JPCERT CC®

サイバーセキュリティにおける脅威動向とJPCERT/CCの取り組み

一般社団法人JPCERTコーディネーションセンター
早期警戒グループ
脅威情報アナリスト
堀 充孝

アジェンダ

- JPCERT/CCの活動紹介
- 近年におけるサイバーセキュリティの動向と課題
- 直近の事案対応
- 制御システムセキュリティに関する取り組み
- おわりに

JPCERT/CCの紹介

一般社団法人JPCERTコーディネーションセンター
Japan Computer Emergency Response Team / Coordination Center

- コンピューターセキュリティインシデントへの対応、ソフトウェアや情報システム・制御システム機器などの脆弱性への対応など国内のセキュリティ向上を推進する活動を**中立機関**として実施
- 1995年から活動を実施。現在は経済産業省や内閣官房からの委託予算で活動
- 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などのセキュリティに関わる担当者
- 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に関する、**日本の窓口となる「CSIRT」**

※各国に同様の窓口CSIRTが存在する（米国のCISA（US-CERT）、韓国のKrCERT/CCなど）

- 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
- サイバーセキュリティ基本法上の「サイバーセキュリティに関する事象が発生した場合における国内外の関係者との連絡調整を行う関係機関」
- サイバーセキュリティ協議会（2019年発足）の事務局をNISCとともに実施（事案対応の相談や情報共有活用の運用面を担当）

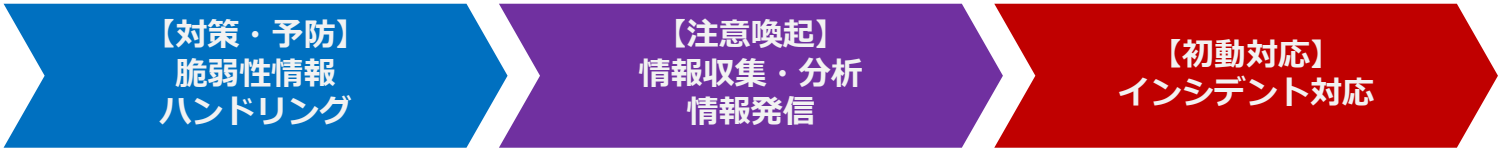
JPCERT/CCの果たす役割

- JPCERT/CC

  Japan Computer Emergency Response Team / Coordination Center

- 国内における“火消し”の役割

  ⇒「インシデントレスポンスチーム」



- 国際間・国内連携における“窓口”の役割

  ⇒「コーディネーションセンター（CC）」

JPCERT/CCの活動（1）

■ 消防と同じで、予防活動⇒注意喚起⇒火災対応を行っている

消防活動の場合

火災予防

火災予防のための方法を周知

注意喚起

火災予防運動や
火災多発時の注意喚起

火災対応

火災発生時の消火活動
救命活動

JPCERT/CCの活動

脆弱性調整

脆弱性対策方法の公表

分析・情報発信

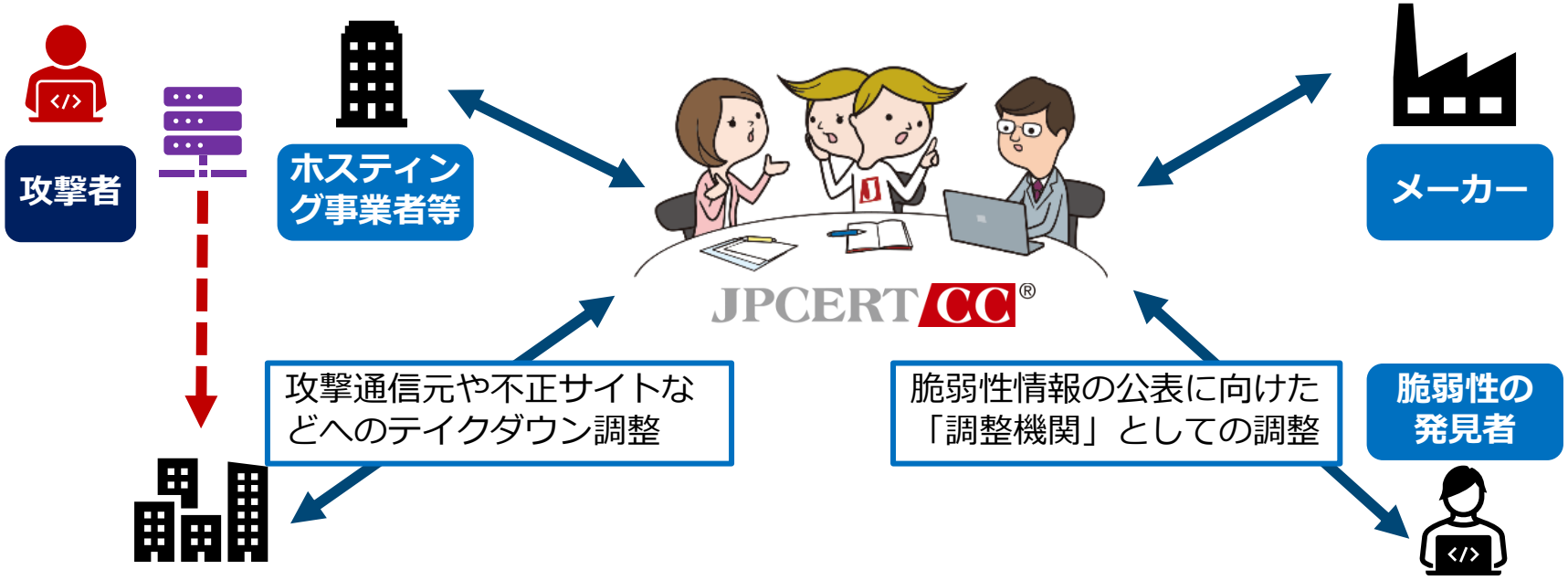
攻撃活動の観測や分析
情報発信

インシデント対応

被害発生時の対応支援

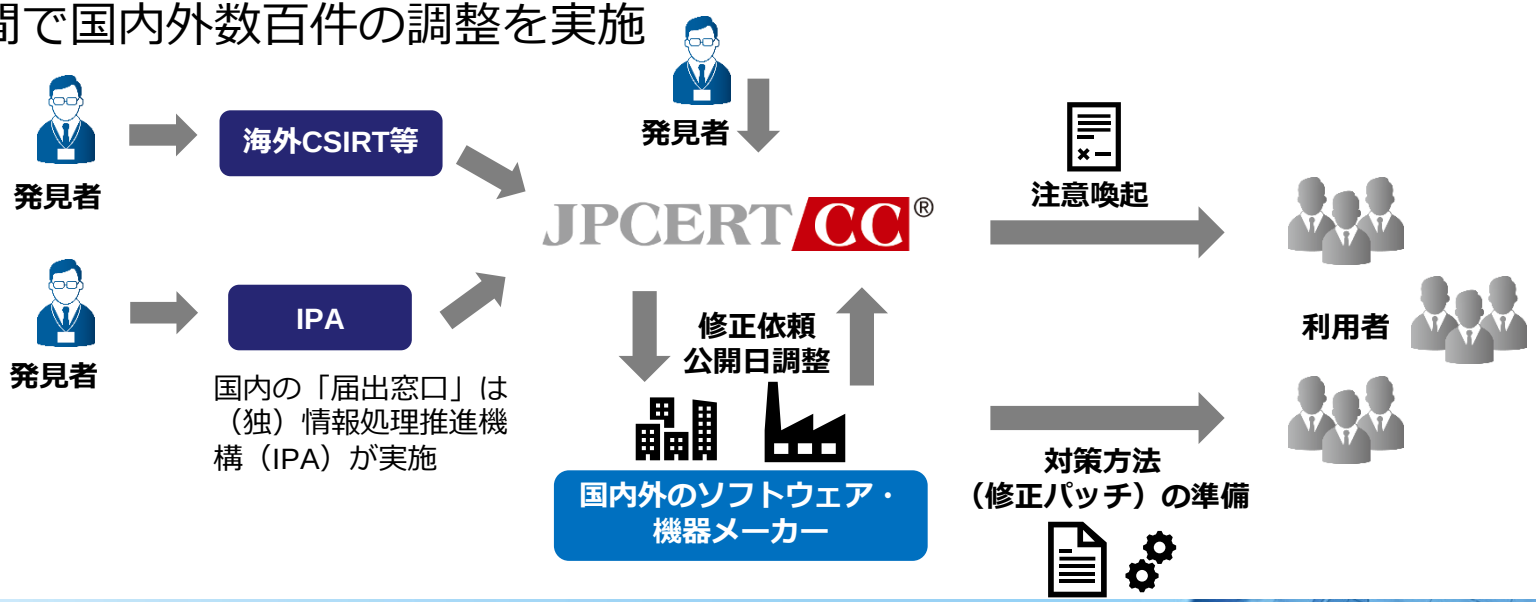
JPCERT/CCの活動（2）

- コーディネーションセンターとして
  国内外のさまざまなパートナーとの調整により事案の解決を目指す



連携活動の例: 脆弱性情報の流通

- 経済産業省告示等に基づく脆弱性情報ハンドリングの制度における「調整機関」を担う
- 発見された脆弱性についてメーカーと調整を行い、「対策の準備」と「対策周知のための公表」を関係者間で準備する。
- 年間で国内外数百件の調整を実施



JVN（Japan Vulnerability Notes）

公開日：2016/04/27　最終更新日：2016/04/27

JVNVU#91375252
Apache Struts2 に任意のコード実行の脆弱性

概要
Apache Struts2 には、任意のコードを実行可能な脆弱性が存在します。

影響を受けるシステム
- Struts 2.3.20 から 2.3.28 まで (Struts 2.3.20.3 および Struts 2.3.24.3 を除く)

詳細情報
Apache Struts2 には、Dynamic Method Invocation を有効にしている場合、任意のコードを実行可能な脆弱性が存在します。

なお、本脆弱性を使用した proof-of-concept コードが公開されています。

想定される影響
遠隔の第三者によって、当該製品が動作しているサーバ上で任意のコードを実行される可能性があります。

対策方法
アップデートする
開発者が提供する情報をもとに、最新版へアップデートしてください。
本脆弱性は Apache Struts 2.3.20.3、2.3.24.3、2.3.28.1 で修正されています。

国内外の脆弱性について記載
- JPCERT/CCで調整、公表
- CERT/CC VU翻訳
- etc.

