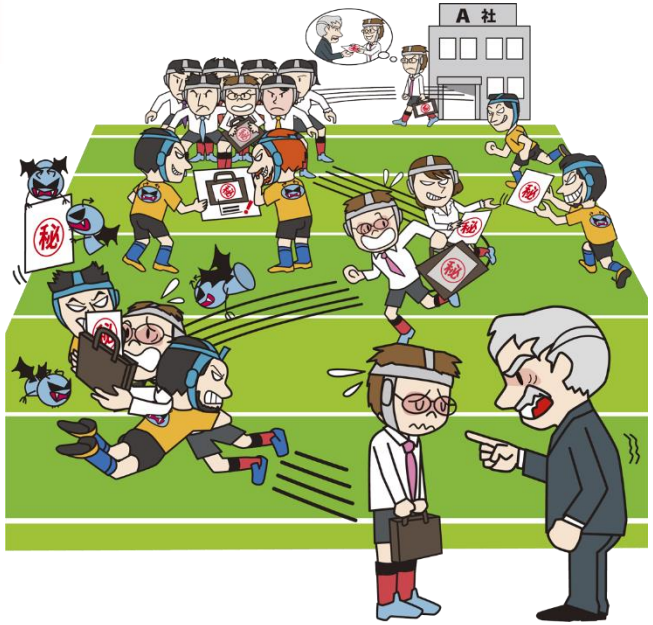
IPA Better Life with IT

情報セキュリティ10大脅威 2020

～セキュリティ対策は一丸となって、Let's Try!!～

[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
2020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」**

- 企業や政府機関などの組織
- 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 2020

IPA

- 「情報セキュリティ10大脅威 2020」の章構成
  - 1章. 知っておきたい用語や仕組み
    パソコンやスマホ、インターネットを安全に使用するための知識を習得するにあたってよく登場する用語や仕組みについて解説
  - 2章. 情報セキュリティ10大脅威 2020
    2019年の事例や傾向をもとに選出した「情報セキュリティ10大脅威 2020」について各脅威の概要や対策等について解説
  - 3章. 情報セキュリティ10大脅威の活用法
    組織や自分の立場・環境によって重要度の高い脅威が異なることを踏まえ、サービスや顧客情報等の「守るべきもの」を明らかにした上で、情報セキュリティ10大脅威を活用しながら効率的に対策を講じるための手順を解説

情報セキュリティ10大脅威 2020 脅威ランキング

IPA

「個人」向け脅威	順位	「組織」向け脅威
スマホ決済の不正利用	1	標的型攻撃による機密情報の窃取
フィッシングによる個人情報の詐取	2	内部不正による情報漏えい
クレジットカード情報の不正利用	3	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	4	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	5	ランサムウェアによる被害
不正アプリによるスマートフォン利用者への被害	6	予期せぬIT基盤の障害に伴う業務停止
ネット上の誹謗・中傷・デマ	7	不注意による情報漏えい
インターネット上のサービスへの不正ログイン	8	インターネット上のサービスからの個人情報の窃取
偽警告によるインターネット詐欺	9	IoT機器の不正利用
インターネット上のサービスからの個人情報の窃取	10	サービス妨害攻撃によるサービスの停止

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

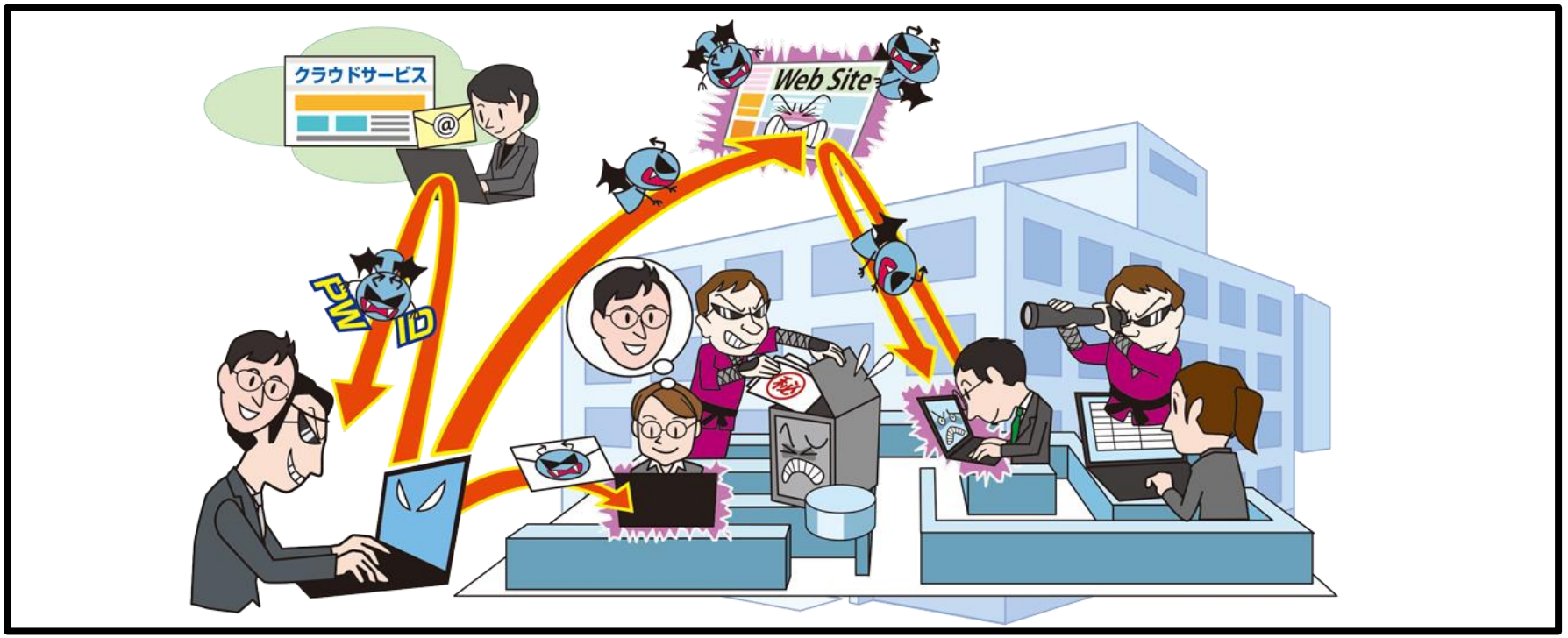
攻撃の糸口	情報セキュリティ対策の基本	目的
ソフトウェアの脆弱性	ソフトウェアの更新	脆弱性を解消し攻撃によるリスクを低減する
ウイルス感染	セキュリティソフトの利用	攻撃をブロックする
パスワード窃取	パスワードの管理・認証の強化	パスワード窃取によるリスクを低減する
設定不備	設定の見直し	誤った設定を攻撃に利用されないようにする
誘導（罠にはめる）	脅威・手口を知る	手口から重要視するべき対策を理解する

情報セキュリティ10大脅威 2020
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】標的型攻撃による機密情報の窃取

～引き続き行われる標的型攻撃、様々な仕掛けで発見を遅らせる～



- メール等によりPCをウイルスに感染させ組織内部へ潜入
- 長期にわたって侵害範囲を徐々に広げる
- 組織の機密情報を窃取

【1位】標的型攻撃による機密情報の窃取

～引き続き行われる標的型攻撃、様々な仕掛けで発見を遅らせる～

● 攻撃手口

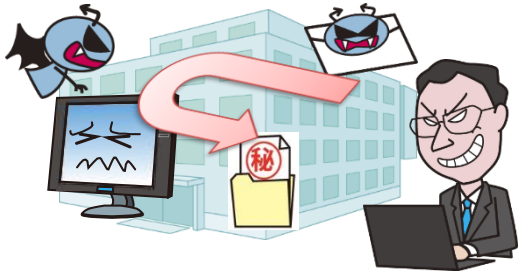
・メールやウェブサイトからウイルスに感染させる

■ 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）



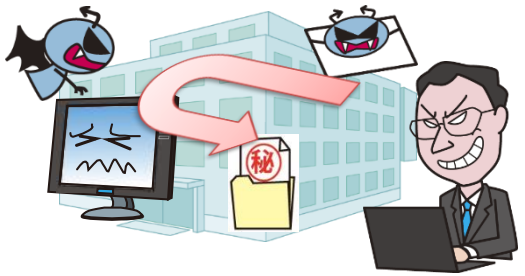
【1位】標的型攻撃による機密情報の窃取
～引き続き行われる標的型攻撃、様々な仕掛けで発見を遅らせる～

攻撃手口

・不正アクセスによってウイルスに感染させる

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へ不正にログイン
- 社内システムへ正規の経路を悪用し不正にアクセス
- 社内システムへウイルスを感染させる



【1位】標的型攻撃による機密情報の窃取
～引き続き行われる標的型攻撃、様々な仕掛けで発見を遅らせる～

- 2019年の事例/傾向
  - サイバー情報共有イニシアティブ(J-CSIP)による報告(※1)
    - ・プラント関連事業者を狙う攻撃メールが多数
    - ・巧妙な仕掛けが施されたウイルスも確認された
      (「アイコンや拡張子の偽装」、「特定のセキュリティソフトの停止」
      「特定の時間帯のみ動作を行う」など)
    - ・マクロ付きのWord文書ファイルを添付した攻撃メールが確認
      された
      (添付ファイルを開き、マクロを有効化してしまうとウイルスに
      感染するおそれ)

