SAMAC
一般社団法人 IT資産管理評価認定協会

ソフトの脆弱性DBと連携した SAMAC辞書の活用

ＩＴ資産管理評価認定協会
脆弱性データベース検討WG　松村達也
2017年6月9日

脆弱性データベース検討WGのご紹介

組織にとって業務上使用するソフトウェアの種類とその使途は多岐にわたり、その資産管理と安全な利用に向けた、脆弱性情報の掌握・対策の徹底は容易なことではありません。
OpenSSL、Apache Struts といった広く普及しているオープンソースの脆弱性では、自組織のサーバーでの使用有無などの影響判定が困難であったため、対策の徹底を一層難しくしました。

これを受け組織が使用する**ソフトウェアの管理と安全な使用の一元的な管理を実現可能にするため、IPAのJVN iPedia が持つ脆弱性対策情報と SAMAC が持つ"ソフトウェア辞書"とのデータ連携**について検討に着手しました。データ連携にあたっては各々のデータベースが保有するソフトウェアの表記が異なる場合があることから、共通プラットフォーム一覧（CPE）を使った紐付けテーブルを新たに作成します。
これが実現すると、ソフトウェア管理に脆弱性（対策）情報が紐付くため、組織で使用しているソフトウェアの脆弱性対策が効率・効果的に実行可能となります。**本WGではデータ連携による新たな価値を広めていき、普及させていくことを目的として活動を行います。**

脆弱性データベース検討WGのご紹介

ソフトウェアの脆弱性データベースとSAMAC辞書

プレス発表　組織で使用するソフトウェアの脆弱性対策の効率・効果的な徹底に向けた調査報告書を公開

～JVN iPedia(*1)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～

2016年3月9日
独立行政法人情報処理推進機構
一般社団法人ソフトウェア資産管理評価認定協会

IPA（独立行政法人情報処理推進機構、理事長：富田 達夫）は、組織で使用するソフトウェアの脆弱性対策の効率・効果的な徹底を目指した「ソフトウェア識別管理に向けた分析事業」報告書を3月9日（水）に公開しました。これをうけ、一般社団法人ソフトウェア資産管理評価認定協会（理事長：高橋 快昇　以後、SAMAC(*2)）は2016年4月以降、脆弱性対策情報とソフトウェア資産管理のデータ連携に向けた紐付けテーブルの作成に着手します。

URL：http://www.ipa.go.jp/sec/reports/20160309.html

ソフトウェアは今やパソコン、スマホだけなく、家電、自動車などあらゆる機器に組み込まれ、便利な機能の実現や、新たな価値を生み出しています。その一方でソフトウェアに潜む脆弱性は、組み込まれた製品を意図せぬ攻撃の標的にし、利用者にもその影響を及ぼします。また、その攻撃では多くの場合、ソフトウェアの脆弱性が悪用されています。

～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

SAMAC
一般社団法人 IT資産管理評価認定協会

脆弱性データベース検討WGメンバー一覧

所属組織	氏名
エムオーテックス株式会社	松村　達也（リーダー）
NECキャピタルソリューション株式会社	森田　聡子
株式会社クロスビート	小野　美由紀
独立行政法人 情報処理推進機構	寺田　真敏
SoftwareONE Japan株式会社	荒巻　智之
株式会社ディー・オー・エス	嶋野　至剛
日本マイクロソフト株式会社	手島　伸行
富士通株式会社	髙橋　快昇

脆弱性ってなんだろう？

SAMAC
一般社団法人 IT資産管理評価認定協会

最近、脆弱性という言葉を耳にしませんか？

- Adobe Flash Playerの脆弱性が多数報告され話題に。他にも・・・

SQLインジェクションの脆弱性を突かれて情報漏えい！！
（菓子販売メーカーにて21万件情報漏えい）

OSコマンドインジェクションの脆弱性を突かれて不正アクセス！！
（民放テレビ会社にて43万件情報漏えい）

新聞から

ウェブニュースから

脆弱性、、、なんだろう…？

SAMAC
一般社団法人IT資産管理評価認定協会

最近、脆弱性という言葉を耳にしませんか？

- Adobe Flash Playerの脆弱性が多数報告され話題に。他にも・・・

SQLインジェクションの脆弱性を突かれて情報漏えい！！
（菓子販売メーカーにて21万件情報漏えい）

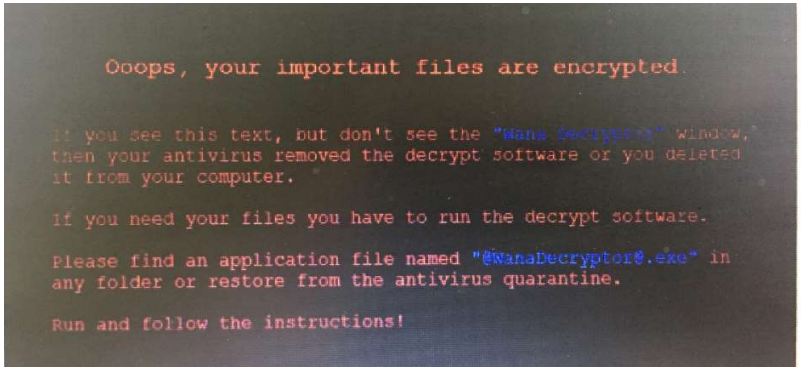
OSコマンドインジェクションの脆弱性を突かれて不正アクセス！！
（民放テレビ会社にて43万件情報漏えい）

新聞から

ウェブニュースから

今年流行りのWannaCryとは？

世界100カ国以上を狙ったランサムウェア



- 政府機関、病院、通信会社、自動車会社など被害が確認されている。
- 感染をするとOfficeファイルを暗号化して、復号するためには金銭（仮想通貨ビットコイン）を要求
- 感染した端末は、Windowsの脆弱性を突いてリモートコード実行し周囲の端末へ感染を拡大
- 当該の脆弱性は、Shadow Brokers ハッカー集団が今年4月に米国のNSAから窃取したとされるハッキングツール や攻撃コードに含まれていた脆弱性の1つ

過去最大級のインシデント

数日で150ヵ国、30万台以上で感染を確認

テレフォニカで保有PCの85%が感染

NHA（国立病院）で48団体に感染。手術中止、患者受け入の混乱

内務省のPCが感染

フランクフルト駅の電光掲示板に感染メッセージ

ペトロチャイナのガソリンスタンド給油機が感染

ルノー自動車工場で感染。ラインが一時Stop

過去最大級のインシデント

日本でも様々な業種で感染が報告されています

- **鉄道会社の端末で感染**
- **大手製造業で感染、一時メール利用不可**
- **樹脂メーカーでXP端末が感染**
- **水道局　１台で現象感染**
- **鉄道会社　本社１台で感染**
- **個人利用端末でも複数台の感染を確認。**
- **その他　スーパーのモニタやゲーム端末、個人PCで感染**

セキュリティパッチでの対応について

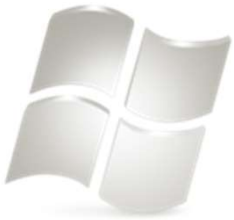
今回の攻撃はマイクロソフト製品の脆弱性（MS17-010）を利用しているため、2017年3月に公開されているセキュリティパッチを適用すれば感染しないと言われており、最優先でセキュリティパッチの適用を行う事が推奨されています。

マイクロソフト社は今回の被害の大きさ、影響度から3年前にサポート期限が切れているWindows XPなどのサポート期限切れOSに対してもセキュリティパッチ（KB4012598）をリリースするという異例の対応を行っています。

また、セキュリティパッチの適用が何らかの理由で出来ない場合の対応として、マイクロソフト社は「SMB v1」を無効化することを案内しています。

セキュリティパッチでの対応について

〇セキュリティパッチ情報



・マイクロソフト セキュリティ情報 MS17-010 - 緊急
https://technet.microsoft.com/ja-jp/library/security/ms17-010.aspx

・サポート切れOS向けのセキュリティパッチ(KB4012598)情報
http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598

〇ランサムウェア WannaCrypt 攻撃に関するお客様ガイダンス

https://blogs.technet.microsoft.com/jpsecurity/2017/05/14/ransomware-wannacrypt-customer-guidance/?wt.mc_id=AID528471_EML_5066212

脆弱性とは・・・

ウイルス対策と脆弱性対策は、同じではありません。
なぜなら、脆弱性は、鍵穴の劣化、鍵そのものの”弱さ”だからです。これは、鍵が付いていない、鍵をかけていないのと同じことです。

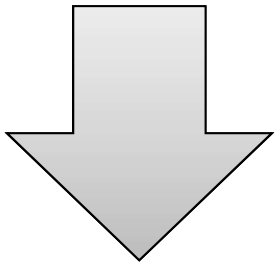
【脆弱性】
鍵穴の劣化、鍵そのものの弱さ

【ウイルス対策】
警備員

いくら、警備員を配置(ウイルス対策ソフトを導入)しても、警備員がよそ見するなどの隙を利用すれば、脆弱性を利用して侵入できてしまいます。

脆弱性とは・・・

- **脆弱性の定義**
  脆弱性とは、ソフトウェア製品やウェブアプリケーション等において、コンピュータ不正アクセスやコンピュータウイルス等の攻撃により、その機能や性能を損なう原因となり得るセキュリティ上の問題箇所(出典：情報セキュリティ早期警戒パートナーシップガイドライン)

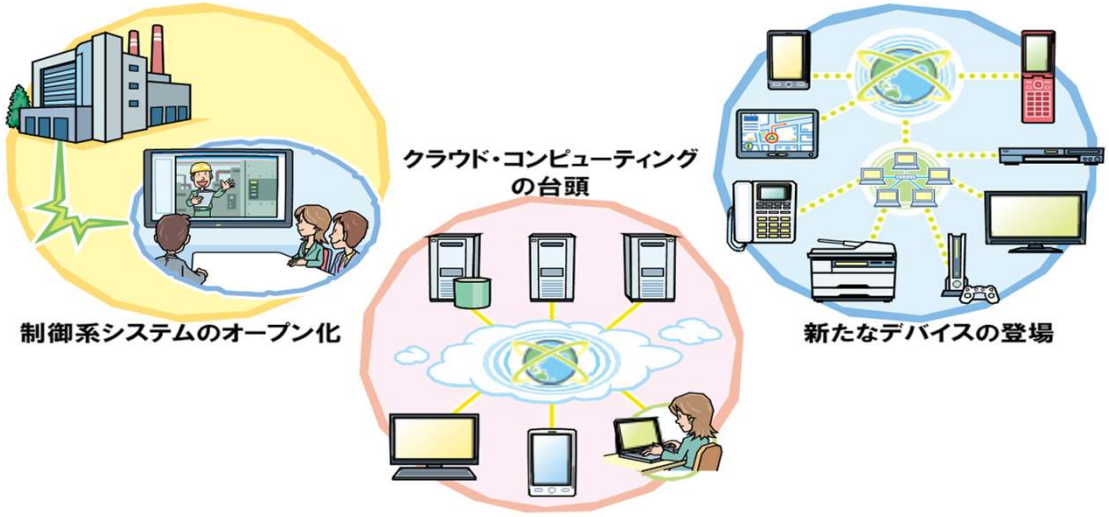


言い換えれば

- **攻撃によりシステムが攻略される可能性**
- **セキュリティ被害をもたらす危険要素**
- **攻撃を受ければ被害、受けなければ無害**

脆弱性を取り巻く環境の変化～様々な分野に広がっていく脆弱性～

- デバイスのスマート化、制御系のオープン化により、新たな分野で、新たな脆弱性が発見され続けている。



- 情報システム脅威：情報窃取、破壊、妨害
- メディカルデバイスの脅威：身体への影響懸念
- 制御系システムの脅威：社会インフラへの影響

脆弱性を取り巻く脅威・危険性～情報セキュリティ10大脅威2017～

- 2016年において社会的影響が大きかったセキュリティ上の脅威について、1位から10位に順位付けして解説した資料

【2位】ランサムウェアを使った詐欺・恐喝
脆弱性を悪用してPCに感染した後ファイルを暗号化

【6位】ウェブサイトの改ざん
脆弱性を悪用して改ざん

【9位】攻撃のビジネス化（アンダーグラウンドサービス）
購入したサービスやツールで脆弱性を悪用した攻撃

ソフトウェアの脆弱性に関する届け出状況

- 2016年度 第4四半期 のソフトウェア製品の脆弱性関連情報に関する届出件数は138件（表1-1）となりウェブサイトに関する届出を上回るペースで年々増加。
- 年度ごとの届出件数合計（図1-2）では 2016年度 のソフトウェア製品の脆弱性関連の届出が 1,045件にも増加していることがわかる。
- 脆弱性対策にはシステム、ソフトウェア資産、データに関するセキュリティリスクの管理（リソース把握・管理）の必要性が益々高まっていることが再認識された。