- 開発ベンダーに修正パッチなどの作成を依頼
- CVEの採番
- 脆弱性公表日などの調整

情報セキュリティ早期警戒パートナーシップ

脆弱性発見者 → **届出** → IPA (受付機関) → **通知** → JPCERT/CC (調整機関)

JPCERT/CC (調整機関) → ユーザー

関係者合意の元 JVN 発行

JPCERT/CC (調整機関) → 海外の調整機関やPSIRTなど

通知

ICSを対象とするSIRT構築の課題に共同で取り組むコミュニティー

■ 製造業のICSセキュリティ担当者コミュニティーを形成して推進

コミュニティー概要（JPCERT/CC主催）

20
組織以上
（発表時点）

複数業種
機器製造・化学鉄鋼・製薬
光学・食品 等

ICS セキュリティ 担当者

■ **次の点を主なモチベーションとして活動してきた**

- ICSセキュリティの共通課題をともに考える
- 実務者ベースでの実践的な検討を行う
- JPCERT/CCの知見を共有し実務的な協力関係強化
- 個々でなく協力することで攻撃者への対抗力を醸成
- 「ICSを対象とするSIRT」の適切な構築を後押し

取り組み例

➢ 取り組み例：

実績：

- ✓ ICSにおけるセキュリティアセスメントについて
- ✓ 近年のICS関連インシデントにみるマルウェアの傾向と対策

直近：

- ✓ **サイバー要因を想定すべきICS特有事象の検討**
- ✓ **ICSを対象とするインシデント対応体制に関する要件の検討**

JPCERT/CCの活用

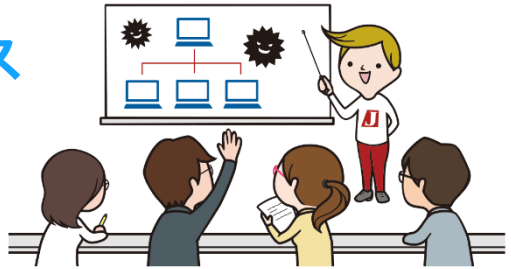
■ コーディネーションセンターの役割と活用

- インシデントレスポンス
- 脆弱性・脅威情報に関する情報流通
  - 脆弱性情報　【JVN】
  - 脅威情報、注意喚起、早期警戒情報他
- アーティファクト分析【検体解析など】
- 国内外 のxSIRT 連携促進、コミュニティー推進

“インシデント”
に向き合った活動を展開
しています

■ 例えば、こんなときにお役立てください

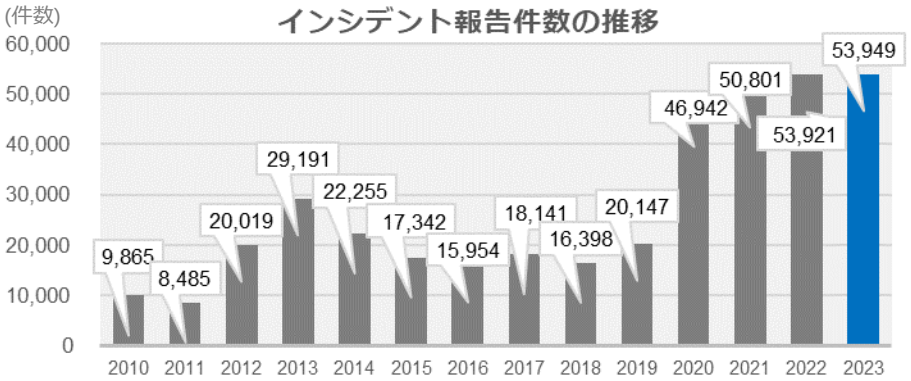
- インシデントが発生し、
  初動対応での技術的な支援や情報が必要となるケース
- 日々の対策を進める上で、
  脆弱性や脅威に関する情報が必要となるケース
- その他、お気軽にご相談ください



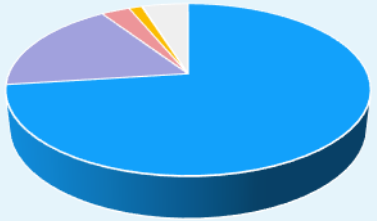
近年における
サイバーセキュリティの動向と課題

インシデント対応状況（2023年1月～2023年12月）

- JPCERT/CCへの報告
  - 全報告件数
    65,669件
  - 全インシデント件数
    28,735件
- JPCERT/CCからの連絡
  - 全調整件数
    19,444件



インシデント件数のカテゴリ別割合

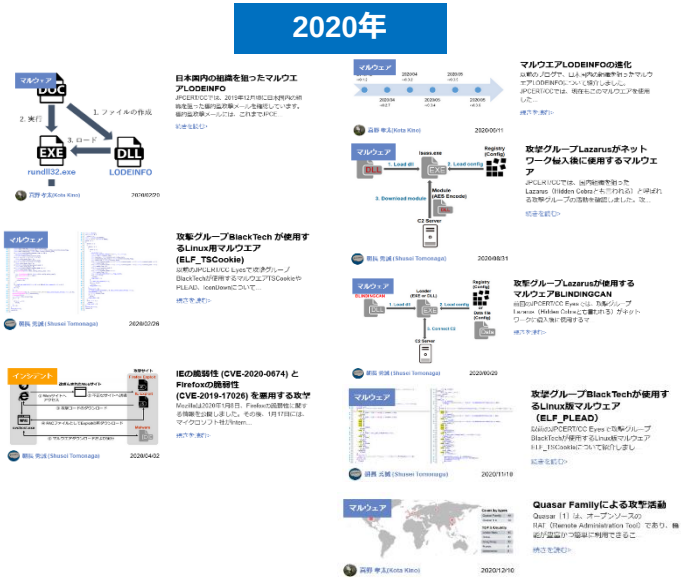


カテゴリ	割合
フィッシングサイト	72.96%
スキャン	17.71%
Webサイト改ざん	3.02%
マルウエアサイト	1.37%
DoS / DDoS	0.07%
標的型攻撃	0.03%
その他	4.82%

「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

標的型サイバー攻撃の傾向

- BlackTech（2019年～2022年）
- LODEINFO（2020年～）
- Lazarus：OpDreamJob（2020年～）、DangerousPassword（2019年～）
  Stonefly（2020年～）



初期侵害経路となる脆弱性公表／注意喚起の増加

2019年
・Pulse Connect Secure（CVE-2019-11510）
・Fortigate（CVE-2018-13379）

2020年
・Citrix（CVE-2019-19781）
・BIG-IP（CVE-2020-5902）
・Trend Micro製品の複数の脆弱性

2021年
・Filezen（CVE-2021-20655）
・SonicWall（CVE-2021-20016）
・Proxyshell（Exchange Serverの複数の脆弱性）
・Trend Micro 製品の脆弱性（CVE-2020-24557等）
・Pulse Connect Secure（CVE-2021-22893）
（・Confluence脆弱性（CVE-2021-26084））
（・ManageEngine ADSelfService Plusの脆弱性（CVE-2021-40539））
（・Vmware Horizon Log4j脆弱性）

※括弧付は国内で注意喚起が発行されなかったもの

2022年
・Sonicwall SMA100シリーズの複数の脆弱性
・BIG-IP（CVE-2022-1388）
・Trend Micro Apex Central製品の脆弱性（CVE-2022-26871）
・FortiOS等の脆弱性（CVE-2022-40684）
・FortiOS（CVE-2022-42475）

2023年
（・MOVEit File Transferの複数の脆弱性）
・Citrix ADCおよびCitrix Gatewayの脆弱性（CVE-2023-3519）
・Proself の複数の脆弱性（CVE-2023-39415等）
・FortiOS等の脆弱性（CVE-2023-27997）
（・Ivanti Endpoint Manager Mobileの複数の脆弱性）
・BarracudaESG（CVE-2023-2868）
・Citrix ADCおよびCitrix Gatewayの脆弱性（CVE-2023-3519）
・Array Networks Array AGシリーズの脆弱性
・ProselfのXML外部実体参照（XXE）に関する脆弱性
・Cisco IOS XEのWeb UIにおける権限昇格の脆弱性（CVE-2023-20198）

