HITACHI
Inspire the Next

Hitachi Systems Security Journal

VOL.67

株式会社 日立システムズ

Human * IT

Hitachi Systems Security Journal VOL.67

TABLE OF CONTENTS

●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

自らが信じる正義のため倫理の境界線上でサイバー犯罪グループと戦う

ヴァンゲリス・スティカス インタビュー

CODE BLUE 2024 で「敵陣の内部へ：ランサムウェア Web パネルへの介入と妨害」と題する講演を行なったヴァンゲリス・スティカス氏。Web アプリケーションや IoT 製品のセキュリティリサーチャーとして活動する彼だが、マルウェアやランサムウェアを駆使して勢力を拡大するサイバー犯罪グループの動きに危機感を抱き、新たな研究に着手した。その研究の核となるのは、犯罪者グループが使用する C2 サーバーへ侵入を通じた犯罪活動の追跡だ。倫理的課題を伴うこのグレーゾーンのアプローチで得られた知見とは何なのか？ そして、犯罪者と向き合う彼の信念とは？ スティカス氏の挑戦的な取り組みについて話を伺った。

取材・文＝斉藤 健一／通訳＝エル・ケンタロウ／撮影＝卯月 梨沙

サイバー犯罪者の脅威となるような研究をしたい

斉藤（以下 S ）：今回発表されたこの研究を始めるきっかけは何だったのですか。

ヴァンゲリス・スティカス（以下 V ）：私はもともと IoT の API を対象に研究を行なっていました。しかし、マルウェアやランサムウェアが台頭する中で、犯罪者たちが自らの存在を誇示するかのような振る舞いが目に付き、無視できないと感じたことがきっかけです。彼らにとって脅威となるような研究をしたいと思うようになった、というのが正直なところです。

S 調査・研究は 1 人で進められているのですか。

V 時には、自分では対応できない高度な専門性が求められる部分について、友人や研究仲間に手伝ってもらうことがあります。また、米国や英国などの法執行機関ともさまざまな形でコンタクトがあり、必要に応じて彼らの協力を仰ぐこともあります。多くの場合、犯罪集団に関する調査がある程度完了した段階でのことで「ここから先は法的な手続きをお願いします」といった形で連絡を取っています。

S この研究は、本業とは別に進めているプロジェクトと考えてよいでしょうか。

V そうですね。日々の業務とは異なる分野ではありますが、セキュリティリサーチャーという観点から見れば、共通点があるともいえます。先ほどお話ししたように、本業では IoT の API に関する研究を行なっていますが、インテリジェンス分野には携わったことがありません。実は、8 年前までは開発者として働いていました。

S 開発者からセキュリティ業界に転身しようと思ったきっかけは何ですか。

V もともとプログラミングが好きだったことから、協力者とともに会社を立ち上げました。その後、シニアエンジニアとして経験を積み、最終的には CTO に就任するまでになりましたが、一方でそれを退屈だと感じる自分もいました。そうした中、システムのバグを発見する過程で「これが仕事になるのか」「これでお金がもらえるのか」という驚きとともに、セキュリティ業界について深く知るようになりました。そして「この業界に挑戦してみよう」と決意し、一歩を踏み出しました。

S なるほど。そういう経緯があったのですね。

V そして、技術的なハッキングを進める中で、次第に犯罪者を追跡するような活動へと発展していきました。そのような経験が重なるうちに、どんどん加速していき、のめり込んでいったのです。

ランサムウェアグループの C2 サーバー内部で行われていたこととは？

S 引き続き、研究の調査方法についてお伺いしたいのですが、まずマルウェアやランサムウェアの

ヴァンゲリス・スティカス（Vangelis Stykas）
ギリシャ出身。開発者としてキャリアをスタートさせ、その後セキュリティ分野に関心を向けるようになる。現在、Atropos の CTO を務めている。Web アプリケーションや IoT 製品の API セキュリティ研究を専門としており、複数の国際的なセキュリティカンファレンスで研究成果を発表している。2023 年の DEFCON 31 では「The Art of Compromising C2 Servers A Web App Vulns Perspective（C2 サーバーを攻略する技術 - Web アプリの脆弱性の視点から -）」と題する講演を行った。サイバー犯罪グループの C2 サーバーへの侵入という倫理の線引きが問われる題材を扱ったもので大きな注目を集めた。

CODE BLUE 2024 での登壇の様子。公式サイトでは講演の動画とスライドが公開されている　https://codeblue.jp/results/results/#result-20

検体を入手するところから始める、という理解でよろしいでしょうか？

V マルウェアとランサムウェアでは状況が異なります。マルウェアに関しては、研究者のコミュニティが成熟しており、検体が比較的容易に入手できる状況にあります。一方、ランサムウェアの検体の入手は簡単なことではありません。ですが、2023 年の DEFCON での発表をきっかけに、脅威インテリジェンス（CTI）を提供する企業との交流が始まりました。彼らは情報共有に積極的で、私の研究を進める支えになっています。また、場合によっては、彼らから依頼を受けて分析を手伝うこともあります。そのため、現在では、検体の入手に苦労することはほとんどありません。

S 数について確認したいのですが、今回の研究で発表された内容に関して、例えばマルウェアやランサムウェアの検体の数について、どの程度調査されたのか教えていただけますか？

