**別紙.TIPS-2　実習資料**

仙台 CTF　2019　セキュリティ技術勉強会　実習

# TIPS-2　イベントログ解析

2019年9月28日

仙台 CTF 推進プロジェクト

# 目次

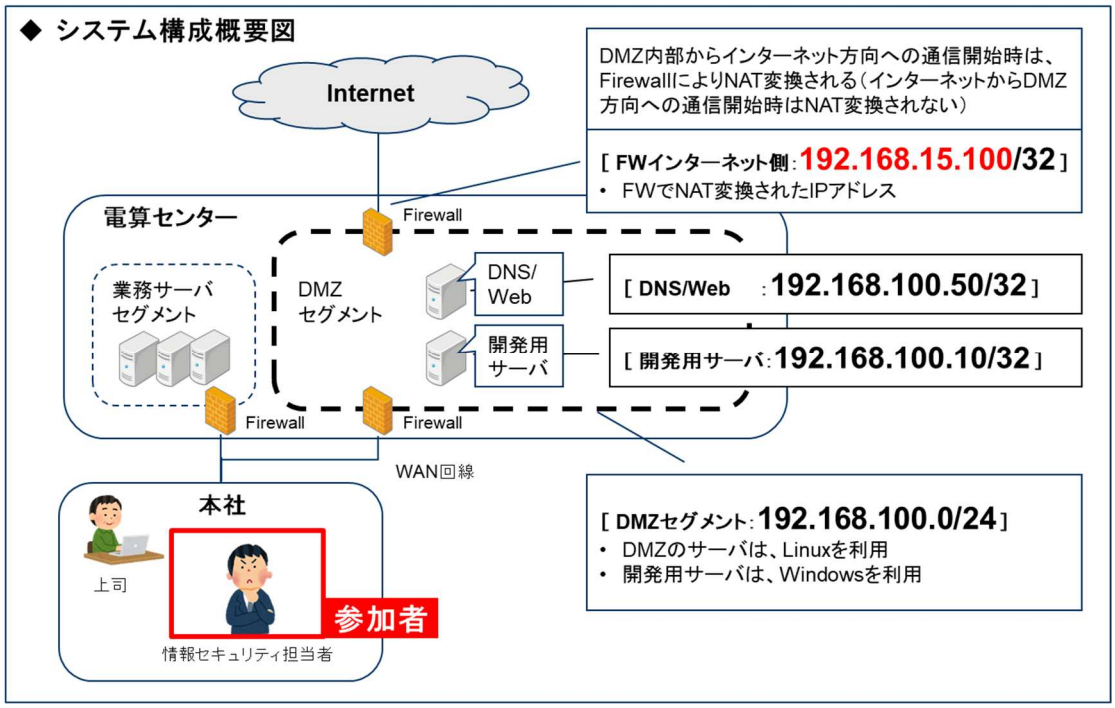
本実習の概要

あなたは、架空の企業「株式会社仙台シーテーエフ」に入社したばかりの新米情報セキュリティ担当者です。

とある休日の夜、あなたが自宅で SNS を閲覧していたところ、「うちのサーバが 192.168.15.100 から大量の RDP アクセス受けてる。仙台シーテーエフの IP みたいだけど乗っ取られているのか？とりあえずファイアウォールで遮断しておこう。」と投稿されていることを発見しました。

DMZ のネットワークを流れる通信の記録を調査した結果、開発用サーバが外部に攻撃していることがわかりました。また、事業部門の担当者に確認したところ、RDP 接続を有効にしており、Administrator パスワードは推測可能なものを設定していたことが分かりました。

開発用サーバのイベントログを調査し、攻撃内容を推測してください。




[補足情報]

- 実習データの都合上、8 月 17 日からのイベントログが記録されています。
- 攻撃を受けたのは、8 月 25 日です。
- 「evtxecmd」で抽出したログの時刻が UTC 時間になっています。9 時間加算した時間に読み替えてください。

# 実習1　イベントログ解析

実習内容

開発用サーバ(Windows サーバ)のイベントログを調査し、いつ・どこから・どのように攻撃されたかを推測してください。

① 不正ログオン試行攻撃元 IP アドレス

② 不正ログオン試行の失敗数と成功数(試行後の別 IP アドレスからの接続を除く)

③ 遠隔操作されたと思われる攻撃元 IP アドレス

④ 遠隔操作(ログオン)していた時間帯

[実習用データ]

実習用仮想マシンに格納してあります。

フォルダ　: /var/samba/public/tips2

ターミナルを開き、次のコマンドを実行してください。csv ファイルの名前(tips2)は任意の名前にしていただいて構いません。現在のディレクトリに、csv ファイルが作成されます。

```
cd /var/samba/public/tips2
evtxecmd -d ./ --csv ./ --csvf tips2.csv
```

本コマンドで作成した「csv 形式」ファイルを、LibreOffice でファイルを開いて下さい。

また、evtxecmd で作成したデータは時系列になっていません。「TimeCreated」列をキーに並び替えてください。

回答記入欄

①不正ログオン試行攻撃元 IP アドレス:

②不正ログオン試行回数　失敗数:　　回　　成功数:　　回

③遠隔操作されたと思われる攻撃元 IP アドレス:

