HITACHI
Inspire the Next

Hitachi Systems Security Journal

VOL.65

株式会社 日立システムズ

Human * IT

Hitachi Systems Security Journal VOL.65

TABLE OF CONTENTS

技術と人をつなぐユーザブルセキュリティを追求する若き研究者
山岸 伶 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 2024.11 …… 9

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　3. Web データ収集編 …… 10

●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

●ご利用条件

本文書内の文章等すべての情報掲載に当たりまして、株式会社日立システムズ（以下、「当社」といいます。）といたしましても細心の注意を払っておりますが、その内容に誤りや欠陥があった場合にも、いかなる保証もするものではありません。本文書をご利用いただいたことにより生じた損害につきましても、当社は一切責任を負いかねます。
本文書に記載した会社名・製品名は各社の商標または登録商標です。
本文書に掲載されている情報は、掲載した時点のものです。掲載した時点以降に変更される場合もありますので、あらかじめご了承ください。
本文書の一部または全部を著作権法が定める範囲を超えて複製・転載することを禁じます。

© Hitachi Systems, Ltd. 2024. All rights reserved.

技術と人をつなぐ ユーザブルセキュリティを追求する若き研究者

山岸 伶 インタビュー

Rei Yamagishi

株式会社 日立製作所 研究開発グループ
サービスシステムイノベーションセンタ
セキュリティ・トラスト研究部 研究員

IT の進化によって生成 AI をはじめとする技術イノベーションの波が押し寄せている。その一方で、攻撃者も新たな環境を攻撃するために技術を磨いている。こうした状況の中、組織の研究・開発分野の重要性は以前にも増して高まっており、日本においても研究者育成の取り組み拡充の声が上がっている。日立製作所のセキュリティ・トラスト研究部の山岸伶氏は、LLM（Large Language Models：大規模言語モデル）のコード生成に関する論文やユーザブルセキュリティに関する論文などが高く評価されている。今回は山岸氏に取り組んでいる研究の内容や今後の課題などについて話を伺った。

取材・文 = 吉澤 亨史／撮影・編集 = 斉藤 健一

大学在学時から取り組む ユーザブルセキュリティ

吉澤（以下 K）：まずは山岸さんの略歴を教えてください。

山岸（以下 Y）：出身校は電気通信大学です。大学ではセキュリティ、とりわけユーザブルセキュリティに関する研究を行なっていました。修士課程を修了後、2019年に日立製作所に入社しました。配属先のセキュリティ・トラスト研究部（当時はセキュリティ研究部）では、セキュリティ運用の高度化や効率化に関する研究を進めてきました。ユーザブルセキュリティの研究も引き続き行なっています。

K ユーザブルセキュリティについては後ほどお聞きしますが、元々セキュリティに興味を持つきっかけは何だったのでしょうか。

Y 大学では、情報系の研究室の先生方による研究プレゼンの授業がありました。その際、ユーザブルセキュリティを研究している先生の話が興味深く、その研究室に入りセキュリティに関する研究に携わるようになりました。具体的には、セキュリティ対策は技術だけでなく、人に関する部分も大きく、そこには認知心理学や行動経済学も関係しています。

K セキュリティを専攻されていたとなると、当時の就職市場では大変需要が高かったのではないでしょうか。そのあたりについてお聞かせいただけますか。

Y セキュリティの仕事に携わりたいと思い、研究とエンジニアを考えました。どちらも経験してみたい気持ちはありましたが、やはり研究を続けたいという思いが強く、大学での研究が非常に面白かったことも影響しています。そのため、研究を続ける道を選び、ご縁があって日立製作所に就職することになりました。

K 就職先に日立製作所を選んだ理由は何だったのでしょうか。

Y 大学の研究に取り組む中で人に起因するセキュリティの問題が多くあると感じました。日立製作所には幅広い事業分野があるので、さまざまな人に関わって、それぞれの人が抱えている課題に対して、セキュリティの研究を通して貢献したいと考えたからです。

山岸 伶（やまぎし・れい）
電気通信大学情報理工学研究科を修了後、日立製作所の研究開発グループに在籍。社会人博士課程で、早稲田大学大学院基幹理工学研究科に在籍し研究を進めている。また、精力的に論文を執筆し、受賞歴も豊富である。主な受賞歴には「アンケートによるビジネスチャットを介したフィッシングに対する感受性の分析」で CSS 優秀論文賞および UWS 論文賞、「入力時の日本語と英語の差異が ChatGPT で生成するコードの安全性に与える影響」で CSS2023 コンセプト研究賞および 2024 年度（令和 6 年度）山下記念研究賞などがある。

多くの賞を獲得した LLM の入力言語の 違いによるコードの安全性に関するに研究

K 具体的な研究内容についてお伺いしたいと思います。まず、LLM のセキュリティを研究されるようになったきっかけについてお聞かせいただけますか。

Y きっかけは、セキュリティ・トラスト研究部で LLM のセキュリティに関する研究の意識が高まっていたことです。私もその必要性を感じ、研究に取り組むことにしました。LLM の登場は非常に衝撃的で、特に自分の専門であるセキュリティの課題にも応用する価値があると考え、チャレンジを始めました。

