IT資産管理とセキュリティ

2022年7月22日

山下　知起(ICT-ISAC情報共有WG／株式会社日立製作所)

ICT-ISAC JAPAN
ICT Information Sharing And Analysis Center Japan

目次

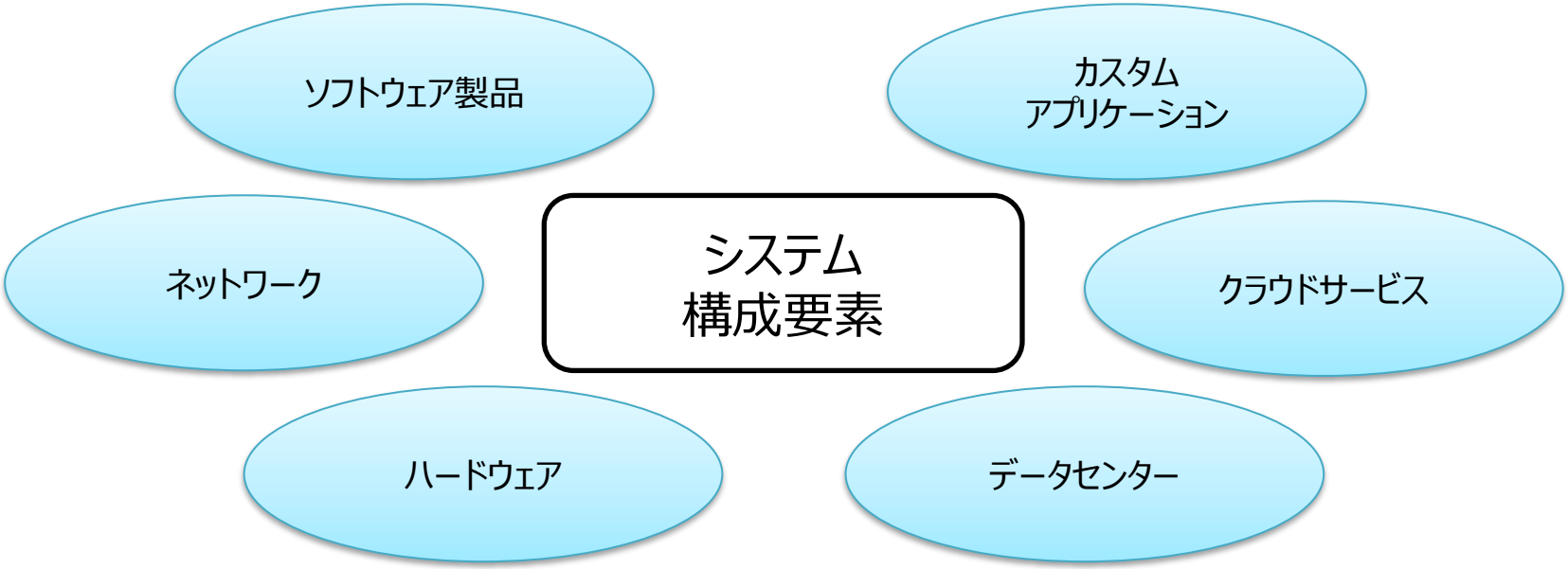
- 背景：IT資産管理とセキュリティ
  - サプライチェーンとアーキテクチャの複雑化
  - 個社視点での対応の限界
  - 脆弱性の報告数の増加

- 情報共有基盤の実証
  - 実証実験の目的
  - 2020年度における連携の概要
  - 2021年度における連携の概要
  - 実証実験で得られた知見

背景：IT資産管理とセキュリティ

サプライチェーンとアーキテクチャの複雑化

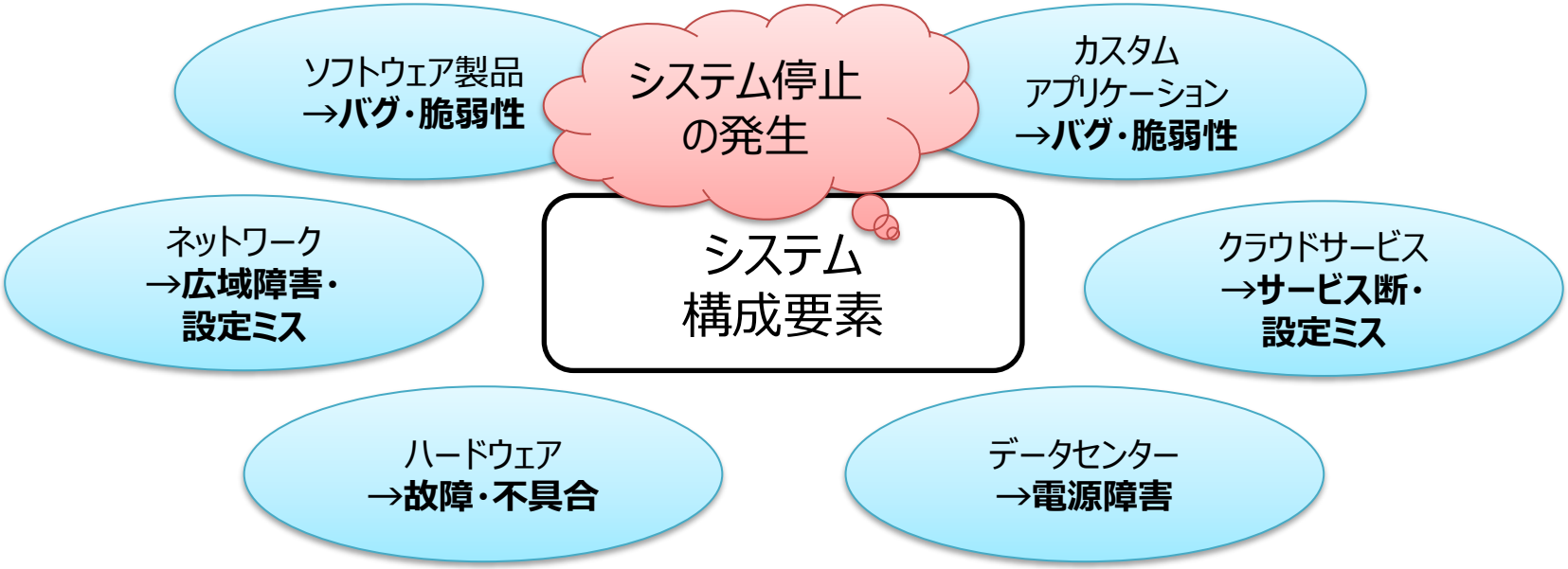
- 複数のベンダが構築したシステムを採用することや、クラウドサービス等外部サービスの利用が当たり前になることに伴って、一組織が抱えるサプライチェーンやアーキテクチャが複雑化
  - 国内の様々な企業のシステムはマルチベンダ化やクラウドサービスの普及を背景に一般的に年々サプライチェーンとアーキテクチャが複雑化する傾向にある。
  - システム障害やインシデントを検知した際に、どの構成要素にどのような不具合が生じたのか判断が難しい。



