Soliton®

MWS Cup 2018 – 課題1 解説

2018年12月20日

株式会社ソリトンシステムズ

はじまり

意味ある出題ができるなら、
Cupで出題しても良い

どういう問題なら意味があるだろうか？

理解あるみなさまのおかげで
出題させていただくことに・・・

正常操作を含む実環境のログから
悪性の動作を見出すような問題はどうでしょう？

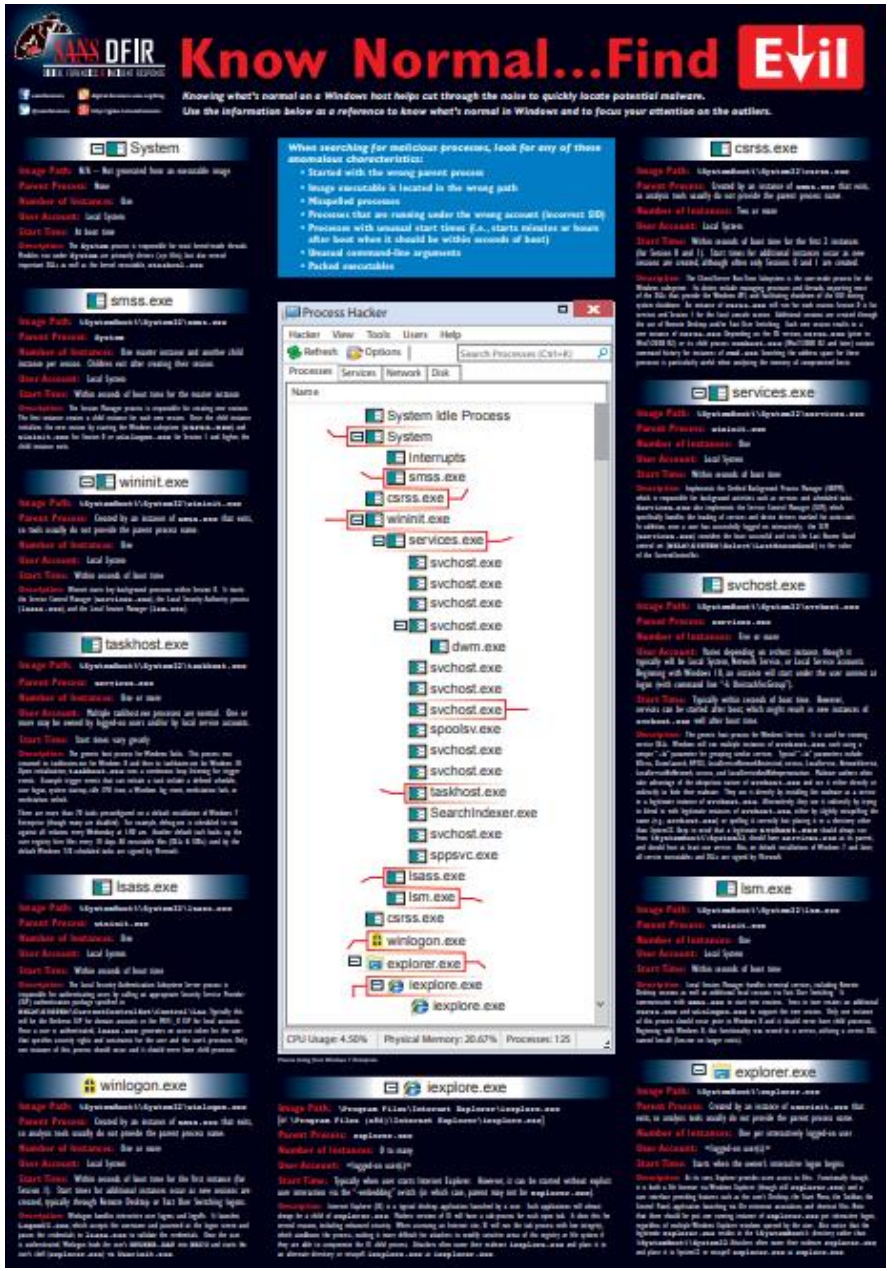
そういうのもありですよ

DFIR ですね！

DFIR: Digital Forensics and Incident Response

方針

- 実環境を知る
- シナリオを理解する
- 自由記述



ご参考： https://www.sans.org/security-resources/posters/dfir/dfir-find-evil-35

2つの攻撃シナリオを用意

A)Webからランサムウェアをダウンロードし実行して感染

B)OutlookでExcelファイルを保存して開き、悪性マクロによりブラウザに保存された認証情報を窃取される

1台の端末で複数の攻撃が同時並行で行われることもある
自由記述であっても解き方の手順を意識してもらえるような設問を目指した

課題１　設問

1. このユーザー（admin1）が行った操作の中から3つを抜き出して簡潔に記述せよ (6点)(各2点)

2. 侵害発生に至ったユーザー操作の一連の流れを記述せよ （複数記述）(8点)

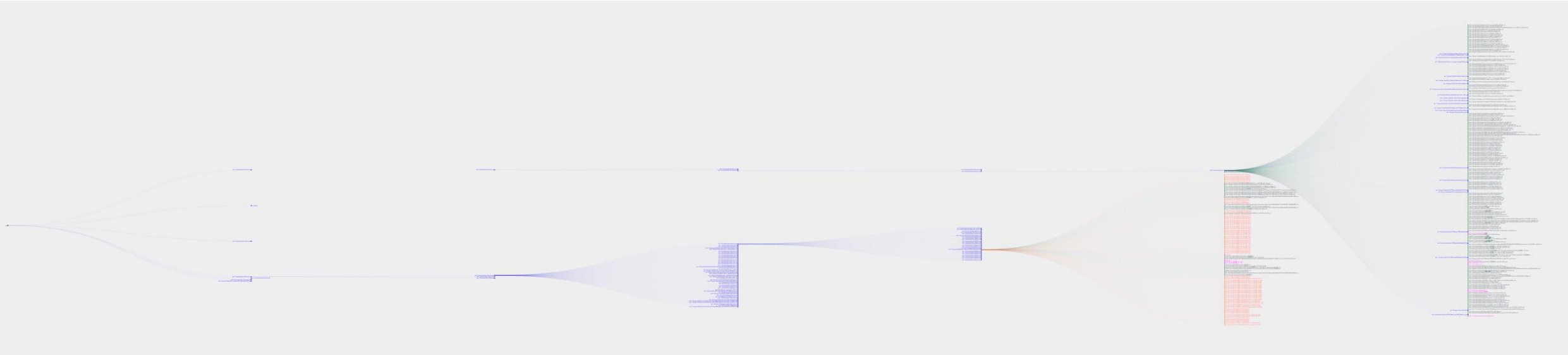
3. 侵害と判断した理由を該当ログのシリアル番号（sn）とともに記述せよ （複数記述）(11点)

