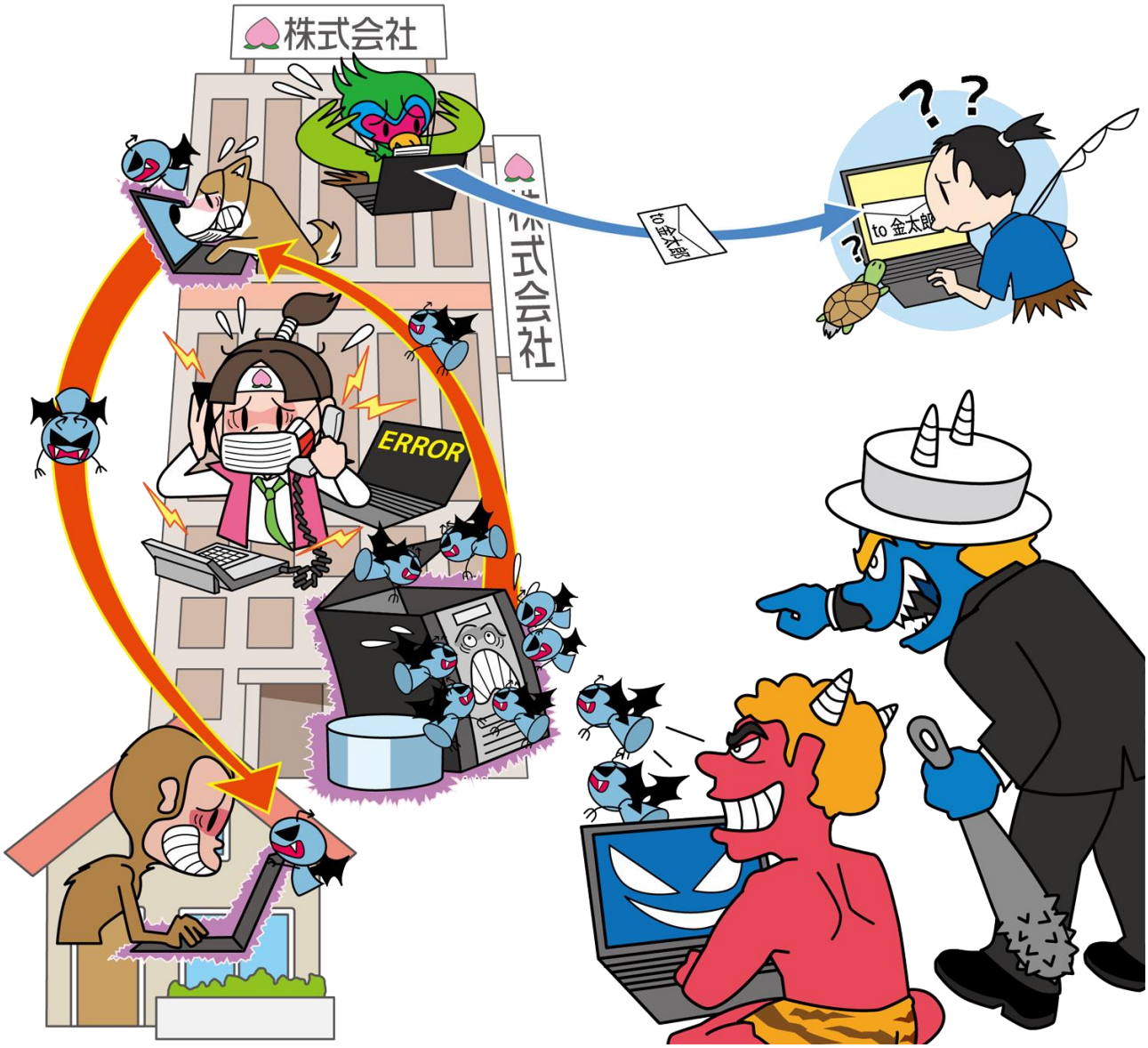
情報セキュリティ

10大脅威 2021

～よもや自組織が被害に！呼吸を合わせて全力防御！～



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

2021年2月

本書は、以下の URL からダウンロードできます。

「情報セキュリティ 10 大脅威　2021」
https://www.ipa.go.jp/security/vuln/10threats2021.html

目次

はじめに

本書「情報セキュリティ 10 大脅威 2021」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、2020 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 2021

個人の 10 大脅威では順位の変動はあるが昨年と同じ 10 個の脅威がランクインした。また、「スマホ決済の不正利用」は昨年の初登場 1 位に続いて 2 年連続 1 位にランクインしている。スマホ決済を狙った攻撃は引き続き発生しており、適切な対策を講じる必要がある。また、組織の 10 大脅威では、3 位に新しく「テレワーク等のニューノーマルな働き方を狙った攻撃」がランクインした。2020 年は新型コロナウイルス感染症（COVID-19）の世界的な蔓延を受けて、組織はテレワークへの積極的な移行を行った。一方、その変換期の中、テレワーク環境を狙った攻撃が行われており、組織には適切な対応が求められる。

本書では、2020 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 2021

情報セキュリティ 10 大脅威 2021

■「情報セキュリティ 10 大脅威 2021」

2020 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 2021」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 2021 「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
スマホ決済の不正利用	1	ランサムウェアによる被害
フィッシングによる個人情報等の詐取	2	標的型攻撃による機密情報の窃取
ネット上の誹謗・中傷・デマ	3	テレワーク等の ニューノーマルな働き方を狙った攻撃
メールや SMS 等を使った 脅迫・詐欺の手口による金銭要求	4	サプライチェーンの弱点を悪用した攻撃
クレジットカード情報の不正利用	5	ビジネスメール詐欺による金銭被害
インターネットバンキングの不正利用	6	内部不正による情報漏えい
インターネット上のサービスからの 個人情報の窃取	7	予期せぬ IT 基盤の障害に伴う業務停止
偽警告によるインターネット詐欺	8	インターネット上のサービスへの 不正ログイン
不正アプリによる スマートフォン利用者への被害	9	不注意による情報漏えい等の被害
インターネット上のサービスへの 不正ログイン	10	脆弱性対策情報の公開に伴う悪用増加

本章で共通的に使われる用語について**表 1.2** に定義を記載する。

表 1.2 情報セキュリティ 10 大脅威 2021 用語定義

用語	意味
個人	家庭等でスマートフォンや PC を利用する人
組織	企業、政府機関、公共団体等の組織およびその組織に所属している人
犯罪者	金銭や情報窃取（ストーカー行為を含む）を目的とした攻撃（犯罪）者
組織的犯行グループ	金銭を目的とした攻撃を組織的に行う攻撃（犯罪）集団
諜報員、産業スパイ	機密情報窃取を目的とした攻撃（犯罪）集団 国家組織の支援を受けた攻撃（犯罪）集団
ハクティビスト	社会的・政治的な主義主張を目的としたハッキング活動（ハクティビズム）を目的とした攻撃（犯罪）者集団
IoT	モノのインターネット（Internet of Things）。ネットワークカメラや情報家電、医療機器といった様々な機器がインターネットにつながり、通信を行う仕組み。機器自体を指す場合は、IoT 機器と呼ぶ。
CSIRT	セキュリティインシデント等の問題が発生した際に原因究明や影響範囲の調査等を行う組織。自組織に関する問題に対応する場合は、自組織 CSIRT と呼ぶ。
マイニング	PC 等を使って仮想通貨の取引に関連する情報を計算し、取引を承認する行為。計算の報酬として仮想通貨を得られる。
セクストーション	被害者のプライベートな写真や動画を入手したとして、それをばらまく等と脅迫する行為

■「情報セキュリティ 10 大脅威 2021」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 2021」は、「10 大脅威選考会」の投票結果に基づき順位付けして「個人」「組織」それぞれ 10 個の脅威を選定している。投票により重要度が高いと考えられるものをより上位の順位としているが、上位の脅威だけ、または上位の脅威から優先して対策を行えばよいということではない。例えば、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、スマートフォンを使った決済を狙った脅威である「スマホ決済の不正利用」（本書、個人 1 位）やスマートフォンのアプリを狙った脅威である「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 9 位）等の対策の必要性は低くなる。また、組織の立場では、オンラインショッピング等の個人情報をメインで取り扱っている組織であれば、その情報を狙った脅威である「インターネット上のサービスへの不正ログイン」（本書、組織 8 位）を優先的に対策しなければならないだろう。そのため、**順位が高いか低いかに関わらず、自身または組織が置かれている立場や環境を考慮して優先度を付け、適切な対応を取る必要がある。**

② ランクインした脅威が全てではない

「情報セキュリティ 10 大脅威 2021」で新しくランクインした脅威もあるが、それに伴いランク外となった脅威もある。しかし、ランク外になったとしてもその脅威が無くなったわけではない。かつてランクインしていた、「ワンクリック請求等の不当請求」や「ウェブサイトの改ざん」等は、依然として攻撃が行われている状況である。そのため、**ランク外の脅威だから対策を行わなくて良いということではなく、継続しての対策が必要となる。**ランク外となった脅威の詳細や対策方法等については、過去の「情報セキュリティ 10 大脅威」を参考にしてほしい。

③ 「情報セキュリティ対策の基本」が重要

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

詳しくは「情報セキュリティ 10 大脅威 2015」の1章で解説しているが、表 1.3 に示すように「攻撃の糸口」を 5 つに分類し、それぞれに該当する対策を「情報セキュリティ対策の基本」としている。「攻撃の糸口」に変化がない限り、「情報セキュリティ対策の基本」による効果が期待できるので、これを意識して継続的に対策を行うことで、被害に遭う可能性を低減できると考える。

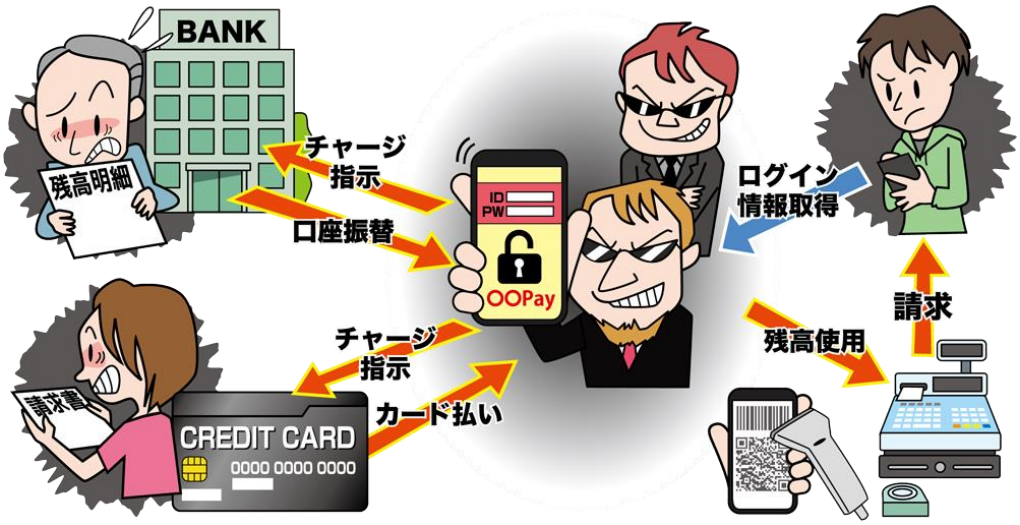
表 1.3 情報セキュリティ対策の基本

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

1. 情報セキュリティ 10 大脅威（個人）

1位 スマホ決済の不正利用

～スマホ決済の不正利用被害に備え利用状況の確認を～



近年のスマートフォンの普及に伴い、2018 年頃よりキャッシュレス決済の 1 つであるスマートフォンを利用した決済（スマホ決済）が登場し、その後スマホ決済を使った各社のサービスも登場しその手軽さから普及が進んだ。一方、利便性の反面、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等も確認されている。

＜攻撃者＞

- 組織的犯行グループ
- 犯罪者

＜被害者＞

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

＜脅威と影響＞

スマホ決済では、スマートフォンをカードリーダーにかざしたり（非接触型決済）、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たり、逆に店舗に置いてある QR コードを決済用アプリで読み込んで決済金額を手動で入力したりして決済する。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等を登録してそこからチャージできる。これらの情報は決済サービス毎に専用のシステムやアプリで管理されているが、決済サービスや仕組みに不備がある場合、攻撃者に不正利用される。

例えば、決済サービスに不正にログインされると、クレジットカード情報等が窃取されたり、意図しない金銭取引をされたり等の被害に遭う。

＜攻撃手口＞

◆ **不正アクセスによるアカウントの乗っ取り**

被害者が複数のサービスで同一のパスワードを使いまわしている場合がある。攻撃者は、過去に漏えいしたパスワードをリスト化し、それをもとにログインを試みる（パスワードリスト攻撃）。不正ログインに成功すれば、なりすまして不正利用する。また、スマホ決済サービスより提供される二要素認証等のセキュリティ強化機能を利用していない場合、漏えいしたパスワードのみで不正ログインできるため、攻撃者に悪用されやすい。

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

スマホ決済サービスを開発する際に、当該サービスのみでなく連携するその他のサービスの機能

等も含めてセキュリティを十分に考慮していない場合、スマホ決済サービスの不正利用に悪用できる脆弱性を作り込んでしまうおそれがある。例えば残高をチャージするために銀行口座とスマホ決済サービスを連携する際や、口座振込を利用して銀行口座からスマホ決済サービスへチャージする際の振込者に対する本人確認方法に不備があると、それを悪用されて銀行口座から不正に預金を使用されるおそれがある。

＜事例または傾向＞

◆ **PayPay で他人の口座から不正引き出し**

スマホ決済サービス「PayPay」に、他人の銀行口座から不正に残高をチャージ（入金）したとして、警視庁サイバー犯罪対策課は電子計算機使用詐欺容疑で 2 名の容疑者を逮捕した。同課によると、容疑者らは他人の口座番号や生年月日などの情報を PayPay の自分のアカウントに紐付けて不正にチャージしたとみられる。[1]

◆ **LINE Pay と連携するゆうちょ銀行口座から不正引き出し**

スマホ決済サービス「LINE Pay」において、連携しているゆうちょ銀行口座から不正な引き出しを確認したと LINE Pay が発表した。LINE Pay に残高をチャージするために、ゆうちょ銀行の口座を連携してウェブ上の手続きで口座振替を行うサービスを悪用された。不正な引き出しの件数は 2 件で、いずれも 2020 年に入ってから発生した。うち 1 件は被害者の身近な人物の引き出しによるものと判明しており、2 件目についても同様のケースと想定して調査中としている。[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
  - ・強い認証方式の利用

    二要素認証や 3D セキュア等を利用することで、仮にパスワードが攻撃者に漏えいしたとしても、不正ログインや、その後の金銭被害等につながる重要な操作を阻止できる確率を高める。[4]
  - ・パスワードは長く、複雑にする
  - ・パスワードの使いまわしをしない

    例えばパスワードの基となるコアパスワードを作成し、その前後にサービス毎に異なる識別子を付加することで他と重複しないパスワードを作成することができる。[3]
  - ・パスワード管理ソフトの利用
  - ・認証に不備がある銀行口座と連携しない
  - ・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。
  - ・利用頻度が低いサービスや不要なサービスのアカウント削除
  - ・スマートフォンの紛失対策

    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
  - ・パスワードの再設定
  - ・スマホ決済サービス運営者への連絡
  - ・連携する金融機関への連絡
  - ・警察への連絡
  - ・二要素認証等の追加設定

参考資料

1. ペイペイ悪用、他人の預金詐取＝不正チャージ疑いで2人逮捕―警視庁
https://sp.m.jiji.com/article/show/2476202
2. LINE Payでも ゆうちょ銀行から不正引き出し
https://www.itmedia.co.jp/business/articles/2009/16/news075.html
3. 不正ログイン被害の原因となるパスワードの使い回しはNG
https://www.ipa.go.jp/security/anshin/mgdayori20160803.html
4. 不正ログイン対策特集ページ
https://www.ipa.go.jp/security/anshin/account_security.html

2位 フィッシングによる個人情報等の詐取

～コロナ禍の生活の変化に乗じてオンラインショッピングに関連するフィッシングが急増～

フィッシング詐欺は、実在する公的機関や有名企業を騙ったメールや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、個人情報や認証情報等を入力させる詐欺である。詐取された情報は悪用され、金銭的な被害が発生することもある。

＜攻撃者＞

- 組織的犯行グループ
- 犯罪者

＜被害者＞

- 個人（インターネット利用者）
- 組織（インターネット利用者）

＜脅威と影響＞

官公庁、金融機関、ショッピングサイト等の実在する組織を偽装したメール等が、PC やスマートフォンに届く。本文には URL が記載されており、受信者の心理につけ込む巧みな言葉でリンクをクリックするよう誘導する。リンク先は実在する組織を装ったフィッシングサイトになっており、クレジットカードや銀行口座等の個人情報、ID やパスワード等の認証情報の入力を促す。2020 年は、コロナ禍の影響で自宅にてインターネットを利用する時間が増えるとともに、ショッピングサイトを騙る等のフィッシング詐欺の件数も増加傾向にあった。

入力した情報は攻撃者に詐取され、売却されたり、その情報を悪用した不正アクセス等により金銭的な被害を受けたりするおそれがある。

＜攻撃手口＞

◆ **公的機関や有名企業に偽装したフィッシングメールを不特定多数に送信**

メールや SMS 等を利用して不特定多数の宛先にフィッシングメールを送信し、公的機関や有名企業等の正規のウェブサイトを装ったフィッシングサイトへ誘導する。フィッシングサイトに入力した個人情報や認証情報等は詐取される。また、二要素認証の情報（ワンタイムパスワード等）も入力させて詐取することもある（中間者攻撃）。

◆ **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等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を騙った広告を表示する。不正な広告のリンクにアクセスすると、フィッシングサイトへ誘導され、個人情報等の入力を促される。[1]

◆ **問い合わせフォームを悪用したフィッシングメールの大量配信**

攻撃者は正規のウェブサイトの問い合わせフォームに問い合わせを入力すると問い合わせ者に自動返信をする機能を悪用し、フィッシングメールを送信する。攻撃者は標的のメールアドレスやフィッ

シングサイトのURL等をフォームに入力し、大量のフィッシングメールを拡散する。[2]

＜詐取した情報の悪用例＞

- 詐取した個人情報等を、ダークウェブ上の違法なウェブサイト等で販売して金銭を得る。
- 詐取した認証情報等を悪用し、オンラインショッピング等の複数のインターネットサービスで不正ログインを試みる。

＜事例または傾向＞

◆ 特別定額給付金に便乗したフィッシング

新型コロナウイルス感染症に係る特別定額給付金に便乗し、申請用のウェブサイトを偽装したフィッシングサイトが存在するとして、総務省が注意喚起を行った。また、申請手続きの代行を装って、重要情報等を詐取する事例も確認されている。[3,4]

