情報セキュリティ
10 大脅威 2025
個人編

～どこから攻撃されても防御ができる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

2025 年 6 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　2025　個人編」
https://www.ipa.go.jp/security/10threats/10threats2025.html

目次

はじめに

本書「情報セキュリティ 10 大脅威 2025 個人編」は、情報セキュリティの専門家を中心に構成した「10 大脅威選考会」の投票により決定した「個人」向けの「10 大脅威」について解説した資料である。

各脅威と自身との関係や影響を確認しながら本書を読み進めることで、脅威の概要・手口・事例・対策について理解できる。

本書が、読者自身のセキュリティ対策への取り組み等に活用されることを期待する。

【本書の概要】

- 情報セキュリティ 10 大脅威 2025

2023 年版までは、ランクインした脅威を順位で紹介していたが、「上位の脅威＝危険度が高い」と捉えらないように、2024 年版から順位の表記をやめ、五十音順の表記としている。脅威の危険度は各人の立場や状況によって異なるため、「自分にとってどのような危険があるのか」を考えながら、脅威の解説を読んでほしい。

「個人」向けの「10 大脅威」では、10 個の脅威全てが 2023 年以降連続してランクインしている。「個人」向け脅威の攻撃手口は、古くから使われ続けているものが多い。このため本書で紹介している攻撃手口を知っておくだけでも被害への抑止効果は期待できる。

本書では、これら「個人」向けの「10 大脅威」について解説する。

情報セキュリティ10 大脅威 2025

情報セキュリティ 10 大脅威 2025

■「情報セキュリティ 10 大脅威 2025」

表 1.1 は 2024 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選ばれた、「情報セキュリティ 10 大脅威 2025」「個人」向け脅威である。

表 1.1 情報セキュリティ 10 大脅威 2025 「個人」向け脅威

「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	6 年連続 9 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	10 年連続 10 回目
クレジットカード情報の不正ログイン	2016 年	10 年連続 10 回目
スマホ決済の不正利用	2020 年	6 年連続 6 回目
偽警告によるインターネット詐欺	2020 年	6 年連続 6 回目
ネット上の誹謗・中傷・デマ	2016 年	10 年連続 10 回目
フィッシングによる個人情報等の詐取	2019 年	7 年連続 7 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	10 年連続 10 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	7 年連続 7 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	3 年連続 5 回目

■「情報セキュリティ 10 大脅威 2025」をお読みになる上での留意事項

1. 順位にとらわれず、立場や環境を考慮する

「情報セキュリティ 10 大脅威 2025」は、「10 大脅威選考会」の投票結果に基づき順位付けして「組織」と「個人」のそれぞれ 10 個の脅威を選定している。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、個人向けの脅威については順位を掲載していない。

例えば、個人がプライベートで、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」への対策の実施は必須になる。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」への対策も、同様に必須である。

順位に関わらず、自身が置かれている立場や環境を考慮して、自分に必要な対策を行う必要がある。

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 2025」で「10 大脅威」に選ばれなかった脅威の中には過去に「10 大脅威」として選ばれた脅威もある。「10 大脅威」に載っていなかったとしてもその脅威が消えたわけではない。例えば「インターネットバンキングの不正利用」等は、依然として被害が発生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 2025」以外の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[1]」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」にランクインした脅威以外にも多数の脅威が存在する。そして、「攻撃の糸口」は共通するものが多い。例えば、脆弱性を悪用する、マルウェアを使う、またはマルウェア等を使わずに情報を詐取するソーシャルエンジニアリングを使う等、技術の進歩、アプリやサービスが多様化した現在でも依然としてこれらの手口が使われている。

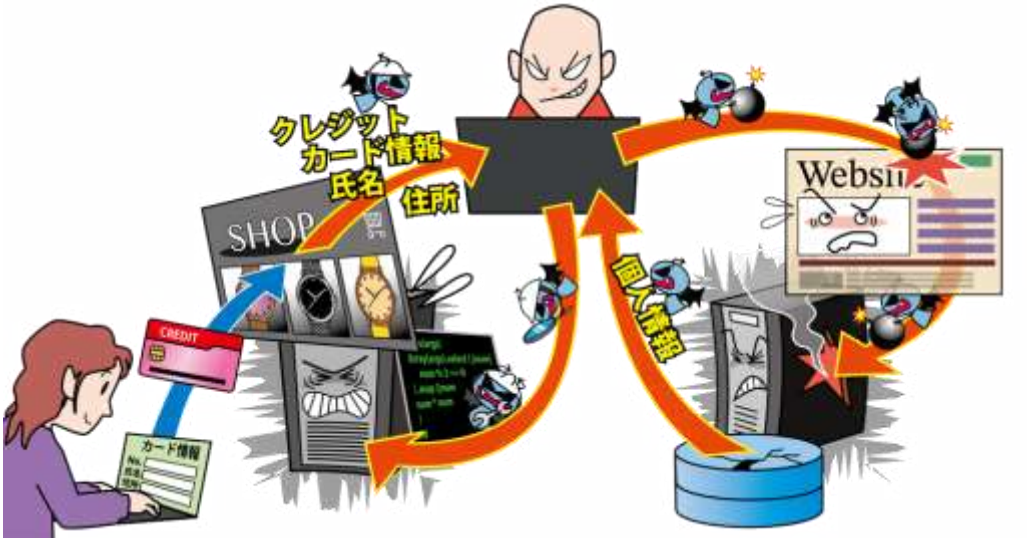
詳しくは「情報セキュリティ10大脅威 2015[2]」の1章で解説しているが、表 1.2 に示すように「攻撃の糸口」を 5 つに分類し、それぞれに該当する対策を「情報セキュリティ対策の基本」としている。「攻撃の糸口」に変化がない限り、「情報セキュリティ対策の基本」による効果が期待できるので、これを意識して継続的に対策を行うことで、被害に遭う可能性の低減が期待できる。

表 1.2 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、脆弱性の悪用による攻撃のリスクを低減する
マルウェアに感染	セキュリティソフトの利用	攻撃を検知してブロックする
パスワード窃取	パスワードの管理・認証の強化 ※「認証を適切に運用する」で詳細を解説	パスワード窃取による情報漏えい等のリスクを低減する
設定不備	設定の見直し	誤った設定を逆手にとった悪用を回避する
誘導（罠にはめる）	脅威・手口を知る	手口から重視すべき対策を理解する

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



ショッピングサイト（EC サイト）等のインターネット上のサービスに対して不正アクセスや不正ログインが行われ、サービスに登録されている個人情報等の重要な情報が窃取される被害が続いている。窃取された情報はダークウェブ（一般的な検索エンジンでは検出されない闇サイト）で拡散され、メールアドレスには詐欺メールが送りつけられ、クレジットカード情報は不正利用の可能性がある。

＜脅威と影響＞

多くの組織がインターネットを利用してサービスを提供している。ショッピング、教育、金融等、日々の生活に関わる色々な場面で利用されている。

サービスの利用には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）の登録が必要なものがある。

サービスを運営する組織は、サービスの維持、運用を適切に行う必要があるが、サービスを構成しているソフトウェアの脆弱性対策やセキュリティ対策が適切に行われていない場合がある。他方、サービスの利用者は、ログインのパスワードを複数のサービスで使い回している場合がある。

攻撃者は、これらの不備を悪用してサービスに不正アクセスし、利用者が登録している重要情報を窃取する。搾取された情報は売買や詐欺メールの送信などに利用されるため、搾取された情報に含まれる個人情報（クレジットカード情報など）が悪用されるおそれがある。

＜攻撃手口＞

◆サービスの脆弱性や設定不備を悪用

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のサービスに対して、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、サービスの脆弱性を悪用して Web サイトを改ざんし、情報の送信先や保存先を変更する場合もある。改ざんされた Web サイトに入力した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

例えば、A サービス等から窃取した認証情報（ID とパスワード）を悪用して別の B 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。詳細は個人編の脅威「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＞

◆不正アクセスによる顧客情報の漏えい

2024 年 5 月 24 日、積水ハウスはサイバー攻撃により顧客情報等が漏えいしたと発表した。同社の住宅オーナー向けの会員制サイト「積水ハウス Net オーナーズクラブ」のアクセス数が急増していたことから発覚した。同社が過去に使用していた Web ページのセキュリティ設定の不備をつかれ「SQL インジェクション」により、顧客（10 万 8,331 人）のメールアドレス・ログインID・パスワード、従業員等（18 万 3,590 人）のメールアドレス・パスワードが漏えいした。

同社は当該 Web サイトで使用しているパスワードを他のサービスで利用している場合は、変更するよう呼びかけている[3]。

◆通販サイトから個人情報とクレジットカード情報が漏えい

2024 年 5 月 17 日、全国漁業協同組合連合会（JF 全漁連）が運営する通販サイト「JF おさかなマルシェ ギョギョいち」本店が受けた不正アクセスについて、個人情報が漏えいした可能性があることを公表した。「クロスサイトスクリプティング」の脆弱性を悪用した不正アクセスにより、不正ファイルの設置およびペイメントアプリケーション（決済フォーム等）の改ざんが行われたことが原因としている。

漏えいした可能性がある情報は、会員登録された個人情報（氏名、生年月日、メールアドレス等）21,728 件と、2021 年 4 月 22 日から 2024 年 5 月 14 日の期間にサイトに登録されたクレジットカード情報（クレジットカード番号、有効期限、セキュリティコード）11,844 件であるとした。

通販サイトは 2024 年 10 月に閉鎖し、これまでに登録された個人情報は全て消去されることが案内された[4]。

◆転職支援サイトの個人情報が海外サイトに掲載

2024 年 6 月 4 日、WorkPort 社は運営する「転職支援サイト」において、第三者による不正アクセスを受けたと公表した。

同社の顧客情報の一部と一致する情報が海外の Web サイトに掲載されており、情報漏えいのおそれがあることが判明した。調査の結果、第三者が同社 Web サイトのサーバーの脆弱性を悪用して不正アクセスした上、不正ファイルを設置して情報を窃取した可能性があることが判明した。

漏えいしたおそれがある情報は、2019 年 1 月 1 日から 2024 年 4 月 19 日までに、会員登録された一部顧客の個人情報（氏名、生年月日、電話番号等）や会員登録時の情報（在住都道府県コード、希望勤務地コード、希望職種名）としている[5]。

＜対策と対応＞

個人（サービス利用者）

- 被害の予防
  - ・利用していないサービスは退会する
  - ・必須項目以外の情報は登録しない
    情報漏えいのリスクを考慮し、サービス利用に必要な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ワンタイムパスワードサービス、指紋や顔認証等、多要素認証の設定を有効にする
  - ・認証情報を適切に運用する ※
- 被害の早期検知
  - ・クレジットカード利用明細を定期的に確認する
    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。
  - ・漏えいしたメールアドレスが検索できるサービス[6]を使い、使用している情報が漏えいしていないか定期的に確認する
  - ・ログイン通知機能（ログインアラート機能）を有効にする
  - ・利用しているサービスのログイン履歴を確認する
- 被害を受けた際の対応
  - ・適切な報告/連絡/相談を行う ※
  - ・認証情報を適切に運用する ※
  - ・クレジットカードの利用を停止する

