Windowsログ分析の基礎 ~基本編~

- ADへの攻撃を理解するために -

一般社団法人
JPCERTコーディネーションセンター

本資料について

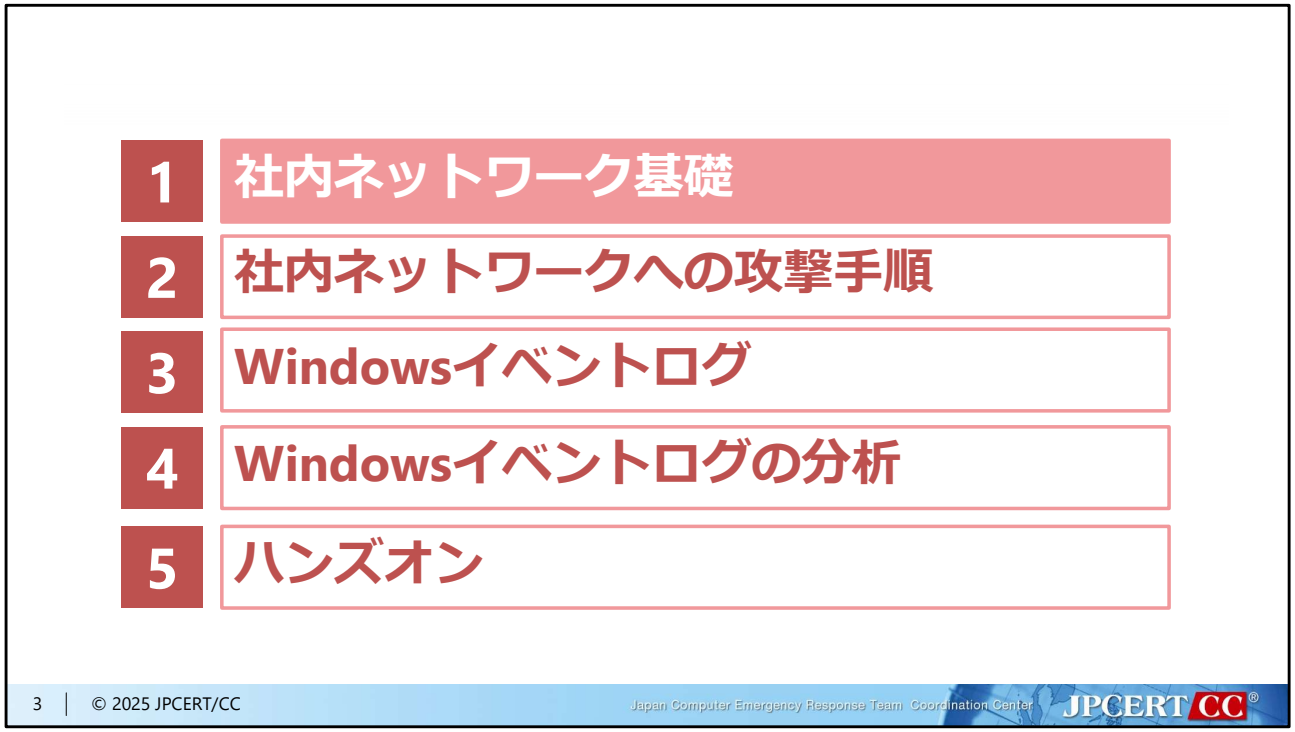
- 本資料は、社内ネットワーク（主にWindowsネットワーク）におけるログ分析の基本的な知識を学ぶための資料です。
- 学習目的でご自由にお使いください。
- 編集・再配布などをご希望の場合は、以下までご連絡ください。
  - pr@jpcert.or.jp

本コンテンツは、攻撃者のネットワーク侵入手法を学びインシデント発生時に必要となるログ調査の中で主にWindowsのイベントログの調査を中心に学習するものになっています。
インシデント対応では、よく行われる流れとしては、検知 → 初動調査 → 一時対処 →本格調査 → 報告→ 恒久対策 という流れで行われることが多くありますが、本コンテンツは、調査の部分に特化しています。

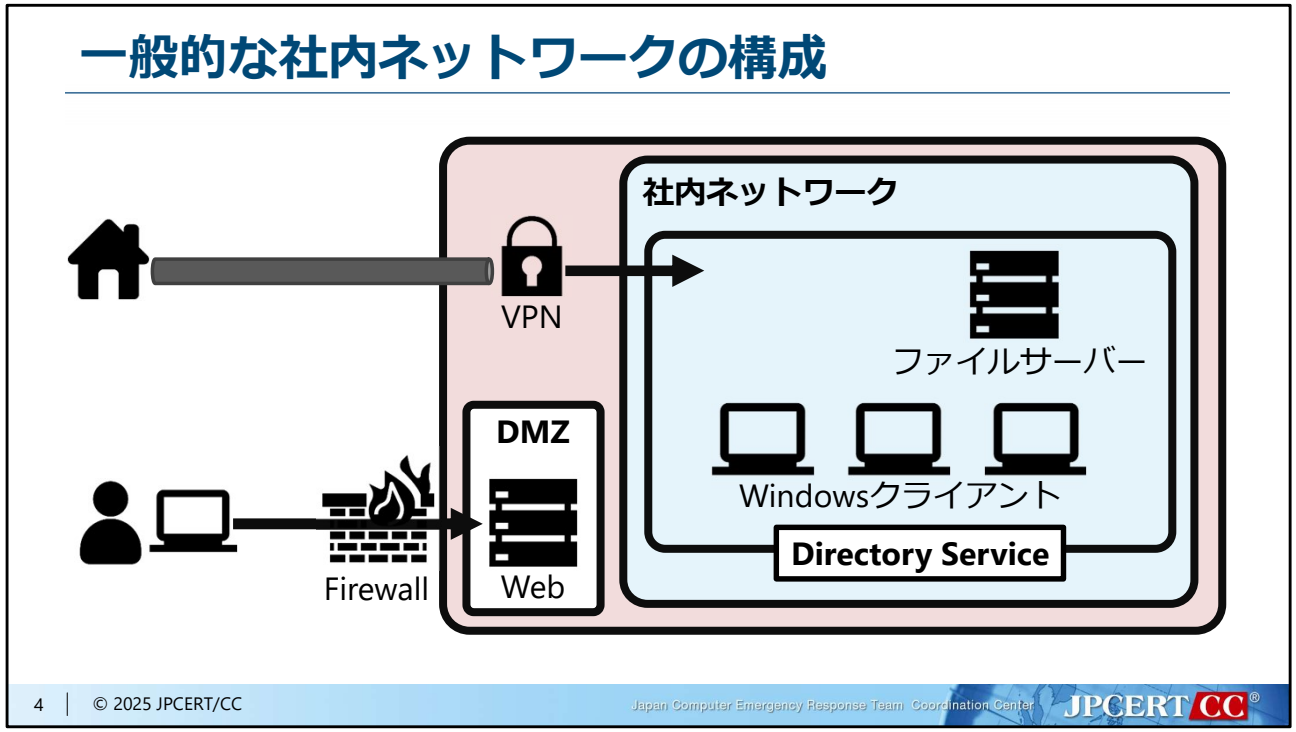
Agenda

1. 社内ネットワーク基礎
2. 社内ネットワークへの攻撃手順
3. Windowsイベントログ
4. Windowsイベントログの分析
5. ハンズオン

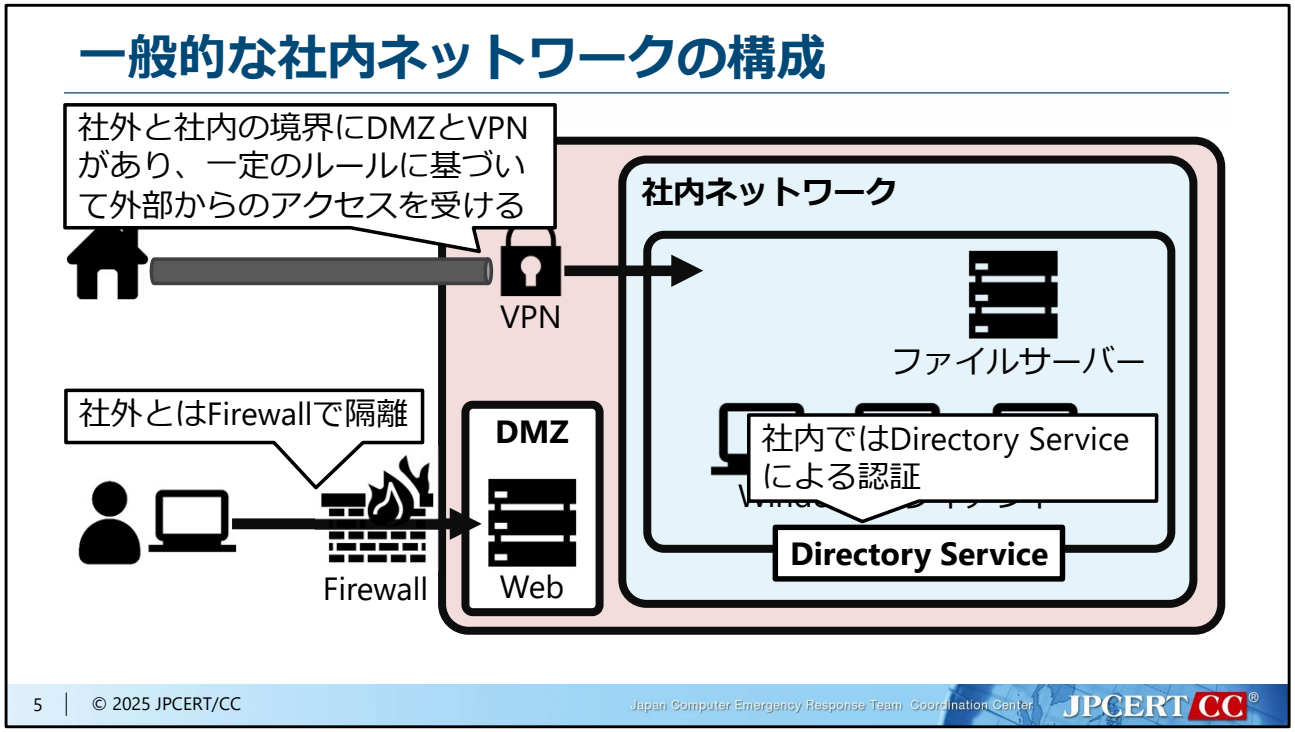
1章から4章までは、座学としてネットワーク侵入時の攻撃手法について学びます。
5章および、~実践編~資料がハンズオンになっています。
基本的な攻撃手法をすでに把握済みの場合は、ハンズオンに進んでください。



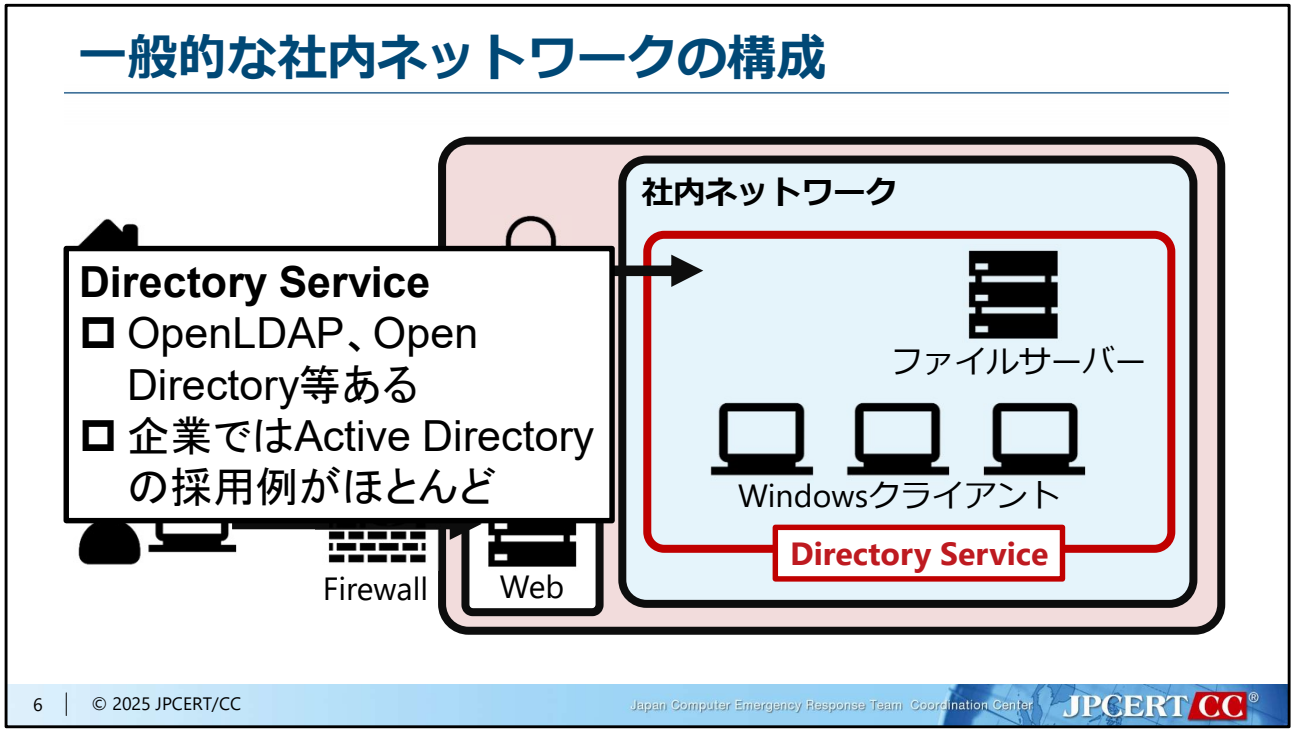
まずは、攻撃から守るべきネットワークの基本となるWindowsネットワークについて説明します。



この図は、一般的な社内ネットワークを主要な要素に絞って簡略化したものです。
昨今の攻撃者のターゲットとなるのは、VPN、Webサーバー、ドメインコントローラー、Windowsクライアント、ファイルサーバー（管理者権限で動作するサーバー群など）です。



一般的な社内ネットワークでは、社外と社内の境界にDMZとVPNがあり、一定のルールに基づいて外部からのアクセスを受け付けます。
そして、社内ネットワークではDirectory Serviceによって社内システムの認証が行われています。



本コンテンツでは、基本的に社内ネットワークをWindowsネットワークで構成した組織を想定して説明を進めます。Windowsネットワークを理解するうえで、AD、DS、ドメインコントローラーという単語がよく使われます。以下に、それらの言葉を整理します。

- Directory Service
  - ネットワーク内に接続されたリソースを管理するためのサービスで、OpenLDAP、Open Directory等がある
- Active Directory
  - WindowsサーバーにあるDirectory Service
- ドメインコントローラー
  - Active Directoryサービスを提供するサーバー

ネットワーク内のリソース、アカウント情報などを管理するサーバーをドメインコントローラーとして、以降では説明します。

Active Directory Domain Service (AD DS)

AD DSとは

- Windows Serverの**機能**で、Windowsネットワーク内の端末管理や認証・認可を行う

例えば、➡ このサービス使える？ | ファイル見て良い？ | USBは使用禁止 | 5分でスクリーンロック

ドメインコントローラーとは

- AD DSがインストールされた、認証・認可を行う**サーバー**
  - ― 管理する範囲は**ドメイン**という
- 複数台で運用することも可能（子会社/海外支局など）

Active Directory には、複数の機能があります。
その中でも、Domain Service を提供する機能をAD DSと呼び、この機能はWindowsネットワーク内の端末管理や認証・認可を行います。
この、AD DSがインストールされたWindowsサーバーがドメインコントローラーとなります。

ドメインとフォレスト

ドメイン

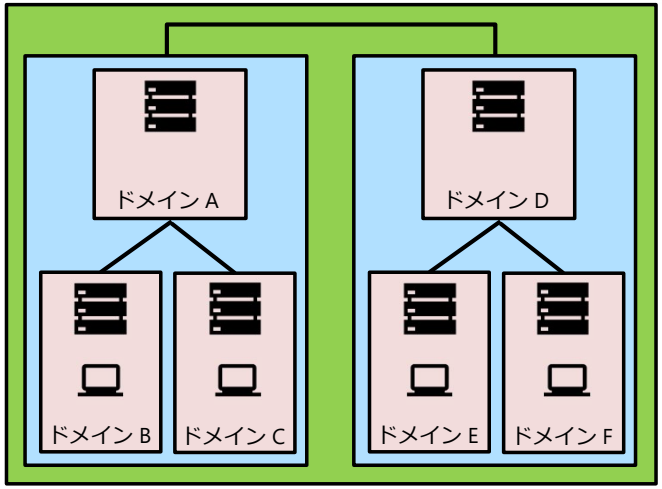
- あるドメインコントローラーが管理する範囲
- 複数台で管理することもある
- 親子：サブドメイン継承
- 信頼：相互に認証しあう

ツリー

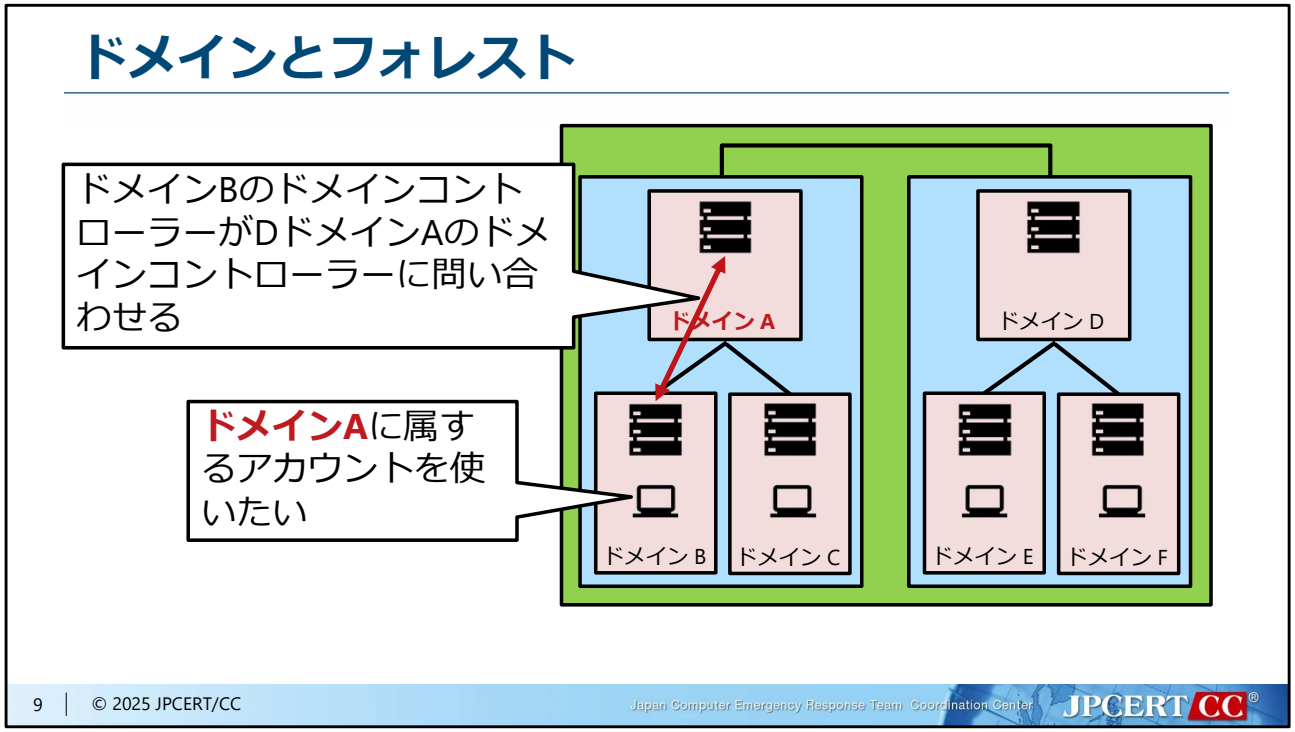
- ドメインの親子関係のみで形成された構造
- 子は親のサブドメインを用いる
- 事業部制・独立部隊がいる・子会社etc...

