HITACHI
Inspire the Next

Hitachi Systems Security Journal

VOL.59

株式会社 日立システムズ

Human*IT

Hitachi Systems security Journal VOL.59

TABLE OF CONTENTS

CODE BLUE 2023 学生スピーカー
Web セキュリティと認証・認可を研究し、オープンソースツールを開発
湯浅 潤樹 インタビュー …… 3

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 2024.03 …… 8

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！ 4. サーバー探索編 …… 9

●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

CODE BLUE 2023 学生スピーカー

Web セキュリティと認証・認可を研究し、オープンソースツールを開発

湯浅 潤樹 インタビュー

取材・文 = 吉澤亨史／編集 = 斉藤健一

今回、話を伺う湯浅潤樹氏は、CODE BLUE 2023 での学生スピーカーの一人である。
OpenID Connect のテストケースを柔軟かつ現実に即したシナリオで記述できるツール（OSBT: OpenID Connect Scenario-Based Tester）を開発、GitHub 上で公開し、これまでは手動によるテストに頼っていた分野に利便性をもたらすとして広く社会に貢献、CODE BLUE 2023 会場でも注目を集めていた。
インタビューでは、OAuth や OpenID Connect などの ID 連携プロトコルとその実装を対象としたセキュリティを研究するにいたった経緯や現在の活動などについて話を伺う。

文系学部から情報系大学院に進学した異色の経歴

吉澤（以下 K）：湯浅さんは NAIST（奈良先端科学技術大学院大学）に在籍しつつ、プライバシーやセキュリティのソリューションを提供する IT 企業でインターンをされていたそうですが、現在はどのような活動をされているのでしょうか。

湯浅（以下 Y）：2022 年から NAIST の情報科学領域に在籍しています。学部生時代は、名古屋大学の経済学部に在籍していました。NAIST では、OAuth や OpenID Connect などの ID 連携プロトコルとその実装を対象としたセキュリティの研究を行なっています。

K インターンではどのような就業体験をされていたのでしょうか。

Y インターン先の企業には、学部 1 年生の時から修士 1 年生までの間、お世話になりました。この間、Web の開発や運用に関する DevOps 関連業務に携わっていました。

K NAIST を選んだ経緯ついて教えてください。

Y 学部生のときには経済学を専攻していましたが、CTF をはじめとするセキュリティに関心を持つようになり、大学院ではセキュリティの研究をしたいと思うようになりました。そこで、セキュリティの研究室を探していたところ、NAIST のサイバーレジリエンス構成学研究室を見つけて、見学に行くことにしました。

K 見学はいかがでしたか。

Y 見学では「自分の好きなことを研究テーマにできる」という説明を受け、自分のスタイルに合っていると感じ、受験を決めました。研究室の他の学生たちも、それぞれが興味のあることを研究

湯浅 潤樹（ゆあさ・じゅんき）
奈良先端科学技術大学院大学（NAIST）情報科学領域 修士課程在籍（2024 年 1 月の取材時点）。Web セキュリティと ID（OAuth、OpenID Connect）を研究し、CODE BLUE 2023 では OSBT: OpenID Connect Scenario-Based Tester を発表。SECCON Beginners 運営メンバー。

テーマに据えていて、とても興味深いと感じました。また、研究室にはコアタイムがないことも魅力でした。

K ちなみに NAIST でレジリエンスというと、門林先生のところですか。

Y はい、門林先生です。

K 門林先生には 2008 年にお目にかかったことがあるのですが、その頃から「レジリエンス」という言葉を使われていました。当時は説明しないと通用しなかったのですが、最近は一般的な言葉になりましたね。もともと門林先生をご存じだったのですか。

Y いいえ、そうではありません。研究室を探す中で偶然にお会いした形です。第一印象は厳格で怖そうなイメージでしたが、実際にお話してみると、とても気さくで優しい方で、少しギャップがありました。

ブロックチェーンへの興味が高じてインターンを開始

K インターン先 IT 企業のブログで湯浅さんのインタビュー記事が公開されているのを拝読しました。本誌読者のために改めてこの企業を選んだ理由を教えて下さい。

Y インターンを考えたのは、プログラミングなどを始めた学部 1 年生の頃で、ブロックチェーンの技術にも関心がありました。当時は名古屋に住んでいましたから「ブロックチェーン + 名古屋」で検索したところ、ヒットしたのがこの企業だったわけです。

K 検索結果以外の理由もあったのでしょうか。

Y この企業は当時、私が在学する名古屋大学の学生が社長を務められていたので、一度お目にかかりたいと DM を送ったのです。実際に話をさせていただいた印象も良く、インターンをお願いしたところ、快諾していただきました。高校生までは徳島に住んでおり、自分の周囲に起業した方はいませんでした。この社長は、自分が今まで出会ったことのないスゴイと思える方でしたので、是非とも一緒に働いてみたいと思ったのです。

K このインタビューでは、湯浅さん自身が時間の使い方を工夫したとおっしゃっていました。特に作業の効率化がポイントだったと思いますが、実際にどのように工夫されたのでしょうか。

Y 学業とインターンの両方において、重要度と緊急度に基づいてタスクの優先順位付けを行なうこと、そして毎日のタイムスケジュールに基づいてタスクを実行することを徹底しました。これにより、例えばバグ取りやコードの改善といった優先度の低いことに長く時間を費やすことがなくなりました。

K それでもなかなか時間どおりにいかないこともあると思うのですが、そういったときはどう工夫されたのでしょうか。

Y 例えばバグシューティングなど、時間どおりには進まない作業もあります。まずは決めた時間だけ集中して、それでも終わらないときは一度寝かして、また日を改めて作業すると、意外とすべて解決することもあります。ダラダラとやり続けないことが大事だと思います。

