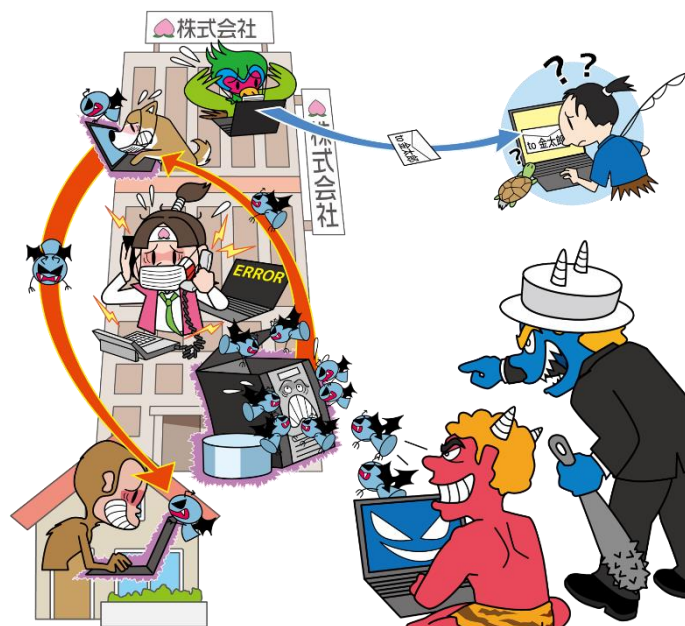


情報セキュリティ10大脅威 2021

～よもや自組織が被害に！呼吸を合わせて全力防御！～

[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
2021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**

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 2021 脅威ランキング



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

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

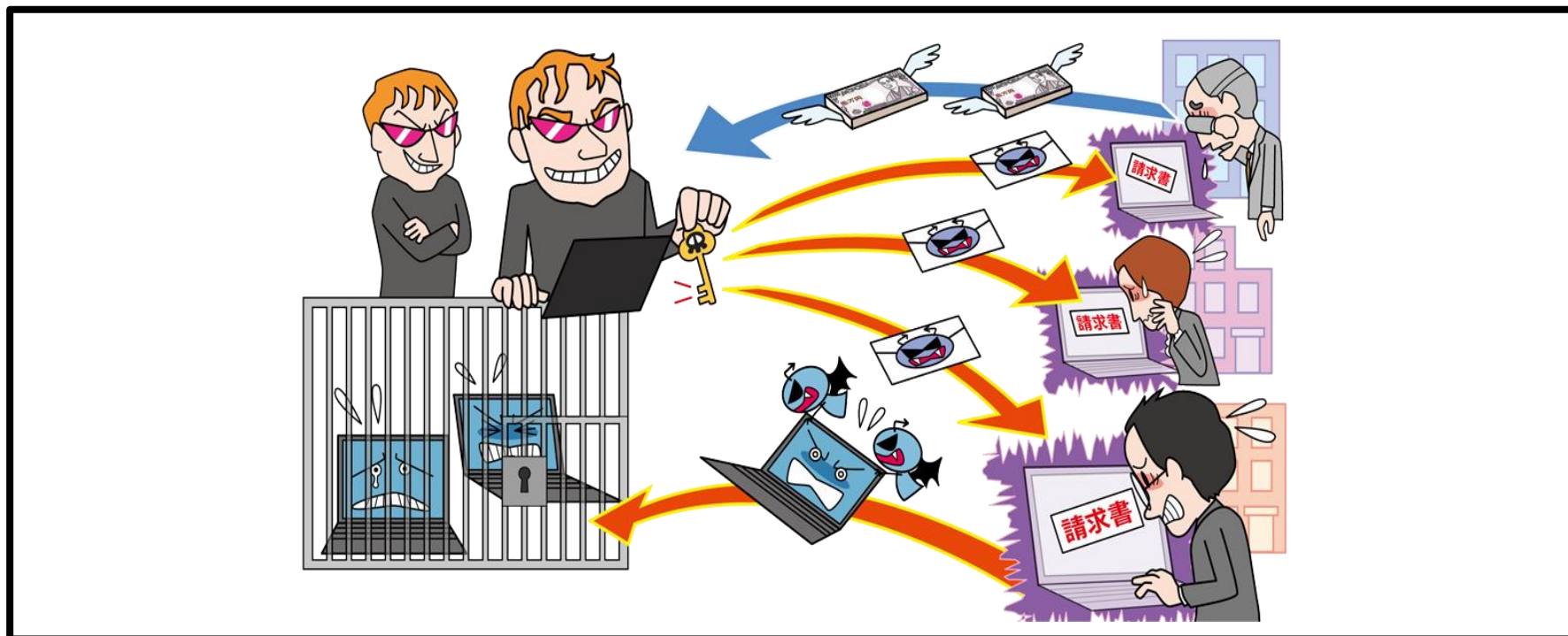
情報セキュリティ10大脅威 2021

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

～組織を狙ったランサムウェアの攻撃が増加～



- 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

～組織を狙ったランサムウェアの攻撃が増加～

● 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変更
- ・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

～組織を狙ったランサムウェアの攻撃が増加～

● 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)



【1位】ランサムウェアによる被害

～組織を狙ったランサムウェアの攻撃が増加～

● 2020年の事例／傾向①

■ ゲームメーカーのサーバーがランサムウェアに感染 (※1)

- ・ゲームメーカーの社内システムにおいてデータが暗号化され、メールやファイルが使えなくなる等の業務一時停止
- ・顧客や株主情報等を暴露すると脅迫
- ・暗号化解除と暴露の取り止めを条件に身代金を要求

【出典】

※1 暗号化と暴露で11億円を要求、カプコン襲った「二重脅迫型」ランサムウェアの脅威

<https://xtech.nikkei.com/atcl/nxt/column/18/00989/112400040/>

【1位】ランサムウェアによる被害

～組織を狙ったランサムウェアの攻撃が増加～

● 2020年の事例／傾向②

■ 特定の組織に特化したランサムウェア (※1)

- ・自動車メーカーがサイバー攻撃から大規模システム障害
- ・国内外の工場で出荷が一時停止
- ・従業員のPCが使えなくなる等オフィス系ネットワークシステムにも影響

【出典】

※1 ホンダを標的に開発か、ランサムウェア「EKANS」解析で見えた新たな脅威

<https://xtech.nikkei.com/atcl/nxt/column/18/00989/062400028/>

【1位】ランサムウェアによる被害

～組織を狙ったランサムウェアの攻撃が増加～

● 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



【1位】ランサムウェアによる被害

～組織を狙ったランサムウェアの攻撃が増加～

● 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
- サポートの切れたOSの利用停止、移行
- アプリケーション許可リストの整備
- フィルタリングツール(メール、ウェブ)の活用
- ネットワーク分離
- 共有サーバー等へのアクセス権の最小化と管理の強化
- 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

- 標的型攻撃対策相当の全般的なセキュリティ対策が必要**



【1位】ランサムウェアによる被害

～組織を狙ったランサムウェアの攻撃が増加～

● 対策

■ システム管理者、従業員

・被害を受けた後の対応

- CSIRT等所定の連絡先への連絡
- バックアップからの復旧
- 復号ツールの活用
- 影響調査および原因の追究、対策の強化
- 迅速な隔離を行い、関連組織、取引先への被害拡大の防止

