IPA
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
2024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。

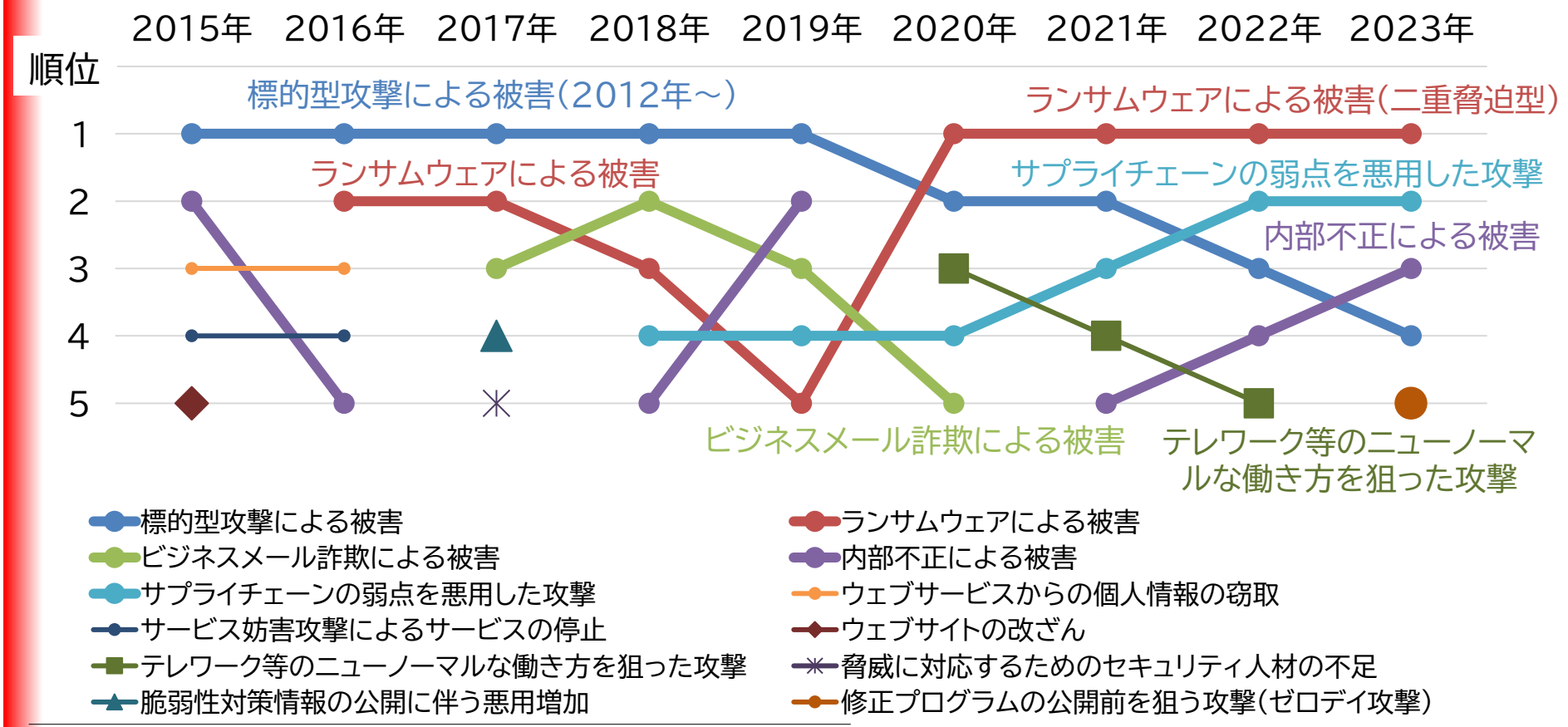
1. トピック[1][2]
2. 情報収集に役立つ技術仕様
3. 自動化(機械化)処理基盤の潮流
4. JVN脆弱性対策機械処理基盤
5. トピック[3]

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 2024

- 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 2024
https://www.ipa.go.jp/security/10threats/10threats2024.html

情報セキュリティ10大脅威 2024

- 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

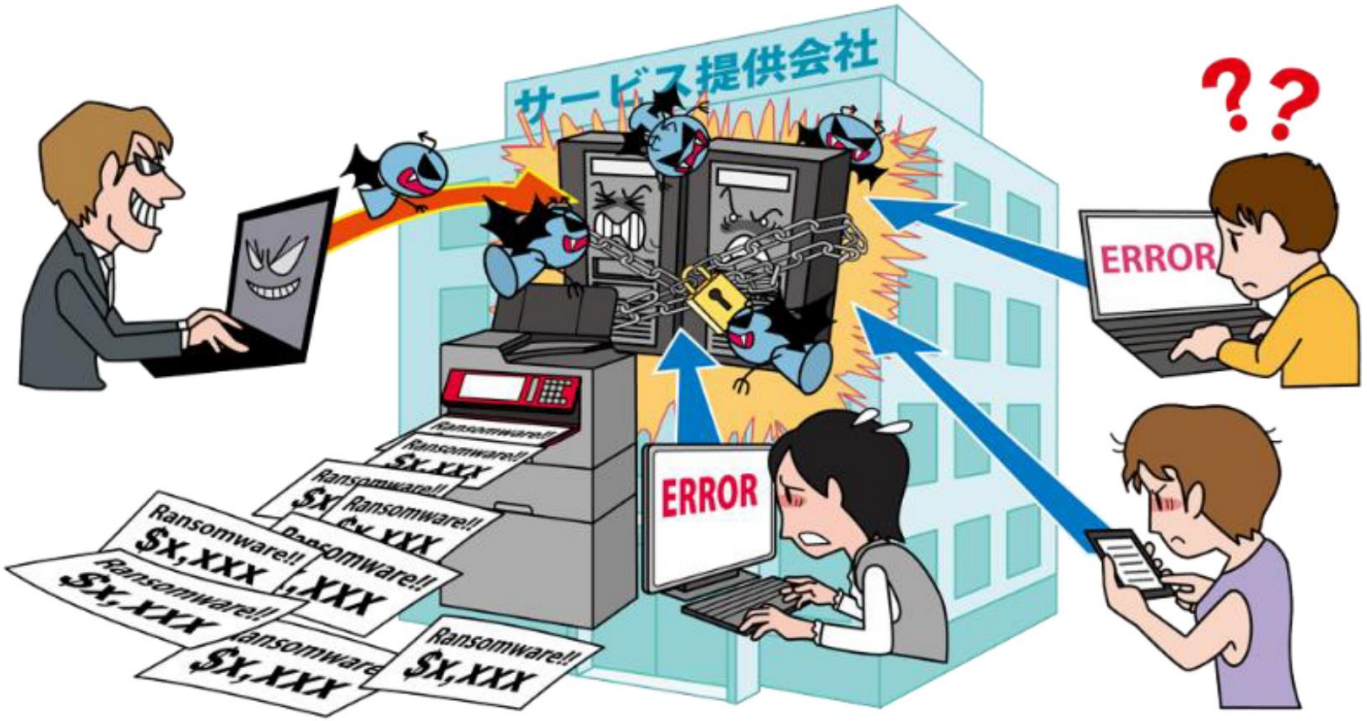
個人
インターネット上のサービスからの個人情報の窃取
インターネット上のサービスへの不正ログイン
クレジットカード情報の不正利用
スマホ決済の不正利用
偽警告によるインターネット詐欺
ネット上の誹謗・中傷・デマ
フィッシングによる個人情報等の詐取
不正アプリによるスマートフォン利用者への被害
メールやSMS等を使った脅迫・詐欺の手口による金銭要求
ワンクリック請求等の不当請求による金銭被害

順位	組織
1位	ランサムウェアによる被害
2位	サプライチェーンの弱点を悪用した攻撃
3位	内部不正による情報漏えい等の被害
4位	標的型攻撃による機密情報の窃取
5位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
6位	不注意による情報漏えい等の被害
7位	脆弱性対策情報の公開に伴う悪用増加
8位	ビジネスメール詐欺による金銭被害
9位	テレワーク等のニューノーマルな働き方を狙った攻撃
10位	犯罪のビジネス化（アンダーグラウンドサービス）

［出典］　情報セキュリティ10大脅威 2024
https://www.ipa.go.jp/security/10threats/10threats2024.html

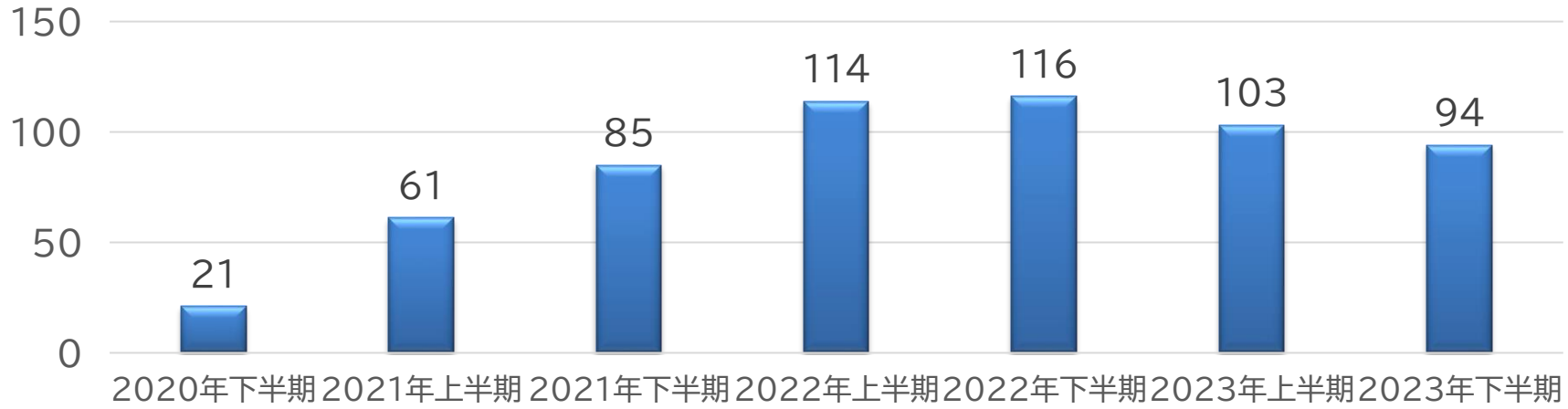
情報セキュリティ10大脅威 2024
ランサムウェアによる被害

- 組織の規模や業種は関係なし！次の標的はあなたの組織かも？
  - 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）



ランサムウェアによる被害
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

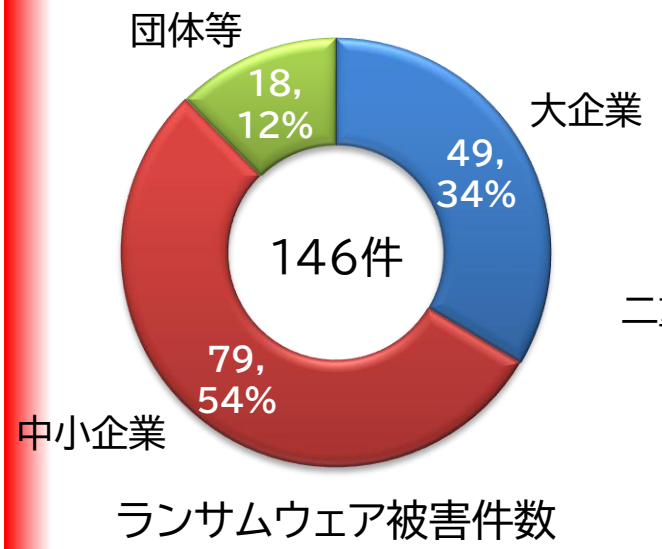


- 2021年～2023年のランサムウェア被害の特徴
  - 二重恐喝(ダブルエクストーション)による被害が多くを占める
  - 暗号資産による金銭の要求が多くを占める
  - 企業・団体等の規模や業種を問わず被害が発生
  - 感染経路は、テレワークにも利用される機器等の脆弱性や強度の弱い認証情報等を利用して侵入したと考えられるものが大半を占めている

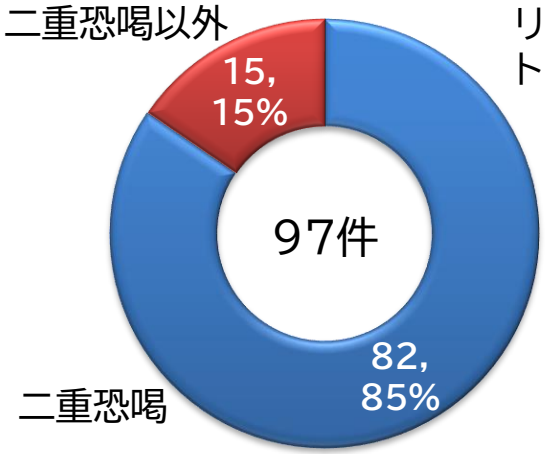
［出典］　令和5年におけるサイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf

ランサムウェアによる被害
被害の状況

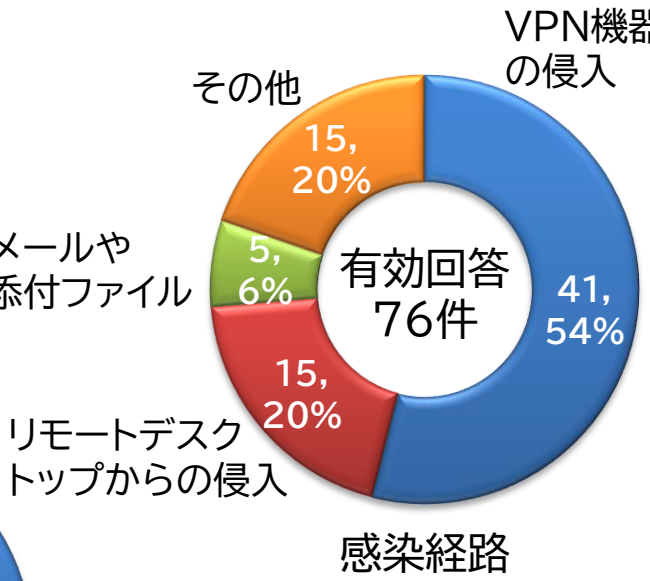
- 2021年のランサムウェア被害の状況



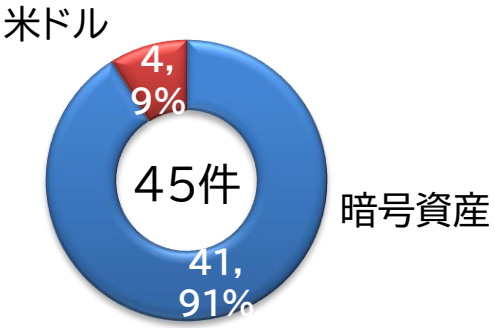
ランサムウェア被害件数



手口を確認できた被害



感染経路

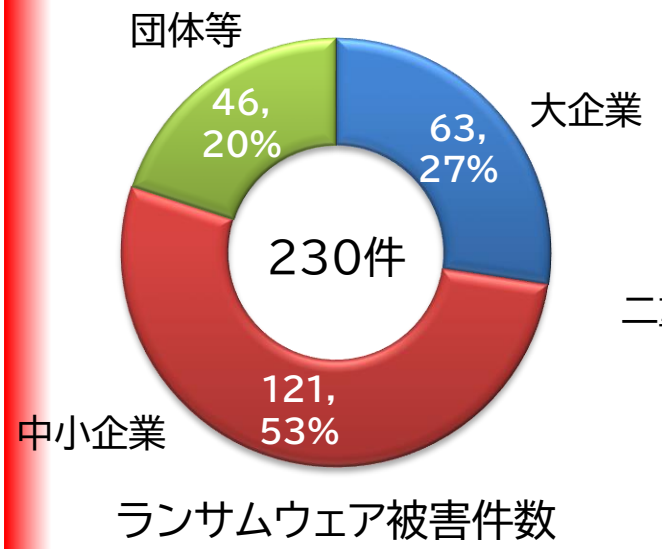


直接的な金銭要求あり

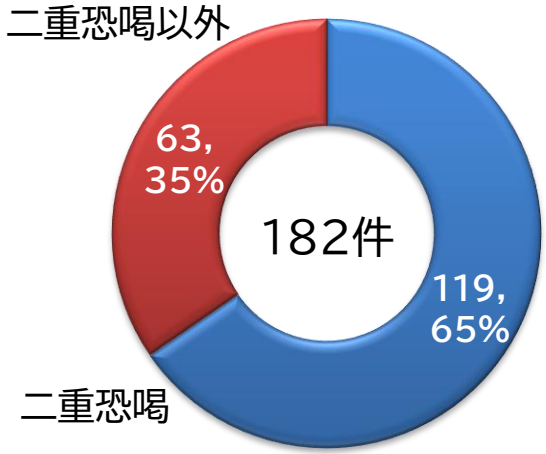
［出典］　令和3年におけるサイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf

ランサムウェアによる被害
被害の状況

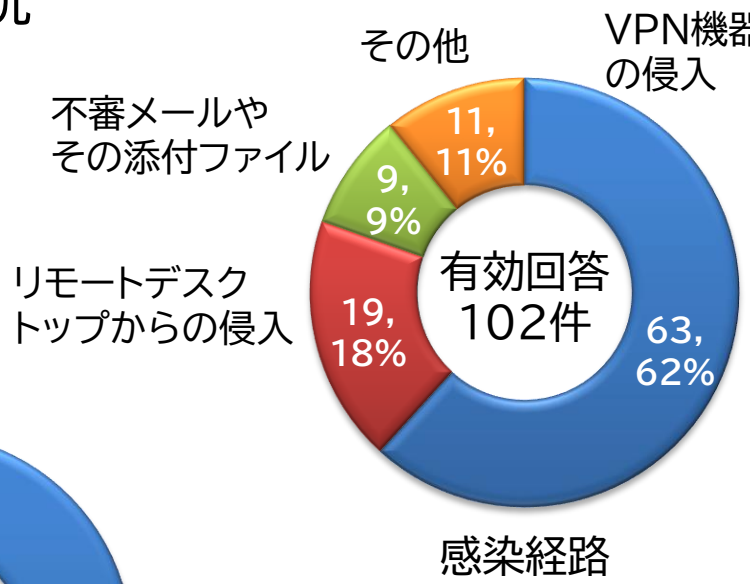
- 2022年のランサムウェア被害の状況



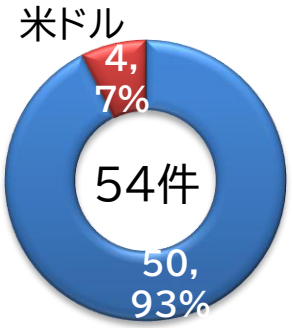
ランサムウェア被害件数



手口を確認できた被害



感染経路

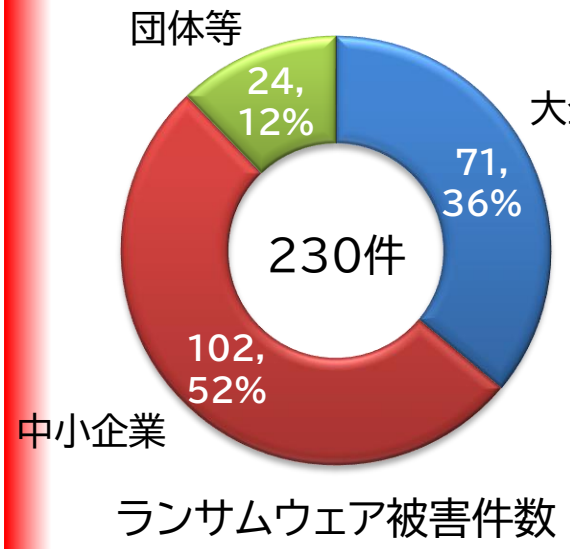


直接的な金銭要求あり

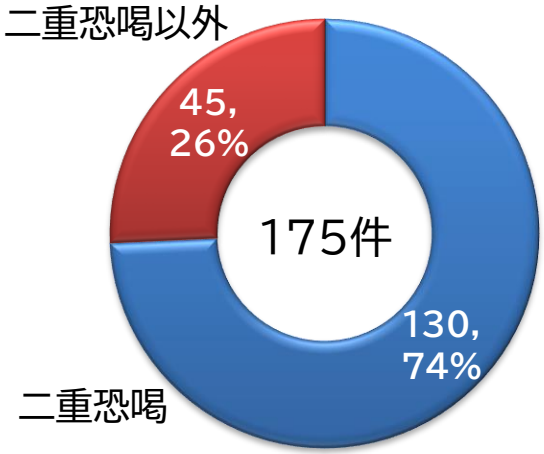
［出典］　令和4年におけるサイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf

ランサムウェアによる被害
被害の状況

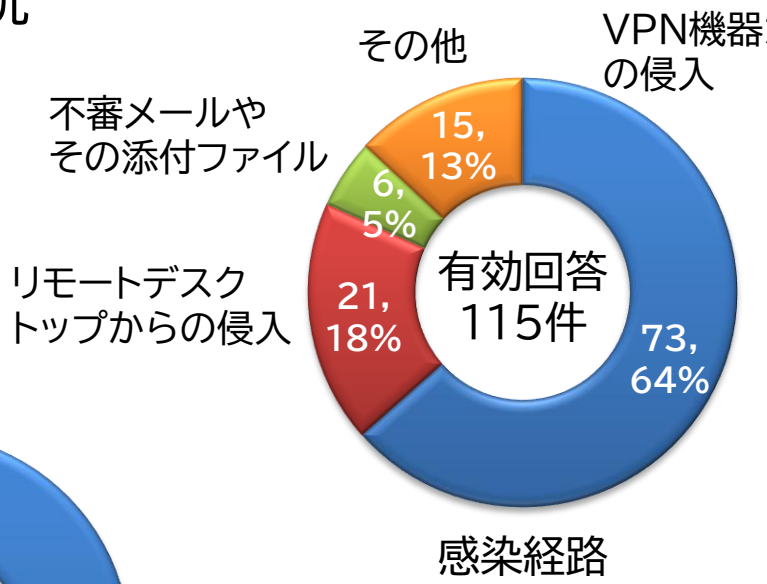
- 2023年のランサムウェア被害の状況



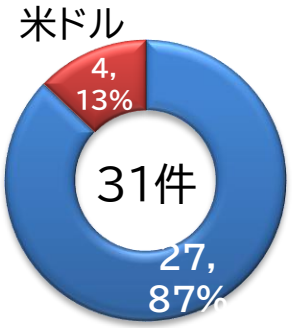
ランサムウェア被害件数



手口を確認できた被害



感染経路

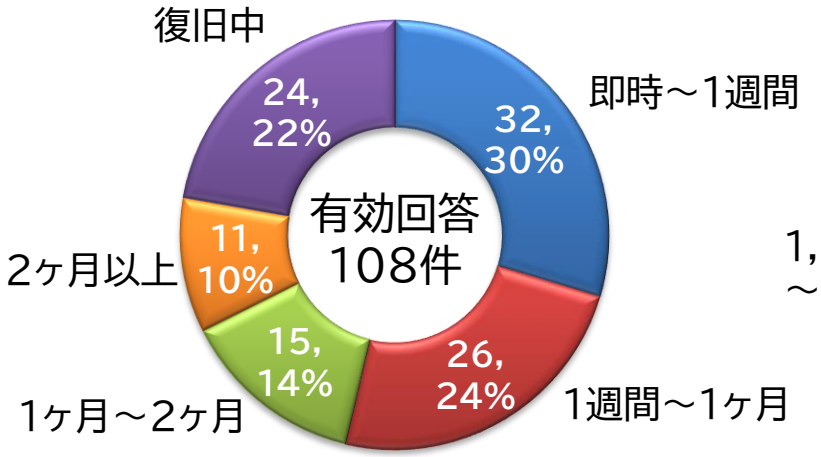


直接的な金銭要求あり

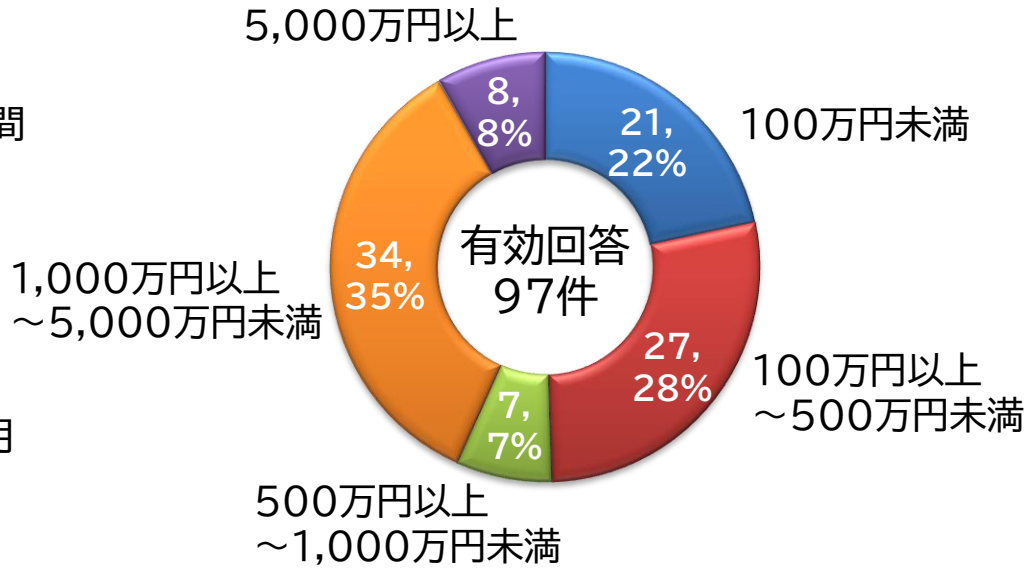
［出典］　令和5年におけるサイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf

ランサムウェアによる被害
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

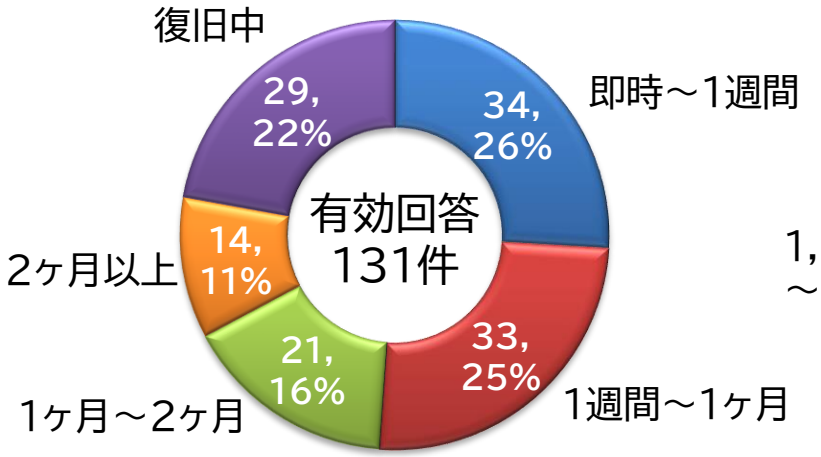


調査・復旧費用の総額

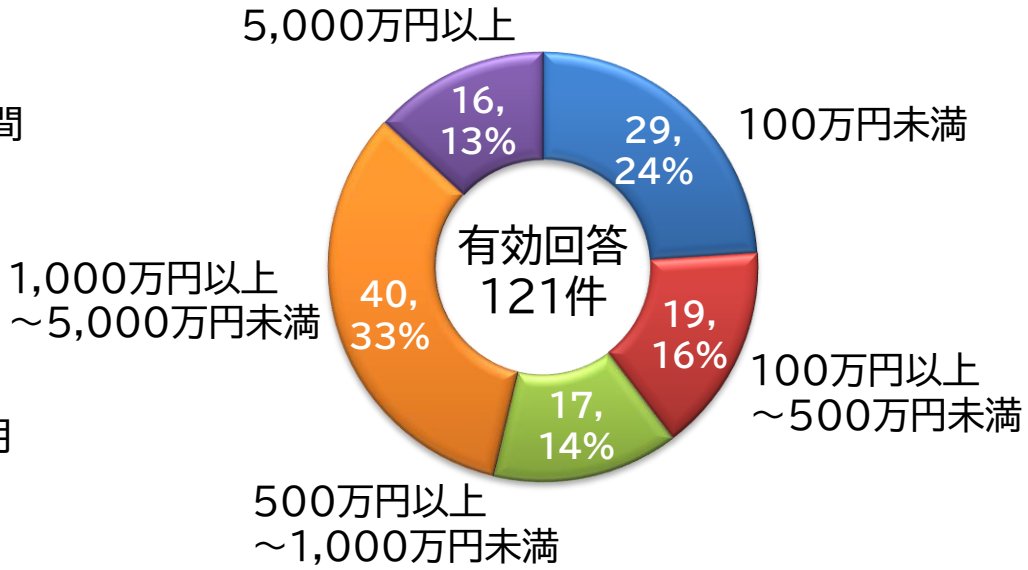
［出典］　令和3年におけるサイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf

ランサムウェアによる被害
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

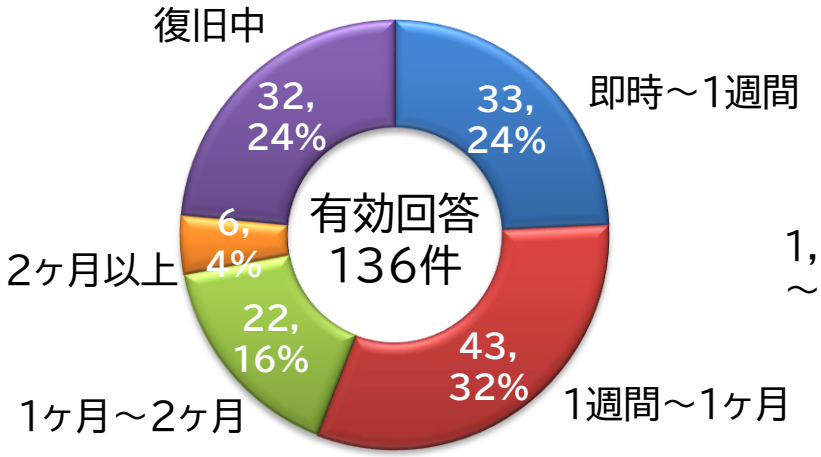


調査・復旧費用の総額

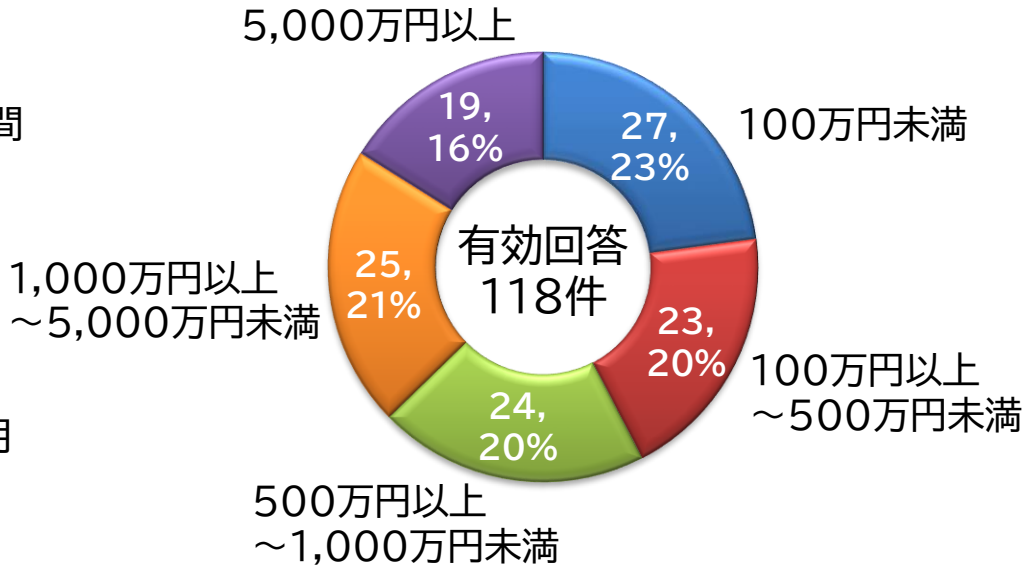
［出典］　令和4年におけるサイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf

