IPA Better Life with IT

情報セキュリティ10大脅威　2023

～全部担当のせいとせず、組織的にセキュリティ対策の足固めを～

［組織編］

独立行政法人情報処理推進機構（IPA）
セキュリティセンター
2023年3月

「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 2023 脅威ランキング

IPA

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

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」は常に意識

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

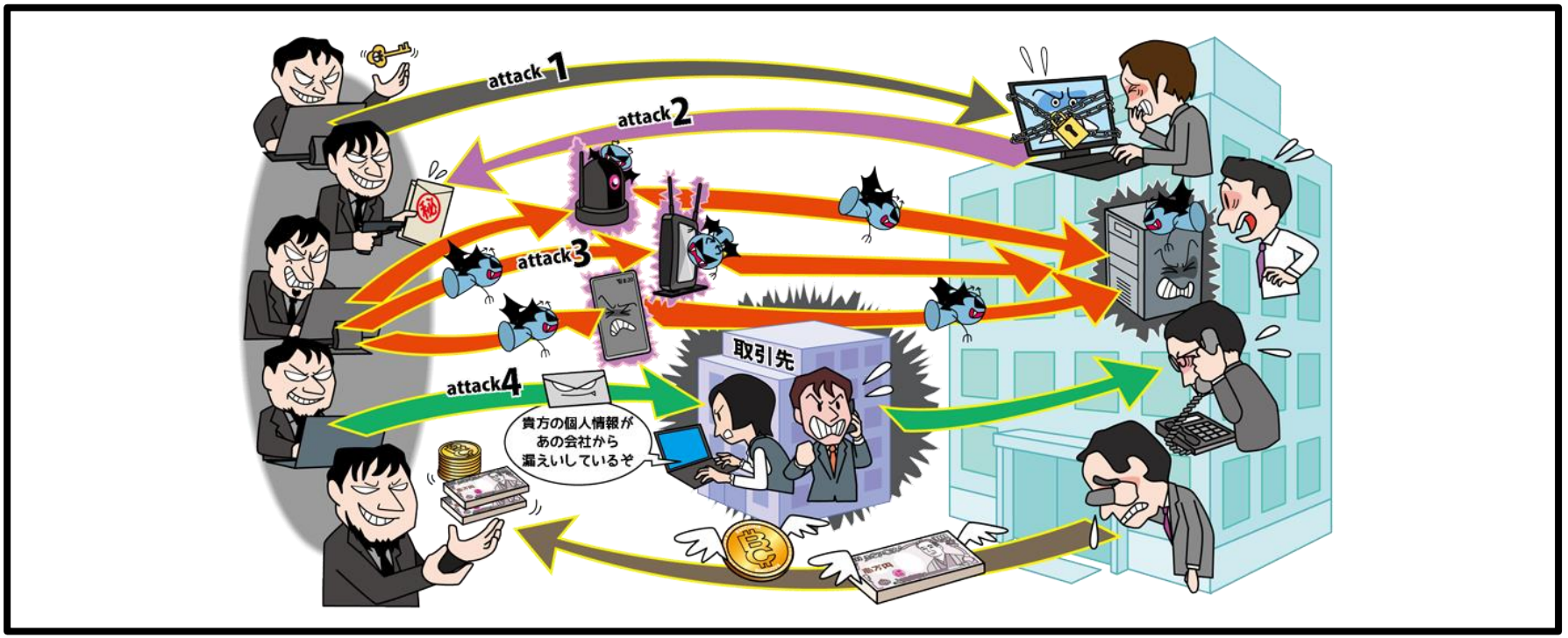
備える対象	情報セキュリティ対策の基本＋α	目的
インシデント全般	責任範囲の明確化（理解）	インシデント発生時に誰（どの組織）が対応する責任があるのかを明確化（理解）する
クラウドの停止	代替案の準備	業務が停止しないように代替策を準備する
クラウドの仕様変更	設定の見直し	仕様変更により意図せず変更された設定を適切な設定に直す（設定不備による情報漏えいや攻撃への悪用を防止する。）

情報セキュリティ10大脅威 2023
組織編　各脅威の解説

※以降の各脅威の対策では、前項の「情報セキュリティ対策の基本」は実施されている前提とし、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

～猛威を振るうランサムウェア。四重の脅迫で被害者を逃がさない～



- PC等に保存されているファイルを暗号化され**使用不可に**
- 復旧と引き換えに**金銭を要求される**
- 情報を窃取しそれを**公開する**、攻撃を受けている事を**ビジネスパートナー等に公表**すると脅迫するケースも

【1位】ランサムウェアによる被害

～猛威を振るうランサムウェア。四重の脅迫で被害者を逃がさない～

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

メールを利用した手口

- 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

ウェブサイトを利用した手口

- ランサムウェアをダウンロードさせるように**ウェブサイトを改ざん**
- 当該サイトを閲覧するように**メール等で誘導**

【1位】ランサムウェアによる被害

～猛威を振るうランサムウェア。四重の脅迫で被害者を逃がさない～

● 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

- ・管理用のRDP（リモートデスクトップ）等で**サーバーに不正アクセス**
- ・サーバー上で攻撃者がウイルスを実行（感染させる）

【1位】ランサムウェアによる被害
～猛威を振るうランサムウェア。四重の脅迫で被害者を逃がさない～

- 2022年の事例/傾向①
  - 脆弱性を悪用してランサムウェアを配置 (※1)
    - 2022年3月、東京コンピュータサービスは、同社のシステムがランサムウェアに感染し、社内管理情報や顧客の**情報等を窃取された**
    - Active Directoryを管理するためのウェブサービスにリバースプロキシサーバ経由でアクセスされ、**ウェブサービスの脆弱性を悪用されて**ADサーバに侵入された
    - ランサムウェアを自動で配布するバッチファイルを設定され、組織内の機器がランサムウェアに感染した

【出典】
※1 ランサム感染で顧客情報の流出を確認 - ソフトウェア開発会社(Security NEXT)
https://www.security-next.com/135115

【1位】ランサムウェアによる被害
～猛威を振るうランサムウェア。四重の脅迫で被害者を逃がさない～

- 2022年の事例/傾向②
  - リモートデスクトップ経由によるランサムウェア感染(※1)
    - 2022年6月、ヴィアックスは同社の勤怠管理システムのサーバーがランサムウェアに感染したことを公表
    - ランサムウェアにより従業員1,871人、退職者2,167人の情報が暗号化された
    - 勤怠管理システムのウェブサーバーはメンテナンス用に外部からリモートデスクトップ接続が可能となっていた
    - ウェブサーバーへのパスワードの総当たり攻撃により不正侵入されたものとみられる

【出典】
※1 勤怠管理システムサーバに対する攻撃について（株式会社ヴィアックス）
https://www.viax.co.jp/pdf/20220601.pdf

【1位】ランサムウェアによる被害
～猛威を振るうランサムウェア。四重の脅迫で被害者を逃がさない～

- **対策**
  - **経営者層**
    - 組織としての対応体制の確立
      - 対策の**予算の確保**と継続的な対策の実施
      - CISO/CIO など**専門知識を持つ責任者**を配置

【1位】ランサムウェアによる被害
～猛威を振るうランサムウェア。四重の脅迫で被害者を逃がさない～

- 対策
  - システム管理者、従業員
    - ・被害の予防
      - －迅速、継続的に対応できる体制（CSIRT等）の構築
      - －多要素認証の設定を有効にする
      - －添付ファイルやリンクを安易にクリックしない
      - －提供元が不明なソフトウェアを実行しない
      - －機器の脆弱性対策を迅速に行う
        - －パッチ適用を迅速に行う
        - －サポート切れのOSは利用停止
      - －セキュリティ対策ツールの利用や設定見直し
        - －アプリケーション実行制限や、メールおよびウェブのフィルタリング
        - －ポリシー設定を見直し、遮断設定を極力有効にする
      - －セキュリティ診断やペネトレーションテストを行う

【1位】ランサムウェアによる被害
～猛威を振るうランサムウェア。四重の脅迫で被害者を逃がさない～

- **対策**
  - **システム管理者、従業員**
    - ・被害の予防
      - －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**
      - －**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
        - ※バックアップから復旧できることを定期的に確認

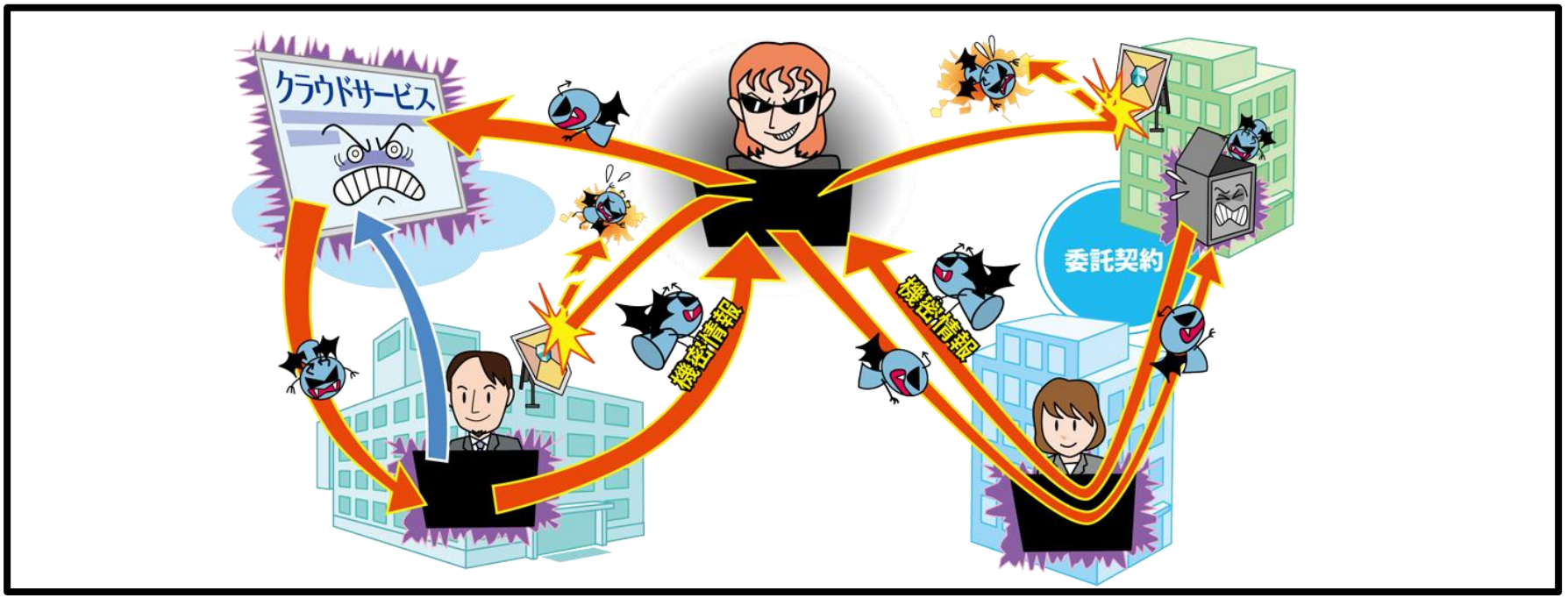
【1位】ランサムウェアによる被害
～猛威を振るうランサムウェア。四重の脅迫で被害者を逃がさない～

