INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

脆弱性対策に向けた機械処理基盤 SCAPと標準化動向

SCAP:Security Content Automation Protocol

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
情報セキュリティ技術ラボラトリー
寺田真敏

IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

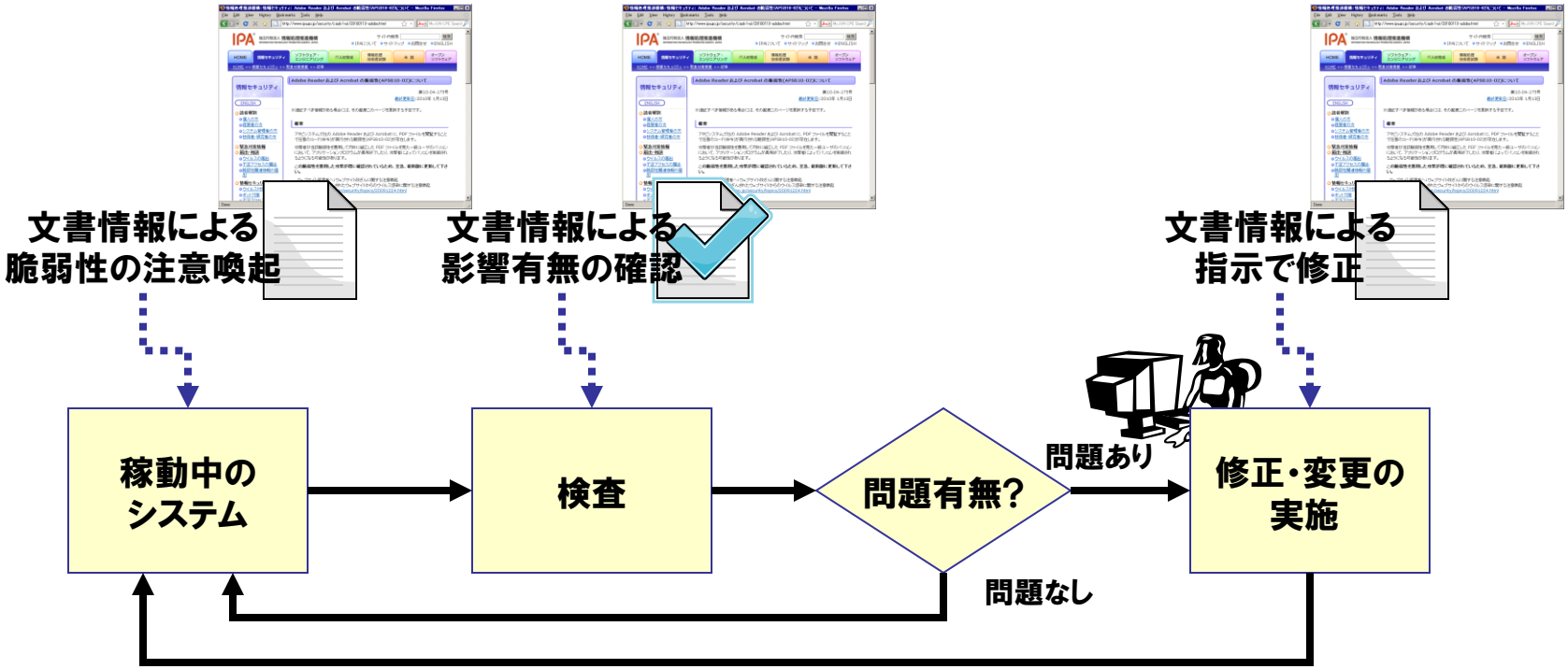
JVNでは、日本国内の脆弱性対策を支援するために、
脆弱性対策に関わる自動化フレームワークの整備を推進しています。
本資料では、
・海外動向
・米国政府の推進するSCAP
・IPAの推進するMyJVN
（JVNの情報を活用するための
脆弱性対策自動化フレームワーク）について
紹介します。

用語一覧

CAPEC: Common Attack Pattern Enumeration and Classification（共通攻撃パタン一覧）
CCE: Common Configuration Enumeration（共通セキュリティ設定一覧）
CEE: Common Event Expression（共通イベント表記）
CPE: Common Platform Enumeration（共通プラットフォーム一覧）
CRF: Common Result Format（共通結果記述形式）
CVE: Common Vulnerability and Exposures（共通脆弱性識別子）
CVSS: Common Vulnerability Scoring System（共通脆弱性評価システム）
CWE: Common Weakness Enumeration（共通脆弱性タイプ一覧）
FDCC: Federal Desktop Core Configuration（連邦政府共通デスクトップ基準）
IODEF: Incident Object Description Exchange Format
ISAP: Information Security Automation Program（情報セキュリティ対策自動化計画）
NCP: National Checklist Program
NVD: National Vulnerability Database
OVAL: Open Vulnerability and Assessment Language（セキュリティ検査言語）
SCAP: Security Content Automation Protocol（セキュリティ設定共通化手順）
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）

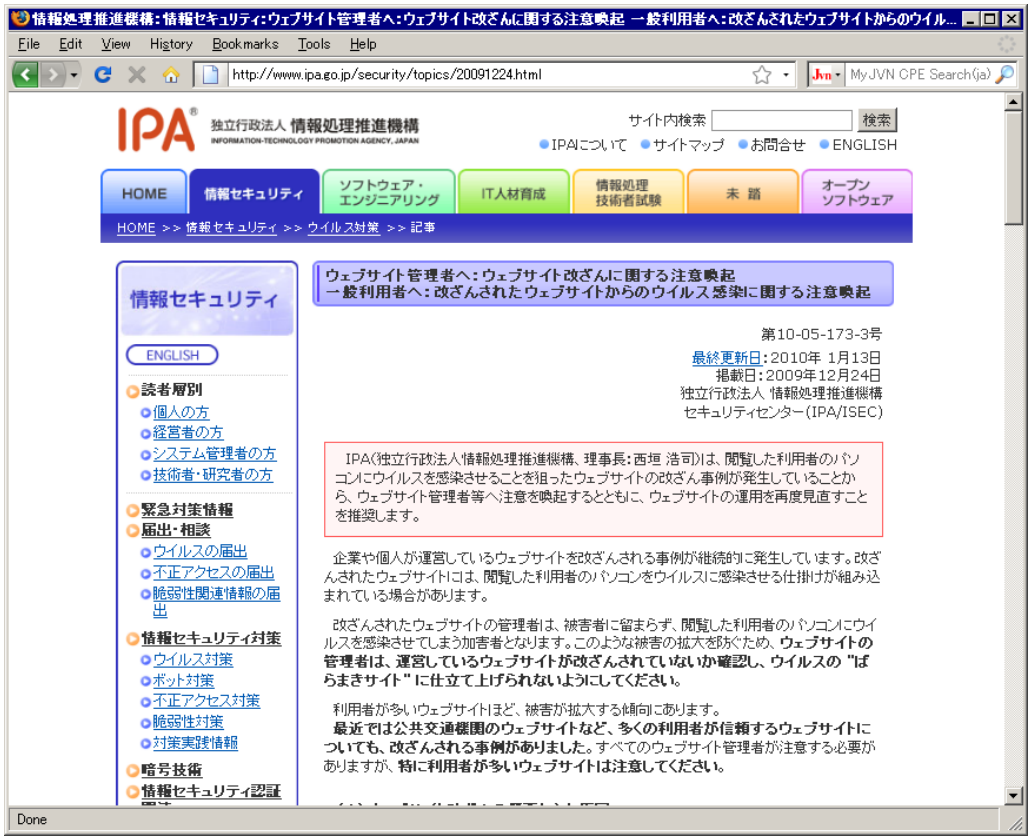
脆弱性対策自動化フレームワークとは

- 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ってしまう可能性がある。
  例えば、文書情報という脆弱性対策情報だけで影響有無を判定する手法では抜け漏れが発生してしまう。



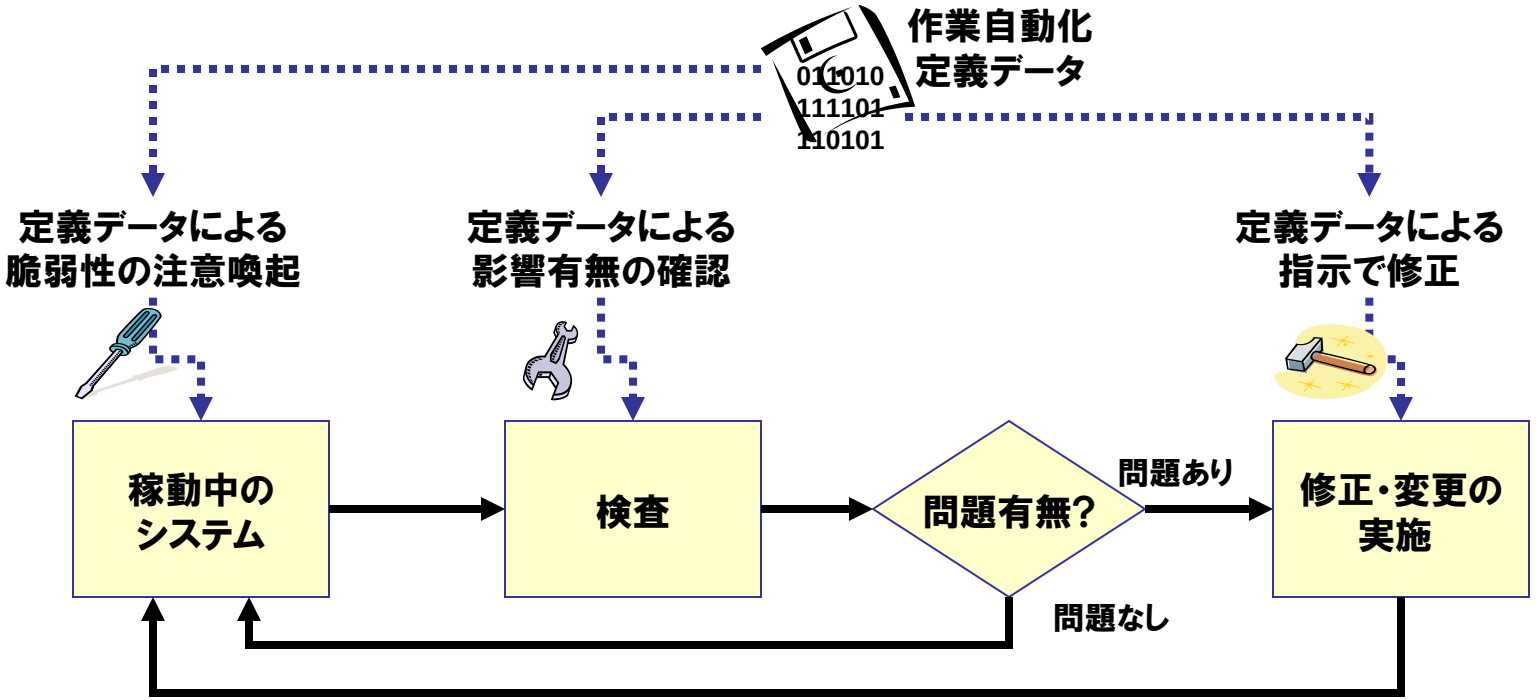
脆弱性対策自動化フレームワークとは

- 文書情報というぜい弱性対策情報の例
  深刻で影響範囲の広い、情報セキュリティ上の脅威を配信する緊急対策情報などがある。
  - 緊急対策情報を読んで対象となるシステムを絞込む
  - 緊急対策情報を読んで影響有無の判定する
  - 緊急対策情報を読んで修正ならびに修正後の確認する



