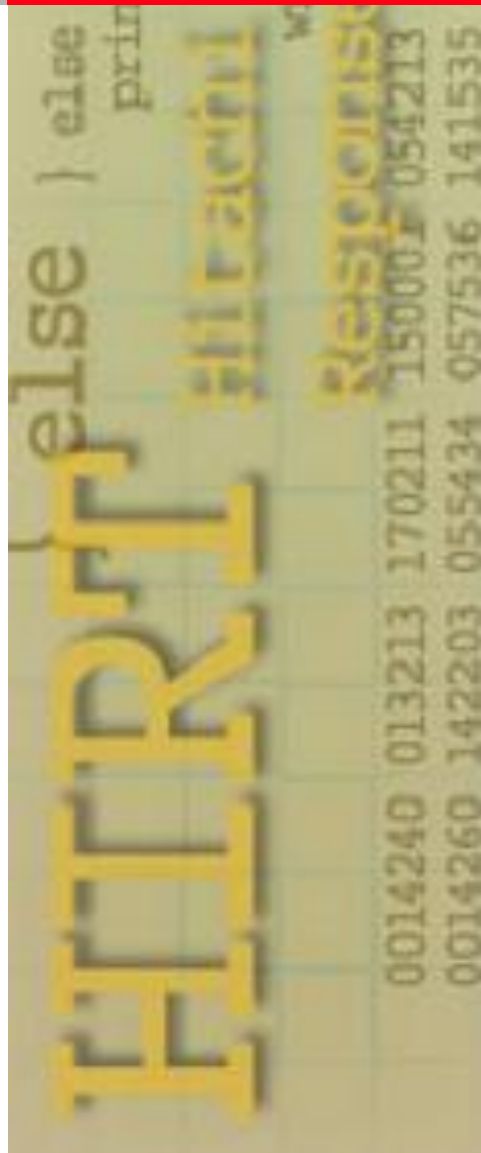
HITACHI
Inspire the Next

脆弱性対策データベースとその自動化基盤 ～JVN, JVN iPedia and MyJVN～

2013/09/30

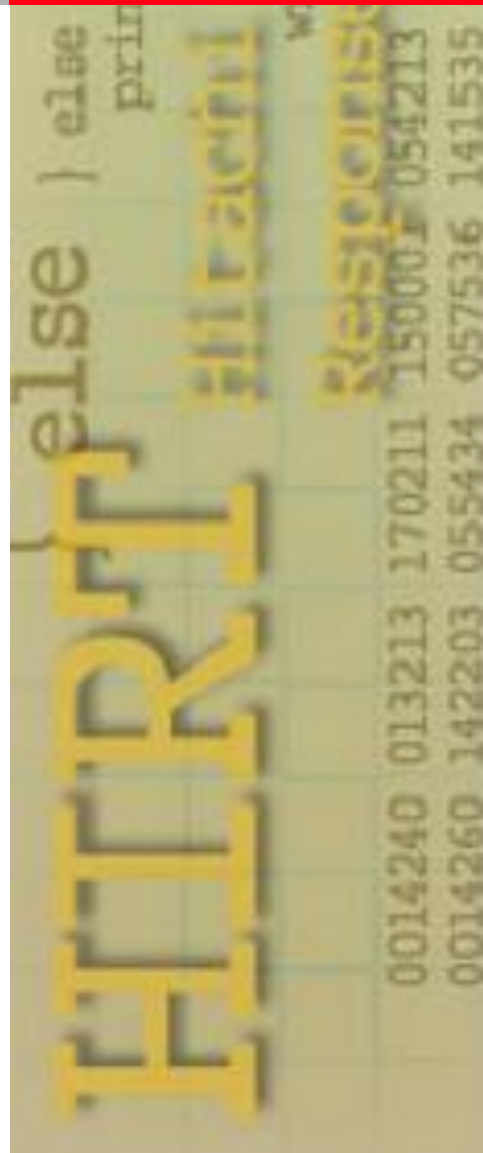
寺田真敏
(株) 日立製作所
Hitachi Incident Response Team
http://www.hitachi.co.jp/hirt/



HITACHI
Inspire the Next

寺田真敏　自己紹介

現在、(株) 日立製作所横浜研究所とHitachi Incident Response Teamに所属。
2002年-2006年慶應義塾大学大学院理工学研究科。
2004年よりJPCERT/CC専門委員、(独) 情報処理推進機構セキュリティセンター研究員。
2008年より中央大学大学院客員講師、日本シーサート協議会副運営委員長、テレコム・アイザック推進会議運営委員、マルウェア対策研究人材育成ワークショップ (MWS) 組織委員。
2004年-2007年中央大学研究開発機構客員研究員。
2006-2008年 (社) 情報処理学会コンピュータセキュリティ研究会主査。



Opening

HITACHI
Inspire the Next

本発表では、JVNに関わることになったきっかけと、X.1500 (CYBEX: Overview of cybersecurity information exchange) の付録に掲載されている日本でのCYBEX活用について紹介します。

III.2 Example: Japan vulnerability information portal site, JVN

JVN stands for "Japan Vulnerability Notes" and provides vulnerability and related information on software used in Japan, with which it intends to contribute to the countermeasure to cyber threats. In order to enable application developers to use data through an open interface, JVN has adopted SCAP and contains local (domestic) information and international information, resulting in the JVN security content automation framework. Just like the National Vulnerability Database (NVD), each of the vulnerability information contains a CVE number, provides a CVSS score, and a CWS number. Moreover, the CPE name of the affected product is also provided.

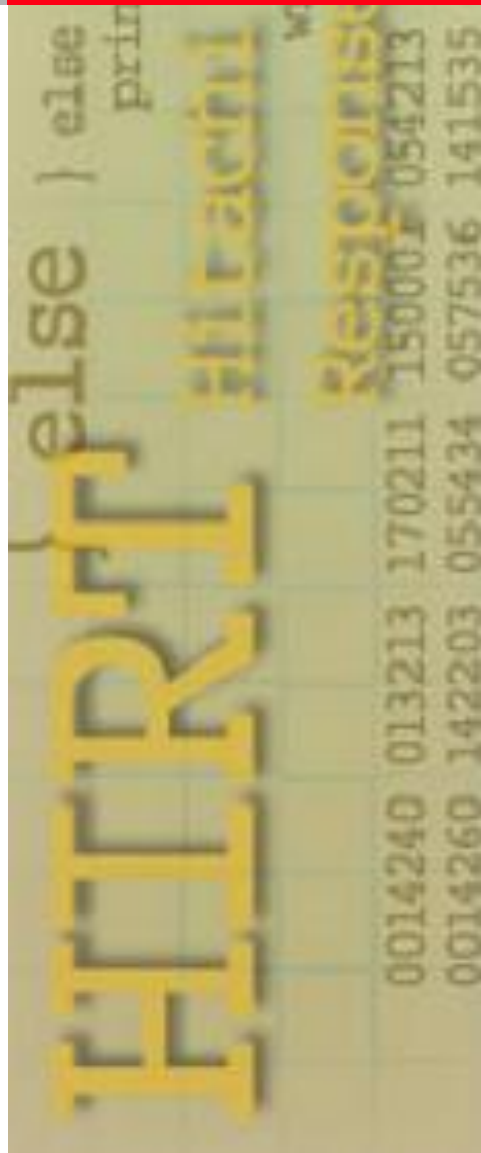
The framework consists of three components: MyJVN, JVN, and JVN iPedia (see Figure III.2), each of which is elaborated below.

掲載にあたり、ご支援を頂いた皆様に、感謝を致します。

Contents

HITACHI
Inspire the Next

1. プロローグ
2. JVNとは
3. JVN脆弱性対策機械処理基盤
4. JVNにおけるCYBEX利用
5. 仕様の概要



Hitachi Incident Response Team

http://jvn.jp/nav/jvn.html

JVNの歴史

JVN：名称の変遷

2003年2月: JVN ワーキンググループ結成、JVN 試行サイトの公開

JPCERT/CCの支援のもと、慶應義塾大学土居・高田研究室を中心に株式会社インターネットイニシアティブ (IIJ)、インターネットセキュリティシステムズ株式会社(当時)が協力して実施。

JVN: JPCERT/CC Vendor status Notes

2004年7月: 情報セキュリティ早期警戒パートナーシップ発足

JVN は IPA と JPCERT/CC の共同運用形態に移行。

JVN: JP Vendor status Notes

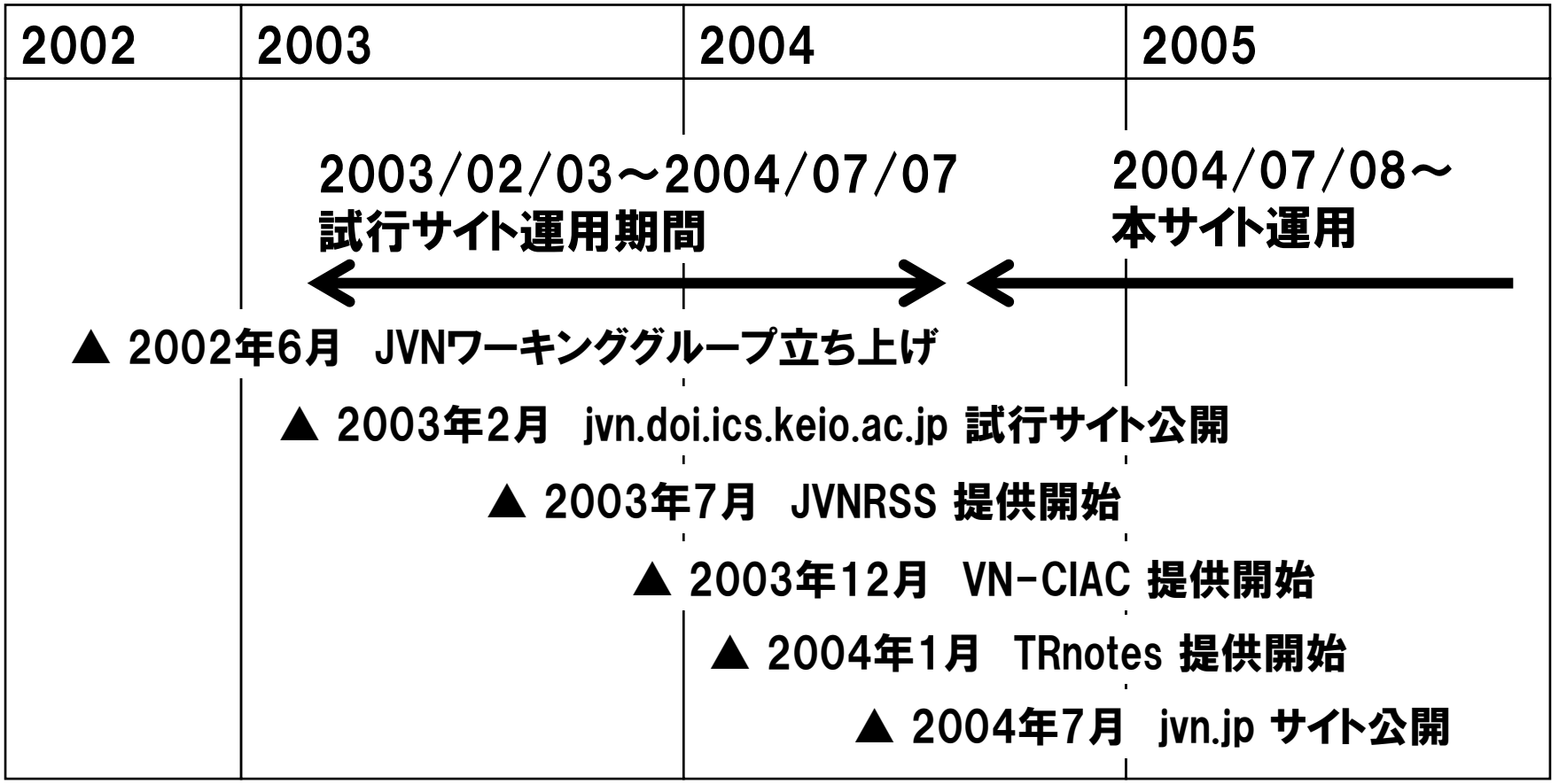
2007年4月: サイトデザインのリニューアルにともない発信情報を充実

詳細情報や脆弱性情報分析結果など案件ページの情報拡充とデザイン更新。JVN iPedia (http://jvndb.jvn.jp/) サービス開始。

JVN: Japan Vulnerability Notes

2008年5月: JVN 英語サイト(http://jvn.jp/en/) および JVNiPedia 英語サイト(http://jvndb.jvn.jp/en/) 開設

2002年6月～　JVNプロジェクトの開始



Hitachi Incident Response Team

JVNを作ろう!!

