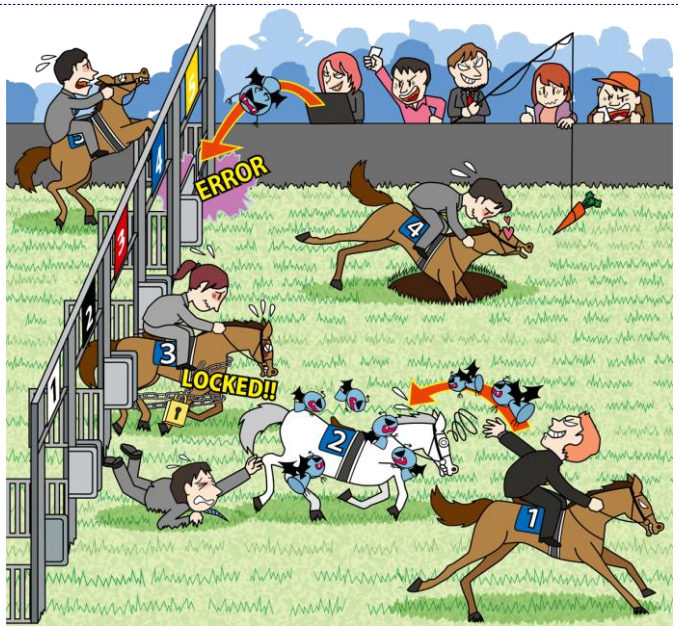
IPA Better Life with IT

情報セキュリティ10大脅威 2022
組織編



2022年 9月14日
MCPC・情報セキュリティセミナー

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
大友　更紗

IPA（情報処理推進機構）のご紹介

Information-technology Promotion Agency, Japan

- 日本のIT国家戦略を技術面、人材面から支える経済産業省所管の独立行政法人
- **「誰もがITの恩恵を享受できる社会」**を目指しています

● 情報セキュリティ

・ウイルス、不正アクセス等の届出機関
・情報セキュリティの調査研究、普及啓発活動
・標的型サイバー攻撃の情報共有・初動対応の実施

● IT人材育成

・国家試験「情報処理技術者試験」の実施機関
・IT人材の育成・発掘・スキル明確のとりくみ。若手人材育成。

● IT社会の動向調査・分析・基盤構築

・新たなIT社会の動向調査、新しい技術の安全性・信頼性の確保に向けた指針策定など

「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

2つの「10大脅威」

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」**

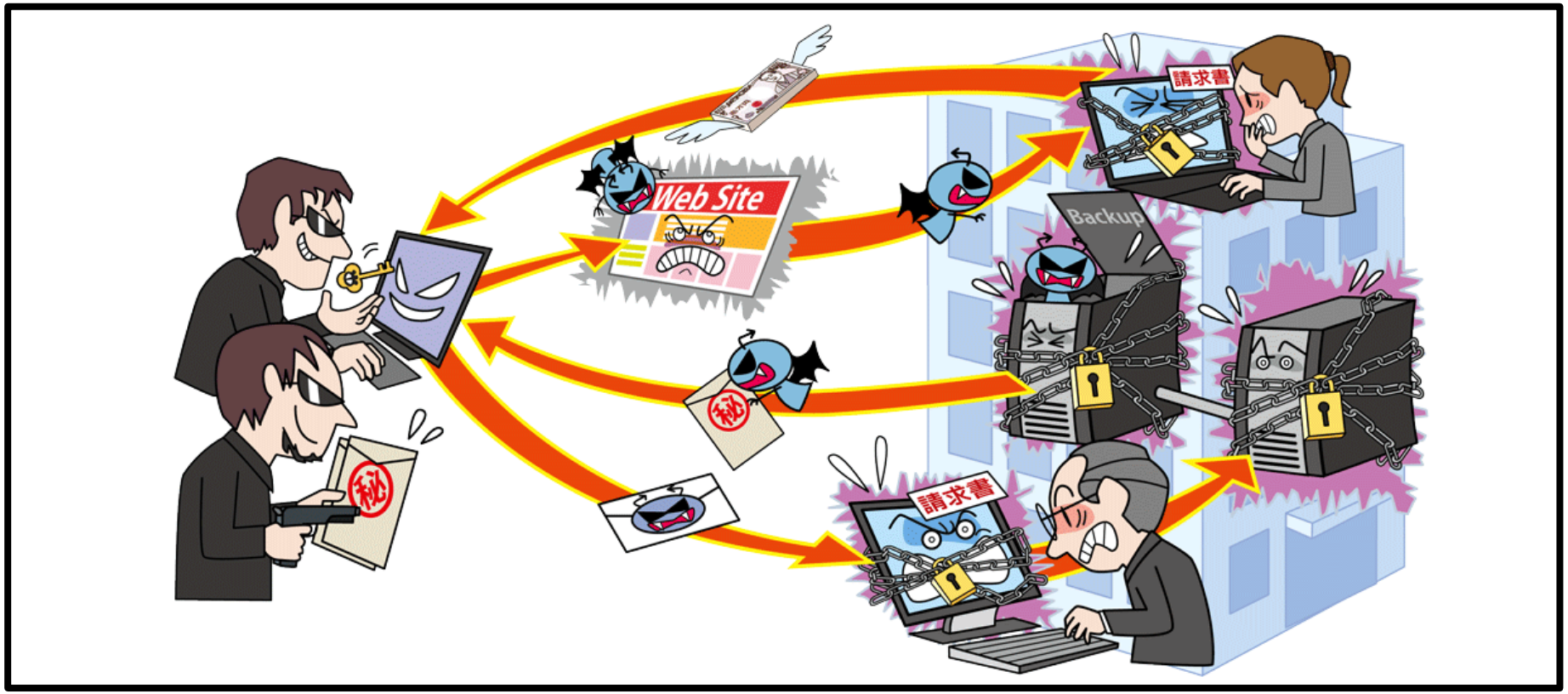
「個人」と「組織」の2つの立場で脅威を解説

情報セキュリティ10大脅威 2022

「個人」向け脅威	順位変動	「組織」向け脅威
フィッシングによる個人情報等の詐取	1 → 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 → 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	4 → 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	3 → 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	6 → 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	10 → 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（New）	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	5 → 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	7 → 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	9 → 10	不注意による情報漏えい等の被害

