IPA Better Life with IT

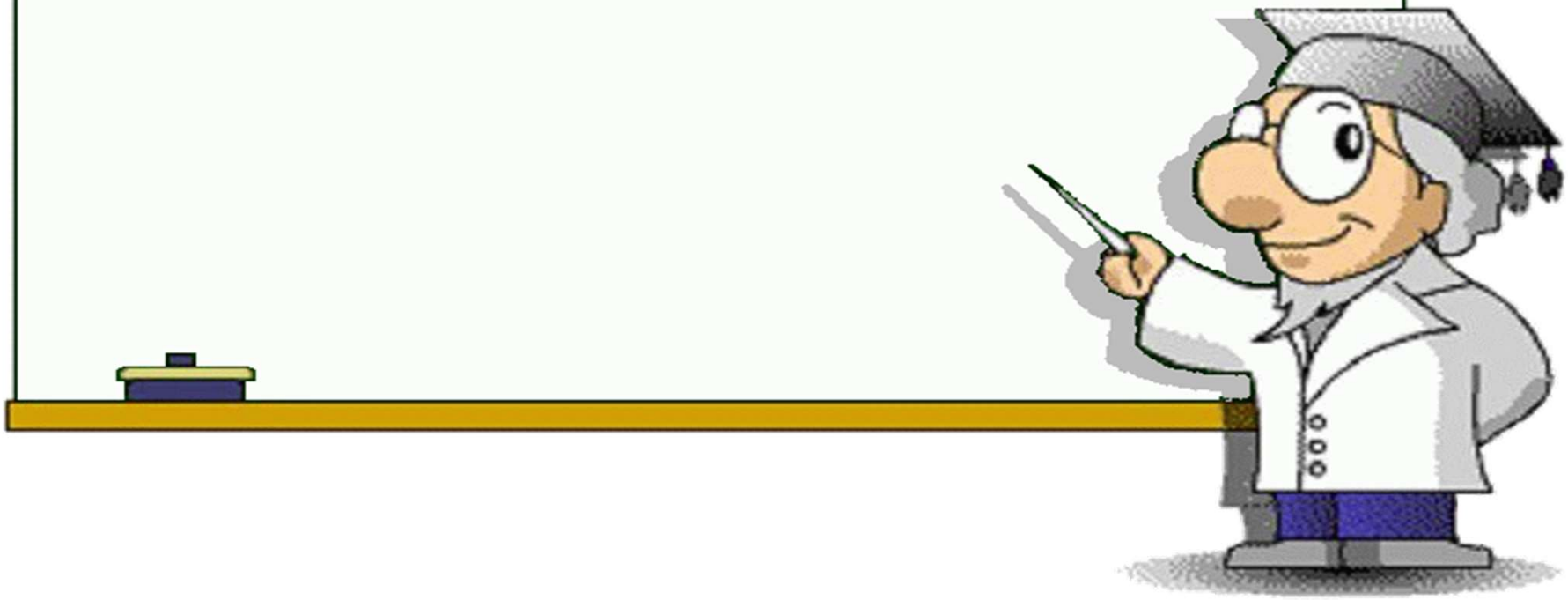
IT資産とサイバーセキュリティ対策

2017/06/09

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

IPAへの脆弱性届出状況について報告すると共に、IPAが取り組んでいる脆弱性対策促進施策を、脆弱性を作りこまない、安全に運営する、問題有無を確認するという3つの視点から紹介します。



目次

- 情報セキュリティ10大脅威 2017
- 脆弱性届出の状況
- 脆弱性を作りこまない
- 安全に運営する
- 問題有無を確認する
- ソフトウエア辞書とのデータ連携

情報セキュリティ10大脅威 2017

- **2016年に発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案から選出**

昨年	個人	順位	組織	昨年
1位	インターネットバンキングやクレジットカード情報の不正利用	1位	標的型攻撃による情報流出	1位
2位	ランサムウェアによる被害	2位	ランサムウェアによる被害	7位
3位	スマートフォンやスマートフォンアプリを狙った攻撃	3位	ウェブサービスからの個人情報の窃取	3位
5位	ウェブサービスへの不正ログイン	4位	サービス妨害攻撃によるサービスの停止	4位
4位	ワンクリック請求等の不当請求	5位	内部不正による情報漏えいとそれに伴う業務停止	2位
7位	ウェブサービスからの個人情報の窃取	6位	ウェブサイトの改ざん	5位
6位	ネット上の誹謗・中傷	7位	ウェブサービスへの不正ログイン	9位
8位	情報モラル欠如に伴う犯罪の低年齢化	8位	IoT機器の脆弱性の顕在化	ランク外
10位	インターネット上のサービスを悪用した攻撃	9位	攻撃のビジネス化(アンダーグラウンドサービス)	ランク外
ランク外	IoT機器の不適切な管理	10位	インターネットバンキングやクレジットカード情報の不正利用	8位

最近、
脆弱性という言葉を耳にしませんか？

Struts2の脆弱性突く不正アクセス、4年前にもStruts2で被害

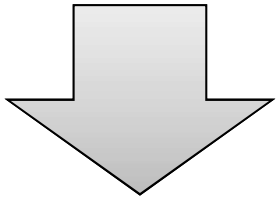
WordPressの脆弱性突く攻撃が激増、
6万以上のWebサイトで改ざん被害

新聞から

ウェブニュースから

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)

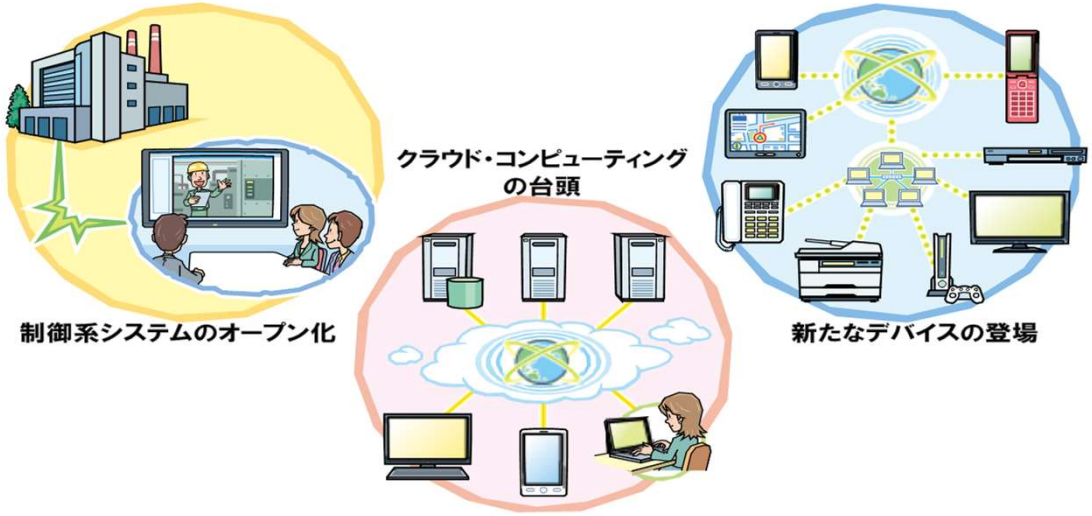


言い換えれば

- **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

脆弱性を取り巻く環境の変化
～海外では脆弱性売買が行われている～

- 脆弱性発見者に報奨金を支払う制度が一般化

- 大手製品ベンダ、大手ウェブサービスベンダなどが採用
- 脆弱性種別によっては、最大10万$の報奨金
- 脆弱性発見を専門とする企業出現(ビジネス化)
- 報奨金を競うコンテストも開かれている

脆弱性を取り巻く環境の変化
～振り返り 2014年～

- 2014年4月
  OpenSSLの情報漏えいを許してしまう脆弱性 ~ Heartbleed問題 ~
- 2014年4月
  Apache Strutsの任意のコード実行を許してしまう脆弱性
- 2014年9月
  GNU bashの脆弱性 ~ shellshock問題 ~
- 2014年10月
  SSL通信の暗号文の解読を許してしまう脆弱性 ~ POODLE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。

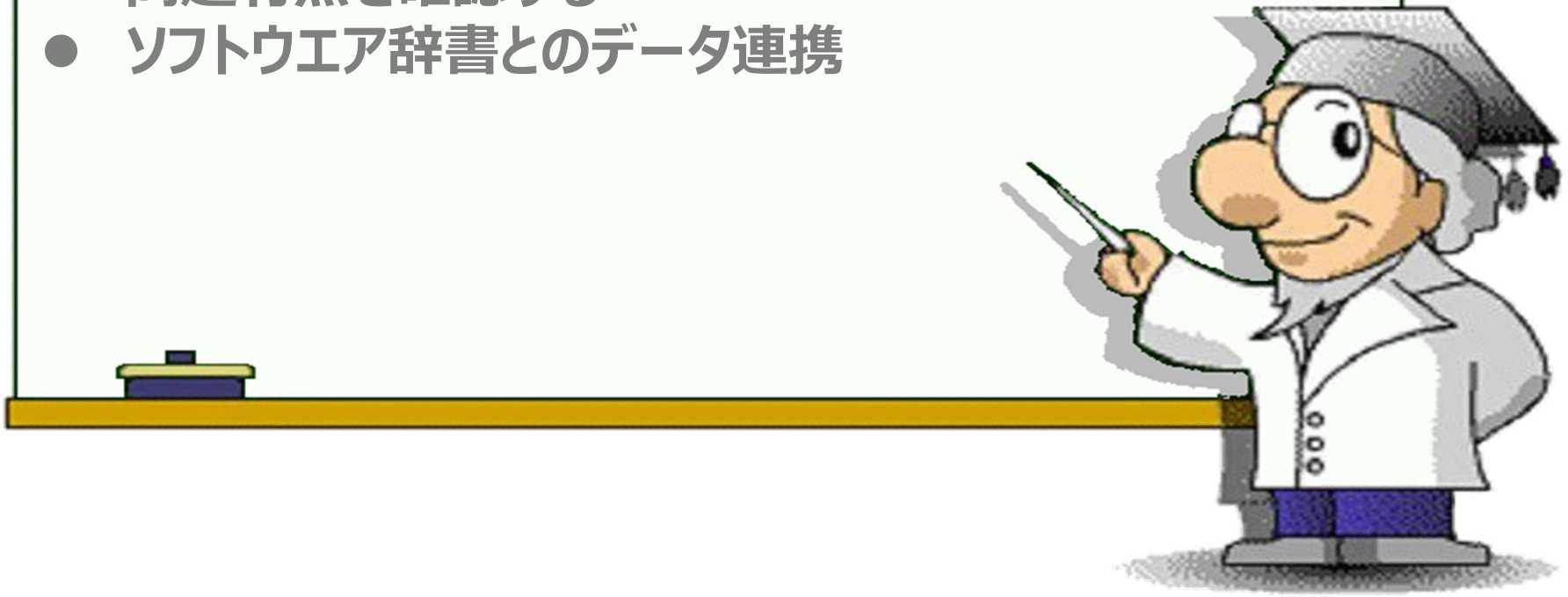
脆弱性を取り巻く環境の変化
～振り返り 2017年～

- 2017年3月
  Apache Struts 2の任意のコード実行を許してしまう脆弱性
- 2017年5月
  ランサムウェアWanna Cryptorの流布
  2017年3月にセキュリティ更新プログラムがリリースされた
  「MS17-010：Windows SMBv1の任意のコード実行を許してしまう
  脆弱性」を悪用