コンピュータセキュリティシンポジウム 2002
平成 14 年 10 月

JPCERT/CC Vendor Status Notes DB 構築に関する検討

寺田真敏†‡
terada@doi.ics.keio.ac.jp

土居範久†
doi@keio.ac.jp

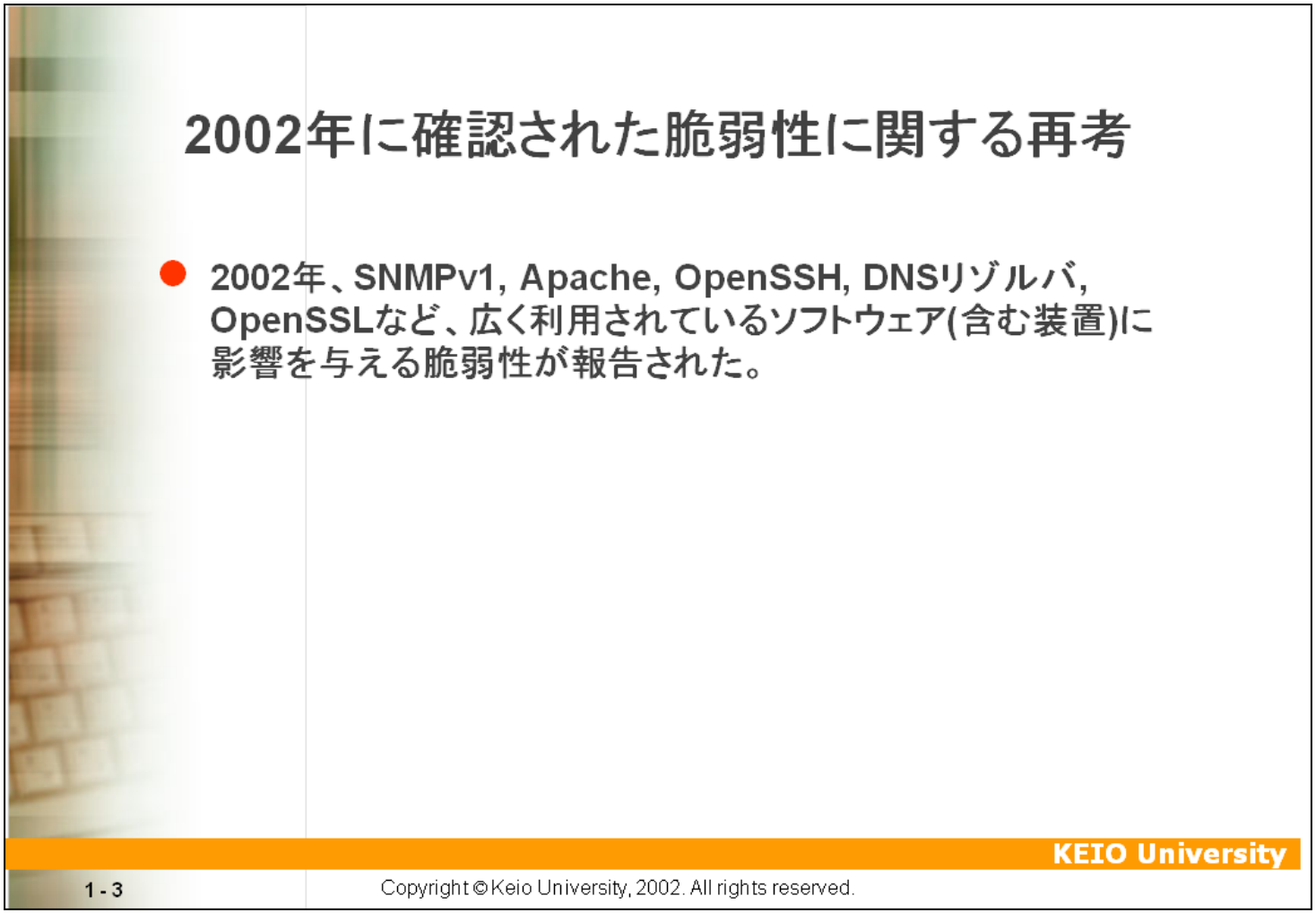
† 慶應義塾大学大学院理工学研究科
〒223-8522 神奈川県横浜市港北区日吉 3-14-1
‡ (株)日立製作所 システム開発研究所
〒224-0817 神奈川県横浜市戸塚区吉田町 292

あらまし：インターネットの常時接続の普及に伴い、マルウェアの流布を含む不正アクセス活動は活発化しており、また、その被害も広範囲かつ多岐に渡るようになってきている。しかし、不正アクセス対策を行なうために必要となる、国内で利用されているソフトウェアや装置を対象とする脆弱性情報ならびに対策情報については、「情報が散々している」「影響範囲の把握が難し

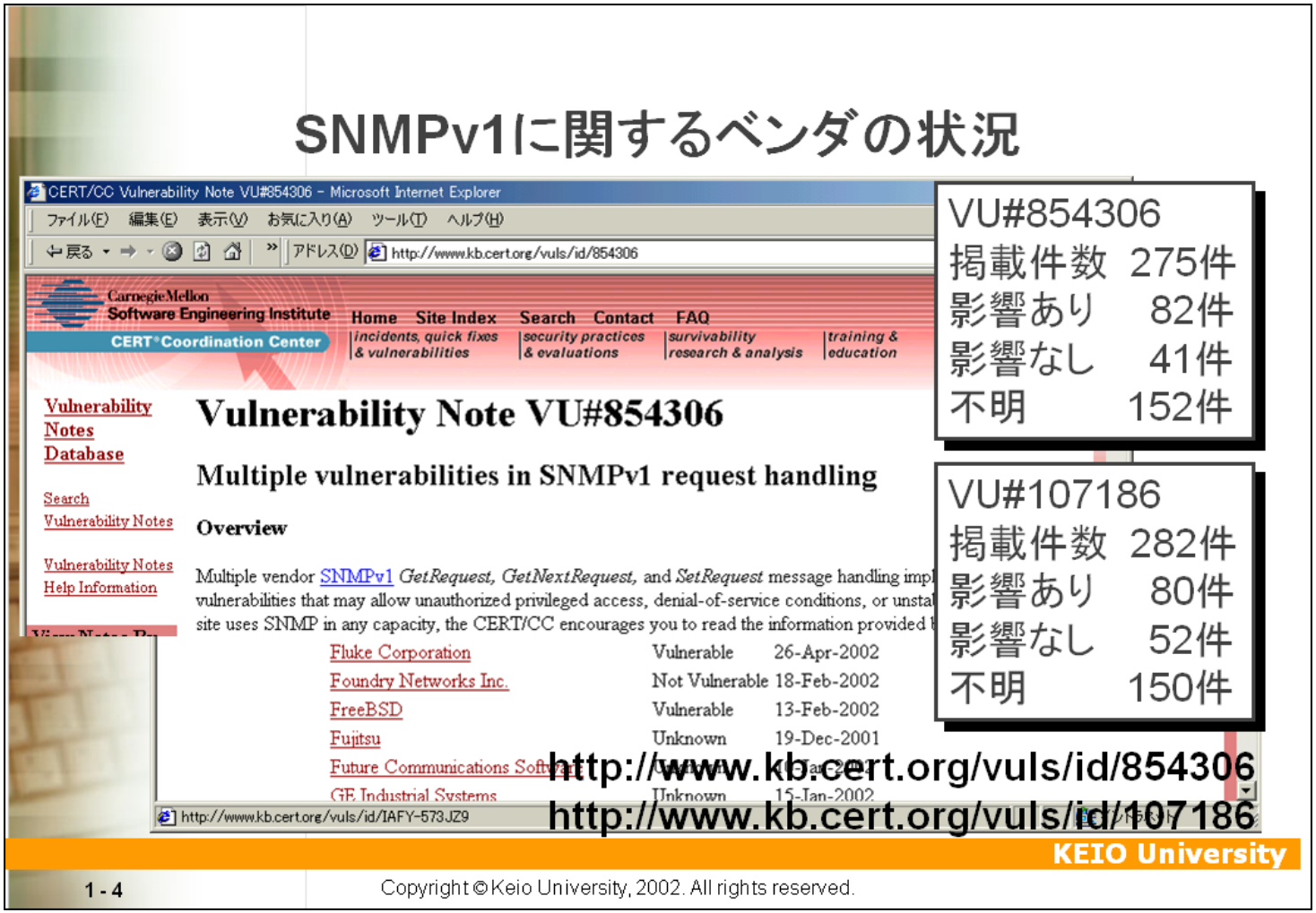
JVNを作ろう!!

JVNを作ろう!!

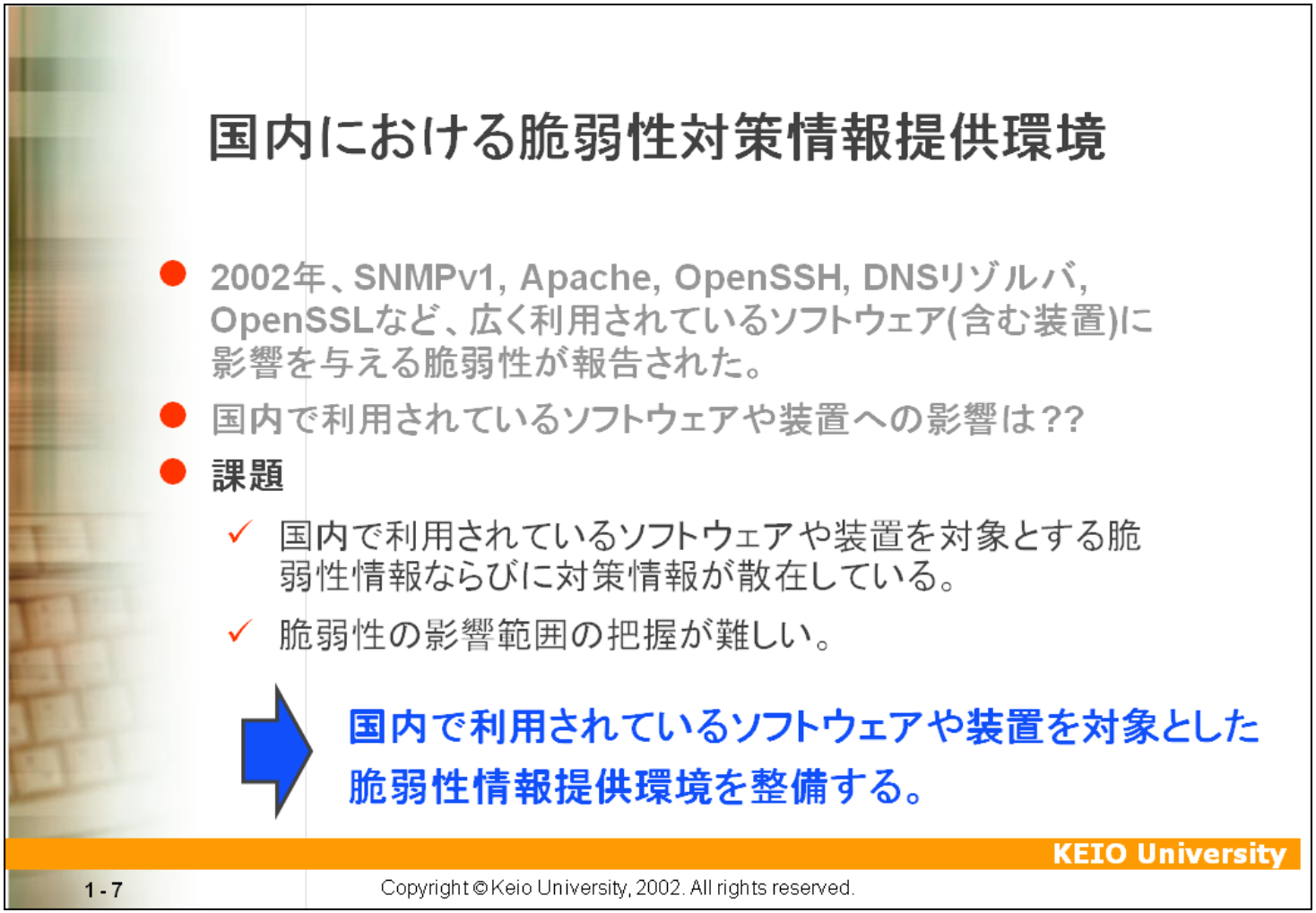
JVNを作ろう!!



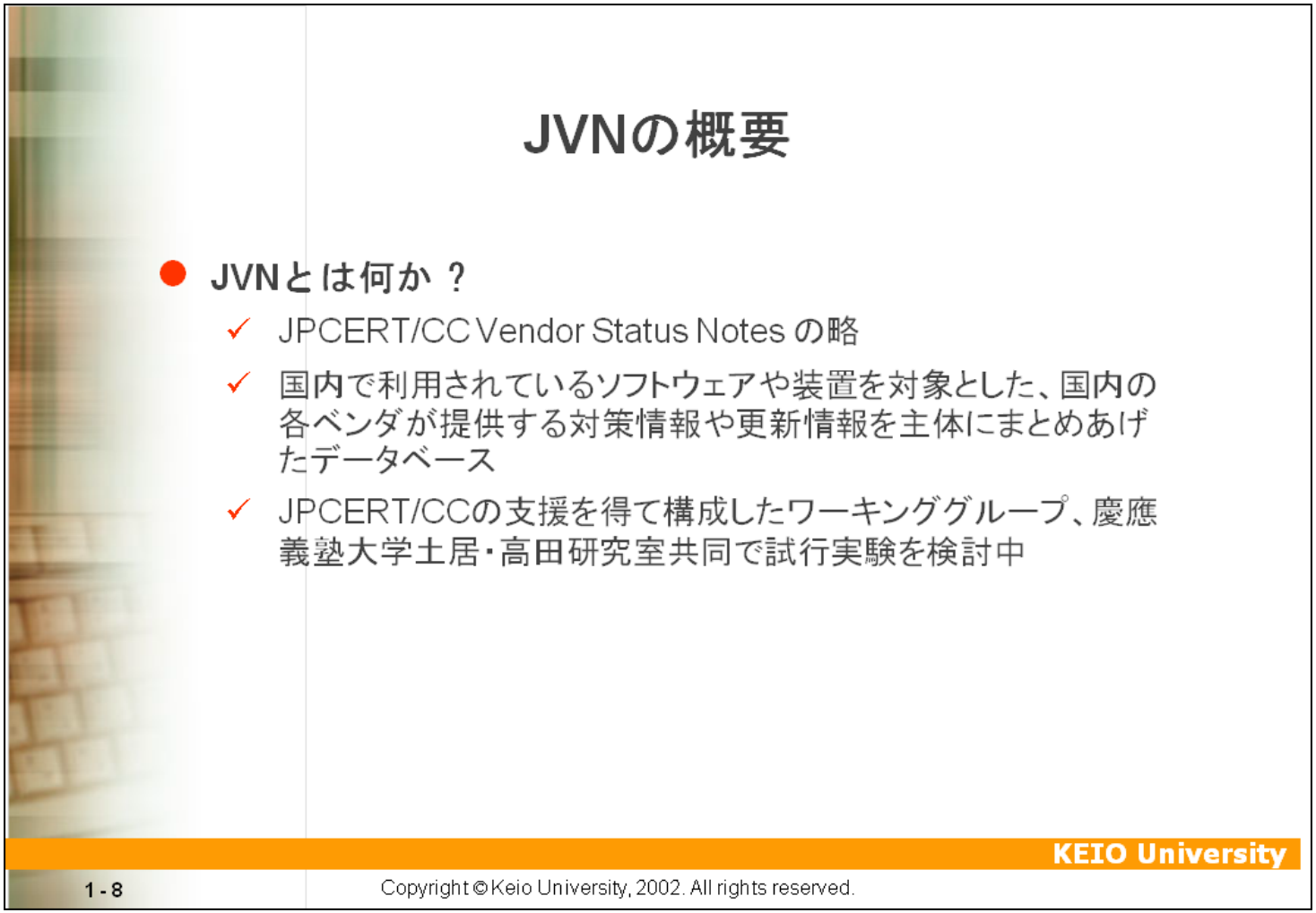
JVNを作ろう!!



