

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.....	1
実習1 イベントログ解析 .....	2
実習1の解説 .....	3

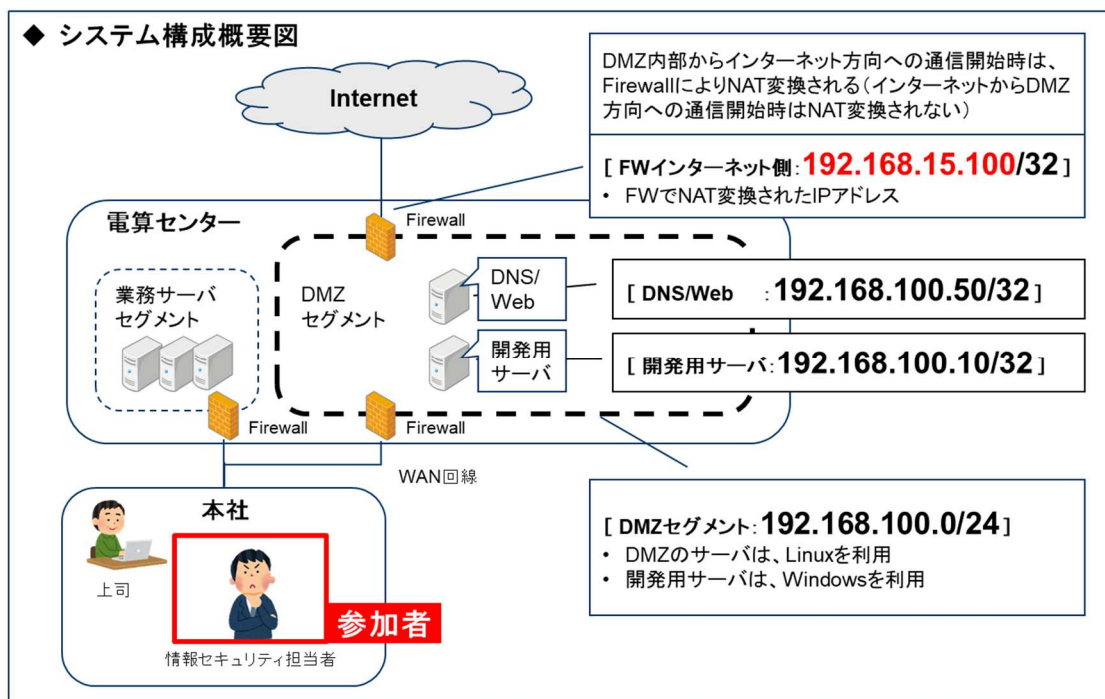
## 本実習の概要

あなたは、架空の企業「株式会社仙台シーTEE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TEEエフの IP みただけで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わかりました。

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

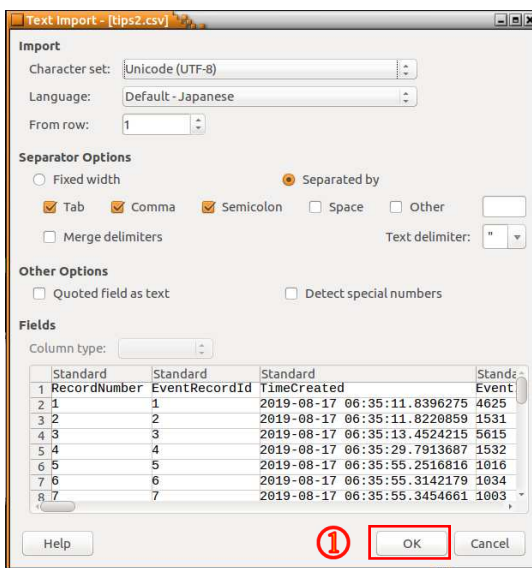
## 実習2の解説

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。

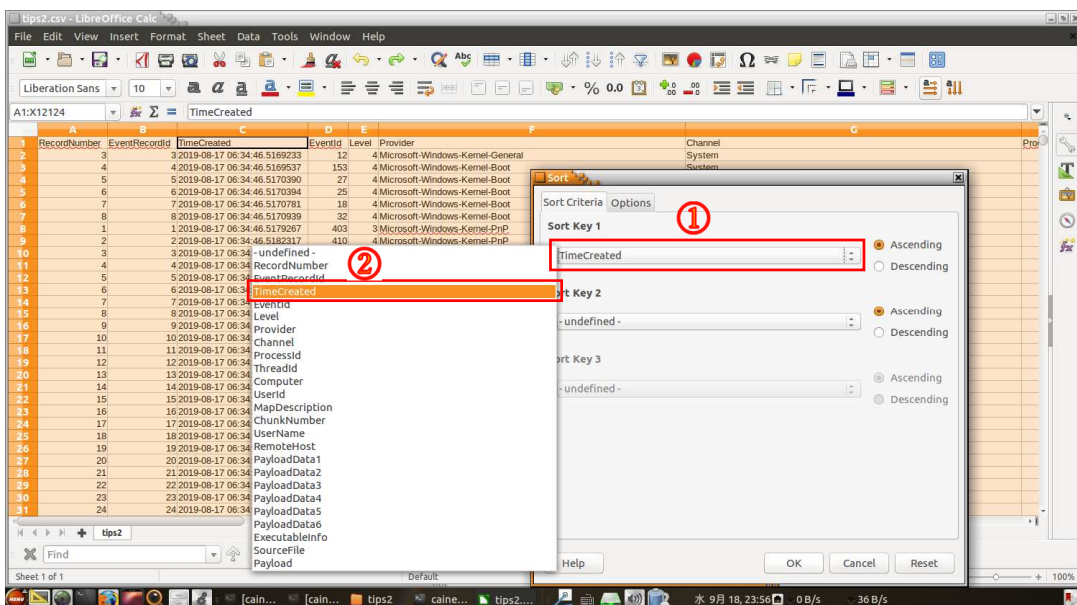
1. 「evtxecmd」で作成した csv 形式ファイルを LibreOffice で開きます。

