

2019 暗号と情報セキュリティシンポジウム
MWS/CWS合同企画セッション(1)

脆弱性届出制度

～ 情報セキュリティ早期警戒パートナーシップの取組み ～

2019年1月24日

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 セキュリティ対策推進部
脆弱性対策グループリーダー 渡辺 貴仁

「情報セキュリティ早期警戒パートナーシップ」 とは



- **情報セキュリティ早期警戒パートナーシップ**は、ソフトウェア製品及びウェブサイトに関する脆弱性関連情報の円滑な流通、および対策の普及を図るため、公的ルールに基づく官民の連携体制として、2004年7月に整備された**脆弱性関連情報の届出制度**。

- 告示

平成29年経済産業省告示第19号

http://www.meti.go.jp/policy/netsecurity/vul_notification.pdf

- ガイドライン

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

<https://www.ipa.go.jp/files/000059694.pdf>

- 脆弱性関連情報は関係者の協力をもと、適切に流通・対応・公表※されている。

※公表はソフトウェア製品の脆弱性の場合

情報セキュリティ早期警戒パートナーシップ ガイドライン構成



<ul style="list-style-type: none">I. はじめにII. 用語の定義と前提III. 本ガイドラインの適用の範囲IV. ソフトウェア製品に係る脆弱性関連情報取扱<ul style="list-style-type: none">1. 概要2. 発見者の対応3. IPA(受付機関)の対応4. JPCERT/CC(調整機関)の対応5. 製品開発者の対応6. その他V. ウェブアプリケーションに係る脆弱性関連情報取扱<ul style="list-style-type: none">1. 概要2. 発見者の対応3. IPA(受付機関)の対応4. ウェブサイト運営者の対応	<ul style="list-style-type: none">付録1 用語の解説付録2 脆弱性情報取扱いのフロー付録3 法的な論点について<ul style="list-style-type: none">1. 発見者が心得ておくべき法的な論点2. 製品開発者が心得ておくべき法的な論点3. ウェブサイト運営者が心得ておくべき法的な論点付録4 脆弱性の影響度に関する考え方について付録5 ソフトウェア製品における連絡不能案件の取扱いについて<ul style="list-style-type: none">1. 連絡不能開発者一覧の公表2. 対象製品情報の公表と関係者へのお願い付録6 ソフトウェアの脆弱性の取扱いに関する国際標準への対応付録7 本ガイドラインの別冊・関連資料一覧
--	---

● 脆弱性の定義

- ソフトウェア製品やウェブアプリケーション等における
セキュリティ上の問題箇所
- コンピュータ不正アクセスやコンピュータウイルス等により、この問題の箇所が攻撃されることで、そのソフトウェア製品やウェブアプリケーションの本来の機能や性能を損なう原因となり得るもの
- また本制度での脆弱性は、個人情報等が適切なアクセス制御の下に管理されていないなど、ウェブサイト運営者の不適切な運用により、ウェブアプリケーションのセキュリティが維持できなくなっている状態も含む

