

## 製品開発ベンダーにおける 脆弱性関連情報取扱に関する 体制と手順整備のための ガイドライン

2004年9月

社団法人 電子情報技術産業協会

*Japan Electronics & Information Technology Industries Association*

社団法人 情報サービス産業協会

*Japan IT Services Industry Association*

情報通信ネットワーク産業協会

*Communications and Information network Association of Japan*

# 目次

1. ガイドライン作成の背景
2. ガイドラインの目的と範囲
3. ガイドラインの概要
4. 国内の脆弱性関連情報取扱手順の全体概要
5. 脆弱性関連情報取扱体制の立上げ
6. 脆弱性関連情報取扱体制の整備
7. 脆弱性関連情報取扱手順の整備
8. まとめと課題

# 1. ガイドライン作成の背景

脆弱性とは、ソフトウェア等において、コンピュータ・ウィルス、コンピュータ不正アクセス等の攻撃により、その機能や性能を損なう原因となり得る安全性上の問題箇所

## □ 背景

### ➤ 脆弱性対策を迅速に行うための国内体制の整備

- ・ 経済産業省の「ソフトウェア等脆弱性関連情報取扱基準」  
(経済産業省告示第235号; 2004年7月7日)  
<[http://www.meti.go.jp/policy/it\\_policy/press/0005399/0/040708jyoho.pdf](http://www.meti.go.jp/policy/it_policy/press/0005399/0/040708jyoho.pdf)>
- ・ IPA, JPCERT/CC他による「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」(2004年7月8日)

### ➤ 製品開発ベンダーの的確な対応が鍵

- ・ できるだけ速やかな調査と対策の準備
- ・ 脆弱性関連情報の漏洩と悪用防止

## 2. ガイドラインの目的と範囲

### □目的

製品開発ベンダーが脆弱性関連情報取扱に関する社内体制や取扱手順を制定する際の最低要件とあるべき方向性を示す

### □範囲

- ソフトウェア自体またはソフトウェアを組み込んだハードウェア等汎用性を有する製品を対象とする  
(経済産業省告示などでの「ソフトウェア製品」に相当)
- 脆弱性関連活動のうち、脆弱性関連情報の受取りから、調査、対策の作成、公表までの活動を取り扱う  
(対策の展開などは範囲外)

### 3. ガイドラインの構成

- 国内の脆弱性関連情報取扱手順の全体概要
- 脆弱性関連情報取扱体制の立上げ
  - 経営者の了解; 対象製品定義; ベンダーCSIRT等
  - JPCERT/CCへの登録
- 脆弱性関連情報取扱体制の整備
  - ベンダーCSIRT  
推進・管理組織
    - 製品開発部門
    - その他の部門
- 脆弱性関連情報取扱手順の整備
  - 情報の受付; 調査; 対策の作成; 対策の周知など

製品開発ベンダーにおいて脆弱性関連情報の受取りと社内の調査展開指示などを担当する窓口チーム; Computer Security Incident Response Team; ベンダー・シーサート

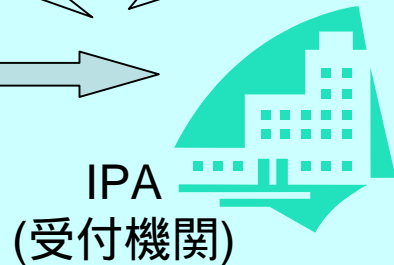
# 4. 国内の脆弱性関連情報取扱手順の全体概要

経済産業省告示「ソフトウェア等脆弱性関連情報取扱基準」

IPA等「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」



海外各国のCSIRT (米国CERT/CCなど)



