HITACHI
Inspire the Next

Hitachi Systems Security Journal

VOL.51

株式会社 日立システムズ

Human * IT

Hitachi Systems security Journal VOL.57

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

クリスチャン・ダメフ＆ジェフリー・タリー

インタビュー

今回、話を伺うクリスチャン・ダメフ氏とジェフリー・タリー氏は、医師でありハッカーでもあるという異色の経歴の持ち主だ。学生時代をハッカー・コミュニティで過ごし、医師となった後も、患者の安全に焦点を当てたヘルスケア・サイバーセキュリティ・カンファレンスの設立・運営などに尽力している。

そんな彼らが CODE BLUE 2023 に登壇した。講演のタイトルは「ランサムウェアの反響：大規模サイバー攻撃の影響範囲の解明」だ。地域の病院がランサムウェアに感染して業務が停止した場合、緊急搬送などは地域内の別の病院が受け入れることとなるが、奇しくも実際の感染事例において彼らが所属する病院が受け入れ側になったという。ランサムウェア被害の発生前、業務停止期間中、システム復旧後、それぞれの時期にどのような変化があったのか、彼らは詳しく調査した。この研究は、ランサムウェアによる被害が地域医療全体に及ぼす影響を示す貴重な事例だと言えるだろう。

取材・文・撮影＝斉藤健一／通訳＝坂恵理子

ハッカー・コミュニティから医療の世界へ

斉藤（以下 S）：2 人は医師でありながらサイバーセキュリティの世界にも携わるという異色の経歴をお持ちです。どのような経緯でこの道を歩むことになったのですか。

クリスチャン・ダメフ（以下 C）：私とジェフリーは大学時代からの友人で、共に DEFCON をはじめとするハッカー・コミュニティの中で過ごしてきました。当時、ハッカーが職業となる時代が来るとは想像もしていませんでした。そのため、私たち 2 人は大学卒業後に専門職の大学院にあたるメディカルスクールへと進学したのです。医師となった後は、それぞれ異なるキャリアを歩んできましたが、2021 年からは共に UC San Diego Health という医療機関に所属しています。

S 地域の病院がランサムウェアに感染して業務が停止した場合、緊急搬送などは地域内にある感染を免れた別の病院が受け入れることとなります。奇しくも実際の感染事例において 2 人が所属する病院が受け入れ側になり、ランサムウェア被害の発生前、業務停止期間中、システム復旧後、それぞれの時期にどのような変化があったのかを調査・研究され、論文も発表されました。これは、医療機関の関係者でありサイバーセキュリティにも携わる 2 人にしかできない研究だと感じました。

C ありがとうございます。私たちは、医療とサイバーセキュリティの 2 つの世界を組み合わせることができたという点で幸運でした。しかし、2 つの異なる世界を知っているがゆえに、困難を感じる部分もありました。

S それはどのような部分でしょう。

C 今日の医療が、EHR（Electronic Health Record：電子健康記録）システムに依存しているという点です。私たちはこの EHR を医療のオペレーティング・システムと称しています。ランサムウェアの感染によってシステムが停止してしまうと、医療行為の継続が困難となります。また、医療機器のセキュリティについても研究者との情報交換などを通じて、いかにぜい弱なものなのかも理解しています。結局のと

クリスチャン・ダメフ（Christian Dameff）

カリフォルニア大学サンディエゴ校（UC San Diego）の救急医学、生物医学情報学、コンピューターサイエンスの助教授であり、UC San Diego Health では、サイバーセキュリティ担当医長として採用された。ダメフ氏はまた、医療、患者安全、サイバーセキュリティの交差点に関心を持つハッカーであり、セキュリティ研究者でもある。DEF CON、RSA、BlackHat、BSides など、世界で最も著名なサイバーセキュリティフォーラムで講演を行ない、医療機器とインフラのサイバーセキュリティに重点を置いた斬新な学際的会議である CyberMed Summit の共同創設者の 1 人でもある。

ジェフリー・タリー（Jeffrey Tully）

UC San Diego Health ヘルスケアサイバーセキュリティセンターの共同ディレクターを務める。タリー氏は、麻酔科医、小児科医、セキュリティ研究者であり、医療とテクノロジーの相互関係がますます深まっていることを理解することに関心を持っている。医学部入学以前は、サルモネラ菌の遺伝子コードを「ハッキング」して抗がんツールを作る研究に従事し、医学研修中は、遠隔診療、埋め込み型医療機器、バイオハッキングの新時代に直面する中、医療を安全にし、患者を守るための対話やプロジェクトに関わり続けている。ダメフ氏とともに CyberMed Summit の共同創設者の 1 人でもある。

ころ私たちが望むのは、すべての患者の回復です。しかし、サイバーセキュリティに対する注意がなければ、常にリスクが存在するのです。

S わかりました。医療機器のセキュリティについては後ほど伺いたいと思います。

ランサムウェアの脅威で議論される 2 つの意見

S CODE BLUE での講演の中で、医療機関に対するランサムウェアの脅威について、米国内で議論される 2 つの意見が紹介されました。1 つは、ランサムウェアは「空が落ちてくる」ほどの大きな災害であり、これによって多くの患者の命が失われたり、そのおそれがあるというものです。もう 1 つは、ランサムウェアの脅威は誇張されたものであり、たとえ攻撃を受けたとしても、患者へのケア能力には大きな影響は与えないというものです。それぞれについて伺います。

ジェフリー・タリー（以下 J）：わかりました。

S まず前者の意見についてですが、日本においても一部の人たちが同様の意見を持っています。単純な疑問なのですが、ランサムウェアの攻撃によって人命が失われた事例はあるのでしょうか。

