HITACHI
Inspire the Next

Hitachi Systems Security Journal

VOL.64

株式会社 日立システムズ

Human * IT

Hitachi Systems Security Journal VOL.64

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

ネットワークの脅威を可視化・分析し、セキュリティ向上に貢献
数々のシステム開発の指揮を執る

NICT サイバーセキュリティ研究所 研究所長

井上 大介
インタビュー

Daisuke Inoue

サイバーセキュリティの世界に接している人ならば、SF 作品に登場しそうなカッコイイ UI（ユーザー・インターフェイス）のネットワーク可視化システムを、一度くらいは目にしたことがあるだろう。NICTER（ニクター）・DAEDALUS（ダイダロス）・NIRVANA 改（ニルヴァーナ・カイ）etc. これらは皆、国立研究開発法人情報通信研究機構（NICT：エヌ・アイ・シー・ティー）サイバーセキュリティ研究所で開発されたシステムだ。
今回は、研究所長を務める井上大介氏に、これらのシステムについて話を伺った。開発の背景や思想を知ることでシステム間のつながりがより鮮明に見えてくるだろう。
また、NICT が注力する CYNEX（サイネックス）についても紹介いただいた。産官学の連携でサイバーセキュリティの結節点をめざすこの取り組みはどのようなものなのだろうか。

取材・文・撮影 = 斉藤 健一

セキュリティを研究のテーマに据えた意外な理由とは？

斉藤（以下 S ）：井上さんのプロフィールを拝見すると、大学時代にセキュリティ分野の研究を開始とありました。このきっかけについて教えてください。

井上（以下 I ）：実はセキュリティ分野は自ら進んで選んだわけではなかったのです。大学では電子情報系の学科に在籍していました。4 年生で研究室に配属されるのですが、成績順で決まる仕組みとなっていました。自慢できる話ではありませんが、学部生時代の私は、学業以外のことに熱中していました。ビデオゲームだったり、テクノミュージックの研究会を作ったり、イタリアのサッカーチームのファンサイトを運営したりしていました。ですから、成績はあまり思わしくなかったのです。

S それは意外に感じました。ただ、さまざまなことに熱中する気質については納得できるような気がします。

I 当時の人気は移動体通信関連でした。ちょうど携帯電話の通信システムが第 2 世代から第 3 世代へと移行する時期でした。当然、私の成績では入れません。それでも、情報系の研究室に入りたいという希望は持っていましたから、人気のなさそうな研究室を探したのです。そして、それがセキュリティだったというわけです。

S 現在だと、セキュリティはメジャーな研究テーマで、卒業後の進路も引く手あまたですが、当時の人気はそれほどでもなかったのですね。

I 当時の認識は、セキュリティはお金にならないと考えられていました。仮にセキュリティを研究したとしても、就職氷河期ということもあり、卒業後の進路が定まらないおそれがありました。また、指導教員が厳しいという噂もあり、自ら進んで志願する学生は少なかったように思います。

S 指導教員はどなたですか。

I 松本勉先生です。日本の暗号研究の大家で、現在は産業技術総合研究所（産総研）のサイバーフィジカルセキュリティ研究センター（CPSEC）の研究センター長を務められています。実際厳しい指導をされる教授でしたが、先見の明がありました。当時のセキュリティといえば暗号だったのですが、暗号に限らず、好きなことを研究してもよいという雰囲気でした。そこで私はネットワークのセキュリティを研究テーマに据えたのです。

S 大学院博士課程修了後、独立行政法人通信総合研究所（現 NICT）に入所されるわけですが、その経緯を教えて下さい。

I 大学院生時代、通信総合研究所の方と共同研究を行ってたのが縁で、入所することになりました。

S どのような研究だったのでしょうか。

I 当時の私は、ステガノグラフィの研究を行っていました。秘匿したい情報を他の情報の中に埋め込む技術のことです。新しいメディアやファイルフォーマットが登場するたびに、情報をどのように隠せる