◆ 国税庁を騙るフィッシング

2020 年 11 月、国税庁を騙るフィッシングメールが確認されているとしてフィッシング対策協議会が注意喚起を行った。[5] また、そのメールから誘導される国税庁を騙るフィッシングサイトもあり、国税庁がウェブサイトのドメイン名を必ず確認し、偽サイトに注意してほしいという旨の注意喚起を行った。[6]

◆ 報告件数は依然として増加傾向

2020 年はフィッシングメールの配信頻度が増加傾向にあり、報告件数も過去最多となっている。また、Amazon、Apple、楽天等のショッピングサイトや金融機関、クレジットカードブランド等を騙るフィッシングが継続して報告されており、宅配業者の不在通知を装った SMS を悪用する事例等も確認されている。[7]

＜対策/対応＞[8]

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
  - ・二要素認証を利用
  - ・メール、SMS、SNS の投稿内の URL を安易にクリックしない

    自身の金銭や重要情報を扱うウェブサイトは、ブックマークやサービス運営者が配布している公式アプリを利用してアクセスする。
  - ・受信メールやウェブサイトの十分な確認

    重要なお知らせ等の緊急性を煽る内容で誘導されたウェブサイトにおいて、重要情報はすぐに入力せず、ドメイン名等を確認してサイトの真偽を確かめる。
  - ・迷惑メールフィルターを利用
- 被害の早期検知
  - ・利用するウェブサイトのログイン履歴の確認

    自分のものではないログイン履歴等、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等の利用明細を確認
- 被害を受けた後の対応
  - ・パスワードの変更
  - ・利用しているサービスへの利用停止を連絡
  - ・信頼できる機関に相談

    警察、国民生活センター、地域の消費生活センター等に相談する。

参考資料

1. Googleサーチ結果に表示される偽広告経由のネット詐欺に注意
https://is702.jp/news/3802/
2. 問い合わせフォームへの攻撃急増　詐欺メールの“送信元”に
https://www.itmedia.co.jp/news/articles/2012/09/news101.html
3. 特別定額給付金の給付を騙ったメールに対する注意喚起
https://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000438.html
4. 特別定額給付金に関する通知を装うフィッシング（2020/10/19）
https://www.antiphishing.jp/news/alert/kyufukin_20201019.html
5. 国税庁をかたるフィッシング（2020/11/20）
https://www.spread.or.jp/phishing/2020/11/20/18612/
6. 偽サイトにご注意ください
https://www.nta.go.jp/data/021120jouhou.pdf
7. 2020/12 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202012.html
8. フィッシング対策ガイドライン
https://www.antiphishing.jp/report/antiphishing_guideline_2020.pdf

3位 ネット上の誹謗・中傷・デマ

～安易な書き込みが、他者と自分の人生を脅かす～

インターネットの匿名性を利用して、特定の個人や組織に対して誹謗・中傷をしたり、デマを発信したりする事件が発生している。被害者は、精神的苦痛に苛まれたり、業務妨害の被害を受けたりする。2020 年においては、特に新型コロナウイルスに関する事例が注目された。

＜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（ソーシャル・ネットワーキング・サービス）等のサービスの普及に伴い、匿名での情報発信が容易に行えるようになっている。一方、そのサービスを利用し、意図的に他人への誹謗・中傷や、脅迫・犯罪予告・デマを書き込む事件が確認されている。さらに、その情報が多くの人に拡散され、大きな問題となる場合がある。

攻撃の対象が個人であれば、精神的苦痛に苛まれることがあり、組織であれば、風評被害による経済的な損失を受ける等、様々な影響が出る。また、非常時に嘘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・中傷やデマ等を発信した側だけではなく悪意はなくとも情報の真偽を確認せず、安易に拡散した人も特定され、社会的責任を問われる場合がある。

＜要因＞

◆ 影響を考慮しないインターネット上への発信

特定の個人に対しての恨みや妬み、また、自身の優位性や正義の誇示、ストレス発散、相手の反応を見たい等の身勝手な理由で、誹謗・中傷やデマ等を、他者や社会に与える影響を考慮せずにインターネット上へ発信してしまう。

◆ 匿名性を過信した安易な発信

昨今、様々なコミュニティサイトが存在し、個人が匿名で、ブログや SNS、動画配信等に情報を発信することができる。一方、匿名性を過信すると、普段人前では言えないことを安易に発信してしまう場合がある。なお、匿名でも警察等が調査すれば身元を容易に特定できる場合が多い。

◆ 情報の真偽を確認せずに拡散

インターネット上には根も葉もない誹謗・中傷やデマが出回ることがある。そうした情報の真偽を確かめることなく、同調したり、面白がったりして拡散してしまう。また、有用な情報を伝えたいという親切心や正義感によってデマを拡散してしまうケースもある。

＜事例または傾向＞

◆ **新型コロナウイルスに感染していると虚偽の書き込み**

2020 年 5 月、県内の商店関係者が新型コロナウイルスに感染しているという虚偽の書き込みをしたとして、福島県警が会社員を業務妨害と名誉毀損の疑いで逮捕した。会社員は匿名のネット掲示板上に、商店の店舗名と場所とともに「店員の家族がコロナに感染している」と嘘の情報を書き込んだ。その後、店には複数回の無言電話があったり、売り上げが減少したりする等の被害が出た。会社員は、「職場で聞いたうわさ話を書き込んだ」と供述している。[1]

◆ **テレビ番組出演者に対する誹謗・中傷**

2020 年 5 月、テレビのバラエティ番組の出演者が、SNS 上で相次いだ匿名での誹謗・中傷によって精神的苦痛を受け、亡くなる事件があった。警視庁は、SNS で誹謗・中傷を書き込んだ男性を侮辱容疑で 2020 年 12 月に書類送検した。事件の直後、多くの誹謗・中傷コメントや書き込んだアカウントが投稿者によって削除されたが、コメントの画像が被害者によって保存されており、同庁は今後も同様の誹謗・中傷にあたる投稿について捜査する方針としている。[2]

＜対策/対応＞

個人（発信者）

- 情報モラルや情報リテラシーの向上、法令遵守の意識の向上

・誹謗・中傷や公序良俗に反する投稿をしない

・投稿前に内容を再確認

SNS やブログ等に投稿する内容は不特定多数の人に見られることを想定し、投稿して問題ない内容かをしっかりと確認する。

・匿名性での発言にも責任を持つ

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

個人（家庭）、組織（教育機関）

・情報モラル、情報リテラシーの教育

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

個人（閲覧者）

- 情報モラルや情報リテラシーの向上、法令遵守の意識の向上

・情報の信頼性の確認

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

個人（被害者）

- 被害を受けた後の適切な対応

・冷静な対応と支援者への相談

一人で抱え込まず、信頼できる周囲の人や公的相談機関へ相談する。[4] 脅迫等犯罪と思われる誹謗・中傷の投稿は、警察へ被害届を提出し、必要に応じて弁護士にも相談する。

・管理者やプロバイダーへ削除依頼

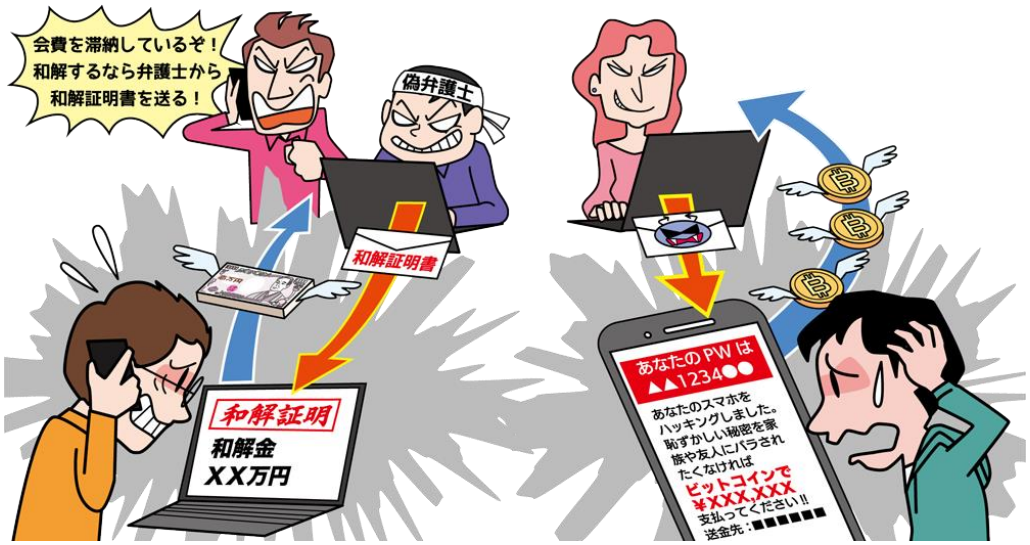
問題ある書き込みを削除したいときは本人または関係者がウェブサイトの管理者やプロバイダーに削除を要請する。なお、削除により炎上の火種になるおそれもあるため、保護者や弁護士等に相談して慎重に行う。

参考資料

1. コロナ感染とネットに虚偽　業務妨害容疑で会社員逮捕　福島県警
https://www.sankei.com/affairs/news/200527/afr2005270010-n1.html
2. 「テラハ」木村花さんを侮辱の疑い　20代男「復讐で」
https://www.asahi.com/articles/ASNDK33MCNDKUTIL009.html
3. インターネットトラブル事例集（2020年度版）
https://www.soumu.go.jp/main_content/000681954.pdf
4. インターネット人権相談受付窓口（法務省人権擁護局）
http://www.moj.go.jp/JINKEN/jinken113.html

4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

～脅迫・詐欺メールの指示に従うと相手のおもうつぼ～



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

＜攻撃者＞

- 組織的犯行グループ

＜被害者＞

- 個人（インターネット利用者）

＜脅威と影響＞

「アダルトサイトを閲覧している姿を撮影した」等の脅迫メールや有料サイトの未納金があるといった架空請求のメールを送信し、金銭を詐取しようとする攻撃が行われている。また、メールだけでなく SMS 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、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。一度攻撃が成功すると、その脅迫は効果が期待できると攻撃者に認識され、同様の手口で多数の宛先へメール送信を行い、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 を不特定多数に送り、金銭を詐取しようとする。指定される支払方法には仮想通貨や電子マネーが多く見られる。また、騙す手口として以下が使われる。

◆　セクストーション

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

◆　ハッキングしたように見せかける

被害者のパスワードや住所等の個人情報をメールに記載し、あたかも被害者の PC をハッキングして情報を得たかのように見せかける。記載している情報はハッキングによるものではなく、外部のサービスから何らかの原因で漏えいした情報を使用している。

◆　メールや電話を併用して信憑性を高める

脅迫・詐欺のメールに問合せ窓口の電話番号を記載して送信し、この電話番号宛に被害者から電話を掛けさせる。電話を掛けてきた被害者に対して、攻撃者は更に脅迫や催促を行ったり、電話口で公的機関を装った偽の相談窓口を紹介し、その窓口に電話を掛けさせて信頼させた上で金銭を支払わせたりする。また、攻撃者から被害者に対して金銭を要求する電話をかけ、その後に弁護士を装った

攻撃者から和解を求める旨のメールを送信し、信憑性を高めて騙そうする手口もある。

＜事例または傾向＞

◆　電話やメールを併用した架空請求新手口

債権回収業者を名乗る人物から、数年前に入会したというオンライン投資塾の月会費等が滞納になっているため支払うように求める架空請求の電話があった。さらにその後、弁護士を装った人物から本件の和解を求める場合に必要な対応が記載されたメールが送信されてきたという相談が国民生活センターに寄せられた。[1]

◆　個人への脅迫メールのばらまき

2020 年 12 月、「あなたのアカウントをハッキングした」、「アダルト動画を見ている姿を撮影した」「あなたのネットワーク上の連絡先に撮影したビデオを送信する」といった脅迫を行い、ビットコインの支払いを要求するメールが電気通信大学内でばらまかれ、注意喚起が行われた。[2,3]

◆　仮想通貨を要求する脅迫メールの相談増加

仮想通貨で金銭を要求する脅迫メールが送信されてくる事例について、IPA の情報セキュリティ安心相談窓口に 2020 年の第 4 四半期に寄せられた相談件数が、同第 1 四半期の 2 倍以上に増加した。不特定多数に仮想通貨を要求する脅迫メールを送信する手口は 2018 年頃から確認されているが、IPA への相談も引き続き寄せられており、2020 年は相談件数が増加傾向のため注意が必要である。[4]

◆　従来からの手口が継続して横行

一般財団法人 日本データ通信協会の迷惑メール相談センターは「よくあるご質問と相談事例」として最近の迷惑メールの相談事例を掲載し、対処方法を紹介している。

2020 年の相談事例は、セクストーションやハッキングを匂わせた脅迫、身に覚えのない料金請求や手数料請求等、メール受信者を脅したり、不安にさせたりするものが多い。これら従来から知られている手口が依然として使われている。[5]

＜対策/対応＞

個人（インターネット利用者）

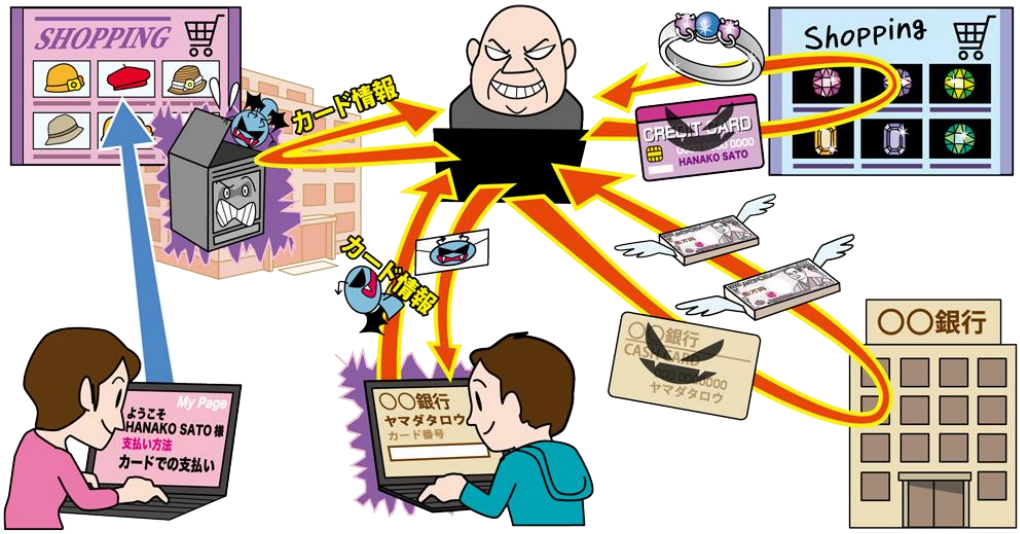
- 被害の予防（被害に備えた対策含む）
  - ・表 1.3「情報セキュリティ対策の基本」を実施
  - ・受信した脅迫・詐欺メールは無視する
    詐欺メールに、被害者のパスワード等が記載されていても、実際にハッキングされているわけではない。被害者のパスワード等は、別のところから漏えいしたものであると思われる。
  - ・メールに記載されている番号に電話をしない
    受信した脅迫や架空請求のメールについて専門機関に相談したい場合は、自分で調べた正規の電話番号やメールアドレスに連絡する。
  - ・パスワードを使いまわさない
    パスワード漏えい時に多数のサービスのパスワード変更を必要とされないために各種サービスでパスワードを使いまわさない。
- 被害を受けた後の対応
  - ・パスワードを変更する
    脅迫・詐欺メールに記載されたパスワードが自分のパスワードと一致しているのであれば、どこかからパスワードが漏えいしたおそれがあるので、早急にパスワードを変更する。
  - ・警察に相談する

参考資料

1. 新手の架空請求手口にご注意！債権回収業者から「過去の契約の未納料金・損害金の和解」を求める電話！？
http://www.kokusen.go.jp/news/data/n-20200130_2.html
2. 【2020/12/5 1:10】ばらまき型脅迫詐欺メールに関する注意喚起
https://www.cc.uec.ac.jp/blogs/news/2020/12/20201205scammail.html
3. 【2020/12/29 13:00】ばらまき型脅迫詐欺メールに関する注意喚起
https://www.cc.uec.ac.jp/blogs/news/2020/12/20201229scammail.html
4. 情報セキュリティ安心相談窓口の相談状況［2020年第4四半期（10月～12月）］
https://www.ipa.go.jp/security/txt/2020/q4outline.html
5. よくあるご質問と相談事例(一般財団法人 日本データ通信協会)
https://www.dekyo.or.jp/soudan/contents/denwa/faq.html

5位 クレジットカード情報の不正利用

～知らない間に流出し不正利用されているかも～



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、所有者を狙ったフィッシング詐欺やクレジットカードが紐付けされているサービスを狙った不正アクセスによる情報漏えい等により、クレジットカード情報が窃取され、攻撃者にクレジットカードを不正利用される被害が継続して発生している。

＜攻撃者＞

- 組織的犯行グループ
- 犯罪者

＜被害者＞

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

＜脅威と影響＞

近年のキャッシュレス決済の普及に加え、電子マネーやモバイル端末等でクレジットカード情報を入力することで決済ができるサービスが次々と登場している。クレジットカード情報は、これらの多くのサービスに対して紐付けが可能となっており、広く活用されている。そのクレジットカード情報を攻撃者が窃取しようと狙っている。クレジットカード情報で決済を行っている端末にウイルスを感染させ窃取したり、フィッシング詐欺により詐取したりする。また、オンラインゲーム、オンラインショップ等へ不正アクセスし、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悪意ある者に窃取されると、正規の利用者の知らない間に不正利用され金銭的な被害を受けたり、クレジットカード情報を公開されたり、販売されたりするおそれがある。

＜攻撃手口＞

以下の手口でクレジットカード情報を入手し、不正利用を行う。

◆　フィッシング詐欺

フィッシングサイト（偽のウェブサイト）を用意し、フィッシングサイトのリンクが記載されたメールを送信する。その後メール受信者をフィッシングサイトに誘導し、フィッシングサイト上で入力させたクレジットカード情報を窃取する。メール内では、実在する企業や組織を騙り、記載されているリンクも正規の URL を模倣しているものもある。

◆　改ざんされたウェブサイトを介した詐取

脆弱性等を悪用し、正規のウェブサイトを改ざんすることで、利用者を偽の決済画面に誘導し、クレジットカード情報を入力させることで、クレジットカード情報を詐取する。正規のウェブサイト上に偽の決済画面が作られているため、利用者がウェブサイトのドメイン等に気をつけていたとしても、偽の決済画面であることに気付くことが極めて困難である。

◆　**ウイルス感染**

ウイルスファイルをメールに添付したり、悪意あるウェブサイトのリンクを記載したメール等を送信し、添付ファイルを開かせたり、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、利用者が認証情報や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送信されて窃取されたり、端末内に保存された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。

