SHIELD Security Research Center

Hisys Security Journal

VOL.58

HITACHI
Inspire the Next

日立システムズ

Hisys Security Journal VOL.58

TABLE OF CONTENTS

●はじめに

本文書は、株式会社日立システムズ サイバーセキュリティリサーチセンタが運営するセキュリティ情報サイト、S.S.R.C.(Shield Security Research Center) の公開資料です。本サイトでは、本文書のバックナンバーをはじめ、S.S.R.C. によるリサーチ結果などを随時公開しています。

S.S.R.C. https://www.shield.ne.jp/ssrc/

八子 浩之 インタビュー

みずほフィナンシャルグループ みずほ銀行
サイバーセキュリティ統括部
サイバーレスポンスチーム 参事役

メガバンクのセキュリティを中心に JC3など幅広くサイバー犯罪対策に注力

「現在、不正送金被害はマルウェアからフィッシングへ完全に移行しています」と話す八子浩之氏は、株式会社ラックからみずほ銀行に移り約６年、一貫してセキュリティに取り組んでいる。また、ラック時代から JC3（一般財団法人日本サイバー犯罪対策センター）に参画している。今回、八子氏に不正送金やフィッシングの現状と対策への取り組みなどについてお話を伺った。

取材・文＝吉澤亨史／撮影・編集＝斉藤健一

セキュリティ企業から銀行へ

吉澤（以下 K）：最初に八子さんの経歴と現在のお仕事について教えてください。

八子（以下 Y）：前職はラックで、2001 年からセキュリティ関連のコンサルティング部門で CIRT の支援やガバナンスを中心に担当していました。そして 2017 年に現職であるみずほフィナンシャルグループのみずほ銀行へ転職しました。現在はサイバーセキュリティ統括部のサイバーレスポンスチームに所属し、CIRT 業務を中心に、インシデントレスポンス、不正送金、フィッシングなどに対応しています。また、最近では SOC（セキュリティ・オペレーションセンター）や脅威インテリジェンスなどにも関わるようになりました。

K セキュリティに関わるきっかけ、あるいは興味を持ったきっかけは何だったのでしょう。

Y 父親が警察官でしたので、警察官になりたいと思った時期もありました。ラックにはセキュリティ業務もあり、警察に近しいと思い興味を持ちました。

K 治安の維持はまさにセキュリティですし、2022 年にはサイバー警察局も設立されました。確かに近しくなっています。

Y 就職活動中に、知り合いからセキュリティは比較的新しい分野であると聞いていました。ですから、このタイミングでセキュリティ分野に携わることで、少しでもアドバンテージが得られるだろうと感じていました。また、「スニーカーズ」という映画にも影響を受けています。この映画は、セキュリティシステムをハッキングするために当時の最新機器を駆使するなどの頭脳戦が描かれており、強く印象に残りました。

K 本業以外の活動として、JC3 に長く参画していらっしゃいます。この経緯について教えてください。

Y ラック時代には金融関係のセキュリティにも関わっていました。サイバー犯罪の知見を高めるためにも外部の団体への参加を促されて、2014 年に JC3 へ参加しました。設立から間もない時期で、犯罪に関するデータの収集も分析も十分ではありませんでした。そこで、当時多発していたマルウェアによる不正送金のデータを分析するところから始めました。2016 年 6 月には JC3 として マルウェア（Gozi）の注意喚起を発表したり、脆弱性攻撃ツール「RIG-EK」の改ざんサイト対策を実施したりしました。他にもマルウェアに感染していないか確認できるチェックサイトの運用なども行ってきました。

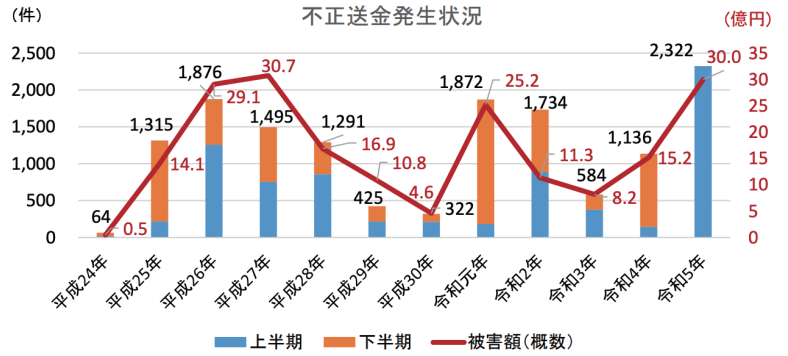
八子浩之（やこ・ひろゆき）
インシデント対応の CSIRT の担当や SOC の運用・企画、脅威インテリジェンスの担当など多岐の業務をこなす。インターネットバンキングの不正送金の対策業務、フィッシング対応も担当。

