HITACHI



Hitachi Systems Security Journal

VOL.81

株式会社 日立システムズ

Hitachi Systems Security Journal VOL.81

TABLE OF CONTENTS

人材育成プログラム「BoB」で結集した学生がマルチ OS ブートキット開発に挑戦
イ・ジュノ＋ソ・ヒョナ インタビュー …… 3

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
Hitachi Systems CSI（Cyber Security Intelligence）Watch 2026.09 …… 8

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 イベントログ調査
2. Hayabusa によるイベントログ調査 平常時確認編 …… 9

●はじめに

本文書は、株式会社日立システムズ の公開資料です。バックナンバーは以下の Web サイトで確認できます。
https://www.hitachi-systems.com/report/specialist/index.html

●ご利用条件

本文書内の文章等すべての情報掲載に当たりまして、株式会社日立システムズ（以下、「当社」といいます。）といたしましても細心の注意を払っておりますが、その内容に誤りや欠陥があった場合にも、いかなる保証もするものではありません。本文書をご利用いただいたことにより生じた損害につきましても、当社は一切責任を負いかねます。
Microsoft、Windows は、マイクロソフト グループの企業の商標です。
NVIDIA は、米国およびその他の国における NVIDIA Corporation の商標または登録商標です。
その他記載の会社名、商品名は、それぞれの会社の商標または登録商標です。
本文書に掲載されている情報は、掲載した時点のものです。掲載した時点以降に変更される場合もありますので、あらかじめご了承ください。
本文書の一部または全部を著作権法が定める範囲を超えて複製・転載することを禁じます。

© Hitachi Systems, Ltd. 2026. All rights reserved.



人財育成プログラム「BoB」で結集した学生がマルチ OS ブートキット開発に挑戦

イ・ジュノ ＋ ソ・ヒョナ インタビュー

サイバーセキュリティ会議「CODE BLUE 2025」U25 トラックで登壇を果たした、イ・ジュノ氏とソ・ヒョナ氏ら韓国の学生研究チーム。彼らは Windows・Linux・Android の主要 3OS を対象とした高度なブートキット研究「BOOTKITTY」を発表し、大きな注目を集めた。 最高峰の講師陣と実践的な課題を備え、世界的に高い水準の教育で韓国のサイバーセキュリティ人財を支えるトップレベル育成プログラム「BoB（Best of the Best）」での出会いから、専門知識ゼロで挑んだマルチ OS 解析の裏側、探求心と実践力を培う手厚い教育環境の中で世界に成果を届けた若きセキュリティ研究者たちの試行錯誤と情熱が詰まったインタビューをお届けする。

撮影 ＝ 松沢雅彦／通訳 ＝ エル・ケンタロウ／取材・文 ＝ 斉藤 健一

CODE BLUE のユース枠で韓国の学生が研究発表

2025 年 11 月に開催された CODE BLUE 2025、U25（25 歳以下）トラックにて、イ・ジュノ氏とソ・ヒョナ氏による講演が行われた。タイトルは「BOOTKITTY: ブートキットからルートキットまでのマルチ OS 信頼チェーンの侵害」。

ブートキットとは、コンピューターの OS が起動する前の初期段階（UEFI ファームウェアなどのブートローダー）の制御権を横取りする悪意あるソフトウェアを指す。一般的なウイルス対策ソフトは OS 起動後に作動するため、OS 起動前に潜伏するブートキットの検知は極めて困難。さらに、端末を再起動してもコードが残存する高い永続性を備えており、システムの最深部から全体を制圧できる点がその最大の脅威だ。

講演者の 2 人は、韓国の国家サイバーセキュリティ人財育成プログラム「BoB（Best of the Best）」に参加した学生チームのメンバーだ。大学に通う学生 5 名とアドバイザー 3 名で構成された彼らは、BoB のプログラムにおける課題活動の一環として本プロジェクトに取り組んだ。

講演者の 2 人は、韓国の国家サイバーセキュリティ人財育成プログラム「BoB（Best of the Best）」に参加した学生チームのメンバーだ。BoB は最高峰の講師陣と実践的な課題を備え、世界的に高い水準の教育で韓国のサイバーセキュリティ人材基盤を強力に支えるプログラムである。受講生は最初期の約 200 名からスタートし、段階的な課題や評価を通じて 30 名、最終的にはわずか 10 名にまで厳しく絞り込まれていく。彼らはその極めて厳格な選抜プロセスの中で過酷な切磋琢磨を経て実力を磨き上げ、大学に通う学生 5 名とアドバイザー 3 名で構成された優秀なチームとして本研究を進めた。

マルチ OS 環境における信頼チェーンの弱点を解明した彼らはいかにしてこの成果を成し遂げたのか。専門知識ゼロからのスタート、研究室での試行錯誤、そして未来への展望まで、彼らの生の声をお届けする。なお、インタビューは英・韓・日の 3 言語で進行したが、日本語がわかるソ・ヒョナ氏を中心に話を進める形をとった。

トップ人財育成プログラム『BoB』でのチーム結成と、ゼロからの研究スタート

斉藤（以下 S）本日はよろしくお願いいたします。CODE BLUE U25 での発表、拝見しました。はじめ



●イ・ジュノ（Junho Lee 写真右）

韓国、木浦大学校の学部生。UEFI やファームウェアなどの低レベル技術に焦点を当てている。BoB（Best of the Best）でのブートキットプロジェクトを通じて「Linux 向け初の UEFI ブートキット」を開発・実証し、高度な UEFI 専門知識と多様な攻撃・防御技術の実装能力を示した。同プロジェクトを主導し、Windows、Linux、Android 環境におけるセキュリティメカニズムのバイパス手法を解明するとともに、実践的なぜい弱性分析の経験を深めた。 これらの経験を基盤とし、低レベル領域のぜい弱性分析やシステムセキュリティ強化において、学術界および産業界の双方に有意義な貢献をめざしている。

●ソ・ヒョナ（HyunA Seo 写真左）

韓国、誠信女子大学校の学部生。システムセキュリティとぜい弱性分析を専攻している。低レベルシステムセキュリティを強みとし、システムハッキングやリバースエンジニアリング、ファームウェアおよび組み込みシステムの解析に取り組んでいる。 ブートプロセスの操作や信頼チェーンのバイパス、カーネル分析、UEFI エクスプロイトといった最深部の攻撃・防御技術を研究。実践的な実験と技術分析を通じてぜい弱性を特定し、ソフトウェアとハードウェアの両領域においてシステム基盤のセキュリティ向上をめざしている。

