

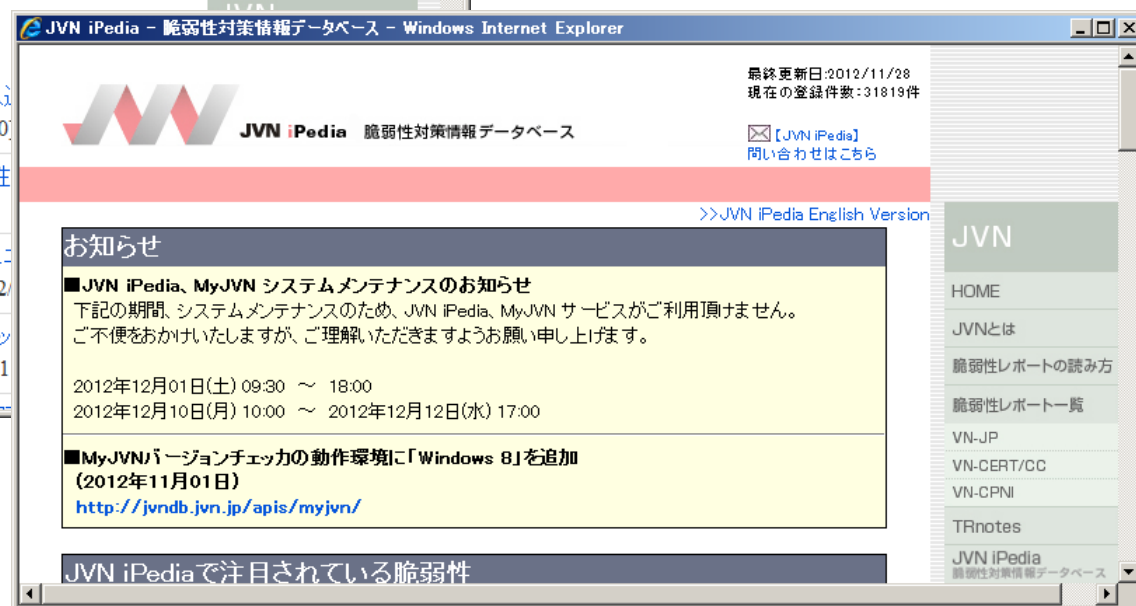
製品識別子を用いた 脆弱性対策情報データベースと 資産管理との連携に関する検討

2022年11月28日
寺田真敏



JVN は "Japan Vulnerability Notes" の略

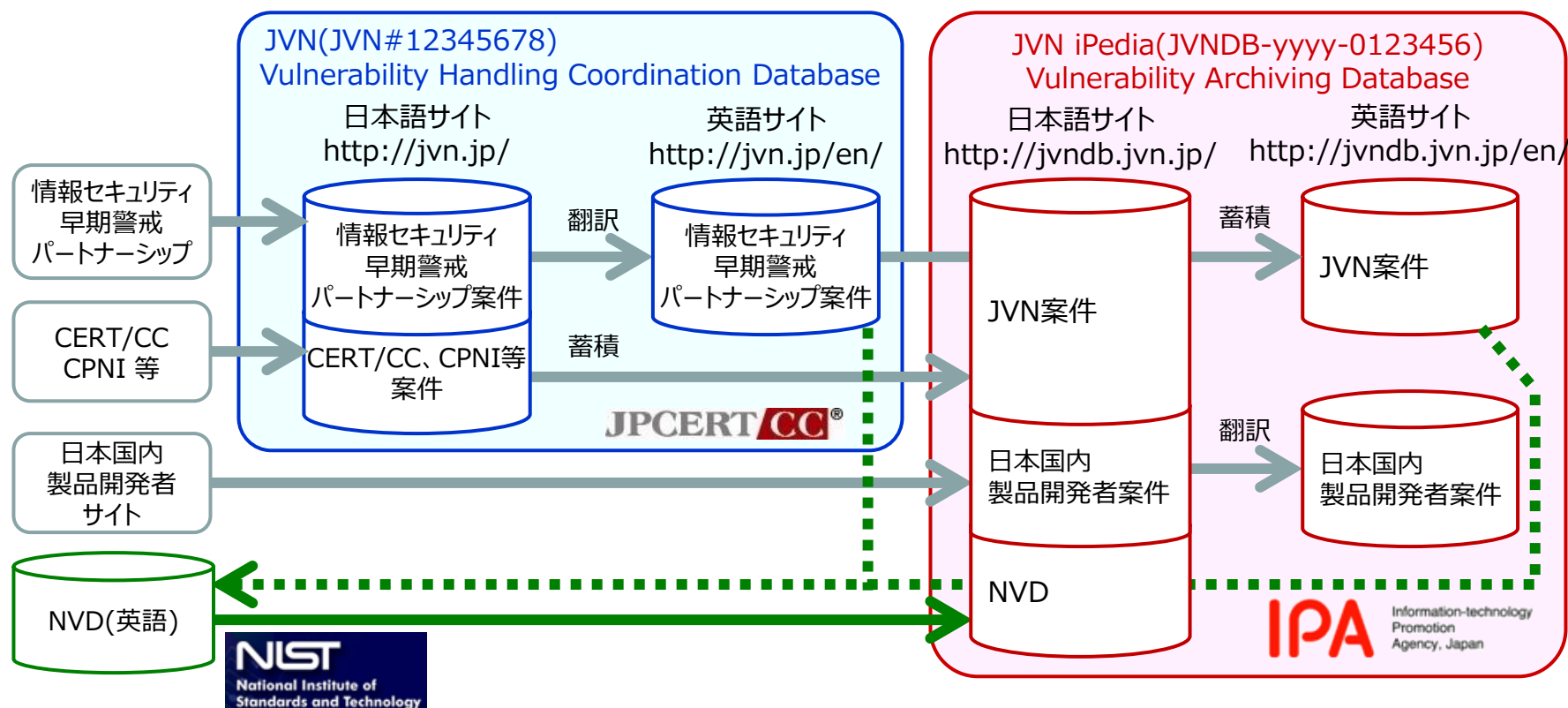
- JVN は “Japan Vulnerability Notes” の略
- 日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供し、情報セキュリティ対策に資することを目的とする脆弱性対策情報サイト