ソフトウェア製品等の脆弱性関連情報に関する取扱規程

3. 定義

(1) ソフトウェア製品

ソフトウェア又はそれを組み込んだハードウェアであって、**汎用性**を有する製品をいう。

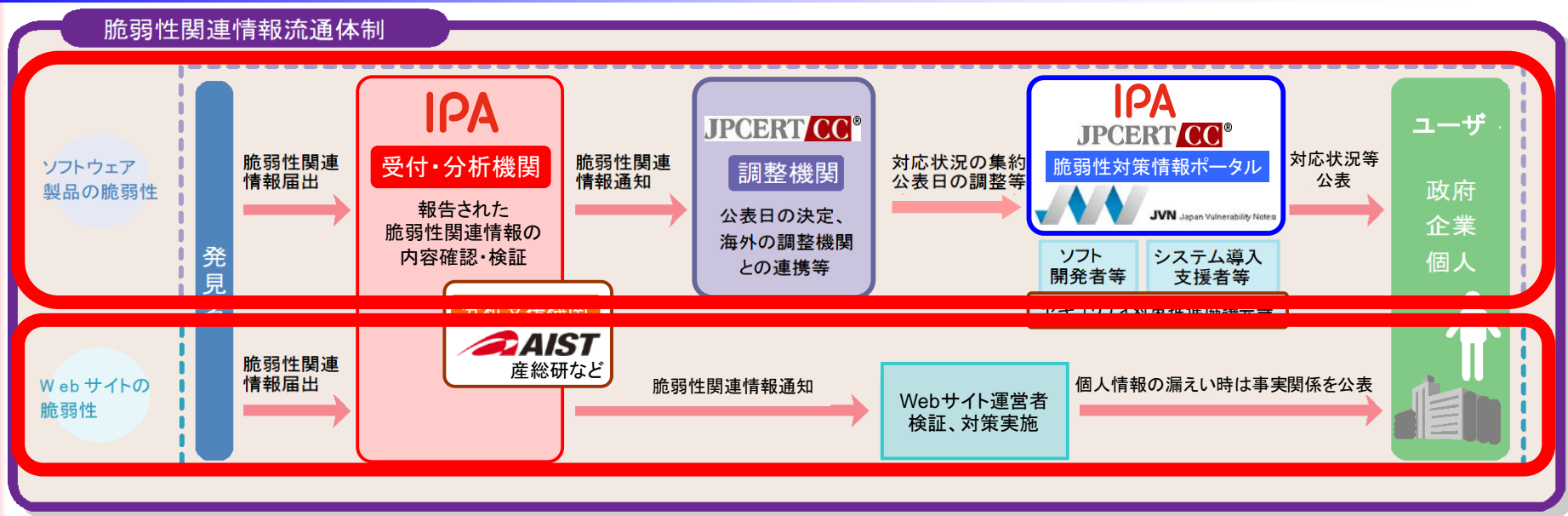
(2) ウェブアプリケーション

インターネット上のウェブサイトで稼働する固有のシステムをいう。

4. 本基準の適用範囲

本規程は、**日本国内で利用されているソフトウェア製品**又は主に**日本国内からのアクセスが想定されているウェブサイト**で稼働するウェブアプリケーションに係る脆弱性であって、その脆弱性に起因する影響が**不特定多数の者に及ぶおそれのあるもの**に適用する。

運営体制と役割(全体フロー)

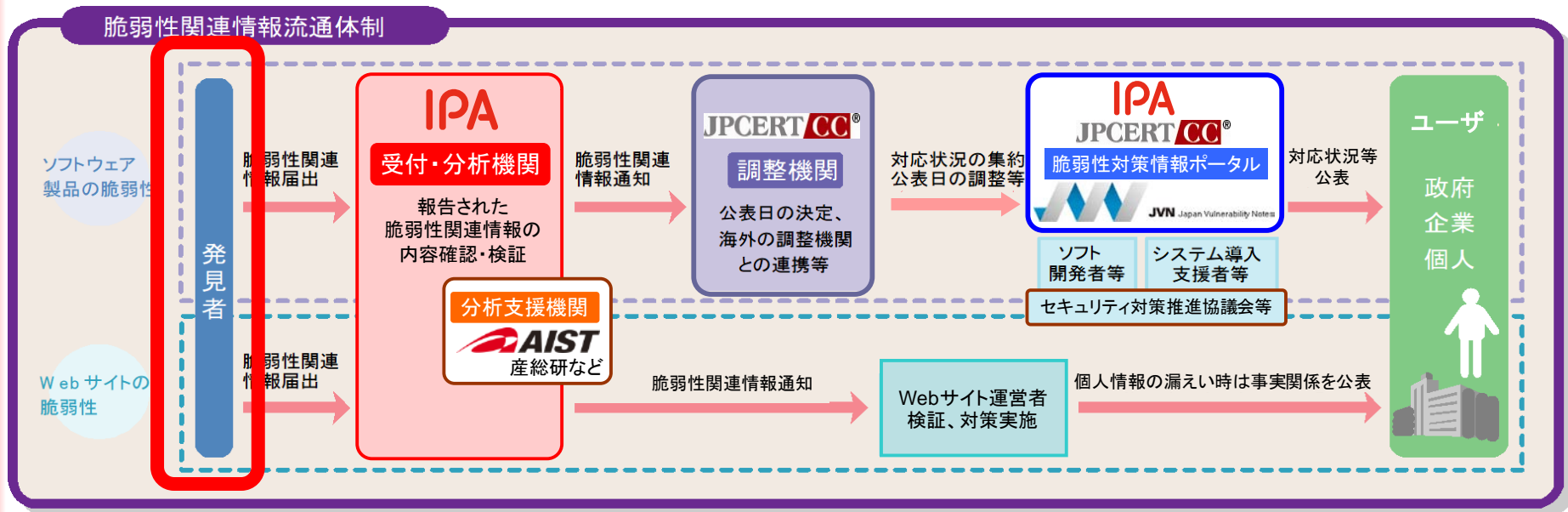


※JPCERT/CC:一般社団法人 JPCERT コーディネーションセンター、産総研:国立研究開発法人産業技術総合研究所

脆弱性関連情報流通体制

- 上段:ソフトウェア製品の脆弱性
- 下段:ウェブサイト(ウェブアプリケーション)の脆弱性

運営体制と役割(発見者)