※対策の詳細は後述の「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

インターネットでサービスを利用する際に個人を識別するためにアカウントの作成が求められることがある。不正ログインはアカウントを作成した本人以外の第三者がログインを行い、アカウントの乗っ取りや、アカウントに紐づいた個人情報を窃取する事案である。よりセキュリティが強固といわれる多要素認証であっても利用者の情報リテラシーの低さから突破されるケースも確認されており、一層の注意が必要である。

＜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。使用する ID とパスワードは、フィッシング等で正規のサイトを模倣した偽サイトから詐取したもの、パスワードリストを用いる場合、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の提供内容、取り扱う情報に応じた被害に遭う。ショッピングサイトであれば、サイトに登録している氏名、住所、電話番号等の個人情報やクレジットカード情報等の窃取、商品の不正購入やサイト内のポイントの盗用が被害として想定される。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、チャージした残高やポイントを不正に利用される。LINE や Instagram 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の覗き見、投稿の削除、フィッシング詐欺につながる内容の投稿等を行われる被害を受けるおそれがある。

＜攻撃手口＞

◆フィッシング詐欺

もっともらしい文面のメールや SMS（電話番号宛に短いメッセージを送受信するサービス）等で、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。詳細は個人編の脅威「フィッシングによる個人情報等の詐取」を参照すること。

◆マルウェア感染

攻撃者の用意した Web サイトにアクセスさせたり、メールに添付したファイルを開かせたりすることで、利用者の端末をマルウェアに感染させる。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 やパスワードを窃取され、不正ログインに使われる。

◆パスワードリスト攻撃

闇サイトでの購入等、何らか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、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 ID とパスワードを使い回してい

ると、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

パスワードに使われることの多い固有名詞などの文字列、数字を類推し、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）などである。

＜事例または傾向＞

◆不正ログインによるサービスの不正利用

2024 年 9 月、日産自動車のカーシェアサービス「NISSAN e-シェアモビ」において自社運用システムに不正ログインがあり、車両の不正利用があったと発表された。加えて不正ログインの際に顧客情報の一部が閲覧された可能性を完全に否定することが難しいとして、個人情報保護委員会への報告と警察に被害届を出したという[7]。

◆フィッシングの連鎖被害

2024 年 5 月、明治薬科大学は教員がフィッシングサイトに Microsoft 365 のログイン情報を入力したことにより、海外から不正ログインがあったことを公表した。更に、不正ログインされた教員アカウントを悪用され、Outlook から 5,600 件超の教員を騙ったフィッシングメールが送信された。その内容を信用した学生約 30 名が自身のログイン情報を入力してしまったという[8]。

◆パスワードリスト攻撃による不正ログイン

2024 年 7 月 10 日から 18 日にかけて、LINE ビジネス ID の一部において、パスワードリスト攻撃が複数回あり、不正ログイン、及び不正ログインに成功した攻撃者による不正操作が行われていたと、LINE ヤフー社が同年 8 月に発表した。同社によれば、被害に遭ったアカウントは全て 2 段階認証を設定していなかったという[9]。LINE ビジネス ID では 2 段階認証機能を提供しており、利用者に対して各自で設定することを強く推奨した[10]。

◆証券会社への不正アクセス・不正取引が急増

2025 年 4 月 3 日、金融庁は、実在する証券会社の Web サイトを装ったフィッシングサイト等で窃取した顧客情報を用いて、インターネット取引サービスでの不正アクセス・不正取引の被害が急増しているとして、注意喚起を行った[11]。

また、2025 年 5 月 2 日、日本証券業協会は大手証券やネット証券 10 社と協議を行い、被害補償を行う方針を公開している[12]。

＜対策と対応＞

個人（サービス利用者）

- 被害の予防
  - ・本書の表 1.2「情報セキュリティ対策の基本」を実施する
  - ・ID とパスワードを入力する Web サイトは、あらかじめブックマークし、ブックマークからのみアクセスする
  - ・危険な Web サイトのアクセスをブロックする
    セキュリティソフトを導入し、アクセスブロック機能を活用する。
  - ・メールの添付ファイルの開封、メールや SMS の URL リンクのクリックを安易にしない ※
  - ・認証情報を適切に運用する ※
  - ・利用しているサービスのワンタイムパスワードサービス、指紋や顔認証等、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
  - ・利用頻度が低いサービスではクレジットカード情報を登録せず、都度入力する
- 被害の早期検知
  - ・ログイン通知機能（ログインアラート機能）を有効にする
  - ・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を定期的に確認する
- 被害に遭った際の対応
  - ・クレジットカードの利用を停止する
  - ・適切な報告/連絡/相談を行う ※

※対策の詳細は後述の「共通対策」を参照

クレジットカード情報の不正利用

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、クレジットカードは日常的に利用されている。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性を悪用した Web サイトの改ざん等によって、クレジットカード情報が詐取され、不正利用される被害が発生している。また、持ち主がカード会社に連絡して利用を停止しても、不正利用が継続するオフライン決裁を悪用した手口も確認されている。

＜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＞

攻撃者は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。

◆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入力させ詐取する。詳細は個人編の脅威「フィッシングによる個人情報等の詐取」を参照すること。

◆ウェブスキミング

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。利用者が改ざんされた決済画面にクレジットカード情報を入力してしまうと攻撃者にその情報を詐取される[13]。

◆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。

◆マルウェア感染

メールの受信者に、添付ファイルや本文中の悪意ある Web サイトのリンクを開かせることで、端末をマルウェアに感染させる。マルウェアに感染した端末で、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、闇サイト等で売買されることもある。

＜事例または傾向＞

◆同一会社で運営する2つの Web サイトでクレジットカード情報流出

2024 年 8 月、エーデルワイスは、運営している「アンテノール オンラインショップ」および「ヴィタメール オンラインショップ」において、それぞれ 7,018 件、45,355 件のクレジットカード情報が流出したおそれがあると公表した。外部機関からの指摘により発覚し調査を行ったところ、2024 年 5 月までの数年間に利用されたクレジットカード情報が漏えい、不正利用されたおそれがあることが判明した。情報流出の原因としては、オンラインショップのシステムの一部の脆弱性が悪用されたことによる第三者に不正アクセスにより、ペイメントアプリケーション（決済フォーム等）の改ざんが行われたためとしている[14]。

◆「タリーズ オンラインストア」でクレジットカード情報流出

2024 年 10 月、タリーズコーヒージャパンは、運営している「タリーズ オンラインストア」で 2021 年 7 月から 2024 年 5 月にかけて利用された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。同年 5 月、第三者による不正アクセスを受け、その調査を行ったところ情報の流出が判明した。調査結果によると、漏えいした利用者の個人情報は 92,685 件で、そのうちクレジットカード情報を含む件数が 52,958 件であった。クレジットカード番号、カード名義人名、有効期限に加え、セキュリティコードも漏えいした可能性があるとしている。攻撃者に当該 Web サイトのシステムの一部の脆弱性を悪用され、ペイメントアプリケーション（決済フォーム等）の改ざんが行われたことを原因としている[15]。

◆不正利用被害額が過去最高

2025 年 3 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、2024 年 1 月～12 月の年間被害額は 555.0 億円で、2023 年の年間被害額 540.9 億円よりも増加し、過去最悪の被害額となった[16]。

＜対策と対応＞

個人（利用者）

- 被害の予防
  - ・本書の表 1.2「情報セキュリティ対策の基本」を実施する
  - ・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の開封、メールや SMS の URL リンク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、デビットカード利用を検討する
  - ・クレジットカードの利用可能枠（利用限度）を抑える
  - ・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および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を定期的に確認する
  - ・サービス利用状況の通知機能を利用する
- 被害を受けた際の対応
  - ・クレジットカードの利用を停止する
  - ・クレジットカードの利用停止後も不審な利用履歴がないか確認する
  - ・マルウェア感染した端末を初期化する
  - ・適切な報告／連絡／相談を行う ※
  - ・認証情報を適切に運用する ※

組織（事業者）

- 被害の予防
  - ・適切なクレジットカード情報の保護対策を行う
  - ・適切な不正利用対策を行う[17]

※対策の詳細は後述の「共通対策」を参照

スマホ決済の不正利用

近年、スマートフォンの普及に伴い、スマートフォンを利用したキャッシュレス決済（スマホ決済）の利用が急増している。便利な支払い方法として、多くの人々が日常的に利用していることから、不正利用のリスクが高まっている。第三者のなりすましによる不正な取引などで、金銭的被害が確認されている。

＜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方法（非接触型決済、タッチ決済[18]）
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ことが多い。

攻撃者は、不正に入手した ID とパスワードを使い、決済サービスに不正ログインを行う。さらに、そこで窃取したクレジットカード情報を用いて、別の決済サービスに登録して不正なスマホ決済を行う。不正利用されると金銭的被害を受けるおそれがある。

＜攻撃手口＞

◆スマートフォンのキャッシュレス決済を悪用

フィッシングサイトに誘導し、ログイン情報やクレジットカード番号などの決済情報を窃取する。窃取したカード情報をスマートフォンの決済サービスに登録する。その後、店頭でスマートフォンのキャッシュレス決済を使い、商品を購入する。

◆スマートフォンのオフライン決済を悪用

スマートフォンのタッチ決済にはサインや暗証番号の入力が不要なオフライン決済があり、利用金額や利用回数の制限内であれば、クレジットカードの利用停止手続き後でも、決済可能である。このため、POSA（ポサ）カード（iTunes カード、Amazon ギフトカード等）をはじめとする少額商品を制限内で購入する。

◆スマホ決済の送金サービスを悪用

ネットショッピングなどで商品を購入した後、販売業者からメールや電話で「欠品のため注文をキャンセルして返金する」等の連絡があり、返金手続きのために「〇〇ペイ」などの決済アプリを使うよう指示される。攻撃者は、返金用と称して送金用の設

定を指示する。これに気づかず利用者が指示に従うと、返金ではなく攻撃者への送金となる。

◆不正ログイン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、スマホ決済に不正ログインし、アカウントを乗っ取る。乗っ取ったアカウントでスマホ決済を行う。

不正ログインの手口については、個人編の脅威「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＞

◆タッチ決済を悪用したクレジットカード不正利用

スマートフォンのタッチ決済機能を悪用した不正利用が報告されている。

大阪府の 30 代の女性は、クレジットカードを停止したにもかかわらず、毎日 1 万円ずつ不正利用され、2 か月間で 23 万円が不正利用された。

また、北海道の 60 代の女性はフィッシングメールからフィッシングサイトに誘導され、クレジットカード情報を入力してしまった後、iPhone を使った電子決済サービス「Apple Pay」にクレジットカード情報が登録された通知を受けた。クレジットカードの利用を停止したが、覚えのない少額の利用明細が 30 回以上届き、総額で約 24 万円を不正利用された。

クレジットカード会社からは、オフライン決済を悪用されている可能性を示唆されており、不正利用をすぐに止められない状況であった[19]。

◆〇〇ペイでの返金を装った詐欺

〇〇ペイ等のコード決済サービスを悪用して金銭を騙し取る手口に関する相談が依然として全国の消費生活センター等に寄せられている。

2024 年 4 月、10 代男性がインターネットで洋服を注文し、電子マネーで約 7,000 円を支払った。その後、事業者から「在庫がないので返金する」と連絡があり、返金手続きのために LINE アカウントの友だち登録を行った。LINE に送られてきた QR コードを読み取り、事業者からの指示に従い、返金コードとして『99980』を入力したが返金はされず、実際にはスマホ決済により 9 万 9,980 円を送金してしまった。

