脅威/脆弱性情報と資産情報の連携による情報共有基盤のこれから

2023年3月3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

はじめに

サイバー攻撃への迅速な対応を可能にする環境を実現するため、脅威/脆弱性情報とソフトウェア資産情報との紐づけにより、影響のある脅威や脆弱性の早期判断を実現する情報共有基盤のこれからについて紹介します。

本日の「情報共有基盤のこれから」のトピックは、特に、製品識別という課題と、その解決アプローチについてです。

サイバー攻撃と脆弱性

脆弱性という言葉をよく耳にしませんか?

- 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

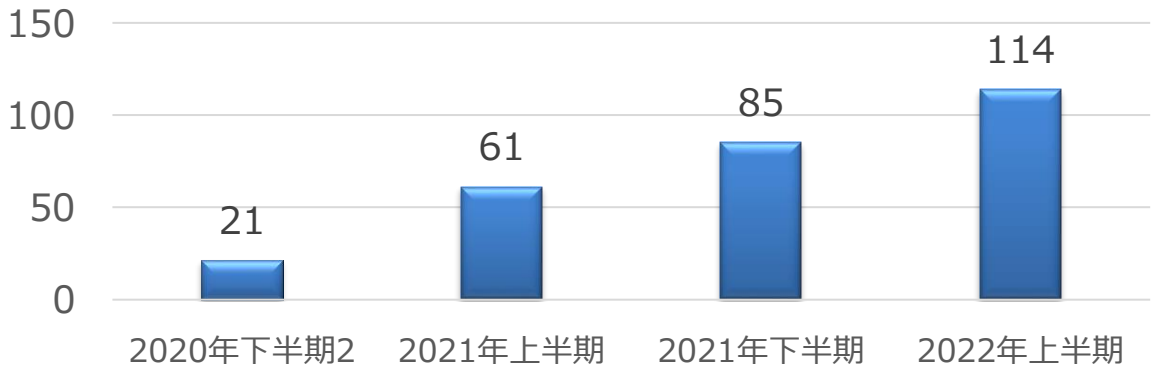
- 振り返り 2021年

  12月　Apache Log4jの任意のコード実行の脆弱性 ～Log4Shell問題～

サイバー攻撃と脆弱性

ランサムウェアによる被害

- 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



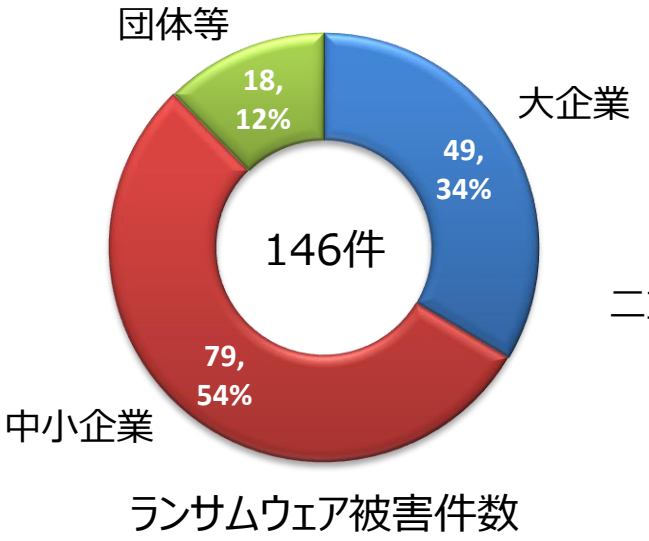
- 2022年上半期のランサムウェア被害の特徴
  - 二重恐喝(ダブルエクストーション)による被害が多くを占める
  - 暗号資産による金銭の要求が多くを占める
  - 企業・団体等の規模を問わず被害が発生
  - 感染経路は、テレワークにも利用される機器等の脆弱性や強度の弱い認証情報等を利用して侵入したと考えられるものが大半を占めている

[出典] 令和４年上半期におけるサイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_kami_cyber_jousei.pdf