脆弱性関連情報



製品開発ベンダー

ベンダーCSIRT

推進・管理組織

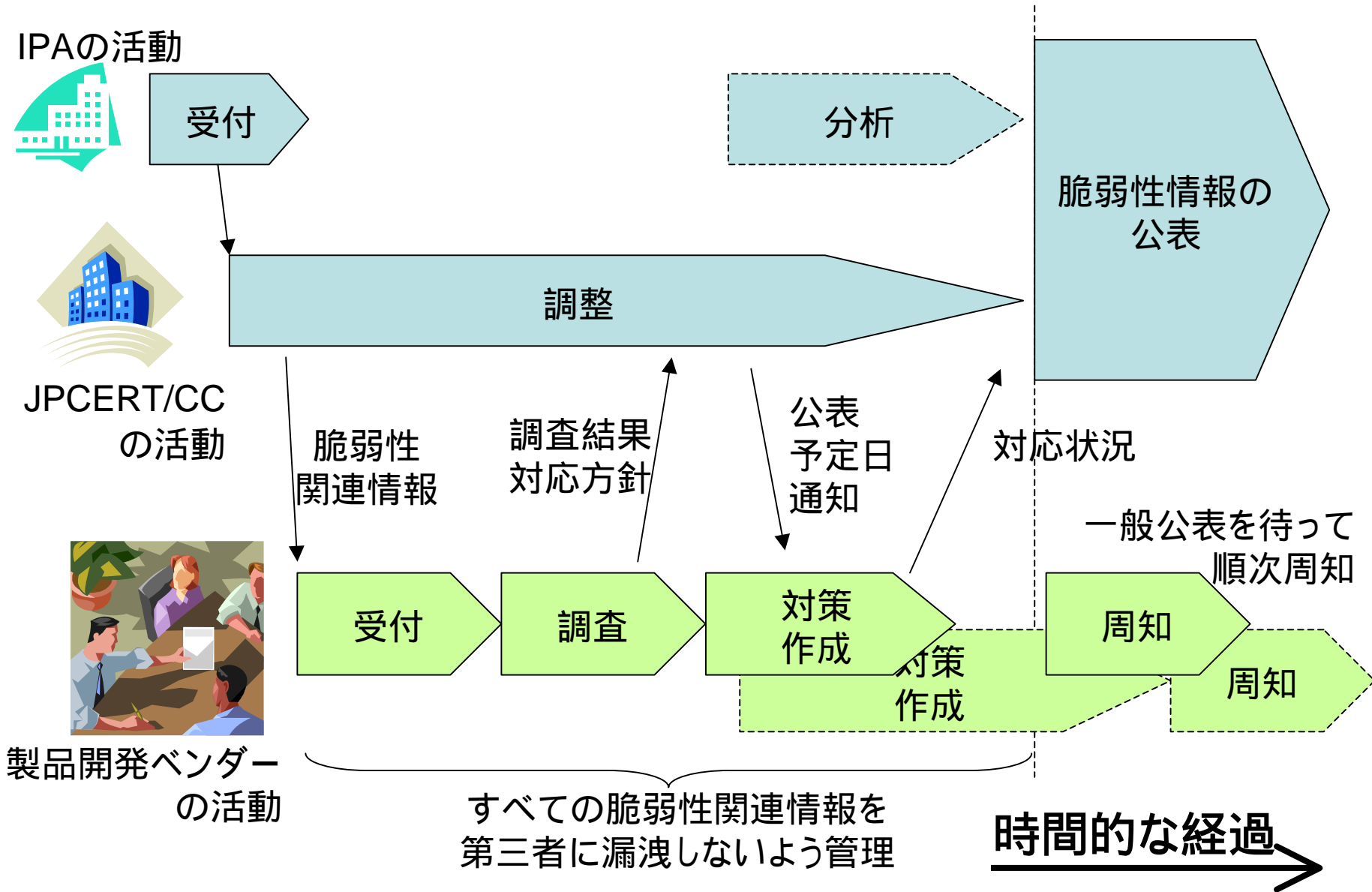
広報部門など

顧客窓口部門

製品開発部門

本ガイドラインの対象範囲

# 4. 国内の脆弱性関連情報取扱手順の全体概要 (時間軸にそって)



## 4. 国内の脆弱性関連情報取扱手順の全体概要(つづき)

### 製品開発ベンダーの責務とその二面性:

- 迅速で網羅度の高い調査と対策の提供  
調査範囲の最大化
- 脆弱性関連情報の漏洩や不適切利用の防止  
開示範囲の最小化

- 開示範囲は、社内でもCSIRT、経営トップ、関連する製品開発部門のみ; 社外は持出し禁止
- 顧客窓口部門や広報部門への開示は公表のタイミングで

- 脆弱性関連情報が悪意ある者に渡り、システム攻撃に利用されることを防ぐ
- 未公表情報を利用した営業や顧客誘導などの行為の禁止

## 5. 脆弱性関連情報取扱体制の立上げ

1. 経営責任をもった適任者の了解を取り付ける
2. 対象となる製品を確認する
3. ベンダーCSIRTを決めてJPCERT/CCに登録
  - ・ 脆弱性関連情報に関するJPCERT/CCとの窓口
  - ・ 1営業日以内にはメール応答を返せる体制が望ましい
  - ・ JPCERT/CCの製品開発者リスト登録規約の確認と同意
4. 製品開発部門内での対応ルール作り
  - ・ 責任者, 対応作業の優先度付け, 守秘
5. 顧客窓口部門の協力の取り付け
  - ・ 企業ウェブ・サイトへの掲載, 顧客への周知
6. 脆弱性関連情報が漏洩しない施策(体制・仕組み・ルール)

## 5. 脆弱性関連情報取扱体制の立上げ (つづき)

JPCERT/CCの「製品開発者リスト」への登録手順

以下のフォームをメールで送り仮登録:

<<http://www.jpccert.or.jp/form/poc.txt>>

JPCERT/CCが要求する以下の書類を提出:

1. 会社の登記簿謄本
2. 会社概要(会社の紹介、パンフレットなど)
3. 主要製品リスト
4. 窓口情報
5. 規約への同意書
6. 暗号化の公開鍵

JPCERT/CCでは面談審査後に本登録

審査時の確認事項: 会社概要, 製品情報, 社内体制等

## 6. 脆弱性関連情報取扱体制の整備

### (1) ベンダーCSIRTの役割

社外に対して:

全社を代表してJPCERT/CCから脆弱性関連情報を受取り、対応の完了までタイムリで一貫した対応を維持する  
JPCERT/CC経由の情報だけでなく、顧客相談窓口や営業部門に入る脆弱性関連情報も掌握するよう努める

社内に対して:

脆弱性対応における情報の分析と集約  
必要かつ最小限に脆弱性関連情報を社内展開  
セキュリティ面から製品開発部門を技術支援

## 6. 脆弱性関連情報取扱体制の整備 (つづき)

JPCERT/CCとの関係

・ JPCERT/CCへの登録

登録後も適宜情報のアップデートを行う

・ 脆弱性関連情報のやりとり

脆弱性関連情報の受付

該当製品の有無, 対応方針の連絡

公表日時の調整

公表情報の連絡

・ JPCERT/CCが開催する定例会への参加

## 6. 脆弱性関連情報取扱体制の整備 (つづき)

### 脆弱性対応における全社への指令塔

- 脆弱性関連情報の機密性管理の要(かなめ)
- 製品利用者の安全の観点に基づき総合的に判断し製品開発ベンダーとしての対応方針を打ち出す
  - 製品開発部門では脆弱性の影響の重大性を見落とすことがある
- 脆弱性対応に関する社内調整
  - 社内の全体スケジュールの管理および対策情報、公表情報の取りまとめ
  - 自社の利害を超えた他社との協調を製品開発部門に求めることもある

## 6. 脆弱性関連情報取扱体制の整備 (つづき)

### (2) 推進・管理組織

品質管理の枠組みを活用した脆弱性対応の推進と管理

ベンダーCSIRTが策定した対応方針に基づいた脆弱性対応の推進と管理

### (3) 製品開発部門の役割 (製品ないし製品ラインごと)

対象となる製品と責任者の確認

製品の脆弱性調査と対策の作成

### (4) その他の部門の役割

顧客への周知, 問合せ対応, 対策の提供など

## 7. 脆弱性関連情報取扱手順の整備

### (1) 脆弱性関連情報の受付

JPCERT/CCに脆弱性関連情報を受領した旨の確認回答を返す

概要情報だけを受け取った場合には、  
該当製品の有無を調べた上で  
必要に応じて詳細情報を請求する

## 7. 脆弱性関連情報取扱手順の整備 (つづき)

### (2-a) 調査 (製品を特定した脆弱性関連情報の場合)

#### 通知された脆弱性の再現性確認

- ・ 結果をJPCERT/CCに報告  
(JPCERT/CCでは報告をもとに公表時期を調整)

