サイバー攻撃の検知、対応における Active Directoryログの重要性について

JPCERTコーディネーションセンター
早期警戒グループ　脆弱性アナリスト
土居　啓介

アジェンダ

- JPCERT/CCの紹介
- Active Directoryとは
- Active Directoryを悪用した事例
- Active Directoryのイベントログによる検知・対応
- 検知に向けた事前検討の注意点
- ログハンズオンの紹介

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**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（主に、情報セキュリティ担当者）**
  - 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、**日本ののの窓口となる「CSIRT」**
    ※各国に同様の窓口となるCSIRTが存在する
    (例、米国のUS-CERT、CERT/CC、中国のCNCERT/CC、 韓国のKrCERT/CC)
- 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をご存知ですか？」

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

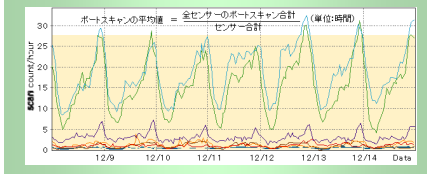
- 未公開の脆弱性関連情報を製品開発者へ提供し、対応依頼
- 関係機関と連携し、国際的に情報公開日を調整
- セキュアなコーディング手法の普及
- 制御システムに関する脆弱性関連情報の適切な流通

JVN Japan Vulnerability Notes

情報収集・分析・発信

定点観測（TSUBAME）

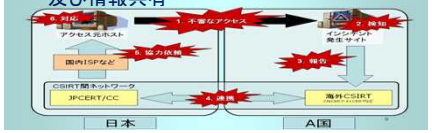
- ネットワークトラフィック情報の収集分析
- セキュリティ上の脅威情報の収集、分析、必要とする組織への提供