④遠隔操作(ログオン)していた時間帯:　　時　　分 ～　　時　　分

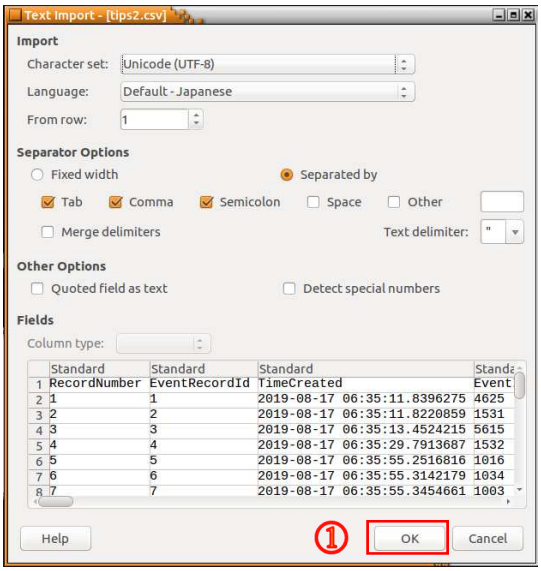
## 実習2の解説

LibreOffice で調査した場合の例を解説します。また、CSV のデータと比較しやすいように UTC 時刻で解説します。

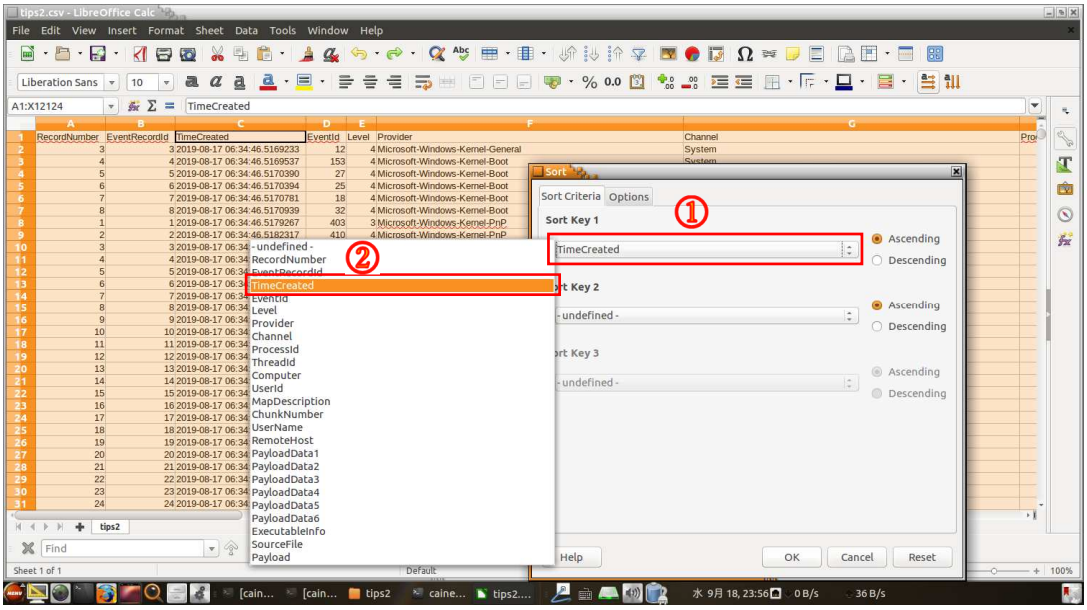
1. 「evtxecmd」で作成した csv 形式ファイルを LibreOffice で開きます。

```
caine@caine:/var/samba/public/tips2$ libreoffice tips2.csv
```

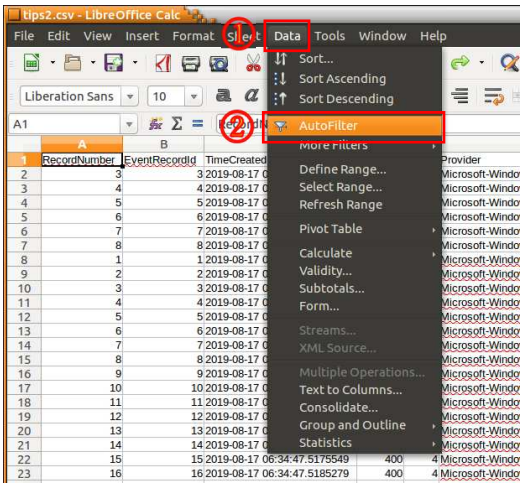
2. 「Text import」ウインドウが表示されますので「OK」ボタンを押してください。



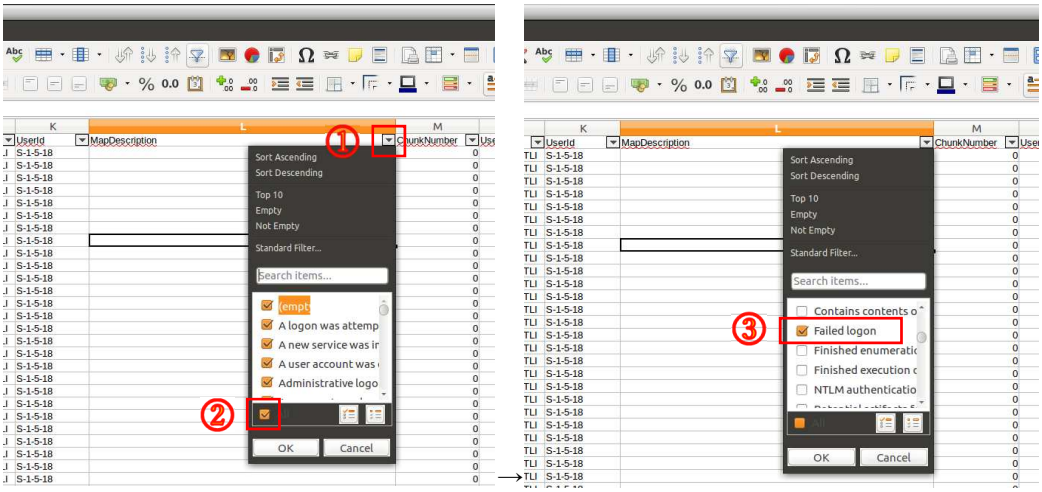

3. メニューバーから「Data」→「Sort」を選択してください。Sort Key 1 の値に「TimeCreated」を選択し、「OK」ボタンを押してください。



