JPCERT CC®

脆弱性情報ハンドリング概要

一般社団法人 JPCERT コーディネーションセンター
情報流通対策グループ　脆弱性情報ハンドリングチーム リーダ
高橋 紀子

アジェンダ

- 脆弱性とは？
- 脆弱性情報ハンドリングとは？
- 日本における脆弱性情報ハンドリング体制について
- 脆弱性情報ハンドリングの流れ
- 国際的な活動について
- 脆弱性対策情報の公表
- 脆弱性情報ハンドリング全体図
- FAQ

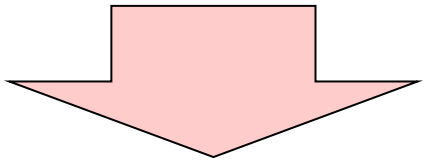
脆弱性とは？

- 経済産業省告示第２３５号：用語の定義より抜粋

  「ソフトウエア等において、コンピュータウイルス、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。ウェブアプリケーションにあっては、ウェブサイト運営者がアクセス制御機能により保護すべき情報等に誰もがアクセスできるような、安全性が欠如している状態を含む」
- 平たく言えば、ソフトウエアの不具合（バグ）の一種。だが、本来の用途とは全く異なった製品の挙動を、製品利用者ではない第三者が利用出来てしまう問題個所を特に指して言う。つまり、**脆弱性が発見された製品では、正規の製品利用者が、第三者の脆弱性利用（攻撃）による被害（データの搾取や改ざん、情報漏えい、システムの遠隔操作など）リスクを、「知らないうちに」「自動的に」負わされてしまう状況が発生する**
- 脆弱性には、影響範囲が特定の製品開発者にのみ関わるものと、複数の製品開発者にまたがるものの２種類がある

脆弱性情報ハンドリングとは？

新たに発見された脆弱性は、必要な情報が整えられたうえで、適切な製品開発者の担当窓口にまで届けられなければ、修正や回避策を提供出来る段階にまで至れない。この状態のまま脆弱性関連情報が表沙汰になってしまえば、**製品利用者が、無防備のまま攻撃の脅威（zero-day attack）に晒される危険な状況が発生してしまう。**



扱いが難しい脆弱性関連情報の届出先を広く示して発見者に届出を促し、問題把握に必要な情報を整えて製品開発者の担当窓口に流通。zero-dayにならぬよう情報を慎重に扱いながら、準備が完了した時点で脆弱性情報と対策情報を周知。その適用を促す事によって、製品利用者が受けうる被害を最小限に食い止める為の活動。

・・・それが脆弱性情報ハンドリング

日本における脆弱性情報ハンドリング体制について

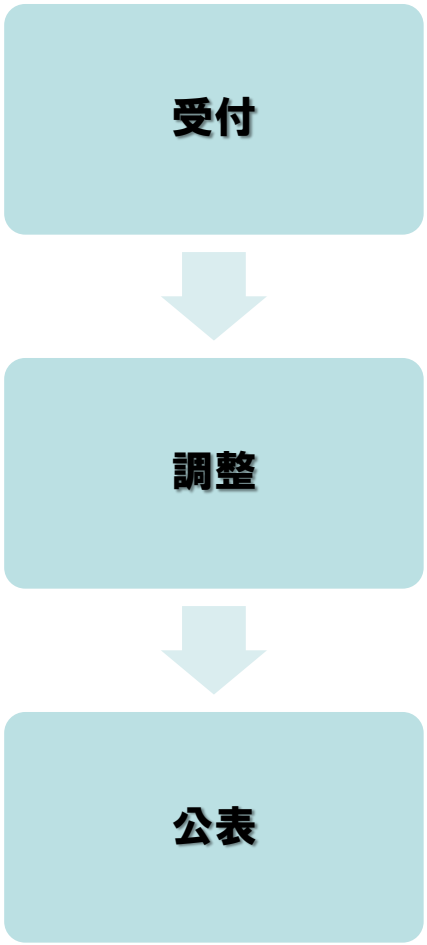
JPCERT CC®

- 経済産業省告示第235号「ソフトウェア等脆弱性関連情報取扱基準」（2004年7月7日制定）に基づき、脆弱性関連情報を届け出るための受付機関として独立行政法人情報処理推進機構（IPA）、製品開発者と必要な調整を行う調整機関として有限責任中間法人（現：一般社団法人）JPCERTコーディネーションセンターが指定された。
- 同告示施行（2004年7月8日）に合わせて、IPA、JPCERT/CC、JEITA、JISA、JPSA、JNSAでは、本枠組みに参画する関係者及び関係業界としての指針「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」を連名で発表。日本における脆弱性情報ハンドリングは、このガイドラインに沿って正式に運用が開始され、現在に至っている。
- 運用上の課題は「情報システム等の脆弱性情報の取扱いに関する研究会」への報告により識者によって協議され、その結果がガイドラインの反映されている。

