HITACHI
Inspire the Next

Hitachi Systems Security Journal

VOL.69

株式会社 日立システムズ

Human * IT

Hitachi Systems Security Journal VOL.69

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

攻撃者の視点で明らかにする潜在的なリスク！
Google レッドチームのリーダーが語る
社内セキュリティチームの運営を成功に導く鍵とは !?

ステファン・フリードリ インタビュー

リスクを無視して快適に過ごすことは、偽りの安心感に過ぎない。レッドチームの役割は見過ごされがちなリスクを明らかにし、組織のセキュリティを強化すること。こう語るのは、Google レッドチームのリーダーであるステファン・フリードリ氏だ。昨年 11 月の CODE BLUE 2024 では「Google をハッキングする - 社内レッドチームの運営と成長の教訓」と題する講演を行ない、人気を博した。今回のインタビューにおいても、チームの目標設定やメンバー間の連携、さらにはバーンアウト（燃え尽き症候群）を防ぐ方法や経営層との関わりなど、幅広いテーマで話を伺った。

取材・文＝吉澤 亨史／通訳＝エル・ケンタロウ／撮影＝卯月 梨沙／編集＝斉藤 健一

テクノロジーに魅了された少年がセキュリティのプロになるまで

吉澤（以下 Y）：今日はとても興味深い講演をありがとうございました。

ステファン・フリードリ（以下 S）：まず、今回は Google の一員としてここに来ているため、Google としての活動の一環であることを強調したいと思います。私はレッドチームや攻撃的セキュリティサービスに長年関心を持ち、キャリアを通じて情熱を持って取り組んできました。欧米での研究成果を日本で発表できることを、大変嬉しく思っています。

Y ステファンさんがセキュリティに興味を持ったきっかけを教えてください。

S もともと、私の祖父は電子技師で、鉄道模型など多くの技術的な趣味を持っていました。その影響もあり、私も幼い頃からさまざまな技術に触れる機会がありました。何にでも興味を持ち、たとえ元に戻せなくても分解せずにはいられないような子供でした。やがて、その興味はコンピューターへと移っていきました。

Y 工学系に興味を持たれていたのですね。大学時代はどのように過ごされましたか？

S 私が入学した当時のスイスの大学には、まだセキュリティに関する学位がありませんでした。そのため、大学に通いながら独学でセキュリティを学びました。コンピューターは短時間で目的を達成できる一方で、意図しないことまでできてしまう。その奥深さに魅力を感じたのです。数年後、オンラインで交流していた仲間から、スイス初のペネトレーションテスト会社を立ち上げたという連絡を受けました。それをきっかけに、私はその会社に入社することになりました。

Y それが、セキュリティのプロとしての第一歩になったのですね。

S 少し変わった経緯ですが、私は運よく、良いタイミングで良い場所にいたのだと思います。今では多くの方からキャリアについてのアドバイスを求められることが増えましたが、私が歩んできた道は、現代では通用しないかもしれないと答えています。何しろ、それは iPhone が登場する前の時代の話ですから。

ステファン・フリードリ（Stefan Friedli）
情報セキュリティ分野で 20 年間以上にわたるキャリアを持ち、特にレッドチーミングとペネトレーションテストに注力している。スイスの金融機関や大規模な産業・政府機関に対してアドバイザーおよびコンサルタントとして従事していた。2019 年に Google に入社し、現在はテック・リード・マネージャーとしてレッドチームを率いている。CODE BLUE をはじめとして、BruCON（ベルギー）や BSidesLisbon（ポルトガル）など多くのセキュリティカンファレンスで講演を行っている。

Y それほどまでにテクノロジーの進展はめまぐるしいのですね。ところで、ステファンさんは講演の中でゲームが好きだとお話しされていましたが、どのようなゲームがお好きなのですか？

S 4 ～ 5 歳のときに、親に任天堂のファミコンを買ってもらって以来、ずっとゲームが大好きです。それ以降の任天堂のゲーム機はすべて持っていました。今はあまり時間が取れませんが、特にシミュレーション系のゲームが好きです。中でも、JRPG の 1 つである『聖剣伝説（LEGEND OF MANA）』には、特にのめり込みました。

Y RPG は、はまりますよね。日本の RPG を JRPG と呼ぶことは知りませんでした。

S ただ、『聖剣伝説』の続編はヨーロッパでは発売されませんでした。しかし、ネット上にはゲームファンによる翻訳があり、それを日本語版の ROM（記憶装置）に自分で組み込むことが流行し

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://archive.codeblue.jp/2024/results/results/#result-7

ていました。バイナリファイルに対して熱心な愛好家たちがこのような変更を加えられることに強い興味を惹かれ、脆弱なテクノロジーの仕組みについてもっと学びたいという好奇心が芽生えました。私は知的財産権の侵害を容認するものではなく、そうした行為に自ら関与することも、他人にそれを奨励することもありません。

Y はい。決して違法行為を推奨するわけではありませんが、実際にリバースエンジニアリングに興味を持つきっかけがゲームの改造だったというハッカーは大勢いると思います。

Google から届いた贈り物に不正アクセスの仕掛け

Y 講演では、Google から社員にプラズマボール※1が届いたという話から始まりました。

S はい。最初に種明かしをすると、このような公式ギフトが存在していたわけではありません。これは信頼できない USB デバイスのリスクを例示し、最終的にそのリスクを低減するための演習の一貫として特別に用意されたものでした。

Y なるほど。そのプラズマボールには不正なプログラムが仕掛けられていたというわけですね。

S そのとおりです。付属の USB ケーブルを PC に接続すると、自動的にコマンドが実行され、さらに別のプログラムをダウンロードして、PC 内にある新製品に関する情報を盗み出そうとしていました。不審に感じた彼はハードウェアチームに連絡し、回収して調査してほしいと依頼しました。しかし、実際に回収に来たのはレッドチームでした。

Y では、Google レッドチームの目的について教えてください

S レッドチームの目的は、攻撃者の視点で考え、行動することで、実際の攻撃を検知・対応し、阻止することです。そのため、内部者と外部者の 2 つの視点を持つことを推奨しています。Google のセキュリティエンジニアの役割は、セキュリティ体制を改善し、ユーザーや従業員を守ることです。しかし、それだけでなく、もう 1 つの視点として、攻撃者がどのような新しい攻撃ベクトル（システムやネットワークを攻撃する際に利用する経路）を狙っているのかを探ることも重要な任務となります。

Y 攻撃者の視点に立つということは、攻撃手法としてソフトウェアやハードウェアだけでなく、オンラインと物理の両方を活用するということですね。

S 起こりうる攻撃を実証することも重要ですが、私が最も重視しているのは、ブルーチームのスパーリングパートナーとしての役割です。ブルーチームは、レッドチームの攻撃に対抗しながらセキュリティを強化するチームです。私たちは、ブルーチームが持つ、インシデントレスポンスに関する手順や要領などをまとめた「プレイブック」を実際にテストし、練習する機会を提供します。そして、新たな問題点を特定し、彼らがまだ気づいていないリスクや盲点を浮き彫りにすることが、レッドチームの重要な役割なのです。

