調整機関の役割

JPCERT コーディネーションセンター
伊藤友里恵

JPCERT CC

JPCERT/CC概要

- Japan Computer Emergency Response Team Coordination Center
  - 緊急事態 (Emergency) への対応 (Response)
  - コンピュータセキュリティインシデントに関する調整、対応の協調、連携など
- 1996年10月設立
  - 1992年ころにボランティアではじまったグループを起源とするエンジニア集団
  - 非営利目的、国からの予算で運営
- 2003年3月有限責任中間法人に
- 日本で最初に ('98) FIRST に加盟した CSIRT
  - 日本のPOC(窓口) CSIRTとして国際的に認知
- 2004年7月8日 経済産業省告示にて脆弱性情報流通調整機関として指定

JPCERT/CCの活動

事後対応から事前対応に

JPCERT CC

脆弱性情報ハンドリング

- 脆弱性情報ハンドリングとは
  - 脆弱性関連情報を必要に応じて開示することで、脆弱性情報の　悪用、または障害を引き起こす危険性を最小限に食い止めるためのプロセスです。JPCERT/CCは、このプロセスの調整役(コーディネーター)として、影響のある製品を持つ製品開発者に脆弱性情報の連絡、対応を依頼します。

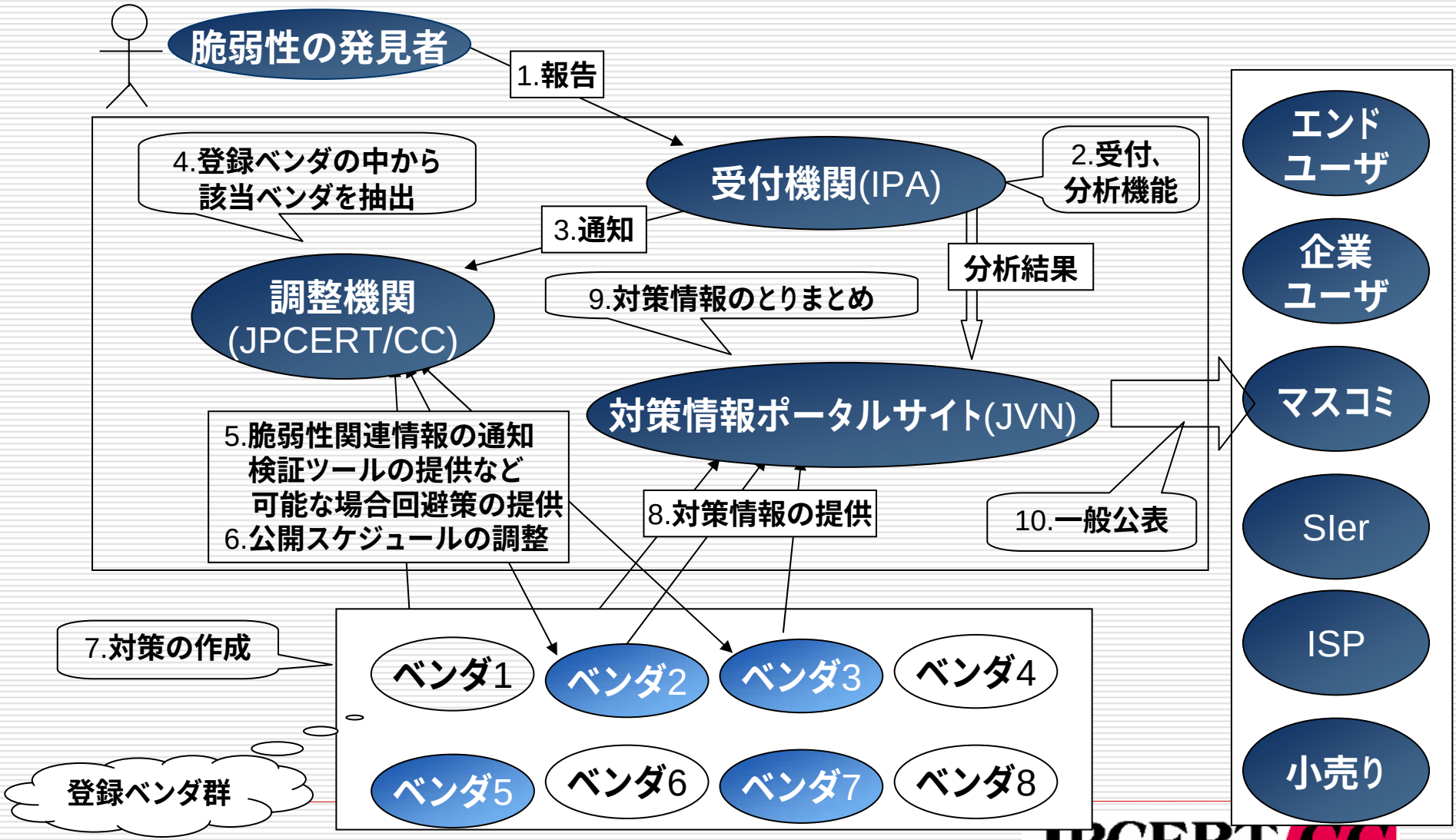
- 一般公開前の脆弱性情報を機密情報として扱いそれを製品開発者に伝えることで、製品の対策情報等を事前に作成してもらう
  - 取り扱う脆弱性情報
    - 特定の製品開発者の特定の製品に関わる脆弱性
    - 複数の製品開発者にまたがる、公開技術の根本的な問題による脆弱性
- 脆弱性情報の一般公開と同時に、対応策等も一般に公開されるようにするための仕組み

