

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

- 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。

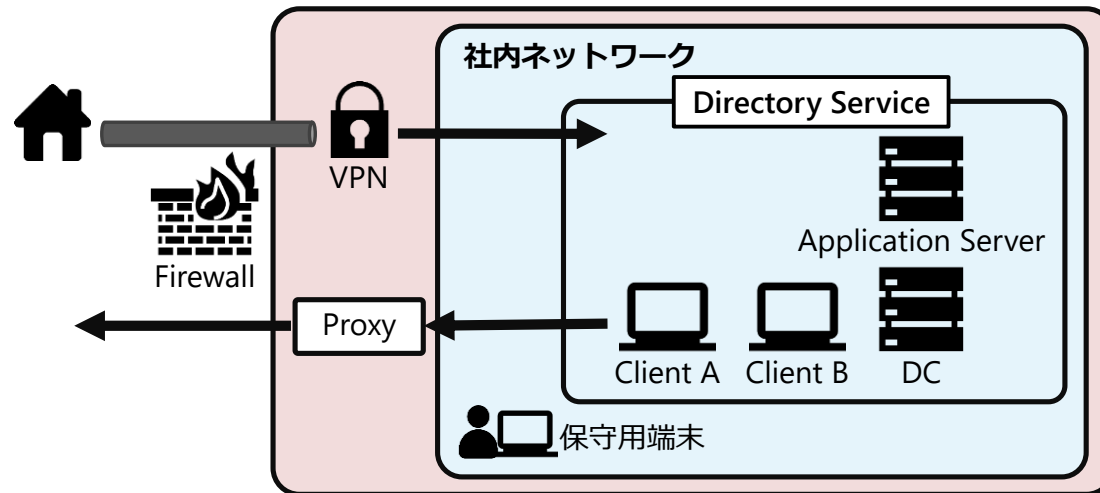
ある日、いくつかの部の職員から「見覚えのないファイルがデスクトップに生成されている」という報告を受けました。

