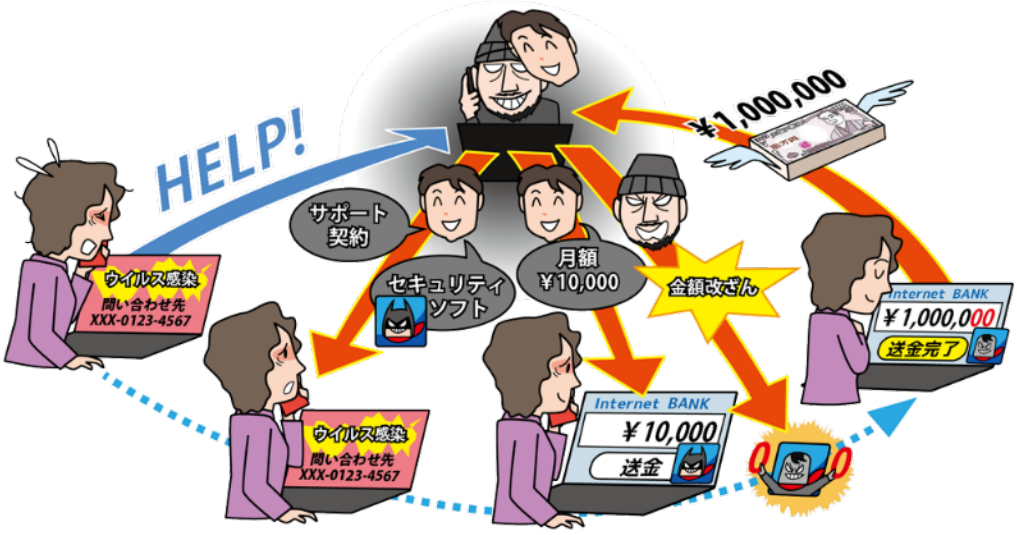
    スマホ決済を行っている企業を騙るフィッシングサイトやフィッシングメールに気を付ける。
  - ・利用していないサービスから退会する
  - ・スマートフォンの紛失時の対策

    紛失したスマートフォンを悪用されないために画面ロック等のセキュリティ対策を実施する。また、キャリア提供やセキュリティベンダーなどが提供する遠隔消去/初期化機能を設定する。
- 被害の早期検知
  - ・スマホ決済サービスの利用状況通知機能の利用および利用履歴の定期的な確認
  - ・連携する銀行口座の出金履歴の確認
- 被害を受けた後の対応
  - ・パスワードを適切に運用する ※
  - ・適切な報告／連絡／相談を行う ※

※巻末「共通対策」を参照

偽警告によるインターネット詐欺

～表示された番号に電話をかけないで！突然の警告画面に要注意～



Web サイトを閲覧中に、突然偽のセキュリティ警告画面が表示され、遠隔操作ソフトウェアをインストールさせられたり、サポート窓口を装った攻撃者にサポート料金を払わされたり、PC を遠隔操作された後に修復費用として金銭を騙し取られたりする被害（サポート詐欺）が発生している。また、画面の指示に従ってしまうと、二次被害につながるおそれもある。

＜攻撃者＞

- 組織的犯罪グループ
- 犯罪者

＜被害者＞

- 個人（インターネット利用者等）

＜脅威と影響＞

Web サイトを閲覧中に、「ウイルスが見つかりました」等の偽の警告画面が突然表示されることがある。表示された画面は、実在する企業からの通知を装っており、被害者に通知される内容を信用させ指示に従うよう促す。

画面の指示に従ってしまうと、遠隔操作ソフトウェアやスマホアプリを、インストールさせられたり購入させられたりする。また、偽のサポート窓口に連絡をしてしまうと、善意を装った攻撃者に PC やスマートフォンを遠隔操作され、最終的にサポート料金を払わされたり、修復費用を要求されたりする。

さらに、ソフトウェアの購入やサポートに連絡した時に入力した氏名、メールアドレス、クレジットカード情報等の個人情報が別の詐欺に悪用されたり、遠隔操作によって情報が漏えいしたりする等、二次被害につながるおそれもある。

＜攻撃手口＞

◆巧妙に細工が施された偽の警告画面

インターネット広告の悪用や Web サイトの改ざんによって、閲覧者を騙すための偽警告を表示する。偽警告は、閲覧者に警告内容を信じさせるために、実在する企業のロゴを使う場合がある。また、警告音を鳴らしたり、警告メッセージを音声で流したり、偽警告のポップアップ画面を閉じられないと誤解させたりすることでさらに不安を煽る。[1]

◆サポート詐欺

閲覧者に偽警告の画面に表示させたサポート窓口へ電話をかけさせ、遠隔操作用ソフトウェアをインストールさせる。その上で、ウイルス除去等の修復費用の支払いへ誘導する。支払い方法はコンビニエンスストアで販売されているプリペイド型電子マネーやギフトカードのほか、クレジットカード決済が使われる。また、インターネットバンキングの画面で、遠隔操作をしながら振り込みをさせる。

◆スマホアプリのインストールに誘導

偽警告をスマートフォンの画面に表示し、解決方法として、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。誘導したことにより広告主からアフィリエイト報酬を得たり、自動継続課金アプリによる料金請求で収益を得たりすることが目的と考えられる。[2]

◆有償セキュリティソフトの購入へ誘導

閲覧者を偽警告の画面からダウンロードページに誘導し、偽のセキュリティソフトをインストールさせる。最終的に有償ソフトウェアの購入へ誘導する。

＜事例または傾向＞

◆偽警告による詐欺で 4,400 万円騙し取られる

2023 年 4 月、埼玉県警浦和署は偽警告を使った詐欺の被害が発生したと発表した。被害者が PC でインターネットを閲覧していた際、「ウイルスに感染しました」との警告が表示され、表示された連絡先に電話したところ、パソコン関連会社の社員を名乗る人物から「ウイルスに感染している。銀行やクレジットカード情報が漏れる」「パソコンを遠隔操作で確認する」と言われた。さらに、「ハッキングされて口座に入っているお金が危ないので、別の口座に振り込む必要がある」と不安を煽られ、指定された口座にインターネットバンキングで 20 回にわたり計約 4,400 万円を振り込んでしまった。[3]

◆PC を遠隔操作し振込金額を変更

2023 年 1 月、兵庫県警は偽警告によるサポート詐欺で PC を遠隔操作され、金銭を騙し取られる被害が相次いでいると発表した。被害者の 1 人は、PC 利用中に表示された「ウイルスに感染」との警告に従い自宅の電話番号を入力し、電話を掛けてきたソフトウェア会社の社員を名乗る人物の指示に従って遠隔操作用ソフトウェアをインストールさせられた。サポート費用 1 万円の他、手数料 490 円を要求されインターネットバンキングから振り込む際に、PC を遠隔操作されて振込金額の桁数を増やされており、49 万円が送金されていた。[4]

◆偽警告被害の相談件数が大幅に増加

IPA 安心相談窓口が四半期ごとに公開している相談状況のレポートによると、2023 年に寄せられた偽のセキュリティ警告に関する相談件数は 4,145 件となり[5]、2022 年の 2,365 件[6]と比較して約 1.75 倍と大きく増加した。相談件数は 2022 年第 2 四半期から概ね増加傾向が続いており、特に 2023 年第 4 四半期は 1,324 件と、過去 6 年間で最多となった。[7]

＜対策と対応＞

個人（インターネット利用者等）

● 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

・表示される警告を安易に信用しない

慌てず冷静に判断し、判断が難しい場合は信頼できる周りの方に相談する。

・偽警告の画面の指示に従わない

警告に指示された遠隔操作ソフトウェアやアプリをインストールしない、電話をかけない、電話してしまったとしても遠隔操作はさせない、サポート料金を払わない、プリペイド型電子マネーの購入はしない。

・偽警告が表示されたらブラウザを終了する[8]

表示された警告画面の消し方が不明な場合やパソコンに関する技術的な相談は、IPA 情報セキュリティ安心相談窓口[9]に相談する。

・ブラウザの通知機能を不用意に許可しない[10]

偽警告の中にはブラウザの正規の通知機能を悪用するものもあるので注意する。

・ポップアップや広告のブロック機能などを設定する

● 被害を受けた後の対応

・PC を遠隔操作された場合はシステムの復元や初期化を行う

・スマホアプリをアンインストールする

自動継続課金設定をされていないかも確認し、設定されていたら解除する

・適切な報告/連絡/相談を行う ※

※巻末「共通対策」を参照

ネット上の誹謗・中傷・デマ

～その情報、本当に本物でしょうか？～

インターネットで自身の意見を自由に発信できることが一般的になった昨今、自身の発信で他者を誹謗・中傷したり、デマで社会的な混乱を引き起こしたり等、問題となる場合がある。発信した内容によっては裁判沙汰になったり、経済的損失を被ったりすることもある。また、AI 技術の発達により嘘か本当か見分けのつかない情報が錯綜することもあり、一層注意が必要である。

＜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 の普及に伴い、広範囲の発信を匿名で容易に行えるようになっている。そして、そのサービスを利用し、意図的に他人への誹謗・中傷や、脅迫・犯罪予告・デマを書き込む行為が確認されている。さらに、その情報が多くの人に拡散され、大きな問題となる場合がある。

攻撃の対象が個人であれば、精神的苦痛を受けたり、組織であれば、風評被害による経済的な損失を受けたりといった、様々な影響が出る。また、非常時に偽の情報が拡散された場合、社会的な混乱を引き起こすおそれがある。さらに、誹謗・中傷やデマの発信は犯罪になりうることや、情報の真偽を確認せず、安易に拡散した人も、その行為を特定され、社会的責任を問われることがある。

＜要因＞

◆影響のある情報を匿名で発信

特定の個人や企業に対する意見や感情を発信する際に、その内容が公になった場合の影響を考えずに発信してしまう。また、SNS での収益化を狙い、センセーショナルな内容を無条件に拡散するような行為も見受けられる。誰もが閲覧できるサービスの場合、1 つの発信が大きな影響をもたらすことがある。匿名での発信なら身元を隠せるとの誤解が内容を過激にしやすい一因である。しかし、匿名であっても名誉毀損や誹謗・中傷などに該当する場合、法律に基づいた手続きにより身元が特定される。

◆第三者による情報の拡散・改変

SNS 等のサービスを使って誰かが発信した、特定の個人や企業を貶める誹謗・中傷や真偽不明のデマについて、それを見た第三者が、悪意の有り無しに関係なく、真偽を確認せずに拡散させる。そして、伝言ゲームのように別の第三者がさらに拡

散させることで、誹謗・中傷やデマが広がっていく。このとき、拡散された内容が改変されて伝わることもある。

また、受け取った情報を別の第三者からの情報に紐づけて拡散することで、その第三者にも誹謗・中傷が広がるおそれもある。

＜事例または傾向＞

◆反応欲しさに…、ネット掲示板で名誉を毀損

2023 年 5 月、匿名掲示板に、被害者を名指しした上で「【緊急速報】ガチで逮捕」というスレッドを作成し、誹謗・中傷の内容の投稿を複数回実施した大学生が、名誉毀損の罪で有罪判決を受けた。中傷の内容は、被害者が交通死亡事故を起こし逮捕されたというものであった。大学生がスレッドを作成した動機は「過激な投稿をすれば多くの人に反応してもらえる」というものであった。[1]

◆インフルエンサーにデマ広告を依頼し、個人情報を窃取

2023 年 10 月、被害者の情報を窃取し、消費者金融から被害者名義で20万円を借り入れ、現金を盗んだ疑いで、京都府警が不正アクセス禁止法と窃盗の疑いで、20 代の男性を逮捕した。その男性は SNS で多数のフォロワーを持つ、インフルエンサーと呼ばれるユーザーに「登録するとポイントが受け取れる」と虚偽の広告を投稿するように依頼し、その広告から登録した被害者の情報を悪用したとみられている。[2]

◆生成 AI を悪用し、報道番組風動画を公開

2023 年 11 月、総理大臣が不適切な発言をする様子を報道したかのようなフェイク動画が SNS 上に投稿された。動画は生成 AI を用いて作成されており、総理大臣が実際に発言したかのように、声や口元の動き等を模倣したものであった。また、動画は日本テレビの報道番組風に似せて作成されていた。SNS 投稿後、このフェイク動画は製作者の予想よりも大きな話題となった。その後、投稿されたフェイク動画は削除され、製作者は業務を妨害するつもりはなかったと謝罪を行った。

一方で日本テレビは「番組を模倣して作成したことは到底許されるべきではない」としており、フェイク動画について今後も必要に応じてしかるべき対応をするという姿勢を見せている。[3]

＜対策と対応＞

個人（発信者、閲覧者）

● 被害の予防（被害に備えた対策含む）

・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

・情報の信頼性を確認する

インターネット上の情報が正しいとは限らないことを認識する。複数の情報元や情報の真偽を発信しているサービスを確認し、信頼できる情報かどうかを総合的に判断する。[7]

・誹謗・中傷や公序良俗に反する投稿や拡散をしない

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、投稿や拡散をして問題ない内容か実行前に確認する。

・投稿や拡散の責任を問われることを理解する

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等に発信者情報の開示を請求できる。発信者の特定は可能であり、発信者は犯罪になりうるという認識を持ち、発言内容には十分に留意する。

個人（家庭）、組織（教育機関）

● 被害の予防（被害に備えた対策含む）

・情報リテラシー、モラルを向上させる ※

個人（被害者）

● 被害を受けた後の適切な対応

・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 Web サイトの管理者やプロバイダーに削除を要請する。なお、削除により事態が悪化する可能性もあるため、要請する際は信頼できる周囲の人や弁護士等に相談して慎重に行う。

・適切な報告/連絡/相談を行う ※

※巻末「共通対策」を参照

フィッシングによる個人情報等の詐取

～金融機関や公的機関を装うフィッシング詐欺に注意を～

フィッシング詐欺は、公的機関や金融機関、ショッピングサイト、宅配業者等の有名企業を騙るメールやSMS を送信し、正規の Web サイトを騙ったフィッシングサイト（偽の Web サイト）へ誘導することで、認証情報やクレジットカード情報、個人情報を入力させ詐取する行為のことである。攻撃者に詐取された情報を悪用されると金銭的な被害等が発生する。

＜攻撃者＞

- 組織的犯罪グループ
- 犯罪者

＜被害者＞

- 個人（インターネット利用者）
- 組織（インターネット利用者）

＜脅威と影響＞

攻撃者は公的機関や有名企業を騙ったメールや SMS を送り付ける。そのメールや SMS を本物だと勘違いした受信者は、本文に記載したフィッシングサイトの URL にアクセスしてしまう。[1] 攻撃者は、そのフィッシングサイトで認証情報やクレジットカード情報、個人情報等を入力させ、情報を詐取する。詐取された情報は攻撃者に悪用されて、最終的に金銭的な被害が発生する。

＜攻撃手口＞

◆フィッシングサイトへ誘導するメールや SMS 等を不特定多数に送信

攻撃者は、公的機関や有名企業等の Web サイトを騙ったフィッシングサイトを作成する。その後、被害者をそのフィッシングサイトに誘導するために、宛先や本文を本物の公的機関や有名企業と信じさせる内容のメッセージをメールや SMS、SNS で不特定多数に送信する。それに騙された被害者をフィッシングサイトに誘導し、個人情報やクレジットカード番号、セキュリティコード等の重要情報を入力させ、情報を詐取する。テキスト表記上の（見た目の）URL と実際のリンク先 URL が異なるものもある。

近年では、宅配業者の不在通知や通信事業者の料金の支払い確認を装った SMS を送信し、フィッシングサイトに誘導する（スミッシング）手口が多く見られるほか、フィッシングサイトの誘導に QR コードを使用する（クイッシング）手口も見られる。いずれもフィッシングサイトで個人情報を入力させ、その情報を詐取するというものである。

◆検索サイトの検索結果に偽の広告を表示

検索エンジンの検索結果に表示される広告の仕組みを悪用し、人気商品の大幅な値引き等で目を

引かせる虚偽の不正な広告を表示する。不正な広告のリンクからフィッシングサイトに誘導し、個人情報等を詐取する。

＜詐取した情報の悪用例＞

- 詐取した個人情報を違法取引の Web サイトで販売し、攻撃者が金銭を得る。
- 詐取した認証情報でインターネットサービスに不正ログインし、不正送金したり、物品を購入しそれを転売したりすることで金銭を得る。

＜事例または傾向＞

◆給付金の受給申請を装ったフィッシング

2023 年 12 月、デジタル庁はマイナポータルを騙った詐欺メールおよび偽サイトについて注意喚起を行った。「電力・ガス・食料品等価格高騰緊急支援給付金（5 万円／1 世帯）のご案内」等といった件名の不審なメールが確認されており、給付金の受給申請を装った内容で偽のマイナポータルサイトへ誘導する。誘導先のサイトでは個人情報、クレジットカード情報等の入力が求められる。[2,3]

◆フィッシングを発端としたインターネットバンキング不正送金被害急増

2023 年 12 月、 警察庁と金融庁の連名で、メールや SMS に記載されたリンクからアクセスしたサイトに ID およびワンタイムパスワード、乱数表等のパスワードを入力しないよう注意喚起を行った。注意喚起は同年 4 月、8 月にも行われている。12 月 8 日時点において 2023 年 1 月から 11 月末におけるフィッシングによるものとみられるインターネットバンキングの不正送金の被害件数は 5,147 件、被害額は約 80.1 億円となり、いずれも過去最多を更新している。[4,5,6]

◆QR コードを用いたフィッシング攻撃に注意

2023 年 12 月 5 日、米連邦取引委員会（FTC）は QR コードに隠された有害なリンクに注意するよう警告文を公開した。QR コードは手軽に目的のサイトにアクセスする手段として広く使われている。攻撃者はその QR コードをフィッシング攻撃に使用している（クイッシング攻撃）。QRコードが記載されたメール等を受け取り、即座の行動が促されている場合はスキャンしないように、当機関では忠告している。[7]

また、2023 年 11 月、サイバー情報共有イニシアティブ（J-CSIP）は、J-CSIP の参加組織にて、2023 年 7 月下旬～8 月上旬にかけて、メールアカウント情報の更新を促す不審なメールが複数届いていたことを公開した。マイクロソフトからのメールを装い、メール本文には、QR コードと、QR コードを読み取ってメールアカウント情報を期限までに更新するように促すメッセージが書かれた画像ファイルが貼り付けられていた。この QR コードは、フィッシングサイトへ誘導するための URL を変換したものだった。[8]

＜対策と対応＞

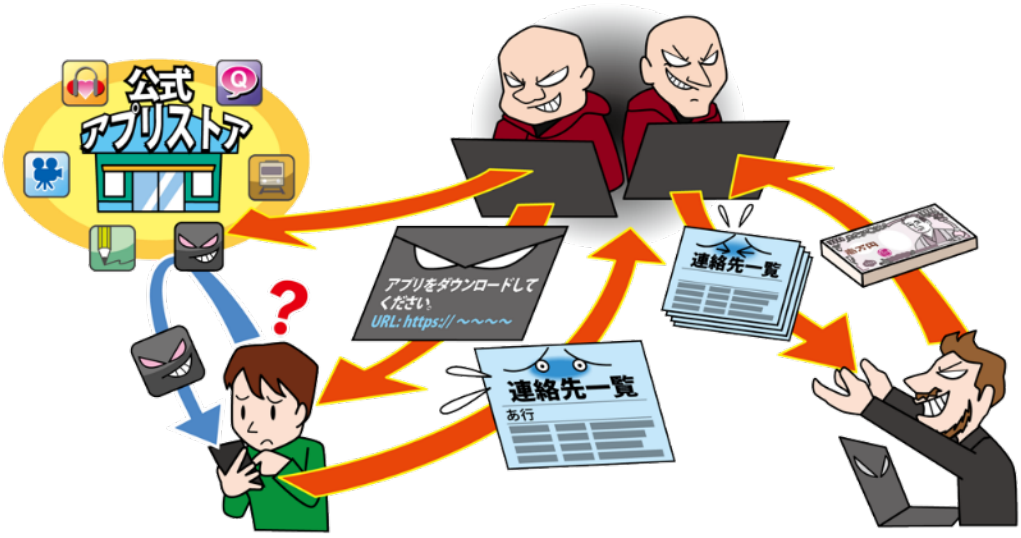
個人（インターネット利用者）

- 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
  - ・メールの添付ファイル開封や、メールや SMS のリンク、URL のクリックを安易にしない ※
  - ・利用しているサービスの多要素認証の設定を有効にする
  - ・迷惑メールフィルターを利用
- 被害の早期検知
  - ・利用しているサービスで、いつもと異なるログインがあった場合に通知する設定を有効にする
    通知があった際は自身のログインによるものかどうかや不正利用がないかを確認する。
  - ・クレジットカードやインターネットバンキングの利用明細を確認
- 被害を受けた後の対応
  - ・大量のフィッシングメールを受信している場合はメールアドレスの変更を検討する。
  （メールアドレスの漏えいを懸念した対応）
  - ・パスワードを適切に運用する ※
  - ・適切な報告/連絡/相談を行う ※

※巻末「共通対策」を参照

不正アプリによるスマートフォン利用者への被害

～アプリ提供者やアクセス権の確認を忘れずに～



スマートフォンの利用者が不正アプリをインストールし、スマートフォン内の個人情報が窃取される等の被害が発生している。不正アプリをインストールさせる手口として、メールや SMS に記載された URL をクリックさせることや、公式マーケットに公開された不正アプリをインストールさせること、SNS でダウンロードサイトに誘導すること等の手口が確認されている。

＜攻撃者＞

- 組織的犯罪グループ
- 犯罪者

＜被害者＞

- 個人（スマートフォン利用者）

＜脅威と影響＞

不正アプリをスマートフォンにインストールすると、スマートフォンに保存されている連絡先等の個人情報が窃取されてしまう。そして、キャリア決済等を悪用した金銭被害につながるおそれがある。また、DDoS 攻撃（分散型サービス妨害攻撃）の踏み台や、暗号資産（仮想通貨）のマイニングに利用される等、被害者が気付かないうちに、スマートフォンが犯罪に悪用されてしまうおそれもある。

さらに、不正アプリによって窃取された電話帳等に含まれる連絡先に、不正アプリをインストールする旨のメールや SMS が送信され、被害がさらに拡大していくおそれもある。

＜攻撃手口＞

◆不正アプリのダウンロードサイトへ誘導する

メールや SMS からダウンロードサイトに誘導することや、SNS で言葉巧みに相手をダウンロードサイトに誘導する等して、不正アプリをインストールさせる。[1] なお、ダウンロードサイトは、実在する Web サイトを騙った作りになっており、ユーザーが偽のサイトとは気付きにくいものになっている。

◆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。そして、利用者にはそのアプリを正規のアプリだと思い込ませ、インストールさせる。

◆アプリの更新時に悪意のある機能を有効化させる

アプリのインストール時は悪意ある機能を停止させておき、アプリの更新時に悪意のある機能を有効にさせて、不正行為を行う。

＜事例または傾向＞

◆公式マーケット以外にある複数の不正アプリ

2023 年 12 月、SBI EVERSPIN は、無償で提供している「Fake Finder for SBI Group」において複数の不正アプリを検出したため、注意喚起を行った。検出した不正アプリには、金融機関または公共機関等を詐称する偽アプリや、電話、ファイルとメディア、SNS、連絡先へのアクセス権限を要求するもの等があった。

このような不正アプリは、公式マーケット以外の場所で配布されることが多いため、原則としてアプリは公式マーケットから入手し、その際は開発元の信頼性やアプリの機能、利用規約等を慎重に確認する必要があると注意を呼び掛けている。[2,3]

◆Google Play にもある多数の不正アプリ

2023 年 11 月、カスペルスキーのリサーチチームは、Google Play 上の悪意のあるアプリの合計ダウンロード数が 6 億回を超えていることと、悪意のあるアプリの事例を紹介した。

それらのアプリには、利用者を盗聴するトロイの木馬、端末内の情報や位置情報をサーバーに送信するスパイウェア、利用者のデータを収集するアドウェアである「SpinOk」のコードライブラリを含んだもの等が見つかっている。同社は、アプリの真正性を確認することや、アプリの評価を過信しないこと、信頼性の高い保護アプリをインストールすること、デバイススキャンをすること等の対策が必要であることも紹介している。[4]

◆宅配業者を装った偽 SMS による不在通知

2023 年 11 月、安中市は、宅配業者を装った偽 SMS による不在通知が増加しているとして注意喚起を行い、具体的な事例を紹介した。

被害者は、数ヶ月前にスマートフォンに宅配便の不在連絡のような SMS が届いたため、SMS に記載された URL にアクセスをした。その時に氏名などの個人情報を入力してしまった可能性があった。

その後、約 11 万円がキャリア決済され、電子マネーが購入されていることが分かった。[5]

＜対策と対応＞

個人（スマートフォン利用者）

● 被害の予防

・表 1.4「情報セキュリティ対策の基本」を実施

・アプリは公式マーケットから入手

公式マーケット以外のサイトからアプリのインストールをしない。ただし、公式マーケットにも不正アプリが紛れていることがあるため、レビューや評価に加え、アプリ開発者の情報やアプリのバージョンアップ履歴があること等も確認し、信頼できるアプリかどうかを判断する。

・アプリインストール時のアクセス権限の確認

アプリのインストール時にアクセス許可が要求された権限について、アプリの機能に対して適切かどうかを確認する。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 端末の設定で、提供元不明のアプリのインストールを許可しない。

−iPhone の設定で、「信頼されていないエンタープライズデベロッパ」の表示がされるアプリをインストールしない。

・不要なアプリをインストールしない

正規のアプリであっても使い方を誤れば意図せず重要情報を公開してしまうこともある。そのため、アプリの機能を理解し、不要なアプリをインストールしない等の適切な利用を心がける。