【組織の脅威：第１位】
ランサムウェアによる被害

【1位】ランサムウェアによる被害



- PC等のファイルを暗号化し、復旧と引き換えに金銭要求
- 最近は、情報を窃取しそれを公開すると脅迫するケースも
- 事業継続にも影響が出るおそれ

【1位】ランサムウェアによる被害

● 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

【1位】ランサムウェアによる被害

● 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

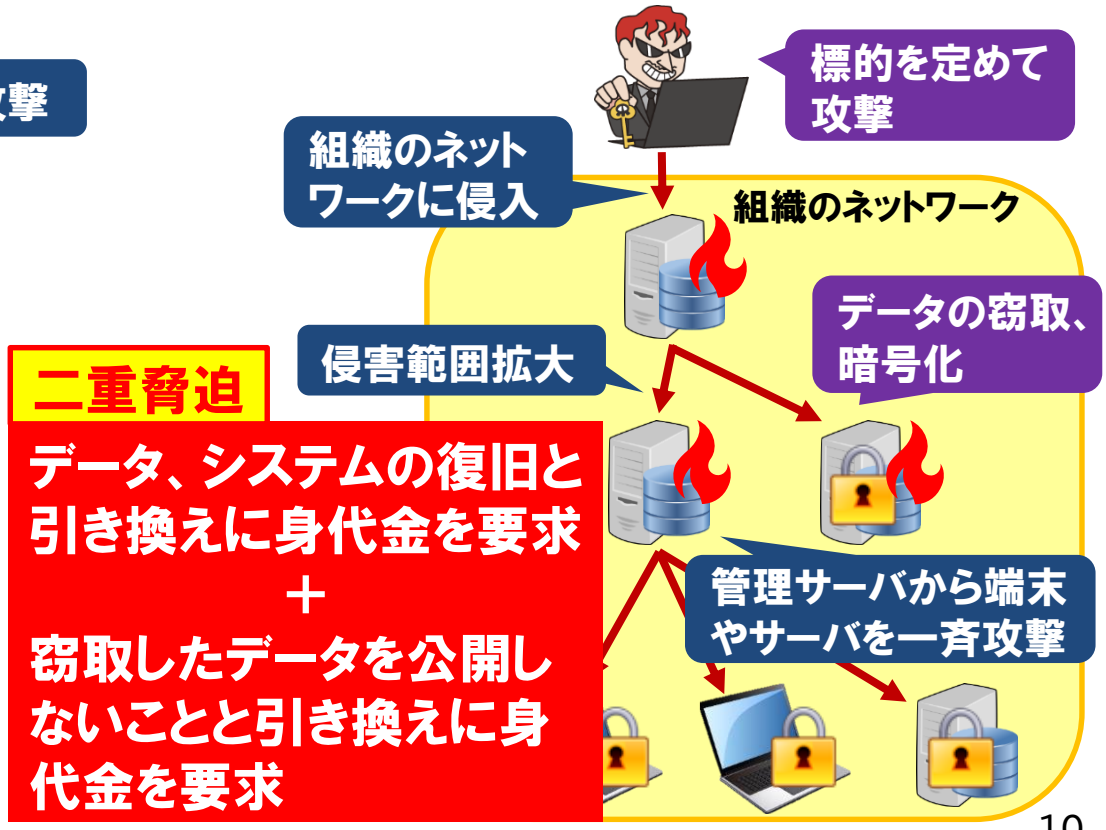
- 管理用のRDP（リモートデスクトップ）等やVPN経由で不正アクセス
- サーバー上で攻撃者がウイルスを実行（感染させる）

【1位】ランサムウェアによる被害

- **事業継続を脅かす新たなランサムウェア攻撃について**
  https://www.ipa.go.jp/security/announce/2020-ransom.html

初期のランサムウェア攻撃

近年のランサムウェア攻撃



【1位】ランサムウェアによる被害

- **多重脅迫**

二重脅迫に留まらない「四重脅迫」も(※1)

サービス妨害（DDoS攻撃）

- 身代金を支払わないとDDoS攻撃を行うと脅迫、
  または攻撃中止のための身代金を要求
  →更なる混乱

顧客や取引先へのリーク

- 身代金を支払わないとランサムウェア攻撃を受けている
  （顧客や取引先の個人情報等が漏えいしている）ことを
  顧客や取引先にリークすると脅迫
  →信用失墜、顧客や取引先からのプレッシャー

【出典】
※1 「ランサムウェア攻撃 グローバル実態調査 2022年版」を発表
https://www.trendmicro.com/ja_jp/about/press-release/2022/pr-20220907-01.html

【1位】ランサムウェアによる被害

- 事例/傾向
  - 社会インフラ関連企業における被害（※1）
    - 2021年5月、アメリカ最大の石油パイプラインがランサムウェア攻撃の被害に
    - **脆弱な設定のVPN経由**での不正アクセスによって感染
    - データの暗号化の他、データ窃取による**二重脅迫**
    - 5日間の操業停止に追い込まれ、ガソリン不足を心配した市民のガソリン買いだめによって価格高騰等の影響

【出典】
※1 ランサムウエア攻撃で石油パイプラインが停止、犯罪組織DarkSideの手口を検証（日経クロステック）
https://active.nikkeibp.co.jp/atcl/act/19/00324/100800001/

【1位】ランサムウェアによる被害

- 事例/傾向
  - バックアップの暗号化による被害の長期化(※1)
    - 国内の製粉会社がサイバー攻撃を受け、基幹システムを含む多くのシステムや端末で暗号化の被害
    - 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等にも影響

【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

● 対策

業務に必要な重要ファイルはバックアップを

■ バックアップ媒体とPCとの接続はバックアップ時のみ

・ランサムウェアの暗号化対象にならないように、通常時はパソコンと切り離しておく。

■ バックアップに使用する装置・媒体は複数用意

・バックアップファイルが暗号化される危険性や、失敗する可能性も考慮し、複数バックアップがあると安心。

■ バックアップ方式の妥当性を定期的に確認

・バックアップを取得していてもそこから復元できなければ意味がない。バックアップデータやバックアップ手法に問題がないことを定期的に確認。

【1位】ランサムウェアによる被害

- 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
  - システム管理者、従業員
    - 被害の予防
      - 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
      - 脆弱性情報の収集およびセキュリティパッチの適用
      - フィルタリングツール（メール、ウェブ）やセキュリティソフトの活用
      - 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

【1位】ランサムウェアによる被害

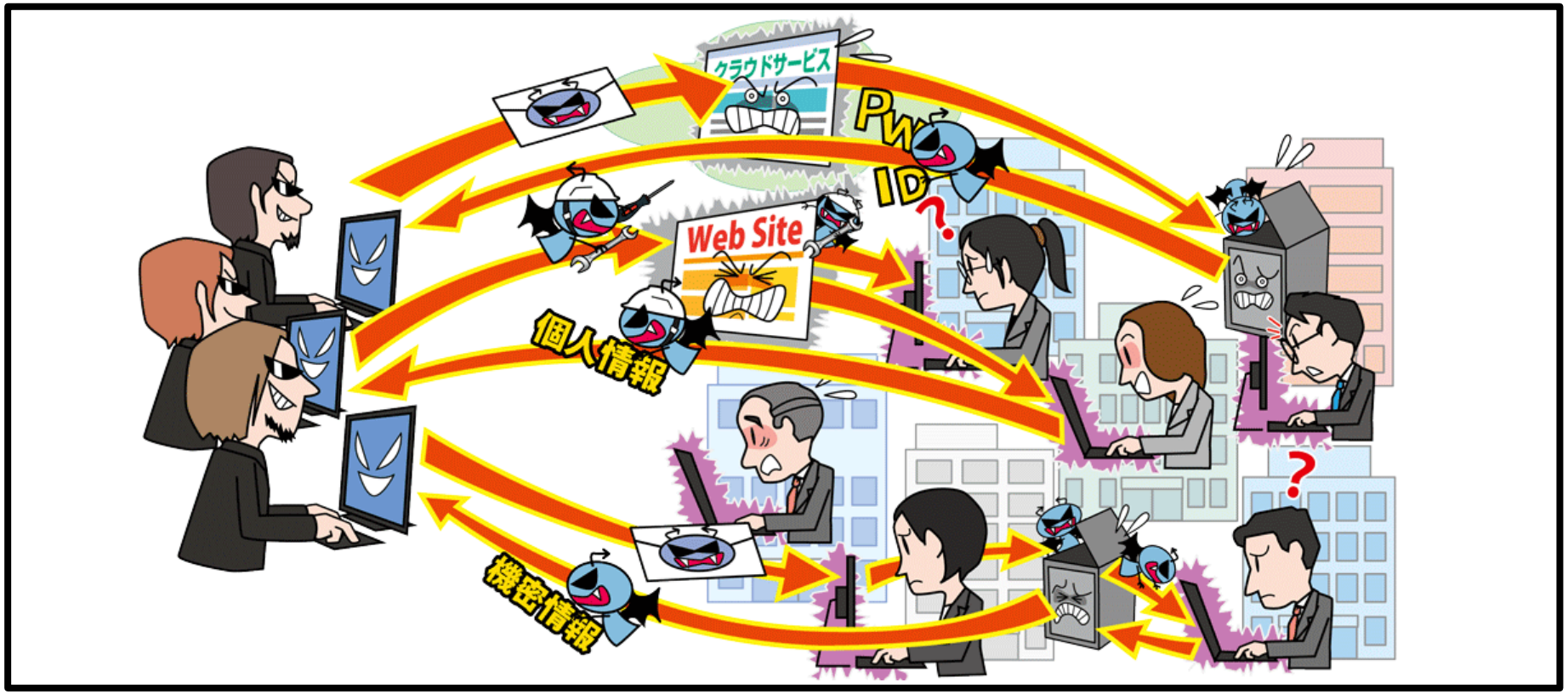
- 対策
  - システム管理者、従業員
    - 被害を受けた後の対応
      - CSIRTへ連絡
      - バックアップからの復旧
      - 復号ツールの活用
        例：No More Ransom (https://www.nomoreransom.org/ja/index.html)
      - 影響調査および原因の追究、対策の強化