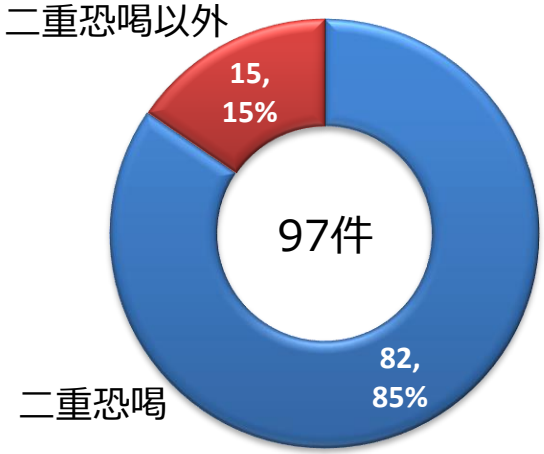
サイバー攻撃と脆弱性

ランサムウェアによる被害

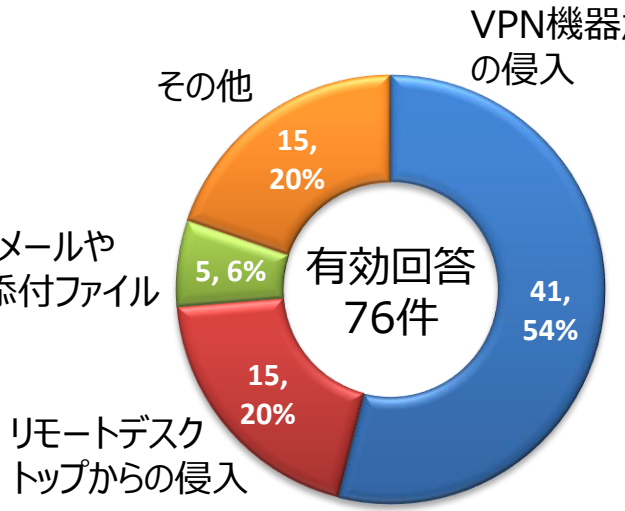
- 2021年のランサムウェア被害の状況



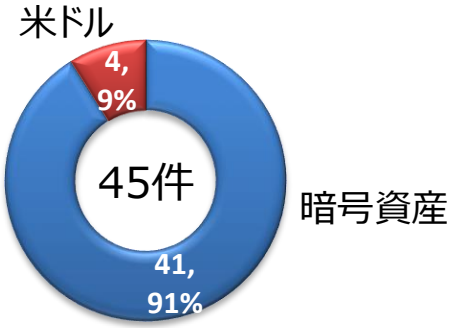
ランサムウェア被害件数



手口を確認できた被害



感染経路

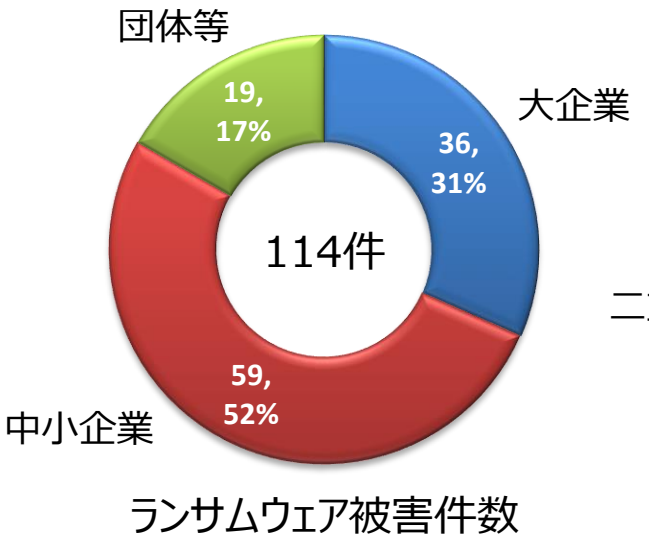


直接的な金銭要求あり

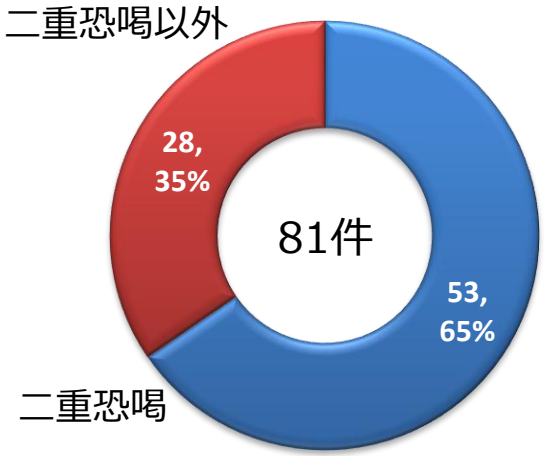
サイバー攻撃と脆弱性

ランサムウェアによる被害

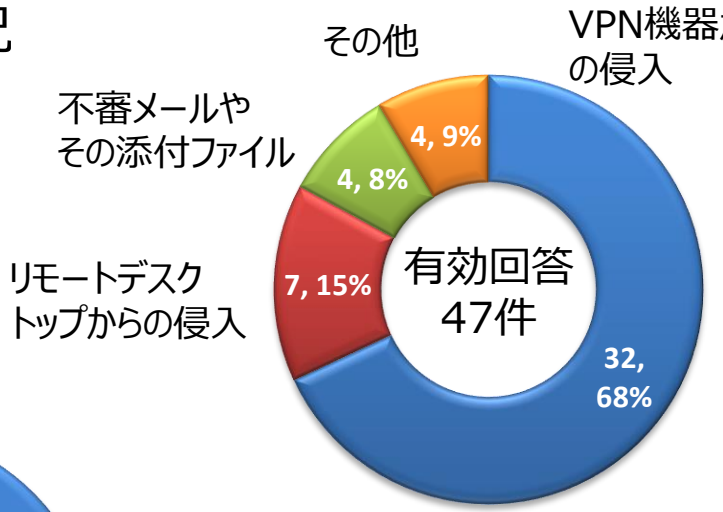
- 2022年上半期のランサムウェア被害の状況



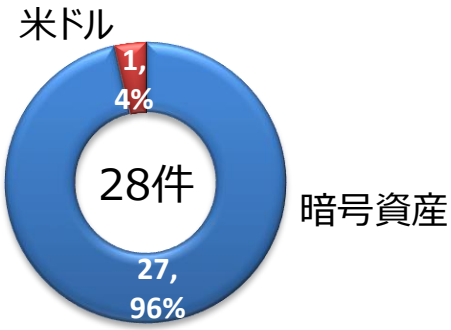
ランサムウェア被害件数



手口を確認できた被害



感染経路



直接的な金銭要求あり

サイバー攻撃と脆弱性

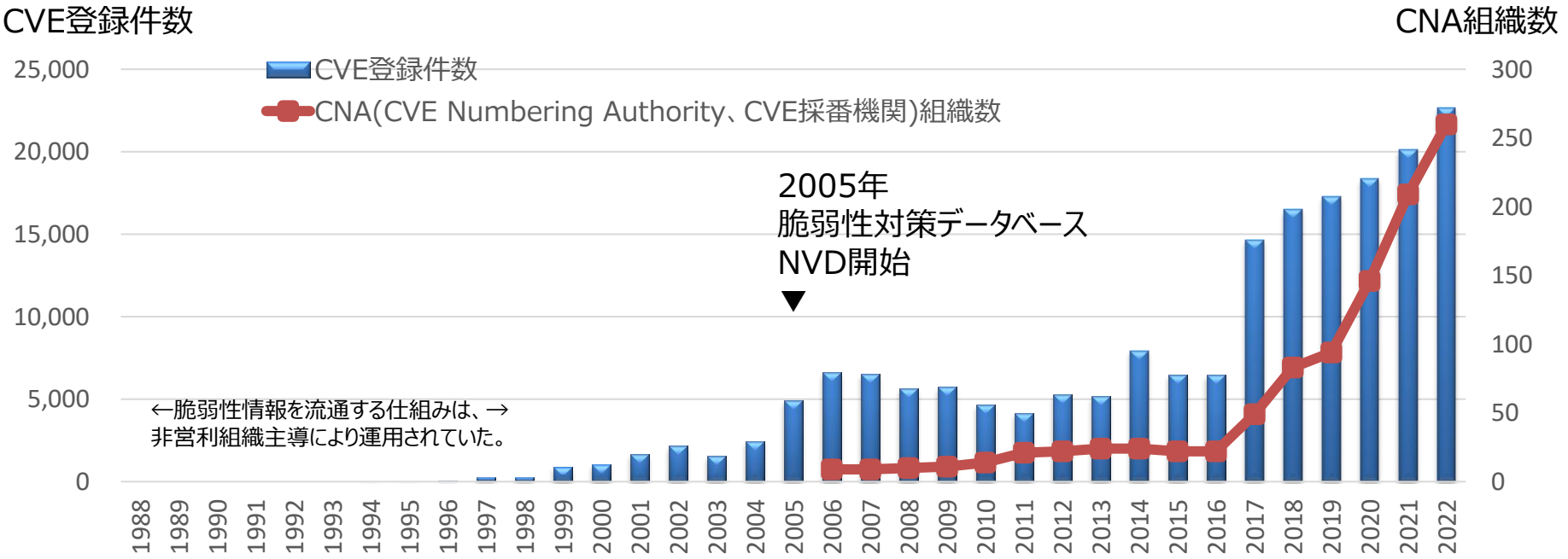
脆弱性対策を進める3つの視点

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	机上レビュー 手動検査 (ペネトレーション検査)	攻撃者視点での セキュリティ検査 (≒オフェンシブ セキュリティ)
コードの脆弱性	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	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	アカウントとパスワードが同じ	セキュリティ設定検査 (ハードニング検査)	

サイバー攻撃と脆弱性

【 課題1 】日々公表される膨大な数の脆弱性

- 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
  - 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。

