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

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

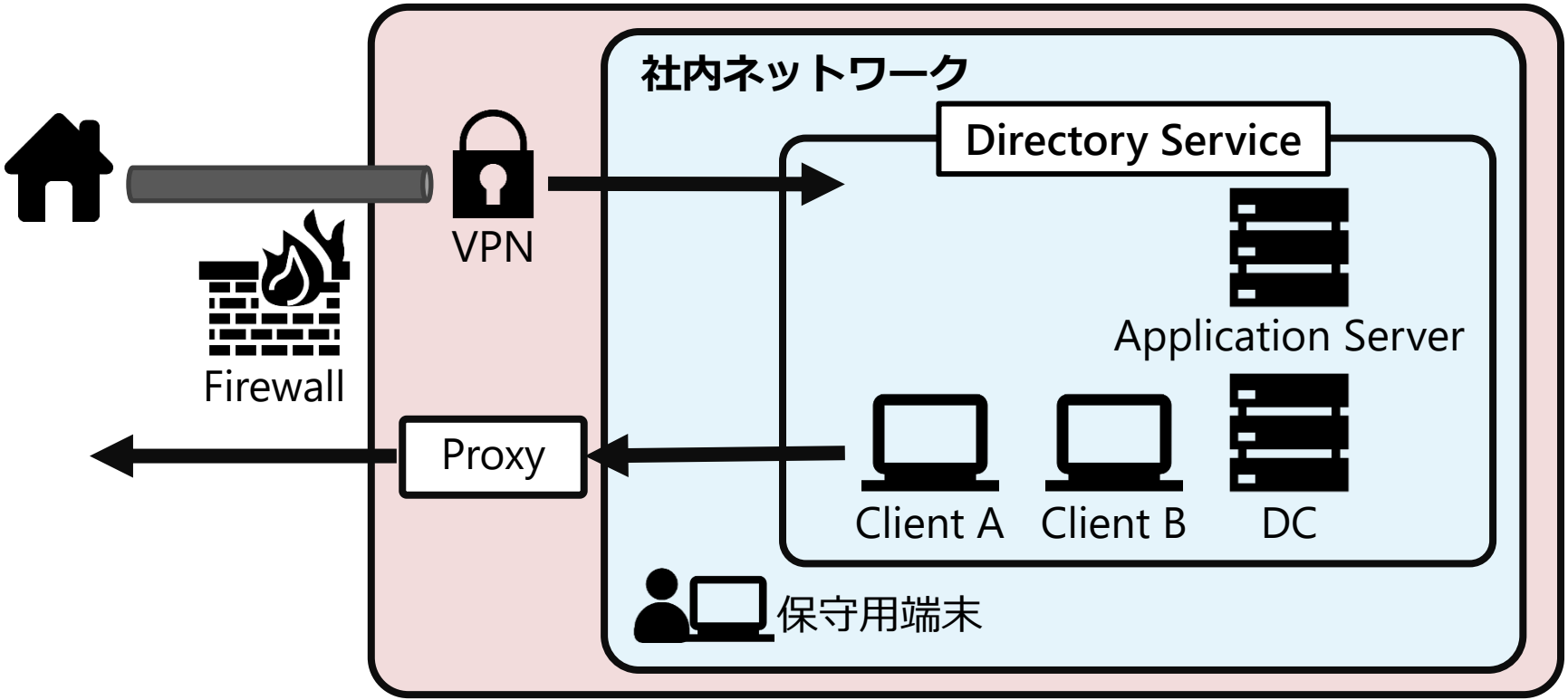
あなたは会社のセキュリティ担当者です。

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。

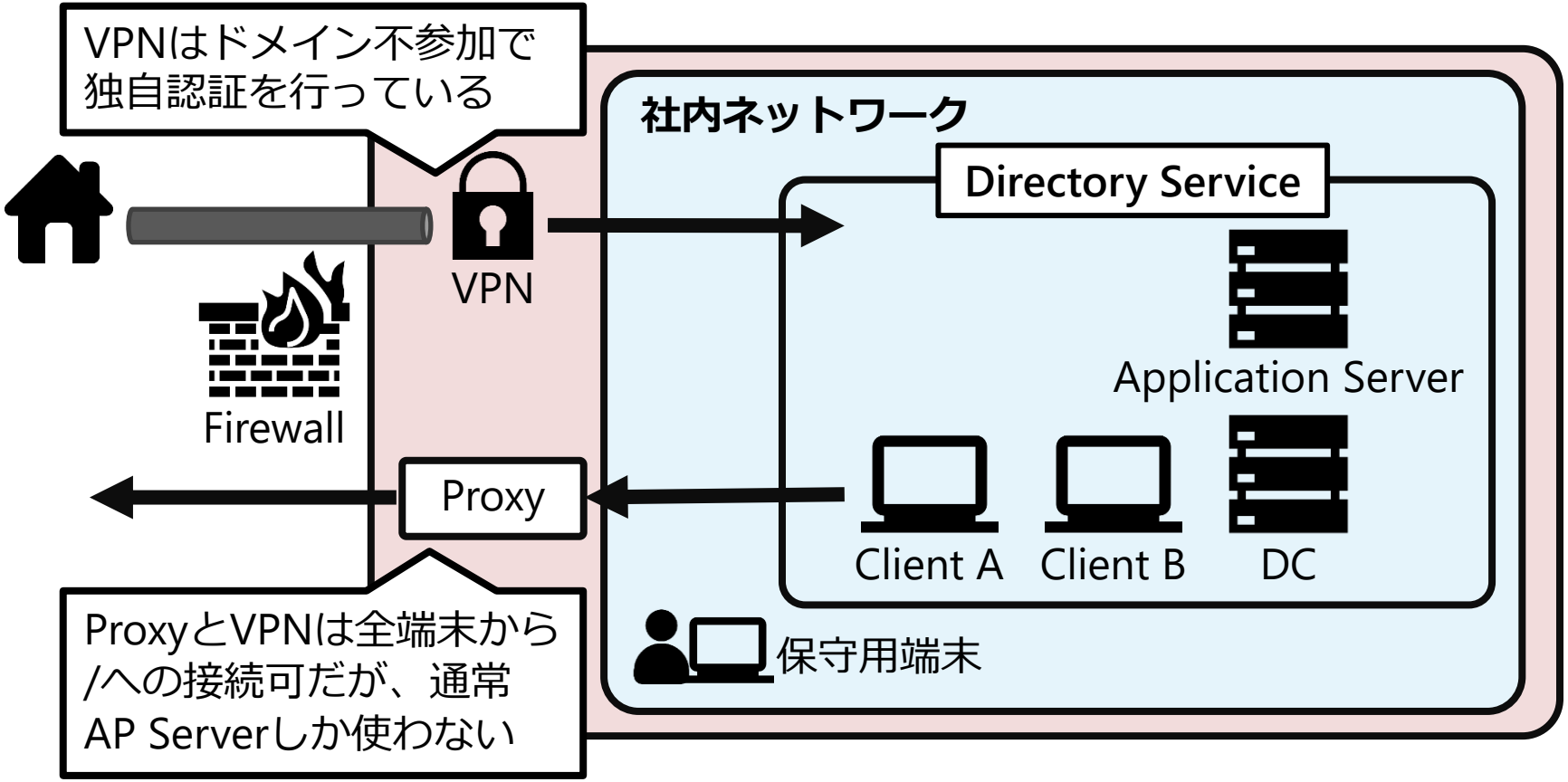
Windows Update等による影響かと考えましたが、ほぼ同じ構成の私用PCではそのようなファイルは生成されておらず、自社の業務PCでのみ確認される事象であることが分かりました。