**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。**

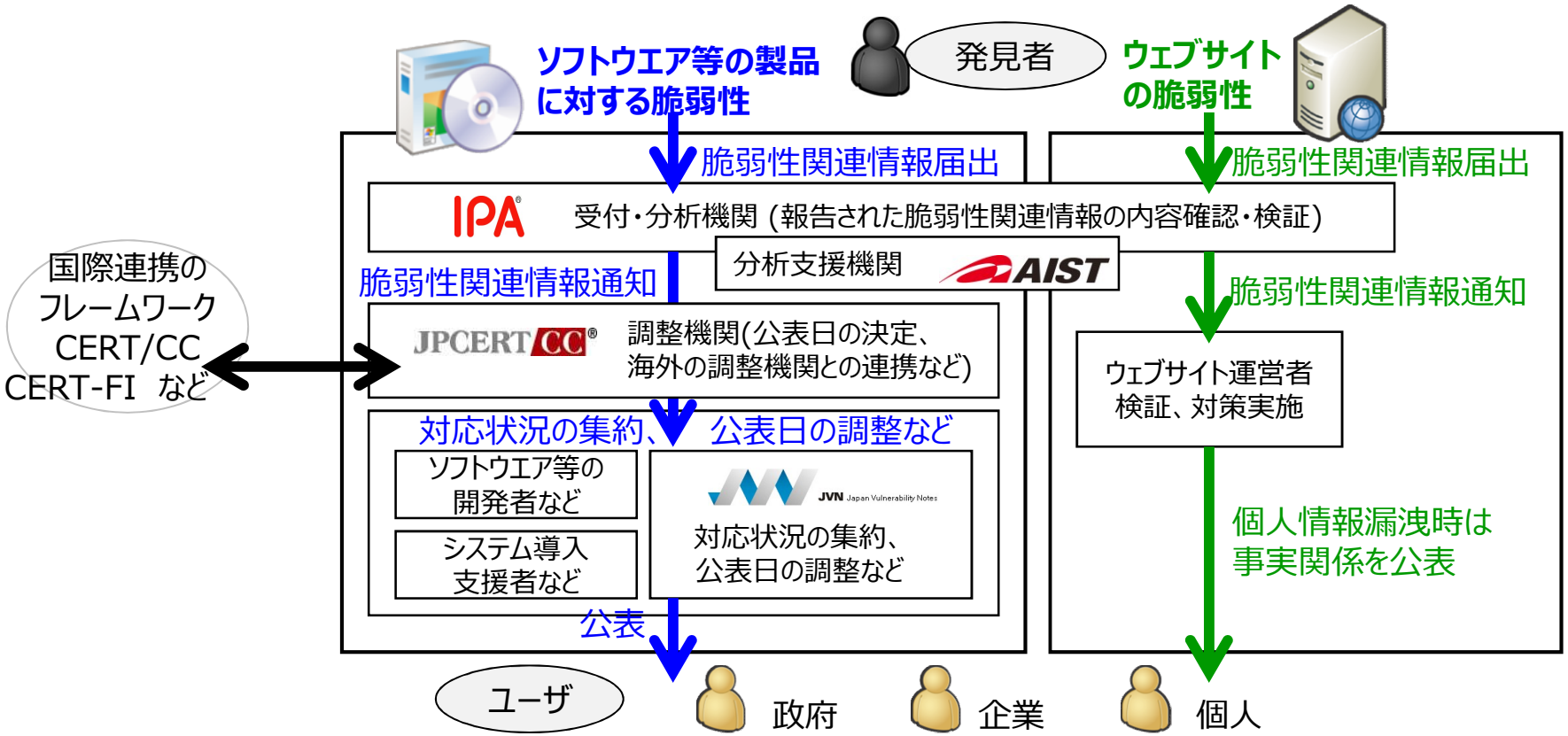
目次

- 情報セキュリティ10大脅威 2017
- **脆弱性届出の状況**
- 脆弱性を作りこまない
- 安全に運営する
- 問題有無を確認する
- ソフトウエア辞書とのデータ連携



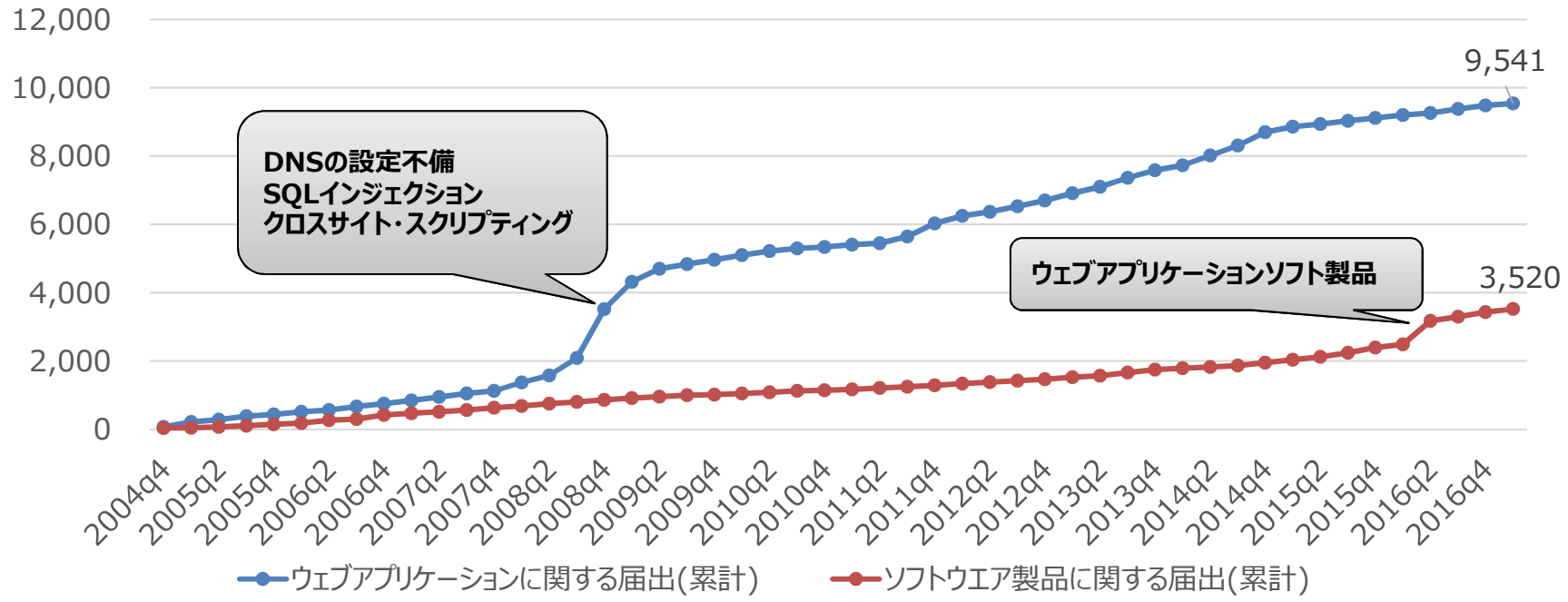
脆弱性届出の状況
～情報セキュリティ早期警戒パートナーシップ～

- 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。



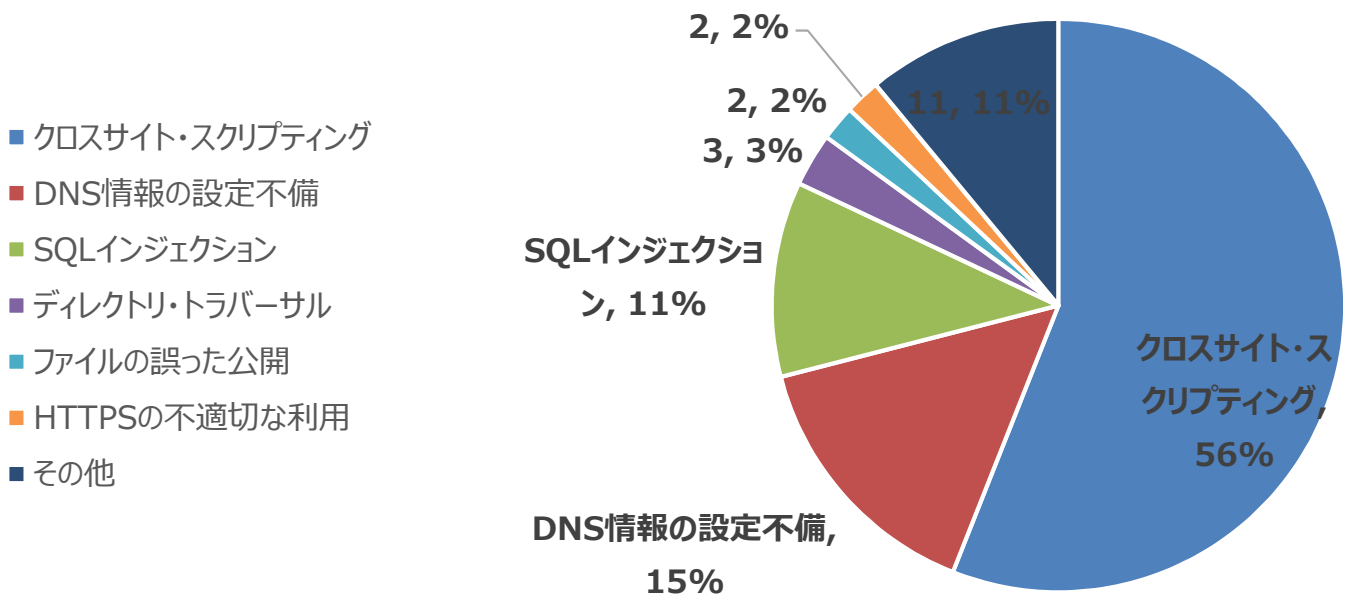
脆弱性届出の状況
～概況～

- 届出は年々増加しており、2017年q1で13,061件に達した。
- 2008年q3頃からウェブサイトにおけるDNSの設定不備、SQLインジェクションの脆弱性の届出が増加し、また、2008年q4に一時的にクロスサイト・スクリプティングの脆弱性の届出が激増した。
- 2016年q2の増加はウェブアプリケーションソフト製品の多数届出による。



脆弱性届出の状況
～概況～

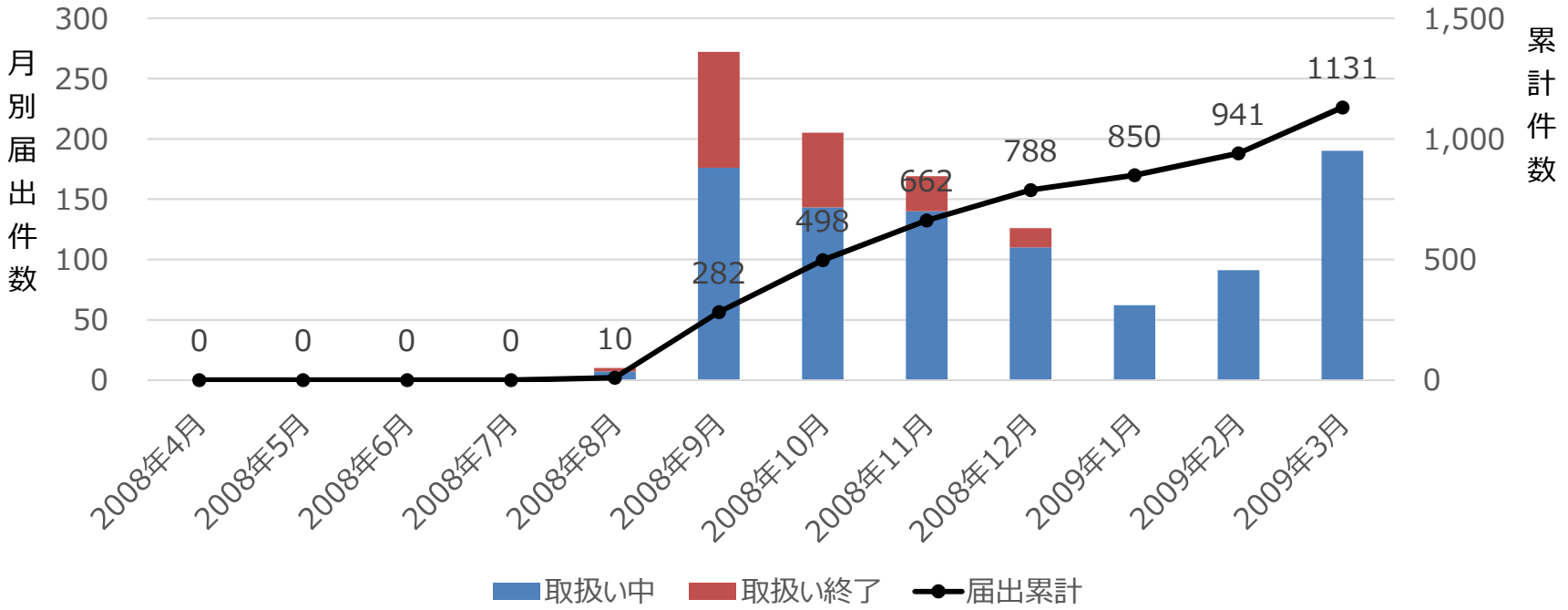
- ウェブサイトの脆弱性の種類別の届出累計のトップ3は、クロスサイト・スクリプティング、DNSの設定不備、SQLインジェクション
- 2017年第一四半期はクロスサイト・スクリプティング(28件)、SQLインジェクション(11件)が約半数を占める