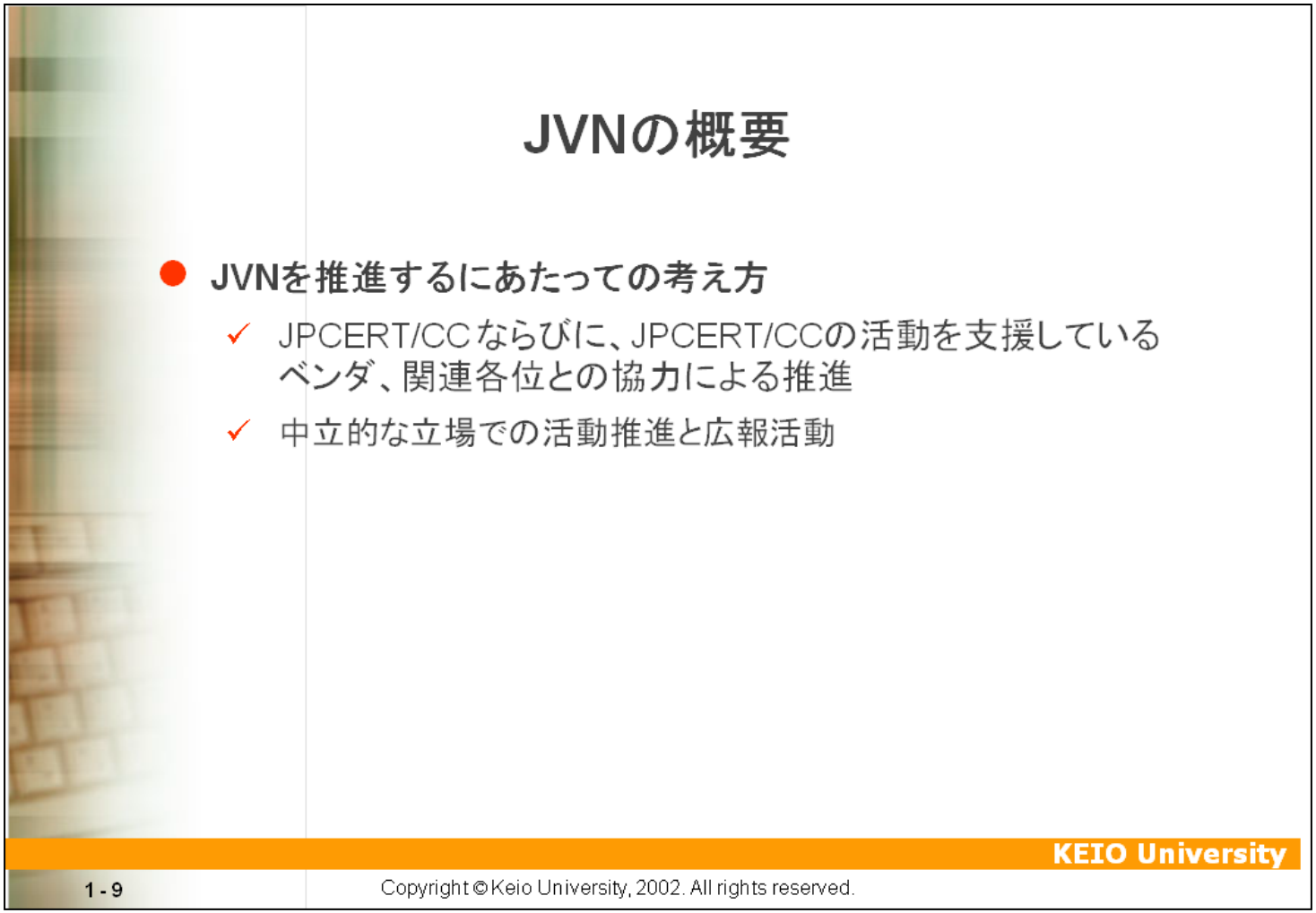
JVNを作ろう!!



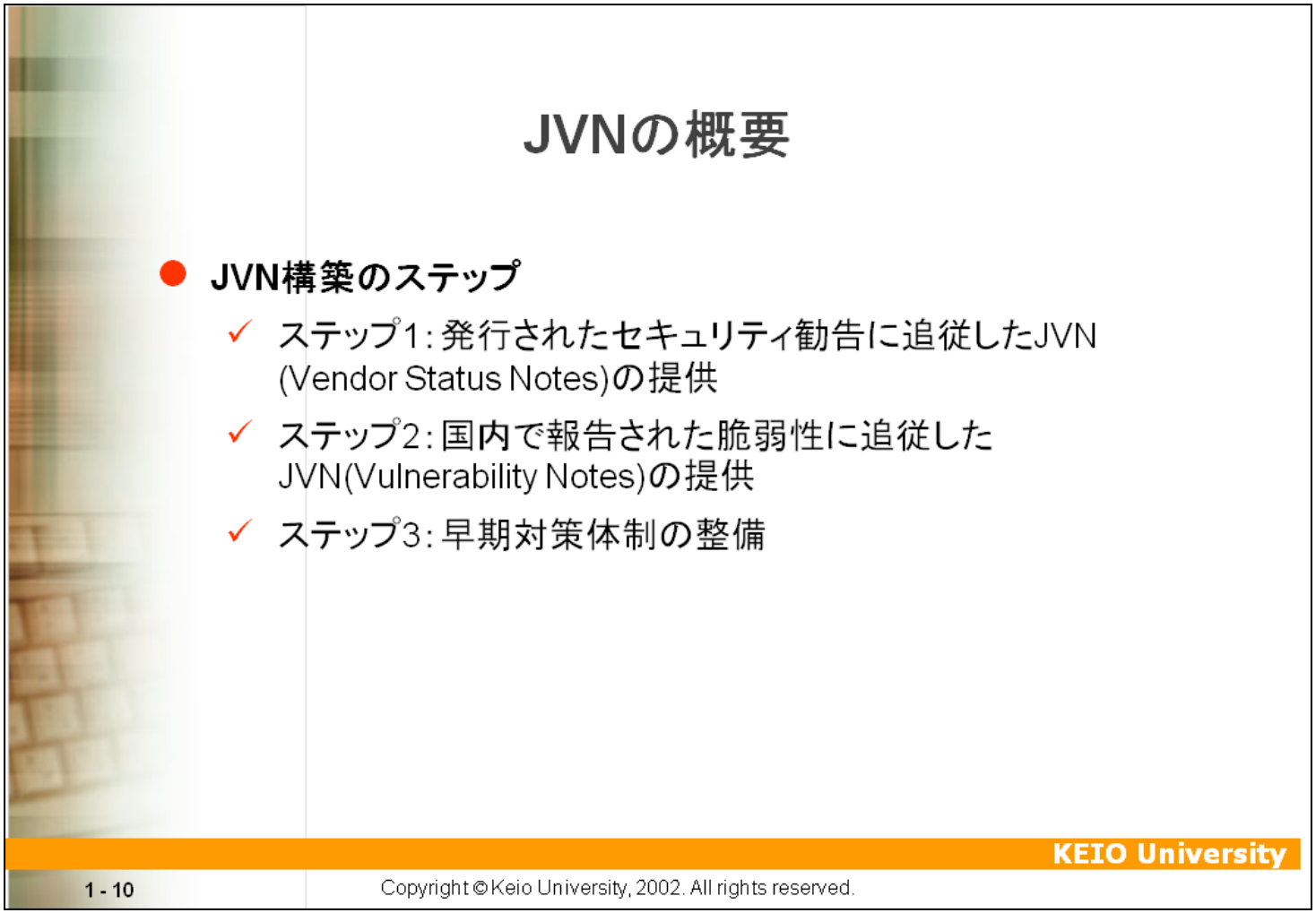
JVNを作ろう!!



JVNを作ろう!!



JVNを作ろう!!



2004年8月～　脆弱性対策機械処理基盤の検討開始

情報処理学会 コンピュータセキュリティ シンポジウム 2005, pp.667-672 (Oct.26-28, 2005)

マルチベンダ環境の情報システムを対象とした脆弱性管理システムの検討

菊地 大輔 †1　　寺田 真敏 †2†3†4　　福澤 淳二 †2　　土居 範久 †1

†1 中央大学大学院 理工学研究科 情報工学専攻　〒 112-8551 東京都文京区春日 1-13-27

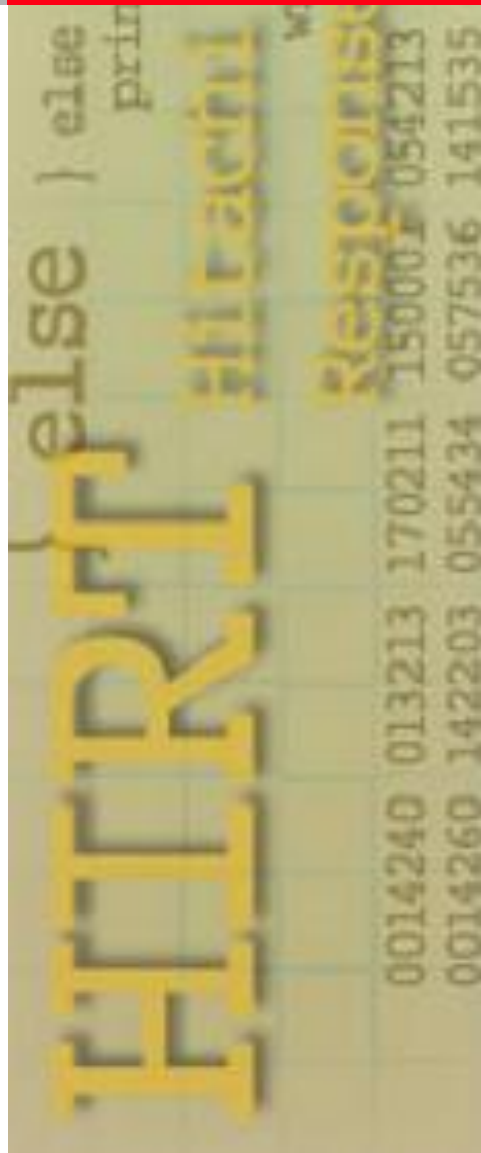
†2 独立行政法人 情報処理推進機構　〒 113-6591 東京都文京区本駒込二丁目 28 番 8 号
文京グリーンコート センターオフィス 16 階

†3 慶應義塾大学 大学院 理工学研究科　〒 223-8522 神奈川県横浜市港北区日吉 3-14-1

あらまし　情報システムを構成するソフトウェア環境は，提供形態ならびに複数のバージョンの混在という視点から見て，多様化が進んでいる．このため，脆弱性対策にあたり，文書という対策情報提供の形態だけで脆弱性の影響有無を判定するという手法では，検査の抜け漏れを完全に防ぐことは難しい．そこで，本稿では，現行の情報システムの脆弱性を管理するために求められる要件を提示すると共に，これら要件を満たすための脆弱性管理システムを提案する．脆弱性管理システムは，パターンファイルによる脆弱性の影響を受けるか否かを判定する機能をベースとし，パターンファイルの配布ならびに，脆弱性による深刻度算出を含んだ機能を提供する．

