Windowsログ分析の基礎
～実践編～

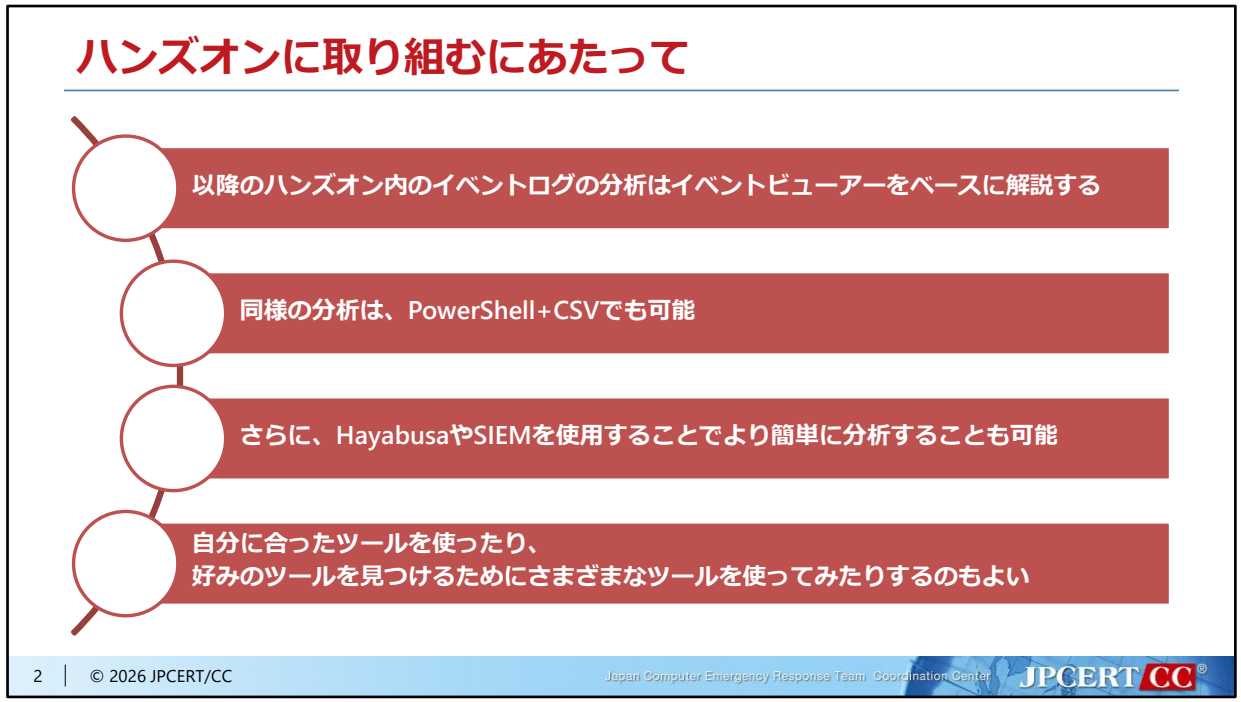
－ADへの攻撃を理解するために－

一般社団法人JPCERTコーディネーションセンター

本コンテンツについて

- 本コンテンツは、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、JPCERT/CC 広報（pr@jpcert.or.jp）までご連絡ください

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、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、本コンテンツは初動調査に特化しています。



ハンズオンに取り組むにあたって、前提知識は「基本編」をご覧ください。
本ハンズオンでは、イベントビューアーをベースに説明を進めますが、その他のツールも併用して、どのツールを使うのが便利なのかを把握し、実際のインシデント対応・調査に備えることをお勧めします。

ハンズオン イントロダクション

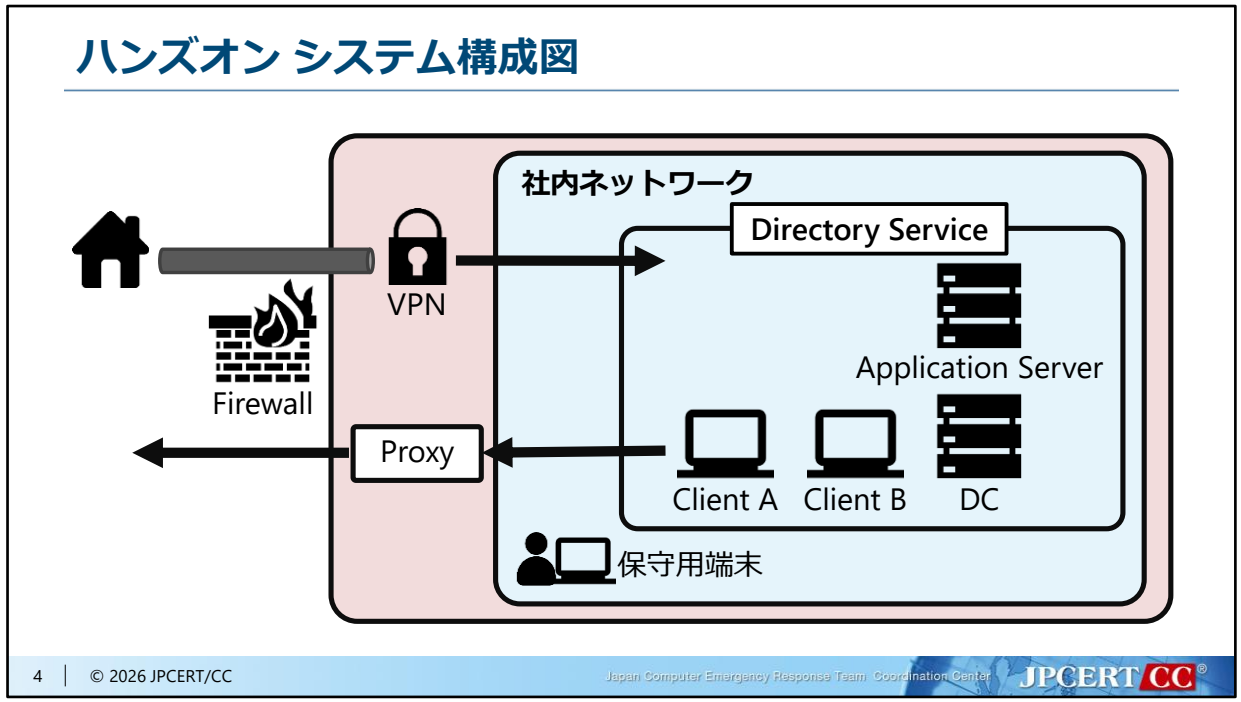
あなたは会社のセキュリティ担当者です。

ある日、いくつかの部の職員から「見覚えのないファイルがデスクトップに生成されている」という報告を受けました。

Windows Update等による影響かと考えましたが、ほぼ同じ構成の私用PCではそのようなファイルは生成されておらず、自社の業務PCでのみ確認される事象であることが分かりました。