国民生活センターは、〇〇ペイによる返金詐欺について、2024 年 12 月に注意喚起を行った[20]。

＜対策と対応＞

個人（スマホ決済サービス利用者）

- 被害の予防
  - ・本書の表 1.2「情報セキュリティ対策の基本」を実施する
  - ・利用しているサービスのワンタイムパスワードサービス、指紋や顔認証等、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

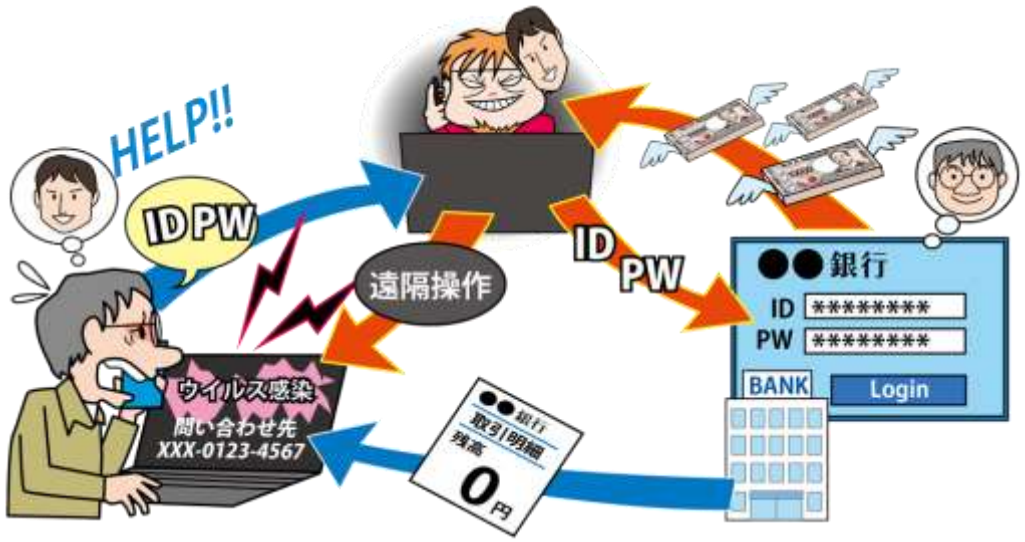
    仮にパスワードが攻撃者に漏えいしたとしても、不正ログインや、その後の金銭被害につながる操作を阻止できる確率を高める。
  - ・認証情報を適切に運用する ※
  - ・フィッシングに注意する

    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は退会する
  - ・スマートフォンの紛失時の対策を行う

    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を行う
  - ・連携する銀行口座の出金履歴やクレジットカード利用履歴を確認する
- 被害を受けた際の対応
  - ・必要に応じて連携しているクレジットカードの利用を停止する
  - ・認証情報を適切に運用する ※
  - ・適切な報告／連絡／相談を行う ※

※対策の詳細は後述の「共通対策」を参照

偽警告によるインターネット詐欺



Web サイトの閲覧中に、突然偽のセキュリティ警告画面が表示され、様々な方法で不安を煽られた閲覧者が画面上の指示に従ってしまうことで金銭を騙し取られる被害が発生している。画面指示に従い、ソフトウェアやスマホアプリを購入してしまうことや、偽の警告画面上の電話番号に連絡してしまい、サポート窓口を装った詐欺グループからサポート料金の請求や遠隔操作を介した金銭の詐取被害（サポート詐欺）を受けてしまう。

＜脅威と影響＞

Web サイトを閲覧中に、「マルウェアが見つかりました」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、閲覧者に通知内容を信用させて指示に従うよう誘導してくる。

画面の指示に従ってしまうと、ソフトウェアやスマホアプリを購入させられてしまうおそれがある。また、偽のサポート窓口に連絡してしまうと、その企業の社員を装った詐欺グループから、マルウェア駆除を名目に遠隔操作ソフトウェアのインストールに誘導され、最終的に PC やスマートフォンを遠隔操作され、サポート料金や修復費用を請求される。

さらに、ソフトウェアの購入やサポート時に入力した氏名、メールアドレス、クレジットカード情報等の個人情報が、別の詐欺への悪用、遠隔操作による漏えい等の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り、警告音を鳴らす、警告メッセージを音声で流す、偽警告のポップアップ画面を閉じられないと誤認させるといった細工により閲覧者の不安を煽る。

IPA では、偽警告の「手口検証動画[21]」や偽警告画面の閉じ方を説明した「偽セキュリティ警告（サポート詐欺）対策特集ページ[22]」を公開している。特集ページ内には偽警告の閉じ方の体験サイトも準備してあるので体験しておくとよい。

◆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、遠隔操作ソフトウェアをインストールさせる。その上で、マルウェア駆除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、クレジットカード決済が用いられる。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場合もある。

◆セキュリティソフトやスマホアプリのインストール・購入に誘導

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のインストールへ誘導する。また、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、最終的にソフトウェアの購入へ誘導する。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ることが目的と考えられる[23]。

＜事例または傾向＞

◆偽警告によるサポート詐欺で 1,000 万円の被害

2024 年 3 月、笛吹市商工会は偽警告によるサポート詐欺の被害に遭ったことを公表した。職員は、PC でインターネットを閲覧していた際、「トロイの木馬に感染した」との警告が表示され、画面上の連絡先に電話をしてしまった。マイクロソフト社の社員をかたる応答者の指示により、業務用 PC に遠隔操作ソフトウェアをインストールしたほか、インターネットバンキングの ID・パスワードも教えてしまったという。その結果、同日中に 3 回にわたり計 1,000 万円が犯人の口座に送金されてしまった[24]。

◆操作不能の偽メッセージが登場

2024 年 6 月、従来の偽警告の対処方法であるブラウザを閉じることでは対処できない操作不能の偽メッセージによる被害が確認された。PC の利用中に、突然画面全体に偽メッセージが表示され、操作不能となり、サポート窓口へ電話するよう促される。原因としては、被害の前にブラウザから意図しないソフトウェア等をインストールしてしまったことが推定されており、そこから PC を遠隔操作され、PC のロック、設定変更、偽メッセージの表示等が行われた可能性がある。信頼できないサイトから、意図せずダウンロードされてしまったファイルはクリックしないことが対策として挙げられる[25]。

◆偽警告被害の相談件数が過去最多

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、2024 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 4,791 件[26]で、年間の相談件数で過去最多だった 2023 年の 4,145 件[27]を超えた。また、2024 年 4 月の相談件数は 828 件で、月間の相談件数の過去最多となっている[28]。

＜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）
  - ・本書の表 1.2「情報セキュリティ対策の基本」を実施する
  - ・危険な Web サイトのアクセスをブロックする
    セキュリティソフトを導入し、アクセスブロック機能を活用する。
  - ・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人に相談する。
  - ・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。
  - ・サポート料金を支払わない[29]
    プリペイド型電子マネーの購入はしない、遠隔操作された状態でネットバンキングの画面を開かない。
  - ・偽警告が表示されたらブラウザを終了する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[30]に相談する。
  - ・ブラウザの通知機能を不用意に許可しない[31]
    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を設定する
- 被害を受けた際の対応
  - ・PC を遠隔操作された場合は初期化やシステムの復元を行う
  - ・スマホアプリをアンインストールする
    自動継続課金が設定をされていないかを確認し、設定されていたら解除する。
  - ・適切な報告/連絡/相談を行う

※対策の詳細は後述の「共通対策」を参照

ネット上の誹謗・中傷・デマ

インターネットで自分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、発信した情報に端を発して、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。

＜脅威と影響＞

SNS の普及に伴い、個人が匿名で、広範囲への発信が容易になっている。そして、そのサービスを利用し、意図的な誹謗・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、名誉毀損等の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できる

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。特定の個人や企業に対する意見・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することで問題となるケースがある。他方で、SNS での収益化を狙い、センセーショナルな内容を意図的に拡散するような行為も見受けられる。匿名での発信なら身元がばれないとの誤解が内容を過激にしやすい一因として挙げられる。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を見た第三者が、真偽を確認せずに無自覚に拡散させる。そして、伝言ゲームのように別の第三者が更に拡散させることで、誹謗・中傷やデマが広がっていく。この際、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＞

◆誹謗・中傷したタレント、芸能活動を休止

2024 年 8 月、お笑いタレントの SNS 投稿を引用する形で、別のタレントが誹謗・中傷する投稿を行い、物議を醸した。誹謗・中傷したタレントは、その投稿を削除した後、謝罪の投稿を行い、お笑いタレント本人へも直接謝罪をしたが騒動は収まらず、後日、芸能活動の休止を発表した[32]。

◆倫理観を欠いた投稿をした医師、解任

2024 年 12 月、グアムの大学で実施された解剖研修の様子を SNS とブログに投稿した医師が解任された。投稿には、献体の前とみられる場でピースサインをしている医師の写真等が含まれていた。同投稿はすぐに拡散され、「死者への冒涜だ」といった批判や、医師免許の取り消しを求める声が相次いだ。その後、同医師は謝罪文を投稿した。

他方、2025 年 3 月、日本解剖学会は、篤志解剖全国連合会、日本篤志献体協会と共同で「献体解剖倫理指針」を公表した。同指針では、献体解剖に関する行動規範が示されており、その中で「スマートフォンなど撮影機能のある電子機器を実習室内に持ち込まないこと」と明記された[33]。

◆情報流通プラットフォーム対処法の施行

2025 年 4 月、従来の「プロバイダ責任制限法[34]」に替わり「情報流通プラットフォーム対処法（正式名称：特定電気通信による情報の流通によって発生する権利侵害等への対処に関する法律）」が施行された。同年 4 月 30 日にはまず、Google、LINE ヤフー、Meta Platforms、TikTok、X の 5 社が大規模プラットフォーム事業者として指定された。施行に伴い、大規模プラットフォーム事業者は、削除対応の迅速化や、運用状況の透明化の措置が義務づけられた。具体的には、削除申出の窓口や手続きを整備して公表することや、削除基準を策定して公表すること等が義務づけられたものである。この法律に関して、総務省から規定の明確化を図るためのガイドラインが公表されている[35]。

＜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）

・情報リテラシー、情報モラルを向上させる、法令遵守の意識を向上させる ※

・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。

・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、投稿や拡散が問題ない内容か事前に確認する。

・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。発信者を特定することは可能であるため、投稿や拡散する内容によっては犯罪になりうるという認識を持ち、発信する内容に十分に留意する。

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、情報モラルを向上させる ※

個人（被害者）

● 被害を受けた際の適切な対応

・管理者やプロバイダーへ削除依頼を行う

問題ある投稿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

※対策の詳細は後述の「共通対策」を参照

フィッシングによる個人情報等の詐取

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。

＜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（URL が仕込まれている文字列や画像を含む）にアクセスしてしまう[36]。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、そのフィッシングサイトに閲覧者を誘導するために、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。それを真に受けた受信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情報、ID・パスワード情報等の重要情報を入力させ、情報を詐取する。URL は表記上の見た目と実際のリンク先 URL が異なるものもある。