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

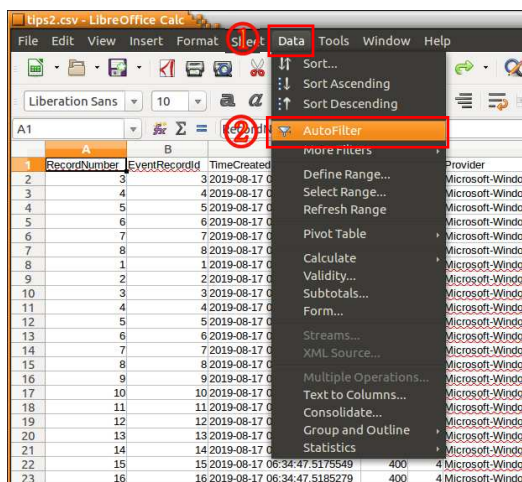
2. 「Text import」ウインドウが表示されますので「OK」ボタンを押してください。



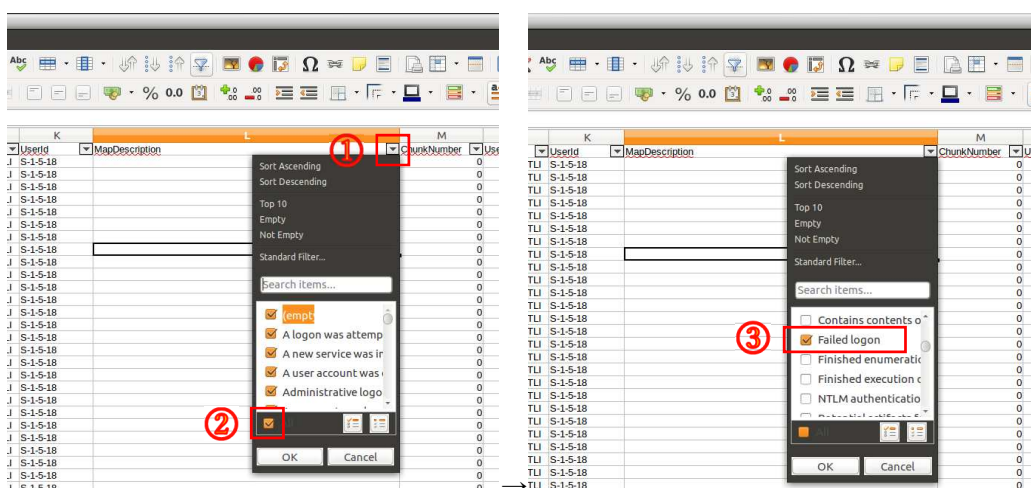
3. メニューバーから「Data」→「Sort」を選択してください。Sort Key 1 の値に「TimeCreated」を選択し、「OK」ボタンを押してください。



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。

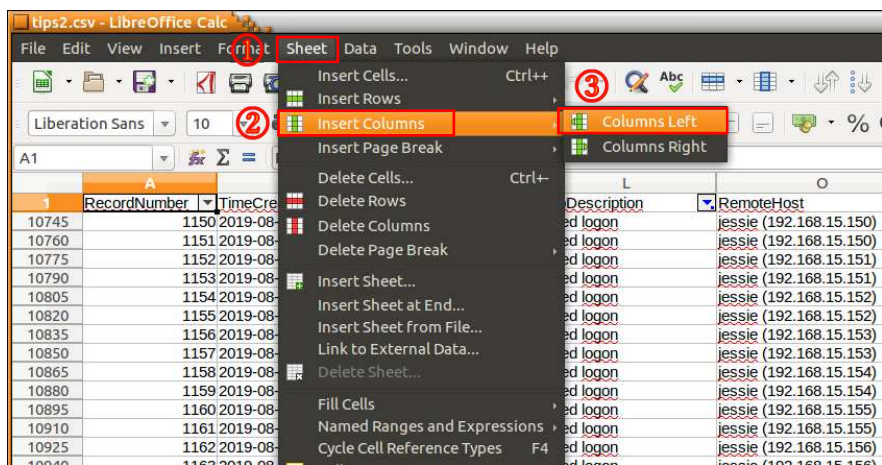


6. 「8/25 13:05:15」以降、「2019/8/25 13:06:39」まで、連続してログオン失敗していることがわかります。

RecordNumber	TimeCreated	EventId	MapDescription	RemoteHost	PayloadData1	PayloadData2	PayloadData3
10745	1150 2019-08-25 13:05:15.9657114	4625	Failed logon	jessie (192.168.15.150)	Target: Administrator	LogonType 3	
10760	1151 2019-08-25 13:05:16.7429072	4625	Failed logon	jessie (192.168.15.150)	Target: Administrator	LogonType 3	
10775	1152 2019-08-25 13:05:18.6097075	4625	Failed logon	jessie (192.168.15.151)	Target: Administrator	LogonType 3	
10790	1153 2019-08-25 13:05:19.4949230	4625	Failed logon	jessie (192.168.15.151)	Target: Administrator	LogonType 3	
10805	1154 2019-08-25 13:05:21.3791111	4625	Failed logon	jessie (192.168.15.152)	Target: Administrator	LogonType 3	
10820	1155 2019-08-25 13:05:22.2650057	4625	Failed logon	jessie (192.168.15.152)	Target: Administrator	LogonType 3	
10835	1156 2019-08-25 13:05:24.1399874	4625	Failed logon	jessie (192.168.15.153)	Target: Administrator	LogonType 3	
10850	1157 2019-08-25 13:05:25.0259744	4625	Failed logon	jessie (192.168.15.153)	Target: Administrator	LogonType 3	
10865	1158 2019-08-25 13:05:26.9370864	4625	Failed logon	jessie (192.168.15.154)	Target: Administrator	LogonType 3	
10880	1159 2019-08-25 13:05:27.8332851	4625	Failed logon	jessie (192.168.15.154)	Target: Administrator	LogonType 3	
10895	1160 2019-08-25 13:05:29.7092373	4625	Failed logon	jessie (192.168.15.155)	Target: Administrator	LogonType 3	
10910	1161 2019-08-25 13:05:30.5974961	4625	Failed logon	jessie (192.168.15.155)	Target: Administrator	LogonType 3	
10925	1162 2019-08-25 13:05:32.4051308	4625	Failed logon	jessie (192.168.15.156)	Target: Administrator	LogonType 3	
10940	1163 2019-08-25 13:05:33.3389419	4625	Failed logon	jessie (192.168.15.156)	Target: Administrator	LogonType 3	
10955	1164 2019-08-25 13:05:35.2270506	4625	Failed logon	jessie (192.168.15.157)	Target: Administrator	LogonType 3	
10970	1165 2019-08-25 13:05:36.1256355	4625	Failed logon	jessie (192.168.15.157)	Target: Administrator	LogonType 3	
10985	1166 2019-08-25 13:05:37.9881252	4625	Failed logon	jessie (192.168.15.158)	Target: Administrator	LogonType 3	
11001	1167 2019-08-25 13:05:38.8928066	4625	Failed logon	jessie (192.168.15.158)	Target: Administrator	LogonType 3	
11016	1168 2019-08-25 13:05:40.7677175	4625	Failed logon	jessie (192.168.15.159)	Target: Administrator	LogonType 3	
11031	1169 2019-08-25 13:05:41.6701353	4625	Failed logon	jessie (192.168.15.159)	Target: Administrator	LogonType 3	
11046	1170 2019-08-25 13:05:43.5501625	4625	Failed logon	jessie (192.168.15.160)	Target: Administrator	LogonType 3	
11061	1171 2019-08-25 13:05:44.4178623	4625	Failed logon	jessie (192.168.15.160)	Target: Administrator	LogonType 3	
11076	1172 2019-08-25 13:05:46.3250418	4625	Failed logon	jessie (192.168.15.161)	Target: Administrator	LogonType 3	
11091	1173 2019-08-25 13:05:47.2008683	4625	Failed logon	jessie (192.168.15.161)	Target: Administrator	LogonType 3	
11111	1174 2019-08-25 13:05:49.0696984	4625	Failed logon	jessie (192.168.15.162)	Target: Administrator	LogonType 3	
11126	1175 2019-08-25 13:05:49.9655727	4625	Failed logon	jessie (192.168.15.162)	Target: Administrator	LogonType 3	
11141	1176 2019-08-25 13:05:51.8375920	4625	Failed logon	jessie (192.168.15.163)	Target: Administrator	LogonType 3	
11156	1177 2019-08-25 13:05:52.7557546	4625	Failed logon	jessie (192.168.15.163)	Target: Administrator	LogonType 3	

