狙われ続けるエッジデバイス
～JPCERT/CC目線で見たサイバー攻撃～

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
久下 達也

自己紹介

- 氏名：久下 達也（くげ たつや）
- 所属：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
- 役職：脅威情報アナリスト
- 経歴：
  - 事業会社の総務部でシステム管理業務に従事
  - 金融機関に転職、CSIRT要員としてサイバーセキュリティ対策の推進・運用などを担当
  - 2025年1月、JPCERT/CCに着任

本日の流れ

- JPCERT/CCの概要
- エッジデバイスを標的とした攻撃活動について
- 実際の攻撃事例
  Ivanti Connect Secure等の脆弱性（CVE-2025-0282、CVE-2025-22457）
- 気を付けたいポイント
- おわりに

JPCERT/CCの概要

JPCERT/CCとは

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、国内外にセンサーを置いた
  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」を実施
- 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）、CERT/CC、中国のCNCERT/CC、韓国のKrCERT/CC等）

- 「サイバー攻撃等国際連携対応調整事業」（経済産業省委託事業）および「被害組織から
  円滑に攻撃技術情報を収集する手法に関する検証業務 」（内閣官房委託事業）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NCO（旧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

■ 国内における“火消し”の役割

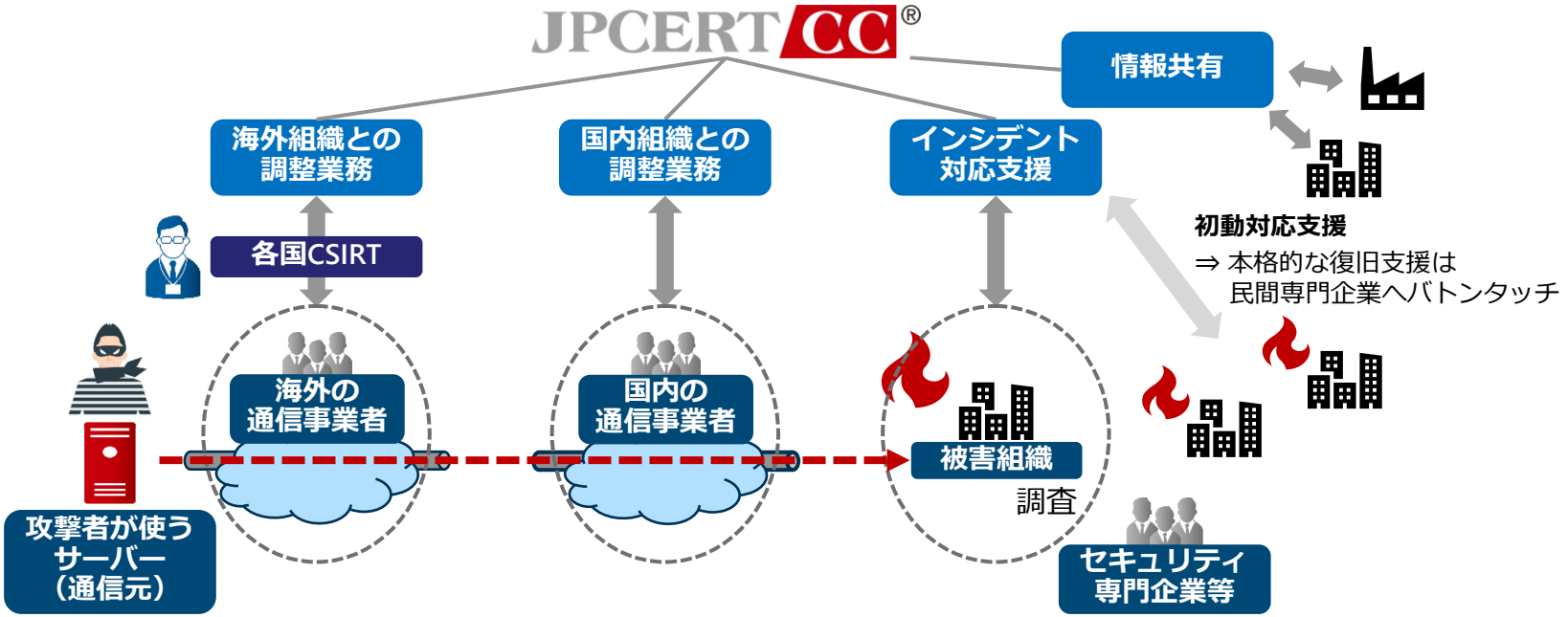
⇒「インシデントレスポンスチーム」

■ 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）」

サイバー攻撃の停止に向けた国内・海外組織との調整

- 攻撃の停止に向けた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



JPCERT/CCの活用

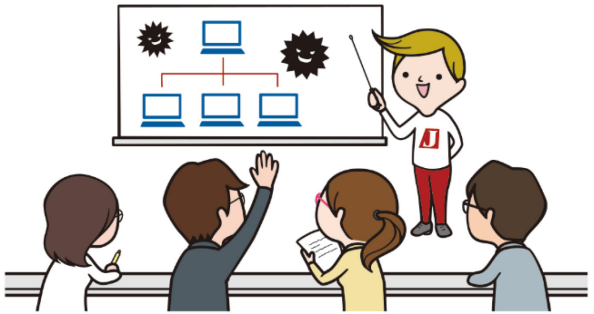
■ コーディネーションセンターの役割

- 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、こんな時にお役立てください

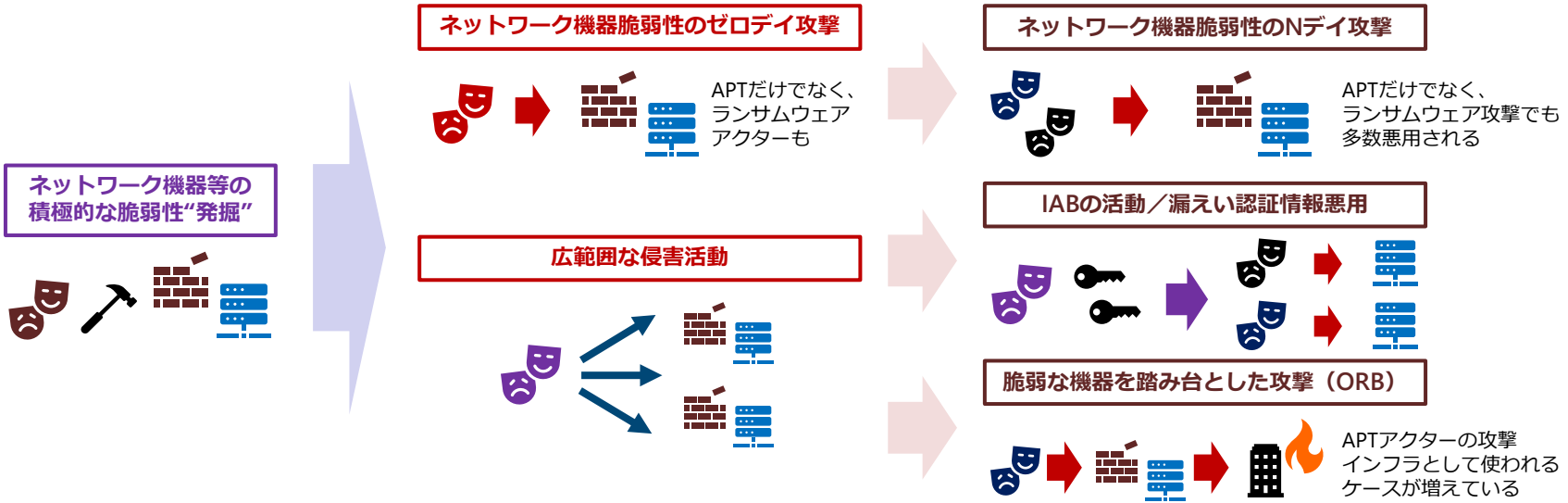
- インシデントが発生し、
  初動対応での技術的な支援や情報が必要な時
- 日々の対策を進める上で、
  脆弱性や脅威に関する情報が必要な時
- その他、お気軽にご相談ください



エッジデバイスを標的とした攻撃活動について

エッジデバイスの脆弱性悪用の傾向

- FW、SSL-VPN機器、ロードバランサー等、いわゆるエッジデバイスの脆弱性悪用ケースが依然として多い
- 従前の「ゼロデイ攻撃⇒脆弱性公表後の広範囲な悪用」というだけでなく、広範囲な侵害活動（バックドアの設置やイニシャルアクセスブローカーのような認証情報の窃取活動）や、侵害したNW機器を攻撃の「中継」として悪用するケースの増加が確認されている



