HITACHI
Inspire the Next

Hitachi Systems Security Journal

VOL.63

株式会社 日立システムズ

Human * IT

Hitachi Systems security Jounral VOL.63

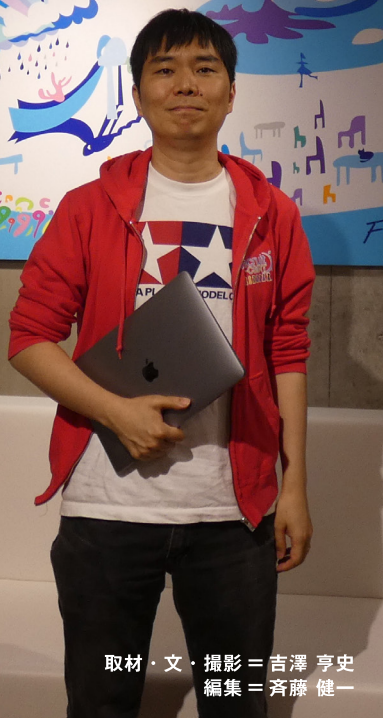
TABLE OF CONTENTS

●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

犯罪の実態を解明するには官民連携が不可欠
企業内でサイバー犯罪対策グループを立ち上げた

猪野 裕司
Yuji Ino
インタビュー



リクルートのビジネスを毀損するネット犯罪の被害を減らすためにサイバー犯罪対策グループを立ち上げた猪野裕司氏。JSAC（Japan Security Analyst Conference）2022 において「国内悪性プロキシサービスとの闘争」と題したセッションを行い話題となった。対象となった 911 Proxy はその後テイクダウンされている。JC3 でも活発に活動している猪野氏に、官民連携のメリットなどをうかがった。

取材・文・撮影＝吉澤 亨史
編集＝斉藤 健一

現職以前「セキュリティは趣味」だった

吉澤（以下、Y）：まず、猪野さんの略歴と現在のお仕事について教えてください。

猪野：（以下、I）：リクルート入社以前は大手国内 SI 企業に在籍していました。当初は研究開発部門に所属していたのですが、製品開発へと部門の方針転換がありました。クオリティを高めるような仕事は苦手で、0 を 1 にする研究開発の方が面白いと感じていたため、新規事業立ち上げの社内公募に応募、事業開発部門へ異動しました。その中で、米国のシリコンバレーに 4 年ほど駐在し、現地ではベンチャー企業の発掘や海外製品の立ち上げなどに携わっていました。

Y しばらくアメリカに行かれていたのですね。

I 帰国後、現在の上司の誘いでリクルートに入社しました。その上司とは元々同じ CTF チーム（sutegoma2）に所属しており、さまざまな形で交流もありました。それまでは、趣味としてセキュリティの勉強会に参加していましたが、セキュリティが仕事となったのは、現職になってからです。

Y 他の記事によると、猪野さんがセキュリティに興味を持つきっかけとなったのは、メールアカウントが乗っ取られたからだそうですね。

I あれは忘れもしない大学 1 年生の春でした。うる星やつらが大好きなとある大学教授から「あなたのメールアカウントが乗っ取られています」と指摘されたのです。当時のインターネットは法律もルールも何も整備もされていない状態で、攻撃もひんぱんに行なわれていました。しかし、その背後にある自由さに興味を持ちました。

Y リクルート入社後はどのような業務をしているのですか？

I しばらく CSIRT としてセキュリティインシデント対応のハンドリングをしていました。ただ、気になったのは情報セキュリティではなく、ビジネスを毀損するような悪意ある人間がサービス中で活動していることでした。数はそれほど多いわけではありませんが、そういった悪意ある人間の行動によってサービス全体の品質が下がってしまう。それを何とかしたいと考えていました。

Y その代表格が不正トラベル※1だったわけですね。

I こうしたサイバー犯罪事件は、犯人を逮捕すれば終わります。しかし、そこにたどり着くまでにはいくつものハードルがあることに気づきました。ほとんどの企業では、従業員が犯罪者の逮捕に関わることなど想定していませんよね。総論としては理解を得られても、各論になると承認を得られないことが多いのです。そこで、経営陣も参加する社内会議に働きかけてサイバー犯罪を着目するリスクの１つとして、認定していただきました。リスクへ対応する部署としてサイバー犯罪対策グループを立ち上げ、ビジネスを毀損する犯罪を定義、エスカレーションのフローを整備しました。

Y 警察へ事件通報することについて、社内ではどのような意見が出たのでしょうか。

I 犯罪者を逮捕することに対する炎上を懸念する声はありました。具体的には、犯罪者逮捕が報道されると SNS などでリクルートに対してネガティブな反応が起こるのではないか、というものです。悪いことをした人に対して、あるべき対応を行なうことで炎上が起こることはないと主張しました。実際に逮捕報道による炎上は起きていません。また、そうした事例を着実に積み上げていくことが実績となっています。

Y 現在もそうした不正を発見するための監視などを行っているのですか。

I サイバー犯罪対策グループの基本的な動きは、事業側で見つかった問題のエスカレーションを受けて解決することです。その中で、私が注力しているのは、重大なインシデントまでにはいたらないと判断されたものを徹底的に調査することです。さらっと流してしまいそうな軽微に見えるものでも、問題になりそうなら分析し、対策の必要のあるリスクを見逃さないようにしています。というのも、対策が再発防止につながると考えているからです。

猪野裕司（いの・ゆうじ）
国内大手 SI 企業を経て 2016 年リクルートテクノロジーズに入社。リクルート CSIRT として、リクルートで発生するさまざまなセキュリティ事故の対応をリード。現在は、サイバー犯罪対策グループでカード不正やなりすましログインなどを専門とした分析、調査を実施。日本サイバー犯罪対策センター（JC3）幹事。

