資料5

IPA Better Life with IT

産業サイバーセキュリティ研究会 WG1　ソフトウェアタスクフォース

脆弱性届出制度
～ 情報セキュリティ早期警戒パートナーシップの取組み ～

2019年11月6日

独立行政法人情報処理推進機構（IPA）
セキュリティセンター セキュリティ対策推進部
脆弱性対策グループリーダー　渡辺 貴仁

情報セキュリティ早期警戒パートナーシップとは

- ***情報セキュリティ早期警戒パートナーシップ***は、ソフトウェア製品及びウェブサイトに関する脆弱性関連情報の円滑な流通、および対策の普及を図るため、公的ルールに基づく官民の連携体制として、2004年7月に整備された脆弱性関連情報の届出制度。
  - 告示

    平成29年経済産業省告示第19号

    http://www.meti.go.jp/policy/netsecurity/vul_notification.pdf
  - ガイドライン

    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

    https://www.ipa.go.jp/files/000059694.pdf
- 脆弱性関連情報は関係者の協力をもと、適切に流通・対応・公表※されている。

  ※公表はソフトウェア製品の脆弱性の場合

本制度で扱う脆弱性

- 脆弱性の定義
  - ソフトウエア製品やウェブアプリケーション等における**セキュリティ上の問題箇所**
  - コンピュータ不正アクセスやコンピュータウイルス等により、この**問題の箇所が攻撃**されることで、そのソフトウエア製品やウェブアプリケーションの本来の**機能や性能を損なう原因**となり得るもの
  - また本制度での脆弱性は、個人情報等が適切なアクセス制御の下に管理されていないなど、ウェブサイト**運営者の不適切な運用**により、ウェブアプリケーションのセキュリティが維持できなくなっている状態も含む

