情報セキュリティ10大脅威　2024

[組織編]

IPA Better Life with IT

「情報セキュリティ10大脅威」とは？

- IPAが2006年から毎年発行している資料
- 前年に発生したセキュリティ事故や攻撃の状況等から**IPAが脅威候補を選出**
- セキュリティ専門家や企業のシステム担当等から構成される**「10大脅威選考会」が投票**
- **TOP10入りした脅威を「10大脅威」**として脅威の概要、被害事例、対策方法等を解説

10大脅威の特徴

脅威に対して様々な立場の方が存在

立場ごとに注意すべき脅威も異なるはず

- 家庭等でパソコンやスマホを利用する人「個人」

- 企業や政府機関等の組織
- 組織のシステム管理者や社員・職員

「組織」

「個人」と「組織」の２つの立場で脅威を解説

情報セキュリティ10大脅威 2024

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

情報セキュリティ10大脅威 2024

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

自組織により強く関係する脅威から対策する
ことが重要

情報セキュリティ対策の基本

- 多数の脅威があるが「攻撃の糸口」は似通っている
- 基本的な対策の重要性は長年変わらない
- 下記の**「情報セキュリティ対策の基本」を常に意識することが重要**

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

情報セキュリティ対策の基本＋α

- 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を想定した＋αの対策を行い、備える必要がある

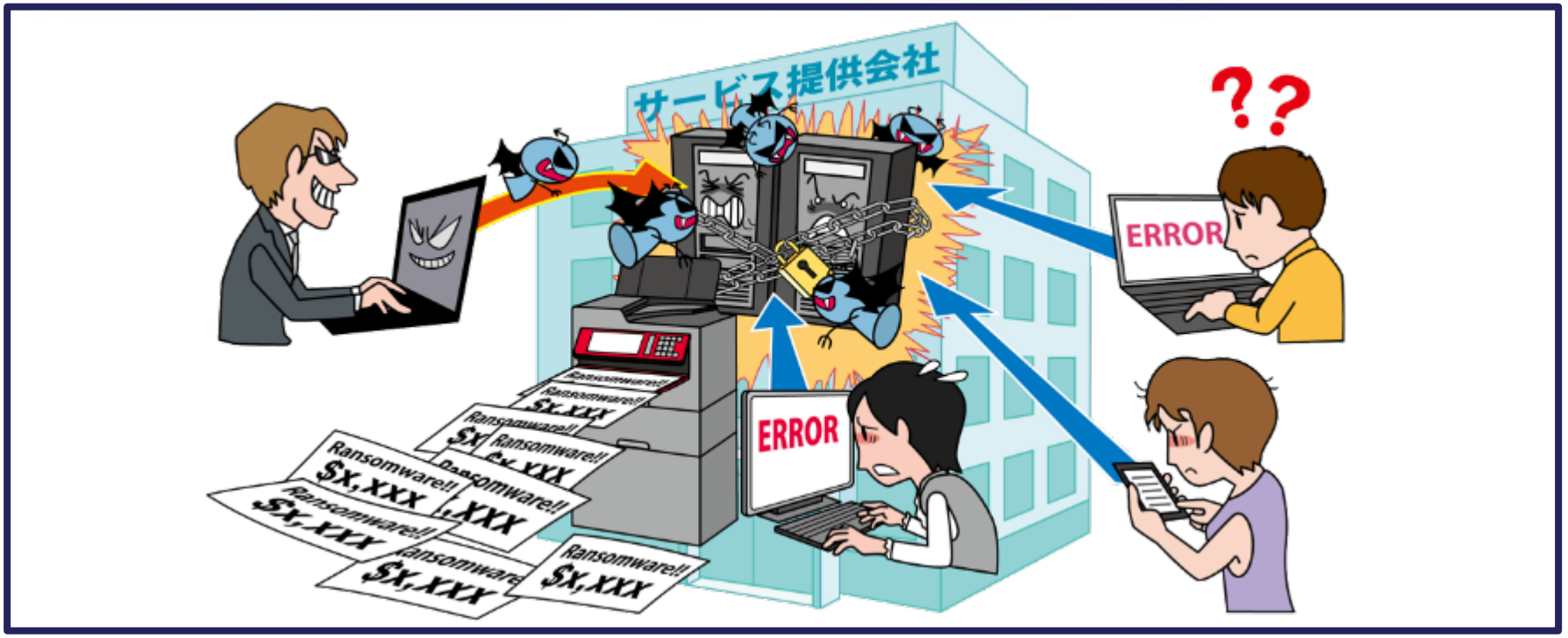
備える対象	情報セキュリティ対策の基本＋α	目的
インシデント全般	責任範囲の明確化(理解)	インシデント発生時に誰(どの組織)が対応する責任があるのかを明確化(理解)する
クラウドの停止	代替案の準備	業務が停止しないように代替策を準備する
クラウドの仕様変更	設定の見直し	仕様変更により意図せず変更された設定を適切な設定に直す(設定不備による情報漏えいや攻撃への悪用を防止する)

「組織」向け脅威の解説

- ここからは脅威毎に解説します
- 組織により強く関係する脅威から確認しましょう
- **各脅威の対策の紹介では前項の「情報セキュリティ対策の基本」は実施していることを前提とし、記載には含めていません**

【1位】ランサムウェアによる被害

～組織の規模や業種は関係なし！次の標的はあなたの組織かも？～



- PC等に保存されているファイルが暗号化され、使用不可にされる
- 復旧と引き換えに金銭を要求される
- 情報が窃取されて、公開され、さらに攻撃を受けている事を
  ビジネスパートナー等に公表すると脅迫されるケースもある
- 組織の規模や業種に関係なく攻撃される

【出典】 令和５年上半期におけるサイバー空間をめぐる脅威の情勢等について(警察庁)
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R05_kami_cyber_jousei.pdf

【1位】ランサムウェアによる被害

～組織の規模や業種は関係なし！次の標的はあなたの組織かも？～

IPA

- **攻撃手口**

・ウイルス(ランサムウェア)に感染させて金銭を要求

- **脆弱性を悪用した手口**
  - ソフトウェアの脆弱性を悪用し
    ウイルスを実行(感染させる)
  - 攻撃ツール等を利用して
    ネットワーク越しに次々と感染させる

- **不正アクセスによる手口**
  - 意図せず公開されているポート(リモートデスクトップ等)から
    サーバーに不正アクセスさせる
  - サーバー上で攻撃者がウイルスを実行させる(感染させる)

【1位】ランサムウェアによる被害

～組織の規模や業種は関係なし！次の標的はあなたの組織かも？～

IPA

- **攻撃手口**

・ウイルス(ランサムウェア)に感染させて金銭を要求

- **メールを悪用した手口**
  - 不正な添付ファイルを開かせる
  - メール内のリンクをクリックさせる
- **Web サイトを悪用した手口**
  - ランサムウェアをダウンロードさせるようにWebサイトを改ざんした
  - 当該サイトを閲覧するようにメールなどで誘導した

【1位】ランサムウェアによる被害

～組織の規模や業種は関係なし！次の標的はあなたの組織かも？～

- **2023年の事例/傾向①**
  - **ランサムウェア感染による業務停止**
    - 2023年7月、名古屋港統一ターミナルシステムがランサムウェアに感染した
    - リモート接続機器の脆弱性を悪用した不正アクセスが原因であった
    - 物理サーバー基盤および全仮想サーバーが暗号化されていることが判明した
    - 約2日半、ターミナルでの作業停止を余儀なくされた

【出典】 NUTS システム障害の経緯報告(名古屋港運協会)
https://meikoukyo.com/wp-content/uploads/2023/07/0bb9d9907568e832da8f400e529efc99.pdf
コンテナターミナルにおける情報セキュリティ対策等検討委員会について(国土交通省)
https://www.mlit.go.jp/kowan/kowan_mn2_000006.html

【1位】ランサムウェアによる被害

～組織の規模や業種は関係なし！次の標的はあなたの組織かも？～

- **2023年の事例/傾向②**
  - **ランサムウェア感染によるサービス提供停止**
    - 2023年6月、エムケイシステムのデータセンターのサーバーが不正アクセスされ、ランサムウェアに感染した
    - データが暗号化され、社会保険労務士向けクラウドサービス「社労夢」をサービス提供できなくなった
    - 約3,400人のユーザーに影響があり、オンプレミスで動作するパッケージ版が代替として提供された
    - インフラ設備の再構築費用などがかかったため、エムケイシステムは業績予想を下方修正した

【出典】 第三者によるランサムウェア感染被害への対応状況のお知らせ(第２報)(株式会社エムケイシステム)
https://contents.xj-storage.jp/xcontents/AS97180/fd524344/99b9/470f/90e6/a580932b7962/140120230620507046.pdf
当社サーバへの不正アクセスに関する調査結果のご報告(第３報)(株式会社エムケイシステ ム)
https://contents.xj-storage.jp/xcontents/AS97180/813d570f/5138/4bc7/a113/f4837598df38/140120230719524126.pdf

【1位】ランサムウェアによる被害

～組織の規模や業種は関係なし！次の標的はあなたの組織かも？～

- **2023年の事例/傾向③**
  - **VPN経由で侵入、ランサムウェアを横展開**
    - 2023年1月、ならコープがランサムウェアによる攻撃を受けていたことを公表
    - 原因は、攻撃者が脆弱性を悪用してVPN経由で侵入後、内部情報を収集し、ランサムウェアを横展開したことにある
    - サーバー11台で約49万人の個人情報を含むデータが暗号化されたが、それらの外部への流出は確認されていない
    - バックアップを取っていたデータベースは感染を逃れていたため、データを復元することができた

【出典】 重大なシステムトラブルに伴う個人情報についてのお知らせ(市民生活協同組合ならコープ)
https://www.naracoop.or.jp/naranews/cat2/4628.html
多数システムでランサム被害、復旧や事業継続に追われる - ならコープ(Security NEXT)
https://www.security-next.com/143034/

【1位】ランサムウェアによる被害

～組織の規模や業種は関係なし！次の標的はあなたの組織かも？ ～

- **対策**
  - **組織(経営者層)**

【組織としての体制確立】

- インシデント対応体制を整備し、対応する
  - CISOを配置する
  - CSIRTを構築する
  - 有事の際の対応フローを確立する
  - 運用手順を社員へ通知する
  - 運用の訓練をする
  - 外部の協力依頼先を用意する
  - 社内規則の整備や予算確保をする

【1位】ランサムウェアによる被害

～組織の規模や業種は関係なし！次の標的はあなたの組織かも？ ～

- **対策**
  - **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
- メールの添付ファイル開封や、メールやSMSのリンク、URLのクリックを安易にしない
- 多要素認証の設定を有効にする
- 提供元が不明の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(取得、保管、復旧訓練)を行う

【1位】ランサムウェアによる被害

～組織の規模や業種は関係なし！次の標的はあなたの組織かも？ ～

- **対策**
  - **組織(システム管理者、従業員)**

【被害を受けた後の対応】

- 適切な報告／連絡／相談を行う
  - 上司、CSIRT、関係組織、公的機関等
- 適切なバックアップ運用(復旧作業)を行う
- 復号ツール※1の活用
- インシデント対応体制を整備し、対応する

