HITACHI
Inspire the Next

Hitachi Systems Security Journal

VOL.66

株式会社 日立システムズ

Human * IT

Hitachi Systems Security Journal VOL.66

TABLE OF CONTENTS

※ 文書中の「中国」という表現は、中華人民共和国を意味する言葉として記載しています。

●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

中国の情報戦を長年監視してきた台湾セキュリティ企業が分析する2024年台湾総統選への影響力工作

リアン・ホアン+チーユン・ホアン インタビュー

CODE BLUE 2024 において TeamT5 の脅威アナリストであるリアン・ホアン氏とチーユン・ホアン氏による講演「進化する中国の戦術：ハック・アンド・リークと影響力工作との組み合わせ」が行われた。TeamT5 は、台湾を拠点とするサイバーセキュリティ企業であり、特にサイバー脅威インテリジェンス・マルウェア解析・標的型攻撃研究において高い専門性を有している。長年にわたり中国によるサイバー脅威の監視・分析を続けており、その成果は CODE BLUE をはじめとする国際カンファレンスで発表されてきた。今回は、2024 年の台湾総統選を題材に、中国による影響力工作の最新事例が紹介された。不正アクセスで入手したデータを漏えいさせる「ハック・アンド・リーク」と呼ばれる手法や、生成 AI を活用して多様な偽コンテンツを流布する手法などが取り上げられた。なお、記事中の中国への見解は TeamT5 のものであり、当社の見解を示すものではないことを、あらかじめご了承いただきたい。

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

自国のサイバーセキュリティ企業を攻撃に利用する中国

吉澤（以下 Y ）：TeamT5 は設立当初から中国、あるいは台湾に影響を与える可能性のあるアクターや国の情報を収集していたのでしょうか。

チーユン・ホアン（以下 C ）：私たちは中国語に対応できるため、言語の面で他の調査機関よりも優位性があります。その強みを生かし、中国や北朝鮮の APT※1 の脅威アクターを中心に調査を行っています。もちろん、それ以外の国家についても調査していますが、TeamT5 は特に APT の研究に強みを持っています。

Y 中国には以前から有名な諜報機関が存在していましたが、現在でもそうした組織がサイバー技術を駆使して影響力を強めているのでしょうか。

リアン・ホアン（以下 L ）：確たる証拠はないものの、私たちの研究過程で、中国の諜報機関内にサイバー部門が設立されていることが見えてきました。さらに、中国国家は自国のサイバーセキュリティ企業を利用してサイバー攻撃を行なっている可能性も示唆されています。

Y それはどのようにして明らかになったのでしょうか。

L それが判明したのは、米国政府が中国のサイバーセキュリティ企業や攻撃グループを起訴したことがきっかけです。起訴文書には、中国政府の依頼を受けて APT 攻撃を展開していることが明示されています。昨年の私たちの発表でも、912 プロジェクト※2 などがボットネットを活用し、情報戦を展開している証拠をいくつか取り上げました。

Y お二方がセキュリティ、特にインテリジェンスに興味を持ったきっかけについて教えてください。

C 私は TeamT5 に入る前、米国と台湾の関係改善を目的とする NGO で活動していました。その活

リアン・ホアン（Li-an Huang）
TeamT5 の脅威インテリジェンス・アナリスト。研究分野は、情報操作、持続的標的型攻撃（APT）、国際関係などで、台湾の Threat Analyst Summit でも発表を行なっている。TeamT5 に加わる前は、台湾の国会で立法補佐官を務めていた。

チーユン・ホアン（Chih-yun Huang）
TeamT5 の脅威インテリジェンス・アナリスト。TeamT5 に加わる前は、ワシントン D.C. に拠点を置く NGO で米台関係のプロモーション活動に従事していた。また、2016 年の台湾大統領選挙では選挙キャンペーンスタッフとして参加。研究分野は、影響力工作、国際関係、中国研究など。

※ 1 **APT（Advanced Persistent Threat）**：特定の標的に対して高度な技術で長期間攻撃を続けるサイバー攻撃のこと。

※ 2 **912 プロジェクト**：中国公安部が主導する越境的弾圧活動。偽の SNS アカウントを利用し、国外の批判者を攻撃するとともに、中国共産党に有利な情報を拡散した。2023 年 4 月に米国司法省が公開した訴状には、反体制派の監視や情報操作の詳細が記されている。https://www.justice.gov/usao-edny/pr/34-officers-peoples-republic-china-national-police-charged-perpetrating-transnational