V 検体の調査といっても、私が主に行なっているのは、C2（Command & Control）サーバーなどの URL を抽出し、攻撃手法を追跡することです。その結果、これまでに 4 つの異なるマルウェアファミリーを確認することができました。それらはおおよそ 3000 ～ 4000 のターゲットにインストールされていたと推定されます。一方で、ランサムウェアに関しては、約 180 件のケースを確認しています。

S 調査で印象的だったことなどあれば、可能な範囲で教えて下さい。

V 幸運だったケースとして、ランサムウェアに関連する C2 サーバーを発見できた事例がありました。この発見により、被害者の端末とランサムウェアの C2 サーバーとの通信を監視することが可能となりました。とはいえ、実際には非常に退屈で時間のかかる監視作業を繰り返す必要がありました。さらに、近年の洗練されたランサムウェアでは、キャンペーンが実行中で被害者が接続しており、かつオペレーターが操作しているタイミングでしか通信しないといった形態のものも出現しています。そのため、これらを常に監視し続ける必要があり、非常に多くの工数と実行力を要する作業となっていました。

S ランサムウェアのオペレーターと被害者の間ではどのような通信が行われているのか、こちらも可能な範囲で教えて下さい。

V 他の C2 サーバーと同様に、コネクションを確立しファイルを探索し、発見したファイルをアップロードする、といった一般的な動作が行われていました。

S つまり、情報の窃取ですね。

V 私が監視したキャンペーンでは、そうした動作が確認できました。例えば、他のキャンペーン

では単にマルウェアをダウンロードし、その後エンドポイントで実行されて横展開するといったパターンも確認できると思います。

S ヴァンゲリスさんが監視の次に取った行動とは、一体何だったのでしょうか？

V 攻撃を目撃したため、クライアントに通知せざるを得ませんでした。これらの攻撃では、AzureやAWSのアクセスキーが窃取されていました。講演でも触れたように、ターゲットとなったのは評価額が10億ドルを超えるユニコーン企業です。ある企業に通知した際、「Hacker One※にプロフィールがあるので、そちらを通じて連絡してください」と言われました。しかし私は「これは単なるバグの報告ではなく、現在進行中の攻撃です」と説明し、ようやく対応してもらうことができました。

S ヴァンゲリスさんが経験した事案では、きちんと対応してもらえたようでなによりです。ただ、一般的に、そのような情報を提供しても、企業側から「金銭目的ではないか」という反応をされたり、「本当に攻撃されているのか」という疑いの目を向けられることも多いと聞きます。このあたりはいかがですか。

V 組織に連絡する場合、私は次のようなメッセージを用意しています。「これは金銭が目的でもありませんし、小さな問題でもありません。現実にそちらの組織が攻撃を受けています。これがその証拠となる情報です。どのように判断し、対応するかは貴社の判断にお任せします。ただし、対応できる時間は限られており、対応が遅れると攻撃が成功し、より大きな被害につながる可能性があります」と。

S あくまで対応する主体はターゲットとなった組織だという姿勢ですね。

V 話はそれますが、私の本業の方でもこれまでに9社にIoT製品の脆弱性について報告しましたが、証拠を基に自主的に対応したのは、わずか1社だけでした。残りの8社のうち4社は、影響力のある第三者機関の介入がなければ対応が進まない状況でした。そして、残りの4社にいたっては、まったく対応する姿勢を見せませんでした。

S 脆弱性の開示や修正は本当に難しい問題だと思います。

V もう1つ、私が問題視している点があります。それは、一部のリサーチャーが、開示を通じて仕事を得ようとしていることです。開示の目的は本来、問題を解決するためであるべきです。しかし、解決を伴わずに単に報酬を得るだけでは、結局のところ何も変わらないのではないでしょうか。

S 解決方法を明らかにせずに問題だけを指摘して報酬を得ようとすることは、システムを暗号化して身代金を要求する犯罪グループがしていることと似ていると感じるのですが、いかがでしょうか。

V 私の見解は異なります。例えば、バグに関する話で言えば、バグバウンティプログラムに参加している場合に、そこを通じて開示するのは、制度的に全く問題のない行為だと思います。また、セキュリティベンダーが「お客さまの脆弱性を見つけました」として、それをもう少し深掘りして特定したりする行為については、確かに脅迫めいた印象を与えることもありますが、違法ではないと考えます。それが伝統的な営業手法であることは間違いありません。しかし、それをランサムウェアと同一視するかと言えば、全く違う話だと思います。ランサムウェアの場合、完全に犯罪行為が含まれるからです。

S なるほど。ありがとうございます。

サイバー犯罪グループとの対峙と各国の法執行機関との連携

S 調査を進める中で、法執行機関との連携が出てくる場面があると思います。その際、法執行機関と協力を始めるきっかけや、研究を進める中でどのように話が広がっていったのか、その経緯について教えていただけますか？

V 最初の案件が、最も緊張しました。しかし、一度その経験を経て、現在では世界中のさまざまな法執行機関とコンタクトを取れるようになり、「こういうことを見つけたので報告したい」と連絡を

※ **HackerOne**：企業とセキュリティ研究者をつなぐプラットフォームで、バグバウンティプログラムを通じて脆弱性を発見・報告し、修正の支援を行う。 https://www.hackrone.com/