Y レッドチームが登場したことで、従来のセキュリティチームがブルーチームと呼ばれるようになりました。また一時期、両者のバランスを取る「パープルチーム」という概念も話題になりまし

※1 **プラズマボール：**透明なガラス球の内部に電極とネオンなどのガスを封入した装置。通電すると、内側の電極から外側のガラス球に向かって色鮮やかな放電が発生し、光の筋が揺らめくように見える。インテリアとしても人気が高い。

たが、現在はレッドチームとブルーチームの2チーム体制が一般的なのでしょうか。

S 確かに、一時期は色でチームを分類することが流行しました。しかし、それが本当に現実的で有効なのかについては、正直なところ疑問を感じています。なぜなら、セキュリティチームの理想は、すべてのメンバーが同じ目的に向かって協力することだからです。チームを色で分けることで、かえって分断が生まれてしまう懸念があります。本来、レッドチームとブルーチームは対立する関係ではなく、異なる役割を担いながら、同じゴールに向かって連携する存在なのです。

Y 企業が自組織で企業がレッドチームを構築する動きが活発化し、それに伴い、従来のセキュリティチームも単なる防御にとどまらず、脅威ハンティングなどより積極的な姿勢のブルーチームへと変化してきています。こういった流れは世界共通なのでしょうか。

S おそらく、世界的にも同様の流れがあると思います。これまで、セキュリティは組織内で二次的な扱いを受けることが多かったと感じています。IT 管理部門の業務の合間に対応したり、専任ではなく兼務の担当者が対応したりするケースが一般的でした。しかし、近年は組織的にセキュリティを強化する動きが進んでいます。その背景には、政府や業界によるさまざまなコンプライアンスの強化があると考えられます。これは、世界的にも共通した傾向だと思います。

Y レッドチームは社内で明確な役割を持っていると思いますが、ブルーチームも同様に独立したグループとして明確に存在しているのでしょうか？

S おそらく、ブルーチーム側も同様に、自分たちの業務を明確に整理していると思います。これは決して悪いことではなく、むしろ自分たちが責任を持って組織内でこの機能を提供していることを示す、重要な開示の一環です。何万、何億ものユーザーを守るうえで、各チームの責務が明確になっていることは不可欠だと考えています。

Y レッドチームとブルーチームは対抗する組織のように思われがちですが、実際には攻撃と防御の両面からセキュリティを強化していくという共通の目的を持っているのですね。

S 私の講演でもお話ししましたが、私たちは必要

「本来、レッドチームとブルーチームは対立する関係ではなく、異なる役割を持ちながら協力し、共通の目的に向かうべき存在であり、セキュリティチームを色で分類することの有効性には疑問がある」と語るフリードリ氏

なツールを自ら開発し、それをオープンにすることでブルーチームを支援してきました。ゴールは同じですが、その目的を達成するためには、適したツールを活用することが重要だと考えています。

Y Google では、レッドチームとブルーチームはそれぞれ何名ほどの規模の組織なのでしょうか？

S 残念ですが、その情報は開示していません。ただ、一般的な大企業では、レッドチームの人数はブルーチームに比べて圧倒的に少ないと思います。 その理由は、ブルーチームには運用側のメンバーが多く含まれるからです。彼らは 24 時間体制でシステムを監視し、実際の攻撃に対する防御策を講じています。その対策の一環として、私たちレッドチームが仕掛けるシミュレーション攻撃にも対応しています。 こうした組織のバランスを考えると、ブルーチームのほうが必然的に大規模になるのは当然のことだと思います。

セキュリティチームのメンタルケア

Y レッドチームもブルーチームも、非常にハードな業務だと思いますが、その中に楽しさを見出すことはできるのでしょうか。他のメンバーから、そのような話を聞くことはありますか。

S 私個人の感覚としては、常に目の前に新しいパ

フリードリ氏は「常に全力を求める組織では若手が燃え尽きる恐れがある。短期的な成果だけでなく、持続的な成長を促す環境と、それを支えるリーダーの存在が重要」だと考えている

ズルが置かれていて、それを解いていくチャレンジの楽しさは確かにあります。さらに、状況が絶えず変化するため、常に刺激的です。しかしその一方で、常に安心できない不安感や焦燥感に追われることもあり、それが大きなストレスになることも事実です。

Y ストレスに対して、どのように気分転換をしているのでしょうか。また、同じような悩みを抱えるメンバーから相談を受けた際には、どのようなアドバイスをされていますか。

S 年齢を重ね、家族ができるなど環境が変わる中で、私自身の人生の優先順位も変化してきました。しかし、若いチームメンバーにとっては、必ずしも同じとは限りません。特にレッドチームでは、常に新しい脅威を見つけ、新たな攻撃手法を考え、これまでにない境界線を発見していくことが求められます。そのため、組織内でのリーダーシップの役割が非常に重要になると考えています。

Y リーダーの影響によって、メンバーの考え方や認識も変わっていくということですね。

S 例えば「常に全力で突き進むこと」を奨励するような組織を作ってしまうと、若いメンバーが燃え尽きてしまう可能性があります。そのため、短期的な成果だけでなく、長期的な視点で持続的に成長できる環境を整え、メンバーを導いていけるリーダーの存在が重要だと考えています。

Y 講演の中で「ホワイトカード」という言葉が出てきましたが、その意味についてもう少し詳しく教えていただけますか。

S 呼び方はいろいろありますが、基本的な考え方として、レッドチームの演習において「実施しないステップ」を設ける必要があるということです。例えば、特定の攻撃手法が実際の製造プロセスや事業運用に大きな影響を与える可能性がある場合、そのステップは一時的に省略すべきケースがあります。代表的な例としては、横展開（Lateral Movement）の検証 などが挙げられます。シナリオを最後まで完遂することを優先する際には、影響の大きい部分を飛ばしながら次のステップへ進むこともあります。「ホワイトカード」とは、そうしたプロセスを指します。

Y 社内への影響を考慮しながら、想定したステップと実際のステップを臨機応変に調整していく、ということですね。

S ホワイトカードをうまく活用している組織は、それを構造化されたプロセスに組み込んでいます。例えば、グローバルで発生するゼロデイのぜい弱性※2 や、nDay のぜい弱性※3 を突いた場合でも、影響範囲をユーザースペース内に制限し、対象領域を明確にすることでリスクを管理しています。こうした運用は、ある程度構造化された形で実施されることが多いと思います。

Y 実際に障害を引き起こしてはいけない、ということですね。

上司や経営層との関わり方

Y 最近気になっている、または興味深いと感じている新しい技術があれば教えてください。

S 私は好奇心が強く、さまざまな分野に興味を持つ性格だとお話ししましたが、最近の技術動向の中で最も分かりやすい答えの 1 つは AI の台頭だ

※ 2 ゼロデイぜい弱性：その存在が公表される前や修正用プログラムがリリースされる前のぜい弱性。
※ 3 nDay ぜい弱性：すでに公開されているぜい弱性であり、ベンダーや開発者がパッチを公開しているか、作成中であるもの。

