Information-technology
Promotion
Agency, Japan

脆弱性対策の動向と効果的な収集に向けて

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
寺田真敏
2025年03月27日

セミナー概要

脆弱性を悪用したセキュリティインシデントに対応するため、対策の基盤を実現する技術仕様も、いろいろな取り組みが進められています。本セミナーでは、脆弱性対策の動向として、脆弱性の動向、米国政府の取り組み、IPAの取り組みを紹介するとともに、脆弱性対策基盤を実現する技術仕様を紹介します。

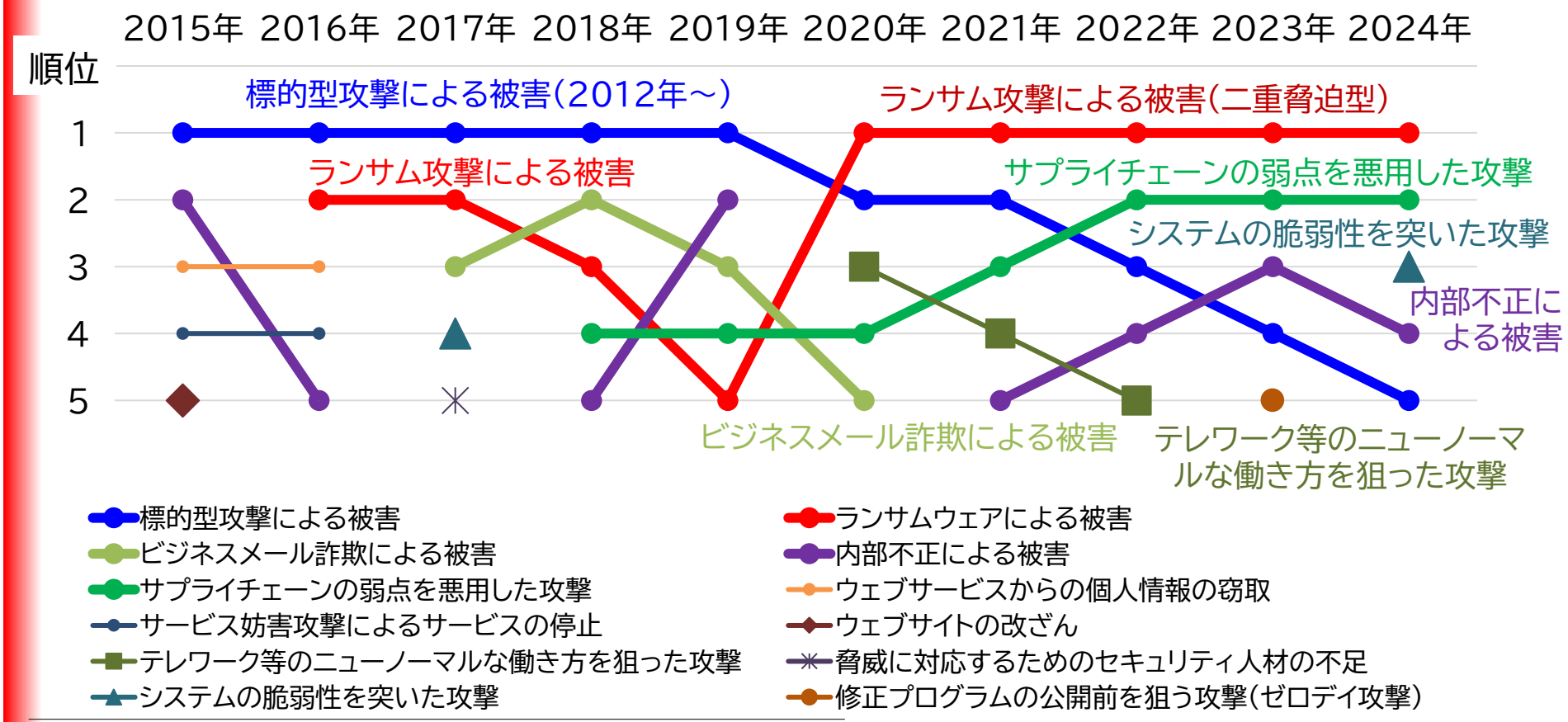
1. トピック[1]
2. 情報収集に役立つ技術仕様
3. 自動化(機械化)処理基盤の潮流
4. JVN脆弱性対策機械処理基盤
5. トピック[2]

トピック[1]

情報セキュリティ10大脅威

情報セキュリティ10大脅威 2025

- 社会的に影響が大きいと考える情報セキュリティにおける事案から選出



［出典］　情報セキュリティ10大脅威 2025
https://www.ipa.go.jp/security/10threats/10threats2025.html

情報セキュリティ10大脅威 2025

- 社会的に影響が大きいと考える情報セキュリティにおける事案から選出

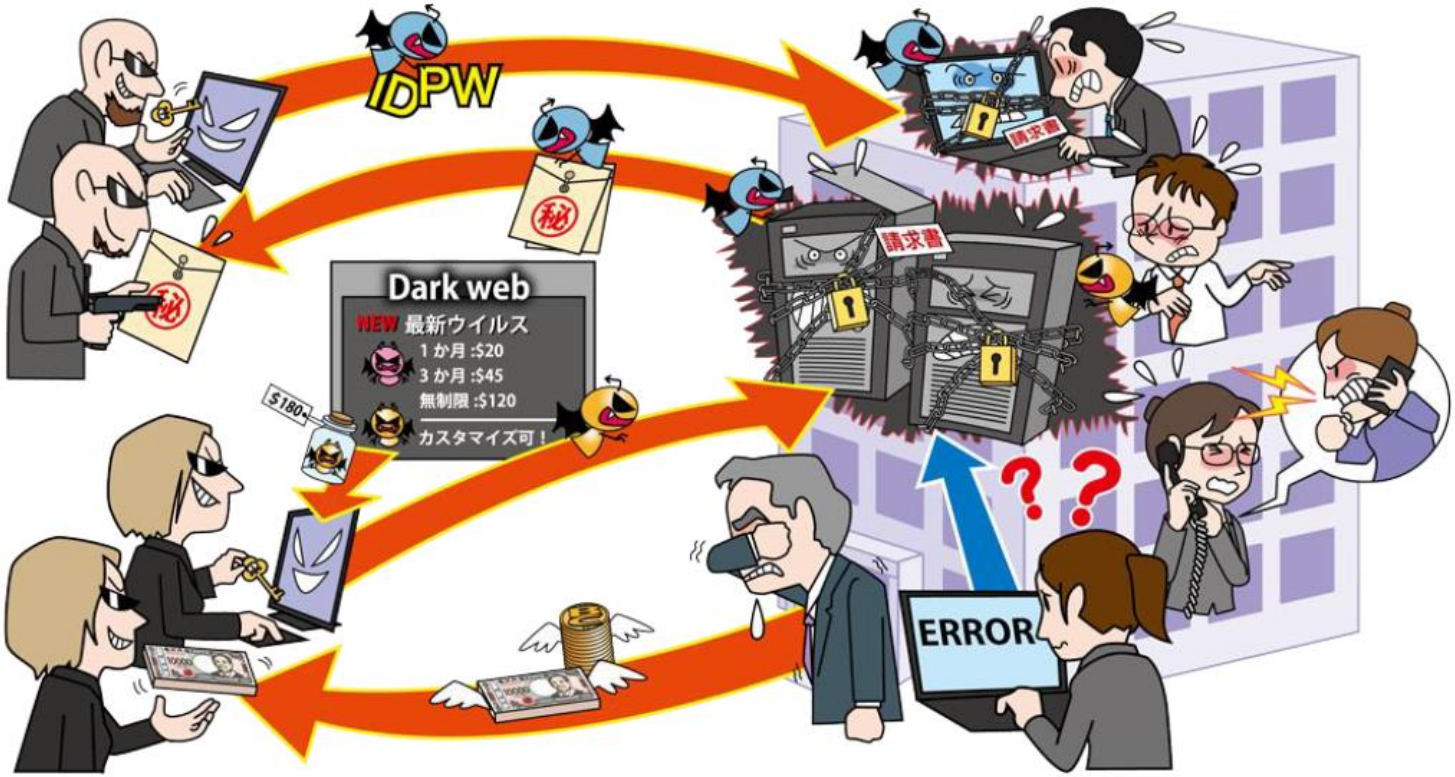
個人
インターネット上のサービスからの個人情報の窃取
インターネット上のサービスへの不正ログイン
クレジットカード情報の不正利用
スマホ決済の不正利用
偽警告によるインターネット詐欺
ネット上の誹謗・中傷・デマ
フィッシングによる個人情報等の詐取
不正アプリによるスマートフォン利用者への被害
メールやSMS等を使った脅迫・詐欺の手口による金銭要求
ワンクリック請求等の不当請求による金銭被害

順位	組織
1位	ランサム攻撃による被害
2位	サプライチェーンや委託先を狙った攻撃
3位	システムの脆弱性を突いた攻撃
4位	内部不正による情報漏えい等
5位	機密情報等を狙った標的型攻撃
6位	リモートワーク等の環境や仕組みを狙った攻撃
7位	地政学的リスクに起因するサイバー攻撃
8位	分散型サービス妨害攻撃（DDoS攻撃）
9位	ビジネスメール詐欺
10位	不注意による情報漏えい等

［出典］　情報セキュリティ10大脅威 2025
https://www.ipa.go.jp/security/10threats/10threats2025.html

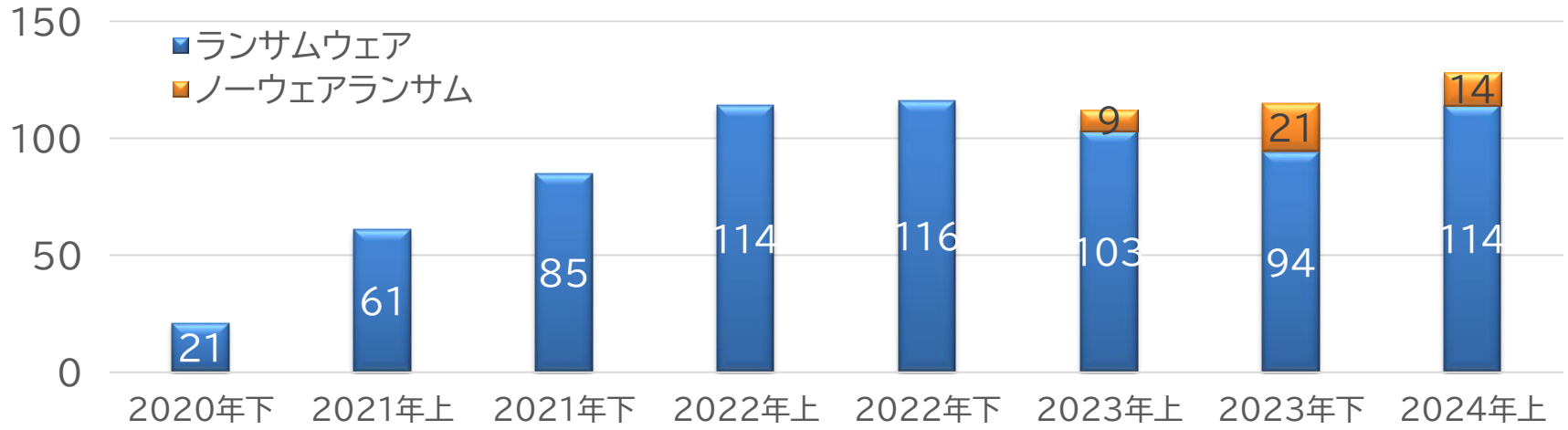
情報セキュリティ10大脅威 2025
ランサム攻撃による被害

- 変わらず続く脅威、リスクを見つけて対策を
  - 二重脅迫：データの暗号化、窃取情報の暴露
  - 四重脅迫：データの暗号化、窃取情報の暴露、DDoS攻撃（予告）、攻撃を受けていることの暴露（顧客やビジネスパートナーからの信用失墜）



ランサム攻撃による被害
報告件数の推移

- 企業・団体等におけるランサムウェア被害の報告件数の推移

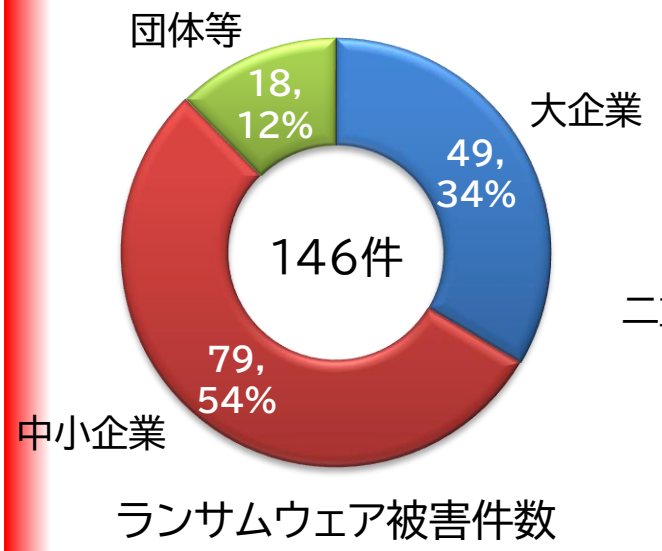


- 2021年～2024年上半期のランサムウェア被害の特徴
  - 二重恐喝(ダブルエクストーション)による被害が多くを占める
  - 暗号資産による金銭の要求が多くを占める
  - 企業・団体等の規模や業種を問わず被害が発生
  - 感染経路は、テレワークにも利用される機器等の脆弱性や強度の弱い認証情報等を利用して侵入したと考えられるものが大半を占めている

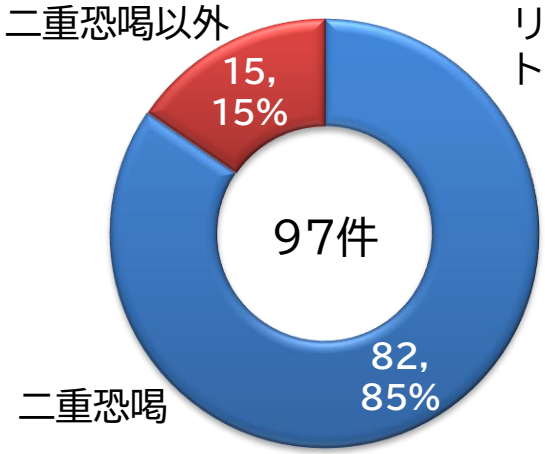
［出典］　令和6年上半期におけるサイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf

ランサム攻撃による被害
被害の状況

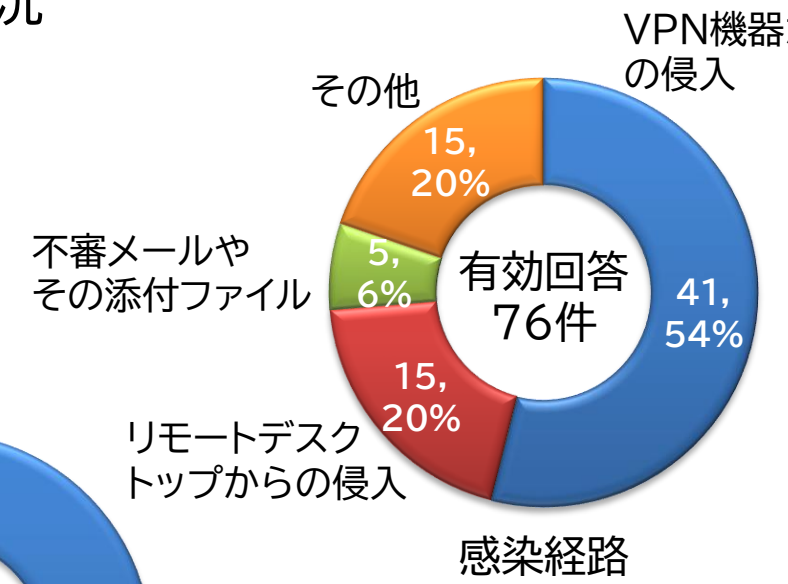
- 2021年のランサムウェア被害の状況



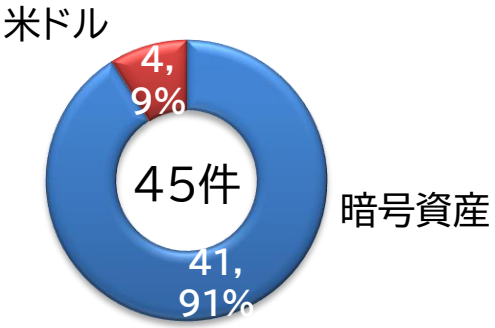
ランサムウェア被害件数



手口を確認できた被害



感染経路

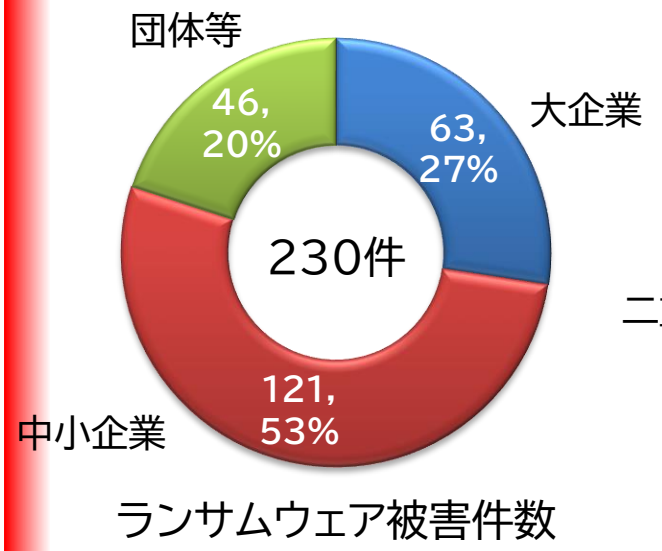


直接的な金銭要求あり

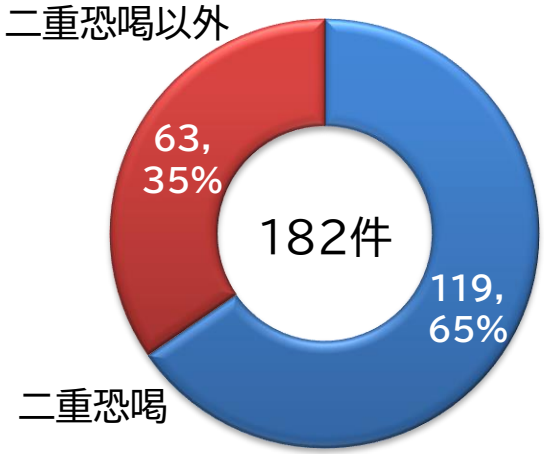
［出典］　令和3年におけるサイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf

ランサム攻撃による被害
被害の状況

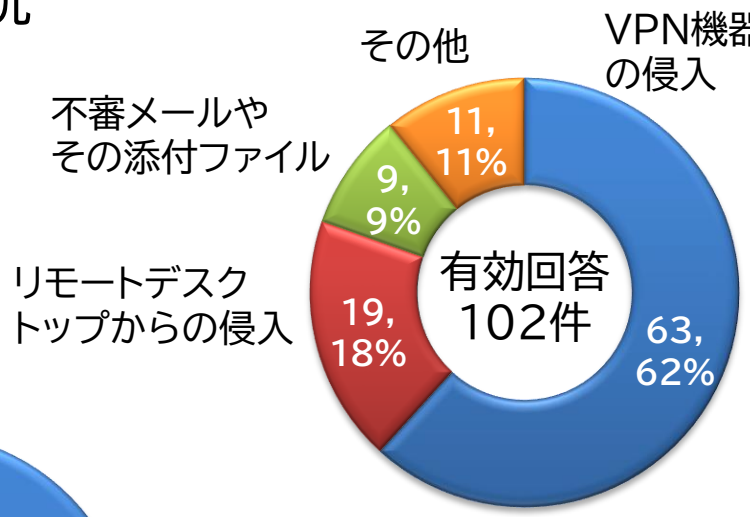
- 2022年のランサムウェア被害の状況



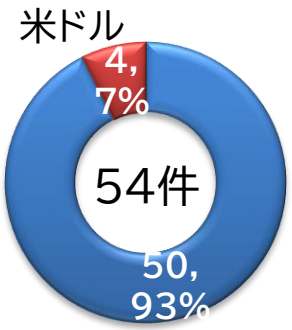
ランサムウェア被害件数



手口を確認できた被害



感染経路

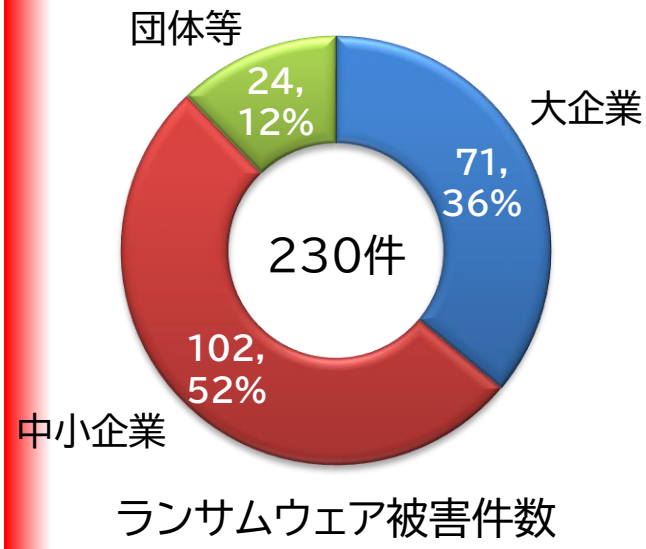


直接的な金銭要求あり

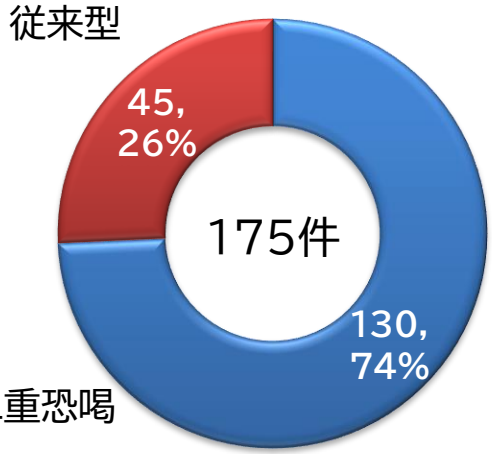
［出典］　令和4年におけるサイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf

ランサム攻撃による被害
被害の状況

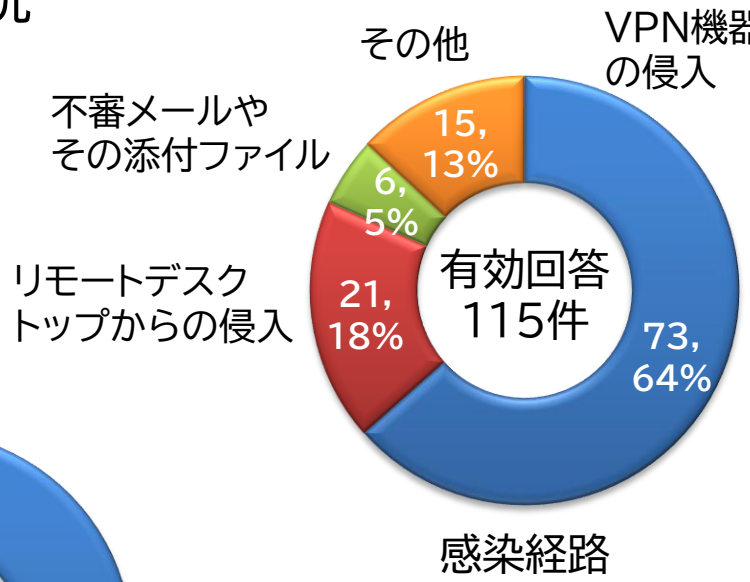
- 2023年のランサムウェア被害の状況



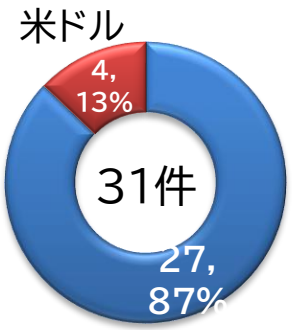
ランサムウェア被害件数



手口を確認できた被害



感染経路

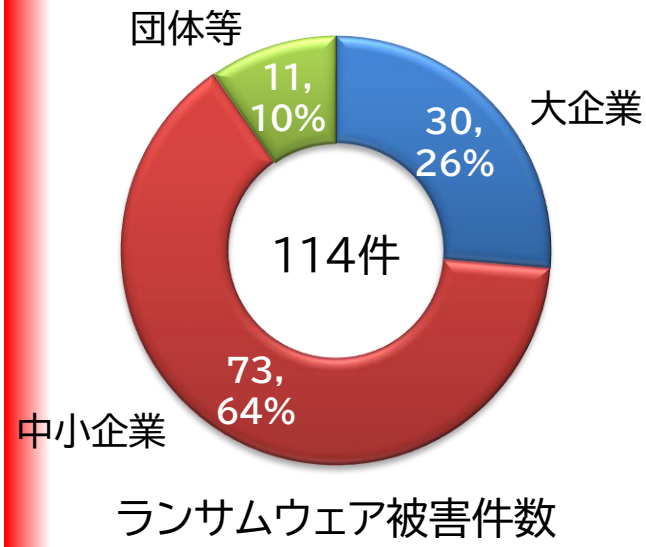


直接的な金銭要求あり

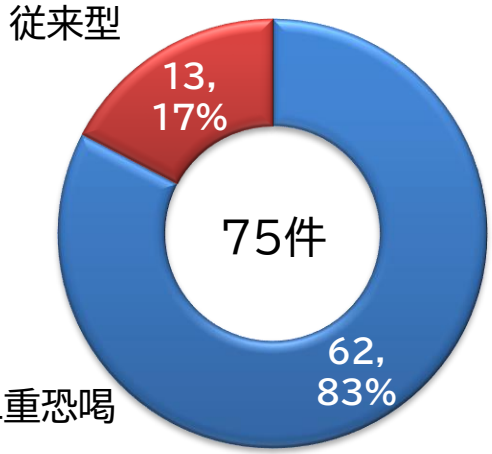
［出典］　令和5年におけるサイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf

ランサム攻撃による被害
被害の状況

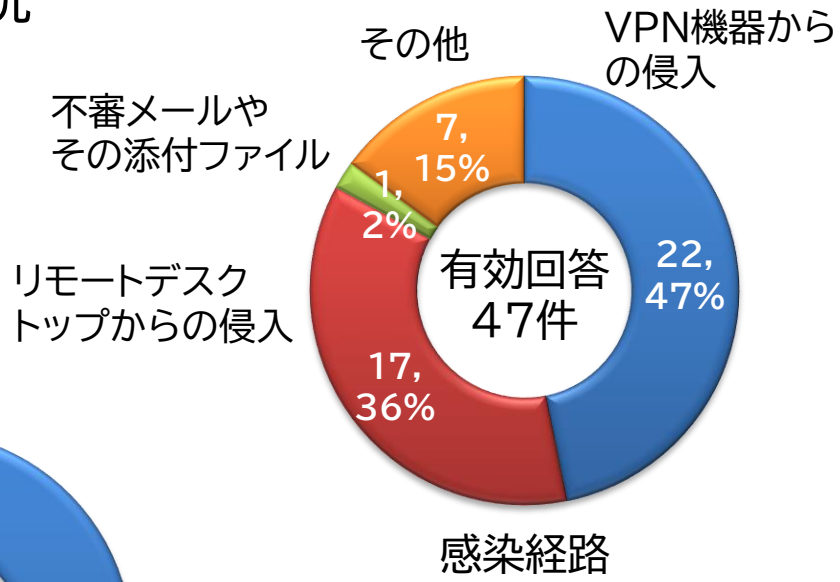
- 2024年のランサムウェア被害の状況



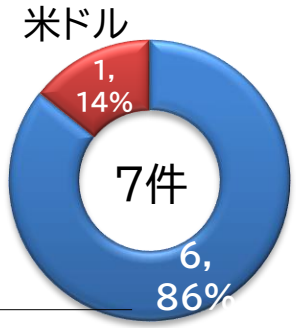
ランサムウェア被害件数



手口を確認できた被害



感染経路

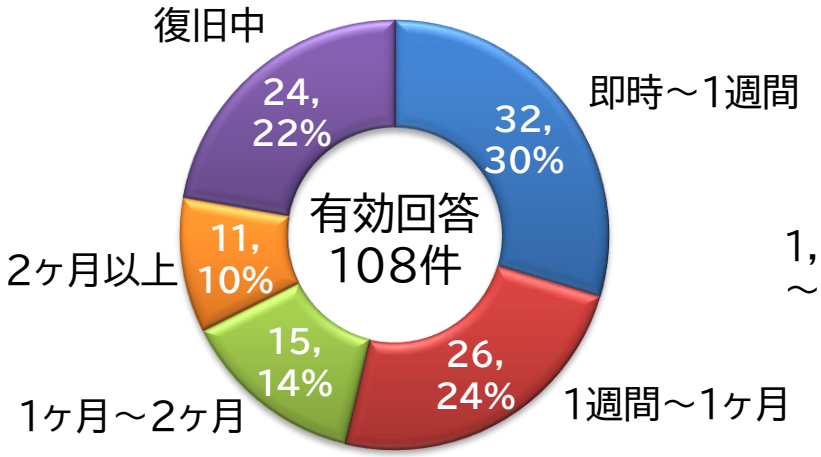


直接的な金銭要求あり

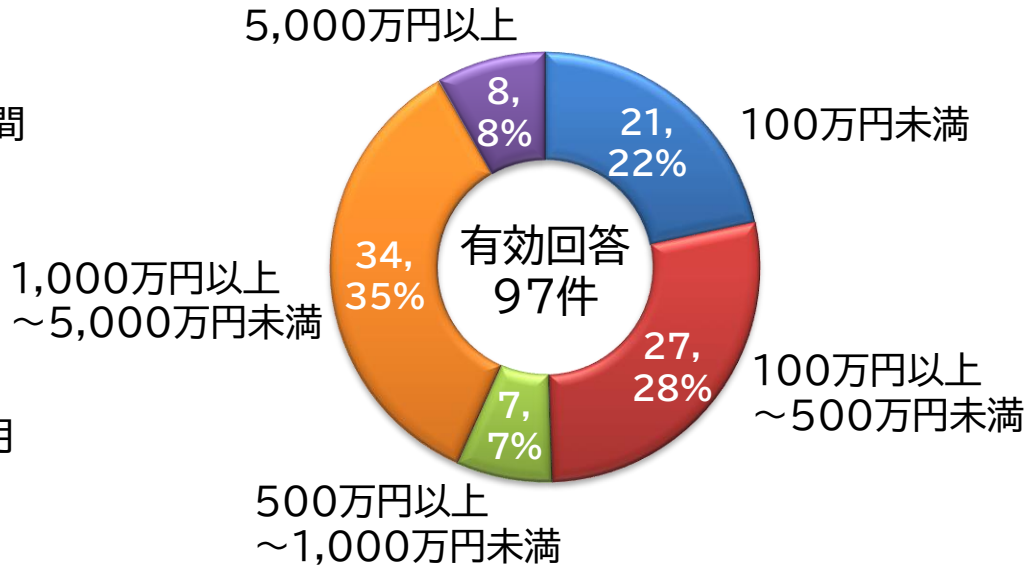
［出典］　令和6年上半期におけるサイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf

ランサム攻撃による被害
復旧等に要した期間・費用

- 2021年のランサムウェア被害の復旧等に要した期間・費用



復旧に要した期間

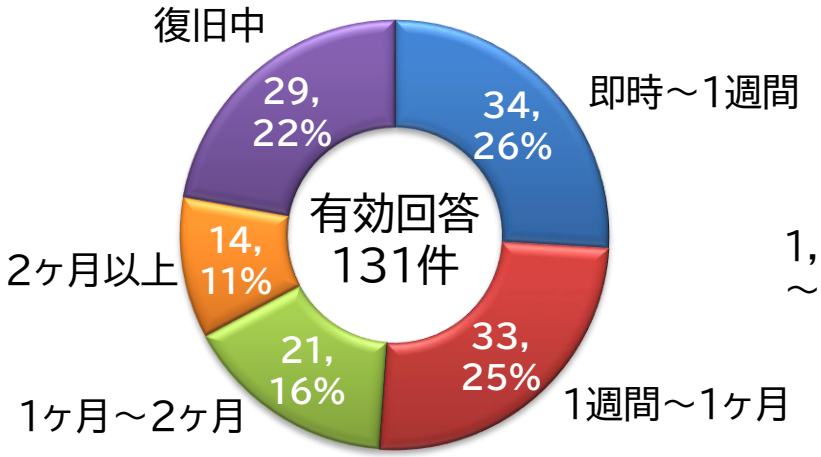


調査・復旧費用の総額

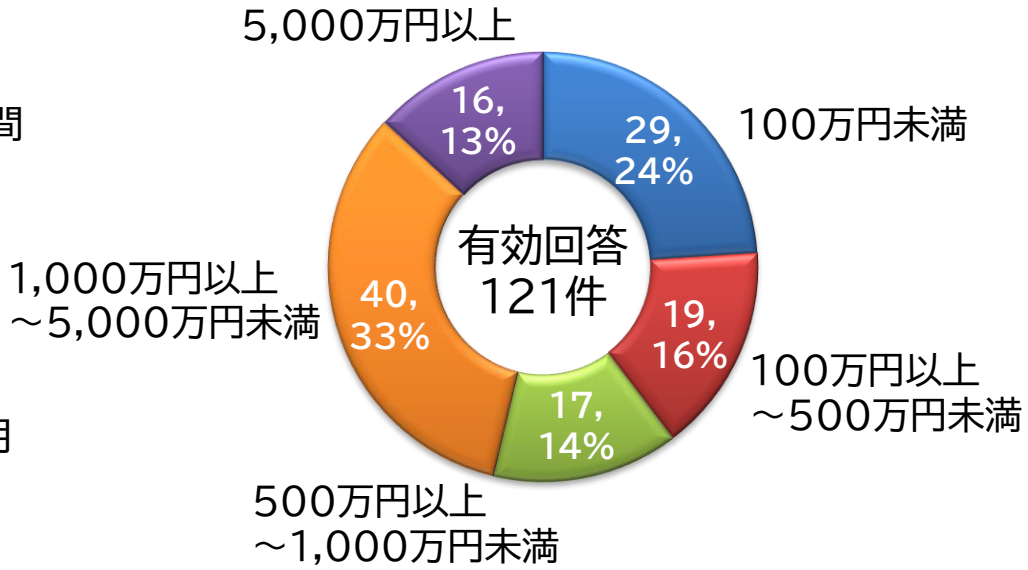
［出典］　令和3年におけるサイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf

ランサム攻撃による被害
復旧等に要した期間・費用

- 2022年のランサムウェア被害の復旧等に要した期間・費用



復旧に要した期間

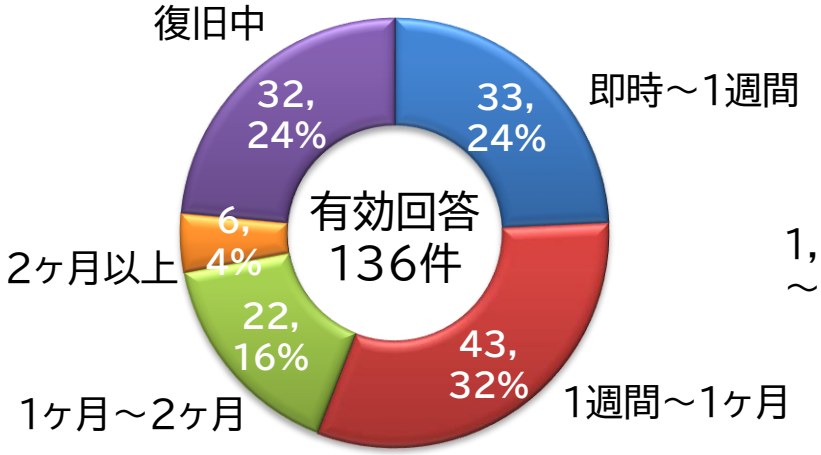


調査・復旧費用の総額

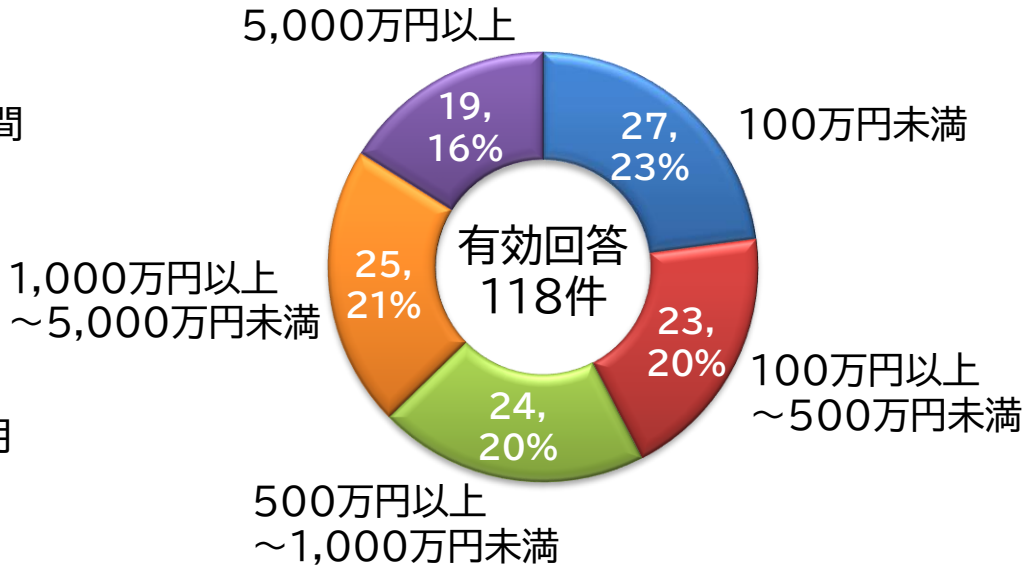
［出典］　令和4年におけるサイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf

ランサム攻撃による被害
復旧等に要した期間・費用

- 2023年のランサムウェア被害の復旧等に要した期間・費用



復旧に要した期間

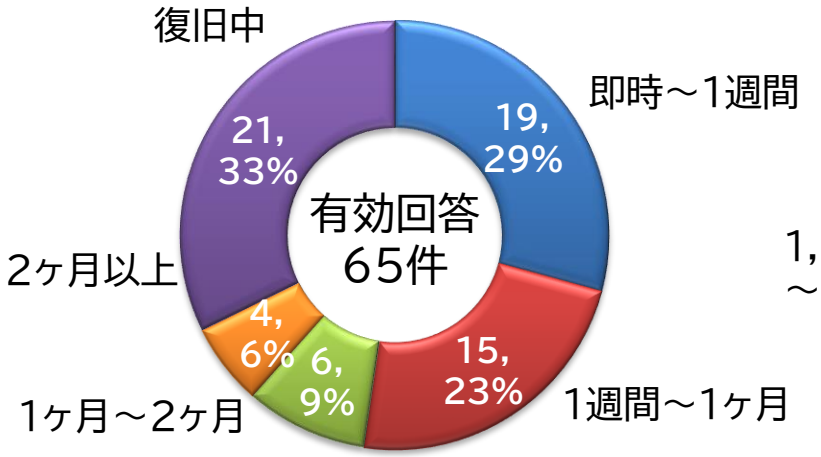


調査・復旧費用の総額

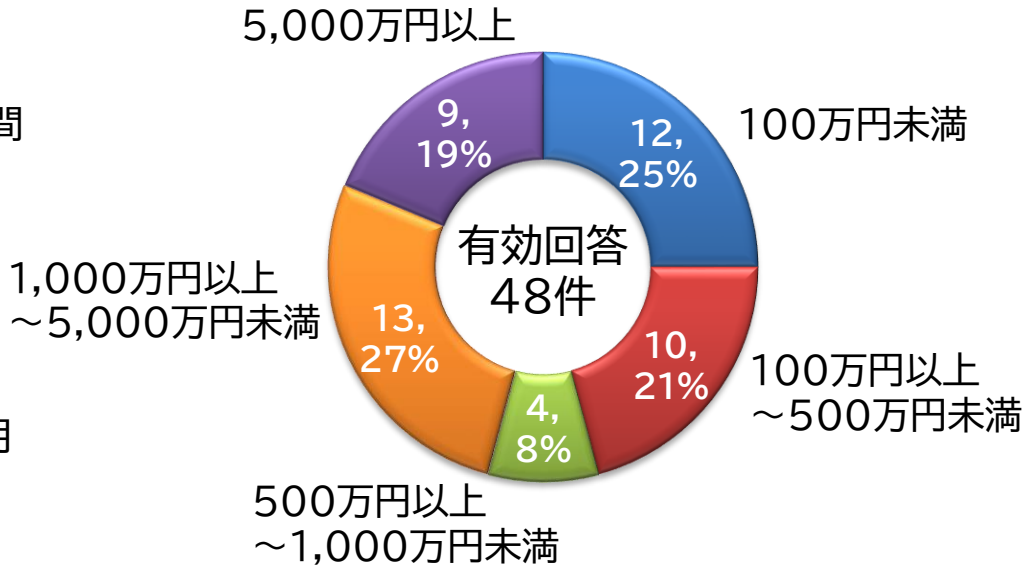
［出典］　令和5年におけるサイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf

