脅威/脆弱性情報と資産情報との連携による情報共有基盤の実証について

2022年3月4日

寺田　真敏(ICT-ISAC情報共有WG主査／株式会社日立製作所)

ICT-ISAC JAPAN
ICT Information Sharing And Analysis Center Japan

脅威/脆弱性情報と資産情報との連携

きっかけ

- 脆弱性を取り巻く環境の変化
  脆弱性対策には、システム、資産、データ、機能に対するサイバーセキュリティリスクの管理(リソース把握・管理)が必要であることが再認識された。

  - 振り返り 2014年

    4月　OpenSSLの情報漏えいを許してしまう脆弱性 ～Heartbleed問題
    Apache Strutsの任意のコード実行を許してしまう脆弱性

    9月　GNU bashの脆弱性 ～shellshock問題～

    10月　SSL通信の暗号文の解読を許してしまう脆弱性 ～POODLE問題～

  - 振り返り 2017年

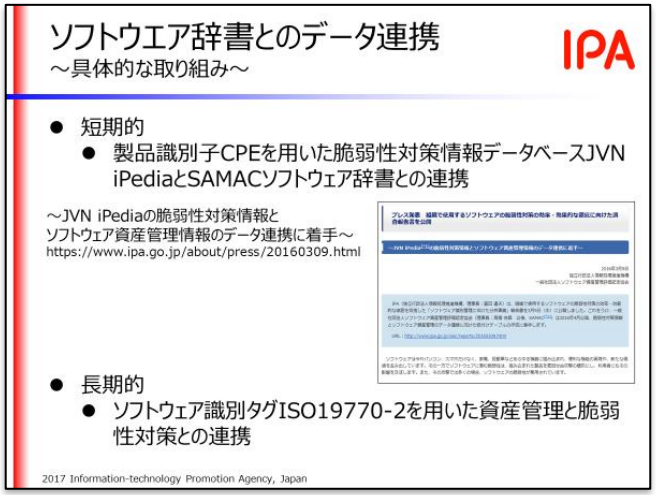
    3月　Apache Struts 2の任意のコード実行を許してしまう脆弱性

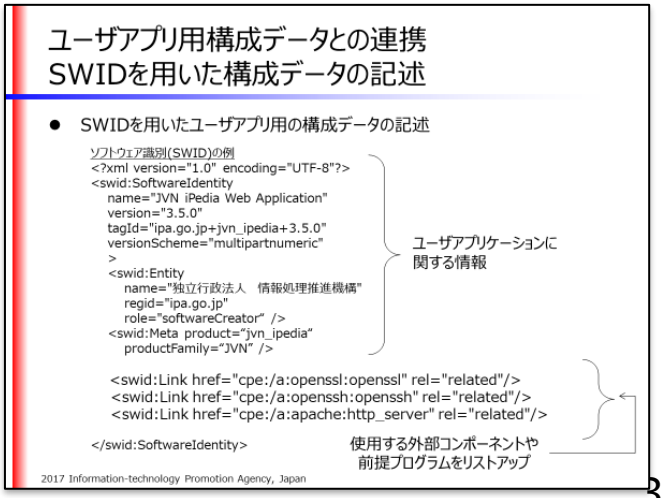
    5月　ランサムウェアWanna Cryptorの流布
    2017年3月にセキュリティ更新プログラムがリリースされた「MS17-010：
    Windows SMBv1の任意のコード実行を許してしまう脆弱性」を悪用

脅威/脆弱性情報と資産情報との連携

課題解決のためのアプローチ

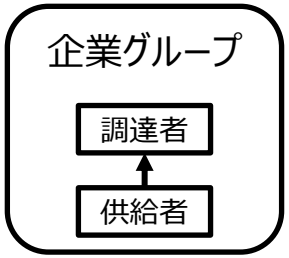
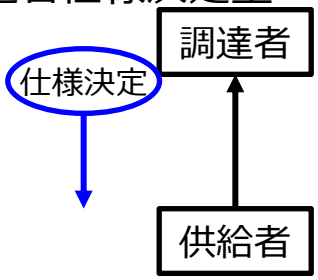
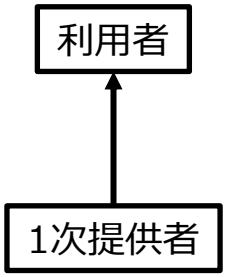
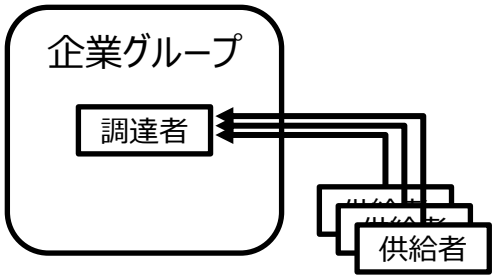
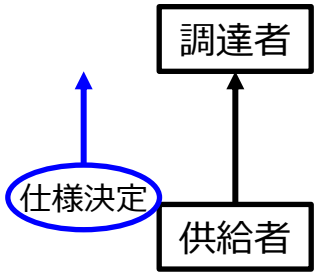
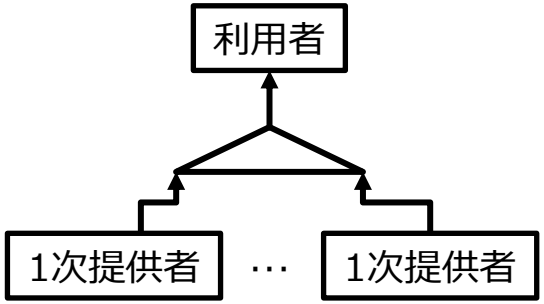
- 資産情報と脆弱性対策情報との連携
  - 短期的：製品識別子CPEを用いた脆弱性対策情報データベースJVN iPediaとSAMACソフトウェア辞書との連携
  - 長期的：ISO/IEC 19770-2 ソフトウェア識別子(SWID)を用いた資産管理と脆弱性対策との連携
- 資産管理と脆弱性管理との連携拡大 (SBOMに近い概念を提案)
  - カスタムアプリケーションと、カスタムアプリケーションで使用している外部コンポーネントや前提プログラムとを把握し管理





脅威/脆弱性情報と資産情報との連携

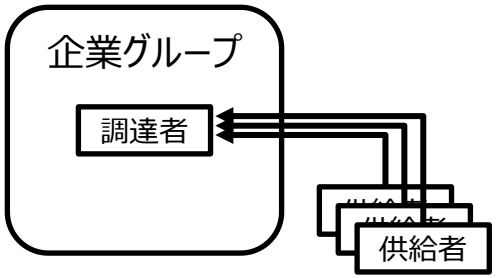
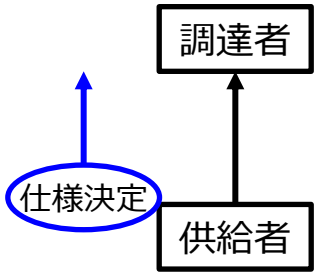
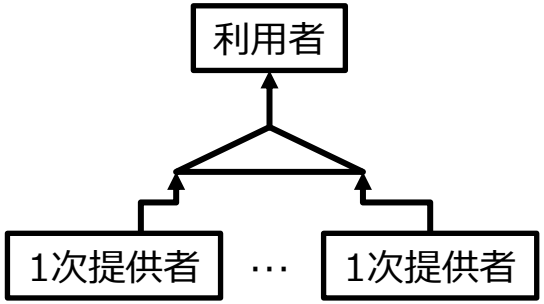
ソフトウェアサプライチェーンにおける変化と課題