と思います。AIは、技術的な側面だけでなく、法的な枠組みや政策面など、多方面で急速に変化し、拡大している点が非常に興味深いと感じています。実際、私のチームの隣にもAI専門のレッドチームが立ち上がっています。

Y それは、AIエージェントをレッドチームの活動に生かすというものなのでしょうか。

S 私はそのチームのメンバーではないため詳細は分かりませんが、現在そのような取り組みが進められているのは確かです。そのため、今後のAIの発展と、それに伴うレッドチームの活動には、引き続き注目していきたいと考えています。

Y 社内でも、特に役員レベルではレッドチームの存在や役割を十分に理解していないケースがまだ多いと思います。そうした方々に対して、レッドチームの重要性を説明する際に効果的なフレーズがあれば教えてください。

S なかなか難しい質問ですが、私がよく使うのは「リスクを無視して快適に過ごすことは、偽りの安心感に過ぎない」という言葉です。一見、安全に思える状況でも、実は私たちが気づいていないリスクが潜んでいるかもしれません。レッドチームの役割は、見過ごされがちなリスクを明らかにし、組織の強化につなげることです。このプロセスを通じて、隠れた不安を顕在化させ、より強固なセキュリティ体制を築くことができます。

Y 先日、CODE BLUEとは別のカンファレンスでGoogle社員のセッションを受講したのですが、Googleでは Chrome ブラウザーをエンドポイントとして捉え、セキュリティ対策を行なう という考え方があると知りました。そのアプローチが非常に新鮮で興味深いと感じました。

S Chrome OSの普及が進み、さらにChrome ブラウザーがあらゆるデバイスに搭載される中で、その利用形態を考えると、組織としてセキュリティ対策に注力するのは必然の流れだと思います。

念願だったCODE BLUEでの登壇

Y CODE BLUEや日本についての印象をお聞かせください。まずは、CODE BLUEについてどのように感じていますか。

S CODE BLUEを非常に楽しく体験させていただきました。実は、もう10年以上前からCODE BLUEに参加したいと思っていたんです。初回か2回目の開催時に、私の友人が登壇し、その体験を話してくれました。その話を聞いて以来、CODE BLUEに強い憧れを抱いていました。

Y 満を持しての参加だったというわけですね。

S なかなか実現する機会がありませんでした。Googleに勤めるようになり、「今度こそ」と思っていたのですが、新型コロナウイルスの流行によりバーチャル開催になってしまいました。コロナが落ち着いた頃、GoogleのCTFで日本を訪れたのですが、その際に参加者の誰かがCODE BLUEの話をしていて、「そうだ、CODE BLUEだ！」と思い出しました。今年、発表の機会をいただけたことは非常に幸運だと感じています。また、これまでのCODE BLUEに関しても、組織全体を含めて、とても楽しい体験をさせていただいています。

Y CODE BLUEと海外のカンファレンスには違いがありますか？もしあるとすれば、どのような点でしょうか？

S CODE BLUEの魅力は、プロフェッショナル向けのカンファレンスとしての雰囲気を保ちつつ、オープンに会話ができる環境があることです。セキュリティに真剣に取り組んでいる方々が多く集まっているにもかかわらず、堅苦しさがなく、自由に意見を交わせる雰囲気があります。参加者一人ひとりの熱意や努力が、直接伝わってくるのを感じます。

Y 世界のセキュリティカンファレンスでは、そういった雰囲気はあまり見られないのでしょうか？

S 世界の大規模なカンファレンスとCODE BLUEの違いは、内容の本質が重視されている点にあると感じます。他のカンファレンスでは、マーケティング色が強く、ベンダーによる製品説明セッションが多くなることもありますが、CODE BLUEはより技術的で実践的な議論が中心となっているのが特徴です。

Y 近年のセキュリティカンファレンスでは、ぜい弱性やマルウェアに関する話題が多く、日本ではそれらに取り組む人がまるでスーパーヒーローのように称賛される雰囲気があると感じます。その中で、ステファンさんの講演は ジェネラルかつ非技術的な視点 で語られていて、新鮮でとても興味

「自由に会話できる雰囲気が魅力。真剣にセキュリティに取り組む参加者が集まりつつも堅苦しさがなく、熱意や努力が直接伝わる場となっている」と CODE BLUE の印象を語るフリードリ氏

深かったです。

S 私自身、さまざまな CFP（Call for Papers：講演募集）のレビューボードに参加していますが、世界のカンファレンスでも幅広い分野から関心を集めるテーマを選ぶことは必然だと考えています。もともと技術的なセッションが得意で、非技術的な講演には今でも自信があるとは言えません。しかし、多くの人にとって技術以外の視点にも大きなニーズがあるということは強く実感しています。

Y 確かに膨大な CFP から講演者を選ぶことは大変だと思います。

S もちろん、技術的なセッションも重要だと思います。CODE BLUE のレビューボードには多くの友人がいますが、講演の選定において 絶妙なバランスを保つ能力 が非常に高いと感じています。昨年、日本政府やさまざまな産業の方々と話す機会があり、その中でレッドチームに対するニーズが日本でも非常に高いことを実感しました。そのため、今回レッドチームに関する講演をする機会をいただけたことは、とても意義深かったと思っています。

Y 最後に、日本についての印象もお聞かせください。

S よく「スイスと日本は似て非なる国」と言われますが、日本に来るたびに、それは確かに間違いではないと感じます。どこか懐かしく、安心できる雰囲気がありながらも、新しい刺激的な要素があるので、とても楽しめます。今回も、新しいスピーカーや運営の方々と交流する機会があり、とても充実した時間を過ごせました。日本語は話せませんが、この独特の雰囲気を感じるために、今後も継続して参加したいと思います。

Y 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 2025.03

文＝日立システムズ

認証情報の管理徹底：情報窃取マルウェアが狙うオンラインに保存した認証情報

【概要】：管理が不十分な認証情報を攻撃者に窃取される情報漏えい被害が発生している。攻撃者に狙われるのは、業務と個人の両端末で管理されたオンラインのパスワードマネージャーに保存する認証情報である。今回は、オンラインで管理された認証情報を攻撃者が窃取する手口を紹介し、認証情報の管理ポリシーの厳格化の重要性を提言する。

【内容】：認証情報の管理不備を狙ったサイバー攻撃が発生し、窃取された認証情報が悪用され、不正アクセスによる情報漏えいが発生している。盗まれた認証情報はダークWebで売買され、暗号資産の不正送金やVPN経由での機密情報漏えい、ランサムウェア感染などの被害につながる。国内外で多くの被害が報告され、豪州のサイバーセキュリティセンターも2024年9月に注意喚起を発している。