本制度での対象範囲

告示：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

3. 定義

(1) ソフトウエア製品

ソフトウエア又はそれを組み込んだハードウエアであって、**汎用性**を有する製品をいう。

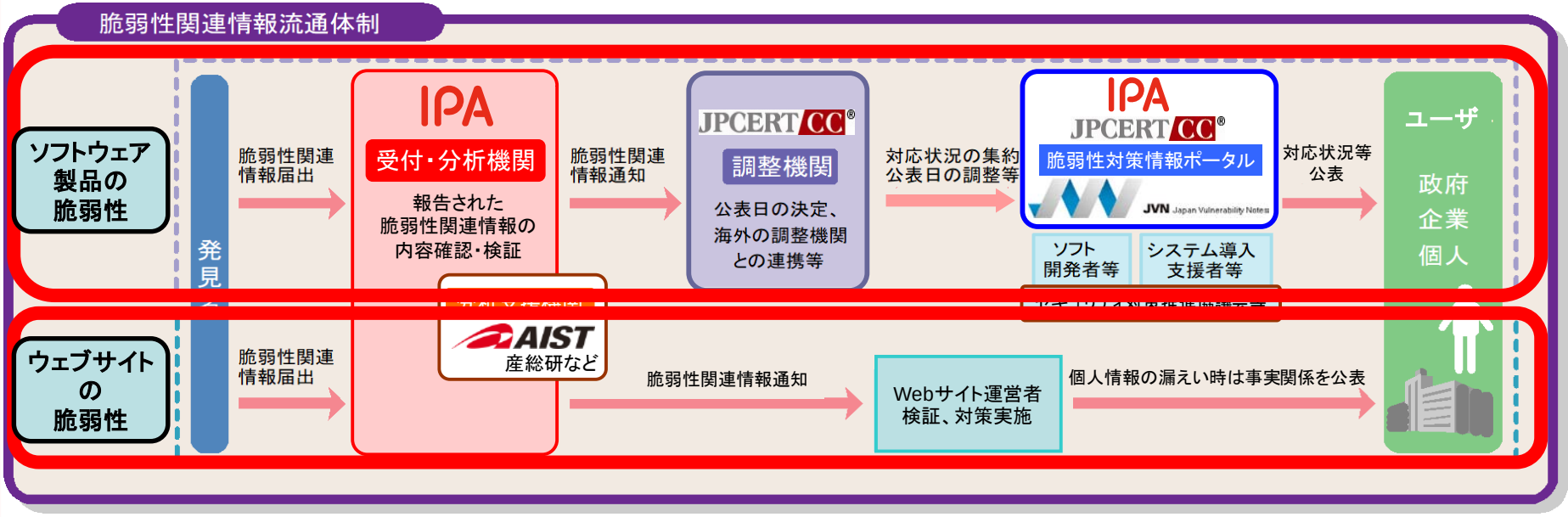
(2) ウェブアプリケーション

インターネット上のウェブサイトで稼働する固有のシステムをいう。

4. 本基準の適用範囲

本規程は、**日本国内で利用されているソフトウエア製品**又は主に**日本国内からのアクセスが想定されているウェブサイト**で稼働するウェブアプリケーションに係る脆弱性であって、 その脆弱性に起因する影響が**不特定多数の者に及ぶおそれのあるもの**に適用する。

脆弱性関連情報流通体制



※JPCERT/CC：一般社団法人 JPCERT コーディネーションセンター、産総研：国立研究開発法人産業技術総合研究所

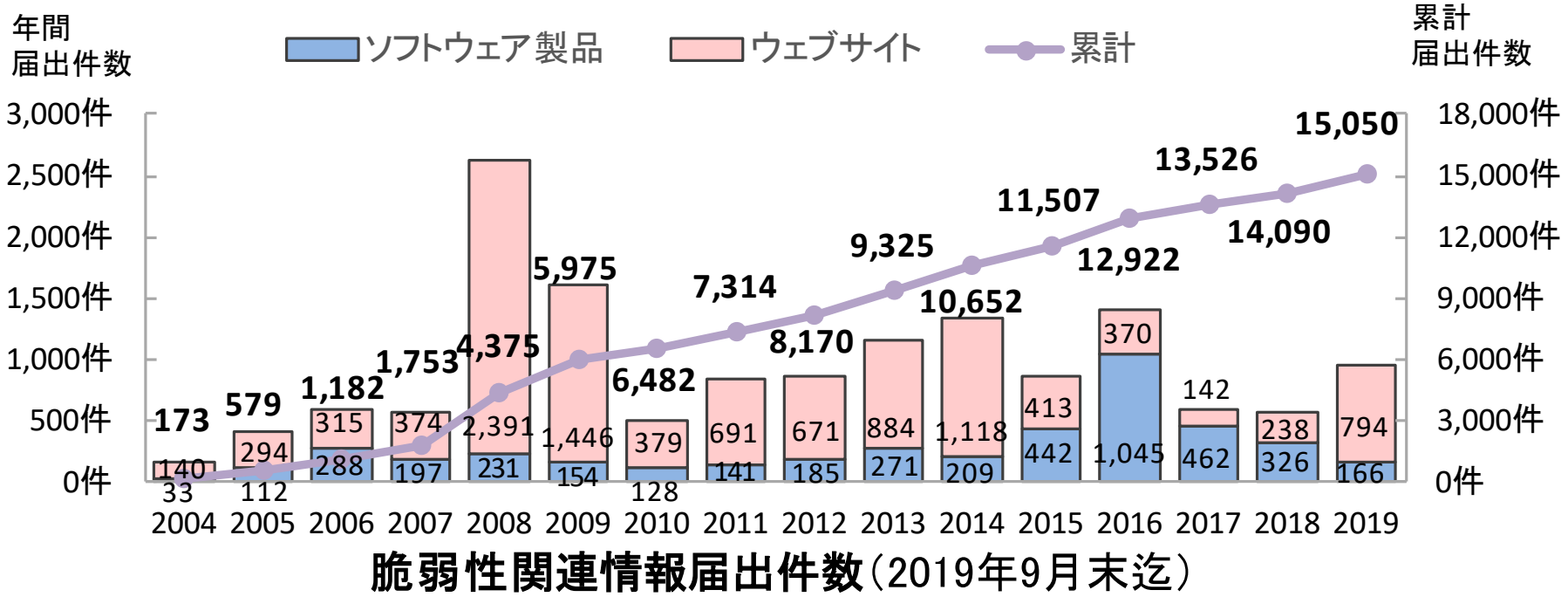
- 発見者
- IPA（受付・分析機関）
- AIST…（分析支援機関）
- JPCERT/CC（調整機関）
- ウェブサイト運営者
- ソフトウェア製品開発者
- JVN（Japan Vulnerability Notes）
- ユーザ（利用者）