再現できない場合には、  
発見者に協力を求めるなどして発生条件を探る  
または、反証を添えた回答を返す

脆弱性の深刻度や影響範囲を評価する

## 7. 脆弱性関連情報取扱手順の整備 (つづき)

### (2-b) 調査 (技術を特定した脆弱性関連情報の場合)

関連製品(調査範囲)の特定

個々の調査対象製品の脆弱性の有無を調べる

- ・ 結果をJPCERT/CCに報告  
(JPCERT/CCでは各社からの報告をもとに公表時期を調整)

脆弱性の深刻度や影響範囲を評価する

## 7. 脆弱性関連情報取扱手順の整備 (つづき)

### (3) 対策の作成

(脆弱性を悪用した攻撃のリスクの回避または低減)

いずれかのタイプの対策を作成

- |                   |   |             |
|-------------------|---|-------------|
| 1. パッチを提供         | } | 修正による対策     |
| 2. 改版による是正        |   |             |
| 3. 設定のパラメタ変更による是正 | } | 回避による<br>対策 |
| 4. 制限事項として明示      |   |             |

対策の有効性を確認

対策に伴う副作用や互換性などの検証に努力

本対策の提供まで時間がかかる場合には  
暫定対策の提供を検討

## 7. 脆弱性関連情報取扱手順の整備 (つづき)

### (4) 対策の公表と周知

JPCERT/CCに「対応状況」を送付

- ・ 「対応状況」は製品開発ベンダーの公式見解としてJVN (<http://jvn.jp/>)上で公表される
- ・ 送付しない場合には  
対応状況「不明」として公表される

JPCERT/CCからの公表後に  
製品開発ベンダーからも速やかに公表

- ・ 正確で分かりやすい情報
- ・ 製品の市場に適した通知方法の選択  
個別通知, ウェブによる公表, など

## 8. まとめと課題

- 脆弱性関連情報に対する本ガイドラインで述べたような適切な対応とそのための体制と手順の整備は製品開発ベンダーの責務である
- 本ガイドラインの範囲外だが、脆弱性を作り込まない開発手法の研究や教育、脆弱性対策の展開のための体制と手順の準備も重要である
- 出荷後の製品に関する脆弱性の是正を推進するため、コスト負担を含めた顧客の理解を得るための継続的な努力を続け、社会的なコンセンサスの形成を目指す必要がある
- SI事業者や受注開発ソフトなどが関連した脆弱性への対応のための枠組みは今後の課題である

# 補 用語集

脆弱性	ソフトウェア等において、コンピュータ・ウィルス、コンピュータ不正アクセス等の攻撃により、その機能や性能を損なう原因となり得る安全性上の問題箇所。
脆弱性情報	脆弱性の性質および特徴を示す情報
対応状況	JPCERT/CCから脆弱性関連情報の通知を受けた製品開発ベンダーが報告する対策方法、取り組みの状況などを含む情報。製品開発ベンダーの公式見解としてJVN (JP Vendor Status Notes)上で公表される。
製品開発ベンダー	ソフトウェア製品を開発した企業（経済産業省告示などでの「製品開発者」に相当）。海外で開発された製品の場合には国内で主たる販売権を有する会社。
IPA	Information-technology Promotion Agency, Japan 独立行政法人 情報処理推進機構 経済産業省告示において受付機関に指定されている < <a href="http://www.ipa.go.jp/">http://www.ipa.go.jp/</a> >
JPCERT/CC	Japan Computer Emergency Response Team Coordination Center 有限責任中間法人JPCERTコーディネーションセンター 経済産業省告示において調整機関に指定されている。 < <a href="http://www.jpccert.or.jp/">http://www.jpccert.or.jp/</a> >