ランサムウェアによる被害
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

ランサムウェアによる被害
グローバル実態調査

- 法人組織におけるIT部門の意思決定者を対象に調査した「ランサムウェア攻撃 グローバル実態調査 2022年版」によれば、
  - ランサムウェア攻撃を受けた国内法人組織の約7割が、顧客やビジネスパートナーへ攻撃を知らされる四重脅迫の被害に
  - 窃取情報の暴露（二重脅迫）で、約半数が顧客やビジネスパートナー・サプライチェーン情報が流出
  - ランサムウェア実行に至る前の各攻撃プロセスの検出は低い傾向

調査期間：2022年5月～2022年6月
調査対象：法人組織におけるIT部門の意思決定者 2,958名
（日本を含む26の国と地域：2,958名、日本のみ：203名）
調査手法：インターネット調査

［出典］ ランサムウェア攻撃 グローバル実態調査 2022年版
https://www.trendmicro.com/ja_jp/about/press-release/2022/pr-20220907-01.html

ランサムウェアによる被害
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。

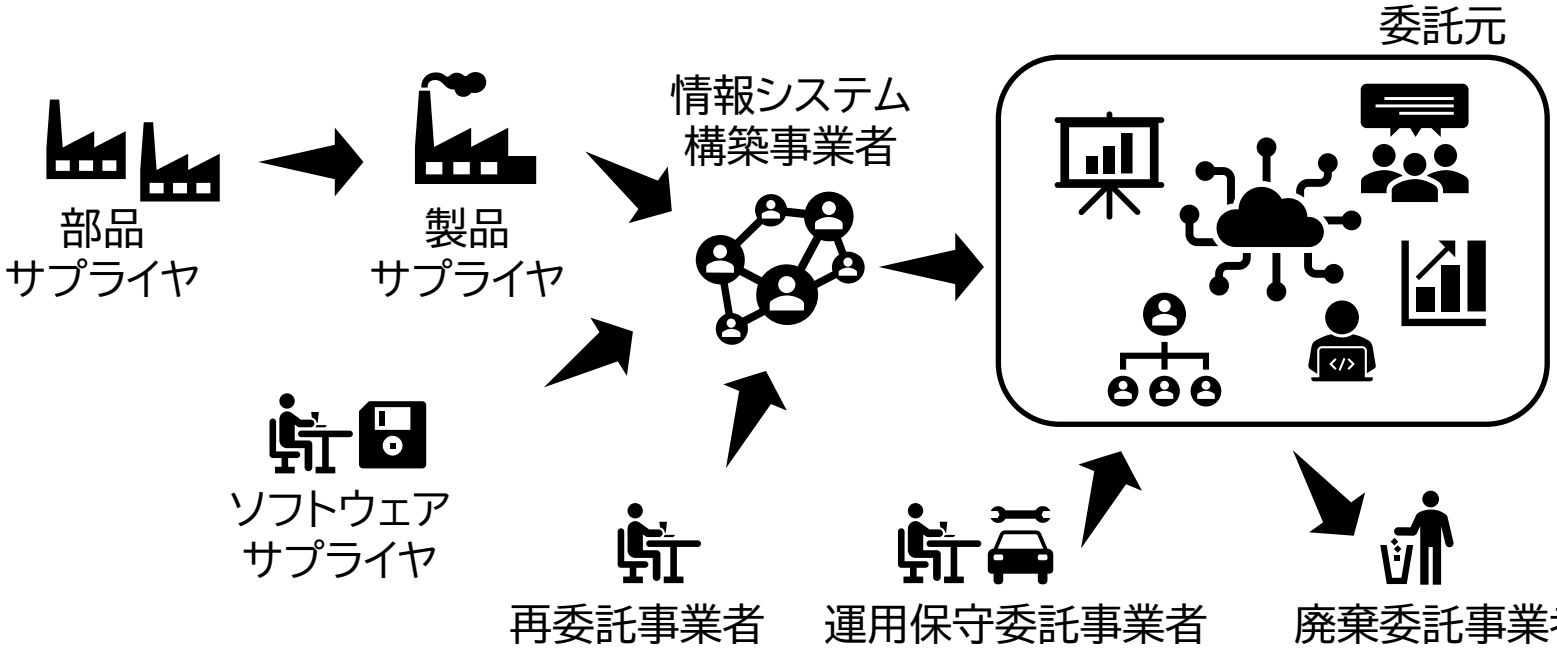
情報セキュリティ10大脅威 2024
サプライチェーンの弱点を悪用した攻撃

- ビジネスもセキュリティ対策も関係組織で二人三脚を
  - 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

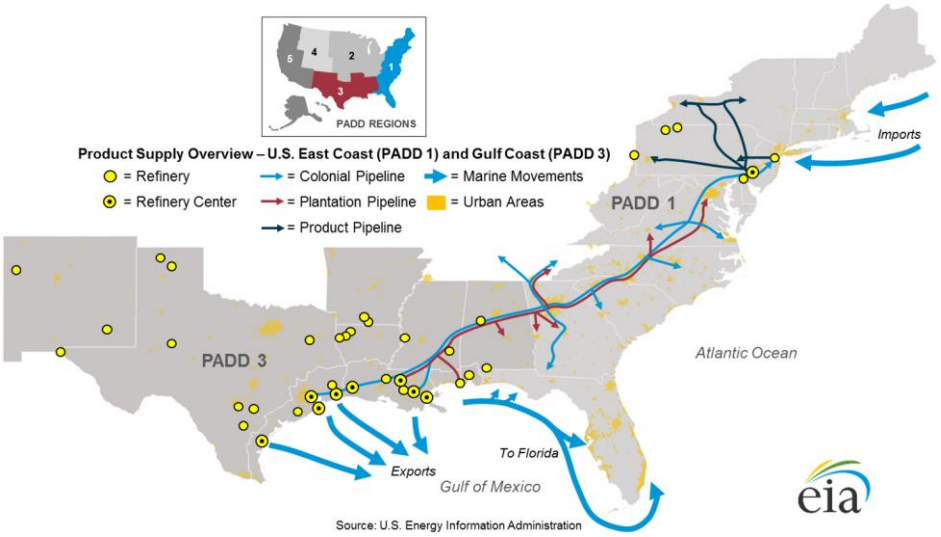
サプライチェーンの弱点を悪用した攻撃
サプライチェーンとは

- 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）



サプライチェーンの弱点を悪用した攻撃
米国石油パイプライン事案(2021年5月7日)

- 脆弱なリモートサービスを悪用したランサムウェア感染であったが、、、
  - ITシステムの一部に影響が及び、封じ込めのためシステムをオフライン化
  - 結果、米東海岸燃料消費の45%を供給するパイプライン網が一次操業停止



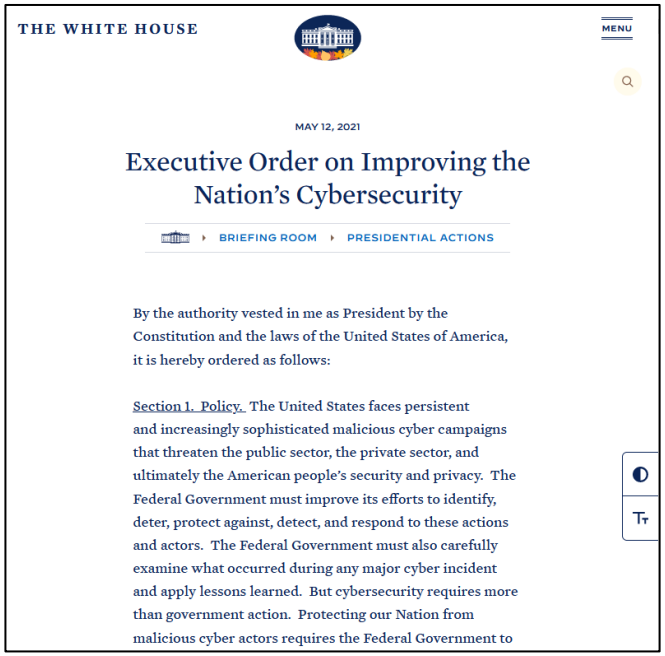
コロニアル・パイプライン社事案

日付	対応経緯
5月6日～7日	サイバー攻撃によりITシステムの一部に影響が及び、封じ込めのため、パイプラインシステムをオフライン化
5月12日	パイプライン操業を再開
5月13日	パイプラインシステム全体を再開 身代金を支払ったとの報道

[出典] East Coast and Gulf Coast Transportation Fuels Markets - Energy Information Administration
https://www.eia.gov/analysis/transportationfuels/padd1n3/
Colonial Pipeline Cyberattack Highlights Need for Better Federal and Private-Sector Preparedness (infographic)
https://www.gao.gov/blog/colonial-pipeline-cyberattack-highlights-need-better-federal-and-private-sector-preparedness-infographic

サプライチェーンの弱点を悪用した攻撃
サイバーセキュリティ強化の大統領令（2021年5月12日）

- 一連の被害を受け、サイバーセキュリティ強化に乗り出す
  - 米国石油パイプライン事案が引き金、5日後大統領令が公布される
  - 大統領令によりソフトウェアサプライチェーンセキュリティ対策の注目度が高まる



THE WHITE HOUSE

MENU

MAY 12, 2021

Executive Order on Improving the Nation's Cybersecurity

BRIEFING ROOM › PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to

【大統領令で言及している実施項目】
- 脅威情報を共有する際の障壁を取り除くこと
- 連邦政府におけるサイバーセキュリティの近代化
- ソフトウェアサプライチェーンのセキュリティの強化
  - 製品が安全に、意図したとおりに機能することを保証すること
- サイバー安全審査委員会の設置
- 連邦政府ネットワークにおけるサイバーセキュリティの脆弱性とインシデントの検出の整備
- 連邦政府の調査および修復能力の改善
- 国家安全保障システムへの適用

［出典］ Executive Order on Improving the Nation's Cybersecurity
https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

サプライチェーンの弱点を悪用した攻撃
品質の見える化：Software Component Transparency

- サイバーセキュリティに関する米国大統領令（2021年5月12日）
  - ソフトウェアサプライチェーンのセキュリティ強化
    - 製品が安全に、意図したとおりに機能することを保証すること

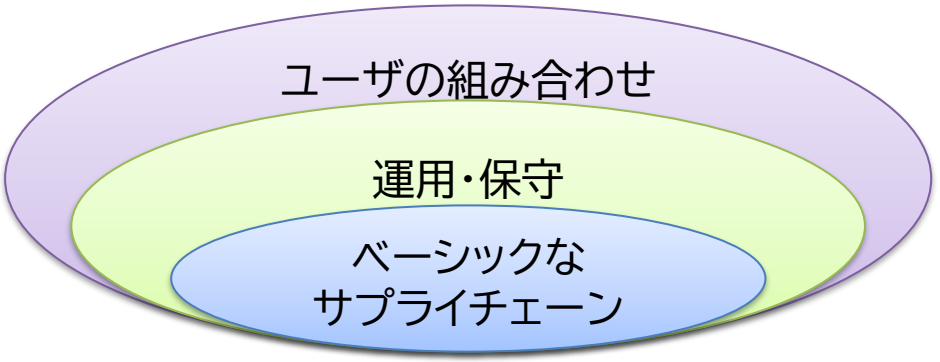
ソフトウェアサプライチェーンのセキュリティを強化するガイダンスの発行

- 安全なソフトウェア開発環境の確保
- 購入者からの要求に従い安全なソフトウェア開発環境を提示する方法
- 自動化されたツールあるいは同等の方法によりサプライチェーンにおけるコードの整合性の確保
- 自動化されたツールあるいは同等の方法により既知あるいは、潜在的な脆弱性の検査
- 購入者からの要求に従いコードの整合性や脆弱性に関する情報を提示する方法
- ソフトウェアコードまたはコンポーネントの出所管理
- 購入者へのソフトウェア部品表（SBOM）の提供（直接提供、公開Webサイトに公開）
- 報告ならびに開示プロセスを含む脆弱性開示プログラムへの参加
- 安全なソフトウェア開発を実践していることの証明
- 可能な範囲で、製品で使用しているオープンソースソフトウェアの完全性と出所の保証と証明

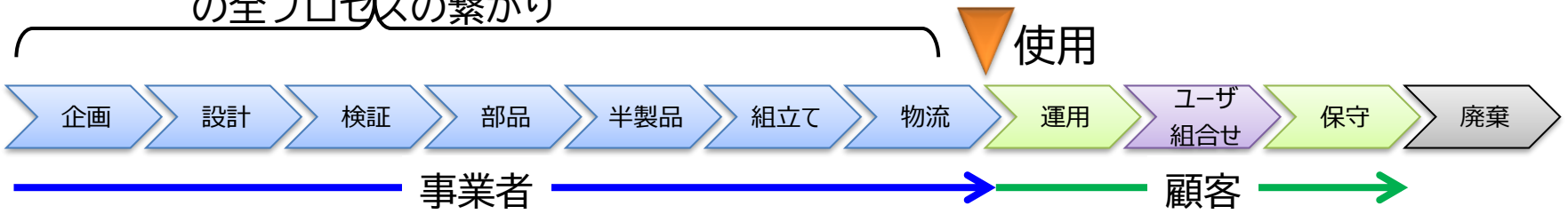
［出典］ CISA, NSA, and ODNI Release Guidance for Customers on Securing the Software Supply Chain
https://www.cisa.gov/news-events/news/cisa-nsa-and-odni-release-guidance-customers-securing-software-supply-chain

サプライチェーンの弱点を悪用した攻撃
ソフトウェアサプライチェーンとは

- ソフトウェアの開発から、それがエンドユーザに使用されるまでの流通、その後の運用・保守、およびユーザが組合せて利用するまでの、それに関与する組織の活動、役割、情報、資源等を指すもの



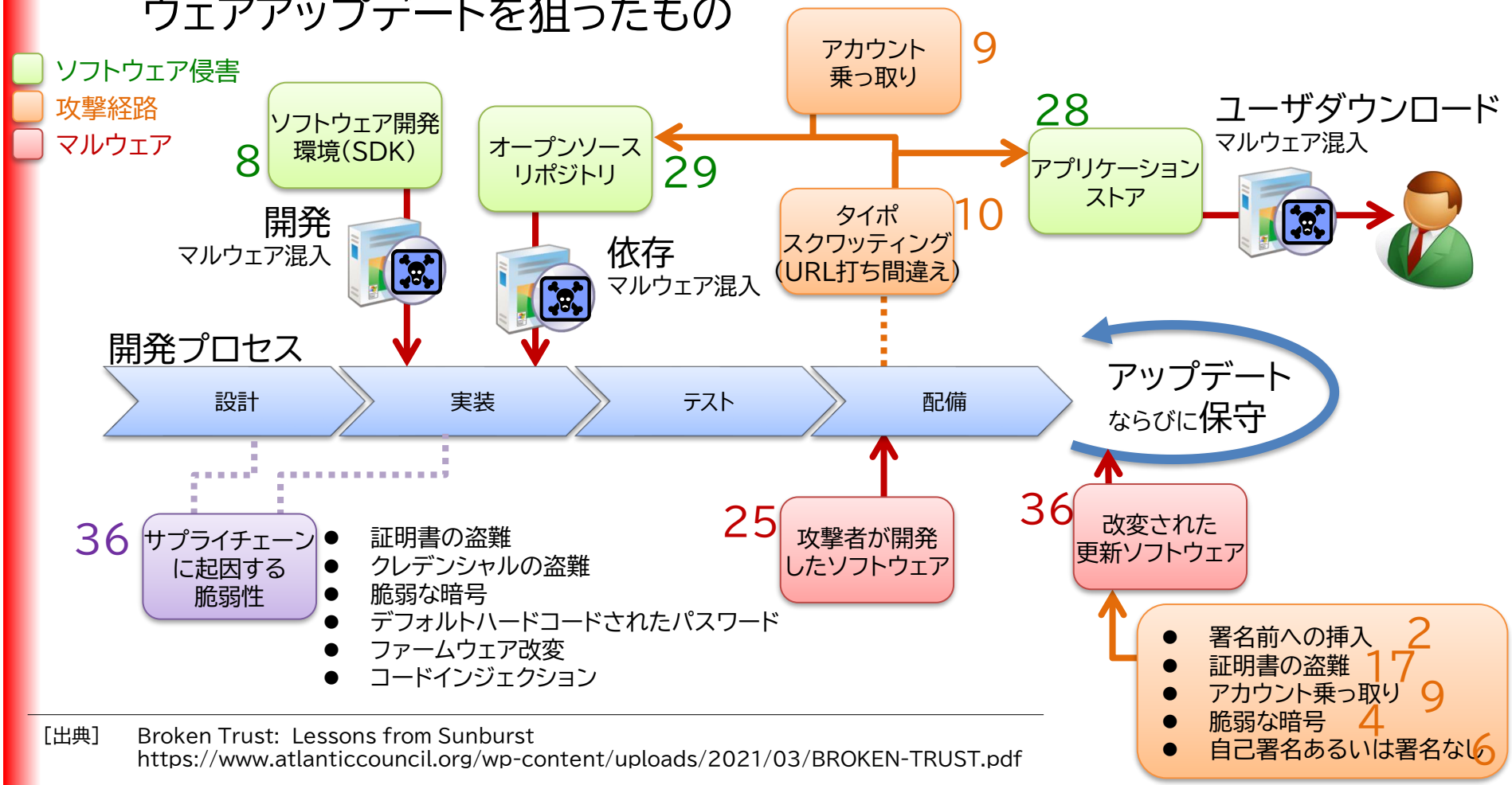
ベーシックなサプライチェーン
個々の企業の役割分担にかかわらず、ソフトウェアの企画の段階からソフトウェア製品やサービスがエンドユーザの手に届くまでの全プロセスの繋がり



［出典］　ソフトウェアサプライチェーンにおける変化と課題（2014）
https://www.ipa.go.jp/files/000040879.pdf

サプライチェーンの弱点を悪用した攻撃
攻撃活動の分析

- 2010年以降の計138件のサプライチェーン攻撃のうち、36件がソフトウェアアップデートを狙ったもの



[出典] Broken Trust: Lessons from Sunburst
https://www.atlanticcouncil.org/wp-content/uploads/2021/03/BROKEN-TRUST.pdf

サプライチェーンの弱点を悪用した攻撃
攻撃の事例

区分	概要
ソフトウェア 自動更新機能の悪用	韓国へのサイバー攻撃事案（2013年3月） 韓国の放送局や金融機関で情報システムが一斉にダウンし、大きな被害をもたらした。ファイル共有／オンラインストレージサービスソフトウェアSimDiskの自動更新機能が悪用された。
	ASUS事案（2018年6月～11月） 数十万台のASUS端末がマルウェアに感染した。ソフトウェアアップデートツールASUS Live Update Utilityが悪用された。
	SolarWinds事案（2019年9月～2020年12月） 少なくとも1万8000の政府および民間ネットワークに侵入されたとしている。事件が発覚したのは2020年12月だが、最初の不正アクセスは2019年9月に発生していた。ネットワーク監視ソフトウェアOrionの自動更新機能が悪用された。

［出典］ 「3万2000台が被害」 韓国サイバー攻撃の全貌
https://www.nikkei.com/article/DGXNASFK2203A_S3A320C1000000/
サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォースの検討の方向性
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/002_03_00.pdf
Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations
https://us-cert.cisa.gov/ncas/alerts/aa20-352a

サプライチェーンの弱点を悪用した攻撃
攻撃の事例

区分	概要
正規ソフトウェアへのマルウェア混入	Juniper事案(2012年～2014年) Netscreenに実装された暗号アルゴリズムの設定を変更し、VPNなどの暗号通信が盗聴可能となった状態で配布された。[コードインジェクション]
	Kingslayer(2015年3月～2016年9月) 政府、通信、金融、防衛、学術機関などで被害が発生した。イベントログ分析ツールであるAltairテクノロジ社製Evlogにマルウェアが混入された状態で配布された。[証明書の盗難]
	CCleaner事案(2017年8月～9月) PC最適化ツールCCleanerにマルウェアが混入された状態で配布され、インテルやマイクロソフトなどへの不正アクセスが発生した。

[出典] A Systematic Analysis of the Juniper Dual EC Incident
https://eprint.iacr.org/2016/376.pdf
How to Bury a Major Breach Notification
https://krebsonsecurity.com/2017/02/how-to-bury-a-major-breach-notification/
サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォースの検討の方向性
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/002_03_00.pdf

サプライチェーンの弱点を悪用した攻撃
攻撃の事例

区分	概要
開発環境への介入	日本スポーツ協会事案（2019年11月） 再委託先の開発環境（動作検証用に構築したサーバ）への不正アクセスによって、データの消失が発生した。
	メルカリ事案（2021年1月～4月） 同社が利用している外部のテストのコード網羅率ツールCodecovに対する不正アクセスによって、同社のソースコードの一部と一部顧客情報が流出した。
設計段階への介入 （情報システムへの不正アクセス）	三菱電機事案（2019年6月～7月） 中国拠点を足掛かりに国内拠点へ侵入され、防衛省の指定した「注意情報」にあたる情報流出の可能性が確認された。

［出典］　国民体育大会参加者データおよび公認スポーツ指導者データの消失について
https://www.japan-sports.or.jp/news/tabid92.html?itemid=4065
「Codecov」への第三者からの不正アクセスによる当社への影響および一部顧客情報等の流出について
https://about.mercari.com/press/news/articles/20210521_incident_report/
不正アクセスによる個人情報と企業機密の流出可能性について（第3報）
https://www.mitsubishielectric.co.jp/news/2020/0212-b.pdf

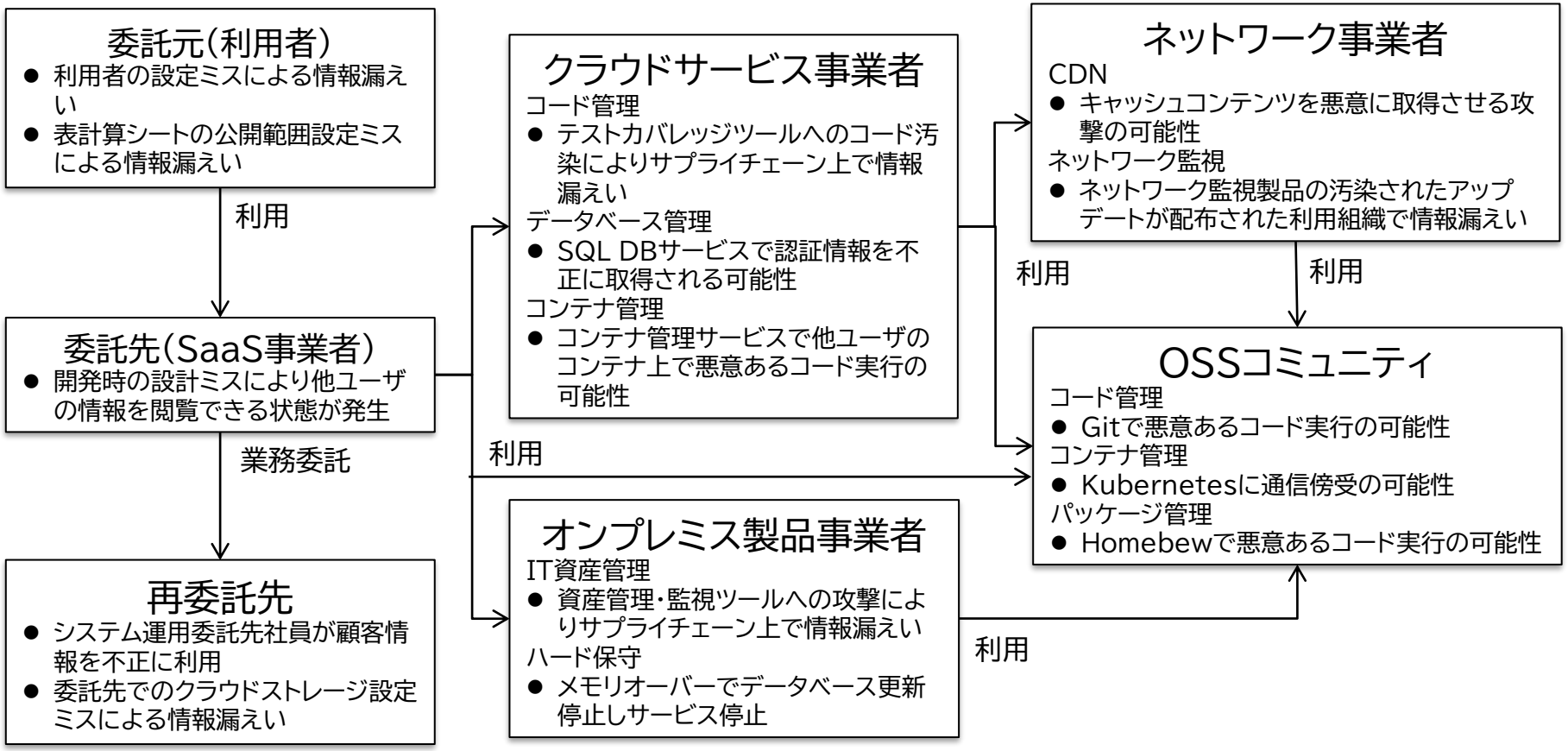
サプライチェーンの弱点を悪用した攻撃
事故の事例

区分	概要
設計や実装の不備	ボーイング737 MAX墜落事故(2019年) 墜落事故が相次いだ737 MAXのソフトウェアMCAS: Maneuvering Characteristics Augmentation System(操縦特性向上システム)の改修が完了したと発表した。
保守の不備	自治体向けクラウドの停止(2019年12月) 日本電子計算の自治体向けクラウド(Jip-Base)が停止し、47自治体などのシステムが一斉にダウンし、業務や住民サービスに影響が出た。ストレージ機器のファームウエア不具合が原因だが、バックアップ機能にも問題があり15%のデータがクラウド上から消失した。

［出典］ 737 MAX、MCASのソフトウェア改修完了
https://www.aviationwire.jp/archives/173037
自治体専用IaaSサービス「Jip-Base」の障害について(続報)
https://www.jip.co.jp/news/20191206/

サプライチェーンの弱点を悪用した攻撃
リスク所在の分析

- SaaSに係るITサプライチェーン上のリスク所在(調査範囲を対象)



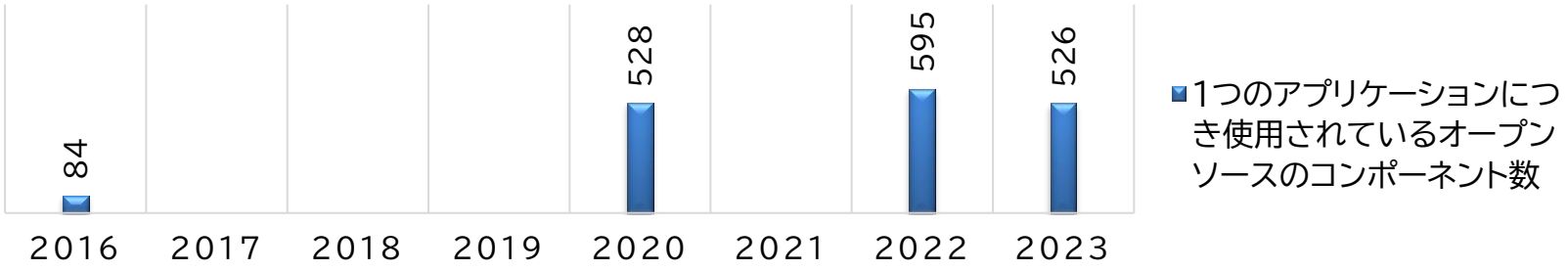
[出典] クラウドサービスのサプライチェーンリスクマネジメント調査
https://www.ipa.go.jp/security/fy2021/reports/scrm/index-cloud.html

トピック[2]

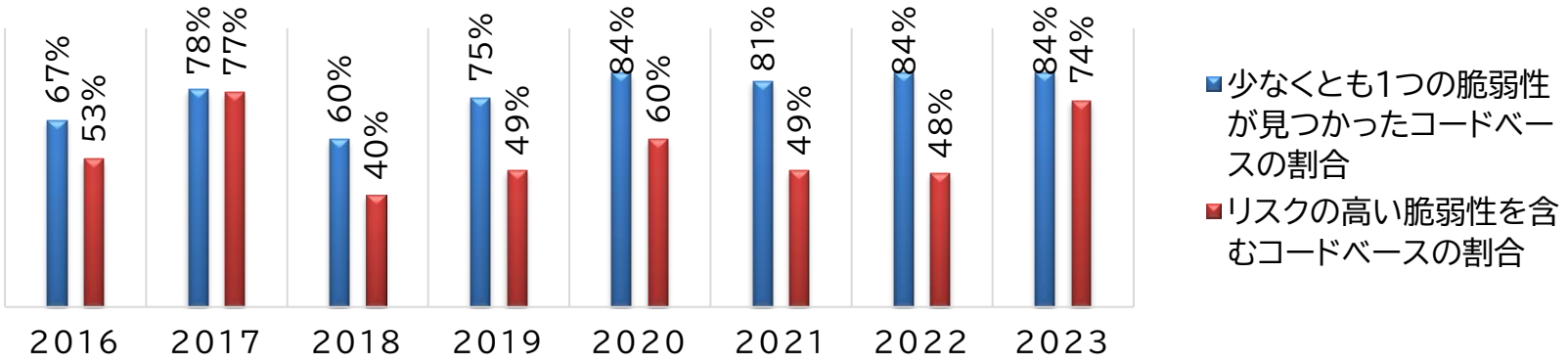
ソフトウェア部品表
SBOM
Software Bill of Materials

