SHIELD Security Research Center

Hisys Security Journal

VOL.54

HITACHI
Inspire the Next

日立システムズ

Hisys Security Journal VOL.54

TABLE OF CONTENTS

●はじめに

本文書は、株式会社日立システムズ サイバーセキュリティリサーチセンタが運営するセキュリティ情報サイト、S.S.R.C.(Shield Security Research Center) の公開資料です。本サイトでは、本文書のバックナンバーをはじめ、S.S.R.C. によるリサーチ結果などを随時公開しています。

S.S.R.C. https://www.shield.ne.jp/ssrc/

AVTOKYO の開催や国際 CTF 大会への挑戦を通して セキュリティ・コミュニティをリードしてきた

tessy（寺島崇幸）インタビュー

取材・文＝吉澤亨史
撮影・編集＝斉藤健一

セキュリティ・コミュニティ内で有名なイベントの 1 つが AVTOKYO だ。「no drink, no hack」を標榜し、コミュニティ主導で企画・運営されている。今回、話を伺う tessy こと寺島崇幸氏は、AVTOKYO の企画・運営の中心にいる人物。2000 年代初頭よりコミュニティ内で積極的に活動を続け、CTF チームを結成。DEFCON CTF 本戦への出場を数回にわたり実現したり、マレーシアで開催された国際大会では 2 度の優勝を果たしたりするなど、数々の成果を残してきた。今回は、tessy さんの話を通じて、セキュリティ・コミュニティを振り返りつつ、11 月開催の AVTOKYO2023 の話題、そして tessy さん自身の信条などについても触れてみたい。

たまたま入った会社がセキュリティだった

吉澤（以下 Y）：まず、tessy さんの経歴についてお願いします。

tessy（以下 T）：大学は北海道で、しかも農学部でした。特に農業をやりたかったというわけではありませんでしたが、トラクターなどの農業用機械や農産物加工などについて学びました。卒業後に就職したのは自動車の部品を CAD で設計する企業でした。情報系には全く縁がなかったのですが、学生時代に触れたインターネットに携わる仕事への思いが強くなり、ネットワーク系の企業に転職することにしました。

Y それはいつ頃のことですか。

T 2001 年のことです。そして、この企業がセキュリティをサービスとして立ち上げることとなり、勉強会に参加したり、書籍を読んだりして研さんを始めました。これがセキュリティとの最初の関わりです。

Y たまたま入った会社でセキュリティに関わったことがきっかけ、というのも興味深いですね。

T 入社した当時はネットワークの知識しかなく、Nmap さえわからない状況でした。ですが、セキュリティ診断やセキュリティの教育コンテンツを作ったり、実際に教えたりしていました。セキュリティプロダクトの部署はあったのですが、新たにサービスを作るということで、未経験でしたがいろいろなことに挑戦しました。

Y 業務以外の活動はいかがでしたか。

T 日経 BP が主催する「WPC EXPO 2002」の中で「セキュリティ・スタジアム 2002」というイベントに参加しました。一般から応募した参加者たちが「攻撃」「防御」「検知」の 3 つのクラスに分かれ、腕を競い合うものでした。これを皮切りに、さまざまなセキュリティイベントに参加し始めました。また、ブログでセキュリティ情報などを発信するうちに、知人も増えていきました。

CTF への挑戦は DEFCON というお祭りをより楽しむため

Y 2000 年代、tessy さんはチームチドリとして活動されていたかと思います。まずこのチームについて教えてください。

寺島崇幸（てらしま・たかゆき）
2001 年からネットワーク、システムのセキュリティなどの仕事に携わる。現在は株式会社ディアイティに勤務。DEFCON CTF 本戦にはじめて出場した日本チーム sutegoma2 のリーダーを務める。2008 年よりコミュニティ主導によるセキュリティイベント AVTOKYO を主催。2012 年より SECCON 実行委員会に参画。副実行委員長を経て、現在はアドバイザーを務めている。

T 2002 年頃、仲の良い 5 ～ 6 人の仲間で活動していました。そこには、私のほかにもう 1 人の「寺島」さんがいて、ダブル寺島だったわけです。チーム名を考えるときに、最初は「T 島」という案も出たのですが、「島」だと面白くないということで「T 鳥」となり、それが「チドリ」になったのです。

Y Twitter（現：X）のアイコンに家紋の「千鳥紋」が使われていますが、そういったいきさつがあったのですね。

T はい。チドリで初めて DEFCON に参加したのが 2005 年でした。このときはまだ CTF には参戦せず、仲間でワイワイと楽しんでいました。DEFCON には、「WALL of SHEEP」というコーナーがあり、暗号化せずに通信している人のパスワードが会場にさらされます。私たちはこれを逆手にとり、平文でパスワードを送ってしまったふりをして架空アカウントのパスワードを表示させる遊びをしていました。

Y なるほど。発想の逆転ですね。

T CTF には翌年の 2006 年から参加しました。

DEFCON というお祭りをもっと楽しみたいという気持ちからです。これも飲み会の席で「出よっか」という軽いノリで決まったのです。

Y もともと海外に行く機会は多かったのですか。

T 実は海外は苦手でした。2000 年頃、最初の会社で 2 ヵ月間ほどアメリカとベルギーに行かされたのですが、嫌で嫌でしかたありませんでした。

Y 現在の tessy さんからは想像できない答えですね。

T この気持ちが変わったのは、自身でセキュリティ情報を収集するようになってからです。セキュリティ業界では、一次情報は海外からの発信がほとんどです。また、海外のカンファレンスに行けば、Windows の脆弱性の話を発見者から直接聞くこともできます。そこで、2006 年ごろから、マレーシアのセキュリティカンファレンスに行くようになったのです。実は、当時在籍していた会社が倒産し、半年間ほど自由の身だったという理由もありましたが。

Y そういった経緯があったのですね。

T マレーシアのセキュリティカンファレンスでは、CTF も開催しているのですが、DEFCON とは違い、当日会場に行けば参加できるものでした。「出場して腕試ししたい」と、毎年、いろいろな人に声をかけて参加しました。実際に、日本からチームとして出場したのは sutegoma2 になったときでした。

Y sutegoma2 になったのは、いつ頃でしたか？

T sutegoma2 をチーム名としたのは 2008 年からです。これまでチドリで DEFCON CTF 本戦出場を目指していたのですが、やはり世界の壁は高く、なかなか予選を突破できずにいました。そんなとき、「DEFCON CTF プロジェクト」として本戦出場を目指す機運がコミュニティ内で高まってきたのです。それまでの複数チームを一本化した合同チームの結成や、勉強会の本格化などに取り組んでいきました。