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及び情報共有

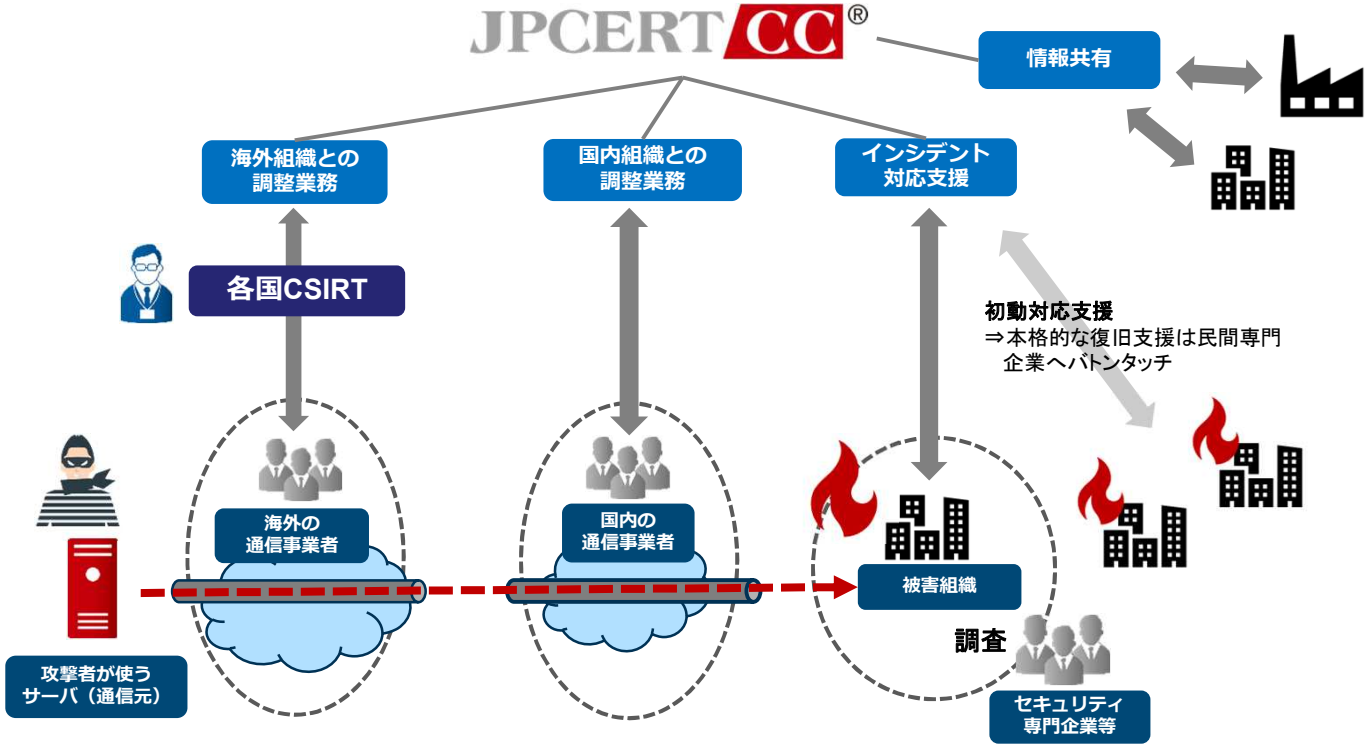


早期警戒情報	重要インフラ、重要情報インフラ事業者等の特定組織向け情報発信
脆弱性情報ハンドリング	ソフトウェア製品等の脆弱性情報に関わる開発者等との調整・公表
CSIRT構築支援	海外のNational-CSIRTや企業内のセキュリティ対応組織の構築・運用支援
アーティファクト分析	マルウェア（不正プログラム）等の攻撃手法の分析、解析
制御システムセキュリティ	制御システムに関するインシデントハンドリング/情報収集,分析発信
国内外関係者との連携	日本シーサート協議会、フィッシング対策協議会の事務局運営等
国際連携	各種業務を円滑に行うための海外関係機関との連携