取る形で対応しています。

S それは、法執行機関側も、そうした報告の受け入れ体制が整ってきたからでしょうか。それともヴァンゲリスさんの人脈が広がったからでしょうか。

V 両方あると思います。おそらく運が良かったのは、最初にコンタクトを取った相手がきちんと対応してくれる方だったという点だと思います。もちろん、名前が有名になったことも影響したかもしれませんが、たとえ私が有名でなかったとしても、その人であればきっと丁寧に対応してくれたと思います。そこからヨーロッパやイギリス、アメリカでも同様に、コンタクトを取った相手が良かったことが大きな要因だと感じています。

S 講演の中で、サイバー犯罪グループからご家族に対して脅迫をほのめかすようなメールが送られたというお話もありました。そのような状況に直面した際、どのような心境だったのでしょうか。恐怖を感じることはありましたか。

V こうした研究を進める中で起こる出来事は、ある意味で避けられない不可抗力だと受け止めています。例えば、朝起きて携帯を確認した際に、Google のアラートで「国家的背景を持つ攻撃主体があなたを標的にしています」といった通知が表示されたり、iPhone から「iPhone が攻撃されています」という警告が届くといった状況です。これらは非常に不思議で異質な感覚を抱かせるものですが、研究を続けるうえでは仕方のないことだと割り切っています。

S サイバー犯罪グループによる攻撃には、たとえ成功しなくとも、ヴァンゲリスさんの心を挫こうとする意図があるのだと思います。しかし、それに屈することのない精神力の強さを感じます。また、このような攻撃が仕掛けられるという事実そのものが、ヴァンゲリスさんの研究が彼らにとって大きな打撃となっていることを示しているのではないでしょうか。

V 精神的に強いとかということではなくて、対立する相手は犯罪者であり、潤沢な資金もあります。繰り返しになりますが、こうした研究を始めることで攻撃されるのは当たり前と受け入れるしかないと考えています。

S 堅い意志を持たれているのですね。

研究を進める中で自身がサイバー犯罪グループの標的となることも受け入れると語るスティカス氏

V 話はそれますが、私の研究内容を利用しながら私の名前を削り、商材化している企業にも犯罪グループと同様に、強い憤りを感じています。これは、私が個人の時間や資金を費やして得た研究成果だからです。

S 本当におっしゃるとおりです。引き続き今後の研究について伺います。このまま、マルウェアやランサムウェアの研究を続けられますか。もしくは何か新たな研究に着手する予定などありますか。

V 私自身、先の予定を細かく決めるのはあまり好きではないため、実際のところ、これからどうなるかはわかりません。マルウェアに関しては、知り合いから依頼を受けて解析を手伝うことはありますが、研究そのものはほぼ終了したと考えています。また、ランサムウェアの研究についても、一段落がついた状態です。今後、いくつかの情報を公開する予定で、2025 年 3 月までに完了させることを目標としています。そして、詳細はまだお話しできませんが、ランサムウェア以外のサイバー犯罪に関する新たな研究にも着手する予定です。

S ありがとうございます。新たな研究のご発展をお祈りしています。

防御のためのサイバー攻撃は是か非か !?

S 次に、防御側がサイバー攻撃を仕掛けることについて、ご意見をお伺いしたいと思います。日本では「アクティブ・サイバー・ディフェンス」という考えが議論されています。この言葉の解釈は人によってさまざまで、具体的な行為を明確にするのも難しいものの、攻撃者のシステムに侵入して無力化したり、反撃したりする行為を容認する意見も見られます。こうしたアプローチについて、どのようにお考えでしょうか？

V 回答は国家全体のサイバーセキュリティに関するものではなく、あくまで私自身の研究に関する考えです。私の活動について言えば、その多くがブラック、つまり法律上は完全に犯罪行為とみなされる領域に入るものであると認識しています。しかし、私の祖国であるギリシャでは、不正アクセスは被害者からの届け出がなければ捜査が行われないという法的枠組みがあります。そのため、現時点では大きな問題には発展していません。

S ギリシャはそうした法的枠組みなのですね。

V それでも、積極的に法律を破ることを推奨するつもりはありませんし、自分の行いが正しいとも考えていません。私は、防御側は防衛に徹するべきだと思っています。この問題について、より明確な答えを導き出すことが理想ではありますが、非常に複雑な状況にあるため、簡単に結論を出せるものではないと感じています。

S 非常に参考になります。この問題について、別の視点から考えてみたいと思います。これまでお話を伺う中で、法執行機関との連携の話題が出ました。日本においては、情報提供が目的だとしても違法行為を正当化することはないと思うのですが、海外の法執行機関はいかがですか。

V 海外でも状況は同様です。たとえ確度の高い情報を提供しても、表立って感謝されることはありません。このことが、この問題の難しさを象徴しているのではないでしょうか。ただし、裏では個人として感謝されているのではないかと思っています。

S 情報提供は無償で行なっているのですか。

V はい、現在は無償で活動しています。ただし、プロジェクトを立ち上げて調査が正式な仕事となり、報酬をいただけるのであれば、それを断ることはありません。

S 今回のインタビューでは、研究成果を盗用される憤りやサイバー犯罪グループから狙われるリスク、さらに法執行機関に報告しても表立った感謝を得られないといったお話を伺いました。このような状況下でも研究を続けるモチベーションは何でしょうか。