※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「○」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。

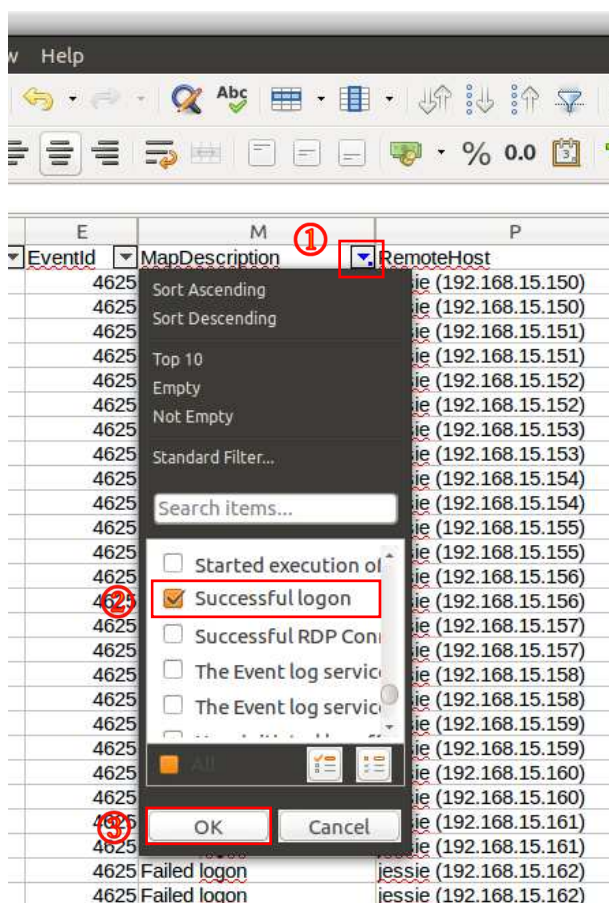
	FLAG	RecordNumber	TimeCreated
10745	○	1150	2019-08-25 13:05:15.9657114
10760	○	1151	2019-08-25 13:05:16.7429072
10775	○	1152	2019-08-25 13:05:18.6097675
10790	○	1153	2019-08-25 13:05:19.4949230
10805	○	1154	2019-08-25 13:05:21.3791111
10820	○	1155	2019-08-25 13:05:22.2650057
10835	○	1156	2019-08-25 13:05:24.1399874
10850	○	1157	2019-08-25 13:05:25.0259744
10865	○	1158	2019-08-25 13:05:26.9370864
10880	○	1159	2019-08-25 13:05:27.8332851
10895	○	1160	2019-08-25 13:05:29.7092373
10910	○	1161	2019-08-25 13:05:30.5974981
10925	○	1162	2019-08-25 13:05:32.4651358
10940	○	1163	2019-08-25 13:05:33.3389419
10955	○	1164	2019-08-25 13:05:35.2270506
10970	○	1165	2019-08-25 13:05:36.1256355
10985	○	1166	2019-08-25 13:05:37.9881252
11001	○	1167	2019-08-25 13:05:38.8928066
11016	○	1168	2019-08-25 13:05:40.7677175
11031	○	1169	2019-08-25 13:05:41.6701353
11046	○	1170	2019-08-25 13:05:43.5501625
11061	○	1171	2019-08-25 13:05:44.4178623
11076	○	1172	2019-08-25 13:05:46.3250418
11091	○	1173	2019-08-25 13:05:47.2008683
11111	○	1174	2019-08-25 13:05:49.0696984
11126	○	1175	2019-08-25 13:05:49.9655727
11141	○	1176	2019-08-25 13:05:51.8375920
11156	○	1177	2019-08-25 13:05:52.7557546

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。

MapDescription	RemoteHost	Pay
625 Failed logon	jessie (192.168.15.150)	Tar
625 Failed logon	jessie (192.168.15.150)	Tar
625 Failed logon	jessie (192.168.15.151)	Tar
625 Failed logon	jessie (192.168.15.151)	Tar
625 Failed logon	jessie (192.168.15.152)	Tar
625 Failed logon	jessie (192.168.15.152)	Tar
625 Failed logon	jessie (192.168.15.153)	Tar
625 Failed logon	jessie (192.168.15.153)	Tar
625 Failed logon	jessie (192.168.15.154)	Tar
625 Failed logon	jessie (192.168.15.154)	Tar
625 Failed logon	jessie (192.168.15.155)	Tar
625 Failed logon	jessie (192.168.15.155)	Tar
625 Failed logon	jessie (192.168.15.156)	Tar
625 Failed logon	jessie (192.168.15.156)	Tar
625 Failed logon	jessie (192.168.15.157)	Tar
625 Failed logon	jessie (192.168.15.157)	Tar
625 Failed logon	jessie (192.168.15.158)	Tar
625 Failed logon	jessie (192.168.15.158)	Tar
625 Failed logon	jessie (192.168.15.159)	Tar
625 Failed logon	jessie (192.168.15.159)	Tar
625 Failed logon	jessie (192.168.15.160)	Tar
625 Failed logon	jessie (192.168.15.160)	Tar
625 Failed logon	jessie (192.168.15.161)	Tar
625 Failed logon	jessie (192.168.15.161)	Tar
625 Failed logon	jessie (192.168.15.162)	Tar
625 Failed logon	jessie (192.168.15.162)	Tar
625 Failed logon	jessie (192.168.15.163)	Tar
625 Failed logon	jessie (192.168.15.163)	Tar