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。

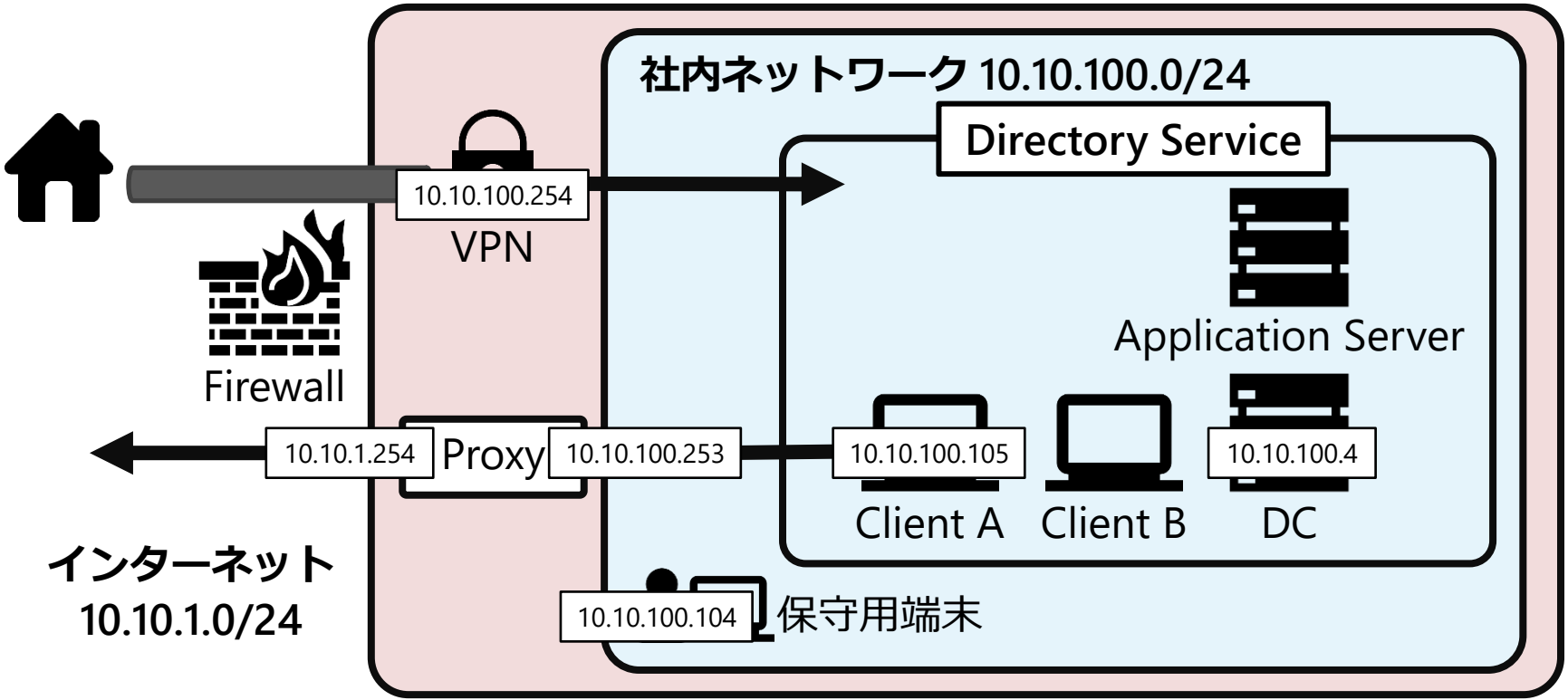
ハンズオン システム構成図



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

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

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

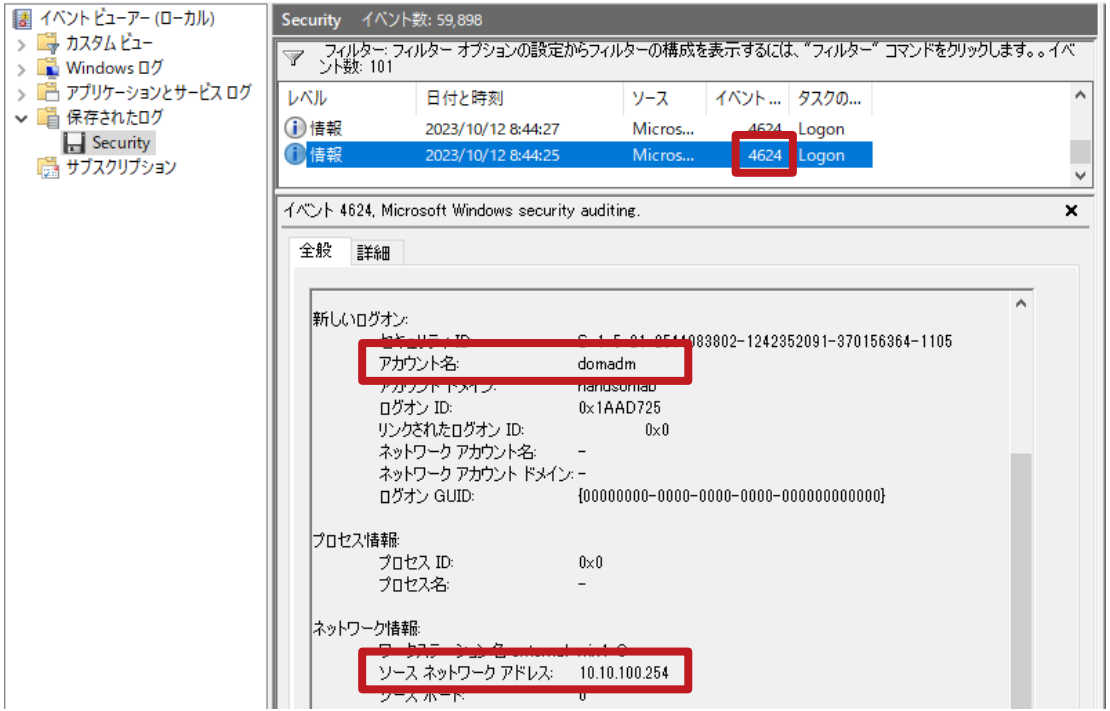
   ➡**ドメイン管理者に対するKerberosチケットの要求直前のログインを確認するとdomuserのログインを確認**

