情報セキュリティ

10 大脅威 2023

～全部担当のせいとせず、組織的にセキュリティ対策の足固めを～

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

2023 年 3 月

本書は、以下の URL からダウンロードできます。

「情報セキュリティ 10 大脅威　2023」
https://www.ipa.go.jp/security/10threats/10threats2023.html

目次

はじめに

本書「情報セキュリティ 10 大脅威 2023」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、2022 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 2023

個人の 10 大脅威では 9 位以上の脅威が 2020 年から 4 年連続で 10 大脅威に選抜されている。10 位となった「ワンクリック請求等の不当請求による金銭被害」は、「10 大脅威 2018」以来 5 年ぶりのランクインとなった。古くからある脅威だが、2022 年 7 月には IPA から注意喚起も発信しており、金銭被害を受けないためには事前に手口を知っておくことが重要である。

一方、組織の 10 大脅威でも、9 位以上の脅威が 2022 年から 2 年連続で 10 大脅威に選抜されている。「サプライチェーンの弱点を悪用した攻撃」は 2013 年から 2 位以上を維持し続けていた「標的型攻撃による機密情報の窃取」を抑えてのランクインとなっている。また、10 位となった「犯罪のビジネス化（アンダーグラウンドサービス）」は「10 大脅威 2018」以来 5 年ぶりにランクインとなった。これは盗んだ情報の売買だけではなく、攻撃に使用するツールやマルウェアの売買が行われることもあり、攻撃のさらなる増加につながる脅威でもあるため、組織としてはセキュリティ対策の重要度がさらに上がっていると言える結果である。

本書では、2022 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 2023

情報セキュリティ 10 大脅威 2023

■「情報セキュリティ 10 大脅威 2023」

2022 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 2023」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 2023 「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	サプライチェーンの弱点を悪用した攻撃
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	標的型攻撃による機密情報の窃取
クレジットカード情報の不正利用	4	内部不正による情報漏えい
スマホ決済の不正利用	5	テレワーク等の ニューノーマルな働き方を狙った攻撃
不正アプリによる スマートフォン利用者への被害	6	修正プログラムの公開前を狙う攻撃 （ゼロデイ攻撃）
偽警告によるインターネット詐欺	7	ビジネスメール詐欺による金銭被害
インターネット上のサービスからの 個人情報の窃取	8	脆弱性対策情報の公開に伴う悪用増加
インターネット上のサービスへの 不正ログイン	9	不注意による情報漏えい等の被害
ワンクリック請求等の 不当請求による金銭被害	10	犯罪のビジネス化 （アンダーグラウンドサービス）

本章で共通的に使用する用語の定義を**表 1.2** に記載する。

表 1.2 情報セキュリティ 10 大脅威 2023 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 2023」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 2023」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 6 位）への対策の必要性は低くなる。

また、組織の立場では、テレワークを行っている組織であれば、テレワーク環境構築のために利用している機器やソフトウェア等を狙った脅威である「テレワーク等のニューノーマルな働き方を狙った攻撃」（本書、組織 5 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 2023」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。「情報セキュリティ 10 大脅威 2022」ランクインしていた、「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、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」「共通対策集」の実施が重要

実施することで多くの事例で被害を受けずに済むまたは軽減できると言える、「情報セキュリティ対策の基本」と、「共通対策集」について、より具体的に巻末で解説する。

これらを読み、理解することで継続的に適切な対策を行い、被害に遭う可能性の低減と被害規模縮小の一助となることを期待する。

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

～不安を煽る巧妙なフィッシングメールに注意！～

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

＜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、本物と勘違いした受信者を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。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。

詐取された情報が悪用されて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や SMS 等を不特定多数に送信**

攻撃者が、公的機関や有名企業等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、セキュリティコード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。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。[1]

◆　**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、悪質なショッピングサイト等に誘導され、金銭的な詐欺等の被害に遭う。

＜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＞

◆　**過去の本物の内容を模したフィッシング**

2022 年 3 月、JR 東日本が指定券予約サービス「えきねっと」を騙った不審メールについて注意喚起を行った。2 年以上サービスにログインしていないと自動退会になるとして、利用継続を希望する場合はメールに記載のリンクからログインするよう促す内容で、個人情報の入力を求める偽サイトに誘導される。メールの内容は、過去に同サービスが利用者に向けて掲載した「【重要】アカウントの自動退会処理について」という文章を模した物だった。[2]

◆　**「国税庁」を騙ったフィッシング**

2022 年 8 月、国税庁は同庁を騙った不審メールや SMS が確認されているとして注意喚起を行った。e-Tax 利用者に送られる「税務署からのお知らせ」に似通ったメールや、税金が未払いであるという不安を煽る内容のメール、SMS 等でフィッシングサイトに誘導される。メールの中には、送信元表記のアドレスや表示名等を国税庁で使用しているものに装ったものも確認された。誘導先の偽サイトでは未払いの税金を納付するよう促され、個人情報やクレジットカード情報等の入力が求められる。[3,4]

◆　**フィッシング報告件数は過去最多**

フィッシング対策協議会のフィッシング報告状況によると、2022 年は 3 月頃からフィッシング報告件数が増加し、1 年間の合計は約 970,000 件となった。これは、2021 年の合計約 530,000 件と比較すると 2 倍弱の件数となっている。特に 2022 年 7 月から 9 月にかけてはクレジットカードの利用確認を装ったフィッシングが急増し、この攻撃ではドメインとサブドメインを組み合わせることで大量の偽サイトの URL を使用する手口が確認されている。また、同年 12 月には偽サイトの URL を QR コードにしてメールに埋め込む手口も増加傾向となった。

SMS を利用したフィッシングでは国税庁のほか、宅配業者の不在通知や Amazon 等のショッピングサイト、通信事業者等を騙ったものも継続して報告されている。[5,6,7]

フィッシング対策協議会ではフィッシング対策の心得として「利用者向けフィッシング詐欺対策ガイドライン」を公開している。[8]

＜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
  - ・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　※
  - ・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

2位 ネット上の誹謗・中傷・デマ

～昨日の友は今日の敵？熱くなりすぎず冷静な対応を！～

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。2022 年はサッカーの世界大会が開催され、試合の結果を元に過剰な誹謗・中傷が発生した。

＜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、広範囲な情報発信が匿名で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・デマを書き込む事案が確認されている。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

特定の個人や企業に対する意見や感情を発言する際に、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。誰もが閲覧できるサービスの場合、1 つの発言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から発信された、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・中傷やデマが広がっていく。

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＞

◆ **「教材に反ワクチンのチラシ封入」のデマ拡散**

2022 年 3 月、「ベネッセの小学 1 年生用教材に、反ワクチンを呼び掛けるチラシが入っていた」というデマの投稿が Twitter 上で拡散された。ツイートはチラシの画像付きで投稿されていたが、これを見た人の中には「デマなのでは？」と疑う者もいた。しかし、Twitter 上で話題になり、ベネッセにも多くの問い合わせがあったため、ベネッセはこどもちゃれんじ編集部の公式 Twitter で「進研ゼミ小学講座ではこうしたビラを封入指示している事実はございません」と否定した。[1] なお、こうしたベネッセの対応は本来なら不要なものであり、Twitter の投稿が業務の妨害を目的としたものではなかったとしても、偽計業務妨害罪にあたるおそれがある。[2]

◆ **デマの投稿者に名誉棄損等で有罪判決**

2022 年 10 月、甲賀市のコンビニ店長の写真を添付し、「私コロナ感染者と近寄って来た」「この店には絶対行かないで」と SNS にデマを投稿した女に有罪判決が下された。名誉毀損と偽計業務妨害の罪に問われ、最終的に投稿者に懲役 8 月、執行猶予 3 年が言い渡された。[3]

また、同月、Twitter 上や掲示板サイトに 2017 年の東名高速道路の煽り運転事件で起訴された被告と関わりがあると同姓の他人に関するデマを書き込んだとして、231 万円の損害賠償の支払いが命じられた事例もある。被害者が経営する会社が休業する事態になり、社会的評価を低下させたことを裁判所が認めた結果となった。[4]

◆ **試合結果に応じて日本代表選手を誹謗・中傷**

2022 年 11 月から 12 月にかけて、カタールでサッカーの世界大会が開催され、連日報道でも取り上げられて話題になった。このような大規模スポーツイベントは国民が一丸となって応援する一方で試合の結果次第では誹謗・中傷の対象にされることも少なくない。本大会において、直前まで応援していた選手に対して、敗戦を機に手のひらを返し、SNS 上での誹謗・中傷が行われた。[5]

これに対し、元日本代表選手も「安易な批判はやめるべき。」等と警鐘を鳴らした。また、FIFA と国際プロサッカー選手会は大会前、大会の出場選手を SNS の誹謗中傷から守るサービスを始めると発表し、差別や脅迫に対して運営元や法務当局に通報する方針を示した。[6]

＜対策/対応＞

個人（発信者、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

  ・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。

  ・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]

  ・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）

- 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

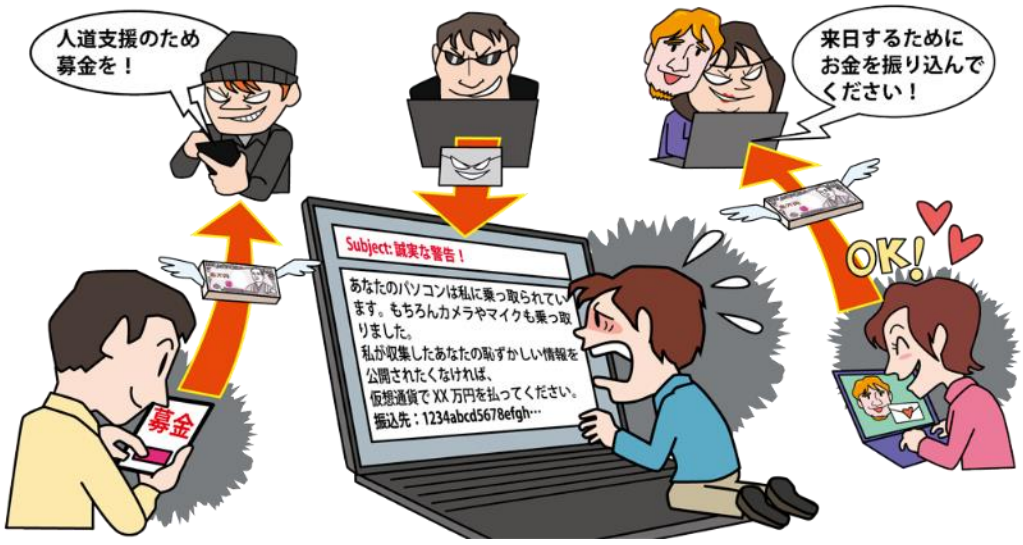
  問題ある書き込みを削除したいときは本人または関係者がウェブサイトの管理者やプロバイダーに削除を要請する。なお、削除により事態が悪化する可能性もあるため、要請する際は信頼できる周囲の人や弁護士等に相談して慎重に行う。

  ・適切な報告/連絡/相談を行う ※

※巻末「共通対策」を参照

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

～人の心の弱みに付け込む詐欺に注意～



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、SMS（ショートメッセージサービス）、SNS（ソーシャル・ネットワーキング・サービス）等を利用した脅迫、詐欺による金銭被害が発生している。2022 年はコロナ禍やウクライナの情勢を悪用した詐欺が行われた。

＜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、SMS、SNS 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すると、その脅迫は効果が期待できるとして、同様の手口で多方面に攻撃が行われ、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、SNS 等を不特定多数に送り、金銭を詐取しようとする。支払方法として暗号資産（仮想通貨）やプリペイド型電子マネーが指定されることが多い。

◆　セクストーション（性的脅迫）

周囲に相談しにくい性的な弱みに付け込んで金銭を恐喝する。例えば、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行わせた後、スマホに不正アプリのインストールを誘導する。不正アプリには連絡先を窃取する機能が仕込まれており、窃取した連絡先内の知人に恥ずかしいやり取りをばらすと脅す。

◆　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、不安を煽る。記載している情報はハッキングで窃取したものではなく、外部のサービスから漏えいしたものである。

◆　公的機関を装う

公的機関等信頼できる組織からのメール等を装うことで信憑性、緊急性を高めて騙す。さらに公的機関からの連絡であることで不安を煽り、連絡を取るよう求めてくることもある。

◆　**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、偽の問い合わせ窓口の電話番号を記載して送信し、この電話番号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掛け、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。

◆　**SNS 等で親交を深めた後に金銭を要求する**

SNS 等を利用し、海外の異性を装いオンライン上で交際を持ち掛ける。ある程度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。（ロマンス詐欺）

＜事例または傾向＞

◆　**大学内のメールアドレス宛に脅迫メール送信**

2022 年 8 月、国立大学法人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、学内に注意喚起を行った。メールには、デバイスをハッキングしたこと、あなたの恥ずかしい場面を録画したこと、暗号資産を送金すれば内容を削除すること、等が記載されており、周りの人に相談しにくい内容で脅迫している。[1]

◆　**巣ごもりでロマンス詐欺が増加傾向**

2022 年 10 月、滋賀県東近江署は、ロマンス詐欺により女性が約 440 万円を騙し取られたと発表した。被害女性は SNS で知り合った外国人宇宙飛行士を名乗る男とやり取りを交わし、チャット上で親密な間柄となった。男から地球に戻るためのロケット費用や、日本への着陸料等の名目で現金を要求され、被害女性は当該金額を支払った。その後、不審に思った女性が警察署に相談して詐欺が発覚した。[2]

滋賀県警によると、2022 年 1 月から 9 月までの県内の国際ロマンス詐欺被害は 41 件で、前年同期より 13 件増えている。また、被害総額は約 2 億 9,200 万円に上り、男女関係なく被害に遭っている。

滋賀県警は被害が増えている理由として、コロナ禍での「巣ごもり」により、SNS をきっかけにした出会いが増加したこと等を挙げている。[3]

◆　**ウクライナ情勢利用し、義援金詐欺が問題に**

2022 年 3 月、SNS を利用してウクライナの義援金を募るように見せかけた義援金詐欺が発生しているとして、国民生活センターが注意喚起を発表した。SNS で見かけたウクライナへの義援金の募集を見てクレジットカードで 1,000 円を募金したが、募金した義援金サイトは偽物の可能性があると知り、返金を求めた相談事例が紹介されている。[4]

また、義援金以外にも SNS を通じて知り合ったウクライナにいる日本人から荷物を日本に送るために 200 万円を暗号資産で送付してほしいと依頼を受けた相談事例も紹介されている。[5]

＜対策/対応＞

個人（インターネット利用者）

- 被害の予防
  - ・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、ハッキングされていることはほぼない。しかし、実際に使用しているパスワードが記載されていた場合は漏洩している可能性があるのでパスワードを変更する。
  - ・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。
  - ・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
- 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

4位 クレジットカード情報の不正利用

～狙われているのは組織、しかし個人でも対策が必要！～

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。一方、クレジットカード所有者を狙ったフィッシング詐欺や EC サイトの脆弱性を狙ったウェブ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

＜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活用する機会が増えている。攻撃者は、フィッシング詐欺やウェブサイトの改ざん等様々な攻撃手口を用いて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、正規の利用者が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。[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 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

EC サイト（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。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。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。

◆ 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＞

◆ **「MACHATT ONLINE STORE」でクレジットカード情報 16,093 件流出**

2022 年 5 月、株式会社 machatt はファッション用品を取り扱う「MACHATT ONLINE STORE」において 2021 年 8 月から 2022 年 2 月にかけて利用された 16,093 件のクレジットカード情報が流出し、一部は不正利用されたおそれがあることを公表した。

攻撃者にシステムの脆弱性を悪用され、不正アクセス後、ペイメントアプリケーションを改ざんされていたことが原因であった。同社は利用者に向けて、身に覚えのない請求項目がないかを確認し、それがあった場合は、クレジットカード会社に問い合わせるよう呼び掛けている。[2]

◆ **「スイーツパラダイスオンラインショップ」でクレジットカード情報 7,645 件流出**

2022 年 6 月、井上商事株式会社は運営する「スイーツパラダイスオンラインショップ」で 2021 年 8 月から 12 月にかけて利用された 7,645 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。

攻撃者にシステムの脆弱性を悪用され、不正アクセス後、ペイメントアプリケーションを改ざんされていたことが原因であった。2021 年 12 月頃、同サイトでクレジットカードを利用した人からクレジットカードが不正利用されたとの報告が Twitter 上で相次いでいた。それを受けて、同サイトは半年に渡り閉鎖したままの状態となっていた。[3]

◆ **クレジットカードの情報の不正利用被害額が年々増加傾向**

2022 年 12 月、一般社団法人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、2022 年 1 月～9 月の被害額は 309.2 億円となった。2021 年同期間の被害額 236.9 億円と比較して、約 30%増加している。被害額の内訳では番号盗用被害額が 291.3 億円で全体の 94.2%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
  - ・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