【JPCERT/CCの活動】

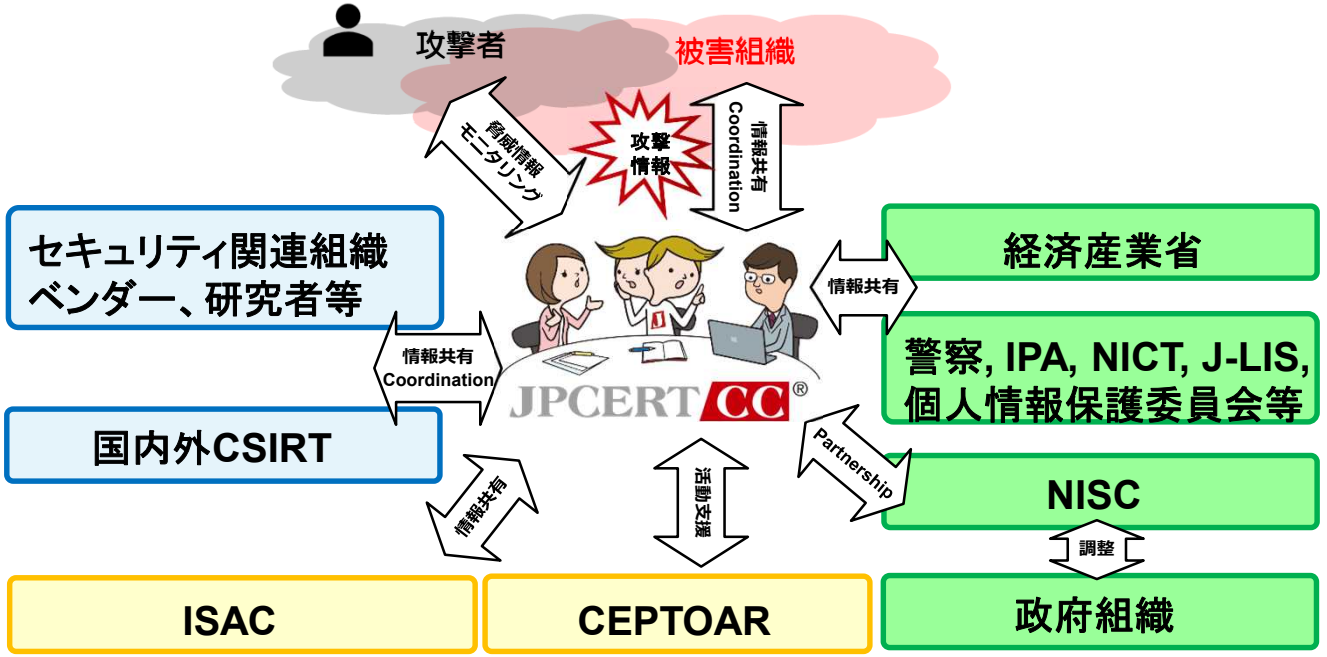
サイバー攻撃の停止に向けた国内・海外組織との調整

- 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



コーディネーションセンターとしての役割

さまざまなパートナーとの調整



インシデントに関する調整 (coordination) 機関として、問題解決に向けて、必要な人に必要な情報を届ける業務を行っています

JPCERT/CCの活用

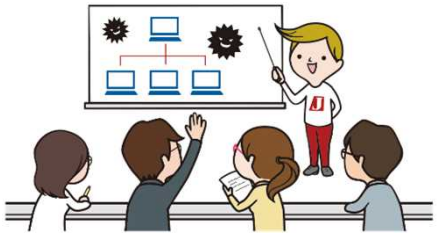
■ コーディネーションセンターの役割と活用

- 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CSIRT 連携促進、コミュニティ推進

“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

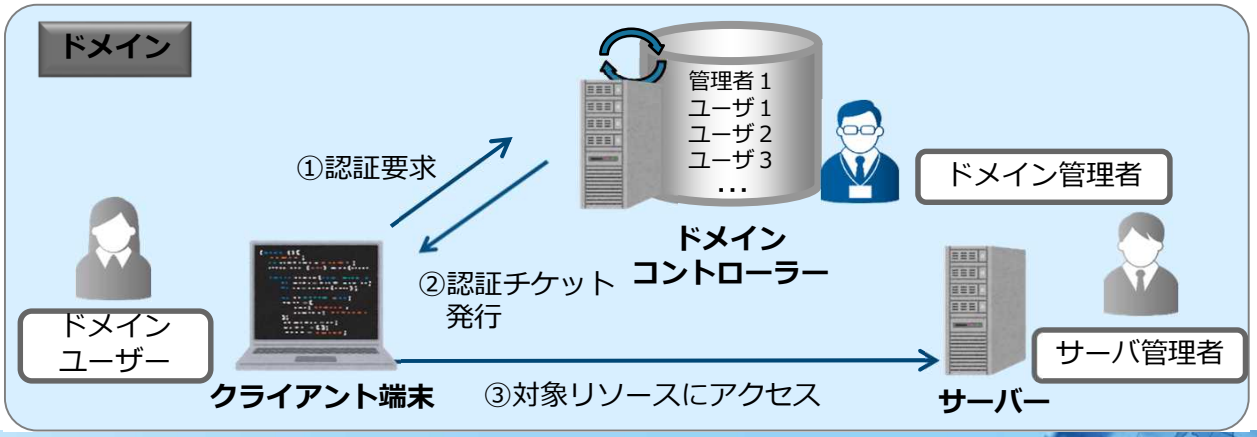
- インシデントが発生し、初動対応での技術的な支援や情報が必要となるケース
- 日々の対策を進める上で、脆弱性や脅威に関する情報が必要となるケース
- その他、お気軽にご相談ください



Active Directoryとは

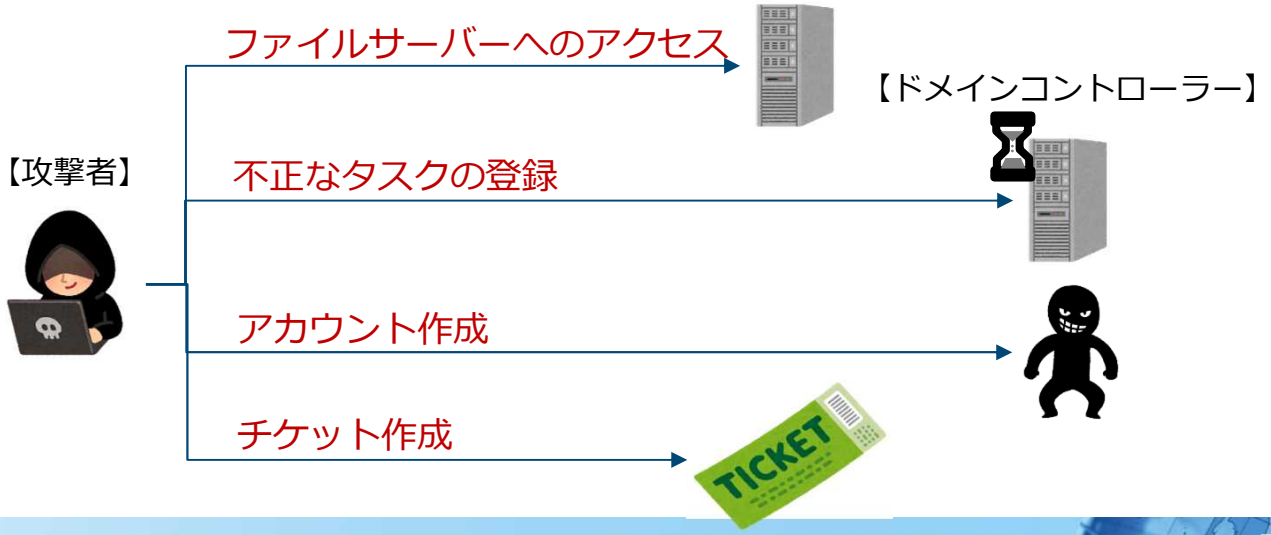
Active Directoryとは

- Active Directoryとは
  - マイクロソフト社が提供している、組織内のコンピューターやユーザーを集中的に管理できる仕組み
  - 利便性が高い反面、攻撃者に狙われやすい
  - 特に、ドメイン内のリソースを管理可能な「ドメイン管理者権限」が狙われる



ドメイン管理者権限

- ドメイン管理者（Domain Admins）
  - ドメインに対する管理者権限を保持するアカウント
  - ドメインに対するあらゆる操作が可能
- ドメイン管理者権限を窃取された場合、ドメイン配下に対して攻撃を行うことができる