ソフトウェア開発の水平分業化への変化	供給部品のソフトウェア仕様決定者の変化	製品・サービスをユーザが組合せて利用する形態への変化
垂直統合型 	調達者仕様決定型 	従来型 
 水平分業型	 供給者仕様決定型	 ユーザ組合せ(サービス連携)型

[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

脅威/脆弱性情報と資産情報との連携

ソフトウェアサプライチェーンにおける変化と課題

ソフトウェア開発の水平分業化への変化	供給部品のソフトウェア仕様決定者の変化	製品・サービスをユーザが組合せて利用する形態への変化
●トレーサビリティ確保が重要であるが、サプライチェーンが複雑になり、部品供給元トレースが困難になる。 ●情報漏えい、不正プログラムの埋込みの危険性が増大する。	●調達者からの仕様決定や不具合修正の優先付け等の制御が利かなくなる。 ●通信におけるセキュリティ問題発生リスクが増大する。	●利用時の品質を出荷時にすべて想定し、検査することが困難になる。 ●製品・サービスを提供する複数企業の責任所在が曖昧になる。 ●利用者が連携時のリスクを十分に理解できていない。
		
水平分業型	供給者仕様決定型	ユーザ組合せ(サービス連携)型

[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

脅威/脆弱性情報と資産情報との連携

ソフトウェアサプライチェーンにおける変化と課題

- 製品・サービスをユーザが組合せて利用する形態への変化における課題と対応

課題	対応
利用時の品質を出荷時にすべて想定し、検査することが困難になる。	ユーザは利用時の品質を把握できない。 ➢ 対応できていることと、できていないことを明確化するという点で設計品質の見える化が必要
製品・サービスを提供する複数の企業の責任の所在が曖昧になる。	少なくとも責任範囲の明確化が必要である。 ➢ 責任を持てる範囲と、持てない範囲を明確化するという点で設計品質の見える化が必要
利用者が連携時のリスクを十分に理解できていない。	ユーザは利用時の品質を把握できない。 ➢ 接続可否や警告を通知するという点で設計品質の見える化が必要

[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

脅威/脆弱性情報と資産情報との連携

品質の見える化

- SBOM(Software Bill of Materials、ソフトウエア部品表)
  - 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中で、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。

脅威/脆弱性情報と資産情報との連携

品質の見える化

- 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

脅威/脆弱性情報と資産情報との連携

品質の見える化

- ソフトウェアにおける具体例
  - ソフトウェア部品表(SBOM：Software Bill of Materials)
    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

脅威/脆弱性情報と資産情報との連携

品質の見える化

- 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)
  - 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立
  - 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改善
  - 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

[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/

脅威/脆弱性情報と資産情報との連携

品質の見える化

- 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

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] 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/

脅威/脆弱性情報と資産情報との連携

ICT-ISAC Japan での取組み

- 1st step (2016～2018) 多層防御としての情報活用
  - 脅威情報
  - 脅威情報(IPアドレス、ドメイン、URL、ハッシュ値)を交換するための場として、STIX v1/TAXII v1環境であるtaxii.ict-isac.jpをSoltraを使用して構築し、試行運用した。
  - 総務省「サイバー攻撃への集団防御に向けた情報共有基盤に関する実証事業」との連携

- 2nd step (2019～) 多層防御としての情報活用
  - (脅威情報＋脆弱性情報)*資産管理連携
  - 脅威情報(IPアドレス、ドメイン、URL、ハッシュ値)と脆弱性情報とを関連付けて活用する、資産管理と連携するための場として、STIX v1+v2/TAXII v1環境であるtaxii.ict-isac.jpをOpenTAXIIを使用して構築し、試行運用中
  - 総務省「ソフトウェア脆弱性を狙ったサイバー攻撃の防御に向けた情報共有基盤に関する実証実験」との連携

脅威/脆弱性情報と資産情報との連携

品質の見える化との連携

サイバーセキュリティ情報共有推進事業

5

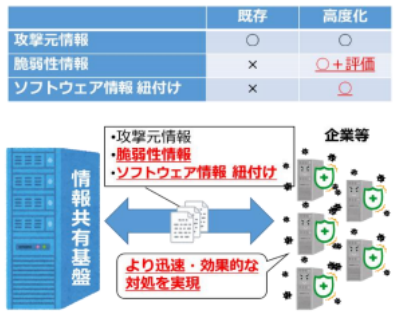
①重要インフラ事業者等がサイバー攻撃情報を共有するための情報共有基盤において、脆弱性情報を新たな共有対象とするとともに、ソフトウェア資産情報と組み合わせることで、迅速かつ効果的な対処を実現
②日々公開される多種多様な脆弱性情報について、AIを活用した高精度な深刻度・信頼度評価を行い、結果を情報共有基盤で共有することにより、迅速かつ効果的な対処を実現
③総合通信局を中心として所管事業者等との情報共有等を実施する体制を構築

【R３要求額：359百万円】

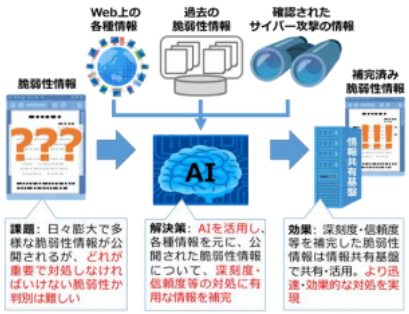
【これまでの取組・現状】
○平成29年度までは、情報共有の取組の推進を支援するため、情報共有基盤による機械処理可能な形式で攻撃者情報を共有する実証事業を実施。
○令和元年度及び２年度は、①情報共有基盤を高度化し、攻撃者情報だけでなく、脆弱性情報とその影響を受けるソフトウェアの情報を共有する実証、②機械学習（AI）を活用し、多種多様な脆弱性情報の深刻度・信頼度を評価する技術の実証、及び①、②の連携のための検証を実施するとともに、③総合通信局を中心とした地域における情報共有体制の確立に向けた取組を実施。

【目標・成果イメージ】
○以下により、サイバー攻撃による被害の甚大化を防ぎ、情報通信インフラをはじめとする我が国社会・経済の強靭性を向上させる。
・通信事業者や放送事業者をはじめとする産業界における関係者間の情報共有促進によるサイバーセキュリティ対策の強化
・総合通信局を中心とした地域の情報共有体制の構築

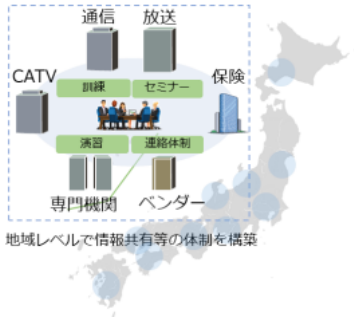
①情報共有基盤の高度化



②深刻度・信頼度評価の高精度化



③総通局を中心とした情報共有体制



[出典]　総務省サイバーセキュリティ
https://www.soumu.go.jp/main_content/000711459.pdf

脅威/脆弱性情報と資産情報との連携

品質の見える化との連携

経済産業省

資料4

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

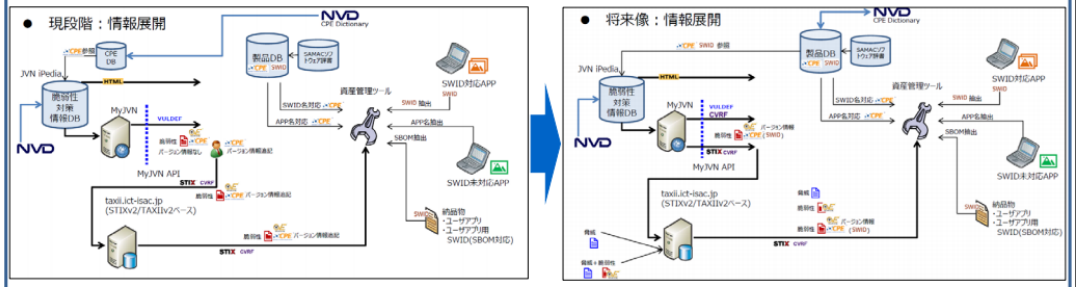
令和元年９月５日
経済産業省　商務情報政策局
サイバーセキュリティ課

脅威情報や脆弱性情報の一元管理・共有への取組

- 脅威情報や脆弱性情報を一元管理・共有することで、各社の情報システムやサービスに対する迅速かつ効率的なセキュリティ対策・対応が進むことが期待される。
- 民間団体（ICT-ISAC、金融ISAC、Software ISAC等）を中心に、上記取組が進められている。