【出典】
※1 サイバー情報共有イニシアティブ(J-CSIP(ジェイシップ)) - 公開レポート Vol.27、28、30、31、32、33、34、35
https://www.ipa.go.jp/security/J-CSIP/

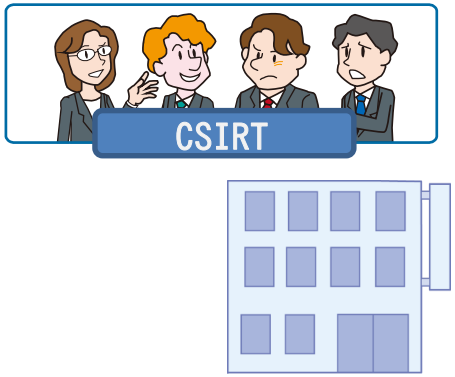
【1位】標的型攻撃による機密情報の窃取
～引き続き行われる標的型攻撃、様々な仕掛けで発見を遅らせる～

- 2019年の事例/傾向
  - 複数の防衛関連企業への不正アクセス報道 (※1,※2)
    - ・外部からの不正アクセス事案について大手総合電機メーカーが公表
    - ・不審な挙動が見られる社内端末が確認され発覚
    - ・その後も複数の企業が立て続けに不正アクセス被害を公表

【出典】
※1 不正アクセスによる個人情報と企業機密の流出可能性について(第3 報)
https://www.mitsubishielectric.co.jp/news/2020/0212-b.pdf
※2 神戸製鋼所とパスコにサイバー攻撃 防衛情報標的か
https://www.nikkei.com/article/DGXMZO55342190W0A200C2CR8000/

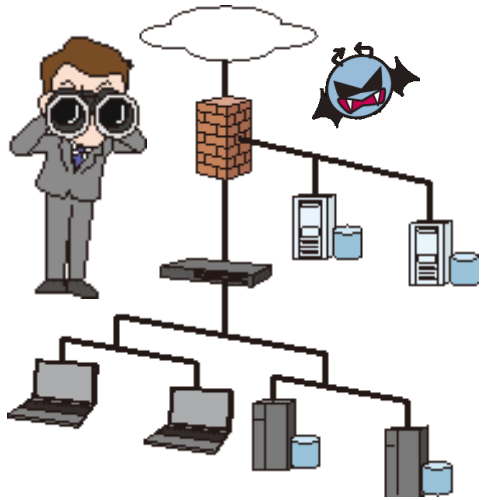
【1位】標的型攻撃による機密情報の窃取
～引き続き行われる標的型攻撃、様々な仕掛けで発見を遅らせる～

- 対策
  - 経営者層
    - ・組織としての体制の確立
      - –迅速かつ継続的に対応できる組織内体制（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



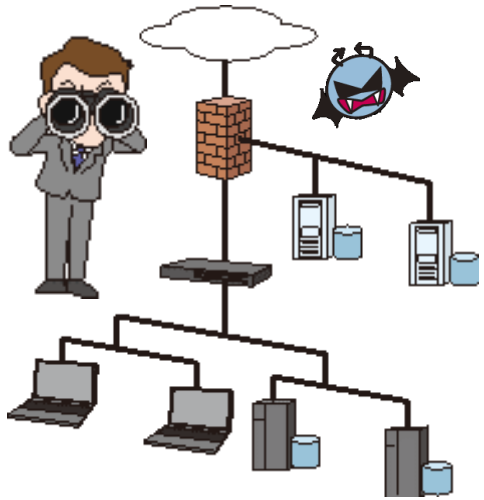
【1位】標的型攻撃による機密情報の窃取
～引き続き行われる標的型攻撃、様々な仕掛けで発見を遅らせる～

- 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と情報共有
      - –セキュリティ教育・インシデント訓練
      - –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
      - –取引先のセキュリティ対策実施状況の確認
      - –セキュアなシステム設計
      - –ネットワーク分離
      - –重要サーバーの要塞化(アクセス制御、暗号化等)
      - –海外拠点等も含めたセキュリティ対策の向上



【1位】標的型攻撃による機密情報の窃取
～引き続き行われる標的型攻撃、様々な仕掛けで発見を遅らせる～

- 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
      - –ネットワーク監視・防御
        UTM・IDS/IPS・WAFなどの導入
      - –エンドポイントの監視・防御
    - ・被害を受けた後の対応
      - –CSIRTの運用によるインシデント対応
      - –影響調査および原因の追究、対策の強化
      - –関係者、関係機関への連絡
        監督官庁、個人情報保護委員会、警察等

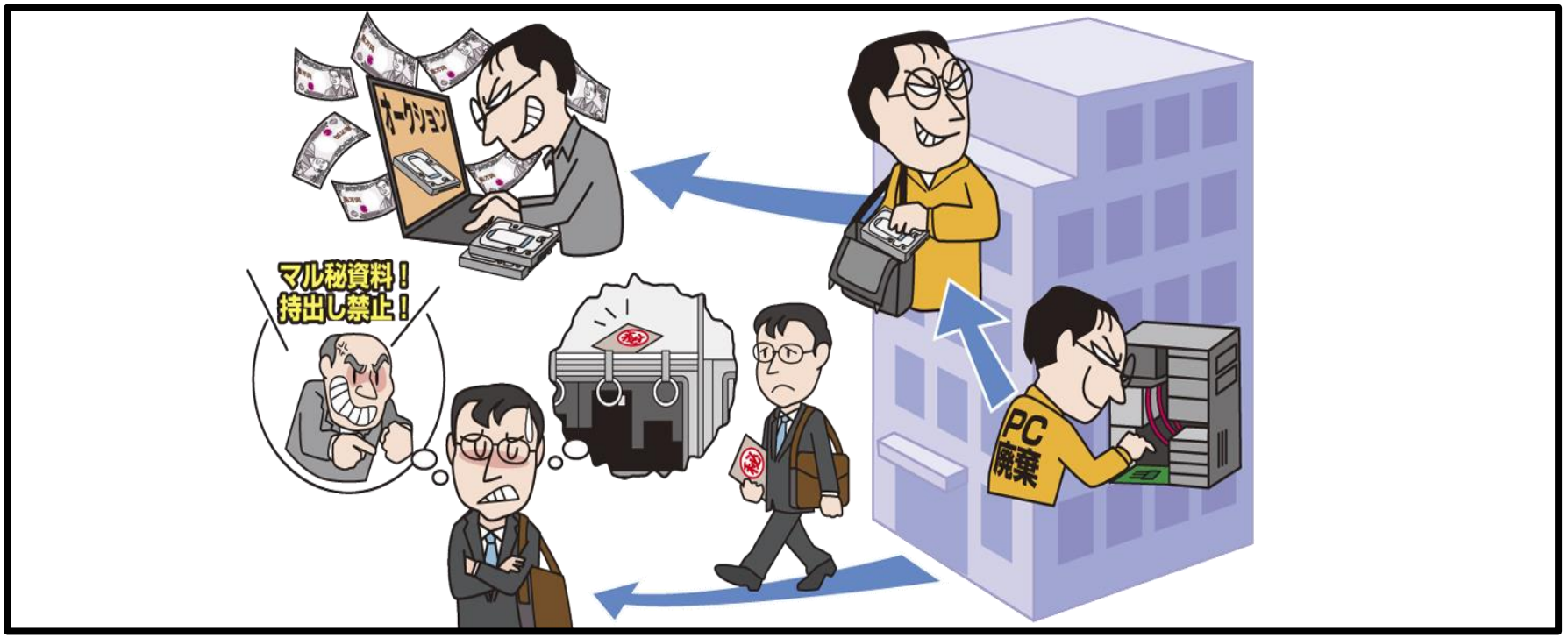


【1位】標的型攻撃による機密情報の窃取
～引き続き行われる標的型攻撃、様々な仕掛けで発見を遅らせる～

- 対策
  - 従業員、職員
    - ・情報リテラシーの向上
      - －セキュリティ教育の受講
        - 「メールの添付ファイルやURLを安易に開かない」
        - 「Officeファイルのマクロを安易に有効化しない」
        - 「被害を受けた際は迅速に連絡」
    - ・被害を受けた後の対応
      - －CSIRTへの連絡

【2位】内部不正による情報漏えい

～内部不正をさせない管理・監視体制を～



- 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り、組織の社会的信用の失墜、損害賠償による経済的損失

【2位】内部不正による情報漏えい

～内部不正をさせない管理・監視体制を～

● 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

・離職前に使用していたアカウントを使って不正に情報を取得

■ USBメモリーやメール等による持ち出し

【2位】内部不正による情報漏えい

～内部不正をさせない管理・監視体制を～

- 2019年の事例/傾向
  - 従業員が破壊処理予定のHDDを不正持ち出し(※1,※2)
    - ・情報機器の再生事業を手掛ける企業の従業員が破壊処理予定のHDDを盗み出してネットオークション等で転売
    - ・当該HDDは神奈川県で使用していたもの
    - ・HDD内に残っていた神奈川県の内部資料や個人情報などが流出
    - ・当該企業は従業員を懲戒解雇し、警察へ被害届を提出

【出典】
※1 （情報システム課からのお知らせ）リース契約満了により返却したハードディスクの盗難について
https://www.pref.kanagawa.jp/docs/fz7/cnt/p0273317.html
※2 当社管理下にあるハードディスク及びデータの外部流出に関するお詫び
https://www.broadlink.co.jp/info/pdf/20191209-02-press-release.pdf

