IPA Better Life with IT

ICT-ISACオープンセミナー

情報セキュリティ10大脅威 2022から

～サプライチェーンの弱点を悪用した攻撃～

2022年7月22日
（独）情報処理推進機構（IPA）
セキュリティセンター
土屋　正

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

「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

個人の10大脅威	順位	組織の10大脅威
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	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	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

10大脅威（組織）［2021→2022］

順位	2021	変動	2022	順位
1	ランサムウェアによる被害	→	ランサムウェアによる被害	1
2	標的型攻撃による機密情報の窃取	→	標的型攻撃による機密情報の窃取	2
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	↘↗	サプライチェーンの弱点を悪用した攻撃	3
4	サプライチェーンの弱点を悪用した攻撃	↗↘	テレワーク等のニューノーマルな働き方を狙った攻撃	4
5	ビジネスメール詐欺による金銭被害	↗↘	内部不正による情報漏えい	5
6	内部不正による情報漏えい	↗↘	脆弱性対策情報の公開に伴う悪用増加	6
7	予期せぬIT基盤の障害に伴う業務停止	↘↗	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	7
8	インターネット上のサービスへの不正ログイン	↘↗	ビジネスメール詐欺による金銭被害	8
9	不注意による情報漏えい等の被害	↘↗	予期せぬIT基盤の障害に伴う業務停止	9
10	脆弱性対策情報の公開に伴う悪用増加	↘↗	不注意による情報漏えい等の被害	10
		↘	ランク外	

情報セキュリティ10大脅威 2022

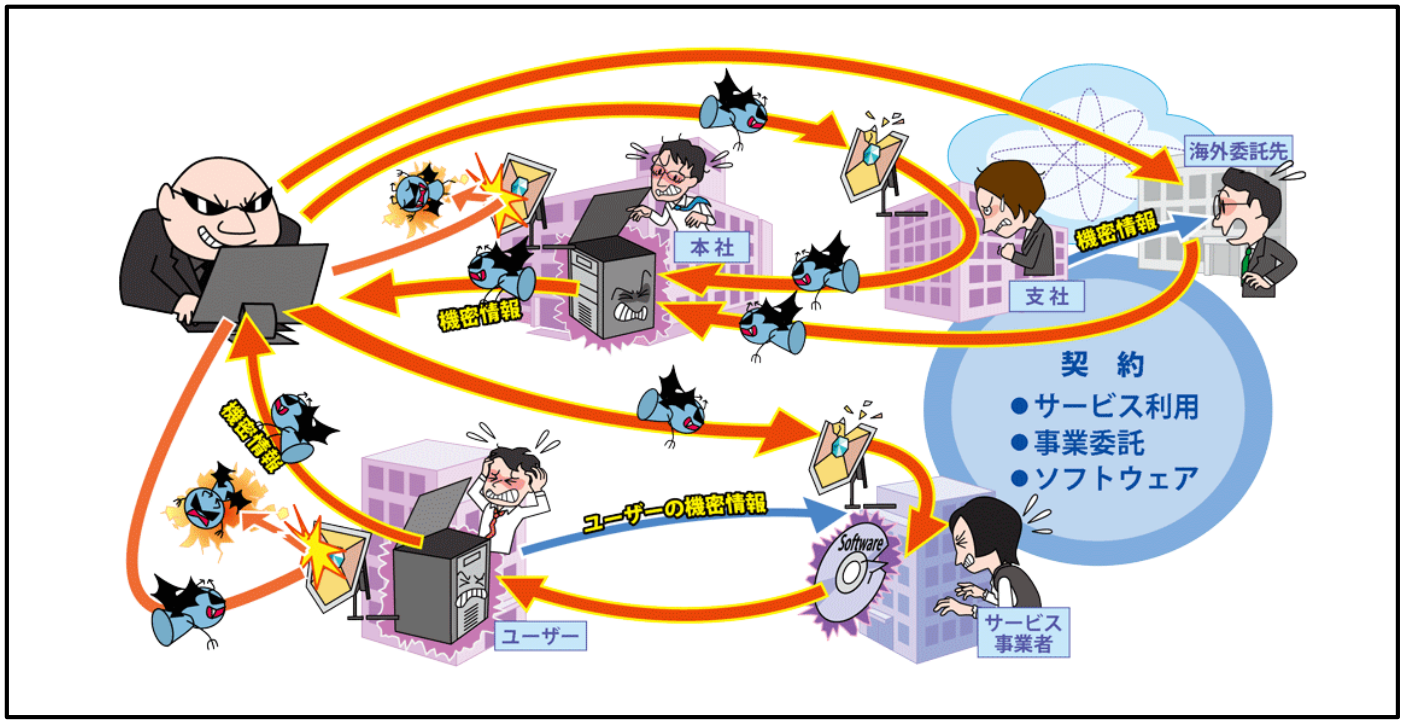
順位	組織の10大脅威
1	ランサムウェアによる被害
2	標的型攻撃による機密情報の窃取
3	**サプライチェーンの弱点を悪用した攻撃**
4	テレワーク等のニューノーマルな働き方を狙った攻撃
5	内部不正による情報漏えい
6	脆弱性対策情報の公開に伴う悪用増加
7	修正プログラムの公開前を狙う攻撃 （ゼロデイ攻撃）
8	ビジネスメール詐欺による金銭被害
9	予期せぬIT基盤の障害に伴う業務停止
10	不注意による情報漏えい等の被害