- **対策**
  - **システム管理者、従業員**
    - ・被害を受けた後の対応
      - －組織の方針に従い各所へ**報告、相談**する
        ※上司、CSIRT、関係組織、公的機関等
      - －バックアップからの**復旧**
      - －復号ツールの活用
      - －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**

＜身代金の支払いと復旧業者の選定について＞
－身代金を支払ってもデータ復旧や情報流出を**防げるとは限らない**

【2位】サプライチェーンの弱点を悪用した攻撃

～自組織だけでなく、委託先や利用しているサービスも適切な管理を～



- 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
- 取引先や業務を委託している**外部組織から情報漏えい**

【2位】サプライチェーンの弱点を悪用した攻撃

～自組織だけでなく、委託先や利用しているサービスも適切な管理を～

● 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

～自組織だけでなく、委託先や利用しているサービスも適切な管理を～

- 2022年の事例/傾向①

  (※1,2)

  - 協力企業の子会社へサイバー攻撃、国内全工場停止
    - 2022年3月、トヨタ自動車が小島プレス工業のシステム障害により国内全工場を停止した
    - システム障害は小島プレス工業の**子会社の社内ネットワークを介して**同社の社内ネットワークに侵入され、**ランサムウェア攻撃**を受けたことによるものであった
    - 子会社は外部企業との専用通信を行うための**リモート接続機器の脆弱性を悪用され**、不正アクセスが行われていた

【出典】

※1 システム停止事案調査報告書(第 1 報)(小島プレス工業株式会社)
https://www.kojima-tns.co.jp/wp-content/uploads/2022/03/20220331_システム障害調査報告書(第1報).pdf

※2 トヨタ、国内全工場を停止へ 部品会社にサイバー攻撃(日本経済新聞)
https://www.nikkei.com/article/DGXZQOFD289MK0Y2A220C2000000/?unlock=1

【2位】サプライチェーンの弱点を悪用した攻撃

～自組織だけでなく、委託先や利用しているサービスも適切な管理を～

- 2022年の事例/傾向②
  - 利用しているサービスの改ざんにより情報漏えい（※1,2,3）
    - 2022年10月、ショーケースは同社が提供する複数の**サービスが改ざんされた**ことを公表した
    - 改ざんの原因は同社システムの**脆弱性を悪用した不正アクセス**により、プログラムを書き換えられたことであった
    - 改ざんされたサービスを利用していた**取引先の複数のサービスから**顧客の個人情報が漏洩した

【出典】

※1　不正アクセスに関するお知らせとお詫び（株式会社ショーケース）
https://www.showcase-tv.com/pressrelease/202210-fa-info/

※2　弊社が運営する「生涯学習のユーキャン」サイトにおける個人情報漏洩に関するお詫びとお知らせ（株式会社ユーキャン）
https://www.u-can.co.jp/info/release.html

※3　弊社が運営する「ABC-MART公式オンラインストア」における個人情報漏えいの可能性に関するお詫びとお知らせ（株式会社エービーシーマート）
https://www.abc-mart.net/shop/pages/info-2022.aspx

【2位】サプライチェーンの弱点を悪用した攻撃

～自組織だけでなく、委託先や利用しているサービスも適切な管理を～

- **対策**
  - **組織（自組織）**
    - ・被害の予防
      - －業務委託や情報管理における規則の徹底
      - －報告体制等の問題発生時の運用規則整備
      - －納品物の検証
        組み込まれているソフトウェアも把握し、脆弱性対策を実施
      - －情報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（※1,2,3）

【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
※2　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
※3　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

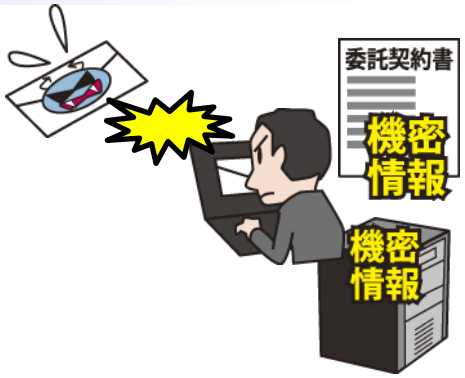
【2位】サプライチェーンの弱点を悪用した攻撃

～自組織だけでなく、委託先や利用しているサービスも適切な管理を～

- **対策**
  - **組織（自組織）**
    - ・被害を受けた後の対応
      - –組織の方針に従い**各所へ報告、相談**する
        ※上司、CSIRT、関係組織、公的機関等
      - –**影響**調査および**原因**の追究、**対策**の強化
      - –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