Y その合同チームが sutegoma2 なのですね。

T はい。sutegoma2 の由来をお話すると、当時の DEFCON CTF の予選ではルール上、アカウントをたくさん持っているチームの方が有利だったのです。そこで、sutegoma、sutegoma2、3、4、5 と数多くのアカウントを作っていたのですが、CTF 運営側のトラブルで多くのアカウントが消えてしまったことがありました。そんな中、sutegoma2 だけが残ったのです。

Y それは幸運でしたね。

T はい。これは縁起がよいということで、そこから sutegoma2 がチーム名となりました。後々になって「私たちは若い人たちの捨て駒、踏み台になる」という意味ですと語るのですが、きっかけはそんな形でした。

Y sutegoma2 の戦績について教えてください。

T 結成 4 年目の 2011 年に DEFCON CTF 予選で 2 位になり、初めて本戦に出場しました。このときは、多くの方々に支援していただきました。結果は残念ながら最下位でしたが、同年の 10 月にはマレーシアの CTF で優勝しました。マレーシアでは 2 回優勝しています。

Y sutegoma2 は日本の CTF プレイヤーの底上げにも寄与したといえますが、当時に比べて、現在の日本人プレイヤーのレベルは上がりましたか？

T 何をもって判断するのかは難しいですが、国際 CTF 大会への参戦は sutegoma2 の活動によって広がった側面はあると思います。DEFCON CTF や韓国の CODEGATE　CTF などで決勝戦に駒を進めることで、多くの経験を積んできました。このことが、「binja（ビンジャ）」や「Tokyo Westerns」をはじめとする次世代のチームへとつながっていると考えます。

BlackHat Japan の後夜祭から始まった「AVTOKYO」

Y それでは本題の AVTOKYO ※1 についてお聞きします。アーカイブ※2 を見ると 2008 年からとなっています。

T もともと、BlackHat JAPAN が 2004 年から 2008 年まで開催されていて、その打ち上げが起源です。ラスベガスで開催している BlackHat USA

※ 1 **AVTOKYO** https://www.avtokyo.org/
※ 2 **AVTOKYO 日本語アーカイブ** https://ja.avtokyo.org/

に行った日本人たちが飲み会をするような感覚で「After Vegas」、略して AV と 2007 年頃から呼ぶようになりました。

Y なるほど。AV にはそういう意味があったのですね。

T 2007 年の BlackHat JAPAN 終了後、新宿の飲食店で、プレゼンをしながらワイワイと盛り上がっていると、BlackHat 創設者のジェフ・モスさんがスピーカー数名とともに会場に来てくれたのです。 これは、当時 BlackHat JAPAN のオペレーションを担当していた篠田佳奈さん（現 CODE BLUE 事務局代表）の尽力によるものです。

Y それはさらに盛り上がりますね。

T はい。英語は話せなくても一緒に飲めば楽しいですし、プログラムコードは彼らとの共通の言語ですから、すぐに打ち解けることができました。これが好評で、翌年からは日本発を掲げるために AVTOKYO としました。2008 年は、昼夜に分けて開催しました。昼間は HackerJapan を刊行していた白夜書房のホールを借りてプレゼンテーション中心のデイ・セッションを行い、夜は「no drink, no hack」をスローガンに掲げてアフター・パーティを行いました。翌年からは、飲みながら・食べながら参加できる形とし、クラブを貸し切って開催する現在のようなスタイルになったのは 2011 年からです。

Y 企業の協賛を受けないのは、ポリシーがあるのでしょうか。

T コミュニティ主導でベンダーニュートラルとしたいという方針があるからです。実は、これまでに何度か企業スポンサーについて検討はしていますが、その度に「なしで頑張ろう」ということとなり現在に至っています。その代わり、AVTOKYO の主旨に賛同いただける方に、個人スポンサーとして支援をお願いしています。

Y 個人スポンサーには、どのようなメリットがありますか。

T これまでは、スペシャルお土産アイテムをお渡ししたり、参加バッジが豪華になっていたり、会場でスポンサー名を掲載したりというものです。あとはイベント後のスタッフの飲み会に招待して

AVTOKYO 歴代イベントバッジ。一部は Booth などで販売されている（写真提供：tessy さん）

交流できるといったことも行っています。

Y AVTOKYO といえば、毎年凝ったバッジが作られていますが、こちらについて教えてください。

T バッジは毎回オリジナルで、DEFCON のような凝ったものを作っています。電子工作などが得意な人たちが作成しています。大抵予算をオーバーするのですが（笑）。過去にはサコシュを入場バッジにしたこともありました。これは、アナログレコード盤を入場バッジとした DEFCON を越えて世界最大のカンファレンスバッジとなりました（笑）。もちろん、今年も世界初に挑戦します。

Y AVTOKYO のグッズ販売ページ※3 でサコシュを含めてさまざまな商品が販売されていますが、入場バッジも販売したら売れるのではないでしょうか。

T 実は過去のバッジは在庫のあるものは Booth（創作物のマーケット）で販売をしています※4。

Y 長年運営を続けてきて参加者に変化はありますか。

T 若い世代の参加者が増えるとともに、新規の参加者も増えています。これはセキュリティに仕事で関わる人が増えてきたからではないかと思います。また、AVTOKYO では、講演に限らずワークショップなども公募していて、近年、こちらへの応募も増えています。

Y 参加者に限らず、AVTOKYO に関心を寄せる人が増えているということですね。講演応募の倍率はどれくらいですか。また、特徴のあるワーク

※3 **AVTOKYO SWAG** https://suzuri.jp/avtokyo
※4 **AVTOKYO - Booth** https://avtokyo.booth.pm/

ショップなどがあれば教えてください。

T 講演の公募は、例年 2 倍ほどの競争率です。内容はテクニカルなものから「ネタ」的なものまで幅広くなっています。酔っている参加者の前での講演は難しいと思います。ワークショップの方は、ハンダ付けのようなハードウェアを扱ったモノや、BlackHat ARSENAL のようなツールの紹介、あと例年 Open xINT CTF が開催されています。

Y 話はそれますが、Open xINT CTF を主催する pinja は、今年 DEFCON で開催された OSINT CTF（Recon Village CTF）で見事優勝を果たしましたね※5。

T はい。本当に快挙ですね。AVTOKYO の Open xINT CTF は、この 3 年ほどはコロナ禍でオンライン開催でしたが、それ以前は現地会場で開催していました。答えとなるフラグを会場や渋谷の街から探し出すなど、趣向が凝らされていました。

Y AVTOKYO 2023 の目玉など、公開できる情報はありますか。

T 今年はロックピッキング的な企画をやりたいと考えています。物理的な鍵のハッキングですね。ただし、日本では一般の人がピッキングツールを所持することは違法にあたるため、鍵穴を探りながらブランクキーを削るワークショップを検討しています。これなら単なる金属加工ですから。