【組織 3位】
サプライチェーンの弱点を悪用した攻撃

10大脅威（組織）の変遷

	10大脅威 2018	10大脅威 2019	10大脅威2020	10大脅威2021	10大脅威2022
1位	標的型攻撃による被害	標的型攻撃による被害	標的型攻撃による 機密情報の窃取	ランサムウェアによる被害	ランサムウェアによる被害
2位	ランサムウェアによる被害	ビジネスメール詐欺による 被害	内部不正による情報漏えい	標的型攻撃による 機密情報の窃取	標的型攻撃による 機密情報の窃取
3位	ビジネスメール詐欺による 被害	ランサムウェアによる被害	ビジネスメール詐欺による 金銭被害	テレワーク等のニューノーマルな働き方を狙った攻撃	サプライチェーンの弱点を悪用した攻撃
4位	脆弱性対策情報の公開に伴う悪用増加	サプライチェーンの弱点を悪用した攻撃の高まり	サプライチェーンの弱点を悪用した攻撃	サプライチェーンの弱点を悪用した攻撃	テレワーク等のニューノーマルな働き方を狙った攻撃
5位	脅威に対応するための セキュリティ人材の不足	内部不正による情報漏えい	ランサムウェアによる被害	ビジネスメール詐欺による 金銭被害	内部不正による情報漏えい
6位	ウェブサービスからの 個人情報の窃取	サービス妨害攻撃による サービスの停止	予期せぬIT基盤の障害に 伴う業務停止	内部不正による情報漏えい	脆弱性対策情報の公開に 伴う悪用増加
7位	IoT機器の脆弱性の顕在化	インターネットサービスから の個人情報の窃取	不注意による情報漏えい	予期せぬIT基盤の障害に 伴う業務停止	修正プログラムの公開前を 狙う攻撃（ゼロデイ攻撃）
8位	内部不正による情報漏えい	IoT機器の脆弱性の顕在化	インターネット上のサービス からの個人情報の窃取	インターネット上のサービス への不正ログイン	ビジネスメール詐欺による 金銭被害
9位	サービス妨害攻撃による サービスの停止	脆弱性対策情報の公開に 伴う悪用増加	IoT機器の不正利用	不注意による情報漏えい等 の被害	予期せぬIT基盤の障害に 伴う業務停止
10位	犯罪のビジネス化（アンダー グラウンドサービス）	不注意による情報漏えい	サービス妨害攻撃による サービスの停止	脆弱性対策情報の公開に 伴う悪用増加	不注意による情報漏えい等 の被害

【組織 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

攻撃される要因

- 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

攻撃の手口

- 取引先や委託先が保有する機密情報を狙う
- ソフトウェア開発元やMSP等を攻撃して
  標的を攻撃するための足掛かりとする

※MSP：Managed Service Provider
企業システムの運用・監視などを請け負う事業者

攻撃事例（その１）

子会社や海外拠点を狙った攻撃 (※1) (※2)

- 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 当社グループの米国子会社に対するサイバー攻撃について（HOYA 株式会社）
https://www.hoya.com/wp-content/uploads/2022/03/30.pdf

※2 HOYAの米国のシステムにランサムウエア攻撃－ハッカー集団（ブルームバーグ L.P.）
https://www.bloomberg.co.jp/news/articles/2021-04-21/QRWN3GT0G1LM01