サイバー攻撃者に狙われるのは、従業員が利用するクラウドのパスワードマネージャーに保存された認証情報である。業務用の認証情報をWebブラウザーに保存すると、意図せず同期され、私用端末にも保存される。この時、私用端末が「情報窃取型マルウェア（Infostealer）」に感染すると、保存された認証情報が盗まれ、不正アクセスにつながる可能性がある。当社でも海外グループで同様の攻撃を観測したが、情報漏えいには至らなかったことを確認している。

ここからは、同期されたパスワードマネージャーの認証情報を窃取する攻撃手法を検証する。まず、「業務用端末（A）」と「私用端末（B）」を用意し、共通のGoogleアカウントでChromeにログインする。同期をオンにすると、端末Aの業務用認証情報が端末Bにも保存される。履歴やブックマーク、Wi-Fiネットワークなども同期される。

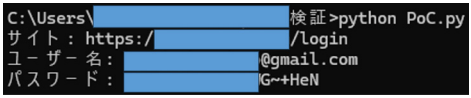


図 復号した認証情報

Chromeの認証情報は、端末のローカルファイル内にAESで暗号化され、SQLite形式で保存されている。マルウェアに感染しても暗号化されているため安全と思われがちだが、復号に使われるAESの鍵は端末内の別ファイルに平文で保存されている。

マルウェアはAESの鍵を用い、暗号化された認証情報を容易に復号できる。模倣プログラムを実行すると、図のように端末Aで入力した認証情報を端末Bで確認できた。本攻撃はGoogleパスワードマネージャーを経由せず、端末のファイルから認証情報を窃取するため、Webブラウザーの対策では検知や防御が難しい。

検証した手法により認証情報が漏えいし、不正アクセスやランサムウェア被害で事業停止や財務損失が発生する可能性がある。個人情報が漏えいすれば法的対応が求められ、リスクが発生する。窃取された情報がダークWebに流出すると、顧客の信頼を失い、株価にも影響を及ぼし、ブランド失墜の恐れがある。業務端末での個人クラウドサービスの利用禁止を徹底し、業務と個人の認証情報を分けて管理することを推奨する。

［情報源］https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/silent-heist-cybercriminals-use-information-stealer-malware-compromise-corporate-networks
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

4. 追加情報編 2

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 氏がブラウザの履歴等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 4 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。

4. 追加情報編 2
NirSoft が提供する「Browser Tools」を利用して、Web ブラウザーを利用した検索履歴を確認します。
また、「Password Tools」を用いて Web ブラウザーに保存された認証情報を確認します。

今回は、「4. 追加情報編 2」として、NirSoft が提供する「Browser Tools」を利用して、Web ブラウザーを利用した検索履歴を確認します。また、「Password Tools」を用いて Web ブラウザーに保存された認証情報を確認します。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、マルウェアの感染拡大経路を確認する際などに利用します。なお、「4. 追加情報編 2」は、当初の予定から変更して掲載しております。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。

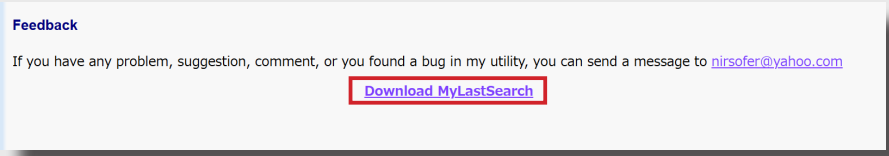
ソフトウェアの導入については、本誌 Vol. 66※で紹介していますので、そちらをご覧下さい。

※ https://www.hitachi-systems.com/-/media/report/specialist/hj/download/hj66_all_20250116.pdf

3. MyLastSearch

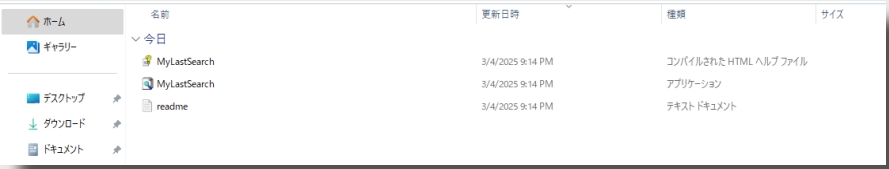
3.1 MyLastSearch の導入

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

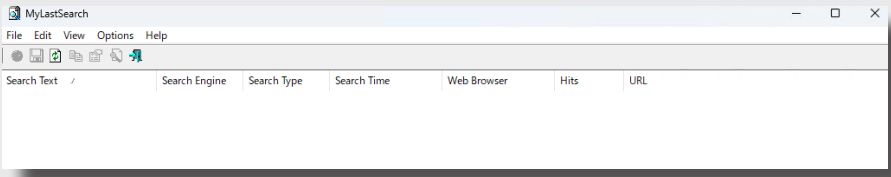


https://www.nirsoft.net/utils/my_last_search.html

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。

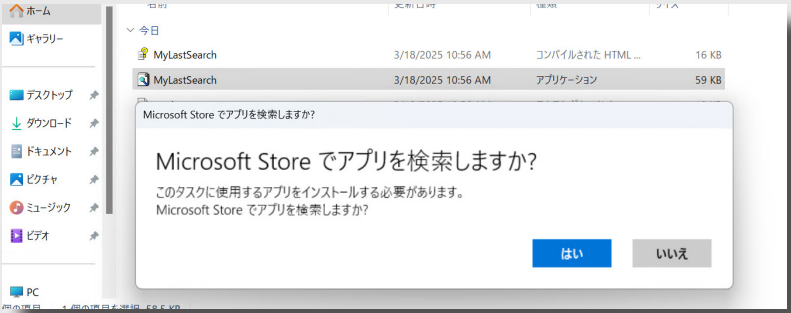


展開が終わりましたら、「MyLastSearch」を起動します。

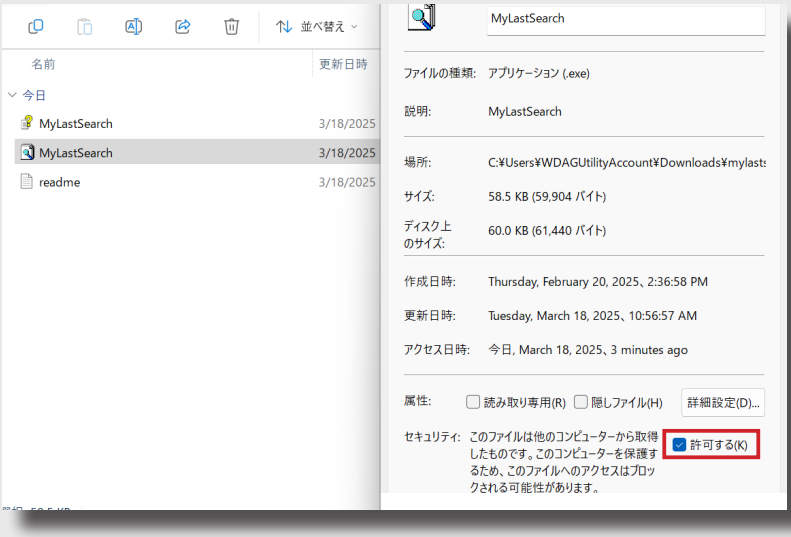


3.2 アプリケーション起動の注意点

Windows11 以降のサンドボックスを利用いている場合、ZoneID が原因で MyLastSearch が正常に起動できない場合があることを確認しています。

