

# 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](mailto:pr@jpcert.or.jp)

# 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
  - 自身に合ったツールを使ったり、自分のお好みのツールを見つけるために様々なツールを使ってみるのもよい

# ハンズオン イントロダクション

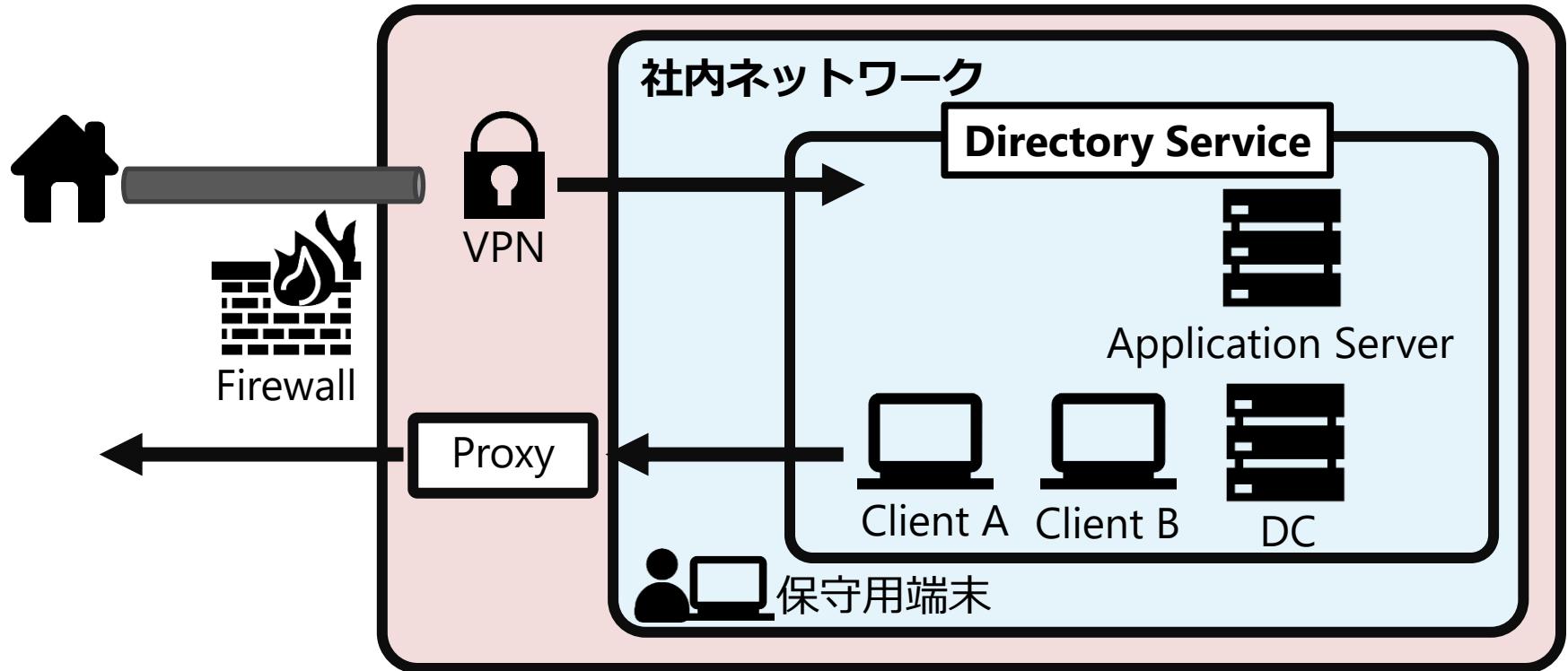
