IPA Better Life with IT

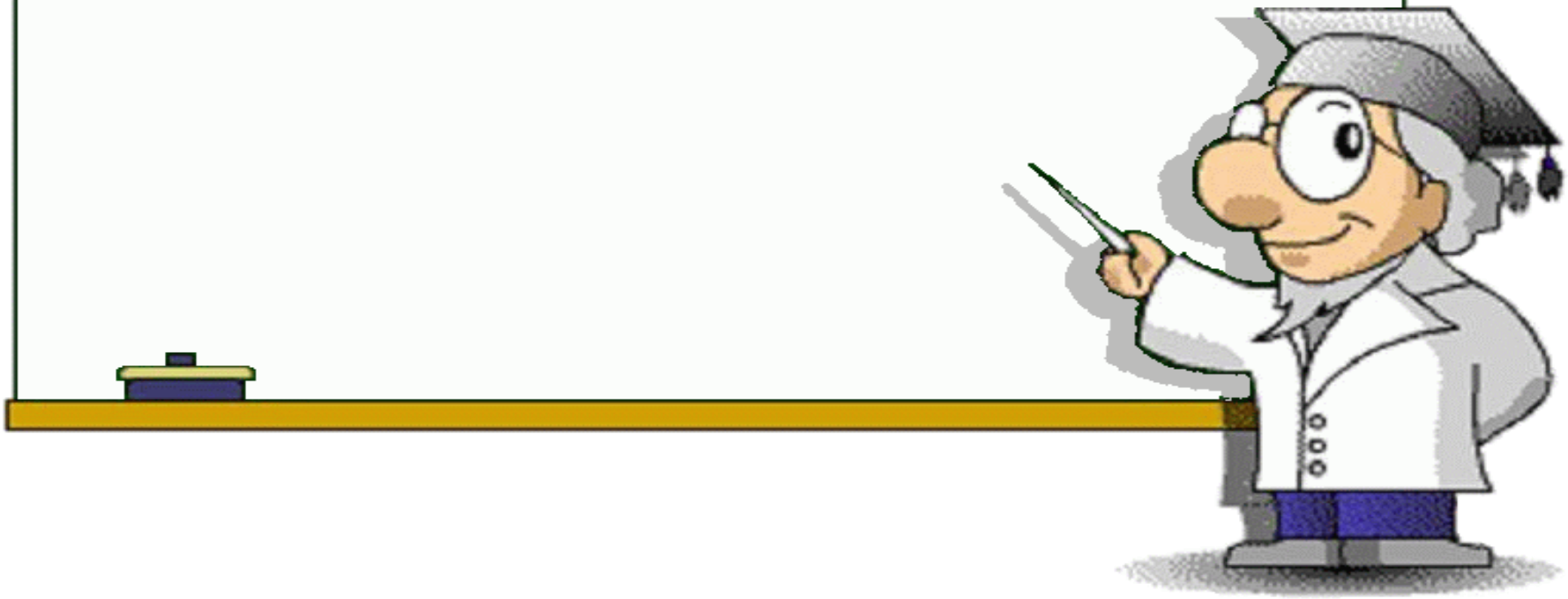
ソフトウエアの脆弱性データベースとSAMAC辞書

2016/06/10

独立行政法人 情報処理推進機構 (IPA)
技術本部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

目次

- 脆弱性とは
- 脆弱性関連情報の収集
- JVN脆弱性対策機械処理基盤
- ソフトウエアの脆弱性データベースとSAMAC辞書



脆弱性、、、なんだろう…？

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)

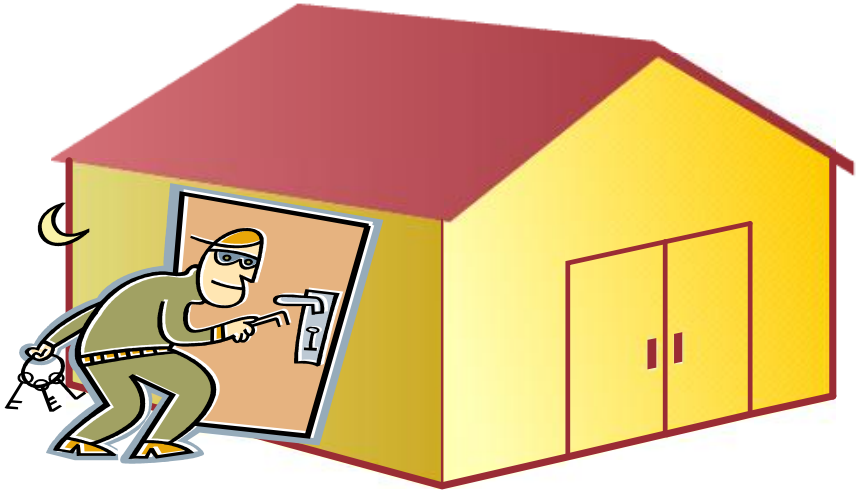
OSコマンドインジェクションの脆弱性を突かれて不正アクセス！！
（民放テレビ会社にて43万件情報漏えい)

新聞から

ウェブニュースから

脆弱性とは・・・

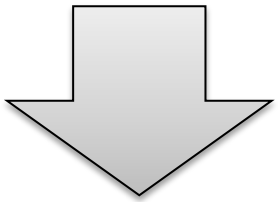
- OSやソフトウエアのセキュリティ上の欠陥
- 家に例えると、
  ドアの鍵穴の劣化、鍵そのものの”弱さ”



脆弱性あると(鍵が付いていない、鍵をかけていないのと同じこと)
・・・侵入者(攻撃者)によって家(PC・サーバ)に
容易に入られてしまうことに。

脆弱性とは・・・

- **脆弱性の定義**
  脆弱性とは、ソフトウエ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)

