情報セキュリティ

10 大脅威 2022

― 個人編 ―

※本書では、10 大脅威 2022 個人の脅威を解説しています。
組織の脅威に関する解説は 2022 年 3 月上旬に公開予定です。

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

2022 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 2022」
https://www.ipa.go.jp/security/vuln/10threats2022.html

目次

はじめに

本書「情報セキュリティ 10 大脅威 2022」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、2021 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 2022

個人の 10 大脅威では昨年に引き続き順位の変動はあるが同じ 10 個の脅威がランクインした。また、1 位となった「フィッシングによる個人情報等の窃取」は、「10 大脅威 2019」以降続いていた 2 位からランクアップし、初めて 1 位となった。

一方、組織の 10 大脅威では、7 位に初めて「修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）」がランクインした。ゼロデイ攻撃は事前の対策ができないため、組織としては攻撃検知後の対応方針を決め、関係者に徹底しておくことが重要である。

本書では、2021 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 2022

情報セキュリティ 10 大脅威 2022

■「情報セキュリティ 10 大脅威 2022」

2021 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 2022」では、「個人」と「組織」向け脅威として、それぞれ表 1.1 の通り順位付けした。

表 1.1 情報セキュリティ 10 大脅威 2022 「個人」および「組織」向けの脅威の順位

「個人」向け脅威	順位	「組織」向け脅威
フィッシングによる個人情報等の詐取	1	ランサムウェアによる被害
ネット上の誹謗・中傷・デマ	2	標的型攻撃による機密情報の窃取
メールや SMS 等を使った 脅迫・詐欺の手口による金銭要求	3	サプライチェーンの弱点を悪用した攻撃
クレジットカード情報の不正利用	4	テレワーク等の ニューノーマルな働き方を狙った攻撃
スマホ決済の不正利用	5	内部不正による情報漏えい
偽警告によるインターネット詐欺	6	脆弱性対策情報の公開に伴う悪用増加
不正アプリによる スマートフォン利用者への被害	7	修正プログラムの公開前を狙う攻撃 （ゼロデイ攻撃）
インターネット上のサービスからの 個人情報の窃取	8	ビジネスメール詐欺による金銭被害
インターネットバンキングの不正利用	9	予期せぬ IT 基盤の障害に伴う業務停止
インターネット上のサービスへの 不正ログイン	10	不注意による情報漏えい等の被害

本章で共通的に使われる用語について**表 1.2** に定義を記載する。

表 1.2 情報セキュリティ 10 大脅威 2022 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
組織的犯行グループ	金銭を目的とした攻撃（犯罪）者集団
諜報員、産業スパイ	機密情報窃取を目的とした攻撃（犯罪）集団 国家組織の支援を受けた攻撃（犯罪）集団
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。

■「情報セキュリティ 10 大脅威 2022」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 2022」は、「10 大脅威選考会」の投票結果に基づき順位付けして「個人」「組織」それぞれ 10 個の脅威を選定している。投票結果により決定した順位ではあるが、上位の脅威だけ、または上位の脅威から優先して対策を行えばよいということではない。

例えば、個人の立場では、フィーチャーフォン（ガラケー）を利用している方であれば、スマートフォン利用者を狙った脅威である「スマホ決済の不正利用」（本書、個人 5 位）や「不正アプリによるスマートフォン利用者への被害」（本書、個人 7 位）への対策の必要性は低くなる。

また、組織の立場では、オンラインショッピング等で個人情報を取り扱う組織であれば、その情報を狙った脅威である「インターネット上のサービスへの不正ログイン」（本書、組織ランク外、昨年の組織 8 位）を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 2022」で新しくランクインした脅威もあるが、それに伴いランク外となった脅威もある。しかし、ランク外になったとしてもその脅威が無くなったわけではない。かつてランクインしていた、「ワンクリック請求等の不当請求」、「ウェブサイトの改ざん」や「サービス妨害攻撃によるサービスの停止」等は、依然として攻撃が行われている状況である。

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。

尚、ランク外となった脅威の詳細や対策方法等については、過去の「情報セキュリティ 10 大脅威」を参考にしてほしい。

③ 「情報セキュリティ対策の基本」が重要

世の中には「情報セキュリティ 10 大脅威」へランクインした脅威以外にも多数の脅威が存在する。とは言え、これらが利用する「攻撃の糸口」は似通っており、脆弱性を突く、ウイルスを使う、ソーシャルエンジニアリングを使う等の古くから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」の1章で解説しているが、表 1.3 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 1.3 情報セキュリティ対策の基本

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

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 1.4 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。

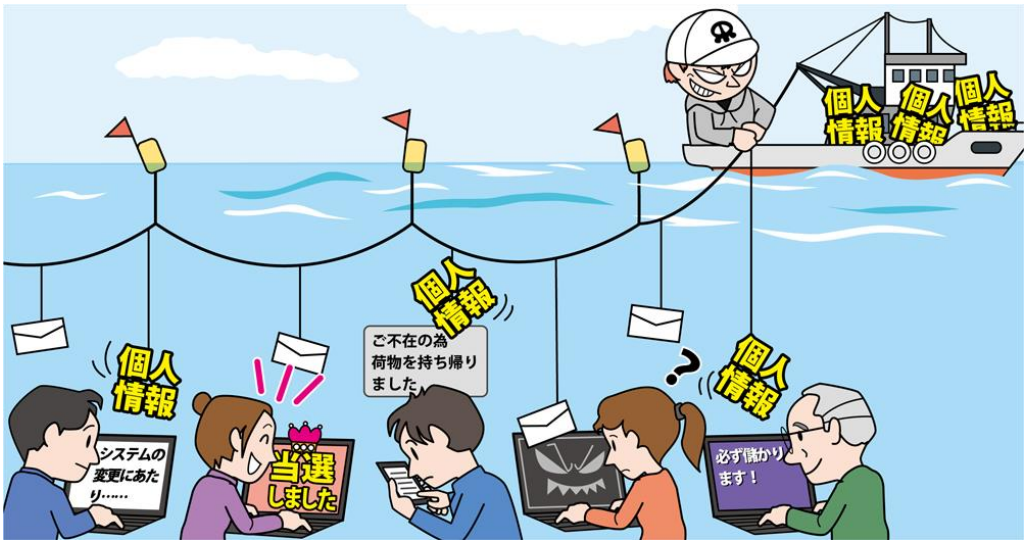
表 1.4 情報セキュリティ対策の基本+ α

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

1. 情報セキュリティ 10 大脅威（個人）

1位 フィッシングによる個人情報等の詐取

～宅配の不在通知を装うフィッシング詐欺に要注意！！～



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（ショートメッセージサービス）を送信し、正規のウェブサイトを模倣したフィッシングサイト（偽のウェブサイト）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手口である。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＞

有名企業を騙ったメールや SMS を送り付け、本文に記載したフィッシングサイトの URL にアクセスさせる。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、個人情報を入力してしまうと、攻撃者に情報を詐取され、詐取された情報は悪用され、最終的に金銭的な被害が発生する。

近年では、メールや SMS 以外に SNS（ソーシャル・ネットワーキング・サービス）を悪用したフィッシング詐欺が発生している。

＜攻撃手口＞

◆ フィッシングサイトへ誘導するメール等を不特定多数に送信

攻撃者が、有名企業のウェブサイトを模倣したフィッシングサイトを作成する。攻撃者は、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有名企業と信じさせる内容のメッセージを SMS、メールや SNS で不特定多数に送信する。それに騙された被害者はフィッシングサイトに誘導され、個人情報やクレジットカード番号等の重要な情報を入力してしまい、情報を詐取される。テキスト表記上の（見た目の）URL と実際のジャンプ先 URL が異なるものもある。

別の手口では、宅配便業者の不在通知を装った 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）ケースがある。誘導された被害者は、個人情報を入力してしまうと、その情報を攻撃者に詐取される。

◆ 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く、虚偽の不正な広告を表示する。不正な広告のリンクにアクセスすると、フィッシングサイトへ誘導され、個人情報の入力を促される。

【詐取した情報の悪用例】

- 詐取した個人情報を違法取引のウェブサイトで販売し、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＞