攻撃事例（その2）

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

攻撃事例（その3）

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

組織における対策

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

商流に関わる組織における対策

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/

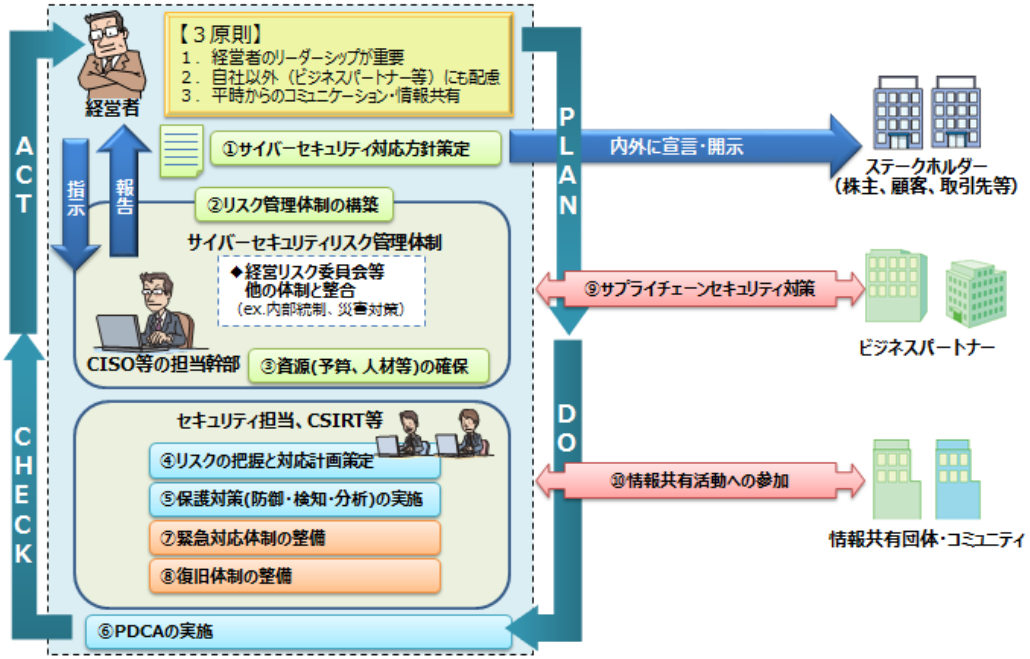
- 被害を受けた後の対応

–委託元への連絡

サイバーセキュリティ経営ガイドライン

- 経営者が認識する必要のある「3原則」
- 経営者が情報セキュリティ対策を実施する上で指示すべき「重要10項目」

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

情報処理推進機構(IPA)
https://www.ipa.go.jp/security/keihatsu/sme/guideline/

- 情報セキュリティ対策の必要性、情報を安全に管理する具体的な手順等を分かりやすい言葉で示したガイドライン
- 経営者が認識すべき「3原則」、実行すべき「重要7項目の取組」を記載
- サンプルを参考に、自社のセキュリテイ規程を作成できる

中小企業の情報セキュリティ対策ガイドライン

IPA

- 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

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

「10大脅威」資料のご紹介

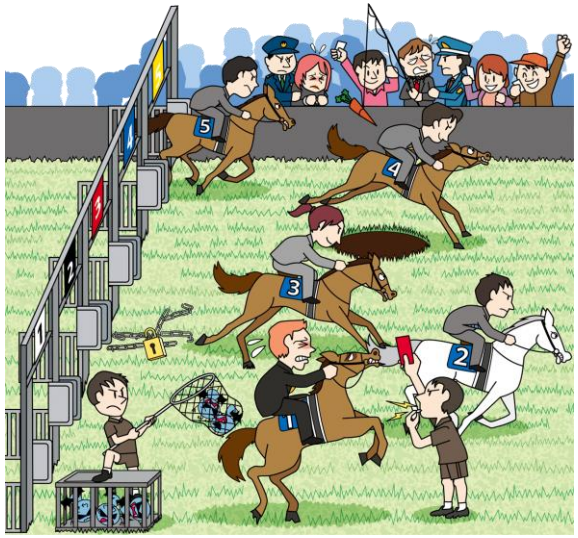
情報セキュリティ10大脅威 2022

- IPAの10大脅威ページに各種資料を公開しています
- ページ内には過去の10大脅威へのリンクもあります

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

ネットで検索！

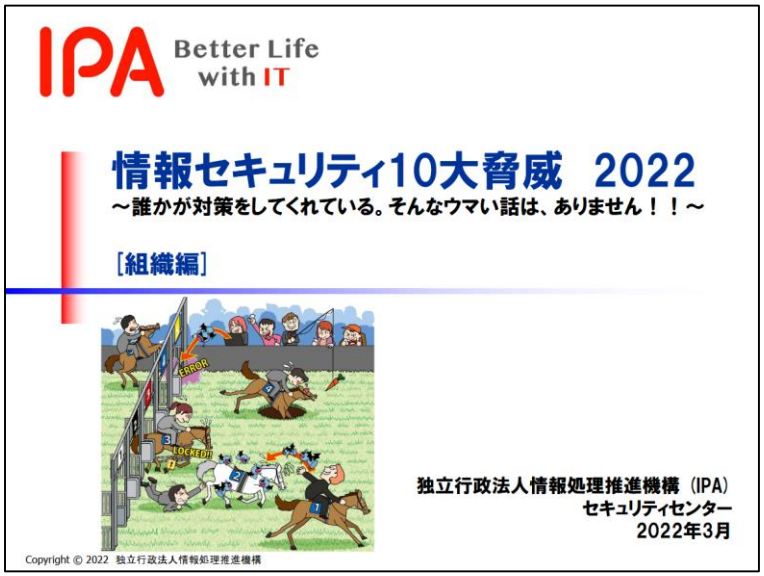
10大脅威2022



情報セキュリティ10大脅威 2022

- スライド形式の 簡易解説資料 を公開しています
  社内研修等にご利用ください

「情報セキュリティ10大脅威 2022」[組織編]（スライド形式）
https://www.ipa.go.jp/files/000096898.pdf



情報セキュリティ10大脅威 2022

- 簡易解説資料の 英語版 も公開しています
  こちらも社内研修等にご利用ください

「情報セキュリティ10大脅威 2022」[組織編]（英語版）
https://www.ipa.go.jp/files/000099785.pdf