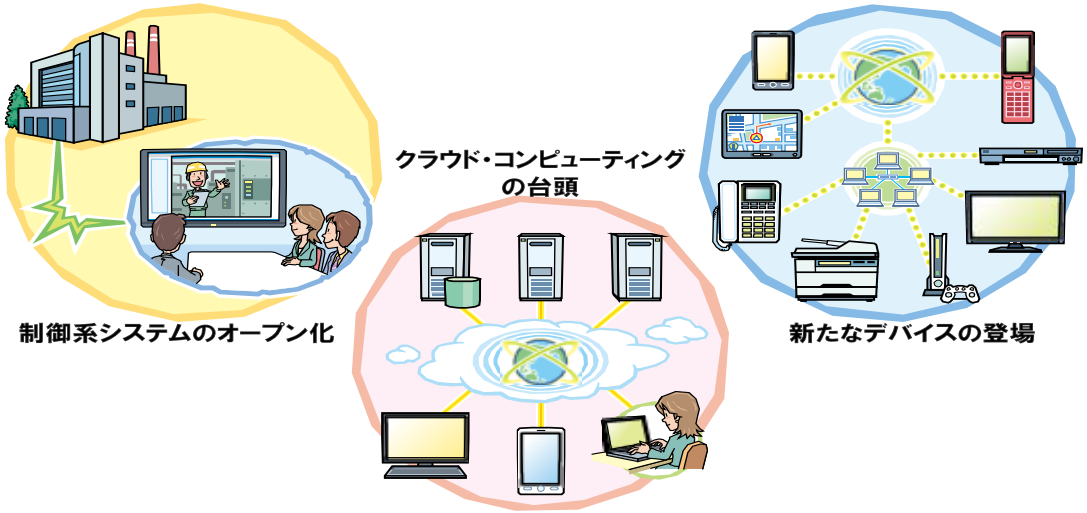


言い換えれば

- **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2016～

IPA

- 2015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

【3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

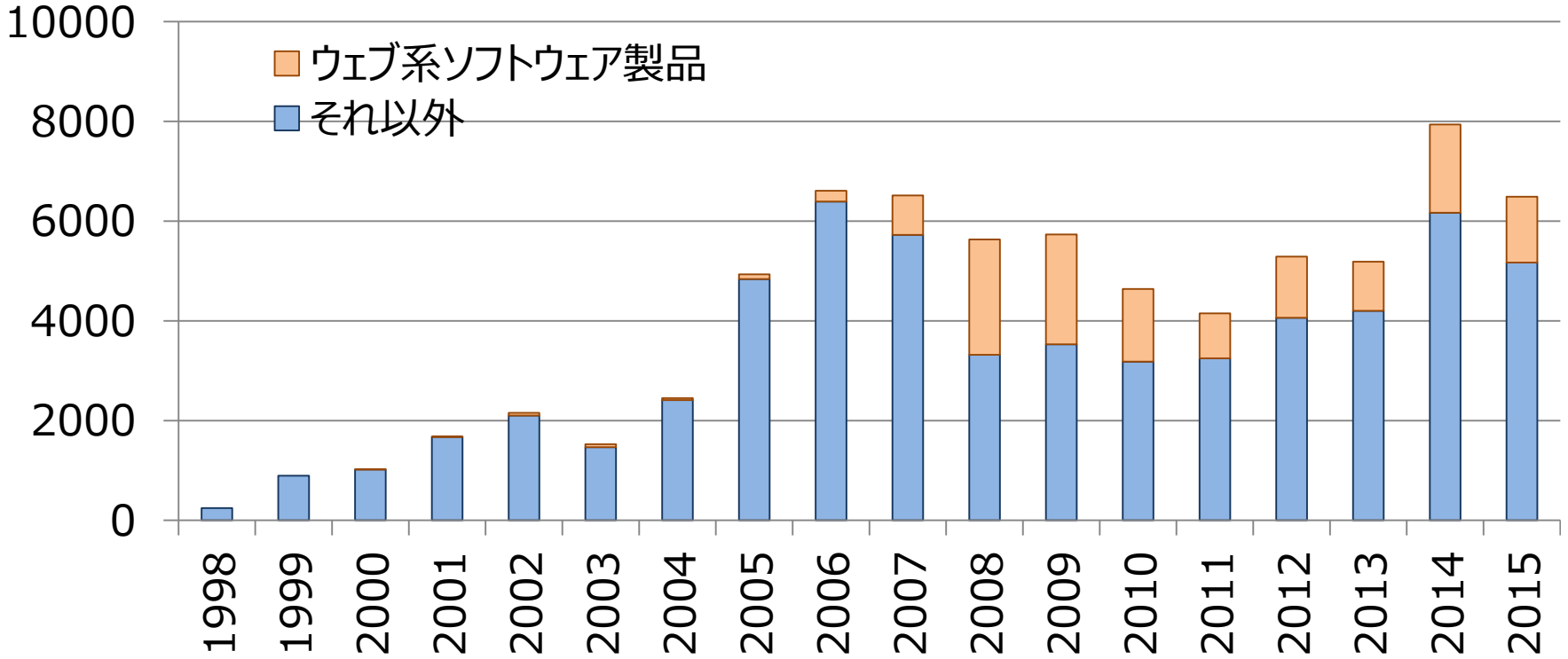
【6位】ウェブサイトの改ざん
脆弱性を悪用して改ざん

【10位】脆弱性公開に伴う公知となる脆弱性の悪用増加
公開された脆弱性情報を基に攻撃

脆弱性を取り巻く脅威・危険性
～脆弱性の報告件数～

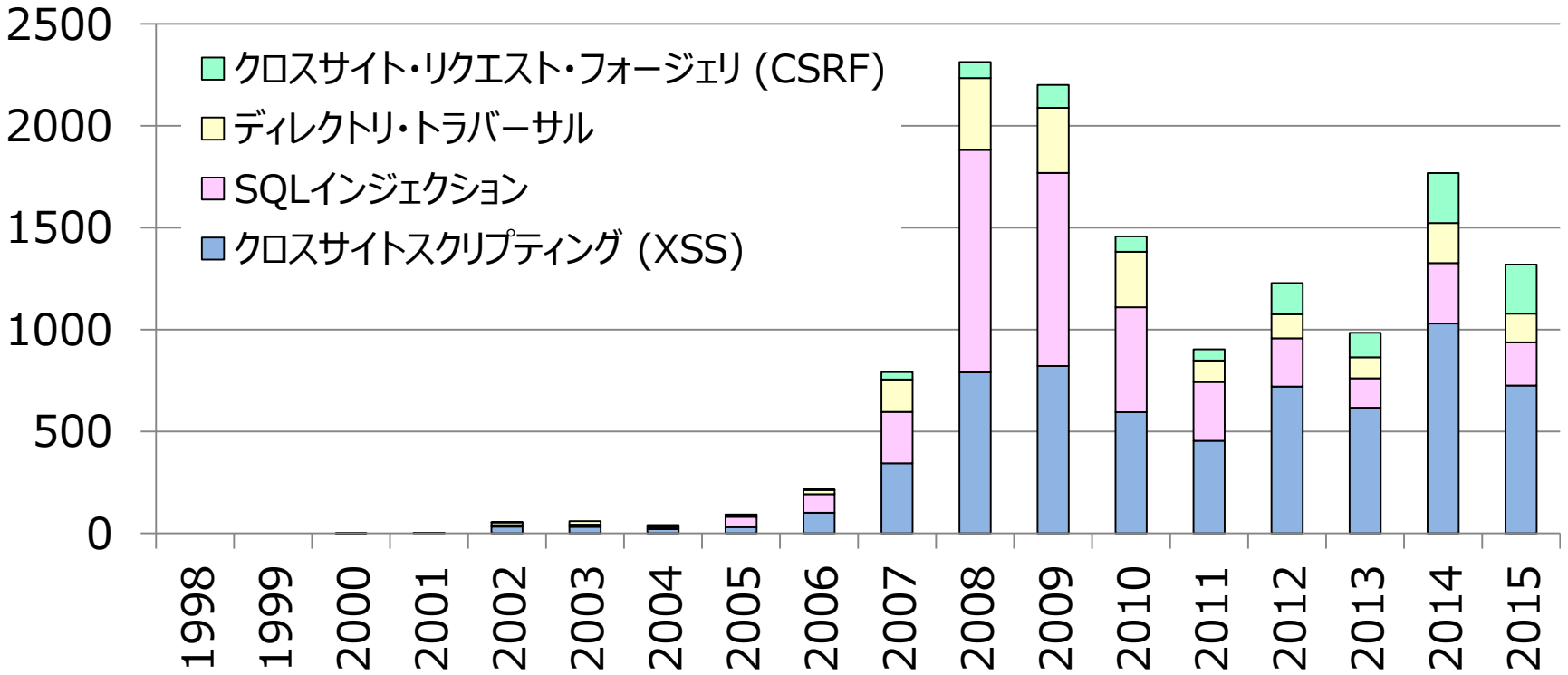
- **米国立標準技術研究所の脆弱性データベースNVDに登録された2015年の脆弱性の総件数は6,488件**

NIST(National Institute of Standards and Technology)
NVD(National Vulnerability Database)



