IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

JVNにおけるSCAP活用について

JVN: Japan Vulnerability Notes
SCAP: Security Content Automation Program

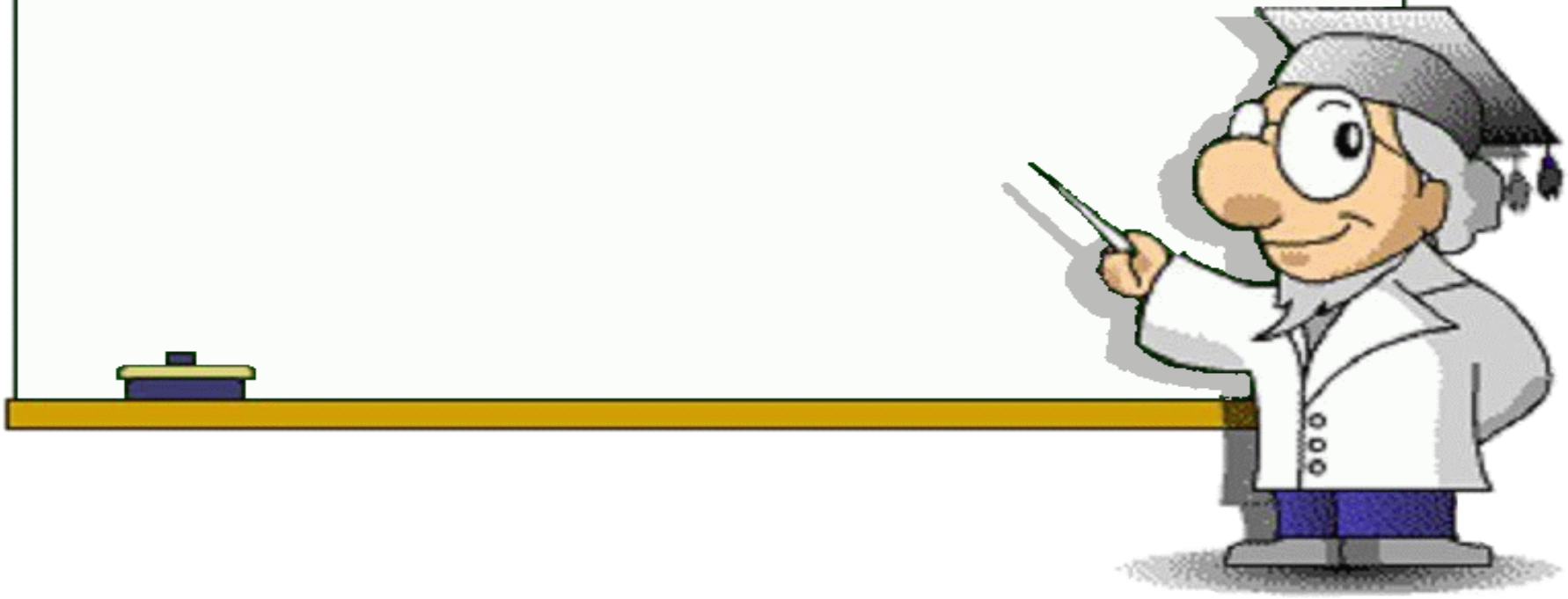
独立行政法人 情報処理推進機構（IPA）
セキュリティセンター　研究員
JPCERTコーディネーションセンター
専門委員

寺田真敏

2010年10月13日

目次

1. JVN脆弱性対策機械処理基盤
2. MyJVNフレームワークでのSCAP利用
3. 参考情報：SCAPの概要



JVN脆弱性対策機械処理基盤

＝（JVN＋JVN iPedia）× MyJVN
＝ MyJVNフレームワーク

- JVN＋JVN iPediaを活用し、必要とされる新たなサービスを整備できる環境（MyJVN）を準備していくことで、自動化などの効率的な脆弱性対策を目指すことのできる利活用基盤
- 国際性（インターネット向け脆弱性対策情報の情報源）と地域性（日本国内向け脆弱性対策情報データベース）とを両立させたグローバルなJVN（世界に冠たるJVN）の実現

MyJVNフレームワークでは
「セキュリティ設定共通化手順SCAP」を
活用しています！

JVN脆弱性対策機械処理基盤

＝（国際性＋地域性）× 利活用基盤

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 Noti

JVN iPedia

JVN iPedia

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**

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。

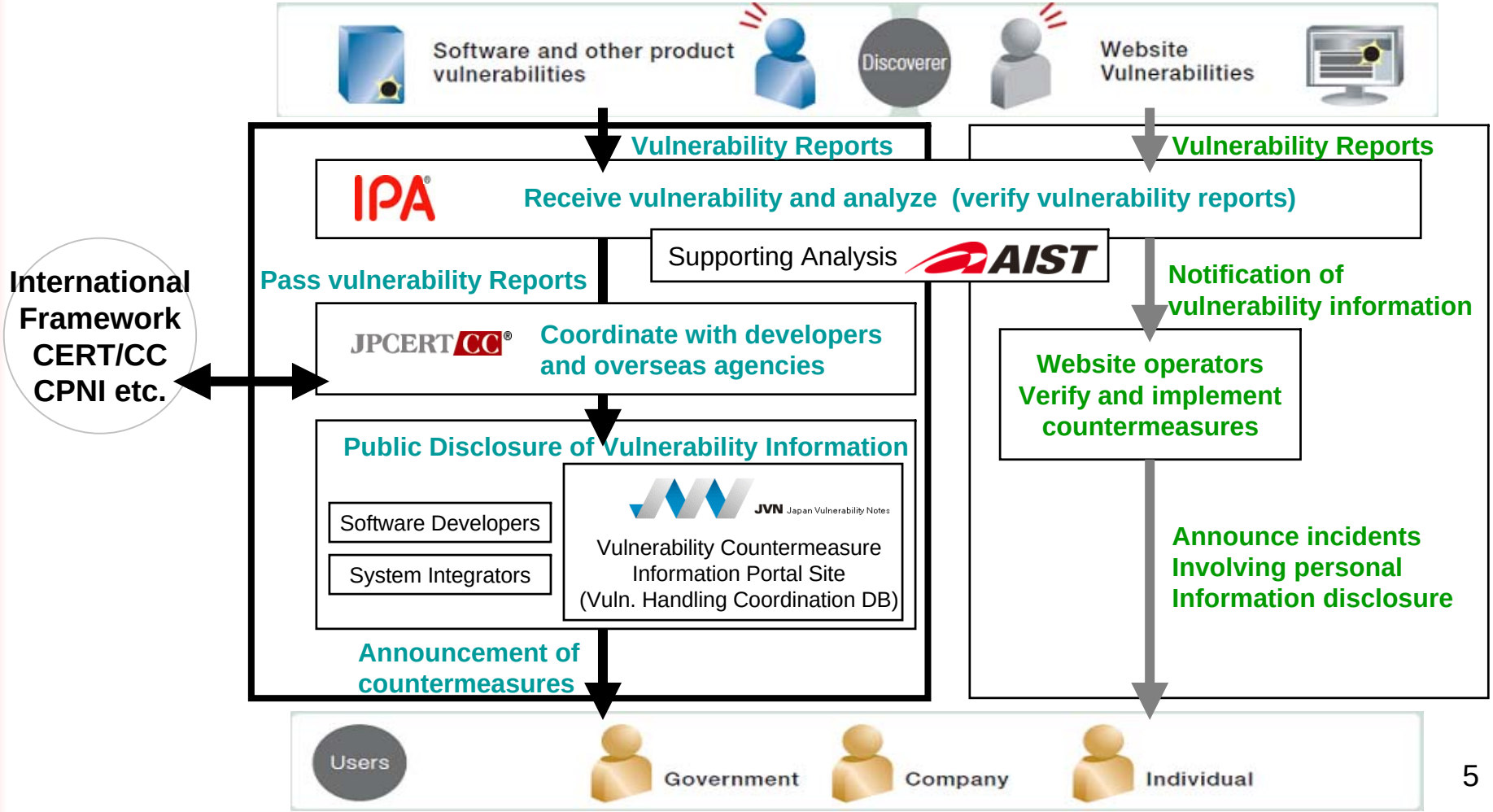
JVN iPedia
国内で利用されている製品を対象にした脆弱性対策情報を広く蓄積する

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脆弱性対策機械処理基盤

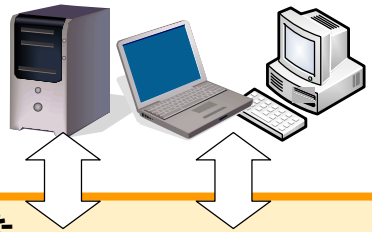
JVN脆弱性対策機械処理基盤

Information Security Early Warning Partnership



JVN脆弱性対策機械処理基盤

共通基準／仕様を用いて国際性と地域性とを兼ね備えたデータベースを活用する。



MyJVN
CVE、CPE、CWE、CVSSなど共通基準を用いた
フレームワークサービス（MyJVN API）の提供

JVN（JVN#12345678）
Vulnerability Handling Coordination Database

日本語サイト
http://jvn.jp/

英語サイト
http://jvn.jp/en/

情報セキュリティ早期警戒パートナーシップ

CERT/CC CPNI 等

日本国内製品開発者サイト

NVD（英語）（約42,896件）

情報セキュリティ早期警戒パートナーシップ案件（426件）

翻訳

情報セキュリティ早期警戒パートナーシップ案件（426件）

CERT/CC、CPNI等案件（361件）

蓄積

JPCERT CC®

JVN iPedia（JVNDB-yyyy-0123456）
Vulnerability Archiving Database

日本語サイト
http://jvndb.jvn.jp/

英語サイト
http://jvndb.jvn.jp/en/

JVN案件（787件）

蓄積

JVN案件（441件）

（計:539件）

日本国内製品開発者案件（98件）

翻訳

日本国内製品開発者案件（98件）

NVD（7,561件）

（計:8,446件）

IPA

2010年第2四半期の登録件数

http://www.ipa.go.jp/security/vuln/report/vuln2010q2.html
http://www.ipa.go.jp/security/vuln/report/JVNiPedia2010q2.html

利活用基盤整備の取り組み

脆弱性対策情報ポータルサイトJVNをベースとした利活用（機械処理）基盤の整備と共通基準／仕様の導入

第1期
対策情報
充実期

2002年	6月	JVNプロジェクトの開始
2003年	2月	JVN試行サイトの開設
	7月	JVNRSSフォーマットによる試行配信の開始
2004年	7月	情報セキュリティ早期警戒パートナーシップの開始 脆弱性対策情報ポータルサイト JVN 開設
	8月	利活用（機械処理）基盤に関する検討開始
2005年	9月	JVNRSSフォーマットによる配信の開始
2007年	2月	共通脆弱性評価システム（CVSS）
	4月	脆弱性対策情報データベース JVN iPedia 開設
2008年	5月	JVN 英語サイト、JVN iPedia 英語サイトの開設
	9月	共通脆弱性タイプ一覧（CWE）、CWE互換宣言

利活用基盤整備の取り組み

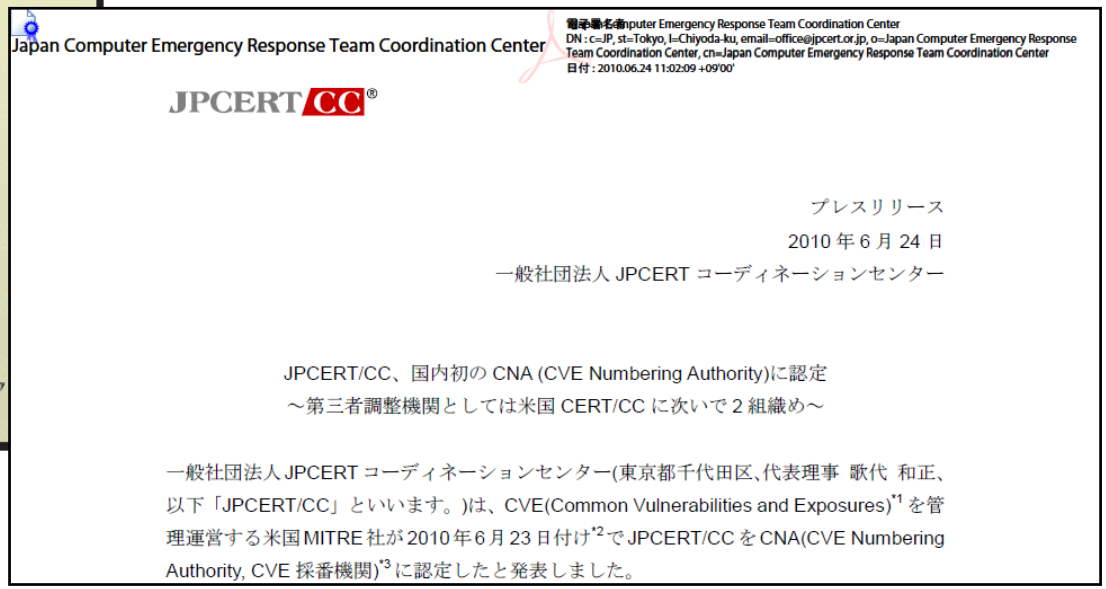
脆弱性対策情報ポータルサイトJVNをベースとした利活用（機械処理）基盤の整備と共通基準／仕様の導入