に、今回の研究チームの成り立ちや概要についてお聞かせいただけますでしょうか。

ソ・ヒョナ（以下 H）本研究は学生 5 人のチームで進めました。私たちは韓国の国家サイバーセキュリティ人財育成プログラム『BoB（Best of the Best）』で出会ったメンバーで、チームのほかに 3 名のアドバイザーの方々にもサポートしていただきました。

S 5 人の皆さんは、BoB のプログラム開始当初から同じチームだったのでしょうか。

H いいえ、最初からこの 5 人だったわけではありません。BoB にはチームでプロダクトを作る課題があるのですが、最初はみんな別のチームに所属していました。その後、チームの再編（解散）があり、最終的に集まった 5 人で新たにチームを結成したんです。

S BoB というのは、どのくらいの規模のプログラムなのでしょうか

H 私たちが参加した期は、当初約 200 名からスタートしました。段階的な評価をもとに成績優秀者 30 名が選抜され、その中から最終的に 10 名が最優秀者として選ばれる仕組みになっています。

S なるほど。BoB のプログラム内で最終的に集まった 5 人が、そのまま今回の研究チームになったというわけですね。発表では、UEFI ブートキットをテーマに研究されていました。UEFI は、PC やスマートフォンが OS を起動する前の段階を担う仕組みですが、その領域を狙うブートキットを研究テーマに選ばれたのは、どのような経緯からだったのでしょうか。

H このテーマは、アドバイザーであるメンターの方から提案していただきました。そのアドバイスを受けて、メンバー全員で話し合い、UEFI ブートキットの研究に取り組むことに決めたんです。

S テーマが決まった当時、メンバーの皆さんは UEFI についてどの程度の知識があったのでしょうか。

H 最初から知識があったわけではありませんでした。テーマが決まってから、まずは『UEFI とは何か』という基本的な仕組みを学ぶところからスタートしたんです。勉強も各自でバラバラに進めるのではなく、5 人で一か所に集まって、一緒に理解を深めていきました。



2 人の講演は、CODE BLUE 2025 のアーカイブから視聴することができる。講演では、イ・ジュノ氏がブートキット全体と Linux 版の解説を担当。Android 版の解説はソ・ヒョナ氏が行なっている。
https://archive.codeblue.jp/2025/results/results/#result-27

S 研究をスタートされた段階では、具体的にどのような目標を設定されていたのでしょうか。

H 最初は、まずブートキットを 1 つ作成することを目標に設定しました。そのために必要な技術要素を洗い出しながら、各自がやりたい領域を主体的に担当して進めていきました。技術面はリーダーの彼（イ・ジュノ氏）が統括し、私は主に発表用のスライド資料作成やデモの準備などを担当しました。

S メンバーそれぞれの自主性と強みを生かした役割分担だったのですね。

ブートキット開発における課題と試行錯誤のプロセス

S 今回の研究では、Linux、Windows、Android の 3 つの OS を対象にされていましたね。この開発には、全体でどのくらいの期間がかかったのでしょうか。

H 全体で約 4 カ月間です。Windows、Linux、Android の各 OS 向けの開発に、それぞれおよそ 1 カ月ずつを費やしました。

S 3 つの OS の中で、特に開発や検証に苦労されたものはありましたか。

H 3 つの中では、特に Android 向けの設計が一番難しかったですね。

S Android はセキュリティ保護が非常に強力で、通常はジェイルブレイク（脱獄）しないとシステ



ソ・ヒョナ氏が日本語を話せることからインタビューでは主に彼女が対応している

ム内部を変更できないイメージがあります。そのあたりの保護機能には、どのように対処されたのでしょうか。

イ・ジュノ（以下 J）Android の保護機能を回避するために、2024 年に公表された 2 つの CVE（ぜい弱性）を利用しました。そのぜい弱性を突くことでプロテクトをバイパスできたため、事前にジェイルブレイクを行わなくてもブートキットを実行することができたんです。

S ブートキットをインストールする際の条件には、ターゲットとなる OS ごとにどのような違いがあったのでしょうか。

J Linux と Windows は、実機に直接触れなくてもリモート経由で実行することができます。一方で、Android に関しては PC と端末を物理的にケーブルで接続して作業する必要がありました。

S 対策を考えるうえでは、ターゲットとなる OS ごとに着目すべきポイントや防御のアプローチが変わってくるのでしょうか。

J Android に関しては、端末に物理的に接触・接続されないように物理セキュリティを確保することが有効な対策の 1 つになります。一方、Linux と Windows ではセキュアブートを有効化しておくことが最も重要な対策です。

S 一口にブートキットと言っても、ターゲットとなる OS の構造や保護機能によって、アプローチや難易度がまったく変わってくるのですね。ブートキットを実際に動作させるまでには、かなりの試行錯誤があったかと思います。一連の開発の中で、特に難しかったのはどのような点でしたか。

H いちばんの苦労は、参考にできる資料や先行研究が非常に少なかったことです。単に『ぜい弱性が存在する』ということと、『それを実際にブートキットとして動作させる』ことの間には大きな壁があり、自分たちのアイデアで一から形にしていく必要がありました。実装に関しても特定のメンバーだけに任せるのではなく、5 人全員で議論を重ねながらチームで進めていきました。

S 資料が少ない中で進めるのは本当に大変だったと思いますが、自分たちの手でゼロから形にしていく面白さも感じられたのでしょうか。

H はい、苦労した分だけすごく面白かったですね。

S 発表資料の中にあった Linux の USB デモ動画では、背景に研究室のようなスペースが映っていましたね。実際にも、そういった研究室や作業スペースに集まって開発を進められていたのでしょうか？

H はい、私たちの研究室です。

S デモ動画のリアルな作業環境からも、メンバーの皆さんが試行錯誤を重ねながら研究を進められていたことが伝わってきました。

研究成果の発表と今後の展望

S 今回の研究成果は、BoB プログラム内のみならず外部のコミュニティへも展開されたそうですが、具体的には、どのような機会や場で成果を発表・共有されたのでしょうか。

H BoB 内での成果発表にとどまらず、論文執筆や国際会議への参加を通じて海外へも研究成果を共有していきました。具体的には、セキュリティ分野のトップカンファレンスである USENIX への論文投稿などを行いました。

S BoB では、プロジェクトの終了後にも継続して教育や試験（選抜）が実施されると伺いました。研究完了後の活動には、どのように関わっていかれたのでしょうか？

H プロジェクトが終わった後も引き続き講義や試験が続いていました。ただ、私たちは研究成果を論文や資料としてまとめる作業に集中していたため、その後の試験対策や準備には十分な時間を割くことができませんでした。

