# 脆弱性情報流通体制

JPCERT コーディネーションセンター
伊藤友里恵

JPCERT CC

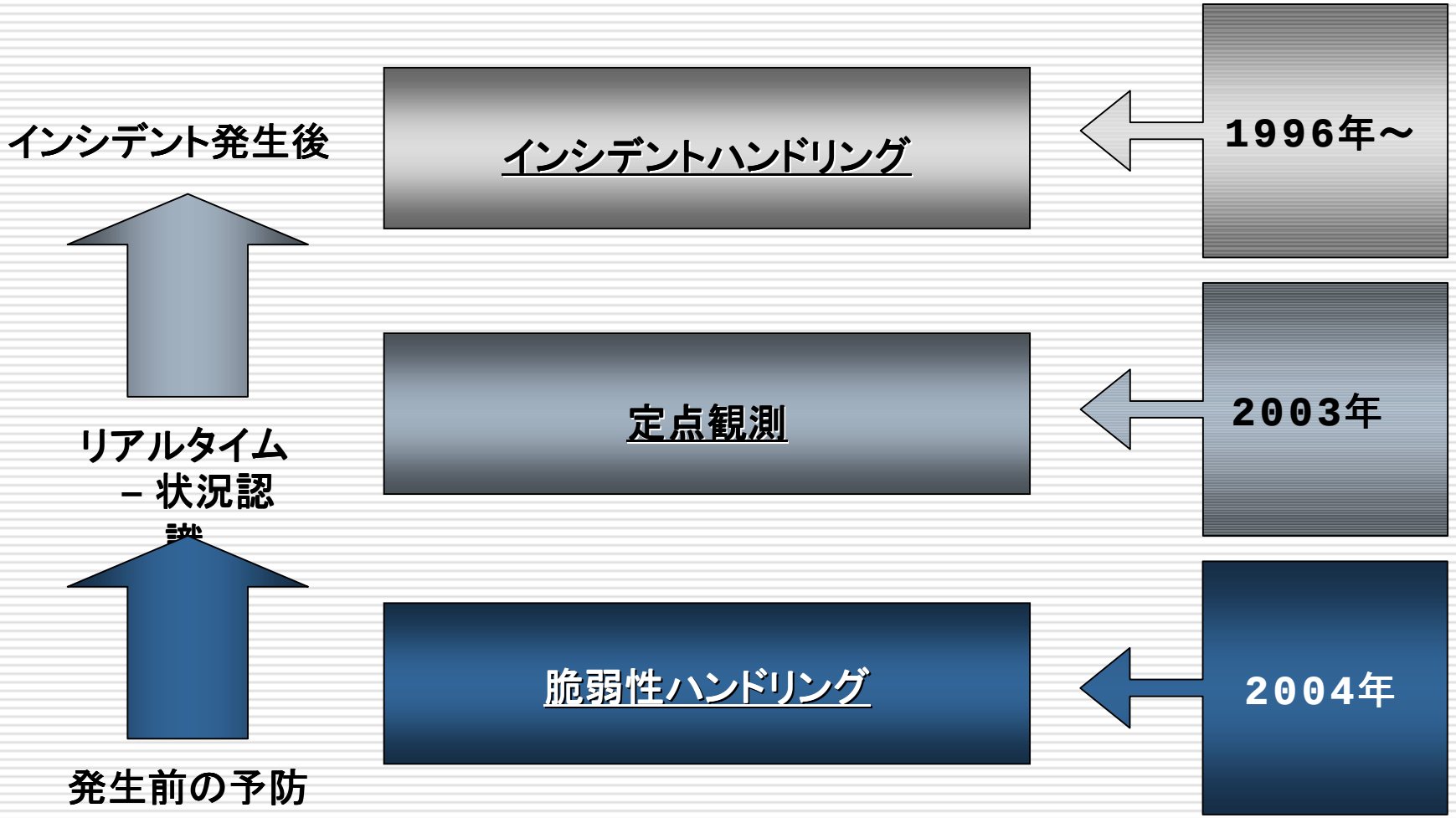
# JPCERT/CC概要

- 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

# JPCERT/CCの活動

事後対応から事前対応に




JPCERT CC

# 脆弱性とは?

- 脆弱性の定義は、人によってまちまち
  - CERT/CCとJPCERT/CCは、下記の認識を共有
  - 明白、または暗示的なセキュリティポリシーの違反
  - 通常ソフトウェアの欠陥によって引き起こされる
  - 頻繁に予期しない挙動を引き起こす
- 明確に脆弱性から除外するもの
  - トロイの木馬 (悪意のある添付つきメール)
  - ウィルス、ワーム (自己増殖型コード)
  - 侵入ツール (スキャナ、ルートキット等)
- 脆弱性とは、技術的欠陥で、上記の事象を存在させるもの