あなたは会社のセキュリティ担当者です。

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。

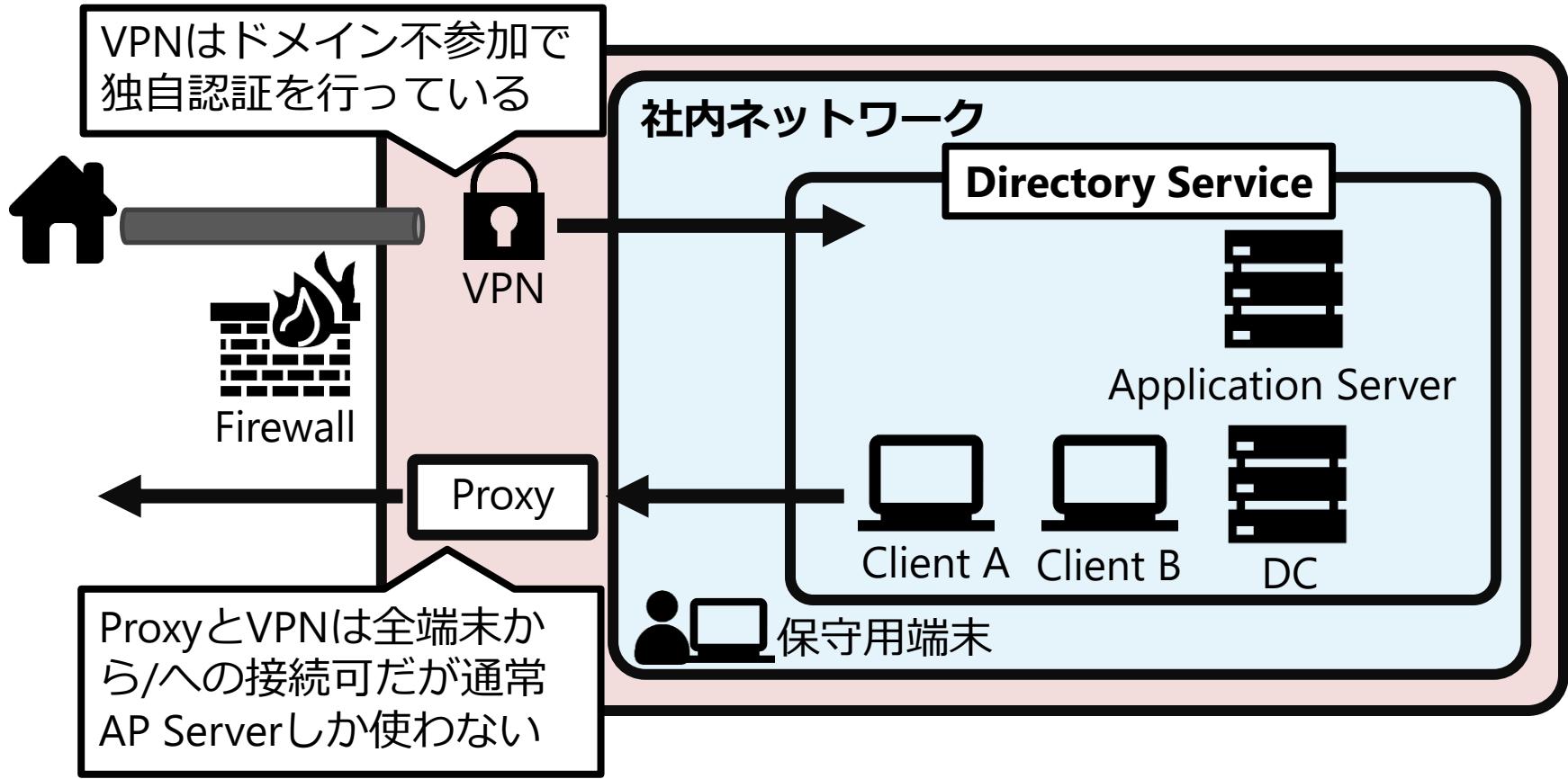
Windows Update等による影響かと考えましたが、ほぼ同じ構成の私用PCではそういうファイルが生成されておらず、自社の業務PCでのみ確認される事象であることが分かりました。