井上 大介（いのうえ・だいすけ）
1997 年 横浜国立大学でセキュリティ分野の研究開発を始め、2003 年 同大学大学院工学研究科 博士課程後期修了後、独立行政法人 通信総合研究所（現 国立研究開発法人 情報通信研究機構）に入所。2006 年よりインシデント分析センター “NICTER”（ニクター）を核としたサイバーセキュリティの研究開発に従事。以降、対サイバー攻撃アラートシステム “DAEDALUS”（ダイダロス）、サイバー攻撃統合分析プラットフォーム “NIRVANA 改 ”（ニルヴァーナ・カイ）、サイバー攻撃誘引基盤 “STARDUST”（スターダスト）、Web 媒介型攻撃対策プロジェクト “WarpDrive”（ワープドライヴ）、セキュリティ情報融合基盤 “CURE”（キュア）など、先進的なセキュリティシステムの研究開発を続けるとともに、社会への実展開を進めている。博士（工学）。

かを試していました。私は音楽ファイルに情報を埋め込む方法を研究していましたが、共同でテキストファイルにも情報を埋め込む研究をしていました。日本語の冗長性を利用し、漢字や平仮名の違いで1ビットの情報を埋め込むことが可能で、どれだけ情報を隠せるかを調べていました。

S 興味深い研究ですね。テキストファイルに情報を隠す場合、元のテキストファイルのサイズに対して、どれくらいの割合まで情報を埋め込むことが可能なのでしょうか。

I 多くの情報を隠すと、テキストの内容から人間の眼でも怪しいとわかってしまいます。研究では、自然な感じであれば数%ほどという結果に落ち着きました。

S 研究に対する周囲の反応はいかがでしたか。

I 当時は「何に使うのか」と研究の有用性に疑念を抱かれることが多くありました。テロリストが隠された通信チャネルを使用する場合、どれほど見つけにくいのかを事前に研究して理解しておく必要があり、そうした技術を把握することで、対テロ対策に役立てることが重要だと説明したのですが、当時はアメリカ同時多発テロ事件の発生前で「テロなんて本当に起きるの？」という牧歌的な雰囲気でした。

S 現在は脅威アクターが当たり前のようにステガノグラフィを使っていますね。

I 1990年代後半は、情報セキュリティの脅威が現実の社会に影響を及ぼすものだと認識されていなかった時代です。2000年に中央省庁のWebサイトの大規模な書き換えが起きて、政府もセキュリティについてきちんと研究すべきだと考えるきっかけになった時期だったと思います。

NICTが提供するさまざまなサイバーセキュリティのシステム

S NICTでは、NICTERをはじめ、DAEDALUS、NIRVANA改、STARDUST、WarpDriveなど、サイバーセキュリティに関連したさまざまなシステムを開発・運営されています。ただ、一般の読者からすると、名前を聞いただけではピンと来ないと思いますので、それぞれのシステムについて簡単に説明していただけますか？

I さまざまなシステムを開発しています。図1を見ていただくとわかりますが、縦横2つの軸があります。横軸はグローバル・ローカルを表しています。グローバル側は、無差別型攻撃の観測を主としており、ローカル側は組織内部を精密に観測していきます。また、縦軸はパッシブ・アクティブを表しています。パッシブはわれわれが受け取った攻撃を解析するもので、アクティブは能動的に情報を収集して解析を行います。

S それでは各システムについて説明をお願いします。

・NICTER（ニクター：Network Incident analysis Center for Tactical Emergency Response）

I まず、NICTERです（次ページ図2）。グローバル・パッシブに位置します。2005年頃からスタートした無差別型攻撃の観測システムです。NICTER

図1 NICTが提供するシステムのマトリックス表

は、未使用のIPアドレス空間であるダークネット※1を観測し、通常の通信が行われないはずの空間に飛んでくる不正な通信を捉えます。主に、マルウェアなどに感染した機器が次の感染対象を探すために行うスキャン攻撃が観測されます。このシステムは、世界的に拡散したワーム型攻撃の広がりや影響をデータとして正確に把握することを目的に開発されました。現在では30万ほどのIPアドレスを観測しています。