初期侵害経路となる脆弱性公表／注意喚起の増加

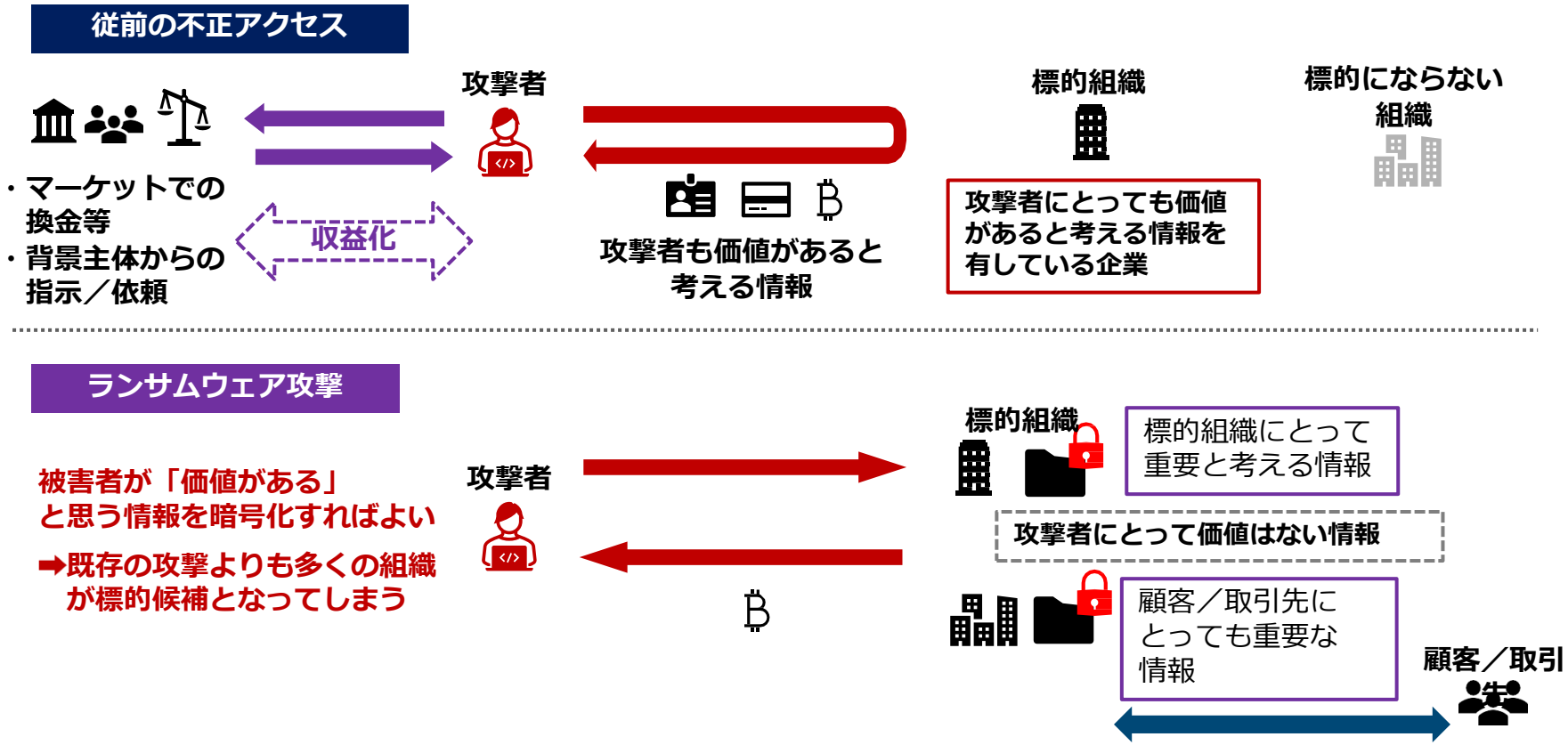
- 標的型サイバー攻撃や侵入型ランサムウェア攻撃の初期侵入経路（Attack Vector／Initial access）として悪用される脆弱性が多く見つかった3年間
- メール経由で侵入を試みる標的型サイバー攻撃も引き続き存在する状況において、特に侵入型ランサムウェア攻撃を中心にインターネットに接続したソフトウェア製品の脆弱性を突く攻撃が相次ぐ
- 他方で、Emotetのテイクダウン（※その後断続的に活動再開）、Trickbotの活動停止など、マルウェアディストリビューターが拡散させるマルウェア経由での侵害事案は想定的に減ったのではないかと推測

初期侵害経路となる脆弱性公表／注意喚起の増加

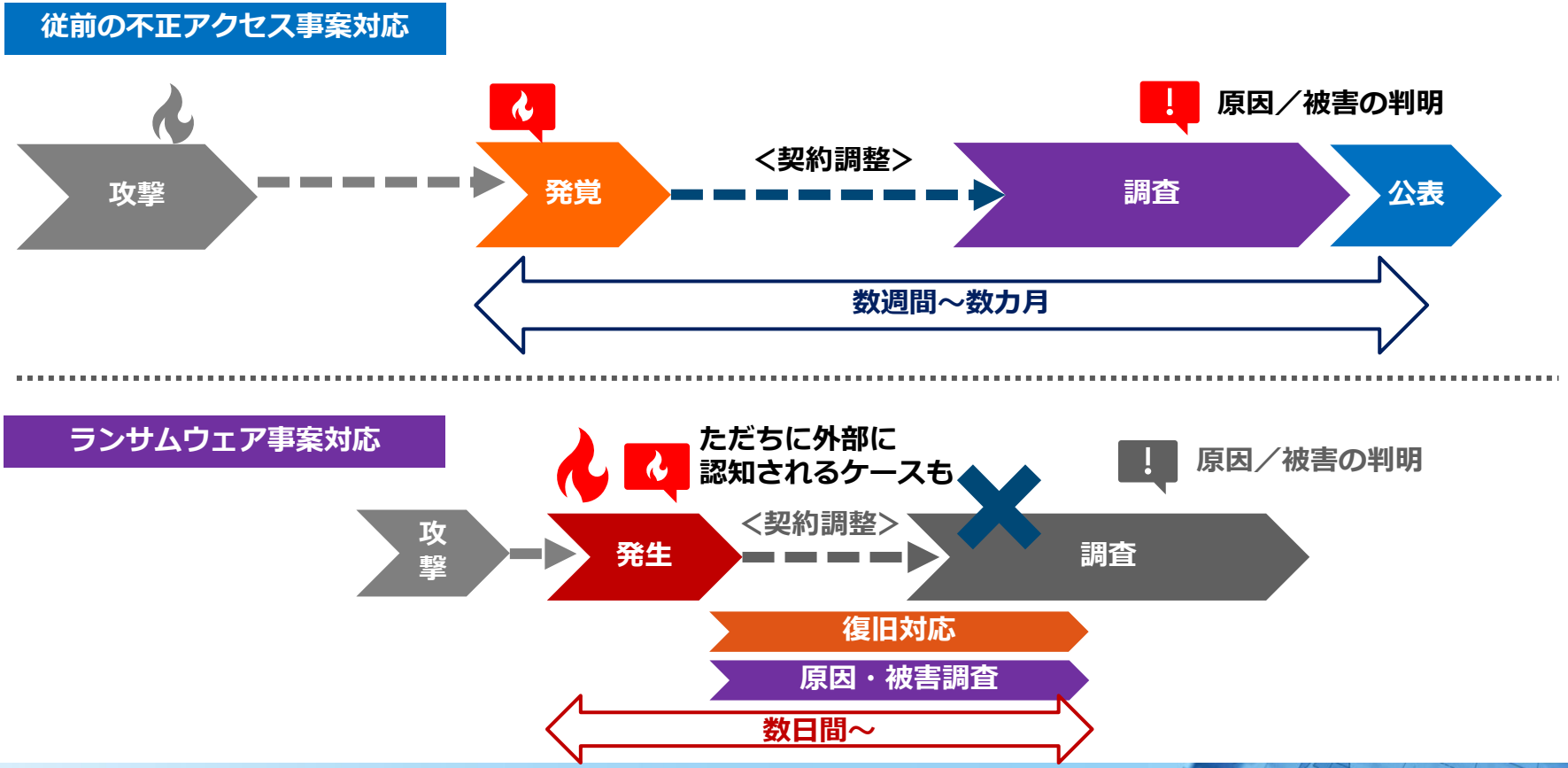
＜傾向＞

- ランサムアクターによるゼロデイ攻撃での悪用
- 特定製品分野でクリティカルな脆弱性が度々見つかる＆悪用される
  （例：SSL-VPN製品、オンラインストレージ）
- 特定製品で度々クリティカルな脆弱性が見つかる＆悪用される
  （例：Fortigate、Sonicwall、Proself）

ランサムウェア攻撃、何が脅威なのか①：標的層の拡大



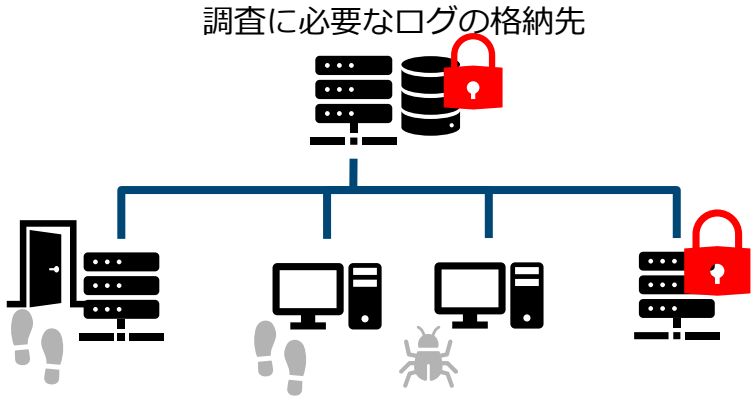
ランサムウェア攻撃、何が脅威なのか②：時間的余裕のなさ



ランサムウェア攻撃、何が脅威なのか③：調査の難しさ

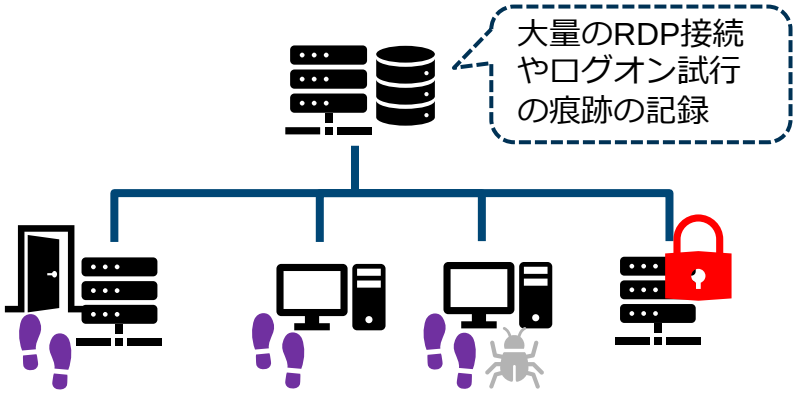
調査に必要なログデータが棄損している場合

- 業務データだけでなく、ADやアンチウイルス製品の各種ログデータも暗号化被害を受けるケース
- 調査に必要なデータも棄損しており、侵害範囲や侵害経路を特定できないため、必要ない端末入れ替えやフォレンジック調査が発生してしまう