＜事例または傾向＞

◆　**「EXILE TRIBE」オンラインショップでクレジットカード情報流出**

2020 年 10 月、「EXILE」等が所属する芸能事務所 LDH JAPAN が運営する公式サイトが不正アクセスを受け、4 万 4,663 件のクレジットカード情報が流出したおそれがあると発表している。流出したクレジットカード情報は、カード名義人、カード番号、有効期限、セキュリティコードで、11 月時点で 209 件のカード情報が第三者に不正利用されたおそれがあった。[1]

◆　**ネット書店からのカード情報流出**

2020 年 11 月、小学館パブリッシング・サービスは、ウェブサイトで提供しているネット書店「BOOK SHOP 小学館」が不正アクセスを受け、1036 件のクレジットカード情報が漏えいした疑いがあると発表した。[2] その一部は不正利用されたおそれがあった。

◆　**被害額は減少傾向、盗用被害の割合増加**

日本クレジット協会が公開したクレジットカード不正利用被害の集計結果によれば、2020 年の 1～9 月において不正利用被害額は約 178.5 億円となった。2019 年の同期間の被害額は約 205 億円であり、前年と比較して被害額は減少している。なお、被害額全体の 87.7%を番号盗用被害が占めており、その割合は年々増加している。[3]

＜対策/対応＞

個人（利用者）

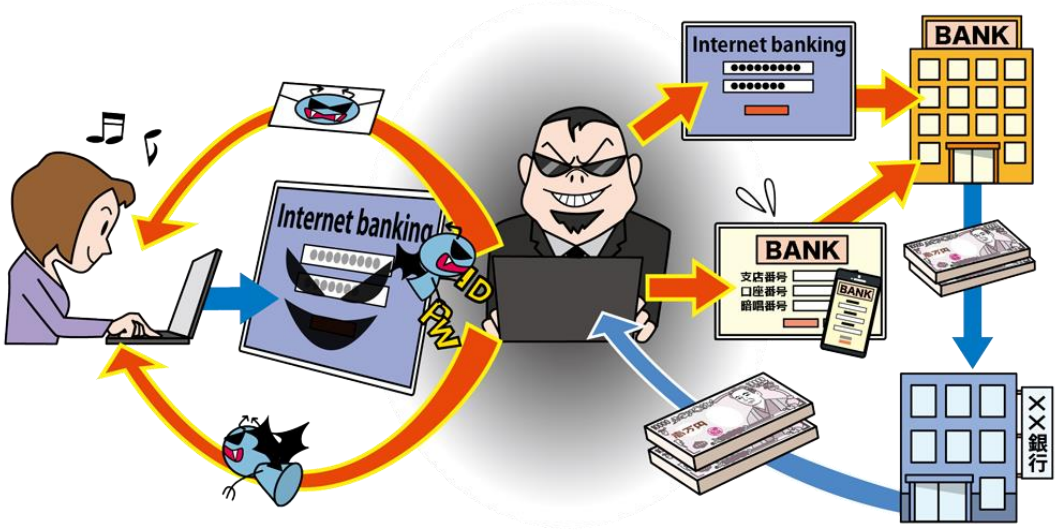
- 被害の予防
  - ・表 1.3「情報セキュリティ対策の基本」を実施
  - ・パスワードの使いまわしをしない
  - ・クレジットカード会社が提供している本人認証サービス（3D セキュア等）の利用
  - ・メールや閲覧ウェブサイトの十分な確認
    メールアドレスやウェブサイトのドメイン名が偽装されていないか確認する。
  - ・添付ファイルや URL を安易に開かない
  - ・クレジットカード情報を安易にウェブサイトに保存しない
  - ・普段は表示されないような画面やポップアップが表示された場合、情報を入力しない
  - ・プリペイドカードの利用を検討
    不正利用被害額の範囲を限定する。
- 被害の早期検知
  - ・クレジットカードの利用明細の確認
  - ・サービス利用状況の通知機能等の利用
- 被害を受けた後の対応
  - ・該当サービスのコールセンターへの連絡
    クレジットカード会社によっては、全額または一部を補償する場合がある。（補償してくれる期間が短い場合があるので注意）
  - ・クレジットカードの再発行
  - ・パスワードの変更
  - ・ウイルス感染した端末の初期化
    警察への被害届の提出

参考資料

1. EXILEの公式ECサイトに不正アクセス　カード情報4万4000件が流出か
https://www.itmedia.co.jp/news/articles/2012/08/news139.html
2. 小学館子会社のネット書店に不正アクセス、1000件超のカード情報流出か
https://www.itmedia.co.jp/news/articles/2011/16/news121.html
3. クレジットカード不正利用被害額の発生状況
https://www.j-credit.or.jp/information/statistics/download/toukei_03_g.pdf

6位 インターネットバンキングの不正利用

～こまめな口座の利用履歴の確認および不審なログイン履歴がないかの確認を～



フィッシング詐欺やウイルス感染により、インターネットバンキングの認証情報を窃取されることで、被害者のアカウントから不正な送金が行われたり、不正にサービスを利用されたりする等の被害が確認されている。2020 年は決済サービスを悪用して別の銀行へと不正送金される被害が発生し、多くのサービス利用者、銀行が影響を受けた。

＜攻撃者＞

- 組織的犯行グループ
- 犯罪者

＜被害者＞

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

＜脅威と影響＞

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

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

＜攻撃手口＞

以下の手口でインターネットバンキングの認証情報を入手し、不正送金を行う。

◆ フィッシング詐欺

偽のメールや SMS を被害者に送信し、フィッシングサイトに誘導して、インターネットバンキングの認証情報を詐取する。また、二要素認証で使う情報（ワンタイムパスワード等）を入力させる場合もある。詳細は、個人 2 位「フィッシングによる個人情報等の詐取」を参照。

◆ ウイルス感染

ウイルスに感染させるように細工したファイルをメールに添付し、ファイルを開くよう誘導して、被害者の端末をウイルスに感染させる。また、改ざんされた正規のウェブサイトを被害者に閲覧させることで、ウイルスに感染させる手口も確認されている。ウイルスに感染した端末でインターネットバンキングにログインしようとすると、偽のログインページが

表示され、そこに入力した認証情報がウイルスによって攻撃者に送信される。

＜事例または傾向＞

◆　決済サービスを悪用した不正送金被害

2020 年 9 月、NTT ドコモが提供する決済サービス「ドコモ口座」を悪用した不正送金が相次いで確認され、2020 年 9 月 29 日時点で銀行からの申告による被害件数は 247 件、被害金額は 2,931 万円にまで上った。「ドコモ口座」を悪用する不正送金被害は、メールアドレスだけで開設できるドコモ口座側の問題と、口座番号や暗証番号等が分かってしまえば他人になりすまして口座の連携ができてしまう銀行側の問題、双方のセキュリティの弱点を突かれる形だったとされている。[1] また、不正送金が確認された銀行の内、ゆうちょ銀行においては、2020 年 9 月時点で被害件数が約 380 件、被害金額は約 6,000 万円にまで上り、同行は決済サービスと連携している約 550 万口座の顧客に対して、不審な取引がないか確認するよう呼びかけている。[2]

◆　フィッシング詐欺で詐取した情報の悪用

2020 年 12 月、北陸銀行にて顧客口座から不正に預金が引き出される被害が確認された。フィッシングサイトに誘導するために「お客さまの北陸銀行に異常ログインの可能性がございます」等と記載された SMS が確認されており、そこで詐取された ID やパスワードを使われたおそれがある。12 月 18 日時点で 3 件約 80 万円の被害が疑われている。[3]

◆　不正送金被害の多くは個人の被害

一般社団法人全国銀行協会によると、2020 年第 3 四半期（7 月～9 月）におけるインターネットバンキングの被害件数は、前四半期の 408 件から 261 件、被害金額は約 4 億 5,600 万円から約 1 億 7,300 万円へと減少している。なお、261 件中の 255 件、約 1 億 7,300 万円中の約 1 億 6,600 万円は個人の不正送金被害であり、被害全体の多くを占める状況が続いている。[4]

＜対策/対応＞

個人（インターネットバンキング利用者）

- 被害の予防（被害に備えた対策含む）
  - ・受信メールやウェブサイトの十分な確認
  - ・添付ファイルや URL を安易にクリックしない
    よく利用するウェブサイトは、予めブックマークに登録し、そこからアクセスする。
  - ・ファイルの拡張子を表示させる設定
  - ・普段は表示されないポップアップ画面に個人情報等は入力しない
  - ・金融機関や公的機関から公開される注意喚起等の確認
  - ・二要素認証等、金融機関が推奨する認証方式の利用
  - ・口座連携済みサービスの確認
  - ・認証に不備がある銀行口座の利用停止
    暗証番号のみ等脆弱な認証で利用可能な銀行口座については、必要がなければインターネット取引を利用停止しておく。
- 被害の早期検知
  - ・不審なログイン履歴の確認
  - ・口座の利用履歴の確認
  - ・サービス利用状況の通知機能等の利用
- 被害を受けた後の対応
  - ・該当サービスのコールセンターへの連絡
    金融機関によっては、全額または一部補償してくれる場合がある。
  - ・警察への被害届の提出
  - ・ウイルス感染した端末の初期化
  - ・パスワードの変更

参考資料

1. 厄介な「ドコモ口座」不正引き出し問題、解決に求められるのは
https://xtech.nikkei.com/atcl/nxt/column/18/00086/00137/
2. ゆうちょ銀行の不正引き出し、被害額が6000万円に拡大
https://xtech.nikkei.com/atcl/nxt/column/18/01421/092400025/
3. 北陸銀行ネットバンクで不正引き出し
https://www.fukuishimbun.co.jp/articles/-/1227954
4. 不盗難通帳、インターネット・バンキング、盗難・偽造キャッシュカードによる預金等の不正払戻し件数・金額等に関するアンケート結果および口座不正利用に関するアンケート結果について
https://www.zenginkyo.or.jp/news/2020/n122201/

7位 インターネット上のサービスからの個人情報の窃取

～利用者でできる対策を忘れずに、ID やパスワードの使いまわしに注意～

ショッピングサイト（EC サイト）等のインターネット上のサービスの脆弱性等を悪用した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、クレジットカードの不正利用等の被害を受ける事態が発生している。

＜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＞

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

重要な情報を窃取されると、クレジットカードを不正利用されたり、詐欺メールを送信されたり、窃取された情報をダークウェブで売買されたり等、さらなる被害につながるおそれがある。

＜攻撃手口＞

◆ サービスの脆弱性や設定不備を悪用

攻撃者は、適切なセキュリティ対策が行な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

他のサービス等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。詳細は個人編 10 位「インターネット上のサービスへの不正ログイン」を参照。

＜事例または傾向＞

◆ **なりすましによる不正ログインで情報漏えい**

2020 年 6 月、カメラのキタムラは通販サイト「カメラのキタムラネットショップ」において、会員になりすましてログインされる不正アクセスがあったと発表した。[1] 氏名、住所、生年月日、電話番号等、約 40 万件の個人情報が閲覧されたおそれがある。なお、不正アクセスに使われたメールアドレス等は当該ネットショップから漏えいしたものではなく、外部で取得したものを使った可能性がある。[2]

◆ **サービスの脆弱性を悪用されて情報漏えい**

2020 年 7 月、人材派遣会社の株式会社アスカにおいて、同社ホームページで派遣の仮登録した個人情報が流出したおそれがあるとの報道がされた。流出した情報は氏名、住所、保育資格の有無等最大約 3 万件であった。攻撃手口は、SQL インジェクションの脆弱性が悪用された可能性が高いとされている。なお、流出した情報はインターネット上の掲示板にアップロードされていることから、金銭目的ではなく愉快犯の犯行の疑いもある。[3]

◆ **組織のデータベースへの不正アクセスによる漏えい**

2020 年 11 月、イベント管理サービス「Peatix」で不正アクセスにより情報漏えいがあったと発表した。氏名、メールアドレス、暗号化されたパスワード等最大 677 万件を不正に引き出されたおそれがある。海外の IP アドレスからデータベースに不正アクセスされたことが原因であるが、不正アクセスの具体的な方法については特定できていない。[4]

＜対策/対応＞

個人（インターネット利用者）

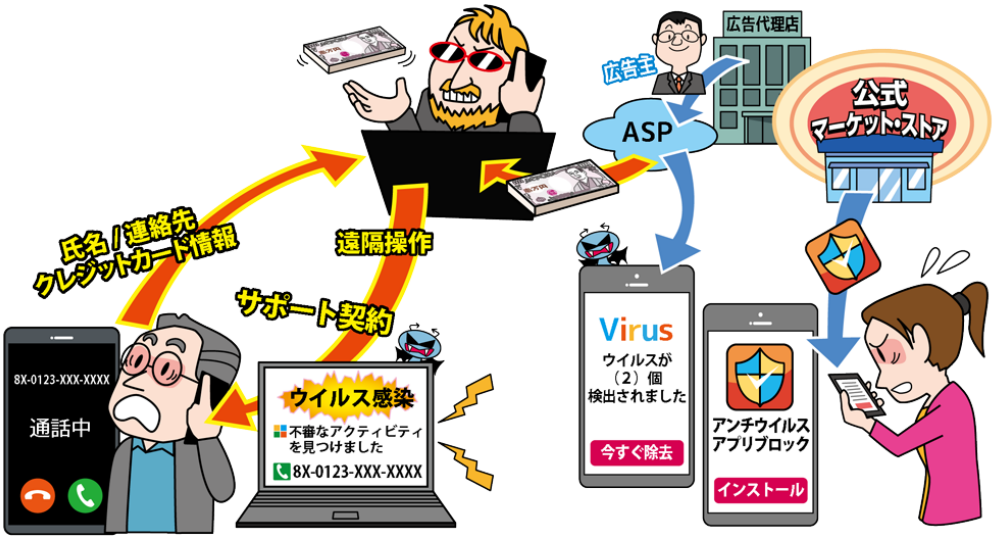
- 情報モラルやリテラシーの向上
  - ・不要な情報は安易に登録しない
    情報漏えいに備えて、サービスを利用するための必須項目以外の情報は登録を避ける。
  - ・パスワードを使いまわさない
  - ・利用していないサービスの退会
  - ・不正ログイン対策
    詳細は個人編 10 位「インターネット上のサービスへの不正ログイン」を参照。
- 被害の早期検知
  - ・クレジットカード利用明細の定期的な確認
    クレジットカード情報が窃取され、不正利用された場合、被害に気づける可能性がある。
- 被害を受けた後の対応
  - ・サービス運営者への問い合わせ
  - ・クレジットカードの停止
    クレジットカード会社へ不正利用の連絡と停止の手続きを行う。
  - ・パスワードの変更
    サービスを継続して利用する場合はパスワードを変更する。
    警察への被害届の提出

参考資料

1. 「カメラのキタムラ ネットショップ」への“なりすまし”による不正アクセス発生について
https://www.kitamura.jp/topics/2020/20200615_01.html
2. 「カメラのキタムラ」通販サイトに不正アクセス 個人情報40万件が閲覧された可能性 二段階認証を採用せず
https://www.itmedia.co.jp/news/articles/2006/15/news138.html
3. 人材派遣のアスカが最大3万件の個人情報を流出…1カ月以上も周知せず
https://president.jp/articles/-/36907?page=1
4. 弊社が運営する「Peatix」への不正アクセス事象に関する第三者調査機関による調査結果のご報告と今後の対応について
https://announcement.peatix.com/20201216_ja.pdf

8位 偽警告によるインターネット詐欺

～突然の警告は本物？慌てず、焦らず、落ち着いて～



PC やスマートフォンからインターネット上で検索した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、攻撃者が用意したサポート窓口に電話を掛けさせて遠隔操作や有償サポート契約を結ばせたりする被害（サポート詐欺）が発生している。偽警告は利用者の不安を煽り、その不安につけこんでくる。

＜攻撃者＞

- 組織的犯行グループ

＜被害者＞

- 個人（インターネット利用者等）

＜脅威と影響＞

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

指示に従ってしまうと不審なソフトウェアのインストールや購入をしてしまう。また、偽のサポート窓口に連絡をしてしまい、PC の遠隔操作や有償サポート契約を結ばされたりする。スマートフォン利用者であれば、不審なアプリをインストールするように誘導される。さらに、ソフトウェアの購入やサポート契約時に登録した氏名、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等に悪用され、二次被害につながるおそれもある。

＜攻撃手口＞

◆ 巧妙に細工が施された偽の警告画面

閲覧者を騙すためにウェブサイト等に表示される偽警告は、警告内容を信じさせるために実在の企業ロゴを使う場合がある。また、警告音を鳴らしたりや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を閉じられないようにし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。

◆ サポート契約詐欺

閲覧者に偽警告の画面に記載されているサポート窓口へ電話をかけさせ、言葉巧みに遠隔操作ツールをインストールさせようとする。その上で、有償のサポート契約やソフトウェアの購入へ誘導する。サポート契約の支払い方法はクレジットカード決済や各種ギフトカード、コンビニ決済、電子マネー等が使われる。[1]

◆　**スマホアプリのインストールへ誘導**

偽警告をスマートフォンの画面に表示し、警告画面に表示された警告の解決方法として、スマホアプリの公式マーケットからスマホアプリをインストールするように誘導する。アプリのインストールへ誘導したことに対してのアフィリエイト収益やサブスクリプション（自動継続課金）による料金請求が目的と考えられる。

＜事例または傾向＞

◆　**有償サポートを断ると遠隔操作で PC をロック**

IPA の安心相談窓口では、2020 年 1 月から 12 月までの 1 年間に、ウイルスを検出したという偽警告の相談が 2,000 件以上寄せられている。[2]

また、偽の警告画面から遠隔操作に誘導し、有償サポートを断ると遠隔操作で PC をロックし、使えないようにする手口も確認されている。遠隔操作では PC の様々な操作を行うことができ、データの閲覧や消去、PC を起動させなくするといった悪質な操作が行なわれる危険が伴う。[3]

◆　**iPhone カレンダーの不審な通知相談が増加**

IPA の安心相談窓口では、「iPhone のカレンダーから、ウイルス感染しているという通知が出る」等の相談が 2020 年に入り急増している。iCloud や iPhone のカレンダーの機能を悪用して他人のカレンダーに書き込みを行う手口であり、カレンダーのイベント詳細に記載された URL をタップしてしまうと、フィッシングサイトへ誘導される。そこで、クレジットカード情報等の個人情報を入力すると、情報を詐取されるおそれがある。[4]