J ランサムウェアは医療機器を直接攻撃するわけではありません。しかし、ランサムウェアの攻撃により病院の業務が停止することで、緊急医療を提供できずに不幸にも患者の死につながったという間接的な事例はあります。2020 年のドイツの事例では、緊急手術を必要とする患者を乗せた救急車が最も近い病院に向かいましたが、その病院がランサムウェアに感染しており受け入れることができず、遠くの病院に搬送する途中で患者が亡くなりました。また、2021 年の米国の事例では、胎児の健康に問題を抱えた女性が、ランサムウェア攻撃を受けていた病院で出産しました。本来、新生児の健康状態はモニタリングされるべきでしたが、医療システムのダウンにより担当医師にはこの事実が伝えられず、新生児は適切なケアを受けられずに死亡しました。この事例では病院側が女性に対してランサムウェア感染を開示していなかったという別の問題もあります。

S どちらの事例も痛ましい限りです。

J 短期的に見て人命に関わるものではありませんが、米国のある病院がランサムウェアによる攻撃後、財政難に陥り閉鎖することとなりました。地域社会において病院の閉鎖は、将来にわたりすべての患者が他の地域でケアを受けなくてはならないことを意味します。長期的に見ると地域社会に与える影響は大きいと言えます。

S わかりました。次に、後者の意見について伺います。前者のときと同じく、日本においても同様の意見があります。多くの病院が自然災害や停電などの不測の事態に備えて BCP（Business Continuity Plan：事業継続計画）を策定しており、ランサムウェアの攻撃によって業務が停止した場合でも、この BCP が適用できるのではないかというものですが、この点についてはどのようにお考えでしょうか。

C その質問に対しては、具体的なデータを持っていませんので、明確な回答はできませんが、個人的には難しいのではないかと予想しています。ランサムウェアに限定したものではありませんが、2018 年の研究で、先にお話した EHR システムの停止が医療現場に与える影響をまとめたものがあります。その研究によると、システム停止中の手続き（ダウンタイム・プロシージャ）が正確に実行されたのは、全体のわずか 27%程度であり、約半数の 46%の事例では、停止中の手続きを実行できなかったか、または手続きが策定されていなかったと報告されています。

S 27%という数値は高いとは言えませんね。
C はい。ダウンタイムの手続きを策定しただけで安心してしまうケースもあるのだと思います。また、ランサムウェア攻撃による業務停止の期間も長期化する傾向にあります。以前なら感染による影響は数日で済んでいましたが、今では数週間に及ぶこともあります。さらに、復旧のための費用も甚大です。現在、米国の病院が被害に遭うと、1億ドル以上のコストがかかると報告されています。
S 財政的な損失も大きいですね。実際のところ、病院がランサムウェアに感染して被害に遭った場合、身代金を支払うケースが多いのでしょうか、それとも支払わずに解決しようとするのでしょうか？
C 具体的なデータを持っているわけではありませんが、聞くところでは多くの病院が身代金を支払っているそうです。実は米国では、重要インフラがサイバー攻撃を受けた場合に報告を義務づける法律（Cyber Incident Reporting for Critical Infrastructure Act of 2022：CIRCIA）が成立しました。もちろん、病院も重要インフラの中に含まれています。この法律の規定によると、重要インフラがサイバー攻撃を受けた場合、その組織は72時間以内に、DHS（米国国土安全保障省）の外局であるCISA（Cybersecurity and Infrastructure Security Agency：サイバーセキュリティ・社会基盤安全保障庁）に報告しなければなりません。
S CISAへの報告によって、復旧がよりスムーズに行なわれることを願っています。

医療業界のサイバーセキュリティを向上させるために

S 2人が所属するUC San Diego Healthは、同じ地域にある別の病院がランサムウェアの被害に遭い業務を停止したため、緊急搬送などを引き受けることになりました。この間、実際にどれほどの負担増があったのでしょうか。
C この時の状況を調査した論文は、2023年5月に米国医師会が発行するジャーナル（Journal of American Medical Association：JAMA）で発表し

ており、誰でも読むことができます※1。この研究は、2021年にサンディエゴ地域の5つの病院がランサムウェアの被害にあったときの状況をまとめたものです。緊急医療部門を対象に、攻撃前・攻撃中・攻撃収束後をそれぞれ4週間ずつに区切り、どのような変化があったのかを調査しています。当然ですが、救急車の到着が急増しましたし、緊急医療を受けるまでの待ち時間も大幅に長くなり、多くの人が医師に診てもらうことなく帰宅せざるを得ない状況となりました。また、業務を停止した病院では脳卒中の患者を受け入れていましたので、攻撃中に私たちの病院が受け入れる脳卒中患者の数もほぼ倍増することとなりました。
S 受け入れる病院スタッフのご苦労や、診察を待つ患者の方々の心労がうかがわれます。論文発表後、周囲からはどのような反響がありましたか。
C 多くのメディアから注目を浴びましたし、他の研究者からの問い合わせも受けました。また、政策立案者も興味を持ってくれました。
S ありがとうございます。今回のインタビューに際し、2人の経歴などを調べていたのですが、クリスチャンさんが連邦議会の公聴会でランサムウェアの脅威について意見陳述を行なったことがわかりました。公聴会の模様は動画としてアーカイブされていたので視聴してみました※2。この公

※1 **Ransomware Attack Associated With Disruptions at Adjacent Emergency Departments in the US**
https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2804585

聴会はいつ行なわれたのでしょうか。

C 2021 年です。ランサムウェアの被害が発生したのと同じ年になります。

S 公聴会では医療のサイバーセキュリティを向上させるため、いくつか提言をされています。こちらについて伺います。まず、『ランサムウェア攻撃が患者の健康に与える影響について科学的に研究するべき』と発言されています。今回の 2 人の調査や論文発表の根底にはこの発言があるのですね。

C そのとおりです。調査の目的は、医療機関のサイバー脅威に関して、データに基づく科学的な根拠を示すというものでした。先にお話ししたランサムウェアの脅威に関する議論は、あくまで「専門家の意見」でしかありません。私たちの研究は、そこから一歩進めた「事例報告」ということになります。もちろん、セキュリティ対策を検討するためには、今後も根拠を積み重ねていく必要があると考えています。公聴会では、国立衛生研究所（NIH）や国立科学財団（NSF）などの連邦機関に、このトピックに関する研究への資金提供を優先させることも提案しました。

