HITACHI
Inspire the Next

Hitachi Systems Security Journal

VOL.68

株式会社 日立システムズ

Human*IT

Hitachi Systems Security Journal VOL.68

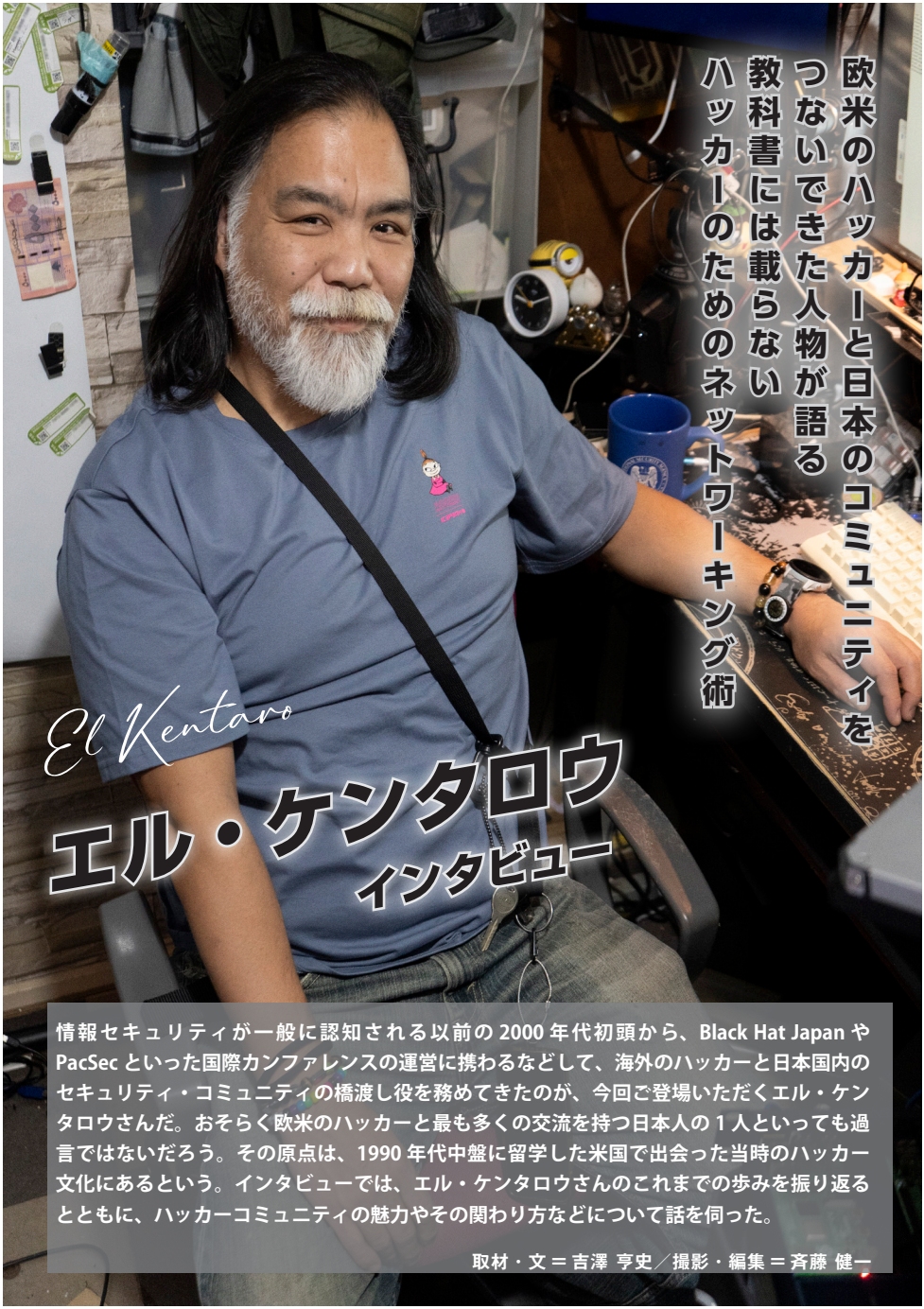
TABLE OF CONTENTS

●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

●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。
本文書に記載した会社名・製品名は各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。



欧米のハッカーと日本のコミュニティをつないできた人物が語る教科書には載らないハッカーのためのネットワーキング術

El Kentaro

エル・ケンタロウ インタビュー

情報セキュリティが一般に認知される以前の 2000 年代初頭から、Black Hat Japan や PacSec といった国際カンファレンスの運営に携わるなどして、海外のハッカーと日本国内のセキュリティ・コミュニティの橋渡し役を務めてきたのが、今回ご登場いただくエル・ケンタロウさんだ。おそらく欧米のハッカーと最も多くの交流を持つ日本人の 1 人といっても過言ではないだろう。その原点は、1990 年代中盤に留学した米国で出会った当時のハッカー文化にあるという。インタビューでは、エル・ケンタロウさんのこれまでの歩みを振り返るとともに、ハッカーコミュニティの魅力やその関わり方などについて話を伺った。

取材・文＝吉澤 亨史／撮影・編集＝斉藤 健一

ラジオ・無線マニアが留学先の米国でハッカー文化と出会う

吉澤（以下、Y）：本日は忙しいところ時間を作っていただき、ありがとうございます。ケンタロウさんには取材の通訳としていつもお世話になっています。まずは略歴を教えてください。

エル・ケンタロウ（以下、K）：大学はアメリカに留学して、演劇映像科を専攻していました。当時からコンピューターが得意だったので、工学部のコンピューターラボでアルバイトとしてアシスタントをしていました。留学生は大学以外でのアルバイトが禁止されていたのです。ラボには高性能なコンピューターがあり、それが深夜は使い放題だったので、アルバイト仲間と自由に遊んでいました。

Y 深夜に自由にコンピューターを使えたというのは、まさにハッカーの原体験ともいえる経験ですね。

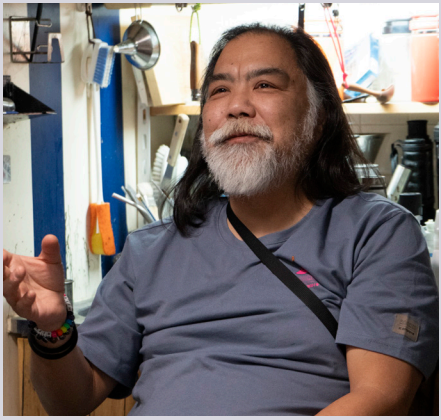
K ハッキングやハッカーという言葉を知らずに、ストレージが足りないから大学の駐車場管理システムのハードディスクに新たにパーティションを切って、勝手にデータを保存したりしていましたね。そのルーツはラジオ・無線のマニア向け雑誌でした。中学、高校時代はそれらの雑誌を読みあさって無線機を作ったり、マニアックな改造をしたりしていました。

