IPA Better Life with IT

情報セキュリティ10大脅威　2022

～誰かが対策をしてくれている。そんなウマい話は、ありません！！～

［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
2022年5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 2022 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	標的型攻撃による機密情報の窃取
メールやSMS等を使った 脅迫・詐欺の手口による金銭要求	3	サプライチェーンの弱点を悪用した攻撃
クレジットカード情報の不正利用	4	テレワーク等の ニューノーマルな働き方を狙った攻撃
スマホ決済の不正利用	5	内部不正による情報漏えい
偽警告によるインターネット詐欺	6	脆弱性対策情報の公開に伴う悪用増加
不正アプリによる スマートフォン利用者への被害	7	修正プログラムの公開前を狙う攻撃 （ゼロデイ攻撃）
インターネット上のサービスからの 個人情報の窃取	8	ビジネスメール詐欺による金銭被害
インターネットバンキングの不正利用	9	予期せぬIT基盤の障害に伴う業務停止
インターネット上のサービスへの 不正ログイン	10	不注意による情報漏えい等の被害

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

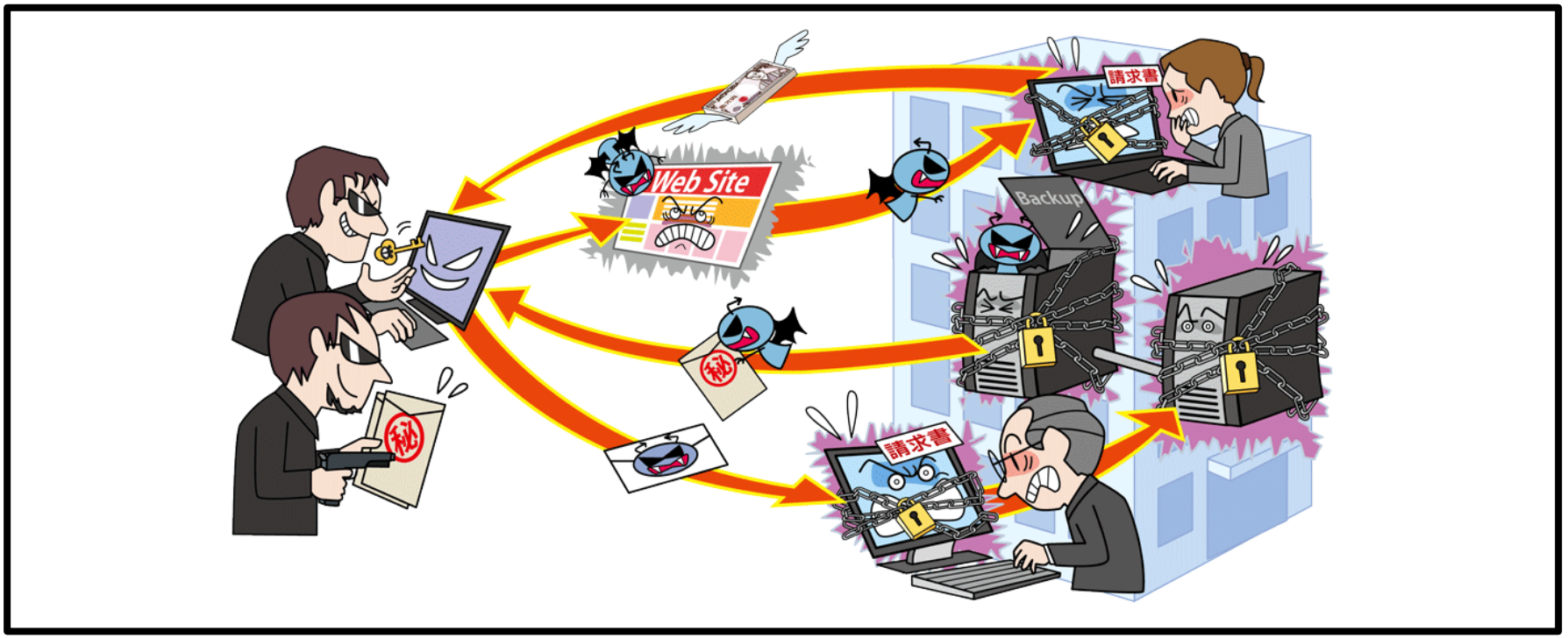
- 昨今はクラウドサービスの利用も一般的になってきている
- クラウドサービスを利用を想定した＋αの対策を行い備える必要がある

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 2022
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
～社会インフラに大きな影響が出る場合も～



- 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と脅迫するケースも

【1位】ランサムウェアによる被害
～社会インフラに大きな影響が出る場合も～

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
～社会インフラに大きな影響が出る場合も～

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**
  - ・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
～社会インフラに大きな影響が出る場合も～

- 2021年の事例/傾向①
  - 病院へのランサムウェア攻撃 (※1)
    - 2021年10月、病院のシステムがランサムウェアに感染し電子カルテや会計システムにアクセスできなくなる等の被害
    - 暗号化解除と引き換えに身代金を要求されたが応じず
    - システム復旧まで新規患者の受け入れを中止する等の影響
    - 2022年1月、通常診療を再開

【出典】
※1 サイバー攻撃受けた徳島・半田病院 約2カ月ぶりに通常診療全面再開（朝日新聞DIGITAL）
https://www.asahi.com/articles/ASQ145J9MQ13PTLCOOP.html

【1位】ランサムウェアによる被害
～社会インフラに大きな影響が出る場合も～

- 2021年の事例/傾向②
  - バックアップの暗号化による被害の長期化(※1)
    - ・製粉会社にサイバー攻撃により、ランサムウェアに感染
    - ・システムのオンラインバックアップを管理していたサーバーも暗号化
    - ・早期復旧が困難となり四半期決算報告書の提出にも影響

【出典】
※1 2022 年 3 月期第 1 四半期報告書の提出期限延長に関する承認申請書提出のお知らせ（株式会社ニップン）
https://www.nippn.co.jp/topics/detail/_icsFiles/afieldfile/2021/08/16/20210816-1.pdf

【1位】ランサムウェアによる被害
～社会インフラに大きな影響が出る場合も～

- 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
      - 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
～社会インフラに大きな影響が出る場合も～