【2位】内部不正による情報漏えい

～内部不正をさせない管理・監視体制を～

- 2019年の事例/傾向
  - 元従業員が患者情報等を不正持ち出し(※1)
    - ・医療機器の製造、販売を手掛ける企業の元従業員が、患者情報、顧客やアンケート回答者の個人情報、技術や営業に関する情報を不正に持ち出し
    - ・患者情報は社用PCからUSBメモリーで私用PCにコピー
    - ・元従業員は不正競争防止法違反の容疑で書類送検

【出典】
※1 当社元従業員の不正行為について（お詫びとご説明）
https://www.arkray.co.jp/japanese/news/press/release20190308_jp_jp.html

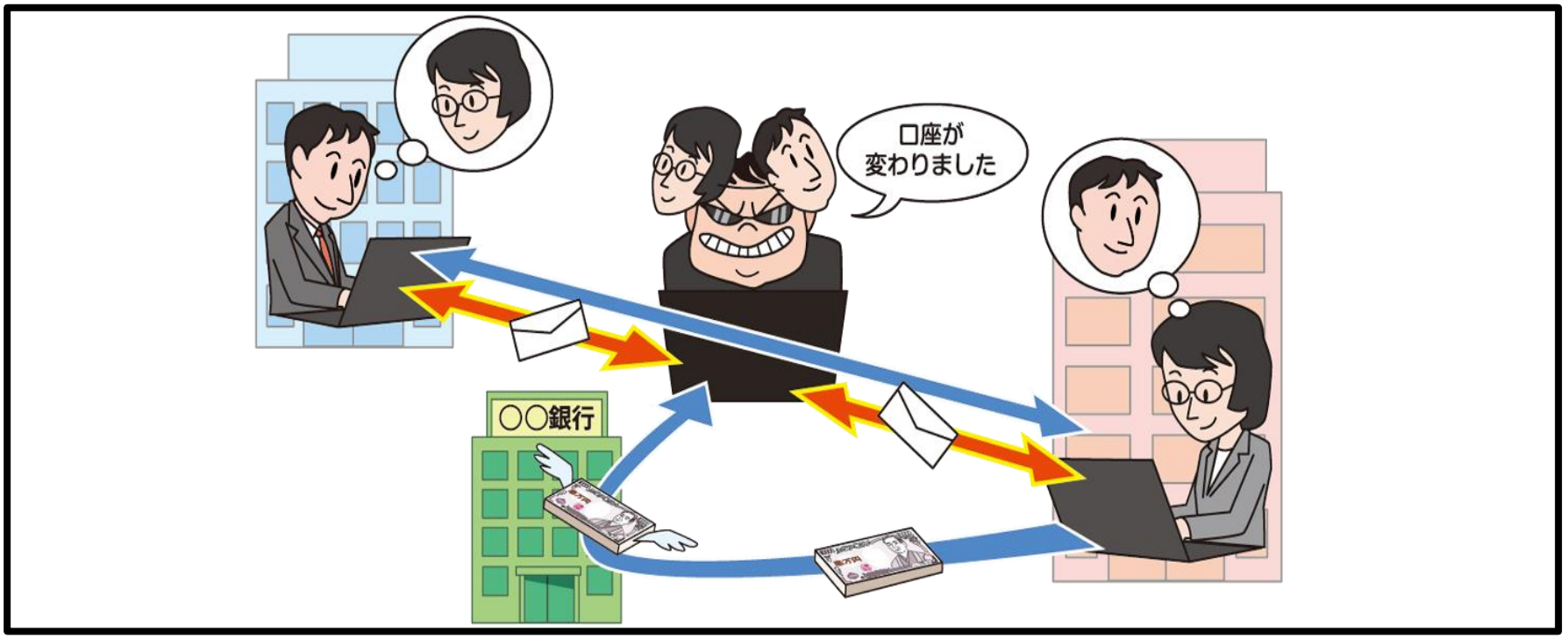
【2位】内部不正による情報漏えい

～内部不正をさせない管理・監視体制を～

- **対策**
  - **経営者、管理者**
    - ・被害の予防
      - －基本方針の策定
      - －情報資産の把握、体制の整備
      - －重要情報の管理、保護
    - ・情報モラルの向上
      - －人的管理、コンプライアンス教育徹底
    - ・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
      - －関係者、関係機関への連絡
        監督官庁、個人情報保護委員会、警察等
      - －内部不正者に対する適切な処罰実施

【3位】ビジネスメール詐欺による金銭被害

～ここ数年でメジャーなサイバーリスクへと変貌～



- 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
- 攻撃者の用意した口座へ送金させる

【3位】ビジネスメール詐欺による金銭被害

～ここ数年でメジャーなサイバーリスクへと変貌～

IPA

● 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

【3位】ビジネスメール詐欺による金銭被害

～ここ数年でメジャーなサイバーリスクへと変貌～

- 2019年の事例/傾向
  - ビジネスメール詐欺容疑、日本で逮捕者(※1)
    - 海外企業の会社代表のメールアカウントを乗っ取り
    - 約1億1千万円を日本国内の信用金庫へ振り込ませた
    - 詐欺と組織犯罪処罰法違反の容疑で日本人2人を逮捕

【出典】
※1 ビジネスメール詐欺容疑、日本で逮捕者 マフィア関与か
https://www.asahi.com/articles/ASM3W7529M3WUTILO6D.html

【3位】ビジネスメール詐欺による金銭被害

～ここ数年でメジャーなサイバーリスクへと変貌～

- 2019年の事例/傾向
  - サイバー情報共有イニシアティブ(J-CSIP)運用状況 [2019年4月～6月](※1)

<確認された手口>

・標的組織が新規取引先とやりとりしているところに介入

・偽口座を記載した見積書を「差し替え」と称して送付

※偽メールで見積金額変更を依頼しつつ振込先口座も改変

【出典】

※1 サイバー情報共有イニシアティブ(J-CSIP)運用状況 [2019年4月～6月]
https://www.ipa.go.jp/files/000076713.pdf

【3位】ビジネスメール詐欺による金銭被害

～ここ数年でメジャーなサイバーリスクへと変貌～

● 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

－メールに電子証明を付与（S/MIME） ※なりすまし防止

<メールの真正性の確認>

－メール以外の方法で事実確認

－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

－ログイン通知機能等で不正ログイン対策

【3位】ビジネスメール詐欺による金銭被害

～ここ数年でメジャーなサイバーリスクへと変貌～

対策

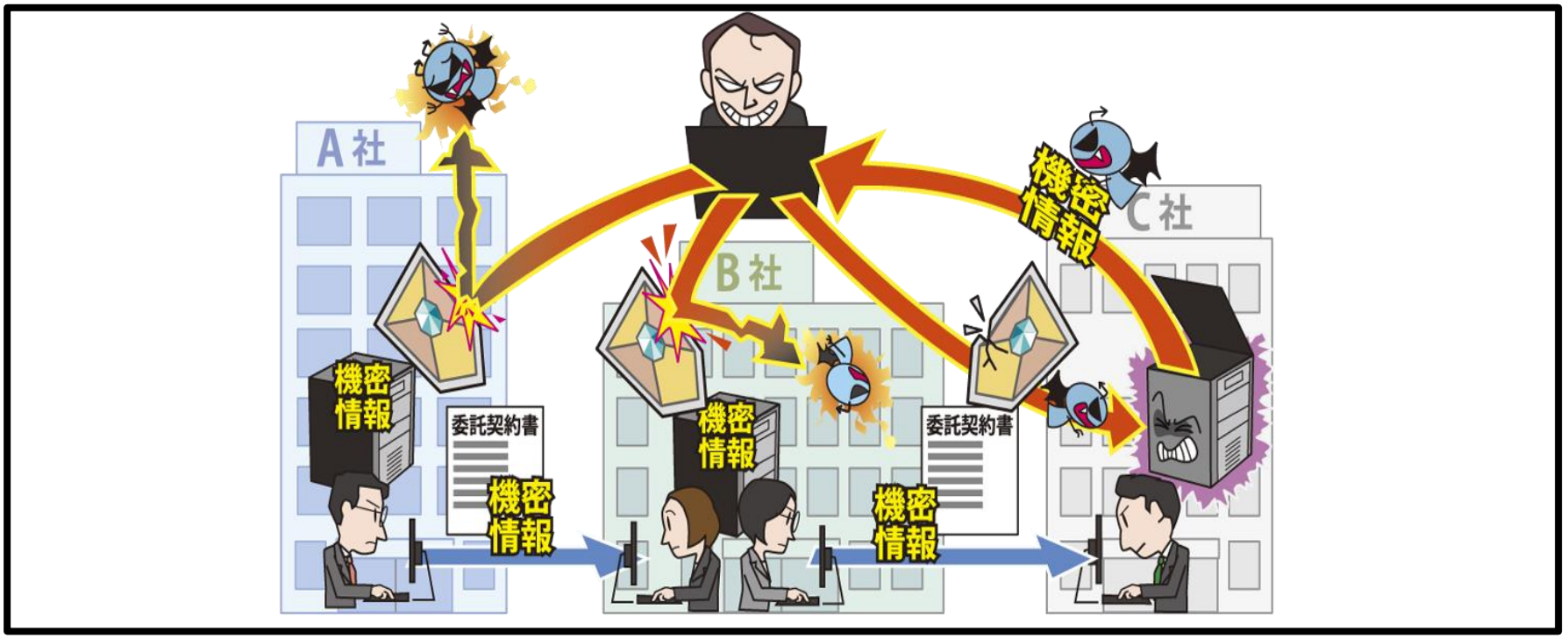
組織（金銭の決裁権限を持つ責任者、金銭を取り扱う担当者）

・被害を受けた後の対応

- CSIRTへの連絡
- 警察に相談
- 踏み台や詐称されている組織への連絡
- 影響調査および原因追及、対策の強化

【4位】サプライチェーンの弱点を悪用した攻撃

～業務委託先にも適切なセキュリティ管理を要求～



- 原材料や部品の調達、製造、在庫管理、物流、販売、業務委託先などの一連の商流（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
- 一部業務を委託している外部委託先組織から情報が漏えい