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

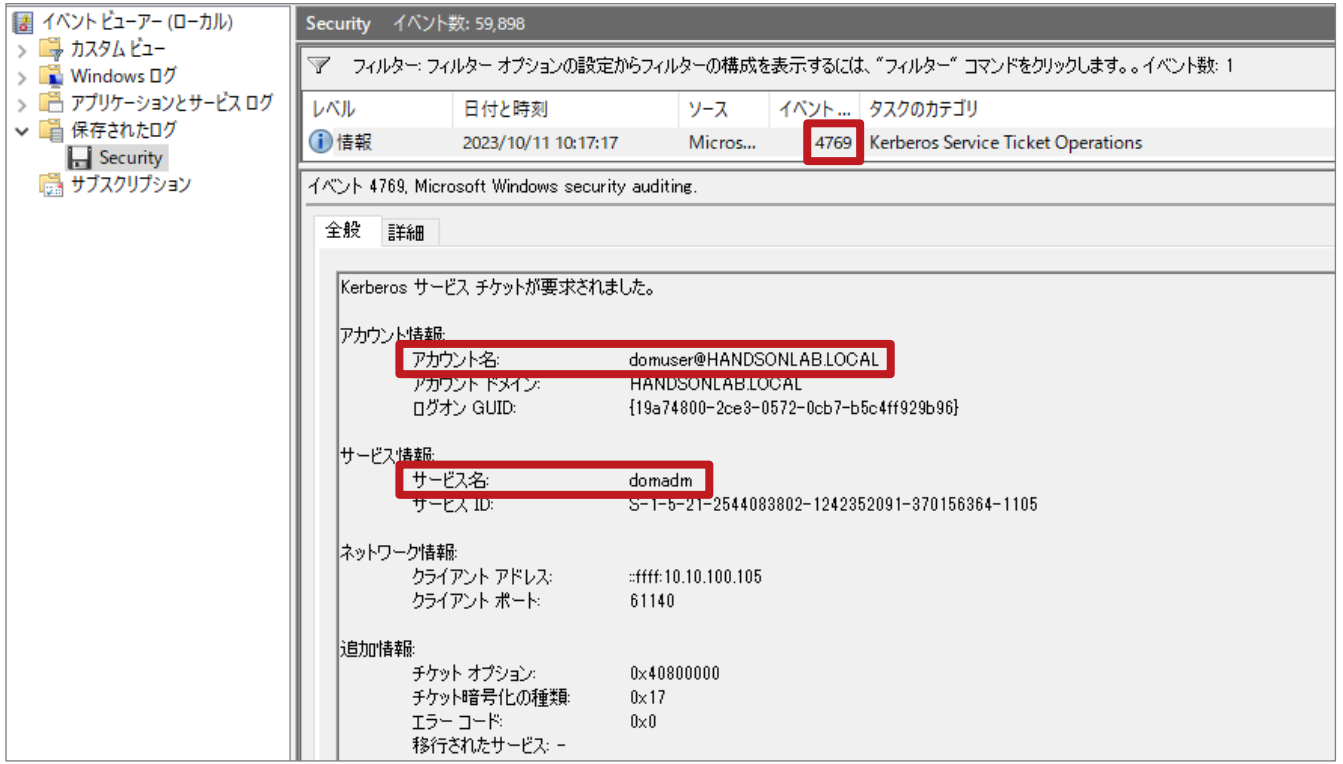
1. 10月12日8:44に10.10.100.254（VPN）からdomadmでログイン

```
<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

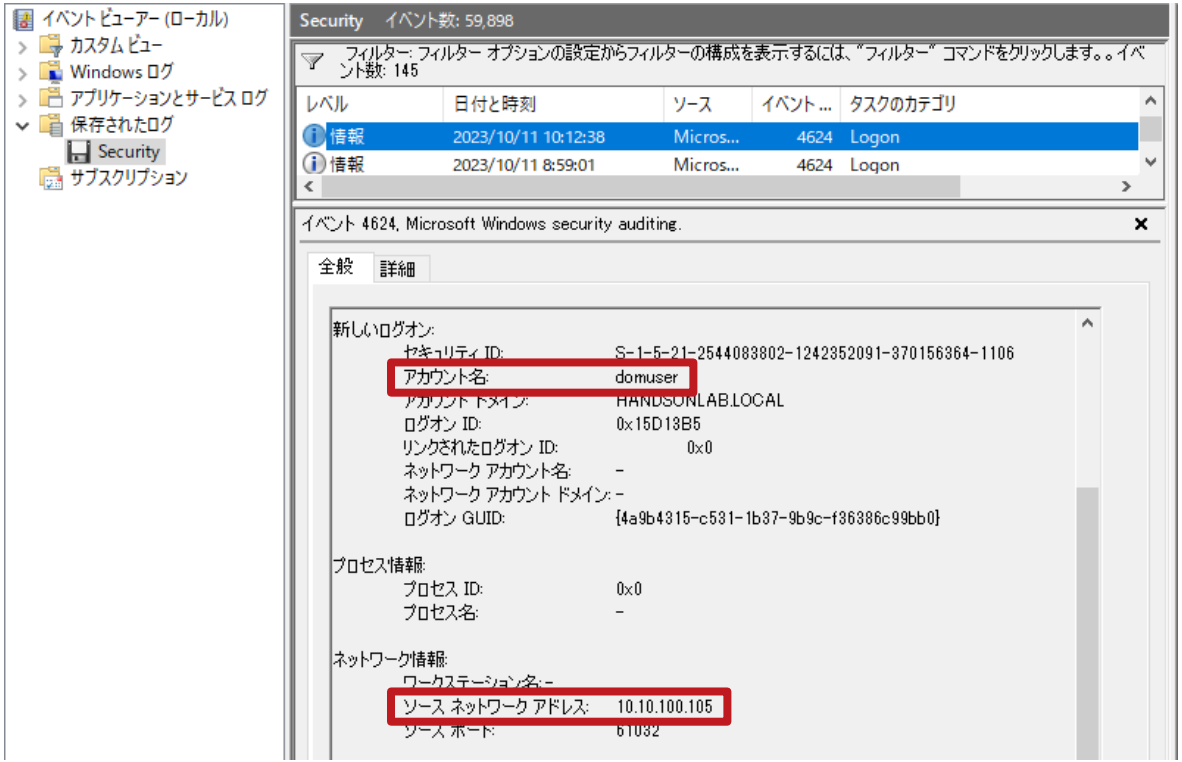
回答 2. 10月11日10:17にdomuserからdomadmへKerberoast

```
<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