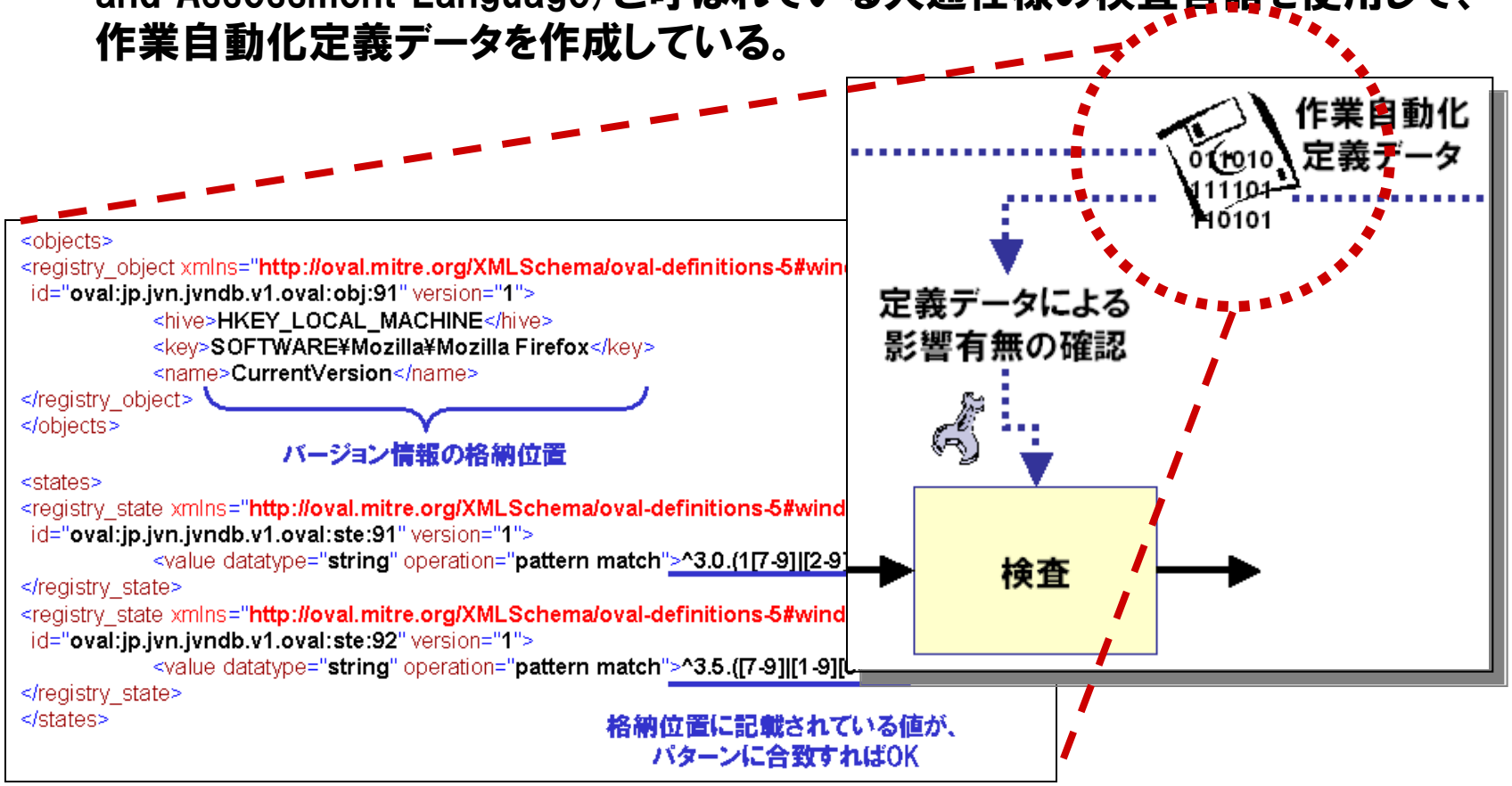
脆弱性対策自動化フレームワークとは

- 作業の省力化と対策の精度向上を図るためには、ツールを用いた脆弱性検査や更新、再確認など作業自動化による対処は有用である。



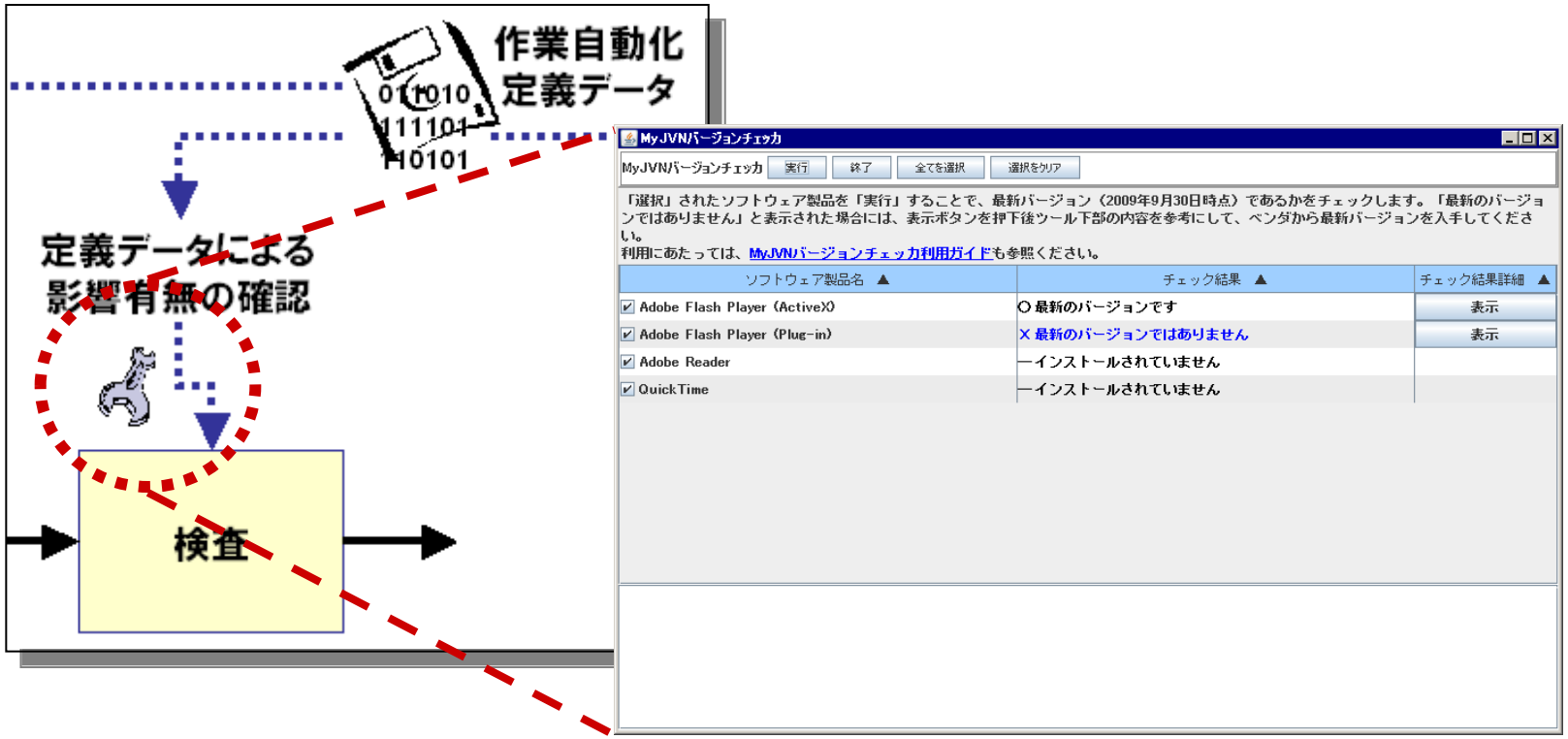
脆弱性対策自動化フレームワークとは

- **作業自動化のための定義データの例**
  MyJVNバージョンチェッカでは、OVAL（セキュリティ検査言語：Open Vulnerability and Assessment Language）と呼ばれている共通仕様の検査言語を使用して、作業自動化定義データを作成している。



脆弱性対策自動化フレームワークとは

- 作業自動化定義データを解釈するプログラム（≒ツール）の例
  共通仕様の検査言語OVALで記載された作業自動化定義データの指示に従い、人の代わって、MyJVNバージョンチェッカ（プログラム）がバージョンチェックを実施する。



脆弱性対策自動化フレームワークとは
≒脆弱性対策機械処理基盤

- 自動・・・
  - 自分で動くこと。
  - 機械などが自身の力で動くこと。

- 自動化するためには、自動化のための仕組みが必要です。脆弱性対策のための『自動化フレームワーク』の場合には、脆弱性対策を推進するための『プログラムによる処理が可能な基盤』という仕組みが必要となります。
- コンピュータ用語に、コンピュータが直接扱えることを意とした『machine-readable』という単語があります。この単語を参考にして、仕組みの視点から表現するならば、脆弱性対策自動化フレームワークとは、マルチベンダ環境において、『machine-readable』な共通仕様や基準など（の機械処理基盤）を整備し、その機械処理基盤に基づくツールを用いて、脆弱性対策を推進することです。

※人が取り扱いやすいことを意とする場合には『human-readable』を使います。

IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

目次

1. 海外動向
脆弱性対策の自動化に関連する施策

- 脆弱性対策情報の流通など、脆弱性対策に関わる処理の自動化を踏まえた基盤整備が進み始めている。
  - 米国では、米NIST（National Institute of Standards and Technology：国立標準技術研究所）が中心となり、米国政府を対象とした情報セキュリティ管理の技術面での自動化と標準化を目指した活動SCAP（Security Content Automation Protocol、セキュリティ設定共通化手順）を進めている。【・・・推進中】
  - 欧州では、EUの情報セキュリティ推進機関であるENISA（European Network and Information Security Agency：欧州ネットワーク情報セキュリティ庁）がセキュリティ関連情報の共有システムを実現するためのプロジェクトEISAS（European Information Sharing and Alert System）を立ち上げ、欧州全域で情報収集と分析を行い、国別に情報配信するモデルを検討している。【・・・企画中】
  - 英国では、英CPNI（国家インフラ防護センター）が中小規模組織向けのセキュリティ情報共有サービスWARP（Warning, Advice and Reporting Point）を立ち上げ、FWA（Filtered Warnings Application）と呼ばれる、セキュリティ情報の選別可能な情報提供ツールを提供している。【・・・構築済み】

1. 海外動向
脆弱性対策に関連する標準化

- ISO SC27 WG3
  責任ある脆弱性情報の開示
  Responsible Vulnerability Disclosure
  文書番号:29147
  略称:RVD
  - **経緯**
    カナダからの提案で、2006年11月に事前検討の開始が決定した。2007年4月の京都会議からワーキングドラフトとしての検討を開始した。
  - **概要**
    製品開発者が脆弱性情報を受信する際の心得、製品開発者ダが脆弱性情報に関する情報を開示する際の心得など、運用上、考慮すべき点を標準化の対象としている。製品開発者などの脆弱性を修正すべき組織が、発見者（含む、調整機関）から脆弱性情報を受け取る手順、さらには、製品開発者などの脆弱性を修正すべき組織がセキュリティ修正プログラムと共に、脆弱性情報を公表または特定者に開示する手順を規定する。

1. 海外動向
脆弱性対策に関連する標準化

- ITU-T Q.4/17
  サイバーセキュリティ情報交換フレームワーク
  Cybersecurity Information Exchange Framework
  文書番号:X.cybex
  略称:Cybex
  - 経緯
    2009年9月にNWI(New Work Item)として採択され、Cybexに関するCG(Correspondence Group)が発足した。このNWI化の背景には、2008年のITUの総会(WTSA08)決議58(開発途上国におけるCERT構築支援)と、決議58を実行するためにまとめられたTD0366(2009年6月)がある。
  - 概要
    脆弱性対策情報(ならびにインシデント対応)のフォーマット、番号体系などの技術仕様について標準化を進めている。
    共通仕様を用いて、グローバルかつタイムリーなサイバーセキュリティ情報の交換、活用ならびに、相互運用を実現するためのフレームワークを実現する。脆弱性対策ならびに回避関連(X.xccdf、X.cpe、X.cce、X.cve、X.crf、X.oval、X.cwe、X.cvssなど)、インシデント対応関連(X.cee、X.iodef、X.capecなど)の共通仕様の策定を想定している。