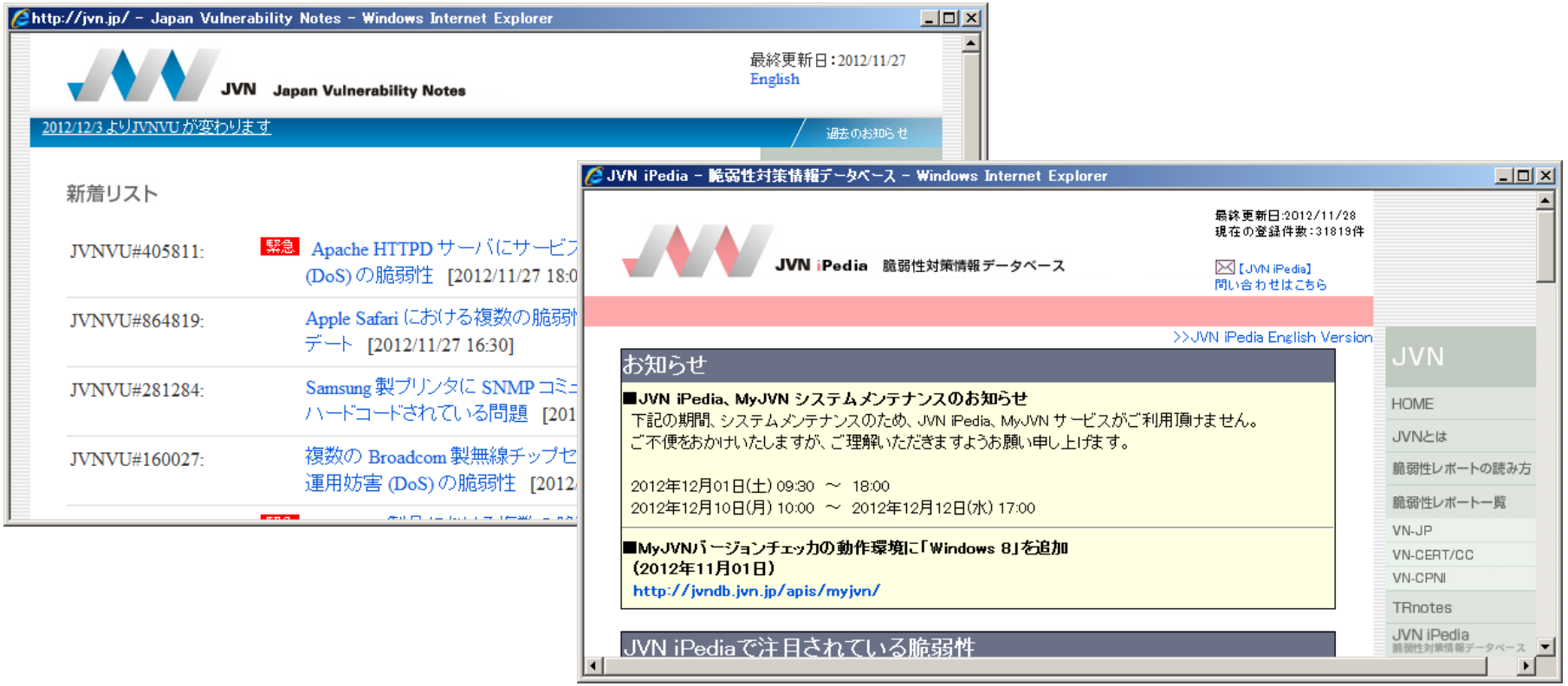
Contents

HITACHI
Inspire the Next



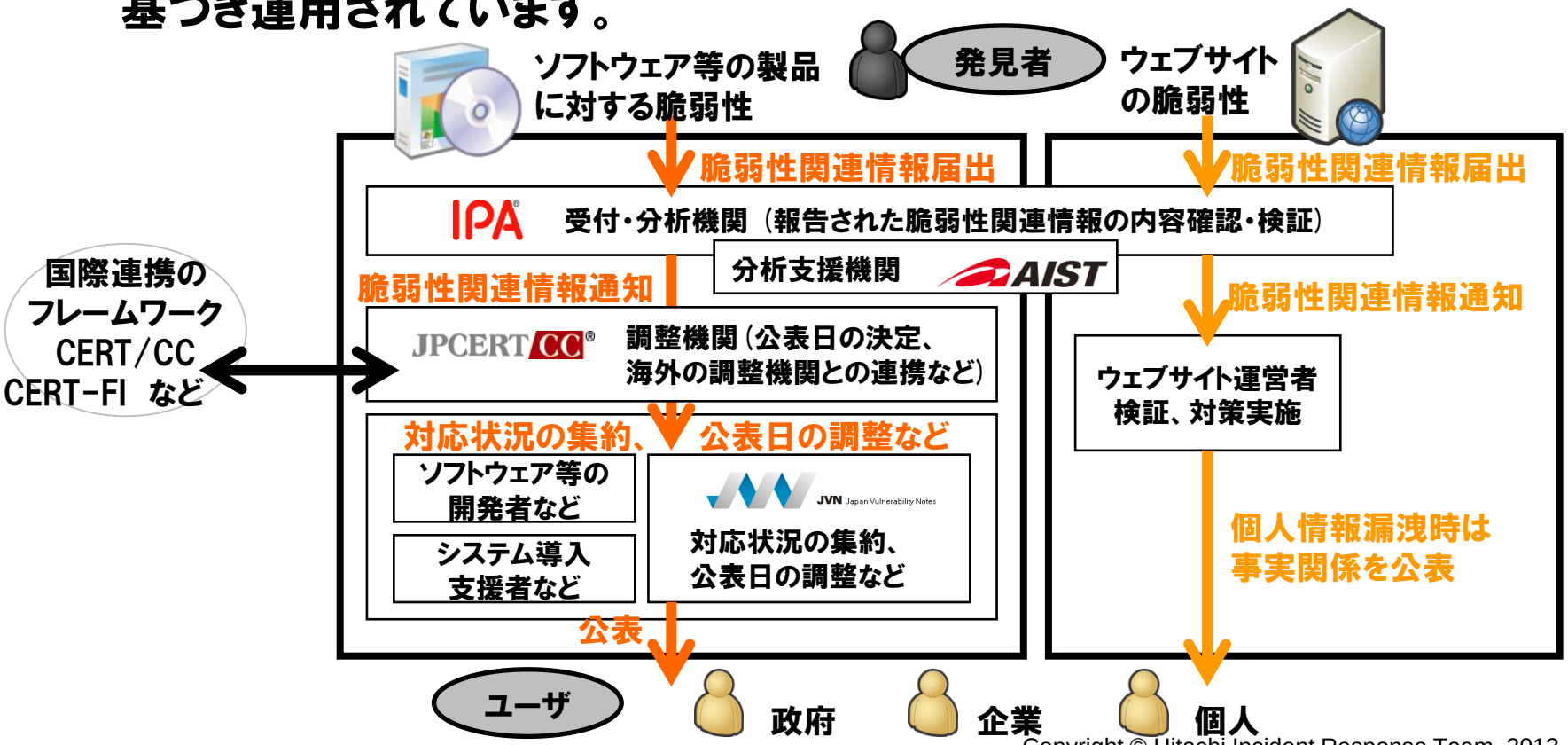
ご存じですか？ JVN

- JVN は、“Japan Vulnerability Notes” の略です。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です。



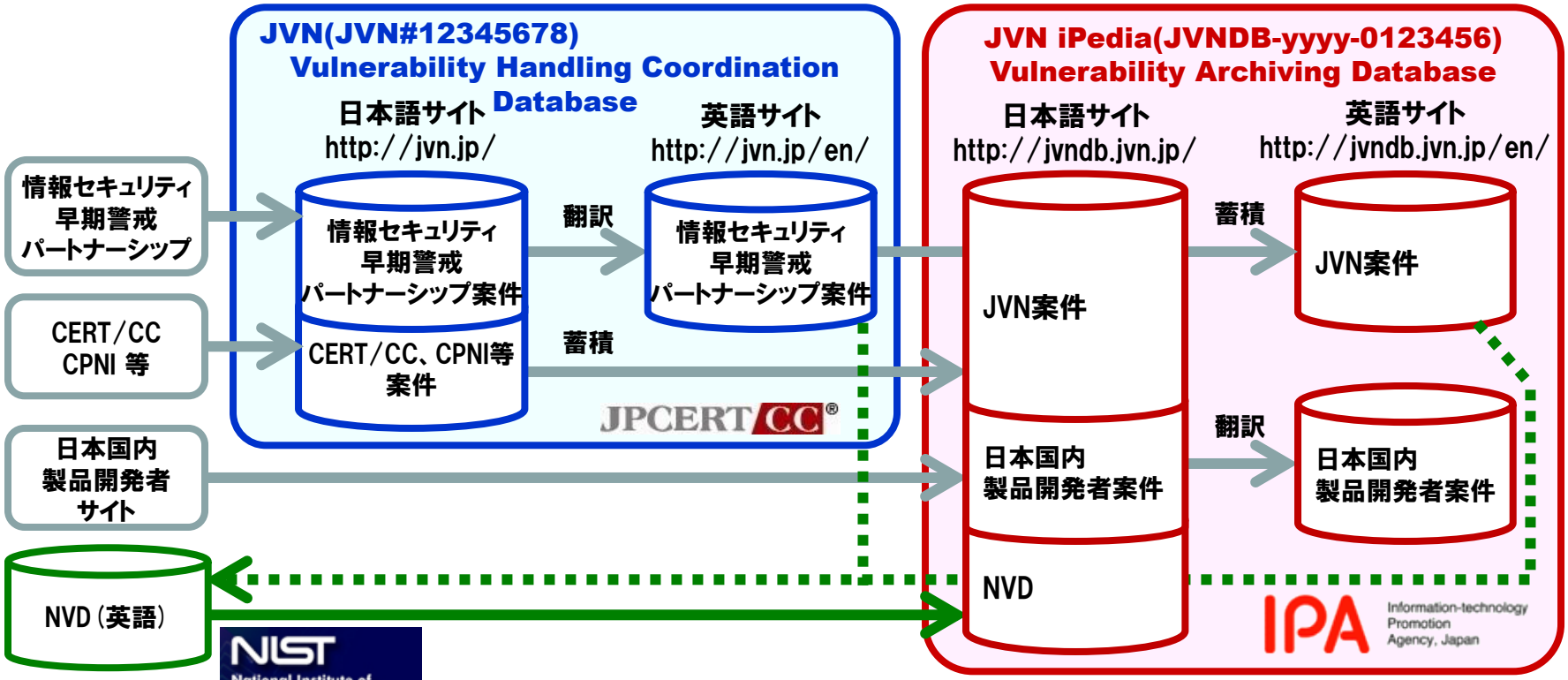
ご存じですか？ 情報セキュリティ早期警戒パートナーシップ

- ソフトウエア等の製品やウェブサイトに見つかった脆弱性に関する情報を受け付け、製品開発者に修正を促すフレームワークです。2004年7月8日施行の脆弱性関連情報の取扱い「ソフトウエア等脆弱性関連情報取扱基準」に基づき運用されています。



ご存じですか？ JVNが2つのDBから構成されていること

- 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）から構成されています。



ご存じですか？ JVN脆弱性対策機械処理基盤

- ＝（JVN＋JVN iPedia）× MyJVN
- ＝（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 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

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

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

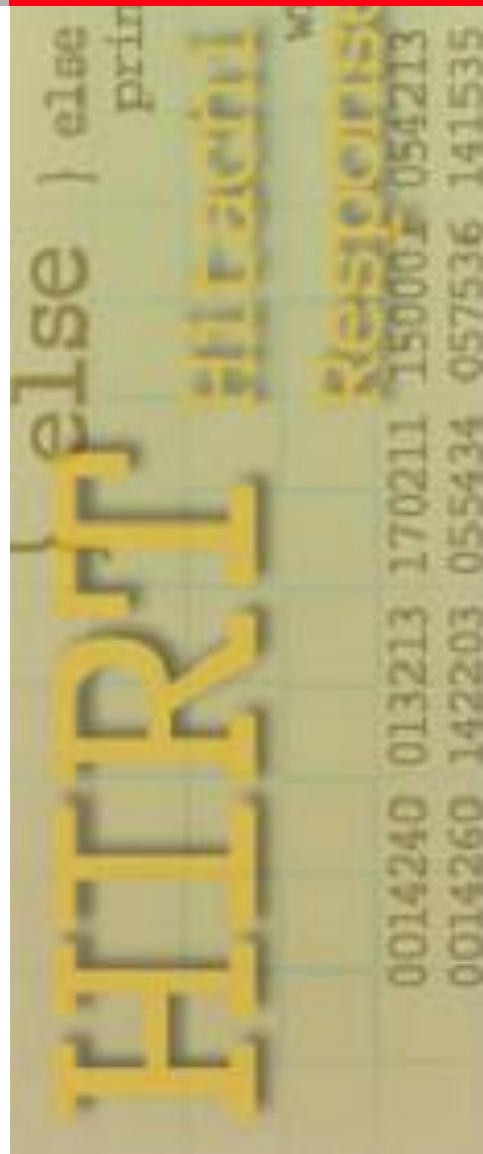
国内で利用されている製品を対象にした脆弱性対策情報を広く蓄積する

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

Contents

HITACHI
Inspire the Next



JVN脆弱性対策機械処理基盤の英語表記は、
JVN Security Content Automation Frameworkです。

JVN脆弱性対策機械処理基盤

＝（JVN＋JVN iPedia）× MyJVN
＝（国際性＋地域性）× 利活用基盤
＝ 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（ワールドワイドに向けた脆弱性対策情報の情報源）と地域性（日本国内に向けた脆弱性対策情報データベース）を両立させたグローバルなJVN（世界に冠たるJVN）の実現