Y 興味の対象が、ラジオや無線からコンピューターに移ったということですね。

K その後、事情があって大学を中退することになるのですが、このときに、仕事を探そうと、スティーブ・ジョブズ氏に「仕事が欲しい」とメールを送ったのです。当時は、有名人のメールアドレスがネット上に公開されていましたから。結局、ジョブズ氏から仕事はもらえなかったのですが、その代わりに、当時の NeXT ジャパンの社長だったジェームス比嘉氏を紹介されたのです。

Y 比嘉さんというと、ジョブズの右腕といわれた人物ですよね。

K iPod や iTunes の発展に大きく貢献した優秀な方です。米国でメールのやりとりをした後、日本に戻ったときにあいさつに行ったのです。自分の中では遊びにいった感覚だったのですが、その日の夕方に人事部から「社長面接ありがとうございました」というメールが届き、その 1 週間後には、比嘉氏が NeXT ジャパンを退職して新たに立ち上げたソフトウェア会社で働くこととなったのです。



エル・ケンタロウ（El Kentaro）
幼少期をオランダで過ごす。留学した米国の大学でハッカー文化と出会う。自主退学を機に帰国し、1990 年代後半より IT 業界でキャリアをスタートする。インターネット系広告代理店やコンサルティング企業で経験を積む。英日バイリンガルであると同時に、IT・セキュリティ技術とビジネス分野の両面に精通している。

Y ドラマチックな話です。

K その後、紆余曲折を経て、1997 年頃に在籍していたデジタル系広告会社を同僚 5 人とともに退職し、新たな会社を立ち上げました。ネットを活用したシステム構築からコミュニケーションまで、より幅広い領域で顧客に寄り添うサービスを提供することを目的としていました。当時、マルチメディアの主役と目されていたのは、CD-ROM などの大容量メディアでしたが、僕らはネットこそがより巨大なマーケットになると考えていたのです。

Y その会社では、ケンタロウさんは具体的にはどのような業務をされていたのですか。

K 僕のメインのミッションは、米国で面白いソフトウェアやテクノロジーを持っている会社を見つけて、それを日本の実験的な広告主に提案してプロジェクト化することでした。Adobe Flash が Future Splash だった時代に、彼らを日本に呼びま

したし、日本で初めて Akamai のサービスに注目したのも僕でした。米国で新しいものを見つけては、日本の顧客に提案していました。

セキュリティ・カンファレンスの運営を通じてハッカーと親しくなる

Y 現在の SIer は、新しい技術を発掘するために現地法人を持つことも一般的ですが、当時、その先駆けとして活動されていたのですね。そこからどのようにセキュリティ分野へとつながっていったのでしょうか？

K 米国とのやり取りの中で知り合った人から「セキュリティのカンファレンス、Black Hat を日本で開催するので現場の手伝いをしてほしい」と相談されました。大学は演劇映像科でしたから、舞台の設営もできますし、英語も日本語も話せるので手伝うことにしました。それがセキュリティとの最初の接点でした。

Y Black Hat Japan の初開催はいかがでしたか？

K セキュリティ業界の人たちと関わってみると「この業界には自分みたいな人間がたくさんいる」と驚きました。オールドスクールなハッカーがいっぱいいたわけです。初めてセキュリティとハッキングと、自分が中高生のときからやってきたものすべてが 1 つにつながったように思えたのです。

Y その驚きというか感動が伝わります。

K アンダーグラウンドなオンラインマガジンの「Phrack」はもちろんのこと、LOD（Legion of Doom）、MOD（Masters of Deception）、L0pht（L0pht Heavy Industries）といった米国のハッカーグループが発信するテキストも読んでいました。その関係者が続々とイベントにやって来るわけです。そして、イベントを通じて彼らと親しくなったのです。これがセキュリティのプロフェッショナルたちと関わるきっかけとなりました。

Y Black Hat Japan にはその後も携わっていたのですか？

K はい。Black Hat Japan や PacSec の運営を手伝っていました。その後、会社を辞めて、海外との折衝に特化した会社を立ち上げたいと考えるようになったからです。当時、欧米のハッカーコミュニティから日本に持ち込まれる案件に対応できる人材は限られており、篠田佳奈さん（現・CODE BLUE 事務局代表）、高間剛典さん（Meta Associates）、そして僕の 3 人だけでした。それぞれの得意分野に応じて案件を振り分けながら対応していました。

Y 高間さんは長年 PacSec の運営に携わっていましたね。

K 僕自身、セキュリティエンジニアとしての経験はありません。SOC や NOC に常駐したこともなければ、マルウェア解析を行なったこともありません。とはいえ、技術に疎いわけではなく、代理店に在籍していた頃には、納品された Flash の挙動の異変からデコンパイルして問題点を特定し、修正を指摘することもありました。また、プレゼン相手の情報を、今でいう OSINT や HUMINT の手法を使って趣味レベルまで把握することもしていました。

Y ハッカーの素養はすでに身につけていたと。

K 代理店時代、僕は特殊案件担当として働いていました。要するに相手と友達になることがミッションだったわけです。そうした背景もあり、Black Hat Japan の運営や PacSec での通訳、さらに AVTOKYO でのボランティアスタッフとして活動する中で、仲間を増やすことができました。

Y そしてフリーになるわけですが、そのきっかけは何だったのでしょうか。

K ちょうど外資系の Web エージェンシーが一気に増えた時期がありました。それに伴い、セキュリティコンサルのような企業も次々と立ち上がりました。セキュリティの重要性が高まり、業界全体でそのウェイトが大きくなっていくのを感じたこともあり、会社を辞めてフリーとして活動することを決めました。

Y ちょうど機が熟したというタイミングだったのですね。

K フリーになった際、当時 Black Hat Japan のスポンサーだった日立システムズ（当時は日立情報システムズ）から、「新たに立ち上げる脅威インテリジェンスフィードの翻訳監修をお願いしたい」と依頼されました。そこから本格的にセキュリティ業界に関わるようになりました。米国の担当から深夜 3 時に脅威インテリジェンスのインシデントレポート（IR）が届き、それを日本向けに

翻訳・修正して朝 11 時までに納品するという作業を繰り返していました。そうした仕事が徐々に広がり、今にいたっています。

PC デスクから離れて町に出よう

Y ケンタロウさんは、世界的な Wi-Fi ハント大会である DEFCON の RF（Radio Frequency）CTF で好成績を残されていますが、どういう経緯で参加するようになったのでしょうか。

K もともと Wi-Fi ハントが好きで、若い頃からずっと取り組んでいました。以前、一度大会にも出場したことがあったのですが、その大会自体が終了してしまったのです。ところが、2020 年に DEFCON で Wi-Fi ハント世界大会 として復活すると聞き「楽勝だろう」と思って参加したのですが、結果は三十何位と散々なものでした。

Y AVTOKYO では、世界中の Wi-Fi AP を可視化する「WiGLE」に関する講演もされていましたね。

K WiGLE は、最初は遊び感覚で始めました。例えば、通訳の仕事で NATO のキャンプや横須賀基地に呼ばれた際、普通の人がなかなか行けないような場所にある AP を登録するのが楽しみでした。しかし、Wi-Fi ハントの世界大会では三十何位という結果に終わり、「1 年間本気で取り組んで、WiGLE のユーザーランキングでトップ 100 にランクインしよう」と決意しました。当時から WiGLE に熱心な友人がいて、彼は一度 2 位になったことを除けば、常に 1 位を獲得し続けていました。