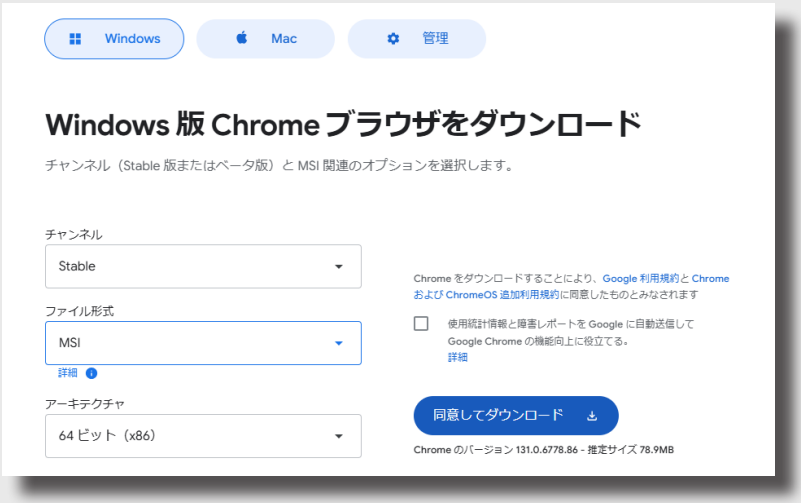


上記のようなダイアログが表示され起動できない場合は、プログラムを右クリックし、セキュリティの項目で「許可する」にチェックを入れてから起動してください。



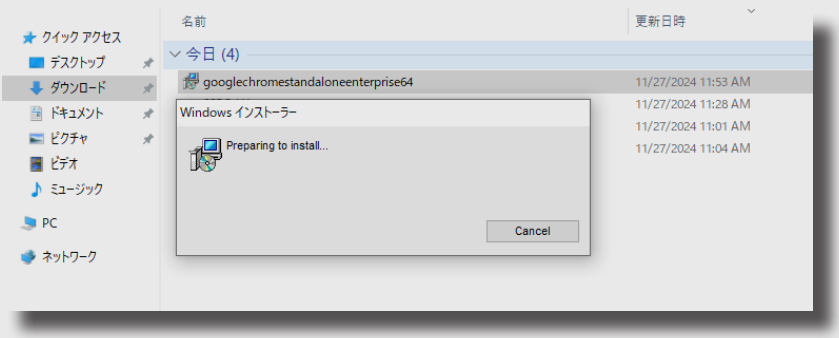
4. Chrome の検索に関する追加情報

4.1 Chrome のインストール（すでに導入されている方は次項にお進みください）
以下にアクセスし、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。筆者は図の設定でダウンロードしました。



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

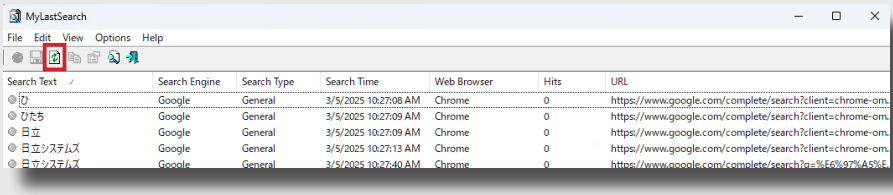
ダウンロードが完了しましたら、インストールを実行してください。



4.2 Google Chrome による検索

Google Chrome を起動し、検索ボックスに**「日立システムズ」を入力 (コピーではなくタイピングしてください) し、検索します。**

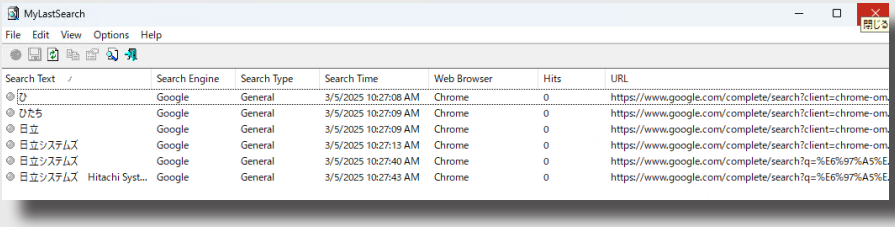
検索が終わりましたら、「MyLastSearch」を更新してください。



更新すると検索ボックスに入力した文字が、表示されていることを確認できます。ユーザーがどのような文字列で検索を実施したのかを確認できます。

次に、**「Hitachi Systems Security Journal」をコピー & ペーストして検索します。**

検索が終わりましたら、「MyLastSearch」を更新してください。



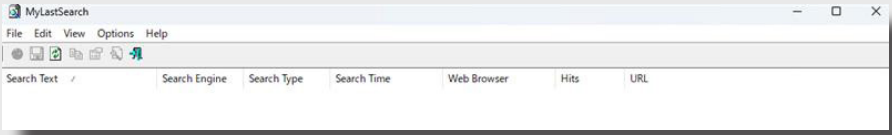
Google Chrome を用いた検索における「検索キーワード」を確認することができました。また、この結果より、「Search Time」が異なることからも Google Chrome を用いた Google 検索においては、タイピングを行なう過程で常に検索リクエストを送信していることがわかります（インクリメンタルサーチと呼びます）。

4.3 Google Chrome の履歴削除による影響

Google Chrome を起動し、右上の設定項目より、「閲覧履歴データの削除」を選択します。

「閲覧履歴データの削除」ダイアログが表示されますので、「データを削除」を押下します。

「MyLastSearch」を更新すると、検索履歴が削除されていることがわかります。



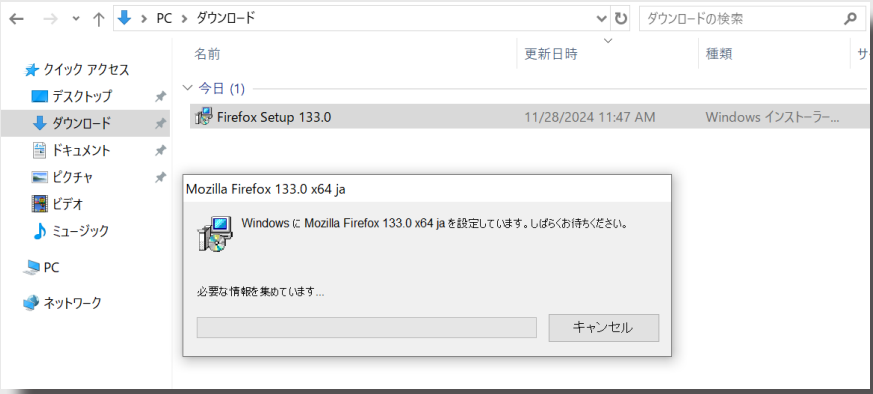
5. 認証情報の確認

5.1 Firefox のインストール（すでに導入されている方は次項にお進みください）

以下にアクセスし、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。筆者は図の設定でダウンロードしました。