JVN（Japan Vulnerability Notes）
脆弱性対策情報ポータルサイト https://jvn.jp/jp/

脆弱性届出の状況

- 届出受付開始から2019年9月末迄の累計件数
  - ソフトウェア製品 **4,390**件、ウェブサイト **10,660**件、合計 **15,050**件

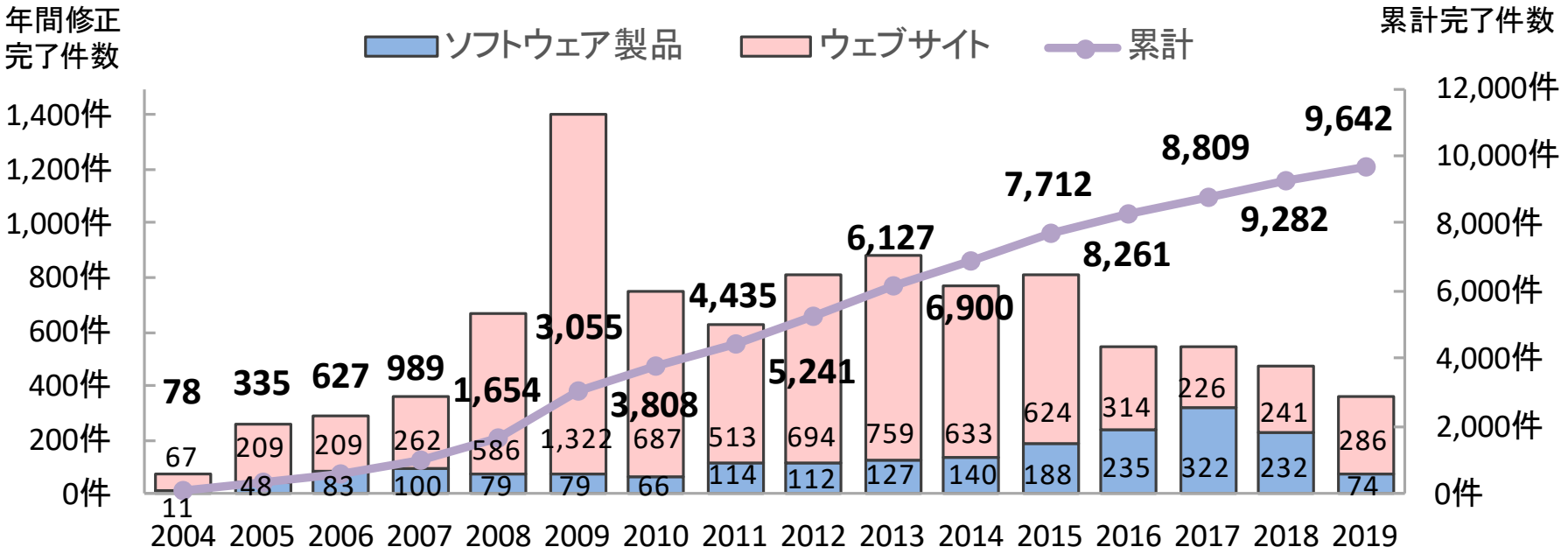
→ 1就労日あたり **4.06** 件



脆弱性関連情報届出件数（2019年9月末迄）