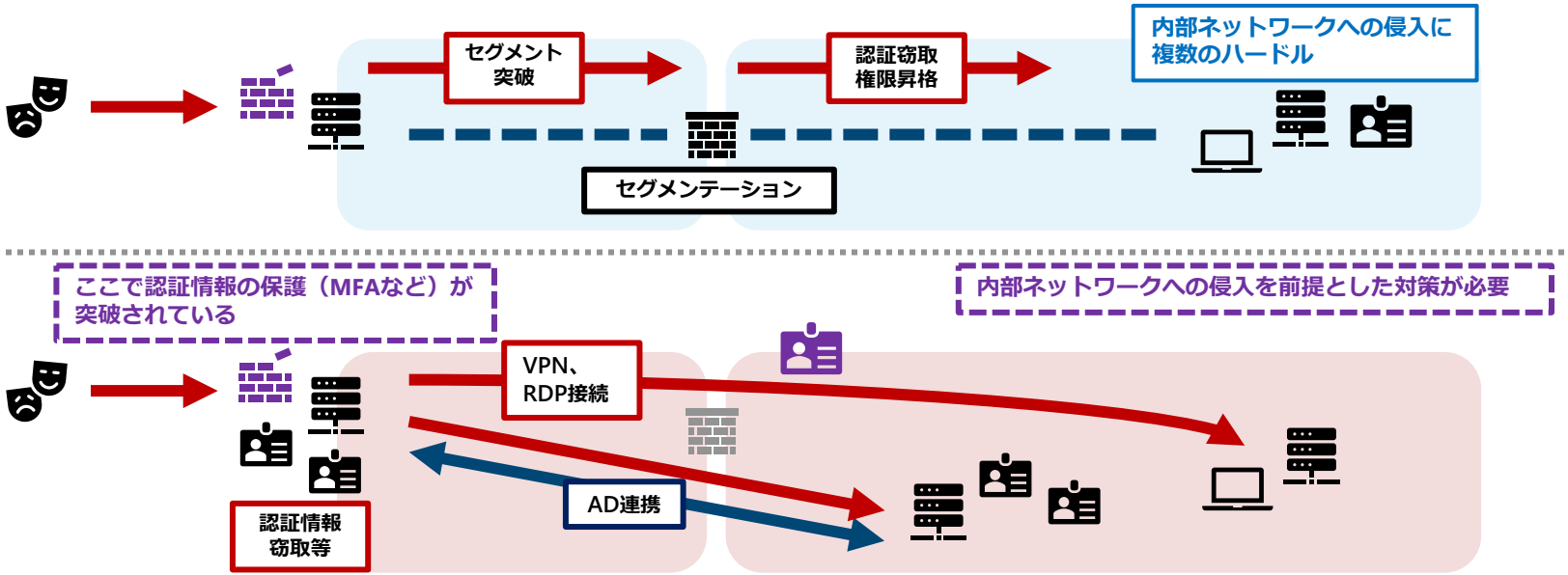
JPCERT/CCが2025年に公開したエッジデバイス関連の警戒情報

■ 注意喚起およびCyberNewsFlash（CNF）は11件（2025年11月5日現在）

タイトル	種別	公開時期
Ivanti Connect Secureなどにおける脆弱性（CVE-2025-0282）に関する注意喚起	注意喚起	1月
Fortinet製FortiOSおよびFortiProxyにおける認証回避の脆弱性（CVE-2024-55591）に関する注意喚起	注意喚起	1月
Ivanti Connect Secureなどにおける脆弱性（CVE-2025-22457）に関する注意喚起	注意喚起	4月
AiCloudが稼働するASUS製WiFiルーターからの通信の観測	CNF	4月
SonicWall製SMA100シリーズにおける複数の脆弱性（CVE-2023-44221、CVE-2024-38475）を組み合わせた攻撃について	CNF	5月
Ivanti Endpoint Manager Mobile（EPMM）の脆弱性（CVE-2025-4427、CVE-2025-4428）に関する注意喚起	注意喚起	5月
SSL-VPN機能が有効化されたSonicWall製ファイアウォールGen 7以降を標的とする脅威活動について	CNF	8月
Citrix Netscaler ADCおよびGatewayの脆弱性（CVE-2025-7775）に関する注意喚起	注意喚起	8月
Cisco ASAおよびFTDにおける複数の脆弱性（CVE-2025-20333、CVE-2025-20362）に関する注意喚起	注意喚起	9月