【出典】 ※1 The No More Ransom Project(No More Ransomプロジェクト)
https://www.nomoreransom.org/

【1位】ランサムウェアによる被害

～組織の規模や業種は関係なし！次の標的はあなたの組織かも？ ～

- **身代金の支払いと復旧業者の選定について**
  - 原則、身代金を支払わずに復旧を行う
  - 身代金を支払ってもデータの復元や情報の流出を防げるとは限らない
  - 対応を依頼した業者が攻撃者との裏取引で身代金を支払うことで復旧した場合、事実上、自組織が攻撃者に資金提供をしたとみなされるおそれもある
  - 対応を依頼する業者の選定※1にも注意が必要

【出典】 ※1 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

～ビジネスもセキュリティ対策も関係組織で二人三脚を～

- 調達から販売、業務委託等一連の商流において、セキュリティ対策が甘い組織が攻撃の足がかりとして攻撃される
- ソフトウェア開発のライフサイクルに関与するモノや人の繋がりを足掛かりとする(ソフトウェアサプライチェーン)攻撃も存在する
- 取引先や業務を委託している外部組織から情報漏えいする

【2位】サプライチェーンの弱点を悪用した攻撃

～ビジネスもセキュリティ対策も関係組織で二人三脚を～

IPA

- **攻撃手口**

・サプライチェーンの中でセキュリティが脆弱な組織を狙う

- **標的組織の取引先や委託先を攻撃し、それらが保有する標的組織の機密情報を狙う**
- **ソフトウェア開発元やMSP(企業システムの運用・監視等を請け負う事業者)等を攻撃し、標的を攻撃するための足掛かりとする**
  - ソフトウェアのアップデートにウイルスを仕込み、アップデートを適用した利用者にウイルスを感染させる等

【2位】サプライチェーンの弱点を悪用した攻撃

～ビジネスもセキュリティ対策も関係組織で二人三脚を～

- **2023年の事例/傾向①**
  - **業務委託先業者からの顧客情報漏えい**
    - 2023年1月、複数の保険会社が業務委託先から顧客の個人情報の流出を公表した
    - 業務委託先の適切なセキュリティ対策がされていないサーバーへの不正アクセスが原因であった
    - 流出した個人情報が海外のWebサイトに掲載されていた
    - 流出の規模は、多いところで約130万人分であり、調査や対処に追われた

【出典】 個人情報流出に関するお詫びとお知らせ(アフラック生命保険株式会社)
https://www.aflac.co.jp/news_pdf/2023011001.pdf
個人情報漏えいに関するお詫びとご報告(チューリッヒ保険会社)
https://www.zurich.co.jp/customerdata/
個人情報流出に関する再発防止策について(アフラック生命保険株式会社)
https://www.aflac.co.jp/news_pdf/20230710.pdf
個人情報漏えいに関する追加のお知らせ(チューリッヒ保険会社)
https://www.zurich.co.jp/aboutus/news/news/2023/0117/

【2位】サプライチェーンの弱点を悪用した攻撃

～ビジネスもセキュリティ対策も関係組織で二人三脚を～

- **2023年の事例/傾向②**
  - **委託先のシステムを介して不正アクセスされ、顧客情報が漏えい**
    - 2023年11月、LINEヤフーは同社の保有する顧客情報が漏えいしたことを公表
    - ユーザーに関する情報が約30万件、取引先等に関する情報が約9万件、従業員等に関する情報が約5万件が漏えい
    - 第三者による社内システムへの不正アクセスが原因
    - 委託先企業であるNAVER Cloud社のさらに委託先の企業で従業員のPCがウイルス感染したことが発端

【出典】 不正アクセスによる、情報漏えいに関するお知らせとお詫び(LINEヤフー株式会社)
https://www.lycorp.co.jp/ja/news/announcements/001002/

【2位】サプライチェーンの弱点を悪用した攻撃

～ビジネスもセキュリティ対策も関係組織で二人三脚を～

- **2023年の事例/傾向③**
  - **提携先企業に不正アクセス、顧客情報漏えい**
    - 2023年11月、JCOMが顧客情報を漏えいしたことを公表
    - JCOMの提供するメッシュ Wi-Fi の提供元の米国Plume Design社の提携先のモバイルアプリのアクセスログサーバーが不正アクセスされたことが原因
    - 約23万件の顧客の氏名と約5,000件の顧客のメールアドレスが漏えい

【出典】 お客さまの個人情報漏えいに関するお知らせとお詫び(JCOM 株式会社)
https://newsreleases.jcom.co.jp/news/20231122_9239.html

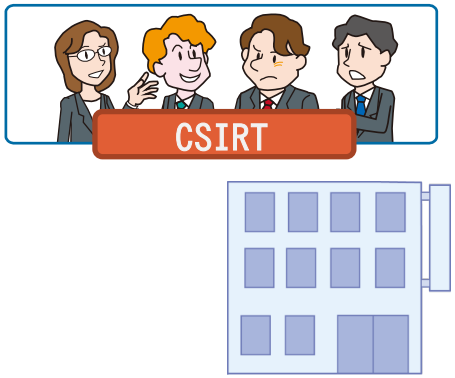
【2位】サプライチェーンの弱点を悪用した攻撃

～ビジネスもセキュリティ対策も関係組織で二人三脚を～

- **対策**
  - **組織(経営者層)**

【被害の予防】

- インシデント対応体制を整備し、対応する
  - CISOを配置する
  - CSIRTを構築する
  - 有事の際の対応フローを確立する
  - 運用手順を社員へ通知する
  - 運用の訓練をする
  - 外部の協力依頼先を用意する
  - 社内規則の整備や予算確保をする



【2位】サプライチェーンの弱点を悪用した攻撃

～ビジネスもセキュリティ対策も関係組織で二人三脚を～

- **対策**
  - **組織(自組織で実施)**

【被害の予防】

- 情報管理規則の徹底
- セキュリティ評価サービス(SRS)を用いた自組織のセキュリティ対策状況の把握
- 信頼できる委託先、取引先、サービスの選定
- 契約内容の確認
- 委託先組織の管理
- 納品物の検証(ソフトウェアの把握や管理※1 、脆弱性対策の実施等)

【出典】 ※1 ソフトウェア管理に向けたSBOM(Software Bill of Materials)の導入に関する手引」を策定しました(経済産業省)
https://www.meti.go.jp/press/2023/07/20230728004/20230728004.html

【2位】サプライチェーンの弱点を悪用した攻撃

～ビジネスもセキュリティ対策も関係組織で二人三脚を～

- **対策**
  - **組織(自組織で実施)**

【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

【2位】サプライチェーンの弱点を悪用した攻撃

～ビジネスもセキュリティ対策も関係組織で二人三脚を～

- **対策**
  - **組織(自組織に関わる組織と共に実施)**

【被害の予防】

- 取引先や委託先との連絡プロセスの確立
- 取引先や委託先の情報セキュリティ対応の確認、監査
- 情報セキュリティの認証取得
- 公的機関等が公開している資料※1の活用

【出典】 ※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
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
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

【2位】サプライチェーンの弱点を悪用した攻撃

～ビジネスもセキュリティ対策も関係組織で二人三脚を～

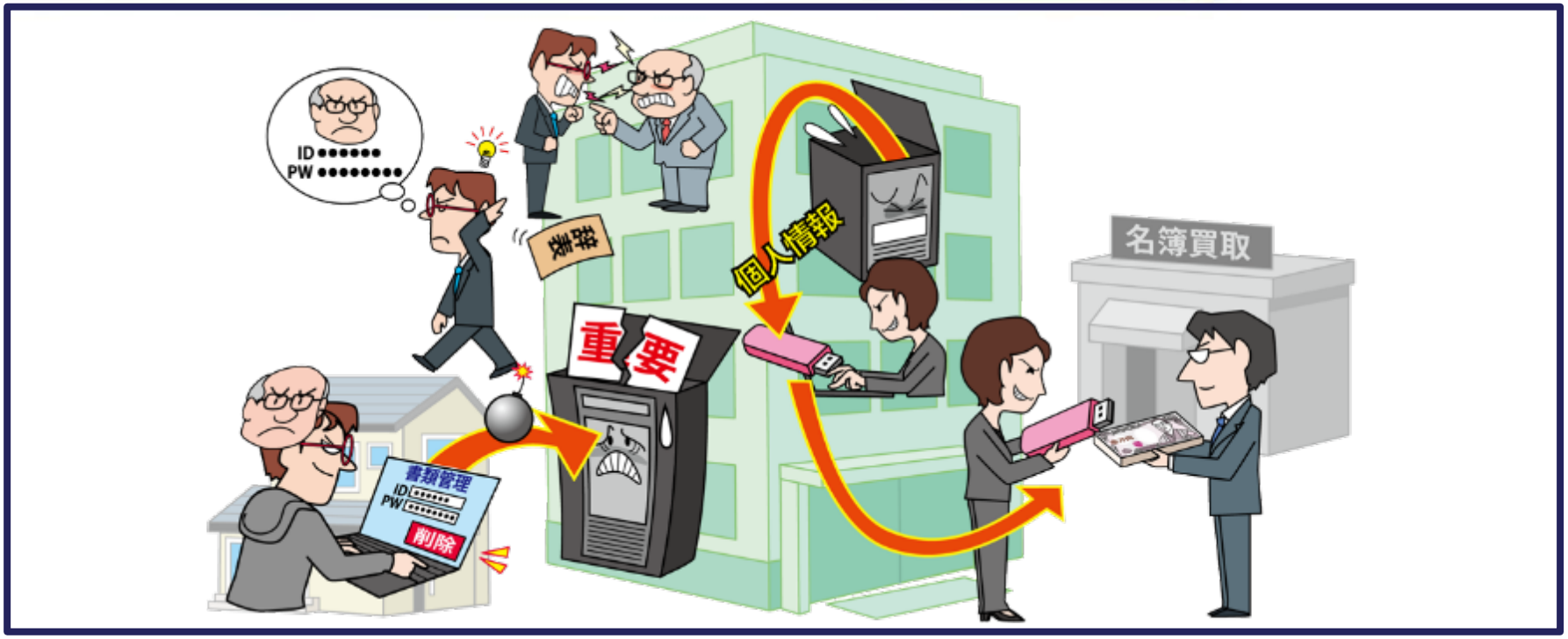
- **対策**
  - **組織(自組織に関わる組織と共に実施)**

【被害を受けた後の対応】

- 適切な報告／連絡／相談を行う
  - 上司、CSIRT、関係組織、公的機関等

【3位】内部不正による情報漏えい等の被害

～組織の情報を狙っているのは身内かも!?不正をゆるさない体制作りを～



- 組織の従業員や元従業員等による機密情報の漏えい
- 組織関係者による不正行為による、組織の社会的信用の失墜、損害賠償による経済的損失
- 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