ランサム攻撃による被害
復旧等に要した期間・費用

- 2024年のランサムウェア被害の復旧等に要した期間・費用



復旧に要した期間



調査・復旧費用の総額

［出典］　令和6年上半期におけるサイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf

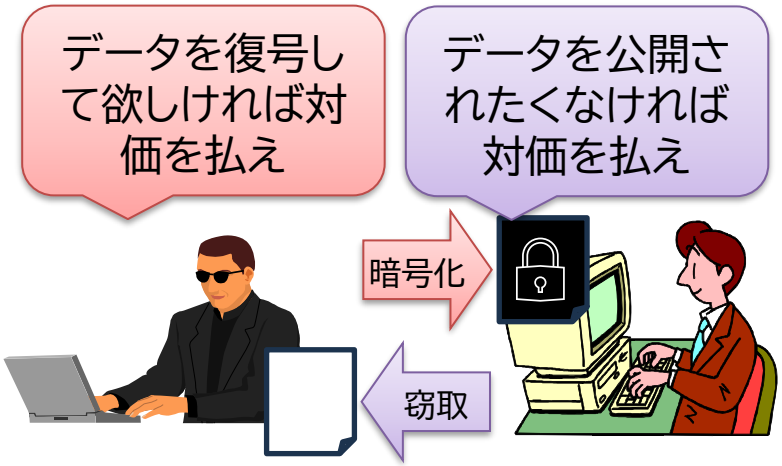
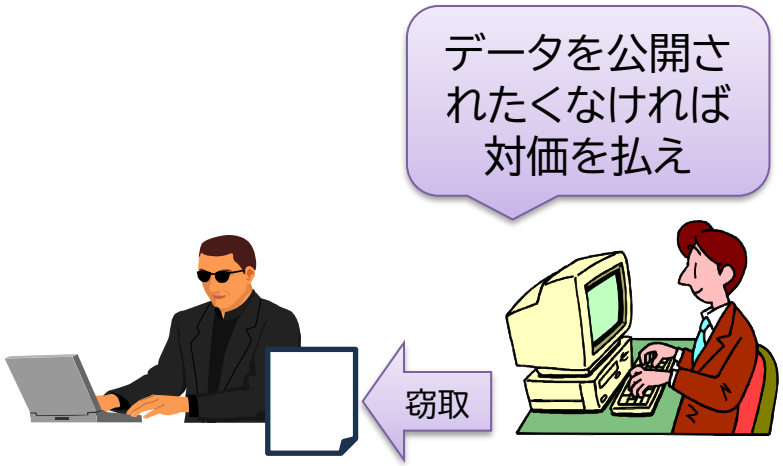
ランサム攻撃による被害
脅迫手段の高度化

- ランサムウェアは、「ランサム（Ransom＝身代金）」と「ウェア（Software）」をつなげた造語で、パソコン内のファイルを人質にとる不正プログラムの総称である。

年代	区分	脅迫の概要
2013年	データの暗号化	感染したコンピュータ内のファイルやハードディスクなどのデータを暗号化し、復号したければと脅迫して金銭を要求する。
2019年	窃取情報の暴露 二重脅迫	感染したコンピュータ内からデータを窃取し、窃取データを公開すると脅迫して金銭を要求する。
2020年	DDoS攻撃 三重脅迫	交渉を開始するまで、DDoS（Distributed Denial of Service；通信過負荷状態を発生させる）攻撃を使ってさらにプレッシャーをかける。
2022年	攻撃を受けていることの暴露 四重脅迫	顧客やビジネスパートナーからの信用失墜を狙い、窃取データにある連絡先に状況を通知することでさらにプレッシャーをかける。

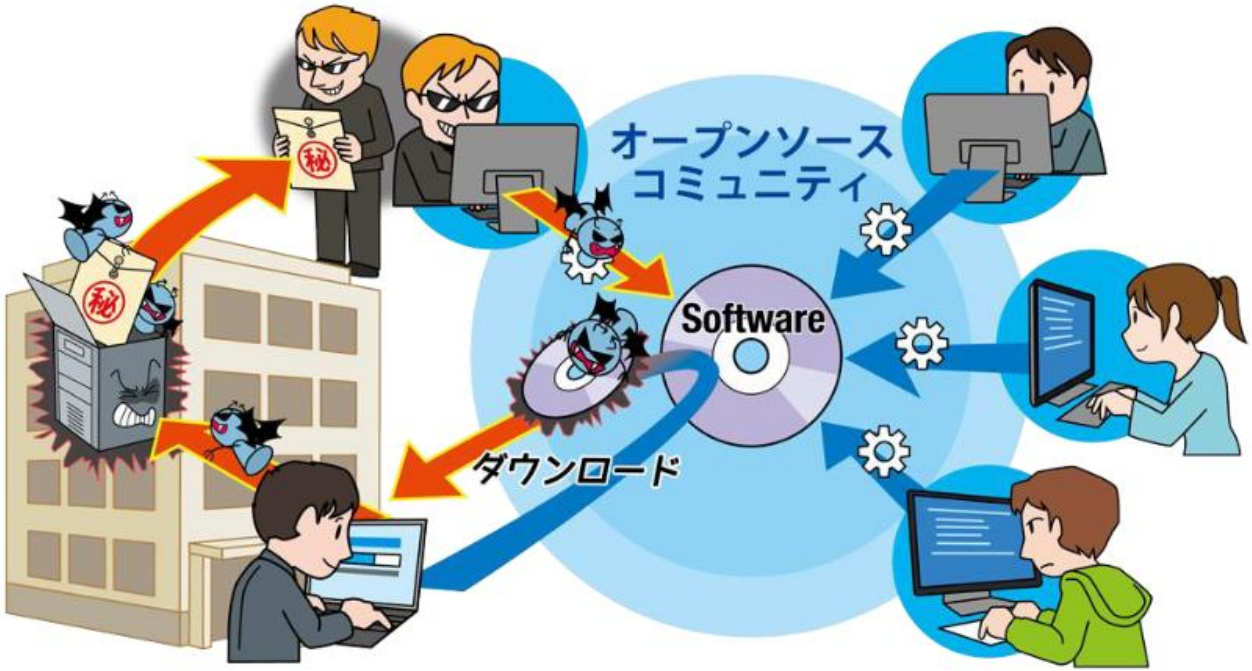
ランサム攻撃による被害
脅迫手段の高度化

- ノーウェアランサム攻撃＝窃取情報の暴露
  - 組織内ネットワークへの侵入には、テレワークにも利用される機器等の脆弱性や強度の弱い認証情報等を利用
  - さらに侵入後には、窃取したデータを公開されたくなければと脅迫して金銭を要求

二重脅迫型ランサムウェア攻撃 ＝データの暗号化＋窃取情報の暴露	ノーウェアランサム攻撃 ＝窃取情報の暴露
	

情報セキュリティ10大脅威 2025
サプライチェーンや委託先を狙った攻撃

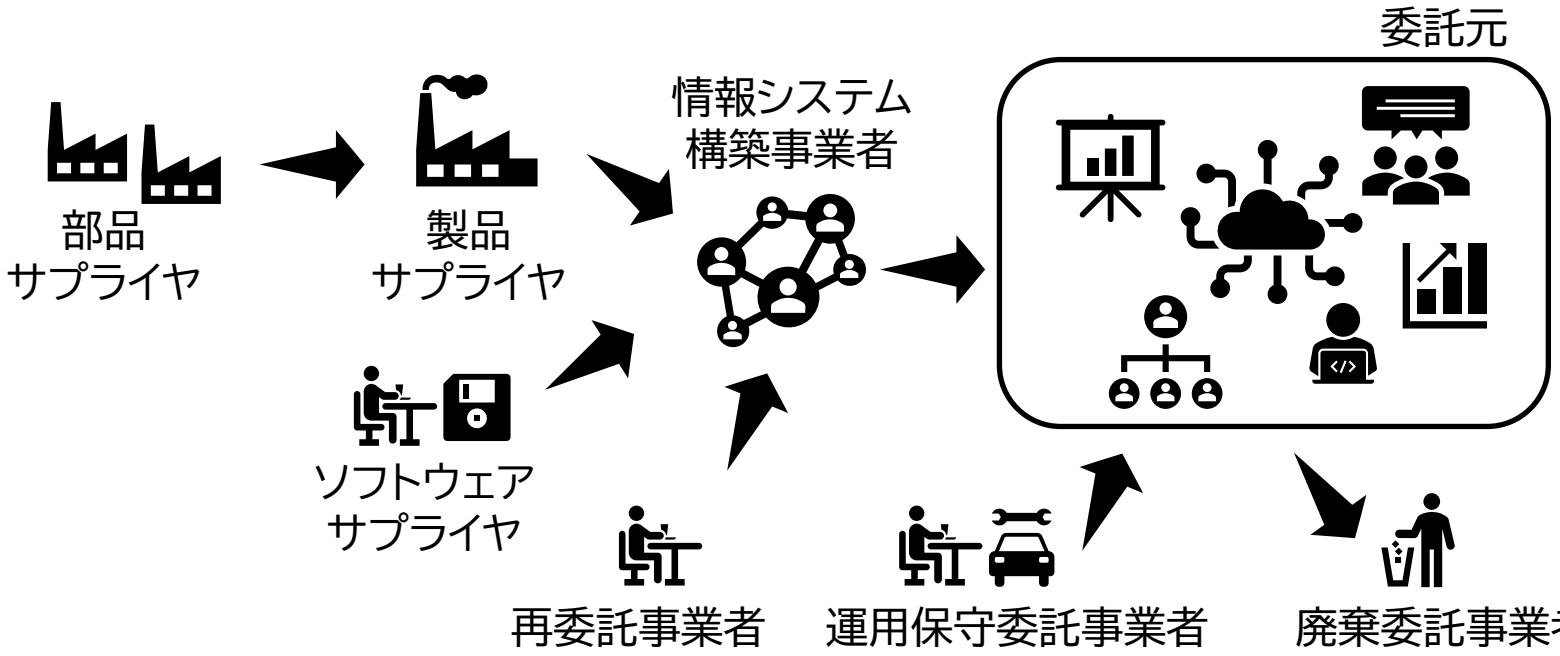
- 委託先が狙われる！関係組織も視野に入れたリスク管理を
  - 取引先や委託先が保有する機密情報を狙う
  - ソフトウェア開発元や企業システムの運用・監視等を請け負う事業者等を攻撃し、標的を攻撃するための足掛かりとする



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
⇒ソフトウェアサプライチェーン

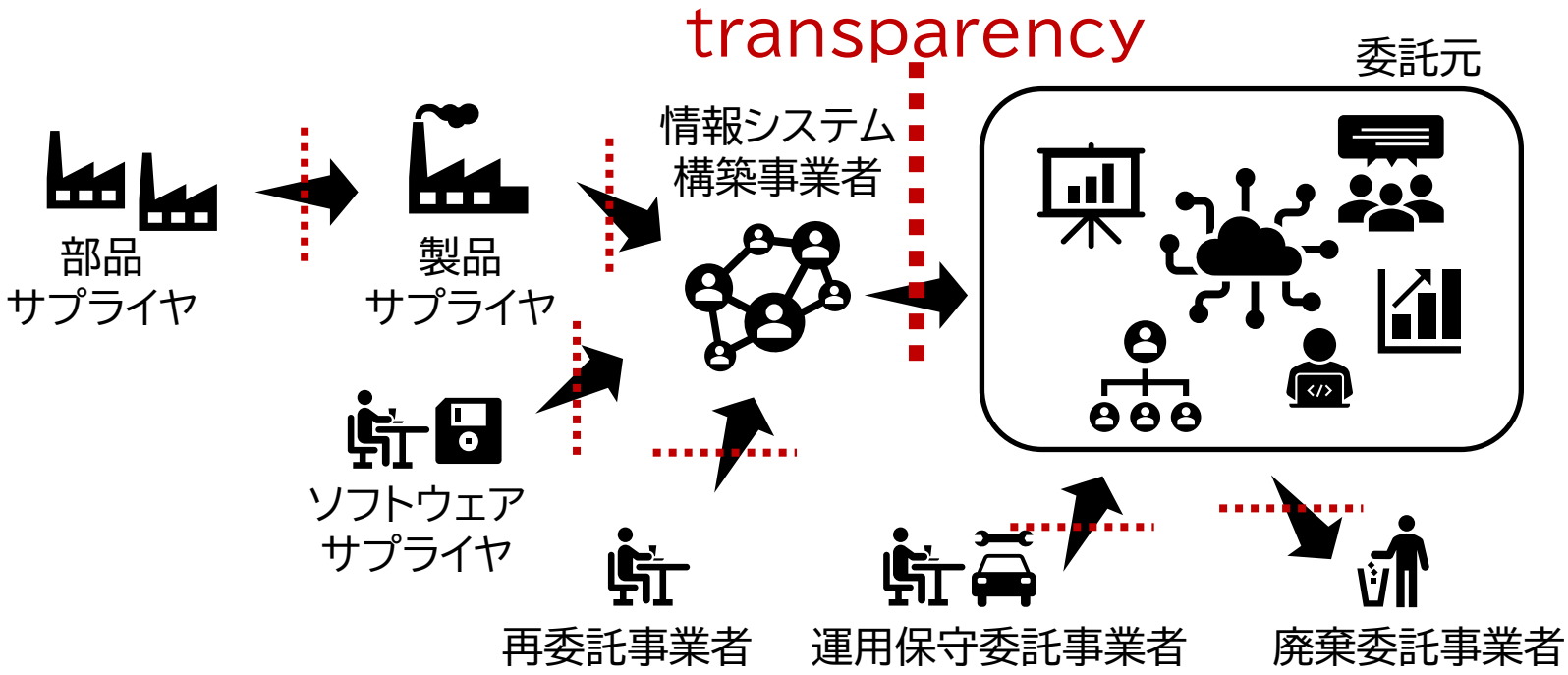
サプライチェーンや委託先を狙った攻撃
サプライチェーンとは

- ITにおけるシステム開発やサービス提供/利用に関する連鎖
- ビジネスパートナーや委託先企業も含めたサプライチェーン全体でのセキュリティ対策の必要性の高まり
  - サイバーセキュリティ経営ガイドラインv2.0（2017年）
  - 米国立標準技術研究所（NIST）サイバーセキュリティフレームワークv1.1（2018年）



サプライチェーンや委託先を狙った攻撃
サプライチェーンとは

- (ソフトウェア)サプライチェーンのセキュリティにおいては、
  - 「見える」セキュリティ、「見せる」セキュリティが求められている。
    - 委託元の視点　「見える」セキュリティ
    - 情報システム構築事業者の視点　「見せる」セキュリティ
  - 共通の仕様や言語でコミュニケーションする必要がある。



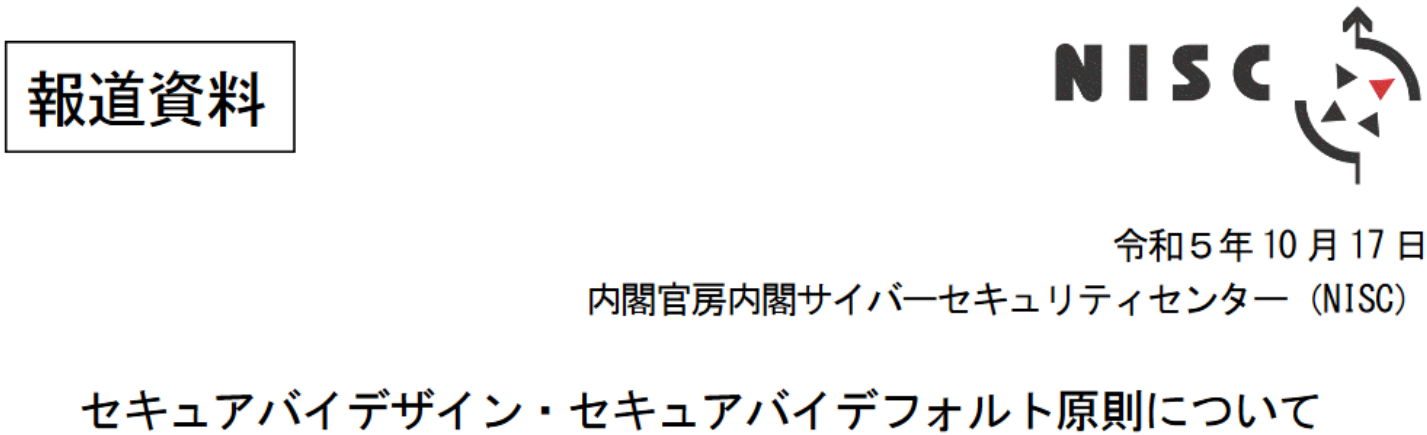
セキュア・バイ・デザインの原則

- 2023年以降急速に国際署名文書が増えている

年月日	イベント
2025年02月04日	国際文書:エッジデバイスのための緩和戦略
2024年12月04日	通信インフラの可視性と強化に関するガイダンス
2024年10月02日	国際文書: OTサイバーセキュリティの原則
2024年08月22日	国際文書: イベントログと脅威検知のベストプラクティス
2024年07月09日	国際アドバイザリー: APT40 グループに関するアドバイザリー
2024年05月15日	国際共同ガイダンス: 人権保護や民主主義の推進に関与する組織や個人のためのガイダンス
2024年01月24日	国際共同ガイダンス: AI使用に関するガイダンス
2023年11月28日	国際共同ガイダンス: セキュアAIシステム開発ガイドライン
2023年10月16日	国際共同ガイダンス: セキュア・バイ・デザインの原則とアプローチに関するガイダンス

［出典］　内閣サイバーセキュリティセンター 新着情報
https://www.nisc.go.jp/news/list/index.html

セキュア・バイ・デザインの原則
セキュア・バイ・デザインの原則とアプローチに関するガイダンス



報道資料

NISC

令和５年 10 月 17 日
内閣官房内閣サイバーセキュリティセンター（NISC）

セキュアバイデザイン・セキュアバイデフォルト原則について

- 2023年10月16日、CISA(米国サイバーセキュリティ・インフラセキュリティ庁)が、日本のNISC(内閣サイバーセキュリティセンター)などのサイバーセキュリティ組織と共同で公開
  - セキュア・バイ・デザインの原則とアプローチに関するガイダンス
    Secure-by-Design - Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software

セキュア・バイ・デザインの原則
セキュア・バイ・デザインの原則とアプローチに関するガイダンス

- セキュア・バイ・デザイン
  悪意ある者が端末機器、データ、インフラに不正にアクセスできないように、設計・開発段階から、合理的に保護されている形で製品を作ること。そのために、セキュリティ対策を後から「追加」するのではなく、製品設計や開発プロセスにあらかじめ組み込んでおくこと。

- セキュア・バイ・デフォルト
  顧客にリスクを生じさせることのない初期状態で製品を出荷すること。そのために、基本的なセキュリティが確保できているというセキュアな初期設定を基準とすること。

- セキュア・バイ・デザインの原則とアプローチに関するガイダンス
  数百の個人、企業、非営利団体から受けたフィードバックを受け、特にソフトウェア作成業者に対する3つの原則、
  原則1：顧客のセキュリティの結果に責任を持つ
  原則2：徹底した透明性と説明責任を負う
  原則3：トップ主導での実施
  を具体的に説明し、ソフトウェア作成業者がこれらの原則を顧客や一般の人々に対し、どのように示すことができるかに焦点を当てた提言となっている。

セキュア・バイ・デザインの原則
原則1：顧客のセキュリティの結果に責任を持つ

- セキュア・バイ・デフォルトのプラクティス

推奨事項	説明
初期パスワードを無くす	デフォルトパスワードで運用し続けることができないようにすること。安易なパスワードを設定できないようにすること。 多くのサイバー攻撃の原因である「脆弱なパスワード」の利用については、そもそも脆弱な状態にできることが問題であり、設定できないようにしておくことが求められている。
実地テストの実施	顧客先の実際の利用環境や利用方法を踏まえたテストを実施すること。特に、セキュリティに重点を置いたユーザ調査を実施するなど、製品セキュリティが現場でどのように機能してるかを把握し、改善すべき箇所を特定して改良すること。 セキュリティ強化ガイドを正しく実施しているか、製品の既存のセキュリティ機能は期待されたとおり機能するか、それらの機能は実際の攻撃を防げるか、被害の可能性をより低減できる機能は何か、などを確認することが求められている。
セキュリティ強化ガイドのサイズを小さくする	セキュリティ強化ガイドではなく、セキュリティ対策の実施プロセスを簡素化するためのツールや自動化手段を提供することで、製品が導入された顧客環境のセキュリティ確保を考えること。 強化ガイドに沿って、管理者がセキュリティ対策を実行することに頼らないことが求められている。

セキュア・バイ・デザインの原則
原則1：顧客のセキュリティの結果に責任を持つ

- セキュア・バイ・デフォルトのプラクティス（続き）

推奨事項	説明
安全でないレガシー機能の使用を積極的にやめさせる	アップグレードは、後方互換性よりもセキュリティ確保を優先すること。 リスクを軽減するというアップグレードの方向に積極的に誘導することが求められている。
注意喚起アラートを導入する	ユーザや管理者がセキュリティ面で危険な使い方や状態にある場合には、適時かつ繰り返し警告すること。 製品の仕様として危険な使い方にある場合には、見える化することが求められている。
セキュアな構成テンプレートを作成する	組織のリスク選好度に応じて、安全な構成を設定できるテンプレートを予め作成しておくこと。 安全な環境を利用しやすくすることが求められている。

セキュア・バイ・デザインの原則
原則1：顧客のセキュリティの結果に責任を持つ

- セキュアな製品開発のプラクティス

推奨事項	説明
SDLCフレームワークへの適合性を文書にする	採用しているSDLC（セキュアソフトウェア開発ライフサイクル）の枠組みと適合性を文書として示すこと。 安全なソフトウェア開発を実施していることが求められている。米国内では、NISTのSSDF（セキュアソフトウェア開発フレームワーク）の利用を推奨している。
サイバーパフォーマンス目標または同等の適合性を文書にする	CISA（米国サイバーセキュリティ・インフラセキュリティ庁）クロスセクタサイバーパフォーマンス目標やNIST（米国標準技術研究所）サイバーセキュリティフレームワークなどとの適合性を文書として示すこと。 攻撃者から企業と開発環境を保護していることが求められている。
脆弱性管理	脆弱性の根本原因を排除することを考えた脆弱性管理をすること。 ソフトウェアの品質計画、品質管理、品質改善、品質測定に関する措置を講じることが求められている。
オープンソースのソフトウェアを責任持って利用する	オープンソースのソフトウェアを利活用する場合、セキュリティ確保に責任を持つこと。 使用するオープンソースの開発や維持を支援することが求められている。

セキュア・バイ・デザインの原則
原則1：顧客のセキュリティの結果に責任を持つ

- セキュアな製品開発のプラクティス（続き）

推奨事項	説明
開発者のためのセキュアデフォルトを提供する	開発者に提供する環境はデフォルトの使い方が安全になるようにすること。
セキュリティを理解するソフトウェア開発者を育成する	自組織のセキュリティ開発者をセキュアコーディングのベストプラクティスで訓練し、セキュリティを理解させること。
SIEMとSOARとの統合をテストする	セキュリティインシデント調査において役立つログを出力するために、SIEM（セキュリティインシデントイベント管理）やSOAR（セキュリティ統合調整・自動化・対応機能）と連携したテストを実施すること。 インシデント対応チームが実際のセキュリティインシデント調査あるいはセキュリティインシデントが疑われる調査において役立つログを出力することが求められている。
ゼロトラストアークテクチャと整合させる	製品導入ガイドがNIST（米国標準技術研究所）やCISA（米国サイバーセキュリティ・インフラセキュリティ庁）のゼロトラストアーキテクチャのモデルと整合していること。 顧客の環境にゼロトラストアーキテクチャの原則を取り入れることを求めている。

セキュア・バイ・デザインの原則
原則1：顧客のセキュリティの結果に責任を持つ

- ビジネスプラクティス

推奨事項	説明
追加費用なしでログ記録機能を提供する	追加料金なしでセキュリティ関連ログを生成し記録できるようにすること。さらに、デフォルトでセキュリティ関連ログに記録すること。
隠れた負担をなくす	セキュリティは価格設定のあるオプションではなく、顧客の権利とみなし、セキュリティやプライバシー機能、または統合について、追加料金を課さないこと。 SSO（シングルサインオン）やMFA（多要素認証）の導入など強固なセキュリティ態勢の実現を妨げている要因を排除することが求められている。
オープンスタンダードを採用する	オープンスタンダードが利用できる場合、独自仕様のプロトコルを使用せずにオープンスタンダードを利用して実装すること。 仕様についても、セキュアな品質であること、セキュアな品質を維持できることが求められている。
アップグレードツールを提供する	安全なネットワーク接続など、最新かつより安全な機能導入などにあたっては、不確実性やリスクの軽減を支援するツールを提供すること。 最新バージョンの導入などのアップグレードをしやすい環境が求められている。

セキュア・バイ・デザインの原則
原則2：徹底的な透明性と説明責任を果たす

- セキュア・バイ・デフォルトのプラクティス

推奨事項	説明
セキュリティ関連の総合的な統計や傾向を公表する	（良い慣習を見える化するため）顧客や管理者のMFA（多要素認証）の採用状況やレガシーなプロトコルの使用などを示すこと。 強固なセキュリティ態勢の実現を妨げている要因を排除するための企業努力の見える化が求められている。
パッチ適用の統計を公表する	製品の最新バージョンを使用している顧客の割合を公表し、更新時の容易さや信頼性への努力を示すこと。 同上
未使用の管理者特権のデータを公表する	顧客ベースに対する過剰な権限付与に関する集計情報と、攻撃を減らすための顧客の行動変容を促す対応や製品の変更を示すこと。 同上

セキュア・バイ・デザインの原則
原則2：徹底的な透明性と説明責任を果たす

- セキュアな製品開発のプラクティス

推奨事項	説明
内部セキュリティ管理の確立	SaaS事業者は強固なセキュリティ態勢の実現を促す内部管理の統計を公表すること。 FIDO（Fast ID Online）認証の導入など強固なセキュリティ態勢の実現が求められている。
高レベルな脅威モデルを公表する	セキュアバイデザインに基づく製品開発にあたっては、何を誰から守ろうとしているか記述した脅威モデルの作成から始めること。 セキュリティリスク分析が求められている。
安全なSDLCの自己検証の証明を公表する	各製品について、採用しているSDLC（セキュアソフトウェア開発ライフサイクル）の枠組みと適合性を自己検証の証明を通して示すこと。 セキュアバイデザインを実践しているという根拠を示すことが求められている。
脆弱性の透明性を活用する	製品の脆弱性については、必要事項を記載したCVE（共通脆弱性識別子）エントリーとして公開すること。 脆弱性に対してはCVEを付与し、グローバルで一意に管理できるようにすることが求められている。

セキュア・バイ・デザインの原則
原則2：徹底的な透明性と説明責任を果たす

- セキュアな製品開発のプラクティス（続き）

推奨事項	説明
SBOMの公表	サプライチェーンを掌握するため、サプライヤにデータを要求してSBOM（ソフトウェア部品表）を作成・維持し、顧客やユーザに提供すること。 購入の決定、運用の支援、悪意のあるサプライチェーン攻撃の検出などにあたり、製品をコンポーネントレベルで管理できるようにすることが求められている。
脆弱性開示ポリシーの公表	脆弱性開示ポリシーを公表すること。 発見された脆弱性の根本原因を分析して、可能な限り脆弱性の属性全体を排除する措置を講ずることが求められている。

セキュア・バイ・デザインの原則
原則2：徹底的な透明性と説明責任を果たす

- ビジネスプラクティス

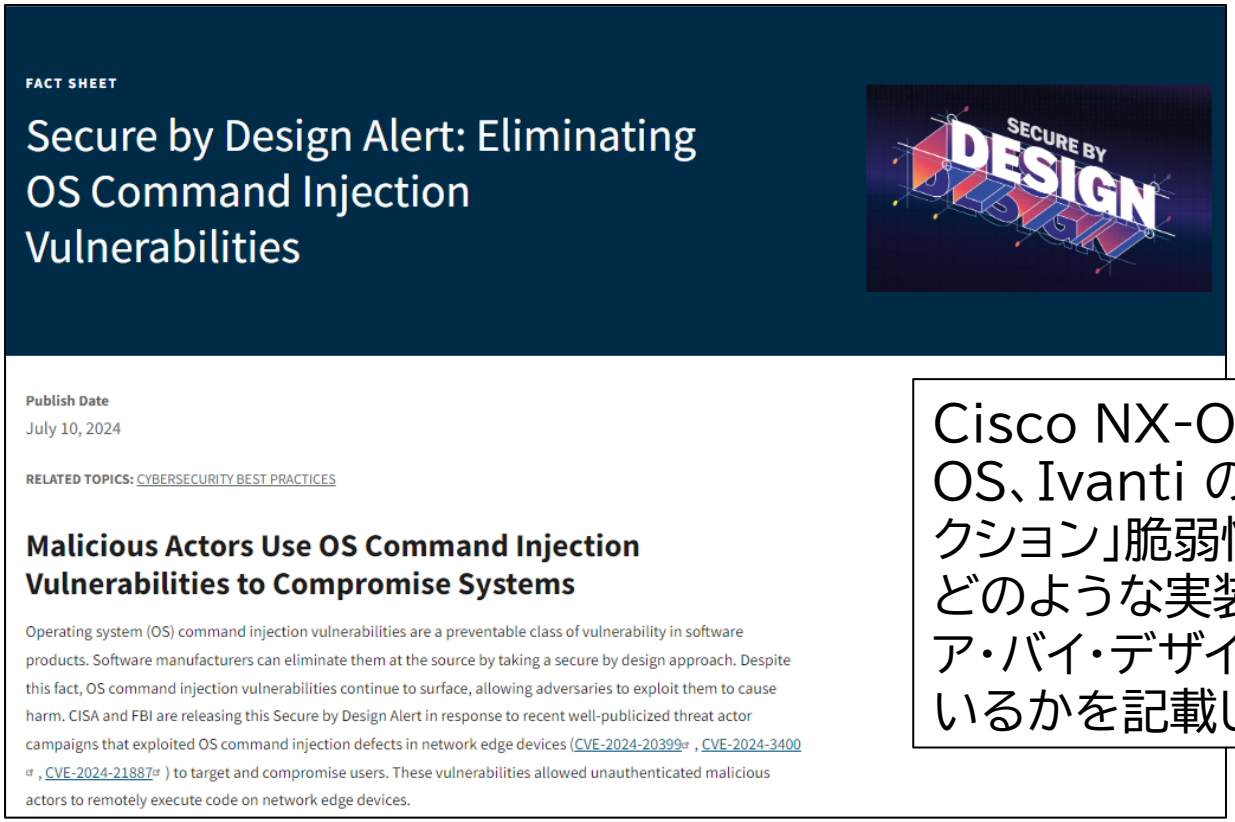
推奨事項	説明
セキュアバイデザインの保証人となる経営層幹部を指名し公表する	セキュアバイデザインのプログラムを監督するトップ経営幹部を指名すること。 製品セキュリティをトップレベルの経営に関わる問題として取り組むことが求められている。
セキュアバイデザインのロードマップを公表する	セキュリティ改善プログラムのロードマップを作成し、セキュリティを改善するためにSDLC（セキュアソフトウェア開発ライフサイクル）に加えた変更を記録として残すこと。 品質改善の取組の場合と同様に、セキュリティ改善プログラムにおいても、計画、管理、改善という取組、実践しているという根拠を示すことが求められている。
メモリ安全性のロードマップを公表する	既存製品についてはメモリセーフな言語に移行すること。新たな製品はメモリセーフな言語を使用すること。 メモリの安全性に起因する脆弱性を排除することが求められている。
結果を公表する	セキュアバイデザインの具現化にあたり実施したSDLC（セキュアソフトウェア開発ライフサイクル）の良い事例（成功）、悪い事例（失敗）を記録として残し、活用すること。 セキュアバイデザインを実践しているという根拠を示すことが求められている。

セキュア・バイ・デザインの原則
原則3:トップ主導での実施

推奨事項	説明
企業の財務報告にセキュアバイデザインのプログラムの詳細を含める	顧客のセキュリティと企業の財務成果を結びつけていることを示すこと。
自組織の取締役会に対し定期的に報告を行う	セキュリティ態勢に関する情報に加え、製品セキュリティおよびそれが顧客のセキュリティに及ぼす影響に関する情報も含めること。
セキュアバイデザイン担当取締役の権限を強化する	顧客のセキュリティ向上を達成するために必要となる製品投資に関する権限を与えること。
企業内部で意味あるインセンティブを作る	顧客のセキュリティ向上を、評価する仕組みを作ること。
セキュアバイデザイン委員会を設置する	セキュアバイデザインに向けて活動するための仕組みを作ること。
顧客協議会を設立し、発展させる	顧客のセキュリティ向上に向けて、協働するための仕組みを作り活用すること。

セキュア・バイ・デザインの原則
Secure by Design Alerts

- CISA(米国サイバーセキュリティ・インフラセキュリティ庁)が発行する「顧客の安全に影響を与える脆弱性や製品の欠陥を排除するために、最初から製品にセキュリティを組み込むよう求めている注意喚起」



FACT SHEET

Secure by Design Alert: Eliminating OS Command Injection Vulnerabilities

Publish Date
July 10, 2024

RELATED TOPICS: CYBERSECURITY BEST PRACTICES

Malicious Actors Use OS Command Injection Vulnerabilities to Compromise Systems

Operating system (OS) command injection vulnerabilities are a preventable class of vulnerability in software products. Software manufacturers can eliminate them at the source by taking a secure by design approach. Despite this fact, OS command injection vulnerabilities continue to surface, allowing adversaries to exploit them to cause harm. CISA and FBI are releasing this Secure by Design Alert in response to recent well-publicized threat actor campaigns that exploited OS command injection defects in network edge devices (CVE-2024-20399 , CVE-2024-3400 , CVE-2024-21887) to target and compromise users. These vulnerabilities allowed unauthenticated malicious actors to remotely execute code on network edge devices.