＜対策/対応＞

個人（インターネット利用者等）

- 被害の予防（被害に備えた対策含む）

・表 1.3「情報セキュリティ対策の基本」を実施

・表示される警告を安易に信用しない

・偽警告が表示されても従わない

偽警告によって指示されるアプリやソフトウェアはインストールしない。また、電話は掛けない、遠隔操作は許可しない、契約には応じない。ただし、警告画面には本物もある。警告が本物か偽物かを冷静に判断するため、OS やセキュリティソフトの仕様を把握する（正規の警告を知る）。判断が難しい場合は信頼できる周りの方に相談する。

・偽警告が表示されたらブラウザを終了

・ブラウザの通知機能を不用意に許可しない

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

・身に覚えのないカレンダーは削除

- 被害を受けた後の対応

・ソフトウェアをアンインストール

インストールしたソフトウェアをアンインストールする。できない場合は端末を初期化する。

・虚偽のサポート契約の解消

近くの消費生活センター[5]に相談する。

クレジットカード会社へ連絡

参考資料

1. IPA 安心相談窓口だより 偽のセキュリティ警告によって有償の「ソフトウエア購入」や「サポート契約」をしてしまう相談が増加中
https://www.ipa.go.jp/security/anshin/mgdayori20180718.html
2. IPA 情報セキュリティ安心相談窓口の相談状況［2020年第4四半期（10月～12月）］
https://www.ipa.go.jp/security/txt/2020/q4outline.html
3. IPA 安心相談窓口だより「遠隔操作を他人に安易に許可しないで！」
https://www.ipa.go.jp/security/anshin/mgdayori20201125.html
4. IPA 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！
https://www.ipa.go.jp/security/anshin/mgdayori20200330.html
5.独立行政法人 国民生活センター 全国の消費生活センター等
http://www.kokusen.go.jp/map/index.html

9位 不正アプリによるスマートフォン利用者への被害

～宅配業者を装った SMS にご用心！油断に付け入る不正アプリ～

スマートフォンに意図せず不正アプリをインストールしてしまい、スマートフォン内の情報を窃取されたり、不正操作されたりする被害が発生している。宅配業者等になりすました SMS がスマートフォンに届き、誘導されたサイトから意図せず不正アプリをダウンロードしてしまう事例や、公式マーケット上に通常のアプリに紛れ込ませて不正アプリが公開されている事例等が確認されている。

＜攻撃者＞

- 組織的犯行グループ
- 犯罪者

＜被害者＞

- 個人（スマートフォン利用者）

＜脅威と影響＞

有名な組織等を装った SMS がスマートフォンに届き、SMS に記載された URL を開いた利用者に対して、不正アプリをインストールするよう誘導してくる。コロナ禍における宅配需要の高まりを受けてか、特に宅配業者になりすました SMS が送信されてくる事例が多く確認されており、IPA でも注意喚起を行っている。[1] また、公式マーケット上で、通常のアプリに紛れて不正アプリが公開されており、利用者が知らずにインストールしてしまう場合もある。

不正アプリをスマートフォンにインストールしてしまうと、スマートフォン内に保存されている連絡先や通話記録、位置情報等の情報を窃取されるおそれがある。また、SMS を送信する踏み台に利用され、意図せず不正な SMS を他者に送信してしまうといった被害も確認されている。

＜攻撃手口＞

◆ **SMS 等を利用して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し、SMS 等を送信してダウンロードサイトに誘導、ブラウザの更新や実在の組織等を装って利用者に誤認させ、インストールさせる。

◆ **公式マーケットに不正アプリを紛れ込ませる**

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

＜不正アプリによるスマートフォンの悪用例＞

- 連絡先等の端末内の重要な情報を窃取
- DDoS 攻撃や悪意のある 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
- 仮想通貨のマイニングに利用

＜事例または傾向＞

◆ **宅配業者の不在通知を装った SMS から不正アプリのダウンロードサイトに誘導**

宅配業者になりすました SMS が届き、本文に記載された URL にアクセスすると、ブラウザアプリ「Chrome」を装って利用者に不正アプリをインストールさせる手口が確認されている。アプリをインストールすると、金融機関を装ったポップアップが表示され、更新手続きをするよう誘導される。[2]

また、宅配荷物の不在通知の SMS を受け、リンクを開き、不正アプリをインストールすることで、意図せず他者を騙す多数の SMS の送信に悪用されていたという被害事例も確認されている。なお、本事例では高額な通信料を請求されるといった二次被害を受けていた。[3]

◆ **公式マーケット上で公開されていた偽クリーナーアプリ**

Google Play 上で公開されていたスマートフォンの機能向上等をうたう（不要なファイルやプロセスを削除したり整理したりすることで機能向上をうたう）クリーナーアプリに不正アプリが含まれていた。対象の不正アプリは、国内でも数多くダウンロードされていることが確認されており、インストールした場合、利用者になりすまし、広告主から不正に広告費を奪うモバイル広告詐欺を行ったり、別の不正アプリをダウンロードして感染させようとしたりする。また、Google Play のアプリ評価に投稿し、不正アプリが高評価となるように操作しようとする挙動も見られた。このため、高評価だからと安易に信用せず、慎重に信頼できるアプリか判断することが利用者には求められる。対象の不正アプリは現在、Google Play 上から削除されている。[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

・アプリの真偽を慎重に見極める

公式マーケット以外からは基本的にインストールしない。公式マーケットのアプリの場合でも、レビュー評価やダウンロード数を鵜呑みにせず、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、信頼できるアプリなのかを総合的に判断する。

・アクセス権限の確認 [1]

アクセス権限の確認の際に、アプリの機能に対して適切かどうか確認を行い、アプリの動作に関係がないと思われる権限が要求されている場合は、当該アプリをインストールしないことが望ましい。特にデバイス管理者になる権限を要求している場合は注意が必要である。

・アプリインストールに関する設定に注意

Android スマートフォンの設定で提供元不明のアプリのインストールを許可しない。

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」を不用意に「信頼」しない。

・不要なアプリをインストールしない

アプリの機能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。

- 被害を受けた後の対応

・不正アプリのアンインストール

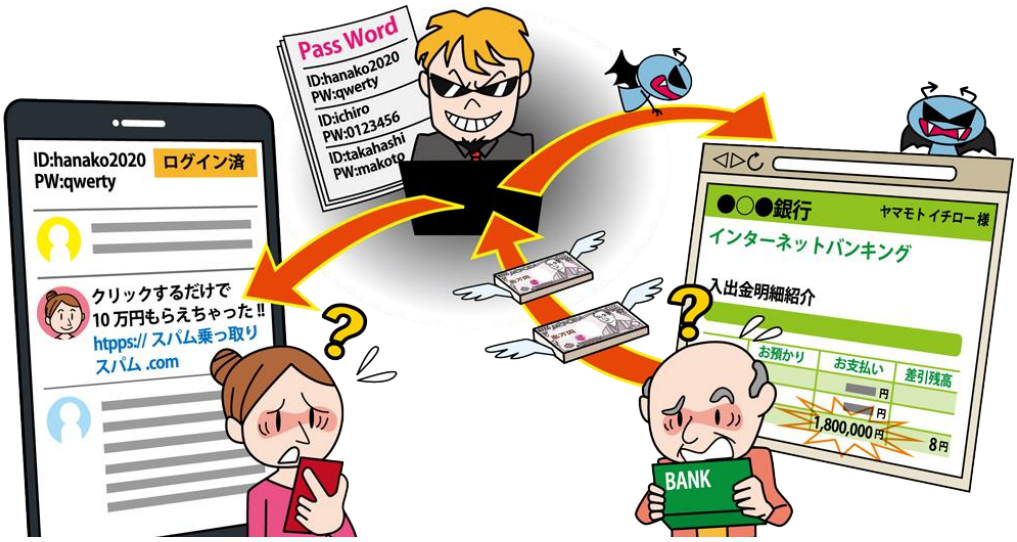
・不正アプリをアンインストールする。できない場合は端末を初期化する。

参考資料

1. 宅配便業者をかたる偽ショートメッセージに引き続き注意！
https://www.ipa.go.jp/security/anshin/mgdayori20200220.html
2. 配送業者などを装った不審なメールに関するご注意
https://www.softbank.jp/mobile/info/personal/news/support/20201005a/
3. 宅配便業者を装った「不在通知」の偽SMSに注意しましょう－URLにはアクセスしない、ID・パスワードを入力しない！－
http://www.kokusen.go.jp/news/data/n-20201126_2.html
4. 国内で過去3カ月間に約5万件の感染被害、不正活動を行う偽クリーナーアプリ
https://is702.jp/news/3636/partner/97_t/

10位 インターネット上のサービスへの不正ログイン

～不正ログインによる大きな金銭的被害や個人情報漏えいのおそれ～



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

＜攻撃者＞

- 組織的犯行グループ
- 犯罪者（愉快犯、ストーカー等）

＜被害者＞

- 個人（サービス利用者）
- 組織（サービス運営者）

＜脅威と影響＞

インターネット上のサービスに対して不正に入手した ID やパスワードを使い、不正ログインを行う攻撃が行われている。ID やパスワードは、別のサービスから漏えいしたものを使う以外にも、被害者が使いそうなものを推測している。

不正ログインされると、サービスに応じた被害を受ける。ショッピングサイトであれば、氏名、住所、電話番号やサイトに登録しているクレジットカード等の情報を窃取されたり、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、金銭を取り扱うサービスの場合、不正に出金操作をされ、金銭被害に遭うおそれがある。さらに、LINE 等の SNS であれば、プライベートな写真やメッセージのやりとり等を覗き見される場合や、不正な広告やフィッシング詐欺に用いられる URL を投稿され、更に他社へ被害が拡大するおそれがある。

＜攻撃手口＞

◆ パスワードリスト攻撃

不正に入手した ID とパスワードのリストを使用し、これら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 ID とパスワードを使いまわしていると、1 つのサービスで ID とパスワードが流出した場合、それら全てのサービスでログインされるおそれがある。

◆ パスワード推測攻撃

使われやすいパスワードを推測し、そのパスワードでログインを試みる。また、芸能人や知人等の個人情報（氏名、誕生日等）からパスワードを推測して、ログインを試みる。

英単語（password、iloveyou）、数字の羅列（123456、111111）、キーボードの配列（qwerty、asdfgh）等の推測が容易なパスワードを利用している場合や、英字、数字、記号を組み合わせたパスワードにおいても、推測が容易なもの [1] である場

合（P@ssw0rd、Sato_0115）、被害を受けるおそれがある。また、SNS 等で公開されている個人に関連する情報（誕生日やメールアドレス等）をヒントにパスワードを推測することもある。

◆ **ウイルス感染**

サービスの利用者に悪意のあるウェブサイトやメールに添付されたファイルを開かせることで、使用している端末をウイルスに感染させる。その後、利用者がその端末でサービスにログインすることで、その時入力した ID やパスワードを窃取し、その認証情報で不正ログインする。

＜事例または傾向＞

◆ **不正ログインによる出金機能の悪用**

2020 年 9 月、証券会社の SBI 証券が運営する証券取引サイトにおいて、パスワードリスト攻撃と思われる攻撃による不正ログインが行われ、約 1 億円の不正送金が発生した。利用者から「身に覚えのない取引がある」とする旨の申告を受け、調査を行った結果、不正ログインが発覚した。SBI 証券は既に発生した被害については補償を行うとしている。[2]

◆ **共通で使える ID を悪用した不正ログイン**

2020 年 4 月、ゲームメーカーの任天堂は自社のアカウントサービス「ニンテンドーネットワーク ID」における不正ログインの被害についての発表を行った。この「ニンテンドーネットワーク ID」を利用して「ニンテンドーアカウント」にログインする「かんたんログイン」を悪用した不正ログインも多数確認されている。この不正ログインによって約 30 万アカウント分の個人情報が閲覧されたおそれがある。[3]

◆ **LINE における乗っ取り被害**

2020 年 2 月、約 4000 人分の LINE アカウントが不正ログインの被害を受け、不正にメッセージやタイムライン投稿が行われた。投稿には購買誘導をするスパム投稿の他、フィッシング詐欺のための URL が含まれていた。[4]

＜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
  - ・添付ファイルや URL を安易にクリックしない
  - ・強い認証方式の利用
    ワンタイムパスワード、二要素認証等の強い認証方式が提供されている場合は利用する。[5]
  - ・パスワードは長く、複雑にする
  - ・パスワードを使いまわさない
    固有のIDを使用しないサービス（メールアドレスを使用する等）においては特に注意する。
  - ・パスワード管理ソフトの利用
  - ・フィッシングに注意
    詳細は個人編 2 位「フィッシングによる個人情報等の詐取」を参照
  - ・利用していないサービスからの退会
- 被害の早期検知
  - ・利用しているサービスのログイン履歴の確認
  - ・クレジットカードやポイント等の利用履歴の定期的な確認
- 被害を受けた後の対応
  - ・パスワードの変更
  - ・クレジットカードの停止
  - ・サービスの運営者へ連絡

参考資料

1. 使ってはいけないダメなパスワードTop200発表 - 2020年版
https://news.mynavi.jp/article/20201124-1520971/
2. 悪意のある第三者による不正アクセスに関するお知らせ
https://www.sbisec.co.jp/ETGate/WPLETmgR001Control?OutSide=on&getFlg=on&burl=search_home&cat1=home&cat2=corporate&dir=corporate&file=irpress/prestory200916_02.html
3. 「ニンテンドーネットワークID」に対する不正ログイン発生のご報告と「ニンテンドーアカウント」を安全にご利用いただくためのお願い
https://www.nintendo.co.jp/support/information/2020/0424.html
4. LINEへの不正ログインに対する注意喚起
https://linecorp.com/ja/security/article/251
5.不正ログイン対策特集ページ
https://www.ipa.go.jp/security/anshin/account_security.html

コラム：2020 年も引き続き猛威を振るった Emotet、今後は・・・

2019 年秋頃より日本で感染拡大が確認された Emotet と呼ばれるウイルスに感染させようとするメールが、2020 年も引き続き観測されました。Emotet に感染すると、他組織とのメールやり取りやメールアカウント情報等の窃取に加え、他のウイルスにも感染させられてしまいます。これにより、10 大脅威の中で解説してきた様々なウイルス感染の手口の足掛かりとして使われてしまうおそれがあります。Emotet に感染すると標的型攻撃やビジネスメール詐欺等、様々な被害に繋がるおそれがあり、組織にとっては適切な対応が求められます。本コラムでは Emotet の感染の手口や対策について解説します。[1,2,3]

【感染拡大の手口】

攻撃者は Emotet に感染させるために受信者にメールの添付ファイルやメール本文内のリンクを開かせ、Word ファイル等を開かせます。さらに、ファイル内でマクロを有効化（コンテンツの有効化）するように誘導してきます。受信者がマクロを有効化してしまうと Emotet に感染します。この一連の流れを行うために巧妙な手口が使われます。

■正規のメールへの返信を装う手口

過去取引先に返信したメールをそのまま引用し、取引先が返信してきたかのようなメールが送られてきます。メールの添付ファイルやリンクを開くと Office 等のロゴと共に英語でコンテンツの有効化を誘導するような内容が記載されています。また、無害な正規のファイルを一緒に添付してくることもあります。

■新型コロナウイルスに便乗した手口

メールのタイトルや本文で新型コロナウイルスに関する情報を発信しているかのように装い添付ファイルやリンクを開かせて、ウイルスに感染させようとします。

■パスワード付き ZIP ファイルを添付した手口

パスワード付き ZIP ファイルを添付し、パスワードを入力させて ZIP ファイルを展開させた上でファイルを開かせることで、ウイルスに感染させようとします。パスワード付き ZIP ファイル使用することによって、添付ファイルを暗号化してメール配送経路上でのセキュリティ製品の検知・検疫をすり抜けやすくし、最終的にメールを受信者に届ける確率を高める狙いで攻撃者に使用されます。

■日本国内の時期や状況から興味を引きやすい内容を記載する手口

例えば、12 月にメールのタイトルや本文で「賞与」、「クリスマス」等と装い添付ファイルやリンクを開かせて、ウイルスに感染させようとします。

■業務に関わる内容を記載する手口

例えば、メールのタイトルや本文で「請求書」や「会議」等と装い添付ファイルやリンクを開かせて、ウイルスに感染させようとします。

【対策】

組織の人員は受信したメールについて以下の点を注意しましょう。

- 身に覚えのないメールの添付ファイルは開かず、メール本文中の URL リンクはクリックしない
- 自分が送信したメールへの返信に見えるメールであっても、不自然な点があれば添付ファイルは開かない
- 信頼できるメール以外は、マクロやセキュリティに関する警告が表示された場合、「マクロを有効にする」「コンテンツの有効化」というボタンはクリックしない　等

また、組織のシステム管理者・セキュリティ管理者は従業員が Emotet の被害に遭わないために事前に以下の対応をとりましょう。

- 従業員に Emotet への注意喚起を実施する
- 業務に利用する PC の OS やソフトウェアを最新にアップデートする
- Word マクロの自動実行をグループポリシー等で無効化する
- メールセキュリティ製品を導入する
- SPF、DKIM、DMARC 等のメール送信者認証を導入する　等

なお、Emotet への感染が疑われる場合は以下の対応をとりましょう。

- Emotet の感染有無をチェックできるツールを利用する [4]
- 感染した疑いのある PC を組織のネットワークから隔離する
- 利用していたメールアカウントや感染が疑われる PC で利用していたアカウント全般のパスワードを変更する　等

【最後に】

2020 年は Emotet に感染させるメール攻撃について、2 月上旬から観測されない状況となっていましたが、7 月より攻撃が観測されるようになり、12 月時点でも引き続き確認されていました。また、時期を追うごとに巧妙に手口を変え、Emotet へ感染させようとしてきました。一方、2021 年 1 月、EUROPOL（欧州刑事警察機構）より Emotet のボットネットをテイクダウンしたとの発表がありました。[5] さらに、ボットネットの遠隔操作を行うサーバー（C&C サーバー）の制御を取得したともされており、世界的に猛威を振るった Emotet の終焉につながる可能性があります。しかし、Emotet に感染させる攻撃は一旦収まったとしても、何かのタイミングでボットネットが復活して攻撃が再開されたり、今後新しいウイルスが拡散されたりするおそれがあります。組織においては日頃から攻撃に備えた対応が求められます。