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

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

ハンズオン２

演習

回答

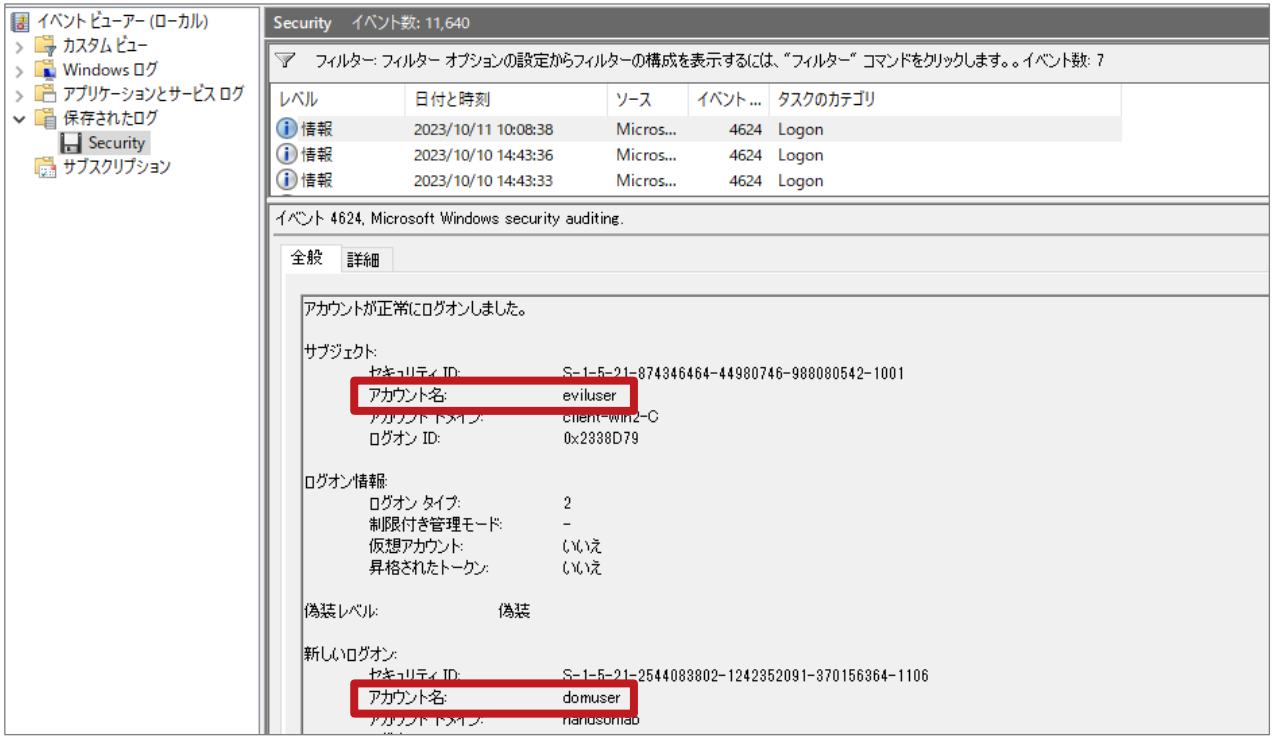
1. 10月11日10:08にeviluserがdomuserへログイン
2. 10月11日9:47にeviluserでRDP接続
3. 10月11日9:46にitmanagerがeviluserを作成
4. 10月11日9:44に10.10.100.104から10.10.100.105のitmanagerへPass-the-Hash