◆ 「水道局」を騙った不審メール

2021 年 12 月、「水道局」を騙った不審メールが確認されているとして、東京都水道局が注意喚起を行った。メールにはフィッシングサイトへ誘導することを目的として「水道料金を支払わなければ断水する」、「リンクをクリックしてお支払いください」といった内容が記載されており、メール内のリンクをクリックすると東京都水道局のサイトを模倣した別サイトに移動する。移動先のサイトでは、フィッシング詐欺やウイルス感染のおそれがあるとしている。[1]

◆ 佐川急便を装った迷惑メールにご注意

2021 年 8 月、佐川急便は自社を装った迷惑メールや SMS が急増しているとして、HP で注意喚起を行った。メールに記載されている URL にアクセスする、または添付ファイルを開くとウイルスに感染するおそれがある。なお、佐川急便では荷物の集配について SMS による案内は行っていない。[2]

◆ フィッシング報告件数は依然として増加傾向

2021 年は 2020 年の報告件数を大幅に上回り、Amazon、三井住友カードを騙るフィッシングが継続して報告されている。[3,4] また、スミッシングについては、宅配業者の不在通知を装った SMS を悪用する事例が依然として確認されている。最近では、Amazon、au、ドコモを騙るものも確認されている。[4]

＜対策/対応＞[5]

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 1.3「情報セキュリティ対策の基本」を実施
  - ・SMS やメールで受信した URL や、SNS の投稿内の URL を安易にクリックしない
    自身の資産や重要情報を扱うウェブサイトは、ウェブブラウザのブックマーク（お気に入り）にあらかじめ登録した URL やサービス運営者が配布している公式アプリを利用してアクセスする。
  - ・多要素認証の設定を有効にする
    詐取後の不正ログインを防ぐ。
  - ・迷惑メールフィルターを利用
  - ・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確認する。
- 被害の早期検知
  - ・利用するウェブサイトのログイン履歴の確認
    自身のものではないログイン履歴、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
  - ・パスワードを変更する（他のサービスで同じパスワードを使っていた場合は同様に対応）
  - ・利用しているサービスへの利用停止を連絡
  - ・信頼できる機関に相談
    警察、国民生活センター、地域の消費生活センターに相談する。

参考資料

1. 料金請求に関する不審メールについて（東京都水道局）
https://www.waterworks.metro.tokyo.lg.jp/press/r03/press211201-01.html
2. 佐川急便を装った迷惑メールにご注意ください（佐川急便株式会社）
https://www2.sagawa-exp.co.jp/whatsnew/detail/721/
3. 2020/12 フィッシング報告状況（フィッシング対策協議会）
https://www.antiphishing.jp/report/monthly/202012.html
4. 2021/12 フィッシング報告状況（フィッシング対策協議会）
https://www.antiphishing.jp/report/monthly/202112.html
5. フィッシング対策ガイドライン（2021年度版）（フィッシング対策協議会）
https://www.antiphishing.jp/report/antiphishing_guideline_2021.pdf

2位 ネット上の誹謗・中傷・デマ

～一つの発言が人生を脅かす可能性も～

SNS（ソーシャル・ネットワーキング・サービス）等の匿名で利用できるサービスで特定の個人あるいは企業への誹謗・中傷の行為が行われることが問題となっている。この行為により被害者は精神的苦痛を受ける、風評被害を受けて信頼や信用を損なうことや、経済的な損失を被ることもある。2021 年に開催された東京 2020 オリンピック・パラリンピックの出場選手をターゲットとした事例もあった。

＜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 のサービスの普及に伴い、匿名での広範囲な情報発信が容易に行えるようになっている。一方、そのサービスを利用し、意図的に他人への誹謗・中傷や、脅迫・犯罪予告・デマを書き込む事件が確認されている。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。一方、誹謗・中傷やデマの発信は犯罪になりうる事ことや、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場合がある。

＜要因＞

◆　匿名性を利用した影響ある情報発信

特定の個人、企業に対する意見や感情を発言する際に、その内容についての影響を考慮せずに発信してしまう。オープンなサービスの場合、一つの発言が内容によっては大きな規模の影響をもたらすことがある。匿名での発信であることでその内容が過激になりやすい環境であることも要因の一つである。なお、匿名であっても警察が調査すれば身元を特定できる場合が多い。

◆　第三者による情報の拡散・改変

SNS 等のサービスで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、悪意の有り無し関係なく真偽を確認せずに拡散する。そして、伝言ゲームのように別の第三者がさらに拡散することで、誹謗中傷やデマが広範囲に周知されてしまう。

また、受け取った内容をさらにまた別の第三者の真偽不明な情報と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場合もある。

＜事例または傾向＞

◆ **オリンピック選手に向けての誹謗・中傷**

2021 年 7 月、オリンピックに出場した選手が自身の SNS に対して誹謗・中傷のメッセージが大量に送られてきていることを告白した。選手は、送られてきた悪質なメッセージについては、スクリーンショットで記録を残し、関係各所へ連絡、然るべき措置を取ると意思を示した。[1]

◆ **デマ画像によるデマの拡散**

2021 年 11 月、SNS 上に、通天閣のネオン表示が新型コロナウイルスのワクチン接種を批判する旨の内容に編集されたデマ画像が出回った。投稿はネット上で拡散され、通天閣の運営会社には事実確認や苦情の連絡が約 30 件寄せられる事態になった。同社は再度デマ画像が拡散された場合、法的措置を検討するとしている。[2]

＜対策/対応＞

個人（発信者）

- 情報モラルや情報リテラシーの向上、法令遵守の意識の向上
  - ・誹謗、中傷や公序良俗に反する投稿をしない
  - ・投稿前に内容を確認する

    SNS やブログ等のソーシャルメディアに投稿する内容は不特定多数の人に見られることを想定し、投稿して問題ない内容かどうかを投稿前にしっかりと確認する。
  - ・匿名性がある場合でも発言には責任を持つ

    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）

- 情報モラル、情報リテラシーの教育
  - ・子供たちへの教育の実施

    自宅や学校で子供たちに情報モラルや情報リテラシーの教育を行う。さらに、トラブルの事例を伝え、悪質な行為は犯罪になりうることを理解させる。[3]

個人（閲覧者）

- 情報モラルや情報リテラシーの向上、法令遵守の意識の向上
  - ・情報の信頼性の確認

    インターネット上に流通している情報が必ずしも正しいとは限らないことを認識し、その情報を安易に拡散せず、一次情報やその他複数の情報元を確認し、信頼できる情報かどうかを総合的に判断する。[4] また、デマの拡散は、犯罪になりうることを理解する。

個人（被害者）

- 被害を受けた後の適切な対応
  - ・冷静な対応と支援者への相談

    一人で抱え込まず、信頼できる周囲の人や公的相談機関へ相談する。[5] 脅迫や名誉毀損に該当する誹謗・中傷等、犯罪と思われる投稿は警察へ被害届を提出し、必要に応じて弁護士にも相談する。
  - ・管理者やプロバイダーへ削除依頼

    問題ある書き込みを削除したいときは本人または関係者がウェブサイトの管理者やプロバイダーに削除を要請する。なお、削除により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。

参考資料

1. 水谷隼「しかるべき措置をとる」 実際の誹謗中傷DMを公開（grape）
https://grapee.jp/991168
2. 通天閣に「射っちゃダメ」 デマ画像拡散に怒り（ITmediaビジネスONLiNE）
https://www.itmedia.co.jp/business/articles/2111/07/news020.html
3. インターネットトラブル事例集 （2021年版）（総務省総合通信基盤局）
https://www.soumu.go.jp/main_content/000707803.pdf
4. 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
5. #NoHeartNoSNS（ハートがなけりゃSNSじゃない！）（総務省sss総合通信基盤局）
https://www.soumu.go.jp/main_sosiki/joho_tsusin/kyouiku_joho-ka/no-heart-no-sns.html

3位 メールや SMS 等を使った脅迫・詐欺の手口による金銭要求

～公的機関を装ったメール等に注意～

個人の秘密を家族や知人にばらすと脅迫したり、身に覚えのない有料サイトの未納料金を請求したりするメールや SMS（ショートメッセージサービス）、LINE 等を使った詐欺による金銭被害が発生している。公的機関を装った偽の相談窓口に誘導するといった手口もある。