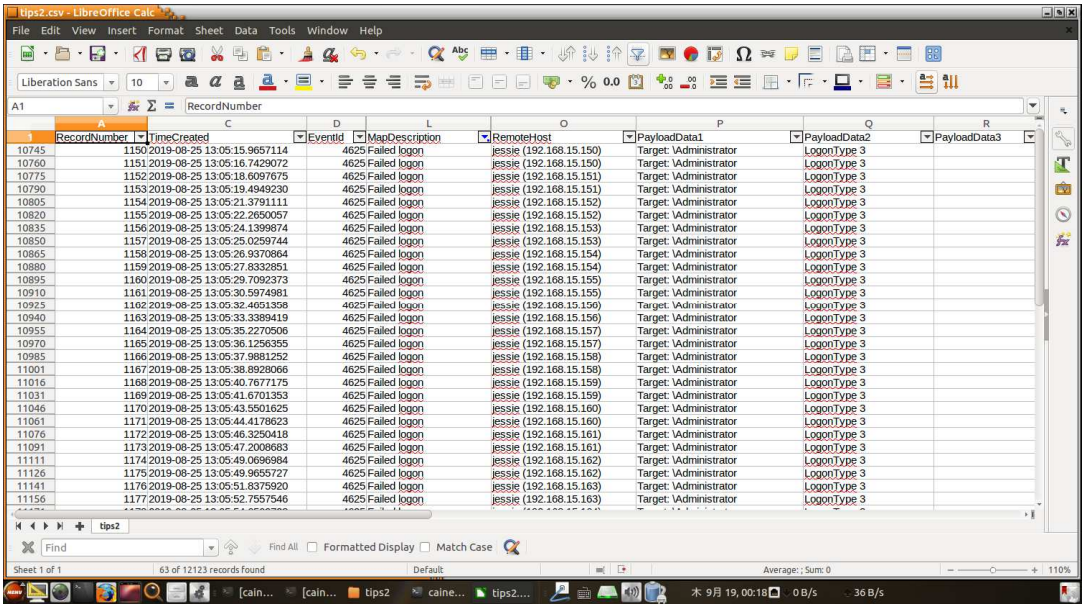
4. メニューバーから「Data」→「AutoFilter」を適用してください。




5. MapDescription 列のフィルタでログオン失敗を示す「Failed logon」を指定します。MapDescription 列の▼ボタンを押してください。一番下の「All」のチェックを外します。「Failed logon」にチェックをつけてください。「OK」ボタンを押してください。

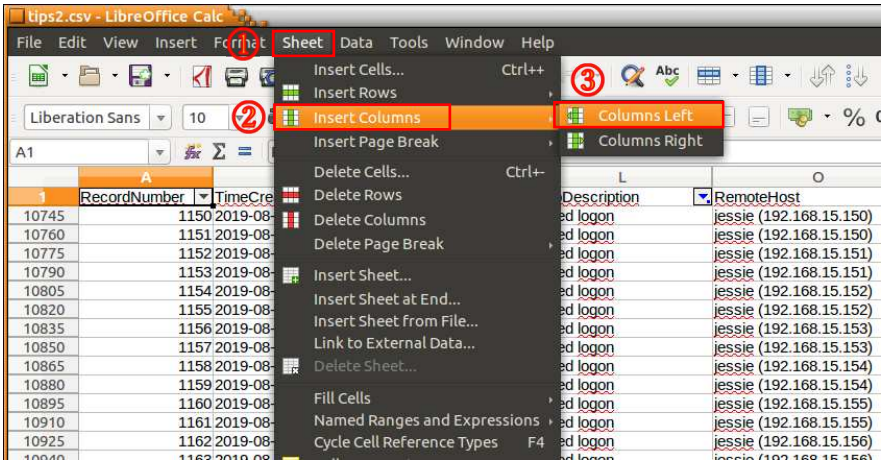


6. 「8/25 13:05:15」以降、「2019/8/25 13:06:39」まで、連続してログオン失敗していることがわかります。

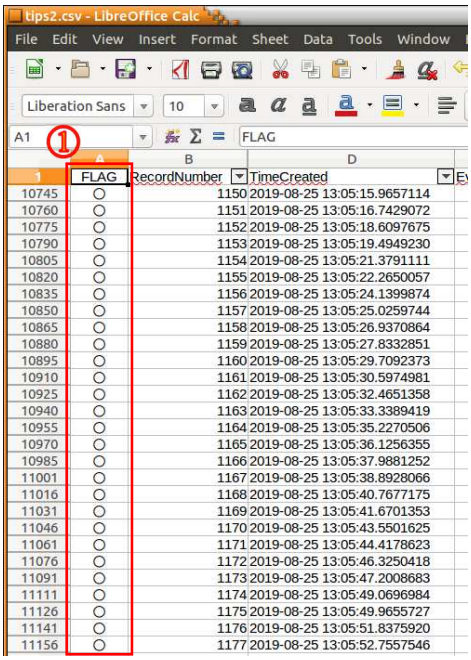



※上図では、不要な列を非表示に設定した画面です。以降も同様です。

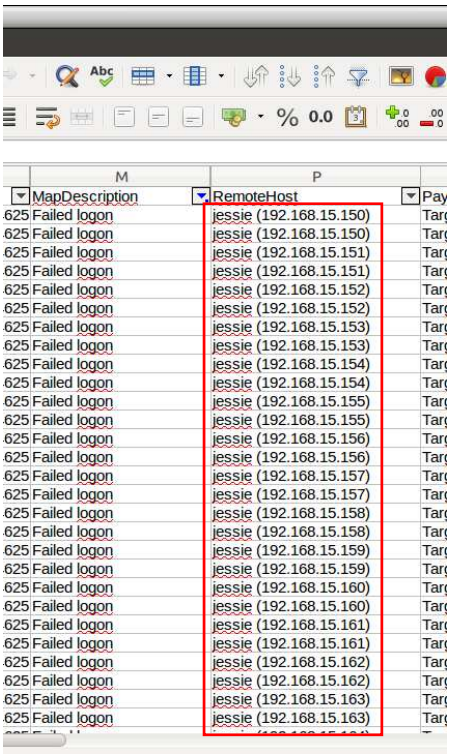
7. 一番左に列を追加してください。A1 セルを選択した後に、メニューバーから「Sheet」→「Insert Columns」→「Columns Left」を選択してください。



