IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

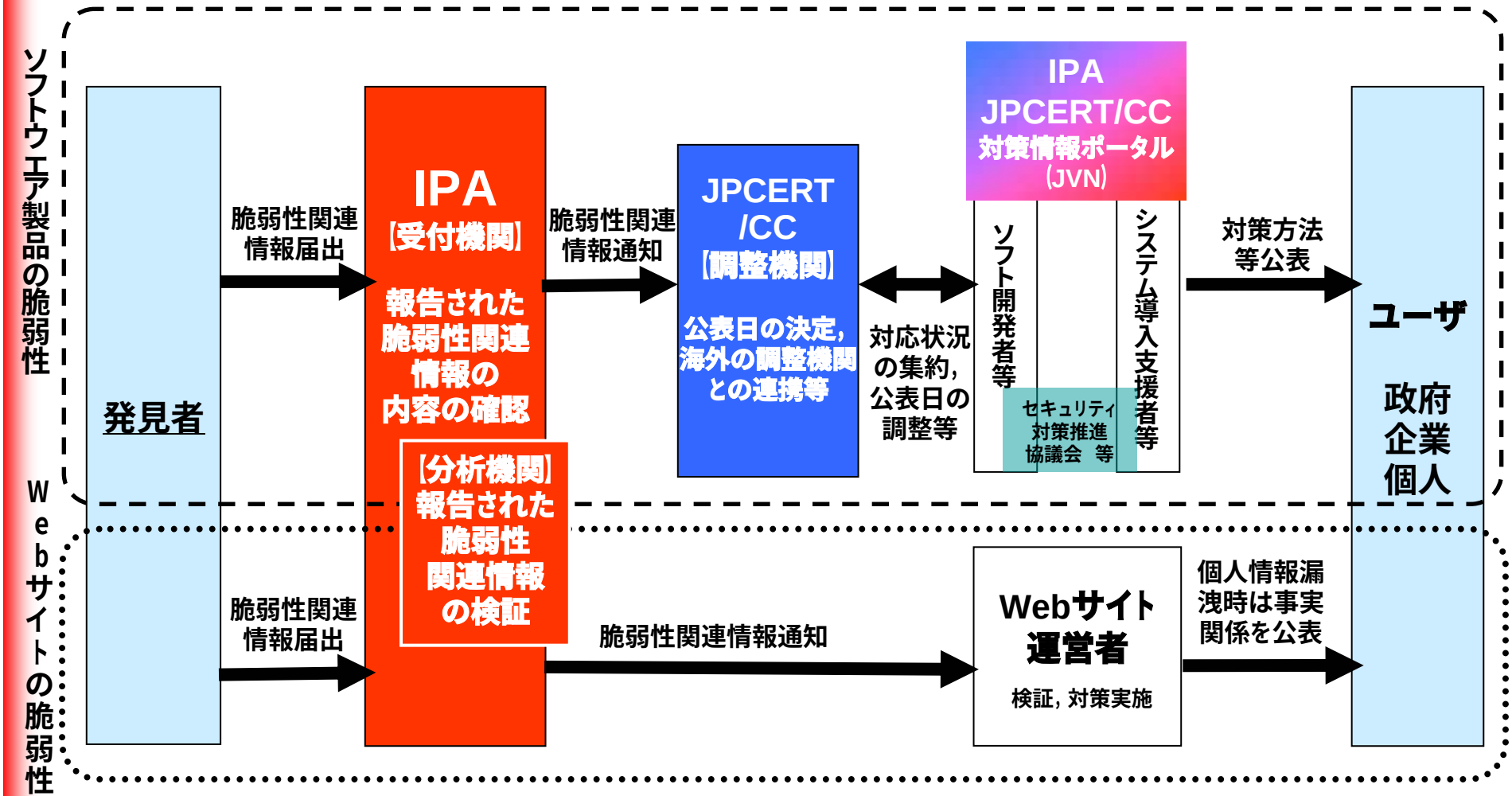
脆弱性情報流通体制における受付･分析機関の役割について

独立行政法人 情報処理推進機構
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

脆弱性情報流通体制における受付，分析機関の役割

- 脆弱性関連情報の届出受付
  - ソフトウェア製品およびウェブアプリケーションに関する脆弱性関連情報の届出受付
  - ソフトウェア製品の場合：JPCERT/CCへの通知
  - ウェブアプリケーションの場合：サイト運営者への通知
  - 発見者と関係者との情報交換の仲介
- 脆弱性関連情報の検証，影響分析
- 対応状況，対策情報の公表（JPCERT/CCと共同）
- 統計情報の定期的公表による脆弱性対策促進
- 海外などで発見・公表された脆弱性の分析・評価