ユーザの操作であればOK
侵害かどうかは問わない

ランサムウェアと
悪性マクロ含むExcelの
2つの流れを見つける

課題１　解き方のポイント（全体）

- 配布したツール(mk2tools)によりプロセスの親子関係を可視化すると良い
  - プロセス関連のログに絞ってから描画するなどの工夫もあり
- 全てのログを追うのは非効率
  - ログの行数は16,843行
  - 問題文から、ユーザー操作を起点とした侵害に注目
  - Windowsやフリーソフトの常駐プロセスなどは追う必要は無い

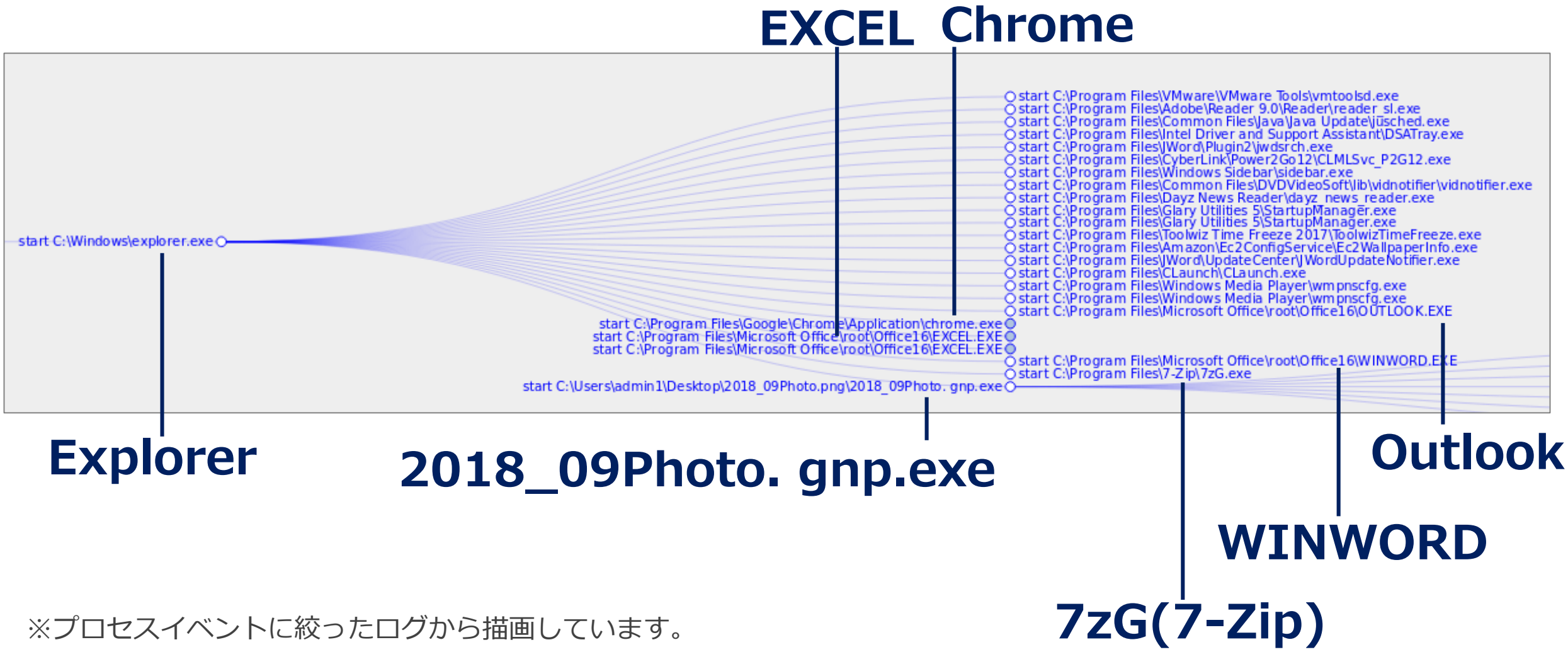


課題1-1)このユーザー（admin1）が行った操作の中から3つを抜き出して簡潔に記述せよ(6点)(各2点)

- 正答例（いずれか3個x2点＝計6点）
  - chromeでYahoo!Japanを開いた
  - chromeでGoogleを開いた
  - chromeでMSN Japanを開いた
  - Wordファイルを開いた（C:¥¥Users¥¥admin1¥¥Documents¥¥2018_10_定例会議.docx）
  - Excelファイルを開いた（C:¥Users¥admin1¥Desktop¥見積書¥見積書.xlsm）
  - Outlookでメール閲覧した（winTitle="株式会社○○向け ライセンス見積書のご案内 - メッセージ (HTML 形式) "）