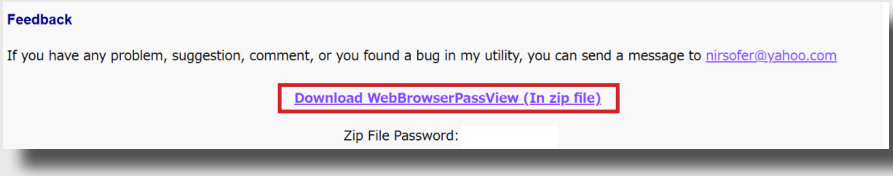
https://www.mozilla.org/ja/firefox/all/desktop-release/

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。



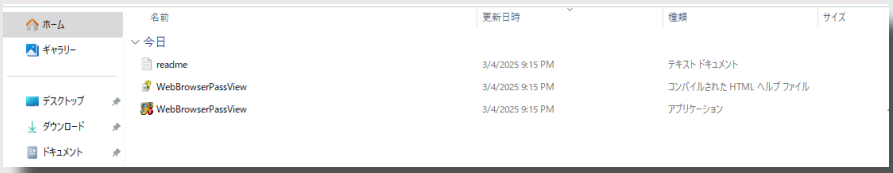
5.2 WebBrowserPassView の導入

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

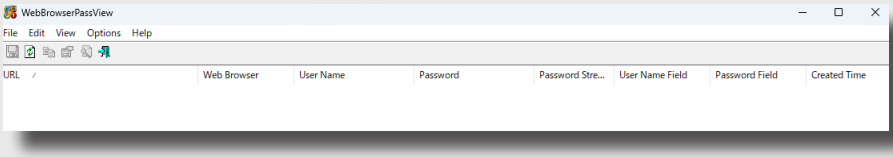


https://www.nirsoft.net/utils/web_browser_password.html

「WebBrowserPassView」の Zip ファイルはパスワードで保護されています。これは、「WebBrowserPassView」がアンチウイルスソフトなどに検出されている可能性があるためと考えられます。展開は、サンドボックス内など必ず安全な環境で実行してください。



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



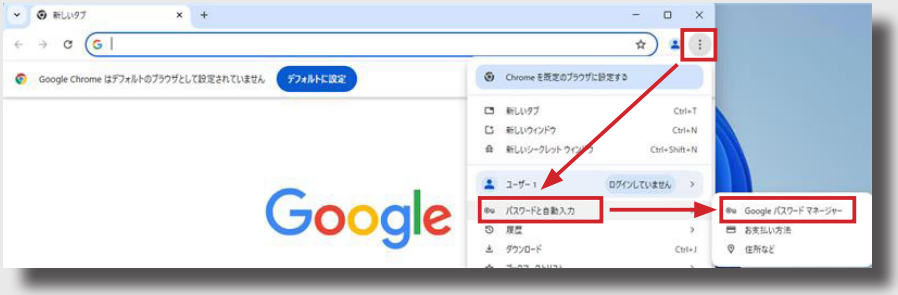
なお、起動ができない場合は、「3.2 アプリケーション起動の注意点」に記載されている注意を確認し、同様の手順で起動してください。

5.3 Web ブラウザーの認証情報確認

「WebBrowserPassView」では、各 Web ブラウザーに保存されている認証情報を容易に確認することができます。**本稿の目的は、各 Web ブラウザーに保存されている認証情報がセキュアに保存されていないことを検証することにあります。本稿で得た知識を決して悪用しないよう、お願いいたします。**

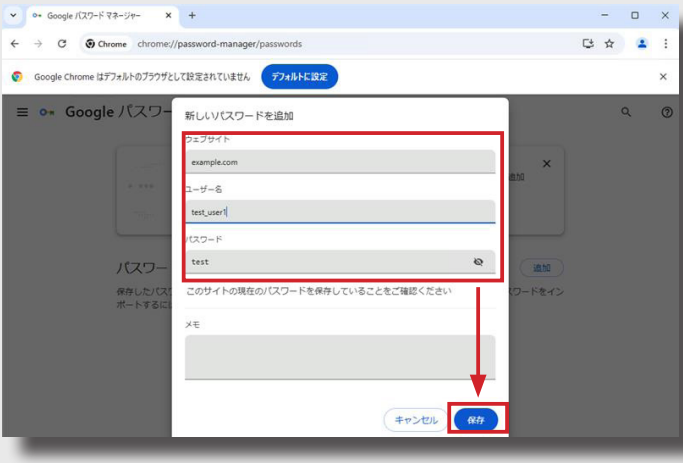
5.4 Google Chrome の認証情報確認

Google Chrome を起動し、右上の設定項目より、「パスワードと自動入力」、「Google パスワードマネージャー」の順に選択します。

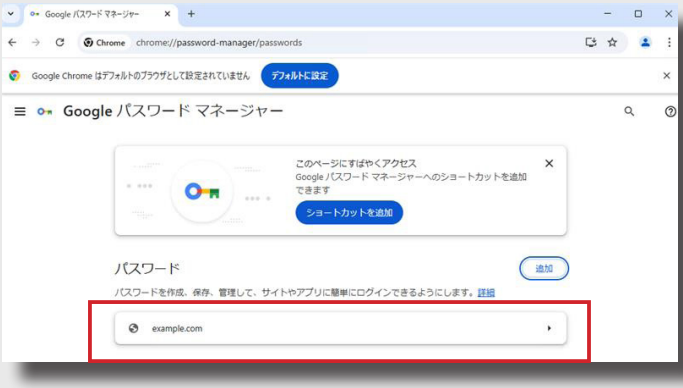


選択後、「Google パスワードマネージャー」が起動しますので追加を押下します。

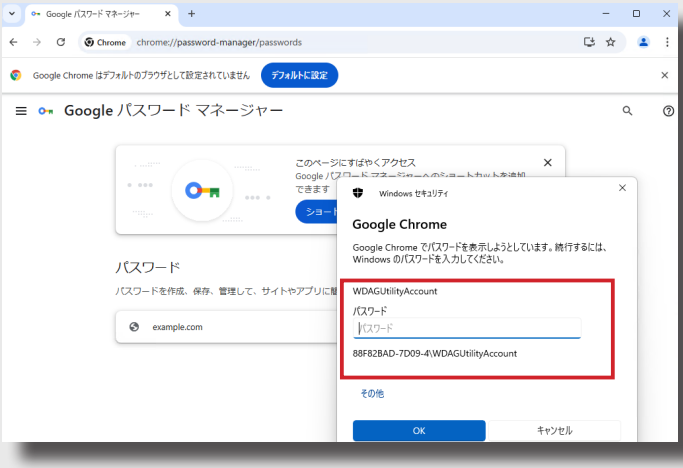
新しいパスワードを追加ダイアログが表示されますので、図の例を参考に入力し、「保存」ボタンを押下します。



