# コーディネーションセンターというお仕事

JPCERTコーディネーションセンター
早期警戒グループ　脅威アナリスト
輿石 隆

# 自己紹介

- 大学では経営工学を専攻
- 2016年4月より現職（中途採用）
- 早期警戒グループにて情報発信業務に従事
  - 国内組織に向けて、
    - 注意喚起などのアラートの情報の発信
    - 対象となる組織ごとにインシデントに関する通知を実施

# JPCERT/CCとは？

# JPCERT/CC とは

## ■ 一般社団法人JPCERTコーディネーションセンター (JPCERT/CC)

**Japan Computer Emergency Response Team / Coordination Center**

**活動内容/役割：**

**技術的な立場から国内の「セキュリティ向上を推進する活動」**を実施

- コンピューターセキュリティインシデントへの対応
- 国内外にセンサーをおいたインターネット定点観測
- ソフトウェアや情報システム・制御システム機器等の脆弱性への対応など

**日本の窓口となる「CSIRT」**

- インシデント対応をはじめとする、国際連携が必要なオペレーションや情報連携を実施
  ※米国のCISA（US-CERT）、韓国のKrCERT/CCなど、各国に同様の窓口CSIRTが存在

**主なサービス対象:**

**国内のインターネット利用者やセキュリティ管理担当者、ソフトウェア製品開発者等（主に、情報セキュリティ担当者）**

■ 経済産業省からの委託事業として、**サイバー攻撃等国際連携対応調整事業を実施**

# JPCERT/CC の活動

**インシデント予防** → **インシデントの予測と捕捉** → **発生したインシデントへの対応**

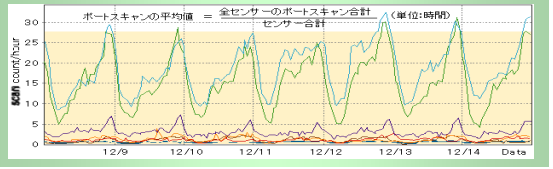
### 脆弱性情報ハンドリング

- 未公開の脆弱性関連情報を製品開発者へ提供し、対応依頼
- 関係機関と連携し、国際的に情報公開日を調整
- セキュアなコーディング手法の普及
- 制御システムに関する脆弱性関連情報の適切な流通

JVN Japan Vulnerability Notes

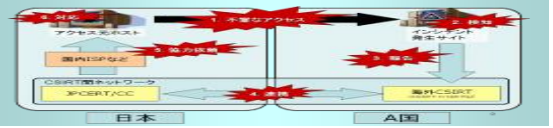
### 情報収集・分析・発信
**定点観測（TSUBAME）**

- ネットワークトラフィック情報の収集分析
- セキュリティ上の脅威情報の収集、分析、必要とする組織への提供




### インシデントハンドリング
**（インシデント対応調整支援）**

- マルウェアの接続先等の攻撃関連サイト等の閉鎖等による被害最小化
- 攻撃手法の分析支援による被害可能性の確認、拡散抑止
- 再発防止に向けた関係各関の情報交換および情報共有

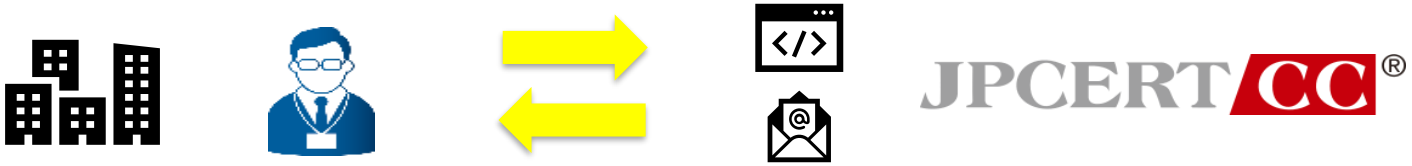



| | |
|---|---|
| **早期警戒情報** | 重要インフラ、重要情報インフラ事業者等の特定組織向け情報発信 |
| **脆弱性情報ハンドリング** | ソフトウェア製品等の脆弱性情報に関わる開発者等との調整・公表 |
| **CSIRT構築支援** | 海外のNational-CSIRTや企業内のセキュリティ対応組織の構築・運用支援 |
| **アーティファクト分析** | マルウェア（不正プログラム）等の攻撃手法の分析、解析 |
| **制御システムセキュリティ** | 制御システムに関するインシデントハンドリング/情報収集,分析発信 |
| **国内外関係者との連携** | 日本シーサート協議会、フィッシング対策協議会の事務局運営等 |
| **国際連携** | 各種業務を円滑に行うための海外関係機関との連携 |

