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	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、Adm inistrator 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。

tips2.csv -	LibreOffice	Calc							×
File Edit	View Insert	t Format Sheet Da	ata Tools Window	Help					×
D. B	. 🖂 . 🗌		A. A. A.	Abs man a	e . (10 til 10 🖶 📼				
•••	1 🖬 1 🛛		s 💷 * 🏓 🎉 i	∽	e • Gu 😳 💷 🔆 🗖	o 🙋 🔯 77 📾			
Liberation	Sans y 1		a . = . =		🛛 💌 🗸 % 0.0 🕅 🔶	0.00 🚃 🚃 📖	· 🕞 · 🗖 · 🚍 · 🚉 🏭		
Liberdelon	Sans I.S. (								
A1:X12124	- 5	r Σ = TimeCreate	d						
A			D		F				
RecordN	umber EventF	RecordId TimeCreated	EventId L	evel Provider		Channel		Pro	2
2	3	3 2019-08-17 06:34	4:46.5169233 12	4 Microsoft-Windows-Kernel-General		System			-
3	4	4 2019-08-17 06:34	4:46.5169537 153	4 Microsoft-Windows-Kernel-Boot	The second se	System		1	T
4	5	5 2019-08-17 06:34	4:46.5170390 27	4 Microsoft-Windows-Kemel-Boot	Solt		<u> </u>		
2	5	6 2019-08-17 06:34	4:46.51/0394 25	4 Microsoft-Windows-Kernel-Boot	Sort Criteria Options	_			
7	0	9 2019-08-17 06:34	4.46.5170020 22	4 Microsoft Mindows Kemel-Boot	Sore criterito Options	<b>M</b>			0
8	1	1 2019-08-17 06:34	4:46.5179267 403	3 Microsoft-Windows-Kemel-PnP	Sort Key 1	U			0
9	2	2 2019-08-17 06:34	4:46.5182317 410	4 Microsoft-Windows-Kernel-PnP			Assenting		3
10	3	3 2019-08-17 06:34	4 - undefined -		TimeCreated		Ascending		822
11	4	4 2019-08-17 06:34	4 RecordNumber	2)			Descending		
12	5	5 2019-08-17 06:3	4 EventRecordid	<u> </u>			-		
13	6	6 2019-08-17 06:3	TimeCreated		ort Key 2				
14	7	7 2019-08-17 06:34	Eventid				Accepding	-	
15	8	8 2019-08-17 06:34	Level		- undefined -		Ascending		
10	10	9 2019-06-17 00.34	Provider				<ul> <li>Descending</li> </ul>		
18	11	11 2019-08-17 06:3	Channel						
19	12	12 2019-08-17 06:34	Processid		ort Key 3				
20	13	13 2019-08-17 06:3	Threadld				Ascending		
21	14	14 2019-08-17 06:34	4 Computer		- undefined -		e Ascending		
22	15	15 2019-08-17 06:34	4 Userid				Descending		
23	16	16 2019-08-17 06:34	4 MapDescription						
24	17	17 2019-08-17 06:3	4 Chunkinumber						
25	18	18 2019-08-17 06:34	DomotoHost						
26	19	19 2019-08-17 06:34	4 Remoteriost						
20	20	20 2019-08-17 06:34	A PayloadData?						
20	22	22 2019-08-17 06:3	A PayloadData2						
30	23	23 2019-08-17 06:34	4 PayloadData4						
31	24	24 2019-08-17 06:3	4 PayloadData5					-	
(C		)	PavloadData6					• 8	
HAPH	+ tips2		ExecutableInfo						
Mr Find		- @	SourceFile						
Filld		▲ .8.	Payload		Help		OK Cancel Reset		
Sheet 1 of 1			-	Default				+	100%
	× 💽 📂		and a finite of	Non all sales white		* 0 8 40 33-55	00/c 0/c0/c		
			cam [cam	calne 🗅 cipsz		JA 975 18, 23:50	0 B/S - 30 B/S		

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。MapDescriptio n 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。

崎 🖽 • 🗊 • 🖓 😳 🕾 🛧	- 🖪 🏉 🕼 Ω 🖛 🖵 🗏 🖓 🖽 • 🚍 Ι	: 🖶 • 🎟 • 🖽 • UP 👯 🗄	🖓 國 🌑 🚺 Ω 🖛 🚽 🛛	
🐷 • % 0.0 🕅	♣ <u>a</u> _o , , , , , , , , , , , , , , , , , ,	% 0.0 f	31 🔹 🥺 💳 💳 💷 - 🕞	· 🗆 • 😑 • 🖭
L L				
W ManDosoriation		ĸ		M
L C 1 E 19		▼UserId ▼ MapDescription		ChunkNumber Vuller
1 \$1.5.19	Sort Ascending	TU S-1-5-18	Sort Ascending	0
1 5.1.5.18	Sort Descending	TU S-1-5-18	Sort Descending	0
I S-1-5-18		TLI 5-1-5-18		0
J S-1-5-18	100 10	TU 0.1.5.10	Top 10	0
J S-1-5-18	Empty 0	TU 01510	Empty	0
J S-1-5-18	Not Empty 0	TU 01510	Not Emoty	
J S-1-5-18	0	TU 01510	Hot Empty	0
J S-1-5-18	Standard Filter 0	TLI 01510	Standard Filter	
J S-1-5-18	0	TLI 5-1-5-18		0
J S-1-5-18	Search items 0	TU 01510	Search items	
J S-1-5-18	0	TU 01510	Starteriteritari	
J S-1-5-18	Cempt a	TU 0.1.5.10		
J S-1-5-18	0	TU 01510		0
J S-1-5-18	A logon was attemp 0	TLI 5-1-5-18	Failed logon	0
J S-1-5-18	A new service was in 0	TLI 5-1-5-18		9
J S-1-5-18	0	TU 01510	Finished enumerati	C
J S-1-5-18	A user account was 0	TU 01510	Finished execution	0
J S-1-5-18	Administrative logo 0	TLI 5-1-5-18		0
J S-1-5-18	0	TLI 5-1-0-18	NTLM authenticatio	0
J S-1-5-18		TLI 5-1-5-18		· · · · · · · · · · · · · · · · · · ·
J S-1-5-18		ILI S-1-5-18		-
J S-1-5-18		TLI S-1-5-18		0
J S-1-5-18	OK Cancel 0	111 5-1-5-18		0
J S-1-5-18	OK Conter 0	111 5-1-5-18	OK Cancel	0
J S-1-5-18	0	ILI S-1-5-18		
J S-1-5-18	0 -	→1U S-1-5-18		0