1. 海外動向
脆弱性対策に関連する標準化

- ITU-T Q.4/17
  サイバーセキュリティ情報交換フレームワーク

【 脆弱性対策ならびに回避関連 】

- X.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）
- X.cpe: Common Platform Enumeration（共通プラットフォーム一覧）
- X.cce: Common Configuration Enumeration（共通セキュリティ設定一覧）
- X.cve: Common Vulnerabilities and Exposures（共通脆弱性識別子）
- X.oval: Open Vulnerability and Assessment Language（セキュリティ検査言語）
- X.cvss: Common vulnerability scoring system（共通脆弱性評価システム）

SCAP

- X.crf: Common Result Format（共通結果出力形式）
- X.cwe: Common Weakness Enumeration（共通脆弱性タイプ一覧）

【 インシデント対応関連 】

- X.cee: Common Event Expression（共通イベント表記）
- X.iodef: Incident Object Description Exchange Format（インシデントオブジェクト記述交換形式）
- X.capec: Common Attack Pattern Enumeration and Classification（攻撃分類体系）

IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

目次

1. 海外動向
2. SCAP
3. MyJI.IN （コンセプト）
4. MyJI.IN （実装）

2. SCAP
米国における脆弱性対策の歩み

- 1999年のiCAT（脆弱性対策メタデータベース）構築からはじまり、2002年のFISMA（連邦情報セキュリティマネジメント法）の施行以降、各種活動が統合されはじめた。

2008年
2007年
2006年
2005年
2004年
2003年
2002年
2001年
2000年
1999年

FDCC 連邦政府システムの共通のデスクトップ基準

SCAP 脆弱性対策管理やコンプライアンス管理
⇒情報セキュリティ管理の技術面での
自動化と標準化

NCP プログラムが稼動するための設定に
内在するセキュリティ問題
⇒チェックリスト

NVD プログラム自身に内在する
コード上のセキュリティ問題
⇒脆弱性対策メタデータベース

2. SCAP
米国政府の推進するSCAPとは【 背景 】

- 米国では、2002年のFISMA（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 】

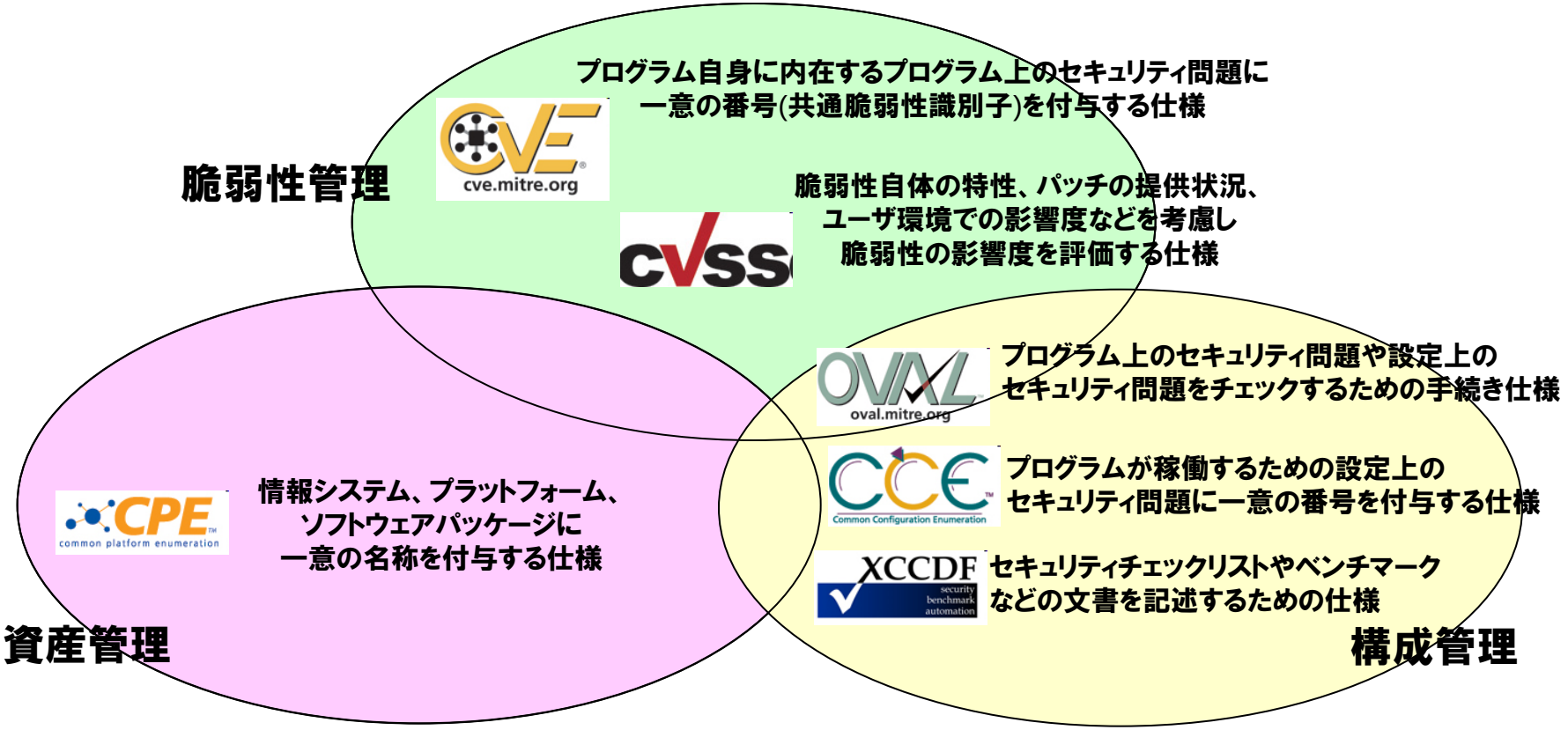
作業の自動化による対処
⇒SCAP (Security Content Automation Protocol)

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

2. SCAP
米国政府の推進するSCAPとは【 技術仕様の概要 】

- 脆弱性管理、コンプライアンス管理の一部を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1月時点で、6つの仕様から構成されている。



2. SCAP
SCAP=FDCC推進を支援するためのツール

- 2007年、米行政予算管理局（OMB：Office of Management and Budget）では、Windowsソフトウエアを『共通セキュリティ設定』に準拠させることにより、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大幅に削減するため、FDCC（Federal Desktop Core Configuration）と呼ぶ、連邦政府のデスクトップ基準を定めた。NISTでは、FDCCの推進にあたり、連邦政府のデスクトップ環境が基準に沿っているかを確認する手段の一つとしてSCAPを普及展開している。

2. SCAP
SCAP=FDCC推進を支援するためのツール

- 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り、SCAPはチェックリストに沿って確認を実行するツールである。

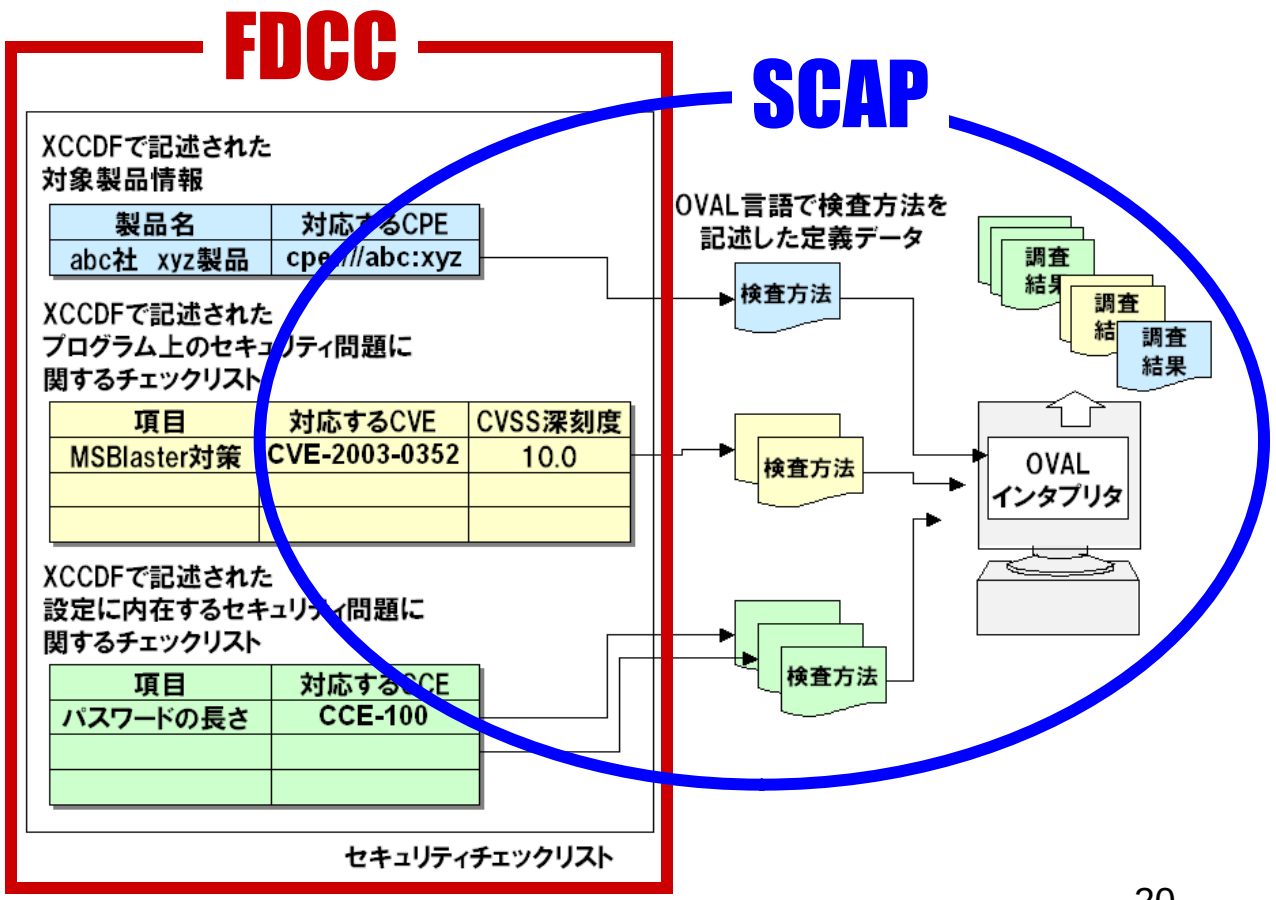
規格やガイドラインを元にセキュリティチェックリストを作成する。

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を識別情報として利用する。

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言語で記述された検査方法に従いOVALインタプリタが調査し、その結果をXCCDF形式で報告する。



2. SCAP
CVE：脆弱性を識別する

- 『プログラム上のセキュリティ問題』を一意に識別するために、脆弱性に対してCVE識別番号を付与する。

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

2. SCAP
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』を一意に識別するために、設定上の問題に対してCCE識別番号を付与する。
  - 項目
    - 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
      - CCE-2920-7　　パスワードの最大有効期限：60日
      - CCE-2981-9　　パスワードの長さ：12文字以上
      - CCE-2735-9　　パスワードの複雑さ：有効
      - ：　　：
    - ネットワークサービス
      - ：
  - CCE v5では、Windows Vista／XP／2000／2008／2003、Office 2007、Internet Explorer 7、Red Hat Enterprise Linux 5、Sun Solaris 10について規定している。