フォレスト

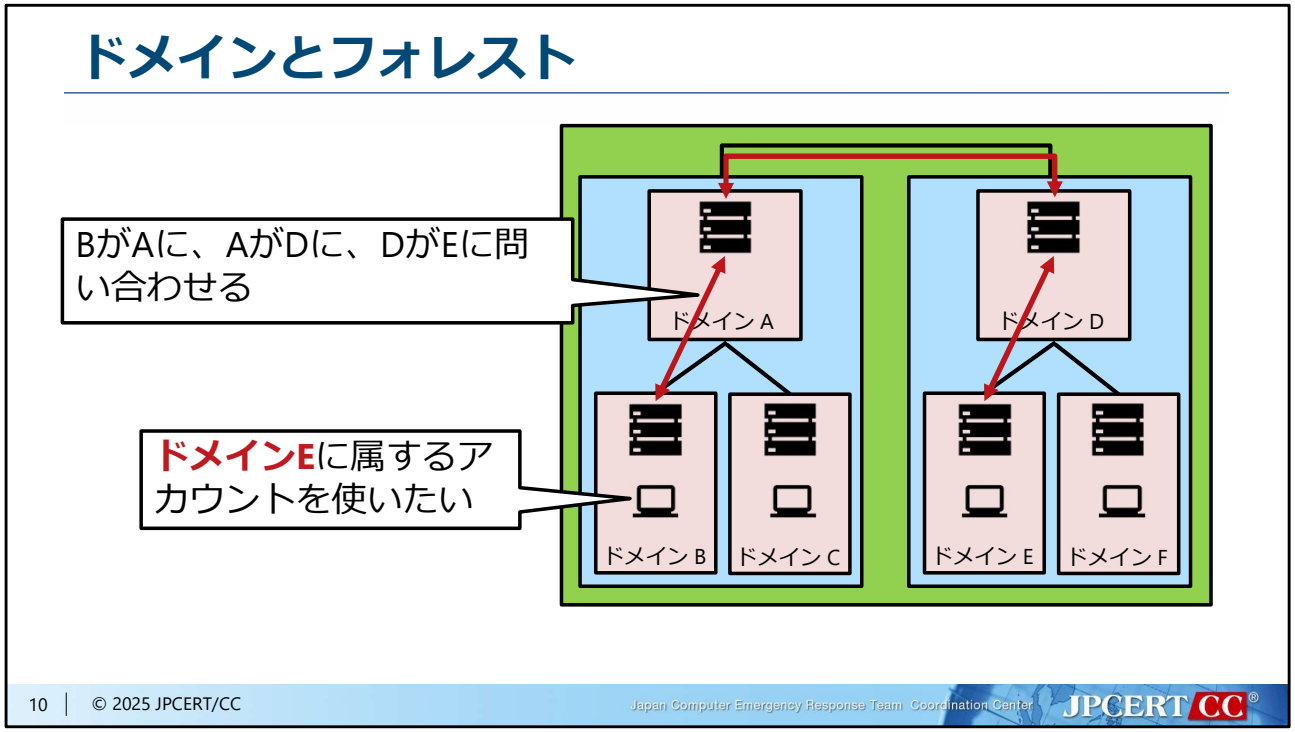
- ツリー同士の信頼で形成された構造
- 信頼関係にあるドメインに命名規則はない
- 企業合併・子会社etc...



ドメインコントローラーが管理する1つの範囲をドメインと呼びます。このドメインは複数台のドメインコントローラーで管理することも可能です。
さらに子会社やグループ会社をドメインで分け、これらの別組織のドメイン同士（サブドメイン）を結び付け、信頼関係を結ぶことで、異なるリソースへのアクセス可能にすることもでき、この信頼関係の構成をドメインツリーと呼びます。
そして、複数のドメインツリーで構成されたものをフォレストと呼びます。フォレスト内のツリー間では全く異なるドメイン名として運用が可能になります。



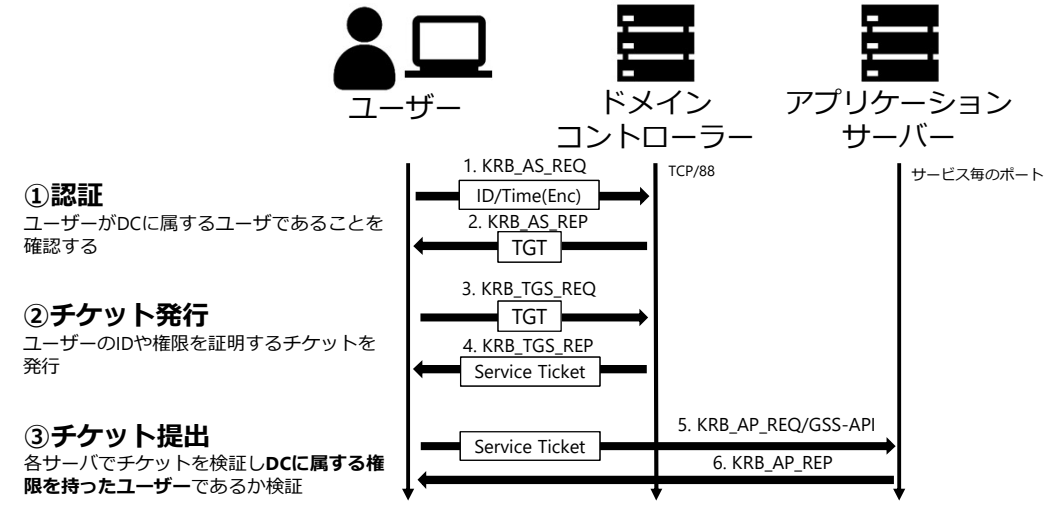
ドメインBのクライアントが、ドメインAのサーバーにアクセスしたい場合この図のような認証確認が行われます。



ドメインBのクライアントが、ドメインEのサーバーにアクセスしたい場合この図のような認証確認が行われます。

ADにおける認証/認可の仕組み

RFC 4120 - The Kerberos Network Authentication Service (V5)



①認証
ユーザーがDCに属するユーザであることを確認する

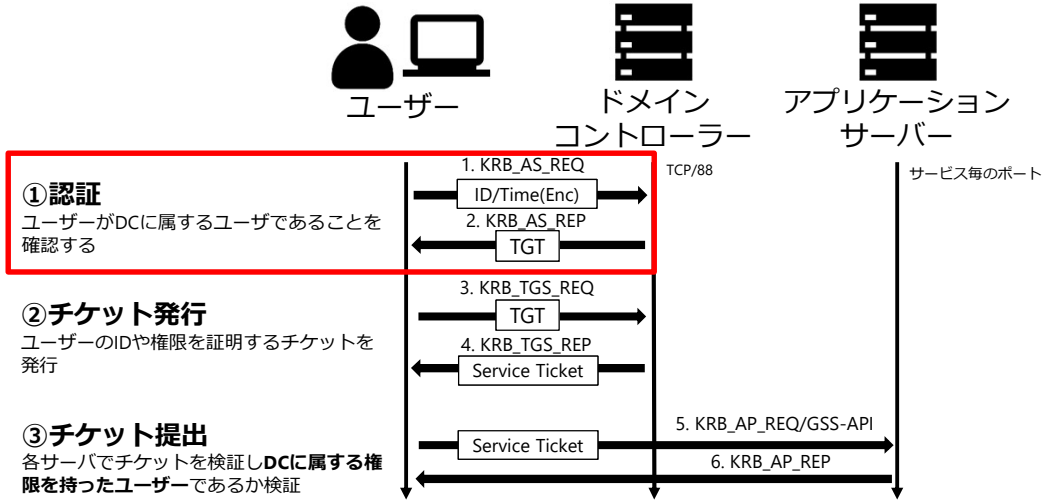
②チケット発行
ユーザーのIDや権限を証明するチケットを発行

③チケット提出
各サーバでチケットを検証し**DCに属する権限を持ったユーザー**であるか検証

ADによる認証はKerberos認証によって実現されています。
以降では、Kerberos認証の流れを図で説明しています。

ADにおける認証/認可の仕組み

RFC 4120 - The Kerberos Network Authentication Service (V5)



①認証
ユーザーがDCに属するユーザであることを確認する

②チケット発行
ユーザーのIDや権限を証明するチケットを発行

③チケット提出
各サーバでチケットを検証し**DCに属する権限を持ったユーザー**であるか検証

①認証：KRB_AS_REQ/REP

1. KRB_AS_REQ

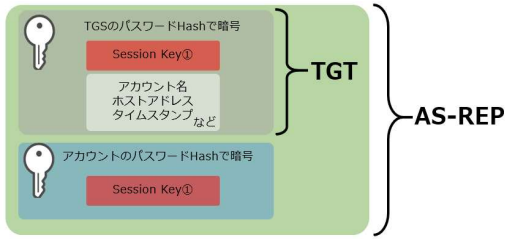
- TGTをもらうための認証情報を含んだリクエスト
  - ✓アカウント名
  - ✓端末のIPアドレス
  - ✓時刻を自身のパスワードハッシュ(NTLM)で暗号化した値
  - ✓nonce（リプレイ攻撃防止のための乱数）

2. KRB_AS_REP

- 時刻を復号し一致していればTGTとSession Key①(チケット用)を発行
- Authentication Server(≒DC)が発行する

TGT(Ticket Granting Ticket)とは

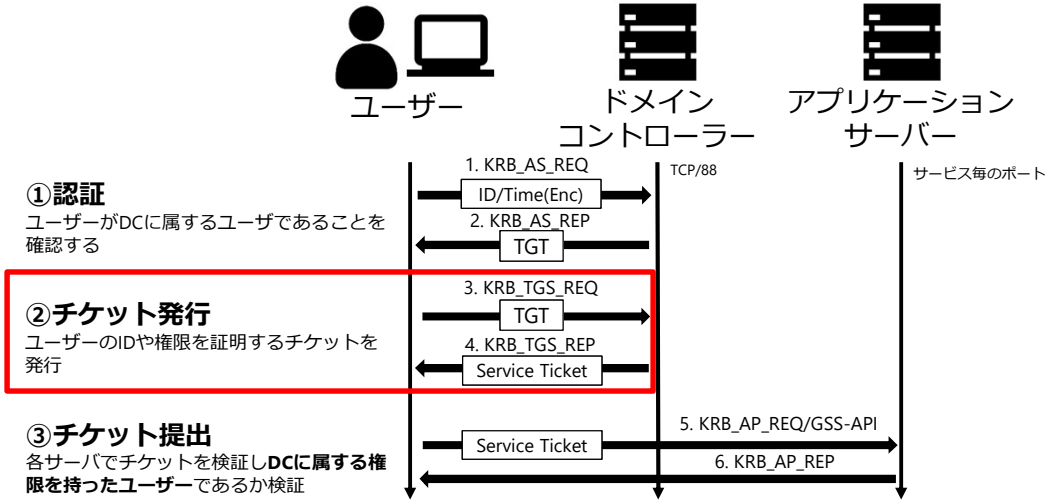
サーバー利用時のチケット発行に用いるための、最初の認証で発行されるチケット(Service Ticketを要求するTicket)



※1 ADはユーザーのPWを知っているので時刻を暗号化/復号できる
※2 ユーザーはkrbtgtのPWを知らないのでTGTを復号できない。
出典: https://www.mbsd.jp/research/20190514/password1/

ADにおける認証/認可の仕組み

RFC 4120 - The Kerberos Network Authentication Service (V5)



①認証
ユーザーがDCに属するユーザであることを確認する

②チケット発行
ユーザーのIDや権限を証明するチケットを発行

③チケット提出
各サーバでチケットを検証し**DCに属する権限を持ったユーザー**であるか検証

②チケット発行：KRB_TGS_REQ/REP

3. KRB_TGS_REQ

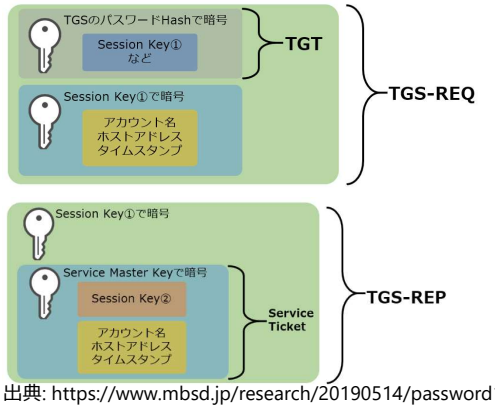
- Session Key①でアカウント名等を暗号化して送信
- サービス プリンシパル名 (SPN)でサービスを指定 (Session Keyで暗号化)
- SPNはアプリケーションサーバ(内で動くサービス）を特定するためのIDで、DC内で一意

4. KRB_TGS_REP

- TGSの暗号鍵（krbtgtのPW=TGS既知の文字列）によってTGTを復号して検証できる
- 検証結果が正しければ、Service Ticketをユーザに送信
- Session Key②(サービス用)を発行

Service Ticketとは

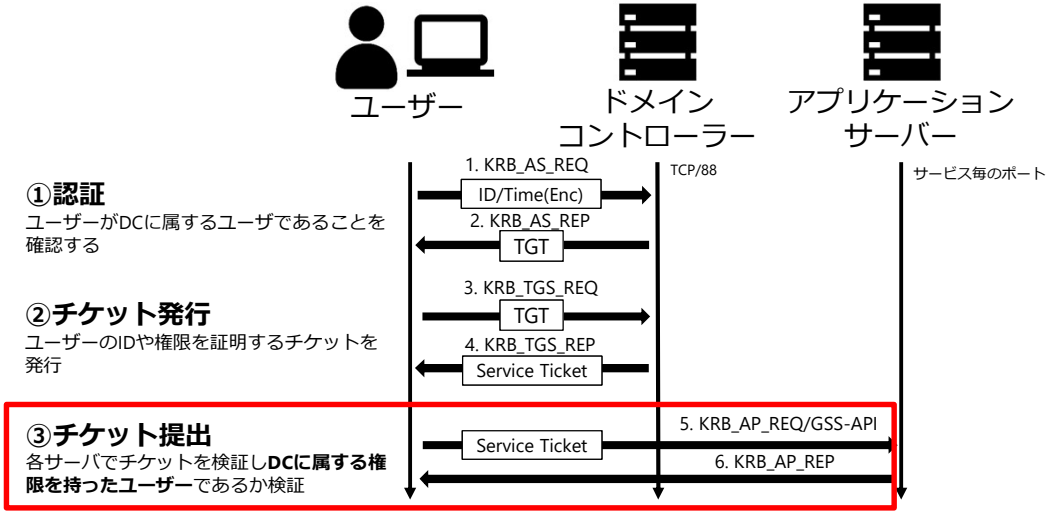
対象サービスで使えるアカウントを認証するためのチケット



出典: https://www.mbsd.jp/research/20190514/password1/

ADにおける認証/認可の仕組み

RFC 4120 - The Kerberos Network Authentication Service (V5)



①認証
ユーザーがDCに属するユーザであることを確認する

②チケット発行
ユーザーのIDや権限を証明するチケットを発行

③チケット提出
各サーバでチケットを検証し**DCに属する権限を持ったユーザー**であるか検証

③チケット提出：KRB_AP_REQ/REP

5. KRB_AP_REQ

- Service Ticketを送信して認可を求める
- Session Key②(サービス用)は別途記録

6. KRB_AP_REP

- 認証結果を返す
- Session Key②で暗号化
- subkey等後続通信用の鍵を返す

通信に使用するポート/プロトコル

アプリケーション毎に異なるポート/プロトコルを利用

- ✓ HTTP/SMB/LDAP etc…
- ✓ GSS-APIという規格をKerberosで実装したものが使われる

確認演習：正常系におけるKerberos認証

演習

演習

1. Wiresharkをインストールして、パケットキャプチャしたデータを閲覧

- 演習ディレクトリ内のSMB.pcappngを見る
- Session Setup Requestでチケットが送信されていることを確認
  - ✓SMB2->Security Blob->GSS-API->Simple Protected Negotiation->negTokenInit->krb5_blob->Kerberos->ap-req->ticket
  - ✓enc-part以上は掘り下げて閲覧できない(cipherパラメータを展開できない)

2. configを設定して再度閲覧

- Preference->Protocols>KRB5
- Try to decrypt Kerberos blobsをチェック
- Kerberos keytab fileにtest.keytabファイル指定
- test.keytabは**アカウントのNTLMハッシュ**の詰め合わせ

問題

なぜ1ではパケットの中身が見れず、2で見れたか？

① このパケットはKRB_(AS|TGS|AP)_(REQ|RES)のどれに当たるか

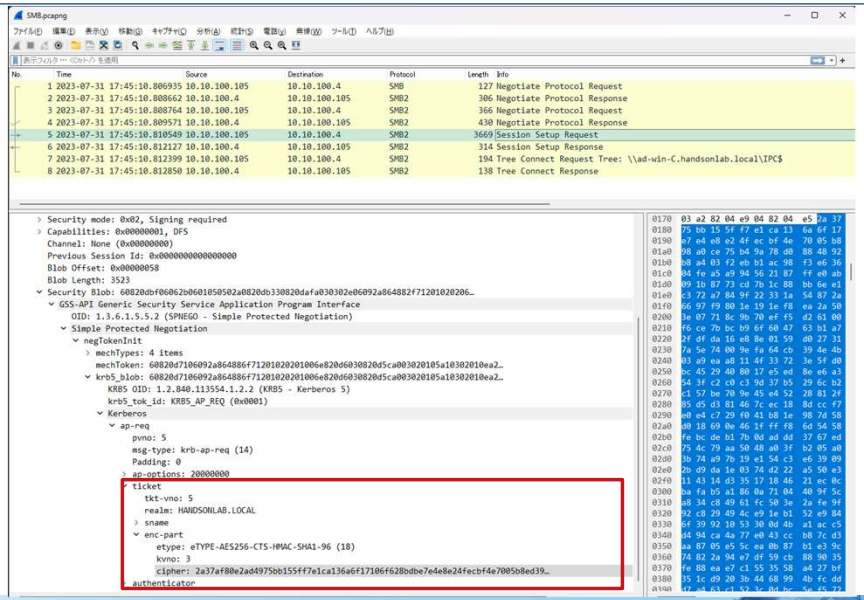
② 何の情報が何の鍵で暗号化されていたか

③ Wiresharkはどういった処理を行っているのか

Kerberos認証の仕組みを、実際の通信パケットから理解する演習です。
Wiresharkを使ってSMB通信パケットを確認してください。

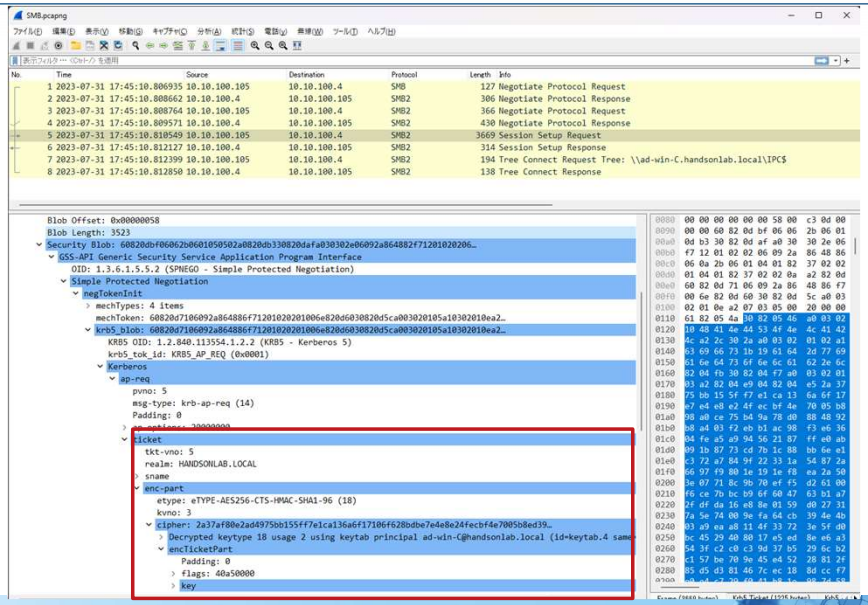
確認演習：config設定前

演習



確認演習：config設定後

演習



確認演習：回答

演習

問題

なぜ1ではパケットの中身が見れず、2で見れたか？

① このパケットはKRB_(AS|TGS|AP)_(REQ|RES)のどれに当たるか

② 何の情報が何の鍵で暗号化されていたか

③ Wiresharkはどういった処理を行っているのか

答え

1では鍵が分からないのでService Ticketを復号できないが、2ではkeytabに鍵が保存されているので復号できた

① このパケットはKRB_(AS|TGS|AP)_(REQ|RES)のどれに当たるか

✓KRB_AP_REQ（Service Ticketの提出リクエスト）

② 何の情報が何の鍵で暗号化されていたか

✓**Service Ticket**が**SPNに紐づく鍵**で暗号化されている

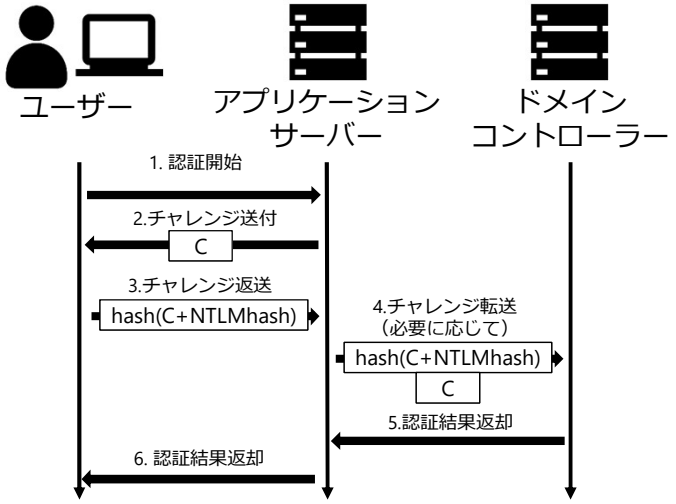
③ Wiresharkはどういった処理を行っているのか

✓keytabに記録されたSPNに紐づく鍵で復号

このパケットは、認証結果を返すKRB_AP_REQであり、Sessin keyで暗号化されているので、そのままでは内容を確認することはできません。そのため、Wiresharkにキーを与えてあげれば、その中身を確認することができるようになります。

