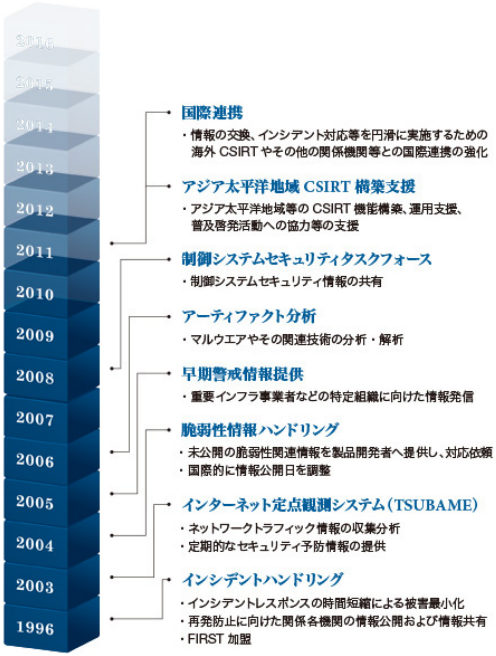
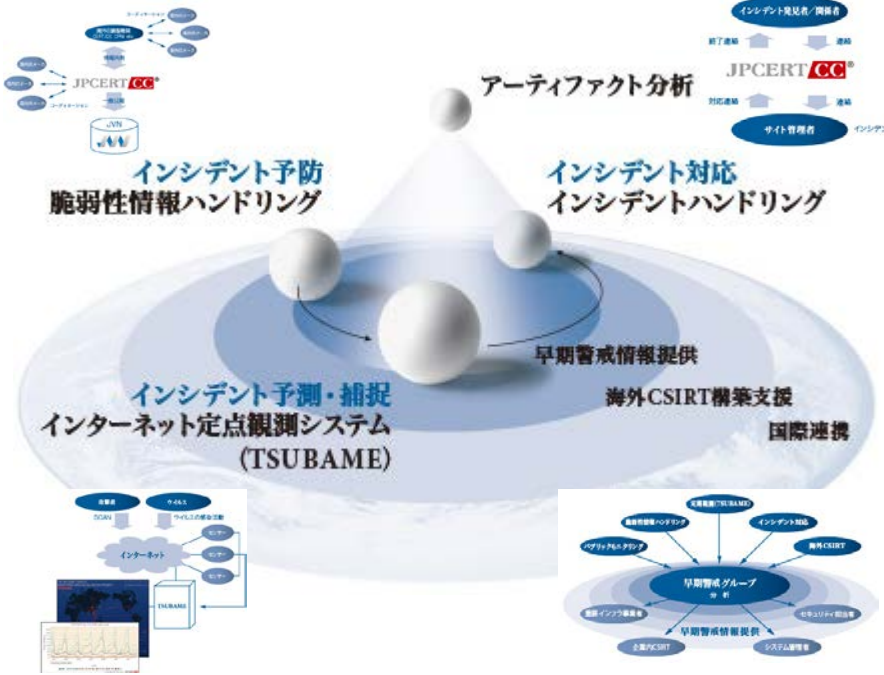
# 脆弱性届出制度における調整活動

JPCERTコーディネーションセンター
脆弱性コーディネーショングループ
リーダー
高橋 紀子

# JPCERT/CCの活動

- JPCERT/CCのさまざまな活動は、予防から事後対応に至る過程で必要となる具体的な対応に直結。先進の分析と培われたコーディネーション活動で、企業や組織のサイバーセキュリティ対策活動を支えます。



# 脆弱性コーディネーショングループの活動

- **インシデントの発生(ゼロデイ攻撃)や拡散を防止するための活動(未然に防止)**
  - **①脆弱性ハンドリング**
    - 脆弱性情報の適切な流通を図るための関係者間調整
    - 脆弱性情報の公表
  - **②セキュアコーディング**
    - 脆弱性の低減方策の調査研究・開発、普及啓発
  - **③潜在する脆弱性の脅威に関する調査・研究**