- 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の初期化
  - ・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

5位 スマホ決済の不正利用

～フィッシングメールに注意、知らないうちにあなたのスマホ決済が悪用されているかも～

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

＜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。攻撃者は、決済サービスに窃取した ID とパスワードで不正ログインしたり、決済サービスや仕組みの不備を悪用したりして不正利用をする。

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

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。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。

◆ **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を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、意図せずに不正利用される。

＜事例または傾向＞

◆ **フィッシングメールで盗まれたIDとパスワードを使いメルペイを不正利用**

2022 年 5 月、警視庁はメルカリグループの電子決済サービス「メルペイ」を悪用し、美容品を詐取したとして、中国籍の複数の女を逮捕した。

被疑者は、2021 年 9～11 月、東京都の百貨店やドラッグストアで、福岡県の男女 3 人の名義で登録されたメルペイの決済用バーコード画像を示し、洗顔フォームや美容液等、55 点（約 50 万円）を不正に購入した疑いがある。中国に住む仲間がフィッシングメールで盗んだ ID とパスワードでメルペイに不正接続し、決済用バーコードの画像を被疑者に送っていた。[1]

◆ **フィッシングメールで盗まれたIDとパスワードを使い au PAY を不正利用**

2022 年 9 月、京都府警は他人名義のアカウントで商品を不正に購入したとして詐欺容疑で複数の中国人留学生を逮捕した。

犯行前、アカウントの所有者のもとに au を装った偽メールが届いており、偽サイトと知らずに接続して ID やパスワードを入力し、窃取されていた。「au でお支払いしている継続利用サービスを更新する必要があります」とする偽メールの文言を信用してしまったという。なお、京都府警では「au PAY」の不正利用に対する相談が相次ぎ、3～8 月の相談件数は 202 件に上っている。[2]

＜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
  - ・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

    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の退会
  - ・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

6位 不正アプリによるスマートフォン利用者への被害

～言葉巧みに不正アプリのインストールを誘導する手口に注意～

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、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。また、有名企業を騙り 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。昨今、SNS を通じたやり取りで言葉巧みに不正アプリをインストールさせる手口も確認されている。

＜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、ウイルスを忍ばせた不正アプリを公式マーケットに公開しておき、不正アプリと気づかず利用者がインストールしてしまったり、SNS 等で言葉巧みに誘導され不正アプリをインストールさせられたりする場合もある。

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。

また、SNS で出会った相手を言葉巧みにダウンロードサイトに誘導して、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。利用者は正規アプリだと思い込み、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

アプリのインストール時には悪意ある機能を顕在化させず、アプリの更新時に顕在化させ、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＞

◆ **マッチングアプリで出会った相手を不正アプリのインストールへ誘導**

2022 年 1 月、マッチングアプリで知り合った異性からの誘導で不正アプリをインストールしたことで連絡先情報等が窃取され、金銭を要求される等の脅迫を受けたとの相談が長崎県警察に寄せられた。

攻撃者は、マッチングアプリで知り合った異性に対し「恥ずかしい姿をライブ中継している」「このアプリをインストールすると見ることができる」とメッセージを送り、不正アプリのインストールサイトの URL を伝え、さらに招待コードを送ってインストールしたアプリでログインするように誘導していた。[1]

◆ **有名 SNS の認証情報を狙った不正アプリ**

2022 年 10 月、Meta（旧称、Facebook）は Facebook のログイン情報を盗み出す悪質な Android アプリ、iOS アプリを 400 件以上確認したと発表し、注意喚起を行った。不正アプリは写真編集、カメラ、VPN サービス、ゲーム、広告管理など、便利そうなものや楽しそうなものが多い。

アプリは Facebook ログイン機能を悪用し、ユーザーが Facebook アカウントでログインすると、Facebook アカウントとパスワードを盗まれる。そして Facebook のアカウントが乗っ取られたり、個人情報が窃取されたりするおそれがある。なお、当該アプリはアプリストアから削除済みとしている。[2]

◆ **国税庁を騙り、不正アプリのインストールを誘導**

2022 年 8 月と 9 月にフィッシング対策協議会が公開したレポートによると、国税庁を騙るフィッシングの報告を多く受領したという。SMS を使ったフィッシングでは、Android スマートフォンを利用している場合は不正アプリのインストールに誘導されることがあり、注意を呼び掛けている。また、宅配関連の不在通知を装う文面や Amazon を騙る文面の SMS の報告も引き続きあるという。[3,4]

＜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

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

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

・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。

7位 偽警告によるインターネット詐欺

～警告画面の連絡先に電話しないで！！～

PC やスマートフォンからインターネット上に公開されている情報や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」等の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、サポート窓口を装った番号に電話をかけさせて PC の遠隔操作や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る被害（サポート詐欺）が発生している。

＜攻撃者＞

- 組織的犯罪グループ

＜被害者＞

- 個人（インターネット利用者等）

＜脅威と影響＞

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。

画面の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うと、PC の遠隔操作や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、不審なスマホアプリをインストールするように誘導される。

また、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

ウェブサイト等のインターネット広告に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

偽警告の画面に表示させたサポート窓口へ閲覧者に電話をかけさせ、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、サポート契約やウイルスの除去など修復代金の支払いへ誘導する。サ

ポート契約等の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。

◆　**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。誘導したことにより広告主からアフィリエイト報酬を得たり、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。

＜事例または傾向＞

◆　**PC を遠隔操作、通信販売で勝手に物品購入**

2022 年 8 月、沖縄県嘉手納署は偽警告によるサポート詐欺が発生したことを発表した。被害者の女性が自宅で PC を使用していたところ、「トロイの木馬スパイウェアに感染」等と記載された画面が音声アナウンスとともに表示され、表示されている連絡先に電話してしまった。その後、片言の日本語で話す男に PC 操作を誘導され、PC を遠隔操作されてしまい、電子マネー等を勝手に購入されたほか、SNS を不正に利用された。なお、押収した PC を確認したところ自動音声が流れる仕組みだったことが分かった。[1]

◆　**偽警告被害の相談件数が増加傾向**

2022 年 10 月、IPA 安心相談窓口が公開したレポートと、「安心相談窓口だより」によると、「ウイルスに感染している」等、偽のセキュリティ警告に関する相談件数は、2022 年第 1 四半期は 625 件、第 2 四半期は 435 件、第 3 四半期は 544 件、第 4 四半期は 761 件となっており、前年同期の 246 件、232 件、192 件、420 件と比較して相談件数が大きく増加している。さらに、2023 年 1 月の相談件数は 401 件となっており、月間の相談件数としては過去最高件数となっている。[2,3,4]

◆　**偽警告によるサポート詐欺に対する支払い方法はプリペイド型電子マネーが大半**

2022 年 2 月、国民生活センターの公表した情報によると、全国の消費生活センター等にはサポート詐欺に関する相談がここ数年は年間 5,000 件以上寄せられており、有償サポートやセキュリティソフトの契約購入金額の平均金額は年々高額化している。また、支払い方法は、クレジットカードに代わりプリペイド型電子マネーが大半を占め、2021 年度においてはクレジットカードが 428 件、プリペイド型電子マネーが 1,821 件であった。[5]

＜対策/対応＞

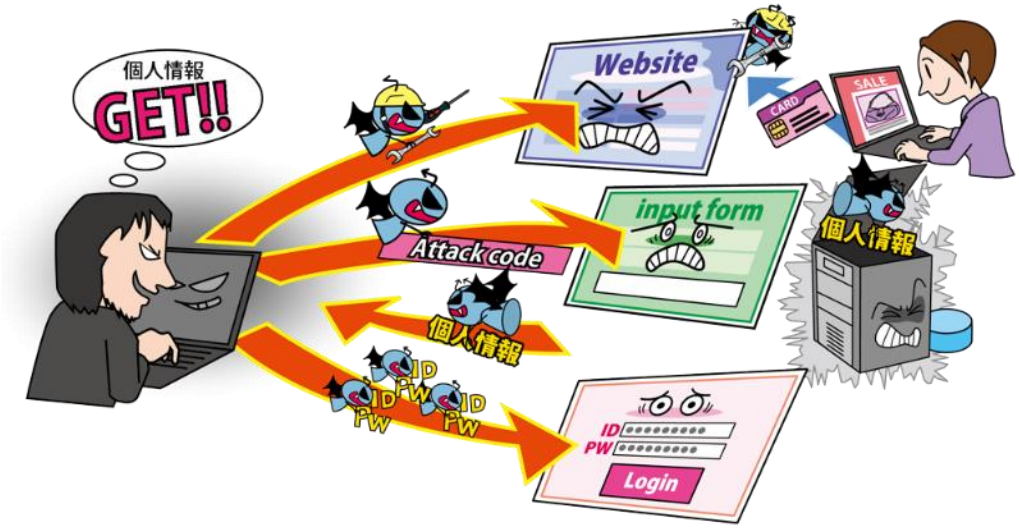
個人（インターネット利用者等）

- 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
    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
    警告に指示されたアプリやソフトウェア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許可しない、契約には応じない、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
    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 [6] に相談する。
  - ・ブラウザの通知機能を不用意に許可しない [7]
    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 [8]
  - ・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
  - ・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
  - ・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
  - ・虚偽のサポート契約の解消
  - ・適切な報告/連絡/相談を行う　※

※巻末「共通対策」を参照

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

～オンラインショッピングの個人情報に注意！～



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。昨今の新型コロナウイルスの影響による巣ごもり需要の拡大や決済方法の多様化等がインターネット上のサービスの利用を促進し、被害発生に拍車をかけているおそれがある。

＜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、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を行っていない場合がある。また、利用者においても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。

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、窃取された情報をダークウェブ（一般的な検索エンジンでは検出されない闇サイト）で売買されたり、詐欺メールを送信される等、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 9 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＞

◆　**データベースに不正アクセスで個人情報窃取**

2022 年 6 月、株式会社 SODA は運営するショッピングサイト「SNKRDUNK」に登録されている個人情報が不正アクセスによって漏えいしたことを公表した。氏名、生年月日のほか、購入履歴や復号が不可能の状態で保存されたパスワードが窃取され、漏えいした件数は約 275 万件であった。なお、クレジットカード番号や本人確認書類は窃取されていないとしている。また、不正なリクエストに対するデータベースのレスポンスに不備があったことが原因として、不備の修正を行った上で脆弱性診断や WAF の導入等の処置を行った。[1]

◆　**システム改ざんでクレジットカード情報窃取**

2022 年 8 月、出光クレジット株式会社は同社が運営する会員サイト「ウェブステーション」において、攻撃者にシステムが改ざんされ特定のページに入力を行った利用者の情報が漏えいしたおそれがあることを公表した。

調査したところ、改ざんが発生した 7 月 19 日からシステムを修正した 7 月 26 日の期間に新規登録、再登録を行った利用者のクレジットカード番号、有効期限、セキュリティコード、生年月日の情報が漏えいしたおそれがあった。

同社は該当する利用者に向けて連絡済みとしており、再発防止に努めている。[2]

◆　**EC サイトへのパスワードリスト攻撃による不正アクセスで個人情報窃取**

2022 年 7 月、株式会社サンドラッグは運営する EC サイト「サンドラッグ e-shop 本店」、「サンドラッグお客様サイト」が不正アクセスされ、約 2 万件の会員情報（氏名、住所、電話番号、メールアドレス、パスワード等）が閲覧された可能性があることを公表した。これはシステム委託会社からの報告により発覚したものである。

攻撃は海外の IP アドレスから行われ、他社サービスから流出した可能性があるユーザーID とパスワードを利用したパスワードリスト攻撃と推測されている。対策として不正ログインが試行された海外 IP アドレスからのアクセスを遮断し、パスワード変更等をユーザーに依頼している。[3]

＜対策/対応＞

個人（インターネット利用者）

- 被害の予防
  - ・サービス利用の必要性を判断し、不要なサービスに登録をしない
  - ・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。
  - ・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からの退会
  - ・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、被害に気づける可能性がある。
- 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

9位 インターネット上のサービスへの不正ログイン

～狙われるインターネット上のサービス、各自でできる限りの対策を～

インターネット上のサービスへ不正ログインされ、個人情報や決済情報等の重要情報が窃取される被害が確認されている。別のサービスのアカウントと同じパスワードを使い回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さら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を行う攻撃が行われている。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したものである。

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（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取り等を覗き見されたり、投稿を削除される等の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＞

◆ パスワードリスト攻撃

攻撃者がダークウェブ（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。複数のサービスで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

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。

◆　**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 1 位「フィッシングによる個人情報等の詐取」を参照。

＜事例または傾向＞

◆　**不正ログインによる個人情報の流出**

2022 年 9 月、ニトリは提供しているスマートフォンアプリ「ニトリアプリ」において不正ログインの被害があったことを公表した。9 月 15 日から 20 日にかけて約 13 万 2,000 件のアカウントが不正ログインされ、メールアドレスやパスワード、氏名や住所等の個人情報のほか、保有ポイント数やクレジットカード情報の一部も流出したおそれがある。なお、クレジットカード決済に必要な情報はシステム内で保持していなかったため、カード決済による金銭被害は確認されていない。手口はニトリ以外のサービスから流出した ID とパスワードのリストを利用しニトリアプリ認証プログラムに対してログインを試みるパスワードリスト攻撃と推測されている。[1]

◆　**TikTok における乗っ取り被害**

2022 年 6 月、バーチャル YouTuber（VTuber）グループ「にじさんじ」に関わる VTuber の TikTok アカウントが相次いで乗っ取りの被害を受けた。被害に遭ったのは同グループに所属または既に卒業していた VTuber 約 10 人のアカウントで、ユーザー名やアイコンが変更されたり、投稿した動画が削除され無関係の動画が投稿されたりといった被害が確認されている。[2,3]

◆　**二要素認証未実施による不正ログイン被害**

2022 年 12 月、熊本県立大学は同大学の名誉教授のメールアカウントが不正ログインされていたことを公表した。身に覚えのないメールが返ってくることで教授本人が被害に気付き、調査の結果、海外からの不正ログインが約 1,000 回確認された。

名誉教授のアカウントに不正ログインされたことにより、同大学のメールユーザー（教職員や学生等）の氏名やメールアドレス等、名誉教授のアドレス帳の情報、名誉教授のメールボックス内のメールと添付ファイルが漏えいしたおそれがある。

同大学ではメールアカウントへのログインには二要素認証を用いることを原則としていたが、名誉教授はスマートフォン等を所持していないため二要素認証を除外されていた。また、パスワードが簡素かつ他サイトでも同じアカウントとパスワードを使用していたことも原因と考えられている。[4]

＜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
  - ・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
  - ・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
- 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
  - ・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

10位 ワンクリック請求等の不当請求による金銭被害

～見せかけの操作や画面に騙されないで～

ウェブサイトやメールに記載されたリンクをクリックやタップしただけで請求画面や登録完了画面が表示され、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）もある。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。

＜攻撃者＞

- 組織的犯行グループ

＜被害者＞

- 個人（ウェブサービス利用者）

＜脅威と影響＞

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

請求画面では、早急に支払わなければ訴訟をするといった脅しにより、被害者の不安な煽り、被害者は焦って料金を支払ってしまっている。支払った後も、再度支払いを要求される場合もある。また、そういった被害者を狙って、ワンクリック請求の対処法を検索サイト等で検索する中で消費者救済を装う怪しい業者に金銭を騙し取られる二次被害も発生している。

＜攻撃手口＞

◆ 悪意あるウェブサイトの閲覧

アダルトサイトや出会い系サイト内に表示されている「18 歳以上」の年齢確認や動画再生のボタンをクリックすることにより、会員登録完了の請求画面が表示される。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、クリックさせる手口のほか、表示しているページを自動的に請求画面へ転送し、支払いを請求する手口（ゼロクリック詐欺）もある。

◆ メールに記載されたリンクのクリック

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

◆ 不正プログラム・アプリをインストールさせる

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

◆　**電話をかけるように誘導**

請求画面にお問い合わせ先の電話番号を表示し、退会を焦る被害者に電話をかけさせるように誘導する。電話をかけると相手に電話番号が知られ、さらに、「再生 OK ボタンを押したから契約は成立しているため解約はできない」等と支払いを迫られることもある。また、電話中に退会や支払いを免除するためと称して個人情報を聞きだそうとする場合がある。個人情報を伝えてしまうと、その情報を悪用されるおそれがある。