Y かなり攻めた企画ですね。期待しています。

T 他には、前述した Open xINT CTF の開催も決定しています。先日の企画会議では、イベントを通じて「縁日感を出そう」ということで話がまとまったので、きっと楽しいものになると思います。また、今年は久々に前夜祭を開催しようかとも考えています。参加者が来ない可能性もありますが、他ではできない「濃い話」をする場にしたいですね。あわせて、開催当日のアフター・パーティの規模縮小も検討しています。まあ、飲みに行かないということはありませんが（笑）。

Y tessy さんにとって、イベント運営の醍醐味は何ですか。

T 毎年、企画をスタートする春頃はあまりやる気がないのです。一方、開催が近づくにつれて、今度は準備が大変になります。AVTOKYO は基本的に CODE BLUE などのイベントの後夜祭という位置づけですから、スタッフはイベントで働きっぱなしで、前夜はだいたい徹夜で準備することになります。ただ、AVTOKYO で皆さんがみんな楽しそうにワイワイ飲んでいるのを見るのはうれしいです。飲み会の幹事のような感覚ですね。それが終了時にピークを迎えて「終了です！また来年！」と、うっかり言ってしまうのです。「あっ、また言っちゃった」って（笑）。

Y 逆に苦労するのは、やはり準備のときですか？

T 準備も大変ですが、グッズやイベントなどの企画面でも苦労します。毎回、何か面白いことをやりたいと考えるのですが、行き詰まってしまいます。コロナ禍でリアルな飲み会がなくなり、くだらないネタが出てこなくなりました。ここ数年、企画面では悶々としていましたが、先日、久しぶりにスタッフが集まり飲み会をしたところ、くだらない話がどんどん出てきました。やはり、対面で人と会うのは重要です。

AVTOKYO がなくなっても、やりたい人が新たな「場」を作ればいい

Y 今後、AVTOKYO をどのようにしていきたいですか。例えば、10 年後も続けていますか。

T 先のことはわかりませんが、「もうやめようかな」という考えは常にあります。運営が大変なので、少しでも楽にするために同じような仕組みに

※5 **優勝してきたぜ！ ハッカーイベント「DEF CON」OSINT CTF 体験記（ASCII）** https://ascii.jp/elem/000/004/158/4158573/

しているのですが、そうすると刺激がなくなってしまうのです。ただ、AVTOKYO を誰かに引き継ぐということは考えていません。なくなったときに、今度は誰かが新しいものを自由に作ればよいと思っています。

Y そうした考えの背景にはご自身の性格が影響していると思いますか。

T そうかもしれません。個人的には、好きなことは仕事に限らずやっていく人生が目標です。一方で制約を受けたり縛られたりすることは嫌なのです。わがままなのだと思います。

Y バイク（自転車）も海外遠征なさったりしていますね。

T 自転車は、社会人になったときに参加したトライアスロンがきっかけです。大学時代に、山登りか岩登りかトライアスロンをやりたいと、漠然と思っていました。それまで文科系だったのに。その後、北海道で山登りをしたので、社会人になってトライアスロンに参加しました。最近また自転車にはまっていて、コロナ禍では ZWIFT（バーチャルサイクリングサービス）を始めて、体重が 10kg 落ちました。今年は 4 年に一度フランスで開催される PBP（パリ～ブレスト～パリ）にも参加し、無事に完走しました。その 1 週間後には、ワインを飲みながらフルマラソンを走るメドックマラソンにも参加しました。

Y すごいですね。何か考えがあったのですか？

T 人生を生きていくためには体力が必要だと思っていまして。仕事もそうですが、忍耐力などにはベースになる体力が必要なのではないかと、CTF に参加した頃から少し思っていたのです。強い人、続けられる人はやはりベースがあるので、それを

PBP 参加中の一枚（大会運営による撮影・販売）。tessy さん曰く「PBP は長くて楽しい 1200km でした」とのこと

心がけています。まあ、もともと体を痛めつけるのが好きなのです。山を走ったりもしましたし。

Y 強靭な体力で、ますますコミュニティを引っ張って欲しいと思います。今回はありがとうございました。

（編注：AVTOKYO の企画内容はインタビューが行われた 2023 年 9 月当時のものであり、11 月の開催時には内容が変更になることがあります）

社会のさまざまな動向を把握し、リスクの変化に対応したセキュリティ体制を構築

HISYS CSI（Cyber Security Intelligence）Watch 2023.10

文＝ SHIELD Security Research Center

カナダで可決された Online News Act について

【概要】カナダ政府は、2023 年 6 月下旬、Meta や Google などに対して、カナダに関わるニュースリンクを表示させるだけで利用料を課す法案「Online News Act」を可決した。本法案に関連して、カナダ国内での影響や諸外国への影響について考察する。

【内容】2023 年 6 月 22 日、カナダ政府は、カナダのメディアを保護する法案「Online News Act」を可決した。この法案は、Facebook、Instagram、Google ニュースなどにカナダに関わる記事が掲載される際に、プラットフォームの提供元である Meta や Google に対し、記事提供元であるカナダのメディアへ利用料支払いを義務付ける内容である。これを受け、同日に Meta は、カナダ国内の全ユーザー向けに Facebook と Instagram でのカナダに関わるニュースの提供を終了すると発表した。さらに 6 月 29 日には、Google もカナダ国内でカナダのニュースを Google 検索や Google ニュースから遮断することを発表した。

法案可決の背景には、各メディアの定期購読や広告収入が減少し、デジタルプラットフォームへシフトしている状況を鑑みて、プラットフォームとメディアの経済的公平性を確保する目的がある。カナダ政府は、大手 IT 企業が彼らのプラットフォームに無償でニュースを掲載することで、ユーザーを集めて膨大な広告利益を得ていると懸念している。一方、この法案に対して、Meta や Google は懐疑的である。なぜなら、Google は多くのメディアに「ニュースショーケースプログラム」を無償で提供しているからだ。このプログラムでは、提供元ごとに「パネル」で記事が表示され、ニュースの提供元が自ら記事を直接届けられたり、記事の掲載方法やブランディングをコントロールしたりすることができる。これを利用することで、読者をニュースの提供元の Web サイトに誘導でき、双方の関係性を深める役割をしていると考えるからだ。さらに、Google は、このプログラムでカナダのメディアは年間 250 億円の収益を上げると試算している。また、Meta も同様に、プラットフォームにニュースを載せることでカナダのメディアは約 230 億円の広告収入を得ていると主張している。

2023 年 7 月初旬、この法案の可決を受けて、Meta が運営する Instagram において、一部のユーザー向けにカナダのニュース表示が試験的に削除された。削除の対象には、以前検索、フォローしたニュースのコンテンツも含まれている。また、Google は、Meta と同様に 12 月 19 日までにはニュースページへのアクセスを停止する予定だが、緊急性の高い情報については対象外とする姿勢だ。2021 年、オーストラリアでも同様な法律が可決され、Meta が一時的にニュースへのアクセスを停止した時期があった。しかし、後に合意に至り、Meta と報道機関の間でコンテンツ取引が成立したためカナダも同様の道を辿るかもしれない。