<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

【組織の脅威：第2位】
標的型攻撃による
機密情報の窃取

【2位】標的型攻撃による機密情報の窃取



- 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

【2位】標的型攻撃による機密情報の窃取

● 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
- Officeファイルのマクロを悪用

■ 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

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等の脆弱性を悪用して不正ログインし、認証情報を窃取することで社内システムへ正規の経路から侵入
- 組織で利用されている機器の脆弱性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

【2位】標的型攻撃による機密情報の窃取

- 事例/傾向
  - 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]

- 2020年1月、**防衛事業部門**のサーバー内の27,445件のファイルが不正アクセスされていたことを公表
- 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

[重工メーカー]

- 2020年12月、外部からの不正アクセスを受けたと公表
- 2020年6月以降、**複数の海外拠点および国内拠点間**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であった

【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

メール利用者における対策

- 不審なメールの添付ファイルは開かない

※不審を抱きにくいような巧妙なメールも増えている。
「添付ファイルを開くとウイルスに感染するかも」という心構えを

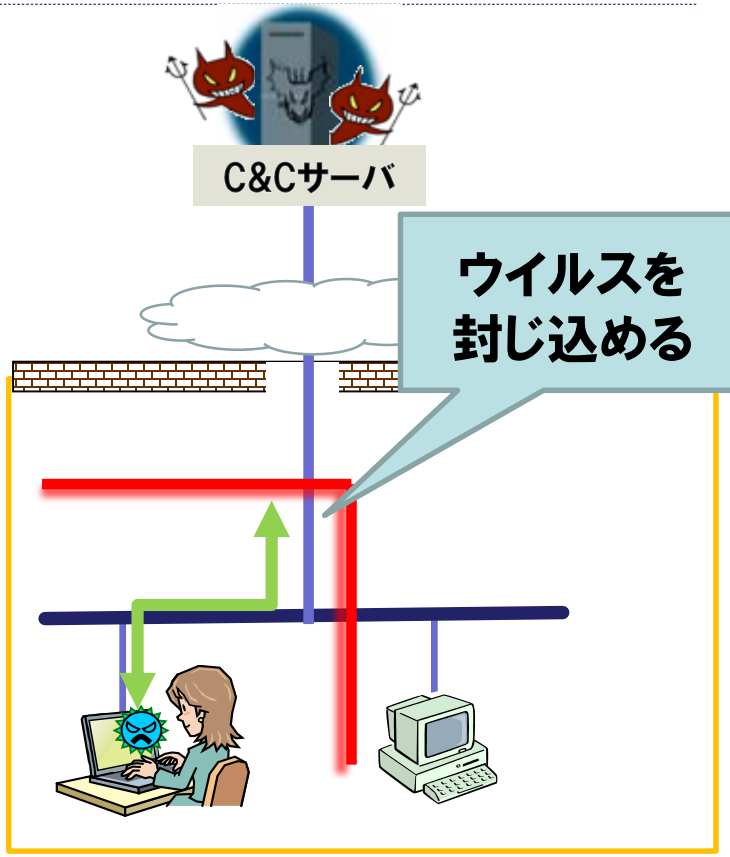
- WordファイルやExcelファイルのマクロに要注意

警告ウィンドウの以下のボタンは押さない
- 「マクロを有効にする」
- 「コンテンツの有効化」
- 「編集を有効にする」

- 「.exe」や「.js」などのファイルにも引き続き要注意

システムにおける対策

巧妙化する標的型メール攻撃
開封率0%は困難

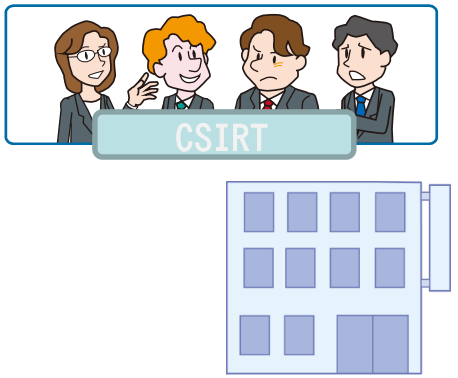


万が一に備えた対策が必要

感染しない対策 ＋ **被害を最小限に抑える対策**

【2位】標的型攻撃による機密情報の窃取

- 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

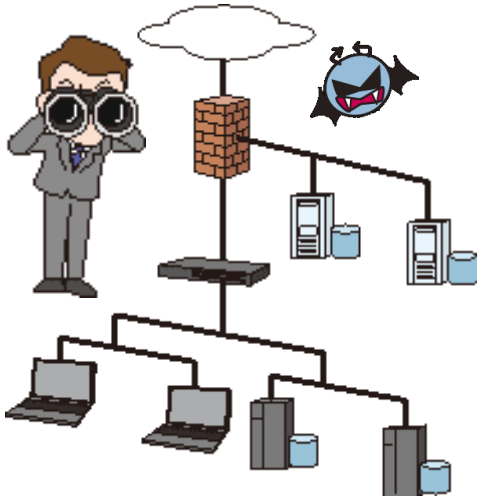
- 対策
  - セキュリティ担当者、システム担当者
    - 被害の予防/対応力の向上
      - 情報の管理とルール策定
      - サイバー攻撃に関する継続的な情報収集と情報共有
      - 脆弱性情報の収集およびセキュリティパッチの適用
      - フィルタリングツール(メール、ウェブ)やセキュリティソフトの活用
      - セキュリティ教育・インシデント訓練
      - 総合運用管理ツール等によるセキュリティ対策状況の把握
      - 取引先のセキュリティ対策実施状況の確認
      - セキュアなシステム設計
      - ネットワーク分離
      - 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