Y リスクを正しく把握してノウハウを蓄積するとともに、対応の幅を広げていくわけですね。

I セキュリティ対策と違い、サイバー犯罪を未然に防止することは、ユーザーの利便性などを考えると非常に難しいのです。そこにコストをかけても、解決はできません。ですが、明らかに度を超えた不正をしている犯罪者が逮捕されれば、同じような不正を行なっている人たちへの大きな牽制にもなりますので、こうした活動を通じてサービスからサイバー犯罪の被害を減らしていきたいと考えています。

Y 警察への通報する案件としない案件の違いは、どのようなものなのでしょう。

I 通報する案件は、基本的に国内に痕跡が残って

※1 **不正トラベル**：旅行関連のサービスを狙った不正行為の一種で、特に宿泊施設や航空券の予約などを対象としている。手口としては、主に盗まれたクレジットカード情報を使って旅行を手配し、被害者は知らない間に不正に購入されたサービスの代金を負担することとなる。 https://www.jc3.or.jp/threats/archive/topics/travel_fraud.html

ミニ四駆が大好きだという猪野氏。講演を行ったり取材を受けたりするときは必ずタミヤのTシャツを着るのだという

いて、犯人逮捕までの道筋が見えやすいもの、その中で影響が大きいものを優先しています。実行犯が海外にいて、犯行がすべてインターネット上で行なわれ、その利益も海外で取得されるパターンは事件解決が非常に難しいです。

不正トラベル問題における官民連携

Y 先ほどの不正トラベルの件では、JC3 との連携があったと聞いています。それも官民連携の 1 つと言えると思いますが、どのような経緯、背景があったのでしょうか。

I JC3 はとても良い組織です。JC3 では警察官の方々とフラットに会話・相談ができ、きちんと対応・協力していただけます。IT に詳しい警察官が多いので、JC3 を通じて事件相談することで、JC3 が警察と事業会社のハブになり連携しやすかったと思います。他にも、最新の犯罪状況を共有していただけるので、非常に勉強になりますし、重要な場だと考えています。

Y 警察に事件捜査を依頼するのに、どのようなことが必要になりますか。

I 警察に通報したら後はお任せ、というわけには行きません。こちらも警察の捜査と歩調を合わせながら、常に新鮮な情報を提供し続ける。ここが非常に重要となります。例えば不正トラベルの事例であれば、不正利用からチャージバック（クレジットカードを保有する顧客が不正利用など理由に利用代金の支払いに同意しない場合にクレジットカード会社がその代金の売り上げを取り消すこと）の発生まで、数カ月かかります。チャージバックが発生してから連絡するのでは遅すぎます。事件解決が困難です。能動的に分析をした上で、チャージバックが発生していない不正予約、チェックイン前の不正予約などの情報を共有し、警察が実態を捜査できる状態を提供できるのがベストです。

Y 事業会社からも捜査に必要となるさまざまな情報提供が必要ということですね。

I 目的に対して必要な情報を適切なタイミングで出さないと、お互いの共通のゴールである事件解決にたどり着けません。幸い、私が取り組んだ事件は、ログを分析することで、不正トラベルの状況を迅速に把握できました。

Y 警察との官民連携では、漠然と「今日から連携して行きましょう」ではなく、犯罪被害が発生しており、証拠がある程度用意できるときに、犯人を逮捕して欲しいと連携するものなのですね。

I はい、警察との連携は、何かしらの課題を解決する目的とした方が良いです。

Y 連携をお願いしてから、ある程度先が見えるまでの時間は割とかかるものなのでしょうか。用意する情報や資料にもよると思いますが。

I ケースバイケースですね。割と時間がかかる傾向があります。時間がかかる理由として、今の手続きではインターネット犯罪の立件に必要とされる証拠が多すぎるという点があります。プロバイダーやカード会社の情報開示の手続きにも時間がかかりすぎます。知り合いの刑事さんなどは「ネット犯罪はつらい」とぼやいていました。

Y 官民連携する上での企業にとってのメリットを挙げるとすると犯人逮捕よる被害防止といった観点になるのでしょうか。

I 言い方は悪いかも知れませんが、警察組織は私たちが払っている税金で動いてもらえるセキュリティソリューションだと言えます。国から提供されている治安維持のサービスなので積極的に利用しましょうということですね。また、警察による逮捕は効果も絶大です。再発防止策には逮捕がい

ちばんわかりやすいですよね。やってた人がいなくなるわけですから。

国内悪性プロキシサービスとの闘い

Y JSAC（Japan Security Analyst Conference）での講演※2について教えて下さい

I もともと不正カード利用を追いかけていたことがきっかけで、国内のプロキシに気がつきました。同一アクターによる攻撃であるにもかかわらず、IP アドレスの分布に偏りがないという特徴がありました。それらの踏み台となったプロキシを検出できれば、カードの不正利用を防げるのではないかと考えたのです。

Y 具体的には、どのように取り組んでいたのでしょうか。

I プロキシの検出手法をいくつか検討しました。IP レピュテーションデータベース※3の利用を検討しましたが、我々が所有する不正利用された IP アドレスを全く検出できませんでした。他の手法を検討していたときに、911Proxy※4がこれらのプロキシの入口サービスであるという話を聞き、検証してみたところ、確かに 911Proxy を通じて不正に利用されているプロキシにアクセスできました。そこで 911Proxy のデータの収集を始めました。2020 年 10 月のことです。収集したデータを用いて不正なトランザクションをチェックすると、リクルートで発生する不正なトランザクションの 9 割以上がマッチしました。本丸を掴んだと思いました。