Y ユーザー数も多そうですから、上位に入るのは大変そうですね。

K 1 位のレベルは 桁違い で、2 位から 20 位までの得点をすべて足しても追いつけないほどでした。そもそも WiGLE では 資金力のある人間が圧倒的に有利 です。クルマに無線受信機を何台も積み、アンテナを大量に立てて走り回れば、それだけで大量の AP 情報を収集できますから。だからこそ、僕は「歩いてハントすること」にこそ意義があると考えていました。地道に努力を積み重ねた結果、2 年目には 4 位〜 5 位にランクインすることができました。

Y ポイントは収集した AP の数で決まるのですか。

K WiGLE のポイントにはさまざまな加算方法がありますが、基本的には 新しく登録した AP の数 によって決まります。100 位以内をめざしたときは、年間で約 140 万 AP を追加しました。徒歩でのハントだったため、自宅周辺の AP はすぐに探索し尽くしてしまい、行動範囲をどんどん広げていくことになりました。その結果、1 年間で 4000km ほど歩きました。例えば、祖母の墓があるあきる野から都内の自宅までの約 40km を歩いたり、小田原から神宮外苑までの 100km を踏破するイベントに参加しながら WiGLE をしたりしていました。

Y 単純計算でも毎日 10km 以上です。もともと山歩きなどは好きだったのですか？

K 去年はいろいろと休んでいましたが、一昨年は高尾山に 30 回以上登りました。ほぼ毎週のペースですね。きっかけは、以前富士山に弾丸登山した際、自分の登山技術の未熟さを痛感したことでした。「山の練習は山でしかできない」と言われるように、行ける日は毎日のように登山していました。

Y 登山のどのような点に魅力を感じていますか？

K 登山は ハッキングにすごく似ている と思います。登山は、ひたすら歩き続けるという地味な作業の積み重ねですが、頂上に到達すると褒められます。しかし、実際には登頂は行程の半分に過ぎません。そこから 無事に下山することが重要なのです。ハッキングも同じで、新たなぜい弱性を見つけるまでは地道な作業の連続ですが、見つけた瞬間は称賛されます。しかし、その後の後片付けとなる、リスク評価・パッチ適用・対策の実施などについては、誰もあまり注目してくれません。そういう「本当に大事な部分ほど、目立たない」というところに、登山とハッキングの共通点を感じています。

Y 確かに似ていますね。登頂やぜい弱性の発見は、実は道半ばだという。

K 僕は 竹内洋岳さん という登山家の文章が大好きで、彼が「登山は想像するスポーツ」と言っているのがとても印象に残っています。彼の考えでは、登山で危険な目に遭うのはリスクに対する想像力が足りないからだと。この言葉が僕にはすごく刺さりました。そして、セキュリティも同じだと思うのです。実際のリスクの多くは想像力の欠落から生まれるものです。一方で、ハッキングは完全

AVTOKYO2024 では「Special hack " 虎の巻 "」と題する講演に登壇。DEFCON RF CTF 優勝チームの戦術を詳しく解説するとともに、日本チームの参戦を呼びかけた

に想像力が鍵であり、暗中模索のプロセスそのものです。そのプロセスが僕はとても好きなのです。

Y 想像力の欠落がリスク。まさにそのとおりだと思います。

K それに、コンピューターの前に座って作業することと、山に登ることってまったくの両極端ですよね。だからこそ、WiGLE や Wi-Fi ハントのような「歩く」ことが主体の活動が楽しいのです。これは、コンピューターに関連するものの中でも数少ない「外に出ないとできないこと」だからです。イメージとしては、ポケモン GO のオタク版みたいなものだと考えれば、分かりやすいかもしれません。

Y しかも、一度行った場所は、次に行ってもポイントにはならない。

K そう、新しい場所や、まだ通っていない道を探していかなくてはなりません。僕は東京に二十数年間住んでいますが、それでも新しい発見がたくさんありました。変わったお店、面白い建物、古い町並みなど、そういうものを見つけるのが楽しかったですね。寺山修司の「書を捨てよ町へ出よう」ではありませんが、まさに「外に出て遊ぼうぜ」という感覚。それがすごく好きでした。

Y 実際のマップを活用して陣地を取り合うゲーム「Ingress」に似ていますね。

K 僕らのように本気で取り組んでいる人たち にとって、WiGLE は塗り絵のようなものです。白地図を自分の足で歩きながら、少しずつ塗りつぶしていく感覚ですね。スマートフォンのアプリを使って GPS の軌跡で絵を描く「STRAVA アート」というものがありますが、WiGLE でも同じように軌跡を活用して遊んでいる人もいます。とはいえ、最終的に前述の友人が 1 位、僕が 2 位を取ることができたので、2 人で「もう引退だね」と言って、WiGLE は卒業しました。

RF CTF の魅力と現地に行くことの重要性

Y WiGLE を卒業して CTF に軸足を移したのですか。

K はい。RF CTF は非常に奥が深く、単に AP を数多く発見すれば勝てるというわけではありません。例えば、競技の 1 つに「キング・オブ・ザ・ヒル」という形式のものがあります。主催者が用意した AP にアクセスし、自分のチーム名を書き込むことでポイントが加算されるのですが、チーム名を書き込んだ瞬間に AP が落ち、60 秒間ロックがかかる ため、その間は誰も得点できません。

Y 単に技術力だけでなく、タイミングや駆け引きも重要になりそうですね。

K そのとおりです。上位 3 ～ 4 チームはニセの AP をたくさん作り、他チームが本物とニセモノ

の AP を見分けられないようにして妨害するのです。僕も妨害担当で、AVTOKYO の講演でも話をしました。

Y なんだかカオスな状況になりそうですね。

K 攻撃対防御ではなく、攻撃対攻撃という構図で、さらに正攻法以外でもポイントが取れるところが、RF CTF の面白さだと思います。例えば、「キング・オブ・ザ・ヒル」以外にも「フォックス・ハント」という競技があります。これは、AP を持って会場内を移動する「フォックス」と呼ばれる人物を探索するものです。僕は競技に参加していないふりをしながら、会場にいる知り合いに聞き込み調査をしました。すると、「誰々の彼女がフォックスらしいよ」といった情報を手に入れることもあります。これもまさに HUMINT の一種ですね。

Y 知り合いが多いからこそ有効な戦略ですね。ちなみにカンファレンスや CTF で仲良くなる秘訣はありますか？

K 最も効果的なのは、カンファレンスなどで自分の研究を発表することです。僕は前から「発表は自分の経歴を飾るためのものではなく、同じことに興味を持つ人と出会う最短の方法」だと言っています。反対に、発表者と仲良くなりたいのならとにかくその人の発表を聞くこと。会場でしっかり座って話を聞くことが大事です。あとは、海外のカンファレンスに行くことですね。やはり現地で直接交流することが、ネットワークを広げるいちばんの近道だと思います。