K LLM のセキュリティに関する研究には、多くの研究者が取り組んでいるかと思います。現在の研究動向や最新の傾向について感じていることなど

本年 4 月より社会人博士課程で早稲田大学大学院基幹理工学研究科に進学。ユーザブルセキュリティの研究を進めているという

があれば教えていただけますか。

Y 学会などを見ていると、LLM セキュリティ研究には大きく 3 つの傾向があると感じています。1 つ目は、LLM 自体への攻撃に関する研究です。これはデータの改ざんやモデルに手を加えて不正な動作を引き起こす可能性を探るものです。2 つ目は、LLM を用いたセキュリティの高度化で、特に自動化や LLM による判断への応用が進んでいます。そして 3 つ目は望ましくない出力に関する研究で、ハルシネーション（誤った、あるいは誤解を招く回答）の問題もその 1 つです。

K セキュリティカンファレンスでの LLM に関する講演も、伺った 3 つの傾向に集約されているように感じます。

Y セキュリティから枠を少し広げると、著作権問題や機密情報の流出に関連する研究も含まれます。さらに、LLM に研究を支援させたり、結果の評価を任せたりするなど、LLM を研究プロセスに組み込む独自の試みも進められています。

K LLM は AI と非常に近しい分野かと思いますが、研究者も多くが AI 分野からこの研究に移行するケースなどもあるのでしょうか。

Y 先ほどの 1 つ目の、モデルに対する研究については、もともと AI や機械学習のモデルに関する研究分野があり、その分野の研究者が LLM の研究にも取り組んでいるイメージです。一方、2 つ目のセキュリティの高度化をめざす研究者も、LLM をいかに活用できるかについて研究しています。

K 国内外で注目を集めた山岸さんの論文「入力時の日本語と英語の差異が ChatGPT によるコード生成の安全性に与える影響の考察」ですが、このテーマを選ばれた理由をお聞かせください。

Y LLM のセキュリティ研究をしようと考えたときに、LLM が生成するコードの品質を人間が正しく判断できるのかという点に興味を持ちました。また、当時 ChatGPT を使ったプログラミングが話題となっており、その安全性を見極めることが今後の課題になるだろうと考えました。そうした背景を踏まえ、この分野に貢献できる研究成果を残したいという思いから、このテーマを選びました。

K 概要を簡単に教えていただけますか。

Y この研究では、ChatGPT に対し英語と日本語それぞれで同じ目的のコードを生成させ、出力されたコードの安全性を検証しました。また、安全性に関する説明があるか、説明があった場合にはその説明を活用してより安全なコードに修正できるかについても検証しました。これらの検証結果を分析し、注意点などを含めて論文にまとめました。

K 検証結果はいかがでしたか。

Y 当時の GPT-4 では、日本語と英語のどちらで入力した場合でも、安全でないコードが生成されるケースが多くみられました。また、英語での出力には注意書きが付されることが多かった一方で、日本語では注意書きがほとんど見られませんでした。そのため、出力されたコードをそのままコピーして使用すると、ぜい弱なコードが組み込まれるリスクがありました。また、API などのモジュールが安全であるかどうかを見極めることも重要であるとわかりました。

K コードの安全性も ChatGPT で調べるようになっていくと想定して、その第一歩として検証されたわけですね。この論文はどのくらいの時間がかかったのでしょうか。

Y 思い立ってすぐ研究にとりかかったので、2 ～ 3 カ月ほどでした。

K LLM に関する研究の今後はどのような方向に進むと思われますか。

Y LLM は急速に進化していますが、研究はまだ始まったばかりです。そのギャップを埋め、追いつ

いていくために、多くの人がさまざまな研究に取り組んでいくでしょう。ただし、利用者がハルシネーションや情報漏えいといったリスクを理解した上で活用できるかどうかが、今後の重要な課題になると考えています。

K 日立製作所は 2023 年 5 月に『Generative AI センター』を立ち上げ、生成 AI の活用に積極的に取り組んでいる印象を受けますが、こうした動きがセキュリティ・トラスト研究部に与える影響についてはいかがでしょうか。

Y これまでに比べ、LLM に関する研究が増加しているように感じます。私が関わった研究では、マルウェアの静的解析において、LLM を用いてコードに対する説明を加えた場合、それが専門家の助けになるかどうかをインタビューや検証を通じて調査しました。

CSS 2022 で優秀論文賞などを受賞したユーザブルセキュリティの研究

K 次に、山岸さんが研究者になるきっかけとなったユーザブルセキュリティについて伺いたいと思います。まず、ユーザブルセキュリティの概念について簡単に説明いただけますか。

Y ユーザブルセキュリティは、元々はシステム利用時に生じるセキュリティ上の課題を、ユーザーが使いやすい形で解決することを目ざす分野です。一般に、セキュリティとユーザビリティの両立は難しいとされています。例えば、パスワードを長く複雑にすればセキュリティは強化されますが、覚えにくくなります。一方で、短く簡単にすれば覚えやすくなりますが、セキュリティが低下するリスクがあります。

K 一般に、セキュリティの強度を上げるためには一定の手間がかかるとされています。

Y そのとおりです。セキュアでユーザビリティが高いシステムをめざす分野です。最近では、ユーザビリティに限定せず、専門家のセキュリティに対する考え方やアプローチを取り入れるなど、人間の視点を考慮したセキュリティ分野へと広がっています。インターネット黎明期から海外で研究が進められており、近年では日本でも多くの研究者の方が研究成果をあげられています。