＜事例または傾向＞

◆　**ワンクリック請求の手口に引き続き注意**

2022 年 7 月、IPA 情報セキュリティ安心相談窓口はワンクリック請求に関する相談が引き続き寄せられていると改めて注意を呼びかけた。2022 年は 1 月から 6 月まではひと月当たり 8～22 件の相談を受け付けており、2021 年の 4 月から 12 月のひと月当たり 5～23 件と比較してほぼ同等の推移となっている。2013 年の多い時でひと月当たり 300 件以上の相談があった頃と比較すると、昨今は大きく件数が減少している状況だが、いまだに相談が無くなっていない。形を変えながらも利用者に「有料会員契約が成立（登録）した」等と表示する古典的な手口が継続して行われている。[1]

◆　**10 代の経験した詐欺被害 1 位は「ワンクリック詐欺」**

2022 年 8 月、SMBC コンシューマーファイナンス株式会社は、「10 代の金銭感覚についての意識調査 2022」を公開した。1,000 名の 15 歳～19 歳の学生を対象とした調査となっており、詐欺等のトラブルの被害にあったことがあると答えたのは全体の 11.6%であった。さらに、遭遇した被害を確認すると、特定ページの閲覧後に契約成立の宣言画面が表示され金銭を要求・請求される「ワンクリック詐欺」が 25.9%と最も高く、「フィッシング詐欺」の 20.7%等が後に続いた。[2]

＜対策/対応＞

個人（ウェブサービス利用者等）

- 被害の予防
  - ・表 1.3「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。画面には個人情報を取得したように書かれているが、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。
  - ・請求画面を閉じる [1]
  - ・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　※
  - ・アクセスするウェブサイトの確認
  - ・不正プログラム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：内部不正、あなたの組織は大丈夫？

企業やその他組織における、内部不正によるセキュリティインシデントのニュースが後を絶ちません。2022 年 5 月には岩手県釜石市[1]、2022 年 12 月には山口県宇部市[2]にて、職員が不正に市民の個人情報を閲覧・持ち出しする事件が発生しています。それ以外にも、2022 年には、例えば官公庁関連では以下のような内部不正に関するニュースが報じられています[3]。

日付	組織名	内部不正概要
2022/12/23	山口県宇部市	職員が、勤務時間中に個人的な理由で住民基本台帳システムや戸籍システムにアクセスし、個人情報を入手した。
2022/11/29	神奈川県川崎市	課長級の職員が、定められた手続きを経ずに児童虐待に関する会議資料（氏名や住所、生年月日等）を無断で持ち出し、紛失した。
2022/11/25	群馬県	係長級の職員が、事務処理を怠り、同県の意思決定を経ず、勝手に公文書を施行したり、文書を紛失したりした。
2022/11/18	福島県郡山市	職員が、他職員のアカウントを用いて庁内のグループウェアに不正アクセスし、書き込みや閲覧を行なった。不正アクセスを受けた職員は、ID より類推できる初期パスワードを変更せずにそのまま利用していた。
2022/11/07	東京都杉並区	住民基本台帳ネットワークシステムより個人情報を取得し、外部に漏洩した。
2022/10/27	静岡県伊東市	職員が、他課のアカウント情報を用いて不正にアクセスし、メールや添付ファイルを閲覧したり、一部ファイルを自身の業務用パソコンに保存したりした。同職員は他課の ID とパスワードを推測し、不正アクセスしていた。
2022/10/13	徳島県牟岐町	職員が、個人情報や特定個人情報（マイナンバー）含む書類を不正に自宅へ持ち帰っていた。職員は、書類の整理が追いつかず、机の上に書類が溜まってしまうことから、自宅に持ち帰ってしまったと証言しているという。

なぜ、このような内部不正事案が発生してしまうのでしょうか。本コラムではその原因と基本対策について、不正のトライアングル（Fraud Triangle）をベースに考えていきます。なお、本編では組織 4 位「内部不正による情報漏えい」でも解説していますので、合わせてご確認ください。

不正のトライアングルというのは、アメリカの犯罪学者、ドナルド・レイ・クレッシー（Donald Ray Cressey）によって提唱された、人間が不正を働くのは、「機会（Opportunity）」、「動機（Motive/Pressure）」、「正当化（Rationalization）」の三要素が揃ったときであるという理論です。

■ 機会（Opportunity）

機会とは、不正行為を実行可能である状況に置かれていることを指します。例えば、公園のベンチに財布が置きっぱなしになっており、監視カメラや周囲の目もないような状態です。組織内の場合だと、自身の社内評価や、他人の給与データが入ったファイルなどの、本来閲覧できないファイルがアクセス可能な箇所に配置されていたら、興味本位で開いてしまうケースもあるのではないでしょうか。このように、不正を働いても発覚しにくい、実行できてしまう状態を「機会」といいます。

対策として、デレク・コーニッシュとロナルド・クラーク（Cornish & Clarke）による「状況的犯罪予防の考え方」を基に、環境を適切に定めることが効果的であると考えられます。簡潔にまとめると、不正行為を「やりにくくする」、「やると見つかる」、「割に合わない」ようにすることが基本となります。[3] あくまで一例ですが、アカウントのライフサイクル、データのライフサイクル、最小権限の原則に基づいたアクセス権限の管理を徹底し、重要情報のアクセスについては多要素認証を実施することで、「やりにくくする」ことに繋がります。また、ログを記録し、定期的に確認することで、「やると見つかる」状態にできます。加えて、ログを取得していることを周知することで、「やると見つかる」という意識をもたせることができ、内部不正の抑止力になります。

また、コピーや印刷の制限やメールの添付制限、USB 等デバイス利用制限の実施、クラウドストレージへのアクセスを職場から行えないようにするなどして、手間がかかって「割に合わない」ようにすることで対策しましょう。

■ 動機（Motive/Pressure）

動機とは、不正を働くに至る必要性や誘因を指します。「生活に困窮している」「組織に不満を抱いている」「ミスを隠蔽したい」など、状況によってさまざまです。プレッシャーともいわれており、人を正当な方法ではなく、不正に向かわせてしまう圧力と言い換えることもできます。

組織内で対策する場合、「その気にさせない」ことが基本となります。職場環境の整備を行い、定期的な対話の場を設けるなどの対策を行うことで、不満を未然に解消したり、ミスの隠蔽を減らしたりする効果が期待できます。また、罰則規定を整備・周知することで、「その気にさせない」ことに繋がります。

■ 正当化（Rationalization）

正当化とは、不正行為をすることを正当化する考え方のことを指します。例えば、「会社が自分を評価しないから」「仕事を終えるにはこうするしかない」「うっかりしていた」などが該当します。こういった正当化によって、行為に対する倫理的な抵抗感を減らす心理的作用です。

正当化を防ぐためには「言い訳させない」ことが基本となります。そのためにはルール化とそのル

ールの周知徹底が大事になります。記録媒体の持ち込み、持ち出しに関しては承認を必要とし、記録を行う必要があるようにしたり、未承認の端末については、持ち込めないようにしたりすることで重要情報を守ることができます。「やってはいけないことだと知らなかった」というケースも多くみられることから、内部不正防止関連の内部講習を実施することも効果的と考えられます。さらに、「うっかりしていた」というケースもあるため、内部講習は定期的に実施することが大切です。

上記の三要素が全て揃ってしまうと不正が発生する可能性が非常に高まりますが、逆に、どれか一つでも排除できていれば、不正は起こりにくくなります。まずは、「機会」を排除することが効率的であると考えられていますが、「機会」の排除にはさまざまな対策や制限が必要不可欠になります。対策や制限を増やし過ぎると、業務に支障が出てしまい、従業員からの不信感にも繋がりかねないため、不正を起こさせない仕組みづくりだけでなく、不正を起こす「動機」の排除や「正当化」をさせないといった方向からのアプローチも必要不可欠です。

近年、テレワークをはじめとした新しい働き方が普及したことにより、クラウド利用やテレワーク端末に関する点にも注意が必要となりました。これらについても、テレワーク端末からクラウド利用する際のルールを定めることや、CASB（クラウドアクセスセキュリティブローカー）や SWG(セキュアウェブゲートウェイ)の導入を実施することで「やりにくくする」ことが可能です。また、テレワーク端末の HDD などを暗号化することで、「割に合わない」状況にすることができます。このようにして機会を減らしつつ、エンドポイントのログも収集することで、「やると見つかる」の範囲を拡張することも重要です。

内部不正はどの組織にも起こりうる事象であり、人が関与している以上、完璧に防ぐことは難しいものです。そのため、予防的対策と併せて、被害が発生した際の対応フローの策定や、連絡先や相談先の確認も実施するよう、ご検討ください。

IPA では企業やその他の組織において必要な内部不正対策を効果的に実施可能とすることを目的として「組織における内部不正防止ガイドライン」[4]を公開していますのでご参考としてください。

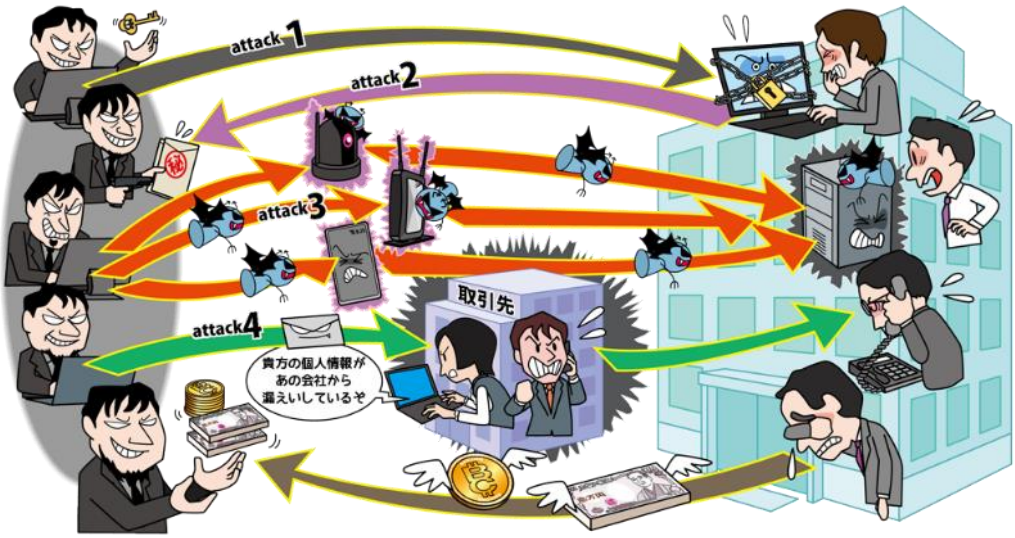
参考資料

1. 釜石市、職員 2 人を懲戒免職 - 全住民情報を持出、監査の不正操作も（Security NEXT）
https://www.security-next.com/136850
2. 宇部市 “私的に個人情報検索”職員を懲戒処分（NHK NEWS WEB）
https://www3.nhk.or.jp/lnews/yamaguchi/20221219/4060015683.html
3. 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
4. 内部犯行関連記事の一覧（Security NEXT）
https://www.security-next.com/category/cat191/cat25/cat173

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

～猛威を振るうランサムウェア。四重の脅迫で被害者を逃がさない～



ランサムウェアと呼ばれるウイルスに PC やサーバーが感染すると、端末のロックや、データの暗号化が行われ、その復旧と引き換えに金銭を要求される。さらに、暗号化だけではなく、重要な情報を窃取されることもあり、その情報を公開すると脅す。このように複数の脅しを組み合わせる（四重脅迫等）ことで、ランサムウェアに感染した組織が金銭を支払わざるを得ない状況を作り出そうとする。

＜攻撃者＞

- 組織的犯行グループ
- 犯罪者

＜被害者＞

- 組織
- 個人

＜脅威と影響＞

PC やサーバーのデータを暗号化し、業務の継続を困難にした上で、データを復旧することと引き換えに、金銭を要求する等の脅迫文を画面に表示するランサムウェアと呼ばれるウイルスの被害が確認されている。暗号化前に重要情報を窃取し、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「二重脅迫」も確認されている。脅迫に従うことによる金銭的被害に加え、窃取された重要情報（組織の機密情報や個人情報等）の漏えいにより信用の失墜にもつながるおそれがある。また、DDoS 攻撃（Distributed Denial of Service Attack：分散型サービス妨害攻撃）を仕掛ける、被害者の利害関係者等へ連絡するといった脅迫を加えた「四重脅迫」も確認されている。なお、金銭を支払ったとしても、データの復旧や漏えいした情報の削除が行われるとは限らない。

＜攻撃手口＞

◆ メールから感染させる

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

◆ ウェブサイトから感染させる

ウェブ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ウェブサイトや攻撃者が用意したウェブサイトを閲覧させることでランサムウェアに感染させる。

◆ 脆弱性を悪用しネットワークから感染させる

ソフトウェアや OS 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、その脆弱性を悪用してインターネット経由で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リモートデスクトッププポートに不正ログインしてランサムウェアに感染させる。

＜事例または傾向＞

◆ **脆弱性を悪用してランサムウェアを配置**

2022 年 3 月、東京コンピュータサービスは 2021 年末に発生したランサムウェアの被害の経緯等をまとめた資料を公開した。それによると、攻撃者は、社員向け AD（Active Directory）のパスワードの変更やリセット機能を提供するウェブサービスに、リバースプロキシサーバーを介して接続し、同 ウェブサービスの脆弱性を悪用して AD サーバーに侵入したという。そして、2021 年 10 月初旬から不正侵入を繰り返し行い、社内管理情報や顧客の情報等を窃取した。その後、同ウェブサービスの脆弱性を悪用して、ランサムウェアを自動的に配布するバッチファイルを配置し、12 月 31 日早朝、組み込まれたバッチファイルが自動実行され、組織内の機器がランサムウェアに感染した。[1]

◆ **リモートデスクトップ経由によるランサムウェア感染**

2022 年 6 月、ヴィアックスは同社の勤怠管理システムのサーバーがランサムウェアに感染し、従業員 1,871 人分、退職者 2,167 人分等の情報が暗号化されたことを公表した。データセンター内の DMZ（DeMilitarized Zone：非武装地帯）上にある勤怠管理システムのウェブサーバーがメンテナンス用に外部からリモートデスクトップ接続が可能となっており、ウェブサーバーへのパスワードの総当たり攻撃により不正侵入されたものとみられる。そして、ウェブサーバー上でランサムウェアを実行され、ウェブサーバーからアクセスできるサーバーのファイルが暗号化された。[2]

◆ **二重脅迫だけでなく、四重脅迫も横行**

2022 年 9 月、トレンドマイクロは法人組織における IT 部門の意思決定者を対象に調査した「ランサムウェア攻撃 グローバル実態調査 2022 年版」を公開した。調査結果では、過去 3 年間でランサムウェア攻撃の被害を受けたのは日本法人の 34.5%に及ぶ。脅迫はデータの暗号化、窃取情報の暴露、DDoS 攻撃予告、攻撃を受けていることの暴露といった内容である。これらを組み合わせて最大で四重の脅迫まで確認されている。被害を受けた組織の内、67.1%が 2 つ目の脅迫である窃取情報の暴露、74.3%が 4 つ目の脅迫である攻撃を受けている事の暴露に関する脅迫を受けたことが明らかになった。[3]

＜対策/対応＞

組織（経営者層）

- 組織としてのランサムウェア対応体制の確立
  - ・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 1.3「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
  - ・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 ※
  - ・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 [4]
  - ・インシデント対応体制を整備し対応する ※

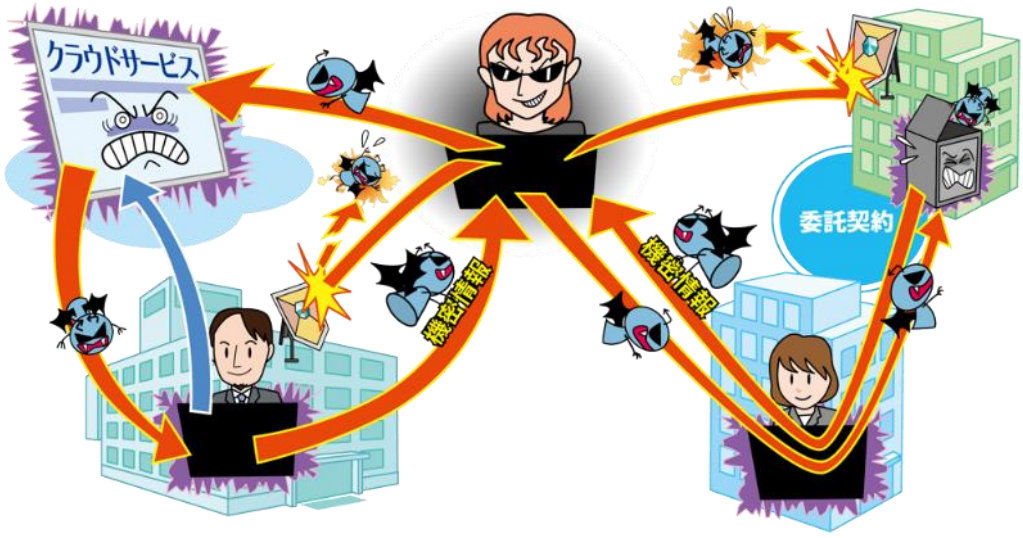
＜身代金の支払いと復旧業者の選定について＞

要求された身代金を支払ってもデータの復旧や情報の流出を防げるとは限りません。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、最終的に自組織が身代金を支払ったとみなされるおそれもあります。対応を依頼する業者の選定 [5] にも注意が必要です。