背景：IT資産管理とセキュリティ

個社視点での対応の限界

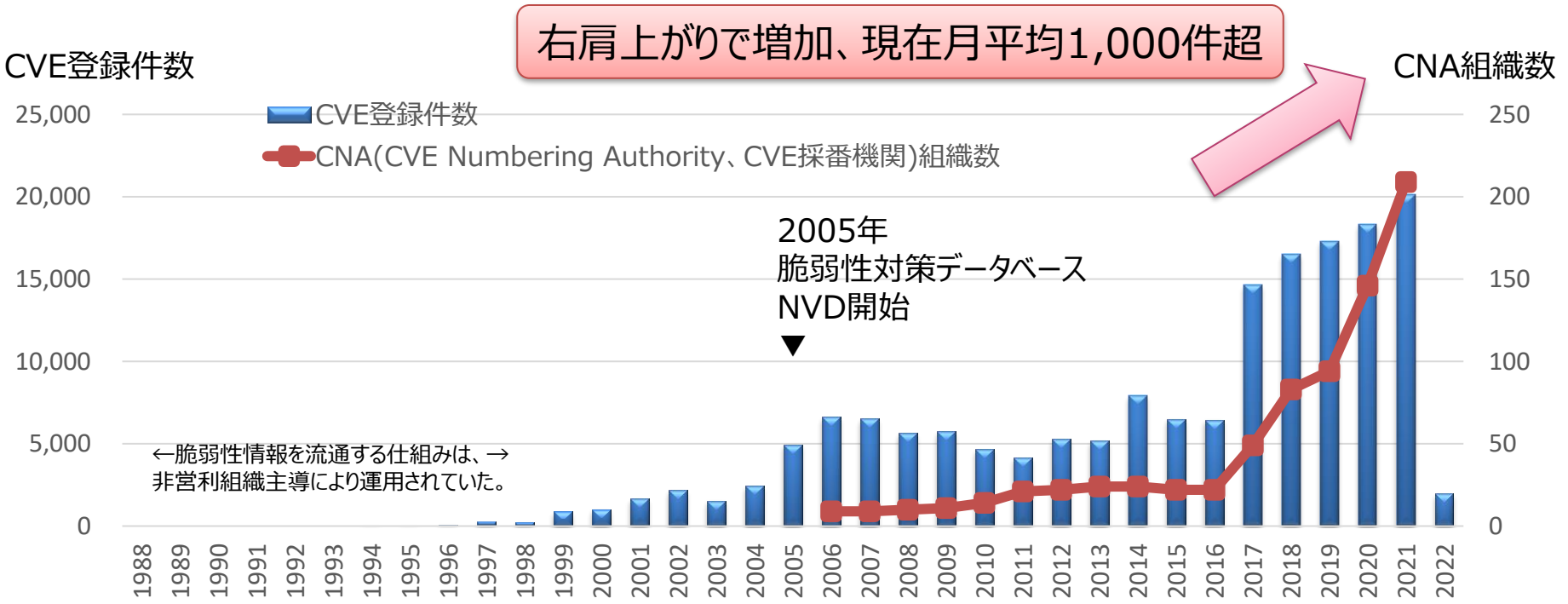
- 例えばシステム停止障害の原因を判断する際、様々なシステム構成要素が原因となっている可能性を検討すべきだが、個社が即座に判断することは難しい。
  - これらのシステム停止に繋がりうる情報は特定のコミュニティや関係者内では速やかに連携されている可能性があるが、誰もがアクセス出来ない＝オープンデータではない。
  - 情報共有は、サプライチェーンの拡大により、多くの企業・組織の関心事となっている共通項を括りだし、オープンデータ化することが必要であると言える。



背景：IT資産管理とセキュリティ

脆弱性の報告数の増加

- システム構成要素の複雑化に伴い、個社が対応すべき脆弱性も増加している。
  - 米国脆弱性対策データベース(NVD:National Vulnerablity Database)によれば、2017年頃より増加しており、全ての脆弱性情報を都度時間をかけて吟味することは現実的ではなくなった。



