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ー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

# 本制度で扱う脆弱性

- 脆弱性の定義
  - ソフトウエ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、そのソフトウエ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

# 現行の告示での対象範囲

ソフトウエア製品等の脆弱性関連情報に関する取扱規程

3. 定義

(1) ソフトウエア製品

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

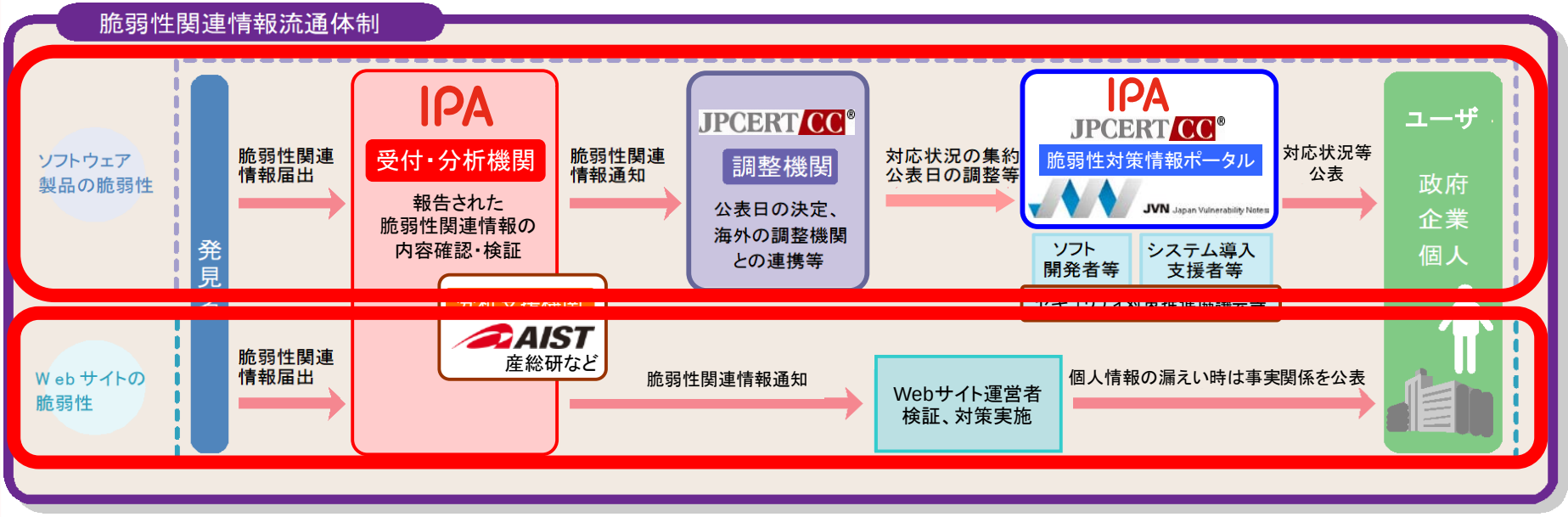
(2) ウェブアプリケーション

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エア製品**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）