・利用しないアプリはアンインストールする。また、インストールした覚えのないアプリもアンインストールする。

・セキュリティソフトをインストールする

● 被害を受けた後の対応

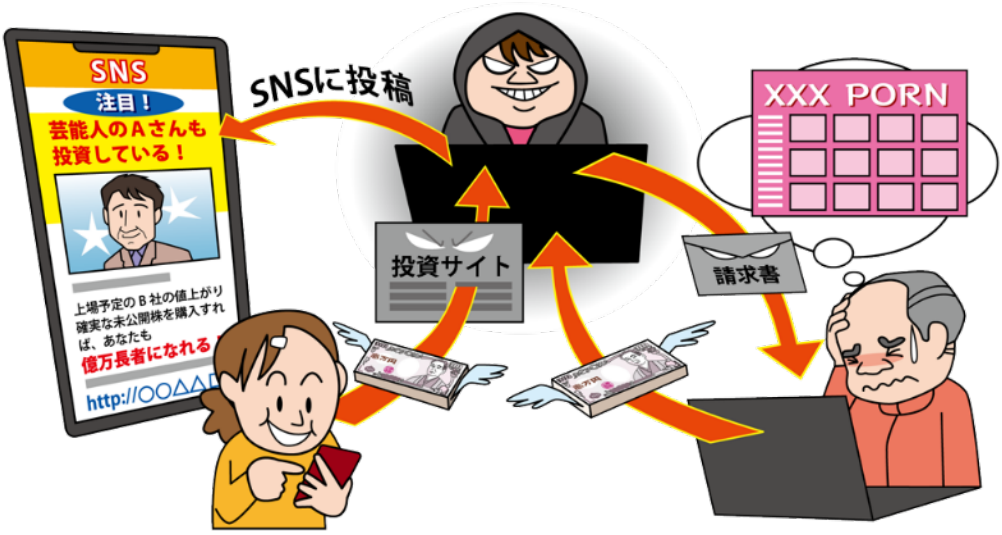
・不正アプリのアンインストール

アンインストールできない場合は端末を初期化する。

・ショッピングサイトや SNS 等、サービスの認証情報を入力してしまった場合は、そのサービスのパスワードを変更する。

メールや SMS 等を使った脅迫・詐欺の手口による金銭要求

～人生いろいろ。詐欺の手口もいろいろ～



世の中には IT を悪用した詐欺が横行している。人の弱みに付け込むものや、公共機関を装って相手の不安を煽るもの、そして、親交を深めて相手を騙すものなどである。これらの詐欺は、メールや SMS 等を悪用して行われることが多い。また、これらの詐欺の手口は様々だが、攻撃者の目的は金銭を詐取することにある。

＜攻撃者＞

- 組織的犯罪グループ
- 犯罪者

＜被害者＞

- 個人（インターネット利用者）

＜脅威と影響＞

攻撃者は、ターゲットとなる個人に脅迫や詐欺のメールを送り付ける。その内容は、基本的に虚偽の内容であり、不安を煽るものであるため、メールの受信者は、その内容を信じてしまうおそれがある。また、受信者は、弱みに付け込まれているという負い目を感じてしまい、周囲に相談できなくなるおそれもある。さらに、募金詐欺の場合、受信者はお金を振り込んでしまい、そもそも詐欺にあったことに気付いていないおそれもある。

そして、攻撃者は一度でもこのような攻撃に成功すると、その手口が効果的であると考え、同様の攻撃を多方面に行う。そのことにより、被害がさらに拡大していくおそれもある。

＜攻撃手口＞

◆メールや SMS で脅迫をする

脅迫や架空請求によって金銭を要求する内容のメールや SMS 等を不特定多数の人に送り、金銭を詐取しようとする。そして、支払方法として、プリペイド型電子マネーや暗号資産（仮想通貨）が指定されることが多い。

◆性的な脅し（セクストーション）をする

周囲に相談しにくい性的な弱みに付け込んだ脅迫をセクストーションと呼ぶ。攻撃者は、被害者に対して SNS 等で言葉巧みに話を持ち掛け、ビデオ動画で恥ずかしいやり取りをさせる。そして、スマートフォンに不正アプリをインストールさせるように誘導する。不正アプリには、遠隔操作機能や連絡先を窃取する機能が仕込まれており、攻撃者は連絡先を窃取すると、恥ずかしいやり取りを知人にばらすと被害者を脅し、金銭を要求する。[1,2,3]

◆ハッキングを装う

攻撃者は、あらかじめ外部のサービスから漏えいした個人情報を基に、被害者にパスワードや住所等の個人情報が書かれたメールを送信する。そして、あたかも被害者の PC をハッキングして情

報を得たかのように見せかけて不安を煽り、金銭を要求する。

◆公的機関等を装い、電話を併用して信憑性を高める

公的機関等の社会的な信用のある組織からのメールを装うことで、攻撃者は自身の信憑性を高めて、被害者に連絡を取るように求める。もし、被害者が連絡をした場合、攻撃者は公的機関からの連絡であることを伝え、被害者の不安を煽り、金銭の振り込みを要求する。さらに、攻撃者から被害者に対して金銭を要求する電話を掛け、その後に弁護士を装って和解を求める旨のメールを送信して騙す手口もある。

◆SNS 等で親交を深める

SNS を利用して有名人を装い、親交を深めた後に投資の勧誘を行う詐欺が行われている。また、海外の異性を装い、SNS 上で交際を持ち掛け、親密になったところで相手の恋愛感情を利用し、様々な名目で金銭を要求することや、投資の勧誘をするなどのロマンス詐欺も行われている。

＜事例または傾向＞

◆大学のメールアドレス宛に脅迫メールを送信

2023 年 5 月、電気通信大学情報基盤センターは、学内のメールアドレスにセクストーションを目的とした複数の迷惑メールが届いていることを確認したため、注意喚起を行った。メールには、「私のソフトウェアはあなたのカメラとマイクも制御しました。あなたを主演とした価値ある卑猥なビデオをいくつか作成しました。私が支払いを受ければ、あなたのプライバシーは守られます。そうでなければ、私はあなたの連絡先に最も有害なコンテンツを漏らし、変質者が見ることができるようにそれを公開 Web サイトに投稿します。」と、性的な内容で脅迫する文面が記載されていた。[4]

◆支援金を受け取れると嘘のメールを送信

2023 年 1 月、大阪の 70 代の男性の携帯電話に「もうすぐがんで死ぬため支援金として 9,000 万円を譲りたい」といったメールが届いた。男性がメールに記載されたサイトにアクセスすると、メッセージのやり取りが始まった。その中で、支援金を受け取るための費用として、現金を振り込むことを繰り返し指示され、指定された口座に総額 5,000 万円あまりを振り込んでいた。11 月に男性が娘に相談した際に、被害が発覚した。警察は特殊詐欺事件として捜査をするとともに、現金がもらえるといった内容のメールは信憑性に欠けるため、すぐに相談するようにと注意を呼び掛けている[5]

◆SNS を利用した投資詐欺が横行中

2023 年 12 月、札幌市の女性が SNS で知り合った男から暗号資産の投資を持ち掛けられ、口座に総額約 1 億 5,000 万円を振り込むという事件が発生した。女性は現金を引き出そうとすると、「引き出すのにも金がかかる」と男に言われたため、騙されたことに気付き警察に相談して事件が発覚した。[6]

＜対策と対応＞

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
  - ・受信した脅迫、詐欺メールは無視する

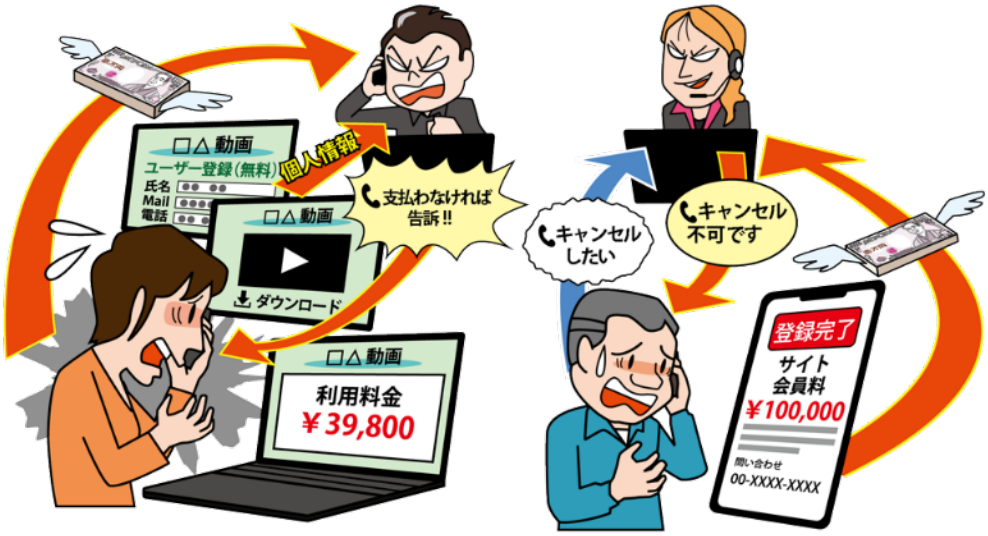
    受信したメールに、被害者が実際に使用しているパスワードが記載されていた場合でも、PC がハッキングされていることはまずない。しかし、パスワードが漏えいしているおそれがあるため、パスワードを変更する。
  - ・利用しているサービスの多要素認証の設定を有効にする
  - ・メールに記載されている番号に電話をしない

    受信した脅迫や架空請求のメールについて専門機関に相談したい場合は、そのメールに記載された連絡先ではなく、自身で調べた正規の電話番号やメールアドレスに連絡する。
- 被害を受けた後の対応
  - ・クレジットカードの利用停止手続きをする
  - ・適切な報告/連絡/相談を行う ※
  - ・パスワードを適切に運用する ※

※巻末「共通対策」を参照

ワンクリック請求等の不当請求による金銭被害

～不当請求は無視！不安な場合は周りに相談を～



Web サイトの閲覧中やメール等に記載されたリンクにアクセスした際に有料サービスの会員登録完了画面や利用料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（ワンクリック詐欺）が依然として発生している。また、複数回のクリックやタップを経てから請求画面等を表示する複数クリック詐欺（ツークリック詐欺とも呼ばれる）もあり、これには確認画面を何回かクリックやタップをさせることで、確認画面で同意した自分に落ち度があると心理的な負い目を感じさせる狙いがある。他には、表示しているページを自動的に請求画面へ転送するゼロクリック詐欺もある。

＜攻撃者＞

- 組織的犯罪グループ
- 犯罪者

＜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したりすると、契約が成立したかのようなメッセージと、有料サービスの会員登録料や利用料といった名目の金銭の請求画面が表示されるワンクリック請求が依然として発生している。

請求画面上や請求画面に記載した問い合わせ窓口で、早急に支払わなければ訴訟になる等と脅す手口もあり、不安を煽られた被害者は焦って料金を支払ってしまうおそれがある。支払った後も、繰り返し支払いを要求される場合もある。また、このようなワンクリック請求の対処法を検索する中で、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 Web サイト上に請求画面を表示

アダルトサイトや出会い系サイト内に表示した「18 歳以上」の年齢確認や動画再生のボタンをクリックさせたり、自動的に画面を転送したりすることで、会員登録完了の請求画面を表示させる。金銭の支払い義務があるように見せ、不当に金銭を請求する。

◆メールに記載されたリンクをクリックさせる

届いたメールに記載されているリンクをクリックさせ、Web サイトで会員登録完了の画面を表示して高額な料金を請求する。

◆不正なソフトウェアや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、不正なソフトウェアやアプリをインストールさせる。請求画面が

閉じられても、数分おきに請求画面を表示させ、PC やスマートフォンが再起動されても、再び請求画面を表示させるようにすることもある。

◆電話による脅迫や情報窃取

請求画面に問い合わせ先の電話番号を記載し、退会を焦る被害者に電話をかけさせる。もしくは、Web サイトに電話番号を登録させて、その人に電話をかける。被害者と連絡が取れると、「再生ボタンを押したので契約は成立しており、解約はできない」等と支払いを迫る。さらに、「退会や支払いを免除するため」等と称して、個人情報を聞きだそうとする場合もある。詐取された個人情報は、別のサイバー攻撃に悪用されるおそれがある。

＜事例または傾向＞

◆不当請求で約 1,000 万円を騙し取られる

2023 年 10 月、アダルトサイトの登録料等の名目で金銭を騙し取る特殊詐欺事件が発生した。被害者がスマートフォンでアダルトサイトを閲覧中、「24 時間以内にお金を支払ってください」という内容のメッセージが画面に表示され、サイト上で退会を選択したものの翌日にサイトの関係者を名乗る人物から電話があり、登録料等として金銭の支払いを請求された。これを信じて電子マネーの送金や現金の振り込みを計 10 回行い、総額約 1,000 万円を騙し取られた。[1]

◆継続して多い不当請求の相談

国民生活センターによると、アダルト情報サイトに関する相談が 2023 年 1 月～5 月に 786 件（2022 年同期 1,384 件）寄せられた。相談内容は、「無料だと思って『18 歳以上』をクリックしたら、いきなり会員登録となり料金請求画面になった」、「料金請求画面がパソコン画面上に張り付き消えない」等、ワンクリック請求等の不当請求に関わるものが多く見られる。同センターに寄せられた同様の相談の総件数は 2021 年が 12,942 件、2022 年が 10,172 件となっており、減少傾向ではあるものの、依然として多くの相談が寄せられている状況である。[2]

＜対策と対応＞

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
  - ・情報リテラシー、モラルを向上させる ※
  - ・不当な請求を安易に信用しない

    慌てず冷静に判断し、判断が難しい場合は信頼できる周りの方に相談する。
  - ・不当な請求には応じない、連絡しない

    不当な料金の請求画面が表示されても連絡しない。画面に個人情報を取得したように書かれている場合もあるが、それは見せかけで、画面を開いた時点では攻撃者に情報は渡っていない。
  - ・請求画面が表示されたらブラウザを終了する[3]

    表示された警告画面の消し方が不明な場合やパソコンに関する技術的な相談は、IPA 情報セキュリティ安心相談窓口[4]に相談する。
  - ・メールの添付ファイル開封や、メールや SMS のリンク、URL のクリックを安易にしない ※
  - ・不正なソフトウェアをダウンロードしない
- 被害を受けた後の対応
  - ・適切な報告/連絡/相談を行う ※
  - ・端末を初期化する

※巻末「共通対策」を参照

コラム：パスキーを知っていますか？新しい認証方式でパスワードレスの時代に！

皆さんは普段オンラインショッピングやインターネットバンキング等のサービスを利用する際にどのようにログインを行っていますか？ID とパスワードのみを入力してログインを行っている方もいれば、指紋等の生体認証でログインを行っている方もいるでしょう。また、セキュリティを気にしている方であれば、SMS 認証等、複数の認証方式を組み合わせた多要素認証（※1）を利用されている方もいるでしょう。どの認証方式を使うかはサービスで使える認証方式の種類や個人の好み等によりますが、昨今、ID とパスワードのみを利用した認証はセキュリティの観点から危険とされており、パスキーを利用したパスワードレス認証方式（パスワードを使わない認証方式）や多要素認証が注目されています。しかし、フィッシング対策協議会が 2023 年 7 月に公開した認証方式に関するアンケートの調査結果によると、オンラインショッピングに関して「ID／パスワードのみ」と答えた方が 80.9%を占めており、多要素認証等のより安全な認証方式の利用はまだまだ進んでいない状況です。[1]

※1：認証の 3 要素である「知識情報」、「所持情報」、「生体情報」などのうち、2 つ以上を組み合わせて行う認証のこと[2]

【不正ログインの被害事例】

サービスを利用する上で不正ログインのリスクが伴います。実際にサービスに不正ログインされ、個人情報を閲覧されたり、不正利用されたりする被害が 2023 年および 2024 年も報じられています。

被害時期または発表時期	サービスの種類	被害の概要
2024 年 1 月	オンラインショッピングサービス	第三者に 8 件の正規利用者のアカウント情報を用いて不正ログインされました。正規利用者とは関係ない宛先へ商品を届ける不正な注文が行われました。注文金額の総額は約 300 万円以上とされています。[3]
2023 年 9 月	ネット取引サービス	サービス提供元以外から入手した口座番号とパスワードを用いて不正ログインされました。保有株式を不正に売却される被害が発生しました。[4]
2023 年 9 月	オンラインショッピングサービス	X（旧 Twitter）上で二段階認証を設定したアカウントが不正アクセスされたという報告が多数ありました。ギフトカードを購入されたという被害報告もされています。[5]
2023 年 5 月	オンラインショッピングサービス	国内の IP アドレスを発信元として、サービスに対して 10 回のログインが試行され、3 件のアカウントが不正ログインされました。氏名、住所、生年月日、クレジットカード番号の一部等が閲覧されたおそれがあります。[6]
2023 年 3 月	転職情報サービス	パスワードリスト攻撃により、利用者 25 万 5,765 名分のアカウントが不正ログインされました。履歴書を閲覧されたおそれがあります。[7]

被害時期または発表時期	サービスの種類	被害の概要
2023 年 1 月	英語検定試験サービス	約 26 万回に及ぶログインの試行がされ、58 件のアカウントが、不正ログインされました。氏名、住所、電話番号、生年月日等が閲覧されたおそれがあります。パスワードリスト攻撃によるものとみられています。[8]

被害の概要を見ると、パスワードリスト攻撃（ダークウェブ（一般的な検索エンジンでは検出されない闇サイト）で購入する等、何らかの方法で入手した ID とパスワードを組み合わせたリストに基づき不正ログインする手口）を用いて不正ログインされる事例が多数確認されています。これらの被害に遭わないためにサービス提供側だけではなく、サービス利用者も安全な認証方式の利用等の適切な対策が求められます。

【ID とパスワードを利用した認証方式の課題・問題点】

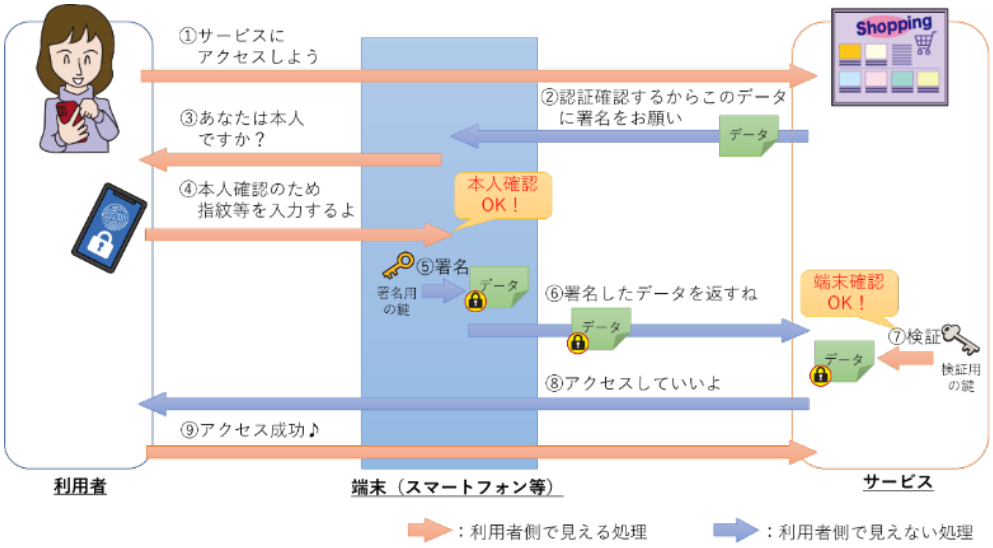
ID とパスワードを利用した認証は昔からあり、広く普及している馴染みのある認証方式です。ID とパスワードを記憶しておけばよく、利用者にとって気軽に使える認証方式である一方、セキュリティの観点ではその認証方式のみでは決して安全とは言えません。例えば、以下のような課題・問題点が挙げられます。

ID とパスワードを利用した認証の課題・問題点	概要
利用者にてパスワードの管理が必要	パスワードは利用者が覚えやすいもの、単純なものになりがちです。また、パスワードを複雑にすると忘れることがあります。さらに、パスワードを複数のサービスで使い回していると、漏えいした際に被害が大きくなるおそれがあります
漏えいしたパスワードは他サービスへの不正ログインに悪用される	漏えいしたパスワードは恒久的にインターネット上に残り続けます。そのため、1 度漏えいしたパスワードは悪用され続けるおそれがあります。なお、インターネット利用者が自らの個人情報が漏えいしていないかを照会できる Web サイトも公開されています。[9]
パスワードを詐取する攻撃の存在	フィッシングメール等利用者の個人情報（パスワード等）の収集を狙った脅威が存在します（詳細は個人の脅威「フィッシングによる個人情報等の詐取」を参照すること）。
認証情報はサービス提供側に保存される（サービス提供側からの漏えいリスクが存在する）	サービス提供側の管理が不適切な場合、攻撃者に狙われて認証情報（ハッシュ化されたパスワード等）が漏えいするおそれがあります。その際、ID も共に漏えいすることが多いため、不正ログインのための手がかりとして悪用されるおそれがあります。

そのため、より安全に認証を行うためには、ID とパスワードのみを利用した認証だけではなく、利用者の記憶に頼らない、別の認証方式と組み合わせた多要素認証の利用が推奨されます。

【パスキーとは】

新しい認証方式としてパスキーが注目されています。パスキーは、FIDO アライアンス（パスワードへの過度の依存を減らすための認証標準を目指すオープンな業界団体）によって策定されたパスワードレスな認証方式です。[10] パスワードの代わりとして、スマホ等のデバイスの生体認証（指紋、顔）や画面ロックの解除（PIN 等）を行うことで認証を行うことができます。コラムの趣旨とは違うため詳細は割愛しますが、パスキーは、公開鍵暗号方式と呼ばれる仕組みを用いた認証を行っています。[11] 簡単に認証の流れを説明すると、サービスにアクセスしている端末とサービスの間で、初回設定時に生成した署名用の鍵を使い変換（署名）した毎回変わるランダムなデータを用いて認証を行います。その際に正しいデータかの判断としてサーバー側で検証用の鍵を用いて正しいアクセスかの検証を行います。また、署名用の鍵は複数の端末間でクラウドを通して同期可能となるため、初期設定を正しく完了しておくことで別の端末を利用しても同じ仕組みで認証が行えます。



図：パスキーの認証のイメージ

【パスキーを利用するメリット】

パスキーを利用することで ID とパスワードを利用した認証の課題・問題点を解決することが期待できます。

パスキーを利用するメリット	概要
パスワードレスによりパスワード管理不要	**利用者によるパスワードの管理は不要です**。そのため、忘れること（覚える必要）はなく、複雑なパスワードを考える必要はありません。また、パスワードを利用しないため**パスワードは漏えいしません**。ネットワーク上を流れるのは認証用のデータで、毎回ランダムに変わるため、再利用（悪用）は困難です。

パスキーを利用するメリット	概要
利用者のパスワードを狙った攻撃への耐性がある	**パスワードを利用しないためパスワードの詐取を狙った攻撃は意味をなさなくなります。**仮にパスキーとして PIN を使っていたとして、フィッシングメールでその PIN を入力してしまっても、それは端末の画面ロックの解除のもので、サービスの認証に使われる認証情報ではありません（※2）。また、SIM スワップ（スマホの SIM を再発行し、乗っ取る攻撃）により、SMS 認証やワンタイムパスワードを不正に閲覧されて、2 要素認証を突破する攻撃にも耐性があります。
パスワードの代わりとなる生体認証（指紋、顔）やデバイスの画面ロックの解除（PIN 等）は端末の中に保存される	**サービス提供側に認証情報（ハッシュ化されたパスワード等）は保存されません。**そのため、仮に認証の検証用の鍵が漏えいしたとしても漏えいした情報のみでの悪用は困難です。

※2：PIN 以外に氏名等の個人情報を合わせて入力した場合は、その情報が悪用されるおそれがあるため注意

これら以外にも、**パスキー自体が多要素認証（二要素認証）になっている**というメリットもあります。なぜなら、パスキーは、本人確認（生体情報）と端末確認（所持情報）の 2 つを同時に行うことができるためです。

【パスキーを利用する上での注意点】

万能に見えるパスキーですが、メリットがある一方注意点もあります。

パスキーの注意点	概要
サービス提供側がパスキーに対応している必要がある	パスキーを利用するにはサービス提供側がパスキーに対応している必要があります。（※3）2023 年以降パスキーに対応したサービスが増えてきていますが、新しい認証方式で普及途中なことから利用しているサービスが対応しているとは限りません。
パスキーを利用する端末の管理が必要	パスキーを利用する端末を全て紛失した場合、認証ができなくなります。端末の紛失を想定して、パスキーの解除方法や別端末でのパスキーの復旧方法等を理解しておく必要があります。主要なサービスであればサポートページ等で案内されています。[12,13]

※3：パスキーの実装に不備があれば利用者に安全な認証を提供できません。サービス提供側は、ガイドラインや SDK の内容を理解し、正しい実装を行う必要があります。また、それを確認する体制を整備しておくことが大切です。

【最後に】

パスキーは新しい認証方式です。2023 年に入り、メルカリ、TikTok、ニンテンドーアカウント等、多くのサービスで対応が始まっています。パスキーはあくまで認証方式の 1 つであり、必ずしも使わなければいけないという訳ではありません。しかし、安全な認証方式の 1 つとして昨今注目されているため、ID とパスワードのみで認証を行っている方は、これを機にパスキーへの移行をされてはいかがでしょうか？また、別の多要素認証を使っている方も現在の認証方式に不便や不安を感じているのであれば、併せてパスキーへの移行を検討してもよいかもしれません。安全な認証方式を活用し、皆さんの推しのサービスを安全に利用しましょう。

参考資料

1. インターネットサービス利用者に対する「認証方法」に関するアンケート調査 コロナ禍を経た利用者の変化について、追跡調査結果を公開 (2023/07/21)（フィッシング対策協議会）
   https://www.antiphishing.jp/report/wg/authentication_20230721.html
2. 多要素認証（株式会社野村総合研究所）
   https://www.nri.com/jp/knowledge/glossary/lst/ta/multi_factor_authentication
3. ケーズデンキ通販サイトに不正ログイン - 約 300 万円の不正注文（Security NEXT）
   https://www.security-next.com/152800
4. ネット取引サービスに不正ログイン、株式不正売却も - SMBC 日興証券（Security NEXT）
   https://www.security-next.com/149297
5. 「Amazon を不正利用された」――SNS 上で報告相次ぐ 「二段階認証を突破された」などの声も（ITmedia News）
   https://www.itmedia.co.jp/news/articles/2309/14/news152.html
6. 不正ログイン被害、10 回の試行で 3 件がログイン許す - セシール（Security NEXT）
   https://www.security-next.com/146246
7. 「エン転職」にパスワードリスト攻撃 - 約 25 万人がアクセス許す（Security NEXT）
   https://www.security-next.com/145012
8. 英語検定試験「TOEIC」の申込サイトに大量のログイン試行（Security NEXT）
   https://www.security-next.com/142803
9. Have I Been Pwned?（HaveIBeenPwned.com）
   https://haveibeenpwned.com/
10. Passkeys（FIDO アライアンス）
    https://fidoalliance.org/passkeys/?lang=ja
11. FIDO 認証＆パスキー総復習（認証の仕組みやパスキー登場までの経緯）（LINE ヤフー株式会社）
    https://techblog.yahoo.co.jp/entry/2023080730431354/
12. パスキーのセキュリティについて（Apple）
    https://support.apple.com/ja-jp/102195
13. パスワードの代わりにパスキーでログインする（Google）
    https://support.google.com/accounts/answer/13548313?hl=ja