背景：IT資産管理とセキュリティ

情報共有・自動処理の必要性

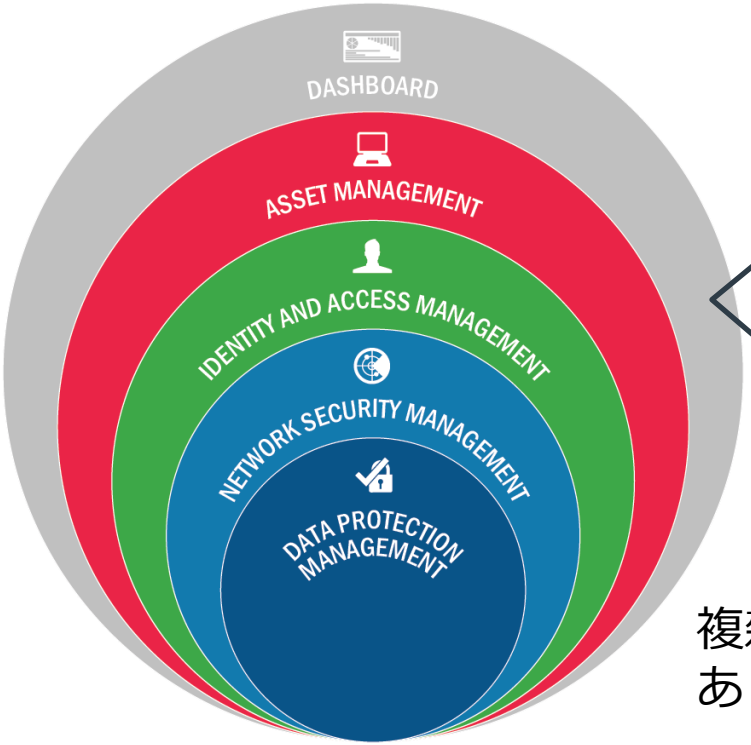
- 複雑化するシステムと、増加する脆弱性に対応するには、各業界・業種に合わせた情報をオープンデータとして共有することと、セキュリティ対策に必要な情報の処理を自動化することが求められている。

課題	課題への対策
システムにおけるサプライチェーンとアーキテクチャの複雑化	情報共有 関心の高い情報のオープンデータ化、脅威情報や各業界・業種にて業界固有の情報を、効率的な対策に役立てる
個社単位での対応の限界	
脆弱性の報告数の増加	自動処理 セキュリティ対策を実施するために行っている判断や対策を、一定の基準で自動的に実施できるようにする

背景：IT資産管理とセキュリティ

情報共有・自動処理を活用した取り組みの例

- 情報共有・自動処理を活用した取り組みの例として、米国で推進している継続的な診断と脅威の緩和(CDM:Continuous Diagnostics and Mitigation)プログラムがある。データ保護管理から資産管理までのシステム構造をダッシュボード化し、セキュリティ対策に活用している。