第2期 利活用基盤整備・共通基準導入期

2008年10月	脆弱性対策情報共有フレームワーク “MyJVN” の開始
	MyJVN脆弱性対策情報収集ツールのリリース
	共通プラットフォーム一覧（CPE）
	共通脆弱性識別子（CVE）
2009年　4月	製品開発者の発信する
	脆弱性対策情報の自動収集の試行開始
2009年11月	MyJVNバージョンチェッカのリリース
	セキュリティ検査言語（OVAL）
2009年12月	MyJVNセキュリティ設定チェッカのリリース
	セキュリティ設定チェックリスト記述形式（XCCDF）
	共通セキュリティ設定一覧（CCE）
2010年　1月	CVE互換取得（JVN、JVN iPedia、MyJVN）
2010年　2月	MyJVN API 公開
2010年　6月	MyJVN - VRDA 連携、JPCERT/CC CNA認定取得

MyJVNフレームワークでのSCAP利用

- **運用面**
  - **CWE互換宣言（2008年10月3日）**
  - **CVE互換取得（JVN、JVN iPedia、MyJVN）（2010年1月5日）**
  - **CNA（CVE Numbering Authority）認定取得（2010年6月24日）**


Japan Computer Emergency Response Team Coordination Center

JPCERT CC®

プレスリリース
2010 年 6 月 24 日
一般社団法人 JPCERT コーディネーションセンター

JPCERT/CC、国内初の CNA (CVE Numbering Authority)に認定
～第三者調整機関としては米国 CERT/CC に次いで 2 組織め～

一般社団法人 JPCERT コーディネーションセンター(東京都千代田区、代表理事 歌代 和正、以下「JPCERT/CC」といいます。)は、CVE(Common Vulnerabilities and Exposures)*1 を管理運営する米国 MITRE 社が 2010 年 6 月 23 日付け*2 で JPCERT/CC を CNA(CVE Numbering Authority, CVE 採番機関)*3 に認定したと発表しました。

MyJVNフレームワークでのSCAP利用

- 技術面
  a. 脆弱性対策情報ポータルサイト JVN
  b. 脆弱性対策情報DB JVN iPedia
  c. CVSS 計算ソフトウェア多国語版
  d. MyJVN API
  e. MyJVN脆弱性対策情報収集ツール
  f. MyJVN - JPCERT/CC VRDA 連携
  g. MyJVNバージョンチェッカ
  h. MyJVNセキュリティ設定チェッカ
  i. Official CPE Dictionary 連携に向けて試行活動

脆弱性対策情報ポータルサイト JVN

http://jvn.jp/

- **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。**

脆弱性対策情報の「関連文書」セクションにCVE番号を記載

脆弱性対策情報DB JVN iPedia

http://jvndb.jvn.jp/

JVN iPedia Vulnerability Countermeasure Information Database

- **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。**

脆弱性対策情報の「CVSSによる深刻度」「参考情報」セクションにCVSS基本値、CVE番号、CWE番号を記載

脆弱性対策情報DB JVN iPedia

http://jvndb.jvn.jp/

JVN iPedia Vulnerability Countermeasure Information Database

- 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。

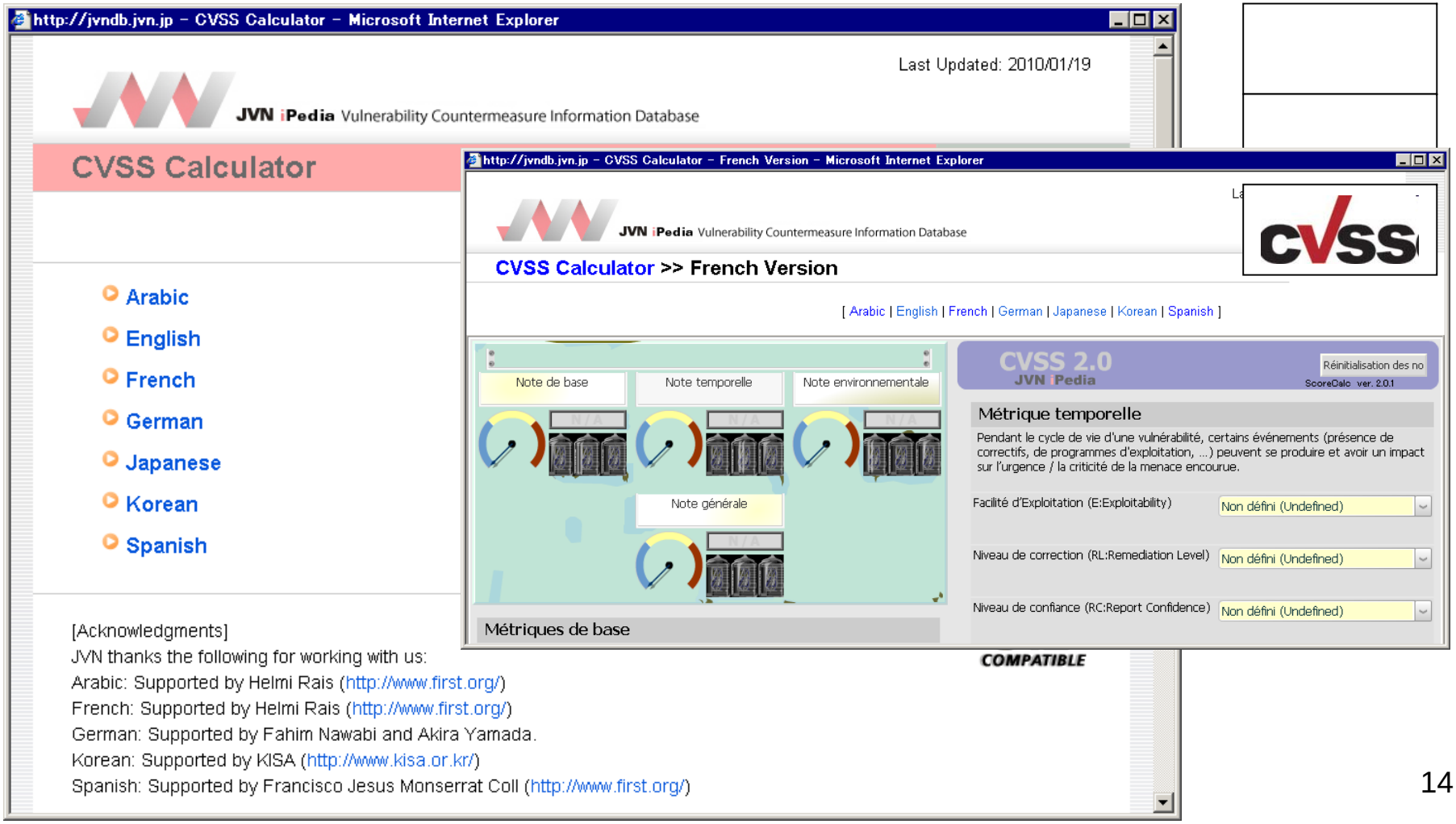
JVNDBRSSファイルの中に、脆弱性の影響を受ける製品のCPE名を記載

CVSS 計算ソフトウェア多国語版

http://jvndb.jvn.jp/cvss/

JVN iPedia Vulnerability Countermeasure Information Database

- **脆弱性対策情報の利活用にあたり、CVSSの普及を図る。**



MyJVN API

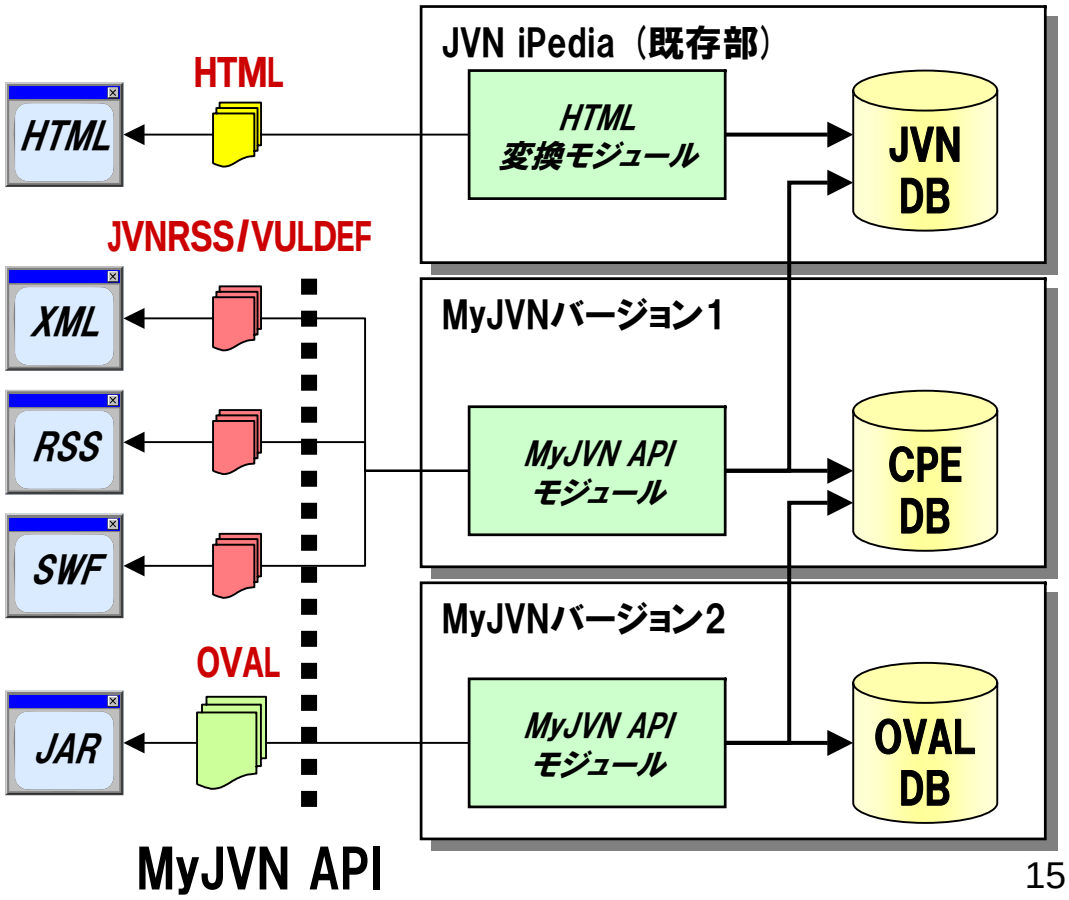
http://jvndb.jvn.jp/apis/

- 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
⇒ JPCERT/CC VRDA連携

検査データ提供
⇒ MyJVNバージョンチェッカ
⇒ MyJVNセキュリティ設定チェッカ



MyJVN API（フィルタリング型情報提供）

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

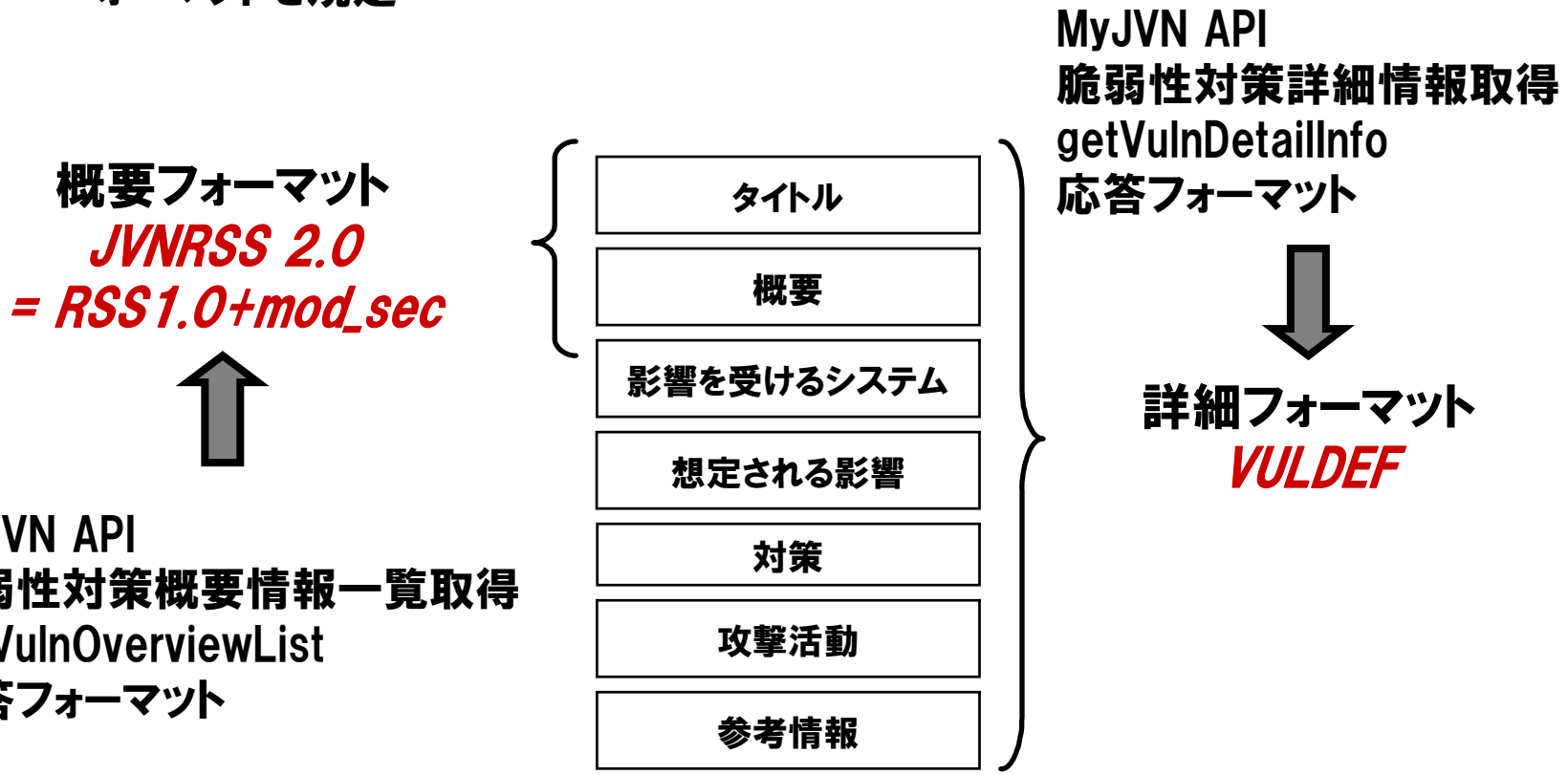
- JVN iPediaを活用し、新たなサービスを準備できる環境を整備する。
  - JVN iPediaの情報を、Webを通じて利用するためのソフトウェアインタフェース
  - フィルタリング型情報提供では、脆弱性対策情報を使用するためのAPIを規定
  - リクエストURLの基本構成
    http://jvndb.jvn.jp/myjvn?method=メソッド&パラメタ