コラム：そのショッピングサイト、本物ですか？

インターネットが普及している現代において、それを悪用し、偽警告によるインターネット詐欺やフィッシングによる個人情報等の詐取などの犯罪が発生していることはご存知のことと思います。[1] それでは、偽物のショッピングサイトがインターネット上に数多く存在し、その被害や相談が年々増加していることをご存知でしょうか。

例として、2023 年 12 月 21 日、消費者庁は、人気ブランドの女性用衣料品等を販売すると称する偽サイトに関する注意喚起を行いました。[2] これは、SNS 等で、人気ブランドロゴが使用された女性用衣料品広告が表示され、同広告からアクセスしたショッピングサイトで商品を注文したところ、当該ブランドのものではない商品が届いたという相談が相次いだものです。

日本サイバー犯罪対策センター（以下、JC3）が 2023 年 10 月に公表した「悪質なショッピングサイト等に関する統計情報（2023 年上半期）」によると、一般社団法人セーファーインターネット協会の悪質 EC サイトホットライン[3] に通報された 2023 年上半期における件数は 23,674 件となっています。[4] これは、2022 年上半期 12,830 件、2022 年下半期 15,988 件と比べると、強い増加傾向にあることが分かります。本コラムでは、偽物のショッピングサイトにフォーカスを当てて、その危険性や対策について、説明していきます。

【偽物のショッピングサイトとは】

まず、偽物のショッピングサイトとはなにか、について説明します。

これは、金銭やクレジットカード情報、個人情報の詐取や非正規品の販売等を目的として設置されたショッピングサイトのことで、警察庁では、実在する Web サイトに似せた「偽サイト」、金銭を騙し取ることを目的とした「詐欺サイト」と区別しています。[5] 本コラムでは、表記による区別はせず、「偽サイト」として表記します。

偽サイトに関しては、インターネット上で買い物をされる方は誰しもがその被害に遭うおそれがあります。想定される直接的な被害の例として以下が挙げられます。

- 金銭やクレジットカード情報、個人情報を詐取される
- 実在サイトの認証情報（ログイン ID やパスワード）を詐取される
- 購入した商品が届かない、または、偽ブランド品や非正規品等が届く

また、間接的な被害として以下のような事例もあります。

- フリマアプリ等で出品している商品を偽サイトの商品として無断転載される

これは、偽サイトの運営者らは、プログラムを用いて、フリマアプリ等を巡回して情報を集めます。そして、半ば自動的に掲載している情報を偽サイトに転載しています。そのため、偽サイトに掲載された商品の説明文や画像は、転載元の情報と同じ内容となっていることも多くあります。無断で転載されたからといって、金銭やクレジットカード情報、個人情報を詐取されることはありませんが、場合によっては、犯罪グループの一員であると取られかねません。

では、どのようにして対策をすればいいのでしょうか。

【対策】

被害に遭わないための対策には、偽サイトの特徴を知り、偽サイトかどうかを疑うことです。

偽サイトの特徴の例として以下が挙げられます。

- 極端な値引きしている、セール期間の残り時間が表示されている
- 架空の購入情報が刻々と更新され、在庫数が減少する
- 商品ラインナップが不自然（例：衣料品販売サイトなのに、電動工具を販売しているなど）
- 会社概要が記載されていない、掲載されていても会社名や住所、連絡先が実在しない、または、実在する別の企業等の情報が掲載されている
- 連絡先情報が限られているまたは一切提供されていない
  （電話番号がない、連絡先がフリーメールアドレス、問い合わせフォームのみ提供）
- プライバシーポリシー、利用規約、返品ポリシーが不明瞭または存在しない
  （文書が Web サイト上で見つからない、または内容があいまいで消費者の権利が不明確）
- 支払い方法が限定されている（銀行振込のみ、クレジットカードのみ）
  または、他の決済方法を選択しても、後から銀行振込やクレジットカードへ変更される
- サイトを褒めている口コミの日本語に違和感がある
- 口コミやレビューが見当たらない、または明らかに偽造されている
  （商品やサイトに関する顧客のフィードバックがない、または提供されているレビューが一方的で不自然）
- ドメイン名が奇妙または有名ブランドの名前を模倣している
  （正規のブランド名に似ているが微妙に異なるドメイン名を使用している）
- URL に見慣れないドメイン（「.xyz」、「.org」、「.top」等）が含まれている、サイトの運営元の企業から案内されているドメインと異なる

セール期間の残り時間や架空の購入情報を表示しているのは、ユーザーに「早く買わないと」等と、冷静さを欠いた状態で注文をさせることが目的であると考えられます。加えて、銀行振込における振込先口座として、違法に売買された外国人名義の銀行口座が使用される事例が多くあります。なお、偽サイトへ誘導する方法として、なりすましメールや SNS 上での投稿、検索サイトにおける検索結果、インターネット広告を悪用しているケースもありますので、どのような媒体であっても注意が必要です。

また、フリマサイト等に出品した商品の無断転載を防ぐ手段は確立されていませんが、犯罪に加担しているととられないためにも、商品説明文や商品画像に出品しているフリマサイト等の名称を明記すること、無断転載を制限する文言を掲載しておくことが有用ではないかと考えます。

しかし、**偽サイトの特徴を理解していても、偽サイトかどうかを正確に見分けることは困難です。**そもそも偽サイトが本物そっくりに偽装している点や、ドメインについても Punycode と呼ばれる特殊な文字エンコードを悪用（URL の一部を形の似た別の文字に入れ替える）した場合、見た目上ドメインが本物のドメインと同じに見えてしまう点[6]等により、不信な点に気づくことが難しくなっています。

そのため、Web サイトの危険性を確認することができる無料のサービスを利用するという方法もあります。例えば、「SAGICHECK」[7] という Web サイトの危険性を確認することができる無料のサービスが存在します。このサービスは、世界各国で展開される「CheckMyLink」という取り組みの一環として提供されています。JC3 は、収集した偽サイト情報を ScamAdviser（オランダに拠点を持つ

Ecommerce Operations B.V.が運営）に提供しており、「SAGICHECK」では、ScamAdviserを含む、複数の団体等の情報を基に Web サイトの危険性を判断しています。[8]

Web サイト「SAGICHECK」

この「SAGICHECK」に Web サイトの URL を入力することで、Web サイトの危険性を確認することができます。

Web サイト「SAGICHECK」での確認結果の例

ただし、「SAGICHECK」で確認した結果は必ずしも正確であるとは限らないため、最終的には、自身で偽サイトの特徴を踏まえた上で、判断する必要があります。

【最後に】

偽サイトの被害に遭わないためには、偽サイトの特徴を知ることが重要ですが、その大前提として、「私に限って偽サイトには騙されない」という考え方をやめて、「誰しもが被害に遭うおそれがある」という考え方へのアップデートが必要なのだと思います。

また、偽サイトとはちょっと異なりますが、ショッピングサイトに掲載されている商品の金額が「￥」表記でありながら、日本円（JPY）ではなく、中国人民元（CNY）で決済された事例もあります。[9] ネットショッピングをするときは、Web サイト内を注意深くチェックするようにしてください。

本コラムがその一助となれば幸いです。

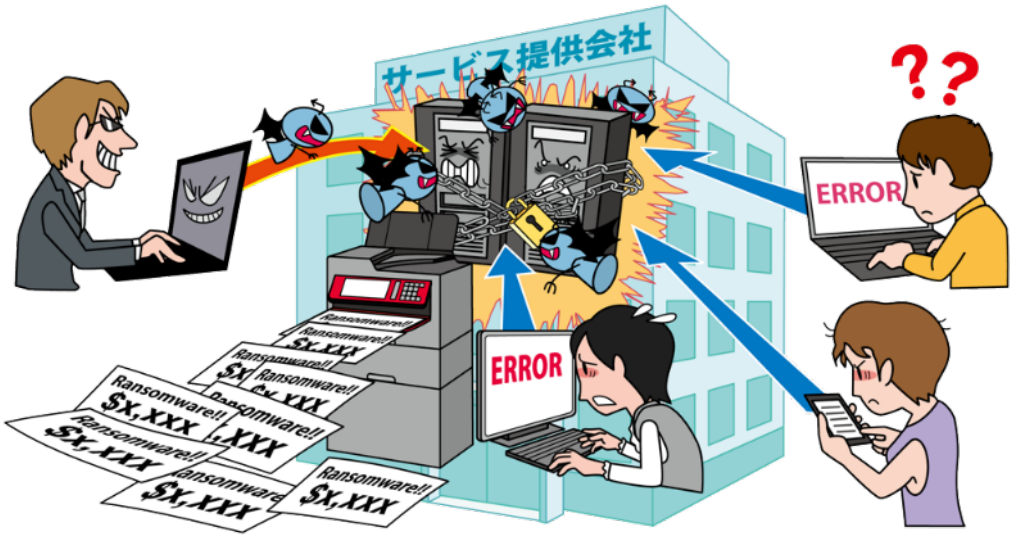
参考資料

1. 偽セキュリティ警告（サポート詐欺）対策特集ページ（IPA）
   https://www.ipa.go.jp/security/anshin/measures/fakealert.html
2. 人気ブランドの女性用衣料品等を販売すると称する偽サイトに関する注意喚起（2023 年 12 月 21 日）（消費者庁）
   https://www.caa.go.jp/notice/entry/035632/
3. 一般社団法人セーファーインターネット協会 悪質 EC サイトホットライン（一般社団法人セーファーインターネット協会）
   https://www.saferinternet.or.jp/akushitsu_ec_form/
4. 悪質なショッピングサイト等に関する統計情報（2023 年上半期）（2023 年 10 月 16 日）（日本サイバー犯罪対策センター）
   https://www.jc3.or.jp/threats/topics/article-515.html
5. 「偽サイト」「詐欺サイト」に注意！（警察庁）
   https://www.npa.go.jp/bureau/cyber/countermeasures/fake-shop.html
6. パスワード管理アプリ「KeePass」の偽サイトが Google 広告によって検索結果のトップに表示される事態が発生（Gigazine）
   https://gigazine.net/news/20231020-malvertising-attack-punycode-keepass/
7. SAGICHECK（SAGICHECK）
   https://sagicheck.jp
8. ScamAdviser(SAGICHECK)への協力（2023 年 3 月 1 日）（日本サイバー犯罪対策センター）
   https://www.jc3.or.jp/news/2023/20230301-488.html
9. その「￥」表示は本当に日本円の表示ですか？ （国民生活センター）
   https://www.kokusen.go.jp/pdf/n-20230419_2.pdf

2. 情報セキュリティ 10 大脅威（組織）

1位 ランサムウェアによる被害

～組織の規模や業種は関係なし！次の標的はあなたの組織かも？～



ランサムウェアとは、Ransom と Software を組み合わせた造語であり、ウイルスの一種である。攻撃者は PC やサーバーをランサムウェアに感染させ、様々な脅迫により金銭を要求する。さらに、攻撃者は複数の脅迫を組み合わせることで、攻撃を受けた組織がシステムを復旧するために金銭を支払うことを検討せざるを得ない状況を作り出そうとする。攻撃者は組織の規模や業種に関係なく攻撃を行う点にも注意が必要である。[1]

＜攻撃者＞

- 組織的犯罪グループ
- 犯罪者

＜被害者＞

- 組織
- 個人

＜脅威と影響＞

攻撃者は PC やサーバーをランサムウェアに感染させた後、以下のような脅迫を行う。

① PC やサーバーのデータを暗号化し、業務の継続を困難にする。その後、データを復元することと引き換えに、金銭要求の脅迫をする。

② 重要情報を窃取し、金銭を支払わなければ窃取した情報を公開すると脅迫する。

③ 金銭を支払わなければ、ランサムウェアに感染したことを被害者の利害関係者等に連絡すると脅迫する。

④ 金銭を支払わなければ DDoS 攻撃（Distributed Denial of Service Attack：分散型サービス妨害攻撃）を仕掛けると脅迫する。

また、これらを組み合わせた「二重脅迫」や「四重脅迫」も確認されている。

ランサムウェアに感染すると、データの暗号化や重要情報の窃取等の被害に遭い、さらにその調査や復旧に多くの費用と時間が掛かる。また、業務やサービス提供の停止による損失や取引先からの信頼失墜の被害につながるおそれもある。広く利用されているサービスがランサムウェアに感染すると、社会に大きな影響を与えることになる。

＜攻撃手口＞

◆脆（ぜい）弱性を悪用しネットワークから感染させる

OS やアプリケーション等のソフトウェアの脆弱性対策をしないままインターネットに接続されている機器に対して、VPN 等の脆弱性を悪用し、インターネット経由で PC やサーバーをランサムウェアに感染させる。

◆公開サーバーに不正アクセスして感染させる

意図せず外部公開されているポート（リモートデスクトップポート等）に不正アクセスしてランサムウェアに感染させる。

◆メールから感染させる

メールの添付ファイルや、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。

◆Web サイトから感染させる

Web サイトの脆弱性等を悪用して、ランサムウェアをダウンロードさせるように改ざんした Web サイトや攻撃者が用意した Web 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。

＜事例または傾向＞

◆ランサムウェア感染による業務停止

2023 年 7 月、名古屋港統一ターミナルシステムにランサムウェア感染による障害が発生した。システム専用のプリンターから脅迫文書が印刷された。サーバー再起動で復旧できないことを確認ののち、愛知県警察本部サイバー攻撃対策隊に通報した。その後、物理サーバー基盤および全仮想サーバーが暗号化されていることが判明した。これはリモート接続機器の脆弱性を悪用した不正アクセスが原因でランサムウェアに感染したと考えられ、約 2 日半ターミナルでの作業の停止を余儀なくされた。[2,3]

◆ランサムウェア感染によるサービス提供停止

2023 年 6 月、システム開発およびクラウドサービス事業者であるエムケイシステムが、データセンターのサーバーに不正アクセスされ、ランサムウェアに感染したことを公表した。この感染により、データが暗号化され、社会保険労務士向けクラウドサービス「社労夢」をサービス提供できなくなった。約 3,400 人のユーザーに影響があり、オンプレミスで動作するパッケージ版を代替として提供した。

また、インフラ設備の再構築費用やセキュリティ対策費用のコスト増、影響があったユーザーへの 6 月の請求を停止するといった対応により、業績予想を修正することとなった。[4,5]

◆VPN 経由で侵入、ランサムウェアを横展開

2023 年 1 月、ならコープが 2022 年 10 月にランサムウェアによる攻撃を受けていたことを公表した。攻撃者はネットワーク機器の脆弱性を悪用して VPN 経由で侵入し、内部情報を収集していた。この結果、攻撃者にランサムウェアを横展開され、サーバー11 台でほとんどのデータが暗号化されていた。暗号化されたデータには約 49 万人の個人情報が含まれるものの、外部への流出は確認されていないとのこと。また、データは復元できなかったが、バックアップを取っていたデータベースは感染を逃れていたため、復元することができた。[6,7]

＜対策と対応＞

組織（経営者層）

- 組織としての体制の確立
  - ・インシデント対応体制を整備し対応する ※

組織（システム管理者、従業員）

- 被害の予防
  - ・インシデント対応体制を整備し対応する ※
  - ・表 1.4「情報セキュリティ対策の基本」を実施
  - ・メールの添付ファイル開封や、メールや SMS のリンク、URL のクリックを安易にしない ※
  - ・多要素認証の設定を有効にする
  - ・提供元が不明なソフトウェアを実行しない
  - ・サーバーやクライアント、ネットワークに適切なセキュリティ対策を行う ※
  - ・共有サーバー等へのアクセス権の最小化と管理の強化
  - ・公開サーバーへの不正アクセス対策
  - ・適切なバックアップ運用を行う ※
- 被害を受けた後の対応
  - ・適切な報告／連絡／相談を行う ※
  - ・適切なバックアップ運用を行う ※
  - ・復号ツールの活用 [8]
  - ・インシデント対応体制を整備し対応する ※

＜身代金の支払いと復旧業者の選定について＞

原則、身代金を支払わずに復旧を行う。身代金を支払ってもデータの復元や情報の流出を防げるとは限らない。また、対応を依頼した業者が攻撃者との裏取引で身代金を支払うことで復旧した場合、事実上、自組織が攻撃者に資金提供をしたとみなされるおそれもある。対応を依頼する業者の選定 [9] にも注意が必要である。

※巻末「共通対策」を参照

2位 サプライチェーンの弱点を悪用した攻撃

～ビジネスもセキュリティ対策も関係組織で二人三脚を～

商品の企画、開発から、調達、製造、在庫管理、物流、販売までの一連のプロセス、およびこの商流に関わる組織群をサプライチェーンと呼ぶ。このような「ビジネス上の繋がり」を悪用した攻撃は、自組織の対策のみでは防ぐことが難しいため、関係組織も含めたセキュリティ対策が必要な脅威と言える。また、ソフトウェア開発のライフサイクルに関与する全てのモノ（ライブラリ、各種ツール等）や人の繋がりをソフトウェアサプライチェーンと呼ぶ。このような「ソフトウェアの繋がり」を悪用した攻撃もまた脅威であり、対策が必要である。

＜攻撃者＞

- 組織的犯罪グループ
- 犯罪者

＜被害者＞

- 組織（自組織／自組織に関わる組織）

＜脅威と影響＞

組織には、サプライチェーンとの関係性が何らかの形で存在する。例えば、取引先や委託先、ソフトウェアやサービスの提供元、提供先と多岐に渡る。強固なセキュリティ対策が行われていて、直接攻撃が困難な標的組織に対し、そのサプライチェーンの脆弱な部分を攻撃者が攻撃する。その脆弱な部分を経由して間接的および段階的に標的組織を狙う。外部に対しては強固なセキュリティ対策を行っていても、サプライチェーン上の取引先や導入しているソフトウェア、サービス等を足掛かりとされることで、攻撃者の侵入を許すおそれがある。

攻撃を受けた場合、機密情報の漏えいや信用の失墜等、様々な被害が発生する。また、自組織が攻撃を受け、足掛かりとされることで取引相手に損害を与えてしまい、取引相手を失ったり、損害賠償を求められたりするおそれがある。

＜攻撃手口＞

◆取引先や委託先が保有する機密情報を狙う

標的組織よりもセキュリティが脆弱な取引先や委託先、国内外の子会社等を攻撃し、その組織が保有する標的組織の機密情報等を窃取する。

◆ソフトウェア開発元やMSP（マネージドサービスプロバイダー）等を攻撃し、標的組織を攻撃するための足掛かりとする

ソフトウェアサプライチェーンを悪用した攻撃を行う。例えば、購入したソフトウェアやサービス、またはソフトウェアの開発元やサービスの提供元に対して、脆弱性等を悪用して不正アクセスを行い、当該ソフトウェアやサービスを改ざんしてウイルスを仕込む。標的組織が調達したソフトウェアやサービスの利用開始時や顧客への提供開始時またはバージョンアップ時にウイルスに感染させる。

他にも、企業システムの運用、監視等を請け負う事業者（MSP）が利用する資産管理ソフトウェア等にウイルスを仕込み、MSP を利用する複数の顧客にウイルスを感染させる手口もある。

＜事例または傾向＞

◆業務委託先業者からの顧客情報漏えい

2023 年 1 月、複数の保険会社が、業務委託先から顧客の個人情報が流出したことを公表した。原因は業務委託先の、適切なセキュリティ対策がされていないサーバーへの不正アクセスであった。流出した個人情報が海外の Web サイトに掲載されていたことで被害が発覚した。流出の規模は保険会社により異なるが、多いところでは約 130 万人分に及んでおり、調査や対処に追われた。[1,2,3,4]

◆委託先のシステムを介して不正アクセス、顧客情報漏えい

2023 年 11 月、LINE ヤフーは、同社の保有する顧客情報が漏えいしたことを公表した。漏えいした顧客情報は、ユーザーに関する情報が約 30 万件、取引先等に関する情報が約 9 万件、従業員等に関する情報が約 5 万件としている。情報漏えいの原因は第三者による社内システムへの不正アクセスであった。これは委託先企業である NAVER Cloud 社のさらに委託先の企業で従業員の PC がウイルス感染したことを発端として、同社のシステムを介して行われていた。[5]

◆提携先企業に不正アクセス、顧客情報漏えい

2023 年 11 月、メッシュ Wi-Fi を提供する JCOM が顧客情報を漏えいしたことを公表した。当該サービスは米国 Plume Design 社が提供元であり、同社の提携先のモバイルアプリのアクセスログサーバーが不正アクセスされたことが原因であった。これにより約 23 万件の顧客の氏名と約 5 千件の顧客のメールアドレスが漏えいした。[6]

＜対策と対応＞

組織（経営者層）

- 被害の予防
  - ・インシデント対応体制を整備し対応する ※

組織（自組織で実施）

- 被害の予防
  - ・情報管理規則の徹底
    調達先や業務委託先等、契約時に取引先の規則を確認する。
  - ・セキュリティ評価サービス（SRS）を用いた自組織のセキュリティ対策状況の把握
  - ・信頼できる委託先、取引先、サービスの選定
    商流に関わる組織、サービスの信頼性評価（ISMAP など）、品質基準を検討し、複数候補を検討する。
  - ・契約内容の確認
    組織間の取引や委託契約における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、賠償に関する契約条項を盛り込む。
  - ・委託先組織の管理
    委託元組織が委託先組織のセキュリティ対策状況と情報資産の管理の実態を定期的に確認できる契約とすることが重要である。
    また、業務委託自体が適切であるかも検討する。
  - ・納品物の検証
    納品物に組み込まれているソフトウェアの把握と脆弱性対策を実施する。ソフトウェアの把握や管理においては SBOM の導入を検討する。[7]
- 被害を受けた後の対応
  - ・インシデント対応体制を整備し対応する ※
  - ・被害への補償

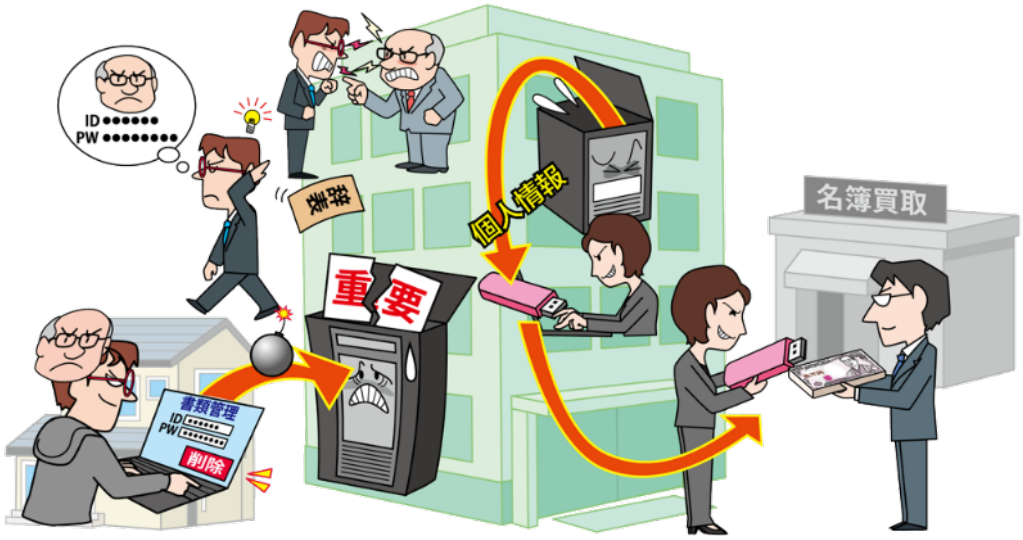
組織（自組織に関わる組織と共に実施）

- 被害の予防
  - ・取引先や委託先との連絡プロセスの確立
  - ・取引先や委託先の情報セキュリティ対応の確認、監査
  - ・情報セキュリティの認証取得
    ISMS、P マーク、SOC2 等を取得し、定期的に見直して必要な運用を維持する。
  - ・公的機関等が公開している資料の活用 [8,9,10]
- 被害を受けた後の対応
  - ・適切な報告／連絡／相談を行う ※

※巻末「共通対策」を参照

3位 内部不正による情報漏えい等の被害

～組織の情報を狙っているのは身内かも！？不正をゆるさない体制作りを～



従業員や元従業員等の組織関係者による機密情報の持ち出しや社内情報の削除等の不正行為が発生している。また、組織内の情報管理の規則を守らずに情報を持ち出し、紛失や情報漏えいにつながるケースもある。組織関係者による不正行為は、組織の社会的信用の失墜や、損害賠償や業務停滞等による経済的損失を招く。また、不正に取得された情報を使用した組織や個人も責任を問われる場合がある。

＜攻撃者＞

- 組織関係者（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＞

悪意を持った組織関係者が、金銭受領や転職先での悪用、組織への私怨等を動機として、組織が保有する技術情報や顧客情報等の重要情報の持ち出しや第三者への提供、不特定多数が閲覧できる場所への公開、情報の削除や改ざん等の不正行為を行うことがある。また、自宅等の社外で作業するために組織の情報管理の規則を守らず情報を外部へ持ち出し、情報漏えいするケースもある。

不正に扱われた情報の重要性や被害規模によっては、組織の社会的信用の失墜や、顧客等への損害賠償や損失補填、復旧作業等による経済的損失が発生し、組織の競争力の大幅な低下につながる。その結果、組織経営の根幹を揺るがすおそれがある。

また、自組織に持ち込まれた情報が不正に取得されたものであることを知りつつ使用した場合、刑事罰の対象になることもある。

＜攻撃手口＞

◆アクセス権限の悪用

付与された権限を悪用し、組織の重要情報に対して窃取や不正操作を行う。必要以上に高いアクセス権限が付与されている場合、より重要度の高い情報が狙われ、被害が大きくなるおそれがある。また、複数人で端末を共用している場合、他人のアカウントで不正アクセスされることもある。

◆在職中に割り当てられたアカウントの悪用

離職者が在職中に使用していたアカウントが削除されていない場合、それを使用して組織の情報にアクセスする。

◆内部情報の不正な持ち出し

組織の情報を、USB メモリーや HDD 等の外部記憶媒体、メール、クラウドストレージ、スマホカメラ、紙媒体等を利用し、外部に不正に持ち出す。

＜事例または傾向＞

◆顧客情報を持ち出し、名簿業者に販売

2023 年 10 月、NTT ビジネスソリューションズは、同社に勤務していた元派遣社員が顧客情報の不正な持ち出しを行っていたことを公表した。同派遣社員は 2013 年 7 月から 2023 年 1 月の間に、自身が運用に関わっていたコールセンターのシステムに、管理者アカウントを悪用して不正アクセスし、少なくとも 69 組織の顧客情報 928 万件を USB メモリーにコピーして持ち出していた。持ち出した顧客情報を名簿業者に販売し、1,000 万円以上を対価として受け取っていたとみられ、逮捕された。[1,2,3]