CDMプログラム

- SCAPなどの活動を背景として、米国で展開されるプログラム
- 複雑化したシステムの構成要素をダッシュボード化し、一括で管理、自動処理を推進

Continuous Diagnostics and Mitigation | CISA
https://www.cisa.gov/cdm を元に作成

複雑化したシステムを統合管理している例であり、目指すべき姿のひとつであると言える。

背景：IT資産管理とセキュリティ

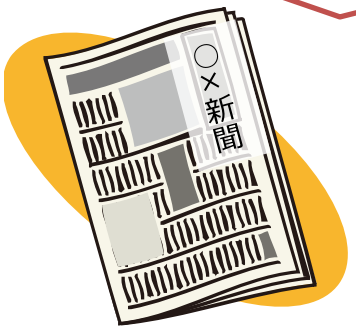
脆弱性という言葉をよく耳にしませんか？

2018年1月
米インテルがCPUの脆弱性対策 半数以上で実施

2019年5月
インテルCPUに脆弱性、情報盗み取られる恐れも

2020年
新型コロナウイルス感染症対策と同期するように、VPN機器の脆弱性が報告され話題に・・・

2021年12月
クラウドやSaaSも狙われるApache Log4j攻撃



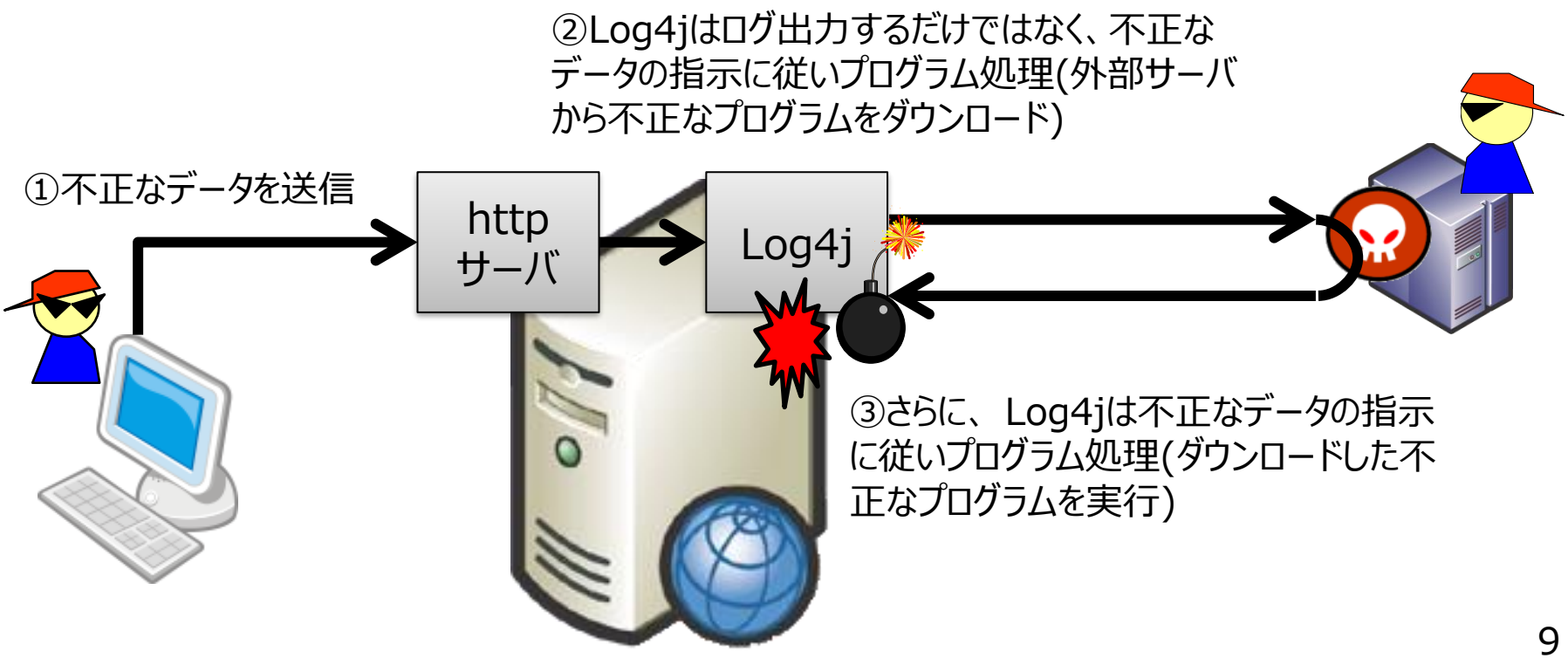
新聞から

ウェブニュースから

背景：IT資産管理とセキュリティ

脆弱性という言葉をよく耳にしませんか?

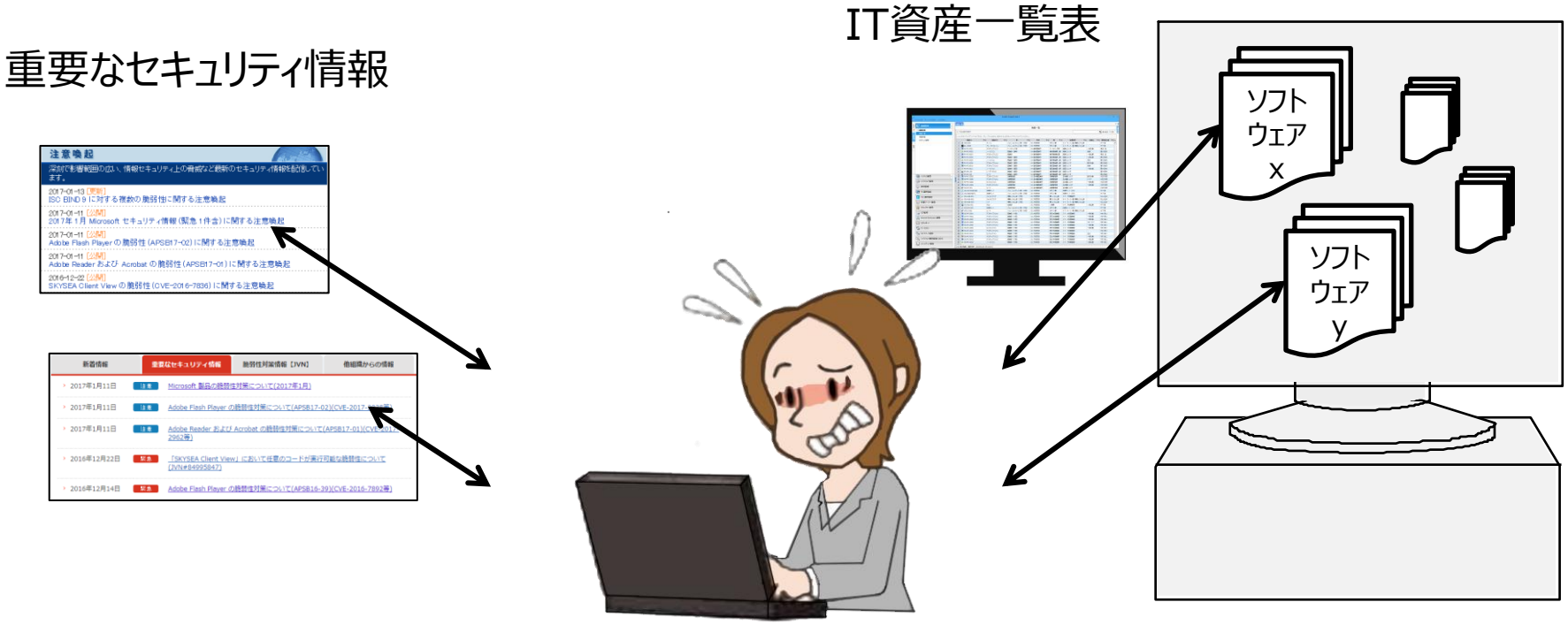
- Log4jの脆弱性?
  - Javaのログ出力ライブラリであるApache Log4jが、ログ出力する際に、入力データを変数としてプログラム処理してしまう問題である。悪用されると、外部サーバから不正なプログラムをダウンロードして実行されてしまうことになる。



背景：IT資産管理とセキュリティ

脆弱性とインストール状況との紐付け

- 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、脆弱性とインストールされているソフトウェアの状況との紐付けを人手で実施している(脆弱性対策と資産管理とが連携できているわけではない)。



情報共有基盤の実証

実証実験の目的

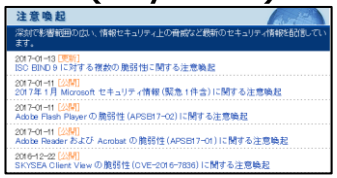
- 情報連携により、人が介在しなくても良い脆弱性対策環境(脆弱性の影響有無の判定など)の実現性を確認する。
  - 重要なセキュリティ情報で使用するソフトウェア名称と、IT資産一覧表で使用するソフトウェア名称の統一を図る。

情報共有基盤の実証

ソフトウェア名称の統一を図るとは

- 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)の実現性を確認する。
  - 重要なセキュリティ情報で使用するソフトウェア名称と、IT資産一覧表で使用するソフトウェア名称が同じものであるという前提で運用できる情報共有基盤を整備する。