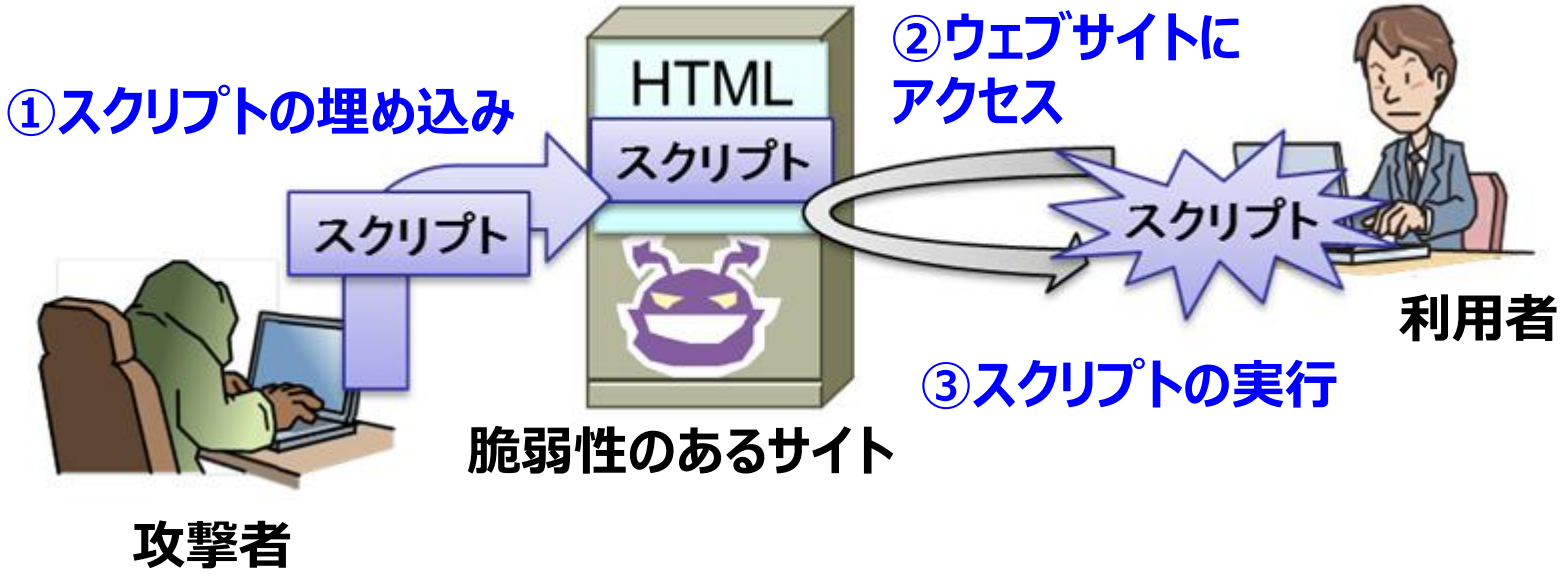
脆弱性を取り巻く脅威・危険性
～脆弱性の報告件数～

- うち、ウェブ系ソフトウエア製品の脆弱性が約2割(1,319件)で、内訳は、クロスサイトスクリプティング (XSS)、SQLインジェクションが約8割



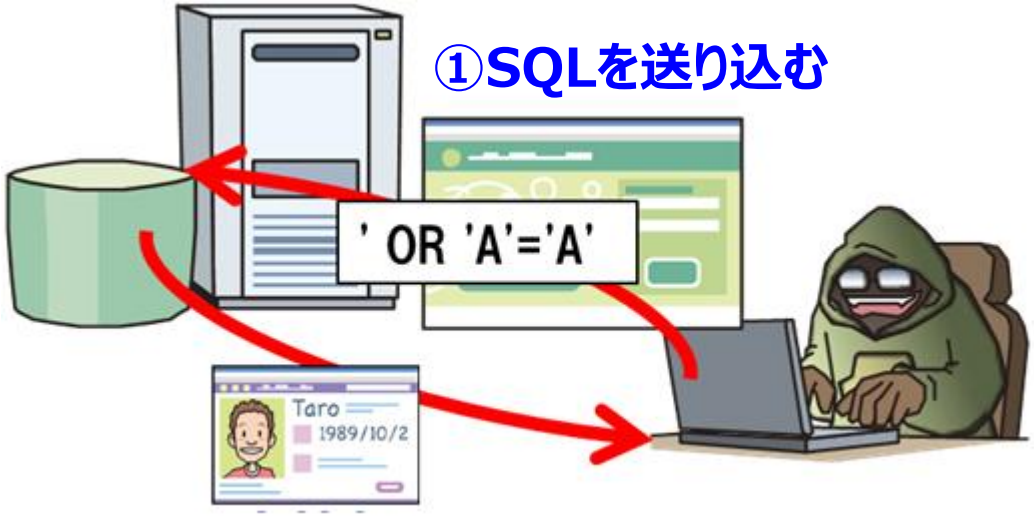
代表的な脆弱性
～クロスサイトスクリプティング(XSS)～

- XSSとは、スクリプトをサイトに送り込み、スクリプトを含むHTMLを出力し、ブラウザ上で実行させる攻撃
- 「開発者」が作り込みやすい脆弱性



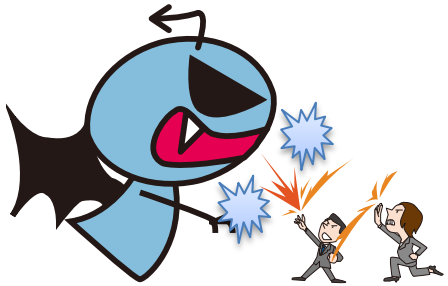
代表的な脆弱性
～SQLインジェクション～

- SQLとは、データベースを操作する為の問合せ言語
- SQL Injection = SQLの注入
- SQLインジェクションとは、外部から意図しないSQLを注入し、不正にデータベースを操作する攻撃
- 「攻撃者」に狙われやすい脆弱性



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。



「彼を知り己を知れば百戦殆うからず」

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。

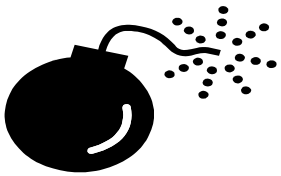
情報収集に役立つ
キーワードについて知ろう

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
ソフトウエア

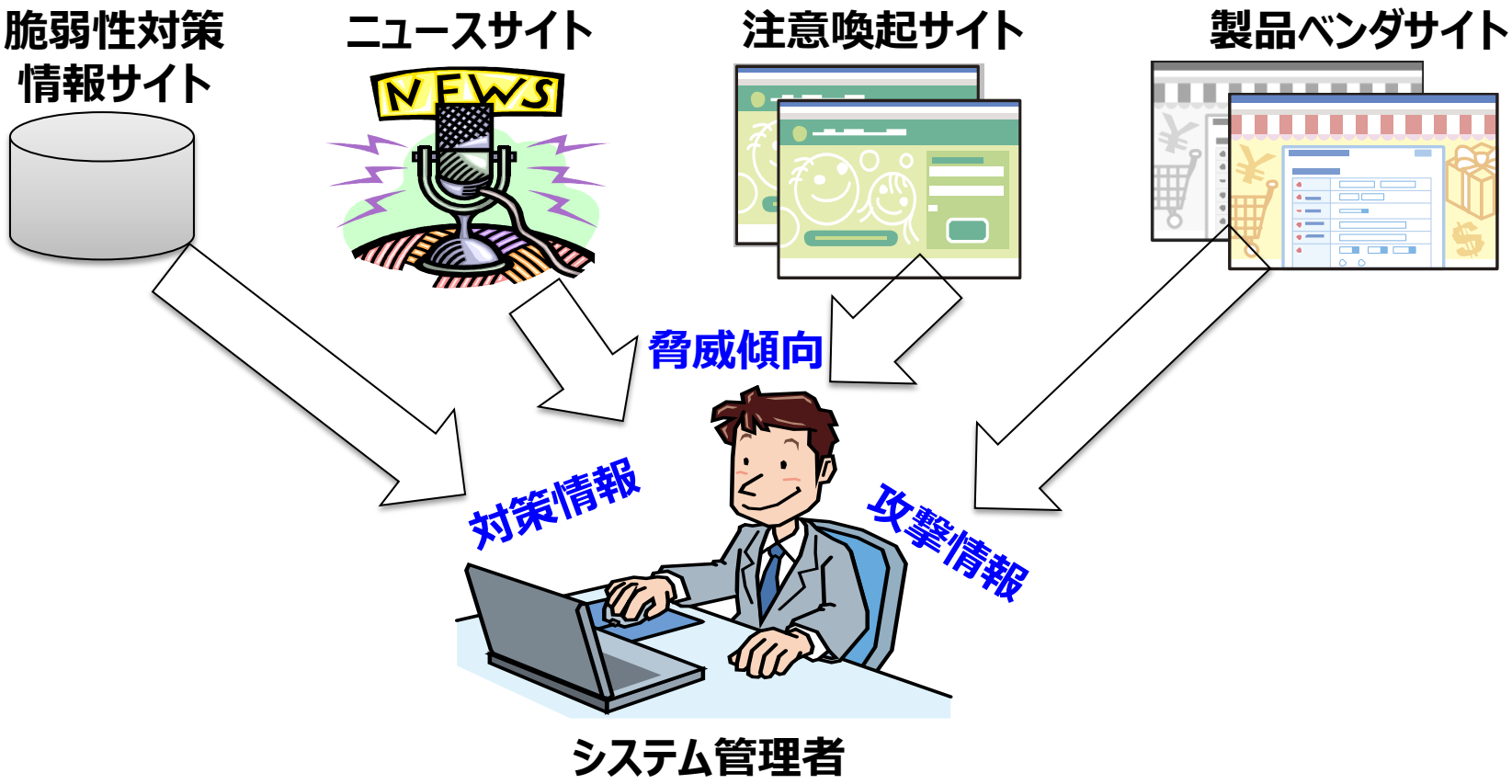
脆弱性を除去する

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

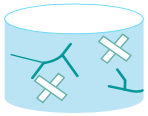
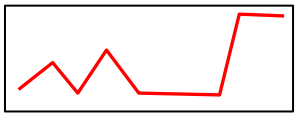
脆弱性関連情報の収集
～外部の情報を収集し、自組織の対策に役立てる～

- 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		Gate	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～