Cisco NX-OS、Paloalto PAN-OS、Ivanti の「OSコマンドインジェクション」脆弱性をきっかけとして、どのような実装をすべきか、セキュア・バイ・デザイン原則とどう関係しているかを記載している。

セキュア・バイ・デザインの原則
Secure by Design Pledge（自主宣言）

- 2024年5月のRSAカンファレンスで発表されたCISAの施策
- Secure by Designを宣言させ、7つの具体的な目標に対し、署名から1年以内に取り組みや達成状況を測定可能な形で公表すること

事項	ゴール
MFA（多要素認証）	1年以内に、製品全体で多要素認証の使用を増加させるために講じた措置を示すこと。
デフォルトパスワード	1年以内に、製品全体でデフォルトパスワードを削減に向けた進捗を示すこと。
脆弱性のクラス全体を削減	1年以内に、製品全体で1つ以上の脆弱性クラスを削減させるために講じた措置を示すこと。
セキュリティパッチ	1年以内に、顧客によるセキュリティパッチのインストールを増加させるために講じた措置を示すこと。
VDP（脆弱性開示ポリシー）	1年以内に、脆弱性開示ポリシーを公開すること。
CVE（共通脆弱性識別子）	1年以内に、脆弱性報告の透明性を示すこと。 CWE（共通脆弱性タイプ一覧）、CPE（共通プラットフォーム一覧）など脆弱性対策に必要となる項目を記載した情報を発信すること。
侵入の証拠	1年以内に、製品に影響を及ぼす侵害の証拠を顧客が収集できる状況を向上させること。

情報収集に役立つ技術仕様

脆弱性対策情報の収集
脆弱性対策に役立つキーワード

- 脆弱性対策情報、注意喚起、ニュース記事等でも使用されているキーワード

CVE® ・・・脆弱性を一意に識別する番号

CVSS ・・・脆弱性の深刻度を評価する指標

CWE ・・・脆弱性の種別を体系的に分類

CPE common platform enumeration ・・・製品を一意に識別する仕様

CVE(共通脆弱性識別子)
Common Vulnerabilities and Exposures

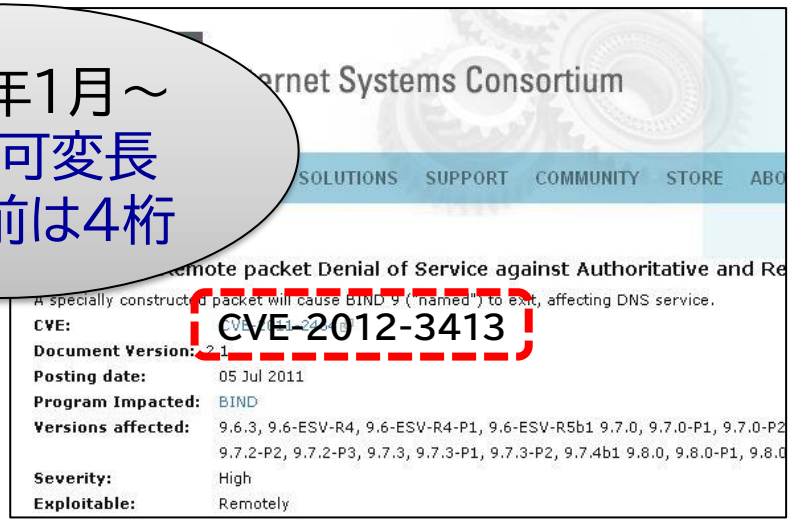
- プログラム上のセキュリティ問題に一意の番号(CVE識別番号)を付与して管理

CVE識別番号の構成

西暦	連番

CVE-2014-1000
CVE-2014-10000
CVE-2014-100000
CVE-2014-1000000

2014年1月～
連番は可変長
それ以前は4桁

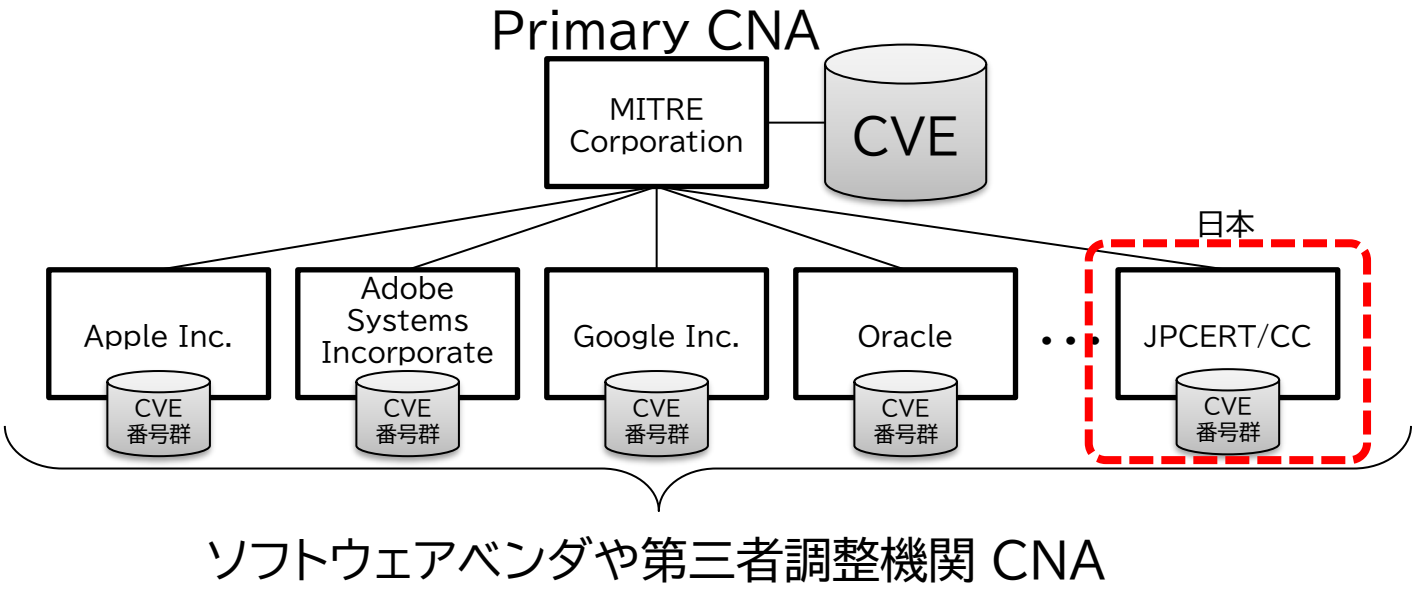


公表されている脆弱性に割り当てられた識別番号で、脆弱性を一意に特定することを可能となる

［出典］ 共通脆弱性識別子CVE概説
https://www.ipa.go.jp/security/vuln/CVE.html
CVE - Common Vulnerabilities and Exposures(CVE)
https://cve.mitre.org/

CVE(共通脆弱性識別子)
Common Vulnerabilities and Exposures

- 採番方法の仕組み
  - 新規脆弱性毎に米国MITREに申請、または
  - 米国MITREに認定されたCNA(CVE採番機関、CVE Numbering Authority)から割り当て



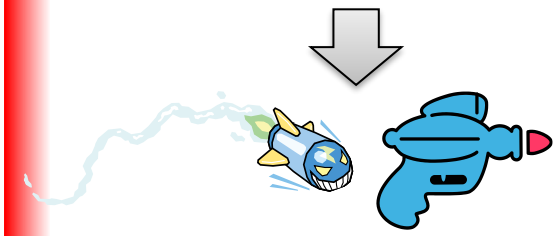
[出典] Submit a CVE Request
https://cveform.mitre.org/
CVE Numbering Authorities (CNAs)
https://www.cve.org/ProgramOrganization/CNAs

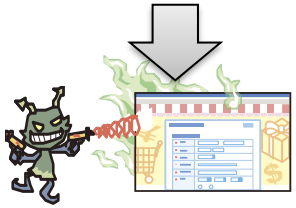
CVSS(共通脆弱性評価システム)
Common Vulnerability Scoring System

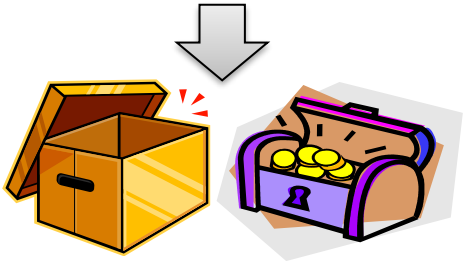
- 攻撃状況やシステムの重要度を加味して脆弱性の深刻度を表す

＝ 「技術的な特性」 × 「脅威の大きさ」 × 「情報資産の価値」

「基本評価基準」 × 「脅威評価基準」 × 「環境評価基準」







何が引き起こされる？

SQLインジェクション
技術面で危険度高

クロスサイトスクリプティング
技術面で危険度中

既に攻撃されている？

攻撃観測
なし

攻撃観測
あり

システムの重要度は？

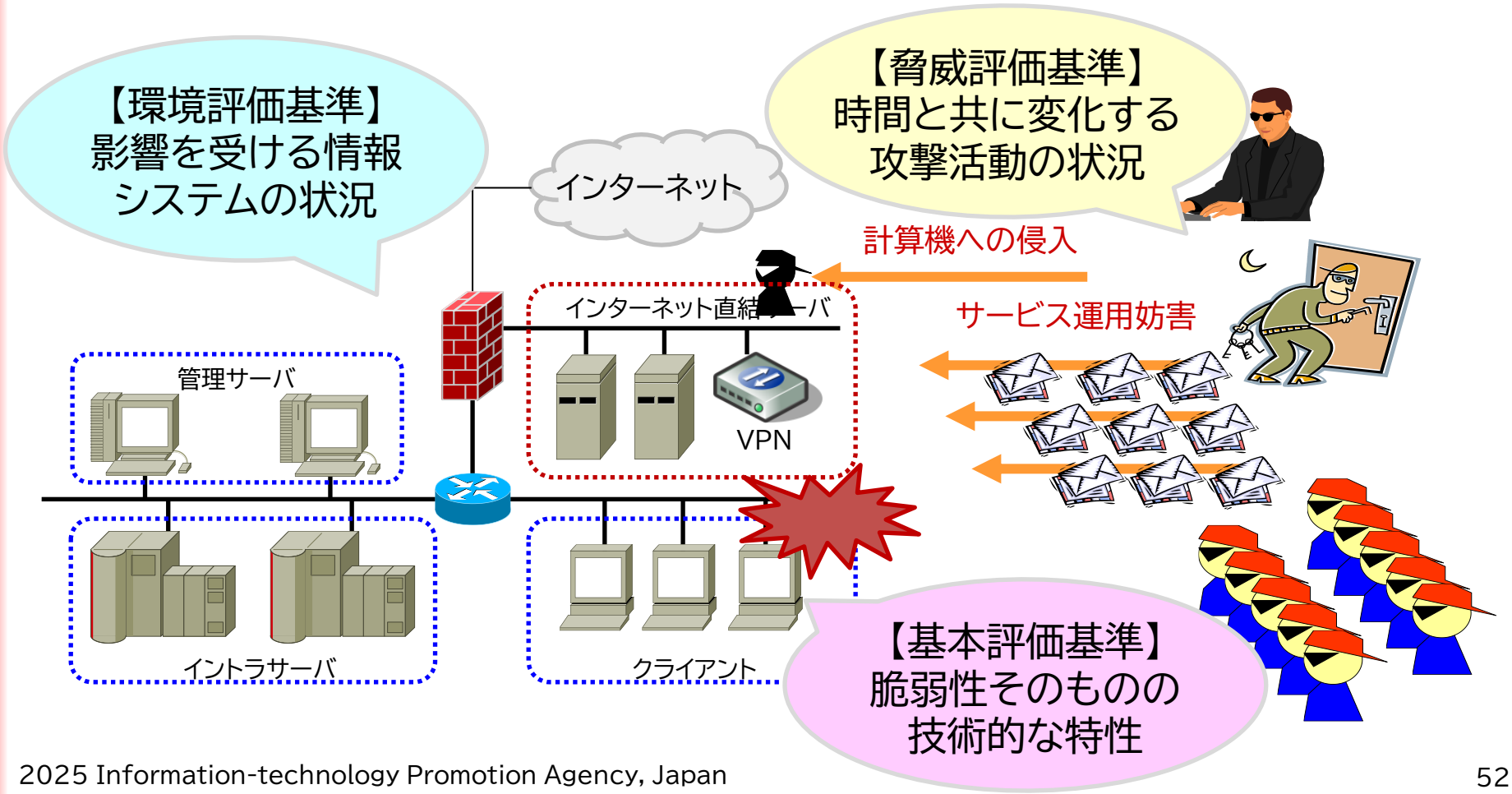
内部システム →深刻度 低

外部システム →深刻度 高

［出典］ 共通脆弱性評価システムCVSS概説
https://www.ipa.go.jp/security/vuln/CVSS.html
Common Vulnerability Scoring System SIG
https://www.first.org/cvss/

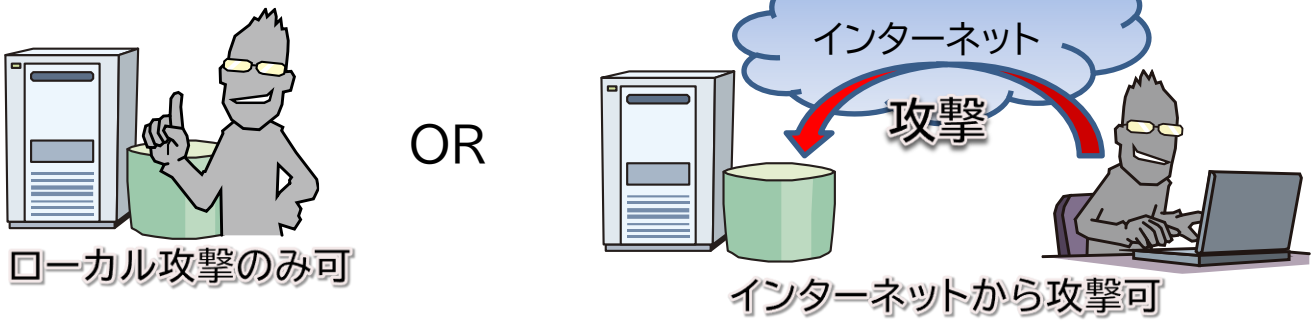
CVSS(共通脆弱性評価システム)
Common Vulnerability Scoring System

- 攻撃状況やシステムの重要度を加味して脆弱性の深刻度を表す

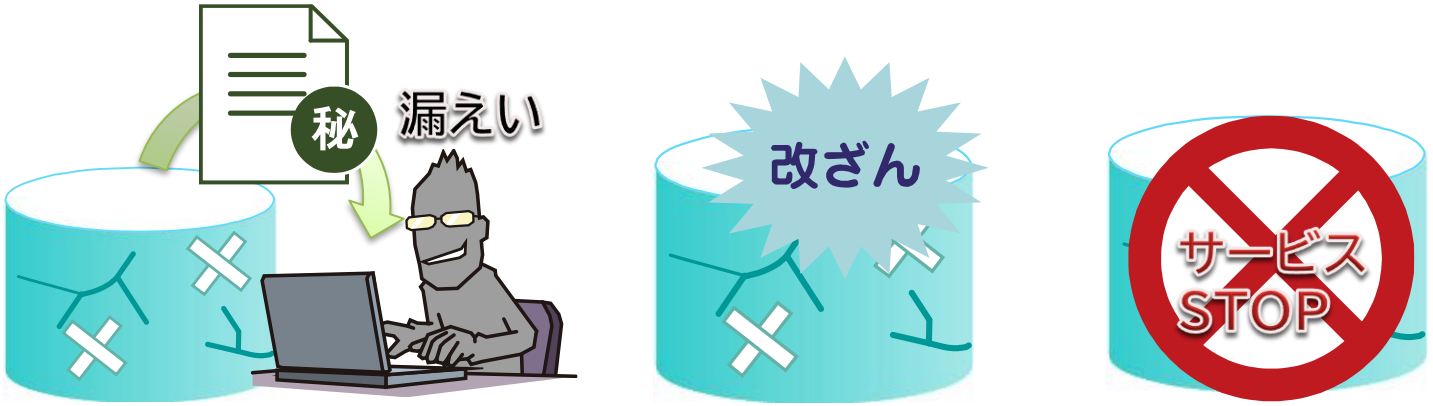


CVSS(共通脆弱性評価システム)
Common Vulnerability Scoring System

- 基本評価基準 ・・・ 脆弱性の技術的な特性を評価
  - 攻撃の難易度



  - 攻撃による影響

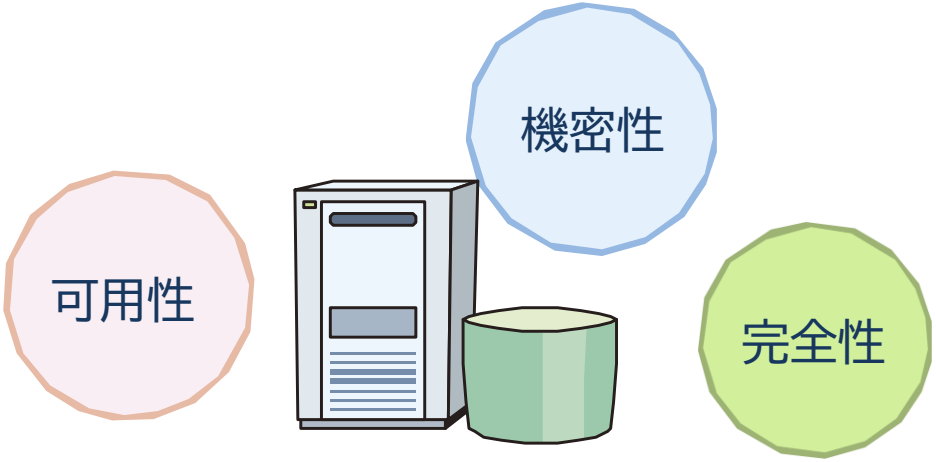


CVSS(共通脆弱性評価システム)
Common Vulnerability Scoring System

- 脅威評価基準 ・・・ 脆弱性を取り巻く状況を評価
  - 実際に攻撃が行われている
  - 攻撃コードが一般に公開(攻撃の予兆)

CVSS(共通脆弱性評価システム)
Common Vulnerability Scoring System

- 環境評価基準 ・・・ システムにおける問題の大きさを評価
  - CVSSv3 / CVSSv4
    - 対象システムのセキュリティ要求度を評価
      (機密性、完全性、可用性を評価)
    - 環境条件を加味した基本評価の再評価



CVSS（共通脆弱性評価システム）
開発

- CVSSは、情報システムの脆弱性に対するオープンで包括的、汎用的な評価手法の確立と普及を目指し、NIAC（米国家インフラストラクチャ諮問委員会、National Infrastructure Advisory Council）のプロジェクトで原案が作成された。
  - 2004年10月　原案の作成

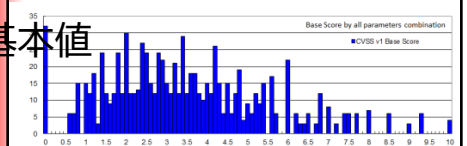
- その後、FIRST（Forum of Incident Response and Security Teams）のCVSS-SIG（Special Interest Group）によって仕様改善と適用推進が行われている。
  - 2005年6月　CVSS v1.0
  - 2007年6月　CVSS v2.0
  - 2015年6月　CVSS v3.0
  - 2019年6月　CVSS v3.1
  - 2023年11月　CVSS v4.0

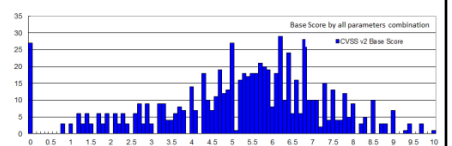
CVSS（共通脆弱性評価システム）
スコアのレベル分けの変遷

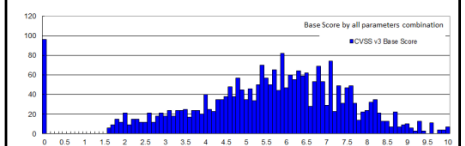
- CVSSスコア（0.0～10.0）のレベル分け

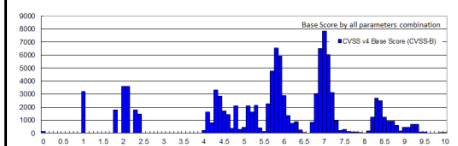
CVSSv1	CVSSv2	CVSSv3 & v3.1	CVSSv4
	危険 7.0～10.0 警告 4.0～6.9 注意 0.0～3.9	緊急 9.0～10.0 重要 7.0～8.9 警告 4.0～6.9 注意 0.1～3.9 なし 0	

基本値

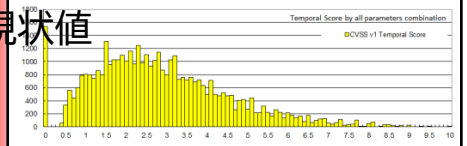


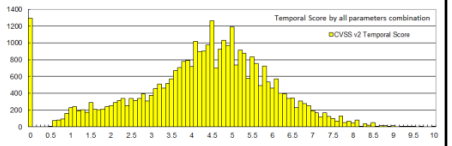


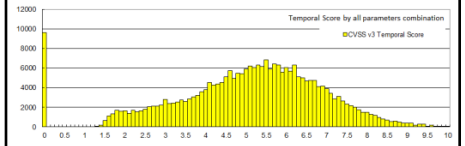


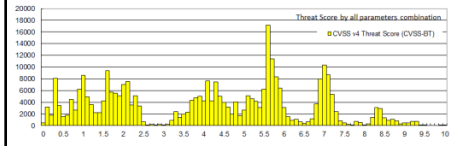


現状値

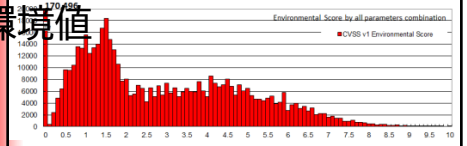


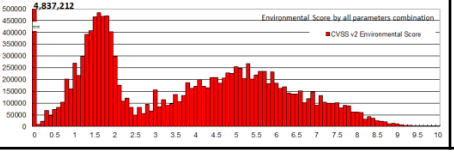


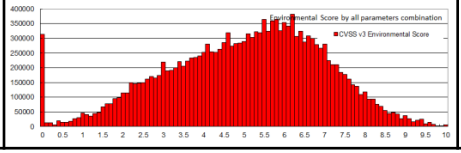


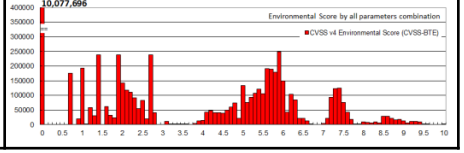


環境値









CVSS（共通脆弱性評価システム）
v1.0からv2.0への変更点

- CVSSスコア算出の計算式を改善

CVSSv1	CVSSv2	CVSSv3 & v3.1	CVSSv4

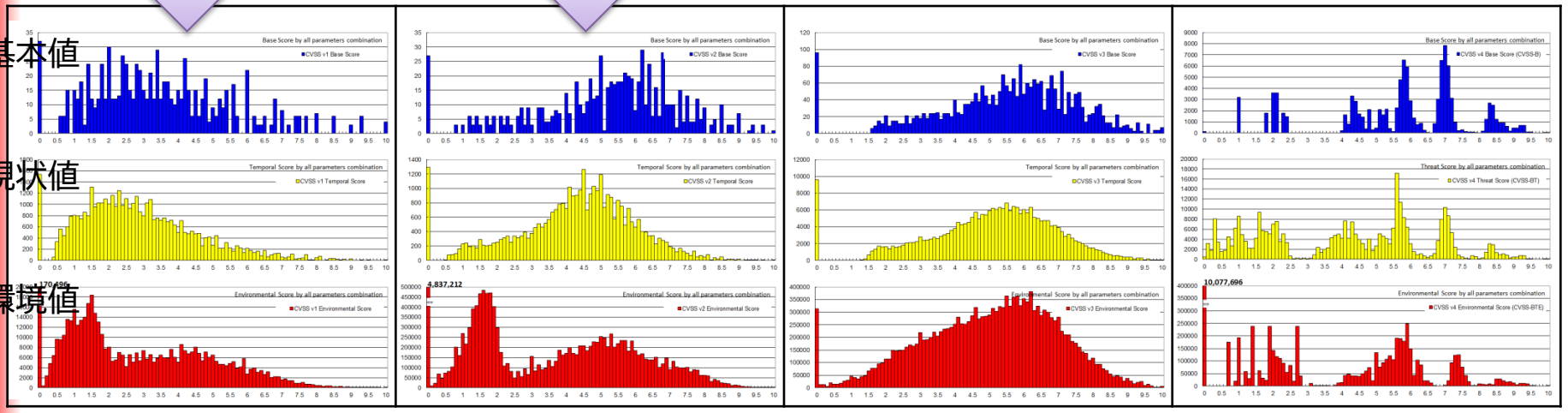
スコアの分布に
偏りがあった

スコアの分布の
偏りを是正した

基本値

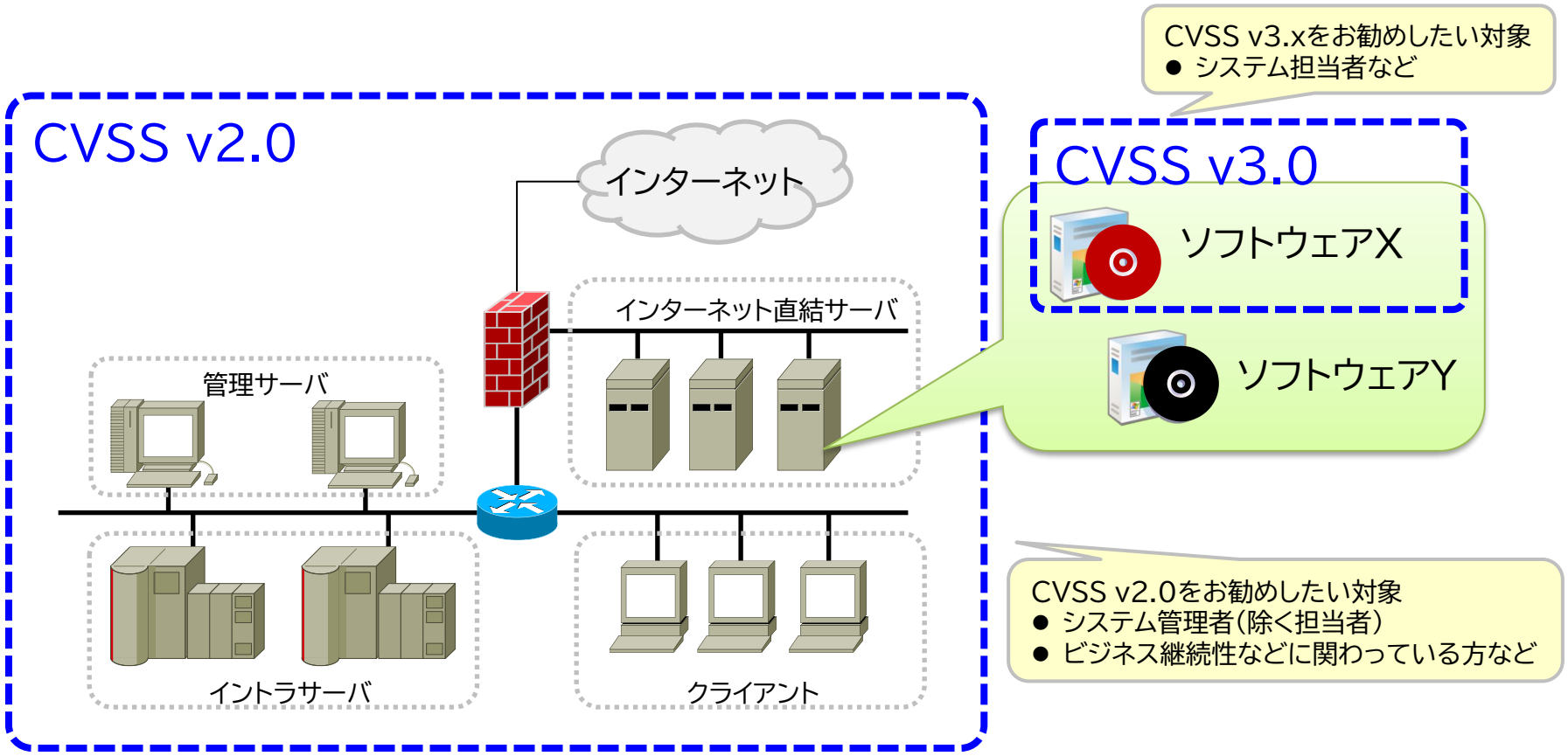
現状値

環境値



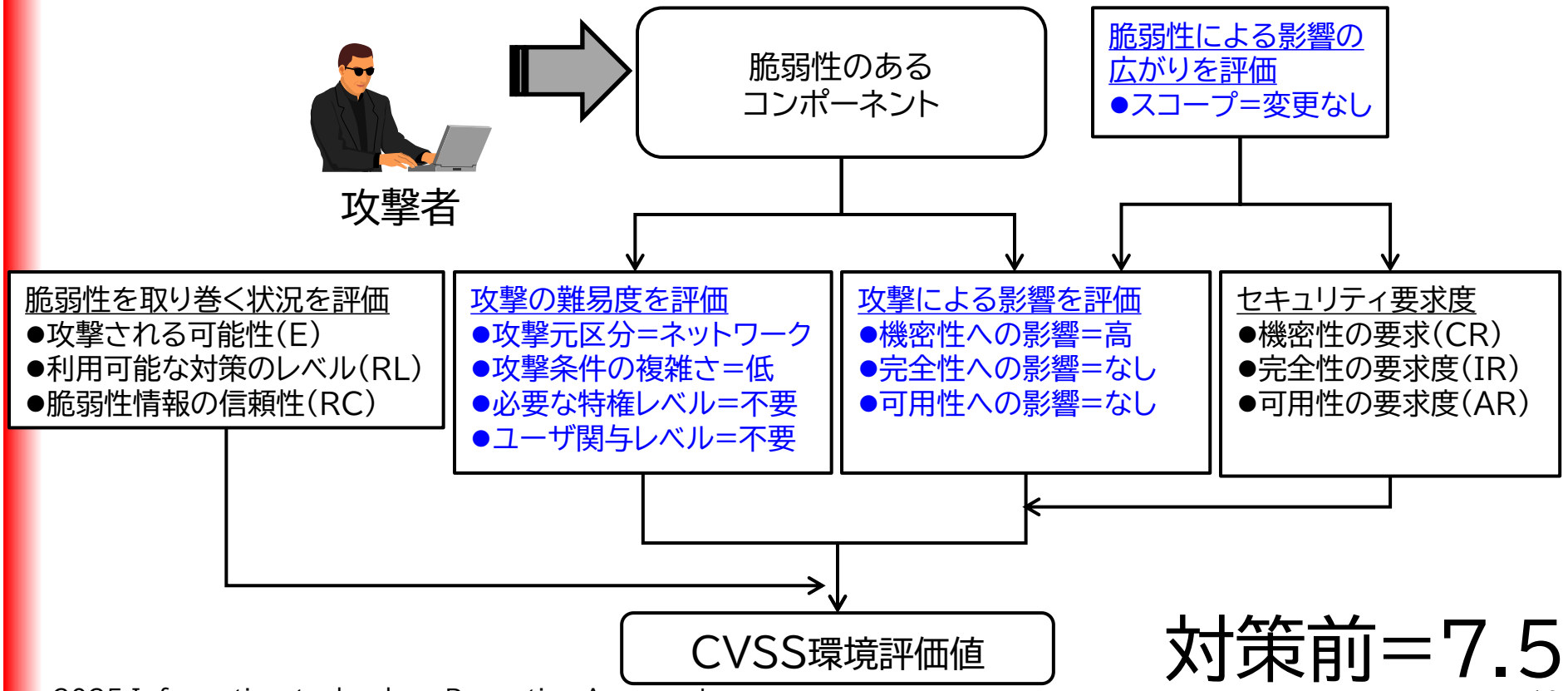
CVSS(共通脆弱性評価システム)
v2.0からv3.0への変更点

- 脆弱性の影響の捉え方を変更
  - CVSS v2.0:大局的(マクロ)に評価するアプローチ
  - CVSS v3.0:局所的(ミクロ)に評価するアプローチ



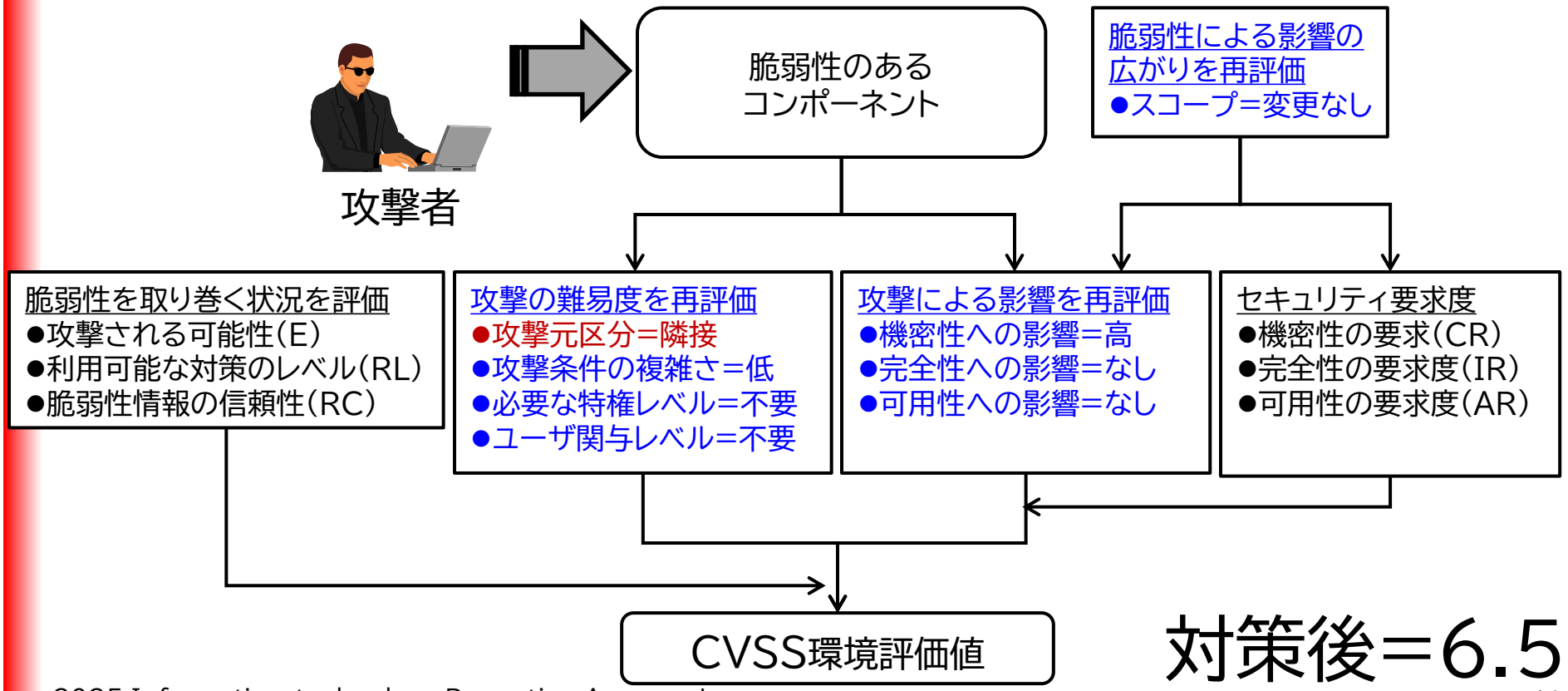
CVSS(共通脆弱性評価システム)
v3.xの良い点

- 対策前後の数値化の活用
  [例] 脆弱性のあるアプリケーションへのアクセスをネットワークファイアウォールで制御した場合



CVSS(共通脆弱性評価システム)
v3.xの良い点

- 対策前後の数値化の活用
  [例] 脆弱性のあるアプリケーションへのアクセスをネットワークファイアウォールで制御した場合



CVSS(共通脆弱性評価システム)
v3.0からv3.1への変更点

- CVSSスコア算出のための指針の明確化
  - CVSSスコアのブレを少なくする。

- v3.0計算式の不具合の修正
  - 言語によって小数計算に誤差が生じる問題
  - 環境評価の再評価において、評価が逆転してしまう問題

- 独自の評価基準を追加できるよう拡張
  - CVSS利用の適用範囲を拡大する。

CVSS（共通脆弱性評価システム）
v3.1からv4への変更点

- 脆弱性そのものの技術的な特性を評価する基本評価基準を改良
  - 攻撃の難易度
    - 脆弱性攻撃の前提条件に関する評価項目の追加
    - ユーザ関与レベル（UI）の細分化（不要、受動的、能動的）
  - 攻撃による影響
    - 影響の想定範囲（S）を、脆弱なコンポーネントへの影響、他のコンポーネントへの影響に細分化

- 脆弱性を取り巻く状況を評価する現状評価基準を改良
  - 現状評価基準から脅威評価基準へ名称変更
  - 利用可能な対策のレベル（RL）、脆弱性情報の信頼性（RC）を削除
  - 攻撃可能性（E）を、攻撃の成熟度に変更

［出典］　共通脆弱性評価システム v4.0
https://blog.isl.im.dendai.ac.jp/cti/cvss4_0

CVSS（共通脆弱性評価システム）
v3.1からv4への変更点

- システムにおける問題の大きさを評価する環境評価基準を改良
  - 影響の想定範囲（S）を、脆弱なコンポーネントへの影響、他のコンポーネントへの影響に細分化して再評価
  - 他のコンポーネントへの影響の再評価において安全性を考慮

- 補助評価基準の新設
  - 安全性、攻撃の自動化可能性、情報の緊急度、回復の手段、攻撃に利用可能な資源、対処するための労力

CVSS v2、CVSS v3の考え方を抑えておくことが重要です。

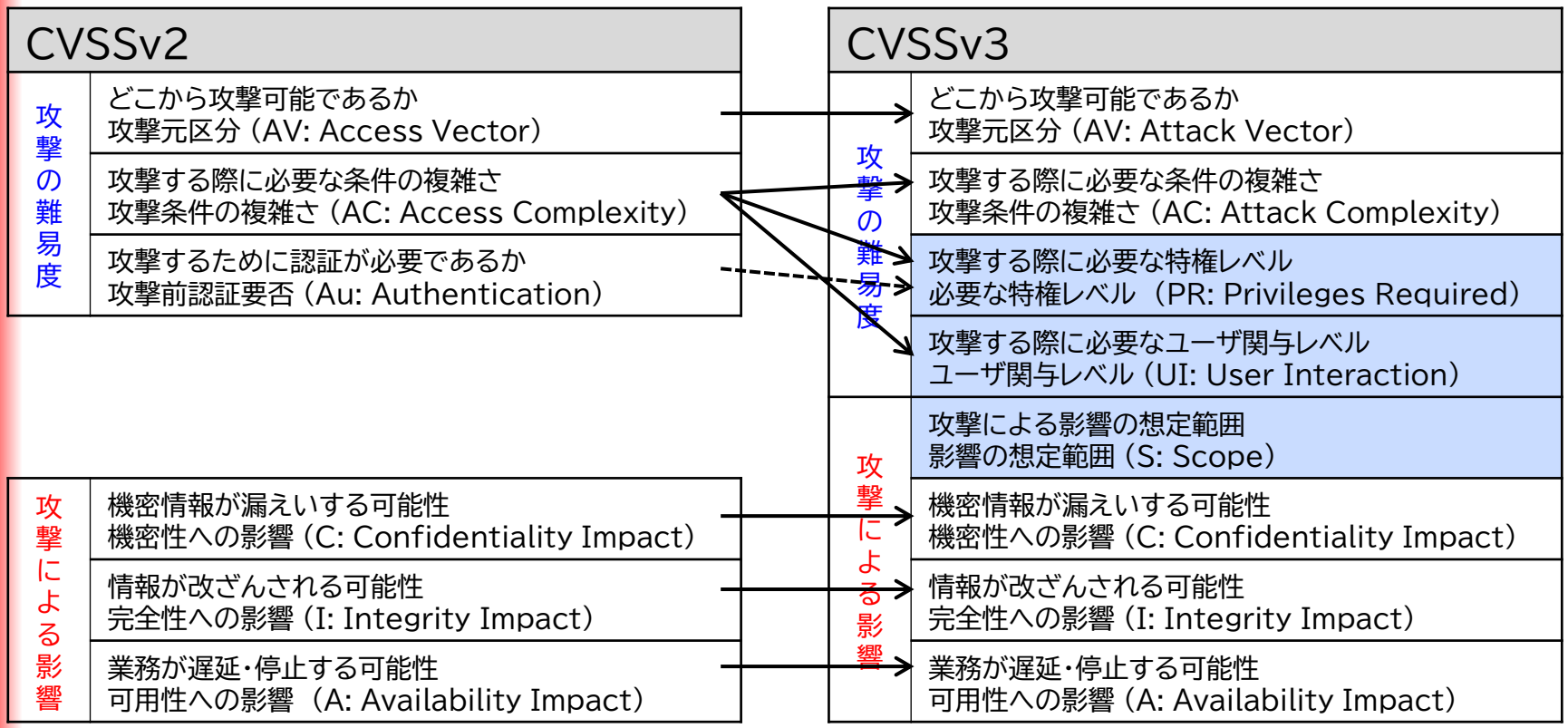
- CVSSスコア算出アプローチの変更
  - CVSS v1～v3.1：計算式から算出
  - CVSS v4：270個のスコア区分に振り分けた後、微調整して算出（MacroVectors and Interpolation）

CVSS（共通脆弱性評価システム）v4.0

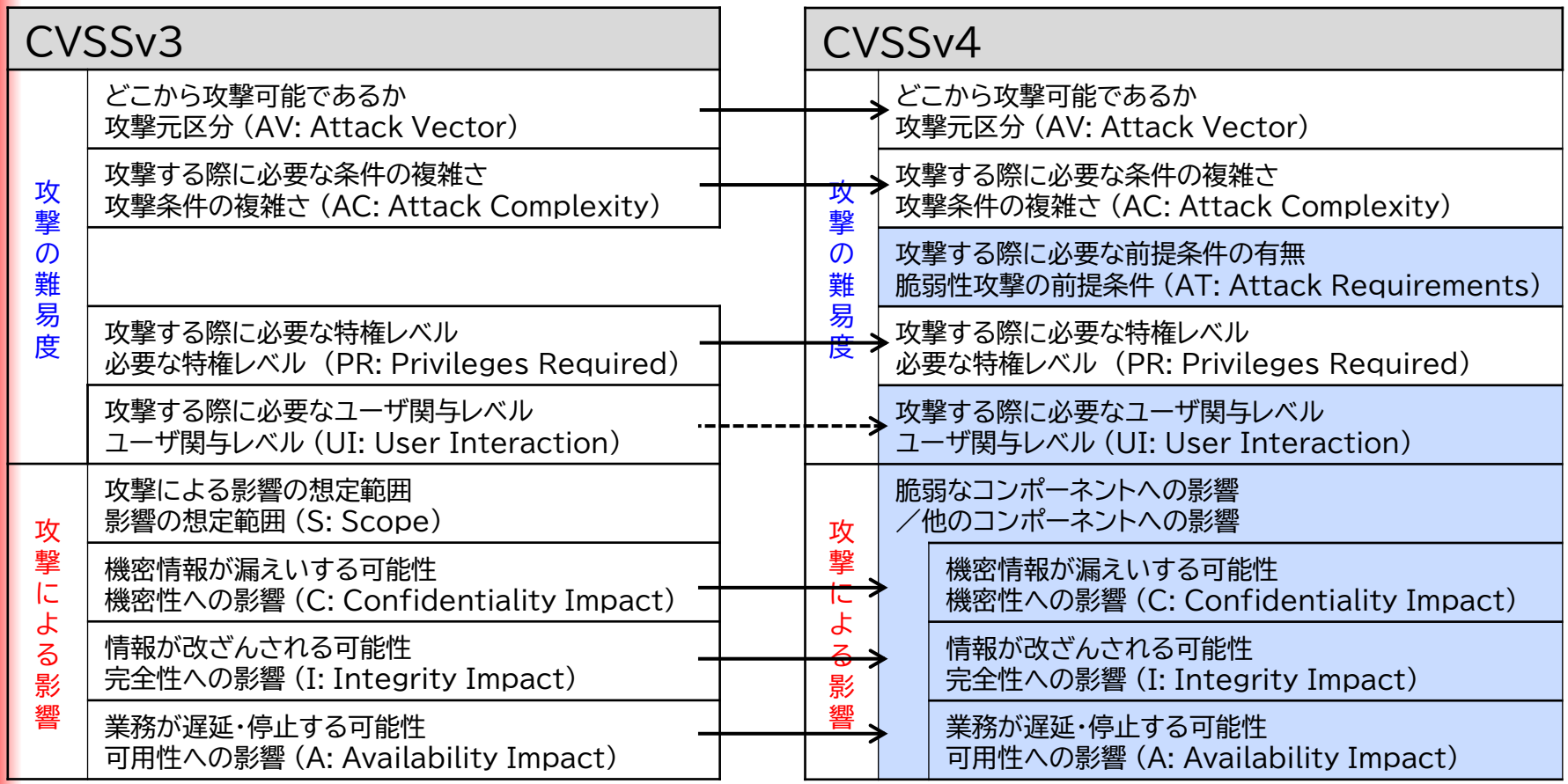
- 基本評価基準、脅威評価基準、環境評価基準、補助評価基準の4つから構成
- CVSSスコア算出に使用するのは、基本評価基準、脅威評価基準、環境評価基準の3つ