V 確かにストレスはあります。ですが、こうして私の話を聞きたいと、わざわざ飛行機代まで負担してカンファレンスに招いてくれる方々もいます。名誉という言葉はあまり好きではありませんが、多くの人が私に興味を持ってくれるということ自体が、とても実りのあることだと感じます。また、自分の活動を認めてもらえているという嬉しさがあります。

S 他者から認められることはモチベーションアップにつながりますね。

V 過去 10 年間にわたり、IoT 製品の API を研究して数多くの脆弱性を発見してきました。もちろん、それらを発見したときには興奮するのですが、犯罪者などの悪人を追い詰めたときの興奮はそれらの比ではありません。

S その興奮は想像するしかありませんが、もしかすると悪と対峙するヒーローだけが体験できるものなのかもしれませんね。本日はありがとうございました。

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 2025.01

文＝日立システムズ

ペンテストを活用したサイバーセキュリティ体制の実践的強化手法

【概要】：近年、サイバー攻撃への防御力を高める手法として「脅威ベースのペネトレーションテスト Threat-Led Penetration Testing（以下、TLPT）」が注目を集めており、その実践的な手法と高い効果から、金融業界を中心に幅広い分野へ導入が進んでいる。

【内容】：TLPT は現実のサイバー攻撃を模倣し、防御、検知、対応能力を向上させることを目的としている。2010 年代、APT（標的型攻撃）が多発した米国では、完全な防御が困難な高度な攻撃に対応するため、侵入後の検知や対応力の強化が必要とされ、TLPT が普及した。APT 攻撃は高度であり、完全な防御が困難であることから、侵入後の検知や対応力を強化する必要性が認識されたことが普及の背景にある。日本においては、金融庁が 2018 年に、諸外国における脅威ベースのペネトレーションテストに関する報告書をまとめ、2024 年には「金融分野におけるサイバーセキュリティに関するガイドライン」を公開した。このガイドラインを契機に、金融機関にとどまらず、官公庁や重要インフラ、商社などでの活用が期待されている。

TLPT の特徴は、攻撃者の視点に立ってシナリオを構築する点にある。具体的には、特定の攻撃者グループを想定し、その目的や使用するツール、攻撃手法を模倣したテストを行う。例えば、国家支援を受けた攻撃者が重要インフラを標的にする場合、DoS 攻撃やランサムウェア攻撃の可能性を含めたシナリオを設定し、模擬攻撃を実施する。これにより、攻撃者が組織の脆弱性をどのように突くのかを具体的に検証することが可能である。

表 TLPT の各段階におけるレッドチームとブルーチームの行動例

段階	レッドチームの行動	ブルーチームの行動
準備	公開情報、OSINT、ダークWeb などを用いて対象への攻撃方法を検討	システムの監視体制を整え、インシデント発生時の即時対応を準備
情報の収集分析	ポートスキャンや脆弱性スキャンツールを用いて対象の情報を収集、潜在的な脆弱性の探索	セキュリティ監視ツールや IDS などから、レッドチームの活動を追跡して攻撃の兆候を検出
攻撃開始段階	脆弱性を悪用してシステム侵入を試行	攻撃に反応し、FW や IDS の設定、システム隔離、通信しゃ断などの防御策を施行
攻撃継続段階	【侵入に成功】権限奪取や情報窃取、水平展開など活動を拡大 【侵入に失敗】ブルーチームの反応を観察し、攻撃手法を変更	【防御が有効】レッドチームの新たな攻撃への防備 【防御に失敗】改善点を明確にして対応を強化

一方で、一般の組織が独自に脅威情報を収集し、分析することは困難である。そのため、IT サービス企業やセキュリティベンダーが提供する TLPT サービスを活用することが一般的であり、プロジェクトマネージャーや CISO が計画段階から参加し、サービス提供者とテスト内容を協議する形が取られている。

TLPT は、表のようにレッドチーム（攻撃側）とブルーチーム（防御側）に分かれて実施されることが多い。攻撃側は脆弱性を突いた模擬攻撃を行い、防御側はリアルタイムでの検知と対応を試みる。これにより、攻撃者の行動パターンや攻撃手法を理解すると同時に、防御側の対応力を評価することが可能である。

従来のペネトレーションテストは脆弱性の発見と修正が目的であり、新規システムの導入後や定期的なセキュリティチェックに適している。一方、TLPT は高度な攻撃に対する対応力の評価やセキュリティチームの訓練に適用できる。これらを目的に応じて組み合わせることで、セキュリティ体制のさらなる強化につながるものである。

［情報源］

https://www.fsa.go.jp/news/r5/sonota/20240628-2/17.pdf

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 Web ブラウザー履歴調査

2. Firefox 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（Vol.66）より「Windows Web ブラウザー履歴調査」と題して、主として NirSoft が提供する「Browser Tools」を取り上げ、基礎となる考えの概説からツールを用いた調査方法までを紹介していきます。「Browser Tools」は、Nir Sofer 氏が公開している Web ブラウザーの履歴などを確認するためのフリーツール群です。