＜攻撃者＞

- 組織的犯行グループ

＜被害者＞

- 個人（インターネット利用者）

＜脅威と影響＞

「アダルトサイトを閲覧している姿を撮影した」等の脅迫メールや有料サイトの未納金があるといった架空請求のメールを送信し、金銭を詐取しようとする攻撃が行われている。また、メールや SMS、LINE 等を使った同様の手口も確認されている。

脅迫・詐欺のメールの内容は虚偽のものであるが、その内容を信じてしまい不安に思ったメール受信者が金銭を支払ってしまう。そして、一度でも攻撃が成功してしまうと、その脅迫は効果が期待できると攻撃者に認識され、同様の手口で多数の宛先へメール送信を行い、さらに被害が拡大するおそれがある。

＜攻撃手口＞

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、LINE 等を不特定多数に送り、金銭を詐取しようとする。指定される支払方法には暗号資産（仮想通貨）や電子マネーが多く見られる。また、騙す手口として以下が使われる。

◆ セクストーション（性的脅迫）

「アダルトサイトを閲覧している姿を撮影した」等、周囲に相談しにくい性的な内容で脅す。

◆ ハッキングしたように見せかける

被害者のパスワードや住所等の個人情報をメールに記載し、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る。記載している情報はハッキングによるものではなく、外部のサービスから何らかの原因で漏えいした情報を使用している。

◆ 公的機関を装う

公的機関等信頼できる組織の発信を装うことでメール等の信憑性、緊急性を高め、騙そうとする。

◆ メールや電話を併用して信憑性を高める

脅迫・詐欺目的のメールに、偽の問合せ窓口の電話番号を記載して送信し、この電話番号宛に被害者から電話を掛けさせる。電話を掛けてきた被害者に対して、攻撃者は更に脅迫を行ったり、電話口で公的機関を装った偽の相談窓口を紹介し、そ

の窓口に電話を掛けさせて信頼させた上で金銭を支払わせたりする。また、攻撃者から被害者に対して金銭を要求する電話をかけ、その後に弁護士を装った攻撃者から和解を求める旨のメールを送信し、信憑性を高めて騙そうする手口もある。

＜事例または傾向＞

◆ **公的機関を騙り、金銭を要求**

2021 年 10 月、消費者庁は、「消費者庁」、「国民生活センター」等を騙り、架空の「和解金」の交付を持ち掛け、「書類作成費用」等の名目で金銭を支払わせるメールや SMS が確認されたとして注意喚起を行った。支払いは、電子マネーを購入して支払うように誘導し、購入した電子マネーの ID を連絡させることで電子マネーを詐取する。また、受信者がメールを無視すると「罰則を科せられる」等、脅かすようなメッセージが送信される。[1]

◆ **警察の LINE アカウントを装い連絡、架空請求の可能性**

2021 年 9 月、広島県警は、同県警サイバー犯罪対策課を装う LINE アカウントが確認されているとして注意喚起を行った。「あなたの LINE アカウントが通報された」、「自宅または連絡可能な所在地へ郵送にて通達文を送付する」等、不安を煽り、連絡を取るよう求めてくる。同県警は架空請求やフィッシング詐欺の可能性があるとしている。[2]

◆ **暗号資産で金銭を要求するメールの相談件数が昨年より増加**

IPA 情報セキュリティ安心相談窓口によると、暗号資産で金銭を要求する迷惑メールの相談件数が、2020 年の 244 件に対して 2021 年は 513 件となり、大幅に増加している。[3,4] また、2021 年 3 月には、受信者が性的な映像を見ていることを知ったとして、知人にばらされたくなかったらビットコインで送金しろと恐喝するメール（セクストーション）が引き続き確認されている。メール文面の日本語は不自然で、英文を翻訳サイト等の機械翻訳にかけたものと考えられるが、年々、違和感が少なくなってきている。[5]

＜対策/対応＞

個人（インターネット利用者）

- 被害の予防（被害に備えた対策含む）
  - ・表 1.3「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、被害者のパスワードが記載されていても、実際にハッキングされていることはほぼない。メールで要求された支払いには応じない。
  - ・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。
  - ・メールで要求された支払いには応じない
  - ・多要素認証の設定を有効にする
- 被害を受けた後の対応
  - ・パスワードを変更する（他のサービスで同じパスワードを使っていた場合は同様に対応）
    脅迫・詐欺メールに記載されたパスワードが自身の実際のパスワードと一致しているのであれば、そのパスワードを利用しているサイトからパスワードが漏えいした可能性があるので、早急にパスワードを変更する。また、パスワードは使いまわさない。
  - ・警察に相談する

参考資料

1. 消費者庁などの公的機関の名称をかたり、架空の「和解金」などの交付を持ち掛けて金銭を支払わせる事業者に関する注意喚起（消費者庁）
https://www.caa.go.jp/notice/entry/026250/
2. 「あなたのアカウントが通報された」 - 偽警察のLINEアカウントに注意（Security NEXT）
https://www.security-next.com/129668
3. 情報セキュリティ安心相談窓口の相談状況［2020年第4四半期（10月～12月）］（IPA）
https://www.ipa.go.jp/security/txt/2020/q4outline.html
4. 情報セキュリティ安心相談窓口の相談状況［2021年第4四半期（10月～12月）］（IPA）
https://www.ipa.go.jp/security/txt/2021/q4outline.html
5. 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/mgdayori20181010.html

4位 クレジットカード情報の不正利用

～不審な利用記録がないか今一度確認を～

キャッシュレス決済やオンラインショッピングの普及に伴い、クレジットカードを利用する機会が増えている。一方、所有者を狙ったフィッシング詐欺やクレジットカード情報が登録されている各種サービスサイトを狙った不正アクセスによる情報漏えいにより、クレジットカード情報が窃取され、攻撃者にクレジットカードを不正利用される被害が継続して発生している。

＜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＞

オンラインショッピングの一般化に加え、近年のキャッシュレス決済の普及に伴い、クレジットカードを活用する機会が増えている。そのクレジットカード情報が攻撃者に狙われている。攻撃者は、フィッシング詐欺により詐取したり、クレジットカードで決済を行っている端末にウイルスを感染させることにより窃取したりする。また、オンラインで提供されている各種サービスへ不正アクセスし、そこに保存されているクレジットカード情報を窃取する。

クレジットカード情報が攻撃者に窃取されると、正規の利用者の知らない間に不正利用され金銭的な被害を受けたり、クレジットカード情報を公開されたり、販売されたりするおそれがある。

＜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。

◆ フィッシング詐欺

メール等を使い、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 1 位「フィッシングによる個人情報等の詐取」を参照。

◆ 正規の決済画面を改ざんし入力情報を詐取

ショッピングサイトの脆弱性を悪用し、正規ウェブサイトの決済画面を改ざんする。その後、改ざんした決済画面に被害者を誘導し、クレジットカード情報を入力させることで、クレジットカード情報を詐取する。

◆ 不正アクセス

脆弱性を悪用し、サービス提供者の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。

◆ **ウイルス感染**

ウイルスをメールに添付して開かせたり、悪意あるウェブ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たり、利用者の端末内の情報が窃取されたりする。

◆ **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、一般的な検索エンジンでは検出されない闇サイト（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＞

◆ **「ブルークレール Web サイト」でクレジットカード情報流出**

2021 年 5 月、ブルークレールは、運営する「ブルークレール Web サイト」が不正アクセスを受け、1,863 件のクレジットカード情報が流出したことを公表した。流出した当該情報の一部は不正利用されたおそれがあった。原因は、システムの一部の脆弱性を悪用した不正アクセスにより、ペイメントアプリケーションの改ざんが行われたためとしている。[1]

◆ **「コスモスオンラインストア」でクレジットカード情報流出**

2021 年 7 月、コスモス薬品は、EC ウェブサイトとして運営している「コスモスオンラインストア」が不正アクセスを受け、2 万 5,484 件のクレジットカード情報が流出したことを公表した。流出した情報の一部は不正利用されたおそれがあることを確認している。[2]

◆ **被害額は増加、約 9 割は番号盗用被害**

日本クレジット協会が公開した「クレジットカード不正利用被害の集計結果」によれば、2021 年 1～9 月における不正利用被害額は約 236 億 9,000 万円となった。前年同期間の被害額は約 180 億 2,000 万円であり、被害額が大幅に増加している。なお、被害額全体に占める番号盗用被害額の割合は年々増加しており、2021 年においては 94.5%を占めている。[3]