2. SCAP
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、ソフトウェアなどを識別するために共通の名称を付与する。

  cpe:/{種別}:{ベンダ名}:{製品名}:{バージョン}

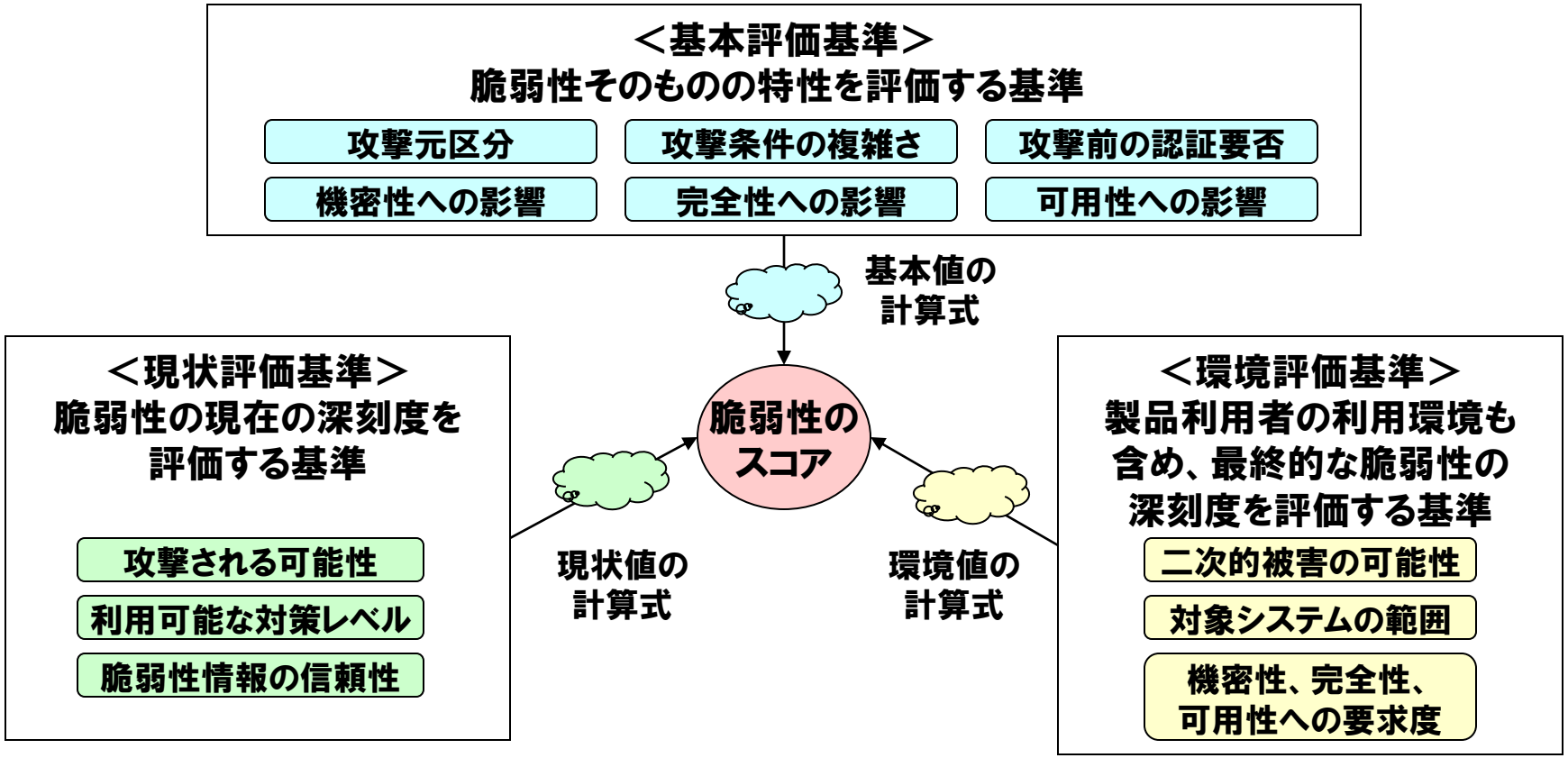
  :{アップデート}:{エディション}:{言語}

- NVDでは、Official Common Product Enumeration (CPE) Dictionaryとして製品一覧を掲載している。
  - official-cpe-dictionary_v2.2.xml (http://nvd.nist.gov/cpe.cfm)

```
<cpe-item name="cpe:/a:adobe:acrobat">
   <title xml:lang="ja-JP">アドビシステムズ アクロバット</title>
   <title xml:lang="en-US">Adobe Acrobat</title>
   <meta:item-metadata modification-date="2009-03-05 …" status="DRAFT" nvd-id="275" />
</cpe-item>
<cpe-item name="cpe:/a:firebirdsql:firebird">
   <title xml:lang="en-US">Firebird Firebird</title>
   <meta:item-metadata modification-date="2008-03-25 …" status="DRAFT" nvd-id="3883" />
</cpe-item>
```

2. SCAP
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、ベンダーに依存しない共通の評価方法を提供する。

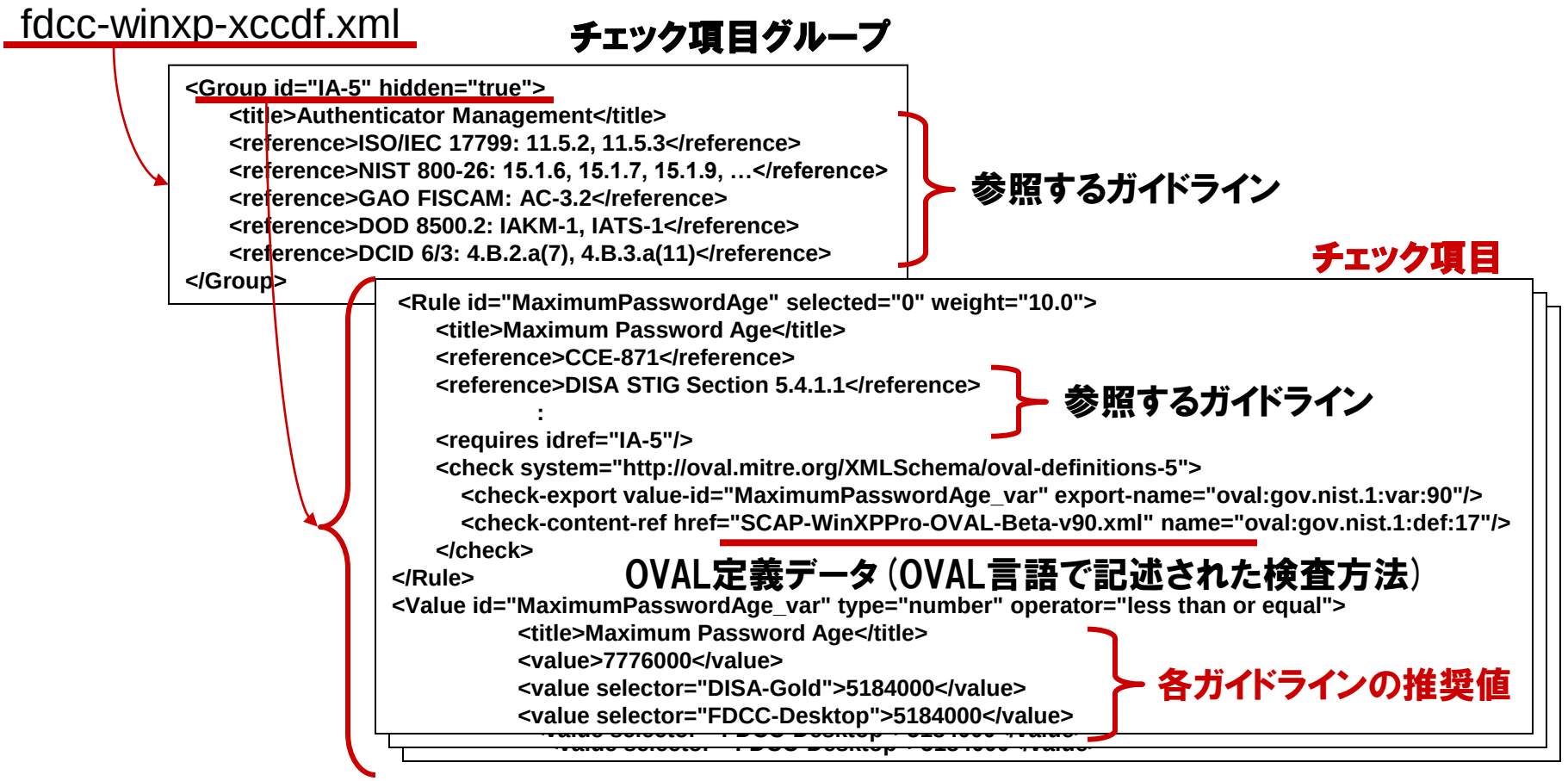


2. SCAP
CVSS：脆弱性の深刻度を評価する

- 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、ベンダーに依存しない共通の評価方法を提供する。

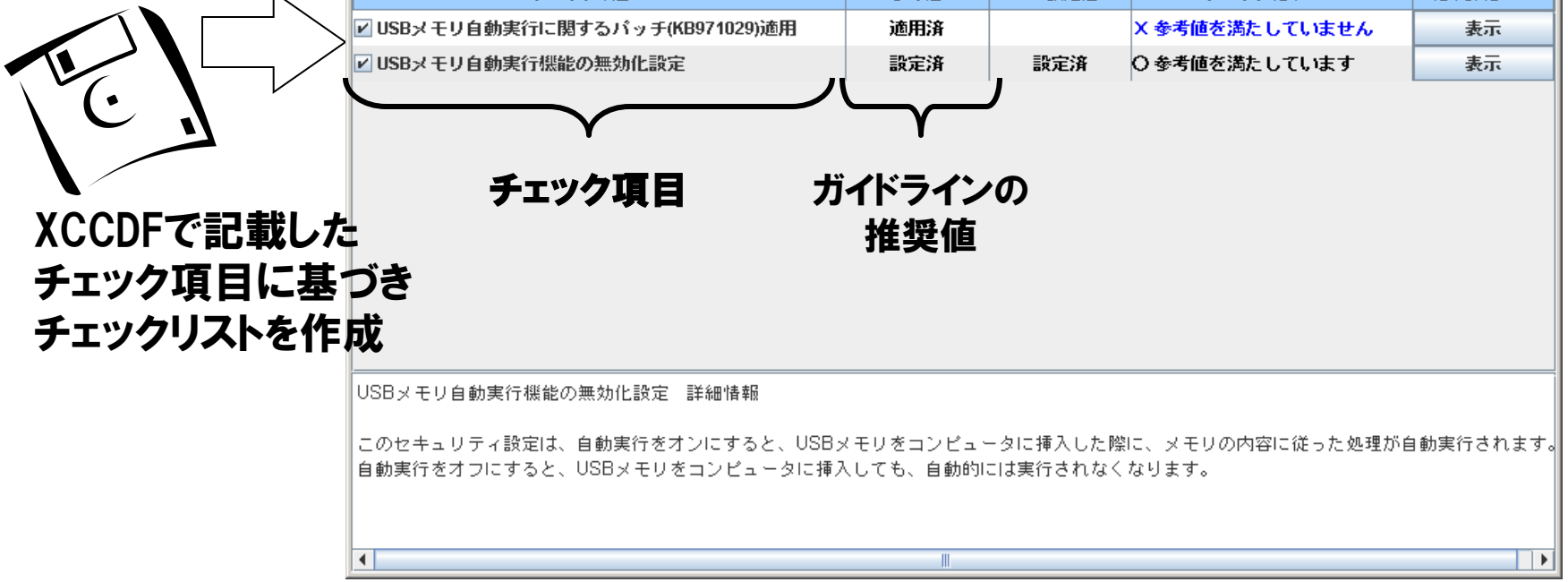
2. SCAP
XCCDF：セキュリティチェックリストを記述する

- 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XML形式で記述する仕様で、参照する各種ガイドライン、その推奨値、使用する検査データなどを記載する。