表1-1．届出件数

分類	今四半期件数	累計
ソフトウェア製品	138 件	3,433 件
ウェブサイト	104 件	9,483 件
合計	242 件	12,916 件

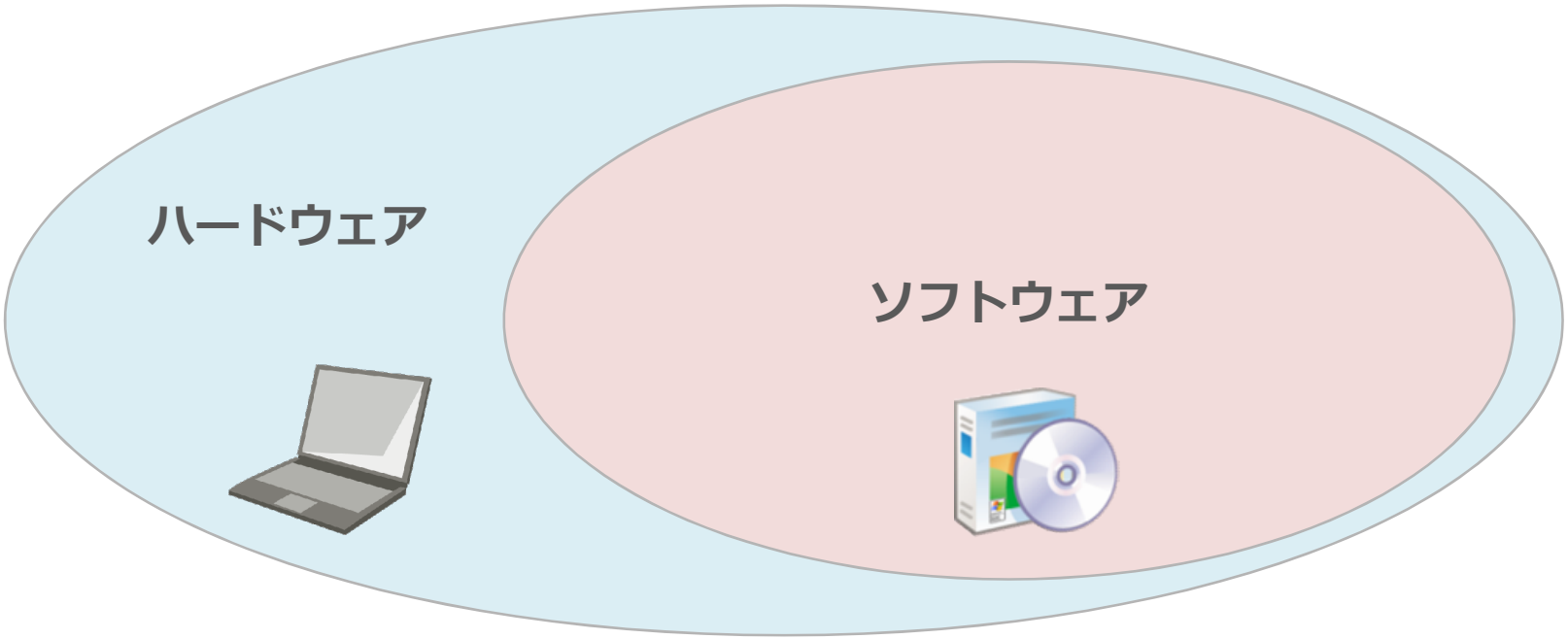
図1-2. 脆弱性関連情報の届出件数の年ごとの推移

出典: IPA 情報処理推進機構 ホームページ
https://www.ipa.go.jp/security/vuln/report/vuln2016q4.html

SAMAC
一般社団法人 IT資産管理評価認定協会

脆弱性対策

- PCやサーバーなど端末の把握が第一に必要で、次にソフトウェアの把握。



パッチが公開されても、端末が把握できていなければ、抜け漏れが発生してしまう。

脆弱性対策

- 脆弱性を放置すると自組織に重大な被害が発生する危険性は大きくなる。

脆弱性(彼)と対策のための関連情報を知っておくことが
適切な対応につながる。

情報収集に役立つキーワードについて知ろう

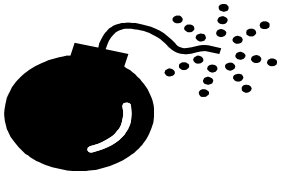
SAMAC
一般社団法人 IT資産管理評価認定協会

脆弱性関連情報の収集～脆弱性と攻撃の関係～

- 脆弱性を構成する要素(脆弱性関連情報)

＜攻撃方法＞
脆弱性を悪用するプログラムや
それらの使い方

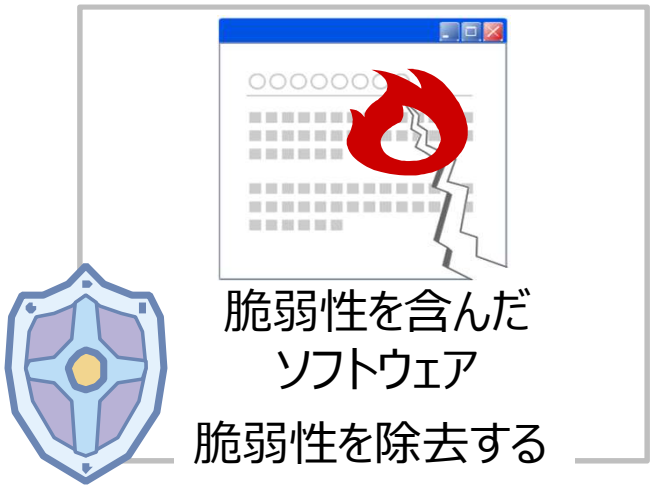
＜脆弱性情報＞
脆弱性の性質及び特徴を示す情報



攻撃コード
(Exploit)

脆弱性を攻撃する

＜検証方法＞
脆弱性が存在することを
調べるための方法



脆弱性を含んだ
ソフトウェア

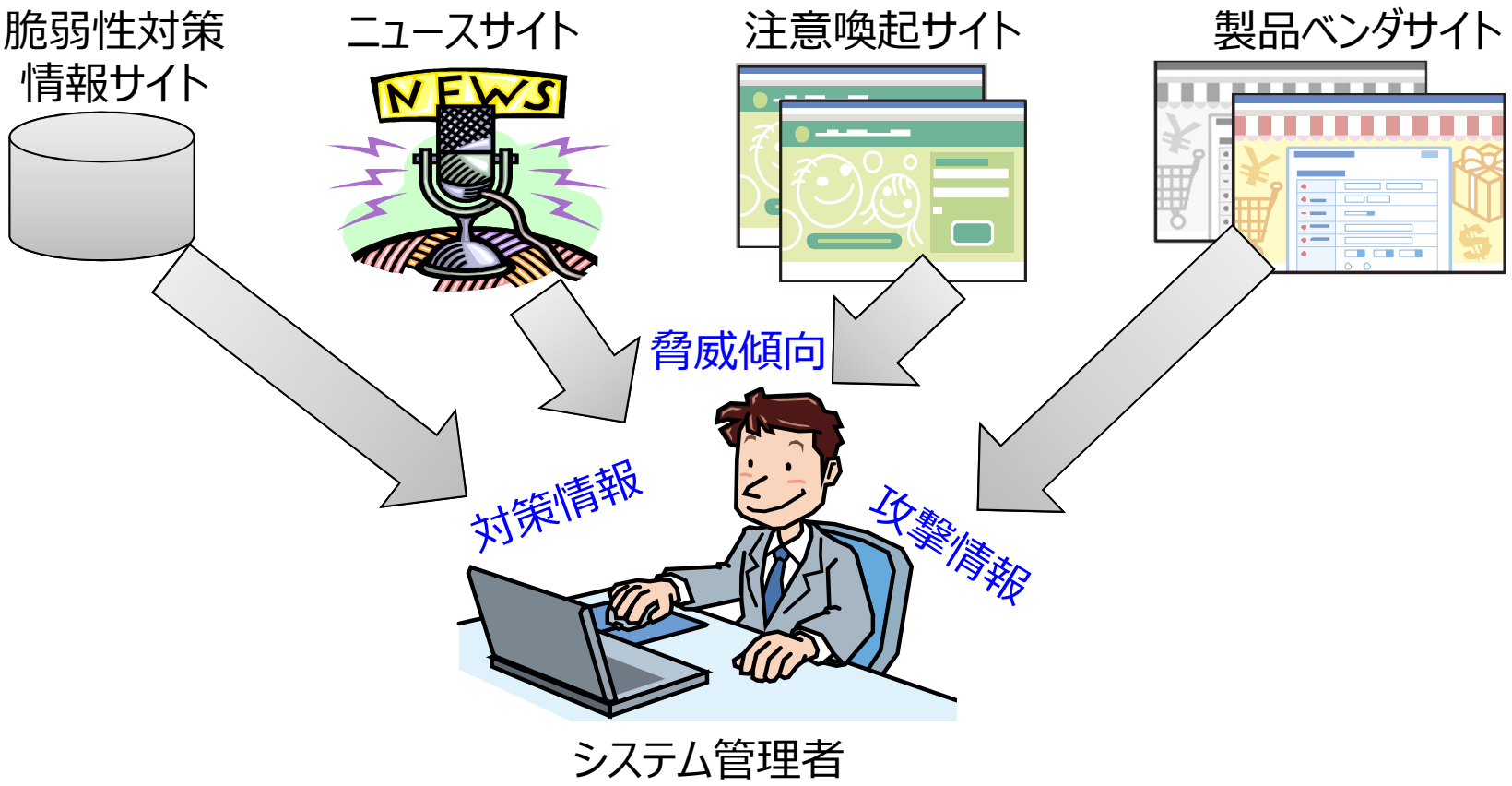
脆弱性を除去する

対策情報/プログラム

＜対策方法＞
脆弱性から生じる問題を
回避するまたは解決を図る方法

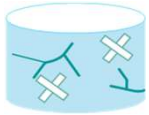
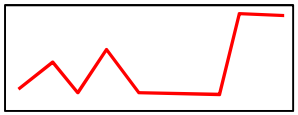
脆弱性関連情報の収集～外部の情報を収集し、自組織の対策に役立てる～

- 脆弱性関連情報の収集とは?
  脆弱性対策の判断要素となる情報を収集すること



脆弱性関連情報の収集～対策判断の為に、どのような情報を掴めば良いのか?～

- 情報種別と対策の考え方
  迅速に対策を実施する為に判断材料となる情報を収集

対象情報	情報の意味合い	活用例
脆弱性対策情報 	被害を受けるポテンシャル	●脆弱性の深刻度の調査 ●当該製品の脆弱性対策
攻撃情報 	実施・発生している事象	●自組織の対策状況のチェック ●攻撃有無のチェック
脅威傾向 	攻撃者の狙い・傾向	●中期的なセキュリティ対策の立案