【4位】サプライチェーンの弱点を悪用した攻撃

～業務委託先にも適切なセキュリティ管理を要求～

● 要因

・サプライチェーンのセキュリティ対策不足

- **サプライチェーンを適切に選定、管理していない**
- **再委託先や再々委託先の管理は困難**

  委託先組織の先に再委託先組織や再々委託先組織がある場合、その管理は委託先組織が行うため、委託元からのセキュリティ対策管理はさらに難しくなる

【4位】サプライチェーンの弱点を悪用した攻撃

～業務委託先にも適切なセキュリティ管理を要求～

- 2019年の事例/傾向
  - 再委託先の開発環境への不正アクセス(※1)
    - ・再委託先のスポーツ関連企業が不正アクセスを受けた
    - ・開発環境のサーバー内からデータが削除された
    - ・開発環境のセキュリティ設定に不備
    - ・削除されたデータは国体参加者データ等で、氏名、性別、生年月日等が含まれる
    - ・データの流出や公開の事実は確認されていない

【出典】
※1 国民体育大会参加者データおよび公認スポーツ指導者データの消失について
https://www.japan-sports.or.jp/news/tabid92.html?itemid=4065

【4位】サプライチェーンの弱点を悪用した攻撃

～業務委託先にも適切なセキュリティ管理を要求～

- 2019年の事例/傾向
  - サプライチェーンに関する調査報告書を公開 (※1)
    - IPAが「ITサプライチェーンにおける情報セキュリティの責任範囲に関する調査報告書」を公開
    - IT業務委託契約書において委託元の約8割が「新たな脅威が顕在化した際の対応」について責任範囲を明記していない
    - 理由は「専門知識・スキルが不足している」が最多の79.6%

【出典】
※1 「ITサプライチェーンにおける情報セキュリティの責任範囲に関する調査」報告書について
https://www.ipa.go.jp/security/fy30/reports/scrm/index.html

【4位】サプライチェーンの弱点を悪用した攻撃

～業務委託先にも適切なセキュリティ管理を要求～

- 対策
  - 委託元組織
    - ・被害の予防
      - –業務委託や情報管理における規則の徹底
      - –信頼できる委託先組織の選定
      - –委託先からの納品物の検証
      - –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

【4位】サプライチェーンの弱点を悪用した攻撃

～業務委託先にも適切なセキュリティ管理を要求～

- 対策
  - 委託先組織
    - ・被害の予防
      - –攻撃者の目的や攻撃手段は多岐にわたるため、他の脅威の対策も参考に業務に応じた広範な対策が必要
    - ・被害を受けた後の対応
      - –委託元への連絡

【4位】サプライチェーンの弱点を悪用した攻撃

～業務委託先にも適切なセキュリティ管理を要求～

- **対策**
  - **委託先/委託元組織共通**
    - ・被害の予防
      - －公的機関が公開しているガイドラインの活用

        「サイバーセキュリティ経営ガイドライン」(※1)

        「中小企業の情報セキュリティ対策ガイドライン」(※2)

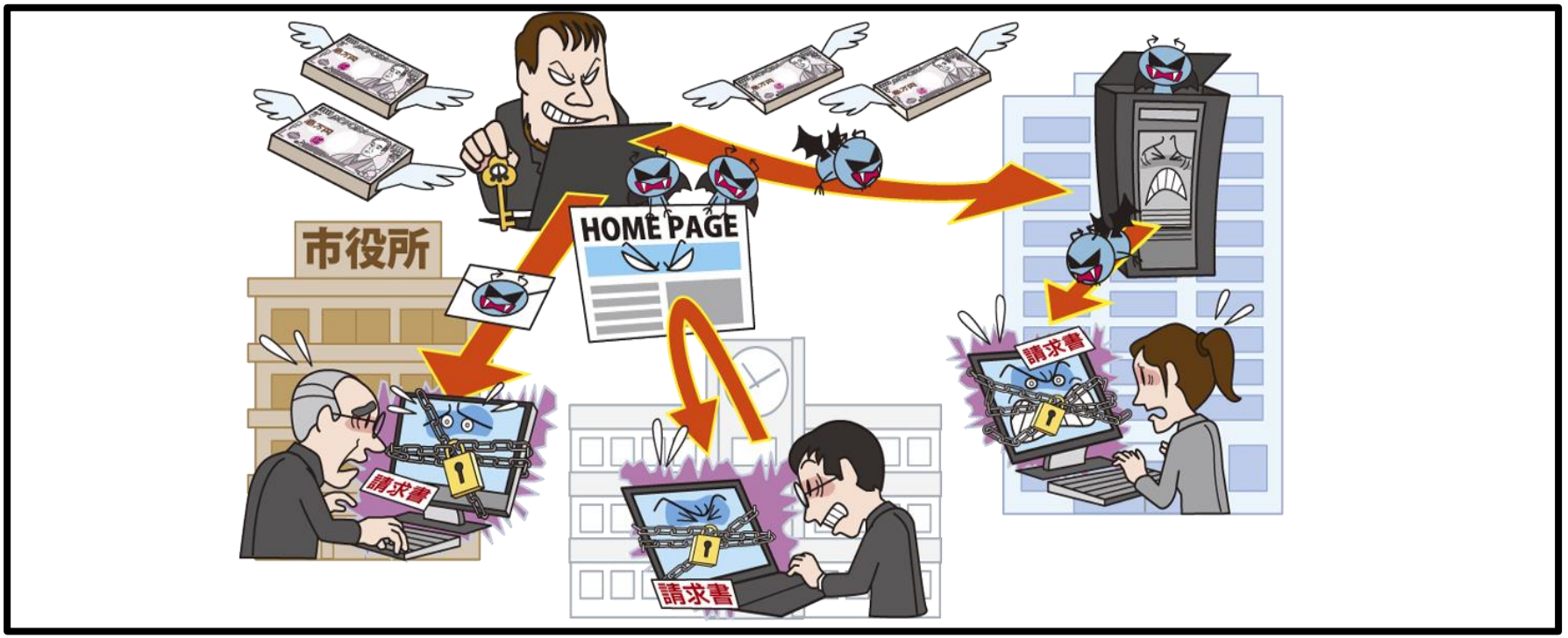
【参考資料】

※1 「サイバーセキュリティ経営ガイドライン」Ver2.0（経済産業省/IPA）
https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf

※2 「中小企業の情報セキュリティ対策ガイドライン」（IPA）
https://www.ipa.go.jp/files/000055520.pdf

【5位】ランサムウェアによる被害

～ランサムウェアに感染しないための対策と感染時の対処を知る～



- 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

【5位】ランサムウェアによる被害

～ランサムウェアに感染しないための対策と感染時の対処を知る～

● 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

■ 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などで誘導

【5位】ランサムウェアによる被害

～ランサムウェアに感染しないための対策と感染時の対処を知る～

● 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

・OS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）

【5位】ランサムウェアによる被害

～ランサムウェアに感染しないための対策と感染時の対処を知る～

- 2019年の事例/傾向
  - 市立高等学校のサーバーがランサムウェアに感染 (※1)
    - ・同校職員がネットワークサーバーにアクセスするとWordドキュメントが暗号化されていた
    - ・画面上には感染を示唆する英文の脅迫ドキュメント
    - ・生徒が作成した成果物等のデータが使用不可に
    - ・感染の原因は不明

【出典】
※1 市立高校の校内サーバがランサムウェアに感染(川崎市)
http://www.city.kawasaki.jp/templates/press/cmsfiles/contents/0000111/111987/20191101houdou.pdf

【5位】ランサムウェアによる被害

～ランサムウェアに感染しないための対策と感染時の対処を知る～

- 2019年の事例/傾向
  - 日本を標的としたランサムウェア攻撃(※1)
    - ・ランサムウェア「Gandcrab」等に感染させようとする攻撃メールが日本を標的にばらまかれた
    - ・メール件名には日本の女性芸能人名が使われていた
    - ・2019年1月29日、本攻撃の95%は日本で検出

【出典】
※1 「Love you(ラブ・ユー)」マルウェア、日本を標的にした大規模な攻撃を展開
https://www.eset.com/jp/blog/welivesecurity/love-you-malspam-makeover-massive-japan-targeted-campaign/

【5位】ランサムウェアによる被害

～ランサムウェアに感染しないための対策と感染時の対処を知る～

- 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

【5位】ランサムウェアによる被害

～ランサムウェアに感染しないための対策と感染時の対処を知る～

- 対策
  - システム管理者、従業員
    - ・被害の予防
      - －受信メール、ウェブサイトの十分な確認
      - －添付ファイルやリンクを安易にクリックしない
      - －不審なソフトウェアを実行しない
      - －サポートの切れたOSの利用停止、移行
      - －フィルタリングツール（メール、ウェブ）の活用
      - －ネットワーク分離
      - －共有サーバー等へのアクセス権の最小化
      - －バックアップの取得