# JPCERT/CCの取り組み

# インシデント対応支援

JPCERT/CC
インシデント対応依頼
https://www.jpcert.or.jp/form/




**国内(国外)組織からインシデントに関する相談/報告（例）**

対応依頼
- フィッシングサイトの閉鎖
- 改ざんされたサイトへの対応
- マルウェアが通信を行うサーバーの管理者への対応依頼　等

情報提供の受領
- 改ざん疑いのサイト情報
- アクセスログの提供
- マルウェアの感染被害の情報　等

**技術的な立場から**の支援活動の範疇を超える対応はできない
- 捜査、取り締まり
- 法的な対応の代行　等

<注意>
JPCERT/CCの活動は、特定の個人や組織の利益を保証することを目的としたものではありません。個別の問題に関するお問い合わせ等に対して、必ずお答えできるとは限らないことをあらかじめご了承ください。

# 初動対応支援

JPCERT/CC
高度サイバー攻撃 (標的型攻撃) に関する連絡
https://www.jpcert.or.jp/incidentcall/

## ■ 標的型攻撃に関連する報告などを受けた際に初動対応を支援

インシデント対応プロセス


### 検知

**連絡を受けた内容に応じ、ネットワーク機器やセキュリティ製品のログなどで調査**

- C&C (C2) サーバやマルウエアの通信先サイトへの通信の有無
- 攻撃者によって改ざんされたサイト (いわゆる水飲み場攻撃) やマルウエア設置サイトへの通信の有無
- 標的型攻撃メールの添付ファイルの実行や誘導先サイトへの通信の有無

JPCERT/CCでは初期の調査支援を実施。プロキシ、ファイアウォールなどのログや被疑端末の分析による被害の有無の調査支援も実施可

調査の結果、被疑端末を特定できた場合、証拠保全を行い、次の調査を推奨している。
（ただし、被疑端末の調査や影響範囲の調査は、専門知識や経験が無い状態で実施すると攻撃の痕跡を消してしまうなどのリスクがあるため、安易に実施せず、セキュリティ事業者などに相談を推奨している）

### 分析

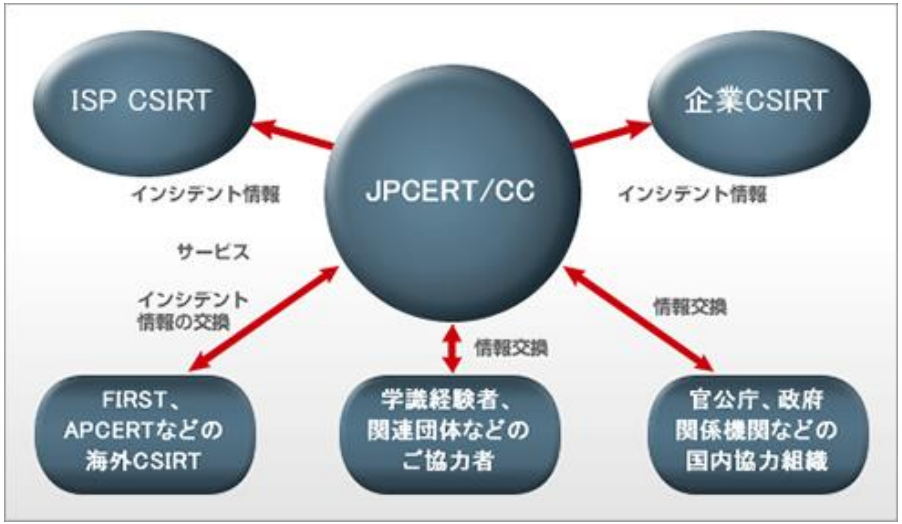
**被疑端末の状況とその端末からネットワーク全体への被害拡大状況の調査**

- 被疑端末の簡易調査
  - 不審なサービスの実行の有無
  - 意図しない待ち受けポートの有無
  - 不審なタスク登録の有無
  - 不審なファイルの有無
  - 連絡を受けた通信先以外への意図しない通信の有無
- 被疑端末と類似する通信の確認
  - 別端末において同じ通信先への通信や類似するリクエストの有無
  - 別端末で同様の標的型攻撃メールの受信
- 内部向けサーバ (Active Directory、ファイルサーバなど) への侵害の確認
  - 不審なサービスの実行の有無
  - 意図しない待ち受けポートの有無
  - 不審なタスク登録の有無
  - 不審なファイルの有無
  - 権限が無いユーザの端末から管理者アカウントへの認証要求の有無
- 侵入経路と侵入時期の調査、推測
  - 標的型攻撃メールの送信元や受信日時
  - 改ざんサイト閲覧による感染とその日時
  - 公開サーバや DMZ サーバ経由での侵入の有無とその日時