～自組織だけでなく、委託先や利用しているサービスも適切な管理を～



● 対策

■ 組織（自組織の商流に関わる組織）

・被害の予防

－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

契約時に取引先における情報管理等の規則を確認

－取引先や委託先組織の管理

情報セキュリティ対応の**定期的な確認、監査**

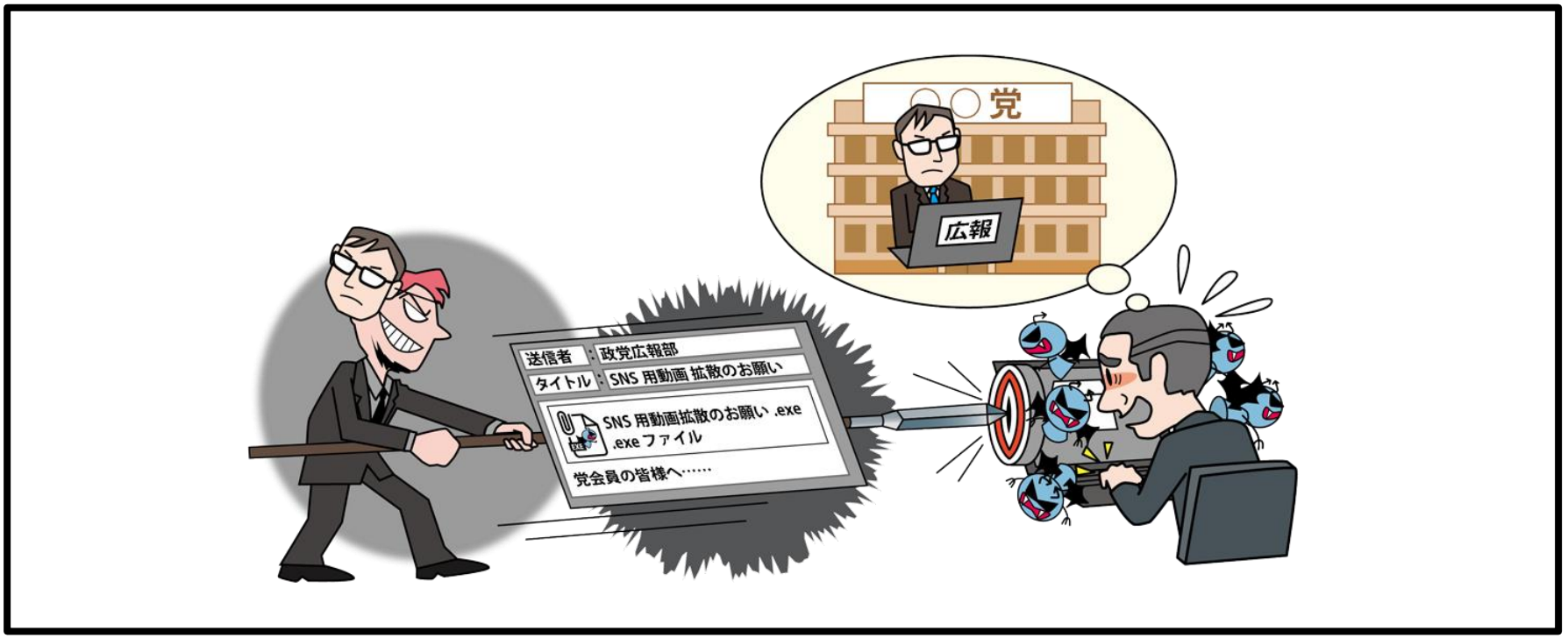
・被害を受けた後の対応

－組織の方針に従い**各所へ報告、相談**する

※上司、CSIRT、関係組織、公的機関等

【3位】標的型攻撃による機密情報の窃取

～メールが来たらまずは疑え！？意識は常に高く～



- 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の破壊**を行う

【3位】標的型攻撃による機密情報の窃取

～メールが来たらまずは疑え！？意識は常に高く～

● 攻撃手口

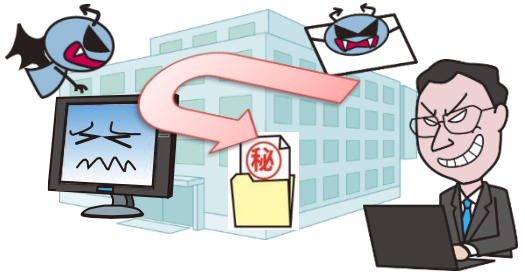
・メールやウェブサイトからウイルスに感染させる

■ メールを利用した手口（標的型攻撃メール）

- 不正な添付ファイルを**開かせる**
- 不正なウェブサイトへのリンクを**クリックさせる**

■ ウェブサイトを利用した手口

- 標的組織が頻繁に利用するウェブサイトを調査し、
  当該サイトを**閲覧する**とウイルスに感染するように改ざん
  （水飲み場型攻撃）



【3位】標的型攻撃による機密情報の窃取

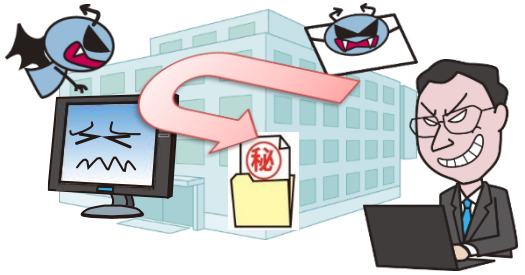
～メールが来たらまずは疑え！？意識は常に高く～

● 攻撃手口

・不正アクセスして認証情報を窃取
・社内システムへ侵入しウイルスを感染させる

■ 不正アクセスによる手口

- 組織が利用するクラウドサービスやウェブサーバー、VPNの**脆弱性を悪用**して不正アクセスし、**認証情報等を窃取**
- 窃取した認証情報等を悪用して正規の経路で社内システムへ侵入し、PCやサーバーを**ウイルスに感染させる**



【3位】標的型攻撃による機密情報の窃取

～メールが来たらまずは疑え！？意識は常に高く～

● 2022年の事例/傾向①

■ シンクタンクへの標的型メール攻撃 (※1,2,3)

・2022年6月に**シンクタンクへの標的型メール攻撃**があったことを警察庁が公開

・メールには個人情報の圧縮ファイルが添付されており、データの代行登録を依頼するという、**業務に関連した内容**であった

・シンクタンクを狙った攻撃は**NISCが注意喚起**しており、IPAも**政府関係機関とよく連携して対応**するよう求めている

【出典】

※1 令和4年上半期におけるサイバー空間をめぐる脅威の情勢等について(警察庁)
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_kami_cyber_jousei.pdf

※2 学術関係者・シンクタンク研究員等を標的としたサイバー攻撃について(注意喚起)(内閣サイバーセキュリティセンター)
https://www.nisc.go.jp/pdf/press/20221130NISC_press.pdf

※3 サイバーレスキュー隊(J-CRAT)活動状況[2022年度上半期](IPA)
https://www.ipa.go.jp/security/j-crat/ug65p9000000nks8-att/000106897.pdf

【3位】標的型攻撃による機密情報の窃取

～メールが来たらまずは疑え！？意識は常に高く～

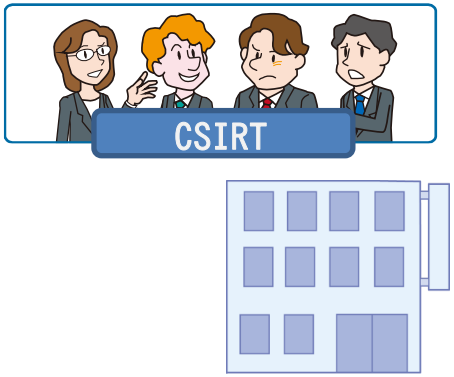
- 2022年の事例/傾向②
  - 日本の政治団体を狙ったスピアフィッシング（※1）
    - 2022年、**参議院選挙の直前期間**にスピアフィッシングキャンペーンが行われていたことをESET Researchが公開
    - **政党の広報を装って**選挙に関する依頼をしたり、**著名な政治家を装ったり**するメールが送られていた
    - メールには**悪意のあるファイルが添付**されており、実行すると「LODEINFO」と呼ばれる**ウイルスに感染する**
    - 感染すると不正にコマンドを実行され、情報窃取等の被害にあう

【出典】
※1 APTグループ「MirrorFace」が日本の政治団体を標的に実行したLiberalFace作戦の詳細（ESETセキュリティニュース）
https://www.eset.com/jp/blog/welivesecurity/unmasking-mirrorface/

【3位】標的型攻撃による機密情報の窃取

～メールが来たらまずは疑え！？意識は常に高く～

- 対策
  - 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



【3位】標的型攻撃による機密情報の窃取

～メールが来たらまずは疑え！？意識は常に高く～

● 対策

■ セキュリティ担当者、システム担当者

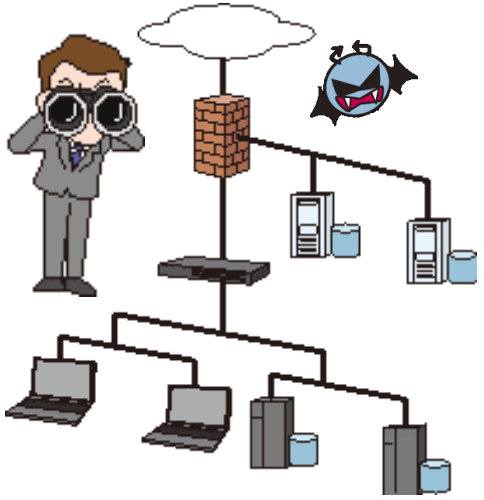
・被害の予防/対応力の向上

- 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
- 従業員に対するセキュリティ教育の実施
- インシデント対応の**定期的**な訓練を実施

※関係者やセキュリティ業者、専門家と迅速に連携できる対応方法や連絡方法を整備する

- 管理端末への**継続的**セキュリティパッチ適用
- 総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**

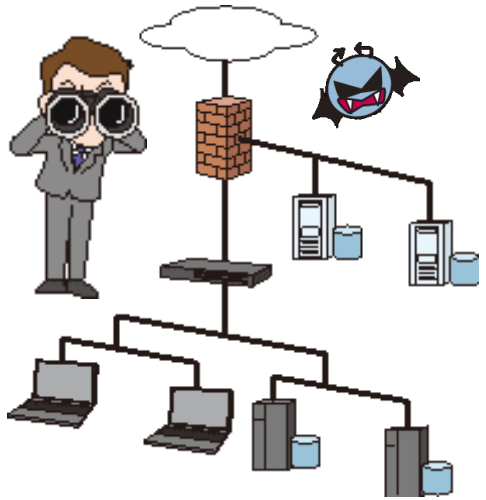
※従業員や職員が利用するPCのソフトウェア更新状況を管理し、リスクの可視化を行う



【3位】標的型攻撃による機密情報の窃取

～メールが来たらまずは疑え！？意識は常に高く～

- 対策
  - セキュリティ担当者、システム担当者
    - ・被害の予防/対応力の向上
      - –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）
      - –**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
      - –**セキュリティ診断**を行う
      - –**ペネトレーションテスト**を行う

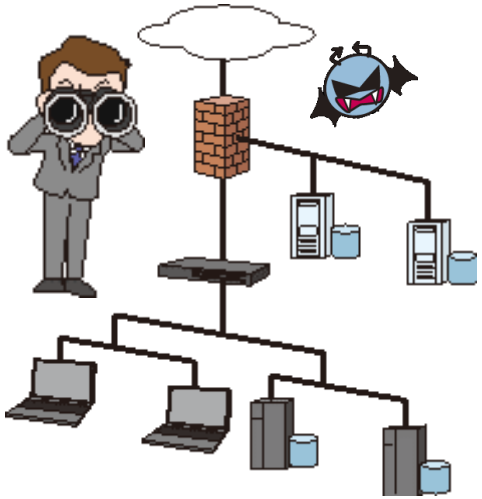


【3位】標的型攻撃による機密情報の窃取

～メールが来たらまずは疑え！？意識は常に高く～

- 対策
  - セキュリティ担当者、システム担当者
    - ・被害の早期検知
      - –UTM、IDS/IPS、WAF、仮想パッチ等の導入
      - –EDR,NDR等を用いたエンドポイントやネットワークの**監視、防御**
      - –ログを取得し**監視や解析**する

        システムログ、アプリケーションログ、サーバーへのアクセスログ、認証ログ、データベース操作ログ、通信ログ等
    - ・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



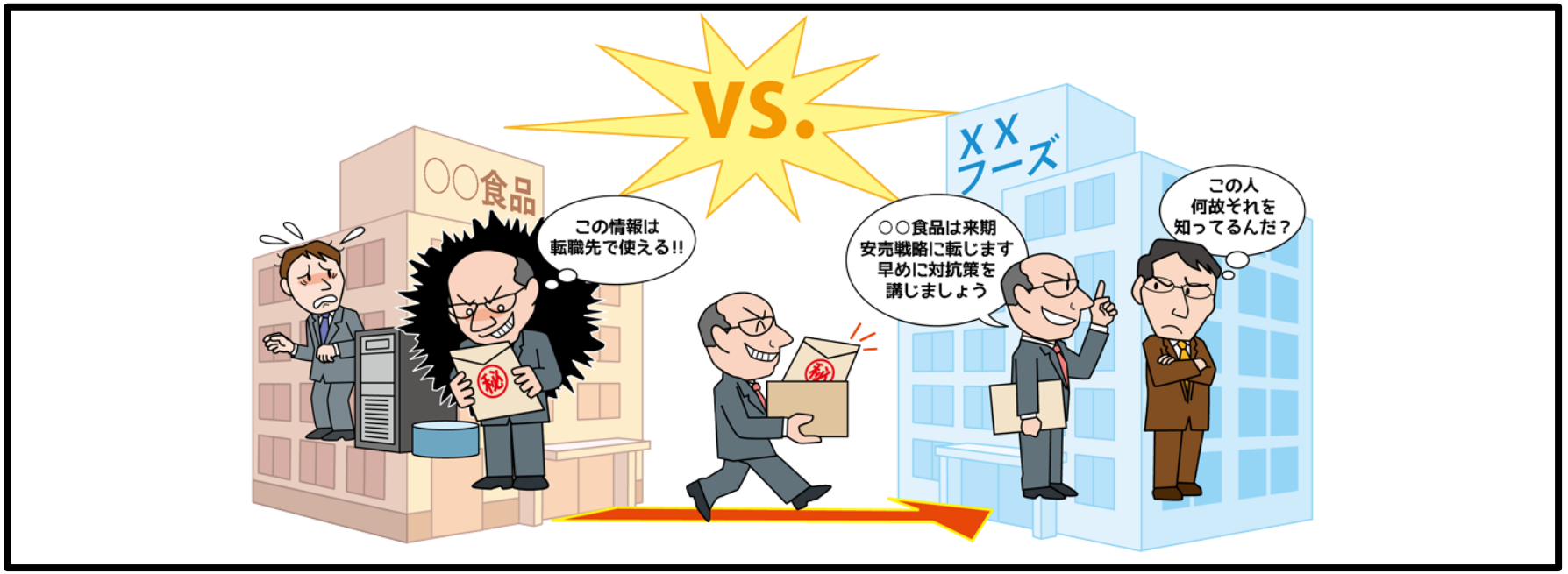
【3位】標的型攻撃による機密情報の窃取

～メールが来たらまずは疑え！？意識は常に高く～

- **対策**
  - **従業員、職員**
    - ・被害の予防（通常、組織全体で実施）
      - －添付ファイルやリンクを**安易にクリックしない**
    - ・被害を受けた後の対応
      - －組織の方針に従い**各所へ報告、相談**する
        - ※上司、CSIRT、関係組織、公的機関等