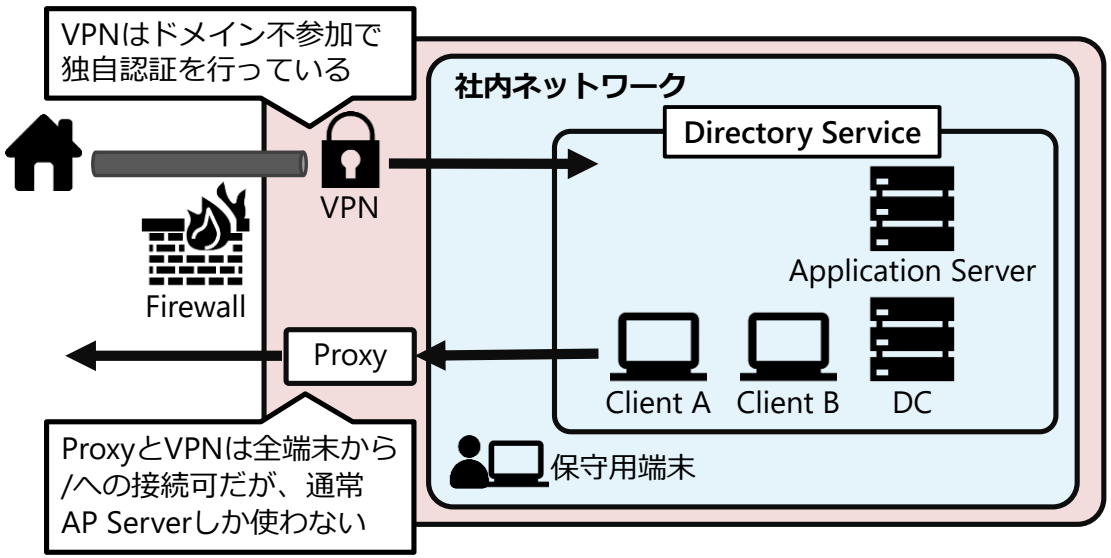
さて、このファイルはどこから来て、誰が設置したものなのでしょうか。

本ハンズオンでは、インシデント発生組織のログを分析することを想定して進めます。

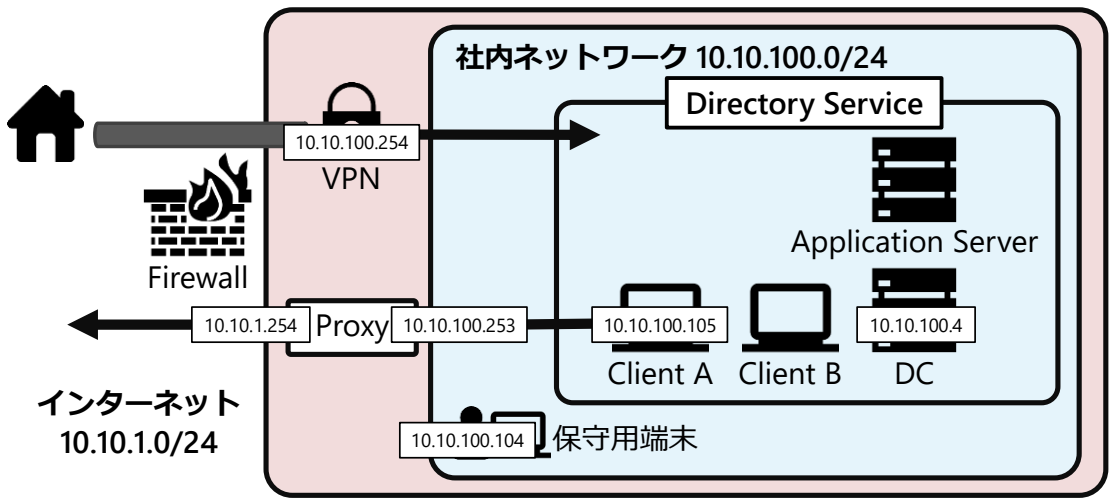


今回ハンズオンで分析するログを取得した環境を図に示します。

ハンズオン システム構成図



ハンズオン システム構成図



会社が把握しているアカウント一覧

ドメインアカウント

- domadm（ドメイン管理者）
- domuser

ローカルアカウント

- testadmin001（保守用端末のローカル管理者）
- itmanager（保守用端末、Client Aのローカル管理者）
- testuser

※ “jpcert”とついたアカウントはシステム設定時に使用した
アカウントなので、分析対象からは除外してください

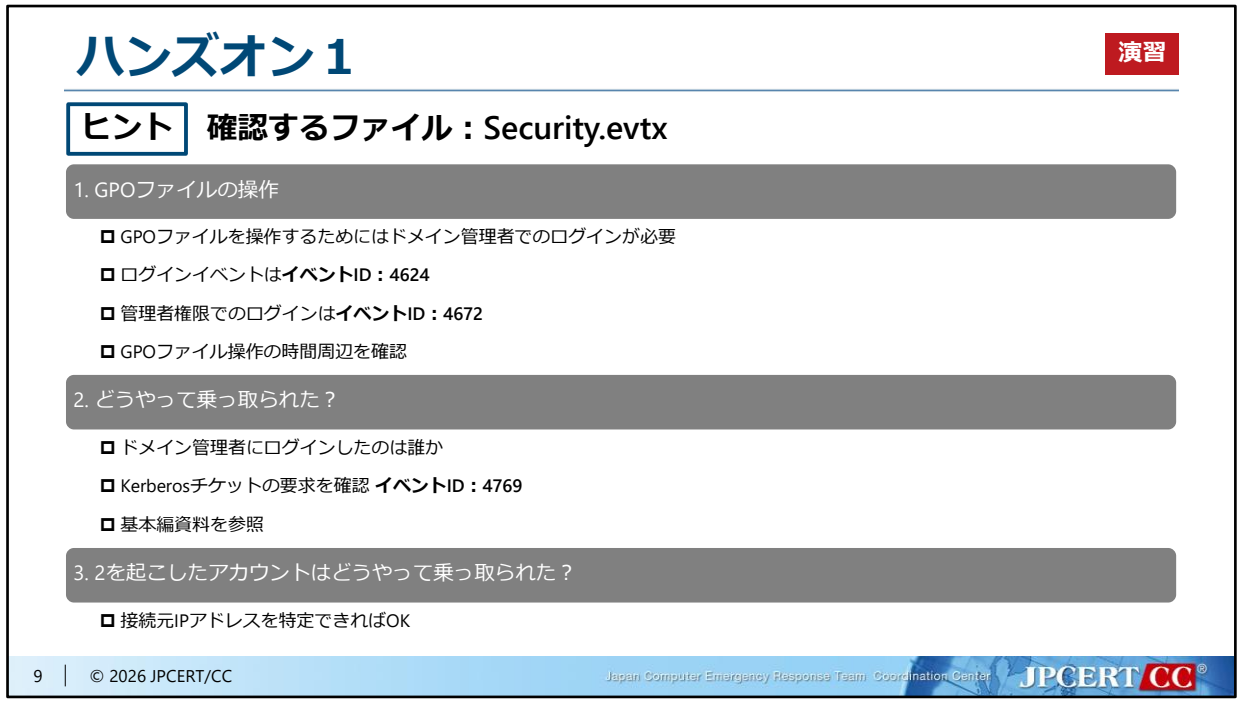
ハンズオン１

演習

複数の職員で同様の現象が発生しているものの、ADに参加していない保守用端末ではファイルが生成されていませんでした。
よって、ADが関わっている可能性が高いと判断し、GPOファイルを確認したところ、10月12日8:55ごろに不審な設定が作成されていることが分かりました。

問題 ログ分析を行い、以下の空欄を埋めてください。

1. 時刻に10.10.100.254（VPN）からアカウント でログイン
2. 時刻にアカウントからアカウント へ攻撃手法
3. 時刻にIPアドレスからアカウント へログイン



管理者権限アカウントは、スライドP.7を確認してください。

ハンズオン１

演習

回答

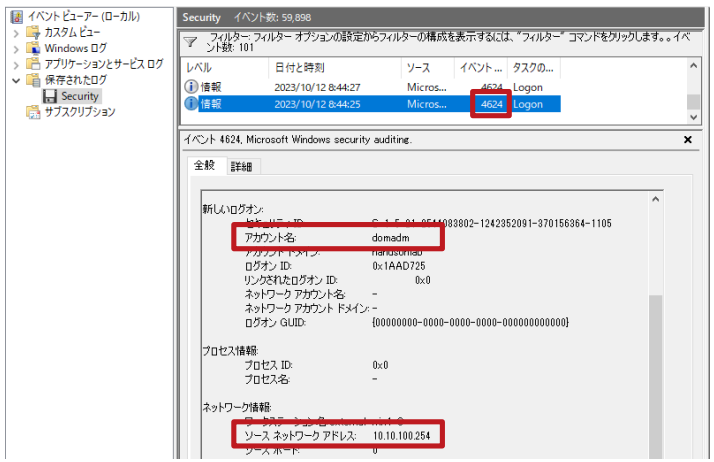
1. 10月12日8:44に10.10.100.254（VPN）からdomadmでログイン
   - ➡**事象発生時（10月12日 8:55）周辺のドメイン管理者のログインを確認**
2. 10月11日10:17にdomuserからdomadmへKerberoast
   - ➡**ドメイン管理者に対するKerberosチケットの要求が発生していることからKerberoastの可能性**