脆弱性関連情報の収集～効率的に進める為に有効なキーワード～

- 脆弱性対策情報、注意喚起、ニュース記事等でも使用されているキーワード

・・・脆弱性を一意に識別する番号

・・・脆弱性の影響度を評価する指標

・・・脆弱性の種別を体系的に分類

・・・製品を一意に識別する仕様

CVE～脆弱性を一意に識別する番号～

- Common Vulnerabilities and Exposures
(共通脆弱性識別子)
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)を付与して管理

cve.mitre.org

CVE識別番号の構成

西暦	連番

CVE-2016-1000
CVE-2016-10000
CVE-2016-100000
CVE-2016-1000000

公表されている脆弱性に割り当てられた識別番号で、
脆弱性を一意に特定することを可能となる

CVSS～脆弱性の影響度を評価する指標～

- Common Vulnerability Scoring System
  (共通脆弱性評価システム)
  脆弱性の深刻度を0.0～10.0のスコアで評価

CVE#	Component	Protocol	Package and/or Privilege Required	Remote Exploit without Auth.?	CVSS VERSION 2.0 RISK (see Risk Matrix Definitions)							Supported Versions Affected	Notes
					Base Score	Access Vector	Access Complexity	Authen-tication	Confiden-tiality	Integrity	Avail-ability		
CVE-2016-0451	Oracle GoldenGate	Oracle Golden Gate	None	Yes	10.0	Network	Low	None	Complete	Complete	Complete	11.2, 12.1.2	See Note 1
CVE-2016-0452	Oracle GoldenGate	Oracle Golden			10.0	Network	Low	None	Complete	Complete	Complete	11.2, 12.1.2	See Note 1
CVE-2016-0450			None	Yes	5.0	Network	Low	None	None	None	Partial+	11.2, 12.1.2	

CVSS値

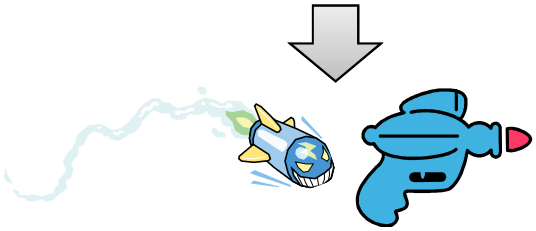
CVE番号

出典：http://www.oracle.com/technetwork/topics/security/cpujan2016-2367955.html

CVSS～脆弱性の影響度を評価する指標～

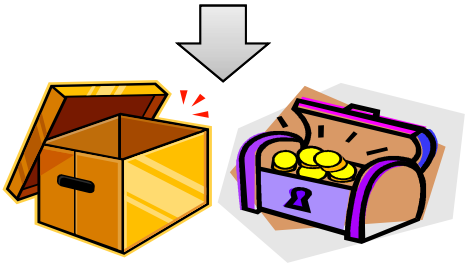
- 攻撃状況やシステムの重要度を加味した
  脆弱性の深刻度を表す評価

＝ 「技術的な特性」 × 「脅威の大きさ」 × 「情報資産の価値」
＝ 「基本評価基準」 × 「現状評価基準」 × 「環境評価基準」



何が引き起こされるのか?

既に攻撃されている?
対策パッチは出ている?



システムの重要度は?

「バッファオーバフロー」×「攻撃観測なし」×「内部システム」
＝深刻度 低

「クロスサイトスクリプティング」×「攻撃観測あり」×「外部システム」
＝深刻度 高

CWE～脆弱性の種別を体系的に分類～

- Common Weakness Enumeration
(共通脆弱性タイプ一覧)
脆弱性を種別毎に分類

ID	概要
CWE-16	環境設定
CWE-20	不適切な入力確認
CWE-22	パス・トラバーサル
CWE-59	リンク解釈の問題
CWE-78	OSコマンドインジェクション
CWE-79	クロスサイトスクリプティング
CWE-89	SQLインジェクション
CWE-94	コード・インジェクション
CWE-119	バッファエラー
CWE-134	書式文字列の問題

ID	概要
CWE-189	数値処理の問題
CWE-200	情報漏えい
CWE-255	証明書・パスワードの管理
CWE-264	認可・権限・アクセス制御
CWE-287	不適切な認証
CWE-310	暗号の問題
CWE-352	クロスサイトリクエスト フォージェリ
CWE-362	競合状態
CWE-399	リソース管理の問題

CPE～製品を一意に識別する仕様～

- 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}:{製品}:{バージョン}
:{アップデート}:{エディション}:{言語}

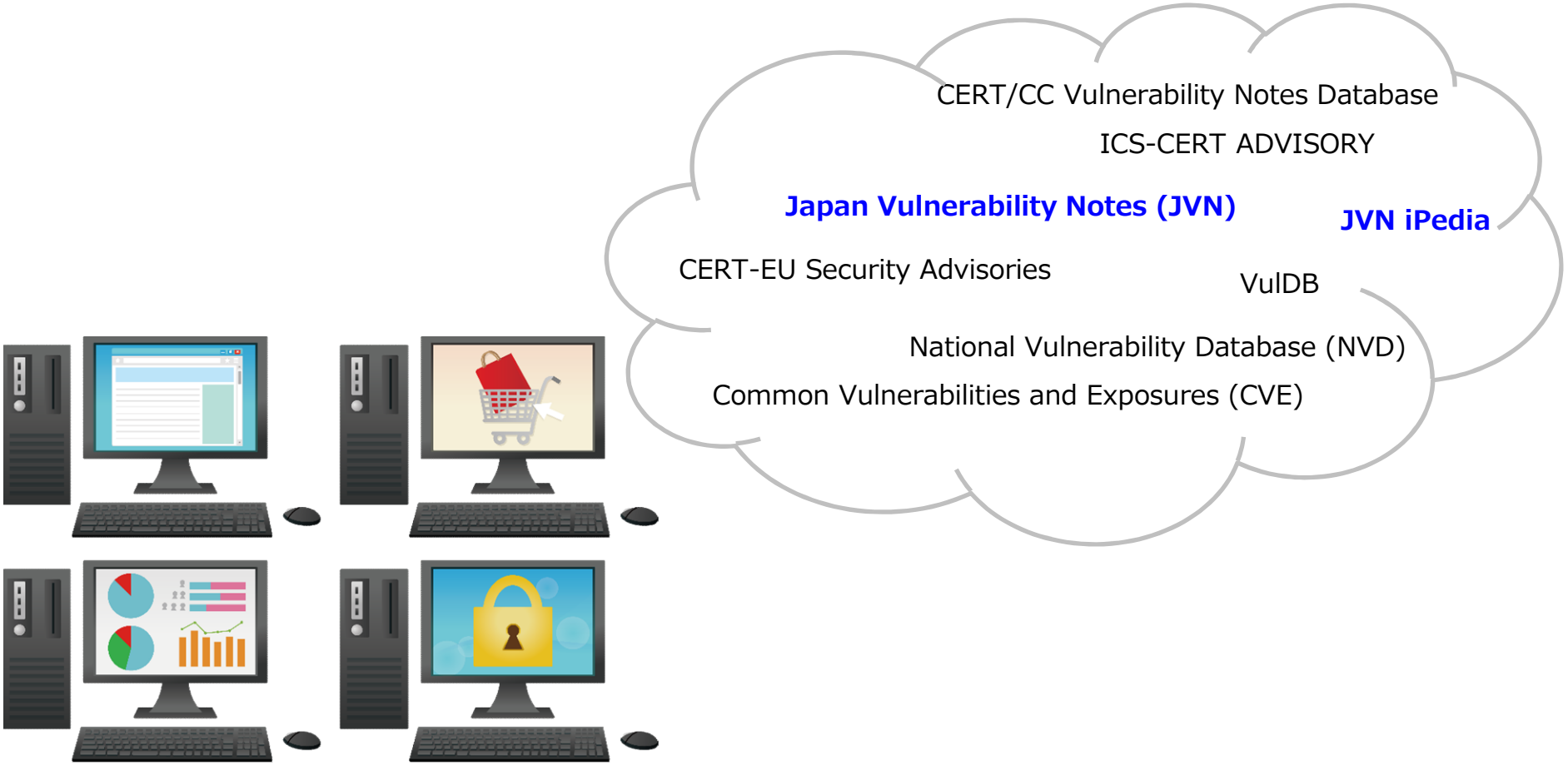
種別：h=ハードウェア、o=OS、a=アプリケーション

脆弱性対策情報データベース 国内の状況は・・・

SAMAC
一般社団法人 IT資産管理評価認定協会

脆弱性対策情報サイトとは

- **脆弱性対策情報データベース、脆弱性データベースと呼ばれている。**
  脆弱性そのもの特性、影響を受ける製品、攻撃コード、対策情報などを調べたいときの情報源となる。



SAMAC
一般社団法人 IT資産管理評価認定協会

脆弱性対策情報サイト ～JVN～

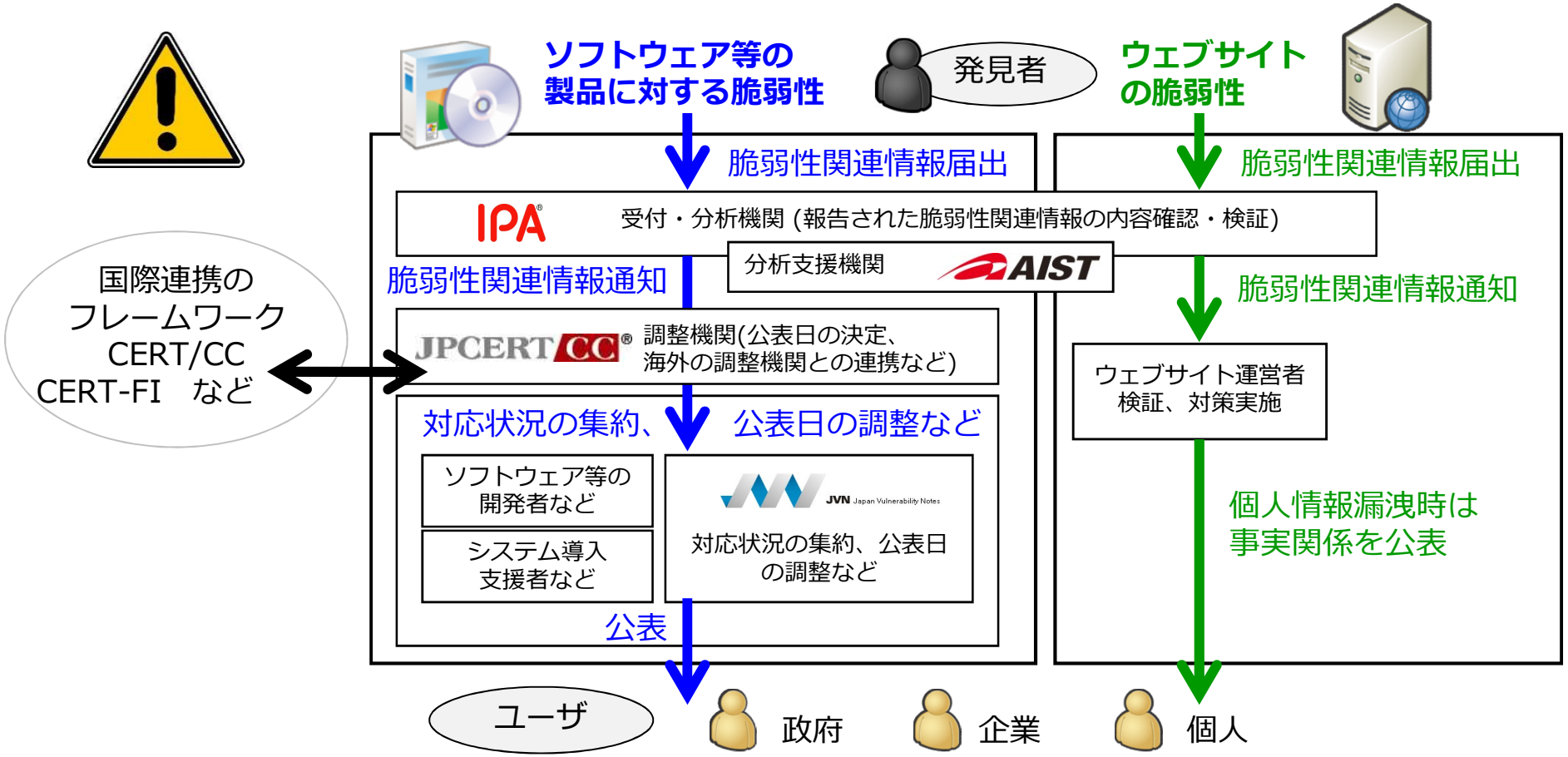
- JVN は、“Japan Vulnerability Notes” の略。
  日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供し、
  情報セキュリティ対策に資することを目的とする脆弱性対策情報サイト。