【4位】内部不正による情報漏えい

～不正に情報を取得しない、取得させない、使用しない！～



- 組織の**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

【4位】内部不正による情報漏えい

～不正に情報を取得しない、取得させない、使用しない！～

● 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
・**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

■ 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**

【4位】内部不正による情報漏えい

～不正に情報を取得しない、取得させない、使用しない！～

- 2022年の事例/傾向①
  - 市立高校で成績流出、内部犯行の可能性(※1)
    - 2022年7月、市立高校に通う生徒3人の成績等の**個人情報がInstagramに投稿**され、約90人に閲覧されていた
    - 何者かが**教員のIDとパスワードを用いて**生徒の成績等を管理している学習支援ソフトにアクセスし、情報を入手したとみられている
    - 生徒用のタブレット端末で学習支援ソフトにアクセスしていたケースがあり、**その端末では誰でも個人情報を閲覧できる状態**になっていた

【出典】
※1 市立函館高校で模試成績など流出・ＳＮＳ掲載 部内者の仕業か（NHK NEWS WEB）
https://www3.nhk.or.jp/sapporo-news/20220722/7000048853.html

【4位】内部不正による情報漏えい

～不正に情報を取得しない、取得させない、使用しない！～

- 2022年の事例/傾向②
  - 寿司チェーン社長、転職先に営業秘密持出し(※1)
    - 2022年9月、カッパ・クリエイトの社長が**不正競争防止法違反**の疑いで警視庁に**逮捕**された
    - 同社長は2020年11月に**ライバル企業から転職**しており、元部下を利用して商品原価等の**営業秘密を持ち出し**ていた
    - 転職先の商品企画部長は**データを不正利用した**として、転職元の元部下はデータの**パスワードを漏えいした**として**共に逮捕**された

【出典】

※1 かっぱ寿司運営会社社長ら逮捕 不正競争防止法違反容疑 警視庁（NHK NEWS WEB）
https://www3.nhk.or.jp/news/html/20220930/k10013843141000.html

【4位】内部不正による情報漏えい

～不正に情報を取得しない、取得させない、使用しない！～

● 対策

■ 経営者、管理者

・被害の予防①

－基本方針の策定

情報取扱**ポリシーの作成**、内部不正者に対する**懲戒処分等**を規定した**就業規則等**を整備する

－資産の把握、対応体制の整備

重要資産を**把握**し、その**重要度をランク付け**した上で重要情報の**管理者を定める**

－重要情報の管理、保護

－重要情報の利用者IDおよびアクセス権の**登録・変更・削除に関する手順**を定めて運用する

－従業員の異動や離職に伴い不要となった利用者ID等は**直ちに削除**する

－それらの適切な管理、**定期的な監査**を実施する

－利用者IDの共用禁止等の処置、DLP等のツールの導入を検討する

【4位】内部不正による情報漏えい

～不正に情報を取得しない、取得させない、使用しない！～

● 対策

■ 経営者、管理者

・被害の予防②

－物理的管理の実施

－重要情報の**格納場所**や執務室への**入退室管理**

－記録媒体の**利用制限、持ち出し/持ち込みの管理**

－記録媒体の廃棄時には適切な**データ消去の運用**を実施

－消去できない場合は媒体の物理的な破壊も検討

－リース品は**初期化**してから返却 等

【4位】内部不正による情報漏えい

～不正に情報を取得しない、取得させない、使用しない！～

● 対策

■ 経営者、管理者

・情報リテラシーや情報モラルの向上

－人的管理およびコンプライアンス教育の徹底

・攻撃の予兆／被害の早期検知

－システム操作履歴の監視

重要情報へのアクセス履歴や利用者の操作履歴等の**ログ、証跡を記録し、監視**する

さらに、監視していることを**従業員に周知**する

・被害を受けた後の対応

－組織の方針に従い各所へ**報告、相談**する

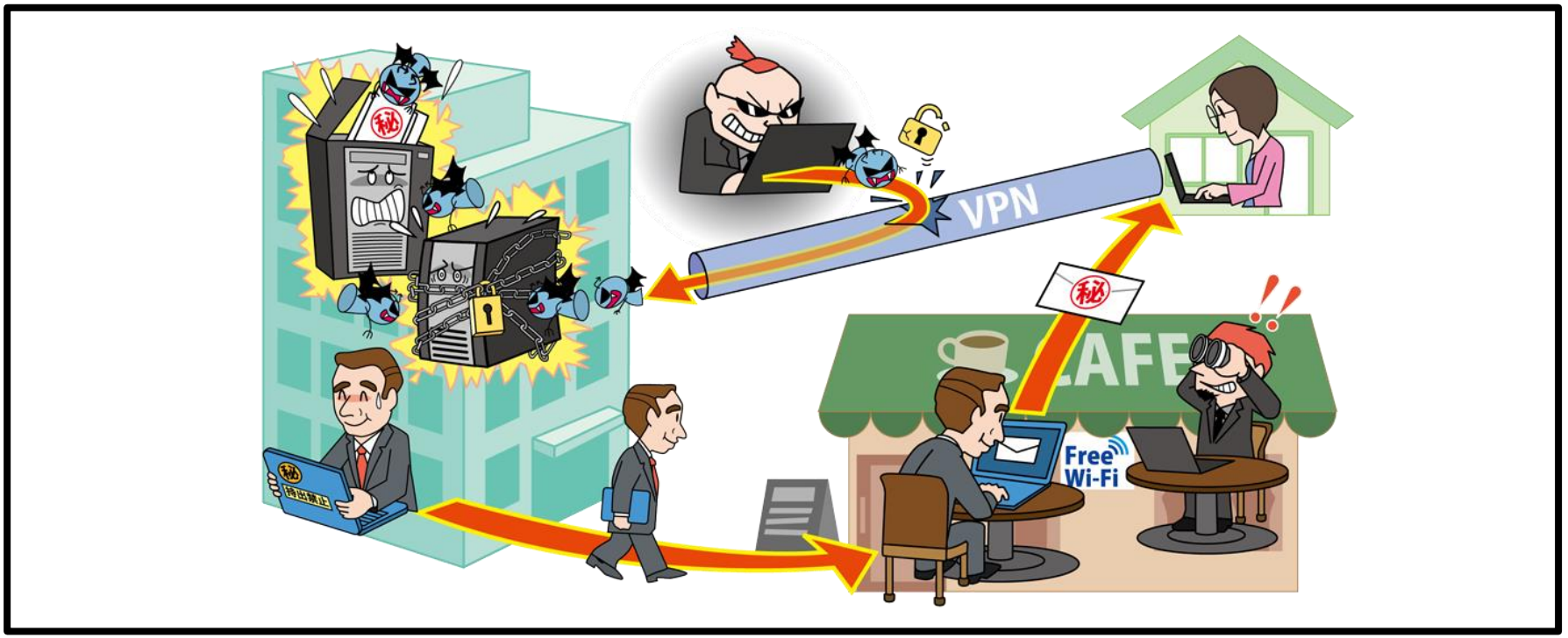
※上司、CSIRT、関係組織、公的機関等

－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**

【5位】テレワーク等のニューノーマルな働き方を狙った攻撃

～未だ脆弱なテレワーク環境が狙われる～



- 新型コロナウイルス対策の1つとして、テレワークが急速に普及
- ウェブ会議サービスやVPNの本格的な活用がされる中、それらを狙った攻撃が発生
- ウェブ会議の**のぞき見**やテレワーク用PCの**ウイルス感染**のおそれ

【5位】テレワーク等のニューノーマルな働き方を狙った攻撃

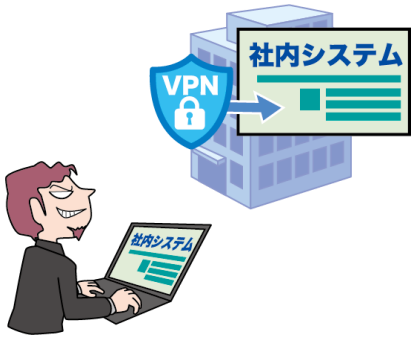
～未だ脆弱なテレワーク環境が狙われる～

● 攻撃手口/発生要因

・テレワーク環境や管理体制の不備

- テレワーク用ソフトの**脆弱性を悪用**した不正アクセス
- テレワーク移行時の、**セキュリティ対策が不十分な暫定状態のまま運用**、**管理体制の不備**
- 私物PCや自宅ネットワークの利用