【5位】ランサムウェアによる被害

～ランサムウェアに感染しないための対策と感染時の対処を知る～

- 対策
  - システム管理者、従業員

・被害を受けた後の対応

－CSIRTへ連絡

－バックアップからの復旧

－復号ツールの活用

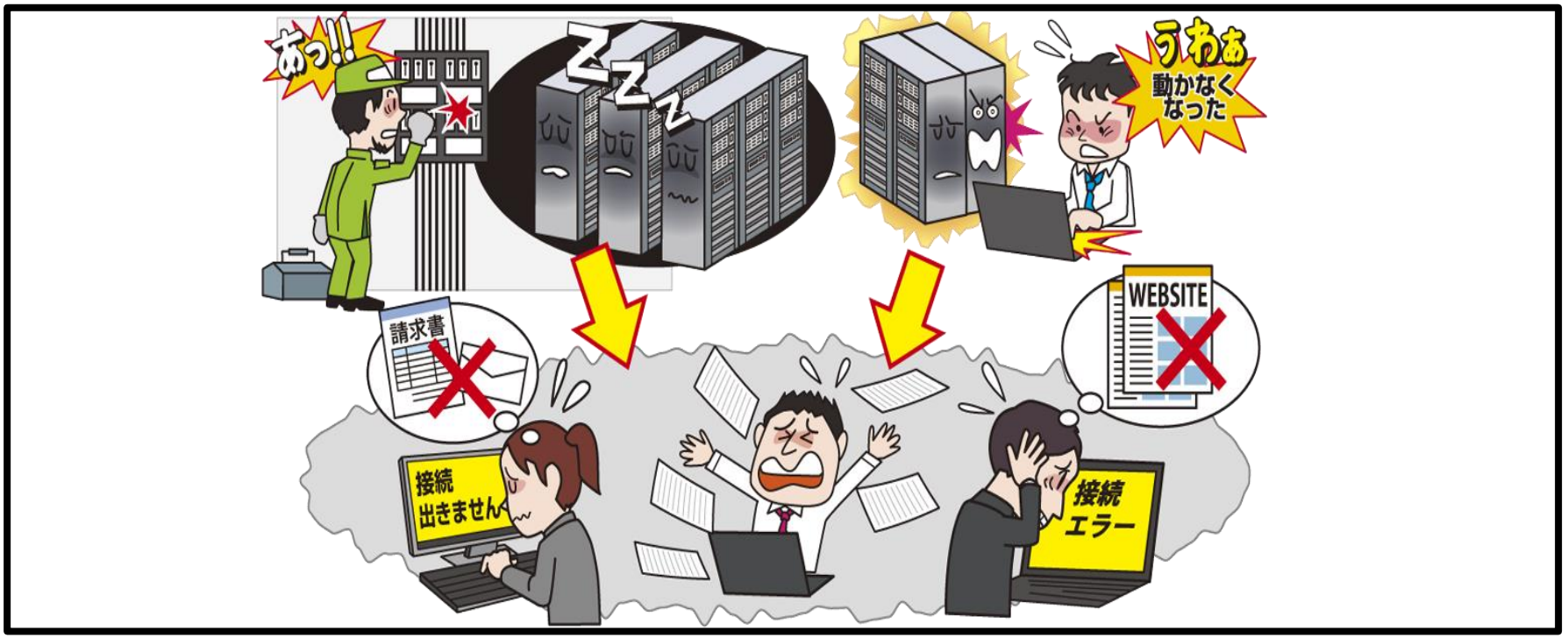
－影響調査および原因の追究、対策の強化

＜例外措置＞

推奨はされないが、人命に関わるファイルが暗号化された場合に、金銭を支払ったケースもある

【6位】予期せぬIT基盤の障害に伴う業務停止

～それは予告もなしに突然やってくる～



- 利用しているデータセンターやクラウドのIT基盤などが停止
- 業務が停止することで利益減少など経済的損失につながる

【6位】予期せぬIT基盤の障害に伴う業務停止

～それは予告もなしに突然やってくる～

● 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作業中の人為的ミス等

■ 設備障害

・電源、空調設備等の制御システムの障害

【6位】予期せぬIT基盤の障害に伴う業務停止
～それは予告もなしに突然やってくる～

- 2019年の事例/傾向
  - 自治体向けIaaSサービスでシステム障害 (※1,※2)
    - ・自治体用IaaS「Jip-Base」で障害が発生
    - ・全国約50の自治体が影響を受けた
    - ・住民向けの窓口サービスや自治体の業務システムに支障
    - ・復旧に長い時間を要した

【出典】
※1 「Jip-Base」の障害における復旧状況のご報告(第3報)
https://www.jip.co.jp/news/20200110/
※2 全国約50の自治体でWeb/電子行政サービスがダウン、自治体専用IaaS「Jip-Base」でシステム障害
https://it.impressbm.co.jp/articles/-/18969

【6位】予期せぬIT基盤の障害に伴う業務停止
～それは予告もなしに突然やってくる～

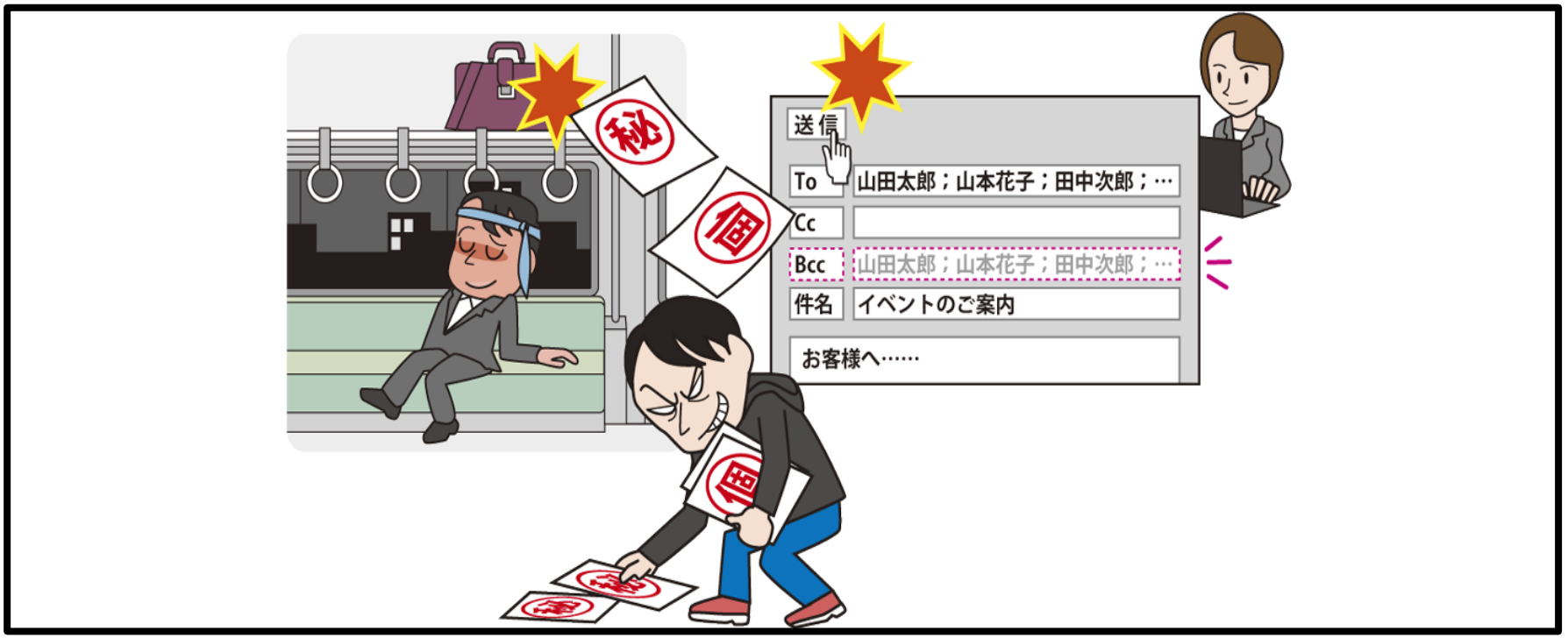
- 2019年の事例/傾向
  - データセンターの電源障害によるシステム停止(※1,※2)
    - ・電源設備のメンテナンス作業事故で電源が7秒間停止
    - ・約260社の顧客システムが利用できない状態に
    - ・クレジットカード決済やスマホ決済等の消費者向けサービスに影響が及んだ

【出典】
※1 データセンターの電源障害による停止について(障害お知らせ)
https://www.qtnet.co.jp/info/2019/20191126.html
※2 【完全復旧】お客様向けサービス復旧のお知らせ(株式会社QTnetの電源設備更新作業に伴う不具合)
https://www.rakuten-card.co.jp/info/news/20191123/

【6位】予期せぬIT基盤の障害に伴う業務停止
～それは予告もなしに突然やってくる～

- 対策
  - サービス提供者
    - ・被害の予防
      - -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
      - -被害を想定し、IT基盤側との事前の連携確認
    - ・被害を受けた後の対応
      - -BCPに従った対応

【7位】不注意による情報漏えい
～ついうっかり、が重大インシデントに～



- 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、漏えいした情報の悪用による二次被害

【7位】不注意による情報漏えい
～ついうっかり、が重大インシデントに～

● 要因

・個人の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

■ 取扱情報の重要性に対する認識不足からの不注意
- ・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