ソフトウェア部品表
品質の見える化

- アプリケーション内でのオープンソース使用の傾向



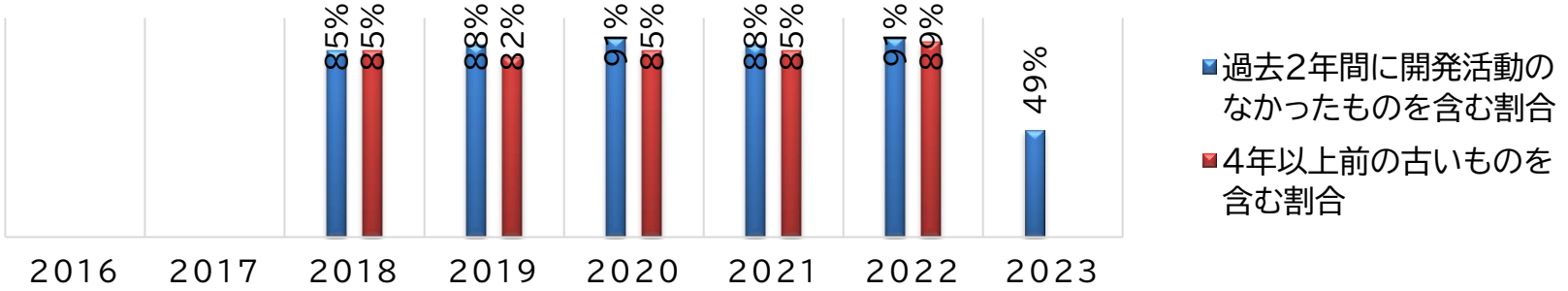
- 脆弱性を包含している傾向
  - 少なくとも1つの脆弱性が見つかったコードベースの割合
  - リスクの高い脆弱性を含むコードベースの割合



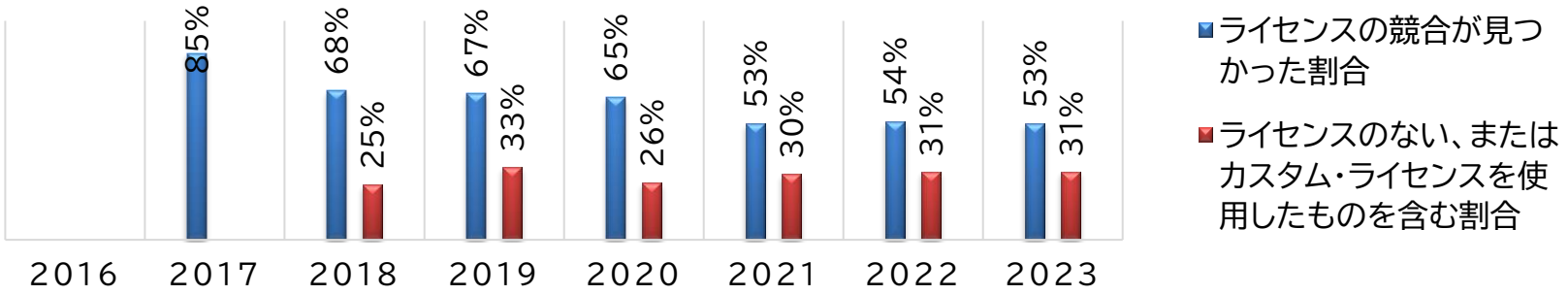
[出典] 2024 Open Source Security and Risk Analysis Report
https://www.synopsys.com/software-integrity/resources/analyst-reports/open-source-security-risk-analysis.html

ソフトウェア部品表
品質の見える化

- 保守の状況
  - 過去2年間に開発活動のなかったコンポーネントを含む割合
  - 4年以上前の古いコンポーネントを含む割合

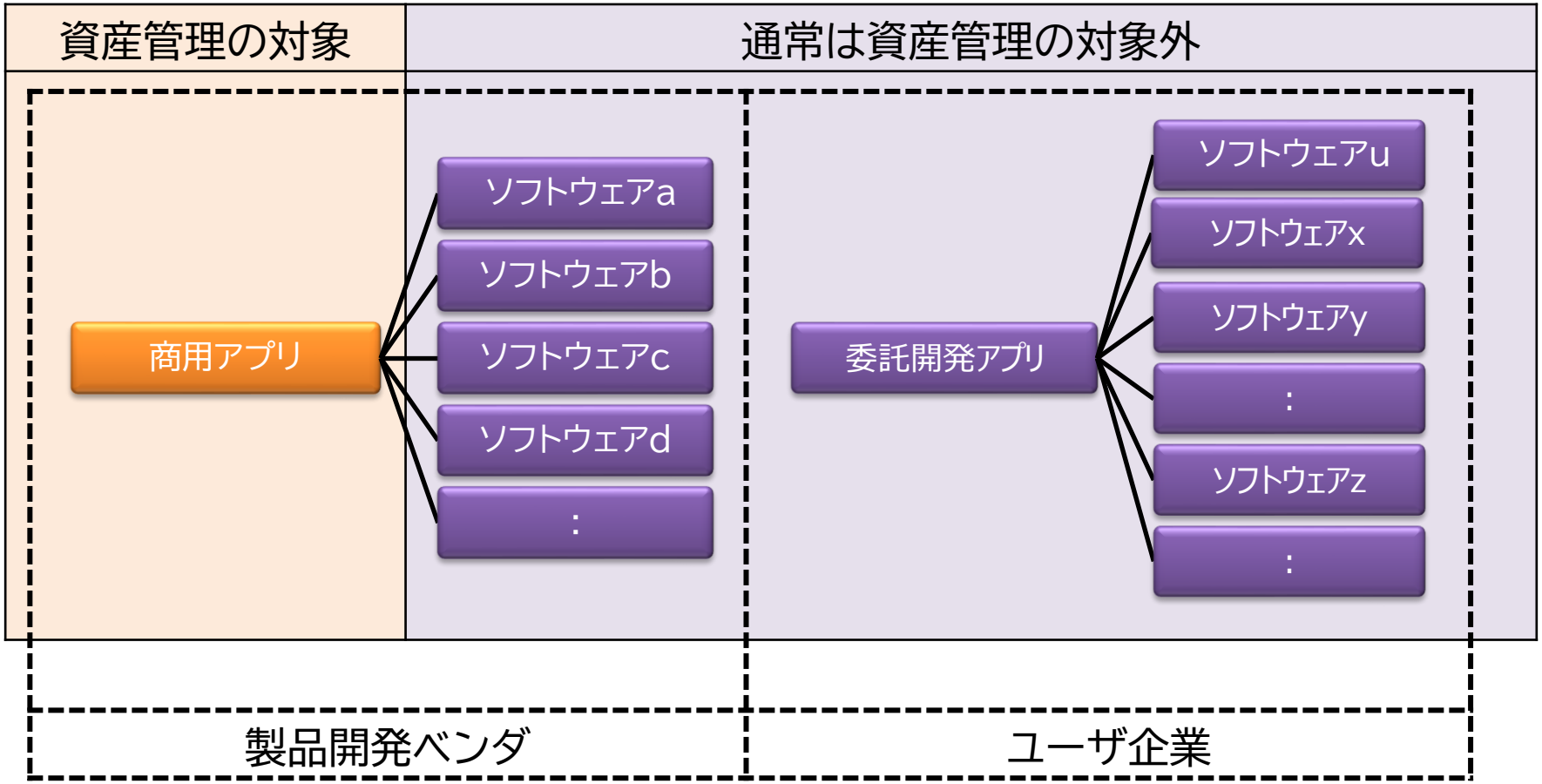


- ライセンスに関する傾向
  - ライセンスの競合が見つかった割合
  - ライセンスのない or カスタム・ライセンスを使用したものを含む割合



ソフトウェア部品表
品質の見える化

- ソフトウェアの依存関係とIT資産管理



ソフトウェア部品表
米国での取組み

- SBOM(Software Bill of Materials、ソフトウェア部品表)
  - ソフトウェアを構成する各コンポーネントを誰が作り、何が含まれ、どのような構成(依存関係)となっているか等をリスト化したもの
  - ソフトウェアを構成する各コンポーネントを把握できることから、ライセンス管理や脆弱性対応への活用を期待

- 経緯

2018年　7月	NTIA(商務省電気通信情報局)、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)を確保する活動を開始
2021年　5月	サイバーセキュリティに関する米国大統領令(EO 14028) ● ソフトウェアサプライチェーンのセキュリティを強化するガイダンスの発行を指示 ● ガイドラインには、購入者へのSBOMの提供(直接提供、公開Webサイトに公開)を明示
2021年　7月	NTIA(米国商務省電気通信情報局)、SBOMの「最小要素」を公開

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

ソフトウェア部品表
米国での取組み

- 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。

項目	内容
E-BOM (設計BOM)	開発・設計段階での部品構成情報に併せて部品の仕様、図面などの設計情報、技術情報などを管理
M-BOM (製造BOM)	製造する際に必要な部品や原材料の情報および製造工程(内製・外製)とその工程順序情報を管理し、生産計画や生産指示、調達、工程管理に使用
購買BOM	購買部門で調達のために、発注業務に必要な発注単位・数量や仕入先ごとの発注価格、代替品の情報などを管理
サービス・メンテBOM (サポートBOM)	製品サービスや保守メンテナンスに必要な部品の情報管理やメンテナンス実績に基づいたその時点のBOM管理

ソフトウェア部品表
米国での取組み

- 加工食品の表示の具体例
  - 表示の方式等
    表示は、容器包装を開かないでも容易に見ることができるように当該容器包装の見やすい箇所に表示します。など
  - 原材料名及び添加物
    使用した原材料は、添加物以外の原材料と添加物を明確に区分し、それぞれに占める重量の割合の多いものから順に記載します。など

名称	マカロニサラダ
原材料名	マカロニ（小麦を含む、イタリア製造）、マヨネーズ（卵を含む）、きゅうり、にんじん、玉ねぎ、ハム（豚肉を含む）、食塩
添加物	調味料（アミノ酸）、リン酸塩（Na）、酸化防止剤（V.C）、カゼインNa（乳・大豆由来）、発色剤（亜硝酸Na）
内容量	２００g
消費期限	令和２年〇月〇日
保存方法	要冷蔵（１０℃以下で保存）
製造者	〇〇食品株式会社 新潟市中央区紫竹山３－３－１１

［出典］　食品表示法による表示について（新法に基づく表記）
https://www.city.niigata.lg.jp/smph/iryo/shoku/shokueigyo/hyoji/shyouzihou20200330.html

ソフトウェア部品表
米国での取組み

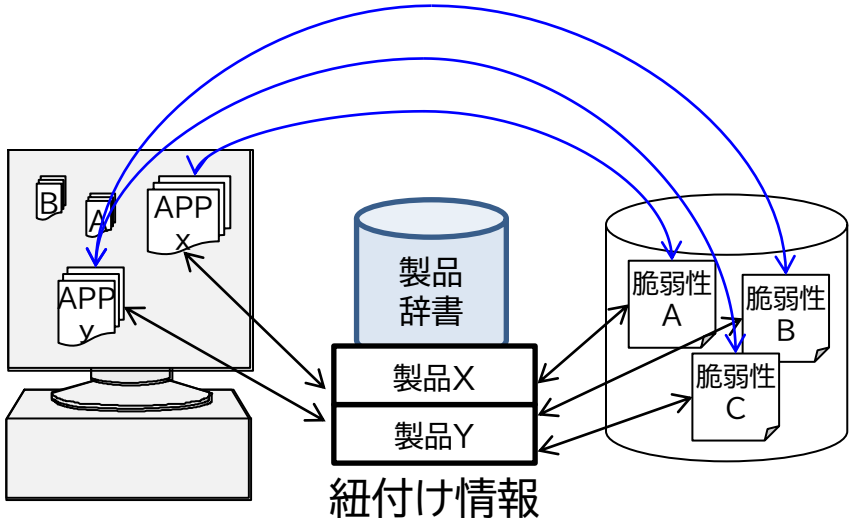
- ソフトウェアにおける具体例
  - ソフトウェア部品表(SBOM)
    ソフトウェアを構成するコンポーネントを明示することで、ソフトウェアの透明性(Software Component Transparency)を確保できる。
    ⇒品質の見える化の一手段として有用

名称	MyJVN API
ソフトウェア部品表 (使用している 外部コンポーネントや 前提プログラム)	● オラクル JRE ● OpenSSL Project OpenSSL ● OpenBSD OpenSSH ● NTP Project NTP ● Apache Software Foundation APR-util (Apache Portable Runtime Utility library) ● pcre.org PCRE (Perl Compatible Regular Expression library) ● Apache Software Foundation Apache HTTP Server ● Apache Software Foundation Apache Tomcat ● MySQL AB MySQL
開発業者	IPAシステムインテグレーション開発

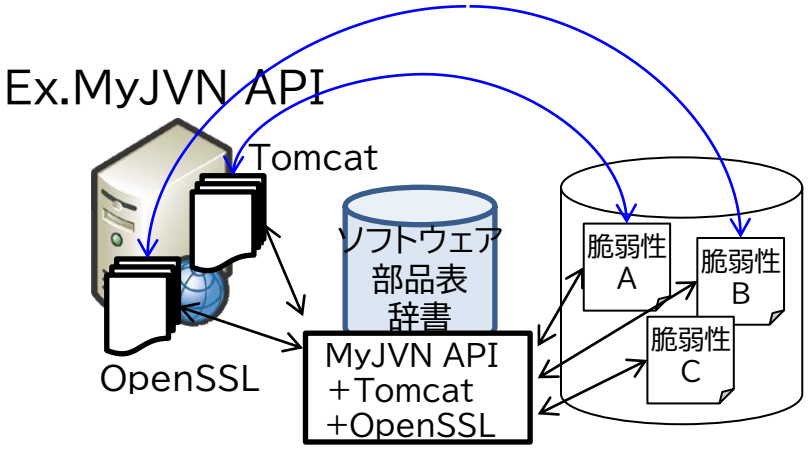
ソフトウェア部品表
米国での取組み

- ソフトウェアにおける具体例
  - ソフトウェア部品表(SBOM)
    ソフトウェアを構成するコンポーネントを明示することで、ソフトウェアの透明性(Software Component Transparency)を確保できる。

資産管理でインストールされているソフトウェアを把握できれば、脆弱性対策情報と紐付けることができる。



カスタムアプリ(SIで開発したアプリケーションなど)のソフトウェア部品表(カスタムアプリの使用コンポーネント一覧)があれば、脆弱性対策情報と紐付けることができる。



ソフトウェア部品表
米国での取組み

- 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

ソフトウェア部品表
経済産業省の取組み：ソフトウェア管理手法等検討タスクフォース

- サイバー・フィジカル一体型社会のセキュリティのための対策フレームワーク(CPSF)を具体化していく上での課題を解決するタスクフォースのひとつ

［出典］　サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/index.html

ソフトウェア部品表
経済産業省の取組み：ソフトウェア管理手法等検討タスクフォース

- 成果物
  - OSS管理手法に関する事例集

OSSの利活用及びそのセキュリティ確保に向けた管理手法に関する事例集

- 企業の OSS 利活用に関する課題の観点を整理し、その観点ごとに各種事例を取りまとめており、各企業が自社の「OSS の利活用及びそのセキュリティ確保に向けた管理手法」を検討する際の参考情報を提供することで、OSS の留意点を考慮した適切な OSS 利活用を促進する。
- 2021年4月21日に公開、2022年8月に事例を拡充
- 構成
  1. 目的
  2. OSSの概要
  3. 事例の整理方法
  4. 事例（ヒアリング調査）
  5. 事例（文献調査）
  6. まとめ

［出典］　OSSの利活用及びそのセキュリティ確保に向けた管理手法に関する事例集
https://www.meti.go.jp/policy/netsecurity/wg1/ossjirei_20220801.pdf

ソフトウェア部品表
経済産業省の取組み：ソフトウェア管理手法等検討タスクフォース

- 成果物
  - SBOMの導入に関する手引

ソフトウェア管理に向けたSBOM(Software Bill of Materials)の導入に関する手引

- SBOMに関する基本的な情報を提供するとともに、企業の効率的・効果的なSBOM 導入を支援するために、SBOM導入に向けた主な実施事項及びSBOM導入に当たって認識しておくべきポイントを示す。
- 構成
  1. 背景と目的
  2. SBOM の概要
  3. SBOM 導入に関する基本指針・全体像
  4. 環境構築・体制整備フェーズにおける実施事項・認識しておくべきポイント
  5. SBOM 作成・共有フェーズにおける実施事項・認識しておくべきポイント
  6. SBOM 運用・管理フェーズにおける実施事項・認識しておくべきポイント
  7. 付録

［出典］　ソフトウェア管理に向けたSBOM(Software Bill of Materials)の導入に関する手引
https://www.meti.go.jp/press/2023/07/20230728004/20230728004.html

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 ・・・脆弱性の影響度を評価する指標

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
脆弱性に番号を割当て、一意に識別することを可能にする

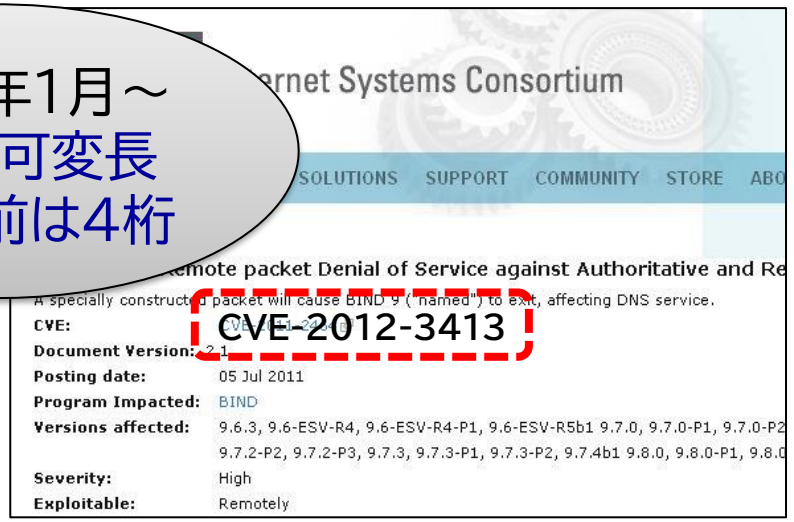
- Common Vulnerabilities and Exposures（共通脆弱性識別子）
- プログラム上のセキュリティ問題に一意の番号（CVE識別番号）を付与して管理

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

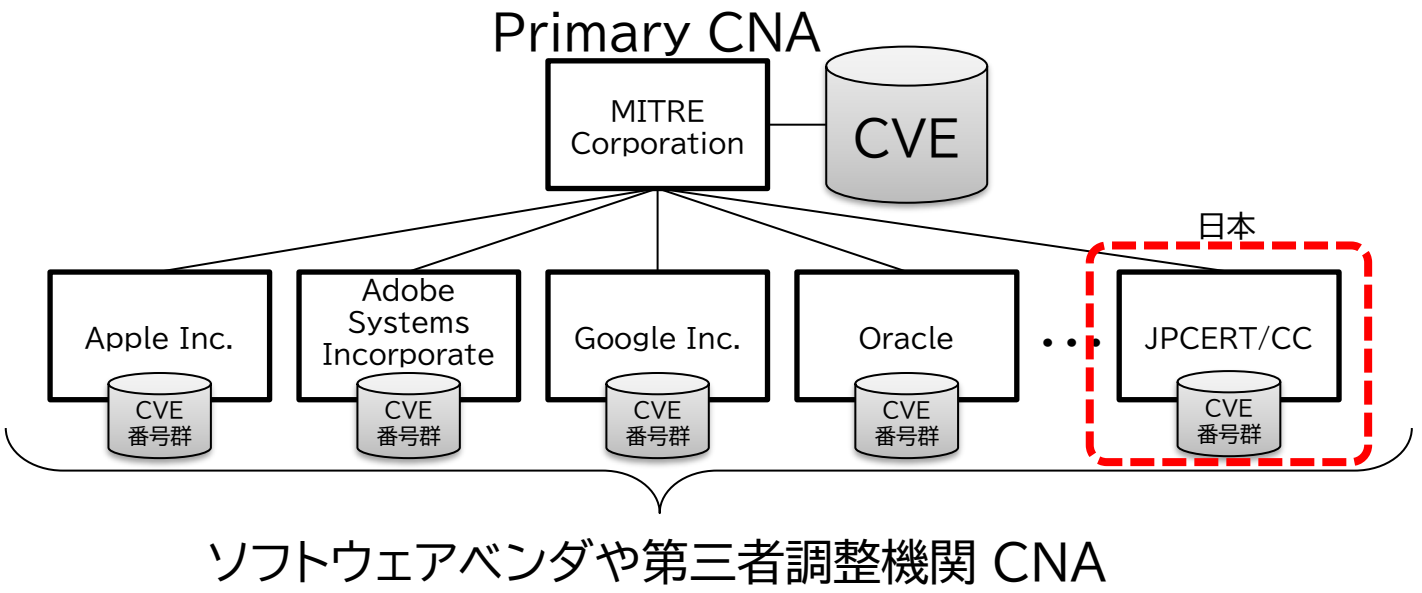


公表されている脆弱性に割り当てられた識別番号で、脆弱性を一意に特定することを可能となる

［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
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 Numbering Authority、CVE採番機関）から割り当て



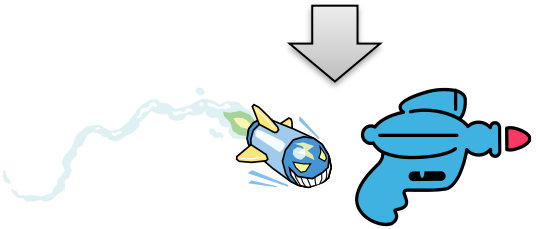
［出典］ Submit a CVE Request
https://cveform.mitre.org/
CVE Numbering Authorities (CNAs)
https://www.cve.org/ProgramOrganization/CNAs

CVSS
脆弱性の深刻度を数値で表現する

- Common Vulnerability Scoring System
  （共通脆弱性評価システム）
- 攻撃状況やシステムの重要度を加味した脆弱性の深刻度を表す評価

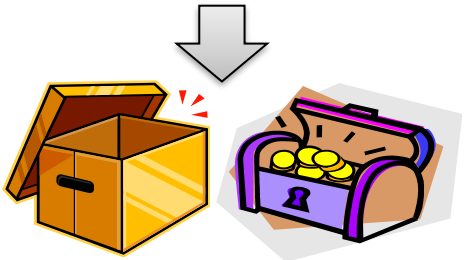
＝ 「技術的な特性」 × 「脅威の大きさ」 × 「情報資産の価値」

＝ 「基本評価基準」 × 「現状評価基準」 × 「環境評価基準」



何が引き起こされるのか？

既に攻撃されている？
対策パッチは出ている？

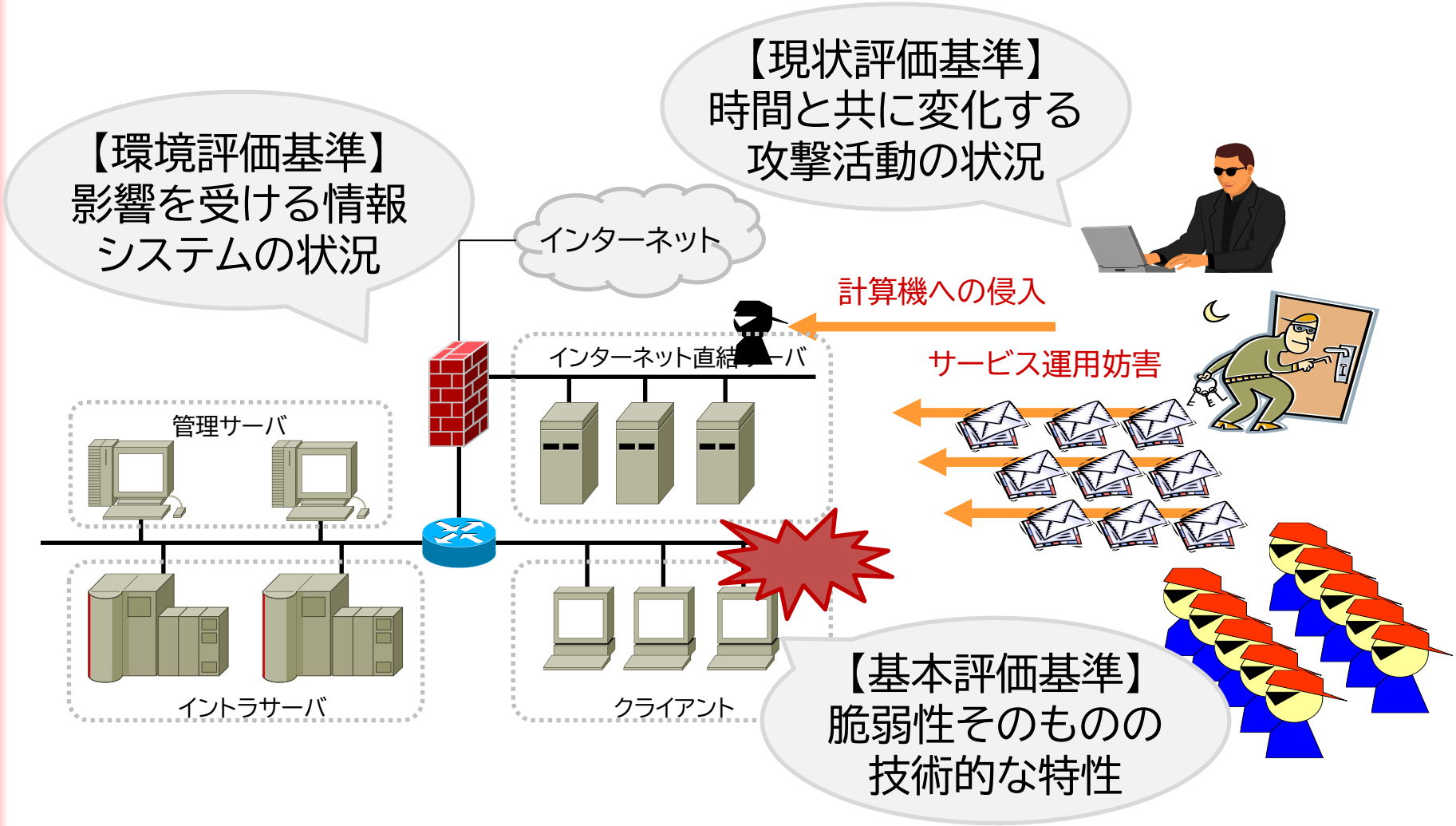


システムの重要度は？

「バッファオーバフロー（技術面で危険度高）」×「攻撃観測なし」×「内部システム」＝深刻度 低
「クロスサイトスクリプティング（技術面で危険度中）」×「攻撃観測あり」×「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/

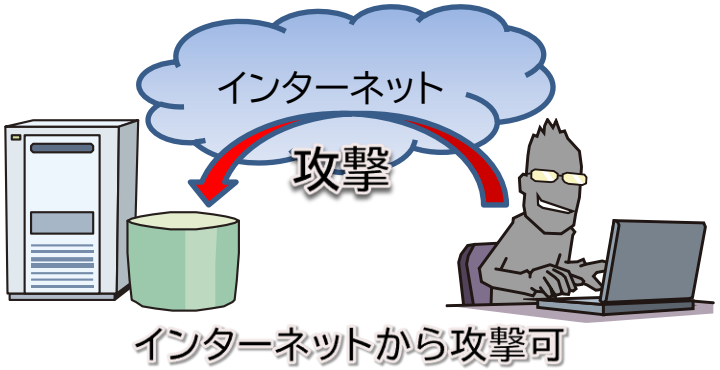
CVSS
脆弱性の深刻度を数値で表現する



CVSS
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

OR



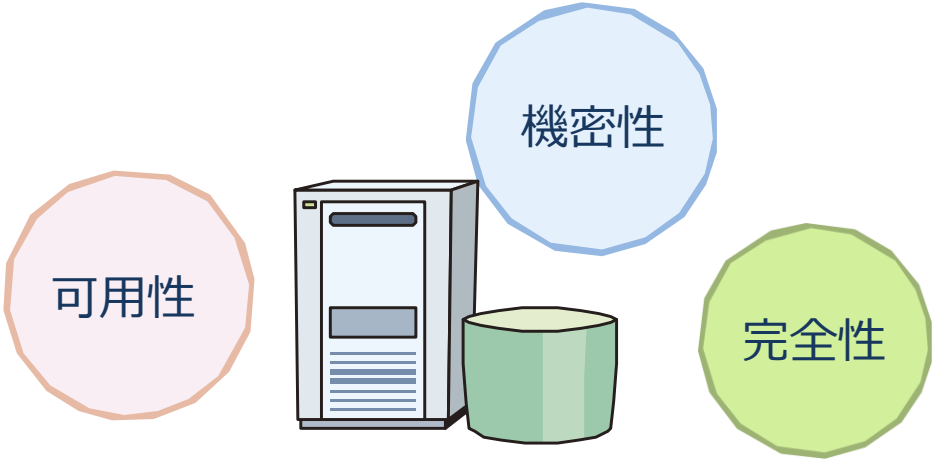
  - 攻撃による影響

CVSS
現状評価基準

- ある時点における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
環境評価基準

- そのシステムにおける問題の大きさを評価
  - CVSSv3
    - 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



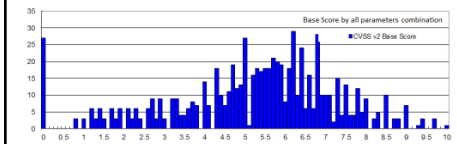
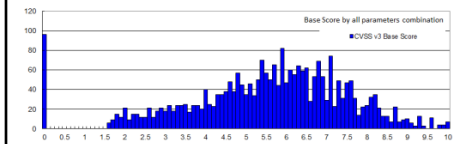
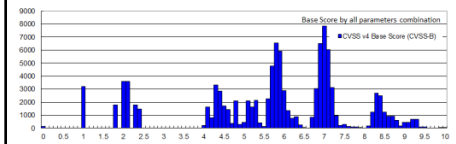
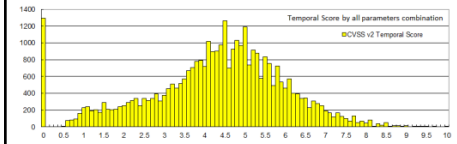
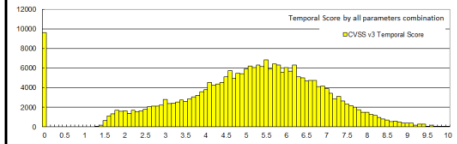
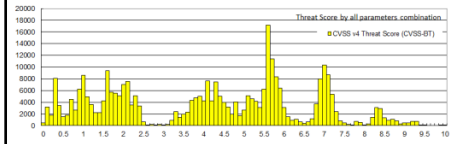
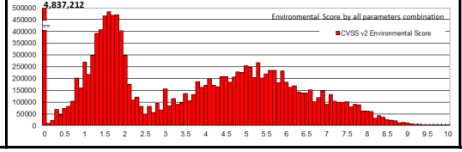
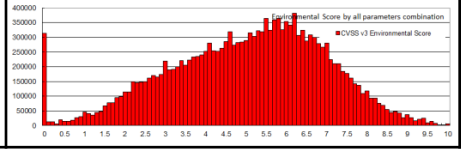
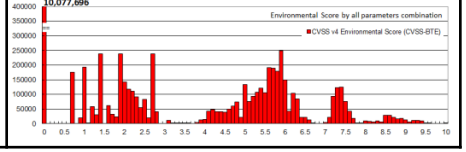
CVSS
CVSS（共通脆弱性評価システム）の開発