動を通じて、中国からの圧力が日々高まっていることを実感しました。そこで、NGO の枠を超えて台湾政府にも理解を深めてもらう手助けがしたいと考え、TeamT5 に参加しました。

L 私はもともと台湾の下院議員の秘書官をしていました。選挙活動を支援する中で、中国による影響力工作に直接触れる機会があり、その際に脅威アクターが使用する TTPs（戦術・技術・手順）やコンテンツなどの手法に興味を持ちました。これをきっかけに、セキュリティ業界へ進むことを決意しました。

中国の影響力工作は福島での処理水放出でも確認

Y 今回の講演も非常に興味深い内容でした。今年の台湾の選挙におけるインテリジェンス調査には、どのくらいの期間をかけて実施されたのでしょうか？

L 今回の発表内容については、2023 年 11 月頃から調査を始めたものです。実際の選挙は今年 1 月に行われたため、調査期間はおよそ 2 カ月間でした。

C とはいえ、その前からある程度の準備は進めていました。2023 年 9 月頃にはすでに怪しい動きが見え隠れしており、それが急速に明確になり始めたのが 11 月頃でした。

Y 講演では今回の選挙に関連するトピックをご紹介いただきましたが、選挙以外にも追跡している情報はあるのでしょうか？

L 特に日々の生活に影響を与える社会的なイベントがあると、中国からの、影響力工作や情報戦が見受けられるので、それらを含めて多くの調査を継続しています。例えば、日本が関係するところで福島の処理水放出が決まった時には中国からの情報作戦の実行が確認されています。

Y ニュースがフェイクか否か見分けるにはどうすればよいでしょう。差し支えない範囲でご説明いただけますか。

L 残念ながら、フェイクニュースのファクトチェック（真偽の判断）は容易ではありません。だからこそ、私たちのように分析を行う人間の重要性が高まっていると考えています。真偽を判断

「偽情報はなくならないので、個々が判断できるお手伝いをしたい」と語るチーユン・ホアン氏

するには経験が不可欠であり、その裏付けとなるのは、内容の精査や IP アドレス、戦術、手法の分析です。これらを通じて、ファクトチェックを可能にしています。

C 台湾にはファクトチェックを行う NGO がいくつか存在しており、ユーザーは例えば話題になったニュースをそれら NGO のプラットフォームに投稿して報告することができます。NGO はその情報を分析し、研究者とも共有しながら真偽を判断していきます。さらに、政府に確認を取る方法もあります。

Y それは良い仕組みですね。

C 影響力工作では、明らかな偽ニュースは使用されません。アクターは真実の伝え方を変えることで（ナラティブ操作）、政治的な意図を反映させようとします。講演では、副総統の蕭美琴氏が台湾に酒を密輸したとするキャンペーンを紹介しました。実際に酒を持ち込んだことは事実ですが、個人使用目的で定められた量であれば合法です。それにもかかわらず、あたかも違法行為であるかのように伝えられていたのです。

Y 今回の講演で、繁体字と簡体字といった文字の違いから偽情報を見抜くというお話がありましたが、その違いは台湾の人なら誰でも気づけるものなのでしょうか。

C 2 つのパターンがあります。1 つは用語で、台湾の人しか使わない、あるいは台湾の人は使わな

「地理的にも文化的にも中国に近いことが台湾の強みです」と語るリアン・ホアン氏

い用語が含まれているパターン。もう 1 つは文字で、台湾では一般的ではない文字が使われているケースですね。ただ、しっかりと見ないとわかりにくいものもあります。

Y この点をお聞きしたのは、講演で生成 AI について触れられていたからです。生成 AI は日本語の文章を非常に自然に作成でき、注意深く読んでも不自然さがほとんどありません。もしかすると、台湾の言葉も独自の言い回しで生成できるのではないかと思ったのです。

L 台湾でも同様のケースが確認されています。最近では、生成 AI を使って画像を作成し、ヘッドラインだけは実際の記事から引用したフェイクニュースがありました。生成 AI は、今後ますます大きな脅威になり得ると感じています。

台湾は中国の「サイバー攻撃実験場」!?