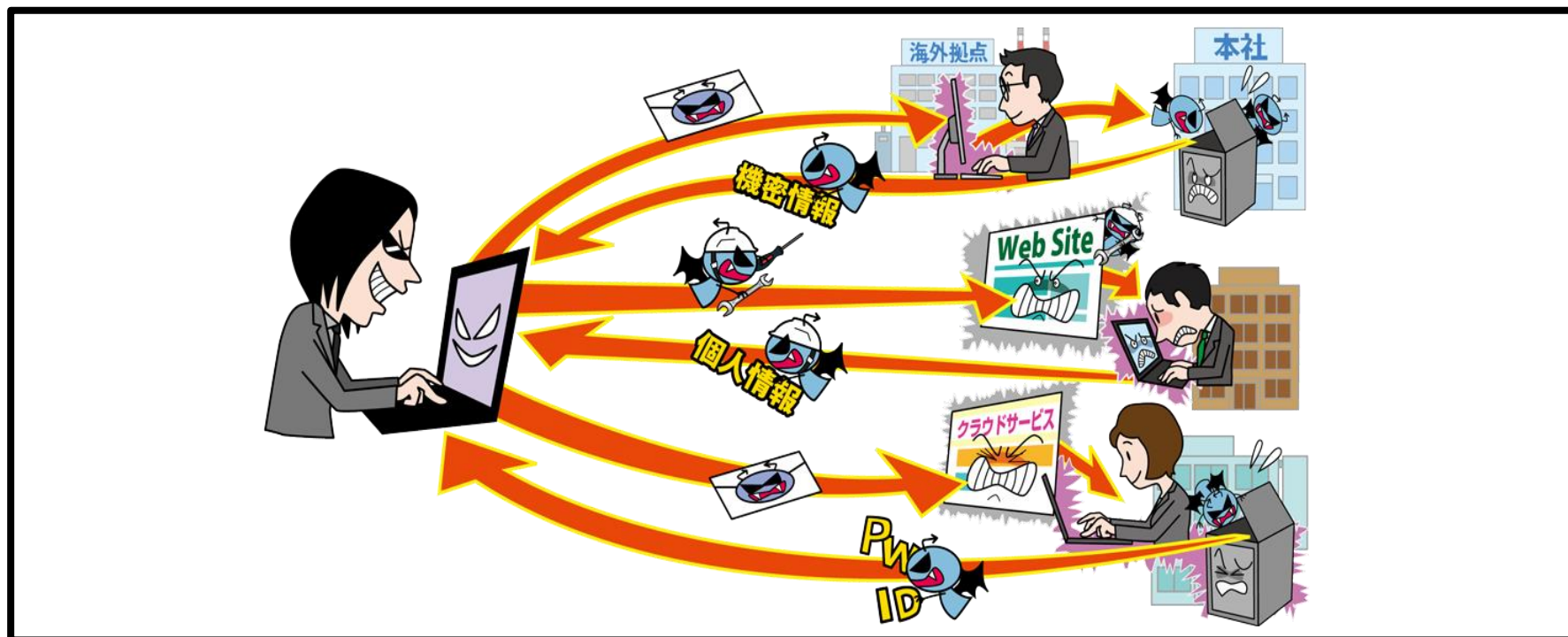
＜例外措置＞

推奨はされないが金銭を支払う(暗号化されたファイルが人命に関わる場合等)



【2位】標的型攻撃による機密情報の窃取

～新型コロナウイルスの影響に便乗した標的型攻撃メールを観測～



- 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

～新型コロナウイルスの影響に便乗した標的型攻撃メールを観測～

● 攻撃手口

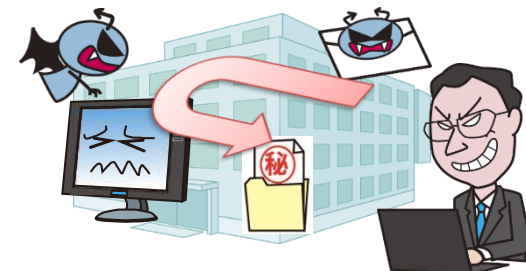
・メールやウェブサイトからウイルスに感染させる

■ 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

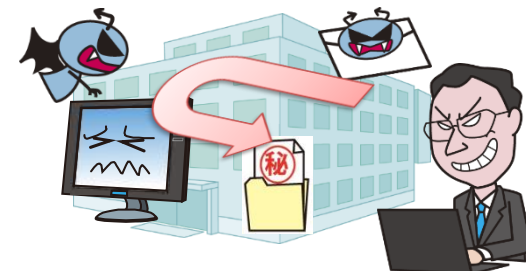
～新型コロナウイルスの影響に便乗した標的型攻撃メールを観測～

● 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

～新型コロナウイルスの影響に便乗した標的型攻撃メールを観測～

● 2020年の事例／傾向①

■ 標的型攻撃と思われる複数の不正アクセス報道 (※1,※2)

[電機メーカー]

- ・防衛事業部門のサーバーが不正アクセスされた
- ・27,445件のファイルが不正にアクセスされた
- ・2016年12月以降に攻撃を受けていたが検知できていなかった

[重工業メーカー]

- ・複数の海外拠点と国内拠点間で不審な通信を確認し発覚
- ・攻撃は痕跡を残さない高度なものだった

【出典】

※1 当社の社内サーバへの不正アクセスについて

https://jpn.nec.com/press/202001/20200131_01.html

※2 当社グループへの不正アクセスについて

https://www.khi.co.jp/pressrelease/news_201228-1j.pdf

【2位】標的型攻撃による機密情報の窃取

～新型コロナウイルスの影響に便乗した標的型攻撃メールを観測～

● 2020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

[2020年10月～12月]

サイバー攻撃に関する情報提供 - 479件

※その中で標的型攻撃メールとみなした情報 - 16件

[2020年11月]

ウイルスが添付された日本語の不審メールに関する情報提供

※ZIPファイル添付、Excelのアイコンに偽装されたEXEファイル

【出典】

※1 サイバー情報共有イニシアティブ(J-CSIP) 運用状況 [2020 年 10 月～12 月]

<https://www.ipa.go.jp/files/000088288.pdf>

【2位】標的型攻撃による機密情報の窃取

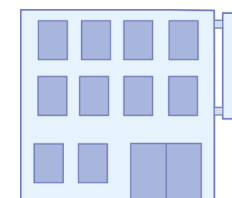
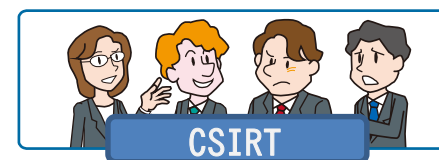
～新型コロナウイルスの影響に便乗した標的型攻撃メールを観測～

● 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



【2位】標的型攻撃による機密情報の窃取

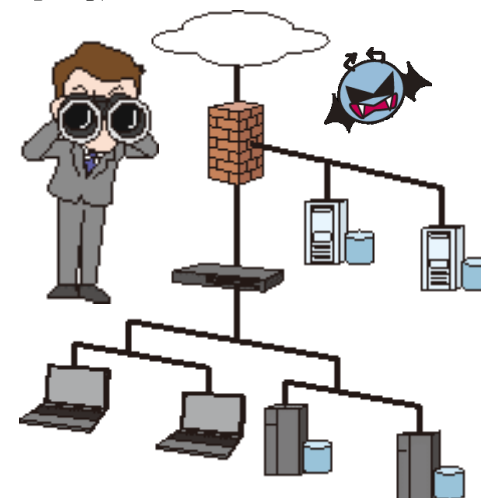
～新型コロナウイルスの影響に便乗した標的型攻撃メールを観測～

● 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
- アクセス権の最小化と管理の強化
- ネットワーク分離
- 重要サーバーの要塞化(アクセス制御、暗号化等)
- 海外拠点等も含めたセキュリティ対策の向上