（取組の一例）ICT-ISAC

ICT-ISACでは、総務省の実証事業において脅威情報と脆弱性情報の共有を機械化し、迅速に処理することによりサイバー攻撃から防御する取組を行っている。



サイバー攻撃に関するJVN iPedia情報をSTIX/TAXII形式で交換する情報共有基盤を構築

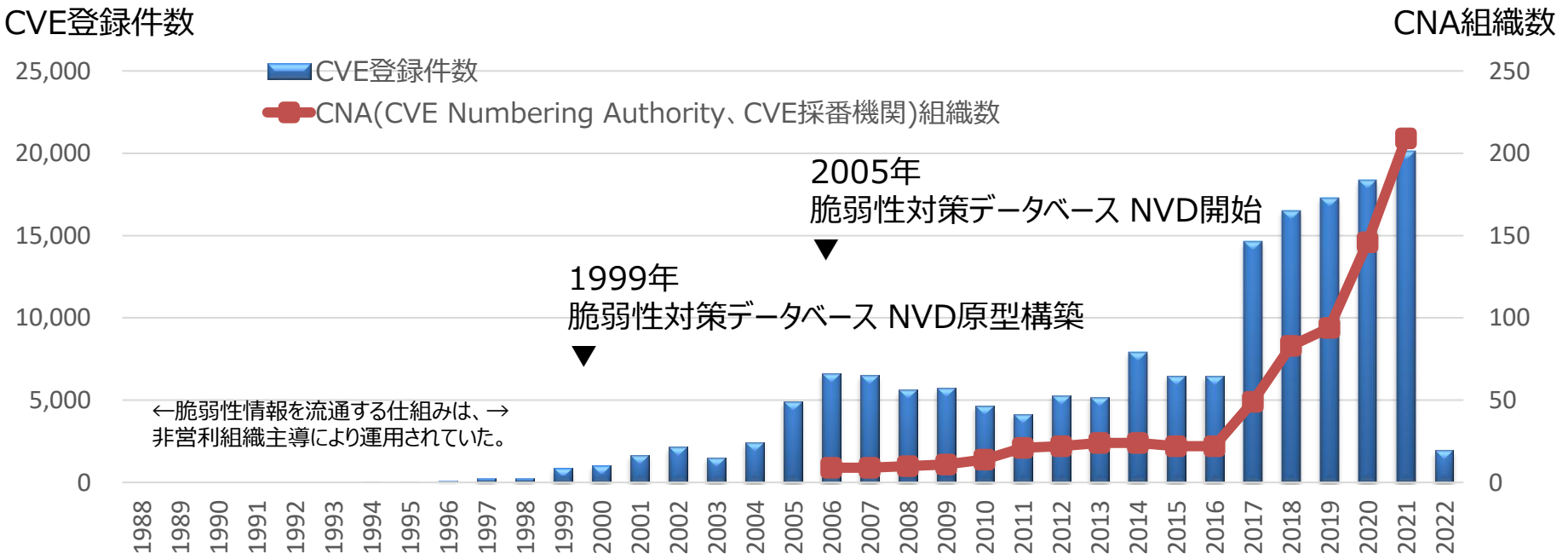
24

[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

情報共有基盤の実証

【 課題1 】脆弱性情報の件数は増加傾向

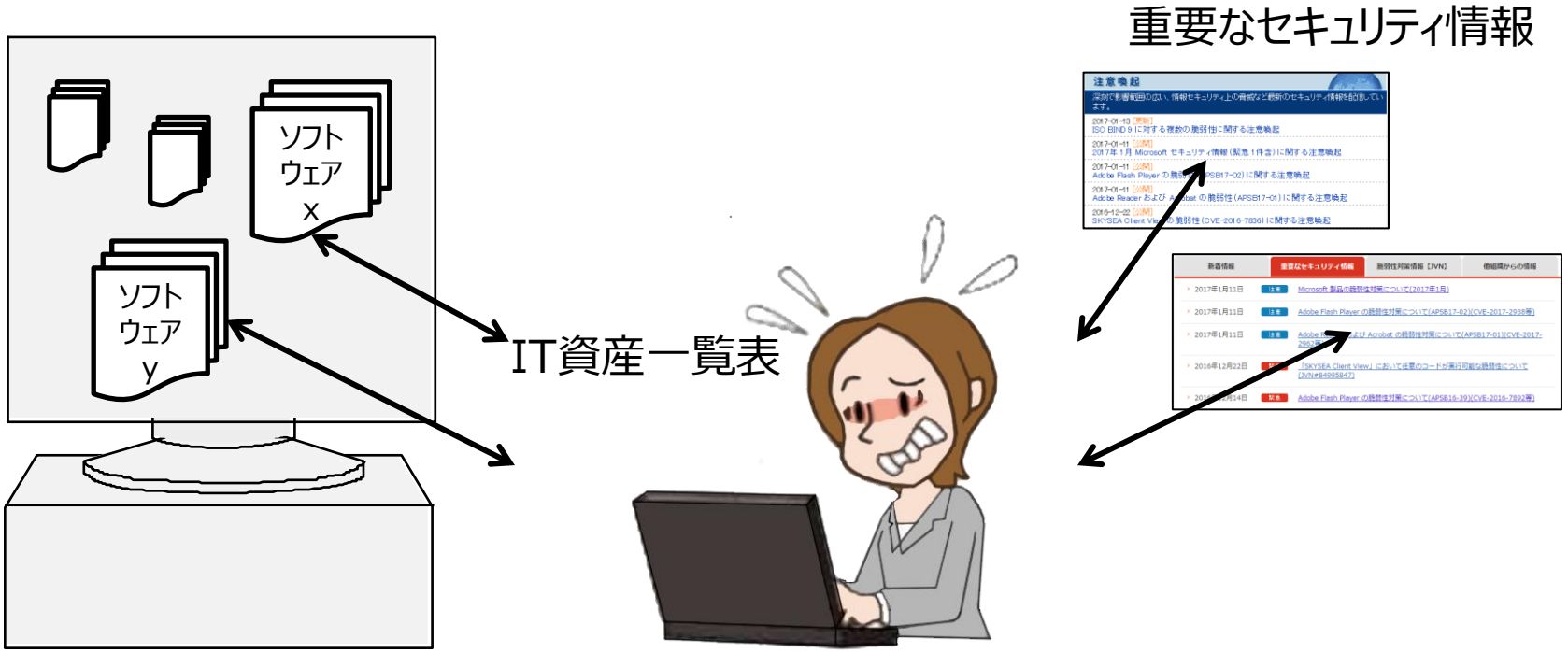
- 米国脆弱性対策データベース(NVD: National Vulnerability Database)に登録されている件数は?
  - 脆弱性を分担協力して登録する組織(脆弱性登録組織)の増加と共に増加している。