2. SCAP
XCCDF：セキュリティ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XML形式で記述する仕様で、参照する各種ガイドライン、その推奨値、使用する検査データなどを記載する。



2. SCAP
OVAL：チェック方法を記述する

- OVAL言語は、プログラム上や設定上のセキュリティ問題の検査方法をXML形式で記述するための仕様である。OVAL言語で記載された定義データを解釈するプログラム（OVALインタプリタ）と組み合わせて使うことで、チェックを手作業ではなく、自動化する。

```
  </definition>
</definitions>
<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

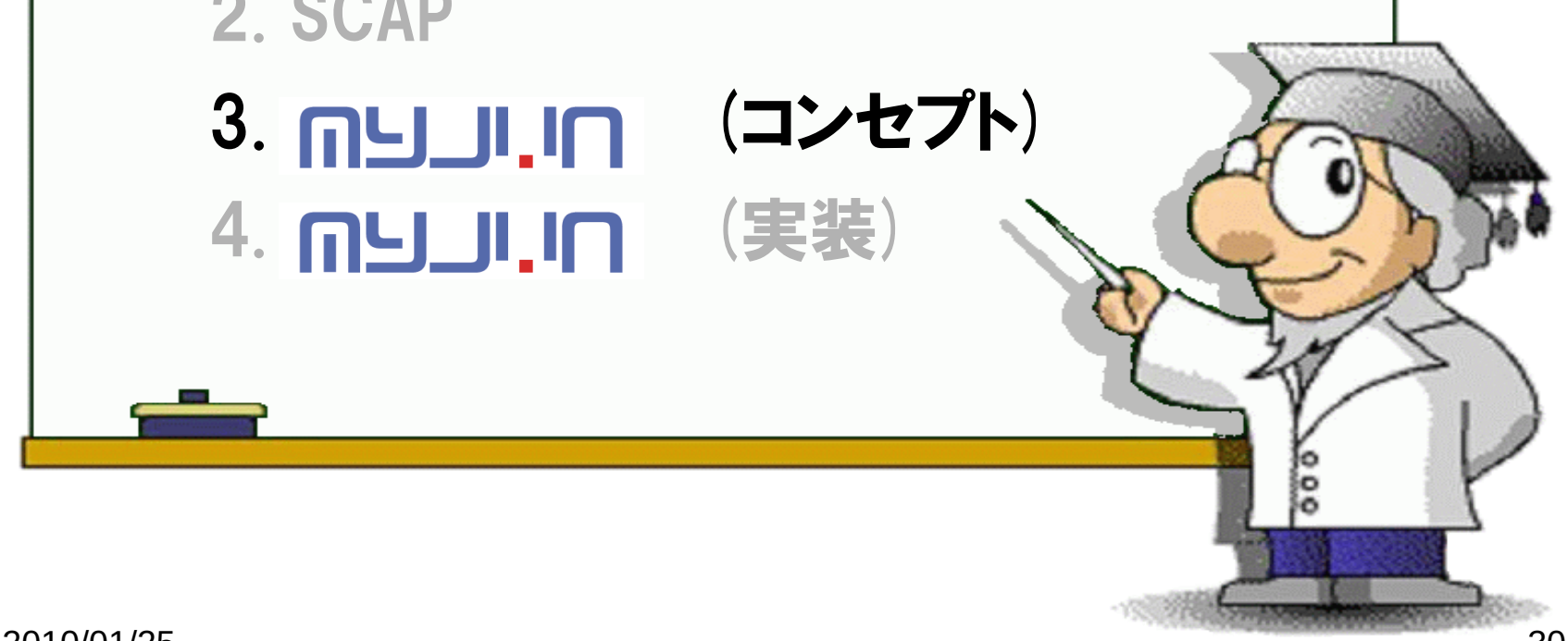
2. SCAP
OVAL：チェック方法を記述する

- OVALインタプリタ（OVAL言語で記載された定義データを解釈するプログラム）は、指定された検査項目の値を参照し、値を比較することで、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の存在有無の判定する。
- MyJVNバージョンチェッカ、MyJVNセキュリティ設定チェッカは、 OVALインタプリタの役割を果たす。

IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

目次

1. 海外動向
2. SCAP
3. MyJI.IN （コンセプト）
4. MyJI.IN （実装）



3. MyJVN （コンセプト）
脆弱性対策自動化フレームワークに関する取り組み（1）

- 脆弱性対策情報ポータルサイトJVNをベースとした
  自動化フレームワークの整備と**国際的な共通基準の積極的な導入**

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
	脆弱性対策情報ポータルサイト JVN 開設
8月	自動化フレームワークに関する検討開始
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）

3. MyJVN （コンセプト）
脆弱性対策自動化フレームワークに関する取り組み（2）

- 脆弱性対策情報ポータルサイトJVNをベースとした
  自動化フレームワークの整備と国際的な共通基準の積極的な導入

第2期
自動化
フレーム
ワーク
共通基準
導入期

2008年10月 脆弱性対策自動化フレームワーク“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

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）

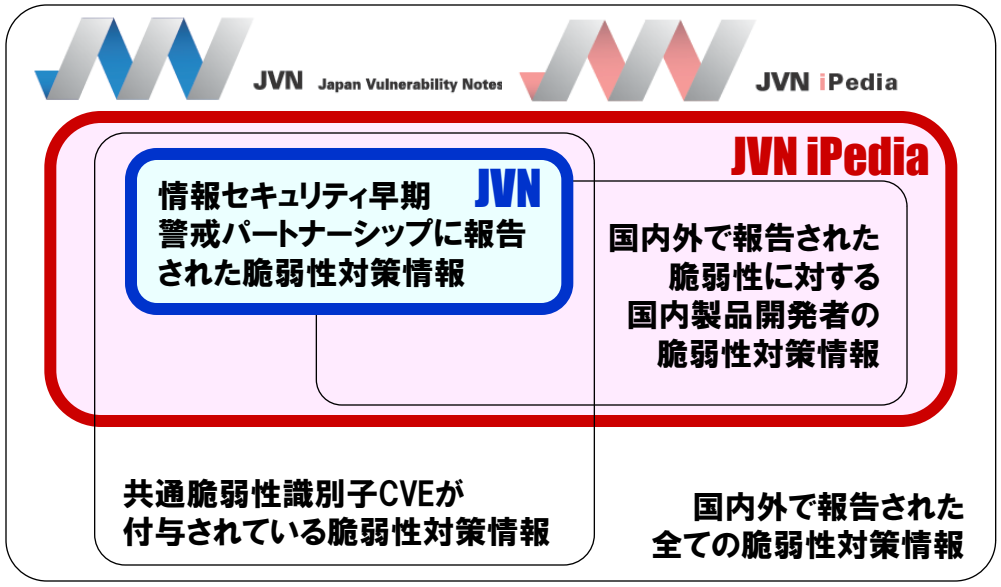
12月 MyJVNセキュリティ設定チェッカのリリース
セキュリティ設定チェックリスト記述形式（XCCDF）
共通セキュリティ設定一覧（CCE）

2010年1月 CVE互換取得（JVN、JVN iPedia、MyJVN）

2月 MyJVN WebサービスAPI 公開予定

3. MyJVN （コンセプト）
脆弱性対策自動化フレームワークに関する取り組み（3）

- **国際性**と国内向け脆弱性対策情報データベースとしての**地域性**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
自動化処理を考慮した利活用基盤上に、JVNとJVN iPediaの脆弱性対策情報を用いたサービスを構築する

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網羅し蓄積する

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

3. MyJVN （コンセプト）
脆弱性対策自動化フレームワークに関する取り組み（4）

- **国際性**と**地域性**とを兼ね備えたデータベースと
  国際的な共通基準を用いた**自動化フレームワーク**の連携

MyJVN　CVE、CPE、CWE、CVSSなど共通基準を用いた
自動化フレームワークサービス（Webサービス 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	情報セキュリティ早期警戒パートナーシップ案件（約400）	翻訳 → 情報セキュリティ早期警戒パートナーシップ案件（約400）
CERT/CC CPNI	CERT/CC、CPNI案件（約300）	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（約700）	蓄積 → JVN案件（約400）