メソッド名称	概要
製品提供者一覧取得 getVendorList	フィルタリング条件に該当する製品提供者一覧をXML形式で取得する
製品一覧取得 getProductList	フィルタリング条件に該当する製品一覧をXML形式で取得する
脆弱性対策概要情報一覧取得 getVulnOverviewList	フィルタリング条件に該当する脆弱性対策情報の概要一覧をJVNRSS形式で取得する
脆弱性対策詳細情報取得 getVulnDetailInfo	フィルタリング条件に該当する脆弱性対策詳細情報をVULDEF形式で取得する

MyJVN API（フィルタリング型情報提供）

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
  - 脆弱性対策情報の記述粒度を考慮し、概要記述向けと詳細記述向けXMLフォーマットを規定



MyJVN API（検査データ提供）

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

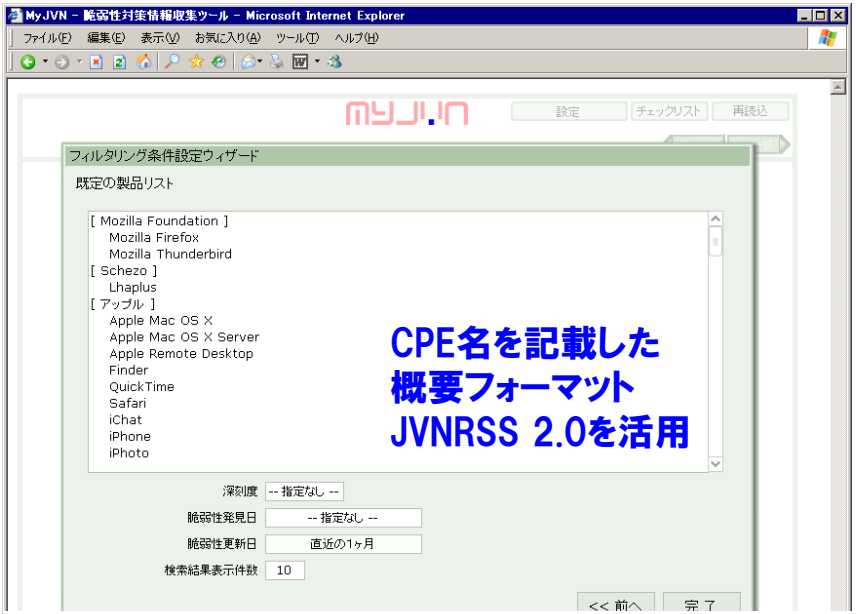
- JVN iPediaを活用し、新たなサービスを準備できる環境を整備する。
  - JVN iPediaの情報を、Webを通じて利用するためのソフトウェアインタフェース
  - 検査データ提供では、OVAL定義データ（チェックするための手続きが記載されたXMLファイル）を使用するためのAPIを規定
  - リクエストURLの基本構成
    http://jvndb.jvn.jp/myjvn?method=メソッド&パラメタ

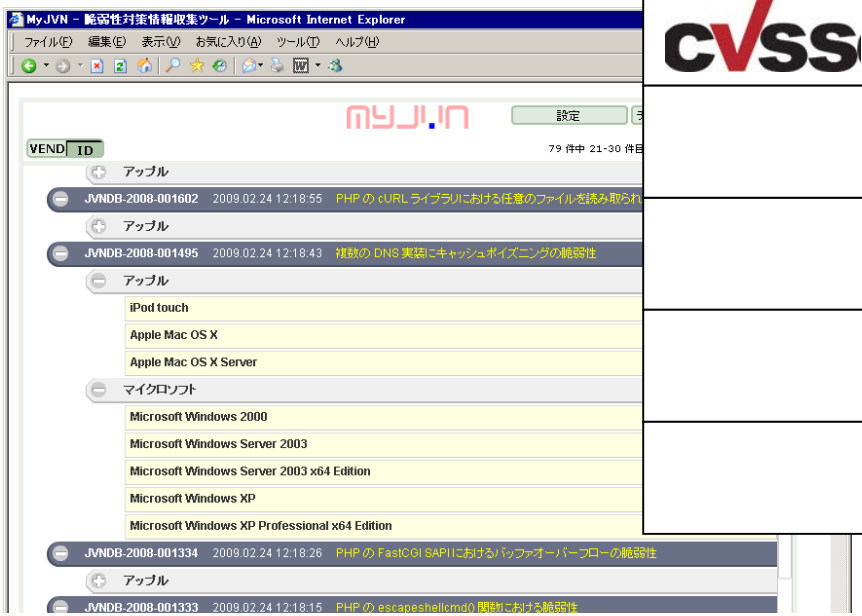
メソッド名称	概要
OVAL定義一覧取得 getOvalList	フィルタリング条件に該当するOVAL定義一覧をXML形式で取得する
OVAL定義データ取得 getOvalData	該当するOVAL定義データをOVAL形式で取得する
チェックリスト取得 getXccdfCheckList	該当するチェックリストをXCCDF形式で取得する

MyJVN脆弱性対策情報収集ツール

http://jvndb.jvn.jp/apis/myjvn/mjcheck.html

- 製品視点から脆弱性対策情報を選別可能なフレームワークを整備する。
  - JVN iPediaの情報を、利用者が効率的に活用できるように、製品視点のフィルタリング条件設定機能を有した脆弱性対策情報収集ツール
  - 利用者に関係する製品視点の脆弱性対策情報のみの表示する。





cve.mitre.org

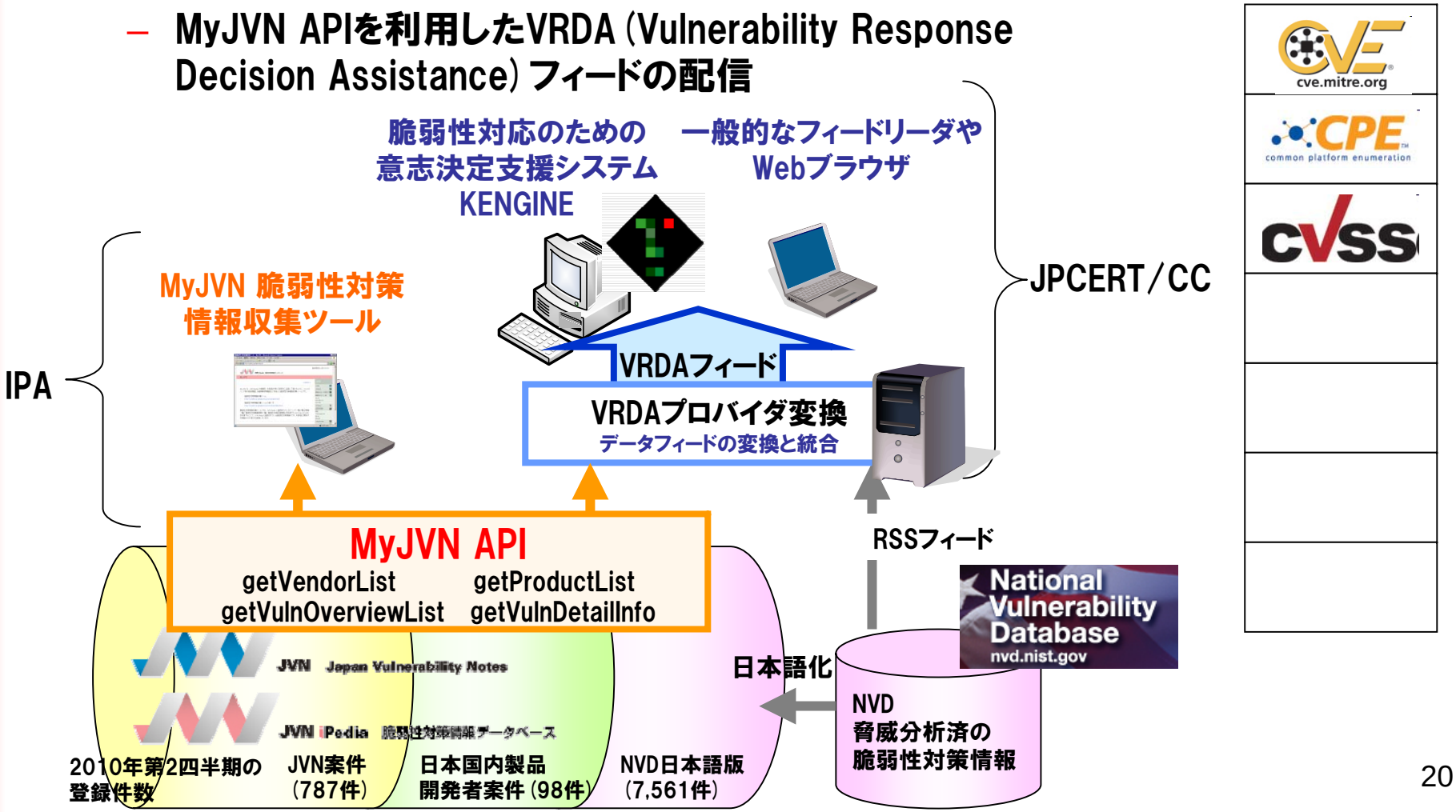
common platform enumeration

http://jvndb.jvn.jp/myjvn?method=getVulnOverviewList&cpeName=cpe:/*:fujitsu:*&rangeDatePublic=n&rangeDatePublished=n&rangeDateFirstPublished=n&lang=en

MyJVN - JPCERT/CC VRDA 連携

http://www.jpcert.or.jp/vrdafeed/

- 脆弱性対策情報サービス同士が連携可能なフレームワークを整備する。
  - MyJVN APIを利用したVRDA (Vulnerability Response Decision Assistance) フィードの配信



MyJVNバージョンチェッカ

http://jvndb.jvn.jp/apis/myjvn/index.html#VCCHECK

- マルチベンダ環境において、ソフトウェア製品の脆弱性対策チェックのフレームワークを整備する。
  - 利用者のPCにインストールされているソフトウェア製品のバージョンが最新であるかを、簡単な操作で確認するツール