情報共有基盤の実証

【 課題2 】インストール状況と脆弱性との紐付けは人手で実施

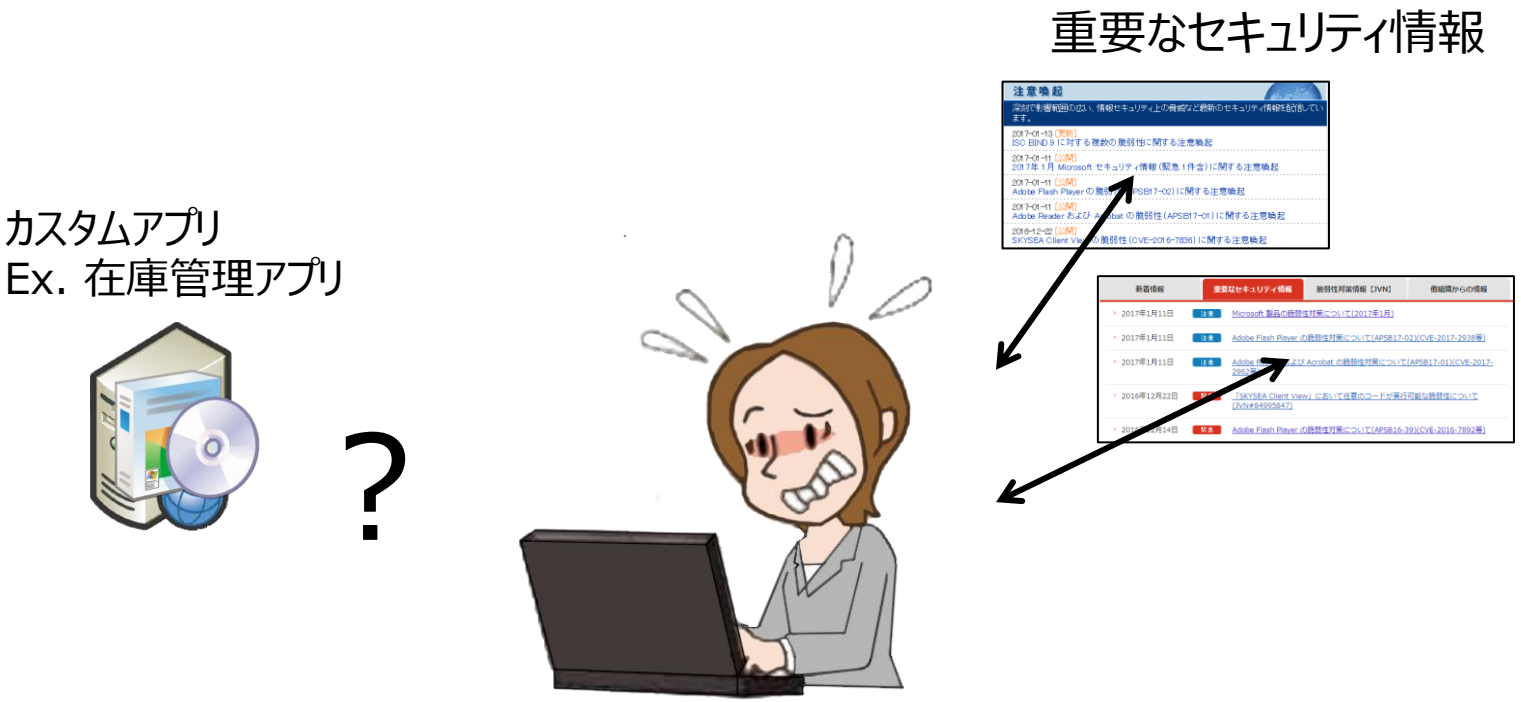
- 重要なセキュリティ情報が発信されるたびに、手作業でIT資産一覧表を検索して、影響範囲の調査をしていませんか?
  - 多くの場合、インストール状況と脆弱性との紐付けを人手で実施している(資産管理と脆弱性対策とが連携できているわけではない)。



情報共有基盤の実証

【 課題3 】カスタムアプリ管理は整備途上

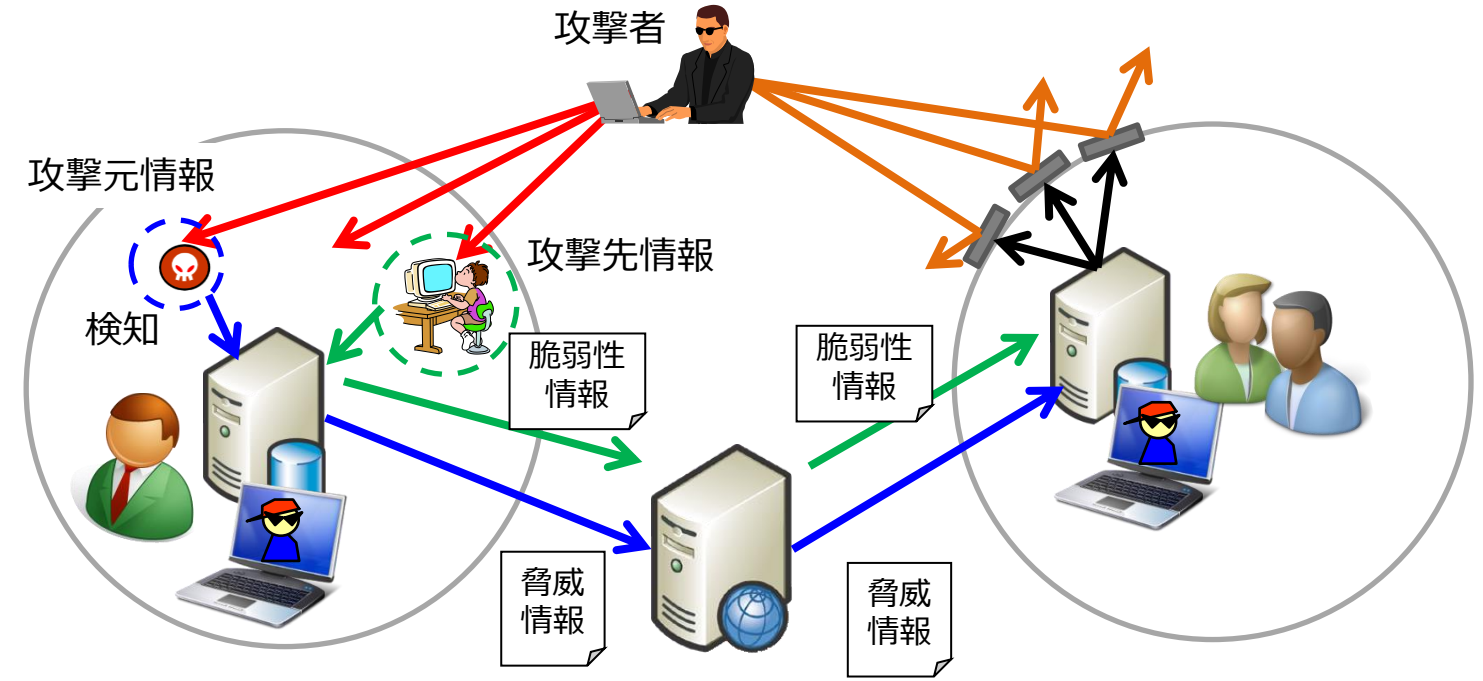
- 重要なセキュリティ情報が発信されたときに、カスタムアプリ(SIで開発した業務アプリケーションなど)の影響範囲を調査していますか?
  - 多くの場合、カスタムアプリ(SIで開発したアプリケーションなど)は、資産管理や脆弱性管理の対象に含まれていない。