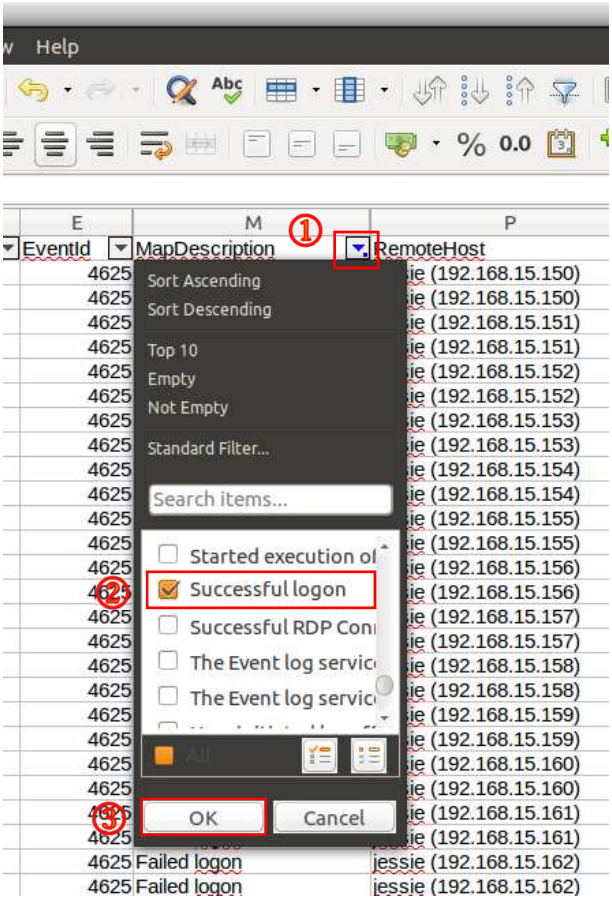
8. 一列目に「FLAG」と入力してください。フィルタで抽出した行の FLAG 列にに「○」を入力してください。これは重要な箇所に目印を付け、フィルタを解除した後でも検索がしやすいようにするための TIPS です。また、行の背景色を変えていただいても構いません。



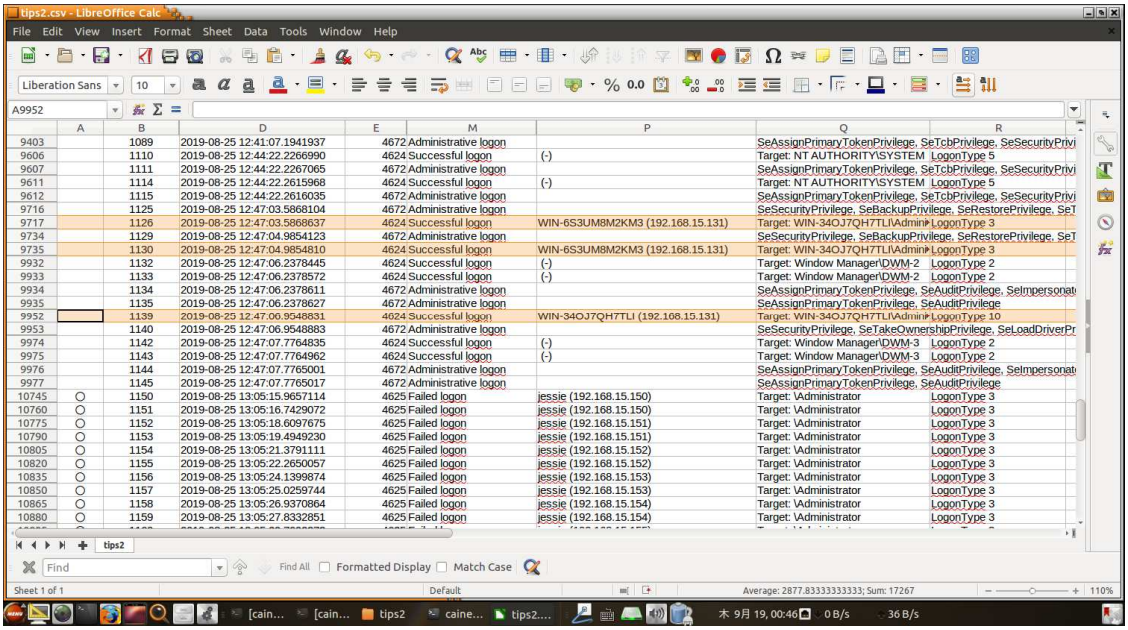

9. 「RemoteHost」列を見ると、ログオン試行を行った攻撃元の IP アドレスが 192.168.15.150～192.168.15.180 であることがわかります。



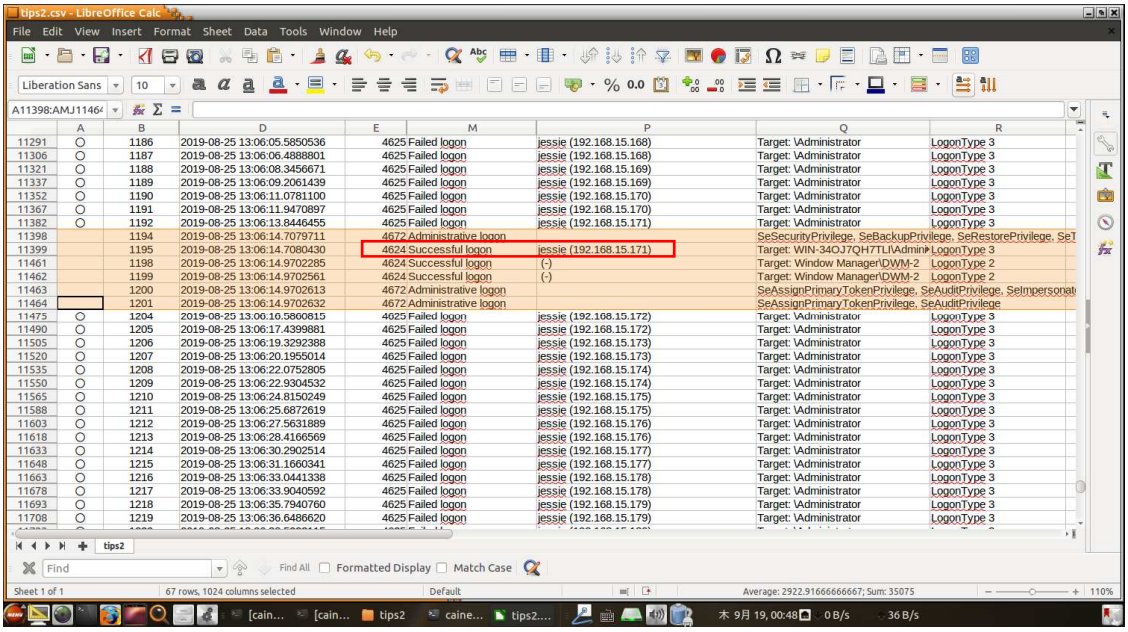
10. MapDescription 列のフィルタでログオン成功を示す「Successful logon」と管理者特権でログオンしたことを示す「Administrative logon」のチェックを追加（「Failed logon」のチェックは残したまま）します。MapDescription 列の▼ボタンを押してください。「Successful logon」と「Administrative logon」にチェックを追加してください。