- **標準化動向調査**
  - 脆弱性の開示 (ISO/IEC 29147)、脆弱性取扱い(ISO/IEC 30111)
  - インシデント管理 (ISO/IEC 29147)

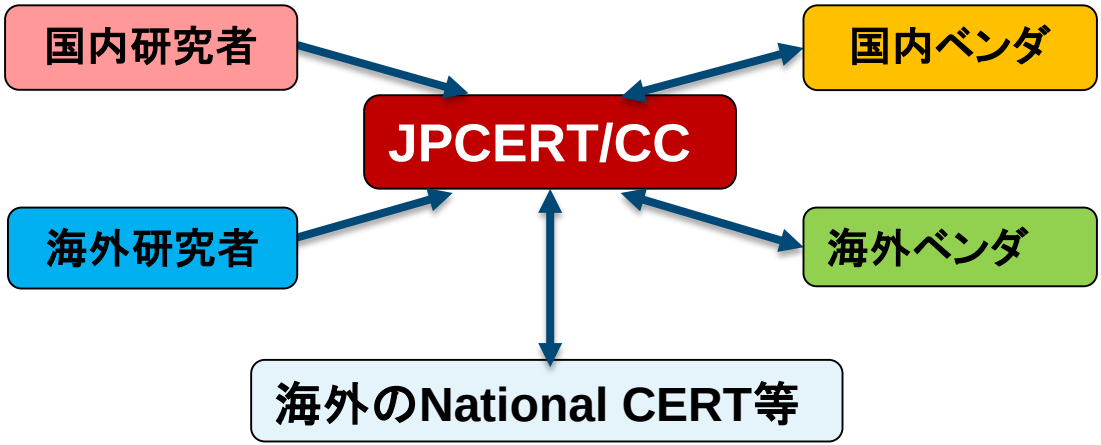
# ①脆弱性ハンドリング、具体的には…

- **IPAとの調整(国際展開案件の場合は海外CERT)**
  - 製品開発者からの報告内容共有、IPAからは発見者からの報告内容共有、JVNアドバイザリ内容、JVN公表日時など
- **製品開発者(ベンダ)との調整**
  - 届出情報展開(海外ベンダの場合は翻訳)、検証結果報告、ベンダ見解や対応方針(異議の際は関係者間の協議・交渉等)、JVNアドバイザリ内容、JVN公表日時、ベンダサイトでの公表日時
- **脆弱性発見者(届出者)との調整**
  - JPCERT/CCに直接届出られた場合は、あらゆる調整を行う
- **JVN公表**
  - JVN日本語版・英語版の作成、公表
- **CVE採番とCVE Description作成・発行**
  - 英文にて所定のルールに従い記載し発行