Cisco ASA、FTD、IOS、IOS XEおよびIOS XRにおける任意のコード実行の脆弱性（CVE-2025-20363）について	CNF	9月
WatchGuard製ファイアウォール「Firebox」のikedにおける境界外書込みの脆弱性（CVE-2025-9242）について	CNF	10月

エッジデバイスの侵害は何がクリティカルなのか

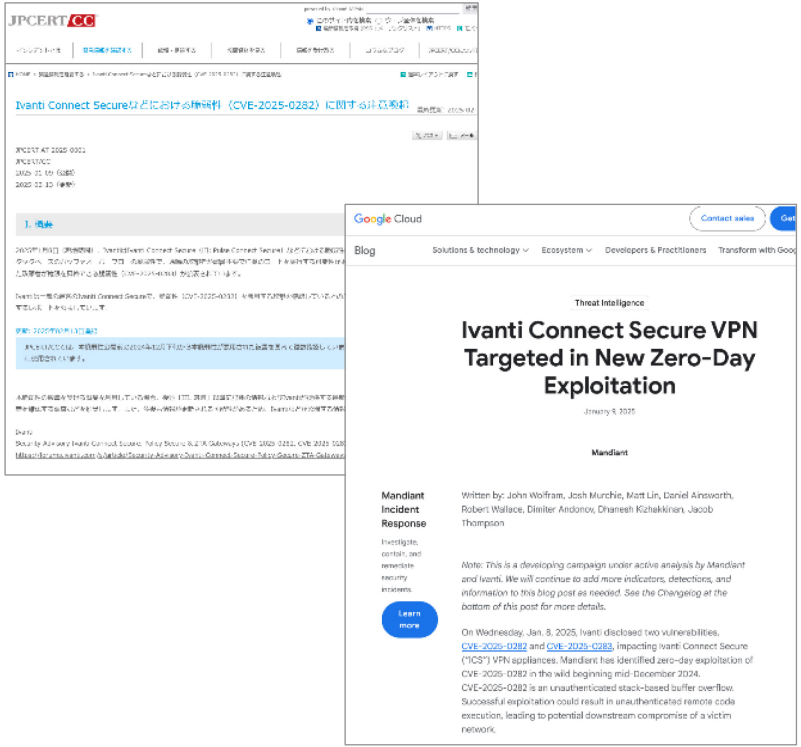
- 従前の攻撃において、DMZ上のWebサーバーなどは、それ自体が標的か、あるいは侵入経路の一つでしかなかった。侵入後に認証情報窃取や権限昇格が行われるため、攻撃プロセスのどこかで検出することが可能
- ここ数年で狙われやすくなった、いわゆるエッジデバイスは、初期侵入経路となるだけでなく、侵害時に認証情報の窃取が行われることが多く、また認証の保護（MFAなど）までが突破されてしまう恐れがある（エッジデバイス侵害により高権限アカウントの認証情報窃取につながるケースもある）



実際の攻撃事例

Ivanti Connect Secure等の脆弱性（CVE-2025-0282、CVE-2025-22457）

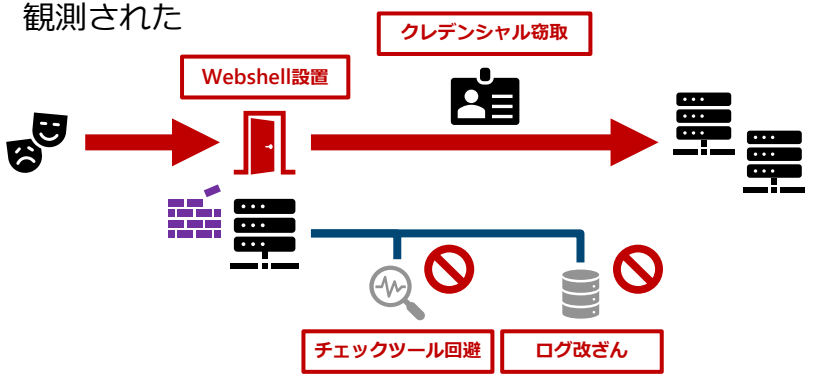
概要



出典（上）：JPCERT/CC「Ivanti Connect Secureなどにおける脆弱性（CVE-2025-0282）に関する注意喚起」
https://www.jpcert.or.jp/at/2025/at250001.html