脆弱性の修正完了状況

- 届出受付開始から2019年9月末迄の累計件数
  - ソフトウェア製品 **2,010**件、ウェブサイト **7,632**件、合計 **9,642**件

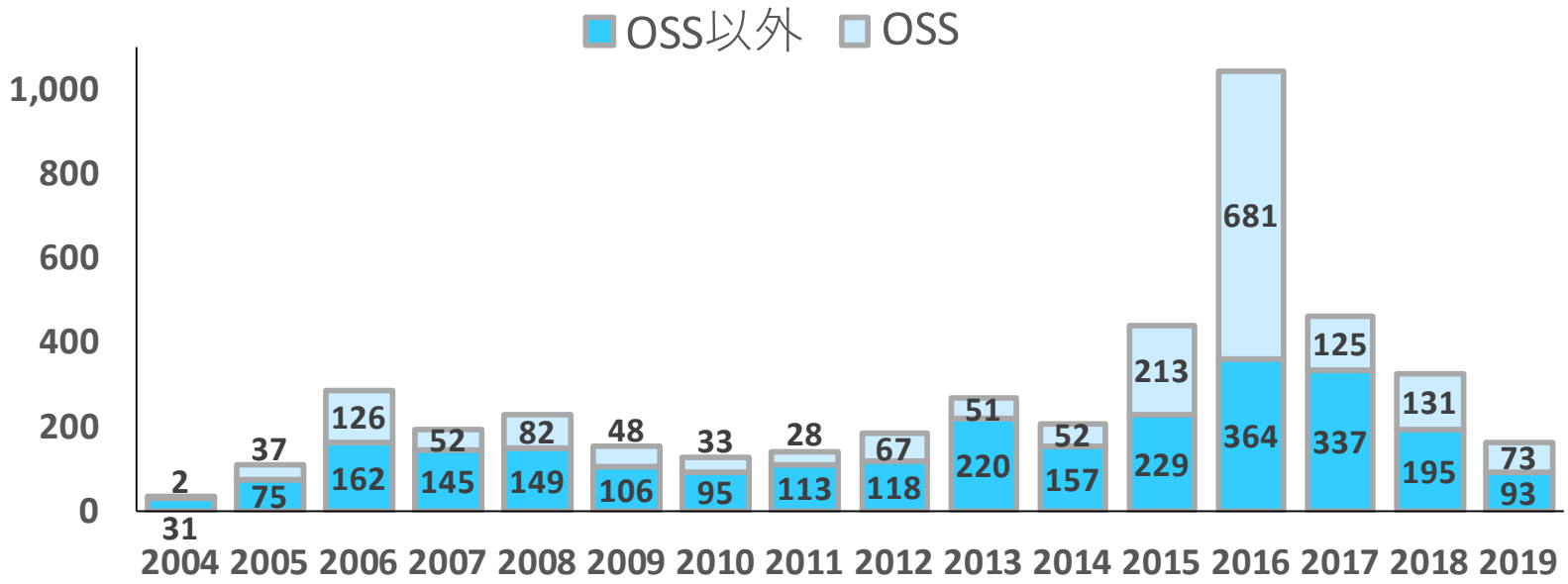


脆弱性関連情報の修正完了件数（2019年9月末迄）

OSSソフトウェア製品の届出状況

- OSS製品 **1,801**件、OSS以外製品 **2,589**件、合計 **4,390**件