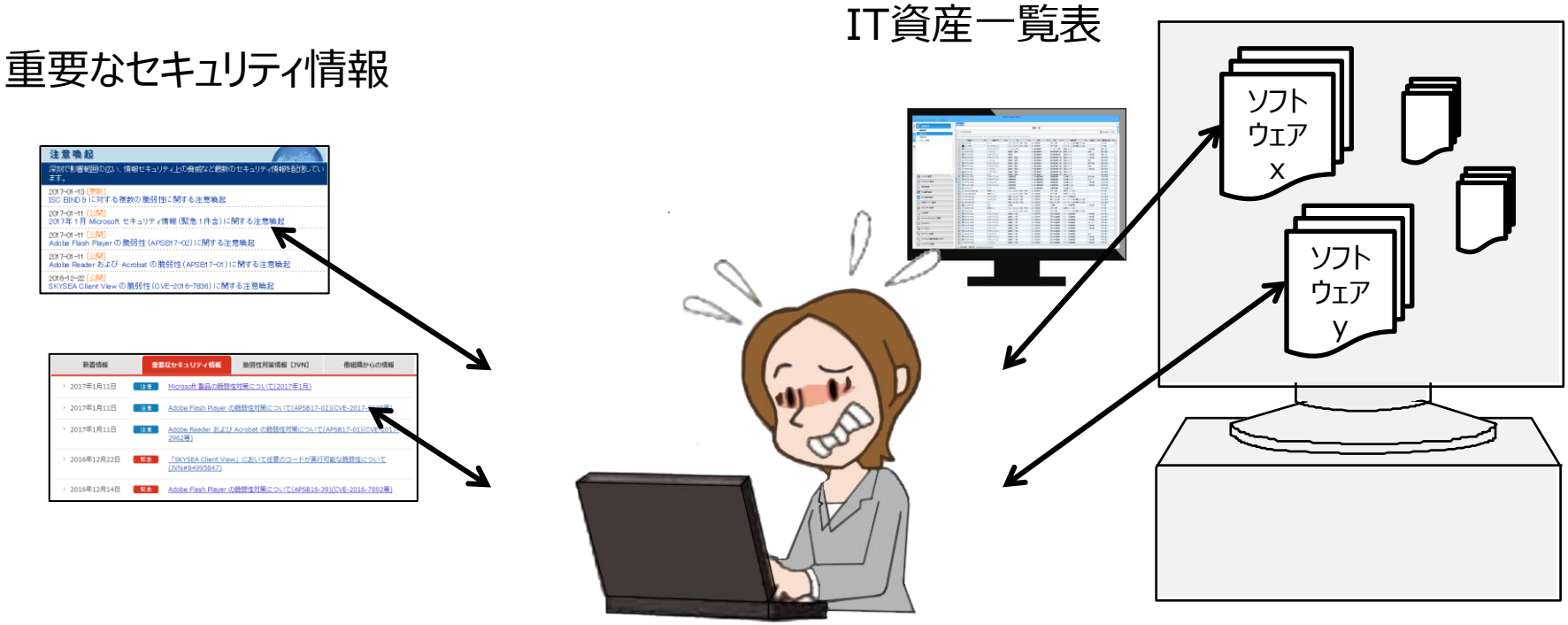


[出典] Search Vulnerability Database
https://nvd.nist.gov/vuln/search

サイバー攻撃と脆弱性

【 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)。



サイバー攻撃と脆弱性

【 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。

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

実証実験の振り返り (2019年～2021年)

情報共有・自動処理の必要性

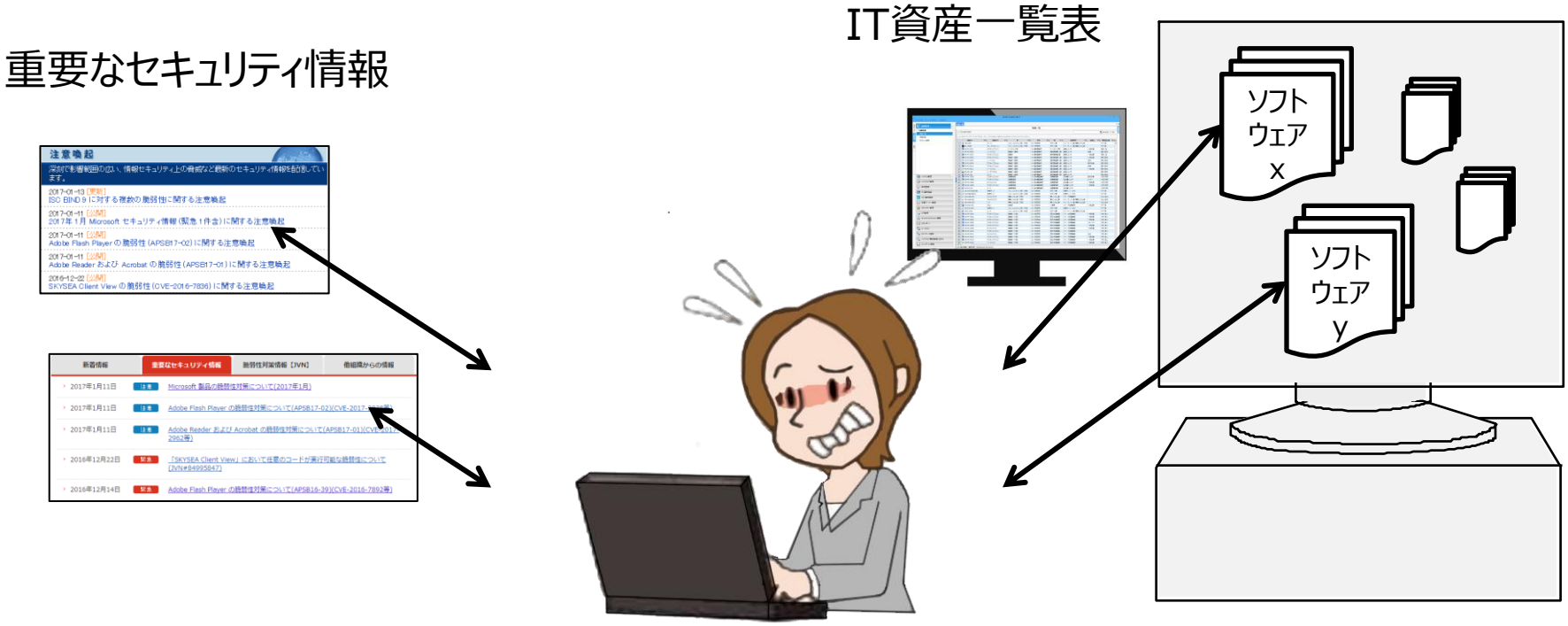
- 複雑化するシステムと、増加する脆弱性に対応するには、各業界・業種に合わせた情報をオープンデータとして共有することと、セキュリティ対策に必要な情報の処理を自動化することが求められている。

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

実証実験の振り返り (2019年～2021年)

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(脆弱性情報と資産情報とが連携できているわけではない)。



実証実験の振り返り (2019年～2021年)

実証実験の目的

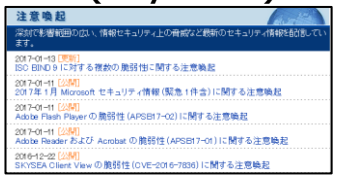
- 情報連携により、人が介在しなくても良い脆弱性対策環境(脆弱性の影響有無の判定など)の実現性を確認する。
  - 重要なセキュリティ情報で使用するソフトウェア名と、IT資産一覧表で使用するソフトウェア名の統一を図る。

実証実験の振り返り (2019年～2021年)

ソフトウェア名の統一を図るとは

- 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と、IT資産一覧表で使用するソフトウェア名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)