※組織の**セキュリティ対策が適用されないところ**からの情報漏えいのおそれ



【5位】テレワーク等のニューノーマルな働き方を狙った攻撃

～未だ脆弱なテレワーク環境が狙われる～

- 2022年の事例/傾向①
  - リモート接続を狙ったランサムウェア攻撃 （※1）
    - 2022年6月、ニチリンの米国子会社がランサムウェア「mlock」に感染していたことを公表
    - 攻撃者は外部とのリモート接続における設定の脆弱性を悪用し、サーバーに侵入
    - 攻撃者は侵入後、別のサーバーにリモートアクセスツールなどをインストールし、ネットワークを偵察。その後ネットワーク全体にランサムウェアを配布していた。

【出典】
※1 ランサム被害、リモート接続の脆弱性が侵入口に - ニチリン（Security NEXT）
https://www.security-next.com/139557

【5位】テレワーク等のニューノーマルな働き方を狙った攻撃

～未だ脆弱なテレワーク環境が狙われる～

● 2022年の事例/傾向②

(※1,2)

■ リモート接続の脆弱性やテレワークのセキュリティの実態

- 警察庁によると、2022年上半期の国内におけるランサムウェア感染経路はVPN機器からの侵入が68％、リモートデスクトップからの侵入が15％と、**8割以上がリモート接続の脆弱性に起因**
- IPAの調査結果では、テレワークのルール順守状況の確認については**改善傾向が見られる**ものの、ITユーザの35.5％、ITベンダの10.7％では**いまだに未確認**
- 確認方法については、ITユーザは49.5％、ITベンダは40.8％の組織が**セルフチェックのみ**

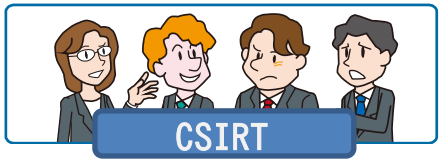
【出典】
※1 令和4年上半期におけるサイバー空間をめぐる脅威の情勢等について（警察庁）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_kami_cyber_jousei.pdf
※2 2021年度 企業・組織におけるテレワークのセキュリティ実態調査（IPA）
https://www.ipa.go.jp/security/reports/economics/scrm/ug65p90000019dg8-att/000099573.pdf

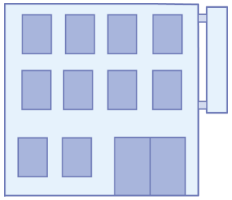
【5位】テレワーク等のニューノーマルな働き方を狙った攻撃

～未だ脆弱なテレワーク環境が狙われる～

- **対策**
  - **組織（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
        （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
      - －組織の方針に従い**各所へ報告、相談**する
        ※上司、CSIRT、関係組織、公的機関等

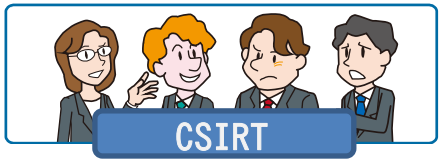


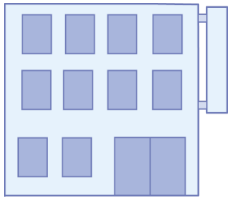


【5位】テレワーク等のニューノーマルな働き方を狙った攻撃

～未だ脆弱なテレワーク環境が狙われる～

- **対策**
  - **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
      - –有事の際の連絡窓口やフローの確立

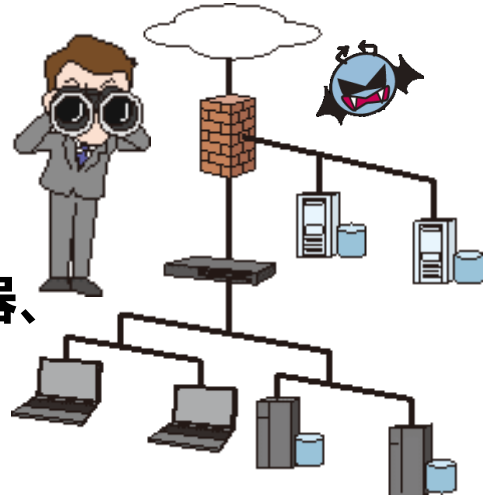




【5位】テレワーク等のニューノーマルな働き方を狙った攻撃

～未だ脆弱なテレワーク環境が狙われる～

- **対策**
  - **組織（セキュリティ担当者、システム担当者）**
    - ・被害の予防（被害に備えた対策含む）
      - －シンクライアント、VDI、VPN、ZTNA/SDP等の**セキュリティに強いテレワーク環境**の採用
      - －テレワークの**規程や運用ルール**の整備
        ※組織支給PCと私物PCの違いも考慮
      - －従業員に対する**セキュリティ教育**の実施
      - －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、スマートフォン等）
      - －ネットワークレベル認証（NLA）の実施
      - －多要素認証の設定を有効にする



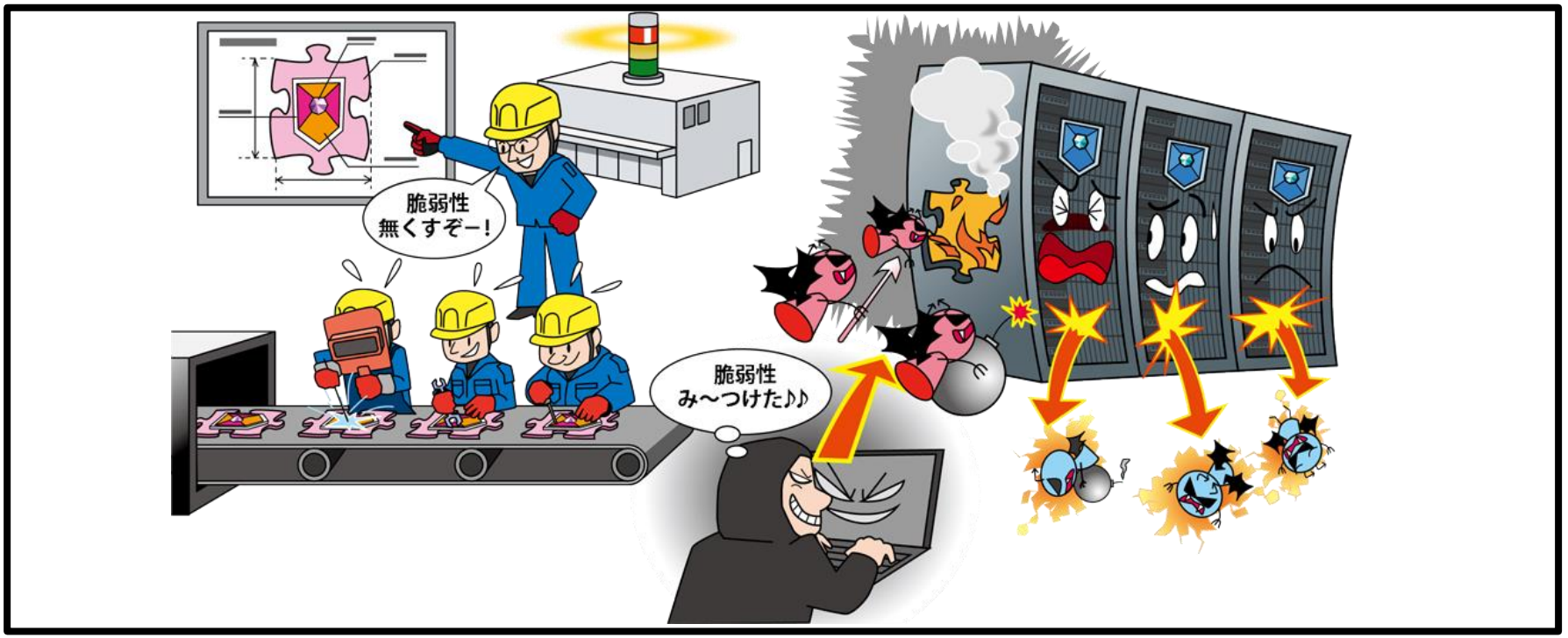
【5位】テレワーク等のニューノーマルな働き方を狙った攻撃

～未だ脆弱なテレワーク環境が狙われる～

- **対策**
  - **組織（セキュリティ担当者、システム担当者）**
    - ・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、WAF、仮想パッチ等の**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
        ※テレワーク環境をリモートから調査する
      - －影響調査および原因の追究、対策の強化

【6位】修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）

～事前に防ぐことは困難。悪用の情報が公表されたら即時対応を～



- 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
- 攻撃を確実に防ぐ事前の対策は難しく、**いつのまにか被害に遭うおそれ**がある

【6位】修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）

～事前に防ぐことは困難。悪用の情報が公表されたら即時対応を～

● 攻撃手口

・開発ベンダー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

・確実な事前の対策は難しく、無防備な状態の組織を狙う

【6位】修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）

～事前に防ぐことは困難。悪用の情報が公表されたら即時対応を～

- 2022年の事例/傾向①
  - Fortinet製品 へのゼロデイ攻撃（※3,4,5）
    - 2022年12月、FortiGate等のセキュリティアプライアンス製品にOSとして搭載されている**FortiOSの脆弱性を公表**
    - 遠隔の第三者に認証を回避され、任意のコードやコマンドを実行されるおそれ
    - 影響する製品には**サポート終了バージョンも含まれていた**
    - 対策や緩和策だけでなく、脆弱性を悪用した**攻撃のログや痕跡等の調査も推奨**された

【出典】
※1 FortiOS - heap-based buffer overflow in sslvpnd（Fortinet, Inc.）
https://www.fortiguard.com/psirt/FG-IR-22-398
※2 Fortinet製品のSSL VPN機能に脆弱性 - すでに悪用、侵害調査を（Security NEXT）
https://www.security-next.com/142121
※3 FortiOSのヒープベースのバッファーオーバーフローの脆弱性（CVE-2022-42475）に関する注意喚起（一般社団法人JPCERTコーディネーションセンター）
https://www.jpcert.or.jp/at/2022/at220032.html

【6位】修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）

～事前に防ぐことは困難。悪用の情報が公表されたら即時対応を～

- 2022年の事例/傾向②

(※1,※2)