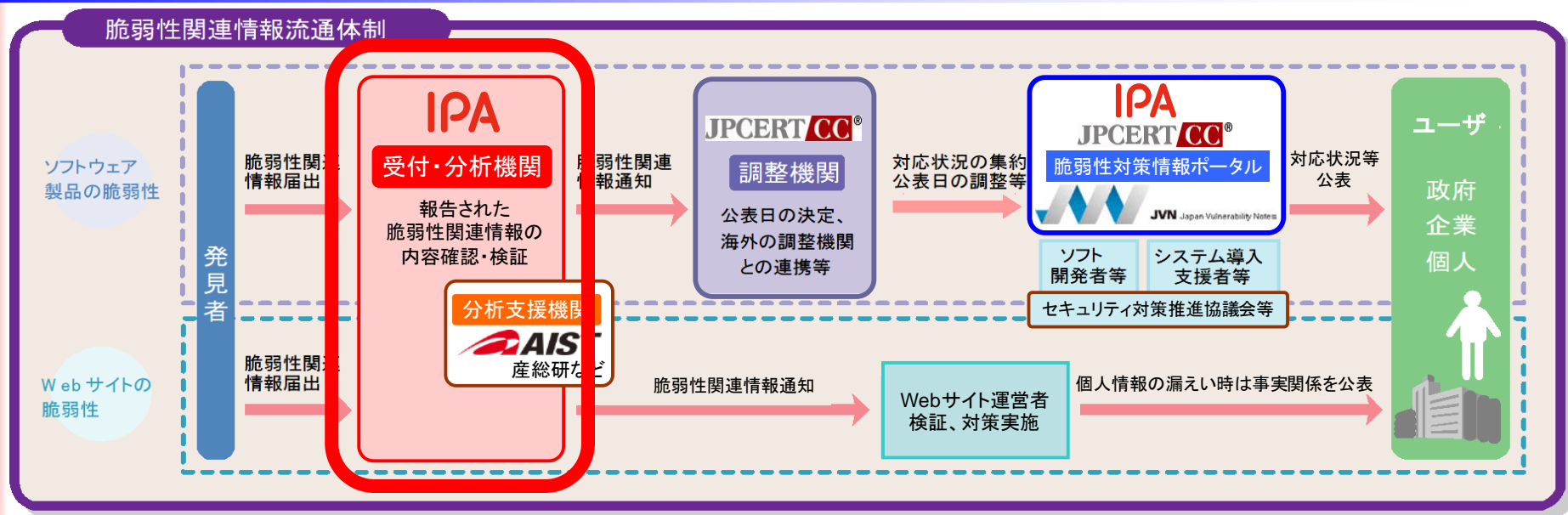
※JPCERT/CC:一般社団法人 JPCERT コーディネーションセンター、産総研:国立研究開発法人産業技術総合研究所

脆弱性を発見し、本制度に脆弱性情報として届出された方

•発見者のタイプ

- 一般のウェブサイト/ソフトウェア製品の利用者
- 学生、セキュリティ研究者、セキュリティベンダー
- ソフトウェア製品開発者(自社製品の脆弱性届出)

運営体制と役割 (IPA 受付・分析機関)