復旧のために詳細な侵害範囲調査ができない

- ”フラット”過ぎるNW設計／設定や、管理権限設定の不備により、攻撃者が派手にNW内で移動した痕跡が残っているケース
- 侵害疑義のある端末をすべて安全確認する余裕はないため、端末入れ替えを判断してしまう場合がある



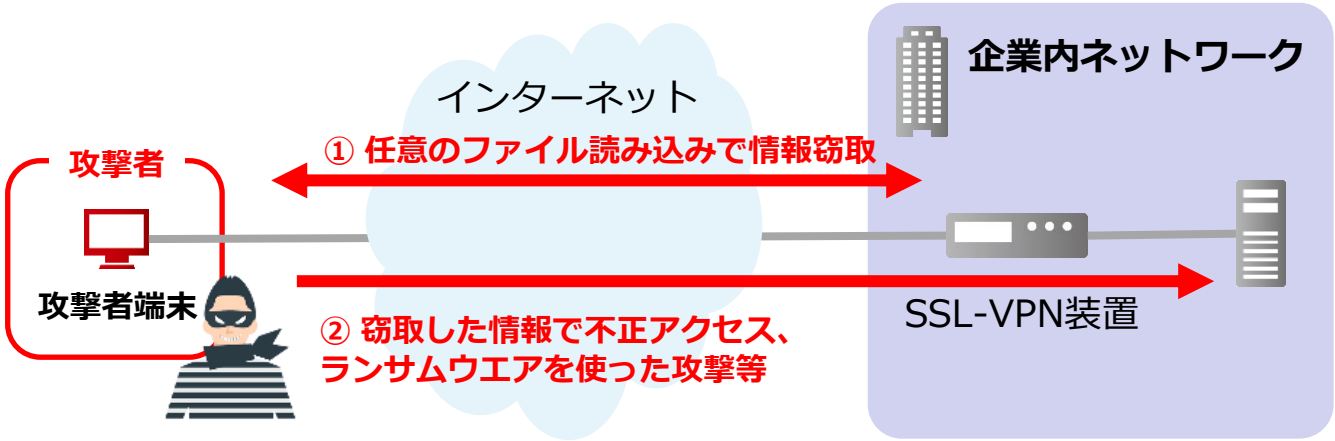
ログオン試行などの痕跡
➡すべて調査している時間的余裕はない

Pulse Connect Secure の脆弱性

■ 任意のファイル読み込みの脆弱性 (CVE-2019-11510)

① 攻撃者が、SSL-VPN装置の任意のファイルを窃取
- パスワード等

② 窃取した情報をもとに不正アクセス、更なる攻撃



Pulse Connect Secure の脆弱性 -時系列1-

■ 脆弱性情報の公開から悪用に至るまで

脆弱性情報の公開		
2019/03/22	DEVCORE	脆弱性を Pulse Secure 社 PSIRT へ報告
2019/04/24	Pulse Secure	脆弱性を修正したバージョンを公開
脆弱性の実証コード/悪用ツールが公開され始める		
2019/08/04	DEVCORE	脆弱性の詳細や悪用方法などについての紹介
2019/08/21	GitHub	脆弱性の攻撃コード／ツールが公開
		この頃から、脆弱性を探索する通信を観測
2019/08/24	Bad Packets	脆弱性 (11510) が残っているホストの数などを公開
2019/09/02	JPCERT/CC	脆弱性の注意喚起
脆弱性を悪用した攻撃が観測され始める		
	JPCERT/CC	同日、脆弱性を悪用した攻撃を確認
2019/09	金融機関	脆弱性を悪用されたとみられる攻撃の被害(金融機関)
2019/10	NSA, CISA等	米国 NSA、CISA、英国NCSC 等の注意喚起
2020/01	通貨交換所	脆弱性を悪用され、ランサム Sodinokibi 感染の被害

Pulse Secure

black hat USA 2019

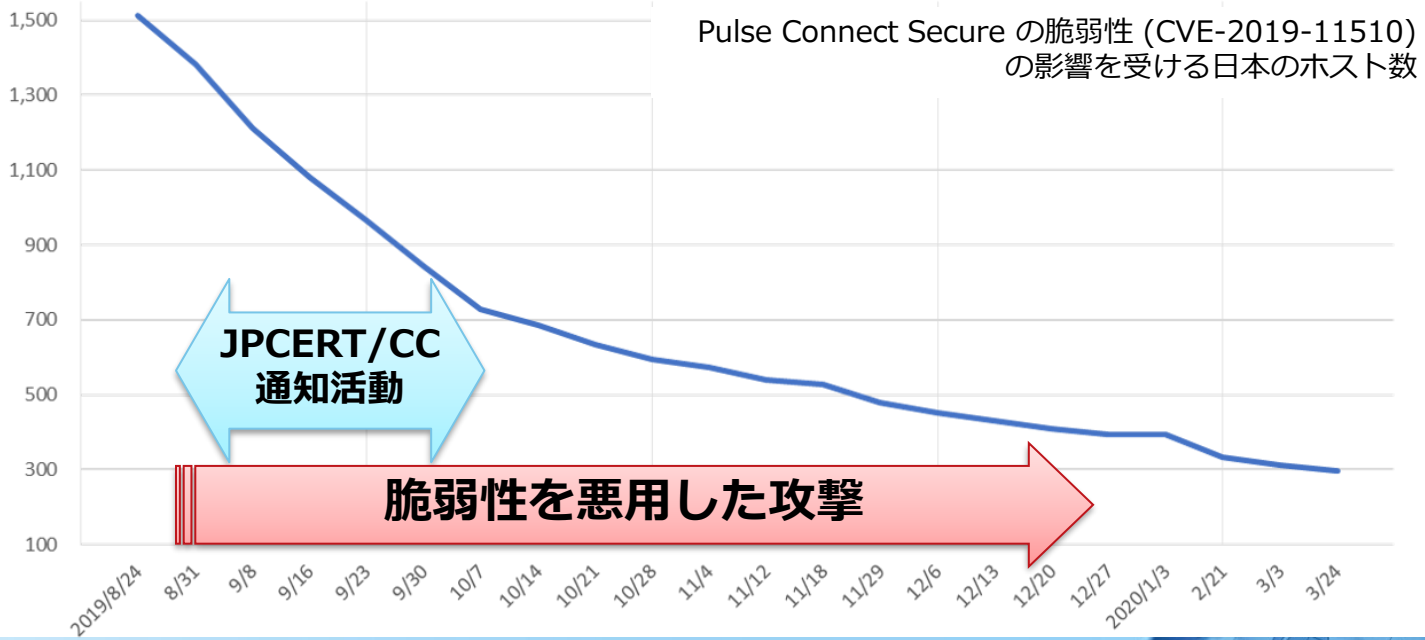
BAD PACKETS

Country	Count of Vulnerable Hosts
United States	5,010
Japan	1,511
United Kingdom	830
Germany	789
France	626
Netherlands	420
Israel	406
Switzerland	307
Canada	296
South Korea	281
All Other Countries	4,052