（1）チェックリストを作成する。

（2）バージョンをチェックする。

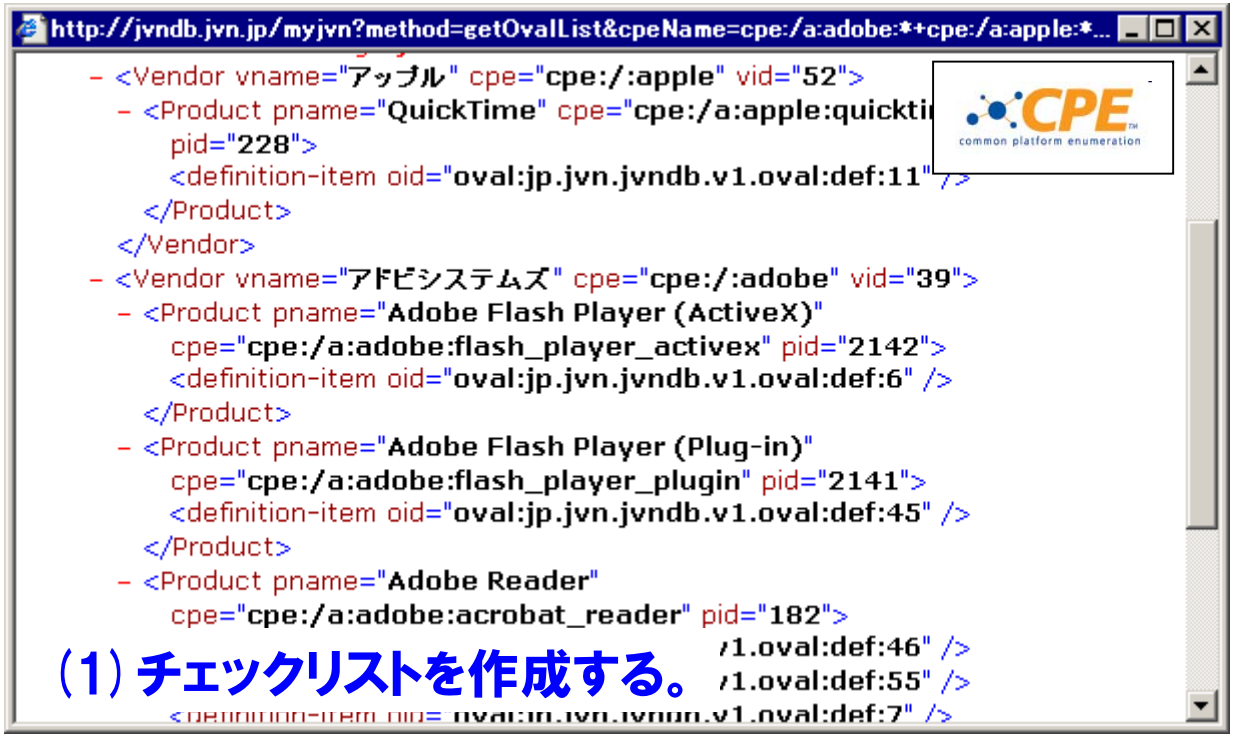
CPE common platform enumeration

OVAL oval.mitre.org

MyJVNバージョンチェッカ

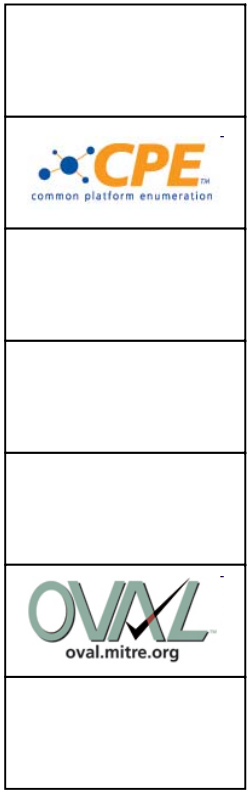
http://jvndb.jvn.jp/apis/myjvn/index.html#VCCHECK

- マルチベンダ環境において、ソフトウェア製品の脆弱性対策チェックのフレームワークを整備する。
  - 利用者のPCにインストールされているソフトウェア製品のバージョンが最新であるかを、 簡単な操作で確認するツール



（1）チェックリストを作成する。

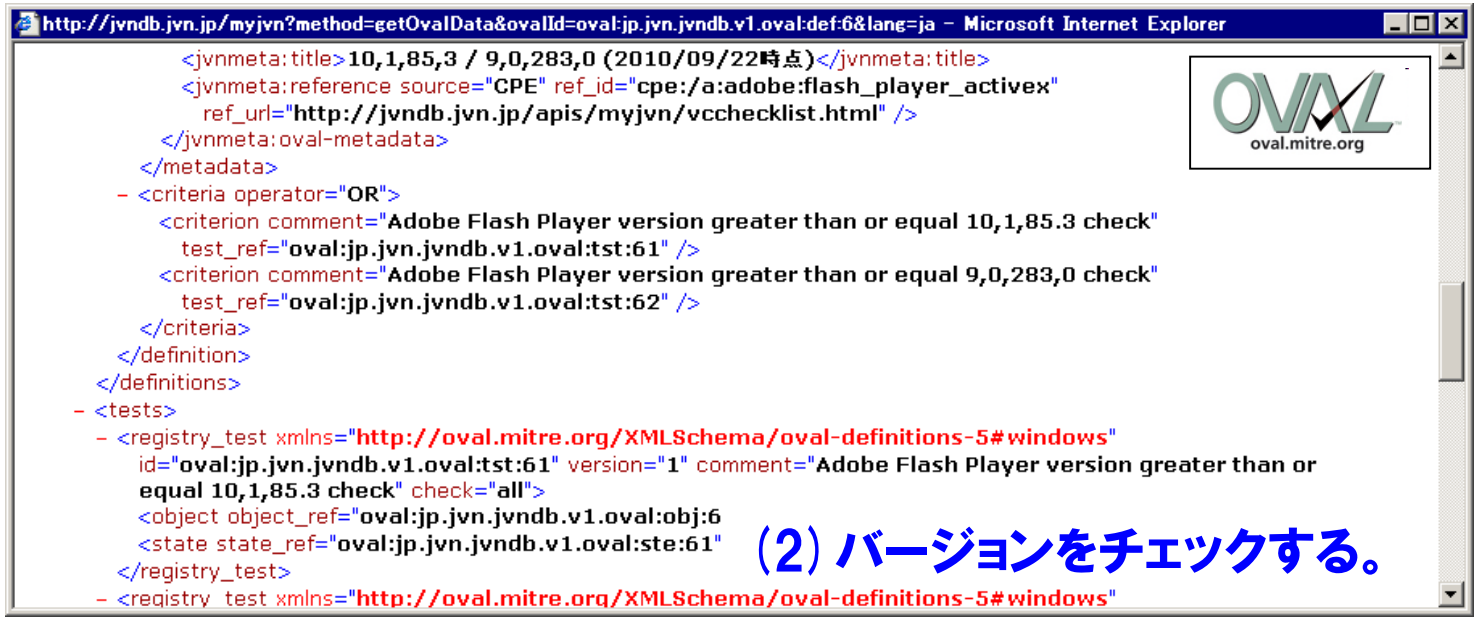
MyJVNバージョンチェッカでは、製品名を記載したチェックリスト作成にあたり、CPE名を利用



MyJVNバージョンチェッカ

http://jvndb.jvn.jp/apis/myjvn/index.html#VCCHECK

- マルチベンダ環境において、ソフトウェア製品の脆弱性対策チェックのフレームワークを整備する。
  - 利用者のPCにインストールされているソフトウェア製品のバージョンが最新であるかを、 簡単な操作で確認するツール
  - チェックリストに基づき、バージョンが最新であるかどうかのチェックを手作業ではなく、ツールにより作業を自動化する。



CPE common platform enumeration

OVAL oval.mitre.org

MyJVNバージョンチェッカでは、製品のバージョンチェックにOVALを利用

MyJVNセキュリティ設定チェッカ

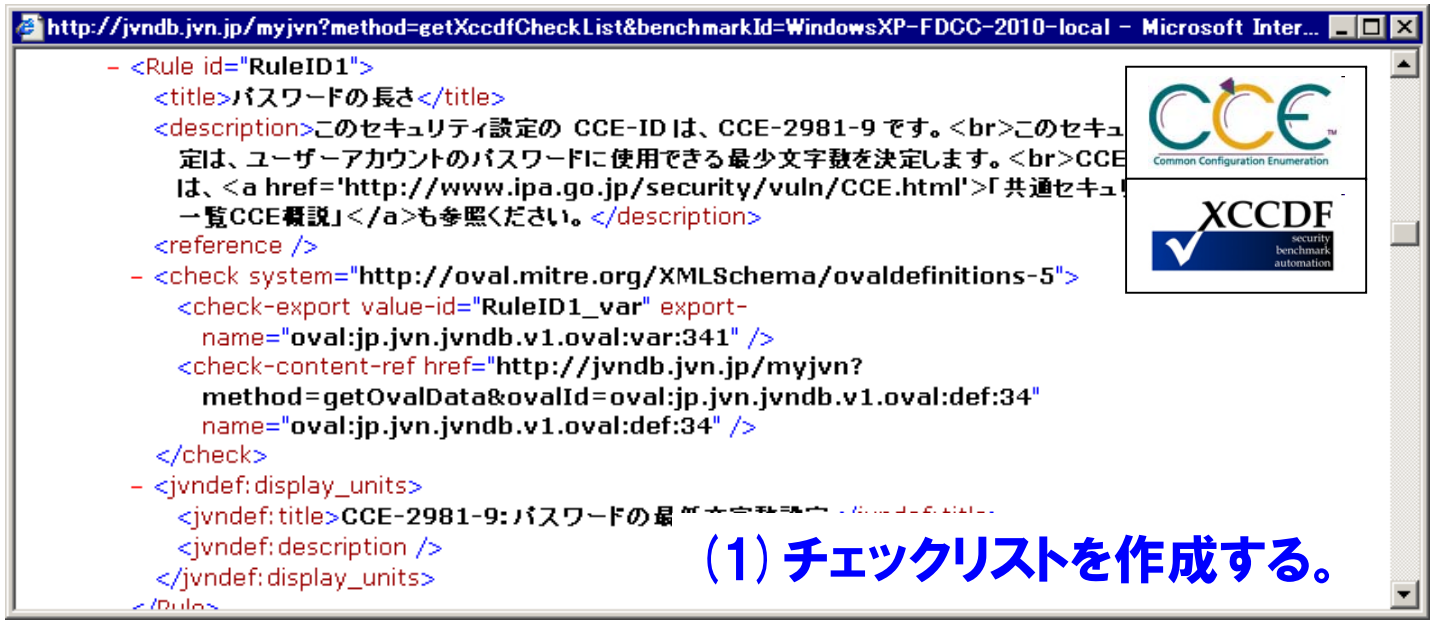
http://jvndb.jvn.jp/apis/myjvn/index.html#CCCHECK

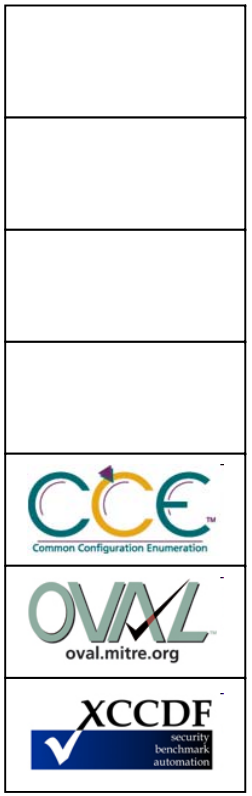
- 設定に関する脆弱性対策チェックのフレームワークを整備する。
  - 利用者のPCの設定を簡単な操作で確認するツール
  - チェックリストに基づき、設定が適切かどうかのチェックを手作業ではなく、ツールにより作業を自動化する。

MyJVNセキュリティ設定チェッカ

http://jvndb.jvn.jp/apis/myjvn/index.html#CCCHECK

- 設定に関する脆弱性対策チェックのフレームワークを整備する。
  - 利用者のPCの設定を簡単な操作で確認するツール
  - チェックリストに基づき、設定が適切かどうかのチェックを手作業ではなく、ツールにより作業を自動化する。



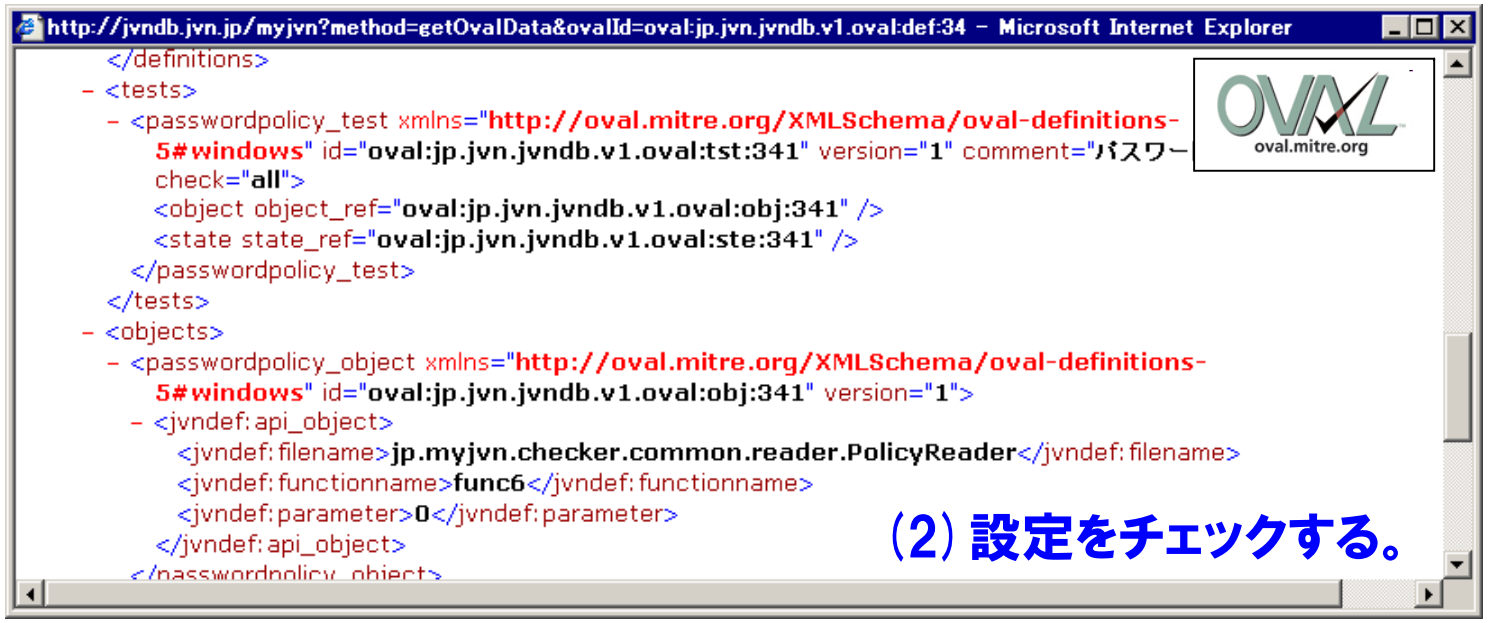


MyJVNセキュリティ設定チェッカでは、設定項目を記載したチェックリスト作成にあたり、CCEとXCCDFを利用

MyJVNセキュリティ設定チェッカ

http://jvndb.jvn.jp/apis/myjvn/index.html#CCCHECK

- 設定に関する脆弱性対策チェックのフレームワークを整備する。
  - 利用者のPCの設定を簡単な操作で確認するツール
  - チェックリストに基づき、設定が適切かどうかのチェックを手作業ではなく、ツールにより作業を自動化する。