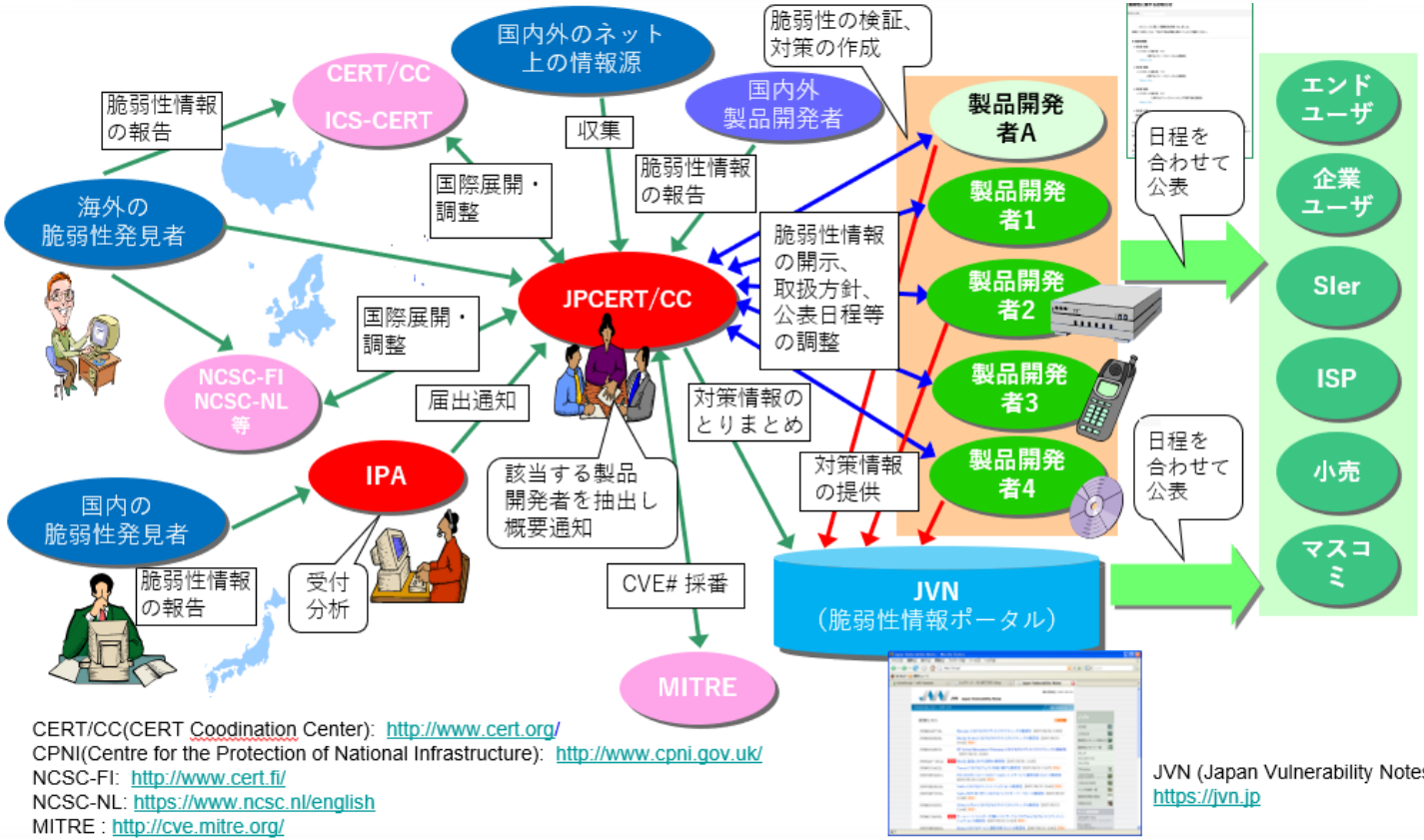
# 役割

- **JPCERT/CC 脆弱性コーディネーショングループ**
  — 2004年から活動

- **国内外の、主に製品開発者(ベンダ)と脆弱性に関わる調整を行う窓口としての機能を担う**



# JPCERT/CCの脆弱性ハンドリング全体像

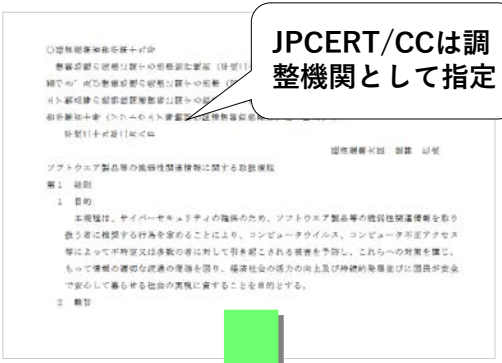



CERT/CC(CERT Coodination Center): http://www.cert.org/
CPNI(Centre for the Protection of National Infrastructure): http://www.cpni.gov.uk/
NCSC-FI: http://www.cert.fi/
NCSC-NL: https://www.ncsc.nl/english
MITRE : http://cve.mitre.org/

JVN (Japan Vulnerability Notes)
https://jvn.jp

# 国内における脆弱性ハンドリング全体像

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(平成29年経済産業省告示第19号)