Pulse Connect Secure の脆弱性 -時系列2-

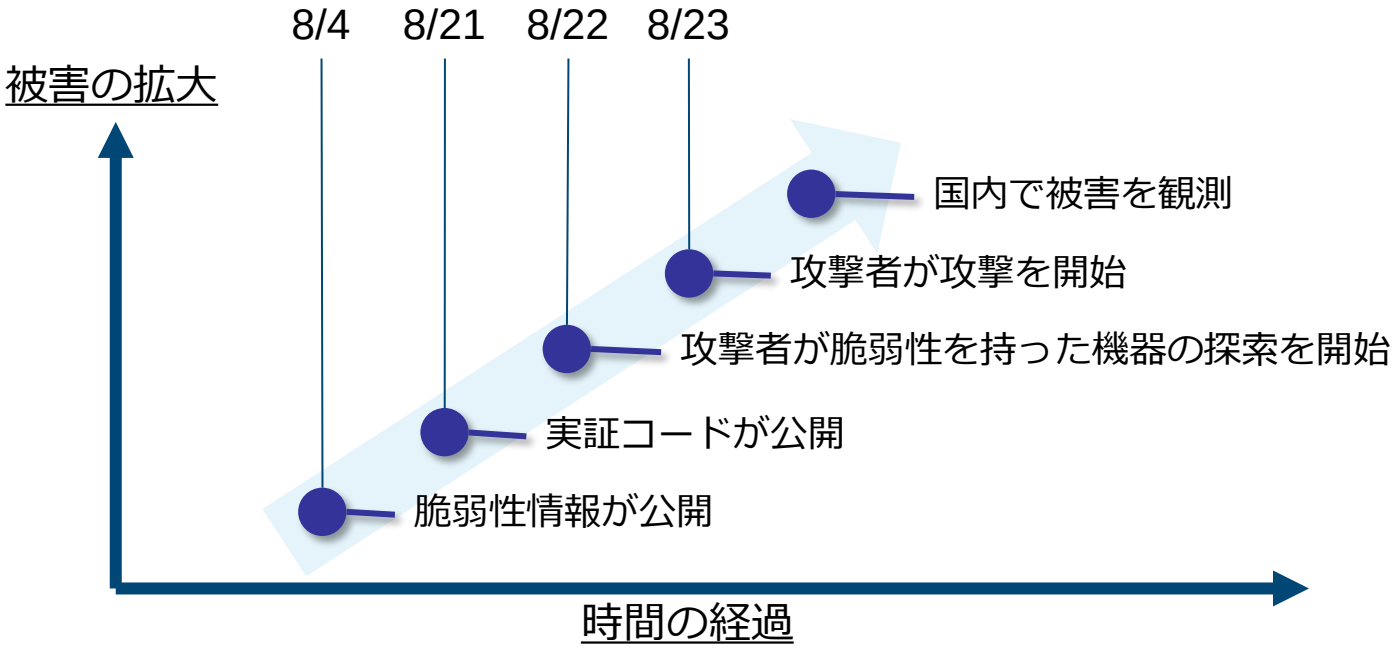
■ 脆弱な機器は長期間にわたり国内に残存

- 2019年9月より JPCERT/CCから脆弱性のある機器の管理者へ通知
- 2020年3月末時点でも約300台が脆弱なまま

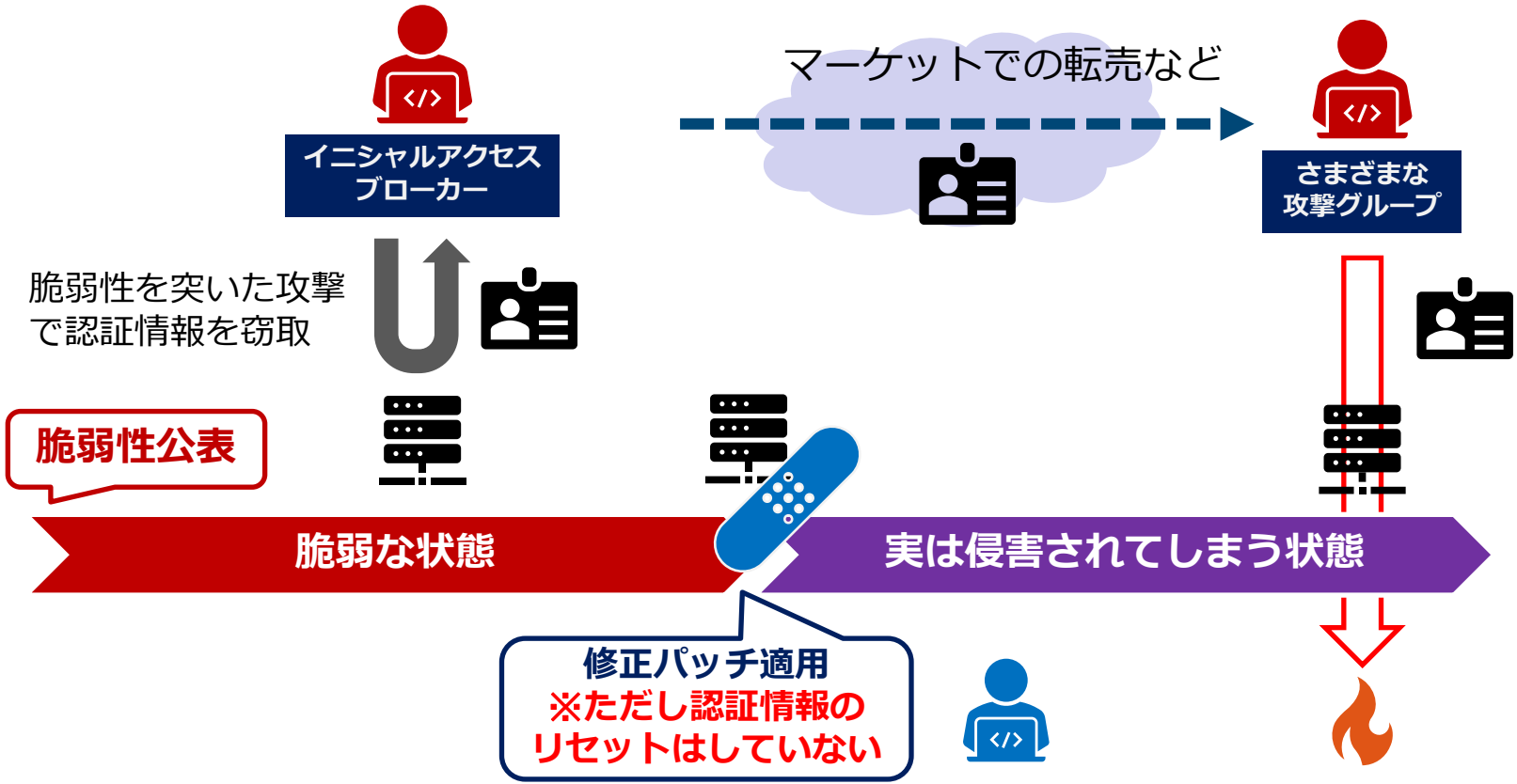


脆弱性対応の時間的制約について

- **脆弱性情報の公開後、3週間程度で攻撃を観測**
  - 実証コードが公開されてからは早い

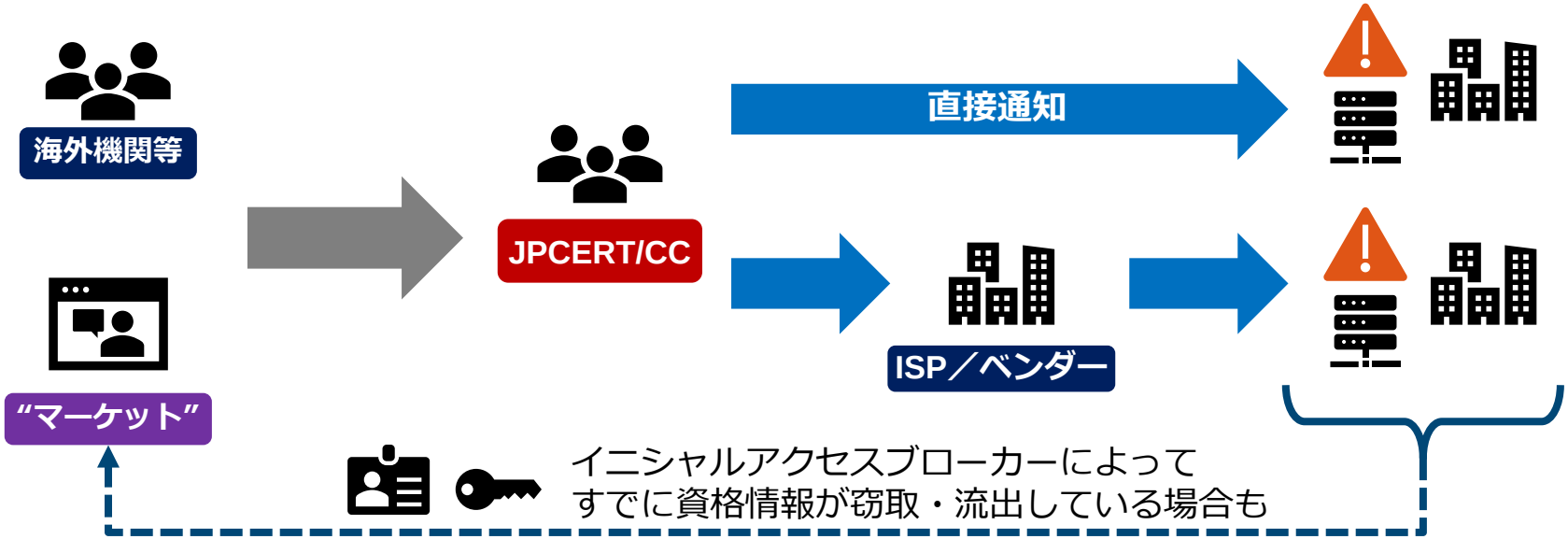


修正パッチの適用だけでは対応が不十分なケースも



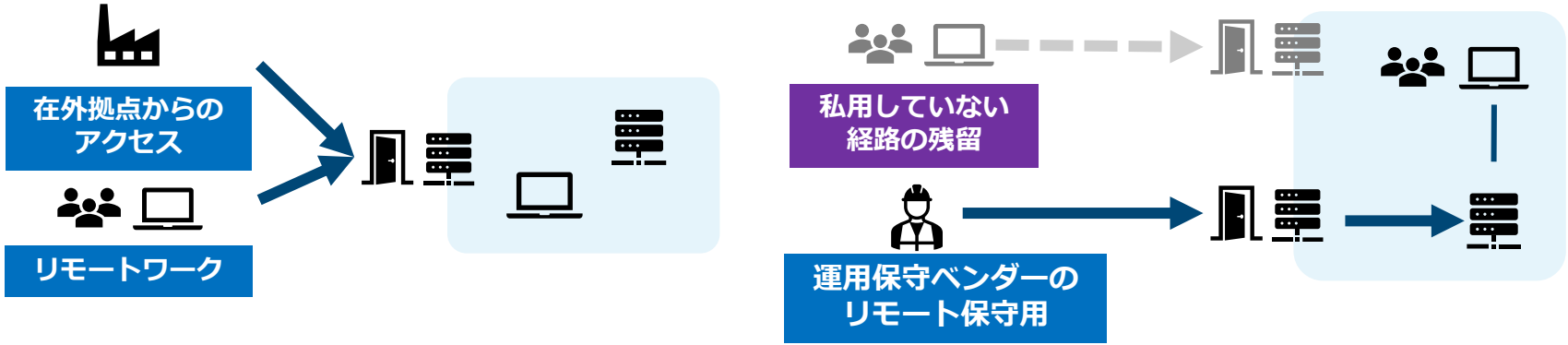
JPCERT/CCによる通知オペレーション

- 脆弱なままのSSL-VPN機器や、すでに脆弱性の悪用により認証情報が窃取されているSSL-VPN機器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が多発