基本評価基準	脅威評価基準	環境評価基準	補助評価基準
攻撃の難易度 ● 攻撃元区分 ● 攻撃条件の複雑さ ● 脆弱性攻撃の前提条件 ● 必要な特権レベル ● ユーザ関与レベル	● 攻撃の成熟度	対策後の基本評価の再評価 ● 攻撃元区分 ● 攻撃条件の複雑さ ● 脆弱性攻撃の前提条件 ● 必要な特権レベル ● ユーザ関与レベル ● 脆弱なシステムへの影響（機密性） ● 脆弱なシステムへの影響（完全性） ● 脆弱なシステムへの影響（可用性） ● 他のシステムへの影響（機密性） ● 他のシステムへの影響（完全性） ● 他のシステムへの影響（可用性）	● 安全性 ● 攻撃の自動化可能性 ● 情報の緊急度 ● 回復の手段 ● 攻撃に利用可能な資源 ● 対処するための労力
攻撃による影響 ● 脆弱なシステムへの影響（機密性） ● 脆弱なシステムへの影響（完全性） ● 脆弱なシステムへの影響（可用性） ● 他のシステムへの影響（機密性） ● 他のシステムへの影響（完全性） ● 他のシステムへの影響（可用性）		● 機密性の要求 ● 完全性の要求度 ● 可用性の要求度	

CVSS（共通脆弱性評価システム）v4.0
基本評価基準：v2からv3への変更点



CVSS（共通脆弱性評価システム）v4.0
基本評価基準：v3からv4への変更点

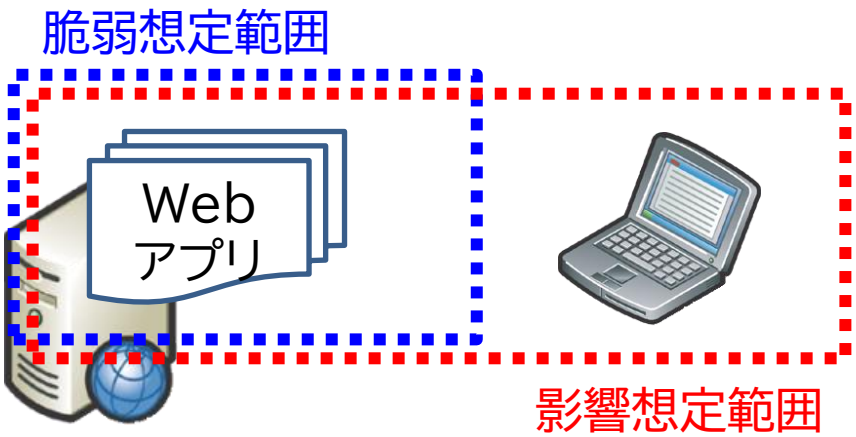


CVSS(共通脆弱性評価システム) v4.0
基本評価基準:脆弱性による二次的な影響波及の表記方法

- 脆弱性による二次的な影響波及の表記方法 (v3)
  - スコープ
    - 脆弱想定範囲(Vulnerable Component):攻撃者がソフトウェアの脆弱性を悪用して攻撃できる対象(コンポーネント)範囲
    - 影響想定範囲(Impacted Component):脆弱性を悪用された場合に及ぶ影響範囲

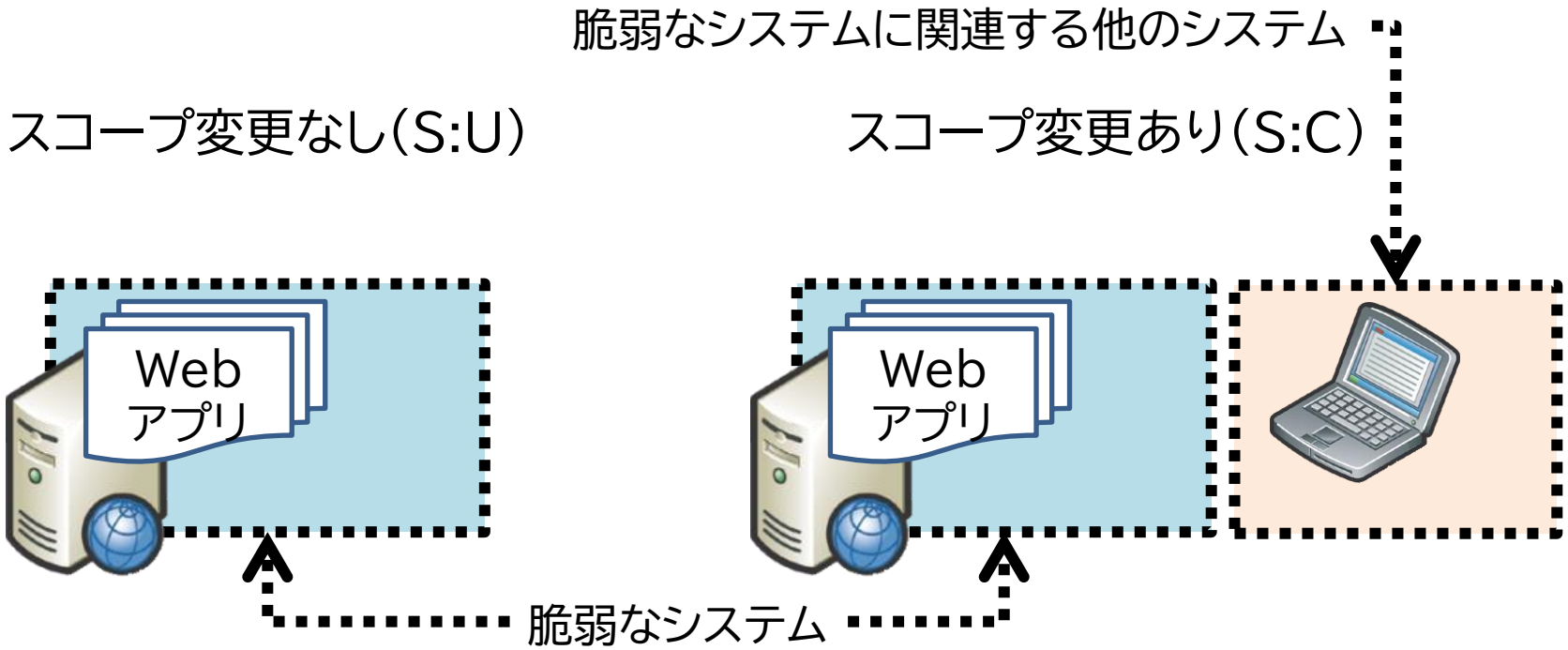
スコープ変更なし(S:U)

スコープ変更あり(S:C)



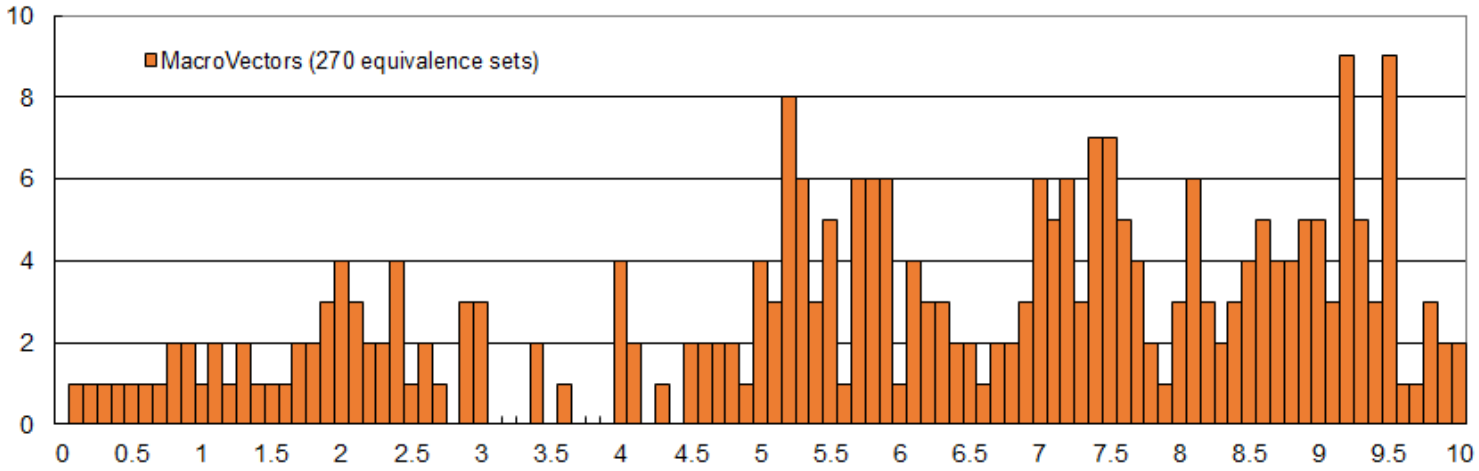
CVSS(共通脆弱性評価システム) v4.0
基本評価基準:脆弱性による二次的な影響波及の表記方法

- 脆弱性による二次的な影響波及の表記方法 (v4)
  - 脆弱なシステムへの影響／他のシステムへの影響
    - 脆弱なシステムを対象とした影響をCIAで表記
    - 脆弱なシステムに関連する他のシステムへの影響をCIAで表記



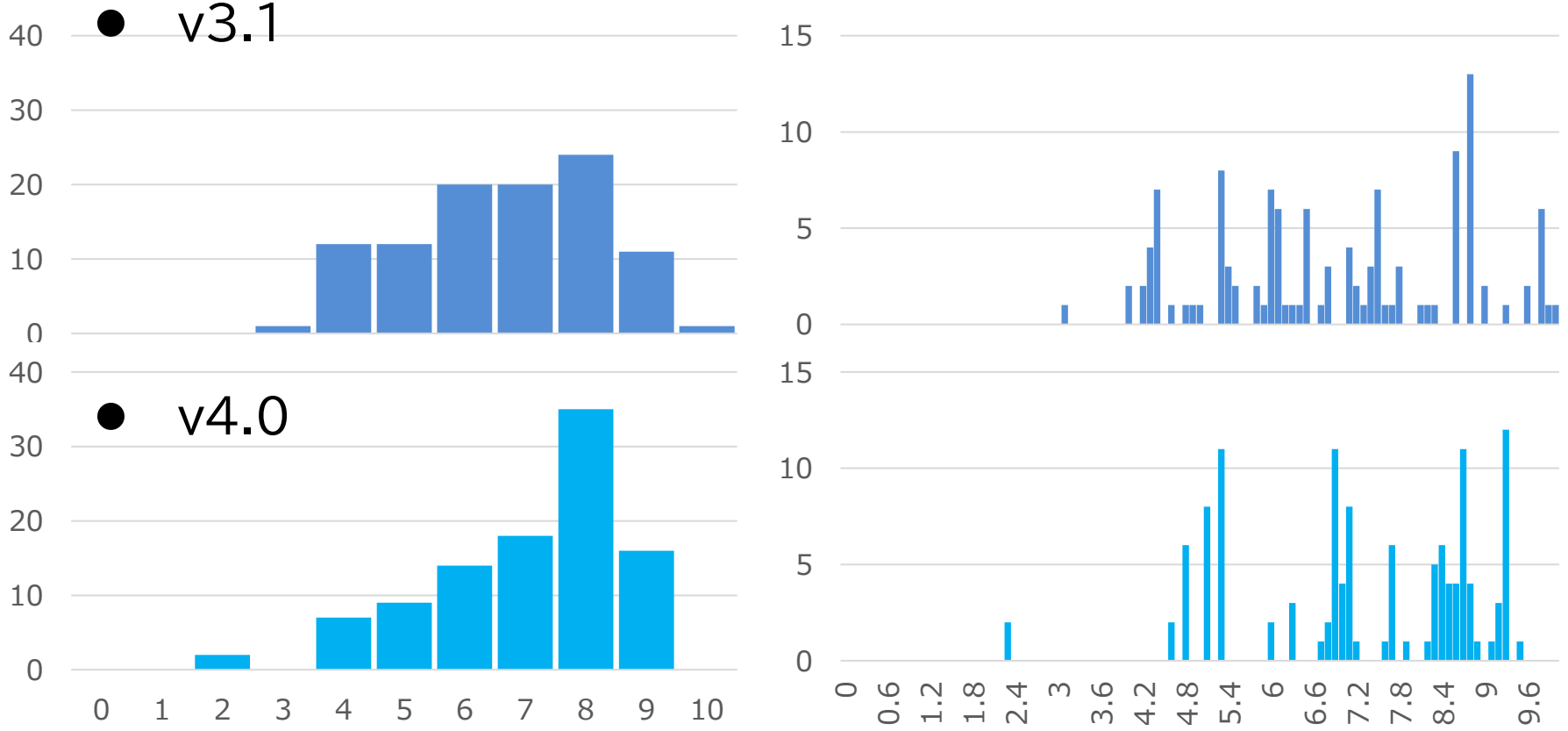
CVSS(共通脆弱性評価システム) v4.0
スコアの算出方法:v4への変更点

- CVSS v1～v3.1:計算式から算出
- CVSS v4:270個のスコア区分に振り分けた後、微調整して算出
  - CVSS環境値(CVSS-BTE:基本評価＋脅威評価＋環境評価)の組合せ、約1500万件を元に270個のスコア区分を作成
  - パラメタ値の組合せの特徴から、270個のスコア区分のいずれかに振分け
  - スコア区分に付与されているCVSSスコア値に対して、CVSSスコア区分値とスコア値が低くなる組合せとの差を元に、微調整をして算出



CVSS(共通脆弱性評価システム) v4.0
スコアの算出方法:v4への変更点

- 基本評価値の比較(事例122件による比較)



CWE(共通脆弱性タイプ一覧)
Common Weakness Enumeration

- 脆弱性を種別毎に分類
  - 2024 CWE トップ 25
    - スコア：NVD(米国脆弱性対策データベース)での出現頻度とCVSS(共通脆弱性評価システム)の深刻度から算出
    - 掲載数：KEV(悪用された既知の脆弱性一覧)での出現数

#	CWE	名称	スコア	掲載数
1	CWE-79	クロスサイトスクリプティング	56.92	3
2	CWE-787	領域外メモリへの書き出し	45.20	18
3	CWE-89	SQL インジェクション	35.88	4
4	CWE-352	クロスサイトリクエストフォージェリ	19.57	0
5	CWE-22	ディレクトリトラバーサル	12.74	4

［出典］ 共通脆弱性タイプ一覧CWE概説
https://www.ipa.go.jp/security/vuln/CWE.html
CWE - Common Weakness Enumeration
https://cwe.mitre.org/

CWE（共通脆弱性タイプ一覧）
Common Weakness Enumeration

- 脆弱性を種別毎に分類
  - 2024 CWE トップ 25

#	CWE	名称	スコア	掲載数
6	CWE-125	領域外のメモリ参照	11.42	3
7	CWE-78	OS コマンドインジェクション	11.30	5
8	CWE-416	メモリの解放後使用	10.19	5
9	CWE-862	認可の欠落	10.11	0
10	CWE-434	適切でないアップロードファイル制限	10.03	0
11	CWE-94	コードインジェクション	7.13	7
12	CWE-20	適切でない入力確認	6.78	1
13	CWE-77	コマンドインジェクション	6.74	4
14	CWE-287	適切でない認証	5.94	4
15	CWE-269	適切でない権限の管理	5.22	0

CWE（共通脆弱性タイプ一覧）
Common Weakness Enumeration

- 脆弱性を種別毎に分類
  - 2024 CWE トップ 25

#	CWE	名称	スコア	掲載数
16	CWE-502	信頼できないデータのデシリアライゼーション	5.07	5
17	CWE-200	機密情報の不正な漏洩	5.07	0
18	CWE-863	適切でない認可	4.05	2
19	CWE-918	サーバサイドリクエストフォージェリ	4.05	2
20	CWE-119	メモリバッファ境界での適切でない操作制限	3.69	2
21	CWE-476	NULL ポインタ参照	3.58	0
22	CWE-798	資格情報がハードコーディングされている問題	3.46	2
23	CWE-190	整数オーバーフロー	3.37	3
24	CWE-400	適切でないリソース消費制限	3.23	0
25	CWE-306	重要な機能に対する認証の欠如	2.73	5

CPE(共通プラットフォーム一覧)
Common Platform Enumeration

- 情報システムを構成するハードウェア、
  ソフトウェアの名称を、プログラムで
  (機械)処理しやすい形式で記述するための仕様≒製品識別子

IPAが提供するMyJVN

IPAが提供するマイ・ジェイ・ブイ・エヌ

情報処理推進機構が
提供するMyJVN

アイ・ピー・エーが
提供するMyJVN

情報処理推進機構が
提供するマイ・ジェイ・ブイ・エヌ

CPE v2.2

cpe:/a:ipa:myjvn

cpe:/{種別}:{ベンダ}:{製品}:{バージョン}
:{アップデート}:{エディション}:{言語}

種別:h=ハードウェア、o=OS、a=アプリケーション

CPE(共通プラットフォーム一覧)
Common Platform Enumeration

- その他の製品識別子
  - CPE v2.3
    cpe:2.3:{種別}:{ベンダ}:{製品}:{バージョン}:{アップデート}:{エディション}:{言語}: {sw_edition}:{target_sw}:{target_hw}:{その他}
    cpe:2.3:a:company_a:application:1.1:*:*:*:*:*:*:*
  - purl(package URL)
    pkg:{タイプ}/{名前空間}/{パッケージ名}@{バージョン}?{修飾子}#{パス}
    pkg:maven/org.company_b/browser@2.1
  - SWID(ソフトウェア識別子、Software identification tag)
    ISO19770-2で標準化されたソフトウェア識別タグの仕様
    グローバルなユニークIDで16バイトのUUID or タグ生成者によって定義された値
  - TEI(Transparency Exchange Identifier)
    OWASPが提案する複数の製品識別子を統合する仕様
    urn:tei:{TEI type}:{DNS domain}:{製品識別子}
    urn:tei:uuid:products.example.com:d4d9f54a-abcf-11ee-･･･

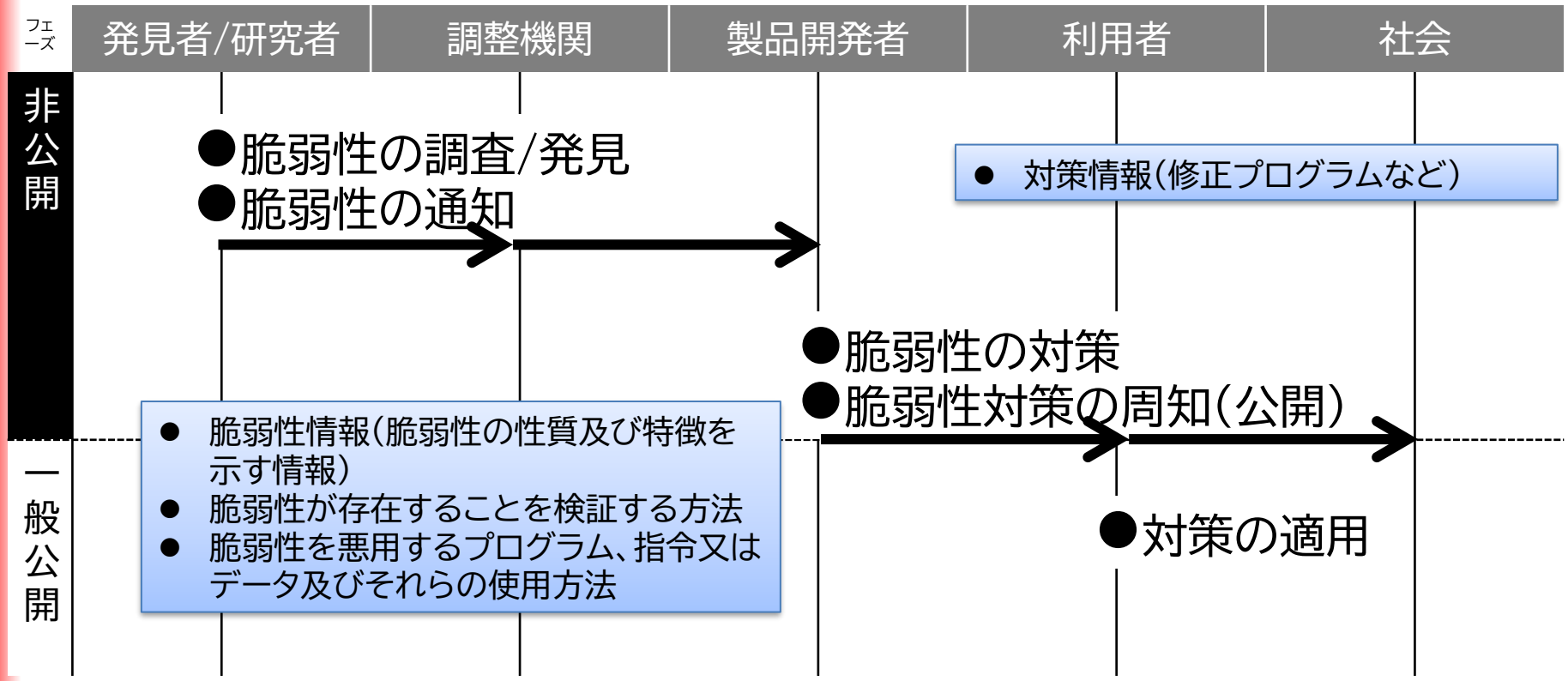
脆弱性(ぜいじゃくせい)の開示

- フルディスクロージャ(Full Disclosure)(1993年)
  セキュリティに関するひとつの考え方であり、「真にセキュアなシステムとは、プロトコル、ソースコードなどすべての視点でオープンレビューに耐えうること」「脆弱性に関する詳細情報はすべてのユーザが利用できること」としている。

- 脆弱性開示ポリシー(Vulnerability Disclosure Policy)
  - 脆弱性情報の取り扱いに関する考え方
  - 発見者、調整機関、製品開発ベンダなどが、自身の立場での考え方をまとめたものであり、全体としての整合性が取れているわけではない。

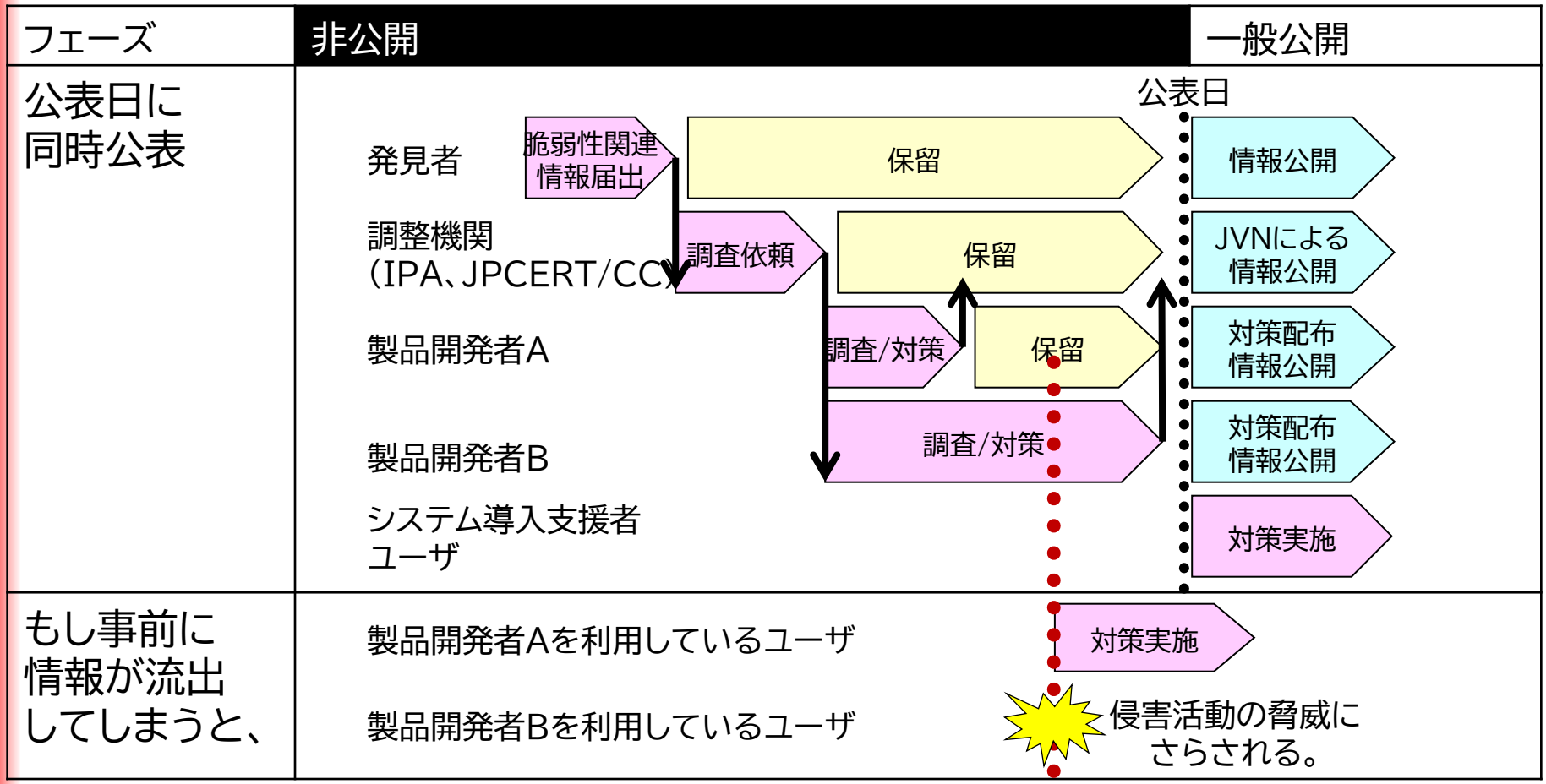
脆弱性(ぜいじゃくせい)の開示
脆弱性ハンドリングとは

- サイバー攻撃による被害発生を抑制するために、関係者が推進する関連情報の適切な流通活動
- 脆弱性の発見、通知、対策、周知(公開)、適用までの一連のプロセス



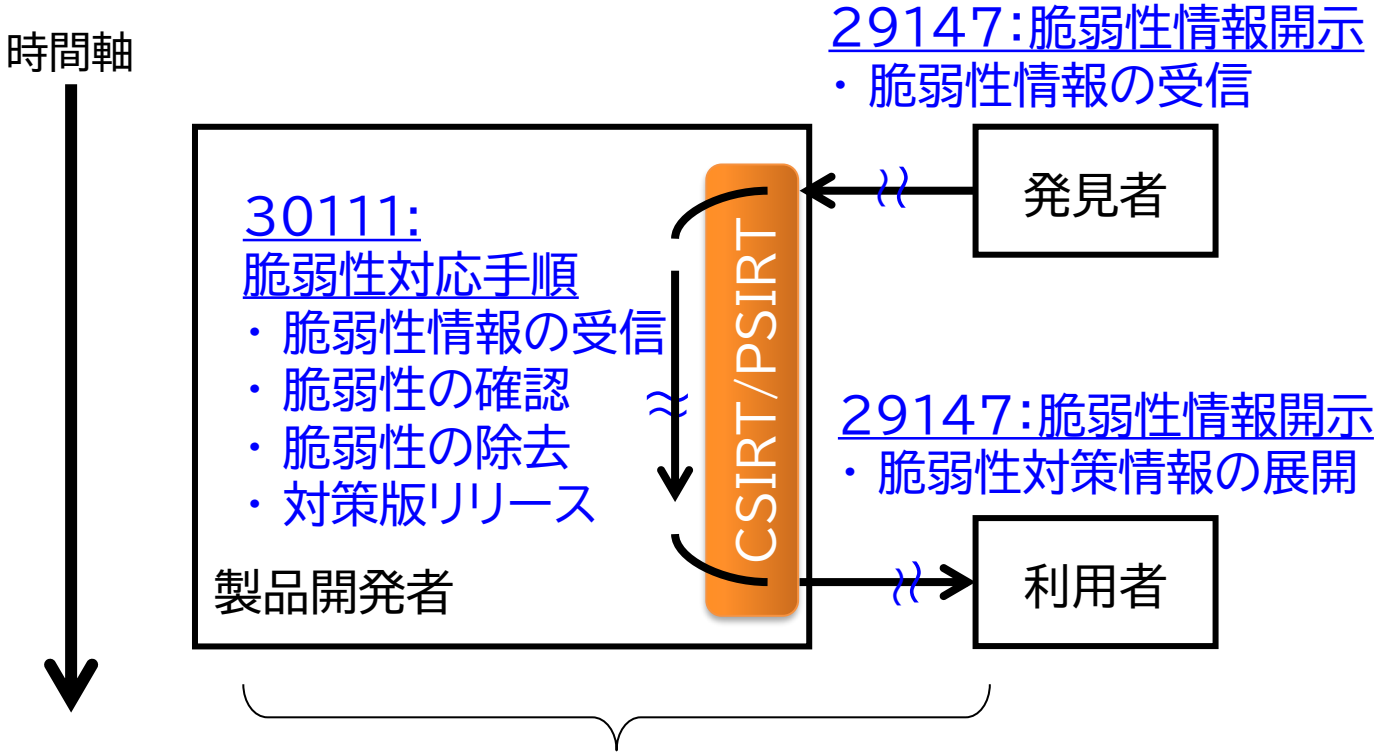
脆弱性(ぜいじゃくせい)の開示
公開日一致の原則

- 該当製品の対策を揃えつつ、格差のない対策環境を提供する考え方



脆弱性(ぜいじゃくせい)の開示
国際標準ISO/IEC

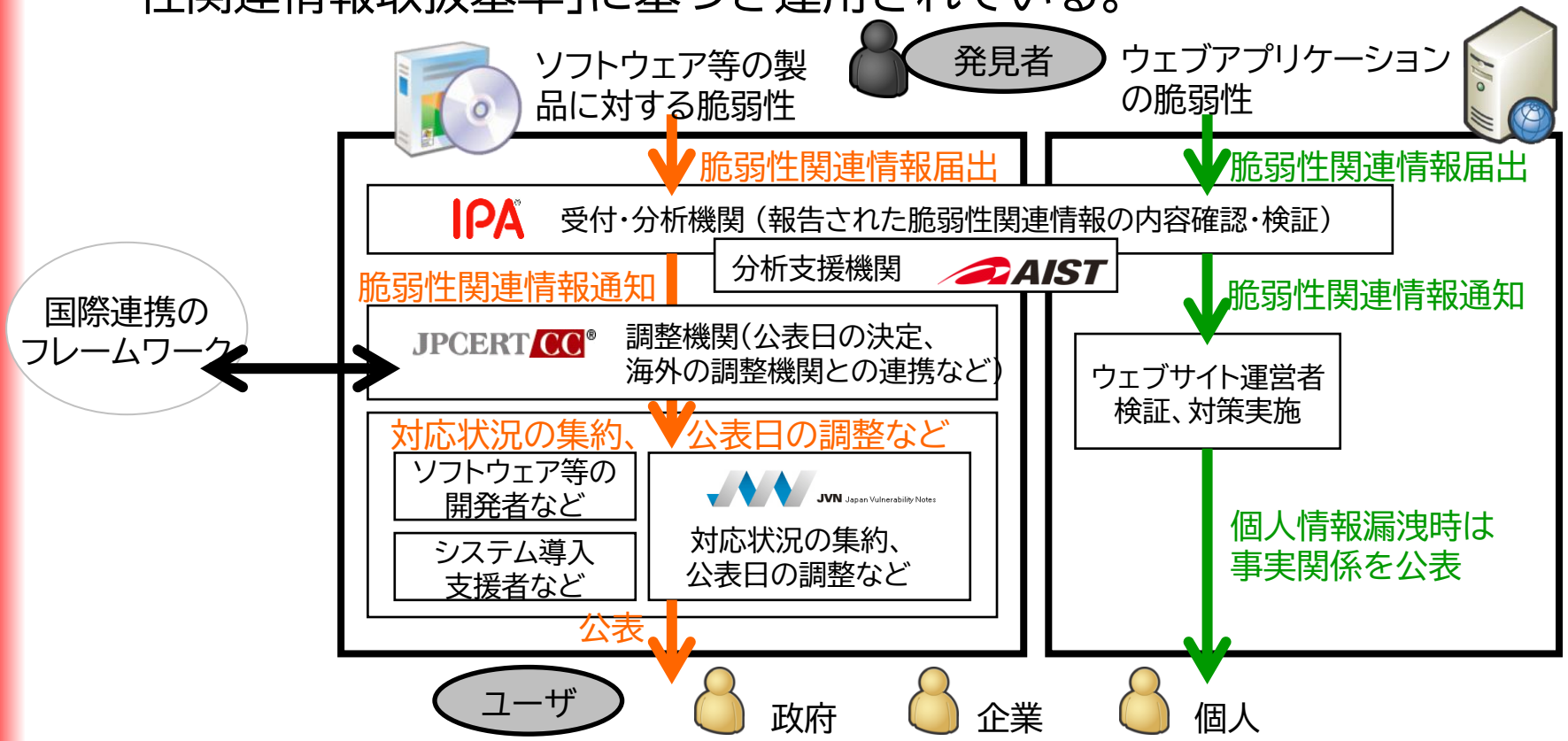
- ISO/IEC 29147、30111（2008年～2014年にかけて初版標準化）



製品開発者の脆弱性開示ポリシー(Vulnerability Disclosure Policy)
＝脆弱性情報開示、脆弱性対応手順の考え方をまとめたもの

脆弱性(ぜいじゃくせい)の開示
情報セキュリティ早期警戒パートナーシップ

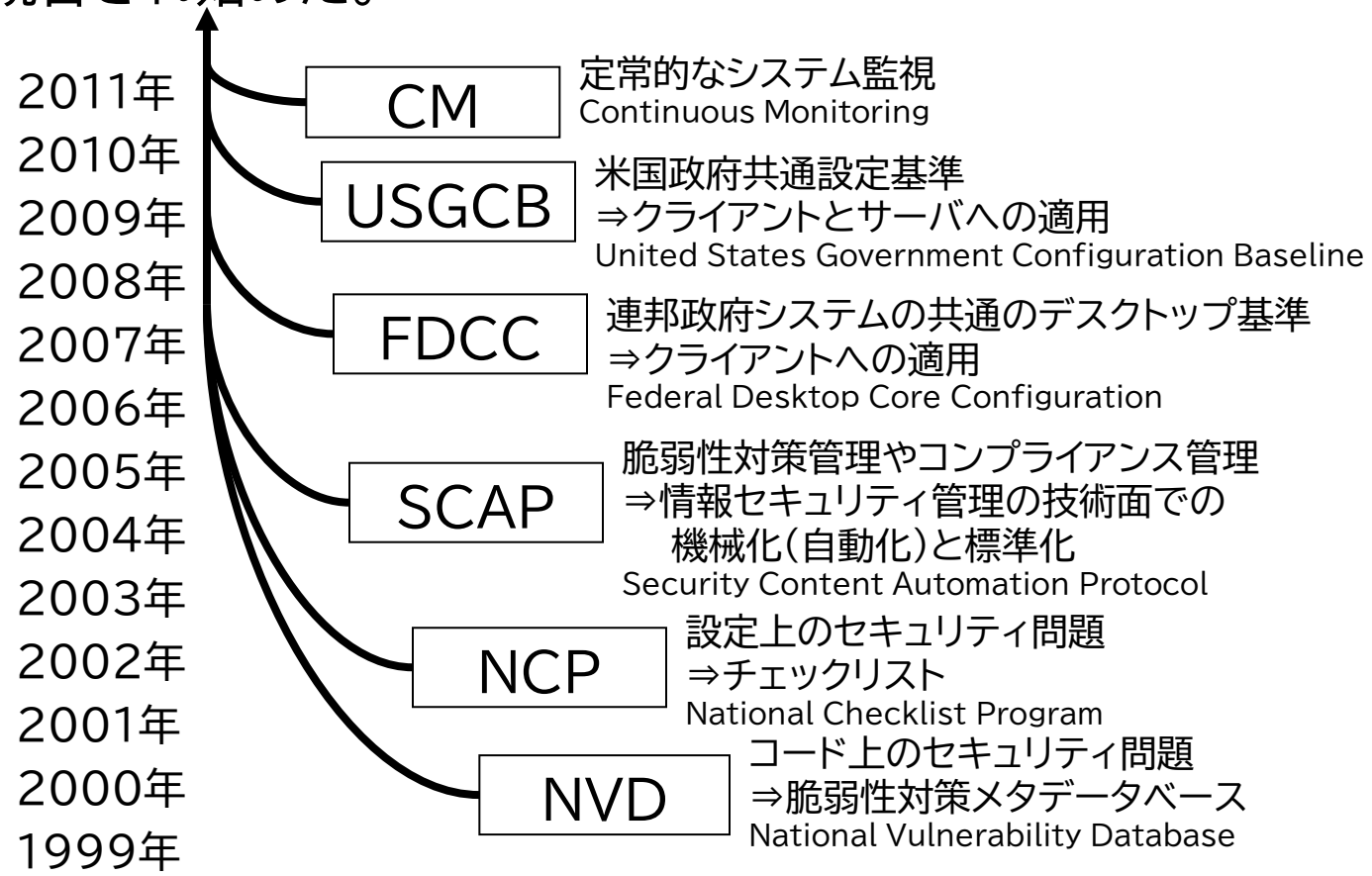
- ソフトウェア等の製品やウェブアプリケーションに見つかった脆弱性に関する情報を受け付け、製品開発者に修正を促すフレームワーク
- 2004年7月8日施行の脆弱性関連情報の取扱い「ソフトウェア等脆弱性関連情報取扱基準」に基づき運用されている。



自動化(機械化)処理基盤の潮流

自動化(機械化)処理基盤の潮流
米国における取り組み:脆弱性対策

- 2002年のFISMA(連邦情報セキュリティマネジメント法、Federal Information Security Management Act)の施行以降、各種活動が統合され始めた。

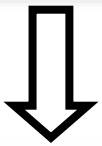


自動化(機械化)処理基盤の潮流
SCAP(セキュリティ設定共通化手順)

- 稼働する情報システムが、抽象レベルで記載された情報システムセキュリティの規格やガイドラインに沿っているかを手作業で確認することは難しいため、機械処理により実現すべきであることから始まった。

【 課題 】

セキュリティ設定に関する作業を手作業で行なうと、設定ミスや設定者のセキュリティ知識の程度や判断の相違などによりセキュリティ要件を損なう可能性大

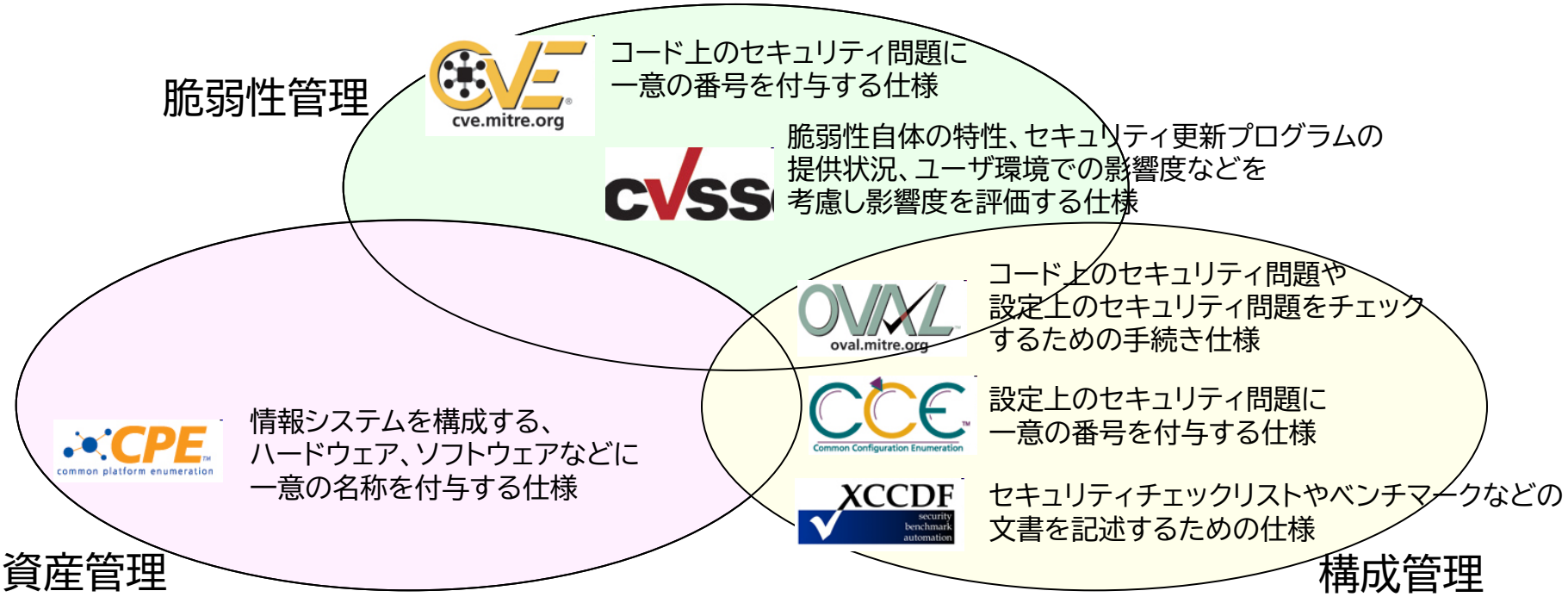


【 解決策 】

作業の機械化(自動化)による対処
⇒ SCAP(Security Content Automation Protocol)