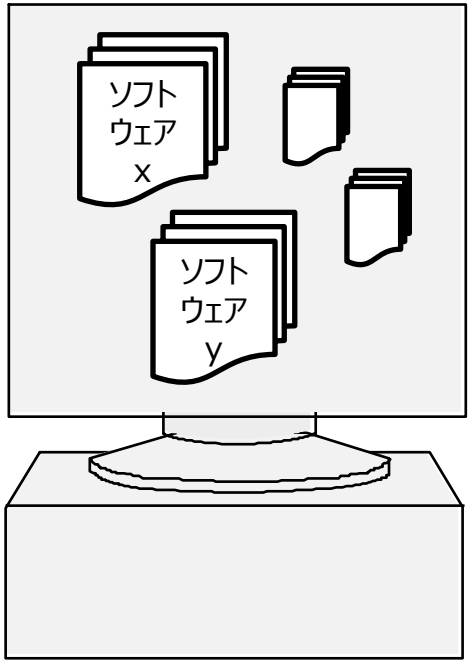
重要なセキュリティ情報に
記載されているソフトウェア名
- 製品ABC

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

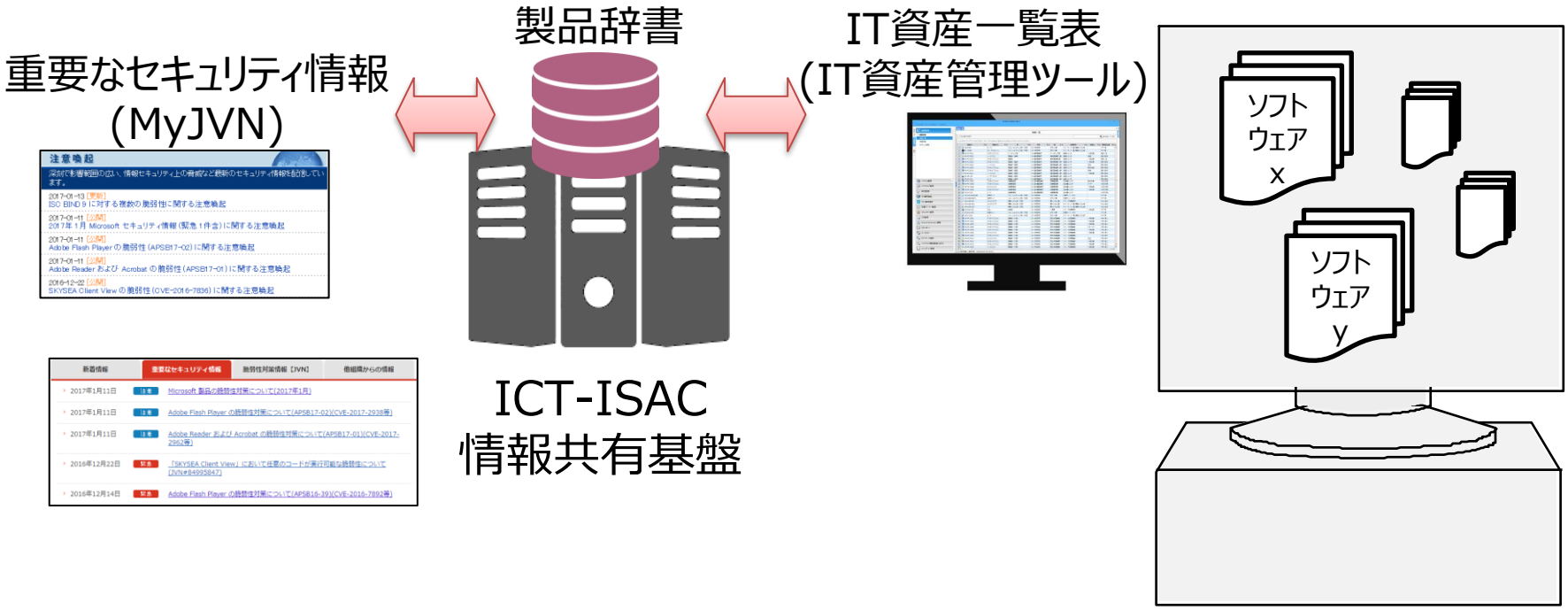
IT資産一覧表
(IT資産管理ツール)



実証実験の振り返り (2019年～2021年)

ソフトウェア名の統一を図るために

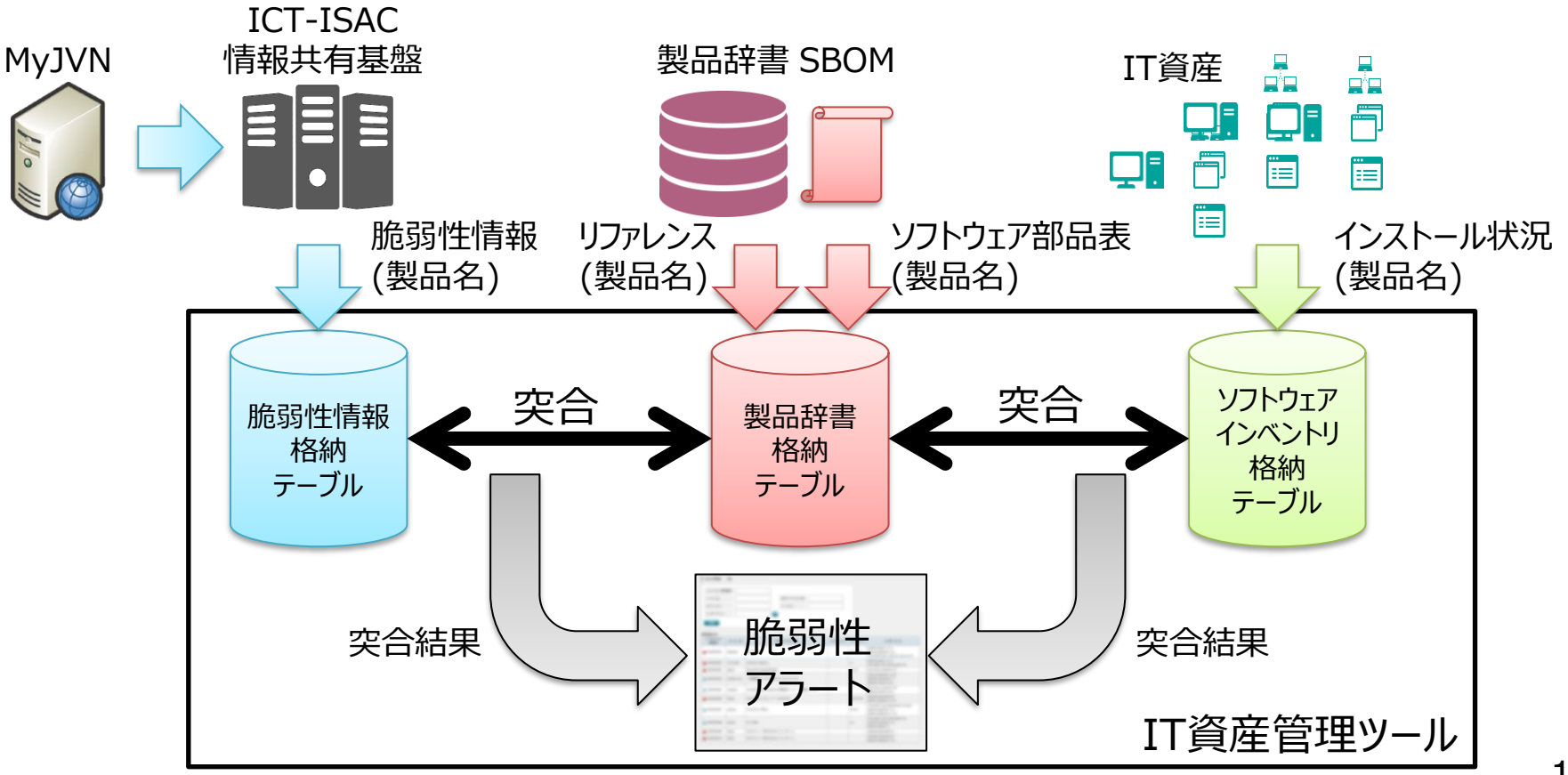
- 情報連携により、人が介在しなくても良い脆弱性対策環境(脆弱性の影響有無の判定など)の実現性を確認する。
  - ソフトウェア名の統一のためのリファレンス(製品辞書)を利用した重要なセキュリティ情報とIT資産一覧表との連携



実証実験の振り返り (2019年～2021年)