K ほぼ JC3 の設立から、現在まで活動を続けられているのですね。JC3 以外での活動はいかがですか。

Y 金融 ISAC にも積極的に参加しています。また、金融 ISAC とは別で金融機関同士でもさまざまな関係を築いています。他にも、フィッシング対策協議会をはじめ、複数の個別のプロジェクトへも参加しています。依頼を受けて講演することもあります。

不正送金の現状と傾向、世界との違いは

K 2023 年 8 月に警察庁・金融庁が発表した注意喚起によると、不正送金被害が 2012 年（平成 24 年）から 2014 年（平成 26 年）にかけて増加し、その後 2018 年（平成 30 年）までは減少、2022 年（令和 4 年）から再び急増しています（図 1）。この推移にはどのような要因があると考えられますか。



警察庁・金融庁「フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増について（注意喚起）」より。
https://www.npa.go.jp/bureau/cyber/pdf/20230808_press.pdf
【編注】今回のインタビューは 2023 年 12 月 19 日に行われた。同 25 日には警察庁が 2023 年 11 月末におけるデータを元に注意喚起を発表している。
https://www.npa.go.jp/bureau/cyber/pdf/20231225_press.pdf

図 1 インターネットバンキングに関連する不正送金の発生状況と被害額の推移

Y これを読み解くのはなかなか難しいと思いますが、2015 年からの盛り上がりは Zeus 系や Gozi 系といったマルウェアを中心とした不正送金だったと考えられます。

K マルウェア関係の盛り上がりとその終焉という流れですね。それで 2018 年（平成 30 年）ごろにほぼ底を打っています。

Y そこからフィッシングに移行していったと考えられます。2019 年（令和元年）はフィッシング元年といえるでしょう。フィッシング増加の要因の 1 つはその効率の良さです。フィッシングサイトの構築が簡単であり、かつ認証情報の窃取も容易です。このことに犯罪者が気づいたのだと思います。

K わざわざコストと時間をかけてマルウェアを開発し、ターゲットに感染させなくても、簡単に ID とパスワードを入手できますからね。

Y もう 1 つは、スマートフォンの普及です。スマートフォン経由の方が画面も小さいことからフィッシングサイトで認証情報を取りやすいということはあるかも知れません。もちろん、増加の要因には他にも複数あるとは思います。

K 不正送金に使われる送金先の傾向に変化はありますか。

Y 以前は個人名義が多く、外国人名が多かったのですが、ここ数年は暗号資産への振り込みが多くなっています。最近では株式会社や有限会社、合同会社などの法人口座宛てへの振り込みが確認され始めています。

K そうした変化が見られるのですね。

Y 届出されている電話番号に連絡しても通じないので、不正送金を目的としたペーパーカンパニーの可能性が高いようです。また、数年前から IP アドレスにレジデンシャルプロキシ IP（ISP が提供する IP アドレス）を使うケースが目立っています。一般の方とほぼ変わらない環境から来るので、端末の IP 情報などで検知することが難しい状態になっています。

K フィッシングから不正送金という流れは、世界的にはどうなのでしょう。この急増は日本だけの状況なのでしょうか。

Y 2023 年に、海外におけるフィッシングの状況をテーマに、JC3 の兄弟組織である NCFTA（National Cyber-Forensics & Training Alliance：サイバー脅威への対処を目的に発足した米国の非営利団体）に行ってきました。現地の方に聞くと、日本のような不正送金がほとんどないとのことでした。

K 海外ではどのような被害が多いのでしょうか。

Y BEC（ビジネスメール詐欺）の被害が多く、特に米国では被害に遭ってしまうと損害額が 1 兆円に及ぶこともあるそうです。また、Stealer 系のマルウェアが多くばらまかれていて、これにより認

証情報や Cookie などのセッション情報を窃取した上で、おそらく Microsoft 365 や Gmail といったメールを侵害していくと推測しています。
米国でも 3 ～ 4 年前はフィッシングが確認されたそうですが、それが徐々に特定の個人を標的としたスピアフィッシングにシフトしていったと聞いています。

K 日本のようなフィッシングが米国でほとんどないのは、どのような理由があると考えられますか。

Y そもそも米国の金融機関は即時振込ができないなど独特ですので、マルウェア全盛のころから傾向が異なっていたと思います。

K 日本のインターネットバンキングを狙う犯罪者グループは日本に精通している印象があります。

Y 日本の言語や商習慣はもちろん、政治や経済、国民の関心事など、さまざまなことに詳しいですね。他の国を狙うアクターとは異なり独特です。これがクレジットカードを狙うアクターになると、アンダーグラウンドのキットを使うケースが多いので、やはりアクター像は異なります。