S 他にも『医療機関の間で経済的な格差が生まれており、十分なリソースを持たない地方の病院などには支援が必要。さらに、サイバー攻撃の犠牲となった組織に対して過度なペナルティを課すことは事態を悪化させる』とも発言されていますね。

C はい。ランサムウェア攻撃を受けた病院は、評判に大きなダメージを受けるだけでなく、ほとんどの場合、財政的な損失も被っています。病院側に重大な過失がない限り、罰則を課すことは有効ではありません。

J 病院が罰則を心配することなく事態を報告し、できるだけ早く助けを求めることを奨励するべきです。財政的に厳しい病院に対して罰則を課すと、先にお話したとおり、病院が閉鎖に追い込まれる可能性があります。彼らに資金を再投資してインフラを強化するよう奨励した方が、社会にとってはるかに良いでしょう。

S サイバー攻撃の被害をセキュリティの強化につなげる良いアイデアだと思います。また、公聴会では『ぜい弱性に関する透明性を高めるため、SBOM（Software Bill Of Materials：ソフトウェア部品表）の有効性を強調。さらに、善意のセキュリティ研究者に対する継続的な支援と法的保護』についても言及されています。

C ぜい弱性に関する透明性を高めることは非常に重要です。悪意あるハッカーに対抗するには倫理的なハッカーや善意のセキュリティ研究者の助けが必要です。

S 全くもってそのとおりです。それと同時に 2 人の出自がハッカー・コミュニティであることを強く感じます。

ベンダーとハッカー・コミュニティとの協調

S 引き続き医療機器のセキュリティについて伺います。医療機器ベンダーとハッカー・コミュニティとの関係についてお聞かせ下さい。

C 現在、多くの医療機器ベンダーは、製品やサービスのセキュリティを強化するためにハッカー・コミュニティと協力しています。

J 倫理的なハッカーやセキュリティ研究者が製品やサービスのぜい弱性を発見した場合に、ベンダー（開発者）などの関係者と調整し、修正されたことを確認した上で一般公開する「協調的なぜい弱性開示」というアプローチが主流となっています。

C 両者の関係は最初から友好的な関係だったわけではありません。長い間、病院システムや医療機器ベンダーはハッカー・コミュニティの声を無視してきました。ですが、過去 15 年間にわたるハッカーの調査・研究によって医療機器メーカーの姿勢が徐々に肯定的なものに変化していきました。これらは 2018 年に心臓ペースメーカーのぜい弱性を発見したビリー・ライオス氏（Billy Rios）※ 3 や、インスリンポンプのぜい弱性を発見したジェロー

※ 2 **Congressional hearing 'Stopping Digital Thieves: The Growing Threat of Ransomware'**
https://www.youtube.com/live/f8EAlfca6l0?feature=share&t=2104
（編注：ダメフ氏の意見陳述は動画の 35 分 02 秒付近から始まる）

※ 3 **Understanding and Exploiting Implanted Medical Devices**
https://www.blackhat.com/us-18/briefings/schedule/#understanding-and-exploiting-implanted-medical-devices-11733

ム・ラドクリフ氏（Jerome Radclife）※4らの成果によるものです。

J 米国ではFDA（米国食品医薬品局）が医療機器のサイバーセキュリティを管理していますが、これもハッカーたちによるぜい弱性開示が大きく貢献しています。現在、多くの医療機器ベンダーが自社の機器をDEFCONのヴィレッジなどに提供し、ハッカーによるセキュリティチェックを積極的に受け入れるようになりました。

S ありがとうございます。ベンダーとハッカー・コミュニティとの協調関係が築かれる過程を知ることができました。最後の質問です。ランサムウェアの被害を予防するという観点から、何か病院にできることはありますか。

C とても難しい質問です。先ほどもお話したとおり、私たちの研究はサイバー脅威に際して正しい意志決定をするための根拠を積み上げることに焦点を当てています。研究はまだ途上にあり、科学的な根拠に基づいた発言をするためには、さらなる調査や研究データが必要です。仮に、10年後であれば、十分な根拠に裏付けされた回答ができるかもしれません。

S まさに科学者の研究に対する姿勢そのものですね。本日は本当にありがとうございました。

※4 **Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System**
https://www.blackhat.com/html/bh-us-11/bh-us-11-archives.html#Radcliffe

文＝日立システムズ

暗号化以外の手口で身代金を要求するランサム攻撃グループへの対応

【概要】：2023 年 9 月、ランサム攻撃グループの 1 つである RansomedVC が日本企業を攻撃したと公表した。このグループの特徴は、ファイルの暗号化はせず、窃取したファイルを公開すると脅して身代金（Ransom）を要求することだ。近年では、暗号化以外の手口を駆使して、身代金を要求するグループが増えている。そのため、ランサム攻撃グループへの対策にはバックアップだけでは対応が難しくなりつつある。サイバー攻撃の被害に遭うことを前提に、情報漏えいの監視を強化して、迅速に対処できる体制構築が重要である。

【内容】：2023 年 9 月、RansomedVC と呼ばれるランサム攻撃グループがソニーとドコモを攻撃したと公表し、その特徴的な手口も相まって話題になった。これまでのランサム攻撃では、業務ファイルを暗号化して、そのファイルの復号と引き換えに身代金を要求するという攻撃手法が一般的であった。しかし RansomedVC では、業務ファイルの暗号化ではなく、窃取したファイルをリークすると脅迫する手法が他のグループにはない特徴である。

主要な脅迫の手法は、①「暗号化した業務ファイルの復号と引き換えに身代金を要求」、②「窃取した業務ファイルを公開すると脅迫」、③「DDoS 攻撃を仕掛けると脅迫」の 3 種類である。ランサム攻撃グループはこれらの手法を組み合わせて攻撃を行なっている。表の攻撃手法と対応させると、①②を行なう攻撃は警察庁では B の二重恐喝と呼んでいる。①②③を行なう攻撃は C の三重恐喝、②のみを行なう攻撃は D のノーウェアランサムと呼ばれている。ノーウェアランサムという単語は、9 月 21 日に警察庁が公開した資料で初めて使用されたものであり、国外では Encryption-less Ransomware などと呼ばれている。