- 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、米国家インフラストラクチャ諮問委員会(NIAC: 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
CVSS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
CVSS 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

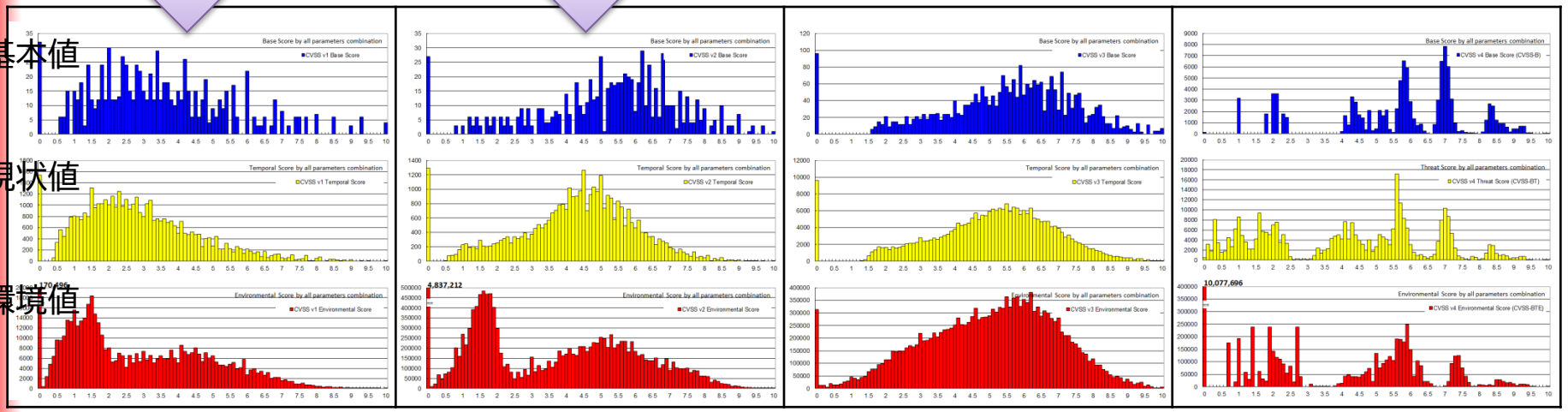
スコアの分布に
偏りがあった

スコアの分布の
偏りを是正した

基本値

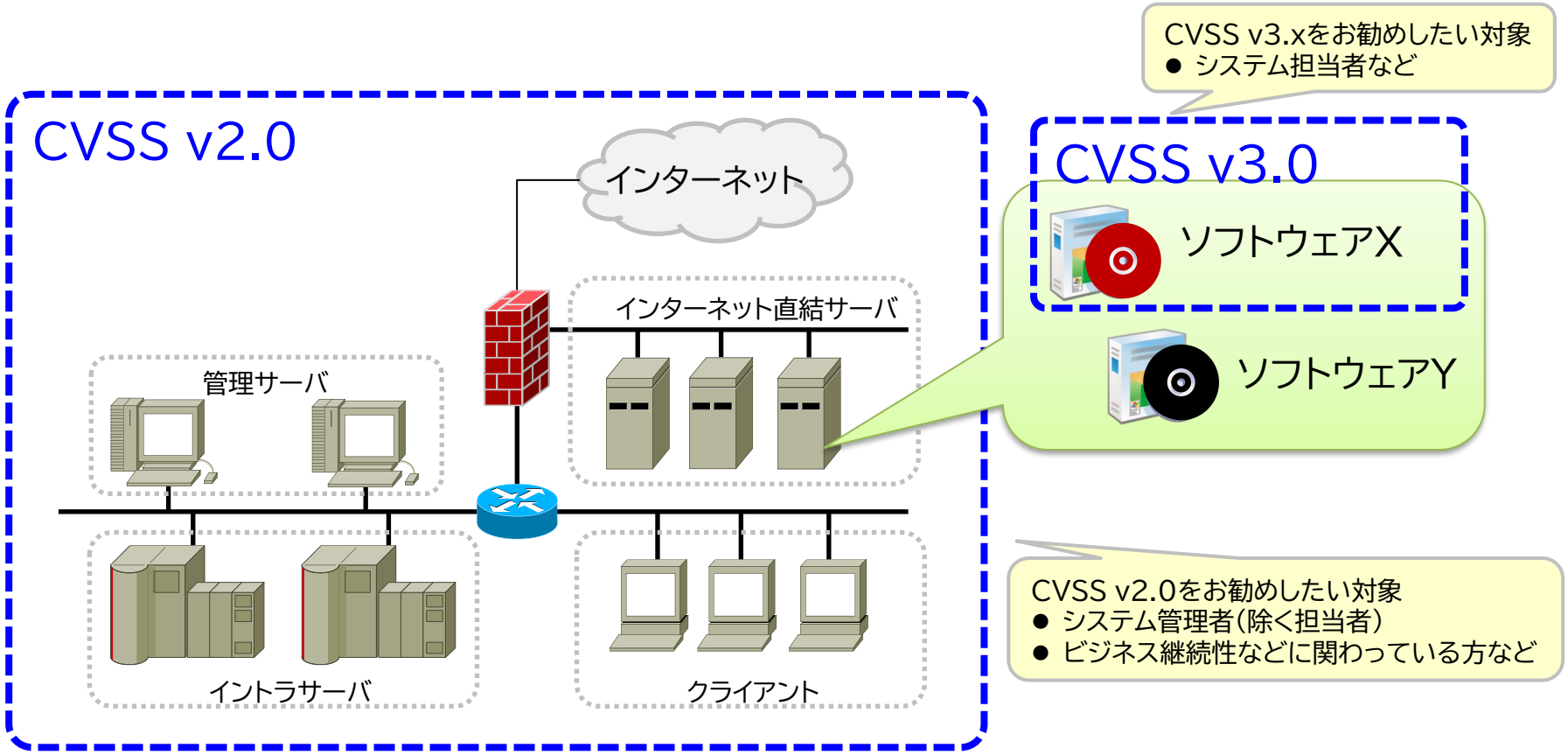
現状値

環境値



CVSS
CVSS 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
CVSS 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

攻撃者

脆弱性のあるコンポーネント

脆弱性による影響の広がりを評価
●スコープ=変更なし

脆弱性を取り巻く状況を評価
●攻撃される可能性(E)
●利用可能な対策のレベル(RL)
●脆弱性情報の信頼性(RC)

攻撃の難易度を評価
●攻撃元区分=ネットワーク
●攻撃条件の複雑さ=低
●必要な特権レベル=不要
●ユーザ関与レベル=不要

攻撃による影響を評価
●機密性への影響=高
●完全性への影響=なし
●可用性への影響=なし

セキュリティ要求度
●機密性の要求(CR)
●完全性の要求度(IR)
●可用性の要求度(AR)

CVSS環境評価値

対策前=7.5

CVSS
CVSS 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

攻撃者

脆弱性のあるコンポーネント

脆弱性による影響の広がりを再評価
●スコープ=変更なし

脆弱性を取り巻く状況を評価
●攻撃される可能性(E)
●利用可能な対策のレベル(RL)
●脆弱性情報の信頼性(RC)

攻撃の難易度を再評価
●攻撃元区分=隣接
●攻撃条件の複雑さ=低
●必要な特権レベル=不要
●ユーザ関与レベル=不要

攻撃による影響を再評価
●機密性への影響=高
●完全性への影響=なし
●可用性への影響=なし

セキュリティ要求度
●機密性の要求(CR)
●完全性の要求度(IR)
●可用性の要求度(AR)

CVSS環境評価値

対策後=6.5

CVSS
CVSS 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
CVSS 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

- ある時点における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
CVSS v3.1からv4への変更点

- その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。

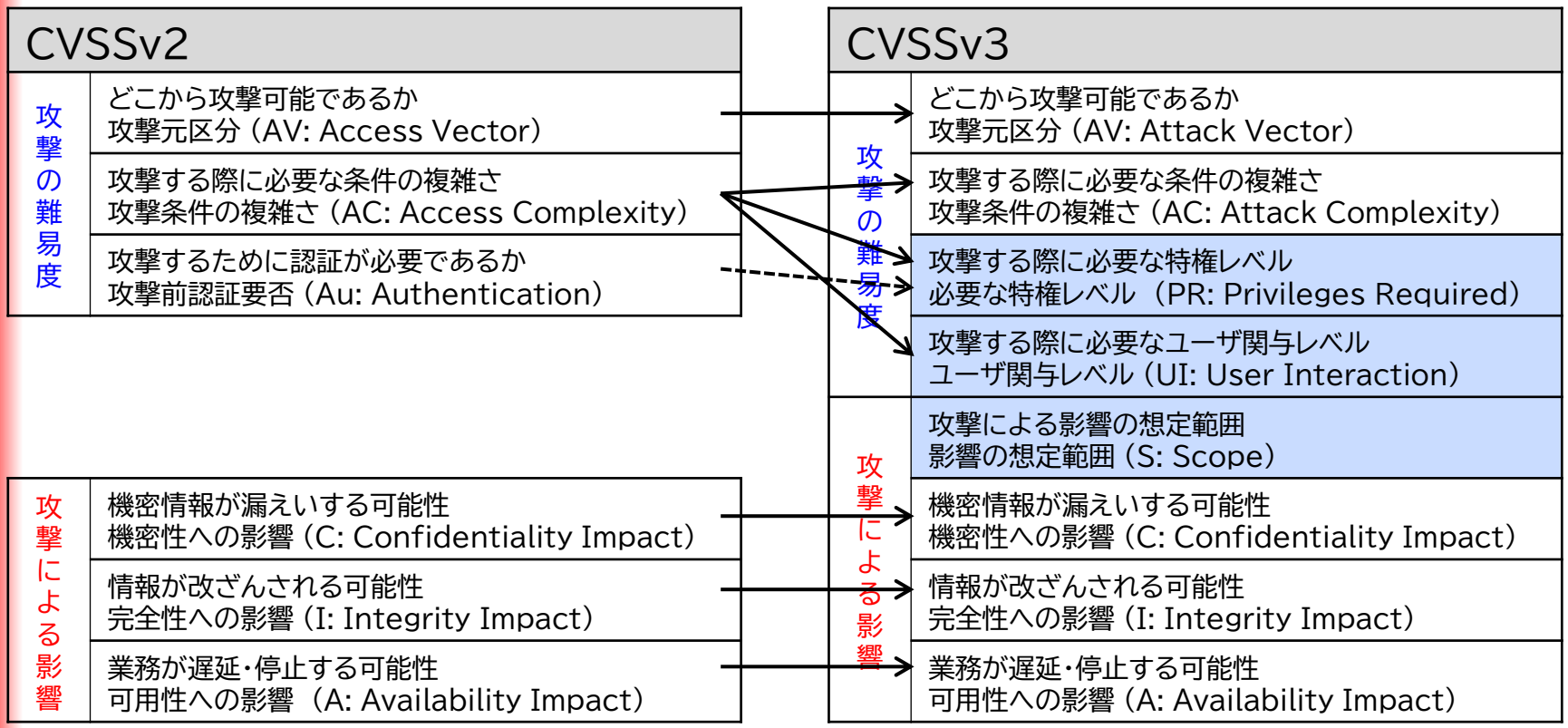
- CVSSスコア算出アプローチの変更
  - CVSS v1～v3.1：計算式から算出
  - CVSS v4：270個のスコア区分に振り分けた後、微調整して算出（MacroVectors and Interpolation）

CVSS v4.0

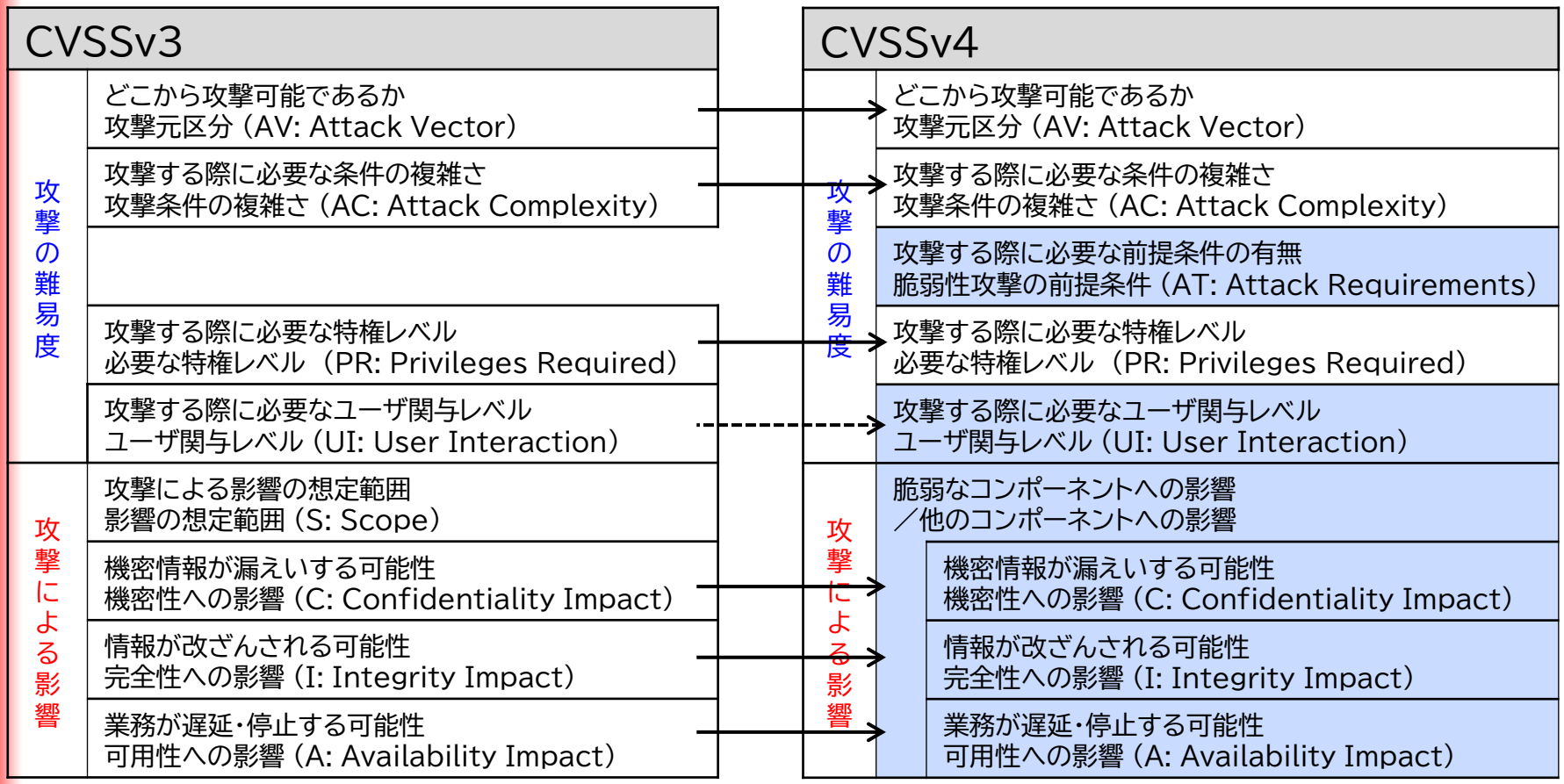
- 基本評価基準、脅威評価基準、環境評価基準、補助評価基準の4つから構成
- CVSSスコア算出に使用するのは、基本評価基準、脅威評価基準、環境評価基準の3つ

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 v4.0
基本評価基準:v2からv3への変更点



CVSS v4.0
基本評価基準：v3からv4への変更点

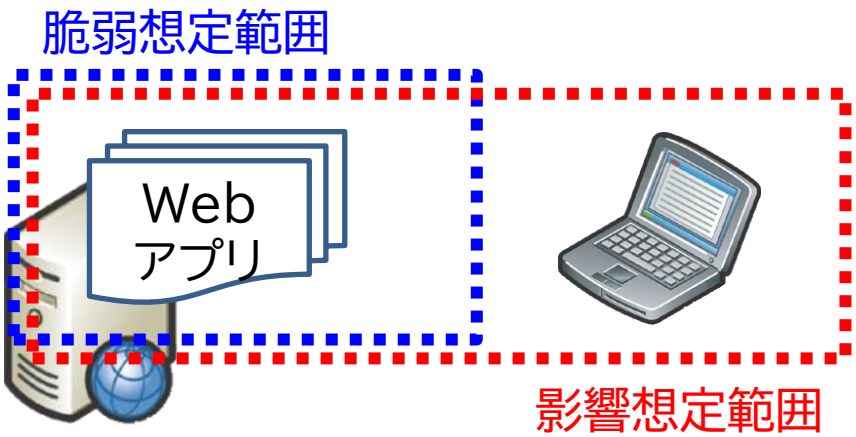


CVSS v4.0
基本評価基準:脆弱性による二次的な影響波及の表記方法

- 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

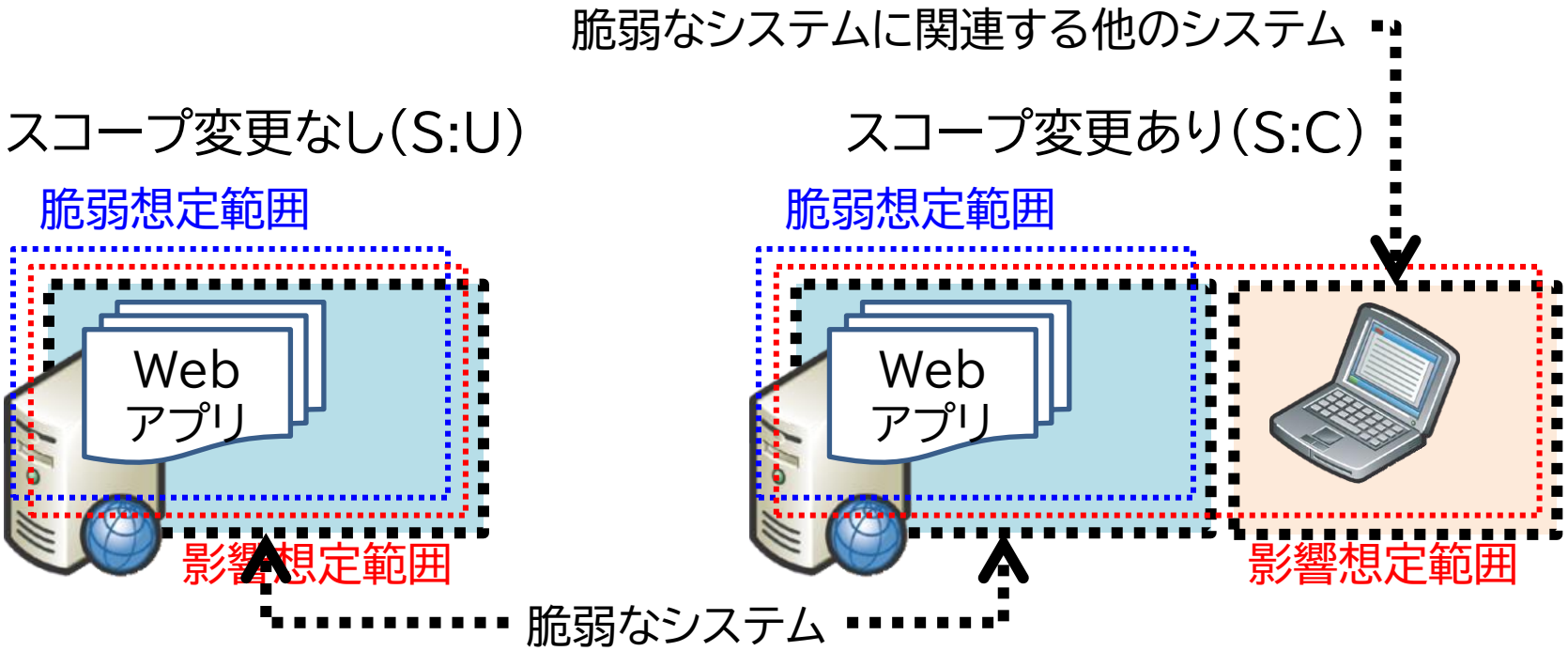
スコープ変更なし(S:U)

スコープ変更あり(S:C)



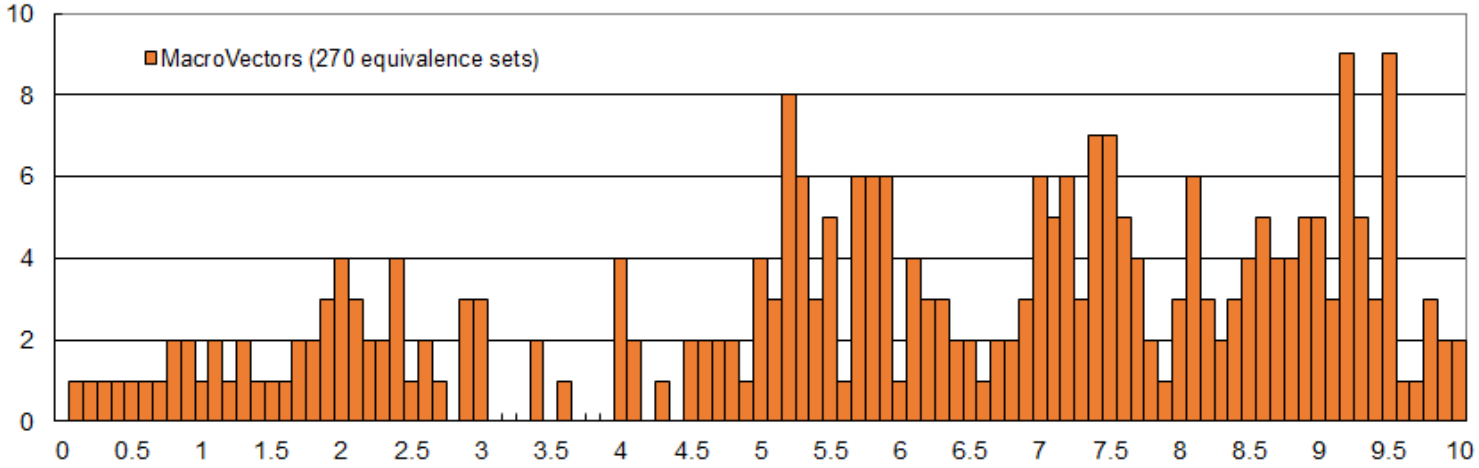
CVSS v4.0
基本評価基準：脆弱性による二次的な影響波及の表記方法

- 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



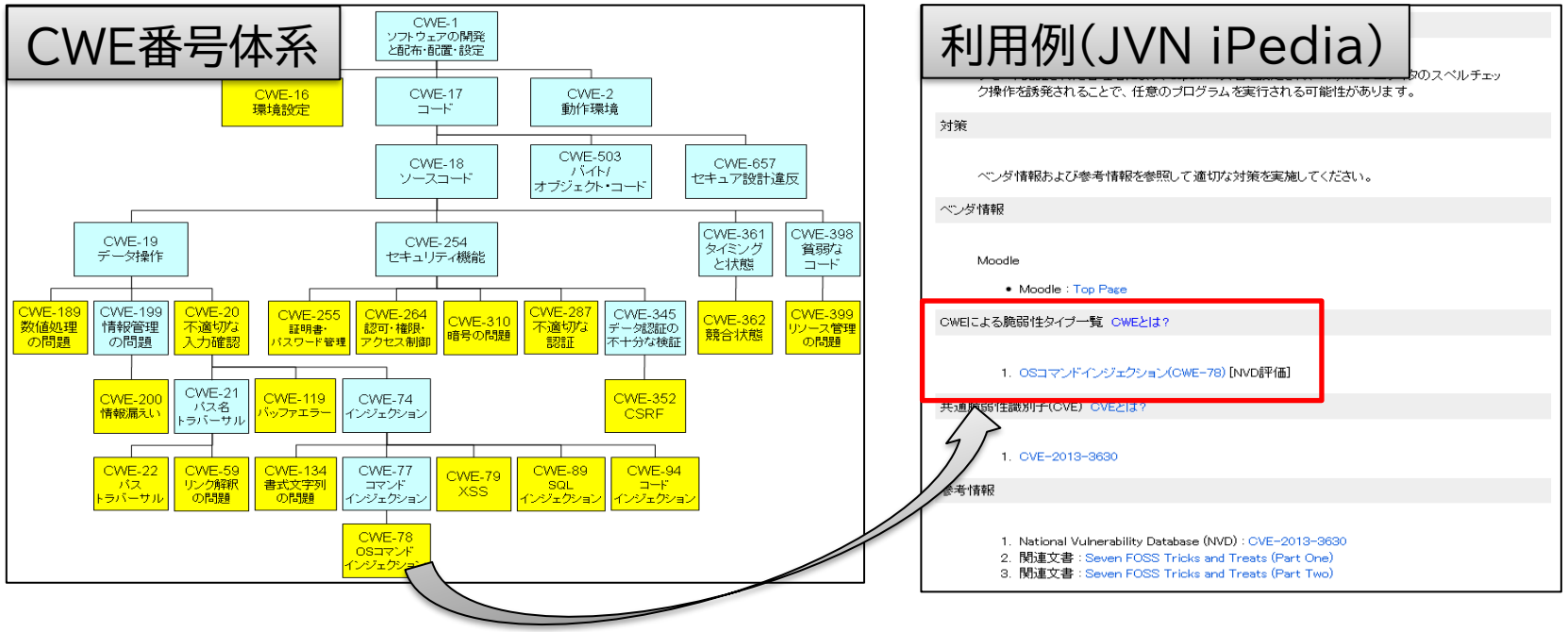
CVSS v4.0
スコアの算出方法：v4への変更点

- 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



CWE
脆弱性のタイプを体系立てて分類した指標

- Common Weakness Enumeration
  （共通脆弱性タイプ一覧）
- 脆弱性を種別毎に分類



［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
脆弱性のタイプを体系立てて分類した指標

- 主な脆弱性タイプとCWE識別子番号

ID	概要
CWE-16	環境設定
CWE-20	不適切な入力確認
CWE-22	パス・トラバーサル
CWE-59	リンク解釈の問題
CWE-78	OSコマンドインジェクション
CWE-79	クロスサイトスクリプティング
CWE-89	SQLインジェクション
CWE-94	コード・インジェクション
CWE-119	バッファエラー
CWE-134	書式文字列の問題

ID	概要
CWE-189	数値処理の問題
CWE-200	情報漏洩
CWE-255	証明書・パスワードの管理
CWE-264	認可・権限・アクセス制御
CWE-287	不適切な認証
CWE-310	暗号の問題
CWE-352	クロスサイトリクエストフォージェリ
CWE-362	競合状態
CWE-399	リソース管理の問題

CPE
製品を識別する

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

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:/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