K 話はそれますが、湯浅さんご自身は例えばセキュリティキャンプや SecHack365 などに参加した経験はあるのでしょうか。

Y セキュリティキャンプは、22 歳以上向けのネクストキャンプに、2022 年に参加しました。2023 年にはチューターとして全国大会に参加しています。SecHack は 2021 年度に参加しました。

K やはりそうでしたか。湯浅さんの時間の使い方のお話を伺っていると、SecHack365 で行なわれる「習慣化への取り組み」を実践されているように思えたので質問させていただきました。実際に役立っているようですね。

Y はい。SecHack365 ではマンダラートという正方形のマス目の中に目標やテーマを書き込んでアイデアなどを発展させる思考ツールも紹介されていました。SecHack365 修了後も、1 年単位で自分のやりたいこと、やるべきことなどをまとめたり、1 日単位のタイムスケジュールを作ったりするなどして、自分なりに継続しています。

プログラミングを始めたきっかけはホリエモン

K 前述のインタビューでは、高校生の頃からプログラミングを始めたということでしたが、プログラミングに興味を持ち、始めたきっかけは何だったのでしょうか。

Y 高校 2 年生の時に堀江貴文（ホリエモン）氏の本を読んだことがきっかけでプログラミングを知り、Progate というオンラインプログラミング学習サービスで遊んでみることから始めました。当時は、面白いと思う反面、難しさも感じました。その一方で、部活や受験勉強で時間がなかったので、本格的にプログラミングを始めたのは大学生になってからです。

K ゲームがきっかけという方は多いですが、ホリエモンの本というのはユニークですね。次に、セキュリティに携わることになったきっかけを教えてください。

Y きっかけは、インターンの企業でブロックチェーンなどを扱う開発業務をしていた時のことです。暗号資産の秘密鍵を GitHub に公開するという大失態をしてしまい、そのウォレットの中の暗号資産をすべて盗まれてしまいました。この経験を通じて、世の中には悪いことを考える人がいるということを知り、セキュリティに興味を持つようになったのです。

K 実体験に根ざしているのですね。ちなみに、盗まれた暗号資産は、どれくらいの額だったのですか。

Y 円換算で当時なら 5000 円ほど、現在なら 10 万円くらいですね。

K 惜しいお金をなくしてしまったわけですね。他の要因などもありますか？

Y 学部時代にゲーム理論とセキュリティに関するテーマで卒業論文を書いたことが、セキュリティ研究者としてのキャリアの始まりでした。当時、経済学部で興味を持って学んでいたゲーム理論と、同じく CTF などを通じて興味を持っていたセキュリティを組み合わせた研究ができるのではないかという、シンプルな疑問から研究を始めました。また、当時はセキュリティ人材育成プログラムである SecHack365 でもゲーム理論とセキュリティに関するテーマで作品作りを行ないました。

K どのような作品なのか、その概要を簡単に教えていただけますか。

Y 組織の内部不正を未然に防ぐことを目的に、組織のメンバーごとに個別対応できるソリューションで、実装にはゲーム理論モデルが用いられています。メンバーの情報や収集されたサーバーの利用ログなどから、メンバーが内部犯行者である確率を推論します。管理者はその情報を元にメンバーそれぞれに対して「権限失効」「注意喚起」「何もしない」といった個別の対策を講じることができるのです。研究成果は ICSS（電子情報通信学会）研究会で発表も行なっています※ 2。

K なるほど。内部不正をゲーム理論で未然に防ぐというのは新規性が高いと思います。

Y 実装をより確実なものにするためには、技術面ばかりでなく、人間の意志決定や心理学的な要素にも着目していく必要があると考えています。

CODE BLUE で OAuth、OpenID Connect 実装のテストツールを発表

K 引き続きセキュリティ・コミュニティでの活動について伺いたいと思います。実際、どのような活動を行なっていますか。

Y CTF の活動です。大学には CTF チームやサークルがありませんでしたので、それを作るところから始めました。メンバーを X（旧 Twitter）で募集したり、セキュリティの研究室にメンバー募集のメールを送ったりしました。当初はなかなか集まりませんでした。ですがその後、CTF に強いプレイヤーが 4 名参加することとなり、SECCON CTF などに挑戦するようになりました。

K CODE BLUE 2023 で講演されましたが、登壇にいたるまでの経緯を教えてください。

Y OAuth、OpenID Connect 実装のテストツールである OSBT を開発している段階で、セキュリティの実務家の方々が集まるイベントで発表して、フィードバックをいただきたいと考えていま

※ 1　**シグナリングゲームによる内部不正モデルの提案と考察**
https://ken.ieice.org/ken/paper/20220307NCiS/

CODE BLUE の公式サイトでは湯浅氏の講演動画とプレゼンテーション資料が公開されている
https://archive.codeblue.jp/2023/result/?content=Junki_Yuasa

した。これには門林先生のアドバイスもありました。そのタイミングで、CODE BLUE と BlackHat の CFP（講演募集）があったので応募してみたのです。残念ながら BlackHat の方は選考に落ちてしまいましたが。

K CODE BLUE への参加ははじめてとのことでしたが、印象はいかがでしたか。

Y 自分が想像していたよりも大規模なイベントでした。著名なセキュリティ研究者の方々の発表を聴講できた貴重な機会となりました。また、セキュリティツールを開発する同年代の人たちと交流できたことも得がたい経験となりました。

K 実務家からのフィードバックはありましたか。

Y 発表することで、多くの実務家の方々から有益なフィードバックをいただけましたし、好印象を持っていただいたと思っています。ただし、ツールの出来については、さらなるブラッシュアップが必要だと感じています。改善して今度は BlackHat に参加したいですね。