不正送金は
マルウェアからフィッシングへ移行

K 現在は、不正送金に関するマルウェアはほとんど検知していない状況でしょうか。

Y 2019 年以降はほとんど検知しなくなりました。年に 1 ～ 2 回検知することはありますが、感染には至っていません。ただ、当行は一般的な傾向と少し異なる傾向があります。例えば、2019 年（令和元年）はフィッシング元年として不正送金被害が急増しましたが、当行ではあまり被害がありませんでした。

K フィッシング以外の攻撃による被害も少なかったのですか？

Y 被害件数が少ない状態で個別分析すると、フィッシングでもマルウェアでもない形で情報を窃取されたケースがあります。お客様に話を聞くと、クラウドサービスから認証情報が漏えいして、その ID とパスワードでログインされたとのことです。現在のようにフィッシングが増加すると埋もれてしまうかも知れませんが、こうしたケースも一定数あると考えられます。

K マルウェアも、不正送金を目的としたもの以外は活発です。

Y マルウェアについても整理が必要です。インターネットバンキングにアクセスする際には、PC とスマートフォンの 2 つの経路があります。PC に感染して、Web インジェクションを使って認証情報を盗むマルウェアは、ほぼ絶滅しています。一方、スマートフォンアプリでは Android を狙うマルウェアが増加しています。これらのマルウェアは感染して悪意のある SMS をばらまくタイプです。

K スマートフォンを狙う攻撃が増えた理由は何でしょう。

Y スマートフォンによるオンラインバンキングの利用増加です。各金融機関とも物理的な店舗を減らしてお客様をオンラインに誘導していますし、スマートフォンからの利用におけるユーザーエクスペリエンスの向上にも取り組んでいることなどが、背景にあると考えられます。

K 銀行をかたるフィッシングは一時期、その対象が地方銀行まで広がり、最近ではまたメガバンク系が中心になっています。これは犯罪者側の試行錯誤のようなものがあったのでしょうか。

Y 2019 年から 2020 年にかけてフィッシングの対象が地方銀行に移る動きがありました。2020 年から 2021 年は標的が銀行以外に移り、不正送金額は減少傾向、フィッシングが増加傾向だったのですが、2022 年 8 月ごろからまた銀行が標的になりました。当行も狙われまして、そこで犯罪者

には成功体験があったのだと思います。2022 年はまた、ワンタイムパスワード（OTP）を突破するパターンが確立されたように感じています。そのため、ユーザーの多いメガバンクを狙っていると思います。今後メガバンクの対策が進んでいけば、再び地方銀行に手を広げていくこともあり得るでしょう。

K フィッシング対策協議会の 10 月のレポート※1 では、検知数は過去最高を更新した一方で、分野別では金融系が大きく減少しています。これは何か要因があると思いますか？

Y 同時期の不正送金の被害額は、従来と桁が違うくらいに高い状態が続いていましたから、報告数との相関関係はあまりないという印象です。その時期はフリーの DNS サービスを使ったフィッシングサイトが非常に多く、また特定の銀行を狙ったフィッシングも多くありました。

K フィッシングサイトの数と被害件数も相関関係はないということですね。

Y ただ、フィッシングメールの数と被害件数は相関関係にあると思います。いわゆる「ばらまき型」の増加ですね。銀行のケースでは、2019 年に金融庁などの金融作業部会の FATF（Financial Action Task Force、金融活動作業部会）から、マネーロンダリング対策として取引時の口座の目的確認と本人確認を重視しなさいという勧告がありました。

K その注意喚起のメールがフィッシングに悪用されましたね。

Y その通りです。銀行はこれを受けて、お客様に対して「ここにアクセスして本人確認をしてください」というメールやハガキを送りましたが、その通知を悪用したフィッシングが増加しました。通知の文面をそっくり使ったため日本語に違和感もなく、慌ててアクセスして被害に遭う人が続出しました。それが成功したので、犯罪者は文面を少し変えて別の銀行をかたるフィッシングも増えました。これがここ 1 ～ 2 年の傾向ですね。

今後のフィッシング動向と対策への取り組み

K アンダーグラウンドでは Phishing as a Service が提供されており、犯罪初心者でも簡単にフィッシングができる環境になっていると言われています。フィッシングの今後の動向について、どのように考えていますか？

Y いろいろな方とお話する中で、クレジットカードを狙うフィッシングはキットが出回っていて、誰でも使えるといいます。銀行業界はクレジットカード業界とは異なりますが、攻撃的なアクターグループが金融機関を順々に狙っている状況が見えています。