＜対策/対応＞

個人（利用者）

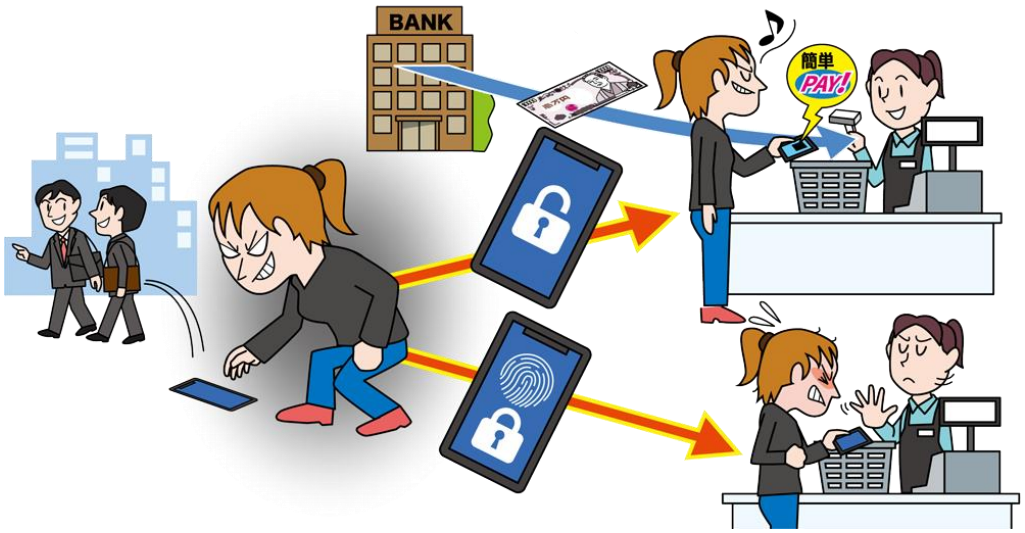
- 被害の予防
  - ・表 1.3「情報セキュリティ対策の基本」を実施
  - ・クレジットカード会社が提供している本人認証サービス（3D セキュア等）の利用
  - ・添付ファイルや URL を安易に開かない
  - ・普段は表示されないような画面やポップアップが表示された場合、情報を入力しない
  - ・プリペイドカードの利用を検討
    不正利用被害額となる利用可能金額の範囲を限定する
- 被害の早期検知
  - ・クレジットカードの利用明細の確認
  - ・サービス利用状況の通知機能の利用
- 被害を受けた後の対応
  - ・該当サービスのコールセンターへの連絡
    クレジットカード会社によっては、全額または一部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）
  - ・クレジットカードの再発行
  - ・パスワードを変更する（他のサービスで同じパスワードを使っていた場合は同様に対応）
  - ・ウイルス感染した端末の初期化
  - ・警察への被害届の提出

参考資料

1. 化粧品通販サイトに不正アクセス - クレカ情報流出の可能性（Security NEXT）
https://www.security-next.com/126477
2. 弊社が運営する「コスモスオンラインストア」への不正アクセスによるお客様情報流出に関するお詫びとお知らせ（株式会社コスモス薬品）
https://www.cosmospc.co.jp/notice/upload/ed661581b067c469eb29047679fa8a86e6446fe7.pdf
3. クレジットカード不正利用被害の集計結果について（（一社）日本クレジット協会）
https://www.j-credit.or.jp/download/news20211228a1.pdf

5位 スマホ決済の不正利用

～今や「スマートフォン」＝「個人情報、財産」の時代！日頃からリスク管理の徹底を～



近年の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、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。一方、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＞

- 組織的犯行グループ
- 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＞

スマホ決済では、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）方法や、決済用アプリで生成した QR コードやバーコードを店舗のバーコードリーダーに読み込ませる方法、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がある。残高をチャージするためには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そこからチャージできる。これらの情報は決済サービス毎に専用のシステムやアプリで管理されているが、決済サービスや仕組みに不備がある場合、攻撃者に不正利用される。

例えば、決済サービスに不正にログインされると、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

被害者が複数のサービスで同一のパスワードを使いまわしている場合がある。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、それをもとにログインを試みる（パスワードリスト攻撃）。不正ログインに成功すれば、なりすまして不正利用する。また、スマホ決済サービスより提供される多要素認証等のセキュリティ強化機能を利用していない場合、漏えいしたパスワードのみで不正ログインできるため、攻撃者に悪用されやすい。

◆　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を開発する際に、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を

十分に考慮していないと、スマホ決済サービスを不正利用できる脆弱性を作り込むおそれがある。

＜事例または傾向＞

◆ **拾ったスマートフォンで PayPay 不正チャージ**

2021 年 10 月、拾ったスマートフォンでスマホ決済サービス「PayPay」に不正チャージした男が「電子計算機使用詐欺」容疑で逮捕された。被害者は携帯電話会社に連絡し、通話や通信機能は使用不能にしていたが、PayPay には届け出ておらず、約 18 万円の不正チャージが行われた。[1]

◆ **PayPay の決済音鳴らし決済完了に見せかけ**

2021 年 8 月、ディスカウントストアでの会計時にスマホ決済サービス「PayPay」の決済音を鳴らすことで会計をしたと見せかけ、食料品等を騙し取った疑い。売り上げと PayPay から店への支払い額が合わないケースが複数回あり、発覚した。[2]

◆ **スマホ決済で身に覚えのない不正な支払い**

神奈川県川崎市の経済労働局産業政策部消費者行政センターによると、2021 年 12 月にスマホ決済サービスにおいて、身に覚えのない支払いが行われているとの相談があり、利用限度額いっぱいの 25 万円が使用されていることがわかった。履歴から 15 分間で 10 件の購入を確認されており、事業者に調査依頼をしている。[3]

＜対策/対応＞

個人（スマホ決済サービスの利用者）

- 被害の予防
  - ・表 1.3「情報セキュリティ対策の基本」を実施
  - ・多要素認証の設定を有効にする
  - ・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。[4]
  - ・パスワードは長く、複雑にする [4,5]
  - ・パスワードの使いまわしをしない

    例えばパスワードの基となるコアパスワードを作成し、その前後にサービス毎に異なる識別子を付加することで他と重複しないパスワードを作成することができる。[5]
  - ・パスワード管理ソフトの利用
  - ・フィッシングに注意

    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。
  - ・不要なサービスのアカウント削除
  - ・スマートフォンの紛失対策

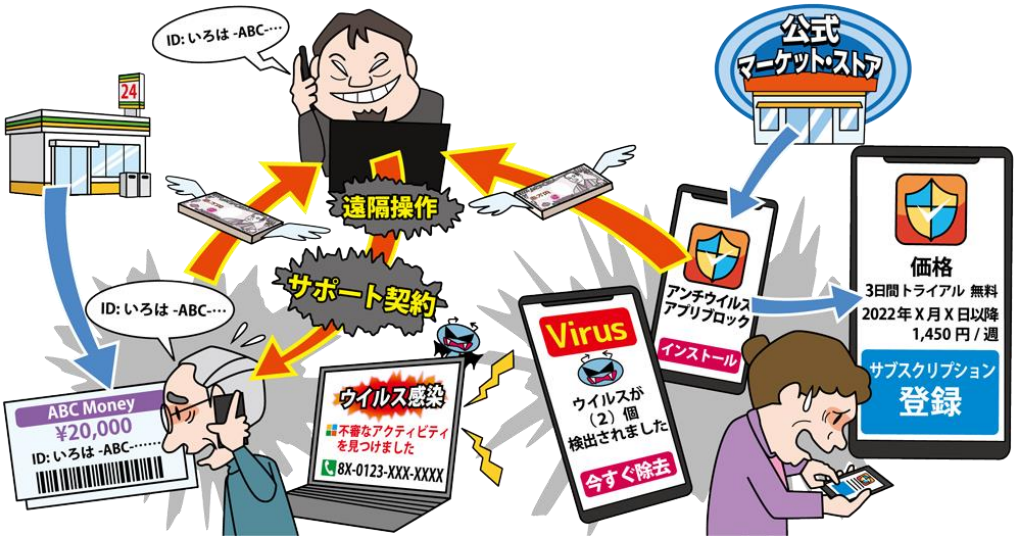
    紛失したスマートフォンを悪用されないために画面ロック等のセキュリティ対策を実施する。
- 被害の早期検知
  - ・スマホ決済サービスの利用状況通知機能の利用および利用履歴の定期的な確認
  - ・連携する銀行口座の出金履歴の確認
- 被害を受けた後の対応
  - ・パスワードを変更する（他のサービスで同じパスワードを使っていた場合は同様に対応）
  - ・スマホ決済サービス運営者への連絡
  - ・連携する金融機関への連絡
  - ・警察への連絡