さて、このファイルは何処から来て、誰が設置したものなのでしょうか。

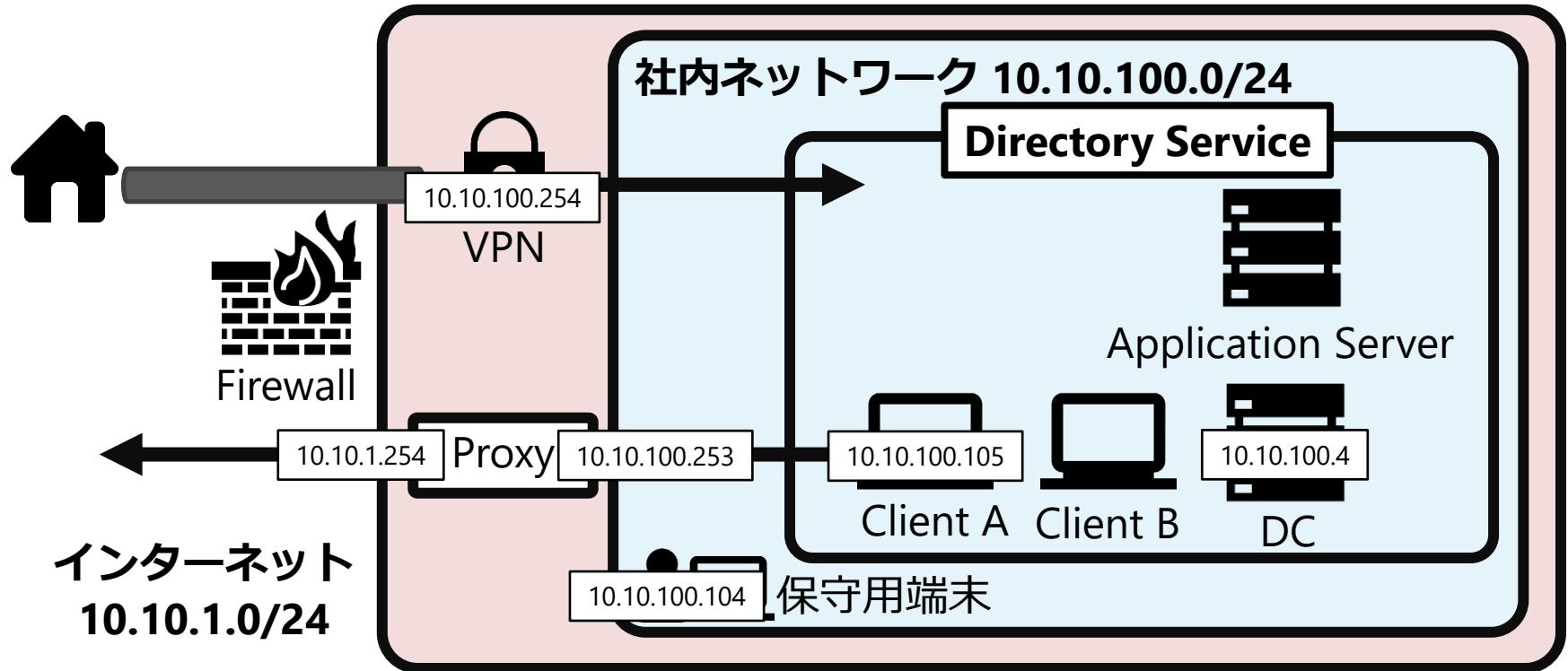
# ハンズオン システム構成図



# 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。

# ハンズオン 1

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、10/12 8:55頃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、以下の空欄をうめてください。

- 時刻 に 10.10.100.254(VPN) から アカウント で ログイン
- 時刻 に アカウント から アカウント へ 攻撃手法
- 時刻 に IPアドレス から アカウント へログイン

# ハンズオン 1

## 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アドレスを特定出来ればOK

# ハンズオン 1

## 回答

1. 10/12 8:44に10.10.100.254(VPN)からdomadmでログイン  
→事象発生(10/12 8:55)時周辺のドメイン管理者でのログインを確認
2. 10/11 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. 10/11 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. 10/12 8:44に10.10.100.254(VPN)からdomadmでログイン

The screenshot shows the Windows Event Viewer interface. The left 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 (highlighted with a red box), 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 4624) is selected, which occurred at 2023/10/12 8:44:25. The event details are shown in a large window:

全般	詳細
新しいログオン:	セキュリティ ID: S-1-5-21-2544083802-1242352091-370156364-1105 アカウント名: domadm (highlighted with a red box) アカウント ライブ: Handoverlab ログオン ID: 0x1AAD725 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: external\win10 ソース ネットワーク アドレス: 10.10.100.254 (highlighted with a red box) ポート: 0

# ハンズオン 1

回答

1. 10/12 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. 10/11 10:17にdomuserからdomadmへkerberoast

Security イベント数: 59,898

filtrer: 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 ...	タスクのカテゴリ
情報	2023/10/11 10:17:17	Micros...	4769	Kerberos Service Ticket Operations

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 プラン:	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:	3-1-0-21-2844088802-1242352091-370156364-1105

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:	-

# ハンズオン 1

回答

2. 10/11 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

## 回答

3. 10/11 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 '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', and '保存されたログ' (Security). 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	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 (Event ID 4624) is shown below. The '全般' tab is selected. The event details are as follows:

**新しいログオン:**

- セキュリティ ID: S-1-5-21-2544083802-1242852091-370156364-1106
- アカウント名: domuser (highlighted)
- アカウント 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:**

- ソース ネットワーク シンボル: ワークステーション
- 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

