HITACHI
Inspire the Next

Hitachi Systems Security Journal

VOL.70

株式会社 日立システムズ

Human * IT

Hitachi Systems Security Journal VOL.10

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

「より健やかな人々に、より健全なテクノロジーを」
ヘルスケアとセキュリティをつなぐ架け橋
Biohacking Village

ニーナ・アリ＋ホルヘ・アセベド・カナバル インタビュー

Biohacking Village（バイオハッキング・ヴィレッジ）は、バイオメディカル技術とサイバーセキュリティの分野における安全性向上を目的とした団体だ。多様なバックグラウンドを持つメンバーで構成され、「より健やかな人々に、より健全なテクノロジーを（Healthier Technology for Healthier People）」をスローガンに掲げている。医療機器に潜む潜在的な課題を明らかにするべく、セキュリティ研究者や医療機器メーカーと連携し、同名のイベントを主催してきた。
このイベントは、2014 年に DEF CON で初めて単独開催されて以来、年々規模を拡大し、いまでは DEF CON 最大級のヴィレッジの 1 つに数えられる。これまで世界各国で展開されてきたが、 2024 年には CODE BLUE を通じて日本初上陸を果たした。今回、CODE BLUE 2024 開催に先立ち、エグゼクティブディレクターであるニーナ・アリ（Nina Alli）氏と、メディカルアドバイザーのホルヘ・アセベド・カナバル（Jorge Acevedo Canabal）氏にインタビューを実施。医療機器セキュリティの歴史からイベント運営まで、幅広い話題を伺った。インタビューはオンラインで行い、開催期間中に会場で写真撮影を行なった。

取材・文 = 斉藤 健一／通訳 = エル・ケンタロウ／撮影 = 卯月 梨沙

Biohacking Village 誕生と医療機器セキュリティ研究の黎明期

斉藤（以下 S ）：Biohacking Village に携わるようになった経緯について教えてください。

ニーナ・アリ（以下 N ）：Biohacking Village は 2013 年の DEF CON で始まりました。当時は他のビレッジとスペースを共有しており、私は参加者として訪れていました。ただ、電子医療記録や医療機器に関わる経歴があったため、この分野に自然と惹かれ、徐々に関わるようになりました。その後、6 カ月ほどで組織に変化があり、プロジェクトマネージャーが必要になった際に志願しました。これをきっかけに運営に関わるようになり、以来 10 年以上、活動を続けています。

S バックグラウンドについて、もう少し詳しく教えていただけますか。

N 当時、私は病院のシステム管理者として勤務し、電子医療記録（EMR）のシステムアナリストやテクニカルスペシャリストとしても活動していました。2010 年代初頭には、医療機器におけるサイバーセキュリティのリスクを指摘する研究発表がいくつか登場しました。例えば 2011 年には、ジェイ・ラドクリフ氏がインスリンポンプを遠隔操作できることを実演しています※ 1。さらに、2014 年に SANS Institute が発表した報告書では、医療機関の 94%がサイバー攻撃を受け、その中には医療機器を標的とした例も含まれていたとされています※ 2。

S ジェイ・ラドクリフ氏の発表は、当時大きな話題となりました。

N 当時、私は生物医学情報学（Biomedical Informatics）の修士課程に在籍しており、病院で起こる問題を観察し、状況を理解しながら、働く

●ニーナ・アリ（Nina Alli）

ニーナ・アリは、医療技術、公共政策、そして草の根のセキュリティ研究を架橋するサイバーセキュリティおよび規制戦略の専門家である。過去 10 年間にわたり、医療とサイバーセキュリティの交差点を実践的な取り組みとオープンな協働、そして公益の視点から探求する先駆的コミュニティ「Biohacking Village」のエグゼクティブディレクターを務めている。バイオテクノロジー、生物医学工学、サイバーセキュリティの分野において 16 年以上の経験を有し、医療分野におけるバイオテクノロジー基盤全体の近代化、インフラの強化、そして電子医療記録（EHR）の統合改善に取り組んできた。EHR を「究極の医療機器」と位置づけ、その安全かつ効果的な活用を中心的課題としている。彼女の取り組みは、患者ケア、臨床業務、接続機器が交差する高リスク環境において、システム思考に基づく規制サイバーセキュリティのアプローチを提示するものである。また、業界横断的な協働、責任ある技術革新の推進、そして医療技術に対する公共の信頼構築を重視している。特に、接続機器のぜい弱性が人命に影響を及ぼし得る分野において、その重要性は極めて高い。DEF CON などのハッカースペースでの長年にわたる活動を通じて、医療機関とセキュリティ研究者との間にある文化的・技術的ギャップの橋渡しを行なってきた。

※ 1 **Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System**
https://media.blackhat.com/bh-us-11/Radcliffe/BH_US_11_Radcliffe_Hacking_Medical_Devices_WP.pdf

※ 2 **編注：**原稿執筆時点で SANS Institute のレポートのリンクが無効であったため、オリジナルの文書を確認することできなかった。参考として SANS Institute のレポートを引用した論文の URL を掲載する。
Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem
https://pmc.ncbi.nlm.nih.gov/articles/PMC4516335/

人々に警鐘を鳴らす立場にありました。こうした経験を通じて、サイバーセキュリティの分野に関わるようになったのです。当時の現場は無防備で、対策も講じられていない状態でした。私たちは、システムを適切に構築し、患者データを守る必要がありました。

S 病院のシステム管理をされていたのであれば、当時注目を集めはじめた医療機器のセキュリティ研究に危機感を持たれたのも当然のことだと思います。

N 私は医療機器と電子医療記録（EMR）をつなぐインターフェイスの構築を担当し、その中でソフトウェア上の問題にいくつか気づきました。EMR の提供元に連絡し、衛生管理や安全性をどう確保するか相談することもありました。同じ時期、2014 年には米国政府が、重要インフラ全体のサイバーセキュリティ強化を目的とした指針「Cybersecurity Framework（サイバーセキュリティ・フレームワーク）」を発表しています※3。

S 一方では、民間研究者による医療機器のセキュリティ研究が進み、もう一方では、政府による重要インフラ全体のセキュリティ強化に向けた取り組みが進められていた。セキュリティへの関心が高まるには絶好のタイミングだったのですね。政府が病院のセキュリティを強化する狙いはどこにあったのでしょうか。また、この取り組みは政府主導で行なわれているのでしょうか。