CYBEXの活用

CYBEX：サイバーセキュリティ情報交換フレームワーク

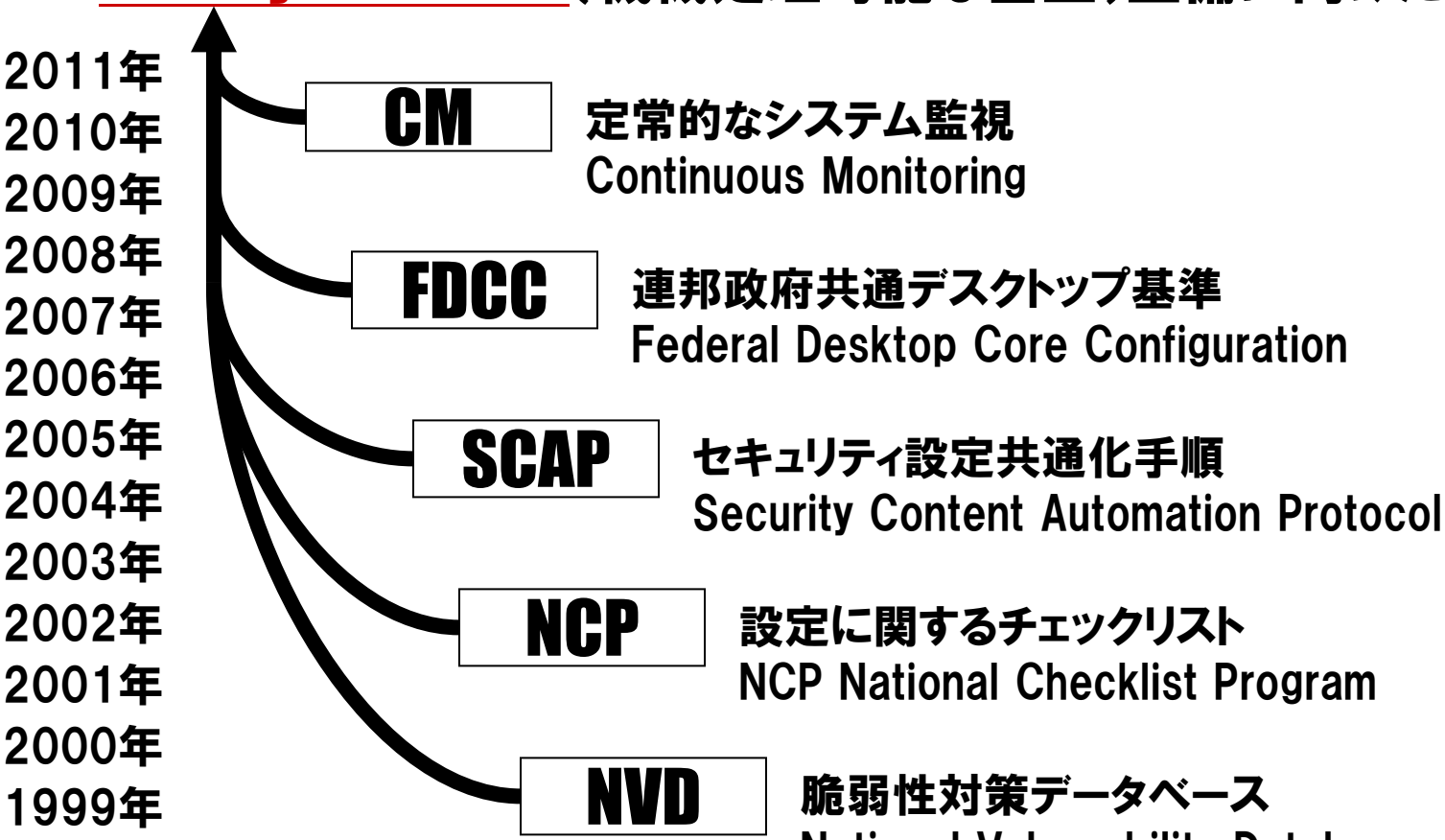
ITU-T Q.4/17:　X.cybex

Global Cybersecurity Information Exchange Framework

- **経緯**
  2009年9月に採択され、X.cybexに関する検討が発足した。X.cybexの背景には、2008年のITU総会決議58（開発途上国におけるCERT構築支援）がある。
- **概要**
  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ため、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。
  脆弱性対策関連（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。

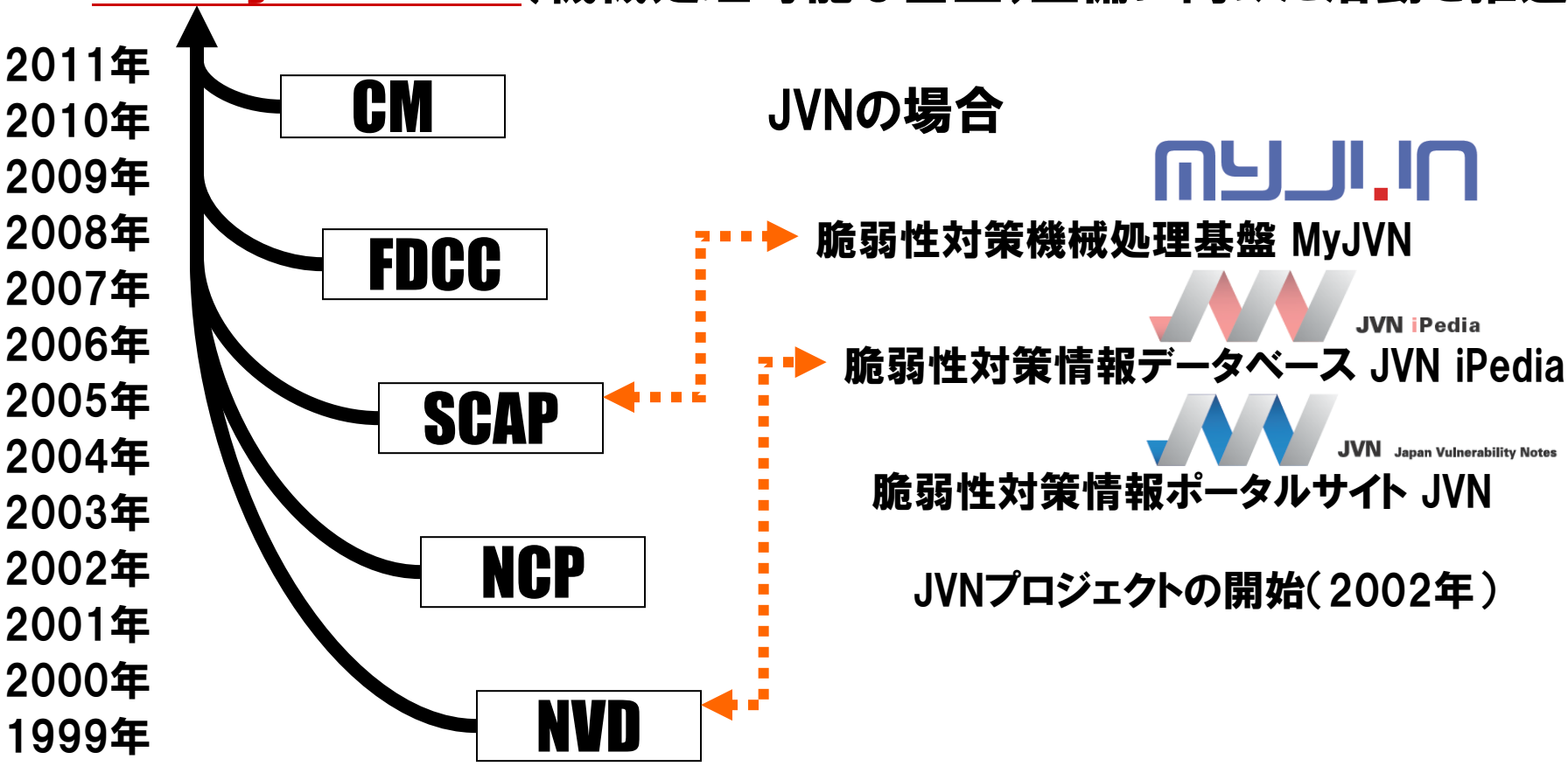
SCAP：セキュリティ設定共通化手順

- 米国：2002年のFISMA（連邦情報セキュリティマネジメント法）以降、Security Automation（機械処理可能な基盤）整備に向けた活動を推進



SCAP：セキュリティ設定共通化手順

- 米国：2002年のFISMA（連邦情報セキュリティマネジメント法）以降、Security Automation（機械処理可能な基盤）整備に向けた活動を推進



利活用基盤整備の取り組み(1)

- (JVN＋JVN iPedia)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(SCAP(CYBEXの仕様群の一部))の導入

第1期 立上げ期

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(慶応義塾大)
	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

第2期 対策情報 充実期

2006年	6月	JVNRSS試行サイトの開設(中央大)
2007年	2月	共通脆弱性評価システム(CVSS)
	3月	MyJVN API 試行サイトの開設(中央大)
	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(2)

- (JVN＋JVN iPedia)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(SCAP(CYBEXの仕様群の一部))の導入

第3期 利活用基盤整備・共通基準仕様導入期

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
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 API 公開
2011年 3月	OVAL準拠認定取得(MyJVN)
8月	評価結果形式(ARF)

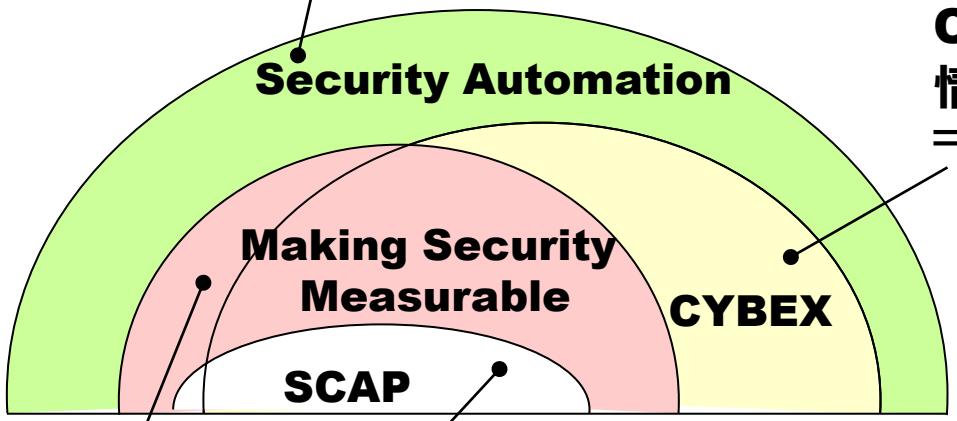
Hitachi Incident Response Team

適用している仕様

名称	概要
CVE(Common Vulnerability and Exposures) 共通脆弱性識別子	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を付与する仕様
CCE(Common Configuration Enumeration) 共通セキュリティ設定一覧	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を付与する仕様
CPE(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、ソフトウェアなどに一意の名称を付与する仕様
CWE(Common Weakness Enumeration) 共通脆弱性タイプ一覧	脆弱性の種類を一意に識別するために、脆弱性タイプの一覧を体系化する仕様
CVSS(Common Vulnerability Scoring System) 共通脆弱性評価システム	脆弱性自体の特性、パッチの提供状況、ユーザ環境での影響度などを考慮し影響度を評価する仕様
OVAL(Open Vulnerability and Assessment Language) セキュリティ検査言語	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仕様
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	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ための仕様
ARF(Assessment Results Format) 評価結果形式	評価結果を記述するための仕様

関連仕様

Security Automation
⇒米NISTがSP800-137 (Information Security Continuous Monitoring for Federal Information Systems and Organizations) で想定する対象の仕様群



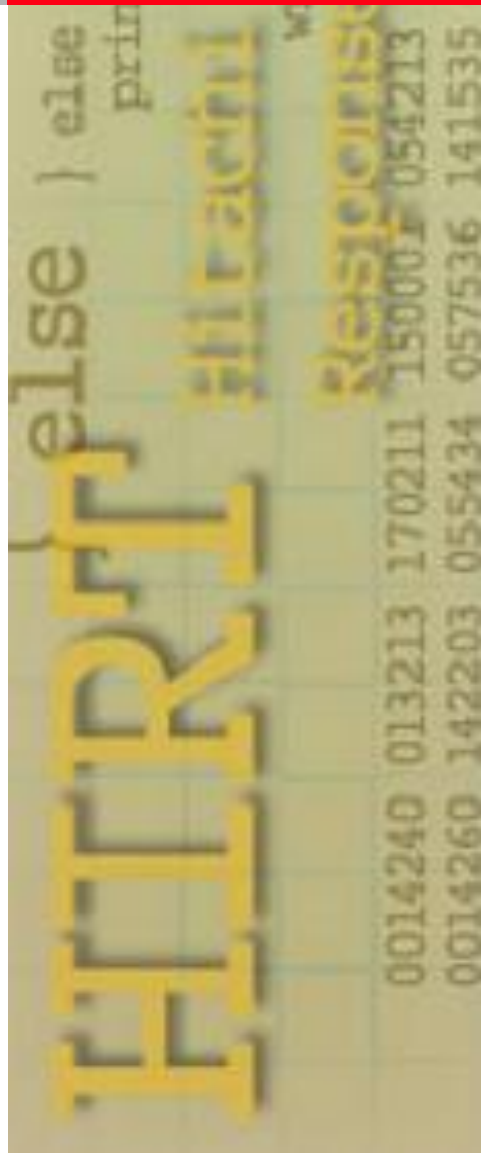
CYBEX (サイバーセキュリティ情報交換フレームワーク)
⇒ITU-Tで規定する仕様群:
CVE, CCE, CPE, CWE, CVSS, OVAL

SCAP (Security Content Automation Protocol: セキュリティ設定共通化手順)
⇒米NISTが連邦政府向けに推進する仕様群 :
CVE, CCE, CPE, CVSS, OVAL, XCCDF