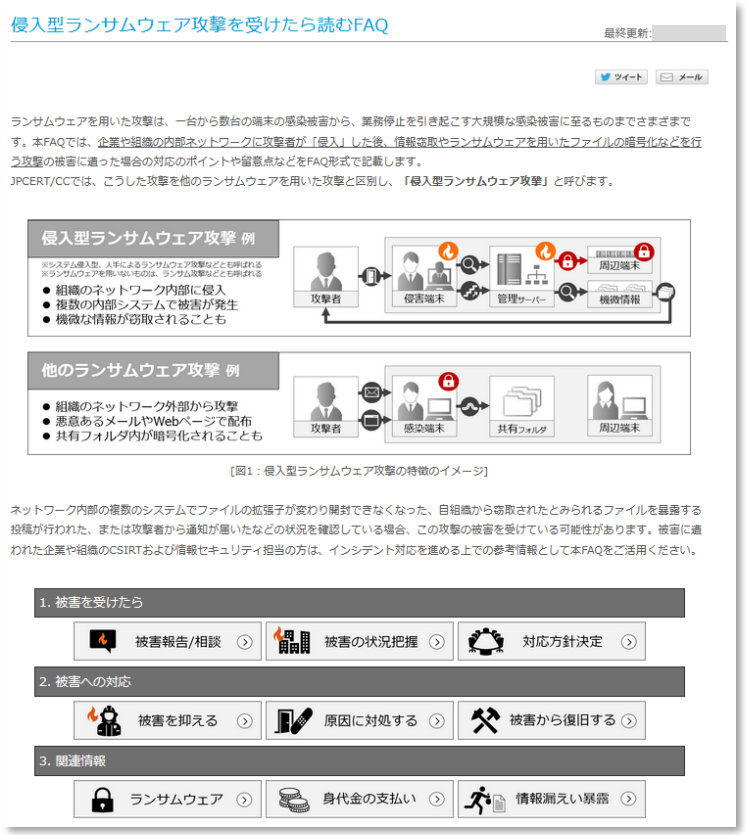


リモートアクセス経路のチェック

- そもそも自組織に外部からアクセスする経路はいくつあるのか？
- 当該機器の脆弱性は誰が対応することになっているのか？
- 侵害されたとき／その恐れがあるときに、ログのチェックなどができるのか？
- 「過去のSSL-VPN製品の脆弱性が悪用され侵害されるケースが相次いでいる」という情報をすでに多くの関係者が知っている状況



侵入型ランサムウェア攻撃被害の初動対応FAQ



（1）コンテンツ内容

- 攻撃を受けた場合の対応のポイントや留意点、よくある質問をFAQ形式を掲載（html形式）
- 攻撃を受けた後の対応に特化したコンテンツ

（2）コンテンツ想定読者

- 被害組織のCSIRT／情報セキュリティ担当
- 被害組織を支援するセキュリティベンダー会社
- 被害組織の支援や捜査にあたる都道府県警　　など

（3）コンテンツ構成

1. 被害を受けたら：被害報告/相談、状況把握、対応方針決定
2. 被害への対応　：被害最小化、原因対処、被害復旧
3. 関連情報　　：ランサムウェア、身代金支払い、情報漏えい調査

（4）コンテンツの期待効果

- 攻撃の全体像や侵害原因を速やかに特定
- 不必要なNW停止などを最小限に留めて対応
- 専門機関等へ速やかに報告・連絡

JPCERT/CC 「侵入型ランサムウェア攻撃を受けたら読むFAQ」より
https://www.jpcert.or.jp/magazine/security/ransom-faq.html

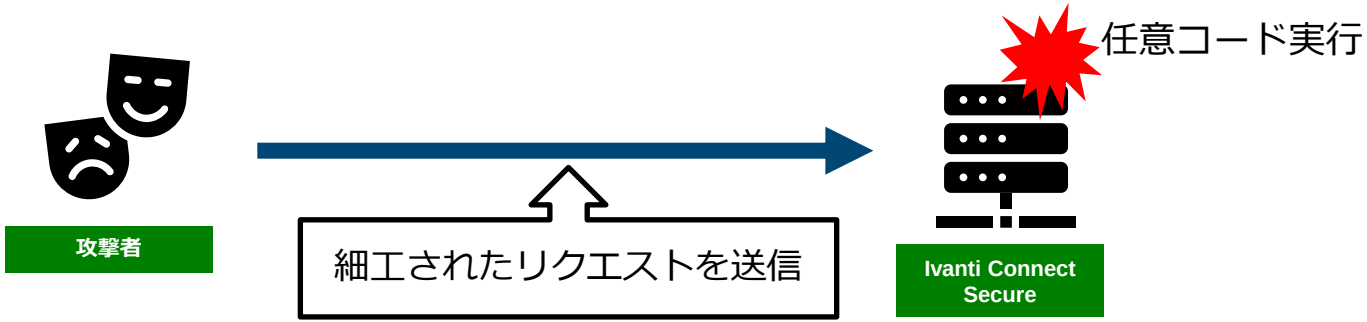
直近の対応事案について

Ivanti Connect Secure、Ivanti Policy Secure Gatewayの脆弱性について

- **CVE-2023-46805、CVE-2024-21887**
- **CVE-2024-21888、CVE-2024-21893**
- **CVE-2024-22024**

脆弱性（CVE-2023-46805、CVE-2024-21887）の概要

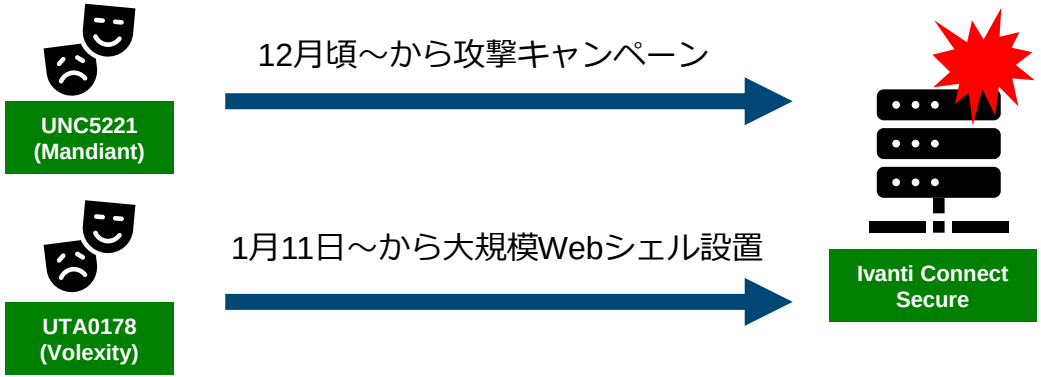
- 本製品はリモートアクセス環境を提供するVPN製品
- 2024年1月10日にIvanti社がアドバイザリを公表
- 認証回避およびコマンドインジェクションの脆弱性



出典元：ivanti「CVE-2023-46805 (Authentication Bypass) & CVE-2024-21887 (Command Injection) for Ivanti Connect Secure and Ivanti Policy Secure Gateways」
https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US

脆弱性（CVE-2023-46805、CVE-2024-21887）の悪用状況

- 限定的な攻撃での悪用（2024年1月10日ナレッジベース記事）
  - Ivanti社のナレッジベースにて攻撃の悪用情報がアドバイザリとあわせて公開
  - アドバイザリ公開以前からの攻撃とアドバイザリ公開直後において本脆弱性を悪用するインシデントの分析記事をセキュリティ企業が公開
    - https://www.volexity.com/blog/2024/01/10/active-exploitation-of-two-zero-day-vulnerabilities-in-ivanti-connect-secure-vpn/
    - https://www.mandiant.com/resources/blog/suspected-apt-targets-ivanti-zero-day