ホルヘ・アセベド（以下 J）：私は Biohacking Village でボランティアのメディカル・アドバイザーを務め、医学の博士号を持っています。以前はプエルトリコの公衆衛生機関でチーフメディカルオフィサーとして、パンデミック対応や遠隔医療の推進に携わっていました。こうした立場から見て、政府の取り組みは「公共の安全を守るのは政府の根本的責務である」という公衆衛生の基本理念に基づいています。医療へのアクセス、健康情報の自己管理、公平な医療の提供は、人間の基本的権利として守られるべき公共福祉の柱です。

N「政府主導の取り組みなのか？」という問いには、「はい」とも「いいえ」とも言えます。病院は重要インフラの 1 つなので、政府主導といえるでしょう。ただ特筆すべきは、病院がすべての重要インフラが交差する場（interdisciplinary landing zones）である点です。電力・通信・医療・人的ネットワークなどが同時に稼働し、すべてを一カ所で保護する必要があります。こうした環境では、保護の考え方そのものが従来とは異なるパラダイムになるのです。

S 病院がさまざまなインフラが交差する特別な場所だという説明には改めて納得しました。また、セキュリティの考え方自体が変わるという視点にも、とても説得力がありました。

N 病院のセキュリティが不十分な場合、それ自体が非対称戦（asymmetric warfare）の一形態とな

●ホルヘ・アセベド・カナバル（Jorge Acevedo Canabal）

Biohacking Village のメディカル・アドバイザーを務める医学博士。現在はプエルトリコ大学医学部の客員教授として活躍。プエルトリコの公衆衛生機関のチーフ・メディカル・ディレクターとしてパンデミック対応プログラムや遠隔医療の推進を主導してきた。また、ハリケーン・マリア（2017 年 9 月にドミニカ国とプエルトリコを襲った大型ハリケーン）発生の際、死者数が大きく増加したことから、災害時の死亡認定に関する医師向け研修プログラム策定の主要メンバーとして参加。危機下における制度的な不備が記録に残らないまま見過ごされているという課題に取り組む。

※ 3 **Cybersecurity Framework** https://www.nist.gov/cyberframework

り得ます。ぜい弱な病院は攻撃の標的となり、被害が出れば経済にも悪影響を及ぼし、広範囲に深刻なダメージをもたらすリスクを抱えています。

S なるほど。

N また、米国では、チェイニー元副大統領が心臓のペースメーカーを装着していたことが、医療機器のセキュリティ強化のきっかけの 1 つになったと言われています。機器同士が通信し、データを送受信するようになったためです。

医療機器のセキュリティにおける情報開示のあり方

S 次に、個人の視点から見た医療機器セキュリティへの関心の高まりについて伺いたいと思います。前述の個人研究者による発表の背景には、eBay などで中古の医療機器が入手しやすくなったことがあると思うのですが、いかがでしょうか。

N 医療機器を入手しやすくなったことも要因の 1 つだと思います。血糖値モニターや心臓のペースメーカーなどは、入れ替え頻度が高く、中古市場に多く出回り、比較的簡単に入手できました。また、医療機器がどのように動いているのかを知りたいというハッカーの純粋な好奇心も背景にあると思います。

S そのような個人の研究活動に対して医療機器メーカーはどのような反応を示していたのでしょうか。

N 当時の医療機器メーカーには、自社のテクノロジーを隠そうとする傾向がありました。また、医療機器には最新のハードウェアが使われていることも多く、組み込みチップも最新のものや、他の市場では見かけないものが搭載されていました。こうした点が、ハッカーたちの興味を引く要因にもなっていたのです。

S 医療機器に最新のチップが使われているというのは初めて知りました。また、メーカーが自社のテクノロジーを隠そうとするのは、かつてのコンピューター業界でも見られたことですから、歴史は繰り返すものだという印象を持ちました。

N 今年（2024 年）の DEF CON 32 で開催された Biohacking Village では 20 台ほどの医療機器に対して 42 件の潜在的な問題が発見されました。これらの問題は、各医療機器メーカーとテストを行なった研究者との間で、「調整されたぜい弱性開示ポリシー（Coordinated Vulnerability Disclosure Policy）」に則って処理が進められます。ですが、こうした情報が公に開示されることはほとんどありません。

S 公に開示されない理由はどこにあるのでしょうか。

N 今では多くの医療機器がネットワークに接続しています。仮に、ある種の医療機器にぜい弱性が発見されたという情報が公表されたとしたら、Shodan（インターネットに接続された機器を探すための検索エンジン）を使って、その機器を探し出すことが可能となり、深刻なサイバー攻撃に発展する恐れもあるからです。

S 情報公開の必要性とセキュリティ確保のバランスという、難しいジレンマについて改めて考えさせられました。とはいえ、最も重要なのは患者の健康であり、病院に対する信頼だと思います。

医療機器のぜい弱性は人命に影響するのか

S 医療機器のぜい弱性が人命に影響する可能性について教えてください。多くの方がこの点に疑問を抱いていると思います。この非常にセンシティブな問題については、センセーショナルな扱いを避け、冷静に考察したいと考えています。

N 正直なところ、慎重に発言すべきテーマだと思います。この質問は、少し漠然としている印象を受けました。ただ、意図されているのは「重大な欠陥によって医療機器が人命に関わる事態を引き起こした事例があるか」ということですよね。その点については「はい」と答えられます。

S ありがとうございます。可能な範囲でもう少し具体的にお話いただけますか。

N 仮に「遺伝子解析装置でデータの漏えいが見つかった」としましょう。ただ、そのような装置の製造メーカーは数社しかありませんからすぐに特定されてしまいます。そのため、ここからの私の話はあくまで例えとしてお聞きください。

S 配慮いただきありがとうございます。

N 私の母は、複数の遺伝子変異を伴う希少ながんを患っており、定期的に病院で血液検査を受けています。家族は彼女の血液型を当然把握していますが、もし機械が異なる型を示したり、誤って記

録されていても、それを疑う人はいないでしょう。私たちは、人より機械を信頼するよう刷り込まれているのです。誤った血液型の輸血では、最初は体が防御反応を示し、2回目には命に関わる危険があります。それほど深刻な結果を招きかねません。

J 医療機器が直接的な死因となるケースは稀で、多くは故障が主因ではなく一因として作用します。例えばペースメーカーや透析装置が使用中に故障しても、それ単体で致命的になるというより、すでに不安定な状況への追い打ちとなります。病院のシステム停止も深刻です。電子カルテ（EHR）や輸液ポンプ、人工呼吸器などが止まれば、患者は適切なタイミングで治療を受けられず、その影響は見過ごされがちです。こうしたトラブルが、患者の状態悪化やケアの長期化、最終的には死亡につながることもあります。