JPCERT/CCは調整機関として指定

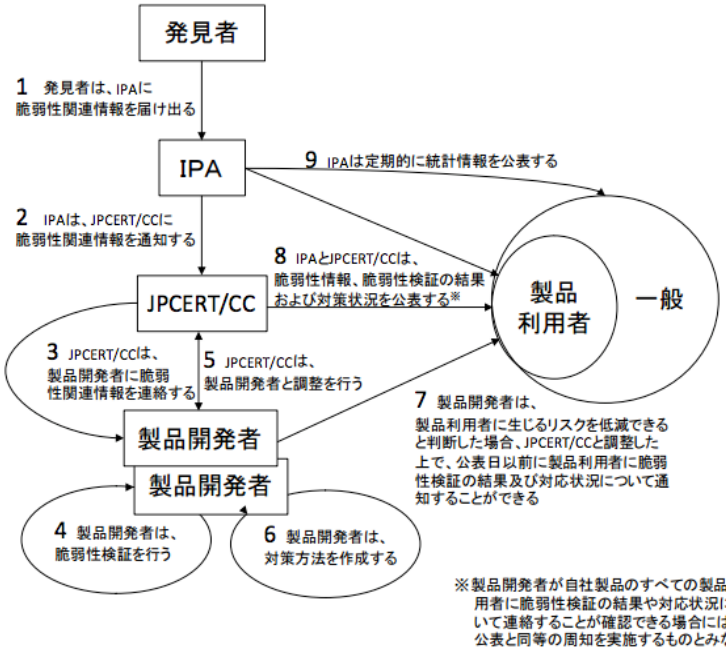


Ⅳ. ソフトウエア製品に係る脆弱性関連情報取扱

※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より抜粋

1．概要

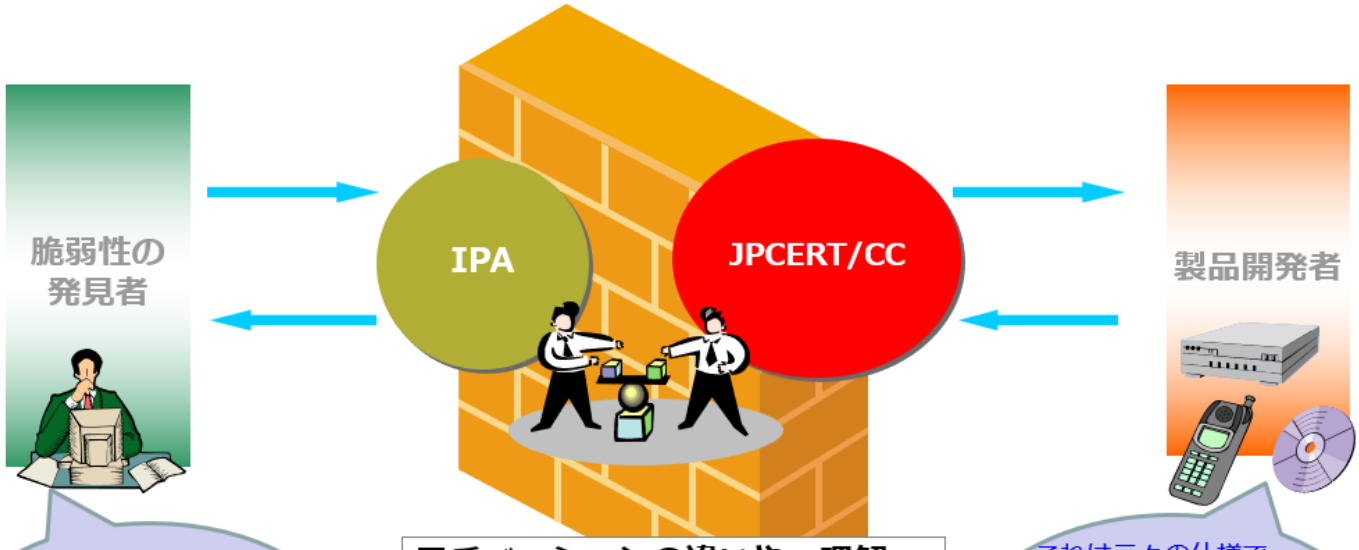
ソフトウエア製品に係る脆弱性関連情報取扱の概要は、図１の通りです。




※製品開発者が自社製品のすべての製品利用者に脆弱性検証の結果や対応状況について連絡することが確認できる場合には、公表と同等の周知を実施するものとみなす

図１　ソフトウエア製品に係る脆弱性関連情報取扱の概要

# 届出制度における発見者とベンダ間の調整



# 日本の届出制度でのメリット：発見者側

- **製品開発者(ベンダ)と直接やりとりをしなくてよい**
  - 匿名での届出も可能
  - 海外ベンダの場合、JPCERT/CCが届出を翻訳して送付
  - ベンダに連絡がつくまで自ら連絡先を探さずにすむ
  - 脆弱性発見に注力ができる。ベンダとの交渉・調整はすべてお任せ。