【7位】不注意による情報漏えい
～ついうっかり、が重大インシデントに～

- 2019年の事例/傾向
  - 顧客の個人情報が保存されたPCを紛失(※1)
    - ・飲食店運営企業の従業員が、同社が運営する店舗に予約をした顧客の個人情報が保存されたPCを紛失
    - ・帰宅途中に立ち寄った店に置き忘れ
    - ・PCには顧客の氏名、企業名、電話番号が最大67,280件
    - ・紛失判明後に遠隔操作でPCのログインパスワードを複雑化した上で警察へ届け出

【出典】
※1 ノートパソコン遺失による個人情報漏洩の可能性に関するお詫びとお知らせ
http://www.zetton.co.jp/company/IR/docs/ir_20190906.pdf

【7位】不注意による情報漏えい
～ついうっかり、が重大インシデントに～

- 2019年の事例/傾向
  - BCCをTOにしてメール送信 (※1)
    - 説明会のリマインドメールを送信する際にBCC欄に入れるべき参加申込者のメールアドレスを誤ってTO欄に
    - メール受信者が他の参加申込者のメールアドレスを見られる状態に
    - メールを送信した申込者全員へ謝罪と当該メールの削除依頼

【出典】
※1　特許庁の請負事業における個人情報の流出について
https://www.meti.go.jp/press/2018/01/20190123005/20190123005.html

【7位】不注意による情報漏えい
～ついうっかり、が重大インシデントに～

- 対策
  - 経営者、管理者、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
    - ・被害の予防
      - －確認プロセスに基づく運用
      - －情報の保護（暗号化、アクセス制限）
      - －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

【7位】不注意による情報漏えい
～ついうっかり、が重大インシデントに～

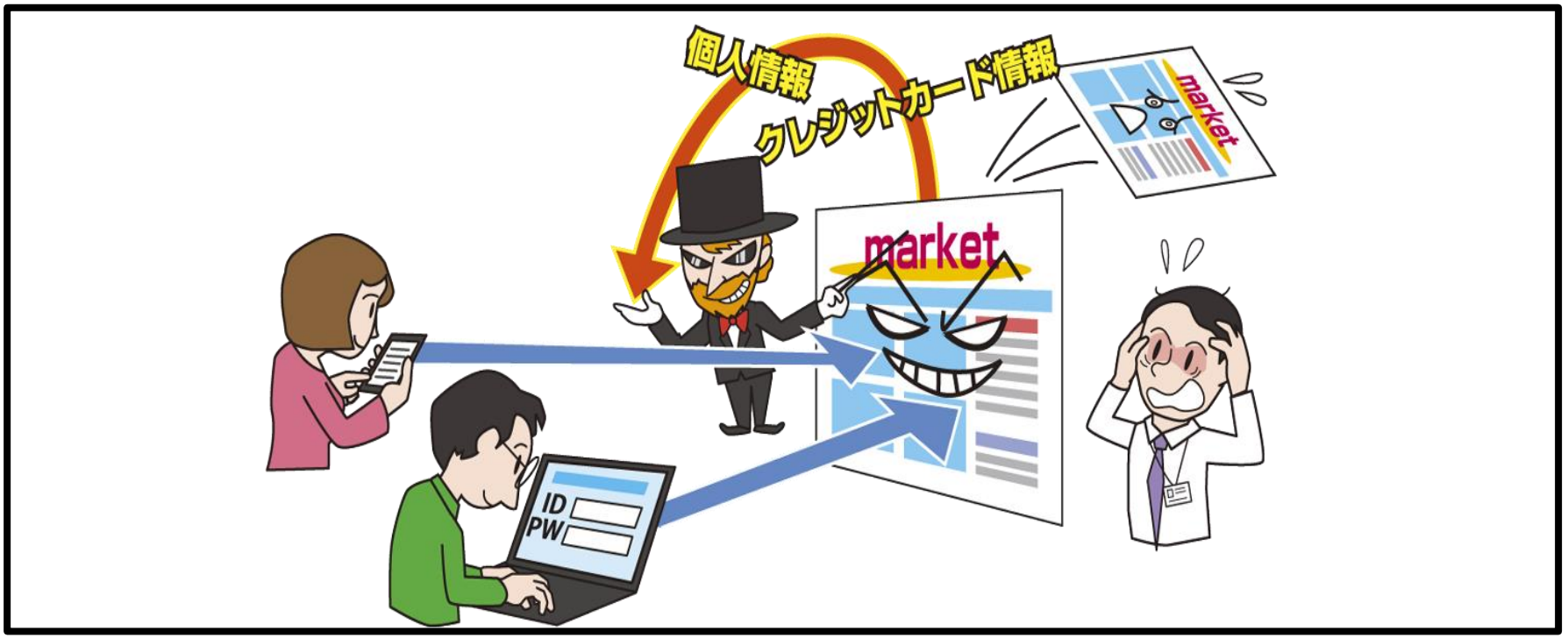
- **対策**
  - ・被害の早期検知
    - –問題発生時の内部報告体制の整備
    - –外部からの連絡窓口の設置
  - ・被害を受けた後の対応
    - –被害拡大や二次被害の要因の削除
    - –漏えいした内容や発生原因の公表
    - –関係者、関係機関への連絡
      監督官庁、個人情報保護委員会等

【7位】不注意による情報漏えい
～ついうっかり、が重大インシデントに～

- 対策
  - 被害者（情報漏えいされた人）
    - ・被害を受けた後の対応
      - －漏えいが発生した組織からの情報に従う
        - ※パスワードの変更、クレジットカードの再発行等

【8位】インターネット上のサービスからの個人情報の窃取

～他人事ではないウェブサイトの脆弱性～



- インターネット上のサービスが脆弱性を悪用された攻撃や不正ログインの被害を受け個人情報が漏えいする
- 窃取された情報を不正利用される

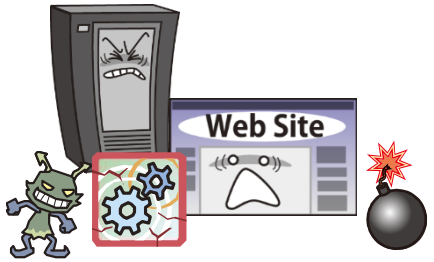
【8位】インターネット上のサービスからの個人情報の窃取

～他人事ではないウェブサイトの脆弱性～

- **攻撃手口**

・広く共通的に使われるソフトウェアの脆弱性を悪用

- **サーバーのソフトウェアの脆弱性を悪用**
  - ・サーバーで稼働するOS、ミドルウェア、CMS等の複数のソフトウェアの脆弱性を悪用
- **ウェブアプリケーションの脆弱性を悪用**
  - ・インターネットサービスで稼働しているウェブアプリケーションの脆弱性を悪用
    （SQLインジェクション攻撃、フォームジャッキングなど）



【8位】インターネット上のサービスからの個人情報の窃取

～他人事ではないウェブサイトの脆弱性～

- 2019年の事例/傾向
  - 決済用モジュールの改ざんによる情報漏えい(※1)
    - ・通販サイトの脆弱性が悪用され決済用モジュールが改ざんされた
    - ・決済のためにクレジットカード情報を入力した顧客34人分の情報が漏えい

【出典】
※1　弊社が運営する「掃除用品オンラインショップ」への不正アクセスによる個人情報流出に関するお詫びとお知らせ
https://clean-shop.ec-cube.shop/user_data/news2019

【8位】インターネット上のサービスからの個人情報の窃取

～他人事ではないウェブサイトの脆弱性～

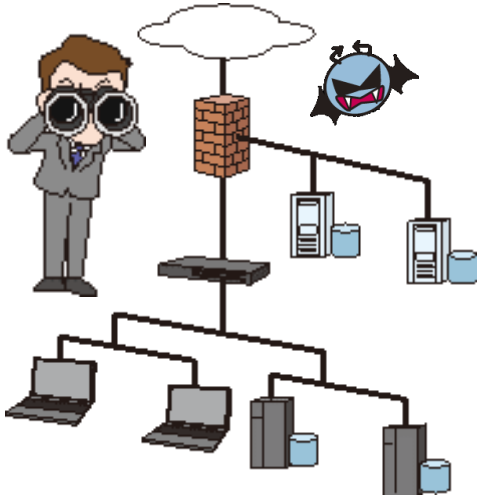
- 2019年の事例/傾向
  - ファイル転送サービスへの不正アクセス(※1,※2)
    - ・サーバーの脆弱性を悪用され不正アクセスされた
    - ・480万件以上の個人情報が漏えい
    - ・脆弱性修正のためには大規模な改修が必要となるため、サービス終了を決定した

【出典】
※1 「宅ふぁいる便」サービスにおける不正アクセスについて　～お客さま情報の漏洩について(お詫びとご報告)～
https://www.filesend.to/news20190314.html
※2 「宅ふぁいる便」サービス終了のお知らせ(2020年1月14日)
https://www.filesend.to/