3. 10月11日10:12に10.10.100.105からdomuserへログイン
   - ➡**ドメイン管理者に対するKerberosチケットの要求直前のログインを確認するとdomuserのログインを確認**

ハンズオン１

演習

回答

1. 10月12日8:44に10.10.100.254（VPN）からdomadmでログイン



ハンズオン１

演習

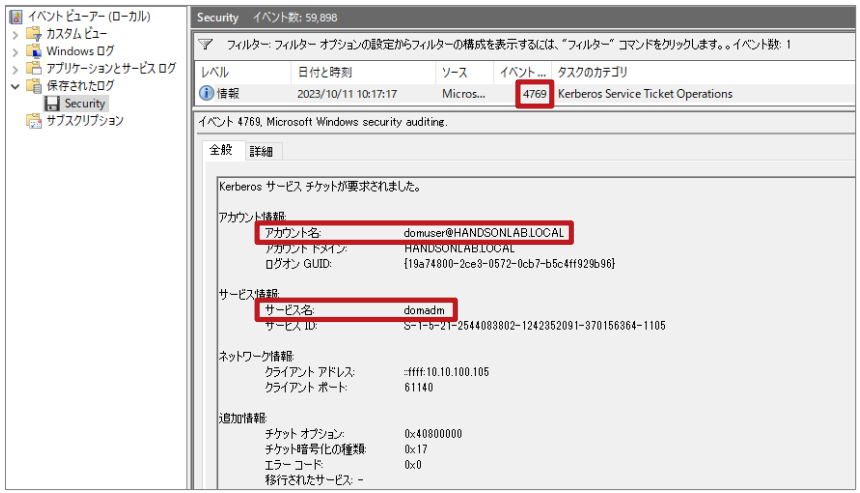
回答 1. 10月12日8:44に10.10.100.254（VPN）からdomadmで
ログイン

```
<QueryList>
  <Query Id="0" Path="file://Security.evtx">
    <Select Path="file://Security.evtx">
    *[
      System[(EventID=4624)] and
      EventData[Data[@Name="TargetUserName"]="domadm" and
                Data[@Name="IpAddress"]="10.10.100.254"]
    ]
    </Select>
  </Query>
</QueryList>
```

ハンズオン１

演習

回答 2. 10月11日10:17にdomuserからdomadmへKerberoast



ハンズオン１

演習

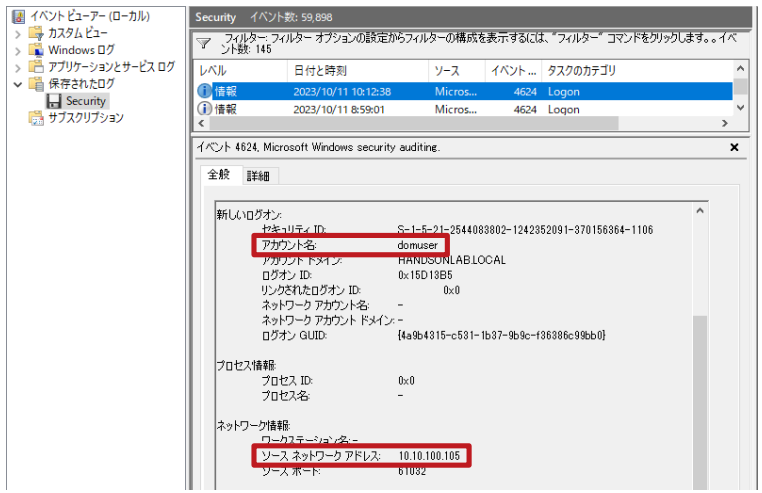
回答 2. 10月11日10:17にdomuserからdomadmへKerberoast

```
<QueryList>
  <Query Id="0" Path="file://Security.evtx">
    <Select Path="file://Security.evtx">
    *[
      System[(EventID=4769)] and
      EventData[Data[@Name="ServiceName"]="domadm"]
    ]
    </Select>
  </Query>
</QueryList>
```