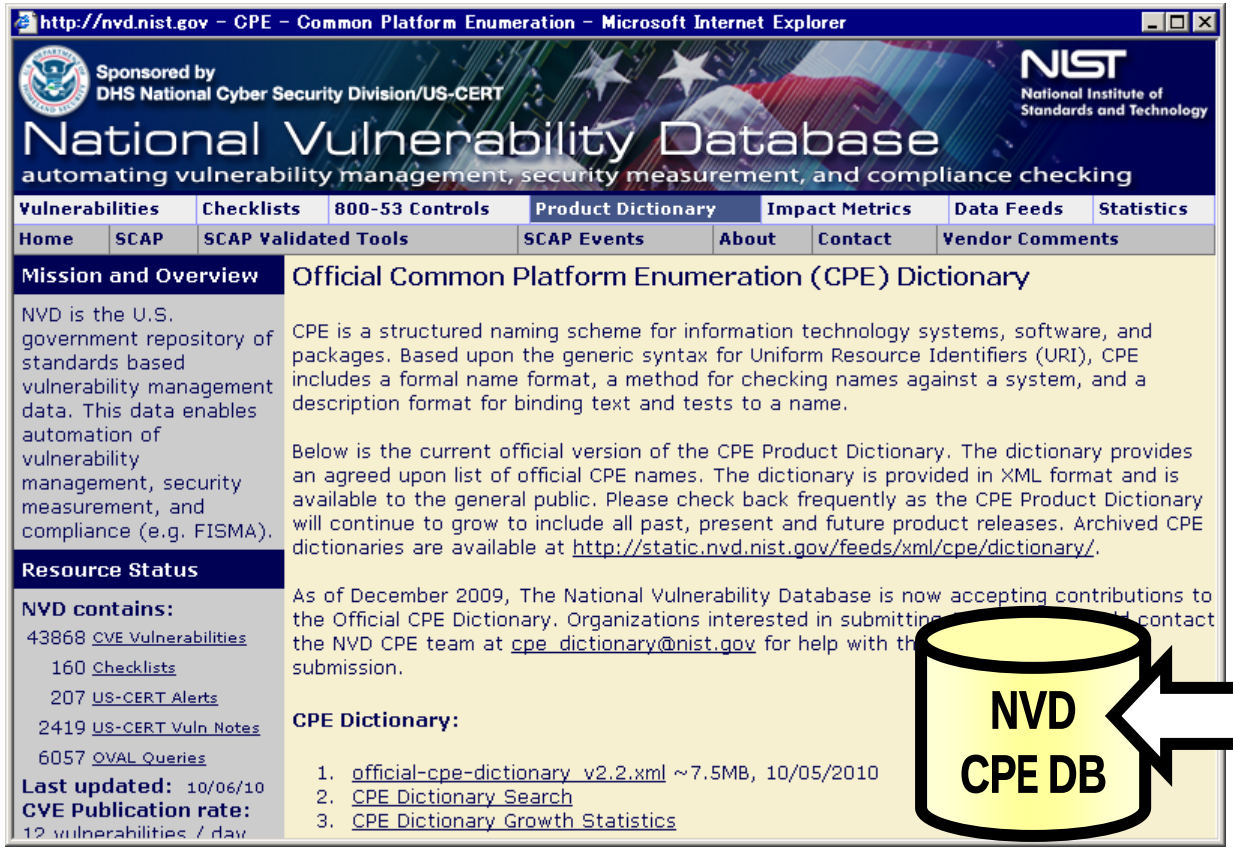
MyJVNセキュリティ設定チェッカでは、設定項目のチェックにOVALを利用

Official CPE Dictionary 連携（試行）

http://nvd.nist.gov/cpe.cfm

JVN iPedia Vulnerability Countermeasure Information Database

- MyJVN CPE DBと米NIST NVD CPE DB “Official CPE Dictionaryとの連携（国内製品のCPE名、日本語名の登録）を通して、CPE名の整合性を確保する）。

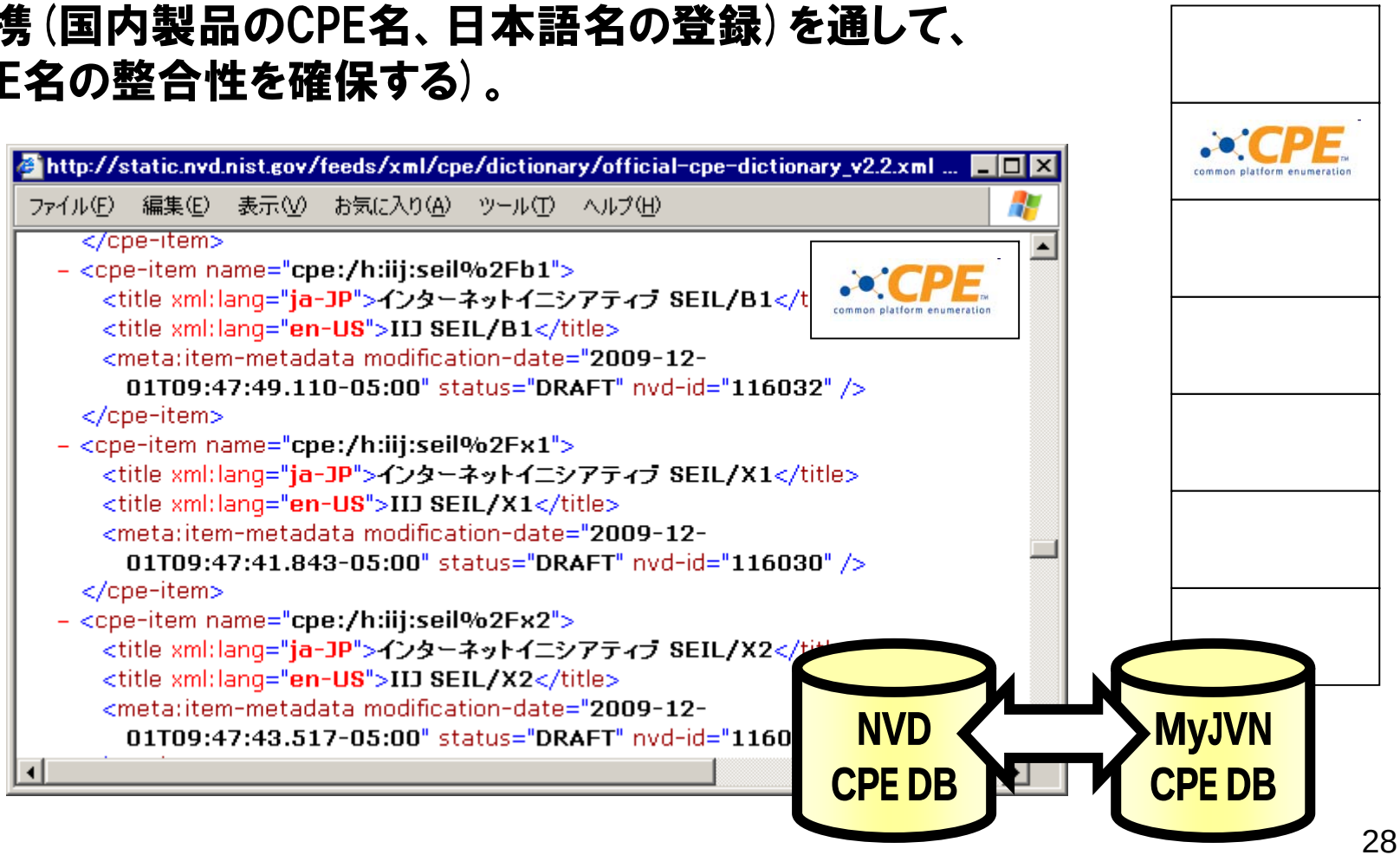


Official CPE Dictionary 連携（試行）

http://nvd.nist.gov/cpe.cfm

JVN iPedia Vulnerability Countermeasure Information Database

- MyJVN CPE DBと米NIST NVD CPE DB “Official CPE Dictionaryとの連携（国内製品のCPE名、日本語名の登録）を通して、CPE名の整合性を確保する）。

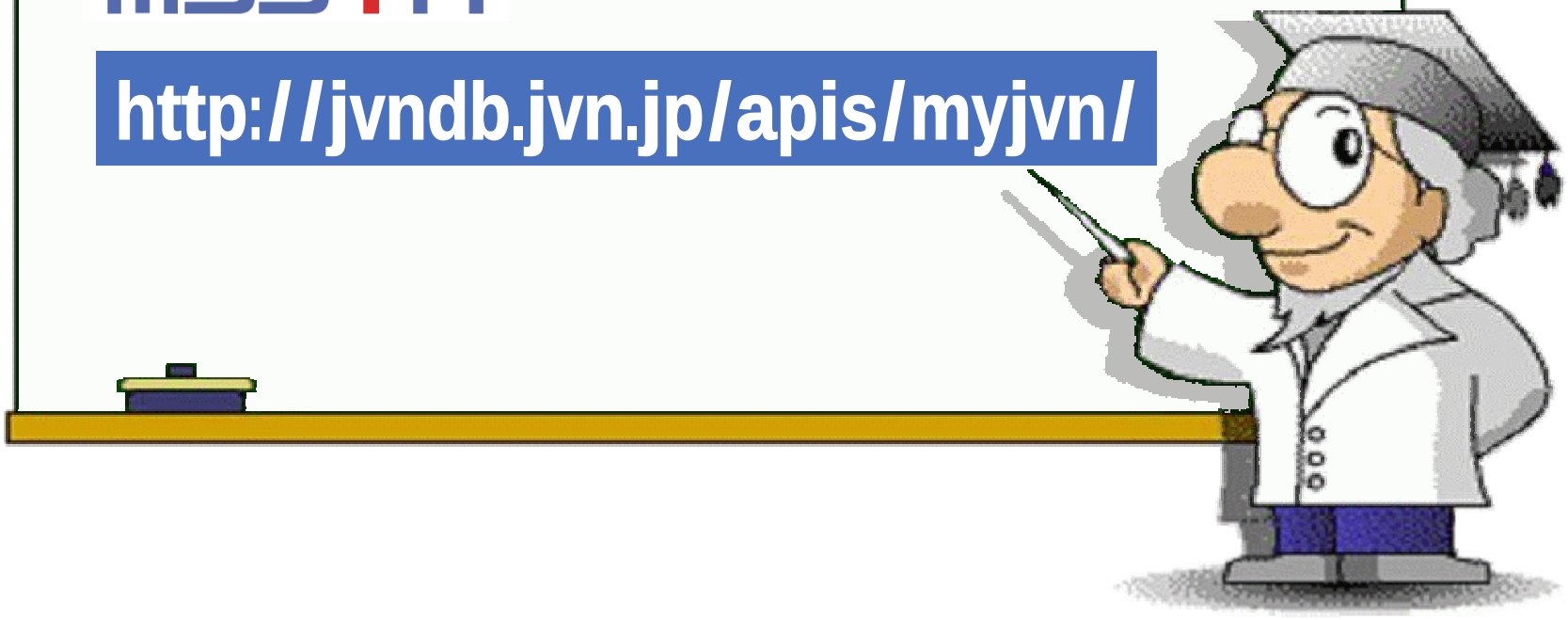


まとめ

MyJVNでは、今後も共通基準／仕様の導入を進めながら、国際性（インターネットにおける脆弱性対策情報の情報源）と地域性（日本国内向けの脆弱性対策情報データベース）とを両立させたグローバルなJVN（世界に冠たるJVN）を実現していく予定です。

MyJVN

http://jvndb.jvn.jp/apis/myjvn/



参考情報：SCAPの概要

米国政府の推進するSCAPとは

- 米国では、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、セキュリティ規格やガイドラインに従い、情報システムにセキュリティ要件を反映する活動を推進している。

