欧州法規制等の法的対応で関心が高まる脆弱性対応に関する国際動向

－共に協調していくために必要なこと－

JPCERTコーディネーションセンター
国際部 Global CVD Project Lead
伊藤 智貴

脆弱性に関する複数の国際議論に参加しています

- 意識している点：
  1. 脆弱性情報が適切な関係者に届き、公表・活用されること
     - その結果、関係者のそれぞれのリスクが低減される
  2. 国際的なバランス
     - 日本の事情が考慮され、なるべく負担が少ない形で進んでほしい
     - そのためには、他のさまざまな国や地域にとっても有益になる形で話が進むことが必要不可欠
  3. さまざまな声が仕組みに組み込まれること
     - 脆弱性管理、調整、活用などの場面における多様な意見が反映された形で進むこと

本発表の趣旨

- 脆弱性情報の取り扱いを巡る議論は、現在、国際的にさまざまな場で進められている
- 本発表では、国際的な動向や存在する課題、議論のポイントを紹介するとともに、それらを踏まえて関係者に意識・実践してほしい取り組みについて共有する

脆弱性情報

脆弱性情報

- ソフトウェアやシステムに存在する脆弱性に関する、第三者に提供可能な情報

- 脆弱性情報には二つの課題が存在する：

1. 技術的課題
   - 脆弱性の内容や影響範囲の正確な記載
   - データクオリティ
2. 運用上の課題
   - 情報の取り扱いや情報公開、関係者への共有等
   - 受け付けや公表等、その情報流通が各立場における様々なリスクに影響する

CVD

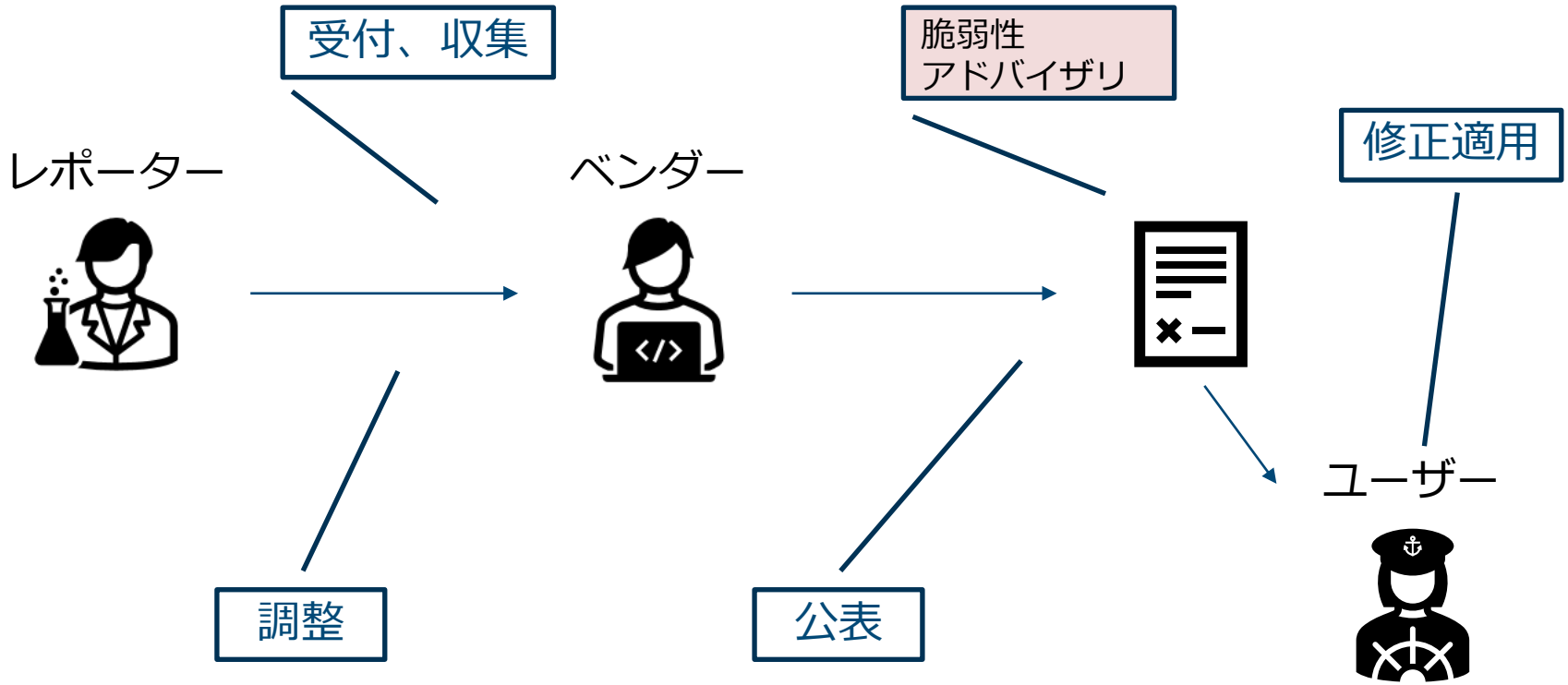
CVD：Coordinated Vulnerability Disclosure