S 2000年代初頭には、Code Red※2・Nimda※3・Blaster※4など、数々のワームが世間を騒がせました。ちなみに、IPアドレス30万という規模は世界的に見ても大規模なのでしょうか？

I セキュリティの観測を専門に行うという点では大規模な部類に入ると思います。ただ、数字だけを見れば、米国ではIPアドレスのクラスA全体を観測しているシステムもあり、約1670万にも及ぶものがあります。ですが、反対にそのIPアドレスのクラスは観測されていることがあらかじめ判明しているというデメリットもあります。NICTERではさまざまな組織から使用していないIPアドレスをお借りしていますから、センシングポイントがばらけているという特徴があります。

・DAEDALUS（ダイダロス：Direct Alert Environment for Darknet And Livenet Unified Security）

I 続いてDAEDALUSです（次ページ図3）。NICTERと同様にこのシステムもグローバル・パッシブに位置します。DAEDALUSは、未使用のIPアドレス空間（ダークネット）に向けて発生する不審な通信を観測し、組織内の機器が外部に対して無差別型のスキャン攻撃を行っているかどうかを検知します。この仕組みは、従来のネットワーク境界での防御モデルとは異なり、すでに組織内部でマルウェア感染が発生した後にその機器が外部に攻撃を仕掛ける際の通信を検知する点が特徴です。

S なるほど。NICTERとDAEDALUSは同じシステムを利用しつつも視点が異なるのですね。NICTERは受信するパケットを観測、一方のDAEDALUSは発信するIPアドレスを観測して、発信元のIPアドレスの所有者にマルウェア感染などの警告を発するわけですね。

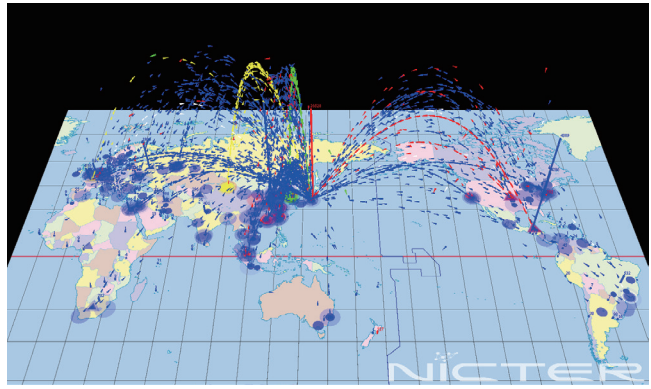

図2 NICTERにより可視化された日本への無差別攻撃の状況

※1 **ダークネット**：インターネットで到達可能なグローバルIP空間のうち、どのネットワークやコンピューターにも割り当てられていない未使用のアドレス群のこと。Torなどを用いて通信を匿名化したネットワークを指す「ダークWeb」とは異なる。

※2 **Code Red（コード・レッド）**：2001年7月にインターネットで猛威を振るったワーム。マイクロソフトIIS Webサーバーを攻撃対象に感染を拡大させた。

※3 **Nimda（ニムダ）**：2001年9月に感染が拡大したワームで、ファイルに感染するコンピューターウイルスでもある。名称は「admin」を逆から綴ったもの。Windowsのぜい弱性やCode Redワームなどのバックドアを利用するなど、複数の感染方法があり、短期間にインターネットに拡散した。

※4 **Blaster（ブラスター）**：2003年8月に感染を広げたワーム。Windowsのぜい弱性を悪用し、ファイル共有などに用いられるTCP135（Remote Procedure Call）からシステムに侵入した。