➡**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

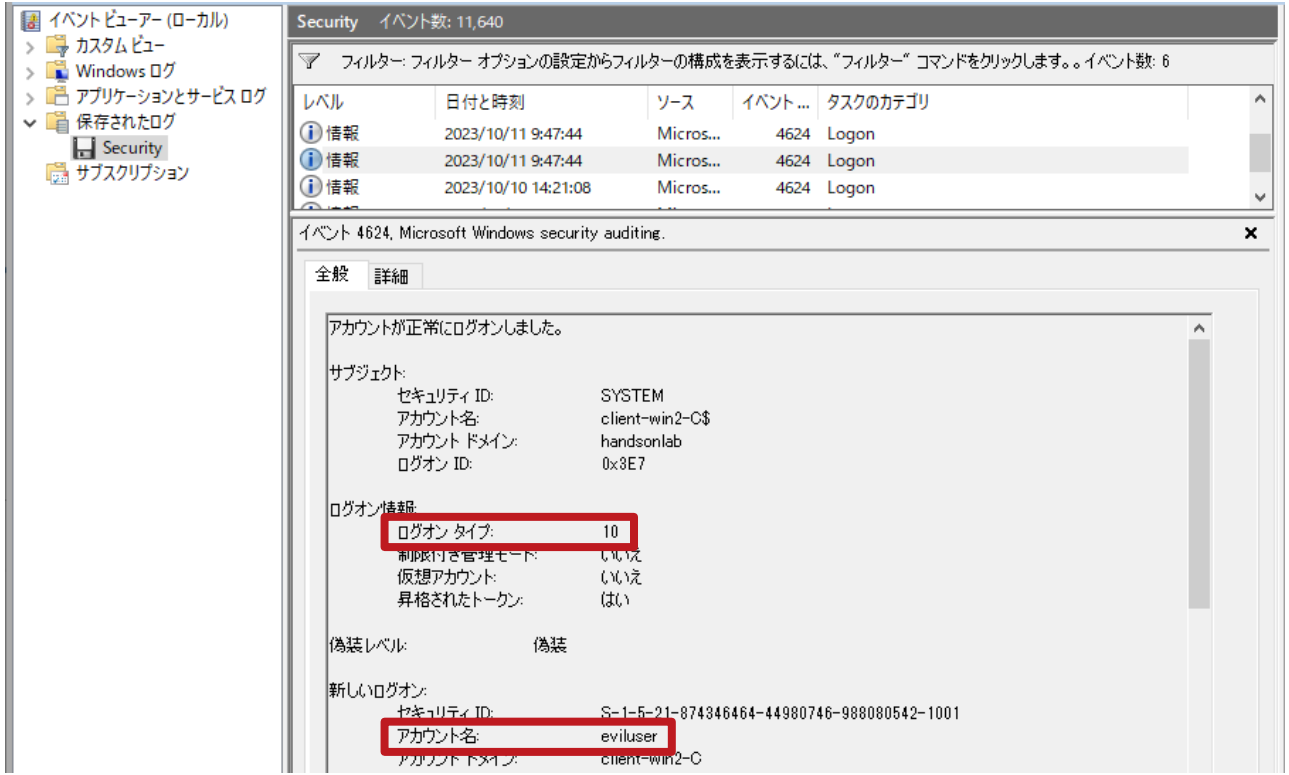
回答 1. 10月11日10:08にeviluserがdomuserへログイン



ハンズオン２

演習

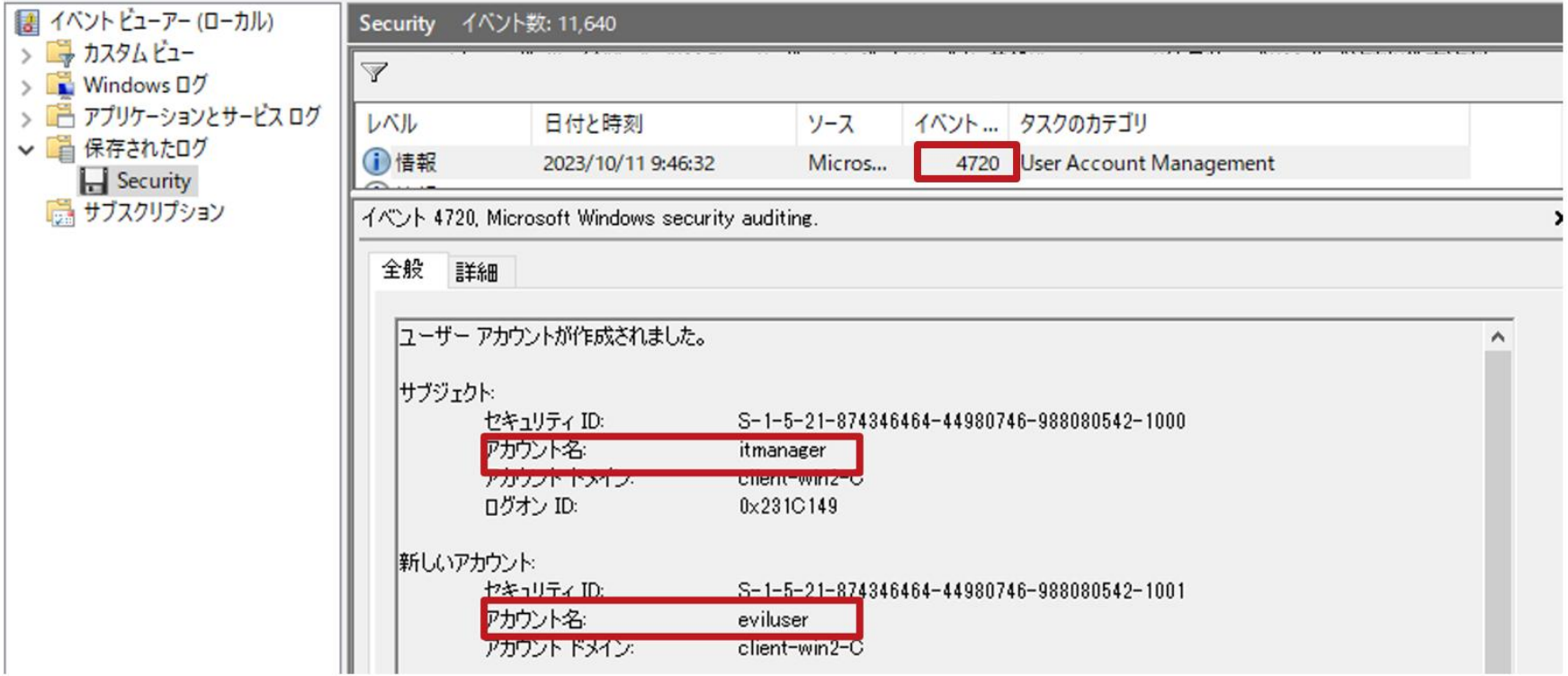
回答 2. 10月11日9:47にeviluserでRDP接続



ハンズオン２

演習

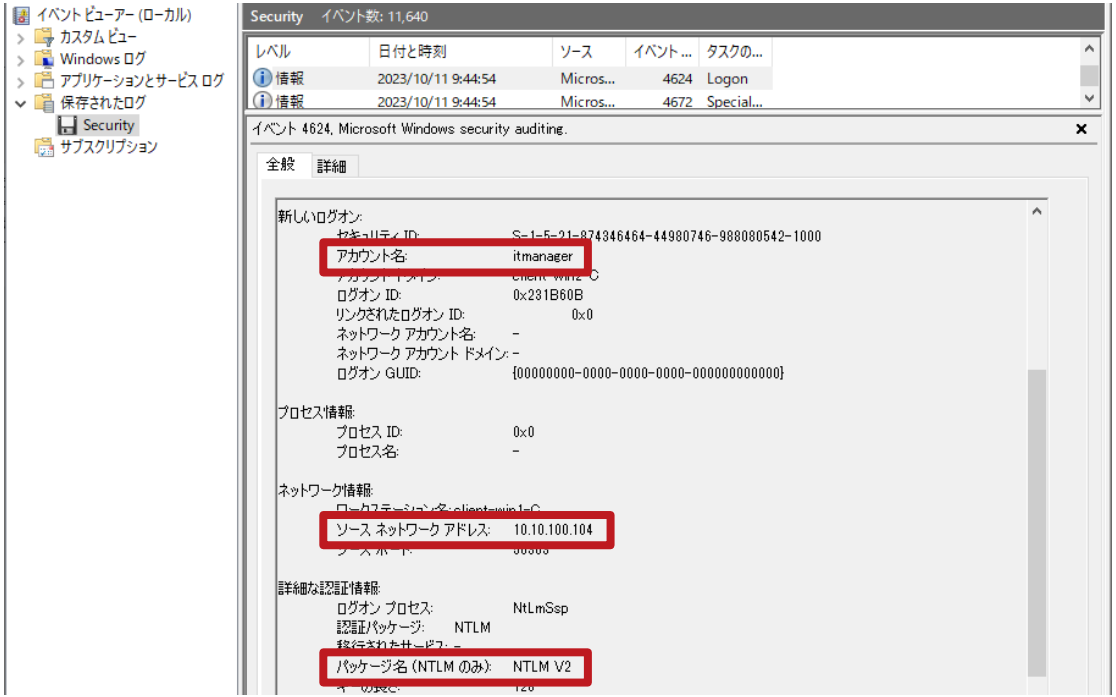
回答 3. 10月11日9:46にitmanagerがeviluserを作成



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



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

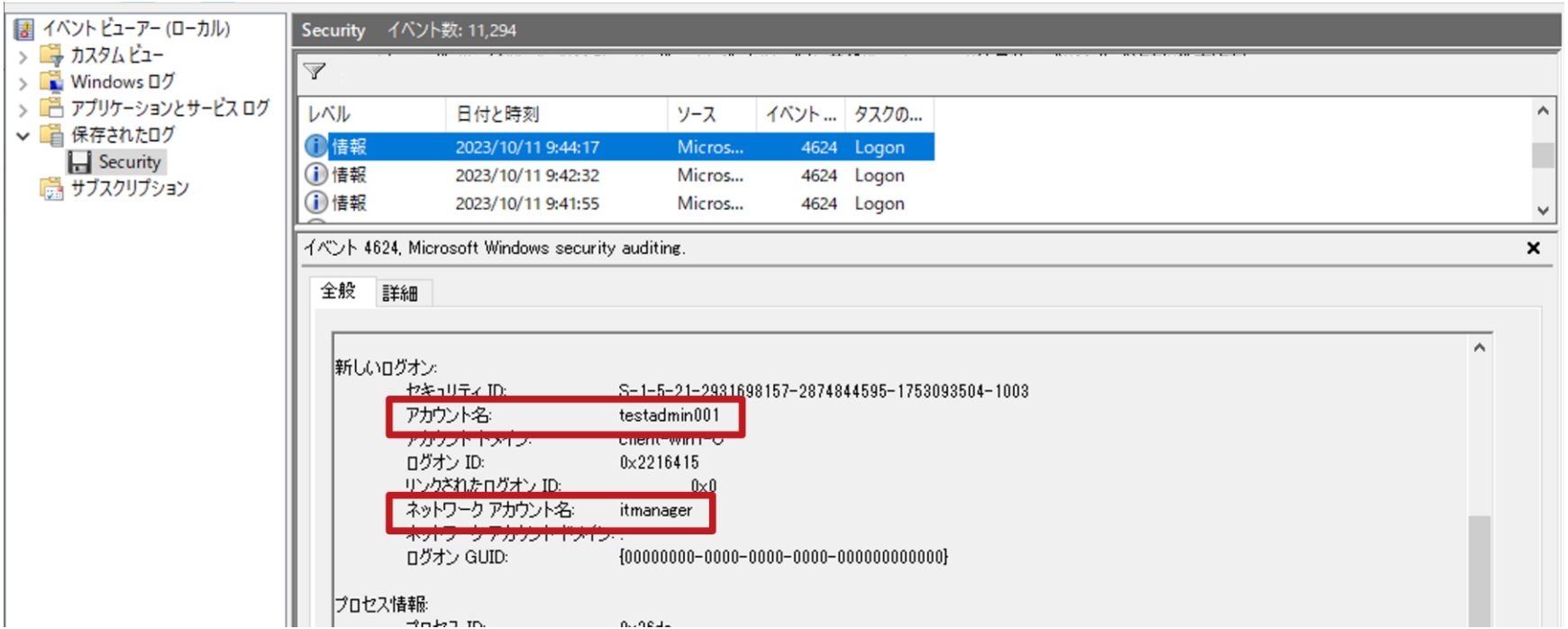
   ➡**ローカル管理者アカウントへのログインが発生**

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



ハンズオン３

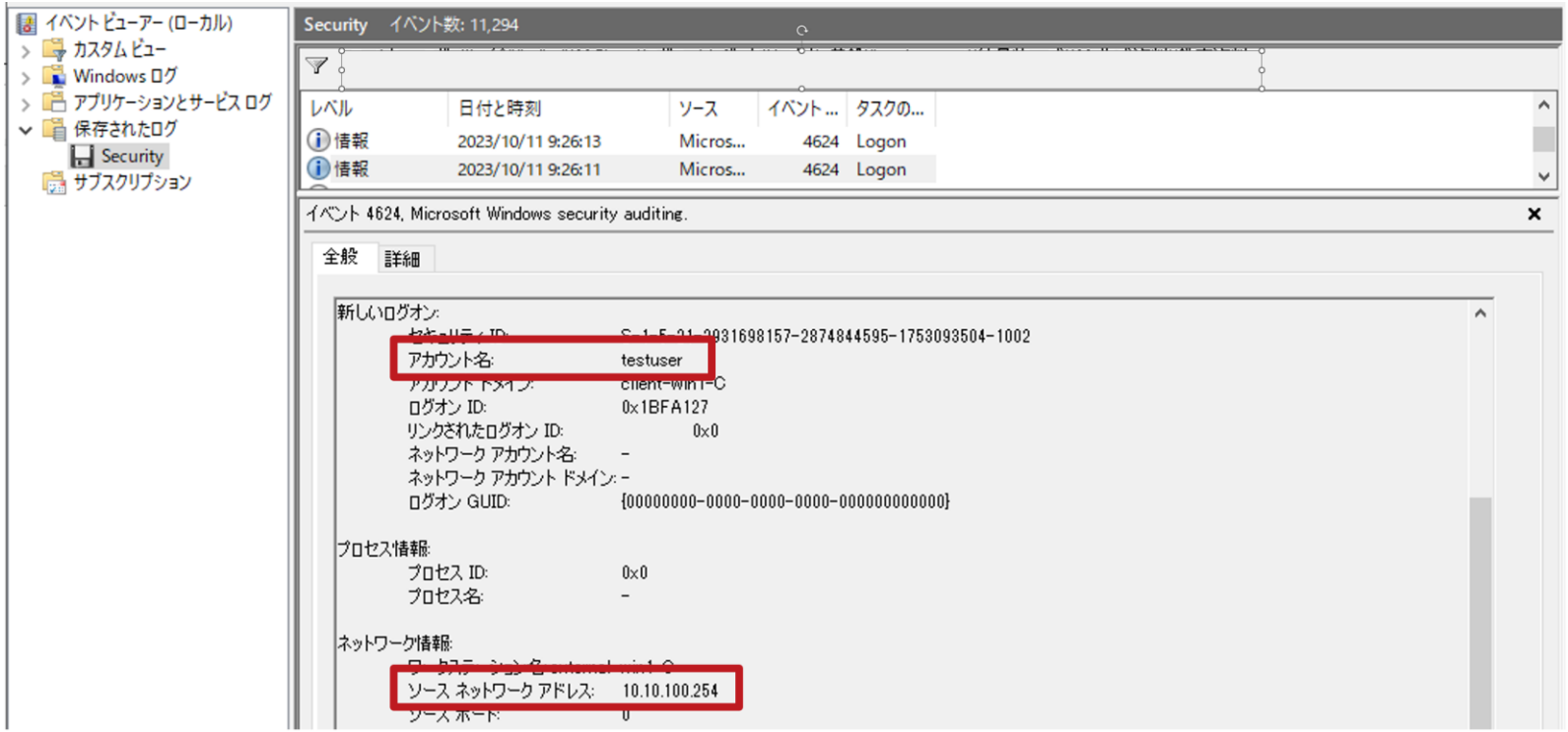
演習

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

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

```
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/UEsDBBQAAAAAAGa_S1cAAAAAAAAAAAAAAAAaAAAAbnRkcy5kaXQvQWN0aXZlIERpcmVjdG9yeS9Q - 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/SwMEFAAAAAgAaL9LVzHK8HIZnhsAAACAASIAAABudGRzLmRpdC9BY3RpdmUgRGlyZWN0b3J5L250 - 