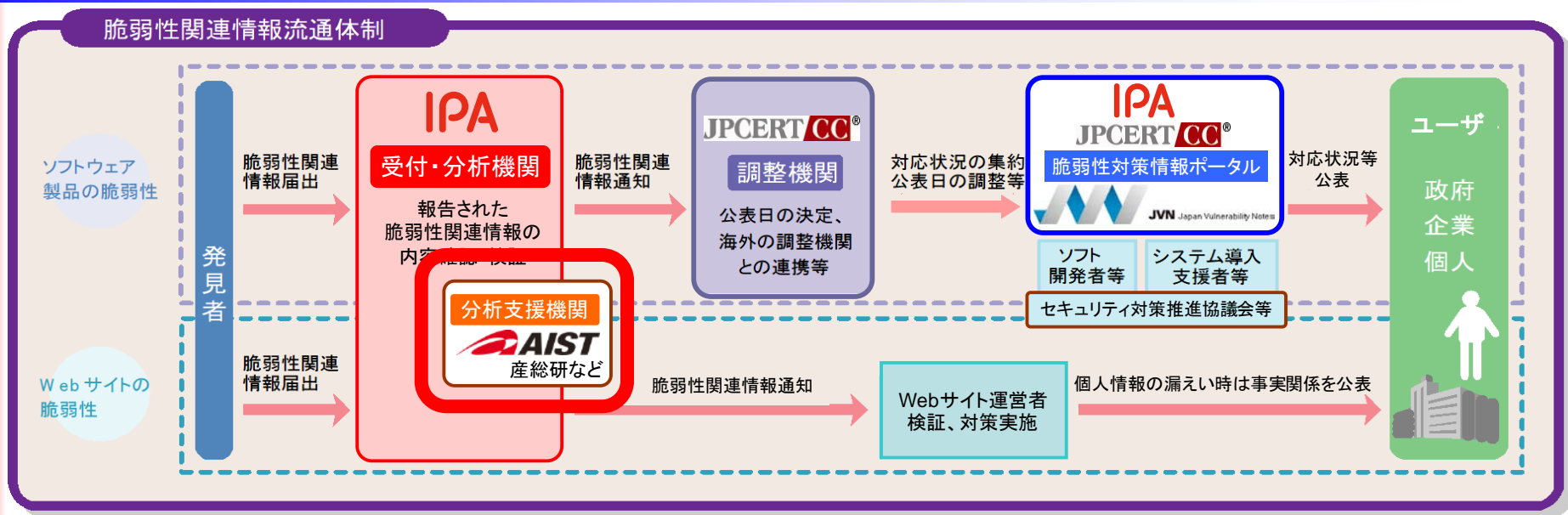


※JPCERT/CC:一般社団法人 JPCERT コーディネーションセンター、産総研:国立研究開発法人産業技術総合研究所

届出られた脆弱性情報を受付け、分析し、流通管理を行う

- 脆弱性関連情報の受付
 - 受理、案件管理
 - 発見者やJPCERT/CCとの調整
- 脆弱性関連情報の分析
 - 脆弱性の検証および判断
 - 注意喚起の検討および公表

運営体制と役割 (AIST... 分析支援機関)



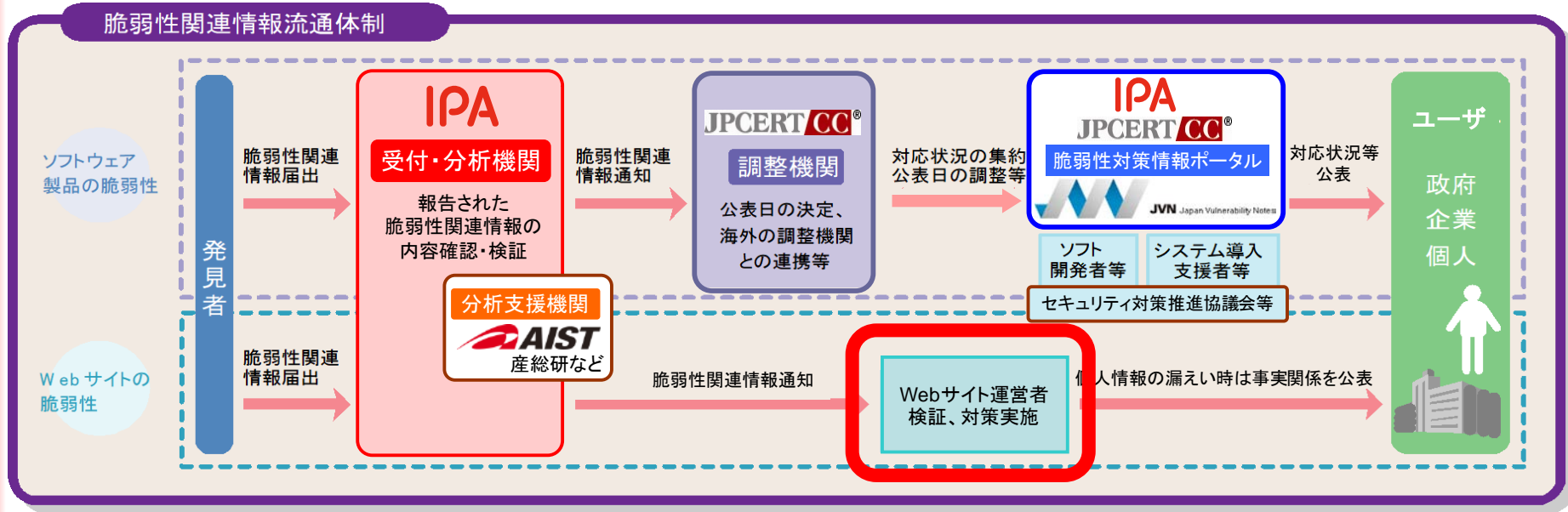
※JPCERT/CC:一般社団法人 JPCERT コーディネーションセンター、産総研:国立研究開発法人産業技術総合研究所