NirSoft は、Nir Sofer 氏が 2001 年頃よりデジタルフォレンジックなどに有用なツールを公開している個人サイトで、米 CISA の関連ドキュメントなどでも紹介されるなど知名度が高いサイトです。

フリーウェアで制約なく利用が可能ですが、その有用性から攻撃者によっても頻繁に悪用されるため、ウイルス対策ソフト等が検知する可能性があります。また、本ツールだけでなく他のプログラムにもいえることですが、第三者機関によって安全性が保障されていない、あるいはソースコードが公開されていないプログラムを利用する場合には、安全のために仮想環境上での実行を推奨します。

「Windows Web ブラウザー履歴調査」は、以下の 3 部により構成されます。

1. Edge / Chrome 編
NirSoft が提供する「Browser Tools」を利用して、Edge、Chrome の閲覧履歴を確認します。

2. Firefox 編
NirSoft が提供する「Browser Tools」を利用して、Firefox の閲覧履歴などを確認します。

3. 追加情報編
NirSoft が提供する「Browser Tools」を利用して、Web ブラウザーに保存されている認証情報を確認します。また、Chrome の履歴が保存されている SQLite を確認します。

今回は、「2. FireFox 編」として、NirSoft が提供する「Browser Tools」を利用して、Firefox の閲覧履歴などを確認します。マルウェア感染した可能性がある PC の感染経路や不審なサイトへの接続状況を確認する際などに利用します。

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ありません。OA 端末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します。

2. Windows サンドボックス

「Windows サンドボックス」とは、「Windows 10 May 2019 Update」で追加された Windows の機能です。Windows OS の中に仮想的なコンピューター（Windows OS）を作り出すことができ、安全にソフトウェアの検証などを行うことが可能です。

ソフトウェアの導入については、前号（Vol. 66）※で紹介していますので、そちらをご覧下さい。

※ https://www.hitachi-systems.com/-/media/report/specialist/hj/download/hj66_placeholder.pdf

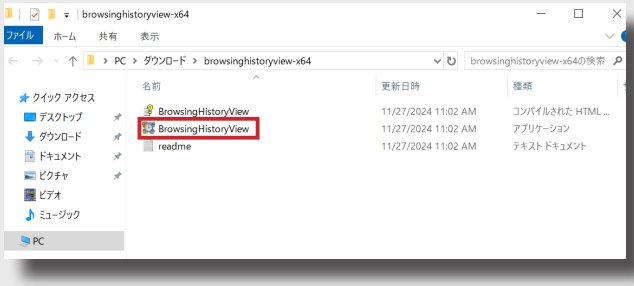
3. BrowsingHistoryView

3.1 BrowsingHistoryView の導入（前号で導入済みの方は次項にお進みください）

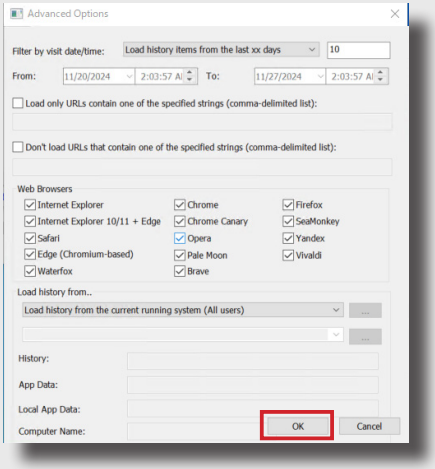
NirSoft で公開されている Browser Tools のうち、「BrowsingHistoryView」をダウンロードします。以下の URL にアクセスし、ご自身の環境に合わせた「BrowsingHistoryView」をダウンロードしてください。今回筆者は、「BrowsingHistoryView 64-bit」をダウンロードしました。

https://www.NirSoft.net/utils/browsing_history_view.html

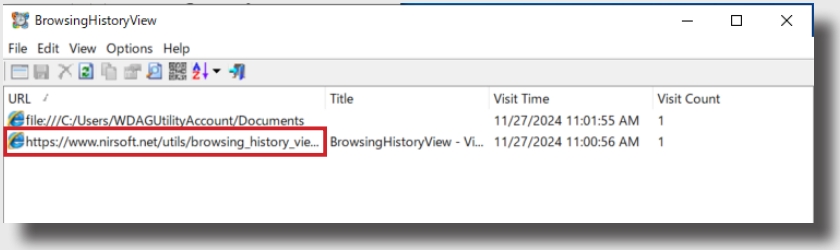
ダウンロードが完了しましたら、Zip ファイルを解凍、展開します。



展開が終わりましたら「BrowsingHistoryView」を起動します。起動すると「Advanced Options」ダイアログが起動しますが、初期設定のまま「OK」を押下して問題ありません。