情報共有基盤の実証

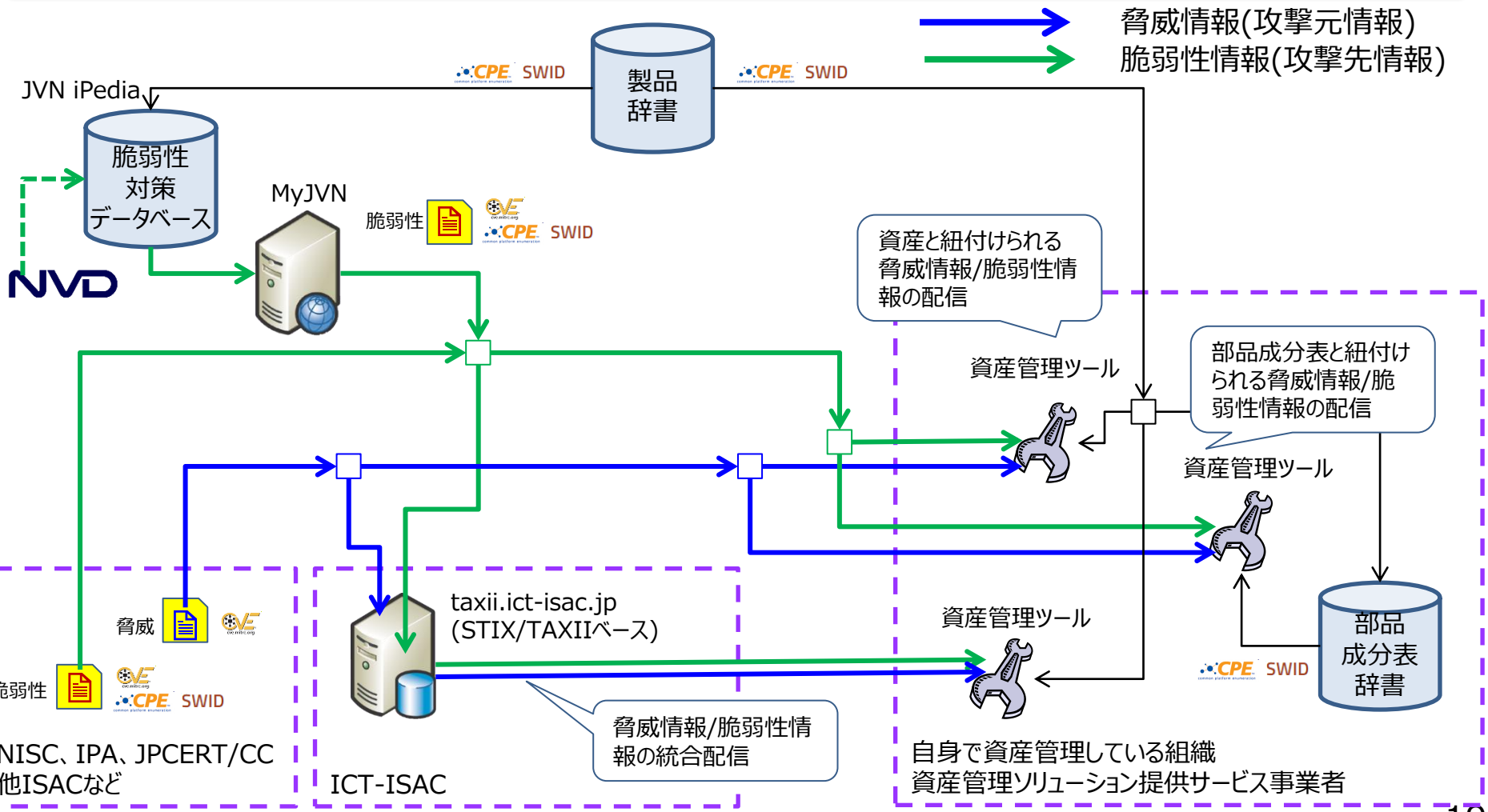
【 課題4 】脅威情報と脆弱性情報の連携

- 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これら情報を資産や部品成分表(SBOM)と紐付けて活用する。



情報共有基盤の実証

多層防御としての(情報活用＋対策)と想定する将来像

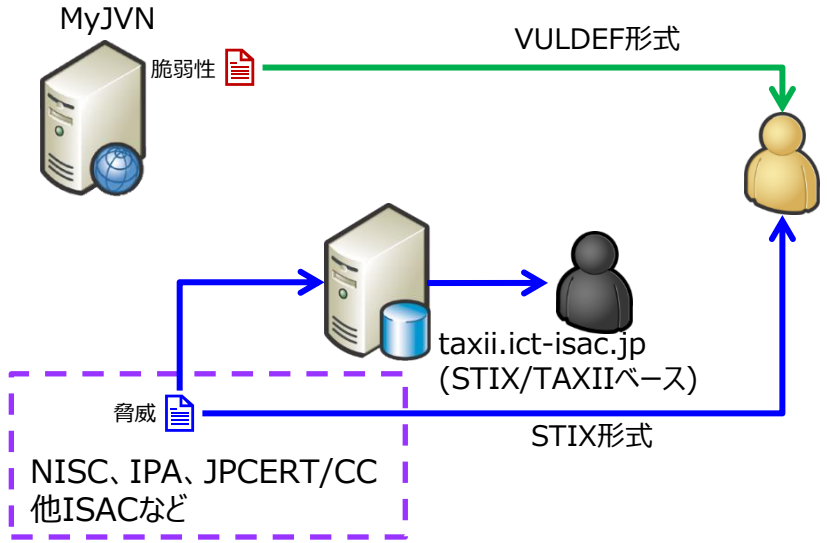


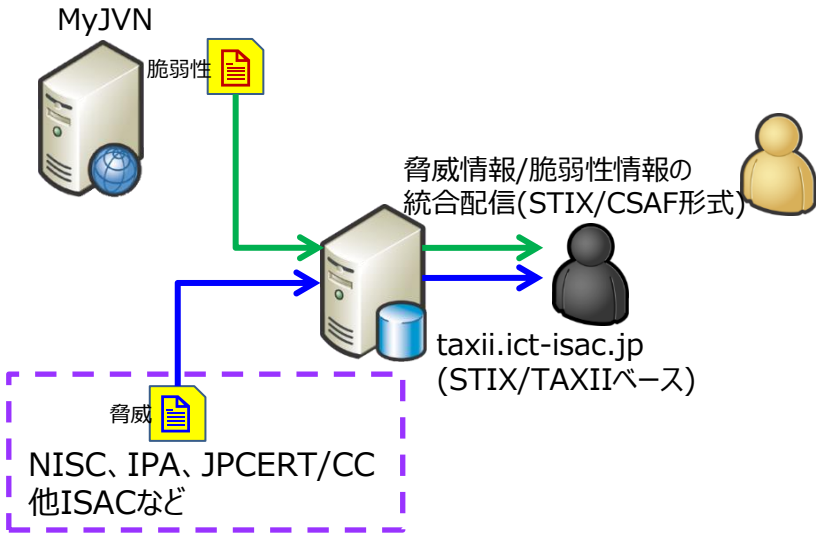
情報共有基盤の実証

①脅威/脆弱性情報の統合配信【課題1】【課題4】

- 脅威などの攻撃元情報と脆弱性などの攻撃先情報が、個別に情報展開
  - 一つの情報展開ストリームに攻撃元/攻撃先情報を重畳させることで、ここにアクセスさえすればという情報共有基盤を作ることができる。