- 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

【1位】ランサムウェアによる被害
～社会インフラに大きな影響が出る場合も～

- 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
～社会インフラに大きな影響が出る場合も～

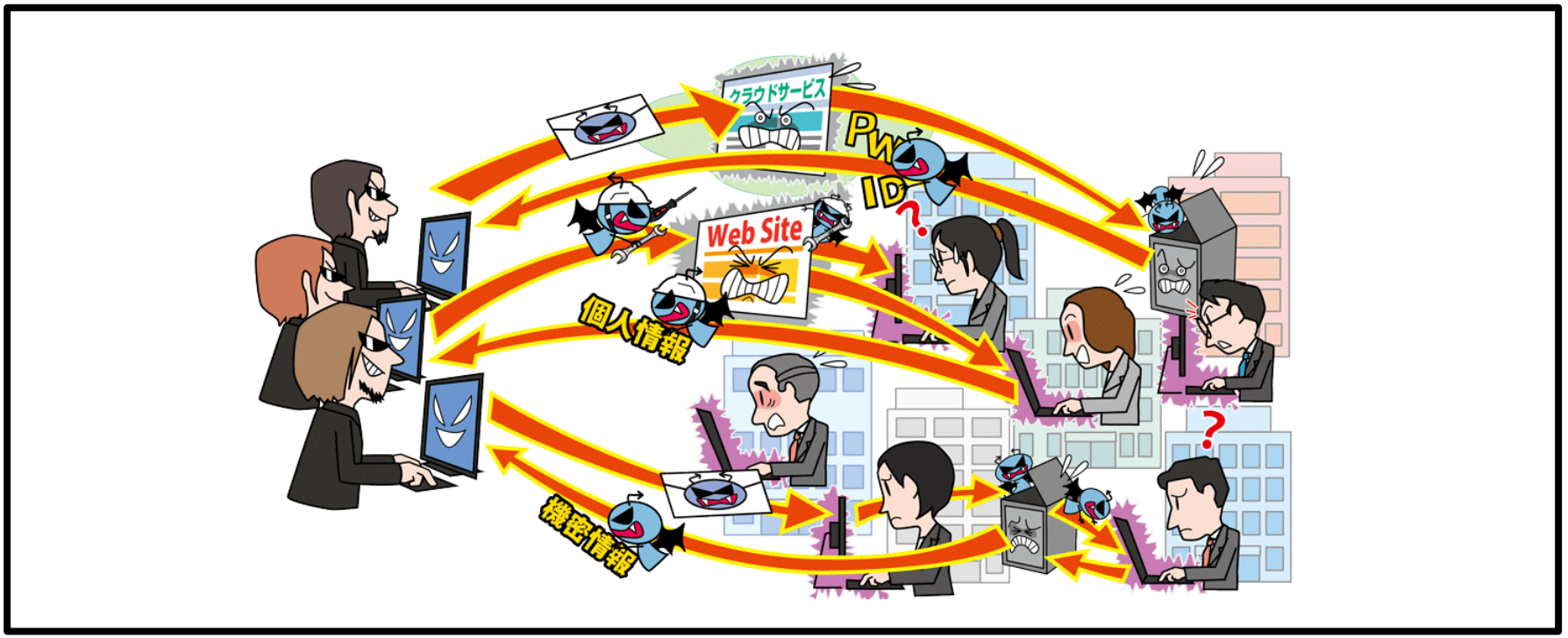
- 対策
  - システム管理者、従業員
    - ・被害を受けた後の対応
      - －組織の方針に従い各所へ報告、相談する
        ※上司、CSIRT、関係組織、公的機関等
      - －バックアップからの復旧
      - －復号ツールの活用
      - －影響調査および原因の追究、対策の強化
      - －迅速な隔離を行い、関連組織、取引先への被害拡大の防止

＜例外ケース＞

推奨はされないが、過去には、組織の事情（暗号化されたファイルが人命に関わる場合等）により、金銭を支払ったケースもあった

【2位】標的型攻撃による機密情報の窃取

～組織化しているサイバー攻撃～



- 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

【2位】標的型攻撃による機密情報の窃取

～組織化しているサイバー攻撃～

● 攻撃手口

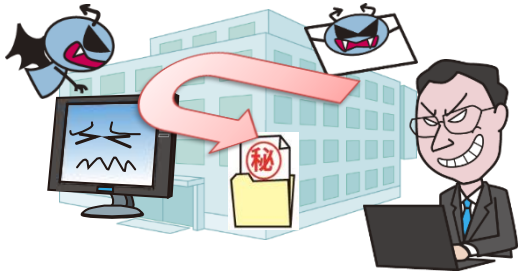
・メールやウェブサイトからウイルスに感染させる

■ 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）



【2位】標的型攻撃による機密情報の窃取

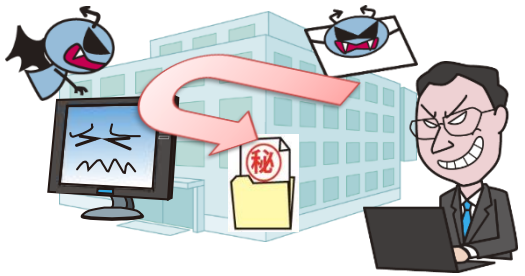
～組織化しているサイバー攻撃～

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



【2位】標的型攻撃による機密情報の窃取

～組織化しているサイバー攻撃～

- 2021年の事例/傾向①
  - 情報共有ツールから受託情報が外部に流出（※1）
    - 2021年5月、大手Sierが、自社が提供するプロジェクト情報共有ツールが不正アクセスされたことを公表
    - 顧客から預かっていた情報の一部が外部に流出
    - 本ツールは、同社やグループ会社、外部の協力企業、顧客間のシステム開発等のプロジェクト管理（開発工程やソース、タスクの管理等）に利用

【出典】
※1 社内外で利用する「プロジェクト情報共有ツール」に不正アクセス - 富士通（Security NEXT）
https://www.security-next.com/126507

【2位】標的型攻撃による機密情報の窃取

～組織化しているサイバー攻撃～

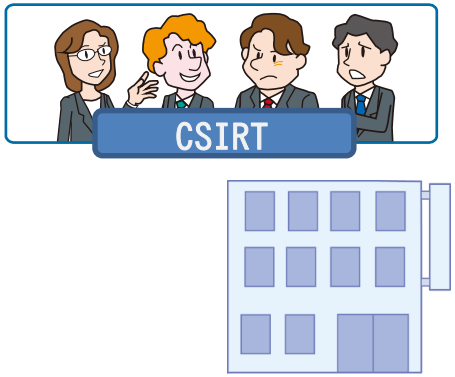
- 2021年の事例/傾向②
  - サイバー攻撃に関する情報共有 (※1)
    - ・サイバー情報共有イニシアティブ(J-CSIP)からの報告
    - ・J-CSIP参加組織からIPAへのサイバー攻撃に関する情報提供
    - ・2021年の標的型攻撃メールとみなした情報提供は36件
    - ・2021年7月～9月の情報提供では、標的型攻撃かは判断できないが、頻繁に利用している無償イラスト素材提供サイトからダウンロードした画像ファイルにURLがリンク
    - ・不正ファイルとしてセキュリティソフトに検知

【出典】
※1 サイバー情報共有イニシアティブ(J-CSIP)運用状況 [2021年1月～3月,2021年4月～6月,2021年7月～9月,2021年10月～12月](IPA)
https://www.ipa.go.jp/security/J-CSIP/index.html

【2位】標的型攻撃による機密情報の窃取

～組織化しているサイバー攻撃～

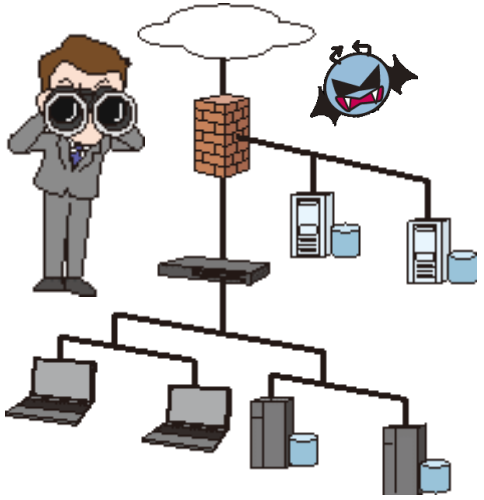
- 対策
  - 経営者層
    - ・組織としての体制の確立
      - -CSIRTの構築
      - -対策予算の確保と継続的な対策の実施
      - -セキュリティポリシーの策定



【2位】標的型攻撃による機密情報の窃取

～組織化しているサイバー攻撃～

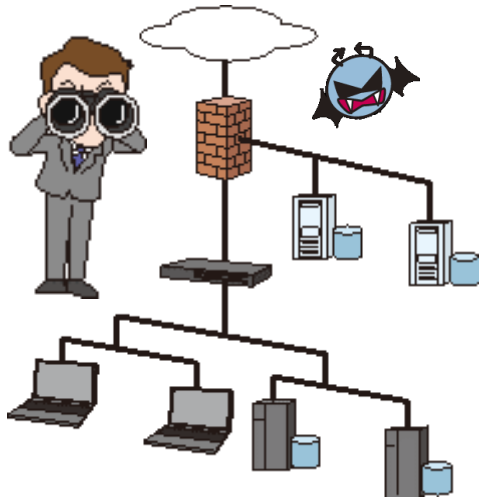
- 対策
  - セキュリティ担当者、システム担当者
    - ・被害の予防/対応力の向上
      - –情報の管理とルール策定
      - –サイバー攻撃に関する継続的な情報収集
      - –従業員に対するセキュリティ教育の実施
      - –インシデント対応の定期的な訓練を実施
        - ※関係者やセキュリティ業者、専門家と迅速に連携できる対応方法や連絡方法を整備する
      - –管理端末への継続的セキュリティパッチ適用
      - –総合運用管理ツール等によるセキュリティ対策状況の把握
        - ※従業員や職員が利用するPCのソフトウェア更新状況を管理し、リスクの可視化を行う