# 国内/海外組織との調整業務

JPCERT/CC
早期警戒情報
https://www.jpcert.or.jp/wwinfo/

インターネット上で発生するインシデントは急速に拡大する可能性があるため、的確なインシデントレスポンスを行う必要があり、そのために、各組織におけるCSIRTやそれに準ずる組織間での情報共有を実施している




関連組織との連携

# 情報発信・情報共有・個別通知

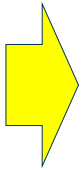
- さまざまなインシデントやサイバーセキュリティに関係する情報を、独自の情報網を活かして収集し、それらを分析して攻撃活動の兆候を探索、具体的な対策などの検討を行い、国内の重要インフラ事業者や企業、CSIRTやITベンダー等に対して情報を発信していく

**JPCERT/CC Webで発信**

- 注意喚起
- CyberNewsFlash
- WeeklyReport
- JPCERT/CC Eyes
- JVN 等

**個別に組織に連絡**

- CISTA経由
- 業務上でのつながり
- 業界団体経由
- Whois から
- コミュニティ 等



・攻撃に悪用されそうな（されている）製品の対策
・攻撃の検知や調査
・実際の被害状況の確認

などに活用してもらう

# JPCERT/CC Webで発信（注意喚起など）

HOME > 緊急情報を確認する > Cisco IOS XEのWeb UIの脆弱性(CVE-2023-20198)に関する注意喚起

通常レイアウトに戻す　印刷

## Cisco IOS XEのWeb UIの脆弱性(CVE-2023-20198)に関する注意喚起

最終更新: 2023-10-23

X ポスト　メール

JPCERT-AT-2023-0025
JPCERT/CC
2023-10-18（公開）
2023-10-23（更新）

### I. 概要

2023年10月16日（現地時間）、CiscoはCisco IOS XE ソフトウェアのWeb UI機能における権限昇格の脆弱性に関する情報を公開しています。同製品のWeb UI機能をインターネットまたは信頼されないネットワークに公開している場合、本脆弱性が悪用され、遠隔の認証されていない第三者が、最上位の特権アカウントを作成し、当該システムを制御する可能性があります。

更新: 2023年10月23日追記

2023年10月22日（現地時間）、Ciscoはアドバイザリを更新し、新たな脆弱性の情報と攻撃の内容に関する情報を公開しています。Ciscoは、CVE-2023-20198に加えて、新たにWeb UI機能の別コンポーネントの脆弱性にCVE-2023-20273を割り当てています。Ciscoの調査によると、攻撃者は、CVE-2023-20198を悪用してシステムに侵入し、最上位の特権レベルのコマンドを発行して新たなローカルユーザーを作成しました。その後、CVE-2023-20273を悪用し、作成したローカルユーザーの権限をルートに昇格させ、インプラントをファイルシステムに書き込んだとのことです。

JPCERT/CCでは、本脆弱性を悪用した攻撃による被害を確認しています。加えて、未精査の情報も含まれますが、本脆弱性を悪用した攻撃にて、対象機器に不審な設定ファイルが設置されているホストに関する情報が複数観測されています。同製品でWeb UI機能を利用している場合、CiscoやCisco Talosが提供する最新の情報を確認の上、推奨事項の適用および侵害痕跡の調査の実施を推奨します。