◆前職場が保有する名刺情報を転職先に提供

2023 年 9 月、ワールドコーポレーションの元従業員が、個人情報保護法違反（不正提供）等の疑いで警視庁に逮捕された。本従業員は同業他社に転職する直前に、転職元の名刺情報管理システムにログインするための ID とパスワードを転職先の従業員に共有していた。不正に取得された名刺情報は転職先の営業活動に使用され、成約事例もあったという。[4,5]

◆元勤務先に不正アクセスし、社内情報を削除

2023 年 1 月、共立電気計器の元従業員が電子計算機損壊等業務妨害罪等の疑いで警視庁に逮捕された。本従業員は退職後に元同僚や元上司の ID やパスワードを悪用し、社内ネットワークやクラウドに不正アクセスして、人事や技術、顧客に関する情報を削除していた。人間関係を理由に退職しており、嫌がらせが目的だったとみられている。データ復旧には約 660 万円を要した。[6]

＜対策と対応＞[7]

組織（システム管理者）

● 被害の予防

・基本方針の策定

「不正のトライアングル[8]」を意識して基本方針を策定し、情報取扱ポリシーの作成、内部不正者に対する懲戒処分等を規定した就業規則等の整備をする。[9] なお、組織内での対策推進は、経営層の積極的な関与が重要である。内部不正対策の責任は経営者にあり、最高責任者である経営者が総括責任者の任命並びに管理体制および実施策の承認を行い、組織横断的な管理体制を構築する必要がある。

・資産の把握、対応体制の整備

情報資産を把握し、その重要度をランク付けした上で重要情報の管理者を定める。

・重要情報の管理、保護

重要情報の利用者 ID およびアクセス権の登録・変更・削除に関する手順を定めて運用する。従業員の異動や離職に伴う不要な利用者 ID 等は直ちに削除する。また、それらの適切な管理、定期的な監査を実施する。さらに、利用者 ID の共用禁止等の処置を検討する。DLP（情報漏えい対策）等のツールの導入を検討する。

・物理的管理の実施

重要情報の格納場所や重要情報を扱う執務室への入退室を管理する。USB メモリー、スマートフォン、プリンター等の外部媒体は利用制限を行い、持ち出しや持ち込みの管理をする。また、記録媒体の廃棄を行う際には、適切なデータ消去の運用を実施する。消去できない場合は媒体の物理的な破壊も検討する。また、リース品は初期化してから返却する。

・情報リテラシー、モラルを向上させる ※

・人的管理およびコンプライアンス教育の徹底

従業員には秘密保持義務を課す誓約書に署名させ、定期的に教育を実施する。

● 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、証跡を記録し、監視する事で早期検知に努める。また、監視していることを従業員に周知することで不正を予防する。

● 被害を受けた後の対応

・適切な報告／連絡／相談を行う ※

・インシデント対応体制を整備し対応する ※

・内部不正者に対する適切な処罰の実施

※巻末「共通対策」を参照

4位 標的型攻撃による機密情報の窃取

～攻撃手口は様々、隙を作らない対策を～

標的型攻撃とは、特定の組織（企業、官公庁、民間団体等）を狙う攻撃のことであり、機密情報等を窃取することや業務妨害を目的としている。攻撃者は社会の変化や働き方の変化に合わせて攻撃手口を変える等、組織の状況に応じた巧みな攻撃手法で機密情報等を窃取しようとする。

＜攻撃者＞

- 組織的犯罪グループ
- 犯罪者

＜被害者＞

- 組織（企業、官公庁、民間団体、研究機関、教育機関等）

＜脅威と影響＞

特定の企業や官公庁、団体等に狙いを定め、機密情報等の窃取や業務妨害を目的として組織内部へ潜入する標的型攻撃が確認されている。攻撃者は PC やサーバーをウイルスに感染させたり不正アクセスしたりして組織内部に侵入し、ウイルスやツール等を用いて情報の窃取や破壊活動等を行う。組織内部に潜伏し、長期にわたり活動を行うケースもある。

窃取された機密情報が悪用された場合、企業の事業継続や国家の安全保障等に重大な影響を及ぼすおそれがある。また、データ削除やシステム破壊により企業等の活動が妨害されたり、その企業のサプライチェーンに属する関連組織への攻撃の踏み台にされたりすることもあり、組織の規模や業種に関わらず狙われるおそれがある。

＜攻撃手口＞

◆メールへのファイル添付やリンクの記載

メールの添付ファイルやメール本文に記載されたリンク先にウイルスを仕込み、そのファイルを開封させたり、リンクにアクセスさせたりすることで PC をウイルスに感染させる。メール本文や件名、添付ファイル名は業務や取引に関連するように偽装され、実在する組織の差出人名が使われる場合もある。また、メールのやり取りを複数回行い被害組織の従業員や職員を油断させ、不信感を抱かれにくいようにする手口もある。（やり取り型攻撃）

◆Web サイトの改ざん

攻撃者は標的組織が頻繁に利用する Web サイトを調査し、改ざんしておく。そして、従業員や職員がその Web サイトにアクセスすることで PC がウイルスに感染する。（水飲み場型攻撃）

◆不正アクセス

標的組織が利用するクラウドサービスや Web サーバー、VPN 装置等の脆弱性を悪用し、不正アクセスを行い、そこから更に組織内部へ侵入する。

また、認証情報等を窃取した上で、正規の経路で組織のシステムへ再侵入することもある。

＜事例または傾向＞

◆複数回のやり取りを伴う標的型メール攻撃

2023 年 10 月、東京大学は標的型攻撃メールにより教員が使用していた PC がウイルスに感染し、PC 内の情報を窃取された形跡があることを公表した。2022 年 7 月に実在する組織の担当者を騙った人物から講演依頼のメールが届き、日程調整のため教員がやりとりをしている中でメールに記載された URL をクリックしたところ、ウイルスに感染した。最終的に「講演が中止になった」との連絡があったため、教員は被害に気付かなかった。この攻撃により、教職員や学生等の個人情報や過去の試験問題等計 4,341 件が流出したおそれがある。[1,2]

◆JAXA にサイバー攻撃=不正アクセス、機微情報含まず

2023 年 11 月、宇宙航空研究開発機構（JAXA）がサイバー攻撃を受け、内部のネットワークに不正アクセスされていたことが分かった。不正アクセスを受けたのは一般業務用の管理サーバーであり、機微情報は含まれていないと説明している。

不正アクセスは同年 6 月に修正されたネットワーク機器の脆弱性を悪用されたものとみられる。外部機関から通報を受けた JAXA は文部科学省に報告し、一部のネットワークを切り離した上で、調査を行っている。[3,4]

◆ネットワーク貫通型攻撃に注意

2023 年 8 月、IPA は企業や組織のネットワークとインターネットとの境界に設置されるセキュリティ製品の脆弱性が狙われ、ネットワーク貫通型攻撃として APT 攻撃に利用されていると注意喚起を行った。[5]

ネットワーク内部へ不正アクセスされた場合、保有情報の漏えいや改ざん、他組織への攻撃の踏み台（中継）になるおそれがあるため、日々の確認や平時の備えが大切である。加えて、同年 5 月に経済産業省が公開した「ASM（Attack Surface Management）導入ガイダンス～外部から把握出来る情報を用いて自組織の IT 資産を発見し管理する～」の活用も有効である。[6]

＜対策と対応＞

組織（経営者層）

- 組織としての体制の確立
  - ・インシデント対応体制を整備し対応する ※

組織（セキュリティ担当者、システム管理者）

- 被害の予防／対応力の向上
  - ・情報の管理と運用規則策定
    情報は暗号化する等、管理や運用の規則を定めて運用する。
  - ・サイバー攻撃に関する継続的な情報収集
  - ・情報リテラシー、モラルを向上させる ※
  - ・インシデント対応の定期的な訓練を実施
    関係者やセキュリティ業者、専門家と迅速に連携する対応方法や連絡方法を整備する。
  - ・サーバーやクライアント、ネットワークに適切なセキュリティ対策を行う ※
  - ・アプリケーション許可リストの整備
  - ・取引先のセキュリティ対策実施状況の確認
  - ・海外拠点等も含めたセキュリティ対策の向上
- 被害の早期検知
  - ・サーバーやクライアント、ネットワークに適切なセキュリティ対策を行う ※
- 被害を受けた後の対応
  - ・インシデント対応体制を整備し対応する ※

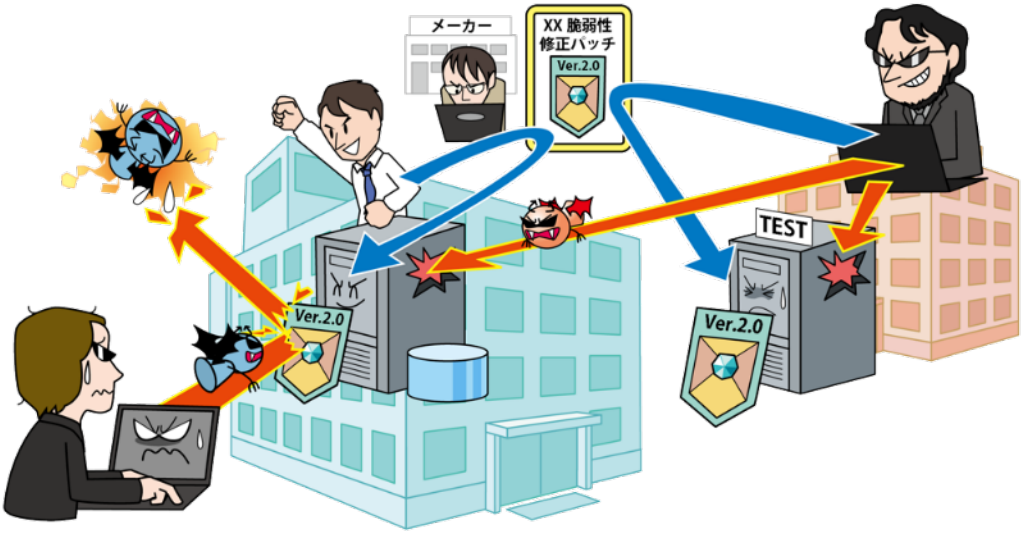
組織（従業員、職員）

- 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
  - ・メールの添付ファイル開封や、メールや SMS のリンク、URL のクリックを安易にしない ※
- 被害を受けた後の対応
  - ・インシデント対応体制を整備し対応する ※

※巻末「共通対策」を参照

5位 修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）

～脆弱性対策情報が公開されたら即時対応を～



ソフトウェアの開発ベンダー等が 脆弱性対策情報を公開する前に、脆弱性を悪用した攻撃が行われることがある。このような攻撃は、ゼロデイ攻撃と呼ばれている。ゼロデイ攻撃が行われた場合、ウイルス感染や情報漏えい等の直接の被害に留まらず、事業やサービスが停止するなど、多くのシステムやユーザーに被害が及ぶことがある。そのため、脆弱性対策情報が公開された場合は、早急な対応が求められる。

＜攻撃者＞

- 組織的犯罪グループ

＜被害者＞

- 組織、個人（ソフトウェアの利用者）
- 組織（システム管理者）

＜脅威と影響＞

OS やアプリケーション等のソフトウェアの脆弱性が発見されると、開発ベンダー等がその脆弱性の調査や分析を行う。そして、脆弱性の修正プログラム（パッチ）や回避策、さらには緩和策等の脆弱性の対策に関する情報を公開する。しかし、脆弱性対策情報の公開前に攻撃者が脆弱性の存在を知った場合、攻撃コード等を作成し、当該ソフトウェアの脆弱性を悪用したゼロデイ攻撃を行うおそれがある。

ゼロデイ攻撃が行われると、ウイルス感染や情報漏えい、さらには Web ページやファイルの改ざん等の被害が起こり、事業やサービスが停止してしまうおそれがある。また、多くのシステムやユーザーに利用されているソフトウェアの脆弱性がゼロデイ攻撃に悪用された場合、その被害が広範囲に及び、社会が混乱状態に陥るおそれもある。

なお、世の中に知られていない脆弱性を悪用した攻撃を受けた場合、被害者は攻撃されたことに気付かないおそれがある。また、仮に被害者が攻撃されたことに気付いたとしても、脆弱性対策情報が公開されていないために、適切な対応を取れないこともある。脆弱性対策情報は公開されているが、ユーザーが対策する前の N デイ脆弱性（詳細は組織の脅威「脆弱性対策情報の公開に伴う悪用増加」を参照すること。）を悪用するケースとは異なり、攻撃されないための対策は難しい。

＜攻撃手口＞

◆ソフトウェアの脆弱性の悪用

開発ベンダー等が脆弱性対策情報を公開する前に、攻撃者は脆弱性を悪用して攻撃する。

悪用の手口としては、脆弱性毎に様々なものがあるが、例えば、通信プロトコルの脆弱性を悪用した DDoS 攻撃（分散型サービス妨害攻撃）、アプリケーションの脆弱性を悪用した簡易プログラム

（スクリプト）の実行、OS の脆弱性を悪用した特権アカウントの作成等がある。

＜事例または傾向＞

◆HTTP/2 プロトコルの脆弱性を利用したゼロデイ攻撃

2023 年 8 月、HTTP/2 プロトコルに存在する脆弱性を狙った大規模な DDoS 攻撃が確認され、一連の攻撃で 1 秒間に 3 億 9,800 万件を超えるリクエストが発生したと報告されている。これは、これまで最も規模が大きいとされていた 2022 年の、1 秒間に 4,600 万件のリクエストが発生したケースをはるかに上回る規模の攻撃である。この攻撃は、HTTP/2 ラピッドリセット攻撃と呼ばれており、Web サーバー、プロキシサーバー、ロードバランサーや Web API 等、HTTP/2 をサポートする多くのソフトウェアに影響を与える。この脆弱性の判明を受け、影響を受けるソフトウェアの開発ベンダー間の協調の下に情報共有が進められた。そして、各社が定例のセキュリティアップデートを公開するいわゆる「パッチチューズデー」にあたる 2023 年 10 月 10 日に、パッチやアップデートの提供等も始まった。[1]

◆ファイル圧縮ソフト「WinRAR」に存在する脆弱性を利用したゼロデイ攻撃

広く利用されているファイル圧縮ソフトの「WinRAR」に複数の脆弱性が存在しており、2023 年 4 月以降に、一部の脆弱性がゼロデイ攻撃に悪用されていることがわかった。アーカイブファイル内の画像ファイルやテキストファイルのプレビューを行おうとすると、同名のフォルダ内に配置されたスクリプトを実行させることが可能になるという脆弱性であった。開発元である「RARLAB」は、2023 年 8 月 2 日に脆弱性の修正をした「WinRAR 6.23」をリリースしている。[2]

◆Cisco Systems 製品へのゼロデイ攻撃

2023 年 10 月、Cisco Systems は「Cisco IOS XE」に、リモートから認証がなくとも特権アカウントを作成できる脆弱性があり、9 月中旬よりゼロデイ攻撃行われていると公表した。同社は、顧客のサポート中に本脆弱性を確認しており、本製品の利用者に対して、開発ベンダー等が推奨する対策を講じるとともに、侵害を受けていないか確認するように呼びかけている。[3]

＜対策と対応＞

組織（経営者層）

- 被害の予防
  - ・インシデント対応体制を整備し対応する ※

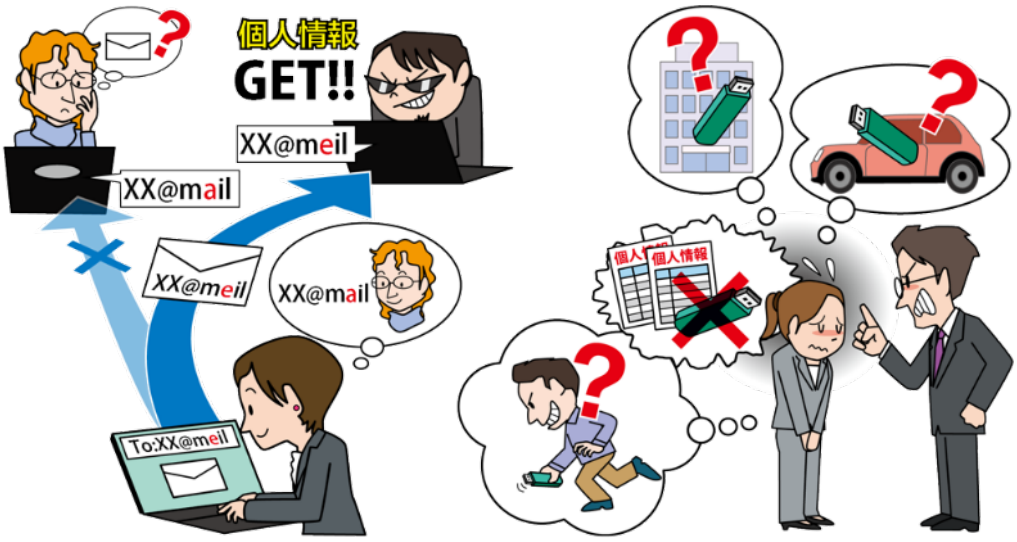
組織（ソフトウェアの利用者、システム管理者）

- 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、対応体制の整備
  - ・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
    修正プログラムや回避策の提供が迅速である製品や開発ベンダーを利用し、サポート対象のソフトウェアを使う。
  - ・利用するソフトウェアの脆弱性情報の収集と周知、対策状況の管理
  - ・サーバーやクライアント、ネットワークに適切なセキュリティ対策を行う ※
- 被害の早期検知
  - ・サーバーやクライアント、ネットワークに適切なセキュリティ対策を行う ※
- 修正プログラムのリリース前の対応
  - ・回避策や緩和策の適用
  - ・当該ソフトウェアの一時的な使用停止
    場合によってはサービスの停止も検討する。
- 修正プログラムリリース後の対応
  - ・修正プログラムの適用
    必要に応じて回避策、緩和策を無効化する。
- 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
  - ・適切な報告／連絡／相談を行う ※

※巻末「共通対策」を参照

6位 不注意による情報漏えい等の被害

～その設定、本当に大丈夫？確認は慎重に！～



システムの設定ミスによる非公開情報の公開や、個人情報を含んだ記憶媒体の紛失等、不注意による個人情報等の漏えいが度々発生し、組織はその対応に追われている。一度でも不注意により個人情報が漏えいしてしまうと、漏えいした組織の信用、信頼に大きな影響を与えるおそれがある。

＜加害者（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＞

組織において、サービス内容や業務内容によっては個人情報や機密情報を従業員が取り扱うことがある。その際に、組織の情報管理に関する規程の不備や、従業員のセキュリティ意識の低さ、情報リテラシーの低さ、不注意によるミス等によってこれらの重要情報を漏えいさせてしまう事件が発生している。

漏えいした情報が悪用されると詐欺被害等の二次被害に繋がるおそれがある。また、社会的信用が失墜し、それに伴う経済的損失が発生するおそれがある。

＜要因＞

◆情報を取り扱う人の情報リテラシーの低さ

自身が扱う情報の機密性や重要性等を理解していないため、不用意に外部へ情報漏えいしてしまう。例えば、重要情報が記載されたメールの宛先の間違いや重要情報が入った端末の紛失等がある。また、重要情報を私的に利用して外部の Web サイト等に公開することで情報漏えいとなる。

◆情報を取り扱う際の本人の状況

体調不良や多忙等の状況により、情報を取り扱う従業員の注意力が散漫になり、メールの誤送信等のミスによる情報漏えい事故を起こしてしまう。

◆組織規程および情報を取り扱うプロセスの不備

組織で規定している情報の取り扱いプロセスに不備があると情報漏えいが起きやすい。例えば、外部に情報を持ち出す際の確認手順や作業時の確認手順等に関するプロセスの不備が挙げられる。

◆誤送信を想定した偽のメールアドレスの存在

組織が利用しているドメインと似たドメインのメールアドレス（ドッペルゲンガードメイン）を、第三者があらかじめ準備している。従業員がそのメールアドレスに誤送信したタイミングで情報が漏えいする。

＜不注意による情報漏えいの例＞

- メールの誤送信（宛先誤り、To/Cc/Bcc の設定間違い、添付ファイル間違い等）
- Web サイトの設定不備（重要情報のマスキングの不備、公開ファイルや参照権限の誤り、クラウドの設定の誤り等）
- 外部サイトへの安易な機密情報の入力
- 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＞

◆意図しないメールアドレスに個人情報を送信

2023 年 2 月、鹿児島大学はメーリングリスト内のメールアドレスの誤記により、意図しない宛先へ学内外 829 名の個人情報を送信してしまったことを公表した。本来、「@gmail.com」とすべきドメインを「@gmai.com」としたメールアドレスをメーリングリストに誤登録してしまったことにより、個人情報が記載されたメールが本来の宛先ではなく、ドッペルゲンガードメイン宛に送られてしまった。同学では誤りを確認してからドッペルゲンガードメイン宛のメール送信の停止とメーリングリストに誤登録されたメールアドレスの削除を行った。[1]

◆設定ミスによる個人情報漏えい

2023 年 12 月、大阪市コミュニティ協会は住吉区役所から委託業務を受けた際に利用していた Google フォームに入力された個人情報を、第三者が閲覧できる状態にあったことを公表した。原因は、入力した個人情報を閲覧できる設定が ON になっていたが、フォーム作成時に、回答後に表示される画面の確認をしないまま運用を開始したことであった。発覚した要因は Google フォームに入力を済ませたユーザーからの指摘によるもので 11 月に連絡があったものの指摘に気が付いたのは 12 月であった。連絡に気が付いた直後から Google フォームを修正し、関係者への連絡を完了させており、再発防止に取り組むとしている。[2]

◆個人情報をコピーした USB メモリーを紛失

2023 年 12 月、天草市立牛深市民病院で業務再委託先担当者が 132 人分の個人情報を含むデータを USB メモリーにコピーして持ち出した。会社にて作業を行う際に USB メモリーの紛失に気が付いた。紛失した可能性のある場所を探すが見つからず、紛失に気が付いてから 3 日後に警察に紛失届を提出した。紛失届の提出から数日後、担当者が使用していたレンタカーを再度捜索した結果、車内から USB メモリーが発見された。天草市では関係する患者に対して報告と謝罪を行っている。[3]

＜対策と対応＞

組織（当事者）

- 被害の予防（被害に備えた対策含む）
  - ・情報リテラシー、モラルを向上させる ※
  - ・確認プロセスに基づく運用
  - ・特定の担当者に業務が集中しない体制の構築
  - ・取り扱う情報の重要度を規定し、それに合わせた運用を行う
  - ・情報の保護（暗号化、認証）、機密情報の格納場所の把握、可視化
  - ・DLP（情報漏えい対策）製品の導入
  - ・外部に持ち出す情報や端末の制限
    外部との適切なファイル送受信の運用を検討する（クラウドストレージ利用、暗号化等）
  - ・メールの誤送信対策等の導入
    外部へのメールを一時滞留させたり、メール送信時にクロスチェックする運用にしたりする。
  - ・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
  - ・適切な報告／連絡／相談を行う ※
  - ・インシデント対応体制を整備し対応する ※

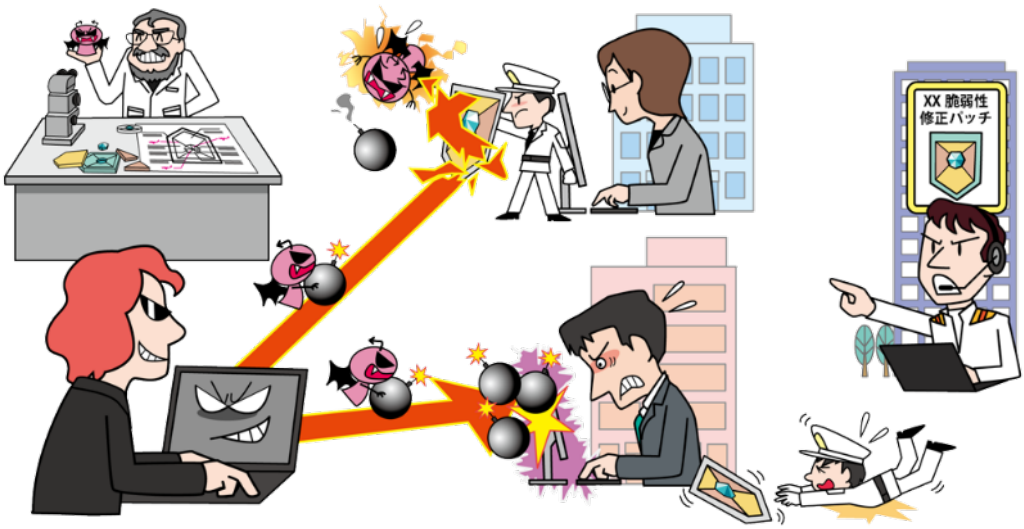
個人/組織（被害者）

- 被害を受けた後の対応
  - ・クレジットカードの停止
  - ・適切な報告／連絡／相談を行う ※

※巻末「共通対策」を参照

7位 脆弱性対策情報の公開に伴う悪用増加

～放置せず、傷口が広がる前に速やかな処置を～



ソフトウェアやハードウェアの 脆弱性対策情報の公開は、脆弱性の脅威や対策の情報を製品の利用者に広く呼び掛けられるメリットがある。一方で、攻撃者はその情報を悪用し、脆弱性対策を講じていない当該製品を使用したシステムを狙って攻撃を行うおそれがある。近年では脆弱性関連情報が公開されるとすぐに攻撃コードが流通し、攻撃が本格化するまでの時間がますます短くなっている。

＜攻撃者＞

- 組織的犯罪グループ

＜被害者＞

- 組織（開発ベンダー）
- 組織、個人（製品利用者）

＜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の修正プログラム（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や対策方法、暫定対策情報を公開し、当該ソフトウェアの利用者へ対策を促す。

一方、攻撃者は、公開された脆弱性対策情報を基に攻撃コード等を作成し、パッチ適用等の対策を実施する前のソフトウェアに対して、脆弱性を悪用した攻撃を行う。

これによる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おり、特にネットワーク機器(VPN 機器等)や CMS（プラグインを含む）といった広く利用されている製品の脆弱性の場合、攻撃コード等が公開されると被害が広範囲に拡散するおそれがある。

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時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（N デイ脆弱性）を悪用

パッチや回避策が公開される前に発見されたソフトウェアの脆弱性をゼロデイ脆弱性と呼ぶ。（詳細は組織の脅威「修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）」を参照すること。）一方、パッチや回避策が公開され、そのパッチの適用や回避策を講じるまでの期間（N 日）の脆弱性を N デイ脆弱性と呼ぶ。特に、ソフトウェアの管理が不適切な企業は、未対応の時間（N 日）が長くなるため、 被害に遭うリスクが大きくなる。

また、脆弱性が攻撃可能であることを実証する PoC（実証コード）が公開され、攻撃に悪用されることもある。

◆公開されている攻撃ツールを使用

公開された脆弱性に対する攻撃ツールは短期間で作成され、ダークウェブ上の Web サイト等での販売や、攻撃サービスとして提供されたりすることがある。また、誰でも利用可能なオープンソースのツールに脆弱性を利用する機能が実装され、それを悪用されることもある。