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。

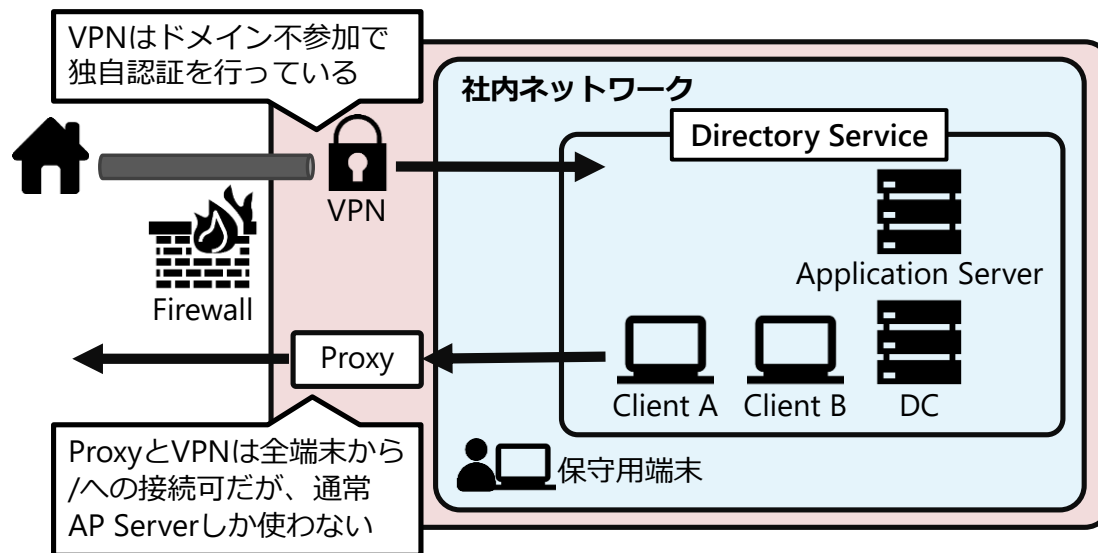
本ハンズオンでは、インシデント発生組織のログを分析することを想定して進めます。

ハンズオン システム構成図

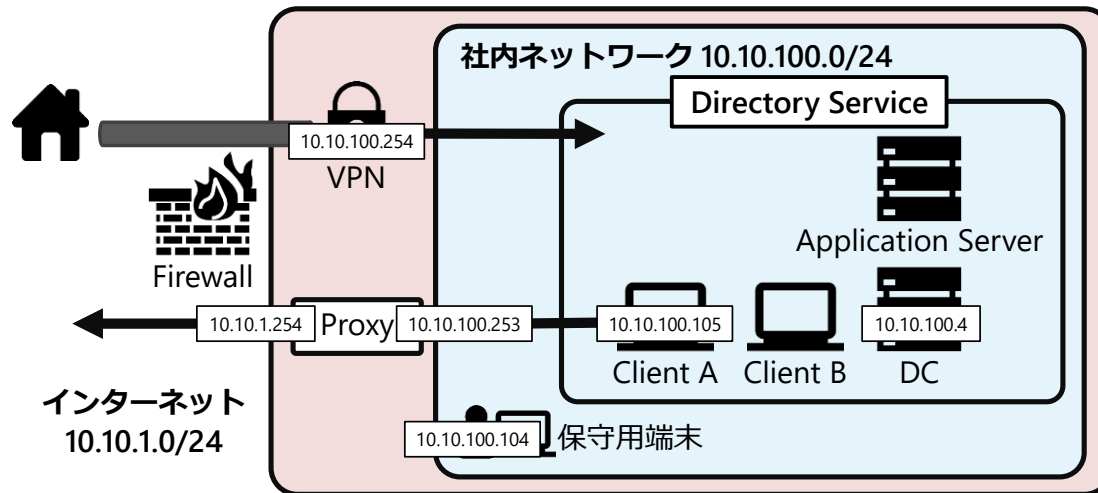


今回ハンズオンで分析するログを取得した環境を図に示します。

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

ハンズオン 1

演習

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

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

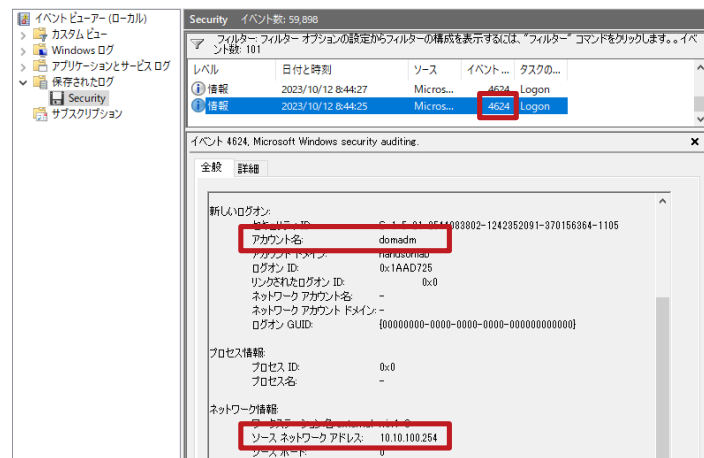
回答

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

The screenshot displays the Windows Security Event Viewer interface. The left-hand pane shows the navigation tree with 'Security' selected. The main pane shows a list of events, with event ID 4769, 'Kerberos Service Ticket Operations', selected. The event details pane on the right provides the following information:

- アカウント情報 (Account Information):**
 - アカウント名 (Account Name): domuser@HANDSONLAB.LOCAL
 - アカウント トメイン (Account Domain): HANDSONLAB.LOCAL
 - ログオン GUID (Logon GUID): {19a74800-2ce3-0572-0cb7-b5c4ff929b96}
- サービス情報 (Service Information):**
 - サービス名 (Service Name): domadm
 - サービス ID (Service ID): S-1-5-21-2544083802-1242852091-370156364-1105
- ネットワーク情報 (Network Information):**
 - クライアント アドレス (Client Address): ::ffff:10.10.100.105
 - クライアント ポート (Client Port): 61140
- 追加情報 (Additional Information):**
 - チケット オプション (Ticket Options): 0x40800000
 - チケット暗号化の種類 (Ticket Encryption Type): 0x17
 - エラー コード (Error Code): 0x0
 - 移行されたサービス (Transferred Service):