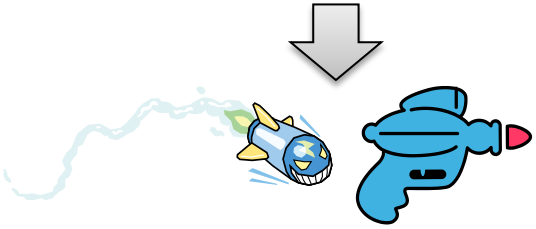
IPA

cvss

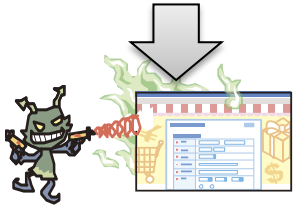
- **攻撃状況やシステムの重要度を加味した脆弱性の深刻度を表す評価**

＝ 「技術的な特性」 × 「脅威の大きさ」 × 「情報資産の価値」

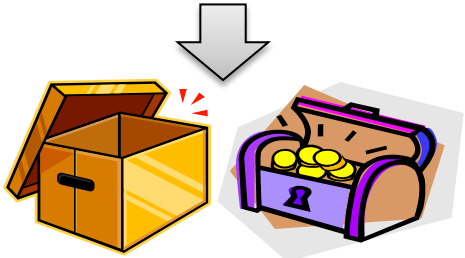
＝ 「基本評価基準」 × 「現状評価基準」 × 「環境評価基準」



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、ソフトウエアの名称を、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

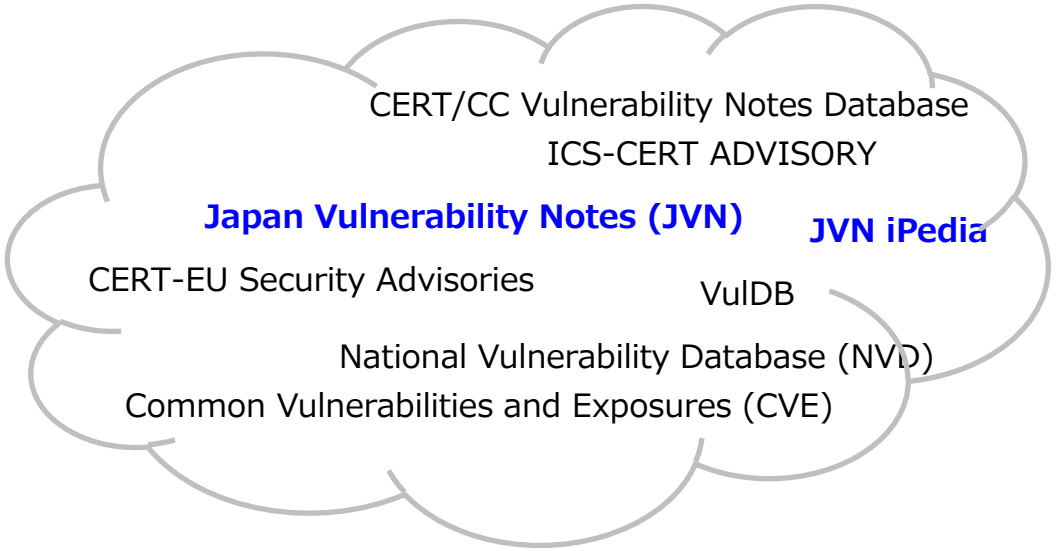
cpe:/{種別}:{ベンダ}:{製品}:{バージョン}:{アップデート}:{エディション}:{言語}

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、、、

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。

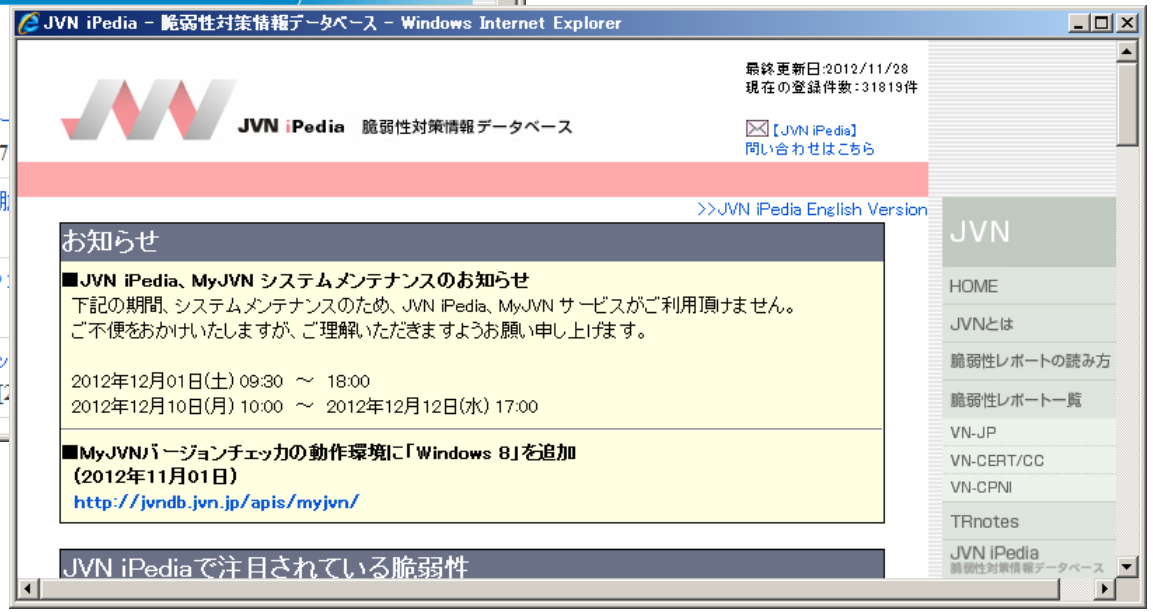


脆弱性対策情報サイト
～JVN～

- JVN は、“Japan Vulnerability Notes” の略。日本で使用されているソフトウエ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。