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。



The screenshot shows a Windows desktop with a LibreOffice Calc spreadsheet open. The spreadsheet is titled "tips2.csv - LibreOffice Calc" and contains a list of system events. The columns are labeled A through R, with A containing dates and times, B containing event IDs, and C through R containing descriptions of the events. The events include logon attempts, security alerts, and system errors. The status bar at the bottom of the window shows "Sheet 1 of 1" and "Average: 2877.83333333333; Sum: 17267".

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
9403	1089		2019-08-25 12:41:07.1941937	4672	Administrative logon											SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivi	
9606	1100		2019-08-25 12:44:22.2266990	4624	Successful logon	(-)										Target: NT AUTHORITY\SYSTEM LogonType 5	
9607	1111		2019-08-25 12:44:22.2267065	4672	Administrative logon											SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivi	
9611	1144		2019-08-25 12:44:22.2615968	4624	Successful logon	(-)										Target: NT AUTHORITY\SYSTEM LogonType 5	
9612	1111		2019-08-25 12:44:22.2616039	4672	Administrative logon											SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivi	
9716	1125		2019-08-25 12:47:03.5668104	4672	Administrative logon											SeSecurityPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeT	
9717	1126		2019-08-25 12:47:03.5668637	4624	Successful logon										WIN-6S3UM8M2KM3 (192.168.15.131)	Target: WIN-34073QH7TLUAdmInn\LogonType 3	
9734	1129		2019-08-25 12:47:04.9841233	4672	Administrative logon											SeSecurityPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeT	
9735	1130		2019-08-25 12:47:04.9844810	4624	Successful logon										WIN-6S3UM8M2KM3 (192.168.15.131)	Target: WIN-34073QH7TLUAdmInn\LogonType 3	
9932	1132		2019-08-25 12:47:06.2370445	4624	Successful logon	(-)										Target: Window Manager\DWm-2 LogonType 2	
9933	1133		2019-08-25 12:47:06.2378572	4624	Successful logon	(-)										Target: Window Manager\DWm-2 LogonType 2	
9934	1134		2019-08-25 12:47:06.2378611	4672	Administrative logon											SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SetpImpersonat	
9935	1135		2019-08-25 12:47:06.2378627	4672	Administrative logon											SeAssignPrimaryTokenPrivilege, SeAuditPrivilege	
9952	1139		2019-08-25 12:47:06.9548831	4624	Successful logon										WIN-34073QH7TLU (192.168.15.131)	Target: WIN-34073QH7TLUAdmInn\LogonType 10	
9953	1140		2019-08-25 12:47:06.9548883	4672	Administrative logon											SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPr	
9974	1142		2019-08-25 12:47:07.7764835	4624	Successful logon	(-)										Target: Window Manager\DWm-3 LogonType 2	
9975	1143		2019-08-25 12:47:07.7764962	4624	Successful logon	(-)										Target: Window Manager\DWm-3 LogonType 2	
9976	1144		2019-08-25 12:47:07.7765001	4672	Administrative logon											SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SetpImpersonat	
9977	1145		2019-08-25 12:47:07.7765017	4672	Administrative logon											SeAssignPrimaryTokenPrivilege, SeAuditPrivilege	
10745	O		2019-08-25 13:05:15.9657114	4625	Failed logon										jessie (192.168.15.150)	Target: Administrator LogonType 3	
10750	O		2019-08-25 13:05:16.7429072	4625	Failed logon										jessie (192.168.15.150)	Target: Administrator LogonType 3	
10775	O		2019-08-25 13:05:18.6097675	4625	Failed logon										jessie (192.168.15.151)	Target: Administrator LogonType 3	
10790	O		2019-08-25 13:05:19.4949320														