Making Security Measurable
⇒米MITRE社で開発中の仕様群
CVE, CCE, CPE, CWE, CVSS, OVAL, ARF

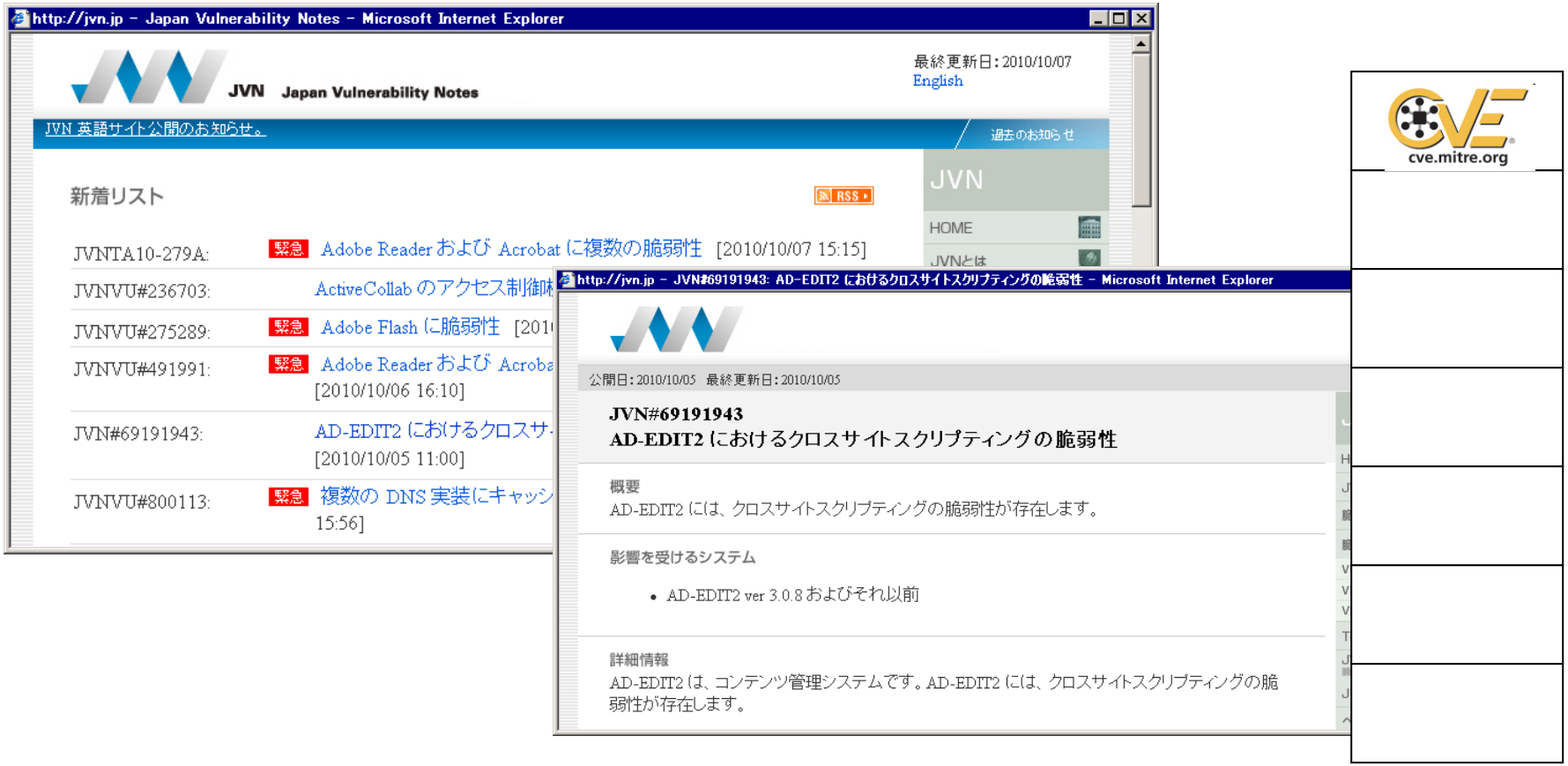
Contents

HITACHI
Inspire the Next



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。



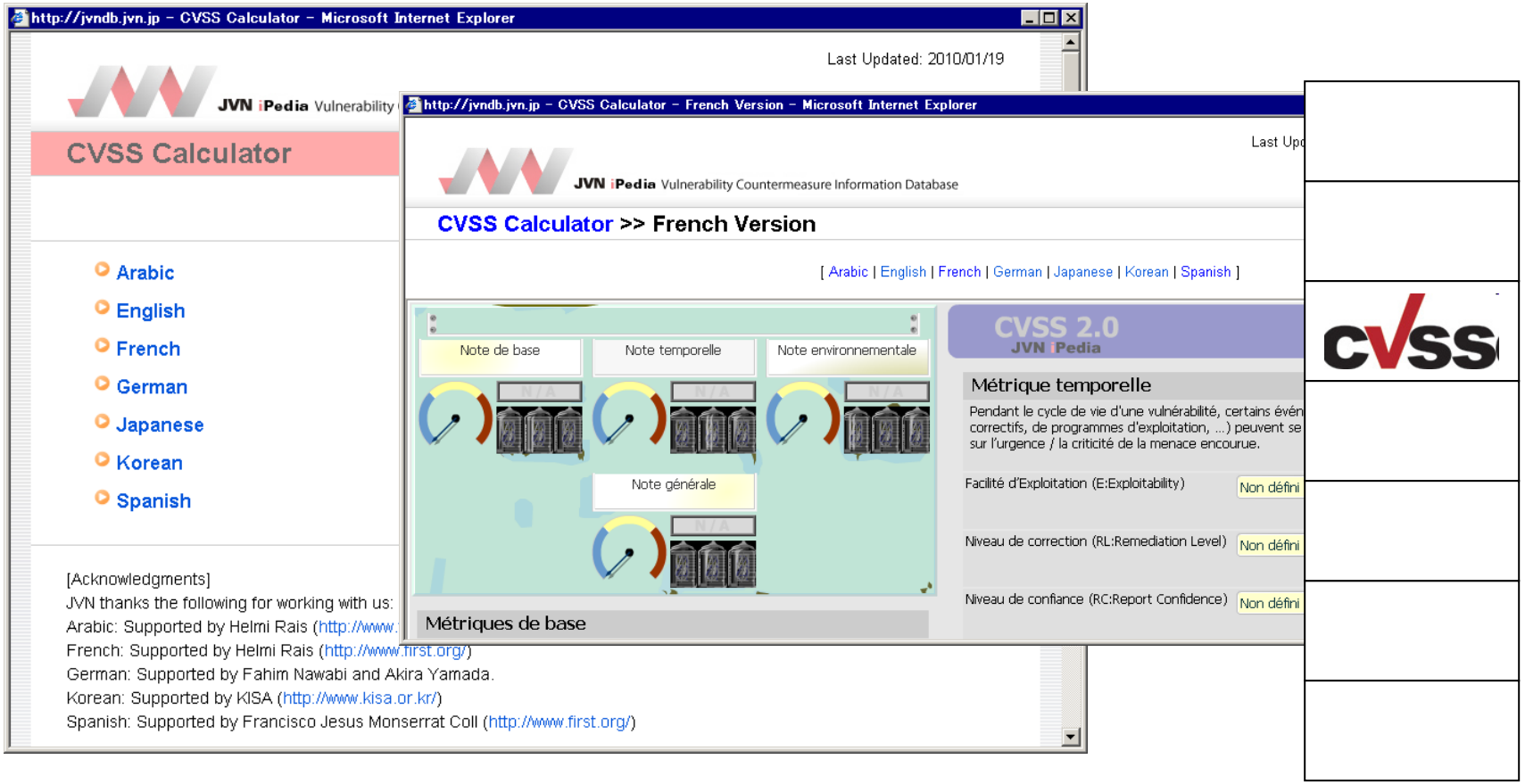
Hitachi Incident Response Team

脆弱性対策情報データベース JVN iPedia

- http://jvndb.jvn.jp/
- 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。

CVSS 計算ソフトウェア多国語版

- http://jvndb.jvn.jp/cvss/
- 脆弱性対策情報の利活用にあたり、CVSSの普及を図る。



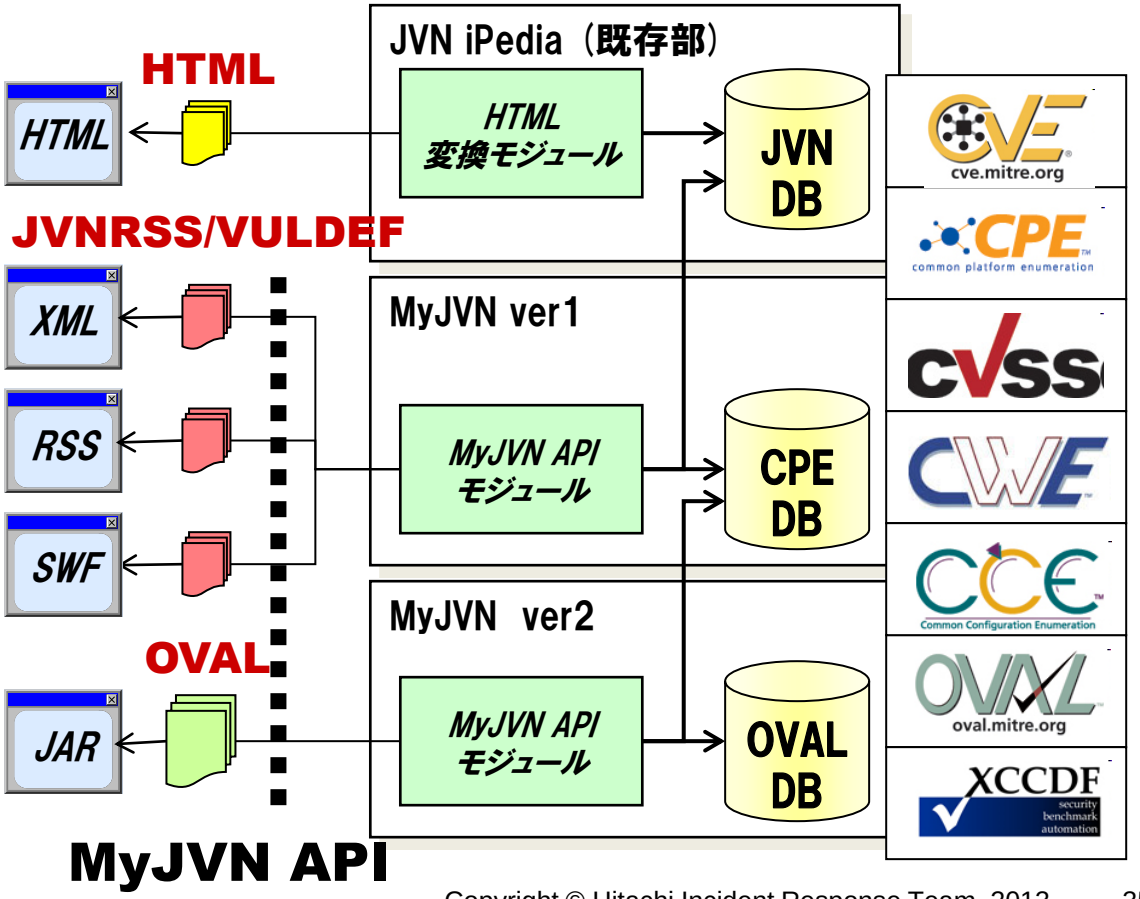
MyJVN API

- 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



JVNにおけるCYBEX利用

Hitachi Incident Response Team

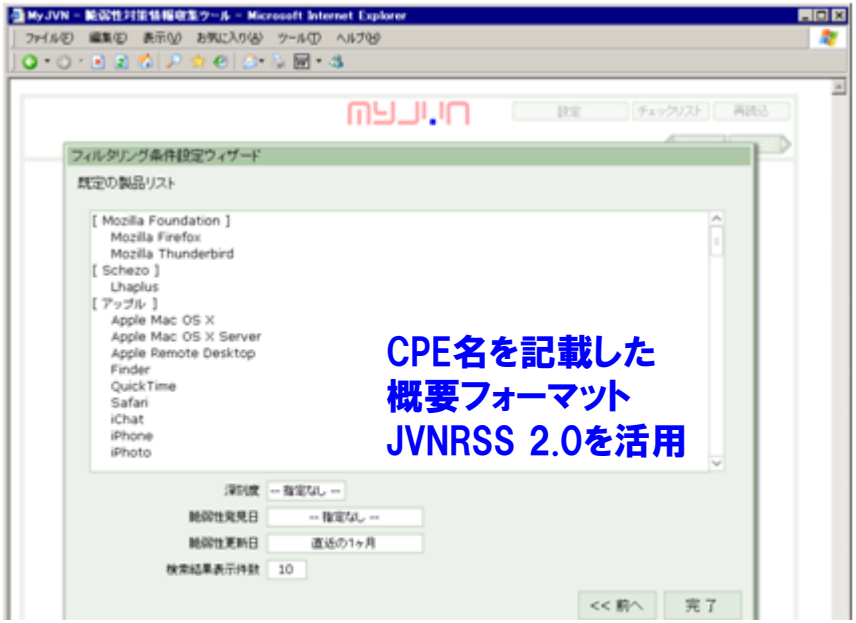
MyJVN API

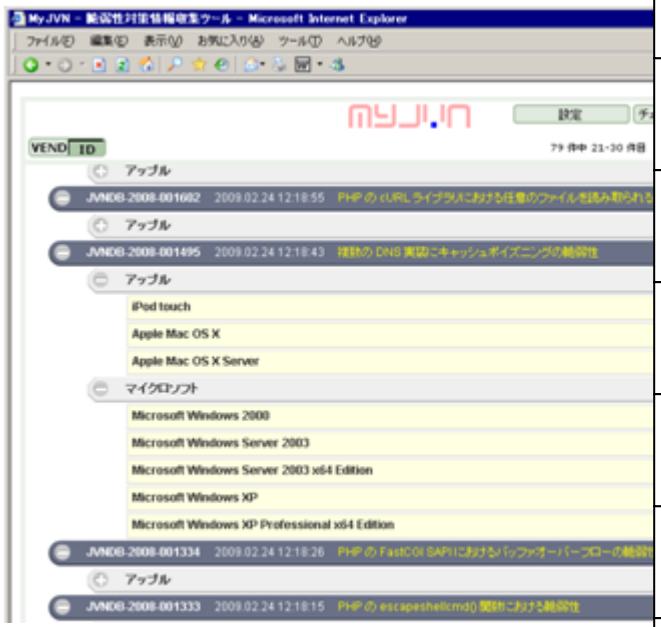
	名称	概要
フィルタリング型情報提供	製品提供者一覧取得 **getVendorList**	フィルタリング条件に当てはまるベンダ名（製品開発者）リストを取得します。
	製品一覧取得 **getProductList**	フィルタリング条件に当てはまる製品名リストを取得します。
	脆弱性対策概要情報一覧取得 **getVulnOverviewList**	フィルタリング条件に当てはまる脆弱性対策の概要情報リストを取得します。
	脆弱性対策詳細情報取得 **getVulnDetailInfo**	フィルタリング条件に当てはまる脆弱性対策の詳細情報を取得します。
検査データ提供	OVAL定義データ一覧の取得 **getOvalList**	フィルタリング条件に当てはまる OVAL 定義データリストを取得します。
	OVAL定義データの取得 **getOvalData**	OVAL 定義データを取得します。
	XCCDFチェックリストデータ一覧の取得 **getXccdfList**	XCCDF チェックリストデータリストを取得します。
	XCCDFチェックリストデータの取得 **getXccdfData**	XCCDF チェックリストデータを取得します。