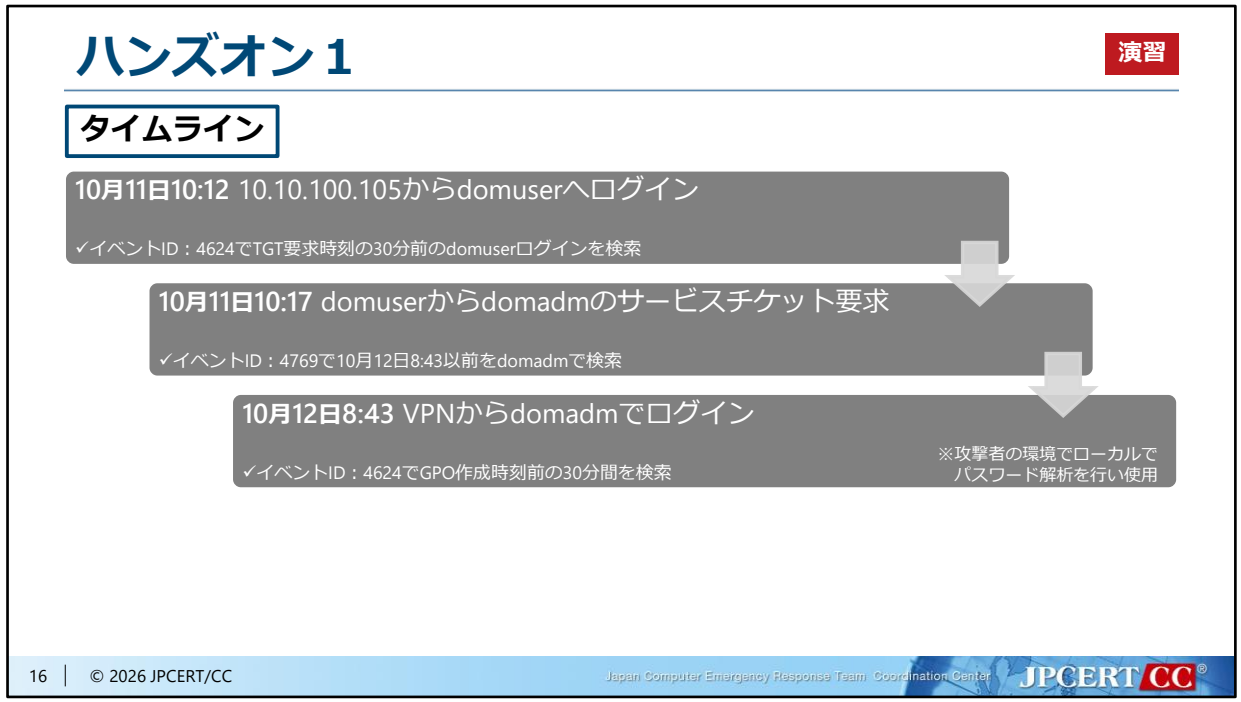
ハンズオン１

演習

回答 3. 10月11日10:12に10.10.100.105からdomuserへログイン



アカウント名domuserでのログインは多数確認できますが、Kerberosチケットの要求直前でログインしているアカウントがこのインシデントに関係している可能性が高いと想定して、domuserと10.10.100.105が怪しいと判断します。



これまでの攻撃の流れをタイムラインとして記載しています。
実際のインシデント発生時には調査で判明した断片を集めてタイムラインとして並べながら調査を進めますので、問題にはありませんが引き続きハンズオンで分かったことをタイムラインに残してください。

ハンズオン２

演習

domuserを使用していたクライアント（10.10.100.105）が侵害を受けている可能性があるので、調べたいと思います。
クライアントのイベントログを取得したので分析してください。

問題 ログ分析を行い、以下の空欄を埋めてください。

1. [時刻] に[アカウントA]がdomuserへログイン
2. [時刻] に[アカウントA]でRDP接続
3. [時刻] に[アカウントB]が[アカウントA]を作成
4. [時刻] に[IPアドレス]から[IPアドレス]の[アカウントB]へ[攻撃手法]

以降では、具体的なX

ハンズオン２

演習

分析の観点

- ハンズオン１から得られた情報をもとに、分析観点を絞る
- どのログを分析するべきか考える
- 知りたいことは、以下のポイント
  - ✓ いつ
  - ✓ 誰が
  - ✓ 何を
  - ✓ どのように

「ハンズオン１から得られた情報」とは、10月11日10:12に10.10.100.105からdomuserへログインしたという調査結果です。

ハンズオン２

演習

ヒント　**確認するファイル：Security.evtx**

1. ハンズオン１で、侵害の起点になったアカウントは？
   - 何のアカウントから何のアカウントにログインを試みているか
2. そのユーザーは正規ユーザーか？
   - 把握していない（本資料 P.7）ユーザーはいないか？
   - ユーザーアカウントが作成された際のイベントIDは、**4720**
3. 把握していないユーザーは、何のアカウントから作成されたか？
   - アカウント作成は管理者権限でないとできないはず
4. ユーザー作成したアカウントはどうやって乗っ取られた？
   - 接続元IPアドレスを特定できればOK

問題１から順番に回答することにこだわらずに、わかるところから調査を進めてください。

ハンズオン２

演習

回答

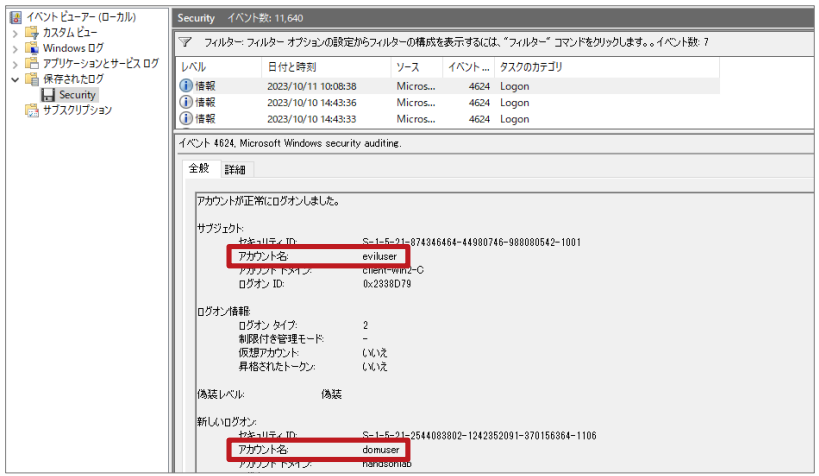
1. 10月11日10:08にeviluserがdomuserへログイン
2. 10月11日9:47にeviluserでRDP接続
3. 10月11日9:46にitmanagerがeviluserを作成
4. 10月11日9:44に10.10.100.104から10.10.100.105のitmanagerへPass-the-Hash