※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

～自組織だけでなく、委託先や利用しているサービスも適切な管理を～



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。攻撃者はそのサプライチェーンを悪用し、セキュリティ対策の強固な関連企業・サービス・ソフトウェア等は直接攻撃せずに、それ以外のセキュリティ対策が脆弱なプロセスを最初の標的とし、そこを踏み台として顧客や上流プロセスの関連企業等、本命の標的を攻撃する。また、もう1つのサプライチェーンとして「ソフトウェアサプライチェーン」もある。これは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（コード、ライブラリ、プラグイン、各種ツール等）や人（開発者、運用者等）の繋がりであり、ここを狙った攻撃も行われている。

＜攻撃者＞

- 組織的犯行グループ
- 犯罪者

＜被害者＞

- 組織（自組織とその商流に関わる他組織）

＜脅威と影響＞

組織には、何らかの形でサプライチェーンとの関係性が存在する。例えば、取引先や委託先、導入しているソフトウェア、利用しているサービスまでと多岐に渡たる。直接攻撃が困難な標的に対し、そのサプライチェーンの脆弱な部分を攻撃し、そこを経由して間接的および段階的に標的を狙う。外部に対しては強固なセキュリティ対策を行っている標的で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、攻撃者の侵入を許してしまうおそれがある。

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、取引先の組織においても、自組織が被害を受けるだけでなく、取引相手にも損害を与えてしまうことで、取引相手を失ったり、場合によっては、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**

標的の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、その組織が保有していた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）等を攻撃し、標的を攻撃するための足掛かりとする**

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。

また、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。

＜事例または傾向＞

◆ **協力企業の子会社へサイバー攻撃、国内全工場停止**

2022 年 3 月、トヨタ自動車が取引先のシステム障害により国内全工場を停止した。その後、取引先の小島プレス工業が公開した報告書によると、同社の子会社が外部の企業との専用通信を行うために利用していたリモート接続機器の脆弱性を悪用した不正アクセスが行われたとのこと。子会社の社内ネットワークへの侵入後に同社の社内ネットワークにも侵入され、サーバーや PC への攻撃の痕跡が確認された。この攻撃はランサムウェアによるものであり、一部のデータが暗号化されたが、データが持ち出された痕跡は確認されていないと公表している。[1,2]

◆ **利用しているサービスの改ざんにより情報漏えい**

2022 年 10 月、ショーケースは同社が提供するウェブフォームの入力をサポートする「フォームアシスト」等複数のサービスが改ざんされ、一部の取引先のウェブサイト等において入力された情報が外部へ流出したおそれがあることを公表した。

同年 7 月に取引先から指摘を受けて調査を行ったところ、対象サービスに対してシステムの脆弱性を悪用した第三者の不正アクセスがあり、ソースコードが書き換えられたことが判明した。

今回の改ざんにより、ユーキャンが運営する「生涯学習のユーキャン」、エービーシーマートが運営する「ABC-MART 公式オンラインストア」等の本サービスを利用する複数のサービスの利用者の個人情報が漏えいした。[3,4,5]

＜対策/対応＞

組織（自組織）

- 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。
  - ・インシデント対応体制を整備し対応する ※
  - ・信頼できる委託先、取引先、サービスの選定
    商流に関わる組織やサービスの信頼性評価や品質基準を導入し、定期的に監査を行う。
  - ・複数の取引先候補の検討
  - ・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の実施
  - ・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。
- 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

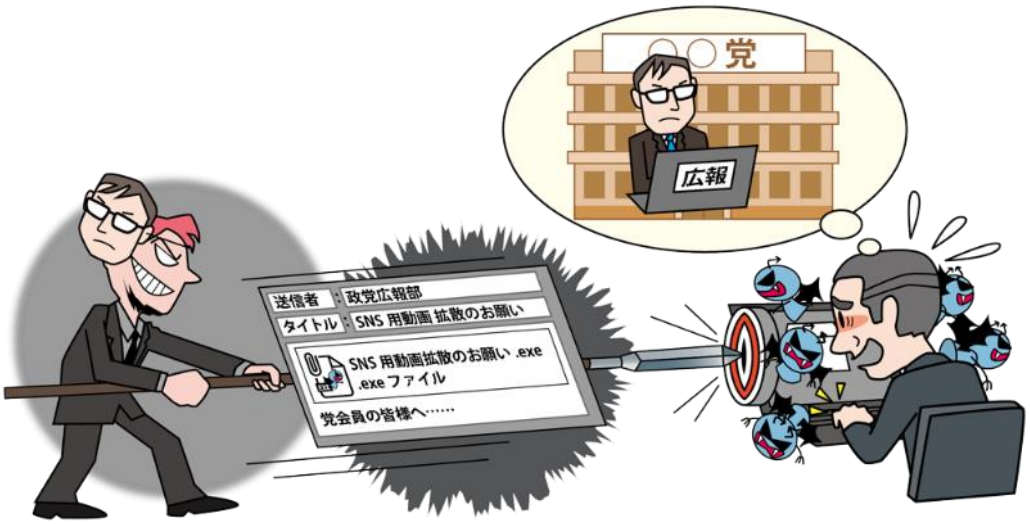
組織（自組織/自組織の商流に関わる組織共通）

- 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、ISMAP 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 [6,7,8]
- 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 標的型攻撃による機密情報の窃取

～メールが来たらまずは疑え！？意識は常に高く～



標的型攻撃とは、特定の組織（官公庁、民間団体、企業等）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、働き方の変化に便乗し、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＞

- 諜報員、産業スパイ
- 組織的犯行グループ
- 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に狙いを定め、機密情報等の窃取等を目的としたウイルスを PC やサーバーに感染させることで、組織内部へ潜入する標的型攻撃が確認されている。攻撃者はウイルスに感染させた PC やサーバーを悪用し、組織内部の侵害範囲を拡大しながら機密情報等の窃取等を行う。

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、業種や組織の規模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、不審を抱かれにくいようにする手口が使われる。（やり取り型攻撃）

◆ ウェブサイトの改ざん

標的となった組織が頻繁に利用するウェブサイトを調査し、そのウェブサイトを改ざんする。従業員や職員が改ざんされたウェブサイトにアクセスするよう誘導され、そのウェブ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

標的の組織が利用するクラウドサービスやウェブサーバー、VPN 等の脆弱性を悪用し、不正アクセスを行い、認証情報等を窃取する。その認証情報等を悪用し、正規の経路で組織のシステムへ侵

入して、PC やサーバーをウイルスに感染させる。

＜事例または傾向＞

◆ **業務に関連する精巧な文面を用いたシンクタンクへの標的型メール攻撃**

2022 年 9 月、警察庁は同年 6 月にシンクタンクへの標的型メール攻撃があったとして事例を公開した。シンクタンクの担当者が受信したメールには個人情報の圧縮ファイルが添付されており、データの代行登録を依頼するという、業務に関連したメール内容になっていた。[1] シンクタンクを狙った攻撃は NISC も注意喚起 [2] を行っており、IPA も政府関係機関とよく連携し対応するように求めている。[3]

◆ **日本の政治団体を狙ったスピアフィッシング**

2022 年 12 月、ESET Research は参議院選挙の直前である 6 月から 7 月にかけて標的型攻撃グループ「MirrorFace」によるスピアフィッシングキャンペーンが行われていたことを公開した。党会員に対して政党の広報部門からのメールを装い、参議院選挙に関する依頼が記載されていたり、著名な政治家を騙っていたりしたメールが送られていた。いずれのメールも悪意のあるファイルが添付されていた。添付されていたファイルを実行すると、「LODEINFO」と呼ばれるバックドア型ウイルスに感染する。その後、攻撃者から様々なコマンドを実行されてしまい、別のウイルスに感染させられたり、ネットワーク情報や認証情報、最終的には端末上に保存されているファイル等の情報を窃取されたりする。[4]

◆ **サイバー攻撃に関する情報共有**

2023 年 2 月、サイバー情報共有イニシアティブ（J-CSIP）は 2022 年に受け付けた標的型攻撃メールとみなした情報提供は 24 件であったことを公開した。また、7 月から 9 月の期間には標的型攻撃の被害に関する情報提供があった。レポートによると、サーバーのディスク使用率の閾値超過のアラートをきっかけに攻撃が発覚し、原因を調査したところ、不審なファイルを発見した。さらに調査を進めたところ、同じネットワーク内にあるグループ会社のサーバーから不正にアクセスされていたことが判明した。グループ会社のサーバーへの侵入経路や原因は不明だが、最も古い攻撃の痕跡が本事案発覚の 1 年半以上も前であり、長期に渡たって攻撃者からサーバーに不正アクセスされ、攻撃の準備や侵害範囲の拡大をされていた。[5]

＜対策/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
- 攻撃の予兆／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 ※

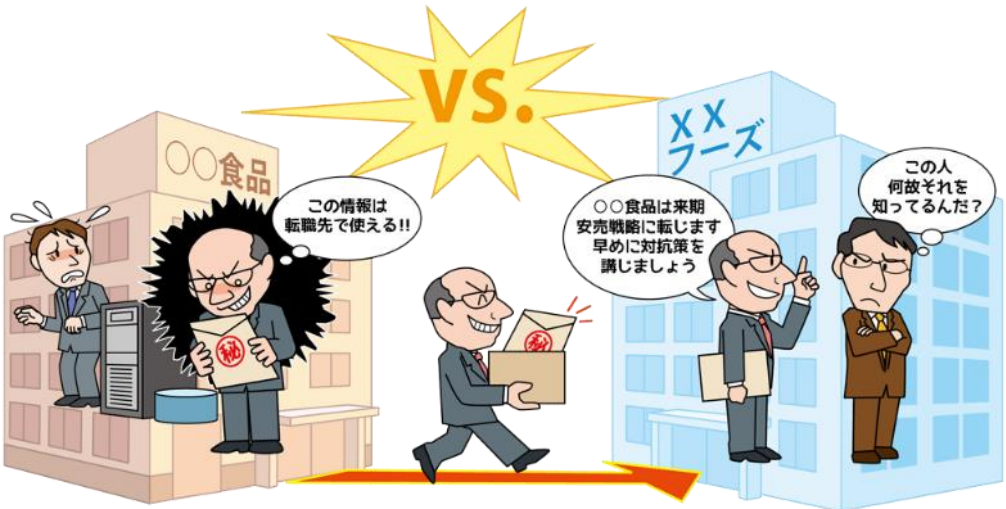
組織（従業員、職員）

- 被害の予防（通常、組織全体で実施）
  - ・表 1.3「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

4位 内部不正による情報漏えい

～不正に情報を取得しない、取得させない、使用しない！～



組織に勤務する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悪用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、損害賠償による経済的損失を与える。また、不正に取得した情報を他組織に持ち込んだ場合、その組織も損害賠償等の対象になるおそれがある。

＜攻撃者＞

- 組織の従業員（在職者、離職者）

＜被害者＞

- 組織
- 個人（顧客、サービス利用者）

＜脅威と影響＞

悪意を持った組織関係者が、組織が保管する技術情報や顧客情報等の重要情報を不正に持ち出し、不特定多数が閲覧できる場所に公開したり、競合他社へ有利に転職するために情報提供したりしたことで、情報が漏えいすることがある。これらの不正は金銭目的や私怨等で行われる。また、自宅で作業するためとして組織の情報管理の規則を守らず情報を外部へ持ち出し、それを紛失してしまい、情報漏えいにつながるケースもある。

漏えいした情報の重要性や規模によっては、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、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、持ち込まれた組織が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、組織の重要情報を窃取する。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窃取され、被害が大きくなるおそれがある。また、複数人で端末やアカウントを共用している場合、他人のアカウントに紐づくアクセス権限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、それを使用してアクセスし、組織の情報を窃取する。

◆　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＞

◆　**区職員が個人情報漏えいの疑いで逮捕**

2022 年 11 月、東京都杉並区が、区職員が住民基本台帳法違反容疑で逮捕されたことを公表した。住民基本台帳ネットワークシステムから得た情報を職員が外部に漏えいしている旨の文書が杉並区に送達されて発覚。当該システムの検索履歴の調査により同職員が検索を行っていたことが判明した。その後、警察による捜査の結果、逮捕に至った。[1]

◆　**市立高校で成績流出、内部犯行の可能性**

2022 年 7 月、市立函館高校に通う生徒 3 人の成績等の個人情報が Instagram に投稿され、約 90 人に閲覧されていたことが発覚した。何者かが教員の ID とパスワードを用いて生徒の成績等を管理している学習支援ソフトにアクセスし、情報を入手したとみられている。同校では、生徒用のタブレット端末で学習支援ソフトにアクセスしていたケースがあり、その端末では誰でも個人情報を閲覧できる状態になっていた。また、外部からの攻撃の形跡がなく、内部犯行の可能性が高いとしている。[2]

◆　**寿司チェーン社長、転職先に営業秘密持出し**

2022 年 9 月、カッパ・クリエイトの社長が不正競争防止法違反の疑いで警視庁に逮捕された。同社長は 2020 年 11 月にライバル企業からカッパ・クリエイトに転職しており、元部下を利用して商品原価等の営業秘密を持ち出していた。また、転職先の商品企画部長はデータを不正利用したとして、さらに転職元の元部下はデータのパスワードを漏えいしたとして共に逮捕されている。[3]

＜対策/対応＞[4]

組織（システム管理者）

- 被害の予防
  - ・基本方針の策定

    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。[5] 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 メモリーやスマートフォン等の記録媒体は利用制限を行い、持ち出し/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

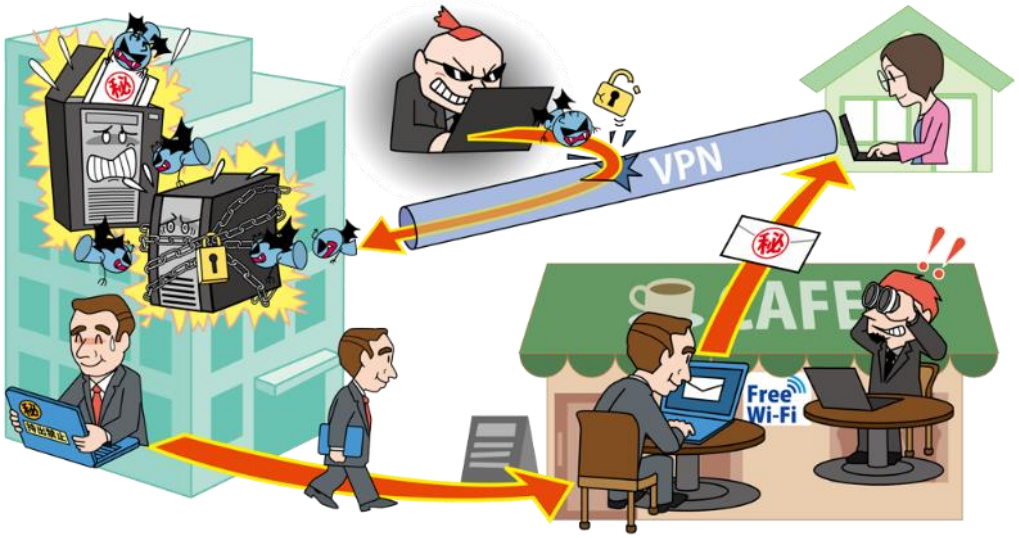
    従業員に対する教育を定期的に実施する。その際、従業員に秘密保持義務を課す誓約書を作成させることも重要である。
- 攻撃の予兆／被害の早期検知
  - ・システム操作履歴の監視

    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

5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

～未だ脆弱なテレワーク環境が狙われる～



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）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、ウェブ会議サービスや VPN 等の本格的な活用がされる中、それらを狙った攻撃が行われている。

＜攻撃者＞

- 組織的犯行グループ
- 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、ウェブ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。そのための私有端末（PC やスマートフォン等）や自宅のネットワークの利用も求められている。一方で攻撃者もこのような業務環境を引き続き狙っている。

業務環境に脆弱性があると、ウェブ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、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/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、ウェブ会議サービスの脆弱な設定を悪用し、ウェブ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＞