※各団体の正式名称は、以下のとおり

JEITA（社団法人電子情報技術産業協会）、JISA（社団法人情報サービス協会）、JPSA（社団法人日本パーソナルコンピュータソフトウエア協会）、JNSA（特定非営利活動法人日本ネットワークセキュリティ協会）

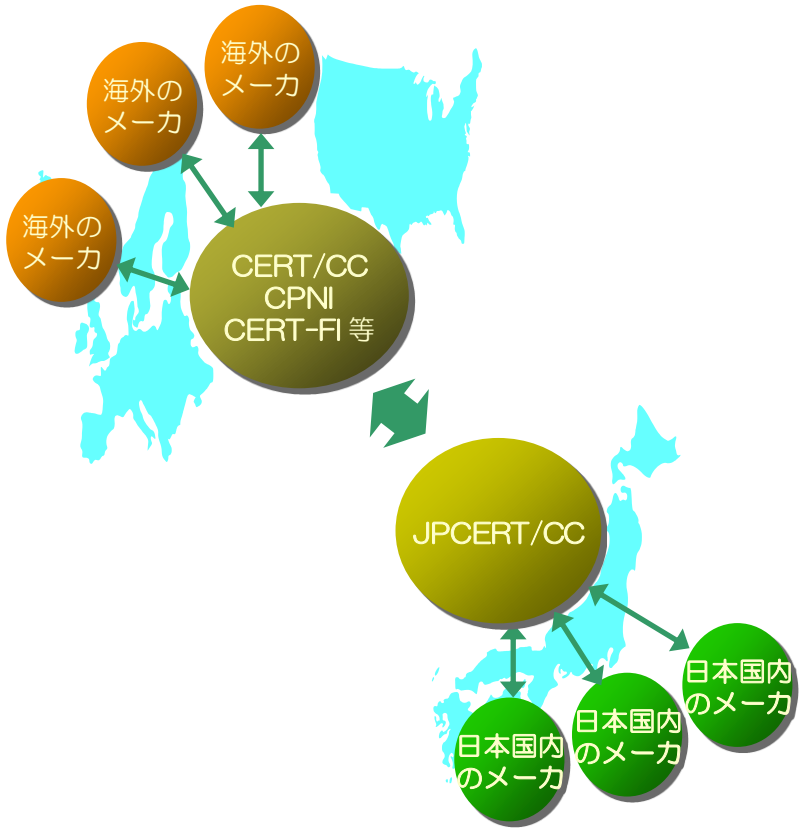
脆弱性情報ハンドリングの流れ



- 脆弱性情報ハンドリングプロセスは大きく分けて3段階
- 第1段階：脆弱性関連情報の届出の受付
  - 発見者からの届出を受付け、内容を確認して過不足があれば補って整え、真に取り扱うべき届出内容か否かを見極める
  - 受付機関であるIPAにより遂行されている
- 第2段階：製品開発者との調整
  - 製品開発者に、脆弱性の対策が提供出来る組織・体制の設置を促し、情報セキュリティ早期警戒パートナーシップに基づいた連携関係を構築する（2012/9/30 現在、登録製品開発者数：449社）
  - 脆弱性の影響範囲を見極め、然るべき製品開発者に情報を提供し、得られた対策の製品利用者への周知計画を設定する
  - 調整機関であるJPCERT/CCによって遂行されている
- 第3段階：脆弱性情報の公表
  - 製品開発者によって提供された対策を、不特定多数の製品利用者に周知する事を目的として、脆弱性情報ポータルサイトのJVN（Japan Vulnerability Notes）において公表を行う
  - JVNは、IPAとJPCERT/CCによって共同運営されている