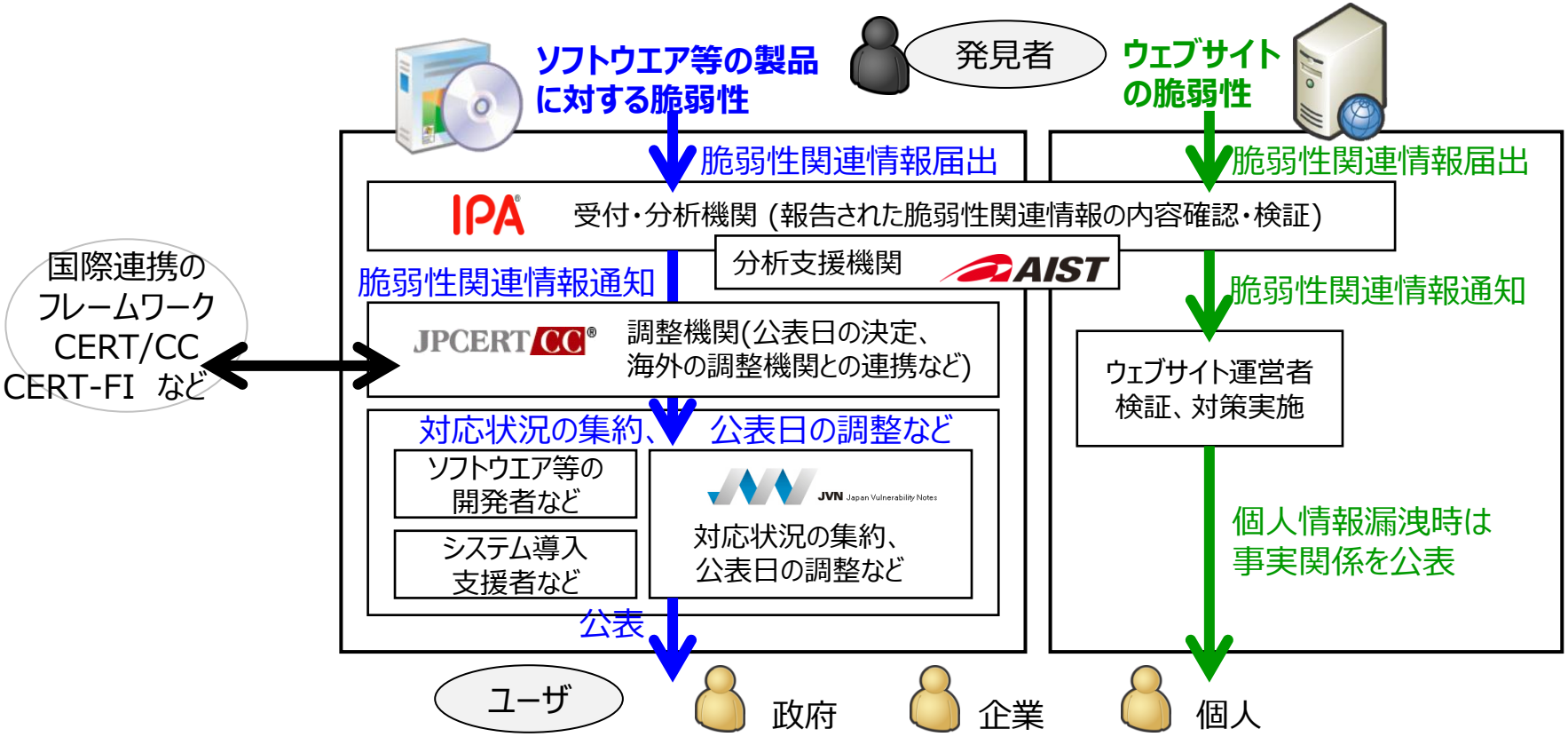
http://jvn.jp/

http://jvndb.jvn.jp/



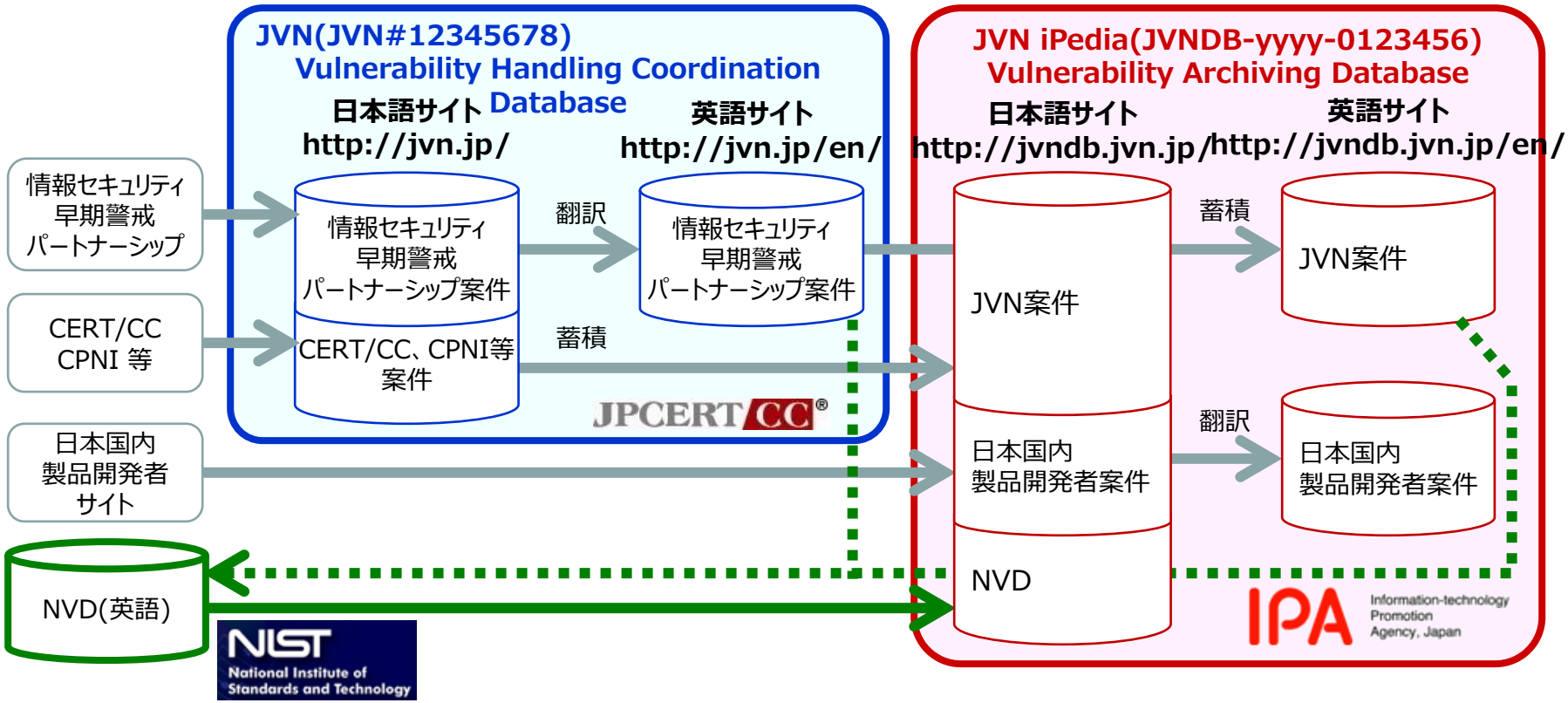
脆弱性対策情報サイト
～情報セキュリティ早期警戒パートナーシップ～

- 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「ソフトウエア等脆弱性関連情報取扱基準」に基づき運用されている。



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

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

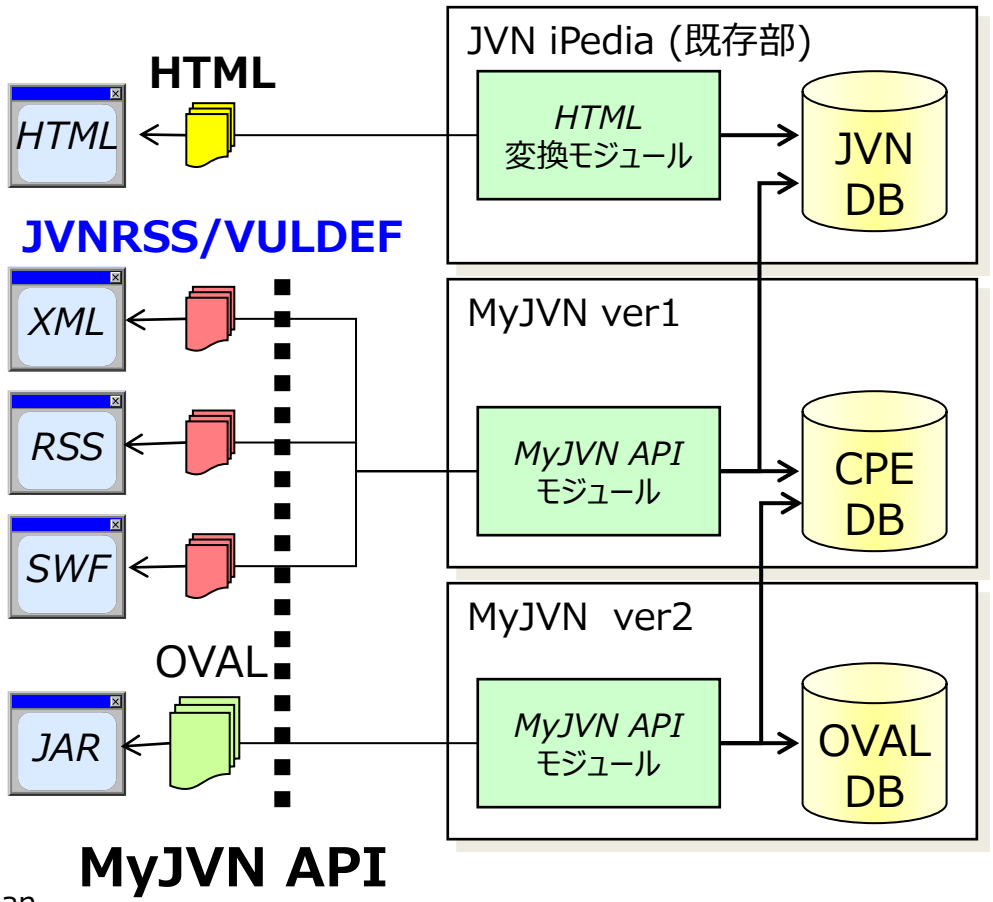
JVN
製品開発者と調整した脆弱性対策情報をタイムリーに公開する

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エアインタフェース
  ⇒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