重要なセキュリティ情報
(MyJVN)



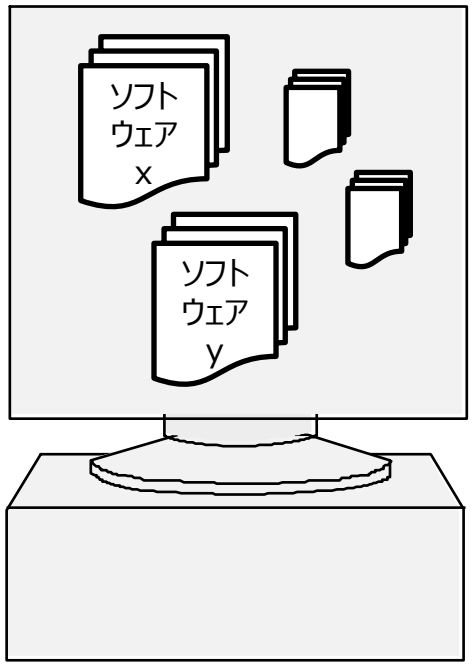
重要なセキュリティ情報に
記載されているソフトウェア名
- 製品ABC

同じ?

同じ

IT資産一覧表に登録
されているソフトウェア名
- 製品ABC

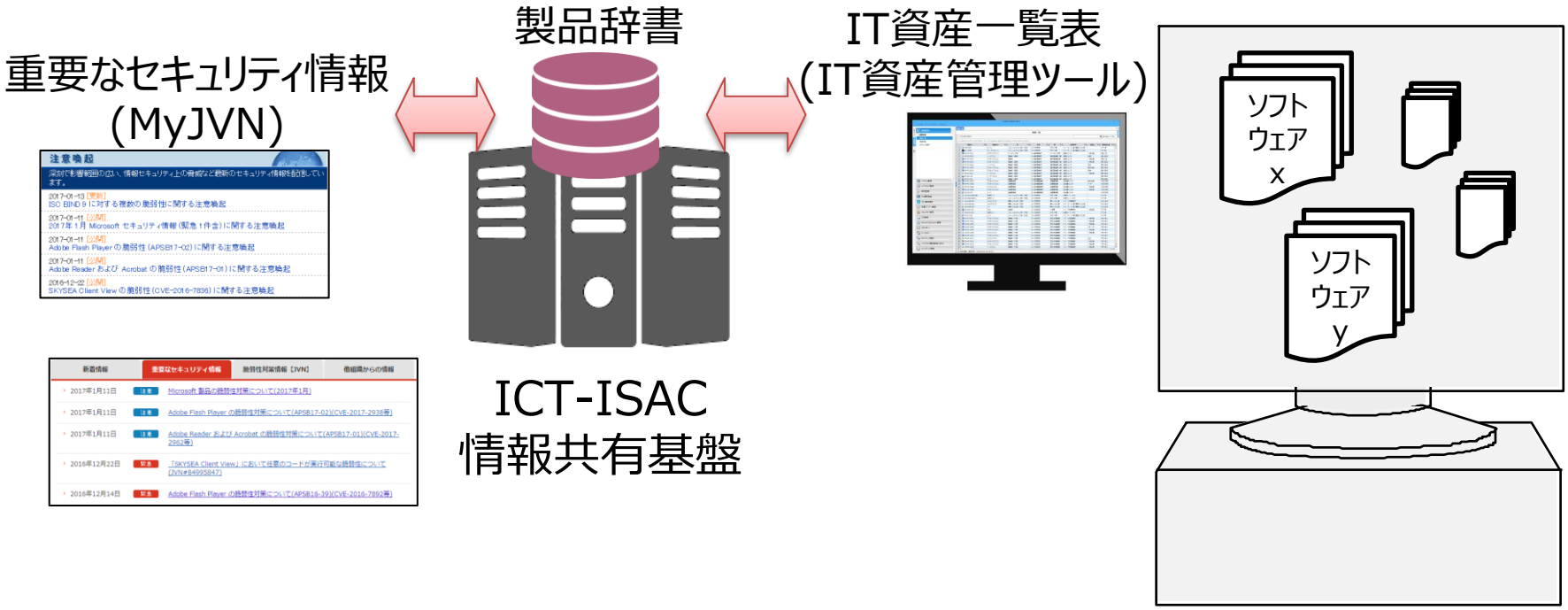
IT資産一覧表
(IT資産管理ツール)