# 脆弱性情報ハンドリングとは

- 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

# 脆弱性ハンドリング

- 脆弱性情報の報告を受ける
  - 海外のパートナーCSIRT
  - 国内の報告はIPAから
  - パブリックモニタリング
    - メーリングリスト
    - ウェブサイト
- 脆弱性報告の再現、分析、優先順位付け
  - 脆弱性として扱うか否か
  - インパクト分析
  - 影響は分析　どんなシステムに影響があるか、重要インフラへの影響は
  - 攻撃手法はあるか
  - 攻撃はアクティブに始まっているか
  - どんな対応が適切か

# 脆弱性ハンドリング　2

- ハンドリング方針きめ
  - 優先順位付け
  - 対応タイプ/レベル付け
    - ベンダコーディネーションするのか
    - アラートを出すのか
    - JVNに情報をアップデートするだけか
    - 重要インフラにヘッズアップが必要か
- セキュリティマトリックス:
  - 既知の脆弱性か?
  - すでに攻撃が始まっているか?
  - インターネットインフラへのリスクは?重要インフラへのリスクは?
  - どの範囲のシステムに影響するか?
  - インパクトは?
  - 攻撃手法は簡単か?それとも困難?
  - 攻撃手段は明らかになっているか?

# 脆弱性ハンドリングの調整の難しさ
# 情報の中継ぎをしているだけではない!

- 脆弱性が報告されたテクノロジーの概要調査・把握
  - コーディネーション用情報、公開用アドバイザリー作成にも必要
  - 一般公開後のメディアへの対応
- マーケット把握、インパクト確認、製品の確認
  - 対策情報の公開方法、対策情報徹底のためにも必須
- 検証ツール等の調査。ハンドリング前に、正常に動くか、使い方をJPCERT/CC内で確認

JPCERT CC

# 脆弱性ハンドリングの調整の難しさ
# 情報の中継ぎをしているだけではない!

- 脆弱性が報告されたテクノロジーの概要調査・把握
  - コーディネーション用情報、
    必要
  - 一般公開後のメディアへの

有益な付加情報の作成

- マーケット把握、インパクト確認、製品の確認
  - 対策情報の公開方法、対策情報徹底のためにも必須

- 検証ツール等の調査。ハンドリング前に、正常に動くか、使い方をJPCERT/CC内で確認

# 多様な開発形態に対応するための努力

- コンフリクトする2つの要素のバランスを取りながら、毎回検討をしつつ事例を重ねている。
  1. 情報の無用な拡散を防ぐこと。情報漏えいのリスクの低減。
  2. できるだけ多くの開発者が製品への対応を確実にタイムリーに行えること。

- 多様な開発形態とシナリオ：
  - OEM、外注先企業、子会社、関連会社、フリーソフト、国際ベンダ
  - 特定製品の脆弱性の対応
  - 複数製品が同時に影響を受ける脆弱性の対応

- 毎回、扱う脆弱性の内容と、開発者の開発形態の条件を鑑みて、情報転送ガイドラインを調整している。
  - グループ会社の事前登録
  - 海外調整機関とのベンダ通知状況のリアルタイムな共有