客観的な判断が必要な情報に関し、専門官に分析を依頼する

•国立研究開発法人 産業技術総合研究所

- 脆弱性届出に関し、研究専門官に客観的な判断を求める
 - 相談内容例:暗号アルゴリズム、IPプロトコル、生体認証
- 関連資料の精査

運営体制と役割(ウェブサイト運営者)

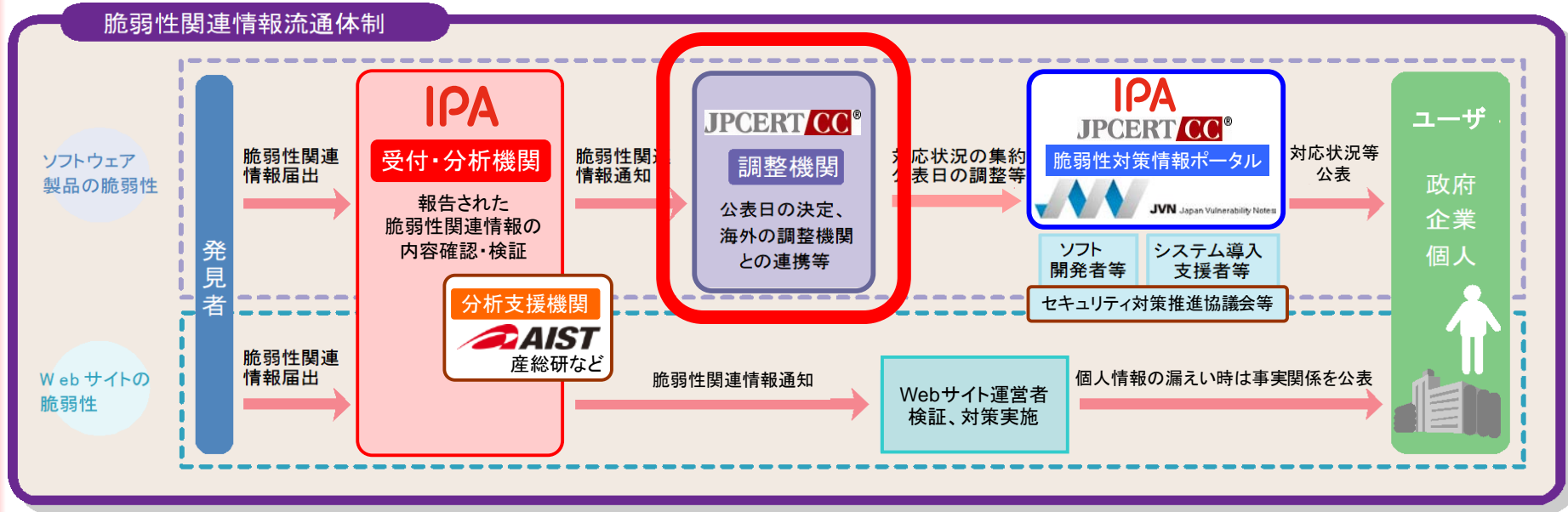


※JPCERT/CC:一般社団法人 JPCERT コーディネーションセンター、産総研:国立研究開発法人産業技術総合研究所

ウェブサイトの脆弱性について対策を行う

- ウェブサイトの運営者のタイプ
 - 官公庁、地方自治体、民間企業、団体、個人
- ウェブサイトの運営者の対応
 - 脆弱性情報への対応(影響の調査、修正の実施)
 - 個人情報漏えい時は事実関係を公表