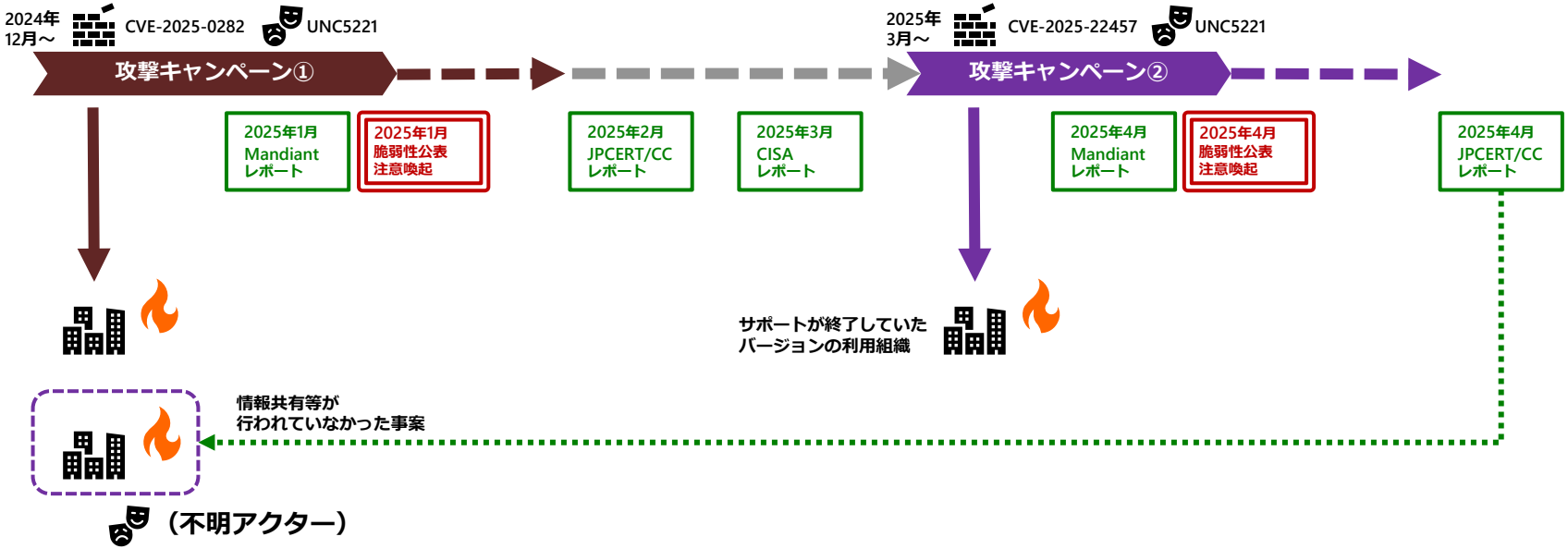
出典（下）：Google Cloud Blog「Ivanti Connect Secure VPN Targeted in New Zero-Day Exploitation」
https://cloud.google.com/blog/topics/threat-intelligence/ivanti-connect-secure-vpn-zero-day/?hl=en

- 2025年1月8日にCVE-2025-0282、4月4日にCVE-2025-22457をIvantiが公表。それぞれゼロデイ攻撃が行われていたもの
- 4月4日公表のCVE-2025-22457については、前年12月にすでにサポートが終了している9.1系が影響対象にて、サポートの終了していたホストが攻撃被害を受けた
- 広範囲な攻撃が行われ、Webshellが設置される被害が多発
- Webshell設置のほか、チェックツールの改ざん、ログ設定の改ざん・消去が行われ、検出が困難な事例が多発
- 窃取されたアカウントにて内部侵害拡大を試みる活動も観測された



大まかなタイムライン

- ゼロデイ攻撃発覚⇒脆弱性公表・注意喚起後も攻撃を継続するケースが確認されている
- また、CVE-2025-22457悪用の攻撃キャンペーンについては、その前年12月にサポート終了となっていたバージョンで稼働するホストを多数狙った



特徴的な点：攻撃者による検知回避

- APTアクターのように侵害環境へのアクセスを長期間維持したいアクターは検知回避を行うことがある
- CVE-2025-0282とCVE-2025-22457のいずれも、整合性チェックツールのスキャン結果が改ざんされていた
- それ以外にも検知回避の結果と見られる痕跡が発見される
  - ログ出力の停止
  - 外部サーバーへのログ転送の停止
  - ログの欠損

Ivanti Connect Secureなどにおける脆弱性（CVE-2025-22457）に関する注意喚起

最終更新：2025-04-30

ポスト　メール

JPCERT-AT-2025-0008
JPCERT/CC
2025-04-04（公開）
2025-04-30（更新）

I. 概要

2025年4月4日（現地時間）、IvantiがIvanti Connect Secure、Policy Secure、ZTAゲートウェイにおけるスタックベースのバッファーオーバーフローの脆弱性（CVE-2025-22457）に関するアドバイザリを公表しました。本脆弱性は2025年2月11日にリリースされたIvanti Connect Secure 22.7R2.6で修正されており、当時は製品のバグと判定されていましたが、同社の再評価によりリモートコード実行につながる可能性があると判明しました。

Ivantiは本脆弱性を悪用する攻撃をすでに確認しており、22.7R2.5以前のバージョンのIvanti Connect Secureとサポートが終了しているIvanti Connect Secure 9.1系（旧名：Pulse Connect Secure）のバージョンを使用する一部の顧客環境で、悪用が確認されているとのことです。アドバイザリの公表と同日、Mandiantがブログを公表し、遅くとも2025年3月中旬から本脆弱性を悪用する攻撃を観測していたと報告しています。JPCERT/CCでは詳細を確認中であるものの、国内ホストでも本脆弱性の悪用と思われる攻撃が発生していることを確認しています。

更新：2025年04月30日追記

JPCERT/CCでは、本注意喚起を公表した2025年4月4日以降も国内ホストで本脆弱性の悪用と思われる攻撃被害が発生していることを確認しています。

初版のIV．侵害検出方法に触れたように、整合性チェックツール（Integrity Checker Tool：ICT）の出力結果が改ざんされる事例が引き続き報告されています。この改ざんの見極めが不十分なために攻撃被害を認知できていないケースも確認しています。

また、海外セキュリティ企業のGreyNoiseによると2025年4月18日にIvanti Connect Secureなどに対する不審なスキャン活動が急増したと公表しており、無差別/広範囲の攻撃活動を示唆しています。

出典：JPCERT/CC「Ivanti Connect Secureなどにおける脆弱性（CVE-2025-22457）に関する注意喚起」
https://www.jpcert.or.jp/at/2025/at250008.html