参考資料

1. スマホ拾った男、「ペイペイ」で電子マネー詐取…ネット上の撮影写真データで発覚（読売新聞オンライン）
https://www.yomiuri.co.jp/national/20211020-OYT1T50001/
2. 「ペイペイ」決済音鳴らし食品だまし取った疑い、男逮捕（朝日新聞DIGITAL）
https://www.asahi.com/articles/ASP7Y2SXWP7WUTNB011.html
3. キャッシュレス決済の不正利用トラブル（神奈川県川崎市　経済労働局産業政策部消費者行政センター）
https://www.city.kawasaki.jp/280/page/0000135952.html
4. 不正ログイン対策特集ページ（IPA）
https://www.ipa.go.jp/security/anshin/account_security.html
5. 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/mgdayori20160803.html

6位 偽警告によるインターネット詐欺

～それは詐欺です。慌てる、焦るは思うツボ！～



PC やスマートフォンからウェブサイトを閲覧中に、突然「ウイルスに感染しています」等、偽のセキュリティ警告画面を表示して、不審なソフトウェアをインストールさせたり、攻撃者が用意したサポート窓口に電話を掛けさせて PC の遠隔操作や有償サポート契約を結ばされたり、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。

＜攻撃者＞

- 組織的犯行グループ

＜被害者＞

- 個人（インターネット利用者等）

＜脅威と影響＞

ウェブサイトを閲覧中に、突然「ウイルスが見つかりました」、「Windows のシステムが破損しています」等の偽の警告画面が表示されることがある。表示された警告画面は、実在する企業からの通知のように偽っており、通知される内容を信用させ指示に従うよう促す。

指示に従ってしまうと不審なソフトウェアのインストールや購入をさせられる。また、偽のサポート窓口に連絡をしてしまい、PC の遠隔操作や有償サポート契約を結ばされたり、修復費用を要求されたりする。スマートフォン利用者であれば、不審なアプリをインストールするように誘導される。さらに、ソフトウェアの購入やサポート契約時に入力した氏名、メールアドレス、クレジットカード情報等の個人情報は別の詐欺に悪用され、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

閲覧者を騙すためにウェブサイト等に表示される偽警告は、警告内容を信じさせるために、実在する企業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。

◆ 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。

◆ サポート詐欺

閲覧者に偽警告の画面に記載されているサポート窓口へ電話をかけさせ、言葉巧みに遠隔操作ツールをインストールさせようとする。その上で、サポート契約や不必要なソフトウェアの購入へ誘導する。サポート契約等の支払い方法はコンビニで

販売されているプリペイド型電子マネーや各種ギフトカードのほか、クレジットカード決済が使われる。

◆　**スマホアプリのインストールへ誘導**

偽警告をスマートフォンの画面に表示し、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。誘導したことに対して広告主からアフィリエイト収益を得たり、サブスクリプション（自動継続課金）による利用者への料金請求で収益を得たりすることが目的と考えられる。[1]

＜事例または傾向＞

◆　**電話をかけさせて偽のサポートへ誘導**

IPA 安心相談窓口には、「ウイルスに感染している」等、偽のセキュリティ警告の相談が多く寄せられている。2021 年は、偽のセキュリティ警告画面に電話番号を表示して、最初から電話をかけさせて偽のサポートへ誘導する手口が広まった。[2]

電話をかけてしまうと、遠隔操作用ソフトウェアをインストールさせられ、虚偽の説明が行われたり、修理費用として電子マネーの購入を求められたりする。遠隔操作では PC の様々な操作を行うことができ、データの閲覧や消去、PC を起動させなくするといった悪質な操作が行われる危険が伴う。

◆　**パソコン PC 修理名目のサポート詐欺事件**

2021 年 11 月、新潟中央警察署はサポート詐欺事案の届出を受理し、特殊詐欺（架空料金請求詐欺）として捜査している。被害者の男性は、自宅で PC を使用していたところ、画面上に「中国にハッキングされている」等のメッセージが表示され、表示されている連絡先に電話したところ、「遠隔操作で PC を修理する。修理費用として電子マネーで支払ってください。」等と言われコンビニエンスストアで電子マネーを購入し、電子マネーの番号を伝え、合計 7 万 5,000 円分騙し取られた。[3]

＜対策/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 1.3「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
  - ・偽警告が表示されても従わない
    偽警告によって指示されるアプリやソフトウェアはインストールしない。また、電話を掛けない、遠隔操作は許可しない、契約には応じない。
  - ・偽警告が表示されたらブラウザを終了する
  - ・ブラウザの通知機能を不用意に許可しない[4]
    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。
  - ・不用意にカレンダーの照会を追加しない[5]
  - ・カレンダー内の不審な予定は削除する
- 被害を受けた後の対応
  - ・端末を初期化する
  - ・虚偽のサポート契約の解消
    近くの消費生活センター[6]に相談する。
  - ・クレジットカード会社へ連絡

参考資料

1. 安心相談窓口だより「スマートフォンで偽のセキュリティ警告からアプリのインストールへ誘導する手口に注意」（IPA）
https://www.ipa.go.jp/security/anshin/mgdayori20190918.html
2. 安心相談窓口だより「偽のセキュリティ警告に表示された番号に電話をかけないで！」（IPA）
https://www.ipa.go.jp/security/anshin/mgdayori20211116.html
3. 新潟中央警察署「パソコン修理名目の特殊詐欺被害が発生！！慌てず落ち着いた行動を」（新潟中央警察署）
https://www.pref.niigata.lg.jp/uploaded/attachment/293015.pdf
4. 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/mgdayori20210309.html
5. 安心相談窓口だより「iPhoneに突然表示される不審なカレンダー通知に注意！」（IPA）
https://www.ipa.go.jp/security/anshin/mgdayori20200330.html
6. 全国の消費生活センター等（（独）国民生活センター）
http://www.kokusen.go.jp/map/index.html

7位 不正アプリによるスマートフォン利用者への被害

～偽装 SMS の URL リンクや不正アプリへの誘導に注意～

スマートフォンの利用者に不正アプリをインストールさせて、スマートフォン内の個人情報を窃取したり、アプリを不正利用して、利用者に不正請求等の損害を与えたりする被害が発生している。昨今は、偽のワクチン接種予約案内や宅配業者になりすました SMS（ショートメッセージサービス）をスマートフォンに送信し、利用者が URL にアクセスすることで不正アプリをインストールさせる他、公式マーケットにウイルスを忍び込ませそのアプリをインストールさせる事例が確認されている。

＜攻撃者＞

- 組織的犯行グループ
- 犯罪者

＜被害者＞

- 個人（スマートフォン利用者）

＜脅威と影響＞

有名な組織を装った SMS がスマートフォンに届き、SMS に記載された URL にアクセスした利用者に対して、不正アプリをインストールするよう誘導してくる。また、公式マーケット上にウイルスを忍ばせた不正アプリを公開し、利用者がそれを知らずにインストールしてしまう場合もある。

不正アプリをスマートフォンにインストールしてしまうと、スマートフォン内に保存されている連絡先や通話記録、位置情報等の情報を窃取される。認証情報を窃取されるとキャリア決済等を不正に使用され、金銭的被害を受けるおそれがある。

また、SMS を送信する踏み台に利用され、意図せず不正な SMS を送信してしまう場合がある。

＜攻撃手口＞

◆ 不正アプリのダウンロードサイトへ誘導する

実在するウェブサイトに似せた不正アプリのダウンロードサイトを用意する。実在の組織やアプリの更新を騙り、SMS や偽警告等からダウンロードサイトに誘導し、直接インストールさせる。