運営体制と役割 (JPCERT/CC 調整機関) IPA

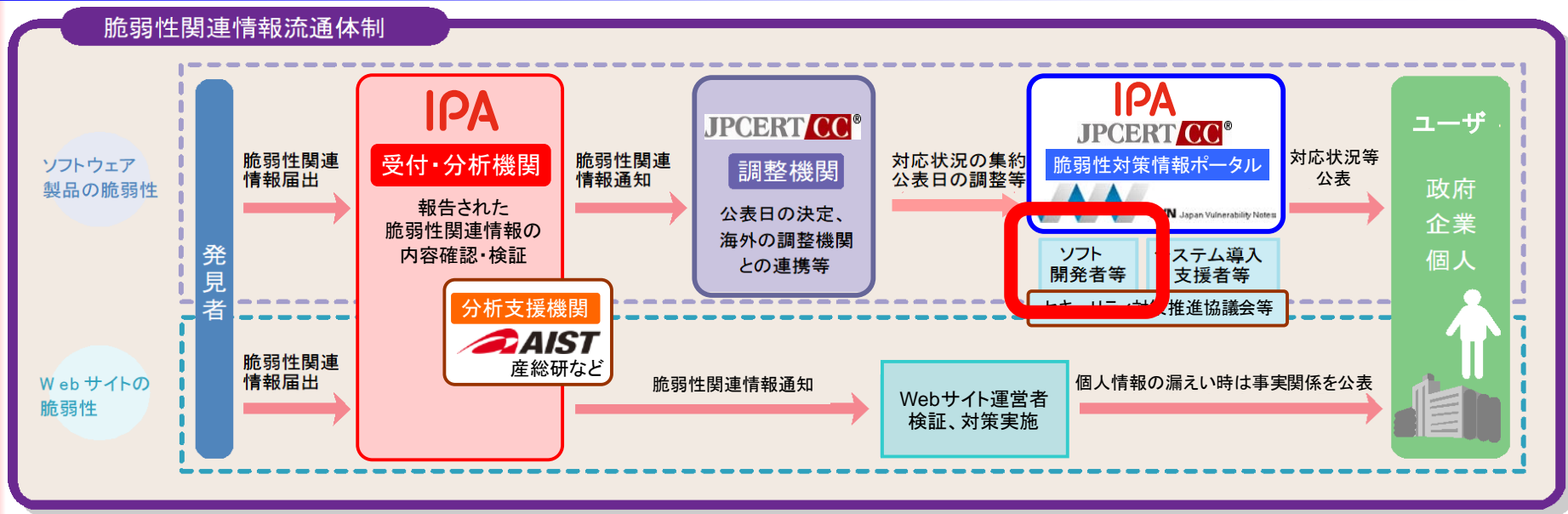


※JPCERT/CC:一般社団法人 JPCERT コーディネーションセンター、産総研:国立研究開発法人産業技術総合研究所

ソフトウェア製品開発者へ脆弱性情報を通知し、調整のうえ、JVNにて公表を行う

- POC (Point Of Contact) 開設
 - 適切な製品開発者との連絡窓口を開設
- 製品開発者との調整
 - 脆弱性情報の通知
 - マルチベンダー調整、公表調整

運営体制と役割(ソフトウェア製品開発者)