K ユーザーの行動特性を踏まえて IT 環境のセキュリティを強化する、といったイメージでしょうか。インターフェイス設計にも関わる要素もありそうですね。

Y 例えば、Web ブラウザーの警告といったセキュリティに関わるインターフェイスデザインの研究があります。他にも Web ブラウザーの左上部に、セキュリティ状態を表現するインジケーターと呼ばれる鍵マークなどのアイコンがあります。これは HTTPS による暗号化の有無やセキュリティに関するエラーなど状態で微妙にデザインが変化していたのですが、どのようにしたらこの違いをユーザーに伝えられるのかデザインの改良をしていた研究もあります。こうしたデザイン改善に関する研究も活発に進められています。

K 逆に、そうした表示がフィッシング詐欺に悪用される流れもありますよね。

Y そのような懸念もありますし、セキュリティはイタチごっこが続きます。フィッシング対策は、ユーザブルセキュリティの中でも古くから研究されている分野です。攻撃者はいかに人を騙すかを研究していますが、守る側はその手口を見抜き、騙されない方法を模索しています。例えば、URL の一部をハイライトしたり警告を出したりすることで、ユーザーがフィッシングかどうかを判断する手助けをするといった研究もあります。ユーザーの判断を支援することは大切だと思います。

K きっかけのところでお話いただいた、認知心理学や行動経済学ですね。

Y 以前は技術面ばかり注目されていましたが、技術だけでなく人間の要因も大きな影響を与える点にに注目が集まっています。近年では、HCI（ヒューマン・コンピューター・インタラクション）という分野がセキュリティにも関わるようになっています。例えば、インタビューやアンケートで人間の行動を調査する際に、いかに信頼性のあるアンケートを作成し、得られた結果をどのように分析するかといった課題も検討されています。

K かなり幅が広くなっていきそうですね。

Y セキュリティの幅は広いですが、取り組めば取り組むほど、人間的な要素が多いと実感しています。また、専門家がサイロ化されている印象もあり、互いに助け合うことでさらに大きな成果が期

待できるのではないかと考えています。非常に重要な分野であり、今後もさらに研究を進めていきたいと思っています。

K ユーザブルセキュリティにおいて、山岸さんはCSS で優秀論文賞を受賞されています。その論文では、どのようなテーマを研究されていたのですか。

Y 私たちの研究では、チャットでのフィッシングはメールよりもユーザーが騙されやすいのではないかと考え、アンケート調査で検証し、分析を行いました。コロナ禍で、メールや対面からチャットにコミュニケーションが急速に移行し、学会の活動も Slack で行うことが増えた中で、悪意のある人物がチャットを悪用するリスクについて意識するようになりました。結果としてはチャットとメールでの騙されやすさは同等だったのですが、チャットにもリスクがあり対策が必要ということが再認識できました。

K チャットの信頼性が十分でない状況では、フィッシングやマルウェアの添付に対する不安もありますね。騙されやすいユーザーの傾向などについても調査されたのでしょうか？

Y そうした研究はすでに多く行われています。私も最終的には、環境面の改善、例えば充実した教育やチャットソフトのデザイン変更などによって、フィッシング被害に遭うユーザーを減らせるのではないかという視点から研究に取り組みました。

K まさに、そのような視点を持った研究であったからこそ、優秀論文賞の受賞につながったのでしょうね。

トップレベルの学術会議で日本人が活躍するために

K ユーザブルセキュリティで今後取り組みたい研究はありますか？

Y ユーザブルセキュリティに関して、さらに深いユーザー分析を進めたいと考えています。せっかく実際のセキュリティオペレーションに携わっている方とお話しする機会をいただくこともありますので、現場でセキュリティに取り組む専門家の方々が感じている課題に対して、少しでも解決の糸口を提供できるような研究を目ざしたいと思います。

精力的に研究を続ける山岸氏。次は世界の難関学術会議での論文採択を目ざすと抱負を語ってくれた

K チャットに限らず、攻撃者の手口は変化が非常に速く、攻撃者が優位であると言われています。攻撃手法に関する研究は数多くありますが、システム側に注目するケースが多く、ユーザー視点での研究は少ない印象です。

Y そのとおりです。ユーザーが陥りやすい要因を理解し、セキュリティ対策に応用することも重要だと考えています。そういった研究にも取り組みたいと考えています。また現在、社会人博士課程で早稲田大学で研究を進めています。そして、学術界ではどの会議で論文が採択されたかが重要視されるということを知りました。

K さまざまな会議にランクがあるということですね。

Y いわゆる Tier1、Tier2 に分類される会議、例えばUSENIX Security [※1] やNDSS [※2] などがあります。ユーザブルセキュリティ分野では、先にお話したHCI の研究も含まれます。なるべくランクの高い会議に挑戦していきたいと考えています。

K そうした会議で発表される論文の数は、まだまだ日本と海外で大きな開きがあると聞きますが、その理由として感じているものはありますか？

Y これは自分にも当てはまるのですが、英語で文章を書くことに慣れていないという点があります。これを克服するためには、英語力を高めることはもちろんですが、海外の論文をより多く読ん

で分析することが重要と感じています。

K 組織からのサポートはいかがですか。

Y チャレンジしたいことに対して、多くの方々がサポートしてくださり、大変ありがたく感じています。実際に多くの機会をいただき、可能性を伸ばしてもらえる環境と文化がある企業だと思います。

K 今後取り組みたいことや将来について教えてください。

Y 個人的には、有用な研究ができるように、まずはスキルを磨き、研究者として成長したいと考えています。また、ユーザブルセキュリティに積極的に取り組み、ユーザーがセキュリティに関して抱えている課題やセキュリティに携わる専門家の方々に貢献したいと思っています。また、その重要性を広く伝えることで、コミュニティの発展にも貢献したいという思いがあります。