現状	実証実験
● 脅威情報と脆弱性情報を異なるフォーマット、いろいろなサイトから受信している。	● 脅威情報と脆弱性情報を同じフォーマット、ひとつのサイトから受信できる。





情報共有基盤の実証

①脅威/脆弱性情報の統合配信【課題1】【課題4】


```
{
  "type": "bundle",
  "id": "bundle--63c46abd-9f5a-472a-8b10-c51208c10000",
  "objects": [
    {
      "type": "jvn-jp-sdo",
      "spec_version": "2.1",
      "id": "jvn-jp-sdo--ac97aae4-83f1-46ca-a351-7aeb76678189",
      "created": "2021-11-15T09:16:08.989000Z",
      "modified": "2021-11-15T09:16:08.989000Z",
      "name": "JVN CSAF embedded in STIX",
      "extensions": {
        "extension-definition--b2440624-45a6-11ec-81d3-0242ac130003":
              {"extension_type": "new-sdo"}
      },
      "document": {
        "lang": "ja",
        "title": "[example] Information Disclosure Vulnerability in Sample Inc.
              Security Information DBX V3.2",
        "category": "Security Advisory“
```


CSAF(Common Security Advisory Framework)形式の記述


```
      }
    }
  ]
}
```


STIX 2.1(2021.6)
標準仕様
脅威情報の記載

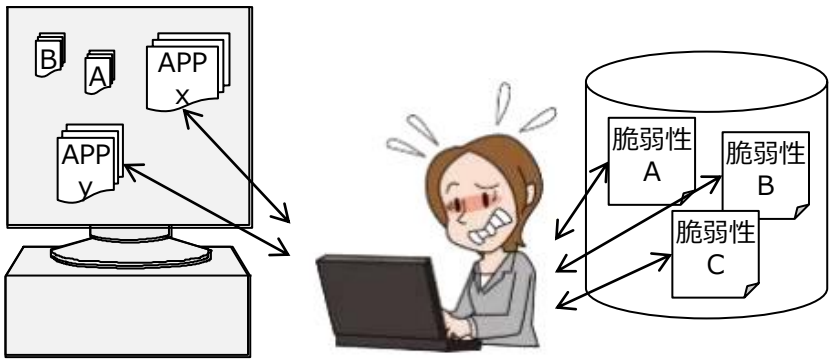
STIX 2.1(2021.6)
STIX Extension Definition
脆弱性情報の記載

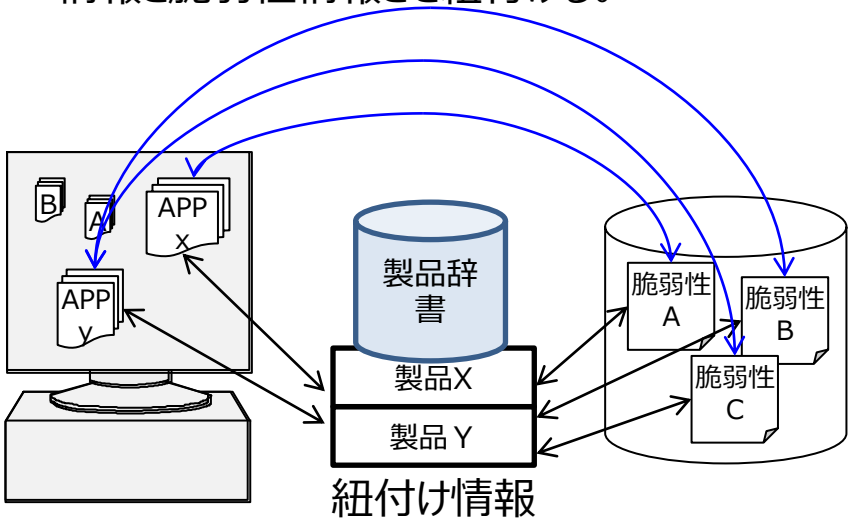
情報共有基盤の実証

②資産と紐付けられる脅威/脆弱性情報の配信【課題2】【課題4】

- 攻撃元/攻撃先情報のいずれも、組織の資産との紐づけを想定していない。
  - 資産管理ツールと連携させることで、攻撃元/攻撃先情報の選別だけではなく、影響有無などの対策につなげることができる。

現状	実証実験
● 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。	● 製品辞書(製品識別子とインストール名との対応表)を試行し、インストール状況を把握できる情報と脆弱性情報とを紐付ける。





情報共有基盤の実証

②資産と紐付けられる脅威/脆弱性情報の配信【課題2】【課題4】

- 製品識別子とインストール名との対応リファレンス表となる製品辞書を試行する。

製品辞書

インストール名一覧
Ex. SAMAC ソフトウエア辞書

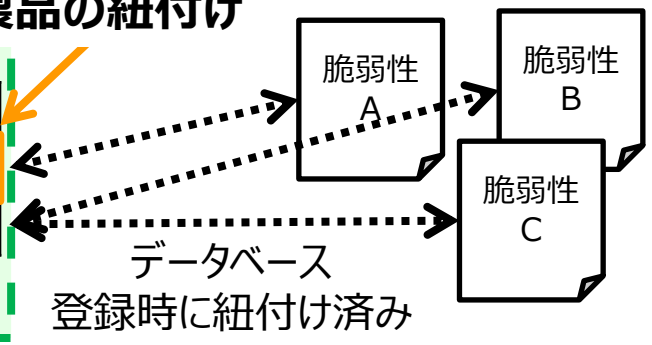
SAMACソフトウエア辞書の既存登録項目(9項目)				連携用項目(1項目)
sw_id	sw_vendor	sw_name	その他項目	CPE
・・・	・・・	Adobe Acrobat 8.2.0 Professional	・・・	cpe:/a:adobe:acrobat
・・・	・・・	Adobe Acrobat 8.2.0 Standard	・・・	cpe:/a:adobe:acrobat
・・・	・・・	Adobe Acrobat 8.2.1 - CPSID_50570	・・・	cpe:/a:adobe:acrobat
・・・	・・・	Adobe Acrobat 8.2.1 Professional	・・・	cpe:/a:adobe:acrobat
・・・	・・・	Adobe Acrobat 8.2.1 Standard	・・・	cpe:/a:adobe:acrobat
・・・	・・・	Adobe Acrobat 9.3.0 - CPSID_52073	・・・	cpe:/a:adobe:acrobat

ソフトウエアの脆弱性情報データベース
Ex. MyJVN

製品識別子CPEを用いた製品の紐付け

ソフトウエア名	CPE
Adobe Acrobat	cpe:/a:adobe:acrobat
製品Y	cpe:/a:y:yyy

JVN製品データベース



情報共有基盤の実証

②資産と紐付けられる脅威/脆弱性情報の配信【課題2】【課題4】

- 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、ソフトウエアの名称を、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

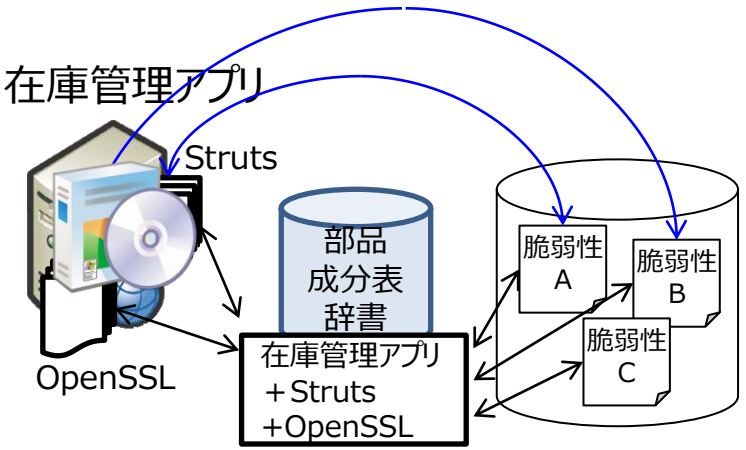
cpe:/{種別}:{ベンダ}:{製品}:{バージョン}
:{アップデート}:{エディション}:{言語}