S 回答を伺っていて、医療事故の中には人間側の運用である程度防げるものもあるのではないかと感じました。このような点について、ガイドラインの策定や議論が行なわれることはあるのでしょうか。

J ガイドラインは存在します。病院には「事前の備え」と「事後の対応」、2段階の計画が必要です。米国では、連邦の医療保険制度の規制下にあるすべての病院が、臨床面およびサイバーセキュリティ上の障害の両方に対応した文書化されたインシデント対応計画を持つことが義務付けられています。

S なるほど。

J 人に起因する問題が大きいというあなたの印象は正しいです。より良いツールの導入は課題の一部にすぎません。私の経験上（特にCOVID-19時）、資金で機器や技術支援、研修が提供されても、スタッフの準備不足や業務プロセスとの不整合、組織の対応力の欠如により、十分に機能しないことがあります。

S 確かに。

J 被害を本当に抑えるには、インシデント対応計画を、継続的な能力チェックや業務監査、各施設の人員体制や資源制約を踏まえた柔軟なガバナンスで支える必要があります。新たな政策や技術を義務化する前に、規制当局は導入現場の負担と吸収力を慎重に見極めるべきです。そうでなければ、善意の取り組みも命を救う対策ではなく、形式的なチェック項目として形骸化してしまいます。

N サイバーセキュリティの専門家として、医療機器が意図通り正しく動作することは極めて重要であり、個人的にも強い関心を持っています。一方で医師の本来の役割は患者の治療であり、機器の理解は必須ではありません。だからこそ、医療機器の高い信頼性が不可欠だと考えます。

S おっしゃるとおり、現場の医師に過度な負担をかけずに、機器の信頼性を担保する仕組みが必要だと感じました。

N 医療業務では、医師と患者のやり取りが定型化されたプロトコルに基づいて行なわれています。これにより統一されたデータを収集し、ヒューマンエラーを防ぎ、事故を予防しています。病院で型にはまった質問や症状の確認が行なわれるのも、こうした運用に基づくものです。

S ありがとうございます。医療機器のセキュリティについて、多面的に貴重なお話を伺うことができ、大変勉強になりました。

Biohacking Village 設立当初の課題と医療機器メーカーとの関係構築

S Biohacking Village 設立当初、医療機器メーカーなどから反発があったことが予想されますが、どのように彼らを説得し、関係を築いていったのか、その経緯をお聞かせください。

N 設立当初の Biohacking Village では、テーブルに出所不明の機器が並び、多くの人が集まる状況でした。医療機器メーカーからの抵抗もありました。

S 敵対的なイベントのように捉えられたのですね。

N 私は、医療機器メーカーを陥れようとか、彼らの評判を傷つけようとか、などとはまったく考えていません。私がめざしているのは、彼ら自身と、彼らの会社、そして彼らが作る機器を、患者にとってより良いものにしていくことです。

S 信頼を得るには自分が正しいと思うことをコツコツと続けていくことですよね。

N そのとおりです。私が Biohacking Village を率いるのにふさわしい人物だと認められるまでには、約4年かかりました。2019年には初めて公式に提供された医療機器を使えるようになり、大きな部屋でイベントを開催し、ついにメーカー自

CODE BLUE 2024 の開催に合わせて来日した Biohacking Village のメンバーと日本側でサポートを担当した Eyes, JAPAN の山寺 純氏（写真左）

身が参加するようにもなりました。当初、彼らは消極的でしたが、裏で何かが起こるリスクを負うよりも、実際に自分たちの目で見て確かめる方が良いと判断したのだと思います。

S 当初は不承不承という感じの参加だったのですね。

N ええ。ですが状況が変わり始めたのは、当時 FDA 長官だったスコット・ゴットリーブ氏が Twitter（現在の X）で「今年の DEF CON では Biohacking Village と協力できそうだ」といった内容の投稿をしてからです。政府機関によるそのような公の支持が、周囲の見方を変えるきっかけになりました。メーカー側も私たちの活動を信頼できるものと見なすようになり、協力に前向きになっていきました。もう 1 つ重要だったのは、「I Am The Cavalry」とのパートナーシップです※ 4。この団体は業界内で大きな影響力を持っており、その支援によって私たちもよりスムーズに移行することができました。

S なるほど。政府機関や影響力を持つ団体からの後押しも、医療機器メーカーが対応を軟化させる要因になったのですね。

Biohacking Village の国際的な展開と CODE BLUE 2024

S これまでに、米国以外では何か国で Biohacking Village が開催されたのでしょうか。また、その中にアジアの国も含まれていますか。

N 正確に数えたことはないのですが、これまでにおよそ 21 か国で開催されていると思います。アジアでは、中国で開催したことがあります。

S 中国で開催した様子を簡単に教えていただけますか。

N 中国でのカンファレンスに講演者として参加した際、この分野への強い関心が寄せられました。医療機器の製造方法、サイバーセキュリティの組み込み方、安全性の確保について多くの質問がありました。また、天津大学では薬品化学専攻の学生に、体内でのバイオハッキングや医薬品が装置・機械内でどう生成されるかを教えました。

S はい。

N 国連の生物兵器禁止条約（BWC）の年次会合で

※ 4 **I am The Cavalry** セキュリティ研究者の力をより安全な環境や社会作りに役立てる目的で組織された市民団体
https://iamthecavalry.org/

も発表したことがあります。多くの参加者にとって、自身のデータが安全でない機器や更新手法によって歪められる可能性を知る貴重な機会となりました。

S 中国でも医療機器のセキュリティに対する関心が高まっているのですね。

N 他のカンファレンスでも登壇したことがありますが、そちらでは医療機器メーカーが使用しているチップや半導体そのものに対して、非常に強い関心を持っているという印象を持ちました。

S ありがとうございます。ところで、CODE BLUE 2024 で Biohacking Village を開催することなった経緯について教えてください。

N CarHacking Village の主催者の 1 人からの紹介です。

S なるほど。Car Hacking Village も DEF CON をはじめとするさまざまなセキュリティ・カンファレンス内で開催されていますからね。ちなみに、CODE BLUE での Biohacking Village では、具体的にどのようなイベントがあるのですか。

N いくつかイベントを用意しています。1 つは、私たちが開催する CTF を日本語化して提供する予定です。もう 1 つはデバイス・ラボで、会場に用意された機器を自由に検証できます。今回は VR の医療用グラスやシーメンスの PLC（プログラマブルロジックコントローラ）など 5 種類を準備しています。他にもホルヘさん主導の Birds of a Feather（自由交流セッション）や、「サイバーセキュリティが医療に与える影響」について議論するトークセッションも予定しています。