【8位】インターネット上のサービスからの個人情報の窃取

～他人事ではないウェブサイトの脆弱性～

- **対策**
  - **インターネット上のサービス運営者等**



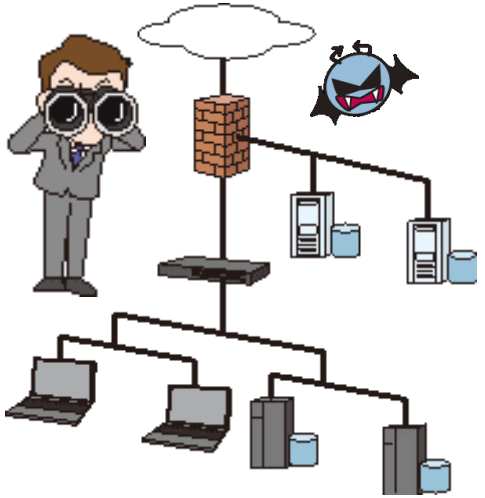
・被害の予防

- -セキュリティ対策の予算・体制の確保
- -セキュアなインターネット上のサービス構築
- -セキュア開発ライフサイクルの実践
- -セキュリティバイデザインの実施
- -セキュリティ診断の実施
  （Webアプリケーション診断やプラットフォーム診断等）
- -WAF、IDS/IPSの導入
- -利用者に対するセキュリティ機能の提供
  二要素認証やログイン履歴、購入履歴を確認できる機能などを提供
- -ミドルウェアやライブラリ利用状況の把握

【8位】インターネット上のサービスからの個人情報の窃取

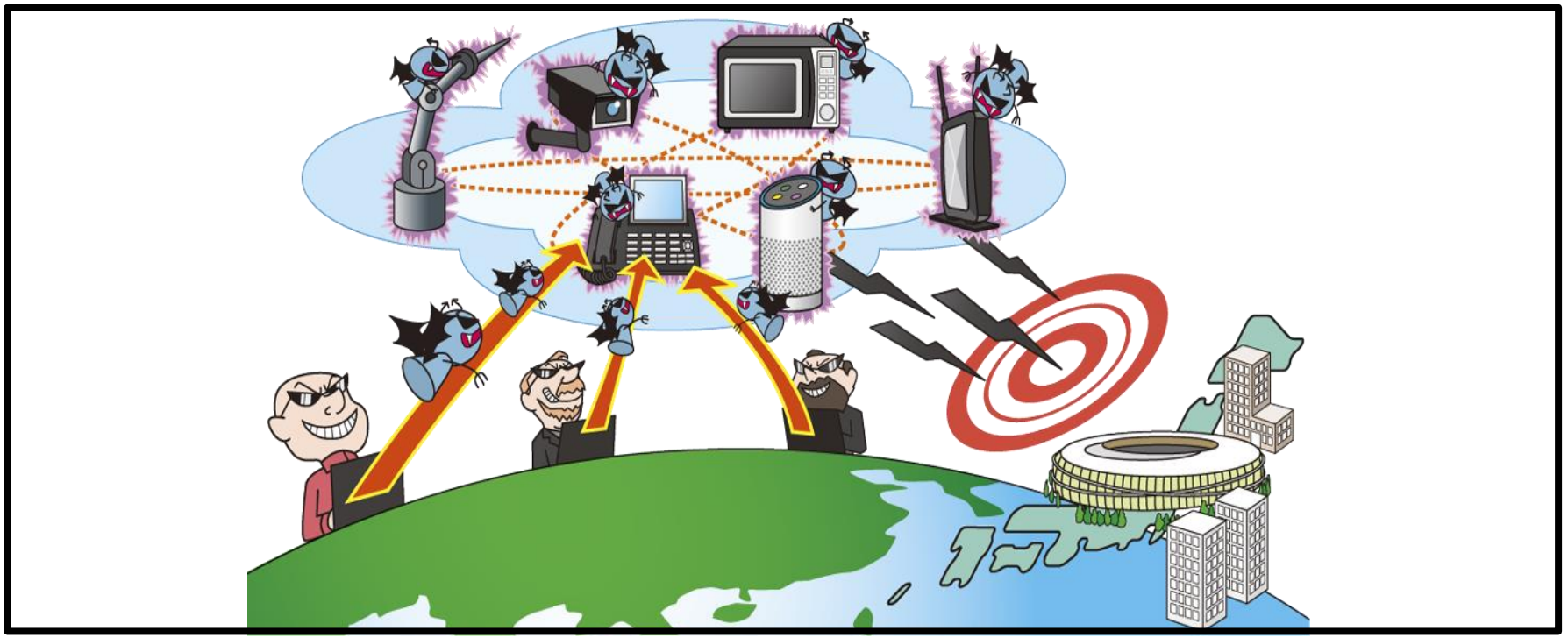
～他人事ではないウェブサイトの脆弱性～

- 対策
  - インターネット上のサービス運営者等
    - ・被害の早期検知
      - －適切なログと継続的な監視
    - ・被害を受けた後の対応
      - －CSIRTへの連絡
      - －セキュリティ専門企業への調査依頼
      - －影響調査および原因の追究、対策の強化
      - －情報漏えいの被害者に対するすみやかな連絡と補償
      - －漏えいした内容や発生原因等の公表
      - －関係者、関係機関への連絡
        監督官庁、個人情報保護委員会、警察等



【9位】IoT機器の不正利用

～IoT機器の普及に伴い脆弱性を悪用する攻撃が多様化、開発ベンダーは対策が急務～



- IoT機器の脆弱性が悪用され乗っ取られる
- 機能を不正に利用される等、業務に支障がでるおそれ
- DDoS攻撃の踏み台等に利用される

【9位】IoT機器の不正利用

～IoT機器の普及に伴い脆弱性を悪用する攻撃が多様化、開発ベンダーは対策が急務～

IPA

● 攻撃手口

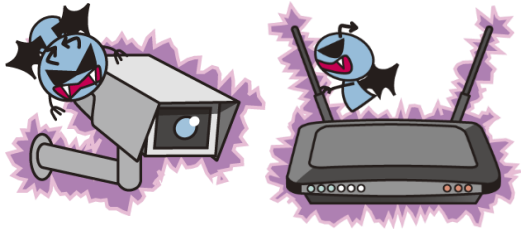
・IoT機器は当然ながらインターネットに接続している
・脆弱性があると不正アクセスやウイルスの被害に

■ 脆弱性を悪用した攻撃

・IoT機器が持つ脆弱性を悪用し、不正アクセスしたりウイルスに感染させたりする

■ インターネット上でウイルスが感染活動を行う

・同じ脆弱性を持つIoT機器がインターネット上にないか探索し、脆弱性があればそのIoT機器もウイルスに感染させる



【9位】IoT機器の不正利用

～IoT機器の普及に伴い脆弱性を悪用する攻撃が多様化、開発ベンダーは対策が急務～

IPA

2019年の事例/傾向

総務省が基準認証に関するガイドラインを公開（※1）

- 「電気通信事業法に基づく端末機器の基準認証に関するガイドライン」が公開された
- IoT機器の技術基準にセキュリティ対策を追加するため、「端末設備等規則」の一部を改正（2020年4月1日施行）
- IoT機器メーカーやサービス提供者は今後本規則に準じたセキュリティ対策が求められる

【出典】
※1　電気通信事業法に基づく端末機器の基準認証に関するガイドライン（第1版）
https://www.soumu.go.jp/menu_news/s-news/01kiban05_02000179.html

【9位】IoT機器の不正利用

～IoT機器の普及に伴い脆弱性を悪用する攻撃が多様化、開発ベンダーは対策が急務～

IPA

● 2019年の事例/傾向

■ 脆弱なIoT機器についての調査結果を発表(※1)

・総務省および情報通信研究機構が、サイバー攻撃に悪用されるおそれのあるIoT機器の調査「NOTICE」を実施

・調査対象IPアドレス約1.1億の内、ID・パスワードが入力可能であったのが約111,000件、さらにログイン可能であったのが1,328件であった　[2019年度第3四半期の調査結果]

・ウイルスに感染したIoT機器の1日あたりの検知数は少ないときは60件、多いときで598件であった

【出典】

※1　脆弱なIoT機器及びマルウェアに感染しているIoT機器の利用者への注意喚起の実施状況（2019年度第3四半期）
https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00058.html

【9位】IoT機器の不正利用

～IoT機器の普及に伴い脆弱性を悪用する攻撃が多様化、開発ベンダーは対策が急務～

IPA

● 対策

■ IoT機器の開発者

・被害の予防

- セキュア開発ライフサイクルの実践
- セキュリティバイデザインの実施
- 初期パスワード変更の強制化
- 脆弱性の解消（セキュアプログラミング、脆弱性検査、ファジング等）
- ソフトウェア更新の自動化
- わかりやすい取扱説明書の作成（適切な管理の呼びかけ）
- 迅速なセキュリティパッチの提供
- 利用者にとって不要な機能の無効化
- セキュリティに配慮したデフォルト設定
- ソフトウェアサポート期間の明確化