➡**通常、Kerberos認証のところNTLM認証が発生しており、Pass-the-Hashの使用が推測できる**

ハンズオン２

演習

回答 1. 10月11日10:08にeviluserがdomuserへログイン

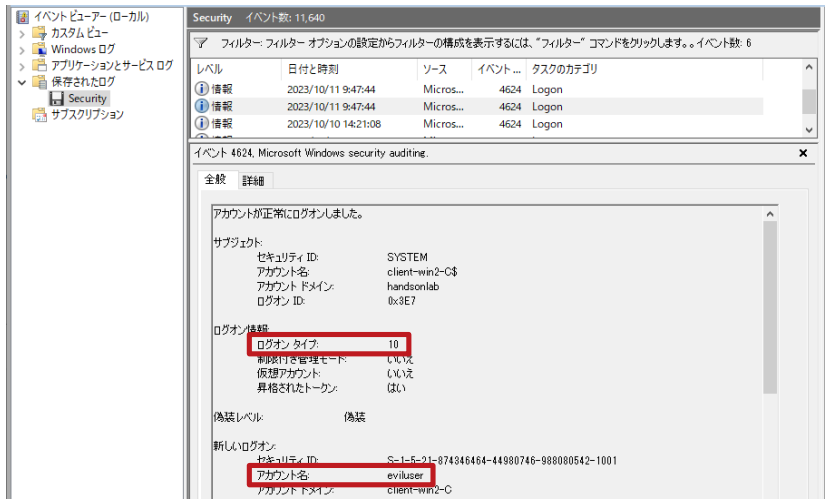


10月11日10:12に10.10.100.105からdomuserへログインしたというハンズオン１の調査結果から、それに最も近い時間のログインが攻撃アクティビティに関連している可能性が高い。