  - Microsoft Exchange Serverでゼロデイ攻撃が発生
    - ベトナムのセキュリティ企業が、Microsoft Exchange Serverの**未修正の脆弱性を悪用する攻撃発生**を2022年9月に公表
    - マイクロソフトは**脆弱性に関する情報と緩和策**を同月に公開
    - マイクロソフトは、脆弱性を悪用してユーザーのシステムに侵入する限定的な標的型攻撃を確認しているとし、11月に**修正プログラムをリリースするまで、暫定的な緩和策を案内**

【出典】

※1　Microsoft Exchange Serverでゼロデイ攻撃が発生（トレンドマイクロ株式会社）
https://www.trendmicro.com/ja_jp/research/22/i/ms-exchange-zero-day.html

※2　Microsoft Exchange サーバーのゼロデイ脆弱性報告に関するお客様向けガイダンス（Microsoft Security Response Center）
https://msrc-blog.microsoft.com/2022/09/30/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server-ja/

【6位】修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）

～事前に防ぐことは困難。悪用の情報が公表されたら即時対応を～

- **対策**
  - **組織（システム管理者）**
    - ・被害の予防
      - –資産の把握、対応体制の整備
      - –NDR等を用いたネットワークの監視および攻撃通信の遮断
      - –EDR等を用いたエンドポイントの監視、防御
      - –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
      - –セキュリティ診断やペネトレーションテストを行う
    - ・攻撃の予兆／被害の早期検知
      - –UTM、IDS/IPS、WAF、仮想パッチ等の導入

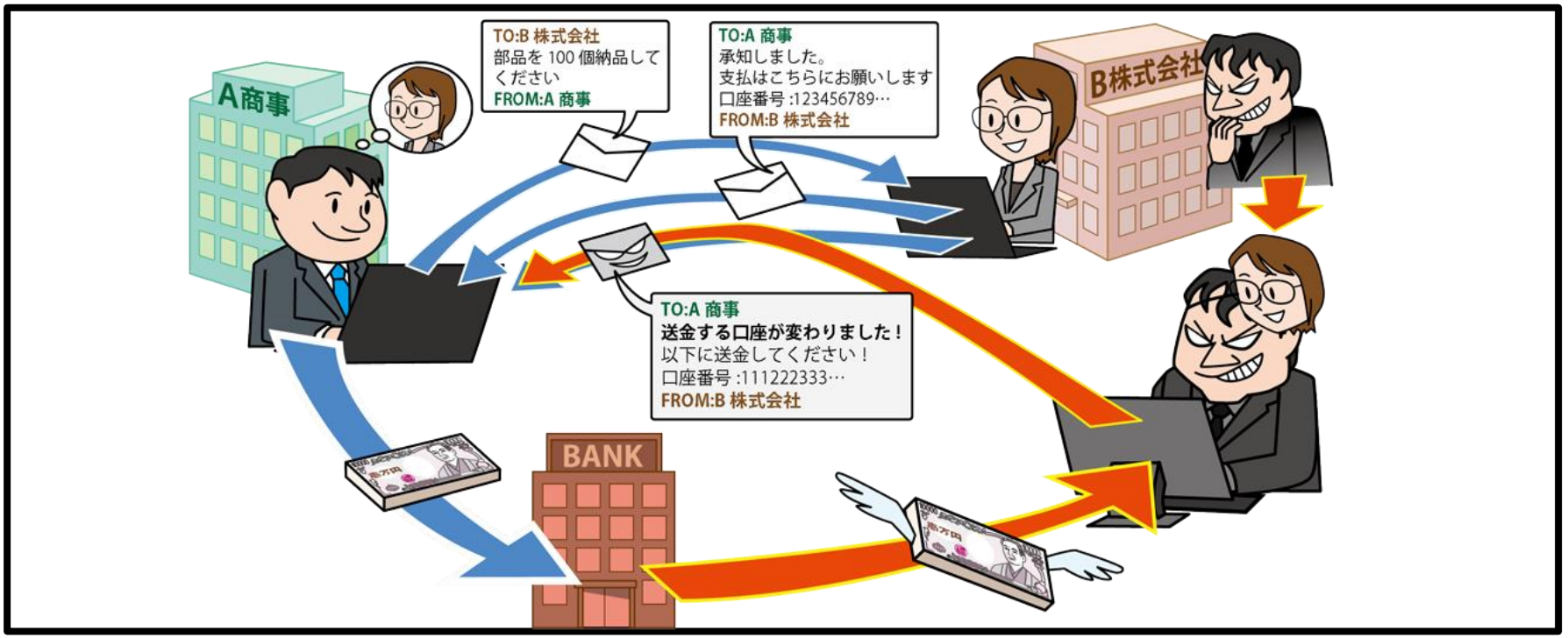
【6位】修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）

～事前に防ぐことは困難。悪用の情報が公表されたら即時対応を～

- 対策
  - 組織（システム管理者）
    - ・修正プログラムリリース前の対応
      - －回避策や緩和策の適用
      - －当該ソフトウェアの一時的な使用停止
    - ・修正プログラムリリース後の対応
      - －修正プログラムの適用
        - 必要に応じて回避策、緩和策を無効化する。
    - ・被害を受けた後の対応
      - －組織の方針に従い各所へ報告、相談する
        - 上司、CSIRT、関係組織、公的機関等
      - －影響調査および原因の追究、対策の強化

【7位】ビジネスメール詐欺による金銭被害

～そのメール、相手が誰か分かりますか？～



- 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

【7位】ビジネスメール詐欺による金銭被害

～そのメール、相手が誰か分かりますか？～

● 攻撃手口

・何らかの手段を用いて標的組織の業務情報等を窃取
・窃取した情報を悪用したメールで送金依頼（金銭詐取）

- 取引先との**請求書を偽装**
- 経営者等への**なりすまし**
- 窃取した**標的組織のメールアカウント**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

【7位】ビジネスメール詐欺による金銭被害

～そのメール、相手が誰か分かりますか？～

- 2022年の事例/傾向①
  - 正規のメールアドレスを乗っ取ったBEC(※1)
    - 2022年7月、サイバー情報共有イニシアティブ(J-CSIP)参加組織が**請求側企業の担当者になりすました**詐欺のメールを受信
    - 攻撃者は請求側担当者の**メールアドレスを乗っ取り**、支払側企業に**入金先の口座を変更**するように指示
    - メールのやり取りの際、Ccに請求側企業の関係者のメールアドレスに似せた偽のメールアドレスが指定されており、**詐欺の発覚を避ける巧妙な手口**

【出典】
※1 サイバー情報共有イニシアティブ(J-CSIP)運用状況[2022年4月～6月](IPA)
https://www.ipa.go.jp/security/j-csip/ug65p9000000nkvm-att/000100056.pdf

【7位】ビジネスメール詐欺による金銭被害

～そのメール、相手が誰か分かりますか？～

- 2022年の事例/傾向②
  - 偽メールに従い送金し…後日、詐欺発覚 (※1)
    - 2022年11月、人材育成を行うウィルソン・ラーニングワールドワイドは**子会社2社**における同年9月の**ビジネスメール詐欺被害**を公表
    - 子会社は**悪意ある第三者より支払代金の送金を指示するメール**を受け取り、2社合わせて約530万円を送金
    - 送金後に詐欺の可能性に気付き、デジタルフォレンジック等による**事実関係確認、保険会社、捜査機関に対し相談等**を実施

【出典】
※1 当社子会社における資金流出事案の発生 並びに特別損失の計上に関するお知らせ(ウィルソン・ラーニング ワールドワイド株式会社)
https://ssl4.eir-parts.net/doc/9610/tdnet/2203725/00.pdf