【2位】標的型攻撃による機密情報の窃取

● 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



【2位】標的型攻撃による機密情報の窃取

- 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

【ご参考】Emotetと呼ばれるウイルスについて

Emotetに感染した場合の被害例

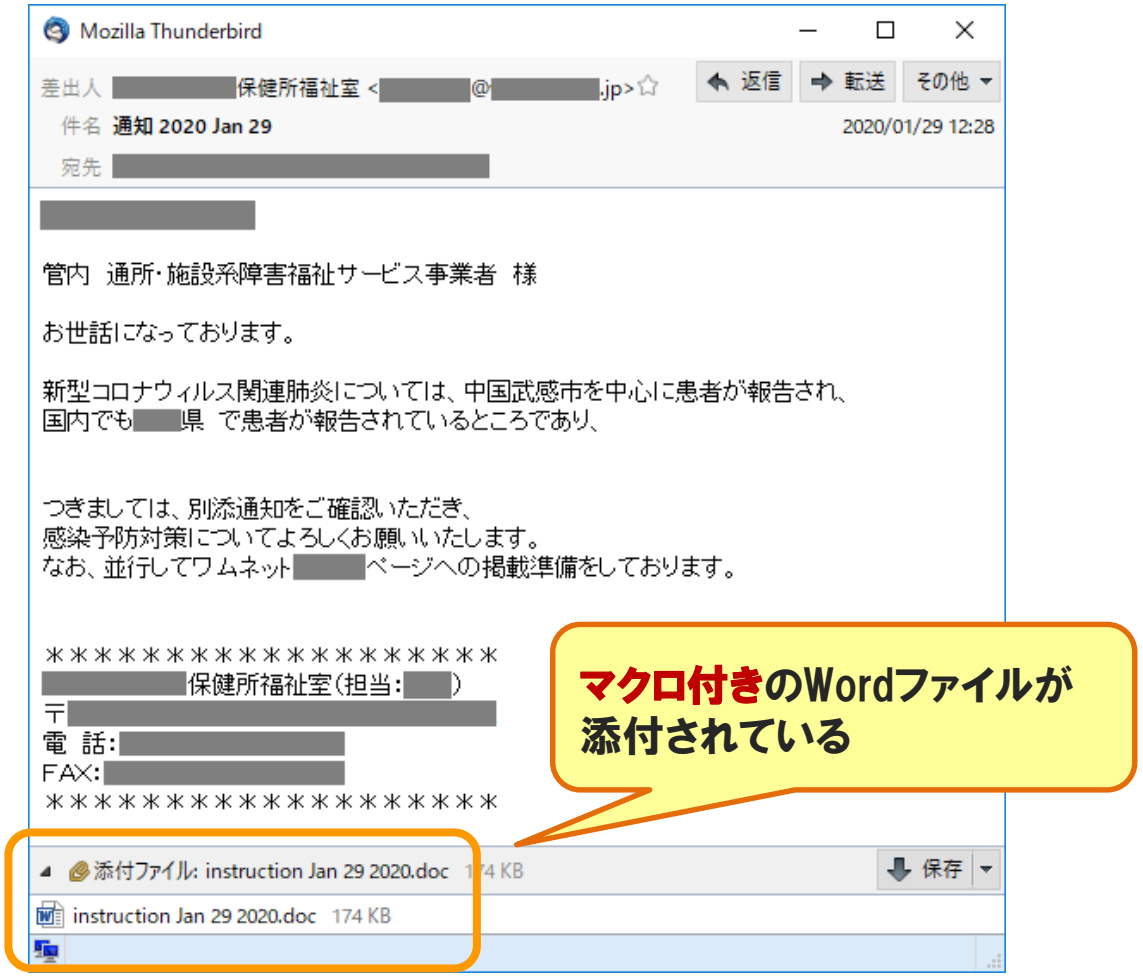
- 端末やブラウザに保存されたパスワード等の認証情報が窃取される
- 窃取された認証情報を悪用され、組織内で感染が広がる
- メールアカウントとパスワードが窃取される
- メール本文やアドレス帳の情報が窃取される
- 窃取されたメールアカウントや本文などが悪用され、Emotetの感染を広げるメールが外部に送信される

など

「Emotet（エモテット）」と呼ばれるウイルスへの感染を狙うメールについて
https://www.ipa.go.jp/security/announce/20191202.html