【 課題 】

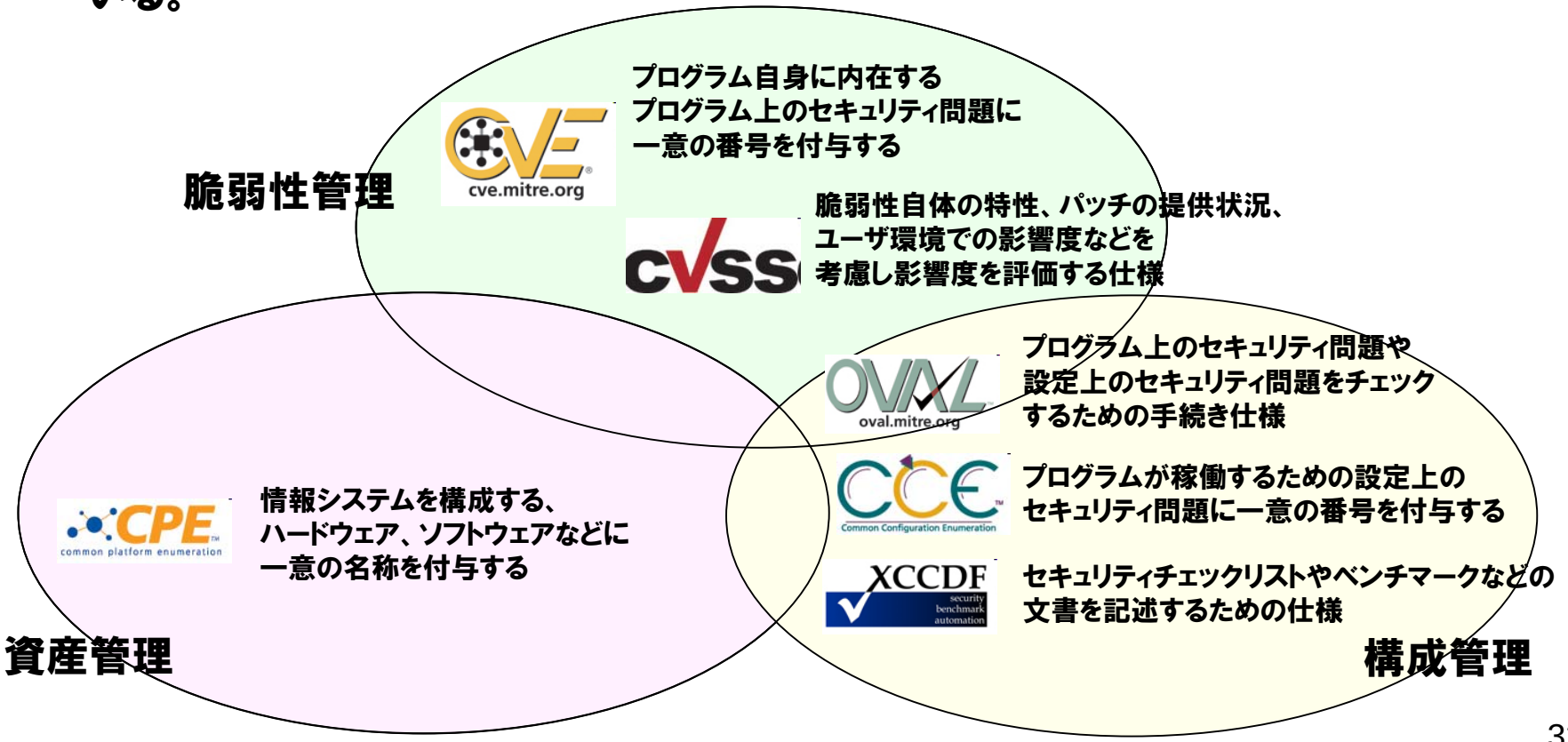
セキュリティ設定に関する作業を手作業で行なうと、設定ミスや設定者のセキュリティ知識の程度や判断の相違などによりセキュリティ要件を損なう可能性大	連邦政府システムのベースラインのセキュリティを確保しつつ、ヘルプデスクおよびパッチ検証にかかる費用を削減

【 解決策 】

作業の機械化 (自動化) による対処 ⇒SCAP (Security Content Automation Protocol)	共通のデスクトップ基準制定による対処 ⇒ FDCC(Federal Desktop Core Configuration)
共通基準制定による (自動化) の普及 ⇒Making Security Measurable	共通の基準制定による対処 ⇒ USGCB(United States Government Configuration Baseline)

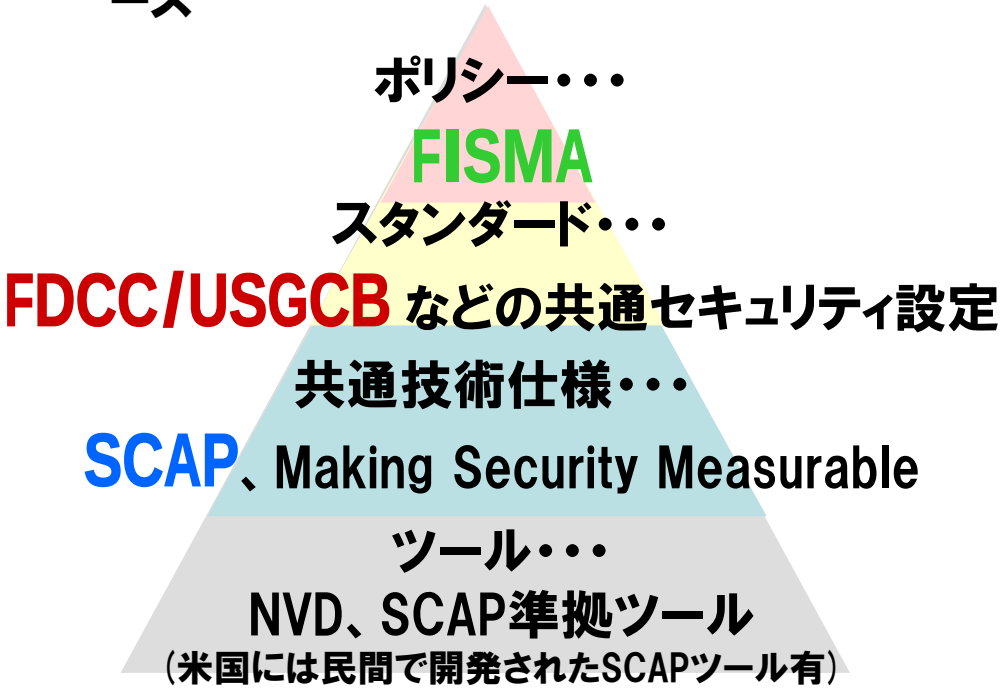
米国政府の推進するSCAPとは

- 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仕様群である。2010年6月時点で、6つの仕様から構成されている。



SCAP ＝FDCC/USGCBを支援する技術仕様

- 2007年3月22日、行政予算管理局（Office of Management and Budget）：連邦政府共通デスクトップ基準（FDCC: Federal Desktop Core Configuration）に関する覚書を発行
- 2010年9月24日、連邦政府CIO評議会（Federal CIO Council）：USGCB（United States Government Configuration Baseline：米国政府共通設定基準）1.0をリリース



IPA提供ツール
注意喚起など緊急時対応
基盤を普及させるための先行実装

JVN脆弱性対策機械処理基盤
（MyJVN API、MyJVN XMLフォーマットなど）

- JVNiPedia
- MyJVN脆弱性対策情報収集ツール
- MyJVNバージョンチェッカ
- MyJVNセキュリティ設定チェッカ

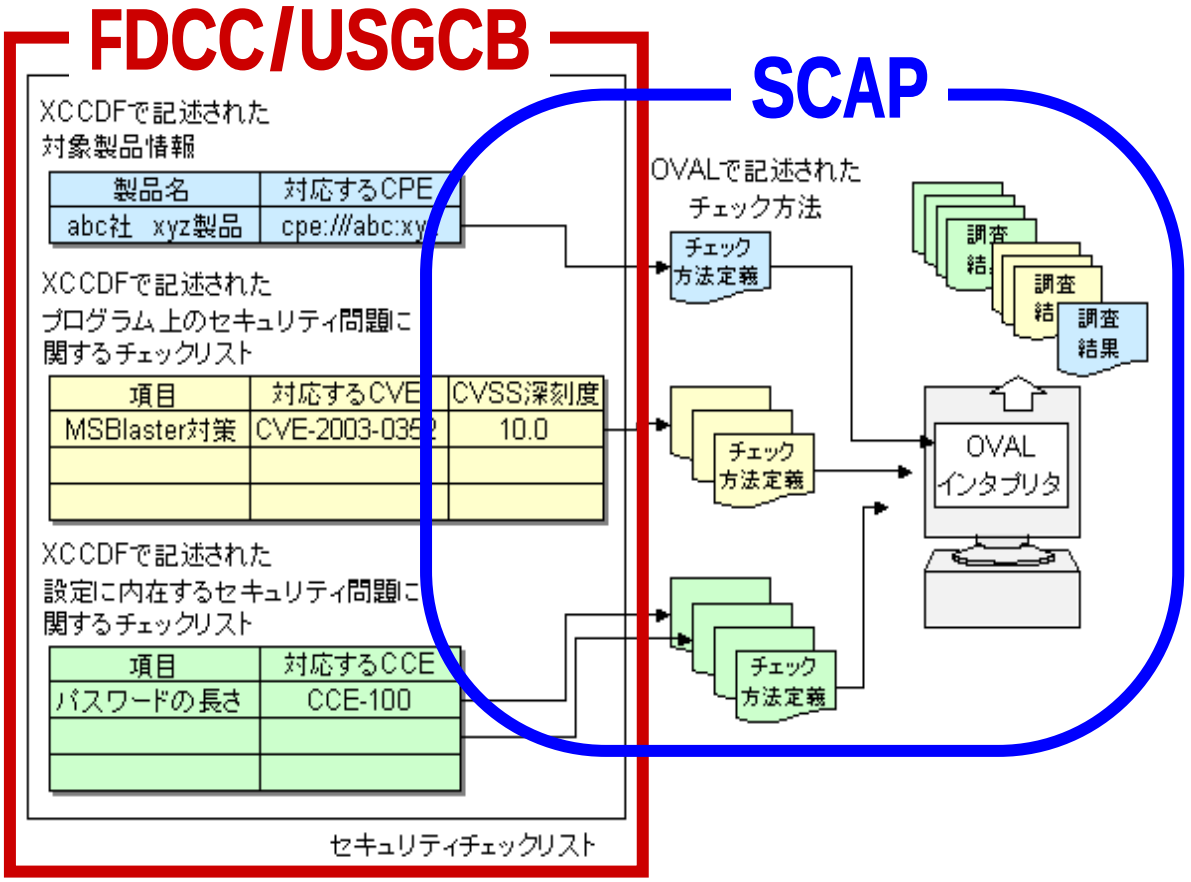
SCAP ＝FDCC/USGCBを支援する技術仕様

- FDCCは連邦政府のデスクトップ基準を確認するためのチェックリストである。
- SCAPはチェックリストに沿って機械（自動）的に確認するための技術仕様である。

規格やガイドラインを元にセキュリティチェックリストを作成する。XCCDFは、このセキュリティチェックリストを記述するための仕様である。

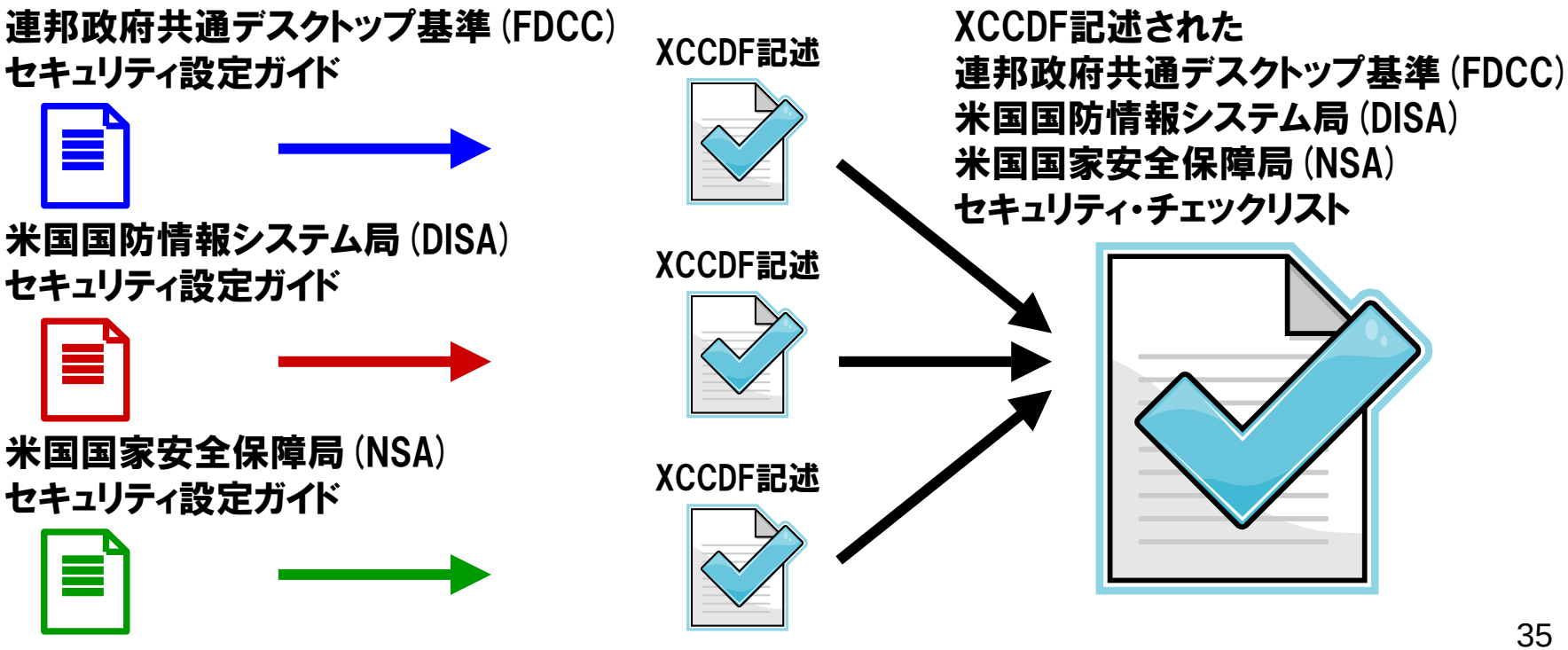
チェックリストを記述する際に、製品情報にはCPE、プログラム上のセキュリティ問題にはCVE、設定上のセキュリティ問題にはCCEを利用する。CVSSはプログラム上のセキュリティ問題の深刻度を判定する際の参考となる。