脆弱性情報流通体制における受付機関，分析機関の位置づけ



脆弱性関連情報の届出受付

- 取り扱う脆弱性関連情報
  - ソフトウェア製品の脆弱性に関する情報
  - ウェブアプリケーションの脆弱性に関する情報
- 届出受付方法
  - 脆弱性関連情報の取扱いホームページ
    届出方法，届出様式，記入の手引き，届出記入例，注意事項など
    http://www.ipa.go.jp/security/vuln/index.html
  - 電子メールで受け付け
    届出メールアドレス： vuln-info@ipa.go.jp
  - PGPによる暗号化を要請
    PGP公開鍵： http://www.ipa.go.jp/security/pgp/index.html
  - 今秋を目処にウェブによる届出システムを開始予定

ソフトウェア製品に関する脆弱性
ー IPAの役割 ー

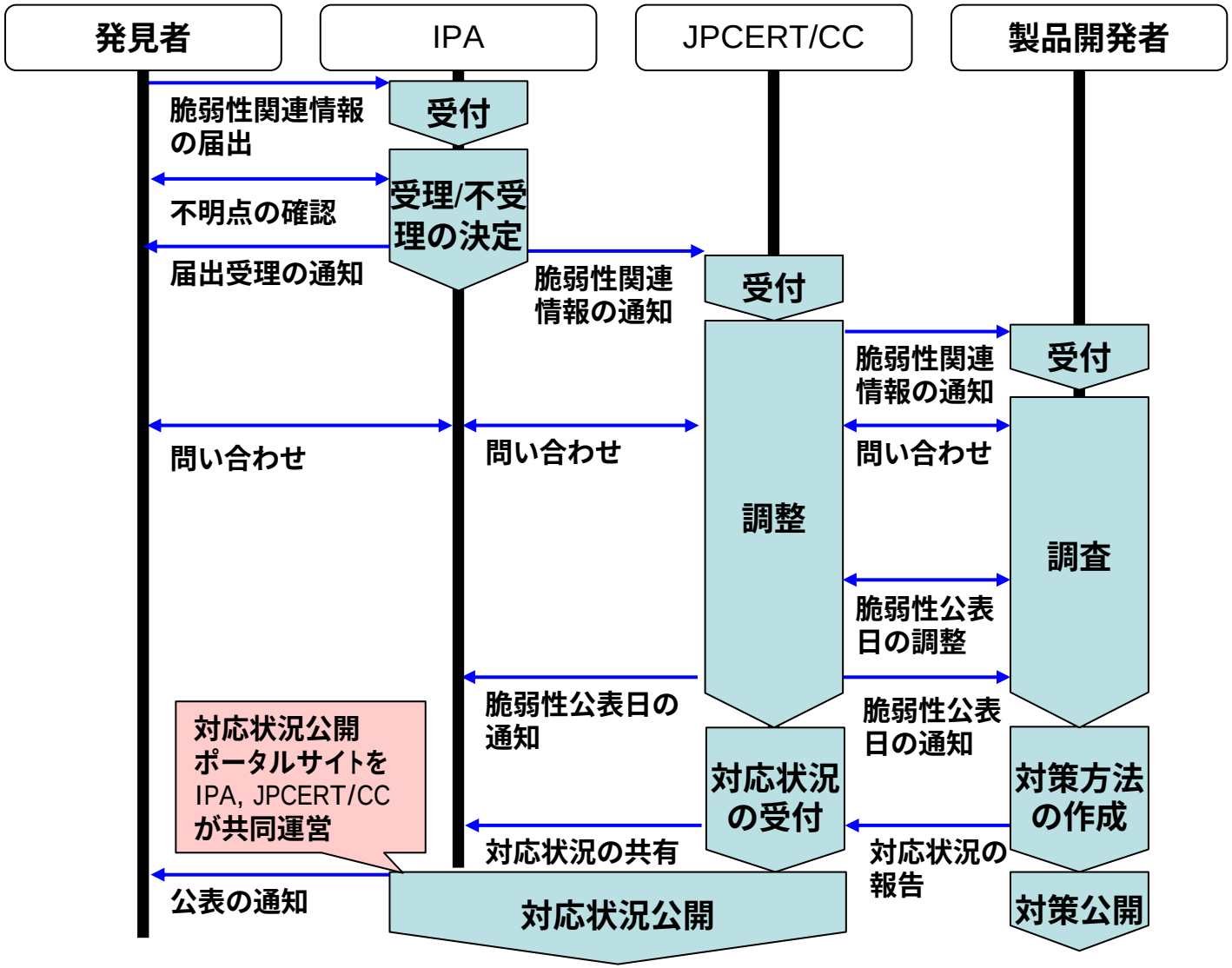
- 発見者の届出窓口はIPA
- 既に報告されている脆弱性かなどの確認を行い，取扱いが妥当と判断した脆弱性関連情報をJPCERT/CCへ通知
- 可能な限り，届出された脆弱性関連情報を検証（検証環境構築が可能な場合）
- 発見者と製品開発者との情報交換の仲介
- JPCERT/CCと連携し対策情報公開
- 統計情報の定期的公表