◆　リモート接続を狙ったランサムウェア攻撃

2022 年 6 月、国内の製造業者ニチリンの米国子会社がランサムウェア攻撃を受けた。外部からのリモート接続の設定の脆弱性を悪用して侵入されたと考えられ、管理者の認証情報を用いた攻撃者がサーバーにリモートアクセスツールをインストールしたり、ネットワークを調査した上でランサムウェアを展開したりした痕跡が残っていた。[1] このようなリモート接続の脆弱性を悪用してランサムウェア攻撃を行う手口が 2022 年も多く見られ、警察庁の調査によると 2022 年上半期における国内のランサムウェアの感染経路は VPN 機器からの侵入が 68%、リモートデスクトップからの侵入が 15%と 8 割以上がテレワークでも利用されるリモート接続の脆弱性に起因するものであった。[2]

◆　テレワークのセキュリティ実態調査

2022 年 2 月、IPA は 2020 年 11 月に行った「企業・組織におけるテレワークのセキュリティ実態調査」を再度実施した。委託元（IT ユーザ）239 社および委託先（IT ベンダ）269 社が回答し、そのうちテレワークを導入しているのは委託元が 64.9%（前回は 50.5%）、委託先が 97.0%（前回は 95.8%）となり前回より導入が進んでいた。

セキュリティ対策状況についてはテレワークに関する規則の見直し等改善した部分が見られる一方で、課題も多く残っていることが明らかとなった。特にテレワーク環境下で一時的に特例や例外による情報の持ち出しを認め、現在も認めている組織の割合は前回より増加する結果となった。書類や USB メモリー等、電子機器の持ち出しについては委託元が 19.4%（前回は 15.6%）、委託先が 8.4%（前回は 9.1%）、PC の持ち出しについては委託元が 24.5%（前回は 16.7%）、委託先が 14.6%（前回は 13.1%）となっており、前回と同程度またはそれ以上となっており、リスクが高い状況となっている。

また、規則の順守状況の確認については実施している組織の割合が委託元、委託先ともに増加していたものの、委託元については依然 35.5%が未実施となっており、確認方法についても委託元の 49.5%、委託先の 40.8%がセルフチェックのみに留まっていた。

その他にもテレワークを前提とした契約が進んでいない等、委託元を中心に未だテレワーク環境におけるセキュリティ対策に課題がある組織が多いことが明らかとなり、今後も脆弱なテレワーク環境を狙った攻撃へのリスクが懸念される。[3]

＜対策/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 1.3「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 ※
  - ・テレワークのセキュリティポリシーの策定

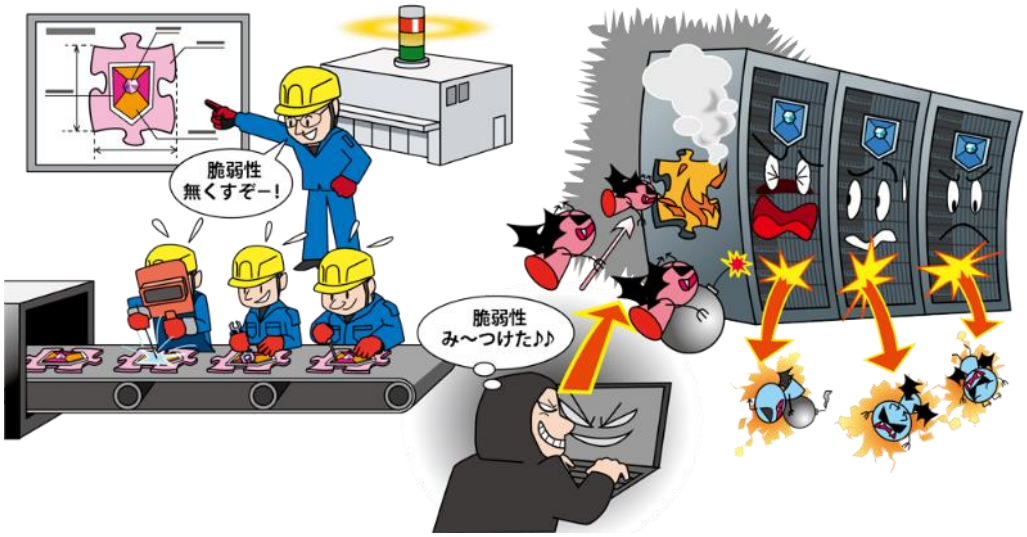
組織（セキュリティ担当者、システム管理者）

- 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とした運用を見直す。
  - ・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
- 攻撃の予兆／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 ※

※巻末「共通対策」を参照

6位 修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）

～事前に防ぐことは困難。悪用の情報が公表されたら即時対応を～



OS やソフトウェアに脆弱性が存在することが判明し、脆弱性の修正プログラム（パッチ）や回避策がベンダーから提供される前に、その脆弱性を悪用してサイバー攻撃が行われることがある。これをゼロデイ攻撃という。多くのシステムで利用されているソフトウェアに対してゼロデイ攻撃が行われると、社会が混乱に陥るおそれがある。

＜攻撃者＞

- 組織的犯行グループ

＜被害者＞

- 組織（開発ベンダー）
- 組織、個人（ソフトウェア利用者）

＜脅威と影響＞

ソフトウェアの開発ベンダー等が脆弱性を発見した場合、脆弱性の修正プログラム（パッチ）や回避策が公開されるが、それより先に攻撃者が脆弱性を発見した場合、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攻撃（ゼロデイ攻撃）が行われる。この場合に組織で事前にできる対策は限られており、確実に防ぐことは難しい。

ゼロデイ攻撃が成功すると、ウイルス感染や情報漏えい、さらにはウェブページやファイルの改ざん等の被害が発生し、事業やサービスが停止するおそれがある。広く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、被害が広範囲で発生するおそれがある。なお、この場合は、攻撃を受けたことに気付けても、開発ベンダー等から脆弱性対策情報が公開されていないため、適切な対応を取ることが難しい。

＜攻撃手口＞

◆ ソフトウェアの脆弱性を悪用

開発ベンダー等が修正プログラムを公開する前に、攻撃者がソフトウェアの脆弱性を悪用して攻撃する。攻撃方法は脆弱性の内容によって様々であり、その被害もウイルス感染や情報漏えい、改ざん等、様々である。

＜事例または傾向＞

◆ **Fortinet 製品 へのゼロデイ攻撃**

2022 年 12 月、Fortinet は FortiGate 等のセキュリティアプライアンス製品に OS として搭載されている FortiOS に、遠隔の第三者が認証を回避し、任意のコードやコマンドを実行する脆弱性があることを公表した。この脆弱性の影響はサポートが終了したバージョンにまで及んでいた。同社では本脆弱性を悪用する攻撃を確認しているとし、対策や緩和策だけでなく、脆弱性を悪用した攻撃のログや痕跡等の調査を推奨している。[3,4,5]

◆ **北朝鮮のサイバー犯罪グループによる Internet Explorer へのゼロデイ攻撃**

2022 年 12 月、Google の脅威分析グループ（TAG）は北朝鮮のサイバー犯罪グループが 10 月に Internet Explorer のゼロデイ脆弱性を悪用して攻撃していたことを公表した。10 月に起きた韓国の梨泰院雑踏事故について書かれた Office 文書がオンライン上にアップロードされており、ファイルを開くと任意のコードを実行されるおそれがあった。Internet Explorer は 6 月にサポート終了していたが、Microsoft Office では、Internet Explorer の機能を一部使っていたため、11 月に配信されたセキュリティ更新プログラムを適用していない場合に影響があった。Google TAG では、パッチの早急な適用と警戒を促している。[6]

◆ **Microsoft Exchange Server でゼロデイ攻撃が発生**

2022 年 9 月、ベトナムのセキュリティ企業の GTSC は、Microsoft Exchange Server の未修正の脆弱性を悪用する攻撃が発生していることをブログ記事で公表した。Zero Day Initiative を経由してマイクロソフトへも報告された。マイクロソフトはこの脆弱性に関する情報と緩和策を同月に MSRC のブログ記事で公開した。記事では脆弱性を悪用してユーザーのシステムに侵入する限定的な標的型攻撃を確認しているとし、11 月に修正プログラムがリリースされるまでは、同社が公開している暫定的な緩和策を実施するよう案内していた。[7,8]

＜対策/対応＞

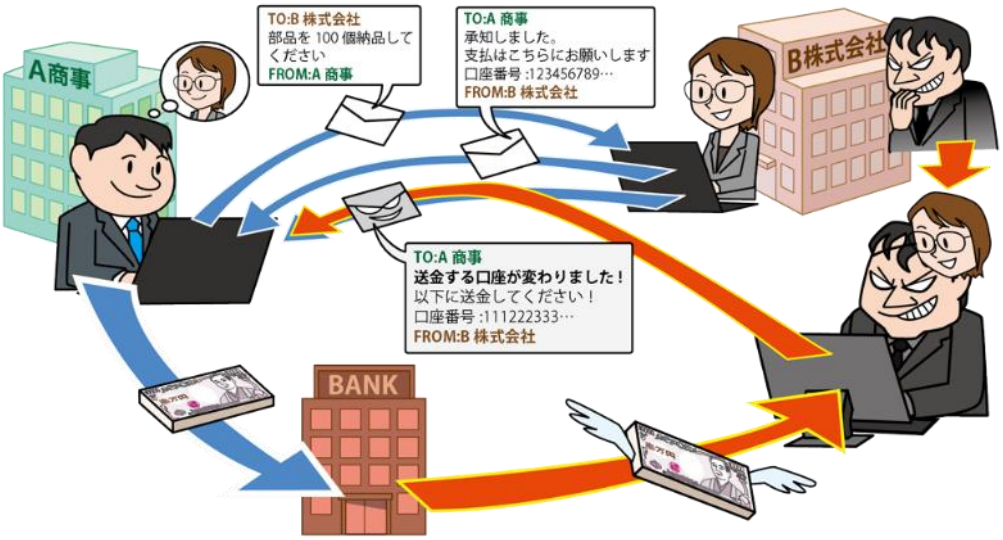
個人、組織（システム管理者）

- 被害の予防
  - ・表 1.3「情報セキュリティ対策の基本」を実施
  - ・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（パッチ）や回避策の提供が迅速である等の製品やベンダーを利用し、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 ※
- 攻撃の予兆／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

7位 ビジネスメール詐欺による金銭被害

～そのメール、相手が誰か分かりますか？～



ビジネスメール詐欺（Business E-mail Compromise：BEC）は、悪意のある第三者が取引先等になりすまして偽のメールを送ったり、組織間のメールのやり取りを乗っ取ったりした上で、最終的に偽の銀行口座に送金させるサイバー攻撃である。組織間取引の送金であることから被害額は大きくなる。

＜攻撃者＞

- 組織的犯行グループ

＜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＞

取引先や自社の経営者等を装い、偽のメールを組織の従業員へ送りつけ、攻撃者が用意した口座へ送金させ、金銭的な被害をもたらすビジネスメール詐欺が行われている。差出人（送信元）のメールアドレスに取引先を模したメールアドレスや取引先の本物のメールアドレスを使ったり、メール本文が自然な日本語であったり、本物のメールと見分けづらいようになっている。受信者が偽のメールを本物のメールとして取り扱ってしまうと、攻撃者が用意した口座に送金してしまうおそれがある。

＜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によって事前に盗み見て、取引や請求に関する情報や、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

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づきにくい。

◆　社外の権威ある第三者へのなりすまし

弁護士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＞

◆　**正規のメールアドレスを乗っ取った BEC**

2022 年 7 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 4 月に J-CSIP 参加組織に請求側企業の担当者になりすましたビジネスメール詐欺が行われていたことが報告された。攻撃者は請求側担当者のメールアドレスを乗っ取り、正規のメールアドレスで請求側の担当者のふりをして、支払側企業に入金先の口座を変更するように指示をした。しかし、指示されたメールに変更後の入金先を尋ねる返信をすると、口座の連絡までに時間がかかると連絡があったため、不審に思った支払側企業は関係者に通報し、一連のメールがビジネスメール詐欺であることが判明した。本件では、メールのやり取りの際、メールの Cc には請求側企業の関係者のメールアドレスに似せた偽のメールアドレスが指定されており、詐欺の発覚を避ける巧妙な手口が行われていた。[1]

◆　**偽メールに従い送金し…後日、詐欺発覚**

2022 年 11 月、人材育成を行うウィルソン・ラーニングワールドワイドは同年 9 月に子会社 2 社がビジネスメール詐欺の被害にあったことを公表した。子会社は悪意ある第三者より支払代金の送金を指示するメールを受け取り、2 社合わせて約 530 万円（USD 約 39,000）を送金した。送金後、詐欺である可能性に気付き、デジタルフォレンジック等による事実関係の確認、保険会社、捜査機関に対し相談等を行った。今回の件を受けて、2023 年 3 月期第 2 四半期の連結決算において特別損失を計上することになった。[2]

＜対策/対応＞

- 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
  - ・ビジネスメール詐欺への認識を深める[3]
  - ・ガバナンスが機能する業務フローの構築

    金銭が関係する処理は、個人の判断や業務命令だけでは完結しない規則やシステムの構築。
  - ・メールに依存しない業務フローの構築
  - ・メールに電子署名を付与（S/MIME や PGP）
  - ・DMARC を導入する

    SPF や DKIM を用いたメールのドメイン認証に失敗した際のメールの処理を判断できるようにする。

  ＜メールの真正性の確認＞
  - ・メールだけでなく複数の手段で事実確認

    振込先の口座変更等がある場合、電話等、メール以外の方法で取引先に確認する。また、口座の名義等を金融機関に確認する。[4]
  - ・普段とは異なるメールに注意

    普段とは異なる言い回しや、表現の誤り、送信元のメールドメインに注意する。
  - ・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。

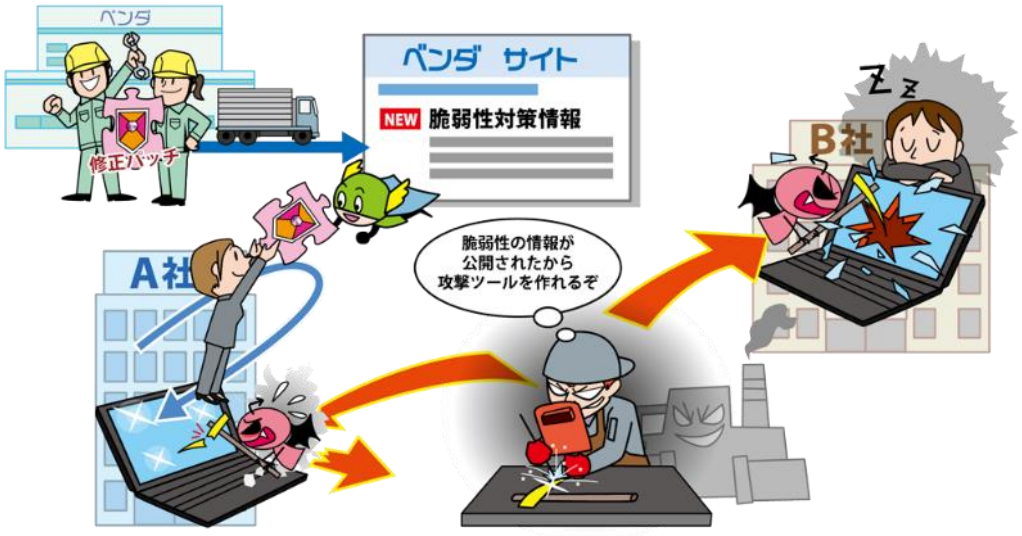
  ＜メールアカウントの適切な管理＞
  - ・パスワードを適切に運用する　※
- 被害を受けた後の対応
  - ・適切な報告/連絡/相談を行う　※
  - ・インシデント対応体制を整備し対応する　※
  - ・メールアカウントの設定を確認する

    攻撃者による不正な転送設定やフォルダー振り分け設定等を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

8位 脆弱性対策情報の公開に伴う悪用増加

～「後で対応しよう」、その数日が命取り～



ソフトウェアやハードウェア（機器類）の脆弱性対策情報の公開は、脆弱性の脅威や対策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、当該製品への脆弱性対策を講じていないシステムを狙って攻撃を行うことができる。近年では脆弱性関連情報の公開後に攻撃コードが流通し、攻撃が本格化するまでの時間も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、VPN 製品や CMS（プラグイン含む）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。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、ダークウェブ上のウェブサイト等で販売されたり、攻撃サービスとして提供されたりすることがある。また、だれ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＞

◆　**修正未実施の機器を狙った攻撃**

2022 年 5 月 4 日（米国時間）、F5 Networks は同社のネットワーク製品 BIG-IP に遠隔の第三者が認証を回避し、任意のコードの実行や不正な操作が可能となる脆弱性を公表した。その後 5 月 9 日にセキュリティベンダーから POC（実証コード）が公開され、その前後から修正パッチが適用されていない機器を探索する通信や脆弱性を悪用する試みが観測された。[1,2]