その他の認証方式

NTLM認証



Kerberos認証以外にもNTLM認証があります。この認証方式で運用された認証を回避する複数の攻撃手法が確立しており、またマイクロソフトが本認証方式を廃止することがアナウンスされています。
https://jpwinsup.github.io/blog/2024/08/22/ActiveDirectory/Authentication/retireNTLM/

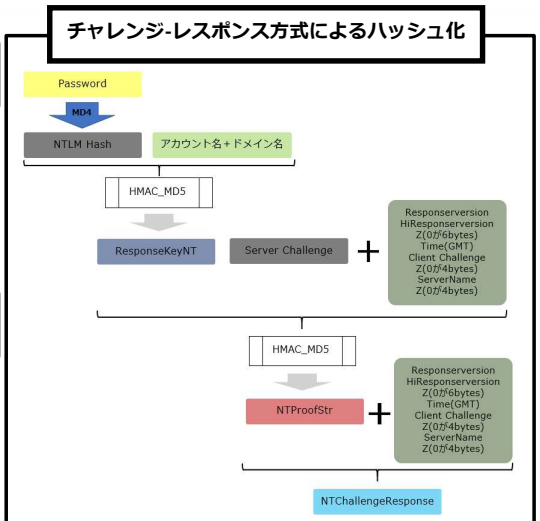
NTLM認証とは

チャレンジ-レスポンス方式

- ランダムな文字列+パスワードをハッシュ化
- サーバ側で同様の処理を行いパスワードと一致するか検証

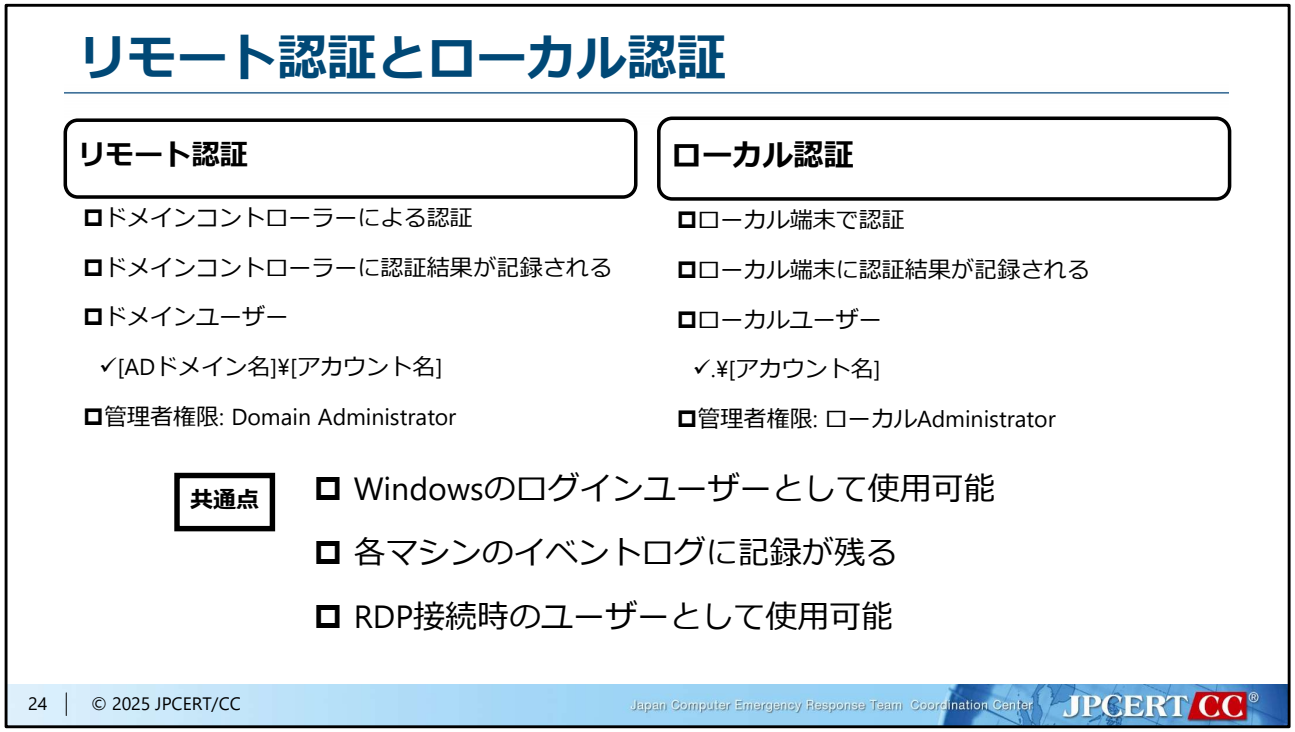
NTLM認証における実装

- パスワードではなくNTLM Hashを用いる
- アカウント名とドメイン名も付与する
- HMAC-MD5を用いる

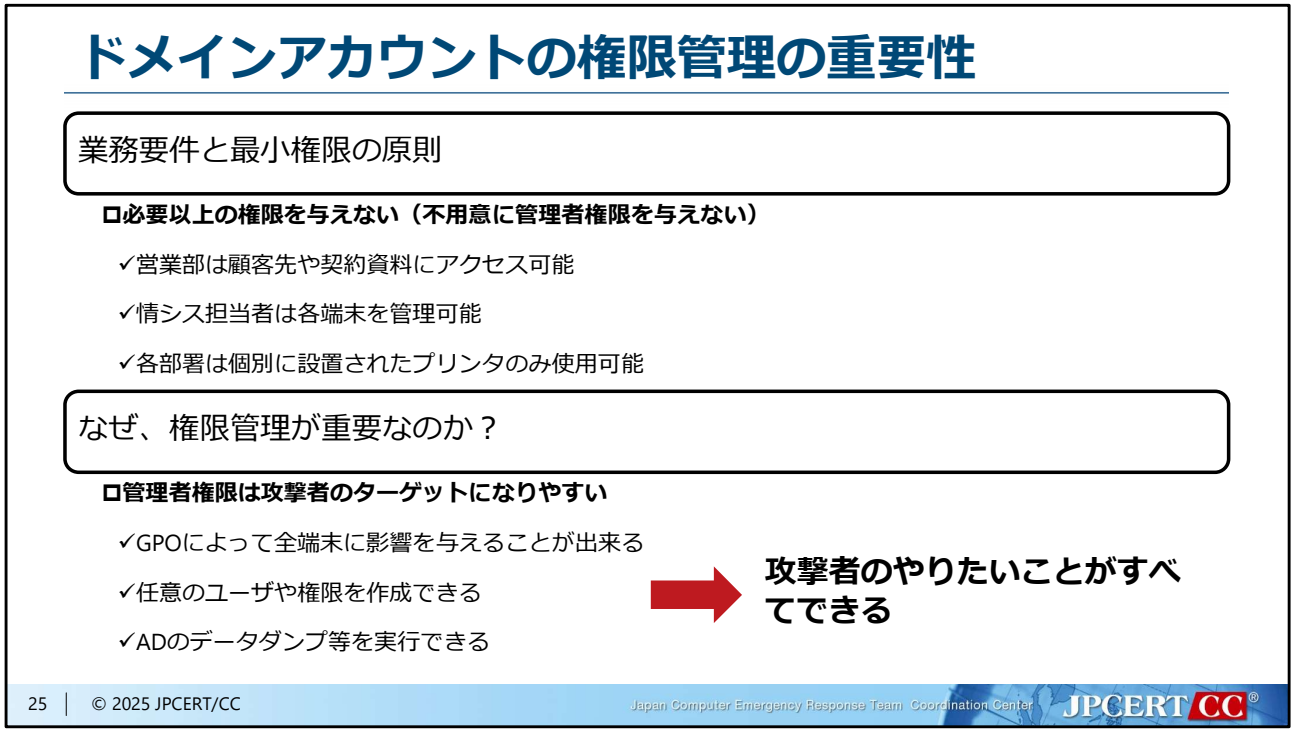


出典: https://www.mbsd.jp/research/20190514/password1/

NTLM認証は、チャレンジ・レスポンス方式の認証でパスワードをハッシュ化・暗号化して送受信します。
そのため、パスワードを知らなくても、ハッシュ化されたパスワード情報を入手できれば悪用できるという問題点があります。



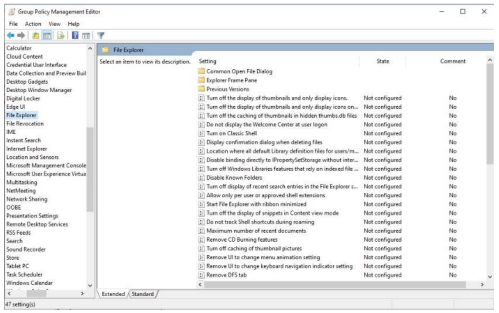
ここまで説明してきた認証方式は、ドメインコントローラーによるリモート認証です。
対して、Windows OSではローカル認証も可能です。これは、端末上で作成されたユーザーにログオンする仕組みで、端末自体にはアクセス可能になりますが、他のWindows ネットワーク上のリソースにはローカル認証したアカウントではアクセスできません。



ドメイン内で使用するアカウントの権限は重要です。
もしも、AdministratorsやDomain Adminsグループの所属するユーザーが使用している端末が乗っ取られたら、そのWindowsネットワーク内を管理者権限であらゆる操作ができてしまいます。
そのため攻撃者は、この管理者権限を持つユーザーにアクセスするために様々なシステムに侵入を繰り返します。
通常の端末やサーバーで使用するユーザーの権限は最小限にして、その端末が乗っ取られたとしてもWindowsネットワーク全体への影響が及ばないようにする必要があります。

グループポリシーオブジェクト(GPO)

ドメインに参加している端末の設定をドメインコントローラー側で管理する仕組み



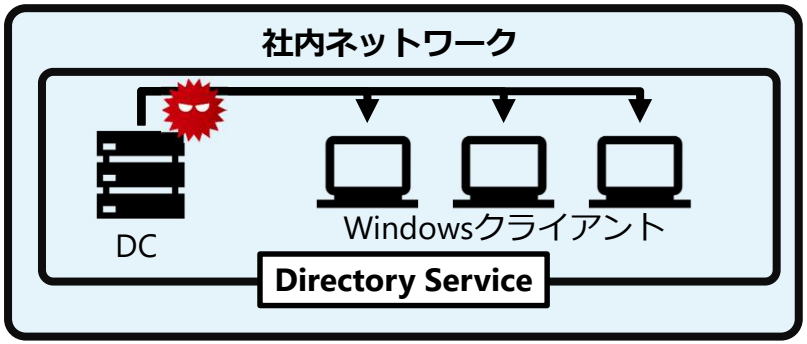
- ルールを定めたGPOをDCの各グループにリンク
  - ✓端末毎の**ローカルGPO**と**DCの持つGPO**がある
  - ✓ローカルGPOが通常優先されるが、DC側から強制することも可能
- GPO保存場所
  - ✓¥¥[ドメインコントローラー]¥SysVol¥[ドメイン名]¥Policies¥
  - ✓XML形式で保存
- 通常は専用エディタを使って操作

Windowsには、ドメインに参加している端末の設定をドメインコントローラー側で管理するグループポリシーオブジェクトという仕組みがあります。
これを使用すると、各端末をリモートから設定したり、アプリケーションのインストールなどができます。
この機能を悪用して攻撃者が、マルウェアを各端末に配信することもあります。

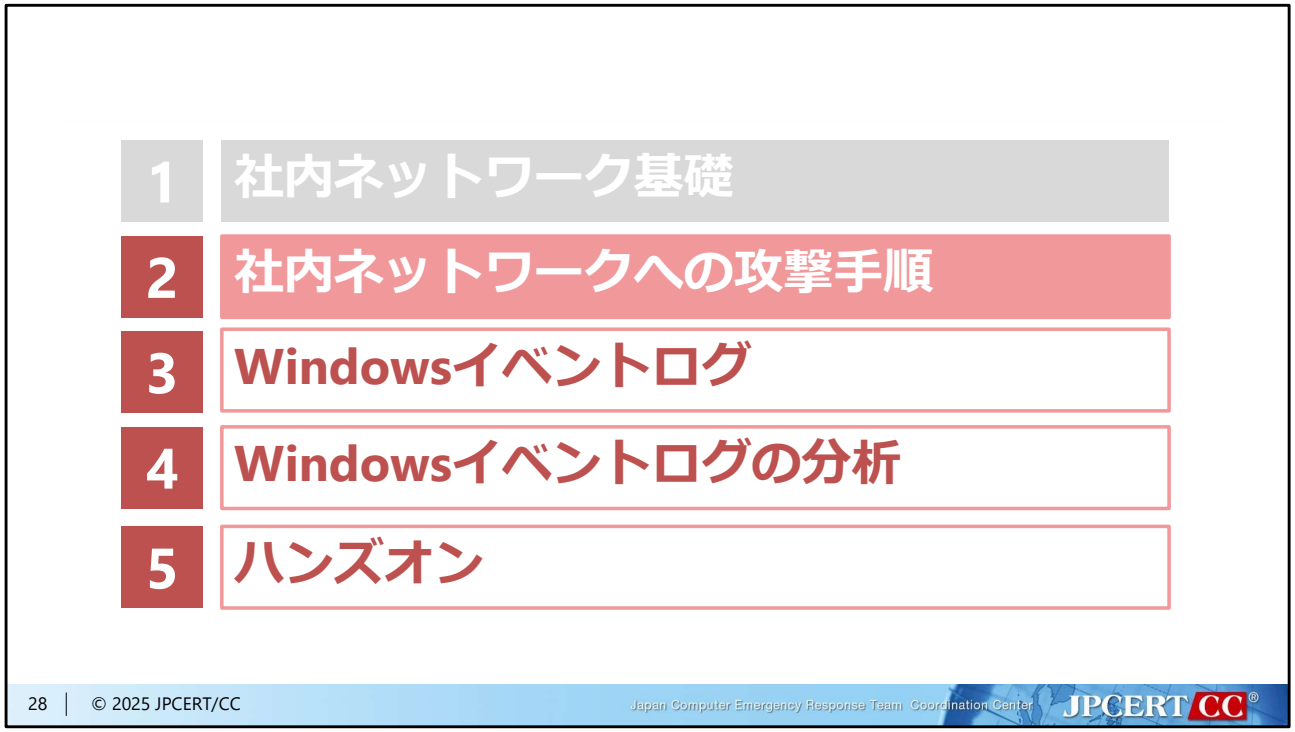
SYSVOLを悪用したマルウェア拡散

Sysvolとは

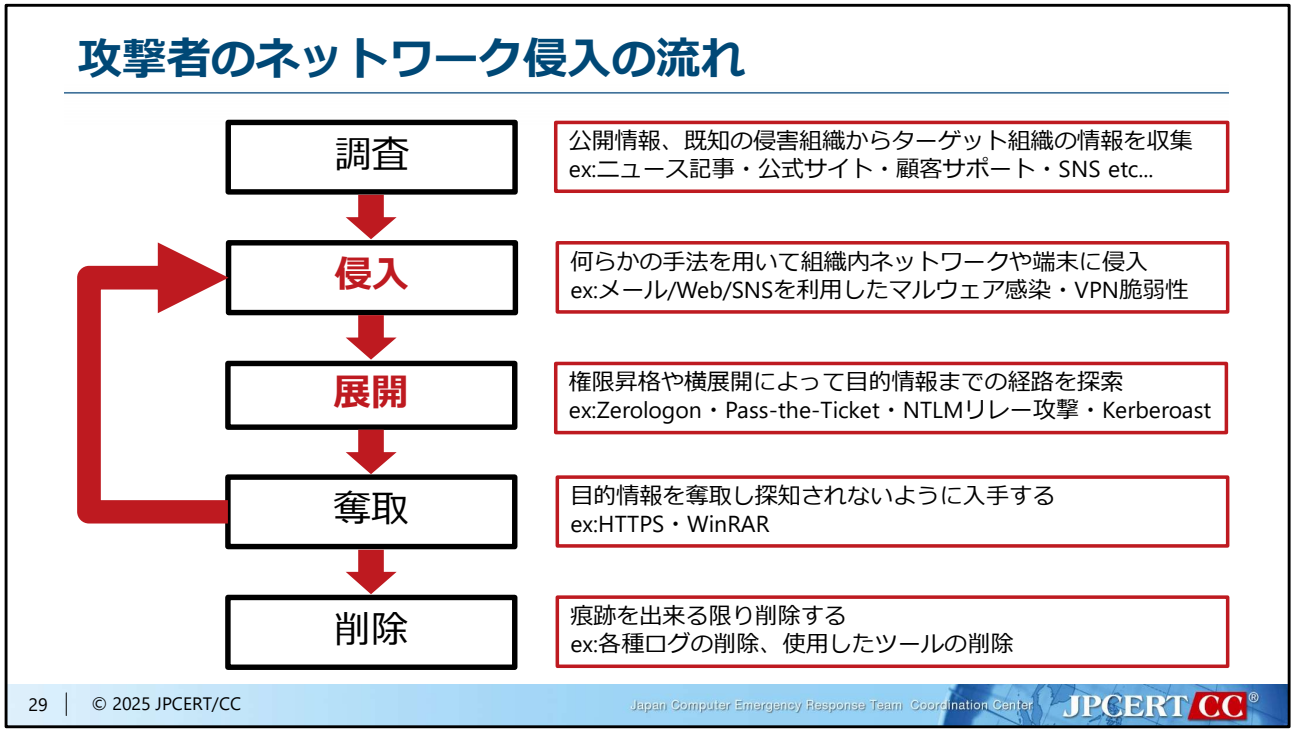
- ドメインコントローラーに存在する共有フォルダー
- クライアントなどに配布するスクリプトなどが保存される
  - ✓ クライアントへのマルウェア拡散に悪用される場合がある
- スクリプト内にパスワードなどの記載がある場合は注意