Cisco
Cisco IOS XE Software Web UI Privilege Escalation Vulnerability

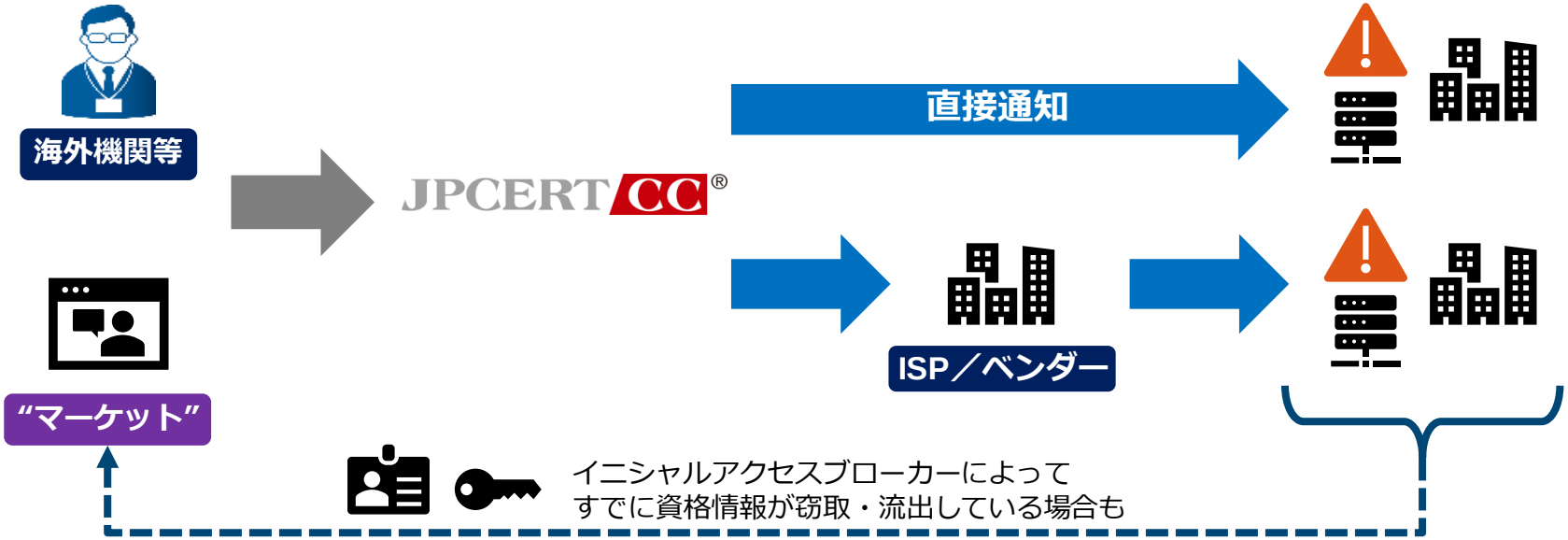
- **深刻かつ影響範囲の広い脆弱性**などに関する情報を告知するための文書
  - 国内で広く使われている製品
  - 既に悪用が確認され、国内にも被害が出ている　など