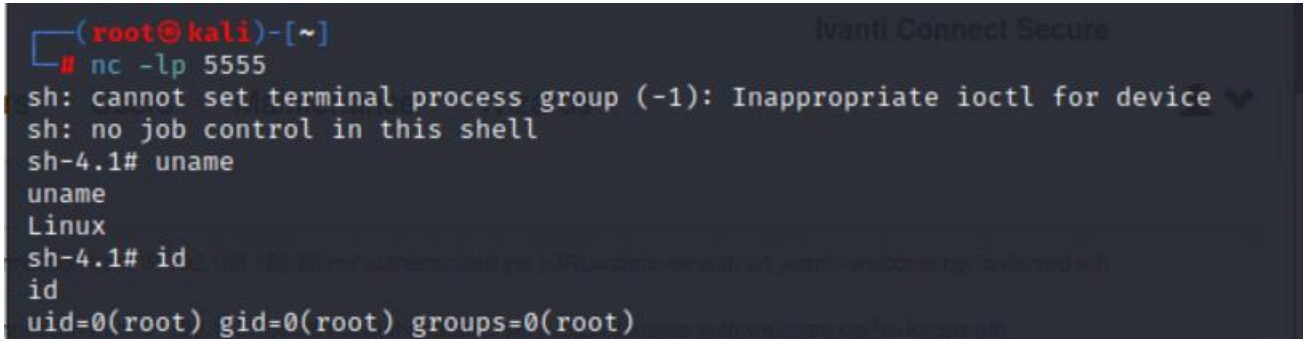


脆弱性（CVE-2023-46805、CVE-2024-21887）の悪用状況

- 国内組織での観測
  - JPCERT/CCでも国内組織に対する被害を観測
    - 対象組織には個別で通知を実施、注意喚起の公開
  - 1月11日の広範囲なWebshell設置は国内でも観測
    - Volexity社によるUTA0188として追跡しているアクターの活動
      - https://www.volexity.com/blog/2024/01/15/ivanti-connect-secure-vpn-exploitation-goes-global/
  - PoCが公開されたため、アクター以外による攻撃活動が開始

脆弱性（CVE-2023-46805、CVE-2024-21887）の悪用状況

- PoCコードおよび解説記事の公開
  - Rapid7社、Assetnote社などによって本脆弱性の解説記事が公開
    - https://attackerkb.com/topics/AdUh6by52K/cve-2023-46805/rapid7-analysis
    - https://www.assetnote.io/resources/research/high-signal-detection-and-exploitation-of-ivantis-pulse-connect-secure-auth-bypass-rce
  - JPCERT/CCでも悪用可能であると確認

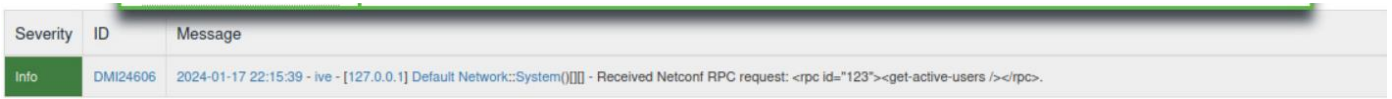


脆弱性（CVE-2023-46805、CVE-2024-21887）の悪用検知

- 侵害検出方法
  - 内部の整合性チェックツール（Integrity Checker Tool）を実行後、外部整合性チェッカーを実行
    - 正規のコンポーネントが改ざんされ、内部の整合性チェックツールを回避する事例、ログが削除される事例が観測
      - https://www.volexity.com/blog/2024/01/18/ivanti-connect-secure-vpn-exploitation-new-observations/

脆弱性（CVE-2023-46805、CVE-2024-21887）の悪用検知

- ログ確認
  - JPCERT/CCでの検証
    - APIを実行された場合(※出力されない場合あり)



Severity	ID	Message
Info	DMI24606	2024-01-17 22:15:39 - ive - [127.0.0.1] Default Network::System()[][] - Received Netconf RPC request: <rpc id="123"><get-active-users /></rpc>.

    - ログを削除された場合(※削除後イベントが発生すると消える)

Severity	ID	Message
Info		Log file is empty or filtering returned no messages

対策、回避策

アップデート

- 2024年1月31日
  - Ivanti Connect Secure バージョン 9.1R14.4、9.1R17.2、9.1R18.3、22.4R2.2、および 22.5R1.1 および ZTA バージョン 22.6R1に対して公開
- 2024年2月1日
  - Ivanti Connect Secure バージョン 22.5R2.2 および Ivanti Policy Secure 22.5R1.1に対して公開

回避策

- ダウンロードポータルよりmitigation.release.20240126.5.xmlをダウンロードし、製品に適用する

※回避策ファイルは1月11日公開のものから差し替えがあり更新が必要

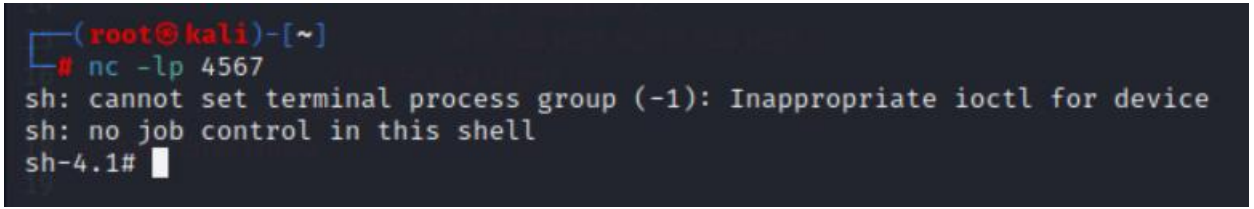
1/31公開の脆弱性（CVE-2024-21888、CVE-2024-21893）

- 脆弱性の概要
  - 2024年1月31日にIvantiよりアドバイザリが公開
    - 権限昇格の脆弱性(CVE-2024-21888)とサーバーサイドリクエストフォージェリ（SSRF）の脆弱性（CVE-2024-21893）
      - https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure
    - Mandiant社による攻撃のレポートも公開
      - https://www.mandiant.com/resources/blog/investigating-ivanti-zero-day-exploitation

- 脆弱性情報の公開
  - Rapid7社等によって脆弱性の詳細が公開
    - https://attackerkb.com/topics/FGlK1TVnB2/cve-2024-21893/rapid7-analysis

1/31公開の脆弱性（CVE-2024-21888、CVE-2024-21893）

- 脆弱性の検証
  - JPCERT/CCでも該当記事より脆弱性が発露できると確認
  - 別ルートにてCVE-2023-46805およびCVE-2024-21887にアクセス可能となっているため同じく任意コード実行が可能



- 対策
  - アップデートを適用する
  - XMLファイルのパッチを適用する

2/8公開の脆弱性（CVE-2024-22024）

- 脆弱性の概要
  - 2024年2月8日にIvantiよりアドバイザリが公開
    - XML外部実体参照（XXE）（CVE-2024-22024）の脆弱性
      - https://forums.ivanti.com/s/article/CVE-2024-22024-XXE-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure
    - watchTowrよる脆弱性の分析レポートも公表されている
      - https://labs.watchtowr.com/are-we-now-part-of-ivanti/
    - 公開時点で本脆弱性を悪用した攻撃に関する情報はなし

- 1/31、2/1にリリースされたパッチを適用している製品のみ影響

2/16時点の回避策・対策の提供状況

CVE ID	1/10回避策	1/31回避策	1/31・2/1パッチ	2/8パッチ
CVE-2023-46805	対策済	対策済	対策済	対策済
CVE-2024-21887	対策済	対策済	対策済	対策済
CVE-2024-21888	影響あり	対策済	対策済	対策済
CVE-2024-21893	影響あり	対策済	対策済	対策済
CVE-2024-22024	影響なし	対策済	影響あり	対策済

- 本件に関する最新の情報については、JPCERT/CCの注意喚起やCyberNewsFlashをご確認いただき、対策実施をご検討ください
  - https://www.jpcert.or.jp/at/2024/at240002.html
  - https://www.jpcert.or.jp/newsflash/2024021601.html

制御システムセキュリティに関する直近の活動

・制御システムセキュリティカンファレンス 2024について

制御システムセキュリティカンファレンス 2024の開催

- **制御システムセキュリティに関する各種講演等を提供**
  - 経済産業省＆JPCERT/CCで共催
  - ICSセキュリティの技術的な情報提供
  - 2021年2月の実施よりオンライン開催
  - プログラム構成の主な特徴
    - さまざまな業種でのICSセキュリティの取り組みを紹介
    - ICSユーザーの対策に資する講演
    - ICSセキュリティの国際的な動向の紹介

※特定企業のサービスや、製品等の宣伝に資する内容を除く、国内のICSステークホルダーにおけるICSセキュリティ向上を目的とした企画を心掛けている

講演資料のダウンロードはこちら
https://www.jpcert.or.jp/event/ics-conference2024.html

講演プログラム

No	講演タイトル	講演者
1	制御システムセキュリティの現在と展望 ～この1年間を振り返って～	JPCERT/CC 技術顧問 宮地 利雄
2	インダストリー4.0時代のCNC機械に潜む サイバーセキュリティリスク	トレンドマイクロ株式会社 セキュリティエバンジェリスト 岡本 勝之 氏
3	攻撃者視点からみたOT環境の通信監視 スモールスタートから始めてみよう	株式会社サイバーディフェンス研究所 技術統括部　OTセキュリティグループ プリンシパルコンサルタント 安井 康二 氏
4	制御システムの脆弱性管理の課題と グローバルにおける事例	Claroty Ltd. Solution Engineer 加藤 俊介 氏
5	ICSセキュリティポリシーの現場への浸透 および具体化に関する支援検討	参天製薬株式会社 Digital & IT本部 / Global Cybersecurity Manager 正木 文統 氏 JPCERT/CC 制御システムセキュリティ対策G 堀 充孝
6	ICS関連のセキュリティインシデント対応に備えて - 製造業を例に対応体制の整備上の課題と対策の第一歩を解説 -	JPCERT/CC 制御システムセキュリティ対策G マネージャー 河野 一之
7	製造業10社の実務者で議論した、制御系SIRTが 日常で取り組みたいインシデント対応訓練	株式会社資生堂 情報セキュリティ部 大林 世昇 氏 積水化学工業株式会社 高機能プラスチックスカンパニー デジタル変革推進部 係長 柴田 卓也 氏 パナソニック オートモーティブシステムズ株式会社 開発本部 プラットフォーム開発センター セキュリティ開発部 主任技師 越智 直紀 氏