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

脆弱性対策データベースの日米間連携

- 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



MyJVN : JVN脆弱性対策機械処理基盤

- 自動化など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
チェック



セキュリティ設定
チェック



脆弱性対策
情報収集ツール



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ための仕組みを提供する

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

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

共通脆弱性識別子CVEが
付与されている脆弱性対策情報



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

国内外で報告された
全ての脆弱性対策情報

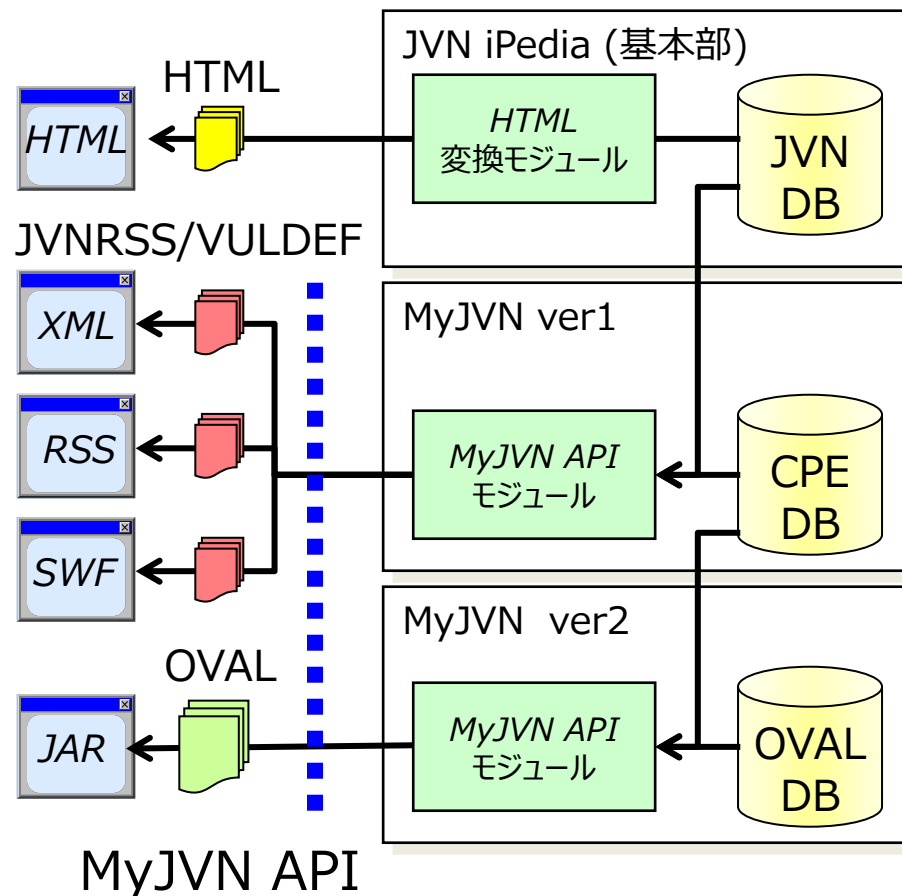
MyJVN : JVN脆弱性対策機械処理基盤

- 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

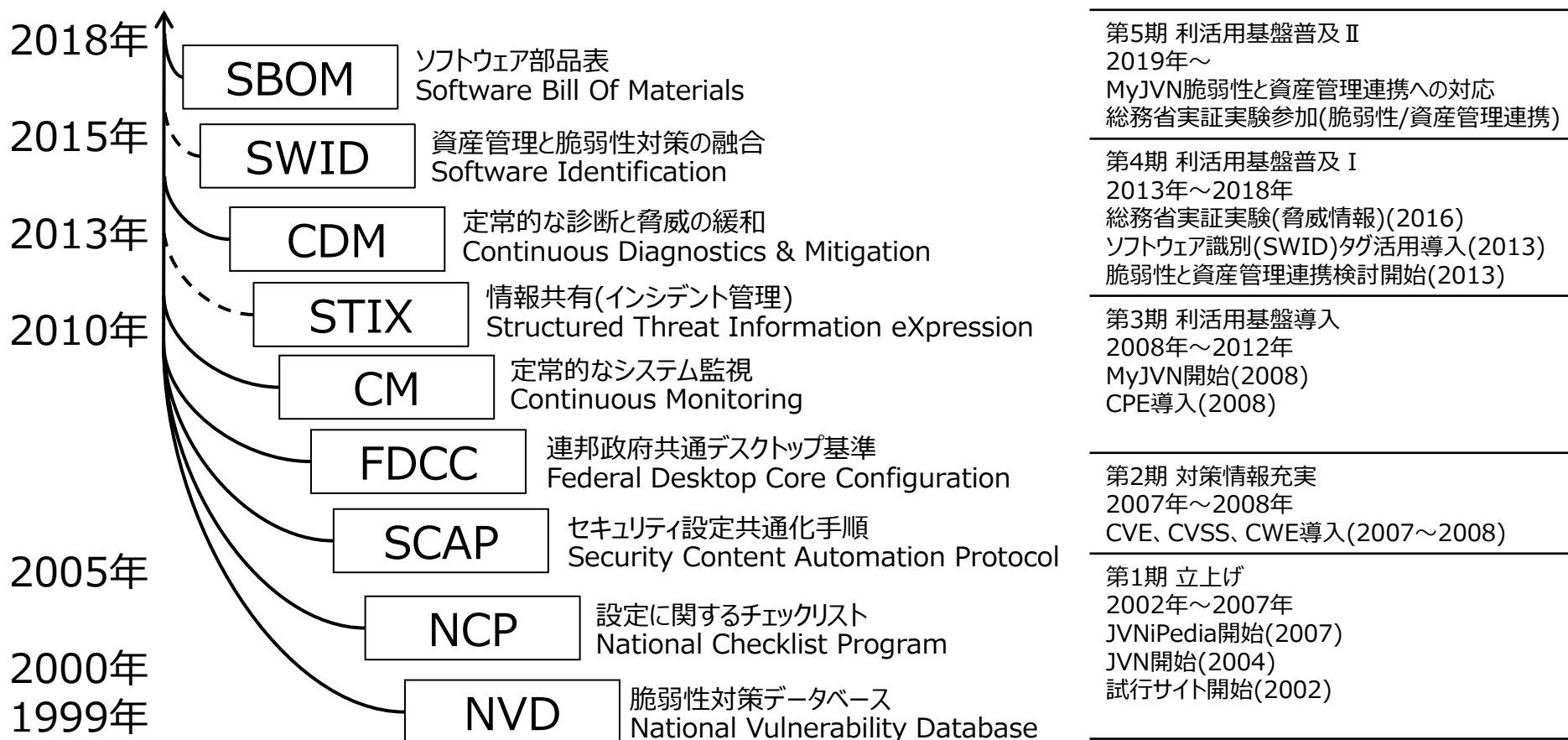
フィルタリング型情報提供
⇒ MyJVN脆弱性対策
情報収集ツール
フィルタリング収集ツール (mjcheck3)
脆弱性対策情報ダッシュボード (mjdashboard)