K まだ大規模で同時並行的なフィッシングは発生していないのですね。

Y この状況が続く限り、フィッシングは減らないと思います。仮に減ったとしても、それはアクターグループが休んでいたり、他の業種を狙っていたりするためだと考えるのが自然です。アクターにとってはメールを送るだけですからコストはかかりませんし、逮捕される可能性も低い。それにもかかわらず数億円を儲けられるわけですから、やめることはないでしょう。

K フィッシング対策の手法の 1 つである OTP によってマルウェアを含めて攻撃が減少していました。しかし、OTP も突破されるようになってきていますから、認証の仕組みを考え直す必要があるということですね。現在でのフィッシング対策の状況についてお聞きしたいと思います。まず、八子さんが行っているフィッシング対策のための活動について教えてください。

Y 私も講演などでお話ししているのですが、フィッシング対策は「点」ではなく、キルチェーンといった「面」での対策が必要です。フィッシングサイトを止めるだけでなく、例えば犯罪者がお金にするところを止める。これにより被害が減り、最終的にフィッシングサイトがなくなるケースはあると思っています。

※1 フィッシング対策協議会「2023/10 フィッシング報告状況」
https://www.antiphishing.jp/report/monthly/202310.html

K フィッシングのライフサイクル全体を止めていくわけですね。

Y 入口となるフィッシングサイトの発見については、コミュニティやフィッシングハンターの方々、あるいは各金融機関、業界をまたいだ連携によって連絡をいただいています。また、テイクダウンの手法などを共有したり、場合によっては他行のフィッシングサイトを一緒に落としてみたりと、フィッシングの対応にできる限り力を入れています。

K JC3 が注力している取り組みですね。

Y 犯罪者が窃取した認証情報でログインして送金する部分について、その検知やモニタリングは金融機関同士で情報交換をしたり、停止方法などを共有したりしています。本当に被害が多くなったときには、サービスを一時的に絞り込むことも検討しています。ただ、そのためには通信キャリアやクレジットカード会社、あるいは警察などとも連携して取り組む必要があると考えています。

K 各社にセキュリティのエース級の人たちがいて、一緒に戦っているのに、被害やフィッシングサイトがなくならないことは悩ましいですね。

Y 産官学の連携も役割がそれぞれにあると思いますし、金融機関は対策、警察サイドは犯人を特定して捕まえるなどの役割もあります。これまで分断されていたところと積極的に情報共有ができるようになっていますので、これをさらに推し進めていきたいですね。

K ユーザー向けの注意喚起など、情報発信への取り組みについて教えてください。

Y ユーザー向けには、「不正送金被害疑似体験コンテンツ」を公開しています（図 2）。このコンテンツでは、スマートフォンの画面で不正送金被害の疑似体験ができるようになっています。JC3 が監修していて、ロゴが入っていることもポイントです。また、Web サイトの更新も頻繁に行っています。最新のフィッシングメールの文面を公開したり、サポート詐欺が確認されればすぐに載せたりするようにしています。

K 取り組みの効果はいかがですか？

Y「受信したメールの文面で検索したら、みずほ銀行のサイトがヒットして、同じ文面だったのでフィッシングメールだとわかった」と、X（旧 Twitter）に書き込んでいた方もいましたので、載せている意味はあると思っています。注意喚起も必要に応じて発表しています。先述の 2023 年 8 月の合同注意喚起は事情があって警察庁と同時に出せませんでしたが、今後も工夫しながら続けていきたいですね。

図 2 みずほ銀行「不正送金被害疑似体験コンテンツ」
https://www.mizuhobank.co.jp/crime/zero/simulation/index.html

不正送金の被害に遭わないために周知に取り組んでいく

K 今後の展望について、どうお考えですか。

Y まず、国として警察庁がサイバー特別捜査隊を作り、国際捜査を積極的に進めていくことは明るい材料ですので、期待したいと思います。ただ、現在主流となっているフィッシングを起点とした不正送金については、ID とパスワードに頼らない認証の仕組みに移行しない限り難しいと考えています。逆に言えば、そこは目指すべきところの 1 つだと思います。

K インタビュー冒頭の質問は警察庁の 2023 年上期の注意喚起をベースにしていますが、下期はどのような状況になりそうでしょうか。

Y かなり悪い状況になると思います。倍では収まらない、信じがたい数字になるでしょう[※2]。最近ではフィッシングの認知度も上がってきていて、増加していることも何となく理解している方も増えていると思います。それでもフィッシングメー