一方、この法案は、カナダの管轄外の仲介業者にも影響を与える可能性がある。例えば、インターネット上のサービス運営者は、カナダからのユーザーやニュースコンテンツのためにサービスの仕組みを変更する可能性もある。その結果、インターネット上のサービスは、カナダ国内外で別の仕様で機能し、諸外国と比べてカナダ国内のユーザーは関連したコンテンツへのアクセスが減少する。この状況がビジネスに不利に働くと考える企業は、事業やサービスをカナダから撤退し、法律遵守のコストを回避することを検討するだろう。今後この法案がどうカナダ国内で施行、運用されていくのかは確認していく必要がある。

［情報源］ https://www.cbc.ca/news/editorsblog/cbc-online-news-act-1.6897060

セキュリティツールを実践的に紹介する連載企画

Let's Try Windows システム確認！

2. プロセス確認編

文＝ SHIELD Security Research Center

1. はじめに

本稿は、各種セキュリティツールを実践的に紹介する連載企画です。前号より第二部「Windows システム確認」と題し、Microsoft 社が提供する「Sysinternals Suite」として利用可能な、いくつかのツールの使い方を確認します。

「Sysinternals Suite」は、多数のトラブルシューティング ユーティリティをまとめたバンドルです。誰でも無償で利用することができ、Windows マルウェアの動的解析などにも利用可能なツールです。

「Sysinternals Suite」を有効活用することで、コンピューターに感染した Windows マルウェアを見つけ出したり、Windows マルウェアの挙動を確認したりすることができます。

一方、「Sysinternals Suite」が動作するコンピューターでは、活動を停止する Windows マルウェアも存在します。

「第二部　Windows システム確認」は次の 3 部構成となっています。

1. 自動起動プログラム確認編
   Autoruns を利用して、Windows の自動起動プログラム設定を確認します。

2. プロセス確認編
   Process Monitor を利用して、Windows 上で起動するプロセスの動きを確認します。

3. ネットワーク状況確認編
   TCPView を利用して、Windows 上でのネットワーク状況を確認します。

今回は、「2. プロセス確認編」として、Windows プロセスのアクティビティ（挙動）の確認方法を解説します。マルウェアの挙動確認、マルウェアの感染確認（ロードされる DLL として）などに利用可能となります。

本稿の安全性には留意していますが、安全を保証するものではございません。
OA 端末（社内ネットワーク接続機器）で実施するのではなく、分離された回線内および機器を利用することを推奨いたします。

なお、本稿は「自動起動プログラム確認編」と同様、Windows Sandbox を利用した手順での解説を予定しておりましたが、Windows Sandbox 上では「Process Monitor」の動作が不安定であることを確認しております。そのため、今回の「プロセス確認編」では、ローカル環境（専用マシーン）または VMWare などの仮想環境を用いて実践することをお勧めいたします。

2. 準　備

2.1 Process Monitor の準備

「Process Monitor」とは、「Sysinternals Suite」に含まれる、Windows で実行中プロセス（プログラム）の挙動を確認するためのツールです。
「Process Monitor」および「Sysinternals Suite」は下記などから、ダウンロードすることができます。

・「Process Monitor」
https://learn.microsoft.com/ja-jp/sysinternals/downloads/procmon
・「Sysinternals Suite」
https://learn.microsoft.com/ja-jp/sysinternals/downloads/sysinternals-suite

今回は、筆者は Procmon64.exe を利用します。読者の皆様は、利用されている環境に合わせて、選択してください。

Eula.txt	テキスト ドキュメント	4 KB	無	8 KB	59%	2023/06/27 16:54
procmon.chm	コンパイルされた HTML ヘル...	55 KB	無	63 KB	12%	2023/06/27 16:55
Procmon.exe	アプリケーション	1,657 KB	無	5,133 KB	68%	2023/06/27 16:55
Procmon64.exe	アプリケーション	866 KB	無	2,651 KB	68%	2023/06/27 16:55
Procmon64a.exe	アプリケーション	796 KB	無	2,688 KB	71%	2023/06/27 16:55

2.2 Putty の準備

「Putty（パティ）」は、Simon Tatham が MIT License（オープンソースソフトウェアライセンスの一種）で開発・公開しているリモートログオンクライアントです。
後ほど、「Putty」を使った確認手順がありますので、準備をしておきます。ソフトウェアは以下の URL よりダウンロードできます。

・「Putty」
https://putty.org/

筆者は下記、64-bit x86 binary file をダウンロードしました。ご自身の環境に合わせてダウンロード、ご準備してください。

Alternative binary files

The installer packages above will provide versions of all of these (except PuTTYtel an

(Not sure whether you want the 32-bit or the 64-bit version? Read the FAQ entry.)

`putty.exe` **(the SSH and Telnet client itself)**

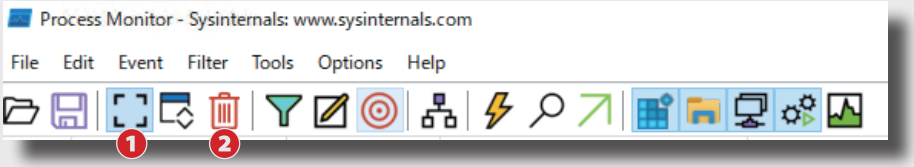
64-bit x86:　`putty.exe`　(signature)

3. プロセス（プログラム）の確認

3.1「Process Monitor」の起動テスト

「Process Monitor」を起動します。

「Process Monitor」を起動すると、プロセスのアクティビティが大量に記録され始めます。Windows のさまざまなプロセスは常に動作を続けているため、このままでは、大量のアクティビティが記録されることとになります。いったん、図のボタン❶を押下し記録を停止し、ボタン❷を押下しこれまでに記録されたアクティビティを削除します。