グループポリシーは、通常SYSVOLフォルダ（C:¥Windows¥SYSVOL¥domain）から共有されます。
このフォルダから、各種設定やスクリプト、アプリケーションなども配布されるのですが、このフォルダに保存されるスクリプトには重要なシステムのアカウント・パスワードなども含まれていることも多く、攻撃者はこのフォルダからアカウント情報を収集する可能性があります。

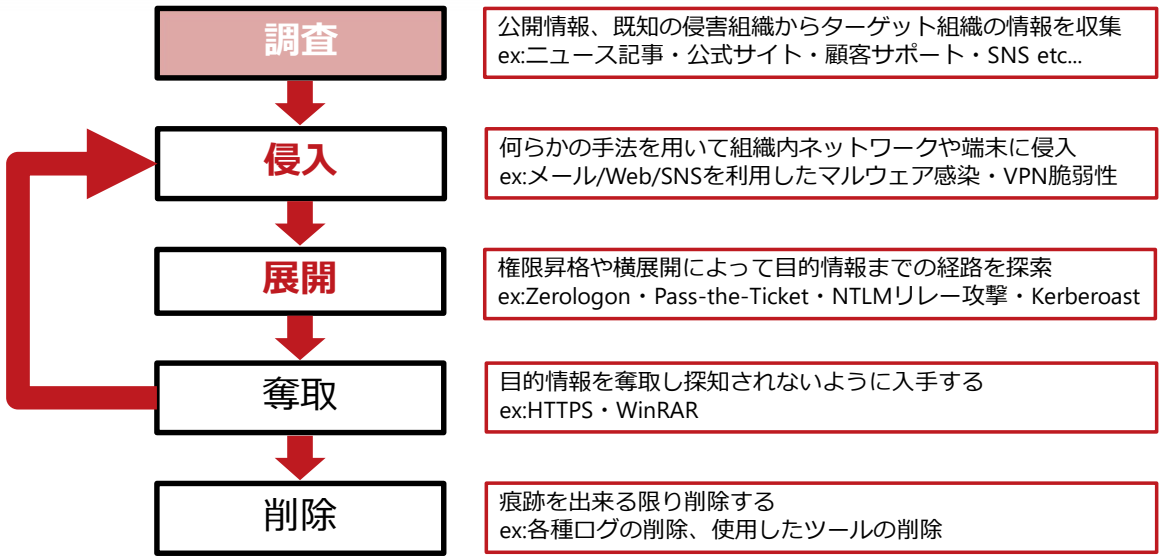


次に、社内ネットワークへの侵入手法について説明します。



攻撃者のネットワーク侵入から目的達成までの活動の流れをフロー化したのがこの図です。
以降では、各パートでよくみられる攻撃手法について解説します。

攻撃者のネットワーク侵入の流れ



調査

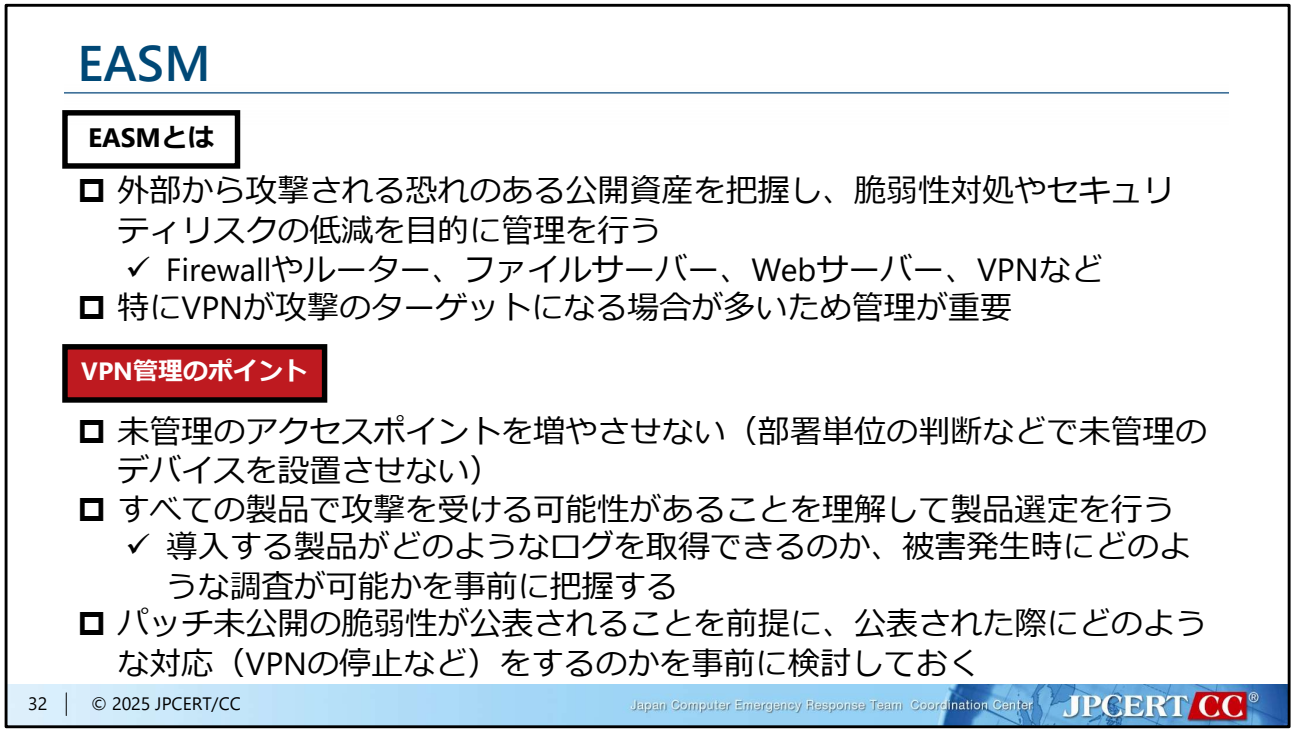
公開情報から相手を調査するフェーズ

- 外部公開資産があるか
  - ✓Firewall、VPN、ルーター、Webサーバーなど
  - ✓RDP、SSHなどアクセスポイントが公開されていないか
- メールアドレス、SNSなど従業員へのコンタクト手段
- すでに侵害された組織からの情報をもとに調査

検知は現実的ではないが**対策は可能**

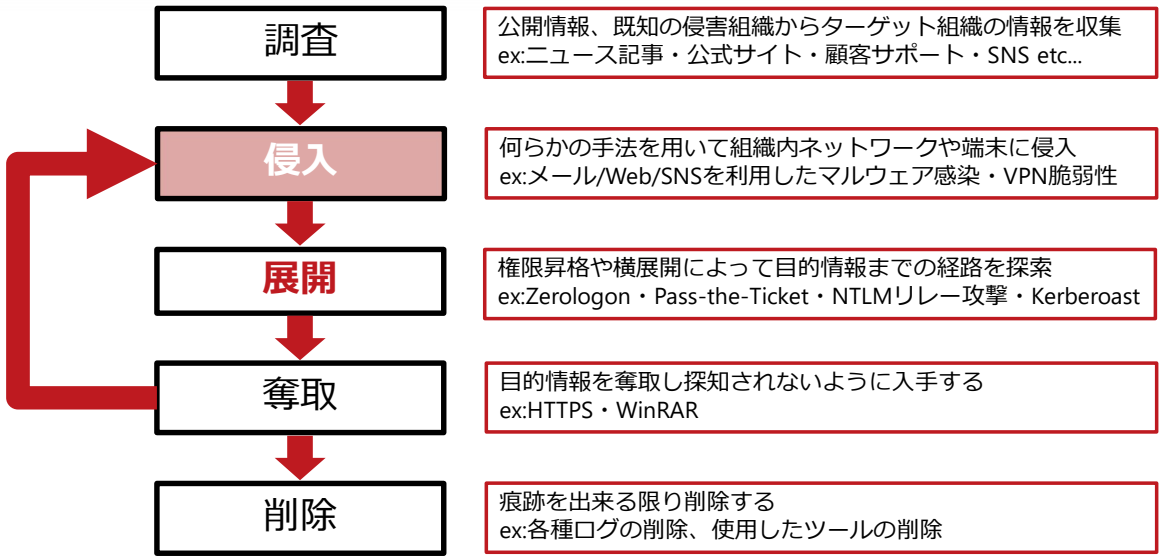
- EASM(External Attack Surface Management)
- 公開メールアドレスの調査
- SNS利用時の注意点を周知

調査フェーズでは、攻撃者はネットワークへの侵入経路を探索します。
最近では、ご存じの通りVPNやFirewallなど外部公開資産が攻撃のターゲットになることが多く、攻撃者はそのような外部からのアクセス先がないかを探索していると考えられます。



外部から攻撃される恐れのある公開資産を把握し、管理することは昨今のセキュリティ対策の中でも重要になってきています。
攻撃者は、公開直後の脆弱性を悪用してVPNに不正ログインしたり、ゼロデイ脆弱性を使って侵入するケースを多く確認しています。
VPNが増えれば増えるほど、攻撃されるリスクを増やすことにつながることを理解し、非管理のアクセスポイントを増加させないようにしてください。
また、どの製品を使えば攻撃されるリスクを抑えられるということはなく、すべての製品が攻撃のターゲットになる可能性があります。そのため、管理している製品の脆弱性が出ることを想定して対応フローを整備しておくことも重要です。

攻撃者のネットワーク侵入の流れ



侵入

実際に攻撃を行って権限を奪取するフェーズ

- 外部公開資産の脆弱性を悪用
- メール経由でマルウェアを実行させる
- SNS経由で従業員にコンタクトし、マルウェアを実行させる

侵入への対策

- 外部公開資産の洗い出しと脆弱性管理
- セキュリティ製品の導入
- セキュリティ教育
- ログ分析

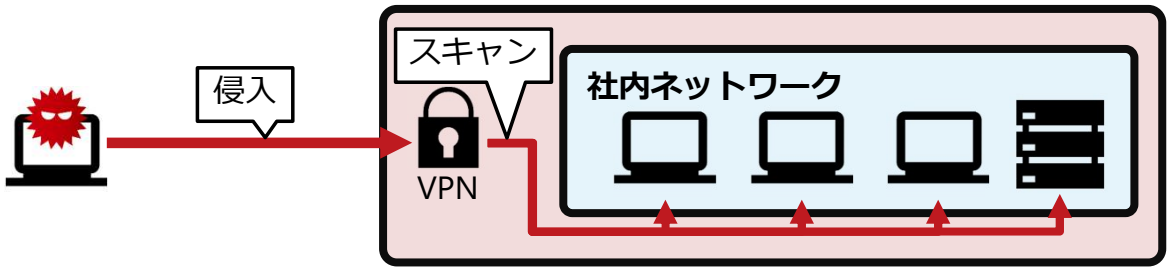
100%侵入を防ぐことは難しいが、対策を取ることでリスクの低減につながる

侵入には多数のパターンがあります。
調査フェーズで説明した、外部公開資産の脆弱性を悪用する以外にも、メールでの攻撃やSNS経由の攻撃があります。

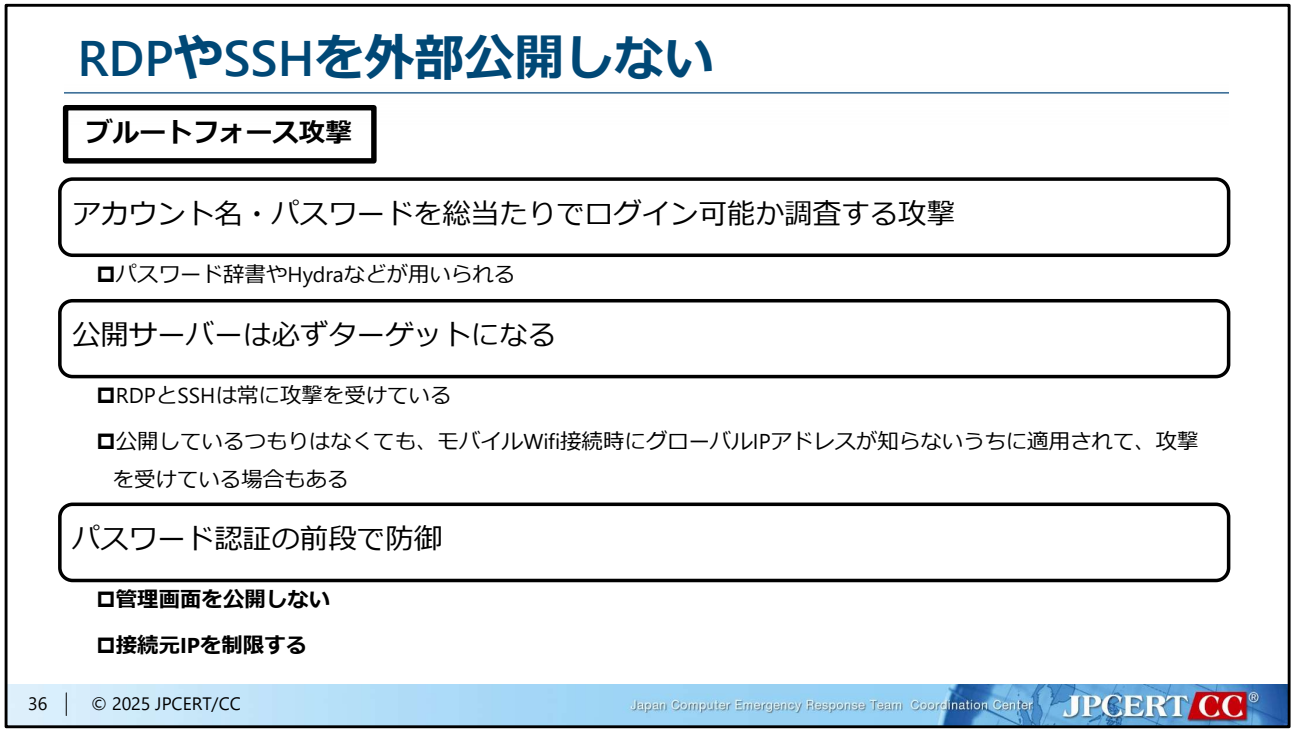
外部公開資産の脆弱性を悪用

VPNへの攻撃

- 狙われることが多いVPN製品
  - FortiGate製品、Ivanti製品、SonicWall製品、Palo Alto製品、Array Networks製品
- VPN機器に侵入した攻撃者は、**VPNから社内ネットワークに対して、ネットワークスキャン**を行い侵入できるターゲットを見つける



外部公開資産経由の攻撃の場合、攻撃者はVPNなどに侵入が成功するとその機器経由で内部ネットワークにスキャンを行い、侵入するターゲットを探索します。
そのため、VPNから直接アクセスできる範囲を制限したり、VPNから不要な通信が出ていないかの監視をするなどの対策が考えられます。



RDPやSSHサーバーを外部公開しないのはセキュリティ対策の基本です。
これらのサーバーは、公開したら必ずパスワード総当たり攻撃をうけます。脆弱なパスワードを使っていれば、侵入されてしまいます。
また、公開していないつもりでも、管理不十分で意図せず公開されてしまっているテストサーバーやモバイルWifi接続時にグローバルIPアドレスが知らないうちに適用されて公開されてしまっているRDP端末などに侵入されるケースもあります。
このようなことにならないように、普段から強固なパスワードを使う・SSHサーバーは認証キーを使用する・アクセス元IPアドレスを制限するなどの対策が必要です。

SNS経由の攻撃

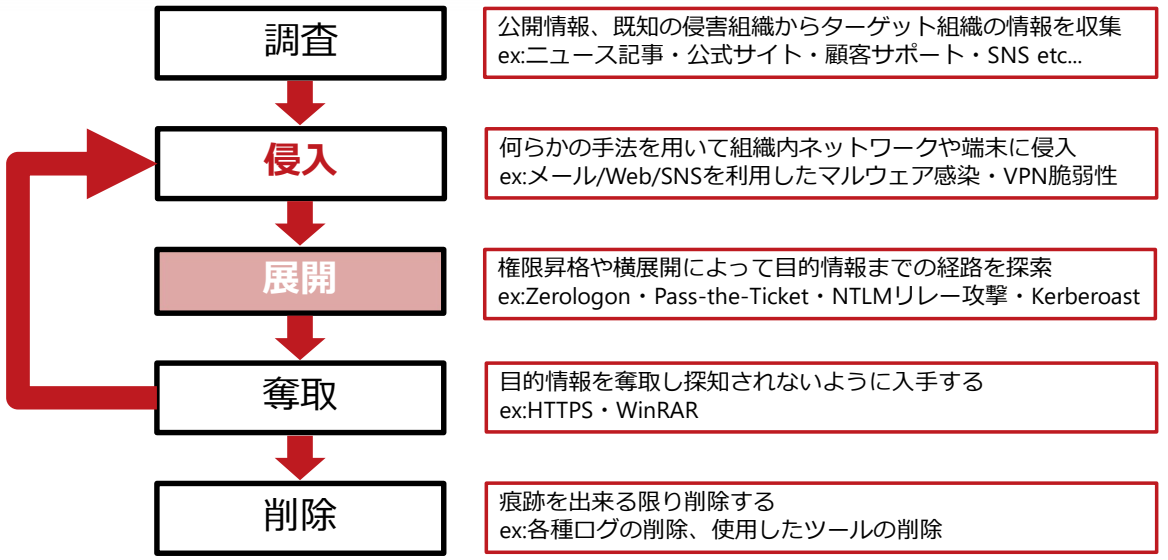
LinkedIn経由の標的型攻撃

- 攻撃者が、従業員に対してSNS経由でマルウェアを送信してくる。
- 業務端末でSNSを使用している場合は、注意が必要。

https://blogs.jpcert.or.jp/ja/2025/01/initial_attack_vector.html

SNS経由の攻撃の場合、従業員の私用アカウントが攻撃のターゲットになります。
そのため、インシデント発生時の侵入フェーズは社内ネットワークではなく、従業員の自宅など外部で発生する可能性があります。マルウェア感染した端末をVPNで社内ネットワークに接続することで、展開フェーズに移行し社内ネットワークへの侵入が発生します。
未監視領域で発生するインシデントであるため、初動検知が難しく、このようなインシデントの場合は、展開フェーズ以降で対処する必要があります。