Emotetへの感染を狙うメールの例①

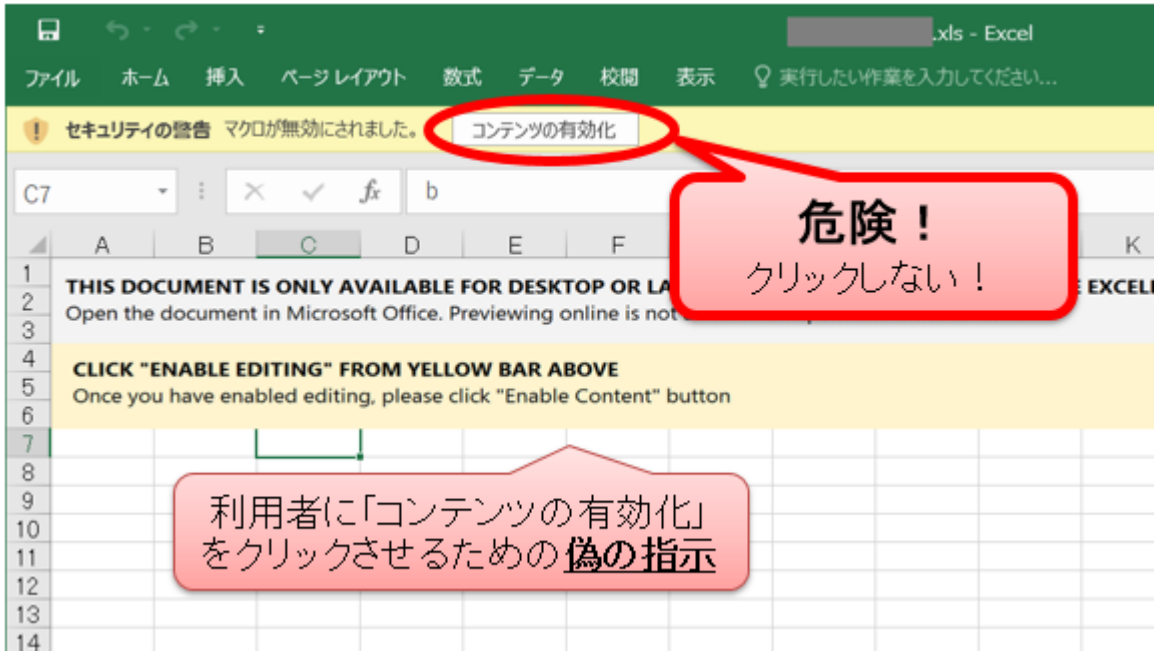
- **新型コロナウイルスを題材としたメール（2020年1月29日）**



Emotetへの感染を狙うメールの例②-1

- 2021年は一度収束に向かったが、11月以降再確認されている

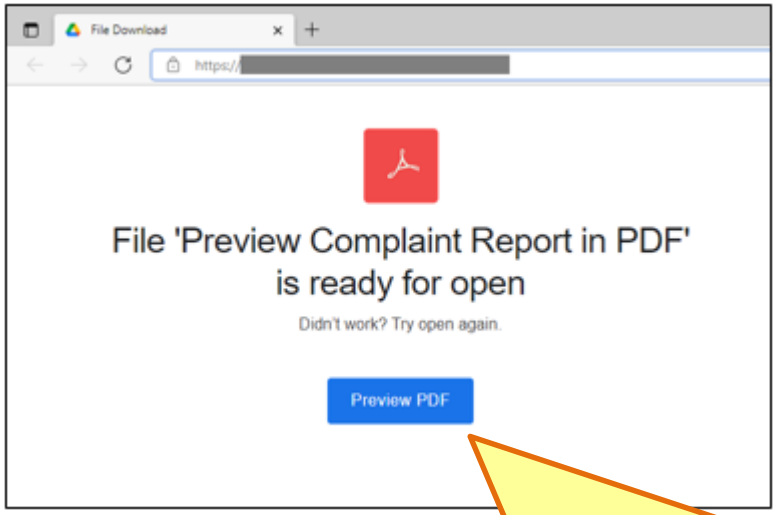
Excelファイルを悪用する手口



Emotetへの感染を狙うメールの例②-2

- 2021年は一度収束に向かったが、11月以降再確認されている

PDF閲覧ソフトを偽装する手口

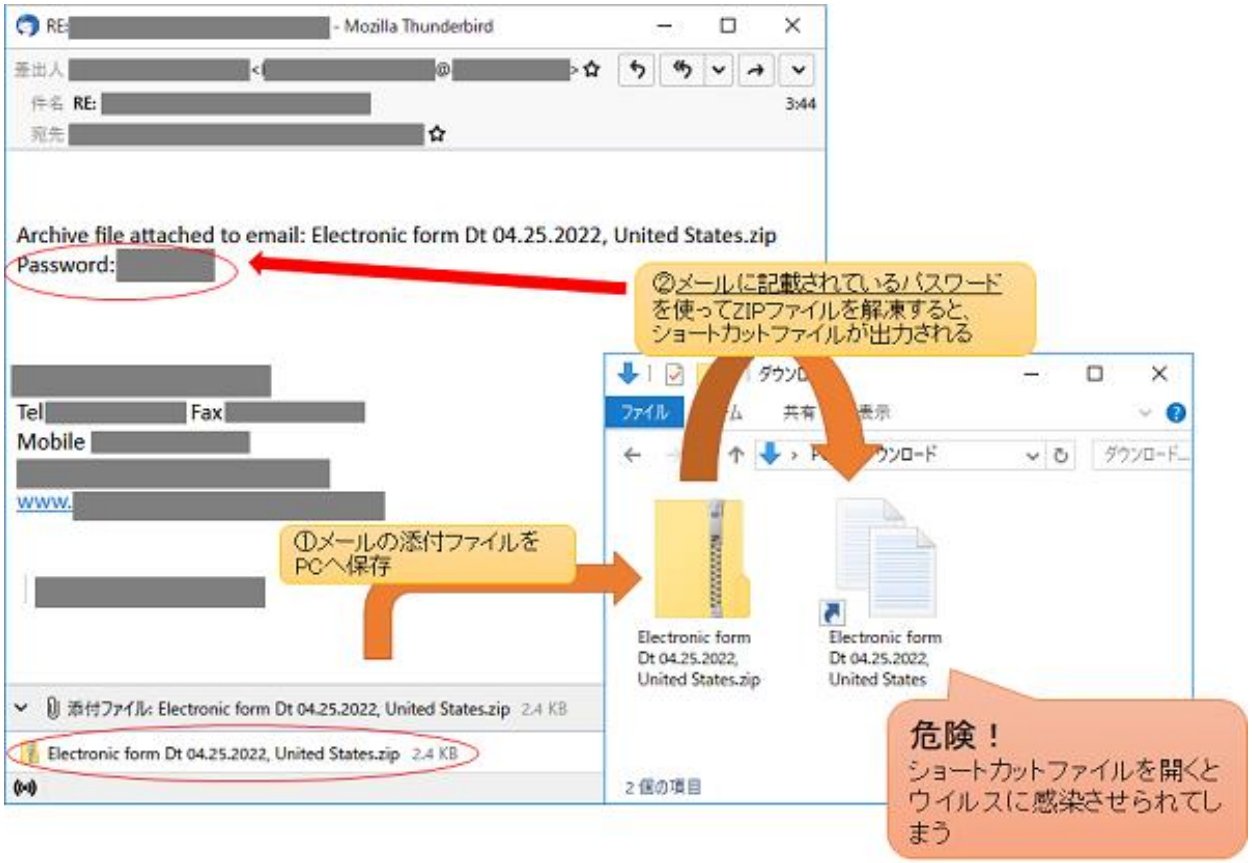


メール本文中のURLから閲覧可能なPDF文書ファイルが存在するかのような偽ページへ誘導
→PDF文書ファイルの閲覧ソフトを装ったウイルスファイルをダウンロードさせる