自動化(機械化)処理基盤の潮流
SCAP(セキュリティ設定共通化手順)

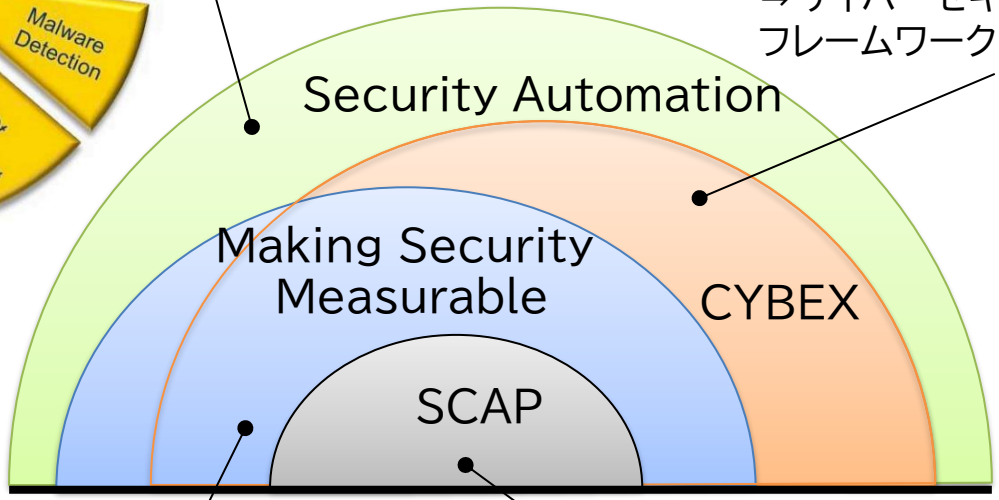
- 脆弱性管理、コンプライアンス管理の一部を機械化(自動化)することにより、情報システムに対するセキュリティ対策の負荷軽減と情報セキュリティ施策の推進の両立を目的とした6つの仕様から構成されている。



自動化(機械化)処理基盤の潮流
自動化(機械化)処理基盤に関連する仕様

Security Automation
⇒米NISTがSP800-137(Information Security Continuous Monitoring for Federal Information Systems and Organizations)で想定する対象の仕様群

X.1500
⇒サイバーセキュリティ情報交換フレームワーク、ITU-Tで規定する仕様群



Making Security Measurable
⇒米MITRE社で開発した仕様群

SCAP
⇒Security Content Automation Protocol:セキュリティ設定共通化手順、米NISTがFDCC、USGCBで使用する仕様群

自動化(機械化)処理基盤の潮流
NCP(National Checklist Program)

- NIST SP800-70で規定された、
  『セキュリティ設定のガイド』の開発ならびに
  共有支援プログラム
- 米国連邦政府内部で使用される(使用される可能性のある)
  コンピュータハードウエアまたはソフトウェア、システムに関連する
  セキュリティリスクを最小限に抑えるための設定とオプション選択を規
  定したチェックリストとリポジトリを整備している。
- NCPチェックリストリポジトリには、825件(単一製品のバージョン違い
  含む)の『セキュリティ設定のガイド』が登録されている。

*)セキュリティ設定ガイドは、セキュリティ設定チェックリスト、ロックダウンガイド、セキュリティ強化ガイド、ベンチマーク等とも呼ばれる。

[出典] National Checklist Program for IT Products: Guidelines for Checklist Users and Developers
https://csrc.nist.gov/publications/detail/sp/800-70/rev-4/final
National Checklist Program Repository
https://nvd.nist.gov/ncp/repository

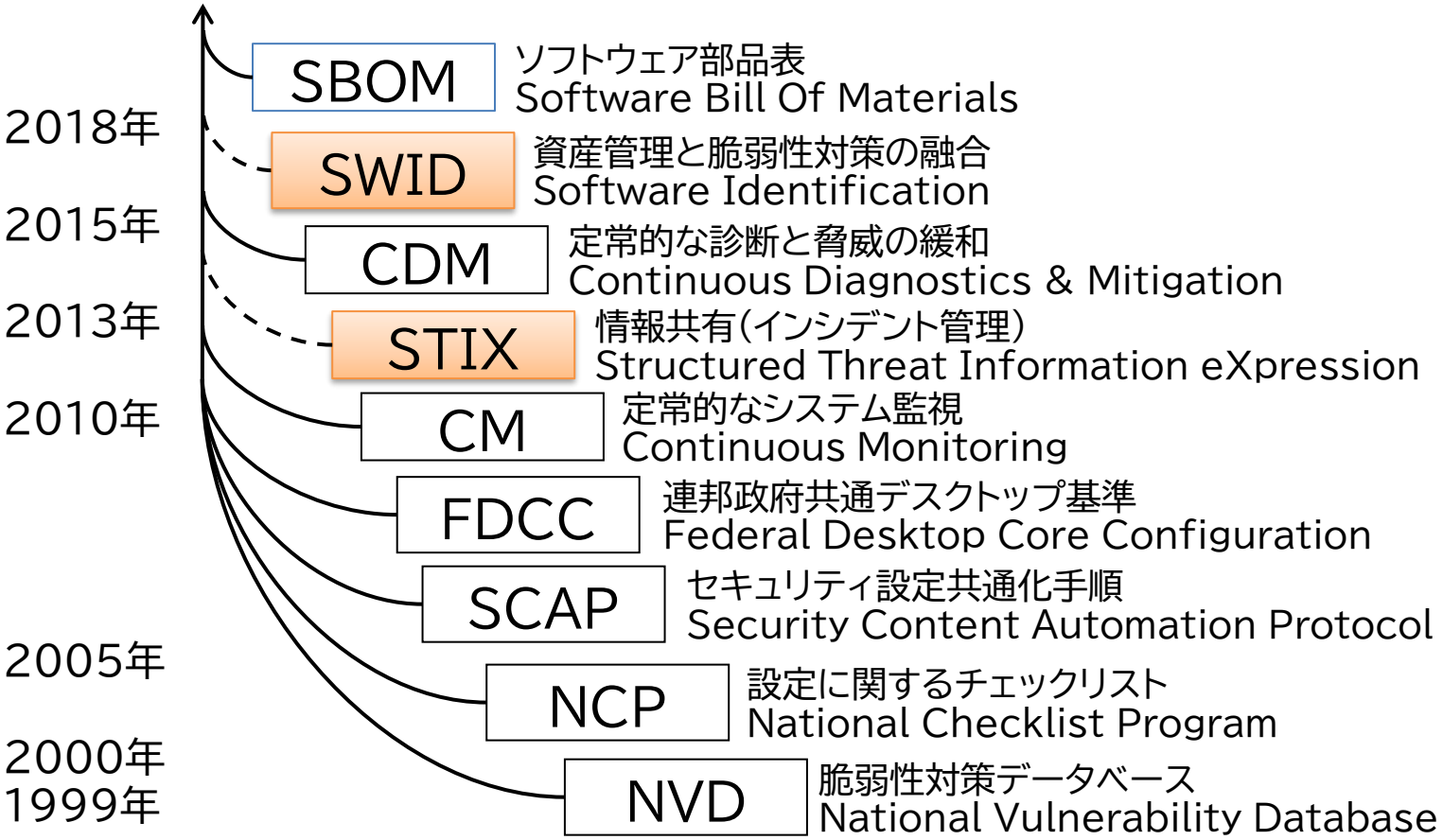
自動化(機械化)処理基盤の潮流
SCAP(セキュリティ設定共通化手順)

- 脆弱性対策を進める4つの視点(仕様、コード、設定、人)

脆弱性の分類	事例	チェック方法
仕様の脆弱性	認証の仕組みがない セキュア バイ デザイン	机上レビュー 手動検査(ペネトレーション検査)
コードの脆弱性 CVE cve.mitre.org	パスワードの値をチェックしていない パスワードがハードコーディングされている セキュア コーディング	ホワイトボックス型 ソースコード検査
		ブラックボックス型 未知の脆弱性　⇒ファジング検査
		ブラックボックス型 既知の脆弱性　⇒脆弱性検査
設定の脆弱性 CCE Common Configuration Enumeration NIST Security Configuration CHECKLISTS http://checklists.nist.gov CSD	アカウントとパスワードが同じ セキュア バイ デフォルト	セキュリティ設定検査 (ハードニング検査)
利用者の脆弱性	ソーシャルエンジニアリング	標的型訓練メールなど

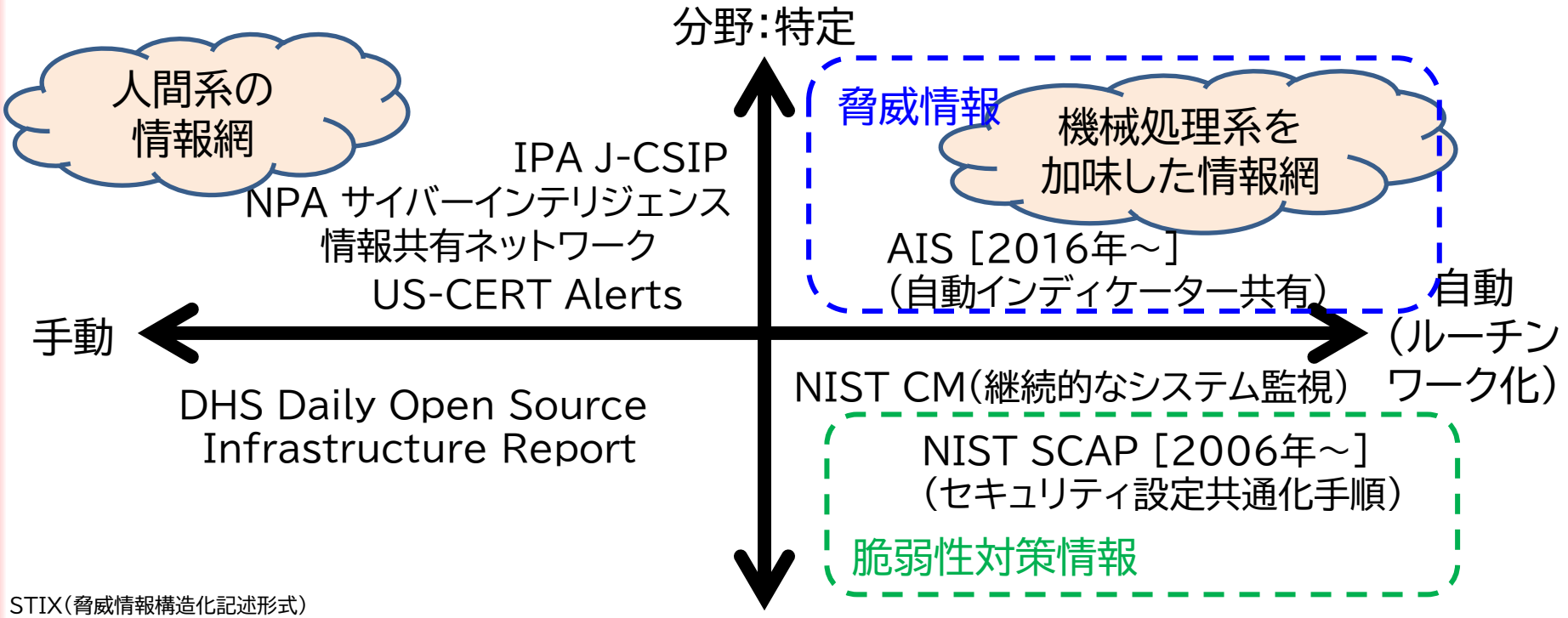
自動化(機械化)処理基盤の潮流
新たな動き

- 米国でのSecurity Automation(機械/コンピュータ処理可能な基盤)は、拡がり始めた。



自動化(機械化)処理基盤の潮流
米国における取り組み:情報共有

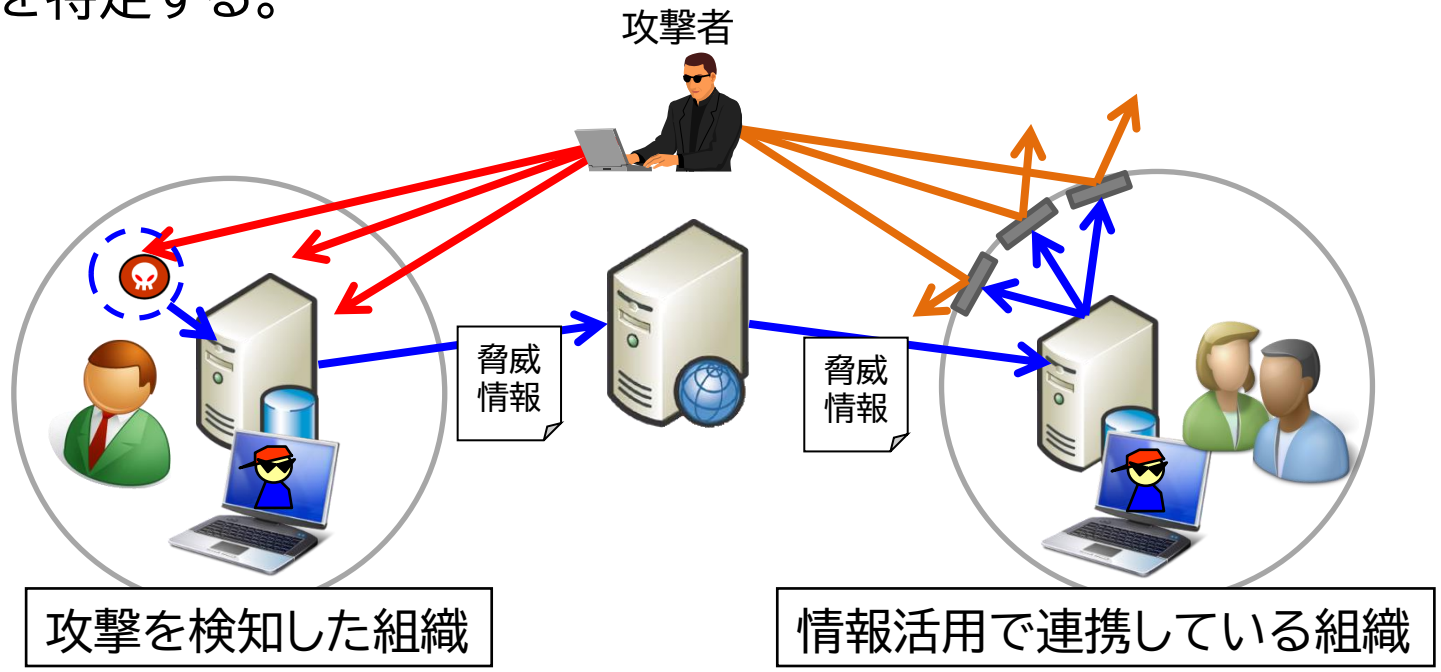
- 2012年頃から機械処理系を想定した大量の脅威情報が流通する仕組みが検討され始める。



STIX(脅威情報構造化記述形式)
Structured Threat Information eXpression
TAXII(検知指標情報自動交換手順)
Trusted Automated eXchange of Indicator Information

攻撃のモデル化と対処
多層防御としての(情報活用＋対策)

- 多層防御としての(情報活用＋対策)連携
  - 事前措置:組織にサイバー攻撃が行われる前に(入手タイミング)、組織にない情報を利用して(カバー率)、サイバー攻撃対策につなげる。
  - 事後措置:組織にない情報を利用してサイバー攻撃による影響有無を特定する。



攻撃のモデル化と対処
サイバー攻撃スピードへの追従

- 認知から対策までの時間短縮



アラートの観測　脅威の把握　対策の決定　脅威への対処

Manual(手動)

最悪のケース　11時間　45分

ベストケース　10分　45分

Automated(ルーチンワーク化)

最悪のケース　10分

ベストケース　1秒

対策までの時間の98%を削減可

トリアージ能力10000倍向上

60秒

30秒

攻撃のモデル化と対処
TLP(Traffic Light Protocol)

- 情報活用のための情報共有レベル区分
- 情報発行元毎に、区分を定義している(区分の定義は必ずしも一致しない場合があるので注意が必要)。

区分	US-CERT/FIRST.org	金融ISAC	会員区分に基づく例
TLP:RED	非公開、関係者限り	特定のグループ(会議参加者等)の受信者のみとし、当該グループ外への転送を禁ずる	宛先限り(ただし、受信者の上長や責任者への説明・報告は可)
TLP:AMBER	公開制限、関係者組織限り	金融ISAC会員限りで共有する	会員のみ
TLP:GREEN	公開制限、コミュニティ限り	金融 ISAC会員及び予め理事会が定める業界団体等の外部組織との共有を行うことが可能	会員に加えて、会員のグループ関係会社や外部委託先を含めた範囲で共有できる
TLP:CLEAN	公開制限なし	公知の情報として扱う ※著作権法その他の法令を遵守する	公開可能(ただし著作権法その他の法令は遵守する必要がある)

[出典] https://www.us-cert.gov/tlp
https://www.first.org/tlp/
http://f-isac.jp/pdf/F-ISACjpn_Management_Rules.pdf

攻撃のモデル化と対処
脅威表現の標準化（2012年）

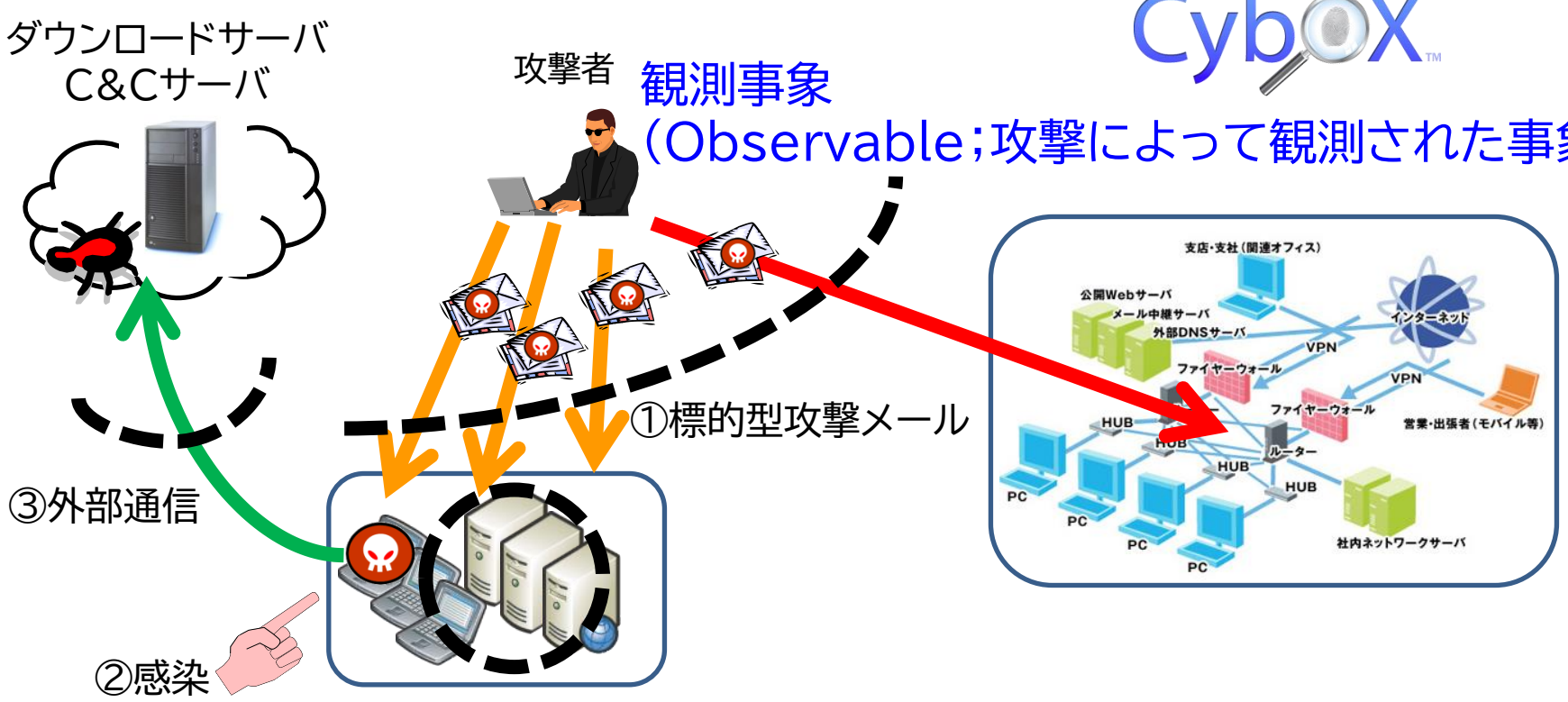
交換

TAXII™

攻撃活動分析(Campaign Analysis)

STIX™

CybOX™



攻撃のモデル化と対処
CybOX（サイバー攻撃観測記述形式）（2012年）

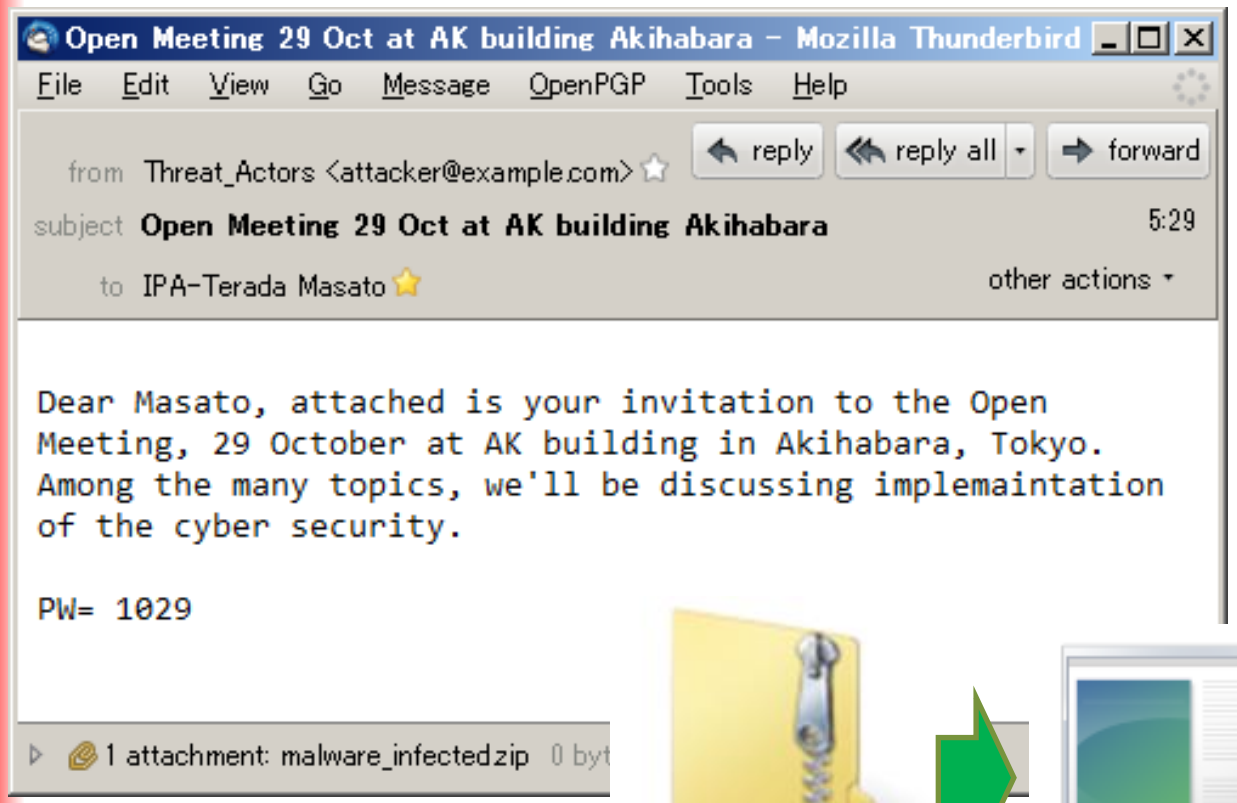
- MITREが中心となり仕様策定を進めてきたもので、サイバー攻撃活動によって観測された事象を記述するためのXML仕様である。MandiantのOpenIOC（侵害を受けたシステムの痕跡(Indicator of Compromise)を記述する仕様)を踏まえた仕様となっている。
- システム(Windows、UNIX)内部状態、ネットワーク通信、アプリケーション動作など、観測できる事象を記録する。

Common
API
Account
Address
Artifact
Code
Device
Disk
DomainName
File
HostName
:

Windows
Win File
Win Mutex
Win Process
Win Registry Key
Win Service
Win Task
Win User Account
Win Volume
:

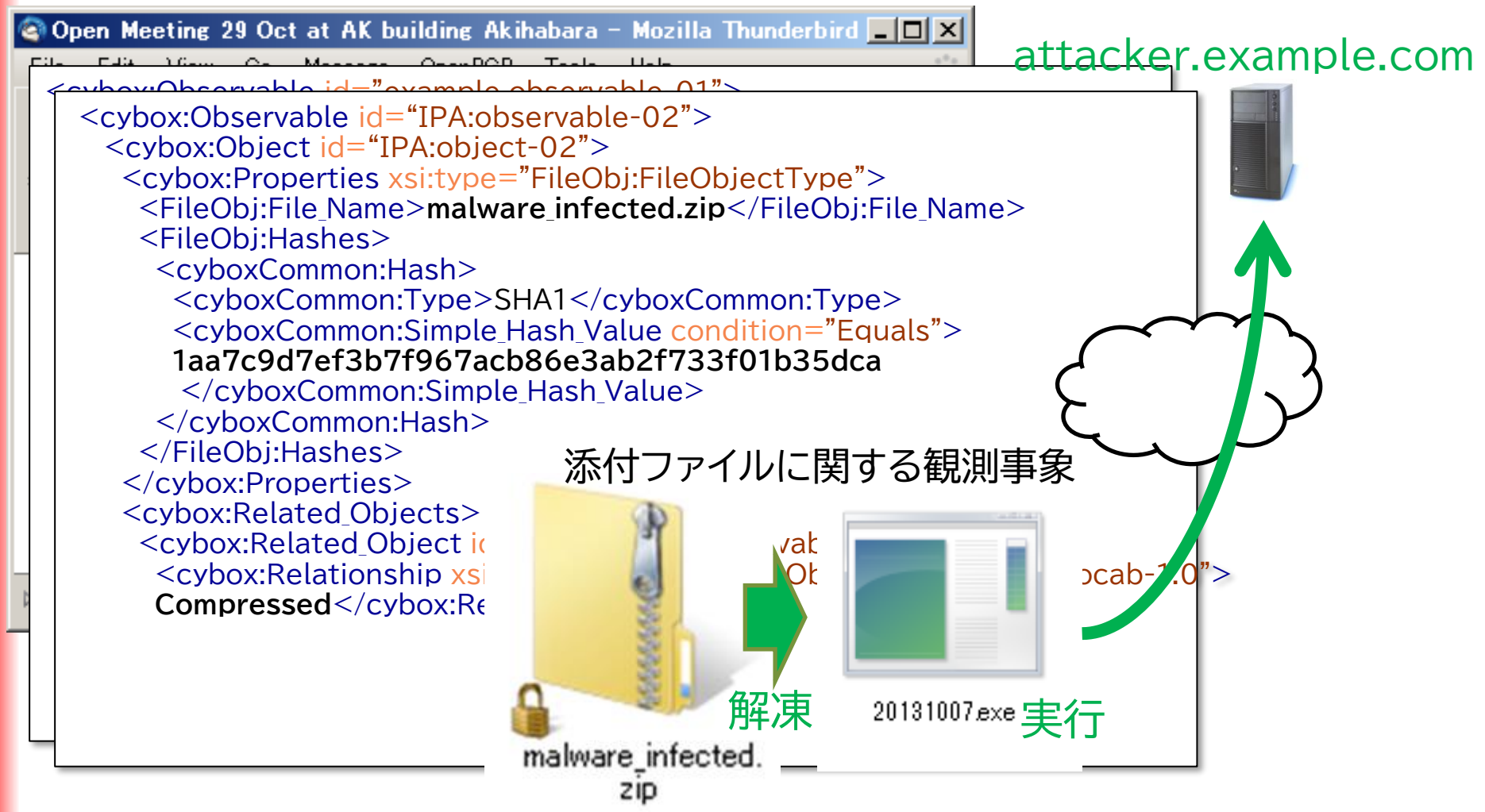
Network
Network Connection
Network Flow
Network Packet
Network Route
Network Socket
Port
Socket Address
:

攻撃のモデル化と対処
標的型攻撃メールの観測事象(Observable)記述例

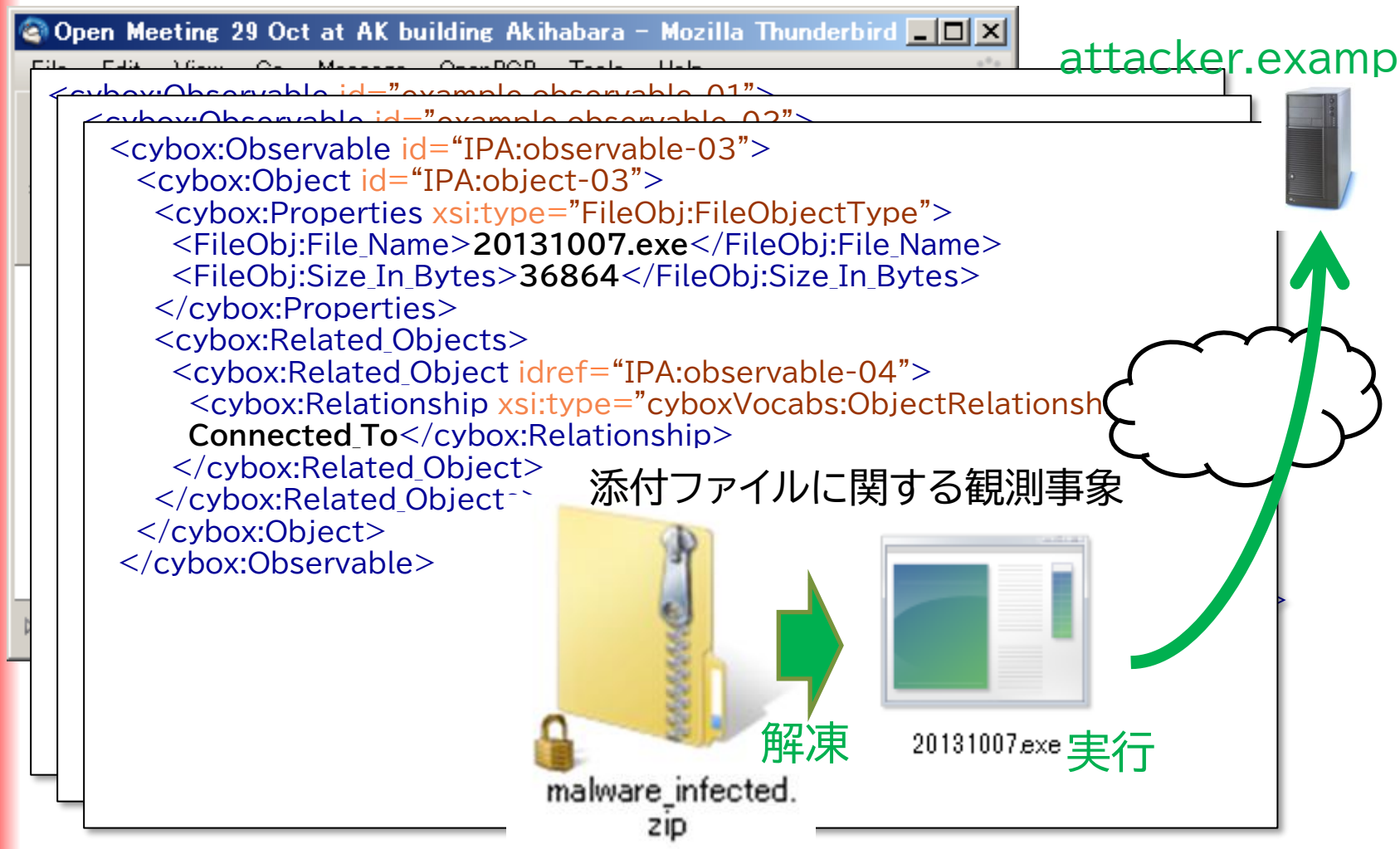


攻撃のモデル化と対処
標的型攻撃メールの観測事象(Observable)記述例

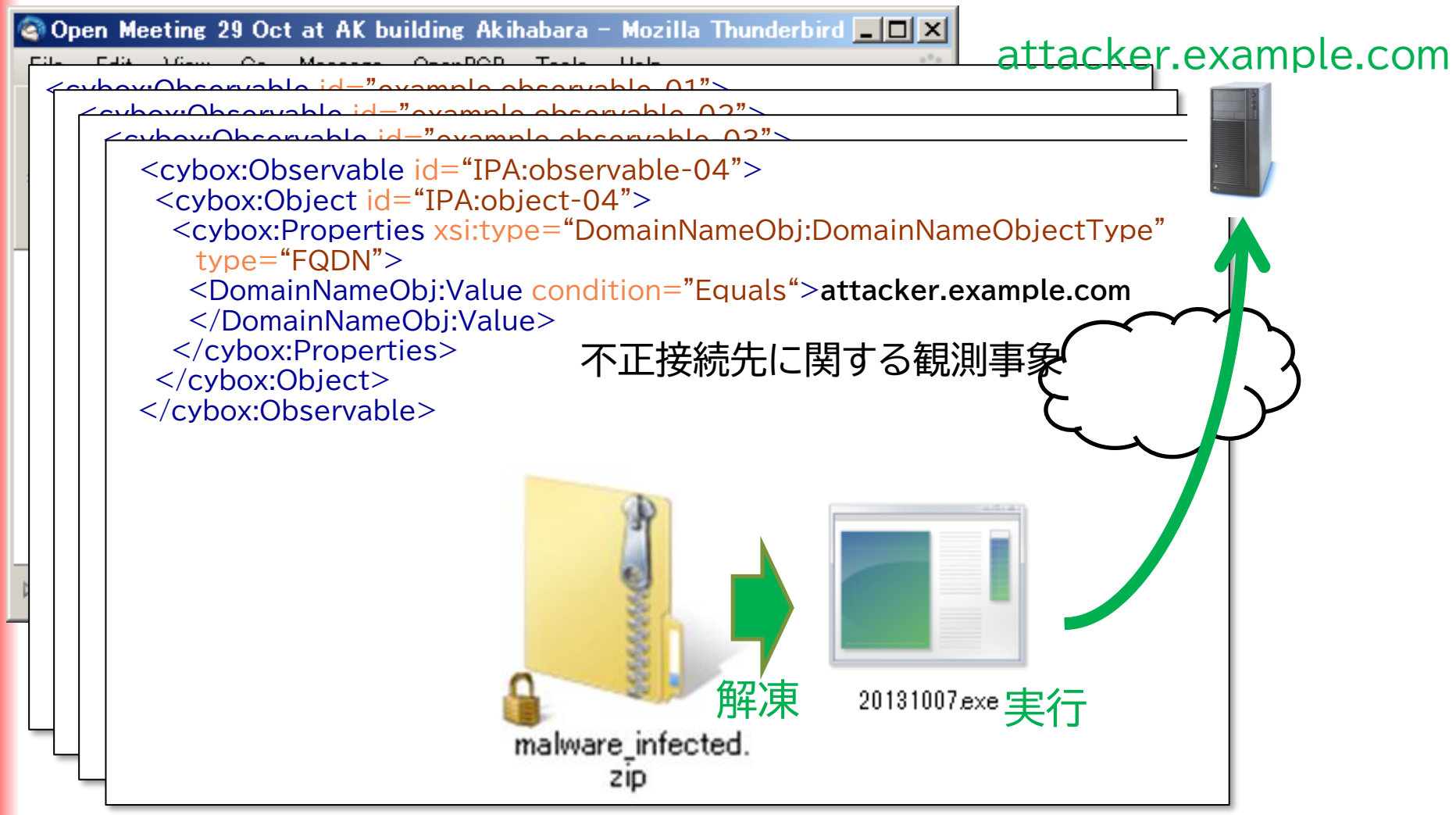
攻撃のモデル化と対処
標的型攻撃メールの観測事象(Observable)記述例



攻撃のモデル化と対処
標的型攻撃メールの観測事象(Observable)記述例



攻撃のモデル化と対処
標的型攻撃メールの観測事象(Observable)記述例



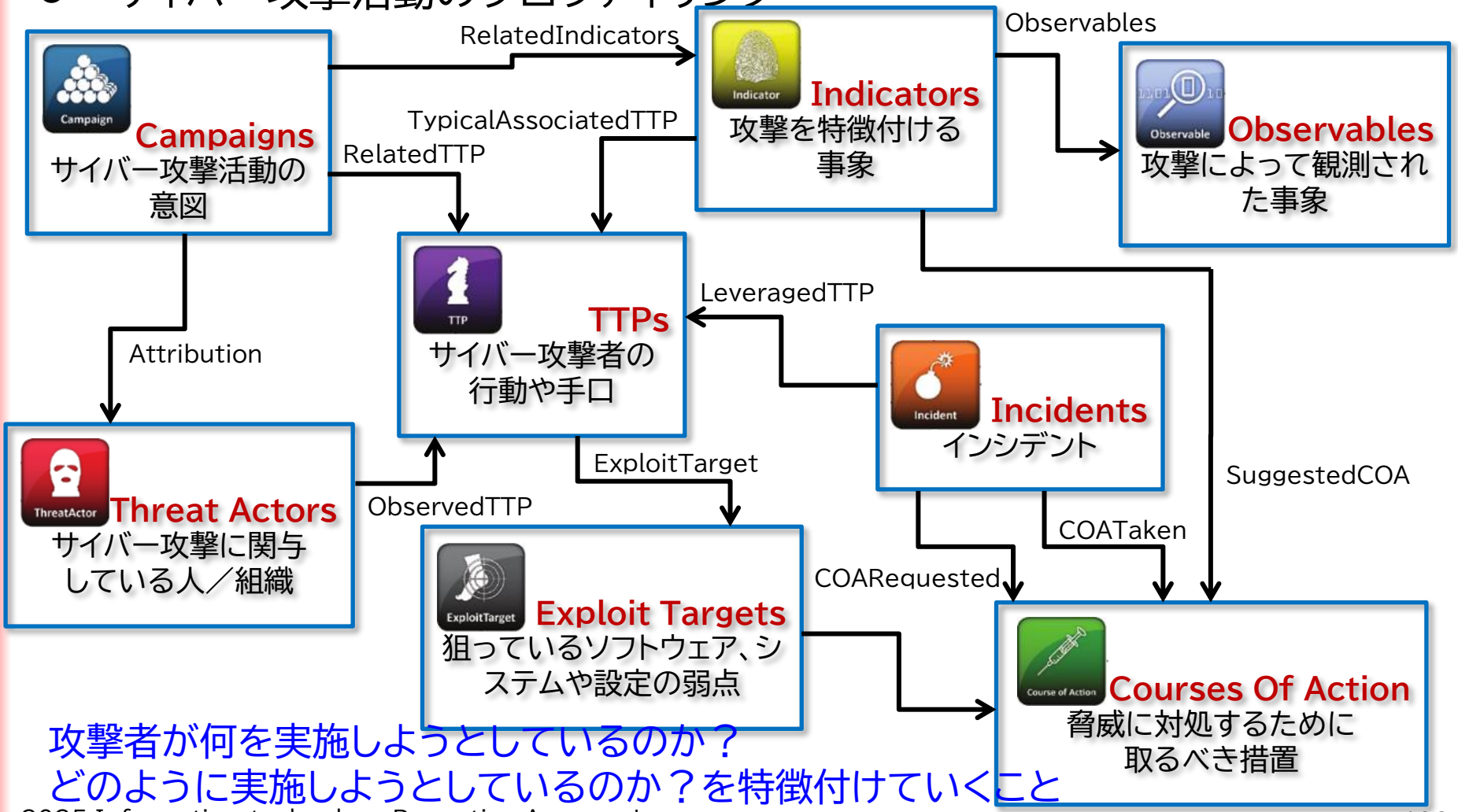
攻撃のモデル化と対処
STIX（脅威情報構造化記述形式）（2012年）

- MITREが中心となり仕様策定を進めてきたもので、サイバー空間における脅威やサイバー攻撃の分析、サイバー攻撃を特徴付ける事象の特定、サイバー攻撃活動の管理、サイバー攻撃に関する情報の共有などを目的としたXML仕様である。
- 8つの情報群から構成され、これらの情報群を関連づけて脅威情報を表現する。