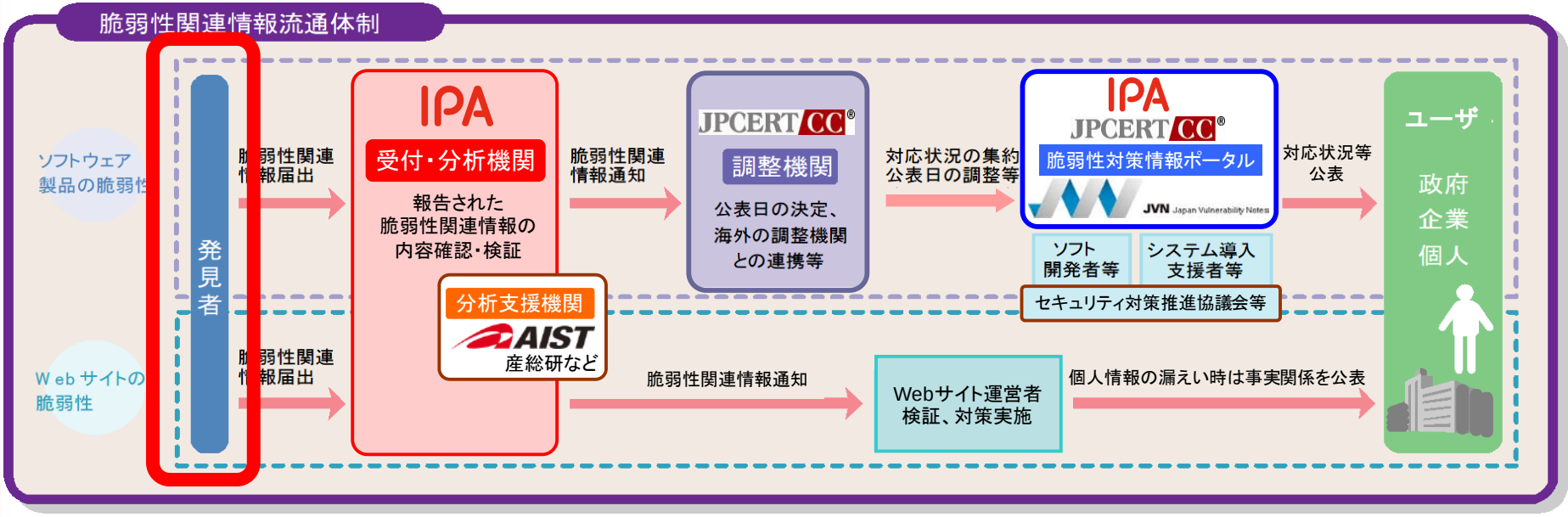



※JPCERT/CC：一般社団法人 JPCERT コーディネーションセンター、産総研：国立研究開発法人産業技術総合研究所

## 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）

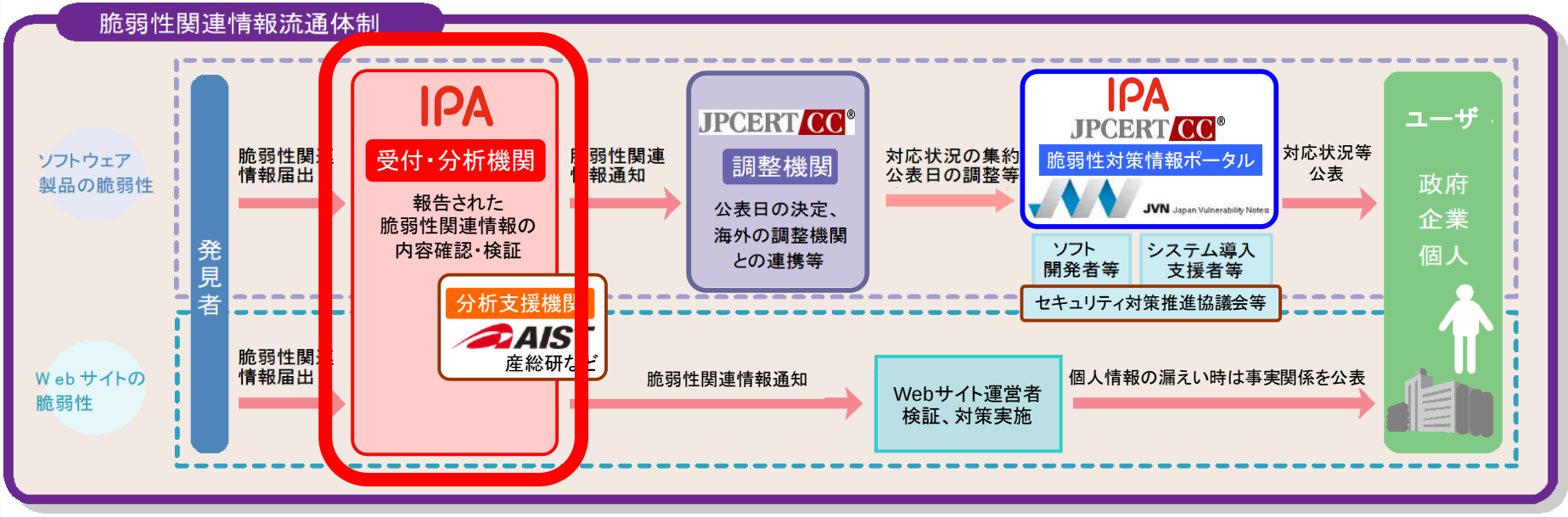



※JPCERT/CC：一般社団法人 JPCERT コーディネーションセンター、産総研：国立研究開発法人産業技術総合研究所