その他	統計データの取得 **getStatistics**	脆弱性対策情報を、脆弱性統計情報）、CVSS統計情報、CWE統計情報で集計したデータを取得します。
	JVN CPE Dictionary情報の取得 **getCPEDictionary**	JVN CPE Dictionary 情報を取得します。

Hitachi Incident Response Team

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





cve.mitre.org

CPE common platform enumeration

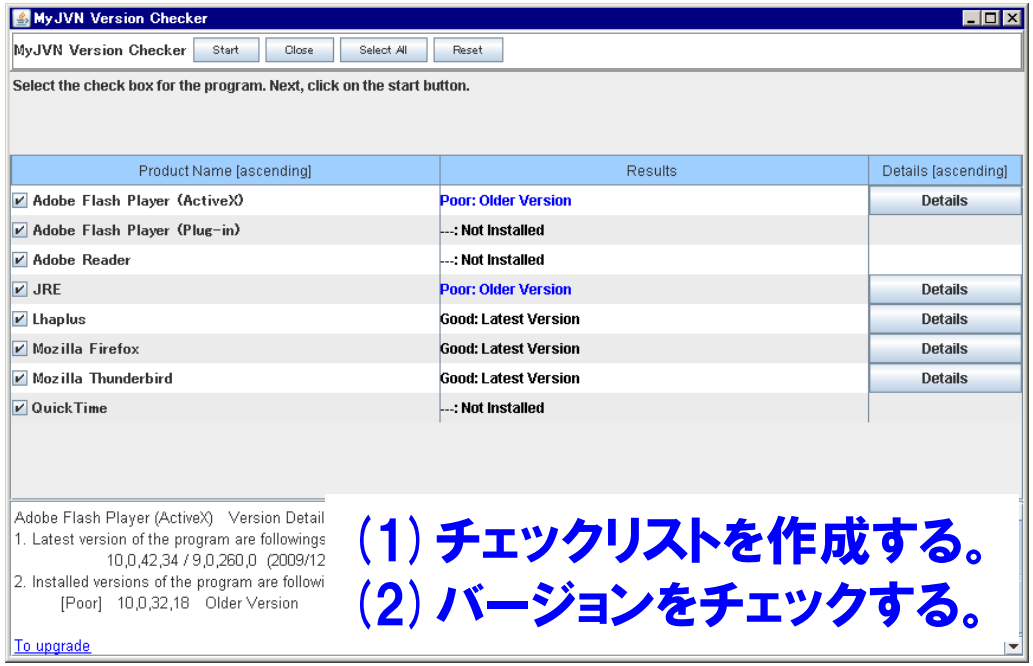
CVSS

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

Hitachi Incident Response Team

MyJVNバージョンチェッカ

- http://jvndb.jvn.jp/apis/myjvn/vccheck.html
- 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

ARF

XCCDF security benchmark automation

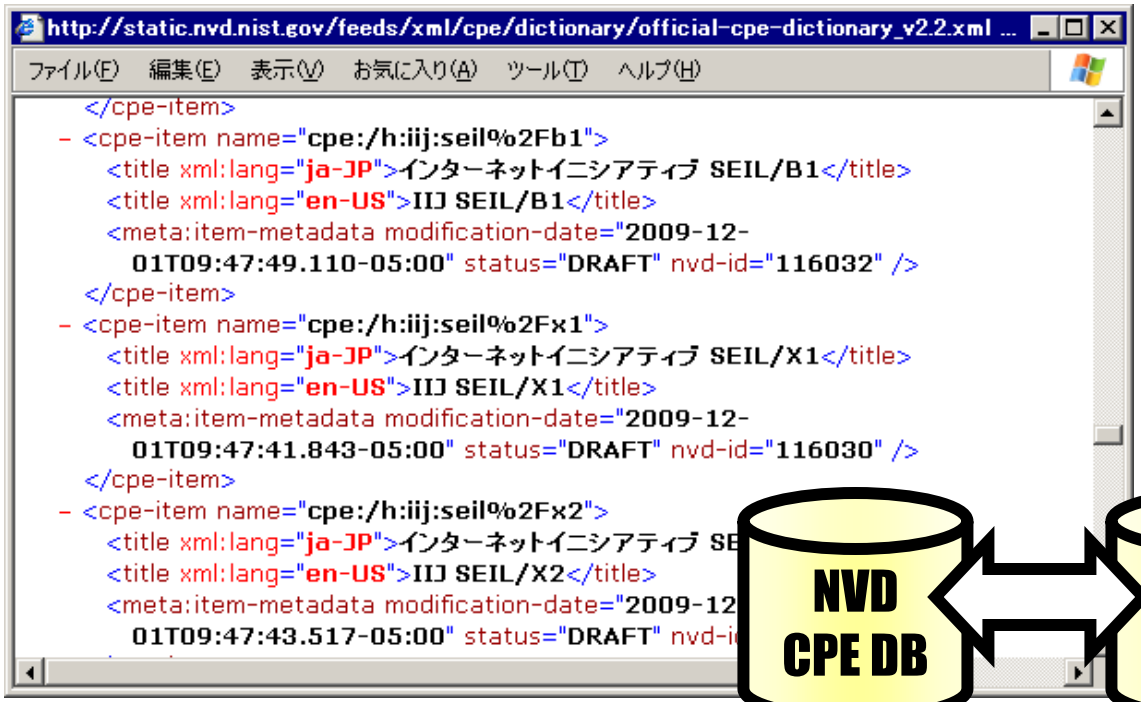
MyJVNセキュリティ設定チェッカ

- http://jvndb.jvn.jp/apis/myjvn/sccheck.html
- 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

ARF

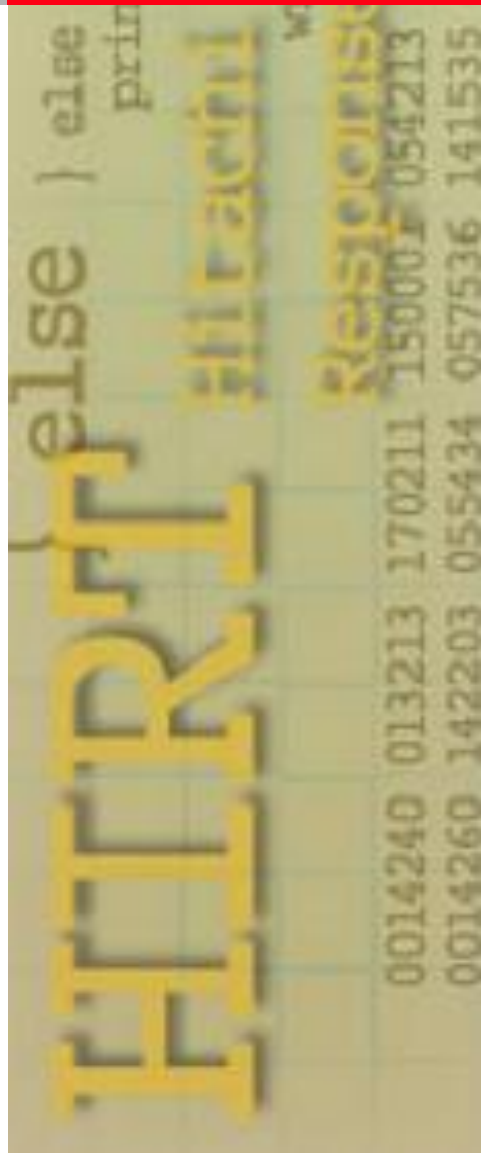
Official CPE Dictionary 連携（試行）

- http://nvd.nist.gov/cpe.cfm
- 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）。



Contents

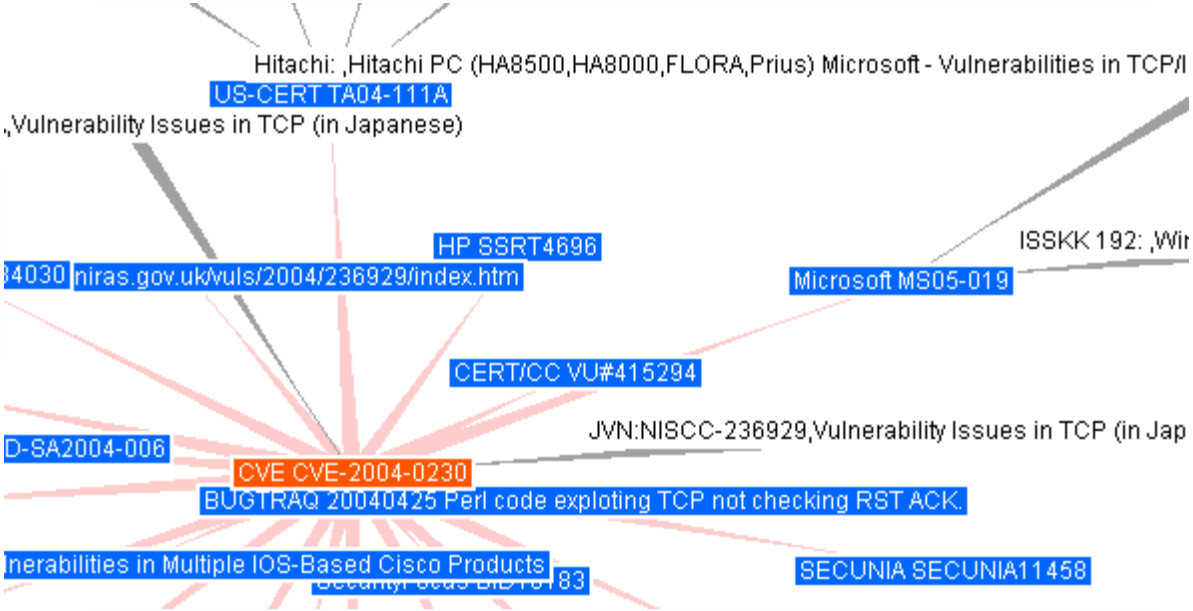
HITACHI
Inspire the Next



CVE：脆弱性を識別する

- http://cve.mitre.org/
- **Common Vulnerability and Exposures：共通脆弱性識別子**
- **コード上のセキュリティ問題に、プログラムで（機械）処理しやすいよう、一意の番号（CVE識別番号）を付与する仕様**
  - **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-2012-0913
［西暦］［連番］