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。

P         X         E         Record/humber         Image: Logical status         Payload/Data         Paylo	ration Sa	ins 🔻 10 💌 🛃 🖉	<u>a</u> -	<mark>=</mark> · • • • • <b>•</b>	= = = 🤜 • % o	).0 🛐 比 🚅 🔝 🚺	🗄 • 🕞 • 🛄 • 📑	· 😫 🏭
A         C         D         L         O         P         Q         R           5         1159/2019-08-25 13:05:15.0691714         Wappescription         RemoteVisit         PayloadData1         PayloadData3           5         1159/2019-08-25 13:05:15.0691714         4625 Failed loggn         ressign (12):081.51:50)         Target: Maministrator         Loggn1ype 3           5         1152/2019-08-25 13:05:15.0691.49420         4625 Failed loggn         ressign (12):081.51:50)         Target: Maministrator         Loggn1ype 3           5         1152/2019-08-25 13:05:12.0691.49420         4625 Failed loggn         ressign (12):081.51:50)         Target: Maministrator         Loggn1ype 3           6         1156/2019-08-25 13:05:21.0562.27         4625 Failed loggn         ressign (12):081.51:50         Target: Maministrator         Loggn1ype 3           1156/2019-08-25 13:05:27.07         4625 Failed loggn         ressign (12):081.51:50         Target: Maministrator         Loggn1ype 3           1156/2019-08-25 13:05:27.07         4625 Failed loggn         ressign (12):081.51:50         Target: Maministrator         Logg01ype 3           1159/2019-08-25 13:05:27.07         4625 Failed loggn         ressign (12):081.51:50         Target: Maministrator         Logg01ype 3           1160/2019-08-25 13:05:23.05:72.07         4625 Failed loggn         re		🔹 😹 ∑ 💻 RecordNu	imber					
Encondunider         Image: Manual Mage: Status         Image: Mage: Mag	-	A C		D L	0	P	Q	R
1192/2019-08-25 13/05:15.069/114       4425 Failed (ggn)       pesses (122,108.15.150)       Target: Varimistrator       Logon) ype 3         1152/2019-08-25 13/05:16.074/20175       4425 Failed (ggn)       pesses (132,108.15.150)       Target: Varimistrator       Logon) ype 3         1152/2019-08-25 13/05:16.074/20175       4425 Failed (ggn)       pesses (132,108.15.150)       Target: Varimistrator       Logon) ype 3         1152/2019-08-25 13/05:16.074.03097       4425 Failed (ggn)       pesses (132,108.15.151)       Target: Varimistrator       Logon) ype 3         1154/2019-08-25 13/05:21.0791117       4425 Failed (ggn)       pesses (132,108.15.152)       Target: Varimistrator       Logon) ype 3         1154/2019-08-25 13/05:20.0597144       4425 Failed (ggn)       pesses (132,108.15.152)       Target: Varimistrator       Logon) ype 3         1159/2019-08-25 13/05:20.0597144       4425 Failed (ggn)       pesses (132,108.15.153)       Target: Varimistrator       Logon) ype 3         1159/2019-08-25 13/05:20.0597344       4425 Failed (ggn)       pesses (132,108.15.154)       Target: Varimistrator       Logon) ype 3         1159/2019-08-25 13/05:20.0597344       4425 Failed (ggn)       pesse (132,108.15.154)       Target: Varimistrator       Logon) ype 3         1162/2019-08-25 13/05:30.057408       4425 Failed (ggn)       pesse (132,108.15.154)       Target: Varimistrator       Logon) ype 3	Recon	dNumber   TimeCreated	L	EventId MapDescription	RemoteHost	PayloadData1	▼PayloadData2	PayloadData3
1112       1121       2019-08-25       12002.10       4625       Failed logon       psssss       (12)       1142       2019-08-25       12002.10 <td>5</td> <td>1150 2019-08-25 13:05:1</td> <td>15.9657114</td> <td>4625 Failed logon</td> <td>jessie (192.168.15.150)</td> <td>Target: VAdministrator</td> <td>LogonType 3</td> <td></td>	5	1150 2019-08-25 13:05:1	15.9657114	4625 Failed logon	jessie (192.168.15.150)	Target: VAdministrator	LogonType 3	
1122/01940-213/0218/04-213/0218/04-025         4425 Falled (ggn)         gssss (132,108,135,11)         Target: Varimistrator         L0000/1ype 3           1134/201940-213/0218/04-2313/0213/0213         4425 Falled (ggn)         gssss (132,108,135,11)         Target: Varimistrator         L0000/1ype 3           1134/201940-213/0213         4425 Falled (ggn)         gssss (132,108,135,12)         Target: Varimistrator         L0000/1ype 3           1134/201940-2313/0221         4425 Falled (ggn)         gssss (132,108,135,12)         Target: Varimistrator         L0000/1ype 3           1136/201940-2513/0252/0397/44         4425 Falled (ggn)         gssss (132,108,135,12)         Target: Varimistrator         L0000/1ype 3           1136/201940-2513/0252/0397/44         4425 Falled (ggn)         gssss (132,108,135,15)         Target: Varimistrator         L0000/1ype 3           1136/201940-2513/0252/03973744         4425 Falled (ggn)         gssss (132,108,15,15)         Target: Varimistrator         L0000/1ype 3           1136/201940-2513/0523/03973491         4425 Falled (ggn)         gssss (132,108,15,15)         Target: Varimistrator         L0000/1ype 3           1136/201940-2513/053.03974941         4425 Falled (ggn)         gssss (132,108,15,15)         Target: Varimistrator         L0000/1ype 3           1136/201940-2513/053.03974941         4425 Falled (ggn)         gssss (132,108,15,15)         Target: Var	)	1151 2019-08-25 13:05:1	16.7429072	4625 Failed logon	jessie (192.168.15.150)	Target: VAdministrator	LogonType 3	
113520190-25130539499200       4225 Falled (bg0)       gBSBR (132,108.1512)       Target: Volministation       L000(1))p2 3         113520190-25130532       113620190-25130522       113620190-25130522       113620190-2513053       11	>	1152 2019-08-25 13:05:	18.6097675	4625 Failed logon	Jessie (192.168.15.151)	Target: VAdministrator	Logon Type 3	
All Accord and a sector of a sector		1153 2019-08-25 13:05:	19.4949230	4625 Failed logon	iossie (192.168.15.151)	Target: V4dministrator	LogonType 3	
1.1.2.2.2.19.02.2.1.3.02.2.1.2.00.2.7         442.5 Falled (agen 1.1.2.2.2.19.2.2.1.2.00.2.1.2.1.2.2.1.2.1.2.1.2.1.2.	1	1155 2010 09 25 12:05:	21.3/31111	4625 Failed logon	iossic (102.169.15.152)	Target: Administrator	LogonTupo 2	
113772019-08:25       13362:53.0529714       1425 Failed begin       pesses 132.01815.1530       Target: Valministator       10001009:3         11372019-08:25       13362:53.0526:2059714       1425 Failed begin       pesses 132.0183.15150       Target: Valministator       10001009:3         11392019-08:25       13365:27.0322851       4625 Failed begin       pesses (132.1681.15150       Target: Valministator       10000109:3         11392019-08:25       13365:27.0322873       4625 Failed begin       pesses (132.1681.15150       Target: Valministator       10000109:8         11012019-08:25       1305:32.0727.03287461       4625 Failed begin       pesses (132.1681.15150       Target: Valministator       10000109:8         11012019-08:25       1305:32.42075.08       4625 Failed begin       pesses (132.1681.15150       Target: Valministator       10000109:8         11032019-08:25       1305:32.520750       4625 Failed begin       pesse (132.1681.15150       Target: Valministator       Logot109:8         11032019-08:25       1305:32.720750       4625 Failed begin       pesse (132.1681.15150       Target: Valministator       Logot109:8         11032019-08:25       1305:34.7207535       4625 Failed begin       pesse (132.1681.15150       Target: Valministator       Logot109:8         11062019-08:25       1305:34.720738       4625 Failed begin<		1156 2019-08-25 13:05:	24 1399874	4625 Failed logon	jessie (192.168.15.152)	Target: \Administrator	LogonType 3	
1118/2010-08-25 13/05:26 397:08-04       #G25 Failed [bgn]       Desse; [132:168.15:150]       Target: Marinistrator       L000010pe 3         118/2010-08-25 13/05:27 397:28-04       #G25 Failed [bgn]       Desse; [132:168.15:150]       Target: Marinistrator       L000010pe 3         118/2010-08-25 13/05:27 397:28-04       #G25 Failed [bgn]       Desse; [132:168.15:150]       Target: Marinistrator       L000010pe 3         118/2010-08-25 13/05:32 07902373       #G25 Failed [bgn]       Desse; [132:168.15:150]       Target: Marinistrator       L000010pe 3         118/2010-08-25 13/05:32 049138       #G25 Failed [bgn]       Desse; [132:168.15:150]       Target: Marinistrator       L0000100210         118/2010-08-25 13/05:32 05733       #G25 Failed [bgn]       pessi; [132:168.15:150]       Target: Marinistrator       L000010029         118/2010-08-25 13/05:33 05894       #G25 Failed [bgn]       pessi; [122:168.15:150]       Target: Marinistrator       L000010029         118/2010-08-25 13/05:33 05894       #G25 Failed [bgn]       pessi; [122:168.15:159]       Target: Marinistrator       L000010029         118/2010-08-25 13/05:43 05733       #G25 Failed [bgn]       pessi; [122:168.15:159]       Target: Marinistrator       L000010029         118/2010-08-25 13/05:43 05733       #G25 Failed [bgn]       pessi; [122:168.15:159]       Target: Marinistrator       L000010029         11	2	1157 2019-08-25 13:05:	25 0250744	4625 Failed logon	iessie (192,100,13,133)	Target: \Administrator	LogonType 3	
11992019-98-25 13/05:27 3322851       4425 Failed logon       psssk (132,198.15.15)       Target Administrator       L0g00Type 3         11012019-08-25 13/05:27 0702373       4425 Failed logon       psssk (132,198.15.15)       Target Administrator       L0g00Type 3         11012019-08-25 13/05:30 0574/081       4425 Failed logon       psssk (132,108.15.15)       Target Administrator       L0g00Type 3         11012019-08-25 13/05:30 0574/081       4425 Failed logon       pssk (132,108.15.15)       Target Administrator       L0g00Type 3         11032019-08-25 13/05:33 05342/05763       4425 Failed logon       pssk (132,108.15.15)       Target Administrator       L0g00Type 3         11032019-08-25 13/05:34 025763       4425 Failed logon       pssk (132,108.15.15)       Target Administrator       L0g00Type 3         11062019-08-25 13/05:34 025763       4425 Failed logon       pssk (132,108.15.15)       Target Administrator       L0g00Type 3         11062019-08-25 13/05:34 0507177       4425 Failed logon       pssk (132,108.15.15)       Target Administrator       L0g00Type 3         1108/2019-08-25 13/05:44 05073       4425 Failed logon       pssk (132,108.15.15)       Target Administrator       L0g00Type 3         1108/2019-08-25 13/05:44 070338       4425 Failed logon       pssk (132,108.15.15)       Target Administrator       L0g00Type 3         1108/2019-08-25 13/05:44 070	;	1158 2019-08-25 13:05:2	26 9370864	4625 Failed logon	jessie (192,168,15,154)	Target: \Administrator	LogonType 3	
1100/2019-08-25 13/05-23 7002373       4025 Failed bggn       pssssk (132, 198.15.155)       Target: Administrator       L0000T/pp8 3         1102/2019-08-25 13/05-23 2005378       4025 Failed bggn       psssk (132, 198.15.155)       Target: Administrator       L0000T/pp8 3         1102/2019-08-25 13/05-23 200538       4025 Failed bggn       psssk (132, 198.15.155)       Target: Administrator       L0000T/pp8 3         1102/2019-08-25 13/05-33 207506       4625 Failed bggn       psssk (132, 198.15.156)       Target: Administrator       L0000T/pp8 3         1104/2019-08-25 13/05-33 207506       4625 Failed bggn       psssk (132, 198.15.157)       Target: Administrator       L0000T/pp8 3         1106/2019-08-25 13/05-33 9881252       4625 Failed bggn       psssk (132, 198.15.157)       Target: Administrator       L0000T/pp8 3         1106/2019-08-25 13/05-43 707175       4625 Failed bggn       pssk (132, 198.15.159)       Target: Administrator       L0000T/pp8 3         1108/2019-08-25 13/05-44 707175       4625 Failed bggn       pssk (132, 198.15.159)       Target: Administrator       L0000T/pp8 3         1107/2019-08-25 13/05-44 7078       4625 Failed bggn       pssk (132, 198.15.159)       Target: Administrator       L000T/pp8 3         117/2019-08-25 13/05-44 2078       4625 Failed bggn       pssk (122, 198.15.150)       Target: Administrator       L000T/pp8 3         1	)	1159 2019-08-25 13:05:2	27 8332851	4625 Failed logon	iessie (192,168,15,154)	Target: \Administrator	LogonType 3	
1111         1112 <t< td=""><td></td><td>1160 2019-08-25 13:05:2</td><td>29 7092373</td><td>4625 Failed logon</td><td>jessie (192 168 15 155)</td><td>Target: \Administrator</td><td>LogonType 3</td><td></td></t<>		1160 2019-08-25 13:05:2	29 7092373	4625 Failed logon	jessie (192 168 15 155)	Target: \Administrator	LogonType 3	
5       1102 2010-02:51 30:03:2.40:13:08       4025 Failed (bgon)       psssp: (122.108.15.15)       Target: Administrator       Logo(T)pc 3         6       1104 2010-02:51 30:05:33.28:41)       4425 Failed (bgon)       psssp: (122.108.15.15)       Target: Administrator       Logo(T)pc 3         5       1104 2010-03:51 30:05:33.28:250:06       4425 Failed (bgon)       psssp: (122.108.15.15)       Target: Administrator       Logo(T)pc 3         5       1106 2010-03:51 30:05:33.28:42:05       4425 Failed (bgon)       psssp: (122.108.15.15)       Target: Administrator       Logo(T)pc 3         5       1106 2010-03:51 30:05:33.08:42:05       4425 Failed (bgon)       psssp: (122.108.15.15)       Target: Administrator       Logo(T)pc 3         5       1108 2010-03:51 30:05:40.7771/5       4425 Failed (bgon)       psssp: (122.108.15.15)       Target: Administrator       Logo(T)pc 3         5       1107 2010-03:51 30:05:40.35010:55       4425 Failed (bgon)       psssp: (122.108.15.15)       Target: Administrator       Logo(T)pc 3         5       1172 2010-03:51 30:05:40.35010:55       4425 Failed (bgon)       psssp: (122.108.15.16)       Target: Administrator       Logo(T)pc 3         5       1172 2010-03:51 30:05:40.3504.412705:24       4425 Failed (bgon)       psssp: (122.108.15.16)       Target: Administrator       Logo(T)pc 3         6       1172 2	)	1161 2019-08-25 13:05:3	30.5974981	4625 Failed logon	jessje (192.168.15.155)	Target: \Administrator	LogonType 3	
11632010-08-25 13:05:33.3398419       4425 Failed (ggn)       pssgc (122.108.15.157)       Target: Vadministrator       Logon7/pge 3         11632010-08-25 13:05:32.27050       4425 Failed (ggn)       pssgc (122.108.15.157)       Target: Vadministrator       Logon7/pge 3         11652010-08-25 13:05:32.0535.27050       4425 Failed (ggn)       pssgc (122.108.15.157)       Target: Vadministrator       Logon7/pge 3         11652010-08-25 13:05:34.0537.9802206       4425 Failed (ggn)       pssgc (122.108.15.159)       Target: Vadministrator       Logon7/pge 3         11672010-08-25 13:05:34.0590.757       4425 Failed (ggn)       pssgc (122.108.15.159)       Target: Vadministrator       Logon7/pge 3         11692010-08-25 13:05:44.0701353       4425 Failed (ggn)       pssgc (122.108.15.159)       Target: Vadministrator       Logon7/pge 3         11692010-08-25 13:05:44.0701353       4425 Failed (ggn)       pssgc (122.108.15.160)       Target: Vadministrator       Logon7/pge 3         1172/2010-08-25 13:05:44.17023       4425 Failed (ggn)       pssgc (122.108.15.160)       Target: Vadministrator       Logon7/pge 3         1172/2010-08-25 13:05:44.0701354       4425 Failed (ggn)       pssgc (122.108.15.160)       Target: Vadministrator       Logon7/pge 3         1172/2010-08-25 13:05:44.0705727       4425 Failed (ggn)       pssgc (122.108.15.161)       Target: Vadministrator       Logon7/pge 3     <	5	1162 2019-08-25 13:05:3	32.4651358	4625 Failed logon	jessie (192.168.15.156)	Target: VAdministrator	LogonType 3	