Y TeamT5 のサービスは 2017 年から日本でも展開され、2022 年には日本法人も設立されています。すでに多くの日本企業がユーザーとなっているかと思いますが、TeamT5 のサービスにはどのような特徴がありますか。

C TeamT5 は台湾に拠点を置く組織であり、中国語や中国の文化を深く理解していることが、圧倒的な強みです。さらに、中国政府がサイバー空間におけるポリシーを決定した際には、その動向について見解を提供できる点も大きな特徴です。

L 台湾は、以前からサイバー分野における中国の「実験場」として使われてきました。中国の新しいマルウェアや攻撃手法が、まず台湾で試されることが多いのです。そうした新たな攻撃を早期に検知し、対応することで、その知見を日本を含むお客さまに提供できる点も大きな特徴だといえるでしょう。

Y 講演では、官民の連携が重要という話をされていましたが、日本の場合、この『民』は企業を指すのでしょうか。

L いくつかのレイヤーで構成されることになると思います。まず政府は、事実の確認や政府としての見解を明示する役割を担います。その下に、例えばファクトチェックを行う NGO のような第三者機関があり、そこに企業が情報を報告する形です。影響力工作や情報戦に対抗するためには、すべてのパートナーが連携して動くことが不可欠です。

Y 情報を共有して連携するということですね。

L 例えば、特定の企業が情報戦の標的になった場合、その企業が「この書き込みは私たちのものではありません」と明示することが重要です。さらに、セキュリティベンダーも分析結果を公表すべきでしょう。TeamT5 も今回の台湾の選挙後、選挙期間中に確認した情報戦の戦術などをホワイトペーパーにまとめて開示しました。これは、脅威アクターを明らかにすることが、民間にとって重要だと考えたためです。

Y 選挙期間中は複数の対象を監視されていたと思いますが、選挙終了後も監視は続けているのでしょうか。また、攻撃者が別のキャンペーンへ移行するケースもあるかと思いますが、そのつながりについても追跡しているのでしょうか。

L 選挙の場合、投票日という明確な締め切りがあります。それ以降、ほとんどのアカウントは活動を停止していました。現在も週に一度は確認していますが、やはり活動は見られないようです。一方で、1 つのキャンペーンを追跡する過程でスクリーンショットなどさまざまな情報を収集します。これらの情報は、新しいキャンペーンが確認された際に比較し、関連性を検証するために活用しています。

今回お話を伺ったお二方はいずれもホアン（黄）さんという同じ姓だが、台湾では非常に一般的な姓であり、血縁や婚姻関係があるわけではないそうだ

偽情報が一切ない ユートピアのような世界は異常

Y それぞれの個人としてでも、TeamT5 としてでも構いませんが、将来の目標についてお聞かせください。例えば、偽情報を見破り、誰もが正しい情報にアクセスできるようにする、といったことでも構いません。思想的なビジョンでも結構です。

C 偽情報が一切存在しないユートピアのような世界は、おそらく逆に異常な世界だと思います。そういった世界では、政治的な意図が強く反映される可能性があり、むしろ危険だと感じます。やはり、多様なコンテンツに触れた人々が、自ら真偽を判断し、自分たちの意思で決定を行える社会こそが理想的だと思います。

Y 偽情報を真実であると捉えてしまう人々が日本には一定数いる印象ですが、台湾でも同じような状況なのでしょうか。

L 台湾も同様です。特に 2018 年頃は、あらゆるニュースを真実だと受け止める人が非常に多かったように思います。しかし、現在は大きく変化しています。今年の選選挙に関連しては、ニュースに対して懐疑的な意見や「他のニュースも確認して判断しよう」といった書き込みが多く見られるようになっています。

Y 最後に、今回の CODE BLUE の印象について教えてください。

L 今回が初めての CODE BLUE 参加でした。会場も広く、スタッフの皆さんが非常にプロフェッショナルに対応してくださり、とても素晴らしい経験となりました。

C 私にとっては 2 度目の CODE BLUE 参加でしたが、非常にユニークだと感じた点は、ハック・アンド・リークや影響力工作といったトピックにも多くの方が興味を持って熱心に聞いてくださることです。しかも、技術的な話にとどまらず、その背景や文脈まで理解しようとする姿勢が感じられました。私たちの取り組みを広く知っていただける、大変貴重な機会だと思いました。

Y 日本の印象はいかがですか。

C 前回の講演から 1 年しか経っていませんが、情報戦に関する興味が高まっている印象があります。

L 日本はサイバーセキュリティへの関心が非常に高いと感じています。今年 2 月に中国のセキュリティ企業である i-SOON 社の情報漏えいが発生した際には、日本のメディアから私たちにアプローチがあり、ドキュメンタリー番組が制作されました。綿密な分析が行われた、とても興味深いストーリーに仕上がっており、これは日本の関心の高さを示していると思います。