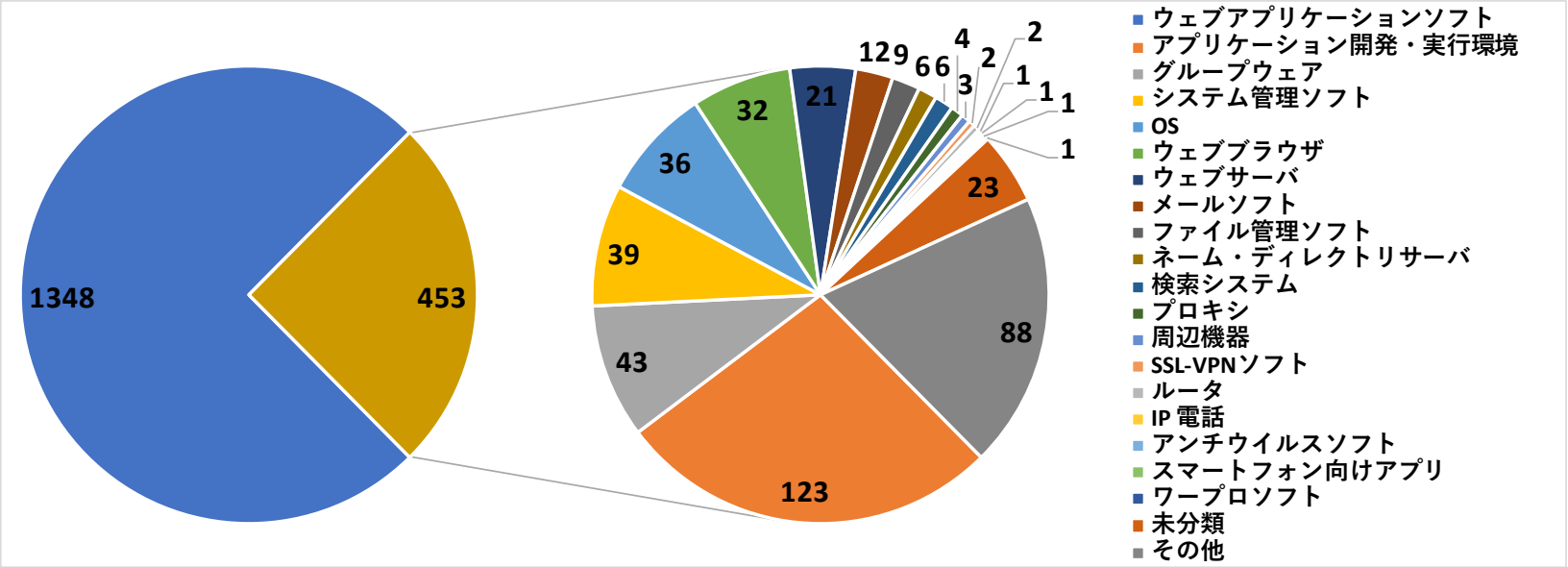
→ 4割強がOSS製品の届出



OSS製品 と OSS以外製品の届出件数（届出受付開始から2019年9月末迄）

OSS製品届出の製品種類内訳

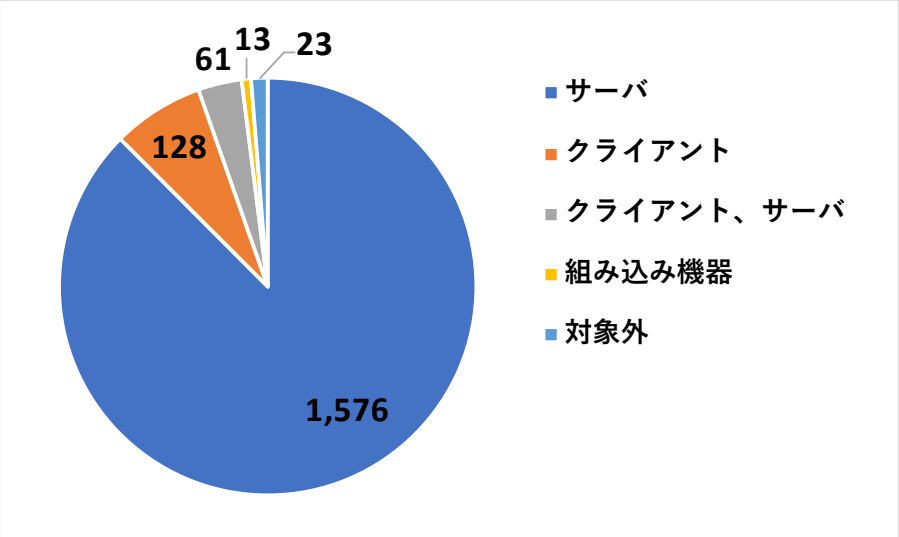
- OSS製品届出のうち
  - 75% が「ウェブアプリケーションソフト」
    → CMS製品が大半を占める
  - 7% が「アプリケーション開発・実行環境」