＜事例または傾向＞

◆ソフトウェアの修正版公開後に攻撃活動の増加

2023 年 10 月 25 日（米国時間）、Apache Software Foundation は同社の Apache ActiveMQ および Apache ActiveMQ Legacy OpenWire Module にリモートからコード実行が可能となる脆弱性を対策したバージョンを公表した。本脆弱性は技術情報や実証コードが公開されており、Rapid7 によると 10 月 27 日に脆弱性を悪用したと見られるランサムウェアの活動を同社の複数の顧客で確認していた。また、NICT（情報通信研究機構）の NICTER におけるダークネット観測網では、同脆弱性に関連した通信を 10 月 27 日頃から観測し、11 月 26 日頃には更なる通信の増加が確認されてボットとみられる感染活動を観測した。[1,2,3]

◆VPN 機器の脆弱性が断続的な攻撃の対象に

2023 年 5 月、Array Networks が提供する VPN アプライアンス「Array AG シリーズ」の脆弱性を悪用した標的型攻撃が断続的に観測されていることを JPCERT コーディネーションセンターが注意喚起した。対象の脆弱性（CVE-2022-42897、CVE-2023-28461）はそれぞれ 2022 年 9 月、2023 年 3 月に修正されているが、海外拠点も標的となっており、自組織の海外拠点における対策や侵害調査を行うことも推奨されている。[4,5,6]

◆脆弱性を修正した機器へ継続的な攻撃

2023 年 5 月 19 日（米国時間）、Barracuda Networks は同社のメールセキュリティ製品の Email Security Gateway アプライアンス（ESG）にリモートからシステムコマンドが実行可能となる脆弱性があることを特定し、翌日の 5 月 20 日に修正パッチを公開した。しかし、本脆弱性の修正対応後も、特定の組織では攻撃者による新たなバックドアの設置や、ネットワーク上での横展開等、継続的な攻撃活動が確認されている。同社では脆弱性の最初の悪用は 2022 年 10 月とし、侵害された組織に対し、アプライアンスの交換を推奨している。また、米連邦捜査局（FBI）および IPA、JPCERT コーディネーションセンターにおいても注意喚起を行っており、本脆弱性の修正パッチを済ませた組織でも、追加の侵害調査を行う事を推奨した。[7,8,9,10]

＜対策と対応＞

組織（経営者層）

- 被害の予防
  - ・インシデント対応体制を整備し対応する ※

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
  - ・サーバーやクライアント、ネットワークに適切なセキュリティ対策を行う ※
  - ・脆弱性関連情報の収集と対応
  - ・一時的なサーバー停止等

    パッチや回避策をすぐに適用できない場合を想定して、システム公開前に一時的なサーバー停止等の回避策を検討しておく。
- 被害の早期検知
  - ・サーバーやクライアント、ネットワークに適切なセキュリティ対策を行う ※
- 被害を受けた後の対応
  - ・適切な報告／連絡／相談を行う ※
  - ・インシデント対応体制を整備し対応する ※

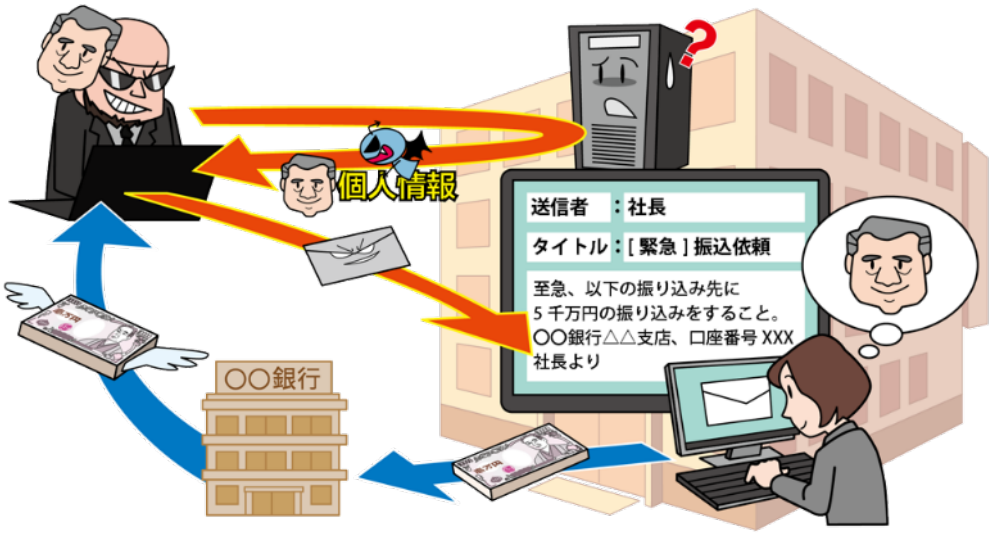
組織（開発ベンダー）

- 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
  - ・サーバーやクライアント、ネットワークに適切なセキュリティ対策を行う ※
  - ・脆弱性発見時の対応手順の作成
  - ・脆弱性情報を迅速に発信する仕組みの整備

※巻末「共通対策」を参照

8位 ビジネスメール詐欺による金銭被害

～組織までも振り込め詐欺の標的に～



悪意のある第三者が標的組織やその取引先の従業員等になりすましてメールを送信し、あらかじめ用意した偽の銀行口座に金銭を振り込ませるサイバー攻撃が行われている。この攻撃は、組織の従業員を標的にした振り込め詐欺とも言えるもので、ビジネスメール詐欺（Business E-mail Compromise：BEC）と呼ばれている。

＜攻撃者＞

- 組織的犯罪グループ

＜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＞

企業の従業員や経営者、または、取引先の関係者等になりすました攻撃者が、標的組織の従業員等へメールを送信する。それらのメールは本物のメールに酷似しているため、メールの受信者はなりすましメールを受信したと気付けないおそれがある。

その結果、メールの受信者は、あらかじめ攻撃者が用意した口座に送金をしてしまい、金銭的な被害が発生してしまう。

＜攻撃手口＞

◆取引先との請求書の偽装

取引先等と請求に関わるやり取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に差し替えた偽の請求書等をメールで送り付け、振り込ませる。

このとき、攻撃者は取引に関わるメールのやり取りをなんらかの方法で事前に盗み見ており、取引や請求に関する情報、関係している従業員のメールアドレスや氏名等を入手していることがある。

◆経営者等へのなりすまし

組織の経営者等になりすまし、同組織の従業員に攻撃者が用意した口座へ金銭を振り込ませる。この時、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

ウイルス感染や不正ログイン等により、従業員のメールアカウントを乗っ取り、取引実績がある組織の担当者へ偽の請求等を送り付け、攻撃者の用意した口座に金銭を振り込ませる。

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付きにくい。

◆社外の権威ある第三者へのなりすまし

弁護士等の社外の権威ある第三者になりすまし、組織の財務担当者等に対して攻撃者が用意した口座へ金銭を振り込ませる。

◆詐欺の準備行為と思われる情報の窃取

ビジネスメール詐欺の準備行為として、標的組織の情報を窃取する場合がある。例えば、攻撃者が標的組織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、組織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＞

◆メールと電話を併用したなりすまし

2023 年 8 月、サイバー情報共有イニシアティブ（J-CSIP）が公表したレポートにおいて、同年 5 月にメールと電話を組み合わせた BEC が行われていたことが報告された。攻撃者は標的組織の会長になりすまし、同組織の海外関連会社の社長に対して機密プロジェクトの連絡等と称したメールを送信していた。さらに、同日に専務になりすまし、メールのフォローアップを口実に電話で連絡をしていた。攻撃者は発信元番号を何らかの方法で同組織の代表番号に偽装し、さらに専務の声を模倣していた。なお、被害者は会話からなりすましに気が付き指摘したところ、一方的に通話を切られ、金銭的な被害等は発生しなかった。

生成AI技術を用いて作成したディープフェイクの音声が悪用された可能性もあるため、J-CSIP は類似した手口に警戒するよう注意喚起をした。[1]

◆信頼できる取引先を騙るメール詐欺

2023 年 12 月、スリー・ディー・マトリックスは、支払口座の変更依頼が書かれた、取引先の名を騙るメールに従い、虚偽の銀行口座に振り込みをしたことを公表した。その後も同様の振り込みをし、合計二回で総額 2 億円を振り込んだことも公表した。その取引先とは創業以来の付き合いがあり、信頼関係があったため、同社は振込先口座の変更依頼の理由を直接電話で確認していなかった。そのため、当面の再発防止策として、送金プロセスの見直しなどを挙げている。[2]

＜対策と対応＞

● 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

・BEC への認識を深める

・ガバナンスが機能する業務フローの構築

金銭が絡む手続きをする際は、複数人で審査、承認をする業務フローを構築し、個人の判断や業務命令だけでは完結させないようにする。

・メールに依存しない業務フローの構築

電話等で事実確認をする。

・メールの電子署名の付与（S/MIME や PGP）

・DMARC の導入

攻撃者の自社ドメインを騙ったなりすましメールを顧客が受信できないようにする。

・パスワードを適切に運用する ※

詐欺の準備行為への対策としてメールアカウントのパスワードを適切に運用する

＜メールの真正性の確認＞

・メールだけでなく複数の手段での事実確認

振込先口座に変更等がある場合は、メール以外に電話等の方法で直接取引先に確認をする。または、金融機関にその口座の名義等を確認する。

・普段とは異なるメールに注意する

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。

・判断を急がせるメールに注意

至急の対応を要求する等、担当者に真偽の判断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策定しておく。

● 被害を受けた後の対応

・適切な報告／連絡／相談を行う ※

・インシデント対応体制を整備し対応する ※

・メールアカウントの設定を確認する

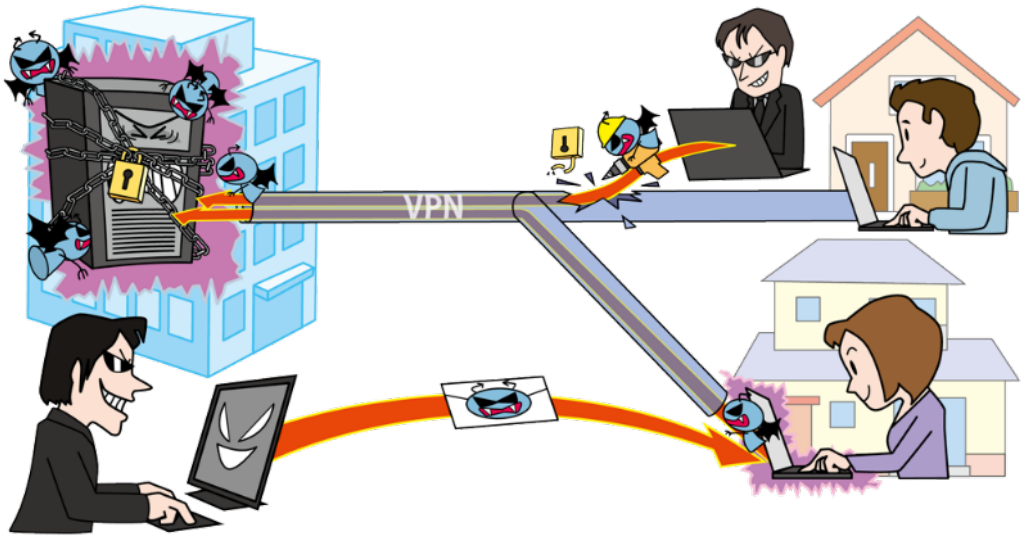
攻撃者による不正な転送設定やメール振り分けの設定等がされていないか確認する。

・パスワードを適切に運用する ※

※巻末「共通対策」を参照

9位 テレワーク等のニューノーマルな働き方を狙った攻撃

～狙われ続けるテレワーク環境、セキュリティ対策を～



2020 年以降、新型コロナウイルス感染症（COVID-19）の世界的な蔓延（まんえん）に伴い、感染症対策の一環として政府機関がニューノーマルな働き方の１つであるテレワークを推奨している。勤労形態としてテレワークが活用され、VPN サービス等が本格的に活用される中、それらを狙った攻撃が引き続き行われている。

＜攻撃者＞

- 組織的犯罪グループ
- 犯罪者

＜被害者＞

- 組織
- 組織（テレワーカー）

＜脅威と影響＞

2020 年以降、新型コロナウイルス感染症対策に伴い、組織によっては自宅等から VPN 経由で社内システムにアクセスしたり、Web 会議サービスを利用して自組織または他組織と会議を行ったりする働き方、いわゆるテレワークが定着してきた。それに伴い、自宅のネットワークの利用や私有の PC やスマートフォンの利用（BYOD）が求められている。それに伴い攻撃者はこのような業務環境を引き続き狙っている。

業務環境に脆弱（ぜいじゃく）性があると、Web 会議をのぞき見されたり、テレワーク用の端末にウイルスを感染させられたり、ウイルスに感染した端末から社内システムに不正アクセスされたりするおそれがある。

＜攻撃手口と発生要因＞

◆テレワーク用製品の脆弱性の悪用

VPN 等のテレワーク用に導入している製品の脆弱性や設定ミス等を悪用し、社内システムに不正アクセスしたり、PC 内の業務情報等を窃取したりする。また、Web 会議サービスの脆弱な設定を悪用し、Web 会議をのぞき見する。

◆テレワーク移行時のまま運用している脆弱なテレワーク環境への攻撃

規則の整備やセキュリティ対策が不十分な状態で、急いでテレワークへ移行したまま運用されている脆弱なテレワーク環境を攻撃する。

◆私有端末や自宅のネットワークを利用

適切なセキュリティ対策が施されていない私有端末でテレワークを行うと、ウイルス感染したり、ソフトウェアの脆弱性を悪用されたりして、業務情報や認証情報を窃取されるおそれがある。また、組織支給の端末を利用している場合でも、自宅やシェアオフィスのネットワーク環境に適切なセキュリティ対策が行われていないと、情報を盗聴されるおそれがある。

＜事例または傾向＞

◆在宅勤務のために用意したリモートアクセス経路より侵入の疑い

2023 年 10 月、セイコーグループはランサムウェアによる被害で顧客や取引先担当者等の個人情報が流出したことを公表した。同社ではコロナ禍において在宅勤務のために用意したリモートアクセス経路より侵入されたものと見ている。データセンターや国内拠点の一部サーバー内部に保存されていたデータを暗号化され、同社含むセイコーウオッチおよびセイコーインスツルが保有する約 60,000 件の個人情報が外部に流出した。[1,2]

◆Web 会議サービスの脆弱性

各社がセキュリティアップデートを公開する「パッチチューズデー」に合わせて Web 会議サービスに影響する脆弱性対策情報が公開されることがある。Microsoft は 2023 年 10 月に、Teams に影響する脆弱性（CVE-2023-4863）を、Zoom は 2023 年 11 月に、Zoom Rooms に影響する脆弱性（CVE-2023-43590）を対策し、最新版リリースしている。このようなセキュリティ対策は定期的に行われており、最新版の製品を利用していない場合、攻撃を受けるリスクが高くなるため、利用者には迅速なアップデートが求められている。[3,4]

◆狙われ続けるテレワーク環境

警察庁によると、令和 5 年上半期におけるランサムウェア被害の感染経路として VPN 機器経由のものが 35 件で最も多く、全体の 71%を占めていた。次いでリモートデスクトップから侵入したものが 5 件で全体の 10%を占めていた。このように、テレワークに利用される機器等の脆弱性や強度の低い認証情報を悪用されたものが全体の約 82%を占めており、令和 4 年に引き続き 80%を超えた。[5,6]

＜対策と対応＞

個人（テレワーカー）

- 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
  - ・組織のテレワークの規則を遵守（使用する端末、ネットワーク環境、作業場所等）
- 被害を受けた後の対応
  - ・適切な報告／連絡／相談を行う ※

組織（経営者層）

- 組織としての体制の確立
  - ・インシデント対応体制を整備し対応する ※
    特に、テレワーク中のウイルス感染により PC が使用できない等、テレワーク環境ならではの連絡方法や対応手順を策定し、社員に周知しておく必要がある。
  - ・テレワークのセキュリティポリシーの策定

組織（セキュリティ担当者、システム管理者）

- 被害の予防（被害に備えた対策含む）
  - ・シンクライアント、VDI、VPN、ZTNA/SDP 等のセキュリティに強いテレワーク環境の採用
  - ・テレワークの規程や運用規則の整備
    組織支給端末と私有端末の違いを考慮する。また、テレワーク開始時の暫定的なセキュリティ対策や例外措置を見直す。
  - ・情報リテラシー、モラルを向上させる ※
  - ・サーバーやクライアント、ネットワークに適切なセキュリティ対策を行う ※
  - ・ネットワークレベル認証（NLA）を行う
  - ・多要素認証の設定を有効にする
- 被害の早期検知
  - ・サーバーやクライアント、ネットワークに適切なセキュリティ対策を行う ※
- 被害を受けた後の対応
  - ・インシデント対応体制を整備し対応する ※

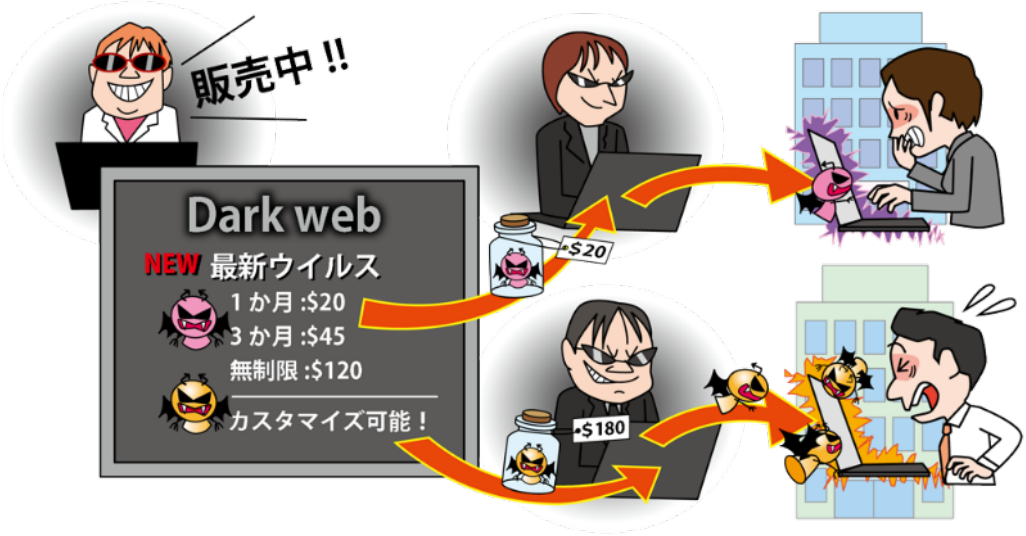
＜テレワーク関連サイトの紹介＞

IPA では「テレワークを行う際のセキュリティ上の注意事項」のページを公開している。このページでは、テレワークを行う際のセキュリティ上の注意事項に加え、テレワークから職場に戻る際のセキュリティ上の注意事項も解説している。また、IPA や他機関のテレワーク関連セキュリティ情報へのリンクも紹介しているので、参考にしていただきたい。[7]

※巻末「共通対策」を参照

10位 犯罪のビジネス化（アンダーグラウンドサービス）

～そのパスワード、すでに誰かが知っているかも？～



アンダーグラウンド市場では、アカウントの ID やパスワード、クレジットカード情報、ウイルスなどが売買され、あまり攻撃スキルがなくてもハッキングなどの犯罪行為を行えるようになっている。また、話題のサービスのアカウント情報などが売買されており、ユーザーはアカウントの管理等の対策に一層努める必要がある。

＜攻撃者＞

- 組織的犯罪グループ
- 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ツールやサービスがアンダーグラウンドで取り引きされている。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ツールやサービスとして、例えば、16SHOP というフィッシングサイトを作成するツールや、RaaS（Ransomware as a Service）、AaaS（Access as a Service）というビジネスモデル等がある。

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 攻撃をされたり、業務を妨害されたりする。

なお、アンダーグラウンドで取り引きされているサービスやツール等はダークウェブと呼ばれる、通常のブラウザでは検索できない Web サイト上に存在する場合がある。攻撃者は、特殊なブラウザを利用してそれらにアクセスしている。また、近年では匿名性の高いメッセージサービスのグループチャットを利用した取引も確認されている。

＜攻撃手口＞

◆ツールやサービスを購入した攻撃

アンダーグラウンドで購入したツールやサービス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。代表的なサービスとしてはランサムウェアを販売するサービスや、不正アクセスの手段を販売するサービスが確認されている。

◆認証情報を購入した攻撃

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、Web サービス等に不正ログインする。

◆サイバー犯罪に加担する人材の募集

サイバー犯罪は組織的に行われることもある。その人材はアンダーグラウンドの掲示板に高額な報酬を提示することで人材募集を行う。

＜事例または傾向＞

◆ChatGPT のアカウントも売買

2023 年 4 月、チェック・ポイント・リサーチは ChatGPT 有料アカウントの取引増加を警告した。有料アカウントはダークウェブ上で販売されており、悪意ある第三者がアカウントを購入した場合、正規ユーザーのアカウントを乗っ取ることができる。同社は、アカウントを乗っ取ることにより情報の漏えいにつながることを指摘しており、有料アカウントに紐づいているクレジットカード情報などの窃取が可能である。ダークウェブ上でアカウントを販売されているものの中には宣伝目的で最初にいくつかの有料アカウントを無料で提供し、巧妙に購入につなげようとしているものもある。[1,2]

◆国内製造業の情報がダークウェブに流出

2023 年 6 月、アイギステックは国内の主要製造業 30 社について、ダークウェブへのアカウント情報漏えい状況調査結果を発表した。結果として今回調査した 30 社全てでダークウェブ上にアカウント情報や機密文書がアップロードされていることが判明した。特に製造業は、過去調査した金融機関、行政機関の結果と比較すると情報漏えい件数やハッキング数等においてすべて上回っていた。[3]

◆月額でウイルスを販売。サポートもあり。

2023 年 10 月、Fortinet は情報窃取ウイルス「ExelaStealer」が登場したことを注意喚起した。このウイルスは Windows プラットフォームを標的にしたもので、クレジットカード等の情報を窃取する。月額や買い切りで利用する方法があり、ダークウェブ上で月額 20 ドルと、安価に提供されている。また、カスタマイズサービスも提供されており、更にビジネス化が進んでいる。[4]

＜対策と対応＞

攻撃に使用され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の他の脅威を参照すること。

組織（経営者層）

- 組織としての体制の確立
  - ・インシデント対応体制を整備し対応する ※

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（インターネットサービスプロバイダー）や CDN（コンテンツデリバリーネットワーク）等を利用する
  - ・システムの冗長化等の軽減策
  - ・Tor ノードの検知/ブロック
  - ・サーバーやクライアント、ネットワークに適切なセキュリティ対策を行う ※
- 被害の早期検知
  - ・ダークウェブの監視

    監視サービス等を用いて、自組織に影響のある攻撃情報や流出情報の存在を確認する
- 被害を受けた後の対応
  - ・適切な報告／連絡／相談を行う ※
  - ・通信制御（DDoS 攻撃元をブロック等）
  - ・Web サイト停止時の代替サーバーの用意と告知手段の整備
  - ・適切なバックアップ運用を行う ※
  - ・インシデント対応体制を整備し対応する ※

組織（PC 利用者）

- 被害の予防
  - ・情報リテラシー、モラルを向上させる ※
  - ・メールの添付ファイル開封や、メールや SMS のリンク、URL のクリックを安易にしない ※
  - ・サーバーやクライアント、ネットワークに適切なセキュリティ対策を行う ※
  - ・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
  - ・インシデント対応体制を整備し対応する ※

※巻末「共通対策」を参照

コラム：AIとうまく付き AI（あい）たい

人工知能（Artificial Intelligence、以下 AI）に関する話題を耳にすることが、日を追うごとに増しているのではないでしょうか。AI は、創造的な業務にも利用できる可能性が高く、人手不足対策や利益率向上等に有効な手段になると期待されています。[1] 特に、いわゆる生成 AI（質問や作業指示等に応じて文章や画像等を生成する AI サービス）に関しては、「大規模言語モデルに代表される「基盤モデル」と言われるタイプの AI の進化と社会実装は、新たな経済成長の起爆剤となりうる。」[2] という意見もあり、大きな期待が寄せられています。

試しにブラウザの検索エンジンで「生成 AI 業務利用」や「生成 AI 業務効率化」のようなキーワードで検索すると、企業での活用事例が多数見つかることから、日本企業への浸透が進んでいることがうかがえます。また、デジタル庁は、2023 年 8 月に中央省庁向けの生成 AI 活用ワークショップを開催しており、政府機関でも生成 AI 活用の気運が高まっています。[3]

さらに、2023 年 11 月、政府の「AI 戦略会議」では、政府や公的機関が保有するデータを国内の AI 開発企業に提供する枠組みがまとめられました。政府は、2024 年の提供開始を目指しており、生成 AI 活用促進の追い風となりそうです。[4,5]

一方、生成 AI を悪用した犯罪も行われています。2023 年 4 月には、ディープフェイク（AI を用いて、人物の動画や音声を人工的に合成する処理技術）を用いて誘拐された本人のように聞こえる音声を作成し、電話上の被害者に聞かせ、身代金を騙し取ろうとする「バーチャル誘拐」が発生しました。また、サイバー犯罪用の生成 AI ツールも登場し、スピアフィッシングやビジネスメール詐欺（BEC）等の実行を支援する「WormGPT」、「FraudGPT」がハッキングフォーラムで宣伝されています。[6]

続いて、生成 AI を悪用したとされる偽情報の拡散も発生しています。国内においては、2023 年 11 月に報道番組に似せて作られた岸田首相のディープフェイク動画が SNS 上で拡散され、大きなニュースとなりました。[7] 海外においては、2023 年 5 月にアメリカの国防総省付近で爆発が起きたとされるフェイク画像が、SNS で拡散されました。[8]

さらに、生成 AI を使えば、人が作成したかのような、自然に近い文章も作成できます。この機能を悪用して自動生成した偽の口コミを投稿すること等も可能になります。[9]

このように良いことにも悪いことにも利用できる生成 AI ですが、そもそも AI とは何でしょうか？

【AI って何だろう？】

AI は耳慣れた言葉ですが、実際のところ AI の定義は明確には定まっておらず、一説には「人間と同様の知識を実現させようという取り組みやその技術」[10] とされています。AI は、機械学習や深層学習（ディープラーニング）といった技術に支えられており、深層学習によって、以下の技術を実現しています。

・画像認識・・・画像や動画から文字や顔等を認識、検出する技術
・音声認識・・・音声情報からテキスト形式への変換や音声の特徴を捉えて発声者を識別する技術
・自然言語処理・・・人間が日常的に使う自然言語をコンピュータに認識・処理させる技術