情報群	脅威情報
サイバー攻撃活動（Campaigns）	サイバー攻撃活動における意図や攻撃活動の状態など
攻撃者（Threat Actors）	サイバー攻撃に関与している人または組織
攻撃手口（TTPs）	サイバー攻撃者の行動や手口、攻撃のパターン
検知指標（Indicators）	検知に有効なサイバー攻撃を特徴づける指標
観測事象（Observables）	サイバー攻撃によって観測された事象
インシデント（Incidents）	サイバー攻撃によって発生した事案
対処措置（Courses Of Action）	脅威に対処するために取るべき措置
攻撃対象（Exploit Targets）	攻撃の対象となりうるソフトウェアやシステムの弱点

攻撃のモデル化と対処
STIX(脅威情報構造化記述形式)(2012年)

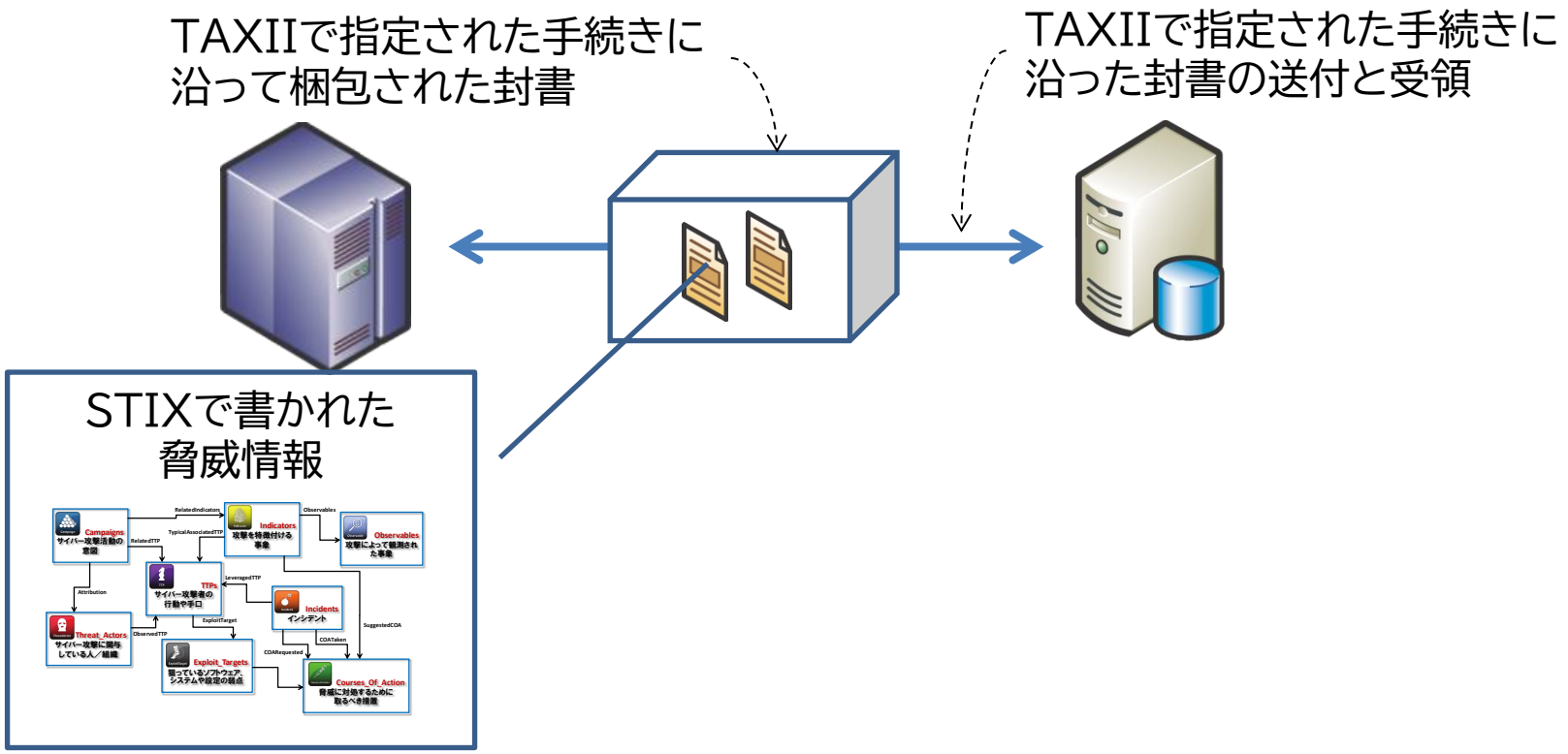
- サイバー攻撃活動のプロファイリング



攻撃者が何を実施しようとしているのか？
どのように実施しようとしているのか？を特徴付けていくこと

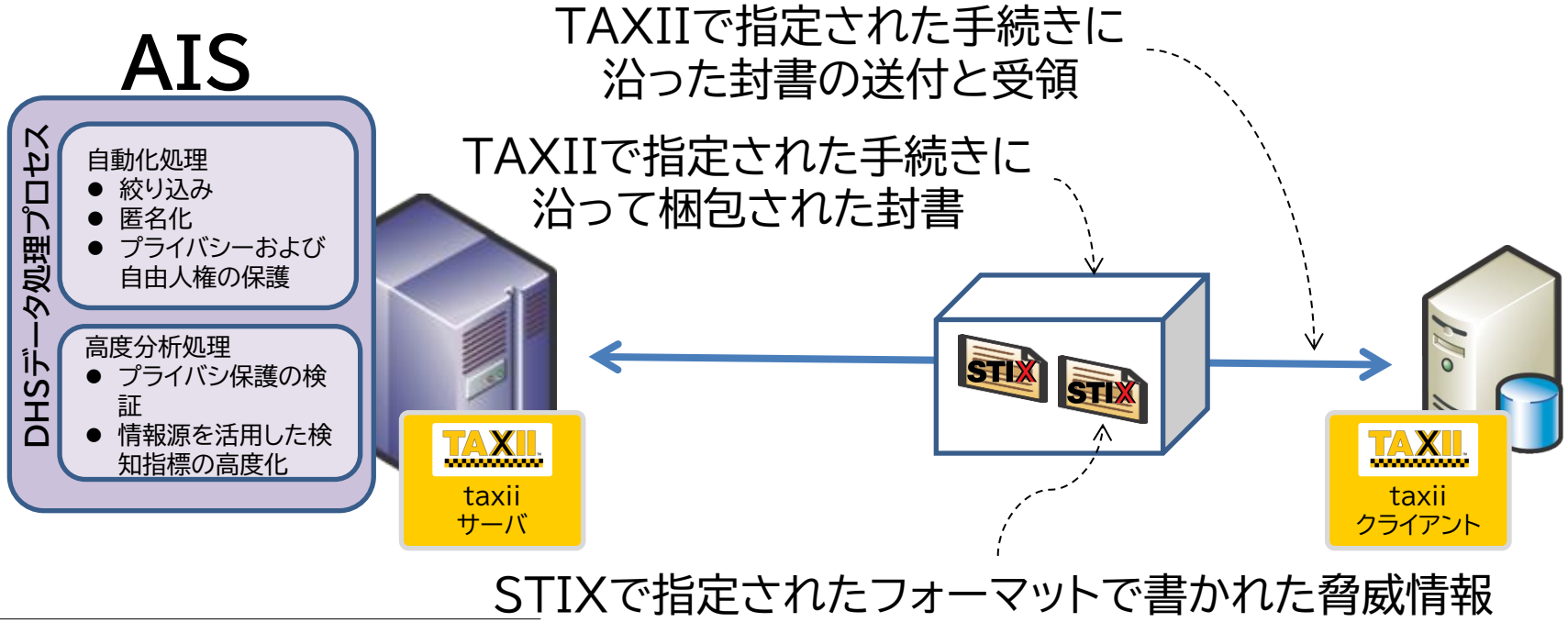
攻撃のモデル化と対処
TAXII(検知指標情報自動交換手順)(2012年)

- DHSが主導し、MITREが中心となり仕様策定を進めてきたもので、サイバー攻撃を検知するために使用できる指標(インディケータ)を交換するためのサービス、プロトコルならびにフォーマットの仕様である。
- STIXで書かれた脅威情報をTAXIIという手順を使って交換する。



攻撃のモデル化と対処
米国AIS(Automated Indicator Sharing)

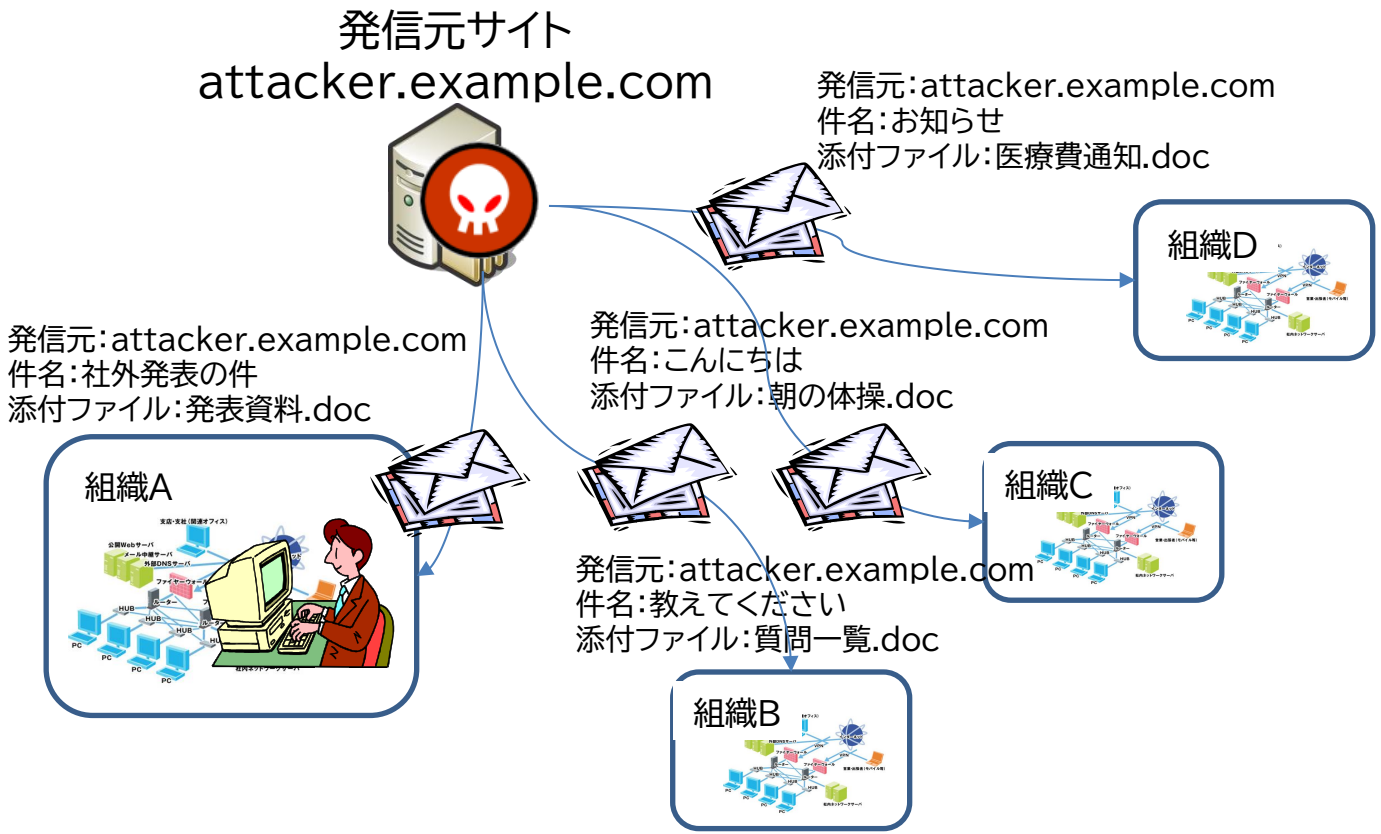
- 米国政府が提供する官民連携の情報共有基盤
- 2015年サイバーセキュリティ法により、2016年3月からDHSの下で活動を開始した。攻撃指令サーバのドメインやIPアドレス、マルウェアのハッシュ値などの検知指標(インディケータ)を共有する情報基盤である。



[出典] Automated Indicator Sharing (AIS)
https://www.cisa.gov/ais

攻撃のモデル化と対処
検知指標(インディケータ)

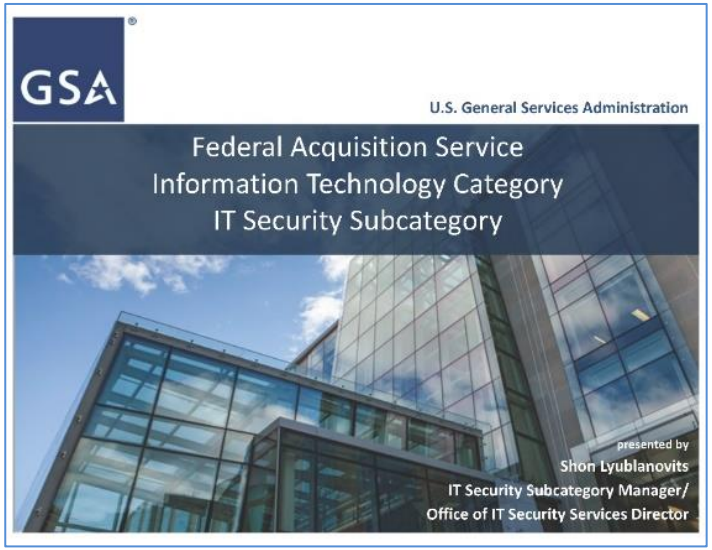
- 検知に有効なサイバー攻撃を特徴づける指標

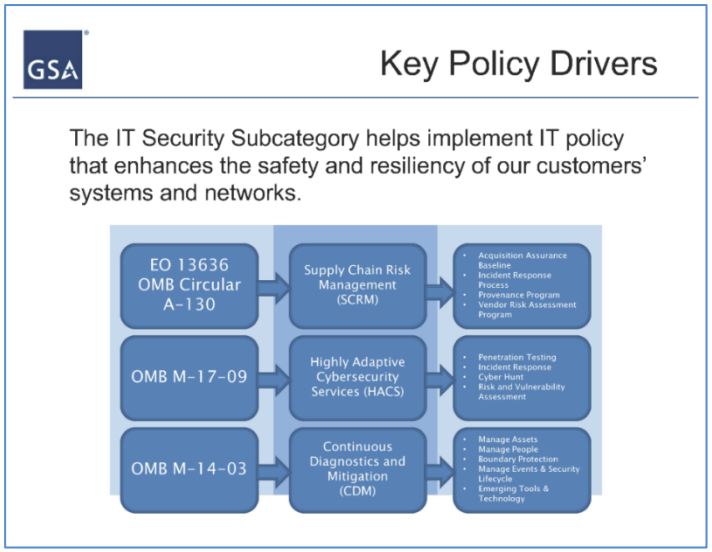


発信元:attacker.example.com
攻撃活動の共通項はインディケータとして使いやすい。

米国政府の脆弱性対策の取組み
公共サービスの調達

- 2013年2月、重要インフラのサイバーセキュリティ向上に関する大統領令13636
- 2013年11月、GSA（連邦調達庁）では、調達におけるサイバーセキュリティとレジリエンスの向上（Improving Cybersecurity and Resilience through Acquisition）報告書を作成。この報告書を具体化する活動の中で、SCRM、HACS、CDMに言及した。





［出典］ https://csrc.nist.gov/CSRC/media/Presentations/Infusing-Cybersecurity-into-the-Government-Acquisi/images-media/GSA%20Federal%20Acquisition%20IT%20Secuity%20Subcategory.pdf

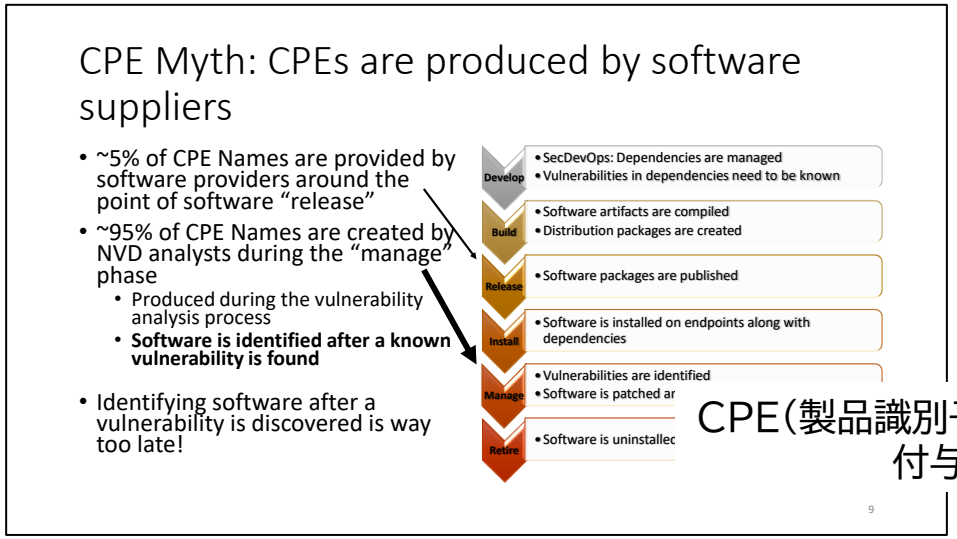
米国政府の脆弱性対策の取組み
公共サービスの調達

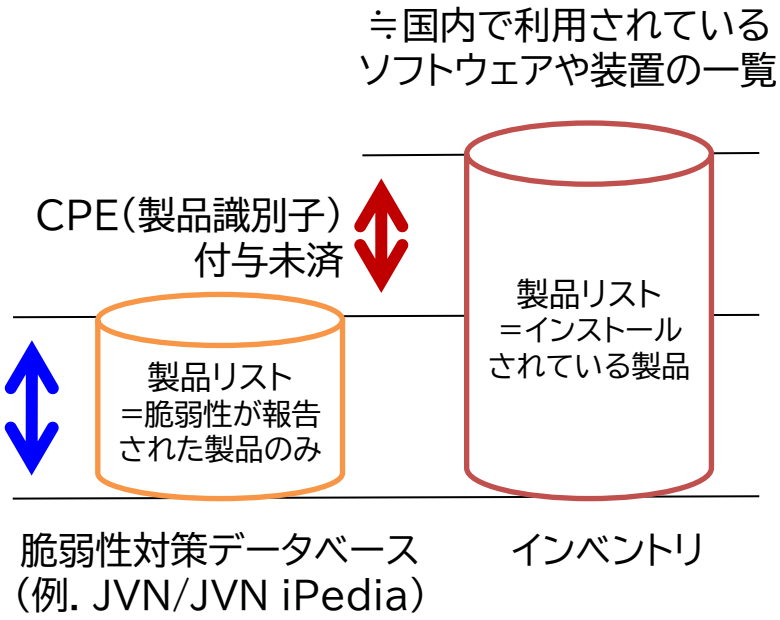
大統領令13636 OMB(行政管理予算局) Circular A-130	SCRM(サプライチェーンリスク管理) Supply Chain Risk Management	Acquisition Assurance Baseline Incident Response Process Provenance Program Vendor Risk Assessment Program (調達保証ベースライン、インシデント対応プロセス、出所プログラム、ベンダリスク評価プログラム)
OMB(行政管理予算局) M-17-09	HACS(高度適応サイバーセキュリティサービス) Highly Adaptive Cybersecurity Services	Penetration Testing Incident Response Cyber Hunt Risk and Vulnerability Assessment (侵入テスト、インシデント対応、サイバーハント、リスクと脆弱性の評価)
OMB(行政管理予算局) M-14-03	CDM(継続的な診断と脅威の緩和) Continuous Diagnostics and Mitigation 継続的に脆弱性診断を行い、その対策を常に継続し続けること	Manage Assets Manage People Boundary Protection Manage Events & Security Lifecycle Emerging Tools & Technology (資産の管理、人の管理、境界保護、イベントとセキュリティライフサイクルの管理、新たなツールと技術)

[出典] https://csrc.nist.gov/CSRC/media/Presentations/Infusing-Cybersecurity-into-the-Government-Acquisi/images-media/GSA%20Federal%20Acquisition%20IT%20Secuity%20Subcategory.pdf

米国政府の脆弱性対策の取組み
製品識別子に関する課題

- CPE(共通プラットフォーム一覧)付与の95%は、脆弱性が発見されてから、、、この課題を解決するため、NVDは製品識別子としてSWIDの採用推進
  - CPE:NVD主体で製品識別子を付与
  - SWID:製品ベンダ主体で製品識別子を付与(インストール時同梱)





[出典] SCAPv2 April Developer Days Face to Face
https://csrc.nist.gov/Projects/security-content-automation-protocol-v2/Material-Archives

米国政府の脆弱性対策の取組み
IT資産管理 ISO/IEC 19770

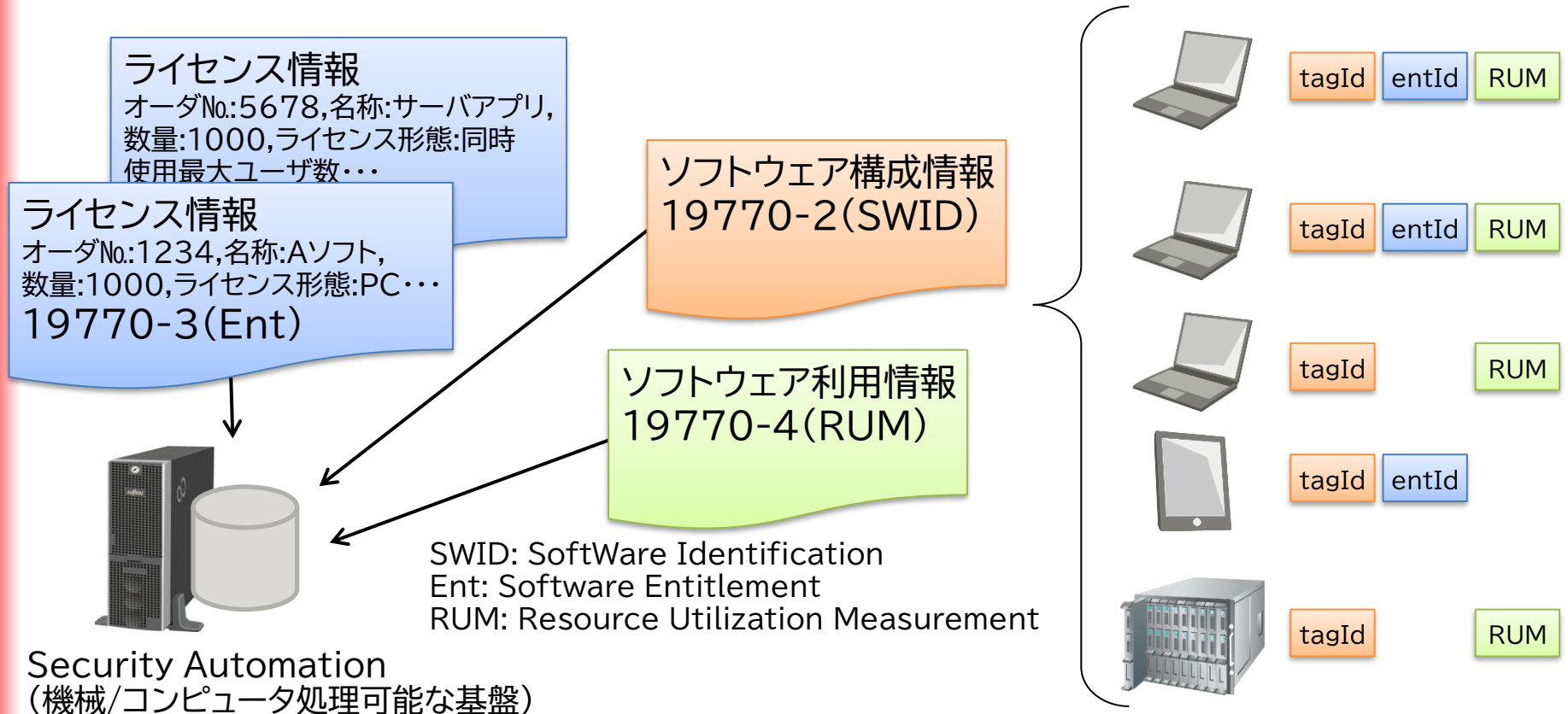
規格名	概要	状況
ISO/IEC 19770-1:2017 Requirements 要求事項	IT資産管理(ITAM)のためのマネジメントシステムの確立, 実施, 維持及び改善の要求事項について規定している。	JIS X 0164-1:2019
ISO/IEC 19770-2:2009 Software identification tag SWID(ソフトウェア識別子)	ソフトウェアの導入状況を把握するために、導入されたソフトウェアを識別するためのタグの規格である。	JIS X 0164-2:2018 (ISO/IEC 19770-2:2015)
ISO/IEC 19770-2:2015 Software identification tag SWID(ソフトウェア識別子)	ISO/IEC 19770-2:2009のタグ必須の多くが任意となった。また、パッチ対応属性(delta)、ハッシュ値属性(sha1, sha256など) がサポートされるようになった。	
RFC 9393 (2023年6月28日) Concise Software Identification Tags (CoSWID)	ISO/IEC 19770-2:2015の記述軽量版で制約を備えたデバイスを想定した仕様である。	2016年3月から 検討開始
ISO/IEC 19770-3:2016 Entitlement schema 権利スキーマ	導入されているソフトウェアのライセンス情報を記述するためのタグの規格である。	JISX 0164-3:2019
ISO/IEC 19770-4:2017 Resource Utilization Measurement 資源利用測定	IT資産の使用に伴うリソースの消費に関する規格である。	JISX 0164-4:2019
ISO/IEC 19770-5:2015 Overview and vocabulary 概要及び用語	IT資産管理のコンセプトや原理を概説し、ISO/IEC 19770シリーズで用いられる用語の定義や、各規格の関連について説明した規格である。	JISX 0164-5:2019
NISTIR 8060 Guidelines for the Creation of Interoperable Software Identification (SWID) Tags	ISO/IEC 19770-2「ソフトウェア識別タグ」の生成に関するガイドライン	2016年4月発行
NISTIR 8085 Forming Common Platform Enumeration (CPE) Names from Software Identification (SWID) Tags.	ISO/IEC 19770-2「ソフトウェア識別タグ」からX.1528「製品識別子」の生成に関する指針	2015年12月 ドラフト発行

米国政府の脆弱性対策の取組み
IT資産管理 ISO/IEC 19770

規格名	概要	状況
ISO/IEC 19770-6:2024 Hardware identification tag	HWIDタグとしてのハードウェア識別(HWID)データのカプセル化の規格である。	
ISO/IEC 19770-8:2020 Guidelines for mapping of industry practices to/from the ISO/IEC 19770 family of standards	業界の慣行をISO/IEC 19770シリーズにマッピングする方法を定義するマッピングドキュメントを作成するときに使用する要件、ガイドライン、形式、およびアプローチを定義する。	
ISO/IEC DTS 19770-10 Guidance for implementing ITAM	ITAMシステムを実装し、現在の市場の需要(調査とその後の検証活動によって決定)を満たすためのガイダンスを提供する。	
ISO/IEC 19770-11:2021 Requirements for bodies providing audit and certification of IT asset management systems	ISO/IEC 19770-1に従ってITAMSの監査および認証を提供する認証機関の要件を指定し、ガイダンスを提供する。	

米国政府の脆弱性対策の取組み
資産管理と脆弱性対策の融合

- 各種情報を集約し、自動チェックするなどの基盤整備に利用可能
- ソフトウェア構成情報(SWID)は19770-2、ライセンス情報(Ent)は19770-3、リソース利用情報(RUM)は19770-4で標準化される。



米国政府の脆弱性対策の取組み
SBOM(ソフトウェア部品表)

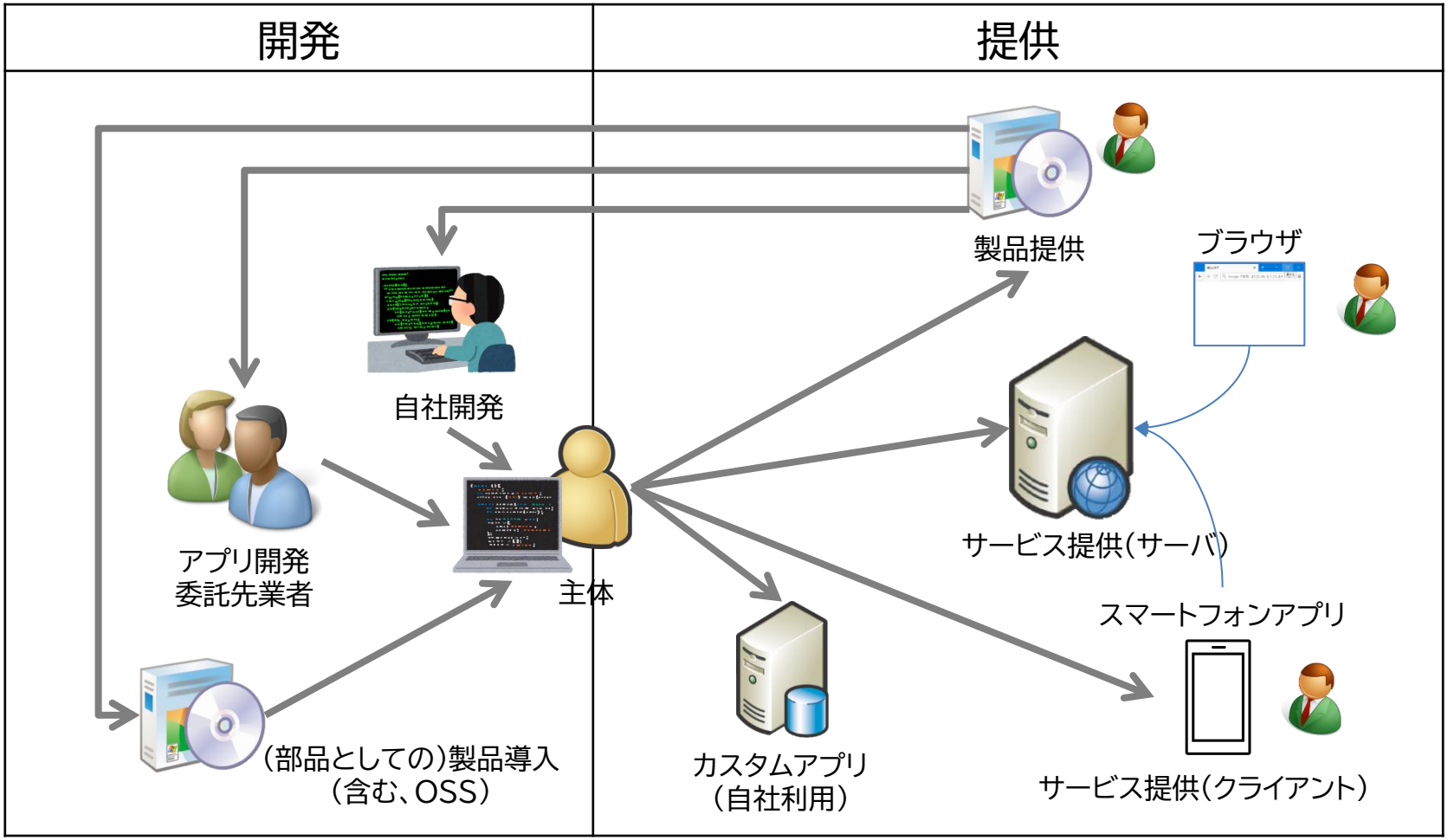
- SBOM(ソフトウェア部品表、Software Bill of Materials)
  - NTIA(米国商務省電気通信情報局、National Telecommunications and Information Administration)が主体となって推進し、2018年7月に、初回打合せが開催された。
  - ソフトウェアを構成するコンポーネントの透明性(Software Component Transparency)をあげることを目的とする。
  - よく使用されている例: 食品の成分表のようなもの

- BOM(Bill of Materials)
  製造業では、製品を製造する際に必要な部品や原材料などの構成情報を部品管理している。部品構成管理はBOM管理と呼ばれたり、プロセス製造業ではレシピ管理と呼ばれたりしている。

[出典] NTIA Software Component Transparency
https://www.ntia.doc.gov/SoftwareTransparency

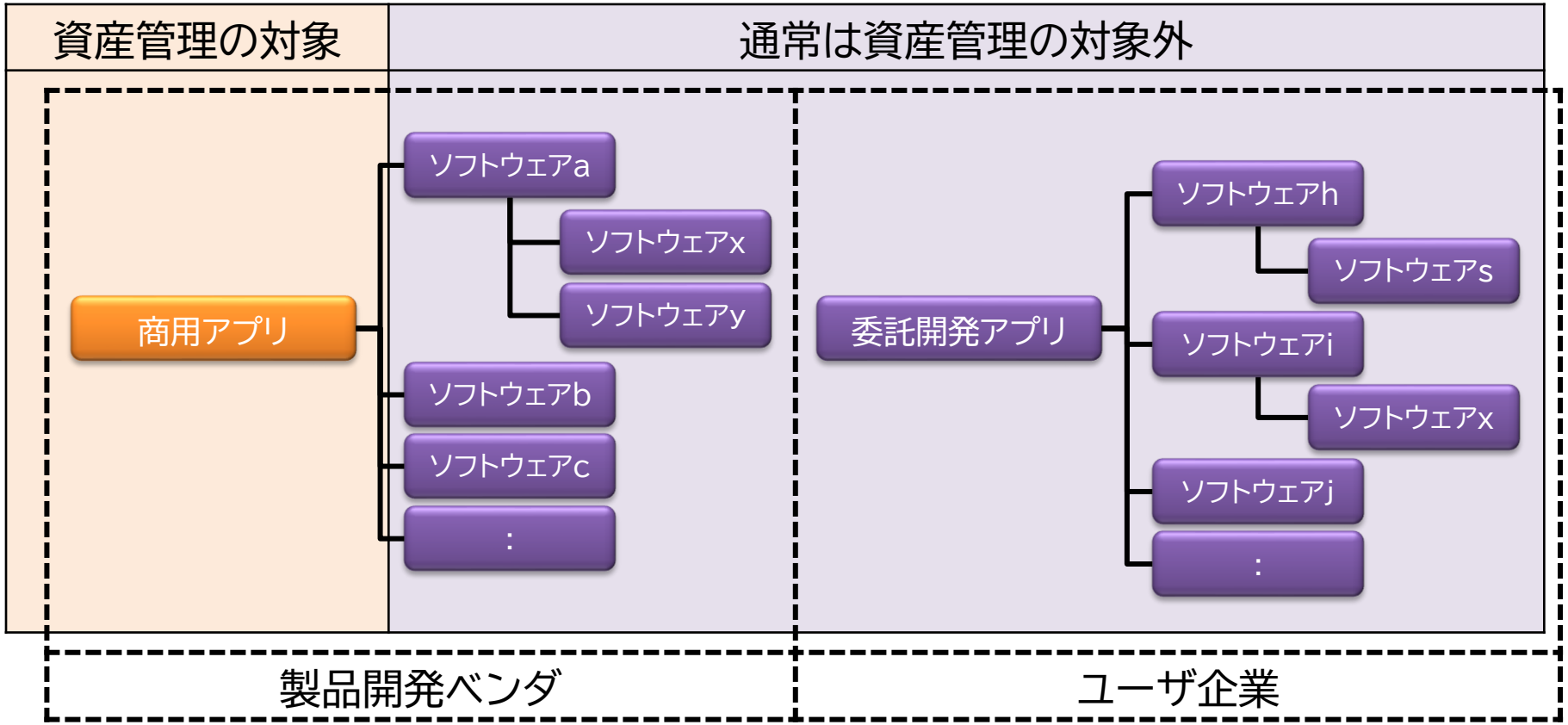
米国政府の脆弱性対策の取組み
SBOM(ソフトウェア部品表)

- ソフトウェア開発ならびに提供形態の多様化



米国政府の脆弱性対策の取組み
SBOM(ソフトウェア部品表)

- ソフトウェアの依存関係とIT資産管理



米国政府の脆弱性対策の取組み
SBOM(ソフトウェア部品表)

- 2021年7月12日、NTIA(米国商務省電気通信情報局)より公開
  SBOM「最小要素」には、コンポーネントを一覧化した部品表に含まれる情報だけなく、SBOMの利活用者が実施すべき事項も規定されている。

区分	概要	具体的な定義
データフィールド	各コンポーネントに関する基本情報を明確化すること	次の情報をSBOMに含めること。 ● サプライヤー名 ● コンポーネント名 ● コンポーネントのバージョン ● その他の一意な識別子 ● 依存関係 ● SBOMの作成者 ● タイムスタンプ
自動化サポート	SBOMの自動生成や可読性などの自動化をサポートすること	SBOMデータは機械判読可能かつ相互運用可能なフォーマットを用いて作成され、共有されること。現状では、国際的な議論を通じて策定された、SPDX、CycloneDX、SWIDタグを用いること。
プラクティスとプロセス	SBOMの要求、生成、利用に関する運用方法を定義すること	SBOMを利活用する組織は、次の項目に関する運用方法を定めること。 ● SBOMの作成頻度 ● SBOMの深さ ● 既知である未知なこと ● SBOMの共有 ● アクセス管理 ● 誤りの許容

[出典] The Minimum Elements For a Software Bill of Materials (SBOM)
https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

米国政府の脆弱性対策の取組み
SBOM(ソフトウェア部品表)

- セキュリティ・トランスペアレンシー・コンソーシアムの活動報告によると

<table>
<tr><th>品質上の課題</th><th>内容</th></tr>
<tr><td>最小要素不足</td><td>SBOMの実データを調査したところ、米国NTIAが定めるSBOMの最小要素のうち、作成者や作成時刻の記載は非常に少ない状況である。
＊NTTによる約1,800件の調査
<table>
<tr><th>要素</th><th>記載割合</th></tr>
<tr><td>SBOMの作成ツールやコンポーネントに関する名称や識別子</td><td>9割程度</td></tr>
<tr><td>ベンダやバージョン</td><td>6割程度</td></tr>
<tr><td>SBOMの作成者</td><td>3割程度</td></tr>
<tr><td>SBOMの作成時刻</td><td>1割程度</td></tr>
</table></td></tr>
<tr><td>要素の表現が
不適切・表記揺れ</td><td>SBOMの要素にはソフトウェアの開発元を示すベンダ項目があるが、開発元が示されない場合がある。また略称等を用いる場合もあり、正式名称とのマッチングがとれない。</td></tr>
<tr><td>コンポーネントの
網羅性</td><td>ソースコードのコピーペーストや一部を改変した再利用によって発生するパッケージ情報には記されないソフトウェアの依存関係があり、脆弱性に気づけない。</td></tr>
</table>