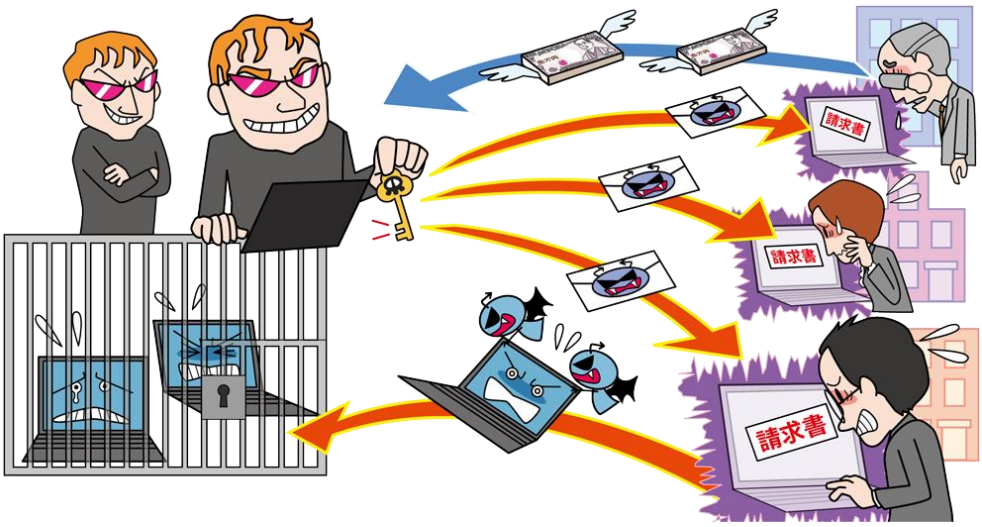
参考資料

1. 「Emotet」と呼ばれるウイルスへの感染を狙うメールについて
https://www.ipa.go.jp/security/announce/20191202.html
2. Emotet への対応 FAQ
https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html
3. マルウエア Emotet の感染に関する注意喚起
https://www.jpcert.or.jp/at/2019/at190044.html
4. JPCERTCC / EmoCheck
https://github.com/JPCERTCC/EmoCheck/releases
5. WORLD'S MOST DANGEROUS MALWARE EMOTET DISRUPTED THROUGH GLOBAL ACTION
https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

2. 情報セキュリティ 10 大脅威（組織）

1位 ランサムウェアによる被害

～組織を狙ったランサムウェアの攻撃が増加～



ランサムウェアとはウイルスの一種で、PC やサーバー、スマートフォンがこのウイルスに感染すると、保存されているデータが暗号化されて利用できなくなったり、画面がロックされて端末が利用できなくなったりする。そしてそれを復旧することと引き換えに金銭を要求される等の被害が発生する。また、データの暴露を行うと脅迫され、金銭の支払い有無にかかわらず、データが暴露されてしまったケースが近年発生している。

＜攻撃者＞

- 組織的犯行グループ
- 犯罪者

＜被害者＞

- 個人
- 組織

＜脅威と影響＞

PC やスマートフォンのデータを暗号化し、データを復旧することと引き換えに、金銭を要求したりコンタクトを促したりする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感染が確認されている。ランサムウェアは、メールの添付ファイルを開いたり、ソフトウェアの脆弱性等を悪用されたりすることで感染する。

また、ランサムウェアにより暗号化したデータを復旧するための金銭要求に加え、暗号化する前にデータを窃取しておき、支払わなければデータを公開する等と脅迫する「二重の脅迫（double extortion）」と呼ばれる攻撃も確認されている。

近年、個人よりも多額の金銭の支払いを見込めるためか、組織が狙われやすい傾向にある。

脅迫に従うことによる金銭的被害に加え、暗号化および窃取されたデータが組織にとって重要な情報であった場合、業務の遂行に大きな支障が出たり、個人情報漏えいによる信用の失墜や経済的損失につながったりするおそれがある。なお、金銭を支払ってもデータが復旧されるとは限らない。

＜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

脆弱性等を悪用しランサムウェアをダウンロードさせるよう改ざんした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。

◆　脆弱性によりネットワーク経由で感染させる

ソフトウェアの脆弱性が未対策のままインターネットに接続されている PC 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**

外部公開しているサーバーにリモートデスクトップ等で不正ログインしランサムウェアに感染させる。

＜事例または傾向＞

◆　**暗号化に加え、情報を暴露すると脅し**[1]

2020 年 11 月、ゲームメーカーのカプコンが不正アクセスされた。社内のデータが盗まれ、さらに社内システムのデータを暗号化され、メールやファイルサーバーが使えなくなる等、一時業務停止に追い込まれた。盗みだされた可能性のある個人情報は顧客や株主情報等最大 39 万件[2]であった。さらに攻撃者は、盗んだ情報をネット上に暴露すると脅し、暗号化解除と暴露の取り止めを引き換えに身代金を要求した。

◆　**特定の組織に特化したランサムウェア**

2020 年 6 月、自動車メーカーのホンダがサイバー攻撃を受け、大規模システム障害を起こした。国内外の工場で生産や出荷が一時止まり、従業員の PC が使えなくなる等オフィス系のネットワークシステムにも影響が出た。使われたとされるランサムウェアを解析すると、ホンダのネットワークでしか動作しないよう作り込まれ、特定の企業を狙う標的型に進化していたものと推測される[3]

◆　**新たなランサムウェア「Avaddon（アヴァドン）」**

2020 年も引き続き、ランサムウェアは新たな攻撃手法が生み出されたり、標的対象を変化させたり等、大きな脅威となっている。近年、Avaddon と呼ばれる新たなランサムウェアが確認されており、不正ファイルとして JavaScript が使われている。[4]

＜対策/対応＞

組織（経営者層）

- 組織としての体制の確立
  - ・対策の予算の確保と継続的な対策の実施

組織（システム管理者、従業員）

- 被害の予防
  - ・表 1.3「情報セキュリティ対策の基本」を実施
  - ・バックアップの取得

    3-2-1 バックアップルールを参考にバックアップを検討する。また、バックアップから復旧できることを定期的に確認する。
  - ・迅速かつ継続的に対応できる体制（CSIRT 等）の構築
  - ・受信メールやウェブサイトの十分な確認
  - ・添付ファイルやリンクを安易にクリックしない
  - ・不審なソフトウェアを実行しない
  - ・サポート切れの OS の利用停止、移行
  - ・アプリケーション許可リストの整備
  - ・フィルタリングツール（メール、ウェブ）の活用
  - ・ネットワーク分離
  - ・共有サーバー等へのアクセス権の最小化と管理の強化
  - ・公開サーバーへの不正アクセス対策
- 被害を受けた後の対応
  - ・CSIRT 等所定の連絡先への連絡
  - ・バックアップからの復旧
  - ・復号ツールの活用[5]
  - ・影響調査および原因の追究、対策の強化
  - ・迅速な隔離を行い、関連組織、取引先への被害拡大の防止

＜例外措置＞

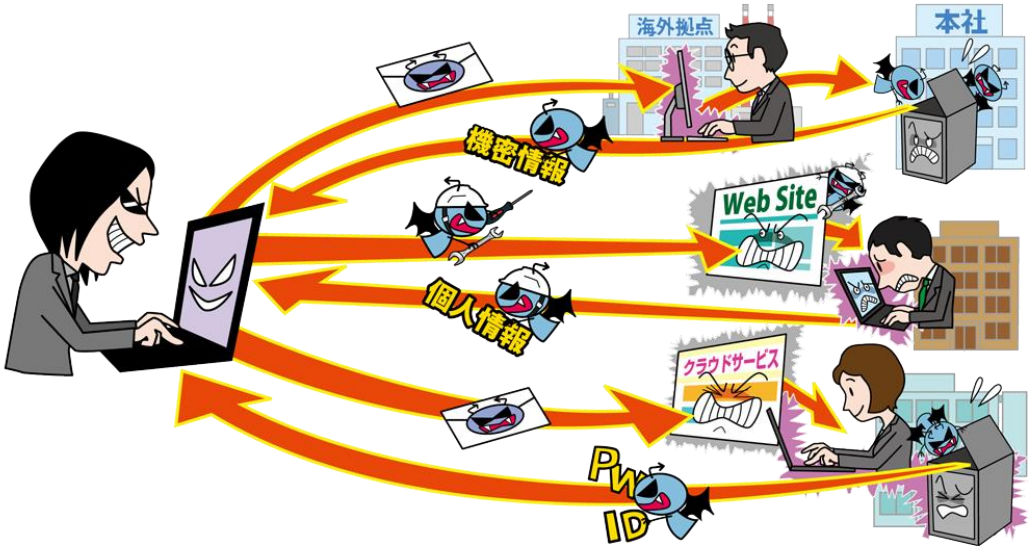
- ・推奨はされないが金銭を支払う（暗号化されたファイルが人命に関わる場合等）

参考資料

1. 暗号化と暴露で11億円を要求、カプコン襲った「二重脅迫型」ランサムウェアの脅威
https://xtech.nikkei.com/atcl/nxt/column/18/00989/112400040/
2. 不正アクセスによる情報流出に関するお知らせとお詫び【第3報】
https://www.capcom.co.jp/ir/news/html/210112.html
3. ホンダを標的に開発か、ランサムウェア「EKANS」解析で見えた新たな脅威
https://xtech.nikkei.com/atcl/nxt/column/18/00989/062400028/
4. 2020年上半期ランサムウェア動向拾遺：「Avaddon」、新たな回避手法、業界別被害事例、など
https://blog.trendmicro.co.jp/archives/26021
5. The No More Ransom Project
https://www.nomoreransom.org/

2位 標的型攻撃による機密情報の窃取

～新型コロナウイルスの影響に便乗した標的型攻撃メールを観測～



企業や民間団体そして官公庁等、特定の組織から機密情報等を窃取することを目的とした標的型攻撃が継続して発生している。攻撃者は新型コロナウイルスの感染拡大による社会の変化や、それに伴うテレワークへの移行という過渡期に便乗し、状況に応じた巧みな手口で金銭や機密情報等を窃取する。

＜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（官公庁、民間団体、企業、研究機関、教育機関等）

＜脅威と影響＞

特定の組織の機密情報等の窃取を目的とし、PC にウイルスを感染させることで、組織内部へ潜入する標的型攻撃が確認されている。従業員が悪意あるメールの添付ファイルを開いたり、悪意あるウェブサイトにアクセスしたりすると、PC がウイルスに感染する。攻撃者はウイルスに感染した PC を起点に組織内部のシステムを探索し、侵害範囲を拡大しながら機密情報等の窃取を行う。

漏えいした機密情報等が悪用された場合、組織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組織の活動が妨害されたり、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＞

◆ メールの添付ファイルやリンク

メールの添付ファイルやリンク先にウイルスを仕込み、それらを開かせることで PC をウイルスに感染させる。本文や件名、添付ファイル名は業務に関連するような内容に偽装され、実在する組織の差出人名が使われる場合もある。また、複数回のメールのやりとりで油断させ、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

標的組織が頻繁に利用するウェブサイトを調査し、ウェブサイトを改ざんする。従業員がそのウェブサイトにアクセスするよう誘導することで、PC がウイルスに感染する。（水飲み場型攻撃）

◆ 不正アクセス

標的組織が利用するクラウドサービスやウェブサーバーの脆弱性を悪用して不正アクセスし、認証情報等を窃取する。窃取した認証情報等を悪用して正規の経路で組織内部のシステムへ侵入し、PC やサーバーをウイルスに感染させる。

＜事例または傾向＞

◆ **複数の組織における標的型攻撃と思われる不正アクセス報道**

2020 年 1 月、日本電気は防衛事業部門のサーバーが不正アクセスを受けたことを公表した。2016 年 12 月以降に行われた攻撃を検知できておらず、27,445 件のファイルに対して不正アクセスが行われたが、情報流出等の被害は確認されていない。[1]

また、2020 年 12 月、川崎重工は外部からの不正アクセスを受けたことを公表した。2020 年 6 月以降、複数の海外拠点と国内拠点間で不審な通信を確認したことで発覚した。同社によれば、攻撃は痕跡を残さない高度なものであり、一部情報が外部に流出した可能性があるとしている。[2]

◆ **サイバー攻撃に関する情報共有**

サイバー情報共有イニシアティブ（J-CSIP）によると、2020 年 10 月～12 月の期間で、J-CSIP 参加組織から IPA に対して、サイバー攻撃に関する情報が 479 件寄せられた。その中で IPA が標的型攻撃メールとみなした情報は 16 件であった。11 月にはウイルスが添付された日本語の不審メールに関する情報提供があった。メールには ZIP ファイルが添付されており、展開すると Excel のアイコンに偽装された EXE ファイルが格納されていた。このファイルを実行すると、遠隔操作ウイルスに感染してしまう。[3]

＜対策/対応＞

組織（経営者層）

- 組織としての体制の確立
  - ・CSIRT の構築
  - ・対策予算の確保と継続的な対策の実施
  - ・セキュリティポリシーの策定

組織（セキュリティ担当者、システム管理者）

- 被害の予防／対応力の向上
  - ・情報の管理とルール策定
  - ・サイバー攻撃に関する継続的な情報収集
  - ・セキュリティ教育の実施
  - ・インシデント発生時の訓練の実施
  - ・統合運用管理ツール等によるセキュリティ対策状況の把握

    統合運用管理ツールを使い従業員や職員が利用する PC のソフトウェア更新状況を管理し、リスクの可視化を行う。
  - ・取引先のセキュリティ対策実施状況の確認
  - ・アプリケーション許可リストの整備
  - ・アクセス権の最小化と管理の強化
  - ・ネットワーク分離
  - ・重要サーバーの要塞化（アクセス制御、暗号化等）
  - ・海外拠点等も含めたセキュリティ対策の向上
- 被害の早期検知
  - ・ネットワーク監視、防御

    UTM、IDS/IPS、WAF 等の導入
  - ・エンドポイントの監視、防御
- 被害を受けた後の対応
  - ・CSIRT の運用によるインシデント対応
  - ・影響調査および原因の追究、対策の強化
  - ・関係者、関係機関への連絡

    監督官庁、個人情報保護委員会、警察等

組織（従業員、職員）

- 情報リテラシーの向上
  - ・セキュリティ教育の受講

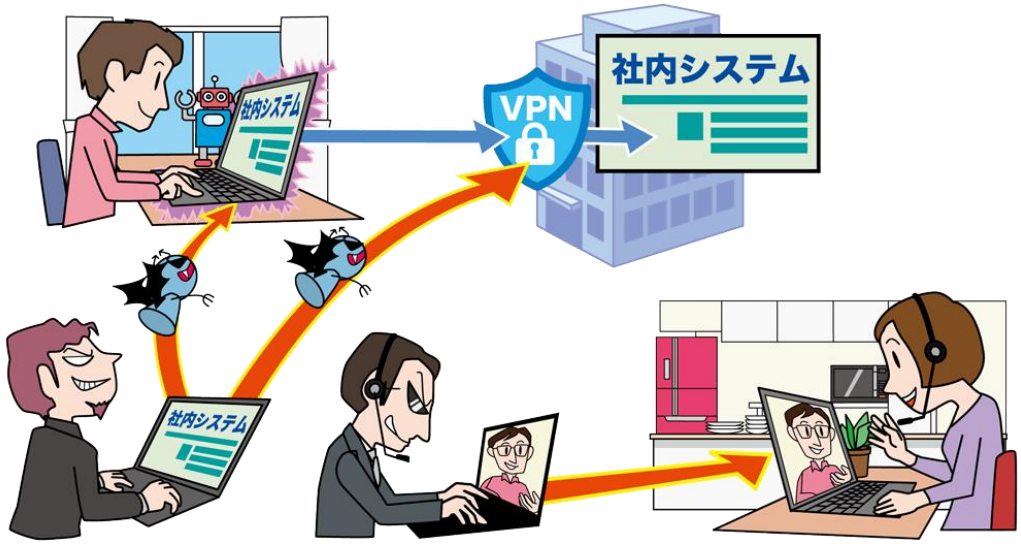
    メールの添付ファイルや URL を安易に開かない。Office ファイルにおいて、可能な場合はマクロを無効化する。被害を受けた際は迅速に連絡する。等
- 被害の予防（通常、組織全体で実施）
  - ・表 1.3「情報セキュリティ対策の基本」を実施
- 被害を受けた後の対応
  - ・CSIRT 等所定の連絡先への連絡

参考資料

1. 当社の社内サーバへの不正アクセスについて
https://jpn.nec.com/press/202001/20200131_01.html
2. 当社グループへの不正アクセスについて
https://www.khi.co.jp/pressrelease/news_201228-1j.pdf
3. サイバー情報共有イニシアティブ（J-CSIP） 運用状況[2020 年 10 月～12 月]
https://www.ipa.go.jp/files/000088288.pdf

3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

～テレワーク環境を意識した対策を～



2020 年は新型コロナウイルス感染症（COVID-19）の世界的な蔓延に伴い、政府機関から感染症対策の一環として日本の組織に対してニューノーマルな働き方の一つであるテレワークが推奨された。組織のテレワークへの移行に伴いウェブ会議サービスや VPN 等の本格的な活用が始まった中、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 年は組織の積極的なテレワークへの移行に伴い、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機会が増えた。また、テレワークのために私物 PC や自宅ネットワークを利用したり、VPN 等のために初めて使うソフトウェアを導入したり、以前までは緊急用として使っていた仕組みを恒常的に使う必要性がでてきた。このような業務環境の急激な変化を狙った攻撃が行われている。

業務環境に脆弱性があると、社内システムに不正アクセスされたり、ウェブ会議をのぞき見されたり、テレワーク用 PC にウイルスを感染させられたりするおそれがある。

＜攻撃手口/発生要因＞

◆ テレワーク用ソフトウェアの脆弱性の悪用

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性を悪用し、ウェブ会議をのぞき見する。

◆ 急なテレワーク移行による管理体制の不備

テレワークで利用している PC 内の OS やソフトウェアのセキュリティ管理を組織側から行うのは難しい。その中で、テレワークへの急な移行によりルール整備やセキュリティ対策のノウハウが不十分なまま利用を開始している。

◆ 私物 PC や自宅ネットワークの利用

私物 PC をテレワークで利用している場合、ウェブサイトや SNS にアクセスしたり、私物のソフトウェアをインストールしたり等の私的利用をすることがある。その際、PC がウイルスに感染したり、攻撃者にソフトウェアの脆弱性を悪用され、テレワーク用の認証情報等を窃取されたりするおそれがある。

また、組織支給の PC を利用している場合でも、適切なセキュリティ対策が行われていない自宅ネットワークを利用することで組織の適切なセキュリティ対策が適用されず、PC がウイルスに感染する等のおそれがある。

＜事例または傾向＞

◆ **脆弱性の悪用により VPN のパスワード流出**

2020 年 8 月、VPN 製品の脆弱性が悪用されて窃取された認証情報約 900 件がインターネット上で公開されていることが判明した。なお、悪用された脆弱性は 2019 年 4 月にアドバイザリが公開されており、更新プログラムを適用していない VPN 製品が狙われた。[1]

◆ **テレワーク中にウイルス感染、社内に拡大**

2020 年 4 月、テレワーク中の従業員が社有 PC で社内ネットワークを経由せずに外部ネットワークに接続し、SNS を利用した際にウイルスに感染した。その後、当該従業員が出社した際に当該 PC を社内ネットワークに接続したところ社内ネットワークにウイルス感染が拡大した。[2]