## 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）

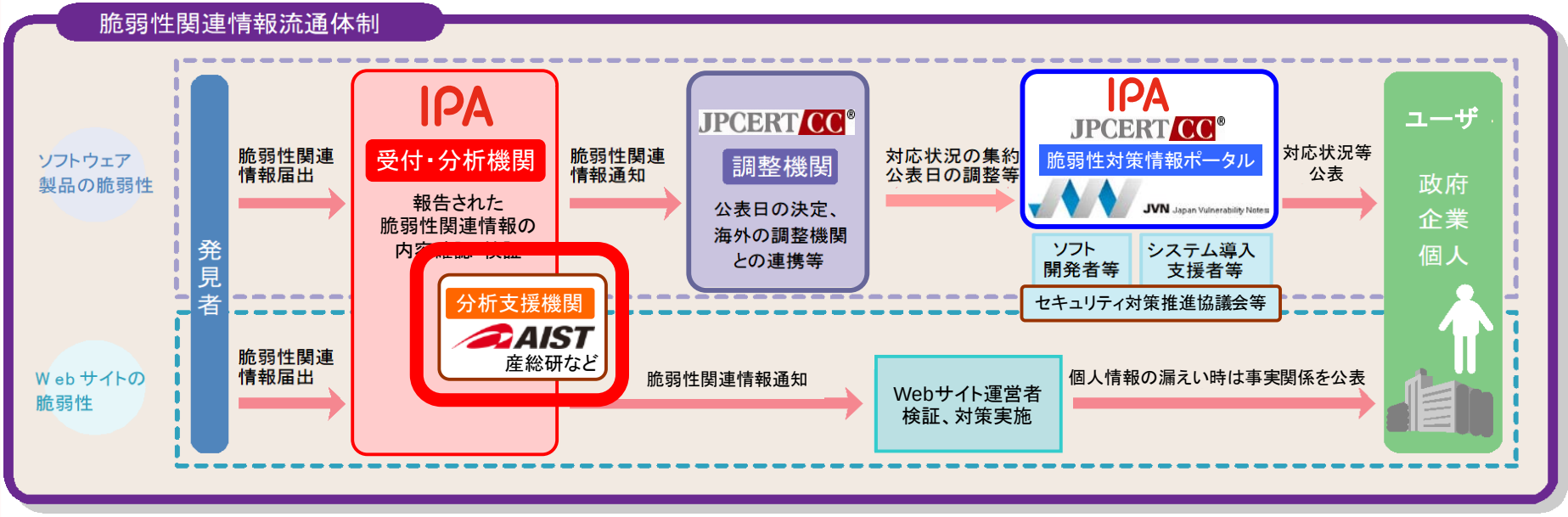



※JPCERT/CC：一般社団法人 JPCERT コーディネーションセンター、産総研：国立研究開発法人産業技術総合研究所

## 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）

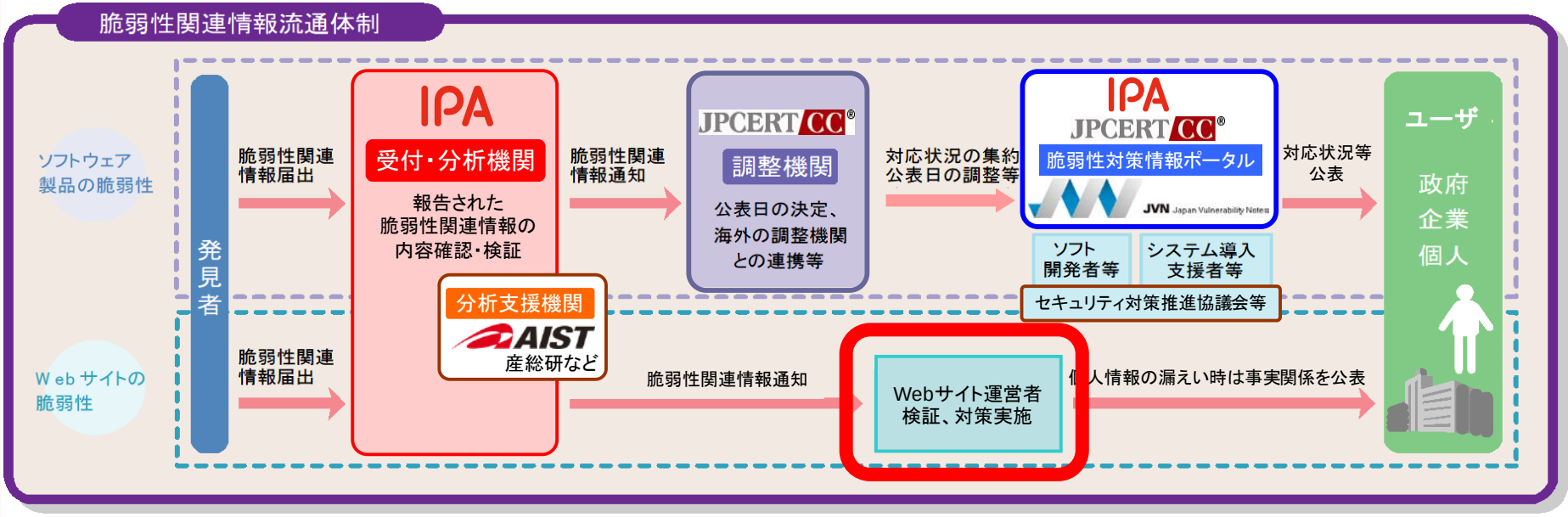



※JPCERT/CC：一般社団法人 JPCERT コーディネーションセンター、産総研：国立研究開発法人産業技術総合研究所