# ハンズオン 1

## タイムライン

**10/11 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

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

✓ イベントID:4769で10/12 8:43以前をdomadmで検索

**10/12 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

## ハンズオン 2

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、以下の空欄をうめてください。

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

# ハンズオン 2

## 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
  - ✓ だれが
  - ✓ 何を
  - ✓ どのように

# ハンズオン 2

## 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. そのユーザは正規ユーザか？

□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出来ないはず

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アドレスを特定出来ればOK

# ハンズオン 2

回答

1. 10/11 10:08 に eviluser が domuser ヘログイン
2. 10/11 9:47 に eviluser で RDP接続
3. 10/11 9:46 に itmanager が eviluser を作成
4. 10/11 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. 10/11 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 several log types: イベントビューアー (ローカル), カスタムビューアー, 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 (Level), 日付と時刻 (Date and Time), ソース (Source), イベント (Event ID), and タスクのカテゴリ (Task Category). There are three entries:

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 10:08:38	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 message reads "イベント 4624, Microsoft Windows security auditing." followed by tabs for "全般" and "詳細".

The "詳細" tab contains detailed information about the first event (Logon ID: 0x2338D79):

- サブプロジェクト: 0x15-24-071346464-44980746-988080542-1001
- アカウント名: eviluser
- ログオンタイプ: Client Win32
- ログオン ID: 0x2338D79

Below this, "ログオン情報" (Logon Information) details are shown:

- 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

At the bottom, "偽装レベル" (Impersonation Level) is listed as "偽装" (Impersonation).

Finally, a "新しいログオン" (New Logon) section shows another event for "domuser":

ソース	アカウント名
0x15-24-071346464-44980746-988080542-1106	domuser

The "アカウント名" (Account Name) field is highlighted with a red box.

# ハンズオン 2

回答

2. 10/11 9:47 に eviluser でRDP接続

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of log types: イベントビューア (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, and 保存されたログ. The 保存されたログ node is expanded, showing Security and Subscription. The main pane is titled "Security" with "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 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 タスクのカテゴリ (Task Category). Three entries are listed:

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 entry states "イベント 4624, Microsoft Windows security auditing.". The right pane shows detailed information for the first logon event. It includes tabs for "全般" (General) and "詳細" (Details). The "全般" tab contains the message "アカウントが正常にログオンしました。" and the "サブジェクト" section with fields: 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. The "ログオン情報" section is highlighted with a red box and contains the following fields:

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

The "偽装レベル" (Impersonation Level) is listed as "偽装" (Impersonation). The "新しいログオン" (New Logon) section is also highlighted with a red box and contains the following fields:

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. 10/11 9:46 に itmanager が eviluser を作成

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 is titled 'Security' with 'イベント数: 11,640'. A table displays event details:

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

Below the table, a message states 'イベント 4720, Microsoft Windows security auditing.' The '詳しい' tab is selected in the bottom-left corner. The detailed view shows the following information:

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. 10/11 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.

新しいログオン:

セキュリティ ID:	3-1-0-21-07454044-44980746-988080542-1000
アカウント名:	itmanager
アカウントタイプ:	client-win20
ログオン ID:	0x231B60B
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:	client-win20
ソース ネットワークアドレス:	10.10.100.104
ポート番号:	30305

詳細な認証情報:

ログオン プロセス:	NtLmSsp
認証ハッシュ:	NTLM
進行中のハッシュ:	-
パッケージ名 (NTLMのみ):	NTLM V2

# ハンズオン 2

## タイムライン

**10/11 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itmagerログイン（NTLM認証）を検索

**10/11 9:46** itmanagerがeviluserを作成

✓イベントID: 4720で検索

**10/11 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

**10/11 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

**10/11 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

# ハンズオン3

先ほどの分析で、**10/11 9:44**に検証機（10.10.100.104）から不正ログインがあった事が分かったため、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、以下の空欄をうめてください。

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3

## 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どこからか？

□接続元IPアドレスを特定出来ればOK

# ハンズオン3

回答

1. 10/11 9:44 に testadmin001 から itmanager ヘログイン
2. 10/11 9:30 に testuser から testadmin001 ヘログイン  
➡ ローカル管理者アカウントへのログインが発生
3. 10/11 9:26 に VPN から testuser ヘログイン

# ハンズオン3

## 回答

- 10/11 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 'イベントビューアー (ローカル)' selected, followed by '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 in blue), and 'サブスクリプション'. The right pane is titled 'Security イベント数: 11,294' and shows a table of events. The first event in the list is highlighted in blue and details a 'Logon' event at 2023/10/11 9:44:17. The event table has columns for 'レベル' (Level), '日付と時刻' (Date and Time), 'ソース' (Source), 'イベント ID' (Event ID), and 'タスクの...' (Task). The event details are as follows:

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 9:44:17	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 reads 'イベント 4624, Microsoft Windows security auditing.'.