表 ランサム攻撃の手法と代表的なグループ

#	攻撃手法	2023 年上半期 警察庁報告件数	攻撃グループ
A	ファイルの暗号化のみ	未記載	Phobos
B	二重恐喝（ファイルのリーク）	65 件 (78%)	Clop, Maze
C	三重恐喝（DDoS 攻撃）	未記載	Lockbit, Ragnar Locker
D	ノーウェアランサム	6 件 (7%)	RansomedVC, BianLian

BianLian と呼ばれる攻撃グループは以前から B の二重恐喝を行なっていた。その後、このグループによって暗号化されたファイルの復号ツールが 2023 年 1 月に公開されたが、この頃からノーウェアランサムの手口に方針転換している。ノーウェアランサムは情報窃取型のマルウェアを用いた脅迫と攻撃手口は変わらないものの、攻撃グループが手口を変えたことから、ランサム攻撃の 1 つとしてノーウェアランサムと呼んでいると推測される。

従来のランサム攻撃に対してはバックアップが主な対策とされてきたが、これだけでは①への対策しか行なえず、②、③を併用した脅迫方法には、バックアップでは不十分とも読み取れる。従来の攻撃であればファイルが暗号化されるため攻撃に気づきやすいが、ノーウェアランサムは見つからないように攻撃を進めるため、気づかない内に情報窃取されている恐れがある。このことから、ダーク Web を含めた情報漏えいの監視を強化して、迅速に対処できる体制構築が重要となる。

［情報源］ https://x.com/MalwareBibleJP/status/1719553784878407798
https://www.bleepingcomputer.com/news/security/amd-investigates-ransomhouse-hack-claims-theft-of-450gb-data/

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 IoT 検索エンジン！

2. 所有サーバー確認編

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を実践的に紹介する連載企画です。前号より第三部「IoT検索エンジン」と題し、「Shodan（ショーダン）、Censys（センシス）」といったIoT検索エンジンを用いたぜい弱性確認手法などを解説しています。「自組織が管理しているサーバーが外部からどのように見えているのか」といった確認に利用したり、管理しきれていない隠れたサーバーなどを探索したりして、リスクの軽減に活用可能です。

「IoT検索エンジン」は次の4部構成となっています。

1. 基礎知識編
   Nmapを利用して、ポートスキャンを試行します。

2. 所有サーバー確認編
   自身が管理しているIPアドレス等がわかるサーバーが「Shodan、Censys」といったIoT検索エンジンでどのように見えるのかを確認します。

3. サービス探索編
   「Shodan、Censys」といったIoT検索エンジンを用いて、探索したいサービスが稼働しているサーバーを探索します。また、自組織で管理できていないサーバーを探索する際にも利用します。

4. サーバー探索編
   「Shodan、Censys」といったIoT検索エンジンを用いて、サーバーを探索します。また、自組織で管理できていないぜい弱なサーバーを探索する際にも利用します。

IoT検索エンジンと呼ばれる「Shodan、Censys」ですが、インターネット上に公開されているサーバーなど、さまざまな情報を収集しており、検索・閲覧が可能なサービスです。

「②所有サーバー確認編」では、「Shodan、Censys」を使った自身が管理しているサーバーの確認方法、「Shodan、Censys」での見え方を確認します。

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ございません。
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いたします。

2. 準　備

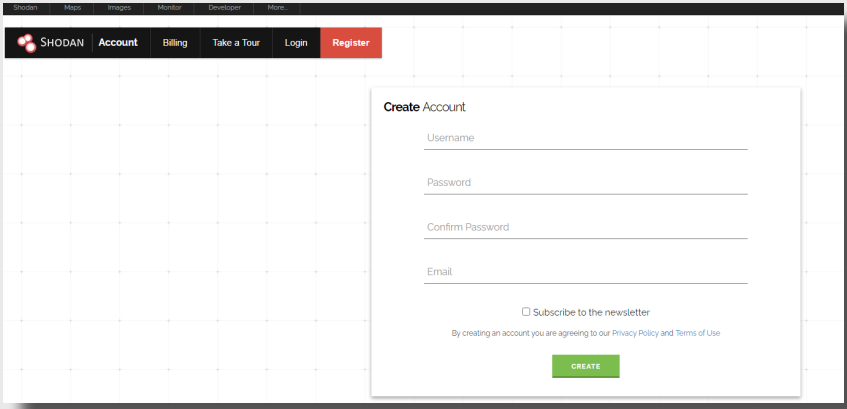
「Shodan、Censys」ともに、アカウント登録なし、無償の範囲では検索回数や閲覧範囲に制限がある場合があります。今回は、“ 無償のアカウント作成 “ までを実施し、「Shodan、Censys」を利用してみます。

なお、「Shodan、Censys」のアカウントを作成しない場合、制限により本稿および次号以降に記載の内容が実施できない場合があります。

2.1 Shodan のアカウント作成

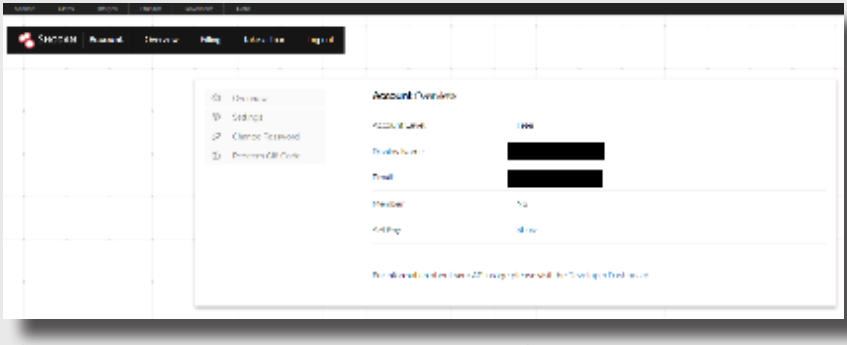
以下の URL よりアクセスします。
https://account.shodan.io/register