5       1164/2019-08-25 13:05:35.2270506       4425 Failed (bggn)       jessige (192,108.15.157)       Target: Vadministrator       LogonType 3         5       1165/2019-08-25 13:05:35.237636       4425 Failed (bggn)       jessige (192,108.15.157)       Target: Vadministrator       LogonType 3         5       1166/2019-08-25 13:05:37.9881252       4425 Failed (bggn)       jessige (192,108.15.158)       Target: Vadministrator       LogonType 3         5       1166/2019-08-25 13:05:43.0767175       4425 Failed (bggn)       jessige (192,108.15.158)       Target: Vadministrator       LogonType 3         5       1168/2019-08-25 13:05:43.0767175       4425 Failed (bggn)       jessige (192,108.15.158)       Target: Vadministrator       LogonType 3         6       1170/2019-08-25 13:05:44.3705.25       4425 Failed (bggn)       jessige (192,108.15.150)       Target: Vadministrator       LogonType 3         6       1172/2019-08-25 13:05:44.0705.25       4425 Failed (bggn)       jessige (192,108.15.160)       Target: Vadministrator       LogonType 3         6       1172/2019-08-25 13:05:44.0706.25       4425 Failed (bggn)       jessige (192,108.15.161)       Target: Vadministrator       LogonType 3         1172/2019-08-25 13:05:44.0706.25       4425 Failed (bggn)       jessige (192,108.15.161)       Target: Vadministrator       LogonType 3         1172/2019-08-25 13:05:41.	)	1163 2019-08-25 13:05:3	33.3389419	4625 Failed logon	jessie (192.168.15.156)	Target: \Administrator	LogonType 3	
0       1165 /2110-08-25 13:05:36.1256355       4425 Failed (ggn)       jessige (192:108.15.159)       Target: Vadministrator       LogonType 3         1       1167 /2110-08-25 13:05:37.088125       4425 Failed (ggn)       jessige (192:108.15.159)       Target: Vadministrator       LogonType 3         1       1167 /2110-08-25 13:05:40.076777       4425 Failed (ggn)       jessige (192:108.15.159)       Target: Vadministrator       LogonType 3         1       1169 /2010-08-25 13:05:40.0767777       4425 Failed (ggn)       jessige (192:108.15.169)       Target: Vadministrator       LogonType 3         1       1169 /2010-08-25 13:05:40.4771353       4425 Failed (ggn)       jessige (192:108.15.160)       Target: Vadministrator       LogonType 3         1       1170 /2010-08-25 13:05:40.4771353       4425 Failed (ggn)       jessige (192:108.15.160)       Target: Vadministrator       LogonType 3         1       1171 /2010-08-25 13:05:40.477623       4425 Failed (ggn)       jessige (192:108.15.160)       Target: Vadministrator       LogonType 3         1       1172 /2010-08-25 13:05:40.0986964       4425 Failed (ggn)       jessige (192:108.15.160)       Target: Vadministrator       LogonType 3         1       1174 /2010-08-25 13:05:40.09869727       4425 Failed (ggn)       jessige (192:108.15.160)       Target: Vadministrator       LogonType 3         1	5	1164 2019-08-25 13:05:3	35.2270506	4625 Failed logon	jessie (192.168.15.157)	Target: \Administrator	LogonType 3	
5       1166/2019-08-25 13:05:37,9881252       4425 Failed (bggn)       jessige (192,108.15.158)       Target: Vadministrator       LogonType 3         6       1166/2019-08-25 13:05:43,07520       4425 Failed (bggn)       jessige (192,108.15.158)       Target: Vadministrator       LogonType 3         5       1168/2019-08-25 13:05:43,0757175       4425 Failed (bggn)       jessige (192,108.15.158)       Target: Vadministrator       LogonType 3         6       1107/2019-08-25 13:05:44,0757125       4425 Failed (bggn)       jessige (192,108.15.159)       Target: Vadministrator       LogonType 3         6       1177/2019-08-25 13:05:44,370524       4425 Failed (bggn)       jessige (192,108.15.160)       Target: Vadministrator       LogonType 3         6       1172/2019-08-25 13:05:44,02564       4425 Failed (bggn)       jessige (192,108.15.160)       Target: Vadministrator       LogonType 3         1172/2019-08-25 13:05:44,005684       4425 Failed (bggn)       jessige (192,108.15.161)       Target: Vadministrator       LogonType 3         1174/2019-08-25 13:05:44,005684       4425 Failed (bggn)       jessige (192,108.15.162)       Target: Vadministrator       LogonType 3         1174/2019-08-25 13:05:44,005782       4425 Failed (bggn)       jessige (192,108.15.162)       Target: Vadministrator       LogonType 3         1176/2019-08-25 13:05:45,075784       4425 Failed (bggn)<	0	1165 2019-08-25 13:05:3	36.1256355	4625 Failed logon	jessie (192.168.15.157)	Target: \Administrator	LogonType 3	
1         1167/2019-08-25 13/05:8.0928066         4425 Failed (ggn)         jessige (192.108.15.159)         Target: Valministrator         LogonType 3           1         1169/2019-08-25 13/05:4.07071375         4425 Failed (ggn)         jessige (192.108.15.159)         Target: Valministrator         LogonType 3           1         1169/2019-08-25 13/05:4.1701353         4425 Failed (ggn)         jessige (192.108.15.159)         Target: Valministrator         LogonType 3           1         1171/2019-08-25 13/05:4.4176623         4425 Failed (ggn)         jessige (192.108.15.160)         Target: Valministrator         LogonType 3           1         1171/2019-08-25 13/05:4.4176623         4425 Failed (ggn)         jessige (192.108.15.161)         Target: Valministrator         LogonType 3           1         1172/2019-08-25 13/05:4.0409654         4425 Failed (ggn)         jessige (192.108.15.161)         Target: Valministrator         LogonType 3           1         1172/2019-08-25 13/05:4.0409577         4425 Failed (ggn)         jessige (192.108.15.162)         Target: Valministrator         LogonType 3           1         1176/2019-08-25 13/05:4.0409577         4425 Failed (ggn)         jessige (192.108.15.163)         Target: Valministrator         LogonType 3           1         1176/2019-08-25 13/05:4.0409577         4425 Failed (ggn)         jessige (192.108.15.153)         Target: Valm	5	1166 2019-08-25 13:05:3	37.9881252	4625 Failed logon	jessie (192.168.15.158)	Target: \Administrator	LogonType 3	
6       1168 2019 08-25 1305:40.7671175       4625 Failed loggn       jessig (192.108.15.195)       Target: Vadministrator       LogonType 3         6       1170 2019 08-25 1305:41.670133       4625 Failed loggn       jessig (192.108.15.195)       Target: Vadministrator       LogonType 3         6       1170 2019 08-25 1305:44.35001625       4625 Failed loggn       jessig (192.108.15.106)       Target: Vadministrator       LogonType 3         6       1172 2019 08-25 1305:44.35001425       4625 Failed loggn       jessig (192.108.15.106)       Target: Vadministrator       LogonType 3         6       1172 2019 08-25 1305:44.25064.41       4625 Failed loggn       jessig (192.108.15.160)       Target: Vadministrator       LogonType 3         1       1173 2019 08-25 1305:47.47006803       4625 Failed loggn       jessig (192.108.15.161)       Target: Vadministrator       LogonType 3         1       1174 2019 08-25 1305:49.0565727       4625 Failed loggn       jessig (192.108.15.162)       Target: Vadministrator       LogonType 3         1       1176 2019 08-25 1305:52.055764       4625 Failed loggn       jessig (192.108.15.163)       Target: Vadministrator       LogonType 3         1       1176 2019 08-25 13055.25.2575764       4625 Failed loggn       jessig (192.108.15.163)       Target: Vadministrator       LogonType 3         1       1176 2019 08-2	1	1167 2019-08-25 13:05:3	38.8928066	4625 Failed logon	jessie (192.168.15.158)	Target: \Administrator	LogonType 3	
1169/2019-09-25 13:05:41.0701353     44257-Failed (gogn)     jessige (192.168.15.160)     Target: Vadministrator     Logon7/bpc 3       117/2019-09-25 13:05:44.170623     44257-Failed (gogn)     jessige (192.168.15.160)     Target: Vadministrator     Logon7/bpc 3       117/2019-09-25 13:05:44.170623     44257-Failed (gogn)     jessige (192.168.15.160)     Target: Vadministrator     Logon7/bpc 3       117/2019-09-25 13:05:44.200548     44257-Failed (gogn)     jessige (192.168.15.160)     Target: Vadministrator     Logon7/bpc 3       117/32019-09-25 13:05:47.000683     44257-Failed (gogn)     jessige (192.168.15.162)     Target: Vadministrator     Logon7/bpc 3       117/32019-09-25 13:05:49.096964     44257-Failed (gogn)     jessige (192.168.15.162)     Target: Vadministrator     Logon7/bpc 3       117/32019-09-25 13:05:49.096964     44257-Failed (gogn)     jessige (192.168.15.162)     Target: Vadministrator     Logon7/bpc 3       117/32019-09-25 13:05:49.9665727     44257-Failed (gogn)     jessige (192.168.15.163)     Target: Vadministrator     Logon7/bpc 3       117/2019-09-25 13:05:49.375950     44255 Failed (gogn)     jessige (192.168.15.163)     Target: Vadministrator     Logon7/bpc 3       117/2019-09-25 13:05:49.375950     44255 Failed (gogn)     jessige (192.168.15.163)     Target: Vadministrator     Logon7/bpc 3       117/2019-09-25 13:05:49.3557576     44255 Failed (gogn)     jessige (192.168.15.163	5	1168 2019-08-25 13:05:4	40.7677175	4625 Failed logon	jessie (192.168.15.159)	Target: \Administrator	LogonType 3	
i     11702019-08-2513054.435501625     44625Failed (ggon)     jessigi (132.168.15.160)     Target: Vadministrator     Logon1ype 3       11712019-08-2513054.4127632     44625Failed (ggon)     jessigi (132.168.15.160)     Target: Vadministrator     Logon1ype 3       11722019-08-2513054.4127632     44625Failed (ggon)     jessigi (132.168.15.160)     Target: Vadministrator     Logon1ype 3       11722019-08-2513054.9     44625Failed (ggon)     jessigi (132.168.15.161)     Target: Vadministrator     Logon1ype 3       11723019-08-2513054.9     44625Failed (ggon)     jessigi (132.168.15.161)     Target: Vadministrator     Logon1ype 3       11742019-08-2513054.9     4625Failed (ggon)     jessigi (132.168.15.162)     Target: Vadministrator     Logon1ype 3       11762019-08-2513054.9     4625Failed (ggon)     jessigi (132.168.15.163)     Target: Vadministrator     Logon1ype 3       11762019-08-25130552.7557546     4625Failed (ggon)     jessigi (132.168.15.163)     Target: Vadministrator     Logon1ype 3       11762019-08-25130552.7557546     4625Failed (ggon)     jessigi (132.168.15.163)     Target: Vadministrator     Logon1ype 3       11762019-08-25130552.7557546     4625Failed (ggon)     jessigi (132.168.15.163)     Target: Vadministrator     Logon1ype 3       11762019-08-25130552.7557546     4625Failed (ggon)     jessigi (132.168.15.163)     Target: Vadministrator     Logon1ype 3   <	<u>1</u>	1169 2019-08-25 13:05:4	41.6701353	4625 Failed logon	jessie (192.168.15.159)	Target: \Administrator	LogonType 3	
11712019-08-25 13:05:44.078623     4625 Failed (ggon)     jessigi (192.168.15.16.)     Target: Vadministrator     Logon7ype 3       11722019-08-25 13:05:46.32504.14     4625 Failed (ggon)     jessigi (192.168.15.16.)     Target: Vadministrator     Logon7ype 3       11732019-08-25 13:05:47.2006683     4625 Failed (ggon)     jessigi (192.168.15.16.)     Target: Vadministrator     Logon7ype 3       11742019-08-25 13:05:49.0656727     4625 Failed (ggon)     jessigi (192.168.15.16.2)     Target: Vadministrator     Logon7ype 3       11752019-08-25 13:05:49.9656727     4625 Failed (ggon)     jessigi (192.168.15.16.2)     Target: Vadministrator     Logon7ype 3       11762019-08-25 13:05:49.9655727     4625 Failed (ggon)     jessigi (192.168.15.16.3)     Target: Vadministrator     Logon7ype 3       11762019-08-25 13:05:54.957564     4625 Failed (ggon)     jessigi (192.168.15.16.3)     Target: Vadministrator     Logon7ype 3       11772019-08-25 13:05:54.757564     4625 Failed (ggon)     jessigi (192.168.15.16.3)     Target: Vadministrator     Logon7ype 3	5	1170 2019-08-25 13:05:4	43.5501625	4625 Failed logon	jessie (192.168.15.160)	Target: VAdministrator	LogonType 3	
5     117220190-82513054.632520418     4625Falled (opgn)     jessge (192.108.15.161)     Target: Vadministrator     Logon/Type 3       117220190-82513054.7200868     4625Falled (opgn)     jessge (192.108.15.161)     Target: Vadministrator     Logon/Type 3       117420190-82513054.7200869     4625Falled (opgn)     jessge (192.108.15.161)     Target: Vadministrator     Logon/Type 3       117420190-82513054.9605727     4625Falled (opgn)     jessge (192.108.15.162)     Target: Vadministrator     Logon/Type 3       117620190-825130552.7557546     4625Falled (opgn)     jessge (192.108.15.163)     Target: Vadministrator     Logon/Type 3       117720190-825130552.7557546     4625Falled (opgn)     jessge (192.108.15.163)     Target: Vadministrator     Logon/Type 3       > N + tip2     tip2	1	1171 2019-08-25 13:05:4	44.4178623	4625 Failed logon	jessie (192.168.15.160)	Target: VAdministrator	LogonType 3	
1173/2019-08-25 13:0547.000663     4625 Failed (gggn)     jessige (132:168.15.162)     Target: Vadministrator     Logon/Type 3       1175/2019-08-25 13:0549.0009604     4625 Failed (gggn)     jessige (132:168.15.162)     Target: Vadministrator     Logon/Type 3       1175/2019-08-25 13:0549.0009604     4625 Failed (gggn)     jessige (132:168.15.162)     Target: Vadministrator     Logon/Type 3       1175/2019-08-25 13:0552.7557566     4625 Failed (gggn)     jessige (132:168.15.163)     Target: Vadministrator     Logon/Type 3       1177/2019-08-25 13:0552.7557566     4625 Failed (gggn)     jessige (132:168.15.163)     Target: Vadministrator     Logon/Type 3       > N +     tips2	5	1172 2019-08-25 13:05:4	46.3250418	4625 Failed logon	jessie (192.168.15.161)	Target: \Administrator	LogonType 3	
11/4/2019-08-25 13:05:49:0969994         4625-Failed (ggg)         jesses (132/168.15.162)         Target: Vadministrator         Logon/Type 3           11/75/2019-08-25 13:05:49:065727         4625-Failed (ggg)         jesses (132/168.15.162)         Target: Vadministrator         Logon/Type 3           11/75/2019-08-25 13:05:52         4625-Failed (ggg)         jesses (132/168.15.162)         Target: Vadministrator         Logon/Type 3           11/75/2019-08-25 13:05:52         4625-Failed (ggg)         jesses (132/168.15.163)         Target: Vadministrator         Logon/Type 3           11/75/2019-08-25 13:05:52         4625-Failed (ggg)         jesses (132/168.15.163)         Target: Vadministrator         Logon/Type 3           > N + tipz         tipz         tipz         tipz         tipz         tipz		1173 2019-08-25 13:05:4	47.2008683	4625 Failed logon	jessie (192.168.15.161)	Target: \Administrator	LogonType 3	
6     11/75/2019-08-25 13/05-49 sep5/27     44525-Failed (ggg)     jessge (192.168.15.163)     Target: Vadministrator     Logon/Type 3       6     11/77/2019-08-25 13/05-52.7557546     44525-Failed (ggg)     jessge (192.168.15.163)     Target: Vadministrator     Logon/Type 3       6     11/77/2019-08-25 13/05-52.7557546     44525-Failed (ggg)     jessge (192.168.15.163)     Target: Vadministrator     Logon/Type 3       ▶ N + tip2     tip2     11/72/2019-08-25 13/05-52.755746     4525-Failed (ggg)     jessge (192.168.15.163)     Target: Vadministrator     Logon/Type 3	1	1174 2019-08-25 13:05:4	49.0696984	4625 Failed logon	jessje (192.168.15.162)	Target: VAdministrator	LogonType 3	
I         I/r0/cut+us-cs.isx0>51.05/52/55764         4425 Failed logging         jessing (192.108.3.15.83)         Target: Vadministrator         LogginType 3           ▶ N         tips2         tip32	5	1175 2019-08-25 13:05:4	49.9655727	4625 Failed logon	jessie (192.168.15.162)	Target: VAdministrator	LogonType 3	
b 11/1/2/UH+VB-/513/0522/150/540 40/20 + alled igggr Jesse (1921168.15.163) Target V.dministrator Logon/Jype 3      H + tips2	1	1176 2019-08-25 13:05:5	51.8375920	4625 Failed logon	Jessie (192.168.15.163)	Target: VAdministrator	LogonType 3	
▶ H +		1177 2019-08-25 13:05:	52.7557546	4625 Falled logon	Jessie (192.168.15.163)	Target: VAdministrator	LogonType 3	
P P + tipsz				)				
	• H +	tips2						
Find 📃 💌 🖗 🧼 Find All 📄 Formatted Display 📄 Match Case 📿	Find	•	Find All	🛛 🗌 Formatted Display 🗌 Match	Case 📿			