Y どのような状況だったのでしょうか。

I 1 日あたり約 8 万件の IP アドレスが観測できました。911Proxy は 2022 年 7 月 22 日にクローズしたのですが、その時までに収集できたユニーク IP アドレス数は 100 万以上、毎日、新しい IP アドレスを 1000 ～ 2000 件収集しました。収集前は全部で 100 ～ 200 IP アドレスくらいかなと考えていたのですが、桁違いでした。これだけの数の不正プロキシが国内に存在することは大問題だと考え、まとめた結果を 2022 年の JSAC で発表しました。

Y それが 911Proxy のテイクダウンにつながったのかも知れませんね。

I つながってはいません。ただし、911 の始まりから FBI に逮捕されるまでの 1 つのストーリーとして完結したことは、他のプロキシ業者への牽制サンプルとしてとてもいい事例だと思います。

Y 結果としてどのような収穫がありましたか。

I レジデンシャルプロキシに取り組んでわかったことは、プロキシの IP アドレスからのアクセスだからといって全て悪性であるとは限らないということです。つまり、当初の目的としていたカード不正への対応には役に立ちませんでした。ただし、不正があったときに、攻撃者がレジデンシャルプロキシを利用していたかどうかを調べるときには有効です。

Y カード不正以外で役立つ手法になったわけですね。

I 法執行機関が捜査をする上で、その IP アドレスの属性情報として非常に役に立ちます。私たちも警察に届け出をするときに IP アドレスの履歴から犯人の属性を判別することができます。その意味では JC3 経由で捜査機関へ提供することで、民から官への情報提供として役立つ活動ができたと思います。911Proxy は、有名セキュリティ・ジャーナリストによる OSINT 調査が行なわれ※5、その直後には「重大なデータ侵害」があったとして、サービスを停止しました。その後、新しいプロキシサービスが大量に出てきて、現在の状況の方が実は混沌としています。

Y プロキシサービスは人気が高く、需要が多いということですね。

I 911Proxy の前と後では完全に不正追跡の状況が変わってしまいました。利用するサービスが一極

※2 **国内悪性プロキシサービスとの闘争** https://jsac.jpcert.or.jp/archive/2022/pdf/JSAC2022_3_ino_jp.pdf

※3 **IP レピュテーションデータベース**：IP アドレスの不正利用状況を収集したデータベース。IPQS（https://www.ipqualityscore.com/）や spur.us（https://spur.us/）などがある。

※4 **911Proxy**：レジデンシャルプロキシサービス（住宅用の IP アドレスを利用したプロキシサービス）の 1 つ。世界中のユーザーの端末にウイルスを仕込みプロキシ出口として提供、犯罪者がオンラインで匿名性を保つのに寄与。2022 年 7 月、重大なデータ侵害を受けたとしてサービスを停止。

※5 **A Deep Dive Into the Residential Proxy Service '911'**
https://krebsonsecurity.com/2022/07/a-deep-dive-into-the-residential-proxy-service-911/

集中から群雄割拠の状態と不正プロキシマーケットが完全に変わりました。変更に追従するために、私たちは複数のサービスの監視を始めましたが、911 の時代に比べるとカバー率が全然足りていません。一つひとつのサービスの監視自体が 911Proxy に匹敵するほど大変なのです。このまま監視サービスを増やしていくことは体力的に厳しいため、何か次の手を打たなければならないことが今の課題です。また、このプロキシの状況を理解している人が少ないことも危機感としてあります。

今後も新しい領域を見つけたら足を踏み入れていく

Y 最後に今後取り組んでいきたいことについて、教えてください。

I 今後もレジデンシャルプロキシの根絶に向けて活動したいです。また、官民連携の強化として、民間企業が警察に対して円滑に通報できる社会を作り、インターネット犯罪が今よりも少なくなる状態を作りたいと思っています。そのために、民から警察に通報する際の「お作法」を共有していきたいと考えています。

Y なるほど。

I カード不正の被害金額も増えている一方で、3D セキュアの導入によって、インターネットにおける不正カード被害がカード会社に行くようになってしまったので、カード社会が成り立たなくなってしまうという危惧もあります。これを防ぐには、悪事を働く人間を捕まえないといけませんし、国内の受け子や海外にいる本犯たちの活動を少しでも妨害する必要があります。

Y 個人としてはいかがですか？

I「少しでも良い景色が眺められるのであれば、結果はともあれ、まずは動いてみよう」というのが、私の行動指針です。ですから、今後新しい領域を見つけたら、どんどん足を踏み入れ、1 つでも 2 つでも成果を出していきたいと考えています。そしてインターネットの安全を高めることに寄与できればと思っています。

Y 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 2024.08

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】：決済権限を持った経理担当者や、権限が高く、機密情報を多く握っている幹部層など、社内の特定の人物を狙った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入念に調べ、関係者になりすまして実施されることもあり、ばらまき型の攻撃よりも危険度が高い。攻撃者にはある程度の内部情報が知られていることを認識し、被害を受けないよう自覚を持った行動が重要である。

【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。英エンジニアリング大手企業のアラップが約 40 億円の詐欺被害を受けた事例がある。この事例では、同社の経理担当者宛てに最高財務責任者（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同じ会議に参加していたため正規取引であると判断し、指示に従い約 40 億円の振り込みを行った。実際には会議に参加していた同僚は全てディープフェイクを利用した偽物であった。この事例から、決済の権限を持つ経理担当者が誰なのかという情報や、メールアドレス、標的の同僚と、その容姿までもが攻撃者側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騙る攻撃者に騙され、偽の銀行口座に送金した事例がある。この事例では被害企業と取引先の正規のやり取りが攻撃者に盗聴されており、取引先からの請求書送付が行われたタイミングで、取引先の担当者になりすました攻撃者から口座変更の連絡が行われた。この際、口座情報の偽の証明書類が送付されており、書類には正規の取引先社長印が押されていたという※。