Y わかりました。本日はお忙しい中を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 2024.12

文＝日立システムズ

“私はロボットではありません”に仕掛けられた罠

【概要】：CAPTCHA は Web サイトへのログイン時に人間か確認する仕組みだが、これを悪用しユーザーに不正操作をさせる手口が確認された。対策として、自組織のサービスが間接的に攻撃に加担しないよう技術選定で攻撃への加担を防ぎ、新たな攻撃事例の共有や意識向上を通じて、日常の行動改善を継続的に行うことが重要である。

【内容】：CAPTCHA はアクセス元が人間であることを確認する仕組みだが、2024 年 8 月頃からこれを装った悪質な攻撃が確認されている。攻撃者のサイトには「私はロボットではありません」と書かれたボタンが設置され、クリックすると偽の確認手順が表示される。同時にクリップボードに悪意のあるコマンドがコピーされ、ユーザーが指示どおりキー操作を行うとそのコマンドが実行される仕組みだ（図 1）。結果、情報窃取型マルウェアがダウンロードされ、実行される被害が発生している（図 2）。

CAPTCHA はボット対策として導入されているが、AI の進歩で突破されやすくなり、確認方法が複雑化している。この戦術はこの背景を悪用し、複雑な確認手順の 1 つと誤認させてユーザーの判断を鈍らせる。さらに、要求される操作がキーを数回押すだけという単純さから、不自然さに気付きにくいよう工夫されている点も特徴である。

本事例は情報窃取だけでなく、攻撃手法を変えさまざまな攻撃の起点となる可能性があり、国内外で増加しているため継続的な注意が必要である。

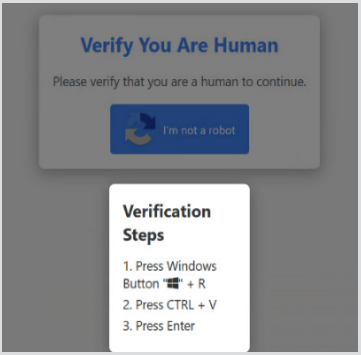


図 1 偽の CAPTCHA 画面

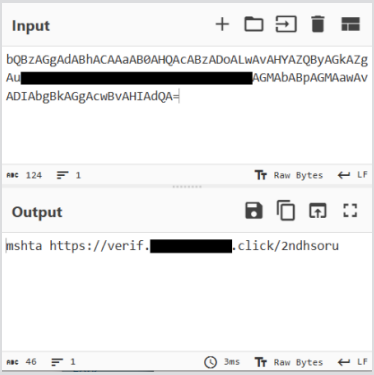


図 2 コピーされた悪意あるコマンド

この戦術への対策は、サービス提供者と利用者の両面から考える必要がある。提供者側は技術選定を慎重に行い、デバイス情報や行動パターンを活用した確認システムや多要素認証の導入を検討すべきだろう。一方、利用者側は新たな攻撃事例を共有し意識を高め、違和感にすぐ相談できる窓口や AI チャットボットなど報告しやすい環境の整備が重要である。

［情報源］

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/behind-the-captcha-a-clever-gateway-of-malware/
https://securelist.com/fake-captcha-delivers-lumma-amadey/114312/

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

1. Edge / Chrome 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。今回より「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。

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、「1. Edge / Chrome 編」として、NirSoft が提供する「Browser Tools」を利用して、Edge や Chrome の閲覧履歴を確認します。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。また、本稿は、実際のサイバー攻撃事例に基づいてシナリオを作成しています。そのため、本稿には攻撃者が使用した攻撃手法やツール名などの情報が記載されていますので、不正に使用しないようお願いします（本稿で紹介する IP アドレスや URL の一部は文字列を置換したり記号をカッコでくくるなどの加工を施しています）。