K 本日はありがとうございました。

※ 1 **USENIX Security Symposium**：https://www.usenix.org/conference/usenixsecurity24
米国の非営利団体 USENIX Association が主催する世界有数の学術会議。システムセキュリティ、プライバシー、暗号技術など、各分野の最新の研究成果が発表される場であり、セキュリティ分野ではトップ会議の 1 つと位置づけられている。

※ 2 **Network and Distributed System Security（NDSS）Symposium**：https://www.ndss-symposium.org/
非営利の国際団体 Internet Society（ISOC）が主催する学術会議。USENIX Security と同様にセキュリティ分野のトップ会議の 1 つとして位置づけられている。

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

Hitachi Systems CSI（Cyber Security Intelligence）Watch 2024.11

文＝日立システムズ

サプライチェーンセキュリティ評価制度について

【概要】：企業のセキュリティリスク管理において、サプライチェーンに特化した評価基準は確立されていない。取引先ごとに求められる対策が異なるため、統一的なリスク評価が困難な状況である。この課題を解決すべく、経済産業省は「サプライチェーン対策評価制度」（以下、本制度）として、評価基準の統一化を進めている。本稿では、本制度の概要や既存ガイドラインとの違い、および利活用について考察する。

【内容】：企業のセキュリティリスク管理は「サイバーセキュリティ経営ガイドライン」に基づき推進されてきたが、取引先のセキュリティ評価基準については各企業の判断に委ねられてきた。一方、政府は「政府情報システムのためのセキュリティ評価制度」を導入し、調達製品やサービスのセキュリティ評価基準を整備している。海外ではサプライチェーンセキュリティ評価制度が確立されており、日本企業も国際的な競争力と信頼性の向上に向け対応が求められている。こうした背景から、経済産業省はサプライチェーン全体のセキュリティ評価基準の標準化を目ざし、2025年度に実証実験を目標とする新たな制度の整備を進めている。

この制度は、企業のサイバーセキュリティ対応能力を5段階で評価するもので、下位3段階を自主申告の「自己宣言型」、上位2段階を独立機関による「第三者認証型」とする柔軟な設計が特徴である（表1）。自己宣言型はコストが低く中小企業にも導入しやすい一方、信頼性に限界がある。これに対し、第三者認証型は高い信頼性を持つがコストと時間がかかるため、リスクの高い取引先に適している。

本制度は、米国のCMMC（Cybersecurity Maturity Model Certification）や英国のCyber Essentialsを参考にしている（表2）。CMMCは3段階のセキュリティ評価基準を導入しており、米国政府調達に関わる企業に必須の基準である。Cyber Essentialsは自己宣言型と第三者認証型を組合せた制度で、迅速かつコスト効率の良いセキュリティ評価を提供する制度となっている。

本制度を活用することで、自社のセキュリティレベルを明確化し競争力を高めるとともに、取引先との基準の共通認識を確立し、連携を強化することが可能となる。自社の求める評価段階に適合するための体制整備や基準とのギャップ分析、内部監査の強化が必要であり、取引先との評価基準の共有や協議体制の構築も重要である。こうした取り組みにより、サプライチェーン全体のセキュリティ向上とリスク管理の効率化が期待される。特にグローバル企業においては、多国間の取引先を対象に共通基準で評価するために、本制度の国際的な適用性が今後の課題となる。

表1 サプライチェーン対策評価制度の概要

評価段階	対策内容	主な対象事業者	認証方法
★1	基本的なセキュリティ対策（OSやソフトウェアを最新に保つ、ウイルス対策ソフトの導入など）	小規模企業	自己宣言型
★2	自社診断項目に基づく対策（基本的対策に加え、従業員教育や情報の持ち出し対策等、より包括的なセキュリティ対策）	中小企業	自己宣言型
★3	サプライチェーン全体で最低限実施すべき基本的なセキュリティ対策（初期侵入防止、基礎的なシステム防御策の実装など）	サプライチェーン企業	自己宣言型
★4	高度なサイバー攻撃に対応するため、標準的な組織的対策とシステム防御（ガバナンス、監視、インシデント対応など）	産業界を代表・牽引する立場の企業	自己宣言型 第三者認証型
★5	重要インフラ事業などに求められる最高レベルのサイバー攻撃に対応するためのセキュリティ対策（早期侵入検知、被害の極小化、システム全体の防御強化など）	重要インフラなど特に重要な機能・役割を担うサプライヤー機能	第三者認証型

表2 国内外の評価制度

制度	対象企業	評価方法
経済産業省 サプライチェーン対策評価制度	全企業	自己宣言型と第三者認証型（5段階の評価基準）
CMMC	政府調達に関わる企業	第三者認証型（3段階の評価基準）
Cyber Essentials	全企業	自己宣言型と第三者認証型

［情報源］

https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_supply_chain/index.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

3. Web サイト／インフラ調査編

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。前々号（Vol.63）より「OSINT体験」と題して、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。

前回は、Web データ収集編として、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した。

今回は、Web サイト／インフラ調査編としてツールなどを用いた Web サイトやインフラに対する情報収集の手法やツールを紹介していきます。

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（本稿で紹介する IP アドレスや URL の一部は文字列を置換したり記号をカッコでくくるなどの加工を施しています）。