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



MyJVN : JVN脆弱性対策機械処理基盤

- 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

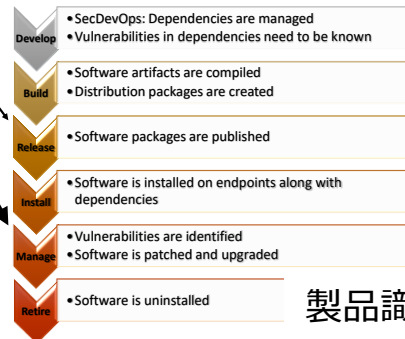


製品識別子に関する課題

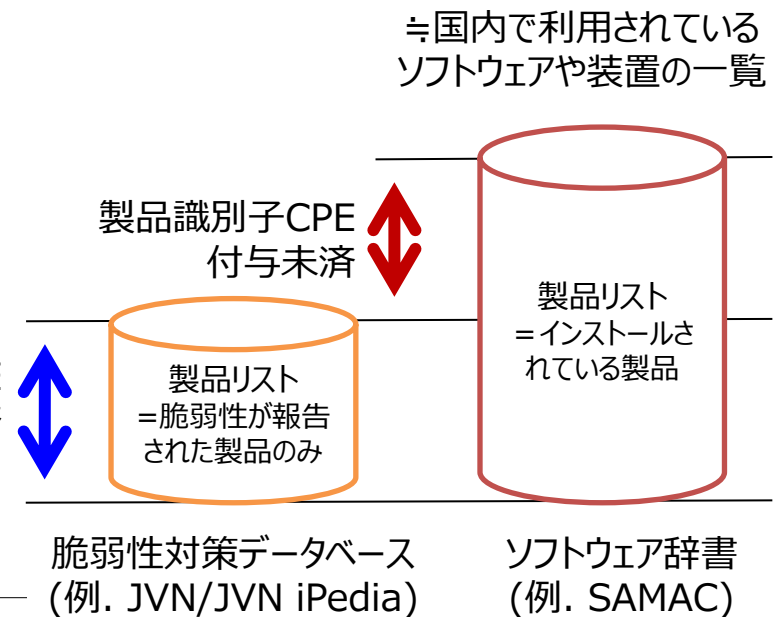
- 製品識別子(CPE)付与の95%は、脆弱性が発見されてから、、、この課題を解決するために、NVDは製品識別子としてSWIDの採用推進
 - CPE : NVD主体で製品識別子を付与
 - SWID : 製品ベンダ主体で製品識別子を付与(インストール時に同梱)

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!



製品識別子CPE
付与済



解決のためのアプローチ：CPEとSWIDの活用

- 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 製品識別子(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

ソフトウェア辞書とのデータ連携
～具体的な取り組み～

IPA

- 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

～JVN iPediaの脆弱性対策情報とソフトウェア資産管理情報のデータ連携に着手～
<https://www.ipa.go.jp/about/press/20160309.html>

2017 Information-technology Promotion Agency, Japan

ユーザアプリ用構成データとの連携
SWIDを用いた構成データの記述

- SWIDを用いたユーザアプリ用の構成データの記述

ソフトウェア識別(SWID)の例

```
<?xml version="1.0" encoding="UTF-8"?>
<swid:SoftwareIdentity
  name="JVN iPedia Web Application"
  version="3.5.0"
  tagId="ipa.go.jp+jvn_ipedia+3.5.0"
  versionScheme="multipartnumeric"
>
  <swid:Entity
    name="独立行政法人 情報処理推進機構"
    regId="ipa.go.jp"
    role="softwareCreator" />
  <swid:Meta product="jvn_ipedia"
    productFamily="JVN" />

  <swid:Link href="cpe:/a:openssl:openssl" rel="related"/>
  <swid:Link href="cpe:/a:openssh:openssh" rel="related"/>
  <swid:Link href="cpe:/a:apache:http_server" rel="related"/>

</swid:SoftwareIdentity>
```