【2位】標的型攻撃による機密情報の窃取

～組織化しているサイバー攻撃～

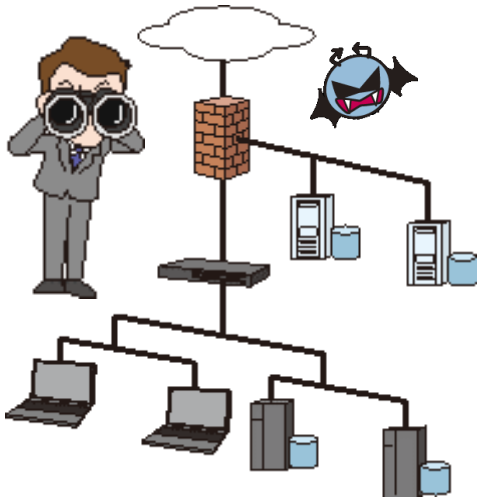
- **対策**
  - **セキュリティ担当者、システム担当者**
    - ・被害の予防/対応力の向上
      - –アプリケーション許可リストの整備
      - –アクセス権の最小化と管理の強化
      - –ネットワーク分離
      - –重要サーバーの要塞化(アクセス制御、暗号化等)
      - –取引先のセキュリティ対策実施状況の確認
      - –海外拠点等も含めたセキュリティ対策の向上



【2位】標的型攻撃による機密情報の窃取

～組織化しているサイバー攻撃～

- 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等を用いた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



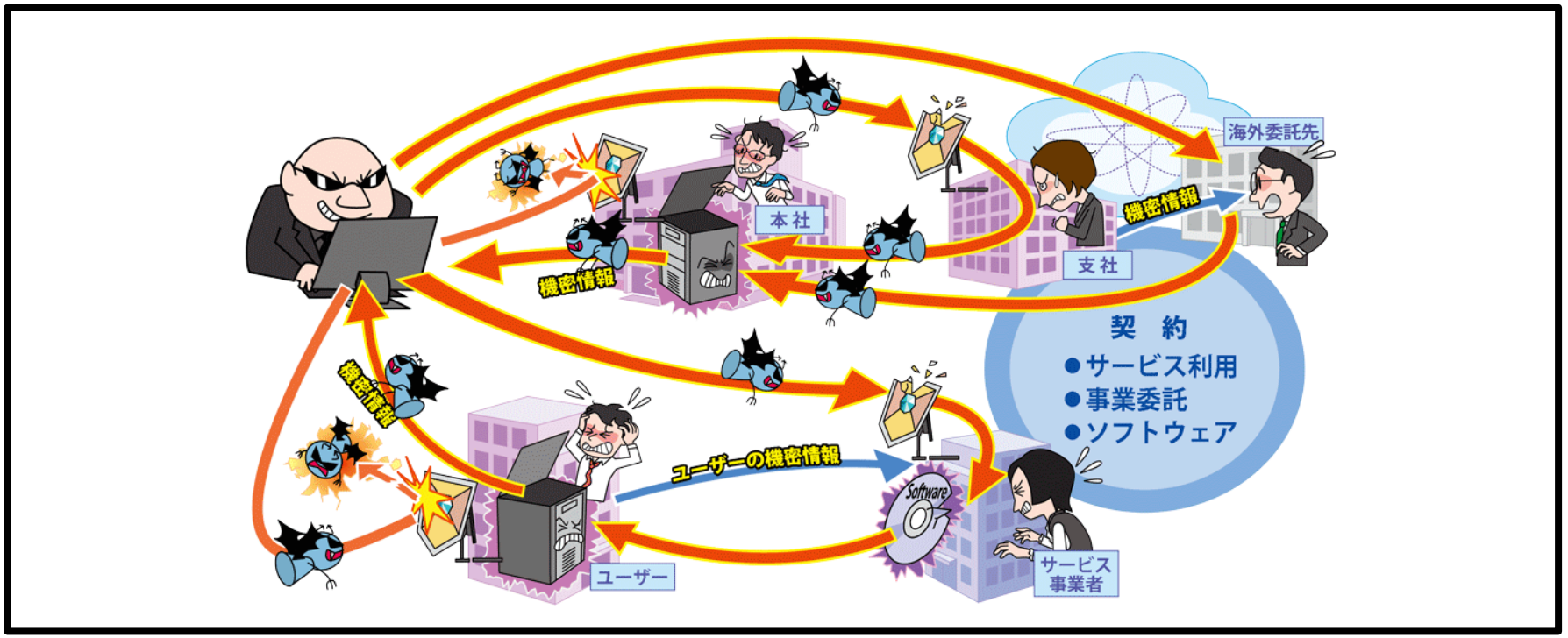
【2位】標的型攻撃による機密情報の窃取

～組織化しているサイバー攻撃～

- **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

【3位】サプライチェーンの弱点を悪用した攻撃

～サプライチェーン攻撃の世界的な被害増加に伴い、今一度リスクの見直しを～



- 原材料や部品の調達、製造、在庫管理、物流、販売、業務委託先等の一連の商流（サプライチェーン）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狙われる
- 取引先や業務を委託している外部組織から情報漏えい

【3位】サプライチェーンの弱点を悪用した攻撃

～サプライチェーン攻撃の世界的な被害増加に伴い、今一度リスクの見直しを～

● 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

【3位】サプライチェーンの弱点を悪用した攻撃

～サプライチェーン攻撃の世界的な被害増加に伴い、今一度リスクの見直しを～

- 2021年の事例/傾向①
  - サプライチェーン攻撃の世界的な増加(※1,※2)
    - ・OSS(オープンソースソフトウェア)を狙ったサプライチェーン攻撃が2021年は1万2,000件を超え前年比約650%増となった
    - ・クラウド運用等を行う技術者のうち36%が情報漏えい等の問題を経験しており、83%がクラウドの設定ミスに関連する情報漏えいに対して企業が脆弱であることを懸念している

【出典】
※1 2021 State of the Software Supply Chain Report(sonatype)
https://www.sonatype.com/resources/state-of-the-software-supply-chain-2021
※2 The State of Cloud Security 2021(sonatype)
https://www.sonatype.com/hubfs/State_of_Cloud_Security_2021.pdf

【3位】サプライチェーンの弱点を悪用した攻撃

～サプライチェーン攻撃の世界的な被害増加に伴い、今一度リスクの見直しを～

- 2021年の事例/傾向②
  - 子会社や海外拠点を狙った攻撃（※1）
    - 2021年4月、国内の光学機器メーカーの米子会社がランサムウェア攻撃を受けた
    - 約300GBの財務情報や顧客情報等が窃取されダークウェブ上で公開されていた
    - サイバー犯罪グループが犯行声明を発信していた

【出典】
※1 HOYA米子会社にサイバー攻撃 機密情報が闇サイトで公開か（日本放送協会）
https://www3.nhk.or.jp/news/html/20210424/k10012994941000.html

【3位】サプライチェーンの弱点を悪用した攻撃

～サプライチェーン攻撃の世界的な被害増加に伴い、今一度リスクの見直しを～

● 対策

■ 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
- 信頼できる委託先、取引先組織の選定
- 複数の取引先候補の検討
- 納品物の検証
- 契約内容の確認
- 委託先組織の管理