- Coordinated Vulnerability Disclosure（CVD）
  - 脆弱性情報の収集／受け付け、調整、公表からなる一連のプロセス
  - 脆弱性情報が適切に流通しない場合、対策が作成されない、また、そのまま公表されてゼロデイ攻撃に悪用される等のリスクが増加
  - CVDはリスク低減活動
  - 時に多くの関係者（ベンダー等）がCVDケースに参加する（MPCVD＝Multi Party Coordinated Vulnerability Disclosure）

CVDにおける基本的なステークホルダー／役割

- レポーター（例：リサーチャーやベンダーによる自社製品脆弱性届け出など）
  - 脆弱性情報を報告する
- ベンダー（例：製品開発主体）
  - 脆弱性に影響を受ける、修正する
  - 脆弱性情報を公表する
- ユーザー（例：製品利用者）
  - 脆弱性の影響を受ける
  - 公表された脆弱性情報に基づき修正などの対応をする
- コーディネーター（例：JPCERT/CC等の調整機関）
  - 第三者コーディネーター
  - 仲介、意見提供、案件リード等、CVDケースを支援する
  - 脆弱性情報を公表する

脆弱性調整時の情報の流れ



JPCERT/CCのCVD活動

- JPCERT/CCは、CVDコーディネーターとして、国内・海外問わず脆弱性調整を行っている
- 関係者と連携し、脆弱性情報を調整
  - ベンダー
  - レポーター
  - 海外コーディネーター
- 情報セキュリティ早期警戒パートナーシップ
  - 日本のCVDフレームワーク
  - JPCERT/CCは調整機関としての役割を担う
- CVDの普及
  - ドキュメント作成
  - PSIRT向けトレーニング