【短期的】脆弱性情報と資産情報の連携

- ソフトウェア名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



連携による情報共有基盤のこれから（1）

実運用に向けて

- 短期的アプローチであるリファレンス(製品辞書)を利用した連携を実運用という形に持っていくためには、

1. リファレンス(製品辞書)に登録されていない製品について、リファレンス(製品辞書)に登録する仕組みを持つこと

2. サイバー攻撃への迅速な対応を可能にするには、脆弱性が発見される前にリファレンス(製品辞書)に登録されていること

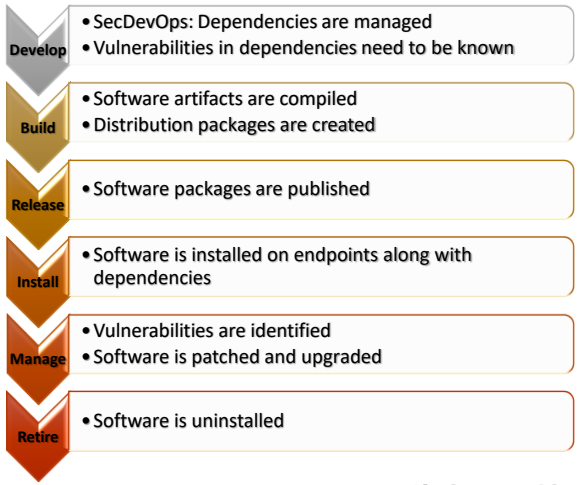
連携による情報共有基盤のこれから (1)

NVDも、同じ悩みを抱えている

- 製品識別子(CPE)付与の95%は、脆弱性が発見されてから、、、
  ≒ リファレンス(製品辞書)に登録されるのは、ほぼ脆弱性が発見されてから、、、

CPE Myth: CPEs are produced by software suppliers

- ~5% of CPE Names are provided by software providers around the point of software “release”
- ~95% of CPE Names are created by NVD analysts during the “manage” phase
  - Produced during the vulnerability analysis process
  - **Software is identified after a known vulnerability is found**
- Identifying software after a vulnerability is discovered is way too late!



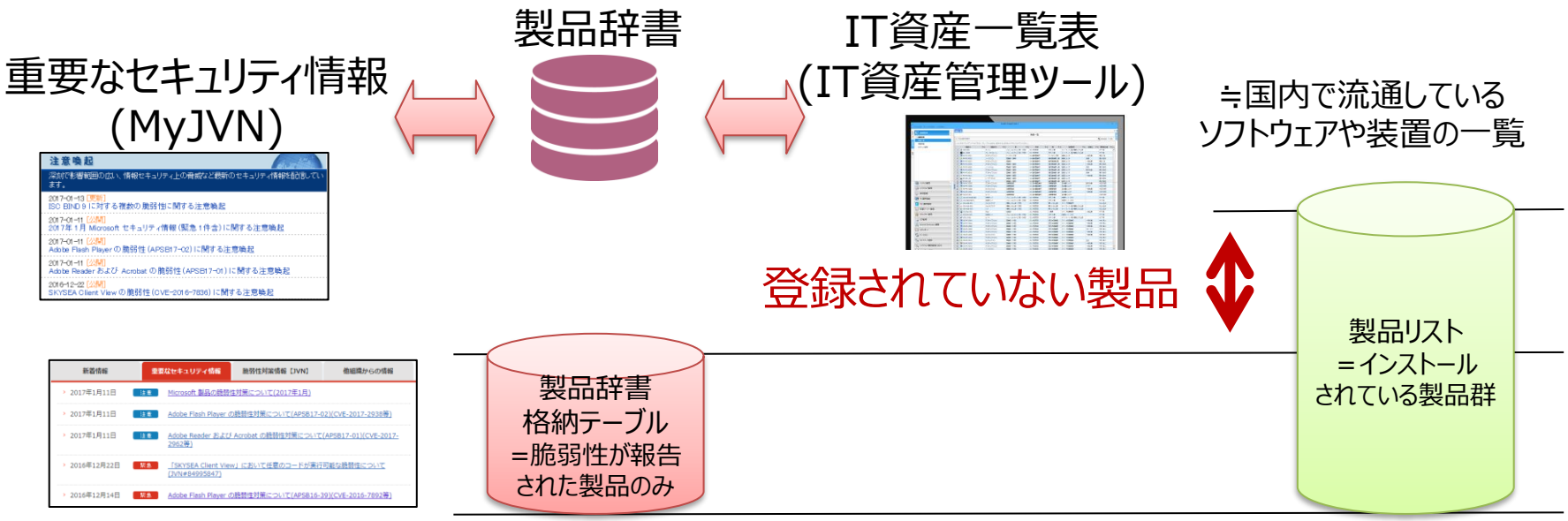
CPE(Common Platform Enumeration ; 共通製品識別子)

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

連携による情報共有基盤のこれから（1）

【短期的】製品識別という課題：現状

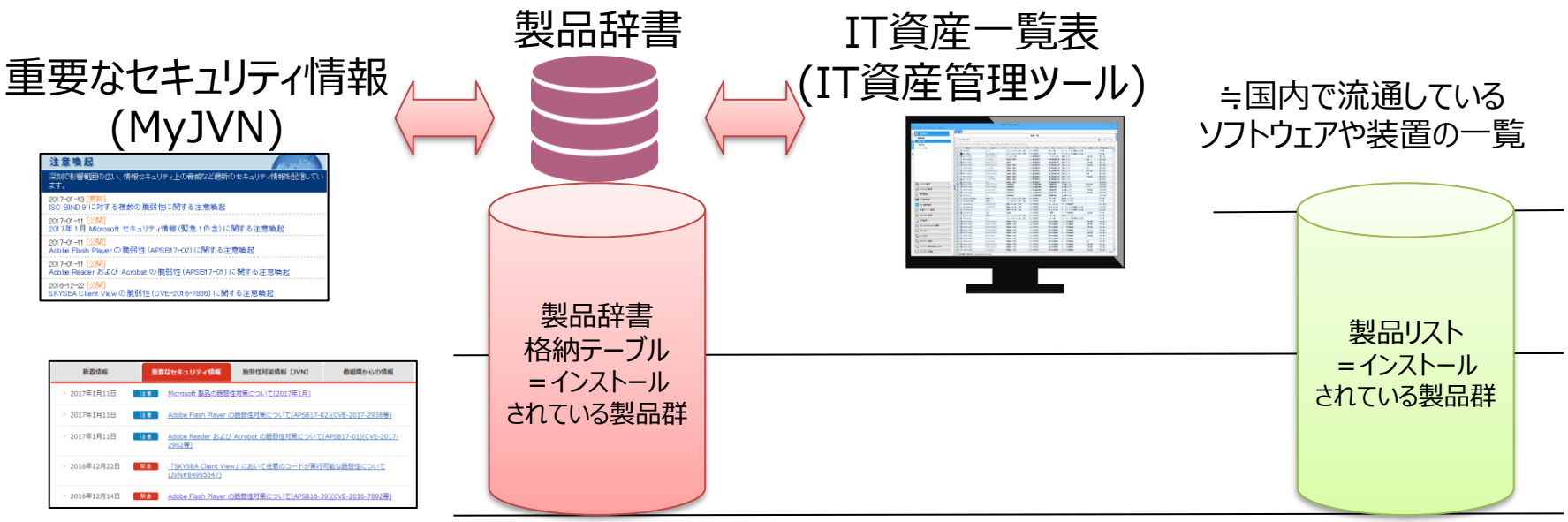
- リファレンス(製品辞書)に登録されているソフトウェア名は、脆弱性が報告された製品のみのソフトウェア名から構成