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. IP レピュテーションサービスを用いた不審な IP アドレス調査

CSIRT や SOC でイベント分析やインシデントレスポンスを行う際、攻撃元の IP アドレスやドメイン情報から攻撃者の情報を深堀して調査することがあります。例えば、C&C サーバーの IP アドレスから攻撃者が使用するツールやマルウェアなどを調査して IoC を確認し、攻撃の痕跡が自組織にないか、感染端末の絞り込みを行うためにネットワーク機器や端末のログを調査したりします。IP レピュテーションサービスは、IP アドレスに関する評判や信頼性を評価し、セキュリティ対策やリスク管理に役立つサービスです。メリットとして、以下が挙げられます。

1. セキュリティ対策の強化
攻撃元の IP アドレスからの通信を事前にブロックすることで、攻撃リスクを軽減できます。サービスによっては、API や Splunk の App が提供されており、自動的にブラックリストとして取り込み、ノイズをフィルタリングすることができます。

2. スパムフィルタリング
スパムメールやフィッシングメールの送信元 IP アドレスを検出し、メールサーバーでのスパム対策を強化できます。

3. パフォーマンスの向上
信頼性の低い IP アドレスからの通信を制限することで、ネットワークのパフォーマンスを維持できます。

4. インテリジェンス情報
インテリジェンスを元にしたリアルタイムの IP レピュテーション情報を得ることで、迅速な対策が可能となります。

上記のメリットを記載しましたが、使用時の注意点として以下も考えられます。

1. 誤検知のリスク
IP レピュテーションサービスは、安全な IP アドレスを悪意がある IP アドｃレスとして評価すること（False Positive）があります。悪意のある IP アドレスを安全なものとして評価する場合もあるため、他のセキュリティ対策と組み合わせて使用することが重要です。

2. プライバシーの懸念
一部のサービスは、ユーザーの IP アドレスやトラフィックデータを収集し、分析することがあります。プライバシーポリシーを確認し、オプトアウトを検討してください。

3. コスト
商用の IP レピュテーションサービスは、有料で高価なことが多くコストが発生します。導入する目的や費用対効果を確認し評価することが必要です。

IP レピュテーションサービスは、数あるセキュリティ対策の 1 つであるため、他のセキュリティ対策と組み合わせることで強固な対策を講じることができます。次に、無料で使用できる IP レピュテーションサービスを紹介します。

2.1 GetIPIntel.net

GetIPIntel.net は、IP アドレスがプロキシ／VPN ／不正な IP である可能性を判断するサービスです。IP アドレスが与えられると、システムは 0 から 1 の値を返します。値が 1 の場合は、IP が GetIPIntel.net の動的リストによって明示的に禁止（Web ホスト、VPN、または TOR ノード）されていることを意味します。サービスは無料で提供されており、ホームページには、「手頃な価格で良い代替品が見つからなかったため、このプロジェクトを作成しました。」と記載されています。また、API も用意されているため、システムに取り込むことも可能です。

Web インターフェイスを用いて IP レピュテーションを確認する方法を図 1 に示します。GetIPIntel.net（hxxps[:]//getipintel[.]net/）のホームページから、「Simple Web Interface IP Lookup page」をクリックすると、IP アドレスを Lookup できる画面に遷移します。Google Puplic DNS の 8[.]8.8.8 を Lookup した結果、スコア 0 が表示されましたが、Tor Exit node の IP アドレスはスコア 1 が表示されました。サービス作成者は、高い値 (0.99 を超える値、または 0.995 を超える値) に対してのみ自動アクションをお勧めしていますが、高い値を返す IP は常に手動で確認することを推奨しています。

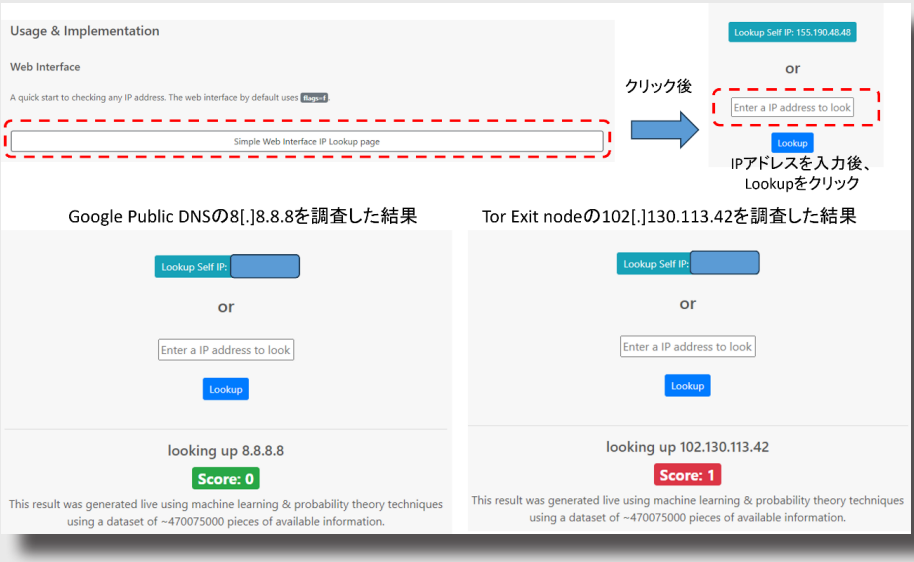
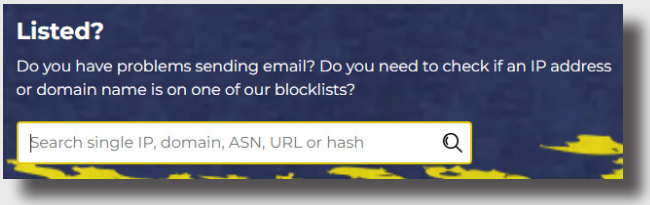