ハンズオン 1

演習

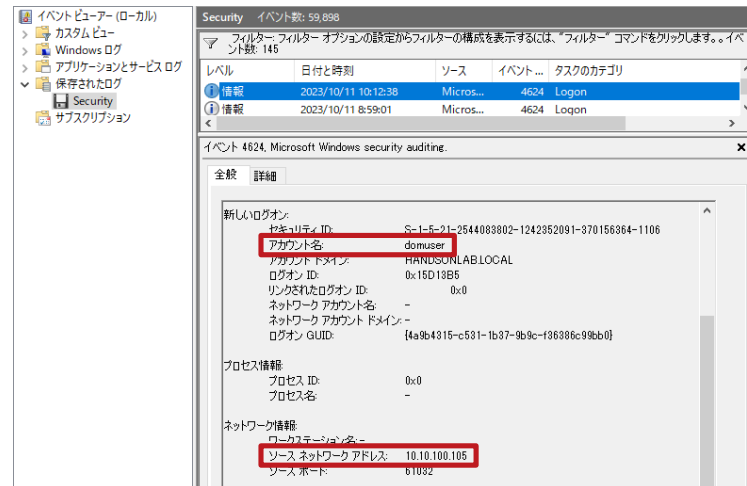
回答 2. 10月11日10:17にdomuserからdomadmへKerberoast

```
<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。

ハンズオン 1

演習

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

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

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

The screenshot shows the Windows Security Event Viewer interface. The left pane displays the 'Security' log. The right pane shows the details of event 4624, 'Microsoft Windows security auditing'. The event description states 'アカウントが正常にログインしました。' (Account successfully logged in). The subject is 'eviluser' (S-1-5-21-874346464-44980746-988080542-1001). The logon information shows 'ログオン タイプ: 2' (Logon type: 2), '制限付き管理モード: -' (Restricted administration mode: -), '仮想アカウント: (なし)' (Virtual account: (none)), and '昇格されたトークン: (なし)' (Elevated token: (none)). The logon source is 'クライアント' (Client). The logon target is 'domuser' (S-1-5-21-2544083802-1242352091-370156364-1106).

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	Microsoft Windows	4624	Logon
情報	2023/10/10 14:43:36	Microsoft Windows	4624	Logon
情報	2023/10/10 14:43:33	Microsoft Windows	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インしました。

サブジェクト:

- セキュリティ ID: S-1-5-21-874346464-44980746-988080542-1001
- アカウント名: eviluser
- アカウントタイプ: Client Win2-C
- ログオン ID: 0x2338079

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: (なし)
- 昇格されたトークン: (なし)

偽装レベル: 偽装

新しいログオン:

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

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

The screenshot displays the Windows Event Viewer interface. On the left, the 'Security' log is selected under 'イベントビューアー (ローカル)'. The main pane shows a list of events with columns for 'レベル', '日付と時刻', 'ソース', 'イベント...', and 'タスクのカテゴリ'. Event 4720 is highlighted, with a red box around the event ID. Below the list, the details for event 4720 are shown, including the message 'ユーザー アカウントが作成されました。' and the subject information. The subject information is divided into 'サブジェクト:' and '新しいアカウント:'. In both sections, the 'アカウント名:' field is highlighted with a red box and contains the value 'eviluser'. Other fields include 'セキュリティ ID:', 'アカウントドメイン:', and 'ログオン ID:'.

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 9:46:32	Micros...	4720	User Account Management