ウェブサイトの脆弱性の種類別の届出(累計)

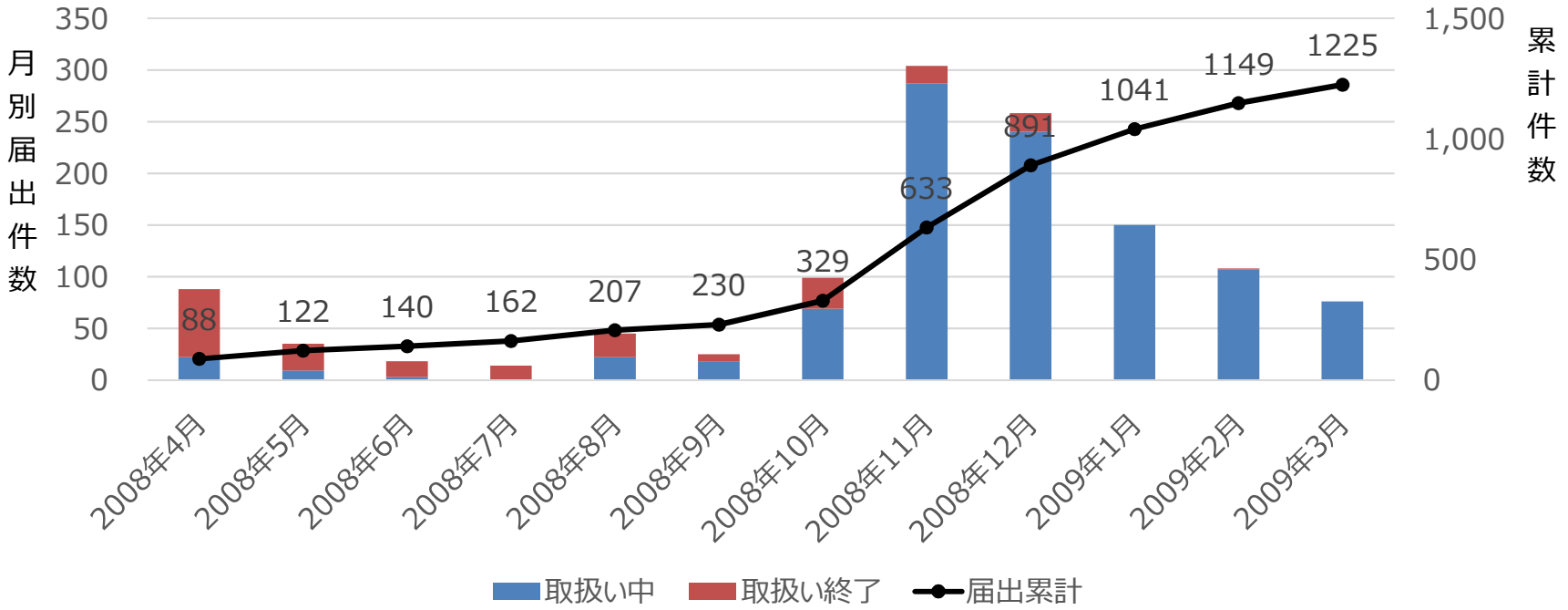
脆弱性届出の状況
～DNSの設定不備の届出～

- 2008年7月に複数のDNSサーバ製品の開発ベンダーからDNSキャッシュポイズニングに関する対策情報が公開された。以降、「実際に運用されているDNSサーバが、脆弱性対策を実施していないのでは？」という旨の届出が継続した。



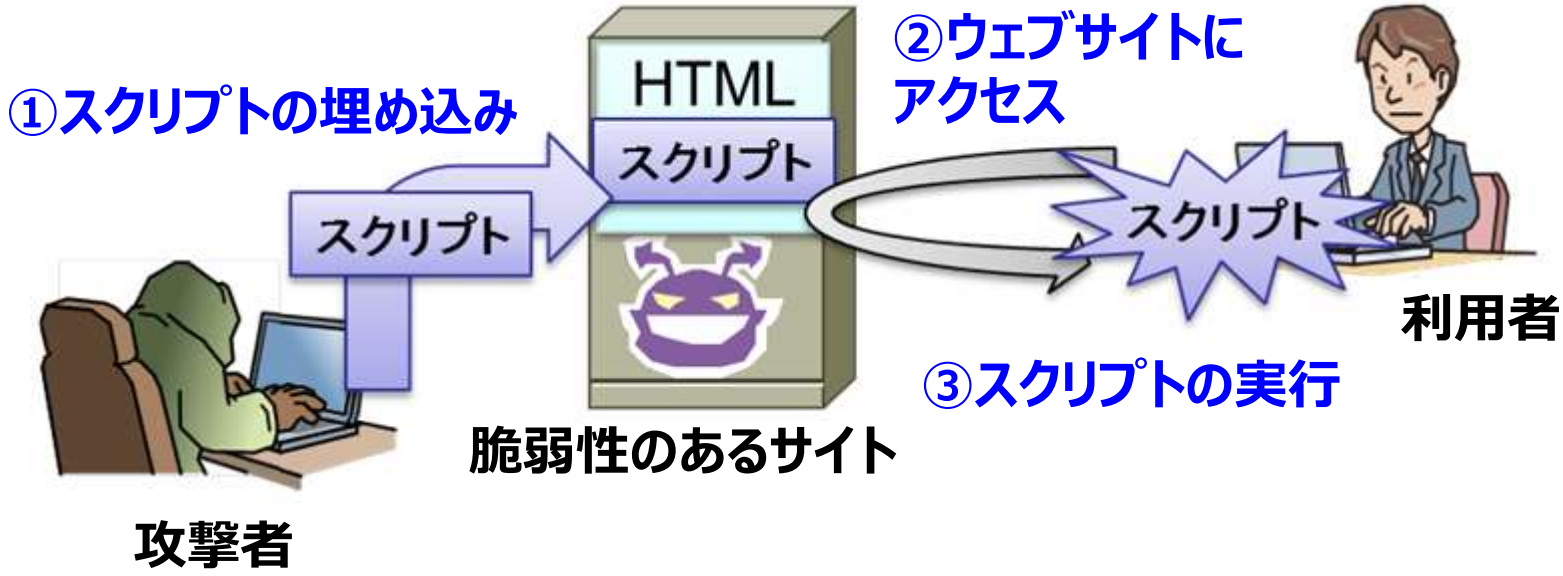
脆弱性届出の状況
～クロスサイト・スクリプティング脆弱性の届出～

- 2000年頃に報告された古典的な脆弱性で、多様な攻撃手法が知られており、近年も届出が継続している。ウェブページの軽微な「出力処理」の追加で脆弱性を作り込んでしまった事例や、脆弱性対策が誤っていた事例などがある。



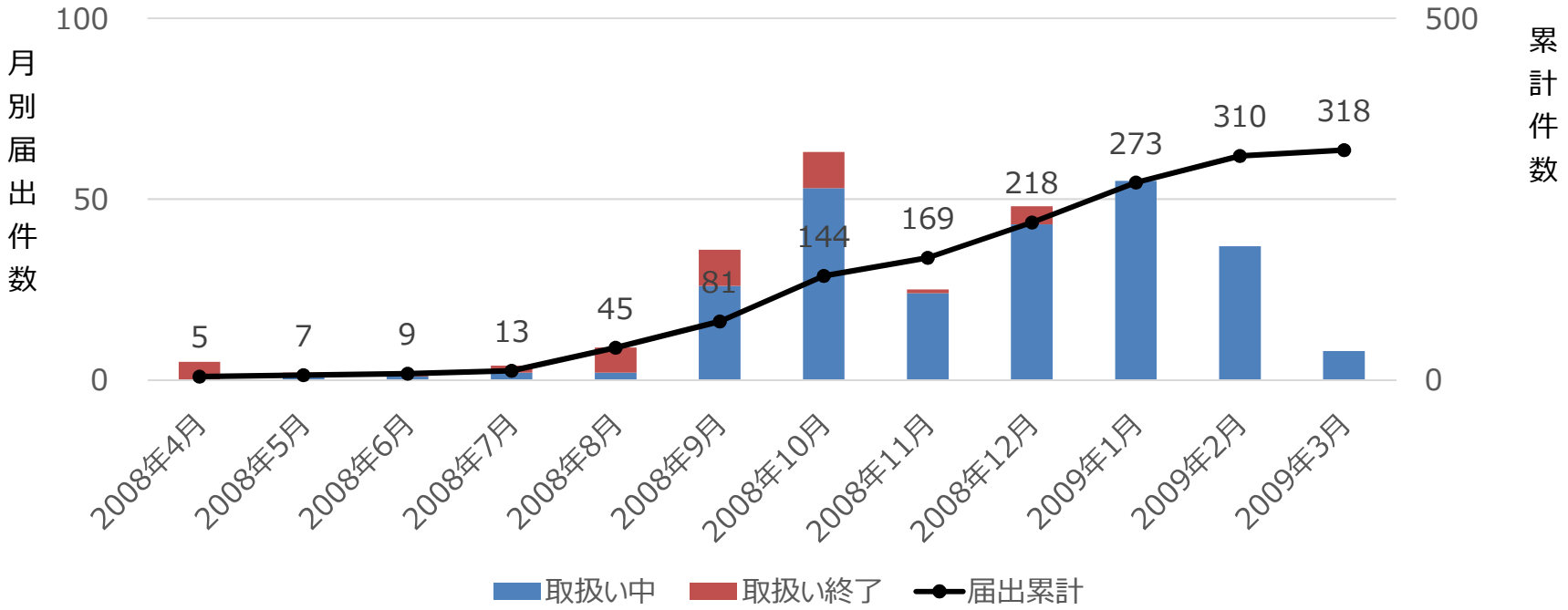
脆弱性届出の状況
～クロスサイト・スクリプティング脆弱性の届出～

- クロスサイト・スクリプティング(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



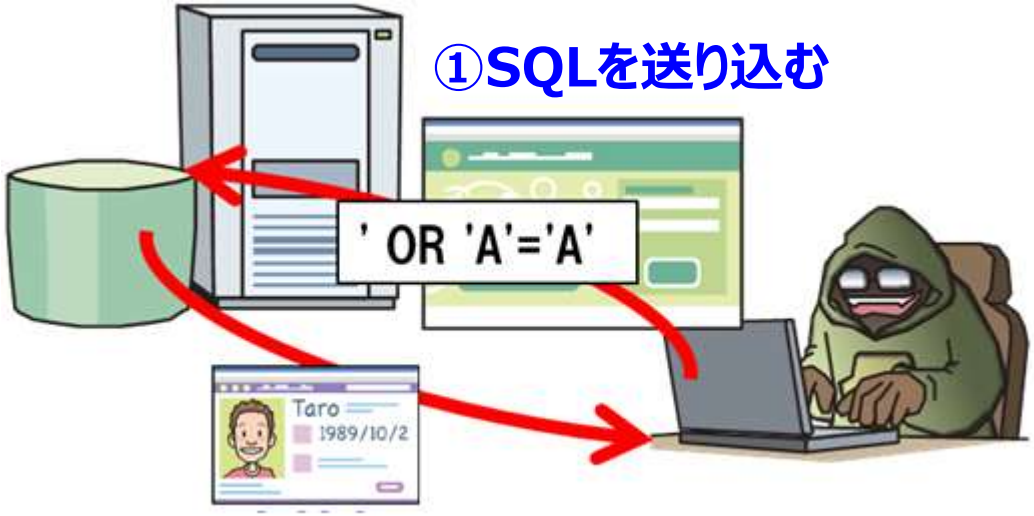
脆弱性届出の状況
～SQLインジェクション脆弱性の届出～

- この脆弱性を悪用した攻撃により、ウェブサイトの情報の改ざんや非公開情報が公開されるなど、深刻な被害が発生している。この被害報道と共に、「実際に運用されているウェブサイトにSQLインジェクションの脆弱性があるのでは？」という旨の届出が継続した。