攻撃者はしっかりと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 サイト検索だけでなく、偽プロフィールを登録した SNS 上で対象組織のコミュニティやグループへ参加しチャットを盗み見る、SNS 上で直接接触を図り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、社外に公開している情報の見直しや、意図せず公開された情報の確認および対処が必要となる。しかし、対策を行っても、何らかの原因で内部情報は流出する可能性があり、どのような情報が攻撃者に知られているかを正確に把握するのは難しい。そのため、攻撃に遭った際、騙されないような予防対策を行うことが推奨される。例えば、取引先や同僚、上司など、自身の関係者から届いた連絡であっても、少しでも通常とは異なる違和感を覚えた場合は別の経路を使ってその関係者に直接コンタクトを図り、当該連絡が正規のものであるのかを確認することが対策として挙げられる。これは SNS 経由で接触を図られた場合も同様であり、相手が信用に足る人物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ことを認識した上で、被害に遭わないよう、やりとりしている相手が信頼できる人物であるかの確認を心掛けるなどの自覚を持った行動が重要である。

［情報源］

※ https://www.ipa.go.jp/security/bec/bec_cases.html

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 OSINT 体験

1. 環境準備編

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。今回から「OSINT 体験」と題して、3 回にわたり基礎となる考えの概説からツールを用いた調査方法までを紹介していきます。

OSINT とは、Open - Source Intelligence の略で、公開情報からインテリジェンス（意志決定のためにデータや情報などを分析して得られる知見）を作成することを指します。

インテリジェンス作成の過程において、さまざまなソースから収集されたものが「データ」であり、データを処理・利用したものが「情報」であり、情報を分析・作成したものが「インテリジェンス」となります。

OSINT は公的な利用可能なソースからインテリジェンスを作成するものですが、他にも人物から情報を収集する HUMINT（Human Intelligence）や、衛星写真や航空写真、地図／地形データから収集する GEOINT（Geospatial intelligence）などがあります。

組織のサイバーセキュリティでは、OPSEC（Operational Security）を意識し、Web データやインフラに対する調査を行ない、自組織に対してフィッシングメールなどの不審なメールが届いた際の調査や情報収集に役立てたり、ASM（Attack Surface Mnagement）などのように自組織の情報やインフラがインターネットからどう見えているか確認したりするのに活用可能です。

今回は、「1. 環境準備編」として、OSINT（Open-Source Intelligence）に関連する解析環境の準備から情報収集の方法を紹介します。

1. 環境準備編

OSINT と OPSEC の概念を理解し、OSINT 用の仮想環境を準備します。その後、OPSEC を強化するために VPN やプラグインを導入し、設定を確認します。

2. Web データ収集編

Web ブラウザーを用いた Google Dorks と Web アーカイブサイトを用いたキャッシュ、クラウドストレージの調査サイトを紹介します。

3. Web/ インフラ調査編

ツールなどを用いて Web やインフラに対する情報収集の手法やツールを紹介します。

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。

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）等に抵触することがありますので、十分にご注意下さい。

2. インテリジェンス・OSINT・OPSEC

2.1 インテリジェンスと OSINT

OSINT（Open-Source Intelligence）とは、洞察やインテリジェンスを得るために、ニュース記事、ソーシャルメディア、政府報告書などの公的に利用可能なソースから情報を収集および分析することを指します。

OSINT は、あらゆる業界のほぼすべての人に利益をもたらすため、セキュリティの重要なコンポーネントです。法執行機関や諜報機関などの政府機関や、サイバー脅威情報、市場調査、採用、競合情報の収集を目的とする民間企業など、さまざまな組織で活用されています。CSIRT 活動の中でも、外部の脆弱性や脅威情報を収集する際や、インシデント対応時の調査の中で OSINT を用いることがあります。

●政府および諜報機関
- 安全保障上の脅威情報を収集、地政学的な出来事を監視し、意思決定をサポート

●法執行機関
- 犯罪行為に関する情報を収集し、犯罪ネットワークを監視し、捜査を支援

●企業や金融組織
- 競合情報を収集し、市場動向を監視し、事業運営に対する潜在的なリスクを特定

●サイバーセキュリティ専門家
- サイバー脅威を特定して監視し、脆弱性に関する情報を収集
- インシデント対応と脅威インテリジェンスの取り組みをサポート

2.2 インテリジェンスのプロセス

インテリジェンスのプロセスは 5 つのステップに分類されます。はじめに「1. 計画」を行い、依頼者の目標を理解して、調査手法や制限、報告形式を決定します。次に、「2. 収集」では、あらゆるソースからデータを収集します。その後、「3. 加工と活用」と「4. 分析と作成」で収集したデータから依頼者の質問に答えるために分析してレポートを作成します。最後に「5. 普及と統合」で依頼者のニーズに応えたレポートを展開して利用してもらいます。レポート結果を元に、次の計画を立ててインテリジェンスのプロセスを回してきます。

1. 計画（Planning and Drirection）
- どのような手法が許可されているか、従う必要があるポリシーや法律を定義
- 依頼者の最終的な目標を理解することが最も大切

2. 収集（Collectoin）
- OSINT で最も注目を集める部分であるがステップの 1 つにすぎない

3. 加工と活用（Processing and Exploitation）
- 収集と分析の間のステップ、生データから使用可能な形式への加工を含む
- 外国語から母国語への翻訳など

4. 分析と作成（Analysis and Production）
- 情報や加工済みデータを確認し、依頼者のニーズに応えるレポート作成のための重要なステップ

5. 普及と統合（Dissemination and Integration）
- 依頼者のニーズに応えた概要や調査結果などを含めたレポートを提供して利用される

2.3 OPSEC

OSINT を始める前に重要な考え方として OPSEC（Operational Security）を紹介します。OPSEC は米国軍に由来する用語で、機密活動の計画と実行に関する一般に機密扱いされていない証拠を特定・制御・保護することで、潜在的な敵対者が能力と意図に関する情報を入手できないようにする体系的で実証済みのプロセスを指します。このプロセスには、重要な情報の特定、脅威の評価・分析、脆弱性の分析、リスクの評価、適切な対策の適用という 5 つのステップが含まれます。