http://jvn.jp/

http://jvndb.jvn.jp/

脆弱性対策情報サイト ～情報セキュリティ早期警戒パートナーシップ～

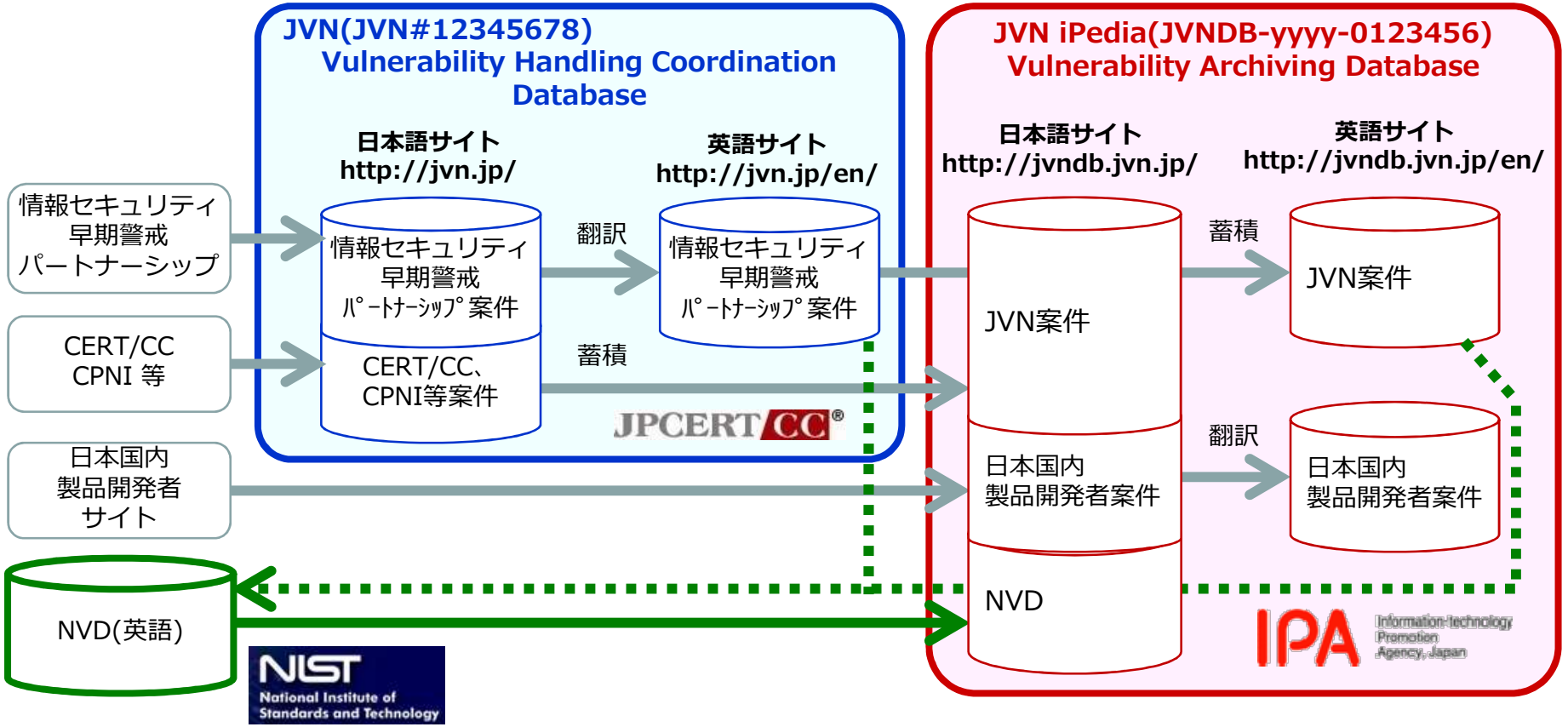
- ソフトウェア等の製品やウェブサイトに見つかった脆弱性に関する情報を受付け、製品開発者に修正を促すフレームワーク。2004年7月8日施行の「ソフトウェア等脆弱性関連情報取扱基準」に基づき運用されている。



SAMAC
一般社団法人 IT資産管理評価認定協会

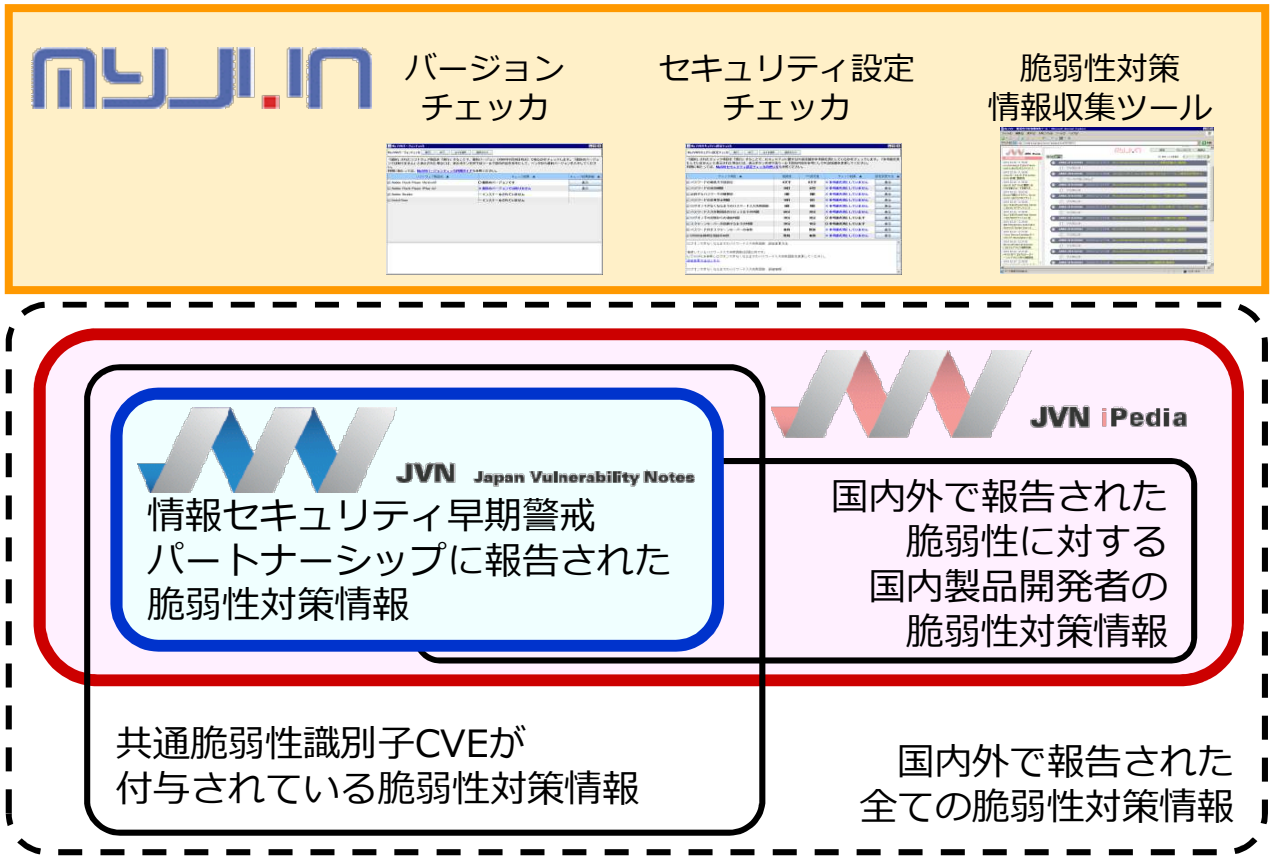
脆弱性対策情報サイト ～JVNは2つのデータベースから構成している～

- 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)から構成している。



脆弱性対策情報サイト ～JVN脆弱性対策機械処理基盤(MyJVN)～

- **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のこと。**



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

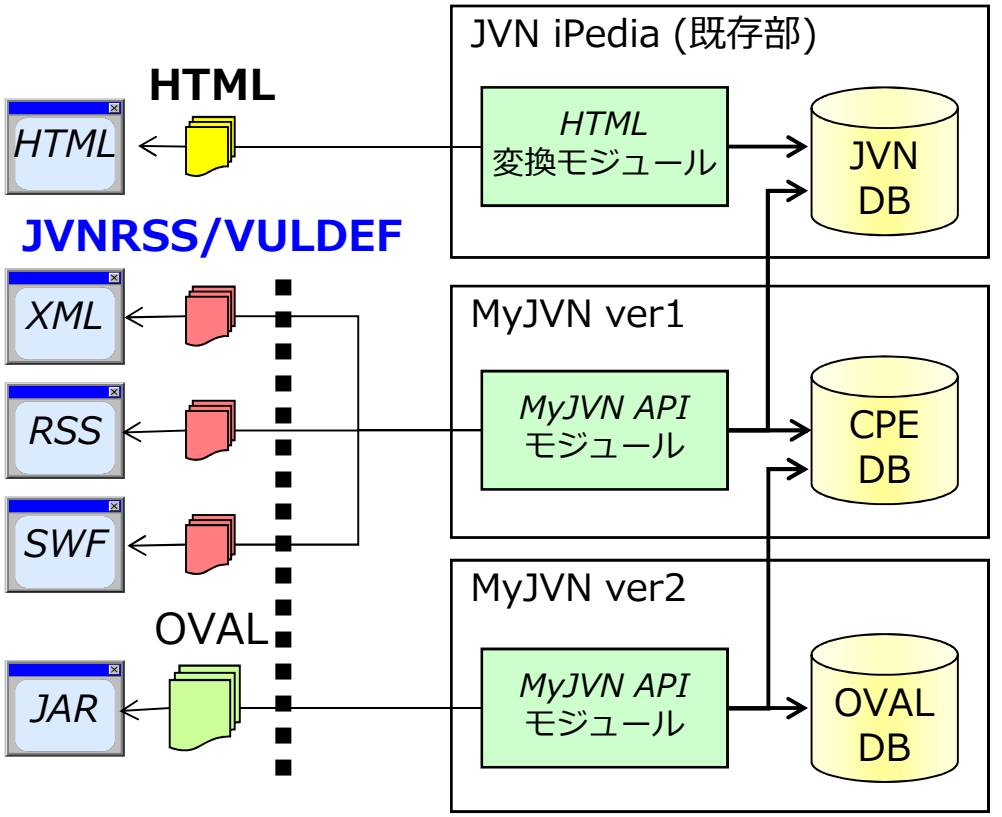
製品開発者と調整した脆弱性対策情報をタイムリーに公開する

脆弱性対策情報サイト～ http://jvndb.jvn.jp/apis/ ～

- **MyJVN API**
  JVN iPediaの情報をウェブ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