ユーザアプリケーションに関する情報

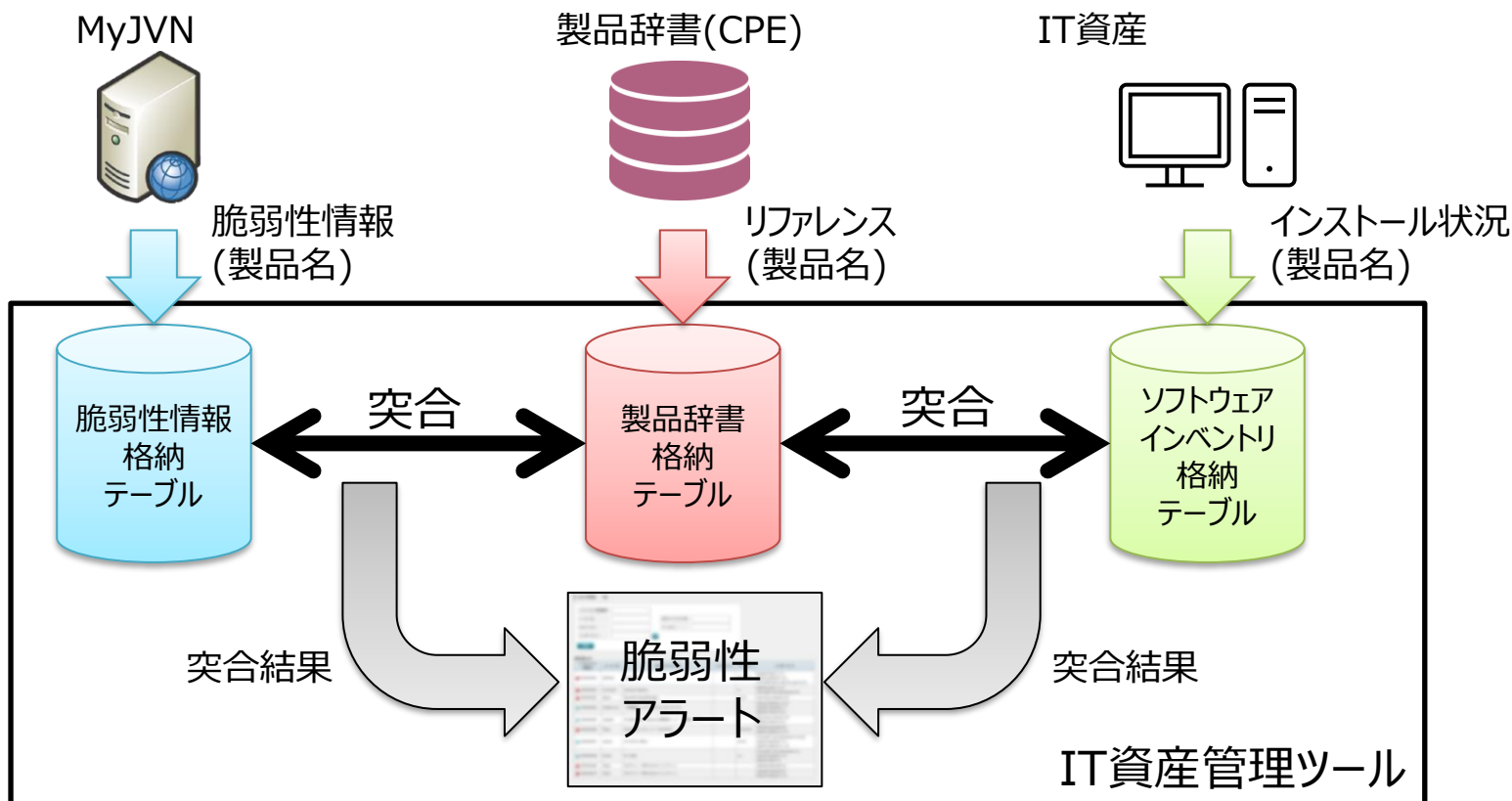
使用する外部コンポーネントや前提プログラムをリストアップ

2017 Information-technology Promotion Agency, Japan

[出典] 「ソフトウェア識別管理に向けた分析事業」の報告書 (2016)
<https://www.ipa.go.jp/files/000051147.pdf>

短期的：製品識別子(CPE)を用いた連携

- 脆弱性情報(製品名)とインストール状況(製品名)との対応表である製品辞書(CPE)を用いた突合



短期的：製品識別子(CPE)を用いた連携

- 製品辞書(CPE)を用いた突合

製品辞書(CPE)

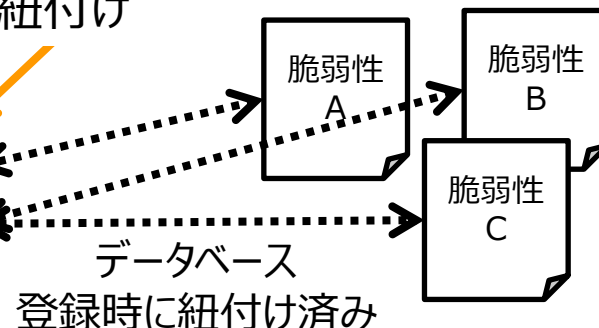
インストール状況
(製品名)

ソフトウェアインベントリ項目				連携用項目
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

脆弱性情報
(製品名)

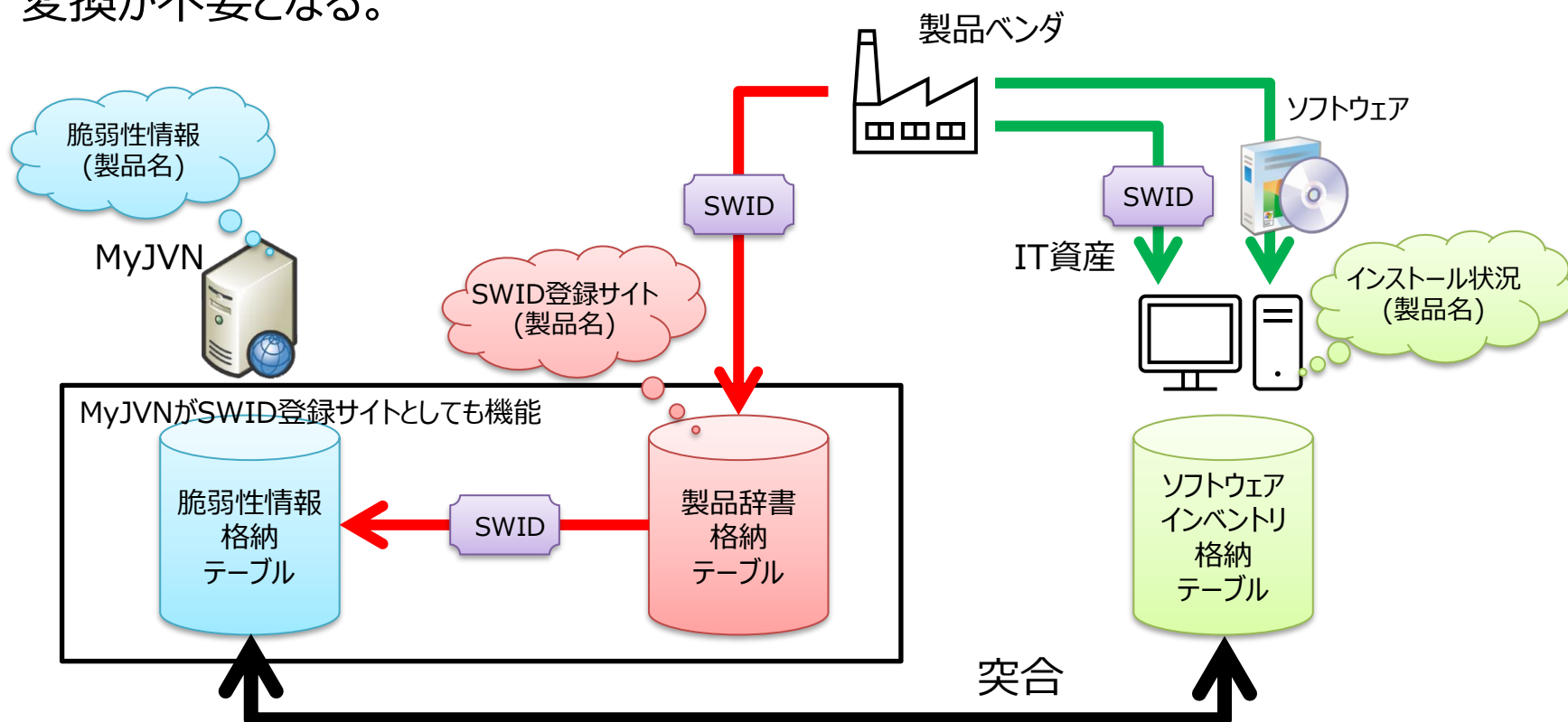
製品識別子CPEを用いた紐付け

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



長期的：ISO/IEC 19770-2 製品識別子(SWID)を用いた連携

- ISO/IEC 19770-2 製品識別子(SWID)の仕組みを用いれば、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。