◆フィッシングの手口

クイッシングは、フィッシングサイトの誘導に QR コードを使用する手口のこと。

スミッングは、クレジットカード系ブランドや電力会社、宅配業者の不在通知等を装った SMS を送信し、フィッシングサイトに誘導する手口のこと。

いずれも近年多く確認されている手口であり、フィッシングサイトで個人情報やクレジットカード情報を入力させ、その情報を詐取するものである。

また、新たに電話による自動ガイダンスを悪用する手口であるビッシングも確認されている。

◆緊急性を訴え、冷静な判断をさせず巧みに誘導

フィッシングに使われるメールは、送信元や URL リンクが偽装され、AI 利用で日本語表現に違和感がなくなってきている。さらに本日中などと猶予の無い期限を設け、対応しなければサービスを停止するなどと緊急性を強調することで、利用者の冷静

さを失わせ、フィッシングサイトへ巧妙に誘導する文面になっている。

また、「セキュリティ強化のための本人確認（お知らせ）」や「ポイントプレゼント」など利用者の興味を引き、本日中や明日中など短い期限内にアクセスを急がせる内容のフィッシングメールも確認されている。

＜詐取した情報の悪用例＞

- 詐取した個人情報を闇サイトで販売し、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、物品の購入、その転売などで金銭を得る。

＜事例または傾向＞

攻撃者からのフィッシングメール配信数は増加傾向にあり、フィッシング対策協議会への 2024 年フィッシング詐欺報告件数は過去最多となった[37]。

◆e-Tax を装ったフィッシング

2024 年 2 月と 5 月、国税庁は e-Tax を装った不審なメールについて注意喚起を行った。「税務署からのお知らせ【e-Tax 個人アカウントの登録確認に関する重要なお知らせ】」や「e-Tax 税務署からの【未払い税金のお知らせ】」等といった不審なメールが確認されており、e-Tax の利用開始届出を模した偽サイトへ誘導する。誘導先のサイトでは個人情報、クレジットカード情報等が詐取される[38]。

◆メガバンクだけではない、JA バンクやろうきんを装ったフィッシング

2024 年はメガバンクや地銀のほかに JA やろうきんを騙るフィッシングを確認した。

口座凍結、取引状況確認、利用制限、アンケートなどの文言で誘い、本日中や明日中に対応するように急かしつつフィッシングサイトへ誘導する。誘導先のサイトではパスワードを含むログイン情報、個人情報、キャッシュカードの暗証番号等が詐取される[39]。

◆QR コードを用いたフィッシング

2024 年には、銀行を装い QR コードから誘導するメールが確認されている。メール本文には、フィッシングサイトへの URL を変換した QR コードが貼り付けられ、アクセスすると本物と見分けのつかないフィッシングサイトへ移動し、パスワードを含むログイン情報、クレジットカード情報、個人情報等が詐取される[40]。

＜対策と対応＞

個人（インターネット利用者）[41]

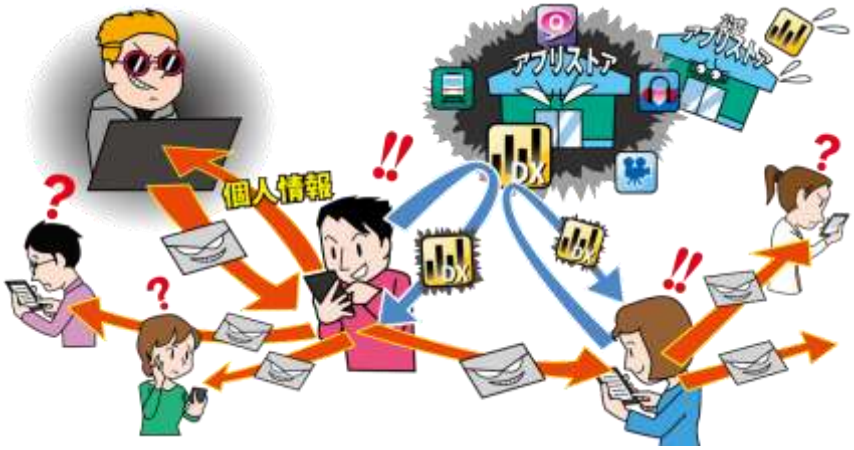
- 被害の予防（被害に備えた対策含む）
  - ・本書の表 1.2「情報セキュリティ対策の基本」を実施する
  - ・突然届いた身に覚えのないメールや SMS は基本的に無視して削除する
  - ・メールや SMS の URL リンクを安易にクリックしない、QR コードに安易にアクセスしない ※
  - ・利用しているサービスの多要素認証の設定を有効にする
  - ・迷惑メールフィルターを利用する
  - ・危険な Web サイトのアクセスをブロックする
    セキュリティソフトを導入し、アクセスブロック機能を活用する。
- 被害の早期検知
  - ・ログイン通知機能（ログインアラート機能）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。
  - ・クレジットカードの利用明細やインターネットバンキング等口座の利用状況をこまめに確認する
- 被害を受けた際の対応
  - ・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

（根本的な対策とはならないが、メールアドレスの漏えいを懸念した対応）

- ・認証情報を適切に運用する ※
- ・クレジットカードの利用を停止する
- ・適切な報告/連絡/相談を行う ※

※対策の詳細は後述の「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



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情報窃取や不正操作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 をタップさせる、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、SNS でダウンロードサイトに誘導する等、様々な手口が確認されている。

＜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様々な情報の窃取やスマートフォンの不正操作のおそれがある。認証情報を窃取された場合は、キャリア決済等を悪用した金銭被害やオンラインサービス等への不正アクセスにもつながる。また、DDoS 攻撃（分散型サービス妨害攻撃）の踏み台に利用される等、スマートフォンが悪用されても被害に気付かないおそれがある。

さらに、不正アプリによって窃取されたアドレス帳内の電話番号やメールアドレスあてに、不正アプリをインストールさせるためのメールや SMS が送信され、被害が一層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 を用いたダウンロードサイトへの誘導や、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。なお、ダウンロードサイトは、実在する Web サイトを装った作りになっており、そこに表示される不正アプリも実在するアプリを模したものとなっている場合もある。そのため、ユーザーが偽のダウンロードサイトや不正アプリとは気付きにくいものになっている[42]。

◆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、アプリの更新時に更新版のアプリが悪意ある機能を有効にして、不正行為を行う。

＜事例または傾向＞

◆不正アプリでスマートフォンが犯罪インフラに

2024 年 11 月、日本サイバー犯罪対策センター（JC3）は、不正アプリを介して意図せず犯罪に悪用されているスマートフォンが国内で数千台規模存在するとみられると注意喚起を行った。

攻撃者は、実在する企業等の名を騙る SMS でフィッシングを行う。利用者に不安や焦りを与えるような内容により、記載されている URL にアクセスさせ、様々な理由を付けて不正なアプリをインス

トールするよう促し、あたかも正規なアプリであると誤信させてインストールさせる。

この不正アプリは、バックグラウンドで稼働する仕組みで、攻撃者からの指令を受信すると、不特定多数の電話番号あてに SMS を送信する機能を有しているという。また、スマートフォン自体も普段どおり利用できるため、異変に気付きにくく、悪用が継続され、犯罪インフラと化しているという[43]。

◆マイナポータルの偽アプリ、デジタル庁が注意喚起

2024 年 3 月、デジタル庁は、マイナポータルの偽サイト、偽アプリへ誘導する事案を確認したとして、注意喚起を行った。

これは、メールや SMS ではなく、年金事務所を騙る電話により、手続きと称して偽サイトへアクセスするよう指示され、apk ファイル（Android にアプリをインストールするためのファイル）をダウンロードしてインストールするよう誘導させられる手口という。本事例は、IPA の情報セキュリティ安心相談窓口にも相談が寄せられており、X（旧 Twitter）及び Facebook にて注意喚起を行っている[44]。

◆偽アプリによる SNS 投資型詐欺、急増

実在する投資アプリを模した偽アプリを用いた SNS 投資型詐欺が急増し、広島県警は動画配信等による注意喚起を行った。

この手口は、SNS でのやりとりで言葉巧みに公式マーケットを模した偽サイトから偽アプリをダウンロードさせ、利用者に取引のための資金を指定口座に送金させる。アプリ上では利益が出ているように見えるものの、実際には取引は行われておらず、送金した資金は戻ってくることはないという[45]。

＜対策と対応＞

個人（スマートフォン利用者）

● 被害の予防

・本書の表 1.2「情報セキュリティ対策の基本」を実施する

・アプリは公式マーケットから入手する

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、アプリ開発者の情報、更新履歴等も確認し、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

アプリインストール時にアクセス許可を要求された権限が、アプリの機能に対して適切かどうかを確認する。そのため、アプリの機能を理解することが肝要である。特にデバイス管理者の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する

−Android 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 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

アプリの機能が利用目的と一致しないようであれば、インストールしない。

・インストールされているアプリを確認する

現在、どのようなアプリがスマートフォンにインストールされているのか把握する。もし、利用しなくなったアプリやインストールした覚えのないアプリがあれば、アンインストールする。

・アプリ更新時に更新内容を確認する

アプリの更新時には、更新内容を確認し、不審な機能、悪意ある機能が追加・有効にされている場合はアンインストールする。

● 被害を受けた際の対応

・不正アプリのアンインストールや端末の初期化

アンインストールできない場合は端末を初期化する。

・認証情報を適切に運用する ※

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。

※対策の詳細は後述の「共通対策」を参照

メールや SMS 等を使った脅迫・詐欺の手口による金銭要求

情報技術の進展に伴い、連絡やコミュニケーション手段が多様化し、これら各種サービス等を悪用した詐欺が横行している。詐欺の内容は人の弱みに付け込むものや、公的機関を装い相手を信用させた上で不安を煽るもの、そして、親交を深めて相手を騙すものなどがある。これらの詐欺は、メールや SMS 等非対面のコミュニケーション手段を使い行われることが多い。また、これら詐欺の手口は様々だが、目的は金銭の詐取である。

＜脅威と影響＞

金銭詐取を目論む詐欺グループは、ターゲットとなる個人に脅迫や詐欺のメッセージを送り付ける。その内容は、基本的に虚偽であるが、不安を煽る内容も含まれ、受信者は、その内容を信じてしまうおそれがある。虚偽であっても、その内容がたまたま自分に心当たりのある後ろめたい内容であると周囲に相談できず、騙しに気がつけず、発覚が遅れるおそれもある。さらに、募金詐欺の場合、受信者はお金を振り込んでしまっても、そもそも詐欺であったことに気付いていない可能性もある。

そして、一度でもこのような手口が成功すると、それが有効であると判断し、同様の手口を多方面に繰り返す傾向にある。これにより、新たな被害者を次々と生み、被害が拡大していくおそれもある。

＜手口＞

◆メールや SMS による脅迫

脅迫や架空請求によって金銭を要求する内容のメッセージを不特定多数の人に送り、金銭を詐取しようとする。支払方法は、足がつかないよう、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ある。

◆性的な脅し（セクストーション）

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。詐欺グループは、ターゲットに対して 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、相手の連絡先を窃取した上で、恥ずかしい動画のやり取りを知人にばらすと脅し、金銭を要求する。