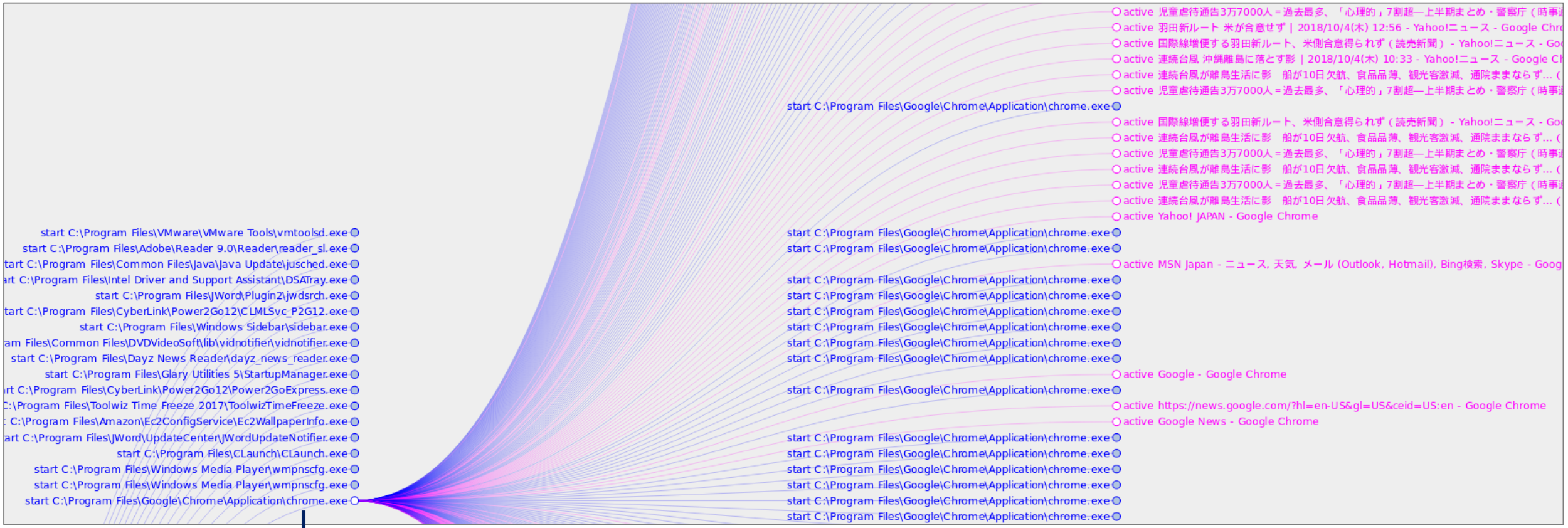
- 誤答例（実際に行っていない動作を指摘したら減点）
  - Excelで文書を作成した
    - 新規作成はしていない（write=0）
  - Excelで表計算した
    - 表計算したかどうかが記録されているわけではない
  - notepad.exeで_READ_THIS_FILE_BYI2E6_.txt を開いた
    - 親プロセスから、ユーザーが実施したことではなく、マルウェアによる実行と判別できる(sn=221047)

課題1-1) Explorerの子プロセスに注目



※プロセスイベントに絞ったログから描画しています。

Explorerの子プロセス① Chrome



Chrome

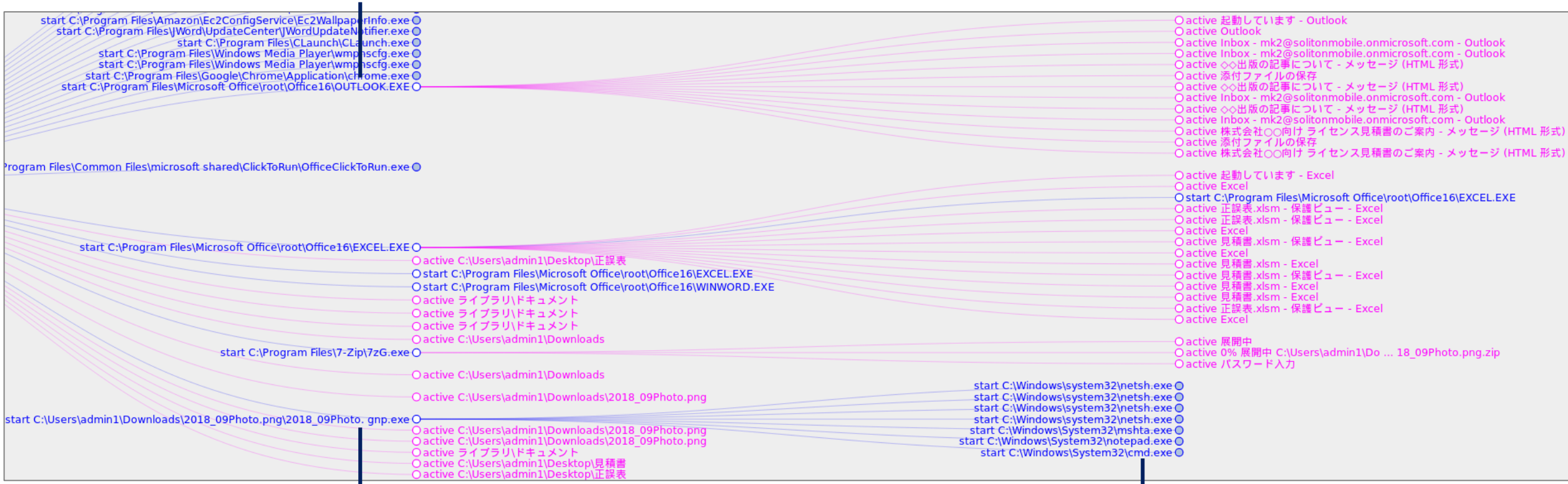
ウィンドウタイトル
（閲覧ページタイトルが分かる）

※ここではプロセス、ウィンドウタイトルで絞っていますが、IP・ドメイン名・URLなどで絞るなどでの工夫が可能です

Explorerの子プロセス② Outlook/Excelなど

ウィンドウタイトル
（Outlook操作の様子が分かる）

Outlook



2018_09Photo. gnp.exe

netsh/mshta/notepad/cmd

課題1-2)侵害発生に至ったユーザー操作の一連の流れを記述せよ（複数記述）(8点) --- ランサムウェア（Cerber）

- 採点基準
  - 実行ファイルへの言及(ファイル名、SHA256等)（1点）
  - ユーザ操作で実行されたこと（1点）
  - 実行ファイルがWebからダウンロードされたこと（2点）