Active Directoryを悪用した事例

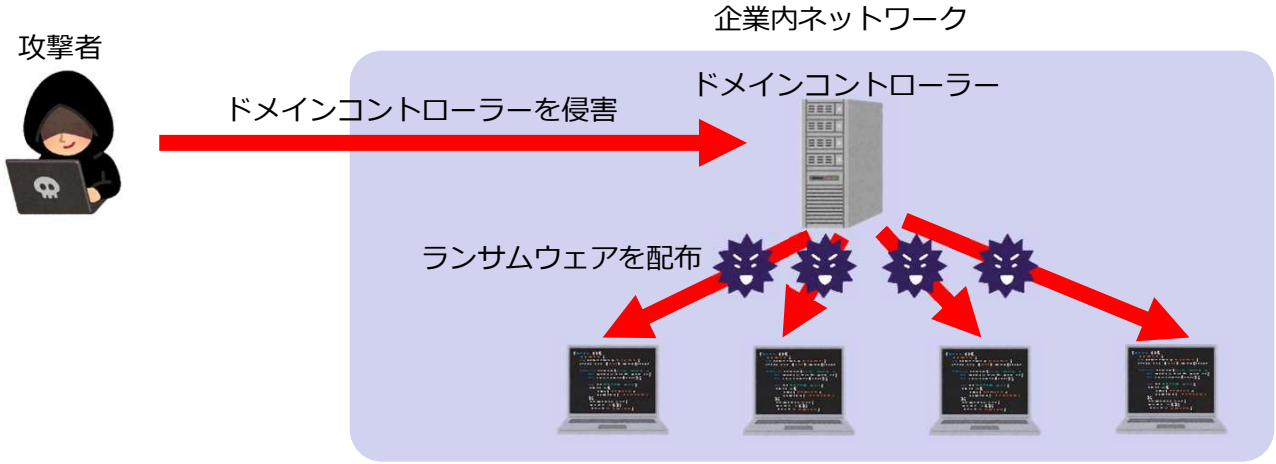
Active Directoryを悪用した事例（1/3）

- 2020年5月、FireEye社はランサムウェアMazeを利用する攻撃者のTTP（戦略/技術/手順）を公開

出展：https://www.fireeye.com/blog/threat-research/2020/05/tactics-techniques-procedures-associated-with-maze-ransomware-incidents.html

Active Directoryを悪用した事例（2/3）

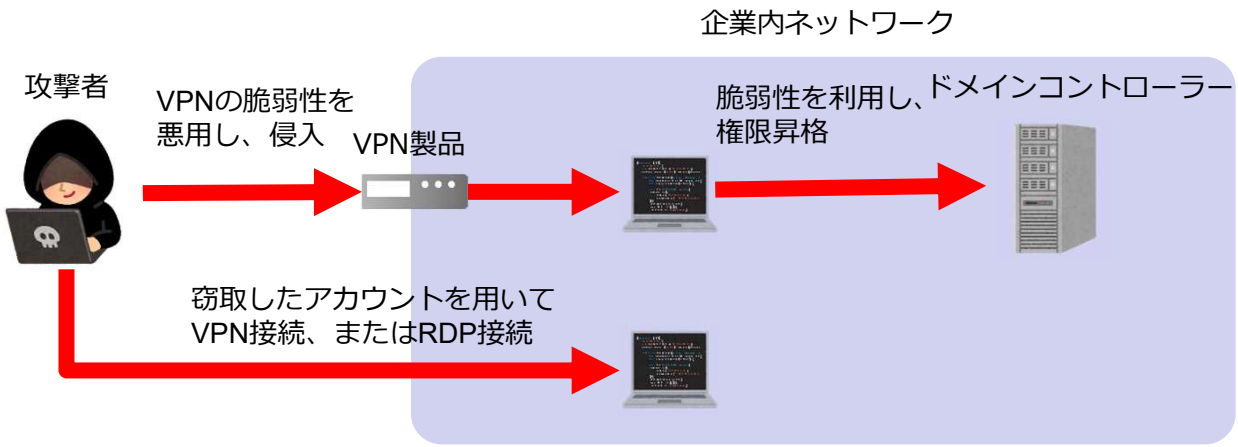
- 2020年7月、アルゼンチンのインターネットサービスプロバイダがランサムウェア被害、約753万ドルを要求
- ドメインコントローラーの管理者権限を奪取し、そこから組織内の18,000台以上の端末にランサムウェアを配布



出典：https://www.zdnet.com/article/ransomware-gang-demands-7-5-million-from-argentinian-isp/#ftag=RSSbaffb68

Active Directoryを悪用した事例（3/3）

- 2020年10月、米CISAはVPN製品の脆弱性と、2020年8月に修正されたNetlogon脆弱性（CVE-2020-1472）を併用した攻撃を複数確認したと公表