◆ **Zoom に非公開会議へアクセスできる脆弱性**

2020 年 7 月、ウェブ会議サービスの Zoom に、特定の状況下において数分で非公開の Zoom 会議へアクセスできる脆弱性があったと発表された。Zoom 会議へアクセスする際に使うデフォルトのパスワードは 6 桁数字であり、パスワードの候補は最大で 100 万個ほどであった。当時、特定のアクセス方法を行うことでパスワード施行回数の制限を回避できる状況だったため、100 万回ほどの試行でログインされるおそれがあるというものであった。なお、当該脆弱性は、Zoom 社が報告を受けた 4 月に修正されている。[3]

＜対策/対応＞[4]

組織（テレワーカー）

- 情報リテラシーや情報モラルの向上
  - ・セキュリティ教育の受講
- 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ルールを遵守（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
  - ・CSIRT への連絡

組織（経営者層）

- 組織としての体制の確立
  - ・CSIRT の構築
  - ・対策予算の確保と継続的な対策の実施
  - ・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）

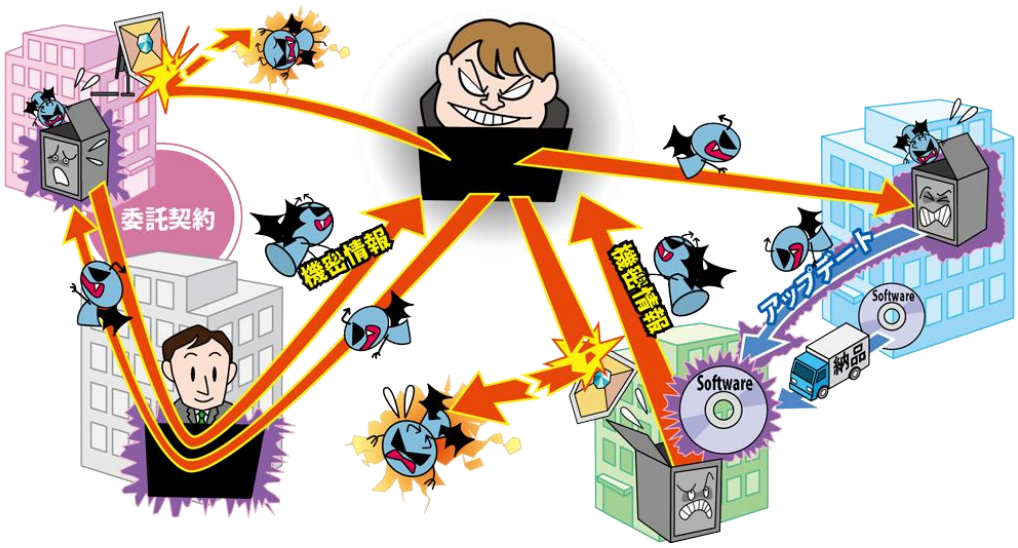
- 被害の予防（被害に備えた対策含む）
  - ・シンクライアント、VPN、ZTNA 等のセキュリティに強いテレワーク環境の採用
  - ・テレワークの規程や運用ルールの整備
    組織支給 PC と私物 PC の違いも考慮する必要がある。
  - ・セキュリティ教育の実施
  - ・テレワークで利用するソフトウェアの脆弱性情報の収集と周知、対策状況の管理
  - ・セキュリティパッチの適用（VPN 装置、ネットワーク機器、PC 等）
- 被害の早期検知
  - ・適切なログの取得と継続的な監視
  - ・ネットワーク監視、防御
    UTM・IDS/IPS 等の導入
- 被害を受けた後の対応
  - ・CSIRT の運用によるインシデント対応
  - 影響調査および原因の追究、対策の強化

参考資料

1. VPN認証情報漏洩に見る脆弱性対策を浸透させる難しさ
https://www.security-next.com/117811
2.在宅勤務時 SNS経由で社用PCが感染、社内ネットワーク接続で被害拡大（三菱重工業）
https://scan.netsecurity.ne.jp/article/2020/08/14/44439.html
3. オンライン会議ツールのZoomに「攻撃者がわずか数分で非公開の会議にアクセスできる脆弱性」があったとの報告
https://gigazine.net/news/20200730-zoom-cracking-private-meeting-passwords/
4. テレワークにおけるセキュリティ確保
https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

4位 サプライチェーンの弱点を悪用した攻撃

～自組織の対策だけでは不十分？広がるサプライチェーンを悪用した攻撃被害～



原材料や部品の調達、製造、在庫管理、物流、販売までの一連の商流、およびこの商流に関わる複数の組織群をサプライチェーンと呼ぶ。このサプライチェーンの関係性を悪用し、セキュリティ対策の強固な企業を直接攻撃するのではなく、その企業が構成するサプライチェーンのセキュリティが脆弱な取引先等を標的とする手口がある。取引先が攻撃されると取引先が保有する企業の機密情報が漏えいしたり、取引先を足掛かりとされ、本来の標的である企業が攻撃を受けたりする被害が発生する。

＜攻撃者＞

- 組織的犯行グループ
- 犯罪者

＜被害者＞

- 組織（自組織、自組織の商流に関わる組織）

＜脅威と影響＞

組織には、必ず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、取引先であったり、委託先であったり、導入しているソフトウェアであったりと多岐にわたる。直接攻撃することが困難な組織に対しそのサプライチェーンの脆弱な部分を攻撃することで、間接的または段階的に標的の組織を狙ってくる。外部に対しては強固なセキュリティ対策を行っている組織でも取引先等のサプライチェーン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**

標的となる組織よりもセキュリティが脆弱な委託先等を攻撃し、その組織が委託業務において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等を攻撃し、標的を攻撃するための足掛かりとする**

ソフトウェアの開発元等を攻撃し、ソフトウェアのアップデートにウイルスを仕込む。その後、開発元から公開されたアップデートを適用した利用者がウイルスに感染し、そのウイルスを介して標的組織に侵入する。

＜事例または傾向＞

◆　中国拠点を足掛かりに国内拠点へ侵入

2020 年 2 月、三菱電機は、2019 年に発生した情報流出に関する調査結果の第 3 報を公開した。その資料によると、攻撃者は同社の中国拠点のサーバーにゼロデイ攻撃を仕掛けウイルスに感染させることで、拠点内の他の端末へと侵入範囲を拡大していった。その後、中国拠点を足掛かりに国内拠点に侵入し、中国拠点と同様に感染を拡大させていった。最終的に感染の疑いのある端末は国内外含め 132 台であった。

一連の攻撃は、既存の防御をすり抜ける高度かつ巧妙な手法が用いられており、三菱電機はこのような高度な標的型攻撃にも対処していけるように、これまで以上に多層防御態勢を整備していくとしている。[1]

◆　ソフトウェアの正規のアップデートにバックドア

2020 年 12 月、SolarWinds は同社のソフトウェア「Orion Platform」にバックドアが含まれていたことを公表した。攻撃者によって「Orion Platform」のアップデートファイルにバックドアが組み込まれ、SolarWinds から配信されたそのアップデートファイルで更新をした組織が感染した。

主に米国を中心に感染が確認され、米政府をはじめ様々な組織で被害が報告されている。また、国内でも感染の形跡が確認されている。感染した組織は、バックドアから攻撃者に侵入され、不正アクセスを受けたとする報告が多くされている。[2,3]

＜対策/対応＞

組織

- 被害の予防
  - ・業務委託や情報管理における規則の徹底

製造においては原材料や部品の調達経路、物流経路等も考慮する。

- ・報告体制等の問題発生時の運用規則整備

攻撃を受けた場合を想定し、インシデント対応計画等を整備することも重要である。

- ・信頼できる委託先、取引先組織の選定

商流に関わる組織の信頼性評価や品質基準を導入する。

- ・複数の取引先候補の検討
- ・納品物の検証
- ・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

委託元組織が責任をもって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
  - ・影響調査および原因の追究、対策の強化
  - ・被害への補償

組織（商流に関わる組織）

- 被害の予防
  - ・セキュリティの認証取得

    ISMS、P マーク、SOC2、ISMAP 等
  - ・公的機関が公開している資料の活用

    -「サプライチェーンのセキュリティ脅威に備える」[4]（IPA）

    -「サイバーセキュリティ経営ガイドライン」[5]（経済産業省／IPA）
- 被害を受けた後の対応

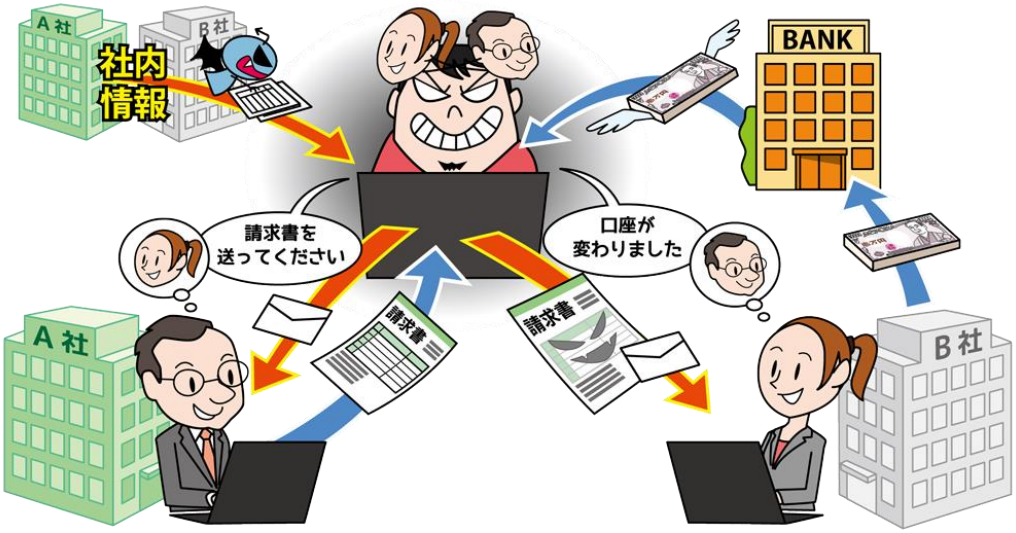
  委託元への連絡

参考資料

1. 不正アクセスによる個人情報と企業機密の流出可能性について（第3報）
https://www.mitsubishielectric.co.jp/news/2020/0212-b.pdf
2. SolarWinds Security Advisory
https://www.solarwinds.com/ja/securityadvisory
3. SolarWindsのサプライチェーン攻撃についてまとめてみた
https://piyolog.hatenadiary.jp/entry/2020/12/20/045153
4. サプライチェーンのセキュリティ脅威に備える
https://www.ipa.go.jp/files/000073868.pdf
5. サイバーセキュリティ経営ガイドライン
https://www.meti.go.jp/policy/netsecurity/mng_guide.html

5位 ビジネスメール詐欺による金銭被害

～その請求書、本物ですか？～



ビジネスメール詐欺（Business E-mail Compromise：BEC）は、巧妙な騙しの手口を駆使した偽のメールを組織・企業に送り付け、従業員を騙して送金取引に関わる資金を詐取する等の金銭被害をもたらすサイバー攻撃である。2020 年は新型コロナウイルス感染症（COVID-19）に関する内容が含まれたビジネスメール詐欺が確認されている。

＜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る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）のメールアドレスは取引先を模したメールアドレスや本物のメールアドレスを使ったり、不自然な日本語が少ないメール本文だったり等、本物のメールと見分けづらいようになっている。

受信者は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。ビジネスメール詐欺は組織内外における金銭の授受を装うため金銭の被害は高額になる傾向があり、組織が被害に遭った際の影響が大きい。

＜攻撃手口＞

◆ 取引先との請求書の偽装

取引先と請求に係るやりとりをメールで行っている際に、攻撃者が取引先になりすまし、攻撃者の用意した口座に差し替えた偽の請求書等を送りつけ、振り込ませる。なお、攻撃者は取引のやりとりや関係している従業員の情報を何らかの方法により入手した上で攻撃している。

◆ 経営者等へのなりすまし

組織の経営者等になりすまし、従業員に攻撃者の用意した口座へ振り込ませる。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、その従業員の取引実績のある組織の担当者へ偽の請求書等を送り付け、攻撃者の用意した口座に振り込ませる。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へなりすまし、組織の財務担当者等に対して攻撃者の用意した口座へ振り込ませる。

◆ **詐欺の準備行為と思われる情報の窃取**

詐欺を実行する前の準備行為として、標的組織の情報を窃取する場合がある。例えば、攻撃者が詐欺の標的とする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＞

◆ **「ビジネスメール詐欺」被害総額 2 億円か**

取引先を装って韓国法人から法人名義の銀行口座へ入金させ、不正に引き出したとして容疑者 2 人を逮捕した。2 人はビジネスメール詐欺グループの指示役とみられている。グループは約 2 億円の不正引き出しに関与した疑いがある。[1]

◆ **巧妙化する日本語の偽メール、新型コロナウイルスを話題としたメールも**

サイバー情報共有イニシアティブ（J-CSIP）はビジネスメール詐欺の事例と注意喚起を公表した。それによると、詐欺メールは日本語に不自然な点が少ないことから日本語を使える攻撃者がおり、国内組織が本格的に標的になってきている。また、新型コロナウイルス感染症（COVID-19）の話題が利用されたメールも確認されている。[2]

◆ **ビジネスメール詐欺の多くは「取引先との請求書の偽装」**

一般社団法人 JPCERT コーディネーションセンターはビジネスメール詐欺の実態調査について公表した。報告書によると攻撃手口では「取引先との請求書の偽装」が多いが、以下に示すポイントからやり取りの過程で気づくこともできるとしている。[3]

・支払済の請求・請求書の体裁が不自然
・見慣れない地域への送金
・送金先口座の凍結
・不自然なローカル言語 等

＜対策/対応＞

組織

- 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
  - ・ガバナンスが機能する業務フローの構築
    個人の判断や命令で取引や金銭の移動がされないルールやシステムの構築。
  - ・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）

＜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、電話や FAX 等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。
- ・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＞

- ・パスワードの適切な管理やログイン通知機能、二要素認証等の利用

- 被害を受けた後の対応
  - ・CSIRT 等所定の連絡先への連絡
  - ・銀行や警察に相談
  - ・踏み台や詐称されている組織への連絡
  - ・影響調査および原因の追究、対策の強化
    メールアカウントに意図しない転送設定やフォルダー振り分け設定等がないかを確認
  - ・被害（侵害）を受けたメールサーバー上の全メールアカウントのパスワード変更

参考資料

1. 「ビジネスメール詐欺」被害総額2億円か　容疑の70代男ら逮捕
https://www.sankei.com/affairs/news/201013/afr2010130012-n1.html
2. ビジネスメール詐欺「BEC」に関する事例と注意喚起（第三報）
https://www.ipa.go.jp/files/000081866.pdf
3. ビジネスメール詐欺の実態調査報告書
https://www.jpcert.or.jp/research/20200325_BEC-survey.pdf

6位 内部不正による情報漏えい

～内部不正が可能な環境を作らない～

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、組織内における情報管理のルールを守らずに情報を持ち出し、紛失、情報漏えいにつながるケースも散見される。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により、組織に多大な損害を与える。

＜攻撃者＞

- 組織の従業員（在職者、離職者）

＜被害者＞

- 組織
- 個人（顧客、サービス利用者）

＜脅威と影響＞

悪意を持った組織関係者が、組織の保管する技術情報や顧客情報等の重要情報を閲覧、不正に持ち出し、外部へ公開、または競合他社等に売却、漏えいする事で組織に損害を与えることがある。これらは金銭目的や組織への私怨で行われる。また、自宅で作業するために、組織の情報管理のルールを守らずに情報を持ち出し、その情報を紛失してしまい、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機密性、漏えいの規模によっては、組織の社会的信用の失墜や、顧客等に対する損害賠償や補填による経済的損失が発生し、組織の経済的競争力の大幅な低下に繋がる。その結果、組織の経営の根幹を揺るがすインシデントに発展するおそれがある。

＜攻撃手口＞

◆ アクセス権限の悪用

付与された権限を悪用し、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。

◆ 在職中に割り当てられたアカウントの悪用

組織の離職者が、在職中に使用していたアカウントを悪用し、組織内部の情報を窃取する。

◆ 内部情報の不正な持ち出し

組織内部の情報を、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＞

◆ 従業員が金銭目的で情報の持ち出し

2020 年 1 月、ソフトバンクの元社員が、金銭目的で同社の営業機密を含む情報をサーバーから自身が保有する記憶媒体にコピーして持ち出し、不正競争防止法違反の疑いで逮捕された。[1]

◆ **市役所職員による情報流出**

2020 年 5 月、青森県弘前市の職員が、業務に使用していた PC から同市の職員約 2,700 人分の個人情報を地元紙のメールアドレス宛に送信して漏えいさせたことで懲戒免職となった。漏えいした情報は当該 PC の前の利用者が PC のごみ箱に捨てたままにしていたものであり、当該 PC を引き継いだ当職員が見つけ、保存していた。市の情報管理の不備も指摘されている。[2]

◆ **社内評価を高めるため秘密情報の漏えい**

2020 年 10 月、積水化学工業の元従業員が、スマートフォンの画面に使用される素材に関する機密情報を自身の USB メモリーに保存、自宅 PC から電子メールで中国企業に送信し、漏えいしたことにより、不正競争防止法違反容疑で書類送検された。元従業員は社内評価を高めるため、SNS を通じて接触した中国企業の従業員からの技術交換の提案に応じたという。[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

組織全体において、効率的な対策を推進するためには、経営層の積極的な関与が重要となる。内部不正対策は経営者の責任であることを示すとともに、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及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。

・重要資産の把握、体制の整備

重要資産を把握し、重要度に合わせてランク付けを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い不要となった利用者 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。

・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。

- 情報リテラシーや情報モラルの向上

・人的管理及びコンプライアンス教育の徹底

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行い、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。