特徴的な点：検知回避手法の一例

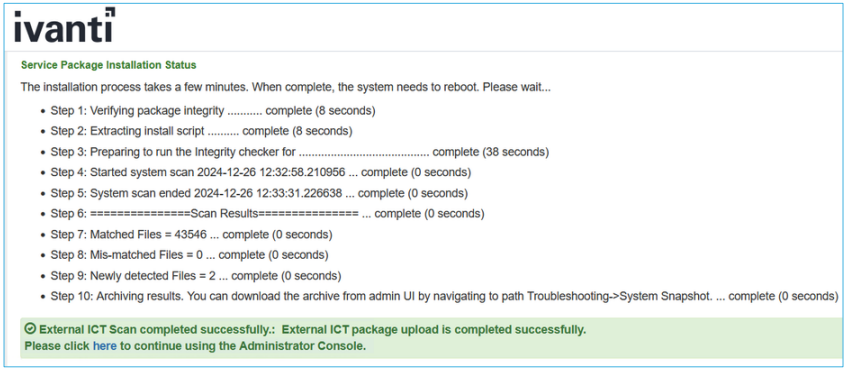
V. 攻撃事例

同脆弱性を悪用する攻撃について解説するMandiant社の情報によると、攻撃者が整合性チェックツール（ICT）による検出の回避を試み、ICTツールの実行が途中で終了する事例を確認しているとのことです。その他にも、侵害後にはユーザーによるアップグレードを妨害しつつ、偽のアップグレードの進捗が表示される機能が埋め込まれるとしています。

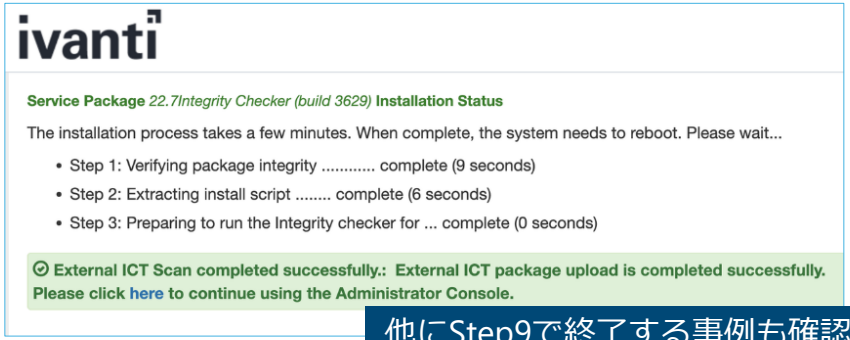
出典：JPCERT/CC「Ivanti Connect Secureなどにおける脆弱性（CVE-2025-0282）に関する注意喚起」
https://www.jpcert.or.jp/at/2025/at250001.html

製品の整合性チェックツール（External Integrity Checker Tool）の動作

（正常）



（異常）ステップの途中にもかかわらず「スキャン成功」と表示させている



他にStep9で終了する事例も確認

出典：Google Cloud Blog「Ivanti Connect Secure VPN Targeted in New Zero-Day Exploitation」https://cloud.google.com/blog/topics/threat-intelligence/ivanti-connect-secure-vpn-zero-day/?hl=en

初期侵入後の侵害活動

横展開

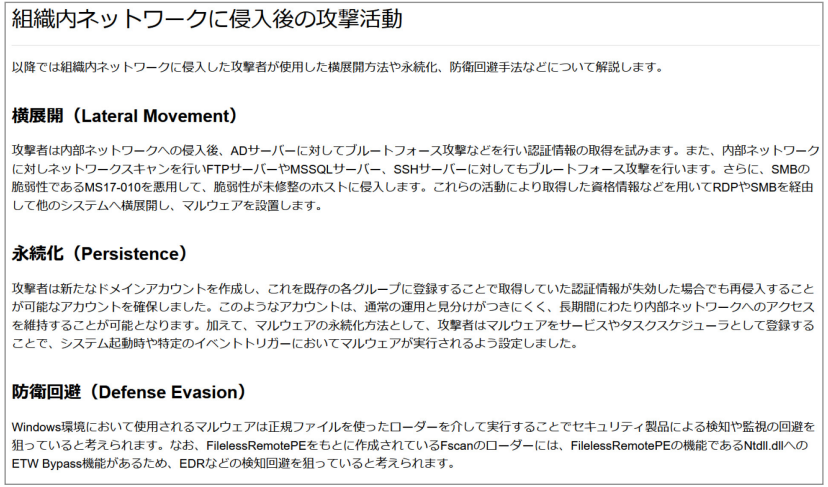
- ADサーバーへのブルートフォース攻撃による認証情報取得
- 内部ネットワークに対するネットワークスキャン
- FTP／MSSQL／SSHサーバーに対するブルートフォース攻撃
- SMBの脆弱性（MS17-010）の悪用
- 上記より窃取した資格情報などを用いたRDP／SMB経由の他システムへのアクセス

永続化

- ドメインユーザーの作成
- 上記の既存グループへの追加
- サービス／タスクスケジューラを用いたマルウェアの実行

防衛回避

- 正規ファイルを使ったローダーを介したマルウェア実行による検知回避
- ntd.dllへのパッチによるETWの無効化



組織内ネットワークに侵入後の攻撃活動

以降では組織内ネットワークに侵入した攻撃者が使用した横展開方法や永続化、防衛回避手法などについて解説します。

横展開（Lateral Movement）

攻撃者は内部ネットワークへの侵入後、ADサーバーに対してブルートフォース攻撃などを行い認証情報の取得を試みます。また、内部ネットワークに対しネットワークスキャンを行いFTPサーバーやMSSQLサーバー、SSHサーバーに対してもブルートフォース攻撃を行います。さらに、SMBの脆弱性であるMS17-010を悪用して、脆弱性が未修整のホストに侵入します。これらの活動により取得した資格情報などを用いてRDPやSMBを経由して他のシステムへ横展開し、マルウェアを設置します。