起動すると、「BrowsingHistoryView」をダウンロードする際に、NirSoft にアクセスした履歴が確認できます。



4. Firefox の履歴確認

4.1 Firefox のインストール

公式サイトにアクセスし、Firefox をインストールします。
インストールの際の設定は、お使いの環境に合わせて指定してください。筆者は図のように、Windows 64bit 日本語版をダウンロードしました。

https://www.mozilla.org/ja/firefox/all/desktop-release/

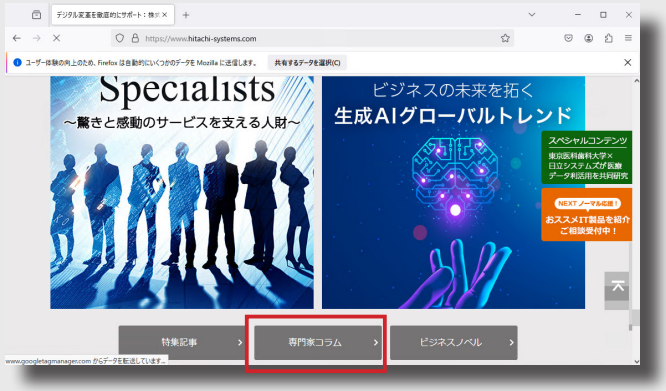
ダウンロードが完了しましたら、インストールを実行してください。

4.2 Hitachi Systems Security Journal の閲覧

日立システムズの公式サイトにアクセスします。

https://www.hitachi-systems.com/

画面をスクロールし、「専門家コラム」をクリックします。



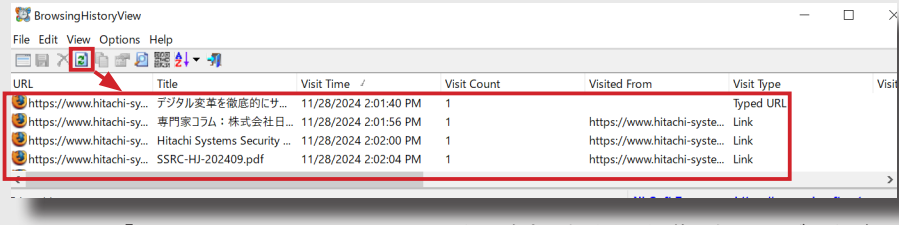
専門家コラム内の「Hitachi Systems Security Journal」をクリックします。

「Hitachi Systems Security Journal」のいずれか（今回は Vol.64）を**左クリック**して開きます。

Web ブラウザー上で PDF ファイルが開きます。

4.3「BrowsingHistoryView」による履歴の閲覧

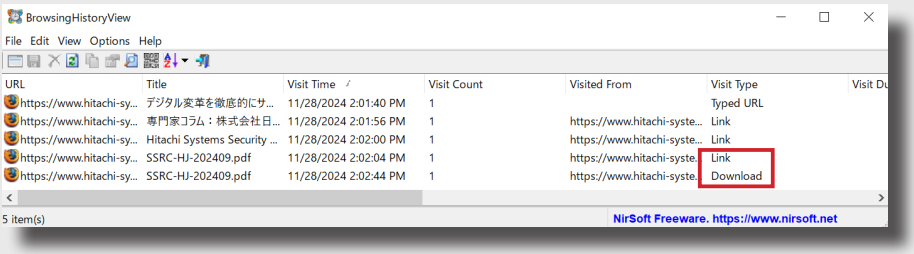
Web ブラウザー上で PDF ファイルが開きましたら、「BrowsingHistoryView」を確認し、更新ボタンを押下します。



Firefox で「Hitachi Systems Security Journal」を閲覧するために、遷移した Web ブラウザーの履歴を確認できました。

次に、「Hitachi Systems Security Journal」のいずれか（今回は Vol.64）を**右クリック**してダウンロードします。

ダウンロードしましたら、「BrowsingHistoryView」を更新してください。Firefox の場合、Edge や Chrome と異なり、PDF ファイルに https で履歴が記録されていることが確認できます。



なお、左クリックで開いた場合には、Visit Type が異なることが確認できます。ダウンロードの有無については、Visit Type を確認することで判断ができそうです。

4.4 Firefox の履歴ファイル格納場所

Firefox の閲覧履歴は、基本的に以下に保存されています。
C:¥Users¥[ユーザー名]¥Roaming¥Mozilla¥Firefox¥Profiles¥<random text>.default¥places.sqlite

場合によっては、以下に保存されているようです（今回はこちらで確認しました）。
C:¥Users¥[ユーザー名]¥Roaming¥Mozilla¥Firefox¥Profiles¥<random text>.default-release¥places.sqlite

なお、古いバージョン (v3-25:) の Firefox を利用していた場合、以下に保存されている場合があります。
C:¥Users¥[ユーザー名] ¥AppData¥Roaming¥Mozilla¥Firefox¥Profi les¥.default¥downloads.sqlite

閲覧履歴を保全する際には注意してください。

【参考】https://www.nri-secure.co.jp/hubfs/SANS/download/DFPS_FOR500_v4.7_1-19_JP.pdf