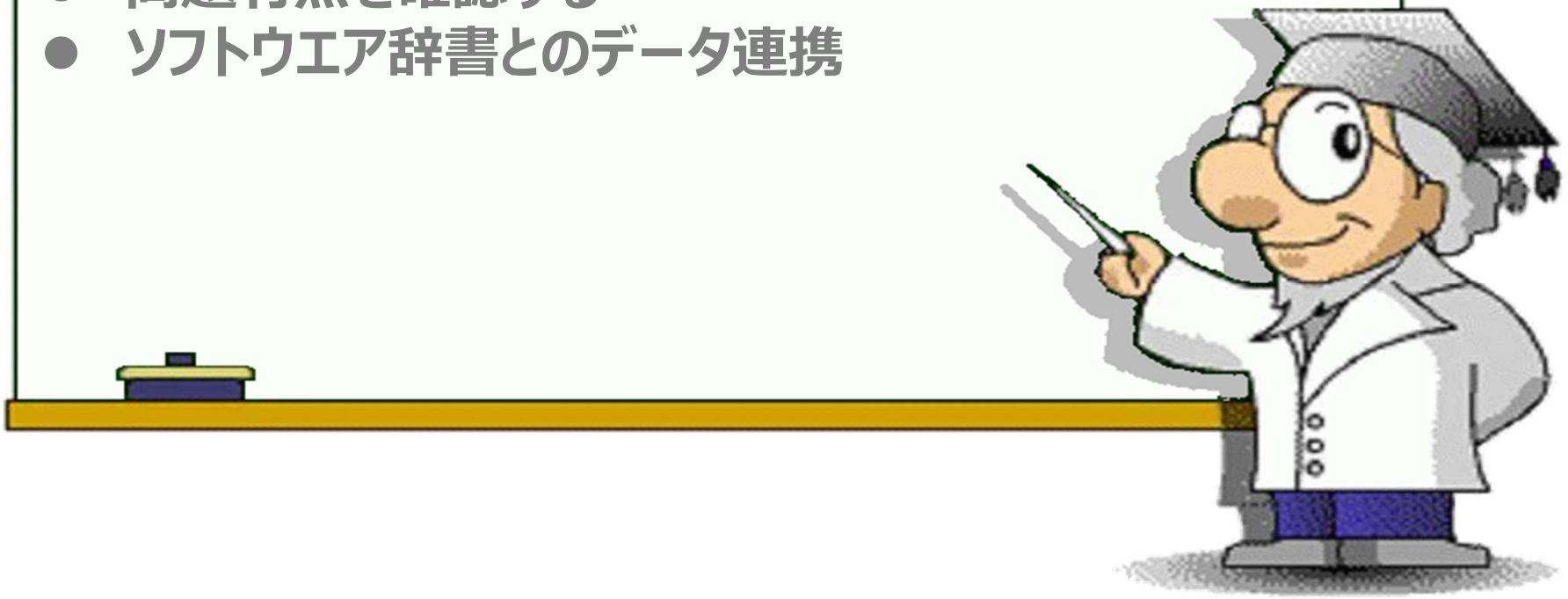
脆弱性届出の状況
～SQLインジェクション脆弱性の届出～

- 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



目次

- 情報セキュリティ10大脅威 2017
- 脆弱性届出の状況
- **脆弱性を作りこまない**
- 安全に運営する
- 問題有無を確認する
- ソフトウエア辞書とのデータ連携



脆弱性を作りこまない

セキュリティを確保したウェブアプリケーションの開発やウェブサイトの構築にはセキュリティ(脆弱性)の知識が必要

- 脅威の仕組みや問題の原因を正しく理解する。
  「知っていますか？脆弱性(ぜいじゃくせい)」
- 安全なプログラムを作成するためのマナーを身に付ける。
  「セキュア・プログラミング講座」
- 失敗から学ぶ。
  「安全なウェブサイトの作り方」

知っていますか？脆弱性

http://www.ipa.go.jp/security/vuln/vuln_contents/index.html

このコンテンツは、ウェブサイトの運営者や一般の利用者の方へ向けて、ウェブサイトにおける代表的な 10 種類の脆弱性（ソフトウェア等におけるセキュリティ上の弱点）について、わかりやすくアニメーションで解説しています。

これらの問題は、根本的にはウェブサイトの運営者が対策を行うべき問題です。しかし、一般の利用者の方も、保険的な対策を取ることで、ウェブサイトの脆弱性が原因となって起こる問題の被害を未然に防いだり、抑えることができます。詳細は、各解説および対策ページをご覧ください。

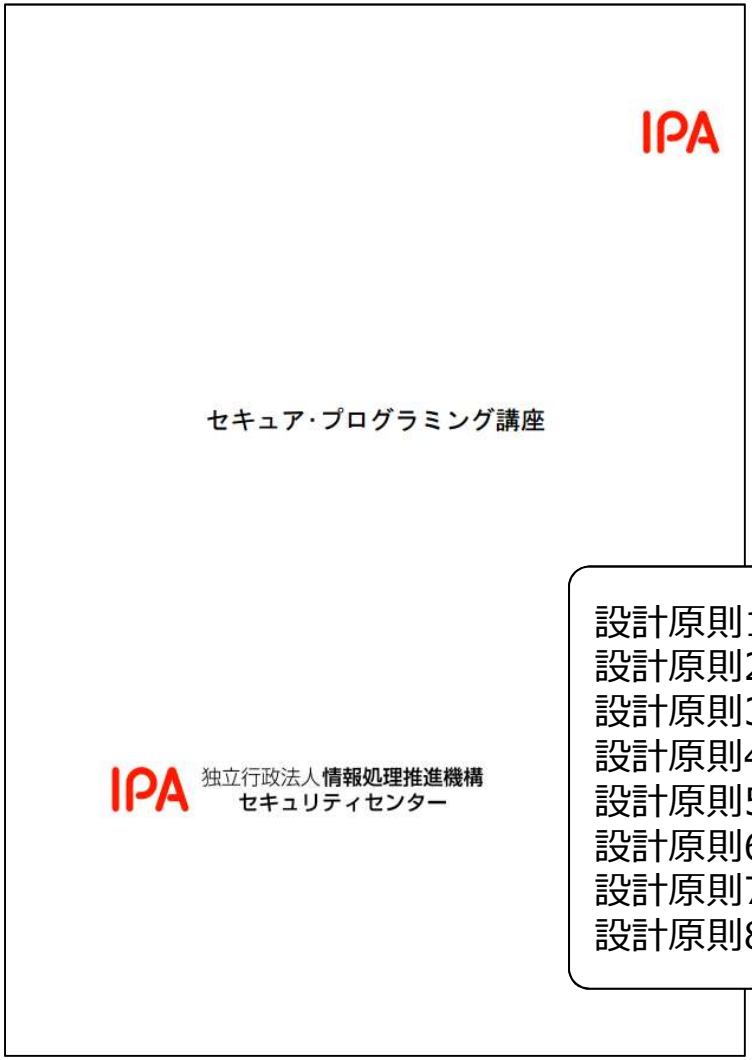
1		●SQLインジェクション ～ショッピングサイトの個人情報が盗まれてしまった！～	▶Flash版	▶HTML版
2		●クロスサイト・スクリプティング ～フィッシング詐欺に悪用されてしまった！～	▶Flash版	▶HTML版
3		●CSRF（クロスサイト・リクエスト・フォージェリ） ～SNS で自分の日記が勝手に公開されてしまった！どうして？～	▶Flash版	▶HTML版
4		●パス名パラメータの未チェック/ディレクトリ・トラバーサル ～ウェブサイトの非公開ファイルが漏洩！？～	▶Flash版	▶HTML版
5		●OSコマンド・インジェクション ～ウェブサイトを乗っ取られてしまった！踏み台ってどういうこと？～	▶Flash版	▶HTML版
6		●セッション管理の不備 ～オンラインショッピングでなりすまし！？～	▶Flash版	▶HTML版
7		●HTTPヘッダ・インジェクション ～続・フィッシング詐欺に悪用されてしまった！～	▶Flash版	▶HTML版
8		●HTTPSの不適切な利用 ～証明書の更新はお忘れなく～	▶Flash版	▶HTML版
9		●サービス運用妨害（DoS） ～急にウェブサイトが見られない！どうして？～	▶Flash版	▶HTML版
10		●メール不正中継 ～知らないうちに迷惑メールの発信元に！～	▶Flash版	▶HTML版

脅威の仕組みや問題の原因を正しく理解する。

- ウェブサイトの運営者や　一般の利用者向け
- ウェブサイトにおける代表的な10種類の脆弱性(クロスサイト･スクリプティング、SQLインジェクションなど)について、アニメーションで解説

セキュア・プログラミング講座

http://www.ipa.go.jp/security/awareness/vendor/programming/index.html



安全なプログラムを作成するためのマナーを身に付ける。

- **脆弱性を作りこまないために設計時と実装時のそれぞれで意識すべき原則について説明**

設計原則1. Economy of mechanism：効率的なメカニズム
設計原則2. Fail-safe defaults：フェイルセーフなデフォルト
設計原則3. Complete mediation：完全な仲介
設計原則4. Open design：オープンな設計
設計原則5. Separation of privilege：権限の分離
設計原則6. Least privilege：最小限の権限
設計原則7. Least common mechanism：共通メカニズムの最小化
設計原則8. Psychological acceptability：心理学的受容性