永続化（Persistence）

攻撃者は新たなドメインアカウントを作成し、これを既存の各グループに登録することで取得していた認証情報が失効した場合でも再侵入することが可能なアカウントを確保しました。このようなアカウントは、通常の運用と見分けがつきにくく、長期間にわたり内部ネットワークへのアクセスを維持することが可能となります。加えて、マルウェアの永続化方法として、攻撃者はマルウェアをサービスやタスクスケジューラとして登録することで、システム起動時や特定のイベントトリガーにおいてマルウェアが実行されるよう設定しました。

防衛回避（Defense Evasion）

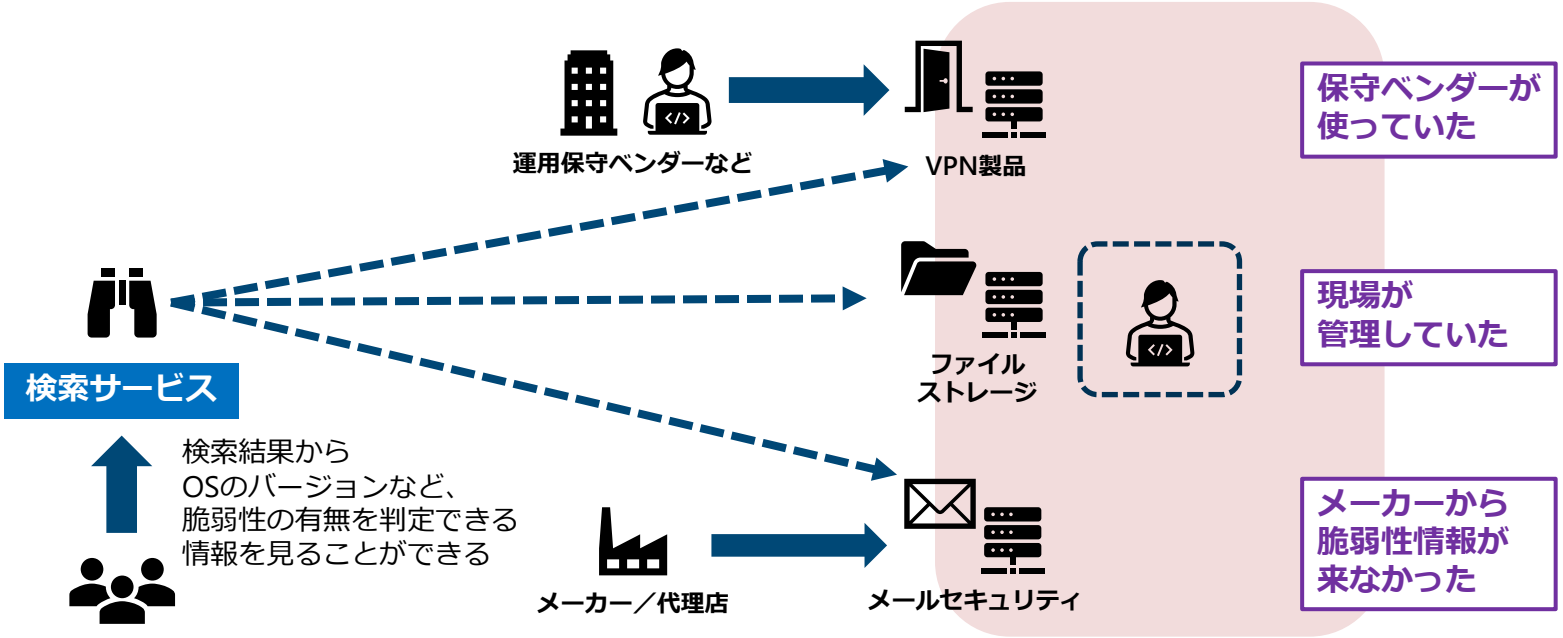
Windows環境において使用されるマルウェアは正規ファイルを使ったローダーを介して実行することでセキュリティ製品による検知や監視の回避を狙っていると考えられます。なお、FilelessRemotePEをもとに作成されているFscanのローダーには、FilelessRemotePEの機能であるNtdll.dllへのETW Bypass機能があるため、EDRなどの検知回避を狙っていると考えられます。

出典：JPCERT/CC「Ivanti Connect Secureの脆弱性を起点とした侵害で確認されたマルウェア」
https://blogs.jpcert.or.jp/ja/2025/07/ivanti_cs.html