製品識別子使用にあたっての課題

- (#1) 製品ベンダ主体で製品識別子が付与されない製品について、
どのように対処していけば良いのか？
- National Software Reference Library (NSRL)のハッシュ値で代用
 - 製品識別子CPEの付与 など
- (#2) 製品ベンダ主体で付与された製品識別子(インストール時に同梱)を、
どのように流通させれば良いのか？
- SWIDを登録する仕組み(TAGVault.Org)を活用するというアプローチもあったが、、、
- (#3) 使用できる製品識別子であることを確認するためには？
- インストール時に同梱するSWIDへのXML署名
 - SWIDを登録する仕組みの活用 など

製品識別子使用にあたっての課題

(#4) どの製品識別子を使えば良いのか?

- CPE v2.3

cpe:2.3:{種別}:{ベンダ}:{製品}:{バージョン}:{アップデート}:{エディション}:{言語}:{sw_edition}:{target_sw}:{target_hw}:{その他}

- purl

pkg:{タイプ}/{名前空間}/{パッケージ名}@{バージョン}?{修飾子}#{パス}

- SWID

グローバルなユニークIDで、16バイトのUUID、またはタグ生成者によって定義された値

多種多様

識別子 形式	CPE	Package-Manager	SWHIDs	Hash	SWID	
					UUID	ユニークID
SPDX	CPEフィールド使用 (CPE 2.2, 2.3)	Package-Manager フィールド使用(maven- central, npm, nuget, bower, purl)	swhフィールド 使用	Otherフィールド使用		
CycloneDX		purlフィールド使用	SWIDフィールド 使用	Hashフィールド 使用	SWIDフィールド使用	
SWID	tagidフィールド使用					

解決のためのアプローチ：製品識別子を関連付けるための製品辞書

- JVN製品識別子を用いた、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(国内)製品に識別子を付与し、その製品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"},
            {"vendorpid": "製品識別子"},
            {"spdxid": "SPDX識別子"},
            {"purl": "purl識別子"},
            {"sha256": "ハッシュ値"}
          ]
        },
        {"製品2"},
        ...
      ]
    },
    {"製品2"},
    ...
  ]
}
```

ベンダ	JVNベンダ識別子
	ベンダ名
	CPEベンダ名



製品	JVN製品識別子
	製品名(日本語 英語)
	cpe(CPE2.3製品識別子)
	nvdpid(SWID(UUID)識別子)
	vendorpid(製品識別子)
	spdxid(SPDX識別子)
	purl(purl識別子)
	ハッシュ(ハッシュ値)

JVN製品識別子

- MyJVN製品辞書で使用する管理用製品識別子

#	課題	解決のためのアプローチ
1	製品ベンダ主体で製品識別子が付与されない製品について、どのように対処していけば良いのか？	製品識別子が付与されない製品の識別子として使用する。
2	製品ベンダ主体で付与された製品識別子を、どのように流通させれば良いのか？	多様な製品識別子を関連付けるための識別子として使用する。
3	使用できる製品識別子であることを確認するためには？	
4	どの製品識別子を使えば良いのか？	

【形式】

jvnpid:1.0:{ベンダ}:{製品}:{バージョン(5桁固定)}:
{アップデート}:{エディション}:{言語}:{sw_edition}:{target_sw}:{target_hw}:{その他}

【例】

jvnpid:1.0:sysbom.sample.jp:bomgen:0.46.3.0.0

JVN製品識別子

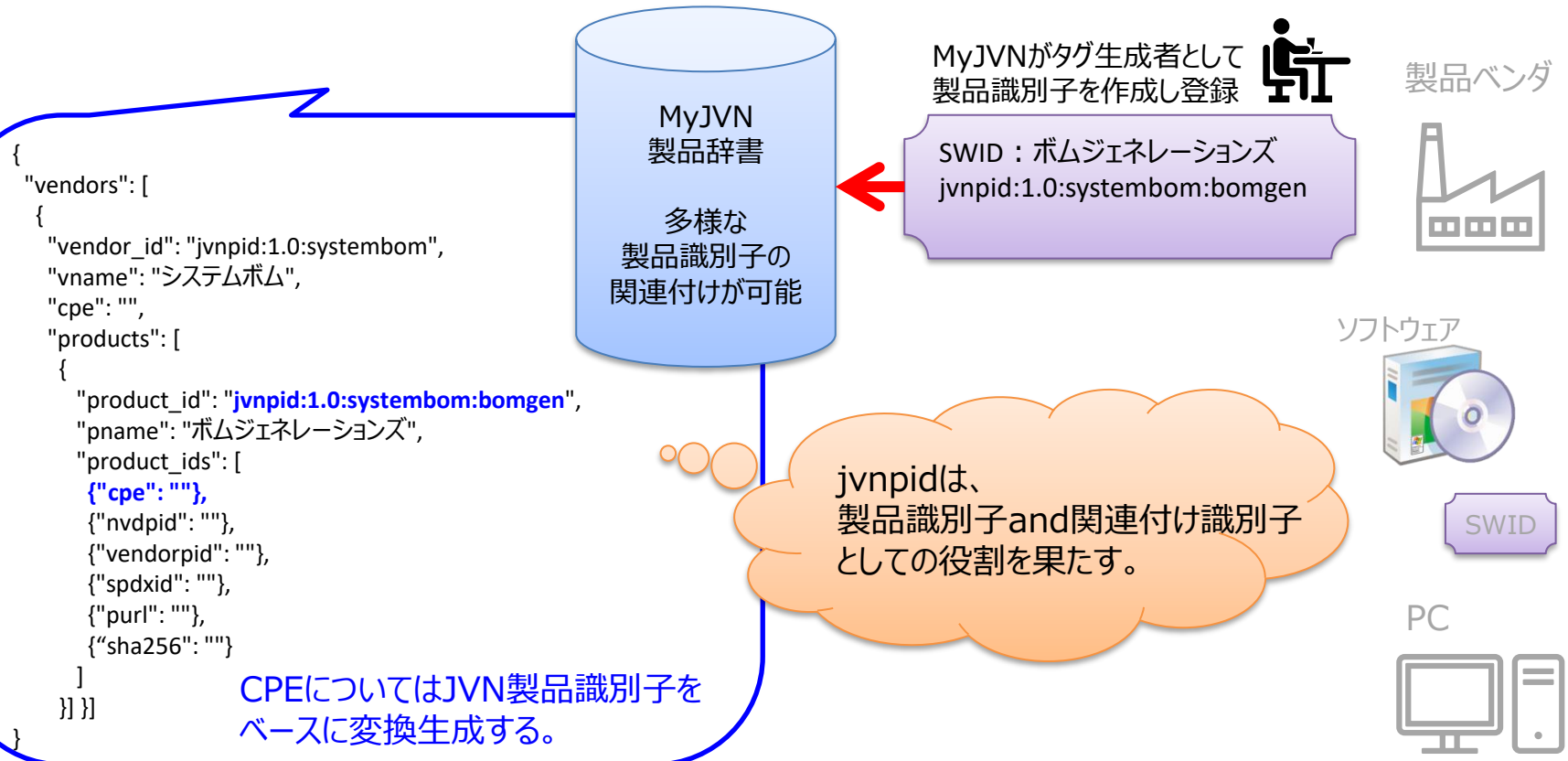
- MyJVN製品辞書で使用する管理用製品識別子
 - CPEとの互換性を考慮した形式
 - 主として{ベンダ}:{製品}を使用することで表記ゆれを防ぐ
 - バージョン(5桁固定)形式を定型化し、バージョン比較の容易性を確保
 - バージョン範囲指定などの記述可とするため、構造型形式を採用
 - 構造型(purl, CPE)
 - 非構造型(ハッシュ、UUID)
 - jvnpidを用いた影響バージョンの範囲指定の例