・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

【3位】サプライチェーンの弱点を悪用した攻撃

～サプライチェーン攻撃の世界的な被害増加に伴い、今一度リスクの見直しを～

● 対策

■ 組織（商流に関わる組織）

・被害の予防

－取引先や委託先の情報セキュリティ対応の確認、監査

－情報セキュリティの認証取得

（ISMS、Pマーク、SOC2、ISMAP等）

－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」（IPA）（※1）

「サイバーセキュリティ経営ガイドライン」（経済産業省/IPA）（※2）

・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

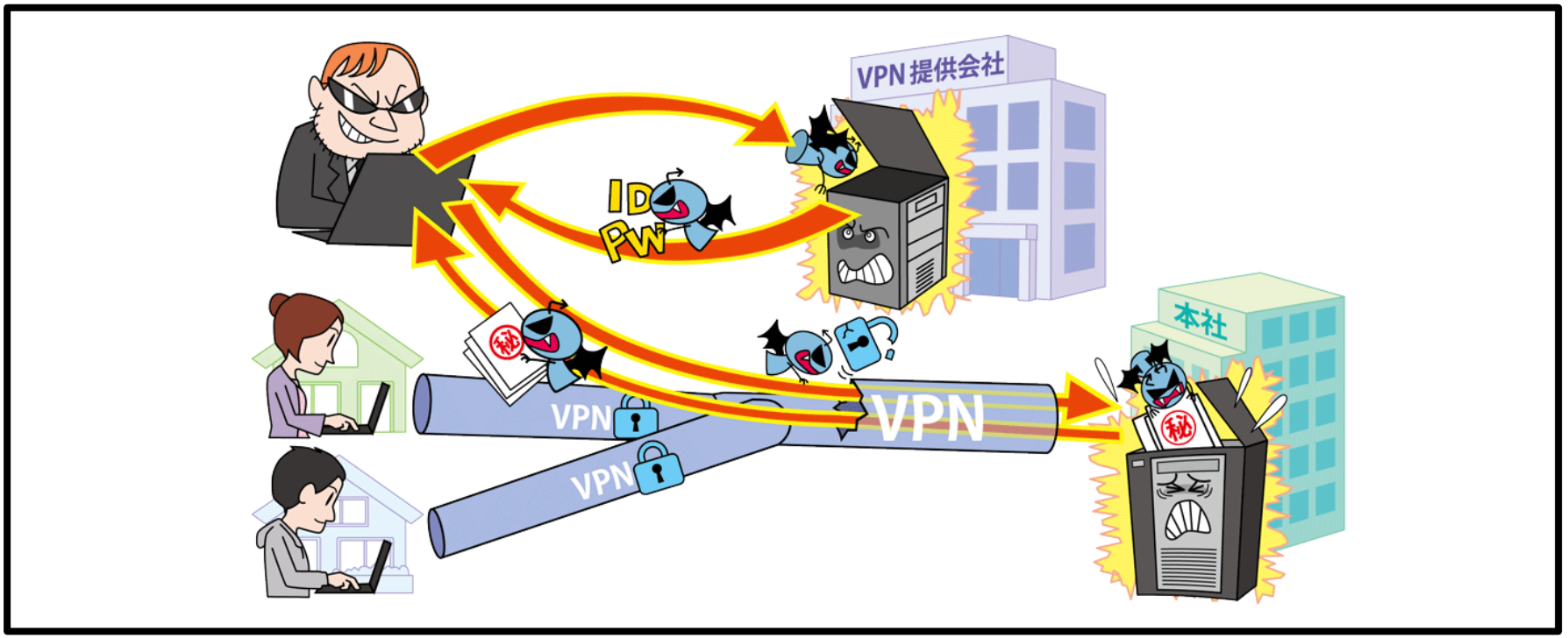
【出典】

※1 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

※2 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

【4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

～テレワークのセキュリティは企業と従業員の結束が不可欠～



- 2020年から続くコロナ禍の影響によりテレワークが普及
- ウェブ会議サービスやVPNの本格的な活用がされるなか、
  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

【4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

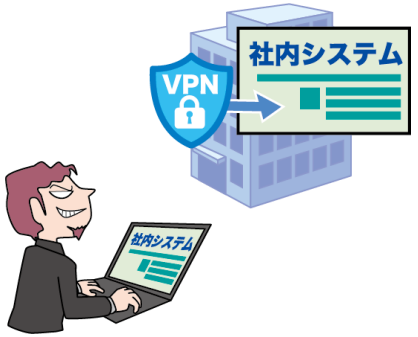
～テレワークのセキュリティは企業と従業員の結束が不可欠～

● 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
- 急なテレワーク移行による管理体制の不備
- 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



【4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

～テレワークのセキュリティは企業と従業員の結束が不可欠～

- 2021年の事例/傾向①
  - 脆弱性の悪用によりVPNのパスワード流出（※1）
    - 2021年9月、VPN製品の脆弱性が悪用されて窃取された数万社分の認証情報がインターネット上で公開されていた
    - 日本企業も中小企業を中心に約1,000社が被害を受けた
    - 悪用された脆弱性やその対策に関する情報は2019年に公開済みだった
    - **更新プログラムを適用していない**VPN製品が狙われる可能性

【出典】
※1 VPN認証情報また流出 日本は1000社、中小企業中心（日経電子版）
https://www.nikkei.com/article/DGXZQOUE110A80R10C21A9000000/

【4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

～テレワークのセキュリティは企業と従業員の結束が不可欠～

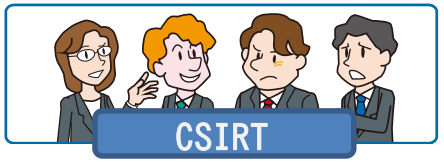
- 2021年の事例/傾向②
  - リモートデスクトップへの総当たり攻撃が急増(※1)
    - WHO(世界保健機関)のパンデミック宣言後、RDPへの不正ログインを試みる総当たり攻撃が増加した
    - 宣言前(2020年2月)の9,310 万件から宣言後(2020年3月)は2億7,740万件と約3倍となった
    - 2021年4月時点では月に3億件を超える状態が続いている

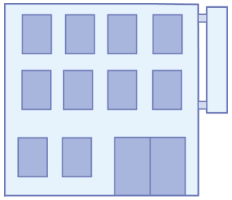
【出典】
※1 カスペルスキー、リモートデスクトップへの総当たり攻撃急増を報告(マイナビニュース)
https://news.mynavi.jp/article/20210406-1865958/

【4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

～テレワークのセキュリティは企業と従業員の結束が不可欠～

- **対策**
  - **組織（テレワーカー）**
    - ・被害の予防
      - －組織のテレワークルールを順守
        （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

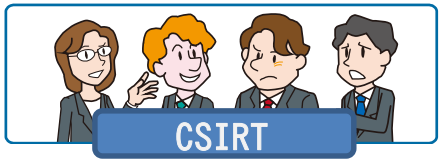


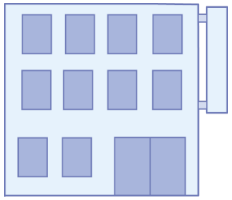


【4位】テレワーク等のニューノーマルな働き方を狙った攻撃

～テレワークのセキュリティは企業と従業員の結束が不可欠～

- **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

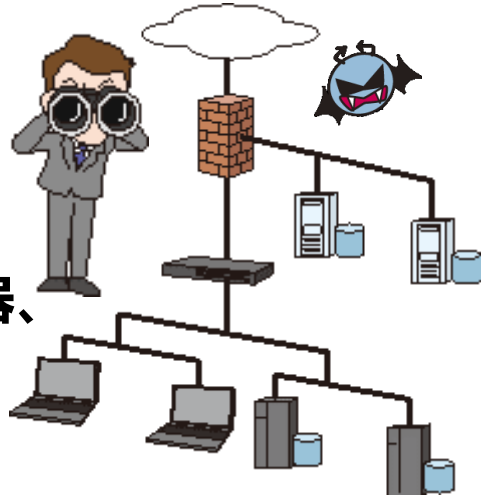




【4位】テレワーク等のニューノーマルな働き方を狙った攻撃

～テレワークのセキュリティは企業と従業員の結束が不可欠～

- **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



【4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

～テレワークのセキュリティは企業と従業員の結束が不可欠～

- **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**

【5位】内部不正による情報漏えい

～組織は内部不正をさせない、内部不正で取得された情報を利用しない～

- 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り、組織の社会的信用の失墜、損害賠償による経済的損失