なお、本稿の内容を不正に使用すると「不正アクセス行為の禁止等に関する法律」(不正アクセ ス禁止法）などに抵触することがありますので、十分にご注意下さい。

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。

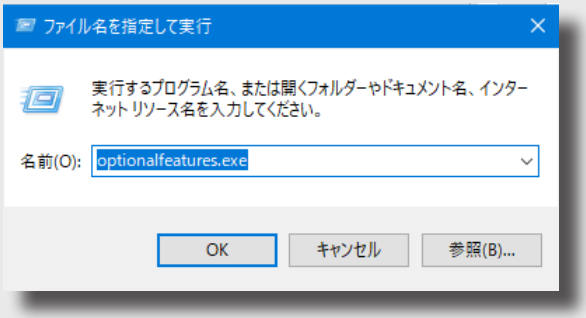
「Windows サンドボックス」の前提条件は下記の通りです※1。

- Windows 10 Pro または Enterprise ビルド バージョン 18305 または Windows 11 を使用していること（Home エディションはサポート対象外）
- ARM64（Windows 11 バージョン 22H2 以降）または AMD64 アーキテクチャ
- BIOS で有効化された仮想化機能
- 少なくとも 4 GB の RAM（8 GB 推奨）
- 空きディスク領域 1 GB 以上（SSD を推奨）
- 少なくとも 2 つの CPU コア（ハイパースレッディングを使用した 4 コアを推奨）

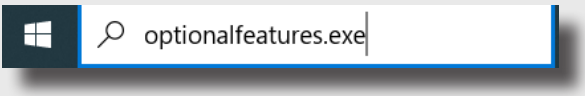
「Windows サンドボックス」は以降の手順で利用可能となります。すでに設定している方は不要です。なお、前提条件を満たしていない方は、「Windows サンドボックス」は利用できませんので、通常の Windows 上で実施してください。

2.1 Windows サンドボックスの導入

Windows キー＋R キーで「ファイル名を指定して実行」ダイアログボックスを起動し、「optionalfeatures.exe」を入力します。

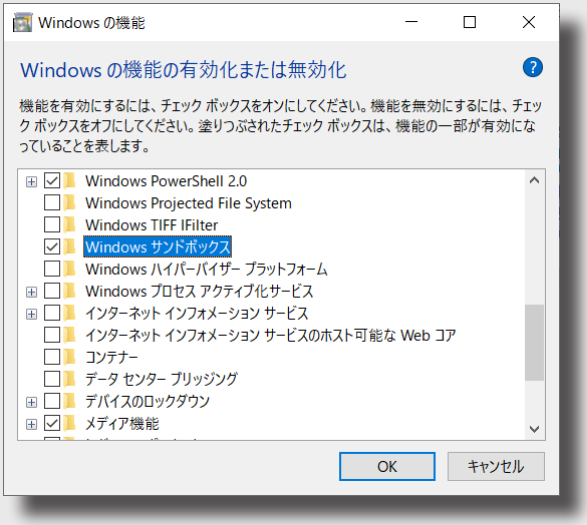


または、Windows 左下の Cortana（コルタナ）に「optionalfeatures.exe」と入力しても起動できます。



※ 1 https://learn.microsoft.com/ja-jp/windows/security/application-security/application-isolation/windows-sandbox/windows-sandbox-overview

Windows の機能ダイアログボックスが立ち上がるので、「Windows サンドボックス」にチェックを入れ、「OK」を押下します。



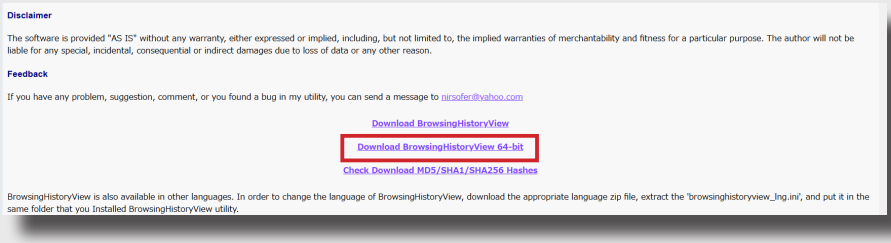
「Windows サンドボックス」のインストールが始まりますので、インストールが完了しましたら再起動します。