安全なウェブサイトの作り方

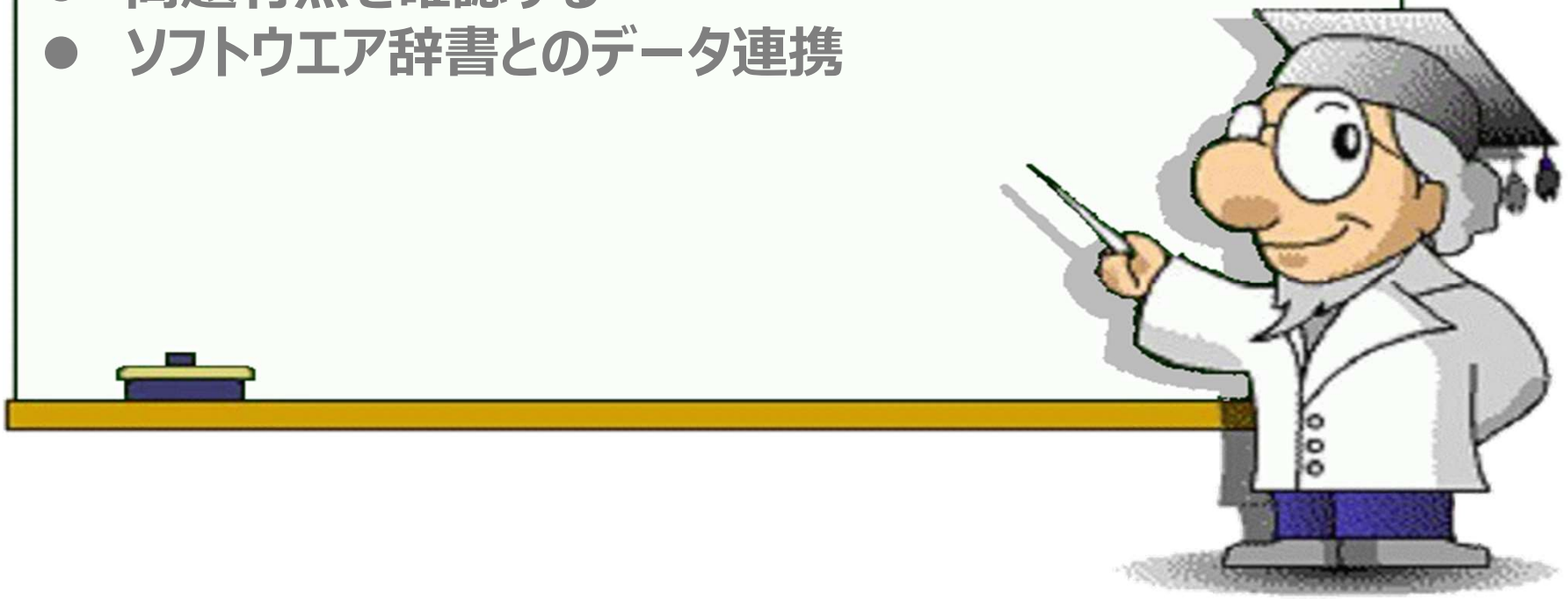
http://www.ipa.go.jp/security/vuln/websecurity.html

失敗から学ぶ。

- IPAに届出られた脆弱性関連情報をもとに、対策をまとめたガイド
- 脆弱性ごとに解説と「根本的解決」「保険的対策」を記載
- 「失敗例」について記載
- ウェブセキュリティの実装状況のチェックリストつき

目次

- 情報セキュリティ10大脅威 2017
- 脆弱性届出の状況
- 脆弱性を作りこまない
- **安全に運営する**
- 問題有無を確認する
- ソフトウエア辞書とのデータ連携



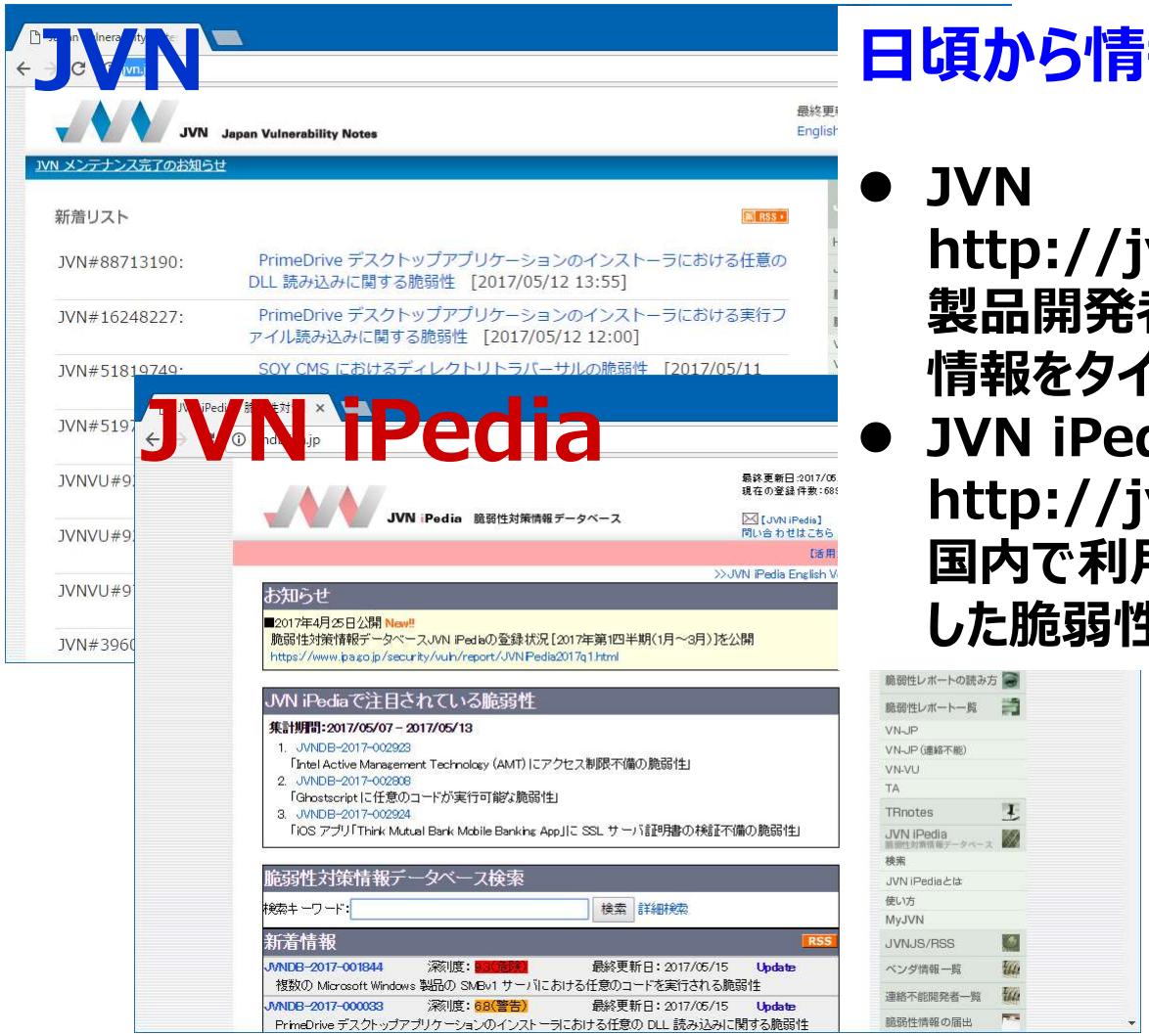
安全に運営する

脆弱性は日々発見されるため、脆弱性情報を継続的に入手し、ソフトウェアの更新や問題の回避が必要
事件や事故が発生した場合の被害を想定し、事前に対策を準備することが必要

- 日頃から情報収集に心がける。
  「脆弱性対策情報サイト」
  「サイバーセキュリティ注意喚起サービス icat」
  「セキュリティ対策情報発信サービス for Twitter」

脆弱性対策情報サイト

http://jvn.jp/　　http://jvndb.jvn.jp/

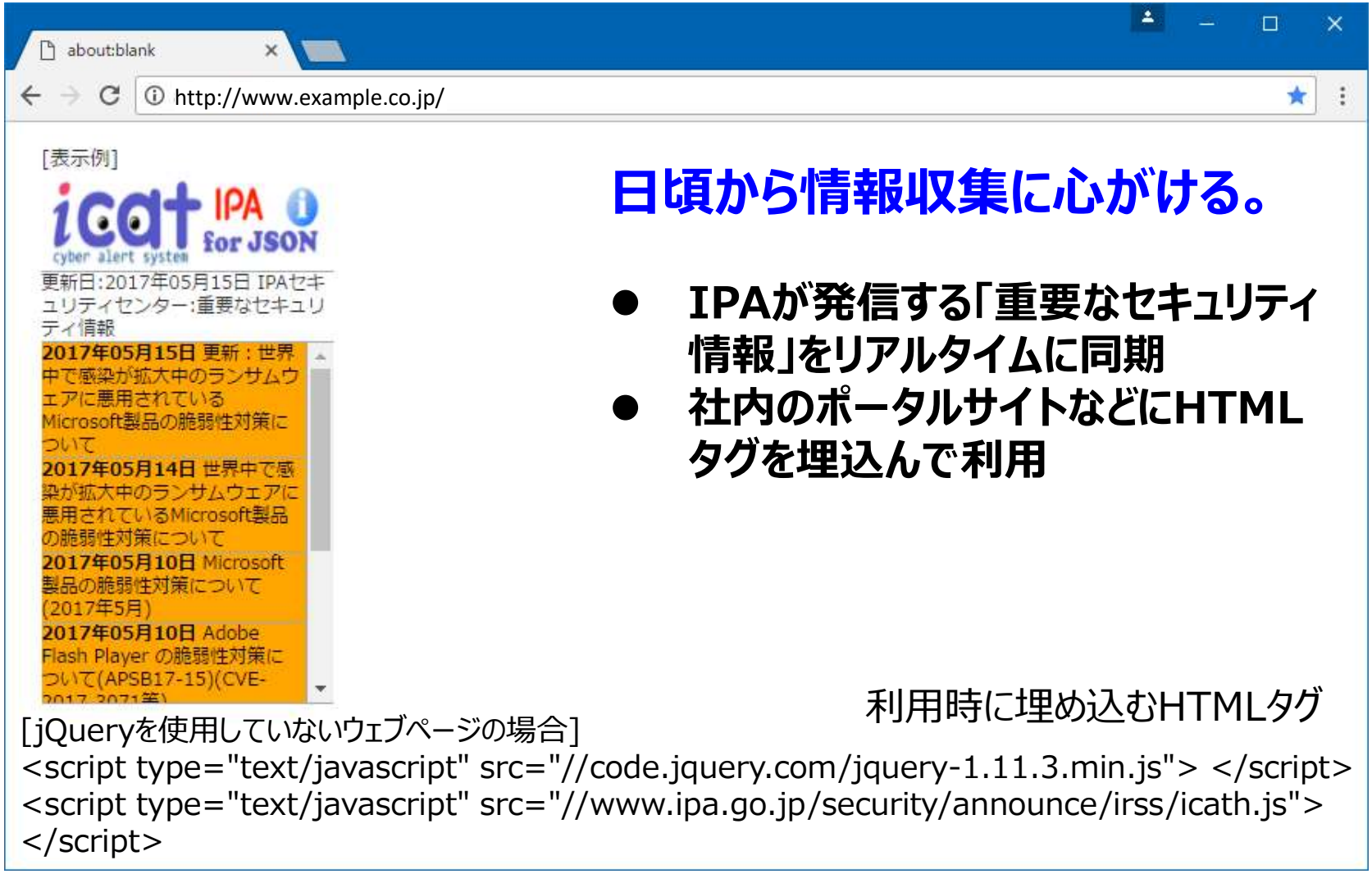


日頃から情報収集に心がける。

- **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
- **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網羅し蓄積