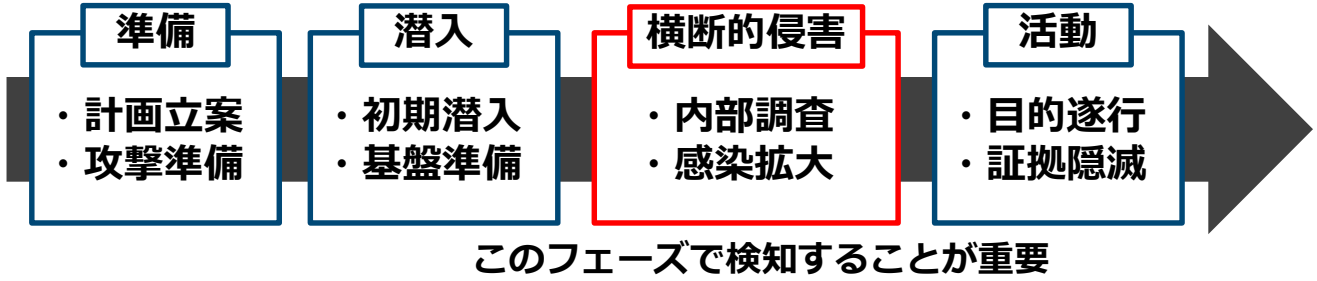


出展:https://twitter.com/MsftSecIntel/status/1308941504707063808
https://us-cert.cisa.gov/ncas/alerts/aa20-283a

Active Directoryの
イベントログによる検知・対応

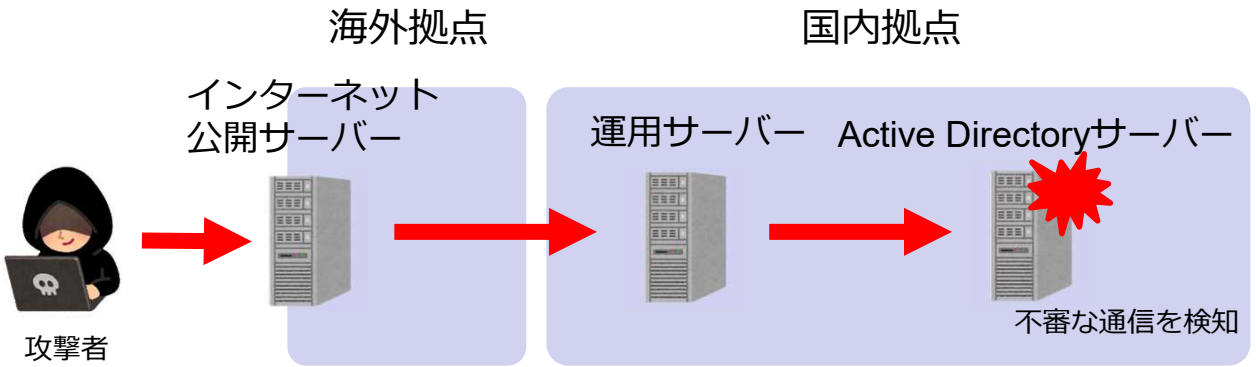
ADイベントログによる検知/対応（攻撃の早期検知）

- サイバーキルチェーン
  - 攻撃者が目的を達成するための段階を分類
- 「横断的侵害」のフェーズで検知し、「活動（資産の暗号化や窃取）」を防ぐ
  - Windowsでは認証ログがイベントログとして記録されることから、ADのログを確認することで、アカウントの悪用を早期に検知できる可能性がある