ルが届いてしまうと慌ててしまい、騙されてしまうのでしょう。

K 厳しい状況ですね。さまざまな媒体での注意喚起も有効だと思いますが、いかがでしょう。

Y はい。講演は今後も依頼いただければ行っていきます。また、テレビなどのメディアは影響力が大きいので、政府や警察庁でのフィッシング、不正送金に対する啓発 CM などの提言は今後も続けていきたいと思います。今回のインタビューも、セキュリティに詳しい方たちだけでなく一般の方にも広く読んでいただきたいと思います。少しでも被害に遭う方が減れば本望です。

K 本日はありがとうございました。

※ 2【編注】2023 年 12 月 25 日に警察庁が 11 月末におけるデータとともに注意喚起を発表している。それによると、被害件数は 5147 件（前年比約 4.5 倍）、被害額は約 80.1 億円（同 5.3 倍）となっている。

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

HISYS CSI（Cyber Security Intelligence）Watch 2024.02

文＝ SHIELD Security Research Center

各機関のフィッシング詐欺増加に関する報告の分析と考察

【概要】：フィッシング詐欺による被害が増加しており、金融庁と警察庁が連名で注意喚起を行った。フィッシング詐欺被害の増加傾向はコロナ禍以降で見られたが、2023 年は顕著に増加している。各機関から発行されたフィッシング詐欺に関する報告を分析し、機関ごとの報告の特色を考慮しつつ、フィッシング増加が確かであることを確認した。

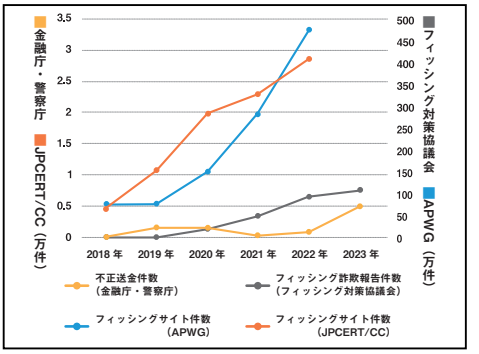


図　各機関のフィッシングに関する統計

【内容】：2023 年 12 月 25 日、メールや SMS などを利用したフィッシング詐欺と推測される手口によってインターネットバンキングの ID、パスワードなどが盗まれ、不正送金される被害が多発しているとして金融庁と警察庁が連名で注意喚起を行った。過去最も被害額が多かった 2015 年の被害額 30.7 億円に比べ、2023 年の被害額は約 2.6 倍の 80.1 億円と急増している。

本件をきっかけに、さまざまな機関から発行されているフィッシング詐欺に関する統計データを分析した。まず、フィッシング対策協議会の報告では 2020 年は 22 万件程度だったものが、2022 年には 96 万件と約 4 倍に増加している。ただ、この結果はフィッシング対策協議会宛に報告された件数であり、暗数も多い。次に APWG（Anti-Phishing Working Group）の報告でもコロナ禍後に増加傾向が見られる。この統計データは APWG の会員組織から報告されたフィッシングメール／サイト情報を集計したものであり、こちらも暗数は多いとみられるが、世界中のデータが集まるため大まかな世界情勢を確認しやすい。次に、JPCERT/CC の報告は、インシデントとして報告されたものの中からフィッシング詐欺をまとめたものであり、検知数はフィッシング対策協議会や APWG に比べ少ない。参考程度の情報となるが、2020 年は約 2 万件、2022 年は約 3 万件と、この報告でも増加傾向を見ることができた。なお、セキュリティベンダーもフィッシング詐欺の報告を行っており、例として、BBSS（BB ソフトサービス株式会社）の報告でも被害の増加が見て取れるが、他機関の報告数と差がある(2023 年 11 月、BBSS は 541 万件、フィッシング対策協議会は 1 万件）ため、総合的に判断する必要がある。

分析により、各機関の統計に差はあれど、総じてフィッシング詐欺の増加が確かであると判断できた。これは、PhaaS（Phishing as a Service）のようなフィッシング詐欺の実行を補助するサービスの充実や、生成 AI 活用による作業効率化によって、より多くの攻撃実施が可能となったことが原因であると推測される。被害を防ぐには不審な URL や広告はクリックしないよう心掛けることや、セキュリティ製品の導入が有効である。また、Google や Yahoo、Microsoft は DMARC への対応を表明しており、それぞれガイドラインを公開している。これに伴い認証基準を満たしていないメールは受信が拒否されるようになるが、これもフィッシング詐欺対策を含めたメールセキュリティの向上が背景にある。

［情報源］ https://www.fsa.go.jp/ordinary/internet-bank_2.html
https://apwg.org/trendsreports/
https://www.antiphishing.jp/report/monthly/
https://www.sagiwall.jp/report/

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！

3. サービス探索編

文＝ SHIELD Security Research Center

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脆弱性確認手法などを解説します。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などを探索したりし、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脆弱なサーバーを探索する際にも利用します。