K 他にも活動していることはありますか。

Y 大阪大学と NAIST の学生による合同 CTF チームである ONsen にも所属しています。ONsen はまだ強豪チームとは言えませんが、2023 年の SECCON 予選では国内 37 位の成績を収めており、今後の成長が見込まれるチームだと思っています。

K コミュニティ活動についてはいかがですか。

Y 現在、CTF 未経験者や初心者をサポートする SECCON Beginners の運営メンバーとしても活動しています。2023 年には、SECCON Beginners 福岡や SECCON 電脳会議などのイベントで CTF の Web 分野についての講義・演習を行ないました。SECCON Beginners CTF では、JWT や OAuth を題材とした問題を出題しています。

認証・認可における現状と課題 そして将来

K 湯浅さんが研究されている認証・認可の分野ついてお聞きしたいと思います。まずは OAuth などの認証に興味を持ったのは、やはり先ほどのブロックチェーンでの失敗が最初だったのですか。

Y 修士 1 年生の頃は Web 関連のぜい弱性診断を効率化するためのツール開発を軸として、研究テーマを練っていました。しかし、なかなか良いテーマが決まらない状況が続いていました。そこで、門林先生に「OAuth などを対象にしてみたら？」と助言をいただいたのが、認証・認可関連の研究を行なうきっかけとなりました。

K その時点で、OAuth に関する知識はあったのですか。

Y 実は、全く知らない状態でした。しかし、技術ブログやプロトコル仕様、論文を読み漁るうちに、OAuth や OpenID Connect に興味がわき始めました。これらは Web をベースとするプロトコルであるため、HTTP 上で動作するように作られています。

K Web に関連するぜい弱性の問題と近しいものがあるわけですね。

Y はい。HTTP ベースであるため、Web セキュリティにおいて扱われるオープンリダイレクトや CSRF などのぜい弱性が、そのまま実装上のぜい弱性として存在することがあります。独自のぜい弱性や攻撃手法についても Web セキュリティの知識を応用したものが多いため、実装上のぜい弱性を検討する上では Web セキュリティの知見をそのまま活かすことができました。

K これまでの湯浅さんの知見を生かすことができたということですね。

Y また、プロトコル仕様の基礎部分では暗号技術が用いられているため、暗号技術との関連性もあります。そして、OAuth や OpenID Connect のプロトコル自体が安全性についての要件を満たすかどうかを検証するために、形式検証という技術が用いられます。ただ、興味を持っている方はまだ少ない印象です。

K 今、特にサイバー攻撃のほとんどが認証情報を窃取してアカウントを乗っ取ったり、その認証情報を販売したり、不正送金に利用したりするなど、さまざまなことに悪用されています。こうした状況において、認証ではどのような解決策が中心になって模索されているのでしょうか。

Y 比較的ユーザビリティが高く安全な認証方式として、パスキーの導入が進んでいます。パスキーは従来のパスワードに基づく認証やワンタイムパスワード（OTP）とは異なり、指紋や PIN を用いてローカルでユーザー認証を行ないます。また、公開鍵暗号を利用することで、認証への古典的な攻撃手法であるフィッシング攻撃やパスワードスプレー攻撃への耐性があります。

K パスキーが注目されているのですね。将来的にはいかがですか。

Y 認証資格情報をクラウド経由で同期すれば、ユーザーの端末に関わらずパスキーによる認証を利用できることもメリットです。セキュリティ強化とユーザビリティ向上の観点からも注目されているので、拡張性のある技術が普及する傾向にあると考えられます。今後は、OAuth・OpenID Connect とパスキーがお互いの弱点を補完するためのコラボレーションが進んでいくと考えています。

将来は認証・認可の仕様策定にも携わっていきたい

K 今後取り組んでいきたいテーマがあれば教えてください。

Y 認証・認可基盤のぜい弱性検査をより効果的に行なうためのぜい弱性検査ツールが発展していく可能性が高いので、そこに取り組んでいきたいと考えています。認証・認可基盤はより複雑化していきますから、そのセキュリティテストにはより専門的な知識が要求されます。

K そこで、それを自動化するツールを開発していくということですね。

Y そのとおりです。ツールによる効果的なテストの自動実行が必要不可欠になると考えています。現状では認証・認可基盤をテストできる汎用的なツールが存在しないため、そうしたツールの開発は急務です。それを実現するツールの開発をはじめ仕様の策定などにも携わっていきたいですね。

K 今回はお忙しい中、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 2024.03

文＝日立システムズ

GPS のジャミング（妨害）とスプーフィング（詐称）について

【概要】：広く普及している GPS だが、衛星から送信される信号自体にセキュリティ対策は施されておらず、ジャミング（妨害）やスプーフィング（詐称）に対してぜい弱である。現在ウクライナなどで問題となっている事例を含めて現状と今後について概説する。

【内容】: GPS は全地球測位システム（Global Positioning System）の略であり、地球上の現在位置を測定する高度約 2 万 km の衛星を用いたシステムである。現在民間・軍事用航空機、船舶、自動車、ドローン、携帯電話など、幅広い分野で利用されている。また GPS は位置情報以外にも衛星に搭載された原子時計から時刻情報も提供しており、精度が高く低価格であることから産業用制御システムなどでは時刻同期に利用している。

GPS を利用していると突然現在位置が大きく変わり明らかに違う位置を示すことがある。これは信号を正常に受信できないことに由来する。人為的に信号を正常に受信できない状態にする方法として、GPS ジャミングと GPS スプーフィングがある。

GPS ジャミングとは、GPS 受信機の周辺にノイズ源や信号源が存在していると、その影響によって正常な受信が妨げられるというものである。近年では意図的に信号を妨害する GPS ジャマーも 1000 円程度から簡単に購入でき、違法ではあるが個人でも簡単に行なうことができる。