攻撃者のネットワーク侵入の流れ



展開

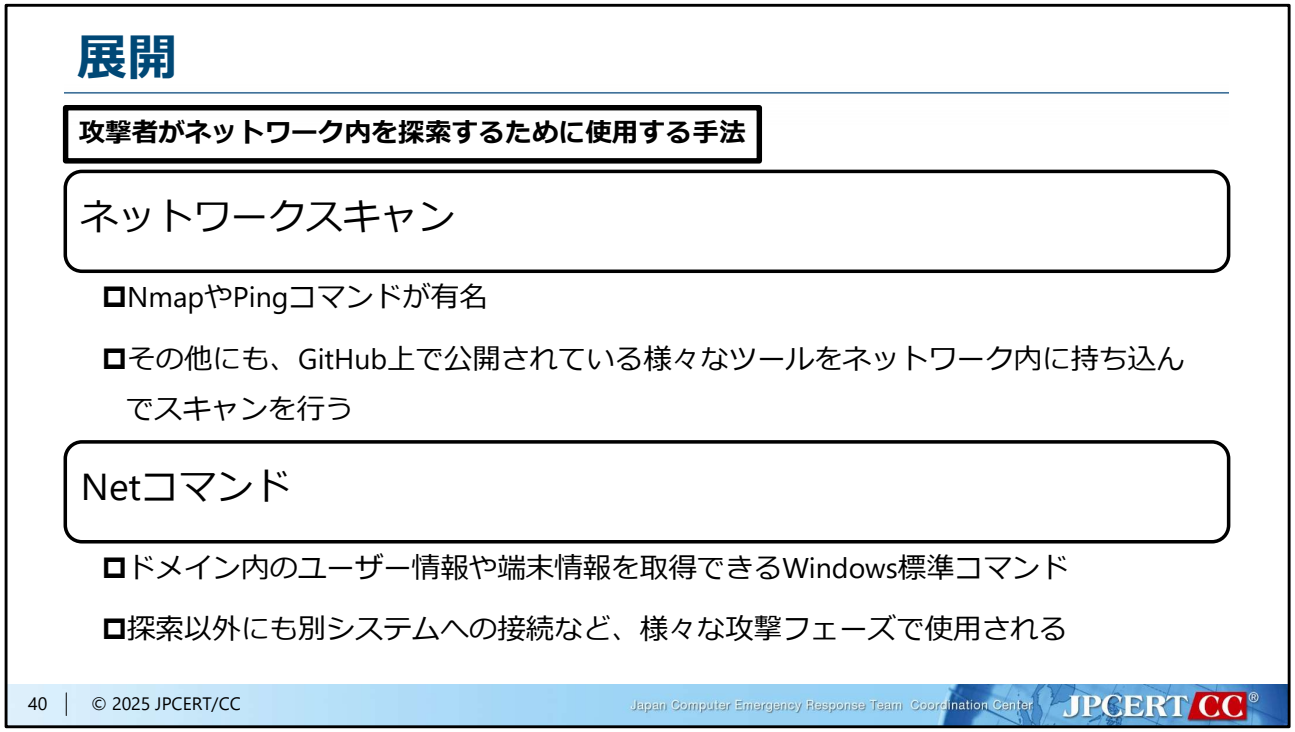
管理者権限の奪取・他のシステムへの侵入

- 別のシステムに侵入するために管理者権限を奪取
  - ✓見つけたクレデンシャルを別システムでも使う
- 踏み台となっている端末から重要なサーバへ侵入

展開への対策

- 設計段階からセキュリティを意識
  - ✓最小権限の原則：余計な権限を持たせない
  - ✓公開サーバと重要な資産を持つサーバはネットワークで分離しておく
  - ✓パスワードを使いまわさない
  - ✓一般端末でDomain Administrator権限（または管理者権限）を持つドメインユーザーを使用しない

展開フェーズでは、社内ネットワークでの横展開（Lateral Movement）です。
このフェーズでも、様々な攻撃手法があり、以降でいくつか取り上げて説明します。



展開フェーズで最初に実施されるのは、侵入可能な他の端末を探索することです。
これには、Windowsにデフォルトで使用可能なPingコマンドやNmap、それ以外にもGitHub上で公開されている様々なツールが使用されます。
そして、Windowsネットワークの探索にはWindowsにデフォルトで使用可能なNetコマンドが多用されます。このコマンドを使用すれば、ドメイン内のアカウントや端末情報を一覧することができます。
さらに、Netコマンドを使えば、他の端末へのアクセスも可能になるので、攻撃者はあらゆる場面でNetコマンドを多用しています。

攻撃者が悪用するWindowsコマンド: https://blogs.jpcert.or.jp/ja/2015/12/wincommand.html

展開に使用される攻撃手法

Windows/AD環境における攻撃手法

- **システム内のパスワードを記載したファイルの奪取・共通アカウント**
- Pass-The-Hash/Ticket
- Kerberoast
- 脆弱性（Zerologonなど）
- NTDSダンプ

Linux環境における攻撃手法

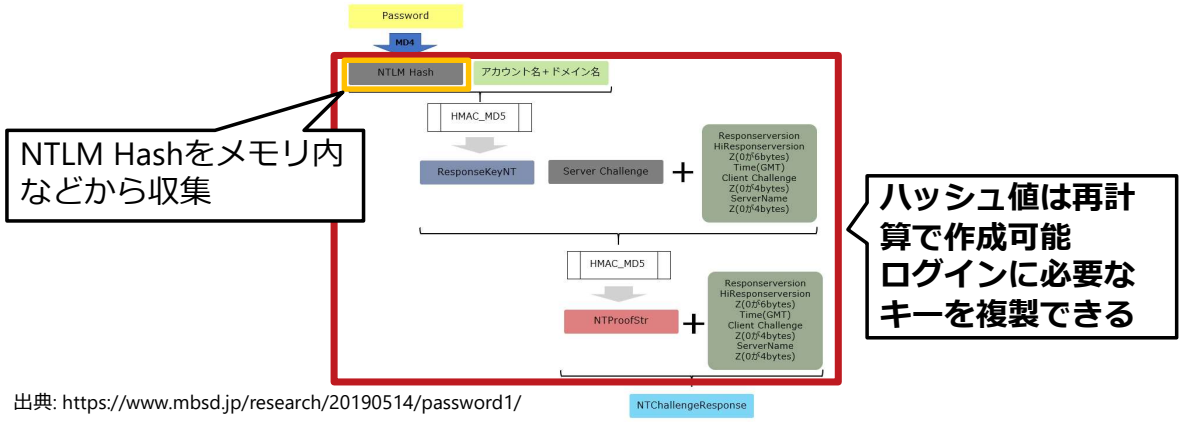
- Kernel Exploit
- ブルートフォース攻撃（SSHへのログイン）

ターゲットとなる端末が見つかったら、次はその端末への侵入が試みられます。
このフェーズで最も多いのが、共通アカウントによる侵害です。
キッティングのためにすべての端末で同じドメインアドミンアカウントでログインしていた場合、その端末に残っているアカウントを使って別の端末にもログインができてしまいます。
また、システム内にパスワードを記載したスクリプトなどが残っていたことで、パスワードが漏洩し侵入されることもあります。

Pass-the-Hash

Pass-the-Hashとは

- ハッシュ化されたパスワード情報を盗み、それを使用して同じネットワーク上に新しいユーザーセッションを作成し、ログインする攻撃



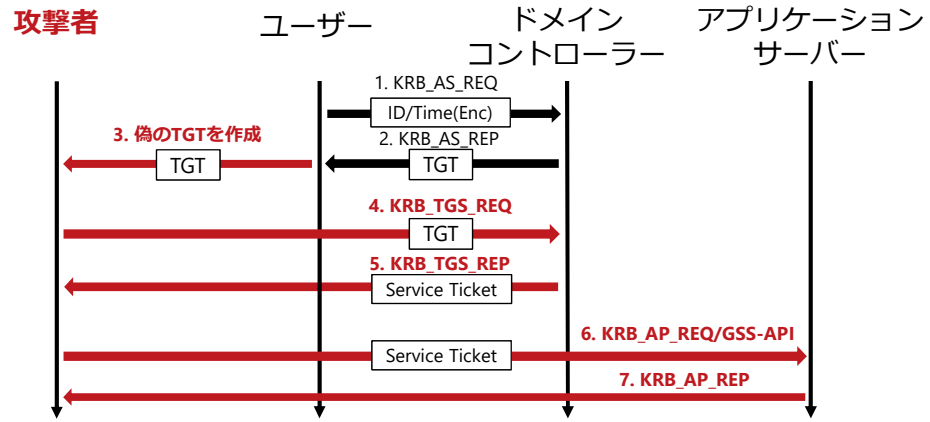
出典: https://www.mbsd.jp/research/20190514/password1/

Pass-the-Hashは、NTLMが有効な環境で使用可能な攻撃手法です。
メモリ内などから、ハッシュ化されたパスワード情報を盗み、それを使用して同じネットワーク上に新しいユーザーセッションを作成し、ログインする攻撃です。
NTLMを無効化することが対策となります。

Pass-the-Ticket

Pass-the-Ticketとは

- Kerberos認証で使用される認証チケットを偽装し、それを使用して同じネットワーク上に新しいユーザーセッションを作成し、ログインする攻撃



Pass-the-Ticketは、Kerberos認証で使用される正規の認証チケットをメモリなどから窃取し、正規のユーザになりすまして攻撃を行う。

この偽の認証チケットを作成する際に使用するチケットの種類によって以下の2種類の偽チケットが存在します。
- Golden Tickets: TGTを不正に作成する（ドメイン管理者権限でなりすましが可能
- Silver Ticket : Service Ticketを不正に作成する（各サーバー管理者の権限でなりすましが可能）

どちらのチケットの場合も、有効期間が10年と長いため、一度発行されてしまうと強制的にリセットするまで継続的に悪用されてしまいます。なお、パスワードのリセットは2回行うことで、チケットが無効になります。
https://learn.microsoft.com/ja-jp/windows-server/identity/ad-ds/manage/forest-recovery-guide/ad-forest-recovery-reset-the-krbtgt-password

NTDSダンプ

NTDSダンプとは

- 認証情報が含まれるNTDS.ditデータベースファイルをダンプ・解析することで、認証情報を窃取する。
- NTDS.ditなどは、ボリュームシャドーコピー（VSS）からコピー可能。

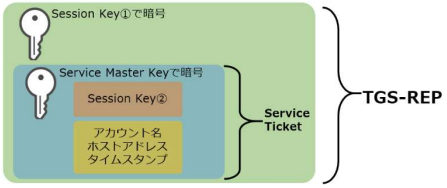
```
# NTDS.ditとレジストリハイブをVSSからコピー
vssadmin create shadow /for=C:
copy ¥¥?¥GLOBALROOT¥Device¥HarddiskVolumeShadowCopy2¥Windows¥NTDS¥NTDS.dit C:¥temp¥
copy ¥¥?¥GLOBALROOT¥Device¥HarddiskVolumeShadowCopy2¥Windows¥System32¥config¥SYSTEM C:¥temp¥


# NTDS.ditからパスワードハッシュを抽出
secretsdump.py -system SYSTEM -security SECURITY -ntds ntds.dit LOCAL
```


NTDSは、ドメインコントローラーに保存されている認証情報などが保存されたデータベースファイルです。
このファイルを持ち出して、解析することで認証情報を入手することができます。通常、NTDSにはアクセスできないため、攻撃者はVSSからファイルを抽出しようとします。

Kerberoast（Kerberoasting攻撃）

Kerberoastとは

- サービスチケットからパスワードを解析する攻撃
  - ✓ サービスチケットの暗号化キーはService Master Key
  - ✓ Service Master KeyはNLTMハッシュ値を元に計算
  - ✓ **オフラインで総当たり解析**
  - ✓ サービスと紐づいたアカウントの**パスワードが脆弱だと乗っ取られる**



出典: https://www.mbsd.jp/research/20190520/password2/

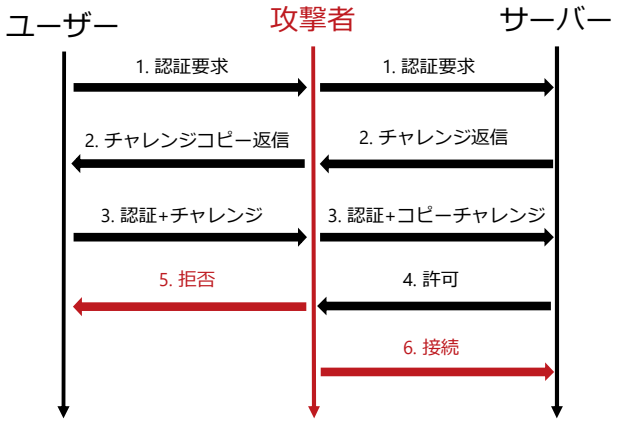
ネットワーク上は正常なやり取りなので検知不可能
（ローカルではLSASSメモリからダンプするためイベントログが残る）

Kerberoastは、Service Ticketからパスワードを解析する方法です。

NTLMリレー攻撃

NTLMリレー攻撃とは

- サーバーとクライアント間のチャレンジレスポンスを窃取し、本来のクライアントに代わって認証を取得する中間者攻撃



NTLMリレー攻撃は、NTLM認証が有効な環境で使用可能な攻撃で、認証時のやり取りを中継してなりすますものです。

認証情報取得ツール：pwdump

パスワードハッシュを取得するツール

- ローカル管理者からドメインユーザへの横展開
- NTLMハッシュ値を取得し、Pass-the-Hash攻撃につなげる

検知

- 顕著なログは残らない
- プロセスの生成と終了から追跡するしかない
- 参考
  - https://jpcertcc.github.io/ToolAnalysisResultSheet_jp/details/PwDump7.htm

ここまでで説明した攻撃手法を実際に実施するツールがいくつか公開されています。

Pwdumpは、端末のNTLMハッシュ値を取得するツールです。

認証情報取得ツール： Mimikatz

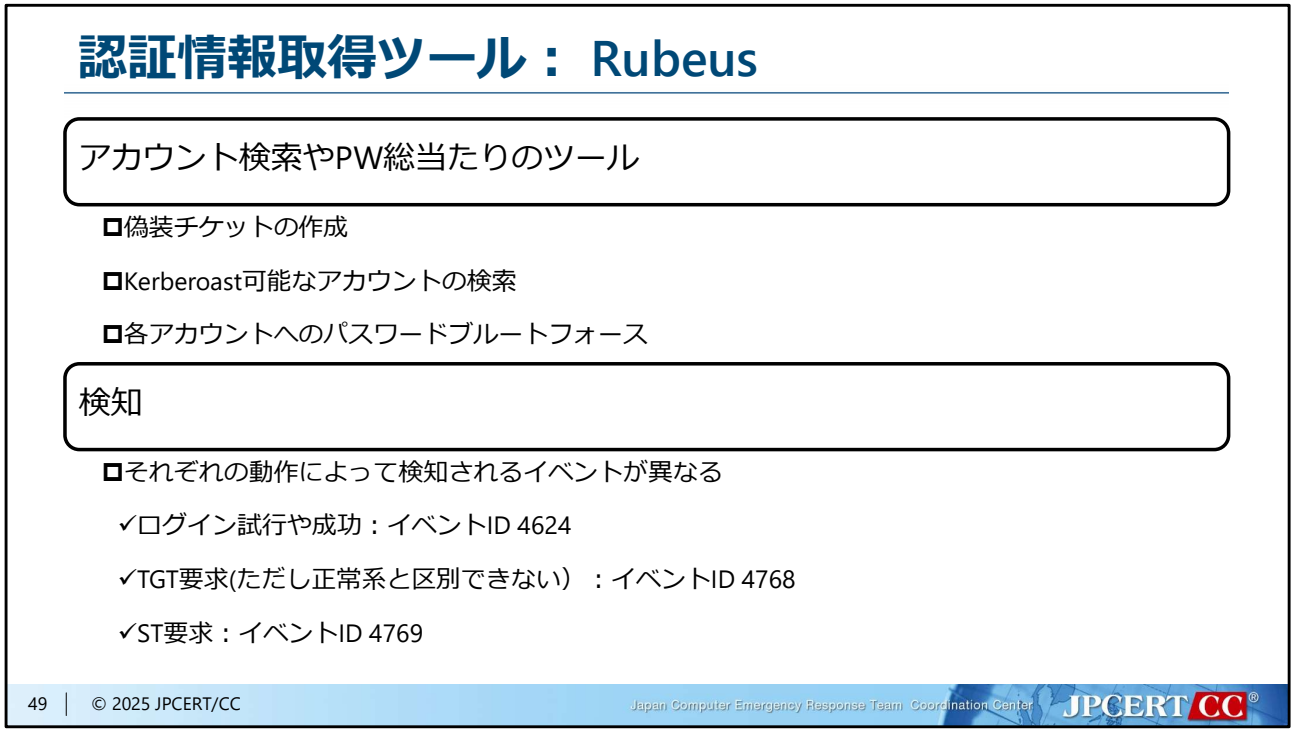
パスワードやチケットの取得に使われるツール

- ローカル管理者からドメインユーザへの横展開
- NTLMハッシュの取得
- ゴールデン/シルバーチケットの作成
- 個人証明書のダンプ
- SAM/SYSTEMの解析

検知

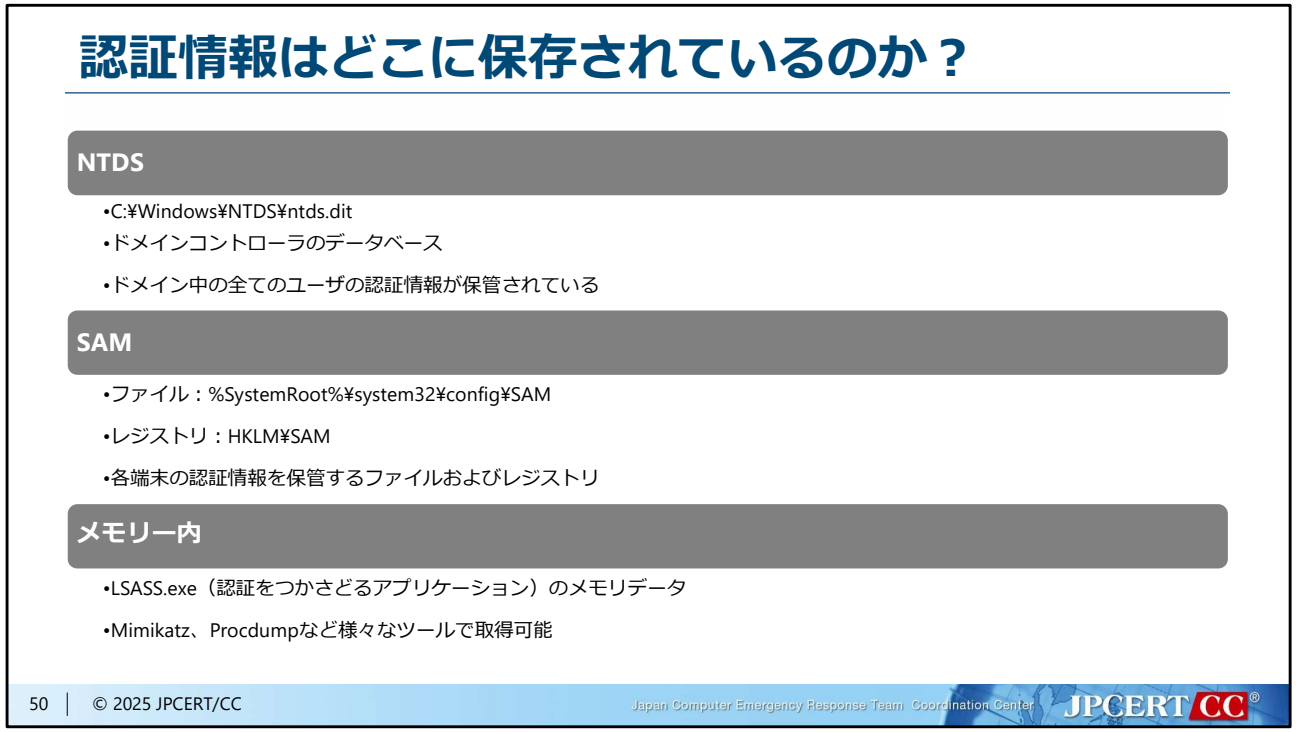
- それぞれの動作によって検知されるイベントが異なる
- 参考
  - https://jpcertcc.github.io/ToolAnalysisResultSheet_jp/details/Mimikatz_lsadump-sam.htm
  - https://jpcertcc.github.io/ToolAnalysisResultSheet_jp/details/Mimikatz_sekurlsa-logonpasswords.htm