JPCERT CC

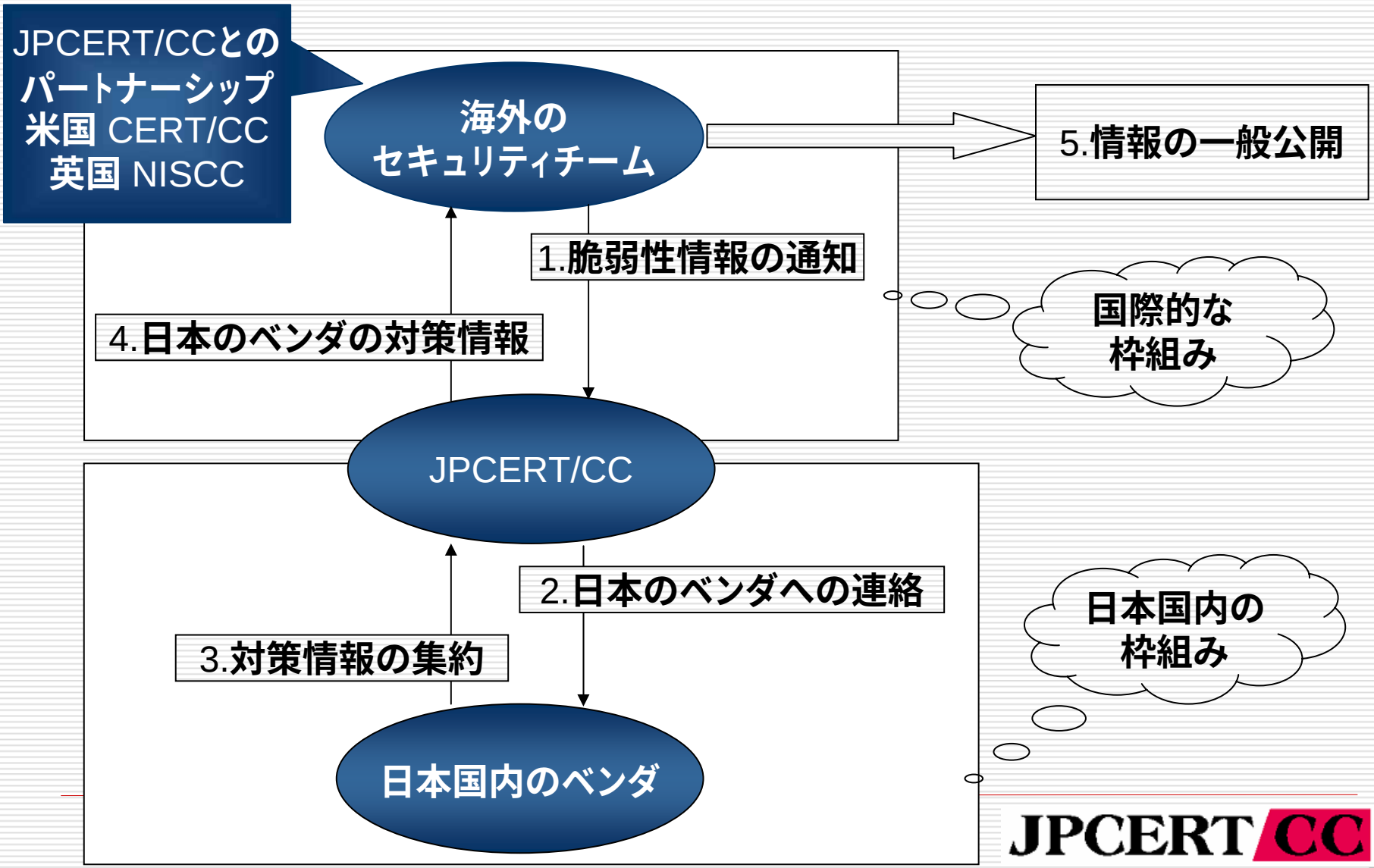
なぜ調整機関が国際的に必要か

- **公表日一致の原則**
  - 脆弱性情報と、製品開発者の対応状況は同時に公表
  - 影響が複数の製品開発者に及ぶ場合、特に同時公表のための、*中立な第三者機関によるスケジュール調整* が必要
- **製品開発者へのコンタクト**
  - 影響のある製品を持つ製品開発者を、一社でも多く把握
    - 可能な限りの範囲への、公平な情報提供
    - 各組織内の、正しい連絡窓口の確保
      情報が適切かつ有効に使われる窓口の構築
- **発見者、製品開発者間の調整**
  - 異なるモチベーションの調整
- **機密性の高い情報の、安全な取り扱い**

国内体制での調整機関のポジション



国際的な枠組みについて



ベンダにとってのメリット

- 脆弱性関連情報を事前に入手することで、
  情報が公開されてから対応を始めるやりかたではなく、
  情報公開前から対応を始めることができる
- 上記理由によって、余裕のある対応ができる
- 脆弱性情報の一般公開と同時に対策情報を公開することで、ユーザへの影響を低減できる
- JPCERT/CCが各製品開発者の対応状況を考慮し、一般公開スケジュールを調整することが可能
- 脆弱性情報への対応状況を、ポータルサイトを通して、周知できる
  - http://jvn.jp

枠組みへの参加：
JPCERT/CC 製品開発者登録リストに登録

- JPCERT/CCから情報連絡を受けるためには、JPCERT/CC 製品開発者リストへのPOC登録をお願いします。

- JPCERT/CC 製品開発者登録リストとは
  - JPCERT/CCが、脆弱性情報を製品開発者に連絡する際、影響を受ける可能性のある製品開発者を特定するためのリスト

- 手順は以下の通りです。
  1. 製品開発者はPOC仮登録情報を提出する
     - 製品開発者リスト仮登録申請様式
       http://www.jpcert.or.jp/form/poc.txt
  2. JPCERT/CC から、POC本登録に必要な書類を提示する
  3. 製品開発者はPOC本登録のための必要書類を作成し提出する
  4. JPCERT/CCと製品開発者の間でミーティングを行う
  5. JPCERTコーディネーションセンター製品開発者リスト登録規約への合意
  6. 実際に登録をする