GPS スプーフィングとは、偽の無線信号で正当な GPS 衛星信号を打ち消して上書きすることである。衛星を介して送信される GPS 信号は非常に弱く、より強い無線送信機を使用すると不正な座標と情報を送信する。

GPS のジャミングやスプーフィングの最近の事例を紹介する。2022 年以降のウクライナ侵攻で行なわれている GPS ジャミングは、単純にミサイル誘導システムの妨害以外にウクライナの高電圧エネルギーサブシステムにも影響を与えている。この例では GPS 信号が妨害されると変電所内のシステムにおいて時刻同期が不可能になり、電力グリッドの状態を正確に把握できなくなる。変電所が物理的な攻撃を受けた場合に修理の遅延や断線などによりグリッド全体に発生した問題の原因究明に支障が発生するという。余談だが、ウクライナ支援を表明している米シスコシステムズは、水晶発振器を使用して GPS が利用できない場合でも正確な時刻を提供できる Ethernet スイッチ（100 万ドル相当分）を無償でウクライナに提供したと 2023 年 11 月に発表した。

他方、現在ロシアでは、ドローンがプーチン大統領に接近するのを防ぐため本物の GPS の 500 倍もの強度を持つスプーフィング信号を送信できる機器で、虚偽の位置データを送信し 1 万件近くの GPS スプーフィングを行なっていると言われている。

GPS のジャミングやスプーフィングの対策としては違法電波として通報し、総合通信局と警察に停波を依頼する方法がある。技術的には複数の他技術（レーダー測位、マップマッチングなど）を併用することが一般的であるが GPS 信号自体は妨害や詐称に対してぜい弱な状態にある。そのため GPS 信号に電子署名を付与しなりすましを防ぐ研究も行なわれている。例えば 2024 年 4 月から iPhone などでも GPS と併用できる日本版 GPS「みちびき」において電子署名付与の「信号認証サービス」の本運用が開始される。みちびきを利用することによってドローン運航の安全性向上が見込まれるため、開発の一要素として検討に値すると考える。

【情報源】 https://www.theregister.com/2023/11/22/cisco_modded_switch_ukraine/
https://qzss.go.jp/index.html
https://www2.jiia.or.jp/pdf/research/R01_Russia/07-koizumi.pdf

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！

4. サーバー探索編

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。Vol.56 より開始した第三部 「IoT 検索エンジン」では、「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ます。Shodan と Censys それぞれには以下のような特徴があり、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するなどして、リスクの軽減に活用可能です。

・Shodan：IoT などの情報を収集、検索可能なエンジンを提供するサービス。米 John Matherly 氏が 2009 年より開始。アカウント登録なしでも利用可能ですが、制限があります。無償アカウントを作ることで制限は回避されますが、検索回数や閲覧範囲に制限が残ります。

・Censys：Shodan と同様、IoT などの情報を収集、検索可能なエンジンを提供するサービス。ミシガン大学の研究者が 2015 年 10 月より開始。Shodan 同様、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ります。サーバー証明書を用いた検索に特徴があります。

「IoT 検索エンジン」は次の 4 回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 アドレスなど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。

「④サーバー探索編」では、「Shodan、Censys」を用いて、特定のぜい弱性を有する可能性のあるサーバーを確認します。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。また、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. Shodan、Censys を用いぜい弱なサーバーの探索

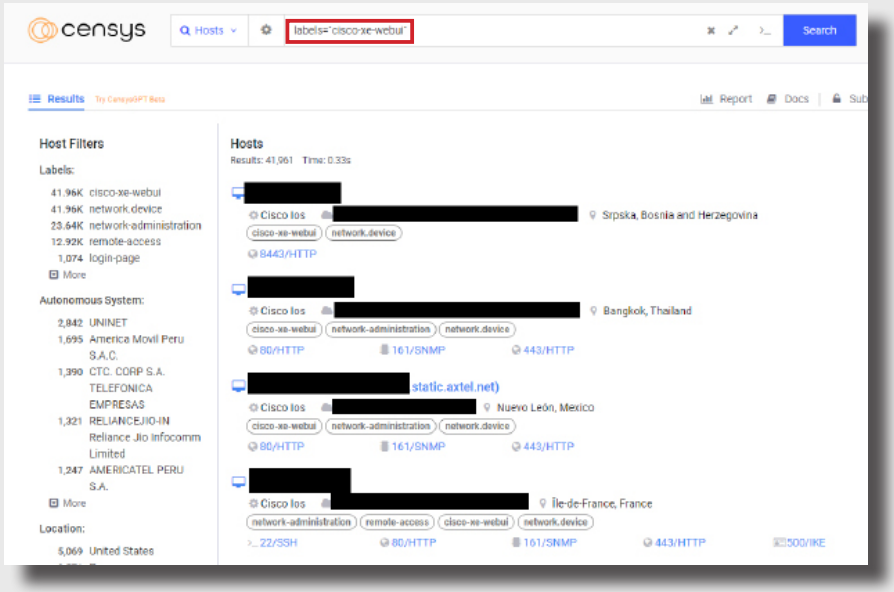
「Shodan、Censys」を用いて、特定のぜい弱性を有する可能性のあるサーバーを確認します。インターネット全体の状況を確認する際などに利用します。なお、本稿の画像、表示内容などは、執筆時点のものであり、時間経過とともに、内容が変化する可能性があることに注意してください。また、本稿を用いて確認されたサーバーが自組織が管理するものではない場合、スキャン行為を始めとする攻撃は絶対に行なわないようにしてください。

2.1 CVE-2023-20198 のぜい弱性を有する可能性がある機器の探索（Censys）

CVE-2023-20198 は、Cisco IOS XE ソフトウェアの Web UI 機能における権限昇格のぜい弱性です。本ぜい弱性が放置されている機器が外部からアクセス可能な状態で放置されている場合、悪意のある第三者により本ぜい弱性が悪用され、機密情報の漏えいなどの被害が発生する可能性があります。