ソフトウェア製品に関する脆弱性 ー 対象，届出項目 ー

- 対象とする製品
  - OSやブラウザなど，クライアント上のソフトウェア
  - データベース管理システム，ウェブサーバなど，サーバ上のソフトウェア
  - ソフトウェアを組み込んだ汎用的なハードウェア製品
- 届出項目
  - 届出者情報

    氏名，メールアドレスなど，連絡に必要な情報
  - 届出者情報の取扱い
  - 脆弱性関連情報
    - 入手先，対象ソフトウェア，脆弱性の種類，再現手順，再現の状況，脆弱性による脅威，回避策等
  - 他組織への届出状況
  - 今後の連絡について

ソフトウェア製品に関する脆弱性
― 処理の流れ ―



ソフトウェア製品に関する脆弱性
― 処理の流れ ―

1. 発見者は，IPA に脆弱性関連情報を届出
2. IPA は，脆弱性関連情報をJPCERT/CC に通知，JPCERT/CC は，製品開発者に脆弱性関連情報を通知
3. 製品開発者は，脆弱性検証を行い，その結果をJPCERT/CC に報告
4. 製品開発者は，脆弱性情報の公表日までに対策方法を作成するよう努力
5. JPCERT/CC と製品開発者は，脆弱性情報の公表に関するスケジュール調整し決定
6. IPA およびJPCERT/CC は，脆弱性関連情報，および 2 および 3 で連絡した製品開発者の脆弱性検証結果と対応状況を公表
7. IPA は，統計情報を少なくとも一年に一度は公表