【3位】内部不正による情報漏えい等の被害

～組織の情報を狙っているのは身内かも!?不正をゆるさない体制作りを～

IPA

- **攻撃手口**

・内部の従業員は重要情報にアクセスしやすい
・悪意をもって情報を外部に提供してしまう

- **アクセス権限の悪用**
  - 付与されたパスワードを悪用し、組織の重要情報を取得する
  - 必要以上のアクセス権限を付与していると被害が大きくなる
- **在職中に割り当てられたアカウントの悪用**
  - 在職中に使用していたアカウントを使って不正に情報を取得する
- **内部情報の不正な持ち出し**
  - USBメモリー、HDD、メール、クラウドストレージ、スマホカメラ、紙媒体等での持ち出し

【3位】内部不正による情報漏えい等の被害

～組織の情報を狙っているのは身内かも!?不正をゆるさない体制作りを～

- **2023年の事例/傾向①**
  - **顧客情報を持ち出し、名簿業者に販売**
    - 2023年10月、NTTビジネスソリューションズは同社に勤務した元派遣社員による顧客情報の不正な持ち出しを公表した
    - 同派遣社員は2013年7月から2023年1月の間に、自身が関わったシステムに管理者アカウントを悪用して不正アクセスした
    - 少なくとも 69組織の顧客情報928万件をUSBメモリーにコピーして持ち出していた
    - 持ち出した顧客情報を名簿業者に販売し、1千万円以上を対価として受け取っていたとみられ逮捕された

【出典】 NTTビジネスソリューションズに派遣された元派遣社員によるお客さま情報の不正流出について(続報)(NTTビジネスソリューションズ株式会社)
https://www.nttbizsol.jp/newsrelease/20231219140000982.html
当社に派遣されていた元派遣社員の逮捕について(NTTビジネスソリューションズ株式会社)
https://www.nttbizsol.jp/newsrelease/20240131150000999.html
NTT西系情報流出、名簿1000万円超で売却か 元派遣社員(日本経済新聞)
https://www.nikkei.com/article/DGXZQOUE07C0X0X01C23A1000000/

【3位】内部不正による情報漏えい等の被害

～組織の情報を狙っているのは身内かも!?不正をゆるさない体制作りを～

- **2023年の事例/傾向②**
  - **前職場が保有する名刺情報を転職先に提供**
    - 2023年9月、ワールドコーポレーションの元従業員が個人情報保護法違反(不正提供)等の疑いで警視庁に逮捕された
    - 同従業員は同業他社に転職する直前に、転職元の名刺情報管理システムにログインするためのIDとパスワードを転職先の従業員に共有した
    - 不正に取得された名刺情報は転職先の営業活動に使用され、成約事例もあった

【出典】 当社元従業員の逮捕について(株式会社ワールドコーポレーション)
https://worldcorp-jp.com/news/2023/20230915.html
名刺データ、管理にリスク 個人情報提供疑いで初逮捕(日本経済新聞)
https://www.nikkei.com/article/DGXZQOUE1421N0U3A910C2000000/

【3位】内部不正による情報漏えい等の被害

～組織の情報を狙っているのは身内かも!?不正をゆるさない体制作りを～

- **2023年の事例/傾向③**
  - **元勤務先に不正アクセスして社内情報を削除**
    - 2023年1月、共立電気計器の元従業員が不正アクセス禁止法違反および電子計算機損壊等業務妨害の疑いで警視庁に逮捕された
    - 本従業員は退職後に、元同僚や元上司の ID やパスワードを悪用し、社内ネットワークやクラウドに不正アクセスして、人事や技術、顧客に関する情報を削除していた
    - 人間関係を理由に退職しており、嫌がらせが目的とみられている
    - データ復旧には約660万円を要した

【出典】 元勤務先に不正アクセス、データ削除した疑い 退職していた男逮捕(朝日新聞)
https://www.asahi.com/articles/ASR1S4HC4R1SUTIL008.html

【3位】内部不正による情報漏えい等の被害

～組織の情報を狙っているのは身内かも!?不正をゆるさない体制作りを～

- **対策※1**
  - **組織(システム管理者)**

【被害の予防】

- 基本方針の策定
  - 「不正のトライアングル」※2を意識する
  - 情報取扱ポリシーの作成や、内部不正者に対する懲戒処分等を規定した就業規則等を整備する※3
- 資産の把握、対応体制の整備
- 重要情報の管理、保護
- 物理的管理の実施
- 情報リテラシー、モラルを向上させる
- 人的管理及びコンプライアンス教育の徹底

【出典】 ※1 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
※2 IPA NEWS Vol.64(2023年12月号)(IPA)
https://www.ipa.go.jp/about/ipanews/ipanews202312.html
※3 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

【3位】内部不正による情報漏えい等の被害

～組織の情報を狙っているのは身内かも!?不正をゆるさない体制作りを～

- **対策**
  - **組織(システム管理者)**

【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を監視する
  - 監視していることを従業員に周知する

【3位】内部不正による情報漏えい等の被害

～組織の情報を狙っているのは身内かも!?不正をゆるさない体制作りを～

- **対策**
  - **組織(システム管理者)**

【被害を受けた後の対応】

- 適切な報告／連絡／相談を行う
  - 上司、CSIRT、関係組織、公的機関等
- 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

【4位】標的型攻撃による機密情報の窃取

～攻撃手口は様々、隙を作らない対策を～

- メール等を利用し、特定組織のPCをウイルスに感染させる
- 組織内部に潜入し、長期にわたり侵害範囲を徐々に広げる
- 組織の機密情報窃取やシステムを破壊する

【4位】標的型攻撃による機密情報の窃取

～攻撃手口は様々、隙を作らない対策を～

IPA

- **攻撃手口**

・メールを使って標的組織を攻撃する

- **メールからウイルスに感染させる**
  - 添付ファイルを開封させる
  - メール本文のリンクにアクセスさせる
- **標的組織の従業員や職員を油断させ、不信感を抱かれにくいようにする**
  - 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する
  - 実在する組織の差出人名が使われる
  - メールのやり取りを複数回行う(やり取り型攻撃)

【4位】標的型攻撃による機密情報の窃取

～攻撃手口は様々、隙を作らない対策を～

- 攻撃手口

・Web サイトの改ざん

- 標的組織が**頻繁に利用する Web サイト**を攻撃者が**改ざん**し、標的組織の従業員や職員がその Web サイトにアクセスした際に、PCが**ウイルスに感染**する(水飲み場型攻撃)

【4位】標的型攻撃による機密情報の窃取

～攻撃手口は様々、隙を作らない対策を～

- **攻撃手口**

・不正アクセス

- **標的組織が利用するものの脆弱性を悪用して不正アクセスをし、組織内部に侵入する**
  - クラウドサービス
  - Webサーバー
  - VPN装置
- **認証情報等を窃取し、組織のシステムへ再侵入する**

【4位】標的型攻撃による機密情報の窃取

～攻撃手口は様々、隙を作らない対策を～

- **2023年の事例/傾向①**
  - **複数回のやり取りを伴う標的型メール攻撃**
    - 2023年10月、東京大学は標的型攻撃メールにより教員のPCがウイルスに感染し、情報を窃取されたことを公表した
    - 2022年7月に実在する組織の担当者を騙った人物からメールが届き、教員がやりとりをしている中でメールに記載されたURLをクリックしたところ、ウイルスに感染した
    - 最終的に教員は被害に気付かなかった
    - 教職員や学生等の個人情報や過去の試験問題等の計4,341 件が流出したおそれがある

【出典】 東京大学大学院総合文化研究科・教養学部への不正アクセスによる情報流出について(東京大学)
https://www.u-tokyo.ac.jp/focus/ja/press/z0109_00952.html
サイバー攻撃か 東大教員のパソコンに不正アクセス、個人情報4300件流出(TBS NEWS DIG)
https://newsdig.tbs.co.jp/articles/-/796546

【4位】標的型攻撃による機密情報の窃取

～攻撃手口は様々、隙を作らない対策を～

- **2023年の事例/傾向②**
  - **JAXAに不正アクセスがあったが情報は取られず**
    - 2023年11月、宇宙航空研究開発機構(JAXA)がサイバー攻撃を受け、内部ネットワークに不正アクセスされた
    - 不正アクセスを受けたのは一般業務用の管理サーバーであり、機微情報は含まれていなかった
    - 不正アクセスはネットワーク機器の脆弱性を悪用されたものとみられる
    - 外部機関から通報を受けたJAXAは文部科学省に報告し、一部のネットワークを切り離した上で、調査をしている

【出典】 JAXAにサイバー攻撃＝不正アクセス、機微情報含まず(時事通信社)
https://sp.m.jiji.com/article/show/3109334
JAXAへの不正アクセスについてまとめてみた(piyolog)
https://piyolog.hatenadiary.jp/entry/2023/11/29/123934

【4位】標的型攻撃による機密情報の窃取

～攻撃手口は様々、隙を作らない対策を～

- **2023年の事例/傾向③**
  - **ネットワーク貫通型攻撃に注意**
    - 2023年8月、IPAは企業や組織のネットワークとインターネットとの境界に設置されるセキュリティ製品の脆弱性が狙われ、ネットワーク貫通型攻撃としてAPT攻撃に利用されていると注意喚起を行った
    - ネットワーク内部へ不正アクセスされた場合、保有情報の漏えいや改ざん、他組織への攻撃の踏み台になるおそれがあるため、日々の確認や平時の備えが大切である
    - 同年5月に経済産業省が公開した「ASM(Attack Surface Management)導入ガイダンス～外部から把握出来る情報を用いて自組織の IT 資産を発見し管理する～」の活用も有効である

【出典】 インターネット境界に設置された装置に対するサイバー攻撃について～ネットワーク貫通型攻撃に注意しましょう～(IPA)
https://www.ipa.go.jp/security/security-alert/2023/alert20230801.html
「ASM(Attack Surface Management)導入ガイダンス
～外部から把握出来る情報を用いて自組織のIT資産を発見し管理する～」を取りまとめました(経済産業省)
https://www.meti.go.jp/press/2023/05/20230529001/20230529001.html

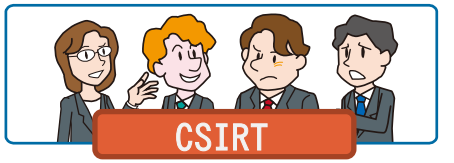
【4位】標的型攻撃による機密情報の窃取

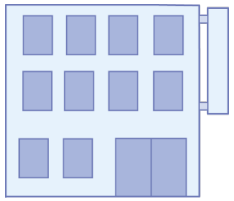
～攻撃手口は様々、隙を作らない対策を～

- **対策**
  - **組織(経営者層)**

【組織としての体制確立】

- インシデント対応体制を整備し、対応する
  - CISOを配置する
  - CSIRTを構築する
  - 有事の際の対応フローを確立する
  - 運用手順を社員へ通知する
  - 運用の訓練をする
  - 外部の協力依頼先を用意する
  - 社内規則の整備や予算確保をする