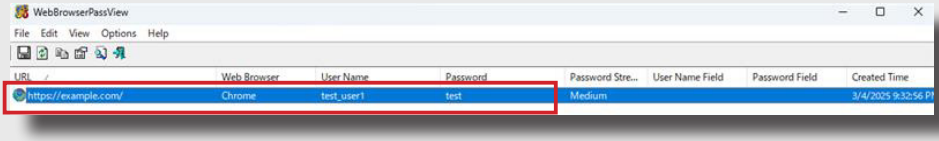
Google パスワードマネージャーに認証情報が追加されたことを確認します。



このとき、パスワード情報を閲覧しようとすると、ログイン中の Windows ユーザーの認証が求められるため、一見するとセキュアに保存されているように思われます。

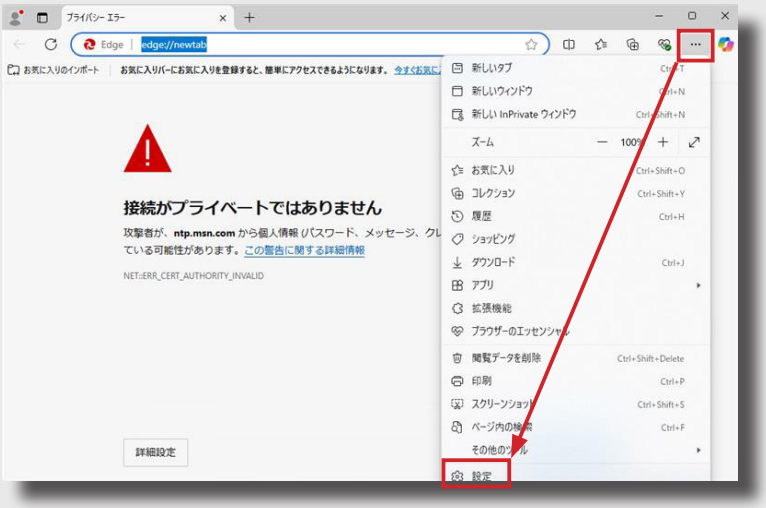


ここで、「WebBrowserPassView」を更新します。Google パスワードマネージャーでセキュアに保存されていると思われていた認証情報が、暗号化されていない状態で表示されることを確認できました。