国際的な課題：異なるギャップの存在

- 文化や言語の壁
- 各関係者間で異なる“CVD”認識
- 経験値や理解のばらつき
  - これらはCVDケースの失敗につながる

これらを埋めるためのアプローチ

- 共通理解の促進：WG等
- 自動化：プロセスや脆弱性アドバイザリ

CVE

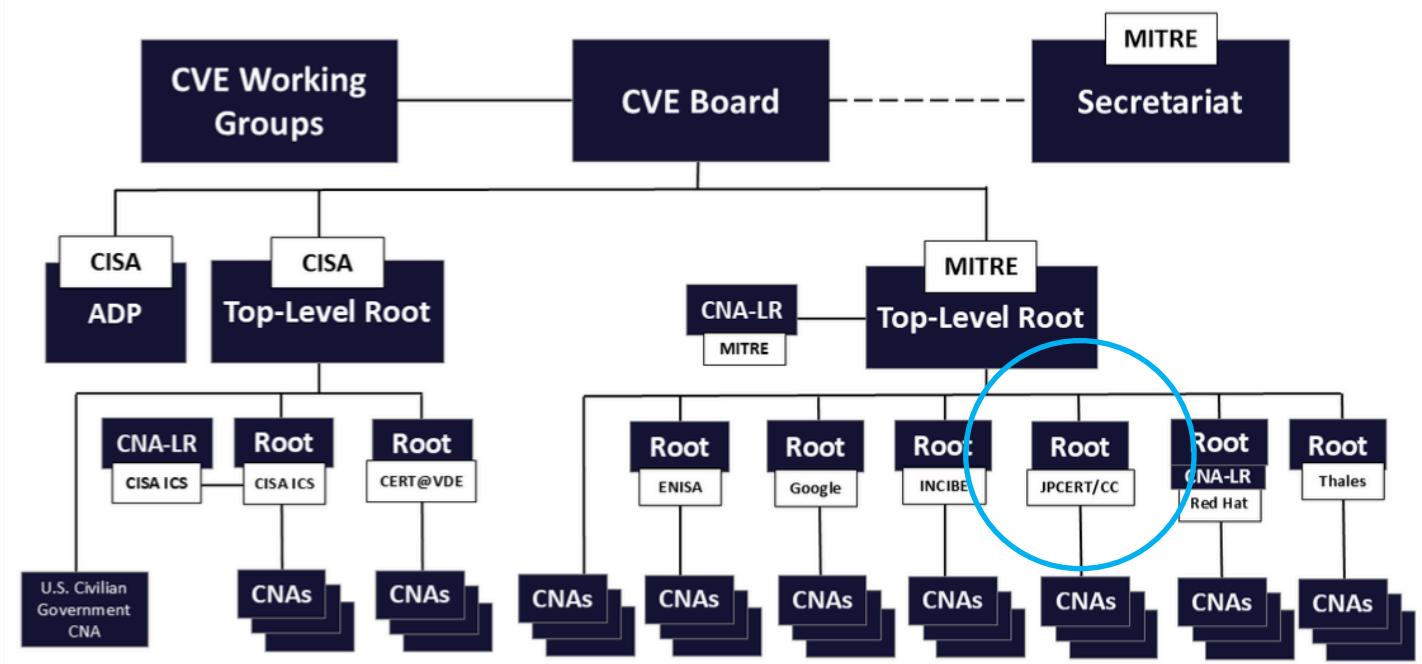
CVE

- CVE（Common Vulnerabilities and Exposures）：
  脆弱性を一意に識別するためのID
  - 同じ脆弱性について、世界中で同じ名前で呼べるようにすることで、組織や国を超えた対応や連携を支援する
- CNA（CVE Numbering Authority）：CVEを付与する組織
  - 設定されたスコープ内の脆弱性に対してCVE IDを付与する

JPCERT/CCのCVE Programにおける役割

- CNAとしての役割
  - スコープ：脆弱性調整において取り扱う脆弱性にCVE IDを付与
- Rootとしての役割
  - スコープ：日本国内の組織が対象
  - 現在、傘下に11のCNAが存在
    - LINEヤフー、三菱電機、キヤノン、オムロン、OpenAMコンソーシアム、NEC、パナソニック、東芝、日立、横河電機、任天堂

CVE Program組織構造図とJPCERT/CC



出典：CVE「Program Organization_Structure」
https://www.cve.org/ProgramOrganization/Structure

CVE Program状況

- CNAの数は増加中：
  - 2026年1月30日時点で490
  - Rootも増加：近年ではRed Hat（OSS）、CERT@VDE（パートナー組織や制御システムベンダー）、ENISA（EU CSIRT）がRootに
- 昨今、NVDの機能停止や、CVE Program停止の恐れなどの問題が発生
  - NVDバックログは解消中。CVE Program停止は回避されたが、そのあり方について引き続き議論されている。
    現在、状況は少し落ち着き、それぞれ運営されている

CVE Programにおける現状の課題

- CVEの普及
  - 国際的に、またさまざまな業種においてCNAを増やすこと
- Enrichment
  - CVE Recordに埋め込む情報の拡充
  - CWE、CVSS記載の推奨
- データクオリティ
  - 正確な脆弱性情報の記載
  - 判断に使える、アクショナブルな情報となっているか
- CNAによる適切な脆弱性対応の推奨
  - 適切な脆弱性ハンドリング、調整、公表ができているか

SBOM

SBOMについて

- Software Bill of Materials＝SBOM
  - ソフトウェア部品リスト
  - 脆弱性対応、脆弱性管理、サプライチェーン管理、法規制対応等に使用される
- 米国NTIA⇨CISAと場を移してきたが、CISA SBOM Communityの消滅によって、現状は“主”となる議論の場が存在していない
  - ただし、異なるコミニュティなどにおいて、引き続き議論は進んでいる
  - CISAも引き続きSBOM Minimum Elementsの更新などを手掛けている

その他SBOM国際状況

- 企業等によるSBOM実装も引き続き進んでいる
- 複数の国がSBOMや、SBOMを含むサプライチェーン課題に関してガイドライン等資料を発行している（ドイツ、韓国、インド等）
- 日本では経済産業省が
  - SBOM等に関する議論を行う“サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース”を主催（JPCERT/CCも参加）
  - 『ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引』を発行
    https://www.meti.go.jp/press/2024/08/20240829001/20240829001-1r.pdf

SBOMの目的：“透明化”