気を付けたいポイント

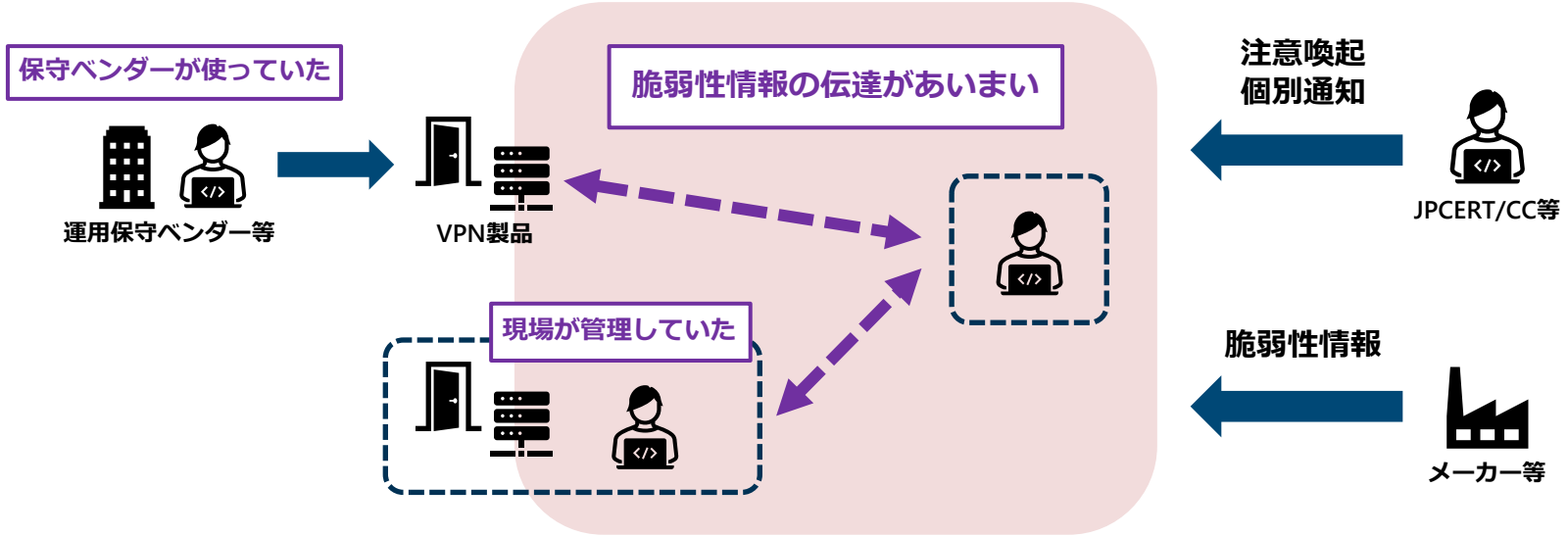
取り残される脆弱なホスト：内部から見えていないホスト

- インターネット接続された各アプライアンスやWebサーバーは、外部の不特定多数の者からは脆弱な状態のホストが「見えている」が、ユーザー組織のシステム管理部門／セキュリティ部門からはホストの状態が「見えていない」というギャップが発生していることが多い



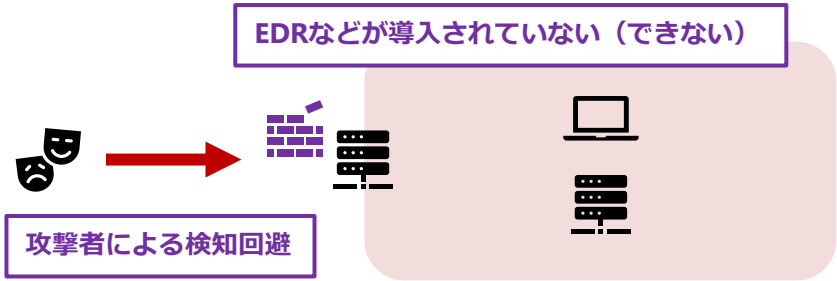
取り残される脆弱なホスト：対処されない一部のホスト

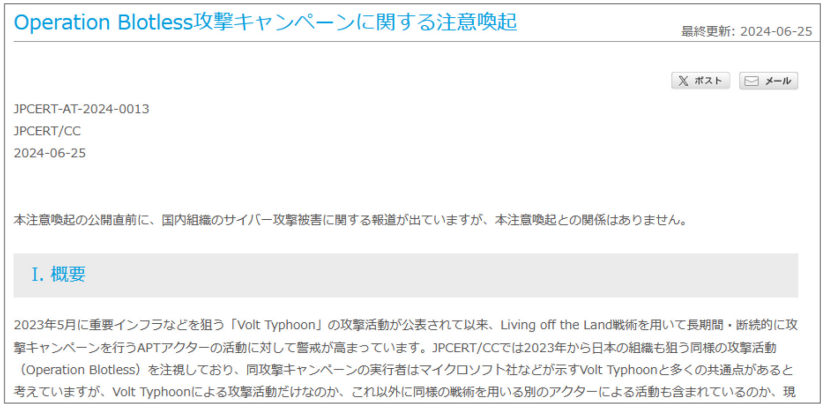
- 外部から脆弱性に関する情報を得られていたとしても、各管理者が異なることで対策が放置されるケースが多い
- 外部専門組織や組織内のCSIRT等と各利用担当部門との間で温度差がある



侵害有無の調査が必要な理由：検知が難しいエッジデバイス

- エッジデバイスは、ホストベースのセキュリティ製品（EDRなど）が未導入などで監視が弱い傾向。加えて、攻撃者は検知回避を試みることから、攻撃時の検知が難しい
- そのため、特に目立った異常が見られない場合も侵害有無の調査が必要
- また、調査の際にログが使えるように次のような状態になっていないかを確認
  - ログの出力設定がされていない
  - 保存期間（容量）が少ない／出力項目が不足している
  - 保全が十分でない（機器内部に保管しており攻撃者に削除されるなど）