ハンズオン２

演習

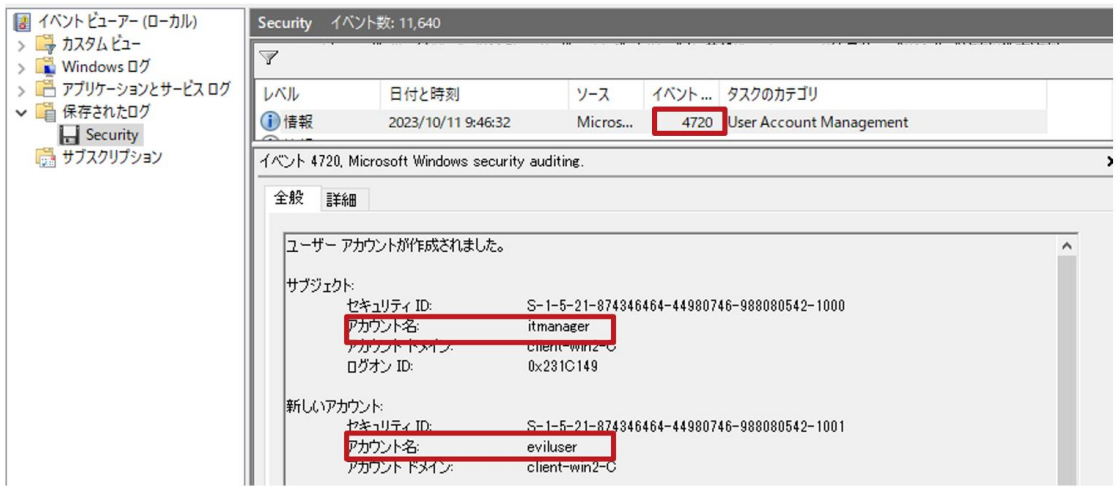
回答 2. 10月11日9:47にeviluserでRDP接続



ハンズオン２

演習

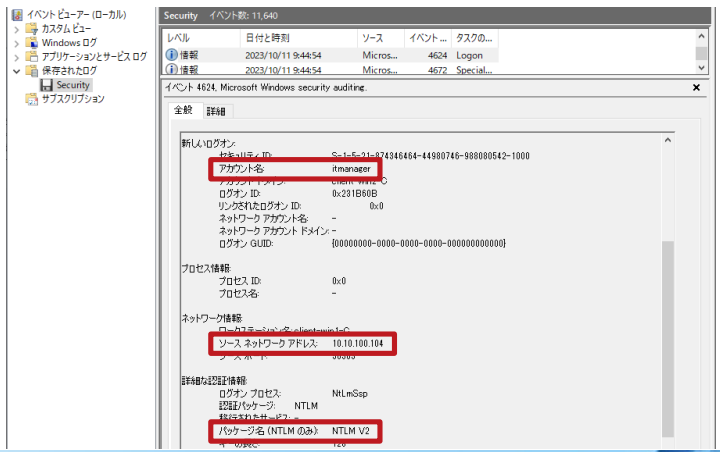
回答 3. 10月11日9:46にitmanagerがeviluserを作成



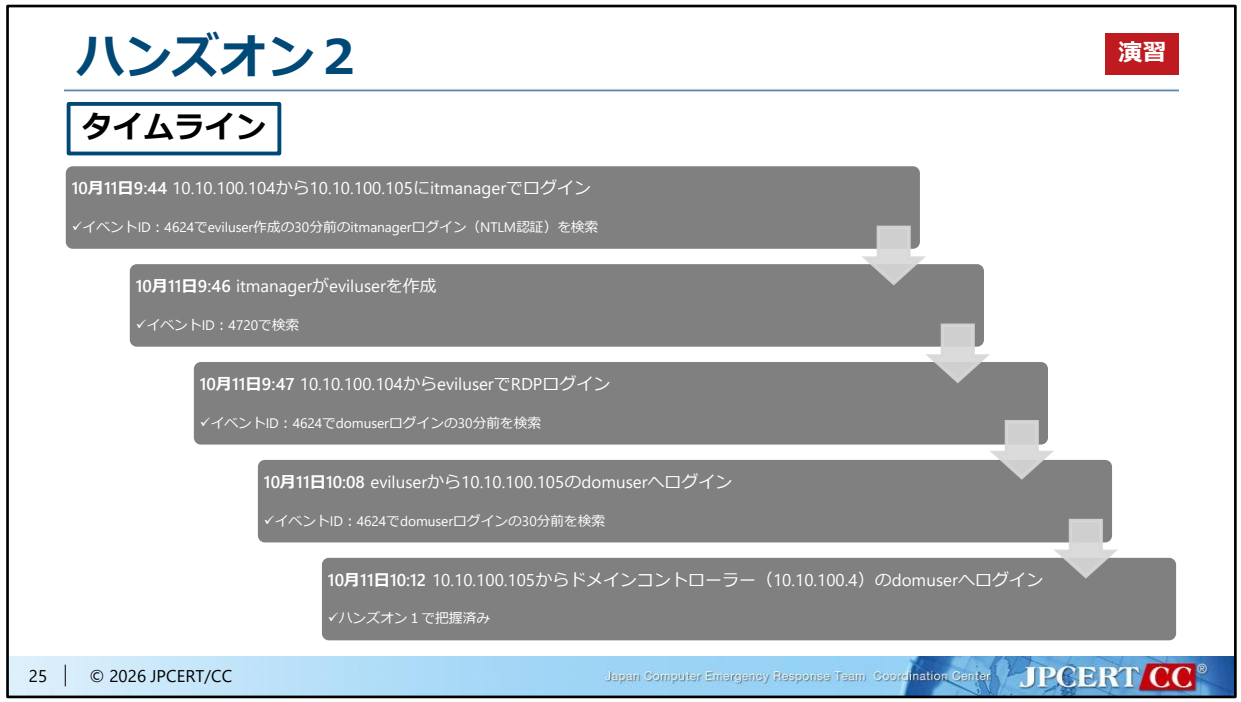
ハンズオン２

演習

回答 4. 10月11日9:44に10.10.100.104から10.10.100.105のitmanagerへPass-the-Hash



このログからだけでは本当にPass-the-Hashが発生したかは断定できませんが、この環境の認証ログを確認するとほとんどがKerberos認証であり、NTLMが何らかの意図しない動作によって発生していることが推測できます。
NTLM認証であることから、Pass-the-Hashが攻撃に使われている可能性があると考えられます。



ハンズオン１とハンズオン２の結果をあわせてタイムラインを作成してください。

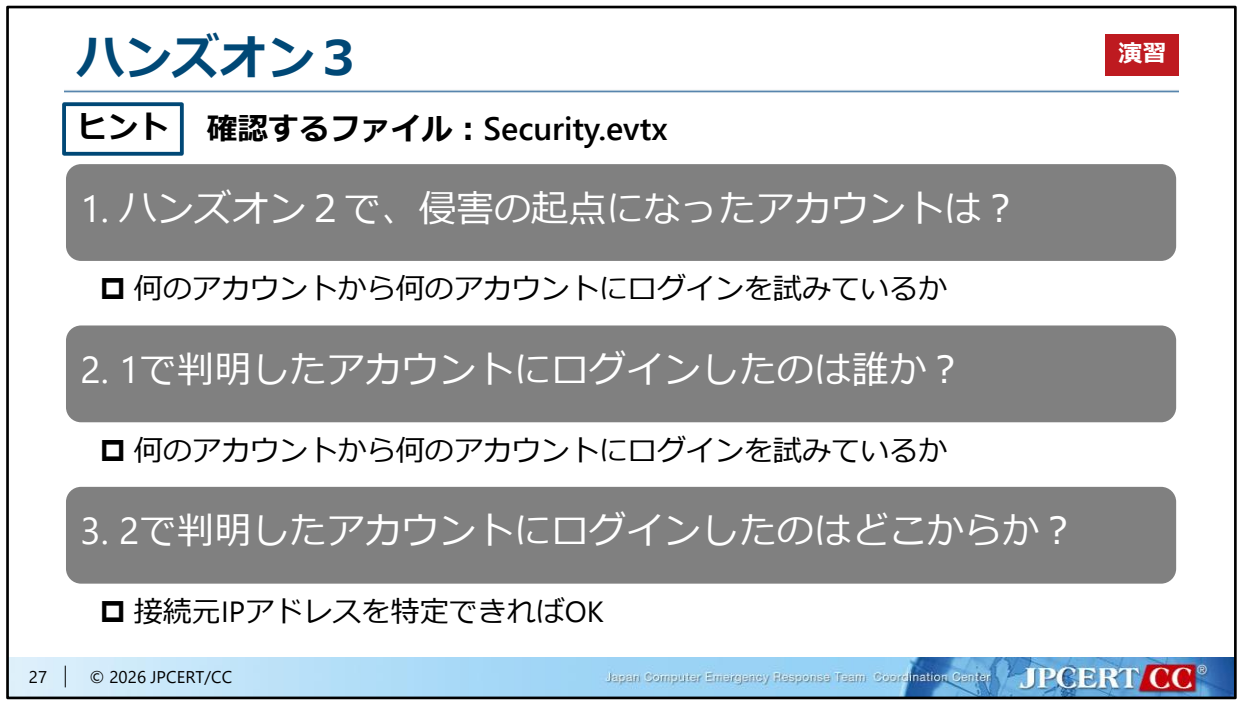
ハンズオン３

演習

先ほどの分析で、**10月11日9:44**に検証機（10.10.100.104）から不正ログインがあったことが分かったため、調べたいと思います。
クライアントのイベントログを取得したので、分析してください。

問題 ログ分析を行い、以下の空欄を埋めてください。

1. 時刻 にアカウント から itmanager へログイン
2. 時刻 にアカウント から アカウント へログイン
3. 時刻 に10.10.100.254（VPN）から アカウント へログイン



ハンズオン２で判明した調査結果は、「10月11日9:44に10.10.100.104から10.10.100.105のitmanagerへPass-the-Hashに10.10.100.104から10.10.100.105のitmanagerへPass-the-Hash」です。

ハンズオン３

演習

回答

1. 10月11日9:44にtestadmin001からitmanagerへログイン
2. 10月11日9:30にtestuserからtestadmin001へログイン