```
{
  "product_status": {
    "known_affected": [
      {
        "product_id": "jvnpid:1.0:systembom:bom",
        "cpe": "cpe:2.3:a:systembom:bom",
        "versions": [
          { "at": "1.1.1.0.0" },
          { "greaterThanOrEqual": "1.33.2.0.0", "lessThan": "2.7.8.0.0" },
          { "greaterThan": "3.33.2.0.0", "lessThanOrEqual": "5.7.8.0.0" },
          { "lessThanOrEqual": "0.9.34.0.0" }
        ]
      }
    ]
  }
}
```

JVN製品識別子

(#1) 製品ベンダ主体で製品識別子が付与されない製品について、
どのように対処していけば良いのか？

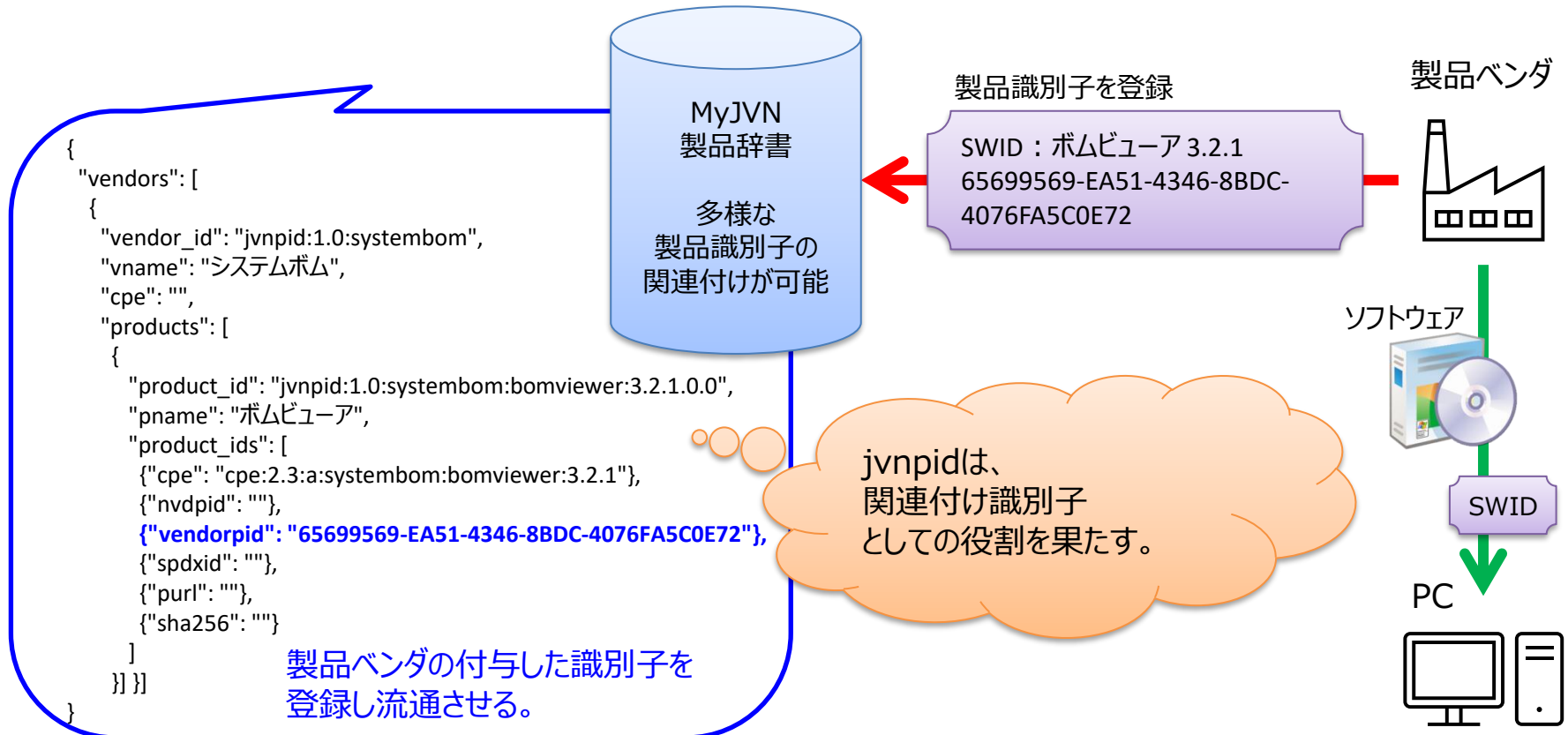
⇒ MyJVN製品辞書は**タグ生成者**ならびに**登録サイト**として機能する。