◆ 公式マーケットに不正アプリを紛れ込ませる

不正アプリを正規のアプリと見せかけて公式マーケットに公開する。利用者は正規のアプリだと思い込み、安易にインストールしてしまう。

◆ アプリの更新で不正アプリに変化する

インストール時は悪意ある機能が顕在化していないが、アプリの更新により顕在化し、不正アプリに変化する。

＜不正アプリによるスマートフォンの悪用例＞

- 連絡先等の端末内の重要な情報を窃取
- DDOS 攻撃（ウェブサーバー等に負荷をかける攻撃）や不正な SMS の拡散等の踏み台
- 録画・写真・通話録音機能を不正に利用
- 暗号資産（仮想通貨）のマイニングに利用

＜事例または傾向＞

◆ **通信事業者を騙った SMS から不正アプリのダウンロードサイトに誘導**

日本サイバー犯罪対策センター（JC3）によると、通信事業者になりすました SMS が届き、本文に記載した URL（偽のサイト）にアクセスさせられ、不正アプリをインストールさせられる手口が確認されている。

Android 端末の場合はアクセスした偽のサイトから不正アプリ（*.apk）のインストールへ誘導する手口、iPhone の場合は偽サイトから各種設定を管理する構成プロファイルをダウンロードさせて、不正アプリをインストールさせる手口が確認されている。インストールした不正アプリで認証情報を入力すると、攻撃者にその情報が詐取される。[1]

◆ **偽のワクチン接種予約案内に注意**

2021 年 5 月、トレンドマイクロは、新型コロナウイルスのワクチン接種予約を装う偽の SMS について注意喚起を行った。Android 端末で、SMS に記載された不正な URL にアクセスすると、Chrome のアップデートを装った不正アプリのインストールが促される。インストールしてしまうと、攻撃者が被害者のスマートフォンを介し、不特定多数に対して偽装 SMS を送り付け、不正サイトに誘導する。[2]

◆ **トロイの木馬が仕込まれたゲームアプリからの情報窃取**

セキュリティベンダ Dr.Web によれば Android 端末のゲームアプリ 190 種にトロイの木馬（Cynos プログラムモジュールの亜種）が仕込まれており、930 万以上のスマートフォンにインストールされている可能性が指摘されている。インストールすると携帯電話番号やモバイルネットワークパラメータ等を利用者に無断で収集し、リモートサーバーに送信する。該当するゲームは既にアプリストアから削除されている。[3]

＜対策/対応＞

個人（スマートフォン利用者）

- 被害の予防

・表 1.3「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

スマートフォンの設定によっては公式マーケット以外からもアプリを入手可能だが、極力公式マーケットから入手する。ただし、公式マーケットにも不正アプリが紛れていることがあるため、レビューの評価に加え、アプリ開発者やアプリのバージョンアップ履歴等の情報を確認し、信頼できるアプリかどうかを判断する。

・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確認を行う。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信頼しない。

・不要なアプリをインストールしない

不正アプリに限らず、正規のアプリであっても使い方を誤れば意図せず重要な情報を公開してしまうこともある。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

- 被害を受けた後の対応

・不正アプリのアンインストール

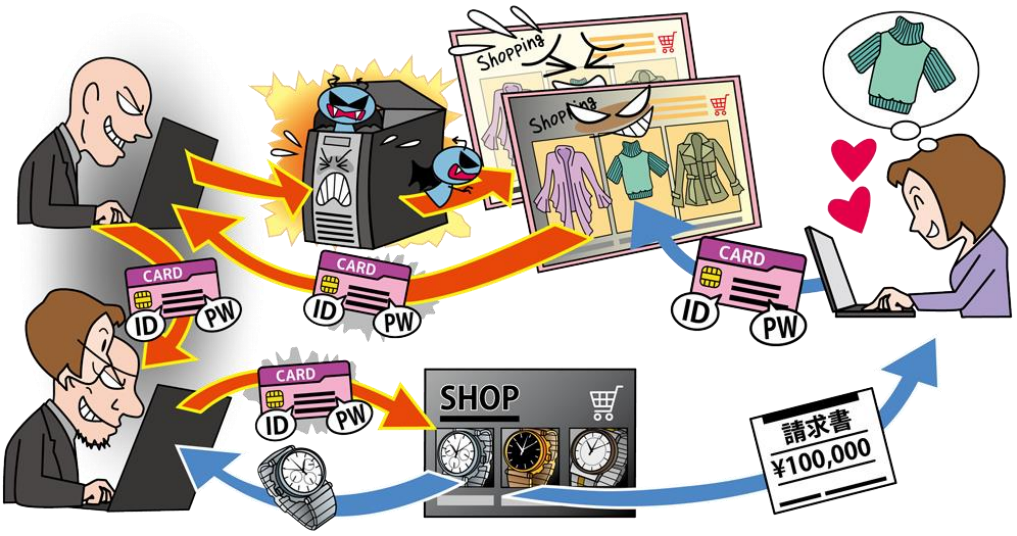
不正アプリをアンインストールする。できない場合は端末を初期化する。

参考資料

1. 通信事業者を装ったフィッシング（（一財）日本サイバー犯罪対策センター）
https://www.jc3.or.jp/threats/examples/article-409.html
2. 【注意喚起】偽のワクチン接種予約案内に注意（トレンドマイクロ株式会社）
https://www.is702.jp/news/3864/
3. トロイの木馬仕込まれたゲームアプリ、Androidユーザー 930万人がダウンロード（株式会社マイナビ）
https://news.mynavi.jp/article/20211125-2198828/

8位 インターネット上のサービスからの個人情報の窃取

～頻発する個人情報の漏えい、利用者もできる限りの対策を～



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な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。

＜攻撃者＞

- 組織的犯行グループ

＜被害者＞

- 個人（サービス利用者）
- 組織（サービス利用者）

＜脅威と影響＞

昨今、多くの企業や組織がインターネット上に様々なサービスを提供している。利用者はそのサービスを利用するために会員登録を行い、個人情報等の重要な情報（氏名、性別、生年月日、メールアドレス、クレジットカード情報等）を登録している。一方、サービスを提供している組織が、サービスを構成しているソフトウェアの脆弱性対策や、適切なセキュリティ対策が不十分なままサービスを提供している場合がある。また、利用者においてもログインに利用する ID、パスワード等の認証情報を複数のサービスで使いまわしている場合がある。攻撃者は、ソフトウェアの脆弱性や他サービスで漏えいした認証情報を悪用して不正アクセスや不正ログインをすることで、サービスに登録されている重要な情報を窃取する。

重要な情報を窃取されると、クレジットカードを不正利用されたり、詐欺メールを送信されたり、窃取された情報を一般的な検索エンジンでは検出されない闇サイト（ダークウェブ）で売買される等、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、ウェブサイト内の個人情報等の重要情報を窃取する。

また、攻撃者はウェブサイトの脆弱性を悪用してウェブサイトを改ざんする場合もある。サービスの利用者が改ざんに気づ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、個人情報等の重要な情報を窃取する。詳細は個人

10 位「インターネット上のサービスへの不正ログイン」を参照。

＜事例または傾向＞

◆ クラウドサーバーへの不正アクセス

2021 年 5 月、ネットマーケティングが運営するマッチングアプリ「Omiai」の利用者の年齢確認書類（運転免許証、健康保険証、パスポート、マイナンバーカード等）の画像 171 万 1,756 件が流出したことが公表された。画像が保存されていたクラウドサーバーにアクセスするための情報を不正に取得した第三者によって、正規のアクセスを装って不正アクセスが行われていた。同社が、サービス退会後も 10 年間会員情報を保持する運用としていたことも被害の大きさにつながったとされている。[1,2]

◆ 改ざんされた EC サイトからの情報流出

2021 年 7 月、読売情報開発大阪が運営する EC サイト「よみファネット」において不正アクセスがあり、1,301 人分のクレジットカード情報が流出したと公表された。そのうち 58 人分のクレジットカードが不正利用され、被害総額は 767 万 4,605 円となった。不正アクセスによって決済処理プログラムの改ざんが行われており、2020 年 10 月 24 日から 2021 年 3 月 2 日の間に同サイトで入力されたクレジットカード情報が窃取された。[3]

◆ SQL インジェクション攻撃による被害

2021 年 9 月、翻訳ソフト等の開発、販売を行っているロゴヴィスタが、サーバーに不正アクセスを受け、登録ユーザーのメールアドレス約 12 万 8,000 件が流出したことを公表した。利用者から迷惑メールが届くようになったとの連絡を受けて調査をしたところ発覚したもので、サーバーの脆弱性を悪用してデータベースを不正に操作する SQL インジェクション攻撃を受けていたことが判明した。[4]