アカウント作成画面にアクセスしますので、所定の手順に沿ってアカウントを作成してください。



アカウント作成が完了しましたら以下の URL にアクセスします。
https://account.shodan.io/

Account Overview にて、登録したアカウント情報が表示されていることを確認してください。

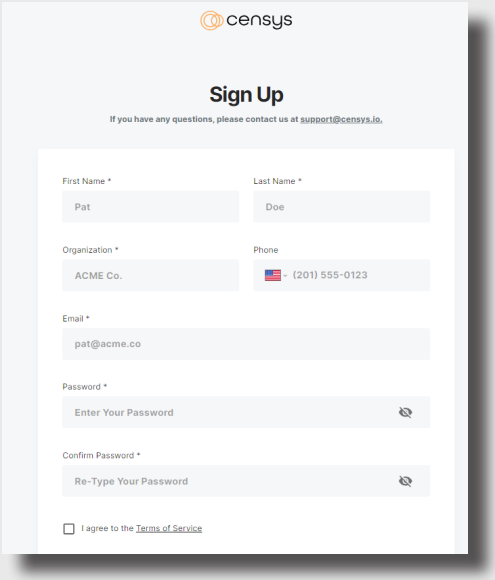


ログインがなされていない場合には、以下の URL よりログインを実施してください。
https://account.shodan.io/login

2.2 Censys のアカウント作成

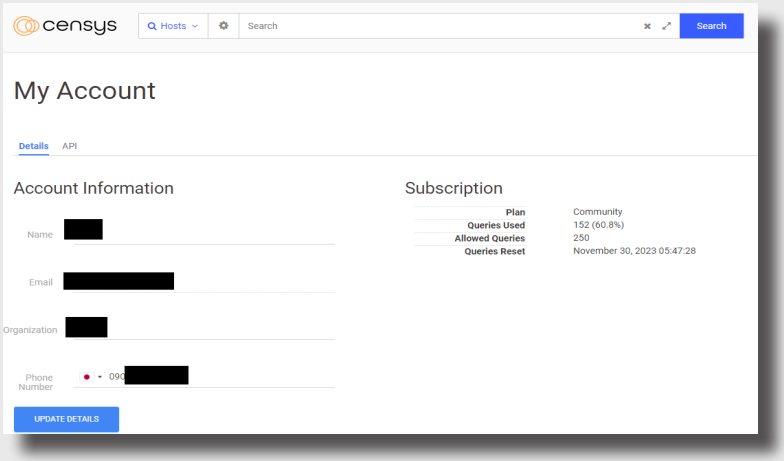
以下の URL よりアクセスします。
https://accounts.censys.io/register

アカウント作成画面にアクセスしますので、所定の手順に沿ってアカウントを作成してください。



アカウント作成が完了しましたら以下の URL にアクセスします。
https://search.censys.io/account

My Account にて、登録したアカウント情報が表示されていることを確認してください。

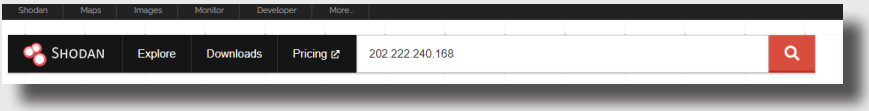


3. Shodan、Censys を用いた外部から見たサーバーの状況確認

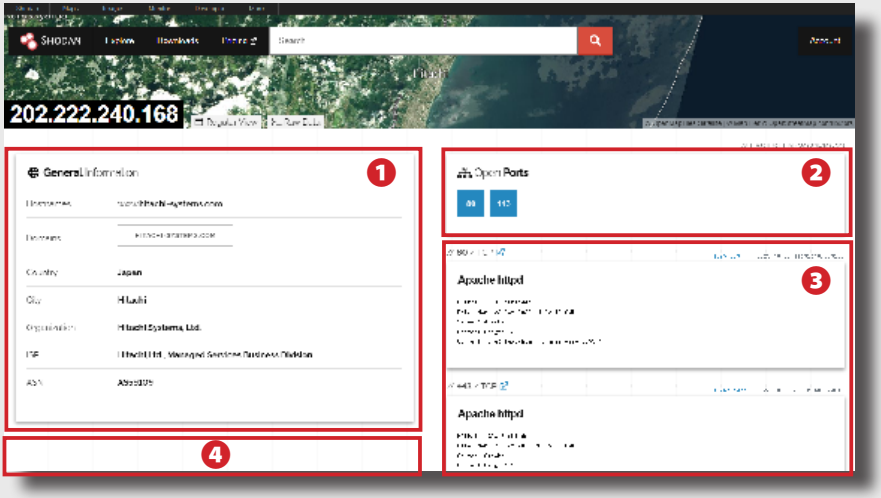
「Shodan, Censys」を用いて自身が管理するサーバーを例に外部から見たサーバーの状況を確認します。なお、本稿の画像や表示内容は執筆時点のものです。時間経過とともに、内容が変化する場合もありますので、注意してください。

3.1 IP アドレスでの検索（Shodan）

まず、IP アドレスを把握している、自身が管理するサーバーを確認します。
「Shodan」の検索欄に「202.222.240.168」を入力して検索します。この IP アドレスは、日立システムズの公開 Web サーバーの IP アドレスです。



検索を実行すると次の画面が表示※1されます。

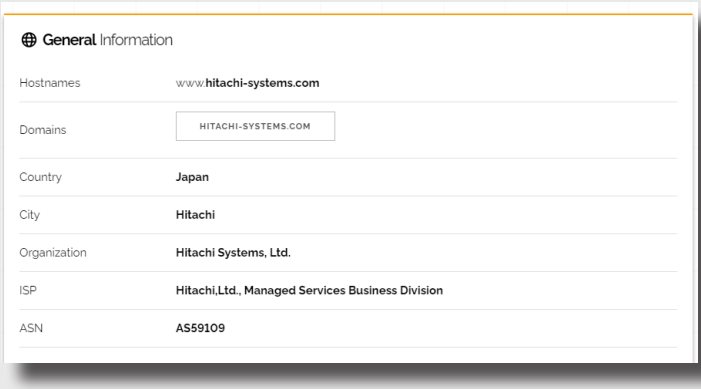


検索結果画面からは、大きく 3 つ情報が見て取れます。
❶ General Information、❷ Open Ports、❸ Port ごとのレスポンス詳細です。
それぞれについて、詳しく見ていきます。