I はい。DAEDALUS は 2013 年に地方自治体向けのアラートサービスとして開始され、当初は 47 自治体が参加していましたが、現在では 770 を超える自治体が利用しています。システムは、各自治体から提供された IP アドレスを観測対象にセットし、不正な通信が検知された場合に即座にアラートを送信することで、感染機器の早期発見と対策を促進しています。

S 自治体から見ると、自組織の IP アドレスを登録するだけですから、お手軽と言えます。

I システムの開発当初、ネットワーク境界での防御が主流であったため、DAEDALUS の仕組みはすぐには広く受け入れられませんでした。しかし、2012 年頃から可視化システムを開発し、わかりやすい形で提示することにより、徐々に利用者が増加しました。このシステムの効果的なアラート機能により、多くの組織がマルウェア感染を早期に検知し、対策を講じることが可能となりました。

・NIRVANA 改（ニルヴァーナ・カイ：NICTER Real-network Visual ANAlyzer KAI）

I ローカル・パッシブに位置するのが NIRVANA 改です（図 4）。開発が始まったのは 2006 年・2007 年ごろです。NICT では、ネットワークの展示会である Interop に出展していますが、NICTER の技術を応用して ShowNet という会場内のネッ

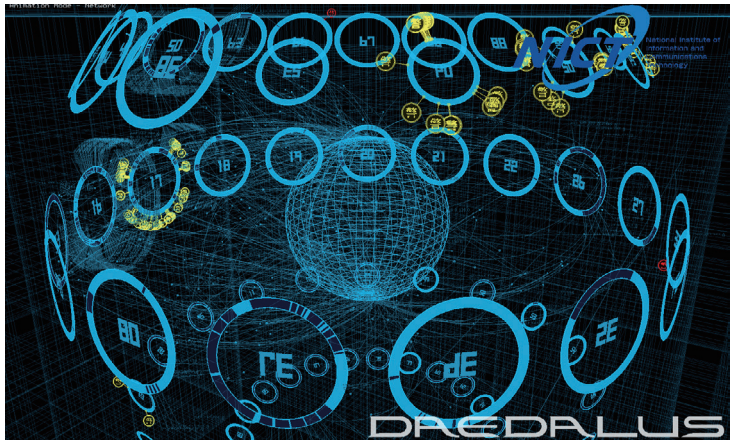

図 3 DAEDALUS は組織内の機器がマルウェア感染によって発信する攻撃パケットを検知しアラートを発報する

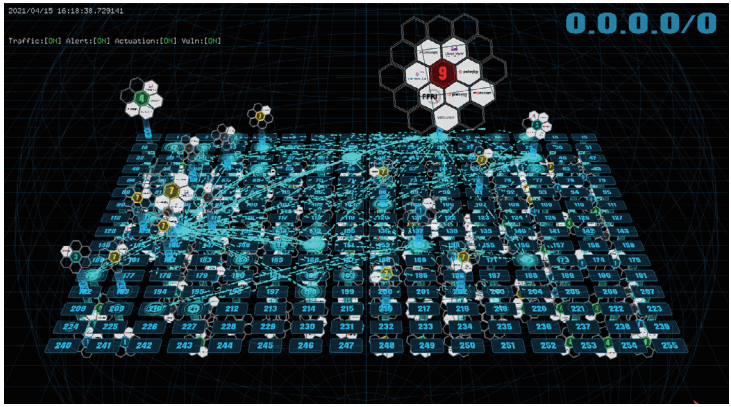

図 4 NIRVANA 改は組織内ネットワークのトラフィックを可視化し、各種セキュリティ機器が発報するアラートの集約・分類・分析を行う

トワーク・トラフィックを可視化するデモを行っていました。それを見た来場者から「この可視化技術を組織のネットワーク管理に使ってみては？」と提案されたことがきっかけです。

S 確かに。可視化することでトラブルなども見つけやすくなりますね。

I NIRVANA 改の特徴の 1 つは、アラートも可視化できるという点です。当時の ShowNet には、さまざまなセキュリティ企業がアプライアンスを持ち込んでおり、それらを一元的に管理する必要がありました。そこで、NIRVANA 改でアラートを集約することに取り組み、各社のアプライアンスからのアラートを表示するだけではなく、分析もできるようにしました。