1. 重要な情報の特定
- 機密情報が何である可能性があるかを理解する

2. 脅威評価
- 潜在的なサイバーセキュリティの脅威を特定する
- 攻撃者が自組織に対して何を悪用できるかを考える

3. 脆弱性分析
- セキュリティ上の脆弱な箇所を特定する

4. リスク評価
- 特定された各脆弱性に関連するリスクのレベルを測定する

5. 対策を適用
- 特定されたリスクを最小限に抑えるための対策を策定する

OSINT 調査の実施者は、優れた OPSEC を備えている必要があります。端末がマルウェアに感染する可能性があったり、アクセス元 IP アドレスからアクセス元の組織が攻撃者に漏れる可能性があったりするため、リスク管理プロセスとして、「業務情報が含まれない端末・環境から、社内ネットワーク以外からアクセス」や「普段している個人アカウント・デバイスを使用しない」など OPSEC を意識する必要があります。

不適切な OPSEC の一例として、使用されていないソーシャルメディアのプロファイルをオンラインに残しておくことが挙げられます。理解すべき一般的なルールは、人はミスを犯す可能性があるということであり、常にミスの影響を軽減することであるべきです。　SANS のページに OPSEC のためのベストプラクティスが掲載されています※ 1。

また、Webcast「Best Practices and Lessons Learned from Starting Up OSINT Teams」も公開されているので、ぜひご参照ください※ 2。

※ 1 https://www.sans.org/blog/what-is-opsec/

※ 2 https://www.sans.org/webcasts/best-practices-lessons-learned-starting-osint-teams/?msc=blog%20what%20is%20opsec

3. OSINT 調査

3.1 OSINT 調査環境の準備

OPSEC を確保するために、今回は Trace labs 社の仮想環境を用いて調査環境を準備します。Trace labs 社のサイトにアクセスすると、図 1 のように OSINT 用の仮想環境が用意されていることが確認できます。実際には Github 上からファイルをダウンロードすることになります。今回は VirtualBox 向けのファイルをダウンロードして環境を構築します。

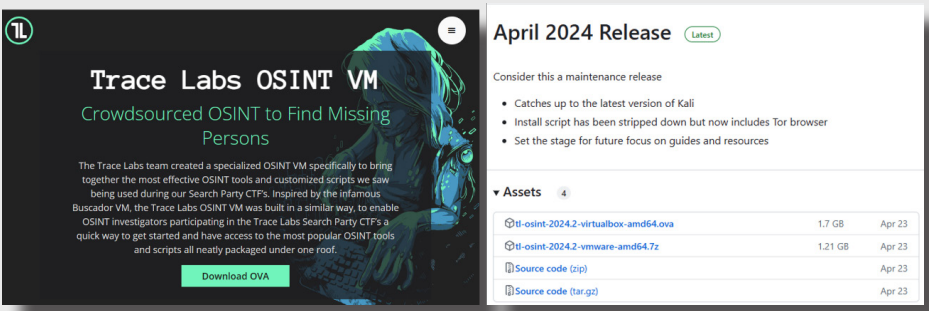


図 1 Trace Labs 社の OSINT 用 VM のダウンロードサイト（https://www.tracelabs.org/initiatives/osint-vm）

ダウンロードした ova ファイルをダブルクリックすると、図 2 のように VirtualBox の仮想アプライアンスのインポートが表示されます。VirtualBox を解析用 PC にインストールしていない場合は、公式サイトから事前にダウンロードしてください※ 3。仮想環境のログイン ID と PASS はそれぞれ osint / osint です。ログインすると図 3 のように OSINT 用にカスタマイズされた仮想環境を使用できるようになります。

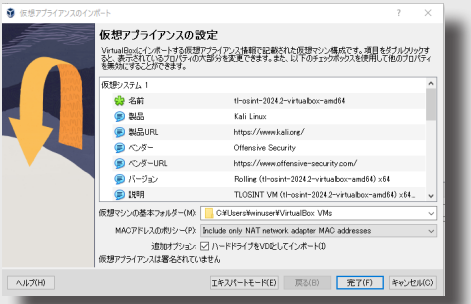


図 2 VirtualBox への仮想環境のインポート

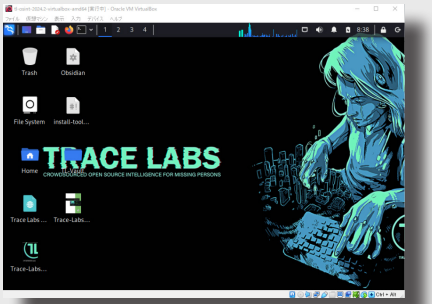


図 3 ログイン後の Trace Labs 社の OSINT 用仮想環境

3.2 OPSEC の確認

準備した仮想環境を用いて OSINT 調査を実施していきますが、その前に OPSEC を確認してみます。“WhatIsMyBrowser.com” ※ 4 は、アクセス元の情報を確認するサイトで、ブラウザの設定や IP アドレス、システム情報などを確認できます。図 4（次ページ）は FireFox で “WhatIsMyBrowser.com”

※ 3 https://www.virtualbox.org/
※ 4 https://www.whatismybrowser.com/

にアクセスした結果ですが、Linux の Firefox 115 バージョンでアクセスしていることが表示されています。また、JavaScript や Coolies が有効化されていることがわかります。JavaScript が有効化されていると、Web サイトにアクセスした際に JavaScript でアクセス元の情報を収集できます。アクセス元の情報を可能なかぎり取得されないためにも無効化することを推奨しますが、JavaScript が有効化されていないと Web ページがうまく表示されない場合もあります。そのため、デフォルトで無効化しておき、必要に応じて有効化するなど柔軟に対応することが必要です。