【2位】標的型攻撃による機密情報の窃取

～新型コロナウイルスの影響に便乗した標的型攻撃メールを観測～

● 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等の導入

－エンドポイントの監視・防御

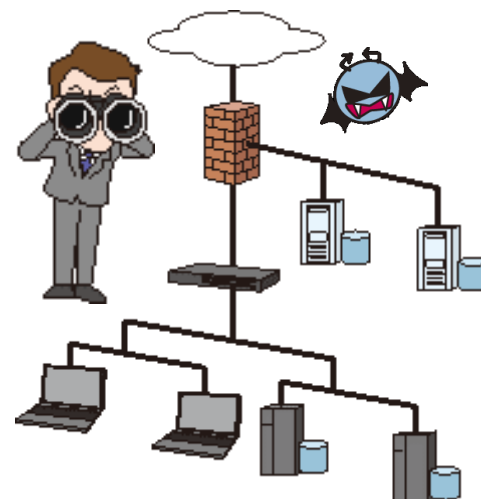
・被害を受けた後の対応

－CSIRTの運用によるインシデント対応

－影響調査および原因の追究、対策の強化

－関係者、関係機関への連絡

監督官庁、個人情報保護委員会、警察等



【2位】標的型攻撃による機密情報の窃取

～新型コロナウイルスの影響に便乗した標的型攻撃メールを観測～

● 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」

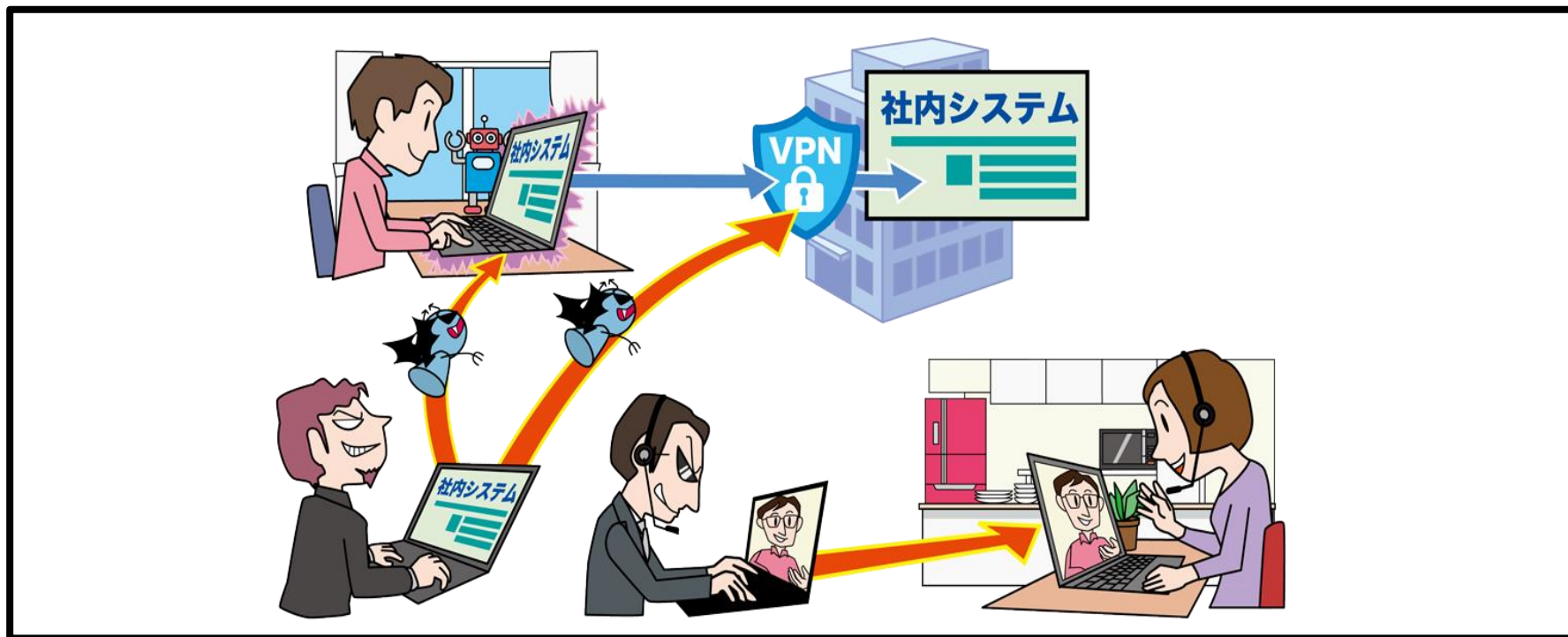
「被害を受けた際は迅速に連絡」

・被害を受けた後の対応

－CSIRT等所定の連絡先への連絡

【3位】テレワーク等のニューノーマルな働き方を狙った攻撃

～テレワーク環境を意識した対策を～



- 2020年はコロナ禍の影響によりテレワークへの移行が増加
- ウェブ会議サービスやVPNの本格的な活用の始まりに伴い、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

【3位】テレワーク等のニューノーマルな働き方を狙った攻撃

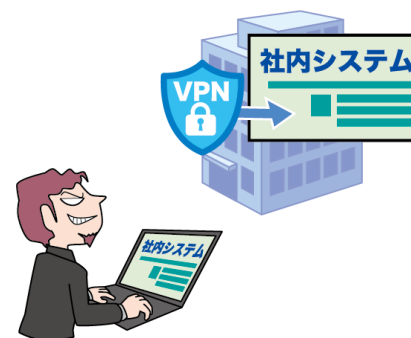
～テレワーク環境を意識した対策を～

● 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

※ 私物PCからの情報漏えいのおそれ



【3位】テレワーク等のニューノーマルな働き方を狙った攻撃

～テレワーク環境を意識した対策を～

● 2020年の事例／傾向①

■ 脆弱性の悪用によりVPNのパスワード流出 (※1)

- ・2020年8月、VPN製品の脆弱性が悪用されて窃取された認証情報、約900件がインターネット上で公開されていた
- ・悪用された脆弱性やその対策に関する情報は2019年4月に公開済みだった
- ・更新プログラムを適用していないVPN製品が狙われた

【出典】

※1 VPN認証情報漏洩に見る脆弱性対策を浸透させる難しさ

<https://www.security-next.com/117811>

【3位】テレワーク等のニューノーマルな働き方を狙った攻撃

～テレワーク環境を意識した対策を～

● 2020年の事例／傾向②

■ テレワーク中にウイルス感染、社内に拡大^(※1)

- ・社有PCにて在宅勤務
- ・社内ネットワークを経由せずに外部ネットワークに接続
- ・SNSを利用した際に**ウイルスに感染**
- ・当該従業員が出社した際に当該PCを社内ネットワークに接続
- ・**社内ネットワークにウイルス感染が拡大**

【出典】

※1 在宅勤務時 SNS経由で社用PCが感染、社内ネットワーク接続で被害拡大(三菱重工業)

<https://scan.netsecurity.ne.jp/article/2020/08/14/44439.html>

【3位】テレワーク等のニューノーマルな働き方を狙った攻撃

～テレワーク環境を意識した対策を～

● 対策

■ 組織(テレワーカー)

・情報リテラシーや情報モラルの向上

－セキュリティ教育の受講

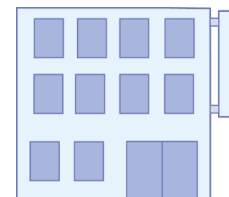
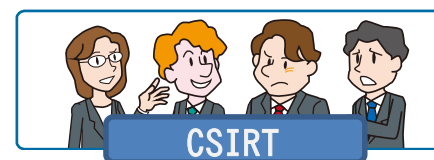
・被害の予防

－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

－CSIRT等所定の連絡先への連絡



【3位】テレワーク等のニューノーマルな働き方を狙った攻撃

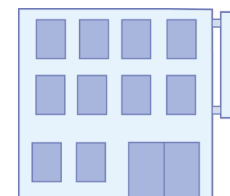
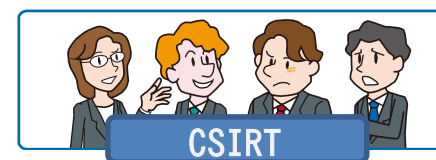
～テレワーク環境を意識した対策を～

● 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



【3位】テレワーク等のニューノーマルな働き方を狙った攻撃

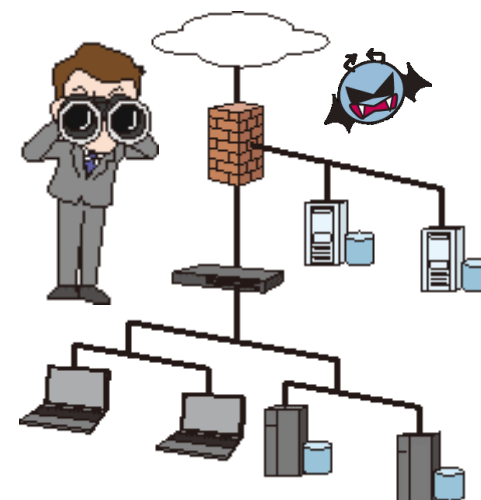
～テレワーク環境を意識した対策を～

● 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)

- セキュリティに強いテレワーク環境の採用
(シンクライアント、VPN、ZTNA等)
- 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
- セキュリティ教育の実施
- テレワークで利用するソフトウェアの脆弱性情報
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)