［出典］　サプライチェーンのサイバーレジリエンス　― セキュリティ透明性の向上と活用―
https://www.st-consortium.org/?download=1297&tmstv=1734422883

米国政府の脆弱性対策の取組み
2025～2026年度 CISA 国際戦略計画

- CISA 戦略計画 2023～2025に整合したもので、NSM-22「重要インフラのセキュリティとレジリエンスに関する国家安全保障覚書」に沿った計画
  - 国際パートナーと積極的に連携して、重要インフラのセキュリティとレジリエンスを強化することに重点を置いている。
  - 3つの短期・中期目標(objective)を設定し、達成するための「Enabling Measure(実現策)」と、その「Measure of Effectiveness(効果測定)」を提示している。

目標1　米国が依存する外国インフラのレジリエンスの強化

目標2　統合サイバー防御の強化

① パートナーと協力してサイバー防御を実現し、集団的リスクを軽減する。
② サイバーの安全性を高めるために、標準とセキュリティを大規模に推進する。
③ 主要パートナーのサイバーおよび物理的なレジリエンス能力を強化する。

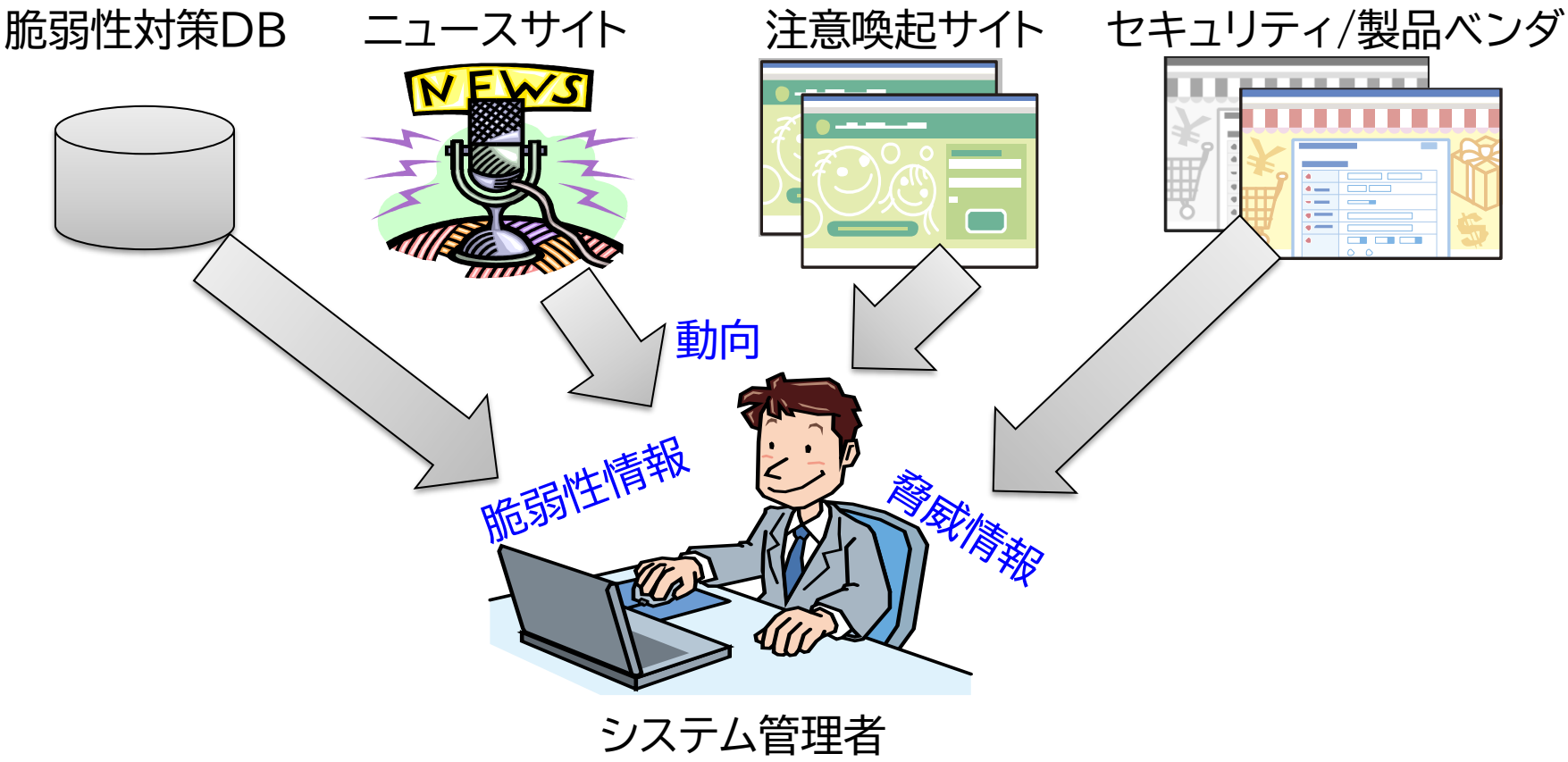
目標3　国際活動に関する機関の調整の統一

［出典］　サプライチェーンのサイバーレジリエンス　― セキュリティ透明性の向上と活用―
https://www.st-consortium.org/?download=1297&tmstv=1734422883

JVN脆弱性対策機械処理基盤

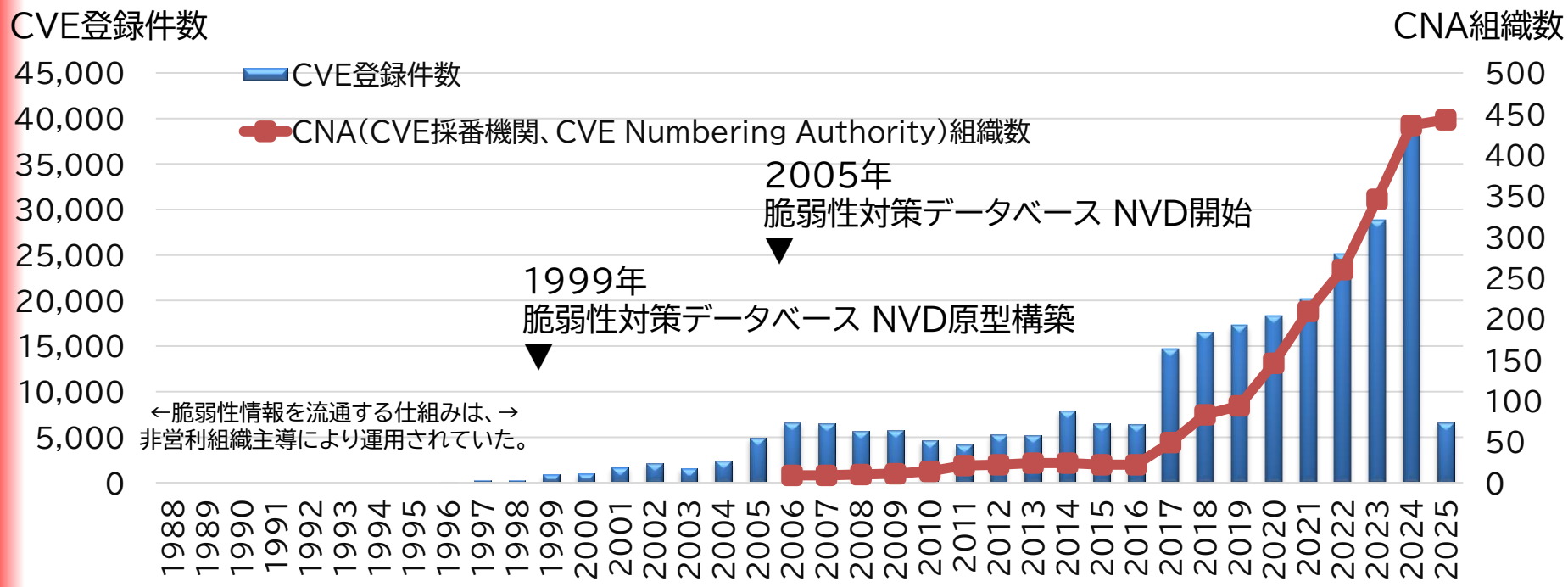
脆弱性関連情報の収集
防御としての（情報活用＋対策）

- 脆弱性対策の判断要素となる情報を収集し、自組織の対策に役立てる。



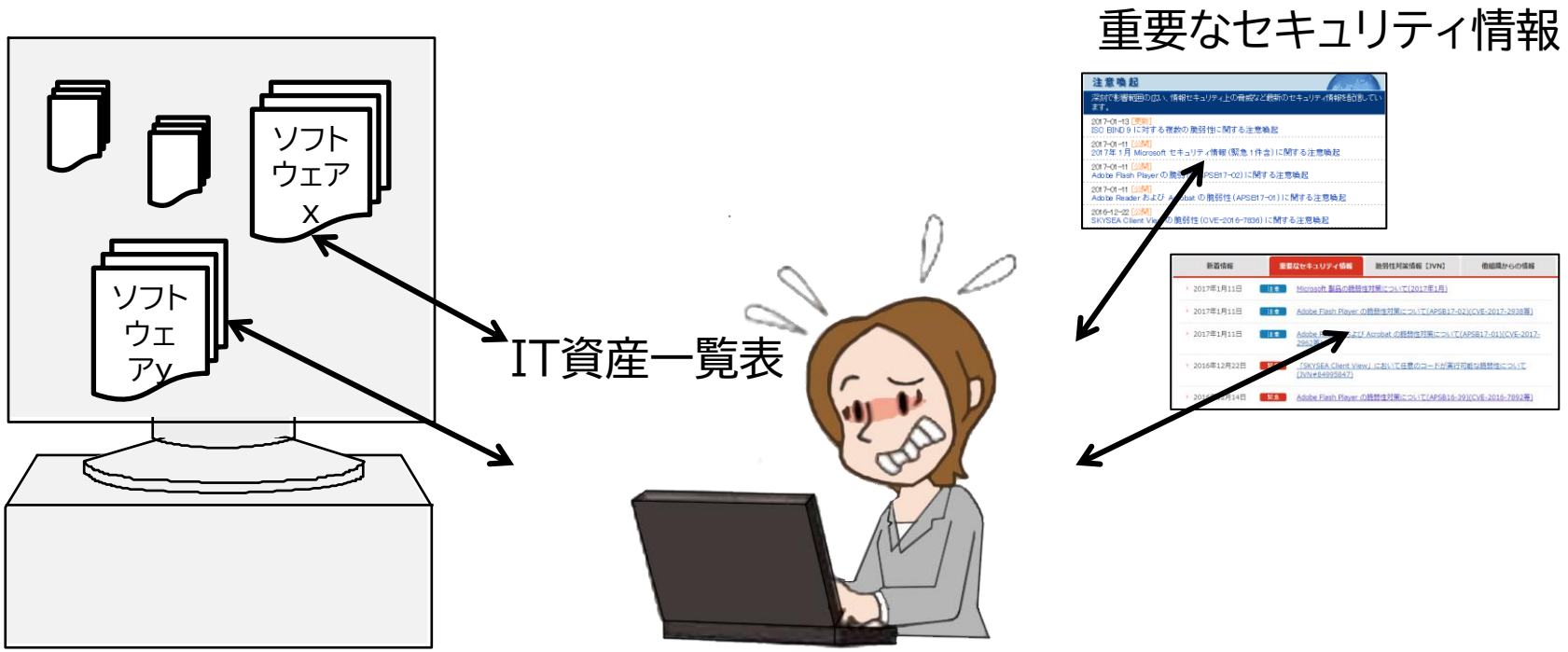
脆弱性関連情報の収集
【 課題 】脆弱性情報の件数は増加傾向

- NVD(米国脆弱性対策データベース、National Vulnerability Database)に登録されている件数は?
  - 脆弱性を分担協力して登録する組織(脆弱性登録組織)の増加と共に増加している。



脆弱性関連情報の収集
【 課題 】インストール状況と脆弱性との紐付けは人手で実施

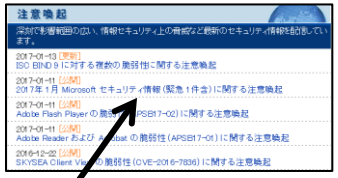
- 重要なセキュリティ情報が発信されるたびに、手作業でIT資産一覧表を検索して、影響範囲の調査をしていませんか？
  - 多くの場合、インストール状況と脆弱性との紐付けを人手で実施している（資産管理と脆弱性対策とが連携できているわけではない）。



脆弱性関連情報の収集
【 課題 】カスタムアプリ管理は整備途上

- 重要なセキュリティ情報が発信されたときに、カスタムアプリ(SIで開発したアプリケーションなど)の影響範囲を調査していますか？
  - 多くの場合、カスタムアプリ(SIで開発したアプリケーションなど)は、資産管理や脆弱性管理の対象に含まれていない。

重要なセキュリティ情報



カスタムアプリ
Ex. 在庫管理アプリ

？

脆弱性関連情報の収集
脆弱性対策作業のルーチンワーク化(コンピュータ処理)

【 課題 】
- 脆弱性情報の件数は増加傾向
- インストール状況と脆弱性との紐付けは人手で実施
- カスタムアプリ管理は整備途上

セキュリティに関する作業を手作業で行なうと、設定ミスや設定者のセキュリティ知識の程度や判断の相違などによりセキュリティ要件を損なう可能性大

⇩
- 識別子の共通化
  - プログラムの脆弱性を一意に識別する。
  - 情報システムを構成するハードウェア、ソフトウェアなどの製品を一意に識別する。
  - 脆弱性の種別を識別する。
- 評価指標の共通化
  - 脆弱性の深刻度を評価する。

【 解決策 】
- ルーチンワーク化(コンピュータ処理)による対処

「ルーチンワーク化」の部分は、一般的にMachine Readableと言われている。直訳すると、機械可読であるが、手順化してコンピュータに処理させることを意味する。

脆弱性関連情報の収集
脆弱性対策データベースに記載されていること

- 脆弱性対策データベースに記載されていることは、、、
  - 概要
  - 影響を受けるシステム
  - 詳細情報
  - 想定される影響
  - 対策方法
  - ベンダ情報
  - 参考情報

- 概要、詳細情報、想定される影響に記載される内容は、セキュリティ専門用語が多く、内容を把握することも、なかなか難しい状況にある。
- さらに、情報システムだけではなく、医療機器、制御系システムなど対象分野が広がりつつあることもあり、分野毎の専門用語も増え始めている。

脆弱性対策データベース
識別子の共通化

- 脆弱性対策作業のルーチンワーク化(機械化/手順化)
  - 識別子の共通化
    - プログラムの脆弱性を一意に識別する。
      - CVE(共通脆弱性識別子)

[形式] CVE-西暦-連番
[例] CVE-2017-0145 (WannaCry(2017年)が悪用した脆弱性)

    - 情報システムを構成するハードウェア、ソフトウェアなどの製品を一意に識別する。
      - CPE(共通プラットフォーム一覧)

[形式] cpe:/{種別}:{ベンダ名}:{製品名}
[例] cpe:/o:microsoft:windows_7
マイクロソフト ウィンドウズ 7と言っても表記方法は様々
Microsoft Windows 7、マイクロソフト Windows 7など

脆弱性対策データベース
評価指標の共通化

- 脆弱性対策作業のルーチンワーク化(機械化/手順化)
  - 識別子の共通化
    - 脆弱性の種別を識別する。
      - CWE(共通脆弱性タイプ一覧)
        [形式] CWE-番号
        [例] CWE-78 (OSコマンドインジェクション)

  - 評価指標の共通化
    - 脆弱性の深刻度を評価する。
      - CVSS(共通脆弱性評価システム)
        脆弱性の深刻度を表す評価
        ＝技術的な特性 ＊ 脅威の大きさ ＊ 情報資産の価値

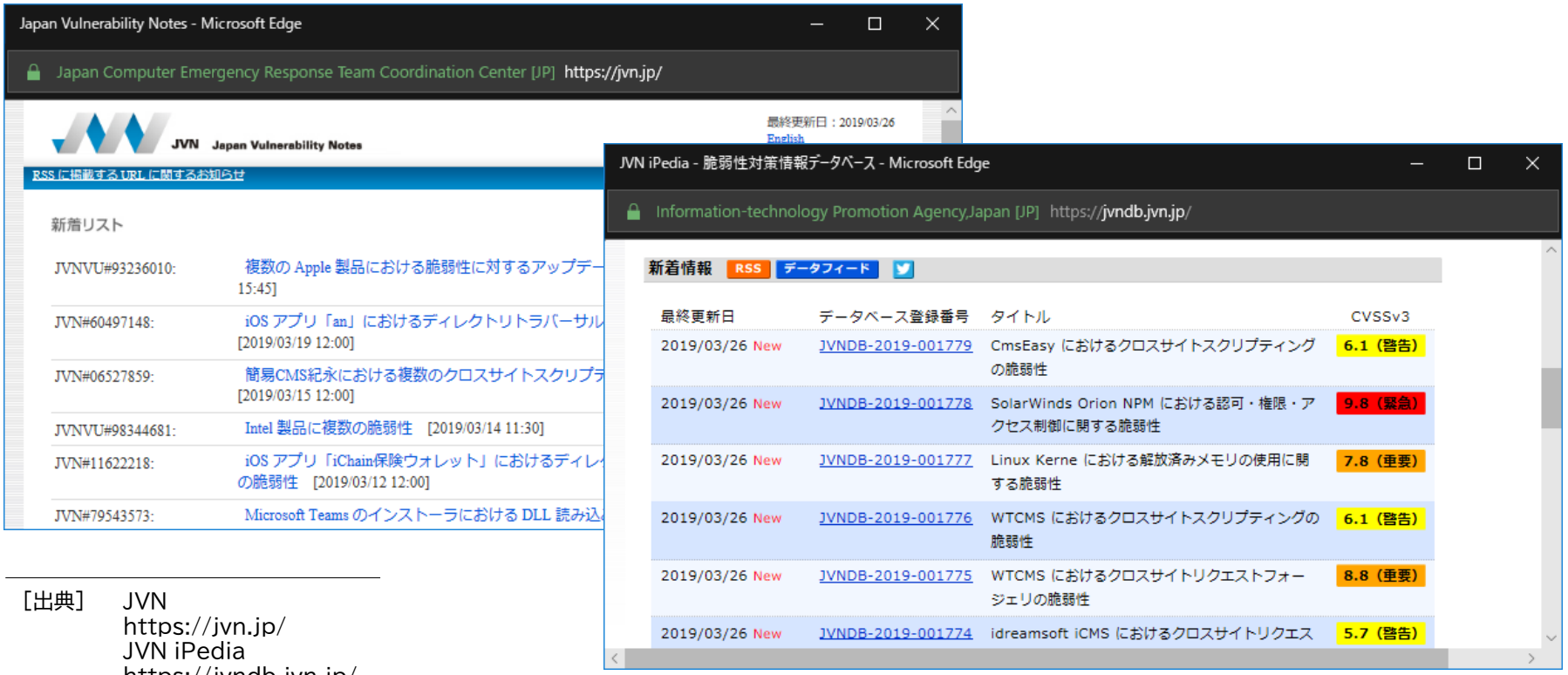
何が起きるのか？

既に攻撃は発生している？
対策は出ている？

システムの重要度は？

JVN脆弱性対策機械処理基盤
JVN

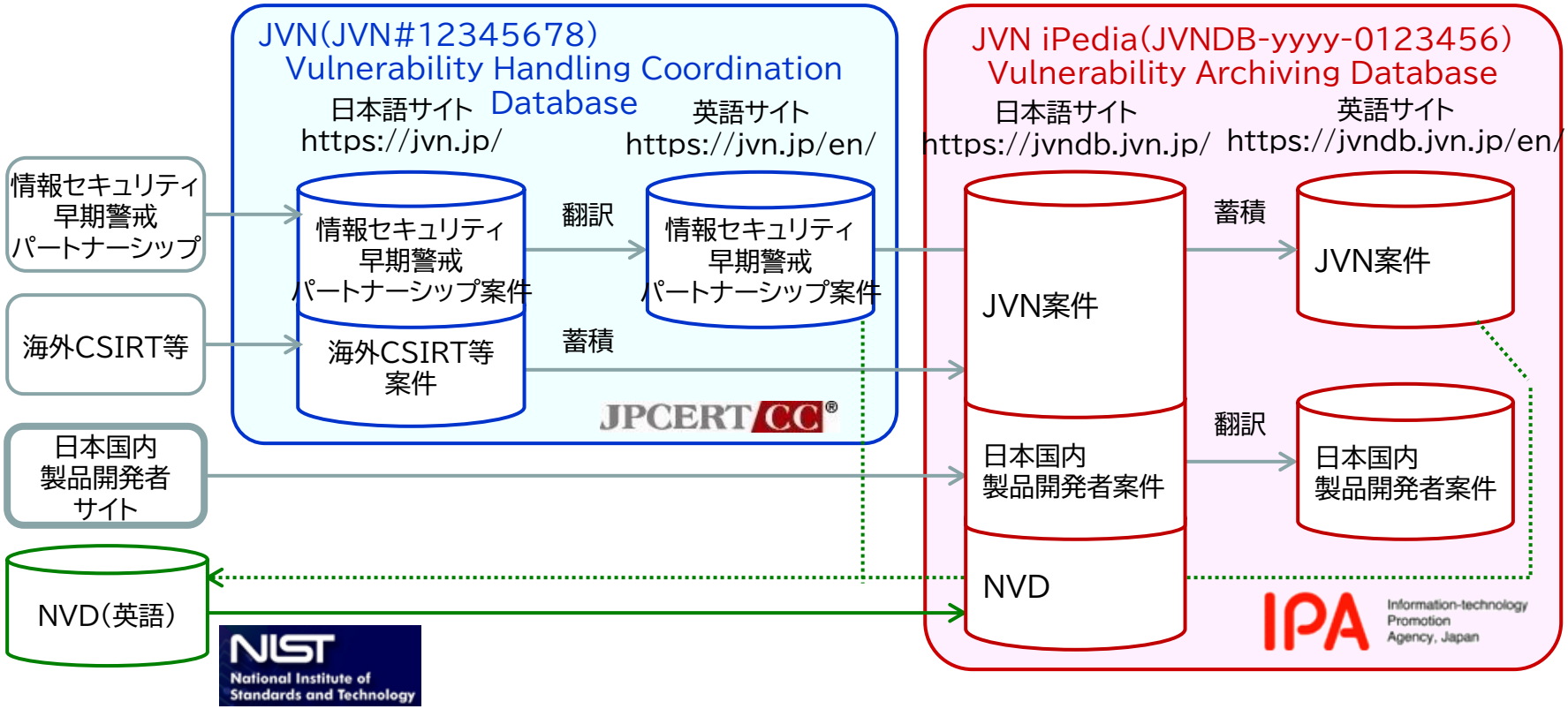
- JVN は、“Japan Vulnerability Notes” の略
- 日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供し、情報セキュリティ対策に資することを目的とする脆弱性対策情報サイト



［出典］ JVN
https://jvn.jp/
JVN iPedia
https://jvndb.jvn.jp/

JVN脆弱性対策機械処理基盤
JVNは2つのDBから構成されている

- 脆弱性対策情報ポータルサイトJVN(製品開発者と調整した脆弱性対策情報をタイムリーに公開)と、脆弱性対策情報データベースJVN iPedia(国内で利用されている製品を対象にした脆弱性対策情報を広く蓄積)から構成



JVN脆弱性対策機械処理基盤
対策実施サービスに繋げるための仕組み

- 効率的な脆弱性対策を目指すことのできるグローバルな利活用基盤
  ＝(国際性:JVN＋地域性:JVN iPedia)× 利活用基盤(MyJVN)

MyJVN

バージョンチェッカ

セキュリティ設定チェッカ

脆弱性対策情報収集ツール

JVN Japan Vulnerability Notes

情報セキュリティ早期警戒パートナーシップに報告された脆弱性対策情報

JVN iPedia

国内外で報告された脆弱性に対する国内製品開発者の脆弱性対策情報

共通脆弱性識別子CVEが付与されている脆弱性対策情報

国内外で報告された全ての脆弱性対策情報

MyJVN
JVNとJVN iPediaに登録されている脆弱性対策情報を対策実施に直結したサービスに繋げる仕組みを提供する

JVN iPedia
国内で利用されている製品を対象にした脆弱性対策情報を広く蓄積する

JVN
製品開発者と調整した脆弱性対策情報をタイムリーに公開する

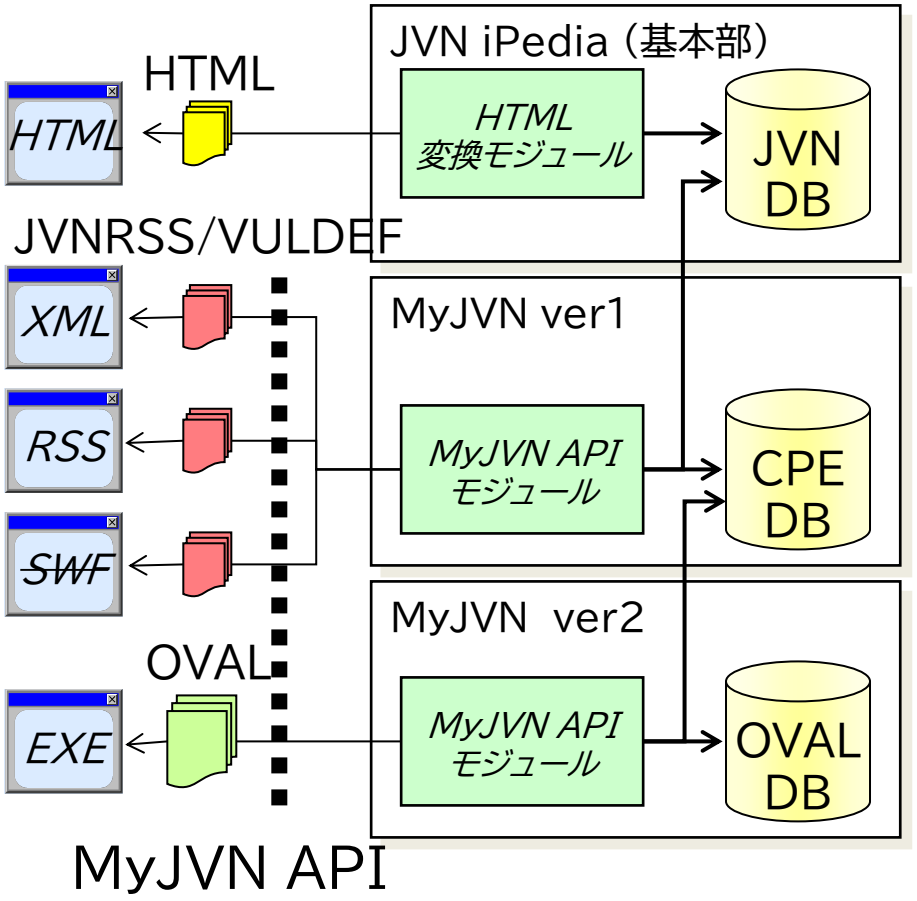
MyJVN API
http://jvndb.jvn.jp/apis/

- JVN iPediaを活用し、新たなサービスを準備できる環境を整備する。

JVN iPediaの情報を
Webを通じて利用するための
ソフトウェアインタフェース
⇒ユーザ側でのツール開発も可能

フィルタリング型情報提供
⇒ MyJVN脆弱性対策
情報収集ツール
フィルタリング収集ツール（mjcheck4）
~~脆弱性対策情報ダッシュボード（mjdashboard）~~

検査データ提供
⇒ MyJVNバージョンチェッカ
バージョンチェック（.NET Framework版）

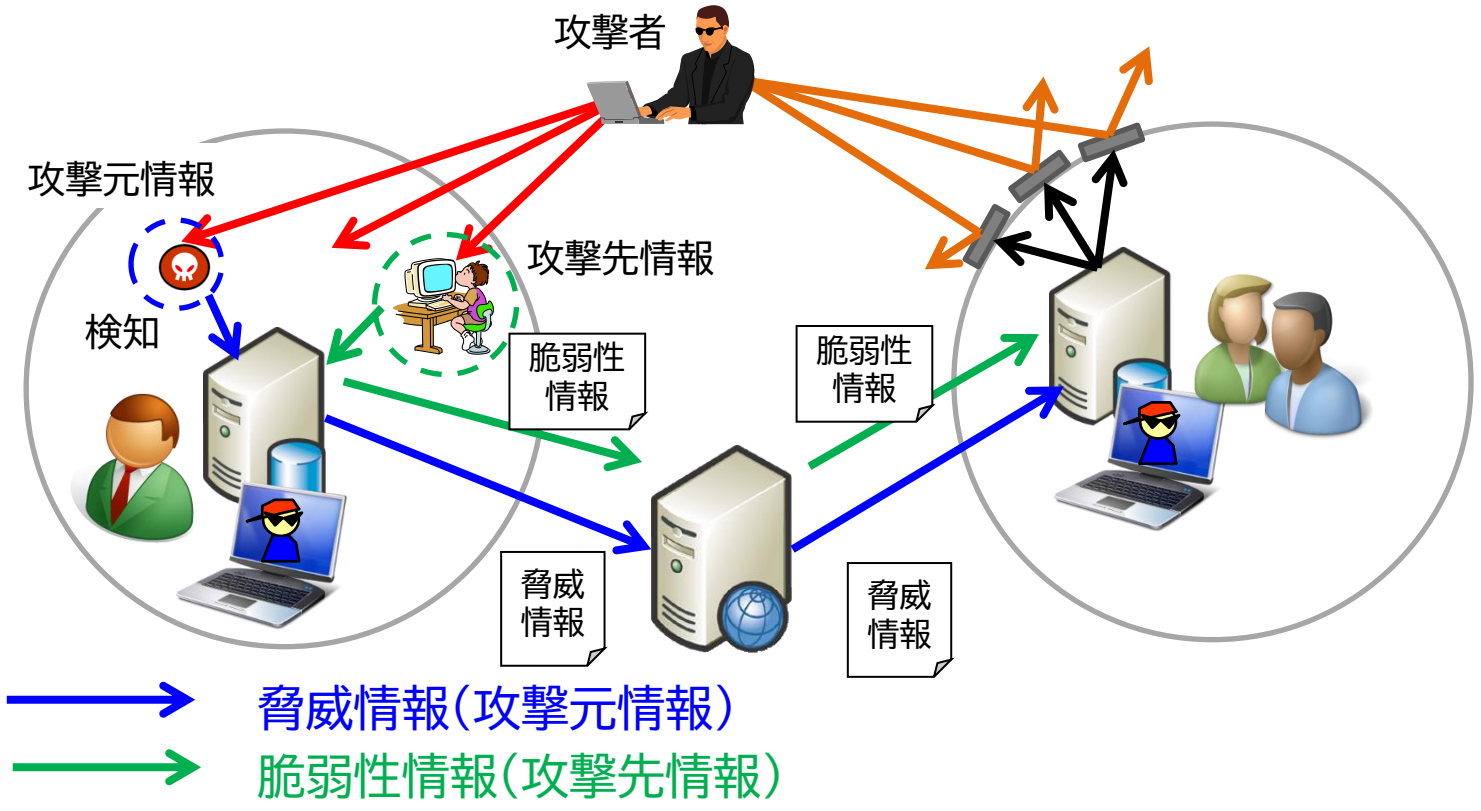


機械処理可能な情報活用基盤の整備
望ましい環境に向けて

- 製品やカスタムアプリ(SIで開発した業務アプリケーションなど)に関わらず、情報連携により、人が介在しなくても良い脆弱性対策環境(脆弱性の影響有無の判定など)が実現できる。

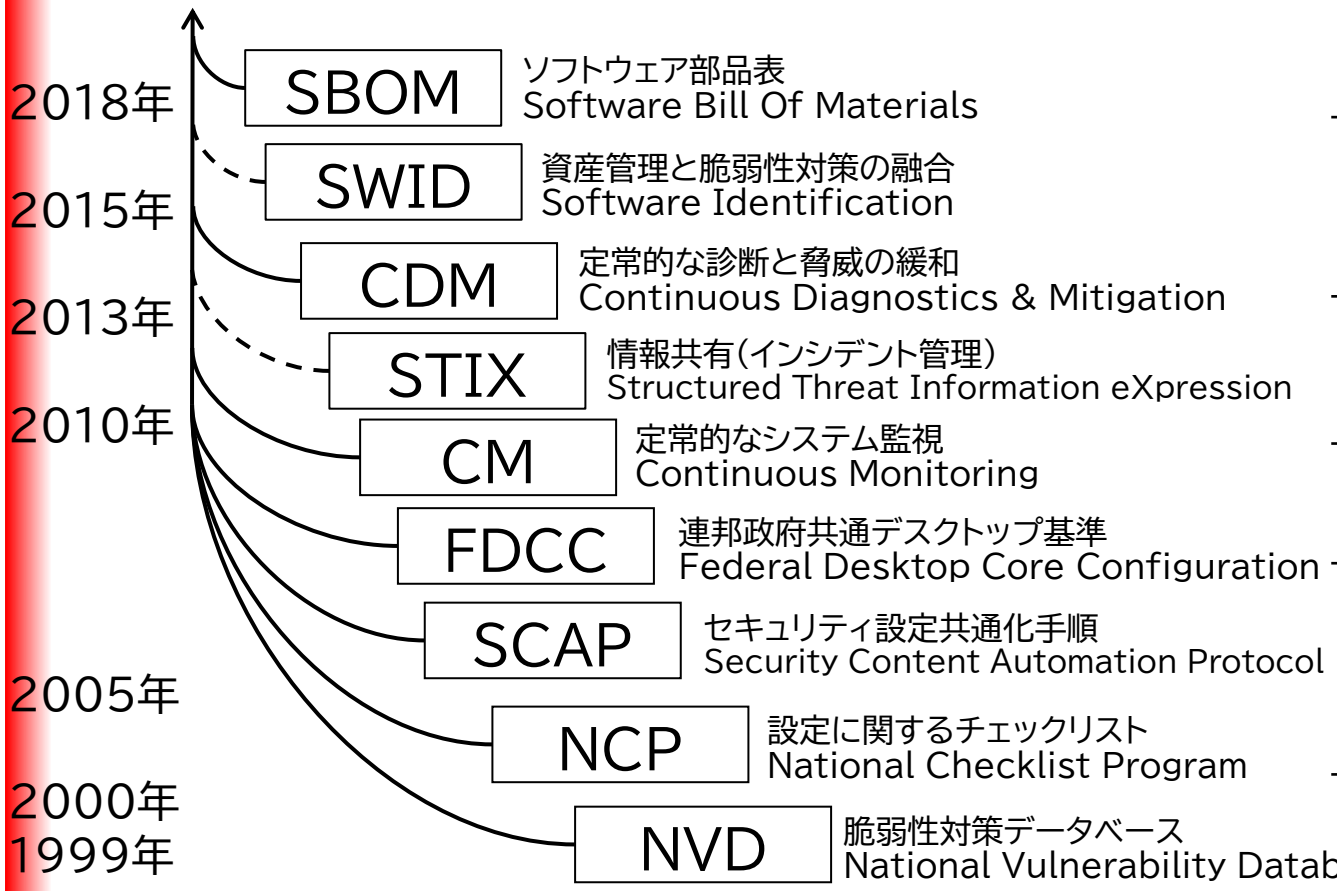
機械処理可能な情報活用基盤の整備
望ましい環境に向けて

- ①脅威などの攻撃元情報だけではなく、脆弱性などの攻撃先情報を活用すると共に、②これら情報を資産情報やソフトウェア部品表(SBOM)と紐付けて活用できる。



機械処理可能な情報活用基盤の整備
望ましい環境に向けて

- グローバルな利活用基盤整備にあたってはNVDとの連携を考慮



第5期 利活用基盤普及Ⅱ
2019年～
MyJVN脆弱性と資産管理連携への対応
総務省実証実験(脆弱性/資産管理連携)

第4期 利活用基盤普及Ⅰ
2013年～2018年
総務省実証実験(脅威情報)(2016)
ソフトウェア識別(SWID)タグ活用導(2013)
脆弱性と資産管理連携検討開始(2013)

第3期 利活用基盤導入
2008年～2012年
MyJVN開始(2008)
CPE導入(2008)

第2期 対策情報充実
2007年～2008年
CVE、CVSS、CWE導入(2007～2008)

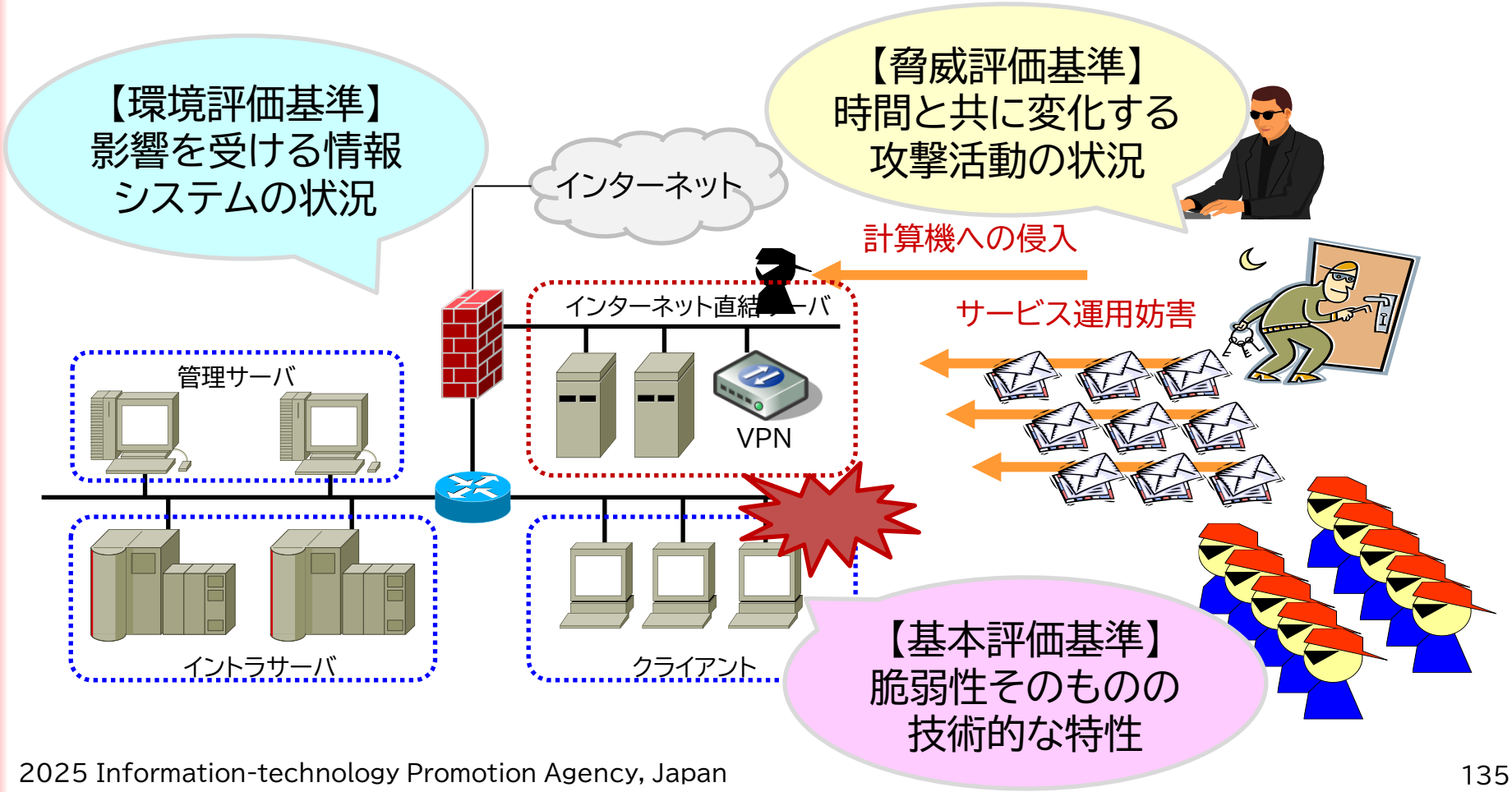
第1期 立上げ
2002年～2007年
JVNiPedia開始(2007)
JVN開始(2004)
試行サイト開始(2002)

トピック[2]

KEV、EPSS、SSVC

CVSS(共通脆弱性評価システム)
Common Vulnerability Scoring System

- 攻撃状況やシステムの重要度を加味して脆弱性の深刻度を表す



CVSS(共通脆弱性評価システム)
Common Vulnerability Scoring System

- 各項目を評価するための情報提供者は？

項目		関係性
基本評価基準	脆弱性そのものの 技術的な特性	NVD JVN/JVN iPedia MyJVN 製品ベンダ セキュリティベンダ
現状評価基準	時間と共に変化する攻撃 活動の状況	セキュリティベンダ
環境評価基準	影響を受ける情報 システムの状況	利用者

CVSS(共通脆弱性評価システム)
Common Vulnerability Scoring System

- 各項目を評価するための情報提供者は？

項目		関係性
基本評価基準	脆弱性そのものの 技術的な特性	NVD JVN/JVN iPedia MyJVN 製品ベンダ セキュリティベンダ
現状評価基準	時間と共に変化する攻撃 活動の状況	現状を踏まえて KEV(悪用された既知の脆弱性一覧) 将来を踏まえて EPSS(脆弱性悪用予測評価システム)
環境評価基準	影響を受ける情報 システムの状況	SSVC(役割に応じた脆弱性対応分類)

KEV、EPSS、SSVCとは

- 脆弱性対策を支援するための情報ならびに手法

用語	概要
KEV Known Exploited Vulnerabilities catalog 悪用された既知の脆弱性一覧	米国サイバーセキュリティ・インフラセキュリティ庁(CISA)が公開している悪用が観測された既知の脆弱性の一覧
EPSS Exploit Prediction Scoring System 脆弱性悪用予測評価システム	脆弱性関連情報と脆弱性悪用の試みに関連するデータを用いて、機械学習を行い、その結果から今後30日間における悪用可能性を予測
SSVC Stakeholder-Specific Vulnerability Categorization 役割に応じた脆弱性対応分類	判断分岐点が設定された決定木を辿ることで、取るべき脆弱性対応の優先度を提示

KEV(悪用された既知の脆弱性一覧)
Known Exploited Vulnerabilities catalog

CISA(米国サイバーセキュリティ・インフラセキュリティ庁)が、2021年11月3日から公開している悪用が観測された既知の脆弱性の一覧

- 用途
  - 悪用されている既知の脆弱性に対処する。
- KEV掲載の条件
  - CVE(共通脆弱性識別子)が割り当てられている。
  - 脆弱性が悪用されているという信頼できる証拠がある。
  - 脆弱性に対処する方法がある。

[出典] Known Exploited Vulnerabilities Catalog
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

KEV(悪用された既知の脆弱性一覧)
Known Exploited Vulnerabilities catalog

- 掲載情報
  - CVE番号（cveID）
  - ベンダー/プロジェクト名（vendorProject）
  - 製品名（product）
  - 脆弱性名（vulnerabilityName）
  - 追加日（dateAdded）
  - 概要（shortDescription）
  - 取るべきアクション（requiredAction）
  - 対応期日（dueDate）
  - 既知のランサム攻撃での使用（knownRansomwareCampaignUse）

KEV(悪用された既知の脆弱性一覧)
Known Exploited Vulnerabilities catalog

CISCO | ADAPTIVE SECURITY APPLIANCE (ASA) AND FIREPOWER THREAT DEFENSE (FTD)

CVE-2020-3259

Cisco ASA and FTD Information Disclosure Vulnerability

Cisco Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) contain an information disclosure vulnerability. An attacker could retrieve memory contents on an affected device, which could lead to the disclosure of confidential information due to a buffer tracking issue when the software parses invalid URLs that are requested from the web services interface. This vulnerability affects only specific AnyConnect and WebVPN configurations.