# 多様な開発形態に対応するための努力

- コンフリクトする2つの要素のバランスを取りながら、毎回検討をしつつ事例を重ねている。
  1. 情報の無用
  2. できるだけ多 ること。

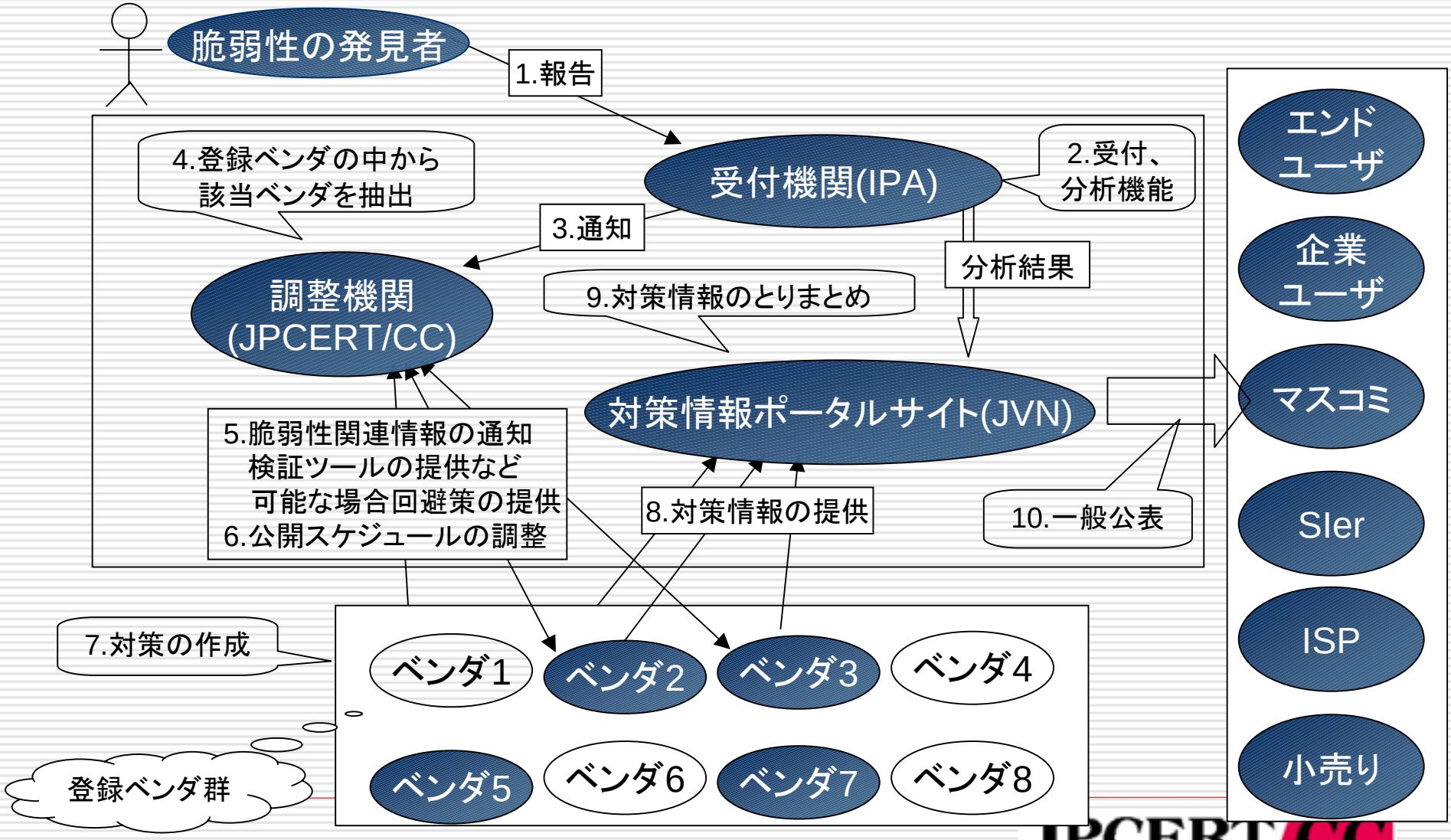
安全側に倒した原則のもと

柔軟に調整できるために