S 盛りだくさんですね。CTF の競技についてもう少し具体的に教えていただけますか。

N CTF は病院を舞台にしたもので、ハッカーたちが病院内にいるという設定です。参加者はチャレンジをクリアしながら進み、そのたびにポイントを獲得します。進むにつれてチャレンジの内容も変わり、データ分析が求められる問題や、自分でコードを書いて解く問題、インターネットで情報を検索して解決する問題などが出題されます。

S 引き続きデバイス・ラボに関連して、日本の状況について、もしご存知でしたら教えていただけますか。日本メーカーの医療機器シェアはどの程度なのでしょうか。

N 見方によります。例えば日立ハイテクは、ロッシュ社（Roche）と業務提携を結んでおり、日立ハイテクが生産する機器をロッシュ社のチャネルを通じて販売しています。ただ、世界市場から見た場合には、純粋な日本メーカーのシェアは大きいとは言えないと思います。

S 今回のデバイス・ラボには日本メーカー製の機器も含まれるのですか。

N オムロンの製品が含まれます。医療機関向けで考えると、それほど大きなプレイヤーというわけではありません。ですが、彼らは間接的に製品にかかわっています。最終製品には別のブランド名がつくことになるかもしれませんが、その内部にはオムロンの PLC が使われることもあります。

S ありがとうございます。CODE BLUE 2024 で日本初開催となる Biohacking Village を通じて、より多くの方にこの取り組みを知っていただくとともに、医療機関や医療機器メーカーとサイバーセキュリティ関係者をつなぐ架け橋となることを期待しています。

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 2025.04

文＝日立システムズ

企業の内部情報は攻撃者に把握されている

【概要】：決済権限を持つ経理担当者や、機密情報を多く握る幹部層など、社内の特定人物を狙う攻撃が増加している。このような攻撃は、標的の同僚や上司など組織内の人間関係を調べ、関係者になりすまして行われることもあり、ばらまき型攻撃より危険度が高い。攻撃者が内部情報をある程度把握していることを認識し、被害防止には自覚ある行動が重要である。

【内容】：組織内の特定人物を取り巻く人間関係や他社とのやり取りを入念に調べたうえで行われる詐欺被害が増加している。このような巧妙な手口により英国では約 40 億円の詐欺被害を受けた事例がある。最新の事例では、英国で約 40 億円の被害が発生している。この事例では、同社の経理担当者宛てに CFO を名乗る人物から秘密取引の連絡が届き、会議参加を依頼された。経理担当者が案内されたビデオ会議に参加すると、同僚も出席していたため正規取引と判断し、指示に従い約 40 億円を振り込んだ。実際には、会議に参加していた同僚はすべてディープフェイクによる偽物だった。この事例から、決済権限を持つ経理担当者やメールアドレス、標的の同僚、さらにその容姿まで攻撃者に把握されていたことが分かる。

国内でも、某輸入販売業者が取引先の担当者をかたる攻撃者にだまされ、偽の口座に送金した事例がある。この際、被害企業と取引先の正規のやり取りは盗聴されており、請求書送付のタイミングで、攻撃者が担当者になりすまし口座変更を連絡してきた。この際、偽の口座情報証明書が送付され、書類には正規の取引先社長印が押されていたという。また、過去には海外グループ会社の在勤者をかたり、社外非公開の部門のメンバーの職位や氏名を把握した上で、職制順に電話をかけてきた事例もある。こうした事例から、「知られているはずがない」と思える内部情報も攻撃者に把握されていると考えるべきである。

表 内部情報が把握されていたことが分かる攻撃の例

事例	把握されていた情報
フェイク映像を利用した会議にだまされ、振込を行った事例	経理担当者情報、メールアドレス、標的の同僚および容姿
口座書類を偽造し、振込先変更を依頼した事例	取引先情報、取引先とのメール内容、取引先社長印情報
電話連絡があった事例	社外非公開の部門のメンバーの職位、氏名、電話番号

攻撃者は時間をかけて対象の情報を収集し、特定人物を狙って攻撃する。具体的には Web 検索に加え、偽プロフィールで SNS のコミュニティやグループに参加してチャットを盗み見たり、SNS 上で直接接触して情報を聞き出すなど、さまざまな OSINT（Open Source Intelligence）を用いて情報収集を行なっていると考えられる。

攻撃者に余計な情報を与えないよう、公開情報の見直しや、意図せず公開された情報の確認・対処が必要となる。ただし、対策を講じても何らかの原因で内部情報が流出する可能性はあり、攻撃者にどの情報が知られているかを正確に把握するのは難しい。そのため、攻撃を受けた際に騙されないよう、予防策を講じることが推奨される。例えば、取引先や同僚、上司など関係者からの連絡でも違和感があれば、別の手段で直接連絡を取り、それが正規のものか確認することが対策として挙げられる。これは SNS 経由での接触も同様であり、相手が信用できると確認できるまで、必要以上の情報を提供しないよう注意すべきである。社内の内部情報は攻撃者に把握されていると認識し、被害を防ぐためにも、やりとりする相手が信頼できる人物かを確認するなど、自覚を持った行動が重要である。また、送金先口座は経理・調達部門などで一元管理し、新規口座への送金時には口座審査を複合的に行える様定型化するなど、正当性の確認を徹底することが対策の 1 つとなる。

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 Web サイト簡易調査

1. Web アーカイブ利用編

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。「Web サイト簡易調査」と題して、フィッシングサイト、改ざんされたサイトなど、直接アクセスする事が危険である Web サイトについて、Web アーカイブの 1 つである urlscan.io を用いた調査を紹介します。例えば、フィッシングサイトにアクセスしてしまったと相談を受けたセキュリティ管理者が実施する調査を想定しています（下図参照）。

「Web サイト簡易調査」は、以下の 2 部により構成されます。

1. **Web アーカイブ利用編**
   過去にキャプチャーされた Web サイトの情報を活用して、Web サイトの危険性や類似のコンテンツなどを調査します。
2. **SandBox 編**
   入力した URL の Web サイトに潜む危険性を確認するサービスを利用して Web サイトを調査します。

今回は、「1. Web アーカイブ利用編」として、urlscan.io を用いた調査を紹介します。urlscan.io は、Web サイトをスキャンしてさまざまな情報を表示してくれるオンラインサービスです。調査したい URL を検索することで、利用者に代わって urlscan がアクセス・スキャンを行います。