◆ハッキングを装う

詐欺グループは、あらかじめ外部のサービスから詐取・窃取された個人情報を基に、ターゲットにパスワードや住所等の個人情報を記載したメッセージを送信する。そして、あたかも受信者の 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信用の高い組織を装い、不安を煽る内容のメールを送りつけ、受信者自らがメールに記載された連絡先に電話するように仕向ける。電話すると、詐欺グループは公的機関の担当者であると騙り、事態の重要度や緊急度を説明することで相手の不安を更に大きくし、金銭の振り込みを要求する。これとは別に、詐欺グループから金銭を要求する電話を掛け、その後に弁護士を装った和解を勧める旨のメールを送信して、金銭を騙しとる手口もある。

◆SNS 等で親交を深める

SNS を利用して有名人を装い、親交を深めた上で投資の勧誘を行う詐欺が行われている。

インターネットから見つけてきた写真を自分のプロフィール写真として登録するなどして海外の異性を装い、SNS 上で交際を持ち掛ける。そして、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、投資を勧誘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＞

◆SNS 型投資詐欺の被害額は前年比 3 倍

警察庁の発表によれば、2024 年 1 月から 12 月までの SNS 型詐欺（投資・ロマンス詐欺）の被害額は 1,200 億円を超え、前年比では約 280%となり、過去最悪を記録している。

投資詐欺の場合、当初接触は instagram、Facebook 等、SNS のバナー等広告が最も多く、次いでダイレクトメッセージで、これらの合計で 7 割を超えるという。

ロマンス詐欺では当初接触に使われるツールはマッチングアプリが約 34%と最も多く、次いで、instagram、Facebook の SNS が続く。そしてこれらツールのダイレクトメッセージ機能を使い接触するという。被害者を年代別にみると男女共、40 歳、50 歳、60 歳代の合計が 7 割を超える[46]。

◆約 2 億 2,400 万円のロマンス・投資詐欺被害

2024 年 7 月、60 歳代の男性が SNS で女性とされる人物と知り合い、趣味の話で意気投合した上で、投資話を持ち掛けられた。8 月以降、投資を始め、最終的に 2 億 2,400 万円を指定の口座に振り込んだという。その後、「アカウントが疑われて現金の引き出しが停止された。解除するには 3 千万円が必要だ」というメッセージが届き、警察に相談し、初めて詐欺に気が付いたという[47]。

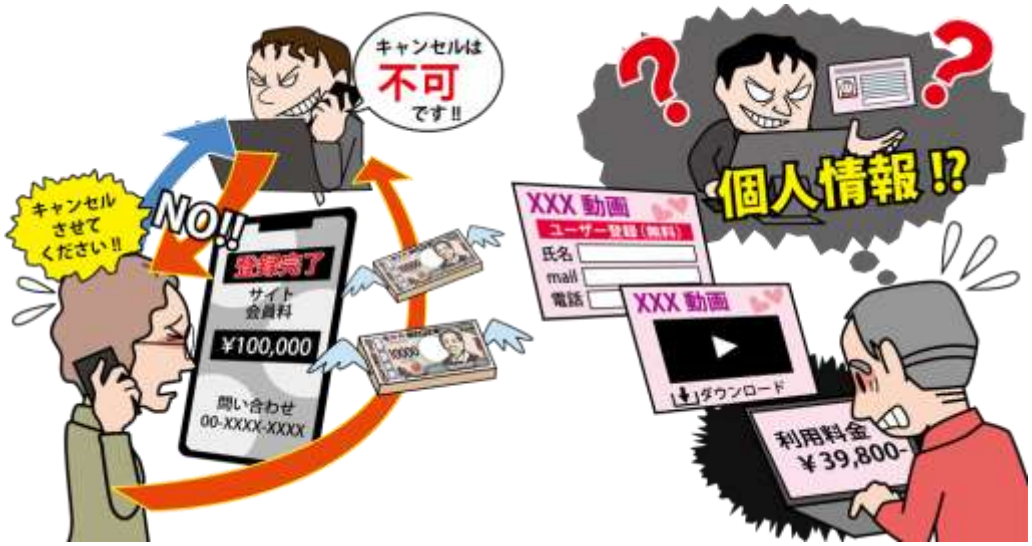
＜対策と対応＞

個人（インターネット利用者）

- 被害の予防
  - ・本書の表 1.2「情報セキュリティ対策の基本」を実施する
  - ・受信した脅迫、詐欺メール・SNS は無視する
    受信した文面に、自分が実際に使用しているパスワードが記載されていても、PC がハッキングされているとは限らないが、悪用されるおそれがあるため、パスワードは速やかに変更する。
  - ・利用しているサービスのワンタイムパスワードサービス、指紋や顔認証等、多要素認証を利用する
  - ・メールに記載されている番号に絶対に電話をしない
    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する場合は、そのメールに記載された連絡先ではなく、別途自身で調べ、正規の電話番号やメールアドレスに連絡する。
- 被害に遭った場合の対応
  - ・クレジットカード、SNS の利用を停止する
  - ・適切な報告/連絡/相談を行う ※
  - ・認証情報を適切に運用する ※

※対策の詳細は後述の「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



Web サイトの閲覧中に、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てしまう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状況である。

＜脅威と影響＞

PC やスマートフォンの利用者がそうとは知らずに悪意あるアダルトサイトや芸能情報サイト等へアクセスすることや、メールや SNS に記載されたリンクをクリックすることで、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の名目で金銭の請求画面が表示される。これをワンクリック請求と呼ぶ。

記載された問い合わせ窓口に電話すると、早急に支払わなければ訴訟になる等と脅される手口も確認されており、不安を煽られるため焦って料金を支払ってしまうおそれがある。また、金銭を支払った後も、繰り返し支払いを要求される場合もある。

＜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させた年齢確認ボタンや動画再生ボタンをクリックさせることや、画面を自動転送することで、会員登録完了の請求画面を表示する。そして、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。

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）の手口もある。これには確認画面を数回クリックさせることで、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。

◆メールに記載したリンクをクリックさせ請求画面を表示

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請求画面を表示

無料で動画をダウンロードできる等と偽り、不正なソフトウェアやアプリをインストールさせる。その後、請求画面を表示させ、画面が閉じられても数分おきに請求画面を表示させる。さらに、PC やスマートフォンを再起動しても再び請求画面を表示させることもある。

◆電話による脅迫や情報窃取

脅迫者は請求画面に問い合わせ先の電話番号を掲載し、閲覧者にその番号に電話させようとする。もしくは、Web サイト上で閲覧者に電話番号を登録させて、その人に電話をかける。そして、電話で連絡が取れると、「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、個人情報を聞きだそうとする場合もある。個人情報を教えてしまった場合、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もある。

＜事例または傾向＞

◆不当請求をされて警察に相談したケース

2024 年 2 月、東京都の青少年がスマートフォンでゲーム関連サイトを見ていた時に広告をタップしてしまい、アダルトサイトが開かれた。18 歳以上かの質問に「はい」を選ぶと、「登録ありがとうございます」という画面が出てお金を請求された。青少年はワンクリック請求のことは知っていたため画面を閉じた。サイト側にはメールも電話もしていないが、個人情報が漏れていないか心配になったため都民安全総合対策本部に相談していた。

警察は、「年齢の質問に答えただけでは有料契約に同意をしたとは言えず、契約は成立していないと考えられる。一方的に請求されているのであればワンクリック請求の手口であり、請求に応じる必要はない。電話をかければ電話番号が伝わり、メールを送信すればメールアドレスが知られてしまう可能性があるが、サイトにアクセスしただけでは個人情報などは知られていないと考えて、このままきっぱりと無視をすることが適切な対応である。」と回答している[48]。

◆依然として続く不当請求の相談

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 2024 年 1 月～5 月に 663 件（2023 年同期 786 件）寄せられた。相談内容は、「スマートフォンのアダルトサイトの年齢確認画面で『18 歳以上』をタップしたところ、登録完了と表示された。登録解除ボタンがあったのでタップしたところ、メールが送信され、『登録解除は電話しないとできない』と返信があったが、請求には応じたくない。」、「アダルトサイトの動画再生ボタンを押すと突然有料登録になった。電話で解約料金を電子マネーで次々請求され、一部支払ったが残額を支払わなければならないか。」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[49]。

また、IPA の安心相談窓口に寄せられた「ワンクリック請求」関する相談件数の推移を見ると、2023 年が 109 件、2024 年が 78 件とこちらも減少傾向にあるものの、依然としてワンクリック請求による被害が続いている[50]。

＜対策と対応＞

個人（インターネット利用者）

● 被害の予防

・本書の表 1.2「情報セキュリティ対策の基本」を実施する

・情報リテラシー、情報モラルを向上させる ※

意思確認画面で安易に「はい」をクリックしない。

・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人に相談する。

・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脅迫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[51]

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[52]に相談する。

・メールの添付ファイルの開封、メールや SMS の URL リンクのクリックを安易にしない ※

・怪しいソフトウェアをダウンロードしない

何らかのファイルダウンロードを促された場合は、すぐにはダウンロードせず、十分注意を払う。

・危険な Web サイトのアクセスをブロックする

セキュリティソフトを導入し、アクセスブロック機能を活用する。

● 被害を受けた際の対応

・適切な報告/連絡/相談を行う ※

・端末を初期化する

※対策の詳細は後述の「共通対策」を参照

2.共通対策

表 2.1 は、10 大脅威にランクインしているほとんどの脅威に有効な対策の一覧である。日常的にこれら対策を意識し、実践することで、インターネットやスマートフォン利用におけるリスクは一定程度、低減される。

本項では表 2.1 の 7 つの「複数の脅威に有効な対策」を、注意事項、検討事項等も含めて具体的に解説する。

読者には本項を自身のセキュリティ対策を進める上での参考としてほしい。なお、共通対策を実施すれば対策は万全ということではない。そのため、各脅威の解説も併せて参照し、対策を実施することが重要である。

表 2.1 複数の脅威に有効な対策

対策	対象	
	個人	組織
認証情報を適切に運用する	○	○
情報リテラシー、情報モラルを向上させる	○	○
メールの添付ファイルの開封、メールや SMS の URL リンク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 PC、ネットワーク機器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	○	○

認証情報を適切に運用する

オンラインショッピングや SNS の利用等、様々な場面でパスワードの設定が必要になってきている。推測可能なパスワードの設定やパスワードの使い回し等の不適切な管理をすると、不正ログインの被害に遭う可能性が高くなる。それを避けるために、適切な設定や運用が記載された本項を読み、適切な対策を実施することでリスク低減を図ってほしい。また、最近ではパスワード認証以外の認証方式の利用も推奨されてきているので、それらについても紹介する。

● 適切な設定をする[53]

・初期設定のままにしない

ネットワークカメラ等のインターネットに接続可能な機器には、製造時に共通パスワードが初期設定されている製品もあり、製品マニュアルにそれが記載されていることがある。共通パスワードのまま使用すると、不正アクセスされるおそれがあるため、必ず変更する。

・推測されにくいパスワードを設定する[54]

推測されにくいパスワードの設定は、文字数を多く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[55]」でも、「最近では、桁数をできるだけ長くする方が安全である」としている。パスワード作成には特に以下を意識する必要がある。

① ID とパスワードを同じ文字列にしない
② 数字、英大文字小文字等、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 規則的な配列にしない
⑤ 単純な単語一語だけにしない