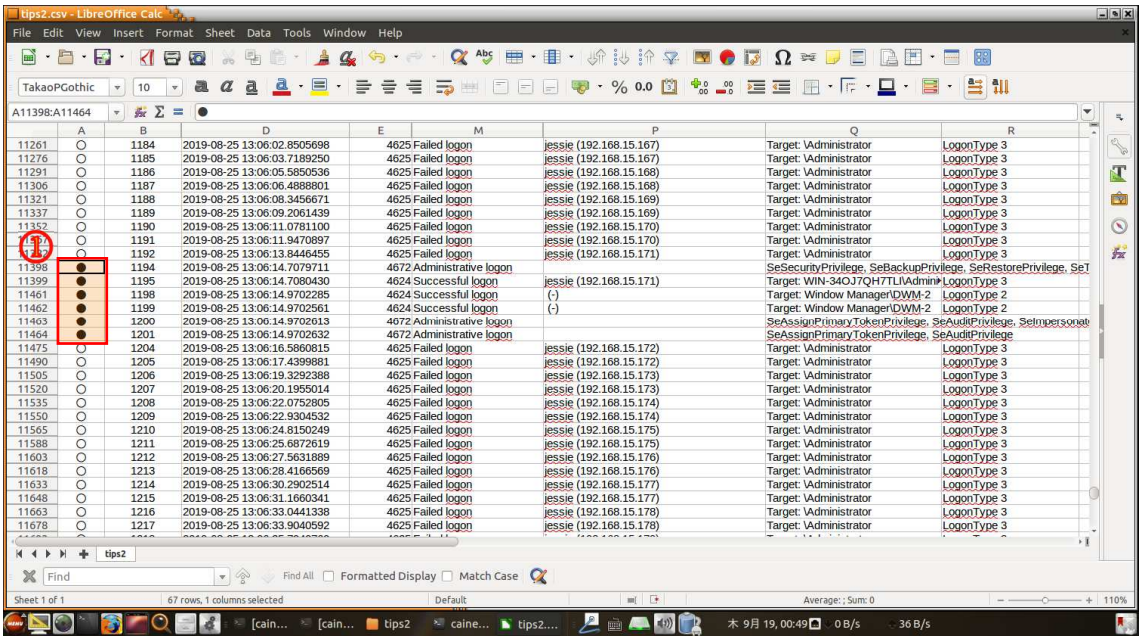
11. RecordNumber「1126」行、「8/25 12:47」付近の「RemoteHost」列を見るとIPアドレス「192.168.15.131」からログオンが成功しています。これは事業部への聞き取り調査の結果（22時前頃に接続）と一致します。



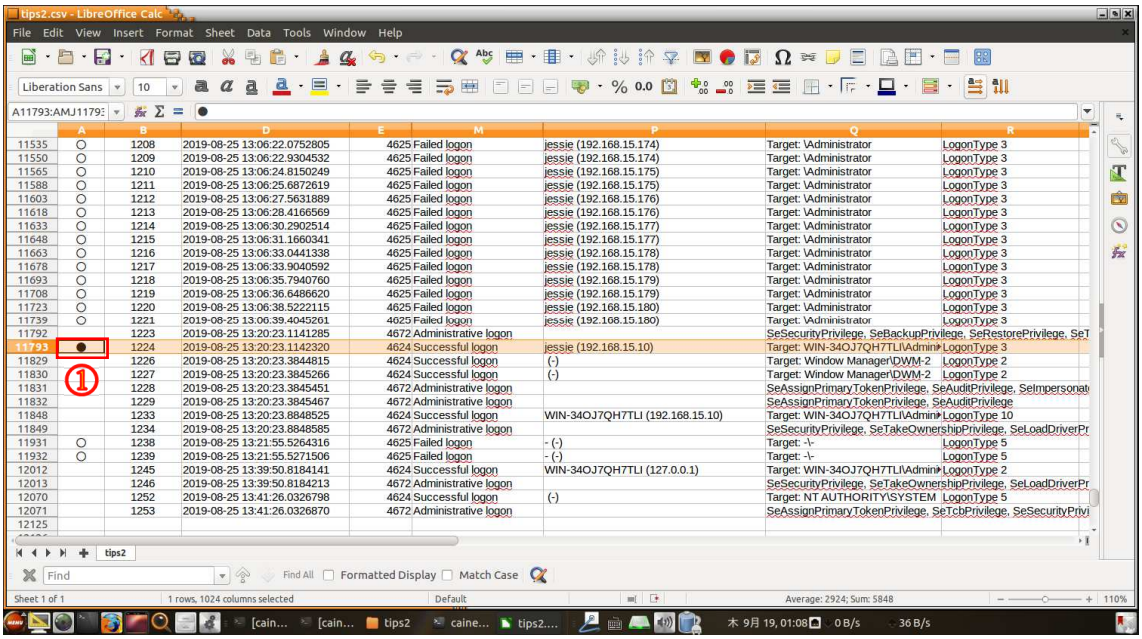

12. それ以降のログを見ていくと、RecordNumber「1195」行で（13:06 頃）、IPアドレス「192.168.15.171」からのログオンが成功しています。その前後の異なるIPアドレスからのログオンが失敗していることから、複数のパソコン（ボットと考えられる）からログオン試行を実施し、「192.168.15.171」からの試行時にログインに成功したと推測できます。