Mimikatzは、Pass-the-HashやPass-the-Ticketが可能なツールです。



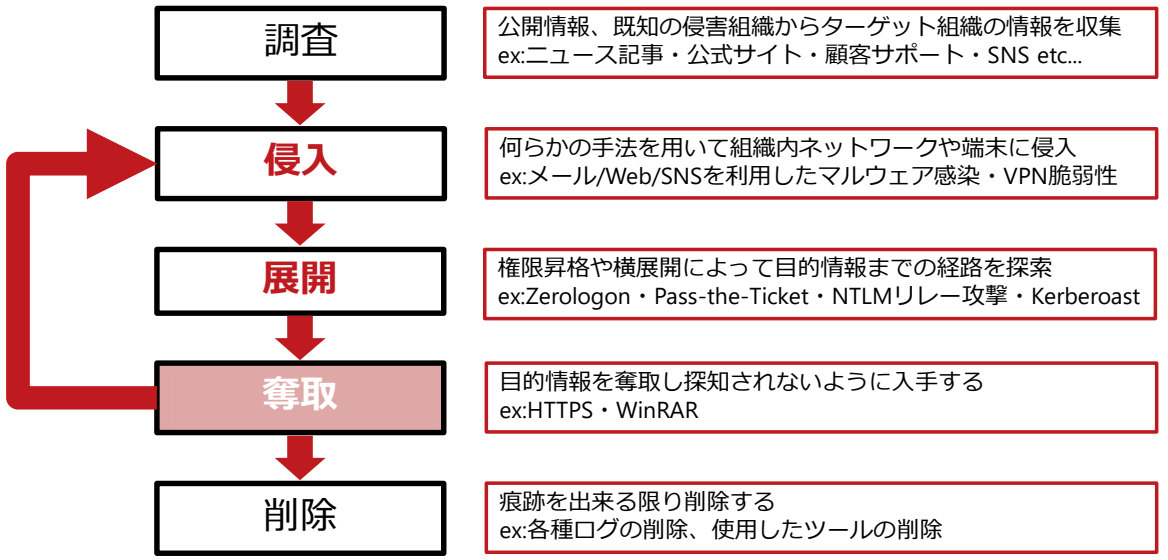
Rubeusは、Kerberoastが可能なツールです。また、偽のチケットの作成も可能です。

これらの各ツールの実行時には、イベントログが記録されます。ただし、これらの攻撃手法は通常のWindowの認証の仕組みを使用しているので、通常のログイン認証との差が分かりづらいという特徴があります。



Windows上で認証情報は、様々なところに記録されています。
NTDSファイル以外にもレジストリやプロセスのメモリ内に存在します。
これらの情報は、先ほど紹介したツールを使用しなくても、攻撃者はレジストリにアクセスしたりメモリダンプを取得することで、認証情報を得る可能性があります。
メモリダンプはWindowsが提供しているProcdumpというツールで取得でき、また、レジストリもWindowsの標準コマンドであるRegコマンドで取得できます。
このように攻撃用のツールを使用しなくてもよく、検知しづらいという特徴があります。

攻撃者のネットワーク侵入の流れ



奪取

侵入のための情報や資産価値のある情報を奪取

- ドキュメント類
  - ✓顧客情報
  - ✓製品の開発情報
- クラウドサービスへのアクセス情報
- データベースのデータ
  - ✓口座や決済の情報

奪取への対策

- 攻撃者の情報持ち出しを検知するのは不可能
  - ✓一次的な外部への通信量の増加などを検知することができればよいが、通常の運用では困難
- 重要情報の隔離、ネットワーク分離が重要

横展開の結果、目的の端末に侵入できたら、攻撃者は情報窃取を試みます。

WinRAR

なぜ攻撃者はWinRARを使用するのか

- 攻撃者は、WinRAR（正規ファイル）を侵入した端末にダウンロードして、RARファイルに圧縮を行う
- WinRAR自体は、異なるファイル名に変更されているので、ファイル名だけでは、特定が難しい
- 攻撃者が、WinRARを使うのには以下の理由が考えられる
  - ✓ 内部のドキュメント群を一斉に持ち出すためには、ファイル一式を圧縮して1つのファイルにする方が良い
  - ✓ なるべく圧縮率が高い手法を用いた方が、外部への転送量が抑えられる

転送後のRARファイルは、削除されることが多い
事後のフォレンジック調査で、RARファイルの存在が判明することが多い

攻撃者が外部に情報を持ち出す際によく利用するツールにWinRARがあります。
このツールを使用して、攻撃者はドキュメントなどをRAR形式に圧縮して外部に送信します。
RAR形式に圧縮されたファイルは、多くの場合、攻撃者によって削除されるので、どのファイルが持ち出されたかを特定することは困難です。
攻撃者が、WinRARを実行する際のコマンドラインを何らかの手段で記録していれば、そこから攻撃者の持ち出したファイルが推測できることがあります。

データの外部持ち出し方法

マルウェアの機能を使用

- 多くのマルウェアは、ファイルを転送する機能を持っており、その機能を使って外部にファイル転送する

SSH、HTTPS、SOCKS5のトンネリング通信

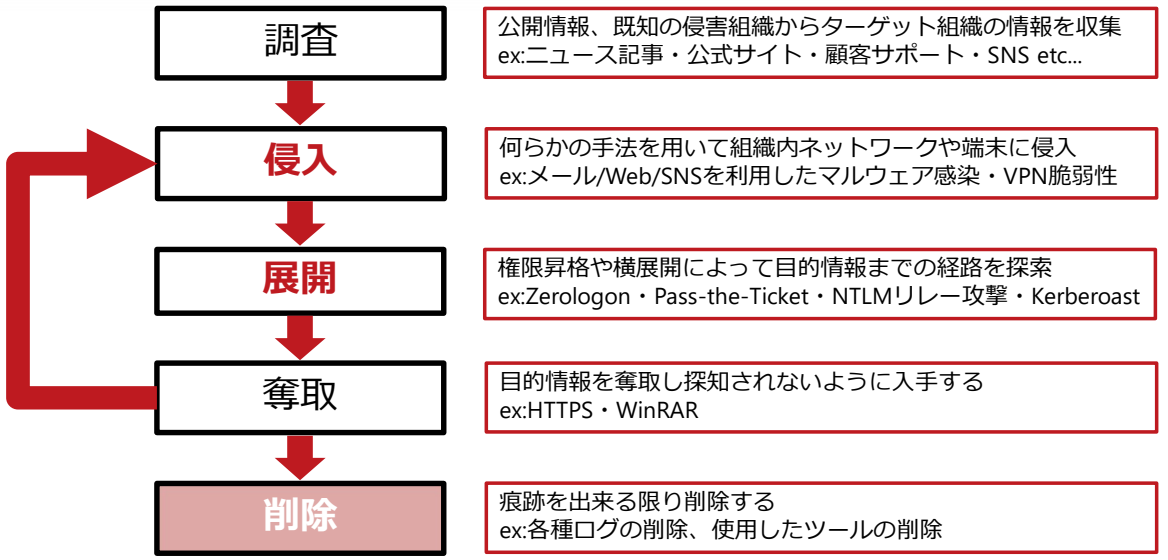
- トンネリングツールを利用して、ネットワーク上許可された経路でファイルを外部に転送する

クラウドサービスへの送信

- 正規のクラウドサービスにファイルを転送する

データを外部に転送する際は、マルウェアの機能を使用したり、トンネリングツールを使用したり、クラウドサービス直接アップロードする場合などがあります。
攻撃者は、プロキシ経由で通信できるように準備をしているため、奪取フェーズまで行ってしまうとデータの持ち出しを防ぐことは困難です。

攻撃者のネットワーク侵入の流れ



削除

侵入した痕跡を削除する

- 侵入し続ける
- 発覚を遅らせる
- 発覚後の捜査を遅延させる

削除への対策

- ファイルの削除は、通常操作と変わりないので、検知不可能
  - Windows標準コマンドdelなどが使用される
- ログの削除は通常操作では行わないため、検知できる可能性がある
  - イベントログの削除は、**イベントID: 1102**で記録される

攻撃者は、攻撃終了または途中に侵入の痕跡を削除します。
削除するものは、使用したツール・ログ・作成したファイルなどです。
削除する際は、マルウェアの機能を使用したり、デフォルトで使用可能なコマンドが使用されます。
また、イベントログの削除にはWindowsの標準コマンドであるWevtutilが使用されます。その際は、イベントID：1102で記録されます。

参考: コマンド実行のログ

攻撃者はコマンドラインを使いこなす

- 調査/侵入/展開/奪取/削除全てのフェーズで使用
- WindowsにおいてはPowerShellまたは、CMDが多用される
- 攻撃者の挙動はコマンドプロンプト/シェルのログを見れば把握可能

Windows（PoweShell）のログ確認　　※ コマンドプロンプトのログは残らない

```
> type (Get-PSReadlineOption).HistorySavePath -Tail 20
> (Get-PSReadlineOption).HistorySavePath
> C:¥Users¥[UserName]¥AppData¥Roaming¥Microsoft¥Windows¥PowerShell¥PSReadLine¥ConsoleHost_history.txt
```

Linuxのログ確認

```
# history
# cat $HISTFILE
```

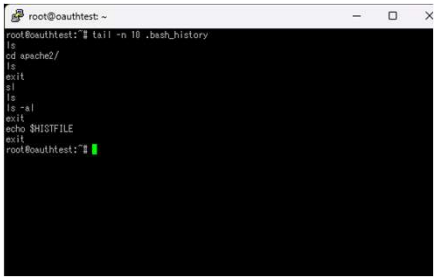
参考: コマンド実行のログ（Bash）

実行したコマンドが毎行記録される

- 日時や出力は記録されない

攻撃者のアクティビティを把握する手掛かりになるが、注意が必要

- 同一権限で削除可能
- 記録されない利用法あり
- 偽装も容易



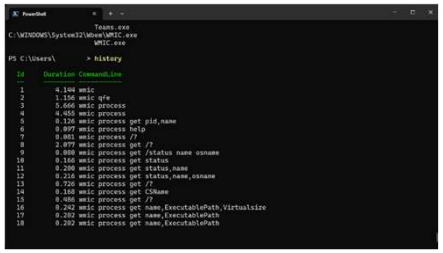
攻撃者自身にログを閲覧される危険性

- サーバの役割
- 機密ファイルのパス
- コマンドで渡したパスワード

参考: コマンド実行のログ（PowerShell ）

Historyコマンドとファイルの双方に記録が残る

- ◘日時等の情報は無い
- ◘プロセス終了後も残るのはファイルのみ
- ◘一般ユーザは使わないため攻撃者のログが大半になる可能性が高い
- ◘デフォルトで4096行分記録される



Windowsイベントログにも残る

- ◘デフォルトでは不完全
- ◘エラー等からコマンドの全容を探る

1 社内ネットワーク基礎

2 社内ネットワークへの攻撃手順

3 Windowsイベントログ

4 Windowsイベントログの分析

5 ハンズオン

Windowsイベントログ

Windowsにおけるログ

- OS内の色々な動作を記録
  - ✓メインは、Security・Application、System
- AD/端末で同一形式

保存フォルダ

- %SystemRoot%¥System32¥winevt¥Logs¥

拡張子

- EVTX

ログ確認方法

- **イベントビューアー**を使用するのがもっと簡単な方法

イベントログは、Windowsのログ機能です。

イベントビューアー

Windowsデフォルトのイベントログビューアー

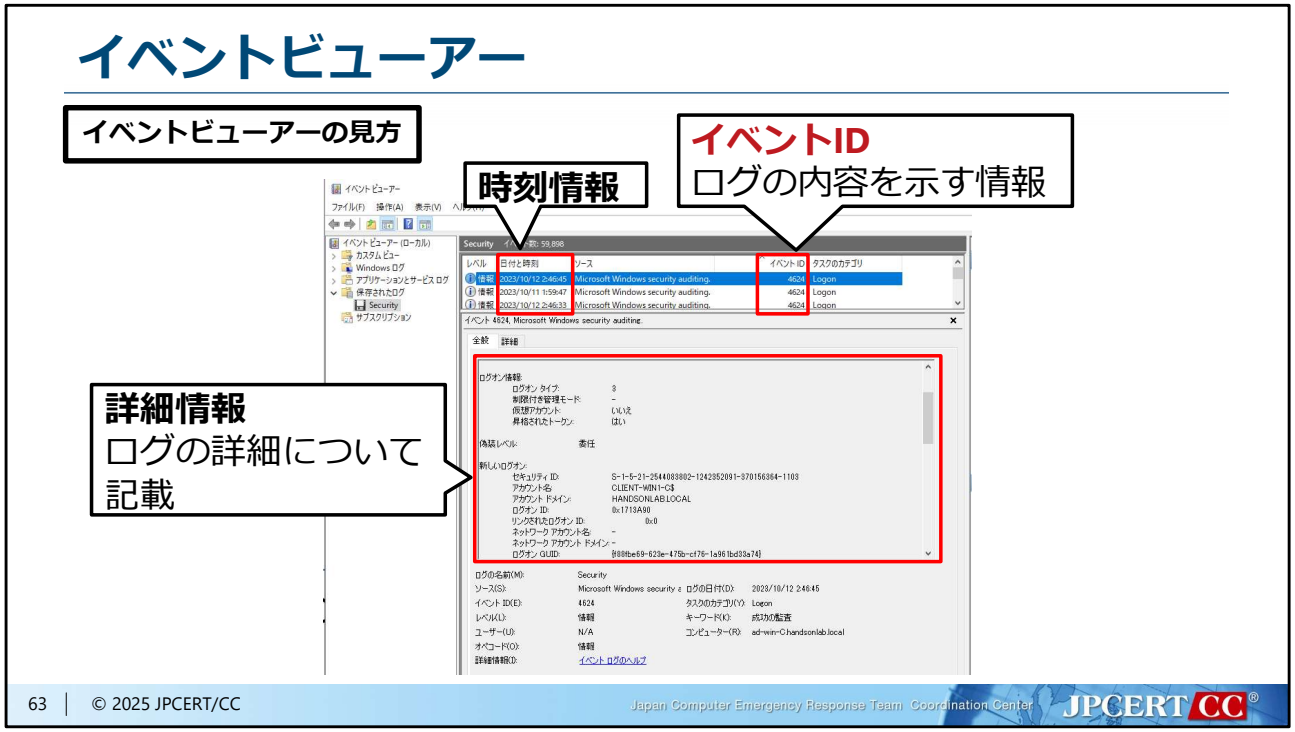
- Windows Client/Server双方に標準搭載されている
- 動作が重い
- 最低限の検索機能がある

簡単な調査に限定して利用する

- 時刻やイベント（攻撃者の挙動）が明確な状態からの追跡に使う
- **大量のログを分析する用途には向かない**（専用の分析ツールを使用する）

イベントログを確認するツールがイベントビューアーです。
イベントビューアーは、検索などの機能がありますが、動作が重いため大量のログを分析するという用途には向きません。

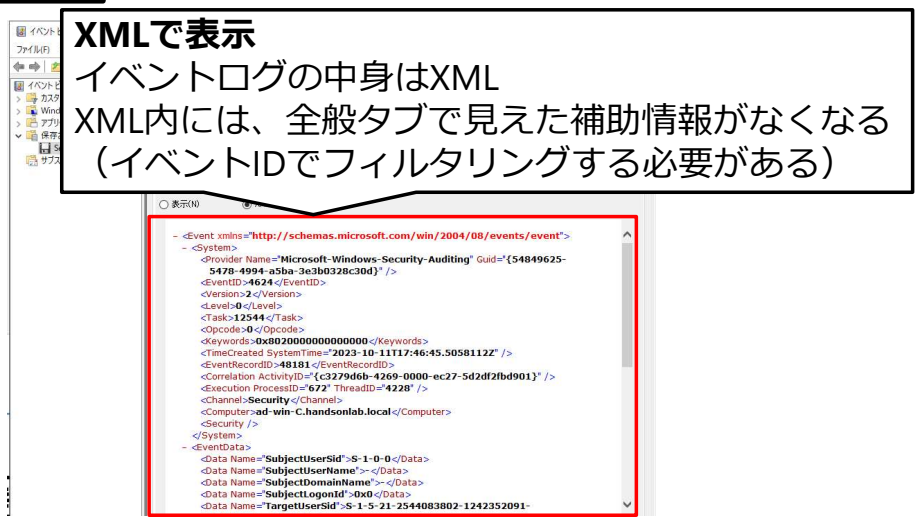
イベントビューアー



イベントログには、各ログにイベントIDが付きます。このIDによってログの内容を識別できます。
また、イベントログの詳細情報は、各イベントIDによってフォーマットが異なります。

イベントビューアー

イベントビューアーの見方



イベントログの中身はXMLで、XMLでエクスポートすることが可能です。XML内には全般タブで見えた日本語の補助情報がないため、どのイベントIDがどのような意味があるのかを把握していなければなりません。

重要なWindowsイベントログ①

アカウント関連（Security）

- イベントID 4624: アカウントが正常にログオンしました
- イベントID 4625: アカウントがログオンに失敗しました
- イベントID 4768: Kerberos 認証チケット (TGT) が要求されました
- イベントID 4769: Kerberos サービス チケットが要求されました
- イベントID 4776: コンピューターがアカウントの資格情報を検証しようとしました
- イベントID 4672: 新しいログオンに割り当てられた特別な特権

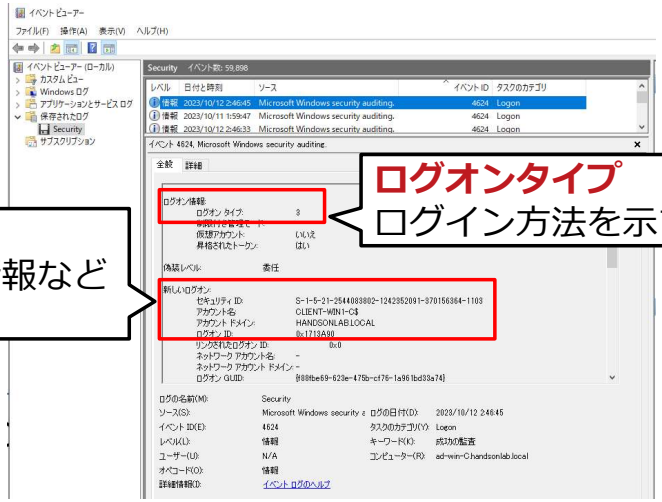
確認ポイント

- 大量のログオン失敗
- 意図しないアカウント作成・管理者アカウントの作成
- 意図しない特権アカウントでのログイン
- 意図しないリモートログイン（普段は行わないRDPからのログインなど）

イベントログを分析する際に、重要なイベントをいくつか紹介します。
まずは、Securityイベントのアカウント関連のイベントログです。
これらのイベントログは、通常のログイン時にも発生しますが、攻撃者のログイン時にも記録されます。