OSS製品の製品種類内訳
（届出受付開始から2019年9月末迄のOSS製品1,801件）

OSS製品届出のプラットフォーム内訳

- OSS製品届出のうち
  - 88% が サーバ上で稼働する製品
    - → CMS製品が大半を占めている事から



OSS製品のプラットフォーム内訳
（届出受付開始から2019年9月末迄のOSS製品1,801件）

パートナーシップへ OSS製品の脆弱性情報を届出る意義

- 発見者によるOSS脆弱性の波及範囲の確認や、網羅的な調整が困難
  - 発見者がOSS脆弱性を発見した際に、派生OSS／OSS組み込み製品に影響があるかまで検証するのは困難である
  - 発見者が派生OSS、OSS組み込み製品をすべて把握している訳ではないため、波及範囲の製品開発者へ網羅的に情報通知、調整を実施するのは困難
  - 仮に把握できたとしても数が膨大となるため、人力での対応は困難
  - 未通知・未修正の状態での脆弱性情報公表となる可能性があり、 攻撃の誘発の恐れあり
- パートナーシップでは長年のノウハウや製品開発者とのチャネルが豊富
- 製品開発者が影響を受けるソフトウェアをJPCERT/CCに登録しているため、情報の提供が効率的
- 複数の製品開発者やJVNでの同時公開の調整が可能

脆弱性情報調整における課題など

JPCERTコーディネーションセンター
早期警戒グループ
国際連携スペシャリスト
伊藤 智貴

脆弱性情報調整
Coordinated Vulnerability Disclosure

脆弱性情報調整 (CVD)

- 脆弱性情報ハンドリング、CVD (Coordinated Vulnerability Disclosure) とも呼ばれる
- 公表前の脆弱性関連情報について、それが悪用される可能性を最小限に食い止めるために、対策に必要な情報を適切な関係者に送達し、関係者による対策のタイミングを調整する等の一連のプロセス

脆弱性ハンドリングとは
https://www.jpcert.or.jp/vh/

脆弱性情報調整 (CVD)

- 「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）」「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」に基づき、ソフトウエア製品に係る脆弱性情報の公表を行っている

- 参考文献

  JPCERT/CC 製品開発者リスト登録規約

  https://www.jpcert.or.jp/vh/vul-agreement20170731.pdf

脆弱性情報調整 (CVD) の流れ

脆弱性情報調整 (CVD)

■ 本枠組みにおける CVD の基本的な流れ

① 発見者がソフトウエア製品の脆弱性を発見
② 発見者が受付機関に脆弱性情報を届け出る
③ 受付機関は届出られた脆弱性情報を確認し、調整機関に共有
④ 調整機関は受付機関から届出を受領、届出の内容の確認
⑤ 調整機関は製品開発者に連絡、情報提供
⑥ 製品開発者による対応
⑦ 調整機関は情報公開日の策定、JVN 公表文案の調整など
⑧ CNAがCVE 採番
⑨ 情報公開 (製品開発者、JVN)

脆弱性情報調整 (CVD)

- ここでは、主に製品開発者との調整に関わる、下記④から⑨の項目について説明する

① 発見者がソフトウエア製品の脆弱性を発見
② 発見者が受付機関に脆弱性情報を届け出る
③ 受付機関は届出られた脆弱性情報を確認し、調整機関と共有
④ 調整機関は受付機関から届出を受領、届出の内容の確認
⑤ 調整機関は製品開発者に連絡、情報提供
⑥ 製品開発者による対応
⑦ 調整機関は情報公開日の策定、JVN 公表文案の調整など
⑧ CNAがCVE 採番
⑨ 情報公開 (製品開発者、JVN)