【7位】ビジネスメール詐欺による金銭被害

～そのメール、相手が誰か分かりますか？～

● 対策

・被害の予防

－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

　　個人の判断や命令で取引が行わ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

－メールに電子証明を付与（S/MIMEやPGP） **※なりすまし防止**

－DMARCを導入する　**※ドメイン認証失敗時のメール処理を判断する**

<メールの真正性の確認>

－メールだけでなく複数の手段で事実確認

－以下のようなメールに注意する

　普段とは異なる表現／**送信元のメールドメイン**／**判断を急がせる**

<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、**多要素認証**等の利用

【7位】ビジネスメール詐欺による金銭被害

～そのメール、相手が誰か分かりますか？～

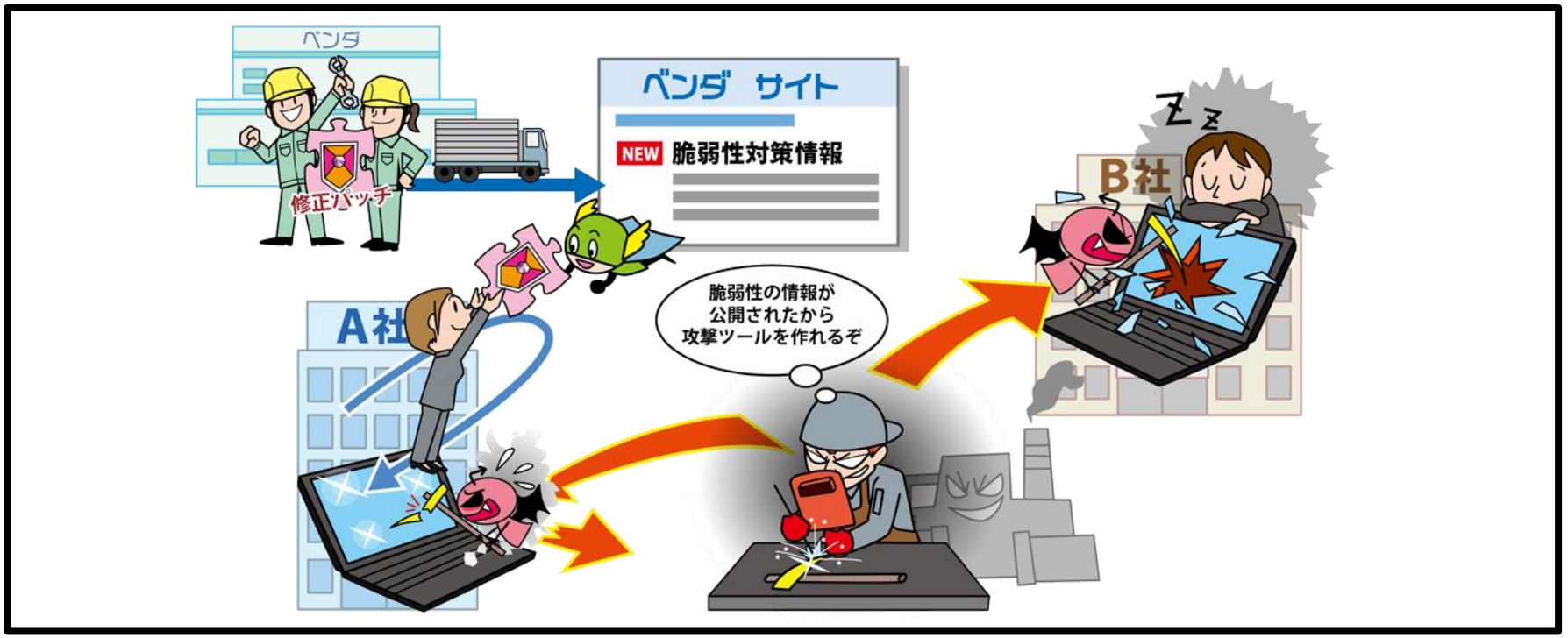
● 対策

・被害を受けた後の対応

- 組織の方針に従い各所へ**報告、相談**する
  上司、CSIRT、関係組織、公的機関等
- メールアカウントの設定を確認する
  攻撃者による**不正な転送設定**や**フォルダー振り分け設定等**を
  されていないか確認
- 被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**

【8位】脆弱性対策情報の公開に伴う悪用増加

～「後で対応しよう」、その数日が命取り～



- 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**
- 脆弱性情報の公開後、攻撃コードが流通して**攻撃が本格するまでの時間が近年は短くなっている**傾向
- 広く利用されている製品の脆弱性の場合は被害が大きくなる

【8位】脆弱性対策情報の公開に伴う悪用増加

～「後で対応しよう」、その数日が命取り～

● 攻撃手口

・公開された脆弱性情報を悪用して攻撃する
・対策が未実施もしくは時間を要している相手を狙う

■ 対策前の脆弱性を悪用

・対策情報が公開されてから**利用者が対策を完了するまでの時間**に存在する脆弱性（Nデイ脆弱性）を悪用

■ 公開されている攻撃ツールを使用

・公開された脆弱性を悪用する攻撃ツールは**短期間で作成されインターネット上（ダークウェブ等）に出回る**

・オープンソースのツールに**脆弱性を利用する機能**が実装される場合があり、それを悪用されることも

【8位】脆弱性対策情報の公開に伴う悪用増加

～「後で対応しよう」、その数日が命取り～

- 2022年の事例/傾向①
  - 修正未実施の機器を狙った攻撃 (※1,2)
    - 2022年5月4日(米国時間)、F5 Networksが同社のネットワーク製品BIG-IPの**脆弱性を公表**
    - 脆弱性を悪用されると、遠隔の第三者に認証を回避され、任意のコードの実行や不正な操作をされるおそれ
    - 5月9日にセキュリティベンダーからPOC(実証コード)が公開され、その前後から**修正パッチが適用されていない機器を探索する通信や脆弱性を悪用する試みが観測**された

【出典】
※1 K23605346: BIG-IP iControl REST vulnerability CVE-2022-1388(F5, Inc.)
https://support.f5.com/csp/article/K23605346
※2 「BIG-IP」脆弱性に注意 - 実証コード公開済み、探索や悪用も(Security NEXT)
https://www.security-next.com/136392

【8位】脆弱性対策情報の公開に伴う悪用増加

～「後で対応しよう」、その数日が命取り～

- 2022年の事例/傾向②
  - 「Spring4Shell」を狙った攻撃(※1,2)
    - 2022年3月31日（米国時間）、Vmwareが、JavaのWebアプリ開発を行うためのフレームワークであるSpring Framework における**脆弱性を公表**
    - 脆弱性**公表時点で既にPOC（実証コード）が公開**されていた
    - **公表当日から悪用を試行する通信が観測**され、4日間で最大37,000件にも上り全世界の約16％の組織が影響を受けた

【出典】
※1　深刻な脆弱性「Spring4Shell」（NTT DATA）
https://www.nttdata.com/jp/ja/data-insight/2022/1012/
※2　Spring4Shell（CVE-2022-22965）を悪用したボットネット「Mirai」の攻撃を観測（トレンドマイクロ株式会社）
https://www.trendmicro.com/ja_jp/research/22/d/Mirai-exploits-Spring4Shell.html

【8位】脆弱性対策情報の公開に伴う悪用増加

～「後で対応しよう」、その数日が命取り～

● 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

- 資産の**把握**、体制の**整備**
- 脆弱性関連**情報の収集と対応**
- ネットワークの**監視**および攻撃通信の**遮断**
- 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
- **一時的なサーバー停止**等

・攻撃の予兆／被害の早期検知

- UTM・IDS/IPS・WAF等の**導入**

・被害を受けた後の対応

- 組織の方針に従い各所へ**報告、相談**する
  上司、CSIRT、関係組織、公的機関等
- 影響調査および原因の追究、対策の強化

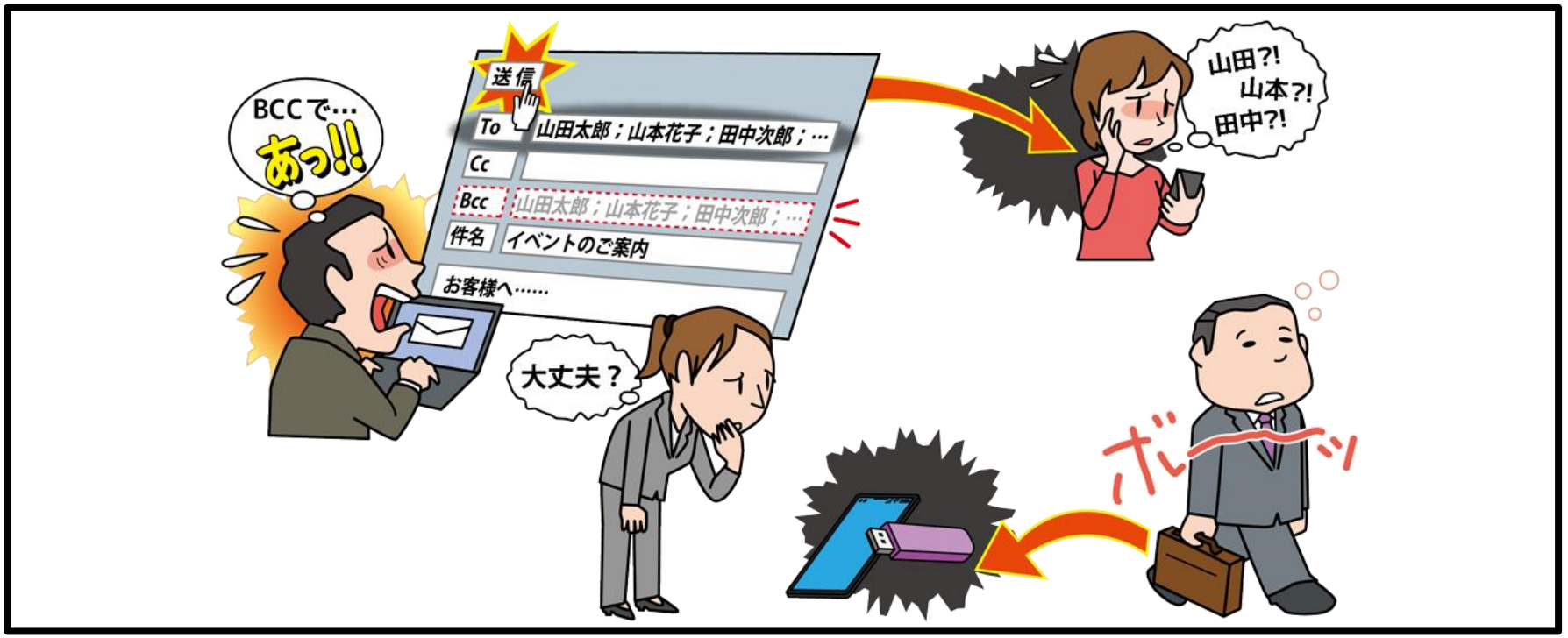
【8位】脆弱性対策情報の公開に伴う悪用増加

～「後で対応しよう」、その数日が命取り～

- **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
      - －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

【9位】不注意による情報漏えい等の被害

～1つのうっかりが大事件につながることも…～



- 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**、漏えいした情報の悪用による**二次被害**

【9位】不注意による情報漏えい等の被害

～1つのうっかりが大事件につながることも…～

● 要因

・個人の情報リテラシーやモラル不足からの不注意

- **従業員の情報リテラシーの低さ**
  - ・重要情報をカバンで持ち出し、カバンを**紛失して漏えい**
  - ・宛先等の**確認不十分**なままメールを送信し誤送信
- **誤送信を想定した偽メールアドレスの存在**
  - ・第三者により組織が利用しているドメインと似たようなドメインのメールアドレスを準備される
  - ・従業員が誤送信したタイミングで情報が漏えい

【9位】不注意による情報漏えい等の被害

～1つのうっかりが大事件につながることも…～

● 要因

・組織の管理体制の不備

- **情報を取り扱う際の本人の状況**
  - ・体調不良や急ぎの用件があることによる**注意力散漫**
- **組織規程および確認プロセスの不備**
  - ・**重要情報の定義**、**取扱規程**、持ち出し許可**手順**等の不備