◆　**POC 公開済みの脆弱性を狙った攻撃**

2022 年 1 月にベンダーから修正パッチが公開されていた Oracle Fusion Middleware における遠隔の第三者が任意のコードを実行可能な脆弱性に対し、9 月頃から脆弱性を悪用する試みが観測されるようになった。同脆弱性については 3 月にセキュリティ研究者が POC（実証コード）を公開するとそれ以降も複数の POC が公開され、悪用されるリスクが高い状態であった。[3,4]

◆　**「Spring4Shell」を狙った攻撃**

2022 年 3 月 31 日（米国時間）、VMware から Java の Web アプリ開発を行うためのフレームワークである Spring Framework において、遠隔の第三者が任意のコードを実行可能な脆弱性が公表された。この脆弱性は 2021 年 12 月に公表され話題となった Apache Log4j の脆弱性の別名「Log4Shell」にちなんで「Spring4Shell」と名付けられた。悪用の試行を観測したセキュリティ企業によると、脆弱性公表時点で既に POC（実証コード）が公開されていたこともあり公表当日から悪用を試行する通信が観測され始め、4 月 3 日までの 4 日間で通信は最大 3 万 7,000 件にも上り全世界の約 16%の組織が影響を受けた。また、4 月上旬には当該脆弱性を悪用し、DDoS 攻撃等に使われるボットネットマルウェア「Mirai」の亜種による攻撃を行おうとする動きが確認されている。[5,6]

【補足】

Spring4Shell は脆弱性対策情報が公開される前の 3 月 29 日時点で Github に一時的に POC が公開されていたことを考えると、組織 6 位「修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）」の事例にもなり得るが、脆弱性対策情報の公開直後から攻撃が活発になった状況を踏まえ本脅威の事例として取り上げている。[7]

＜対策/対応＞

個人、組織（システム管理者／ソフトウェア利用者）

- 被害の予防
  - ・表 1.3「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、一時的にサーバー停止等を実施して、攻撃を回避する対策を取ることも検討する。
- 攻撃の予兆／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 ※

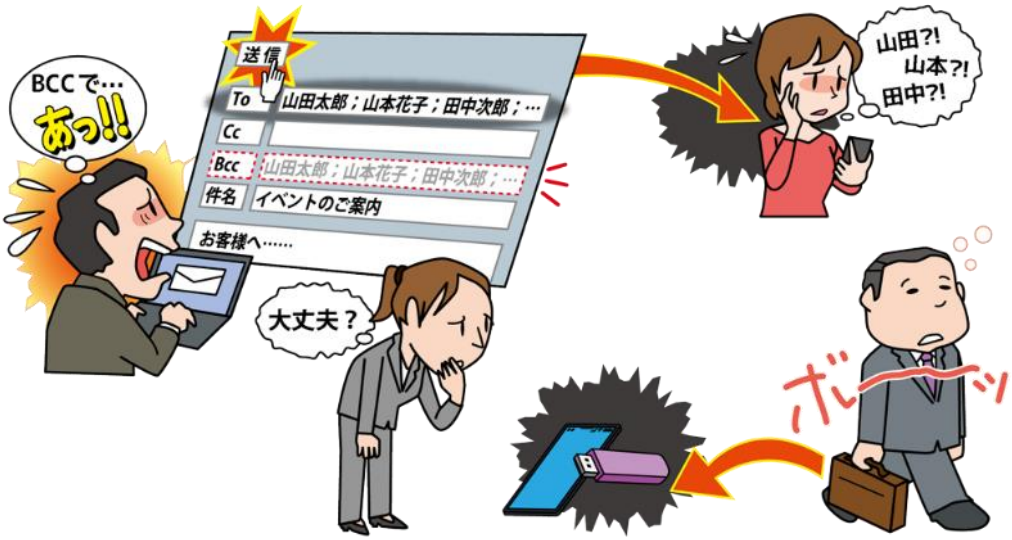
組織（開発ベンダー）

- 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

9位 不注意による情報漏えい等の被害

～1 つのうっかりが大事件につながることも…～



メールの誤送信や記録端末や記録媒体の紛失等の不注意による個人情報等の漏えいが発生している。漏えいした情報が第三者に売買されるとさらなる悪用につながるおそれもある。情報漏えいした組織は社会的信頼の失墜や経済的な損失につながるおそれもあり、組織はデータに対して慎重な扱いが求められる。

＜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取り扱うことがある。しかし、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、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害等の二次被害に繋がるおそれがある。また、社会的信用の失墜やそれに伴う経済的損失が発生する可能性がある。

＜要因＞

◆　取り扱い者の情報リテラシーの低さ

自身の扱う情報の機密性や重要性等を理解していないために、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間違いや重要情報が入った端末の紛失等。また、重要情報を私的に利用して外部のサイト等に公開することで情報漏えいにつながるケースもある。

◆　情報を取り扱う際の本人の状況

体調不良や多忙等、情報を取り扱う従業員が置かれた状況から注意力散漫になり、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。

◆　組織規程および取り扱いプロセスの不備

組織で制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メールアドレスの存在

第三者により組織が利用しているドメインと似たようなドメインのメールアドレスを準備されている。従業員が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例＞

- メールの誤送信（宛先間違い、To/Cc/Bcc の設定間違い、添付ファイル間違い等）
- 情報の不適切なウェブ公開（重要情報のマスキ

ング不備、公開ファイルや参照権限設定誤り、クラウドの設定誤り等）
- 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＞

◆ **Bcc を To に入れて送信**

2022 年 4 月、デジタル庁は新型コロナワクチン接種証明書アプリに関する問い合わせメールに返信する際、Bcc 欄に入れるはずだった 5 件のメールアドレスを To 欄に入れて送信してしまい、メールの受信者が他のメールアドレスを閲覧できる状態になってしまっていたことを公表した。原因は担当者が問い合わせ対応時にメールアドレスの貼り付け先を間違えたことによるものであった。デジタル庁は受信者に対して謝罪と該当メールの削除の依頼を行った。[1]

また、同月、デジタル庁は行政ポータルサイト e-Gov の運用委託先が問い合わせの回答対象とは別の人に対してメールを誤送信してしまった事案も公表し、再発防止に努めるとしている。[2]

◆ **個人情報の入った USB メモリーを紛失**

2022 年 6 月、兵庫県尼崎市は全市民の住民基本台帳の情報（46 万 517 人分）や住民税に関わる税情報（36 万 573 件）等が記録された USB メモリーを紛失したことを公表した。

尼崎市から業務を受託した企業の再々委託先の社員が、データ移管作業に必要なデータを USB メモリーに記録して持ち出した。データ移管作業が完了し、飲食店で食事や飲酒をした後、帰宅時に USB メモリーを入れていた鞄が無くなっていることに気がついて紛失が発覚した。当該 USB メモリーは、パスワードが設定され、内容については、暗号化処理が施されている状態であった。尼崎市は紛失の報告を受け、連携機関と調査を行い、個人情報の漏えいは無かったことを続報として公表している。[3]

◆ **クラウドのアクセス権限誤設定により、個人情報を漏えい**

2022 年 10 月、JTB が地域振興事業の補助金を申請した事業者等 1 万 1,483 人の個人情報を漏えいしたことを公表した。クラウドにログイン権限を持つ事業者のデータが相互に閲覧可能になっており、他の事業者の申請書をダウンロードできる状態になっていた。原因は情報共有に利用していたクラウドのアクセス権限を誤設定したことによるものであった。[4]

＜対策/対応＞

組織（当事者）

- 情報リテラシー、モラルを向上させる ※
  - ・組織規程および確認プロセスの確立
    特定の担当者への業務集中が発生しないような体制の構築も重要である。
  - ・組織規程および確認プロセスの見直し
    確立した規程やプロセスが適切に運用できているか定期的に見直す。
- 被害の予防（被害に備えた対策含む）
  - ・確認プロセスに基づく運用
  - ・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したり、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
- 攻撃の予兆／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

10位 犯罪のビジネス化（アンダーグラウンドサービス）

～攻撃者もショッピング。商品はあなたの情報～

犯罪に使用するためのサービスやツール、ID やパスワードの情報等がアンダーグラウンド市場で取り引きされ、これらを悪用した攻撃が行われている。攻撃に対する専門知識が無い者でもサービスやツールを利用することで、容易に攻撃を行えるため、サービスやツールが公開されると被害が広がるおそれがある。

＜攻撃者＞

- 組織的犯行グループ
- 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引されている。攻撃者は、IT に関する高度な知識がなくても、これらを購入して、容易にサイバー攻撃を行うことができる。アンダーグラウンドで商用化されたツールやサービスとして、例えば、エクスプロイトキットやオンライン銀行詐欺ツール、DDoS（分散型サービス妨害）攻撃代行サービスや RaaS（Ransomware 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、業務を妨害される。

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

＜攻撃手口＞

◆ ツールやサービスを購入し攻撃

アンダーグラウンドで購入したサービスやツールを利用して攻撃を行う。脆弱性の悪用やボットネットの利用等、ツールやサービスの種類によって攻撃方法は異なる。

◆ 認証情報を購入し攻撃

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

◆ サイバー犯罪に加担する人材のリクルート

サイバー犯罪は個人だけでなく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で高額な報酬を提示することでリクルートする。新型コロナウイルスの蔓延後にはこうした書き込みが 4 倍に増加し、IT 技術者の取り込みが図られている。[1]

＜事例または傾向＞

◆　**窃取した個人情報をダークウェブで売買**

2022 年 1 月、NHK のテレビ番組「クローズアップ現代」によると、フィッシング等で窃取された個人情報がブラックマーケットで売買され、悪用されているとのこと。大手ショッピングサイトのアカウント情報も売買されており、日本人の情報も多く含まれている。売買されている個人情報にはアカウント情報だけでなく、セキュリティコードもセットとなったクレジットカード情報、免許証や保険証の情報、パスポートの画像等、フィッシングだけでなく企業から不正に窃取したとみられる情報も含まれている。[1]

◆　**不正アクセス用データをダークウェブで売買**

2022 年 6 月、カスペルスキーは 2 つのダークウェブ上で企業のネットワークに不正アクセスするための情報を販売する約 200 件の投稿を分析した結果を公開した。それによると、分析対象の 75%がリモートデスクトップへのアクセス情報の販売であった。また、販売価格にばらつきがあり、業種や事業を行っている地域により変動し、対象の企業の収益の多いほどに情報の販売価格も上昇していた。[2]

◆　**パチンコホール事業者へサイバー攻撃、個人情報がダークウェブに流出**

2022 年 9 月、パチンコホール事業を展開するダイナムジャパンホールディングスは個人情報の流出を確認したことを公表した。同社のサーバーがランサムウェアによる攻撃を受け、データの暗号化をされ、この際のアラートで被害が発覚した。グループ会社が運営する店舗の地権者の氏名や口座情報等 2042 件や、入金情報 172 件、取引先に関する名刺情報や証券口座情報 1218 件等が流出していた。流出した情報はいずれもダークウェブ上で公開されている事も確認された [3]

＜対策/対応＞

攻撃に悪用するツールやサービスの目的・仕様によって対策は異なる。そのため、以下には代表的な対策を記載している。より具体的な対策については、本書に記載されている他の脅威の項も合わせて確認してほしい。

組織（経営者層）

- 組織としての体制の確立
  - ・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）や CDN（コンテンツデリバリーネットワーク）等のサービスを利用する
  - ・システムの冗長化等の軽減策
  - ・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　※
  - ・通信制御（DDoS 攻撃元をブロック等）
  - ・ウェブサイト停止時の代替サーバーの用意と告知手段の整備
  - ・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
  - ・ダークウェブの監視

    自組織情報流出の有無を確認する。
- 被害を受けた後の対策
  - ・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　※

※巻末「共通対策」を参照

コラム：医療機関におけるランサムウェア被害の増加

警察庁が 2022 年 9 月に公表した「令和4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」によると、国内のランサムウェアによる被害件数は、2021 年には 146 件、2022 年は上半期で 114 件となっており、増加傾向にあります。また、感染経路としては VPN 機器やリモートデスクトップからの侵入が大半を占めており、テレワークなどで利用されるネットワーク機器の脆弱性を利用して、ランサムウェアに感染させるケースが増えています。

ランサムウェアの被害は業種や企業規模を問わず広範囲に及びますが、2021 年に 7 件であった医療機関の被害が、2022 年は 20 件であり、3 倍弱と過去最多となっています。[1]

近年では、以下のような事例がメディアで取りあげられました。

■2021 年 10 月 31 日：徳島県つるぎ町立半田病院 [2]

電子カルテをはじめとする院内システムがランサムウェアに感染し、カルテが閲覧できなくなるなどの大きな被害が生じました。2022 年 1 月までのおよそ 2 か月間、治療行為を含む正常な病院業務が滞ったとされています。

調査報告書によると、侵入経路としては VPN 機器の管理者の資格情報がダークウェブで公開されていた事実などから、電子カルテなどの医療システムのメンテナンスの際に接続する VPN 機器の脆弱性を悪用された可能性が高いと報告されています。

■2022 年 6 月 19 日：徳島県鳴門山上病院 [3,4,5]

ランサムウェアによるシステムへの侵入被害を受け、電子カルテ、院内システムが使用不能になり、新規患者の受け付けを停止しました。その後、バックアップデータからシステムを復旧させ、6 月 22 日から新規患者の受け付けを再開しています。

なお、徳島県から公表されている危機管理連絡会議の協議概要によると、2021 年の半田病院の事案を受けた対応として、県立病院ではシステムの脆弱性把握や、外部から病院システムへのアクセス経路の VPN 統合、振る舞い検知機能をもったアンチウイルス製品の導入などを行ったとあり、2022 年度もバックアップ対策などのセキュリティ体制の整備を進めているところと報告されています。

■2022 年 10 月 31 日：大阪府立病院機構 大阪急性期・総合医療センター[6,7,8]

ランサムウェアと思われる攻撃により、電子カルテシステムに障害が発生し、緊急以外の手術や外来診療の一時停止など通常診療ができない状況に陥りました。

病院からの公表によると、2022 年 12 月 12 日に電子カルテシステムを含む基幹システムが再稼働し、2023 年 1 月 11 日から従来どおりの診療を再開しています。

また、復旧にあたっては全てのサーバーと端末を初期化し、再インストールすることで対応したと報告されています。

たとえ一定レベルのセキュリティ対策を設けていたとしても、攻撃グループの標的とされた場合、ランサムウェアなどの不正ソフトウェアの侵入を全て防ぐのは困難であることが読み取れます。

厚生労働省が策定した「医療情報システムの安全管理に関するガイドライン」では、医療情報システムで実施すべき不正ソフトウェア対策として、以下のものが挙げられています。[9]

・不正ソフトウェアのスキャン用ソフトウェアの導入
・脆弱性が報告されているソフトウェアへのパッチ適用
・利用していないサービスやポートの非活性化、マクロの利用停止、メールやファイルの無害化
・EDR（Endpoint Detection and Response）や「振る舞い検知」などの導入

上記に加えて、災害およびサイバー攻撃など非常時の対応として、事業継続計画（BCP）を作成し、想定されるあらゆるレベルの異常時について、対策を立て、文書化し、訓練を繰り返すことが有用であるとされています。半田病院の事例でも、災害を主として作成、運用していた事業継続計画があり、それによってインシデント対応に円滑に入ることができたと調査報告書で述べています。

これら対策を限られたリソースで満たすのは難しいとは言え、同様の事案が自院にいつ起きても不思議ではありません。事業を脅かすことが起き得るという教訓としていただければと思います。

国や組織による取り組みも行われています。経済産業省・総務省では、IT サービス事業者が対応すべきガイドラインとして「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」[10] を策定しています。IT サービス事業者からも、ガイドラインに準拠したサービスが提供されており、国内での導入事例も紹介されています。[11,12]

また、一般社団法人医療 ISAC では医療機関へのアンケートを実施し、医療という公的インフラに対しセキュリティ予算を公的に補助すること、病院・IT 事業者が一体となり医療システムを守るという観点でガイドラインを見直すこと、などの提言がされています。[13]