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/ZHMuZGl07J0LjBvHece_5ft175Nk2dYjkNM4ah3f-2EZqXkkz6LFO9JH3tmCDSvUHSWdTR0vd1Qd - 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/JQVE6fS0Lb8bt6mBNiiQqG3gtkZbo3DiR2GgthEjQNECrR23TeqiLRI0QRv0ESS6zuzucGaWy7tT - 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-f7fzM7OzLcrisOvG195_gdv_e6FnQEy8Xcb5uvK97_6T9E9W6KRL7waIgde5X2r - 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/afOXZNmeiDmPCzz0_vH3LEXs97-ctV67-Wanq_nPHN6W3esZfQBYtWmWz69ZzLyOv9HQB5xs-4Ox - 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/Fec1F7xwuPq3zfLWwFjPAAAAAAAAAAAAAAAAAAAAAAAgOTr-Pz_Zw4-_9fB5_8AAAAAAAAAAAA - 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_z7MvGPTg5QcvjzuO8w9fX9tB1M7eeS8RbVeOv5-f5QMAAAAAAAAAAAAAAAAAAAAA - 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-swXRn5818pdK1tv1vP45_xf2kH0KfLRrkuNX8X28c327fY77-W_81rvgpetLAAAAAAA - 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/AAAAAFxdInQtS-3m8z8AAAAAAAAAAA-ekToBu35_80X6fJLFF_9k079M36-d2kHMWsv7brU6Mf6 - 