## 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）

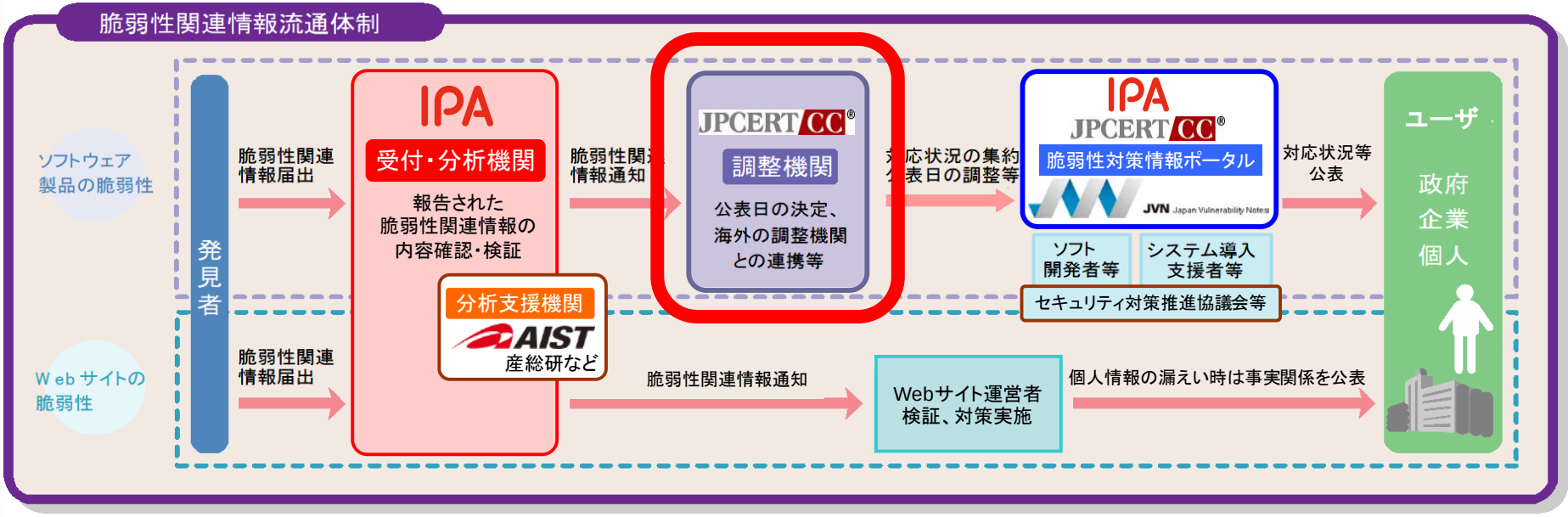



※JPCERT/CC：一般社団法人 JPCERT コーディネーションセンター、産総研：国立研究開発法人産業技術総合研究所

## 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
- ウェブサイト運営者の対応
  - 脆弱性情報への対処（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）