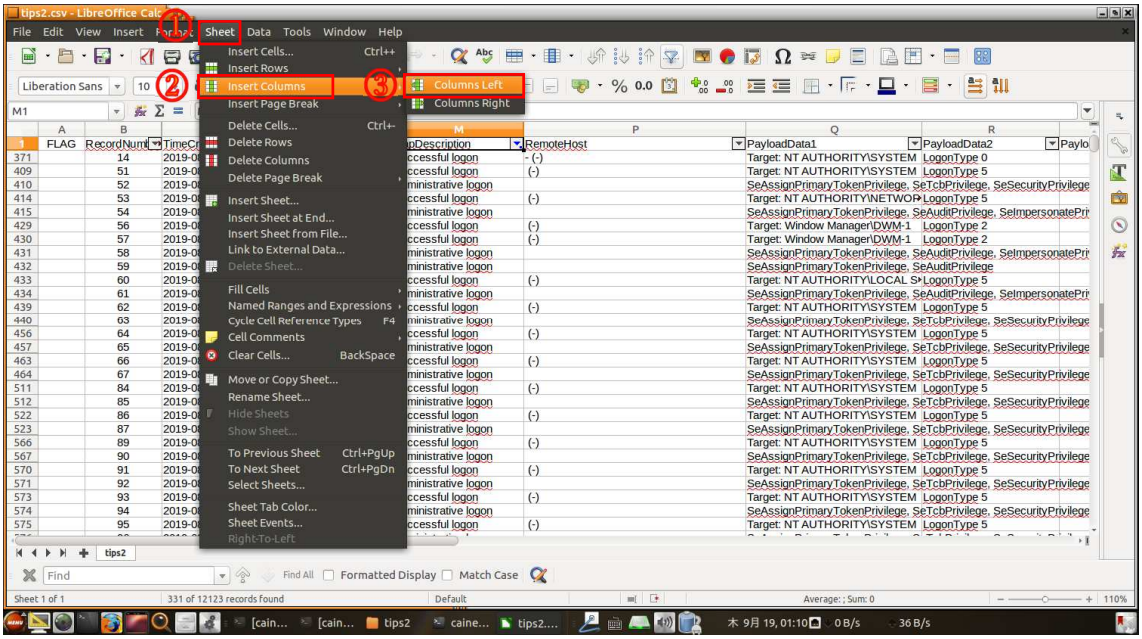
14. この行の FLAG 列に「●」を入力してください。



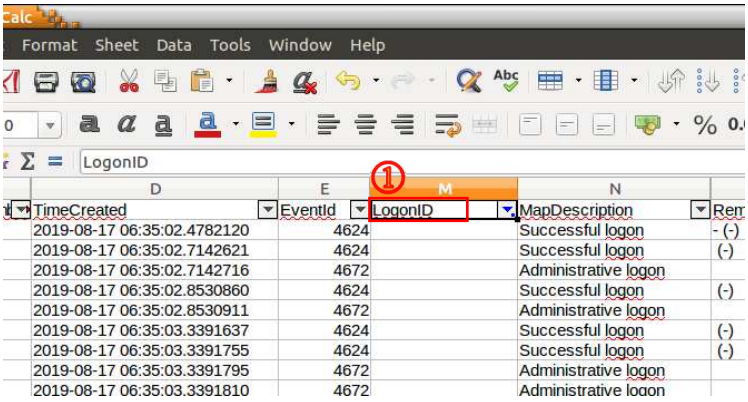

15. さらにそれ以降のログを見ていくと、RecordNumber「1224」行で（13:20 頃）、IP アドレス「192.168.15.10」からのログオンが成功しています。これは、ログオン試行で入手したパスワードを利用して攻撃者が RDP で接続したと考えられます。この行の FLAG 列に「●」を入力してください。