日本国内製品開発者サイト	日本国内製品開発者案件（約100）	翻訳 → 日本国内製品開発者案件（約100）
NVD（英語）（約40,500）	NVD（約6,800）	（約7,600）

（約500）

IPA INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

2009年第4四半期の登録件数

3. MyJVN （コンセプト）
MyJVNバージョン1、 MyJVNバージョン2

- MyJVNバージョン1

  ⇒MyJVN脆弱性対策情報収集ツール
  （Flash GUIを用いた情報収集ツール）【2008年10月】
  - 製品を識別するために共通の名称CPE（共通プラットフォーム一覧、Common Platform Enumeration）、Webサービス API、XMLフォーマット（概要フォーマット：JVNRSS、詳細フォーマット：VULDEF）の整備
  - 製品視点から対策情報を選別するフィルタリング型情報サービスの実現

JVNRSS: Japan Vulnerability Notes RDF Site Summary
VULDEF: The VULnerability Data publication and Exchange Format data model

3. MyJVN （コンセプト）
MyJVNバージョン1、MyJVNバージョン2

- MyJVNバージョン2

  ⇒MyJVNバージョンチェッカ【2009年11月】
  - セキュリティ問題をチェックする手続き仕様OVAL (Open Vulnerability Assessment Language) の導入とMyJVN Webサービスの拡張
  - 脆弱性対策のための検査データ（バージョンチェック用）の提供

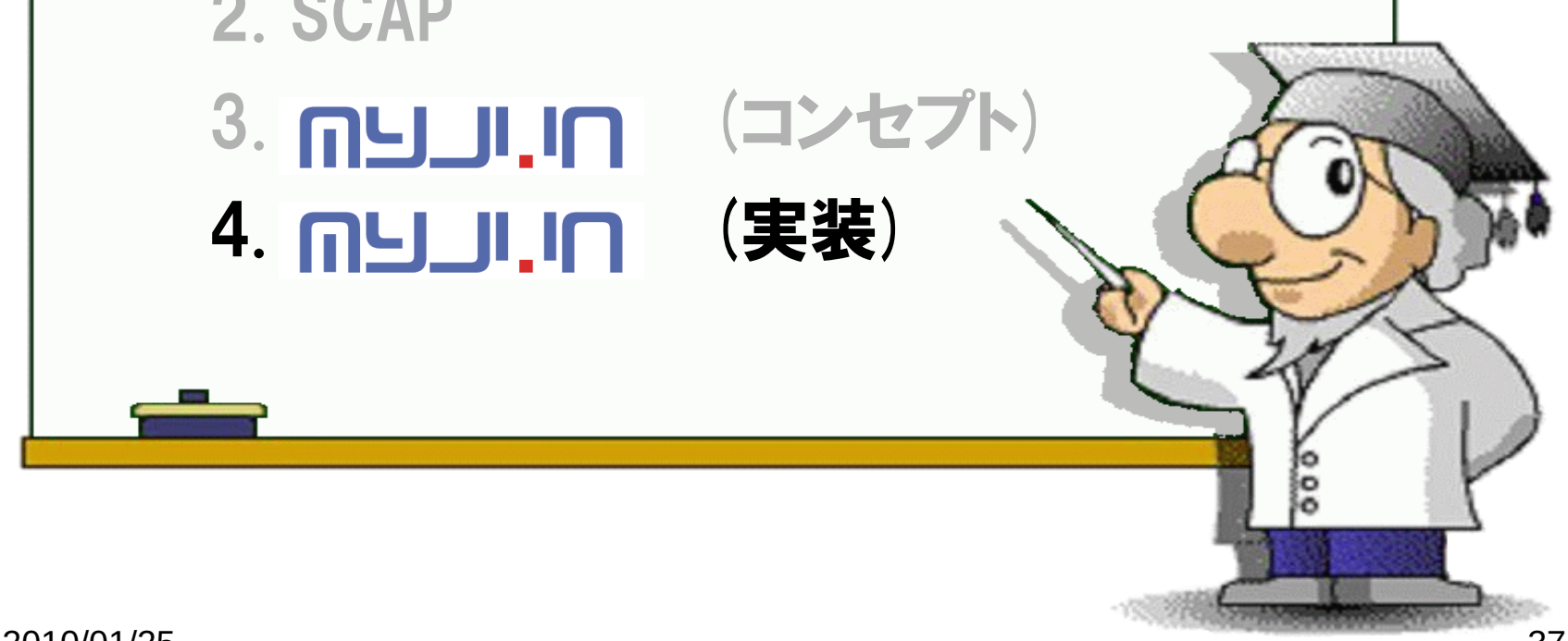
  ⇒MyJVNセキュリティ設定チェッカ【2009年12月】
  - 設定上の問題を取り扱うCCE (Common Configuration Enumeration)、セキュリティチェックリストを記述するXCCDF (Extensible Configuration Checklist Description Format)、セキュリティ問題をチェックする手続き仕様OVAL (Open Vulnerability Assessment Language) の導入とMyJVN Webサービスの拡張
  - 脆弱性対策のための検査データ（設定チェック用）の提供

脆弱性対策を「文書情報による人手でのチェック」から「ツールによる自動的なチェック」へと移行するための導入フェーズ

IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

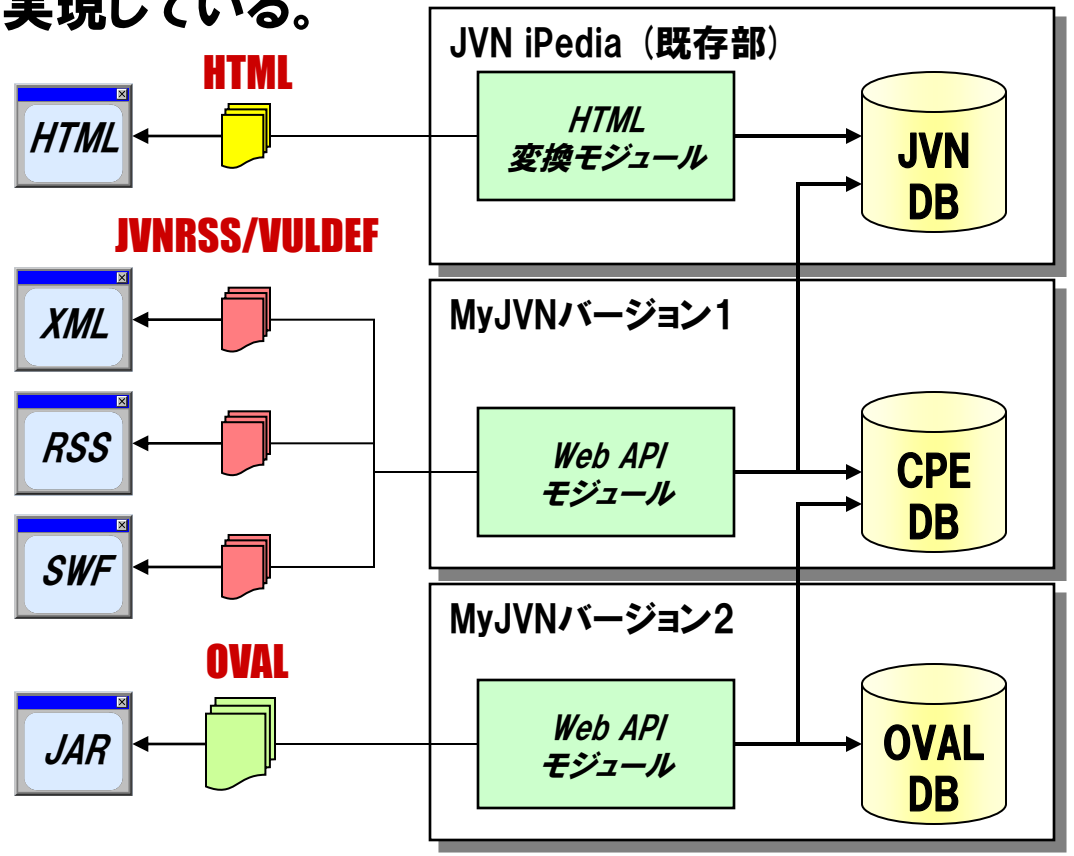
目次

1. 海外動向
2. SCAP
3. MyJI.IN （コンセプト）
4. **MyJI.IN （実装）**



4. MyJVN （実装）
システム構成（バージョン1 ＋ バージョン2）

- JVNならびにCPEデータベースを組合せて製品視点から対策情報を選別するフィルタリング型情報提供を実現し、CPEとOVALデータベースを組み合わせて検査データ提供を実現している。



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

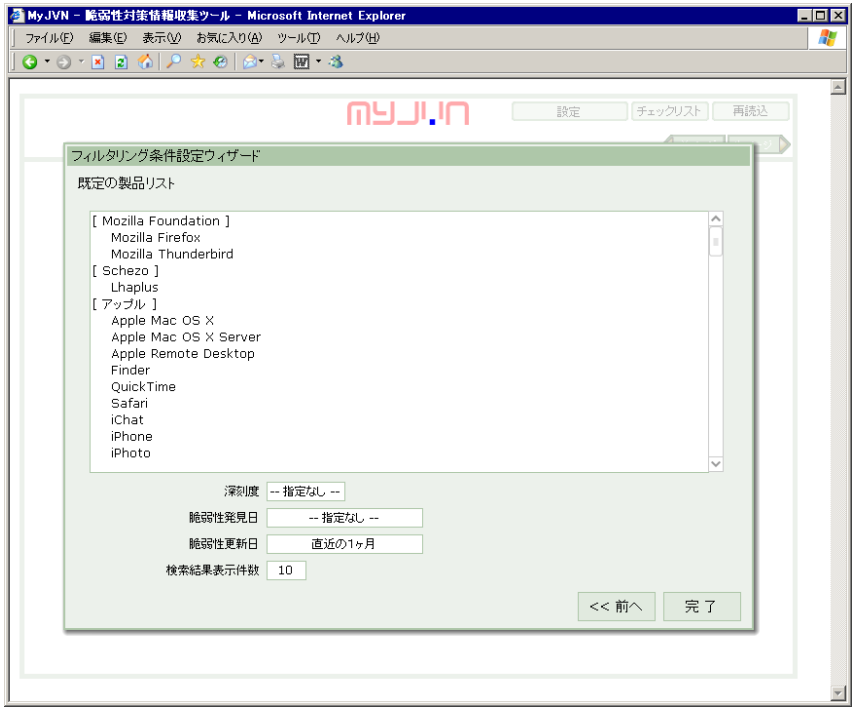
検査データ提供
⇒ MyJVNバージョンチェッカ
⇒ MyJVNセキュリティ設定チェッカ

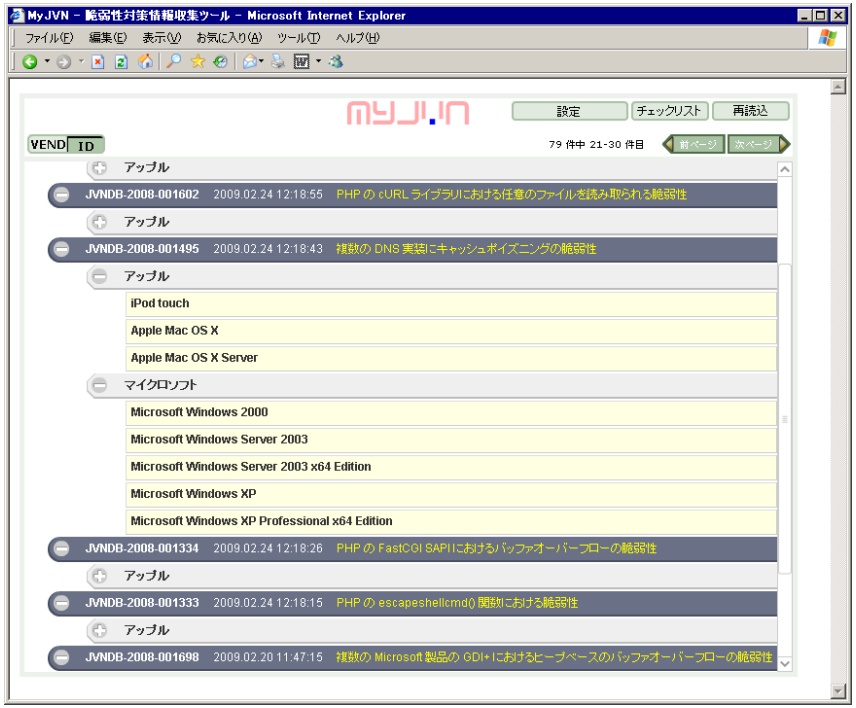
4. MyJVN （実装）
MyJVN脆弱性対策情報収集ツール

- 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自動化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。





4. MyJVN （実装）
フィルタリング型情報提供

- **ポイント①：共通プラットフォーム一覧の導入**
  - **CPE（共通プラットフォーム一覧：Common Platform Enumeration）は、情報システムを構成するハードウェア、ソフトウェアなどを識別するための共通の名称基準である。**
  - **このようなプラットフォーム識別の仕組みを整備していくことで、将来的に脆弱性有無やパッチ適用有無の確認といった自動化処理の範囲拡大と、脆弱性対策情報の相互参照や国際間での脆弱性対策情報の相互運用といった可能性が広がる。**