- **Action:** Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
- **Known To Be Used in Ransomware Campaigns?:** Known
- **Date Added:** 2024-02-15
- **Due Date:** 2024-03-07

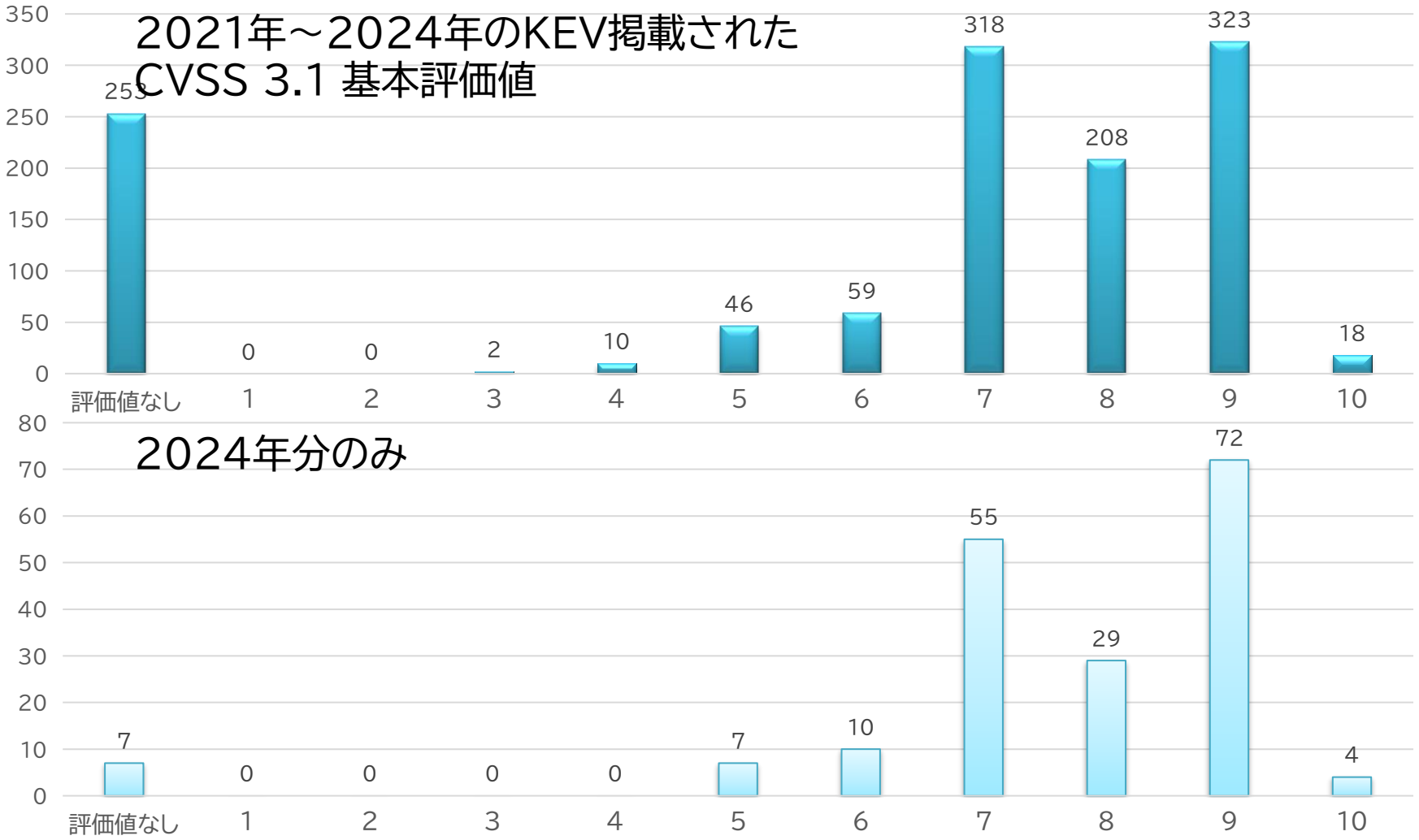
Resources and Notes +

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-info-disclose-9eJtycMB

JVNDB-2020-005198
CVE-2020-3259
Cisco Adaptive Security Appliance および Cisco Firepower Threat Defense ソフトウェアにおける脆弱性
2020年06月09日

KEV(悪用された既知の脆弱性一覧)
Known Exploited Vulnerabilities catalog

KEV(悪用された既知の脆弱性一覧)
Known Exploited Vulnerabilities catalog



KEV(悪用された既知の脆弱性一覧)
Known Exploited Vulnerabilities catalog

- 2021年~2024年のKEV掲載 CVSS 3.1 基本評価値 3.0~4.9

cveID	vulnerabilityName	dateAdded	CVSS 3.1基本
CVE-2023-26083	Arm Mali GPU Kernel Driver Information Disclosure Vulnerability	2023/4/7	3.3
CVE-2023-20867	VMware Tools Authentication Bypass Vulnerability	2023/6/23	3.9
CVE-2020-9819	Apple iOS, iPadOS, and watchOS Memory Corruption Vulnerability	2021/11/3	4.3
CVE-2020-8196	Citrix ADC, Gateway, and SD-WAN WANOP Appliance Information Disclosure Vulnerability	2021/11/3	4.3
CVE-2020-4430	IBM Data Risk Manager Directory Traversal Vulnerability	2021/11/3	4.3
CVE-2020-0878	Microsoft Edge and Internet Explorer Memory Corruption Vulnerability	2021/11/3	4.2
CVE-2021-20023	SonicWall Email Security Path Traversal Vulnerability	2021/11/3	4.9
CVE-2017-0059	Microsoft Internet Explorer Information Disclosure Vulnerability	2022/3/28	4.3
CVE-2012-0518	Oracle Fusion Middleware Unspecified Vulnerability	2022/3/28	4.7
CVE-2016-0162	Microsoft Internet Explorer Information Disclosure Vulnerability	2022/5/24	4.3
CVE-2018-13374	Fortinet FortiOS and FortiADC Improper Access Control Vulnerability	2022/9/8	4.3
CVE-2021-25370	Samsung Mobile Devices Memory Corruption Vulnerability	2022/11/8	4.4
CVE-2023-24880	Microsoft Windows SmartScreen Security Feature Bypass Vulnerability	2023/3/14	4.4
CVE-2023-21492	Samsung Mobile Devices Insertion of Sensitive Information Into Log File Vulnerability	2023/5/19	4.4

EPSS（脆弱性悪用予測評価システム）
Exploit Prediction Scoring System

脆弱性関連情報と脆弱性悪用の試みに関連するデータを用いて、機械学習を行い、その結果から今後30日間における悪用可能性を予測

- 用途
  - 今後、既知の脆弱性が悪用される可能性を踏まえて対処する。

- 悪用可能性
  - EPSSスコア
    - 今後30日間に悪用される確率
    - 0～100% の確率で表記

  - EPSSパーセンタイル
    - 悪用される可能性を相対的に表現
    - EPSSスコアを小さい順で並べたとき、あるスコアがデータの小さい方から見て何%の位置にあるかを表す

［出典］ EPSS Data and Statistics
https://www.first.org/epss/data_stats

EPSS(脆弱性悪用予測評価システム)
Exploit Prediction Scoring System

- 仕組み
  - 脆弱性関連情報
    ベンダ情報、CVEが公開されてからの日数、脆弱性の説明で使用されている用語、脆弱性の種別、CVSSスコア、掲載されているCVE情報、攻撃コードの公開など)
  - 脆弱性悪用の試みに関連するデータ
    データパートナーから提供されるハニーポット、IDS/IPSセンサーなどのデータで、実際に脆弱性悪用が試みられた証拠

EPSS(脆弱性悪用予測評価システム)
Exploit Prediction Scoring System

- 悪用可能性
  - EPSSスコア(今後30日間に悪用される確率を0～100%で表記)
  - EPSSパーセンタイル(EPSSスコアを小さい順で並べたとき、あるスコアがデータの小さい方から見て何%の位置にあるかを表す)

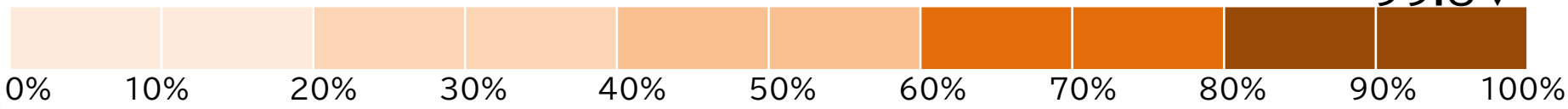
EPSSスコア

We selected the 48 highest rated CVEs published in the last 30 days. They are shown here with the CVE and EPSS score.

CVE-2024-27198 97.2%	CVE-2024-23225 0.1%	CVE-2024-21795 0.1%	CVE-2024-24794	CVE-2023-43552	CVE-2023-47534
CVE-2024-1709 93.5%	CVE-2024-26000 0.1%	CVE-2024-21812 0.1%			
CVE-2024-27199 0.9%	CVE-2024-23296 0.1%	CVE-2024-22097 0.1%			
CVE-2024-1212 0.7%	CVE-2024-27743 0.1%	CVE-2024-23305 0.1%			
CVE-2024-26492 0.1%	CVE-2024-27744 0.1%	CVE-2024-23310 0.1%	CVE-2024-23605 0.1%	CVE-2024-25995 0.1%	CVE-2024-21400 0.1%

JVNDB-2024-002919
CVE-2024-27198
JetBrains の TeamCity における脆弱性
2024年03月07日

パーセンタイル



EPSS（脆弱性悪用予測評価システム）
Exploit Prediction Scoring System

- 情報発信の形態
  - EPSSスコアを、CSVやJSON（API経由）などで提供
  - 例 https://epss.cyentia.com/epss_scores-current.csv.gz （最新データ）
    https://epss.cyentia.com/epss_scores-2024-11-30.csv.gz
- 悪用可能性
  - EPSSスコア（今後30日間に悪用される確率を0～100%で表記）
  - EPSSパーセンタイル（EPSSスコアを小さい順で並べたとき、あるスコアがデータの小さい方から見て何%の位置にあるかを表す）

EPSSスコア↓　　↓パーセンタイル

	A	B	C	D
1	#model_version:v2	score_date:2024-11-30T00:00:00+0000		
2	cve	epss	percentile	
246575	CVE-2024-27193	0.00043	0.10425	
246576	CVE-2024-27194	0.00043	0.10425	
246577	CVE-2024-27195	0.00043	0.10425	
246578	CVE-2024-27196	0.00043	0.10425	
246579	CVE-2024-27197	0.00043	0.10425	
246580	CVE-2024-27198	0.97238	0.9988	
246581	CVE-2024-27199	0.0099	0.84158	
246582	CVE-2024-27200	0.00043	0.10425	
246583	CVE-2024-27201	0.00045	0.15556	
246584	CVE-2024-27202	0.00043	0.10425	
246585	CVE-2024-27204	0.00043	0.10425	
246586	CVE-2024-27205	0.00043	0.10425	

epss_scores-2024-11-30

編集　アクセシビリティ: 利用不可　100%

EPSS（脆弱性悪用予測評価システム）
Exploit Prediction Scoring System

- 情報発信の形態
  - EPSSスコアを、CSVやJSON（API経由）などで提供
  - 例 https://api.first.org/data/v1/epss?cve=CVE-2024-27198（最新データ
    https://api.first.org/data/v1/epss?cve=CVE-2024-27198&date=2024-03-19
- 悪用可能性
  - EPSSスコア（今後30日間に悪用される確率を0～100%で表記）
  - EPSSパーセンタイル（EPSSスコアを小さい順で並べたとき、あるスコアがデータの小さい方から見て何%の位置にあるかを表す）


```
{
    "status": "OK",
    "status-code": 200,
    "version": "1.0",
    "access": "public",
    "total": 1,
    "offset": 0,
    "limit": 100,
    "data": [
        {
            "cve": "CVE-2024-27198",
            "epss": "0.972090000",
            "percentile": "0.998110000",
            "date": "2024-03-19"
        }
    ]
}
```


← EPSSスコア
←パーセンタイル

SSVC(役割に応じた脆弱性対応分類)
Stakeholder-Specific Vulnerability Categorization

判断分岐点が設定された決定木を辿ることで、取るべき脆弱性対応の優先度を提示

- 用途
  - 役割(=対象者)に応じて、脆弱性対応の優先度を分類する。

- 対象者(=役割)
  - デプロイヤー(修正プログラム利用側) v2.1.0
  - サプライヤー(修正プログラム提供側) v2.0.0
  - 米国政府、州、地方、部族、準州政府、および重要なインフラストラクチャ事業体 v2.0.3
  - コーディネーター(脆弱性ハンドリング調整役)[脆弱性情報公開] v2.0.0
  - コーディネーター(脆弱性ハンドリング調整役)[脆弱性トリアージ] v2.0.0

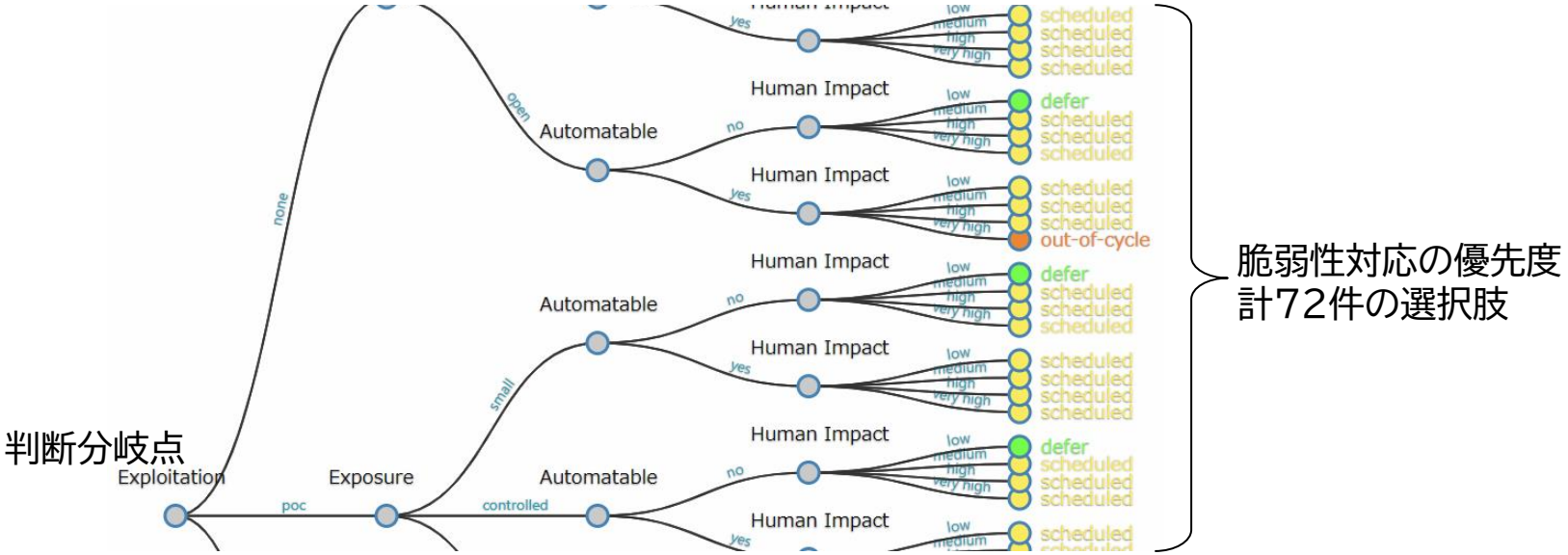
[出典] SSVC
https://certcc.github.io/SSVC/

SSVC（役割に応じた脆弱性対応分類）
Stakeholder-Specific Vulnerability Categorization

- デプロイヤー（修正プログラム利用側）
  - 判断分岐点
    - 脆弱性の悪用状況（Exploitation）：未報告、実証可能、攻撃可能
    - システムの露出状況（Exposure）：閉域的、限定的、オープン
    - 攻撃の自動化可能性（Automatable）：なし、あり
    - 影響の大きさ（Human Impact）：低、中、高、極めて高
      - 安全への影響（Situated Safety Impact）：なし、軽微、重大、危険、壊滅的
      - 業務遂行への影響（Mission Impact）：なし、間接的、直接的、長期的、全体的
  - 脆弱性対応の優先度
    - Immediate：迅速な対応
    - Out-of-cycle：定期メンテナンス以外の早い時期での対応
    - Scheduled：定期メンテナンス時に対応
    - Defer：現時点では対応不要

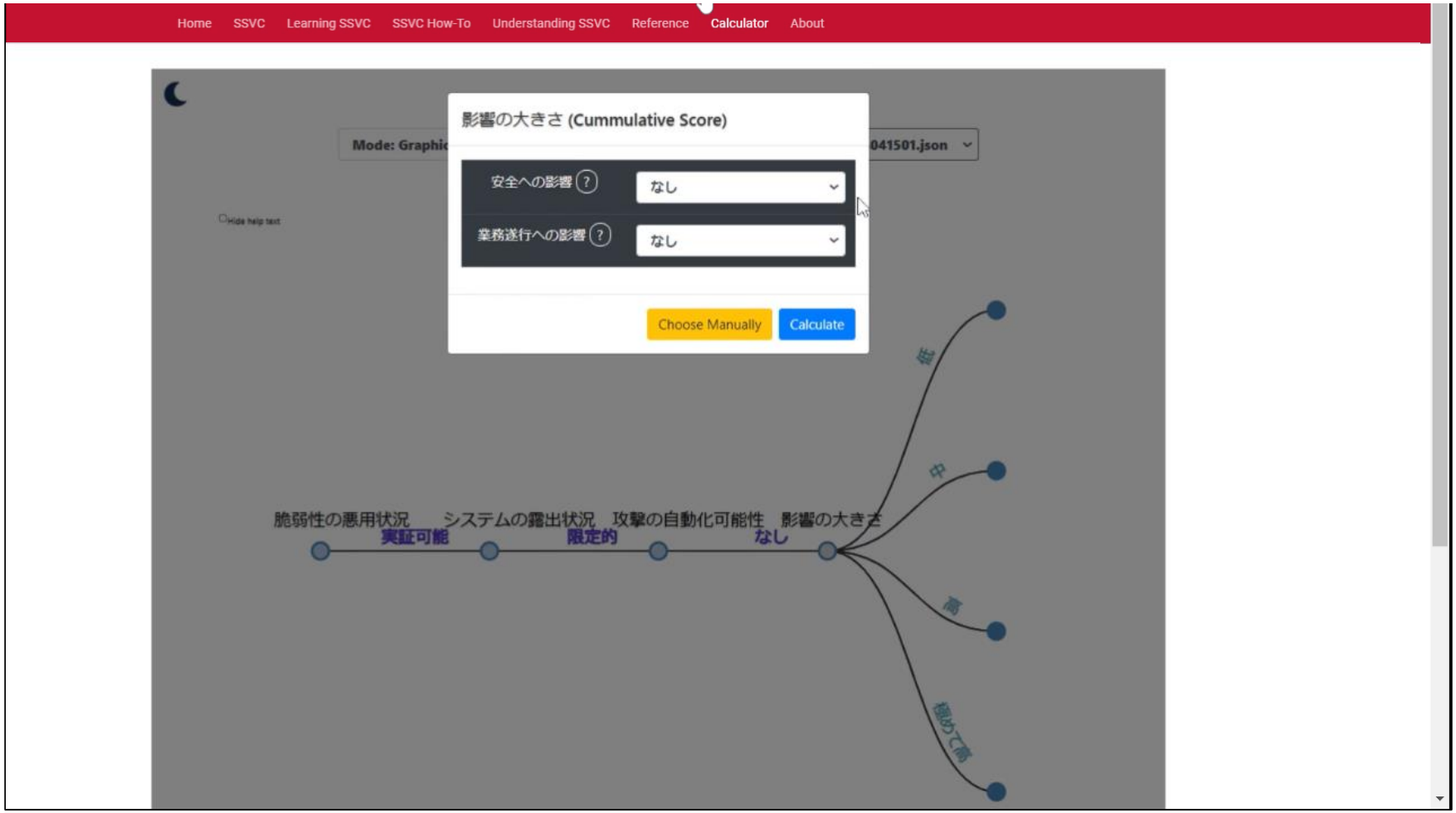
SSVC（役割に応じた脆弱性対応分類）
Stakeholder-Specific Vulnerability Categorization

- デプロイヤー（修正プログラム利用側）
  - 判断分岐点
    - 脆弱性の悪用状況（Exploitation）：未報告、実証可能、攻撃可能
    - システムの露出状況（Exposure）：閉域的、限定的、オープン
    - 攻撃の自動化可能性（Automatable）：なし、あり
    - 影響の大きさ（Human Impact）：低、中、高、極めて高
      - 安全への影響（Situated Safety Impact）：なし、軽微、重大、危険、壊滅的
      - 業務遂行への影響（Mission Impact）：なし、間接的、直接的、長期的、全体的



SSVC（役割に応じた脆弱性対応分類）
Stakeholder-Specific Vulnerability Categorization

- デプロイヤー（修正プログラム利用側）

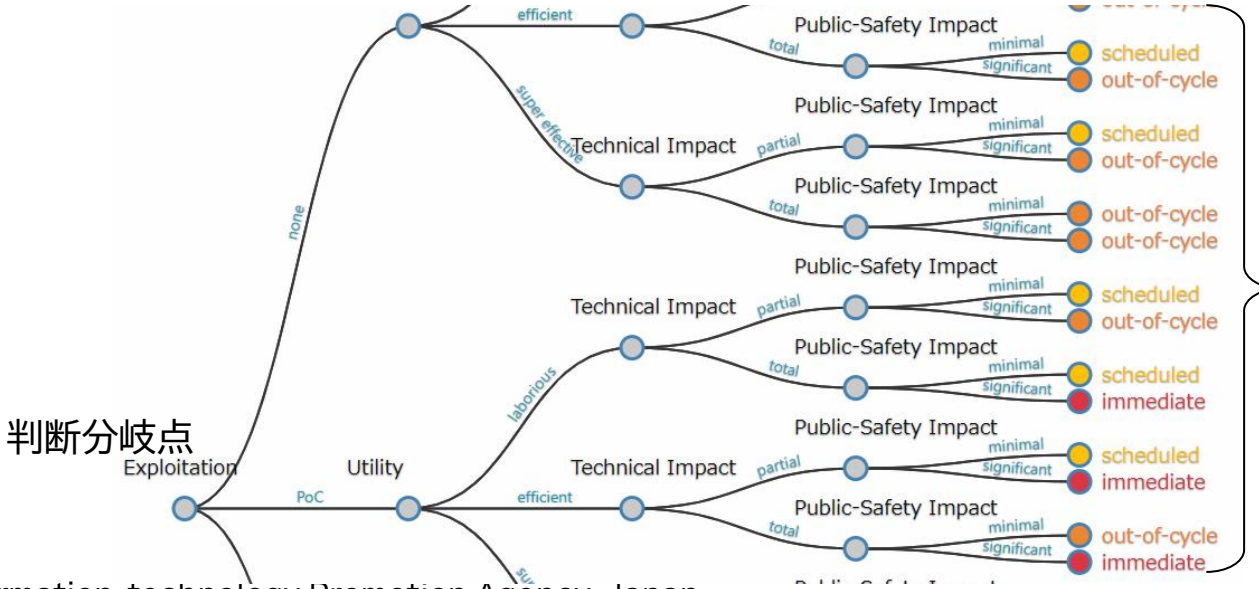


SSVC（役割に応じた脆弱性対応分類）
Stakeholder-Specific Vulnerability Categorization

- サプライヤー（修正プログラム提供側）
  - 判断分岐点
    - 脆弱性の悪用状況（Exploitation）：未報告、実証可能、攻撃可能
    - 攻撃の実効性（Utility）：手間、効率的、極めて効率的
      - 攻撃の自動化可能性（Automatable）：なし、あり
      - 攻撃に利用可能な資源（Value Density）：少ない、多い
    - 技術的な影響（Technical Impact）：部分的、全面的
    - 安全性全般への影響（Public-Safety Impact）：最小、重大
  - 脆弱性対応の優先度
    - Immediate：迅速な対応
    - Out-of-cycle：定期メンテナンス以外の早い時期での対応
    - Scheduled：定期メンテナンス時に対応
    - Defer：現時点では対応不要

SSVC（役割に応じた脆弱性対応分類）
Stakeholder-Specific Vulnerability Categorization

- サプライヤー（修正プログラム提供側）
  - 判断分岐点
    - 脆弱性の悪用状況（Exploitation）：未報告、実証可能、攻撃可能
    - 攻撃の実効性（Utility）：手間、効率的、極めて効率的
      - 攻撃の自動化可能性（Automatable）：なし、あり
      - 攻撃に利用可能な資源（Value Density）：少ない、多い
    - 技術的な影響（Technical Impact）：部分的、全面的
    - 安全性全般への影響（Public-Safety Impact）：最小、重大

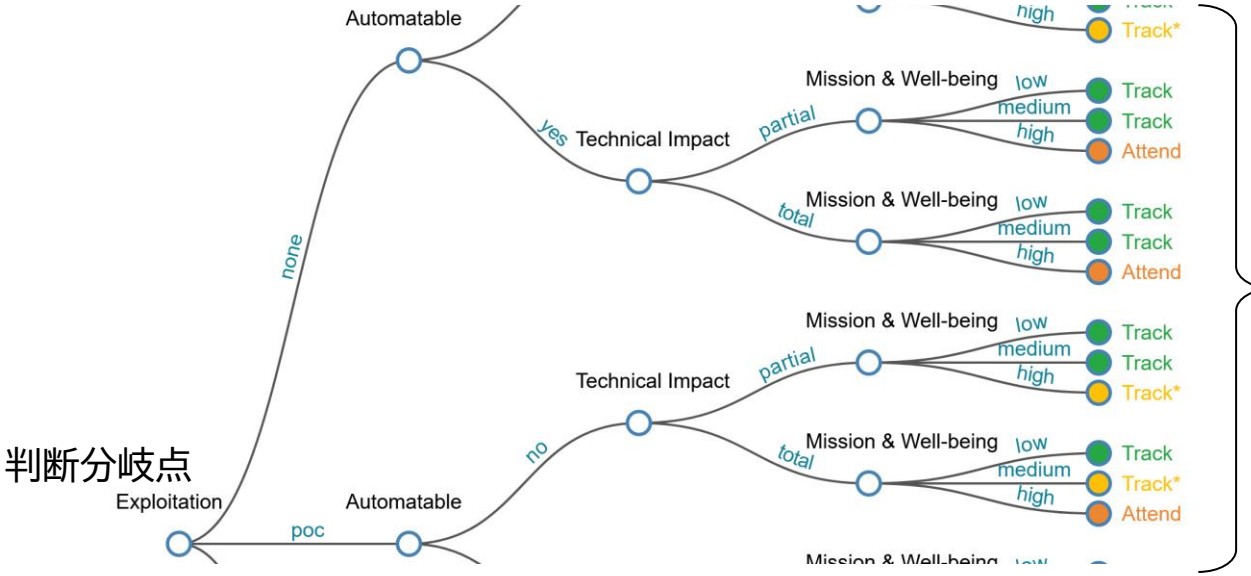


SSVC（役割に応じた脆弱性対応分類）
Stakeholder-Specific Vulnerability Categorization

- 公的機関、重要なインフラストラクチャ事業体
  - 判断分岐点
    - 脆弱性の悪用状況（Exploitation）：未報告、実証可能、攻撃可能
    - 攻撃の自動化可能性（Automatable）：なし、あり
    - 技術的な影響（Technical Impact）：部分的、全面的
    - 業務遂行・社会への影響（Mission & Well-being）：低、中、高
      - 業務遂行への関与（Mission Prevalence）：最小、補助、必須
      - 社会への影響（Public Well-being Impact）：最小、重要、不可逆的
  - 脆弱性対応の優先度
    - Act：迅速な対応
    - Attend：定期メンテナンス以外の早い時期での対応
    - Track*：定期メンテナンス時に対応
    - Track：現時点では対応不要

SSVC（役割に応じた脆弱性対応分類）
Stakeholder-Specific Vulnerability Categorization

- 公的機関、重要なインフラストラクチャ事業体
  - 判断分岐点
    - 脆弱性の悪用状況（Exploitation）：未報告、実証可能、攻撃可能
    - 攻撃の自動化可能性（Automatable）：なし、あり
    - 技術的な影響（Technical Impact）：部分的、全面的
    - 業務遂行・社会への影響（Mission & Well-being）：低、中、高
      - 業務遂行への関与（Mission Prevalence）：最小、補助、必須
      - 社会への影響（Public Well-being Impact）：最小、重要、不可逆的

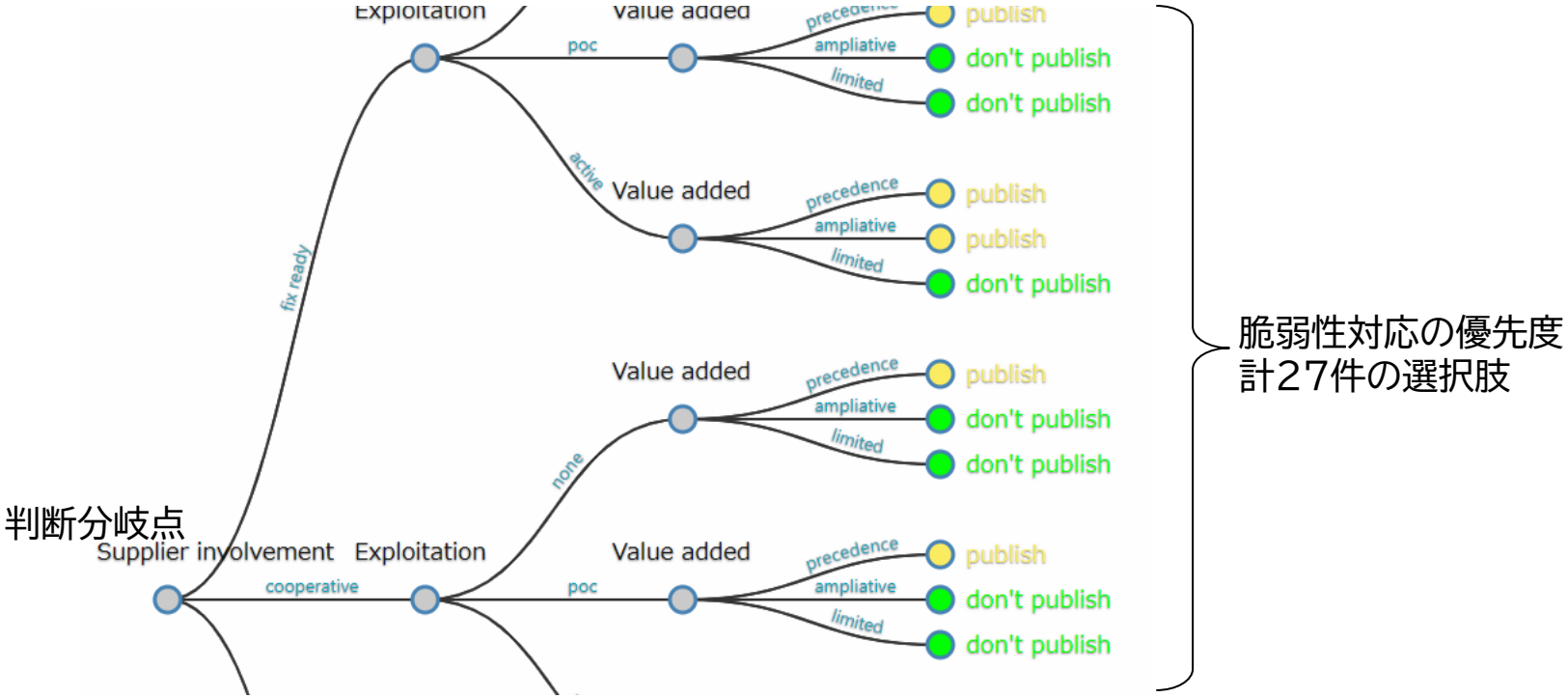


SSVC（役割に応じた脆弱性対応分類）
Stakeholder-Specific Vulnerability Categorization

- コーディネーター（脆弱性ハンドリング調整役）[脆弱性情報公開]
  - 判断分岐点
    - サプライヤーの関与（Supplier involvement）：対応済、調整中、応答なし
    - 脆弱性の悪用状況（Exploitation）：未報告、実証可能、攻撃可能
    - 情報の位置付け（Value added）：初版、改訂版、付録
  - 脆弱性対応の優先度
    - publish：公開
    - don‘t publish：公開しない

SSVC(役割に応じた脆弱性対応分類)
Stakeholder-Specific Vulnerability Categorization

- コーディネーター(脆弱性ハンドリング調整役)[脆弱性情報公開]
  - 判断分岐点
    - サプライヤーの関与(Supplier involvement): 対応済、調整中、応答なし
    - 脆弱性の悪用状況(Exploitation): 未報告、実証可能、攻撃可能
    - 情報の位置付け(Value added): 初版、改訂版、付録

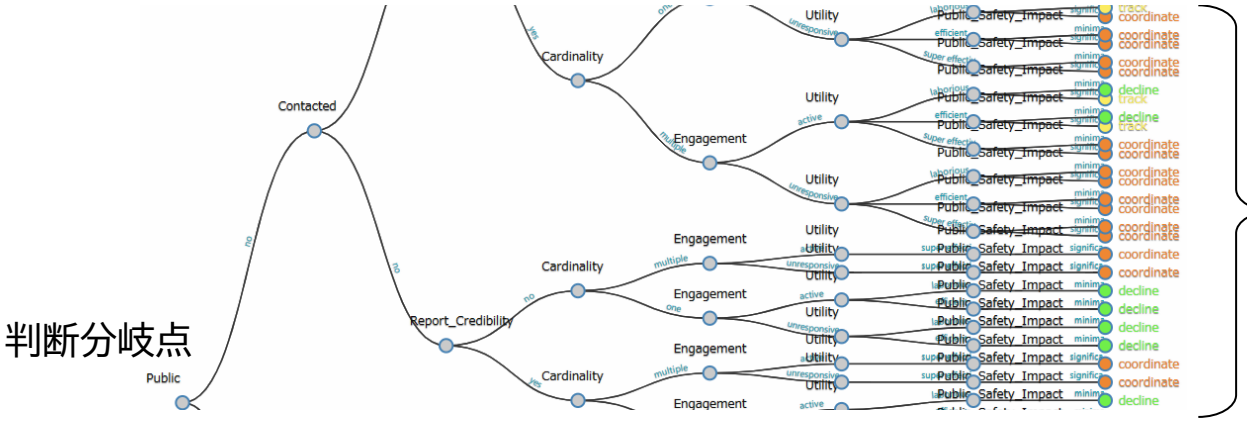


SSVC（役割に応じた脆弱性対応分類）
Stakeholder-Specific Vulnerability Categorization

- コーディネーター（脆弱性ハンドリング調整役）[脆弱性トリアージ]
  - 判断分岐点
    - 情報の公開（Public）：されている、されていない
    - 報告者の報告調整（Contacted）：良い、悪い
    - 報告の信頼性（Report Credibility）：あり、なし
    - 対応関係者の数（Cardinality）：シングル、マルチ
    - 対応関係者の関与（Engagement）：積極的、応答なし
    - 攻撃の実効性（Utility）：手間、効率的、極めて効率的
      - 攻撃の自動化可能性（Automatable）：なし、あり
      - 攻撃に利用可能な資源（Value Density）：少ない、多い
    - 社会安全への影響（Public Safety Impact）：最小、重要
  - 脆弱性対応の優先度
    - decline：対応せず
    - track ：様子見
    - coordinate：対応する

SSVC（役割に応じた脆弱性対応分類）
Stakeholder-Specific Vulnerability Categorization

- コーディネーター（脆弱性ハンドリング調整役）[脆弱性トリアージ]
  - 判断分岐点
    - 情報の公開（Public）：されている、されていない
    - 報告者の報告調整（Contacted）：良い、悪い
    - 報告の信頼性（Report Credibility）：あり、なし
    - 対応関係者の数（Cardinality）：シングル、マルチ
    - 対応関係者の関与（Engagement）：積極的、応答なし
    - 攻撃の実効性（Utility）：手間、効率的、極めて効率的
      - 攻撃の自動化可能性（Automatable）：なし、あり
      - 攻撃に利用可能な資源（Value Density）：少ない、多い
    - 社会安全への影響（Public Safety Impact）：最小、重要



脆弱性対策の動向と
効果的な収集に向けて

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
2025年03月27日