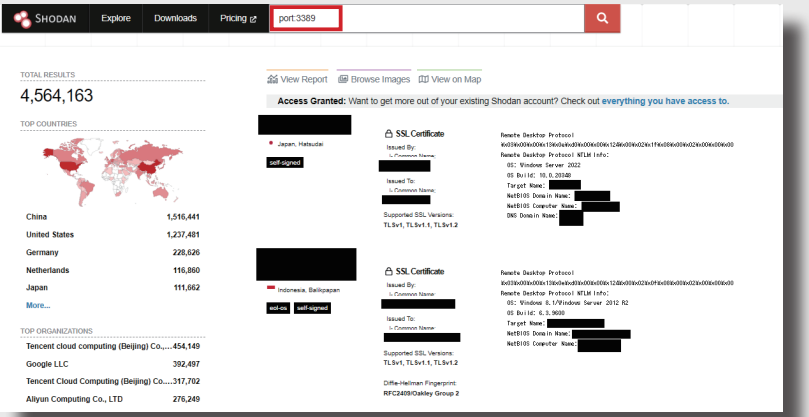
IoT 検索エンジンと呼ばれる「Shodan、Censys」ですが、インターネット上に公開されているサーバーなど、さまざまな情報を収集しており、検索・閲覧が可能なサービスです。
「③サービス探索編」では、「Shodan、Censys」を用いて、特定のサービスが稼働・公開されているサーバを確認します。
本稿の安全性には留意していますが、安全を保証するものではございません。
OA 端末で実施するのではなく、分離された回線内および機器を利用することを推奨いたします。

2. Shodan、Censys を用いた脆弱なサーバーの探索

「Shodan、Censys」を用いて、特定のサービスが稼働・公開されてい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。本稿の画像、表示内容などは、本稿執筆時点のものです。時間経過とともに、内容が異なる場合があることにご注意ください。なお、本稿を用いて確認されたサーバーへ、スキャンを始めとした攻撃は絶対に行わないようにしてください。

2.1 ポート番号による検索（Shodan）

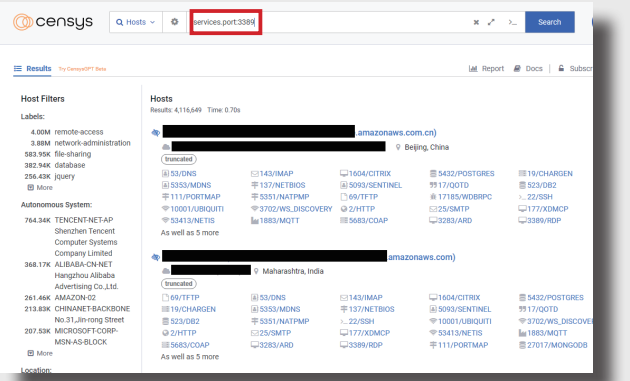
特定の Port が開いているサーバーを確認します。「Shodan」を開き、「port:3389」で検索します。検索結果は次の通りです。



3389 番ポートは、リモートデスクトップ接続に必要なポートです。「Shodan」からは、3389 番ポートが空いているサーバーが、400 万台以上存在することが確認できました（本稿執筆時点）。「Shodan」では、検索する際に「検索対象：キー」の形で検索します。

2.2 ポート番号による検索（Censys）

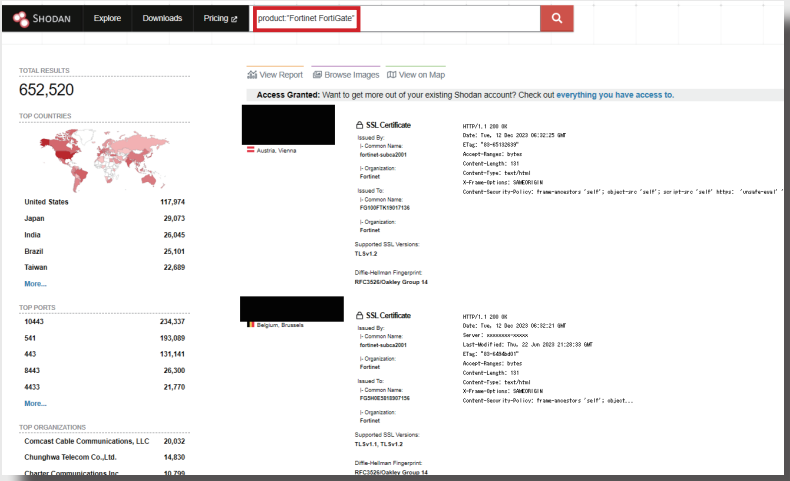
「Shodan」同様、特定の Port 番号が開いているサーバーを確認します。「Censys」を開き、「services.port:3389」で検索します。検索結果は次の通りです。