Y 積極的にコミュニケーションを取っていくことが必要なのですね。

K ただ、そういう友人と会っても セキュリティの話はほとんどしません。話題になるのは もっぱら趣味のことですね。それでも、友人が増えると困ったときに相談に乗ってくれますし、自然と最新の脅威情報が伝わってくる ようになります。気がつけば、そうしたつながりがいつの間にかネットワークになっているわけです。

Y カンファレンスには国内外を問わず、積極的に参加すべきなのですね。

K 多分、DEFCON、ShmooCon、AVTOKYO という世界三大ハッカーカンファレンス すべてで発表した数少ない日本人の 1 人だと思います。これは僕の自慢の 1 つですね。残念ながら、ShmooCon はもうなくなってしまいましたが。

Y 日本の AVTOKYO が世界三大ハッカーカンファレンスに入るとは驚きです。

K AVTOKYO は世界的に高く評価されています。海外に行くと、周囲から「AVTOKYO に行きたい」と言われます。これは、実際に参加した海外の人たちが「AVTOKYO、日本のハッカーカンファレンスが超楽しいよ！」と宣伝してくれているおかげですね。CODE BLUE も同様だと思います。

Y どちらも海外からの参加者が増えている印象があります。

K それはとても良いことなのですが、1 つ悩みの種があります。それは、海外から日本を訪れたハッカーを誰がアテンドするかということです。年間を通じてだと何十人にもなりますから対応には苦労します。

Y 反対に、日本人が海外のセキュリティ・カンファレンスに参加するケースが減ってきている印象があります。去年の Black Hat USA でも日本企業のブース出展がなかったと聞きます。

K 以前ならセキュリティ・カンファレンスに行けば、日本人や日本人グループに会うことができました。ですが、年々その数は減っています。たまに見かけても「キーノートだけ聞いて帰ります」と言われることもあります。でも、それではせっかく来た意味が薄れてしまうと感じます。海外のカンファレンスは、参加すればするほどメリットが返ってくる。 特に DEF CON はその傾向が顕著です。ただ「行くだけ」ではなく、コンテストに参加するなど他の人と積極的に関わることが重要だということを、もっと意識してほしいと思います。

若い世代こそ海外に行くべき

Y これまでのお話を伺っていると、セキュリティ・カンファレンスや CTF のようなコンテストに、もっと多くの人が参加してほしいと思いますね。

K エンジニアは「PC の前に座っている時間が大事」という考えが根強いですが、若いうちはいろいろな場所に遊びに行った方がいいと思っています。エンジニアのメインのミッションは「問題解決」ですよね。でも、普通の人が何に困っているのかを知らなければ、問題を解決できるはずがな

い。だからこそ、映画や芝居を観に行ったり、飲みに行ったり、散歩や海に出かけたりすることが、実はとても重要だと思います。僕はいつもそう思っています。

Y よい仕事を続けるためには、周囲からの刺激を受けることも大切ですね。

K「自分の得意なことだけを突き詰めるのが美徳」という考え方をアピールされることも、正直苦手です。例えば「夜な夜な取り組んでいます」と言われると、単に効率が悪いのでは？ と思ってしまうこともあります。僕自身も 地味な作業はしますが、それと同じくらい 外に出て違うことをすることが刺激になり、想像力を育む糧になっています。例えば、さまざまなセキュリティ・カンファレンスに参加し続けることで、業界の潮流が感じ取れるようになると思います。大切なのは、感性のアンテナの精度を高めることです。

Y 世界の CTF 大会に出場する日本チームも減っていると聞きます。

K 一時期は台湾のチームが世界中の CTF を席巻していました。その次は韓国、そしてその次は中国の時代がありました。ですが今はもう、台湾も韓国も中国も、CTF で勝てなくなってきています。では彼らはどこに行ったのかというと、Pwn2Own やバグバウンティに参戦し、本気で金もうけをする方向にシフトしています。今、CTF で優勝しているのは 特定の国のチームではなく、国を超えた混合チームばかりですよね。

Y カンファレンスの方でも日本の若い人の参加は少ないですか？

K カンファレンスの会場内でも外でも、顔を合わせるのは昔からの知り合いばかりで、若い世代と会う機会は少ないです。若い人に話を聞くと「行きたいけど、会社が行かせてくれない」という声をよく聞きます。でも、それでは駄目ですよね。若いうちは必ずしも重要なポストにいるわけではないですし、会社としても 1 週間くらい行かせてあげるべきです。若いうちに海外経験を積ませることは、企業にとっても圧倒的なメリット になると思います。

Y 若い人の方がいろいろなことを吸収できますし、それを会社に還元できると思いますね。

K そのとおりです。社会に出て長い年月がたち、

都内某所にあるエル・ケンタロウさんの事務所には、機材や資料が所狭しと並び、まるでコックピットか秘密基地のよう。その一画には、これまでに参加したセキュリティ・カンファレンスの参加証コレクションがある

すでに自分の価値観ややり方が固まってから海外に行くのは、むしろ大変だと思います。若いうちの方が、柔軟に吸収できるし、経験を楽しめる。そして、その経験の価値は将来的に必ず戻ってきます。僕も今まで、こうしたインタビューはあまり受けてこなかったのですが、最近は「受けてもいいかな」と思うようになりました。海外の窓口を務めることに少し疲れてきたからです。

Y そろそろ次の世代にバトンタッチしたいですね。

K 若い世代の人には、組織の上下の序列などを重視する日本の旧来のタテ社会から離れて活躍してほしいですね。それが結果的に国力のアップになります。若い人たちにどんどんチャンスを与えるべきだと思うし、きれい事ではなく年長者が生き残るためには若い人たちに頑張ってもらうしかないです。本当に、年長者による年長者のためのセキュリティ・カンファレンスは必要ないと思います。

Y 以前に比べれば、ハードウェアやサービスも充実しているので、セキュリティやハッキングの勉強のハードルも低くなっていると思います。その一方で若い人はなんだかピンと来ないという話も聞きます。

K それはもう、セキュリティ業界全体の問題ですね。今の若い世代にとって、インターネットは水道と変わらない当たり前の存在なのです。そのときに何人が「俺は配管屋になる」と思うのか、という話なのですよね。あまりにも透明で、意識する必要がないものになったからこそ、人々との意識の乖離（かいり）が生まれているのだと思います。

Y 仕組みや役割を正しく理解する必要がありますね。

K 現在、「公衆 Wi-Fi は危険です」といった記事が数多く出回っていますが、それだけでは本質が伝わりません。本当に伝えるべきなのは、「なぜ今、無線セキュリティが面白いのか？」という点です。僕は、これまでその魅力を伝えてきたつもりです。

Y かといって、昔話になってはいけませんよね。

K 昔のものの方が良かったわけではないのです。僕は、「昔のコンピューターの方がよかった」なんて言う人は信用しません。最先端の今の方が、圧倒的に良いに決まっています。ハッカー文化もセキュリティも、音楽と同じようなものだと思っています。好きなミュージシャンが「誰に影響を受けたのか？」をたどっていくように、ハッキングの歴史をさかのぼって学ぶことで、面白さがどんどん広がっていくはずです。