tips2.csv - LibreOffice Calc

File Edit View Insert Format Sheet Data Tools Window Help

LibreOffice Calc

Liberation Sans 10

A11398:AMJ11464

A	B	C	D	E	F	G
11291	O	1186	2019-08-25 13:06:05.5850536	4625 Failed logon	jessie (192.168.15.168)	Target: Administrator LogonType 3
11306	O	1187	2019-08-25 13:06:06.4888801	4625 Failed logon	jessie (192.168.15.168)	Target: Administrator LogonType 3
11321	O	1188	2019-08-25 13:06:08.3456711	4625 Failed logon	jessie (192.168.15.169)	Target: Administrator LogonType 3
11337	O	1189	2019-08-25 13:06:09.1818999	4625 Failed logon	jessie (192.168.15.169)	Target: Administrator LogonType 3
11352	O	1190	2019-08-25 13:06:11.0781100	4625 Failed logon	jessie (192.168.15.170)	Target: Administrator LogonType 3
11367	O	1191	2019-08-25 13:06:11.9470979	4625 Failed logon	jessie (192.168.15.170)	Target: Administrator LogonType 3
11382	O	1192	2019-08-25 13:06:13.8446455	4625 Failed logon	jessie (192.168.15.171)	Target: Administrator LogonType 3
11398	1194	1194	2019-08-25 13:06:14.7079711	4672 Administrative logon		SeSecurityPrivilege, SeBackupPrivilege, SeRestorePrivilege, Set
11399	1195	1195	2019-08-25 13:06:14.7080340	4624 Successful logon	jessie (192.168.15.171)	LogonType 3
11461	1198	1198	2019-08-25 13:06:14.9702285	4624 Successful logon	()	Target: Window Manager\DWDM-2 LogonType 2
11462	1199	1199	2019-08-25 13:06:14.9702561	4624 Successful logon	()	Target: Window Manager\DWDM-2 LogonType 2
11463	1200	1200	2019-08-25 13:06:14.9702613	4672 Administrative logon		SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, Setpersonat
11464	1201	1201	2019-08-25 13:06:14.9702632	4672 Administrative logon		SeAssignPrimaryTokenPrivilege, SeAuditPrivilege
11475	O	1204	2019-08-25 13:06:19.5808015	4625 Failed logon	jessie (192.168.15.172)	Target: Administrator LogonType 3
11490	O	1205	2019-08-25 13:06:17.4398881	4625 Failed logon	jessie (192.168.15.173)	Target: Administrator LogonType 3
11505	O	1206	2019-08-25 13:06:19.3292388	4625 Failed logon	jessie (192.168.15.173)	Target: Administrator LogonType 3
11520	O	1207	2019-08-25 13:06:20.1955014	4625 Failed logon	jessie (192.168.15.173)	Target: Administrator LogonType 3
11535	O	1208	2019-08-25 13:06:22.0752805	4625 Failed logon	jessie (192.168.15.174)	Target: Administrator LogonType 3
11550	O	1209	2019-08-25 13:06:22.9045342	4625 Failed logon	jessie (192.168.15.174)	Target: Administrator LogonType 3
11565	O	1210	2019-08-25 13:06:24.8150249	4625 Failed logon	jessie (192.168.15.175)	Target: Administrator LogonType 3
11588	O	1211	2019-08-25 13:06:25.6872619	4625 Failed logon	jessie (192.168.15.175)	Target: Administrator LogonType 3
11603	O	1212	2019-08-25 13:06:27.5631889	4625 Failed logon	jessie (192.168.15.176)	Target: Administrator LogonType 3
11618	O	1213	2019-08-25 13:06:28.4166569	4625 Failed logon	jessie (192.168.15.176)	Target: Administrator LogonType 3
11633	O	1214	2019-08-25 13:06:30.2902514	4625 Failed logon	jessie (192.168.15.177)	Target: Administrator LogonType 3
11648	O	1215	2019-08-25 13:06:31.1603041	4625 Failed logon	jessie (192.168.15.177)	Target: Administrator LogonType 3
11663	O	1216	2019-08-25 13:06:32.0405992	4625 Failed logon	jessie (192.168.15.178)	Target: Administrator LogonType 3
11678	O	1217	2019-08-25 13:06:33.9040592	4625 Failed logon	jessie (192.168.15.178)	Target: Administrator LogonType 3
11693	O	1218	2019-08-25 13:06:35.7940760	4625 Failed logon	jessie (192.168.15.179)	Target: Administrator LogonType 3
11708	O	1219	2019-08-25 13:06:36.6486620	4625 Failed logon	jessie (192.168.15.179)	Target: Administrator LogonType 3

tips2

Find

Find All Formatted Display Match Case

Sheet 1 of 1 67 rows, 1024 columns selected Default Average: 2922.91666666667; Sum: 35075 110%



14. この行の FLAG 列に「●」を入力してください。

tips2.csv - LibreOffice Calc

File Edit View Insert Format Sheet Data Tools Window Help

TakoaoPothic 10

A11398:A11464

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
11261	○	1184		2019-08-25 13:06:02.8505698	4625 Failed login	jessie (192.168.15.167)											Target: Administrator	LoginType 3
11276	○	1185		2019-08-25 13:06:03.7189250	4625 Failed login	jessie (192.168.15.167)											Target: Administrator	LoginType 3
11291	○	1186		2019-08-25 13:06:05.5850536	4625 Failed login	jessie (192.168.15.168)											Target: Administrator	LoginType 3
11306	○	1187		2019-08-25 13:06:06.4888901	4625 Failed login	jessie (192.168.15.168)											Target: Administrator	LoginType 3
11321	○	1188		2019-08-25 13:06:08.3456671	4625 Failed login	jessie (192.168.15.169)											Target: Administrator	LoginType 3
11337	○	1189		2019-08-25 13:06:09.2061439	4625 Failed login	jessie (192.168.15.169)											Target: Administrator	LoginType 3
11352	○	1190		2019-08-25 13:06:11.0781100	4625 Failed login	jessie (192.168.15.170)											Target: Administrator	LoginType 3
11352	○	1191		2019-08-25 13:06:11.9470897	4625 Failed login	jessie (192.168.15.170)											Target: Administrator	LoginType 3
11352	○	1192		2019-08-25 13:06:13.8446455	4625 Failed login	jessie (192.168.15.171)											Target: Administrator	LoginType 3
11398	●	1194		2019-08-25 13:06:14.7079711	4672 Administrative login												SeSecurityPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeT	
11399	●	1195		2019-08-25 13:06:14.7080430	4624 Successful login	jessie (192.168.15.171)											Target: WIN-340J7QH7TLU\Administrator	LoginType 3
11461	●	1198		2019-08-25 13:06:14.9702285	4624 Successful login	(-)											Target: Window Manager/DWM-2	LoginType 2
11462	●	1199		2019-08-25 13:06:14.9702561	4624 Successful login	(-)											Target: Window Manager/DWM-2	LoginType 2
11463	●	1200		2019-08-25 13:06:14.9702613	4072 Administrative login												SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonate	
11464	●	1201		2019-08-25 13:06:14.9702632	4672 Administrative login												SeAssignPrimaryTokenPrivilege, SeAuditPrivilege	
11475	○	1204		2019-08-25 13:06:16.5860815	4625 Failed login	jessie (192.168.15.172)											Target: Administrator	LoginType 3
11490	○	1205		2019-08-25 13:06:17.4399881	4625 Failed login	jessie (192.168.15.172)											Target: Administrator	LoginType 3
11505	○	1206		2019-08-25 13:06:19.3292388	4625 Failed login	jessie (192.168.15.173)											Target: Administrator	LoginType 3
11520	○	1207		2019-08-25 13:06:20.1955014	4625 Failed login	jessie (192.168.15.173)											Target: Administrator	LoginType 3
11535	○	1208		2019-08-25 13:06:22.0752805	4625 Failed login	jessie (192.168.15.174)											Target: Administrator	LoginType 3
11550	○	1209		2019-08-25 13:06:22.9304532	4625 Failed login	jessie (192.168.15.174)											Target: Administrator	LoginType 3
11565	○	1210		2019-08-25 13:06:24.8150249	4625 Failed login	jessie (192.168.15.175)											Target: Administrator	LoginType 3
11588	○	1211		2019-08-25 13:06:25.6872619	4625 Failed login	jessie (192.168.15.175)											Target: Administrator	LoginType 3
11603	○	1212		2019-08-25 13:06:27.5631889	4625 Failed login	jessie (192.168.15.176)											Target: Administrator	LoginType 3
11618	○	1213		2019-08-25 13:06:28.4166569	4625 Failed login	jessie (192.168.15.176)											Target: Administrator	LoginType 3
11633	○	1214		2019-08-25 13:06:30.2902514	4625 Failed login	jessie (192.168.15.177)											Target: Administrator	LoginType 3
11648	○	1215		2019-08-25 13:06:31.1660341	4625 Failed login	jessie (192.168.15.177)											Target: Administrator	LoginType 3
11663	○	1216		2019-08-25 13:06:33.0441338	4625 Failed login	jessie (192.168.15.178)											Target: Administrator	LoginType 3
11678	○	1217		2019-08-25 13:06:33.9040592	4625 Failed login	jessie (192.168.15.178)											Target: Administrator	LoginType 3