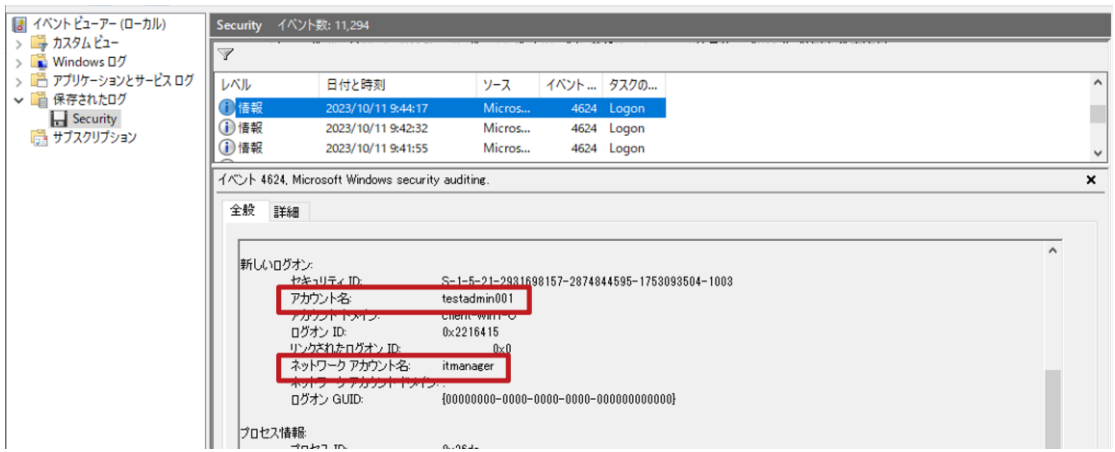
   ➡**ローカル管理者アカウントへのログインが発生**

3. 10月11日9:26にVPNからtestuserへログイン

ハンズオン３

演習

回答 1. 10月11日9:44にtestadmin001からitmanagerへログイン

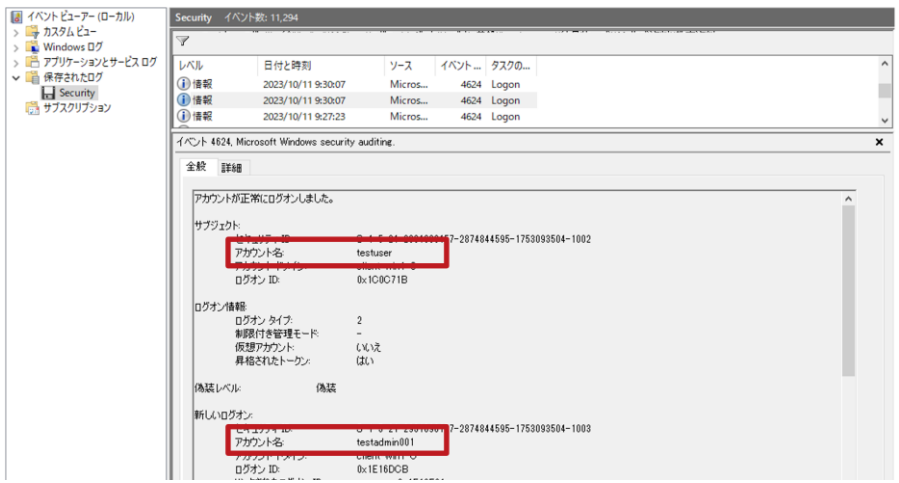


10月11日9:44に10.10.100.104から10.10.100.105のログインがハンズオン１で確認されていることから、その時刻に最も近いログインが関係していると推測できます。

ハンズオン３

演習

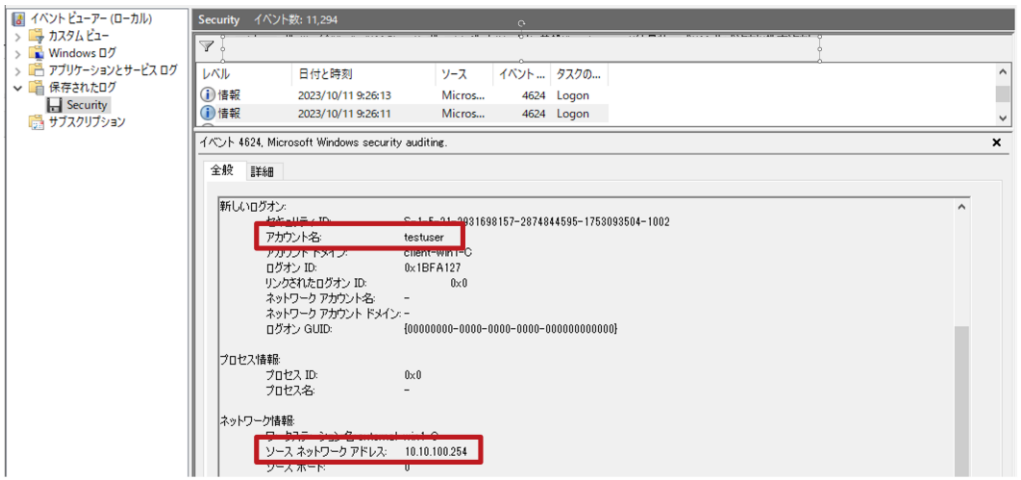
回答 2. 10月11日9:30にtestuserからtestadmin001へログイン



ハンズオン３

演習

回答 3. 10月11日9:26にVPNからtestuserへログイン



ハンズオン３

演習

タイムライン

testuserからtestadmin001への複数回の認証失敗

✓イベントID：4625でtestadmin001への昇格時30分前を検索

10月11日9:26 VPNからtestuserへログイン **10月11日9:38** testuserからtestadmin001へログイン

✓イベントID：4624でitmanagerログインの30分前を検索

10月11日9:41 VPNからtestadmin001へログイン

✓イベントID：4624でitmanagerログインの30分前を検索

✓LogonType 9かつログオンプロセスがseclogoでRunASをVPN越しに使っている

10月11日9:44 testadmin001からitmanagerへログイン

✓イベントID：4624でitmanagerログインの30分前を検索

10月11日9:44 10.10.100.104からitmanagerでログイン

✓ハンズオン２で把握済み

ハンズオン４

演習

ドメインコントローラーを再度見てみると、NTDSをダンプした痕跡がありました。そのため、情報を外部に送信していないか調べたいと思います。
プロキシサーバー（Squid）のログを取得したので、分析してください。