表 2.2　悪いパスワードの例

パスワード	悪い点
12345678	規則的な配列 単一な文字種
Password p@ssw0rd	単純な単語や その類似系
taro1202	生年月日や名前
1qaz2wsx Qwerty	規則的な配列 （キーボードの配列）

・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るべきである。複数のサービスで同じパスワードを利用すると、いずれかのサービスでパスワードの漏えいが起きた時に、全てのサービスが不正ログインされるおそれがある。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ことを推奨する[56]。

● 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等、オフラインの媒体への記録、OS やブラウザのパスワード管理機能の利用、パスワードマネージャ(パスワード管理ソフト)の利用を推奨する。

・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、本人以外の人が本人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。

・メールでのログイン通知の設定をする

・信頼できるチェックサイト[57]で自身のパスワードが漏えいしていないかを確認する

- 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、早急に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。

・「適切な報告／連絡／相談を行う」に書かれた連絡先に連絡をする

- パスワード認証以外の認証方式の併用

・多要素認証を利用する

多要素認証とは、認証の 3 要素である「知識情報」、「所持情報」、「生体情報」のうち、2 つ以上を組み合わせて認証することを指す。「知識情報」であるパスワードだけではなく、「生体情報」等も加えた多要素認証や知識情報を用いないパスワードレス認証を利用することを推奨する。多要素認証の具体例としては、まず Web サイトでパスワード認証を行う。すると、所持しているスマートフォンに SMS でワンタイムパスワードが通知される。これを Web サイトで入力してログインする。これは「知識情報」と「所持情報」を用いた多要素認証である。

・パスキー[58]を利用する

パスワードを利用しない認証方式であるパスキーが提供されていれば利用することを推奨する。

情報リテラシー、情報モラルを向上させる

SNS に流れてきた衝撃的な瞬間をとらえた動画や非常識に感じられる投稿を衝動的に共有すると、自分が非難の的になってしまうかもしれない。 共有した動画が本当に実在のものなのか、ある意図をもって捏造、創作されたものなのか、個人で判断することは難しい。また、常識・非常識の判断は一概には難しく、誹謗中傷や自身への攻撃につながる可能性もある。そしてネットに一度投稿された情報を完全に削除することは難しく、衝動的なふるまいは、一呼吸おいて慎むことを考えたい。

● PC やスマートフォンの利用者を教育する

情報リテラシー・情報モラル[59]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。これから PC やスマートフォンを使う未成年者、使い慣れていない保護者、組織の従業員に対し教育を行う[60]。以下に教育する際のポイントを示す。

① SNS の利用

・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、誤った情報が掲載されてい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

情報を安易に拡散すると名誉毀損で訴えられ、逮捕されることや損害賠償を請求されることがある。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もある。情報を拡散する場合は一次情報を探し、発信者や発信内容のファクトチェック等もした上で拡散する必要がある[61]。

・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から発信する。

② インターネットの利用

・本物を騙った偽の Web サイトがある

・偽の警告を出した上で偽のサポート(サポート詐欺)に誘導する 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。

③ 生成 AI の利用

・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、誤った情報が掲載されているおそれもあるため、情報を鵜呑みにしない。

メールの添付ファイルの開封、メールや SMS の URL リンク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ることや、SMS でお知らせが届けられることがある。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場合、そこをきっかけに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。また、ランサム攻撃や標的型攻撃等の大企業等を狙った組織的な一連の攻撃の一部として実行され、手口が高度化しているため、真偽の見極めが困難になっている。

● 被害に遭うタイミング

悪意があるメール・SMS を受信して、内容を閲覧しただけでは情報を盗まれたり、PC やスマートフォンがマルウェアに感染したりする可能性は低い。そのメール・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ることや、添付ファイルを開くことでマルウェアに感染してしまうことがある。

PC やスマートフォンは、マルウェアに感染すると正常に動作しなくなったり、保存しているデータを攻撃者に送られてしまったりする。

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・SMS、SNS に関する注意事項

・安易に URL リンクにアクセスしたり、QR コードを読み取ったりしない

メールの添付ファイル開封や、メール・SMS のリンク、SNS のチャットの URL を安易にクリックしない。また、QR コードを読み取った後に、安易に個人情報やクレジットカード情報を入力しないようにする。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・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。

・リンクをクリックしてしまった等の場合は、表 2.3 の「報告／連絡／相談する相手」に行う。

● メール固有の注意事項

・メールや SMS に記載されたショッピングサイトやサービス等を利用しているかを確認する

・HTML 形式ではなくテキスト形式で表示する設定にする

・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 Web サイトへのリンクになっており、クリックやタップをすると偽の Web サイトにアクセスする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、マルウェアに感染するおそれがある。Microsoft Word や Excel を開いた際に「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マクロ（プログラム）が起動する。さらに、Word や Excel を指定のフォルダにコピーするように指示するものもある。指定されたフォルダでファイルを開くと、上記のボタンは表示されずにマクロを実行してしまう問題もある[62]。そのため、業務でマクロ機能を使用しない場合は、マクロを無効化するべきである。他にも、「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が、開いたファイルに懸念があれば、ボタンをクリックやタップ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・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」

このような表現だと、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り、確認した方が良いのではと感じてしまうことがある。
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ことを推奨する。

① よく利用している Web サイトは事前にブックマーク（お気に入り）に登録しておき、ブックマークからアクセスする
② よく利用するサービスは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 メールの送信元の情報や電話番号を Web 検索して悪評が立っていないか確認する
④ あまり利用しないサービスは、対象の Web サイトを検索して開いて確認する
　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。このとき検索サイトの上部にある広告は偽のサイトである可能性があるので、それらをクリックしないように注意する。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することや、注文履歴を確認することや、問い合わせることで確認する。

IPA の Web ページでは攻撃手口を紹介しているので、これを確認し、不審なメール・SMS に備えることを推奨する[63]。

適切な報告／連絡／相談を行う

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 人で対応するとさらなる被害につながることもある。

まずは落ち着く、そして、**IT に詳しい知人に相談**した上で、以下の相談先に連絡することが望ましい。

表 2.3【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・SMS を受信した 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	①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 ②サービス提供会社 ※不審なメール・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 ③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） ④フィッシング対策（警察庁） https://www.npa.go.jp/bureau/cyber/countermeasures/phishing.html ⑤フィッシング対策協議会 https://www.antiphishing.jp/registration.html https://www.antiphishing.jp/contact_faq.html
メール・SMS で脅迫された、金銭の要求をされた	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使われた 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
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使用しているセキュリティソフトのベンダ ②IPA（情報セキュリティ安心相談窓口） https://www.ipa.go.jp/security/anshin/about.html
自身のアカウントにログインされた	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（情報セキュリティ安心相談窓口） 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/

サーバーや PC、ネットワーク機器に適切なセキュリティ対策を行う

個人でサーバーを利用している人は少ないことを考えると、まずは PC やスマートフォン、Wi-Fi ルーターなど身近な機器を考えるとよい。また、スマートテレビや Blu-ray レコーダーなどのスマート家電もある。スマートホームであれば HEMS（Home Energy Management System）[64]等も対象となる。PC やスマートフォンには重要な情報が含まれ、Wi-Fi ルーターはこれら機器への出入口となるため、これら機器へのセキュリティ対策が重要である[65]。

- 脆弱性対策を適切に行う

  ・サポート切れのソフトウェアやハードウェアを使用しない

  PC やスマートフォンの OS やインストールされているソフトウェア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後継のソフトウェアに移行する。

  ・迅速に更新プログラムや更新ファームウェアを適用する

- 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。マルウェアの検出・駆除、迷惑メールのフィルタリング、不審な Web サイトへのアクセスをブロック等、様々な機能を搭載している。

  セキュリティソフトのインストール後は、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、スキャン結果を確認することが必要である。

- スマートフォンのアプリは公式マーケットからインストールする

  スマートフォン内のデータを不正に外部送信するような不正アプリは、公式マーケット以外のサーバーから配信されることが多い。スマートフォンのアプリは基本的に公式マーケットからインストールする。また、提供元が不明なソフトウェアはインストールしない。

適切なバックアップ運用を行う

データ破損の原因は PC やスマートフォンの故障、ランサムウェアへの感染だけではなく、操作ミスによる消去や誤った更新など多岐に渡る。失ったデータの復旧は困難であるが、バックアップを取得しておくことで、被害を軽減できる。

- バックアップを取得する
  - ・バックアップする対象を選定する
    全てのデータのバックアップを取得するとデータ量が膨大になるので、バックアップするデータ量に注意して対象を選定する。
  - ・バックアップは PC やスマートフォンとは別の媒体やクラウドストレージに取得する

- バックアップを保管する
  - ・保管場所を検討する
    普段使用するPC やスマートフォンとは別の端末、外付けハードディスク、SD カード、クラウド上のストレージ等にデータを保存する。
    ランサムウェア対策として、データを使用しないときは、データを保存した媒体を PC やスマートフォンとは接続せずに保管する。

- 適切にバックアップできているか確認する
  - ・バックアップしたデータ（写真データや文書ファイル等）が表示できることを確認する

【情報セキュリティ 10 大脅威 2025】

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

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

「インターネット上のサービスからの個人情報の窃取」

3 住宅オーナー様等向けの会員制サイトにサイバー攻撃を受けたことによるお客様情報等の外部漏えいについて（積水ハウス）
https://www.sekisuihouse.co.jp/company/topics/library/2024/20240524_1/20240524_1.pdf
積水ハウスが29万人超の個人情報漏洩、過去のページでセキュリティー設定に不備（日経クロステック）
https://xtech.nikkei.com/atcl/nxt/news/24/00849/

4 全国漁業協同組合連合会 通販サイト「JFおさかなマルシェ ギョギョいち」への不正アクセスによる個人情報漏えいの恐れに関する調査結果のご報告（全国漁業協同組合連合会）
https://www.zengyoren.or.jp/news/press_20240819/
弊会通販サイト「JFおさかなマルシェ ギョギョいち」本店閉店のお知らせ（全国漁業協同組合連合会）
https://www.zengyoren.or.jp/news/press_20241004/

5 当社が運営する「転職支援サイト」への不正アクセスに関するお知らせとお詫び（株式会社ワークポート）
https://www.workport.co.jp/corporate/news/detail/896.html

6 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」

7 日産のカーシェア「e-シェアモビ」 不正ログインで車両不正利用 最大約 7 万件の個人情報閲覧された可能性（ITMedia）
https://www.itmedia.co.jp/news/articles/2409/03/news125.html

8 本学M365アカウントへの第三者による不正アクセス及びフィッシングメール送信について（明治薬科大学）
https://www.my-pharm.ac.jp/files/pv/158/PDF1/2024.06.04本学M365%20アカウントへの第三者による不正アクセス及びフィッシングメール送信について.pdf

9 LINE企業アカウント688件で乗っ取り 不正にログイン（日本経済新聞）
https://www.nikkei.com/article/DGXZQOUC26B8E0W4A820C2000000/

10 LINE公式アカウントにおけるアカウント乗っ取りに関するお知らせとお願い（LINEヤフー株式会社）
https://www.lycbiz.com/jp/news/line-official-account/20240826/

11 インターネット取引サービスへの不正アクセス・不正取引による被害が急増しています（金融庁）
https://www.fsa.go.jp/ordinary/chuui/chuui_phishing.html