Emotetへの感染を狙うメールの例③

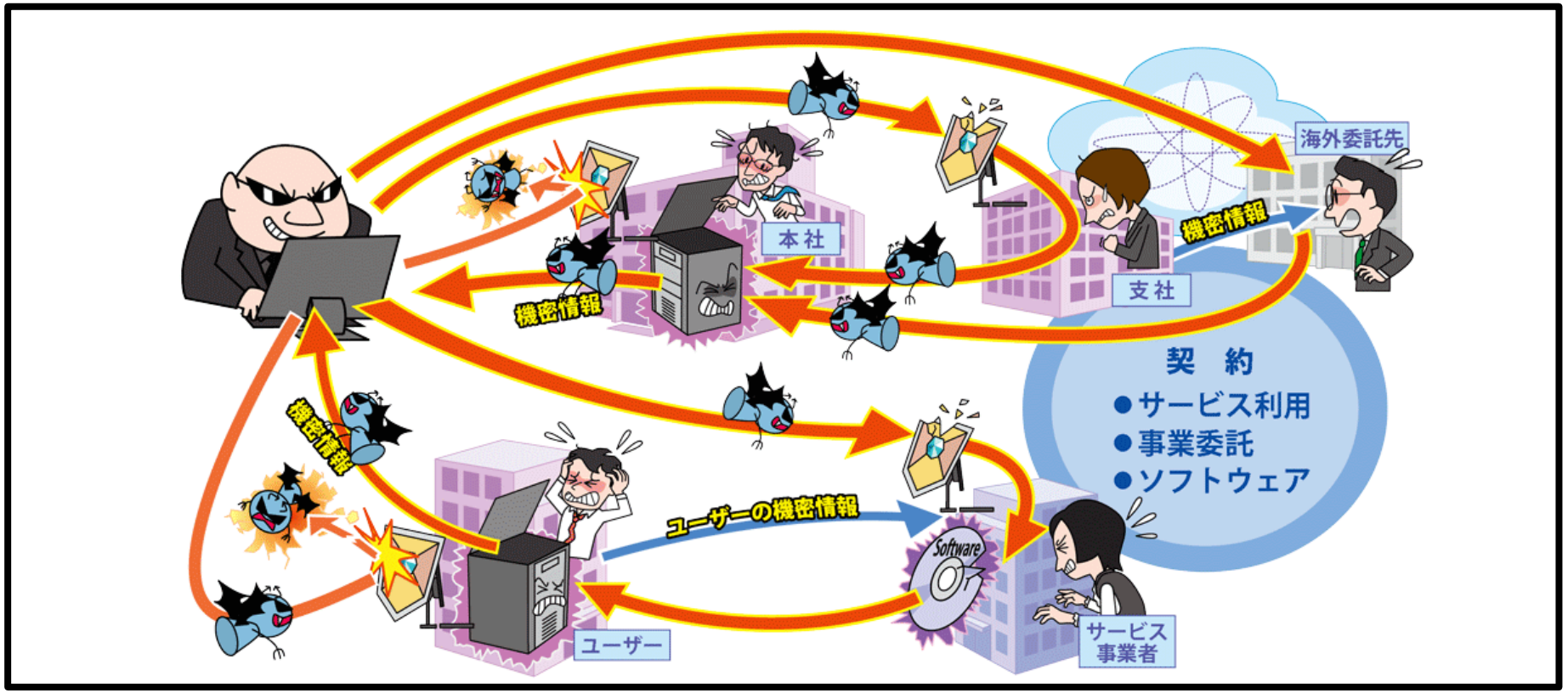
- 2022年4月下旬頃より新しい手口が確認されている

ショートカットファイルを悪用する手口



【組織の脅威：第3位】
サプライチェーンの弱点を悪用した攻撃

【3位】サプライチェーンの弱点を悪用した攻撃



- 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

【3位】サプライチェーンの弱点を悪用した攻撃

- 要因
  - 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
  - 契約における責任が不明確（※1）
    - 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

【3位】サプライチェーンの弱点を悪用した攻撃

- 事例/傾向
  - 業務委託先企業の顧客情報を狙った攻撃（※1）
    - 2021年5月、大手ITベンダーのプロジェクト情報共有ツールが不正アクセスを受け、官公庁を含む顧客から預かった情報の一部が窃取された
    - ツールに複数の脆弱性があったことが原因とされる
    - 多要素認証を実装していない、ログの収集が不十分で不正アクセスの原因や時期が特定できていない等の、セキュリティ対策の問題も指摘されている
    - 当該ツールは廃止が発表されている

【出典】
※1 プロジェクト情報共有ツールへの不正アクセスについて
https://pr.fujitsu.com/jp/news/2021/05/25.html

【3位】サプライチェーンの弱点を悪用した攻撃

- 事例/傾向
  - 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、配信されたアップデートファイルでソフトウェアの更新をした組織が感染
    - その後、攻撃者がバックドアから組織内部に侵入
    - 米政府をはじめ多くの米国組織で感染被害が報告され、日本国内でも感染の形跡が確認されている

【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てみた
https://piyolog.hatenadiary.jp/entry/2020/12/20/045153

【3位】サプライチェーンの弱点を悪用した攻撃

● 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

● 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
    - **・サイバーセキュリティ経営ガイドライン（経済産業省）**
      https://www.meti.go.jp/policy/netsecurity/mng_guide.html
    - **・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/security/keihatsu/sme/guideline/
- **被害を受けた後の対応**
  - －委託元への連絡

【紹介】中小企業の情報セキュリティ対策ガイドライン

● 経営者は、以下の3原則を認識し、対策を進める

原則1 情報セキュリティ対策は経営者のリーダーシップで進める

- 経営者は、IT 活用を推進する中で、情報セキュリティ対策の重要性を認識し、自らリーダーシップを発揮して対策の実施を主導

原則2 委託先の情報セキュリティ対策まで考慮する

- 必要に応じて委託先が実施している情報セキュリティ対策も確認し、不十分な場合は対処を検討

原則3 関係者とは常に情報セキュリティに関するコミュニケーションをとる

- 情報セキュリティに関する取組方針を常日頃より関係者に伝えておくことで、サイバー攻撃によるウイルス感染や情報漏えいなどが発生した際にも、説明責任を果たすことができ、信頼関係を維持することが可能

【紹介】中小企業の情報セキュリティ対策ガイドライン

- 経営者は、以下の7項目を自ら実践するか、実際に情報セキュリティ対策を実践する責任者・担当者に対して指示し、確実に実行することが必要

取組1	情報セキュリティに関する組織全体の対応方針を定める
取組2	情報セキュリティ対策のための予算や人材などを確保する
取組3	必要と考えられる対策を検討させて実行を指示する
取組4	情報セキュリティ対策に関する適宜の見直しを指示する
取組5	緊急時の対応や復旧のための体制を整備する
取組6	委託や外部サービス利用の際にはセキュリティに関する責任を明確にする
取組7	情報セキュリティに関する最新動向を収集する

【組織の脅威：第6位】
脆弱性対策情報の公開に伴う悪用増加

【6位】脆弱性対策情報の公開に伴う悪用増加

- 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化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

● 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

- 脆弱性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期間を狙う

■ 公開されている攻撃ツールを使用

- 脆弱性情報が公開されると短期間で攻撃ツールが作成され、それがインターネット上に出回ると攻撃が活発化する
- 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

IPA

● 事例/傾向

(※1,※2,※3)

■ Javaのログ出力ライブラリ「Apache Log4j」の脆弱性

- 2021年12月9日、多くの組織が利用しているJava製品に組み込まれているログ出力ライブラリ「Apache Log4j」の脆弱性情報が公表された
- リモートから任意のコードを実行されるおそれのある深刻な脆弱性で、「Log4Shell」という別名が付けられた
- 脆弱性情報が公表された翌日にはPOC(実証コード)がネット上に公開され、それを悪用した攻撃が国内外で多数観測された

【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

● 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 (Software Bill Of Materials) の活用
  - －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

【6位】脆弱性対策情報の公開に伴う悪用増加

- 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
      - –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

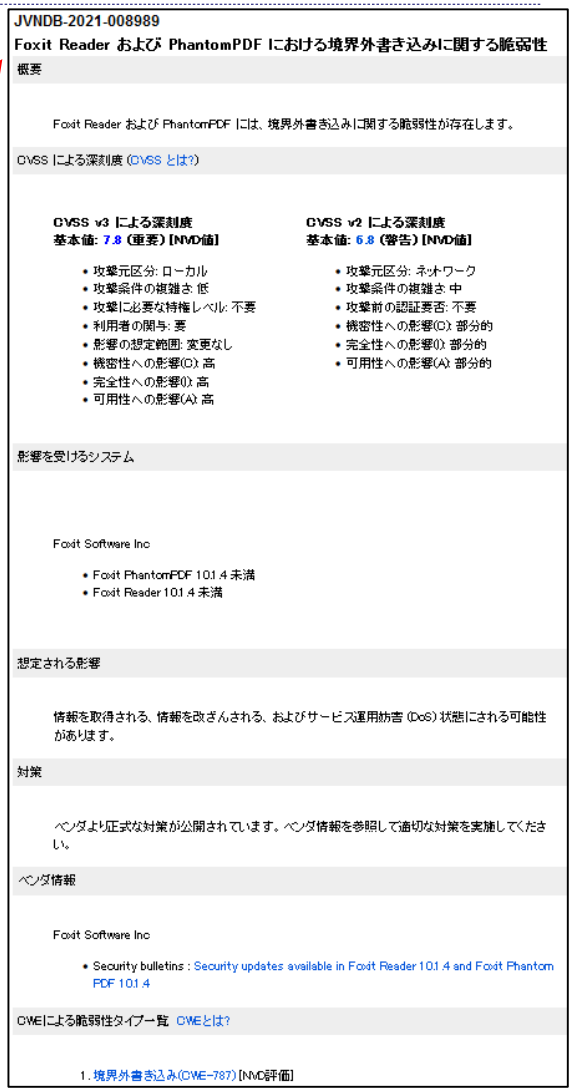
- **参考**

JVN iPedia 脆弱性対策情報データベース

https://jvndb.jvn.jp/index.html

新着情報 RSS データフィード

最終更新日	データベース登録番号	タイトル	CVSSv3
2022/04/01 New	JVNDB-2021-008989	Foxit Reader および PhantomPDF における境界外書き込みに関する脆弱性	7.8（重要）
2022/04/01 New	JVNDB-2021-008988	Foxit Reader および PhantomPDF における例外的な状態の処理に関する脆弱性	5.5（警告）
2022/04/01 New	JVNDB-2021-008987	FortiSandbox における競合状態に関する脆弱性	5.3（警告）
2022/04/01 New	JVNDB-2021-008986	FortiMail における古典的バッファオーバーフローの脆弱性	8.8（重要）
2022/04/01 New	JVNDB-2021-008985	FortiMail における SQL インジェクションの脆弱性	9.8（緊急）
2022/04/01 New	JVNDB-2021-008984	FortiMail における暗号強度に関する脆弱性	9.8（緊急）