サイバーセキュリティ注意喚起サービス

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



セキュリティ対策情報発信サービス

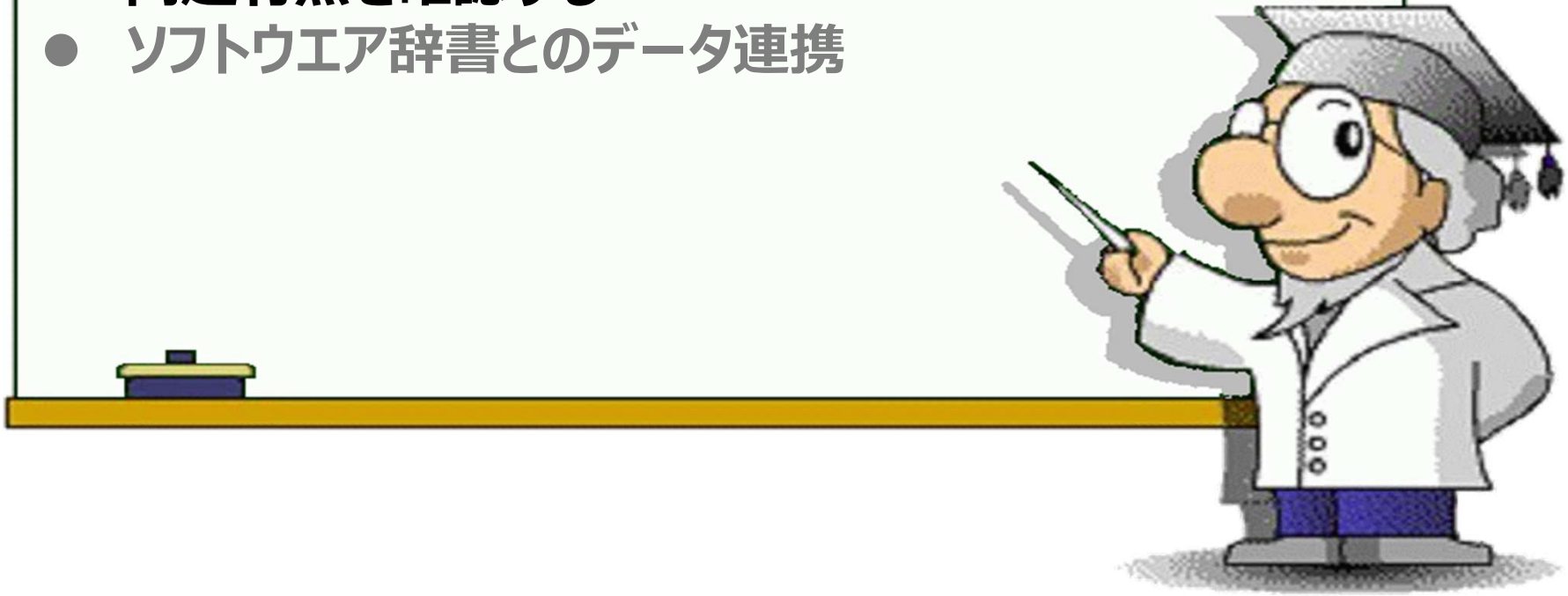
http://www.ipa.go.jp/security/vuln/twitter_policy.html

日頃から情報収集に心がける。

- @JVNiPedia
  脆弱性対策情報データベース JVN iPediaの新規登録情報
- @MyJVN
  MyJVN バージョンチェッカの更新情報
- @ICATalerts
  緊急対策情報

目次

- 情報セキュリティ10大脅威 2017
- 脆弱性届出の状況
- 脆弱性を作りこまない
- 安全に運営する
- **問題有無を確認する**
- ソフトウエア辞書とのデータ連携



問題有無を確認する

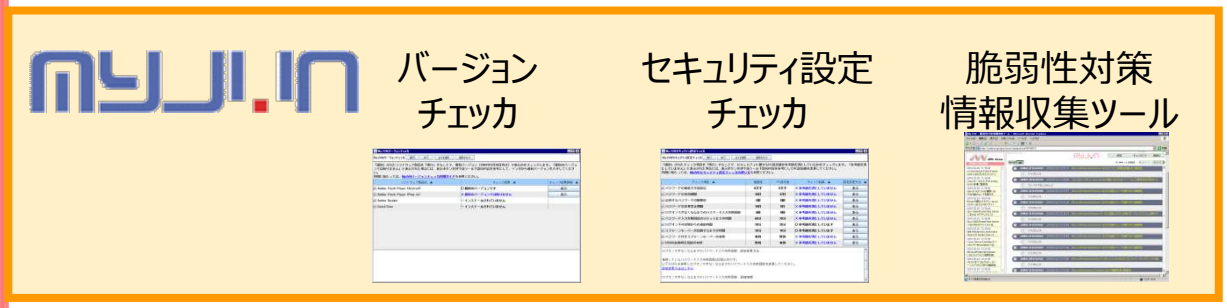
セキュリティに関する作業を手作業で行なうと、設定ミスや管理者のセキュリティ知識の程度や判断の相違などによりセキュリティ要件を損なう可能性大

⇒ 脆弱性対策に関わる基盤の整備

- 製品視点から脆弱性対策情報を選別する。
  「MyJVN 脆弱性対策情報フィルタリング収集ツール(略称：mjcheck3)」
- ソフトウェアのバージョンが最新であるかを確認する。
  「MyJVNバージョンチェッカ」

脆弱性対策に関わる基盤の整備
～JVN脆弱性対策機械処理基盤～

- 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においては、JVN＋JVN iPediaを活用し、必要とされる新たなサービスを提供できる環境を整備していく



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

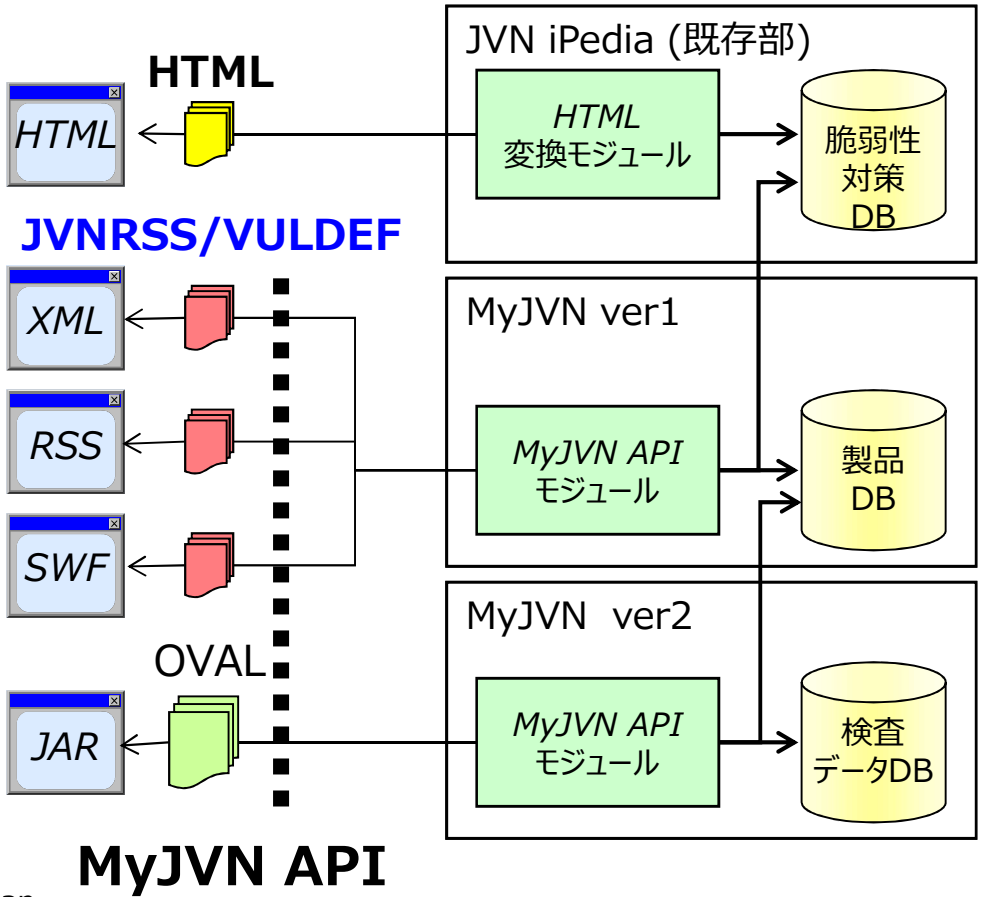
JVN
製品開発者と調整した脆弱性対策情報をタイムリーに公開する

脆弱性対策に関わる基盤の整備
～JVN脆弱性対策機械処理基盤～

- **MyJVN API** (http://jvndb.jvn.jp/apis/)
  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



脆弱性対策に関わる基盤の整備
～JVN脆弱性対策機械処理基盤～

- 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においては、国際的な共通基準の積極的な導入を進めていく

・・・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

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

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			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～

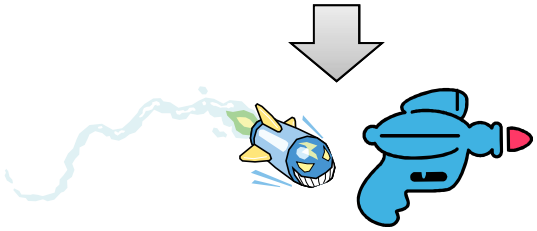
IPA

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**

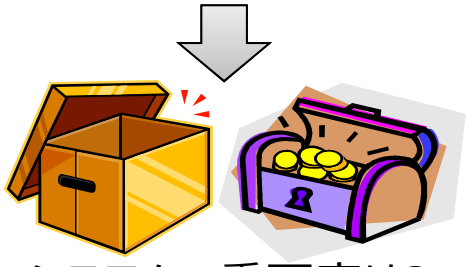
＝ 「技術的な特性」 × 「脅威の大きさ」 × 「情報資産の価値」

＝ 「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

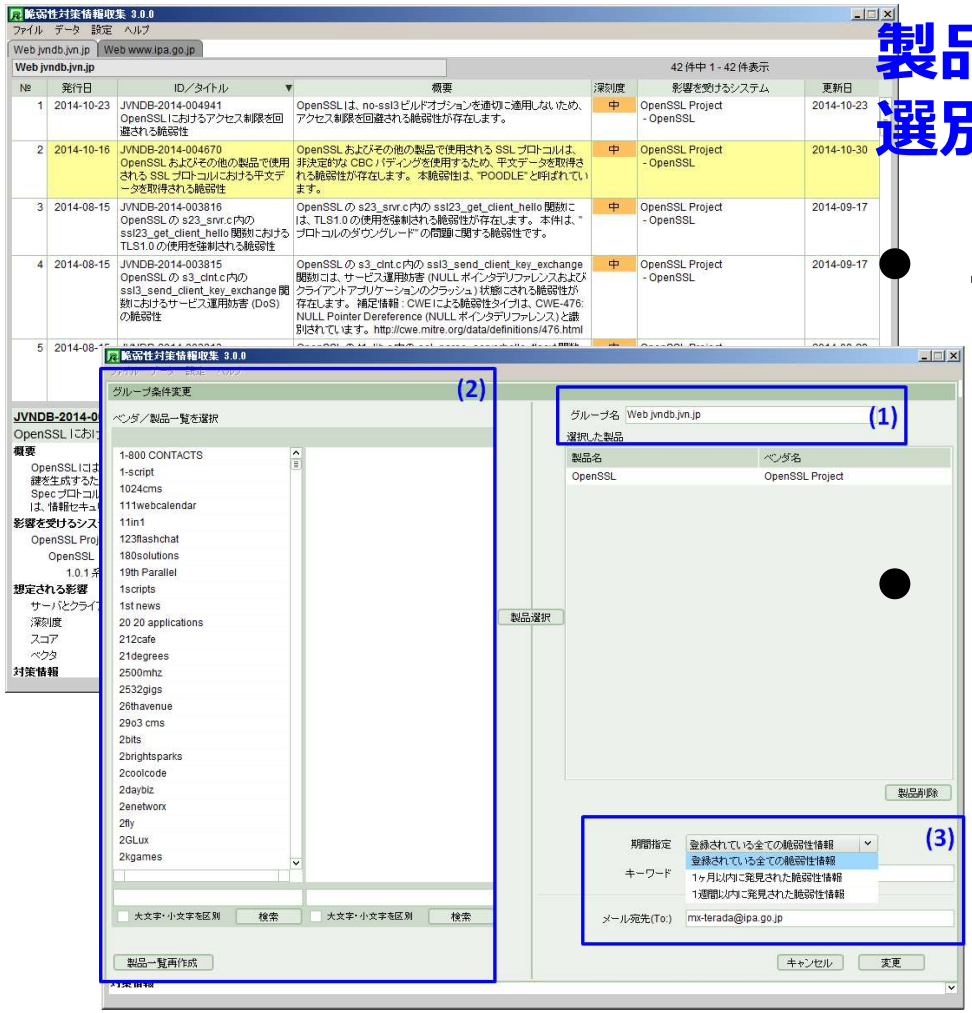
cpe:/a:ipa:myjvn

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

MyJVN脆弱性対策情報収集ツール

http://jvndb.jvn.jp/apis/myjvn/mjcheck3.html



製品視点から脆弱性対策情報を選別する。

- JVN iPedia の情報を、利用者が更に効率的に活用できるように、CPEを用いた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
- 常に、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