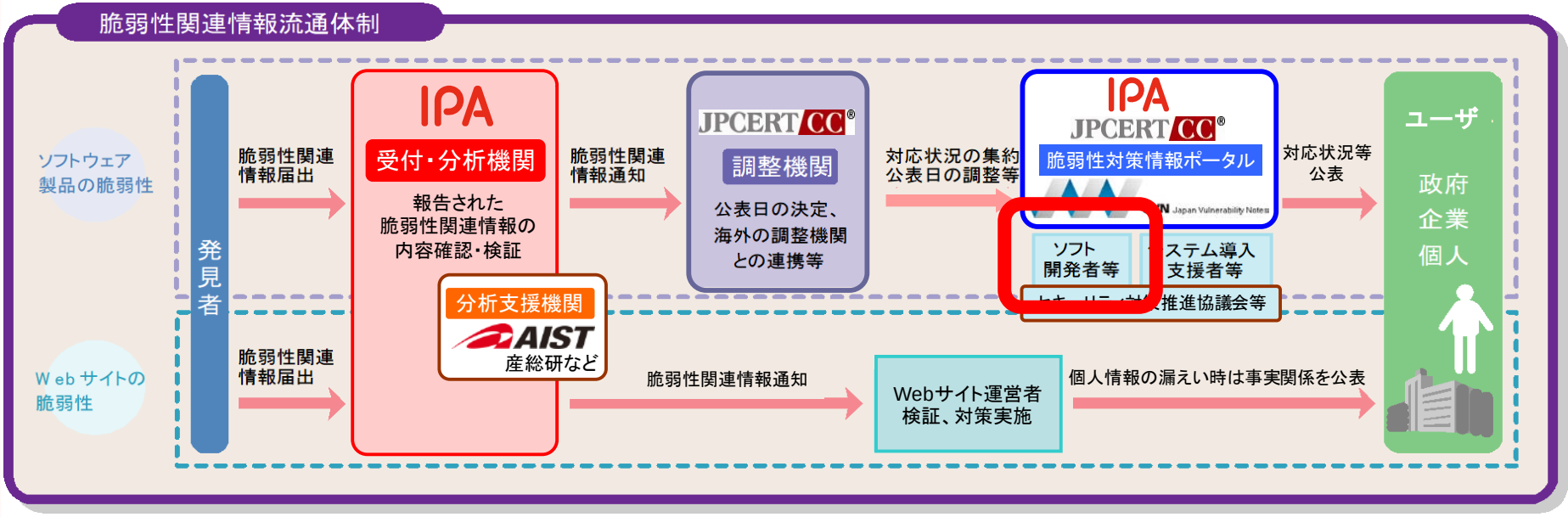



※JPCERT/CC：一般社団法人 JPCERT コーディネーションセンター、産総研：国立研究開発法人産業技術総合研究所

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）

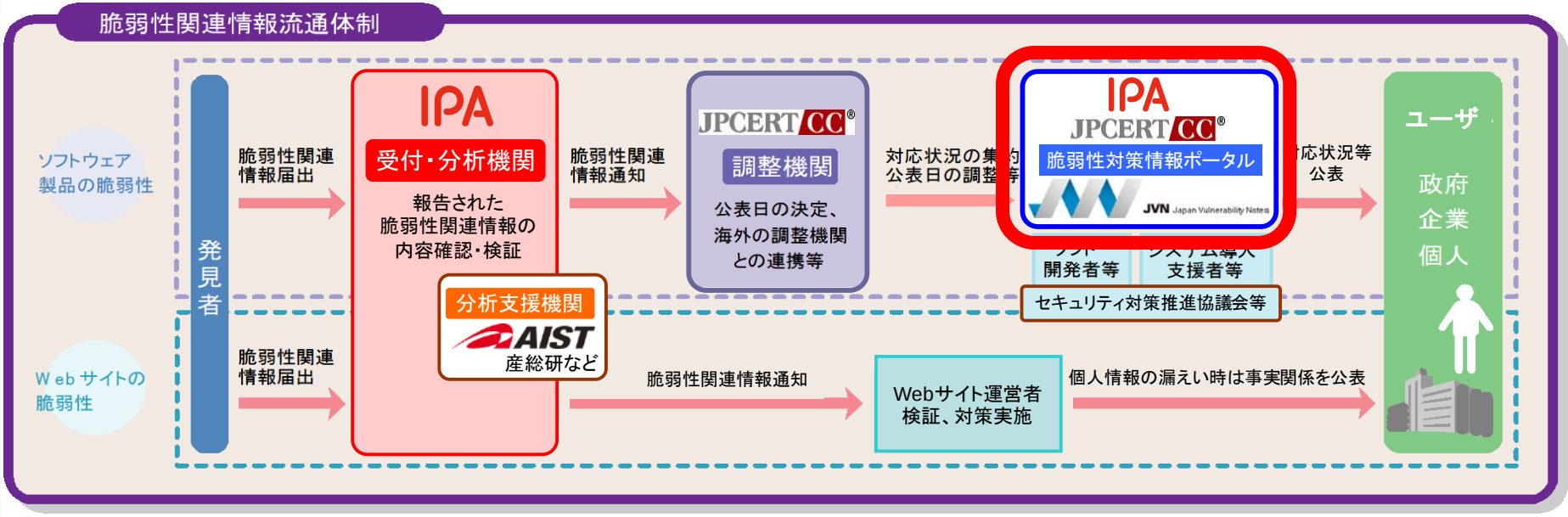



※JPCERT/CC：一般社団法人 JPCERT コーディネーションセンター、産総研：国立研究開発法人産業技術総合研究所