- 正答例
  - Chromeでfile.ioにアクセスし、”2018_09Photo.png.zip”をデスクトップにダウンロードした
  - 7zG.exeで” C:¥Users¥admin1¥Desktop¥2018_09Photo.png.zip”を”C:¥Users¥admin1¥Desktop¥2018_09Photo.png¥2018_09Photo.gnp.exe”に展開した
  - 2018_09Photo. gnp.exeを実行した

課題1-2)侵害発生に至ったユーザー操作の一連の流れを記述せよ（複数記述）(8点) --- Excelバックドア

- 採点基準
  - Excelバックドアファイルへの言及(ファイル名、SHA256等)（1点）
  - Excelバックドアファイルがユーザ操作で開かれたことの指摘（1点）
  - Excelバックドアがメール(Outlook)で受信したことの指摘（2点）

- 正答例
  - Outlookで添付ファイル「見積書.zip」をデスクトップに保存した
  - 「見積書.zip」を解凍し「C:¥Users¥admin1¥Desktop¥見積書¥見積書.xlsm」に展開した
  - 「見積書.xlsm」を開いた

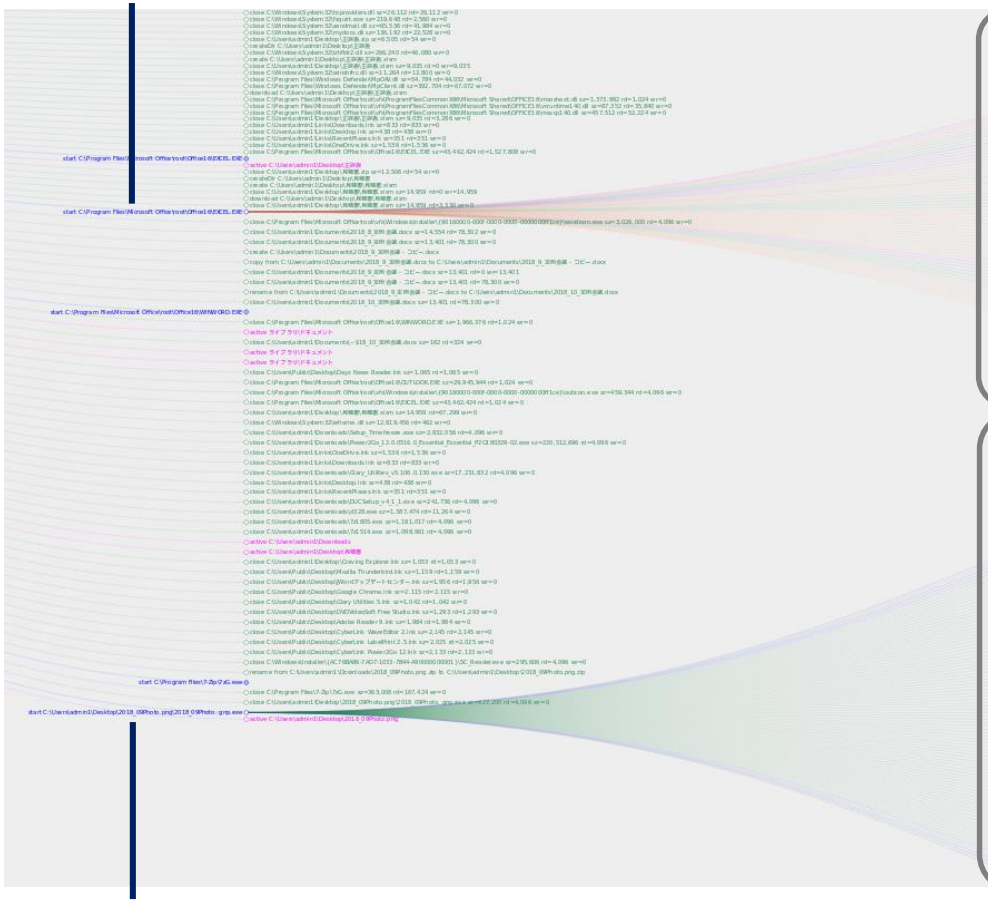
課題1-3)侵害と判断した理由を該当ログのシリアル番号（sn）とともに記述せよ（複数記述）(11点)

- 採点基準
  - ランサムウェア
    - 不審なファイルアクセスへの言及（3点）
    - 脅迫文表示の指摘、RLO、Windows Defenderへの干渉など、その他の不審点の指摘（3点）
  - Excelバックドア
    - EXCELからローカルアドレスへの80番ポートへの通信（2点）
    - EXCELからchromeに保存された認証情報などをReadしていることの指摘（3点）

- 正答例
  - 課題1-2で指摘した「2018_09Photo. gnp.exe」がsn=107413からsn=107494にかけてファイルアクセスしており、例えばThunderbirdの設定ファイルや見積書.zipを上書きし「.8840」という拡張子にリネームしている
  - 課題1-2で指摘した「2018_09Photo. gnp.exe」がnotepad.exeを利用して「C:¥Users¥admin1¥Desktop¥_READ_THIS_FILE_BYI2E6_.txt」を表示させている（sn=221047）
  - EXCELからローカルアドレスへの80番ポートへの通信している（sn=208554）
  - EXCELが、Chromeに保存された認証情報である「C:¥Users¥admin1¥AppData¥Local¥Google¥Chrome¥User Data¥Default¥Login Data」をReadしている（sn=208588）