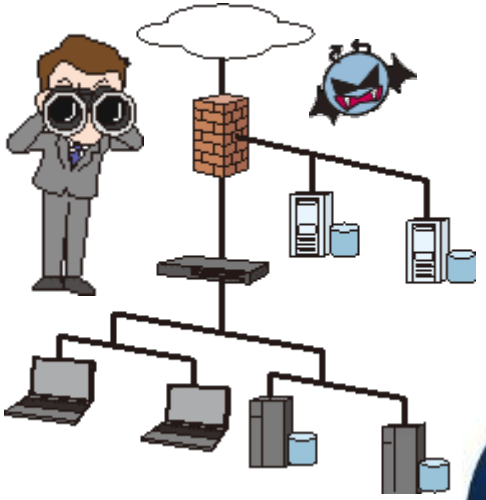
【4位】標的型攻撃による機密情報の窃取

～攻撃手口は様々、隙を作らない対策を～

- **対策**
  - **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
- 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
- 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



【4位】標的型攻撃による機密情報の窃取

～攻撃手口は様々、隙を作らない対策を～

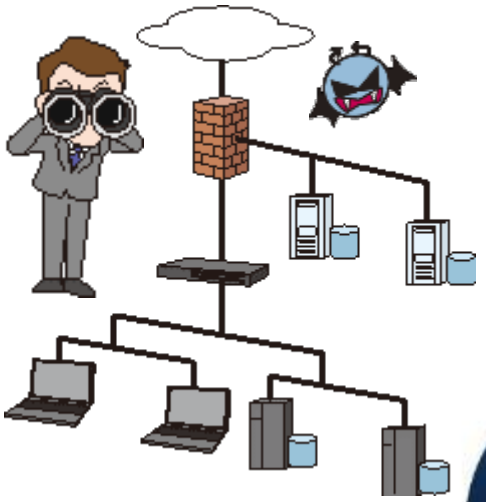
- **対策**
  - **組織(セキュリティ担当者、システム管理者)**

【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



【4位】標的型攻撃による機密情報の窃取

～攻撃手口は様々、隙を作らない対策を～

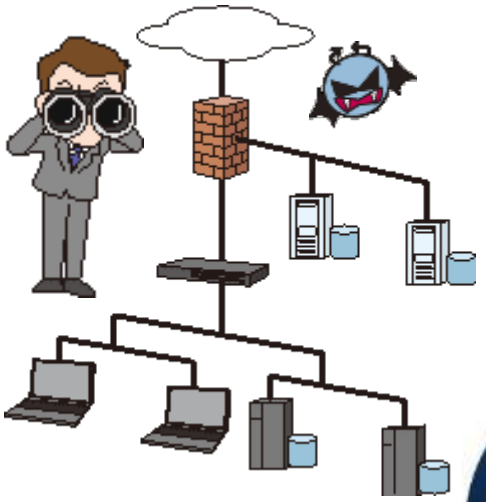
- **対策**
  - **組織(従業員、職員)**

【被害の予防(通常、組織全体で実施)】

- 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

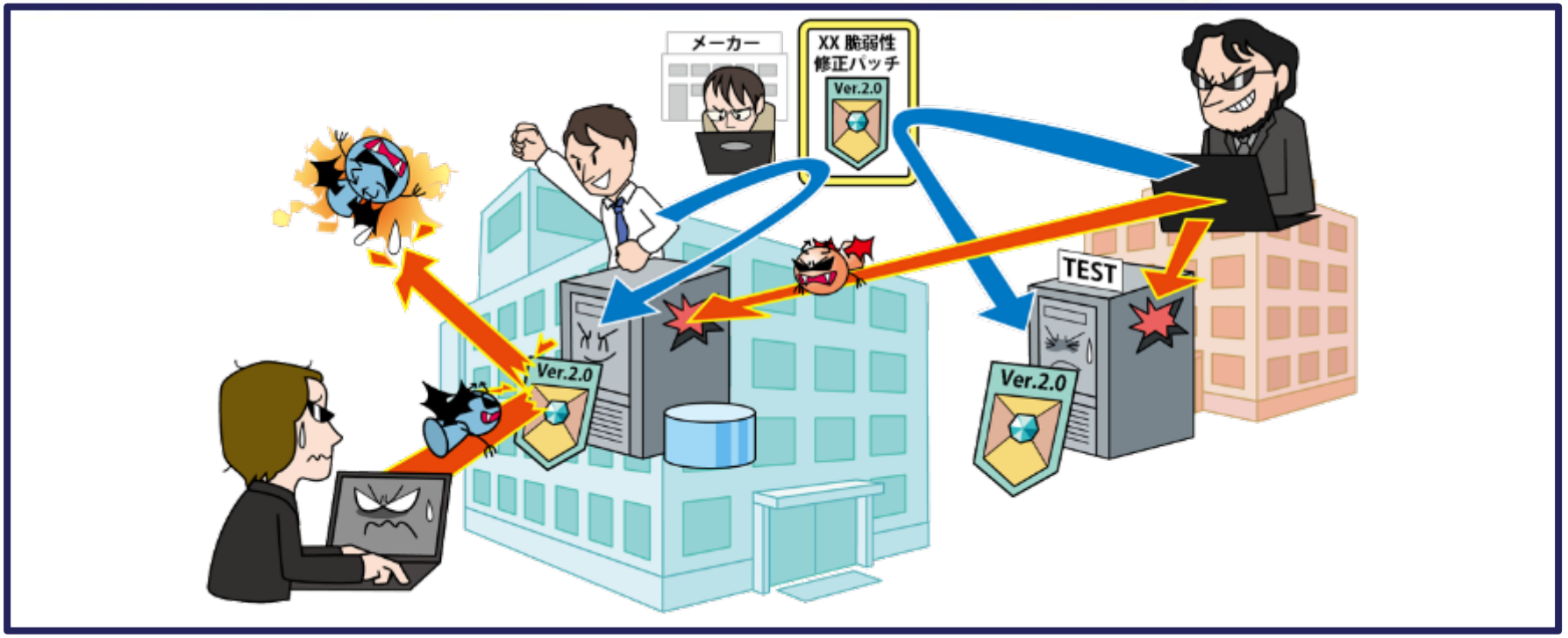
【被害を受けた後の対応】

- インシデント対応体制を整備し、対応する



【5位】修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)

～脆弱性対策情報が公開されたら即時対応を～



- 脆弱性の修正プログラム(パッチ)や回避策が公開される前に脆弱性を悪用した攻撃が行われる
- 事業やサービスの停止など、多くのシステムやユーザーに被害が及ぶ
- 脆弱性対策情報が公開された場合は、早急な対応が求められる

【5位】修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)

～脆弱性対策情報が公開されたら即時対応を～

IPA

- **攻撃手口**

・開発ベンダ―等が脆弱性を認識しないとその脆弱性に対する修正プログラムは作成されない
・その修正プログラムが公開される前の脆弱性を悪用

- **修正プログラムが公開される前に発見した(された)脆弱性を悪用**
- **悪用の手口は脆弱性毎に様々なものがある**
  - DDoS攻撃(分散型サービス妨害攻撃)
  - 簡易プログラム(スクリプト)の実行
  - 特権アカウントの作成

【5位】修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)

～脆弱性対策情報が公開されたら即時対応を～

- **2023年の事例/傾向①**
  - **HTTP/2の脆弱性を悪用したゼロデイ攻撃**
    - 2023年8月、HTTP/2プロトコルの脆弱性を狙った大規模なDDoS攻撃が確認される
    - 一連の攻撃で1秒間に3億9,800万件を超えるリクエストが発生しており、過去最大規模の4,600万件のリクエストが発生したケースをはるかに上回る規模の攻撃である
    - この攻撃は、HTTP/2ラピッドリセット攻撃と呼ばれており、HTTP/2 をサポートする多くのソフトウェアに影響を与える
    - 影響を受けるソフトウェアの開発ベンダー間で情報共有が進められて、パッチやアップデートが提供された

【出典】 ラピッドリセット攻撃」が発生 - 1秒間で約4億リクエスト(Security NEXT)
https://www.security-next.com/150165

【5位】修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)

～脆弱性対策情報が公開されたら即時対応を～

- **2023年の事例/傾向②**
  - **「WinRAR」の脆弱性を悪用したゼロデイ攻撃**
    - 2023年4月、ファイル圧縮ソフトの「WinRAR」に複数の脆弱性が存在しており、一部の脆弱性がゼロデイ攻撃に悪用されていることが分かった
    - 圧縮ファイル内のファイルのプレビューを行おうとすると、同名のフォルダ内に配置されたスクリプトを実行させることが可能になるという脆弱性であった
    - 2023年8月2日、開発元である「RARLAB」は、脆弱性の修正をしたバージョンアップ版「WinRAR 6.23」をリリースしている

【出典】 4月以降「WinRAR」狙うゼロデイ攻撃が発生 - 最新版に更新を(Security NEXT)
https://www.security-next.com/148924

【5位】修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)

～脆弱性対策情報が公開されたら即時対応を～

- **2023年の事例/傾向③**
  - **Cisco Systems製品へのゼロデイ攻撃**
    - 2023年10月、Cisco Systems は「Cisco IOS XE」に、リモートから認証がなくとも特権アカウントを作成できる脆弱性があることを公表した
    - 2023年9月中旬よりゼロデイ攻撃が行われていることも公表した
    - 同社は、顧客のサポート中に脆弱性を確認した
    - 同製品の利用者に対して、開発ベンダー等が推奨する対策を講じるとともに、侵害を受けていないか確認するように呼びかけている

【出典】「IOS XE」の深刻なゼロデイ脆弱性 - JPCERT/CCも攻撃被害を確認(Security NEXT)
https://www.security-next.com/150345

【5位】修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)

～脆弱性対策情報が公開されたら即時対応を～

- **参考情報（2024年の最新事例）**
  - **Ivanti VPN製品へのゼロデイ攻撃**
    - 現地時間2024年1月10日にIvantiからIvanti Connect Secure および Ivanti Policy Secure Gatewaysに関する脆弱性情報が公開された
    - 本脆弱性（CVE-2024-21887,CVE-2023-46805）を悪用されると、認証を回避されて第三者にコマンドを実行されるおそれがあった
    - 日本時間1月11日にIPAにおいても注意喚起を行っており、1月15日には国内での悪用も確認され、侵害の調査などの対応を推奨した
    - その後さらに、CVE-2024-21888,CVE-2024-21893,CVE-2024-22024などの脆弱性も確認され、2月16日までに修正パッチが順次公開された

【出典】CVE-2023-46805 (Authentication Bypass) & CVE-2024-21887 (Command Injection) for Ivanti Connect Secure and Ivanti Policy Secure Gateways (Ivanti)
https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US
KB CVE-2023-46805 (Authentication Bypass) & CVE-2024-21887 (Command Injection) for Ivanti Connect Secure and Ivanti Policy Secure Gateways (Ivanti)
https://forums.ivanti.com/s/article/KB-CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US
Ivanti Connect Secure（旧Pulse Connect Secure）および Ivanti Policy Secure Gateways の脆弱性対策について(CVE-2023-46805 等) (IPA)
https://www.ipa.go.jp/security/security-alert/2023/20240111.html
Ivanti Connect SecureおよびIvanti Policy Secureの脆弱性（CVE-2023-46805およびCVE-2024-21887）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/2024/at240002.html