連携による情報共有基盤のこれから（1）

【短期的】製品識別という課題：課題が解決された望ましい姿

- リファレンス(製品辞書)に登録されているソフトウェア名は、国内で流通している製品のソフトウェア名から構成

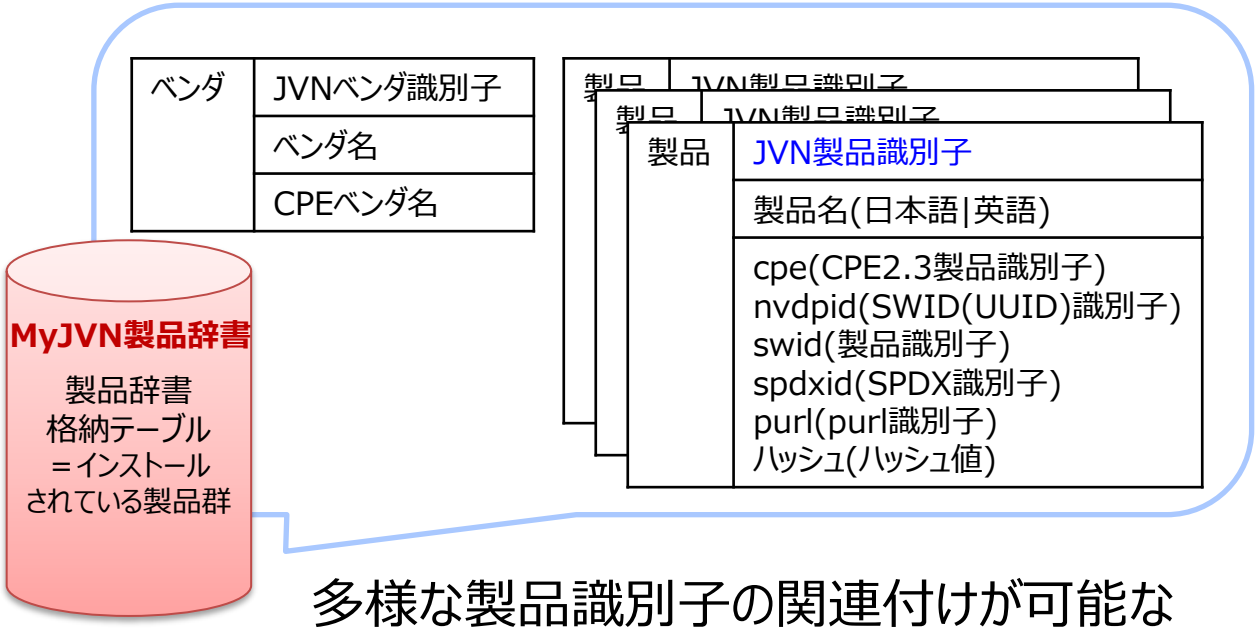


連携による情報共有基盤のこれから（1）

【短期的】製品識別という課題：解決のためのアプローチ

- 多様な製品識別子を関連付けるための製品辞書の整備を通して、グローバルな連携を可能としつつ、製品識別子の付与されていない製品(≒製品辞書に登録されていないソフトウェア)に識別子を付与し、その識別子の流通を支援する。

```
{
 "vendors": [
  {
   "vendor_id": "JVNベンダ識別子",
   "vname": "ベンダ名",
   "cpe": "CPEベンダ名",
   "products": [
    {
     "product_id": "JVN製品識別子",
     "pname": "製品名",
     "product_ids": [
      {"cpe": "CPE2.3製品識別子"},
      {"nvdpid": "SWID(UUID)識別子"},
      {“swid": "製品識別子"},
      {"spdxid": "SPDX識別子"},
      {"purl": "purl識別子"},
      {“sha256": "ハッシュ値"}
     ]
    },{製品2},{・・・}] }]
}
```