→早急に対策を行い、攻撃に備えてもらう、または被害がないかを確認してもらう

JPCERT/CC「注意喚起」から https://www.jpcert.or.jp/at/2023/at230025.html

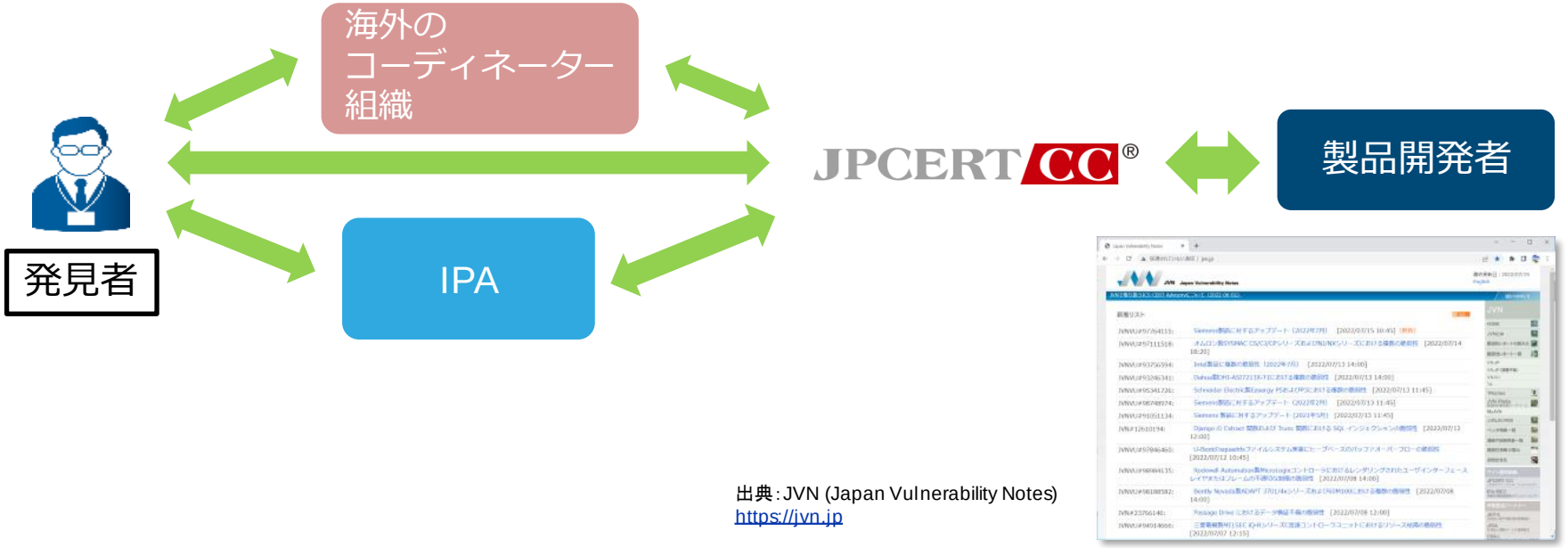
# 個別に組織に連絡（JPCERT/CCによる通知オペレーション）

- 脆弱なままのホストや、すでに脆弱性の悪用により不正プログラム設置や改ざん、認証情報が窃取されているホストの利用組織に対して通知オペレーションを実施
- 残念ながら、対応いただけなかったり、情報が伝わらないケースもある



# 脆弱性情報流通

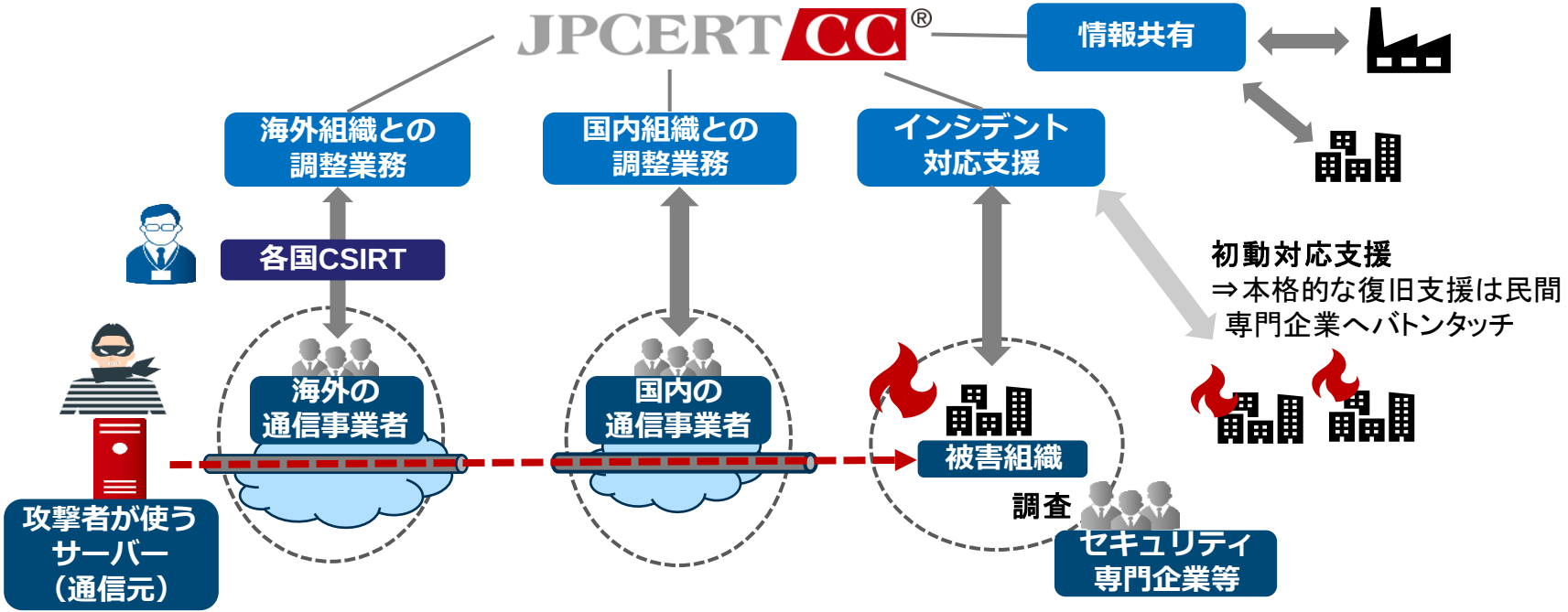
- 脆弱性情報流通の枠組みにおけるコーディネーターとして活動
  - 情報セキュリティ早期警戒パートナーシップ
    （経産省告示にもとづく脆弱性情報流通の枠組み）
  - 海外のコーディネーター組織／機関や発見者コミュニティーとの連携