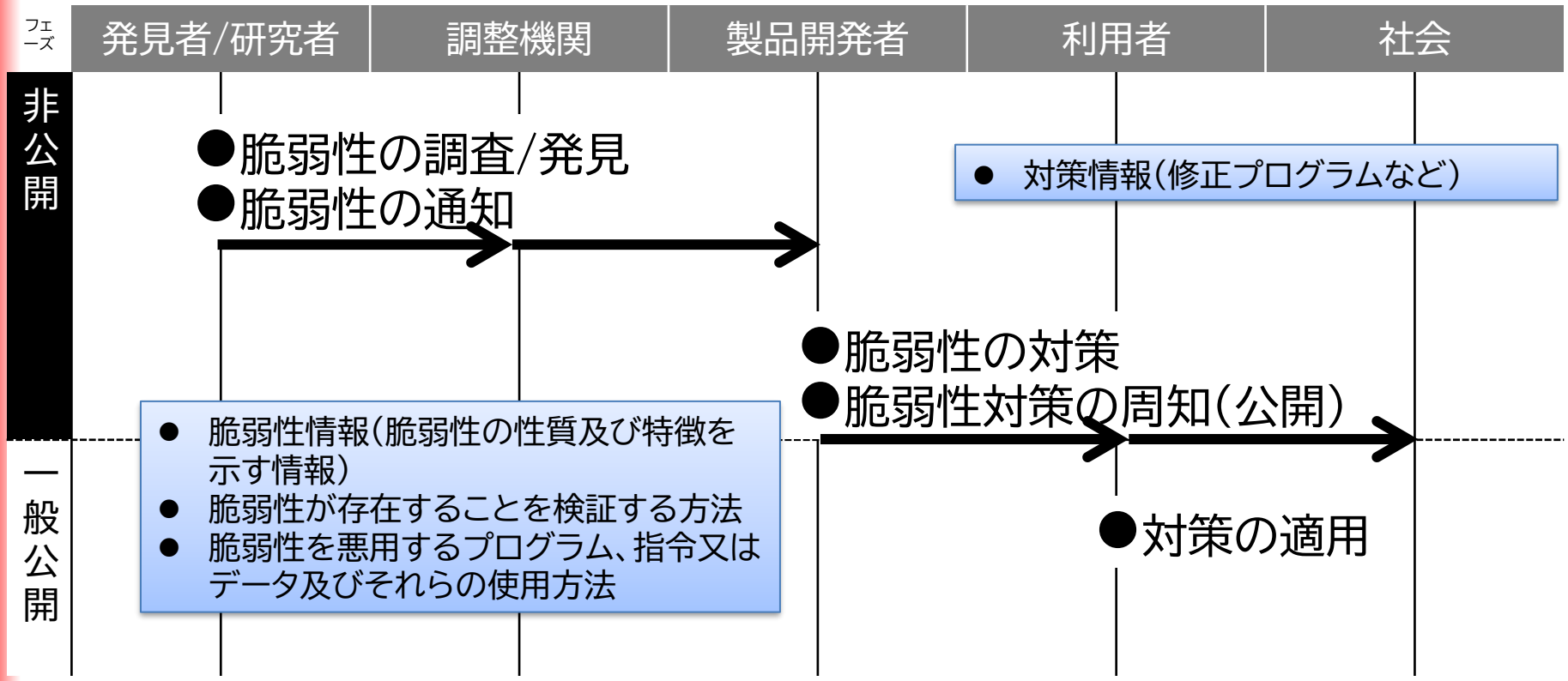
脆弱性(ぜいじゃくせい)の開示

- 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。

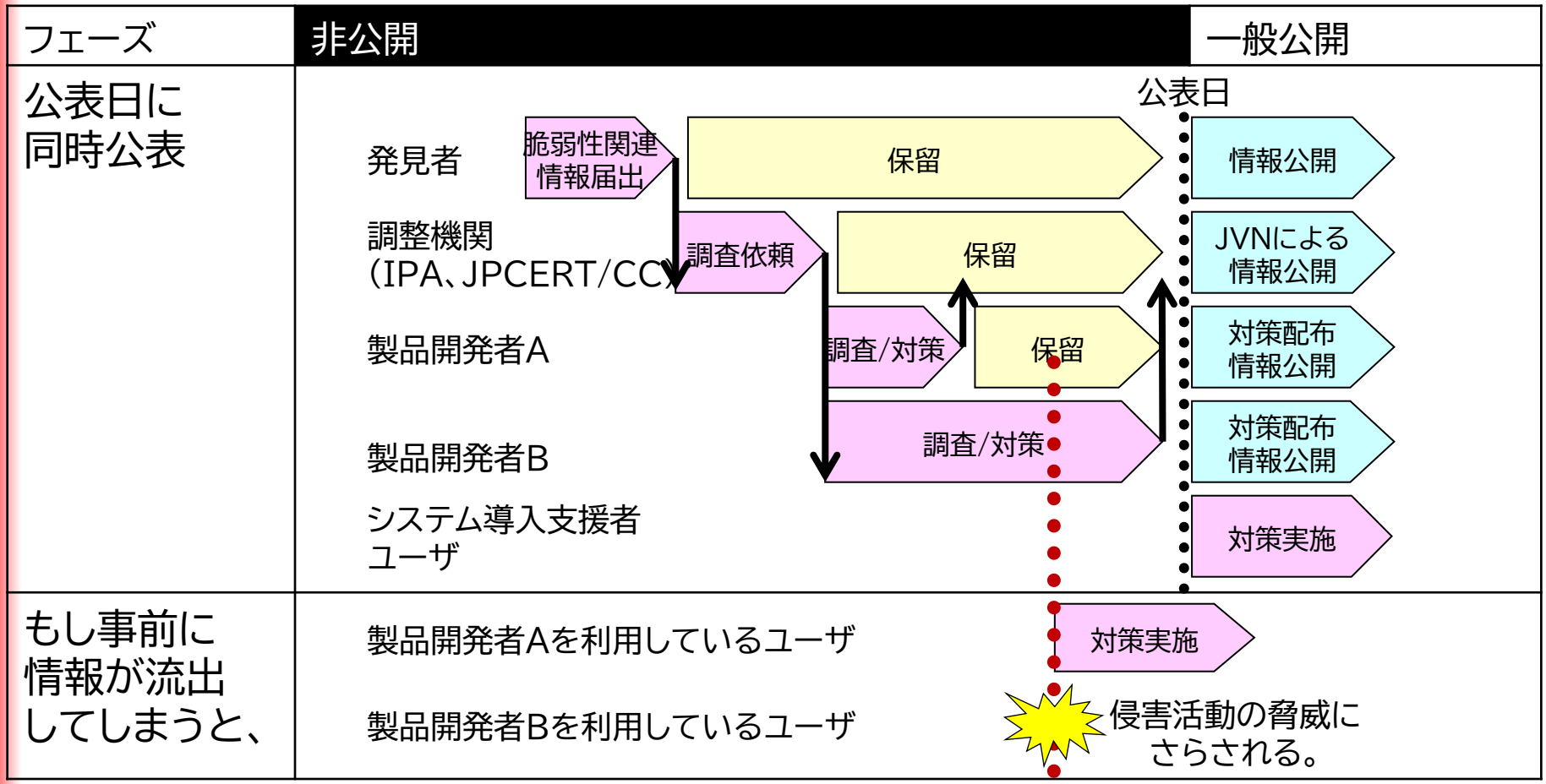
脆弱性(ぜいじゃくせい)の開示
脆弱性ハンドリングとは

- 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



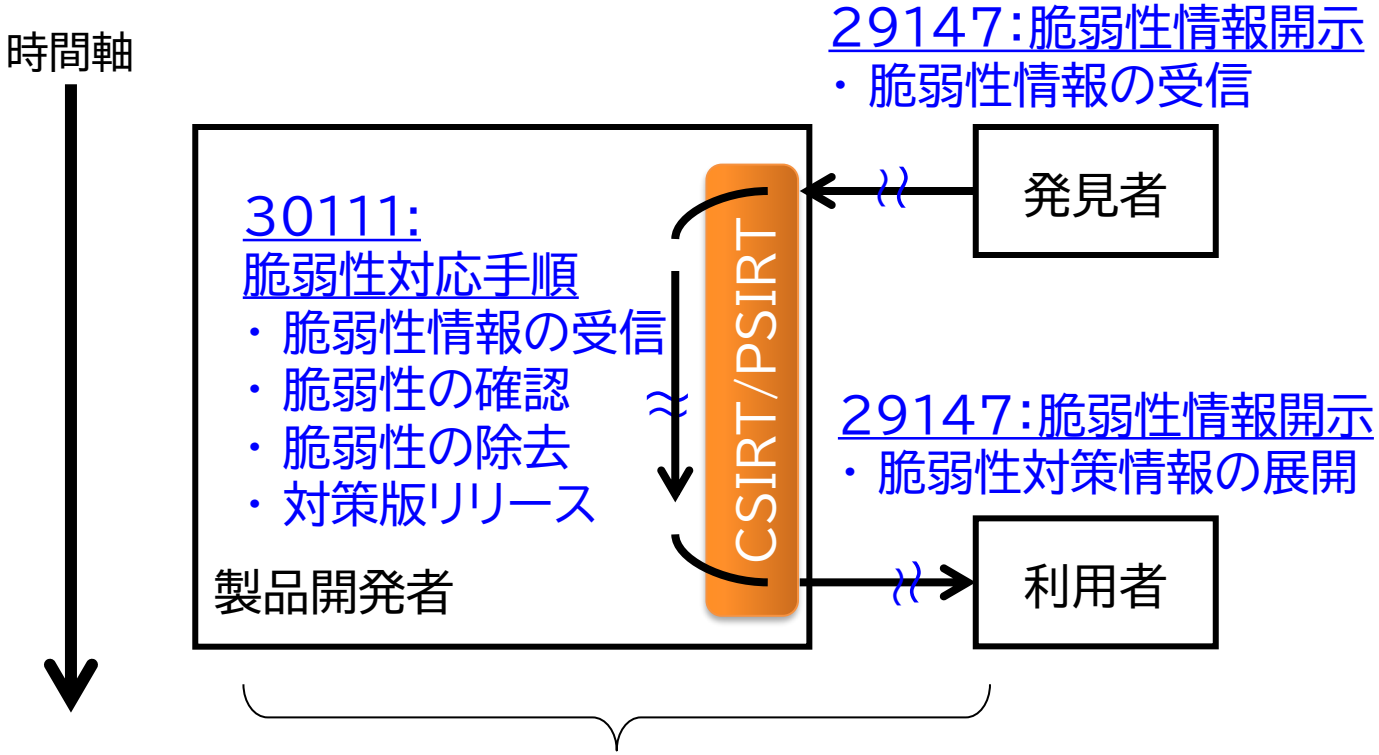
脆弱性(ぜいじゃくせい)の開示
公開日一致の原則

- 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

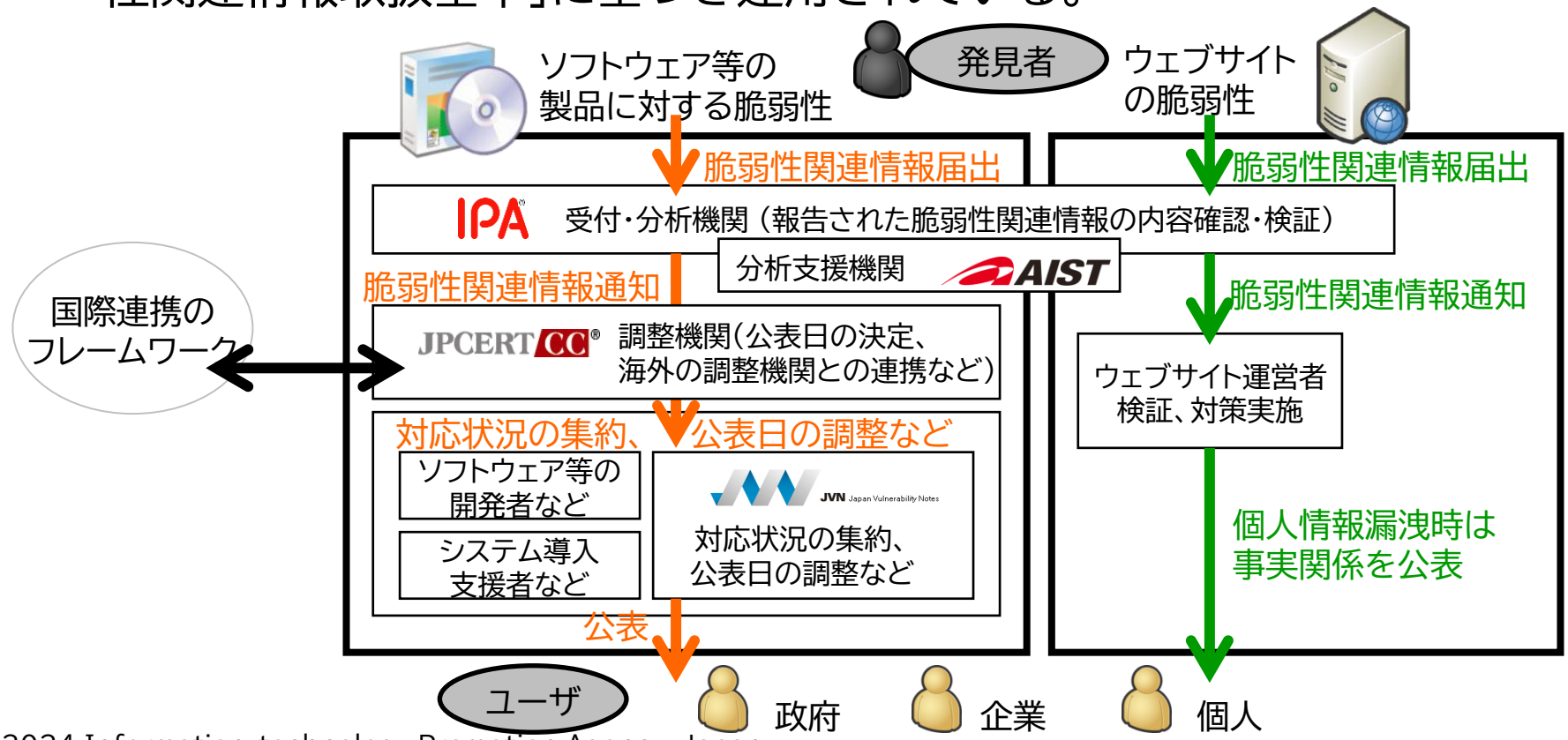
- ISO/IEC 29147、30111（2008年～2014年にかけて初版標準化）



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

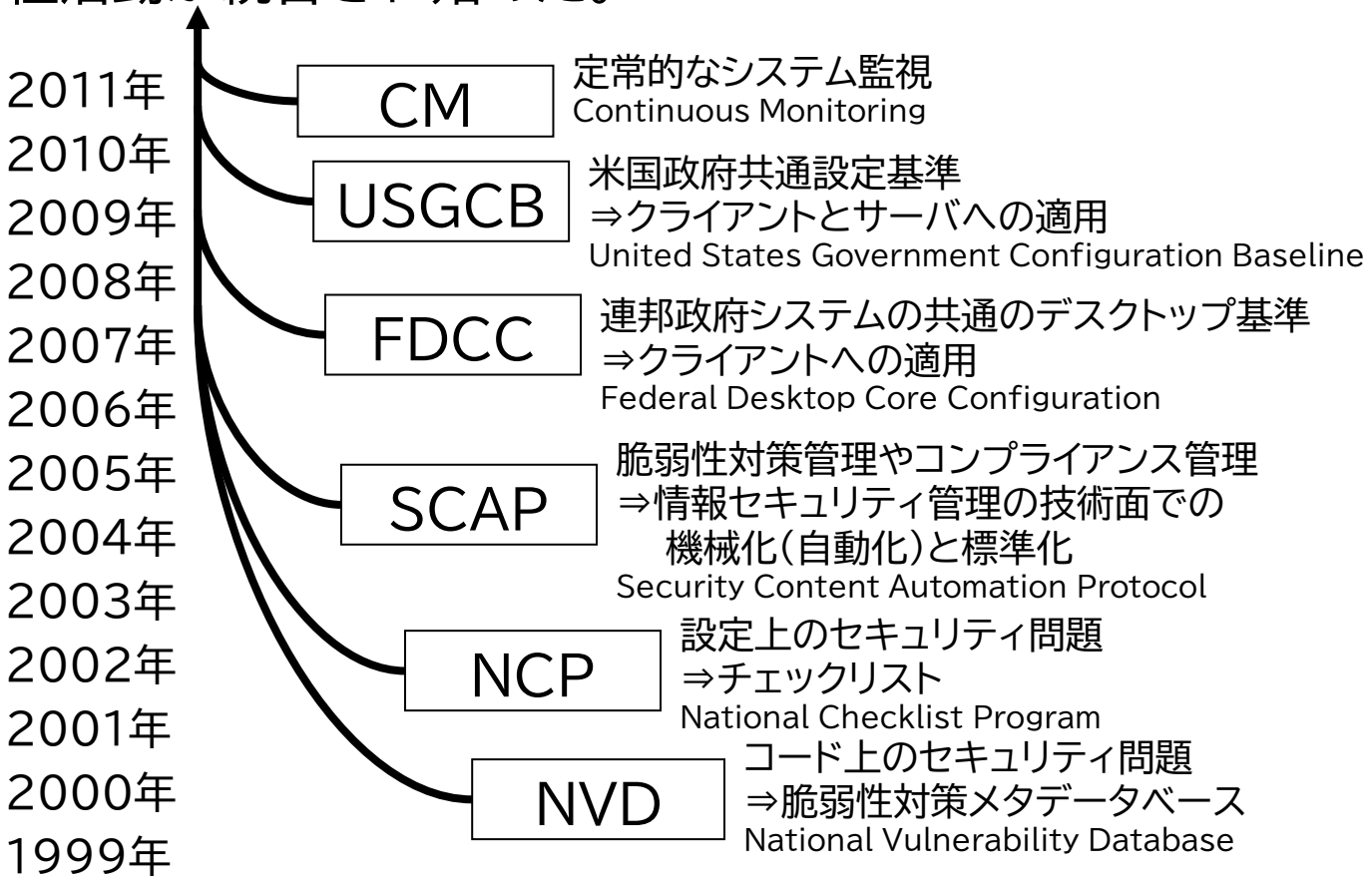
- ソフトウェア等の製品やウェブサイトに見つかった脆弱性に関する情報を受け付け、製品開発者に修正を促すフレームワーク
- 2004年7月8日施行の脆弱性関連情報の取扱い「ソフトウェア等脆弱性関連情報取扱基準」に基づき運用されている。



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(Federal Information Security Management Act:連邦情報セキュリティマネジメント法)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
セキュリティ設定共通化手順SCAP

- 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

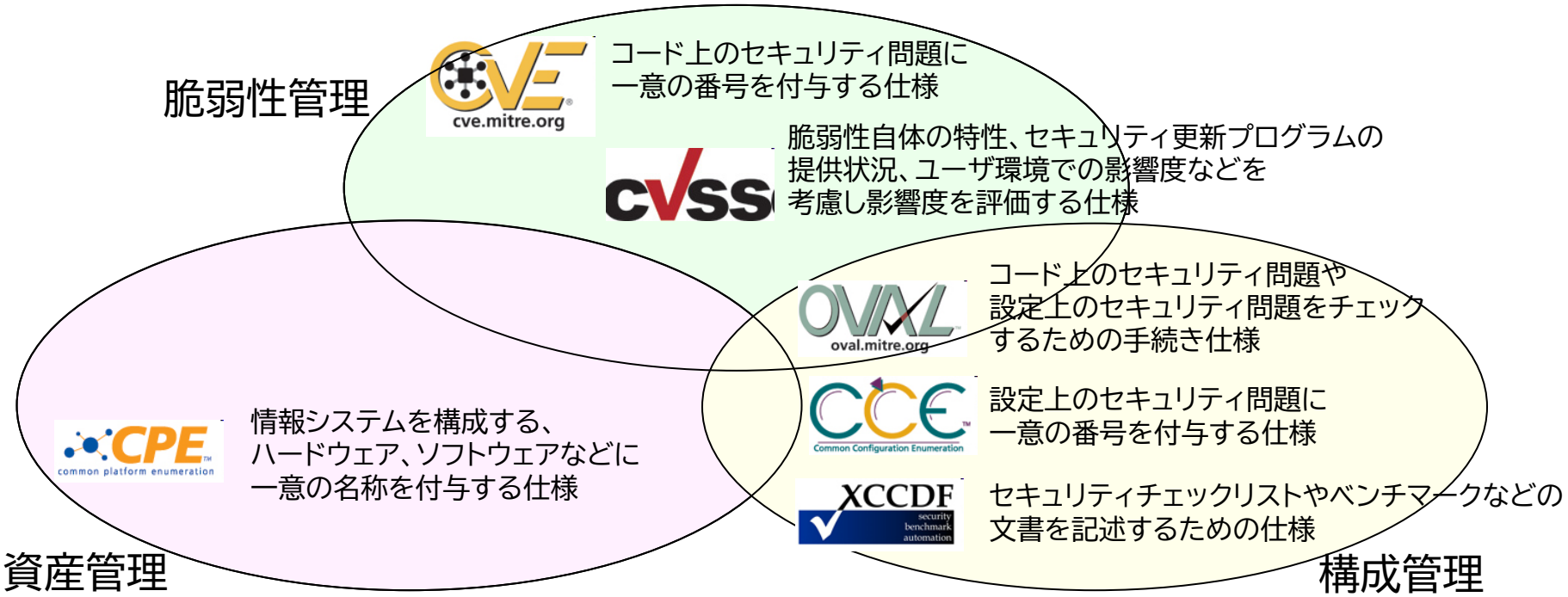
⇩

【 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
セキュリティ設定共通化手順SCAP

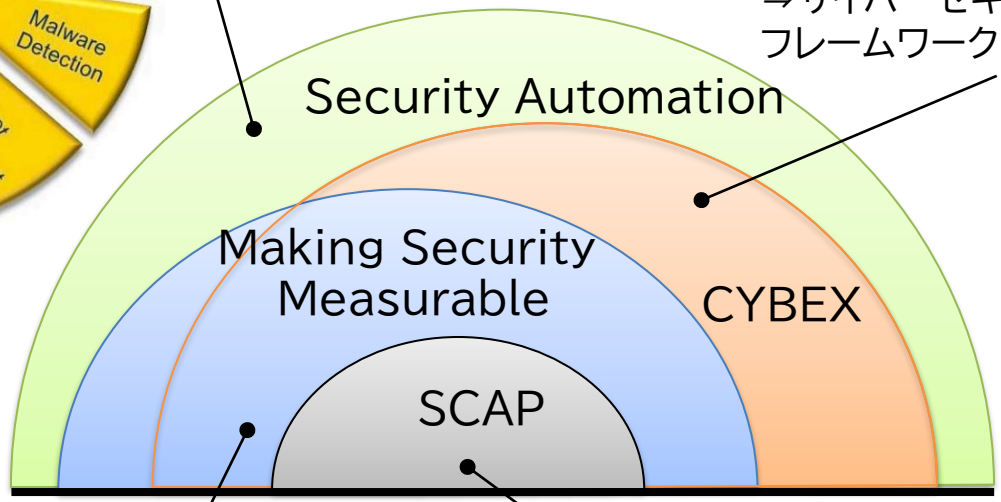
- 脆弱性管理、コンプライアンス管理の一部を機械化(自動化)することにより、情報システムに対するセキュリティ対策の負荷軽減と情報セキュリティ施策の推進の両立を目的とした6つの仕様から構成されている。



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、783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

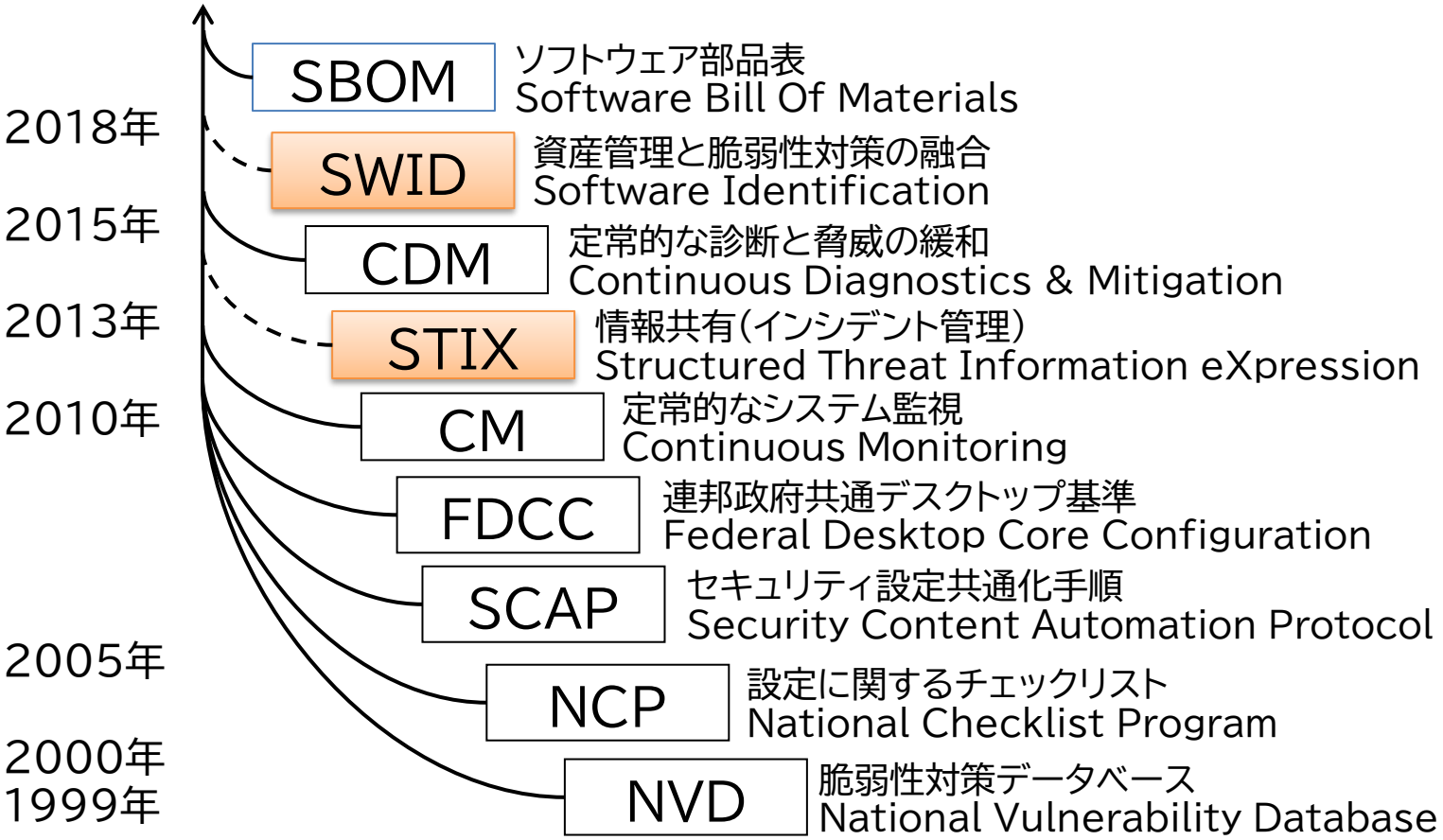
自動化(機械化)処理基盤の潮流
セキュリティ設定共通化手順SCAP

- 脆弱性対策を進める3つの視点(仕様、コード、設定)

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.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

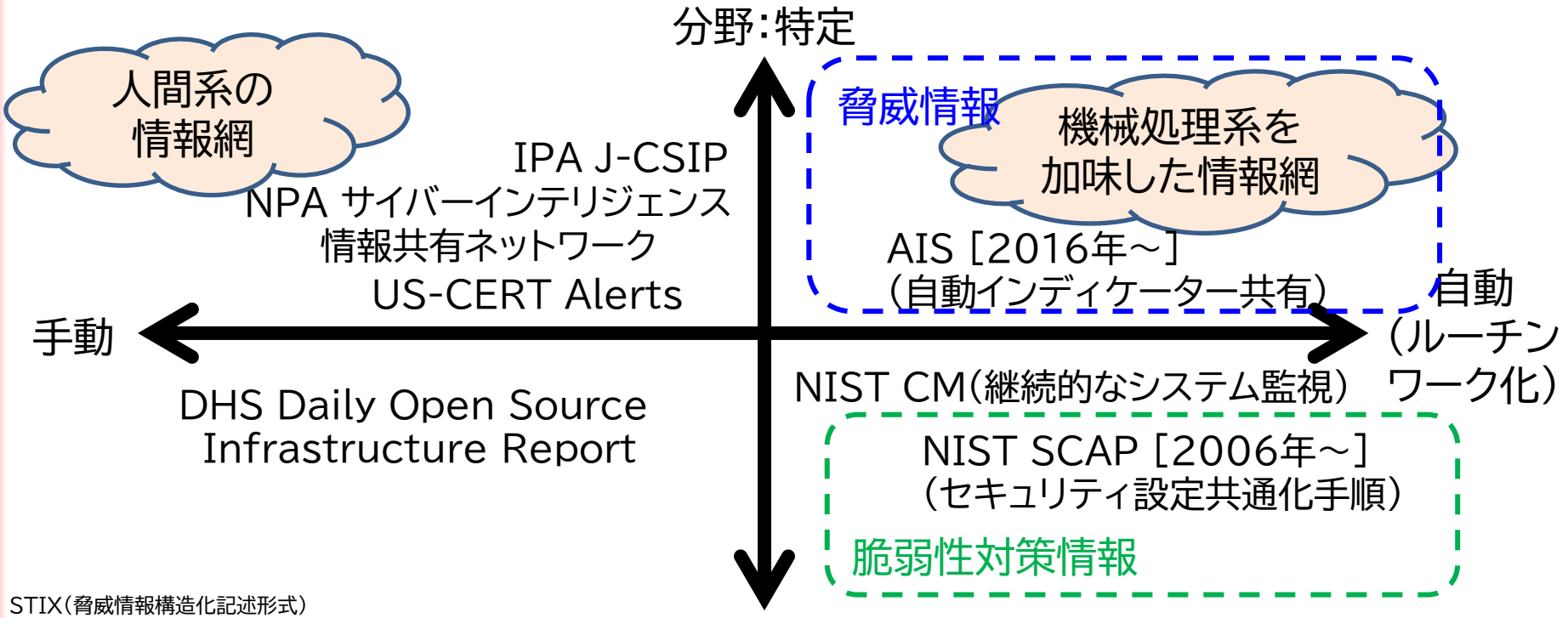
自動化(機械化)処理基盤の潮流
新たな動き

- 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

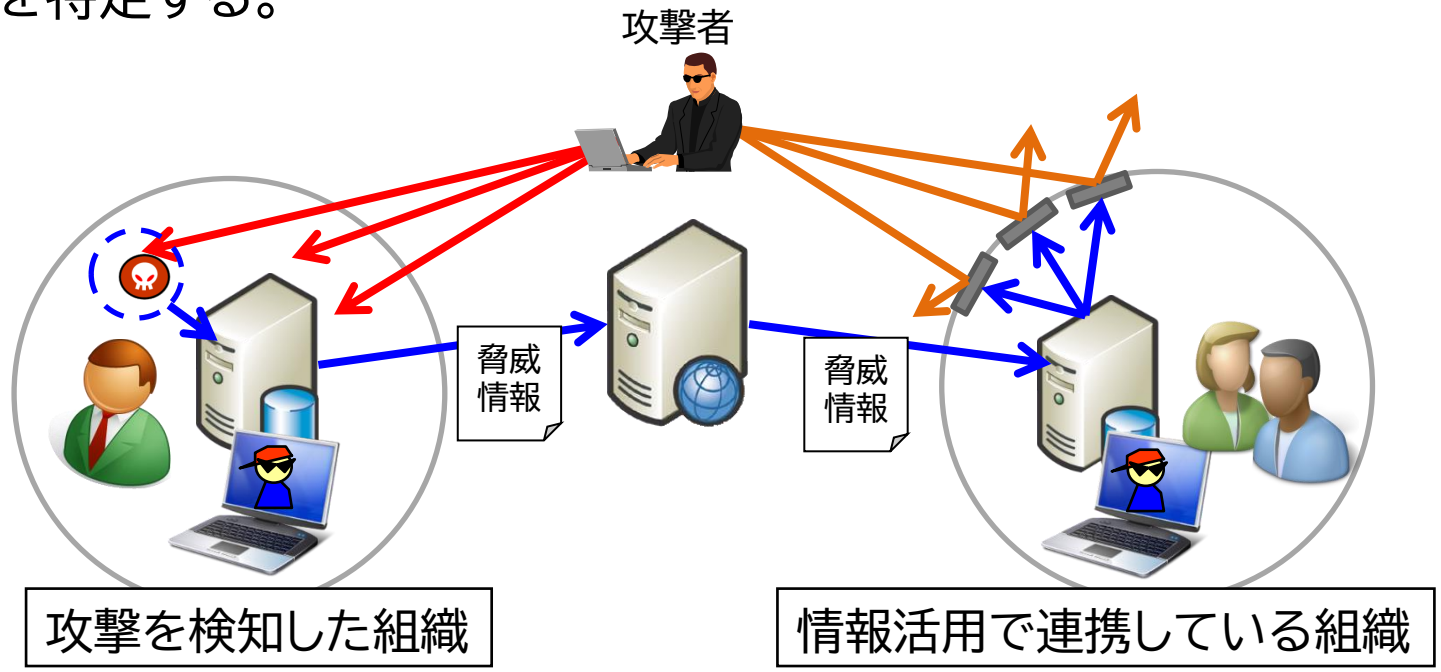
- 2012年頃から機械処理系を想定した大量の脅威情報が流通する仕組みが検討され始める。



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)

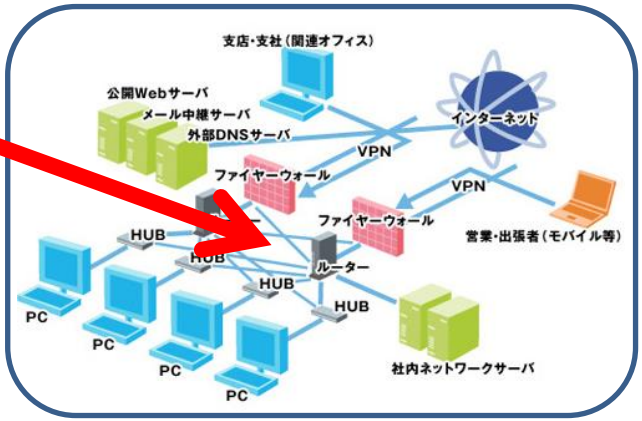
STIX™

CybOX™

ダウンロードサーバ
C&Cサーバ

攻撃者

観測事象
(Observable;攻撃によって観測された事象)