```
<?xml version="1.0" encoding="UTF-8"?>
 <cpe-item name="cpe:/h:iij:seil%2fx1">
       <title xml:lang="en-US">IIJ SEIL/X1</title>
       <title xml:lang="ja-JP">インターネットイニシアティブ SEIL/X1</title>
       <notes>
          <note>Vendor URL http://www.iij.ad.jp/en/index.html</note>
          <note>Product URL http://www.seil.jp/</note>
       </notes>
       <references>
          <reference href
          <reference href
       </references>
    </cpe-item>
</cpe-list>
```

```
 <cpe-item name="cpe:/a:adobe:acrobat">
    <title xml:lang="ja-JP">アドビシステムズ アクロバット</title>
    <title xml:lang="en-US">Adobe Acrobat</title>
</cpe-item>
<cpe-item name="cpe:/a:firebirdsql:firebird">
    <title xml:lang="en-US">Firebird Firebird</title>
</cpe-item>
```

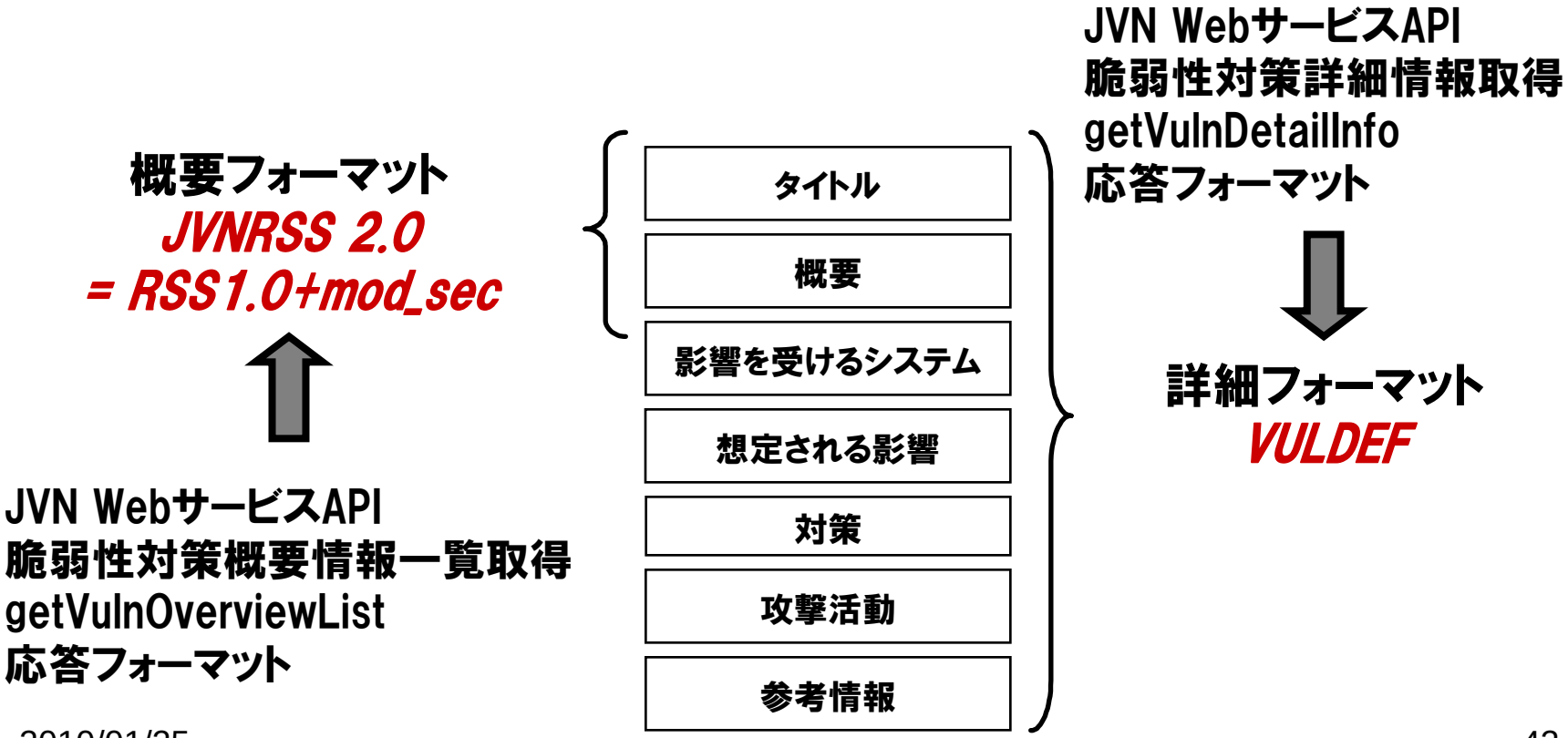
4. MyJVN （実装）
フィルタリング型情報提供

- ポイント②：JVN Webサービスの提供
  - 利用者自身ならびに開発者らがJVNを活用し、必要とされる新たなサービスを作り出すことのできる自動化フレームワークの整備につなげるため、JVNに登録されている脆弱性対策情報を使用するためのWebサービスAPIを規定した。
  - 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

4. MyJVN （実装）
フィルタリング型情報提供

- ポイント③：脆弱性対策情報のためのXMLフォーマットの規定
  - 利用者自身ならびに開発者らがJVNを活用し、必要とされる新たなサービスを作り出すことのできる自動化フレームワークの整備につなげるため、脆弱性対策情報の記述粒度を考慮した概要記述向けと詳細記述向けXMLフォーマットを規定した。

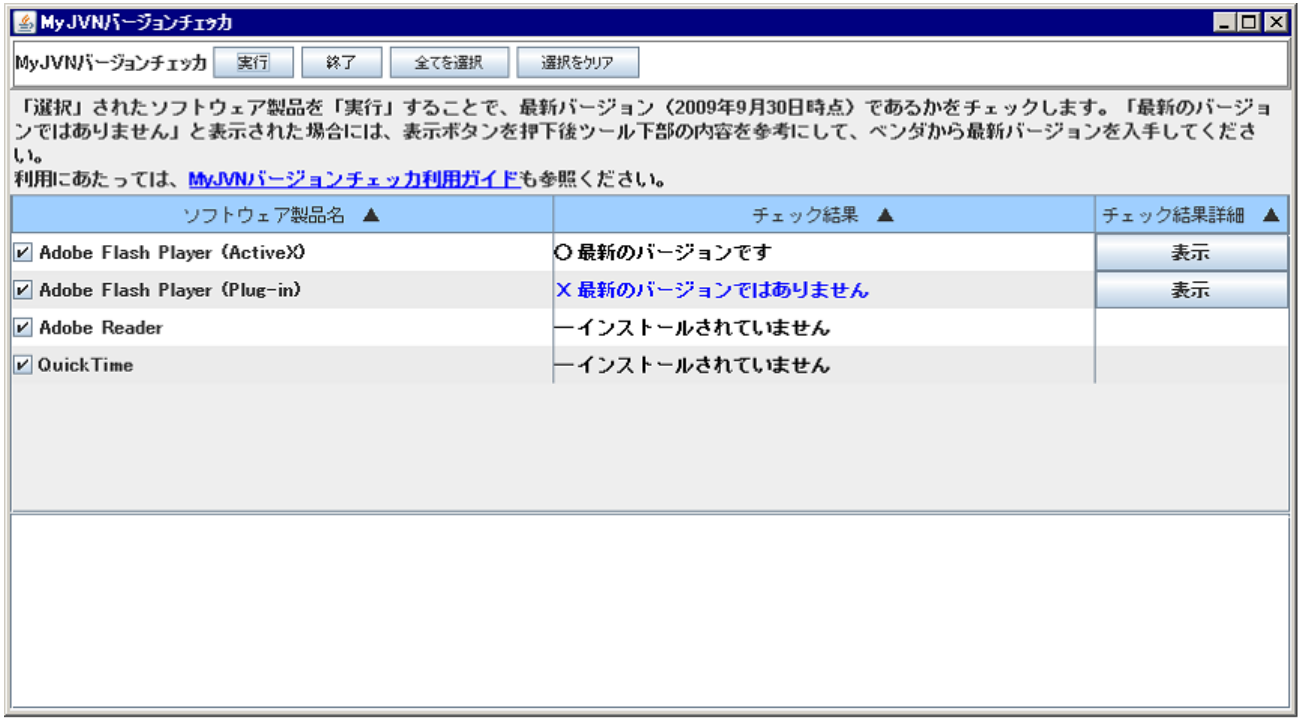


4. MyJVN （実装）
MyJVNバージョンチェッカ

- 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自動化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。**



4. MyJVN （実装）
MyJVNセキュリティ設定チェッカ

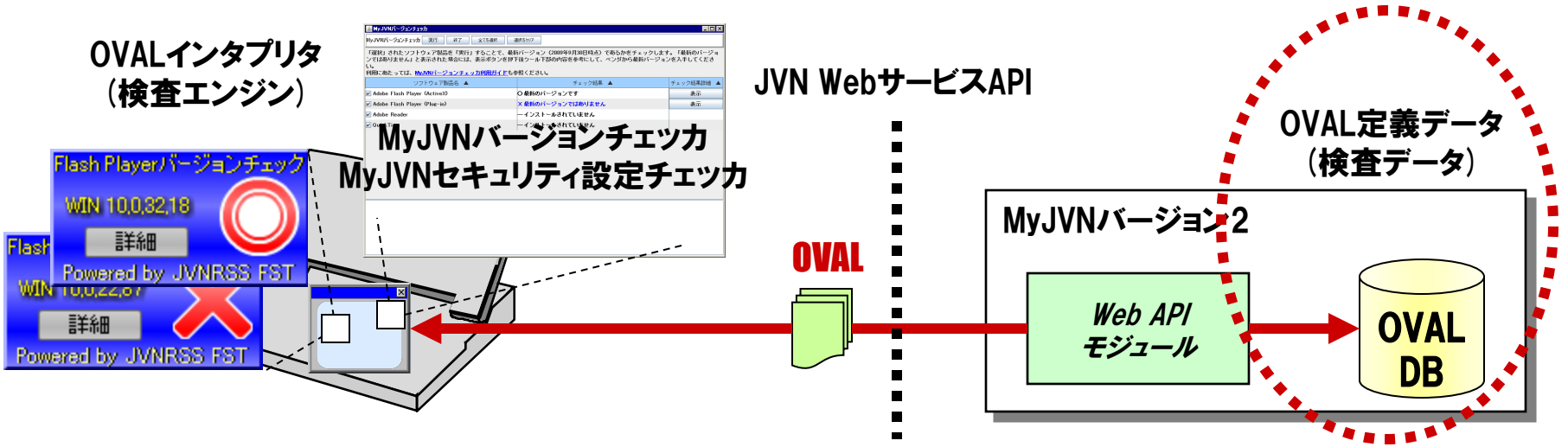
- http://jvndb.jvn.jp/apis/myjvn/index.html#CCCHECK

  設定に関する脆弱性対策チェックの自動化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。**

4. MyJVN （実装）
検査データ提供

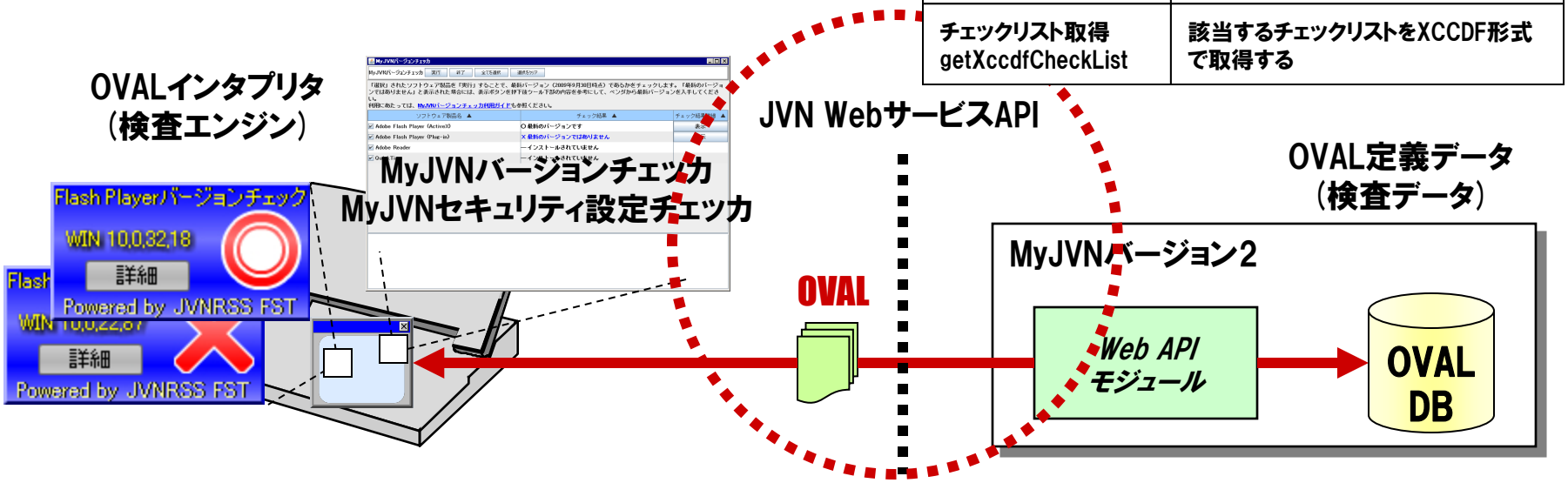
- ポイント④：セキュリティ検査言語の導入
  - OVAL（セキュリティ検査言語：Open Vulnerability and Assessment Language）は、OVAL言語で作成された脆弱性対策情報（OVAL定義データ）と、そのOVAL定義データを解釈するプログラム（OVALインタプリタ）とを用いて脆弱性対策のための確認作業を自動化する。



4. MyJVN （実装）
検査データ提供

- ポイント⑤：JVN WebサービスAPIの拡張
  - プログラム上のセキュリティ問題、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の有無をチェックして対策を促すなどの脆弱性対策自動化フレームワークの整備につなげるため、OVAL定義データ（チェック項目が記載されたXMLファイル）を提供するWebサービスAPIを追加した。
  - リクエストURLの基本構成
    http://jvndb.jvn.jp/myjvn?method=メソッド

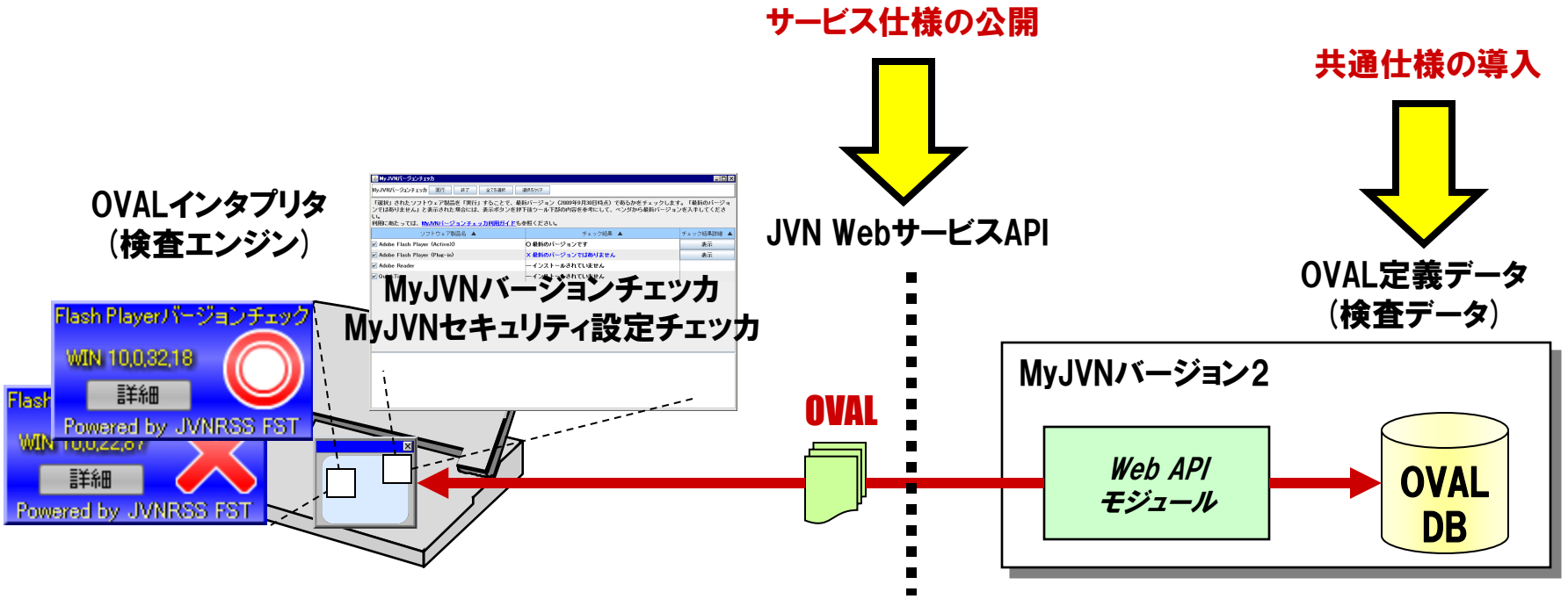
メソッド名称	概要
OVAL定義一覧取得 getOvalList	フィルタリング条件に該当するOVAL定義一覧をXML形式で取得する
OVAL定義データ取得 getOvalData	該当するOVAL定義データをOVAL形式で取得する
チェックリスト取得 getXccdfCheckList	該当するチェックリストをXCCDF形式で取得する



4. MyJVN （実装）
MyJVNの考える脆弱性対策機械処理基盤の整備とは、

- **共通仕様の導入とサービス仕様の公開**

  共通仕様に基づき作成された定義データを流通させることの利点は、チェック対象となるオブジェクトの位置、その位置に格納されている値など確認手続きを共有できること、さらに、その定義データに従ってチェックするプログラムを誰もが開発できることであり、自動化処理の範囲拡大と相互運用といった可能性が広がる。

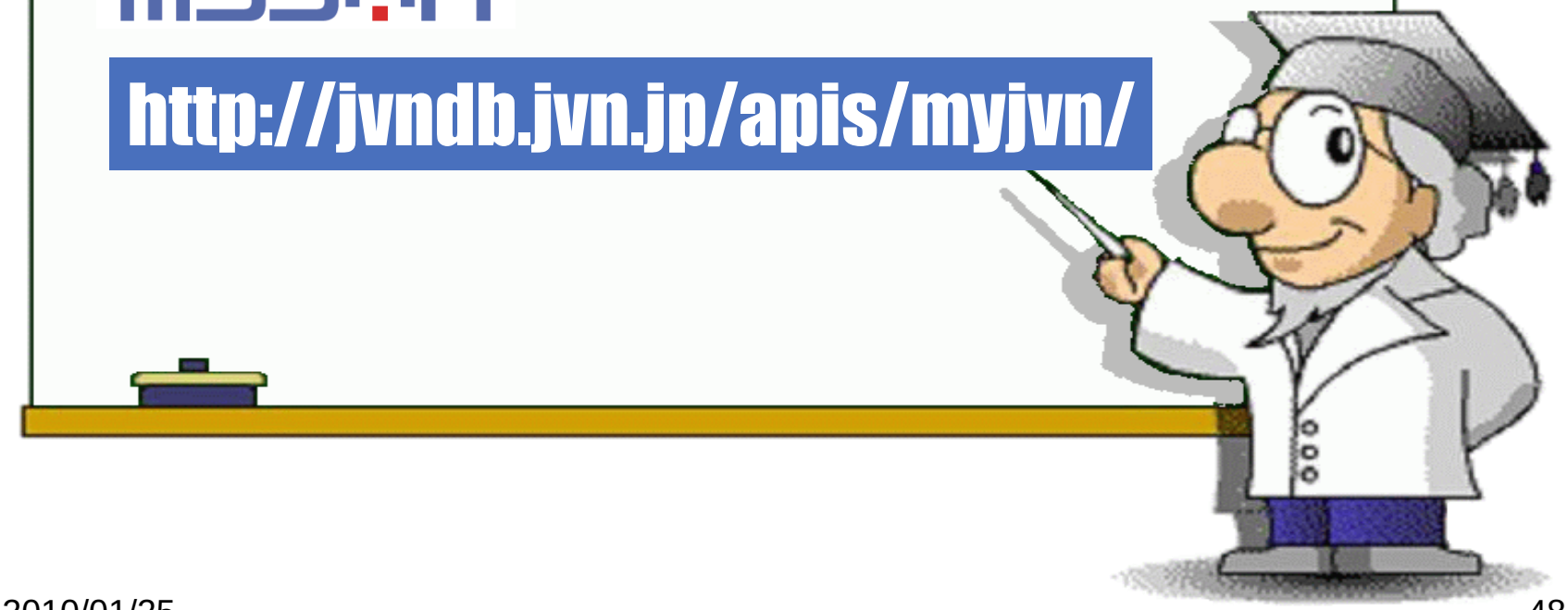


IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

MyJVNでは、脆弱性対策自動化フレームワークの整備と共通基準の導入を進めながら、脆弱性対策情報データベースとして国際性と地域性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

- JVN (Vulnerability Handling Coordination DB)
  http://jvn.jp/en/
- JVN iPedia (Vulnerability Archiving DB)
  http://jvndb.jvn.jp/en/
- MyJVN
  http://jvndb.jvn.jp/apis/myjvn/