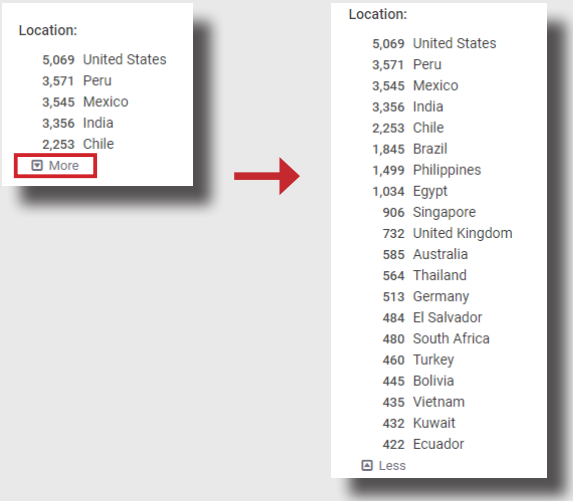
2023 年 10 月末 CVE-2023-20198 が公開されました。このような状況下、日本国内への影響を確認するため、CVE-2023-20198 を有する可能性機器の状況を確認します。

「Censys」を開き、「labels=`cisco-xe-webui`」で検索します。検索結果は次のとおりです。

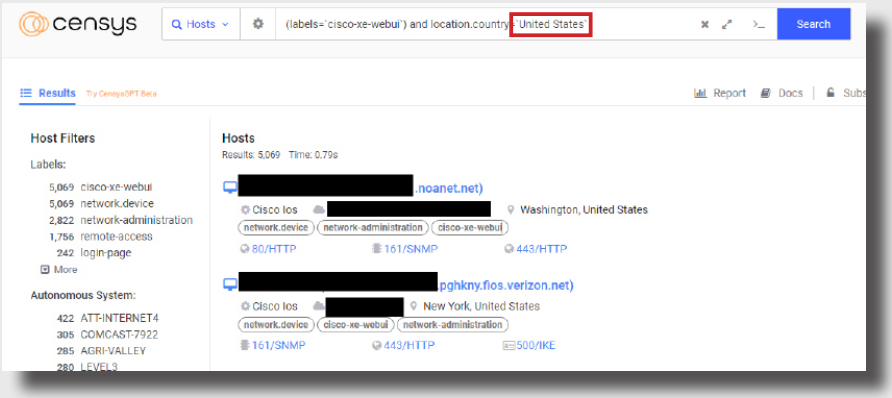


Cisco IOS XE ソフトウェアの Web UI 機能にアクセス可能な機器が、4 万台以上存在することが確認できました (本稿執筆時点)。

検索の結果を特定の国のものに限定する際には、「Location」から絞り込めます。「More」から、6 位以下の国を表示することができます（次ページ図）。

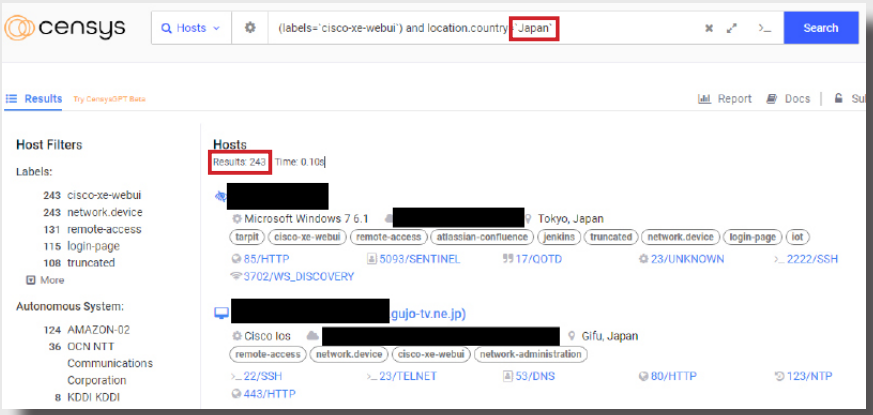


ただし、今回は日本が表示されませんでした。そこで、いったん、Cisco IOS XE ソフトウェアの Web UI 機能を有する機器のうち、ロケーションがアメリカとなっている機器で絞り込みます。「Location」から「United States」をクリックすると、検索クエリに「Location.country=` United States `」が自動的に追加され、「United States」に関する情報に絞り込まれます。



本来の目的は、日本のサーバーに関する情報です。そのため、「United States」となっている検索クエリを、「Japan」に手動で変更し、検索します。

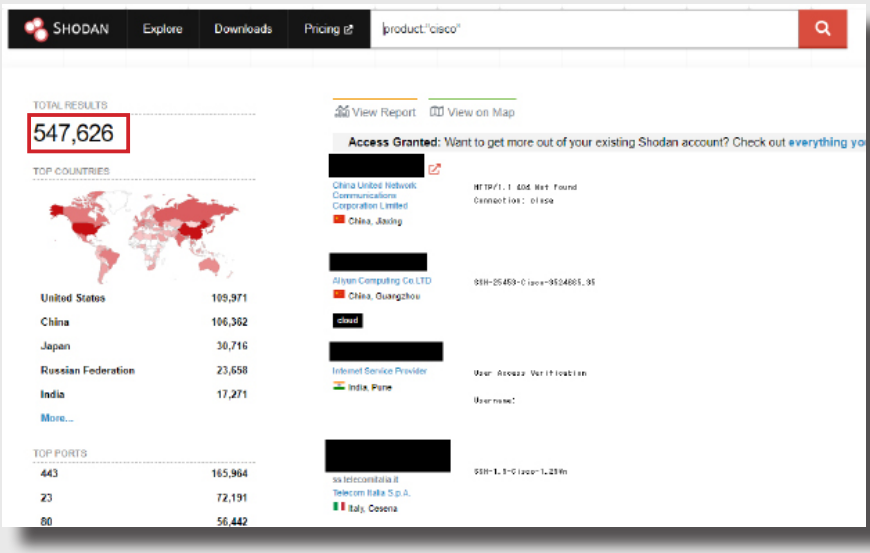
本稿執筆時点では、Cisco IOS XE ソフトウェアの Web UI 機能を有する機器のうち、ロケーションが日本となっているサーバー 243 台が、外部からのアクセスが可能な状態であることがわかります (本稿執筆時点・次ページ図)。