チェックリストの各項目を実際に調査する際には、OVALで記述されたチェック方法に従いOVALインタプリタが調査し、その結果をXCCDF形式で報告する。



XCCDF：チェックリストを記述する

- セキュリティ・チェックリストやベンチマークなどの文書を記述する。
  - 文書で記載されたセキュリティ設定ガイドを、プログラムで（機械）処理しやすい形式で記述する。
  - 複数のセキュリティ・チェックリストをひとつのファイルに統合する。



XCCDF：チェックリストを記述する

- セキュリティ・チェックリストやベンチマークなどの文書を記述する。
  - XML形式での記述
  - 参照する各種セキュリティ設定ガイドに基づく項目のグループと推奨値の併記
    - 参照する各種セキュリティ設定ガイドに基づく項目のグループ化

```
<Group id="IA-5" hidden="true">
  <title>Authenticator Management</title>
  <reference>ISO/IEC 17799: 11.5.2, 11.5.3</reference>
  <reference>NIST 800-26: 15.1.6, 15.1.7, 15.1.9, 15.1.10, 15.1.11 ・・・</reference>
  <reference>GAO FISCAM: AC-3.2</reference>
  <reference>DOD 8500.2: IAKM-1, IATS-1</reference>
  <reference>DCID 6/3: 4.B.2.a (7), 4.B.3.a (11) </reference>
</Group>
```

セキュリティ設定ガイド毎の違いが明らかになる。

    - セキュリティ設定ガイド毎の推奨値の記載

```
<Value id="MinimumPasswordLength_var" type="number" operator="greater tha
  <title>Minimum Password Length</title>
  <description>The minimum number of characters required for a password</description>
  <value>8</value>
  <value selector="Specialized-Security-Limited Functionality">12</value>
  <value selector="DISA-Gold">9</value>
  <value selector="DISA-Platinum">9</value>
  <value selector="NSA">12</value>
  <value selector="FDCC-Desktop">12</value>
</Value>
```

CPE：製品を識別する

- 情報システムを構成する、ハードウェア、ソフトウェアなどに一意の名称を付与する。
  - 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。

IPAが提供するMyJVN

IPAが提供するマイ・ジェイ・ブイ・エヌ

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：製品を識別する

- 情報システムを構成する、ハードウェア、ソフトウェアなどに一意の名称を付与する。
  - Official Common Product Enumeration (CPE) Dictionaryとして製品一覧を提供中 (http://nvd.nist.gov/cpe.cfm)

cpe:/{種別}:{ベンダ名}:{製品名}:{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

```
<cpe-item name="cpe:/a:adobe:acrobat_reader">
 <title xml:lang="ja-JP">アドビシステムズ アクロバット リーダー</title>
  <title xml:lang="en-US">Adobe Acrobat Reader</title>
  <meta:item-metadata modification-date="2009-03-05" status="DRAFT" nvd-id="280" />
</cpe-item>
<cpe-item name="cpe:/a:mozilla:firefox">
    <title xml:lang="en-US">Mozilla Firefox</title>
    <meta:item-metadata modification-date="2007-09-14" status="DRAFT" nvd-id="7356" />
</cpe-item>
```

CVE：脆弱性を識別する

- プログラム自身に内在する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）を付与する。
  - 脆弱性対策情報の参照番号としての利用
  - 脆弱性対策情報同士の関連付け

CVE識別番号の構成

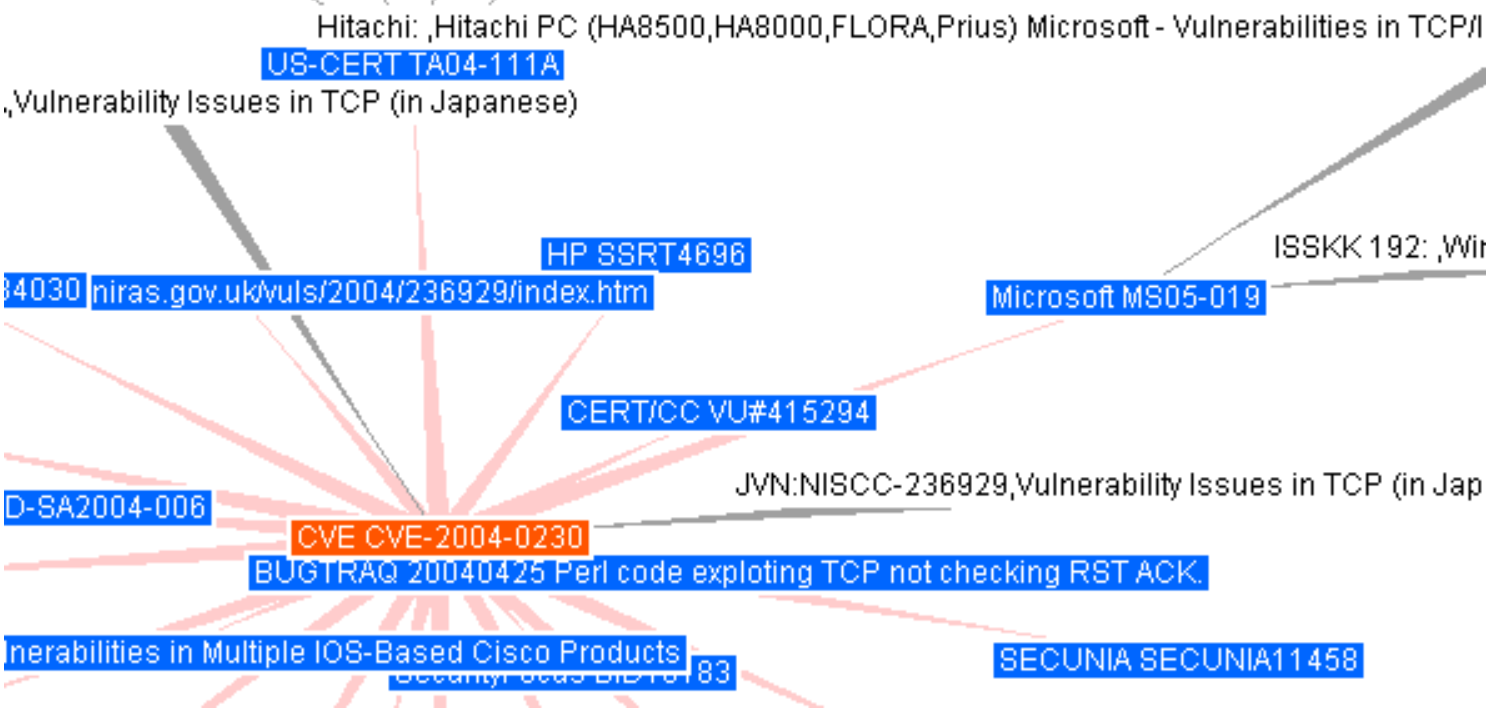
CVE-2007-5000

CVE識別番号とJVN、JVN iPediaのID対応例

CVE識別番号（CVE-ID）	JVNのID（識別番号）	JVN iPediaのID（登録番号）	脆弱性関連情報のタイトル
CVE-2007-5000	JVN#80057925	JVNDB-2007-000819	Apache HTTP Server のmod_imapおよびmod_imagemapにおけるクロスサイトスクリプティングの脆弱性
CVE-2008-0006	JVN#88935101	JVNDB-2008-001043	X.Org Foundation製Xサーバにおけるバッファオーバーフローの脆弱性
CVE-2008-3271	JVN#30732239	JVNDB-2008-000069	Apache Tomcatにおいて権限のないクライアントからのリクエストが実行されてしまう脆弱性
CVE-2008-5382	JVN#70599814	JVNDB-2008-000079	アイ・オー・データ製HDL-Fシリーズにおけるクロスサイトリクエストフォージェリの脆弱性

CVE：脆弱性を識別する

- プログラム自身に内在する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）を付与する。
  - 脆弱性対策情報の参照番号と関連付けを利用すると、脆弱性対策情報同士の参照関係、情報の展開度合いを知ることができる。



CVE-2004-0230 TCP にサービス運用妨害を伴う脆弱性

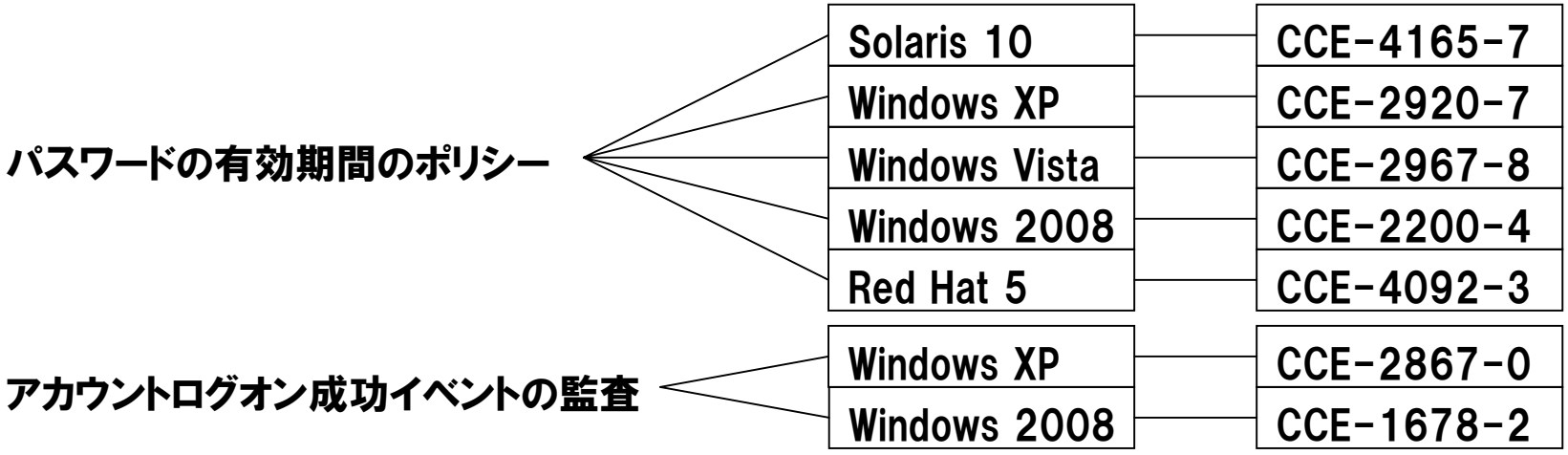
CCE：設定上の問題を識別する

- プログラムが稼働するための設定上のセキュリティ問題に一意の番号（CCE識別番号）を付与する。

CCE識別番号の構成

※チェック番号はコピー等のミスを検知するための番号
　Luhnアルゴリズムを使用
<確認手順>
(a) チェック番号込で右から偶数桁を2倍：1*2, 9*2
(b) 9+ (2) +8+ (1+8) +2　　*二桁になった場合、一桁目と二桁目を分割
(c) (b) の和が10で割り切れる　=　正しい番号

- アプリケーション・プラットフォーム別のセキュリティ設定項目に番号付与する。



CCE：設定上の問題を識別する

- プログラムが稼働するための設定上のセキュリティ問題に一意の番号（CCE識別番号）を付与する。
  - セキュリティ設定項目の推奨値は各種セキュリティ設定ガイドを参照する。
    - ファイルとレジストリのアクセス権限と監査
    - ユーザの権限
    - 監査とアカウントのポリシー