【9位】IoT機器の不正利用

～IoT機器の普及に伴い脆弱性を悪用する攻撃が多様化、開発ベンダーは対策が急務～

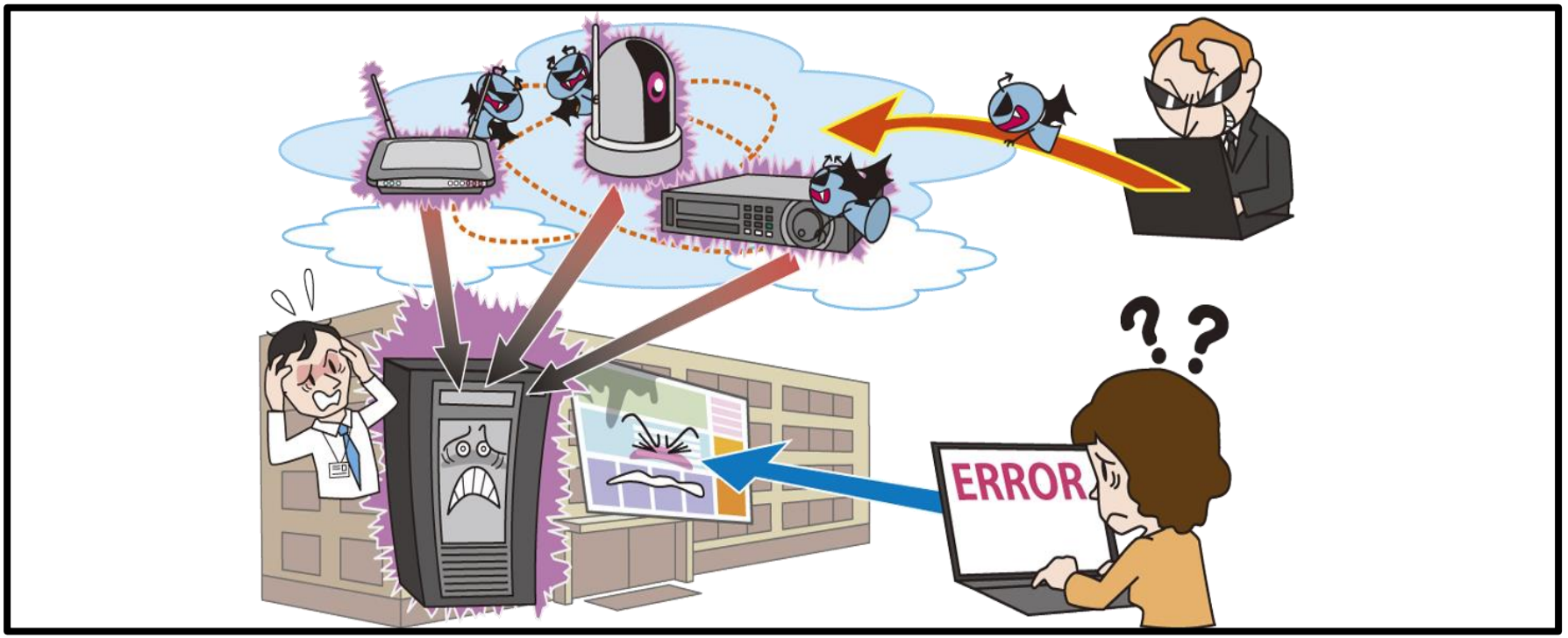
対策

組織のシステム管理者・利用者、個人

- ・情報リテラシーの向上
  - －使用前に説明書を確認
- ・被害の予防
  - －セキュリティパッチが公開されたら迅速に更新
    （自動更新機能の有効化等）
  - －機器の管理画面や管理ポートに対する適切なアクセス制限
  - －廃棄時は初期化
- ・被害を受けた後の対応
  - －CSIRTへの連絡
  - －IoT機器の電源オフ
  - －IoT機器の初期化後、上記「被害の予防」を実施
  - －影響調査および原因の追究、対策の強化

【10位】サービス妨害攻撃によるサービスの停止

～DDoS攻撃の被害に遭わないために事前準備を強化する～



- 標的組織のサーバー等に大量の通信による高負荷をかける
- 高負荷をかけられたサーバーは処理遅延やサービス停止
- サービス停止による機会損失、信用失墜等の被害

【10位】サービス妨害攻撃によるサービスの停止

～DDoS攻撃の被害に遭わないために事前準備を強化する～

● 攻撃手口

・サーバーに大量の処理要求を送信し高負荷状態に

■ ボットネットを利用したDDoS攻撃

・ウイルス感染させた端末等からボットネットを形成し、DDoS攻撃に利用する

■ リフレクション攻撃

・送信元のIPアドレスを標的組織のサーバーに偽装したパケットを多数のDNSサーバーやNTPサーバー等に送信する

■ DDoS代行サービスの利用

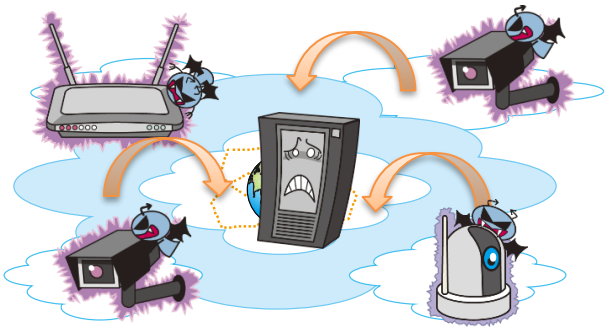
・ダークウェブ等にあるDDoS代行サービスを利用

・専門的な技術が無くても比較的容易に攻撃を行える

【10位】サービス妨害攻撃によるサービスの停止

～DDoS攻撃の被害に遭わないために事前準備を強化する～

- 2019年の事例/傾向
  - マンション向けプロバイダーで通信障害（※1）
    - 2019年10月2日から21日にかけてDDoS攻撃を受け、一部マンションにて断続的に通信の異常が発生
    - 時間経過とともに攻撃元IPアドレスが変化し、被害が長期化
    - 再発防止に向け共有部設置機器の順次交換や攻撃自体への対策も継続して行う

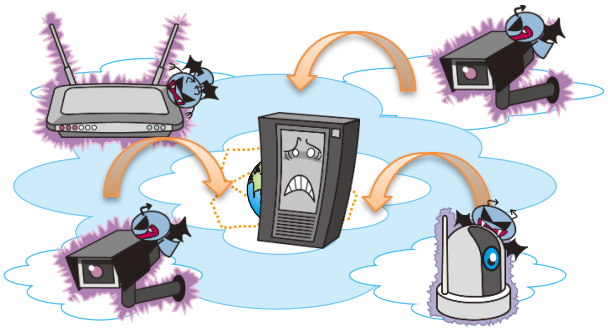


【出典】
※1 インターネット通信障害のお知らせ
http://www.fiberbit.net/news/info/2091/

【10位】サービス妨害攻撃によるサービスの停止

～DDoS攻撃の被害に遭わないために事前準備を強化する～

- 2019年の事例/傾向
  - DDoS攻撃脅迫メールで、仮想通貨を要求 (※1)
    - 複数の組織を対象にDDoS攻撃を示唆して仮想通貨を要求する脅迫メールが送付されていると観測
    - 攻撃手法はDNS、NTP、CLDAPを使用したリフレクション攻撃
    - JPCERT/CCは日本国内でも同様の事例を確認

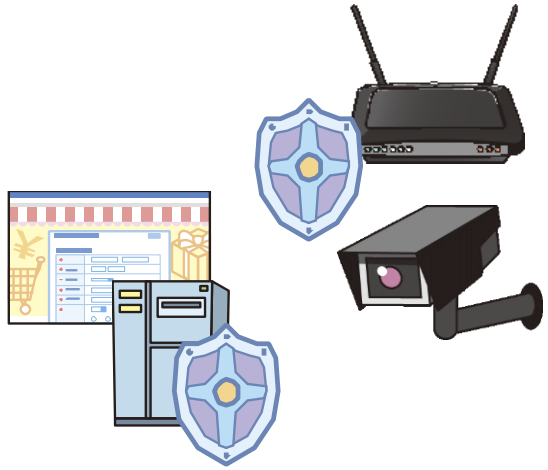


【出典】
※1 DDoS 攻撃を示唆して、仮想通貨を要求する脅迫メールについて
https://www.jpcert.or.jp/newsflash/2019103001.html

【10位】サービス妨害攻撃によるサービスの停止

～DDoS攻撃の被害に遭わないために事前準備を強化する～

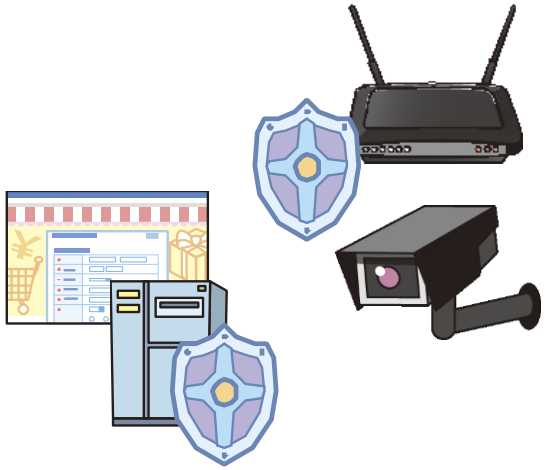
- 対策
  - ウェブサイトの運営者
    - ・被害の予防
      - -DDoS攻撃の影響を緩和するISPやCDN等の利用
      - -システムの冗長化等の軽減策
      - -ネットワークの冗長化
      - -ウェブサイト停止時の代替サーバーの用意や告知手段の整備
    - ・被害を受けた後の対応
      - -CSIRTへの連絡
      - -通信制御
        （攻撃元IPアドレスからの通信遮断等）
      - -サービス利用者への状況の告知
      - -影響調査および原因の追究、対策の強化



【10位】サービス妨害攻撃によるサービスの停止

～DDoS攻撃の被害に遭わないために事前準備を強化する～

- **対策**
  - **サービス事業者**
    - ・被害の予防
      - -公開サーバーの設定の見直し
        DNSサーバーやNTPサーバー等
      - -IoT機器の脆弱性対策
        ボットネットとして攻撃の踏み台にされないために
        IoT機器のセキュリティ対策を強化



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　2020

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/10threats2020.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