各講演のハイライト

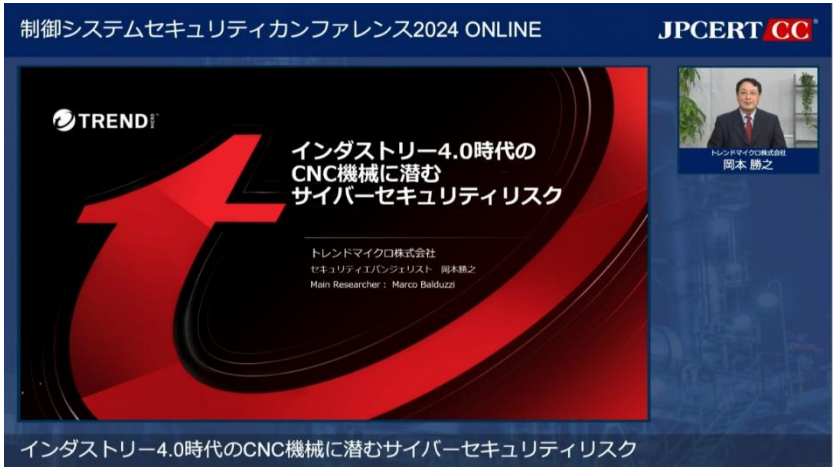
制御システムセキュリティの現在と展望 ～この1年間を振り返って～

- 2023年のOTセキュリティに関するできごとを次の観点で振り返り
  - ランサムウェアに関連したインシデントの動向
  - 戦争に関連したインシデントの動向
  - その他のサイバーインシデント
  - 脆弱性の動向
  - 標準の整備と規制の強化
  - 新しい技術を採用して変貌するICSのセキュリティ

各講演のハイライト

インダストリー4.0時代のCNC機械に潜むサイバーセキュリティリスク

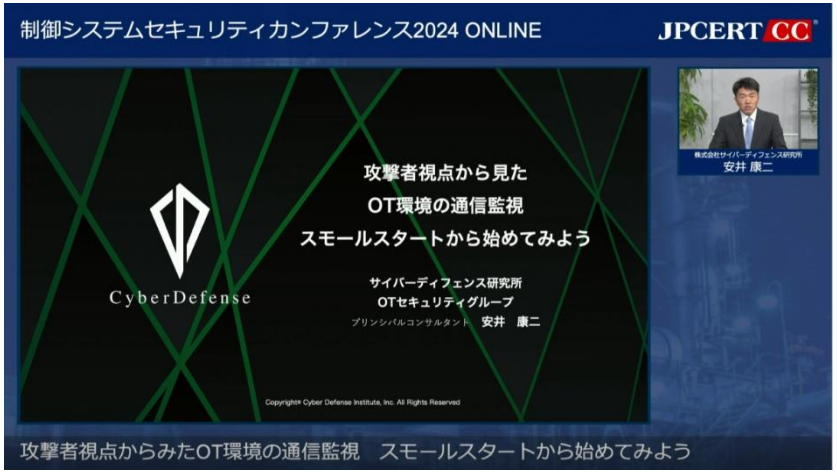
- ネットワーク接続されるCNC機械のセキュリティリスクについて検証
  - 国内ベンダーを含む4社の製品が対象
  - 4社すべてのコントローラーで遠隔での攻撃が可能
    - 工具の情報を改ざんして制作物を失敗させる、工具自体を損傷させる
    - コントローラーをランサムウェアに感染させる
    - コントローラーを乗っ取る　など
  - 本件に関する脆弱性情報は公表済み



各講演のハイライト

攻撃者視点からみたOT環境の通信監視
スモールスタートから始めてみよう

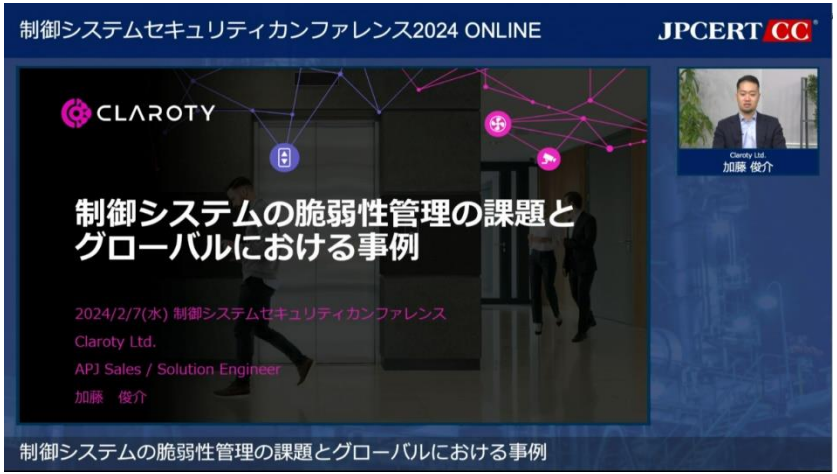
- OSSツール「Arkime」を使用したOT環境の通信監視についての提案
  - 自社の模擬環境を使用してOT環境の通信監視を実践
  - どのパケットを監視するか
  - パケットを監視する際の工夫
  - 2つの攻撃シナリオに対して、
パケット監視の結果を確認
    - サプライチェーンから
保守用サーバーに侵入
    - BadUSBをHMIの空きポートに挿す



各講演のハイライト

制御システムの脆弱性管理の課題とグローバルにおける事例

- OT環境における脆弱性管理に参考となる考え方や事例の紹介
  - OT環境における脆弱性管理の取り巻く状況と重要性
  - 脆弱性管理の課題（特定、追従、優先付け）
  - グローバルでの事例について紹介
    - 資産可視化ツールの活用
    - 脆弱性の優先度付けに関する指針
    - 脆弱性対応の優先付け
    - 脆弱性対応の例



各講演のハイライト

ICSセキュリティポリシーの現場への浸透および具体化に関する支援検討

- ICSセキュリティ担当者がICSセキュリティ対策を現場へ浸透させる際に活用するための文書の作成に関する活動紹介
  - 文書作成の背景や文書の内容についての紹介
    - 解説文書、テスト問題、登場人物ごとのアクション一覧を文書として用意
    - ICS運用者を対象に順守すべき事項を整理
    - 外部記憶媒体、持ち込みPCなど7つの管理項目について記載
    - 何が、なぜ、どのようにを一つの文書に
  - 文書は今後公開される予定

各講演のハイライト

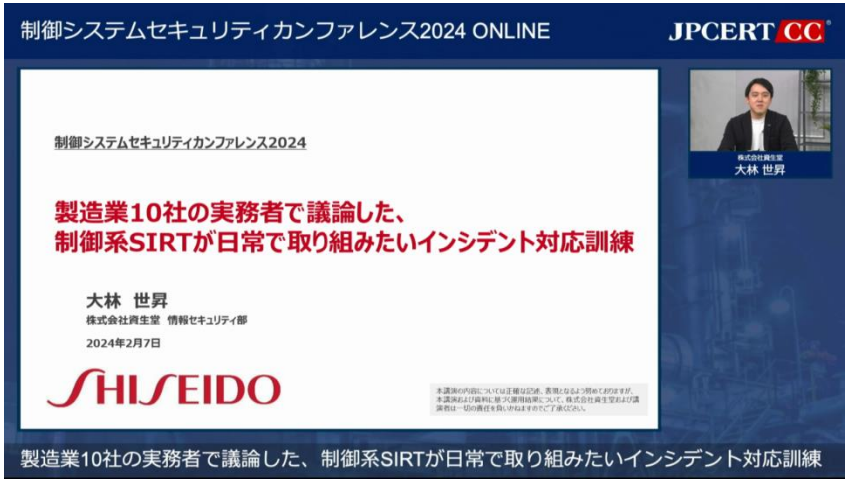
ICS関連のセキュリティインシデント対応に備えて
- 製造業を例に対応体制の整備上の課題と対策の第一歩を解説 –

- ICSのセキュリティインシデント対応に向けてどのような点を考慮すべきかについてICSユーザー組織と共同で検討した内容の紹介
  - サイバー要因を想定すべきICS特有事象についての検討
    - ランサムウェア以外の判別が難しい事象も含む
  - サイバー要因となり得るICS特有事象の収集と評価について
    - 各社の取り組みについて紹介

各講演のハイライト

製造業10社の実務者で議論した、
制御系SIRTが日常で取り組みたいインシデント対応訓練

- 製造業のICSセキュリティ担当者コミュニティーの中で結成された インシデント対応訓練に特化したWG活動の紹介
  - ICSユーザー組織の工場セキュリティ に関する取り組みの紹介
    - パネルディスカッションに参加した ICSユーザー組織も含む
  - WGの活動紹介
  - 成果物（工場セキュリティIR訓練 シナリオ素材案）の紹介
    - FSIRTのメンバーが中心となって対処 できるシナリオ
    - 日々のFSIRT活動の中で取り組むこと を想定



おわりに

まとめ

- インターネットに面したソフトウェア製品の脆弱性を突く攻撃が相次いでおり、初期侵入として利用されている
- まずは「侵害経路」をふさぐこと（脆弱性対応）が一番の基本
- 一例として、直近の事案対応（Ivanti製品の脆弱性の件）を紹介
- 制御システムセキュリティに関する直近の活動について紹介

セキュリティに関して何かございましたら、JPCERT/CCまでご一報ください！
（些細なことでも構いません）

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：pr@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/