JVNDB-2021-008989

Foxit Reader および PhantomPDF における境界外書き込みに関する脆弱性

概要

Foxit Reader および PhantomPDF には、境界外書き込みに関する脆弱性が存在します。

CVSS による深刻度 (CVSS とは?)

CVSS v3 による深刻度
基本値: 7.8 (重要) [NVD値]
- 攻撃元区分: ローカル
- 攻撃条件の複雑さ: 低
- 攻撃に必要な特権レベル: 不要
- 利用者の関与: 要
- 影響の想定範囲: 変更なし
- 機密性への影響(C): 高
- 完全性への影響(I): 高
- 可用性への影響(A): 高

CVSS v2 による深刻度
基本値: 6.8 (警告) [NVD値]
- 攻撃元区分: ネットワーク
- 攻撃条件の複雑さ: 中
- 攻撃前の認証要否: 不要
- 機密性への影響(C): 部分的
- 完全性への影響(I): 部分的
- 可用性への影響(A): 部分的

影響を受けるシステム

Foxit Software Inc
- Foxit PhantomPDF 10.1.4 未満
- Foxit Reader 10.1.4 未満

想定される影響

情報を取得される、情報を改ざんされる、およびサービス運用妨害 (DoS) 状態にされる可能性があります。

対策

ベンダより正式な対策が公開されています。ベンダ情報を参照して適切な対策を実施してください。

ベンダ情報

Foxit Software Inc
- Security bulletins : Security updates available in Foxit Reader 10.1.4 and Foxit Phantom PDF 10.1.4

CWEによる脆弱性タイプ一覧 CWEとは?

1. 境界外書き込み(CWE-787) [NVD評価]

- 米国の脆弱性情報データベースや国内ベンダ等から収集した14.6万件以上（2022年8月末時点）の脆弱性対策情報を日本語で公開
- 製品名などのキーワードで検索可能