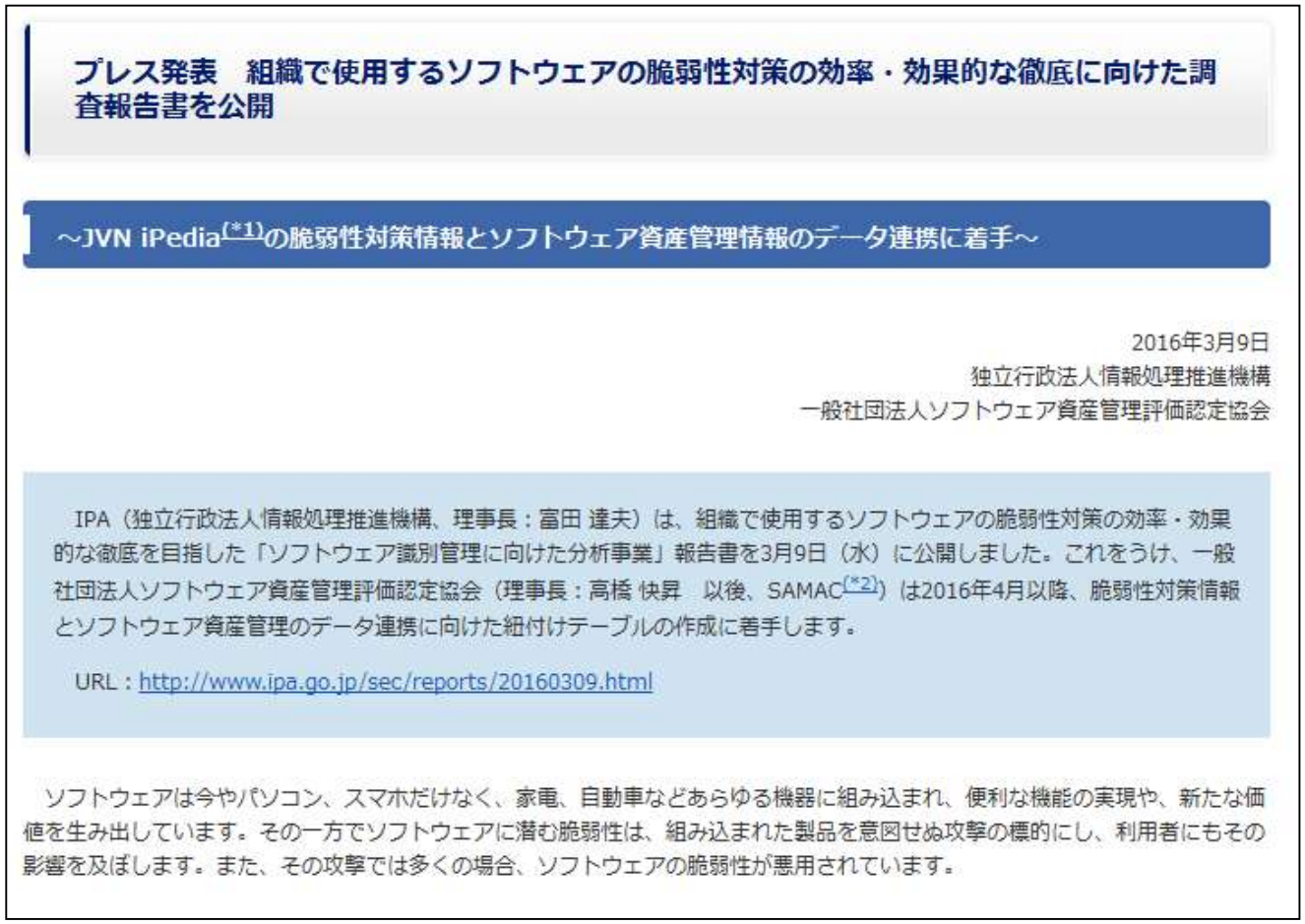


MyJVN API

ソフトウェア脆弱性データベースと SAMAC 辞書

SAMAC
一般社団法人 IT資産管理評価認定協会

～ 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 ～



プレス発表　組織で使用するソフトウェアの脆弱性対策の効率・効果的な徹底に向けた調査報告書を公開

～JVN iPedia(*1)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～

2016年3月9日
独立行政法人情報処理推進機構
一般社団法人ソフトウェア資産管理評価認定協会

IPA（独立行政法人情報処理推進機構、理事長：富田 達夫）は、組織で使用するソフトウェアの脆弱性対策の効率・効果的な徹底を目指した「ソフトウェア識別管理に向けた分析事業」報告書を3月9日（水）に公開しました。これをうけ、一般社団法人ソフトウェア資産管理評価認定協会（理事長：高橋 快昇　以後、SAMAC(*2)）は2016年4月以降、脆弱性対策情報とソフトウェア資産管理のデータ連携に向けた紐付けテーブルの作成に着手します。

URL：http://www.ipa.go.jp/sec/reports/20160309.html

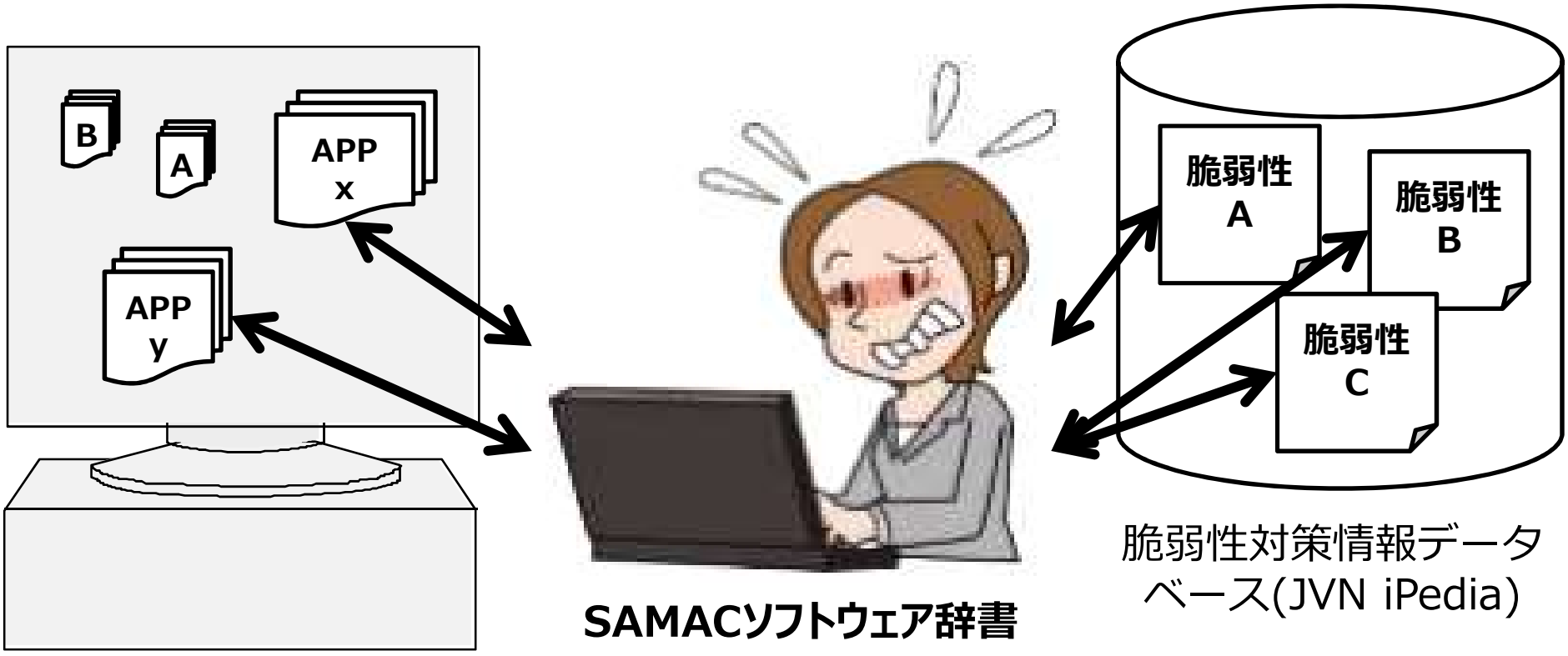
ソフトウェアは今やパソコン、スマホだけなく、家電、自動車などあらゆる機器に組み込まれ、便利な機能の実現や、新たな価値を生み出しています。その一方でソフトウェアに潜む脆弱性は、組み込まれた製品を意図せぬ攻撃の標的にし、利用者にもその影響を及ぼします。また、その攻撃では多くの場合、ソフトウェアの脆弱性が悪用されています。

https://www.ipa.go.jp/about/press/20160309.html

ソフトウェア辞書とのデータ管理

～インストール状況と脆弱性との紐付け～

- 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が連携できていない)