図 1　GetIPIntel.net で IP アドレスを調査した結果を比較
hxxps[:]//getipintel.net/free-proxy-vpn-tor-ip-lookup/#web

2.2 SPAMHAUS

不審な IP アドレスとドメインのリストを提供し、フィルタリングやブロックに適用できるサービスです。フィッシングサイトや不審な通信先を発見した際には、報告できるフォームも用意されており、SPAMHAUS の Project に貢献できます。



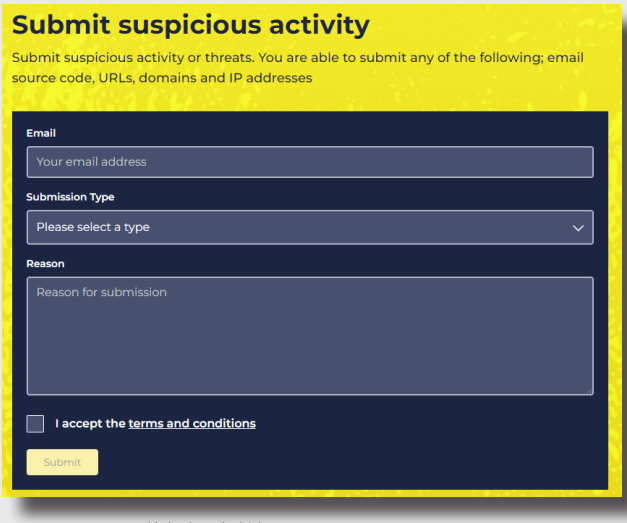


図 2 SPAMHAUS の検索ページ（上）hxxps[:]//www[.]spamhaus.org/
登録フォーム（下）hxxps[:]//www[.]spamhaus.org/submit

フィッシングを疑うメール図 3（次ページ）を受信した際に、SPAMHAUS を用いて調査を行なってみます。メールヘッダーを見ると、117[.]69.190.253 から始まるメールサーバーから送信されました。また、メール中に記載された「ご利用確認はこちら」のリンクをするとフィッシングサイト「www[.]01fq.cn」に飛びます。IP アドレスとドメインを検索します。

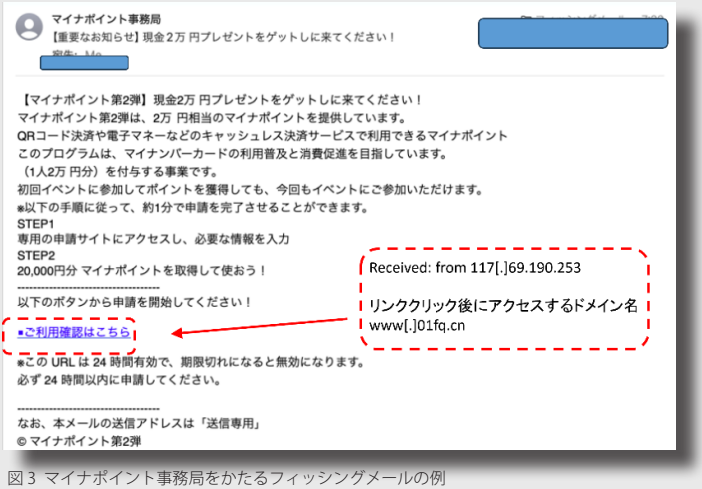


図 3 マイナポイント事務局をかたるフィッシングメールの例

IP アドレスとドメインを SPAMHAUS で検索した結果を図 4 に示します。IP アドレスとドメイン名は、SPAMHAUS のブロックリストに含まれていることがわかり、不審な送信元からのメールでリンク先も信用できない可能性があることがわかります。より確度を高めるためには、他のデータベースを参照し、実際にフィッシングサイトにアクセスしてソースコードを解析するなどする必要があります。

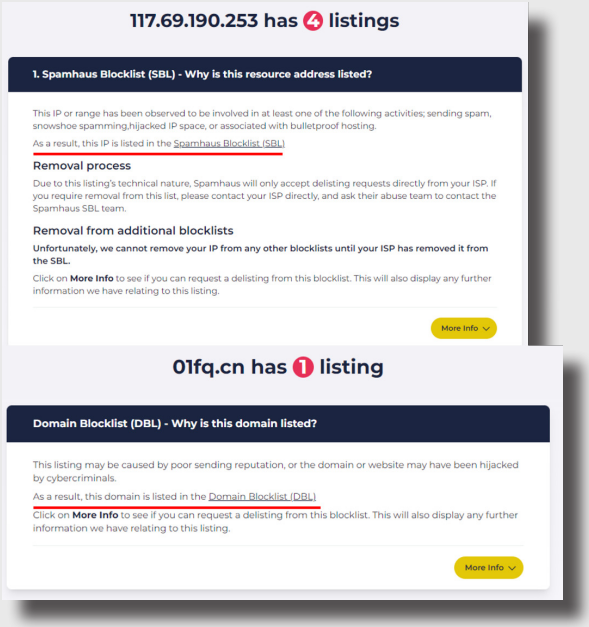


図 4 SPAMHAUS を用いた IP アドレスとドメインのレピュテーション評価

2.3 その他サービス

2.3.1 IPQualityScore.com（IPQS）

IP アドレスのスコアを特定するだけではなく、電子メールの検証やプロキシ／ VPN の検証ができるサービスです。検証するには無料アカウントの登録が必要ですが、さまざまなツールが使用できるので、ぜひ登録して試してみてください。API のユースケースも提供されており、例えば、プロキシ検出では、住宅プロキシ、プライベート VPN ネットワーク、Tor ノード、匿名プロキシ、ボットネット、およびボットによって悪用される悪意のある IP アドレスや危険な IP 範囲などを検出が可能です。