12 今般のインターネット取引サービスにおけるフィッシング詐欺等による証券口座への不正アクセス等による対応について（日本証券業協会）
https://www.jsda.or.jp/about/hatten/inv_alerts/alearts04/higai/higai10_20250502.pdf

「クレジットカード情報の不正利用」

13 ウェブスキミング（Wikipedia）
https://ja.wikipedia.org/wiki/%E3%82%A6%E3%82%A7%E3%83%96%E3%82%B9%E3%82%AD%E3%83%9F%E3%83%B3%E3%82%B0

14 弊社が運営する「アンテノール オンラインショップ」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
（株式会社エーデルワイス）
https://www.edelweiss.co.jp/news/16138/
弊社が運営する「ヴィタメール オンラインショップ」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
（株式会社エーデルワイス）
https://www.edelweiss.co.jp/news/16140/

15 【重要】弊社が運営する「タリーズ オンラインストア」への不正アクセスによる個人情報漏洩の恐れに関するお詫びと調査結果のご報告
（タリーズコーヒージャパン株式会社）
https://www.tullys.co.jp/information/2024/10/post-14.html
【重要】「タリーズ オンラインストア」不正アクセスによるシステム侵害発生のお詫びとお知らせ（タリーズコーヒージャパン株式会社）
https://www.tullys.co.jp/information/2024/05/post-13.html

16 クレジットカード不正利用被害の発生状況（一般社団法人日本クレジット協会）
https://www.j-credit.or.jp/information/statistics/download/toukei_03_g.pdf

17 クレジットカード・セキュリティガイドライン【6.0 版】（クレジット取引セキュリティ対策協議会）
https://www.j-credit.or.jp/security/pdf/Creditcardsecurityguidelines_6.0_published.pdf

「スマホ決済の不正利用」

18 第 10 回　タッチ決済（1）－タッチ決済のしくみ－（独立行政法人国民生活センター）
https://www.kokusen.go.jp/wko/pdf/wko-202303_07.pdf
第 11 回　タッチ決済（2）－タッチ決済に関する注意事項－（独立行政法人国民生活センター）
https://www.kokusen.go.jp/wko/pdf/wko-202304_06.pdf

19 なぜ？クレジットカード"停止したのに"不正利用が止まらない…毎日１万円ずつ被害に「意味分からない」利用者に募る不安　スマホタッチ決済悪用か（MBS）
https://www.mbs.jp/news/feature/hunman/article/2024/07/101374.shtml
カード停止後も不正利用相次ぐ　スマホのタッチ決済悪用か（NHK）
https://www3.nhk.or.jp/news/html/20240915/k10014582481000.html

20 引き続き返金詐欺に注意！「〇〇ペイで返金します」と言われたら詐欺を疑って！（独立行政法人国民生活センター）
https://www.kokusen.go.jp/news/data/n-20240731_2.html

「偽警告によるインターネット詐欺」

21 【手口検証動画】偽のセキュリティ警告（IPA）
https://www.youtube.com/watch?v=SP00wbawM1k

22 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

23 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

24 笛吹市商工会におけるサポート詐欺被害事案について（笛吹市商工会）
https://r.goope.jp/fuefukishokokai/info/5634762
「サポート詐欺」で1000万円の被害 - ネット銀を遠隔操作（Security NEXT）
https://www.security-next.com/156231
サポート詐欺による不正アクセスに関する調査報告と再発防止策について（笛吹市商工会）
https://r.goope.jp/fuefukishokokai/info/5684735

25 パソコンの画面全体に偽のメッセージが表示され操作不能になる手口が増加中（IPA）
https://www.ipa.go.jp/security/anshin/attention/2024/mgdayori20240917.html
正規ツールを悪用しPCを操作不能にさせるサポート詐欺の新手口を解説（トレンドマイクロ株式会社）
https://www.trendmicro.com/ja_jp/research/24/j/support-fraud-new-technique.html

26 情報セキュリティ安心相談窓口の相談状況［2024年第4四半期（10月～12月）］（IPA）
https://www.ipa.go.jp/security/anshin/reports/2024q4outline.html

27 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¥

28 パソコンに偽のウイルス感染警告を表示させるサポート詐欺に注意（IPA）
https://www.ipa.go.jp/security/anshin/attention/2024/mgdayori20241119.html

29 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

30 情報セキュリティ安心相談窓口（IPA）
https://www.ipa.go.jp/security/anshin/index.html

31 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」

32 フワちゃんが芸能活動休止…やす子さんへの不適切投稿で「一つの区切りとして、しばらくの間」（読売新聞）
https://www.yomiuri.co.jp/culture/tv/20240811-OYT1T50088/
フワちゃん「やす子へ公開暴言」が示す根深い問題　単なる誤爆では済まず、イメージに甚大な影響か（東洋経済オンライン）
https://toyokeizai.net/articles/-/794645

33 献体前でピース写真、ブログ公開の美容外科医に「免許剥奪」求める声、SNSで大反発…厚労省の見解は（弁護士ドットコム）
https://www.bengo4.com/c_18/n_18269/
献体解剖倫理指針について（篤志解剖全国連合会、日本篤志献体協会、日本解剖学会）
https://www.anatomy.or.jp/file/pdf/guideline/ethics_202503.pdf

34 総務省、Google・LINE ヤフーら 5 社を「大規模プラットフォーム事業者」に指定、誹謗中傷などの迅速な対応求める
https://internet.watch.impress.co.jp/docs/news/2011282.html

35 インターネット上の違法・有害情報に対する対応（情報流通プラットフォーム対処法）（総務省）
https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/ihoyugai.html

「フィッシングによる個人情報等の詐取」

[36] 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

[37] フィッシング詐欺メールの報告件数 去年170万件余 過去最多に（NHK）
https://www3.nhk.or.jp/news/html/20250203/k10014710551000.html

[38] 国税庁をかたるフィッシング（2024/05/22)（フィッシング対策協議会）
https://www.antiphishing.jp/news/alert/nta_20240522.html
e-Taxを装った不審なメール等にご注意ください（国税庁）
https://www.e-tax.nta.go.jp/topics/2024/topics_hushinmail.htm

[39] 農業協同組合（JAバンク）をかたるフィッシング（2024/09/02)（フィッシング対策協議会）
https://www.antiphishing.jp/news/alert/jabank_20240902.html
フィッシング詐欺にご注意ください（JAバンク）
https://www.jabank.org/attention/phishing/
全国労働金庫協会（ろうきん）をかたるフィッシング（2024/08/26)（フィッシング対策協議会）
https://www.antiphishing.jp/news/alert/rokin_20240826.html
ろうきん（労働金庫・全国労働金庫協会）を騙った不審メール・偽サイトにご注意ください（2024年8月22日）（ろうきん）
https://all.rokin.or.jp/important/2024/08/2024822.html

[40] QR コードから誘導するフィッシング（2024/08/28)（フィッシング対策協議会）
https://www.antiphishing.jp/news/alert/qr_20240828.html

[41] 利用者向けフィッシング詐欺対策ガイドライン（フィッシング対策協議会）
https://www.antiphishing.jp/report/guideline/consumer_guideline2025.html

「不正アプリによるスマートフォン利用者への被害」

[42] 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

[43] あなたのスマートフォンが犯罪のインフラに（日本サイバー犯罪対策センター）
https://www.jc3.or.jp/threats/examples/article-592.html

[44] 【注意喚起】年金事務所を騙り、マイナポータルの偽サイト・偽アプリへの誘導される事案について（デジタル庁）
https://www.digital.go.jp/news/b32e5c16-8272-4cc3-9171-b4c583325feb
【マイナポータルの偽アプリを確認！】IPA（情報セキュリティ安心相談窓口）（X（旧Twitter））
https://x.com/IPA_anshin/status/1772552023877021762
【マイナポータルの偽アプリを確認！】IPA情報セキュリティ安心相談窓口（Facebook）
https://www.facebook.com/ipa.anshin/posts/pfbid02Tc9FVeCsrBdKYg1RG7hsRiDJ73LxCvrmSEu7QNGRmpm43eq3EEv3BBXMnLHxpwfvl

[45] SNS型投資・ロマンス詐欺の被害が急増（広島県警察）
https://www.pref.hiroshima.lg.jp/site/police3/toushisagi-tyuuikannki.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」

[46] 令和6年における特殊詐欺及びSNS型投資・ロマンス詐欺の認知・検挙状況等について（暫定値版）（警察庁）
https://www.npa.go.jp/bureau/criminal/souni/tokusyusagi/hurikomesagi_toukei2024.pdf

[47] SNS 型ロマンス詐欺か　石川小松 60 代男性　約 2 億 2400 万円の被害（NHK）
https://www3.nhk.or.jp/news/html/20241025/k10014619421000.html

「ワンクリック請求等の不当請求による金銭被害」

[48] 相談事例「架空請求」| こどものネット・スマホのトラブル相談！こたエール（都民安全総合対策本部）
https://www.tokyohelpdesk.metro.tokyo.lg.jp/consult/jirei/kakuu.html

[49] アダルト情報サイト（各種相談の件数や傾向）（独立行政法人国民生活センター）
https://www.kokusen.go.jp/soudan_topics/data/adultsite.html

[50] 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
情報セキュリティ安心相談窓口の相談状況［2024 年第 4 四半期（10 月～12 月）］（IPA）
https://www.ipa.go.jp/security/anshin/reports/2024q4outline.html

[51] 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

[52] 情報セキュリティ安心相談窓口（IPA）
https://www.ipa.go.jp/security/anshin/index.html

「認証情報を適切に運用する」

53 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

54 チョコっとプラスパスワード（IPA）
https://www.ipa.go.jp/security/chocotto/index.html

55 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

56 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

57 Have I Been Pwned? （HaveIBeenPwned.com）
https://haveibeenpwned.com/

58 情報セキュリティ10大脅威 2024「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！」（IPA）
https://www.ipa.go.jp/security/10threats/nq6ept000000g22h-att/kaisetsu_2024.pdf

「情報リテラシー、情報モラルを向上させる」

59 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

60 情報セキュリティ関連サイト（IPA）
https://www.ipa.go.jp/security/guide/keihatsu.html

61 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

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

62 Emotet（エモテット）攻撃の手口（IPA）
https://www.ipa.go.jp/security/emotet/attack.html

63 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

「利用している PC、ネットワークにつながる機器に適切なセキュリティ対策を行う」

64 HEMS とは
https://www.jema-net.or.jp/energy/hems.html

65 国民のためのサイバーセキュリティサイト（一般利用者向けの対策）（総務省）
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/security/end_user/general/