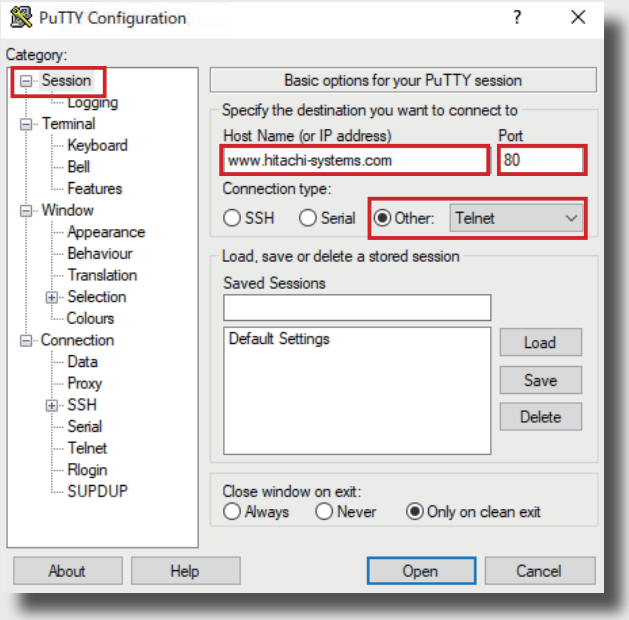
アクティビティを削除したら、起動テストは完了です。

3.2 Putty の起動、リモートサイトへの Telnet（HTTP 接続）テスト

次に、「Putty」を利用した Telnet（HTTP 接続）のテストを実施します。

準備した「Putty」を起動します。

図の通り、Session タブの Host Name に「www.hitachi-systems.com」、Port に「80」を入力し、Connection Type を Other で「Telnet」を選択し、Open ボタンを押下します。



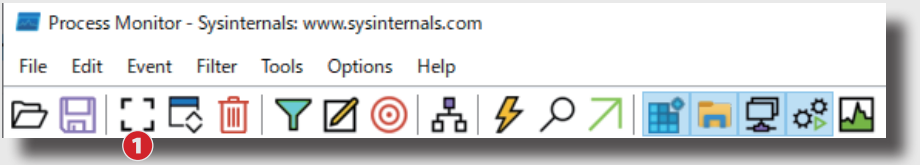
起動すると、黒いプロンプト画面が表示されます。

プロンプトが表示されましたら「GET . HTTP/1.1」を入力します。これは、Web ページなどにアクセスした際に、通常ブラウザーが行っている HTTP リクエストのうちの、リクエストラインを表しています。

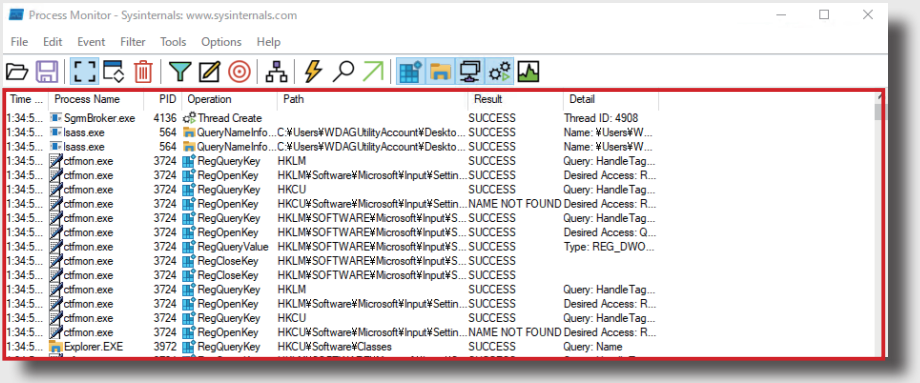
入力後、「Enter」を押し、HTTP レスポンスが一瞬だけ表示され（表示が見えない場合もあります）、プロンプト画面が閉じたら、確認は終了です。
HTTP レスポンスがいつまでも返ってこない場合には、通信路上に問題がある可能性がありますので、確認してください。
なお、HTTP レスポンスの内容については、確認をする必要はありません。

3.3 アクティビティの記録

それでは実際に、「Process Monitor」を用いて、「Putty」のプロセスのアクティビティを記録してきます。図のボタン❶を押下し、「Process Monitor」によるプロセスのアクティビティの記録を開始します。