Y ほかに若い世代へのメッセージはありますか。

K 特に若い世代を見ていると、アウトプットにすごく注力している 印象があります。ただ、うまくコントロールできていない ことも多いように感じます。インプットをもっと取捨選択し、フィルタリングすることで精度を上げれば、アウトプットも自然と洗練されていくと思います。あとは何にでも興味を持って経験を積んでほしいですね。どんな経験もセキュリティにつながっていきます。

ハッキングとハイキングを続ける人生

Y 今後の抱負を教えてください。

K 僕がハッキングという言葉を知る前からハッキングしていたことを考えると、この先ハッキングという言葉がなくなっても続けていると思います。それと、僕のライフゴールの 1 つはハッカーのプロ化です。セキュリティのプロではないですが、ハッカーのプロになりたい。研究することをサポートしてもらえる体制ができたらいいですね。

Y スポーツがそうですよね。野球やサッカーをはじめプロ化が進んでいます。

K 例えば、野球で大谷翔平選手のようなスターが出てくると、野球界全体だけでなく、関連する産業や広告、メディア業界も活気づきますよね。セキュリティ業界は少し事情が違い、もう少し成熟が必要 だとは思いますが、それでもロックスター的な存在が何人かいる方が、さまざまな産業が盛り上がるのではないかと思います。

Y 将来はアムステルダムに移住したいとおっしゃっていたとか。

K 今でも移住したいと思っています。欧州にはハードウェア系のハッカーが多く、面白いことをたくさんやっている からです。欧州は圧倒的にローレイヤーのハッカーが多く、米国はミドルからハイレイヤーのハッカーが多い傾向があります。これは文化の違いやお金を稼げる環境の違いからきているのだと思います。欧州は、どちらかというと「マイスター感」を大事にしている印象があります。

Y 今、インタビューでお邪魔しているこの拠点も畳むことになるのでしょうか？ 秘密基地のような雰囲気があって、とても楽しい場所ですが。

K ここは手狭になってきたので、西八王子あたりにしたいですね。西八王子なら高尾山にも近いですし。以前はここが打ち合わせスペースになっていて、お客さんの出入りもありました が、今はそれもなくなったので、この場所にこだわる必要はありません。どこに拠点を移しても、これまでのようにハッキングとハイキングを続け、新たな発見をしていきたいですね。

Y 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 2025.02

文＝日立システムズ

年末年始に多発した DDoS 攻撃に関する事例の整理と影響について

【概要】：2024 年末から 2025 年始にかけて世界各地で大規模な DDoS 攻撃が確認されており、国内では航空会社や金融機関などが被害を受けた。本稿では、公開情報に基づいた事例の整理・分析を通じて、システム障害の背景にある要因についての考察を行ない、セキュリティ対策や事業継続計画の重要性を示す。

【内容】：2024 年末から 2025 年始にかけて、国内の航空会社や金融機関をはじめとしたさまざまな組織でシステムに障害が発生した。原因は、攻撃者が乗っ取った大量のコンピューターで構成されるボットネットから一斉にアクセスし、サーバーに負荷をかけてサービスを妨害する DDoS（Distributed Denial of Service）攻撃と推測される。そこで、マルウェアに感染しボット化したコンピューターの探索行為や DoS/DDoS 攻撃の跳ね返りなどのデータを収集・公開する Web サイト（NICTERWEB ※）で事実を確認した。

その結果、年年末年始にかけて、パケット送信元のホスト数が数分間で約 1.5 倍に急増した箇所が複数確認された。被害を受けた組織のシステム障害の発生時期と相関が見られ、データからも DDoS 攻撃の発生が確認できた。

航空会社や銀行など複数の組織で、システム接続の障害が発生し、多くが復旧までに 2 時間から 1 日程度を要した。システムが完全に停止したわけではないものの、一定の影響が生じたとみられる。 また、被害組織の調査では、障害発生から 1 時間後に原因とみられるルーターを特定し、一時的に切り離すことで復旧した事例も確認された。

この事例では、利用者がアクセスする Web システムは CDN（Content Delivery Network）上に配置され、その背後でアプリケーションサーバーやデータベースなどの関連システムが内部で通信・処理を行なっていた。今回の DDoS 攻撃により Web システムに過剰な負荷がかかり、背後のシステムのプログラム処理に問題が生じたことで通信障害が発生した可能性がある。このため、内部通信を中継していたルーターを取り除いたことで、大量の通信処理が収束し、システムが復旧したと考えられる。

このように、攻撃を契機に内部設計の問題が顕在化する可能性がある。平時から設計や設定にミスがないか確認することが重要である。ただし、DDoS 攻撃は対策を徹底しても完全に防ぐことはできない。常に攻撃のリスクを認識し、システム停止がビジネスやブランドの毀損に直結するサービスを洗い出し、事前に事業継続計画を準備しておくことが求められる。

今回の攻撃は多くの組織に影響を及ぼした大規模なものであり、十分なリソースを持ち何らかの意図を持った組織が関与している可能性がある。攻撃に関する声明は確認されていないものの、攻撃者は対象への負荷を通じて、対象だけでなく CDN などの大規模インフラの弱点や対応能力を探ろうとしている可能性が考えられる。

また、DDoS 攻撃に注意を引き、その背後で進行する別のサイバー攻撃を隠ぺいしようとしている可能性もある。そのため、DDoS 攻撃に対する確認や対策を行なうことは重要だが、システム全体のセキュリティを再点検することも推奨される。

※ **NICTERWEB** https://www.nicter.jp/

［**情報源**］https://www3.nhk.or.jp/news/html/20250112/k10014691191000.html

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

3. 追加情報編

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。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 社が提供する「Browser Tools」を利用して、Web ブラウザー履歴の特殊な挙動を確認します。また、Chrome の履歴が保存されている SQLite を確認します。

今回は、「3. 追加情報編」として、NirSoft 社が提供する「Browser Tools」を利用して、Web ブラウザー閲覧履歴などの特殊な挙動例や Chrome 履歴を SQLite から手動で確認する方法を実践します。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。なお、「3. 追加情報編」は、当初の予定より内容を変更を変更させていただきます。ご了承ください。

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なうことが可能です。

ソフトウェアの導入については、本誌 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

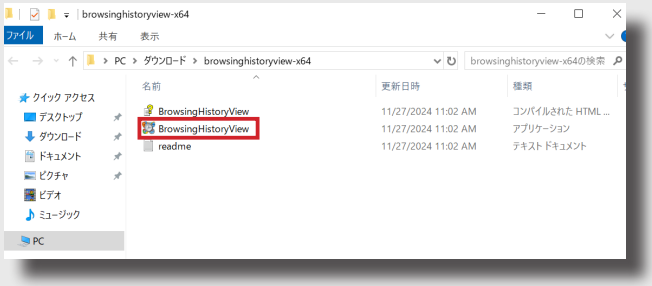
3. BrowsingHistoryView

3.1 BrowsingHistoryView の導入（すでに導入済みの方は次項にお進みください）

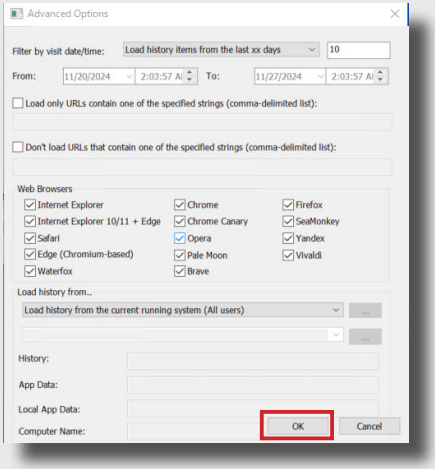
NirSoft で公開されている Browser Tools のうち、「BrowsingHistoryView」をダウンロードします。以下の URL にアクセスし、ご自身の環境に合わせた「BrowsingHistoryView」をダウンロードしてください。今回筆者は、「BrowsingHistoryView 64-bit」をダウンロードしました。