Operation Blotless攻撃キャンペーンに関する注意喚起

最終更新: 2024-06-25

JPCERT-AT-2024-0013
JPCERT/CC
2024-06-25

本注意喚起の公開直前に、国内組織のサイバー攻撃被害に関する報道が出ていますが、本注意喚起との関係はありません。

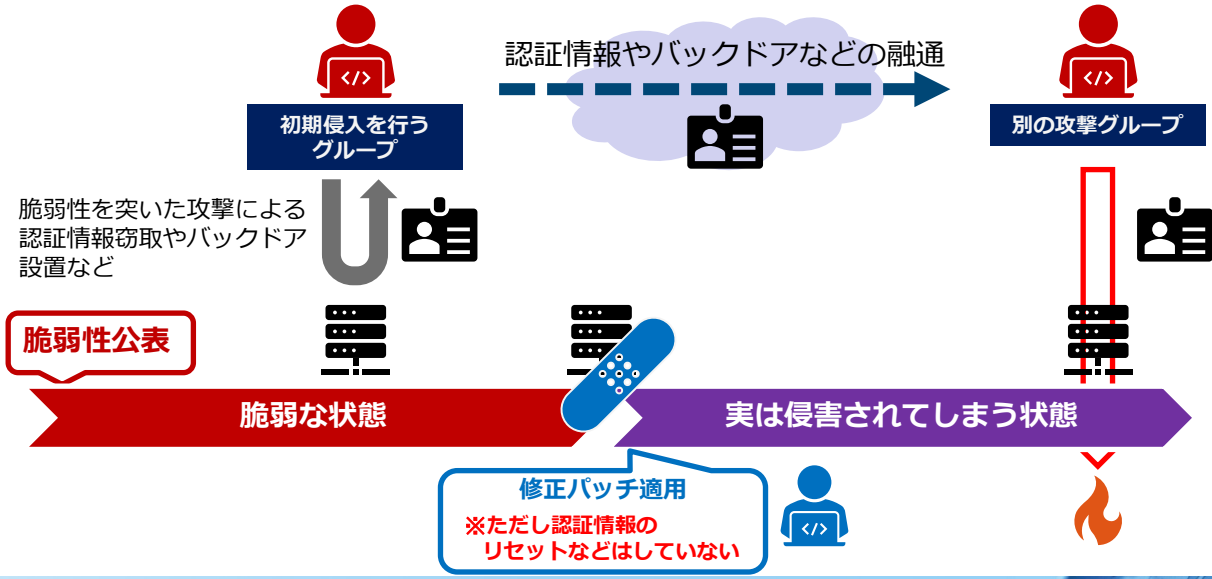
I. 概要

2023年5月に重要インフラなどを狙う「Volt Typhoon」の攻撃活動が公表されて以来、Living off the Land戦術を用いて長期間・断続的に攻撃キャンペーンを行うAPTアクターの活動に対して警戒が高まっています。JPCERT/CCでは2023年から日本の組織も狙う同様の攻撃活動（Operation Blotless）を注視しており、同攻撃キャンペーンの実行者はマイクロソフト社などが示すVolt Typhoonと多くの共通点があると考えていますが、Volt Typhoonによる攻撃活動だけなのか、これ以外に同様の戦術を用いる別のアクターによる活動も含まれているのか、現

出典：JPCERT/CC「Operation Blotless攻撃キャンペーンに関する注意喚起」
https://www.jpcert.or.jp/at/2024/at240013.html

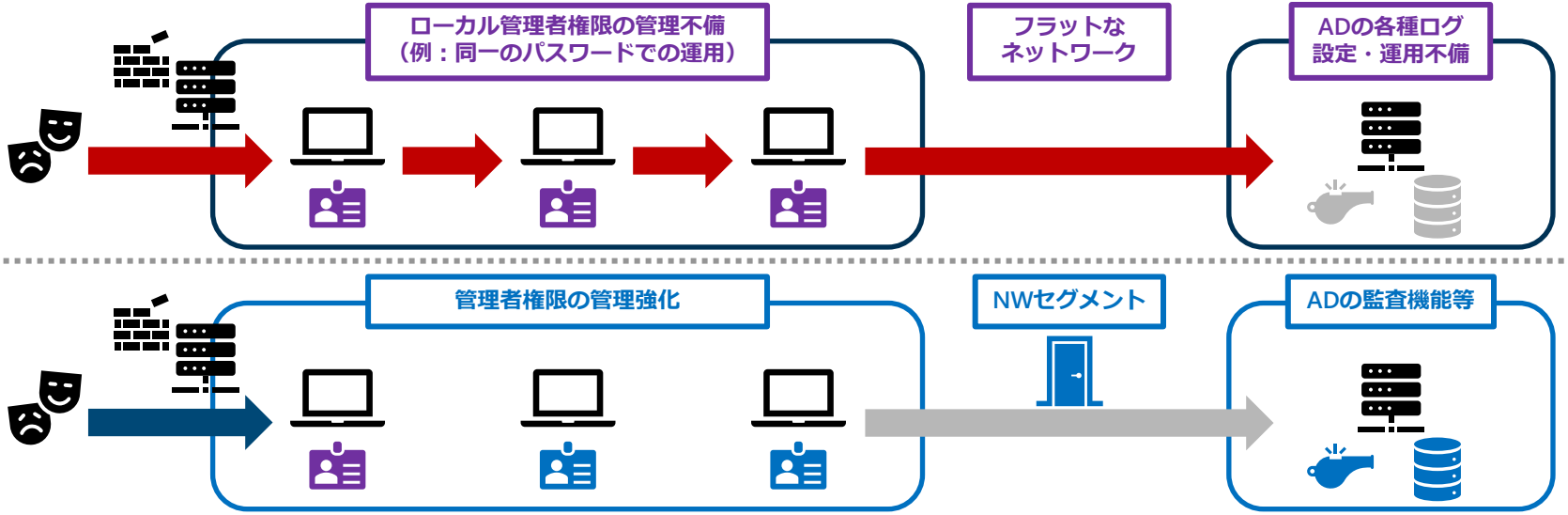
侵害有無の調査が必要な理由：複数の攻撃グループが連携するケース

- パッチ適用前に窃取された認証情報／設置されたバックドアは後から悪用される可能性がある。
  その場合、パッチを適用してもその後の攻撃を防げないため、侵害有無の調査を行うことが重要
- ゼロデイ悪用後の公表・注意喚起後に、間を置かず、次のNデイ悪用が広範囲に始まってしまうため、
  パッチ適用時点ですでに侵害を受けている可能性がある
- 過去に窃取されたとみられる認証情報が悪用された事例が引き続き報告されている状況



ラテラルムーブメント（横展開）対策の基本的強化

- 境界線で破られて侵入されたとしても、その後、攻撃者が「動きにくい」環境づくり
- さまざまなセキュリティ製品、認証製品等の導入もあるが、ネットワーク構成・運用、アカウント管理（最小権限の付与や定期的な権限の見直し、不要アカウントの削除）などの基本的な対策も引き続き有効
- 下記の各対策を実装していない場合、万が一侵入された後の「追跡」や「トリアージ」（安全な箇所とそうでない箇所の切り離し等）が困難に



おわりに

本日のまとめ

- 攻撃者により検知回避が行われるケース
  - 検知回避に関する情報が公開されている場合は、調査結果を慎重に確認
- パッチ適用前にすでに攻撃を受けている可能性
  - 目立った異常が見られなくても、まずは侵害有無を調査
  - 調査が行えるよう、ログを保全
  - 侵害が確認された場合は、認証情報リセット／マルウェア削除などの対応を実施
- 管理体制の見直しや侵害を前提とした対策
  - 組織内に対策漏れのホストが生じないよう注意が必要
  - 侵害された場合のラテラルムーブメント対策の強化

JPCERT/CCでは、各組織からの情報を組み合わせてインシデントの分析を実施しています。情報提供へのご協力をお願いいたします。

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/

ご清聴ありがとうございました