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

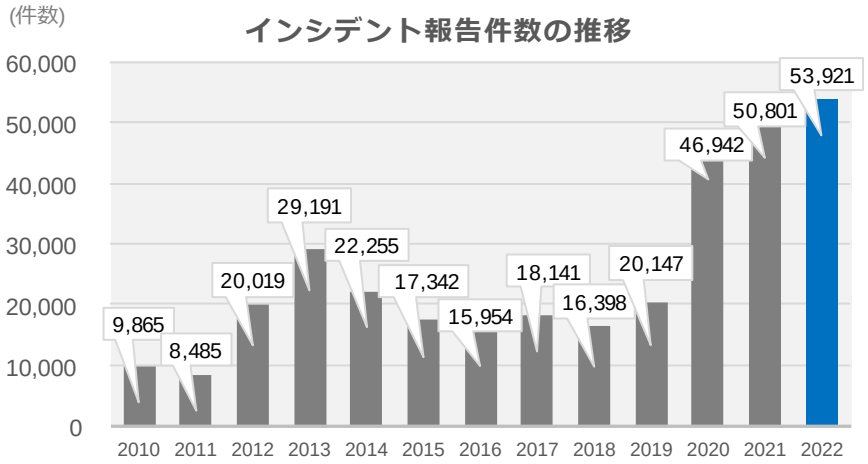
# サイバー攻撃の停止活動

- 攻撃の停止に向けて国内外の複数組織間の情報共有・調整業務を実施
- 国内複数組織への広範囲な攻撃について情報を収集し、各方面へ共有



# インシデント対応状況（2022年4月～2023年3月）

- JPCERT/CCへの報告
  - 全報告件数 53,921件
  - 全インシデント件数 40,263件
- JPCERT/CCからの連絡
  - 全調整件数 23,419件




インシデント件数のカテゴリー別割合

| カテゴリー | 割合 |
|---|---|
| フィッシングサイト | 68.12% |
| スキャン | 21.75% |
| Webサイト改ざん | 5.07% |
| マルウェアサイト | 1.77% |
| DoS / DDoS | 0.07% |
| 標的型攻撃 | 0.02% |
| その他 | 3.20% |

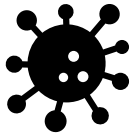
「JPCERT/CC インシデント報告対応四半期レポート」から
https://www.jpcert.or.jp/ir/report.html

# 今の組織に所属して

# 【今の組織に所属して】難しさ

## ■ アラートを出すということ

ある人曰く、とある製品に
深刻な脆弱性が出た



どんな脆弱性？

悪用/PoCは出ている？

対策は？

製品は国内でどれくらい
使われている？

どんな使い方？

**どうやって共有する？**

## ■ 常に万全のコミュニケーション、100%の対応ができるとは限らない

とある製品の侵害
情報を確認→通知

そもそも連絡口がない

適切な部署につながらない

バージョンアップできない

ログがない

Whois情報が古い

# 【今の組織に所属して】面白さ

- 思うままに日本のインターネットを守ることができる
  - 一般組織では自組織やユーザーを守ることが中心となる中、自分たちが助けたい人を助けられる！
- セキュリティの仕事にストイックに挑める
  - 発生しているインシデントに対して、ひたすら試行錯誤で解決を目指していく
- 常に新たな情報に触れることができる
  - 常に勉強