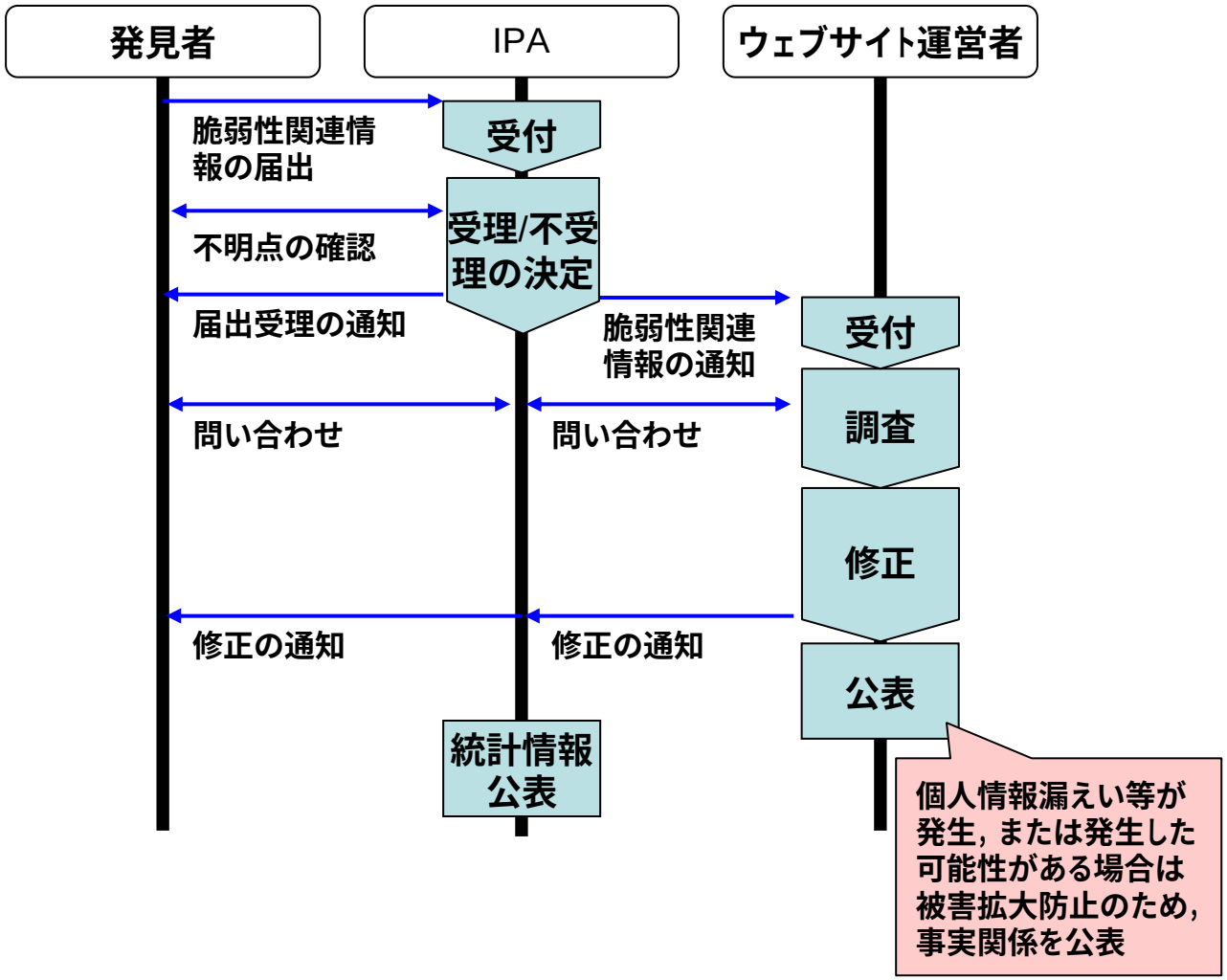
ウェブアプリケーションに関する脆弱性 ー IPAの役割 ー

- 発見者の届出，問合せ窓口
- 脆弱性の報告を受けたウェブアプリケーションの検査，修正についてウェブサイト運営者と調整
- 検証，修正の支援が必要な場合，検証方法，修正方法の助言
- ウェブ運営者の要請＆IPAが必要と判断した場合，脆弱性の再現確認，修正完了時の確認
- 発見者とウェブサイト運営者との情報交換の仲介
- 統計情報の公表

ウェブアプリケーションに関する脆弱性 ー 対象，届出項目 ー

- 対象：カスタムウェブアプリケーション
  - インターネットのウェブサイトなどで、公衆に向けて提供するサービスを構成するシステムで，そのソフトウエアがサイトごとに個別に設計･構築され、一般には配布されていないもの
- 届出項目
  - 届出者情報
    - 氏名，メールアドレスなど，連絡に必要な情報
  - 届出者情報の取扱い
  - 脆弱性関連情報
    - ウェブサイトのURL，脆弱性の種類，発見経緯，脆弱性と判断した理由，脆弱性により発生しうる脅威など
  - 他組織への届出状況
  - 今後の連絡について