Hitachi Incident Response Team

CPE：製品を識別する

- http://cpe.mitre.org/
- 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

Hitachi Incident Response Team

CVSS：脆弱性の深刻度を評価する

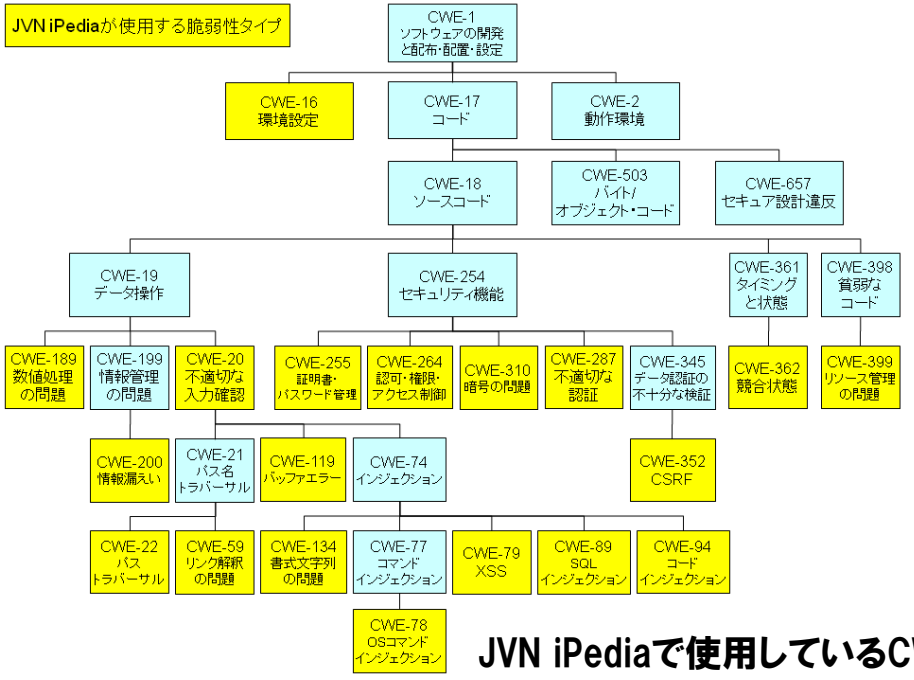
- http://www.first.org/cvss/
- **Common Vulnerability Scoring System：**
  共通脆弱性評価システム
- **脆弱性の技術的な特性＜基本評価＞、脆弱性を取巻く状況＜現状評価＞、利用者環境における問題の大きさ＜環境評価＞を考慮し、プログラムで（機械）処理しやすいよう、深刻度を評価する仕様**

基本評価	脆弱性の技術的な特性を評価 例：システムを乗っ取りが可能な脆弱性⇒深刻度大 システムへの影響が小さく攻撃が難しい脆弱性⇒深刻度小
現状評価	ある時点における脆弱性を取巻く状況を評価 例：脆弱性を悪用する侵害活動が発生している⇒深刻度大 攻撃手法が理論上のみで、正式な対策情報がある⇒深刻度小
環境評価	利用者環境における問題の大きさを評価 例：該当する脆弱性が基幹システムに存在する⇒深刻度大 該当する脆弱性は限られた環境にしか存在しない⇒深刻度小

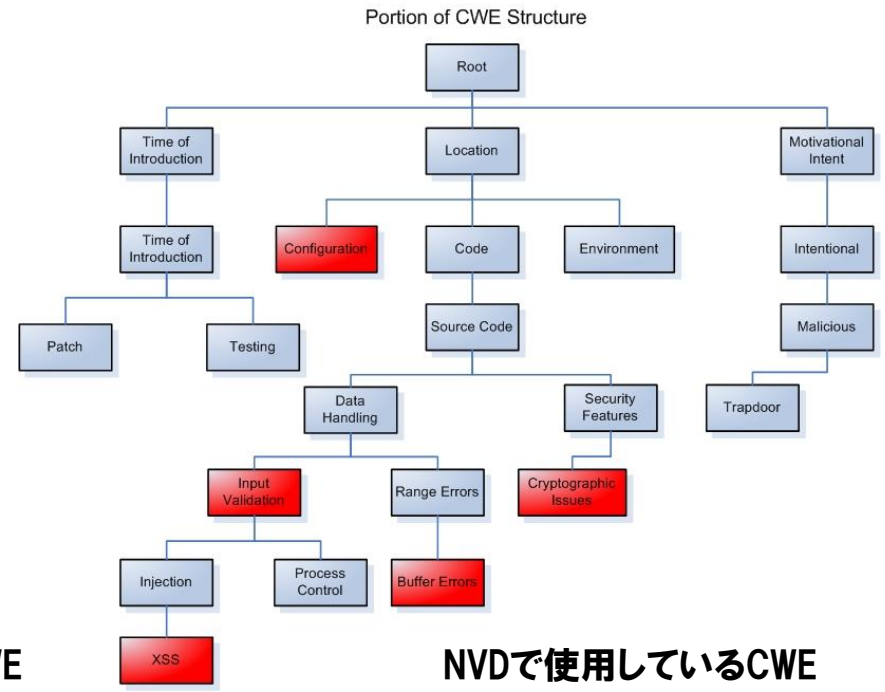
最終的な脆弱性の深刻度（0.0～10.0）

CWE：脆弱性を分類する

- http://cwe.mitre.org/
- Common Weakness Enumeration：共通脆弱性タイプ一覧
- コード上のセキュリティ問題の種類を一意に識別するために、脆弱性タイプの一覧を体系化する仕様
  - CWE-IDを階層構造で体系化



JVN iPediaで使用しているCWE



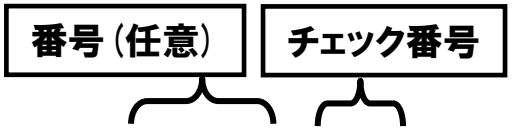
NVDで使用しているCWE

Hitachi Incident Response Team

CCE：設定上の問題を識別する

- http://cce.mitre.org/
- Common Configuration Enumeration：共通セキュリティ設定一覧
- 設定上のセキュリティ問題に、プログラムで（機械）処理しやすいよう、一意の番号（CCE識別番号）を付与する仕様

CCE識別番号の構成



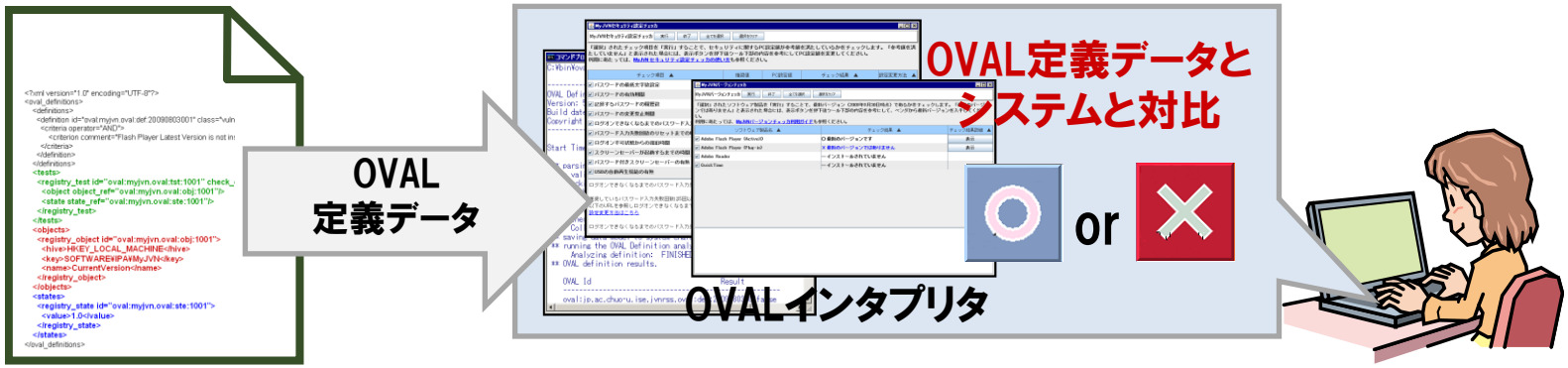
CCE-2981-9

※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/プラットフォーム毎に設定一覧を用意
  AIX 5.3, HP-UX 11.23, Internet Explorer 7/8, Microsoft Exchange 2007/2010, Polycom HDX 3.X, Red Hat Enterprise Linux 4/5, Sun Solaris 8/9/10, Oracle WebLogic Server 11g, Windows 2000/XP/Vista/Server 2003/Server 2008/7
- セキュリティ設定項目の設定推奨値については各種セキュリティ設定ガイドを参照

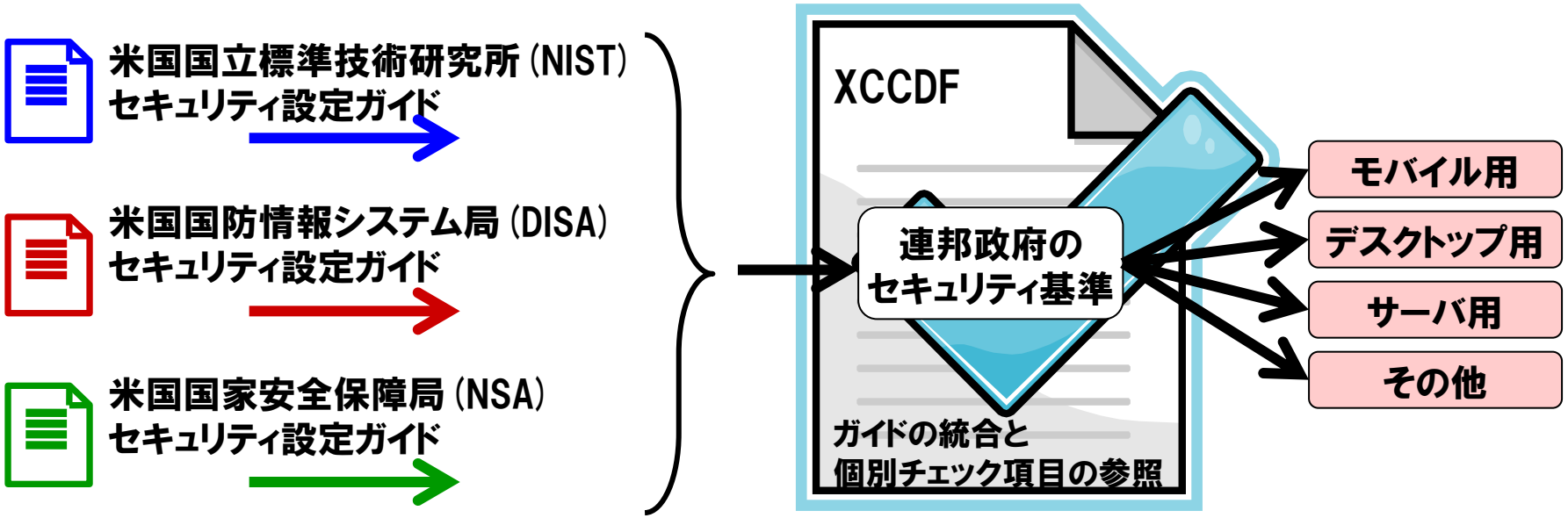
OVAL:チェック方法を記述する

- http://oval.mitre.org/
- **Open Vulnerability and Assessment Language:**
  セキュリティ検査言語
- **コード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に、プログラムで(機械)処理しやすいようXML形式で記述する手続き仕様**
- **OVALを用いたチェックの流れ**
  - **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。**
  - **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。**



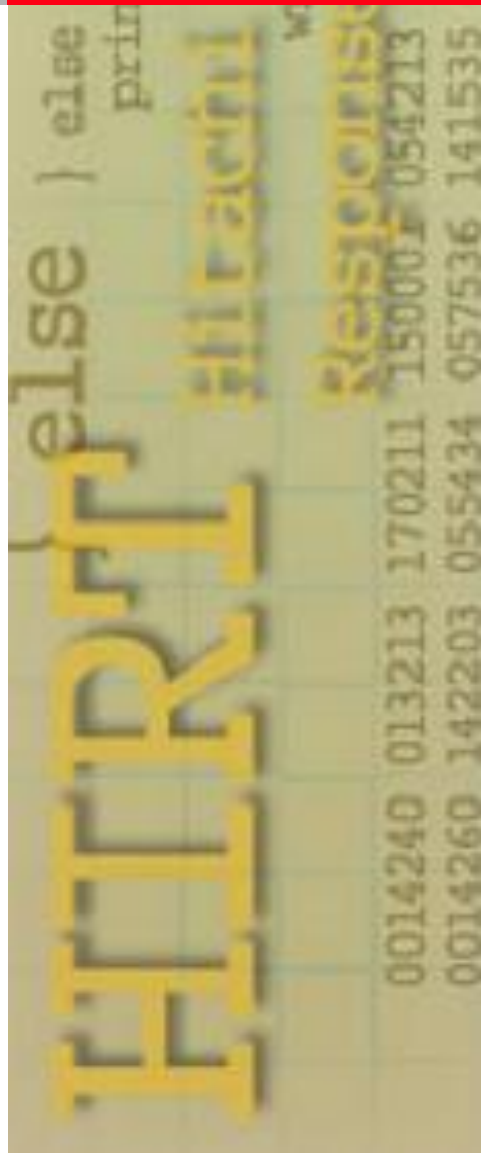
XCCDF：チェックリストを記述する

- http://scap.nist.gov/specifications/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**
- **文書で記載されたセキュリティ設定ガイド、セキュリティチェックリストやベンチマークなどを、プログラムで（機械）処理しやすいXML形式で記述するための仕様**



Contents

HITACHI
Inspire the Next



機械処理基盤の実現に向けて

データベースの連携、その前に、お互いを良く知ろう

- Oct 2012: 8th Annual IT Security Automation Conference
- Nov 2012: Kyoto 2012 FIRST Technical Colloquium
  (Future of Global Vulnerability Reporting Summit)
- Feb 2013: FIRST.org VRDX-SIG
  Vulnerability Reporting and Data eXchange SIG
- Jun 2013: meeting #1

http://www.first.org/global/sigs/vrdx

Ending

HITACHI
Inspire the Next

MyJVN

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

JVN脆弱性対策機械処理基盤（MyJVNフレームワーク）では、共通基準／仕様としてのCYBEXの活用を進めながら、国際性（ワールドワイドに向けた脆弱性対策情報の情報源）と地域性（日本国内に向けた脆弱性対策情報データベース）を両立させたグローバルなJVN（世界に冠たるJVN）の実現が進められています。

HITACHI
Inspire the Next

Thank you

脆弱性対策データベースと
その自動化基盤
～JVN, JVN iPedia and MyJVN～

2013/09/30

寺田真敏
(株)日立製作所
Hitachi Incident Response Team