種別：h=ハードウェア、o=OS、a=アプリケーション

情報共有基盤の実証

③部品成分表と紐付けられる脅威/脆弱性情報の配信【課題3】【課題4】

- カスタムアプリの扱いや部品成分表(SBOM)との紐づけを想定していない。
  - ➢ カスタムアプリの部品成分表(SBOM)を管理することで、攻撃元/攻撃先情報の適用可能性を広げることができる。

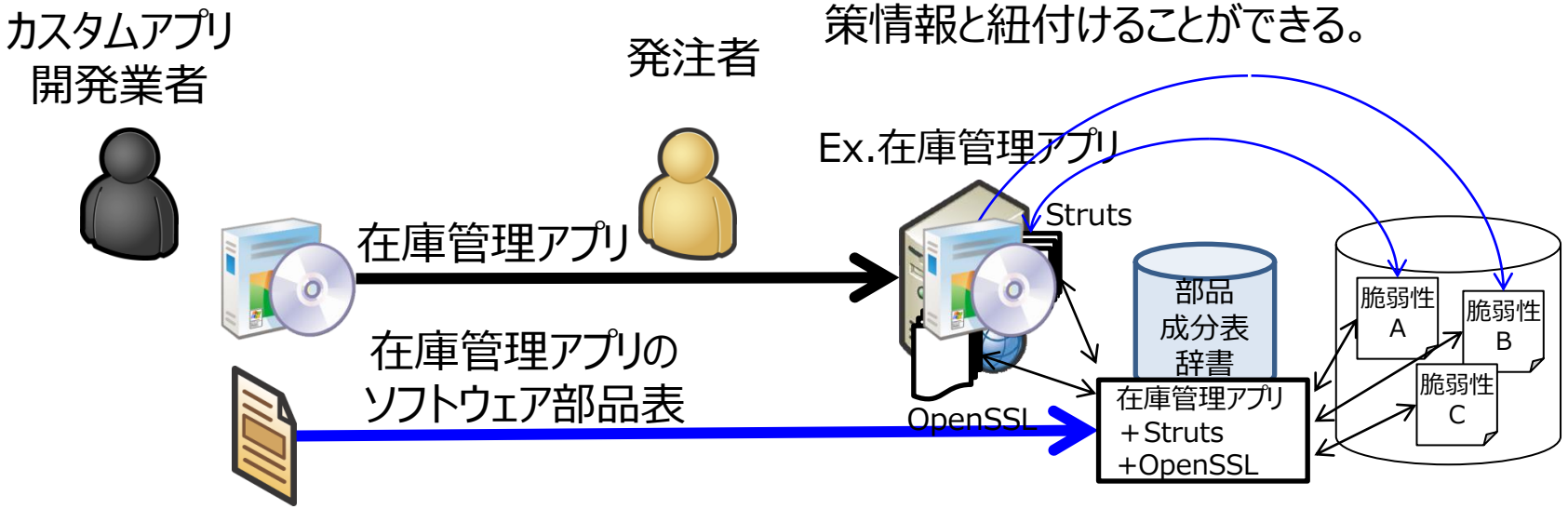
現状	実証実験
● カスタムアプリ(SIで開発したアプリケーションなど)は、資産管理や脆弱性管理の対象に含まれていないことが多い。 Ex.在庫管理アプリ 	● カスタムアプリの部品成分表辞書(カスタムアプリで使用しているアプリケーション一覧)を試行し、アプリケーション一覧と脆弱性情報とを紐付ける。 Ex.在庫管理アプリ 

情報共有基盤の実証

③部品成分表と紐付けられる脅威/脆弱性情報の配信【課題3】【課題4】

- SBOM(Software Bill of Materials、ソフトウエア部品表)
  - 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。

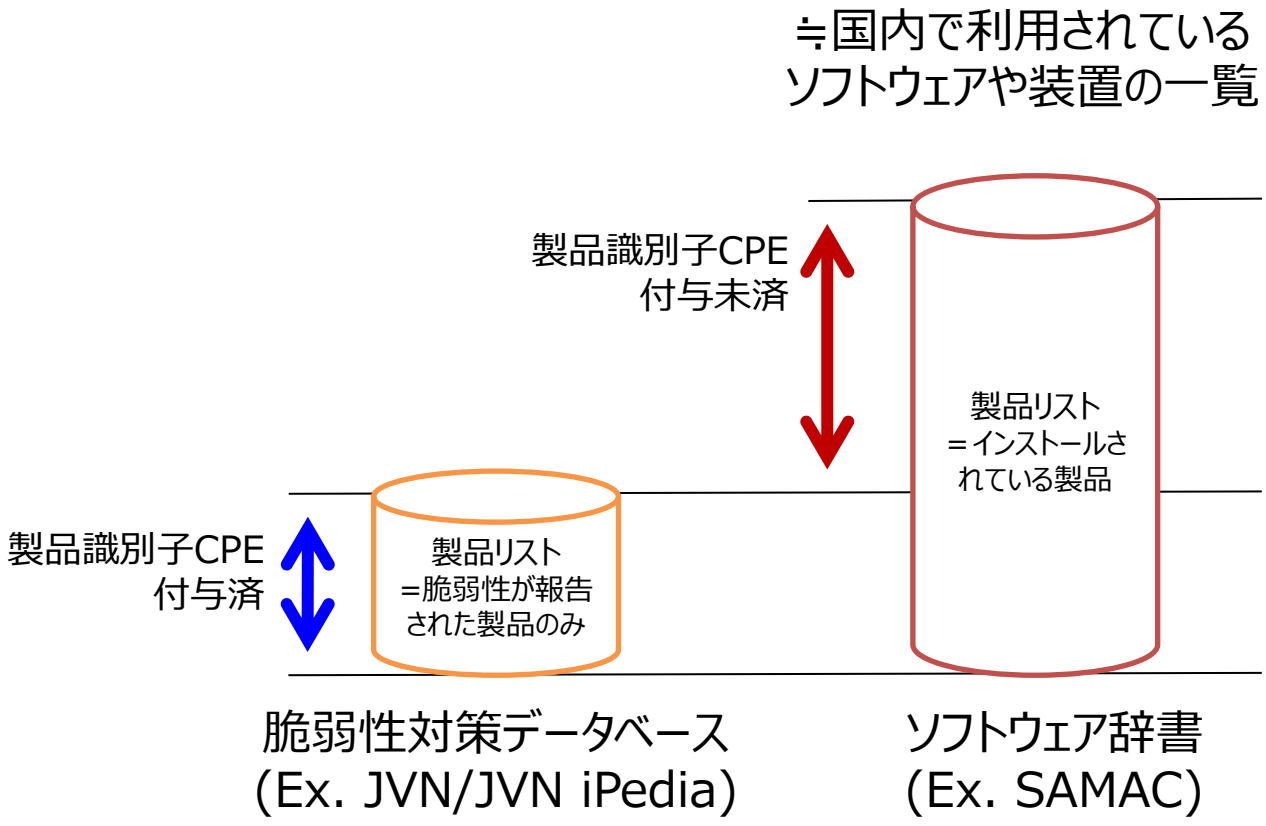
カスタムアプリ(SIで開発したアプリケーションなど)のソフトウェア部品表(カスタムアプリの使用コンポーネント一覧)があれば、脆弱性対策情報と紐付けることができる。