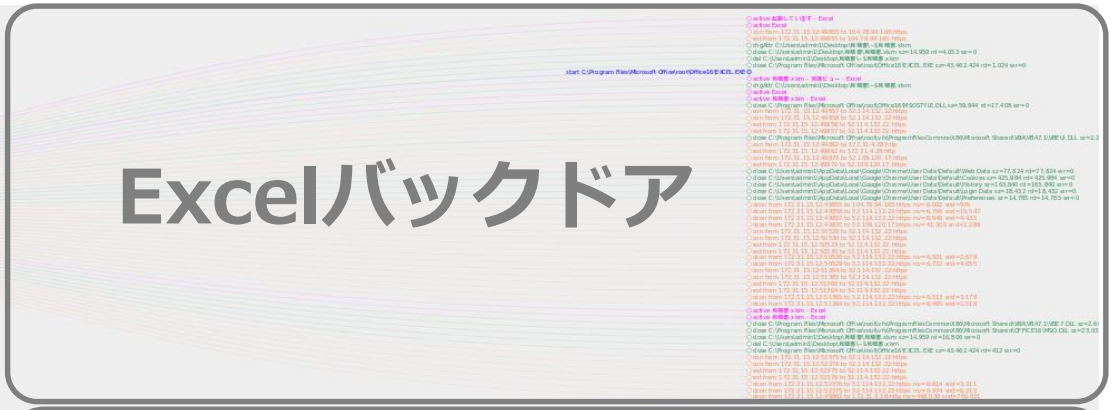
課題1-3) 全体像の把握

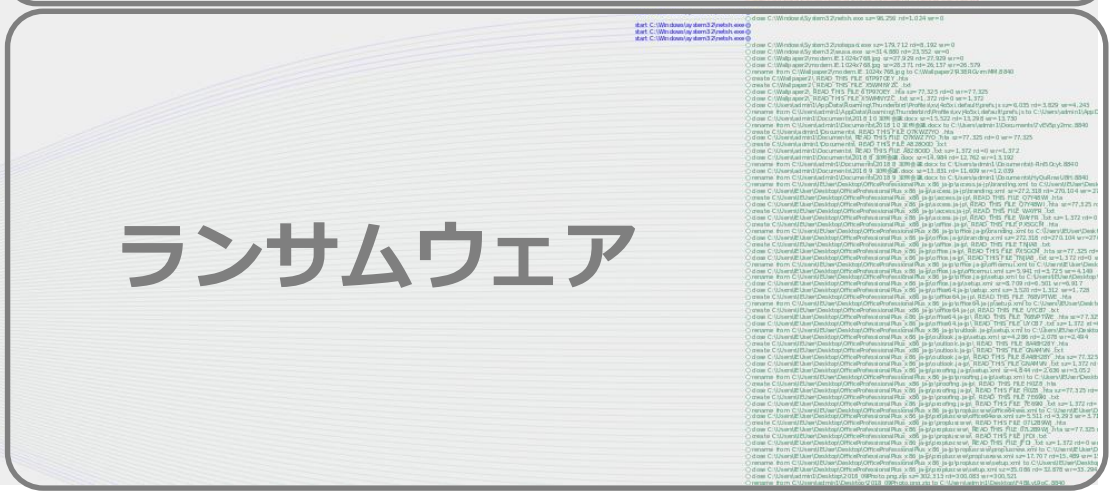
EXCEL



2018_09Photo. gnp.exe

ファイルアクセス・通信





大量のファイル読み・書き・リネーム

課題1-3) ランサムウェア – 侵害判断例（2018_09Photo. gnp.exe）

```
ps start C:\Windows\system32\netsh.exe
args: "advfirewall firewall add rule name=""0MFTZJFCiF"" dir=out action=block program=""C:\Program Files\Windows Defender\MpCmdRun.exe"""

time: 2018-10-17T20:57:40.000Z
elapsed_from_parent: 00:00:12.000
runtime: 00:00:01.000
```

MpCmdRun.exe（Windows Defender 定義更新）通信ブロック

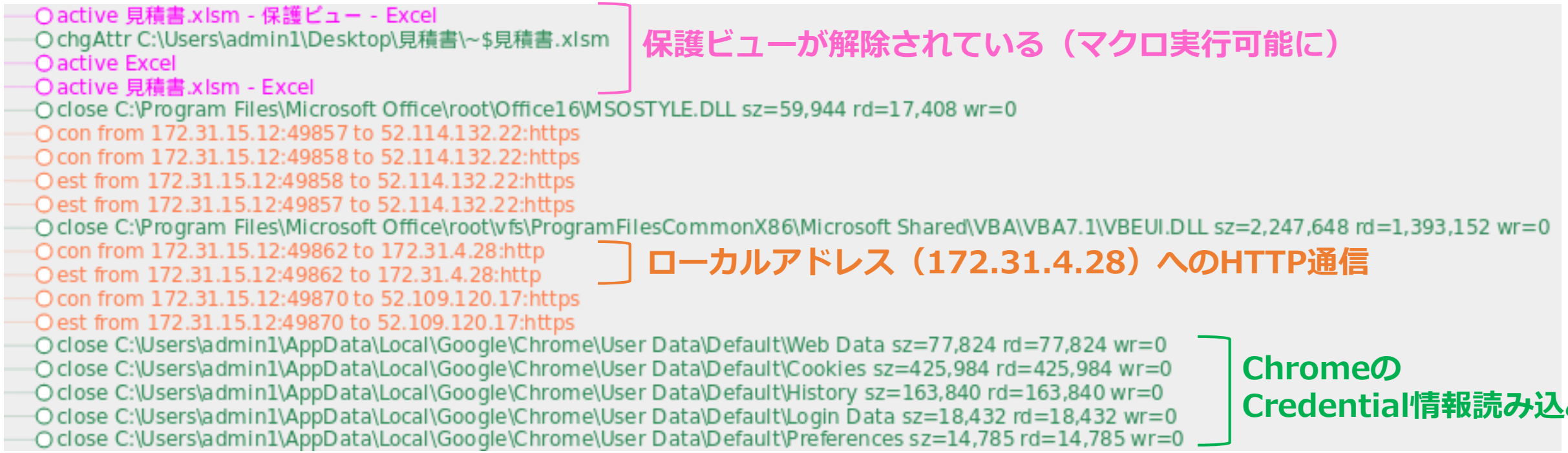
```
ps start C:\Windows\system32\netsh.exe
args: "advfirewall firewall add rule name=""n6Oqi5WVME"" dir=out action=block program=""C:\Program Files\Windows Defender\MSASCui.exe"""

time: 2018-10-17T20:57:41.000Z
elapsed_from_parent: 00:00:13.000
runtime: running
```