これで「Windows サンドボックス」のインストールが完了しましたので、スタートプログラムから「Windows サンドボックス」を起動します。

3. BrowsingHistoryView

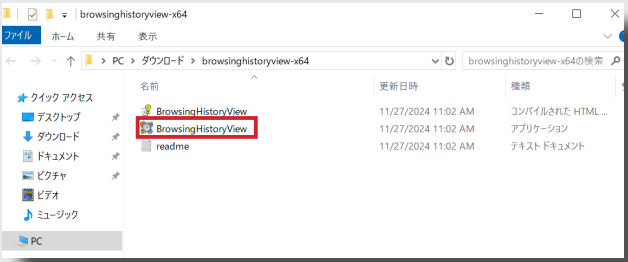
3.1 BrowsingHistoryView のダウンロードと起動

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。

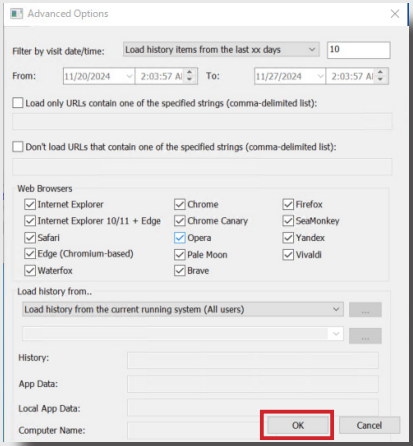


https://www.NirSoft.net/utils/browsing_history_view.html

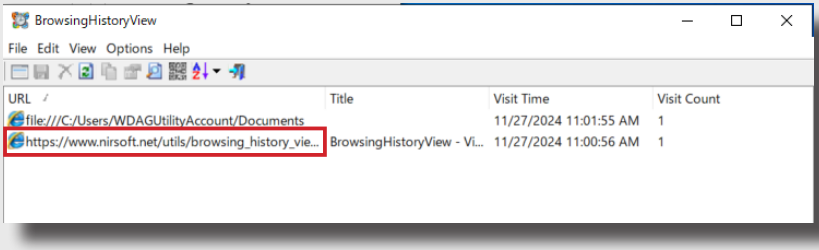
ダウンロードが完了しましたら、Zip ファイルを解凍、展開します。



展開が終わりました、「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。



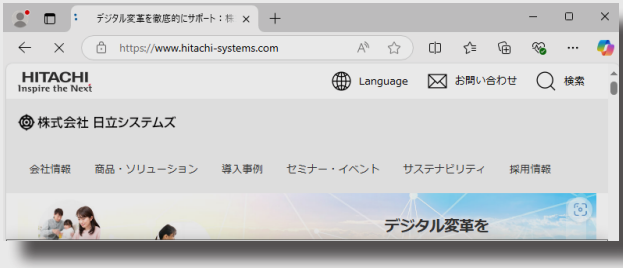
起動すると、「BrowsingHistoryView」をダウンロードする際に、NirSoft にアクセスした履歴が確認できます。



4. Edge の履歴確認

4.1 Web ブラウザーでの閲覧

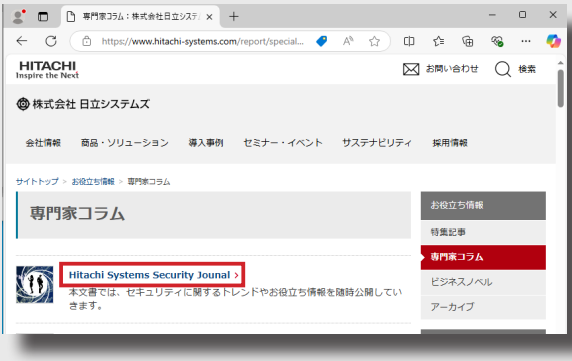
Edge を起動し、Web サイトを閲覧します。今回は例として当社の Web サイトにアクセスしてみます。