JVN製品識別子

(#2) 製品ベンダ主体で付与された製品識別子(インストール時に同梱)を、
どのように流通させれば良いのか?

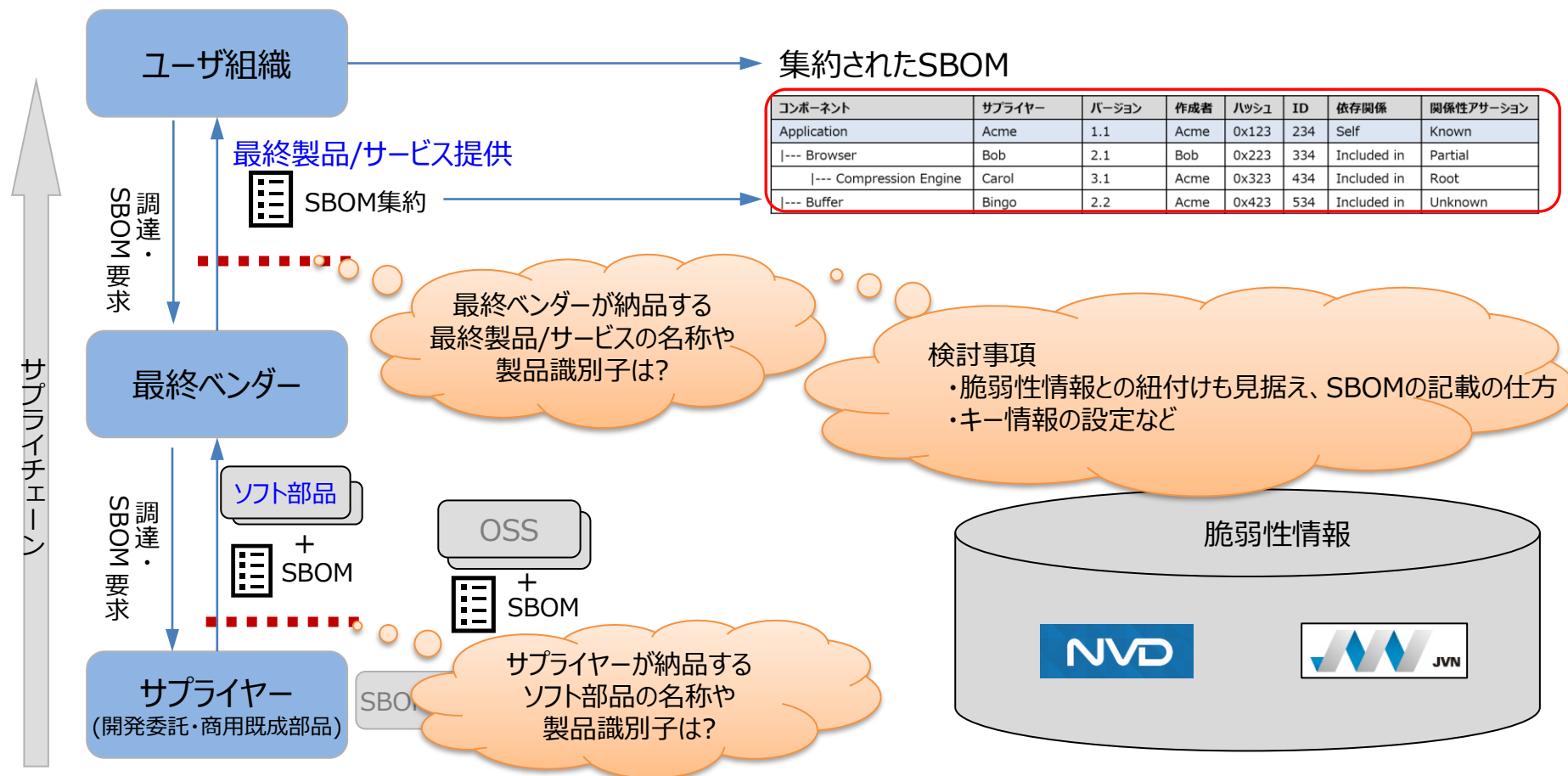
⇒ MyJVN製品辞書は登録サイトとして機能する。



SBOMを用いた脆弱性対応

SBOMにおけるソフトウェア名称などの記載に係る課題

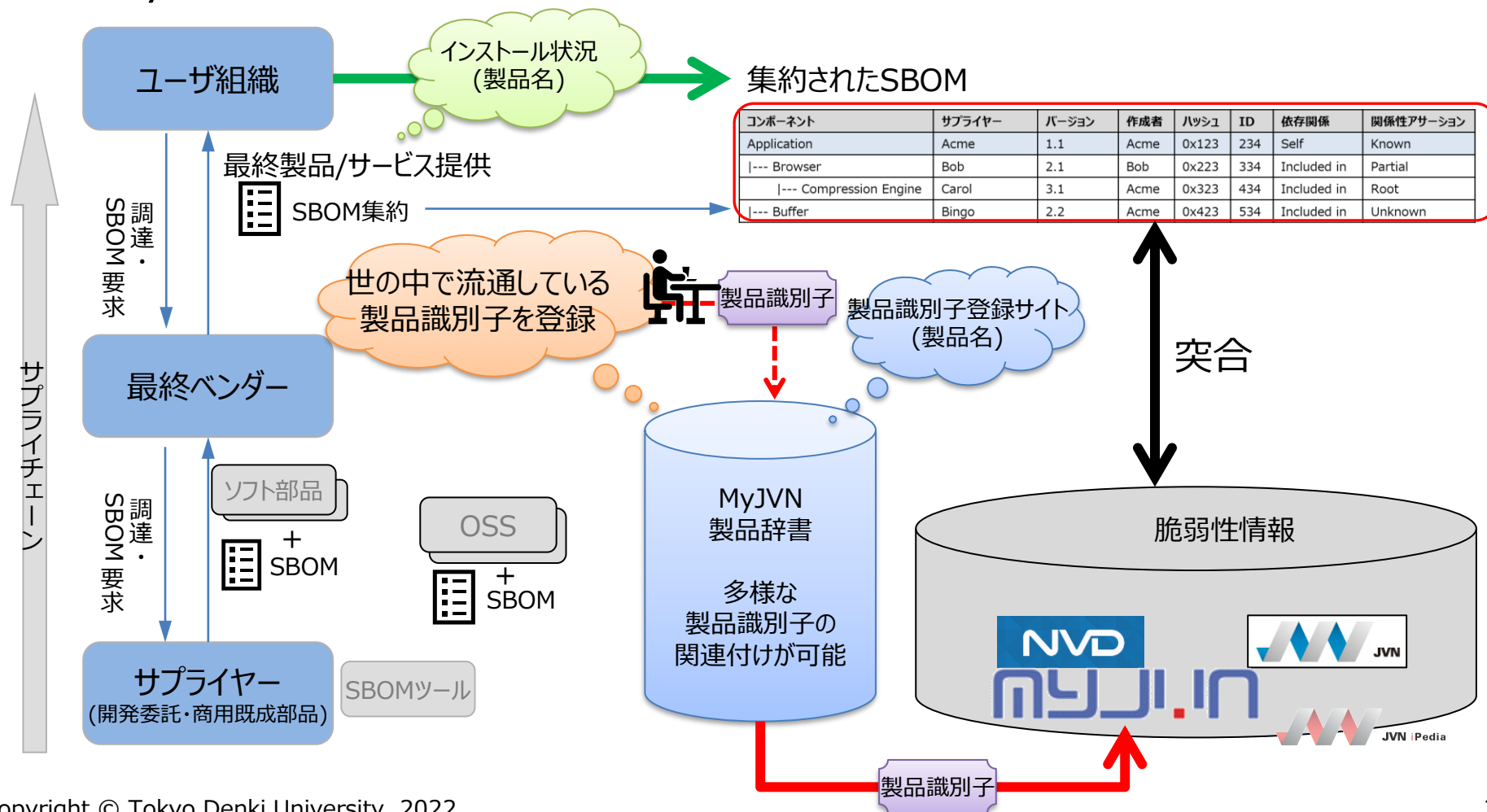
- 表記ゆれなど、SBOMを用いた脆弱性対応も踏まえ、検討が必要



SBOMを用いた脆弱性対応

解決のためのアプローチ：MyJVN製品辞書の活用

- MyJVN製品辞書に世の中で流通している製品識別子を登録



解決のためのアプローチ：MyJVN製品辞書の活用

- MyJVN製品辞書を用いた製品識別子変換により突合を支援

集約されたSBOM(例えば、purlベース)

pkg:rpm/sysbom/bomgen

脆弱性管理ツール(例えば、CPEベース)

cpe:2.3:a:systembom:bomgen

突合



脆弱性対策情報

CVE-2022-000000

cpe:2.3:a:systembom:bomgen

MyJVN
製品辞書

多様な
製品識別子の
関連付けが可能

脆弱性情報