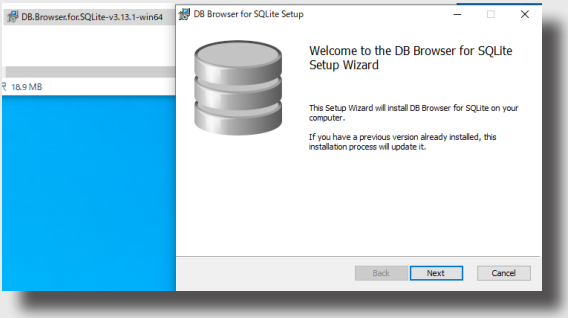
5. Firefox のダウンロード履歴（SQLite）の確認

5.1 DB Browser for SQLite の導入

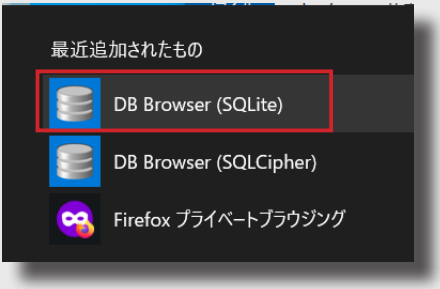
Firefox の履歴を閲覧するために「DB Browser for SQLite」を導入します。
インストールプログラムは下記の配布サイトから入手します。ご自身の環境にあわせてダウンロードしてください。今回、筆者は Windows 64bit 版のスタンダード・インストーラーを選択しました。

https://sqlitebrowser.org/dl/

ダウンロード後はインストールを実施してください。

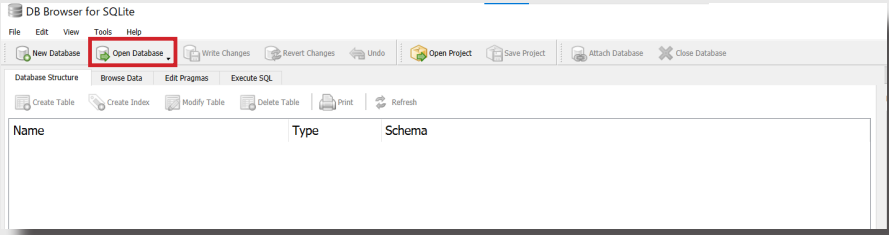


インストールが完了しましたら、スタートメニューより「DB Browser（SQLite）」を選択し、起動します。

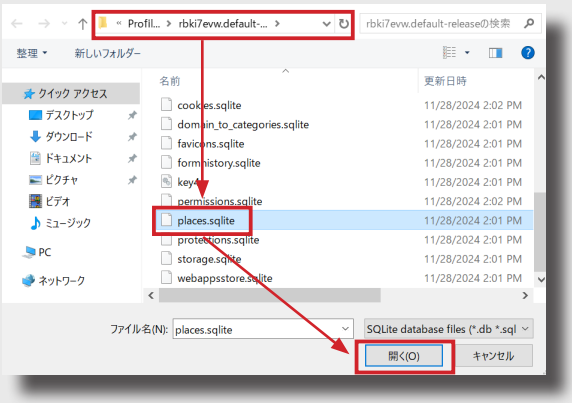


5.2 Firefox の履歴の閲覧

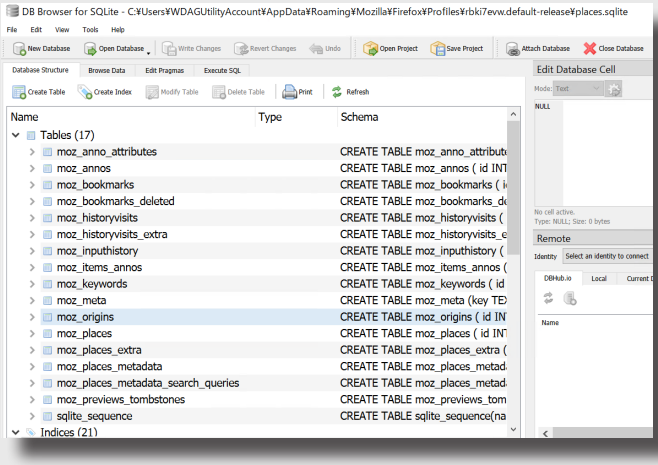
「DB Browser for SQLite」が起動しましたら、「Open Database」をクリックします。



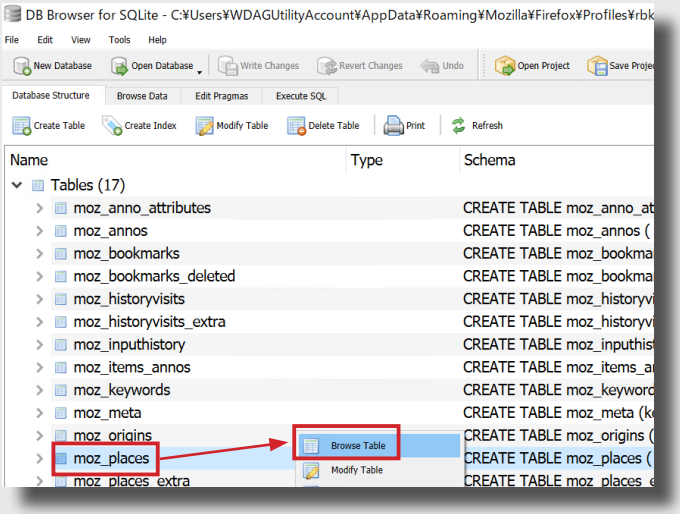
開くファイルは、「4.4 Firefox の履歴ファイル格納場所」で紹介した以下のファイルとなります。
C:¥Users¥[ユーザー名]¥Roaming¥Mozilla¥Firefox¥Profiles¥<random text>.default-release ¥places.sqlite