ソフトウエ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

ソフトウエア辞書とのデータ連携
～2014年の振り返り～

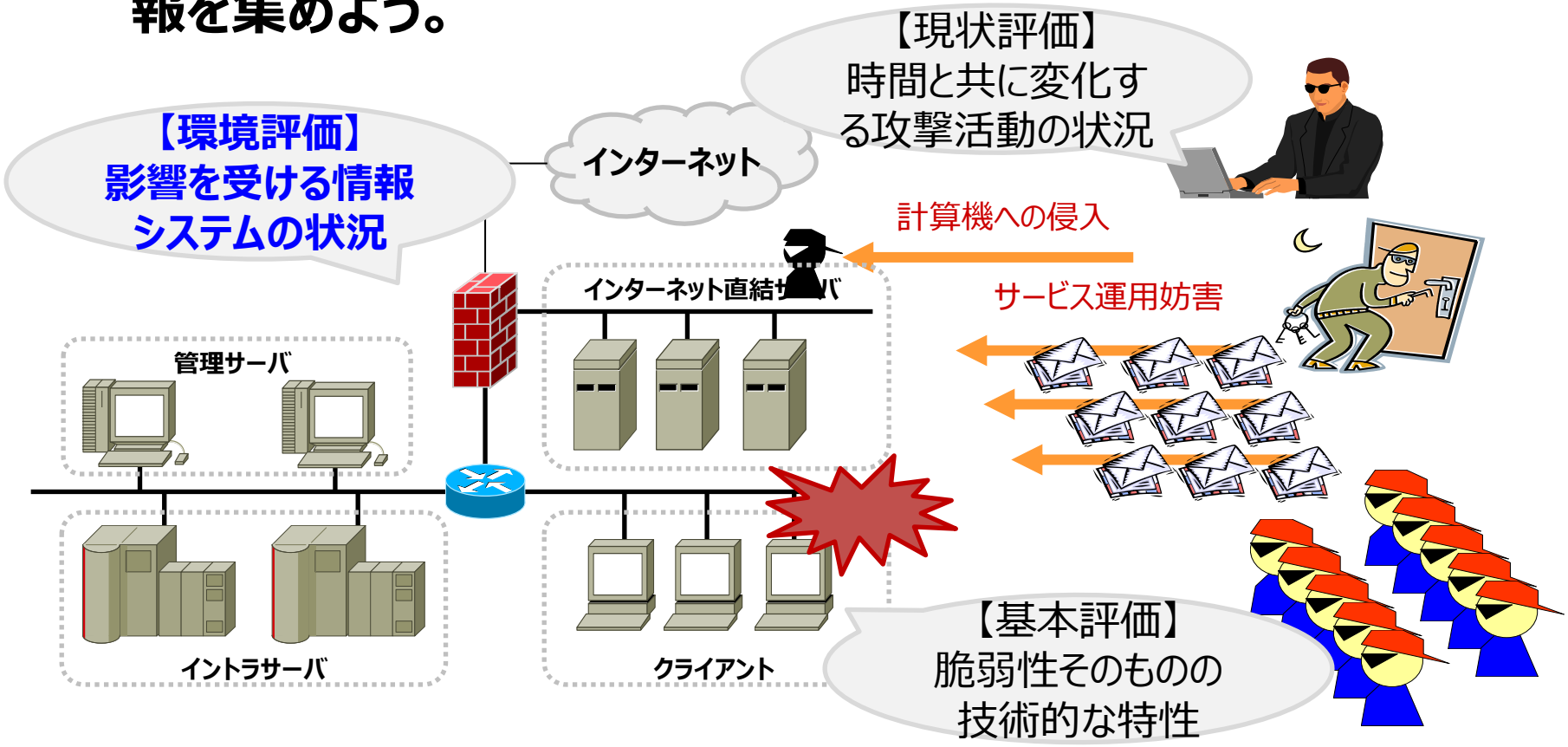
IPA

- **2014年4月**
  OpenSSL 情報漏えいを許してしまう脆弱性
  ～Heartbleed 問題～
- **2014年4月**
  Struts: ClassLoader の操作を許してしまう脆弱性
- **2014年9月**
  GNU bash の脆弱性 ～shellshock 問題～

脆弱性対策には、システム、資産、データ、機能に対するサイバーセキュリティリスクの管理(リソース把握・管理)が必要であることが再認識された。

ソフトウエア辞書とのデータ連携
～影響を受ける情報システムの状況～

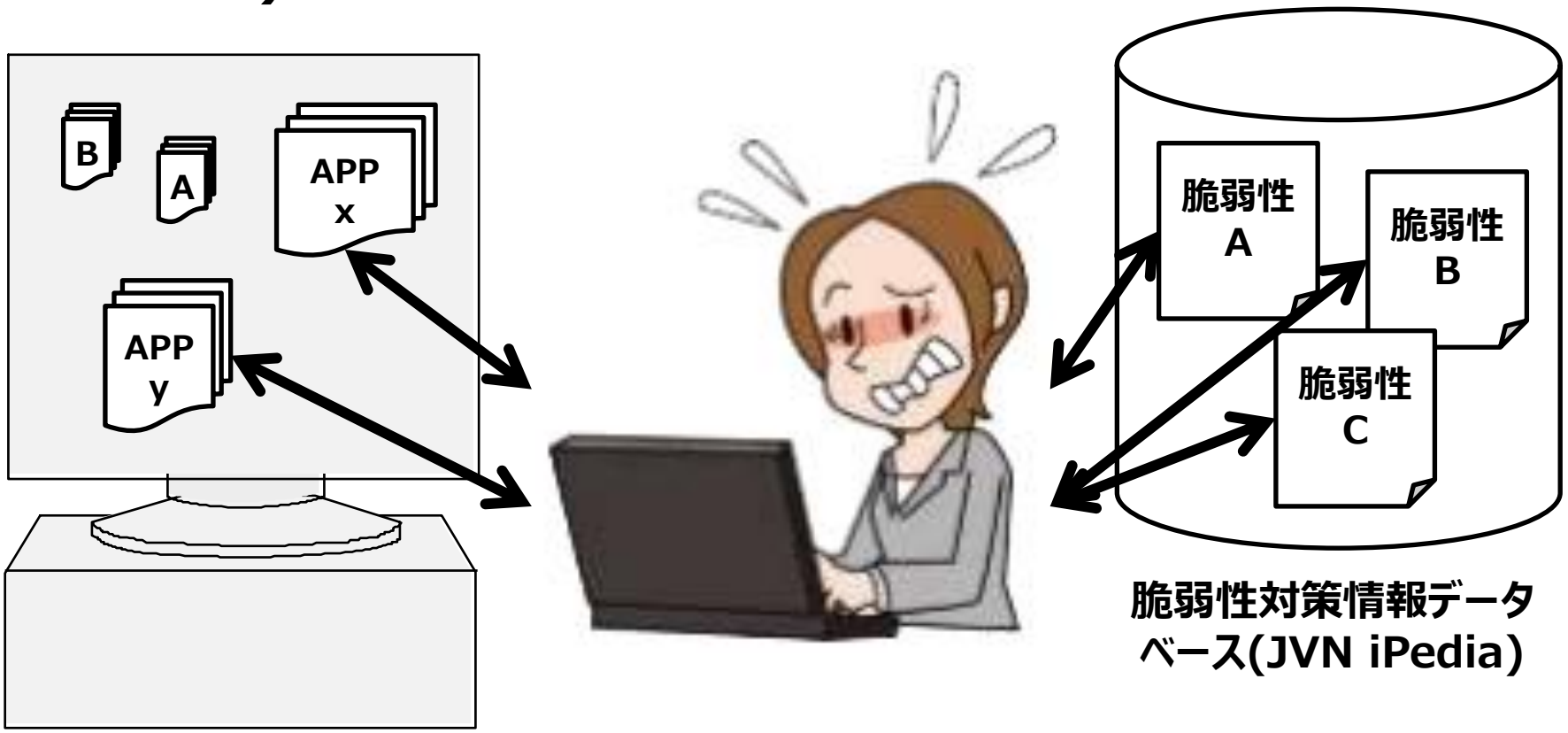
- どこが影響を受けるのか?
  ＝資産管理と連携して、自組織で利用している脆弱性関連情報を集めよう。