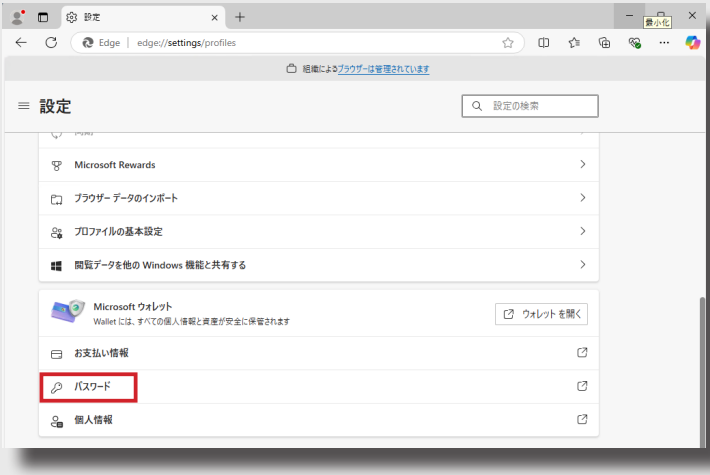


5.5 Edge の認証情報確認

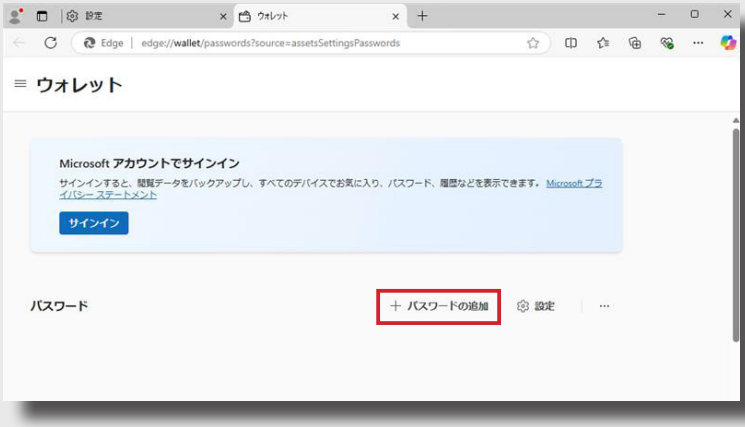
Edge を起動し、右上の設定項目より、「設定」を選択します。



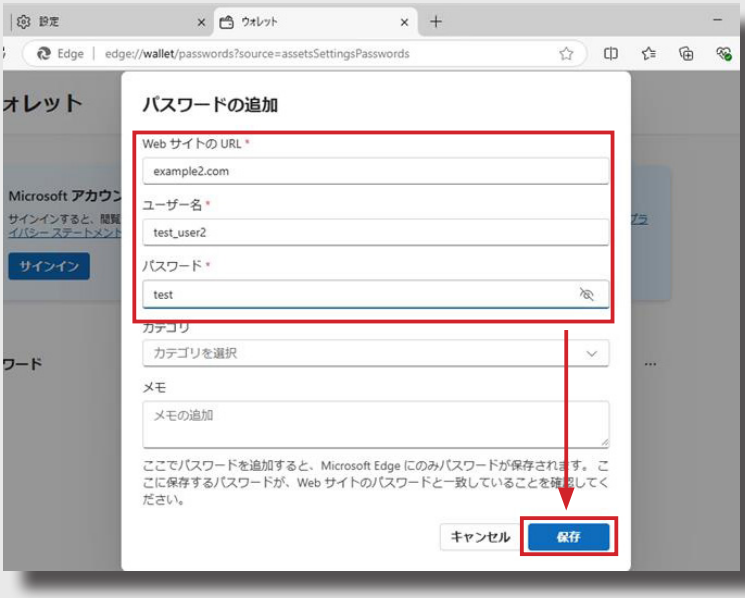
設定画面より、パスワードを選択します。



「ウォレット」タブが開きますので、「パスワードの追加」を押下します。

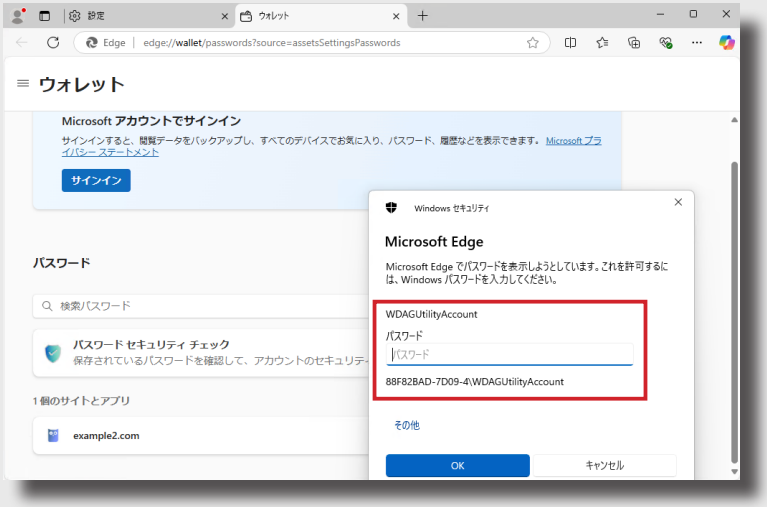


パスワードの追加ダイアログが表示されますので、図の例を参考に入力し、「保存」ボタンを押下します。

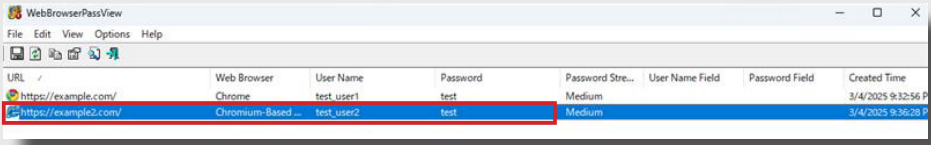


パスワードに認証情報が追加されていることを確認します。

このとき、パスワード情報を閲覧しようとすると、ログイン中の Windows ユーザーの認証が求められるため、一見するとセキュアに保存されているように思われます。



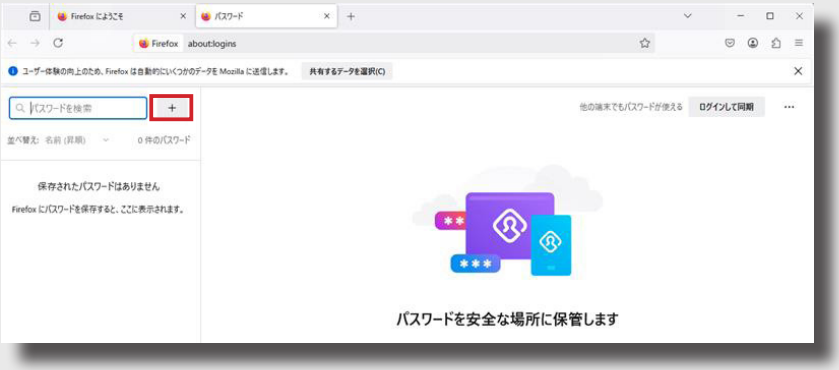
次に、「WebBrowserPassView」を更新します。セキュアに保存されていると思われていた認証情報が、暗号化されていない状態で表示されることを確認できました。



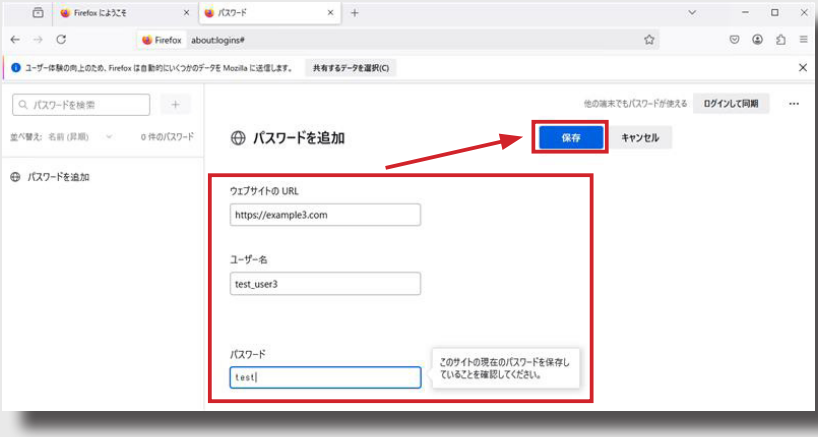
5.6 Firefox の認証情報確認

Firefox を起動し、右上の設定項目より、「パスワード」を選択します。

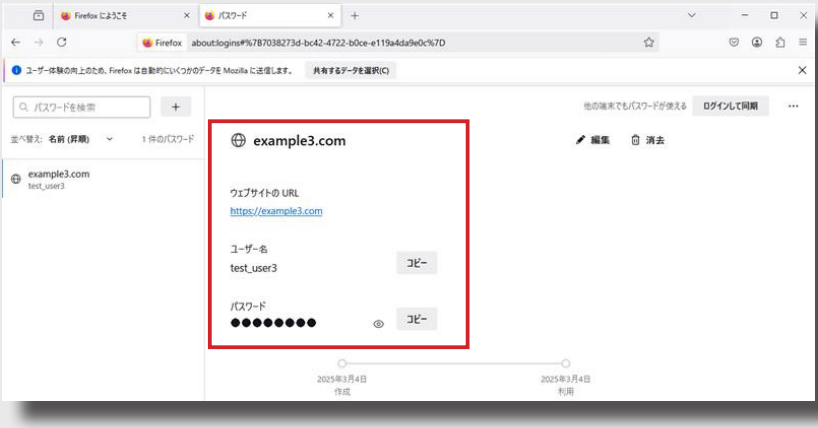
選択後、パスワードタブが起動しますので「＋（追加）」を押下します。



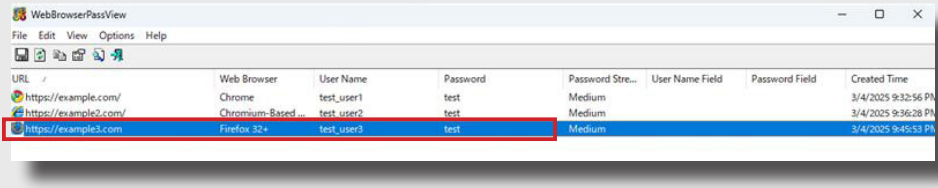
パスワードを追加ダイアログが表示されますので、図の例を参考に入力し、「保存」ボタンを押下します。



Firefox に認証情報が追加されたことを確認します。



ここで、「WebBrowserPassView」を更新します。認証情報が、暗号化されていない状態で表示されることを確認できました。



なお、Firefox で認証情報を閲覧する場合には、Google Chrome や Edge と比較して容易に閲覧可能です。

6. おわりに

今回はここまでとなります。

今回は、「4. 追加情報編 2」として、NirSoft が提供する「Browser Tools」を利用して、Web ブラウザーを利用した検索履歴を確認しました。また、「Password Tools」を用いて Web ブラウザーに保存された認証情報を確認しました。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、マルウェアの感染拡大経路を確認する際などに活用可能です。

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.69

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