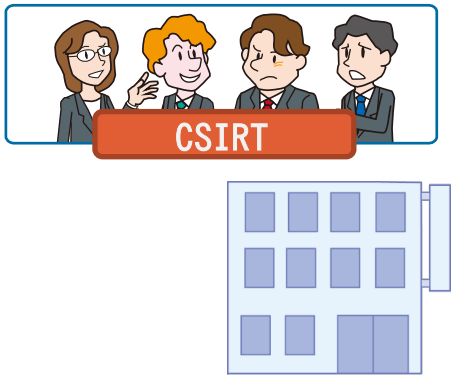
【5位】修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)

～脆弱性対策情報が公開されたら即時対応を～

- **対策**
  - **組織(経営者層)**

【被害の予防】

- インシデント対応体制を整備し、対応する
  - CISOを配置する
  - CSIRTを構築する
  - 有事の際の対応フローを確立する
  - 運用手順を社員へ通知する
  - 運用の訓練をする
  - 外部の協力依頼先を用意する
  - 社内規則の整備や予算確保をする



【5位】修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)

～脆弱性対策情報が公開されたら即時対応を～

- **対策**
  - **組織(ソフトウェアの利用者、システム管理者)**

【被害の予防】

- 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
- 利用するソフトウェアの脆弱性情報の収集と周知、対策状況の管理
- サーバーやクライアント、ネットワークに適切なセキュリティ対策を行う

【被害の早期検知】

- サーバーやクライアント、ネットワークに適切なセキュリティ対策を行う

【5位】修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)

～脆弱性対策情報が公開されたら即時対応を～

- **対策**
  - **組織(ソフトウェアの利用者、システム管理者)**

【修正プログラムのリリース前の対応】

- 回避策や緩和策の適用
- 当該ソフトウェアの一時的な使用停止、場合によってはサービスの停止も検討する

【修正プログラムリリース後の対応】

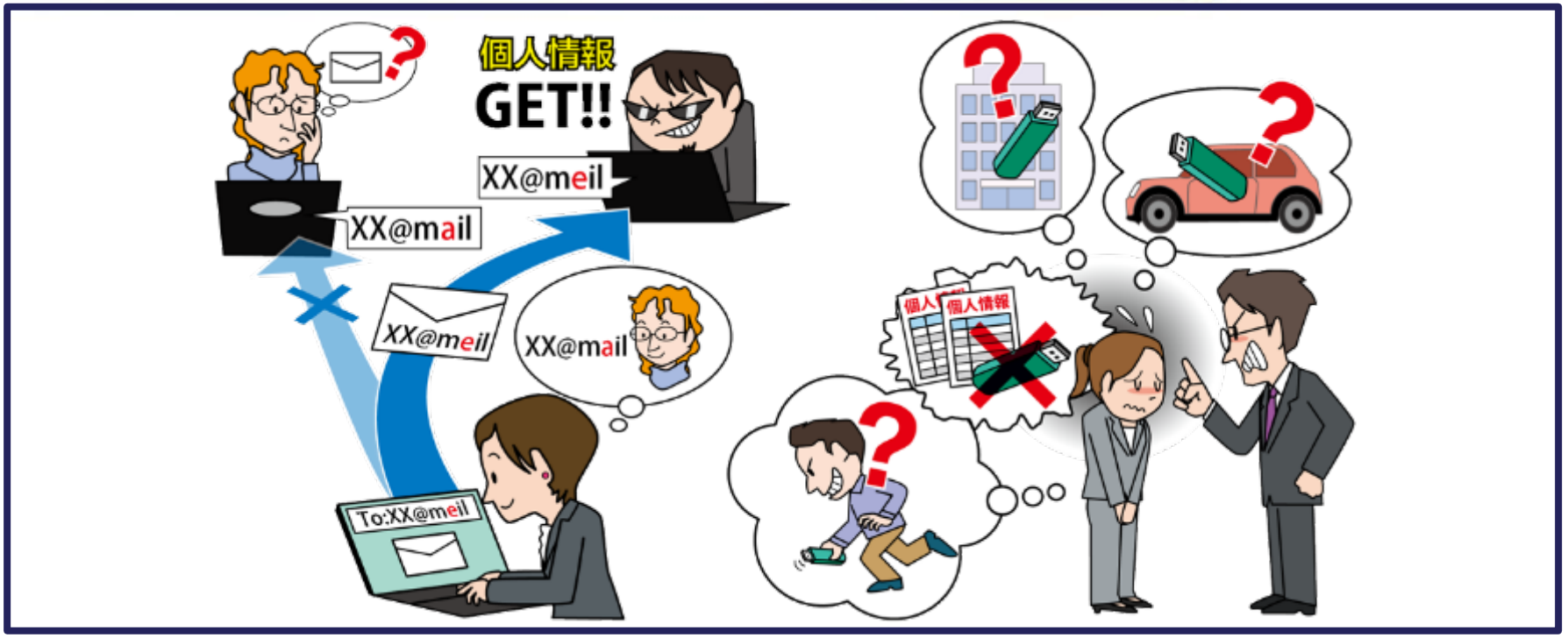
- 修正プログラムの適用

【被害を受けた後の対応】

- 影響調査、原因の追究、対策の強化
- 適切な報告／連絡／相談を行う
  - 上司、CSIRT、関係組織、公的機関等

【6位】不注意による情報漏えい等の被害

～その設定、本当に大丈夫？確認は慎重に！～



- 従業員の不注意等によって意図せず機密情報を漏えい
- 情報漏えいすることによる社会的信用の失墜、経済的損失、漏えいした情報の悪用による二次被害

【6位】不注意による情報漏えい等の被害

～その設定、本当に大丈夫？確認は慎重に！～

IPA

- **要因**

・情報を扱う本人の問題

- **情報を取り扱う人の情報リテラシーの低さ**
  - 扱う情報の機密性や重要性等を理解していないため、不用意に外部へ情報漏えいしてしまう
    - 重要情報が記載されたメールの宛先を間違う
    - 重要情報が入った端末を紛失する
    - 重要情報を私的に利用して外部のWebサイト等に公開する
- **情報を取り扱う際の本人の状況**
  - 体調不良や多忙等により、従業員の注意力が散漫になり、メールの誤送信等による情報漏えい事故を起こしてしまう

【6位】不注意による情報漏えい等の被害

～その設定、本当に大丈夫？確認は慎重に！～

- **要因**

・組織規程および情報を取り扱うプロセスの不備

- **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**

・誤送信を想定した偽のメールアドレスの存在

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

【6位】不注意による情報漏えい等の被害

～その設定、本当に大丈夫？確認は慎重に！～

- **不注意による情報漏えいの例**
  - メールの誤送信(宛先誤り、To/Cc/Bccの設定間違い、添付ファイル間違い等)
  - Webサイトの設定不備(重要情報のマスキングの不備、公開ファイルや参照権限の誤り、クラウドの設定の誤り等)
  - 外部サイトへの安易な機密情報の入力
  - 重要情報を保存した情報端末(PCやスマートフォン等)、記録媒体(USBメモリー等)の紛失
  - 重要書類(紙媒体)の紛失

【6位】不注意による情報漏えい等の被害

～その設定、本当に大丈夫？確認は慎重に！～

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

【出典】「gmail」ドメインを「gmai」と誤記、2年半放置で800人分の情報漏えいか 鹿児島大が「ドッペルゲンガー・ドメイン」の毒牙に(ITmedia NEWS)
https://www.itmedia.co.jp/news/articles/2302/13/news085.html

【6位】不注意による情報漏えい等の被害

～その設定、本当に大丈夫？確認は慎重に！～

- **2023年の事例/傾向②**
  - **設定ミスによる個人情報漏えい**
    - 2023年12月、大阪市コミュニティ協会は委託業務を受けた際に利用していたGoogleフォームに入力された個人情報を、第三者が閲覧できる状態にあったことを公表した
    - 入力した個人情報を閲覧できる設定がONになっていたが、フォーム作成時に、回答後に表示される画面の確認をしないまま運用を開始したことが原因であった
    - Googleフォームに入力を済ませたユーザーの指摘で発覚した
    - 連絡に気が付いた直後にGoogleフォームを修正し、関係者への連絡を完了させており、再発防止に取り組むとしている

【出典】 申込フォームで個人情報が閲覧可能に - 大阪市コミュニティ協会(Security NEXT)
https://www.security-next.com/151685

【6位】不注意による情報漏えい等の被害

～その設定、本当に大丈夫？確認は慎重に！～

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

【出典】 個人情報を含むUSBメモリの紛失および発見について(天草市)
https://www.city.amakusa.kumamoto.jp/kiji00311498/index.html

【6位】不注意による情報漏えい等の被害

～その設定、本当に大丈夫？確認は慎重に！～

- **対策**
  - **組織(当事者)**

【被害の予防(被害に備えた対策を含む)】

- 情報リテラシー、モラルを向上させる
- 確認プロセスに基づく運用
- 特定の担当者に業務が集中しない体制の構築
- 取り扱う情報の重要度を規定し、それに合わせた運用を行う
- 情報の保護(暗号化、認証)、機密情報の格納場所の把握、可視化
- DLP(情報漏えい対策)製品の導入
- 外部に持ち出す情報や端末の制限
- 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

【6位】不注意による情報漏えい等の被害

～その設定、本当に大丈夫？確認は慎重に！～

- **対策**
  - **組織(当事者)**

【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
  - 上司、CSIRT、関係組織、公的機関等
- インシデント対応体制を整備し、対応する