MSASCui.exe（Windows Defender GUI）通信ブロック

```
start C:\Windows\system32\netsh.exe
                                    close C:\Windows\System32\netsh.exe sz=96,256 rd=1,024 wr=0
start C:\Windows\system32\netsh.exe
start C:\Windows\system32\netsh.exe
start C:\Windows\system32\netsh.exe
                                    close C:\Windows\System32\notepad.exe sz=179,712 rd=8,192 wr=0
                                    close C:\Windows\System32\wusa.exe sz=314,880 rd=23,552 wr=0
                                    close C:\Wallpaper2\modern.IE.1024x768.jpg sz=27,929 rd=27,929 wr=0
                                    close C:\Wallpaper2\modern.IE.1024x768.jpg sz=28,371 rd=26,137 wr=26,579
                                    rename from C:\Wallpaper2\modem.IE.1024x768.jpg to C:\Wallpaper2\R38RGvrmMM.8840
                                    create C:\Wallpaper2\_READ_THIS_FILE_6TP97OEY_.hta
                                    create C:\Wallpaper2\_READ_THIS_FILE_X5WMNYZC_.txt
                                    close C:\Wallpaper2\_READ_THIS_FILE_6TP97OEY_.hta sz=77,325 rd=0 wr=77,325
                                    close C:\Wallpaper2\_READ_THIS_FILE_X5WMNYZC_.txt sz=1,372 rd=0 wr=1,372
```