hxxps[:]//www.ipqualityscore.com/

2.3.2 CISCO TALOS

IP アドレスの他に、URL やドメイン、ファイルのハッシュ値などを検索できるインテリジェンス検索サービスです。

hxxps[:]//www[.]talosintelligence.com/reputation_center

2.3.3 Greynoise

Mirai などの Botnet 活動を行うものや Shodan や Censys などの有償サービスのスキャン元 IP、研究機関の IP などタグ付けがされているので、日々 SOC などで大量のアラートを対処している解析者がノイズ軽減するために使用するのに役立ちます。

hxxps[:]//viz[.]greynoise.io/

3. Web インフラ調査

3.1 Amass

Amass（hxxps[:]//github[.]com/owasp-amass/amass/tree/master）というオープンソースを用いた Web インフラの調査を紹介します。OWASP Amass プロジェクトは、オープン ソースの情報収集とアクティブ偵察技術を使用して、攻撃対象領域のネットワーク マッピングと外部資産の検出を実行します。表 1 （次ページ）に示すように、多くのデータベースを元に調査を実施できます。

表 1　Amass で情報収集に使用している技術一覧

技術	データソース
APIs	360PassiveDNS, Ahrefs, AnubisDB, BeVigil, BinaryEdge, BufferOver, BuiltWith, C99, Chaos, CIRCL, DNSDB, DNSRepo, Deepinfo, Detectify, FOFA, FullHunt, GitHub, GitLab, GrepApp, Greynoise, HackerTarget, Hunter, IntelX, LeakIX, Maltiverse, Mnemonic, Netlas, Pastebin, PassiveTotal, PentestTools, Pulsedive, Quake, SOCRadar, Searchcode, Shodan, Spamhaus, Sublist3rAPI, SubdomainCenter, ThreatBook, ThreatMiner, URLScan, VirusTotal, Yandex, ZETAlytics, ZoomEye
Certificates	Active pulls (optional), Censys, CertCentral, CertSpotter, Crtsh, Digitorus, FacebookCT
DNS	Brute forcing, Reverse DNS sweeping, NSEC zone walking, Zone transfers, FQDN alterations/permutations, FQDN Similarity-based Guessing
Routing	ASNLookup, BGPTools, BGPView, BigDataCloud, IPdata, IPinfo, RADb, Robtex, ShadowServer, TeamCymru
Scraping	AbuseIPDB, Ask, Baidu, Bing, CSP Header, DNSDumpster, DNSHistory, DNSSpy, DuckDuckGo, Gists, Google, HackerOne, HyperStat, PKey, RapidDNS, Riddler, Searx, SiteDossier, Yahoo
Web Archives	Arquivo, CommonCrawl, HAW, PublicWWW, UKWebArchive, Wayback
WHOIS	AlienVault, AskDNS, DNSlytics, ONYPHE, SecurityTrails, SpyOnWeb, WhoisXMLAPI

まずは、「Vol. 5-1 第五部 OSINT 体験 環境準備編」の「3.1. OSINT 調査環境の準備」で用意した仮想環境にログインし、以下のコマンドで amass をインストールしてください。

```
$ sudo apt update
$ sudo apt upgrade
$ sudo apt install amass

#Do you want to notinue? [Y/n] が表示されたら、y を入力して Enter
# 途中で設定を聞かれる項目があればデフォルトの設定で進めてください
```

インストールが完了後、Amass を用いて調査対象のサブドメインを列挙してみます。本誌 Vol. 63 Let's Try OSINT 体験 1. 環境準備編」の「3.3. VPN を用いたアクセス元 IP の変更方法」で仮想環境の VPN 設定を行い、以下のコマンドを実行してください。今回は調査対象として日立システムズのドメイン「hitachi-systems.com」を対象にしています。

```
$ amass intel
$ amass enum
# 使用方法が表示される

$ amass enum –d hitachi–systems.com
#amass 実行
```

Amassのサブコマンドは、表2に示すようにいくつか用意されています。上記のコマンドは、「enum」でDNSとネットワークのマッピングを行うものです。

表2 Amassのサブコマンド

サブコマンド	説明
intel	対象組織の調査のためにオープンソースの情報を収集する
enum	インターネットに公開されているシステムのDNS列挙とネットワークマッピングを実行する
db	列挙結果を保存するグラフデータベースを管理する