上記技術に人間がインプット（入力）を与えることで AI が自動的にアウトプット（出力）を提供し、利用者に様々なメリットをもたらします。

【AI のメリット】

AI を活用するメリットとしては、労働力不足の解消（労働力の補填や人間の負担の軽減）や生産性の向上（作業スピードの短縮やヒューマンエラーの防止）等が挙げられます。今まで人間が行ってきた業務の一部をデータ化したものをインプットとして AI に対して与えることで、AI が自動的に判断し、レポートを生成する等、業務に応じたアウトプットを提供します。このように AI に任せることにより、人間はそれ以外のクリエイティブな業務に専念できるようになります。また、人間が行うにはリスクがある作業を AI に任せることも可能です。例えば、工事現場等において、仮設足場を設置して高所で行わなければいけない作業を、AI を搭載したドローンに作業してもらうことで人間が怪我をするリスクを低減することができます。[11]

【生成 AI を活用したサービス】

AI を活用することで業務等が便利になることがわかりました。それでは、今注目されて生成 AI はどのようなサービスがあり、どのように活用されているのでしょうか。まず、生成 AI を活用したサービスとして、有名なものは OpenAI 社が提供している ChatGPT や Google 社が提供している Gemini（旧、Bard）が挙げられます。これらのサービスは対話型 AI とも呼ばれ、質問事項等をテキストでインプットすると、その内容に応じた回答をテキストでアウトプットしてくれます。

また、地方公共団体においても生成 AI の活用は進められています。例えば、神奈川県横須賀市では、2023 年 4 月から ChatGPT の全庁的な活用実証を行い、同年 6 月に結果報告を行いました。職員の更なるスキルアップやノウハウを積極的に他自治体に伝える等前向きな利用が検討されています。[12] また、三重県桑名市では、2026 年 4 月の開校を計画している小中一貫校において生成 AI を活用して、校歌の作詞・作曲を行う計画を進めています。[13]

【生成 AI 利用における注意点】

ここでは、生成 AI を利用・提供する上での注意点を簡単に紹介したいと思います。

・AI は間違える

チャットボット等の生成 AI に質問を投げかけると、簡潔でもっともらしい回答を得ることができます。しかし、その回答には誤りが含まれていることがあります。回答が本当に正しいのかどうか、自身で確認することが大切です。また、プログラムのソースコードをアウトプットする生成 AI サービスを利用する場合には、アウトプットされたコードが脆弱でないかどうか等を確認することも大切です。

・AI はおしゃべり

生成 AI を利用する際、機密情報をインプットすることにより、その生成 AI が機密情報を学習に利用し、第三者に機密情報が漏えいする可能性があります。生成 AI にインプットする機密情報や個人情報が、生成 AI でどのように取り扱われるのか規約や仕様を確認することが大切です。契約のプランによって学習の有無が異なる場合もあります。また、所属組織において機密情報や個人情報の取り扱いについて規則が決められている場合は、その規則に従うことも重要です。

・AI は騙される

生成 AI は、悪意を持った利用者により、サービス提供者の意図せぬ回答をアウトプットすることがあります。また、学習データに利用するインプットに誤りが含まれていると、誤った学習をしてしまい、誤ったアウトプットを行います。これらを防止するために、生成 AI を活用したサービスを提供する場合、サービスの公開前に、アウトプットの正当性検証を実施するとともに、プロンプトインジェクション（AI に対して特殊な質問をインプットし、AI 開発者が想定していない機密情報等の情報を窃取する攻撃）やデータポイズニング（悪意のあるデータを AI に学習させ、AI 開発者が想定していない動作をさせる攻撃）等への対策も実施しましょう。

また、その他の注意点として、トラブルが発生した時、責任の所在を明らかにすることが難しい等が挙げられます。例えば、現在、生成 AI に関する法律は国内にはまだないため、現時点では地盤となる法整備が固まっていない中での利用になってしまうリスクがあります。また、生成 AI がどのようなプロセスでトラブルとなる判断をしたかが明確に提示されないリスクがあります。これについては、「説明可能な AI（XAI）」が昨今注目されています。[14]

【まとめ】

経済発展や社会問題の解決に寄与する可能性がある一方でリスクも秘めている生成 AI。うまく付き合っていくためにも、正しい最新情報を入手していくことが求められます。

【参考：AI に関する活用ルール検討の動向】

AI の安全安心な活用が促進されるように、政府機関や団体からも情報発信が行われているため、ここからは、それらの動向についてご紹介します。

■広島 AI プロセス

2023 年 5 月の G7 広島サミットでの議論の結果を受けて、生成 AI に関する国際的なルールの検討を行うため、「広島 AI プロセス」が立ち上げられました。そして、同年 12 月には、G7 デジタル・技術担当大臣等により、高度な AI システムに対処するための初の国際的枠組みとされる「広島 AI プロセス包括的政策枠組み」が承認され、[15] 同枠組みにおいて、「全ての AI 関係者向けの広島プロセス国際指針」[16]（以下、国際指針）や「高度な AI システムを開発する組織向けの広島プロセス国際行動規範」[17]（以下、国際行動規範）が示されました。

国際指針では、AI システムの設計、開発、導入、提供および利用を確保するために、開発者と利用者の双方に対して適用されるべき 12 の指針が示されています。他方、国際行動規範では、開発者に対して、遵守するべき行動が示されており、内容としては、国際指針における第 1 から第 11 の指針を具体化したものとなっています。また、国際行動規範では、高度な AI システムに関するリスクやリスクに対処するための具体例等も示されています。

■欧州連合（EU）「AI 規則案（AI Act）」

2023 年 6 月、生成 AI を含む包括的な AI の規制案である「AI 規則案」が、欧州連合（EU）欧州議会本会議において賛成多数で採択されました。生成 AI の急激な進化と普及を受け、生成 AI に関する考え方や要求事項が追加で盛り込まれています。本規制では、AI を特性別にカテゴライズし、そのリスクレベルに応じた規制が適用されることになります。他の欧州規制同様に、欧州市場に関係する

日本企業をはじめ、域外企業が提供するAIも対象となり、違反時には全世界売上ベースでの制裁金が課されることになるとされています。[18]さらに、2023 年 12 月、EU 理事会（閣僚理事会）と欧州議会は、AI 規則案について暫定的な政治合意に達したと発表しています。[19]

■セキュア AI システム開発ガイドライン（Guidelines for secure AI system development）

英国国家サイバーセキュリティセンター（NCSC）等が作成したガイドラインであり、2023 年 11 月に公表されました。作成には、内閣サイバーセキュリティセンター（NISC）等も協力機関として参加しています。[20] このガイドラインは、広島 AI プロセスを補完するもので、AI を使用するシステムのプロバイダーによるセキュアな AI システムの構築を支援するための指針とされています。「セキュアな設計」、「セキュアな開発」、「セキュアな導入」および「セキュアな運用とメンテナンス」の 4 つのセクションに区分されており、各セクションにおいて、組織の AI 製品開発プロセスに対するリスク全般の低減に資する考察や緩和策が示されています。なお、本ガイドラインでは、AI コンポーネントのプロバイダーがサプライチェーンの先にいる利用者の「セキュリティ結果」の責任を負うとされています。

■AI 事業者ガイドライン案

総務省・経済産業省が共同事務局として、既存のガイドライン（「国際的な議論のための AI 開発ガイドライン案」[21]、「AI 利活用ガイドライン」[22]および「AI 原則実践のためのガバナンス・ガイドライン」[23]）について、諸外国の動向や新技術も踏まえつつ、統合・アップデートする形で、とりまとめが進められており、2024 年 3 月に公表が予定されています。[24,25]

■OWASP Top 10 for Large Language Model Applications

Web をはじめとするソフトウェアのセキュリティに関する啓発活動を行っている OWASP（Open Worldwide Application Security Project）にて作成されているドキュメントです。[26,27] 対象読者は、大規模言語モデル（LLM: Large Language Models）技術を活用したアプリケーション等の開発者やデータサイエンティスト等の専門家とされています。ドキュメントにおいては、プロンプトインジェクションをはじめとした、LLM に関する最も重大な 10 の脆弱性について、各脆弱性の概要、対策・緩和策、攻撃シナリオ等が示されています。

参考資料

1. 経済対策における主な AI 施策について（AI 戦略会議　第 6 回の資料 4、2023 年 11 月 7 日）（内閣府）
https://www8.cao.go.jp/cstp/ai/ai_senryaku/6kai/4aishisaku.pdf
2. AI ホワイトペーパー　～AI 新時代における日本の国家戦略～（2023 年 4 月）（自民党）
https://storage2.jimin.jp/pdf/news/policy/205802_1.pdf
3. 中央省庁向けに「働き方改革促進のための生成 AI 活用ワークショップ」を開催しました（デジタル庁）
https://www.digital.go.jp/news/5896883b-cc5a-4c5a-b610-eb32b0f4c175/
4. AI 学習データの提供促進に向けたアクションプラン（第 6 回　AI 戦略会議　資料 2）（内閣府）
https://www8.cao.go.jp/cstp/ai/ai_senryaku/6kai/2aidata.pdf
5. 生成 AI の学習に政府保有データを提供へ、国会図書館の蔵書や国の研究データも対象（日経クロステック）
https://xtech.nikkei.com/atcl/nxt/news/18/16244/
6. 2023 年上半期のサイバーセキュリティに対する脅威の動向：生成 AI の浮上（トレンドマイクロ株式会社）
https://www.trendmicro.com/ja_jp/research/23/j/cybersecurity-threat-2023-generative-ai.html
7. 生成AIで岸田首相の偽動画、SNSで拡散…ロゴを悪用された日テレ「到底許すことはできない」（読売新聞）
https://www.yomiuri.co.jp/national/20231103-OYT1T50260/
8. “米国防総省近くで爆発”偽画像拡散　株価一時下落する騒動に（NHK）
https://www3.nhk.or.jp/news/html/20230523/k10014075821000.html
9. そのロコミ、AI が書いたかも！？通販サイトに不審なレビュー（NHK）
https://www3.nhk.or.jp/news/html/20230711/k10014123961000.html
10. ソフトインフラレポート～DX の本質と産業変革に向けた提言～（2022 年 4 月）（日本政策投資銀行、東京大学松尾研究室）
https://www.dbj.jp/upload/investigate/docs/7ba43732d18265cda516c88b6c56ea03_1.pdf
11. 【完全版】AI のメリット・デメリットを解説！活用法や具体例 7 選を紹介（2023 年 9 月 13 日）（株式会社電算システム）
https://www.dsk-cloud.com/blog/merits-and-demerits-of-ai
12. ChatGPT の全庁的な活用実証の結果報告と今後の展開（市長記者会見）(2023 年 6 月 5 日)（横須賀市）
https://www.city.yokosuka.kanagawa.jp/0835/nagekomi/20230605_chatgpt2.html
13. 三重　桑名“新たに開校する小中一貫校校歌に AI を活用”全国初（NHK）
https://www3.nhk.or.jp/news/html/20230821/k10014169511000.html
14. その AI の思考、説明できますか？いま求められる Explainable AI（説明可能な AI）（NRIセキュアテクノロジーズ株式会社）
https://www.nri-secure.co.jp/blog/explainable-ai
15. 広島　AI　プロセス　G7　デジタル・技術閣僚声明（2023 年 12 月 1 日）（主要国首脳会議）
https://www.soumu.go.jp/hiroshimaaiprocess/pdf/document02.pdf
16. 全ての AI 関係者向けの広島プロセス国際指針（主要国首脳会議）
https://www.soumu.go.jp/hiroshimaaiprocess/pdf/document03.pdf
17. 高度な AI システムを開発する組織向けの広島プロセス国際行動規範（主要国首脳会議）
https://www.soumu.go.jp/hiroshimaaiprocess/pdf/document05.pdf
18. 欧州「AI 規則案」の解説（pwc）
https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/generative-ai-regulation03.html
19. EU、AI を包括的に規制する法案で政治合意、生成型 AI も規制対象に（独立行政法人日本貿易振興機構）
https://www.jetro.go.jp/biznews/2023/12/8a6cd52f78d376b1.html
20. セキュア AI システム開発ガイドラインについて（2023 年 11 月 28 日）（内閣府、内閣サイバーセキュリティセンター）
https://www8.cao.go.jp/cstp/stmain/20231128ai.html
21. 国際的な議論のための AI 開発ガイドライン案（総務省）
https://www.soumu.go.jp/main_content/000499625.pdf
22. AI 利活用ガイドライン（総務省）
https://www.soumu.go.jp/main_content/000624438.pdf
23. AI 原則実践のためのガバナンス・ガイドライン（経済産業省）
https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20220128_1.pdf
24. AI 事業者ガイドライン案　概要（2023 年 12 月 21 日）（総務省、経済産業省）
https://www8.cao.go.jp/cstp/ai/ai_senryaku/7kai/12gaidoraingaiyou.pdf
25. AI 事業者ガイドライン案（2024 年 1 月 19 日）（総務省、経済産業省）
https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/20240119_report.html
26. OWASP Top 10 for Large Language Model Applications（英語）（OWASP）
https://owasp.org/www-project-top-10-for-large-language-model-applications/
27. OWASP Top 10 for LLM（日本語）（OWASP）
https://github.com/owasp-ja/Top10-for-LLM/tree/main

「共通対策」

脅威の種類は多岐に渡るが対策に着目すると、共通しているものもある。このような対策は、複数の脅威に対して同時に行えるため効率的に対策を進めることができる。そこで、本項では表 1.6 の 7 つの対策について、「複数の脅威に有効な対策」として、注意事項、検討事項等も含めて具体的に解説する。

本項を読み、自身や自組織のセキュリティ対策を進める上で参考としてほしい。なお、共通対策を実施すれば完全な対策になるというものではない。各脅威の解説も参照し、対策を実施することが重要である。

表 1.6 複数の脅威に有効な対策集

対策	対象	
	個人	組織
パスワードを適切に運用する	○	○
情報リテラシー、モラルを向上させる	○	○
メールの添付ファイル開封や、 メールや SMS のリンク、URL のクリックを 安易にしない	○	○
適切な報告／連絡／相談を行う	○	○
インシデント対応体制を整備し対応する		○
サーバーやクライアント、ネットワークに 適切なセキュリティ対策を行う		○
適切なバックアップ運用を行う	○	○

パスワードを適切に運用する

個人や組織に関わらず、オンラインショッピングや SNS を利用したり、AppleID や Google アカウントを利用したりする機会が増え、様々な場面でパスワードの設定が必要になる。推測可能なパスワードの設定や不適切な管理をすると、攻撃者に不正ログインされやすくなってしまう。それでは適切な設定や運用とは具体的には何か？本項を読み、適切な対策を実施することでリスク低減の参考にしてほしい。

● 適切な設定をする[1]

・初期設定のままにしない

ネットワークカメラ等の IoT 機器では出荷の際、共通したパスワードが初期設定されている場合もあり、危険性が高いため変更する。

・推測されにくいパスワードを設定する[2]

推測されにくくするためには長く複雑にすることが有効である。内閣サイバーセキュリティセンター（NISC）が発行している「インターネットの安全・安心ハンドブック」[3]では、大文字と小文字のアルファベット、数字、記号を含んだ 10 桁以上を推奨している。パスワード作成は特に以下を意識するとよい。

① ID とパスワードを同じ文字列にしない
② 数字、アルファベット、記号等の複数の文字種を組み合わせる
③ 生年月日や名前を使わない
④ 連続した数字やアルファベットにしない
⑤ 単純な単語一語だけにしない

表 1.6　悪いパスワードの例

パスワード	悪い点
123456	連続した数字
Password p@ssw0rd	単純な単語や その類似系
taro1202	名前や誕生日
1qaz2wsx	キーボードの縦配列
qwerty	キーボードの横配列

・パスワードを使い回さない

個人情報や金銭情報を登録しているサービスや、登録したメールアドレスを ID として利用するサービスでは、特にパスワードの使い回しを避けた方がよい。複数のサービスで同じパスワードを利用していると、いずれかのサービスでパスワードの漏えいが起きたときに軒並み不正ログインされてしまう。また、使い回しを避けるためのパスワード作成方法を IPA で紹介しているのでパスワード作成時は参考にするとよい。[4]

・パスキーを利用する

パスキーと呼ばれる、生体情報等で認証を行う方式が提供されていれば利用するとよい。（詳細はコラムを参照すること）

● 適切な保管、運用を行う

・パスワードは他人に教えない

・PC やスマートフォンにパスワードを書いた付箋等のメモを貼らない

PC やスマートフォンを紛失した際に簡単に不正ログインされてしまう。覚えきれない場合は自宅で保管するノートに記録したり、パスワード管理ソフトを利用したりするとよい。

・複数人で使用する PC ではブラウザにパスワードを記憶させない

便利な機能だが複数人で利用している PC では、自分以外の人が自分になりすましてログインできてしまうので注意が必要である。

● 不正ログインされてしまったときの対応

・パスワードを変更する

今後の不正ログインを防ぐために即時パスワードを変更する。

・パスワードを使い回していないか確認する

他のサービスでパスワードを使い回しているのであれば合わせてパスワードを変更する。

情報リテラシー、モラルを向上させる

意図せず情報モラル[1]に反することを行ったり、故意に不正を行ったりする人がいる。組織においては業務で急いでいたり、緊急対応をしていたり等、精神的に追い込まれて、組織のためによかれと考えて規則に反してしまうこともあると考える。いずれにしても、悪気があるかないかに関わらず自身の行為には責任が伴う。特に、組織においてはたとえ従業員の勝手な行動であったとしても組織に影響が及ぶことや責任が問われることが多くある。本項を読み、「個人として」、「組織として」どのように対策すべきかの参考にしてほしい。

● 家族や組織従業員を教育する

情報リテラシーの向上が必要な人は気を付けるべきことに自身で気付けないことが多い。個人であれば、これから PC やスマートフォンを使う子へ[2]、使い慣れていない親へ、組織であれば従業員への教育を行う。教育内容は教育対象とするケースにより異なるため一例として以下に記載する。

【個人、組織共通】

① SNS の利用に関するケース

・掲載されている情報が正しいとは限らない

悪意の有無に関わらず、誤った情報が広まるおそれもあるため、情報を鵜呑みにしない。

・安易に情報を拡散しない

情報を安易に拡散してしまうと責任を問われることがある。特に SNS では簡単に情報を見つけ、拡散できるが、意図せずデマの拡散や誹謗・中傷に加担してしまうおそれがある。

拡散する場合は一次情報を探し、発信者や発信内容が正しいのかファクトチェック等も活用して確認した上で拡散する。[3]

・情報発信は慎重に行う

真偽を判断できない情報や他人を攻撃するような発言は控える。情報を拡散する場合と同様に情報が正しいか確認した上で発信する。

一度インターネット上に発信した内容は完全に消去することは難しい。(デジタルタトゥーと呼ばれている)そのため、感情のままに発信せず、一旦時間をおいて落ち着いて行う。

② インターネット利用に関するケース

・本物を騙った偽の Web サイトがある

・個人情報を盗もうとする Web サイトがある

特に個人情報や金銭に関する情報の入力を求められたときには注意が必要である。

【組織】

① 情報セキュリティに関するケース

・情報リテラシーや情報モラルの向上を図る

② コンプライアンスに関するケース

・内部不正に対する懲戒処分やそれを規定した就業規則に関する周知を行う

教育のコンテンツに何を取り入れるべきか業務により異なるが IPA から発信しているコンテンツを紹介するので参考にしてほしい。[4, 5]

③ 教育受講者への意識付け

教育する際は受講者に以下のことを意識づけすることも必要である。

・他人事と考えずに受講すること

・就業規則、社内運用規則を理解すること

・事故を起こさないことは自身を守る意味もあること

・緊急時の報告先、報告方法を把握すること

● 継続的に取り組む

・定期的に、適切な時期に教育する

組織における教育では、人の入れ替わり(新入社員、中途社員、派遣、出向等)やイベント(長期休暇、社会情勢等)を考慮することも有効である。これらを考慮した上で、毎回同じ教育コンテンツではなく、従業員の行動やポリシーを定期的に評価し、コンテンツを定期的に見直すことも必要である。

メールの添付ファイル開封や、メールや SMS のリンク、URL のクリックを安易にしない

様々なサービスからの連絡がメールで行われたり、SMS でお知らせが届けられたりすることがある。本物の連絡である場合もあるが、本物を騙った偽の連絡であると、それに起因として個人情報を盗まれたり、金銭被害に繋がったりするおそれがある。

● 被害に遭うタイミング

悪意があるメールや SMS を受信して、内容を閲覧した時点ではまだ情報を盗まれたり、PC やスマートフォンがウイルス感染したりする可能性は低い。そのメールや SMS から誘導された Web サイトに情報を入力することで入力した情報が盗まれたり、添付ファイルを開くことでウイルス感染してしまったりする。

ウイルスに感染すると PC やスマートフォンに保存されている情報が盗まれたり、PC やスマートフォンが正常に動作しなくなったりしてしまう。

さらに盗まれた情報がクレジットカードや銀行口座の情報であると、それを利用されて金銭被害につながってしまう。

● メールや SMS、SNS に関する注意事項

・安易にリンクや QR コードを開かない

メールや SMS、SNS で受信したメッセージ内のリンクを安易にクリックやタップをしない、QR コードを安易に読み取らないようにする。メール本文に記載されている URL をブラウザに安易に入力して開かないようにする。

これらの方法で開いた Web サイトは、正規の物を騙った偽物のおそれがある。

・記載された電話番号に電話をかけない

悪意があるメールや SMS に記載された電話番号は偽のサポート窓口につながるおそれがあり、嘘の案内をされることで情報を聞き出されてしまう等の被害につながる。

● メール固有の注意事項

・画像をクリックやタップしない

一見ただの画像であってもリンクになっていて、クリックやタップをすると偽の Web サイトが開くおそれがあるので注意する。

・添付ファイルを開かない

添付ファイルを開くと悪意のあるプログラムが起動し、ウイルス感染するおそれがある。

Microsoft Word や Excel を開いてしまった際に「マクロを有効にする」「コンテンツの有効化」というボタンが表示されることがあり、このボタンを押すと悪意のあるプログラムが動いてしまうことがある。そのため、業務でマクロ機能を使用しない場合は、マクロを無効化しておくとよい。他にも、開いたファイルが安全ではないおそれがある場合に「編集を有効にする」というボタンが表示されることもある。これらのボタンを安易にクリックやタップはしないように注意が必要である。

● リンクや URL をクリックせずに確認する方法

不審なメールや SMS の案内は以下のような、リンクや URL をクリックさせる文面が多い。

「〇〇について下記よりご確認ください。」

「詳細はコチラ」

このような文面であるため、クリックやタップをしてはいけないとはいえ内容が気になる、確認はした方がよいと感じることがある。

その場合はメール内のリンクは使用せず、以下のようにして正規の情報を確認するとよい。

① 事前にブックマーク（お気に入り）に登録しておく

よく利用している Web サイトはブックマークしておき、ブックマークからアクセスする

② あらかじめ正規のアプリをインストールしておき、そのアプリを使ってサービスを参照する

③ Web サイトを検索して開き、確認する

対象のサービスをブラウザで検索して正規の Web サイトを開く。そして、例えば不在通知なら

ば追跡番号で調べるか問い合わせをする。
ショッピングサイトならばログインしてアカウント情報を確認したり、注文履歴を確認したり、問い合わせることで確認する。

IPA では実際の画面を用いて紹介しているので、是非 IPA の Web サイトで手口を確認し、不審なメールや SMS に備えてほしい。[1]

適切な報告／連絡／相談を行う

【個人】

被害を受けたときは適切な人や機関への相談が必要である。誰にも相談せずに 1 人で対応してしまうとさらなる被害につながってしまうおそれもある。不安に感じたときや被害に遭ったときは慌てず、まずは落ち着いて、以下の相談先に連絡することが望ましい。

表 1.7【個人】に関する相談先の例

発生した出来事	相談する相手
不審なメールや SMS を受信した	①信頼できる知人 ②迷惑メール相談センター（日本データ通信協会） (https://www.dekyo.or.jp/soudan/index.html) ③サービス提供会社 ※不審なメールや SMS のリンクはクリックせず、不審な Web サイトからではなく、自身でサービス提供会社の窓口を調べ直して問い合わせる ④クレジットカード会社や金融機関（情報を入力してしまった場合） ⑤フィッシング対策（警察庁） (https://www.npa.go.jp/bureau/cyber/countermeasures/phishing.html) ⑥フィッシング対策協議会 (https://www.antiphishing.jp/registration.html)
不審な Web サイトを見つけた	
不審な Web サイトに個人情報や金銭情報を入力してしまった	
メールや SMS で脅迫された、金銭の要求をされた	①信頼できる知人 ②都道府県警察本部のサイバー犯罪相談窓口 (https://www.npa.go.jp/bureau/cyber/soudan.html)
クレジットカードを勝手に使われた	①クレジットカード会社、電子決済の提供会社 ※クレジットカード会社によっては、全額または一部を補償する場合がある。（補償してくれる期間が短い場合があるので注意） ②勝手に使われたサービスや商品の提供会社 ③金融機関 ④都道府県警察本部のサイバー犯罪相談窓口 (https://www.npa.go.jp/bureau/cyber/soudan.html)
インターネットバンキングで不正送金された ※③と④に連絡	
電子決済を勝手に使われた	
PC やスマートフォンに不審な警告が表示された	基本的には表示に従ってはいけないが心配な場合は以下に相談する。 ①信頼できる知人 ②IPA（安心相談窓口） (https://www.ipa.go.jp/security/anshin/about.html)
自身のアカウントに勝手にログインされた	ログインされたサービスの提供会社
誹謗・中傷を受けた	①インターネット上の誹謗中傷への対策（総務省） (https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/hiboutyusyou.html) ②ネットの誹謗中傷（セーファーインターネット協会） (https://www.saferinternet.or.jp/bullying/) ③誹謗・中傷が掲載されている Web サイトや SNS の提供会社 ④都道府県警察本部のサイバー犯罪相談窓口 (https://www.npa.go.jp/bureau/cyber/soudan.html) ⑤弁護士、日本司法支援センター法テラス（https://www.houterasu.or.jp/）
上記のどれに当てはまるか分からない	①IPA（安心相談窓口） (https://www.ipa.go.jp/security/anshin/about.html) ②国民生活センター／消費生活センター (https://www.kokusen.go.jp/map/)

【組織】

組織においては上司や責任者、経営者層に適切な報告や連絡をしないと被害の拡大につながるだけでなく、外部からは隠蔽したとみなされ、さらなる信頼の失墜につながるおそれもある。それを防ぐためにあらかじめエスカレーション先を定めて対応マニュアルを作成し、これに従ってエスカレーションを行う必要がある。また、場合によっては組織外への情報発信もしなければならない。これら一連のエスカレーションを迅速に行うために、組織に所属する全員がインシデント発生時の対応を十分に理解すること、経営者や上司、責任者は部下や担当者が包み隠さず躊躇なくエスカレーションできる風土や関係性を築くことも重要である。