※1 https://www.shodan.io/host/202.222.240.168

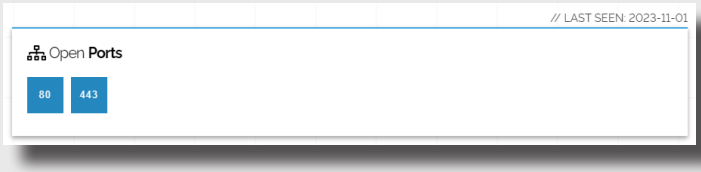
1. General Information

Whois で得られる情報など、当該サーバーに関する基本的な情報が表示されます。



2. Open Ports

当該サーバーで空いている（Listen）ポートのうち、外部からアクセス可能なものが表示されています。「1. 基礎知識編」にて Nmap を用いてネットワーク状況を確認したように、「Shodan」もまた、ポートスキャンなどの方法で定期的に情報を収集しています。

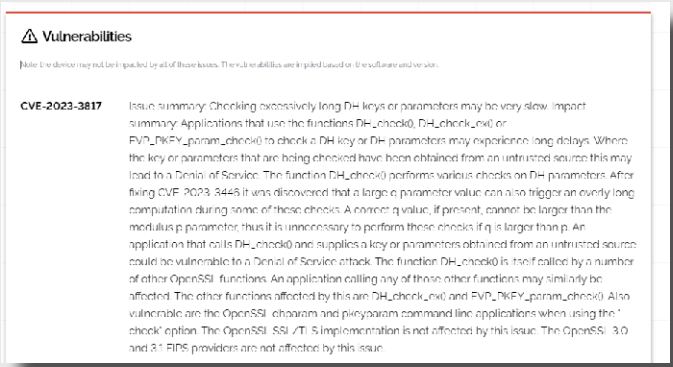


3. Port ごとのレスポンス詳細

「❷ Open Ports」で確認できる空いている（Listen）ポートのレスポンスの内容を表示しています。例えば、80 番ポートのレスポンス内容には、「Server：Apache」の記載があり、Apache HTTP サーバーが起動していることが伺えます。

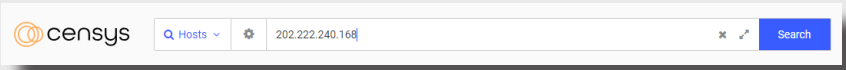
4. Vulnerabilities

「202.222.240.168」のサーバーにはぜい弱性情報が表示されていませんでした。しかし、管理しているサーバがぜい弱な場合（ぜい弱性が残存している場合）、次ページの図のような表記が❹の箇所に表示される場合があります。

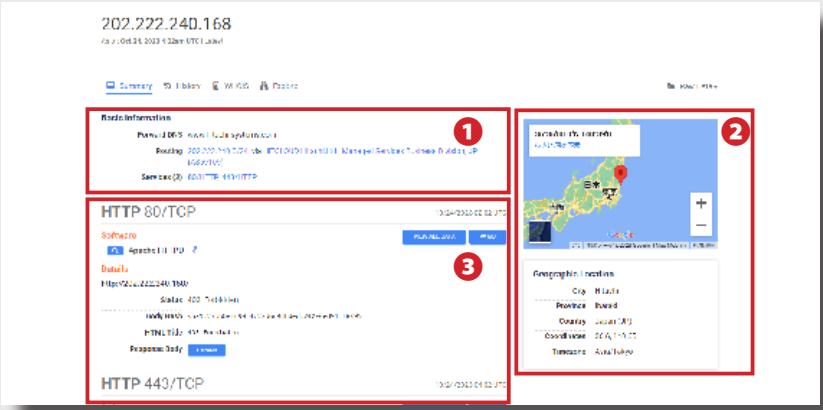


3.2 IP アドレスでの検索（Censys）

「Shodan」と同様に、「Censys」でも自身が管理するサーバーを確認します。
「Censys」の検索欄に「202.222.240.168」を入力して検索します。



検索を実行すると次の画面が表示※2されます。



検索結果画面からは、大きく３つ情報が見て取れます。
❶ Basic Information、❷ Geographic Location、❸ Port ごとのレスポンス詳細です。
それぞれについて、詳しく見ていきます。

1. Basic Information

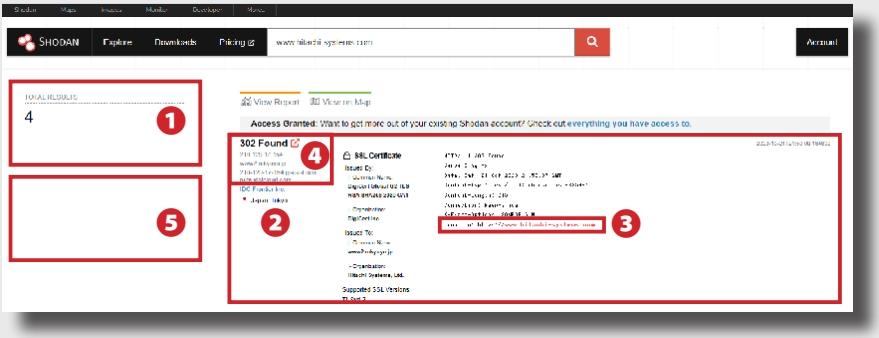
Whois で得られる情報など、当該サーバーに関する基本的な情報が表示されます。また、「Shodan」でいう「Open Ports」に該当する情報も「Service」項目として表示されています。当該サーバーで空いている（Listen）ポートの内、外部からアクセス可能であることを意味しています。