Active Directoryの監視により侵害を検知した事例

- 2020年に、Active Directoryへの不審な通信の検知から攻撃に気づいた事例も公表されている



ADのイベントログによる検知・対応（効率的な調査）

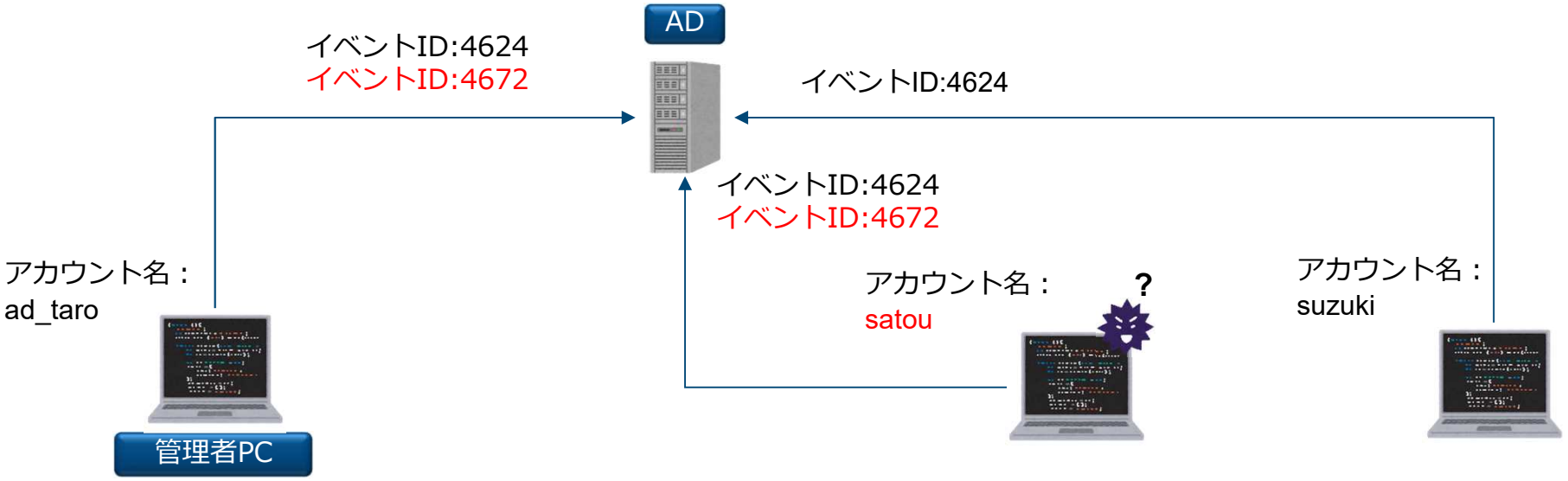
- 多数の端末を監視・調査するのは困難
  - VPNの脆弱性等を悪用した侵入においては、事案発生時にどこから調査をするべきか迷うことも
- まず、ドメインコントローラーやサーバーのイベントログを確認し、不審な端末を絞り込んだ調査により、効率的な調査が可能

ログ分析時の観点について

- ADに対する攻撃の検知、特にドメイン管理者アカウントの悪用の検知に有効な一部の例を紹介
  - 攻撃時に記録されるイベントログによる検知・対応
    - 不審なタスクの作成 (イベント ID:4698)
    - イベントログ消去の調査 (イベントID:1102)
  - 平常時との比較による検知・対応
    - 特権利用状況
    - 認証端末
    - 認証試行回数
    - 認証時間

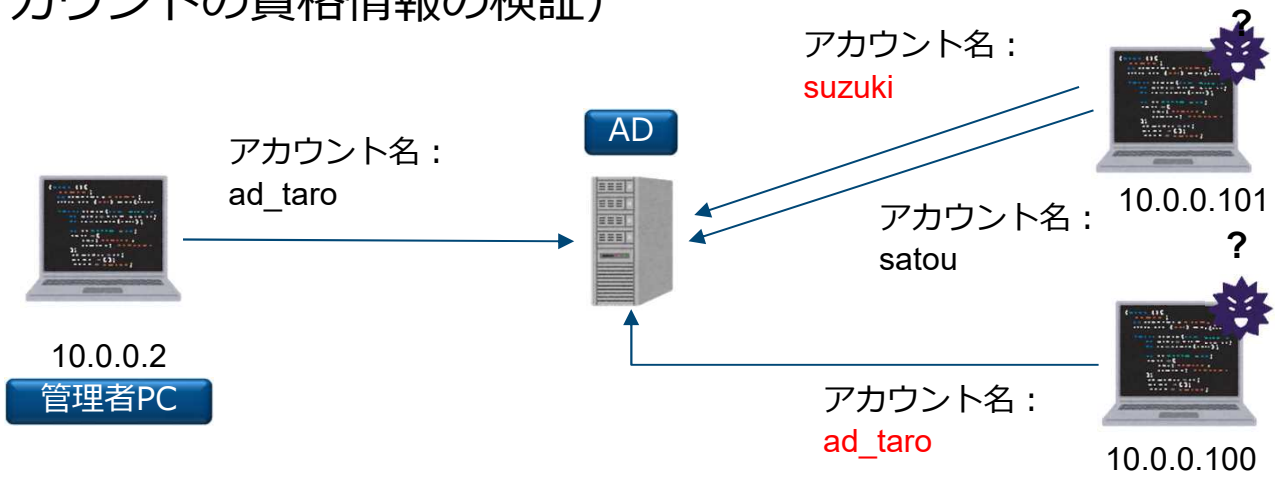
平常時との比較による検知 - 特権利用状況

- 管理者権限を利用しないユーザーへの特権割り当てを確認
  - 着目するイベントID: 4672（新しいログオンへの特権割り当て）



平常時との比較による検知 - 認証端末

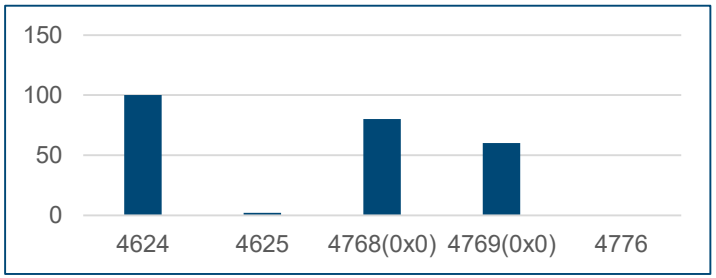
- 一般ユーザの端末からの管理者権限アカウント要求や、同一端末から複数アカウントへの認証要求有無を確認
  - 着目するイベントID：4624（ログオン成功）、4625（ログオン失敗）、4768（Kerberos 認証チケット (TGT) の要求）、4769（Kerberos サービス チケットの要求）、4776（ドメイン コントローラーによるアカウントの資格情報の検証）