S 研究成果をしっかりドキュメント化して外部へ発信することに、多くの時間とエネルギーを注が

れたわけですね。そうした発信活動の一環として、CODE BLUE U25 に応募されたきっかけは何だったのでしょうか

H 応募は、私たちのチームで決めました。25 歳以下の若手研究者を対象とした U25 という募集枠があることを知り、自分たちの研究成果を試すために応募してみようとなったんです。

S 採択の通知を受け取ったときは、率直にどのようなお気持ちでしたか。

H 本当に嬉しかったですね。国際的な舞台で発表できる貴重な機会を得られたことが、光栄でした。

S 今後はどのようなテーマや領域の研究に取り組んでいきたいと考えていますか

H 今後は、ブートキットを防ぐための防御・検知技術の研究に取り組んでいきたいと考えています。ブートキットの本当の危険性を多くの人に知ってもらい、こうした脅威が存在することを理解してもらえるよう発信していきたいです。

S 単に『攻撃ができる』と実証して終わりではなく、その知見をベースにして実効性のあるセキュリティ対策の研究につなげるのですね。話は変わりますが、今後の進路については、どのように考えていますか。やはり将来はセキュリティ分野の研究者をめざしているのでしょうか。

H はい。現在は大学（学部）に在籍しているのですが、卒業後は大学院の修士課程に進学したいと考えています。将来は研究者として活躍するのが目標です。



大学院に進学し、将来はセキュリティ研究者をめざしたいと語る 2 人

J 私も大学院修士課程に進学して研究者をめざしています。ファームウェアや低レイヤーの研究したいですね。

S 最後に、これからセキュリティを学び始める学生の皆さんや、実務を通してセキュリティに関心を持っている方々へ向けて、アドバイスやメッセージをお願いします。

H 辛くても、諦めずに続けていけば大丈夫です。いつかは自分にも機会が来ると思います。それまで諦めずに頑張ってください。

S 今後のご活躍を期待します。本日はありがとうございました。

斉藤 健一（さいとう・けんいち） ハッカー専門誌「ハッカージャパン」の創刊から休刊まで（1998 年〜 2013 年）、編集長を務める。現在は、本誌の編集制作を担当する傍ら、サイバーセキュリティ国際会議「CODE BLUE」や、日本ハッカー協会が主催する「Hack Fes.」の運営にも携わっている。

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

Hitachi Systems CSI（Cyber Security Intelligence）Watch 2026.09

文＝日立システムズ

韓国 BoB に見るサイバーセキュリティリーダー人財育成の循環

【概要】韓国の BoB（Best of the Best）は、満 15 歳以上の学生等を対象とした政府主導のサイバーセキュリティ人財育成プログラムである。約 8 カ月の専門教育とプロジェクト活動を通じ、2012 年以降 2,000 名超の修了生を輩出。国際ハッキング大会の上位入賞やセキュリティ企業創業などの成果を上げている。発掘・育成・産業界での活躍など、修了生による次世代育成という循環を制度設計した点に特徴がある。この考え方は、日本の次世代セキュリティリーダー育成の参考にもなる。

【本文】サイバーセキュリティ人財不足は各国共通の課題であり、人数確保に加え、高度な専門人財をいかに発掘・育成するかが問われている。韓国では 2012 年より、次世代セキュリティリーダー育成プログラム「BoB（Best of the Best）」を実施している。運営元の韓国インターネット振興院（KISA）は、情報セキュリティをリードする人財の集中育成と、産業・安全保障など各分野の活動支援を事業目的に掲げる。

BoB の成功要因は、発掘から育成、産業界での活躍、次世代育成までの循環を制度設計した点にある。循環の起点は若い段階での発掘である。対象は韓国国籍を持つ満 15 歳以上の高校・大学・大学院生などの非在職者で、筆記・面接評価で選抜される。教育費は政府支援で無料。2026 年度は 110 名を募集し、ぜい弱性分析・企業セキュリティ・デジタルフォレンジック・セキュリティコンサルティング・セキュリティ製品開発の 5 トラックで教育を行う。7 月～翌年 2 月の約 8 カ月間、集合教育・チームプロジェクト・高度化教育を通じ、メンターとなる専門家の指導を受け実践課題に取り組む。2026 年 2 月時点で累計 2,000 名超の修了生を輩出している。

次の段階は修了生を産業界へつなぐことである。課程後半ではプロジェクト成果を事業として磨き上げる教育を実施。最終評価を経て優秀な修了生が「BEST 10」、最優秀チームプロジェクトが「グランプリ」に選ばれる。修了後も創業や技術の事業化、就職・進学などの支援が用意されている。第 4 期グランプリのアン・ウニ氏は、サイバーインテリジェンス企業 WhiteScan を創業し、2020 年に Forbes「30 Under 30 Asia」に選出。また第 8 期のヤン・ヒョクジェ氏は、課程内のクラウドセキュリティプロジェクトでグランプリを受賞し、同期とテイタムセキュリティを設立した。同社は大手セキュリティ企業などから投資を受け、韓国主要銀行を顧客に持つまでに成長。こうした先輩の成果は、次世代が BoB をめざす契機にもなっていると考えられる。

循環の最後は、修了生が次世代を育てる側に回ることである。前述のアン・ウニ氏も、現在は BoB 講師として後進育成に携わっている。BoB はこれまでも、修了後の研究会や社会貢献、才能寄付などを通じ、修了生が制度に関わり続ける仕組みを設けてきた。KISA 担当幹部は専門メディアで、BoB 同窓会をパートナーとし、後輩へのメンタリングや研究活動を公式支援する構想を示す。同幹部は修了生を国の税金で育成された人財と位置付け、大規模なサイバー侵害事故の官民合同調査などに自発参加できる道を開くとする。一方で、特定の進路を強制することはないという。

この循環を支えるため制度見直しも続く。メンター任期を 1 年とし資格を再審査する仕組みを導入したほか、現役セキュリティ企業がカリキュラム設計に参加しメンターも担うプログラムを新設。育成対象もクラウドやガバナンス、OT・ICS セキュリティなど産業界が求める領域に広げている。

各国の教育制度や産業構造は異なるため、BoB の仕組みをそのまま日本に適用はできないかもしれない。しかし、若手人財の発掘から育成、産業界での活躍、次世代育成までを一連の循環として設計する考え方は、次世代セキュリティリーダー育成の参考になる。