図 4 WhatIsMyBrowser.com で確認できる情報（その 1）

その他には、図 5 に示すように IP アドレスやコンピューターやブラウザーの解像度も表示されています。これらの情報が相手に伝わると、複数情報を組み合わせることでアクセス元を識別される可能性があります。そのため、自組織のネットワークから OSINT 調査を実施すると、組織が情報収集していることがアクセス先に伝わり、OPSEC が損なわれます。右下には TOR を使用しているかの項目も確認できます。TOR でアクセス元を秘匿するのに有効なソフトウェアですが、今回は VPN を用いて IP アドレスを秘匿する方法を紹介します。

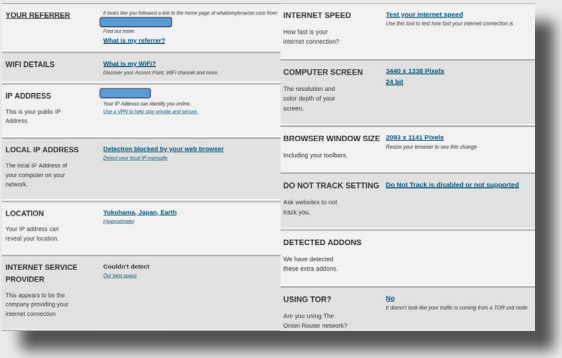


図 5 WhatIsMyBrowser.com で確認できる情報（その 2）

3.3 VPN を用いたアクセス元 IP の変更方法

VPN とは “Virtual Private Network” の略称で、インターネット通信を暗号化し、IP アドレスを秘匿することでデータを第三者から保護するサービスのことです。テレワークを行うために、自宅から社内ネットワークへ VPN 接続し業務を行なうためなどに使用されています。一方で、重大な脆弱性が公開され、認証情報の漏えいなどでサイバー攻撃者の侵入経路にも悪用されることもあります。今回は、OPSEC を確保するために IP アドレスを秘匿する目的で VPN を使用します。

VPN は商用サービスが数多くあり、Google のサブスクリプション・サービスである Google One に含まれる Google One VPN や NordVPN などがあります。今回は、筑波大学が学術実験プロジェクトとして提供している “VPN Gate” [※5] を用いて VPN 接続する方法を紹介します。VPN Gate 学術実験プロジェクトは、日本に所在する筑波大学における学術的な研究を目的として実施されているオンラインサービスで、グローバルな分散型公開 VPN 中継サーバーに関する知見を得ることを目的とされています。VPN Gate にアクセスすると、図 6 に示すように VPN 中継サーバーがある国と DDNS 名／ IP アドレスや使用可能な接続方式が確認できます。

国・地域 (推定位置)	DDNS 名 / IP アドレス (ISP ホスト名)	VPN 接続数 / 運転稼働期間 / 累積利用者数	回線品質 (回線速度および Ping / 累積通信量 / ログ記録ポリシー)	SSL-VPN Windows・快適	L2TP/IPsec Windows, Mac, iPhone, Android クライアントソフト不要	OpenVPN Windows, Mac, iPhone, Android	MS-SSTP Windows Vista, 7, 8, RT クライアントソフト不要	ボランティア運営者名 (= 運営者によるメッセージ)	スコア (前週)
United States	vpn954093955.opengw.net 23.241.209.22	50 セッション 0 分間 過去 237,201 人利用	85.62 Mbps Ping: 14 ms 4,159.95 GB ログ記録ポリシー: ログ最低 2 週間保存	SSL-VPN 接続方法 TCP: 1842 UDP: サポート		OpenVPN 設定ファイル TCP: 1842 UDP: 1750	MS-SSTP 接続方法 SSTP ホスト名: vpn954093955.opengw.net:1842	By IVI2's owner	1,973,148
United States	vpn727618301.opengw.net 76.115.176.177	4 セッション 0 分間 過去 49,531 人利用	50.66 Mbps Ping: 16 ms 471.00 GB ログ記録ポリシー: ログ最低 2 週間保存	SSL-VPN 接続方法 TCP: 1206 UDP: サポート		OpenVPN 設定ファイル TCP: 1206	MS-SSTP 接続方法 SSTP ホスト名: vpn727618301.opengw.net:1206	By Jsamo's owner	1,938,252
Japan	public-vpn-184.opengw.net 219.100.37.162 (public-vpn-11-02.vpngate.v4.open.ad.jp)	270 セッション 3 日間 過去 8,761,387 人利用	752.80 Mbps Ping: 13 ms 436,222.87 GB ログ記録ポリシー: ログ最低 2 週間保存	SSL-VPN 接続方法 TCP: 443 UDP: サポート	L2TP/IPsec 接続方法	OpenVPN 設定ファイル TCP: 443	MS-SSTP 接続方法 SSTP ホスト名: public-vpn-184.opengw.net	By Daiyuu Noborl, Japan. Academic Use Only.	1,811,629
Japan	public-vpn-200.opengw.net 219.100.37.213 (public-vpn-14-05.vpngate.v4.open.ad.jp)	208 セッション 3 日間 過去 8,007,125 人利用	332.49 Mbps Ping: 11 ms 376,370.40 GB ログ記録ポリシー: ログ最低 2 週間保存	SSL-VPN 接続方法 TCP: 443 UDP: サポート	L2TP/IPsec 接続方法	OpenVPN 設定ファイル TCP: 443 UDP: 1195	MS-SSTP 接続方法 SSTP ホスト名: public-vpn-200.opengw.net	By Daiyuu Noborl, Japan. Academic Use Only.	1,778,816