ソフトウエ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～

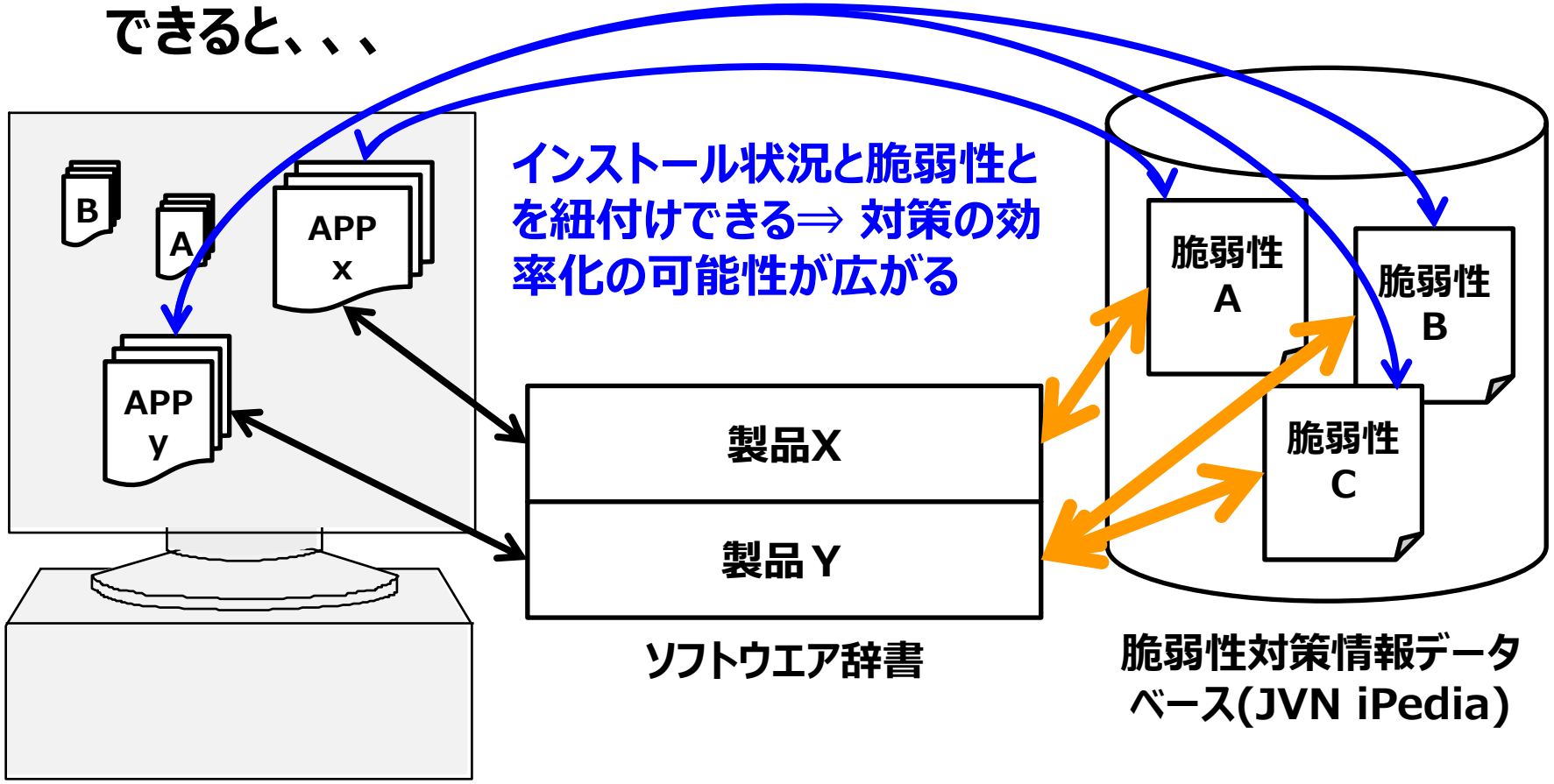
IPA

- 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とが連携できているわけではない)。



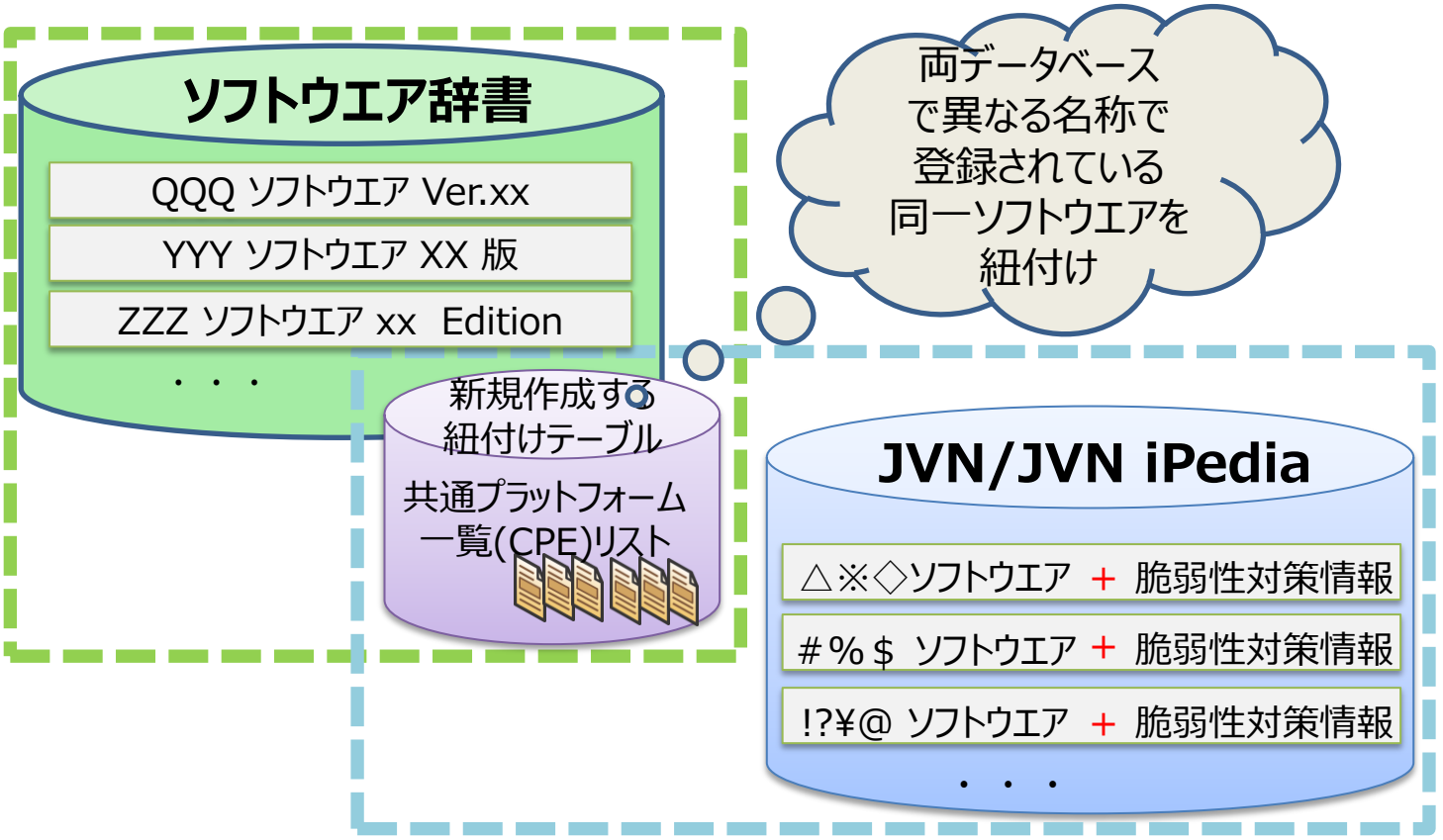
ソフトウエア辞書とのデータ連携
～インストール状況と脆弱性との紐付け～

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



ソフトウエ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**
  ソフトウエ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エアを関連付けること



ソフトウエア辞書とのデータ連携
～SAMACソフトウエア辞書～

- **SAMAC(一般社団法人ソフトウエ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
  - ソフトウエア辞書に登録されている項目は、ベンダ名、ソフトウエア名、エディション、バージョン、ソフトウエア種別(有償ソフトウエア・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

ソフトウエ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～

IPA

- **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、ソフトウエアの名称を、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

ソフトウエ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～

IPA

- インストール状況を把握できるSAMACソフトウエア辞書に連携用項目に製品識別子CPEを用いた製品を追記

SAMAC ソフトウエア 辞書

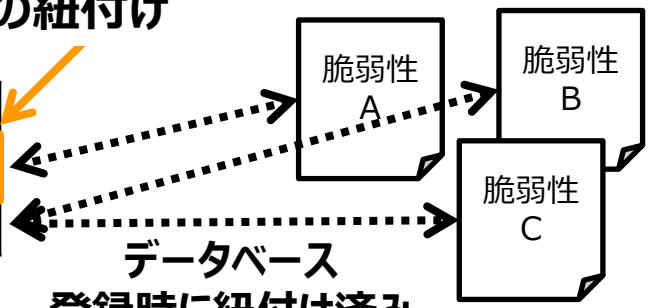
SAMACソフトウエア辞書の既存登録項目(9項目)				連携用項目(1項目)
sw_id	sw_vendor	sw_name	その他項目	CPE v2.2
・・・	・・・	Adobe Acrobat 8.2.0 Professional	・・・	cpe:/a:adobe:acrobat
・・・	・・・	Adobe Acrobat 8.2.0 Standard	・・・	cpe:/a:adobe:acrobat
・・・	・・・	Adobe Acrobat 8.2.1 - CPSID_50570	・・・	cpe:/a:adobe:acrobat
・・・	・・・	Adobe Acrobat 8.2.1 Professional	・・・	cpe:/a:adobe:acrobat
・・・	・・・	Adobe Acrobat 8.2.1 Standard	・・・	cpe:/a:adobe:acrobat
・・・	・・・	Adobe Acrobat 9.3.0 - CPSID_52073	・・・	cpe:/a:adobe:acrobat