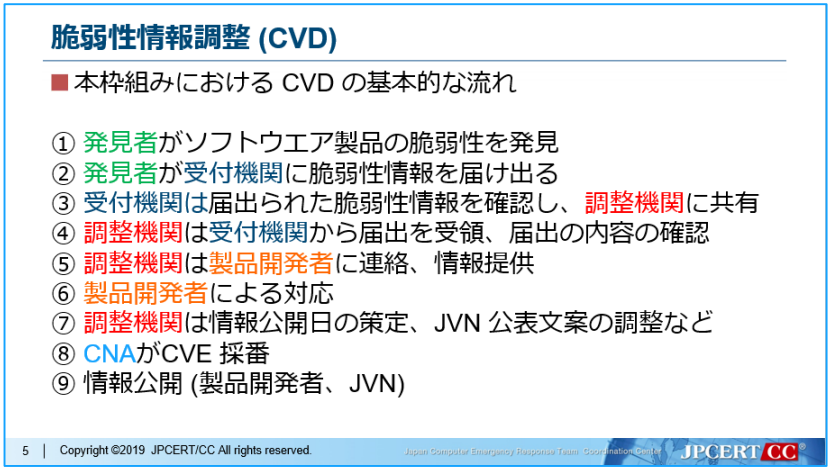
脆弱性情報調整 (CVD) におけるポイント

- JVN 公表文の調整
  - 製品開発者による問題への対応 (修正版作成など) 完了後の情報公開
  - 製品開発者、JPCERT/CC、 IPA 3者間で公表文案を調整

- 脆弱性への CVE ID の採番
  - JPCERT/CC は Root CNA として活動
    - 脆弱性を識別するCVE番号の新体系による採番のお知らせ
      https://www.jpcert.or.jp/pr/2014/pr140006.html
    - CNA (CVE Numbering Authority)
      https://www.jpcert.or.jp/vh/cna.html

- 必ずしもすべてのプロセスがシステム化されているのではない
  - システム化されている箇所とそうでない箇所が含まれる
    - 届け出された情報の確認や新規の連絡先の捜索など

CVD 課題



脆弱性情報調整 (CVD)

■ 本枠組みにおける CVD の基本的な流れ

① 発見者がソフトウエア製品の脆弱性を発見
② 発見者が受付機関に脆弱性情報を届け出る
③ 受付機関は届出られた脆弱性情報を確認し、調整機関に共有
④ 調整機関は受付機関から届出を受領、届出の内容の確認
⑤ 調整機関は製品開発者に連絡、情報提供
⑥ 製品開発者による対応
⑦ 調整機関は情報公開日の策定、JVN 公表文案の調整など
⑧ CNAがCVE 採番
⑨ 情報公開 (製品開発者、JVN)

調整手順と各段階における課題 (1/3)

- ④調整機関は 受付機関から届出を受領、届出の内容の確認
  - 登録作業や管理作業などで手動による作業が伴う
    - システム化、SBOM、 VDOなどのシステム化が解決への途を開ける可能性はあるのではないか

- ⑤ 調整機関は製品開発者に連絡、情報提供
  - 製品開発者とのコミュニケーションに対する課題
    - 連絡先が見つからない、もしくは見つけにくいケース
      - 発見した連絡先は正しい連絡先であるかの確認も必要
    - 連絡が返ってこないケース
    - など
  - 調整コスト、スケーリングなどにも課題
  - 電子メールを利用した連絡に頼らざるを得ない

調整手順と各段階における課題 (2/3)

- ⑥ 製品開発者による対応
  - 製品開発者での対応におけるコスト、調整が課題
  - 脆弱性調整においては…
    - 脆弱性であるか否か、製品開発者との見解相違
    - JVN 公表への合意がとれないケース
    - 製品開発者のコスト (脆弱性への対応に遅れが発生するなど)

- ⑦ 調整機関は情報公開日を策定、JVN 公表文案の調整など
  - 調整における情報漏えいリスク
    - 現状においては、連絡手段として電子メールに頼らざるを得ない
  - JVN の記述に関する見解相違が発生することもある

調整手順と各段階における課題 (3/3)

- ⑧ CVE 採番
  - CVE 採番プロセス
    - 現在は、JVN に採番する CVE ID の管理、CVE Description の作成を JPCERT/CC (Root CNA) が行っている
    - Sub CNA と分業することは可能
      - 脆弱性について最も理解しているのは製品開発者
      - 製品開発者が Sub CNA として活動した場合に、登録情報の確認がスムーズに行えるだけでなく、CVD コミュニティの底上げ、コスト分散につながる可能性があるのではないか

- ⑨情報公開 (製品開発者、JVN)
  - 対応速度への課題
    - JVN では製品開発者の情報公開と基本的に「同日公表」を行うが、公表文案の作成や、関係者間での調整に時間がかかるなどの理由により、公表が遅れることがある

マルチパーティ CVD

マルチパーティ CVD とは (特徴など)