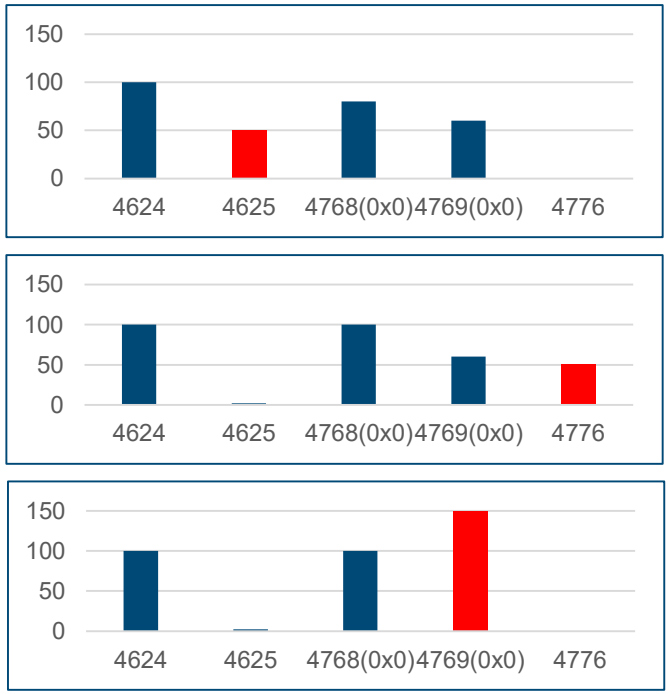


平常時との比較による検知 - 認証施行回数

- 時間単位や日単位での総認証回数や失敗回数等の変動から、イレギュラーな認証要求を行っているアカウントや端末を推定する

平日の認証平均回数

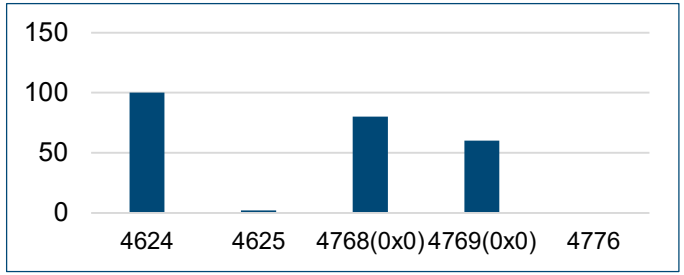


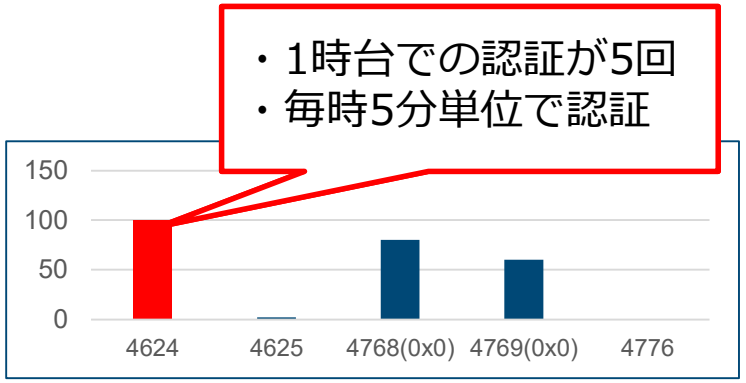


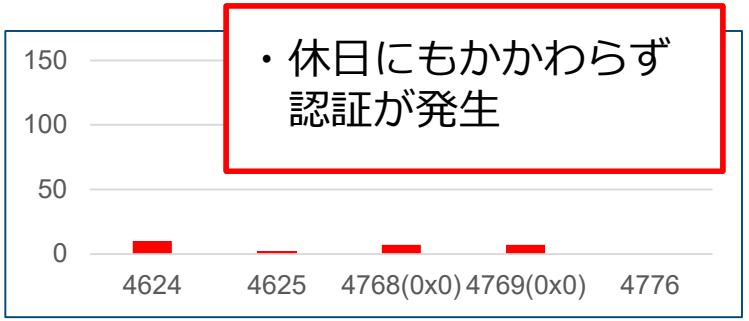
平常時との比較による検知 - 認証時間

- 業務時間外の認証要求、一定間隔での認証が発生しているアカウント、端末を確認する

【平時の傾向】
アカウント利用者が不在のため
0:00 - 6:00 や休日では基本的に認証は発生しない



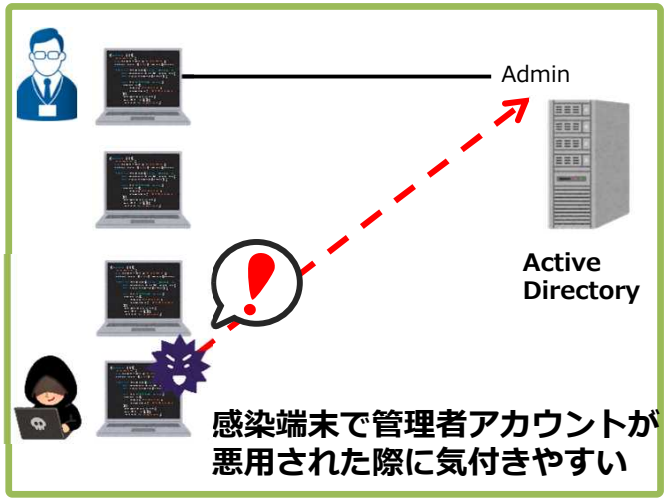




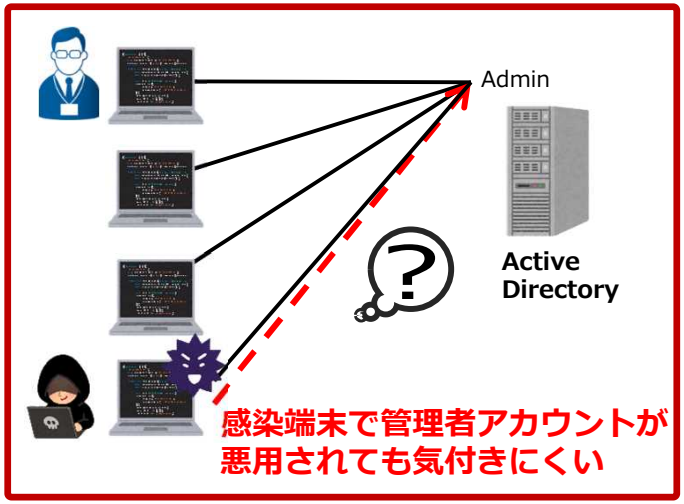
検知/対応に向けた事前検討の注意点

- いざという時に備えて、事前の検討が重要
  - ログの保存サイズ、監査ポリシーの有効化、外部への保存 etc.
- 管理者アカウントの使用端末を限定などの検知しやすい運用

悪用を検知しやすい例
（端末とアカウントが1:1）



悪用を検知しにくい例
（端末とアカウントが多:1 または多:多）



まとめ

- Active Directoryは、情報リソースの管理を一元的に行うことができるなど利便性が高い反面、侵害時の影響が大きい
  - ランサムウェア等で利用されるケースも
- イベントログを利用することで、侵害の早期検知による被害範囲の限定、事案発生時の効率的な調査に活用できる
- 活用にあたっては、事前の監視やアカウント管理の運用に関する設計/設定が必要となる

- 本資料では、「検知」「対応」の部分に焦点をあてたが、「特定」「防御」「復旧」といった観点での検討も必要
  - 詳細は参考文献を参照ください

紹介：ログ分析ハンズオン