※ 2 https://search.censys.io/hosts/202.222.240.168

2. Geographic Location
IP アドレスから推測可能な、おおよその所在地を表示しています。「Shodan」にも同様の内容が記載されています。

3. Port ごとのレスポンス
「Shodan」と同様、空いている（Listen）ポートのレスポンスの内容を表示しています。「Shodan」のように、HTTP レスポンスの Server ヘッダーまでの表示はありませんが、「Apache HTTPD」であると判断していることが伺えます。

3.3 FQDN での検索（Shodan）
次は、「Shodan」にて、FQDN(Fully Qualified Domain Name：完全に指定されたドメイン名) で検索します。
検索クエリ「www.hitachi-systems.com」で検索します。検索結果※ 3 は下記のとおりです。

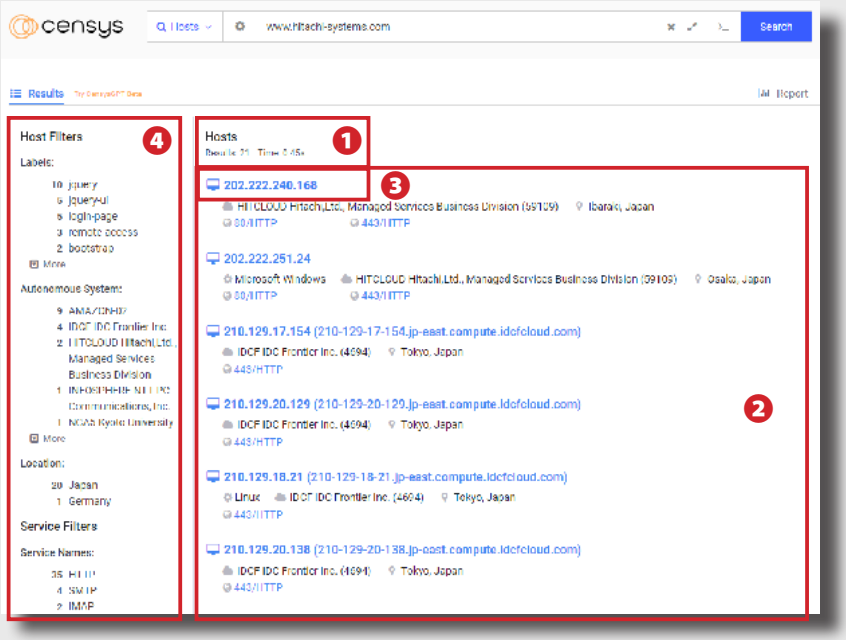


❶は、検索クエリ「www.hitachi-systems.com」で検索した結果のサーバー台数で、今回は 4 台あることがわかります。
❷がそれぞれのサーバーの状況を表します。
❸の赤文字が、「www.hitachi-systems.com」にマッチしたことを表しています。今回は、HTTP レスポンスの Location ヘッダーにマッチしています。302 Found は、リダイレクトステータスのレスポンスコードとなりますので、当該サーバーにアクセスすると、「www.hitachi-systems.com」にリダイレクトされる形になり、いわゆる、hostname にマッチしているわけではない点に注意が必要です。
本稿執筆時点で検索にマッチした 4 件は全て同じで、「www.hitachi-systems.com」の実サーバーは検索結果に表示されていないことがわかります。検索結果に表示されたサーバーの詳細は、❹のタイトル（例示では「302 Found」）をクリックすることで、前項の 3.1 で確認した形式で確認することができます。
なお、検索結果によっては、❺の位置に、次ページの図のようにサマリ情報が表示される場合があります。それぞれの、項目を選択することで、絞り込みを実施することができます（詳細は次号で解説する予定です）。

※ 3 https://www.shodan.io/search?query=www.hitachi-systems.com

3.4 FQDN での検索（Censys）

「Shodan」と同様に、「Censys」でも FQDN で検索します。
検索クエリ「www.hitachi-systems.com」で検索します。検索結果※4 は下記のとおりです。



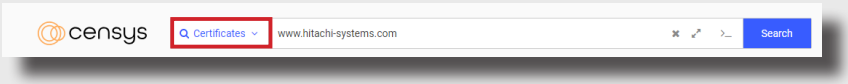
❶は、検索クエリ「www.hitachi-systems.com」で検索した結果のサーバー台数で、今回は 21 台あることがわかります（本稿執筆時点）。❷がそれぞれのサーバーの状況を表します。

https://search.censys.io/search?resource=hosts&sort=RELEVANCE&per_page=25&virtual_hosts=EXCLUDE&q=www.hitachi-systems.com

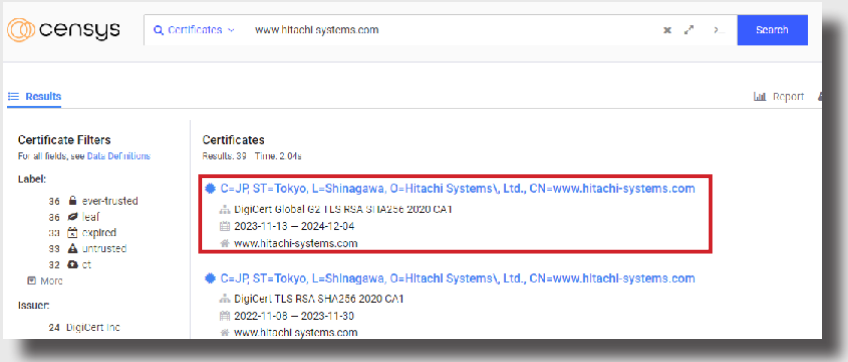
「Censys」では、「Shodan」と異なり、どの部分で検索クエリとマッチしたのかはわからない仕組みです。検索結果の最上段に「www.hitachi-systems.com」の IP アドレス「202.222.240.168」が表示されていることがわかります。
詳細は、❸のタイトル「202.222.240.168」をクリックすることで、前項の 3.2 で確認した形式で確認することができます。❹は、サマリ情報が表示される場合があります。それぞれの項目を選択することで、絞り込みを実施することができます（詳細は次号で解説する予定です）。