情報共有基盤の実証

ソフトウェア名称の統一を図るために

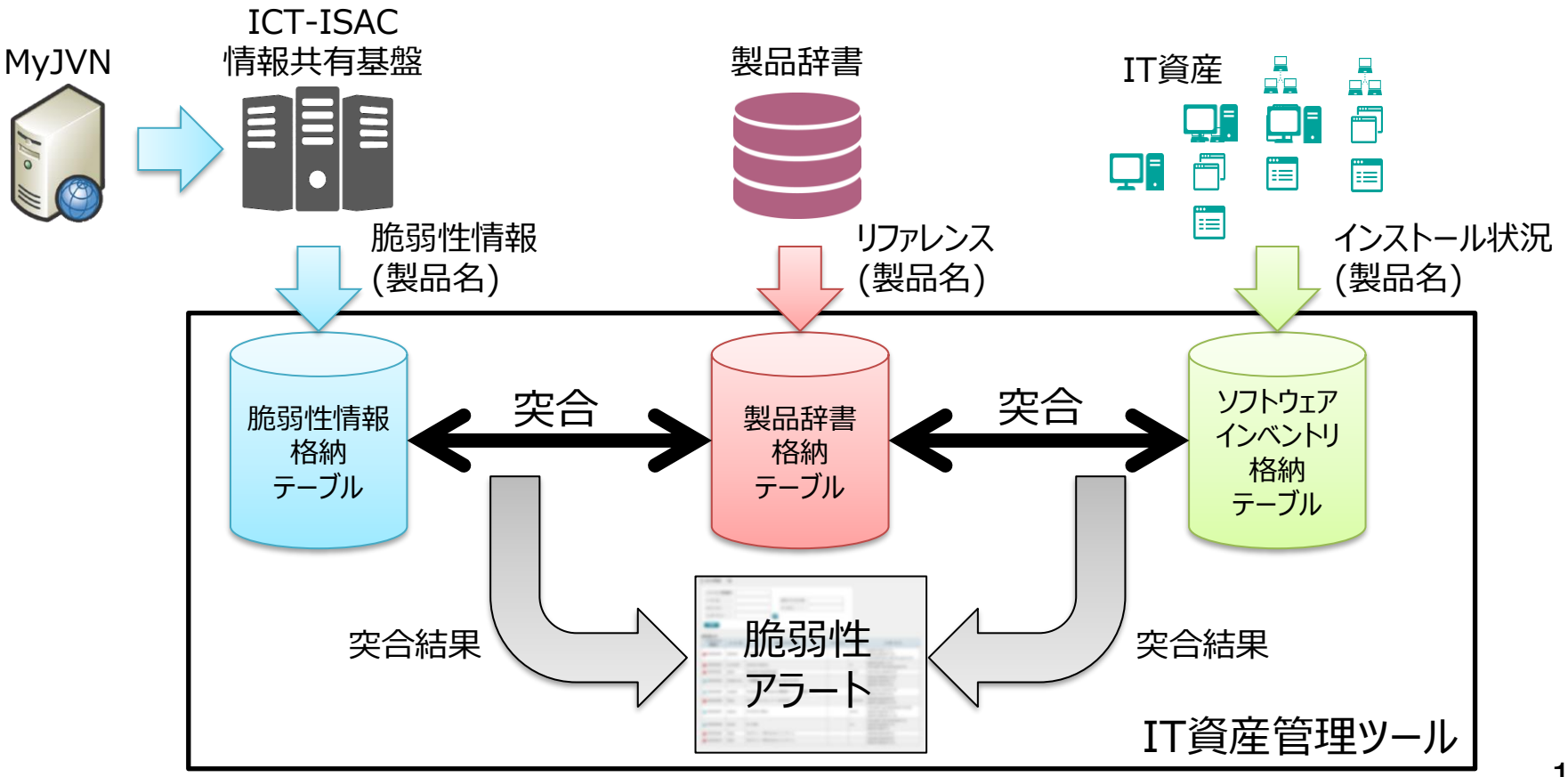
- 情報連携により、人が介在しなくても良い脆弱性対策環境(脆弱性の影響有無の判定など)の実現性を確認する。
  - ソフトウェア名称の統一のためのリファレンス(製品辞書)を利用した重要なセキュリティ情報とIT資産一覧表との連携