【情報源】https://www.kisa.or.kr/401/form?postSeq=3643

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 イベントログ調査

2. Hayabusa によるイベントログ調査 平常時確認編

文＝日立システムズ

1. はじめに

本稿は、各種セキュリティツールなどを実践的に紹介する連載企画です。前号より、「Hayabusa でのイベントログ調査」と題して、インシデント調査を行なううえで重要な情報の 1 つである Windows イベントログを、脅威ハンティングツールの Hayabusa を用いて調査する方法および観点を解説します。「Hayabusa でのイベントログ調査」は全 3 回であり、Windows イベントログの基礎から平常時ログの確認、攻撃痕跡調査の観点までを、ハンズオンを交えて段階的に理解する構成となっています。

今回の「平常時確認編」では、前号の「前編」で学んだ Windows イベントログ（以下、「イベントログ」）や Hayabusa の知識を活用し、平常時の自身の PC のイベントログをより詳細に確認します。

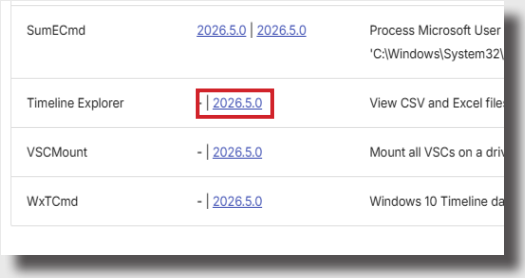
なお、本稿の安全性には留意していますが、安全を保証するものではありません。OA 端末（社内ネットワーク接続機器）で実施するのではなく、分離された回線内および機器を利用する事を推奨いたします。また、記載されている手順は意図的に無害化・簡略化していることをあらかじめご了承ください。

2. 準備

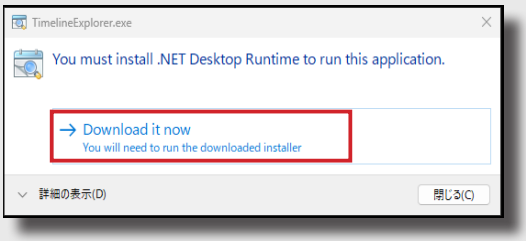
前編で利用した環境を引き続き利用します。
環境の準備ができていない場合は、前号、基本編の 2 章および 4.3 節を参考に、Windows PC と Hayabusa の準備をしてください。
今号のハンズオンでは、Hayabusa の CSV 出力結果を効率的に分析するために、Timeline Explorer を利用します。
Timeline Explorer は、ログ調査をはじめとしたデジタルフォレンジック向けに開発された CSV ビューアーです。
Excel と比較して、高速に大量データのフィルタリングや検索などの操作を行なうことができるという特長があります。
また、ログ分析では、原本の完全性を保つためにファイル自体を変更する可能性があるツールの使用は避けるべきとされていますが、Timeline Explorer はファイルを読み取り専用モードで開く仕様であるため、原本を変更する操作が発生しません。

下記のサイトにアクセスし、Timeline Explorer の最新バージョンのリンクをクリックして ZIP ファイルをダウンロードします。

https://ericzimmerman.github.io/



ダウンロードした ZIP ファイルを任意の場所に展開し、展開したフォルダーの中の TimelineExplorer.exe を実行することで起動します。（インストール不要）
なお、起動時に .NET Runtime のインストールを求められた場合は、ポップアップのボタンをクリックすることで、実行に必要な .NET Runtime のインストーラーがダウンロードされます。



ダウンロードされたインストーラーを実行し、画面の指示に従って .NET Runtime をインストールしてください。

3. 平常時のイベントログ確認（後編）

本章では、イベントログ調査において重要な観点を意識しながら、Hayabusa を用いて平常時イベントログの確認を行ない、調査時に注意すべき点を説明します。

3.1 認証・アカウント管理

認証関連のイベントは、攻撃者の侵入や横展開の可能性を推測する際に優先的に確認すべきイベントです。本節では、自身の PC における平常時のログオン傾向やアカウント利用傾向を把握し、普段アクセスしないアカウントによる認証や、通常と異なる時間のログオン、心当たりのない権限変更などの不審な兆候を確認します。

3.1.1 ログオンサマリーの確認

まず、logon-summary コマンドでログオンサマリー（ログオン関連イベントの集計表）を出力

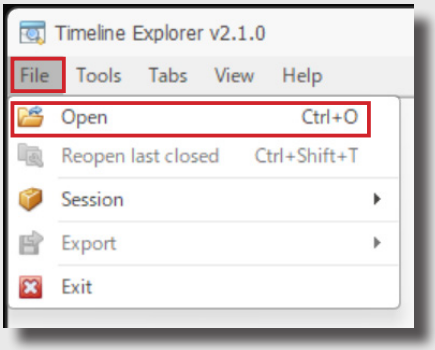
することで、ログオン関連イベントの傾向を確認します。
Hayabusa を起動するため、Windows キー +R で ファイル名を指定して実行 ダイアログを開き、「cmd」と入力後 Ctrl+Shift+Enter で管理者権限としてコマンドプロンプトを起動します。
次のコマンドを実行し、Hayabusa のフォルダーに移動します。

```
cd C:¥Tools¥hayabusa
```

次のコマンドを実行し、ログオンサマリーを CSV ファイルとして出力します。

```
hayabusa.exe logon-summary -l -o logon-summary
```

その結果、logon-summary-successful.csv（ログオン成功イベントサマリー）と logon-summary-failed.csv（ログオン失敗イベントサマリー）の 2 つの CSV ファイルが、hayabusa.exe のあるフォルダーに出力されます。
前章で起動した Timeline Explorer 画面左上の「File」から「Open」をクリックし、出力された 2 つの CSV ファイルを選択して開きます。



2 つの CSV ファイルが開かれ、タブ形式で確認するファイルを選択することができます（ログオン失敗イベントが存在しない場合はログオン成功イベントサマリーしか開きません）。
下記のようにログオンサマリーが表示されます。

logon-summary-successful.csv × logon-summary-failed.csv

Drag a column header here to group by that column　Enter text to search...