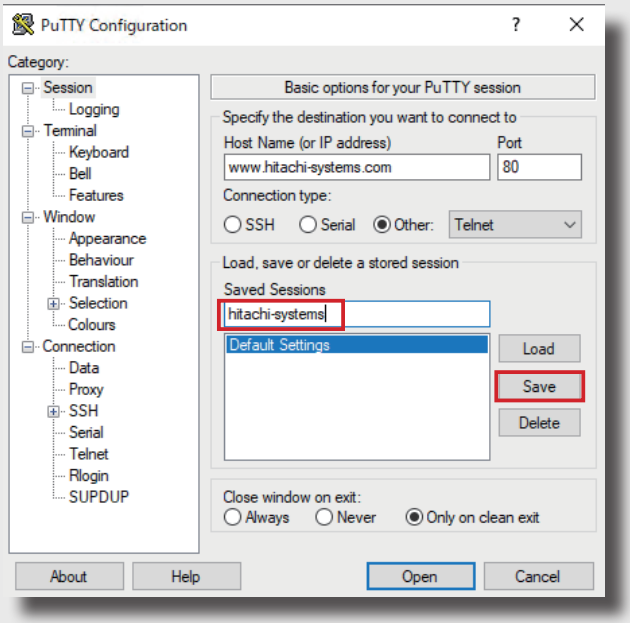


下図のようにアクティビティの記録が始まっていることを確認します。

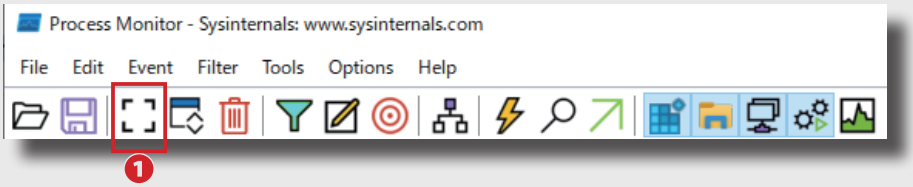


Time ...	Process Name	PID	Operation	Path	Result	Detail
1:34:5...	SgmBroker.exe	4136	Thread Create		SUCCESS	Thread ID: 4908
1:34:5...	lsass.exe	564	QueryNameInfo...	C:¥Users¥WDAGUtilityAccount¥Deskto...	SUCCESS	Name: ¥Users¥W...
1:34:5...	lsass.exe	564	QueryNameInfo...	C:¥Users¥WDAGUtilityAccount¥Deskto...	SUCCESS	Name: ¥Users¥W...
1:34:5...	ctfmon.exe	3724	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
1:34:5...	ctfmon.exe	3724	RegOpenKey	HKLM¥Software¥Microsoft¥Input¥Settin...	SUCCESS	Desired Access: R...
1:34:5...	ctfmon.exe	3724	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...
1:34:5...	ctfmon.exe	3724	RegOpenKey	HKCU¥Software¥Microsoft¥Input¥Settin...	NAME NOT FOUND	Desired Access: R...
1:34:5...	ctfmon.exe	3724	RegQueryKey	HKLM¥SOFTWARE¥Microsoft¥Input¥S...	SUCCESS	Query: HandleTag...
1:34:5...	ctfmon.exe	3724	RegOpenKey	HKLM¥SOFTWARE¥Microsoft¥Input¥S...	SUCCESS	Desired Access: Q...
1:34:5...	ctfmon.exe	3724	RegQueryValue	HKLM¥SOFTWARE¥Microsoft¥Input¥S...	SUCCESS	Type: REG_DWO...
1:34:5...	ctfmon.exe	3724	RegCloseKey	HKLM¥SOFTWARE¥Microsoft¥Input¥S...	SUCCESS	
1:34:5...	ctfmon.exe	3724	RegCloseKey	HKLM¥SOFTWARE¥Microsoft¥Input¥S...	SUCCESS	
1:34:5...	ctfmon.exe	3724	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
1:34:5...	ctfmon.exe	3724	RegOpenKey	HKLM¥Software¥Microsoft¥Input¥Settin...	SUCCESS	Desired Access: R...
1:34:5...	ctfmon.exe	3724	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...
1:34:5...	ctfmon.exe	3724	RegOpenKey	HKCU¥Software¥Microsoft¥Input¥Settin...	NAME NOT FOUND	Desired Access: R...
1:34:5...	Explorer.EXE	3972	RegQueryKey	HKCU¥Software¥Classes	SUCCESS	Query: Name

次に、3.2 で実践した「Putty」を用いた Telnet 接続（HTTP 接続）を、今一度実施します。
この時、次のように、「Saved Sessions」に「hitachi-systems」と入力し、「Save」ボタンを押下してから、Open ボタンを押下してください。

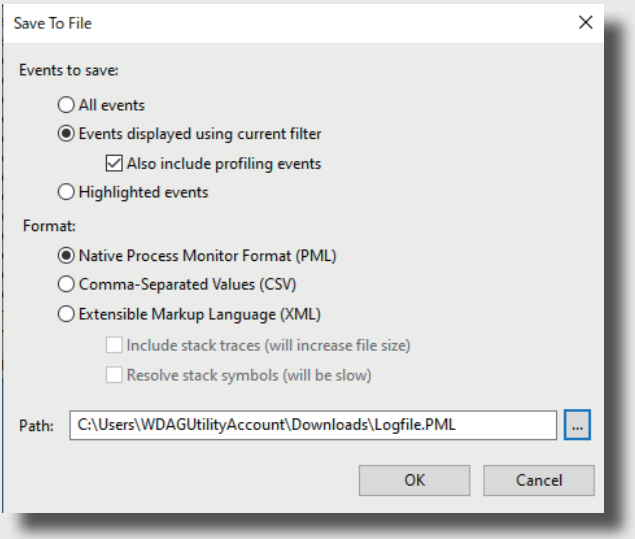


Telnet 接続が完了したら、下記のボタン❶を押下し、「Process Monitor 」によるプロセスのアクティビティの記録を停止します。



3.4 アクティビティの保存

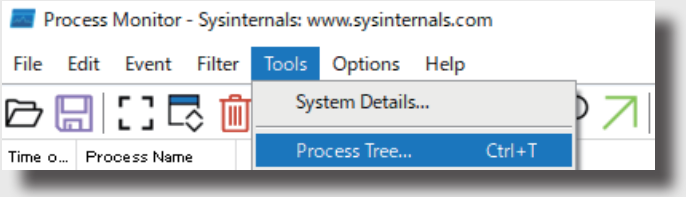
次に、アクティビティをログとして保存します。
メニューバー「File->Sava」を選択すると、Save To File ダイアログが開きます。保存する場所「Path」を適宜変更し、OK ボタンを押下して保存します。
設定項目がいくつかありますが、今回はデフォルト設定（初期状態）で問題ありません。



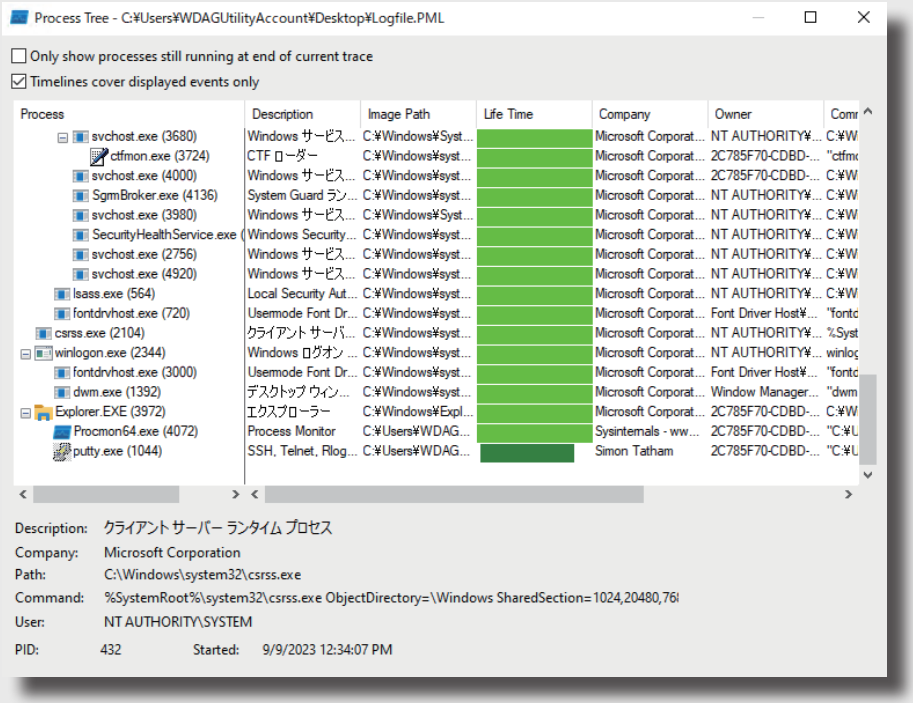
3.5 プロセスツリーの確認

「Process Monitor」は、Windows で動作している多くのプロセスに関わるアクティビティを記録します。そのため、必要な情報のみに絞って確認することが必要となります。その 1 つの方法が、画面出力内容のフィルター機能です。
フィルターを設定する方法はいくつかあるのですが、今回はもっとも簡単な手法として、プロセスツリーを用いて、確認を行いたいプロセス「Putty」の特定を行い、フィルター設定を行ったうえでアクティビティを確認していきます。

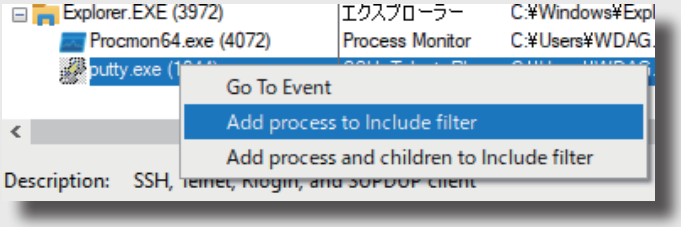
「Process Monitor 」のメニューバーより、「Tools->Process Tree」を選択します。