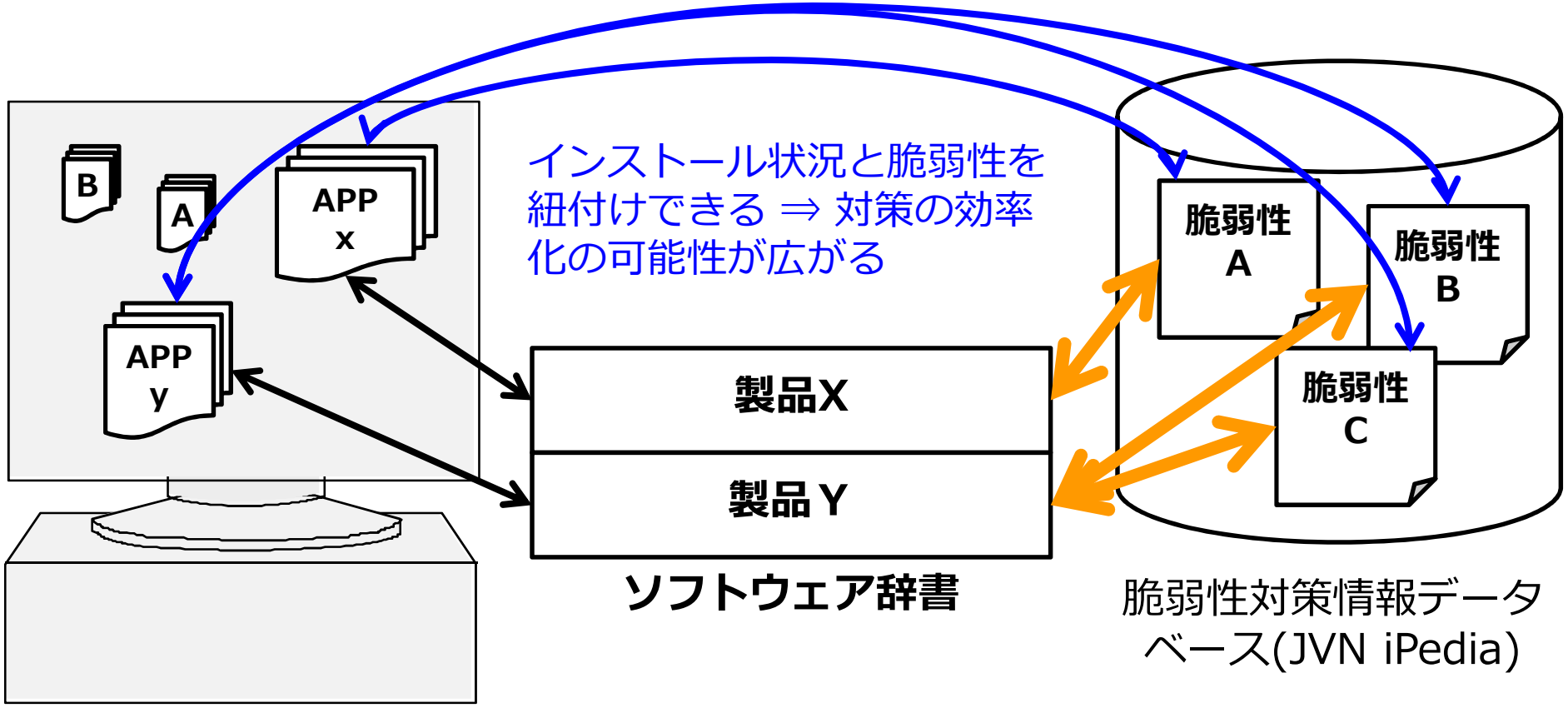


SAMAC
一般社団法人 IT資産管理評価認定協会

ソフトウェア辞書とのデータ連携

～インストール状況と脆弱性との紐付け～

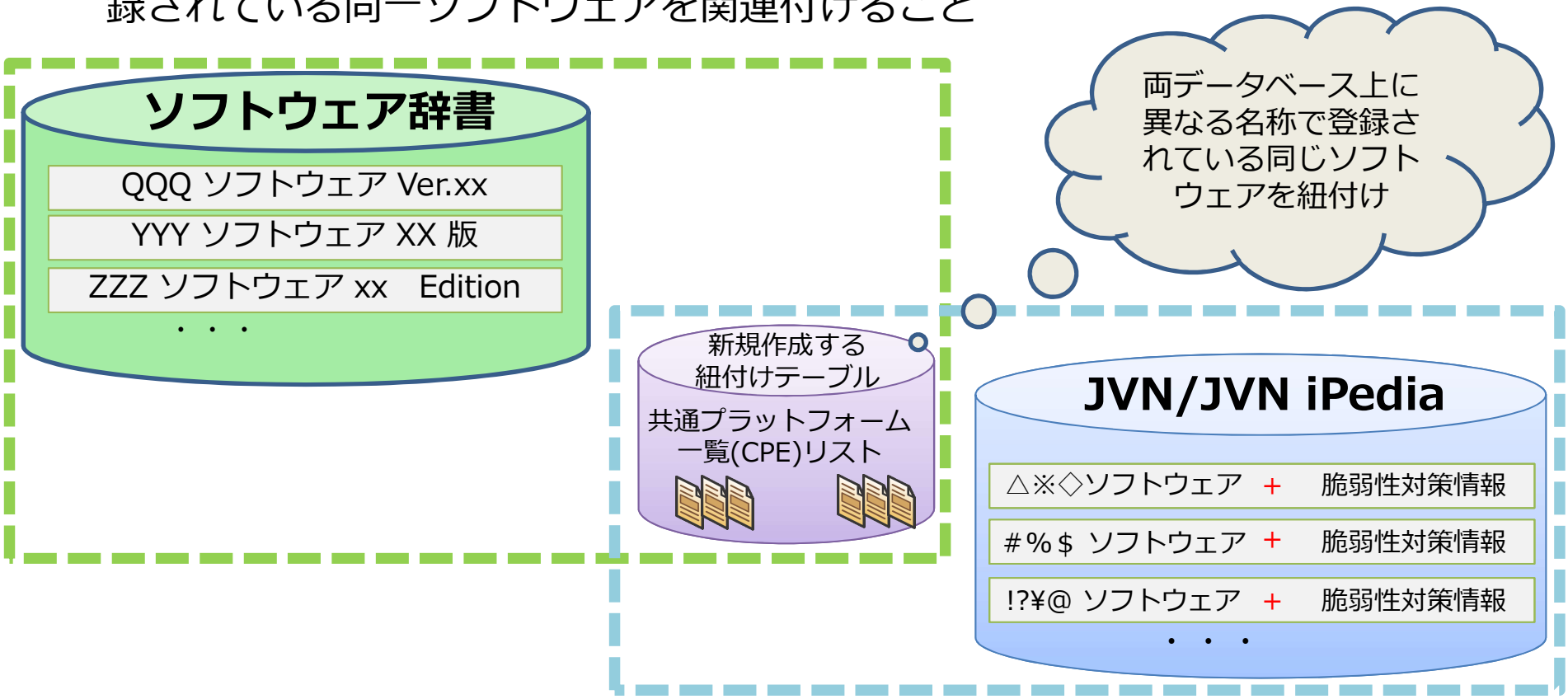
- もし、インストール状況を把握できるソフトウェア辞書と脆弱性対策情報サイト(JVN/JVN iPedia)を紐付け [橙色の線] できると・・・



ソフトウェア辞書とのデータ連携

～インストール状況と脆弱性との紐付け～

- **紐付けとは**
  ソフトウェア辞書と脆弱性対策情報サイト(JVN/JVN iPedia)で異なる名称で登録されている同一ソフトウェアを関連付けること



ソフトウェア辞書とのデータ連携

～ SAMAC ソフトウェア辞書 ～

- **SAMAC (一般社団法人ソフトウェア資産管理評価認定協会) が保守提供しているインストール状況を把握できるデータベース**
  - インベントリ収集ツールで収集可能な [プログラムの追加と削除] に表示されているインストール名称をベースに作成
  - ソフトウェア辞書に登録されている項目は、ベンダ名、ソフトウェア名、エディション、バージョン、ソフトウェア種別(有償ソフトウェア・フリーウェア、HOTFIX、ドライバ・ユーティリティ等)

ソフトウェア名	ベンダ名	エイリアス	バージョン	エディション	種別
Adobe Flash Player 10 ActiveX	ADOBE SYSTEMS	Flash Player	10	ActiveX	フリーウェア
Realtek High Definition Audio Driver	Realtek Semiconductor	High Definition Audio Driver	-	-	ドライバー・ユーティリティー等
Microsoft .NET Framework 3.5 SP1	Microsoft	.NET Framework	3	-	フリーウェア
IP Messenger for Win32	白水 啓章	IP Messenger	32	-	フリーウェア
Microsoft Office Personal 2007	Microsoft	Office	2007	Personal	有償ソフトウェア
JUSTSYSTEMｱﾌﾟﾘｹｰｼｮﾝの追加と削除	JUSTSYSTEMS	アプリケーションの追加と削除	-	-	ドライバー・ユーティリティー等
Google Toolbar for Internet Explorer	Google	Google Toolbar	-	-	フリーウェア
Intel(R) Graphics Media Accelerator Driver	Intel	Graphics Media Accelerator Driver	-	-	ドライバー・ユーティリティー等

ソフトウェア辞書とのデータ連携

～ 製品識別子CPEを用いた製品の紐付け ～

- **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
- **MyJVN APIでは、CPE v2.2をサポート**