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_240mAAAAAAAAAAAAAuIrYz_-3ta9nCAAAAAAAAAAAAgA8t6vP_P8__2rFfffXwp78V0z__ - 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://10.10.1.4/52v8F7cT9Rsd5L9k_Z69YSe_aTHF3rbQiRpR6ETNw16NzS3kPPRUq_OQp62r4dAj3c5D3vCmhkNn - 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-TxbGg6d6HPWy_eTfc5D_l_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_I99ib3T6qXW6jRKVcPb6YXcodXqiMJ3OWO4_twi9d-Ju5iFB-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_TReLh5e1oVBKQw2E7ZQjhW4nF3KVGaLZUfJJ4O1HbaDk2wbZmmVLLiDmp_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://10.10.1.4/2emEyCw1RFOVSpVXWdeekgWeIt7RHQW2UKF0dLFcrJYKxYPO2oZlWbymXpK_dFEvOEZTpdnK0lz2 - 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://10.10.1.4/0KHlUlXXr8jCV8jlbGOULB0qHitXZ4rlY46yT0vtaTdtmPaVjo-X59JJR2udkcIz7sKZ4lK-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-uSC3Pz1fnKQrHMeuexowuOoiOyvXhDi-4hPNi9MpOYKC66dK6oVEfZtoNcWjvI - 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/z3qisuxo6HOy6ufcqh6lwrHFcikzf3Te2bnOS-l5N2mQZkpLy-ycddkFKbvgJgtQvrJUTSc1lUFS - 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-WDxdkHksVqUdcaUmu4abultrRYWpgrLczOl_STNTzSh8fNB5sySovFJTYaMjO6 - 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://10.10.1.4/0iuV3iZKPtnsnV9wNLDhk0qfe71NJRsJpaWl0lxmxsWHX_rwu5duTTaTxaOOYRSTnSpGzbvkTOLI - 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/sYUHJoqfs9RsFjfM11BtpznsDXN7DUs5S_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-a1zDjBkh5mB-TpmAhNoj1fwcxASkqX1UOL7o0HmlztusVA-l53RVjbeypWJ79blSqGo-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/ND5ZkiiloaQmsUy48EsXVxDLhDog1RuLZUIYlMIri2XCwUnZXOvHMiEKyVI3HMuE9pQscOOxTIjD - 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/suAcimVCvvIL33AsF9nTUpvaTdsOv4TwiBRuLJY14VkpvMJYJixEZHtdOSwT6qbUR2lisUxIz8mq - 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** 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

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
- **10月11日09:47** evilユーザでRDP接続　ハンズオン２
- **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