【5位】内部不正による情報漏えい

～組織は内部不正をさせない、内部不正で取得された情報を利用しない～

● 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

【5位】内部不正による情報漏えい

～組織は内部不正をさせない、内部不正で取得された情報を利用しない～

- 2021年の事例/傾向①
  - 元従業員の転職先に対して損害賠償請求(※1,※2,※3)
    - ・2021年1月、大手通信キャリアの元従業員が同業他社へ転職する際不正にネットワーク技術に関わる情報を持ち出したとして逮捕された
    - ・元従業員は持ち出した機密情報を転職先に開示していた
    - ・情報漏えいの被害を受けた企業は元従業員の転職先の企業に対し情報の利用停止、廃棄、損害賠償として10億円を請求する民事訴訟を提起した

【出典】
※1 楽天モバイルへ転職した元社員の逮捕について（ソフトバンク株式会社）
https://www.softbank.jp/corp/news/press/sbkk/2021/20210112_01/
※2 楽天モバイルと楽天モバイル元社員に対する訴訟を提起 1,000億円規模の損害賠償請求権を主張（ソフトバンク株式会社）
https://www.softbank.jp/corp/news/press/sbkk/2021/20210506_01/
※3 当社に対する訴訟の提起について（楽天モバイル株式会社）
https://corp.rakuten.co.jp/news/update/2021/0506_01.html

【5位】内部不正による情報漏えい

～組織は内部不正をさせない、内部不正で取得された情報を利用しない～

- 2021年の事例/傾向②
  - 取引先の顧客情報を不正利用(※1)
    - ・2021年3月、証券会社のシステムの保守・運用等を委託されていた企業の元従業員が職務中に証券会社の顧客情報を不正に取得し使用したとして逮捕された
    - ・顧客15名の ID、パスワード、暗証番号等を利用して顧客になりすまし有価証券の売却や現金の不正出金
    - ・被害総額は約2億円となった

【出典】
※1 当社元社員による不正行為について（SCSK株式会社）
https://www.scsk.jp/news/2021/pdf/20210324.pdf

【5位】内部不正による情報漏えい

～組織は内部不正をさせない、内部不正で取得された情報を利用しない～

● 対策

■ 経営者、管理者

・被害の予防

- －基本方針の策定
- －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
- －物理的管理の実施

【5位】内部不正による情報漏えい

～組織は内部不正をさせない、内部不正で取得された情報を利用しない～

● 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

・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

【6位】脆弱性対策情報の公開に伴う悪用増加

～その脆弱性は実は関係してるかも？情報収集と適切な対応を！～

- 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
- 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

【6位】脆弱性対策情報の公開に伴う悪用増加

～その脆弱性は実は関係してるかも？情報収集と適切な対応を！～

IPA

● 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

【6位】脆弱性対策情報の公開に伴う悪用増加

～その脆弱性は実は関係してるかも？情報収集と適切な対応を！～

- 2021年の事例/傾向①
  - Javaのログ出力ライブラリ「Apache Log4j」の脆弱性（※1,※2,※3）
    - 2021年12月9日、Apache Log4jにおいて、リモートから任意のコードが実行可能な脆弱性（CVE-2021-44228）が公表された
    - 翌日10日に、実証コード（POC）が公開、多数の悪用を確認

【出典】
※1 【注意喚起】Log4jの脆弱性を狙う攻撃を多数検知、至急対策を！（株式会社ラック）
https://www.lac.co.jp/lacwatch/alert/20211213_002820.html
※2 Javaライブラリ「Apache Log4j」の脆弱性（CVE-2021-44228）を標的とした攻撃の観測について（警察庁）
https://www.npa.go.jp/cyberpolice/important/2021/202112141.html
※3 Apache Log4jの任意のコード実行の脆弱性（CVE-2021-44228）に関する注意喚起（（一社）JPCERTコーディネーションセンター）
https://www.jpcert.or.jp/at/2021/at210050.html

【6位】脆弱性対策情報の公開に伴う悪用増加

～その脆弱性は実は関係してるかも？情報収集と適切な対応を！～

- 2021年の事例/傾向②
  - Movable Typeの脆弱性を狙う攻撃が発生 (※1,※2)
    - 2021年10月20日、Movable Typeの脆弱性(CVE-2021-20837)が公表された
    - 数日後の26日には、POCが公開
    - 翌27日、脆弱性を探索しようとする通信を観測
    - 11月1日以降、脆弱性を悪用する攻撃を確認
    - 11月7日、ウェブサイトが改ざんされる被害発生

【出典】
※1 Movable TypeのXMLRPC APIにおける脆弱性(CVE-2021-20837)に関する注意喚起((一社)JPCERTコーディネーションセンター)
https://www.jpcert.or.jp/at/2021/at210047.html
※2 弊社ホームページへの不正アクセスと改ざんの経緯と原因、今後の対策について(株式会社サンメディア)
https://www.sunmedia.co.jp/news20211110/

【6位】脆弱性対策情報の公開に伴う悪用増加

～その脆弱性は実は関係してるかも？情報収集と適切な対応を！～

- 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
      - -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