【3位】テレワーク等のニューノーマルな働き方を狙った攻撃

～テレワーク環境を意識した対策を～

● 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

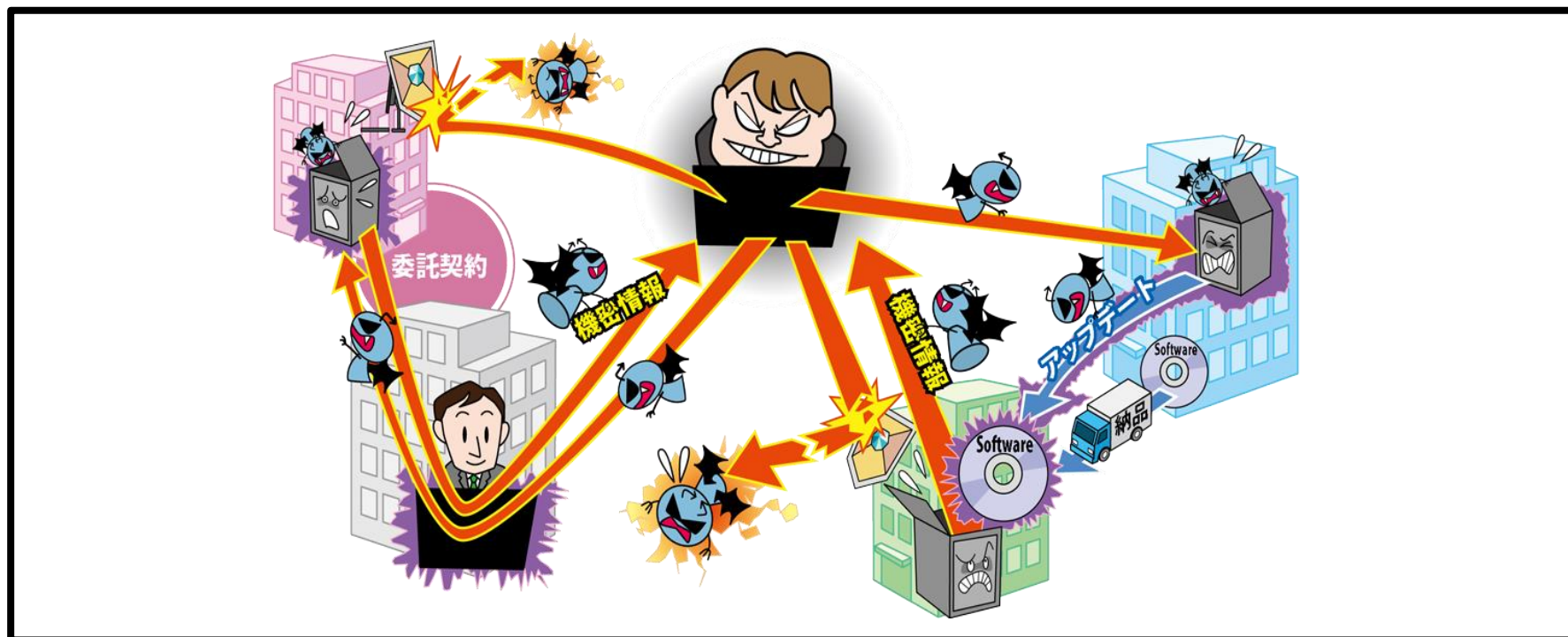
- 適切なログの取得と継続的な監視
- ネットワーク監視、防御
UTM・IDS/IPS等の導入

・被害を受けた後の対応

- CSIRTの運用によるインシデント対応
- 影響調査および原因の追究、対策の強化

【4位】サプライチェーンの弱点を悪用した攻撃

～ 自組織の対策だけでは不十分？ 広がるサプライチェーンを悪用した攻撃被害～



- 原材料や部品の調達、製造、在庫管理、物流、販売、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
- 取引先や一部業務を委託している外部組織から情報漏えい

【4位】サプライチェーンの弱点を悪用した攻撃

～自組織の対策だけでは不十分？広がるサプライチェーンを悪用した攻撃被害～

● 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



【4位】サプライチェーンの弱点を悪用した攻撃

～自組織の対策だけでは不十分？ 広がるサプライチェーンを悪用した攻撃被害～

● 2020年の事例／傾向①

■ 中国拠点を手掛かりに国内拠点へ侵入 (※1)

- ・2019年に大手電機メーカーから情報流出が確認された
- ・中国拠点のサーバーがウイルスに感染していた
- ・中国拠点を手掛かりに国内拠点へ侵入しウイルス拡散
- ・最終的に感染の疑いがある端末は国内外含め132台
- ・既存の防御をすり抜ける高度かつ巧妙な攻撃だった

【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>

【4位】サプライチェーンの弱点を悪用した攻撃

～自組織の対策だけでは不十分？広がるサプライチェーンを悪用した攻撃被害～

● 2020年の事例／傾向②

■ ソフトウェアの正規のアップデートにバックドア (※1,※2)

- ・2020年12月、セキュリティベンダーがサプライチェーン攻撃の発生を発表
 - ・ソフトウェアのアップデートファイルにバックドアが仕込まれた
 - ・アップデートファイルで更新した組織が感染
 - ・その後バックドアから攻撃者が組織に侵入
 - ・米政府をはじめ多くの米国組織で感染被害の報告あり
- ※国内でも感染の形跡が確認された

【出典】

※1 SolarWinds Security Advisory

<https://www.solarwinds.com/ja/securityadvisory>

※2 SolarWindsのサプライチェーン攻撃についてまとめた

<https://piyolog.hatenadiary.jp/entry/2020/12/20/045153>

【4位】サプライチェーンの弱点を悪用した攻撃

～自組織の対策だけでは不十分？ 広がるサプライチェーンを悪用した攻撃被害～

● 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



【4位】サプライチェーンの弱点を悪用した攻撃

～自組織の対策だけでは不十分？ 広がるサプライチェーンを悪用した攻撃被害～

● 対策

■ 組織(商流に関わる組織)

・被害の予防

－セキュリティの認証取得

(ISMS、Pマーク、SOC2、ISMAP等)

－公的機関が公開している資料の活用

「サプライチェーンのセキュリティ脅威に備える」(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

－委託元への連絡



【出典】

※1 サプライチェーンのセキュリティ脅威に備える

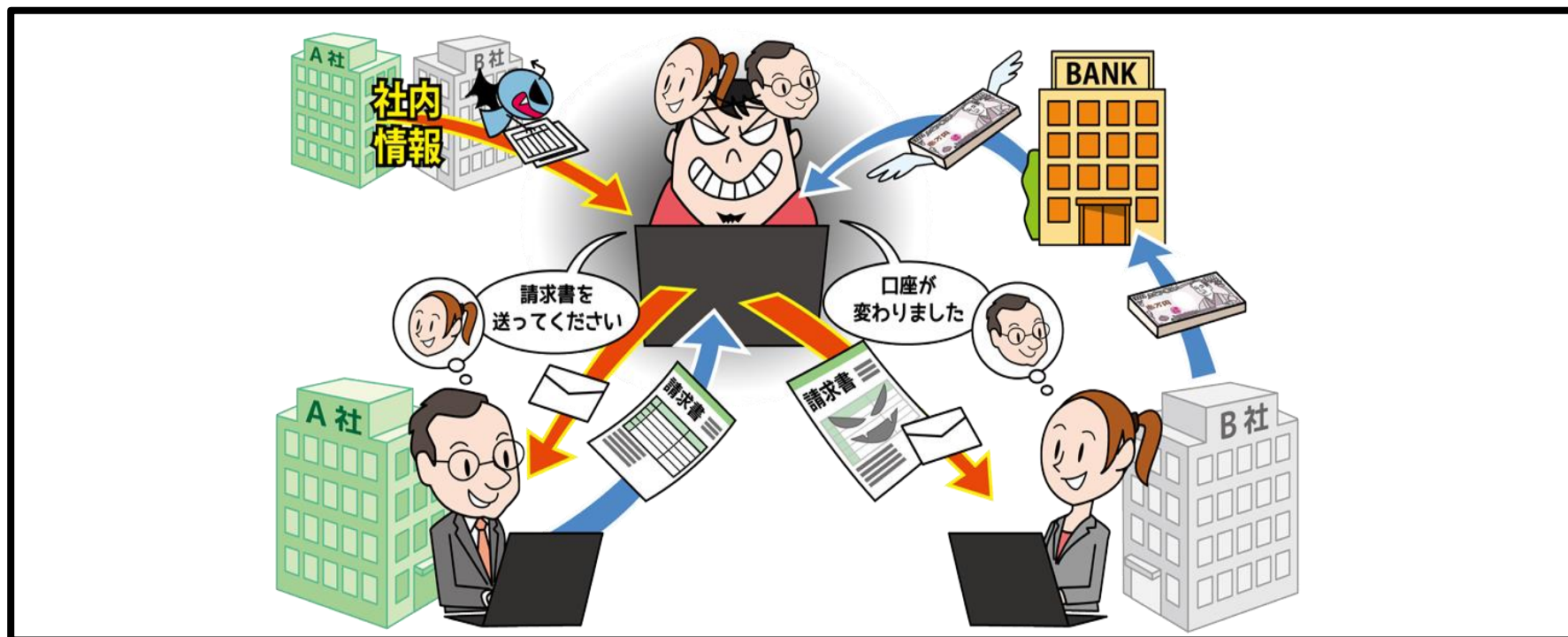
<https://www.ipa.go.jp/files/000073868.pdf>