## 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）




※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。

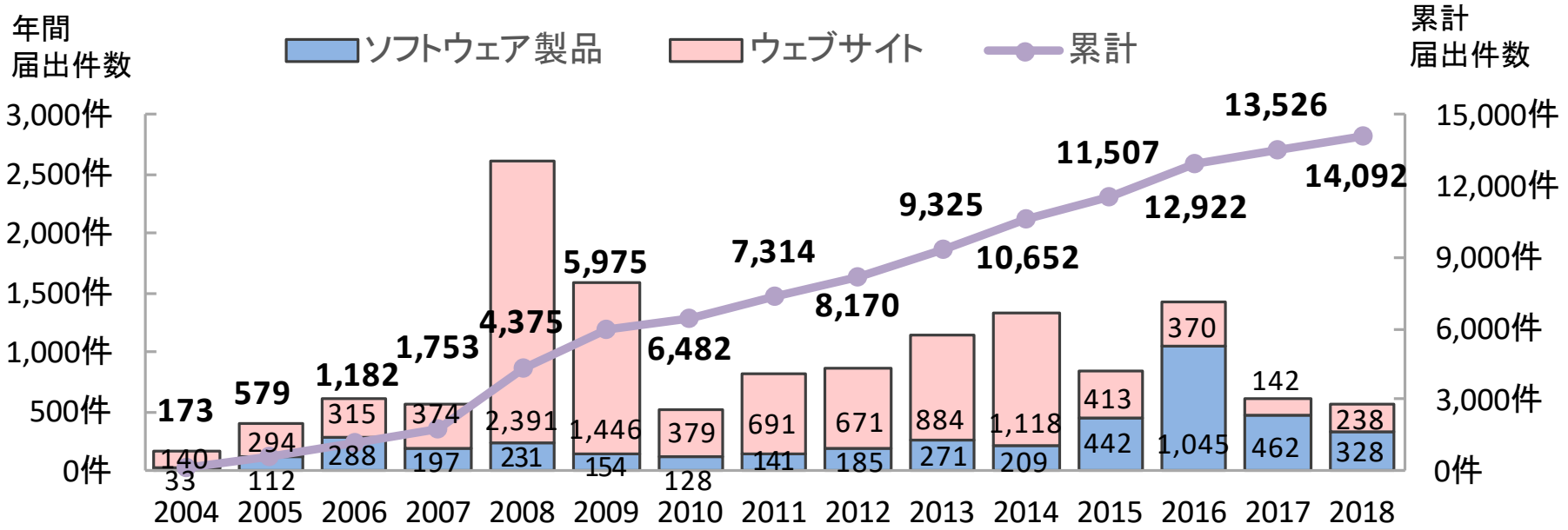
# JVN（Japan Vulnerability Notes）
## 脆弱性対策情報ポータルサイト