図 6 VPN Gate で利用可能な VPN サーバー覧

図 6 の OpenVPN 設定ファイルをクリックすると、図 7 が表示され DDNS ホスト名か IP アドレスが設定されている ovpn ファイルをダウンロードできます。ダウンロードした ovpn ファイルを設定し、VPN サーバー経由でインターネットに接続できるようにします。

図 7 DNS ホスト名 または IP アドレスが設定された ovpn ファイル

※ 5 https://www.vpngate.net/ja/

ovpn ファイルを設定する方法を解説します。図 8 に示すように右上の赤枠で囲ったアイコンをクリックし、「VPN Connections」→「Add a VPN connection」を選択します。その後、「Choose a VPN Connection Type」が表示されるので、「Import a saved VPN configuration」を選択し、ダウンロードした ovpn ファイルを選択します。 ovpn ファイルを選択すると設定内容が反映されるため、図 9 のように右下の「Save」をクリックして設定を保存します。

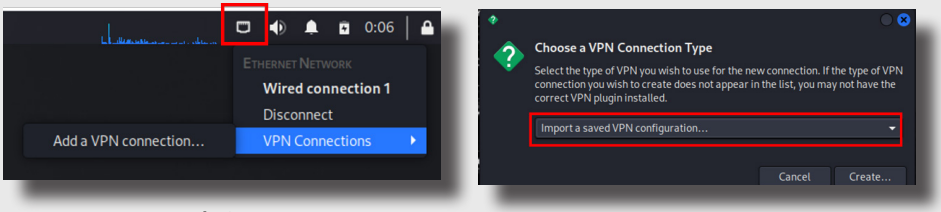


図 8 ovpn ファイルのインポート

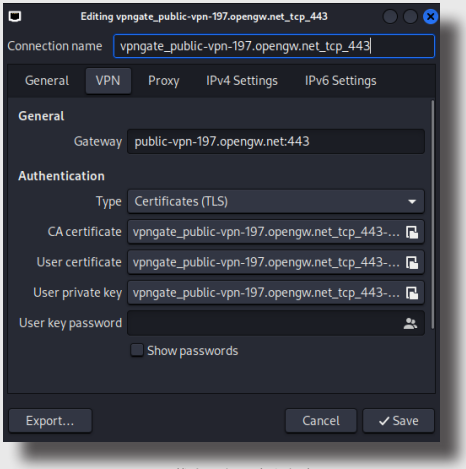


図 9 ovpn ファイルに記載された設定を保存

ovpn ファイル設定後、図 10 のように “VPN Connections” から設定した VPN のチェックボックスをクリックすることで、VPN 接続が成功したメッセージが表示され、VPN が接続された状態になります。

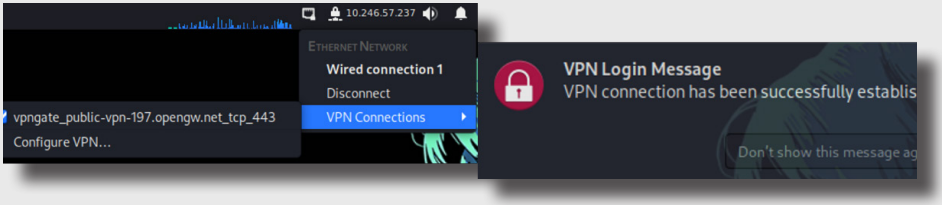


図 10 VPN 設定が適用された状態

VPN が接続された状態で、再度「WhatIsMyBrowser.com」へアクセスすると、図 11 のように “VPN Gate” で選択した IP アドレスが表示されることが確認できます。このように自身の IP アドレスを秘匿して、Web サイトにアクセスできる状態になったことなったことを確認できます。

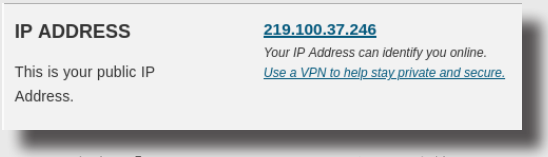


図 11 VPN 経由で「WhatIsMyBrowser.com」にアクセスした結果

3.4 コンテンツブロッカーの導入

ここでは Web ブラウザでサイトにアクセスする際に表示される不要な広告やトラッカーをブロックするブラウザー用のプラグイン ”uBlock Origin” を紹介します。準備した仮想環境には Firefox がデフォルトでインストールされているため、Firefox 用の “uBlock Origin” を設定していきます。図 12 のように、Firefox 上で Firefox Browser ADD-ONS にアクセスし、右上の検索ボックスに “uBlock Origin” を入力して検索します。

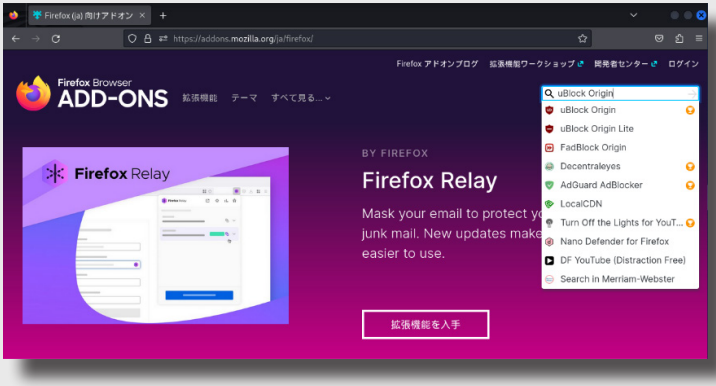


図 12 Firefox Browser ADD-ONS のページ（https://addons.mozilla.org/ja/firefox/）

すると、図 13 のように ”uBlock Origin” のページが表示されるため、“Firefox へ追加 ” をクリックします。クリック後、ポップアップが表示されますが、“Add” をクリックすることで、図 14（次ページ）のように Firefox の右上に “uBlock Origin” のアイコンが表示されるようになります。