【6位】脆弱性対策情報の公開に伴う悪用増加

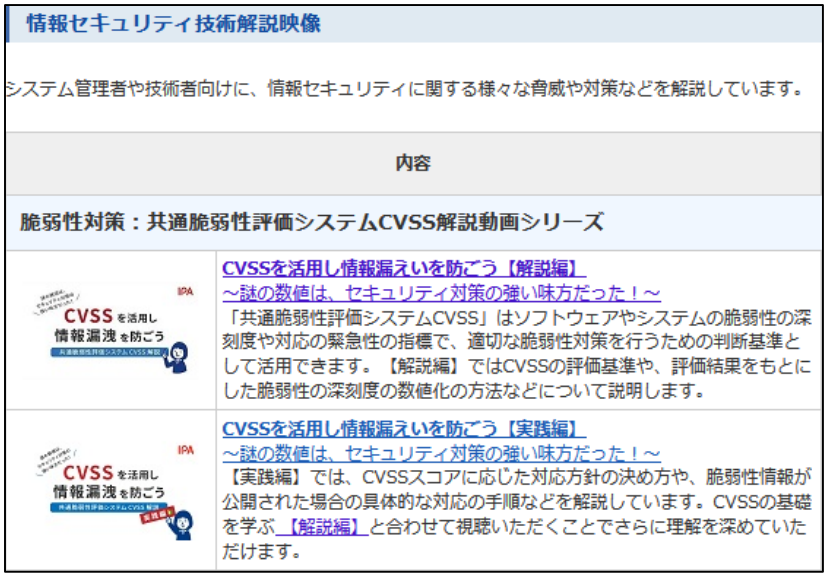
- **参考**

共通脆弱性評価システムCVSS解説動画シリーズ

https://www.ipa.go.jp/security/keihatsu/videos/

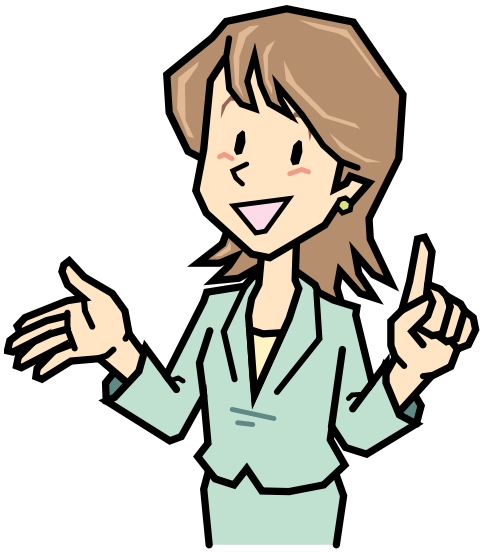
CVSS（共通脆弱性評価システム）

- 脆弱性に対する汎用的な評価指標
- 脆弱性の深刻度を0.0～10.0で数値化
- 収集した脆弱性情報の深刻度評価、対応の優先順位決定等に活用できる



IPA YouTubeチャンネル
で公開中！！

情報セキュリティ対策の基本



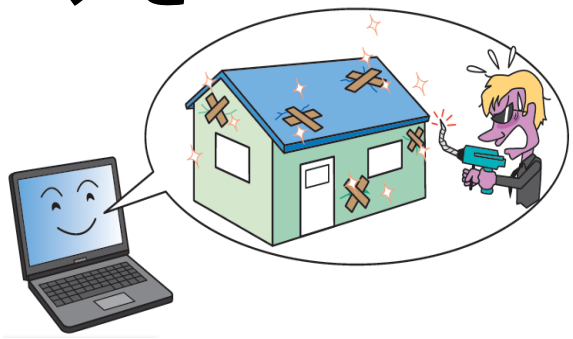
情報セキュリティ対策の基本

- 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

ソフトウェアの更新

- ソフトウェアが持つ脆弱性は、ソフトウェアを更新して根本的に解消する
- 継続的な脆弱性対策情報の収集



■例えばウェブサーバー管理者は・・・

・ウェブサーバー関連ソフトウェアの更新
（Apache、WordPressなど）

■例えば一般ユーザーは・・・

・OSや主にインターネット関連のソフトウェアを更新
（Windows、Adobe、Javaなど）

セキュリティソフトの利用

- ウイルス対策機能でウイルスの感染を未然に防ぐ
- ファイアウォール機能で不正な通信をブロックする

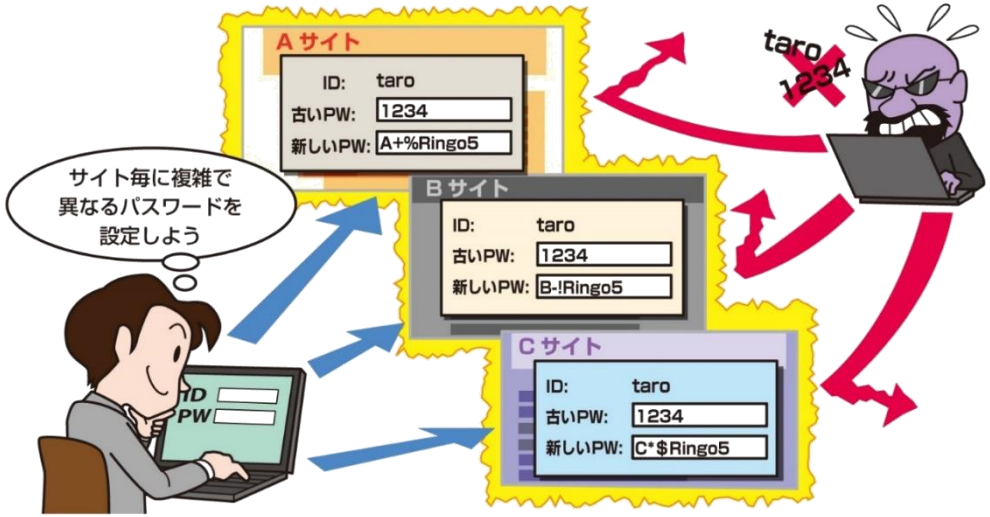
■例えばWindowsユーザーは・・・

・最低限Windows標準のセキュリティ機能は有効にする
（Windows Defenderなど）

・その他市販のセキュリティソフトの利用も検討

パスワードの管理・認証の強化

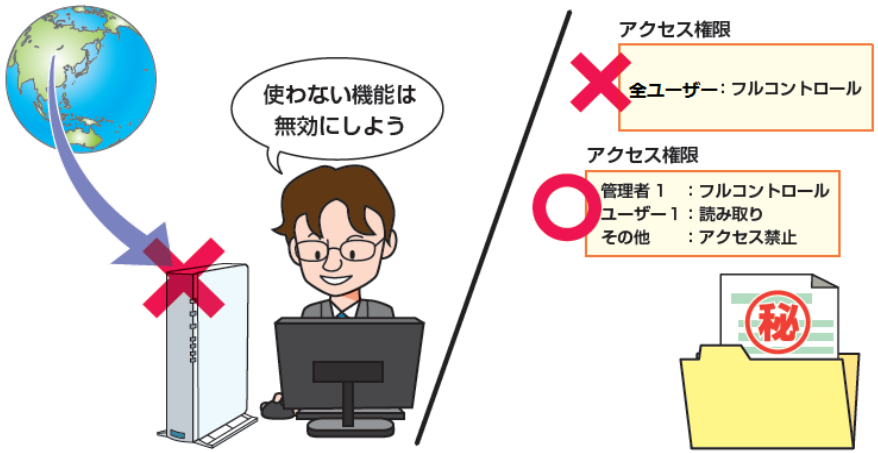
- 推測されにくいパスワードを設定（長く複雑に）
- 複数のインターネットサービスでパスワードを使い回さない
- 二要素認証等、強い認証方式が利用できれば利用する



■長く複雑なパスワードを複数管理するのは大変・・・
・パスワード管理ソフトの利用も検討

設定の見直し

利用する機器やソフトの仕様を理解して適切に運用する



■例えば・・・

- 不要な設定（機能）は無効にする
- 初期パスワードのまま使用しない
- ソフトウェア更新の自動化

脅威・手口を知る

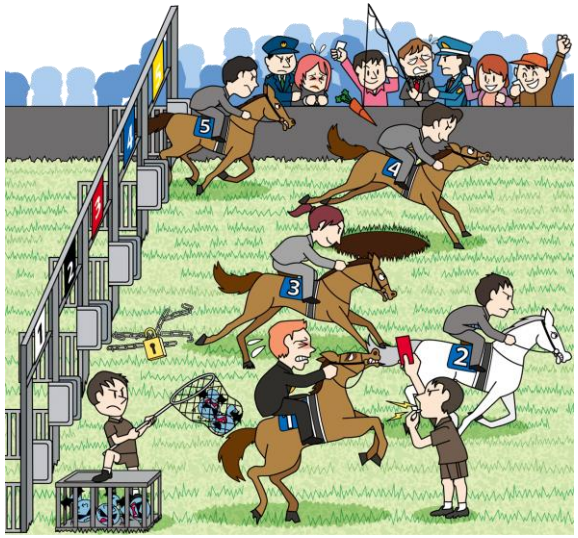
- 公的機関の注意喚起やニュースなどから脅威の手口に関する情報を収集
- 変化する手口を理解して適切な対策を実践

■日々脅威に関する情報を収集するのは大変・・・
- 注意喚起や情報発信しているSNSアカウントのフォロー
- メールマガジンの登録

情報セキュリティ10大脅威 2022

- 以下のWebページに資料を公開しています

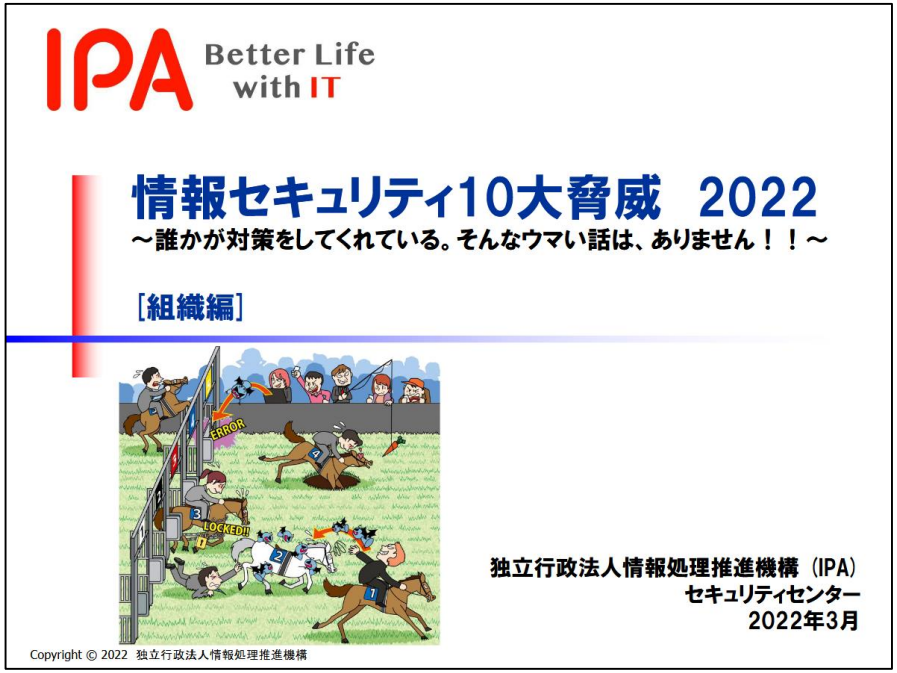
情報セキュリティ10大脅威 2022
https://www.ipa.go.jp/security/vuln/10threats2022.html



情報セキュリティ10大脅威 2022

- 以下のWebページに資料を公開しています

「情報セキュリティ10大脅威 2022」簡易説明資料/スライド形式
https://www.ipa.go.jp/files/000096898.pdf



IPA

IPA Better Life with IT

ありがとうございました