「Censys」からも、3389 番ポートが空いているサーバーが、400 万台以上存在することが確認できました（本稿執筆時点）。「Censys」でも、検索する際に「検索対象：キー」の形で検索しますが、検索対象の指定が異なり「.（ドット）」を用いて細かく指定します。

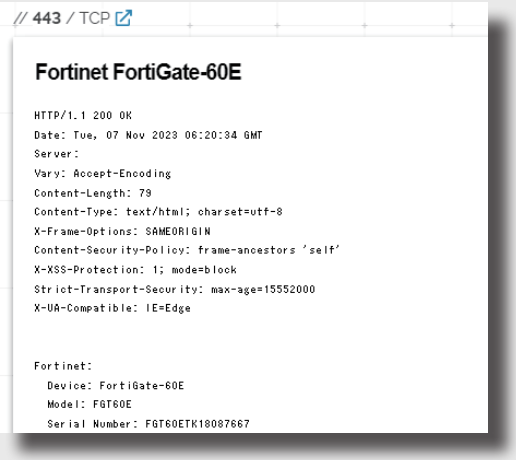
2.3 プロダクト（製品名）による検索（Shodan）

特定のプロダクトを確認します。「Shodan」を開き、「product:"Fortinet FortiGate"」で検索します。検索結果は次の通りです。



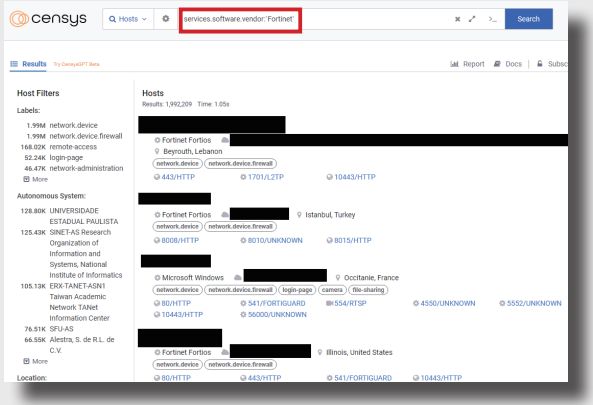
「Fortinet 社製 FortiGate」と認識されている機器が、約 65 万存在することが確認できました（本稿執筆時点）。

次に、各サーバーの詳細ページへ遷移します。以下の図のように製品の型番など詳細情報が閲覧できる場合があります。



2.4 プロダクト（製品名）による検索（Censys）

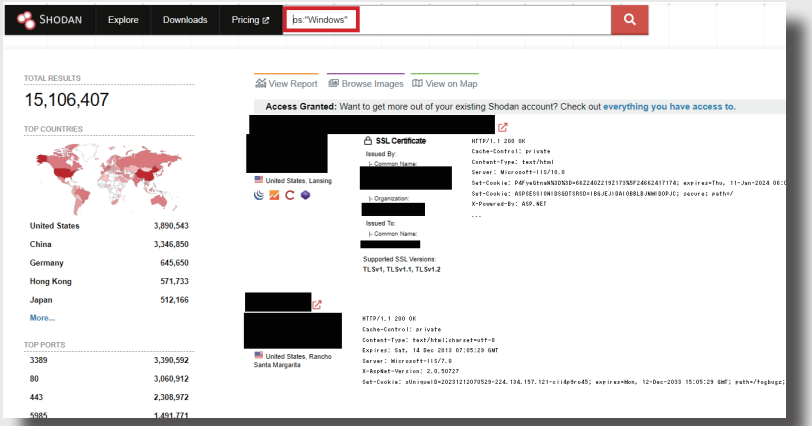
「Shodan」同様、特定のプロダクトを確認します。「Censys」を開き、「services.software.vendor:`Fortinet`」で検索します。検索結果は次の通りです。



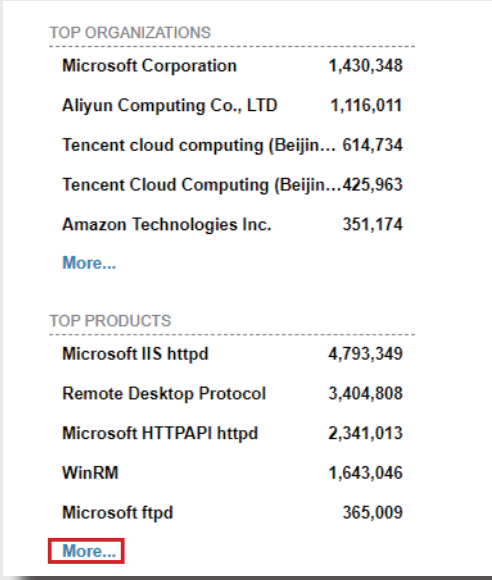
「Fortinet 社製」と認識されている機器が、約 200 万存在することが確認できました（本稿執筆時点）。