※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

【5位】ビジネスメール詐欺による金銭被害

～その請求書、本物ですか？～



- 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

【5位】ビジネスメール詐欺による金銭被害

～その請求書、本物ですか？～

● 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



【5位】ビジネスメール詐欺による金銭被害

～その請求書、本物ですか？～

● 2020年の事例／傾向①

■ 巧妙化する日本語の偽メール

- ・サイバー情報共有イニシアティブ(J-CSIP)が注意喚起 (※1)
- ・新型コロナウイルスを話題とする偽メールの事例を確認
- ・日本語に不自然な点が少なく日本語を使える攻撃者がいる
ものと見られる

⇒国内組織が本格的に標的になってきている

【出典】

※1 ビジネスメール詐欺「BEC」に関する事例と注意喚起(第三報)

<https://www.ipa.go.jp/files/000081866.pdf>



【5位】ビジネスメール詐欺による金銭被害

～その請求書、本物ですか？～

● 2020年の事例／傾向②

■ ビジネスメール詐欺の多くは「取引先との請求書偽装」

- ・JPCERT/CCがビジネスメール詐欺の実態調査について公表 ^(※1)
- ・攻撃手口では「**取引先との請求書の偽装**」が多数
- ・以下のポイントからやり取りの過程で気づくこともできる
 - －支払い済みの請求・請求書の体裁が不自然
 - －見慣れない地域への送金
 - －送金先口座の凍結
 - －不自然なローカル言語 等



【出典】

※1 ビジネスメール詐欺の実態調査報告書

https://www.jpcert.or.jp/research/20200325_BEC-survey.pdf

【5位】ビジネスメール詐欺による金銭被害

～その請求書、本物ですか？～

● 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) ※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

＜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、二要素認証等で不正ログイン対策



【5位】ビジネスメール詐欺による金銭被害

～その請求書、本物ですか？～

● 対策

■ 組織

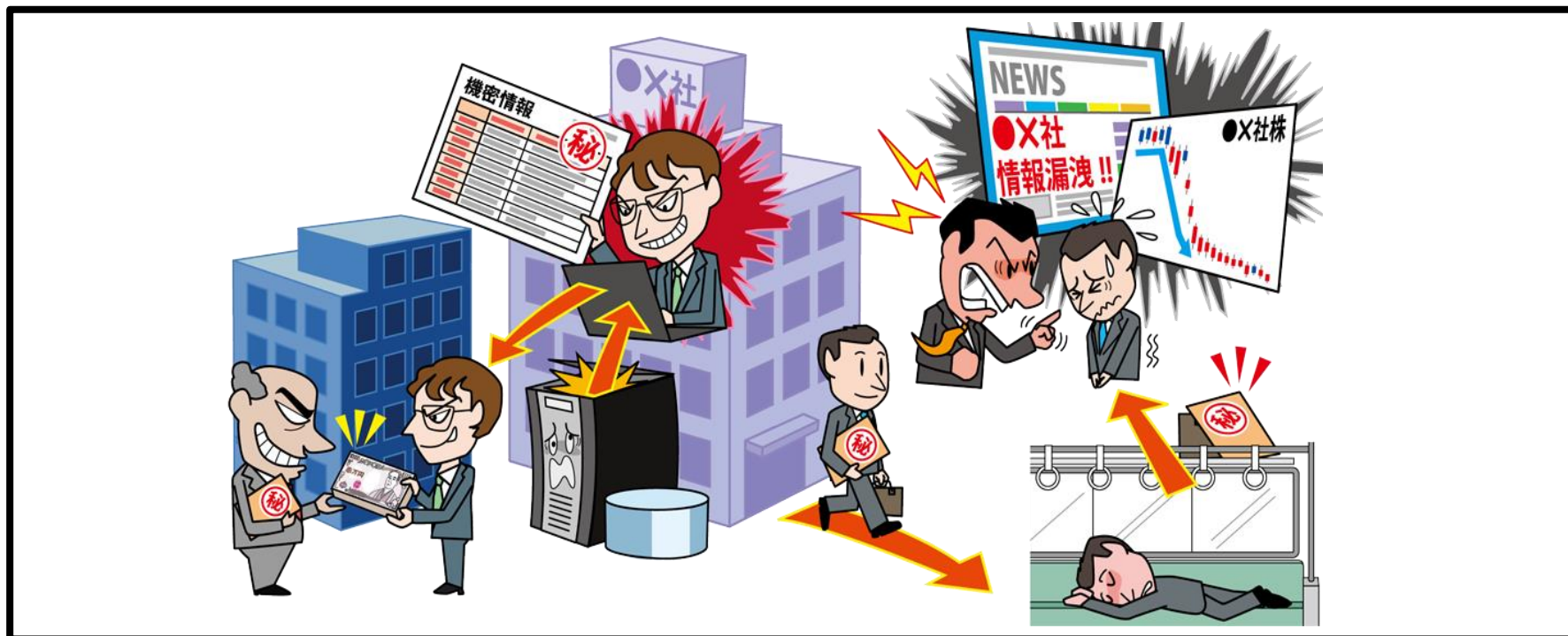
・被害を受けた後の対応

- CSIRT等所定の連絡先への連絡
- 銀行や警察に相談
- 踏み台や詐称されている組織への連絡
- 影響調査および原因追及、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



【6位】内部不正による情報漏えい

～内部不正が可能な環境を作らない～



- 組織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

【6位】内部不正による情報漏えい

～内部不正が可能な環境を作らない～

● 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

■ 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



【6位】内部不正による情報漏えい

～内部不正が可能な環境を作らない～

● 2020年の事例／傾向①

■ 市役所職員による情報流出 (※1)

- ・市の職員が業務に使用していたPCから同市の職員約2,700人分の個人情報や地方紙のメールアドレス宛に送信
- ・情報漏えいしたことが発覚し職員は懲戒免職となった
- ・漏えいした情報はPCの前の利用者がPCのごみ箱に捨てたままにしていたものを見つけ保存していた
- ・市の情報管理の不備も指摘された

【出典】

※1 データ流出で男性主査を懲戒免職／弘前市

<http://www.mutusinpou.co.jp/news/2020/06/60112.html>

【6位】内部不正による情報漏えい

～内部不正が可能な環境を作らない～

● 2020年の事例／傾向②

■ 社内評価を高めるため秘密情報の漏えい (※1)

- ・従業員がスマートフォンの画面に使用される素材に関する機密情報を自身のUSBメモリーに保存
- ・自宅のPCからメールで中国企業へ送信し情報漏えい
- ・従業員は不正競争防止法違反の容疑で書類送検
- ・従業員は社内評価を高めるためにSNSを通じて接触した中国企業従業員からの技術交換の提案に応じた