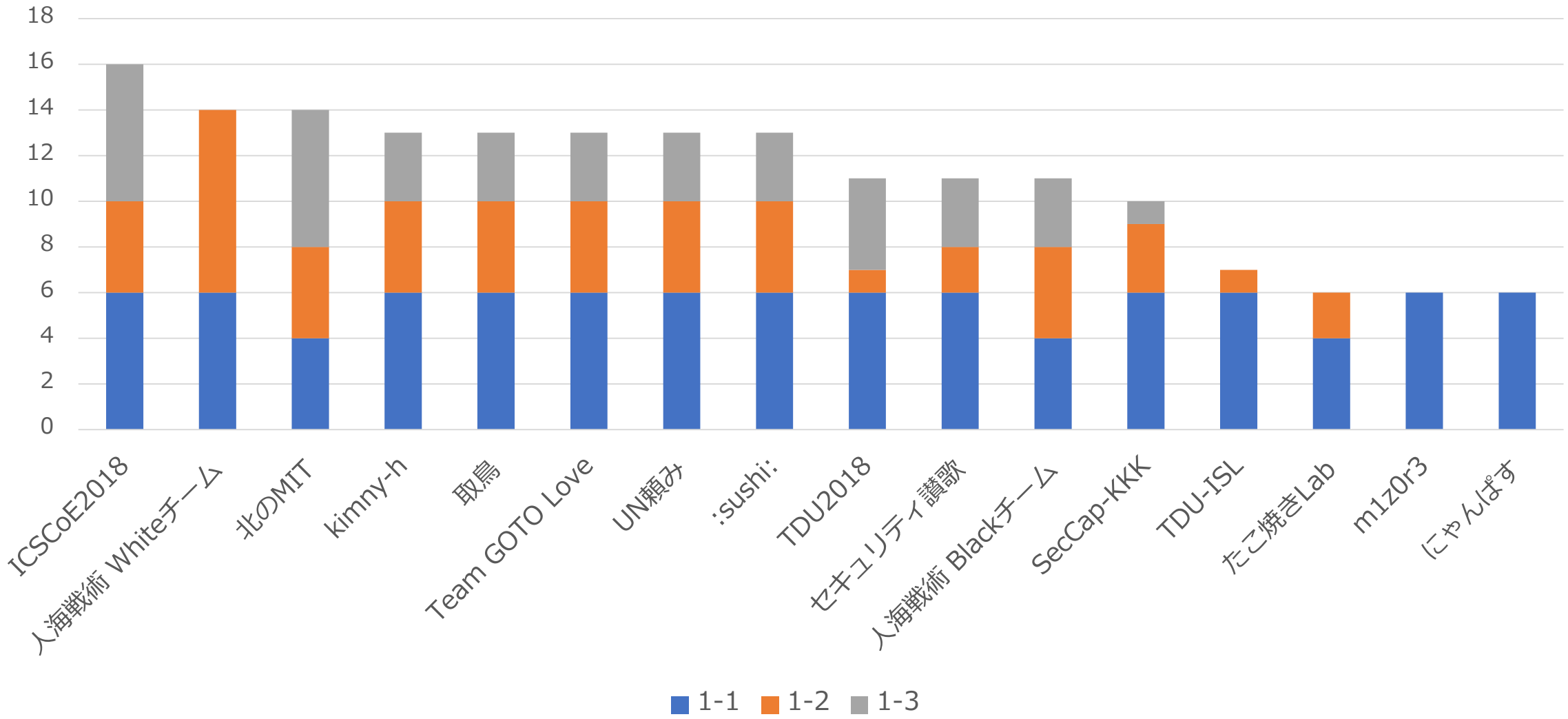
ファイル読み込み
暗号化
拡張子変更
脅迫文作成

課題1-3) Excelバックドア – 侵害判断例（Excel.exe - 見積書.xlsm）



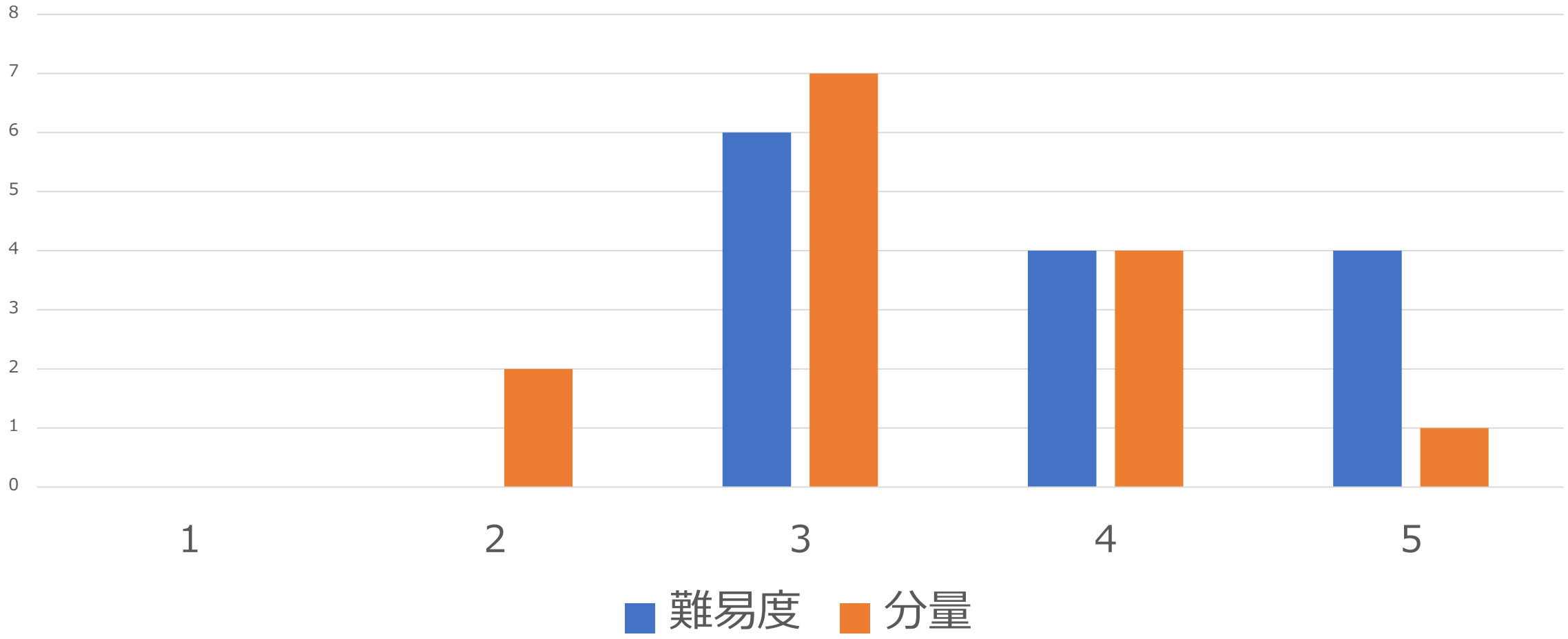
Mark II Analyzer ログ分析画面

課題１：採点結果



アンケート – 難易度・分量

ちょうど良かったでしょうか？



アンケート – コメント

意図を理解して下さるチームあり
出題者冥利に尽きます、ありがとうございます

- ログを読み込めば回答できる、非常に良い内容と感じました。
- 実際の製品のログの分析は実務的だと感じた
- しっかり読むとシナリオがわかる問題で非常に良かったと思う
- treeを可視化してくれるツールがとても使いやすくて役に立ちました．ありがとうございました.
- 実際にありそうなログを解析することができて、リアルな体験ができました。ただChromeのログが膨大すぎて、ブラウザで可視化すると重たすぎるので、何か良い方法があればとも思いました。
- 前提知識が必要ない問題だったため、解いててやりがいがあった。ツールの動作環境なども掲載して欲しい。
- 普段はSoliton Datasetにふれる機会が無くても、ツールを活用したり目grepで頑張ることで十分回答可能な問題設定でとてもよかった。回答の粒度がどの程度のレベルを期待しているのか分からなかったため、今回回答例を出していただけると参考になると思う。excelの部分は気がついていたのに答えられなかったのが悔しい。
- ボリュームが多くて処理が大変だった
- とにかく難しかった
- データセットが事前にもらってないので、分類器の作成が難しい
- 動作が重い
- 新しい傾向の問題でつらかった

所感

- 良かったこと
  - 初出題にも関わらず、良いフィードバックをいただけた
- 改善したいこと
  - 問題文の読解・当日のヒント
    - 「侵害は1つとは限りません」とお伝えしたものの、お手つき禁止ルールにより抑制されてしまった？
    - 当日の資料を配布するつもりがすっかり失念していました…。
  - 時間制約によるプレッシャー（競技なので仕方ないがお互い残念）
    - 課題2の回答を課題3に書いてしまったケースも散見
  - Google Form
    - 自由記述だと再編集できないと辛い。事前に周知徹底すべきでした。

今後に向けて

- 来年もデータセット取り組みます！
  - Mark IIログ**＋α**
- データセットへのご意見お待ちしています
  - 対象にして欲しいマルウェア
  - データセットに含めて欲しい情報

MWS Cup 2018当日の説明資料

MWS Cup 2018 – 課題1について

2018年10月22日

株式会社ソリトンシステムズ

課題1について

- 目的
  - 実環境に近いエンドポイントのログから侵害を見出す

- 概要
  - ソリトンシステムズ製のエンタープライズ向けEDR製品「InfoTrace Mark II for Cyber」（以下Mark II）のログから、ユーザー操作や侵害に至った操作、侵害と判断した理由などを問います。

提供物

- Mark II ログ
  - MWSCup2018_Soliton.log
- ログ仕様マニュアル（Soliton Dataset 2018より）
  - InfoTraceMarkIIforCyberV20_ClientLogItemList_Rev9.pdf
- Tools（Soliton Dataset 2018より）
  - JSON化、描画スクリプトなど。利用は必須ではありません。
  - mk2tree.jsのみ、改良版を収録しています
    - Key-bindingオプション”x”にてプロセスチェインを全開できるようにしました

課題

1. このユーザー（admin1）が行った操作の中から
   3つを抜き出して簡潔に記述せよ(6点)(各2点)