※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。

tips2.c	sv - LibreOffice Calc					
File Ed	lit View Insert Format	She	et Data Tools Window	Help		
•			Insert Cells Insert Rows	Ctrl++ ,	3 🗭 Abc	
Libera	ition Sans 👻 10 😢		Insert Columns		💶 Columns Lef	🦁 - % (
A1	- 5 Σ =		Insert Page Break		📕 Columns Rig	ht
<u>La 16</u>	A		Delete Cells	Ctrl+-	L	0
1	RecordNumber TimeCre	-	Delete Rows		Description	RemoteHost
10745	1150 2019-08	-	Delete Columns		ed logon	jessie (192.168.15.150)
10760	1151 2019-08-		Delete Dage Break		ed logon	jessie (192.168.15.150)
10775	1152 2019-08-		Delete Page Bi eak		ed logon	jessie (192.168.15.151)
10790	1153 2019-08-		Insert Sheet		ed logon	jessie (192.168.15.151)
10805	1154 2019-08-		Incost Shoot at End		ed logon	jessie (192.168.15.152)
10820	1155 2019-08-		insert sheet at End		ed logon	jessie (192.168.15.152)
10835	1156 2019-08-		Insert Sheet from File		ed logon	jessie (192.168.15.153)
10850	1157 2019-08-		Link to External Data		ed logon	jessie (192.168.15.153)
10865	1158 2019-08-				ed logon	jessie (192.168.15.154)
10880	1159 2019-08-				ed logon	jessie (192.168.15.154)
10895	1160 2019-08-		Fill Cells		ed logon	jessie (192.168.15.155)
10910	1161 2019-08-		Named Ranges and Expres	sions +	ed logon	jessie (192.168.15.155)
10925	1162 2019-08-		Cycle Cell Reference Types	F4	ed logon	jessie (192.168.15.156)
10040	1162 2010 09	h			nd logon	ioccio (102 169 15 156)

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「O」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。

tips2.c	sv - Libre	Office Calc	
File Ed	it View	Insert Format Sheet Data Tools Windo	w I
<b>.</b>	PA • D	] · <b>/ E 6</b> · 4 <i>a</i>	
			91 C
Libera	tion Sans	• 10 • <b>a</b> <i>a</i> <u>a</u> · = ·	=
A1 (1	)	- ∰ Σ = FLAG	
6		B D	
1	FLAG	RecordNumber TimeCreated	TEN
10745	0	1150 2019-08-25 13:05:15.9657114	-
10760	0	1151 2019-08-25 13:05:16.7429072	
10775	0	1152 2019-08-25 13:05:18.6097675	
10790	0	1153 2019-08-25 13:05:19.4949230	
10805	0	1154 2019-08-25 13:05:21.3791111	
10820	0	1155 2019-08-25 13:05:22.2650057	
10835	0	1156 2019-08-25 13:05:24.1399874	
10850	0	1157 2019-08-25 13:05:25.0259744	
10865	0	1158 2019-08-25 13:05:26.9370864	
10880	0	1159 2019-08-25 13:05:27.8332851	
10895	0	1160 2019-08-25 13:05:29.7092373	
10910	0	1161 2019-08-25 13:05:30.5974981	
10925	0	1162 2019-08-25 13:05:32.4651358	
10940	0	1163 2019-08-25 13:05:33.3389419	
10955	0	1164 2019-08-25 13:05:35.2270506	
10970	0	1165 2019-08-25 13:05:36.1256355	
10985	0	1166 2019-08-25 13:05:37.9881252	
11001	0	1167 2019-08-25 13:05:38.8928066	
11016	0	1168 2019-08-25 13:05:40.7677175	
11031	0	1169 2019-08-25 13:05:41.6701353	
11046	0	1170 2019-08-25 13:05:43.5501625	
11061	0	1171 2019-08-25 13:05:44.4178623	
11076	0	1172 2019-08-25 13:05:46.3250418	
11091	0	1173 2019-08-25 13:05:47.2008683	
11111	0	1174 2019-08-25 13:05:49.0696984	
11126	0	1175 2019-08-25 13:05:49.9655727	
11141	0	1176 2019-08-25 13:05:51.8375920	
11156	0	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 192.168.15.150~192.1 68.15.180 であることがわかります。

🚽 - 📿 Abc 📖 -	■ • JA: JA: A 🔽	
	- 🐺 • % 0.0 🛐 '	00 00
M	P	T.
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	jessje (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	jessje (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
00F F 1 11	1 1000 400 45 400	-

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。

w Help		
( <b>6</b> ) • ( <b>2</b> )	- 🕵 🍫 🏢 - 📋	I •  \$A \$\$ }A ₹  ]
		🤜 - % 0.0 🛐 🖣
F	M	P
Fventid T		PemoteHost
4625	Interpretention	ie (192 168 15 150)
4625	Sort Ascending	ie (192,168,15,150)
4625	Sort Descending	ie (192,168,15,151)
4625	Top 10	ie (192,168,15,151)
4625	Franki	ie (192,168,15,152)
4625	Епірсу	ie (192.168.15.152)
4625	Not Empty	ie (192.168.15.153)
4625	Standard Filter	ie (192.168.15.153)
4625		ie (192.168.15.154)
4625	Search items	ie (192.168.15.154)
4625	bedreffternom	ie (192.168.15.155)
4625		, ie (192.168.15.155)
4625	Started execution	ol je (192.168.15.156)
4629	🛛 🗹 Successful logon	ie (192.168.15.156)
4625		ie (192.168.15.157)
4625		ie (192.168.15.157)
4625	The Event log serv	ic ie (192.168.15.158)
4625	The Event log serv	ic ie (192.168.15.158)
4625		- ie (192.168.15.159)
4625		ie (192.168.15.159)
4625		ie (192.168.15.160)
4625		ie (192.168.15.160)
499	OK Cance	ie (192.168.15.161)
4025	0-00	ie (192.168.15.161)
4625	Failed logon	jessie (192.168.15.162)
4625	Failed logon	jessje (192.168.15.162)

RecordNumber「1126」行、「8/25 12:47」付近の「RemoteHost」列を見るとIP アドレス「192.168.1
 5.131」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。

				= = .	= = = = = = = = = = = = = = = = = = = =			· = ···
952		▼ Ba L	-	-		1 -	-	
10.2	A	B	D	E	M	P	Q	R
03		1089	2019-08-25 12:41:07.1941937	4672	Administrative logon	0	SeassignPrimaryTokenPrivilege, ;	sercoprivilege, sesecurityprivi
00		1110	2019-08-25 12:44:22.2266990	4024	successiuliogon	(5)	Target: NTAUTHORITYSTSTEM	LogonType 5
1		1111	2019-08-25 12:44:22.2267065	4672	Administrative logon	()	SeassignPrimary TokenPrivilege, ;	sercoprivilege, sesecurityprivi
		1114	2019-08-25 12:44:22.2015908	4024	Successiunogon	(-)	Target: NTAUTHORITYSTSTEM	1 LogonType 5
2		1115	2019-08-25 12:44:22.2616035	4072	Administrative logon		SeassignPrimaryTokenPrivilege, ;	sercoprivilege, sesecurityPrivi
7		1125	2019-08-25 12:47:03.5868104	4072	Administrative logon	MIN 6021 MOMOK M2 (102 169 15 121)	SesecurityPhyliege, SeBackupPh	vilege, serestoreprivilege, ser
1		1120	2019-06-25 12:47:03.5606057	4024	Successiul logon	WIN-0550/MOM2KIN5 (192.100.15.151)	Target, WIN-34037QH71LIWumin	PLOUGHTYPE 3
4		1129	2019-06-25 12:47:04.9654123	4072	Auministrative logon	MIN 6021 MON2KM2 (102 169 15 121)	Terret MIN 240 170 H7T IN drain	Vilege, SerrestorePrivilege, Ser
2		1120	2019-00-25 12:47:04.9654610	4024	Successful logon	()	Target: Window Managord DM/M 2	LogonType 3
2		1132	2019-00-25 12:47:06 2378572	4024	Successful logon	()	Target: Window Manager DWM-2	LogonType 2
1		1124	2010-00-25 12:47:06 2279611	4024	Administrative logon	6	SaAssignDriman/TokanDrivilage	CoAuditDrivilage Colmonroom
		1134	2019-00-25 12:47:06 2378627	4072	Administrative logon		SeAssignPriman/TokenPrivilege	SeAuditPrivilege, Sempersonal
2	_	1139	2019-08-25 12:47:06 9548831	4672	Successful logon	WIN-340.170H7TLL (192.168.15.131)	Target: WIN-340.170H7TLI\Admin	el ogonType 10
3		1140	2019-08-25 12:47:06 9548883	4672	Administrative logon	(Louizoniania)	SeSecurityPrivilege SeTakeOwne	ershinPrivilege Sel oadDriverPr
4		1142	2019-08-25 12:47:07 7764835	4624	Successful logon	(-)	Target: Window Manager/DWM-3	LogonType 2
5		1143	2019-08-25 12:47:07 7764962	4624	Successful logon	8	Target: Window Manager/DWM-3	LogonType 2
5		1144	2019-08-25 12:47:07.7765001	4672	Administrative logon	0	SeAssignPrimaryTokenPrivilege.	SeAuditPrivilege, Selmpersonat
7		1145	2019-08-25 12:47:07.7765017	4672	Administrative logon		SeAssignPrimaryTokenPrivilege, S	SeAuditPrivilege
5	0	1150	2019-08-25 13:05:15.9657114	4625	Failed logon	jessje (192.168.15.150)	Target: \Administrator	LogonType 3
0	0	1151	2019-08-25 13:05:16.7429072	4625	Failed logon	jessie (192.168.15.150)	Target: \Administrator	LogonType 3
5	0	1152	2019-08-25 13:05:18.6097675	4625	Failed logon	jessje (192.168.15.151)	Target: \Administrator	LogonType 3
0	0	1153	2019-08-25 13:05:19.4949230	4625	Failed logon	jessie (192.168.15.151)	Target: \Administrator	LogonType 3
5	0	1154	2019-08-25 13:05:21.3791111	4625	Failed logon	jessje (192.168.15.152)	Target: \Administrator	LogonType 3
0	0	1155	2019-08-25 13:05:22.2650057	4625	Failed logon	jessie (192.168.15.152)	Target: \Administrator	LogonType 3
15	0	1156	2019-08-25 13:05:24.1399874	4625	Failed logon	jessie (192.168.15.153)	Target: \Administrator	LogonType 3
0	0	1157	2019-08-25 13:05:25.0259744	4625	Failed logon	jessie (192.168.15.153)	Target: \Administrator	LogonType 3
55	0	1158	2019-08-25 13:05:26.9370864	4625	Failed logon	jessie (192.168.15.154)	Target: \Administrator	LogonType 3
0	0	1159	2019-08-25 13:05:27.8332851	4625	Failed logon	jessie (192.168.15.154)	Target: \Administrator	LogonType 3
-	~	44.00				· / · · · · · · · · · · · · · · · · · ·	·······	