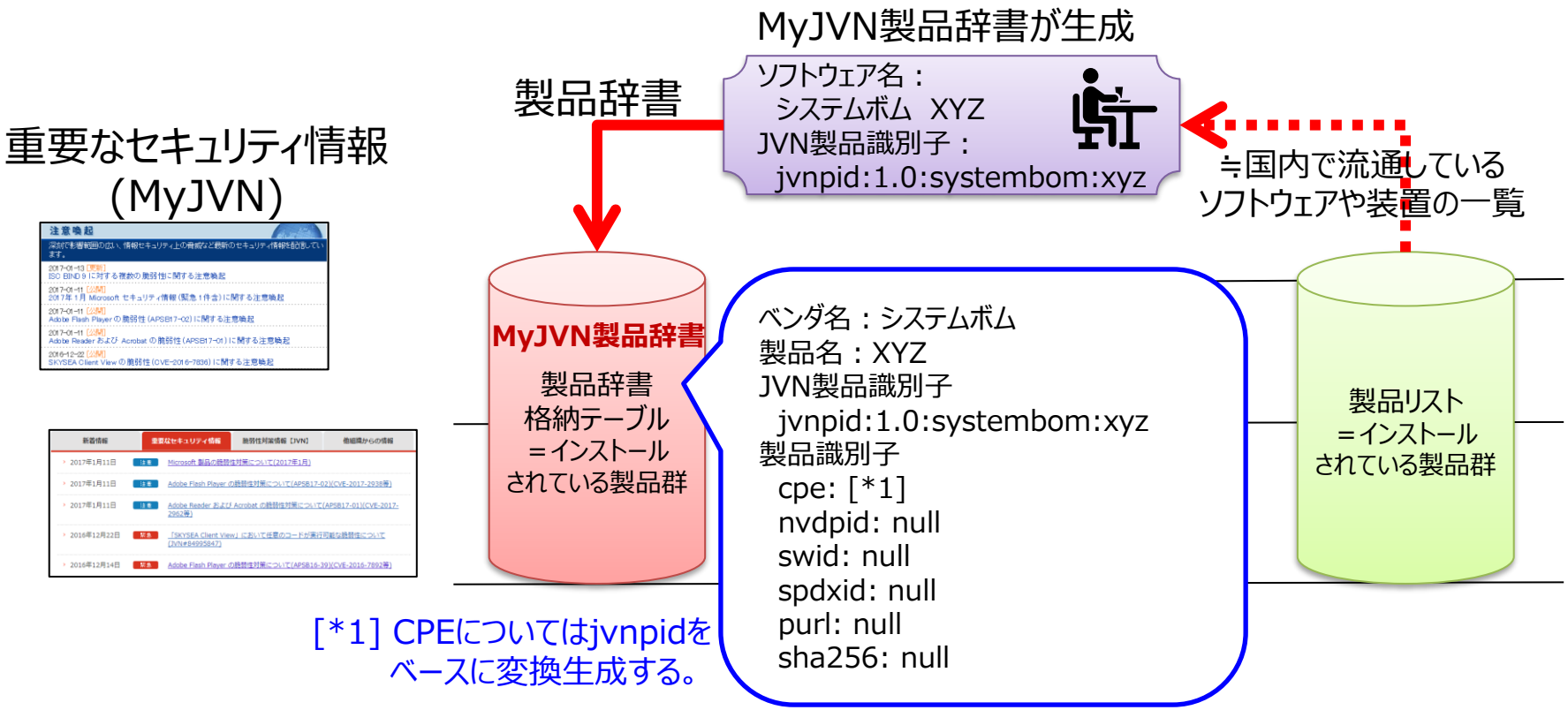


多様な製品識別子の関連付けが可能な
MyJVN製品辞書の整備

連携による情報共有基盤のこれから（1）

【短期的】製品識別という課題：解決のためのアプローチ

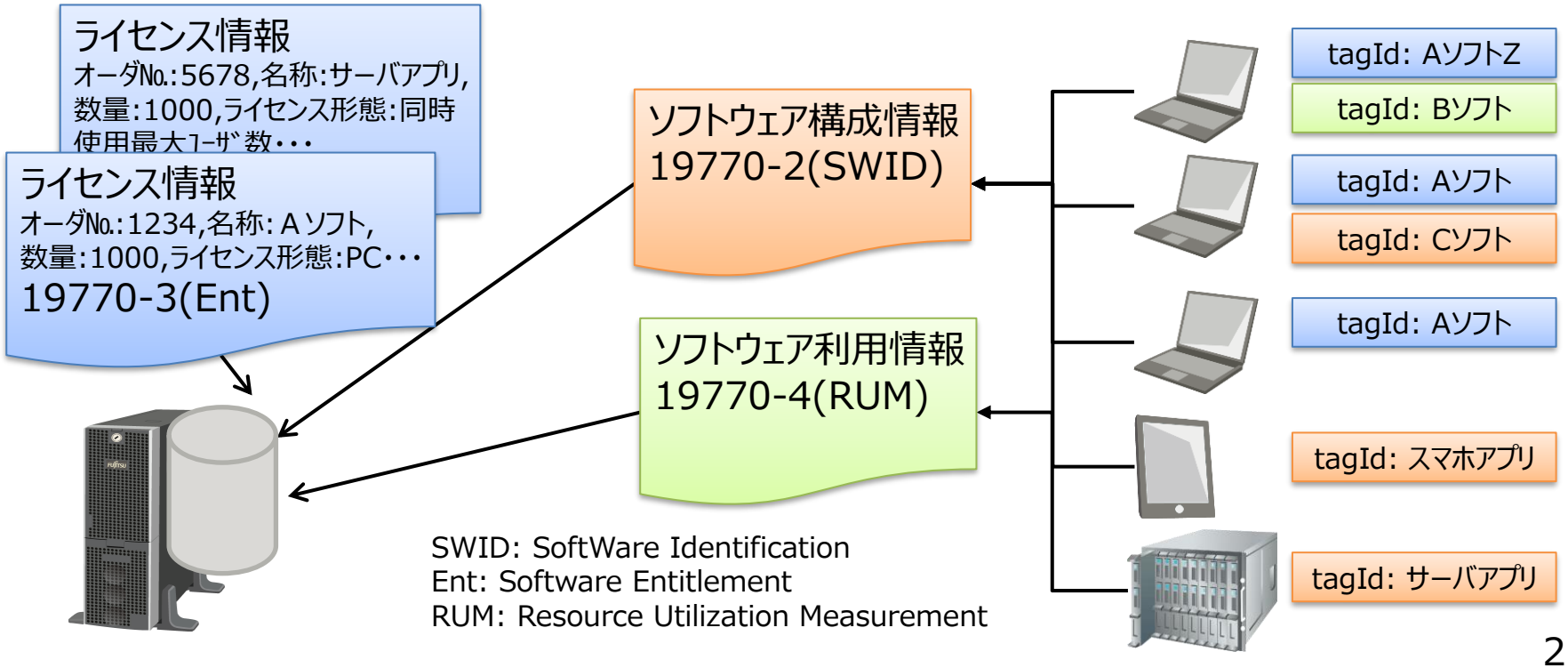
- 国内で流通している製品のソフトウェア名については、MyJVNが製品識別子を付与してMyJVN製品辞書に登録



連携による情報共有基盤のこれから (2)

【長期的】脆弱性情報と資産情報の連携のあるべき姿は?

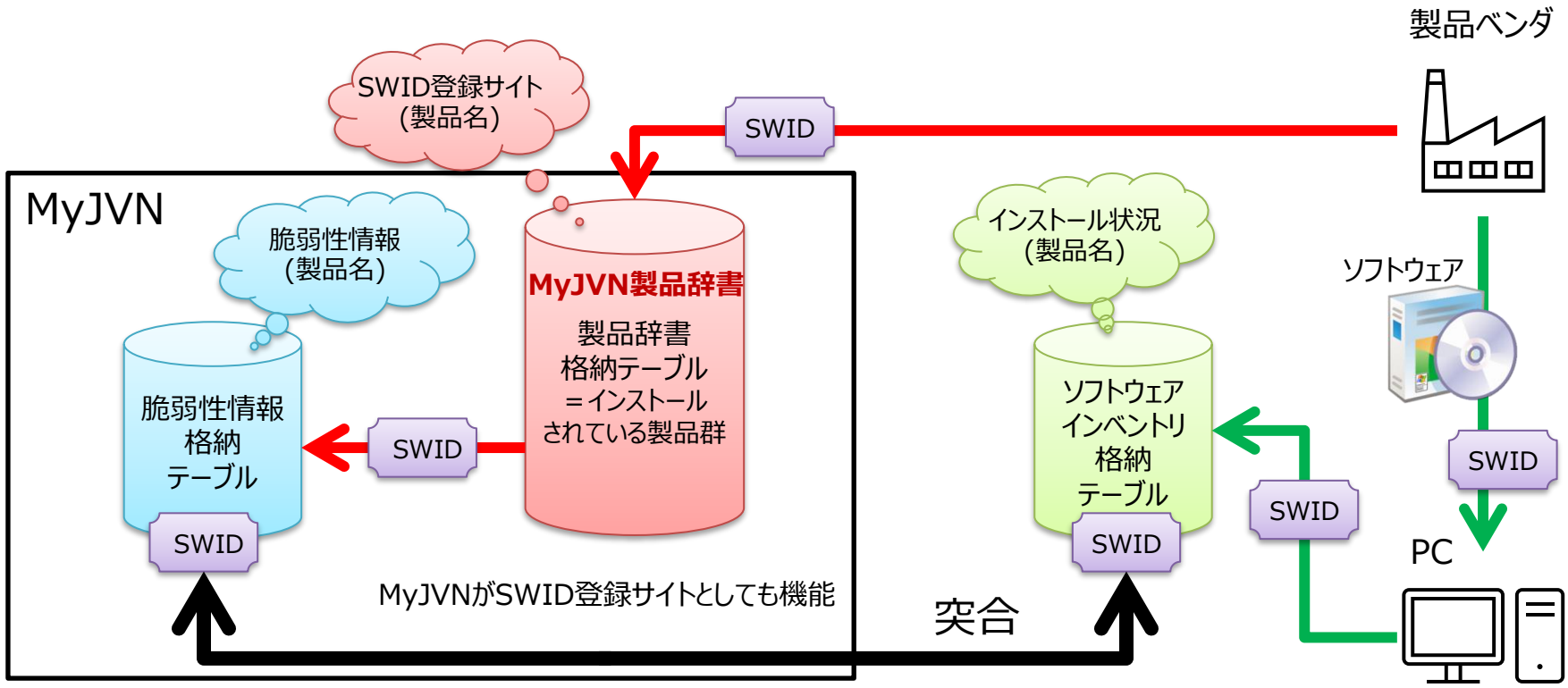
- ISO/IEC 19770の仕組みを参考に考えてみよう。
  - 各種情報を集約し、自動チェックするなどの基盤整備に利用可能
  - ソフトウェア構成情報(SWID)は19770-2、ライセンス情報(Ent)は19770-3、リソース利用情報(RUM)は19770-4で情報構造が標準化



連携による情報共有基盤のこれから (2)

【長期的】脆弱性情報と資産情報の連携のあるべき姿は?