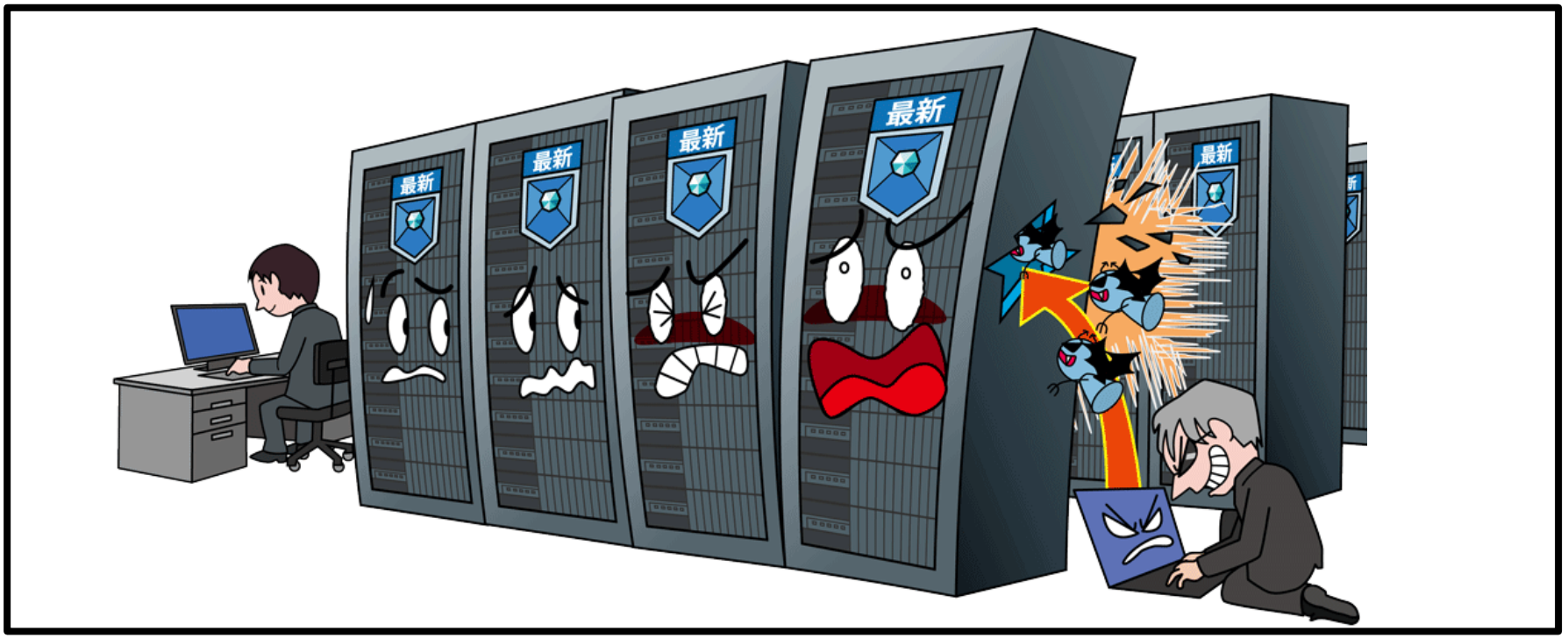
【6位】脆弱性対策情報の公開に伴う悪用増加

～その脆弱性は実は関係してるかも？情報収集と適切な対応を！～

- **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掌握、管理の徹底（SBOMを活用する）**
      - **－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**

【7位】修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）

～ゼロデイの脆弱性はセキュリティ担当者泣かせ～



- 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

【7位】修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）

～ゼロデイの脆弱性はセキュリティ担当者泣かせ～

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

【7位】修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）

～ゼロデイの脆弱性はセキュリティ担当者泣かせ～

- 2021年の事例/傾向①
  - VPN製品へのゼロデイ攻撃 (※1,※2)
    - 2021年4月20日（米国時間）、Pulse Secure社から、VPN製品「Pulse Connect Secure」の脆弱性が公開
    - 遠隔の第三者によって認証を回避し、任意のコードを実行されるおそれ
    - 米国では公表時点で既に脆弱性を悪用した攻撃が確認済み
    - 5月6日に修正プログラムがリリースされるまでは、暫定的な回避策を実施するか、当該製品を一時的に使用停止する必要があった

【出典】

※1 Pulse Connect Secureの脆弱性（CVE-2021-22893）に関する注意喚起（（一社）JPCERTコーディネーションセンター）
https://www.jpcert.or.jp/at/2021/at210019.html

※2 Pulse Connect Secure の脆弱性対策について（CVE-2021-22893）（IPA）
https://www.ipa.go.jp/security/ciadr/vul/alert20210421.html

【7位】修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）

～ゼロデイの脆弱性はセキュリティ担当者泣かせ～

- 2021年の事例/傾向②
  - 印刷スプーラーへのゼロデイ攻撃（※1,※2）
    - 2021年7月1日、Microsoftより Windowsの印刷スプーラー「Windows Print Spooler」の脆弱性に関する情報が公開
    - 「PrintNightmare」と呼ばれ、攻撃者によって任意のコードを実行される等の被害が発生するおそれ
    - 脆弱性の公開時点では修正プログラムのリリースはなし
    - 7月7日から修正プログラムが段階的に公開さるまで回避策や緩和策を適用する必要があった

【出典】

※1　Windowsの印刷スプーラーの脆弱性（CVE-2021-34527）に関する注意喚起（（一社）JPCERTコーディネーションセンター）
https://www.jpcert.or.jp/at/2021/at210029.html

※2　Microsoft Windows 製品の Windows Print Spooler の脆弱性対策について（CVE-2021-34527）（IPA）
https://www.ipa.go.jp/security/ciadr/vul/20210705-ms.html

【7位】修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
～ゼロデイの脆弱性はセキュリティ担当者泣かせ～

- 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
      - -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
    - ・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

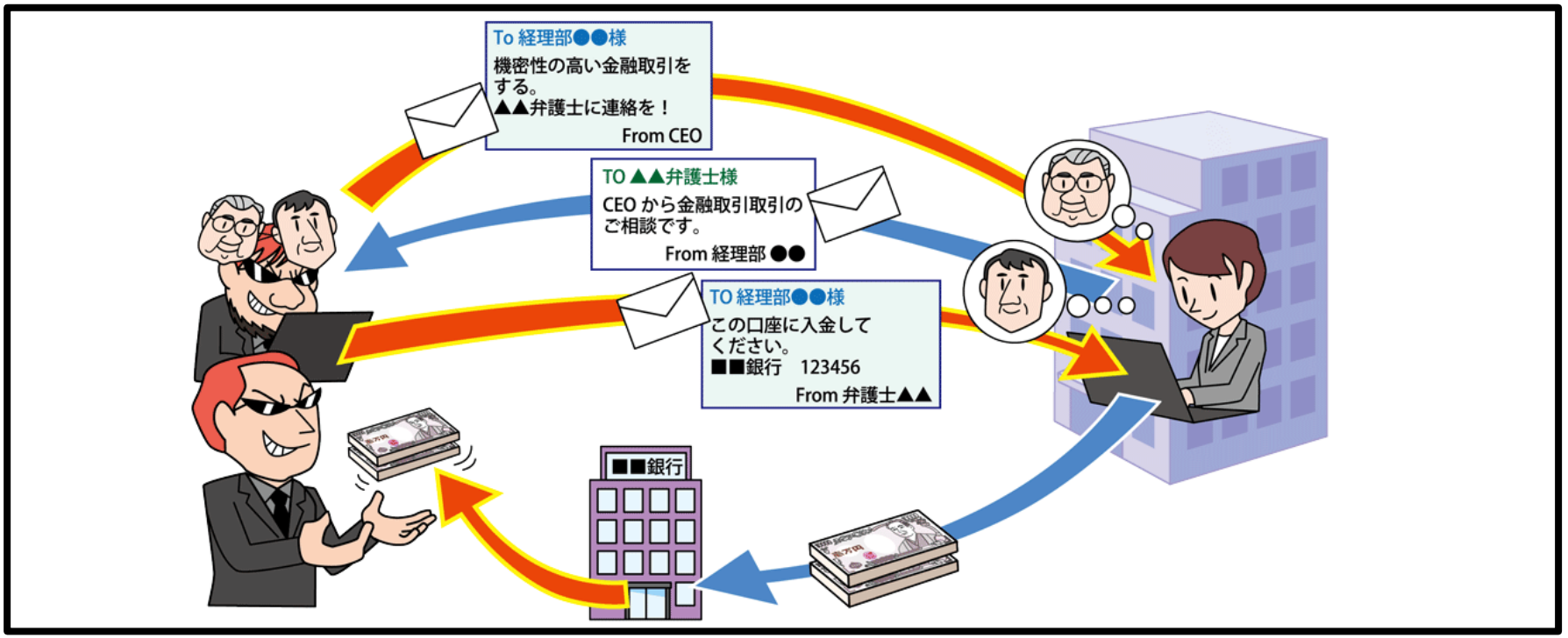
【7位】修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）