ランサムウェア攻撃に対して、一医療機関としてだけではなく、国や事業者とともに取り組み、一丸となって対策を行っていくことが重要と考えられます。

参考資料

1.令和4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/R04_cyber_jousei.pdf
2.徳島県つるぎ町立半田病院 コンピュータウイルス感染事案有識者会議調査報告書について（つるぎ町立半田病院）
https://www.handa-hospital.jp/topics/2022/0616/index.html
3.令和 4 年 6 月 20 日　サイバー攻撃による被害について（第 1 報）（鳴門山上病院）
https://kyujinkai-mc.or.jp/info/20220620/
4.令和 4 年 6 月 21 日　サイバー攻撃による被害について(第 2 報)（鳴門山上病院）
https://kyujinkai-mc.or.jp/info/20220621/
5.危機管理連絡会議の開催結果について（徳島県）
https://anshin.pref.tokushima.jp/docs/2022062000017/files/kekka.pdf
6.「電子カルテシステム」の障害発生について（大阪急性期・総合医療センター）
https://www.gh.opho.jp/pdf/info20221031.pdf
7.通常の外来診療の再開について（第8報）（大阪急性期・総合医療センター）
https://www.gh.opho.jp/pdf/info20221222.pdf
8.診療体制の復旧について（第9報）（大阪急性期・総合医療センター）
https://www.gh.opho.jp/pdf/info20230110.pdf
9.医療情報システムの安全管理に関するガイドライン　第 5.2 版（令和 4 年 3 月）（厚生労働省）
https://www.mhlw.go.jp/stf/shingi/0000516275_00002.html
10.医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン（経済産業省）
https://www.meti.go.jp/policy/mono_info_service/healthcare/teikyoujigyousyagl.html
11.Microsoft Cloud for Healthcare（Microsoft）
https://www.microsoft.com/ja-jp/industry/health/microsoft-cloud-for-healthcare
12.日本の医療情報ガイドライン（Amazon.com）
https://aws.amazon.com/jp/compliance/medical-information-guidelines/
13.四病院団体協議会セキュリティアンケート調査結果（（一社）医療 ISAC）
https://m-isac.jp/2022/04/02/report01-3/

「情報セキュリティ対策の基本」
と
「共通対策」

①情報セキュリティ対策の基本

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、攻撃者が利用する「攻撃の糸口」は似通っており、脆弱性を悪用する、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 1.3 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、被害に遭うリスク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 ※「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 1.4 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

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

②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 1.5 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。

表 1.5 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 [1]

個人や組織に関わらずパスワードの設定はオンラインショッピングやネットワークカメラ（見守りカメラ）等の様々な場面で必要になる。安易な設定や不適切な扱いをすると、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 機器では初期設定のパスワードは共通して使わ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

推測されにくくするためには長く複雑にする事が有効である。内閣サイバーセキュリティセンター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 [2] 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

②生年月日や名前を使わない

③連続した数字やアルファベットにしない

④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 ID が登録したメールアドレスにな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、どこかで漏れ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設定時は参考にするとよい。[3]

- 適切な保管、運用を行う

・パスワードは他人に教えない

・ID とパスワードをセットで保管しない

例えば ID とパスワードのメモを端末に貼り付けていると、紛失した際に簡単に不正ログインされてしまう。どうしても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。

・スマホや PC にパスワードのメモを貼らない

・複数人で使用する端末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端末では、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。

参考資料

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. 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
3. 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

意図せず情報モラルに反する事を行ったり、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への影響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者は気を付けるべき事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 やスマホを使う子へ、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】

①SNS 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。

・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。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ぶ)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

・本物に似せた偽のウェブサイトがある

・個人情報を盗もうとするウェブサイトがある

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組織の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組織の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。[1,2,3,4]

③教育受講時の心得

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

・事故を起こさない事は自分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、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。

また、毎回同じ教育コンテンツではなく運用状況を確認し、コンテンツを見直すことも必要である。

参考資料

【個人、組織共通】

1. 情報セキュリティ教材(IPA)
https://www.ipa.go.jp/security/net-anzen/index.html

【個人】

2. サイバーセキュリティのひみつ(IPA)
https://www.ipa.go.jp/security/security-himitsu/

【組織】

3. 対策のしおり(IPA)
https://www.ipa.go.jp/security/guide/shiori.html
4. 講習能力養成セミナー(IPA)
https://www.ipa.go.jp/security/sme/seminar.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]

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を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、端末がウイルス感染したりすることはない。そのメールや SMS から誘導されたウェブサイトに情報を入力することで入力した情報が盗まれ、添付ファイルを開くことでウイルス感染してしまう。

ウイルスに感染すると端末に保存されている情報が盗まれたり、端末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

悪意があるメールや SMS、SNS で受信したメッセージ内のリンクをクリックやタップして開く、または URL をブラウザに入力して開いたウェブサイトは正規のウェブサイトを模倣した偽のウェブサイトであるおそれがある。

・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ウェブ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。

さらに、万が一 Microsoft Word や Excel を開いてしまった際は「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る。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ため、安易にクリックやタップをしてはいけない。

● 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を疑い以下のようにして確認するとよい。

①あらかじめブックマーク（お気に入り）しておく

よく利用しているウェブ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ウェブページを検索して開き、確認する

対象のサービスをブラウザで検索して正規のウェブページを開く。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、是非以下のウェブページで手口を確認し、不審なメールや SMS に備えてほしい。

参考資料

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

■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、以下の相談先に相談してほしい。

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 不審なウェブサイトを見つけた 不審なウェブサイトに個人情報や金銭情報を入力してしまった	①信頼できる知人 ②日本データ通信協会（迷惑メール相談センター） (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、不審なウェブ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都道府県警察のフィッシング報告専用窓口一覧 (https://www.npa.go.jp/bureau/cyber/countermeasures/phishing.html#contact) ⑥フィッシング対策協議会 (https://www.antiphishing.jp/registration.html)
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警察
クレジットカードを勝手に使われた インターネットバンキングで不正送金された ※③以下に連絡 電子決済を勝手に使われた	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警察
PC やスマホ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/index.html)
自分のアカウントに勝手にログインされた	①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（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/bullying/) ③誹謗・中傷が掲載されているウェブサイトや SNS の提供会社 ④警察や弁護士
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/index.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】

組織においては適切に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隠蔽したとされ、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してほしい。

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端末や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	従業員としての対応だけでなく、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ておくことが重要である。 ①組織内の関連部署へ横展開する ②組織外への情報発信を検討、判断する
経営者や組織として	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警察へ被害届を提出する ⑤監督省庁、IPA、JPCERT/CC、個人情報保護委員会に報告する ※発生したインシデントに併せて公的機関等に報告する ⑥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物になる。特に、サイバー攻撃を受けた際はより迅速な対応が必要になってきている。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を解説するので、自組織における対策準備の参考としてほしい。

● 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

インシデント対応は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連絡先や対応フローを確立し、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、予算の確保を行う

● インシデント対応として CSIRT が行うべき事

①検知/連絡受付

セキュリティ機器での検知や組織の外部や組織内の人間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が必要な場合や情報共有をすべき場合は注意喚起や情報発信を行う。

③インシデントレスポンス

インシデントの事象を分析し、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推進し、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、監督官庁への報告を行う。

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]

参考資料

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. 付録 C サイバーセキュリティインシデントに備えるための参考情報（経済産業省）
https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_app_C_for_3.0.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 [1.2]

組織に対する脅威はサーバーやクライアント、ネットワークが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、攻撃者からは今後も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「更新プログラム適用」1 つを見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。

● 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

・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。

また、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

仮想パッチとは、直接的にソフトウェアの脆弱性を解決せずに、ネットワークレベルで攻撃の通信を遮断することである。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物であり、迅速な適用は難しいという問題を解決するための手法である。なお、根本的な問題を解決できるわけではない、あくまで暫定対策であることに注意が必要である。

・提供元不明のソフトウェアを利用しない

・不要なサービスを停止または無効化する

停止するだけでなく、自動起動が有効になっていないことも確認しないと、サーバー再起動により起動されてしまうので確認する必要がある。

● 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 の面以外の対策も行う。例えば、運用担当者の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等、運用手順の面での対策も有効である。

・定期的にアカウントの棚卸を行う

・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

「共通対策」内、別項を参照

● 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。アンチウイルスに関しては特に、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できる。

・NDR(Network Detection and Response)

ネットワークトラフィック（通信量）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。

・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。

・WAF (Web Application Firewall)

ウェブサーバーの前面またはウェブ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できる。

● ネットワーク

・ネットワークを分離し、個別遮断できるようにする

・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を許可するのか必要最小限にする。

・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。

・不要なポートを閉じる

● 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構築、暗号化等が可能である。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メリットは大きいといえるツールである。

・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

・セキュリティ診断を行う

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

・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、取得レベルや保管期間については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 ではウェブサーバーや 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[3]）を無料で提供しているので利用を検討するとよい。

参考資料

1. サイバーセキュリティ経営ガイドライン付録B（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（総務省）
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/index.html
3. 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

■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による暗号化だけではなく、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縮小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(3-2-1-1-0 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。

・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センター内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もあるためである。

また、バックアップにはいつ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た上書きや消去してしまうといった事故を防ぐ。

・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

普段使用する端末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端末は接続せずに保管する。

参考資料

1. Data Backup Options（アメリカ合衆国サイバーセキュリティ・社会基盤安全保障庁）
https://www.cisa.gov/uscert/sites/default/files/publications/data_backup_options.pdf

参考資料

【個人】

・1 位「フィッシングによる個人情報等の詐取」

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. 「これ詐欺だったの？」――「えきねっと」をかたるメール、手口の巧妙さが話題に “自動退会処理”に注意（ITmedia NEWS）
   https://www.itmedia.co.jp/news/articles/2203/07/news095.html
3. 不審なショートメッセージやメールにご注意ください（国税庁）
   https://www.e-tax.nta.go.jp/topics/topics_20220815.htm
4. 国税庁をかたるフィッシング (2022/09/20)（フィッシング対策協議会）
   https://www.antiphishing.jp/news/alert/nta_20220920.html
5. 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
6. 2022/07 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/202207.html
7. 2022/12 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/202212.html
8. 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/consumer_antiphishing_guideline_2022.pdf

・2 位「ネット上の誹謗・中傷・デマ」

1. ベネッセに風評被害 「教材に反ワクチンのチラシを封入」デマ対応に追われる（ITmedia NEWS）
   https://www.itmedia.co.jp/news/articles/2203/23/news085.html
2. 反ワクチンチラシ「チャレンジに入ってた」デマ投稿が話題に、偽計業務妨害罪の可能性も（弁護士ドットコムニュース）
   https://www.bengo4.com/c_23/n_14277/
3. SNS デマ投稿の女に有罪判決 「コンビニ店長がコロナ感染」名誉棄損（京都新聞）
   https://www.kyoto-np.co.jp/articles/-/901904
4. デマ投稿5人の賠償増額 東名あおり事故 福岡高裁（産経新聞）
   https://www.sankei.com/article/20221027-ODQDEYMWLVMNNOCAOTI72GJJEQ/
5. サッカーW 杯、伊藤洋輝の SNS に批判殺到 本田圭佑氏「安易な批判はやめるべき」と擁護（東京新聞）
   https://www.tokyo-np.co.jp/article/217002
6. 選手を誹謗中傷から保護 W杯中にSNSを監視―FIFA（時事通信社）
   https://www.jiji.com/jc/article?k=2022111700261&g=spo
7. 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

・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」

1. 【2022/8/11 9:20】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/2022/08/20220811scammail.html
2. 自称ロシア人宇宙飛行士に440万円だまし取られる ロマンス詐欺か（朝日新聞）
   https://www.asahi.com/articles/ASQB95TH6QB7PTJB00J.html
3. 国際ロマンス詐欺増加、外国人名乗りSNSで甘言（中日新聞）
   https://www.chunichi.co.jp/article/573151?rct=shiga
4. ウクライナ情勢を悪用した手口にご注意！－SNSでの義援金詐欺－（国民生活センター）
   https://www.kokusen.go.jp/news/data/n-20220325_1.html
5. ウクライナ情勢を悪用した手口にご注意！（No.3）－送金依頼や書籍の強引な販売トラブル等－
   https://www.kokusen.go.jp/news/data/n-20220627_1.html

・4 位「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. お知らせ（株式会社 machatt）
   https://machatt.jp/support/information/20220518.html
3. 【スイーツパラダイス オンラインショップ】不正アクセスによる個人情報漏えいの可能性のあるお客様へのお詫びとお知らせ（井上商事株式会社）
   https://www.sweets-paradise.jp/news/%25news_cat%25/2022/06
4. クレジットカード不正利用被害の集計結果について（一般社会法人日本クレジット協会）
   https://www.j-credit.or.jp/download/news20220930c1.pdf

・5 位「スマホ決済の不正利用」

1. 他人のメルペイに接続、中国人グループが2300万円不正購入か…中国で転売（読売新聞オンライン）
   https://www.yomiuri.co.jp/national/20220526-OYT1T50124/
2. 「au PAY」アカウント不正使用で詐欺の罪　被告無罪主張（関西　NEWS WEB）
   https://www3.nhk.or.jp/kansai-news/20220916/2000066361.html

・6 位「不正アプリによるスマートフォン利用者への被害」

1. 国内で脅迫被害、マッチングアプリを装うモバイル不正アプリ（トレンドマイクロ株式会社）
   https://www.trendmicro.com/ja_jp/research/22/c/malicious-app-disguised-dating-app.html
2. 「Facebookでログイン」でパスワード盗むアプリ、100万人以上被害（ITmedia）
   https://www.itmedia.co.jp/news/articles/2210/08/news049.html
3. 2022/08 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/202208.html
4. 2022/09 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/202209.html

・7 位「偽警告によるインターネット詐欺」

1. 「スパイウェアに感染」PC から偽の警告と音声が…遠隔操作で乗っ取る「サポート詐欺」 嘉手納署が注意喚起 （琉球新報 DIGITAL）
   https://ryukyushimpo.jp/news/entry-1563486.html
2. 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
3. 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/anshin/reports/2021q4outline.html
4. 安心相談窓口だより「偽セキュリティ警告（サポート詐欺）の月間相談件数が過去最高に」（IPA）
   https://www.ipa.go.jp/security/anshin/attention/2022/mgdayori20230228.html
5. そのセキュリティ警告画面・警告音は偽物です！「サポート詐欺」にご注意！！（独立行政法人国民生活センター）
   https://www.kokusen.go.jp/news/data/n-20220224_2.html
6. 情報セキュリティ安心相談窓口（IPA）
   https://www.ipa.go.jp/security/anshin/index.html
7. 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
8. 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/attention/2020/mgdayori20200330.html

・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」

1. 不正アクセスによるお客さま情報漏えいに関するお詫びとご報告（08.23 追記）（株式会社 SODA）
   https://snkrdunk.com/information/130/
2. 【重要】個人情報漏洩に関するお詫びとお知らせについて（出光クレジット株式会社）
   https://www.idemitsucard.com/important/information2210-02.html
3. サンドラッグ　e-shop　本店及びサンドラッグお客様サイトへの不正ログインについてのお詫びとお知らせ（株式会社サンドラッグ）
   https://contents.xj-storage.jp/xcontents/99890/ee3648ea/747e/4df2/b2eb/b139a2d300bd/140120220712598541.pdf

・9 位「インターネット上のサービスへの不正ログイン」

1. ニトリ、不正アクセスで 13 万 2000 件の個人情報流出か　リスト型攻撃で（ITmedia NEWS）
   https://www.itmedia.co.jp/news/articles/2209/21/news213.html
2. にじさんじ、VTuber の TikTok 乗っ取り相次ぐ　伏見ガク、夢追翔など（ITmedia NEWS）
   https://www.itmedia.co.jp/news/articles/2206/29/news094.html
3. にじさんじの VTuber 多数が TikTok の乗っ取り被害に（yutura）
   https://yutura.net/news/archives/77843
4. 熊本県立大学メールアカウントの不正利用事案の発生について（熊本県立大学）
   https://www.pu-kumamoto.ac.jp/sys/wp-content/uploads/2022/12/PR_20221213.pdf

・10 位「ワンクリック請求等の不当請求による金銭被害」

1. 安心相談窓口だより「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
2. 10 代の金銭感覚についての意識調査 2022（SMBCコンシューマーファイナンス株式会社）
   https://www.smbc-cf.com/news/news_20220825_1028.html

【組織】

・1 位「ランサムウェアによる被害」

1. ランサム感染で顧客情報の流出を確認 - ソフトウェア開発会社（Security NEXT）
   https://www.security-next.com/135115
2. 勤怠管理システムサーバに対する攻撃について（株式会社ヴィアックス）
   https://www.viax.co.jp/pdf/20220601.pdf
3. 「ランサムウェア攻撃 グローバル実態調査 2022年版」を発表（トレンドマイクロ株式会社）
   https://www.trendmicro.com/ja_jp/about/press-release/2022/pr-20220907-01.html
4. The No More Ransom Project（No More Ransomプロジェクト）
   https://www.nomoreransom.org/
5. 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. システム停止事案調査報告書（第 1 報）（小島プレス工業株式会社）
   https://www.kojima-tns.co.jp/wp-content/uploads/2022/03/20220331_システム障害調査報告書（第1報）.pdf
2. トヨタ、国内全工場を停止へ 部品会社にサイバー攻撃（日本経済新聞）
   https://www.nikkei.com/article/DGXZQOFD289MK0Y2A220C2000000/?unlock=1
3. 不正アクセスに関するお知らせとお詫び（株式会社ショーケース）
   https://www.showcase-tv.com/pressrelease/202210-fa-info/
4. 弊社が運営する「生涯学習のユーキャン」サイトにおける個人情報漏洩に関するお詫びとお知らせ（株式会社ユーキャン）
   https://www.u-can.co.jp/info/release.html
5. 弊社が運営する「ABC-MART公式オンラインストア」における個人情報漏えいの可能性に関するお詫びとお知らせ
   （株式会社エービーシーマート）
   https://www.abc-mart.net/shop/pages/info-2022.aspx
6. 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
7. 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
8. 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「標的型攻撃による機密情報の窃取」