The 'Security' event details window is open, showing the 'General' tab. It displays information about a new logon:

- セキュリティ ID: S-1-5-21-2931698157-2874844595-1753093504-1003
- アカウント名: **testadmin001** (highlighted)
- ノードタイプ: client-win32
- 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** (highlighted)
- ネットワークノードタイプ: {00000000-0000-0000-0000-000000000000}
- ログオン GUID: {00000000-0000-0000-0000-000000000000}

# ハンズオン3

## 回答

### 2. 10/11 9:30 に testuser から testadmin001 へログイン

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of logs, with the 'Security' log selected. The right pane shows a list of events with the following details:

レベル	日付と時刻	ソース	イベントID	タスクの種類
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

A detailed view of the third event (Logon ID: 0x1C0C71B) is shown in the foreground. The 'アカウント名' (Account Name) field is highlighted with a red box and contains 'testuser'. Another event (Logon ID: 0x1E16DCB) is also partially visible at the bottom.

# ハンズオン 3

回答

3. 10/11 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 'イベントビューアー (ローカル)' and several log types. The 'Security' log is selected, showing two logon events at 2023/10/11 9:26:13 and 2023/10/11 9:26:11. Both events are for source 'Micros...' and task ID 4624, labeled 'Logon'. A detailed view of the second event is open. The event details show a new logon for account 'testuser' (client=win10c). The source network address is listed as '10.10.100.254'. The event viewer window title is 'イベント 4624. Microsoft Windows security auditing.'

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

新しいログオン:

セッション ID:	S-1-5-21-9831698157-2874844595-1753093504-1002
アカウント名:	testuser
アカウント ドメイン:	client=win10c
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:

ワークステーション名:	10.10.100.10
ソース ネットワーク アドレス:	10.10.100.254
ソース ポート:	0

# ハンズオン3

## 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

**10/11 9:26** VPNからtestuserへのログイン **10/11 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

**10/11 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

**10/11 9:44** testadmin001からitmanagerへログイン

✓EventID:4624でitmanagerログインの30分前を検索

**10/11 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

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、情報を外部送信していないか調べたいと思います。

プロキシサーバ（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、以下の空欄をうめてください。

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

## 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. 10/12 2時ごろ 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：