①標的型攻撃メール

③外部通信

②感染

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）

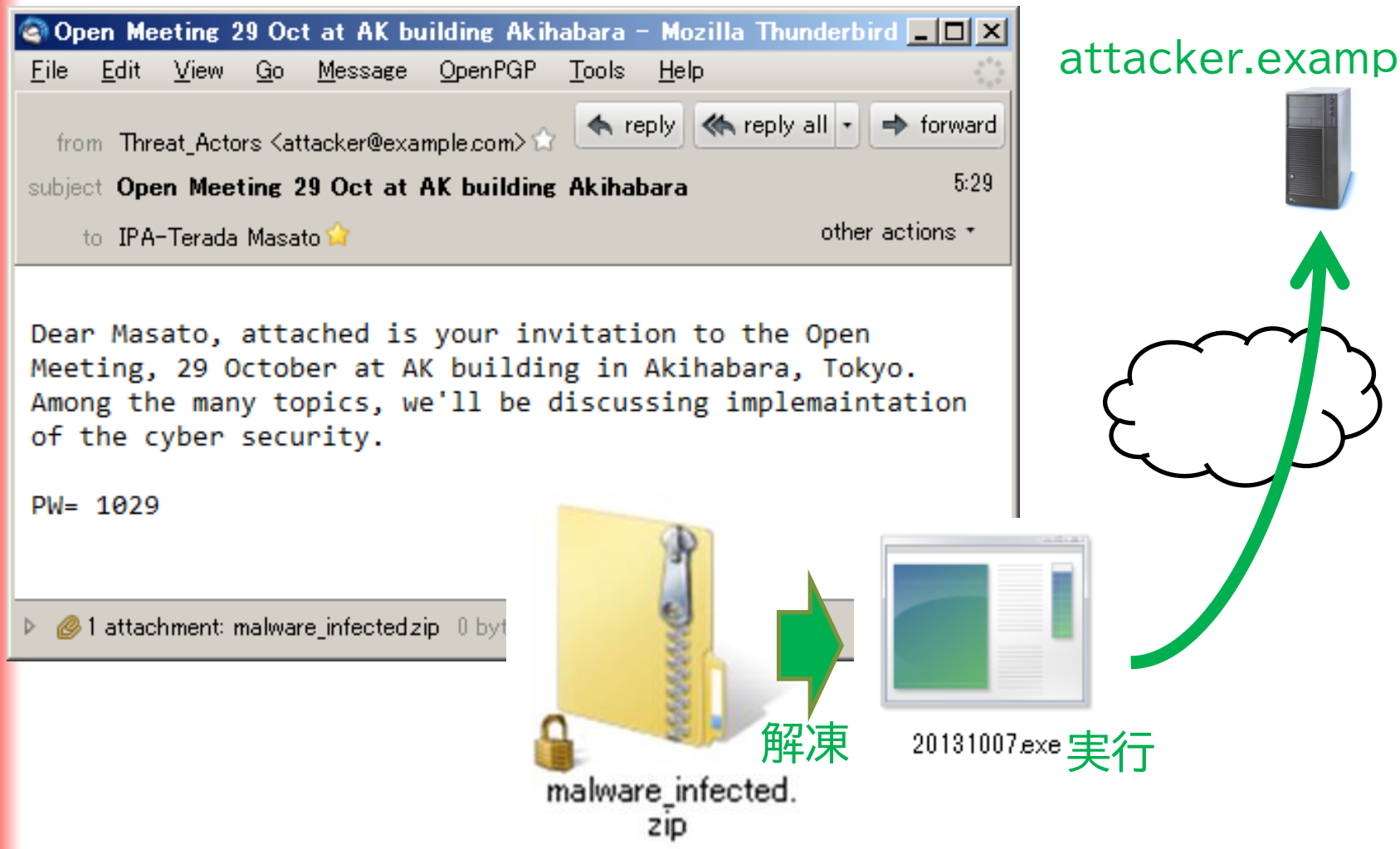
- MITREが中心となり仕様策定を進めてきたもので、サイバー攻撃活動によって観測された事象を記述するためのXML仕様である。MandiantのOpenIOC（侵害を受けたシステムの痕跡(Indicator of Compromise)を記述する仕様)を踏まえた仕様となっている。
- システム(Windows、UNIX)内部状態、ネットワーク通信、アプリケーション動作など、観測できる事象を記録する。

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
:

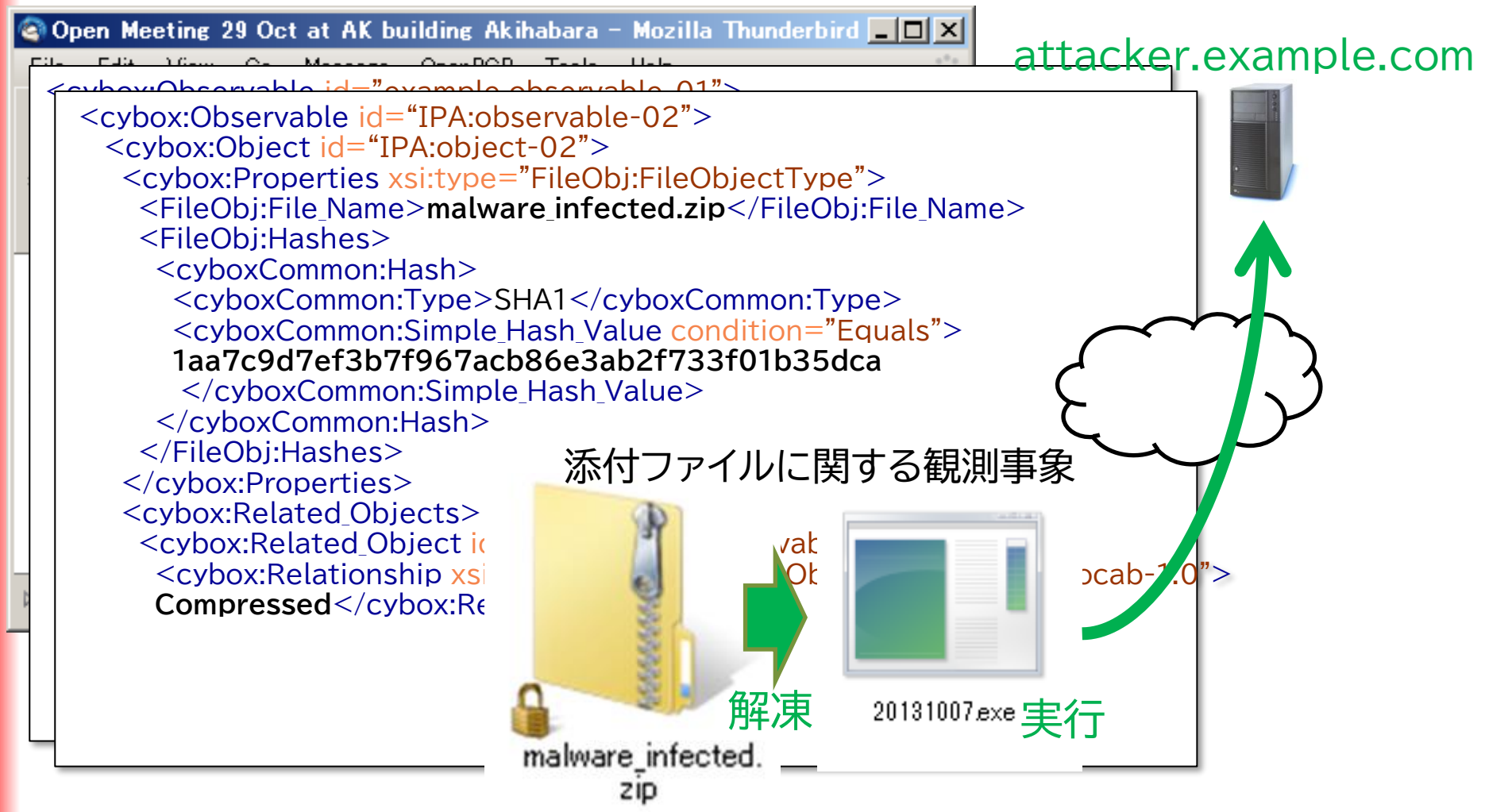
Network
Network Connection
Network Flow
Network Packet
Network Route
Network Socket
Port
Socket Address
:

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

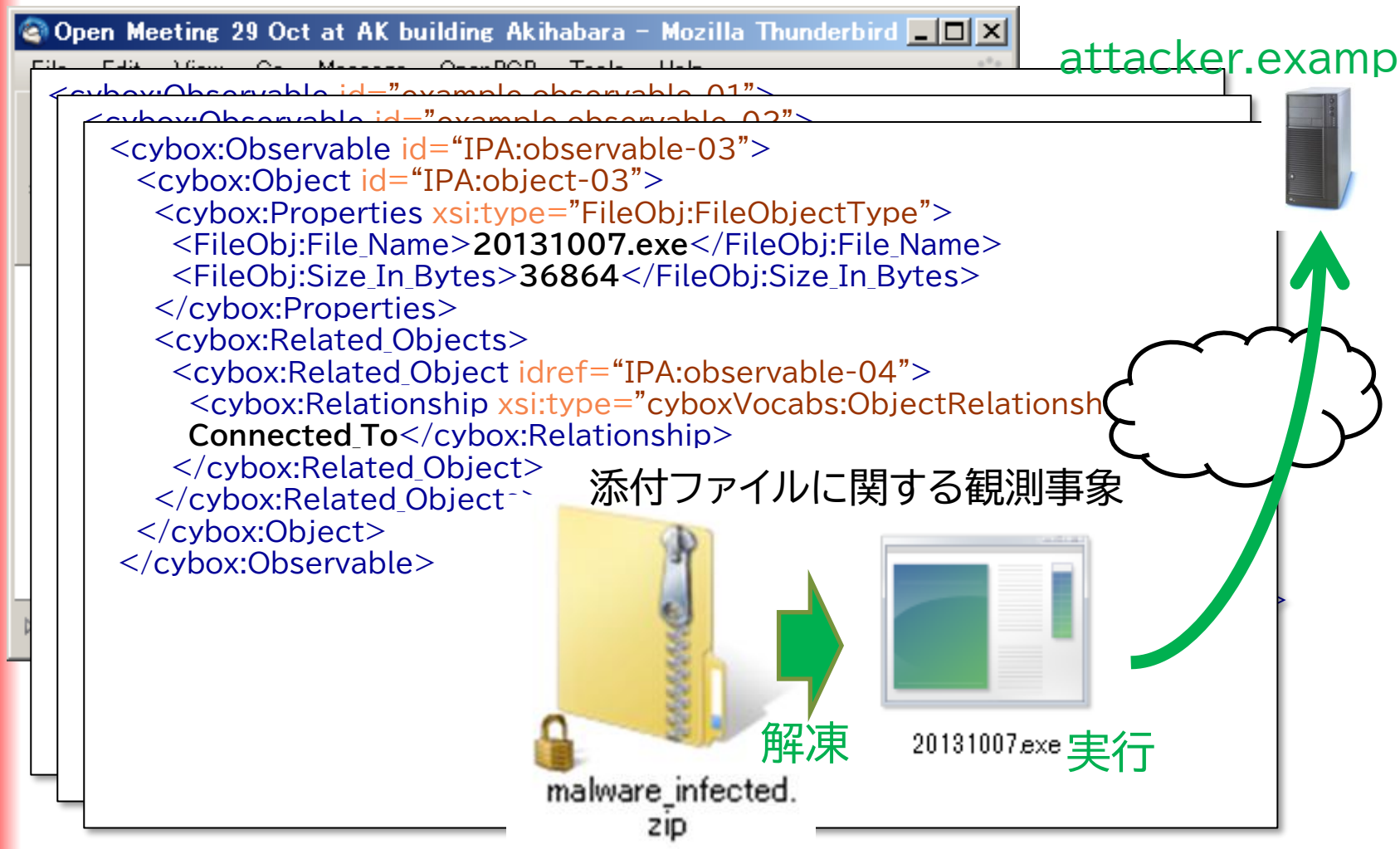


攻撃のモデル化と対処
標的型攻撃メールの観測事象(Observable)記述例

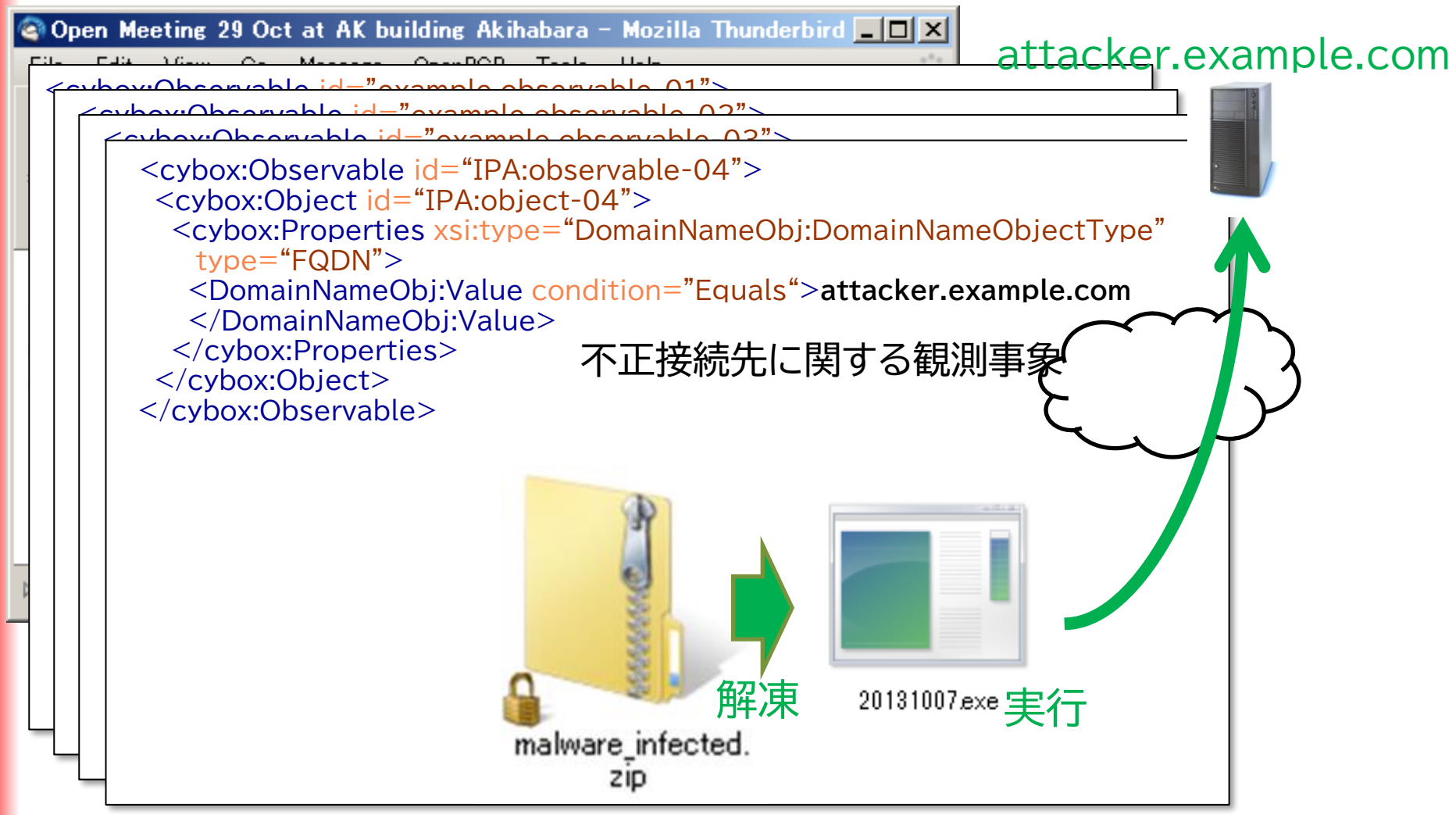
攻撃のモデル化と対処
標的型攻撃メールの観測事象(Observable)記述例



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



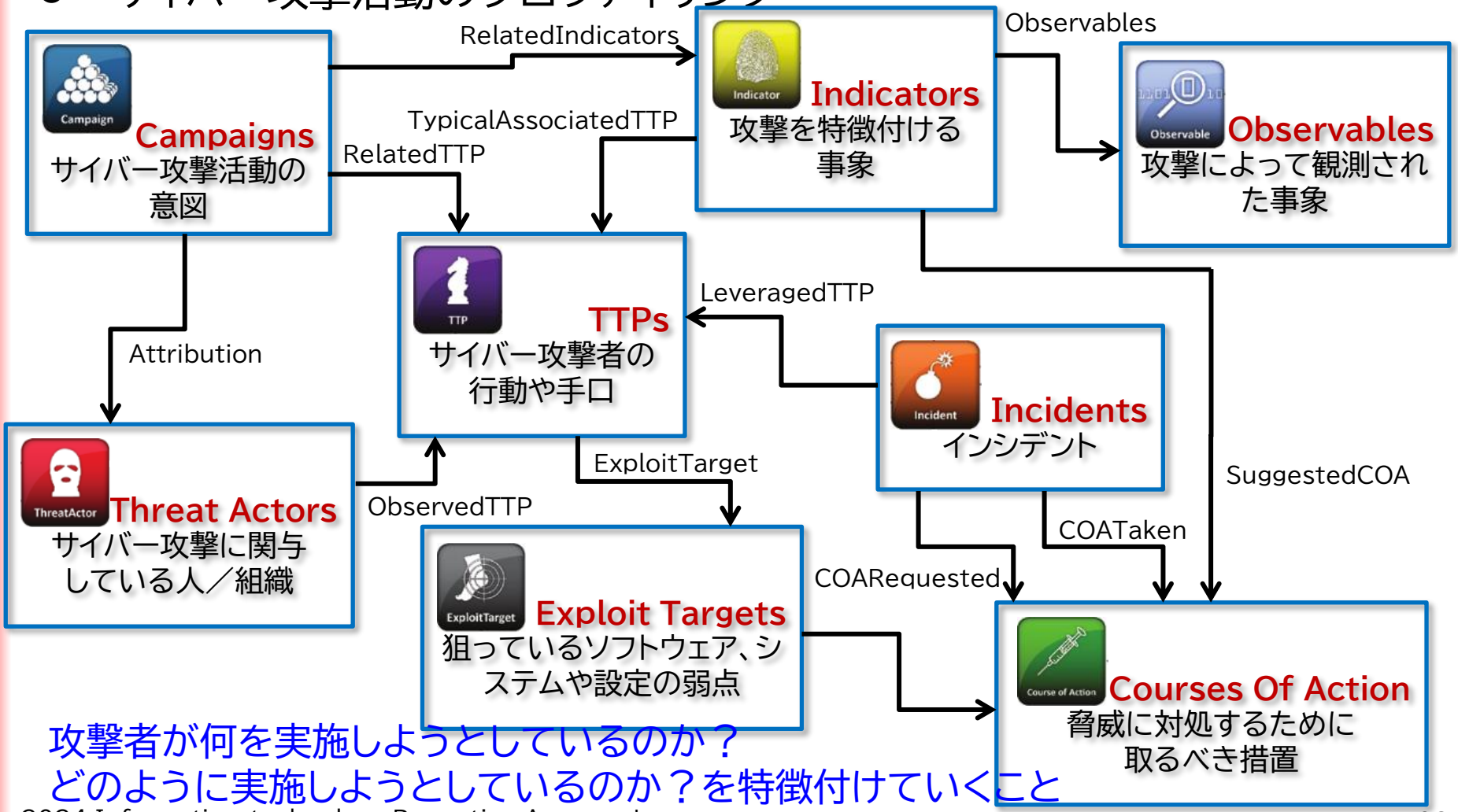
攻撃のモデル化と対処
STIX（脅威情報構造化記述形式）（2012年）

- 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)

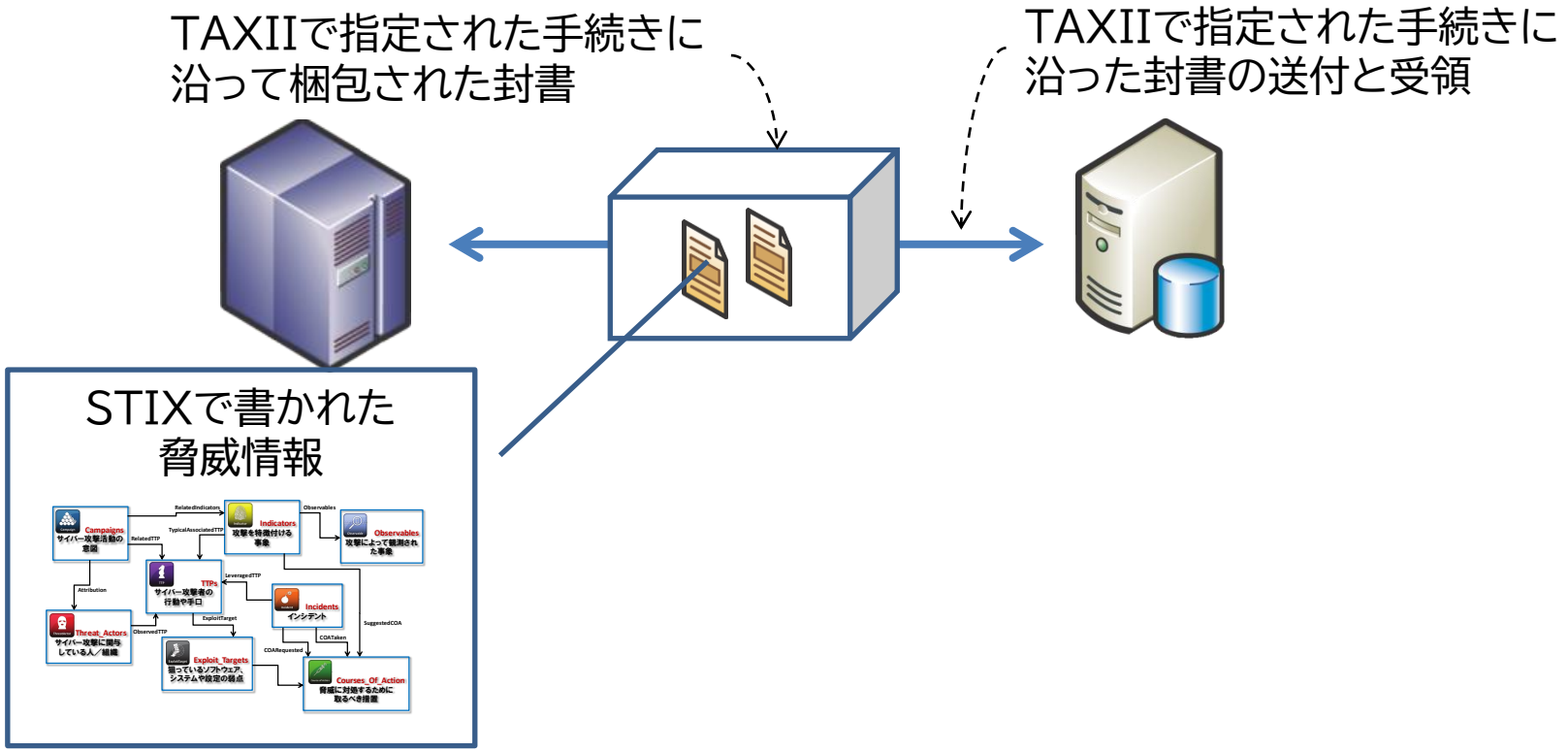
- サイバー攻撃活動のプロファイリング



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

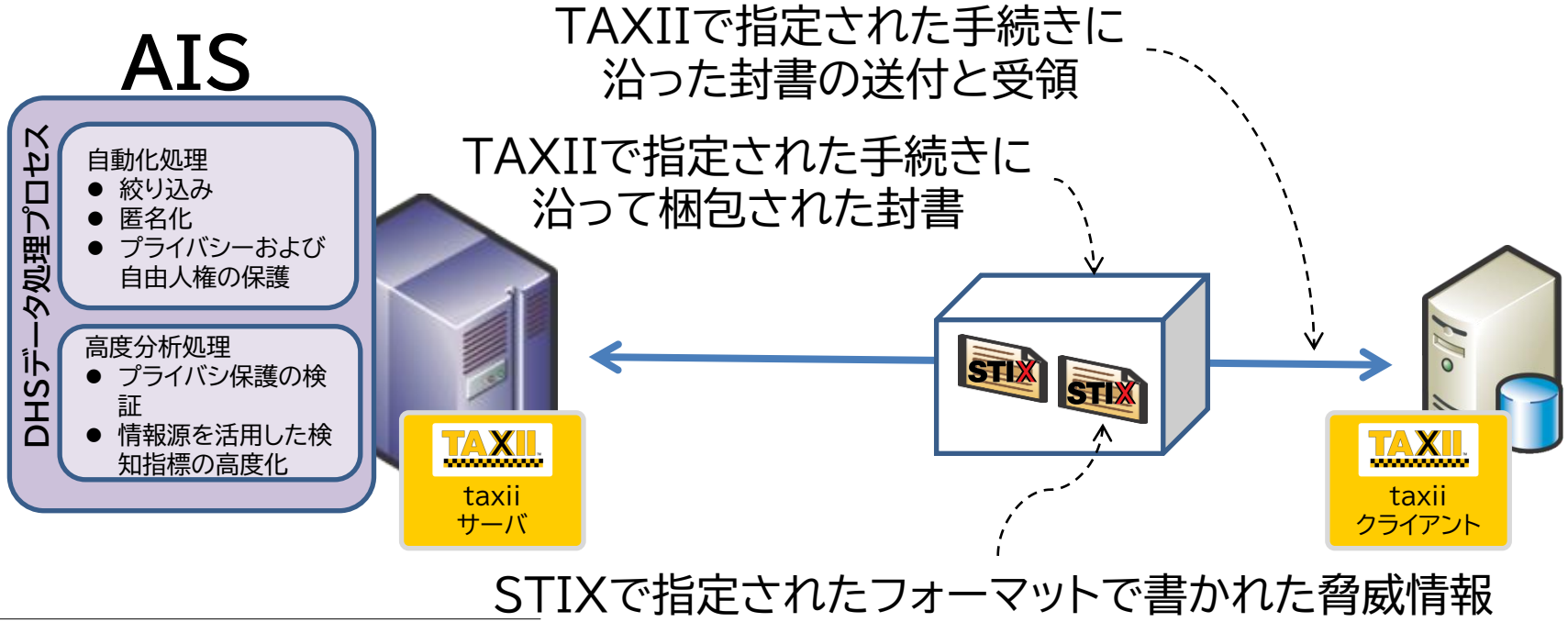
攻撃のモデル化と対処
TAXII(検知指標情報自動交換手順)(2012年)

- 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)

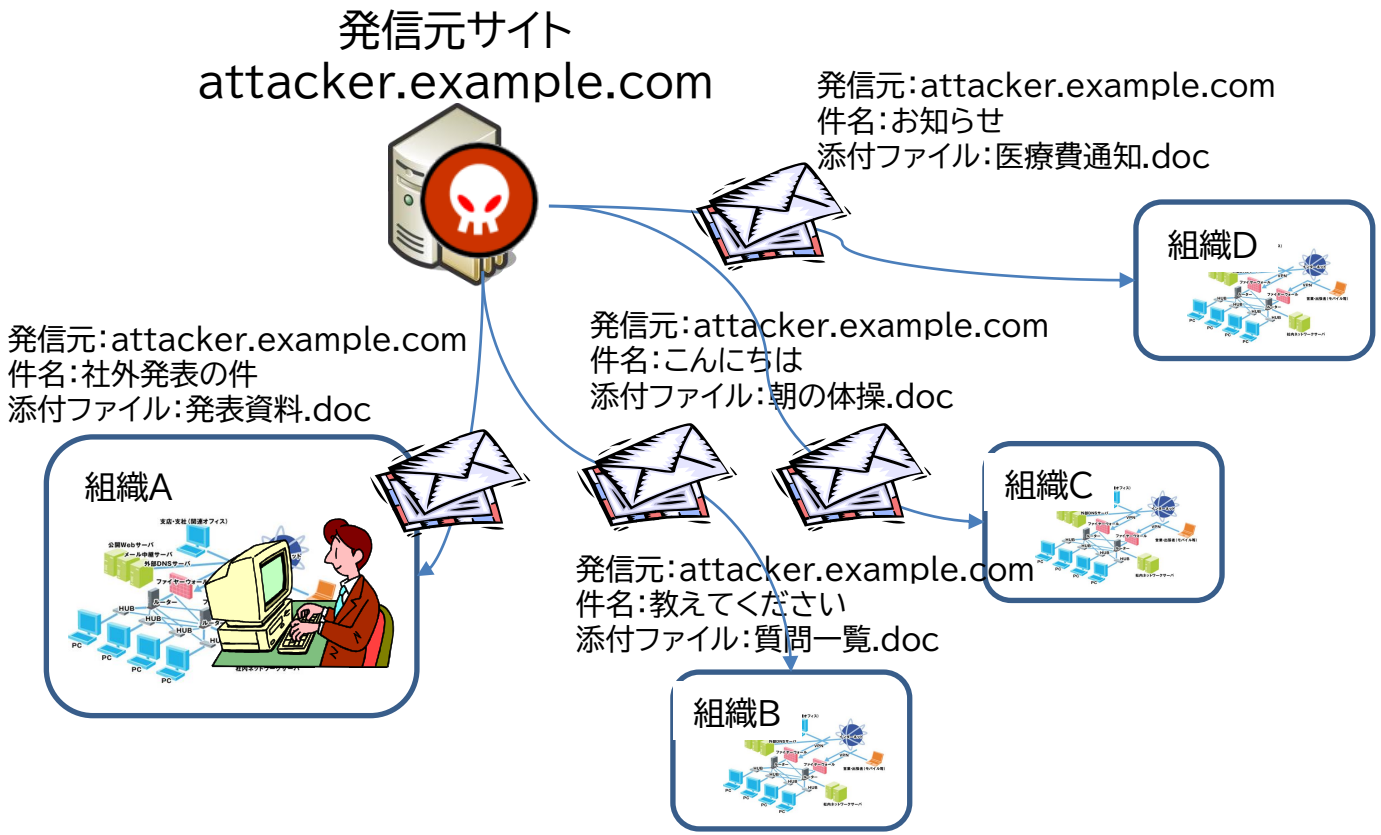
- 米国政府が提供する官民連携の情報共有基盤
- 2015年サイバーセキュリティ法により、2016年3月からDHSの下で活動を開始した。攻撃指令サーバのドメインやIPアドレス、マルウェアのハッシュ値などの検知指標(インディケータ)を共有する情報基盤である。



[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)