Windows XPを対象としたCCE識別番号とセキュリティ設定ガイド推奨値

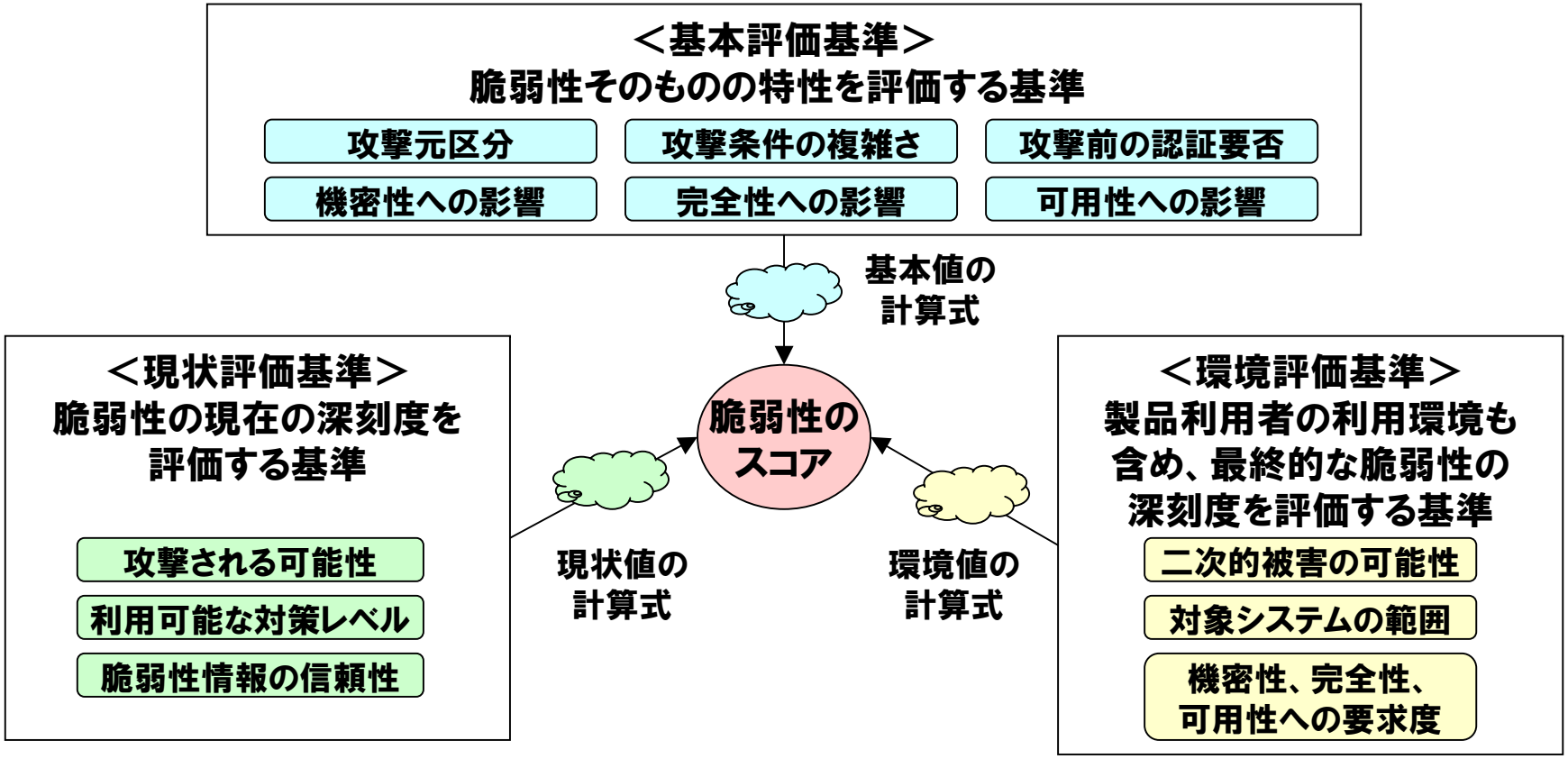
CCE識別番号	セキュリティ設定項目	セキュリティ設定ガイド		
		FDCC	DISA	マイクロソフト
CCE-2981-9	パスワードの最低文字数設定（パスワードの長さ）のポリシー	12文字以上	14文字以上	8文字以上
CCE-2920-7	パスワードの有効期間のポリシー	60日以下	60日以下	90日以下
CCE-2994-2	パスワードの履歴管理（同じパスワードを連続して使えない回数）のポリシー	24個以上	24個以上	24個以上

- ネットワークサービス

：

CVSS：脆弱性の深刻度を評価する

- 情報システムの脆弱性に対するオープンで汎用的な評価手法であり、共通の評価方法を提供する。



CVSS：脆弱性の深刻度を評価する

- 脆弱性自体の特性＜基本評価基準＞、パッチの提供状況＜現状評価基準＞、ユーザ環境＜環境評価基準＞での影響度などを考慮し影響度を評価する。

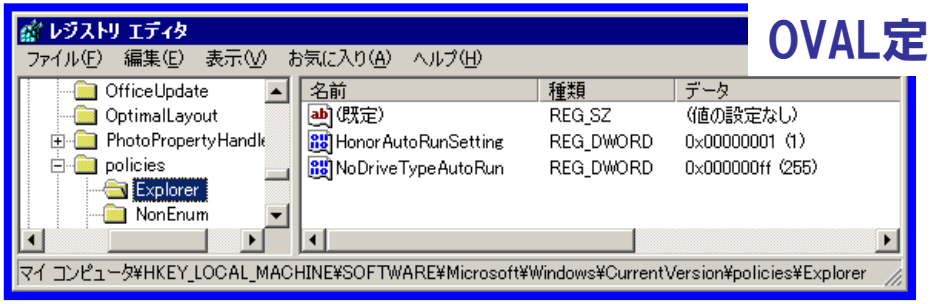
＜基本評価基準＞の目安

深刻度	基本値
レベルIII（危険）	7.0～10.0
レベルII（警告）	4.0～6.9
レベルI（注意）	0.0～3.9

OVAL：チェック方法を記述する

- プログラム上のセキュリティ問題や設定上のセキュリティ問題をチェックするための手続きを記述する。

セキュリティ設定ガイド
すべての種類のドライブの自動再生は、無効（0xFF）を推奨する。



OVAL定義データ
レジストリNoDriveTypeAutoRun値が0xFF（255）であればOK。

セキュリティ設定ガイド
MyJVN脆弱性対策情報収集ツールが最新であること。

OVAL定義データ
C:¥Program Files¥myjvn¥mjcheck.exeのファイルバージョンが1.4であればOK。

OVAL：チェック方法を記述する

- プログラム上のセキュリティ問題や設定上のセキュリティ問題をチェックするための手続きを記述する。
  - ステップ1
    OVAL定義データ（OVALの記述仕様に則ったXML形式の定義ファイル）を作成する。

```
<tests>
  <registry_test id="oval:myjvn.oval:tst:1001" check_existence="at_least_one_exists" check="at least one">
    <object object_ref="oval:myjvn.oval:obj:1001"/>
    <state state_ref="oval:myjvn.oval:ste:1001"/>
  </registry_test>
</tests>
<objects>
  <registry_object id="oval:myjvn.oval:obj:1001">
    <hive>HKEY_LOCAL_MACHINE</hive>
    <key>SOFTWARE¥IPA¥MyJVN</key>
    <name>CurrentVersion</name>
  </registry_object>
</objects>
<states>
  <registry_state id="oval:myjvn.oval:ste:1001">
    <value>1.0</value>
  </registry_state>
</states>
</oval_definitions>
```

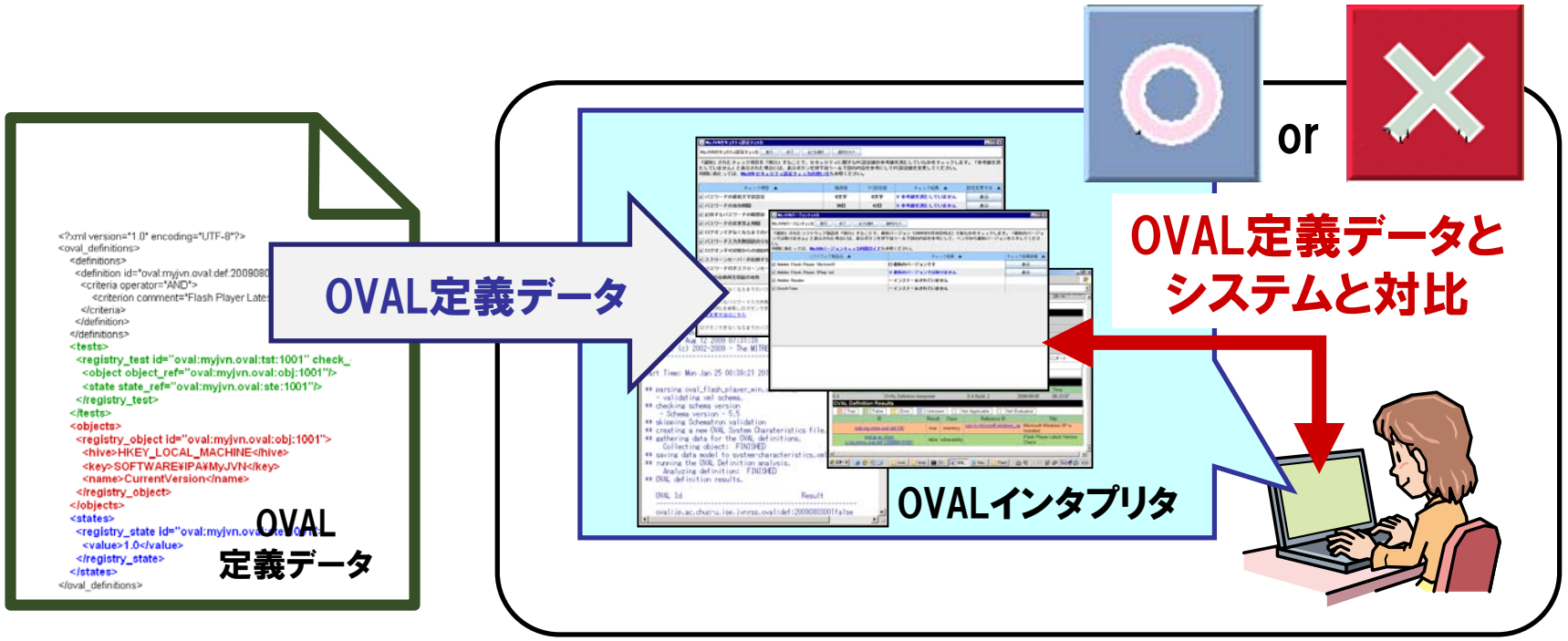
レジストリCurrentVersion値が1.0であれば最新である

バージョンが格納されている
レジストリ位置

比較対象となる
最新バージョン値

OVAL：チェック方法を記述する

- プログラム上のセキュリティ問題や設定上のセキュリティ問題をチェックするための手続きを記述する。
  - ステップ2
    OVALインタプリタ（OVAL定義データを解釈するプログラム）で、
    OVAL定義データに示されている条件を満たしているかどうかを判定する。



参考情報

- 動向
  - 脆弱性情報共有フレームワークに関する調査報告書（2007）
    http://www.ipa.go.jp/security/fy19/reports/vuln_Framework/vuln_Framework.pdf

- SCAP
  - FDCC (Federal Desktop Core Configuration：連邦政府共通デスクトップ基準)
    http://nvd.nist.gov/fdcc/index.cfm
  - NCP (National Checklist Program)
    http://nvd.nist.gov/ncp.cfm
  - NVD (National Vulnerability Database)
    http://nvd.nist.gov/
  - SCAP (Security Content Automation Protocol：セキュリティ設定共通化手順)
    http://nvd.nist.gov/scap.cfm
  - USGCB (United States Government Configuration Baseline：米国政府共通設定基準)
    http://usgcb.nist.gov/

参考情報

- **共通識別子**
  - CAPEC (Common Attack Pattern Enumeration and Classification)
    http://capec.mitre.org/
  - CCE (Common Configuration Enumeration：共通セキュリティ設定一覧)
    http://cce.mitre.org/
    http://www.ipa.go.jp/security/vuln/CCE.html
  - CME (Common Malware Enumeration)
    http://cme.mitre.org/
  - CPE (Common Platform Enumeration：共通プラットフォーム一覧)
    http://cpe.mitre.org/
    http://www.ipa.go.jp/security/vuln/CPE.html
  - CVE (Common Vulnerability and Exposures：共通脆弱性識別子)
    http://cve.mitre.org/
    http://www.ipa.go.jp/security/vuln/CVE.html
  - CWE (Common Weakness Enumeration：共通脆弱性タイプ一覧)
    http://cwe.mitre.org/
    http://www.ipa.go.jp/security/vuln/CWE.html

参考情報

- **共通仕様**
  - CEE (Common Event Expression)
    http://cee.mitre.org/
  - CRF (Common Result Format)
    http://makingsecuritymeasurable.mitre.org/crf/
  - CVSS (Common Vulnerability Scoring System:共通脆弱性評価システム)
    http://www.first.org/cvss/
    http://www.ipa.go.jp/security/vuln/CVSS.html
  - OCIL (Open Checklist Interactive Language:チェックリスト対話言語)
    http://scap.nist.gov/specifications/ocil/
  - OVAL (Open Vulnerability and Assessment Language:セキュリティ検査言語)
    http://oval.mitre.org/
    http://www.ipa.go.jp/security/vuln/OVAL.html
  - XCCDF (Extensible Configuration Checklist Description Format:セキュリティ設定チェックリスト記述形式)
    http://nvd.nist.gov/xccdf.cfm