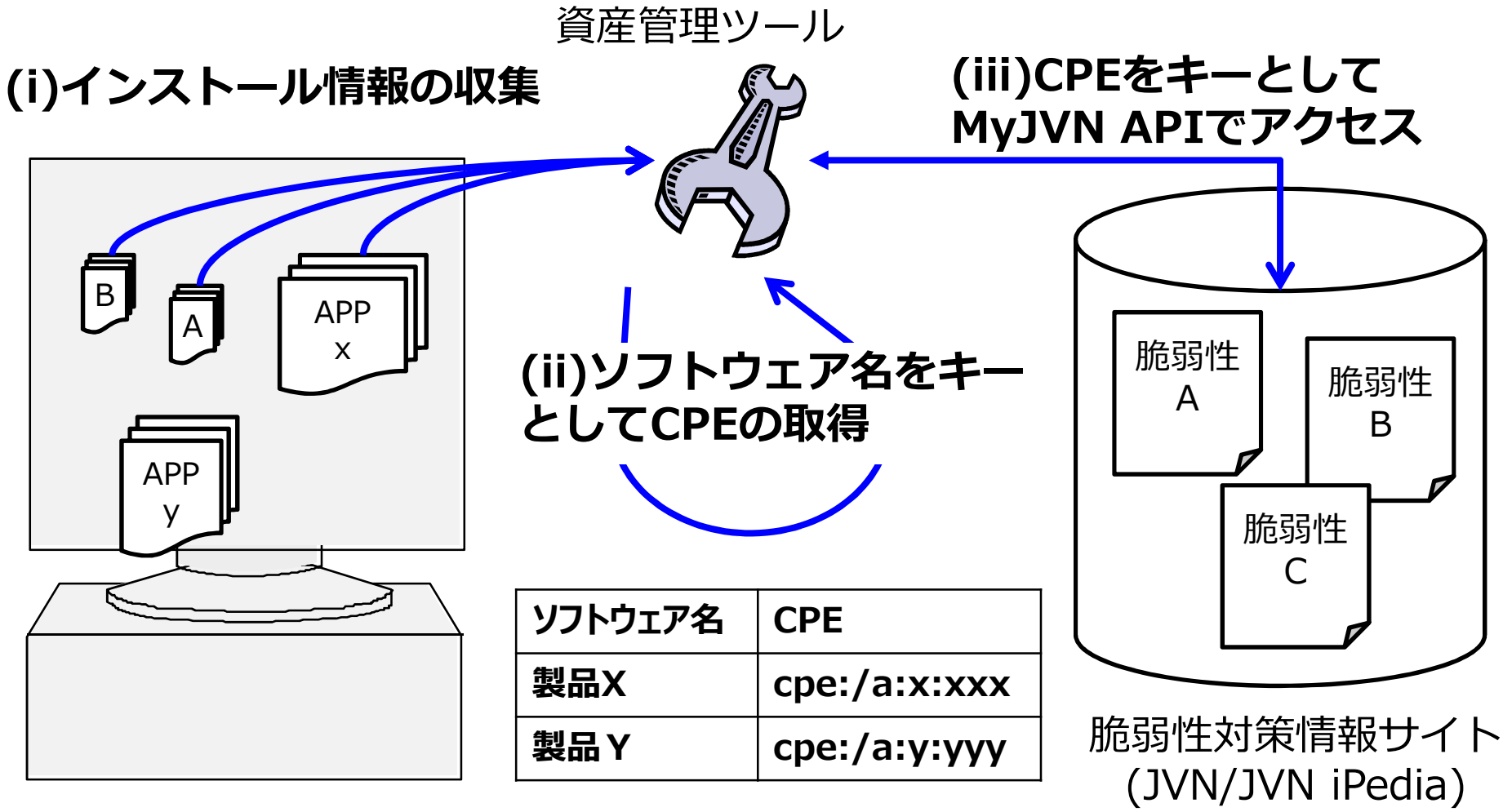
cpe:/a:ipa:myjvn

cpe:/{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}

種別：h=ハードウェア, o=OS, a=アプリケーション

ソフトウェア辞書とのデータ連携

～脆弱性対策情報参照までの流れ～

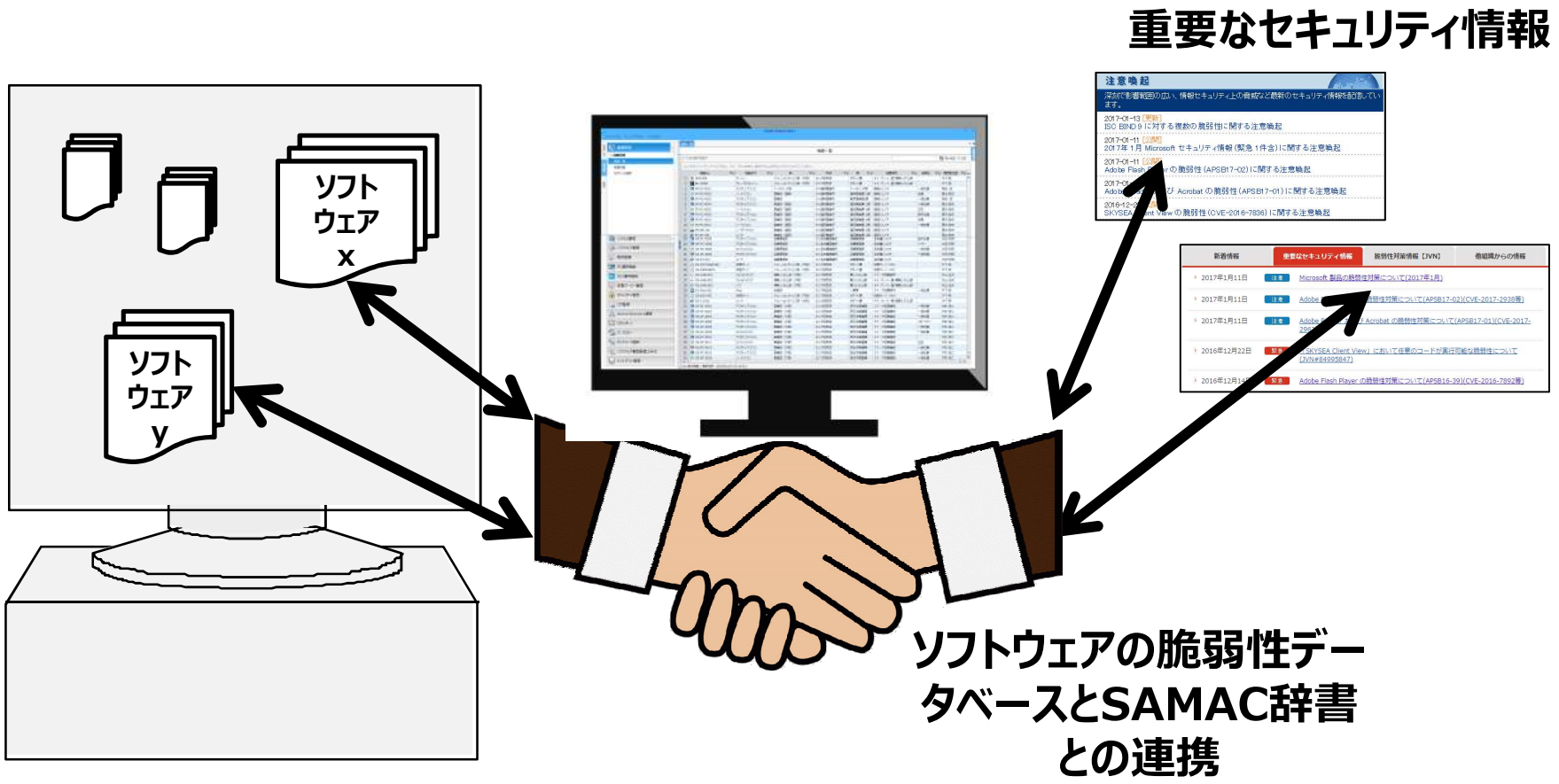


ソフトウェア名	CPE
製品X	cpe:/a:x:xxx
製品Y	cpe:/a:y:yyy

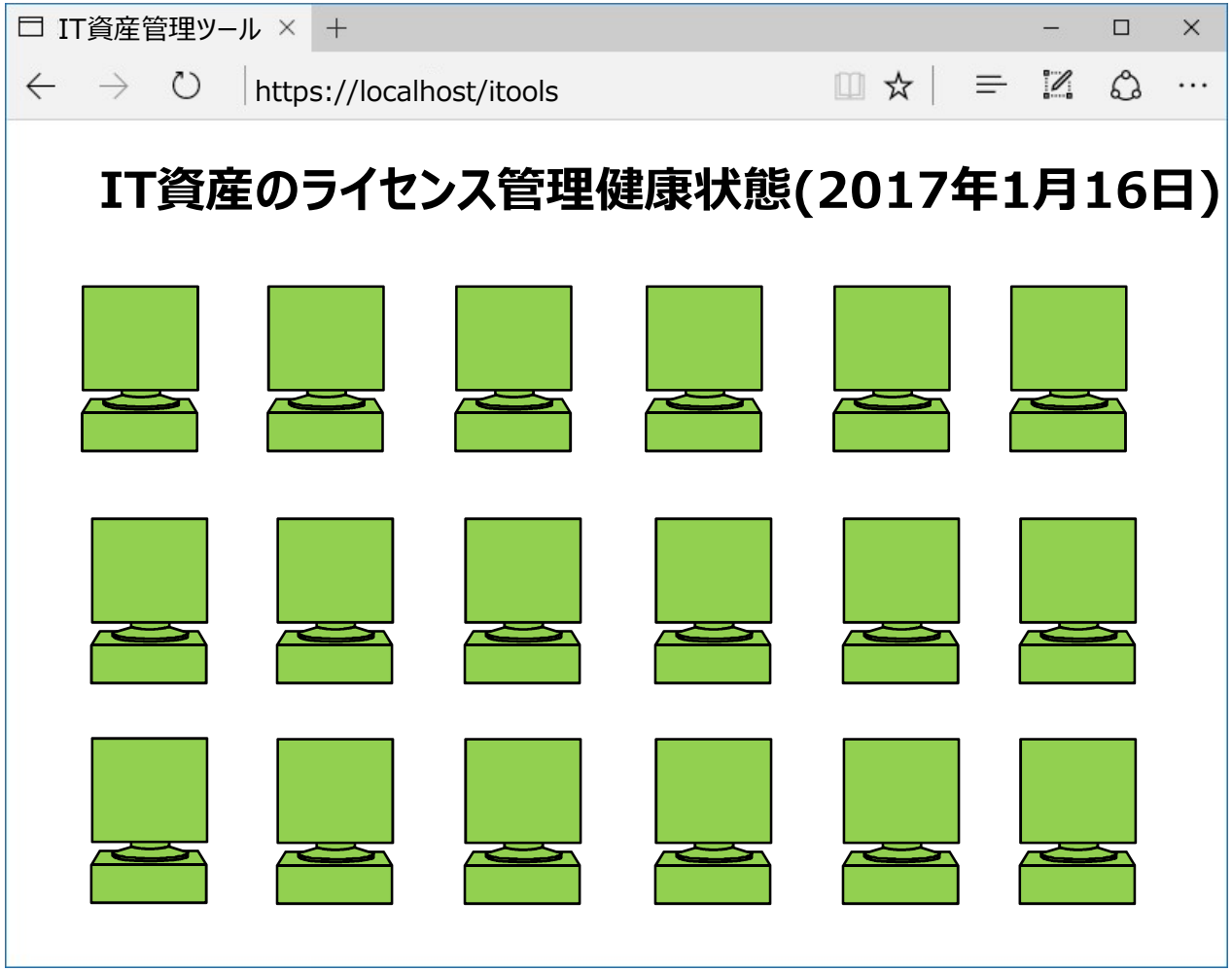
IT資産管理ツールでの脆弱性管理イメージ

IT資産管理ツールで脆弱性管理もしてみませんか？

- ソフトウェアの脆弱性データベースとSAMAC辞書とを紐付けることにより、IT資産管理ツールで脆弱性管理もできるようになるんです。



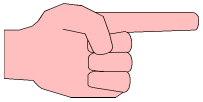
IT資産管理ツールでの脆弱性管理



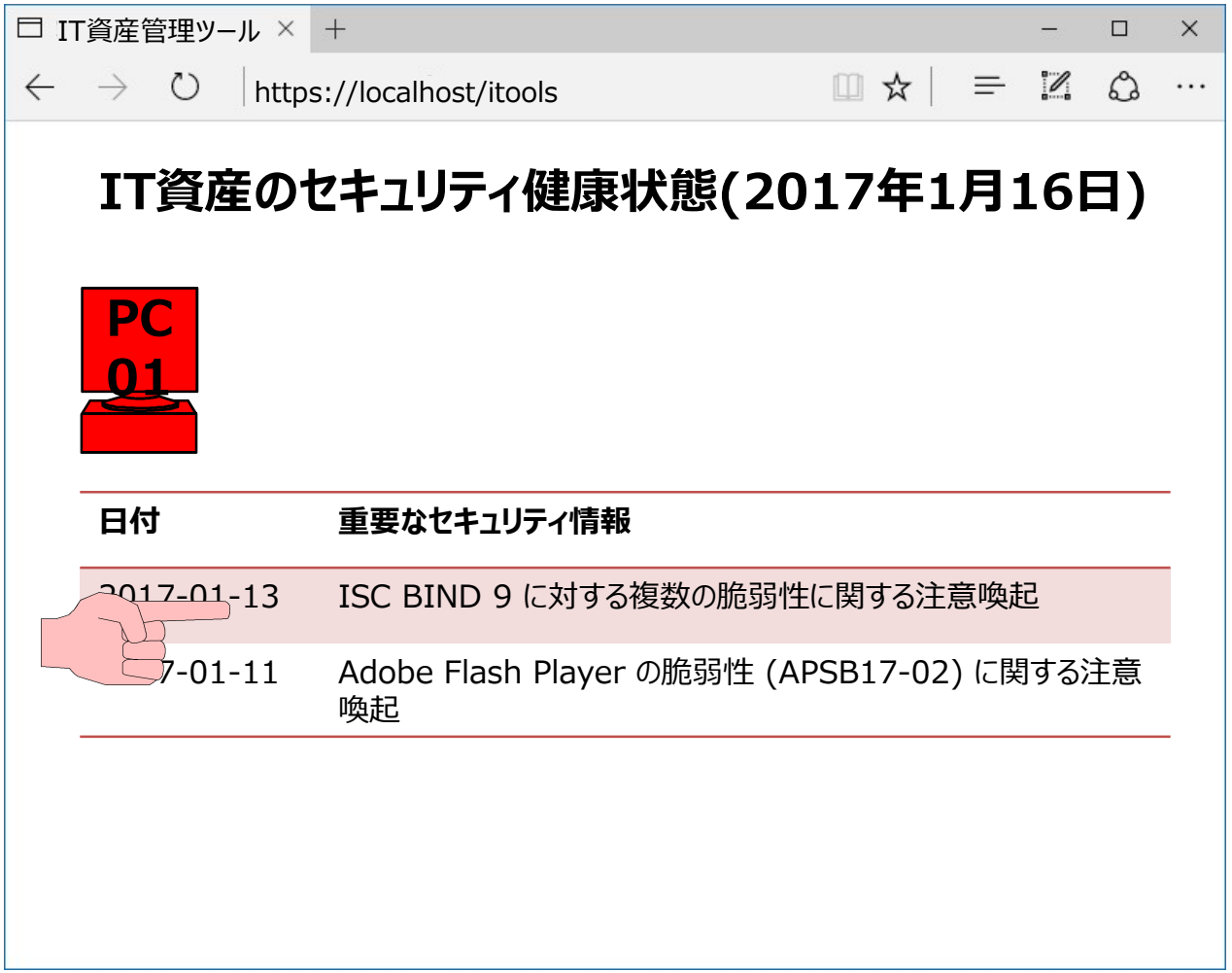
SAMAC
一般社団法人 IT資産管理評価認定協会

IT資産管理ツールでの脆弱性管理

IT資産管理ツールでの脆弱性管理



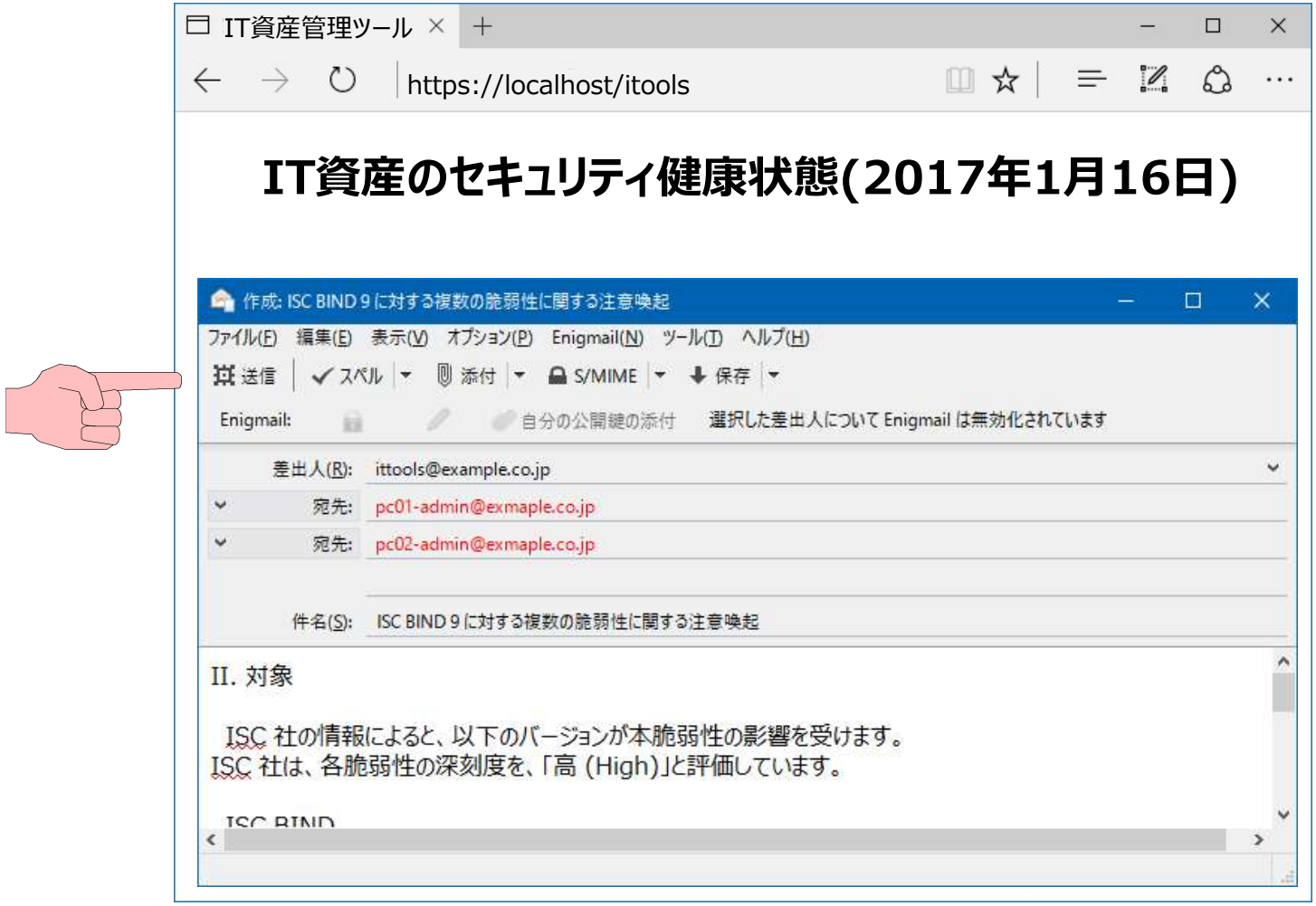
IT資産管理ツールでの脆弱性管理



IT資産管理ツールでの脆弱性管理

IT資産管理ツールでの脆弱性管理

IT資産管理ツールでの脆弱性管理



SAMAC
一般社団法人 IT資産管理評価認定協会

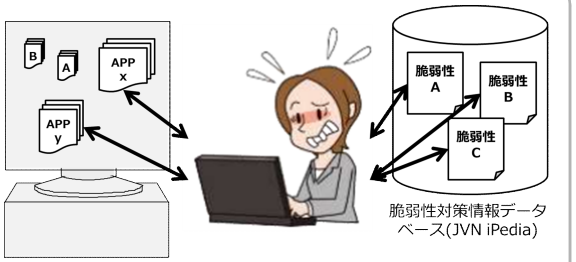
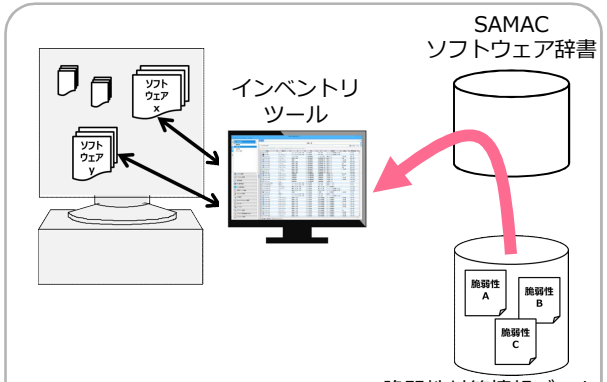
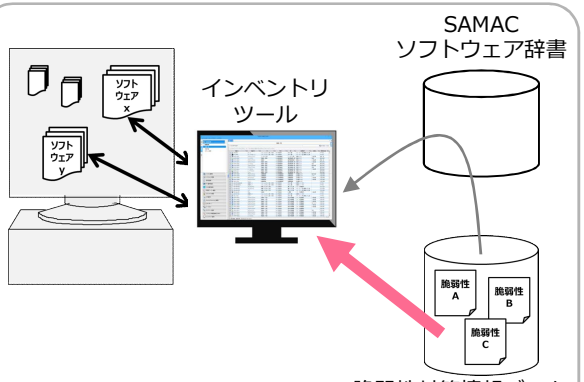
IT資産管理ツールでの脆弱性管理

連携辞書の更新計画

- 更新頻度　：月1回（6月以降を予定）
  - WGで作成した手順を元に作業の外部委託を検討
  - IPAより脆弱性情報を月に1回CSVでもらう

- 今回のリリースは脆弱性の情報公開が多い次の製品
  - Adobe（Reader, Flash, ShockW）,JRE,一太郎,OpenSSL
  - 辞書契約しているユーザー以外にも公開する予定だが、今後の更新で会員限定のものを増やしていく予定

脆弱性情報への取り組みと今後

現在	① 現在の取組み 『JVN iPedia情報の活用』	② 将来的な連携 『JVN iPedia Tag連携』
		
人が脆弱性情報を検索し、各ソフトウェアを確認する。	SAMACソフトウェア辞書に脆弱性対策情報を連携する。	ソフトウェア識別タグが正式化すると直接インベントリツールと連携できる。
『全部なんて調べきれない！』	『辞書登録にあるものは、ツールの中で視覚的に分かる！』	『辞書登録に関わらず、Tagがあればツールの中で視覚的に分かる！』
『いつの間にか脆弱性のあるソフトが入ってた！』	『でも直近の新しい情報は反映が遅くなってしまう・・・。』	『かなりリアルタイムに情報が反映される！』

ソフトウェア辞書とのデータ連携

～具体的な取り組み～

- **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

プレス発表　組織で使用するソフトウェアの脆弱性対策の効率・効果的な徹底に向けた調査報告書を公開