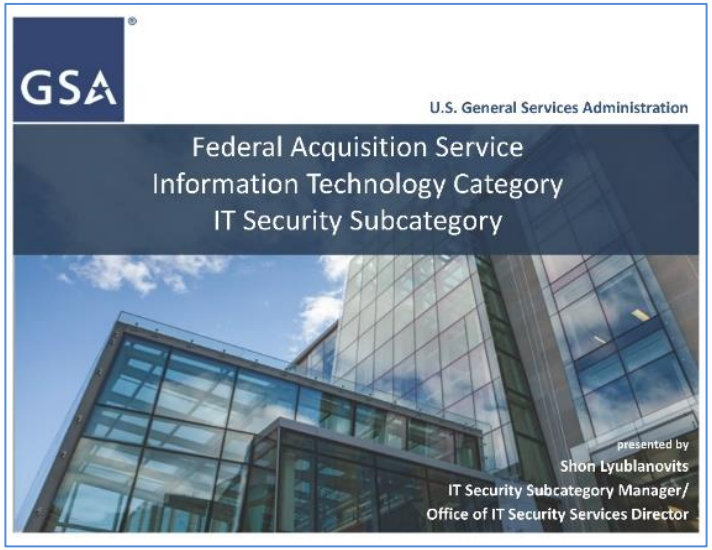
- 検知に有効なサイバー攻撃を特徴づける指標

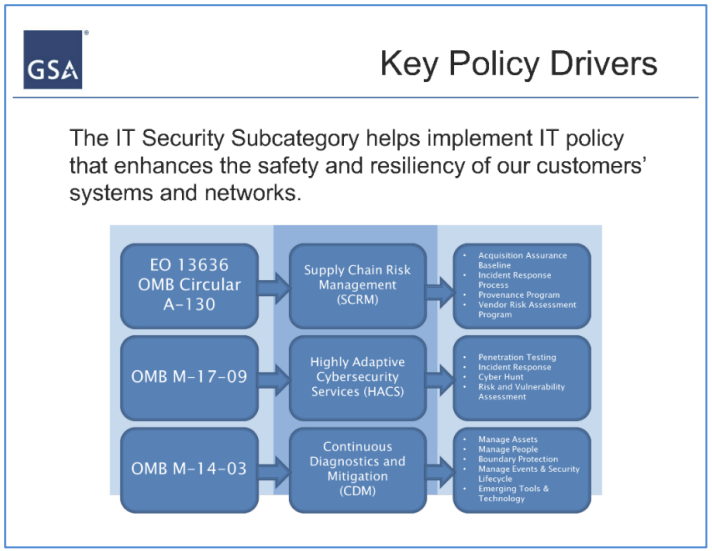


発信元:attacker.example.com
攻撃活動の共通項はインディケータとして使いやすい。

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(EO 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

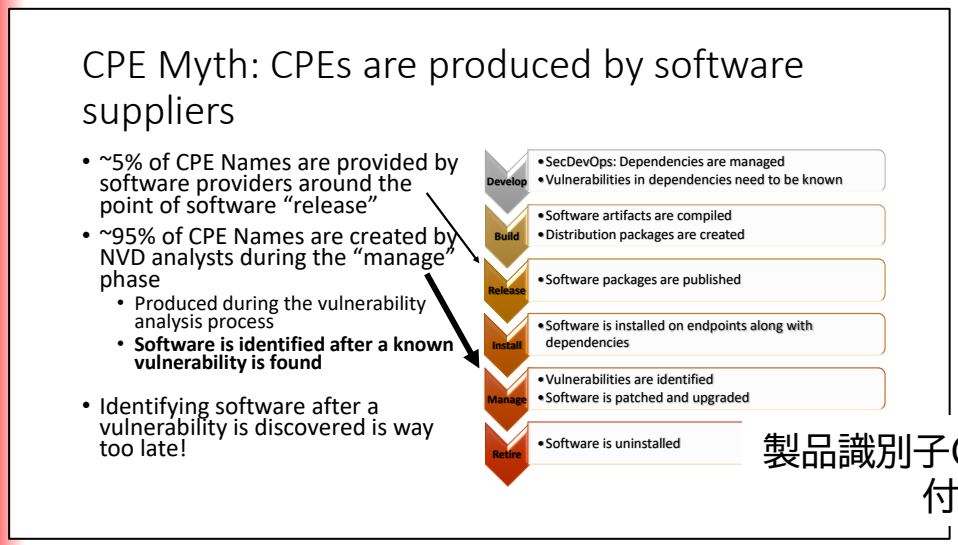
米国政府の脆弱性対策の取組み
公共サービスの調達

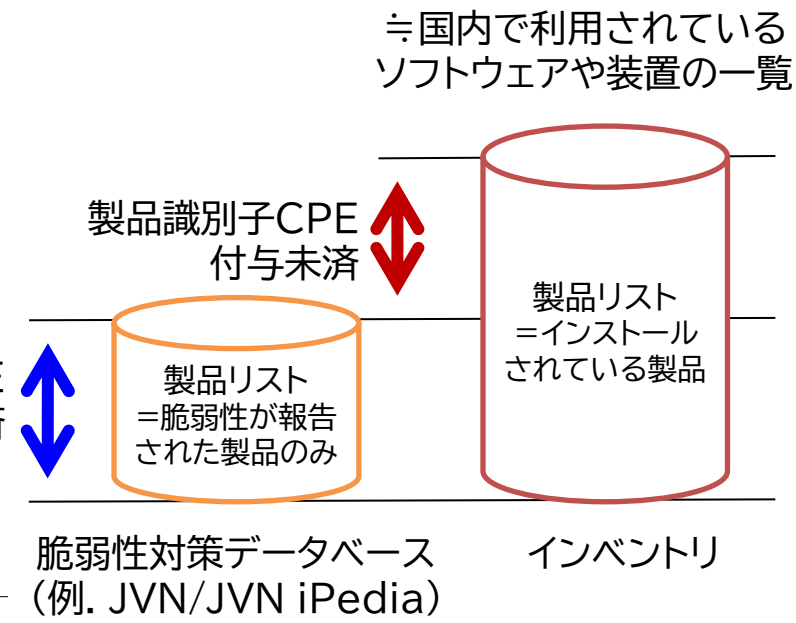
EO 13636 OMB Circular A-130	SCRM(サプライチェーンリスク管理) Supply Chain Risk Management	Acquisition Assurance Baseline Incident Response Process Provenance Program Vendor Risk Assessment Program (調達保証ベースライン、インシデント対応プロセス、出所プログラム、ベンダリスク評価プログラム)
OMB M-17-09	HACS(高度適応サイバーセキュリティサービス) Highly Adaptive Cybersecurity Services	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 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

- 製品識別子(CPE)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)





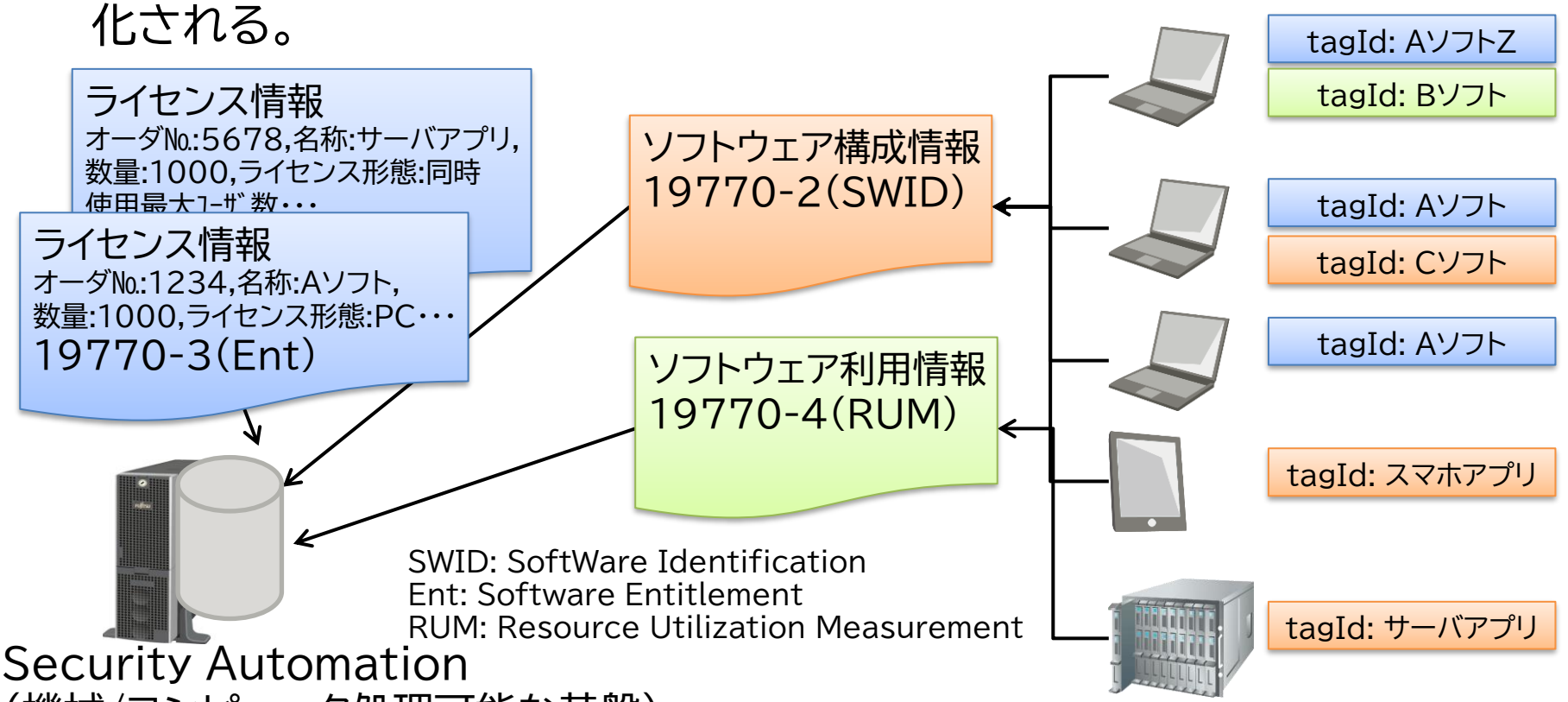
[出典] SCAPv2 April Developer Days Face to Face
https://csrc.nist.gov/Projects/security-content-automation-protocol-v2/Material-Archives

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 Processes and tiered assessment of conformance 価評性合適的階段び及スセロプ	ソフトウェア資産管理(SAM)のための統合されたプロセス群のベースラインを定める国際規格。2012年の改訂で、付加的な導入, アセスメント及び認識を可能にする「段階」という考え方が取り入れられている。また、ISO/IEC 20000と緊密な整合がとられており、ISO/IEC 20000のITサービスマネジメントを支援することを意図している。	JIS X 0164-1:2019
ISO/IEC 19770-2:2009 Software identification tag ソフトウェア識別子 (SWID)	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 ソフトウェア識別子 (SWID)	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。	
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	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
資産管理と脆弱性対策の融合

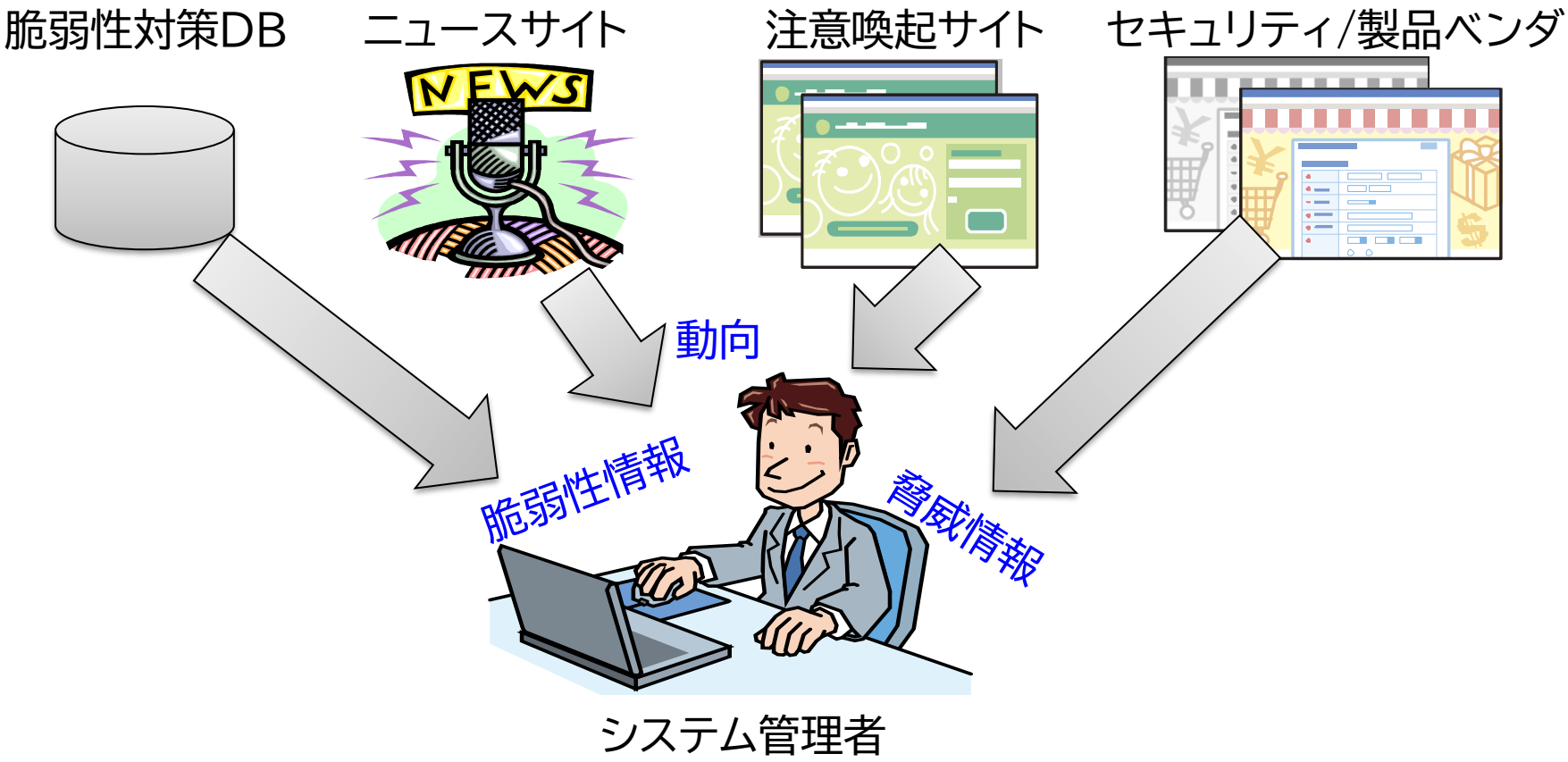
- 各種情報を集約し、自動チェックするなどの基盤整備に利用可能
- ソフトウェア構成情報(SWID)は19770-2、ライセンス情報(Ent)は19770-3、リソース利用情報(RUM)は19770-4で情報構造が標準化される。



JVN脆弱性対策機械処理基盤

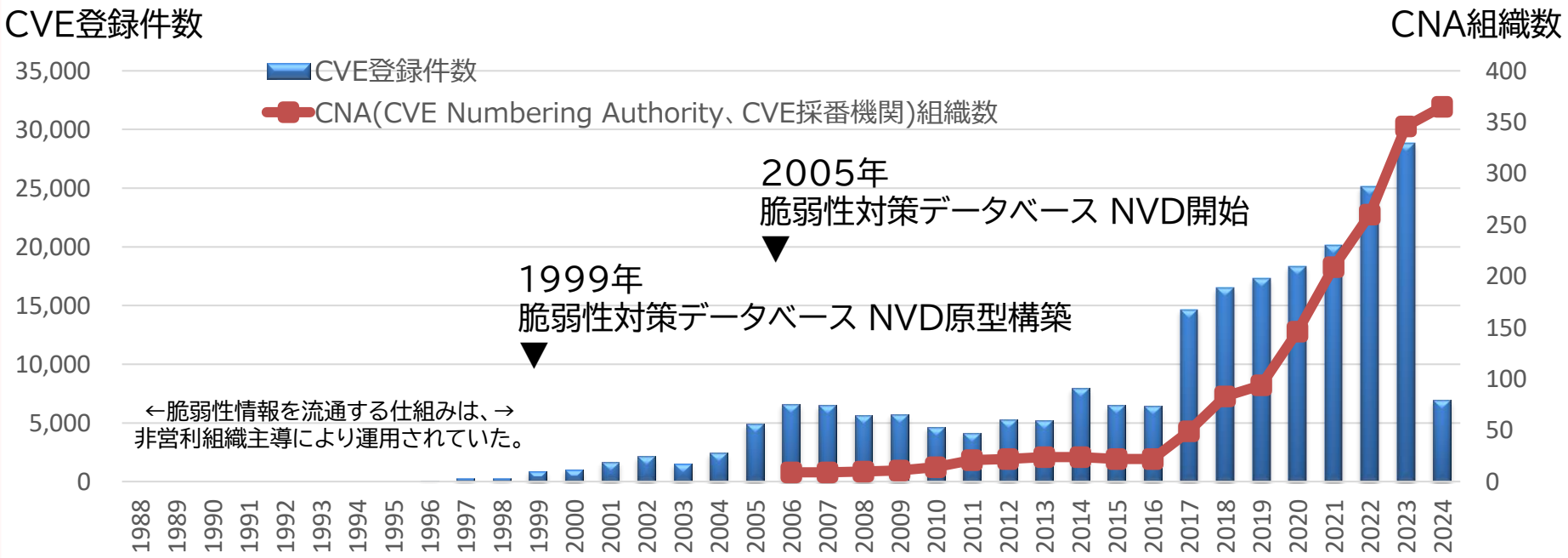
脆弱性関連情報の収集
防御としての（情報活用＋対策）

- 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

- 米国脆弱性対策データベース(NVD: 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。

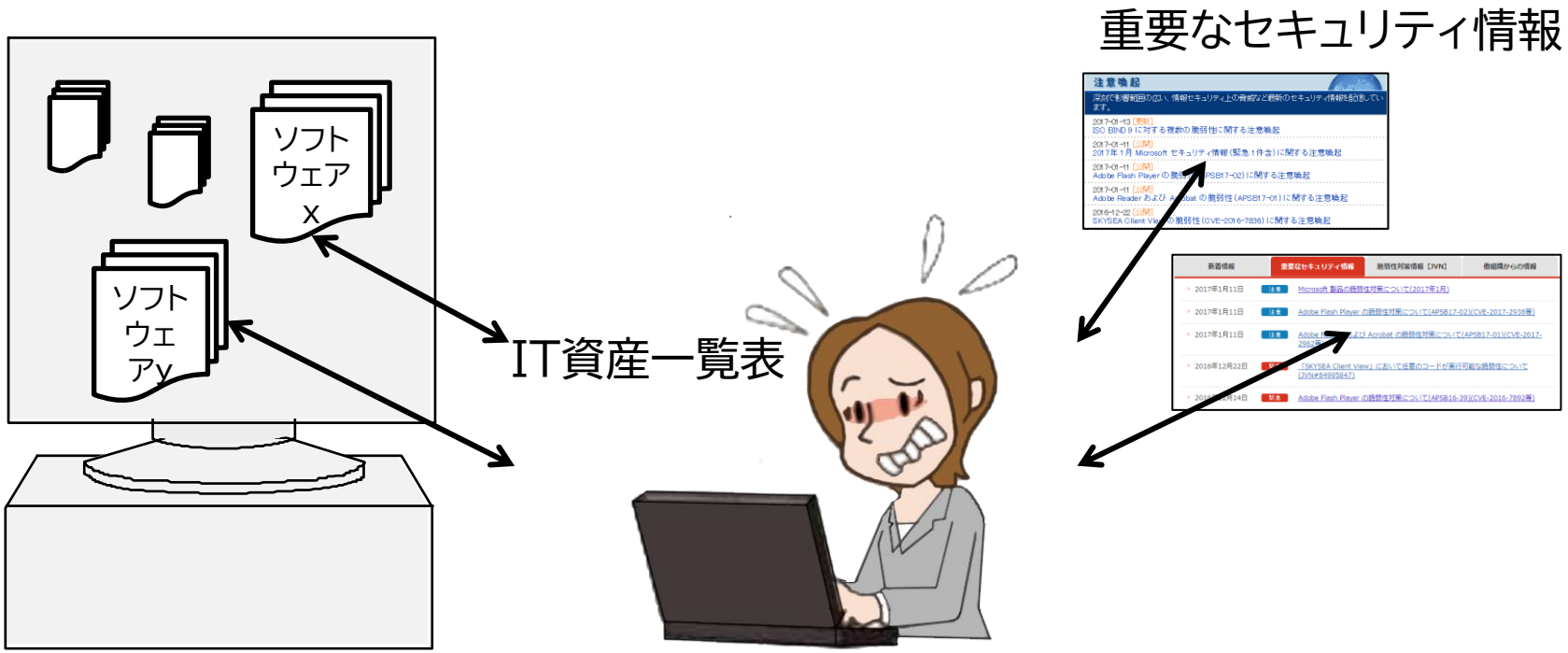


[出典] https://nvd.nist.gov/vuln/search
https://www.cve.org/PartnerInformation/ListofPartners

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

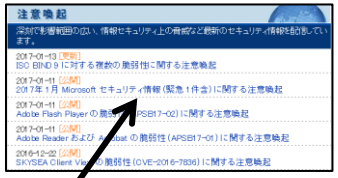
- 重要なセキュリティ情報が発信されるたびに、手作業でIT資産一覧表を検索して、影響範囲の調査をしていませんか？
  - 多くの場合、インストール状況と脆弱性との紐付けを人手で実施している（資産管理と脆弱性対策とが連携できているわけではない）。



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。
- 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(Common Vulnerabilities and Exposures)

[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(Common Platform Enumeration)

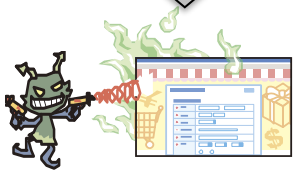
[形式] cpe:/{種別}:{ベンダ名}:{製品名}
[例] cpe:/o:microsoft:windows_7
マイクロソフト ウィンドウズ 7と言っても表記方法は様々
Microsoft Windows 7、マイクロソフト Windows 7など

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)
  - 評価指標の共通化
    - 脆弱性の深刻度を評価する。
      - CVSS(Common Vulnerability Scoring System)
      - 脆弱性の深刻度を表す評価

CVSS ＝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？

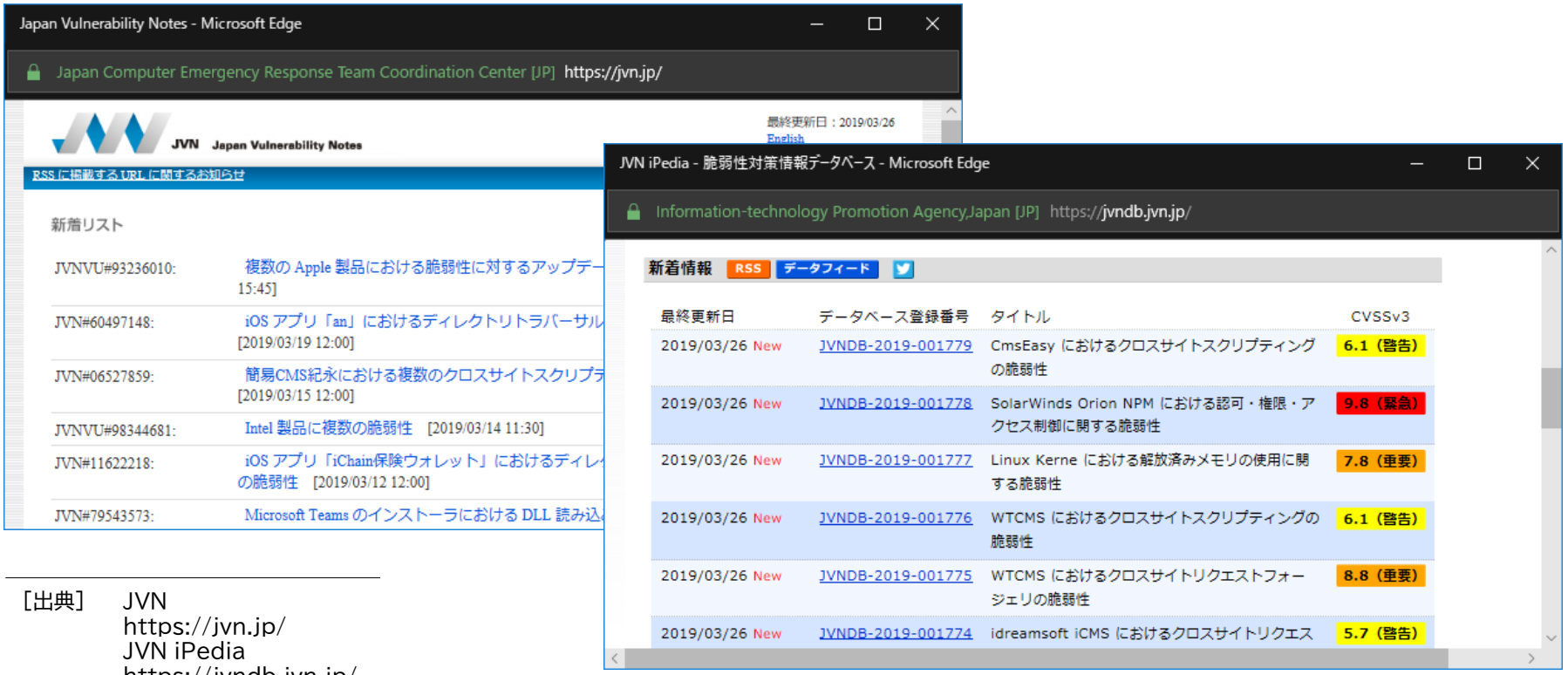


既に攻撃は発生している？
対策は出ている？

システムの重要度は？

JVN脆弱性対策機械処理基盤
JVN

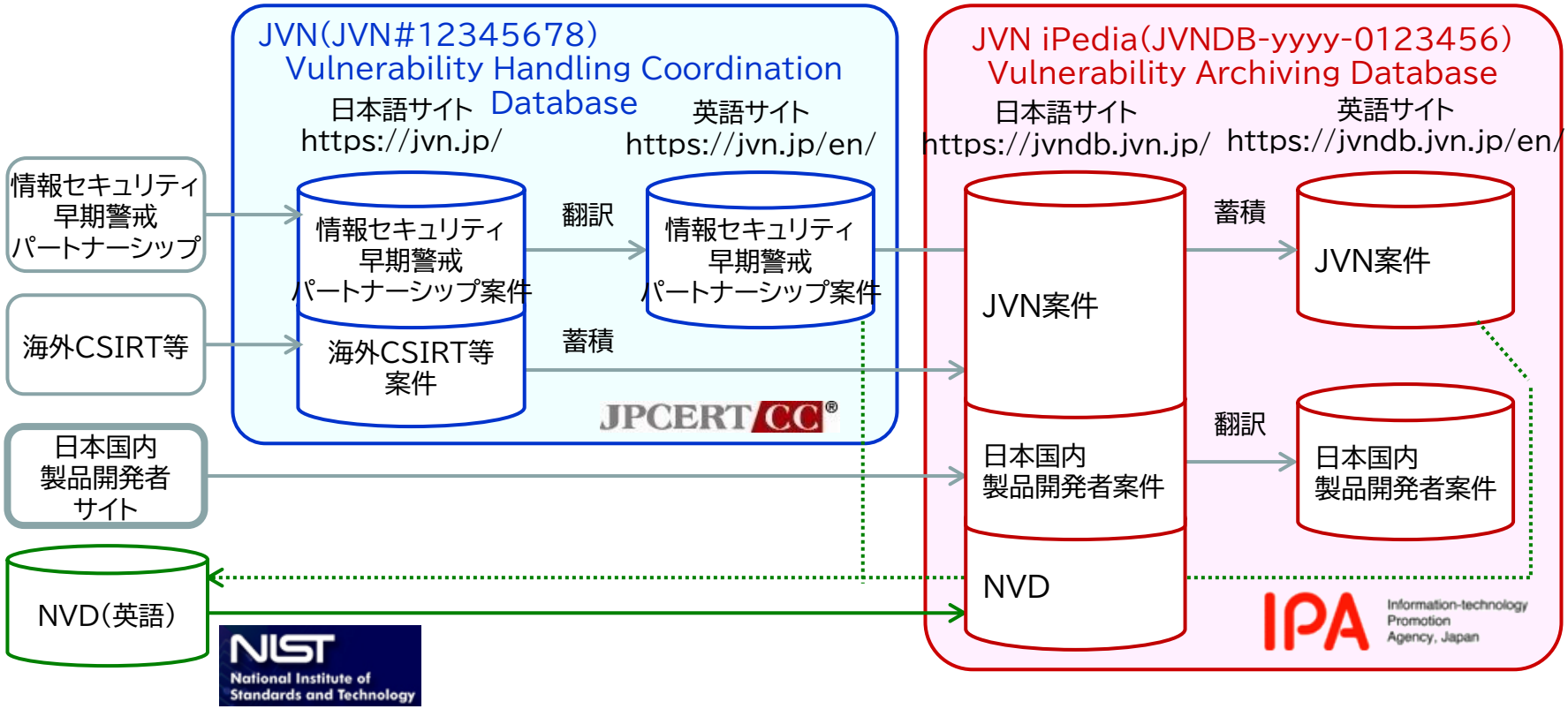
- JVN は、“Japan Vulnerability Notes” の略
- 日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供し、情報セキュリティ対策に資することを目的とする脆弱性対策情報サイト