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。

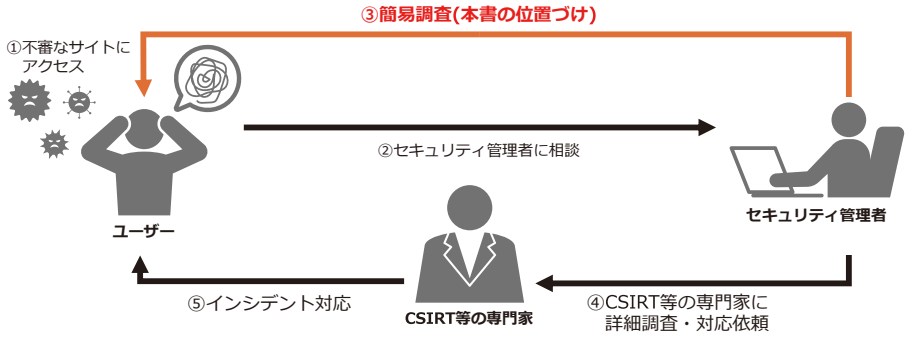


図 不審な Web サイトに対する簡易調査

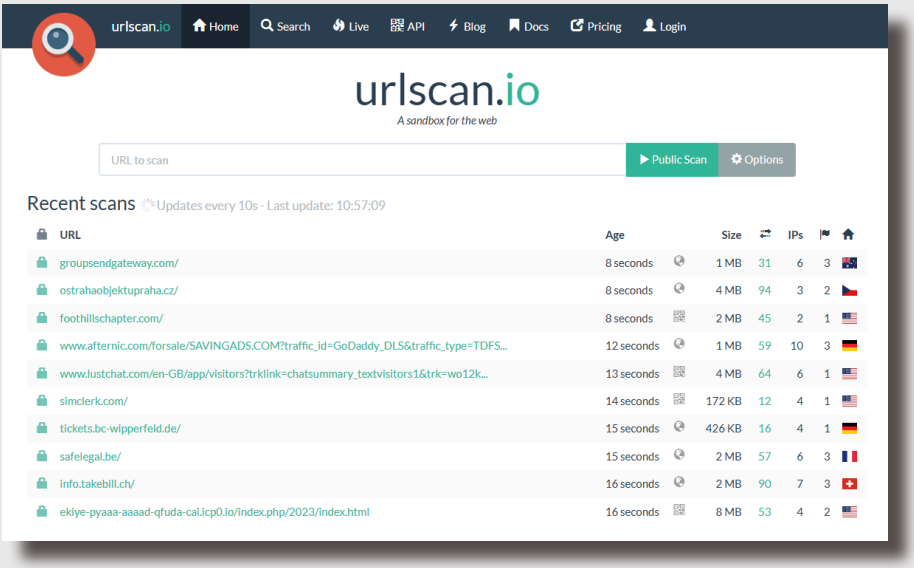
2. 事前準備

今回は、過去に確認されているフィッシングサイトの内容を確認します。フィッシングサイトは、悪意ある Web サイトです。安全な調査環境を準備して、調査をすべきです。調査環境例については、本誌 Vol. 63「Let's try OSINT 体験 1. 環境準備編」でも紹介しています。そちらも参照してください。

3. urlscan.io

3.1 urlscan.io を使った調査

urlscan.io は、Web サイトをスキャンしてさまざまな情報を表示してくれるオンラインサービスです。調査したい URL を検索することで、urlscan.io が代わりにアクセスしてスキャンを行い、IP アドレスや HTTP レスポンスの情報を確認することができます。例えば、自組織にフィッシングを疑う不審なメールが届いた場合、直接アクセスするのではなく、urlscan.io の Public Scan を実施することで、サイトの画面やレスポンス情報を確認し、それらの情報を深堀して分析するなどして活用できます。



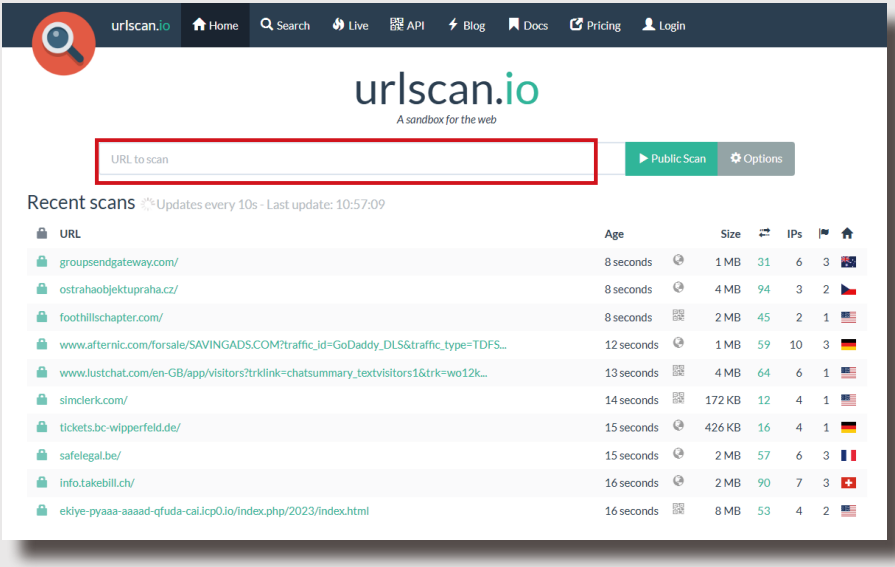
https://urlscan.io/

なお、urlscan.io については、本誌 Vol. 64「Let's try OSINT 体験 2. Web データ収集編」※1 においても紹介しています。そちらも参照してください。

※1 https://www.hitachi-systems.com/-/media/report/specialist/hj/download/SSRC-HJ-202409.pdf