Find tips2

17 rows, 1 columns selected

Default

Formatted Display Match Case

Sheet 1 of 1

calin...

calin...

tips2

calin...

tips2...

水 9月 19, 00:49

0 B/s

36 B/s

Average: Sum 0

110%

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。

tips2.csv - LibreOffice Calc

File Edit View Insert Format Sheet Data Tools Window Help

LibreOffice Sans 10

0.0

A11793:AMJ11792

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
11535	○	1208		2019-08-25 13:06:22.0752805	4625 Failed login	jessie (192.168.15.174)											Target: Administrator	LoginType 3
11550	○	1209		2019-08-25 13:06:22.9304532	4625 Failed login	jessie (192.168.15.174)											Target: Administrator	LoginType 3
11565	○	1210		2019-08-25 13:06:24.8150249	4625 Failed login	jessie (192.168.15.175)											Target: Administrator	LoginType 3
11588	○	1211		2019-08-25 13:06:25.6872619	4625 Failed login	jessie (192.168.15.175)											Target: Administrator	LoginType 3
11603	○	1212		2019-08-25 13:06:27.5631889	4625 Failed login	jessie (192.168.15.176)											Target: Administrator	LoginType 3
11618	○	1213		2019-08-25 13:06:28.4166569	4625 Failed login	jessie (192.168.15.176)											Target: Administrator	LoginType 3
11633	○	1214		2019-08-25 13:06:30.2902514	4625 Failed login	jessie (192.168.15.177)											Target: Administrator	LoginType 3
11648	○	1215		2019-08-25 13:06:31.1660341	4625 Failed login	jessie (192.168.15.177)											Target: Administrator	LoginType 3
11663	○	1216		2019-08-25 13:06:33.0441338	4625 Failed login	jessie (192.168.15.178)											Target: Administrator	LoginType 3
11678	○	1217		2019-08-25 13:06:33.9040592	4625 Failed login	jessie (192.168.15.178)											Target: Administrator	LoginType 3
11693	○	1218		2019-08-25 13:06:35.7940760	4625 Failed login	jessie (192.168.15.179)											Target: Administrator	LoginType 3
11708	○	1219		2019-08-25 13:06:36.6486620	4625 Failed login	jessie (192.168.15.179)											Target: Administrator	LoginType 3
11723	○	1220		2019-08-25 13:06:38.5222115	4625 Failed login	jessie (192.168.15.180)											Target: Administrator	LoginType 3
11739	○	1221		2019-08-25 13:06:39.4045201	4625 Failed login	jessie (192.168.15.180)											Target: Administrator	LoginType 3
11792	○	1223		2019-08-25 13:20:23.1141285	4672 Administrative login												SeSecurityPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeT	
11723	○	1224		2019-08-25 13:20:23.1142320	4624 Successful login	jessie (192.168.15.10)											Target: WIN-340J7QH7TLU\Administrator	LoginType 3
11829	○	1226		2019-08-25 13:20:23.3844815	4624 Successful login	(-)											Target: Window Manager/DWM-2	LoginType 2
11830	○	1227		2019-08-25 13:20:23.3845266	4624 Successful login	(-)											Target: Window Manager/DWM-2	LoginType 2
11831	○	1228		2019-08-25 13:20:23.3845451	4672 Administrative login												SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonate	
11832	○	1229		2019-08-25 13:20:23.3845467	4672 Administrative login												SeAssignPrimaryTokenPrivilege, SeAuditPrivilege	
11848	○	1233		2019-08-25 13:20:23.8848525	4624 Successful login	WIN-340J7QH7TLU (192.168.15.10)											Target: WIN-340J7QH7TLU\Administrator	LoginType 10
11849	○	1234		2019-08-25 13:20:23.8848565	4672 Administrative login												SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPr	
11931	○	1238		2019-08-25 13:21:55.5264316	4625 Failed login	(-)											Target: -\-	LoginType 5
11932	○	1239		2019-08-25 13:21:55.5271506	4625 Failed login	(-)											Target: -\-	LoginType 5
12012	○	1245		2019-08-25 13:39:50.8184141	4624 Successful login	WIN-340J7QH7TLU (127.0.0.1)											Target: WIN-340J7QH7TLU\Administrator	LoginType 2
12013	○	1246		2019-08-25 13:39:50.8184213	4672 Administrative login												SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPr	
12070	○	1252		2019-08-25 13:41:26.0326798	4624 Successful login	(-)											Target: NT AUTHORITY\SYSTEM	LoginType 5
12071	○	1253		2019-08-25 13:41:26.0326870	4672 Administrative login												SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivi	
12125																		