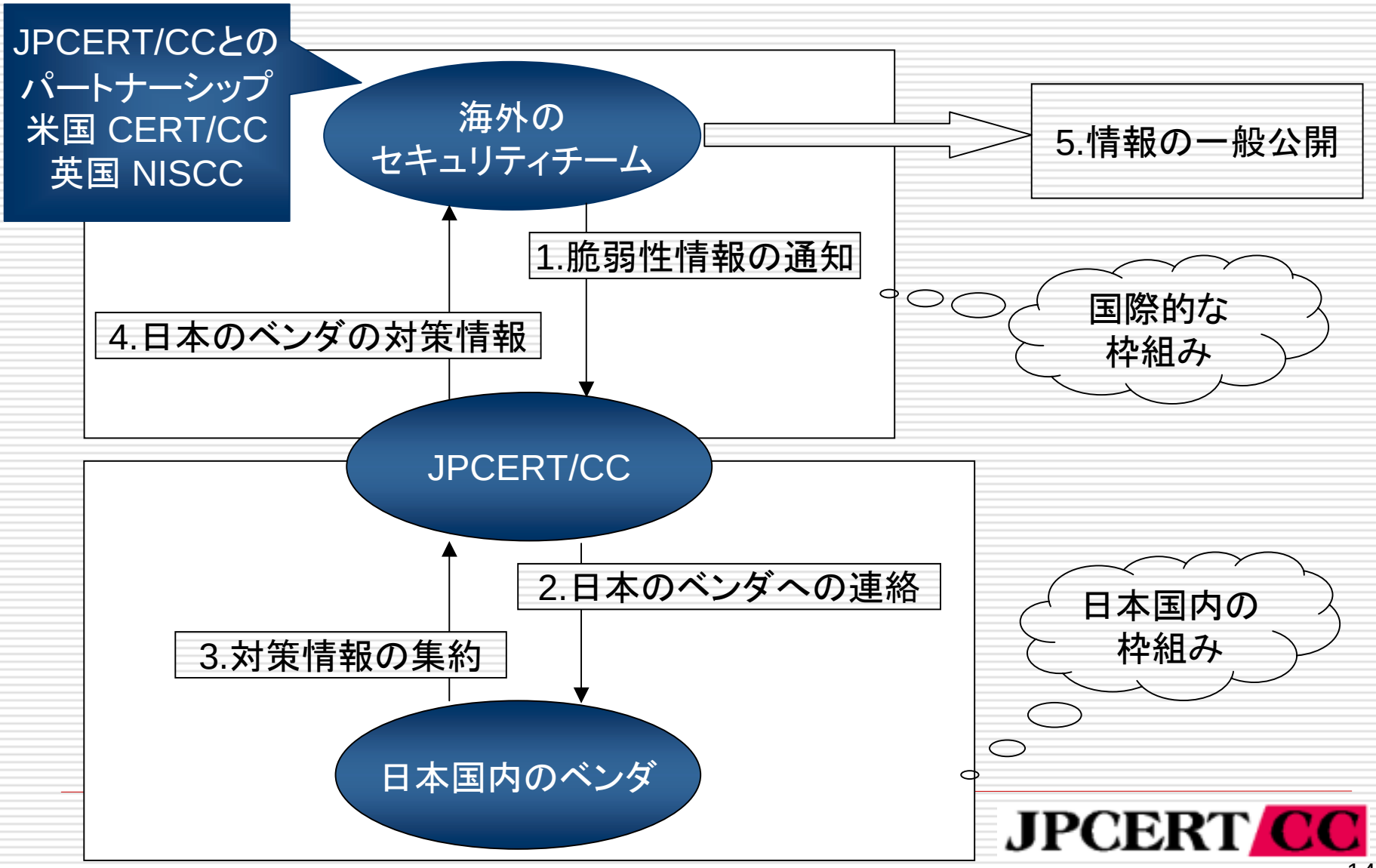
**強い信頼関係の構築が必要**

- 多様な開発形態
  - OEM、外注
  - 特定製品の
  - 複数製品が
- 毎回、扱う脆弱性の と、開発者の開発形態の条件を鑑みて、情報転送ガイドラインを調整している。
  - グループ会社の事前登録
  - 海外調整機関とのベンダ通知状況のリアルタイムな共有