情報共有基盤の実証

2020年度における連携の概要

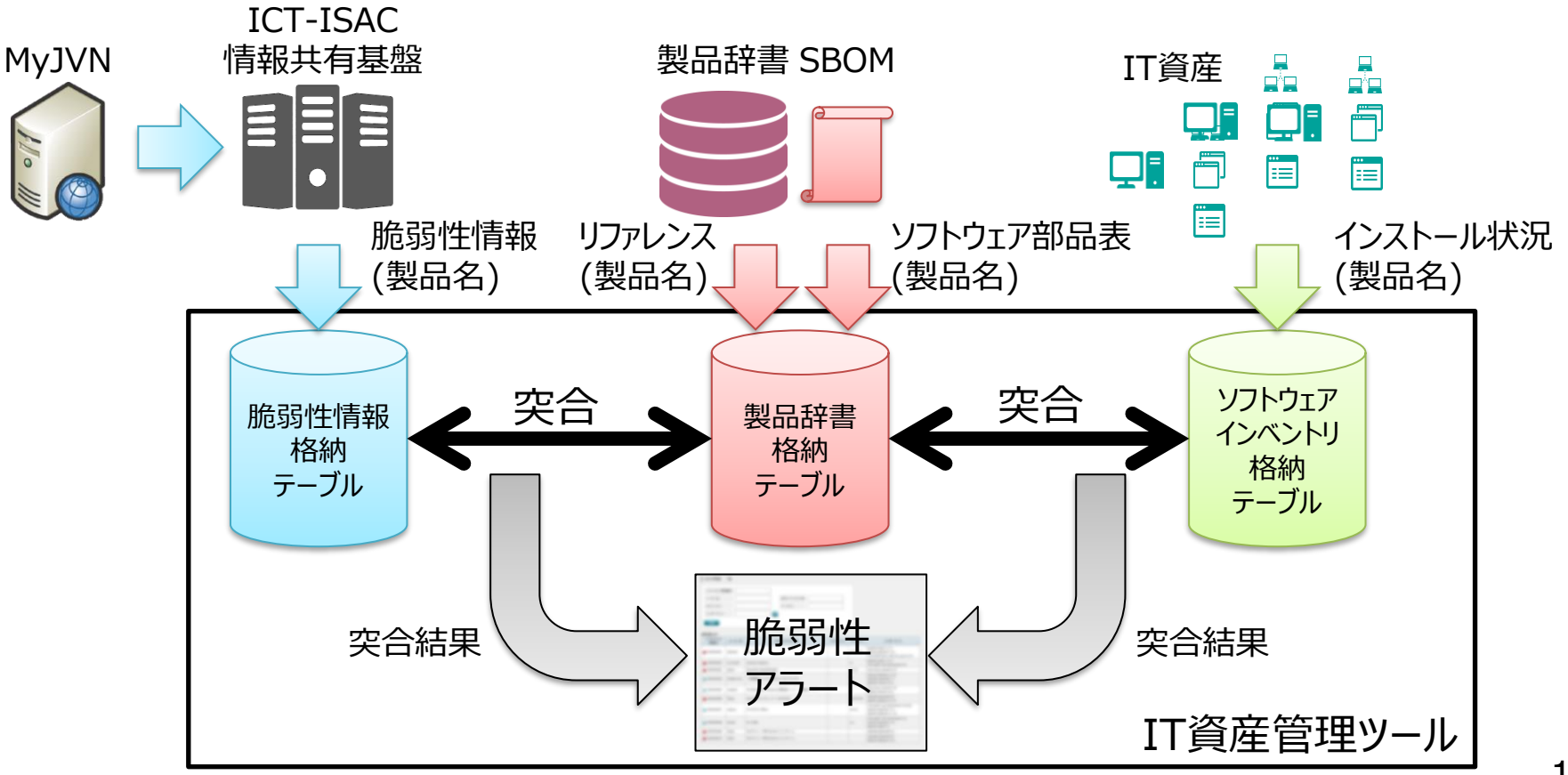
- ソフトウェア名称の統一のためのリファレンス(製品辞書)を利用した連携



情報共有基盤の実証

2021年度における連携の概要

- ソフトウェア名称の統一のためのリファレンス(製品辞書)を利用した連携
- ソフトウェア部品表(SBOM:Software Bill of Materials)を利用した連携

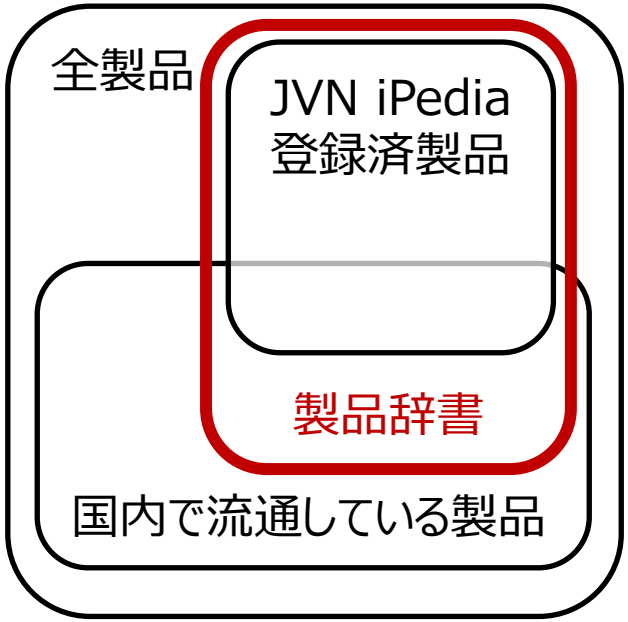


情報共有基盤の実証

製品辞書について

- 国際標準であるソフトウェア資産管理 ISO/IEC 19770シリーズを活用
  - 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規格であるISO/IEC 19770-2 ソフトウェア識別子(SWID:Software identification tag)
    - ソフトウェア名称の統一のためのリファレンスとして
    - ソフトウェア部品表(SBOM)の記述形式として

- 実証実験で使用した製品辞書は、MyJVN(JVN iPedia)に登録されている製品のソフトウェア名称＋国内で流通している製品のソフトウェア名称から構成



情報共有基盤の実証

脆弱性情報について

- 業界標準であるOASIS(Organization for the Advancement of Structured Information Standards Group)のCSAFとSTIXを活用
  - CSAF:Common Security Advisory Framework
    共通セキュリティアドバイザリ記述形式
  - STIX:Structured Threat Information eXpression
    脅威情報構造化記述形式

- 実証実験では、脆弱性の影響を受けるソフトウェアを精査するために
  - 該当するバージョンを記述
  - 該当するバージョン範囲を記述

- 実証実験では、脆弱性の対策判断を支援するために
  - 技術的な側面からの影響(なりすまし、改ざん、情報漏えい、サービス拒否、権限昇格など)を記述
  - 社会的な側面からの影響(影響する分野、影響するシステム区分など)を記述

情報共有基盤の実証で得られた知見

IT資産管理ツールベンダからの視点で整理

- IT資産管理ツールベンダ 4社へのヒアリング
  - 情報収集に関する作業性の改善
  - ソフトウェア資産の特定に関する作業性の改善
  - 製品辞書及びソフトウェア部品表の利用
  - 技術的と社会的な側面からの影響の記述付与

情報共有基盤の実証で得られた知見

情報収集に関する作業性の改善

- 脆弱性の影響確認を行うにあたってソフトウェア部品表(SBOM)を利用することで、今まで見えなかった関連ソフトウェア(主にカスタムアプリケーション)の脆弱性を把握できる。
- 加えて、資産管理ツールによる脆弱性有無の運用観点における重要な可視化を可能とし、システム運用者の業務負荷軽減と脆弱性対策が完了するまでの時間を短縮し、情報漏洩リスクを下げることができると考える。

- 対策することでバージョンが上がるソフトウェアについては問題はないが、それ以外のソフトウェアについては、対策を行ったかどうかの判定が機械的にできない。

情報共有基盤の実証で得られた知見

ソフトウェア資産の特定に関する作業性の改善

- 脆弱性が公開された際に、多くの場合にはまず社内でどれくらいの影響があるかを確認、分析する必要がある。その際に、ソフトウェア部品表(SBOM)の活用や技術的と社会的な側面からの影響情報を活用することによって効果的かつ効率的な脆弱性対策を実現することが可能になる。
- ソフトウェア部品表(SBOM)を利用することで、ソフトウェアの中に含まれるコンポーネントレベルでの脆弱性をIT資産管理ツールで検知できるようになった。