- **JVNに自分の名前(謝辞)が載る**

- **CNAであるJPCERT/CCにより、各脆弱性に対しCVEが採番・登録される**

**CNA(CVE Numbering Authorities)**
https://cve.mitre.org/cve/cna.html

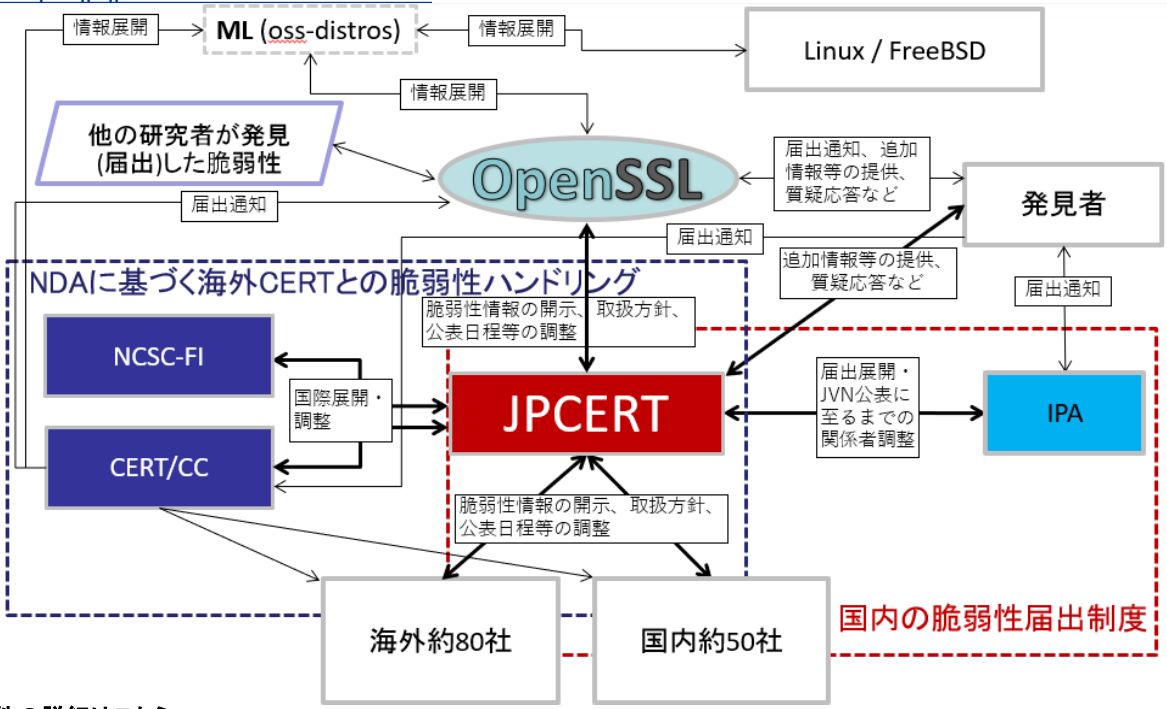
*CVE Numbering Authorities (CNAs) are organizations from around the world that are authorized to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed-upon scope, for inclusion in first-time public announcements of new vulnerabilities. These CVE IDs are provided to researchers, vulnerability disclosers, and information technology vendors.*