- 10/12 02:52～05:41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繋げ  
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. 10/12 2時ごろ 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
2023/10/12 02:51:34.392 3 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/UeSDBBQAAAAAGa_S1cAAAAAAAAAAAAAAaAAAAbnRkcy5kaXQvQWN0aXz1IERpcmVjdG9yeS9Q - 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/SwMEFAAAAAAgAaL9LzHk8HIZnhnsAACAAASIAAAAbudGrzLmRpdc9By3RpdmUgRgLyZWN0b3J5L250 - 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/ZHuMzG1070LjBvHece_f5f175Nk2dYjkN4ah3f-2EzqXkkz6_lF09JH3tmCDSvUHSWdTR0vd1Qd - 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/JQVE6fs8Lb8bt6mBnij0dg3gtkZbo3diR2ggthEj0NECr23TeqIRI0Qrv0ESS6uzucGaWly7T - 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/m1q2-_8dzsnd-f7fz7M0zLcrisOvg195_gdv_e6FnQEqy8Xcb5uvK97_6T9E9W6KRL7waIgde5Xr - 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/afOXZNmeiDmPCCzz0_vH3LEXs97-ctV67-Wanq_nPHN6W3esZfQBYtWmWz69ZzLy0v9HQB5xs-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/Fec1F7xwuPq3zfLWwFjPAaaaaaaaaaaaaaaaAgOTr-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/AAAAAAAAPB_z7MvgPTg5Qcqjzu08w9fx9tB1M7eeS8RbVe0v5-f50Maaaaaaaaaaaaaaaaaaaaaa - 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/AABgbdpZ-swXRn5818pd1kt1vP45_xf2K0H0kfLrkunNx828c327fY77-W_81rvgetLAAAAAA - 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-3m8zBAAAAAAAekToBu35_80x6fJLFF_9k079M36-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_240mAAAAAAAaIrYz_3ta9nCaaaaaaaAgAt6vP_P8_2rFffffXwp78v0z_ - 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://10.10.1.4/52v8F7c79Rsds5l9k_Z69YSe_aTHf3rBqirpR6ETnw16Ns3kppruQ_QOp62r4dAj3c5D3vCmhkNn - 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-TxbGg6d6HPWyeTfc5D_1_KNBz61wn1kJe_fnKy4VAp23Doy7n6oTcsx-S9kx2y3_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_yohEm_I99ib3T6qXw6jRKvCpb6YXcodXqimj30W04_twi9d-Ju5iBf-sThbml4uHi7p6oBu - 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_TreLh5el0vBKQw2E7ZQjh4nf3KVGaLZUfJJ401HbaDk2wbZmmVLliDmp_y1WLvUWp1lhoi - 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://10.10.1.4/2emEyCv1RF0VSpVxWdeegkWeIt7RHQ2MUKf0dLfCrjYKxYP02oZlwbymXpk_dFEoEZTpndk01z2 - 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://10.10.1.4/0KhlU1XXr8jCV8j1bGOULB0qHitXz4r1Y46yT0vtaTdtmPaVyo-X59jjR2udkcIkz7sKZ41K-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/OKslz0rhWTdhJ-uSc3Pz1fnKqrHMeuxewouOoi0yvXhd-i4PhN19Mp0YKc66dK6oVefZtoNcwjvI - 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/z3qisuxo6Hoy6ufcqh61lrHfcikzf3Te2bnOS-15NmZkplY-yccdkFkbgvJgtYvrJUTSc11UFS - 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/xbtwlCR2h0gUy-WDxdkHksVqUdaUm4abultrRYWpgrLcz01_STNTzSh8fNb5sySovFJTyA MJ06 - 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://10.10.1.4/0iuV3izKPttsnV9wNLdh0qfe71NJRjsJaWl0lxmxswHX_rwu5duTTaxaOoYRStnSpGzbvkTOLI - 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/sYUHJqofs9RsFjfM1BtpznsDXN7DUss5_wKn3ZxwSedyB9Fzh68vzRbXc4fKc5VHqx7Mms3ePnw - 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-alzDjBkh5mB-TpmAhNoj1fwcxAsqkx1U0L7o@HmlztusVA-153RVjbeypWJ79b1SqGo-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/ND5ZkiloaQmsUy48EsXvDlhDog1ruLzUIY1Miri2XcwUnZx0vHmIEkyVi3HMuE9pQsc00xtijD - 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/suArimVCvylTL33AsF9rTluvaTdsOv4Tw1Bpu1JY14VkpvM7Y1jlyF7HtdosW76ghB21iLsuyTzRmg - HIER_DIRECT/10.10.1.4 text/html

```

# 攻撃の全容（タイムライン）

---

- **10/11 00:17** testuserで接続（パスワード漏えい？）
- **10/11 09:26** VPNからtestuserへログイン（パスワード推測？）
- **10/11 09:30** testuserからtestadmin001へログイン（パスワード推測？）
- **10/11 09:44** testadmin001からitmanagerへログイン（Pass-the-Hash）
- **10/11 09:44** 10.10.100.104から105のitmanagerへログイン
- **10/11 09:46** itmanagerがeviluser作成
- **10/11 09:47** eviluserでRDP接続
- **10/11 10:08** domuserへログイン（パスワード推測？）
- **10/11 10:12** 10.10.100.105からdomuserへログイン
- **10/11 10:17** domuserからdomadmへkerberoast
- **10/12 08:44** VPNからdomadmでログイン
- **10/12 08:55頃** GPOファイル作成
- **10/12 14:58頃** 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）

- **10/11 00:17** testuserで接続（パスワード漏えい？）VPNの調査は省略
- **10/11 09:26** VPNからtestuserへログイン（パスワード推測？）
- **10/11 09:30** testuserからtestadmin001へログイン（パスワード推測？）ハンズオン3
- **10/11 09:44** testadmin001からitmanagerへログイン（Pass-the-Hash）
- **10/11 09:44** 10.10.100.104から105のitmanagerへログイン
- **10/11 09:46** itmanagerがeviluser作成
- **10/11 09:47** eviluserでRDP接続ハンズオン2
- **10/11 10:08** domuserへログイン（パスワード推測？）
- **10/11 10:12** 10.10.100.105からdomuserへログイン
- **10/11 10:17** domuserからdomadmへkerberoastハンズオン1
- **10/12 08:44** VPNからdomadmでログイン
- **10/12 08:55頃** GPOファイル作成
- **10/12 14:58頃** 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