16. MapDescription 列の右側に列を追加します。M1 セルを選択した後に、メニューバーから「Sheet」→「Insert Columns」→「Columns Left」を選択してください。

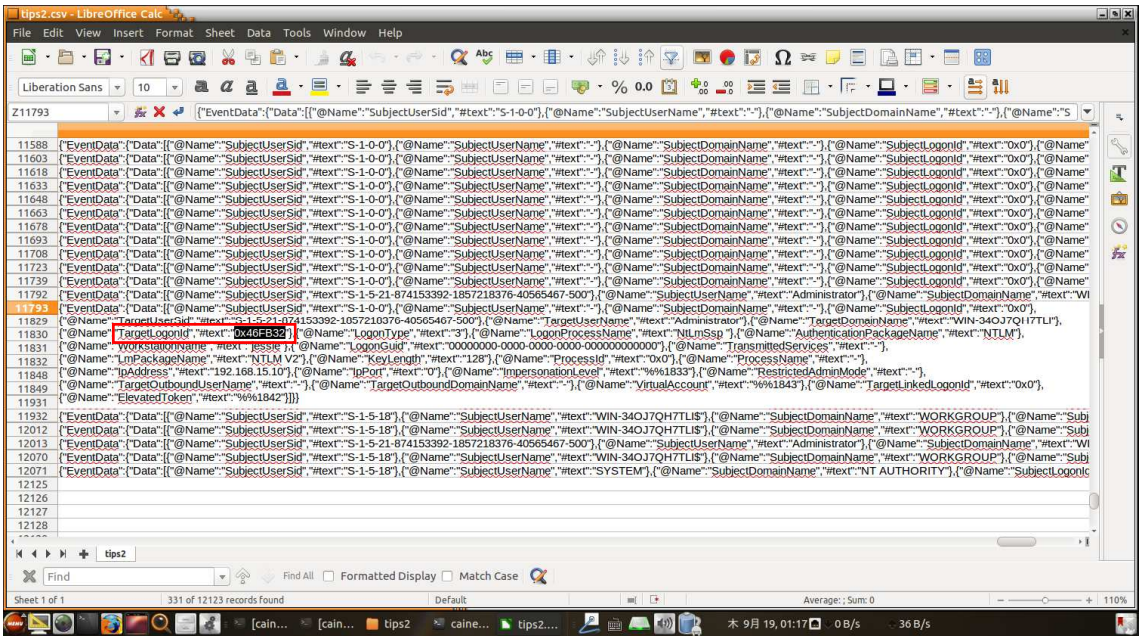


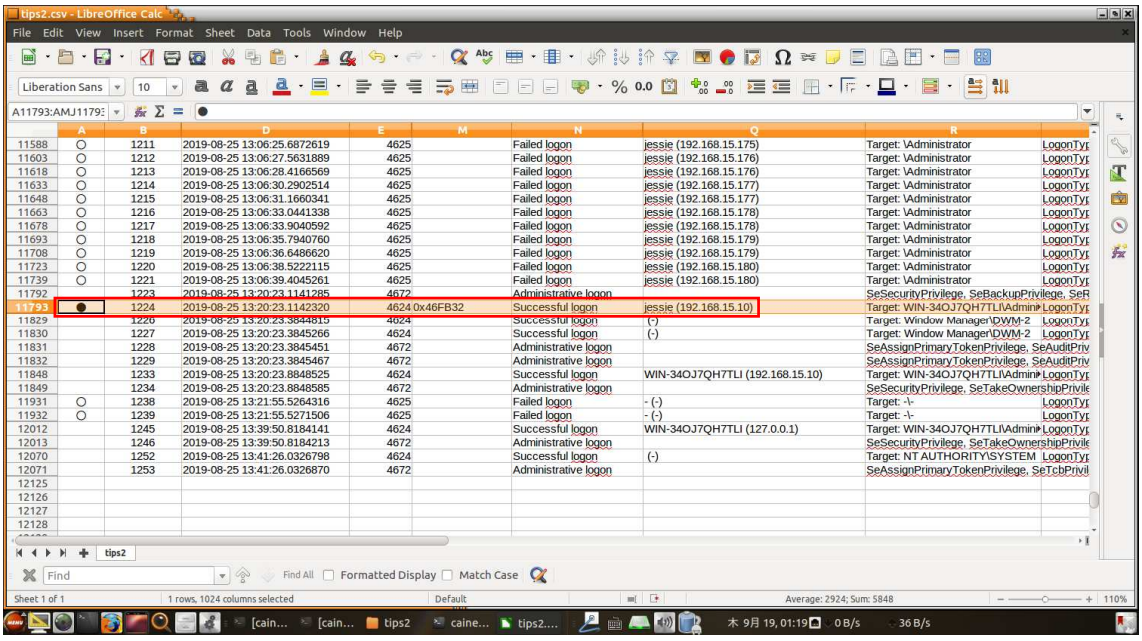

17. 一列目に「LogonID」と入力してください。




| | D | E | M | N | |
|---|---|---|---|---|---|
| | TimeCreated | EventId | LogonID | MapDescription | Rem |
| | 2019-08-17 06:35:02.4782120 | 4624 | | Successful logon | - (-) |
| | 2019-08-17 06:35:02.7142621 | 4624 | | Successful logon | (-) |
| | 2019-08-17 06:35:02.7142716 | 4672 | | Administrative logon | |
| | 2019-08-17 06:35:02.8530860 | 4624 | | Successful logon | (-) |
| | 2019-08-17 06:35:02.8530911 | 4672 | | Administrative logon | |
| | 2019-08-17 06:35:03.3391637 | 4624 | | Successful logon | (-) |
| | 2019-08-17 06:35:03.3391755 | 4624 | | Successful logon | (-) |
| | 2019-08-17 06:35:03.3391795 | 4672 | | Administrative logon | |
| | 2019-08-17 06:35:03.3391810 | 4672 | | Administrative logon | |

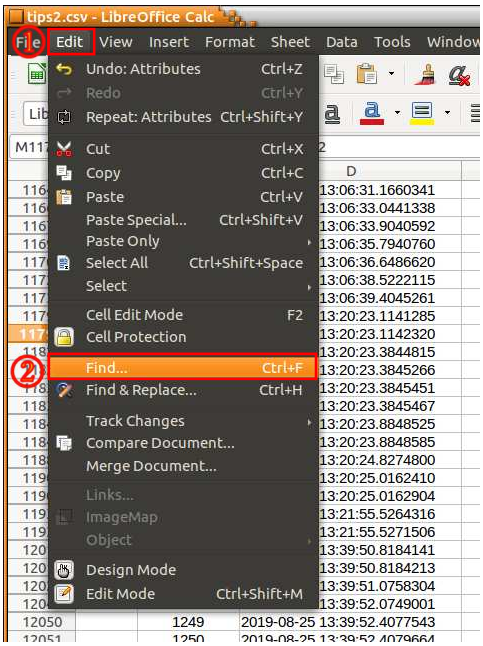
19. 攻撃者が RDP でログオンしたと思われる RecordNumber「1224」行の「Payload」列の値を参照し、「TargetLogonId」の値「0x46FB32」をコピーし、「LogonID」列に追加します。