【6位】不注意による情報漏えい等の被害

～その設定、本当に大丈夫？確認は慎重に！～

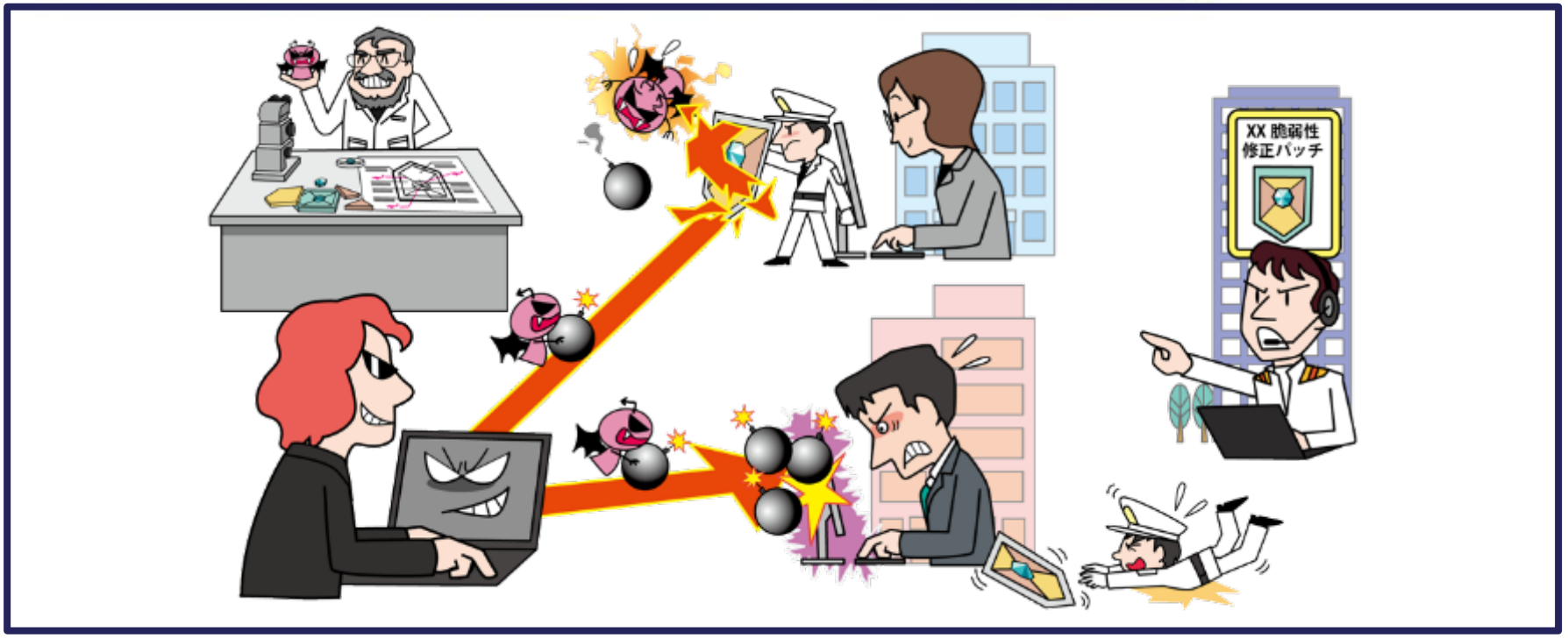
- **対策**
  - **組織(被害者)**

【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
  - 上司、CSIRT、関係組織、公的機関等

【7位】脆弱性対策情報の公開に伴う悪用増加

～放置せず、傷口が広がる前に速やかな処置を～



- 脆弱性対策のために公開された脆弱性情報を攻撃者が悪用する
- 広く利用されている製品の脆弱性の場合は被害が広範囲に及ぶ
- 脆弱性情報の公開後、それらを悪用した攻撃が発生するまでの時間が近年は短くなっている傾向がある

【7位】脆弱性対策情報の公開に伴う悪用増加

～放置せず、傷口が広がる前に速やかな処置を～

- **攻撃手口**

・対策前の脆弱性(Nデイ脆弱性)を悪用

- **公開された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**
  - 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
  - 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

【7位】脆弱性対策情報の公開に伴う悪用増加

～放置せず、傷口が広がる前に速やかな処置を～

IPA

♦ 攻撃手口

・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**短期間で作成される**
- **ダークウェブ上**のWebサイト等での**販売**や、**攻撃サービスとして提供**されたりする
- 誰でも利用可能なオープンソースのツールに**脆弱性を利用する機能が実装**され、それを**悪用**される

【7位】脆弱性対策情報の公開に伴う悪用増加

～放置せず、傷口が広がる前に速やかな処置を～

- **2023年の事例/傾向①**
  - **ソフトウェアの修正版公開後に攻撃活動の増加**
    - 2023年10月25日、Apache Software Foundationは Apache ActiveMQ等で、リモートからコード実行が可能な脆弱性を対策したバージョンを公表した
    - 本脆弱性は技術情報や実証コードが公開されており、Rapid7によると10月27日に脆弱性を悪用したと見られるランサムウェアの活動を同社の複数の顧客で確認していた
    - NICTのダークネット観測網では、同脆弱性に関連した通信を10月27日頃 から観測し、11月26日頃には更なる通信の増加が確認されてボットとみられる感染活動を観測した

【出典】「Apache ActiveMQ」の脆弱性が標的に - ランサム攻撃にも悪用か(Security NEXT)
https://www.security-next.com/150846
CVE-2023-46604: Apache ActiveMQ の悪用の疑い(ラピッドセブン・ジャパン株式会社)
https://www.rapid7.com/ja/about/japan-blog-and-news/etr-suspected-exploitation-of-apache-activemq-cve-2023-46604/
ActiveMQの脆弱性(CVE-2023-46604)を悪用したボットの感染活動について(NICTER Blog)
https://blog.nicter.jp/2023/12/cve-2023-46604/

【7位】脆弱性対策情報の公開に伴う悪用増加

～放置せず、傷口が広がる前に速やかな処置を～

- **2023年の事例/傾向②**
  - **VPN機器の脆弱性が断続的な攻撃の対象に**
    - 2023年5月、Array Networksが提供する「Array AG シリーズ」の脆弱性を悪用した標的型攻撃が観測されていることをJPCERTコーディネーションセンターが注意喚起した
    - インターネットとの境界に設置されるセキュリティ製品の脆弱性が狙われ、ネットワーク貫通型攻撃が行われているとして、 IPAにおいても2023年8月に注意喚起を行った
    - 本脆弱性は２つあり、それぞれ2022年の9月、2023年3月に修正されているが、海外拠点も標的となっており、自組織の海外拠点における対策や侵害調査を行うことも推奨されている

【出典】 Array Networks Array AGシリーズの脆弱性を悪用する複数の標的型サイバー攻撃活動に関する注意喚起
(一般社団法人JPCERTコーディネーションセンター)
https://www.jpcert.or.jp/at/2023/at230020.html
インターネット境界に設置された装置に対するサイバー攻撃について～ネットワーク貫通型攻撃に注意しましょう～(IPA)
https://www.ipa.go.jp/security/security-alert/2023/alert20230801.html
Array Networks製VPN機器、標的型攻撃の対象に - 侵害状況の確認を(Security NEXT)
https://www.security-next.com/149480

【7位】脆弱性対策情報の公開に伴う悪用増加

～放置せず、傷口が広がる前に速やかな処置を～

- **2023年の事例/傾向③**
  - **脆弱性を修正した機器へ継続的な攻撃**
    - 2023年5月19日、Barracuda Networksは同社の製品のESGにリモートからシステムコマンドが実行可能となる脆弱性があることを特定し、翌日に修正パッチを公開した
    - 本脆弱性の修正対応後も、特定の組織では攻撃者による継続的な攻撃活動が確認されている
    - 同社では脆弱性の最初の悪用は2022年10月とし、侵害された組織にアプライアンスの交換を推奨している
    - FBI、IPA、JPCERTコーディネーションセンターにおいても注意喚起を行っており、修正パッチを済ませた組織でも追加の侵害調査を行う事を推奨した

【出典】 Barracuda製メールセキュリティ製品に脆弱性 - すでに悪用も(Security NEXT)
https://www.security-next.com/146475
Barracuda、「ESGアプライアンス」の交換を呼びかけ(Security NEXT)
https://www.security-next.com/146896
Barracuda 製 Email Security Gateway Appliance (ESG) の脆弱性について(CVE-2023-7102)(CVE-2023-7101)(IPA)
https://www.ipa.go.jp/security/security-alert/2023/alert20231225.html
Barracuda Email Security Gateway(ESG)の脆弱性(CVE-2023-2868)を悪用する継続的な攻撃活動に関する注意喚起
(一般社団法人JPCERTコーディネーションセンター)
https://www.jpcert.or.jp/at/2023/at230017.html

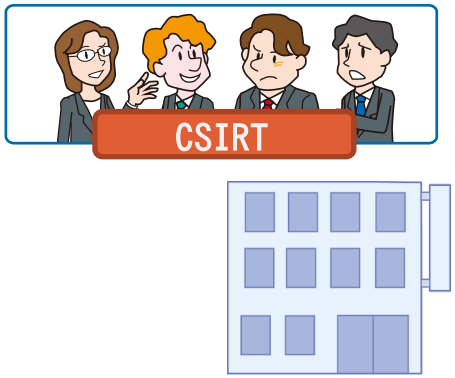
【7位】脆弱性対策情報の公開に伴う悪用増加

～放置せず、傷口が広がる前に速やかな処置を～

- **対策**
  - **組織(経営者層)**

【被害の予防】

- インシデント対応体制を整備し、対応する
  - CISOを配置する
  - CSIRTを構築する
  - 有事の際の対応フローを確立する
  - 運用手順を社員へ通知する
  - 運用の訓練をする
  - 外部の協力依頼先を用意する
  - 社内規則の整備や予算確保をする



【7位】脆弱性対策情報の公開に伴う悪用増加

～放置せず、傷口が広がる前に速やかな処置を～

- **対策**
  - **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】

- 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

【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
  - 上司、CSIRT、関係組織、公的機関等
- インシデント対応体制を整備し、対応する

【7位】脆弱性対策情報の公開に伴う悪用増加

～放置せず、傷口が広がる前に速やかな処置を～

- **対策**
  - **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

【8位】ビジネスメール詐欺による金銭被害

～組織までも振り込め詐欺の標的に～

- 取引先や経営者とやりとりするようなビジネスメールを装う
- メールを巧妙に細工し、企業の金銭を取り扱う担当者を騙す
- 攻撃者が用意した口座へ送金させる

【8位】ビジネスメール詐欺による金銭被害

～組織までも振り込め詐欺の標的に～

- 攻撃手口

・偽装、なりすまし、悪用、窃取

- 取引先との**請求書の偽装**
- 経営者等への**なりすまし**
- 窃取した**メールアカウントの悪用**
- 社外の権威ある第三者への**なりすまし**
- 詐欺の準備行為と思われる**情報の窃取**

【8位】ビジネスメール詐欺による金銭被害

～組織までも振り込め詐欺の標的に～

- **2023年の事例/傾向①**
  - **メールと電話を併用したなりすまし**
    - 2023年8月、サイバー情報共有イニシアティブ(J-CSIP)が同年5月にメールと電話を組み合わせたビジネスメール詐欺が行われたことを報告した
    - 攻撃者は標的組織の会長になりすまして同組織の海外関連会社の社長にメールを送信し、さらに専務になりすまして発信元番号を同組織の代表番号に偽装して電話で連絡をしていた
    - 被害者は会話からなりすましに気が付き指摘したところ、一方的に通話を切られ、金銭的な被害等は発生しなかった
    - 生成AI技術を用いたディープフェイクの音声が悪用された可能性もあるため、J-CSIPは類似した手口に警戒するよう注意喚起をした

【出典】 サイバー情報共有イニシアティブ(J-CSIP)運用状況[2023 年 4 月～6 月](IPA)
https://www.ipa.go.jp/security/j-csip/ug65p9000000nkvm-att/fy23-q1-report.pdf