Line	Tag	Successful	Event	Target Account	Target Domain
=					
1		382	Sec 4624	SYSTEM	NT AUTHORITY
2		58	RDS-LSM 21	[redacted]	GLOBAL
3		4	Sec 4624	DWM-1	Window Manager
4		2	Sec 4624	NETWORK SERVICE	NT AUTHORITY
5		2	Sec 4624	SYSTEM	NT AUTHORITY
6		2	Sec 4624	UMFD-1	Font Driver Host
7		2	Sec 4624	LOCAL SERVICE	NT AUTHORITY
8		2	Sec 4624	UMFD-0	Font Driver Host
9		2	Sec 4624	DWM-2	Window Manager
10		2	Sec 4624	[redacted]	GLOBAL

logon-summary コマンドの集計対象は、セキュリティログのイベント ID 4624（ログオン成功）、4625（ログオン失敗）や、リモートデスクトップサービス（RDS）のログオンイベントです。

また、ログオンサマリーにある Logon Type は、認証関連イベントで記録される値であり、それぞれの数値はログオン方法を表しています。主な Logon Type の意味を以下に示します。

Logon Type	名称	意味
0	System	SYSTEM アカウント（OS など）による内部的な処理
2	Interactive	ユーザーによるコンソールログオンなどの対話型ログオン
3	Network	ネットワーク経由でのログオン
5	Service	サービスによるログオン
10	RemoteInteractive	リモートデスクトップなどのリモート操作での対話型ログオン

筆者の環境のログオンサマリーを抜粋し、以下に示します（公開不可部分は [マスク] と記載）。

件数	Event（イベント ID）	Target Account（対象アカウント）	Logon Type（ログオンタイプ）	Source IP（送信元 IP）
382	Sec 4624	SYSTEM	5 - Service	-
58	RDS-LSM 21	[マスク]	-	ローカル
2	Sec 4624	[マスク]	2 - Interactive	127.0.0[.]1
2	Sec 4625	[マスク]	2 - Interactive	127.0.0[.]1

筆者の平常時環境のログオンサマリー抜粋の表から分かることを以下に示します。
・1 行目より、ログオン成功の大半が SYSTEM アカウントによる Logon Type 5（サービス）のログとして記録されていることが分かります。

・2 行目の RDS-LSM は、RDS に関するイベントが記録されるイベントログで、Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx というファイルに保存されています。イベント ID 21 はログオン成功を意味します。
RDS-LSM は、環境によってはリモートデスクトッププロトコル（RDP）を用いた接続だけでなく、ローカルログオン時にも記録される場合があり、筆者の環境では送信元 IP がローカルとして扱われていました。

・2、3、4 行目では、マスクしている対象アカウントに正規のユーザーアカウントを示す文字列が記録されており、3、4 行目の送信元 IP にはループバックアドレス（自分自身を示す IP アドレス）である 127.0.0[.]1 などが記録されていました。

以上のことから、以下のことが推測できます。
・1 行目は、システムによるログオンに関連するイベントである。
・2、3、4 行目は、ユーザーによる正規のログオンに関連するイベントである。

しかしながら、2 行目の RDS-LSM 21 と 3 行目の Sec 4624 がユーザーによるログオン成功に関するイベントである場合、件数が 58 件と 2 件で大きく差がある点に違和感があります。

この差が生じる要因として、前編で説明した「ログの保存期間」の違いが関係していると推測できます。推測を検証するため、前編で扱った log-metrics コマンドを実行して得られる、筆者の環境での各ログの保存期間とデータサイズを以下に示します。

イベントログファイル名	件数	保存期間	データサイズ
Security.evtx (Sec)	20,684	約 2.5 日	20.0 MiB
Microsoft-Windows-TerminalServicesLocalSessionManager%4Operational.evtx (RDS-LSM)	1,649	約 94 日	1.0 MiB

前編で述べたように、筆者の環境ではセキュリティログのサイズ制限は標準設定の 20 MiB となっており、サイズ制限に達するとログローテーション（古いログの上書き）が行なわれます。
セキュリティログには、ログオンサマリー 1 行目で確認したようなシステムやサービスによる認証、監査イベントが高頻度で記録されます。そのため、ログローテーションの期間が短くなり、保存期間が約 2.5 日となっています（保存期間は記録頻度によって変動します）。

一方で、RDS-LSM は、標準設定で 1 MiB にサイズ制限されているものの比較的記録頻度が低いため、保存期間が約 94 日となっており、約 3 カ月前までのユーザーログオン成功イベントが記録されています。
これらのことから、ログオンに関するイベントの件数の差は、ログの保存期間の違いに起因していることが分かります。

このように、サイズ制限によるログローテーションが設定されていた場合、システムの状況によっては短期間でローテーションされ、目的の期間の記録が確認できない可能性があります。そういった場合に備え、セキュリティログだけではなく、他のログについても平常時の傾向を把握しておくことが重要です。

3.1.2 ログオン時間帯の確認

ログオンサマリーの確認の際に立てた、システムによるログオンとユーザーによるログオンの推測について検証するため、それぞれのログオンの時間帯の傾向を確認します。
ログオンサマリーでは、ログオン成功 / 失敗のアカウント、ログオン種別、件数といった情報が得られますが、どの時間帯にログオンしたかは分かりません。時間帯を確認するため、前編で扱った csv-timeline コマンドを実行し、得られた検知結果のタイムラインを Timeline Explorer で確認します。

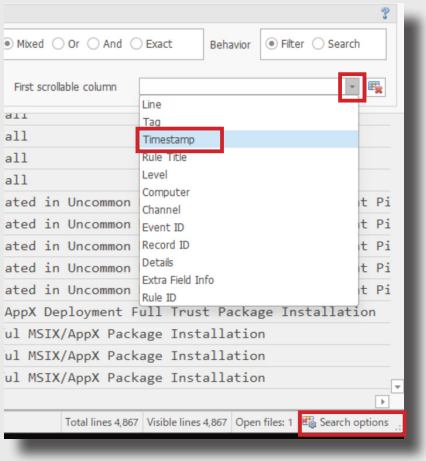
次のコマンドを実行します（実行には時間がかかる場合があります）。

```
hayabusa.exe csv-timeline -l --time-offset 7d -o normal_timeline_info.csv
```

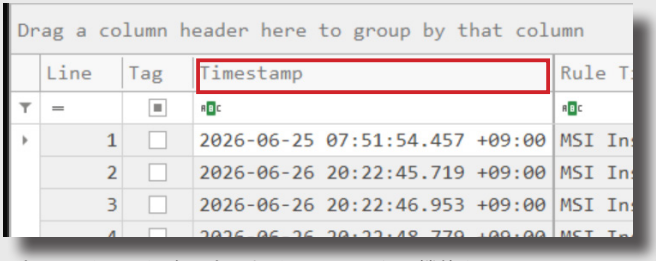
スキャンウィザード画面が表示されますが、検知ルールは「informational」以上のレベルが読み込まれる「5. All event and alert rules」を選択し、以降の選択はすべて「n」（no）を入力します。
なお注意点として、今回のように検知範囲を「informational」以上とするとタイムラインのサイ