# 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/

# 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

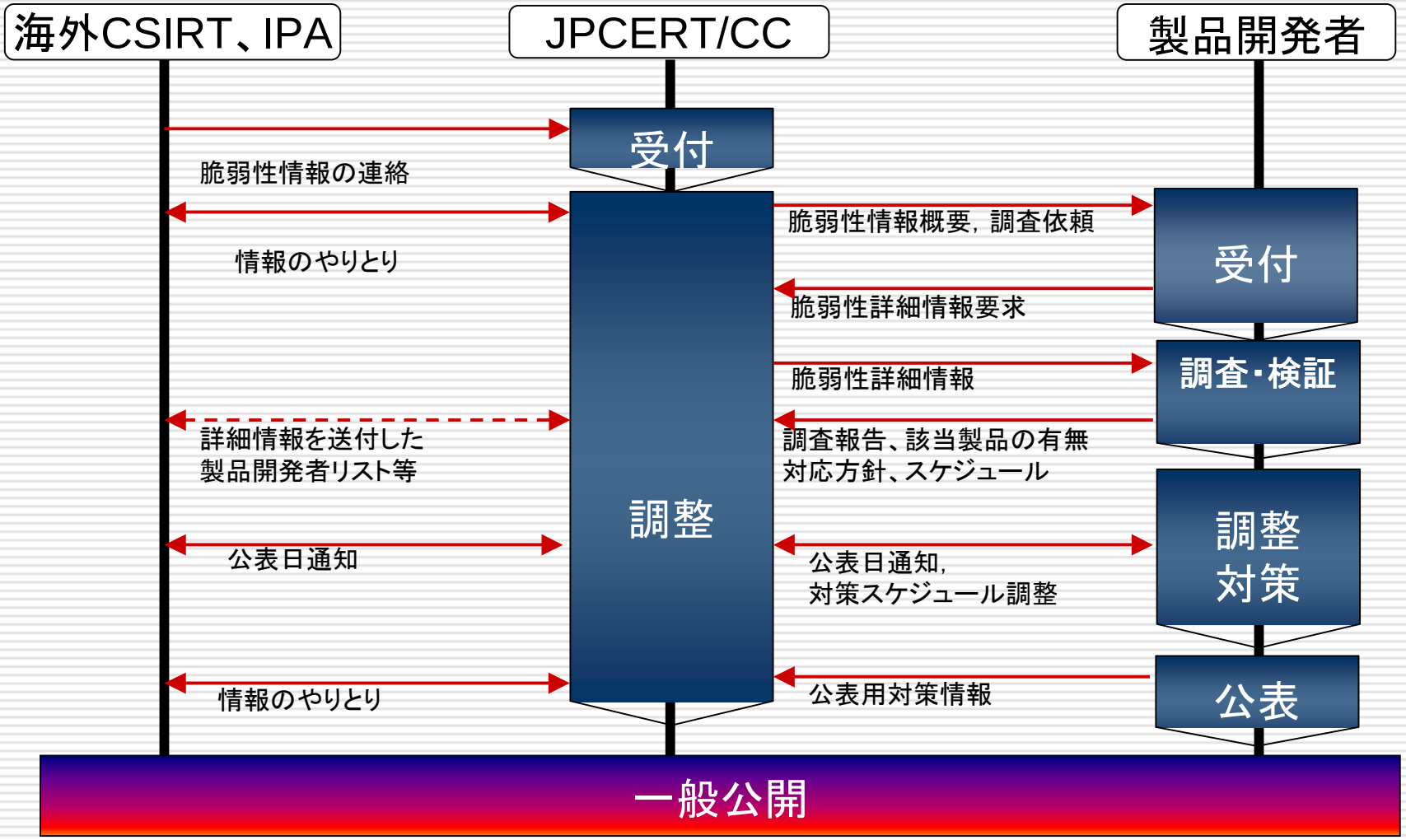
- 製品開発者支援
  - 製品開発者、研究者、関係者と調整し、スケジューリング
  - 脆弱性情報と、対策情報の同時公表
  - 影響を受ける製品開発者の情報公開をサポートする

# システム管理者の人工に換算すると

- 2003年に5500件の脆弱性が報告されたこととは?
- 誰かが脆弱性の内容を読む必要あり
  - 5500×読解20分＝229日(脆弱性情報を読むだけに費やす)
- その内10%の脆弱性に影響を受けているとすると
  - 550脆弱性×パッチのインストールに1時間＝一台のマシンにパッチをあてるだけで69日
- セキュリティニュースを読んで、マシン一台にパッチをあてるだけで229＋69＝298日間

- セキュリティ速報を5分だけ読んで、ヒット確率を1%とすると、ほとんど65日間のコスト、または、非常に有能な管理者の25%のコストをかけることになる。

# 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/

JPCERT CC