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「192.168.15.17
 1」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、「192.168.15.17
 1」からの試行時にログインに成功したと推測できます。

	7	-				10
398:AMJ1140	~ * 200 L	-				
A	B	U D	E M	P		R
291 0	1186	2019-08-25 13:06:05.5850536	4625 Failed logon	Jessie (192.168.15.168)	Target: VAdministrator	LogonType 3
00 0	1187	2019-08-25 13:06:06.48888801	4625 Failed logon	Jessie (192.108.15.108)	Target: vadministrator	LogonType 3
21 0	1188	2019-08-25 13:06:08.3456671	4625 Failed logon	Jessie (192.108.15.109)	Target: vAdministrator	LogonType 3
37 0	1189	2019-08-25 13:06:09.2061439	4625 Failed logon	Jessie (192.168.15.169)	Target: vadministrator	LogonType 3
52 0	1190	2019-08-25 13:06:11.0781100	4625 Failed logon	jessie (192.168.15.170)	Target: VAdministrator	LogonType 3
5/ 0	1191	2019-08-25 13:06:11.9470897	4625 Failed logon	Jessie (192.168.15.170)	Target: vadministrator	LogonType 3
82 0	1192	2019-08-25 13:06:13.8446455	4625 Failed logon	Jessie (192.168.15.171)	Target: VAdministrator	Logon1ype 3
18	1194	2019-08-25 13:06:14.7079711	4672 Administrative lodon	The second second second	SeSecurityPrivilege, SeBackupPri	vilege, SeRestorePrivilege, Sel
99	1195	2019-08-25 13:06:14.7080430	4624 Successful logon	lessie (192.168.15.171)	Target: WIN-340J7QH71LIVAdmin	LogonType 3
51	1198	2019-08-25 13:06:14.9702285	4624 Successful logon	(-)	Target: window Manager\DvvM-2	LogonType 2
2	1199	2019-08-25 13:06:14.9702561	4624 Successful logon	(-)	Target: Window Manager\DWM-2	LogonType 2
3	1200	2019-08-25 13:06:14.9702613	4672 Administrative logon		SeAssignPrimaryTokenPrivilege,	SeAuditPrivilege, Selmpersonal
64	1201	2019-08-25 13:06:14.9702632	4672 Administrative logon		SeAssignPrimaryTokenPrivilege,	SeAuditPrivilege
5 0	1204	2019-08-25 13:00:16:5860815	4025 Failed logon	jessie (192.108.15.172)	Target: vadministrator	LogonType 3
0 0	1205	2019-08-25 13:06:17.4399881	4625 Failed logon	Jessie (192.168.15.172)	Target: vAdministrator	LogonType 3
05 O	1206	2019-08-25 13:06:19.3292388	4625 Failed logon	Jessie (192.168.15.173)	Target: VAdministrator	LogonType 3
20 0	1207	2019-08-25 13:06:20.1955014	4625 Failed logon	jessie (192.168.15.173)	Target: VAdministrator	LogonType 3
35 O	1208	2019-08-25 13:06:22.0752805	4625 Failed logon	jessie (192.168.15.174)	Target: VAdministrator	LogonType 3
0 0	1209	2019-08-25 13:06:22.9304532	4625 Failed logon	jessie (192.168.15.174)	Target: VAdministrator	LogonType 3
5 O	1210	2019-08-25 13:06:24.8150249	4625 Failed logon	jessie (192.168.15.175)	Target: VAdministrator	LogonType 3
38 O	1211	2019-08-25 13:06:25.6872619	4625 Failed logon	jessje (192.168.15.175)	Target: \Administrator	LogonType 3
)3 O	1212	2019-08-25 13:06:27.5631889	4625 Failed logon	jessie (192.168.15.176)	Target: VAdministrator	LogonType 3
18 O	1213	2019-08-25 13:06:28.4166569	4625 Failed logon	jessie (192.168.15.176)	Target: VAdministrator	LogonType 3
33 O	1214	2019-08-25 13:06:30.2902514	4625 Failed logon	jessie (192.168.15.177)	Target: \Administrator	LogonType 3
18 O	1215	2019-08-25 13:06:31.1660341	4625 Failed logon	jessje (192.168.15.177)	Target: \Administrator	LogonType 3
53 O	1216	2019-08-25 13:06:33.0441338	4625 Failed logon	jessie (192.168.15.178)	Target: \Administrator	LogonType 3
78 O	1217	2019-08-25 13:06:33.9040592	4625 Failed logon	jessie (192.168.15.178)	Target: \Administrator	LogonType 3
93 O	1218	2019-08-25 13:06:35.7940760	4625 Failed logon	jessie (192.168.15.179)	Target: VAdministrator	LogonType 3
08 0	1219	2019-08-25 13:06:36.6486620	4625 Failed logon	jessję (192.168.15.179)	Target: \Administrator	LogonType 3
-	4.000		toole 3 11		la Tana Ara a	

14. この行の FLAG 列に「●」を入力してください。

	dottile	* 10		<b>e e e e e</b> e e e	% 0.0 🖸 🐝 -			
398:A	11464	- 5π Σ	= •	1				
	A	В	D	E M	P	Q	R	
61	0	1184	2019-08-25 13:06:02.8505698	4625 Failed logon	jessie (192.168.15.167)	Target: VAdministrator	LogonType 3	_
76	0	1185	2019-08-25 13:06:03.7189250	4625 Failed logon	jessie (192.168.15.167)	Target: VAdministrator	LogonType 3	
91	0	1186	2019-08-25 13:06:05.5850536	4625 Failed logon	jessie (192.168.15.168)	Target: VAdministrator	LogonType 3	
06	0	1187	2019-08-25 13:06:06.4888801	4625 Failed logon	jessie (192.168.15.168)	Target: VAdministrator	LogonType 3	
21	0	1188	2019-08-25 13:06:08.3456671	4625 Failed logon	jessie (192.168.15.169)	Target: \Administrator	LogonType 3	_
37	0	1189	2019-08-25 13:06:09.2061439	4625 Failed logon	jessie (192.168.15.169)	Target: VAdministrator	LogonType 3	
52	0	1190	2019-08-25 13:06:11.0781100	4625 Failed logon	jessie (192.168.15.170)	Target: VAdministrator	LogonType 3	
5	0	1191	2019-08-25 13:06:11.9470897	4625 Failed logon	jessie (192.168.15.170)	Target: VAdministrator	LogonType 3	
2	0	1192	2019-08-25 13:06:13.8446455	4625 Failed logon	jessie (192.168.15.171)	Target: \Administrator	LogonType 3	
8		1194	2019-08-25 13:06:14.7079711	4672 Administrative logon		SeSecurityPrivilege, SeBack	upPrivilege, SeRestorePrivileg	ge, SeT
9		1195	2019-08-25 13:06:14.7080430	4624 Successful logon	jessie (192.168.15.171)	Target: WIN-34OJ7QH7TLIV	dmini+LogonType 3	
1	۲	1198	2019-08-25 13:06:14.9702285	4624 Successful logon	(-)	Target: Window Manager\DW	M-2 LogonType 2	
2		1199	2019-08-25 13:06:14.9702561	4624 Successful logon	(-)	Target: Window Manager\DW	M-2 LogonType 2	
3	٠	1200	2019-08-25 13:06:14.9702613	4672 Administrative logon		SeAssignPrimaryTokenPrivile	ege, SeAuditPrivilege, SeImpe	ersonate
4	•	1201	2019-08-25 13:06:14.9702632	4672 Administrative logon		SeAssignPrimaryTokenPrivile	ege, SeAuditPrivilege	
5	0	1204	2019-08-25 13:06:16.5860815	4625 Failed logon	jessie (192.168.15.172)	Target: VAdministrator	LogonType 3	
0	0	1205	2019-08-25 13:06:17.4399881	4625 Failed logon	jessie (192.168.15.172)	Target: VAdministrator	LogonType 3	
5	0	1206	2019-08-25 13:06:19.3292388	4625 Failed logon	jessie (192.168.15.173)	Target: \Administrator	LogonType 3	
0	0	1207	2019-08-25 13:06:20.1955014	4625 Failed logon	jessie (192.168.15.173)	Target: VAdministrator	LogonType 3	
5	0	1208	2019-08-25 13:06:22.0752805	4625 Failed logon	jessje (192.168.15.174)	Target: \Administrator	LogonType 3	
0	0	1209	2019-08-25 13:06:22.9304532	4625 Failed logon	jessie (192.168.15.174)	Target: \Administrator	LogonType 3	
5	0	1210	2019-08-25 13:06:24.8150249	4625 Failed logon	jessje (192.168.15.175)	Target: VAdministrator	LogonType 3	
8	0	1211	2019-08-25 13:06:25.6872619	4625 Failed logon	jessie (192.168.15.175)	Target: \Administrator	LogonType 3	
3	0	1212	2019-08-25 13:06:27.5631889	4625 Failed logon	jessie (192.168.15.176)	Target: \Administrator	LogonType 3	
8	0	1213	2019-08-25 13:06:28.4166569	4625 Failed logon	jessje (192.168.15.176)	Target: VAdministrator	LogonType 3	
3	0	1214	2019-08-25 13:06:30.2902514	4625 Failed logon	jessie (192.168.15.177)	Target: \Administrator	LogonType 3	
8	0	1215	2019-08-25 13:06:31.1660341	4625 Failed logon	jessje (192.168.15.177)	Target: VAdministrator	LogonType 3	
3	0	1216	2019-08-25 13:06:33.0441338	4625 Failed logon	jessie (192.168.15.178)	Target: VAdministrator	LogonType 3	
8	0	1217	2019-08-25 13:06:33.9040592	4625 Failed logon	jessie (192.168.15.178)	Target: VAdministrator	LogonType 3	
	~	4040		1000 E 1 1		le Transformer		11