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

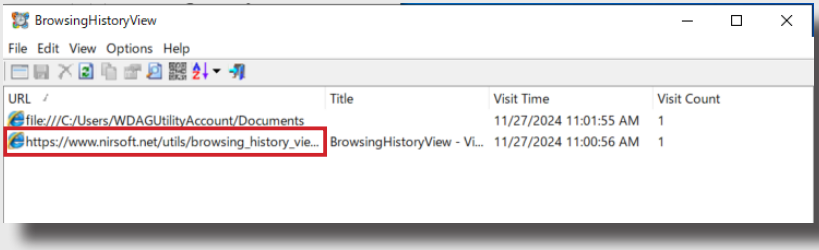
ダウンロードが完了しましたら、Zip ファイルを解凍、展開します。



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。



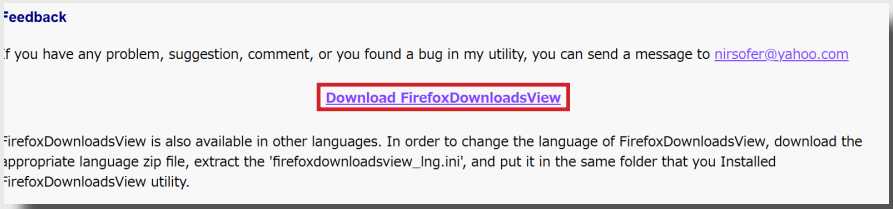
起動すると、「BrowsingHistoryView」をダウンロードする際に、NirSoft にアクセスした履歴が確認できます。



4. FirefoxDownloadsView

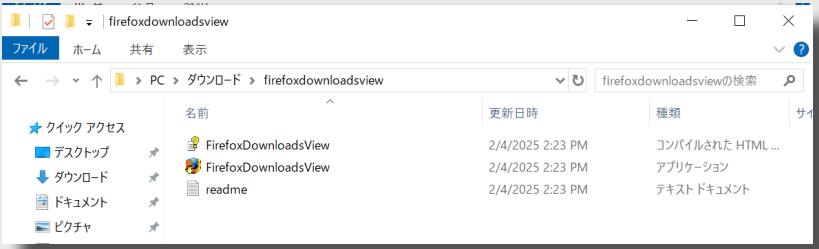
4.1 FirefoxDownloadsView の導入

Nirsoft で公開されている Browser Tools のうち、「FirefoxDownloadsView」をダウンロードします。以下の URL にアクセスし、「BrowsingHistoryView」をダウンロードしてください。

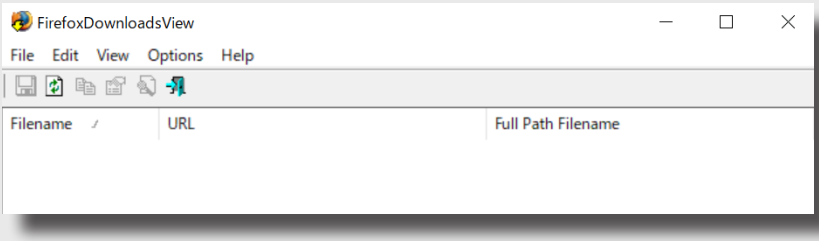


https://www.nirsoft.net/utils/firefox_downloads_view.html

ダウンロードが完了しましたら、Zip ファイルを展開します。



展開が終わりましたら、「FirefoxDownloadsView」を起動します。

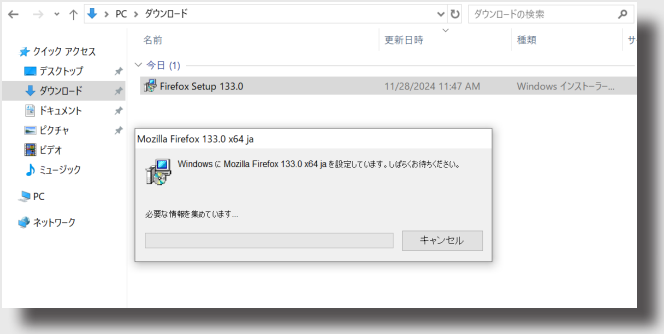


5. Firefox の特殊な履歴確認

5.1 Firefox のインストール（すでに導入済みの方は次項にお進みください）
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。



5.2 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。画面をスクロールして「専門家コラム」をクリック、「Hitachi Systems Security Journal」を開きます。次に、ドキュメントのいずれか（今回は Vol.66）を**左クリック**で開きます。

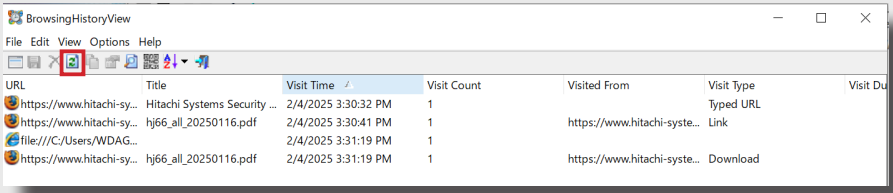
https://www.hitachi-systems.com/report/specialist/hj/index.html

Web ブラウザー上で PDF ファイルが開きます。

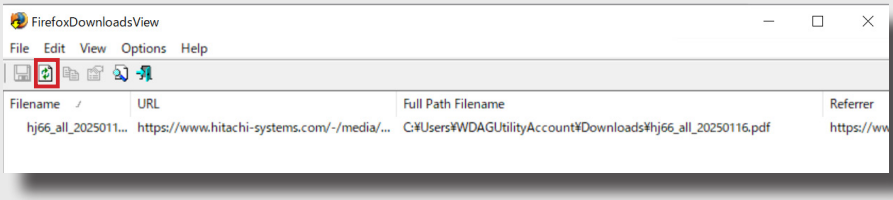
前のタブに戻り、「Hitachi Systems Security Journal」のいずれか（今回は Vol.66）を今度は**右クリック**して、「名前をつけてリンク先を保存」からダウンロードします。

5.3 ユーザーの操作の違いによる痕跡の違いを確認

BrowsingHistoryView、FirefoxDownloadsView を確認します。もしも、何も表示されない場合はリフレッシュボタンを押下してください。