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

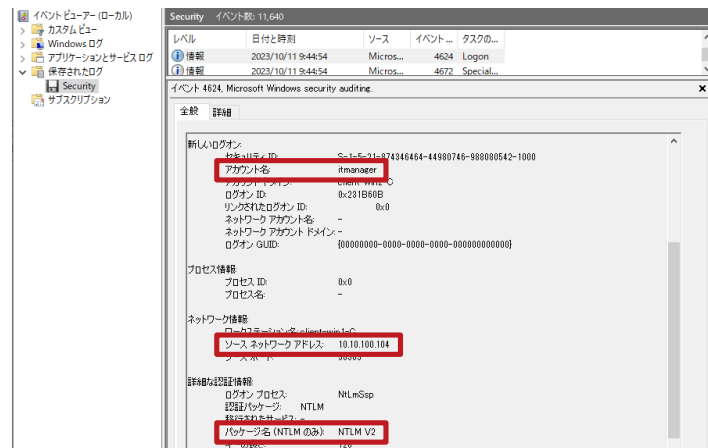
新しいアカウント:

- 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

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



24 | © 2026 JPCERT/CC

Japan Computer Emergency Response Team Coordination Center

JPCERT/CC

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ります。

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

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3

演習

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

The screenshot shows the Windows Event Viewer interface. The left pane displays the 'Security' log. The right pane shows a list of events, with event 4624 (Logon) selected. The details pane below shows the event data for event 4624, Microsoft Windows security auditing. The 'New Logon' section is expanded, showing the following details:

- セキュリティ ID: S-1-5-21-2931698157-2874844595-1753093504-1003
- アカウント名: testadmin001
- アカウントタイプ: Client - win...
- 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 アカウント ID: {00000000-0000-0000-0000-000000000000}
- ログオン GUID: {00000000-0000-0000-0000-000000000000}

The bottom of the window shows the footer: 29 | © 2026 JPCERT/CC Japan Computer Emergency Response Team Coordination Center JPCERT/CC

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

The screenshot displays the Windows Security Event Viewer interface. On the left, the 'Security' log is selected. The main pane shows a list of events, with event 4624 (Logon) selected. The details pane on the right shows the event information for event 4624, which is a successful logon for the user 'testuser'.

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インしました。

サブジェクト:

- ドメインID: 7-2674044595-1753093504-1002
- アカウント名: testuser
- クライアントIPアドレス: 192.168.1.100
- ログインID: 0x1C0C71B

ログイン情報:

- ログインタイプ: 2
- 制御付き管理モード: -
- 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

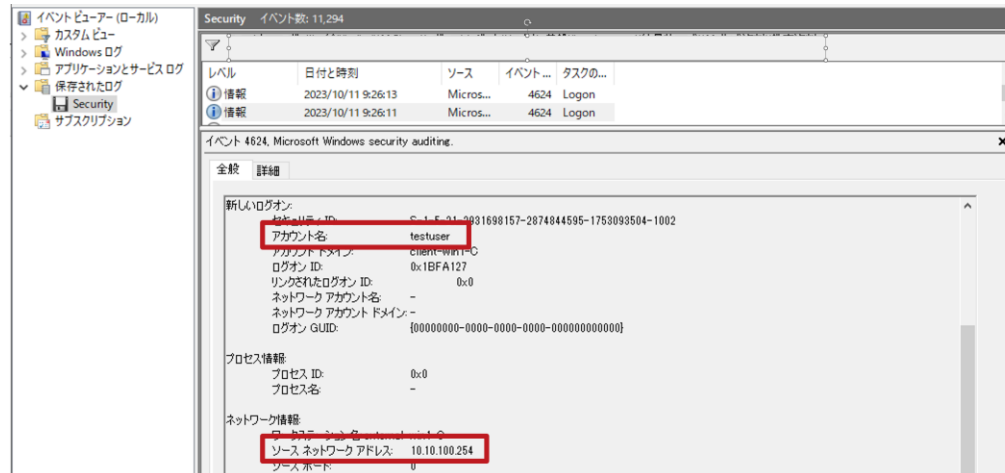
新しいログイン:

- ドメインID: 7-2674044595-1753093504-1003
- アカウント名: testadmin001
- クライアントIPアドレス: 192.168.1.100
- ログインID: 0x1E18DCB

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

演習

回答

© 2026 JPCERT/CC

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

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、どこが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