ズが大きくなってしまうため、実際のイベントログ調査時はまず高い検知ルールのレベルに絞って確認することを推奨します。
今回は平常時のため高い検知ルールに絞ると検知数が少なく、以降のハンズオンを行ないづらくなるため、検知範囲を広げています。また、タイムラインのサイズが大きくなることを防ぐため、「--time-offset」オプションで直近 7 日間（7d）のイベントのみを対象としています。

hayabusa.exe のあるフォルダーに CSV ファイルが出力されるため、ログオンサマリーと同様の手順で Timeline Explorer で開きます。
イベントログ調査時は Timestamp に記録されている時刻を頻繁に確認するため、横スクロールしても常に確認できるように列の固定を行ないます。
右下の Search options をクリックし、上部に表示された First scrollable column のプルダウンメニューで Timestamp を選択すると固定されます。

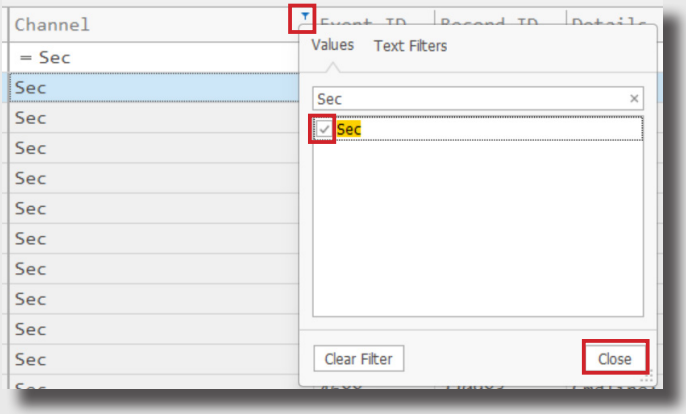


また、タイムラインは標準では Channel ごとに分かれて時系列で並んでいます。今回は Channel を区別せず時系列で確認するため、Timestamp 列ヘッダーをクリックし、昇順に並べ替えます。

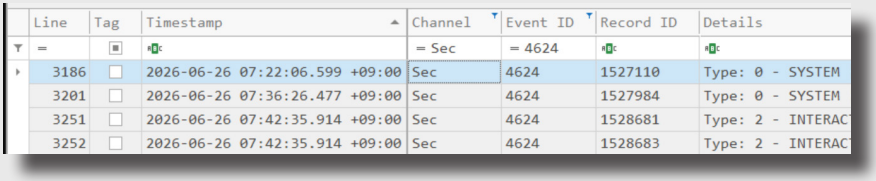


ログオンに関するイベントを確認するため、フィルター機能を用いてセキュリティログに絞り込みます。

Channel 列ヘッダー右上のフィルターアイコンをクリックし、search 欄に「sec」と入力し、Sec をチェック後、Close をクリックします。

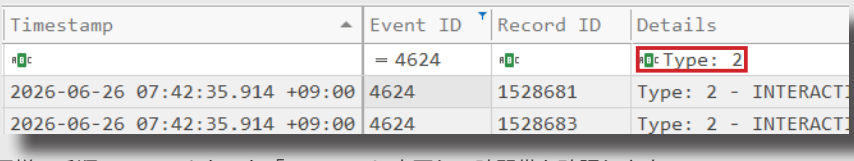


ログオン関連イベントに絞るために、同様の手順で Event ID 列で 4624（ログオン成功）、4625（ログオン失敗）のフィルターを適用します。
下記のようにログオン関連イベントが時系列で表示されます。



Line	Tag	Timestamp	Channel	Event ID	Record ID	Details
=			= Sec	= 4624		
3186		2026-06-26 07:22:06.599 +09:00	Sec	4624	1527110	Type: 0 - SYSTEM
3201		2026-06-26 07:36:26.477 +09:00	Sec	4624	1527984	Type: 0 - SYSTEM
3251		2026-06-26 07:42:35.914 +09:00	Sec	4624	1528681	Type: 2 - INTERAC
3252		2026-06-26 07:42:35.914 +09:00	Sec	4624	1528683	Type: 2 - INTERAC

ここでは、ログオンサマリーにおいてユーザーによるログオンイベントと推測した Logon Type 2 と、システムによるログオンイベントと推測した Logon Type 5 のイベントで時間帯を比較します。
Details 列に含まれる「Type: ○」が Logon Type を表すため、「Type: ○」の文字列が含まれるかどうかでフィルターを適用します。
Details 列ヘッダーの下の入力欄に「Type: 2」と入力して Enter を入力し、Logon Type 2 のイベントが記録される時間帯を確認します。



Timestamp	Event ID	Record ID	Details
	= 4624		Type: 2
2026-06-26 07:42:35.914 +09:00	4624	1528681	Type: 2 - INTERACTI
2026-06-26 07:42:35.914 +09:00	4624	1528683	Type: 2 - INTERACTI

同様の手順で、フィルターを「Type: 5」に変更して時間帯を確認します。

筆者の環境では、以下の傾向が確認できました。

・**Logon Type 2**：筆者の業務開始時間帯に集中して記録
・**Logon Type 5**：時間帯を問わず記録

これらの時間帯の傾向や対象アカウントなどの情報より、Logon Type 2 のログは筆者の業務開始時の正規のログオンに関連したイベントであり、Logon Type 5 のログは OS やサービスなどのシステムによるログオンに関連したイベントであると考えられます。

ただし、実際のログ調査においては、時間帯や Logon Type の確認だけでは推測の検証として十分とは言えないため、他の情報もあわせて確認し調査結果の精度を高めることが重要です。

例えばセキュリティログでは、Extra Field Info 列に記載されている LogonProcessName が User32 であれば対話型ログオン、Advapi であればシステム関連のログオンであることを示しており、ログオンに関する推測の裏付けに活用できます。
また、ユーザーへのヒアリングなどを通して当該時刻の業務実績を確認し、ログのタイムスタンプと照合することで、正規の操作であるかを確認することができます。
後述するプロセス ID（プロセスを一意に識別する ID）の確認なども含めて、さまざまな情報から平常時のログオン関連イベントの傾向を把握し、実際のログ調査に備えておきましょう。

3.1.3 アカウント管理操作の確認

攻撃者は、侵入後の権限維持や昇格、痕跡の隠ぺいのために、アカウントの作成 / 削除、グループ追加、ポリシー変更などのアカウント管理操作を行なうことがあります。
イベント ID 4720（アカウント作成）、4723（パスワード変更）、4724（パスワードリセット）、4726（アカウント削除）、4728（グローバルグループにメンバー追加）、4732（ローカルグループにメンバー追加）、4739（ポリシー変更）などのイベントでフィルターを行ない、アカウント管理関連のイベントを確認してみましょう。
筆者の環境では、平常時にアカウント管理関連イベントは記録されていませんでした。例として、アカウント管理操作を行なった場合に記録されるイベントを下記に示します。