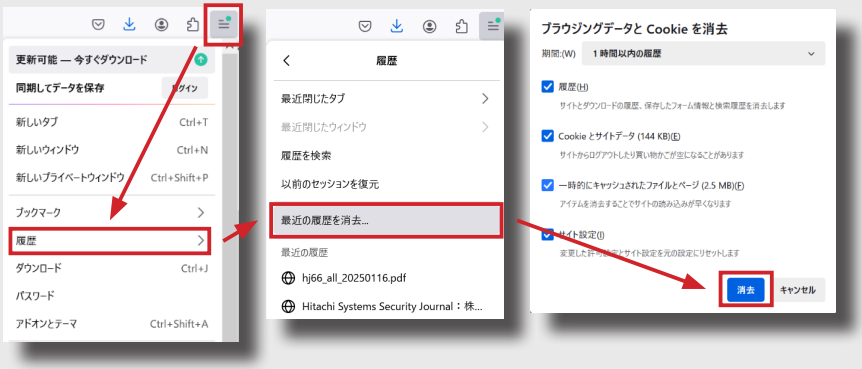
BrowsingHistoryView の画面



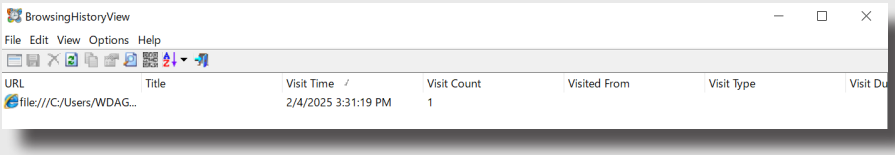
FirefoxDownloadsView の画面

BrowsingHistoryView では、右クリックしてダウンロードしたときのみ、file スキームによるログが表示されています。一方、FirefoxDownloadsView では、右クリックしてダウンロードしたときのログが表示されています。もしも、わかりにくい場合は、保存する際に別のファイル名やディレクトリを指定するよいでしょう。また、「FirefoxDownloadsView」では、「BrowsingHistoryView」では確認できない、保存先などの痕跡が確認できます。

次に、Firefox の右上のメニューをクリックし、「履歴」-「最近の履歴を消去」-「消去」と順にクリックして、閲覧履歴を消去します。
なお、消去が完了したら、必ず Firefox を終了してください。Firefox を終了させないとデータベースがロックされているため、次の作業が解説どおりに進みません。



再び、BrowsingHistoryView、FirefoxDownloadsView を確認します。閲覧履歴が削除されており、閲覧した URL がどこかは確認できなくなります。しかし、BrowsingHistoryView には file スキームのみが残存しており、ファイルの痕跡は確認できます。これは、file スキームの履歴が、Firefox ではなく別のアプリケーションによって管理されている領域に保存されているためと考えられます。



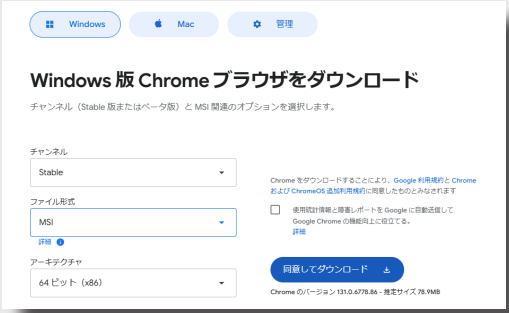
BrowsingHistoryView の画面

FirefoxDownloadsView の画面

今回確認したように、PDF の閲覧方法によって履歴の残り方が異なる、Web ブラウザーの履歴を消去してもコンテンツの閲覧履歴の一部が残存するなど、ユーザーの行動によって残存する痕跡が異なります。閲覧履歴を確認する際は、痕跡の残り方の特徴を調査し、理解しておくことが、ユーザーの行動を推測する上で重要な要素となります。

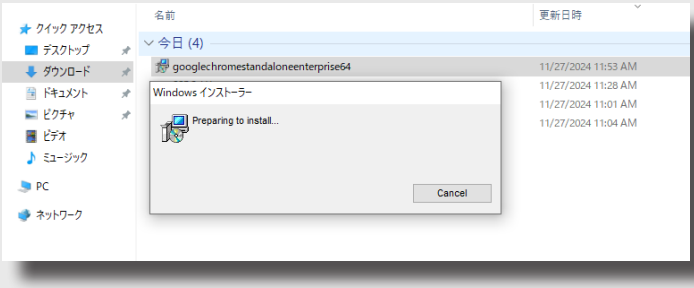
6. Chrome の履歴に関する追加情報

6.1 Chrome のインストール（すでに導入済みの方は次項にお進みください）
公式サイトにアクセスし、Chrome 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。筆者は以下の設定でダウンロードしました。



https://chromeenterprise.google/intl/ja_jp/download/#windows-tab

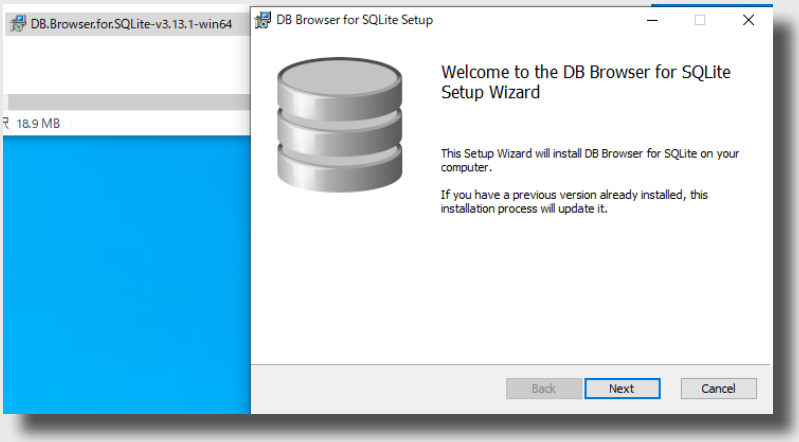
ダウンロードが完了しましたら、インストールを実行してください。



6.2 DB Browser for SQLite のインストール（すでに導入済みの方は次項にお進みください）
以下の URL より、「DB Browser for SQLite」をダウンロードします。
ご自身の環境に合わせてダウンロードしてください。今回、筆者は以下をダウンロードしました。

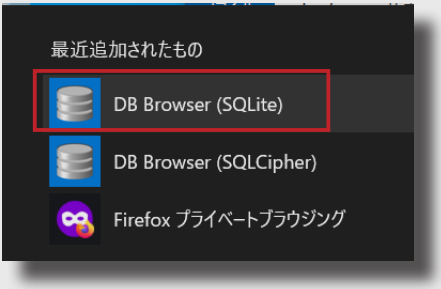
https://sqlitebrowser.org/dl/

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。

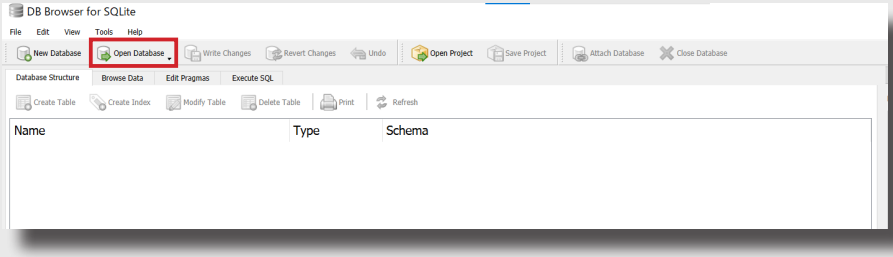


6.3 Chrome のダウンロード履歴（SQLite）の確認

Chrome を起動し、5.2 の手順で Hitachi Systems Security Journal を閲覧してください。
閲覧が終わりましたら、メニューより「DB Browser（SQLite)」を選択して、起動します。