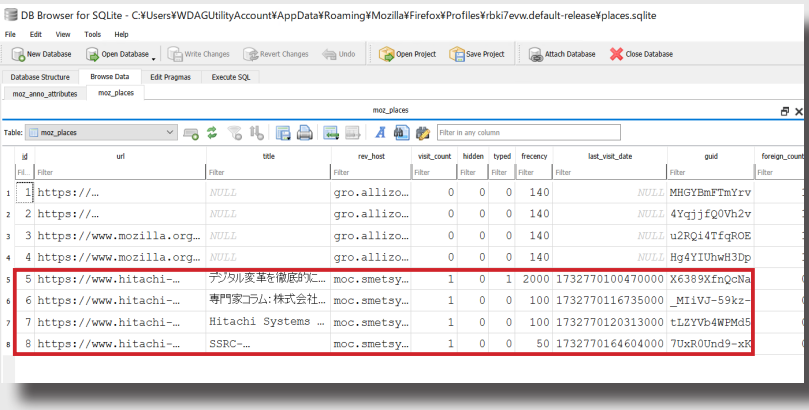
当該ファイルを開くと、図のように Firefox のデータベーステーブルが閲覧可能となります。



データベーステーブルが閲覧できたら、「moz_places」を選択し、右クリックで「Browse Tables」をクリックします。



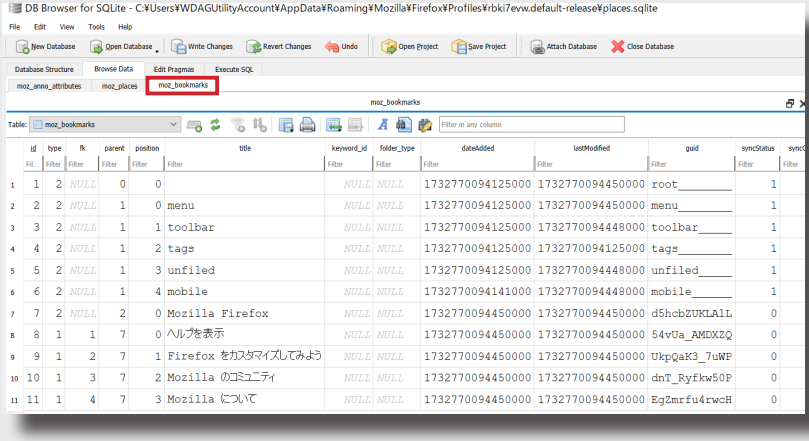
新たなタブが開き、Firefox での閲覧履歴を確認することができました。



Last_visit_date は、micro 秒までの unix epoch で格納されています。例えば、PDF にアクセスした最終時刻は「1732770164604000」ですが、micro 秒までの unix epoch で変換すると Thu Nov 28 2024 14:02:44 GMT+0900 (日本標準時) となり、BrowsingHistoryView と同じ時刻となります。なお、変換には下記のサイトなどが参考になります。

【参考】https://www.unixtimestamp.com/ja/index.php

また、DB Browser for SQLite では、ブックマークの情報なども閲覧できます。



	id	type	fk	parent	position	title	keyword_id	folder_type	dateAdded	lastModified	guid	syncStatus
1	1	2	NULL	0	0		NULL	NULL	1732770094125000	1732770094450000	root_____	1
2	2	2	NULL	1	0	menu	NULL	NULL	1732770094125000	1732770094450000	menu_____	1
3	3	2	NULL	1	1	toolbar	NULL	NULL	1732770094125000	1732770094448000	toolbar_____	1
4	4	2	NULL	1	2	tags	NULL	NULL	1732770094125000	1732770094125000	tags_____	1
5	5	2	NULL	1	3	unfiled	NULL	NULL	1732770094125000	1732770094448000	unfiled_____	1
6	6	2	NULL	1	4	mobile	NULL	NULL	1732770094141000	1732770094448000	mobile_____	1
7	7	2	NULL	2	0	Mozilla Firefox	NULL	NULL	1732770094450000	1732770094450000	d5hcbZUKLAlL	0
8	8	1	1	7	0	ヘルプを表示	NULL	NULL	1732770094450000	1732770094450000	54vUa_AMDXZQ	0
9	9	1	2	7	1	Firefox をカスタマイズしてみよう	NULL	NULL	1732770094450000	1732770094450000	UkpQaK3_7uWP	0
10	10	1	3	7	2	Mozilla のコミュニティ	NULL	NULL	1732770094450000	1732770094450000	dnT_Ryfkw50P	0
11	11	1	4	7	3	Mozilla について	NULL	NULL	1732770094450000	1732770094450000	EgZmrfu4rwcH	0

7. おわりに

今回は、「2.　Firefox 編」として、NirSoft の「Browser Tools」を利用して、Firefox の閲覧履歴などを確認しました。また、「DB Browser for SQLite」を利用して、データベースの中身も確認しました。マルウェア感染した可能性がある PC の感染経路や不審なサイトへの接続状況を確認する際などに利用します。

次回も NirSoft が提供する「Browser Tools」を利用して、Web ブラウザーに保存されている認証情報を確認します。また、Chrome の履歴が保存されている SQLite 確認のコツなどもご紹介します。

Human * IT

人と IT のチカラで、驚きと感動のサービスを。

Hitachi Systems Security Journal VOL.67

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