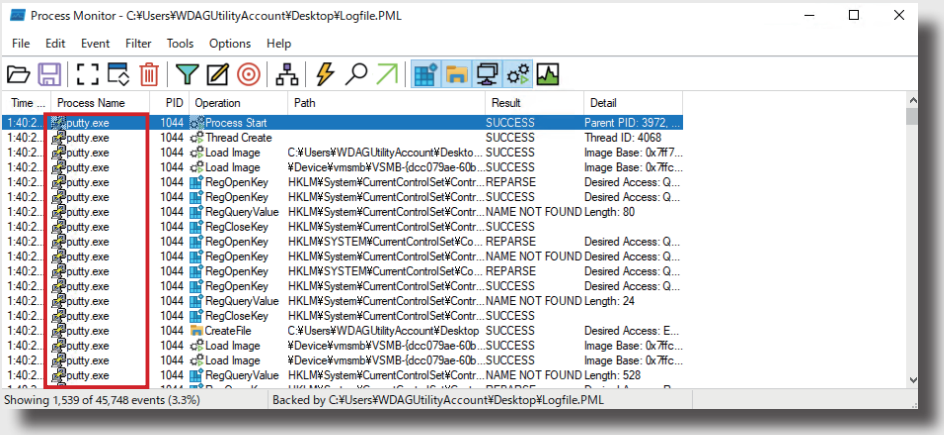
「Process Tree」を開くと下記のような画面が表示されます。時系列で起動していたプロセスを確認することができ、プロセスの親子関係も確認できます。



プロセスツリーより、「Putty」をさがし、右クリックから「Add Process to Include filter」を選択します。

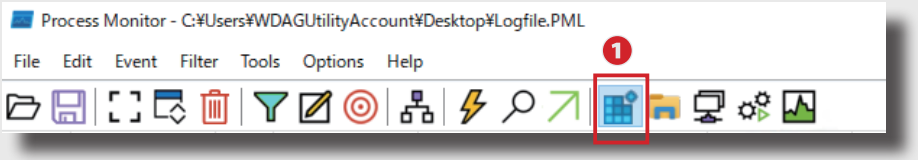


選択が終わると、PID（プロセス ID）でフィルターに追加が行われます。「Process Monitor」の画面上に「Putty」のアクティビティのみが表示されていることを確認してください。

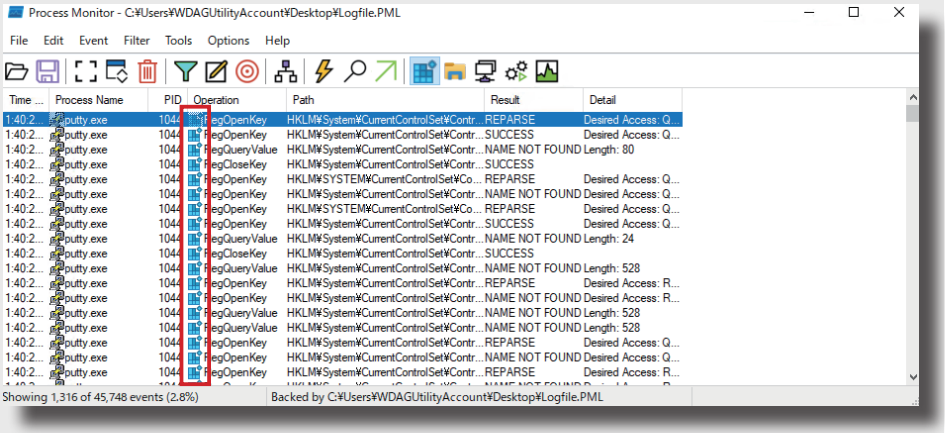


3.6 レジストリアクティビティの確認

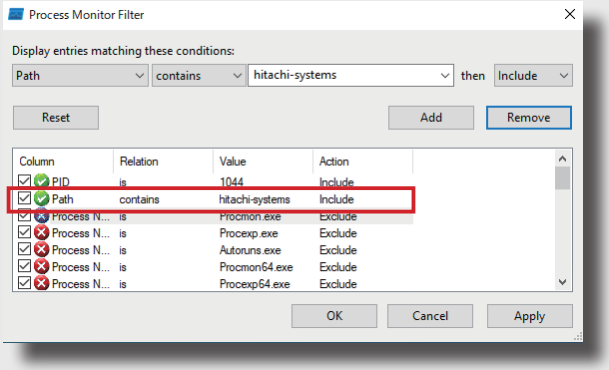
「Putty」プロセスの、レジストリに関するアクティビティを確認します。
下の図の❶のみが有効 (背景が水色) の状態となるように設定します。



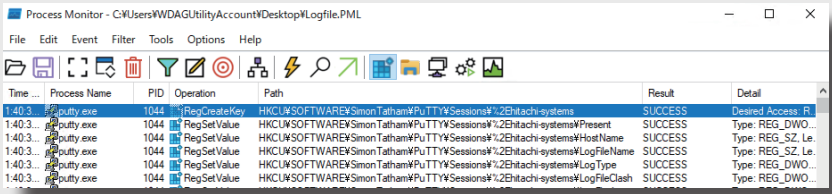
下の図と同じように、「Putty」プロセスのレジストリに関するアクティビティのみが表示されたことを確認します。



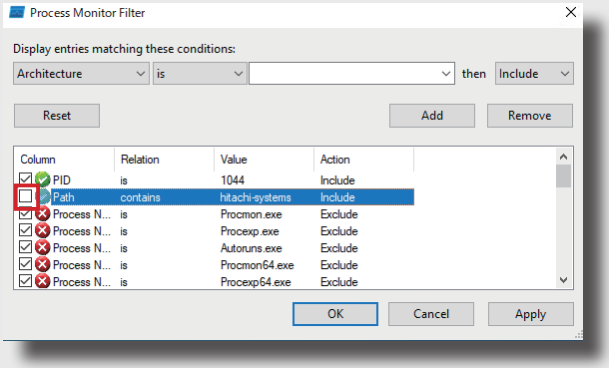
次に手動で Filter を設定します。
メニューバーの「Filter->Filter」を選択します。
その後、条件に「Path」「contains」「hitachi-systems」「then」「Include」を設定し、Add ボタンを押下し、フィルターを追加します。



フィルターを設定すると Path に「hitachi-systems」の文字列が含まれるアクティビティのみが表示されます。
そして、Path「HKCU\SOFTWARE\SimonTatham\PuTTY\Sessions\hitachi-systems」に対して RegCreateKey を行っていることが確認できます。これは、「Process Monitor」で「Putty」が保存したセッション情報をレジストリーキ―に保存する過程のアクティビティとして記録したものになります。