【9位】不注意による情報漏えい等の被害

～1つのうっかりが大事件につながることも…～

2022年の事例/傾向①

個人情報の入ったUSBメモリーを紛失（※1）

・2022年6月、兵庫県尼崎市は全市民の住民基本台帳や住民税に係る情報等が記録されたUSBメモリーの紛失を公表

・業務を受託した企業の再々委託先の社員が、作業のためUSBメモリーに記録して持ち出し

・作業完了後に飲食店で飲酒、帰宅時にUSBメモリーを入れていた鞄が無くなっていることに気がついて紛失が発覚

・当該USBメモリーは、パスワードが設定や、暗号化処理を施しており、個人情報の漏えいは無かったと公表

【出典】

※1 個人情報を含むUSBメモリーの紛失事案について（尼崎市）

https://www.city.amagasaki.hyogo.jp/kurashi/seikatusien/1027475/1030947.html

【9位】不注意による情報漏えい等の被害

～1つのうっかりが大事件につながることも…～

- 2022年の事例/傾向②
  - クラウドのアクセス権限誤設定、個人情報漏えい（※1）
    - 2022年10月、JTBが、地域振興事業の補助金を申請した事業者等1万1,483人の**個人情報を漏えい**したことを公表
    - クラウドにログイン権限を持つ事業者の**データが相互に閲覧可能**になっており、**他の事業者の申請書をダウンロードできる**状態になっていた
    - 原因は情報共有に利用していた**クラウドのアクセス権限を誤設定**したことによるものであった

【出典】
※1　JTB、クラウドサービスの設定ミスで1万人超の個人情報漏洩（日経XTECH）
https://xtech.nikkei.com/atcl/nxt/news/18/14005/

【9位】不注意による情報漏えい等の被害

～1つのうっかりが大事件につながることも…～

● 対策

■ 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**と**定期的な見直し**

・被害の予防（被害に備えた対策含む）

- 確認プロセスに基づく運用
- 取り扱う情報の**重要度を規定**し、それに合わせた運用を行う
- 情報の**保護（暗号化、認証）**、機密情報の**格納場所の把握、可視化**
- DLP（情報漏えい対策）製品の**導入**
- 外部に持ち出す情報や端末の**制限**
- メール**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

【9位】不注意による情報漏えい等の被害

～1つのうっかりが大事件につながることも…～

- **対策**
  - ・攻撃の予兆／被害の早期検知
    - －問題発生時の**内部報告体制の整備**
    - －外部からの**連絡窓口の設置**
  - ・被害を受けた後の対応
    - －組織の方針に従い各所へ**報告、相談**する
      上司、CSIRT、関係組織、公的機関等
    - －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の**要因の削除**
    - －漏えいした内容や発生原因の**公表**

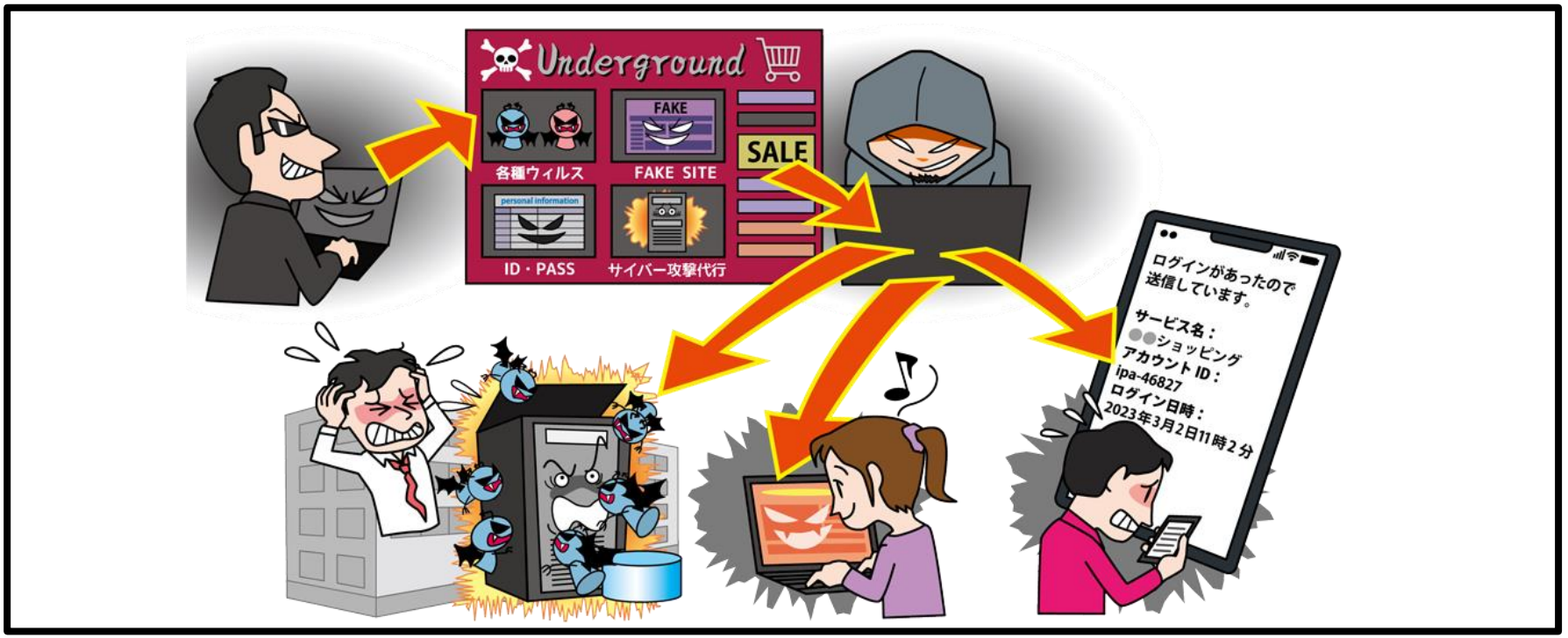
【9位】不注意による情報漏えい等の被害

～1つのうっかりが大事件につながることも…～

- **対策**
  - **個人/組織（被害者）**
    - ・被害を受けた後の対応
      - –クレジットカードの停止
      - –被害を警察や公的機関へ**相談**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）

～攻撃者もショッピング。商品はあなたの情報～



- 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
- 通常のブラウザでは検索できないウェブサイト上に存在
- 専門知識は不要で容易にサイバー攻撃が可能

【10位】犯罪のビジネス化（アンダーグラウンドサービス）

～攻撃者もショッピング。商品はあなたの情報～

- 攻撃手口
  - 購入したサービスやツールを利用して攻撃
    - ・攻撃の**代行サービス**や攻撃に利用できる**ツール**の取引
  - 購入した認証情報を利用してウェブへ不正ログイン
    - ・窃取した**個人情報や認証情報**を販売・購入
  - サイバー犯罪に加担する人材のリクルート
    - ・組織的に行われる**サイバー犯罪の人材確保**

【10位】犯罪のビジネス化（アンダーグラウンドサービス）

～攻撃者もショッピング。商品はあなたの情報～

- 2022年の事例/傾向①
  - 窃取した個人情報をダークウェブで売買（※1）
    - 2022年1月、クローズアップ現代によると、フィッシング等で窃取された個人情報がブラックマーケットで売買されていた
    - 大手ショッピングサイトのアカウント情報や個人情報も売買
    - 売買されている個人情報にはセキュリティコードもセットとなったクレジットカード情報、免許証や保険証の情報、パスポートの画像等が存在
    - 販売されている情報はフィッシングだけでなく企業から不正に窃取したとみられる

【出典】

※1 追跡！サイバー犯罪組織 コロナ禍の日本を狙う闇（NHK）

https://www.nhk.or.jp/gendai/articles/4631/

【10位】犯罪のビジネス化（アンダーグラウンドサービス）

～攻撃者もショッピング。商品はあなたの情報～

- 2022年の事例/傾向②
  - 窃取された個人情報がダークウェブに流出（※1）
    - 2022年9月、ダイナムジャパンホールディングスは**個人情報の流出**を確認したことを公表
    - 同社のサーバーが**ランサムウェアによる攻撃**を受け、データを暗号化され、この際のアラートで被害が発覚
    - グループ会社が運営する店舗の地権者の氏名や口座情報等2,042件や、入金情報172件、取引先に関する名刺情報や証券口座情報1,218件等が**流出**
    - 流出した情報はいずれも**ダークウェブ上で公開**されていた

【出典】

※1 ダークウェブで個人情報流出を確認 - ダイナムJHD（Security NEXT）
https://www.security-next.com/140249

【10位】犯罪のビジネス化（アンダーグラウンドサービス）

～攻撃者もショッピング。商品はあなたの情報～

対策一覧（一例）

経営者

- 組織としての対応体制の確立
  - 問題に対応できる**体制（CSIRT等）構築**
  - **予算の確保と**継続的な対策の実施

【10位】犯罪のビジネス化（アンダーグラウンドサービス）

～攻撃者もショッピング。商品はあなたの情報～

対策一覧（一例）

システム管理者

・被害の予防

- DDoSの攻撃の影響を緩和するISPやCDN等のサービス利用
- システムの冗長化など軽減策

・被害を受けた時の対応

- 組織の方針に従い各所へ報告、相談する
  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）
- ウェブサイト停止時の代替サーバの用意と告知手段の整備
- 影響調査および原因の追究

【10位】犯罪のビジネス化（アンダーグラウンドサービス）

～攻撃者もショッピング。商品はあなたの情報～

対策一覧（一例）

PC利用者

- 被害の予防
  - セキュリティ**教育**
  - 受信メール、ウェブサイトの**十分な確認**
    不信なメールのリンクをクリックしたり、添付ファイルを開かない
  - 迅速に**更新プログラムを適用**する
  - セキュリティソフトの導入
  - 多要素認証方式などの認証方式の利用

【10位】犯罪のビジネス化（アンダーグラウンドサービス）

～攻撃者もショッピング。商品はあなたの情報～

対策一覧（一例）

PC利用者

・被害の早期検知

－不審なログイン履歴の確認

・被害を受けた後の対策

－組織の方針に従い各所へ**報告、相談**する

上司、CSIRT、関係組織、公的機関等

－バックアップからの普及

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長年変わらない**

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。**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可能

※情報セキュリティ10大脅威 2023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　2023

本資料に関する詳細な内容は以下のウェブサイトをご覧ください

※以下のURLへアクセス、または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み、ウェブサイトをご覧ください

https://www.ipa.go.jp/security/10threats/10threats2023.html