https://jvn.jp/jp/


# 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

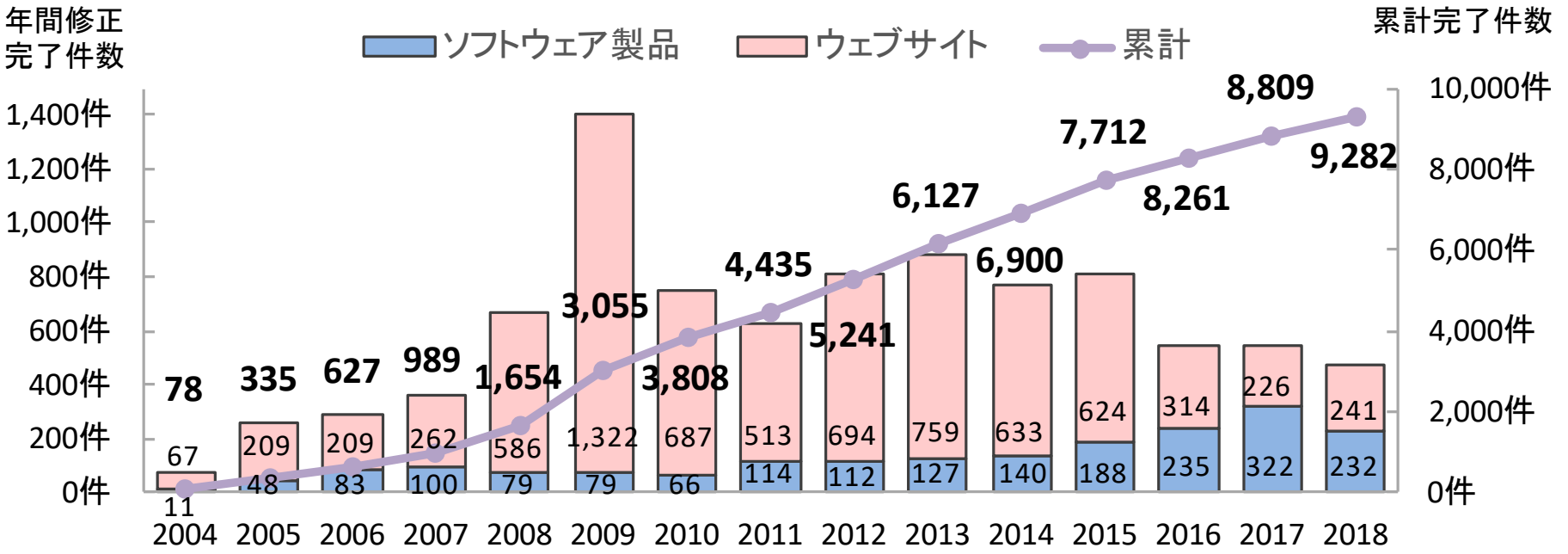
→ 1就労日あたり **3.99** 件




**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




**脆弱性関連情報の修正完了件数**（2018年12月末迄）