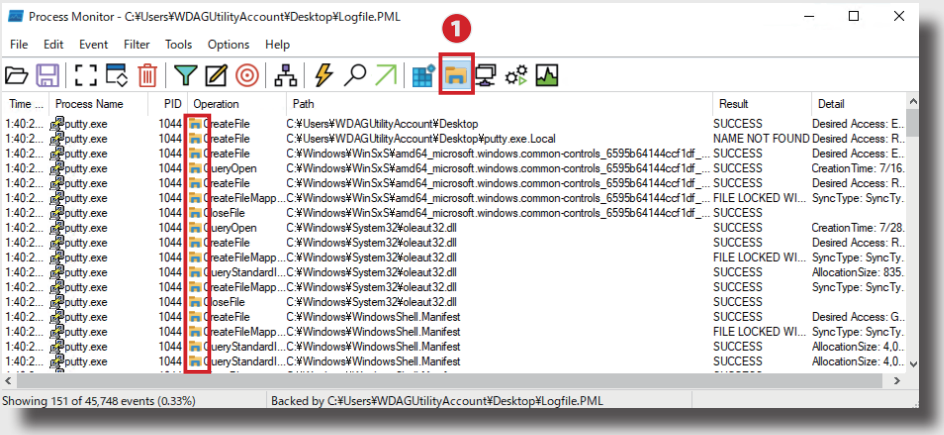


確認ができましたら、次の作業のため、設定したフィルターのチェックボックスを外し、「OK」を押下し、フィルター条件から削除してください。

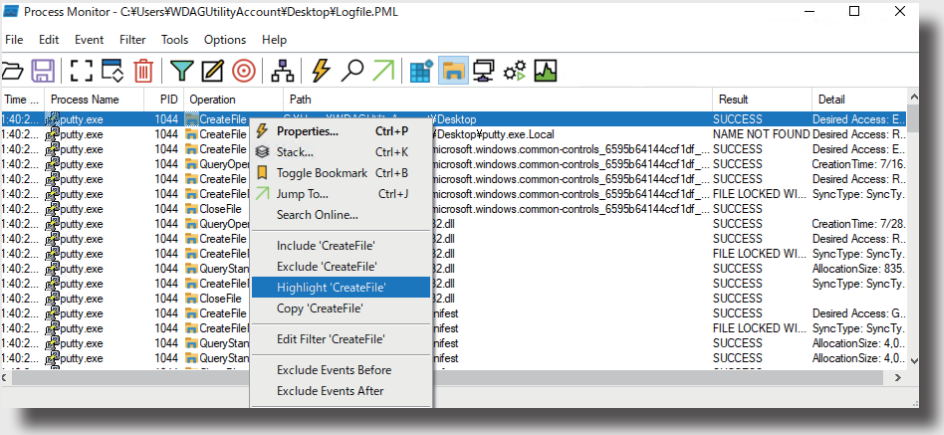


3.7 ファイルアクティビティの確認

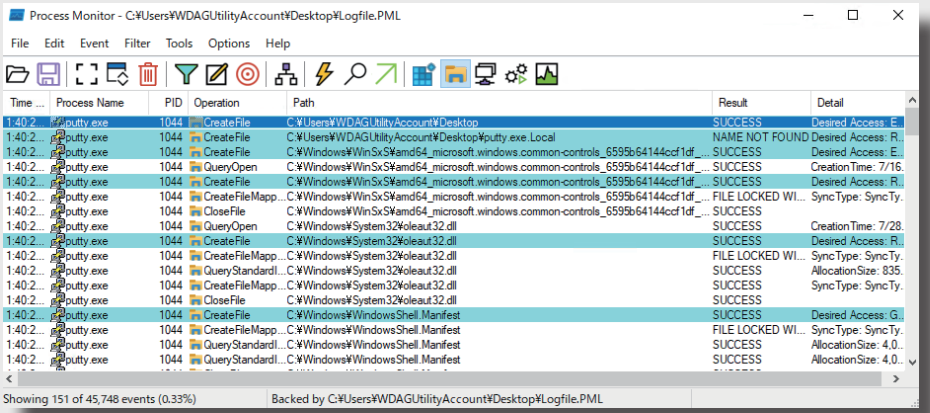
「Putty」プロセスの、ファイル操作に関するアクティビティを確認します。
次の図の❶のみが有効（背景が水色）の状態となるように設定し、「Putty」プロセスのファイルに関するアクティビティのみが表示されたことを確認します。



次に、「Operation」が「CreateFile」となっている行を探し、右クリックから「Highlight 'CreateFile'」を選択します。

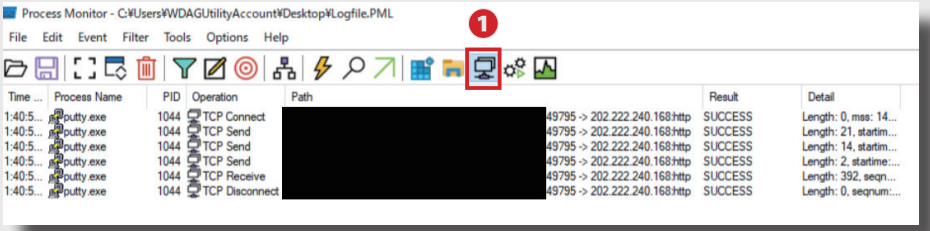


選択が終わると水色で「CreateFile」のみがハイライトなされます。フィルターとは違い、全体のアクティビティを確認しながら、着目したい箇所のみに焦点を当てる有効な手法となります。



3.8 ネットワークアクティビティの確認

「Putty」プロセスの、ネットワークに関するアクティビティを確認します。
次の図の❶のみが有効 (背景が水色) の状態となるように設定します。
また、「Putty」プロセスのネットワーク関するアクティビティのみが表示されたことを確認します。



「putty」が、「202.222.240.168」に HTTP 接続をしていることがわかります。「202.222.240.168」は、www.hitachi-systems.com に関わる IP アドレスです。「Process Monitor」が「Putty」で Telnet 接続（HTTP 接続）した通信記録を、アクティビティとして記録していることが確認できました。

6. おわりに

今回は、「2. プロセス確認編」として「Sysinternals Suite」に含まれる「Process Monitor 」を用いた、Windows プロセスのアクティビティ（挙動）の、レジストリ・ファイル・ネットワークの確認方法を確認しました。

マルウェアに感染していることがわかり、マルウェアのファイル名などがわかっている場合は、マルウェアの挙動の記録、詳細を確認することが可能です。

次回は、同「Sysinternals Suite」に含まれる「TCPView」を用いて、ネットワーク通信状況の確認方法を確認します。