国際的な活動について

- 調整機関であるJPCERT/CCは、届出られた脆弱性情報について、国内だけでなく、海外の製品についても直接調整を行なっている。
- 取り扱う案件の影響範囲によっては、連携関係にある海外の調整機関、 CERT/CC(US)、CERT-Fi(Finland)、CPNI(UK)等と相互に脆弱性関連情報を提供しあい、それぞれの担当エリアでの調整を委任している
- IPA とJPCERT/CC が運営するJVN は、脆弱性を特定するための世界共通識別子である CVE 互換認定をMITRE 社より受けており、CVE 番号を併記して公表される JVN の脆弱性情報は、海外からの利用でも識別が容易となっている。また、JPCERT/CC はCVE 採番機関(CNA)としても認定を受けており、独自に採番を行うことが出来る



CVE: Common Vulnerabilities and Exposures
CNA: CVE Numbering Authorities

脆弱性対策情報の公表

- 脆弱性情報ハンドリングにより得られた対策情報は、不特定多数の製品利用者への周知を目的として、脆弱性対策情報ポータルサイト「JVN」(Japan Vulnerability Notes)で、脆弱性情報とともに公表している
- 日本発の脆弱性情報は、公表日から2日以内に英語化してJVN英語版にも公表し、英語圏の製品利用者に対しても注意喚起を行っている
- 活動成果は、受付機関であるIPAと共に四半期に一度まとめられ、「ソフトウェア等の脆弱性関連情報に関する届出状況」としてプレスリリース公表されている

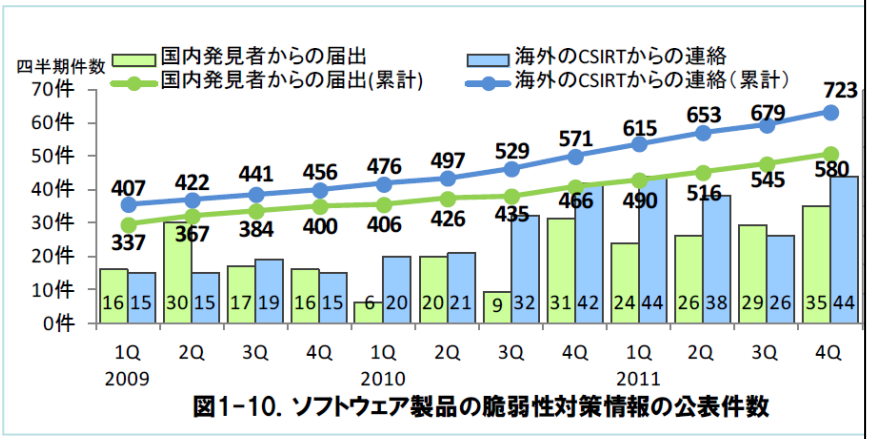


図1-10. ソフトウェア製品の脆弱性対策情報の公表件数


IPA Information-technology Promotion Agency, Japan
JPCERT CC®
プレスリリース
2012年10月22日
独立行政法人情報処理推進機構
一般社団法人 JPCERTコーディネーションセンター
ソフトウェア等の脆弱性関連情報に関する届出状況 [2012年第3四半期(7月～9月)]
～スマホ関連製品の脆弱性対策情報の公表が急増～