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

Web ページの画面をスクロールして「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。

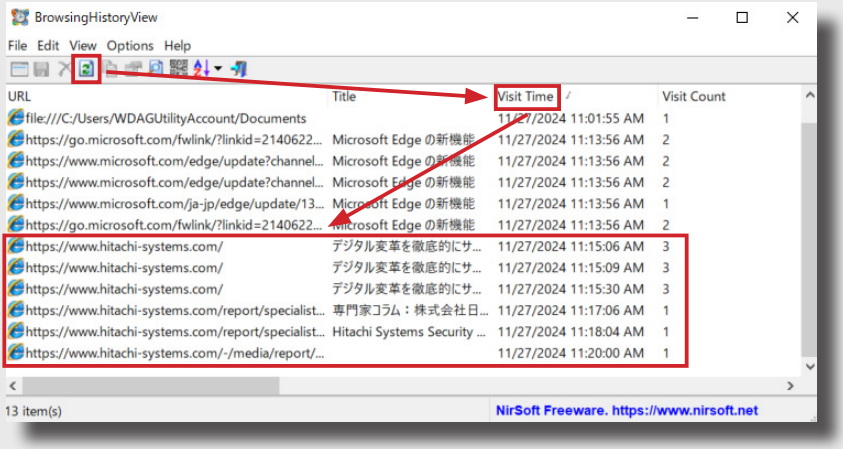


「Hitachi Systems Security Journal」のいずれか（今回は Vol.64）を**左クリック**して開きます。

Web ブラウザー上で PDF ファイルが開きます。

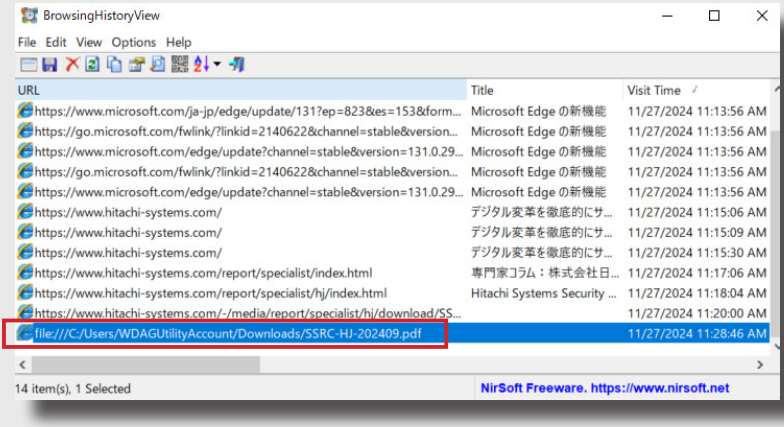
4.2「BrowsingHistoryView」による履歴の閲覧

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。加えて、「Visit Time」をクリックして、履歴を昇順に並び替えます。



Edge 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。

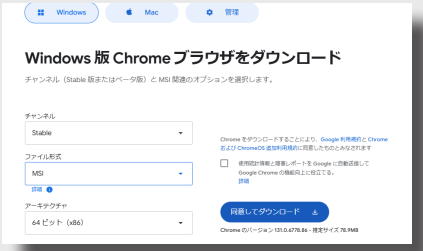
ダウンロードしましたら、「BrowsingHistoryView」を更新してください。今度は、「Hitachi Systems Security Journal」の PDF ファイルに file: スキームでアクセスしていることが確認できました。なお、アクセスの経路により見え方が異なるので、注意が必要です。



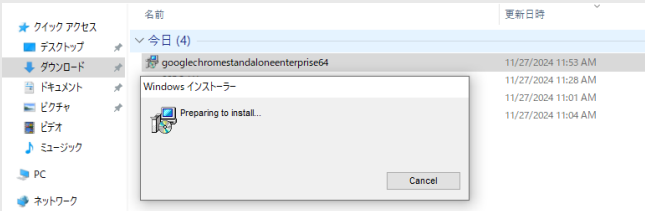
5. Chrome の履歴確認

5.1 Chrome のインストール

Google にアクセスして Chrome をインストールします。どのバージョンをインストールするかは、お使いの環境にあわせて選択してください。筆者は以下の設定でダウンロードしました。



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。なお、ゲスト OS 側から Chrome をダウンロードできない場合は、Sandbox を起動している側の OS（ホスト OS）側で、Chrome ダウンロード後、Sandbox 内にコピーしてください。