【8位】ビジネスメール詐欺による金銭被害

～組織までも振り込め詐欺の標的に～

- **2023年の事例/傾向②**
  - **信頼できる取引先を騙るメール詐欺**
    - 2023年12月、スリー・ディー・マトリックスは、支払口座の変更依頼が書かれた取引先の名を騙るメールに従い、虚偽の銀行口座に振り込みをしたことを公表した
    - その後も同様の振り込みをし、合計2回の総額2億円を振り込んだことも公表した
    - その取引先とは信頼関係があったため、同社は振込先口座の変更依頼の理由を直接電話で確認していなかった
    - 再発防止策として、送金プロセスの見直しなどを挙げている

【出典】 送金詐欺による資金流出被害のお知らせ(株式会社スリー・ディー・マトリックス)
https://pdf.irpocket.com/C7777/ZoWa/awjA/EOHM.pdf

【8位】ビジネスメール詐欺による金銭被害

～組織までも振り込め詐欺の標的に～

- **対策**
  - **組織**

【被害の予防(被害に備えた対策を含む)】

- ビジネスメール詐欺への認識を深める
- ガバナンスが機能する業務フローの構築
- メールに依存しない業務フローの構築
- メールの電子署名の付与(S/MIMEやPGP)
- DMARCの導入
- パスワードを適切に運用する
- メールだけでなく複数の手段での事実確認
- 普段とは異なるメールに注意する
- 判断を急がせるメールに注意

【8位】ビジネスメール詐欺による金銭被害

～組織までも振り込め詐欺の標的に～

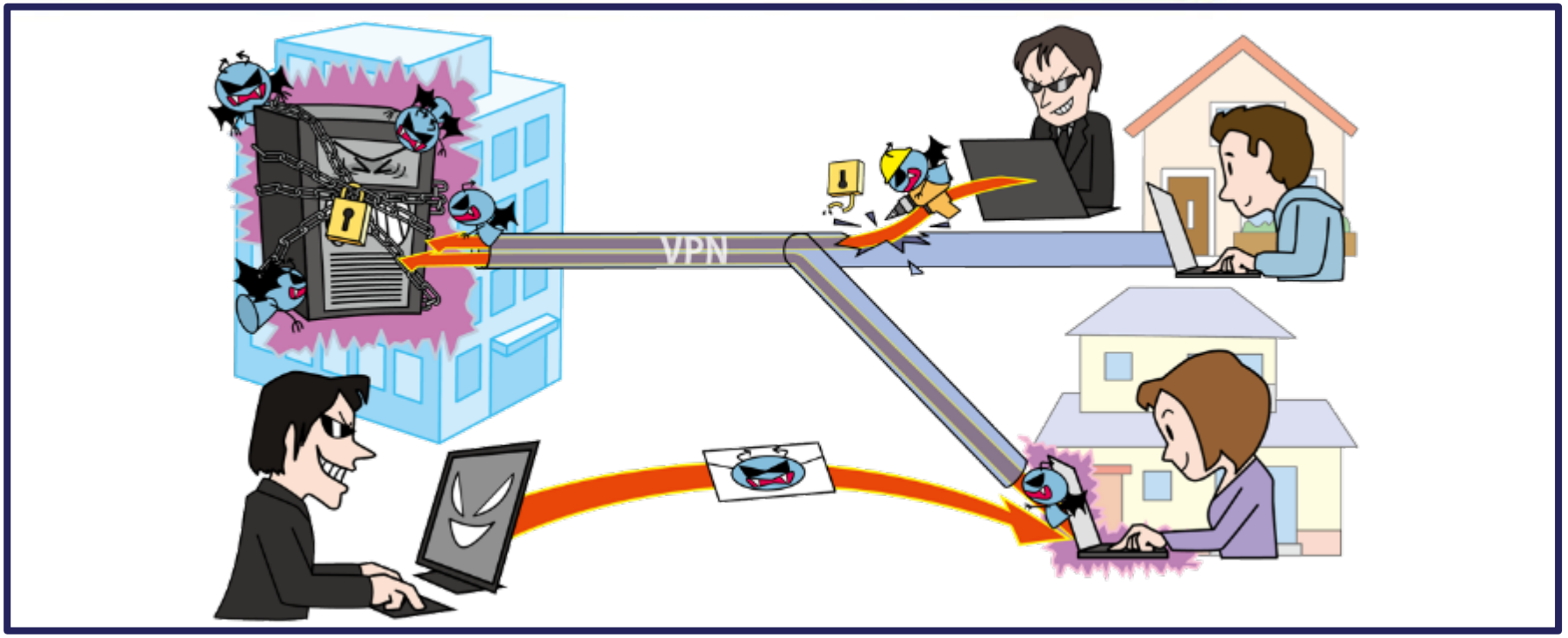
- **対策**
  - **組織**

【被害を受けた後の対応】

- 適切な報告／連絡／相談を行う
  - 上司、CSIRT、関係組織、公的機関等
- 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
- パスワードを適切に運用する

【9位】テレワーク等のニューノーマルな働き方を狙った攻撃

～狙われ続けるテレワーク環境、セキュリティ対策を～



- 2020年以降、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
- VPN等の本格的な活用がされる中、それらを狙った攻撃が発生
- 業務環境に脆弱性があると、Web会議をのぞき見されるリスクが高まる

【9位】テレワーク等のニューノーマルな働き方を狙った攻撃

～狙われ続けるテレワーク環境、セキュリティ対策を～

IPA

- **攻撃手口/発生要因**

・テレワーク環境や管理体制の不備

- **テレワーク用製品の脆弱性を悪用して不正アクセスする**
  - 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する
    - 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
    - Web会議サービスの脆弱な設定を悪用してWeb会議をのぞき見する
- **テレワーク移行時のまま運用している脆弱なテレワーク環境を攻撃する**
- **脆弱な私物PCや自宅ネットワークの利用を狙う**
  - 適切なセキュリティ対策が施されていない私有端末および自宅のネットワーク環境でテレワークを行うと情報を盗聴されるおそれがある

【9位】テレワーク等のニューノーマルな働き方を狙った攻撃

～狙われ続けるテレワーク環境、セキュリティ対策を～

- **2023年の事例/傾向①**
  - **在宅勤務のために用意したリモートアクセス経路より侵入の疑い**
    - 2023年10月、セイコーグループは顧客や取引先担当者等の個人情報約60,000件が流出したことを公表した
    - 原因は在宅勤務のために用意したリモートアクセス経路より侵入されたものとみられている
    - ランサムウェアに感染し、データセンターや国内拠点の一部サーバー内部に保存されていたデータの暗号化もされた

【出典】 ランサムウェアによる個人情報流出を確認、リモートアクセス経路より侵害か - セイコー(Security NEXT)
https://www.security-next.com/150579
当社サーバに対する不正アクセスに関するお知らせ(第３報)(セイコーグループ株式会社)
https://www.seiko.co.jp/information/202310251000.html

【9位】テレワーク等のニューノーマルな働き方を狙った攻撃

～狙われ続けるテレワーク環境、セキュリティ対策を～

- **2023年の事例/傾向②**
  - **Web会議サービスの脆弱性**
    - Microsoftは2023年10月に、Teamsに影響する脆弱性(CVE-2023-4863)を、Zoomは2023年11月に、Zoom Roomsに影響する脆弱性(CVE-2023-43590)を対策し、最新版リリースした
    - セキュリティ対策は定期的に行われており、最新版の製品を利用していない場合、攻撃を受けるリスクが高くなるため、利用者には迅速なアップデートが求められている

【出典】 ビデオ会議サービスの「Zoom」、脆弱性9件を修正(Security NEXT)
https://www.security-next.com/151283
WebPのゼロデイ脆弱性は「Teams」や「Skype」にも ～Microsoftが影響製品を公表【10月10日追記】(窓の社)
https://forest.watch.impress.co.jp/docs/news/1536304.html

【9位】テレワーク等のニューノーマルな働き方を狙った攻撃

～狙われ続けるテレワーク環境、セキュリティ対策を～

- **2023年の事例/傾向③**
  - **狙われ続けるテレワーク環境**
    - 警察庁によると、令和5年上半期におけるランサムウェア被害の感染経路としてVPN機器経由のものが35件で最も多く、全体の約71%を占めていた
    - リモートデスクトップから侵入したものは5件で全体の約10%を占めていた
    - テレワークに利用される機器等の脆弱性や強度の低い認証情報を悪用されたものが全体の約82%を占めていた

【出典】 令和５年上半期におけるサイバー空間をめぐる脅威の情勢等について(警察庁)
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R05_kami_cyber_jousei.pdf

【9位】テレワーク等のニューノーマルな働き方を狙った攻撃

～狙われ続けるテレワーク環境、セキュリティ対策を～

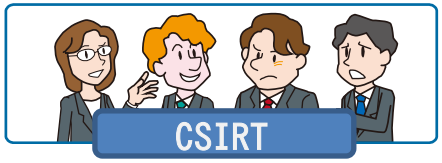
- **対策**
  - **個人(テレワーカー)**

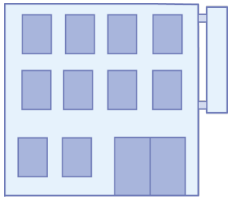
【被害の予防】

- 組織のテレワークのルールを順守する
  (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
  - 上司、CSIRT、関係組織、公的機関等





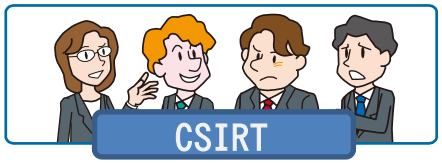
【9位】テレワーク等のニューノーマルな働き方を狙った攻撃

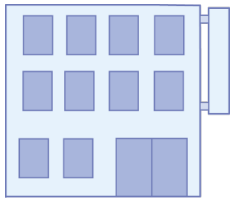
～狙われ続けるテレワーク環境、セキュリティ対策を～

- **対策**
  - **組織(経営者層)**

【組織としての体制確立】

- インシデント対応体制を整備し、対応する
  - CISOを配置する
  - CSIRTを構築する
  - 有事の際の対応フローを確立する
  - 運用手順を社員へ通知する
  - 運用の訓練をする
  - 外部の協力依頼先を用意する
  - 社内規則の整備や予算確保をする
  - テレワーク環境ならではの連絡方法や対応手順の作成
- テレワークのセキュリティポリシーを策定する



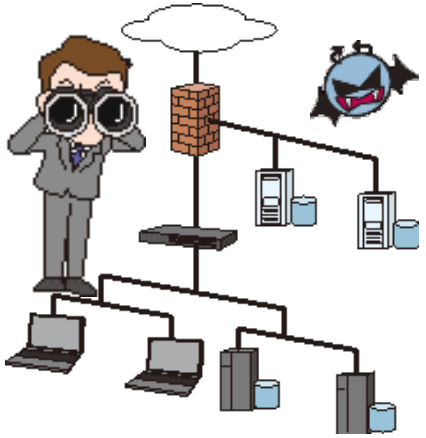


【参考】 テレワークを行う際のセキュリティ上の注意事項(IPA)
https://www.ipa.go.jp/security/anshin/measures/telework.html