情報共有基盤の実証

実現のカギは製品識別

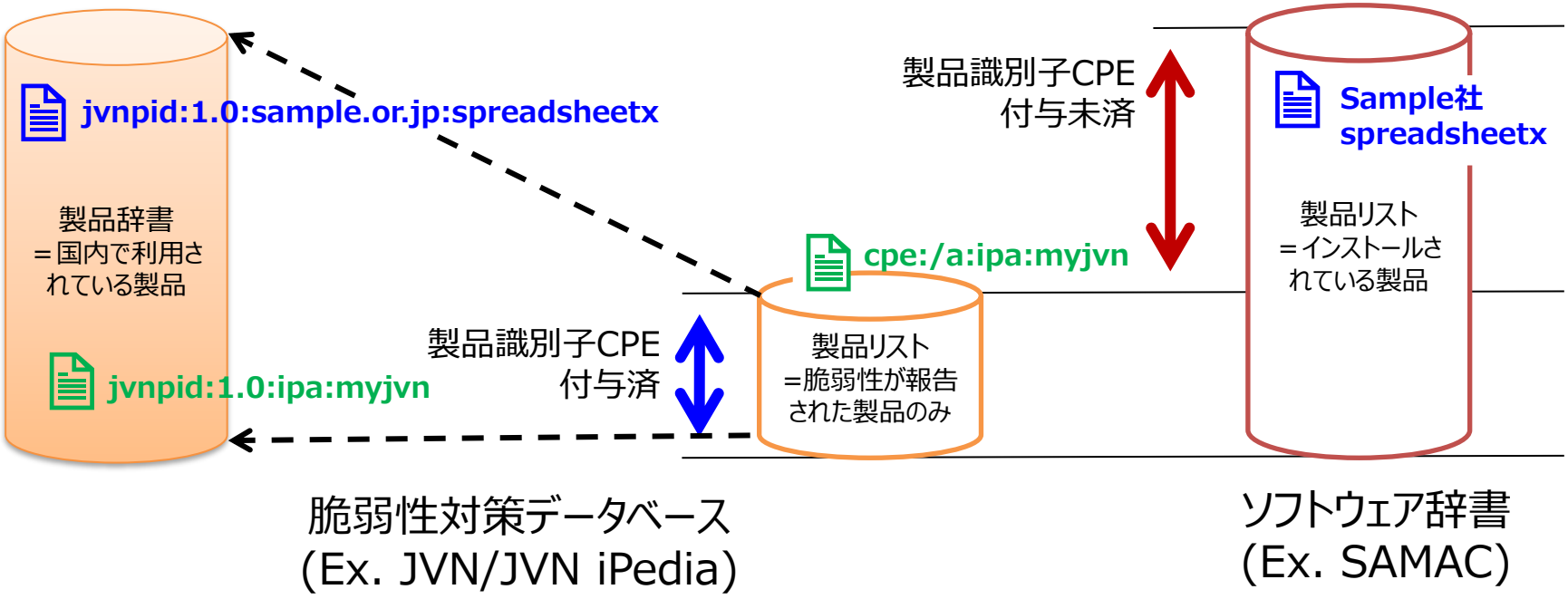
- 実現のための最初の一歩は、製品識別子CPE付与未済への対応



情報共有基盤の実証

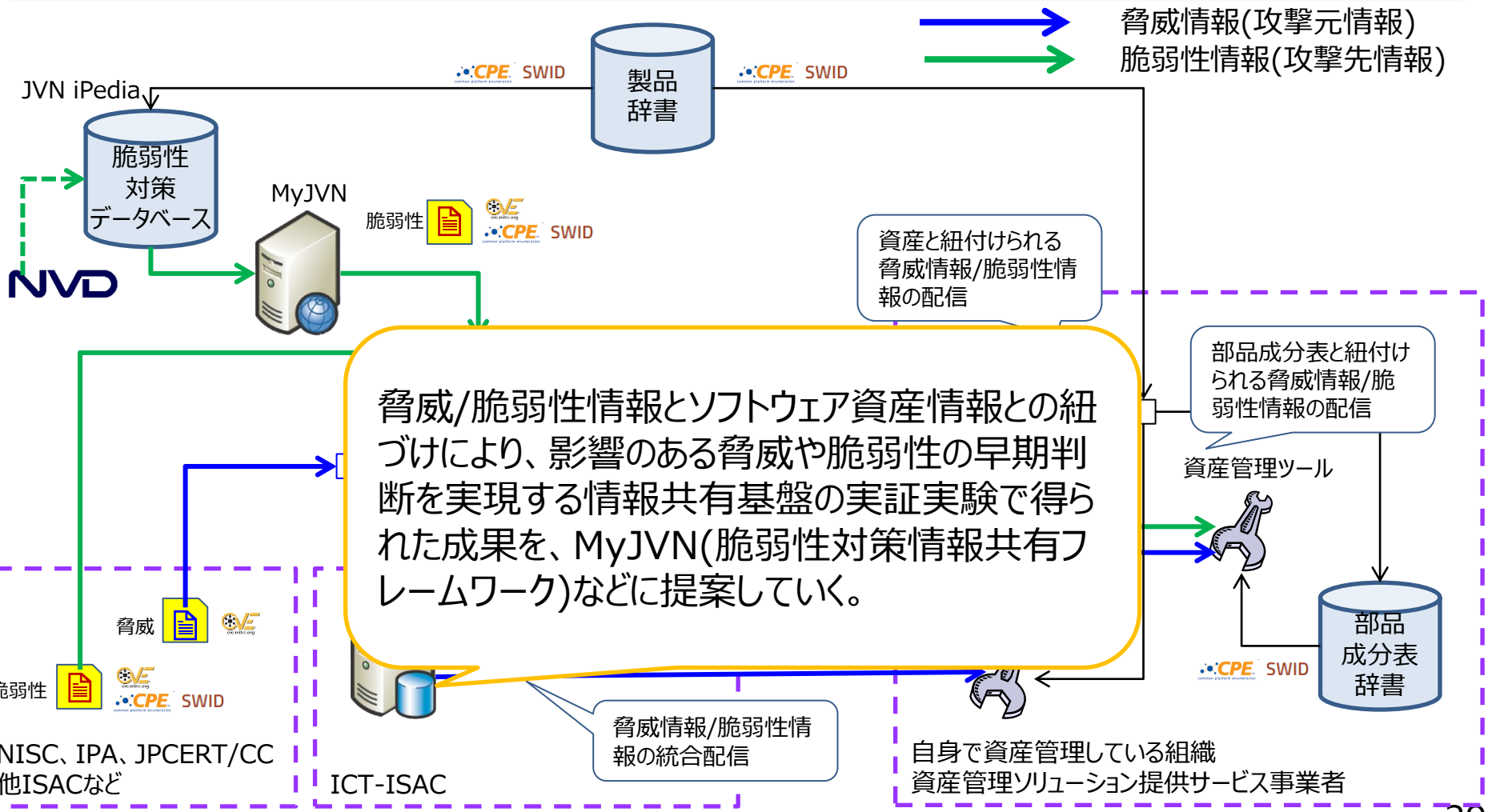
実現のカギは製品識別

- 課題解決のアプローチ
  - IT資産管理規格 ISO/IEC 19770-2 ソフトウェア識別子(SWID)活用
    - SWIDを用いて、国内で利用されているソフトウェアや装置に、CPEとの互換性を持つjvnpidをオーソリティとした構造化識別子を適用する。
      jvnpid:識別子バージョン:製品ベンダ名:製品名:バージョン



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