3.5 証明書の検索（Censys）

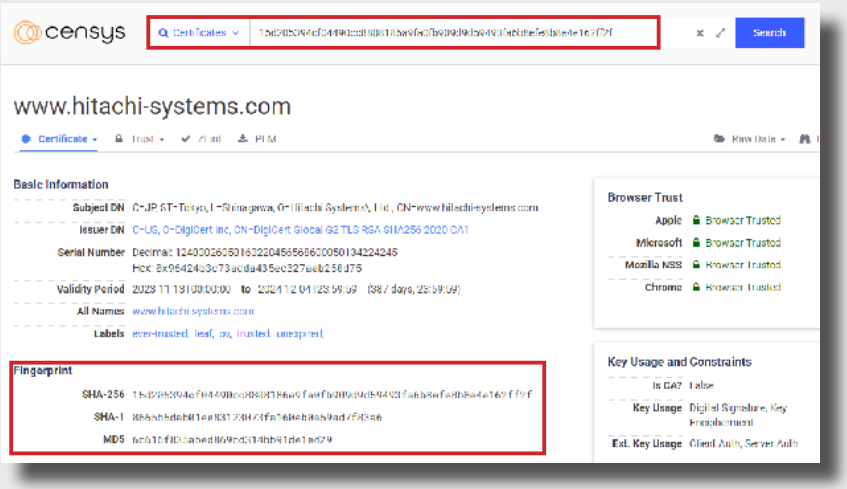
下図のように、検索対象を「Certificates」とすることで、証明書を対象に検索することが可能です。



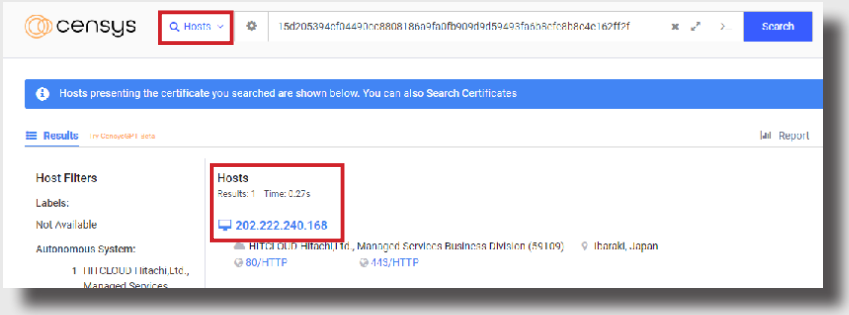
この例では、CN（Common Name）にマッチングしていると考えられます。



タイトル行をクリックすると下図のように証明書の詳細を確認することができます。



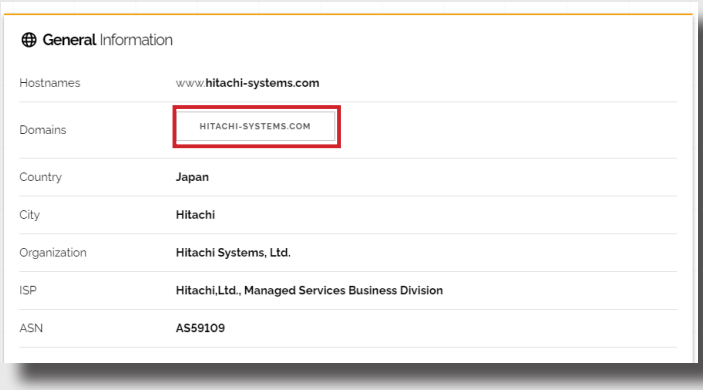
「Censys」では証明書を、Fingerprint（母印や指紋という意味で、自己署名証明書のデータから計算される数値）で管理していると考えられます。検索欄にも Fingerprint が自動で入力されていることがわかります。この Fingerprint を用いて、機器を検索します。
検索対象を「Host」に変更することで、当該機器を一意に特定することができました。



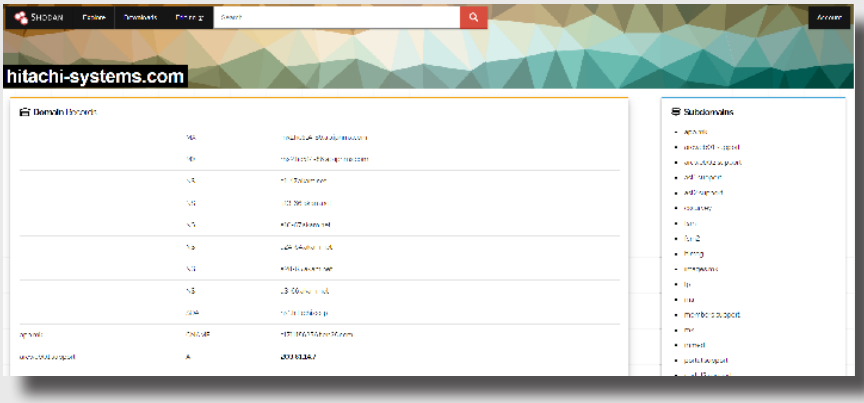
3.6 サブドメインの検索（Shodan）

今一度、以下の URL にアクセスします。
https://www.shodan.io/host/202.222.240.168

次に「General Information」内の Domains の項をクリックします。



遷移先のページ内においては、「hitachi-systems.com」に関するドメインのレコード一覧、サブドメインの一覧が表示されます（次ページ図）。



Shodan が把握できるドメイン情報のみと考えられますが、攻撃者にとっては、攻撃対象選定において、有用な情報となる可能性があります。無駄なドメインやサーバーが存在しないか確認することをお勧めします。

4. おわりに

今回はここまでとなります。「2. 所有サーバー確認編」では、自身が管理しているサーバーの「Shodan、Censys」での確認方法、「Shodan、Censys」での見え方を確認しました。

攻撃者による攻撃ポイント（Attack Surface）がないかなどを確認する際に利用します。

次回からは「3. サービス探索編」となります。「Shodan、Censys」といった IoT 検索エンジンを用いて、探索したいサービスが稼働しているサーバーを探索します。自組織で管理できていないサーバーを探索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.57

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