3.2. urlscan.io を活用したス調査例（スキャン）

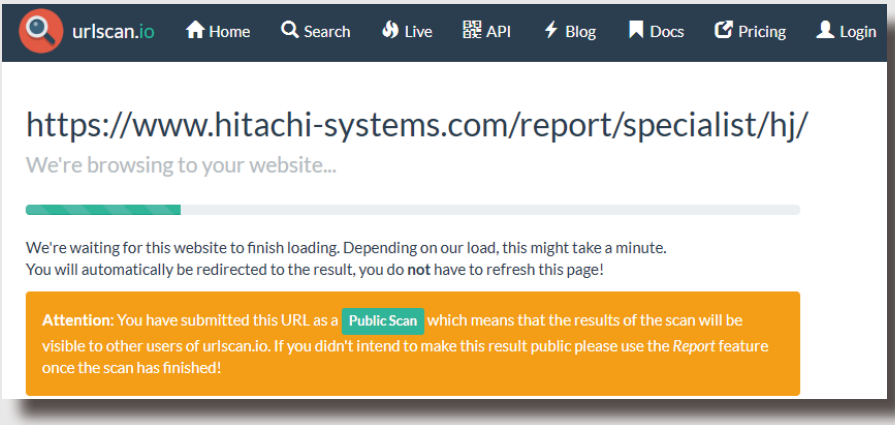
ここでは、urlscan.io を活用した調査例（スキャン）をご紹介します。まずは、urlscan.io にアクセスし、当該ドメインで検索を行います。



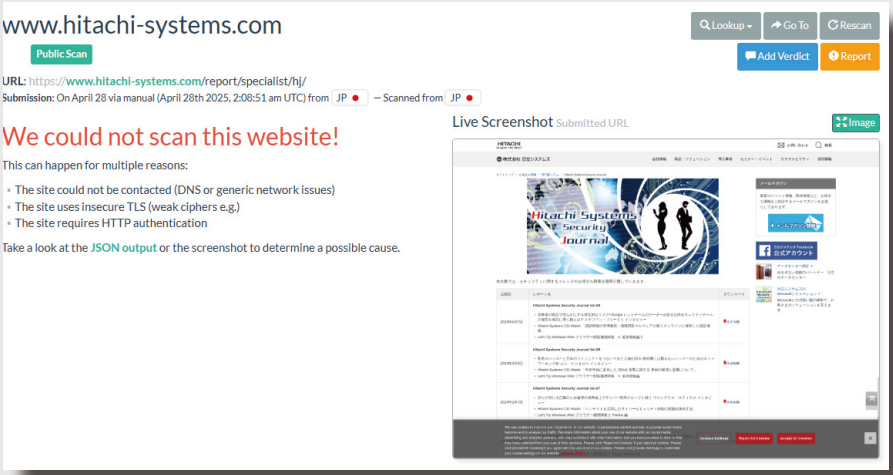
ここでは便宜上、以下の Hitachi Systems Security Journal のページで検索します。

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

Scan を実施すると、以下のようにスキャン中の画面が進行します。



Scan が終了すると次のような画面に遷移します。



本稿執筆時点では、いくつかの理由で完全な調査はできませんでしたが、スクリーンショットの取得は完了しました。
なお、URL にメールアドレスや識別するための ID などが含まれている場合、メールアドレスを含むスキャン結果が一般に公開されてしまう場合がありますので注意が必要です。

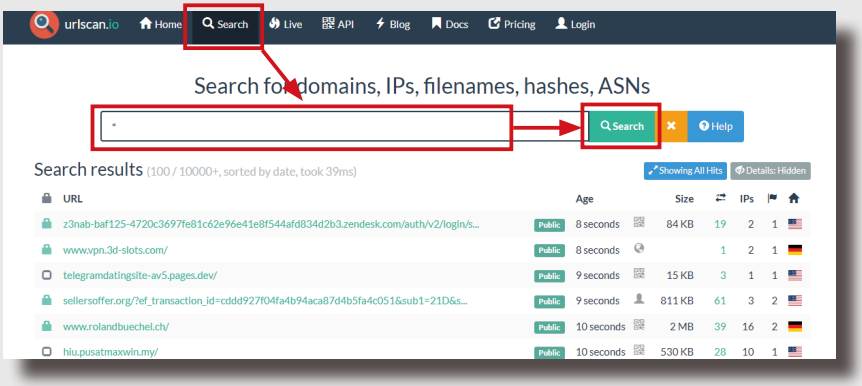
3.3. urlscan.io を活用した調査例（スキャン結果確認）

次は、調査した URL のスキャンが完了、または、他の方々が先行してスキャンを実施済みであったものと想定して、スキャン結果を用いて調査していきます。
例えば、相談を受けたドメインが下記であったと想定します。

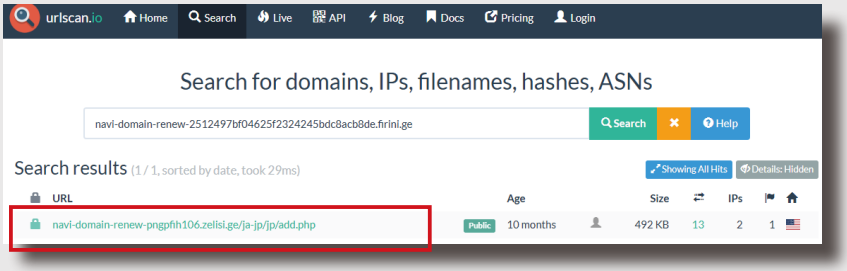
navi-domain-renew-2512497bf04625f2324245bdc8acb8de[.]firini[.]ge

なお、上記のドメインは、安全のためデファング（無害化）しています。調査実行時は、[.] を . に置き換えてください。

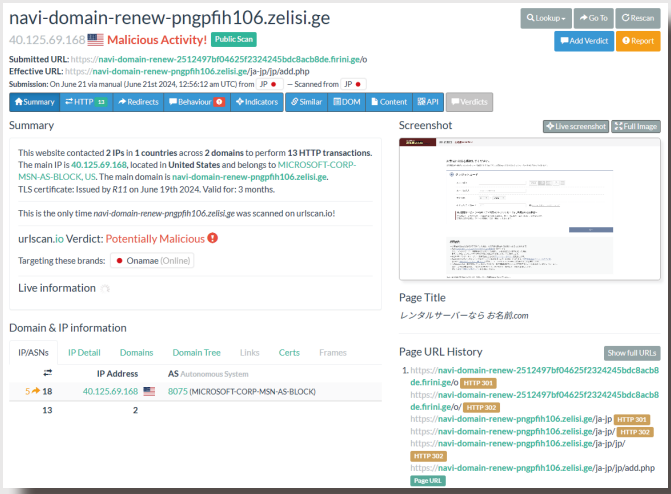
urlscan.io にアクセスし、上部タブの「Search」をクリックし、検索画面に遷移し、調査ドメインを入力し、「Search」ボタンを押下します。