＜対策/対応＞

個人（インターネット利用者）

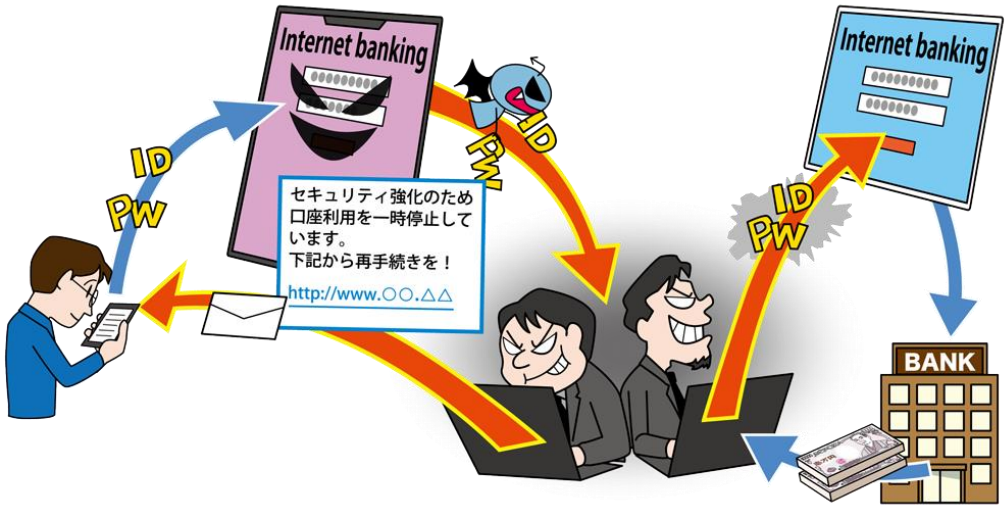
- 情報モラルやリテラシーの向上
  - ・サービス利用の必要性を判断する
  - ・不要な情報は安易に登録しない
    情報漏えいに備えて、サービスを利用するための必須項目以外の情報は登録を避ける。
  - ・多要素認証の設定を有効にする
  - ・パスワードを使いまわさない
    パスワード漏えい時の影響を極小化する。
  - ・利用していないサービスの退会
  - ・不正ログイン対策を実施する [5]
- 被害の早期検知
  - ・クレジットカード利用明細の定期的な確認
    クレジットカード情報が窃取され、不正利用された場合、被害に気づける可能性がある。
- 被害を受けた後の対応
  - ・サービス運営者への問い合わせ
  - ・クレジットカードの停止
    クレジットカード会社へ不正利用の連絡と停止の手続きを行う。
  - ・パスワードを変更する（他のサービスで同じパスワードを使っていた場合は同様に対応）
    サービスを継続して利用する場合はパスワードを変更する。
  - ・警察への被害届の提出

参考資料

1. 不正アクセスによる会員様情報流出の調査結果と今後の対応について（株式会社ネットマーケティング）
https://www.net-marketing.co.jp/news/6001/
2. Omiaiの「個人情報流出」が深刻化した根本原因（東洋経済ONLINE）
https://toyokeizai.net/articles/-/431661
3. 読売新聞子会社でクレカ情報流出　すでに767万円の金銭的被害も確認（ITmedia NEWS）
https://www.itmedia.co.jp/news/articles/2107/14/news116.html
4. 弊社ホームページへの不正アクセスによる被害発生のお詫びとお知らせ（ロゴヴィスタ株式会社）
https://www.logovista.co.jp/Iverp/information/information/emergency.html
5. 不正ログイン対策特集ページ（IPA）
https://www.ipa.go.jp/security/anshin/account_security.html

9位 インターネットバンキングの不正利用

～金融機関から SMS が送られてきても、ひとまず落ち着こう～



フィッシング詐欺やウイルス感染により、インターネットバンキングの認証情報を窃取されることで、被害者のアカウントから不正な送金が行われたり、不正にサービスを利用されたりする等の被害が確認されている。2021 年もスミッシング（SMS を用いたフィッシング）をきっかけに不正送金される事件が発生している。

＜攻撃者＞

- 組織的犯行グループ
- 犯罪者

＜被害者＞

- 個人（インターネットバンキング利用者）
- 組織（インターネットバンキング利用者）
- 組織（金融機関）

＜脅威と影響＞

実在する金融機関等を装ったメールや SMS からフィッシングサイト（偽のウェブサイト）へと誘導され、偽物であると気付かずに入力してしまい、攻撃者に認証情報を詐取（フィッシング詐欺）される。また、メールに添付された悪意あるファイルを開いて、端末をウイルスに感染させてしまい、攻撃者に認証情報を窃取される等の被害も発生している。

攻撃者に認証情報を窃取された場合、被害者が持つインターネットバンキングアカウントに不正ログインされ、攻撃者が作成した別の口座に不正送金されたり、インターネットバンキング上のサービスを不正利用されたり等の被害に遭うおそれがある。

＜攻撃手口＞

以下の手口でインターネットバンキングの認証情報を入手し、不正送金を行う。

◆ フィッシング詐欺

偽のメールや SMS を被害者に送信し、フィッシングサイトに誘導して、インターネットバンキングの認証情報を入力させ詐取する。また、多要素認証で使う情報（ワンタイムパスワード等）を入力させる場合もある。詳細は、個人 1 位「フィッシングによる個人情報等の詐取」を参照。

◆ ウイルス感染

ウイルスに感染させるように細工したファイルをメールに添付し、巧妙な文面で被害者にファイルを開くよう誘導して、被害者の端末をウイルスに感染させる。また、改ざんされた正規のウェブサイトを被害者に閲覧させることで、ウイルスに感染させる手口も確認されている。ウイルスに感染した端末でインターネットバンキングにログインしようとすると、偽のログインページが表示され、そこに入力した認証情報が攻撃者に送信される。

＜事例または傾向＞

◆　件数は半減、1 件当たりの被害額は増加

警察庁によると、2021 年 1 月から 6 月のインターネットバンキングに関わる不正送金事犯の発生件数は 376 件、被害額は約 4 億 7,900 万円であった。前年同期の 888 件、約 5 億 4,200 万円に比べて、発生件数は半分以下に減少したが、被害額はやや減少に留まり、1 件あたりの被害額は増加している。被害額の約 87%にあたる約 4 億 1,700 万円は個人口座からの不正送金であり、依然として個人の被害が多い状況が続いている。

手口の多くは以前からある SMS やメールを利用したフィッシングと考えられており、メモアプリ等に不正アクセスされ、インターネット上に保存してあった ID やパスワードを用いてインターネットバンキングから不正送金されたと思われるケースも確認されている。[1]

◆　メモアプリ利用時の注意点

警察庁がメモアプリ等へ不正アクセスする手口について公表したことから、2021 年 12 月、日本サイバー犯罪対策センター（JC3）はメモアプリ利用に関する注意喚起を行った。

この注意喚起の中で JC3 は、メモアプリのフィッシングサイトを確認しており、メールや SMS からメモアプリのインターネットサービス（ログイン画面）へ促されても安易にアクセスしないよう注意を呼び掛けている。[2]

◆　幹部ら 3 人逮捕、被害 130 人 9,300 万円

2021 年 11 月、沖縄県警サイバー犯罪対策課等 9 県警合同捜査本部は、インターネットバンキングに不正アクセスし、17 都府県の約 130 人から総額約 9,300 万円を窃取した事件で、犯行の首謀者ら 3 人を「不正アクセス禁止法違反」、「電子計算機使用詐欺」、「窃盗」の容疑で逮捕した。

被害者のスマートフォン等にメガバンクを装った SMS を送り、口座番号やパスワードを入力させるスミッシングが用いられ、メガバンクにある被害者の口座から県内銀行の口座に不正送金され引き出されていた。[3]