- ISO/IEC 19770-2 製品識別子(SWID)の仕組みの考え方を用いれば、インストール状況(製品名)とSWID登録サイト(製品名)のデータは一致する。すなわち、インストール状況(製品名)と脆弱性情報(製品名)のデータも一致し、名寄せなどの変換が不要となる。

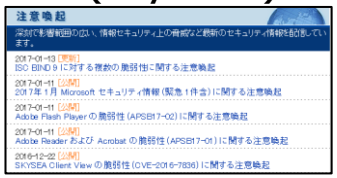


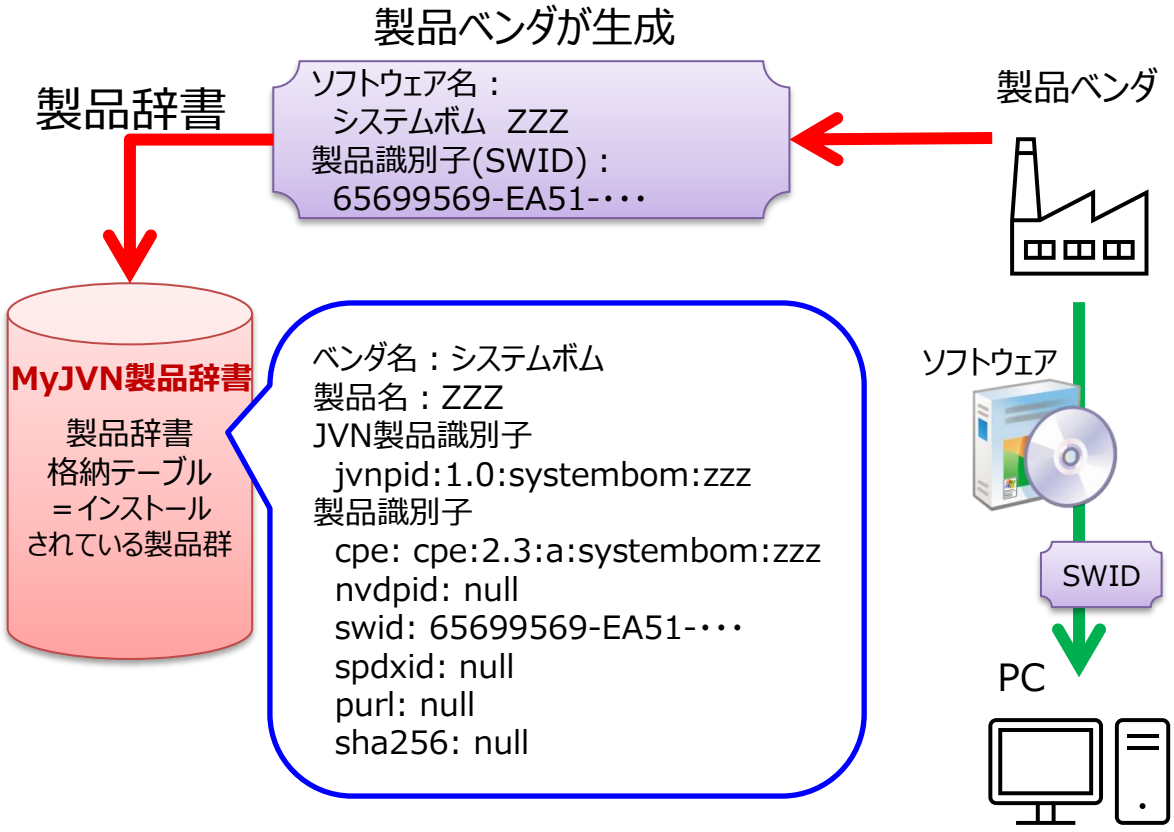
連携による情報共有基盤のこれから (2)

【長期的】製品識別という課題：解決のためのアプローチ

- 国内で流通している製品のソフトウェア名については、ベンダが製品識別子を付与してMyJVN製品辞書に登録・・・ MyJVN製品辞書は登録サイトとして機能する。

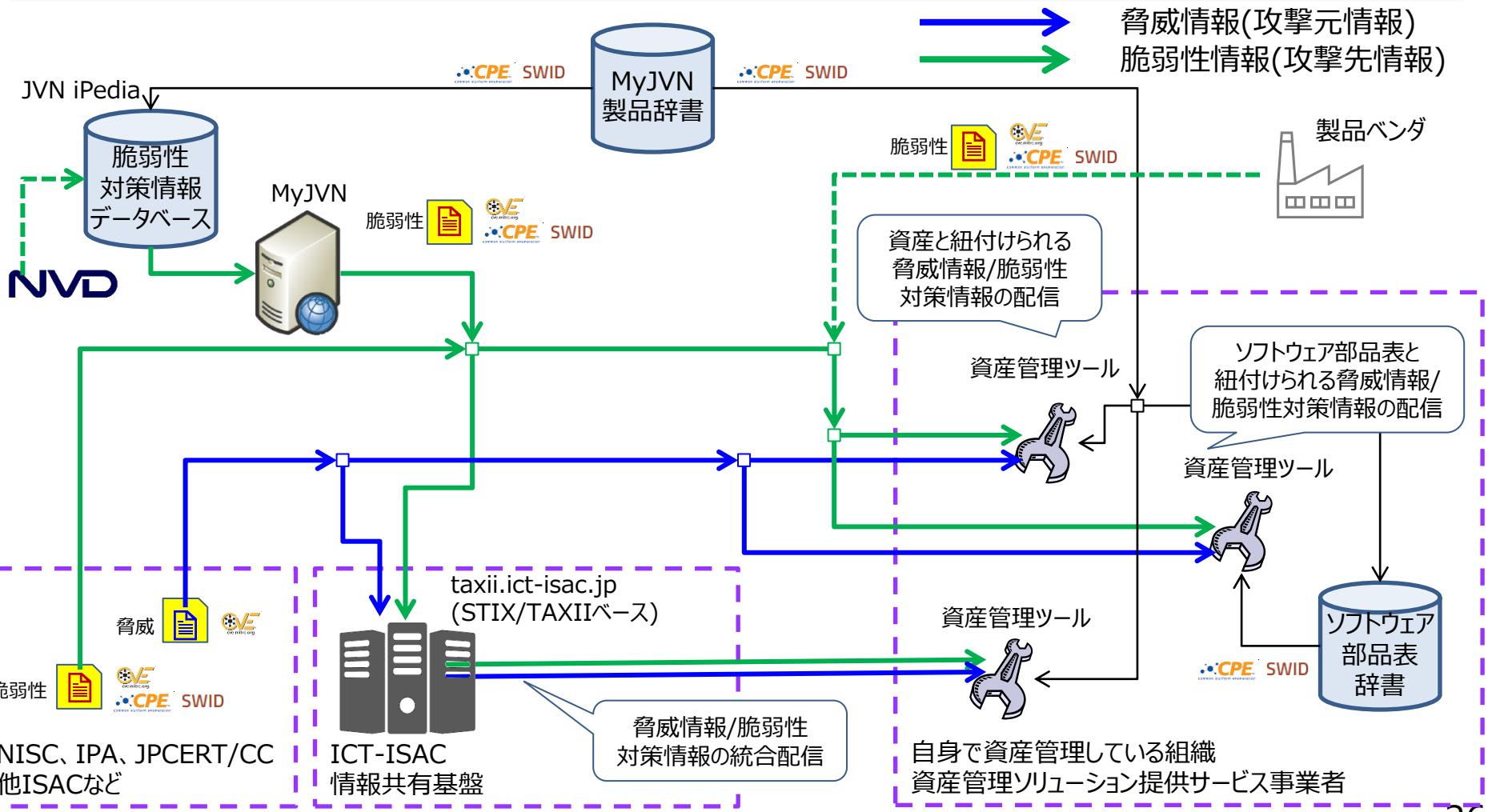
重要なセキュリティ情報
(MyJVN)





多層防御としての情報活用基盤と想定する将来像

脅威情報／脆弱性対策情報と資産管理との連携



おわりに

ICT-ISACでは、 STIX/TAXIIベースとした情報共有基盤を試行運用しており、脅威/脆弱性情報とソフトウェア資産情報との紐づけにより、影響のある脅威や脆弱性の早期判断を実現する情報共有基盤の整備に向け取り組んでいます。

影響のある脅威や脆弱性の早期判断の実現には、脅威/脆弱性情報とソフトウェア資産情報との紐づけがしやすい環境を作ることが「これから」の第一歩であると考えます。情報共有基盤の活用や機能改善など、検討を進めておりますので、いろいろご意見などを頂ければ幸いです。

Collaborate
together
to make our
Internet
secure.

ICT-ISAC JAPAN
ICT Information Sharing And Analysis Center Japan