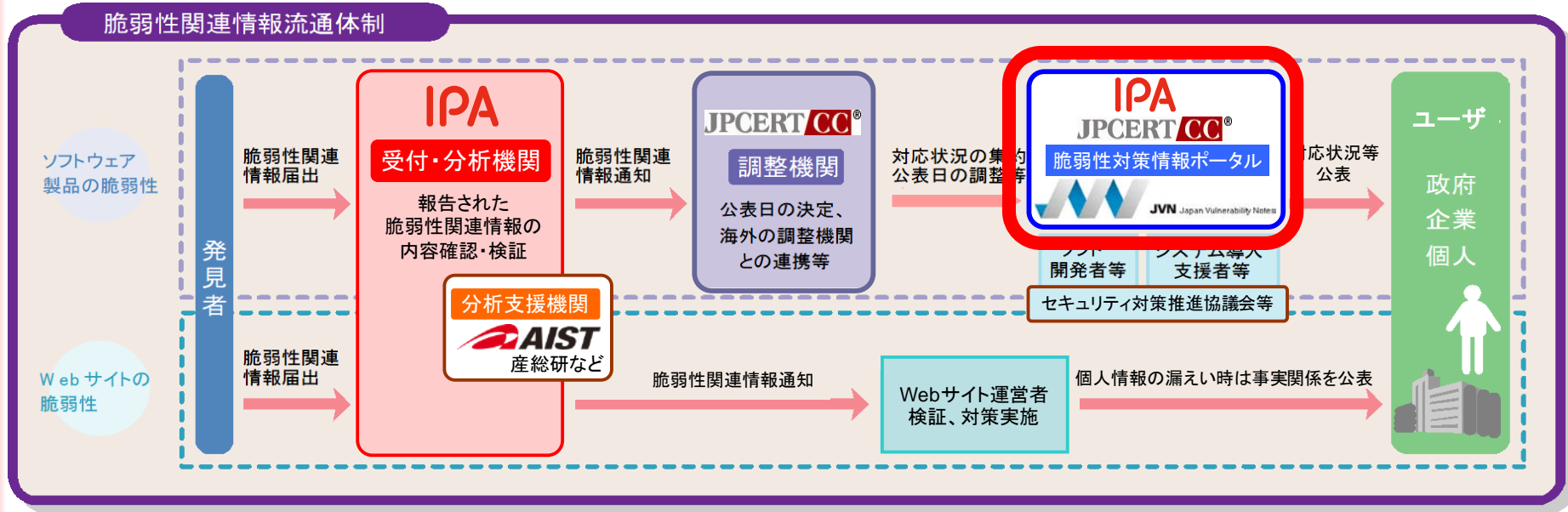


※JPCERT/CC:一般社団法人 JPCERT コーディネーションセンター、産総研:国立研究開発法人産業技術総合研究所

ソフトウェア製品の脆弱性について対策を行い公表を行う

- ソフトウェア製品開発者のタイプ
 - 大手製品ベンダー、中小製品ベンダー
 - OSS開発者、個人製品開発者、海外ベンダー
- ソフトウェア製品開発者の対応
 - 脆弱性検証(影響の調査、他製品への影響)
 - JVN公表日の調整、対策方法の作成、周知

運営体制と役割 (JVN: Japan Vulnerability Notes) IPA



※JPCERT/CC:一般社団法人 JPCERT コーディネーションセンター、産総研:国立研究開発法人産業技術総合研究所

JVNにて脆弱性対策情報を公表をする

- 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ポータルサイト。
- 本パートナーシップで扱い製品開発者が対策を施した情報や、海外CSIRTから連絡を受けた情報を公表。

JVN (Japan Vulnerability Notes)

脆弱性対策情報ポータルサイト

https://jvn.jp/jp/



最終更新日: 2019/01/10

Japan Vulnerability Notes JP 一覧

最新12ヶ月 | 2018年 | 2017年 | 2016年 | 2015年 | 2014年 | 2013年 | 2012年 | 2011年 | 2010年 | 2009年 | 2008年 | 2007年 | 2006年 | 2005年以前

2019年

2019/01/10 JVN#58010349:
WordPress 用プラグイン spam-byebye におけるクロスサイトスクリプティングの脆弱性

2018年

2018/12/26 JVN#96493183:
GROWI におけるクロスサイトスクリプティングの脆弱性

2018/12/25 JVN#33677949:
マッピングツールのインストーラにおける DLL 読み込みに関する脆弱性

2018/12/25 JVN#27052429:
WordPress 用プラグイン Google XML Sitemaps におけるクロスサイトスクリプティングの脆弱性

2018/12/21 JVN#13199224:
PgpoolAdmin におけるアクセス制限不備の脆弱性

2018/12/21 JVN#69812763:
cordova-plugin-ionic-webview におけるバストラバーサルの脆弱性

2018/12/19 JVN#99810718:
東芝ラテック製ホームゲートウェイにおける複数の脆弱性

2018/12/14 JVN#87535892:
Aterm WF1200CR および Aterm WG1200CR における複数の脆弱性

2018/12/10 JVN#25385698:
サイボウズ Garoon におけるアクセス制限回避の脆弱性

2018/12/10 JVN#23161885:
サイボウズ リモートサービスにおける複数の脆弱性

2018/12/07 JVN#32155106:
i-FILTER における複数の脆弱性

2018/12/06 JVN#89767228:
セイコーエプソン製の複数のプリンタおよびスキャナにおける複数の脆弱性

2018/11/29 JVN#36895151:
パナソニック製アプリケーションが登録する一部の Windows サービスにおいて実行ファイルのパスが引用符で囲まれていない脆弱性

https://jvn.jp/index.html JVN#25359688:

公開日: 2018/12/21 最終更新日: 2018/12/21

JVN#13199224 PgpoolAdmin におけるアクセス制限不備の脆弱性

概要
PgpoolAdmin (こは、アクセス制限不備の脆弱性が存在します。

影響を受けるシステム

- PgpoolAdmin 4.0 およびそれ以前

詳細情報
PgPool Global Development Group が提供する PgpoolAdmin (こは、アクセス制限不備 (CWE-264) の脆弱性が存在します。

想定される影響
当該製品にアクセス可能な第三者によって、ログイン認証を回避され、PostgreSQL データベースの管理者権限を取得される可能性があります。

対策方法
アップデートする
開発者が提供する情報をもとに、最新版へアップデートしてください。

ベンダ情報

ベンダ	ステータス	ステータス 最終更新日	ベンダの告知ページ
PgPool Global Development Group	該当製品あり	2018/12/21	PgPool Global Development Group の告知ページ

参考情報

JPCERT/CCからの補足情報

JPCERT/CCによる脆弱性分析結果

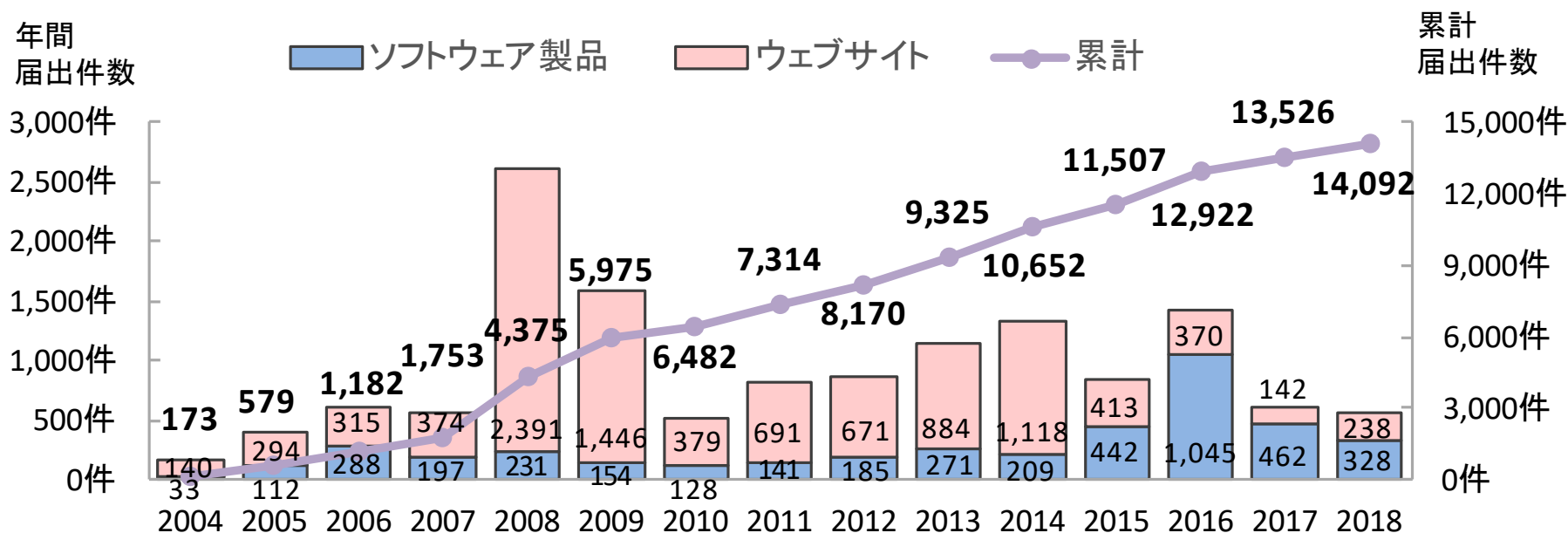
CVSS v3	CVSS 3.0 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	基本値: 9.8
CVSS v2	AV:N/AC:L/Au:N/C:P/I:P/A:P	基本値: 7.5

脆弱性届出の状況

● 届出受付開始から2018年12月末迄の累計件数

■ ソフトウェア製品 **4,226**件、ウェブサイト **9,866**件、合計 **14,092**件

→ 1就労日あたり **3.99** 件



脆弱性関連情報届出件数(2018年12月末迄)

脆弱性の修正完了状況

● 届出受付開始から2018年12月末迄の累計件数

■ ソフトウェア製品 **1,936**件、ウェブサイト **7,346**件、合計 **9,282**件