MyJVNバージョンチェッカ

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

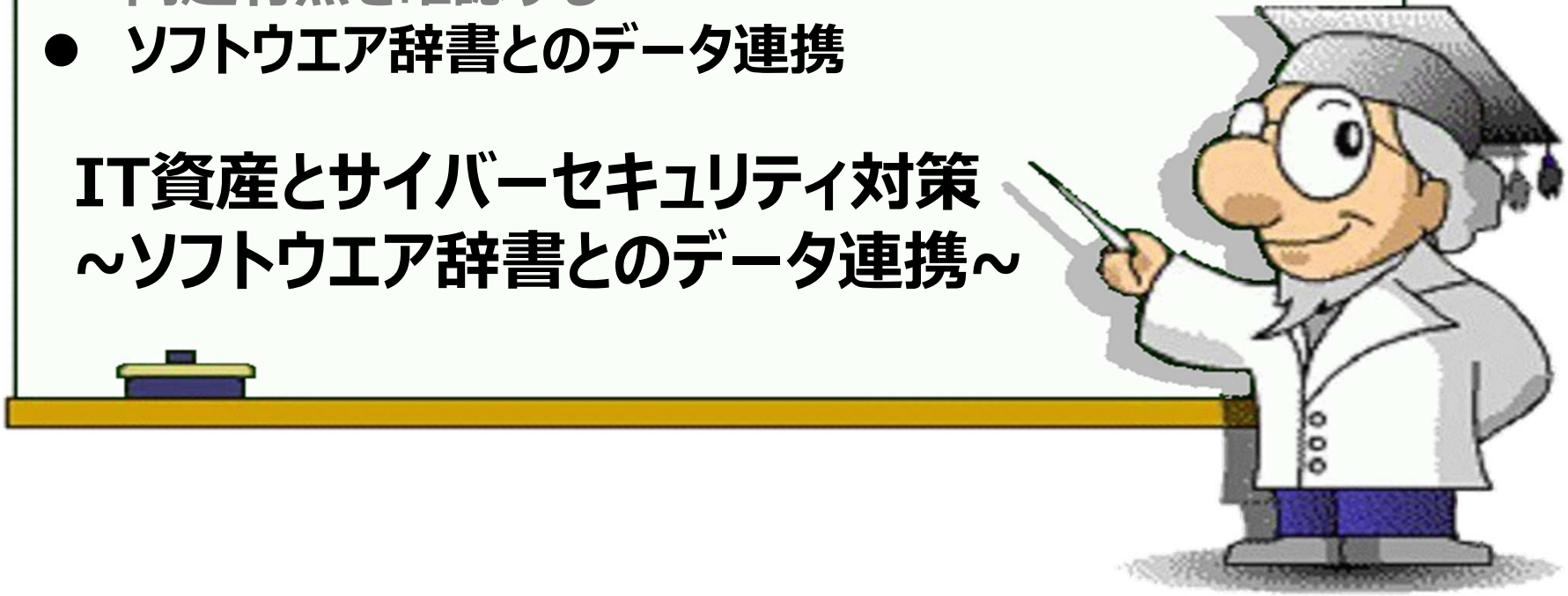
ソフトウェアのバージョンが最新であるかを確認する。

- 利用者のPCにインストールされているアプリケーションソフトウェア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
- バージョンが最新であるかどうかのチェックリストを手作業ではなく、機械的に確認

目次

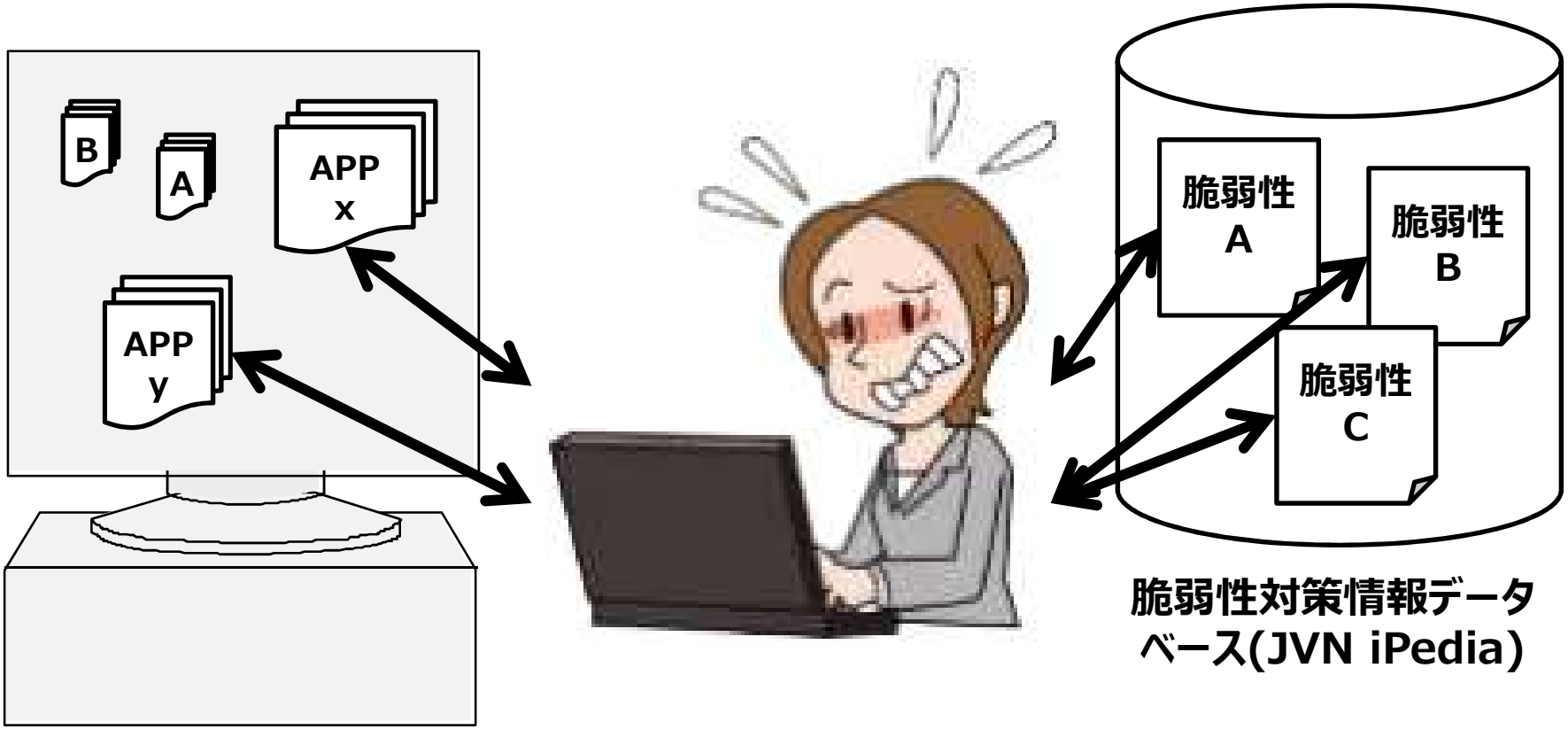
- 情報セキュリティ10大脅威 2017
- 脆弱性届出の状況
- 脆弱性を作りこまない
- 安全に運営する
- 問題有無を確認する
- **ソフトウエア辞書とのデータ連携**