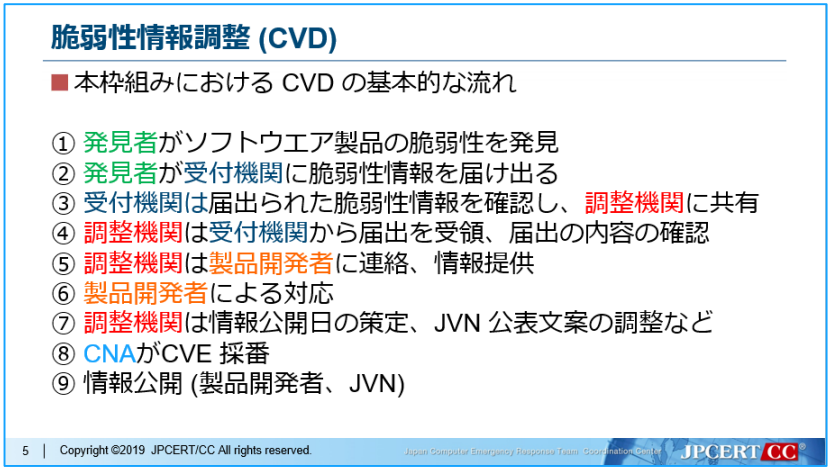
- 複数関係者間で行われる脆弱性情報調整
- 脆弱性の影響が広範囲に渡るもの
  - 脆弱性が発見されたコンポーネントを自社製品に取り込んでいる開発者が複数存在するケースなど…
- 修正時期など、各社ごとの状況の相違が発生
- 関係者複数存在するゆえに、調整がより複雑
  - 共通した認識を持つことが必要

複数製品開発者 (マルチパーティ) 間における CVD

- 本フレームワークにおけるマルチパーティ CVD の流れ
  - 基本的な流れは “CVD” と同様であるが、項目⑤の工程が追加される

① 発見者がソフトウエア製品の脆弱性を発見
② 発見者が受付機関に脆弱性情報を届け出る
③ 受付機関は届出られた脆弱性情報を確認し、調整機関と共有
④ 調整機関は受付機関から届出を受領、届出の内容の確認
⑤ 調整機関は脆弱性の影響を受ける可能性のある製品開発者を特定
⑥ 調整機関は製品開発者に連絡、情報提供
⑦ 製品開発者による対応
⑧ 調整機関は情報公開日の策定、JVN 公表文案の調整など
⑨ JPCERT/CCがCVE 採番
⑩ 情報公開 (製品開発者、JVN)

マルチパーティ CVD 特有の課題



調整手順と各段階における課題 (1/2)

- ⑤ 問題に影響を受ける可能性のある製品開発者を特定
  - 手動での対応が求められるため対象組織特定の正確性、速度の確保に課題
    → SBoM への課題

- ⑥ 製品開発者への連絡、情報提供
  - 情報管理に対する課題
    - 製品開発者から OEM 元など他組織への展開など、情報の漏えい(情報管理との相反)が発生する可能性

調整手順と各段階における課題 (2/2)

- ⑦ 製品開発者による対応
  - 脆弱性影響範囲特定の正確性確保
    - 対象製品開発者による自社製品への影響確認

    → SBOM に期待

- ⑧ 情報公開日策定、JVN 公表文案の調整など
  - 各関係者間での対応速度の相違
    - 製品開発者ごとの対応速度に差異が存在し、情報公開日の決定が難しくなるケースがある

まとめ

- CVD、 マルチ CVD の様々な場面において、正確性、速度、コストの確保の問題など、各関係者間で共通する課題が存在している
- これらの課題の解決のために、CVE、 SBOM などをツールとして使用し、CVD コミュニティの拡大、底上げを行うことが必要と考える

ご清聴ありがとうございました

お問合せ、インシデント対応のご依頼は

JPCERTコーディネーションセンター

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

インシデント報告

- Email：info@jpcert.or.jp
- https://www.jpcert.or.jp/form/

制御システムインシデントの報告

- Email：icsr-ir@jpcert.or.jp
- https://www.jpcert.or.jp/ics/ics-form.html