ソフトウエアの 脆弱性 データベース

製品識別子CPEを用いた製品の紐付け

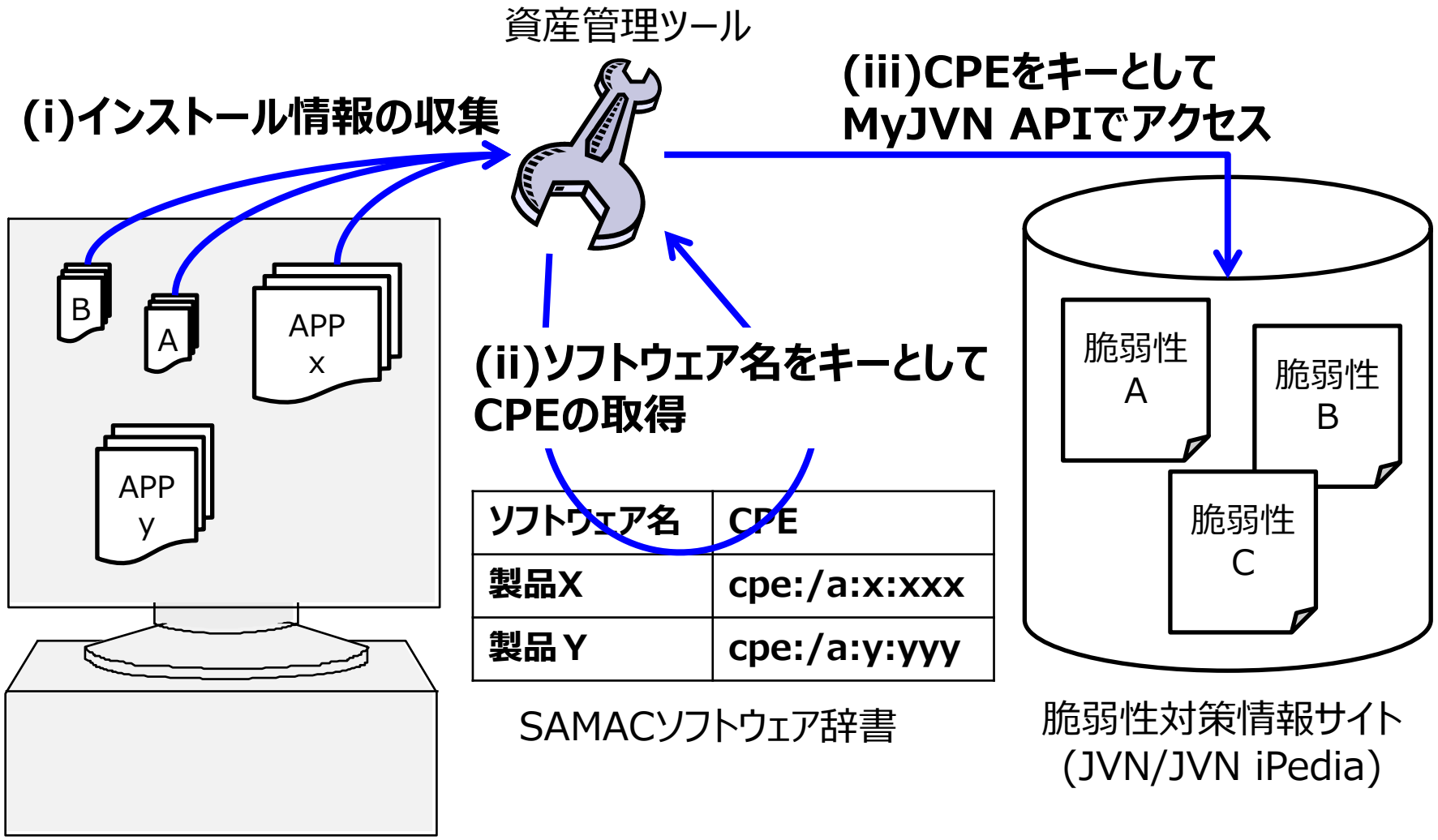
ソフトウエア名	CPE v2.2
Adobe Acrobat	cpe:/a:adobe:acrobat
製品Y	cpe:/a:y:yyy

JVN製品データベース



データベース 登録時に紐付け済み

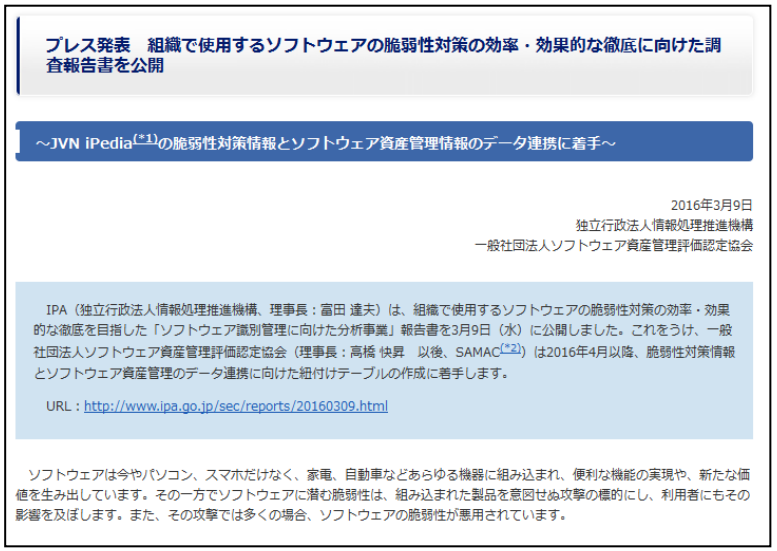
ソフトウエア辞書とのデータ連携
～脆弱性対策情報参照までの流れ～



ソフトウエ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

最後に

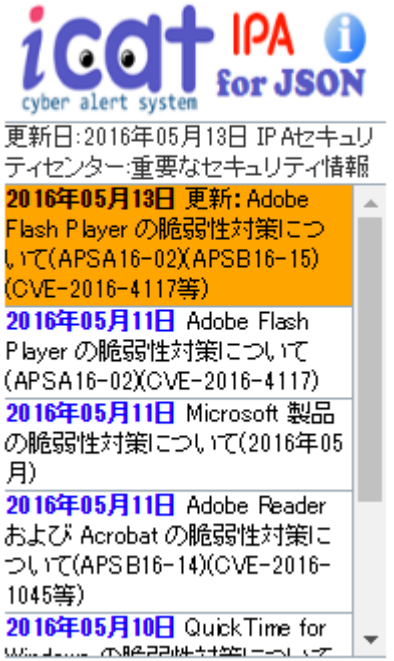
日々の脆弱性関連情報の収集だけではなく、資産管理と連携させた対策を進めることで、サイバーセキュリティリスクの管理を加味した脆弱性対策を実現していく必要があります。
JVN脆弱性対策機械処理基盤では、共通基準／共通仕様の活用、データ連携により、これら脆弱性対策を支援する基盤の整備を進めています。
脆弱性に対して適切な対応をとっていきましょう。

参考情報
～サイバーセキュリティ注意喚起サービス icat for JSON ～

https://www.ipa.go.jp/security/vuln/icat.html

- **IPAが発信する「重要なセキュリティ情報」をリアルタイムに同期できます。**
- **社内のポータルサイトなどにHTMLタグを埋込んでご利用ください。**

[表示例]



- **利用時に埋め込むHTMLタグ**

[jQueryを使用していないウェブページの場合]

```
<script type="text/javascript" src="//code.jquery.com/jquery-1.11.3.min.js"> </script>
<script type="text/javascript" src="//www.ipa.go.jp/security/announce/irss/icath.js">
</script>
```


IPA
Better Life
with IT