また、離職者と秘密保持契約等を締結し、離職後の情報漏えいを防止する。

- 被害の早期検知

・システム操作履歴の監視

重要情報へのアクセス履歴及び利用者の操作履歴等のログ、証跡を記録し、定期的に監視する事で早期検知に努める。

- 被害を受けた後の対応

・関係者、関係機関への連絡

・警察への連絡

・CSIRT 等所定の連絡先への連絡

・影響調査および原因の追究、対策の強化

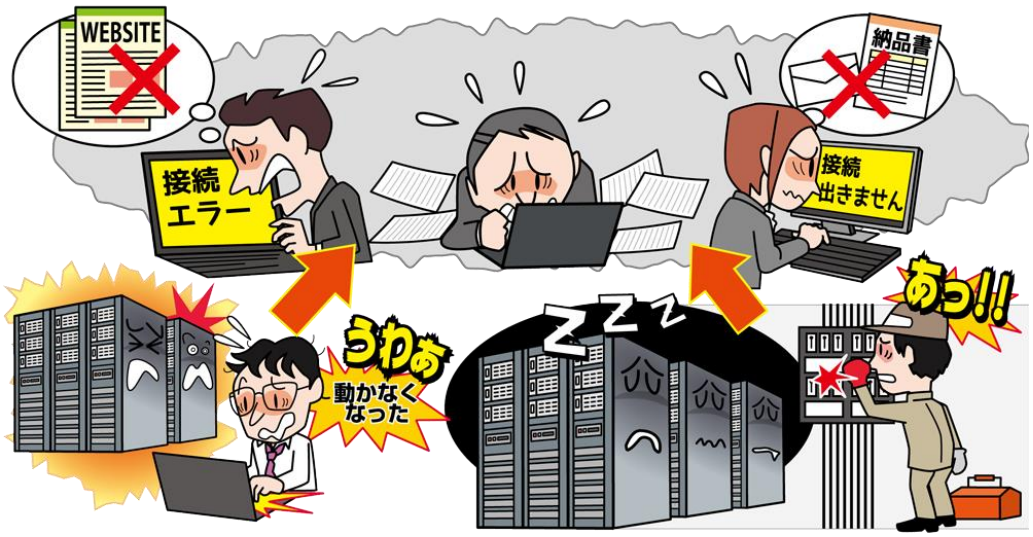
・内部不正者に対する適切な処罰の実施

参考資料

1. ロシアによるスパイ活動か　SB営業秘密を不正入手疑い
https://www.asahi.com/articles/ASN1T72QKN1TUTIL00W.html
2. データ流出で男性主査を懲戒免職／弘前市
http://www.mutusinpou.co.jp/news/2020/06/60112.html
3. 積水化学元社員が情報漏洩疑い　大阪府警が書類送検
https://www.nikkei.com/article/DGXMZO64966730T11C20A0AC8000
4. 組織における不正防止ガイドライン
https://www.ipa.go.jp/security/fy24/reports/insider/

7位 予期せぬ IT 基盤の障害に伴う業務停止

～IT 基盤が停止するおそれがあることを意識する～



組織がインターネット上のサービスや業務システム等で使用しているネットワークやクラウドサービス等の IT 基盤に予期せぬ障害が発生し、長時間にわたり利用者や従業員に対するサービスを提供できなくなるケースがある。IT 基盤の停止はシステムの可用性を侵害する情報セキュリティリスクであり、IT 基盤を利用している組織の事業に大きな影響を与えるおそれがある。

＜当事者＞

- 企業（IT 基盤提供事業者）
- 組織(組織内 IT 基盤設備)

＜被害者＞

- 個人（IT システム利用者）
- 組織（IT システム利用者、IT 基盤利用者）

＜脅威と影響＞

企業や民間団体、官公庁等多くの組織は費用面や運用負担の軽減のため、自社の機器をデータセンターに設置する場合や、クラウドの IT 基盤を利用するケースがある。利用している IT 基盤で、自然災害、データセンターの設備故障や停電、ハードウェア・ソフトウェア障害等により、予期しない障害が発生すると、IT 基盤を利用して外部に提供しているサービスや社内の業務システムが突然停止する。

それにより、組織が提供しているサービスの利用者がそのサービスを利用できなくなったり、組織の業務が停止したりする。長時間停止した場合、組織の利益減少や競争力の弱体化等、経済的損失につながる。また、人々の日常生活にも支障がでるおそれがある。

＜発生原因＞

◆ 自然災害

地震や台風、洪水等の自然現象により、IT 基盤の設備や施設が被害を受け、IT 基盤に障害が発生する。

◆ 作業事故

インフラ設備のメンテナンス作業における人為的ミスにより通信回線断や電力供給断等の事故が発生したり、システムの設定変更作業における作業ミス等によりシステムの正常動作に影響を及ぼしたりすることで、IT 基盤に障害が発生する。

◆ 設備障害

データセンター等、様々なサービスが稼働している施設において、空調設備等の制御システムの障害により、施設内にある機器の稼働環境（温度や湿度等の条件）を維持できなくなり機器が停止し、IT 基盤に障害が発生する。

◆　**ハードウェア・ソフトウェア障害**

IT 基盤を構成する機器のハードウェアに障害が発生したり、OS やソフトウェアに不具合が発生したりすることにより、IT 基盤に障害が発生する。

＜事例または傾向＞

◆　**「Google」システム移行時に大規模障害**

2020 年 12 月、Google がサービスを提供するシステムにおいて障害が発生した。根本的な原因はストレージのクォータ自動管理システムの不備であったが、同年 10 月に実施した Google User ID Service を移行する作業も遠因となっていた。本障害は 50 分ほどで解消したが、ユーザー認証処理を必要とする Google の多数のサービスがアクセス不能に陥り、世界中の数十億のユーザーが Gmail や YouTube などにアクセスできなくなったり、Google のユーザー認証処理を必要とするサードパーティーのサービスも利用できなくなったりするという影響が発生した。[1]

◆　**「AWS」障害で PayPay などに影響**

2020 年 10 月、Amazon Web Services が提供するクラウドサービス「AWS」の一部で障害が発生した。この影響で、スマホ決済サービス「PayPay」や一部のスマートフォンゲーム等が利用しづらい状態になった。また、「Amazon Elastic Compute Cloud（EC2）」の一部でネットワーク接続に問題が発生し、EC2 で利用できるストレージの一部でもパフォーマンスが低下する等の影響が確認された。なお、本障害は、東京にあるデータセンターにて発生したものであった。[2]

◆　**東証の売買システムで NAS 故障による障害**

2020 年 10 月、東証の売買システム「arrowhead」で終日取引停止となる大規模な障害が発生した。[3] 原因は NAS の故障によるものであった。NAS は 2 台の冗長化構成であったため、システム設計上は NAS の 1 台で障害が発生してももう 1 台での縮退運用を行うことで、arrowhead 全体の運用は継続できるようになっていた。ただし、NAS 導入時のファームウェア設定に不備があり、縮退運用への切り替えが正常に動作しなかったことで大規模障害となった。

＜対策/対応＞

組織（IT システム利用者、IT 基盤利用者）

- 被害の予防（被害に備えた対策を含む）

  ・BCM の実践（BCP 策定と運用）[4]

  IT 基盤の様々なトラブルを事前に想定し、対応策を準備しておく。また、事業の継続や早期復旧を可能にするため、行動計画や復旧目標を定め、事業継続計画（BCP）を策定し、運用する。

  ・可用性の確保と維持（システム設計や監視）

  システムの冗長化についても検討する。（クラウド基盤の場合はマルチリージョンのフェイルオーバー構成等）

  ・データバックアップ（復旧対策）

  ・契約や SLA 等を確認

  組織は IT 基盤側との契約や SLA 等を確認しておく。IT 基盤を利用して顧客にサービスを提供する場合は、顧客との契約や SLA 等も確認しておく。

  ・被害を想定し IT 基盤側との事前の連携確認

- 被害を受けた後の対応

  ・BCP に従った対応

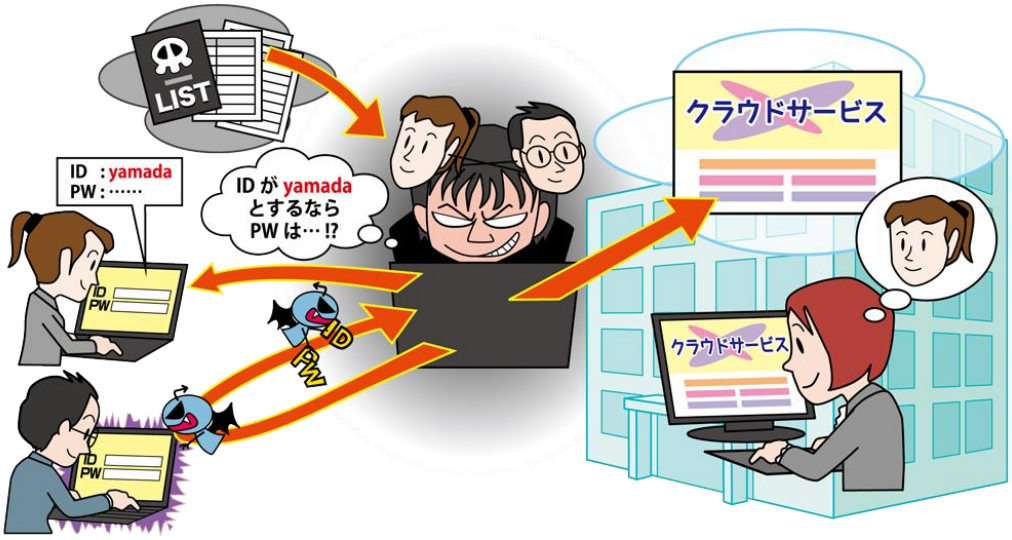
  影響調査、対策強化、CSIRT や関係者への迅速な連絡等

参考資料

1. グーグル、大規模障害の詳しい経緯を公表--システム移行時のミスが原因
https://japan.cnet.com/article/35164342/
2. AWSで障害、PayPayやスマホゲームなどに影響
https://www.itmedia.co.jp/news/articles/2010/22/news094.html
3. 10月1日に株式売買システムで発生した障害について
https://www.jpx.co.jp/corporate/news/news-releases/0060/20201019-01.html
4 事業継続計画策定ガイドライン
https://www.meti.go.jp/policy/netsecurity/docs/secgov/2005_JigyoKeizokuKeikakuSakuteiGuideline.pdf

8位 インターネット上のサービスへの不正ログイン

～パスワードの使いまわしや安易なパスワードの設定をやめるよう呼び掛けを～



組織が利用している、または提供しているインターネットサービスに対して不正ログインが行われ、顧客情報やサービス利用者の個人情報等が窃取されたり、不正に操作されたりする被害が発生している。不正に入手された ID とパスワードを使われ、正規の経路でログインされた場合、そのアクセスが正規のアクセスなのか不正アクセスなのか判断することは難しく、知らぬ間に被害が拡大してしまうおそれがある。

＜攻撃者＞

- 組織的犯行グループ
- 犯罪者

＜被害者＞

- 個人（サービス利用者）
- 組織（サービス利用者・運営者）

＜脅威と影響＞

インターネット上のサービスに対して不正に入手した ID やパスワードを使い、不正ログインを行う攻撃が行われている。ID やパスワードは、別のサービスから漏えいしたものを使う以外にも、被害者が使いそうなものを推測している。

不正ログインされると、サービスに応じた被害を受ける。組織が利用している業務用サービスであれば、顧客や取引先などに関する重要な情報が窃取されたり、不正にメールを送信されたりする。組織が提供しているサービスであれば、利用者の氏名、住所、電話番号やサイトに登録しているクレジットカード等の情報を窃取される。組織においては、損害賠償の支払いによる金銭的被害や社会的信用失墜による機会損失、利用者においては窃取された情報の不正利用等の二次被害を受ける。

＜攻撃手口＞

◆ パスワードリスト攻撃

不正に入手した ID とパスワードのリストを使用し、自動的に入力するプログラム等を用いて、ログイン機能を持つインターネット上のサービスにログインを試みる。複数のサービスで ID とパスワードを使いまわしていると、1 つのサービスで ID とパスワードが流出した場合、それら全てのサービスでログインされるおそれがある。

◆ パスワード推測攻撃

使われやすいパスワードを推測し、そのパスワードでログインを試みる。また、アカウントの所有者が公開している個人情報（氏名、誕生日等）からパスワードを推測して、ログインを試みる。

◆ ウイルス感染

サービスの利用者に悪意あるウェブサイトやメールに添付されたファイルを開かせることで、使用し

ている端末をウイルスに感染させる。その後、利用者がその端末でサービスにログインすることで、その時入力した ID やパスワードを窃取し、その認証情報で不正ログインする。

＜事例または傾向＞

◆ **不正ログインによる取引先情報の流出**

2020 年 11 月、三菱電機が利用しているクラウドサービスに対して不正ログインが行われ、取引先の名前や住所、金融機関口座等 8,635 件が流出した。攻撃者が何らかの方法で入手した ID とパスワードを使い、同社社員になりすましていたとみられる。同社は拠点間の不審な通信を制限する仕組みを導入する等、セキュリティ強化を行っていたが、正規の ID とパスワードを使ったログインであったため、既存の対策では防げなかったとしている。[1]

◆ **フィッシングメール送信の踏み台**

2020 年 10 月、岡山大学教員のメールアカウントに対して不正ログインがあり、合計 1 万 4,666 件のフィッシングメールが送信された。不正ログインの原因は、同教員がメールアカウントに安易なパスワードを設定していたためであった。尚、メールの窃取や個人情報など重要情報の流出は確認されておらず、また、二次被害の報告も受けていないとしている。[2]

◆ **大量の不正ログイン試行による業務妨害**

2020 年 7 月、神奈川県川崎市が運営する公共利用施設予約システム「ふれあいネット」において、大量の不正ログインが試行された。この攻撃により、利用者約 1,300 人分のアカウントがロックされ、システムの適切な運用ができなくなった。川崎市は同システムを用いない方法での運用を余儀なくされたとして、同年 11 月、攻撃者に対する偽計業務妨害罪の告訴状を警察庁に提出している。[3]

＜対策/対応＞

組織（インターネットサービス利用者）

- 被害の予防
  - ・表 1.3「情報セキュリティ対策の基本」を実施
  - ・添付ファイルや URL を安易にクリックしない
  - ・パスワードの使いまわしをしない
  - ・パスワード管理ソフトやブラウザのパスワード管理機能の利用
  - ・サービスが推奨する認証方式の利用 [4]

  その他の対策は、個人 10 位「インターネット上のサービスへの不正ログイン」を参照。

組織（インターネットサービス運営者）

- 被害の予防
  - ・表 1.3「情報セキュリティ対策の基本」を実施
  - ・セキュリティ対策の予算・体制の確保

    システムの導入時や保守作業時の十分な予算と体制を確保する必要がある。
  - ・利用者に対するセキュリティ機能の提供

    二要素認証やリスクベース認証、利用履歴を確認できる機能等を提供する。
  - ・アカウントの存在有無の確認に悪用されないサービス設計

    アカウントの存在有無がわかるような認証エラー表示の抑止、連続アクセスの検知等。
- 被害の早期検知
  - ・適切なログの取得と継続的な監視
- 被害を受けた後の対応
  - ・CSIRT 等所定の連絡先への連絡
  - ・セキュリティ専門企業への調査依頼
  - ・影響調査及び原因の追究、対策の強化
  - ・被害者に対するすみやかな連絡と補償
  - ・漏えいした内容や発生原因等の公表
  - ・関係者、関係機関への連絡

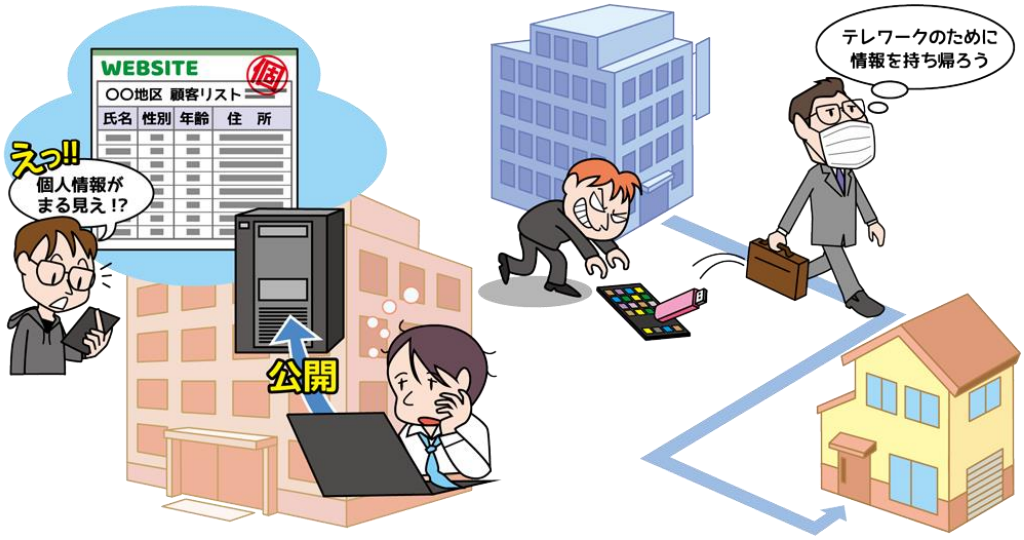
    監督官庁、個人情報保護委員会、警察等

参考資料

1. 三菱電機、不正アクセスで取引先の口座情報8000件流出
https://www.nikkei.com/article/DGXMZO66468150Q0A121C2TJC000
2. 不正アクセスによるフィッシングメールの送信に関するお知らせとお詫び
https://www.okayama-u.ac.jp/tp/news/news_id9690.html
3. ふれあいネットへの不正ログイン試行、偽計業務妨害罪として川崎市が告訴へ
https://scan.netsecurity.ne.jp/article/2020/11/24/44853.html
4. 不正ログイン対策特集ページ
https://www.ipa.go.jp/security/anshin/account_security.html

9位 不注意による情報漏えい等の被害

～業務環境の変化に合わせて対策の見直しを～



組織において、情報管理体制の不備や情報リテラシーの不足等が原因となり、個人情報や機密情報を漏えいさせてしまう事例が 2020 年も引き続き多く見られた。特にテレワークの導入等で働く環境が変化している今、状況に応じた対策が求められる。

＜当事者（情報を漏えいさせた側）＞

- 組織（従業員）

＜被害者（情報を漏えいされた側）＞

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

＜脅威と影響＞

組織において、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から、従業員の不注意等によってこれらの重要情報を漏えいさせてしまう事件が発生している。

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

＜要因＞

◆ 従業員のセキュリティ意識の低さ

個人情報や機密情報を取り扱う従業員のセキュリティ意識が低いと、情報に対する重要性の認識不足から不用意な扱いをして情報を漏えいさせてしまう。例えば、重要情報を保存した端末を外出先で紛失したり、宛先を十分に確認しないまま重要情報を含むメールを誤送信したりするケースが見られる。

◆ 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情報漏えい事故を起こしてしまう。

◆ 組織規程および確認プロセスの不備

組織内の重要情報の定義・取り扱い規程・持ち出し許可手順や、作業時の確認プロセスに不備がある場合、情報漏えいが起こりやすい。

＜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）
- 不適切なウェブ公開（重要情報への対処が不十分なまま公開）
- 重要情報を保存した情報端末（PC やスマートフォン等）・記録媒体（USB メモリー等）の紛失
- 重要書類（紙媒体）の紛失