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。

bergen	on Sans	* 10	- a u	₫ 🚨	• 💻 •	= = .	= =	) 🖽 🗆 🖻	E 😵	- % 0.0	00 -0	<u>&gt;= &lt;=  </u>	H • 117 • 1	• 8	· 😑 🎹	
793:AN	4J11793	- 5π Σ	=													
	A	В		Ð		E		M		P			Q		R	
35	0	1208	2019-08-25 1	3:06:22.0	)752805	4625	Failed	ogon	jessie (192	2.168.15.174)		Target: V	Administrator		LogonType 3	_
50	0	1209	2019-08-25 1	L3:06:22.9	304532	4625	5 Failed	ogon	jessie (192	2.168.15.174)		Target: V	Administrator		LogonType 3	_
55	0	1210	2019-08-25 1	13:06:24.8	3150249	4625	5 Failed	ogon	jessie (192	2.168.15.175)		Target: V	Administrator		LogonType 3	
38	0	1211	2019-08-25 1	13:06:25.6	3872619	4625	5 Failed	ogon	jessie (192	2.168.15.175)		Target: V	Administrator		LogonType 3	_
)3	0	1212	2019-08-25 1	13:06:27.5	631889	4625	5 Failed	ogon	jessie (192	2.168.15.176)		Target: V	Administrator		LogonType 3	
8	0	1213	2019-08-25 1	13:06:28.4	1166569	4625	5 Failed	ogon	jessie (192	2.168.15.176)		Target: V	Administrator		LogonType 3	
3	0	1214	2019-08-25 1	13:06:30.2	2902514	4625	5 Failed	ogon	jessie (192	2.168.15.177)		Target: V	Administrator		LogonType 3	
8	0	1215	2019-08-25 1	13:06:31.1	1660341	4625	5 Failed	ogon	jessie (192	2.168.15.177)		Target: V	Administrator		LogonType 3	
3	0	1216	2019-08-25 1	13:06:33.0	)441338	4625	5 Failed	ogon	jessie (192	2.168.15.178)		Target: V	Administrator		LogonType 3	
8	0	1217	2019-08-25 1	13:06:33.9	+040592	4625	5 Failed	ogon	jessie (192	2.168.15.178)		Target: V	Administrator		LogonType 3	
13	0	1218	2019-08-25 1	13:06:35.7	/940760	4625	5 Failed	ogon	jessie (192	2.168.15.179)		Target: V	Administrator		LogonType 3	
8	0	1219	2019-08-25 1	13:06:36.6	\$486620	4625	5 Failed	ogon	jessie (192	2.168.15.179)		Target: V	Administrator		LogonType 3	
3	0	1220	2019-08-25 1	13:06:38.5	5222115	4625	5 Failed I	ogon	jessie (192	2.168.15.180)		Target: V	Administrator		LogonType 3	
9	0	1221	2019-08-25 1	13:06:39.4	4045261	4625	Failed	ogon	jessię (192	2.168.15.180)		Target: V	Administrator		LogonType 3	
2		1223	2019-08-25 1	13:20:23.1	141285	4672	2 Admini	strative logon				SeSecur	ityPrivilege, Se	BackupPrivi	lege, SeRestorePrivilege	, SeT
3	•	1224	2019-08-25 1	3:20:23.1	142320	4624	1 Succes	ssful logon	jessie (192	2.168.15.10)		Target: V	VIN-340J7QH	7TLI\Admini*	LogonType 3	
9	~	1226	2019-08-25 1	13:20:23.3	3844815	4624	Succes	ssful logon	(-)			Target: V	Vindow Manag	er\DWM-2	LogonType 2	
0	(1)	1227	2019-08-25 1	13:20:23.3	\$845266	4624	1 Succes	ssful logon	(-)			Target: V	Vindow Manag	er\DWM-2	LogonType 2	
1		1228	2019-08-25 1	13:20:23.3	3845451	4672	2 Admini:	strative logon				SeAssig	nPrimaryToker	Privilege, Se	eAuditPrivilege, Selmpers	sonati
2		1229	2019-08-25 1	13:20:23.3	3845467	4672	2 Admini:	strative logon				SeAssig	<b>PrimaryToker</b>	Privilege, Se	eAuditPrivilege	
8		1233	2019-08-25 1	13:20:23.8	3848525	4624	1 Succes	ssful logon	WIN-340.	17QH7TLI (192	2.168.15.10)	Target: V	VIN-340J7QH	7TLI\Admini	LogonType 10	
9		1234	2019-08-25 1	13:20:23.8	3848585	4672	2 Adminis	strative logon				SeSecur	ityPrivilege, Se	TakeOwner	shipPrivilege, SeLoadDriv	verPr
1	0	1238	2019-08-25 1	13:21:55.5	5264316	4625	Failed	ogon	- (-)			Target: -	r		LogonType 5	
2	0	1239	2019-08-25 1	13:21:55.5	5271506	4625	5 Failed	ogon	- (-)			Target: -	F <sup>2</sup>		LogonType 5	
2		1245	2019-08-25 1	13:39:50.8	3184141	4624	Succes	ssful logon	WIN-3403	17QH7TLI (127	7.0.0.1)	Target: V	VIN-340J7QH	7TLI\Admini	LogonType 2	
3		1246	2019-08-25 1	13:39:50.8	3184213	4672	2 Admini:	strative logon				SeSecur	ityPrivilege, Se	TakeOwner	shipPrivilege, SeLoadDriv	verPr
0		1252	2019-08-25 1	13:41:26.0	)326798	4624	1 Succes	ssful logon	(-)			Target: N	IT AUTHORIT	Y\SYSTEM	LogonType 5	
1		1253	2019-08-25 1	13:41:26.0	326870	4672	Admini:	strative logon				SeAssig	nPrimaryToker	Privilege, Se	eTcbPrivilege, SeSecurity	vPrivi
25																- L.
· ·																× 1
	alle Fi	ne2														

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「Shee t」→「Insert Columns」→「Columns Left」を選択してください。

tips2.csv -	LibreOffice Ca	K CRO										-	- • ×
	View Insert	For hac S	iheet Data Tools W	indow Help									×
			Insert Cells	Ctrl++	Abc	-		-			7	_	_
•••	· 🖬 · 🤘	10 M	Insert Rows	Contraction of the			ar i 🕸 i an 😿	) 🖾 🔽 🚺	M ≈ 🖻 🗖	La 🖽 • 🖮 🧯	16. 1		
Liberation	Sans = 10	<b>M</b>	Insert Columns		Columns Left		- % 0.0 131		= = 📖 - 🗁 -	🗖 · 🚍 · 🔤	en l		
Liberation		<b>W</b>	Insert Columns		Columna Dia		/0 0.0 [3]	-00 <b>-</b> 0 🖴					
M1	- <b>5</b>	$\Sigma = 1$	Inserc Page Break		Columns Rig	nt							-
A	В		Delete Cells	Ctrl+-	м		Р		0		R	-	
FLAG	RecordNum	TimeCr	Delete Rows		Description	RemoteHost		ΨP	avloadData1	▼ PavloadData	a2 Pi	avlo	2
371	14	2019-01	Delete Columns		ccessful logon	- (-)		Т	arget: NT AUTHORITY\	SYSTEM LogonType	0	- 9	60
409	51	2019-0	Delete Break		ccessful logon	(-)		Ti	arget: NT AUTHORITY\	SYSTEM LogonType	5		T
410	52	2019-0	Delece Page Break		ministrative logon			S	eAssignPrimaryTokenP	rivilege, SeTcbPrivileg	e, SeSecurityPrivi	lege	
414	53	2019-01	Insert Sheet		ccessful logon	(-)		T	arget: NT AUTHORITY\	NETWOR LogonType	5		
415	54	2019-0	Insert Sheet at End.		ministrative logon			S	eAssignPrimaryTokenP	rivilege, SeAuditPrivile	ge, Selmpersonate	ePri	-
429	56	2019-0	Incert Sheet from Fil	•	ccessful logon	(-)		T	arget: Window Manager	DWM-1 LogonType	2		$\odot$
430	57	2019-0	Link to External Date		ccessful logon	(-)		т	arget: Window Manager	DWM-1 LogonType	2		
431	58	2019-00	Link to External Data	••••	ministrative logon			S	eAssignPrimaryTokenP	rivilege, SeAuditPrivile	ge, Selmpersonate	ePrr	870
432	59	2019-00	Delece Sheet		ministrative logon	0		2	eAssignPrimary TokenP	rivilege, SeAuditPrivile	ge		
433	60	2019-08	Fill Cells		ccessful logon	(-)		10	arget: NTAUTHORITY	LOCAL SELOGONTYPE	D Colorado a	. Dei	
434	62	2019-00	Named Pandes and I	- voressions	ministrative logon	()		2	PASSIGNPHIMARY TOKENP	EVETEM LogonTune	ge, Seimpersonau	PIL	
433	63	2019-00	Curle Cell Reference	Trans Ed	ministrative logon	()		9	eAssignPriman/TokenP	rivilege SetchPrivileg	e SeSecurityPrivi	lene	
456	64	2019-01		types 14	ccessful logon	(-)		T	arget: NT AUTHORITY\	SYSTEM LogonType	5	1×9×	
457	65	2019-01	Cell Comments		ministrative logon	0		S	AssignPrimaryTokenP	rivilege, SeTcbPrivileg	e. SeSecurityPrivi	leae	
463	66	2019-0	3 Clear Cells	BackSpace	ccessful logon	(-)		Ť	arget: NT AUTHORITY\	SYSTEM LogonType	5	CAR .	4
464	67	2019-01			ministrative logon	.,		S	eAssignPrimaryTokenP	rivilege, SeTcbPrivileg	e, SeSecurityPrivi	lege	
511	84	2019-0	Move of Copy sheet.		ccessful logon	(-)		Ti	arget: NT AUTHORITY\	SYSTEM LogonType	5		
512	85	2019-0	Rename Sheet		ministrative logon			S	eAssignPrimaryTokenP	rivilege, SeTcbPrivileg	e, SeSecurityPrivi	lege	
522	86	2019-0			ccessful logon	(-)		Ta	arget: NT AUTHORITY\	SYSTEM LogonType	5		
523	87	2019-00			ministrative logon			S	eAssignPrimaryTokenP	rivilege, SeTcbPrivileg	e, SeSecurityPrivi	lege	
566	89	2019-00			ccessful logon	(-)		Ti	arget: NT AUTHORITY\	SYSTEM LogonType	5		
567	90	2019-0	To Previous Sheet	Ctri+PgUp	ministrative logon			S	eAssignPrimaryTokenP	rivilege, SeTcbPrivileg	e, SeSecurityPrivi	lege	
570	91	2019-00	To Next Sheet	Ctrl+PgDn	ccessful logon	(-)		T	arget: NT AUTHORITY	SYSTEM LogonType	5		
571	92	2019-00	Select Sheets		ministrative logon	()		S	eAssignPrimaryTokenP	rivilege, SeTcbPrivileg	e, SeSecurityPrivi	lege	
5/3	93	2019-0	Sheet Tab Color		ccessiul logon	(-)		T	arget: NT AUTHORITY	SYSIEM LogonType		1	
5/4	94	2019-08	Choot Events		ministrative logon	()		2	eassignerimary rokene	nvilege, sercoprivileg	e, sesecuntyPhyl	lege	
575	95	2019-00	Diable To Loft		ccessiuriogon	(-)		10	arget: NT AUTHORITY	SYSTEM LODONTYPE	0 0 0 0 0 0		
	de tips2	_	Righteroscerc									-1	
X Find			Find All	Formatted I	Display 🗍 Match C	ase 📿							
Sheet 1 of 1		331 of 121	123 records found		Default		at D.		Average: - Sum: I	1		- 4	110%
and the Fort		00101121			Der dow		1.441 1.444	~	Averuger, Suite		1	- T.	. 1070
			👔 🔄 [cain 👋 [ca	in 🦲 tip:	52 🞽 caine	🗈 tips2 🎽	- iii 🔔 🐠 🛛	🔣 木 9月	19, 01:10 💼 🗸 0 B/s	- 36 B/s			

17. 一列目に「LogonID」と入力してください。

Calc		
Format Sheet Data Tools V	vindow Help	
📶 🕞 🔯 👗 🗛 🛍 · 🌛	🤹 🥱 • 🐡 •	🕵 😼 🖽 • 🖽 • 🕼 🕹
• • <b>a</b> <i>a</i> <u>a</u> • =	· = = = =	5 🖮 E E E 🐺 • % 0
r Σ = LogonID		
D	E V	1 N
TimeCreated	Eventid  LogonID	MapDescription
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。

ips2.csv - LibreOffice Calc <sup>1</sup> A
e Edit View Insert Format Sheet Data Tools Window Help
📓 • 🛅 • 🛃 • I 🗶 👦 🔯 🐇 🐏 💼 • I 🐊 ⊈ 🖘 • 🛷 • I 🛠 🂖 I 🏛 • 🎚 • I 🕼 🐼 🏠 🐼 🖉 🖉 🖉 🖉 🖉 🖉 🖉 🖉
uberation Sans 🝷 10 💌 🛎 🖉 🧧 🖳 🗧 🚍 🗮 🗧 🚍 🖮 🗉 🖃 🚽 🦁 • % 0.0 🔯 🎭 📰 🖅 🔚 • 🦷 • 🕞 • 🗮 • 🗮
Understands
Find V Match Case V
eet 1 of 1         331 of 12123 records found         Default         mt         E         Average; Sum: 0        c+         1109
🕎 🕙 👕 🗑 📶 🔍 📑 🔏 🔍 [cain 🔍 [cain 🗋 bips2 🔍 caine 🖹 tips2 🖉 🖉 🚔 🌆 💭 🎼 🛧 9月 19,01:17 🖬 0.05/s 🛛 36.0/s