～ゼロデイの脆弱性はセキュリティ担当者泣かせ～

- 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

【8位】ビジネスメール詐欺による金銭被害

～経営者からの秘密の依頼、取引先からの口座変更依頼、電話で確認しよう～



- 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

～経営者からの秘密の依頼、取引先からの口座変更依頼、電話で確認しよう～

● 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

【8位】ビジネスメール詐欺による金銭被害

～経営者からの秘密の依頼、取引先からの口座変更依頼、電話で確認しよう～

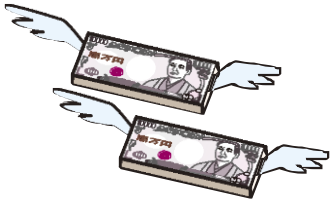
- 2021年の事例/傾向①
  - 会社役員を騙り海外関連企業を狙った攻撃（※1）
    - 2021年8月、サイバー情報共有イニシアティブ（J-CSIP）参加組織の海外関連企業の担当者が同社役員を騙ったビジネス詐欺メールを受信
    - 「機密性の高い金融取引を個人的に依頼したい」という内容で、実在する弁護士事務所の弁護士への連絡を依頼
    - 差出人（From）の表示名には会社役員の名前とメールアドレスが設定されていたが、フリーメールアドレスから送信されていた
    - 同報先（CC）には、弁護士のメールアドレスを騙った偽のメールアドレスが設定され、同報を装う

【出典】
※1 サイバー情報共有イニシアティブ（J-CSIP）運用状況 [2021 年 7 月～9 月]（IPA）
https://www.ipa.go.jp/files/000094117.pdf

【8位】ビジネスメール詐欺による金銭被害

～経営者からの秘密の依頼、取引先からの口座変更依頼、電話で確認しよう～

- 2021年の事例/傾向②
  - 一般社員になりすました詐欺メールを確認（※1）
    - トレンドマイクロによると、ビジネスメール詐欺（BEC）の脅威動向監視において、2021年1～9月にかけて検出数が増加
    - 特に、8月に大幅な増加
    - 攻撃者が経営幹部等になりすました詐欺メールだけではなく、一般社員になりすましたものも確認



【出典】
※1　電子メールサービスの特性を悪用する様々なビジネスメール詐欺の手口を解説（トレンドマイクロ株式会社）
https://blog.trendmicro.co.jp/archives/29272

【8位】ビジネスメール詐欺による金銭被害

～経営者からの秘密の依頼、取引先からの口座変更依頼、電話で確認しよう～

● 対策

■ 組織

・被害の予防

－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

<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

－普段とは異なるメールに注意

－送信元のメールドメインに注意

－判断を急がせるメールに注意

<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

【8位】ビジネスメール詐欺による金銭被害

～経営者からの秘密の依頼、取引先からの口座変更依頼、電話で確認しよう～

● 対策

■ 組織

・被害を受けた後の対応

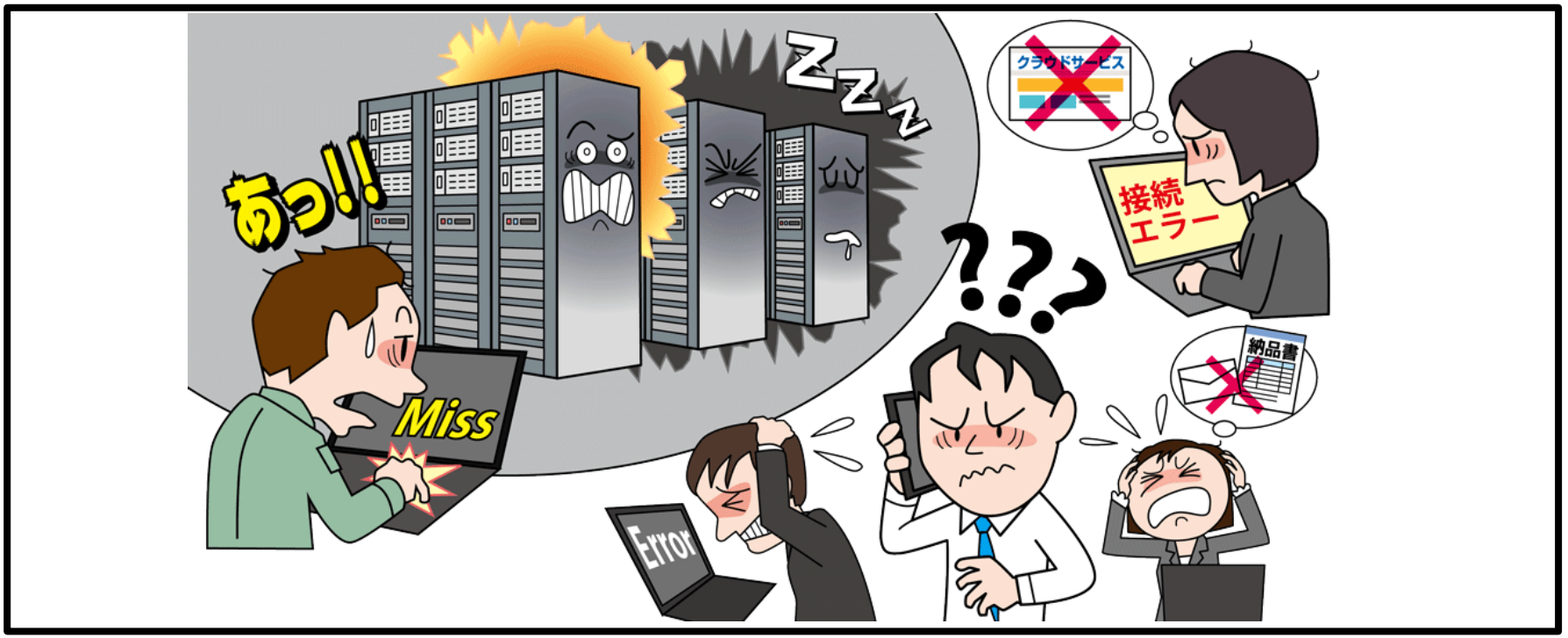
－組織の方針に従い各所へ報告、相談する
　上司、CSIRT、関係組織、公的機関等

－影響調査および原因追及、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

【9位】予期せぬIT基盤の障害に伴う業務停止

～平常時から代替手段の検討を～



- 利用しているデータセンターやクラウドのIT基盤等が停止
- 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

【9位】予期せぬIT基盤の障害に伴う業務停止

～平常時から代替手段の検討を～

発生要因

- 予期できない事象によりIT基盤が停止する
- BCMが適切に実践できていない

自然災害

- 地震や台風、洪水等の自然現象

作業事故

- インフラ設備のメンテナンスや、システムの設定変更作業における人為的ミス等

設備障害やシステム障害

- 電源、空調設備等の制御システムの障害
- IT基盤を構成する機器のハードウェアやソフトウェアに不具合等

【9位】予期せぬIT基盤の障害に伴う業務停止

～平常時から代替手段の検討を～

● 2021年の事例/傾向①

■ Amazon Web Servicesで障害発生 (※1,※2)

・2021年9月、Amazon Web Servicesが提供する専用ネットワーク接続「AWS Direct Connectクラウドサービス」で障害

・原因は、ネットワークの反応時間を最適化するために新しく導入した仕組みの影響で、東京リージョンのデータセンターのネットワーク機器に障害が発生したため

・障害により、銀行のアプリ、ネット証券のWebサイト、スマホ決済の入金等に影響

【出典】

※1 東京リージョン(AP-NORTHEAST-1)で発生したAWS Direct Connectの事象についてのサマリー(Amazon Web Services)
https://aws.amazon.com/jp/message/17908/

※2 アマゾン子会社AWSで障害 データ管理サービス 広範囲に影響(日本放送協会)
https://www3.nhk.or.jp/news/html/20210902/k10013238691000.html

【9位】予期せぬIT基盤の障害に伴う業務停止

～平常時から代替手段の検討を～

- 2021年の事例/傾向②
  - NTTドコモで通信障害発生(※1,※2)
    - 2021年10月、大手携帯キャリアが提供する音声通話・データ通信サービスで障害
    - 原因は、ネットワーク工事の切り戻しに伴う信号量増大によるネットワーク輻輳のため
    - 障害発生の同日に回復が発表されたものの、利用者が利用しづらい状態は翌日まで続いた
    - 影響は延べ1,290万人に及んだ