製品開発者へのお願い

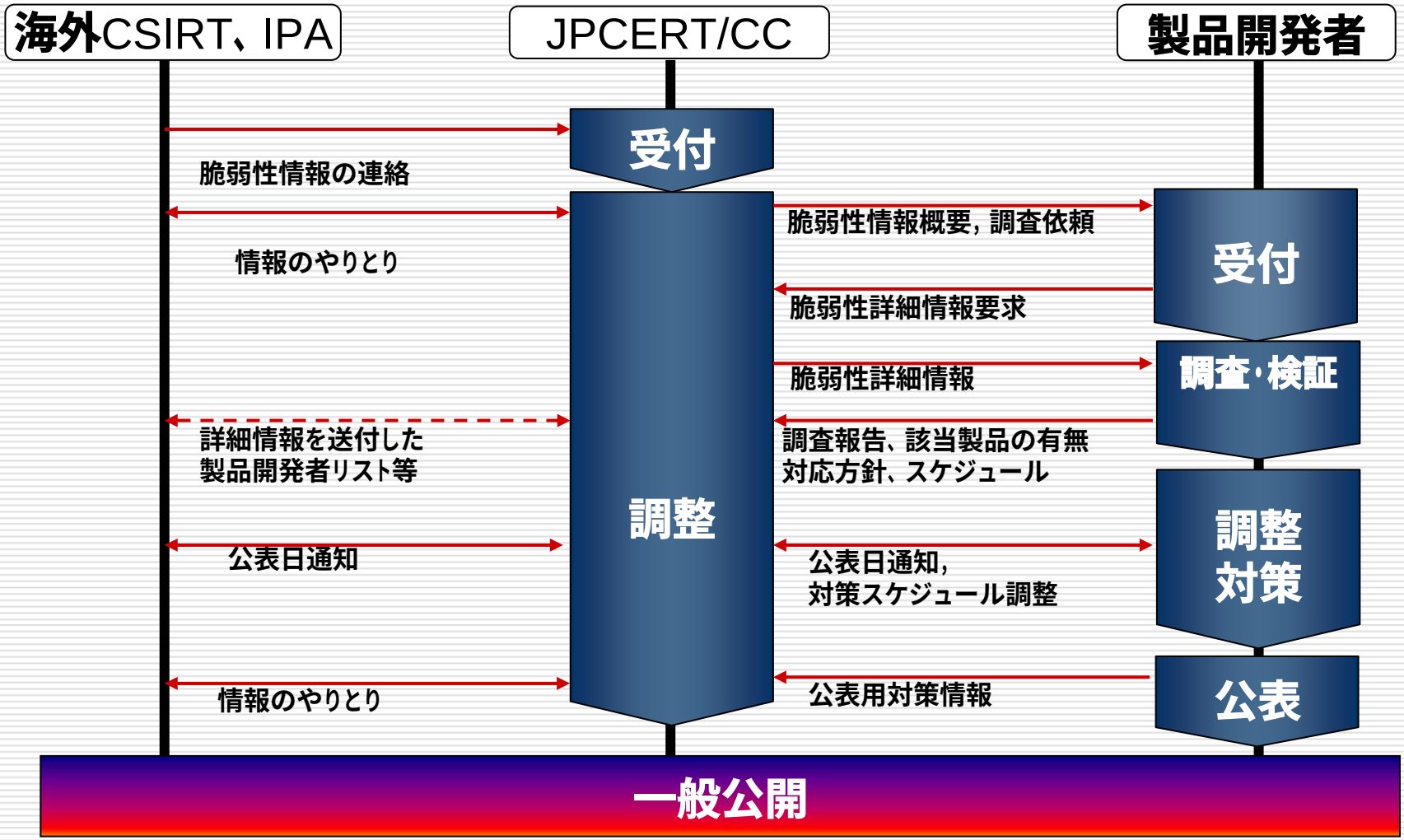
1. 社内体制の構築と窓口の登録
2. 受付：脆弱性概要情報の取り扱い
3. 検証：脆弱性詳細情報の取り扱いと製品の調査、JPCERT/CC への連絡
4. 調整：公表日時の決定
5. 対策：対策情報の作成
6. 公表：対応状況の連絡と公表

脆弱性情報の公表

- 脆弱性情報を公表する理由
  - 汎用目的のソフトウェアの脆弱性は公開される必要がある
  - 悪意のある第3者が、脆弱性情報を発見し、対策情報なく公開してしまうケースを防ぐ
  - 管理者に、パッチの適用を動機付けさせる
  - 全ての安全性の懸念を認識しきれない

- 製品開発者支援
  - 製品開発者、研究者、関係者と調整し、スケジューリング
  - 脆弱性情報と、対策情報の同時公表
  - 影響を受ける製品開発者の情報公開をサポートする

JPCERT/CCと製品開発者のハンドリング(やり取り)概要図



参照情報

お問い合わせ先

JPCERTコーディネーションセンター

- Email：office@jpcert.or.jp
- Tel：03-3518-4600

- http://www.jpcert.or.jp