【参考】

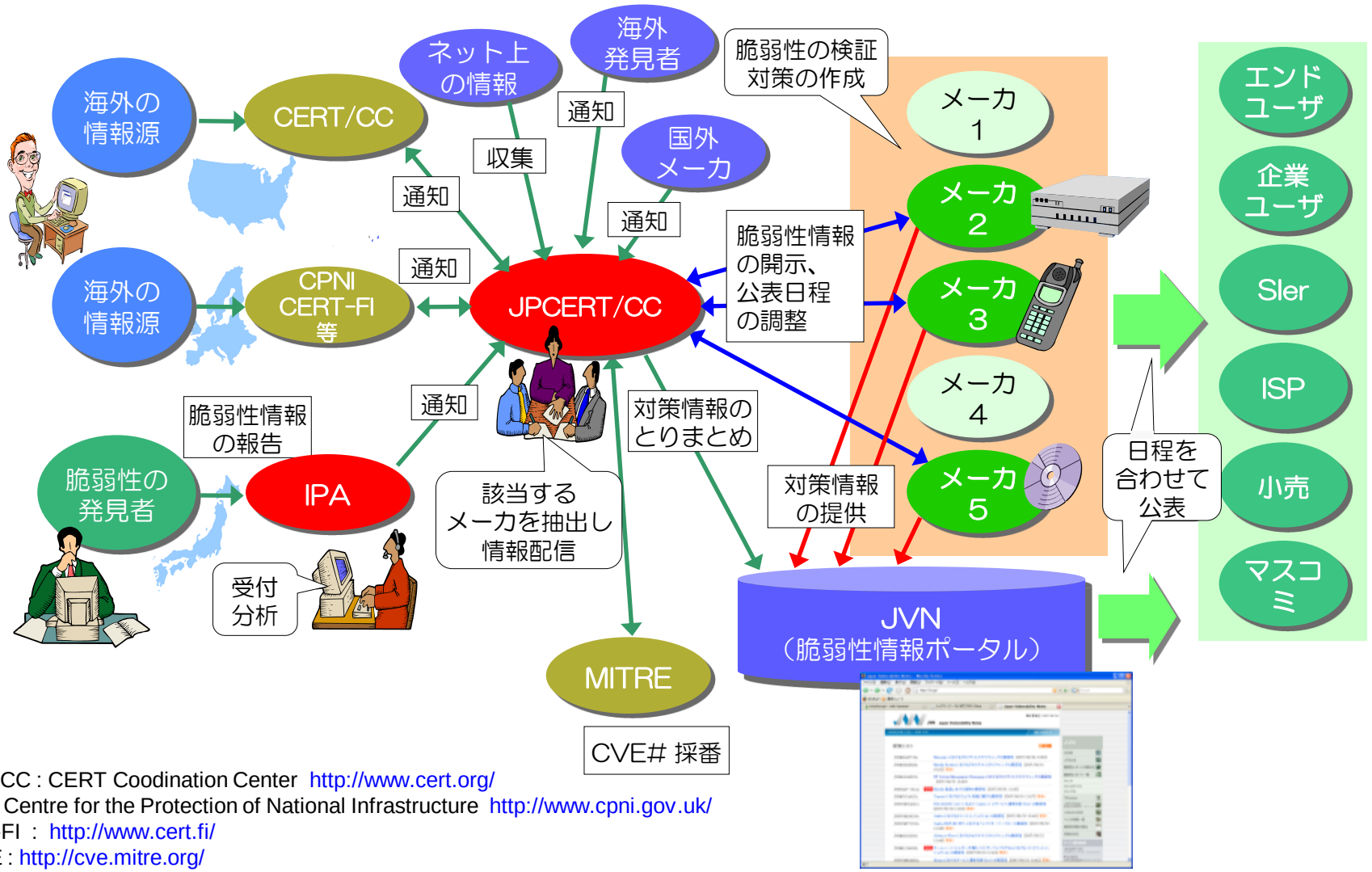
2012/9/30時点での
公表件数累計

IPA案件： 667件

海外CSIRT案件： 830件

合計：1497件

脆弱性情報ハンドリング全体図



CERT/CC : CERT Coodination Center http://www.cert.org/
CPNI : Centre for the Protection of National Infrastructure http://www.cpni.gov.uk/
CERT-FI : http://www.cert.fi/
MITRE : http://cve.mitre.org/

FAQ

Q: 調整開始から45日経過すると、製品開発者の対策提供を待たずに、脆弱性情報が公表されると聞きましたが、本当ですか？

A: 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では、「公表日は、JPCERT/CC およびIPA が脆弱性関連情報の取り扱いを開始した日時から起算して、45日後を目安とします」と書かれていますが、45日はあくまで目安です。製品利用者への被害を回避すべく、良心的に対応している製品開発者の都合を、全く無視するような公表日の設定はしておりません。

FAQ

Q: なぜ、脆弱性情報を JVN（Web）公表するのですか？

A: 利用者が不特定多数の製品の場合、脆弱性情報と対策情報を届けられる手段が他に無いためです。直接メッセージを届けられない多くの製品利用者に、脆弱性の存在と対策を知らせる事を目的として、JVN 公表しています。

- **本件に関するお問合せ**
  JPCERTコーディネーションセンター
  情報流通対策グループ脆弱性情報ハンドリングチーム宛
  - **Email：office@jpcert.or.jp**
- **脆弱性関連情報の届出**
  - **Web: http://www.ipa.go.jp/security/vuln/report/**
- **脆弱性関連情報流通（自社製品に関する脆弱性情報についての連絡を受け取る）**
  製品開発者リストへの登録
  - **Web: https://www.jpcert.or.jp/vh/regist.html**
- **脆弱性対策情報ポータルサイトJVN（Japan Vulnerability Notes）**
  - **Web: https://jvn.jp/**

ご清聴ありがとうございました。