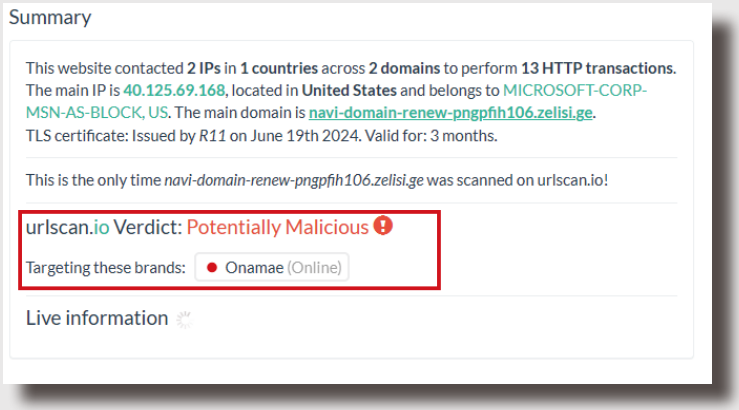
検索が完了すると以下の画面が表示されます。本稿執筆時点では Age「10months」となっていますので、10 カ月前に誰かがスキャンした結果が存在していることがわかります。



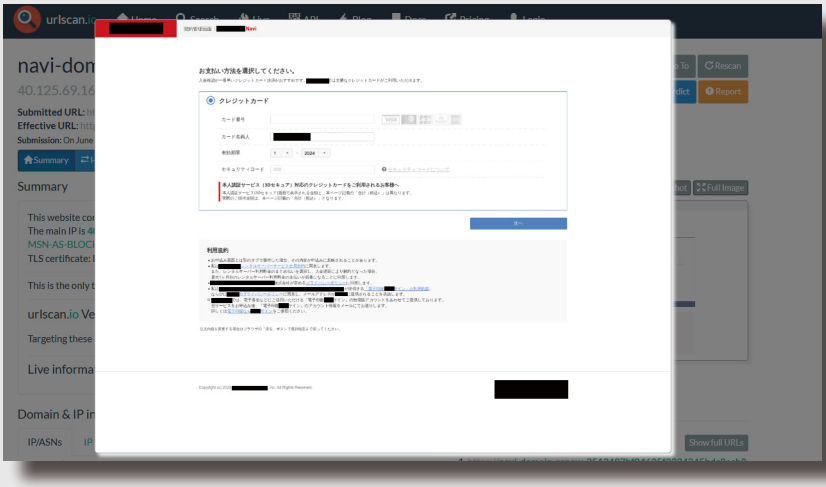
次にリンクをクリックして、詳細を確認すると、以下のページが表示されます。



左側の「Summary」に当該サイトの概要が記載されています。

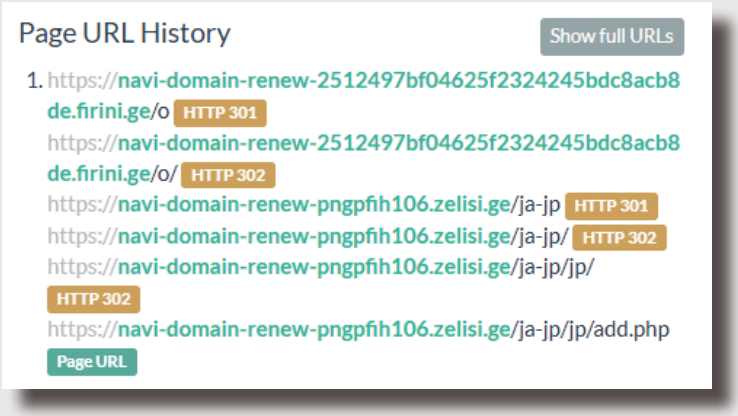


ここでは、urlscan.io が「危険な可能性」を指摘、さらに、「Onamae」というブランドを標的としていることが読み取れます。
次に右側「Screenshot」の画像を押下します。

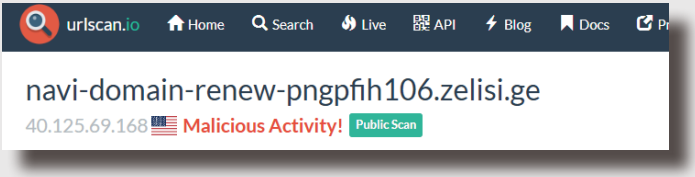


画面から、ドメイン登録サービスをかたり、クレジットカードを窃取しようとしているフィッシングサイトとであったと推察することが可能です。

次に、右下の Page URL History を確認します。



こちらは、当該ドメインにアクセスした際に自動的にリダイレクトされた遷移履歴を表示しています。すでにお気づきかと思いますが、最終的に urlscan.io のタイトルとして表示されるドメインは、検索したドメイン（いちばん最初にアクセスするドメイン）と異なり、リダイレクトと先であるフィッシングサイト自体のドメイン（最後に目をするドメイン）となっている点に注意してください。



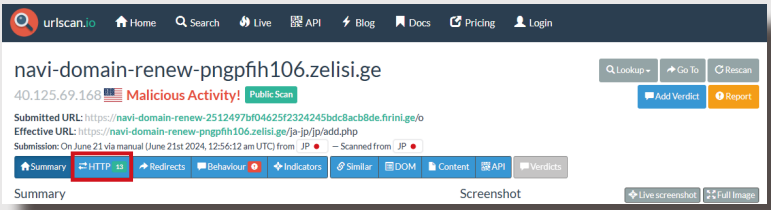
urlscan.io では、このような遷移も関連付けて保存しています。もし、調査ドメインが最終的なドメイン（今回の場合 navi-domain-renew-pngpfih106.zelisi.ge）しかわからない場合、このドメインで検索することで、履歴をさかのぼり、利用者が最初にアクセスした URL またはドメインなどを調査できる場合があります。
判明したドメインなどを URL フィルターに登録するなど対応するとともに、必要に応じて CSIRT などの専門家に詳細調査・対応を依頼します。

3.4. urlscan.io を活用した調査例 (追加調査)

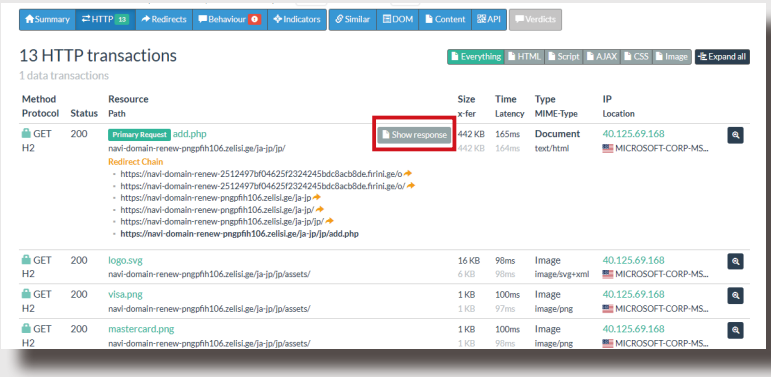
組織の情報資産を守るために、セキュリティ対策を推進する役割を担う人財「セキュリティ管理者」の立場であれば、前項までの内容で調査は十分かもしれませんが、ここでは、もう一歩だけ調査を進めてみます。