2.5 OS による検索（Shodan）

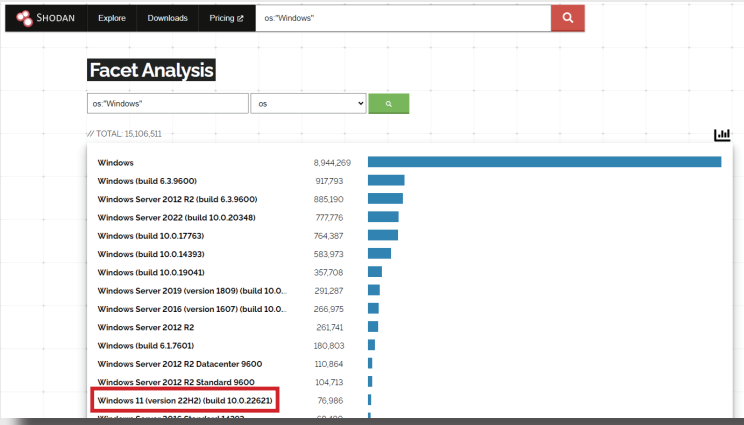
特定の OS の機器を確認します。「Shodan」を開き、「os:"Windows"」で検索します。検索結果は次の通りです。



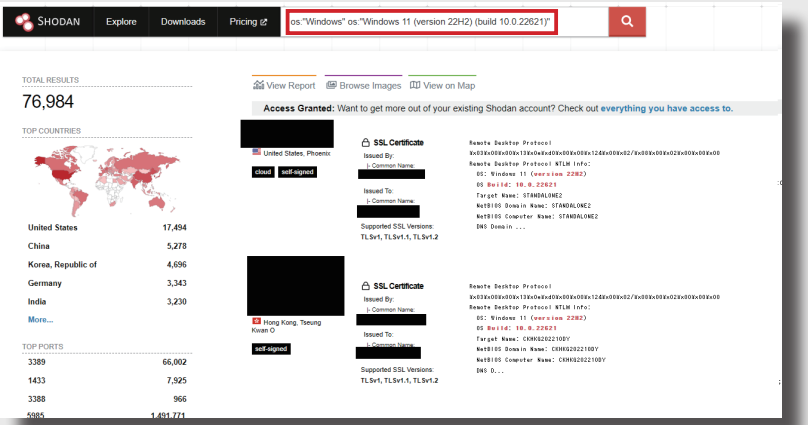
さらに詳細の OS の数を確認したい場合には、左側のサマリから絞り込むと便利です。「TOP OPERATING SYSTEMS」の「More」をクリックします（次ページ図）。



利用率が高い OS が表示されますので、絞りたい OS をクリックします。ここでは、「Windows 11（version 22H2）（build 10.0.22621）」をクリックします。

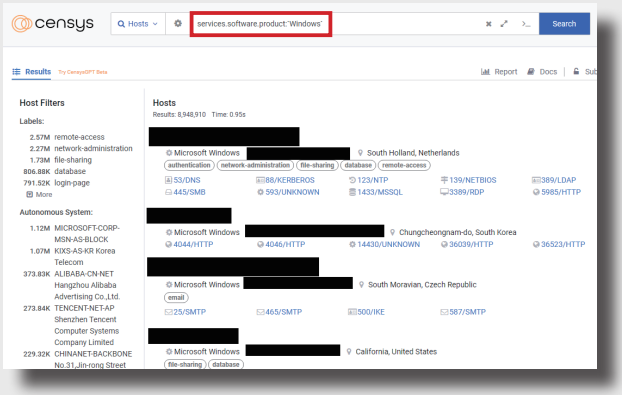


クリックした結果は、以下の通りです。「Windows 11 (version 22H2) (build 10.0.22621)」で絞り込んだ結果が表示されます（次ページ図）。



2.6 OS による検索 (Censys)

特定の OS の機器を確認します。「Censys」を開き、「services.software.product:`Windows`」で検索します。検索結果は次の通りです。



3. おわりに

今回はここまでとなります。「3. サービス探索編」では、「Shodan、Censys」を用いて、特定のサービスが稼働・公開されているサーバーを確認しました。自組織で管理できていないサーバーを探索する際等に利用したり、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。

次回は「4. サーバー探索編」となります。「Shodan、Censys」といった IoT 検索エンジンを用いて、脆弱なサーバを探索します。自組織で管理できていない脆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する際などに利用します。