【出典】

※1 積水化学元社員が情報漏洩疑い 大阪府警が書類送検

<https://www.nikkei.com/article/DGXMZO64966730T11C20A0AC8000/>

【6位】内部不正による情報漏えい

～内部不正が可能な環境を作らない～

● 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
- 物理的管理の実施

・情報リテラシーや情報モラルの向上

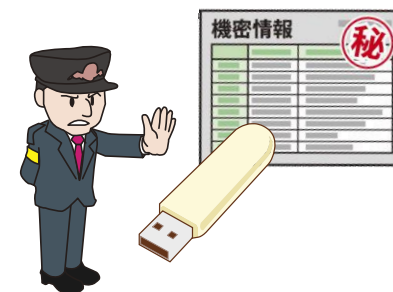
- 人的管理およびコンプライアンス教育の徹底

・被害の早期検知

- システム操作履歴の監視

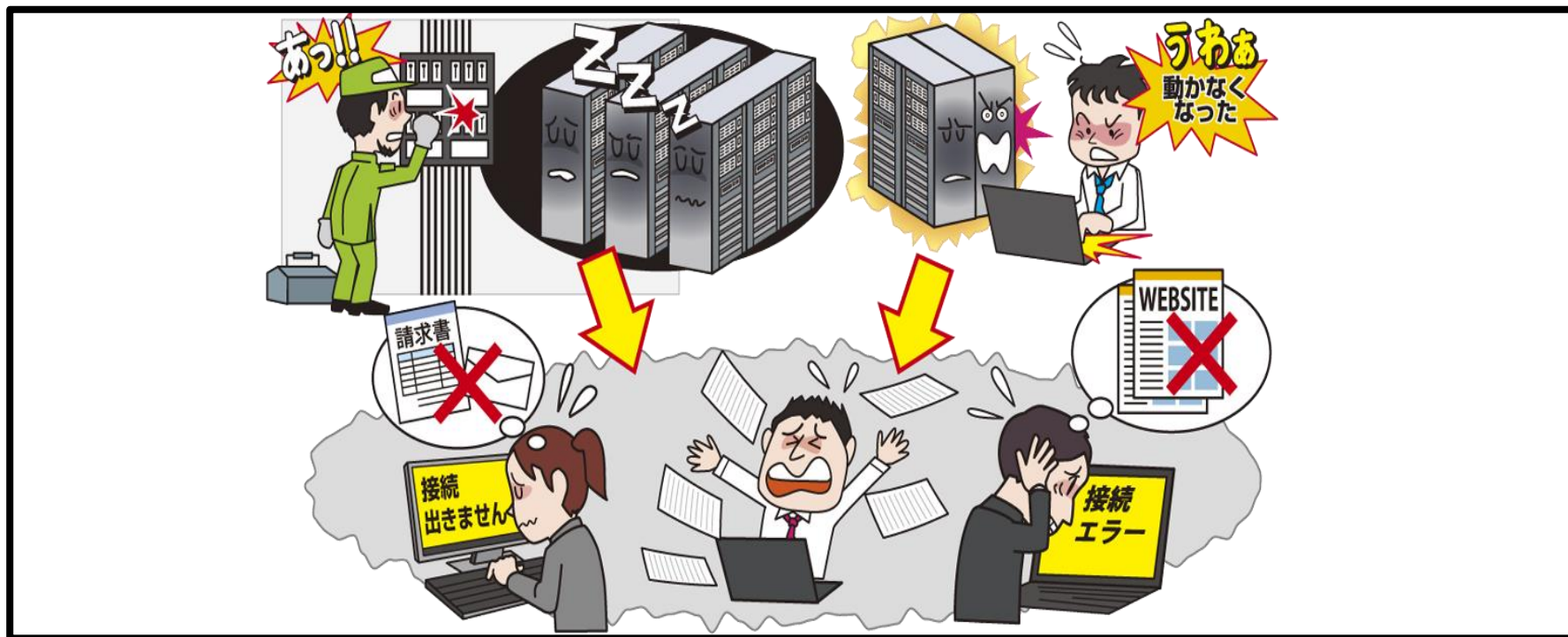
・被害を受けた後の対応

- 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



【7位】予期せぬIT基盤の障害に伴う業務停止

～IT基盤が停止するおそれがあることを意識する～



- 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

【7位】予期せぬIT基盤の障害に伴う業務停止

～IT基盤が停止するおそれがあることを意識する～

● 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

- ・電源、空調設備等の制御システムの障害

【7位】予期せぬIT基盤の障害に伴う業務停止

～IT基盤が停止するおそれがあることを意識する～

● 2020年の事例／傾向①

■ IT基盤の障害に伴う多数の重要サービスの停止 (※1)

- ・2020年12月、IT基盤に大規模な障害が発生
- ・ストレージのクォータ自動管理システムの不備が原因
- ・10月に別途実施していた他の作業も遠因となっていた
- ・当該IT基盤を利用する多数のサービスがアクセス不能に

【出典】

※1 グーグル、大規模障害の詳しい経緯を公表――システム移行時のミスが原因

<https://japan.cnet.com/article/35164342/>

【7位】予期せぬIT基盤の障害に伴う業務停止

～IT基盤が停止するおそれがあることを意識する～

● 2020年の事例／傾向②

■ 株式売買システム障害による終日取引停止 (※1)

- ・2020年10月、株式売買システムの大規模障害発生
- ・原因はNAS導入時のファームウェア設定の不備
- ・NASは冗長化構成であったが、NAS障害時の縮退運用への切り替えが正常に動作しなかった

【出典】

※1 10月1日に株式売買システムで発生した障害について

<https://www.jpx.co.jp/corporate/news/news-releases/0060/20201019-01.html>

【7位】予期せぬIT基盤の障害に伴う業務停止

～IT基盤が停止するおそれがあることを意識する～

● 対策

■ 組織（ITシステム利用者、IT基盤利用者）

・被害の予防

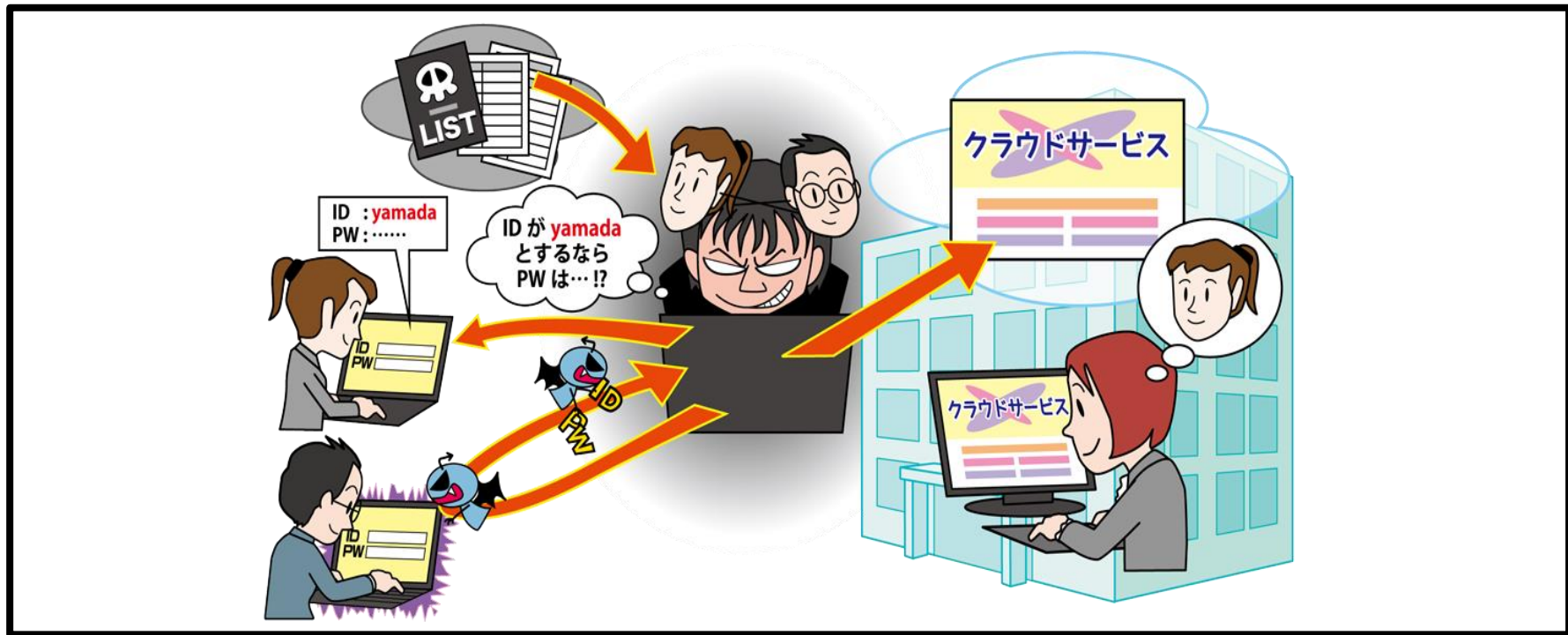
- BCMの実践（BCP策定と運用）
- 可用性の確保と維持（システム設計や監視）
- データバックアップ（復旧対策）
- 契約やSLA等を確認
 - IT基盤側との契約、SLA
 - 顧客側との契約、SLA
- 被害を想定し、IT基盤側との事前の連携確認

・被害を受けた後の対応

- BCPに従った対応
 - 影響調査、対策強化、CSIRTや関係者への迅速な連絡等

【8位】インターネット上のサービスへの不正ログイン IPA

～パスワードの使いまわしや安易なパスワードの設定をやめるよう呼びかけを～



- 利用しているインターネット上のサービスの認証情報(ID、パスワード)が窃取または推測され、不正ログインされる
- インターネット上のサービスの機能に応じて発生する被害は様々