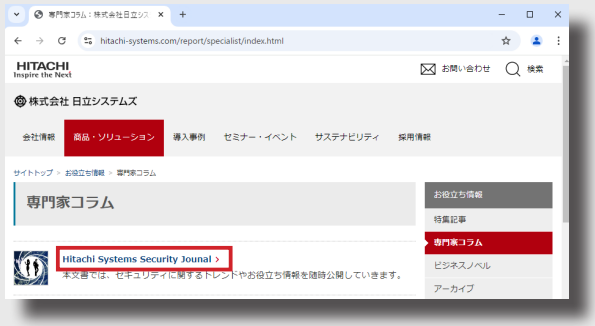
5.2 Web ブラウザーでの閲覧

Chrome を起動し、Web サイトを閲覧します。今回は例として当社の Web サイトにアクセスしてみます。

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

Web ページの画面をスクロールして「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。

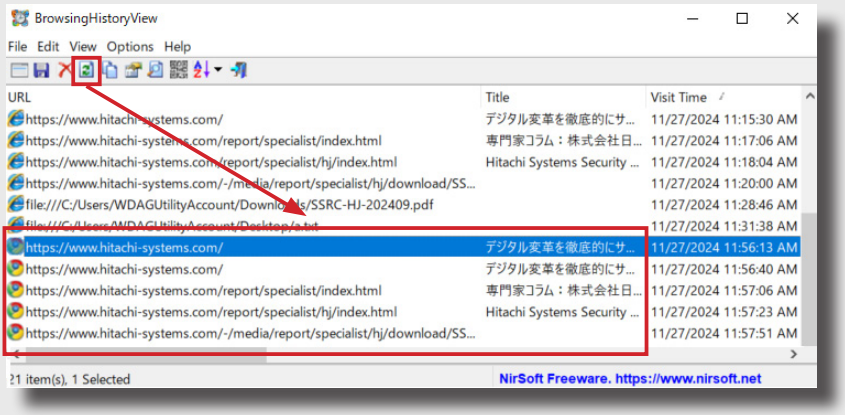


「Hitachi Systems Security Journal」のいずれか（今回は Vol.64）を左クリックして開きます。

Web ブラウザー上で PDF ファイルが開きます。

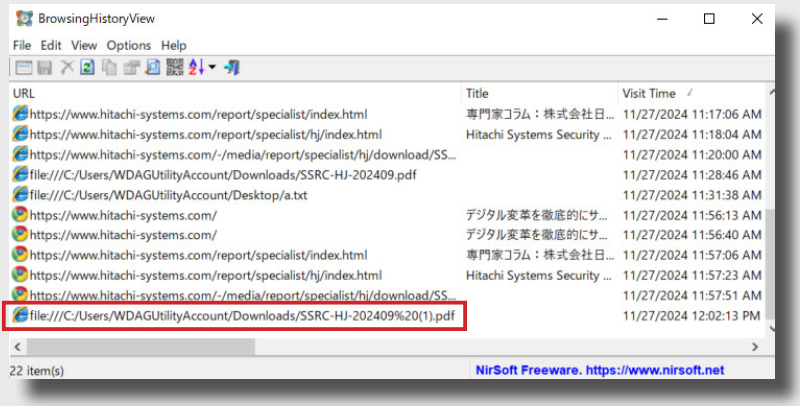
5.3「BrowsingHistoryView」による履歴の閲覧

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。



Chrome 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。Edge と同様、「Hitachi Systems Security Journal」の PDF ファイルに file: スキームで保存されていることが確認できます。なお、アクセスの経路により、見え方が異なる点に注意が必要です。



6. Edge と Chrome の履歴ファイル格納場所

Edge の閲覧履歴は、以下に保存されています。

C:¥Users¥[ユーザー名]¥AppData¥Local¥Microsoft¥Edge¥User Data¥Default¥History

Chrome の閲覧履歴は、以下に保存されています。

C:¥Users¥[ユーザー名]¥AppData¥Local¥Google¥Chrome¥User Data¥Default¥History

現行の Edge は、Chrome がベースとなっていることから、どちらも同様の保存場所にあり、同じ SQLite と呼ばれる軽量な関係データベース管理システム（RDBMS）で管理されています。この閲覧履歴ファイルを SQLite から直接閲覧する方法については、次回以降に確認します。

インシデント発生時などには、Windows アーティファクト（システムに残された痕跡や証拠）として当該履歴ファイルを保全し、不審なサイトへの接続状況などを確認します。

なお、古いバージョン（バージョン 79 より前）の Edge や Internet Explore10、11 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¥[ユーザ名]¥AppData¥Local¥Microsoft¥Windows¥WebCache¥WebCacheV*.dat

また、古い Internet Explore の場合、以下などに保存されている可能性があります。

C:¥Users¥[ユーザー名]¥AppData¥Local Setting¥History¥History.IE5

C:¥Users¥[ユーザー名]¥AppData¥Local¥Microsoft¥Windows¥History¥History.IE5

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

7. おわりに

今回は、「1.Edge / Chrome 編」として、NirSoft が提供する「BrowsingHistoryView」を使用した Edge や Chrome での閲覧履歴の確認方法を介しました。閲覧履歴を調査することで、管理する PC がマルウェアに感染した際の感染経路や不審な Web サイトへの接続状況などが判明することがあります。

次回は、同じく、NirSoft が提供する「BrowsingHistoryView」を用いて、Firefox の閲覧履歴などを確認します。

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.66

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