重要なWindowsイベントログ

アカウント関連（Security）



詳細情報
アカウント情報などが記載される

ログオンタイプ
ログイン方法を示す情報

ログオンタイプを確認することでどの手段でログインしたかを知ることができます。

ログオン種別

ログオンの種類	ログオン タイトル	説明
0	System	システム の起動時など、システム アカウントでのみ使用されます。
2	Interactive	ユーザーがこのコンピューターにログオンしました。
3	**Network**	ネットワークからこのコンピューターにログオンしたユーザーまたはコンピューター。
4	Batch	バッチ ログオンの種類はバッチ サーバーによって使用され、そこではプロセスが直接介入せずにユーザーの代わりに実行される可能性があります。
5	Service	サービス コントロール マネージャーによってサービスが開始されました。
7	Unlock	このワークステーションのロックが解除されました。
8	NetworkCleartext	ユーザーがネットワークからこのコンピューターにログオンしました。 ユーザーのパスワードは、非ハッシュ化形式で認証パッケージに渡されました。 組み込みの認証では、ネットワーク経由で送信する前に、すべてのハッシュ資格情報がパッケージ化されます。 資格情報は、プレーンテキスト (クリアテキストとも呼ばれます) でネットワークを通過しません。
9	NewCredentials	送信元が現在のトークンを複製し、送信接続用に新しい資格情報を指定しました。 新しいログオン セッションのローカル ID は同じですが、他のネットワーク接続には異なる資格情報を使用します。
10	**RemoteInteractive**	ターミナル サービスまたはリモート デスクトップを使用してリモートでこのコンピューターにログオンしたユーザー。
11	CachedInteractive	コンピューターにローカルに保存されたネットワーク資格情報を使用してこのコンピューターにログオンしたユーザー。 資格情報を確認するために、ドメイン コントローラーに接続できませんでした。
12	CachedRemoteInteractive	RemoteInteractive と同じです。 これは、内部監査に使用されます。
13	CachedUnlock	ワークステーション ログオン。

攻撃者のログインの場合、通常はリモートからのログインとなるため、ログオンタイプは3または10になることが多いです。

重要なWindowsイベントログ②

プロセス関連（Security）

- イベントID 4688: 新しいプロセスが作成されました
- イベントID 4689: プロセスが終了しました
- イベントID 5154: Windows フィルターリング プラットフォームで、アプリケーションまたはサービスによるポートでの着信接続のリッスンが許可されました
- イベントID 5156: フィルタリング プラットフォームによる接続の許可

確認ポイント

- 通常と異なるプロセスの生成/終了を検知する
  - ✓ 深夜にPowerShellが立ち上がっている
  - ✓ 知らないドメインに通信している

これらのログは、デフォルト設定では記録されない
監査ポリシーの設定をする必要がある

次に、プロセス関連のイベントログです。
イベントログでは、プロセスの実行や終了を記録することができます。
ただし、この機能は監査ポリシーと呼ばれる機能で、デフォルトでは無効化されています。

重要なWindowsイベントログ③

Windows Defender（Microsoft-Windows-Windows Defender Operational）

- イベントID 1013: マルウェアやその他の望ましくない可能性のあるソフトウェアの履歴を削除しました。
- イベントID 1150: エンドポイント保護クライアントは正常に稼働しています
- イベントID 1151: エンドポイント保護 クライアントの正常性レポート
- イベントID 5001: リアルタイム保護が無効になっています。
- イベントID 5007：Microsoft Defender ウイルス対策 の構成が変更されま

確認ポイント

- Windows Defenderをオフにしたり、マルウェアを検知した際に残る
- ノイズが少なく攻撃の全容もつかめる
- 使用しているウイルス対策ソフトで検知できなかったファイルを検知している可能性がある

Windows Defenderのログもイベントログとして記録されます。

監査ポリシー

監査ポリシーとは

- Windowsに標準で搭載されているログオン・ログオフやファイルアクセスなどの詳細なログを取得するための設定
- アカウント関連の監査ログは有効にしておくことを推奨

監査ポリシー使用の注意点

- 監査ポリシーを有効にすることで、**ログが増加**する
  - ✓ ログのローテーションが早くなり古いログが残りにくくなる
- 監査ポリシーを有効化する場合は、**イベントログの最大サイズの変更**もあわせて検討
  - ✓ イベントビューアーやwevtutilコマンドで変更可能

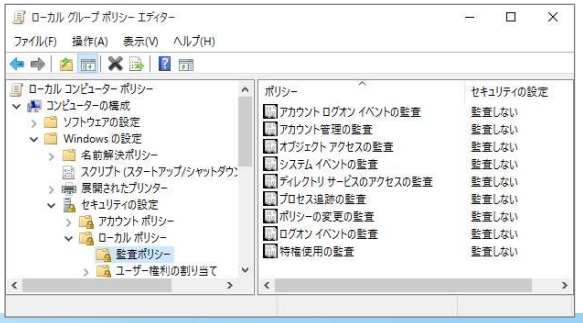
監査ポリシーは、Windowsに標準で搭載されているログオン・ログオフやファイルアクセス、プロセスの実行・終了などの詳細なログを取得するための設定で、デフォルトでは無効化されています。
監査ポリシーを有効化すると、ログの量が増加しますが、インシデント発生時に有用なログが記録されることになるため、有効化するk十を推奨します。

参考: 監査ポリシーの有効化方法

設定方法 ①

■ローカル グループ ポリシーの編集

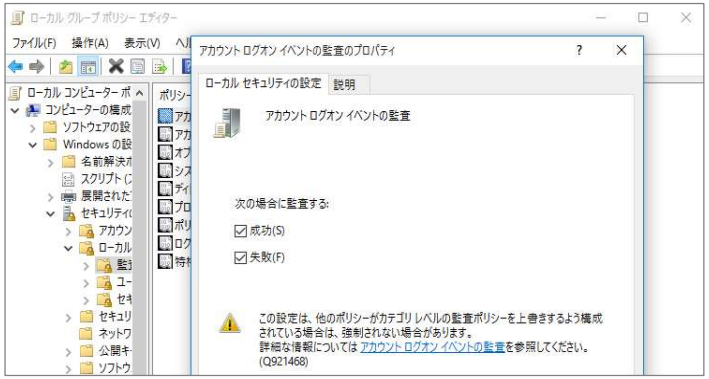
✓[コンピューターの構成]→[Windowsの設定]→[セキュリティの設定] →[ローカル ポリシー]→[監査ポリシー]



参考: 監査ポリシーの有効化方法

設定方法 ②

- 各ポリシーの「成功」「失敗」を有効



Sysmon

Sysmonとは

- 監査ログと同じく、デフォルトでは取得できないWindows上のアクティビティをログとして保存することができるマイクロソフトの提供するツール
- 以下のアクティビティをログに記録できる
  - ✓ ファイル作成・削除
  - ✓ プロセス起動・終了・インジェクション関連
  - ✓ レジストリ操作
  - ✓ DNS通信
  - ✓ ネットワーク通信
  - ✓ WMIイベント
  - ✓ ドライバ読み込み
- https://learn.microsoft.com/ja-jp/sysinternals/downloads/sysmon

Sysmonも、監査ポリシーと同じくWindows上の詳細なログを残すために有用なツールです。
このツールはデフォルトではインストールされていないため、インストールする必要があります。
また、監査ポリシーと同じくログ量が多いため、不要なログをチューニングすることが重要です。

Sysmonの設定情報に関しては、以下をご参照ください。
https://github.com/SwiftOnSecurity/sysmon-config

イベントログ分析のポイント

ポイント

- イベントログは、見る必要がない大量のログが記録されているので、ある程度絞り込みを行う必要がある

ログ絞り込みのポイント

- 見るイベントIDを特定する
  - ✓ 攻撃時に**どのようなイベントIDが記録されるのか**を理解する
- インシデント発生時刻前後に絞り込む
- ログ分析ツールを使用する
  - ✓ Splunk
  - ✓ Microsoft Sentinel
  - ✓ LogonTracer(OSS)
  - ✓ Hayabusa(OSS)

イベントログには、見る必要がない大量の正常なログが記録されているので、ある程度絞り込みを行う必要があります。
そのためには、①どのイベントIDを見る必要があるのかというのを把握しておくことが重要です。
さらに、イベントビューアーで分析が困難な場合（ログ量が多いとき）は②別のツールを使って分析することを検討する必要があります。

攻撃時にどのようなイベントIDが記録されるのか？

ポイント

- ブログやレポートなどで、攻撃時に記録されたイベントログの情報を知る

参考

- 侵入型ランサムウェア攻撃発生時に残るWindowsイベントログの調査
  https://blogs.jpcert.or.jp/ja/2024/09/windows.html
- ツール分析結果シート
  https://jpcertcc.github.io/ToolAnalysisResultSheet_jp/
- 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
- 攻撃グループMirrorFaceの攻撃活動
  https://blogs.jpcert.or.jp/ja/2024/07/mirrorface.html

①どのイベントIDを見る必要があるのかについては、様々なドキュメントが公開されていますのでご覧ください。
これ以外にも、セキュリティベンダーなどから様々なイベントIDに関する文書が出ていますので、そちらもご確認ください。

参考: 攻撃グループMirrorFaceの攻撃活動

(4) ファイアウォールのルール追加

- Windows Firewallの除外リストに、NOOPDOORで使用する特定ポート宛ての通信を許可する設定を追加
- イベントログ Firewall With Advanced Security/Firewall：**イベントID 2004**で記録される

(5) 登録したサービスの隠蔽

- 登録したサービスが表示されないように、アクセス制御を設定

(6) Windowsイベントログの消去

- システムログの削除
- 各イベントログ：**イベントID 1102**で記録される

(7) Windows Defenderの停止

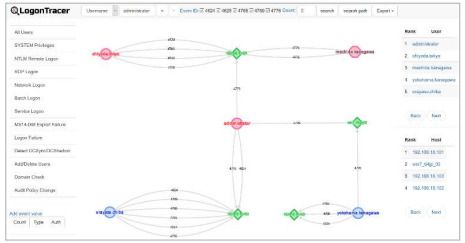
- イベントログ Windows Defender/Operational：**イベントID 5001**で記録される

https://blogs.jpcert.or.jp/ja/2024/07/mirrorface.html

LogonTracer

イベントログの分析をサポートするツール

- イベントログを可視化
- アカウントのログイン情報を一画面に表示可能
- 重要性の高いアカウントおよびホストの抽出
- イベントログのタイムライン表示



膨大なログから着眼すべきログを教えてくれる

- あやしいアカウントやホストの"あたりをつける"ためのツール
- 意図しないアカウントとホストの結びつきを見るだけでも良い

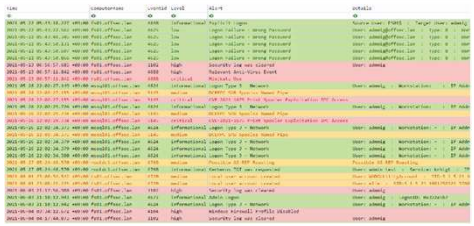
https://github.com/JPCERTCC/LogonTracer/wiki

②別のツールを使って分析するについては、いくつかのイベントログを分析するツールがあります。
LogonTracerは、JPCERT/CCが公開するツールで、ドメインコントローラーのSecurityログを可視化して分析することができるツールです。

Hayabusa

イベントログのタイムライン分析をサポートするツール

- イベントログをCSVとして整形
- イベントビューアーでExportするよりも分析しやすいフォーマットで出力可能
- 分析結果をサマリーとして取得可能



ルールによる不審なログの検知

- SIGMAルールを使って、あやしいイベントログを検知
- 見るべきポイントを絞ることができるので分析の効率化に有効

https://github.com/Yamato-Security/hayabusa

HayabusaはYamato Securityグループが公開しているツールです。
SIGMAルールを使ってイベントログを分析し、さらにイベントビューアーでExportするよりも分析しやすいフォーマットで出力可能なツールです。
このツールは、すべてのイベントログに対応できるため、非常に有益なツールなので、イベントログ分析時には使用することをお勧めします。

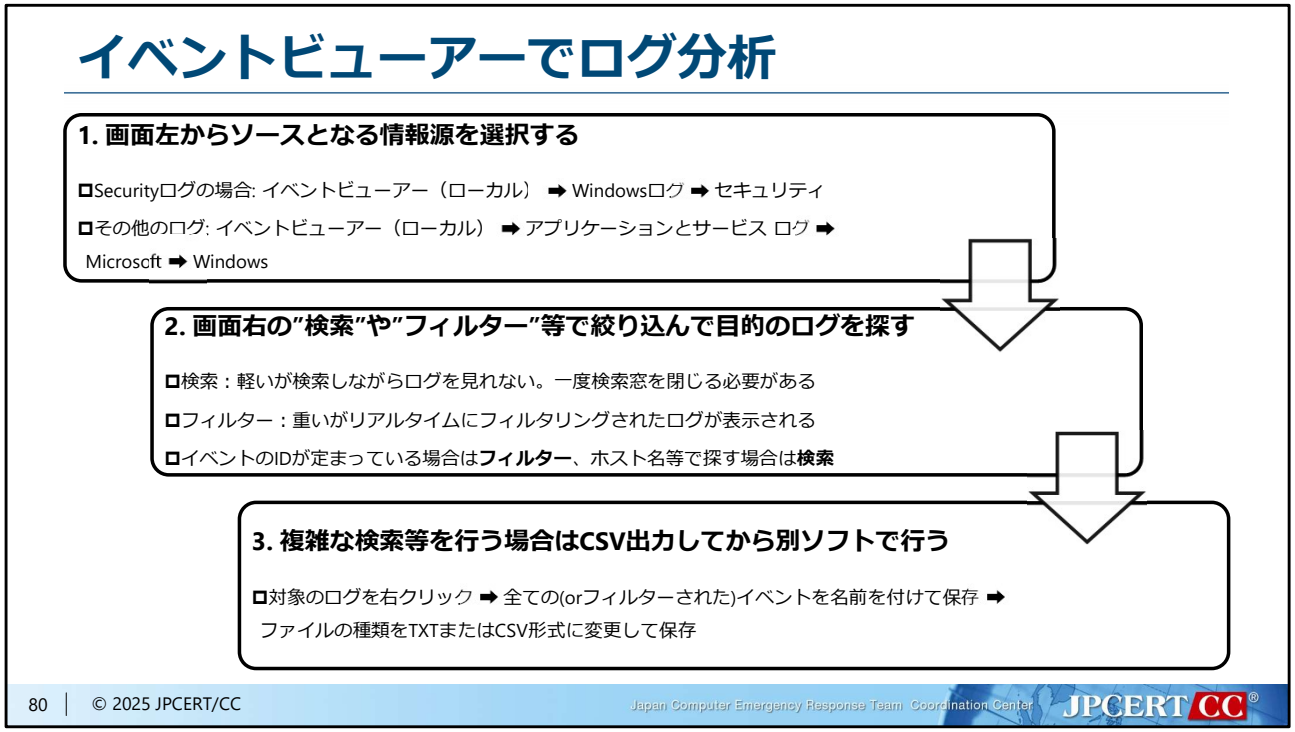
1 社内ネットワーク基礎

2 社内ネットワークへの攻撃手順

3 Windowsイベントログ

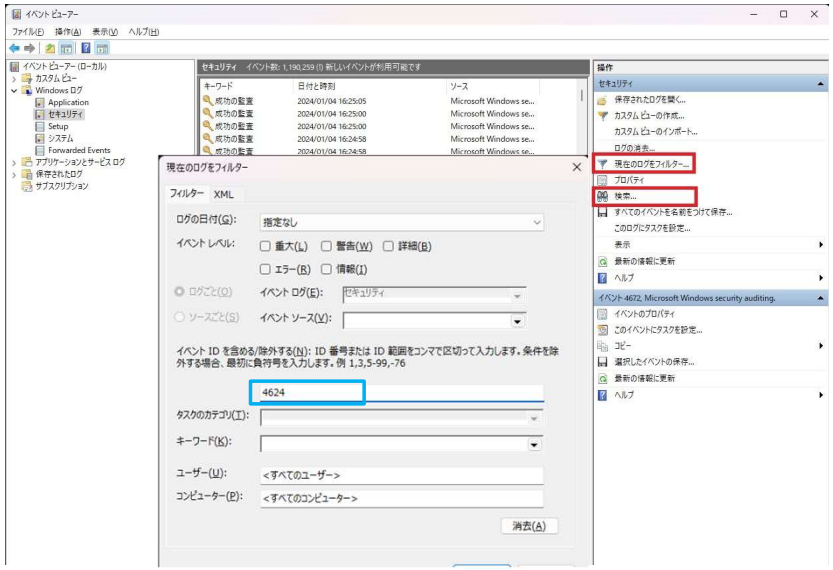
4 Windowsイベントログの分析

5 ハンズオン



イベントビューアーでイベントログを分析する流れを示します。
基本的には、イベントビューアーではすべてのログを見ることが難しいため、フィルタリングしたうえでCSV形式などにExportして分析する方法が良いと考えます。

イベントビューアーのフィルタリング



よく使うフィルター条件

日時検索

- 大量のログを分析するには適さないので、**日時である程度絞り込む**

イベントIDの範囲で検索

- 「8000-8010」　8000～8010のイベントを検索
- 「8000,8010」　8000と8010のイベントを検索

日時・イベントID以外はXMLタブからXPathによるフィルター

- 分析手順は以下の通り

①GUI上のフィルターを適用

②XPathによるフィルターを適用

③テキストとして出力後、ツールやPython等を用いて加工

イベントビューアーを使ったフィルタリング条件で最もシンプルなものは、イベントIDでのフィルタリングです。また、日時で絞り込むのも有効です。
これらのフィルタリングは、GUIから操作可能なのですが、より複雑なフィルタリングを実施したい場合は、Xpathを使用します。

XPathによるフィルター

イベントビューアーでは、XPath1.0を利用可能

- イベントログはXMLの集合体

XPathの一部のみサポート

- contains等の関数は使えない
- 基本的なクエリのみ利用可能
- 演算子も利用可能
- XPath 1.0 の制限事項
  - ✓https://learn.microsoft.com/ja-jp/windows/win32/wes/consuming-events

イベントビューアーでは、XPath1.0を利用可能です。XPath1.0については、ドキュメントなどをご覧ください。
イベントIDなどのフィルター条件を指定して、図のようにXMLタブに移動すると、現在しているフィルターのXpathが確認できます。
ですので、まずはフィルタータブである程度条件を設定してからXMLタブに移動し、「手動でクエリを編集する」をクリックし、Xpathを編集していくことをお勧めします。

参考: XPathの基礎知識

フィルターパターン1: *[タグ名[子タグ名]]

- フィルター例：***[hoge[fuga[piyo]]]**
- フィルター結果：piyoタグがどちらもヒット

フィルターパターン2: *[タグ名[@属性=値]]

- フィルター例：***[piyo[@id=1]]**
- フィルター結果：id=1のpiyoタグがヒット

フィルターパターン3: *[タグ名 = 値]

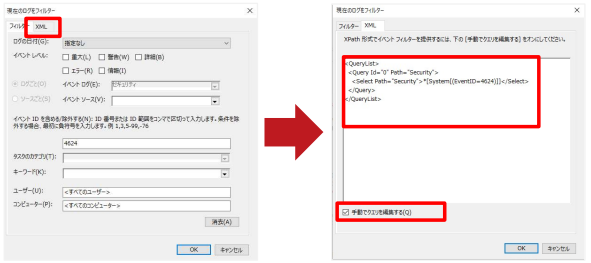
- フィルター例：***[piyo = "aaa"]**
- フィルター結果：id=1のpiyoタグがヒット

```
<!-- XML例 -->

<hoge>
  <fuga>
    <piyo id=1>aaa</piyo>
    <piyo id=2>bbb</piyo>
  </fuga>
</hoge>
```

参考: XPathのフィルタールールの組み立て方

1. フィルタータブでログのフィルターを実施

- 自動で検索用XMLに反映される
- 必要な一部だけ書き替える



2. イベントログのXMLと見比べる

- 全般/詳細タブを確認
- 何の値を対象にしたいか等

参考: XPathのフィルタールールの組み立て方

フィルター例1

□ 任意の要素 *[] の中から<System>の子の<EventID>の値が4769のもの

```
<QueryList>
  <Query Id="0">
    <Select Path="file://C:¥work¥sample¥Security.evtx">
      *[  System[EventID=4769]    ]
    </Select>
  </Query>
</QueryList>
```