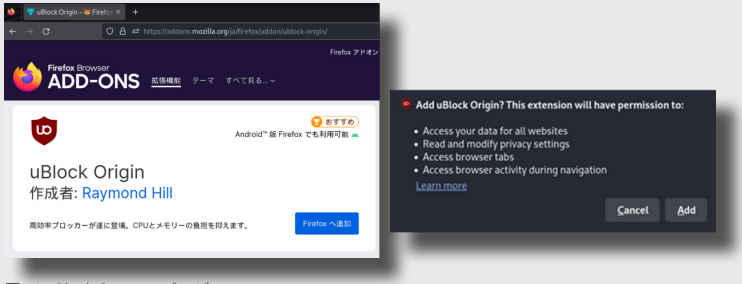


図 13 uBlock Origin のページ

“uBlock Origin” の使い方を図 14 を参照しながら簡単に説明します。①の電源マークのようなものがフィルタリングの適用状況となり、青が有効、白が無効を示します。また、左下の ”More” をクリックすることで、左側のドメイン一覧が表示されるようになります。②で囲んだ緑や赤はブロックの状態を示しており、緑：許可、赤：ブロック、黄色：許可とブロックの状態を示します。また、③で囲んだ個所の＋が許可、－がブロックを表しており、＋が 1-9 個の要素を許可、＋＋が 10-99 個の要素を許可、－は逆にブロックしている要素を示しています。④をクリックすることで現在アクセスしているサイトの JavaScript をブロックされるように設定されます。

図 14 uBlock Origin の画面

図 15 に、uBlock Origin で JavaScript をブロックした状態で WhatIsMyBrowser.com にアクセスした結果を示します。JavaScript の有効化の個所を見ると、” No - JavaScript is not enabled” と表示されるようになったことから、設定が適切に動作していることが分かります。このように “uBlock Origin” を用いることで不要な JavaScript が動作せず、広告のブロックが行われることから、アクセス元の情報を保護できるようになり OPSEC が強化されます。

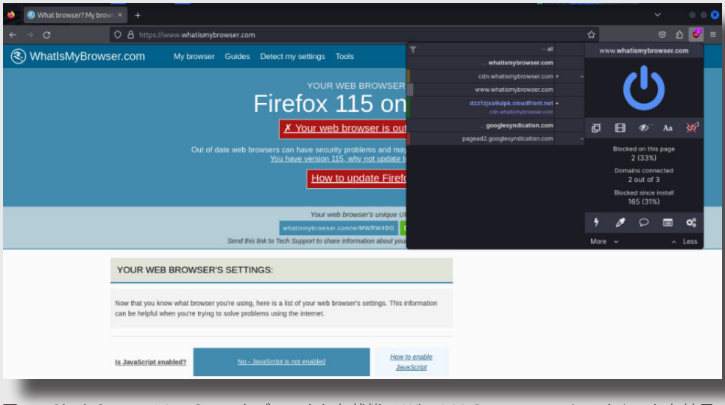


図 15 uBlock Origin で JavaScript をブロックした状態で WhatIsMyBrowser.com にアクセスした結果

4. OSINT ツールのブックマーク

本稿の最後にOSINTに有益なツールがブックマークされたサイトを紹介します。図16のサイトは、さまざまなテーマごとに利用可能な OSINT ツールやサイトがまとまったブックマークです。興味があるテーマを確認して準備した仮想環境からアクセスして、どのようなツールなのか皆さんでそれぞれ試してみてください。

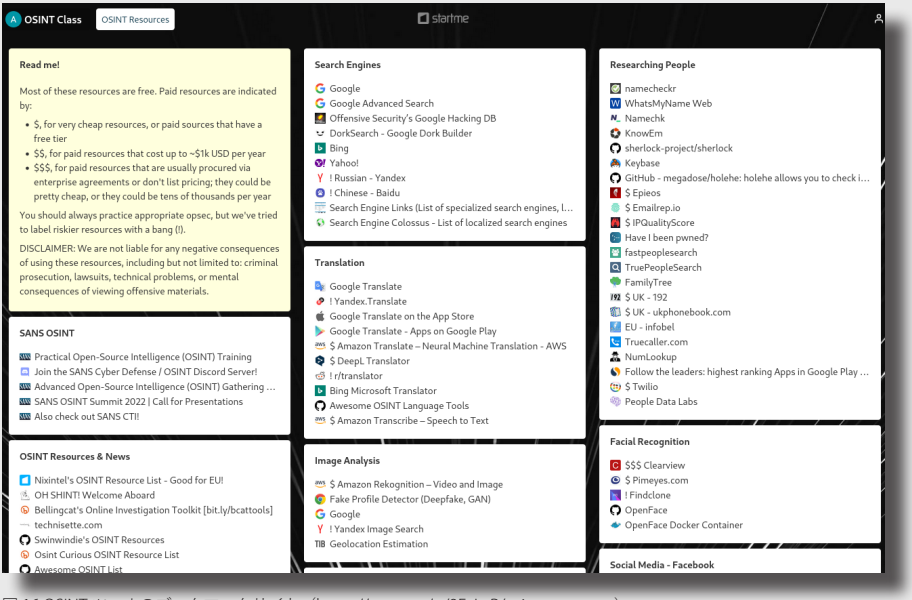


図 16 OSINT ツールのブックマークサイト（https://start.me/p/9ExLyR/osint-resources）

5. おわりに

今回はここまでとなります。今回は、OSINT 体験「1. 環境準備編」として、OSINT の説明と調査のための仮想環境の準備を行いました。次回から準備した環境を用いて実施に OSINT 調査を実施します。

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.63

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