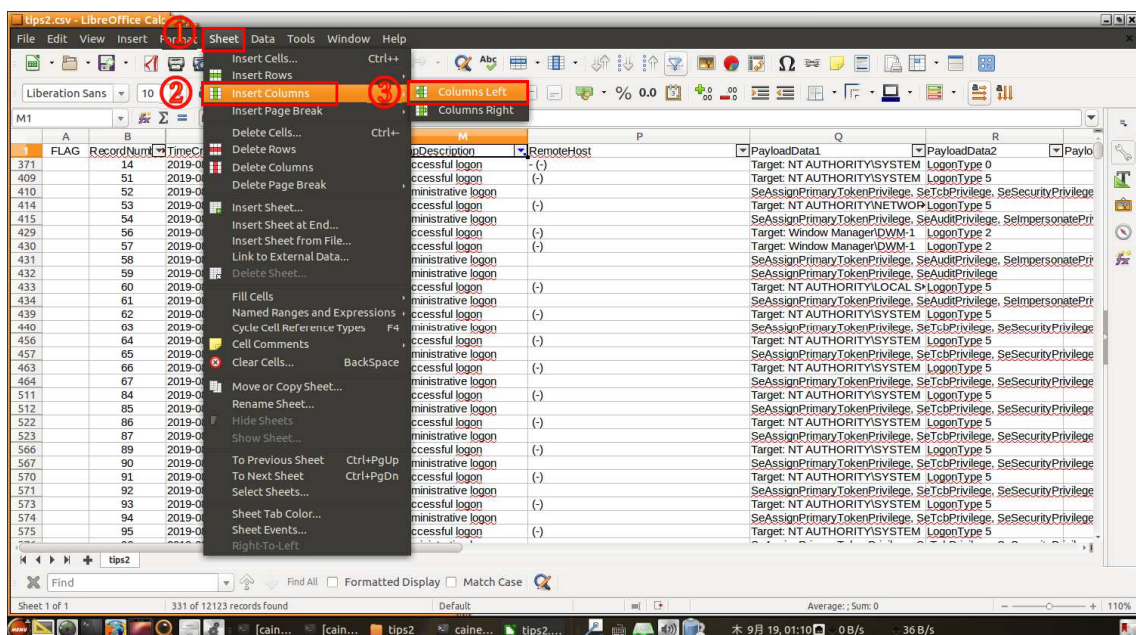
tips2

Find

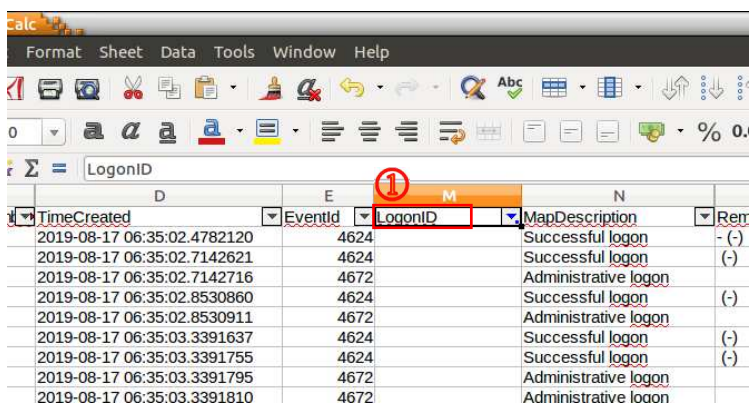
Find all Formatted Display Match Case

Sheet 1 of 1 1 rows, 1024 columns selected Default 19, 01:08 0 B/s 36 B/s Average: 2924, Sum: 5848 110%

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。

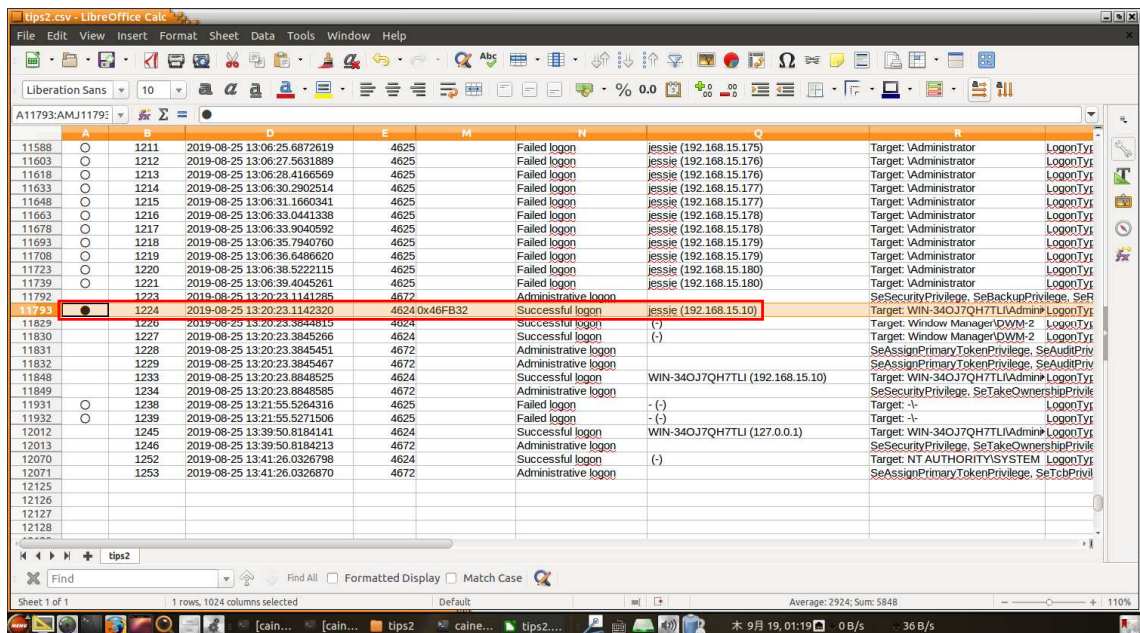
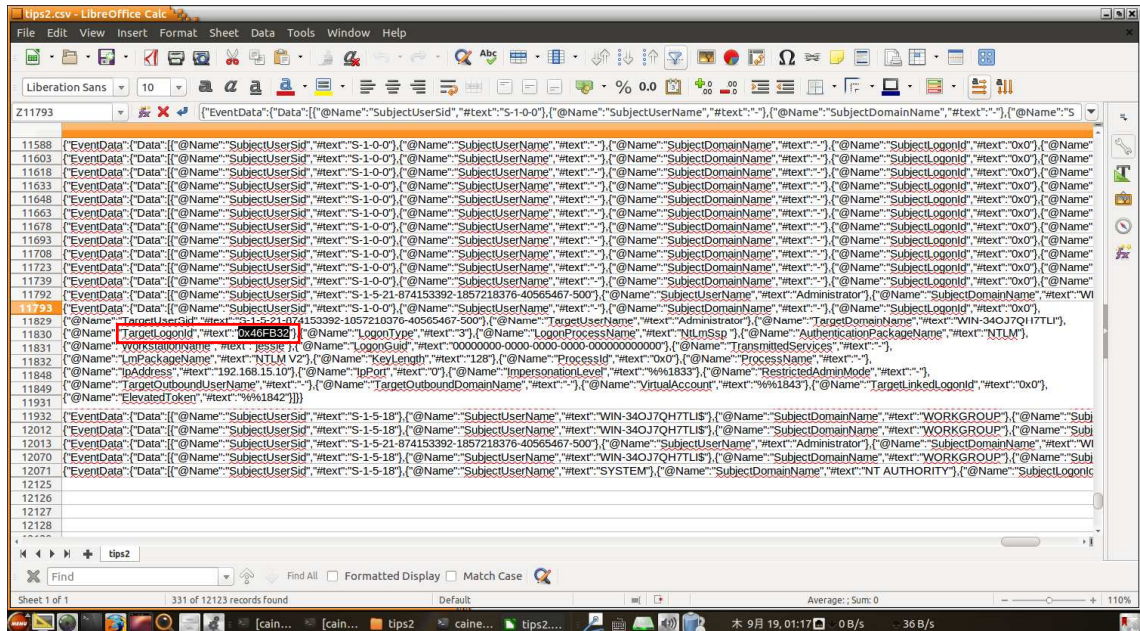