IT資産とサイバーセキュリティ対策
~ソフトウエア辞書とのデータ連携~



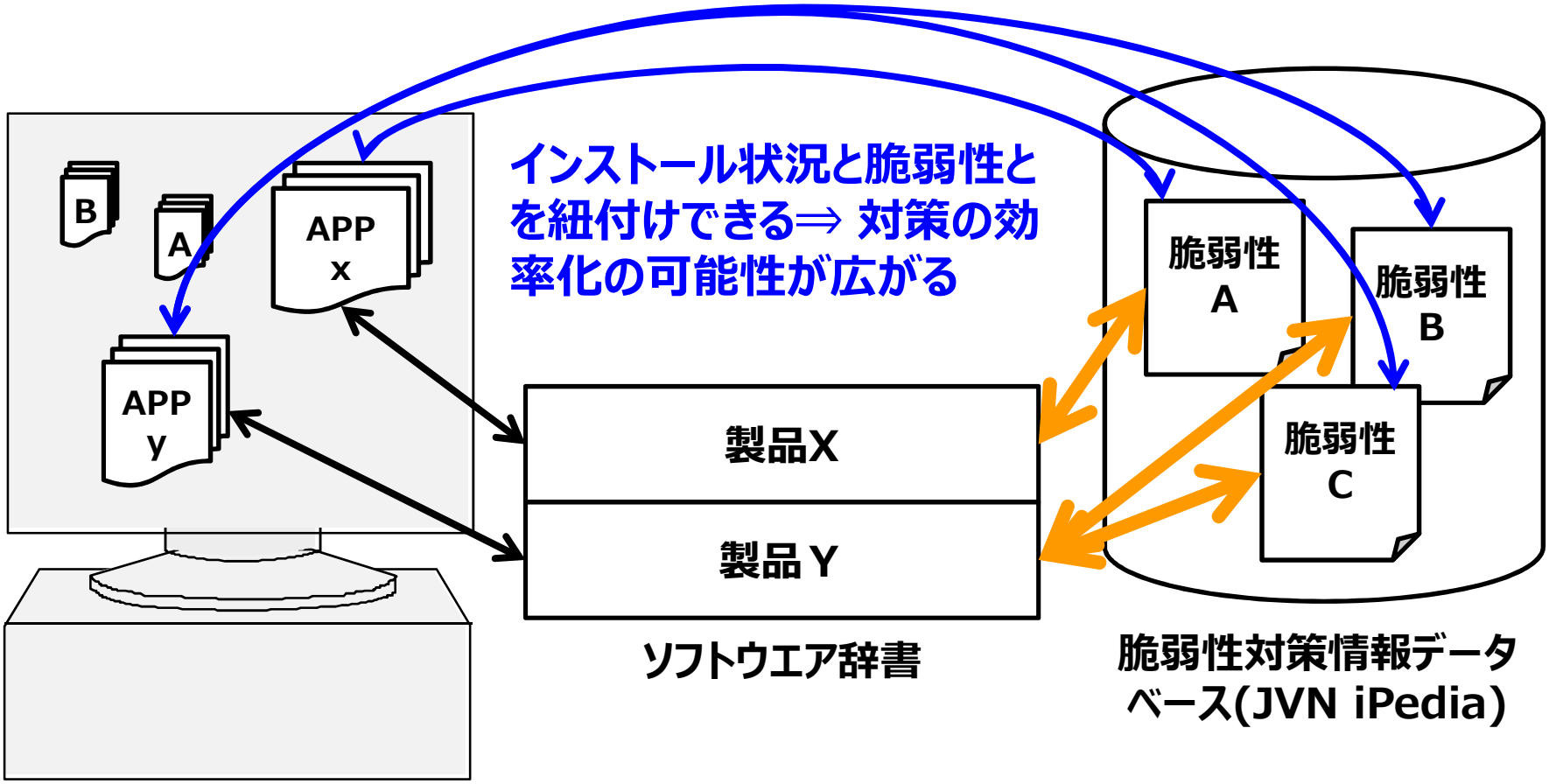
ソフトウエア辞書とのデータ連携
～インストール状況と脆弱性との紐付け～

- 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)。



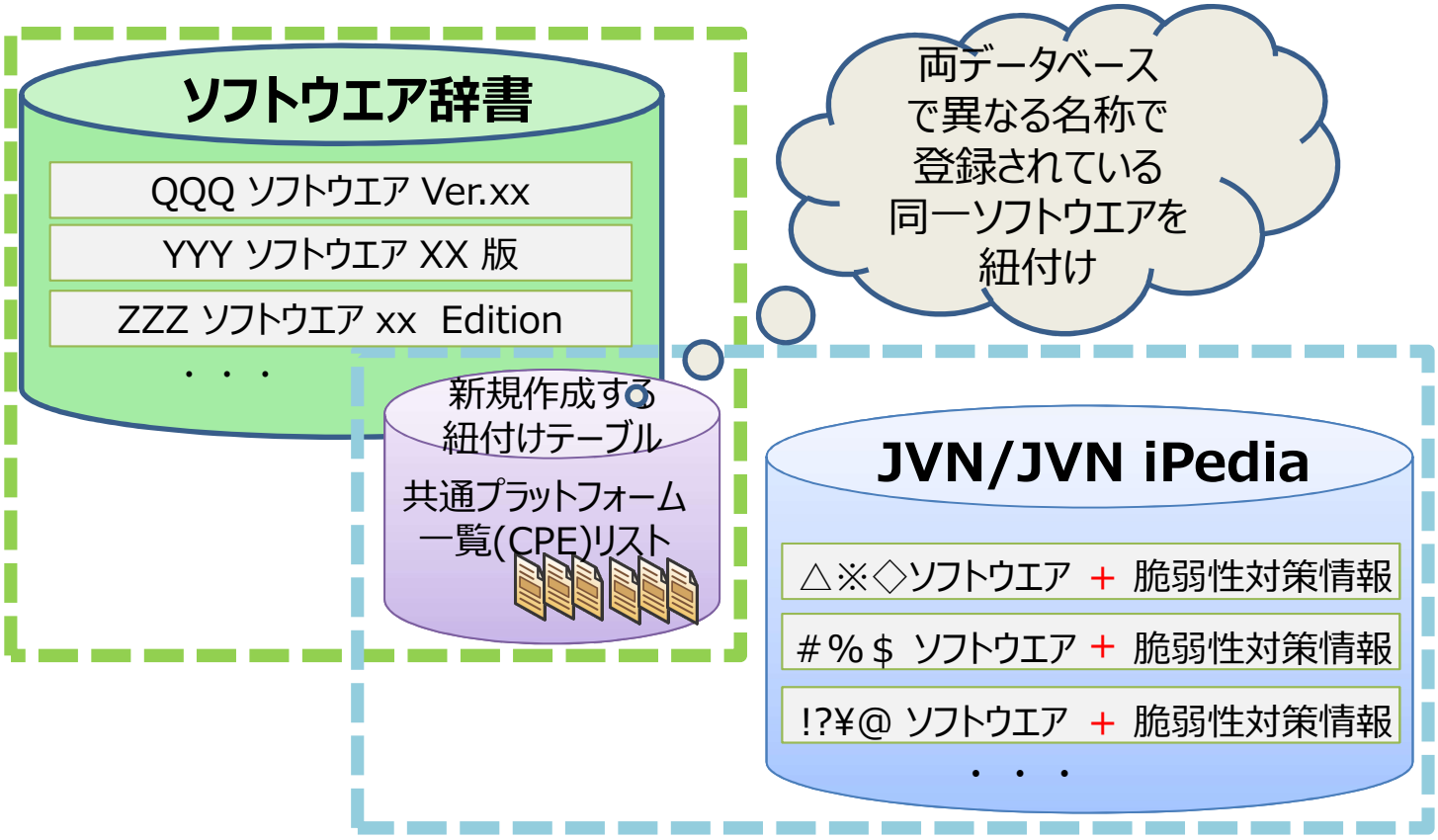
ソフトウエア辞書とのデータ連携
～インストール状況と脆弱性との紐付け～

- 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～

- **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～

- 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

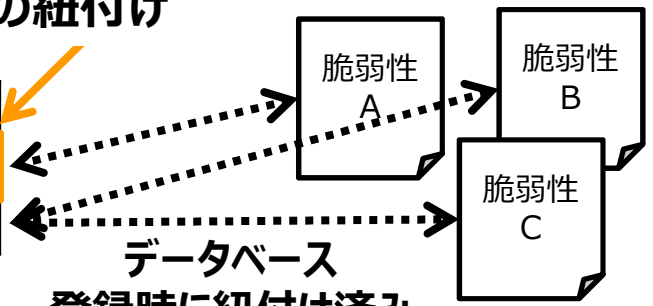
SAMACソフトウエア辞書の既存登録項目(9項目)				連携用項目(1項目)
sw_id	sw_vendor	sw_name	その他項目	CPE v2.2
・・・	・・・	Adobe Acrobat 8.2.0 Professional	・・・	cpe:/a:adobe:acrobat
・・・	・・・	Adobe Acrobat 8.2.0 Standard	・・・	cpe:/a:adobe:acrobat
・・・	・・・	Adobe Acrobat 8.2.1 - CPSID_50570	・・・	cpe:/a:adobe:acrobat
・・・	・・・	Adobe Acrobat 8.2.1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

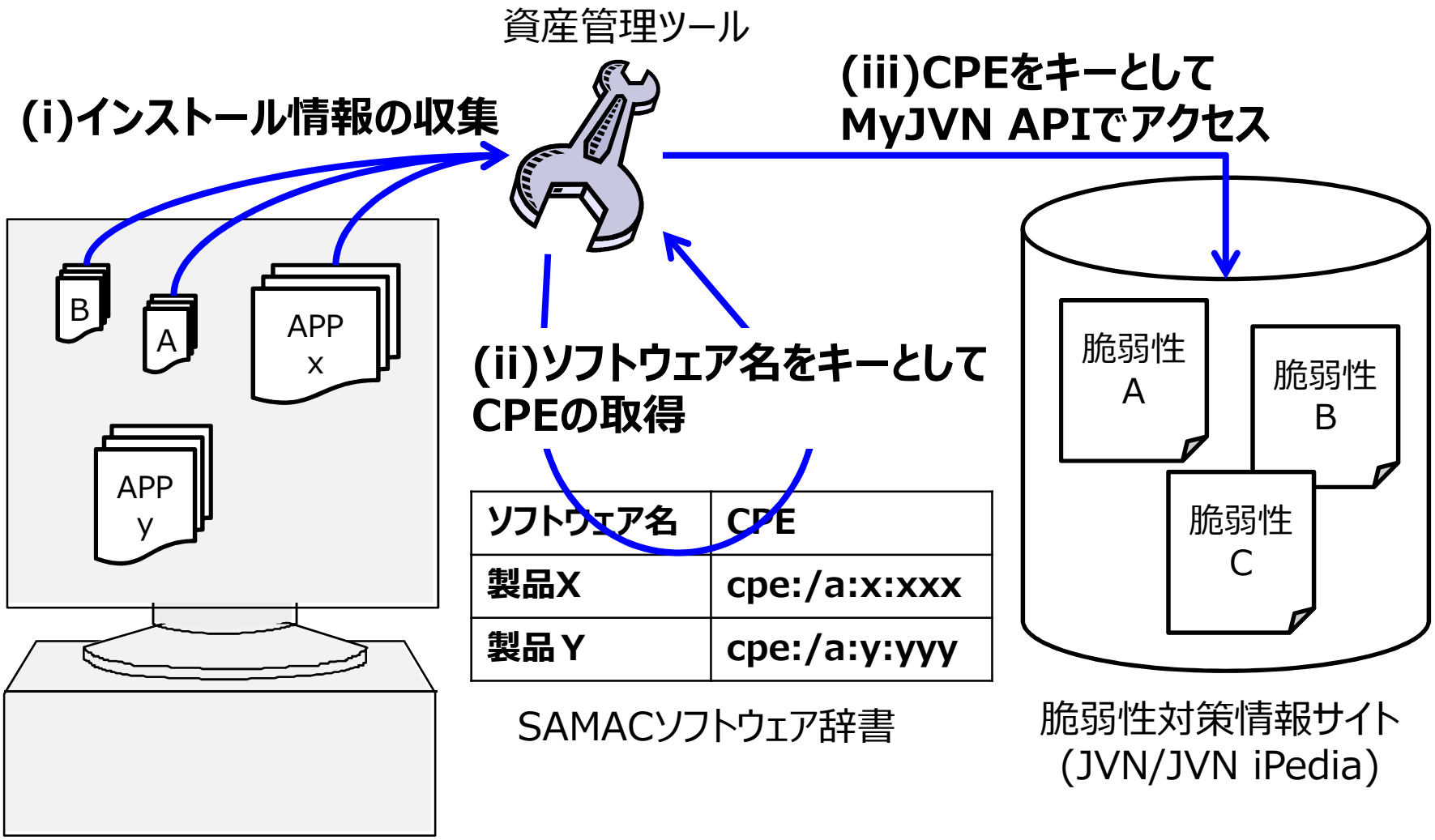
ソフトウエア名	CPE v2.2
Adobe Acrobat	cpe:/a:adobe:acrobat
製品Y	cpe:/a:y:yyy

JVN製品データベース



データベース 登録時に紐付け済み

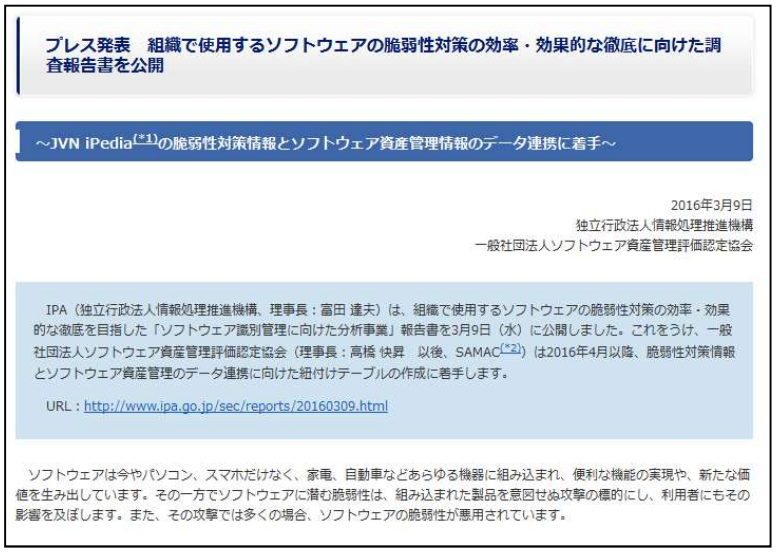
ソフトウエア辞書とのデータ連携
～脆弱性対策情報参照までの流れ～



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、IT資産と脆弱性対策との一元的な管理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。


IPA
Better Life
with IT