＜対策/対応＞

個人（インターネットバンキング利用者）

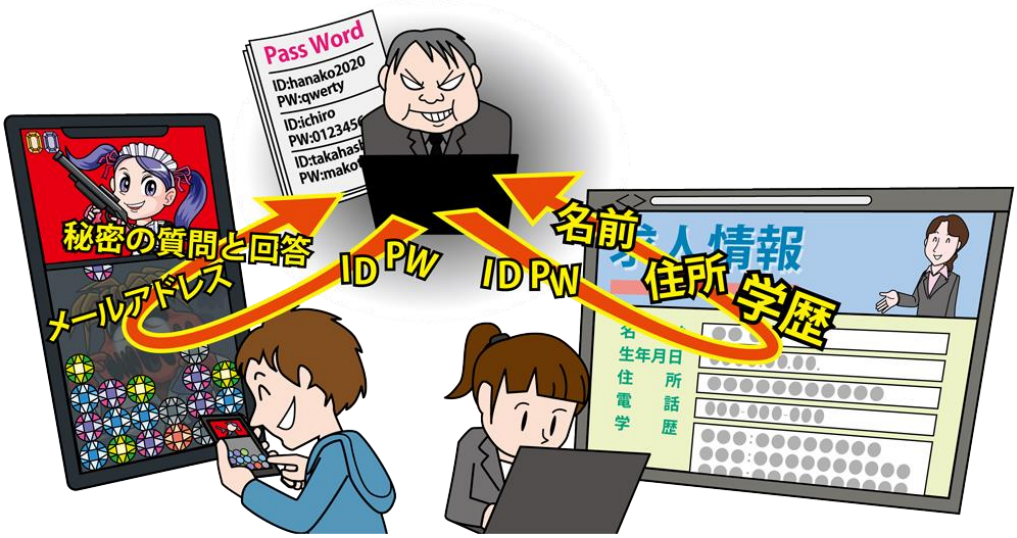
- 被害の予防（被害に備えた対策含む）
  - ・受信メールやウェブサイトの十分な確認
  - ・添付ファイルや URL を安易にクリックしない
    よく利用するウェブサイトは、予めブックマークに登録し、メール等のリンクではなくそこからアクセスする。
  - ・PC 等でファイルの拡張子表示設定をする
    不審なファイルに気づきやすくする。
  - ・普段は表示されないポップアップ画面に個人情報を入力しない
  - ・金融機関や公的機関から公開される注意喚起を確認する
  - ・多要素認証の設定を有効にする
  - ・口座連携済みサービスを確認する
  - ・認証に不備がある銀行口座を利用停止する
    暗証番号のみ等、脆弱（ぜい）な認証で利用可能な銀行口座については、必要がなければインターネット取引の利用を停止しておく。
- 被害の早期検知
  - ・不審なログイン履歴の確認
  - ・口座の利用履歴の確認
  - ・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
  - ・当該サービスのコールセンターへの連絡
    金融機関によっては、全額または一部補償してくれる場合がある。
  - ・警察への被害届の提出
  - ・ウイルス感染した端末の初期化
  - ・パスワードを変更する（他のサービスで同じパスワードを使っていた場合は同様に対応）

参考資料

1. 令和3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/R03_kami_cyber_jousei.pdf
2. メモアプリ利用時の注意点（（一財）日本サイバー犯罪対策センター）
https://www.jc3.or.jp/threats/topics/article-414.html
3. 旭琉会幹部ら3人逮捕　ネットバンク不正容疑、被害130人9300万円　沖縄県警など（琉球新報）
https://ryukyushimpo.jp/news/entry-1422467.html

10位 インターネット上のサービスへの不正ログイン

～パスワードの使いまわしに注意、あなたの個人情報が閲覧されるかも～



インターネット上のサービスへ不正ログインされ、個人情報や金銭等の重要情報が窃取される被害が確認されている。別のサービスと同じ ID やパスワードを使いまわす利用者を狙ったパスワードリスト攻撃による不正ログインが行われている。また、不正ログインで得た情報を悪用して更に被害を拡大させるおそれがある。

＜攻撃者＞

- 組織的犯行グループ
- 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 やパスワードを使い、インターネット上のサービスに対して不正ログインを行う攻撃が行われている。使用される ID やパスワードは、別のサービスから漏えいしたものを使う以外にも、被害者が使いそうなものを類推する手口もある。

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の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。さらに、LINE 等の SNS（ソーシャル・ネットワーキング・サービス）であれば、プライベートな写真やメッセージのやりとり等を覗き見されたり、偽の投稿（フィッシング詐欺等）をされたりする。

＜攻撃手口＞

◆ パスワードリスト攻撃

攻撃者が一般的な検索エンジンでは検出されない闇サイト（ダークウェブ）で購入する等何らかの不正な方法で事前に入手した ID とパスワードのリストを使用し、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。複数のサービスで ID とパスワードを使いまわしていると、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

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あるウェブ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＞

◆ **転職情報サイトに不正ログインされ、履歴書を閲覧**

2021 年 2 月、マイナビが運営する転職情報サイト「マイナビ転職」において、外部で不正に取得されたと思われるパスワードを使い、不正ログインされる被害が確認された。同サイトに登録したユーザーのうち 21 万 2,816 人のアカウントが不正ログインされ、ユーザーの Web 履歴書にアクセスされた。被害拡大防止策として全ユーザーのパスワードをリセットし、パスワードの再設定を依頼した。[1]

◆ **通販サイトに不正ログイン**

2022 年 1 月、2020 年から 2021 年にかけて自身のスマートフォンを使い、女子大学生の SNS アカウントに 4 回の不正アクセスし、女性タレントの SNS アカウントのログイン ID やパスワードをインターネット上で保管した疑いで男が逮捕された。
被害者は、名前や生年月日にちなんだパスワードを設定しており、男はアカウント名やプロフィールの情報を組み合わせてパスワードを類推していた。[2]

◆ **モバイル向けゲームの会員サービスに不正ログイン**

2021 年 10 月、モバイル向けゲームを提供する KLab の会員サービス「KLab ID」において、パスワードリスト型攻撃により、不正ログインされる被害が確認された。不正ログインされたユーザーは 2,846 件で、メールアドレス、ひみつの質問と回答、生年月日等、当該サービスと連携したアプリで閲覧できる全ての情報が閲覧されたおそれがある。同社は、全ユーザーのアカウントに対して二段階認証を必須とする対応を行った。[3]

＜対策/対応＞

個人（ウェブサービス利用者）

- 被害の予防
  - ・表 1.3「情報セキュリティ対策の基本」を実施
  - ・添付ファイルや URL を安易にクリックしない
  - ・パスワードは長く、複雑にする [4,5]
    ID にメールアドレスを用いている場合は、他のサービスでも不正ログインされやすくなるため特に注意する。
  - ・パスワードの使いまわしをしない
  - ・パスワード管理ソフトの利用
  - ・サービスが推奨する認証方式の利用
    多要素認証や多段階認証の設定を有効にする。[4]
  - ・不審なウェブサイトで安易に認証情報を入力しない（フィッシングに注意）
  - ・利用していないサービスからの退会
- 被害の早期検知
  - ・利用しているサービスのログイン履歴の確認
  - ・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
- 被害を受けた後の対応
  - ・パスワードを変更する（他のサービスで同じパスワードを使っていた場合は同様に対応）
  - ・クレジットカードの停止
  - ・不正ログインされたサービスの運営者へ連絡
  - ・警察への被害届の提出

参考資料

1. 「マイナビ転職」への不正ログイン発生に関するお詫びとお願い（株式会社マイナビ）
https://www.mynavi.jp/topics/post_29797.html
2. 弊社「ディノスオンラインショップ」への“なりすまし”による不正アクセスについて（株式会社DINOS CORPORATION）
https://www.dinos.co.jp/guide/info/topics_20210514.pdf
3. KLab ID への不正ログインに関するお知らせ（KLab株式会社）
https://www.klab.com/jp/press/info/2021/1027/klab_id_2.html
4.不正ログイン対策特集ページ（IPA）
https://www.ipa.go.jp/security/anshin/account_security.html
5. 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/mgdayori20160803.html

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　内海 百葉　亀山 友彦
大友 更紗　吉本 賢樹　丹野 菜美
佐々木 敬幸　佐藤 輝夫　湯澤 凱貴

IPA 執筆協力者　瓜生 和久　桑名 利幸　渡辺 貴仁
松坂 志　加賀谷 伸一郎

情報セキュリティ 10 大脅威 2022

2022 年 2 月 28 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/