17. 一列目に「LogonID」と入力してください。



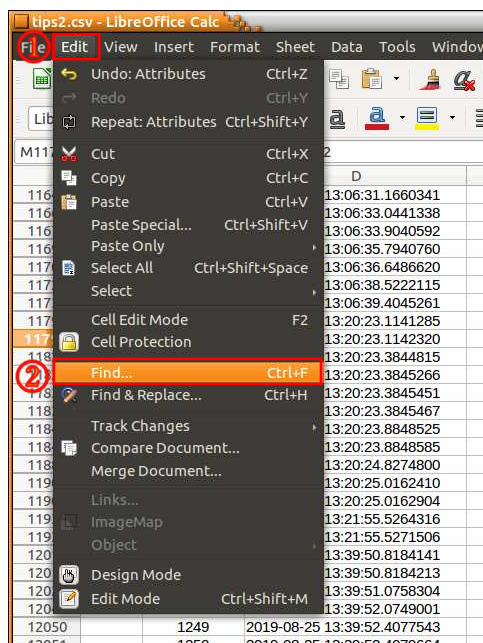


19. 攻撃者が RDP でログオンしたと思われる RecordNumber「1224」行の「Payload」列の値を参照し、「TargetLogonId」の値「0x46FB32」をコピーし、「LogonID」列に追加します。

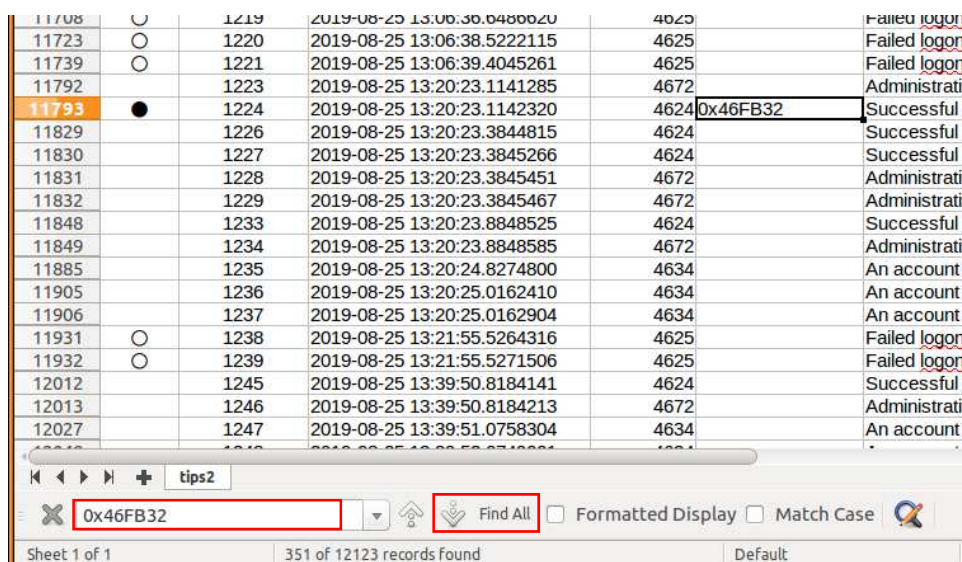


21. MapDescription 列のフィルタでログオフを示す「An account was logged off」と「User initiated logoff」のチェックを追加(これまで選択したチェックは残したまま)します。

22. メニューバーから「Edit」→「Find」を選択します。

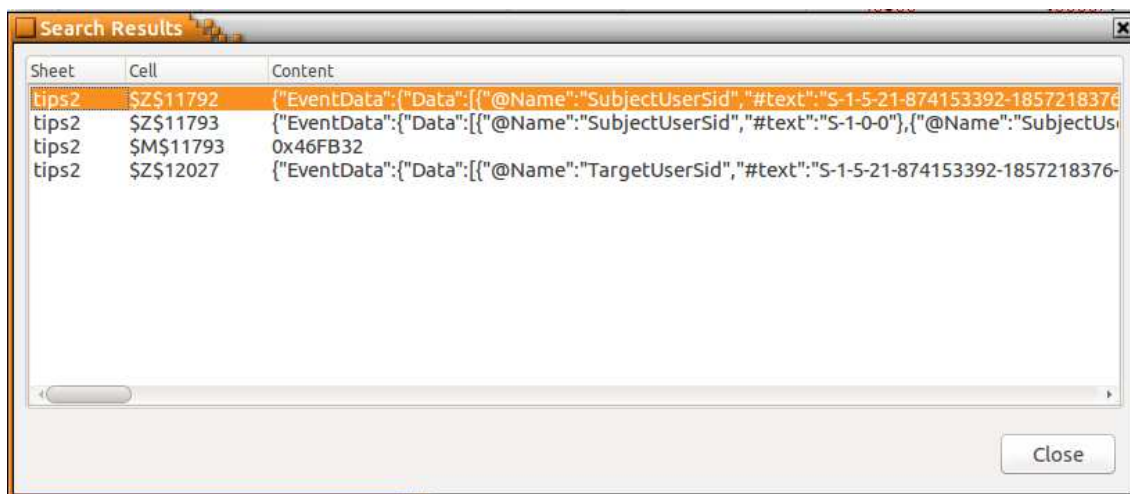


23. 画面下に検索キーワード入力フォームが表示されますので、検索文字列入力欄に TargetLogonId の値「0x46FB32」をコピーし、「Find All」ボタンを押します。





25. 別ウィンドウが開き、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。



#### 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**