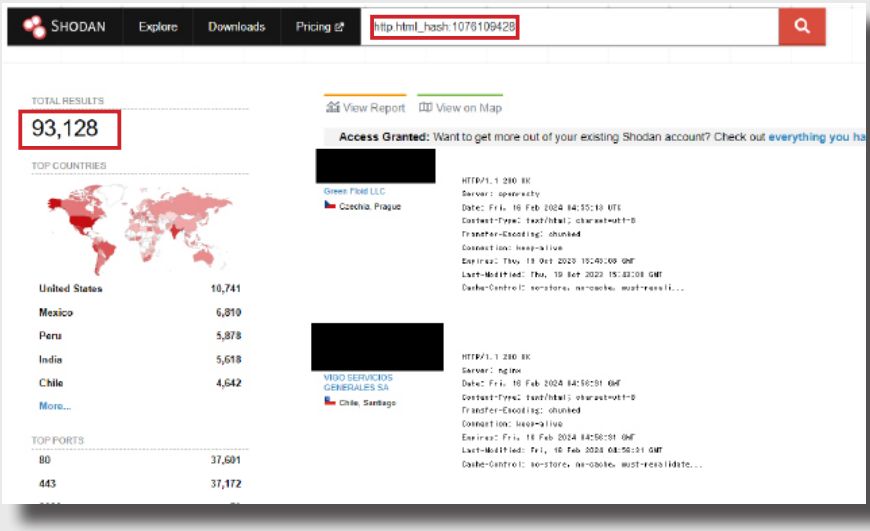
これはあくまでも、Cisco IOS XE ソフトウェアの Web UI 機能を有する機器の確認です。当初の目的である CVE-2023-20198 を有する機器であるかは、ＯＳのバージョン番号などの詳細を確認して判断する必要があります。

2.2 CVE-2023-20198 のぜい弱性を有する可能性がある機器の探索（Shodan）

「Censys」同様、Cisco IOS XE ソフトウェアの Web UI 機能を有する機器を確認します。「Shodan」を開き、「product:"cisco"」で検索します。検索結果は次のとおりです。

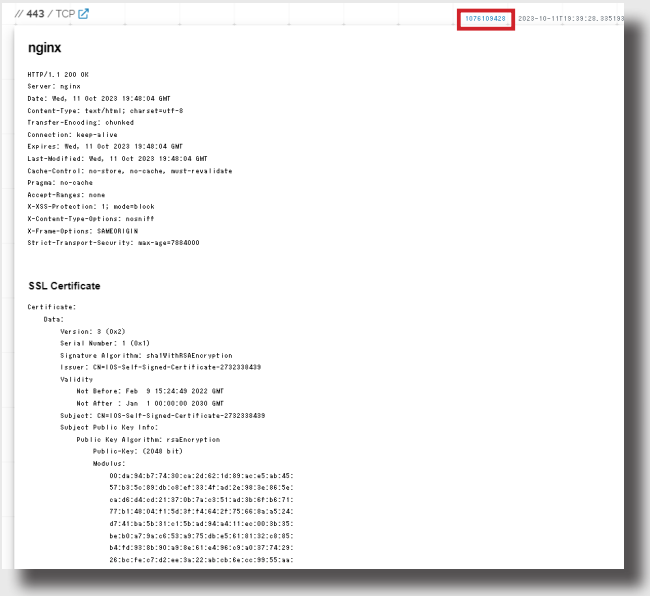


外部からのアクセスが可能な Cisco 社製の機器が、約 55 万台存在することが確認できました（本稿執筆時点）。ただし、この数は、Cisco 社製機器の数であり、CVE-2023-20198 を有する機器の数ではありません。そこで、「http.html_hash:1076109428」で検索します（次ページ図）。



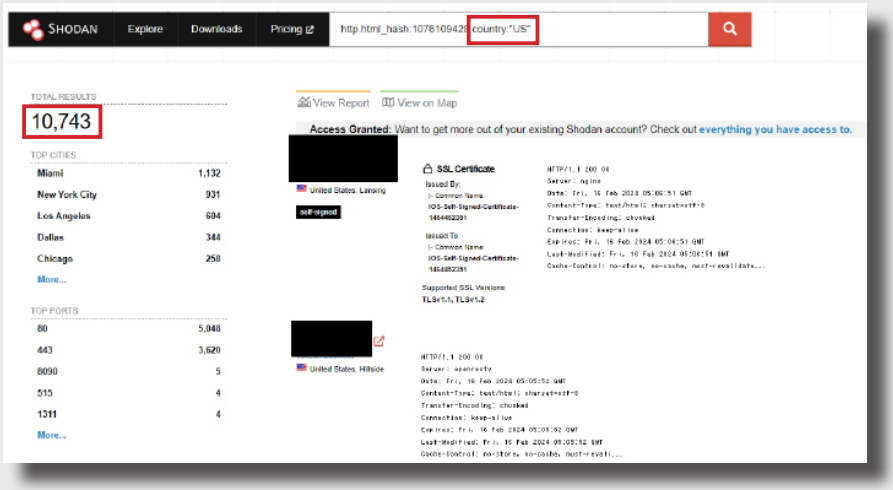
約 9 万台存在するという検索結果が表示されました（本稿執筆時点）。この検索「http.html_hash:1076109428」は、CVE-2023-20198 を有する機器の HTML のハッシュ値が同じである、という前提で、同じ HTML のハッシュを返答しているその他の機器を検索している形です。