対応マニュアルの作成においては、連絡先の例を以下に列挙するので参考にするとよい。

表 1.8【組織】に関する報告／連絡／相談先の例

組織内の立場	報告／連絡／相談する相手
従業員	些細なことから重大インシデントを発見できる可能性がある。また、自身がインシデントを起こしてしまった場合は適切にエスカレーションをしないと隠蔽を疑われ、責任を問われるおそれがある。 そのため、躊躇せずにエスカレーションすることが重要である。 ①上司や責任者、セキュリティの管理者にエスカレーションする ※自身がインシデントを起こした、発見した場合 ②システム管理者にエスカレーションする ※自身が利用している PC やスマートフォン、システムに関するインシデントの場合 ③CSIRT にエスカレーションする ※組織内で CSIRT が構築されている場合
上司や責任者	報告を受け、対応を判断する必要もある。日頃から関係者を把握しておくことや対応手順を理解し、組織内の関連部署へ横展開する。
経営者層や組織として	組織として、自組織や関係者の被害拡大防止、社会的責任を果たすために、外部へ報告、相談、公表する必要がある。場合によって、被害拡大防止や原因と対応の報告等を 1 次報告、2 次報告と段階を分けて適切に行うことが重要である。 ①セキュリティの専門会社に技術支援依頼をする（契約がなくても、スポットで緊急対応してくれるサービスもある） ※自組織だけでは調査や解決できない場合 ②顧客、取引先、委託先、委託元、関連組織に報告する ※場合によってはメディアへの公表を検討する ③金融機関、クレジットカード会社へ連絡する ※情報漏えい等によるさらなる被害拡大防止 ④監督省庁、IPA、JPCERT/CC に報告する ※発生したインシデントに併せて公的機関等に報告する J-CRAT 標的型サイバー攻撃特別相談窓口 (https://www.ipa.go.jp/security/todokede/tokubetsu.html) コンピュータウイルス・不正アクセスに関する届出 (https://www.ipa.go.jp/security/todokede/crack-virus/index.html) JPCERT/CC インシデント対応依頼 (https://www.jpcert.or.jp/form/) ⑤個人情報保護委員会に報告する ⑥警察に相談する ⑦弁護士に相談する

インシデント対応体制を整備し対応する

セキュリティインシデントが発生した際、誰がどのように、何から行えばよいのか？これを理解してあらかじめ対応する仕組みを整えているのといないのとでは、同じ事象の問題が起きたとしても受ける被害の大きさは全く異なる。特に、サイバー攻撃を受けた際はより迅速な対応が必要である。そこで、本項ではセキュリティインシデント発生時の対応やそれを行うために必要なことについて解説するので、自組織における対応計画を作成する参考としてほしい。

【組織】

● インシデント対応の事前準備

・CISO（Chief Information Security Officer）等、専門知識をもつ責任者を配置する

・CSIRT（Computer Security Incident Response Team）を構築する

インシデント対応を一般社員が兼務して対応するのは難しい。そのため組織内の情報セキュリティ問題を専門に扱う CSIRT の構築が望ましい。構築するのが厳しい場合はインシデント対応の統制をする責任者を決めておく。

・CSIRT を中心とした有事の際の対応フローを確立し、連絡先を明確にした運用手順を作成する

・作成した運用手順を社員へ周知する

・実際に運用できるか確認する（訓練する）

作成した運用手順は、実際に運用できるのか定期的に訓練を行い、その結果を元に手順を見直すことも必要である。

・自組織で解決できない場合を想定して外部の協力依頼先を用意する

・これら全てを継続的に行える体制と社内の規則やポリシーの整備、予算の確保を経営者層が主体となって行う

● インシデント対応として CSIRT が行うべきこと

① 検知／連絡受付

セキュリティ機器での検知や組織内外からの通報によりインシデントの発生を認知する。

② トリアージ

認知したインシデントについて通報者やインシデントに関係する可能性がある者とやり取りし、情報を収集することで事実確認をする。その後、確認した結果から CSIRT で対応すべきかどうかを判断する。判断した結果は通報者や関係者に連絡する。その際、対応すべきかどうかに関わらず、速やかな対応を必要とする場合や情報共有をすべき場合は注意喚起や情報発信を適切に行う。

③ インシデントレスポンス

対応すべきと判断したインシデントを分析し、対応計画を策定する。組織内の関連部門だけでは対応しきれない場合は外注先への技術支援依頼も視野に入れて、経営者等の責任者と連携して計画を立てることも必要である。技術的なこと以外でも外部の専門機関や関係する組織に支援依頼をしたり、情報を提供してもらったりする。

その後、策定した計画に従って対応を実施し、問題が解決しているかの確認をする。

④ 報告／情報公開

対応計画の策定や実施と並行してインシデントの通報者や関係者、メディアや社会、監督省庁への報告を行う。

CSIRT の構築が難しい組織であっても最低限インシデント対応を取り纏める者を定めておく必要がある。インシデント発生時に対応すべきことは公的機関が様々なガイドライン等を公開している。自組織では対応の準備ができているか事前に確認しておくことを推奨する。[1,2,3,4]

サーバーやクライアント、ネットワークに適切なセキュリティ対策を行う

組織に対する脅威はサーバーやクライアント、ネットワークに関連したものが多い。これらには重要な情報が含まれており、企業活動の生命線であることは今後も変わらないと考えられる。つまり、今後も攻撃者から狙われやすいということである。個人の PC やスマートフォンとは異なり、組織のサーバーは例えば、「更新プログラム適用」ひとつとっても組織としてのポリシーの制定や要員確保、事前検証、手順の確立、そしてそれを維持し続ける予算の確保と仕組みが必要であり検討事項は多く、頭を抱える組織も多いと考える。本項ではサーバーやネットワークに対するセキュリティ対策の検討事項をまとめるので今後の運用の参考としてほしい。

【組織】[1,2]

● 脆弱性対策を適切に行う

・サポート切れの OS やソフトウェア、ハードウェアを使用しない

自組織で使用している製品のサポート期限を把握しておき、サポート切れになる前に移行計画を立てて運用を検討する。

・提供元不明のソフトウェアを利用しない

・迅速に更新プログラムの適用をする

漏れなく適用するために資産管理や脆弱性情報の収集、更新プログラムの適用状況を管理する手順や体制を整備しておく必要がある。

特に、利用しているソフトウェアの管理においては SBOM の導入を検討する。[3]

また、誰がどのように動作検証を行うか、構築時や保守契約時に考慮しておく必要がある。

・仮想パッチを導入する

サーバーに更新プログラムを適用するには事前検証や再起動が伴う。そのため、迅速に更新プログラムを適用できない場合に、ネットワークレベルで攻撃の通信を遮断することで一時的に問題を解決する手法が仮想パッチである。根本的な問題を解決できるわけではなく、あくまで暫定対策であることに注意が必要である。

・不要なサービスを停止または無効化する

サーバー再起動により、停止したサービスが自動起動されないよう、自動起動が無効の設定になっていることを確認する。

● アクセス権限管理を適切に行う

・アクセス権限を最小化する

不要なアカウントを作成せず、作成したアカウントに過剰な管理者権限や更新権限を与えない。

・管理者権限の運用体制を整える

内部不正防止のため、IT を伴わない対策も行う。例えば、運用担当者を制限をすることや利用記録を残すこと、クロスチェックをすること等、運用方法で対策することも有効である。

・定期的にアカウントの棚卸を行う

従業員や職員の離任時に対象者のアカウントを削除し、その上で定期的に棚卸を行うことで、権限付与の妥当性や、不要なアカウントが存在していないか等を確認する。

・同一のアカウントを複数人で運用しない

・アクセスログを収集し監視する

インシデント発生時には過去に遡って調査できるよう、保存期間やログファイルの運用方法も組織の方針に併せて検討する必要がある。

・パスワードを適切に運用する（詳細は「共通対策_パスワードを適切に運用する」を参照すること。）

・多要素認証の設定を有効にする

利用している機器が多要素認証に対応している場合は設定を有効にしておくことで不正アクセスを防止する。

● セキュリティ製品を導入する

・セキュリティソフト

セキュリティソフトとは様々なセキュリティ機能が統合されたソフトウェアである。アンチウイルスや迷惑メールのフィルタリング、Web アクセスのフィルタリングをはじめ、製品によって様々な機能を搭載している。特にアンチウイルスに関しては、最初に導入するだけでなく、定期的なス

キャンやパターンファイルの更新を行うように設定し、結果を確認することが必要である。

・EDR (Endpoint Detection and Response)

サーバーおよびクライアント内の処理や外部との通信等の不審な振る舞いを検知することで迅速な対応を可能にする。

・NDR (Network Detection and Response)

ネットワーク上の通信を監視、分析することで不審な通信を検知し、迅速な対応を可能にできる。

・DLP (Data Loss Prevention)

特定のデータのコピー等持ち出しを検知し、ブロックする。例えば、管理対象のデータがメールに添付されている場合にアラートを出したりブロックしたりすることで誤送信等、作業ミスによる漏えいの防止等も可能である。

・CSPM (Cloud Security Posture Management)

クラウドの設定ミスによる情報漏えいを防ぐ。あらかじめ自社のポリシーを元にチェックのルールを設定しておき、そのルールに抵触する設定がなされた場合にアラートを出すことで設定ミスに気が付けるようにする。

・IDS (Intrusion Detection System)

不正侵入検知システムと呼び、ネットワーク通信を監視し、不審な通信が見つかった際に担当者へ通知を行う。自動でブロックする機能はないが、通知を受けることで、担当者が内容を確認し対応を開始する契機となる。

・IPS (Intrusion Prevention System)

不正侵入防止システムと呼び、ネットワーク通信を監視し、不審な通信が見つかった場合は担当者への通知だけでなく自動でブロックも行う。IDS よりリスクの低減はできるが正規の通信をブロックしてしまうおそれもあり、組織の方針を踏まえた上での選定が必要である。

・DNS フィルタリング

新しく登録された未検証のドメインや不審なドメイン、悪性な類似ドメインへのアクセスを名前解決の段階で防止する。

・WAF (Web Application Firewall)

Web サーバーの前面または Web サーバー内に設置することで通信を監視し、Web サイトを保護する。IDS、IPS がネットワークレベルでの監視を行うのに対して WAF はアプリケーションレベルでの監視であるため、組み合わせて適用することでより強固な防御が可能になる。

・UTM (Unified Threat Management)

統合脅威管理と呼び、IDS や IPS の機能やファイアウォール、アンチウイルス等、他の機能も備えた製品である。1 つに統合されていることで運用コストや手間を低減することが期待できる。

● ネットワーク管理を適切に行う

・ネットワークの分割と個別遮断を行う

ネットワークを事業所や部署、機器の用途などの単位等で論理的、もしくは物理的に分割する。インシデントが発生した際は分割されたネットワークを隔離することでウイルス感染時の被害を局所化する。

・ファイアウォールを設置し、アクセス制御する

どこから、どのサーバーに、どのサービスにアクセスさせるかを検討し、必要最小限のアクセス制御を行う。

・プロキシサーバーを導入する

利用者認証を受けない外部への不正通信をブロックする。

・ASM（Attack Surface Management）を行う

ASM とは組織の外部（インターネット）からアクセス可能な IT 資産を発見し、それらに存在する脆弱性などのリスクを継続的に検出・評価する一連のプロセスのことである。組織管理者の未把握の機器や意図しない設定ミスを攻撃者視点から発見でき、脆弱性管理活動において、リスク低減の効果が期待できる。[4]

・不要なポートへの通信や不要なプロトコルの通信は遮断する

● その他

・セキュリティのサポートが充実している製品を使う

導入するソフトウェアもパッチや回避策の提供が迅速である物を使用する。

・統合運用管理ツールを導入する

統合運用管理ツールとは社内ネットワーク機器やサーバー等の IT 機器を一元管理するツールである。様々な管理項目があり、セキュリティ管理機能ではシステムへのアクセス権限の管理やファイアウォールの設定、暗号化方式の選択等が可能である。他にも様々な機能があるため、セキュリティ対策だけでなく導入することにより、大きなメリットを期待できるツールである。

・重要データやファイルを暗号化する

・外部記憶媒体の接続を制限する

・脆弱性診断を行う

セキュリティベンダーから提供されている診断サービスはサーバーやネットワーク全体を診断でき、適切な助言を受けられるため実施を検討するとよい。

・ペネトレーションテストを行う

実際の攻撃シミュレーションを通じてセキュリティ体制の実効性を評価する。

・ログを取得し、監視や解析する

システムログ、アプリケーションログ、サーバーへのアクセスログ、認証ログ、データベース操作ログ、通信ログ等の各種ログを取得し、監視や解析をすることで不審な振る舞いの迅速な検知だけでなく被害に遭った際の原因特定が可能になる。

また、ログの取得は、ログレベルや保管期間について事前に検討が必要である。特に、運用を外注するのであればログの取得や監視、解析に関する仕様や運用の確認を行う。

IPA では Web サーバーや SSH、FTP サーバーのログを解析することで攻撃と思われる痕跡を検出するためのツール（iLogScanner[5]）を無料で提供しているので利用を検討するとよい。

・サイバーセキュリティお助け隊サービス

「見守り」「駆付け」「保険」など中小企業のセキュリティ対策に不可欠なワンパッケージのサービスを要件としてまとめ、これを満たすことが所定の審査機関により確認された民間サービスを IPA で公表している。これを活用してワンパッケージで安価にセキュリティ対策を行う。[6]

適切なバックアップ運用を行う

データの破損の原因は記憶装置の故障やランサムウェア等のサイバー攻撃だけではなく、運用時の操作ミスによる消去や誤った更新と多岐に渡る。失ったデータの復旧は困難であり、復旧には人手と時間を要する。しかし、バックアップを取得しておくことでこの被害を軽減することが可能である。迅速にデータを復旧し業務継続できなければ、組織の信頼も失墜し、存続の問題に繋がりかねない大きなリスクとなる。そこで本項では適切なバックアップ運用について解説するので今後の運用の参考にしてほしい。

● バックアップを取得する

・対象を選定する

バックアップの対象は業務データだけではない。システムの稼働に必要な設定ファイルや、プログラムも含め、バックアップ対象を選定する。

・取得方法や取得日時、間隔を検討する

サーバーの稼働要件に併せてオフライン、オンラインバックアップのどちらか検討する。

対象のデータごとに適切な取得日時、間隔を検討する。例えば、業務データは週に1回フルバックアップ、その他の日に差分バックアップをする。プログラムファイルはシステム改修が無い限り変更はないためリリース時のみバックアップをする。設定ファイルは随時変更があるため週に1回取得する等のように検討する。

● バックアップを保管する

・3-2-1 ルール [1]

データはコピーして 3 つ持ち、2 種類のメディアでバックアップを保管し、バックアップの 1 つは違う場所で保存するというルールがある。ランサムウェアに対しては「3-2-1-1-0 ルール」も提唱されているので参考にするとよい。[2]

・保管場所を検討する

ランサムウェア攻撃に備えて、ネットワーク上から隔離された場所へ保管する。外部記憶装置に保管し、バックアップ取得時以外は物理的に接続を切ることが望ましい。さらに、災害対策も含めるのであれば地理的に離れた異なる場所で保管するとさらによい。

・世代管理を行う

最新だけでなく、過去のバックアップも保管し、複数の時点に復旧できるようにしておくことが望ましい。データの破損からそれを認知するまでに時間がかかると最新のバックアップもすでに破損しているおそれがあるためである。

また、バックアップにはいつの時点のどのデータが含まれているのか、ファイルの名称や保管している外部記憶装置を判別できるようにする。それらを扱う際の運用手順を定めることで誤って上書きしてしまったり、消去してしまったりする事故を防ぐ。

・保管期間を決める

バックアップの保管方法や世代管理と合わせて組織の方針を満たせる保管期間を決定する。

● バックアップからリストアする

・復旧計画を立てる

バックアップは取得するだけで終わりではなく、それを利用していかに早く復旧するかが重要である。そのために想定される障害とその被害をあらかじめ考え、それぞれに対して復旧する時点やリストア手順を確立する。

・正しく復旧できることを確認する

計画に基づいて正しく復旧できるか定期的に確認し、必要に応じて手順の見直しを行う。

● PC やスマートフォンを使う個人の対策

・大切なデータは別の媒体にも保存しておく

普段使用する PC やスマートフォンとは別の端末や外付けハードディスク、SD カード等にデータを保存する。

使わない時は保存した媒体と、普段使用する PC やスマートフォンとは接続せずに保管する。

参考資料

【個人】（五十音順）

・「インターネット上のサービスからの個人情報の窃取」

1.「エン転職」への不正ログイン発生に関するお詫びとお願い（エン・ジャパン株式会社）
https://corp.en-japan.com/newsrelease/2023/32484.html
2. 不正アクセスによる個人情報漏えいの可能性に関するお詫びとお知らせ（株式会社ビッグモーター）
https://www.bigmotor.co.jp/lib/news/news_list.php?id=703&page=
3. 不正アクセスによる個人情報漏えいのお詫びとご報告（カシオ計算機株式会社）
https://www.casio.com/jp/information/1018-incident/
4. Have I Been Pwned?（HaveIBeenPwned.com）
https://haveibeenpwned.com/

・「インターネット上のサービスへの不正ログイン」

1. 著名人を狙った金銭目的のSNS公式アカウントののっとりについてまとめてみた（piyolog）
https://piyolog.hatenadiary.jp/entry/2023/05/12/002134
2. 「Amazonを不正利用された」──SNS上で報告相次ぐ 「二段階認証を突破された」などの声も（ITmedia NEWS）
https://www.itmedia.co.jp/news/articles/2309/14/news152.html
3. お客様へのお知らせ：日興イージートレードにおける不正アクセスにご注意ください（SMBC日興証券株式会社）
https://www.smbcnikko.co.jp/news/customer/2023/n_20230904_01.html
4. ネット取引サービスに不正ログイン、株式不正売却も - SMBC日興証券（SecurityNEXT）
https://www.security-next.com/149297
5. 不正ログイン対策特集ページ（IPA）
https://www.ipa.go.jp/security/anshin/measures/account_security.html

・「クレジットカード情報の不正利用」

1. 最近の主な漏えい事案（経済産業省）
https://www.meti.go.jp/shingikai/mono_info_service/credit_card_payment/pdf/001_04_02.pdf
2. 当サイトへの不正アクセスによる個人情報漏えいに関するお詫びとお知らせ（株式会社FANSMILE）
https://nico-online.com/news/54
3. 本市が運営する「志布志市ふるさと納税特設サイト」への不正アクセスによる個人情報漏えいに関するお詫びとお知らせ（志布志市）
https://www.city.shibushi.lg.jp/soshiki/5/22233.html
4. クレジットカード不正利用被害の集計結果について（一般社団法人日本クレジット協会）
https://www.j-credit.or.jp/download/news20231228_a1.pdf
5. コンピュータウイルス・不正アクセスの届出事例［2023 年上半期（1 月～6 月）］（IPA）
https://www.ipa.go.jp/security/todokede/crack-virus/ug65p9000000nnpa-att/2023-h1-jirei.pdf
6. クレジットマスターとは？手口や被害を防ぐための対策を徹底解説（Cyber Security.com）
https://cybersecurity-jp.com/column/77900

・「スマホ決済の不正利用」

1. PayPayの送金で8万円をだまし取る 神戸市職員を逮捕（産経新聞）
https://www.sankei.com/article/20230412-XQE4VBCLEFMZTGDR4YSJUDUWVY/
2. レジで支払った女逮捕、一緒にいた男も…関係ない女性の「auPAY」を使っていた 夜のコンビニで（埼玉新聞）
https://www.saitama-np.co.jp/articles/15070/postDetail
3. スマホ決済不正利用容疑 39歳逮捕 eSIM乗っ取りか（読売新聞オンライン）
https://www.yomiuri.co.jp/local/aichi/news/20230927-OYTNT50233/

・「偽警告によるインターネット詐欺」

1. 偽セキュリティ警告（サポート詐欺）対策特集ページ（IPA）
https://www.ipa.go.jp/security/anshin/measures/fakealert.html
2. スマートフォンの偽セキュリティ警告から自動継続課金アプリのインストールへ誘導する手口にあらためて注意！（IPA）
https://www.ipa.go.jp/security/anshin/attention/2022/mgdayori20221025.html
3. 大惨事…男性のPCに驚きの警告出現 表示された番号に電話し、片言の男に案内され4400万円失う 何があった（埼玉新聞）
https://www.saitama-np.co.jp/articles/23485
4. 個人のパソコンを遠隔操作、ネットバンキングから現金だまし取る 新たな手口、兵庫で被害相次ぐ（神戸新聞NEXT）
https://www.kobe-np.co.jp/news/sougou/202302/0016081001.shtml
5. 情報セキュリティ安心相談窓口の相談状況［2023年第4四半期（10月～12月）］（IPA）
https://www.ipa.go.jp/security/anshin/reports/2023q4outline.html
6. 情報セキュリティ安心相談窓口の相談状況［2022年第4四半期（10月～12月）］（IPA）
https://www.ipa.go.jp/security/anshin/reports/2022q4outline.html
7. 情報セキュリティ安心相談窓口公開レポート（IPA）
https://www.ipa.go.jp/security/anshin/reports/index.html
8. サポート詐欺で表示される偽のセキュリティ警告画面の閉じ方（IPA）
https://www.ipa.go.jp/security/anshin/doe3um0000005cag-att/20231115173500.pdf
9. 情報セキュリティ安心相談窓口（IPA）
https://www.ipa.go.jp/security/anshin/index.html
10. 安心相談窓口だより「ブラウザの通知機能から不審サイトに誘導する手口に注意」（IPA）
https://www.ipa.go.jp/security/anshin/attention/2021/mgdayori20210309.html

・「ネット上の誹謗・中傷・デマ」
1:高須克弥氏への名誉毀損事件で大学生に有罪判決　さいたま地裁（朝日新聞 DIGITAL）
https://www.asahi.com/articles/ASR5C54TZR5CUTNB00D.html
2: 消費者金融を不正利用疑い　SNSに偽広告、男逮捕（熊本日日新聞）
https://kumanichi.com/articles/1206209
3: 番組に似せた岸田首相の偽動画拡散　日本テレビが注意呼びかけ（NHK NEWS WEB）
https://www3.nhk.or.jp/news/html/20231104/k10014247171000.html

・「フィッシングによる個人情報等の詐取」
1. URLリンクへのアクセスに注意（IPA）
https://www.ipa.go.jp/security/anshin/attention/2021/mgdayori20210831.html
2. マイナポータルをかたるフィッシング（2023/12/06）（フィッシング対策協議会）
https://www.antiphishing.jp/news/alert/mynaportal_20231206.html
3. マイナポータルを騙った詐欺メール及び偽サイト（フィッシング詐欺）に関する注意喚起（デジタル庁）
https://www.digital.go.jp/news/4750a8f5-1061-4ae6-903b-cfb327a50465
4. 2023年4月24日 フィッシングによるものとみられるインターネットバンキングに係る 不正送金被害の急増について（警察庁）
https://www.npa.go.jp/bureau/cyber/pdf/20230424_press3.pdf
5. 2023年8月8日 フィッシングによるものとみられるインターネットバンキングに係る 不正送金被害の急増について（警察庁）
https://www.npa.go.jp/bureau/cyber/pdf/20230808_press.pdf
6. 2023年12月26日 フィッシングによるものとみられるインターネットバンキングに係る 不正送金被害の急増について（警察庁）
https://www.npa.go.jp/bureau/cyber/pdf/20231225_press.pdf
7. 米FTC、QRコードを用いた「クイッシング」攻撃について注意喚起（CNET Japan）
https://japan.cnet.com/article/35212658/
8. サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2023年7月～9月]（IPA）
https://www.ipa.go.jp/security/j-csip/ug65p9000000nkvm-att/fy23-q2-report.pdf

・「不正アプリによるスマートフォン利用者への被害」
1. 宅配便業者に加えて通信事業者をかたる偽ショートメッセージサービス（SMS）が増加中（IPA）
https://www.ipa.go.jp/security/anshin/attention/2021/mgdayori20211222.html
2. Android向けAI基盤の不正アプリ検知アプリ「Fake Finder」が検知した悪性アプリに関する注意喚起のお知らせ
～2023年10月における不正アプリ状況をレポート～（SBIホールディングス株式会社）
https://www.sbigroup.co.jp/news/2023/1206_14275.html
3. App Store以外の配信アプリによるセクストーション被害を確認（IPA）
https://www.ipa.go.jp/security/anshin/attention/2019/mgdayori20191224.html
4. Google Playのアプリにマルウェア 2023年は6億回以上ダウンロードされる（kaspersky daily）
https://blog.kaspersky.co.jp/malware-in-google-play-2023/35124/
5. 宅配便業者を装った「不在通知」の偽SMSに注意しましょう（安中市）
https://www.city.annaka.lg.jp/page/1591.html

・「メールや SMS 等を使った脅迫・詐欺の手口による金銭要求」
1. 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（IPA）
https://www.ipa.go.jp/security/anshin/attention/2018/mgdayori20181010.html
2. App Store以外の配信アプリによるセクストーション被害を確認（IPA）
https://www.ipa.go.jp/security/anshin/attention/2019/mgdayori20191224.html
3. 遠隔操作ソフト（アプリ）を悪用される手口に気をつけて！（IPA）
https://www.ipa.go.jp/security/anshin/attention/2023/mgdayori20230411.html
4. 【2023/5/25 6:50】ばらまき型脅迫詐欺メール（性的脅迫メール）に関する注意喚起（国立大学法人 電気通信大学情報基盤センター）
https://www.cc.uec.ac.jp/blogs/news/2023/05/20230525scammail.html
5. 「もうすぐがんで死ぬ」メールで詐欺被害 警察が注意呼びかけ（NHK NEWS WEB）
https://www3.nhk.or.jp/news/html/20231110/k10014254201000.html
6. “約1億5000万円の詐欺”2023年北海道内最高被害額 SNSで知り合った男「収益利率20%を超える」札幌の女性『暗号通貨の投資話』でだまされる（北海道ニュースUHB）
https://nordot.app/1106921703885538061?c=900039697665425408

・「ワンクリック請求等の不当請求による金銭被害」
1. アダルトサイト閲覧…「登録料」要求され1000万円だまし取られる 静岡・伊豆市の男性が特殊詐欺被害（gooニュース）
https://news.goo.ne.jp/article/tvsdt/region/tvsdt-2023122202869594.html
2. 各種相談の件数や傾向 > アダルト情報サイト（独立行政法人国民生活センター）
https://www.kokusen.go.jp/soudan_topics/data/adultsite.html
3. ワンクリック請求の手口に引き続き注意（IPA）
https://www.ipa.go.jp/security/anshin/attention/2022/mgdayori20220706.html
4. 情報セキュリティ安心相談窓口（IPA）
https://www.ipa.go.jp/security/anshin/index.html