～JVN iPedia(*1)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～

2016年3月9日
独立行政法人情報処理推進機構
一般社団法人ソフトウェア資産管理評価認定協会

IPA（独立行政法人情報処理推進機構、理事長：富田 達夫）は、組織で使用するソフトウェアの脆弱性対策の効率・効果的な徹底を目指した「ソフトウェア識別管理に向けた分析事業」報告書を3月9日（水）に公開しました。これをうけ、一般社団法人ソフトウェア資産管理評価認定協会（理事長：高橋 快昇　以後、SAMAC(*2)）は2016年4月以降、脆弱性対策情報とソフトウェア資産管理のデータ連携に向けた紐付けテーブルの作成に着手します。

URL：http://www.ipa.go.jp/sec/reports/20160309.html

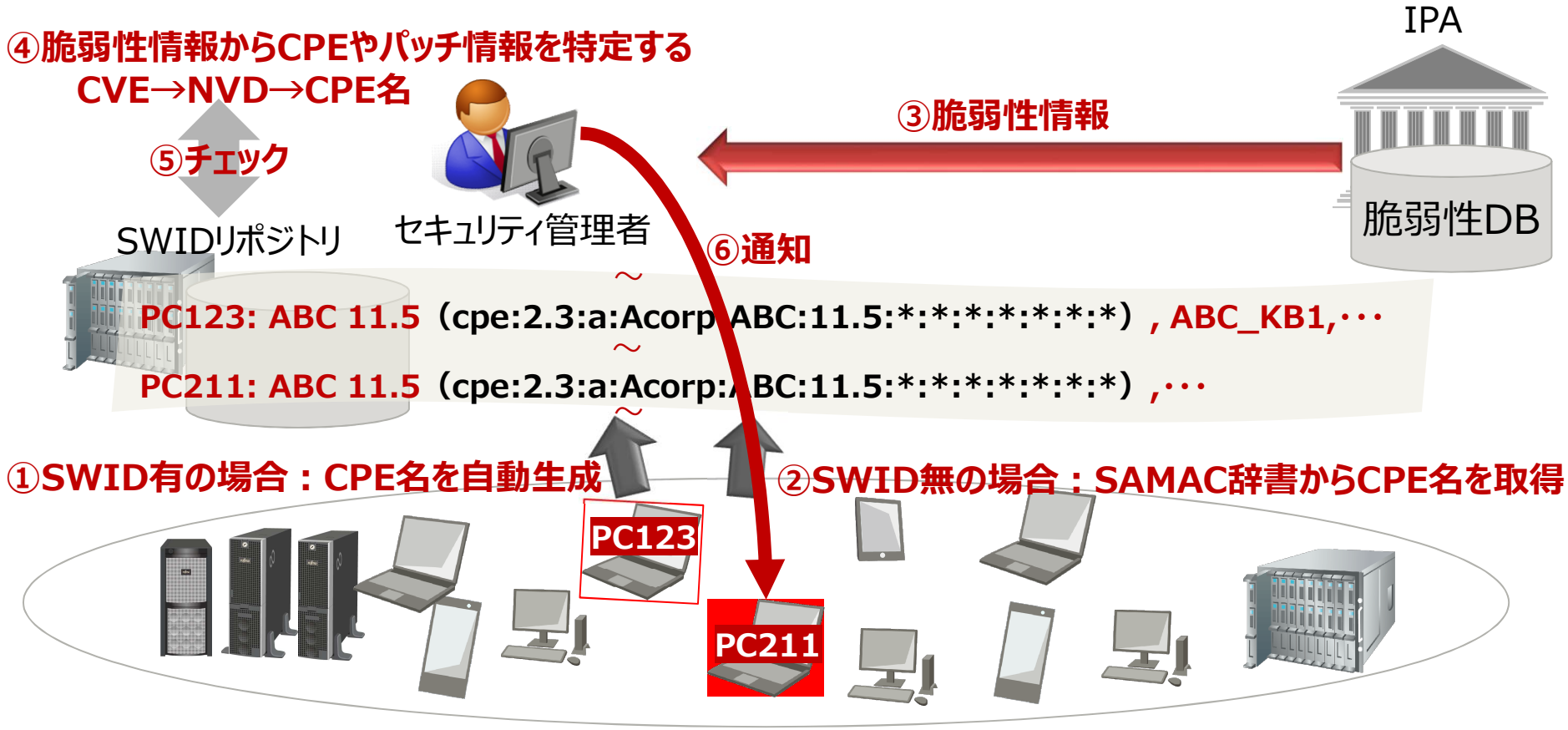
ソフトウェアは今やパソコン、スマホだけなく、家電、自動車などあらゆる機器に組み込まれ、便利な機能の実現や、新たな価値を生み出しています。その一方でソフトウェアに潜む脆弱性は、組み込まれた製品を意図せぬ攻撃の標的にし、利用者にもその影響を及ぼします。また、その攻撃では多くの場合、ソフトウェアの脆弱性が悪用されています。

- **長期的**
  - ソフトウェア識別タグ ISO19770-2 を用いた資産管理と脆弱性対策の連携

将来像:19770-2:2015（SWID）を活用した脆弱性対策

脆弱性情報から該当プログラムが正確に検出され(SWIDの場合),自動化が可能となる

例　AcorpのABCソフト、バージョン11.1から11.7、バージョン12.0から12.1（12.1から12.1まで）に脆弱性。バージョン12.2以降で修正。修正パッチは ABC_KB1がある；SWIDリポジトリを調べ、ABC 11.5の導入されたPC123とPC211を発見するが、PC123にはパッチABC_KB1が当たっているため、PC211のみに脆弱性がある。



凡例　CVE:共通脆弱性識別子, NVD:国際脆弱性DB, CPE:共通プラットフォーム一覧

将来像:実現させるために

- ソフトウェア開発者がNISTIR 8060のUS３（脆弱性エンドポイントを特定できるレベルの運用パターン）に従ったSWIDの生成を実施する。
- SWIDに対応しないソフトウェアとの共存のために以下の対策が考えられる：
  - ✓SAMAC辞書とIPAの脆弱性対策情報データベース との連携をSWIDの運用と共存させる。
  - ✓SAMAC辞書のCPE名をもとにSWIDを作成し、資産管理ツールベンダーに提供する。
- NVDに登録されるCPE名がSWIDから自動生成されるようにする。（NISTIR 8085で自動生成するPGが公開されている）
- SWIDの信頼性を保証するために電子署名を導入する。

- NISTIR 8060 “Guidelines for the Creation of Interoperable Software Identification (SWID) Tags”
- NISTIR 8085 “Forming Common Platform Enumaration(CPE)Names from Software Identification(SWID)Tags”

凡例　NISTIR:National Institute of Standards and Technology Interagency Report

一般社団法人IT資産管理評価認定協会