「http.html_hash:1076109428」で検索ヒットした機器の 443 ポートの詳細をいくつか確認すると、右上に「1076109428」を確認することできるかと思います。これが、HTML のハッシュ値を表しています。このハッシュ値をクリックするとクエリに「http.html_hash:1076109428」が追加されます。同様の HTML ハッシュ値を有する機器を検索する際などに利用可能です。



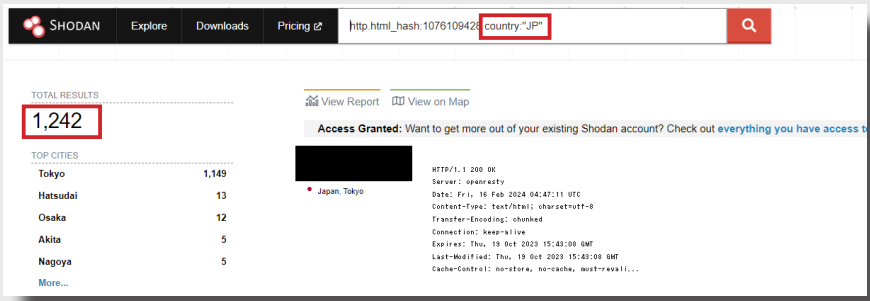
「Censys」同様、検索の結果を特定の国のものに限定する際には、「TOP COUNTRIES」から絞り込めます。「More...」から、6 位以下の国を表示することができます。

今回は、「Censys」同様、「TOP COUNTRIES」の「United States」をクリックし、Cisco IOS XE ソフトウェアの Web UI 機能を有する機器のうち、ロケーションがアメリカとなっているサーバーを確認します。



検索クエリに、「Country：“US”」が追加されていることが確認できます。

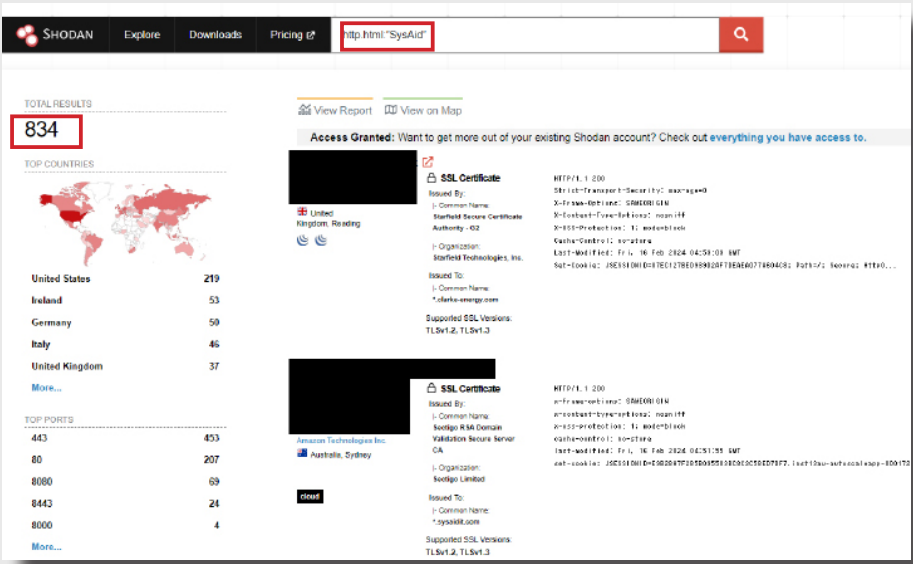
「Country：“US”」を「Country：“JP”」に変更します。CVE-2023-20198 を有する可能性があるサーバーのうち、ロケーションが日本となっているサーバーが 1242 台あることがわかります（本稿執筆時点・次ページ図）。



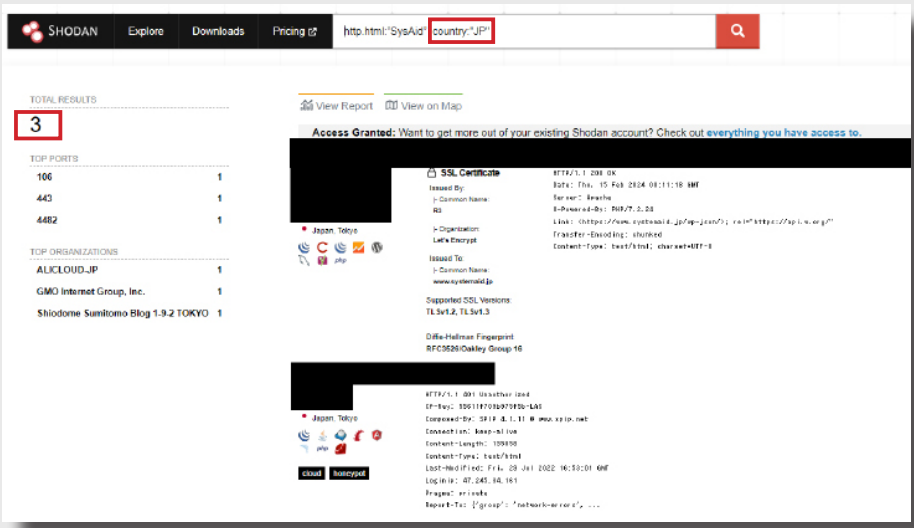
2.3 CVE-2023-47246 のぜい弱性を有する可能性がある機器の探索（Shodan）