【8位】インターネット上のサービスへの不正ログイン IPA

～パスワードの使いまわしや安易なパスワードの設定をやめるよう呼びかけを～

● 攻撃手口

・不正に入手した認証情報で不正ログインする

■ パスワードリスト攻撃

- ・何らかの方法で入手した認証情報をリスト化し、それを利用して複数のサービスにログインを試みる攻撃
- ・複数のサービスでパスワードを使いまわしている場合、パスワードが漏えいすると利用している複数のサービスに不正ログインされるおそれがある



【8位】インターネット上のサービスへの不正ログイン IPA

～パスワードの使いまわしや安易なパスワードの設定をやめるよう呼びかけを～

● 攻撃手口

・不正に入手した認証情報で不正ログインする

■ パスワード推測攻撃

- ・利用者が使いそうなパスワードを推測して不正ログインを試みる(名前や誕生日等をパスワードに使用していると推測されやすくなる)
- ・SNSで公開している情報等から推測される場合も

■ ウイルス感染による窃取

- ・悪意あるウェブサイトやメール等でウイルス感染させ、その端末で利用したサービスのパスワード等を窃取

【8位】インターネット上のサービスへの不正ログイン IPA

～パスワードの使いまわしや安易なパスワードの設定をやめるよう呼びかけを～

● 2020年の事例／傾向①

■ 不正ログインによる取引先情報の流出 (※1)

- ・大手電機メーカーが利用しているクラウドサービスに対して不正ログインが行われた
- ・取引先の名前や金融機関口座等、8,635件の情報流出
- ・攻撃者が何らかの方法で入手したIDとパスワードを使い同社社員になりすましていたとみられる
- ・正規のIDとパスワードを使ったログインであったため既存の対策では防げなかったとしている

【出典】

※1 三菱電機、不正アクセスで取引先の口座情報8000件流出

<https://www.nikkei.com/article/DGXMZO66468150Q0A121C2TJC000>

【8位】インターネット上のサービスへの不正ログイン IPA

～パスワードの使いまわしや安易なパスワードの設定をやめるよう呼びかけを～

● 2020年の事例／傾向②

■ 施設予約システムへの大量の不正ログイン試行 (※1)

- ・市が運営する公共利用施設予約システムにおいて大量の不正ログインが試行された
- ・利用者約1,300人分のアカウントがロックされ、システムの適切な運用ができなくなった
- ・同市は攻撃者による偽計業務妨害罪に該当するとして告訴状を警察に提出したと発表

【出典】

※1 ふれあいネットへの不正ログイン試行、偽計業務妨害罪として川崎市が告訴へ

<https://scan.netsecurity.ne.jp/article/2020/11/24/44853.html>

【8位】インターネット上のサービスへの不正ログイン



～パスワードの使いまわしや安易なパスワードの設定をやめるよう呼びかけを～




● 対策

■ 組織(サービス利用者)

・被害の予防

- 添付ファイルやURLを安易にクリックしない
- パスワードは長く、複雑にする
- パスワードの使いまわしをしない
- パスワード管理ソフトの利用
- サービスが推奨する認証方式の利用(二要素認証等)



	PW:	A+%Ringo5
	PW:	B-!Ringo5
	PW:	C*\$Ringo5

【8位】インターネット上のサービスへの不正ログイン



～パスワードの使いまわしや安易なパスワードの設定をやめるよう呼びかけを～

● 対策

■ 組織(サービス運営者)

・被害の予防

- セキュリティ対策の予算・体制の確保
- 利用者に対するセキュリティ機能の提供
 - 二要素認証やリスクベース認証、利用履歴を確認できる機能等を提供する
- アカウントの存在有無の確認に悪用されないサービス設計
 - アカウントの存在有無がわかるような認証エラー表示の抑止、連続アクセスの検知等



SNS PW: A+%Ringo5
アプリ PW: B-!Ringo5
メール PW: C*\$Ringo5

【8位】インターネット上のサービスへの不正ログイン



～パスワードの使いまわしや安易なパスワードの設定をやめるよう呼びかけを～

● 対策

■ 組織(サービス運営者)

・被害の早期検知

－適切なログの取得と継続的な監視

・被害の早期検知

－CSIRT等所定の連絡先への連絡

－セキュリティ専門企業への調査依頼

－影響調査及び原因の追究、対策の強化

－被害者に対するすみやかな連絡と補償

－漏えいした内容や発生原因等の公表

－関係者、関係機関への連絡

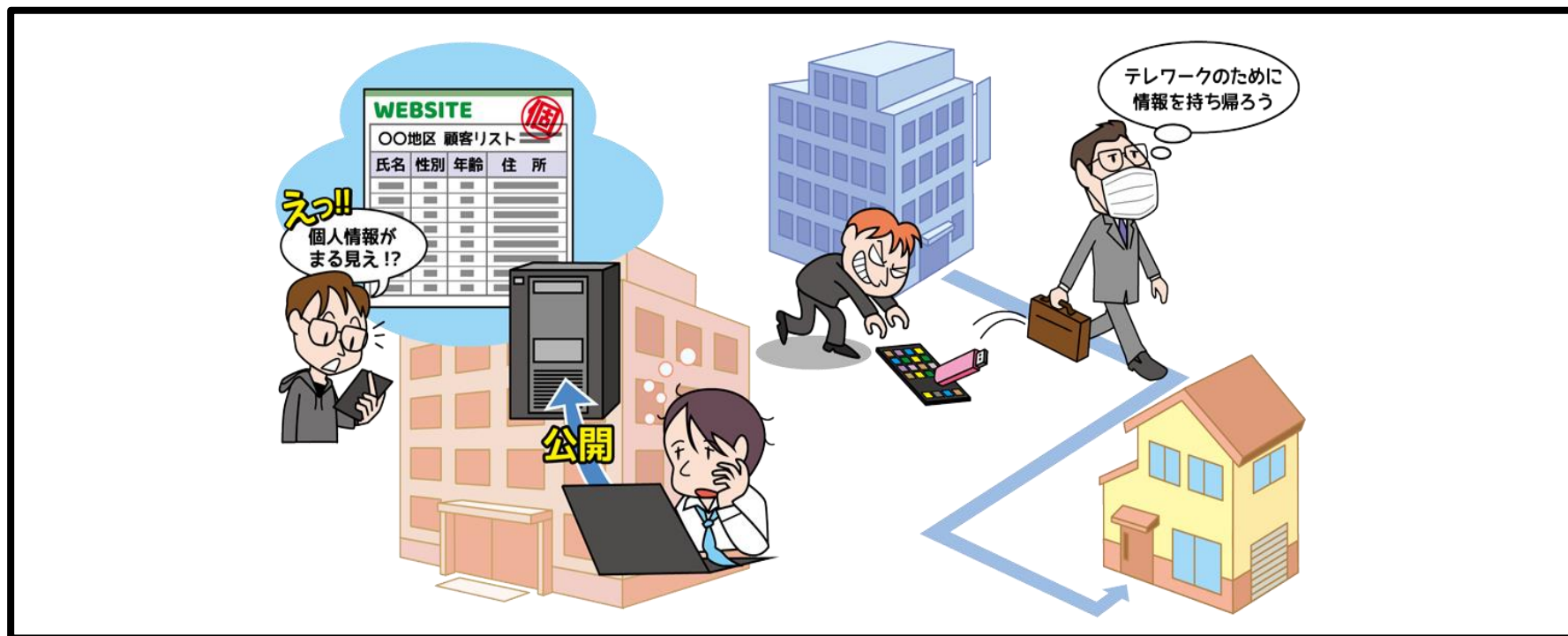
監督官庁、個人情報保護委員会、警察等



SNS PW: A+%Ringo5
アプリ PW: B-!Ringo5
メール PW: C*\$Ringo5

【9位】不注意による情報漏えい等の被害

～業務環境の変化に合わせて対策の見直しを～



- 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

～業務環境の変化に合わせて対策の見直しを～

● 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

■ 従業員のセキュリティ意識の低さ

- ・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

【9位】不注意による情報漏えい等の被害

～業務環境の変化に合わせて対策の見直しを～

● 2020年の事例／傾向①

■ メールの誤送信や対応不備による情報流出 (※1)