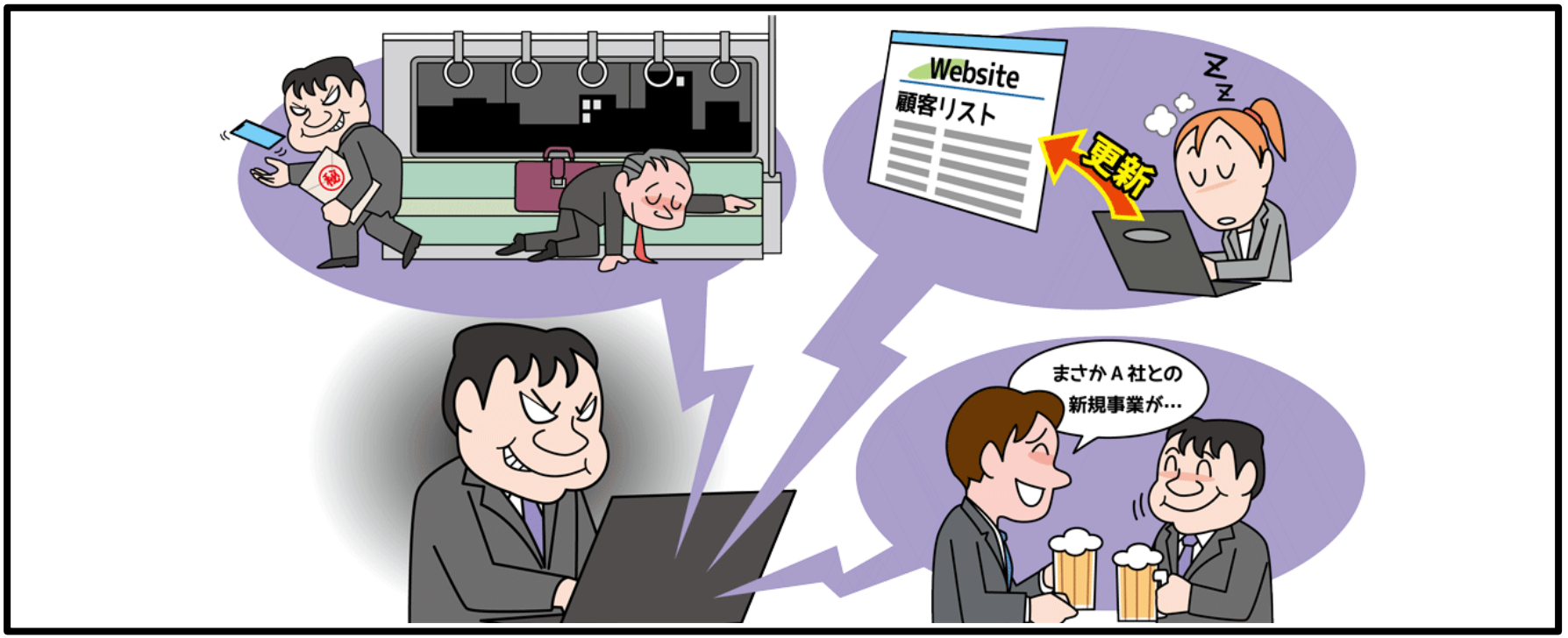
【出典】
※1 音声通話・データ通信サービスがご利用しづらい事象について(株式会社NTTドコモ)
https://www.nttdocomo.co.jp/info/network/kanto/pages/211014_00_m.html
※2 ドコモの10月通信障害、延べ1290万人に影響((日経電子版)
https://www.nikkei.com/article/DGXZQOUC080YW0Y1A101C2000000/

【9位】予期せぬIT基盤の障害に伴う業務停止
～平常時から代替手段の検討を～

- 対策
  - 組織（システム管理者）
    - ・被害の予防（被害に備えた対策を含む）
      - －事業継続マネジメント（BCM）の実践（BCP策定と運用）
      - －可用性の確保と維持（システム設計や監視）
      - －データバックアップ（復旧対策）
      - －契約やSLA等を確認
        - IT基盤側との契約、SLA
        - 顧客側との契約、SLA
      - －障害時のIT基盤側との連携を確認
    - ・被害を受けた後の対応
      - －BCPに従った対応
      - －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

【10位】不注意による情報漏えい等の被害

～そのメールの宛先、本当にあっていますか？～



- 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

【10位】不注意による情報漏えい等の被害

～そのメールの宛先、本当にあっていますか？～

● 要因

・個人の情報リテラシーやモラル不足からの不注意

・組織の管理体制の不備

■ 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

■ 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

【10位】不注意による情報漏えい等の被害

～そのメールの宛先、本当にあっていますか？～

- 2021年の事例/傾向①
  - 委託先のソースコードを私的利用で情報漏えい(※1)
    - ・2021年1月、金融機関が同行のシステムで使用しているソースコードが外部サイトにて公開
    - ・原因は、同行より委託されていた企業の社員が、自身の書いたソースコードをアップロードすることで年収を診断できるサービスを利用するために外部サイトにソースコードをアップロードしたため
    - ・同行は顧客情報の流出はなくセキュリティには問題ないとしている

【出典】

※1　三井住友銀行などのソースコードが流出　“年収診断”したさにGitHubに公開か【追記あり】(ITmedia NEWS)
https://www.itmedia.co.jp/news/articles/2101/29/news107.html

【10位】不注意による情報漏えい等の被害

～そのメールの宛先、本当にあっていますか？～

- 2021年の事例/傾向②
  - 送付データに不備があり情報漏えい（※1）
    - 2021年9月、クレジットカード・信販会社はカード会員向けサービスで使用する47万5,813人分のIDとパスワードが、本来は渡す必要のない委託先2社に誤送信
    - 原因は、委託先に送付する際の、確認手法に不備があったため
    - 対策として、データを渡す際の仕組みを見直すほか、社員の意識改善を進めている

【出典】
※1　親会社の委託先にID・パスワード47万人分を誤提供、新生銀行傘下のアプラスがクレカ会員向けサービスで（ITmedia NEWS）
https://www.itmedia.co.jp/news/articles/2109/17/news126.html

【10位】不注意による情報漏えい等の被害

～そのメールの宛先、本当にあっていますか？～

- 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
      - －組織規程および確認プロセスの見直し
    - ・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
      - －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（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

【10位】不注意による情報漏えい等の被害

～そのメールの宛先、本当にあっていますか？～

- **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

【10位】不注意による情報漏えい等の被害

～そのメールの宛先、本当にあっていますか？～

- 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

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

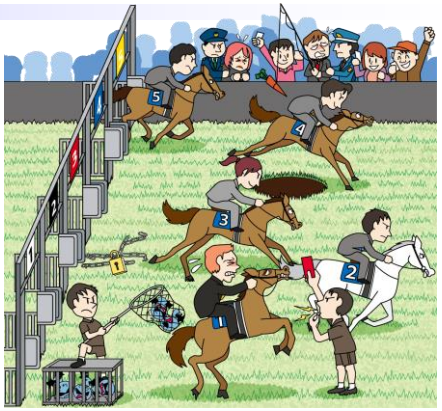
- 脅威に備えるためには攻撃手口や動向、および自組織が抱える要因等を把握することが重要
- 「10大脅威」のランキングは、各組織において実施すべき対策の優先度とは必ずしも一致はしない。組織ごとの状況を考慮して対策の優先度を決定する

詳細な資料のダウンロード

■情報セキュリティ10大脅威　2022

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/vuln/10threats2022.html

■アンケートご協力のお願いについて

IPAが公開しているツールや資料の品質向上のため、アンケートへのご協力をお願い致します

https://touroku.ipa.go.jp/?url=http%3A%2F%2Fspd-evsan-ap01.ipa.go.jp%2Fentry%2FMemberLogin%3Fevent_id%3DEA0000000074