Rule Title	Level	Event ID	Details
User Added To Non-Admin Global Grp	low	4728	SrcSID: S-1-5-21
User Added To Global Security Grp	med	4728	SrcSID: S-1-5-21
A Member Was Added to a Security-Enabled Global Group	low	4728	SrcSID: S-1-5-21
Local User Account Created	low	4720	TgtUser: strikep
Password Reset By Admin	med	4724	SubjectDomainNam
Password Reset By Admin	med	4724	SubjectDomainNam
User Added To Local Admin Grp	high	4732	SrcSID: S-1-5-21
A Member Was Removed From a Security-Enabled Global Group	low	4729	MemberName: -

3.1.4 イベントログ調査時の注意点

認証・アカウント管理に関して、イベントログ調査時の注意点を以下に示します。

・Logon Type の確認：

Logon Type：3（ネットワーク）や 10（リモート対話型）のイベントが平常時に記録されない端末において、それらのイベントが発生している場合、攻撃者によるリモートからの侵入や横展開の可能性も考えられます。そのためにも、平常時にどの Logon Type によるログオンがどの程度発生しているのかを把握しておくことは重要です。

・ログオン失敗のエラーコードの確認：

ログオン失敗（4625）イベントの Status や Sub Status の項目には、ログオン失敗の原因を示すエラーコードが記録されており、エラーコードから「ユーザー名が存在しない」「パスワード誤り」などの原因を読み取ることができます。例えば、攻撃者によるログオン試行で「パスワード誤り」によりログオンが失敗している場合は、攻撃者がパスワードを把握していなくても、ユーザー名については認識している可能性があります。

・特権グループ追加：

Local Administrators（ローカル管理者）グループへの追加（4732）や、Domain Admins（ドメイン管理者）グループへの追加（4728）といったイベントが記録されている場合、攻撃者による権限昇格の兆候の可能性として注意が必要です。

特に、筆者の環境のように平常時にアカウント管理関連イベントが発生しない場合は、少数でも記録があれば正規の操作による記録なのかユーザーへのヒアリングやその他ログなどで確認するようにしましょう。

3.2 プロセス・動作

本節では、自身の PC で平常時に実行されているプロセスの傾向を把握します。平常時の傾向を把握しておくことで、侵入後の不審活動（マルウェアの実行、永続化など）の検知につながります。

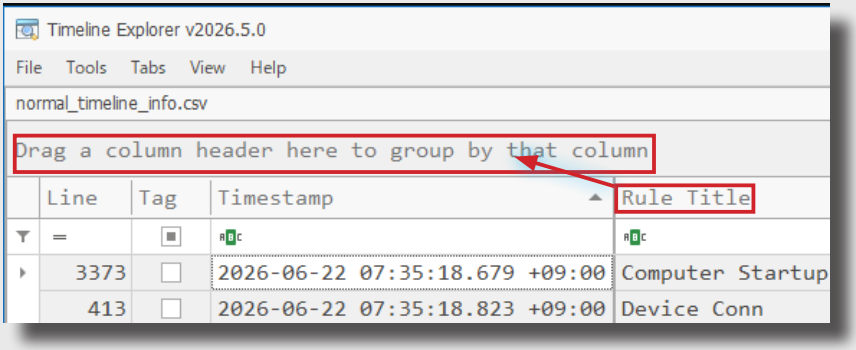
3.2.1 タイムラインにおける検知ルール確認

前節で実行した csv-timeline コマンドで出力されるタイムラインでは、検知ルール（Rule Title）が各イベントに付加されます。

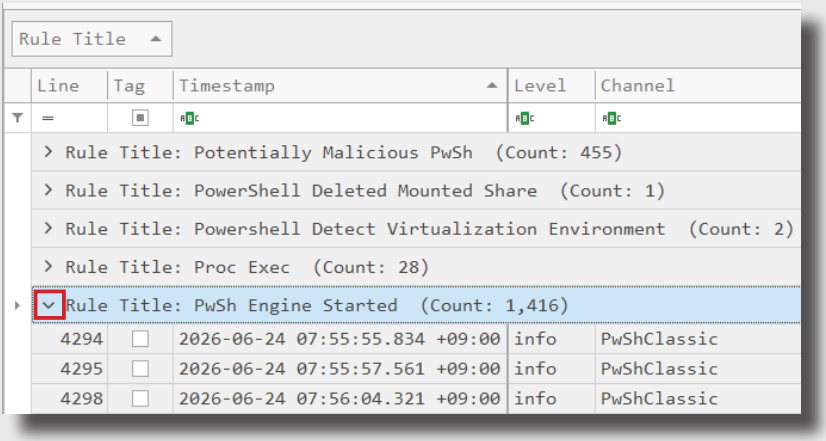
検知ルールを確認することで、イベントの概要を効率よく把握することができます。

コマンド実行時のサマリーにおいて、各レベルでの検知ルール数上位 5 つが表示されますが、今回はタイムラインですべての検知ルールを確認してみましょう。

まず、Timeline Explorer において、フィルターアイコンクリック画面左下の Clear Filter をクリックし、前節で適用したフィルターを解除しておきましょう。
次に、検知ルールが書かれている Rule Title 列ヘッダーをグループ化エリアにドラッグアンドドロップします。



グループ化された検知ルールの一覧およびそれぞれの件数（Count）が確認できます。
また、各グループの「>」をクリックすると、グループ内のイベントを確認できます。