  - JVNRSS (JP Vendor Status Notes RSS)
    http://jvndb.jvn.jp/schema/jvnrss.html
  - Qualified Security Advisory Reference (mod_sec)
    http://jvndb.jvn.jp/schema/mod_sec.html
  - VULDEF: The VULnerability Data publication and Exchange Format data model
    http://jvndb.jvn.jp/schema/vuldef.html
  - 脆弱性対策情報の利活用基盤MyJVNの提案
    情報処理学会 コンピュータセキュリティ シンポジウム 2008 (Oct.8-10, 2008)
  - MyJVNを用いた脆弱性対策情報提供サービスの検討
    情報処理学会 コンピュータセキュリティ 研究報告 Vol.2009 No.20, pp.283-288 (Mar. 5-6, 2009)

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関連サイト
  - SCAP（The Information Security Automation Program and The Security Content Automation Protocol）
    http://nvd.nist.gov/scap.cfm
  - NCP（National Checklist Program）
    http://nvd.nist.gov/ncp.cfm
  - FDCC（Federal Desktop Core Configuration）
    http://nvd.nist.gov/fdcc/index.cfm
  - NVD（National Vulnerability Database）
    http://nvd.nist.gov/

参考情報

- SCAP関連ドキュメント
  - NIST Interagency Report 7343
    The Security Content Automation Program (SCAP): Automating Compliance Checking, Vulnerability Management, and Security Measurement (2006)
    http://nvd.nist.gov/scap/docs/SCAP-NISTIR-7343.pdf
  - NIST IR-7511 Rev. 1
    DRAFT Security Content Automation Protocol (SCAP) Version 1.0 Validation Program Test Requirements (2009)
    http://csrc.nist.gov/publications/drafts/nistir-7511/draft-nistir-7511_rev1.pdf
  - SP 800-117: DRAFT Guide to Adopting and Using the Security Content Automation Protocol (SCAP) (2009)
    http://csrc.nist.gov/publications/drafts/800-117/draft-sp800-117.pdf
  - SP 800-126: DRAFT The Technical Specification for the Security Content Automation Protocol (SCAP) (2009)
    http://csrc.nist.gov/publications/drafts/sp800-126/Draft-SP800-126.pdf

参考情報

- 共通基準
  - CVE（Common Vulnerabilities and Exposures）
    http://cve.mitre.org/
    http://www.ipa.go.jp/security/vuln/CVE.html
  - CCE（Common Configuration Enumeration）
    http://cce.mitre.org/
  - CPE（Common Platform Enumeration）
    http://cpe.mitre.org/
    http://www.ipa.go.jp/security/vuln/CPE.html
  - XCCDF（EXtensible Checklist Configuration Description Format）
    http://nvd.nist.gov/xccdf.cfm
  - OVAL（Open Vulnerability Assessment Language）
    http://oval.mitre.org/
  - CVSS（Common Vulnerability Scoring System）
    http://www.first.org/cvss/
    http://www.ipa.go.jp/security/vuln/SeverityCVSS2.html

参考情報

- Making Security Measurable
  - CWE（Common Weakness Enumeration）
    http://cwe.mitre.org/
    http://www.ipa.go.jp/security/vuln/CWE.html
  - CAPEC（Common Attack Pattern Enumeration and Classification）
    http://capec.mitre.org/
  - CEE（Common Event Expression）
    http://cee.mitre.org/
  - CRF（Common Result Format）
    http://crf.mitre.org/
  - CMSS（Common Misuse Scoring System）
    http://csrc.nist.gov/publications/drafts/nistir-7517/Draft-NISTIR-7517.pdf
  - CCSS（Common Configuration Scoring System）
    http://csrc.nist.gov/publications/drafts/nistir-7502/Draft-NISTIR-7502.pdf