- SBOM＝透明化、把握のための道具といえる
  - 何が入っているか、どのバージョンか、どこから来た部品か
- SBOMとCVD：ベンダーによる使用部品の把握
  - ベンダーが脆弱性情報の通知を受けても、自社製品に含まれている部品を把握していないと影響に気付けない
- SBOMとCVE：脆弱性管理における、ソフトウェア部品とCVE（脆弱性情報）との突き合わせ

手持ちの部品を把握していないと適切な対応を取ることができない

SBOM実用に向けて国際的に議論されている課題

- ソフトウェア識別子
  - 異なる仕組みや取得方法の識別子フォーマットが存在
  - 同じ部品でも、異なるIDで登録されると別部品として認識される
  - 追跡、脆弱性対応、ライフサイクル管理が困難
- カバレッジ（SBOM情報の網羅性）
  - ソフトウェアを構成する部品リストを作成⇨それらの部品に使用されているライブラリ等はどこまでSBOMに含めるのか？（脆弱性調整・対応における“影響の把握”）
- ツール
  - 自動的なSBOM活用に必要不可欠
  - ツール性能や価格の問題
  - 異なるツールによって異なるSBOMが生成される

EU法規制関連

EU Cyber Resilience Act（CRA）

- デジタル要素を含む製品のサイバーセキュリティを強化し、消費者を保護するための規制
- 脆弱性関連要件：
  - Vulnerability Disclosure Policy（VDP／脆弱性公表ポリシー）の準備、公開
    - CVD、脆弱性公表の仕組みを持つこと
  - 悪用されている脆弱性の報告
    - 実際に悪用されている製品の脆弱性について、悪用を認識してから原則として24時間以内にCSIRT／ENISAに報告
  - SBOMの準備、（要求がある場合）当局への提供
    - 対象部品のTop-level dependencies（直接依存関係）情報の記載
    - 独BSIが補完的な文書を作成・公開している（BSI TR-03183）

NIS2 Directives（NIS2指令）

- エネルギーや交通、医療、公共行政などの“Essential entities”と、特定分野の製造業、デジタルサービスなどの“Important entities”を対象とした、組織・事業者向けのEUサイバーセキュリティ規制指令

- セキュリティリスク管理、インシデント対応体制、インシデント／重大な脆弱性の報告が求められる
  - 重大な脆弱性＝組織が使用／運営しているシステムやサービスに存在し、提供するサービスに重大な影響を与え得るもの
    - 機密性、可用性、完全性への影響
    - 悪用されている、社会への影響

      …等、リスク評価によって決まる
    - 報告先はEU各加盟国のCSIRT／監督当局

その他EUに関する状況

- 法規制を背景に、EUのCSIRT等関係者がCVDやCVE、SBOM議論に参加し、発言することが増えている
  - 各議論においてEUの影響も増している
- EUの脆弱性データベース“EUVD（European Vulnerability Database）”が立ち上がり、運用されている

  https://euvd.enisa.europa.eu/
  - エコシステム情報源がよりマルチソースな形に
  - 歓迎する声がある一方、運用コストや国際的な互換性等について懸念も生じている

EU規制による国内関係者への影響

- EU CRAにおいて、規制の対象となるのはベンダー
- ただし、CRAで特定・公表された脆弱性の情報は、ユーザー等データ利用者に届く
  - データ量の増加
  - データの判断：情報の受付や判断基準等の準備が必要
- NIS2における“重大な脆弱性”に関するリスクベースの考え方も、国際的な一つの参考基準となる可能性がある
  - 直接的または間接的に、多くの関係者が影響を受ける
- ベンダーであるか・EUで商売するか否かにかかわらず、脆弱性情報を適切に取り扱うための体制・構えの準備が重要となる

脆弱性対応を共に進めるために、
関係者に対応を検討いただきたい事項

– ここまでに紹介した国際動向を踏まえて –

変化する状況の中、今できること

- 脆弱性情報をどう取り扱うかが、それぞれの立場におけるさまざまなリスクに影響
- CVD、CVE、SBOM等、異なる手法や概念、仕組みの実装が国際的に進んでいる。EU規制の影響が日本国内にも出てくる
- そのような状況の中、情報の受け付けから調整、公表、活用まで、各関係者の情報取り扱い能力の確保や向上が求められている
- 置かれている立場に応じて必要な機能の実装を進めていただきたい。大きく分けると
  - ベンダーには：脆弱性公表、ハンドリング
  - ユーザーには：脆弱性管理