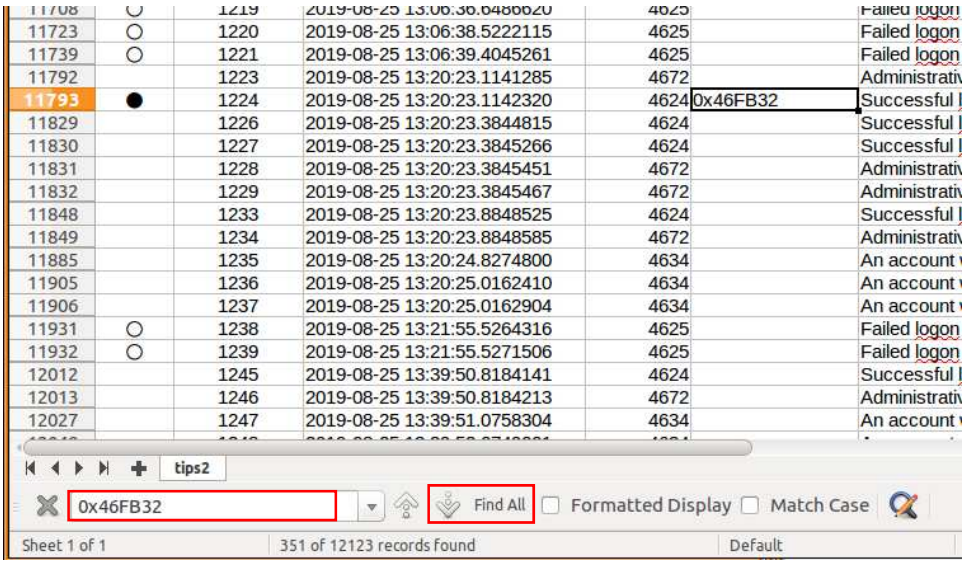



21. MapDescription 列のフィルタでログオフを示す「An account was logged off」と「User initiated logoff」のチェックを追加（これまで選択したチェックは残したまま）します。

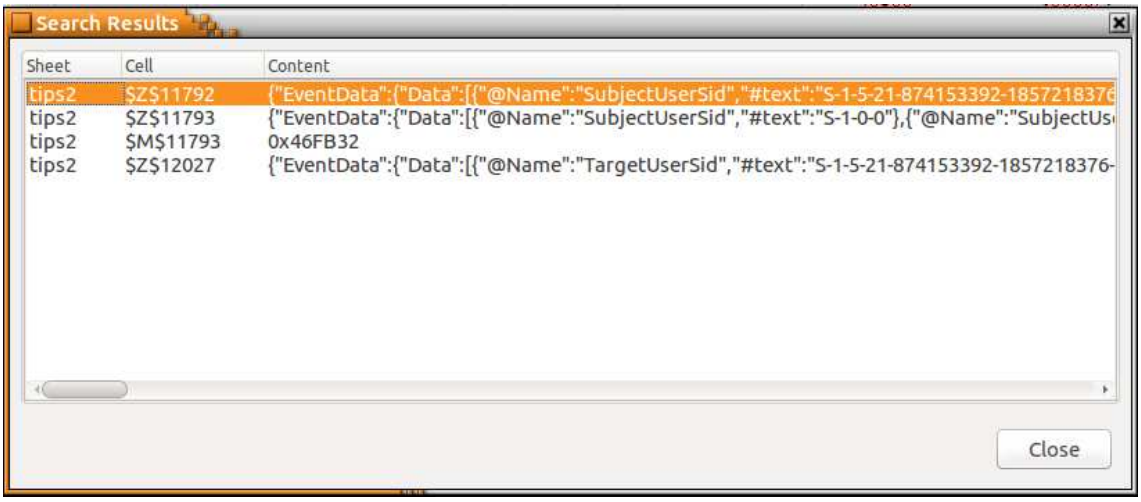
22. メニューバーから「Edit」→「Find」を選択します。



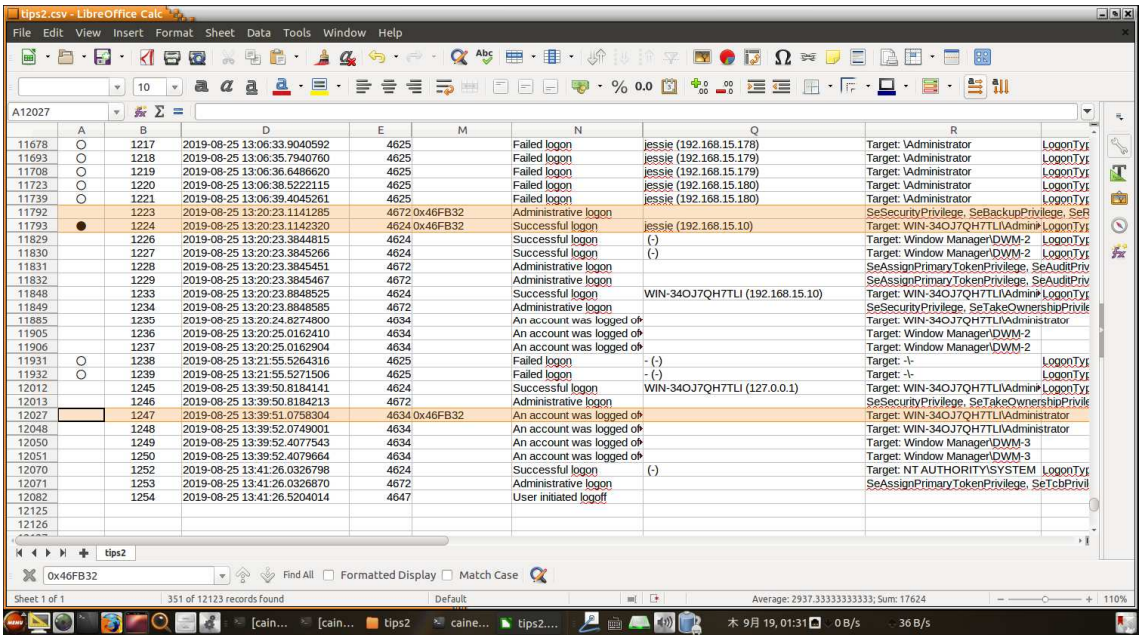

23. 画面下に検索キーワード入力フォームが表示されますので、検索文字列入力欄に TargetLogonId の値「0x46FB32」をコピーし、「Find All」ボタンを押します。



25. 別ウインドウが開き、その文字列が含まれるセルの場所が表示されます。該当する行（11792 行、11793 行、12027 行）の「LogonID」列に値「0x46FB32」をコピーします。




26. この結果から、RecordNumber「1224」行 UTC　13 時　20 分　23 秒にログオンしたユーザが、RecordNumber「1247」行 13 時　39 分　51 秒にログオフしたことがわかります。




以上で演習は終了です。お疲れさまでした。

回答例

①不正ログオン試行攻撃元 IP アドレス：192.168.15.150 ～ 192.168.15.180

②不正ログオン試行回数　失敗数：61 回　　成功数：1 回

③遠隔操作されたと思われる攻撃元 IP アドレス：192.168.15.10

④遠隔操作（ログオン）していた時間帯：UTC 13 時 20 分 23 秒 ～ 13 時 39 分 51 秒
JST 22 時 20 分 23 秒 ～ 22 時 39 分 51 秒