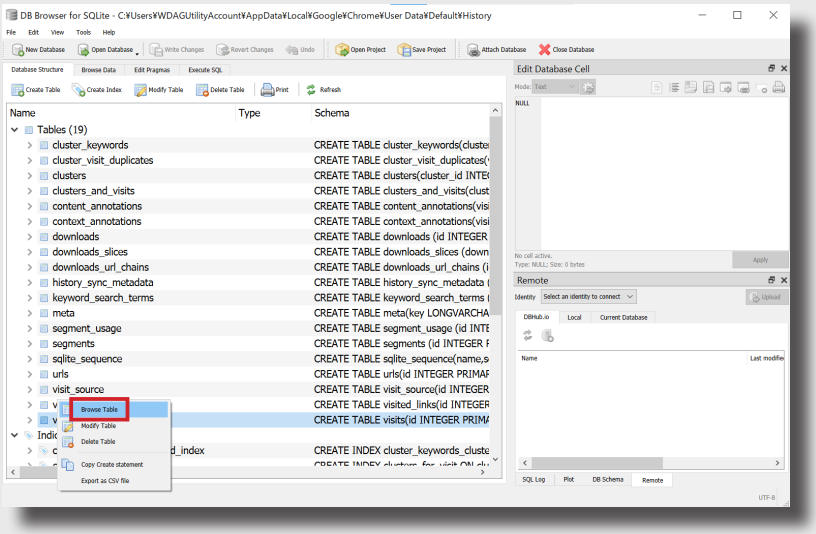


起動後、「Open Database」をクリックします。

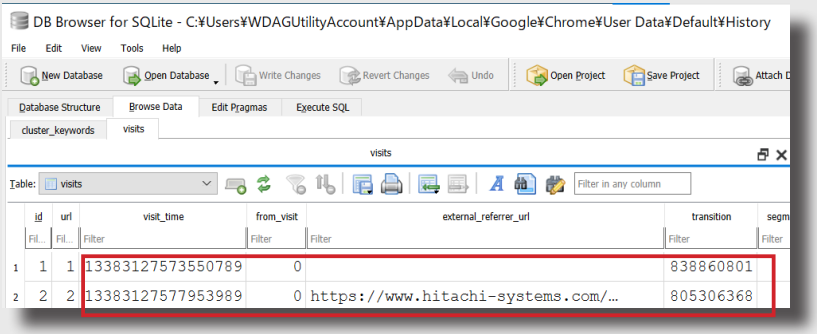


開くファイルは、前号で紹介した以下のファイルとなります。
C:¥Users¥[ユーザー名]¥AppData¥Local¥Google¥Chrome¥User Data¥Default¥History

次に、「visits」を右クリックし、「Browse Table」をクリックします。

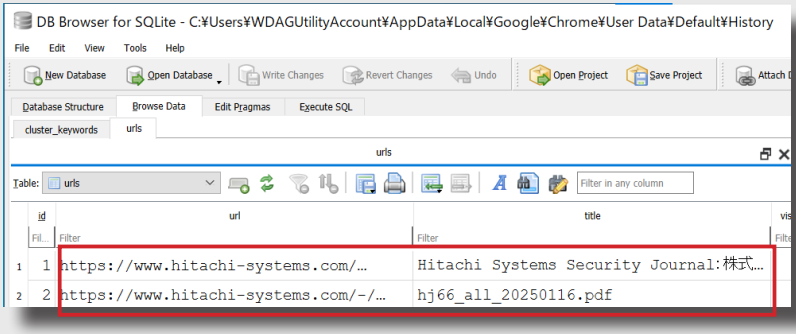


「visits」テーブルの中身が確認できます。



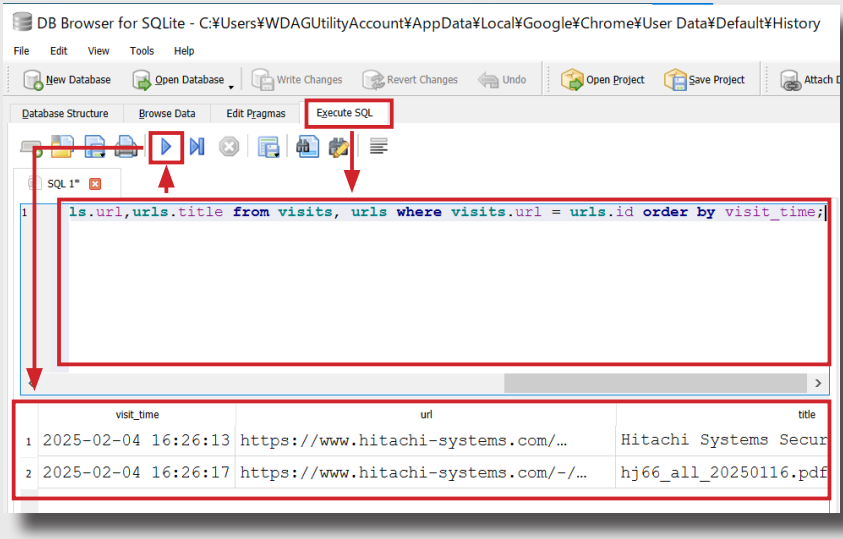
6.4 Chrome のダウンロード履歴（SQLite）の整形

先ほど確認した「visits」テーブルには、URL やページタイトルが存在しません。（前ページの図にある external_referrer_url は、遷移元の URL）。URL やページタイトルは、別テーブルの「urls」に正規化され格納されています。



今回は、「DB Browser for SQLite」を利用して SQL でデータを整形します。今回のタイムスタンプは、「WebKit datetime」と推察されます。「Execute SQL」タブを選択し、次の SQL を入力、実行ボタンを押下してください。

```
select strftime('%Y-%m-%d %H:%M:%S', (visits.visit_time/1000000) - (11644473600) + 9 * 60 * 60 ,'unixepoch') as visit_time, urls.url,urls.title from visits, urls where visits.url = urls.id order by visit_time;
```



閲覧履歴が整形されて出力されることを確認できました。

7. おわりに

今回はここまでとなります。

今回は、「3. 追加情報編」として、NirSoft 社が提供する「Browser Tools」を利用して、Web ブラウザー閲覧履歴などの痕跡や Chrome の履歴を SQLite から手動で確認する方法を実践しました。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 Web サイトへの接続状況を確認する際などに利用します。

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.68

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