ベンダーに意識、対応を検討いただきたい点

a. 脆弱性対応体制の整備
   - 脆弱性公表
   - 脆弱性ハンドリング
     - ポリシー設置の検討

b. 製品サプライチェーン関係の把握
   - 使用部品
     - OSやプロトコル、インタフェースなどに使用されるOSSも含む
     - 脆弱性情報のやり取りのため、連絡経路の把握も重要

c. 作成するデータのクオリティ確保、向上
   - 情報は正確か、判断に必要な情報が記載されているか

d. CVE：自社製品の脆弱性に継続的にCVEを付与する必要がある場合、CNAになることを検討

ユーザーに意識、対応を検討いただきたい点

a. 脆弱性管理

1. 対象ソフトウェア・部品の把握
   - SBOM活用等
2. 識別方法・IDの統一
   - CPE、PURL…等
3. 情報取得のルートの確保
   - 脆弱性データベースから情報を受け取れる仕組み
4. 脆弱性評価と優先度付け
   - 優先度付け：SSVC（意思決定）やEPSS（脆弱性悪用可能性）など使用可能
5. 修正・パッチ対応

b. 活用する脆弱性情報のクオリティの確認

— 情報は正確か、判断に必要な情報が記載されているか
   - データ作成者にフィードバックを提供して欲しい

CVDに関連して次の状況の場合…

- ベンダー
  - “脆弱性調整に参加したい。脆弱性情報を受け取りたい”
  - “報告者または海外コーディネーター等から自社の脆弱性に関する連絡があったが、どう動いて・判断していいかわからない”
  - “その他脆弱性調整について知りたい”
    - **JPCERT/CCにご連絡ください**
- ユーザー
  - “JVNアドバイザリの内容で不明な点がある”
    - **JPCERT/CCにご連絡ください**

また、CVEに関連して次のような状況の場合…

- ベンダー
  - “自社製品の脆弱性に（単発で）CVEを付与したい”
  - “自社製品の脆弱性をスコープとしたCNAになりたい”
  - “その他CVEやCVE Programについて質問がある”
    - **JPCERT/CCにご連絡ください**
- ユーザー
  - “CVE情報に不明点や指摘がある”
    - **該当CNAに連絡してみてください。**
      難しい場合は、JPCERT/CCにご相談ください

SBOMについてよく聞かれる質問①

- 関係者全般
  - “SBOMについて知りたい”“SBOMをどこから始めていいかわからない”
    - **まずは前述の経産省手引を参照してください。基本や実装について網羅的に記載されています**
- ベンダー
  - “SBOMフォーマットをどう選択すべきかわからない”
    - **一般的に**
      - **SPDX：OSS、ライセンス表記の正確性**
        CycloneDX：脆弱性・依存関係把握の容易さ
        … などの強みがあると言われますが、利点は立場によって異なります
      - **自社のポリシーや事情に沿って選んでください。両方出しているベンダーも存在します**
  - “SBOMにどの程度の情報を記載すればいいのかわからない”
    - **業界等によって要求レベルが異なります**
    - **まずはSBOM Minimum Elements情報を記載することから始めてみてください**
      （※Minimum Elementsは現在更新中）

SBOMについてよく聞かれる質問②

- ユーザー
  - “SBOMを使いこなせる環境作りが必要、どこから始めるのがいいか”
    - **まずは手持ち資産の把握が大事です。すべてでなくても、次のような観点で資産と優先順位を整理してみてください**
      - **どのような製品・サービスがあるか**
      - **どの製品・サービスが止まると困るか**
  - “SBOMを取得して脆弱性管理に活用したい”
    - **可能であればベンダーにSBOMをリクエストしてみてください。入手できない場合は、ツールを使用し、自社で解析・SBOM生成するという手もあります**
  - “SBOMツールが高額で導入できない”
    - **Linux FoundationやOWASPによるものも含め、無料のツールが多く提供されています**

まとめ

まとめ

- 脆弱性に関連する多くの議論とその手法等の実装が国際的に進んでいる
- そのような状況において、脆弱性情報取り扱い能力の確保・向上が、国や地域、業種、立場を超えて求められている
- 国際的に、また分野を問わず、脆弱性情報がバランスの取れたフェアな形で適切に流通し、活用される世界を皆さまと協力して作っていきたい
- 各地域や関係者になるべく負担がなく物事が進むよう、声を集めている。本イベント中においても、皆さまの状況やICS環境について、いろいろ教えていただけるとありがたいです

ご清聴ありがとうございました