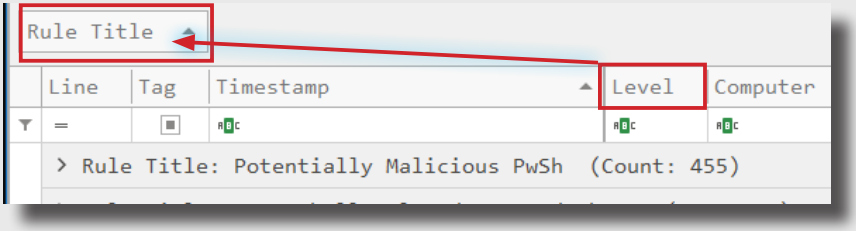
検知ルール名から概要は分かりますが、各検知ルールの詳細な意味を調べたい場合は、以下の URL から Hayabusa の検知ルールの GitHub リポジトリにアクセスして、検知ルール名やイベント ID でのファイル検索などを用いて定義ファイルを確認することをおすすめします（検知ルール名と定義ファイル名は一致しているとは限らないため、検知ルール名内の単語で検索するなどの工夫が必要です）。

https://github.com/Yamato-Security/hayabusa-rules

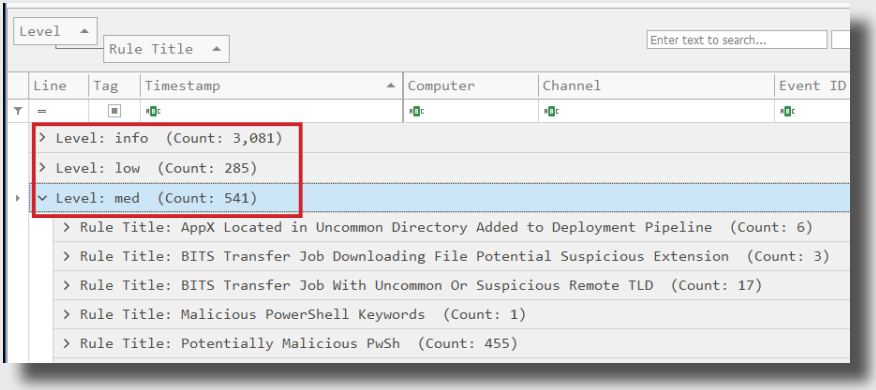
自身の PC でどのような検知ルールのイベントが、どのような頻度、タイミングで発生しているかを確認し、平常時に記録されるイベントの傾向を把握しておきましょう。

3.2.2 イベントの詳細確認

今回は、レベルが高い検知ルールのイベントについて確認します。
Level 列ヘッダーを、グループ化エリアにある Rule Title 列ヘッダーの左側にドラッグアンドドロップします。



下記のようにレベルごとに検知ルールを確認することができます。



確認したい検知ルールグループを展開し、検知ルールに該当したイベントを確認します。
Details 列の内容をダブルクリックで開くことで、イベントの詳細を確認することができます。

自身の PC で、レベルが高い検知ルールで検知されているイベントの詳細を確認してみましょう。

筆者の環境で検知された中で、比較的レベルが高く件数が多い検知ルールを抜粋し、定義ファイル記載の説明と共に以下に示します。

Rule Title （検知ルール）	Level （レベル）	Count （件数）	Channel （チャネル）	Event ID （イベント ID）	Description （説明）
Potentially Malicious PwSh	med	455	PwSh	4104	Windows は不審と判断された PowerShell の実行を自動的に記録し、ログレベルを「警告（Warning）」としてマークする

上記の検知ルール Potentially Malicious PwSh のイベントの一例として、筆者の環境では以下のような情報が記録されていました。

・**スクリプト名（ScriptName）**：UsersInfoCollector
・**保存パス（Path）**：
C:¥ProgramData¥Microsoft¥Windows Defender Advanced Threat Protection¥DataCollection¥.....80.ps1
・**プロバイダー名（EventSource(Name)）**：Microsoft.Windows.Sense.Tvm.Collector

これらの情報を、Microsoft の公式ドキュメントなどの情報を参照しながら読み取ると、スクリプト名がユーザー情報を収集するスクリプトであること、保存パスが Microsoft Defender for Endpoint（MDE）という EDR のデータ収集フォルダーであること、プロバイダー名に記録されている「Sense」が MDE の内部サービス名であることなどを読み取ることができます。また、スクリプト末尾に Microsoft のコード署名が記録されていることからも、本イベントは MDE が定期実行する正規の情報収集イベントであると考えられます。

このように、イベントログの詳細情報を確認することで、処理の目的や、通常動作かどうかを読み取ることができます。
また、各イベントの動作に関してより詳しく調査したい場合は、セキュリティログのイベント ID 4688（プロセス作成）を確認する方法があります。
確認したいイベントのプロセス ID（PID）を確認し、同一のプロセス ID を持つセキュリティログ 4688 のイベントを抽出することで、当該プロセスの実行アカウント（User）、実行パス（Proc）、親プロセス（ParentProcessName）、コマンドライン（Cmdline）などを確認することができます。もし見慣れないアカウントや、一時フォルダーなどからの実行、通常と異なる親プロセス、不審なコマンドラインなどが確認された場合は、異常動作が疑われます。
なお、Sysmon ログにはプロセスの情報がより詳細に記録されるため、もし環境に Sysmon が導入されている場合は、優先的に確認するようにしましょう。

3.2.3 イベントログ調査時の注意点

プロセス・動作に関して、イベントログ調査時の注意点を以下に示します。

・検知ルール名やレベルだけで判断しない：
レベルが high の検知ルールや、検知ルール名が Potentially Malicious PwSh（不審な PowerShell 実行）といった名前の検知ルールであっても、筆者の環境のように正規のソフトウェアによるイベントである場合があります。
イベントログ調査の際に正常動作かどうかを判断するためにも、平常時に定期実行などで記録されるイベントログの傾向や、実行パス、ユーザーなどの詳細情報を把握しておき、総合的に判断することが重要です。

・定期的に発生するイベント：
定期的に発生するイベントは、グループポリシー適用や EDR 定期収集などの自動処理の可能性

が高い一方で、マルウェアの定期的な自動実行による永続化（侵入状態の維持）が行なわれている可能性もあります。また、業務時間外に発生するプロセスは攻撃の兆候の 1 つですが、バッチ処理や更新処理などの可能性もあるため、平常時のベースラインとの差分や、その他痕跡をもとに判断することが重要です。

4. おわりに

今回はここまでとなります。
「Hayabusa でのイベントログ調査 平常時確認編」では、Hayabusa と Timeline Explorer を用いて平常時の自身の PC のイベントログを確認するハンズオンを実施し、イベントログ調査における観点や注意点を理解しました。
次回は、サンプルの攻撃イベントログを対象に、Hayabusa を用いた攻撃痕跡調査の方法や観点を解説します。

Hitachi Systems Security Journal

株式会社 日立システムズ　本社：〒141-8672　東京都品川区大崎 1-2-1　www.hitachi-systems.com

お問い合わせは

※本カタログに記載されている会社名、製品名は、それぞれの会社の登録商標または商標です。
※本カタログに記載されている内容、仕様については、予告なく変更する場合があります。
※本製品を輸出する場合には、外国為替および外国貿易法ならびに、米国の輸出管理関連法規などの規制を御確認の上、必要な手続きをお取りください。なお、ご不明な場合は、当社営業にお問い合わせください。

Printed in Japan