3.4.1 HTTP（HTML など）データ確認

当該ページの HTTP（HTML など）データを確認したい場合は、「HTTP」タブをクリックします。



その結果、以下のようなページが表示されます。各行が HTTP レスポンスを表しており、どの Web サーバーとどのような通信が行われたのかを確認できます。

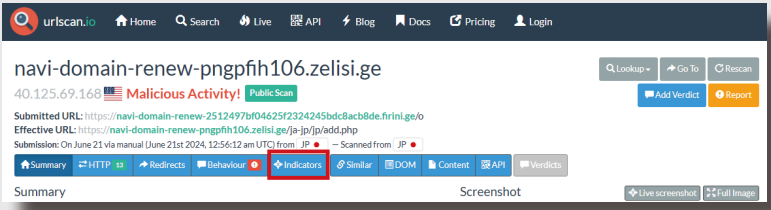


例えば、「Show response」を押下すると、HTML ソースコードを確認することができます。
なお、「Show response」は生データを閲覧します。アンチウイルスなどに検知される可能性がありますので注意してください。

```
<!DOCTYPE html><html itemscope="" itemtype="http://schema.org/WebPage" lang="ja" class="">
<head>
<link rel="icon" href="./assets/favicon.png">
<meta charset="utf-8">
<title>レンタルサーバーなら お名前.com</title>
<link rel="icon" href="./assets/favicon.png" type="image/png">
<meta name="csrf_token" content="AJAflAAISP8twS5xrepvykFfFDKNlemCtXnhMhTI">
<meta http-equiv="X-UA-Compatible" content="IE=Edge">
<meta name="viewport" content="width=1024">
```

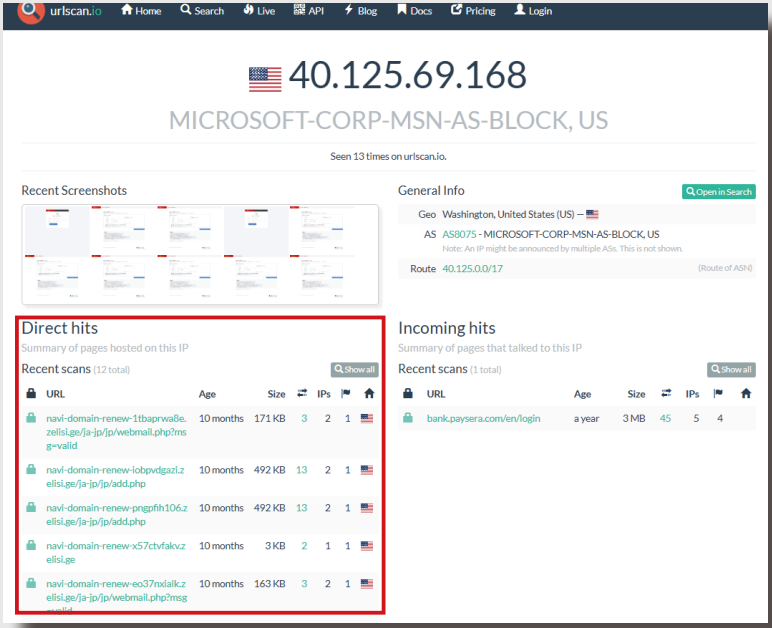
3.4.2 関連サイトの確認

特徴点を用いて、類似攻撃者のサイトなどを確認します。タブより「Indicators」を押下します。

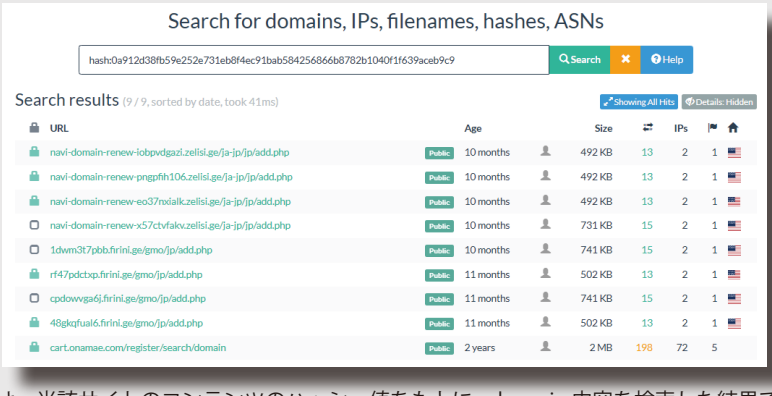


その結果、以下のようなページが表示されます。

「Indicators」に記載の内容が、このサイトの特徴点となる指標です。
例えば、「IP アドレス：40[.]125[.]69[.]168」をクリックすると、次の画面が表示されます。
「Direct hits」の URL が記載されるなど、今回の遷移では確認できなかったその他不審なドメインが関連付けられていることがが確認できます。



また、「Hash 値：0a912d38fb59e252e731eb8f4ec91bab584256866b8782b1040f1f639aceb9c9」も押下してみます。



これは、当該サイトのコンテンツのハッシュ値をもとに urlscan.io 内容を検索した結果です。
同様のコンテンツを所有している (または所有していた) サイトに関する URL 情報を得ることができました。
なお、「Hash 値：937486b8bf9320622c4928d92d813611f37cc1ee829df6cba69db2befd37a032」で検索すると、正規の「onamae.com」が多数検索結果に表示されます。これは、フィッシングサイトが、正規の「onamae.com」のコンテンツを流用していたことに起因すると考えられます。

4. おわりに

今回はここまでとなります。「1. Web アーカイブ利用編 」では、フィッシングサイト、改ざんされた Web サイトなど、直接アクセスする事が危険である Web サイトについて、Web アーカイブの 1 つである urlscan.io を用いたフィッシングサイトを例に調査手法を確認しました。次回、SandBox 編では、入力した URL の Web サイトに潜む危険性を確認するサービスを利用した調査を行います。

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.70

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