参考: XPathのフィルタールールの組み立て方

フィルター例2

- 任意の要素 *[] の中から<System>の子の<EventID>の値が4769のもの
- <EventData>の子の<Data>のName属性がTargetUserNameであって、値がdomuser@LAB.LOCALのもの

```
<QueryList>
  <Query Id="0">
    <Select Path="file://C:¥work¥Security.evtx">
*[
  System[EventID=4769] and
  EventData[
    Data[@Name="TargetUserName"] ="domuser@LAB.LOCAL"
  ]
]
    </Select>
  </Query>
</QueryList>
```

参考: XPathのフィルタールールの組み立て方

フィルター例3

- 任意の要素 *[] の中から<System>の子の<EventID>の値が4769のもの
- <TimeCreated>のSystemTime属性値が2024/1/18～2024/1/31まで

```
<QueryList>
  <Query Id="0"
    <Select Path="file://C:¥work¥Security.evtx">
*[System[
  (EventID=4611) and
  TimeCreated[
    @SystemTime>='2024-01-18T00:00:00.000Z' and
    @SystemTime<='2024-01-31T00:00:00.000Z'
  ]
]]
</Select>
  </Query>
</QueryList>
```

PowerShellを使ったイベントログ分析

Get-WinEventを使ったイベントログ分析

- PowerShellのコマンドGet-WinEventを使うことで、イベントビューアーと同様の分析を行うことが可能
- ただし、コマンドラインで大量のログを分析するのは困難なため、CVSなどにExportして分析する
- イベントビューアーと同じく、XPathによるフィルタリングが可能

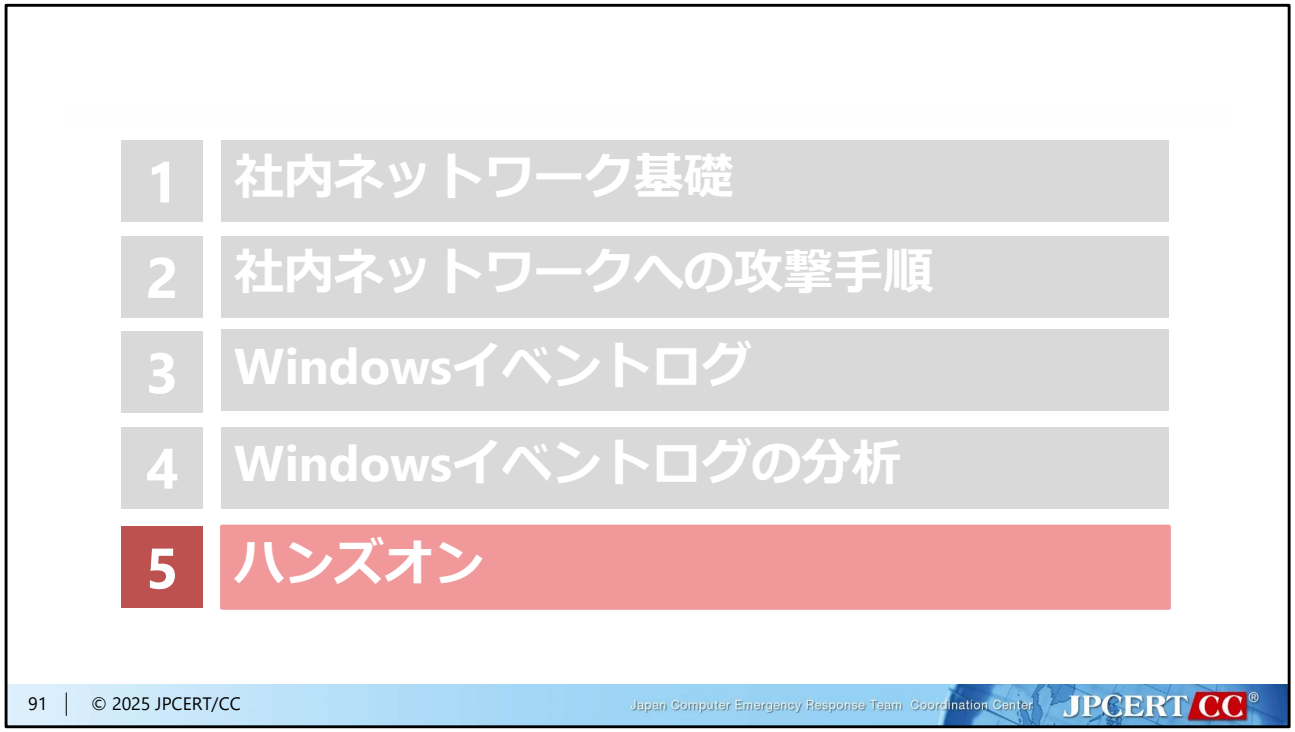
イベントビューアー以外にも、PowerShellを使うことで、イベントログをフィルタリングしたり、Exportすることができます。
この場合も、イベントビューアーと同様にXPathをつかったフィルタリングが可能です。

PowerShellを使ったイベントログ分析

Get-WinEvent例

```
Get-WinEvent -Path C:¥test¥Security.evtx  -
FilterXPath '*[System[(EventID=4624)]' | Select-
Object RecordID,TimeCreated,Id,Message | Sort-
Object RecordId | Export-Csv -Path test.csv -
NoTypeInformation -Encoding UTF8
```


Get-WinEventを使い、イベントログを読み込み、XPathでフィルタリングするコマンド例を示しています。
イベントビューアーとできることはほぼ変わらないため、使いやすい方法をご利用ください。



ここからハンズオンに入ります。
最初は、4章で説明したフィルタリングの使い方を中心にハンズオンでふれていきます。

ハンズオン 1

演習

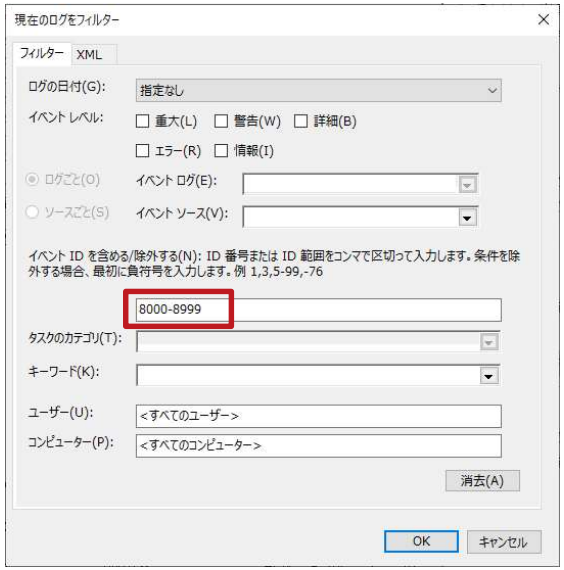
問題

- イベントビューアーを使って、sample1.evtxログファイルから、ID:8000-8999までのログをまとめたCSVファイルを作成してください。

ハンズオン 1

演習

回答


現在のログをフィルター
フィルター
XML
ログの日付(G):
指定なし
イベント レベル:
重大(L)
警告(W)
詳細(B)
エラー(R)
情報(I)
ログごと(O)
イベント ログ(E):
ソースごと(S)
イベント ソース(V):
イベント ID を含める/除外する(N): ID 番号または ID 範囲をコンマで区切って入力します。条件を除外する場合、最初に負符号を入力します。例 1,3,5-99,-76
8000-8999
タスクのカテゴリ(T):
キーワード(K):
ユーザー(U):
<すべてのユーザー>
コンピューター(P):
<すべてのコンピューター>
消去(A)
OK
キャンセル

ハンズオン 2

演習

問題

- sample1.evtxログファイルから、Microsoft Edgeが起動した時刻を抽出してください。

ハンズオン 2

演習

問題

- sample1.evtxログファイルから、Microsoft Edgeが起動した時刻を抽出してください。

ヒント

プロセス起動のイベントID

- 4688

Microsoft Edgeのプロセス名

- C:¥Program Files (x86)¥Microsoft¥Edge¥Application¥msedge.exe

プロセス名のフィールドは、`NewProcessName`です。

ハンズオン 2

演習

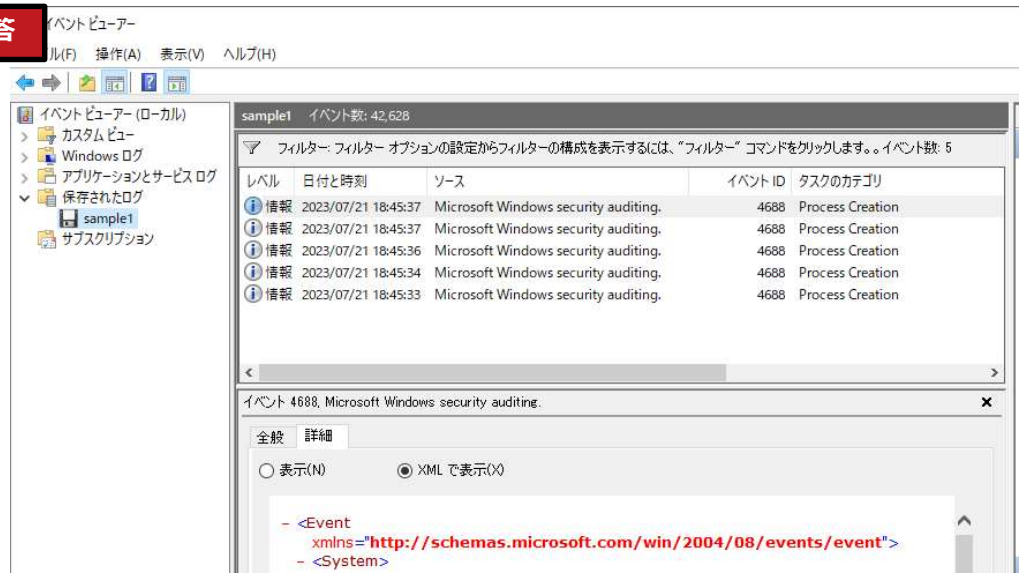
回答 **※ イベントビューアーの場合**

```
<QueryList>
  <Query Id="0" Path="file://sample1.evtx">
    <Select Path="file://sample1.evtx">
    *[
      System[(EventID=4688)] and
      EventData[Data[@Name="NewProcessName"]="C:¥Program Files
(x86)¥Microsoft¥Edge¥Application¥msedge.exe"]
    ]
    </Select>
  </Query>
</QueryList>
```

ハンズオン 2

演習

回答


イベント ビューアー
ル(F) 操作(A) 表示(V) ヘルプ(H)
イベント ビューアー (ローカル)
カスタム ビュー
Windows ログ
アプリケーションとサービス ログ
保存されたログ
sample1
サブスクリプション
sample1 イベント数: 42,628
フィルター: フィルター オプションの設定からフィルターの構成を表示するには、"フィルター" コマンドをクリックします。。イベント数: 5
レベル 日付と時刻 ソース イベント ID タスクのカテゴリ
情報 2023/07/21 18:45:37 Microsoft Windows security auditing. 4688 Process Creation
情報 2023/07/21 18:45:37 Microsoft Windows security auditing. 4688 Process Creation
情報 2023/07/21 18:45:36 Microsoft Windows security auditing. 4688 Process Creation
情報 2023/07/21 18:45:34 Microsoft Windows security auditing. 4688 Process Creation
情報 2023/07/21 18:45:33 Microsoft Windows security auditing. 4688 Process Creation
イベント 4688, Microsoft Windows security auditing.
全般 詳細
表示(N)
XML で表示(X)
- <Event
xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>

ハンズオン 2

演習

回答 ※ PowerShellの場合

```
Get-WinEvent -Path C:¥sample1.evtx  -FilterXPath
'*[System[(EventID=4688)] and
EventData[Data[@Name="NewProcessName"]="C:¥Progra
m Files (x86)¥Microsoft¥Edge¥Application¥msedge.exe"]]' |
Select-Object RecordID,TimeCreated,Id,Message | Sort-
Object RecordId | Export-Csv -Path test.csv -
NoTypeInformation -Encoding UTF8
```

ハンズオン 3

演習

問題

- sample1.evtxログファイルから、アカウント：jpcertuserでRDP経由でログインしたログをフィルターしてCSVファイルを作成してください。

ハンズオン 3

演習

問題

- sample1.evtxログファイルから、アカウント名 "**jpcertuser**" で**RDP**経由でログインしたログをフィルターしてCSVファイルを作成してください。

ヒント

ログオン成功のイベントID

- イベントID：4624

RDP接続のLogonType

- 10

アカウント名のフィールドは`TargetUserName`
LogonTypeのフィールドは`LogonType`

ハンズオン 3

演習

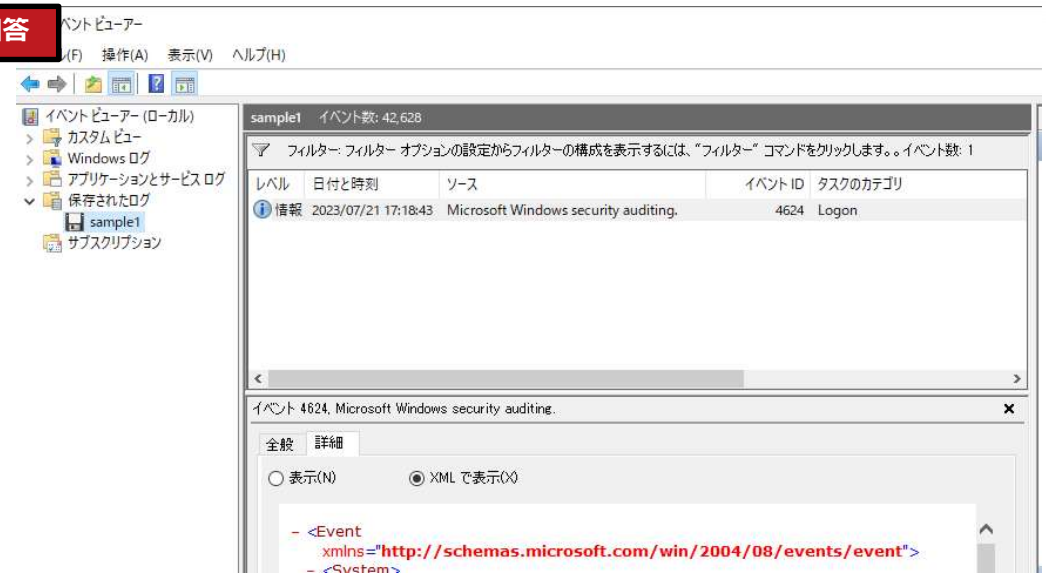
回答

```
<QueryList>
  <Query Id="0" Path="file://sample1.evtx">
    <Select Path="file://sample1.evtx">
    *[
      System[(EventID=4624)] and
      EventData[Data[@Name="LogonType"]="10" and
                Data[@Name="TargetUserName"]="jpcertadmin"
               ]
    ]
    </Select>
  </Query>
</QueryList>
```

ハンズオン 3

演習

回答


ベント ビューアー
(F) 操作(A) 表示(V) ヘルプ(H)
イベント ビューアー (ローカル)
カスタム ビュー
Windows ログ
アプリケーションとサービス ログ
保存されたログ
sample1
サブスクリプション
sample1 イベント数: 42,628
フィルター: フィルター オプションの設定からフィルターの構成を表示するには、"フィルター" コマンドをクリックします。。イベント数: 1
レベル 日付と時刻 ソース イベント ID タスクのカテゴリ
情報 2023/07/21 17:18:43 Microsoft Windows security auditing. 4624 Logon
イベント 4624, Microsoft Windows security auditing.
全般 詳細
表示(N)
XML で表示(X)
- <Event
xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>

ハンズオン 4

演習

問題

sample2.evtxはバックドアツールがインストールされていた端末のイベントログです。通常このツールはWindows Defenderに検知されるはずでしたが、この時は検知されませんでした。誰がDefenderを切ったのか、特定してください。

ハンズオン 4

演習

問題

sample2.evtxはバックドアツールがインストールされていた端末のイベントログです。通常このツールはWindows Defenderに検知されるはずでしたが、この時は検知されませんでした。誰がDefenderを切ったのか、特定してください。

ヒント

Windows Defenderの停止時間を特定

- イベントID：5001

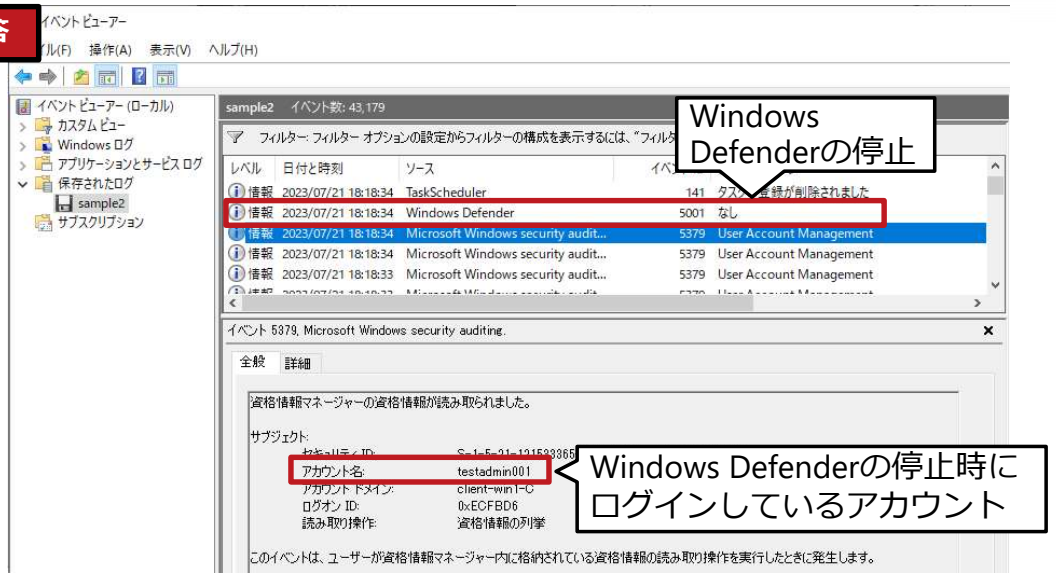
Windows Defenderの停止時間周辺でログインしているアカウントを特定

Windows Defenderを停止させたアカウント情報は記録されないので、Windows Defenderの停止時間周辺でログインしているアカウントがその操作をした可能性があると推測できます。

ハンズオン 4

演習

回答


イベント ビューアー
ファイル(F) 操作(A) 表示(V) ヘルプ(H)
イベント ビューアー (ローカル)
カスタム ビュー
Windows ログ
アプリケーションとサービス ログ
保存されたログ
sample2
サブスクリプション
sample2 イベント数: 43,179
フィルター: フィルター オプションの設定からフィルターの構成を表示するには、"フィルタ
レベル 日付と時刻 ソース
情報 2023/07/21 18:18:34 TaskScheduler 141 タスク登録が削除されました
情報 2023/07/21 18:18:34 Windows Defender 5001 なし
情報 2023/07/21 18:18:34 Microsoft Windows security audit... 5379 User Account Management
情報 2023/07/21 18:18:34 Microsoft Windows security audit... 5379 User Account Management
情報 2023/07/21 18:18:33 Microsoft Windows security audit... 5379 User Account Management
Windows Defenderの停止
イベント 5379, Microsoft Windows security auditing.
全般 詳細
資格情報マネージャーの資格情報が読み取られました。
サブジェクト:
アカウント名: testadmin001
アカウント ドメイン: client-win1-C
ログオン ID: 0xECFBD6
読み取り操作: 資格情報の列挙
このイベントは、ユーザーが資格情報マネージャー内に格納されている資格情報の読み取り操作を実行したときに発生します。
Windows Defenderの停止時に
ログインしているアカウント