- インベントリツールで検出が難しいソフトウェア(インストーラ形式ではなく、EXE本体を起動させるタイプのソフトウェアなど)に含まれる脆弱性の検知ができない。

情報共有基盤の実証で得られた知見

製品辞書及びソフトウェア部品表の利用

- ソフトウェア部品表を利用することで、ソフトウェアの中に含まれるコンポーネントレベルでの脆弱性をツール側で検知できるようになった。これにより従来よりも幅広い範囲の脆弱性を取り扱うことが可能となった。
- 製品辞書及びソフトウェア部品表(SBOM)を活用する方向性については、非常に有効であると考える。特に、ソフトウェア部品表については、今まで見えなかった関連ソフトウェア(主にカスタムアプリケーション)の脆弱性を把握するとともに、システム内に存在する脆弱性に対して、効果的な脆弱性対策を実現できる。

- 精度の高い情報共有基盤を実現するためには、製品辞書及びソフトウェア部品表の統一仕様に基づいた製品識別情報の登録が重要である。

情報共有基盤の実証で得られた知見

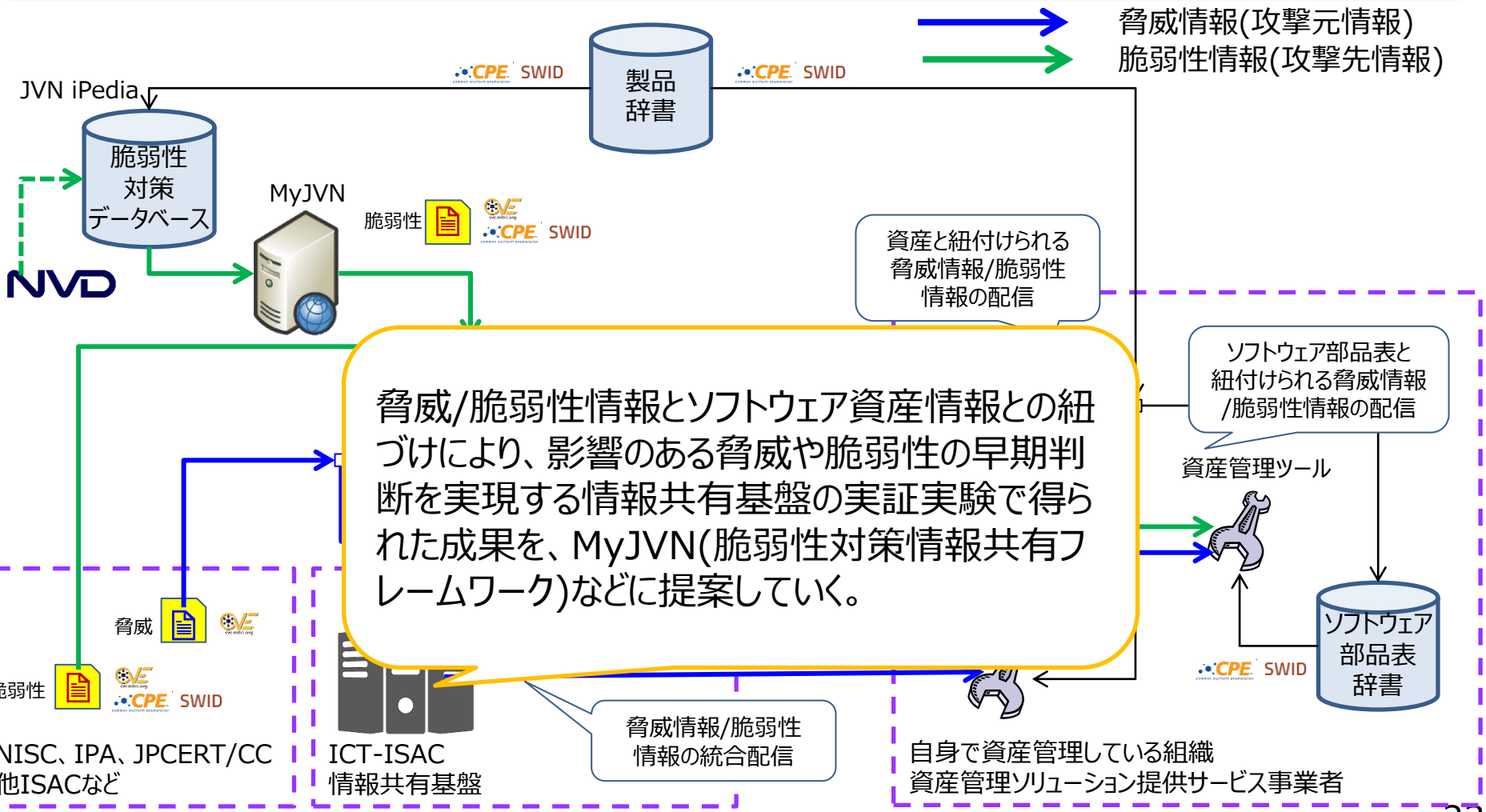
技術的／社会的な側面からの影響の記述付与

- 影響の記述が付与されることにより、自社への影響を確認するための判断基準として使え、検討時間の時間短縮に繋がると思われる。
- 設定可能な値を明確に定義したことで、機械的な取り込みが容易となった。IT資産管理ツール側でも容易に情報を検索/絞込できるようになった。
- 業界分野に特化した攻撃手法、具体的な攻撃者、攻撃の対象となっているシステムなど、より優先度の高い問題は何かを適切に判断が出来るようになると考える。

- 深刻度等、脆弱性情報と重複する情報もあるため、重複する情報に揺らぎがあった場合、どちらを正として扱えば良いか、判断が難しい。
- 詳細情報を多く取り扱えるようになったため、情報提供者側の負荷が高まり、枠組を用意したもの、運用されない事態になる恐れがある。

情報共有基盤の実証

今後の活動



Collaborate
together
to make our
Internet
secure.

ICT-ISAC JAPAN
ICT Information Sharing And Analysis Center Japan