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)	植草 祐則	(株)NTT データ先端技術
小林 大介	あいおいニッセイ同和損害保険(株)	佐藤 功視	(株)NTT データ先端技術
宮﨑 清隆	ICMS(株)	藤原 稔也	(株)NTT データ先端技術
中嶋 美貴	アクセンチュア(株)	井上 茂	NTT ビジネスソリューションズ(株)
大泉 久	AKKODiS コンサルティング(株)	前田 典彦	(株)FFRI セキュリティ
石井 彰	旭化成(株)	中西 克彦	(株)FFRI セキュリティ
高橋 広	旭有機材(株)	橋田 幸浩	MS&AD インシュアランスグループホールディングス(株)
早崎 敏寛	(株)アシュアード	青山 昇司	MS&AD インターリスク総研(株)
鈴木 康弘	(株)アシュアード	辻本 竜一	MS&AD インターリスク総研(株)
真藤 直観	(株)アシュアード	梶浦 勉	MS&AD インターリスク総研(株)
中山 貴禎	(株)アズジェント	福地 有紀	MS&AD システムズ(株)
岡田 良太郎	(株)アスタリスク・リサーチ	西城 秀行	MS&AD システムズ(株)
石田 淳一	(株)アールジェイ	和田 泰宜	エムオーテックス(株)
徳丸 浩	EG セキュアソリューションズ(株)	頭島 龍正	エムオーテックス(株)
岡田 琢央	Infoblox(株)	廣田 優樹	エムオーテックス(株)
一條 敦	VMware(株)	池田 耕作	(株)オージス総研
山根 康裕	(株)エーピーコミュニケーションズ	姫野 猛	(株)オージス総研
小澤 志織	(株)エーピーコミュニケーションズ	猪俣 敦夫	大阪大学
田中 潤子	(株)エーピーコミュニケーションズ	山本 裕介	キャディ(株)
斎藤 泰輔	au フィナンシャルホールディングス(株)	岡村 耕二	九州大学
溝口 英利	(株)AIT	小松 香織	京セラ(株)
野口 敏宏	SMBC コンシューマーファイナンス(株)	赤﨑 洋一	京セラ(株)
佐藤 直之	SCSK セキュリティ(株)	小関 直樹	京セラ(株)
鈴木 寛明	SCSK セキュリティ(株)	小松 佳昭	京セラコミュニケーションシステム(株)
辻 伸弘	SB テクノロジー(株)	刀川 郁也	京セラコミュニケーションシステム(株)
大島 悠司	NRI セキュアテクノロジーズ(株)	西山 健太	京セラコミュニケーションシステム(株)
大塚 淳平	NRI セキュアテクノロジーズ(株)	大脇 旭洋	キンドリルジャパン(株)
奥村哲平	NRI セキュアテクノロジーズ(株)	小林 義孝	キンドリルジャパン(株)
笠井 靖記	NEC ネクサソリューションズ(株)	小西 健博	キンドリルジャパン(株)
川内 裕文	(株)エヌ・ティ・ティ エムイー	宮内 雄太	(一社)金融 ISAC
高橋 昌士	(株)エヌ・ティ・ティ エムイー	古澤 一憲	グーグル・クラウド・ジャパン(同)
斯波 彰	NTT コミュニケーションズ(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(Grafsec)
神田 敦	NTT コミュニケーションズ(株)	鈴木 貴志	グローバルセキュリティエキスパート(株)
坪井 祐一	NTT コミュニケーションズ(株)	三輪 晋平	グローバルセキュリティエキスパート(株)
松橋 亜希子	NTT 社会情報研究所	加藤 連	グローバルセキュリティエキスパート(株)
杉野 明宏	NTT 社会情報研究所	小熊 慶一郎	KBIZ /ISC2
川口 雄己	NTT 社会情報研究所	平良 元輝	KDDI デジタルセキュリティ(株)
北河 拓士	NTT セキュリティ・ジャパン(株)	遠藤 誠	(株)ケイテック
杉山 毅	NTT セキュリティ・ジャパン(株)	保村 啓太	KPMG コンサルティング(株)
大久保 佐太郎	(株)NTT データ	坂 明	(公財)公共政策調査会
星野 亮	(株)NTT データ	北田 高之	(株)神戸デジタル・ラボ
大石 眞央	(株)NTT データグループ	松田 康司	(株)神戸デジタル・ラボ
大嶋 真一	(株)NTT データグループ	前園 博文	コベルコシステム(株)
馮 菲	(株)NTT データグループ	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)

氏名	所属	氏名	所属
松本 純	サイボウズ(株)	花田 隆仁	東京海上日動火災保険(株)
宮内 伸崇	(株)サイント	石山 圭佑	東京海上日動システムズ(株)
大澤 陽子	(株)佐賀IDC	猪狩 大祐	東京海上日動システムズ(株)
熊坂 駿吾	GMO サイバーセキュリティ by イエラエ(株)	石川 朝久	東京海上ホールディングス(株)
飯山 志保	(株)JR東日本情報システム	嶋谷 巧	東京海上ホールディングス(株)
佐藤 勤子	(株)JR東日本情報システム	富山 寛之	東京海上ホールディングス(株)
萩谷 文	(株)JR東日本情報システム	佐々木 良一	東京電機大学
椎野 紘平	(株)JTB	小島 健司	(株)東芝
佐久間 義明	(株)JTB	原田 博久	(株)Doctor Web Pacific
齋藤 美香	(一社)JPCERT コーディネーションセンター	山室 太平	Trellix
藤堂 伸勝	(一社)JPCERT コーディネーションセンター	岡本 勝之	トレンドマイクロ(株)
唐沢 勇輔	Japan Digital Design(株)	林 憲明	トレンドマイクロ(株)
加藤 雅彦	順天堂大学	須川 賢洋	新潟大学
大久保 隆夫	情報セキュリティ大学院大学	堀江 昌宏	ニッセイ・ウェルス生命保険(株)
伊東 寛	(国研)情報通信研究機構(NICT)	柳 優	日本アイ・ビー・エム(株)
山田 宜史	(株)スクエアエニックス	髙﨑 庸一	(一社)日本サイバーセキュリティ人材キャリア支援協会
竹林 和賢	スターネット(株)	名和 利男	日本サイバーディフェンス(株)
山本 幸稔	スターネット(株)	又江原 恭彦	(一社)日本シーサート協議会
正木 義和	スワットブレインズ(株)	松本 多恵	(一社)日本シーサート協議会
東 恵寿	NPO セカンドワーク協会	青木 聡	日本電気(株)
金城 夏樹	(株)セキュアイノベーション	谷川 哲司	日本電気(株)
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
鉢嶺 光	(株)セキュアイノベーション	宮本 久仁男	(一社)日本ハッカー協会
服部 祐一	(株)セキュアサイクル	仲上 竜太	ニューリジェンセキュリティ(株)
長谷川 陽介	(株)セキュアスカイテクノロジー	藤本 博史	ニューリジェンセキュリティ(株)
阿部 実洋	(株)セキュアベース	小島 博行	(国研)農業・食品産業技術総合研究機構(農研機構)
上村 理	ゼットスケーラー(株)	橋本 賢一郎	Nozomi Networks, Inc.
澤永 敏郎	ソースネクスト(株)	櫻井 理沙	(株)ノートンライフロック
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	中野 透	(株)ノートンライフロック
小島 陽平	ダイキン工業(株)	生田 玲	(株)ノートンライフロック
岩脇 正浩	ダイキン工業(株)	小林 克巳	(株)野村総合研究所
楢原 盛史	タニウム(同)	山崎 英人	パーソルキャリア(株)
永野 英世	(一社)地域セキュリティ協議会	伊藤 秀明	パーソルクロステクノロジー(株)
鈴木 一弘	地方公共団体情報システム機構	南 和哉	パナソニック(株)
德丸 力蔵	中外製薬(株)	勝見 松則	パナソニックコネクト(株)
三木 基司	TIS(株)	高橋 洋一	パナソニックコネクト(株)
田中 卓朗	TIS(株)	常川 直樹	パナソニックコネクト(株)
遠藤 宗	DXC テクノロジー・ジャパン(株)		情報経営イノベーション専門職大学
浅西 修	DXC テクノロジー・ジャパン(株)	楢崎 晃太	パロアルトネットワークス(株)
福田 かおり	DNV ビジネス・アシュアランス・ジャパン(株)	安岡 祥吾	パロアルトネットワークス(株)
松本 隆	(株)ディー・エヌ・エー	大泰司 章	(同)PPAP総研
大山 水帆	(一社)デジタル広域推進機構	司東 秀浩	東日本電信電話(株)
吉村 修	デロイト トーマツ サイバー(同)	齊藤 純一郎	東日本電信電話(株)
羽場 満	デロイト トーマツ サイバー(同)	平本 陽介	東日本電信電話(株)
駒澤 悠二	(株)電算	折田 彰	(株)日立システムズ
近藤 修一	(株)電算	関谷 信吾	(株)日立システムズ
河合 翔平	東京海上日動あんしん生命保険(株)	寺田 真敏	(株)日立製作所

氏名	所属	氏名	所属
沼田 亜希子	(株)日立製作所	六宮 智悟	(株)リクルート
田中 秀和	(株)日立ソリューションズ	上原 哲太郎	立命館大学
古賀 洋一郎	ビッグローブ(株)	有森 貞和	(株)両備システムズ
山口 裕也	(株)ファイブドライブ	鈴木 堅太	(株)両備システムズ
田中 昌弘	富士通(株)	矢儀 真也	(株)両備システムズ
濱田 達也	富士通(株)	内山 巧	
原 和宏	富士通(株)	今 佑輔	
菅原 尚志	フューチャー(株)	清水 秀一郎	
海老原 俊一	(株)Bridge	piyokango	
柳川 俊一	(株)Bridge		
吉井 史和	(株)Bridge		
鴫原 祐輔	(株)Blue Planet-works		
荒井 大輔	PayPay(株)		
小野 洲平	PayPay(株)		
川口 元輝	PayPay(株)		
倉田 尚希	(株)ベリサーブ		
樅山 清	(株)ベリサーブ		
太田 良典	弁護士ドットコム(株)		
結城 亮史	(株)BOX Japan		
垣内 由梨香	マイクロソフトコーポレーション		
高倉 万記子	万記子コミュニケーションズ(同)		
中西 基裕	(株)マクニカ		
政本 憲蔵	(株)マクニカ		
瀬治山 豊	(株)マクニカ		
中村 直樹	三井住友海上火災保険(株)		
阿部 巧	(株)三井住友銀行		
武笠 雄介	(株)三井住友銀行		
関原 優	三井物産セキュアディレクション(株)		
東内 裕二	三井物産セキュアディレクション(株)		
篠原 巧	(株)三菱総合研究所		
平田 真由美	みゅーらぼ		
石井 崇喜	(株)ユービーセキュア		
勝田 嵐士	(株)ユービーセキュア		
西大條 春仁	(株)ユービーセキュア		
江面 祥行	(株)ユビテック		
島田 理枝	(株)ユビテック		
吉岡 克成	横浜国立大学		
佐久間 矩仁	横浜市役所		
牧野 尚彦	横浜市役所		
三国 貴正	(株)YONA		
橘 喜胤	楽天カード(株)		
福本 佳成	楽天グループ(株)		
原子 拓	楽天グループ(株)		
鳥越 真理子	楽天ペイメント(株)		
伊藤 彰嗣	楽天モバイル(株)		
山崎 圭吾	(株)ラック		
若居 和直	(株)ラック		

著作・制作　独立行政法人情報処理推進機構（IPA）

編集責任　土屋 正

イラスト製作　株式会社 創樹

執筆協力者　10 大脅威選考会

10 大脅威執筆者　白石 歩　井上 佳春　土屋 正
篠塚 耕一　吉本 賢樹　横山 美晴
山下 恵一　大久保 直人

IPA 執筆協力者　高柳 大輔　中野 美夏　沖田 孝裕
加賀谷 伸一郎　中島 尚樹　小山 明美

情報セキュリティ10大脅威 2025 個人編

2025 年 6 月 18 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/