実行完了には時間がかかりますが、図5のようにhitachi-systems.comに関連するIPアドレスやドメインの一覧を取得できます。攻撃者はこのようなツールで攻撃対象のインフラを調査し、攻撃対象を選定します。

```
┌──(osint㉿tlosint)-[~/Desktop]
└─$ amass enum -d hitachi-systems.com
hitachi-systems.com (FQDN) --> ns_record --> a3-66.akam.net (FQDN)
hitachi-systems.com (FQDN) --> ns_record --> a1-47.akam.net (FQDN)
hitachi-systems.com (FQDN) --> ns_record --> a24-64.akam.net (FQDN)
hitachi-systems.com (FQDN) --> ns_record --> a28-65.akam.net (FQDN)
hitachi-systems.com (FQDN) --> ns_record --> a16-67.akam.net (FQDN)
hitachi-systems.com (FQDN) --> ns_record --> a13-66.akam.net (FQDN)
a24-64.akam.net (FQDN) --> a_record --> 2.16.130.64 (IPAddress)
a24-64.akam.net (FQDN) --> aaaa_record --> 2600:1480:9800::40 (IPAddress)
shayukai.hitachi-systems.com (FQDN) --> cname_record --> d2by70ajnp73as.cloudfront.net (FQDN)
d2by70ajnp73as.cloudfront.net (FQDN) --> a_record --> 99.86.91.12 (IPAddress)
d2by70ajnp73as.cloudfront.net (FQDN) --> a_record --> 99.86.91.40 (IPAddress)
d2by70ajnp73as.cloudfront.net (FQDN) --> a_record --> 99.86.91.107 (IPAddress)
d2by70ajnp73as.cloudfront.net (FQDN) --> a_record --> 99.86.91.105 (IPAddress)
d2by70ajnp73as.cloudfront.net (FQDN) --> aaaa_record --> 2600:9000:21ee:8e00:1a:88cc:5d00:93a1 (IPAddress)
d2by70ajnp73as.cloudfront.net (FQDN) --> aaaa_record --> 2600:9000:21ee:f400:1a:88cc:5d00:93a1 (IPAddress)
d2by70ajnp73as.cloudfront.net (FQDN) --> aaaa_record --> 2600:9000:21ee:3800:1a:88cc:5d00:93a1 (IPAddress)
d2by70ajnp73as.cloudfront.net (FQDN) --> aaaa_record --> 2600:9000:21ee:4200:1a:88cc:5d00:93a1 (IPAddress)
d2by70ajnp73as.cloudfront.net (FQDN) --> aaaa_record --> 2600:9000:21ee:5e00:1a:88cc:5d00:93a1 (IPAddress)
d2by70ajnp73as.cloudfront.net (FQDN) --> aaaa_record --> 2600:9000:21ee:6200:1a:88cc:5d00:93a1 (IPAddress)
d2by70ajnp73as.cloudfront.net (FQDN) --> aaaa_record --> 2600:9000:21ee:7000:1a:88cc:5d00:93a1 (IPAddress)
d2by70ajnp73as.cloudfront.net (FQDN) --> aaaa_record --> 2600:9000:21ee:7200:1a:88cc:5d00:93a1 (IPAddress)
portal2.support.hitachi-systems.com (FQDN) --> a_record --> 20.89.239.38 (IPAddress)
arcweb02.support.hitachi-systems.com (FQDN) --> a_record --> 203.81.14.8 (IPAddress)
2.16.130.0/24 (Netblock) --> contains --> 2.16.130.64 (IPAddress)
21342 (ASN) --> managed_by --> AKAMAI-ASN2 (RIROrganization)
21342 (ASN) --> announces --> 2.16.130.0/24 (Netblock)
```

図5 Amassでhitachi-systemsのサブドメインを調査した結果（一部抜粋）

Amass ではその他にも、図 6 のように指定したドメイン名を検索できるデータソースをリスト化したり、図 7 のように指定した組織が管理する ASN をリスト化したりなど引数によって多くの情報を取得することができます。
ユーザーガイド（hxxps[:]//github[.]com/owasp-amass/amass/blob/master/doc/user_guide.md）に使用例が記載されているので、確認してコマンドを試してみてください。

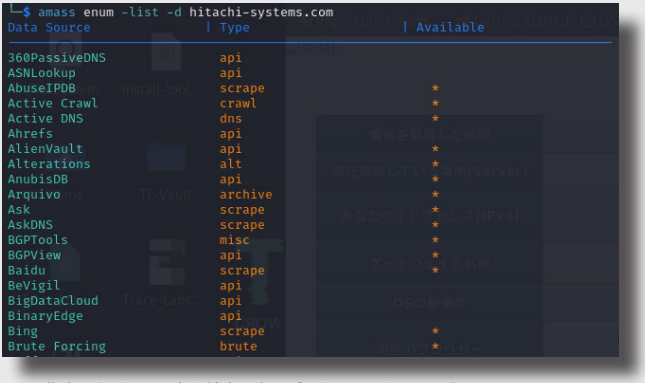


図 6　指定したドメイン名を検索できるデータソースをリスト化

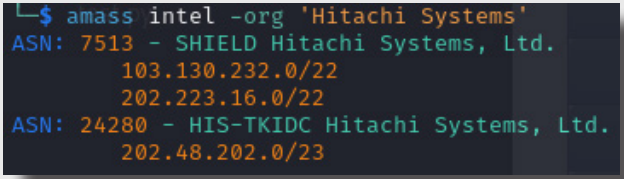


図 7 指定した組織が管理する ASN をリスト化

4. おわりに

今回は、OSINT 体験「Web サイト／インフラ調査編」として、ツールなどを用いて Web サイト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した。OSINT 体験は今回で終了ですが、OSINT 用のツールは他にも数多く存在します。チーム内での調査の目的に応じてツールを調査して、使いやすいツールを探してみることもお勧めします。

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.65

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