問題 ログ分析を行い、以下の空欄を埋めてください。

1. 時刻 に 外部IPアドレス からドメインコントローラーの情報が送信された

ハンズオン4では、イベントログの分析から離れて、プロキシログの分析を行います。

ハンズオン４

演習

ヒント

通信量の多いログはどれか？

- データを外部に送信する際は、それなりの通信量になる

送信されたデータは、どのような形式になっているか？

- 送信データは平文で送信されているのか、エンコードされているのか

ハンズオン４

演習

回答

1. 10月12日2:00ごろに10.10.100.105から
   ドメインコントローラーの情報が送信された

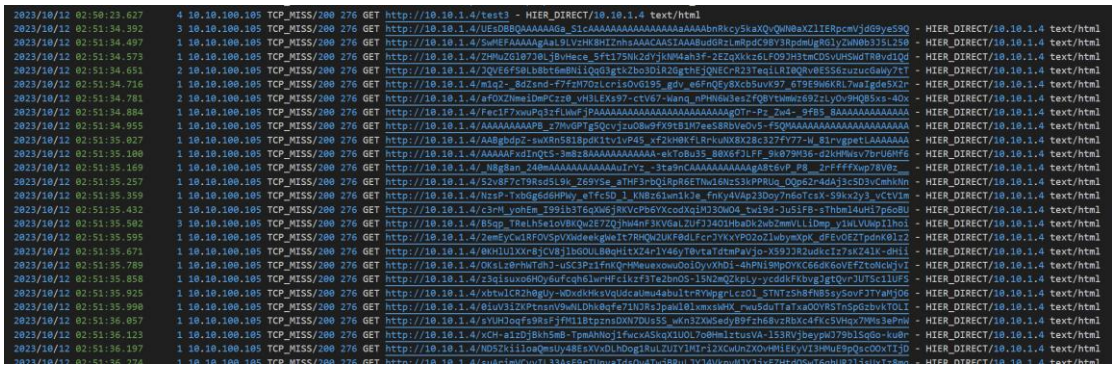
解説：

- 10月12日2:52から5:41まで、膨大な量の通信が
  確認できる
- 通信データはBase64エンコードされており、
  10.10.1.4に向けて送信されたデータを番号順につなげて
  デコードすると、ZIP圧縮されたNTDSファイルになる

ハンズオン４

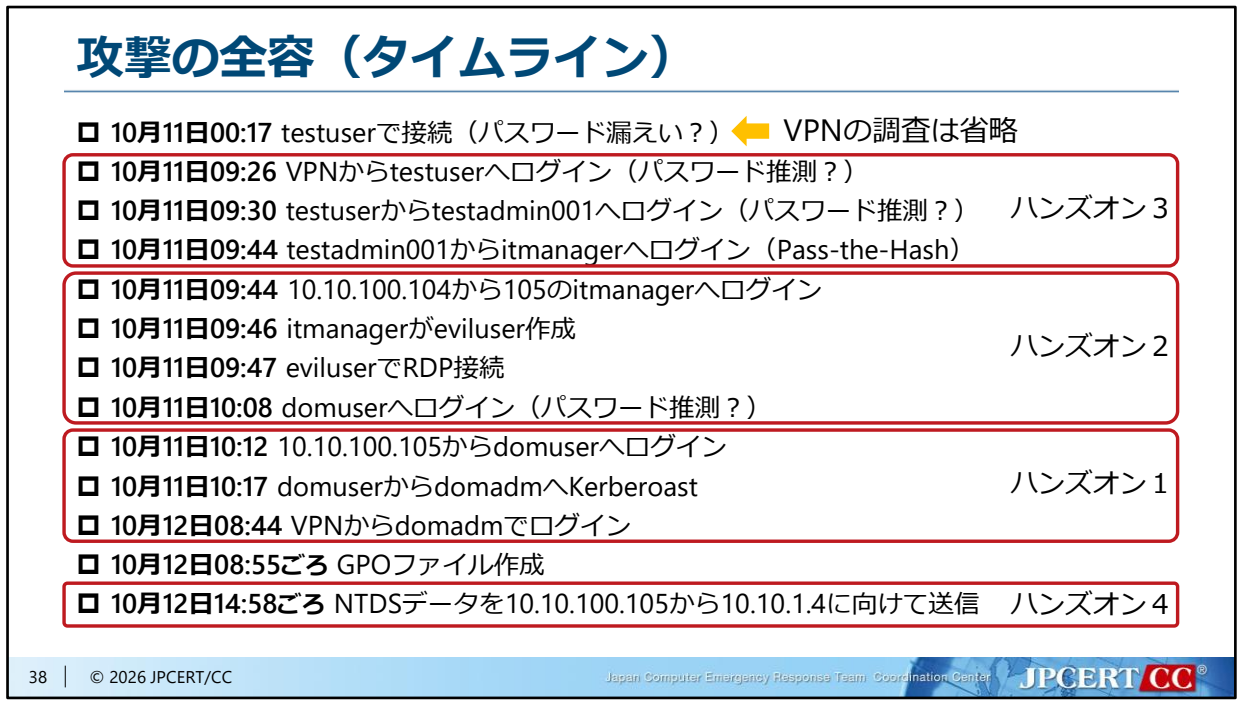
演習

回答 1. 10月12日2:00ごろに10.10.100.105から
ドメインコントローラーの情報が送信された



攻撃の全容（タイムライン）

- **10月11日00:17** testuserで接続（パスワード漏えい？）
- **10月11日09:26** VPNからtestuserへログイン（パスワード推測？）
- **10月11日09:30** testuserからtestadmin001へログイン（パスワード推測？）
- **10月11日09:44** testadmin001からitmanagerへログイン（Pass-the-Hash）
- **10月11日09:44** 10.10.100.104から105のitmanagerへログイン
- **10月11日09:46** itmanagerがeviluser作成
- **10月11日09:47** evilユーザでRDP接続
- **10月11日10:08** domuserへログイン（パスワード推測？）
- **10月11日10:12** 10.10.100.105からdomuserへログイン
- **10月11日10:17** domuserからdomadmへKerberoast
- **10月12日08:44** VPNからdomadmでログイン
- **10月12日08:55ごろ** GPOファイル作成
- **10月12日14:58ごろ** NTDSデータを10.10.100.105から10.10.1.4に向けて送信



本ハンズオンで判明した調査結果をタイムラインにすると、このようになります。
このように、イベントログを活用すると、どのアカウントが悪用されて、どの端末にログインされているのかを追うことができます。
しかし、イベントログだけでは攻撃手法の断定までは難しく、Sysmonや監査ログ、その他セキュリティ製品など別の手段でログを取得しなければいけません。

イベントログではどこまでの調査が可能かを把握して、不足点を補うログ取得の準備を平常時に進めることをお勧めします。

おわりに

Windowsログをイベントビューアーだけで分析するのは難しい

- イベントビューアー以外の分析方法を普段からトレーニングしておくことで、実際の調査をスムーズにすることができる
- SIEMなどでログを一元管理することで調査のスピードは上がる

調査で判明した事象をタイムライン化することで、どこの調査が不足しているのか、攻撃の起点の推測につながる

- 各端末から得られる断片情報をメモしながら、常にタイムラインを作成することを意識しながら分析する

イベントログで判明する事象もあるため、ログの管理が重要

- ドメインコントローラーなどのイベントログはログ量が多いため、過去のログが上書きされないようにする
  - ✓ 別サーバーでの管理
  - ✓ EVTXファイルのサイズ変更