ウェブアプリケーションに関する脆弱性 ― 処理の流れ ―



ウェブアプリケーションに関する脆弱性 ― 処理の流れ ―

1. 発見者は，IPA に脆弱性関連情報を届出
2. IPA は，受け取った脆弱性関連情報に関し，原則としてウェブサイト運営者に通知
3. ウェブサイト運営者は，脆弱性関連情報の内容を検証し，影響の分析を行った上で，必要に応じて脆弱性を修正
4. 個人情報漏洩等の事件があった場合，ウェブサイト運営者は，その事実を一般に公表するなど適切な処置
5. IPA は，統計情報を少なくとも一年に一度は公表

ウェブアプリケーションに関する脆弱性 ー ウェブサイト運営者へのお願い ー

- 通知を受けたら，脆弱性の内容の検証および脆弱性のおよぼす影響を正確に把握した後，影響の大きさを考慮し，脆弱性を修正してください。
- 当該脆弱性関連情報に関して検証した結果，および修正した場合その旨をIPA に連絡してください。
- IPA からの問合せに的確に答えてください。
- 脆弱性を修正するために，IPA と協議の上，発見者の了解のある場合，発見者と情報交換を行うことが可能です。
- 脆弱性が修正されるまでの間は，脆弱性関連情報を第三者に漏洩しないように管理してください。ただし，ウェブサイト運営者が脆弱性修正を依頼した外部機関，およびウェブサイトの管理を委託している外部機関には，秘密保持契約を締結した上で脆弱性関連情報を連絡することができます。

ウェブアプリケーションに関する脆弱性 ー ウェブサイト運営者へのお願い ー

- ウェブアプリケーションの脆弱性関連情報に関して，積極的に公表する必要はありません。
- ただし，この脆弱性が原因で，個人情報が漏洩したなどの事案が発生した，または発生した可能性がある場合，二次被害の防止および関連事案の予防のために，以下の項目を含むように公表してください。また，当該個人からの問い合わせには，的確に回答するようにしてください。
  - 個人情報漏洩の概要
  - 漏洩したと推察される期間
  - 漏洩したと推察される件数
  - 漏洩したと推察される個人情報の種類（属性など）
  - 漏洩の原因
  - 問合せ先

発見者に関する情報の取扱い

IPA

- 個人情報の収集目的と利用範囲
  - 届出られた脆弱性関連情報の内容を確認するため
  - 発見者の承諾に基づき，対策情報とともに謝辞等に示すため
- 個人情報の第三者への開示
  - 発見者の承諾がない限り，個人情報を第三者に開示することはありません。
  - ただし，裁判所命令を受けた場合，法律に基づき開示しなければならない場合，発見者の皆さんの権利/財産/安全などを保護/防御するために必要であると合理的に判断できる場合には，個人情報を開示することがあり ます。

発見者に関する情報の取扱い

- 個人情報は厳重に管理します
  - 個人情報の紛失，誤用，改変を防止するために，セキュリティ対策を実施します。
  - 個人情報は，IPAセキュリティセンターが管理する区画の外に持ち出されることはありません。
  - 電子データについてはIPAセキュリティセンターの担当職員以外が参照できないような処置を講じます。
  - FAX等の印刷物については施錠可能な収納庫に保管し利用記録等による管理を行います。
- 不要となった情報は破棄します
  - 届出いただいた情報の取扱いを終了する時点（取扱期限を経過した場合，脆弱性の修正が完了するなど取り扱う必要が無くなった場合）で，関連する個人情報はすべて適切な方法で破棄します。

発見者となる皆様へのお願い

- 脆弱性関連情報の発見，取得にあたっては，法律に触れることのないよう注意をお願いします。
- IPAは情報の入手方法については関知しませんが，違法な手段で入手された事が明らかなものは受け付けない場合があります。
- IPAが届出を受け付けた場合であっても，入手手段が合法であると判断したわけではありませんし，発見者の法的責任が免責されるわけではありません。
- 法的問題に関しては「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」の21～23ページを参考にしてください。

http://www.ipa.go.jp/security/ciadr/partnership_guide_200407.html