# 今までの
# 私のセキュリティに関する仕事の経緯

# 【私の場合】今の仕事に出合う前

- 経営工学を専攻

→情報セキュリティについてはほとんど知らなかった

- 大学では部活動に多くの時間を費やす
  - 主務的な担当もしており、調整を行うことに慣れていた

- システム開発の会社に就職

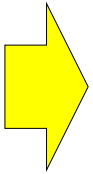
→基本的なITスキルは覚えていった

# 【私の場合】はじめてのセキュリティの仕事

■出向元で脆弱性に関する業務に従事

脆弱性に関する情報

・概要
・対象製品（バージョン）
・CVE-2023-XXX
・参考文献
・etc



確認・調査

・組織の中で対象製品が利用されているか（そのバージョンは該当するか）
・他に該当する条件はあるか
・緊急の対応が必要か

判定

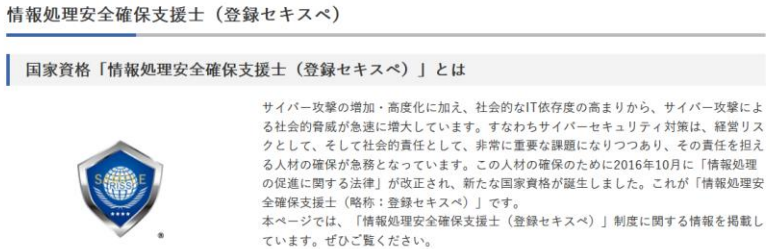
・バージョンアップ（orパッチの適用）を依頼
・いつ適用できるか
・過去に依頼したものの状況

# 【私の場合】挑戦をしてみることに

- セキュリティ業務に触れている中で、もっと知りたいというモチベーションに！

→資格を取ってみた
（セキュリティスペシャリスト）

- その中で、せっかくなら、セキュリティの仕事をもっとしてみたいという気持ちに！




出典：IPA（独立行政法人 情報処理推進機構）
情報処理安全確保支援士（登録セキスペ）
https://www.ipa.go.jp/jinzai/riss/index.html


JPCERT/CC「採用メッセージ」 https://www.jpcert.or.jp/recruit/

# 【今回のお題】どうしたらなれるの？

募集要項（**インシデントレスポンスグループ：マルウェアアナリスト／フォレンジックアナリスト**）

| | |
|---|---|
| 必須条件<br>（経験・スキル） | - 情報セキュリティ、ネットワーク、IT関連技術に関する広い知識（基本情報技術者試験、CCNA、LPICレベル1相当）<br>- システム管理・運用、システム構築、ソフトウェア開発、インシデントレスポンス、ネットワーク構築、セキュリティ関連業務のいずれかの経験<br>- コンパイラ系言語、スクリプト系言語それぞれ1つ以上のプログラミング経験がある方<br>- Unix/Linuxの基本機能について知識とシステムの使用経験<br>- 論理的で誤解のない技術文書を作成できる方(ボリュームは問わず)<br>- 英語の技術文書が読める方(辞書使用可)<br>- 技術トピックスについて簡単な英語でのメールのやり取りができる方<br>なお、マルウェア分析やフォレンジック分析の経験は必須ではありません。 |
| あると望ましい経験・スキル | - C/C++ などによるシステムプログラミングの経験がある方<br>- マルウェアに関連したインシデント対応や分析の経験がある方<br>- 技術的な勉強会などを主催している、または主催経験者<br>- コミュニティー活動などに参加している、または参加経験者<br>- 学会やカンファレンスなどで自身の技術的な成果の発表、講演の経験がある方<br>- 海外担当者と技術トピックスについて、会話によるコミュニケーション力がある方<br>- Twitterなどでセキュリティの最新情報を収集し、分析する経験<br><br>求める人物像：<br>- 高い探求心と強い倫理観をもって業務に当たれる方<br>- チームプレイができる方<br>- 主体的に問題解決に取り組める方<br>- 最新のIT技術に対して常に興味をもって自学習できる方 |

基本的な社会人スキルやITスキルは必要だが、実際のセキュリティの経験は不問
→自身のキャリアを積む中で、セキュリティへの志があったら見てみてください

# まとめ

- JPCERT/CCは「コーディネーションセンター」
  - インシデントの相談／報告を受領・調整、国内／海外組織との連携、情報の共有を行うことで、国内組織のインシデントの対応の支援をしている
  - 採用も実施中

日本の平和を守ることに
つながるお仕事をしている


JPCERT/CC
https://www.jpcert.or.jp/

# お問い合わせ、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：ew-info@jpcert.or.jp
- https://www.jpcert.or.jp/reference.html

## インシデント報告

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

## 脆弱性に関するお問い合わせ

- Email：vultures@jpcert.or.jp
- https://jvn.jp/

# ご清聴ありがとうございました