［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

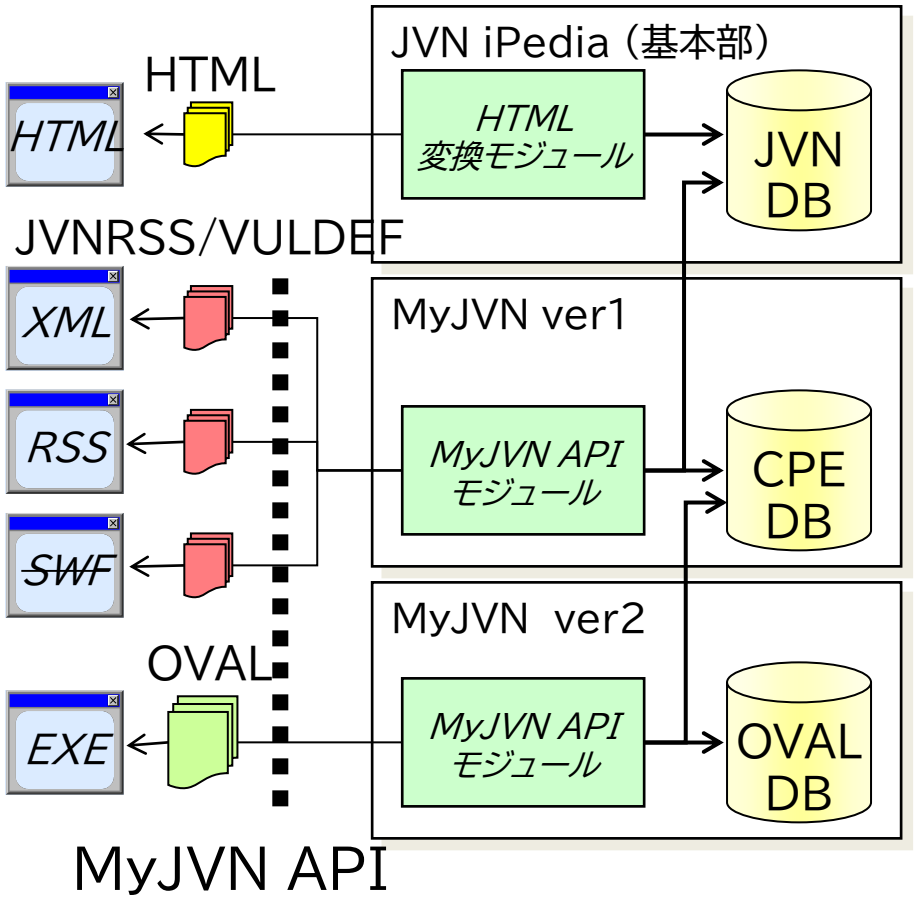
MyJVN API
http://jvndb.jvn.jp/apis/

- 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）

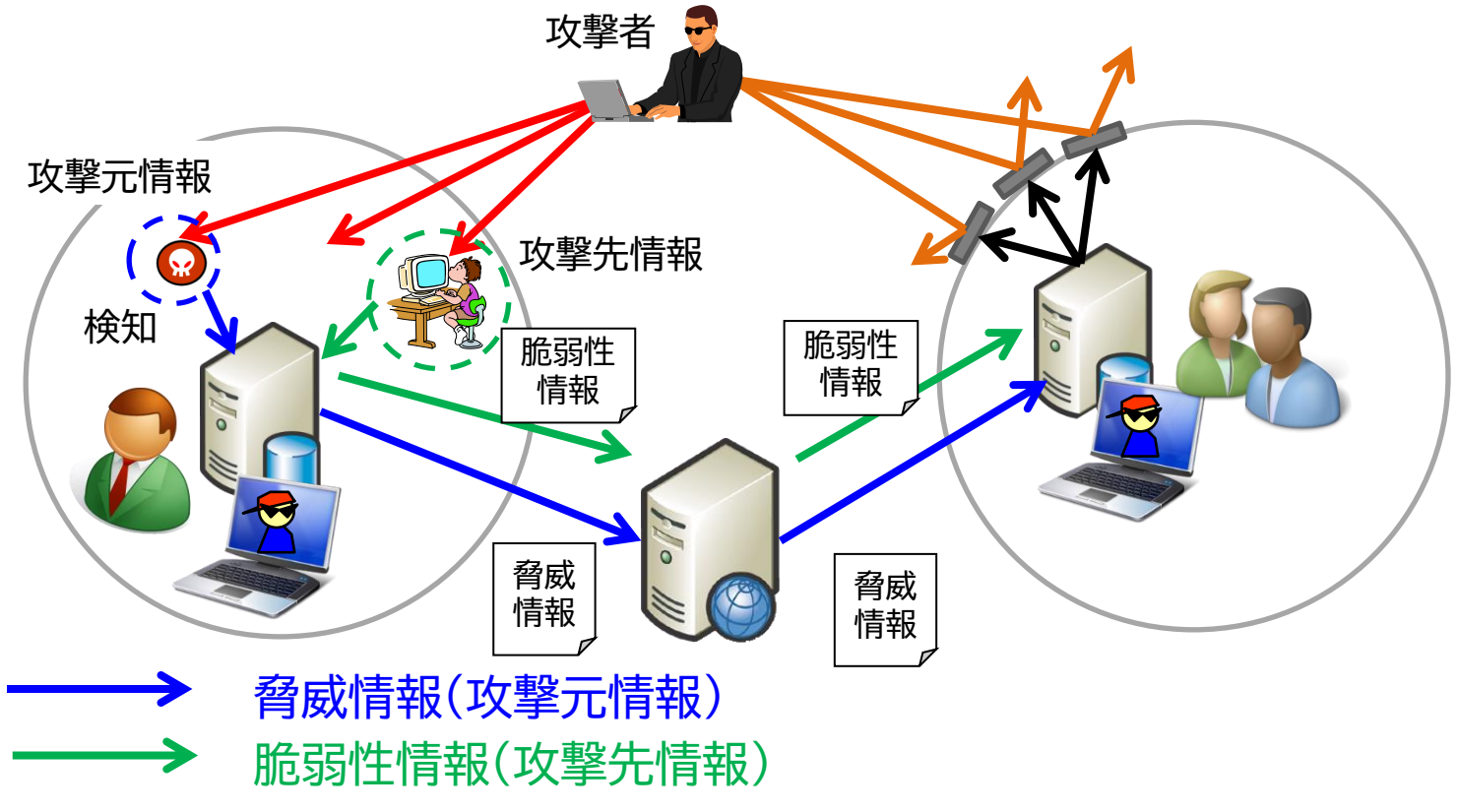


機械処理可能な情報活用基盤の整備
望ましい環境に向けて

- 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。

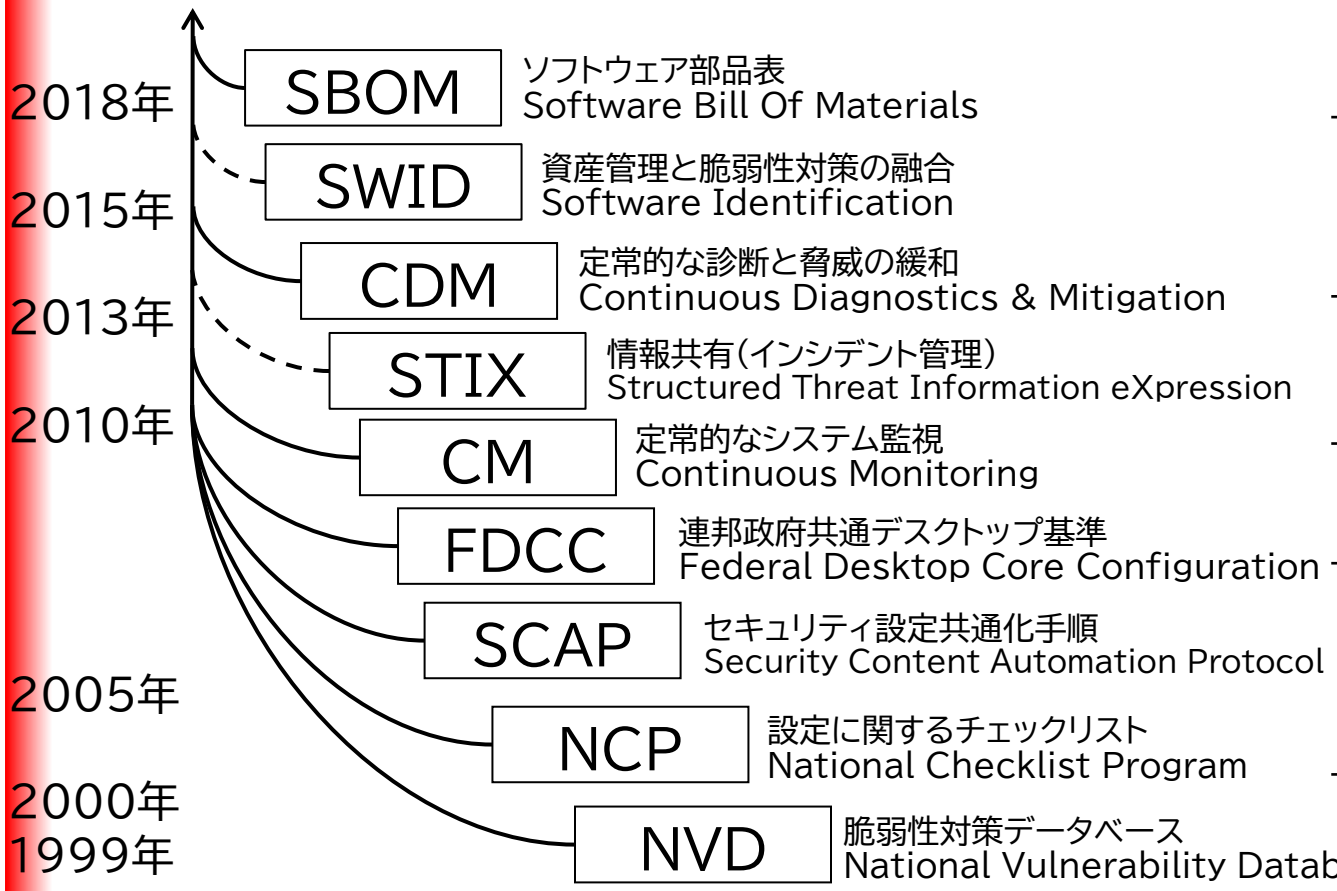
機械処理可能な情報活用基盤の整備
望ましい環境に向けて

- 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[3]

KEV、EPSS、SSVC

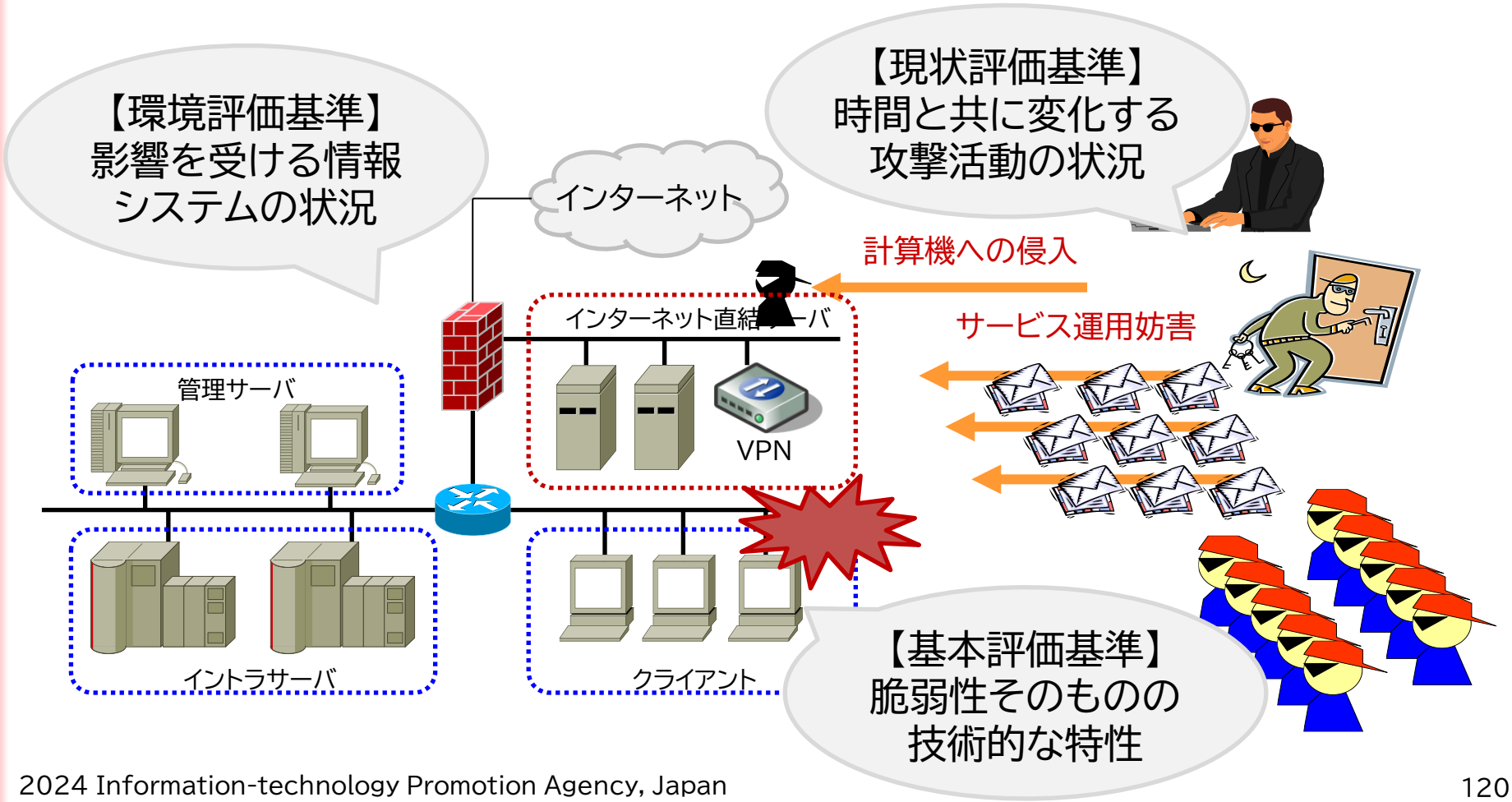
KEV、EPSS、SSVCとは

- 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 脆弱性の悪用可能性評価システム	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

CVSS
脆弱性の深刻度を数値で表現する

- CVSS（共通脆弱性評価システム）
- 攻撃状況やシステムの重要度を加味した脆弱性の深刻度を表す評価



CVSS
脆弱性の深刻度を数値で表現する

- CVSS（共通脆弱性評価システム）
- 攻撃状況やシステムの重要度を加味した脆弱性の深刻度を表す評価

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	JVN JVN iPedia MyJVN
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（脆弱性の悪用可能性予測評価システム） SSVC（役割に応じた脆弱性対応分類）
環境評価基準	影響を受ける情報システムの状況	

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

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

- 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
  - 共通脆弱性識別子（CVE）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

悪用された既知の脆弱性一覧
KEV（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）

悪用された既知の脆弱性一覧
KEV（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
Cisco Adaptive Security Appliance および Cisco Firepower Threat Defense ソフトウェアにおける脆弱性

脆弱性の悪用可能性評価システム
EPSS（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

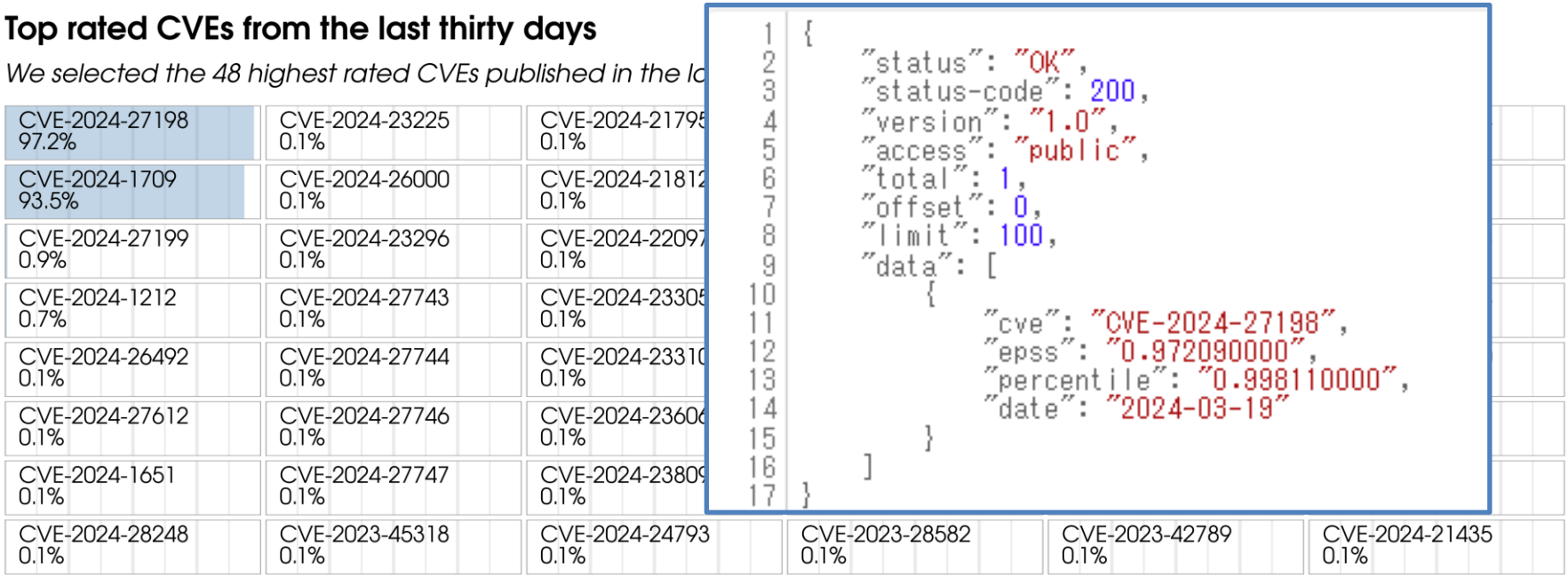
脆弱性の悪用可能性評価システム
EPSS（Exploit Prediction Scoring System）

- 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

脆弱性の悪用可能性評価システム
EPSS (Exploit Prediction Scoring System)

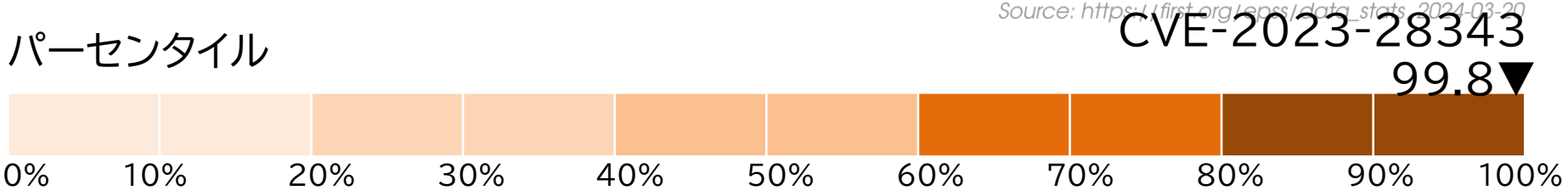
- EPSSスコア、EPSSパーセンタイル

https://api.first.org/data/v1/epss?cve=CVE-2024-27198




```
{
    "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"
        }
    ]
}
```


パーセンタイル



役割に応じた脆弱性対応分類
SSVC (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

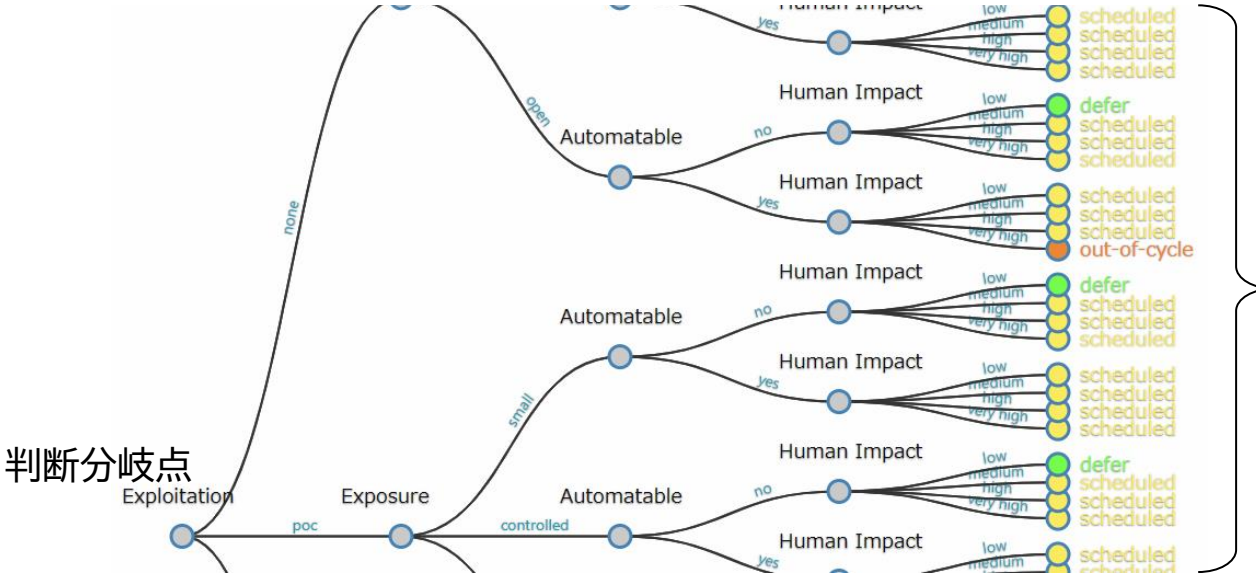
[出典] SSVC
https://certcc.github.io/SSVC/

役割に応じた脆弱性対応分類
SSVC (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

役割に応じた脆弱性対応分類
SSVC (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

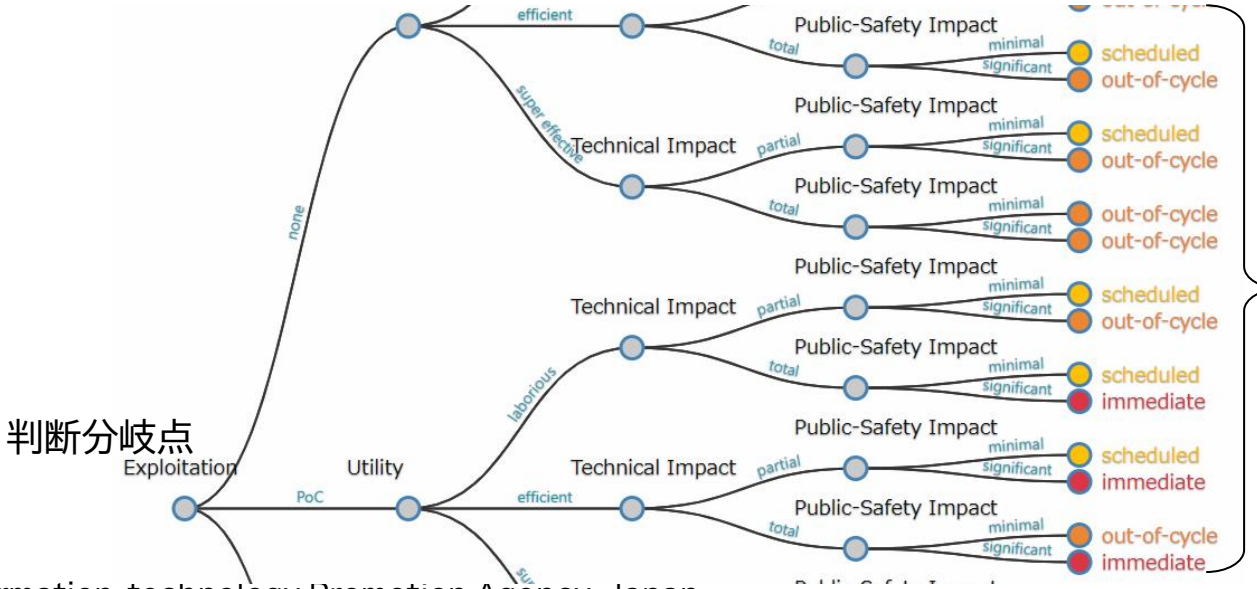


役割に応じた脆弱性対応分類
SSVC (Stakeholder-Specific Vulnerability Categorization)

- 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

役割に応じた脆弱性対応分類
SSVC (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

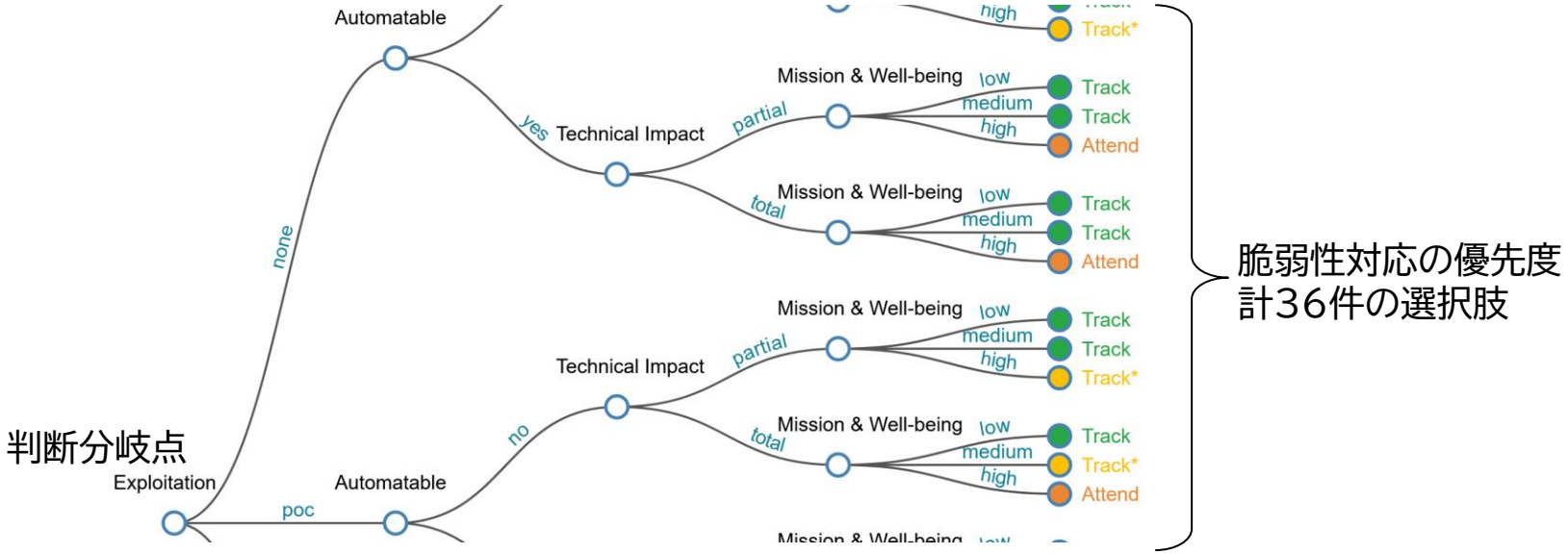


役割に応じた脆弱性対応分類
SSVC (Stakeholder-Specific Vulnerability Categorization)

- 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

役割に応じた脆弱性対応分類
SSVC (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

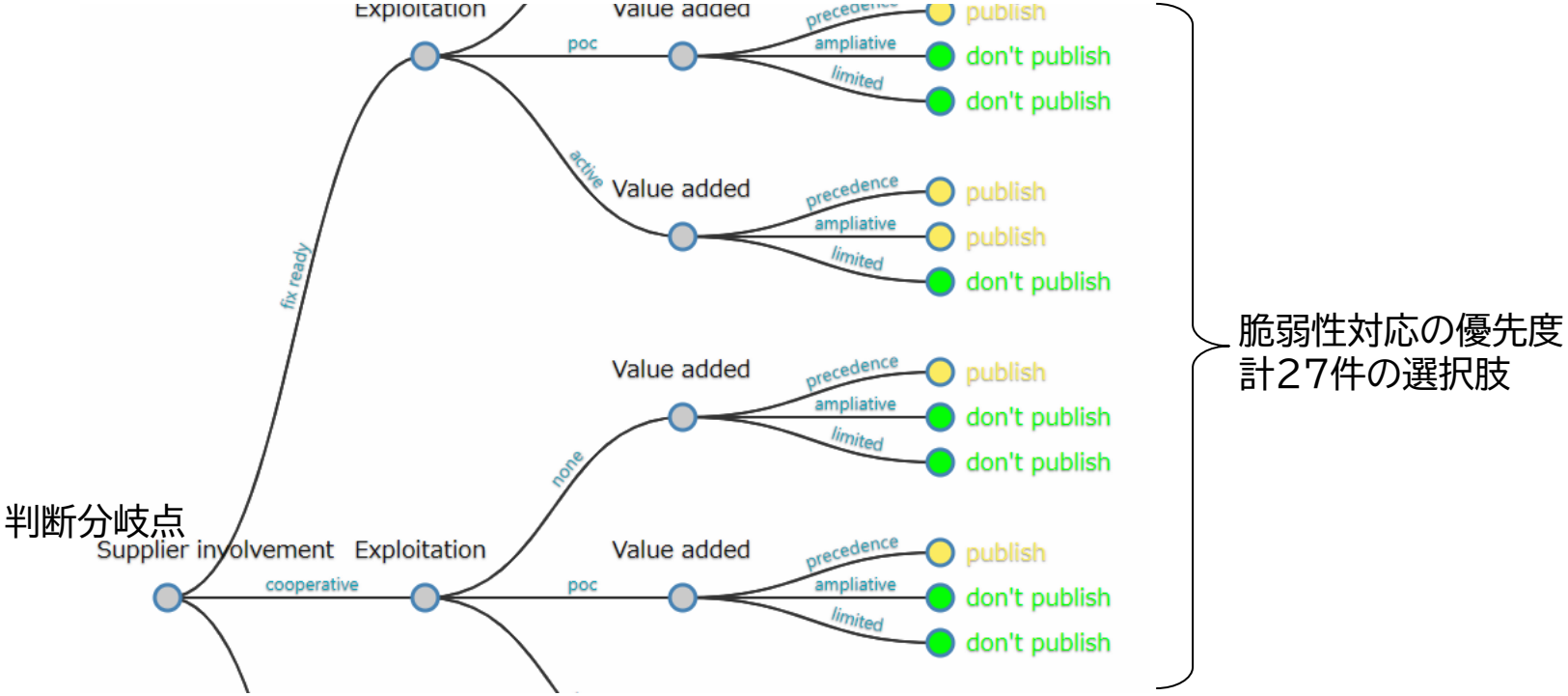


役割に応じた脆弱性対応分類
SSVC (Stakeholder-Specific Vulnerability Categorization)

- 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

役割に応じた脆弱性対応分類
SSVC (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

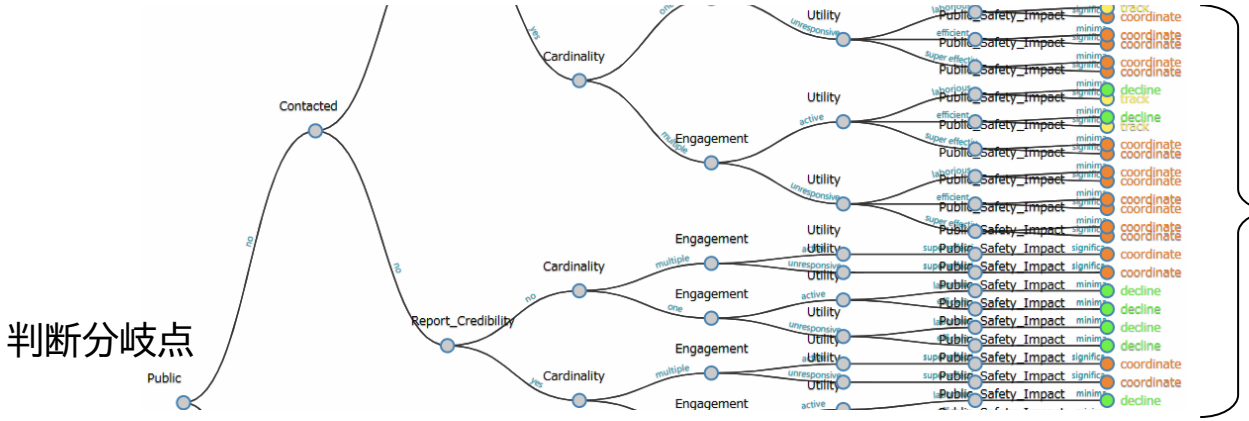


役割に応じた脆弱性対応分類
SSVC (Stakeholder-Specific Vulnerability Categorization)

- 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

役割に応じた脆弱性対応分類
SSVC (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
2024年03月27日