```
{
  "vendors": [
    {
      "vendor_id": "jvnpid:1.0:systembom",
      "vname": "システムボム",
      "cpe": "cpe:2.3:a:systembom",
      "products": [
        {
          "product_id": "jvnpid:1.0:systembom:bomgen",
          "pname": "ボム",
          "product_ids": [
            {"cpe": "cpe:2.3:a:systembom:bomgen"},
            {"nvdpid": ""},
            {"vendorpid": ""},
            {"spdxid": ""},
            {"purl": "pkg:rpm/sysbom/bomgen"},
            {"sha256": ""}
          ]
        }
      ]
    }
  ]
}
```

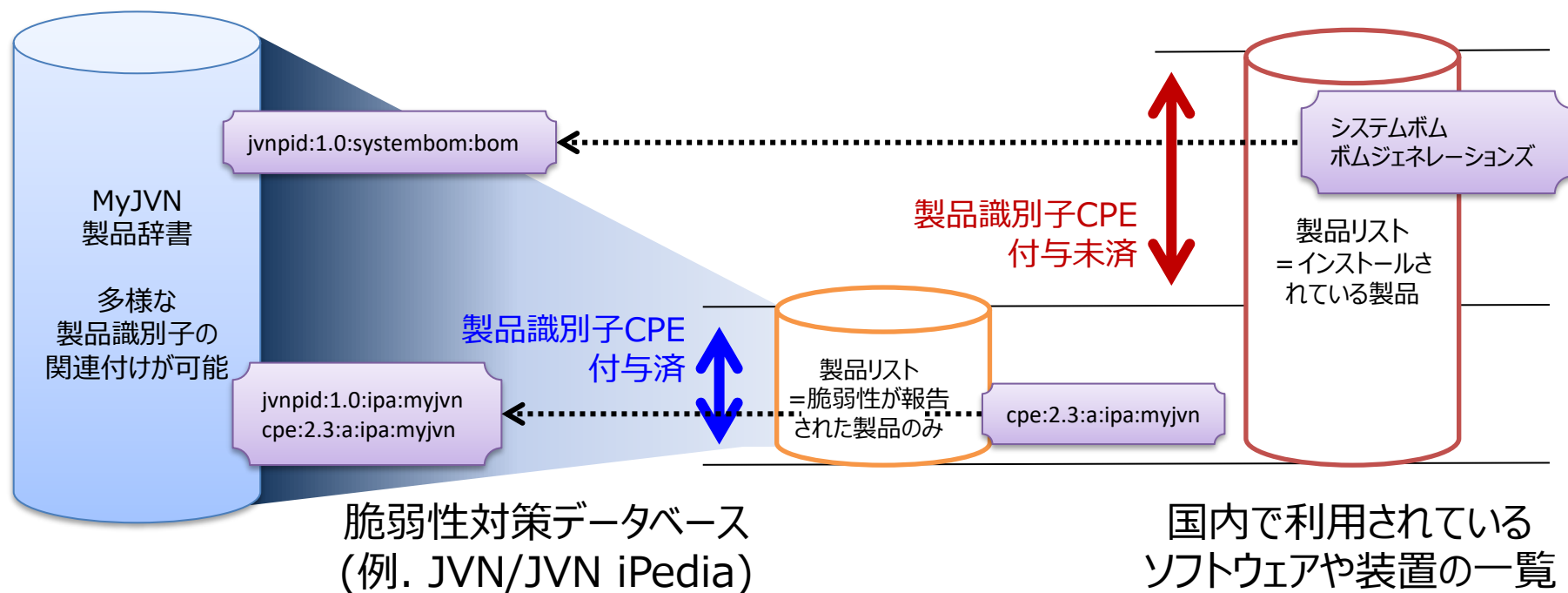
脅威情報／脆弱性対策情報と資産管理との連携



多層防御としての情報活用基盤と想定する将来像

実現のカギは製品識別

- 実現のための最初の一步は、製品識別子CPE付与未済への対応
 - IT資産管理規格 ISO/IEC 19770-2 SWID(ソフトウェア識別子)活用
 - SWIDの仕組みを用いて、国内で利用されているソフトウェアや装置に、CPEとの互換性を持つ構造化識別子を適用する。



Collaborate
together
to make our
Internet
secure.