L         E           2019-08-25         13:062         5:687.2619           2019-08-25         13:062         5:681.889           2019-08-25         13:063         10:062           1         2019-08-25         13:063         10:063           1         2019-08-25         13:063         3:04038           2019-08-25         13:063         3:040592         10:02           2019-08-25         13:063         3:040592         10:02           2019-08-25         13:063         3:040592         10:02           2019-08-25         13:063         3:040592         10:02           2019-08-25         13:063         3:040592         10:02           2019-08-25         13:063         4:040591         10:01           2019-08-25         13:063         4:040591         10:01         10:01           2019-08-25         13:063         4:04591         10:01         10:01         10:01           2019-08-25         13:063         10:02         10:02         10:02         10:02         10:02         10:02         10:02         10:02         10:02         10:02         10:02         10:02         10:02         10:02         10:02         10:02         <	E M 4625 4625 4625 4625 4625 4625 4625 4625	N Failed logon Failed logon	essie (192.168.15.175)           essie (192.168.15.176)           essie (192.168.15.177)           essie (192.168.15.177)           essie (192.168.15.177)           essie (192.168.15.178)           essie (192.168.15.178)           essie (192.168.15.178)           essie (192.168.15.178)           essie (192.168.15.178)           essie (192.168.15.179)           essie (192.168.15.179)           essie (192.168.15.179)           essie (192.168.15.179)	R Target: Wdministrator Target: Wdministrator Target: Wdministrator Target: Wdministrator Target: Wdministrator Target: Wdministrator Target: Wdministrator Target: Wdministrator Target: Wdministrator	LogonTyr LogonTyr LogonTyr LogonTyr LogonTyr LogonTyr LogonTyr LogonTyr LogonTyr
2019-08-25 13:06-25.6872619 2019-08-25 13:06:27.563189 2019-08-25 13:06:28.4166569 2019-08-25 13:06:33.062341 2019-08-25 13:06:33.1660341 2019-08-25 13:06:33.046318 2019-08-25 13:06:33.040592 2019-08-25 13:06:35.7940760 2019-08-25 13:06:36.846620 2019-08-25 13:06:36.846620 2019-08-25 13:06:38.4045261 2019-08-25 13:06:38.4045261 2019-08-25 13:06:23.114230	4625 4625 4625 4625 4625 4625 4625 4625	Failed logon Failed logon	essie         (192.160.15.175)           gesse         (192.160.15.176)           gesse         (192.160.15.176)           gesse         (192.160.15.177)	Target: Vadministrator Target: Vadministrator Target: Vadministrator Target: Vadministrator Target: Vadministrator Target: Vadministrator Target: Vadministrator Target: Vadministrator Target: Vadministrator	LogonTyr LogonTyr LogonTyr LogonTyr LogonTyr LogonTyr LogonTyr LogonTyr
2 2019-09-25 13:00:27 5531809 2 2019-09-25 13:00:28 446559 4 2019-09-25 13:06:38 146559 4 2019-09-25 13:06:33 146338 4 2019-09-25 13:06:33 146338 4 2019-09-25 13:06:33 046578 4 2019-09-25 13:06:35 5740/700 2 2019-09-25 13:06:35 5740/700 2 2019-09-25 13:06:38 5520175 2 2019-09-25 13:06:38 4465201 2 2019-09-25 13:06:38 04465201 2 2019-09-25 13:06:38 1465201 2 2019-09-25 13:07.02 31 142/320	4625 4625 4625 4625 4625 4625 4625 4625	Failed [990] Failed [990] Failed [990] Failed [990] Failed [990] Failed [990] Failed [990] Failed [990] Failed [990] Failed [990]	Image: Section 2.1         Section 2.1 <td>Target: Valministrator Target: Valministrator Target: Valministrator Target: Valministrator Target: Valministrator Target: Valministrator Target: Valministrator Target: Valministrator Target: Valministrator</td> <td>LogonTyr LogonTyr LogonTyr LogonTyr LogonTyr LogonTyr LogonTyr</td>	Target: Valministrator Target: Valministrator Target: Valministrator Target: Valministrator Target: Valministrator Target: Valministrator Target: Valministrator Target: Valministrator Target: Valministrator	LogonTyr LogonTyr LogonTyr LogonTyr LogonTyr LogonTyr LogonTyr
2019-08-25 13:06:22 #146559           2019-08-25 13:06:30.2902514           2019-08-25 13:06:30.2902514           2019-08-25 13:06:33.160331           2019-08-25 13:06:33.0441338           2019-08-25 13:06:33.044591           2019-08-25 13:06:33.044592           2019-08-25 13:06:33.044591           2019-08-25 13:06:33.044591           2019-08-25 13:06:36.3648620           2019-08-25 13:06:36.3648620           2019-08-25 13:06:37.241741282           2019-08-25 13:06:37.21141282           2019-08-25 13:07.23.1142320	4625 4625 4625 4625 4625 4625 4625 4625	Failed logon Failed logon Failed logon Failed logon Failed logon Failed logon Failed logon Failed logon Failed logon Failed logon	Jessie (192,168,15,176)           Jessie (192,168,15,177)           Jessie (192,168,15,177)           Jessie (192,168,15,177)           Jessie (192,168,15,178)	Target: Vadministrator Target: Vadministrator Target: Vadministrator Target: Vadministrator Target: Vadministrator Target: Vadministrator Target: Vadministrator	LogonTyr LogonTyr LogonTyr LogonTyr LogonTyr LogonTyr
2019-08-25 13:06:30 2902514 2019-08-25 13:06:33 1.660341 2019-08-25 13:06:33 0.441338 2019-08-25 13:06:33 0.441338 2019-08-25 13:06:33 0.940592 2019-08-25 13:06:33 6.446620 2019-08-25 13:06:33 6.464620 2019-08-25 13:06:33 0.445261 2019-08-25 13:06:33 0.445261 2019-08-25 13:06:33 1.44230	4625 4625 4625 4625 4625 4625 4625 4625	Failed (ggon Failed (ggon Failed (ggon Failed (ggon Failed (ggon Failed (ggon Failed (ggon Failed (ggon Failed (ggon Failed (ggon	jessje (192.168.15.177) jessje (192.168.15.177) jessje (192.168.15.177) jessje (192.168.15.178) jessje (192.168.15.178) jessje (192.168.15.179) jessje (192.168.15.179) jessje (192.168.15.179)	Target: Vadiministrator Target: Vadiministrator Target: Vadiministrator Target: Vadiministrator Target: Vadiministrator Target: Vadiministrator	LogonTyr LogonTyr LogonTyr LogonTyr LogonTyr
2019-09-25 13:00:33.1.660:341 2019-09-25 13:00:33.1.660:341 2019-09-25 13:00:33.004:592 2019-09-25 13:00:33.004:592 2019-09-25 13:00:36.30:045920 2019-09-25 13:00:36.4646620 2019-09-25 13:00:36.30:462501 2019-09-25 13:00:33.0045201 2019-09-25 13:00:33.11412820	4625 4625 4625 4625 4625 4625 4625 4625	Failed logon Failed logon Failed logon Failed logon Failed logon Failed logon Failed logon	jessje (192.168.15.177) jessje (192.168.15.177) jessje (192.168.15.178) jessje (192.168.15.178) jessje (192.168.15.179) jessje (192.168.15.179)	Target: Vadministrator Target: Vadministrator Target: Vadministrator Target: Vadministrator Target: Vadministrator Target: Vadministrator	LogonTyr LogonTyr LogonTyr LogonTyr
2019-08-25 13:06:33:0441338 2019-08-25 13:06:33:9040592 2019-08-25 13:06:35:9040590 2019-08-25 13:06:35:7940760 2019-08-25 13:06:36:6486620 2019-08-25 13:06:38:4045261 2019-08-25 13:20:33:4045261 2019-08-25 13:20:23 11412820	4625 4625 4625 4625 4625 4625 4625	Failed logon Failed logon Failed logon Failed logon Failed logon Failed logon	essie (192.168.15.178) jessie (192.168.15.178) jessie (192.168.15.178) jessie (192.168.15.179) jessie (192.168.15.179) jessie (192.168.15.180)	Target: Vadministrator Target: Vadministrator Target: Vadministrator Target: Vadministrator Target: Vadministrator	LogonTyr LogonTyr LogonTyr
2019-08-25 13:06:33.9040592 2019-08-25 13:06:35.9940592 2019-08-25 13:06:35.7940760 2019-08-25 13:06:36.6486620 2019-08-25 13:06:39.4045261 2019-08-25 13:20:23 1141285 2019-08-25 13:20:23 1141285	4625 4625 4625 4625 4625 4625	Failed logon Failed logon Failed logon Failed logon Failed logon	jessje (132.168.15.178) jessje (192.168.15.178) jessje (192.168.15.179) jessje (192.168.15.179)	Target: Vadministrator Target: Vadministrator Target: Vadministrator Target: Vadministrator	LogonTyr
2019-08-25 13:06:35.7940760 2019-08-25 13:06:35.7940760 2019-08-25 13:06:36.6486620 2019-08-25 13:06:38.5222115 2019-08-25 13:06:39.4045261 2019-08-25 13:20:23 1142285 2019-08-25 13:20:23 1142285	4625 4625 4625 4625 4625	Failed logon Failed logon Failed logon Failed logon	jessie (192.168.15.179) jessie (192.168.15.179) jessie (192.168.15.179)	Target: VAdministrator Target: VAdministrator	LogonTyr
2019-08-25 13:06:36.6486620 2019-08-25 13:06:38.6222115 2019-08-25 13:06:38.4045261 2019-08-25 13:20:23 1141285 2019-08-25 13:20:23 1141285	4625 4625 4625 4625	Failed logon Failed logon	jessje (192.168.15.179) jessje (192.168.15.179)	Target: VAdministrator	Logoniy
2019-08-25 13:06:38.5222115 2019-08-25 13:06:38.5222115 2019-08-25 13:06:39.4045261 2019-08-25 13:20:23 1141285 2019-08-25 13:20:23 1142320	4625 4625	Failed logon	jessie (192,168,15,180)	rage. Marinistator	LogonTvr
2019-08-25 13:06:39.4045261 2019-08-25 13:20:23 1141285 2019-08-25 13:20:23 114285	4625	Failed logon		Target: \Administrator	LogonTyr
2019-08-25 13:20:23.1141285 2019-08-25 13:20:23.1141285 2019-08-25 13:20:23.1142320	4020		jessie (192 168 15 180)	Target: \Administrator	LogonTyr
2019-08-25 13:20:23 1142320	46/2	Administrative locon	(132.100.13.100)	SeSecurityPrivilege SeBackunPriv	ilege SeP
	4624 0x46EB32	Successful logon	jessie (192 168 15 10)	Target: M/M-34O 17OH7TI //Admini	LogonTyr
2019-08-25 13:20:23 3844815	4624	Successful logon	(-)	Target: Window Manager\DW/M-2	LogonTyr
2019-08-25 13:20:23 3845266	4624	Successful logon	(-)	Target: Window Manager\DWM-2	LogonTyr
2019-08-25 13:20:23 3845451	4672	Administrative logon	0	SeAssignPrimaryTokenPrivilege S	eAuditPriv
2019-08-25 13:20:23 3845467	4672	Administrative logon		SeAssignPrimaryTokenPrivilege S	eAuditPriv
2019-08-25 13:20:23 8848525	4624	Successful logon	WIN-340,170H7TLL (192 168 15 10)	Target: WIN-340.170H7TLI\Admini	LogonTyr
2019-08-25 13:20:23.8848585	4672	Administrative logon		SeSecurityPrivilege, SeTakeOwner	shipPrivile
2019-08-25 13:21:55 5264316	4625	Failed logon	- (-)	Target: -)-	LogonTyr
2019-08-25 13:21:55 5271506	4625	Failed logon	- (-)	Target: -\-	LogonTyr
2019-08-25 13:39:50 8184141	4624	Successful logon	WIN-340.170H7TLL(127.0.0.1)	Target: WIN-340.170H7TLI\Adminit	LogonTyr
2019-08-25 13:39:50 8184213	4672	Administrative logon		SeSecurityPrivilege_SeTakeOwner	shipPrivile
2019-08-25 13:41:26 0326798	4624	Successful logon	(-)	Target: NT AUTHORITY/SYSTEM	LogonTyr
2019-08-25 13:41:26 0326870	4672	Administrative logon		SeAssignPrimaryTokenPrivilege S	eTchPrivil
	TOTE				
					1
	2019-08-25 13:20:23 844547 2019-08-25 13:20:23 844547 2019-08-25 13:20:23 844567 2019-08-25 13:20:23 844655 2019-08-25 13:20:23 844655 2019-08-25 13:21:55:524516 2019-08-25 13:21:55:524516 2019-08-25 13:21:55:524516 2019-08-25 13:39:50 8184213 2019-08-25 13:341:26:032670 2019-08-25 13:41:26:0326870	2019-08-25         13.20.23.3845451         4672           2019-08-25         13.20.23.3845467         4672           2019-09-25         13.20.23.3845457         4662           2019-08-25         13.20.23.3845655         4672           2019-09-25         13.20.23.3845655         4672           2019-09-25         13.21.55.5264316         4625           2019-09-25         13.21.55.5275506         4625           2019-09-25         13.395.08.1841.41         4624           2019-09-25         13.395.08.1842.13         4672           2019-09-25         13.345.08.1842.13         4672           2019-09-25         13.41.26.0326970         4624           2019-08-25         13.41.26.0326870         4672	2019-08-25         13.20:23.3845451         4672         Administrative loggn           2019-08-25         13.20:23.3845467         4672         Administrative loggn           2019-08-25         13.20:23.3845467         4672         Administrative loggn           2019-08-25         13.20:23.3846455         4662         Successful loggn           2019-08-25         13.20:23.3846455         4672         Administrative loggn           2019-08-25         13.20:23.3846455         4672         Administrative loggn           2019-08-25         13.21:55.527.556         4625         Failed loggn           2019-08-25         13.39:50.8184.141         4624         Successful loggn           2019-08-25         13.39:50.8184.213         4672         Administrative loggn           2019-08-25         13.41:26.0326870         4672         Administrative loggn           2019-08-25         13.41:26.0326870         4672         Administrative loggn	2019-08-25         13.202.33845451         4672         Administrative loggn           2019-08-25         13.202.33845467         4672         Administrative loggn           2019-08-25         13.202.33845467         4672         Administrative loggn           2019-08-25         13.202.33845455         4672         Administrative loggn           2019-08-25         13.202.33845455         4672         Administrative loggn           2019-08-25         13.202.33845455         4672         Administrative loggn           2019-08-25         13.215.55264316         4625         Failed loggn         - (-)           2019-08-25         13.395.08184141         4624         Successful loggn         VIN-34037QH7TLI (127.0.0.1)           2019-08-25         13.395.08184213         4672         Administrative loggn         VIN-34037QH7TLI (127.0.0.1)           2019-08-25         13.412.6.0326870         4672         Administrative loggn         (-)           2019-08-25         13.412.6.0326870         4672         Administrative loggn         (-)           2019-08-25         13.412.6.0326870         4672         Administrative loggn         (-)	2019-08-25         13.202.33845451         4672         Administrative logon         SeAssignPrimary TokenPrivilege, Status           2019-08-25         13.202.33845467         4672         Administrative logon         WN-340J7QH7TLI (192.168.15.10)         SreassignPrimary TokenPrivilege, Status           2019-08-25         13.202.23845457         4672         Administrative logon         WN-340J7QH7TLI (192.168.15.10)         Target: WN-340J7QH7TLI (192.168.15.10)           2019-08-25         13.202.23845455         4672         Administrative logon         - (-)         Target: -           2019-09-25         13.212.55.5264.316         4625         Failed logon         - (-)         Target: -           2019-09-25         13.395.08.184.141         4624         Successful logon         WIN-340J7QH7TLI (127.00.1)         Target: WN-340J7QH7TLI (407.01)           2019-09-25         13.395.08.184.21         4672         Administrative logon         SeesurityPrivilges, SeTakeOvmer           2019-09-25         13.395.08.184.21         4672         Administrative logon         SeesurityPrivilges, SeTakeOvmer           2019-09-25         13.41.26.0326798         4624         Successful logon         (-)         Target: NT AUTHORITYSYSTEM           2019-08-25         13.41.26.0326870         4672         Administrative logon         SeAssignPrivaryTokenPrivilge