CVE-2023-47246 は、SysAid Technologies 社製の IT 資産管理ツールである SysAid のパストラバーサルのぜい弱性です。本ぜい弱性が放置されているサーバーが外部からアクセス可能な状態で放置されている場合、悪意のある第三者により本ぜい弱性が悪用され、機密情報の漏洩等の被害が発生する可能性があります。

「Shodan」を開き、「http.html:"SysAid"」で検索します。検索結果は次のとおりです。

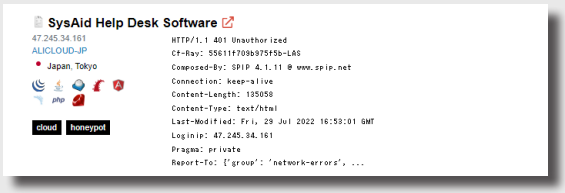


この検索では、HTML 内に「SysAid」という文字が含まれている機器が検索結果として表示されます。次は、SysAid のうち、ロケーションが日本となっている機器に絞り込みます。前項で試行した「country:"JP"」を検索クエリに追記すると、ロケーションが日本となっている機器を 3 台確認することができます（本稿執筆時点・次ページ図）。



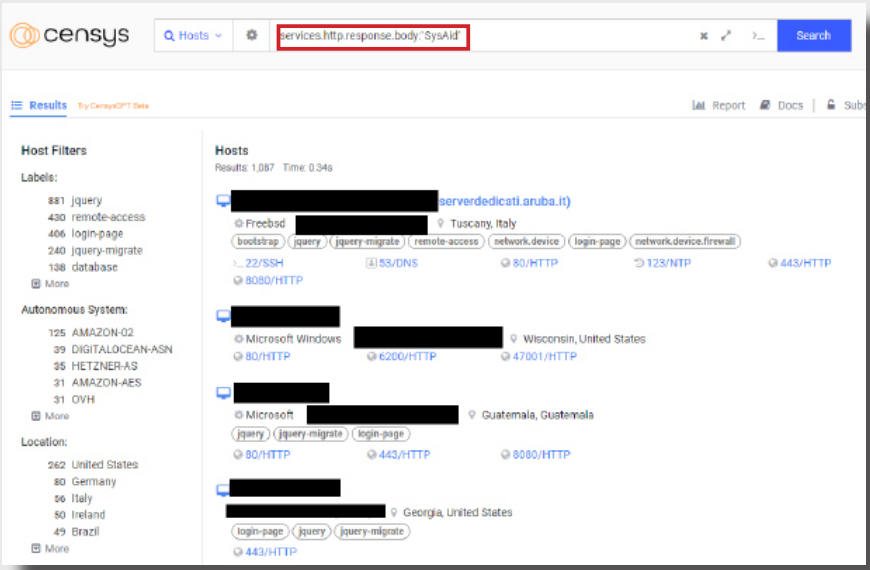
この検索結果は、あくまでも、HTML に「SysAid」という文字列が含まれるものです。現時点では、確実に「CVE-2023-47246」を有するものではありません。

機器それぞれの詳細を確認し、ぜい弱性の有無を判断する必要があります。

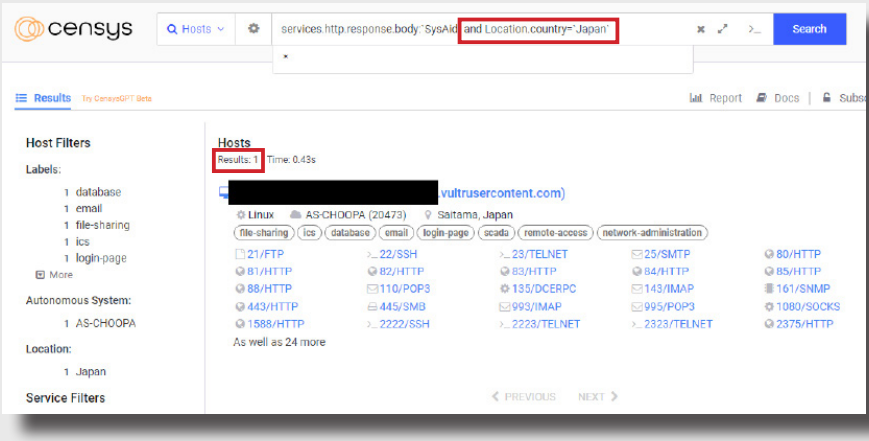


2.4 CVE-2023-47246 のぜい弱性を可能性がある機器の探索（Censys）

同ツールを「Censys」で検索してみます。「Censys」を開き、「services.http.response.body:`SysAid`」で検索します。結果は次のとおりです（次ページ・図）。



次に、日本の情報に絞るため、「and Location.country=`Japan`」を追記します。ロケーションが日本となっているサーバー 1 台が、外部からのアクセスが可能な状態であることがわかります（本稿執筆時点）。



こちらも、Shodan 同様、HTML に「SysAid」という文字列が含まれるものです。現時点では、確実に「CVE-2023-47246」を有するものでありません。機器それぞれの詳細を確認し、ぜい弱性の有無を判断する必要があります。

2.5 その他の検索方法

これまでに Shodan、Censys の基本的な検索手法を紹介してきました。これらの IoT 検索エンジンにはその他のフィルターなどが提供されていますので、事前に確認、試行しておくと有事の際に即座に対応可能となります。以下のドキュメントなどを確認、試行しておくことをお勧めします。

・Shodan Filter Reference
https://www.shodan.io/search/filters

・Censys Search
https://support.censys.io/hc/en-us/categories/4405770552724-Censys-Search

おわりに

今回はここまでとなります。「④サーバー探索編」では、「Shodan、Censys」といった IoT 検索エンジンを用いて、ぜい弱性を有する可能性のあるサーバーを探索しました。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などに利用したり、インターネット全体の状況を確認したり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.59

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