- ・県が保有する新型コロナウイルス感染症陽性者約9,700人分の個人情報が流出した
- ・患者情報等が含まれるファイルが入ったクラウド上のフォルダーへのアクセス権が付与されたメールを関係者宛に送信する際に、メールアドレスが似ていた第三者に誤送信
- ・誤送信発覚後にアクセス制限対応を実施したが、設定ミスがあり第三者が閲覧できる状態が継続した

【出典】

※1 新型コロナウイルス感染症対策本部(調整本部)における個人情報の漏えい等事案について

<https://www.pref.fukuoka.lg.jp/contents/covid19-rouei.html>

【9位】不注意による情報漏えい等の被害

～業務環境の変化に合わせて対策の見直しを～

● 2020年の事例／傾向②

■ 顧客情報が保存された記録媒体を紛失 (※1)

- ・重要な情報が含まれるバックアップ用の磁気テープを紛失
- ・磁気テープの中には顧客の個人情報やサービス利用実績、委託された業務に関する情報等約250万件
- ・誤廃棄の可能性が高く、外部への情報の流出は確認されていないとしている

【出典】

※1 みずほ総合研究所株式会社におけるお客さま情報の紛失について

<https://www.mizuho-ri.co.jp/company/release/pdf/20200721release.pdf>

【9位】不注意による情報漏えい等の被害

～業務環境の変化に合わせて対策の見直しを～

● 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

- 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
- DLP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

～業務環境の変化に合わせて対策の見直しを～

● 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

- CSIRT等所定の連絡先への連絡
 - 影響調査および原因の追究、対策の強化
 - 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



【9位】不注意による情報漏えい等の被害

～業務環境の変化に合わせて対策の見直しを～

● 対策

■ 個人／組織（被害者）

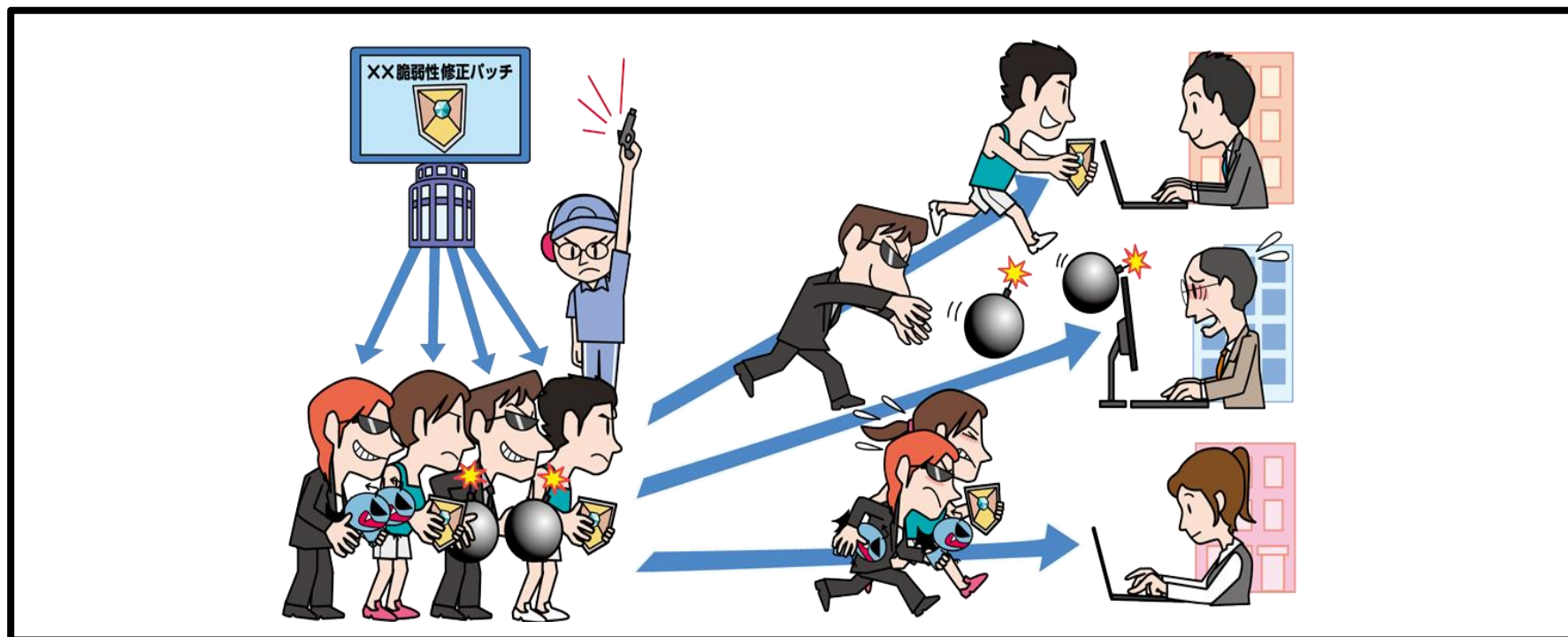
・被害を受けた後の対応

- －漏えいが発生した組織からの情報に従う
- －パスワードやクレジットカード情報の変更等



【10位】脆弱性対策情報の公開に伴う悪用増加

～公開された脆弱性を知っているのは自分たちと悪人たち～



- 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には被害が大きくなる

【10位】脆弱性対策情報の公開に伴う悪用増加

～公開された脆弱性を知っているのは自分たちと悪人たち～

● 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

【10位】脆弱性対策情報の公開に伴う悪用増加

～公開された脆弱性を知っているのは自分たちと悪人たち～

● 2020年の事例／傾向①

■ 製品の脆弱性を狙う攻撃活動を観測 (※1)

- ・2020年7月1日、ネットワーク製品においてリモートから任意のコードの実行が可能な脆弱性情報が公開された
- ・脆弱性情報公開の4日後には、脆弱性を悪用するための攻撃コードがインターネット上に公開された
- ・翌日には公開された攻撃コードを悪用した攻撃が確認された

【出典】

※1 【注意喚起】F5 BIG-IP製品の任意コード実行可能な脆弱性(CVE-2020-5902)を狙う攻撃活動を観測

https://www.lac.co.jp/lacwatch/alert/20200708_002231.html

【10位】脆弱性対策情報の公開に伴う悪用増加

～公開された脆弱性を知っているのは自分たちと悪人たち～

● 2020年の事例／傾向②

■ Windows Serverに「ZeroLogon」の脆弱性 (※1)

- ・2020年8月11日(米国時間)、Windows Server製品に影響がある「ZeroLogon」と呼ばれる、特権の昇格の脆弱性に対する更新プログラムが公開された
- ・2020年9月15日(日本時間)に本脆弱性に対する実証コード(PoC)が公開された
- ・9月24日(米国時間)にPoCを悪用した攻撃が確認された

【出典】

※1 Netlogon の特権の昇格の脆弱性 (CVE-2020-1472) への早急な対応を

<https://www.jpcert.or.jp/newsflash/2020091601.html>

【10位】脆弱性対策情報の公開に伴う悪用増加

～公開された脆弱性を知っているのは自分たちと悪人たち～

● 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
- 脆弱性情報の収集と対応
- UTM・IDS/IPS・WAF等の導入
- 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

・被害を受けた後の対応

- CSIRT等所定の連絡先への連絡
- 影響調査および原因の追究、対策の強化

【10位】脆弱性対策情報の公開に伴う悪用増加

～公開された脆弱性を知っているのは自分たちと悪人たち～

● 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
- 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

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

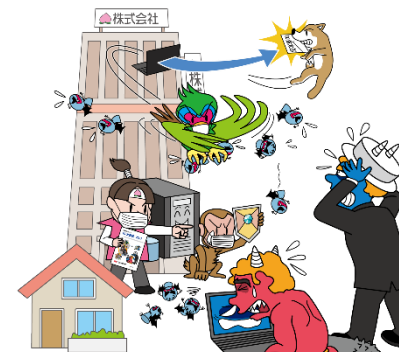
- ・脅威に備えるためには攻撃手口や動向、および自組織が抱える要因等を把握することが重要
- ・「10大脅威」のランキングは、各組織において実施すべき対策の優先度とは必ずしも一致はしない。組織ごとの状況を考慮して対策の優先度を決定する

詳細な資料のダウンロード

■情報セキュリティ10大脅威 2021

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/10threats2021.html>



■アンケートご協力をお願いについて

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%3DEA000000074