21. MapDescription 列のフィルタでログオフを示す「An account was logged off」と「User initiated I ogoff」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 TargetLog onId の値「0x46FB32」をコピーし、「Find All」ボタンを押します。

11/08	U	1219	2013-08-23 13:00:30.0480020	4020	Falled logor		
11723	0	1220	2019-08-25 13:06:38.5222115	4625	Failed logor		
11739	0	1221	2019-08-25 13:06:39.4045261	4625	Failed logor		
11792		1223	2019-08-25 13:20:23.1141285	4672	Administrati		
11793	٠	1224	2019-08-25 13:20:23.1142320	4624 0x46FB32	Successful		
11829		1226	2019-08-25 13:20:23.3844815	4624	Successful		
11830		1227	2019-08-25 13:20:23.3845266	4624	Successful		
11831		1228	2019-08-25 13:20:23.3845451	4672	Administrati		
11832		1229	2019-08-25 13:20:23.3845467	4672	Administrati		
11848		1233	2019-08-25 13:20:23.8848525	4624	Successful		
11849		1234	2019-08-25 13:20:23.8848585	4672	Administrati		
11885		1235	2019-08-25 13:20:24.8274800	4634	An account		
11905		1236	2019-08-25 13:20:25.0162410	4634	An account		
11906		1237	2019-08-25 13:20:25.0162904	4634	An account		
11931	0	1238	2019-08-25 13:21:55.5264316	4625	Failed logon		
11932	0	1239	2019-08-25 13:21:55.5271506	4625	Failed logon		
12012		1245	2019-08-25 13:39:50.8184141	4624	Successful		
12013		1246	2019-08-25 13:39:50.8184213	4672	Administrati		
12027		1247	2019-08-25 13:39:51.0758304	4634	An account		
		1010	0040 00 05 40 00 50 0340004				
4 4 4	H + H	tips2					
X Ox	46FB32		🔻 🗞 🕉 Find All 🔽 For	matted Display 🗍 Matc	h Case 📿		
Sheet 1 of	1		351 of 12123 records found	Default			

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。

Search	Results	
Sheet	Cell	Content
tips2 tips2 tips2 tips2	\$Z\$11792 \$Z\$11793 \$M\$11793 \$Z\$12027	<pre>("EventData":{"Data":{"@Name":"SubjectUserSid","#text":"S-1-5-21-874153392-1857218376 {"EventData":{"Data":[{"@Name":"SubjectUserSid","#text":"S-1-0-0"},{"@Name":"SubjectUser 0x46FB32 {"EventData":{"Data":[{"@Name":"TargetUserSid","#text":"S-1-5-21-874153392-1857218376- "EventData":{"Data":{"@Name":"TargetUserSid","#text":"S-1-5-21-874153392-1857218376-</pre>
		Close

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、Re cordNumber「1247」行 13 時 39 分 51 秒にログオフしたことがわかります。

tips2.cs	v - Libre	Office Calc							- • ×
File Edi	t View	Insert For	mat Sheet Data Tools Wind	ow Help					×
- T-	A • D	3 · 7 E	3 63 💟 🖻 😤 • 🔺 🤌	L 🔚 🗸 🖂 . 🔿 Al	s 🗰 • 💷 • 📖 🕯	in 👓 💌 🌰 🔽 O 😖 📮			
	_ 0								
		* 10	• a a a 🛓 • 🗏 •		E E E 🤛 • % 0	).0 🛍 比 🔐 📰 💷 🖪 - [	F•• 🖵 • 📑 • 🚔 🛍		
A12027		- <u>5π</u> Σ	= (						-
	A	В	D	E M	N	Q	R		
11678	0	1217	2019-08-25 13:06:33.9040592	4625	Failed logon	jessie (192.168.15.178)	Target: \Administrator	ogonTyr	2
11693	0	1218	2019-08-25 13:06:35.7940760	4625	Failed logon	jessie (192.168.15.179)	Target: \Administrator	ogonTyr	60
11708	Õ	1219	2019-08-25 13:06:36.6486620	4625	Failed logon	jessie (192.168.15.179)	Target: \Administrator L	ogonTyr	T
11723	Ó	1220	2019-08-25 13:06:38.5222115	4625	Failed logon	jessje (192.168.15.180)	Target: VAdministrator	ogonTyp	1.000
11739	0	1221	2019-08-25 13:06:39.4045261	4625	Failed logon	jessie (192.168.15.180)	Target: \Administrator L	ogonTyr	Ŕ
11792		1223	2019-08-25 13:20:23.1141285	4672 0x46FB32	Administrative logon		SeSecurityPrivilege, SeBackupPrivile	qe, SeR	
11793		1224	2019-08-25 13:20:23.1142320	4624 0x46FB32	Successful logon	jessję (192.168.15.10)	Target: WIN-340J7QH7TLI\Admini+L	ogonTyr	
11829		1226	2019-08-25 13:20:23.3844815	4624	Successful logon	(-)	Target: Window Manager\DWM-2 L	ogonTyp	
11830		1227	2019-08-25 13:20:23.3845266	4624	Successful logon	(-)	Target: Window Manager\DWM-2	ogonTyr	5x
11831		1228	2019-08-25 13:20:23.3845451	4672	Administrative logon		SeAssignPrimaryTokenPrivilege, SeA	AuditPriv	
11832		1229	2019-08-25 13:20:23.3845467	4672	Administrative logon		SeAssignPrimaryTokenPrivilege, SeA	AuditPriv	
11848		1233	2019-08-25 13:20:23.8848525	4624	Successful logon	WIN-34OJ7QH7TLI (192.168.15.10)	Target: WIN-340J7QH7TLI\Admini≯L	ogonTyr	
11849		1234	2019-08-25 13:20:23.8848585	4672	Administrative logon		SeSecurityPrivilege, SeTakeOwnersh	nipPrivile	
11885		1235	2019-08-25 13:20:24.8274800	4634	An account was logged of	*	Target: WIN-340J7QH7TLI\Administr	ator	
11905		1236	2019-08-25 13:20:25.0162410	4634	An account was logged of	>	Target: Window Manager\DWM-2		
11906		1237	2019-08-25 13:20:25.0162904	4634	An account was logged of	<b>,</b>	Target: Window Manager\DWM-2		
11931	0	1238	2019-08-25 13:21:55.5264316	4625	Failed logon	- (-)	Target: -\-	ogonTyr	
11932	0	1239	2019-08-25 13:21:55.5271506	4625	Failed logon	- (-)	Target: -\-	ogonTyr	
12012		1245	2019-08-25 13:39:50.8184141	4624	Successful logon	WIN-340J7QH7TLI (127.0.0.1)	Target: WIN-34OJ7QH7TLI\Admini+L	ogonTyr	
12013		1246	2019-08-25 13:39:50.8184213	4672	Administrative logon		SeSecurityPrivilege, SeTakeOwnersh	nipPrivile	
12027	_	1247	2019-08-25 13:39:51.0758304	4634 0x46FB32	An account was logged of	<b>b</b>	Target: WIN-340J7QH7TLI\Administr	ator	
12048		1248	2019-08-25 13:39:52.0749001	4634	An account was logged of	•	Target: WIN-340J70H7TLI\Administr	ator	
12050		1249	2019-08-25 13:39:52.4077543	4634	An account was logged of	•	Target: Window Manager\DWM-3		
12051		1250	2019-08-25 13:39:52.4079664	4634	An account was logged of	•	Target: Window Manager\DWM-3		
12070		1252	2019-08-25 13:41:26.0326798	4624	Successful logon	(-)	Target: NT AUTHORITY\SYSTEM L	ogonTyr	
12071		1253	2019-08-25 13:41:26.0326870	4672	Administrative logon	0	SeAssignPrimaryTokenPrivilege, SeT	Coprivil	
12082		1254	2019-08-25 13:41:26.5204014	4647	User initiated logoff			~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	
12125								U	
12126									
(casan				1					
4 + H	H +	tips2							
M Ox	46FB32		🔹 💩 🖗 Find All 🗆 Fe	ormatted Display 🗍 Mate	h Case 📿				
Choot 1 -5	101 0 02		IE1 of 12122 corordr found	Def-uk		Ce	1111111 Sum 17614	14	110%
Sheet 1 OF	1	3	151 0F12125 Tecords Found	Derault	III.	Average: 2937.33333:	222222; sum: 1/024 =		110%
MENU 📐 🤇			🚍 🔏 : 🐃 [cain 🐃 [cain	. 🦲 tips2 🛛 🐸 caine	🗈 tips2 🛛 🔎 📠 🞑	칠 🐠 📄 🔭 🔺 9月 19, 01:31 🖬 🗉 0	B/s 36 B/s		

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