- 日頃、インシデントの対応ではログの情報が必要不可欠だが、実際に取得している組織は多くない
  - さらに、活用までしている組織となるとかなり限られたものになる
- JPCERT/CCではActive Directoryをはじめとした各種ログの取得の重要性と、実際に活用する際のポイントを説明する**ログ分析ハンズオン（5時間程度）を有償で提供**
- ハンズオンの対象
  - ログ分析ができる体制を作ろうとしている組織
  - CSIRTに所属したばかりの経験の浅い人員　etc.

お問い合わせはこちらへ

ew-info@jpcert.or.jp

参考文献

- マイクロソフト株式会社
  - Active Directory のセキュリティ保護に関するベスト プラクティス
    - https://docs.microsoft.com/ja-jp/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory
- 情報処理推進機構(IPA)
  - 情報システム開発契約のセキュリティ仕様作成のためのガイドライン
    - https://www.softwareisac.jp/ipa/index.php
- JPCERTコーディネーションセンター
  - ログを活用したActive Directoryに対する攻撃の検知と対策
    - https://www.jpcert.or.jp/research/AD.html
  - インシデント調査のための攻撃ツール等の実行痕跡調査に関する報告書
    - https://www.jpcert.or.jp/research/20160628ac-ir_research.pdf

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
- Tel：03-6271-8901
- 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

脆弱性に関するお問い合わせ

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