2. 侵害発生に至ったユーザー操作の一連の流れを記述せよ
   （複数記述）(8点)

3. 侵害と判断した理由を該当ログのシリアル番号（sn）と
   ともに記述せよ（複数記述）(11点)

（参考）Mark II ログ例

（以下はOlympic Destroyerの例であり課題ログとは関係ありません）

シリアル番号　　イベント　サブイベント

03/27/2018 19:44:53.926 +0900 loc=ja-JP type=ITM2 sn=1818 lv=5 rs=5 trs=70 rf=C8 evt=ps subEvt=start os=Win
com="PC4" domain="WORKGROUP" profile="1803Tsurutusv204ALL3" tmid= csid=S-1-5-21-623506775-2833361433-
4044451033
ip=169.254.19.167,fe80::55e2:e812:6f2a:13a7,169.254.162.70,fe80::8c8f:d8ac:7c85:a246,169.254.25.247,fe80::c549:
5c7f:5731:19f7,169.254.153.216,fe80::b467:e9bc:b93:99d8,172.24.1.4,fe80::d51f:c8b1:d18f:ba84
mac=00:16:eb:cb:13:0c,02:16:eb:cb:13:08,02:16:eb:cb:13:09,00:16:eb:cb:13:08,f4:4d:30:6d:94:33
usr="taro.yamada" usrDomain="PC4" sessionID=1 psGUID={486E9E21-3D5C-43D0-A660-3952DC610339}
psPath="C:¥Users¥taro.yamada¥AppData¥Local¥Temp¥_jsh.exe" プロセス名（このプロセスがスタートした、という意味になります）

cmd="¥¥172.24.0.1 -u ""PC4¥taro.yamada"" -p ""S0lit0n"" -accepteula -d -s -c –f プロセスコマンドライン（引数）

""C:¥Users¥TARO~1.YAM¥AppData¥Local¥Temp¥_bbh.exe""" psID=5788 parentGUID={1CA3AFB2-3C03-4358-A5E2-
085002A97A40}
parentPath="D:¥28858cc6e05225f7d156d1c6a21ed11188777fa0a752cb7b56038d79a88627cc.exe" 親プロセス名

psUser=“taro.yamada” psDomain="PC4" プロセス実行ユーザーとドメイン
arc=x86 sha256=3337e3875b05e0bfba69ab926532e3f179e8cfbf162ebb60ce58a0281437a7ef
sha1=e50d9e3bd91908e13a26b3e23edeaf577fb3a095 md5=27304b246c7d5b4e149124d5f93c5b01
company="Sysinternals - www.sysinternals.com" copyright="Copyright (C) 2001-2016 Mark Russinovich"
fileDesc="Execute processes remotely" fileVer="2.2" product="Sysinternals PsExec" productVer="2.2"
crTime="03/27/2018 19:41:47.879" acTime="03/27/2018 19:41:47.879" moTime="03/27/2018 19:41:47.879"
size=339096 sig=Valid signer="Microsoft Corporation" issuer="Microsoft Code Signing PCA 2011" cerSN="33 00 00 00 64
47 84 94 86 db 41 19 38 00 00 00 00 00 64" validFrom="10/29/2015 05:31:46.000" validTo="01/29/2017 05:31:46.000"

ログ種類（抜粋）

※詳細はマニュアルをご参照ください。

イベント(evt)	サブイベント(subEvt)	説明
プロセス(ps)	起動(start)	プロセスが起動したときに出力されます。
	停止(stop)	プロセスが停止したときに出力されます。
ファイル(file)	作成(create)	ファイルが作成されたときに、対象ファイルpath="<ファイルパス>"にて出力されます。
	閉じる(close)	ファイルにアクセスされたときに閉じられるタイミングで出力されます。
	削除(del)	ファイルが削除されたときに出力されます。
	名前変更(rename)	ファイル名が変更されたときにPath="<元ファイル>", dstPath="<コピー先ファイル>"にて出力されます。
	コピー(copy)	ファイルがコピーされたときにPath="<元ファイル>", dstPath="<コピー先ファイル>"にて出力されます。
	属性変更(chgAttr)	ファイルの属性が「隠しファイル」に変更されたとき、またはファイルの属性が「隠しファイル」のファイルで「読み取り専用」の属性が変更されたときに、出力されます。
レジストリ(reg)	値指定(setVal)	レジストリのキーに値が新規に設定されたとき、または値（値の種類がREG_BINARY の場合はサイズ）に変化があったときに、出力されます。
	キー削除(delKey)	レジストリのキーが削除されたときに、出力されます。
ネットワーク(net)	TCP接続(con)	TCP 接続を行ったときに、出力されます。
	TCP切断(dcon)	TCP 接続が切断されたときに、出力されます。
	ブラウザーによるWeb アクセス(webURL)	WebブラウザーによってWebアクセスが行われたときに出力されます。
ウィンドウ(win)	アクティブ(active)	デスクトップ上のウィンドウがアクティブになったときに、出力されます。アクティブな状態で、ウィンドウタイトルが変化したときも出力されます。
クリップボード(clip)	貼り付け(paste)	クリップボードのデータが貼り付けられたときに、出力されます。
ユーザーセッション(session)	ログイン(login)	コンピューターにログインしたときに、出力されます。

注意事項

- 監視範囲は独自に設定しており、ログ量低減などの理由で監視対象外としているものがあります
  - 例) evt=file subEvt=openは、設定で記録していません

- Windowsの仕様にしたがって出力しているため、一般的な操作の感覚とは差異がある場合もあります
    - 例) evt=file subEvt=downloadは、ZoneIdの仕様に従い同一ファイルで複数出力されることがあります

採点について

- インターネット上の情報を活用しても問題ありませんが、採点はあくまでログから読み取った内容に対して行います
- 記述された要点が多いほど高得点になる可能性がありますが、誤った記述があった場合は減点します
- 問題の意味や、問題に関係するログ仕様の不明点は、出題者（早川、村瀬、荒木）に質問してください