1. 令和4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/R04_kami_cyber_jousei.pdf
2. 学術関係者・シンクタンク研究員等を標的としたサイバー攻撃について（注意喚起）（内閣サイバーセキュリティセンター）
   https://www.nisc.go.jp/pdf/press/20221130NISC_press.pdf
3. サイバーレスキュー隊（J-CRAT）活動状況［2022年度上半期］（IPA）
   https://www.ipa.go.jp/security/j-crat/ug65p9000000nks8-att/000106897.pdf
4. APTグループ「MirrorFace」が日本の政治団体を標的に実行したLiberalFace作戦の詳細（ESETセキュリティニュース）
   https://www.eset.com/jp/blog/welivesecurity/unmasking-mirrorface/
5. サイバー情報共有イニシアティブ（J-CSIP） 運用状況［2022年1月～3月,2022年4月～6月,2022年7月～9月,2022年10月～12月］（IPA）
   https://www.ipa.go.jp/security/j-csip/about.html

・4 位「内部不正による情報漏えい」

1. 区職員が住民基本台帳法違反容疑で逮捕されました（第1報）（東京都杉並区）
   https://www.city.suginami.tokyo.jp/news/r0411/1078406.html
2. 市立函館高校で模試成績など流出・SNS掲載 部内者の仕業か（NHK NEWS WEB）
   https://www3.nhk.or.jp/sapporo-news/20220722/7000048853.html
3. かっぱ寿司運営会社社長ら逮捕 不正競争防止法違反容疑 警視庁（NHK NEWS WEB）
   https://www3.nhk.or.jp/news/html/20220930/k10013843141000.html
4. 組織における不正防止ガイドライン（IPA）
   https://www.ipa.go.jp/security/guide/insider.html
5. 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

・5 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. ランサム被害、リモート接続の脆弱性が侵入口に - ニチリン（Security NEXT）
   https://www.security-next.com/139557
2. 令和4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/R04_kami_cyber_jousei.pdf
3. 2021年度 企業・組織におけるテレワークのセキュリティ実態調査（IPA）
   https://www.ipa.go.jp/security/reports/economics/scrm/ug65p90000019dg8-att/000099573.pdf

・6 位「修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）」
1. Twitter、ゼロデイ脆弱性悪用の約540万アカウントデータ漏えいを正式に認める（ITmedia NEWS）
https://www.itmedia.co.jp/news/articles/2208/08/news065.html
2. Verified Twitter Vulnerability Exposes Data from 5.4 Million Accounts（RESTORE PRIVACY）
https://restoreprivacy.com/twitter-vulnerability-exposes-5-million-accounts/
3. FortiOS - heap-based buffer overflow in sslvpnd（Fortinet, Inc.）
https://www.fortiguard.com/psirt/FG-IR-22-398
4. Fortinet製品のSSL VPN機能に脆弱性 - すでに悪用、侵害調査を（Security NEXT）
https://www.security-next.com/142121
5. FortiOSのヒープベースのバッファーオーバーフローの脆弱性（CVE-2022-42475）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/2022/at220032.html
6. 北朝鮮のサイバー犯罪グループ「APT37」がInternet Explorerのゼロデイ脆弱性を突く攻撃を行っていたと判明（GIGAZINE）
https://gigazine.net/news/20221208-north-korean-apt37-internet-explorer-exploit/
7. Microsoft Exchange Serverでゼロデイ攻撃が発生（トレンドマイクロ株式会社）
https://www.trendmicro.com/ja_jp/research/22/i/ms-exchange-zero-day.html
8. Microsoft Exchange サーバーのゼロデイ脆弱性報告に関するお客様向けガイダンス（Microsoft Security Response Center）
https://msrc-blog.microsoft.com/2022/09/30/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server-ja/

・7 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[2022年4月～6月]（IPA）
https://www.ipa.go.jp/security/j-csip/ug65p9000000nkvm-att/000100056.pdf
2. 当社子会社における資金流出事案の発生 並びに特別損失の計上に関するお知らせ（ウィルソン・ラーニング ワールドワイド株式会社）
https://ssl4.eir-parts.net/doc/9610/tdnet/2203725/00.pdf
3. ビジネスメール詐欺（BEC）対策（IPA）
https://www.ipa.go.jp/security/bec/index.html
4. 突然の口座変更依頼メールにご注意を!（警視庁Twitter）
https://twitter.com/MPD_cybersec/status/1400256494134693895

・8 位「脆弱性対策情報の公開に伴う悪用増加」
1. K23605346: BIG-IP iControl REST vulnerability CVE-2022-1388（F5, Inc.）
https://support.f5.com/csp/article/K23605346
2. 「BIG-IP」脆弱性に注意 - 実証コード公開済み、探索や悪用も（Security NEXT）
https://www.security-next.com/136392
3. 「Oracle Fusion Middleware」の既知脆弱性に対する攻撃が発生（Security NEXT）
https://www.security-next.com/142036
4. Oracle Fusion Middleware Vulnerability Exploited in the Wild（SECURITYWEEK）
https://www.securityweek.com/oracle-fusion-middleware-vulnerability-exploited-wild
5. 深刻な脆弱性「Spring4Shell」（NTT DATA）
https://www.nttdata.com/jp/ja/data-insight/2022/1012/
6. Spring4Shell（CVE-2022-22965）を悪用したボットネット「Mirai」の攻撃を観測（トレンドマイクロ株式会社）
https://www.trendmicro.com/ja_jp/research/22/d/Mirai-exploits-Spring4Shell.html
7. 「Spring Core」にゼロデイ脆弱性「Spring4Shell」の指摘（Security NEXT）
https://www.security-next.com/135304

・9 位「不注意による情報漏えい等の被害」
1. メールの宛先誤りについて（2022年4月1日）（デジタル庁）
https://www.digital.go.jp/press/a9874a8b-c99e-495f-8117-2f342403153b/
2. 委託事業者におけるメールの誤送信について（2022年4月6日）（デジタル庁）
https://www.digital.go.jp/press/a264aa83-154e-4677-8481-d29dcab34eed/
3. 個人情報を含むUSBメモリーの紛失事案について（尼崎市）
https://www.city.amagasaki.hyogo.jp/kurashi/seikatusien/1027475/1030947.html
4. JTB、クラウドサービスの設定ミスで1万人超の個人情報漏洩（日経XTECH）
https://xtech.nikkei.com/atcl/nxt/news/18/14005/

・10 位「犯罪のビジネス化（アンダーグラウンドサービス）」
1. 追跡！サイバー犯罪組織 コロナ禍の日本を狙う闇（NHK）
https://www.nhk.or.jp/gendai/articles/4631/
2. 大企業に不正アクセスするためのデータ、約2000～4000ドルで売買-カスペルスキー（TECH+）
https://news.mynavi.jp/techplus/article/20220624-2377889/
3. ダークウェブで個人情報流出を確認 - ダイナムJHD（Security NEXT）
https://www.security-next.com/140249

10 大脅威選考会

氏名	所属	氏名	所属
菅原 尚志	アクセンチュア（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
中嶋 美貴	アクセンチュア（株）		（Grafsec）
石井 彰	旭化成（株）	小関 直樹	京セラ（株）
宮崎 清隆	ICMS（株）	桜井 健人	京セラ（株）
岡田 良太郎	（株）アスタリスク・リサーチ	増尾 康寛	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	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）	刀川 郁也	京セラコミュニケーションシステム（株）
井部 俊生	ヴイエムウェア（株）	小林 勝	キンドリルジャパン（株）
橋本 賢一郎	ULTRA RED, Ltd.	村田 紗矢子	キンドリルジャパン（株）
安西 真人	（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）
関根 鉄平	（株）エーアイセキュリティラボ	宮内 雄太	（一社）金融 ISAC
溝口 英利	（株）SRA	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	三木 剛	グローバルセキュリティエキスパート（株）
佐藤 直之	SCSK（株）	浜田 譲治	クラウドストライク（株）
鈴木 寛明	SCSK（株）	古澤 一憲	グーグル・クラウド・ジャパン（同）
辻 伸弘	SB テクノロジー（株）	遠藤 誠	（株）ケイテック
大塚 淳平	NRI セキュアテクノロジーズ（株）	小川 善功	KDDI デジタルセキュリティ（株）
田中 悠一郎	NRI セキュアテクノロジーズ（株）	小熊 慶一郎	（ISC）2 ／ （株）KBIZ
芳賀 夢久	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）
笠井 靖記	NEC ネクサソリューションズ（株）	板橋 功	（公財）公共政策調査会（CPP）
杉井 俊也	NEC フィールディング（株）	坂 明	（公財）公共政策調査会（CPP）
大湊 健一郎	（株）NTT-ME	北田 高之	（株）神戸デジタル・ラボ
高橋 昌士	（株）NTT-ME	バローズ ダニエル	（株）神戸デジタル・ラボ
北河 拓士	NTT セキュリティ・ジャパン（株）	久柴 克宏	（株）神戸デジタル・ラボ
真鍋 太郎	NTT セキュリティ・ジャパン（株）	前園 博文	コベルコシステム（株）
大石 眞央	（株）NTT データ	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
大嶋 真一	（株）NTT データ		（CSIJ）
矢竹 清一郎	（株）NTT データ	松本 純	サイボウズ（株）
池田 和生	NTTデータ先端技術（株）	宮内 伸崇	（株）サイント
植草 祐則	NTTデータ先端技術（株）	佐藤 裕二	（一社）JPCERT コーディネーションセンター
前田 典彦	（株）FFRI セキュリティ		（JPCERT/CC）
岡田 祐太朗	エムオーテックス（株）	萩谷 文	（株）JR 東日本情報システム
西井 晃	エムオーテックス（株）	阿部 慎司	GMO サイバーセキュリティ by イエラエ（株）
前田 誉彦	エムオーテックス（株）	熊坂 駿吾	GMO サイバーセキュリティ by イエラエ（株）
池田 耕作	（株）オージス総研	三村 聡志	GMO サイバーセキュリティ by イエラエ（株）
大月 一孝	（株）オージス総研	唐沢 勇輔	Japan Digital Design（株）
姫野 猛	（株）オージス総研	大久保 隆夫	情報セキュリティ大学院大学
岡村 耕二	九州大学	印藤 晃	（国研）情報通信研究機構（NICT）
初見 卓也	（株）キクチメッセンジャー	岡 邦彦	（株）スクウェア・エニックス

氏名	所属	氏名	所属
山本 幸稔	スターネット(株)	山室 太平	Trellix
林 達也	SPREAD 情報セキュリティサポーター	今 佑輔	トレンドマイクロ(株)
広瀬 努	Sumo Logic ジャパン(株)	岡本 勝之	トレンドマイクロ(株)
正木 義和	スワットブレインズ(株)	加藤 雅彦	長崎県立大学
東 恵寿	NPO セカンドワーク協会(SWA)	須川 賢洋	新潟大学
鈴木 恵一	(株)西友	柳 優	日本アイ・ビー・エム(株)
原子 拓	(株)西友	山下 慶子	日本アイ・ビー・エム(株)
金城 夏樹	(株)セキュアイノベーション	高倉 万記子	(一財)日本情報経済社会推進協会(JIPDEC)
栗田 智明	(株)セキュアイノベーション	青木 聡	日本電気(株)
鉢嶺 光	(株)セキュアイノベーション	谷川 哲司	日本電気(株)
阿部 実洋	(株)セキュアベース	淵上 真一	日本電気(株)
上村 理	ゼットスケーラー(株)	住本 順一	日本電信電話(株)
澤永 敏郎	ソースネクスト(株)	松橋 亜希子	日本電信電話(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	今野 俊一	日本電信電話(株)
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	上野 宣	(一社)日本ハッカー協会
阿部 巧	ソフトバンク(株)	斎藤 健一	(一社)日本ハッカー協会
直井 信次郎	ソフトバンク(株)	宮本 久仁男	(一社)日本ハッカー協会
中西 基裕	ソフトバンク(株)	大島 悠司	ニューリジェンセキュリティ(株)
楢原 盛史	タニウム合同会社	大野 祐一	ニューリジェンセキュリティ(株)
鈴木 一弘	地方公共団体情報システム機構(J-LIS)	仲上 竜太	ニューリジェンセキュリティ(株)
八島 一司	地方公共団体情報システム機構(J-LIS)	小島 博行	(国研)農業・食品産業技術総合研究機構
筒井 英樹	中外製薬(株)		(農研機構)
徳丸 力蔵	中外製薬(株)	小林 克巳	(株)野村総合研究所
宮崎 弘己	中外製薬(株)	山崎 英人	パーソルキャリア(株)
田中 卓朗	TIS(株)	渡辺 久晃	パナソニック(株)
三木 基司	TIS(株)	菊谷 美緒	パナソニックコネクト(株)
中山 貴禎	(株)ディアイティ	高橋 洋一	パナソニックコネクト(株)
浅西 修	DXC テクノロジー・ジャパン(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
前田 隆行	DXC テクノロジー・ジャパン(株)	林 薫	パロアルトネットワークス(株)
松本 隆	(株)ディー・エヌ・エー	司東 秀浩	東日本電信電話(株)
内山 巧	(株)電算	水越 一郎	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)	田中 秀和	(株)日立ソリューションズ
髙木 優	東京海上日動火災保険(株)	沼田 亜希子	(株)日立製作所
花田 隆仁	東京海上日動火災保険(株)	古賀 洋一郎	ビッグローブ(株)
石山 圭佑	東京海上日動システムズ(株)	澤山 高士	PwC コンサルティング(同)
西城 秀行	東京海上日動システムズ(株)	山口 裕也	(株)ファイブドライブ
中西 祐介	東京海上日動システムズ(株)	大高 利夫	藤沢市役所
石川 朝久	東京海上ホールディングス(株)	原 和宏	富士通(株)
嶋谷 巧	東京海上ホールディングス(株)	中村 洋介	富士通(株)
大徳 達也	東京海上ホールディングス(株)	濱田 達也	富士通(株)
小島 健司	(株)東芝	荒井 大輔	(株)Bridge
大浪 大介	東芝インフォメーションシステムズ(株)	海老原 俊一	(株)Bridge
原田 博久	(株)Doctor Web Pacific	柳川 俊一	(株)Bridge
大山 水帆	戸田市役所	鴫原 祐輔	(株)Blue Planet-works

氏名	所属	氏名	所属
森マーク	ベライゾンジャパン（同）	江面 祥行	（株）ユビテック
島田 敏宏	（株）ベリサーブ	高岡 隆守	横浜市役所
倉田 尚希	（株）ベリサーブ	牧野 尚彦	横浜市役所
太田 良典	弁護士ドットコム（株）	三国 貴正	（株）YONA
結城 亮史	（株）BoxJapan	福本 佳成	楽天グループ（株）
垣内 由梨香	マイクロソフトコーポレーション	橘 喜胤	楽天ウォレット（株）
花村 実	マイクロソフトコーポレーション	伊藤 彰嗣	楽天モバイル（株）
軍司 祐介	（株）マキナレコード	山崎 圭吾	（株）ラック
東内 裕二	三井物産セキュアディレクション（株）	若居 和直	（株）ラック
篠原 巧	（株）三菱総合研究所	猪野 裕司	（株）リクルートテクノロジーズ
山中 翔太	（株）三菱総合研究所	六宮 智悟	（株）リクルート
平田 真由美	みゅーらぼ	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	矢儀 真也	（株）両備システムズ
鈴木 魁斗	（株）ユービーセキュア	鈴木 堅太	（株）両備システムズ
堀口 明日香	（株）ユービーセキュア	清水 秀一郎	–
島田 理枝	（株）ユビテック	piyokango	–

著作・制作　独立行政法人情報処理推進機構（IPA）

編集責任　土屋 正

イラスト製作　株式会社 創樹

執筆協力者　10 大脅威選考会

10 大脅威執筆者　土屋 正　内海 百葉　亀山 友彦
大友 更紗　吉本 賢樹　丹野 菜美
田村 智和　木村 泰介　鈴木 慧
三橋 正一

IPA 執筆協力者　高柳 大輔　桑名 利幸　渡辺 貴仁
中島 尚樹

情報セキュリティ 10 大脅威 2023

2023 年 2 月 28 日　初 版
2023 年 3 月 16 日　二 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/