【組織】

・1 位「ランサムウェアによる被害」

1. 令和5年上半期におけるサイバー空間をめぐる脅威の情勢等について（警察庁）
   https://www.npa.go.jp/publications/statistics/cybersecurity/data/R05_kami_cyber_jousei.pdf
2. NUTS システム障害の経緯報告（名古屋港運協会）
   https://meikoukyo.com/wp-content/uploads/2023/07/0bb9d9907568e832da8f400e529efc99.pdf
3. コンテナターミナルにおける情報セキュリティ対策等検討委員会について（国土交通省）
   https://www.mlit.go.jp/kowan/kowan_mn2_000006.html
4. 第三者によるランサムウェア感染被害への対応状況のお知らせ（第2報）（株式会社エムケイシステ ム）
   https://contents.xj-storage.jp/xcontents/AS97180/fd524344/99b9/470f/90e6/a580932b7962/140120230620507046.pdf
5. 当社サーバへの不正アクセスに関する調査結果のご報告（第3報）（株式会社エムケイシステ ム）
   https://contents.xj-storage.jp/xcontents/AS97180/813d570f/5138/4bc7/a113/f4837598df38/140120230719524126.pdf
6. 重大なシステムトラブルに伴う個人情報についてのお知らせ（市民生活協同組合ならコープ）
   https://www.naracoop.or.jp/naranews/cat2/4628.html
7. 多数システムでランサム被害、復旧や事業継続に追われる - ならコープ（Security NEXT）
   https://www.security-next.com/143034/
8. The No More Ransom Project（No More Ransomプロジェクト）
   https://www.nomoreransom.org/
9. データ被害時のベンダー選定チェックシート Ver.1.0（特定非営利活動法人デジタル・フォレンジック研究会）
   https://digitalforensic.jp/higai-checksheet/

・2 位「サプライチェーンの弱点を悪用した攻撃」

1. 個人情報流出に関するお詫びとお知らせ（アフラック生命保険株式会社）
   https://www.aflac.co.jp/news_pdf/2023011001.pdf
2. 個人情報流出に関する再発防止策について（アフラック生命保険株式会社）
   https://www.aflac.co.jp/news_pdf/20230710.pdf
3. 個人情報漏えいに関するお詫びとご報告（チューリッヒ保険会社）
   https://www.zurich.co.jp/customerdata/
4. 個人情報漏えいに関する追加のお知らせ（チューリッヒ保険会社）
   https://www.zurich.co.jp/aboutus/news/news/2023/0117/
5. 不正アクセスによる、情報漏えいに関するお知らせとお詫び（LINEヤフー株式会社）
   https://www.lycorp.co.jp/ja/news/announcements/001002/
6. お客さまの個人情報漏えいに関するお知らせとお詫び（JCOM 株式会社）
   https://newsreleases.jcom.co.jp/news/20231122_9239.html
7. 「ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引」を策定しました（経済産業省）
   https://www.meti.go.jp/press/2023/07/20230728004/20230728004.html
8. サイバーセキュリティ経営ガイドラインと支援ツール（経済産業省）
   https://www.meti.go.jp/policy/netsecurity/mng_guide.html
9. 外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書（内閣サイバーセキュリティセンター）
   https://www.nisc.go.jp/pdf/policy/general/risktaiou28.pdf
10. 自動車産業サイバーセキュリティガイドライン（一般社団法人日本自動車工業会）
    https://www.jama.or.jp/operation/it/cyb_sec/cyb_sec_guideline.html

・3 位「内部不正による情報漏えい」

1. NTTビジネスソリューションズに派遣された元派遣社員によるお客さま情報の不正流出について（続報）（NTTビジネスソリューションズ株式会社）
   https://www.nttbizsol.jp/newsrelease/202312191400000982.html
2. 当社に派遣されていた元派遣社員の逮捕について（NTTビジネスソリューションズ株式会社）
   https://www.nttbizsol.jp/newsrelease/202401311500000999.html
3. NTT西系情報流出、名簿1000万円超で売却か 元派遣社員（日本経済新聞）
   https://www.nikkei.com/article/DGXZQOUE07C0X0X01C23A1000000/
4. 当社元従業員の逮捕について（株式会社ワールドコーポレーション）
   https://worldcorp-jp.com/news/2023/20230915.html
5. 名刺データ、管理にリスク 個人情報提供疑いで初逮捕（日本経済新聞）
   https://www.nikkei.com/article/DGXZQOUE1421N0U3A910C2000000/
6. 元勤務先に不正アクセス、データ削除した疑い 退職していた男逮捕（朝日新聞）
   https://www.asahi.com/articles/ASR1S4HC4R1SUTIL008.html
7. 組織における内部不正防止ガイドライン（IPA）
   https://www.ipa.go.jp/security/guide/insider.html
8. IPA NEWS Vol.64（2023年12月号）（IPA）
   https://www.ipa.go.jp/about/ipanews/ipanews202312.html
9. 営業秘密管理指針（経済産業省）
   https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/h31ts.pdf

・4 位「標的型攻撃による機密情報の窃取」
1. 東京大学大学院総合文化研究科・教養学部への不正アクセスによる情報流出について（東京大学）
https://www.u-tokyo.ac.jp/focus/ja/press/z0109_00952.html
2. サイバー攻撃か　東大教員のパソコンに不正アクセス、個人情報4300件流出（TBS NEWS DIG）
https://newsdig.tbs.co.jp/articles/-/796546
3.JAXAにサイバー攻撃＝不正アクセス、機微情報含まず（時事通信社）
https://sp.m.jiji.com/article/show/3109334
4.JAXAへの不正アクセスについてまとめてみた（piyolog）
https://piyolog.hatenadiary.jp/entry/2023/11/29/123934
5.インターネット境界に設置された装置に対するサイバー攻撃について～ネットワーク貫通型攻撃に注意しましょう～（IPA）
https://www.ipa.go.jp/security/security-alert/2023/alert20230801.html
6.「ASM（Attack Surface Management）導入ガイダンス～外部から把握出来る情報を用いて自組織のIT資産を発見し管理する～」を取りまとめました（経済産業省）
https://www.meti.go.jp/press/2023/05/20230529001/20230529001.html

・5 位「修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）」
1. 「ラピッドリセット攻撃」が発生 - 1秒間で約4億リクエスト（Security NEXT）
https://www.security-next.com/150165
2. 4月以降「WinRAR」狙うゼロデイ攻撃が発生 - 最新版に更新を（Security NEXT）
https://www.security-next.com/148924
3. 「IOS XE」の深刻なゼロデイ脆弱性 - JPCERT/CCも攻撃被害を確認（Security NEXT）
https://www.security-next.com/150345

・6 位「不注意による情報漏えい等の被害」
1. 「gmail」ドメインを「gmai」と誤記、2年半放置で800人分の情報漏えいか　鹿児島大が「ドッペルゲンガー・ドメイン」の毒牙に（ITmedia NEWS）
https://www.itmedia.co.jp/news/articles/2302/13/news085.html
2. 申込フォームで個人情報が閲覧可能に - 大阪市コミュニティ協会（Security NEXT）
https://www.security-next.com/151685
3. 個人情報を含むUSBメモリの紛失および発見について（天草市）
https://www.city.amakusa.kumamoto.jp/kiji00311498/index.html

・7 位「脆弱性対策情報の公開に伴う悪用増加」
1. 「Apache ActiveMQ」の脆弱性が標的に - ランサム攻撃にも悪用か（Security NEXT）
https://www.security-next.com/150846
2. CVE-2023-46604: Apache ActiveMQ の悪用の疑い（ラピッドセブン・ジャパン株式会社）
https://www.rapid7.com/ja/about/japan-blog-and-news/etr-suspected-exploitation-of-apache-activemq-cve-2023-46604/
3. ActiveMQの脆弱性(CVE-2023-46604)を悪用したボットの感染活動について（NICTER Blog）
https://blog.nicter.jp/2023/12/cve-2023-46604/
4. Array Networks製VPN機器、標的型攻撃の対象に - 侵害状況の確認を（Security NEXT）
https://www.security-next.com/149480
5. Array Networks Array AGシリーズの脆弱性を悪用する複数の標的型サイバー攻撃活動に関する注意喚起（一般社団法人JPCERTコーディネーションセンター）
https://www.jpcert.or.jp/at/2023/at230020.html
6. インターネット境界に設置された装置に対するサイバー攻撃について～ネットワーク貫通型攻撃に注意しましょう～（IPA）
https://www.ipa.go.jp/security/security-alert/2023/alert20230801.html
7. Barracuda製メールセキュリティ製品に脆弱性 - すでに悪用も（Security NEXT）
https://www.security-next.com/146475
8. Barracuda、「ESGアプライアンス」の交換を呼びかけ（Security NEXT）
https://www.security-next.com/146896
9. Barracuda 製 Email Security Gateway Appliance (ESG) の脆弱性について(CVE-2023-7102)(CVE-2023-7101)（IPA）
https://www.ipa.go.jp/security/security-alert/2023/alert20231225.html
10. Barracuda Email Security Gateway（ESG）の脆弱性（CVE-2023-2868）を悪用する継続的な攻撃活動に関する注意喚起（一般社団法人JPCERTコーディネーションセンター）
https://www.jpcert.or.jp/at/2023/at230017.html

・8 位「ビジネスメール詐欺による金銭被害」
1. サイバー情報共有イニシアティブ（J-CSIP）運用状況[2023 年 4 月～6 月]（IPA）
https://www.ipa.go.jp/security/j-csip/ug65p9000000nkvm-att/fy23-q1-report.pdf
2. 送金詐欺による資金流出被害のお知らせ（株式会社スリー・ディー・マトリックス）
https://pdf.irpocket.com/C7777/ZoWa/awjA/EOHM.pdf

・9 位「テレワーク等のニューノーマルな働き方を狙った攻撃」
1. ランサムウェアによる個人情報流出を確認、リモートアクセス経路より侵害か - セイコー（Security NEXT）
https://www.security-next.com/150579
2. 当社サーバに対する不正アクセスに関するお知らせ（第3報）（セイコーグループ株式会社）
https://www.seiko.co.jp/information/202310251000.html
3. ビデオ会議サービスの「Zoom」、脆弱性9件を修正（Security NEXT）
https://www.security-next.com/151283
4. WebPのゼロデイ脆弱性は「Teams」や「Skype」にも ～Microsoftが影響製品を公表【10月10日追記】（窓の社）
https://forest.watch.impress.co.jp/docs/news/1536304.html
5. 令和5年上半期におけるサイバー空間をめぐる脅威の情勢等について（警察庁）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R05_kami_cyber_jousei.pdf
6. 令和4年におけるサイバー空間をめぐる脅威の情勢等について（警察庁）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf
7. テレワークを行う際のセキュリティ上の注意事項（IPA）
https://www.ipa.go.jp/security/anshin/measures/telework.html

・10 位「犯罪のビジネス化（アンダーグラウンドサービス）」
1. チェック・ポイント・リサーチ、ChatGPTに関する新たな懸念となる窃取された有料アカウントの売買増加を確認（PR TIMES）
https://prtimes.jp/main/html/rd/p/000000202.000021207.html
2. New ChatGPT4.0 Concerns: A Market for Stolen Premium Accounts（Check Point Software Technologies Ltd.）
https://blog.checkpoint.com/security/new-chatgpt4-0-concerns-a-market-for-stolen-premium-accounts/
3. 国内主要製造業30社、 ダークウェブ への情報流出調査結果（株式会社アイギステック）
https://www.aegistech.jp/news/view/id/23#u
4. 月額20ドル・3カ月45ドル・無期限120ドルのお買い得マルウェア登場、警戒を（TECH+）
https://news.mynavi.jp/techplus/article/20231023-2800152/

【共通対策】

・「パスワードを適切に運用する」

1. 不正ログイン対策特集ページ（IPA）
   https://www.ipa.go.jp/security/anshin/measures/account_security.html
2. チョコっとプラスパスワード（IPA）
   https://www.ipa.go.jp/security/chocotto/index.html
3. インターネットの安全・安心ハンドブック（内閣サイバーセキュリティセンター）
   https://security-portal.nisc.go.jp/guidance/handbook.html
4. 安心相談窓口だより「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」（IPA）
   https://www.ipa.go.jp/security/anshin/attention/2016/mgdayori20160803.html

・「情報リテラシー、モラルを向上させる」

1. 第5章　情報モラル教育（文部科学省）
   https://www.mext.go.jp/b_menu/shingi/chousa/shotou/056/shiryo/attach/1249674.htm
2. サイバーセキュリティのひみつ（IPA）
   https://www.ipa.go.jp/security/security-himitsu/index.html
3. ファクトチェックとは（認定NPO法人　ファクトチェック・イニシアティブ）
   https://fij.info/introduction
4. 情報セキュリティ関連サイト（IPA）
   https://www.ipa.go.jp/security/guide/keihatsu.html
5. 対策のしおり（IPA）
   https://www.ipa.go.jp/security/guide/shiori.html

・「メールの添付ファイル開封や、メールや SMS のリンク、URL のクリックを安易にしない」

1. 安心相談窓口だより「URLリンクへのアクセスに注意！」（IPA）
   https://www.ipa.go.jp/security/anshin/attention/2021/mgdayori20210831.html

・「インシデント対応体制を整備し対応する」

1. サイバーセキュリティ経営ガイドラインと支援ツール（経済産業省）
   https://www.meti.go.jp/policy/netsecurity/mng_guide.html
2. インシデント発生時に組織内で整理しておくべき事項（経済産業省）
   https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_app_C.xlsx
3. CSIRTマテリアル　運用フェーズ（一般社団法人JPCERTコーディネーションセンター）
   https://www.jpcert.or.jp/csirt_material/operation_phase.html
4. サイバーインシデント緊急対応企業一覧（特定非営利活動法人日本ネットワークセキュリティ協会）
   https://www.jnsa.org/emergency_response/

・「サーバーやクライアント、ネットワークに適切なセキュリティ対策を行う」

1. サイバーセキュリティ経営ガイドライン　付録B－2（経済産業省）
   https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_app_B-2.pdf
2. 国民のためのサイバーセキュリティサイト（総務省）
   https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/index.html
3. 「ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引」を策定しました（経済産業省）
   https://www.meti.go.jp/press/2023/07/20230728004/20230728004.html
4. 「ASM（Attack Surface Management）導入ガイダンス～外部から把握出来る情報を用いて自組織のIT資産を発見し管理する～」を取りまとめました（経済産業省）
   https://www.meti.go.jp/press/2023/05/20230529001/20230529001.html
5. ウェブサイトの攻撃兆候検出ツール　iLogScanner（IPA）
   https://www.ipa.go.jp/security/vuln/ilogscanner/index.html
6. サイバーセキュリティお助け隊サービス（IPA）
   https://www.ipa.go.jp/security/otasuketai-pr/index.html

・「適切なバックアップ運用を行う」

1. Data Backup Options（サイバーセキュリティ・インフラストラクチャセキュリティ庁）
   https://www.cisa.gov/sites/default/files/publications/data_backup_options.pdf
2. What is the 3-2-1 backup rule?（Veeam Software）
   https://www.veeam.com/blog/321-backup-rule.html

10 大脅威選考会

氏名	所属	氏名	所属
神山 太朗	あいおいニッセイ同和損害保険(株)	前田 誉彦	エムオーテックス(株)
橋田 幸浩	あいおいニッセイ同和損害保険(株)	和田 泰宜	エムオーテックス(株)
堀江 昌宏	AKKODiS コンサルティング(株)	猪俣 敦夫	大阪大学
石井 彰	旭化成(株)	姫野 猛	(株)オージス総研
高橋 広	旭有機材(株)	岡村 耕二	九州大学
宮﨑 清隆	ICMS(株)	小関 直樹	京セラ(株)
早崎 敏寛	(株)アシュアード	野中 義孝	京セラ(株)
岡田 良太郎	(株)アスタリスク・リサーチ	美濃部 啓介	京セラ(株)
中島 豊	アライドテレシス(株)	小松 佳昭	京セラコミュニケーションシステム(株)
石田 淳一	(株)アールジェイ	刀川 郁也	京セラコミュニケーションシステム(株)
岡田 琢央	Infoblox(株)	西山 健太	京セラコミュニケーションシステム(株)
一條 敦	ヴイエムウェア(株)	清水 将人	(一財)草の根サイバーセキュリティ推進協議会
橋本 賢一郎	ULTRA RED, Ltd.		(Grafsec)
徳丸 浩	EG セキュアソリューションズ(株)	小林 勝	キンドリルジャパン(株)
大桶 夏津	(株)エーアイセキュリティラボ	田中 真一郎	キンドリルジャパン(株)
関根 鉄平	(株)エーアイセキュリティラボ	吉田 未樹	キンドリルジャパン(株)
溝口 英利	(株)SRA	宮内 雄太	(一社)金融 ISAC
田中 潤子	(株)エーピーコミュニケーションズ	高崎 庸一	グローバルセキュリティエキスパート(株)
山根 康裕	(株)エーピーコミュニケーションズ	古澤 一憲	グーグル・クラウド・ジャパン(同)
佐藤 直之	SCSK(株)	遠藤 誠	(株)ケイテック
鈴木 寛明	SCSK(株)	武藤 孝浩	KDDI デジタルセキュリティ(株)
辻 伸弘	SB テクノロジー(株)	小熊 慶一郎	KBIZ / ISC2
大塚 淳平	NRI セキュアテクノロジーズ(株)	保村 啓太	KPMG コンサルティング(株)
芳賀 夢久	NRI セキュアテクノロジーズ(株)	坂 明	(公財)公共政策調査会
小林 淳史	(株)NTT-ME	森井 昌克	神戸大学
高橋 昌士	(株)NTT-ME	北田 高之	(株)神戸デジタル・ラボ
大湊 健一郎	NTT 社会情報研究所 NTT-CERT	バローズ ダニエル	(株)神戸デジタル・ラボ
今野 俊一	NTT 社会情報研究所 NTT-CERT	松田 康司	(株)神戸デジタル・ラボ
松橋 亜希子	NTT 社会情報研究所 NTT-CERT	前園 博文	コベルコシステム(株)
北河 拓士	NTT セキュリティ・ジャパン(株)	持田 啓司	サイバーセキュリティイニシアティブジャパン(CSIJ)
杉山 毅	NTT セキュリティ・ジャパン(株)	名和 利男	(株)サイバーディフェンス研究所
斯波 彰	NTT コミュニケーションズ(株)	福森 大喜	(株)サイバーディフェンス研究所
大石 眞央	(株)NTT データグループ	松本 純	サイボウズ(株)
大嶋 真一	(株)NTT データグループ	宮内 伸崇	(株)サイント
星野 亮	(株)NTT データグループ	木村 浩樹	(一社)JPCERT コーディネーションセンター
池田 和生	NTTデータ先端技術(株)		(JPCERT/CC)
植草 祐則	NTTデータ先端技術(株)	齋藤 美香	(一社)JPCERT コーディネーションセンター
永澤 貢平	NTTデータ先端技術(株)		(JPCERT/CC)
井上 茂	NTT ビジネスソリューションズ(株)	飯山 志保	(株)JR東日本情報システム
前田 典彦	(株)FFRI セキュリティ	佐藤 勤子	(株)JR東日本情報システム
中西 克彦	(株)FFRI セキュリティ	萩谷 文	(株)JR東日本情報システム
青山 昇司	MS&AD インターリスク総研(株)	阿部 慎司	GMO サイバーセキュリティ by イエラエ(株)
岡田 智之	MS&AD インターリスク総研(株)	熊坂 駿吾	GMO サイバーセキュリティ by イエラエ(株)
辻本 竜一	MS&AD インターリスク総研(株)	椎野 紘平	(株)JTB
前田 征大	エムオーテックス(株)	佐久間 義明	(株)JTB

氏名	所属	氏名	所属
唐沢 勇輔	Japan Digital Design(株)	大山 水帆	戸田市役所
大久保 隆夫	情報セキュリティ大学院大学	山室 太平	Trellix
伊東 寛	(国研)情報通信研究機構（NICT）	岡本 勝之	トレンドマイクロ(株)
印藤 晃	(国研)情報通信研究機構（NICT）	今 佑輔	トレンドマイクロ(株)
岡 邦彦	(株)スクウェア・エニックス	加藤 雅彦	長崎県立大学
山田 宜史	(株)スクウェア・エニックス	渡辺 研司	名古屋工業大学
竹林 和賢	スターネット(株)	須川 賢洋	新潟大学
山本 幸稔	スターネット(株)	柳 優	日本アイ・ビー・エム(株)
正木 義和	スワットブレインズ(株)	山下 慶子	日本アイ・ビー・エム(株)
東 恵寿	NPO セカンドワーク協会	高倉 万記子	(一財)日本情報経済社会推進協会（JIPDEC）
西本 伸夫	(株)西友	青木 聡	日本電気(株)
原子 拓	(株)西友	谷川 哲司	日本電気(株)
金城 夏樹	(株)セキュアイノベーション	上野 宣	(一社)日本ハッカー協会
佐久川 悠	(株)セキュアイノベーション	斎藤 健一	(一社)日本ハッカー協会
長谷川 陽介	(株)セキュアスカイテクノロジー	宮本 久仁男	(一社)日本ハッカー協会
阿部 実洋	(株)セキュアベース	大島 悠司	ニューリジェンセキュリティ(株)
上村 理	ゼットスケーラー(株)	仲上 竜太	ニューリジェンセキュリティ(株)
澤永 敏郎	ソースネクスト(株)	藤本 博史	ニューリジェンセキュリティ(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	小島 博行	(国研)農業・食品産業技術総合研究機構（農研機構）
坂本 高史	(株)ソニー・インタラクティブエンタテインメント	小林 克巳	(株)野村総合研究所
直井 信次郎	ソフトバンク(株)	山崎 英人	パーソルキャリア(株)
楢原 盛史	タニウム合同会社	渡辺 久晃	パナソニック(株)
鈴木 一弘	地方公共団体情報システム機構（J-LIS）	勝見 松則	パナソニックコネクト(株)
筒井 英樹	中外製薬(株)	高橋 洋一	パナソニックコネクト(株)
徳丸 力蔵	中外製薬(株)	常川 直樹	パナソニックコネクト(株)
戸田 貴裕	中外製薬(株)		情報経営イノベーション専門職大学
田中 卓朗	TIS(株)	浅野 貴志	パロアルトネットワークス(株)
三木 基司	TIS(株)	林 薫	パロアルトネットワークス(株)
中山 貴禎	(株)ディアイティ	安岡 祥吾	パロアルトネットワークス(株)
浅西 修	DXC テクノロジー・ジャパン(株)	川内 裕文	東日本電信電話(株)
遠藤 宗	DXC テクノロジー・ジャパン(株)	杉井 俊也	東日本電信電話(株)
大原 正嗣	DXC テクノロジー・ジャパン(株)	水越 一郎	東日本電信電話(株)
松本 隆	(株)ディー・エヌ・エー	折田 彰	(株)日立システムズ
吉村 修	デロイト トーマツ サイバー(同)	関谷 信吾	(株)日立システムズ
内山 巧	(株)電算	田中 秀和	(株)日立ソリューションズ
駒澤 悠二	(株)電算	沼田 亜希子	(株)日立製作所
近藤 修一	(株)電算	古賀 洋一郎	ビッグローブ(株)
河合 翔平	東京海上日動あんしん生命保険(株)	山口 裕也	(株)ファイブドライブ
花田 隆仁	東京海上日動火災保険(株)	大高 利夫	藤沢市役所
石山 圭佑	東京海上日動システムズ(株)	田中 昌弘	富士通(株)
今成 勇人	東京海上日動システムズ(株)	濱田 達也	富士通(株)
中西 祐介	東京海上日動システムズ(株)	原 和宏	富士通(株)
石川 朝久	東京海上ホールディングス(株)	菅原 尚志	フューチャー(株)
嶋谷 巧	東京海上ホールディングス(株)	荒井 大輔	(株)Bridge
富山 寛之	東京海上ホールディングス(株)	海老原 俊一	(株)Bridge
佐々木 良一	東京電機大学	柳川 俊一	(株)Bridge
小島 健司	(株)東芝	鴫原 祐輔	Blue Planet-works(株)
大浪 大介	東芝インフォメーションシステムズ(株)	倉田 尚希	(株)ベリサーブ
原田 博久	(株)Doctor Web Pacific	島田 敏宏	(株)ベリサーブ

氏名	所属	氏名	所属
太田 良典	弁護士ドットコム(株)	吉岡 克成	横浜国立大学
結城 亮史	(株)Box Japan	佐久間 矩仁	横浜市役所
垣内 由梨香	マイクロソフトコーポレーション	牧野 尚彦	横浜市役所
中西 基裕	(株)マクニカ	三国 貴正	(株)YONA
西城 秀行	三井住友海上火災保険(株)	橘 喜胤	楽天カード(株)
阿部 巧	(株)三井住友銀行	福本 佳成	楽天グループ(株)
武笠 雄介	(株)三井住友銀行	伊藤 彰嗣	楽天モバイル(株)
東内 裕二	三井物産セキュアディレクション(株)	稲葉 理沙	(株)ラック
篠原 巧	(株)三菱総合研究所	山崎 圭吾	(株)ラック
山中 翔太	(株)三菱総合研究所	若居 和直	(株)ラック
平田 真由美	みゅーらぼ	猪野 裕司	(株)リクルート
湯淺 墾道	明治大学	六宮 智悟	(株)リクルート
山岡 裕明	八雲法律事務所	有森 貞和	(株)両備システムズ
石井 崇喜	(株)ユービーセキュア	鈴木 堅太	(株)両備システムズ
髙木 勇史郎	(株)ユービーセキュア	矢儀 真也	(株)両備システムズ
谷島 有珠	(株)ユービーセキュア	清水 秀一郎	–
江面 祥行	(株)ユビテック	piyokango	–
島田 理枝	(株)ユビテック		

著作・制作　独立行政法人情報処理推進機構（IPA）

編集責任　土屋 正

イラスト製作　株式会社 創樹

執筆協力者　10 大脅威選考会

10 大脅威執筆者　土屋 正　篠塚 耕一　内海 百葉
亀山 友彦　大友 更紗　吉本 賢樹
丹野 菜美　田村 智和　大久保 直人
山下 恵一

IPA 執筆協力者　高柳 大輔　大澤 淳　山下 龍夫
板橋 博之　入澤 康紀　中島 尚樹
松坂 志　江島 将和　横山 尚人
小山 祐平　田島 凛

情報セキュリティ 10 大脅威 2024

2024 年 2 月 29 日 初 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/