＜事例または傾向＞

◆　**新型コロナウイルスに関する個人情報が流出**

福岡県は同県が保有する新型コロナウイルス感染症陽性者約 9,700 人分の個人情報が流出したと公表した。発端は、2020 年 11 月に関係者宛に患者情報等が含まれるファイルが入ったクラウド上のフォルダーへのアクセス権が付与されたメールを送信する際、似たメールアドレスの第三者に誤送信したことであった。更に、誤送信発覚後に行ったアクセス制限対応で設定ミスがあり、ファイルの URL に直接アクセスできる状態が継続した。

同県はファイルを全て削除し、誤送信先に対してデータの削除を要請する等の対応を行った。[1]

◆　**顧客情報が保存された記録媒体を紛失**

2020 年 7 月、みずほ総合研究所が、約 250 万件の顧客の個人情報や法人情報が含まれるバックアップ用の磁気テープを紛失したと公表した。情報の中には、顧客の個人情報やサービス利用実績、みずほ銀行等から委託された業務に関する情報などが含まれていた。

同社によると誤廃棄の可能性が高く、外部への情報の流出は確認されていないとしている。[2]

◆　**委託先の設定ミスにより取引先情報が流出**

2020 年 3 月、道新サービスセンターが、15,599 件の個人情報を含む 28,515 件の取引先情報が外部から閲覧できる状態であったと公表した。同社の委託先の従業員が委託業務について作業をする際に利用していた、ソフトウェア開発プラットホーム GitHub の設定ミスが原因であった。

問題が判明した時点で、委託先会社からの秘密保持契約に基づく報告はなく、同社が情報漏えいに気付き委託先に確認を行ったところ、外部への情報の流出が確認された。[3]

＜対策/対応＞

組織（当事者）

- 情報リテラシーや情報モラルの向上
  - ・従業員のセキュリティ意識教育
  - ・組織規程および確認プロセスの確立
    特定の担当者への業務集中が発生しないような体制の構築も重要である。
  - ・組織規程および確認プロセスの見直し
    テレワークの導入等、業務環境に変化があった場合、規程を見直すことが必要である。
- 被害の予防（被害に備えた対策含む）
  - ・確認プロセスに基づく運用
  - ・情報の保護（暗号化、認証）、機密情報の格納場所の掌握、可視化
  - ・DLP 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
  - ・業務用携帯端末の紛失対策機能の有効化
- 被害の早期検知
  - ・問題発生時の内部報告体制の整備
  - ・外部からの連絡窓口の設置
- 被害を受けた後の対応
  - ・CSIRT への連絡
  - ・影響調査および原因の追究、対策の強化
  - ・被害拡大や二次被害要因の排除
  - ・漏えいした内容や発生原因の公表
  - ・関係者、関係機関への連絡
    監督官庁、個人情報保護委員会等

個人/組織（被害者）

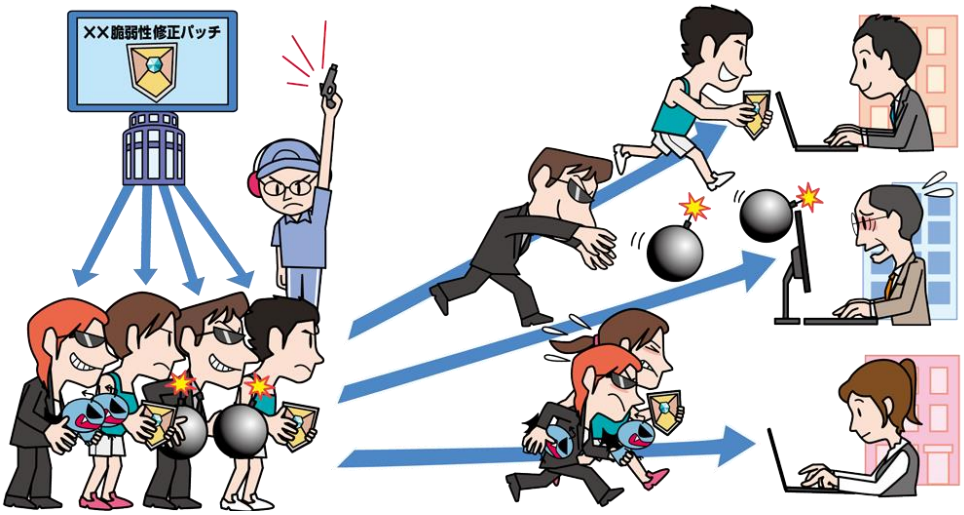
- 被害を受けた後の対応
  - ・漏えいが発生した組織からの情報に従う
  - ・パスワードやクレジットカード情報の変更等

参考資料

1. 新型コロナウイルス感染症対策本部（調整本部）における個人情報の漏えい等事案について
https://www.pref.fukuoka.lg.jp/contents/covid19-rouei.html
2.みずほ総合研究所株式会社におけるお客さま情報の紛失について
https://www.mizuho-ri.co.jp/company/release/pdf/20200721release.pdf
3. GitHubの設定ミスが原因、取引先情報が外部から閲覧可能に（道新サービスセンター）
https://scan.netsecurity.ne.jp/article/2020/03/30/43876.html

10位 脆弱性対策情報の公開に伴う悪用増加

～公開された脆弱性を知っているのは自分たちと悪人たち～



ソフトウェアの脆弱性対策情報の公開は、脆弱性の脅威や対策情報を広く呼び掛けられるメリットがある。一方、その情報を攻撃者に悪用され、当該ソフトウェアに対する脆弱性対策を行っていないシステムを狙った攻撃が行われている。近年では脆弱性情報の公開後、攻撃コードが流通し、攻撃が本格化するまでの時間が短くなっている。

＜攻撃者＞

- 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＞

一般的に、ソフトウェアに脆弱性が発見された場合、当該ソフトウェアの開発ベンダー等が脆弱性を修正するためのプログラム（パッチ）を作成する。その後、ベンダーはセキュリティ対応機関等と連携するか、または自身で脆弱性対策情報として脆弱性の内容とパッチまたは対策方法を公開し、当該ソフトウェアの利用者へ対策を促す。

一方、公開された脆弱性対策情報を元に攻撃者が攻撃コード等を作成し、パッチを適用していない利用者に対して脆弱性を悪用した攻撃を行うことで、情報漏えいや改ざん、ウイルス感染等の被害の発生が確認されている。特に、Apache Struts2 やWordPress（プラグイン含む）といった広く利用されているソフトウェアの脆弱性の場合、攻撃コード等が公開されると被害が大きくなるおそれがある。

昨今、脆弱性が発見されてからそれを悪用した攻撃が発生するまでの期間が短くなっており、より迅速な対応が求められる。

＜攻撃手口＞

◆ 対策前の脆弱性（N デイ脆弱性）を悪用

ソフトウェアに脆弱性が発見され、パッチが公開されたものの、そのパッチを適用するまでにはいくらかの時間が掛かる。このパッチ未適用の時間に存在する脆弱性が N デイ脆弱性である。

システムで使用しているソフトウェアの管理が不適切な企業は、この時間が長くなるため、被害に遭うおそれがある。

◆ 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ることがある。また、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＞

◆　**製品の脆弱性を狙う攻撃活動を観測**

2020 年 7 月 1 日、F5 Networks 社のネットワーク製品「BIG-IP」シリーズにおいて、リモートから任意のコードの実行が可能な脆弱性が公開された。この脆弱性が悪用された場合、認証の有無によらず任意のシステムコマンドや Java コードの実行、ファイルの生成・削除を実行されるおそれがある。脆弱性公開の 4 日後には、脆弱性を悪用するための攻撃コードがインターネット上に公開され、その翌日には攻撃が確認された。[1]

◆　**Windows Sever に Zerologon の脆弱性**

2020 年 8 月 11 日（米国時間）、Microsoft より Windows Server 製品に影響がある「Zerologon」と呼ばれる Netlogon の特権の昇格の脆弱性の更新プログラムが公開された。その後、9 月 15 日（日本時間）に本脆弱性に対する実証コード（PoC）が公開され、同社より同月 24 日（米国時間）に PoC を悪用した攻撃が確認されたと発表された。本脆弱性は深刻度（CVSS v3.0）が最大の 10.0 と非常に危険なものであった。[2]

◆　**パッチ公開から 1 週間強で攻撃発生**

Oracle は 2020 年 10 月 20 日（米国時間）の定例パッチで「Oracle WebLogic Server」の脆弱性対策を公開した。この脆弱性を悪用されるとシステムの権限を奪われるおそれがあり、注意喚起が出されていた。このパッチ公開の 8 日後には脆弱性の実証コード（PoC）が公開され、その翌日には PoC を悪用した攻撃が確認された。[3]

＜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
  - ・資産の把握、体制の整備

    パッチを適用する場合、サービスが正常に動作することを事前に検証する必要がある。そのため、検証するための体制や環境も事前に準備する必要がある。
  - ・脆弱性関連情報の収集と対応
  - ・UTM、IDS/IPS、WAF 等の導入

    導入後も対策情報（設定等）を定期的に更新する作業があることを想定し、予算や体制を確保しておくこと。
  - ・ネットワークの監視および攻撃通信の遮断

    ネットワーク経由で脆弱性を悪用する攻撃を監視する。攻撃の疑いがある場合は、ファイアウォール等により通信を遮断する。
  - ・セキュリティのサポートが充実しているソフトウェアやバージョンを使う

    利用するソフトウェア製品やアプリケーションについては、パッチの提供が早い等のセキュリティサポートが充実したものを選択する。
  - ・一時的なサーバー停止等

    すぐにパッチが適用できない場合、一時的にサーバー停止等を実施して、攻撃を回避する対策を取ることも検討する。サーバー停止等に伴うサービス停止の影響については事前に検討をしておく。また、速やかにサービス利用者への通知を行う。
- 被害を受けた後の対応
  - ・CSIRT 等所定の連絡先への連絡
  - ・影響調査および原因の追究、対策の強化

組織（開発ベンダー）

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

    情報を迅速に発信できる仕組みの整備

参考資料

1. 【注意喚起】F5 BIG-IP製品の任意コード実行可能な脆弱性（CVE-2020-5902）を狙う攻撃活動を観測
https://www.lac.co.jp/lacwatch/alert/20200708_002231.html
2. Netlogon の特権の昇格の脆弱性 (CVE-2020-1472) への早急な対応を
https://www.jpcert.or.jp/newsflash/2020091601.html
3. 早急に「WebLogic Server」脆弱性の修正を - パッチ公開より1週間強で攻撃発生
https://www.security-next.com/120204

10 大脅威選考会

氏名	所属	氏名	所属
石田 淳一	(株)アールジェイ	三木 剛	グローバルセキュリティエキスパート(株)
菅原 尚志	アクセンチュア(株)	遠藤 誠	(株)ケイテック
中嶋 美貴	アクセンチュア(株)	飯塚 修平	KDDI デジタルセキュリティ(株)
石井 彰	旭化成(株)	川谷 友理恵	KDDI デジタルセキュリティ(株)
岡田 良太郎	(株)アスタリスク・リサーチ	小岩 航介	KDDI デジタルセキュリティ(株)
徳丸 浩	EG セキュアソリューションズ(株)	小熊 慶一郎	(株)KBIZ / (ISC)2
安西 真人	(株)エーアイセキュリティラボ	保村 啓太	KPMG コンサルティング(株)
関根 鉄平	(株)エーアイセキュリティラボ	北田 高之	(株)神戸デジタル・ラボ
佐藤 直之	SCSK(株)	窪田 敏明	(株)神戸デジタル・ラボ
鈴木 寛明	SCSK(株)	久柴 克宏	(株)神戸デジタル・ラボ
辻 伸弘	SB テクノロジー(株)	宮﨑 清隆	国際マネジメントシステム認証機構(株)
大塚 淳平	NRI セキュアテクノロジーズ(株)	前園 博文	コベルコシステム(株)
芳賀 夢久	NRI セキュアテクノロジーズ(株)	福森 大喜	(株)サイバーディフェンス研究所
中西 克彦	NEC ネクサソリューションズ(株)	荒川 大	(一社)サイバーリスク情報センター
杉井 俊也	NEC フィールディング(株)	宮内 伸崇	(株)サイント
大湊 健一郎	(株)NTT-ME	奥石 隆	(社) JPCERT コーディネーション センター
川端 誠	NTT コミュニケーションズ(株)	福本 郁哉	(社) JPCERT コーディネーション センター
真鍋 太郎	NTT コミュニケーションズ(株)	齊藤 和男	(株)ジェイピー・セキュア
北河 拓士	NTT コム ソリューションズ(株)	唐沢 勇輔	Japan Digital Design(株)
斯波 彰	NTT コム ソリューションズ(株)	大久保 隆夫	情報セキュリティ大学院大学
大石 眞央	(株)NTT データ	正木 義和	スワットブレインズ(株)
宮本 久仁男	(株)NTT データ	東 恵寿	NPO セカンドワーク協会
矢竹 清一郎	(株)NTT データ	金城 夏樹	(株)セキュアイノベーション
池田 和生	NTTデータ先端技術(株)	栗田 智明	(株)セキュアイノベーション
植草 祐則	NTTデータ先端技術(株)	阿部 実洋	(株)セキュアベース
前田 典彦	(株)FFRI セキュリティ	林 達也	(一社)セキュリティ対策推進協議会
結城 亮史	(株)FFRI セキュリティ	持田 啓司	(一社)セキュリティ対策推進協議会
河野 真一郎	エフセキュア(株)	澤永 敏郎	ソースネクスト(株)
島田 秋雄	エフセキュア(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
楯 研人	エムオーテックス(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
徳毛 博幸	エムオーテックス(株)	相馬 基邦	(株)ソニー・インタラクティブエンタテインメント
間嶋 英之	エムオーテックス(株)	阿部 巧	ソフトバンク(株)
池田 耕作	(株)オージス総研	中西 基裕	ソフトバンク(株)
大月 一孝	(株)オージス総研	楢原 盛史	タニウム合同会社
松田 康司	(株)オージス総研	小島 博行	地方公共団体情報システム機構
岡村 耕二	九州大学	鈴木 一弘	地方公共団体情報システム機構
小関 直樹	京セラコミュニケーションシステム(株)	田中 卓朗	TIS(株)
佐藤 宏昭	京セラコミュニケーションシステム(株)	三木 基司	TIS(株)
西山 健太	京セラコミュニケーションシステム(株)	大谷 毅典	DXC テクノロジー・ジャパン(株)
清水 将人	(一社)草の根サイバーセキュリティ運動全国連絡会	前田 隆行	DXC テクノロジー・ジャパン(株)
高崎 庸一	グローバルセキュリティエキスパート(株)	松本 隆	(株)ディー・エヌ・エー

氏名	所属	氏名	所属
内山 巧	(株)電算	大高 利夫	藤沢市役所
坂 明	(公財)東京オリンピック・パラリンピック競技大会組織委員会	福田 達夫	藤沢市役所
南 博康	東京海上日動あんしん生命保険(株)	原 和宏	富士通(株)
花田 隆仁	東京海上日動火災保険(株)	原田 弘和	富士通(株)
中西 祐介	東京海上日動システムズ(株)	綿口 吉郎	富士通(株)
石川 朝久	東京海上ホールディングス(株)	中村 洋介	(株)富士通研究所
小島 健司	(株)東芝	荒井 大輔	(株)Bridge
田岡 聡	(株)東芝	柳川 俊一	(株)Bridge
大浪 大介	東芝インフォメーションシステムズ(株)	今野 俊一	Broadcom Inc.
江川 暢	(株)Doctor Web Pacific	山内 正	Broadcom Inc.
原田 博久	(株)Doctor Web Pacific	近藤 隆雄	(株)ベリサーブ
森 周	(株)Doctor Web Pacific	樅山 清	(株)ベリサーブ
大山 水帆	戸田市役所	太田 良典	弁護士ドットコム(株)
今 佑輔	トレンドマイクロ(株)	垣内 由梨香	マイクロソフトコーポレーション
岡本 勝之	トレンドマイクロ(株)	花村 実	マイクロソフトコーポレーション
加藤 雅彦	長崎県立大学	山室 太平	マカフィー(株)
須川 賢洋	新潟大学	高江洲 勲	三井物産セキュアディレクション(株)
上村 理	日本アイ・ビー・エム(株)	東内 裕二	三井物産セキュアディレクション(株)
柳 優	日本アイ・ビー・エム(株)	山谷 晶英	三井物産セキュアディレクション(株)
山下 慶子	日本アイ・ビー・エム(株)	篠原 巧	(株)三菱総合研究所
高倉 万記子	(一財)日本情報経済社会推進協会(JIPDEC)	古澤 一憲	(株)三菱総合研究所
初見 卓也	(一財)日本情報経済社会推進協会(JIPDEC)	平田 真由美	みゅーらぼ
谷川 哲司	日本電気(株)	石井 崇喜	(株)ユービーセキュア
住本 順一	日本電信電話(株)	淵上 智史	(株)ユービーセキュア
金 明寛	(株)ネクストジェン	島田 理枝	(株)ユビテック
常川 直樹	パナソニック(株)	松田 和宏	(株)ユビテック
渡辺 久晃	パナソニック(株)	牧野 尚彦	横浜市役所
林 薫	パロアルトネットワークス(株)	三国 貴正	(株)YONA
浜田 譲治	PwC コンサルティング合同会社	福本 佳成	楽天(株)
岩佐 功	東日本電信電話(株)	橘 喜胤	楽天ウォレット(株)
齊藤 純一郎	東日本電信電話(株)	伊藤 彰嗣	楽天モバイル(株)
水越 一郎	東日本電信電話(株)	山崎 圭吾	(株)ラック
折田 彰	(株)日立システムズ	若居 和直	(株)ラック
関口 竜也	(株)日立システムズ	猪野 裕司	(株)リクルートテクノロジーズ
本川 祐治	(株)日立システムズ	六宮 智悟	(株)リクルートテクノロジーズ
寺田 真敏	(株)日立製作所	有森 貞和	(株)両備システムズ
田中 秀和	(株)日立ソリューションズ	清水 秀一郎	
古賀 洋一郎	ビッグローブ(株)	piyokango	
山口 裕也	(株)ファイブドライブ		

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　黒谷 欣史　亀山 友彦
渡邉 祥樹　大友 更紗　吉本 賢樹
堀江 亘　佐々木 敬幸　柴本 憲一
鈴木 慧

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

情報セキュリティ 10 大脅威 2021

～よもや自組織が被害に！呼吸を合わせて全力防御！

2021 年 2 月 26 日　初 版

［事務局・発行］　独立行政法人情報処理推進機構

〒113-6591

東京都文京区本駒込二丁目 28 番 8 号

文京グリーンコートセンターオフィス

https://www.ipa.go.jp/

IPA 独立行政法人 **情報処理推進機構**
セキュリティセンター
〒113-6591
東京都文京区本駒込二丁目 28 番 8 号
文京グリーンコートセンターオフィス
TEL:03-5978-7527
https://www.ipa.go.jp/security/