【9位】テレワーク等のニューノーマルな働き方を狙った攻撃
～狙われ続けるテレワーク環境、セキュリティ対策を～

- **対策**
  - **組織(セキュリティ担当者、システム管理者)**

【被害の予防】



- シンクライアント、VDI、VPN、ZTNA/SDP等の<u>セキュリティに強いテレワーク環境</u>を採用する
- テレワークの<u>規程や運用規則を整備</u>する
  - 組織支給PCと私物PCの違いも考慮する
- <u>情報リテラシー、モラルを向上</u>させる
- サーバーやクライアント、ネットワークに<u>適切なセキュリティ対策</u>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

【9位】テレワーク等のニューノーマルな働き方を狙った攻撃

～狙われ続けるテレワーク環境、セキュリティ対策を～

- **対策**
  - **組織(セキュリティ担当者、システム管理者)**

【被害の早期検知】

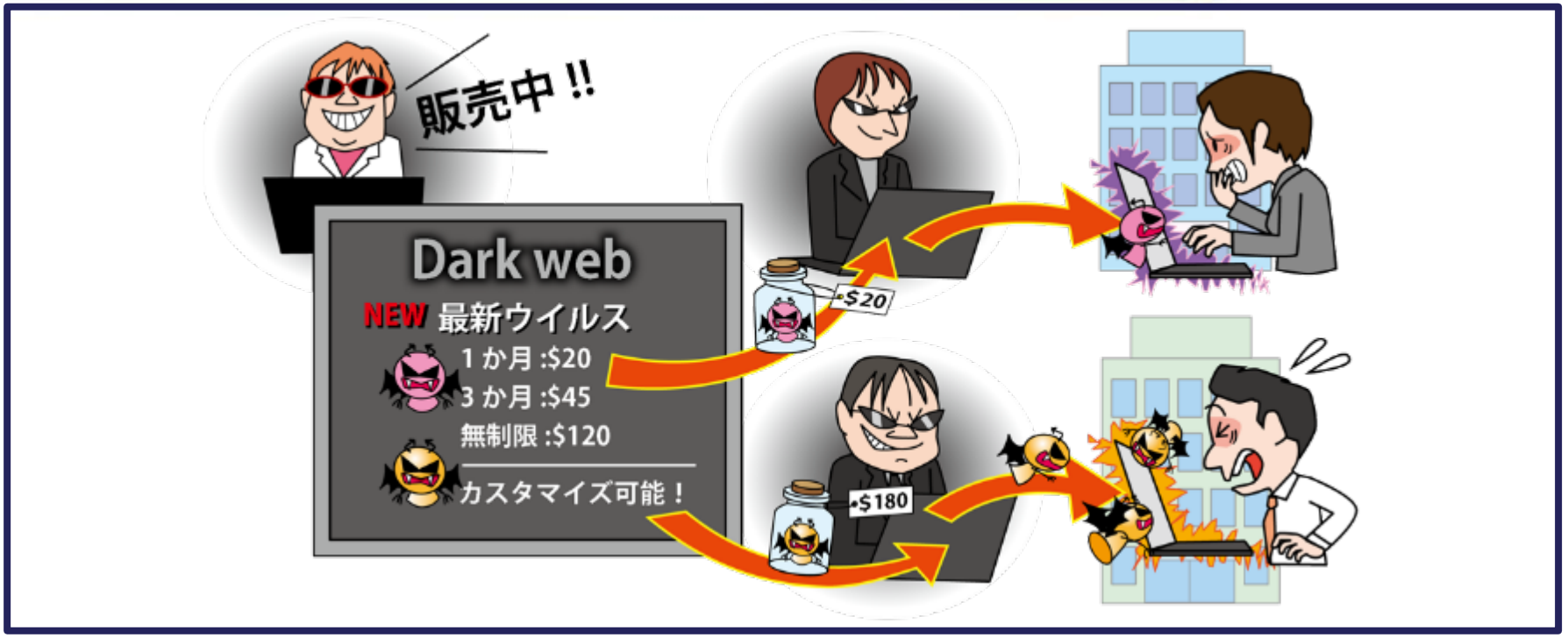
- サーバーやクライアント、ネットワークに適切なセキュリティ対策を行う

【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

【10位】犯罪のビジネス化(アンダーグラウンドサービス)

～そのパスワード、すでに誰かが知っているかも？～



- サイバー犯罪に使用するサービスやツール等の取引市場が存在する
- 通常のブラウザでは検索できないWebサイト上に存在する
- 専門知識は不要で容易にサイバー攻撃が可能になってきている

【10位】犯罪のビジネス化(アンダーグラウンドサービス)

～そのパスワード、すでに誰かが知っているかも？～

- **攻撃手口**
  - **購入したサービスやツールを利用して攻撃する**
    - 攻撃の代行サービスや攻撃に利用できるツールを取引する
      - ランサムウェアや不正アクセスの手段を販売するサービスが確認されている
  - **購入した認証情報を利用してWebへ不正ログインする**
    - 窃取した個人情報や認証情報を販売・購入してWebサービス等に不正ログインする
  - **サイバー犯罪に加担する人材のリクルートをする**
    - 組織的に行われるサイバー犯罪の人材確保をする

【10位】犯罪のビジネス化(アンダーグラウンドサービス)

～そのパスワード、すでに誰かが知っているかも？～

- **2023年の事例/傾向①**
  - **ChatGPTのアカウントを売買**
    - 2023年4月、チェック・ポイント・リサーチはChatGPTの有料アカウントの取引増加を警告した
    - アカウントを乗っ取ることにより情報の漏えいにつながり、有料アカウントに紐づいているクレジットカード情報等の窃取が可能になる
    - 宣伝目的で最初にいくつかの有料アカウントを無料で提供し、巧妙に購入につなげようとしているものもある

【出典】 チェック・ポイント・リサーチ、ChatGPTに関する新たな懸念となる窃取された有料アカウントの売買増加を確認(PR TIMES)
https://prtimes.jp/main/html/rd/p/000000202.000021207.html
New ChatGPT4.0 Concerns: A Market for Stolen Premium Accounts(Check Point Software Technologies Ltd.)
https://blog.checkpoint.com/security/new-chatgpt4-0-concerns-a-market-for-stolen-premium-accounts/

【10位】犯罪のビジネス化(アンダーグラウンドサービス)

～そのパスワード、すでに誰かが知っているかも？～

- **2023年の事例/傾向②**
  - **国内製造業の情報がダークウェブに流出**
    - 2023年6月、アイギステックは国内の主要製造業30社について、ダークウェブへのアカウント情報漏えい状況調査結果を発表した
    - 調査対象の30社全てでダークウェブ上にアカウント情報や機密文書がアップロードされていることが判明した
    - 特に製造業は、過去調査した金融機関、行政機関の結果と比較すると情報漏えい件数やハッキング数等においてすべて上回っていた

【出典】 国内主要製造業30社、ダークウェブ への情報流出調査結果(株式会社アイギステック)
https://www.aegistech.jp/news/view/id/23#u

【10位】犯罪のビジネス化(アンダーグラウンドサービス)

～そのパスワード、すでに誰かが知っているかも？～

- **2023年の事例/傾向③**
  - **月額でウイルスを販売し、サポートも存在**
    - 2023年10月、Fortinetは情報窃取ウイルス「ExelaStealer」が登場したことを注意喚起した
    - このウイルスはWindowsプラットフォームを標的にしたもので、クレジットカード等の情報を窃取する
    - 月額や買い切りで利用する方法があり、ダークウェブ上で、月額20ドルと、安価に提供されている。また、カスタマイズサービスも提供されていた。

【出典】 月額20ドル・3カ月45ドル・無期限120ドルのお買い得マルウェア登場、警戒を(TECH+)
https://news.mynavi.jp/techplus/article/20231023-2800152/

【10位】犯罪のビジネス化(アンダーグラウンドサービス)

～そのパスワード、すでに誰かが知っているかも？～

IPA

- **対策**

攻撃に使用されるツールやサービスの目的・仕様によって対策は異なる。
より具体的な対策については本書の他の脅威を参照すること。

- **組織(経営者層)**

【組織としての体制確立】

- インシデント対応体制を整備し、対応する
  - CISOを配置する
  - CSIRTを構築する
  - 有事の際の対応フローを確立する
  - 運用手順を社員へ通知する
  - 運用の訓練をする
  - 外部の協力依頼先を用意する
  - 社内規則の整備や予算確保をする

【10位】犯罪のビジネス化(アンダーグラウンドサービス)

～そのパスワード、すでに誰かが知っているかも？～

- **対策**
  - **組織(システム管理者)**

【被害の予防】

- DDoS攻撃の影響を緩和するISP(インターネットサービスプロバイダー)やCDN(コンテンツデリバリーネットワーク)等を利用する
- システムの冗長化等の軽減策を検討する
- Torノードの検知/ブロックする
- 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

【被害の早期検知】

- ダークウェブを監視する
  - 監視サービス等を用いて、自組織に影響のある攻撃情報や流出情報の存在を確認する

【10位】犯罪のビジネス化(アンダーグラウンドサービス)

～そのパスワード、すでに誰かが知っているかも？～

- **対策**
  - **組織(システム管理者)**

【被害を受けた後の対応】

- 適切な報告／連絡／相談を行う
  - 上司、CSIRT、関係組織、公的機関等
- 通信制御(DDoS攻撃元をブロック等)
- Webサイト停止時の代替サーバーの用意と告知手段の整備をする
- 適切なバックアップ運用(復旧作業)を行う
- インシデント対応体制を整備し、対応する

【10位】犯罪のビジネス化(アンダーグラウンドサービス)

～そのパスワード、すでに誰かが知っているかも？～

- **対策**
  - **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
- 多要素認証方式などの認証方式を利用する

【10位】犯罪のビジネス化(アンダーグラウンドサービス)

～そのパスワード、すでに誰かが知っているかも？～

- **対策**
  - **組織(PC利用者)**

【被害の早期検知】

- 不審なログイン履歴を確認する

【被害を受けた後の対策】

- インシデント対応体制を整備し、対応する

まとめ

情報セキュリティ対策の基本を実践

・「10大脅威」の順位は毎回変動するが、基本的な対策の重要性は変わらない

各脅威の手口の把握および対策を実践

・脅威に備えるためには攻撃手口や動向、および自組織が抱える要因等を把握することが重要

・「10大脅威」のランキングは、各組織において実施すべき対策の優先度とは必ずしも一致はしない。そのため、組織ごとの状況を考慮して対策の優先度を決定する。

まとめ

共通対策を実践

- 対策の種類単位で見ると、複数の脅威に有効な対策がある
- 下記の「共通対策」を「情報セキュリティ対策の基本」と共に実施することでより効率的に広範囲な対策を進めることが可能

※情報セキュリティ10大脅威 2024のページで共通対策の詳細な解説資料を公開中

共通対策
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
インシデント体制の整備し、対応を行う
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

詳細な資料のダウンロード

- 情報セキュリティ10大脅威　2024

  本資料に関する詳細な内容はWebサイトをご覧ください

https://www.ipa.go.jp/security/10threats/10threats2024.html

※こちらのQRコードをスマートフォンの
QRコードリーダーアプリで読み込む
ことでもアクセスできます