# 日本の届出制度でのメリット：ベンダ側

- **製品に関係する脆弱性情報を早期に入手し、計画的に対応できる**
  - 他社製品(サードパーティ製ライブラリ等)の脆弱性情報も、条件があえば必要に応じて入手できる
- **脆弱性の公表と同時に対策情報を公開し、ユーザへの影響を低減できる**
- **中立な第三者機関(JPERT/CC)がクッションになる**
  - 情報の適切なフィルタリング、検証等
  - 海外の発見者やCERT等と直接英語で交渉・調整しなくてよい
  - 適切な脆弱性情報の管理と提供（OEM元や部品ベンダ等）
- **脆弱性およびその対策の情報を告知する媒体として、JVNを利用でき、CVEも採番・登録される**
  - JVN掲載により各種メディアを通じてユーザに広く周知が期待できる

# 国際調整案件となったハンドリング事例

**JVN#61247051**
**OpenSSL における Change Cipher Spec メッセージの処理に脆弱性**
https://jvn.jp/jp/JVN61247051/index.html




**本件の詳細はこちら**
**Lessons (to be) Learned from Handling OpenSSL Vulnerabilities**
https://www.slideshare.net/jpcert_securecoding/lessons-to-be-learned-from-handling-openssl-vulnerabilities

# 発見者・研究者の皆さまに知っておいてほしいこと

- **脆弱性を発見したら、届出窓口にご連絡を！**
  - ベンダとの調整を行っているCERT組織は世界でも限られています
    - JPCERT/CC, CERT/CC, ICS-CERT, NCSC-FI, NCSC-NL
    - JPCERT/CCは、各国CERTとNDAを締結し国際連携をしています
- **JPCERT/CCは、CVE Numbering Authorities (CNA) です**
  - 世界でも数少ないRoot CNA。MITREより事前にCVEブロックを取得しており、JVNで脆弱性情報公表する際、各脆弱性にCVEを採番し、CVEデータベースにDescriptionを投稿しています
- **海外のベンダとも、頻繁にやり取りがあります**
  - 複数社より自社製品の届出や事前情報提供を受け取っています
  - 例：Adobe, Apple, Google, ASF, ISC, Intel, OpenSSL, etc…
- **JPCERT/CCは、Responsible Disclosureの精神に則り調整します**
  - 原則、Coordinated Disclosure(公表前調整)をおこないます
  - ただし、ゼロデイ時はこの限りではなく、緊急注意喚起発行もします

# 届出制度に報告する際、ご協力いただきたい点

- **学会・カンファレンス等での発表を控えている案件の場合、その名称・発表タイトルと発表日**
  - 脆弱性対策を進めるベンダにとっては、とても重要
  - 受付機関・調整機関にとっても、発見者による発表日(同日または翌日)が脆弱性情報公表日となるため、必要な情報

- **影響範囲や懸念点等**
  - プラグイン、ライブラリ、ウェブアプリケーション等である場合、それを取込んだ製品が多数存在していると、マルチ案件(国際展開・調整に転じる)となり、調整も大掛かりに。影響範囲が多岐であったり、その懸念がある場合は、届出に記載をお願いします。

- **海外製品の場合、届出・検証結果や提示可能なペーパーは、可能であれば英文でご提示いただけると助かります**
  - JPCERT/CCで届出の翻訳はしていますが、誤訳防止、かつ届出時に英文であれば早期展開も可能となります。

脆弱性情報の届出等詳細については、IPA様からの公開資料がとても参考になります！
**脆弱性届出制度に関する説明会 資料(PDF2.06MB)**
https://www.ipa.go.jp/files/000063028.pdf

# 脆弱性ハンドリングに関するお問い合わせ

**脆弱性情報・ハンドリングに関して**

- Email：vultures@jpcert.or.jp
- https://www.jpcert.or.jp/vh/top.html

**製品開発者登録に関して**

- Email：poc-vh@jpcert.or.jp
- https://www.jpcert.or.jp/vh/register.html

**JPCERTコーディネーションセンター**

- Email：pr@jpcert.or.jp
- https://www.jpcert.or.jp/

# ご清聴ありがとうございました