S ネットワークの可視化にとどまらず、サイバー攻撃の分析にまで踏み込んだ点に感心しました。

・WarpDrive（ワープドライヴ：Web - based Attack Response with Practical and Deployable Reserch InitiatiVE）

I グローバル・アクティブに WarpDrive というプロジェクトがあります（図 5）。2009 年の GUMBLAR※5 を契機に、インターネット上でのドライブバイダウンロード攻撃※6 を観測するためにプロジェクトが始まりました。Web 媒介型攻撃を捉えるためには、Web ブラウザーとアクセスする Web サイト間の通信を観測する必要があり、日本国内でその仕組みが欠如していることが問題視されました。この解決策として、Web ブラウザーにプラグインを導入し、Web ブラウザーをセンサーとして機能させる実証実験が行われました。

S 攻殻機動隊とコラボレーションされていますね。

I 実験開始当初は、参加ユーザーが定着せず、うまく進みませんでした。そこで「攻殻機動隊」とコラボレーションし、「タチコマ」をモチーフにして、ユーザーの関心を引く取り組みが行われました。これにより「WarpDrive」プロジェクトが始まり、現在では 1 日あたり約 700 万 URL へアクセスする状況となっています。

・STARDUST（スターダスト）

I ローカル・アクティブに位置するのが STARDUST です（次ページ図 6）。STARDUST は、

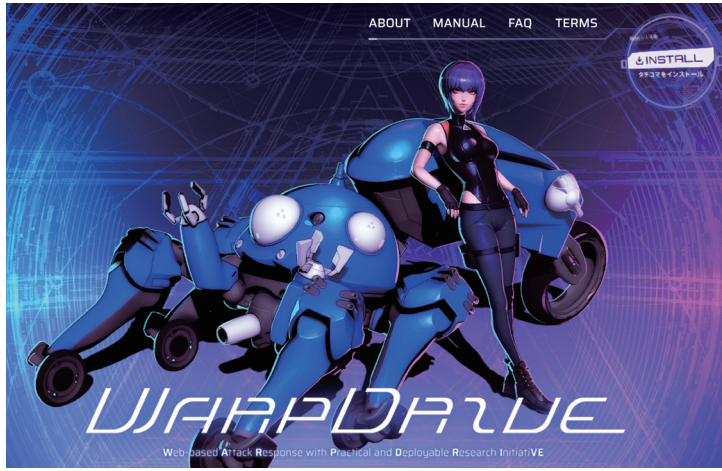

図 5 WarpDrive のポータルサイト（https://warpdrive-project.jp/）

※5 **Gumblar（ガンブラー）**：Web サイトの改ざんとマルウェアを組み合わせて感染拡大を狙う攻撃手口、および攻撃に使用されるマルウェア。2009 年 3 月頃から被害が確認されはじめた。日本国内においても大手企業の Web サイトが改ざん被害を受けたことから、被害が拡大した。

※6 **ドライブバイダウンロード攻撃**：Web ブラウザーなどを介して、ユーザーに気付かれないようにマルウェアをダウンロードさせる攻撃手法。

人間の攻撃者を引き込んで観測するための基盤であり、標的型攻撃の目的や手法を明らかにするために設計されています。単にマルウェアによる初期侵入の解析だけでは攻撃者の目的がわからないため、攻撃者をダミー空間に誘導し、どのようなソフトウェアやテクニックを使うのか、何を狙っているのかを観測します。当初、標的型攻撃に対して過剰な対策が提案されていましたが、実際には初期の攻撃者はそれほど高度な技術を持たない人が多いことが判明し、正確なデータに基づいた対策が必要とされていました。

S 確かに。攻撃者の活動が 9 時から 17 時までに限られ、まるで勤め人だと話題になったこともあ

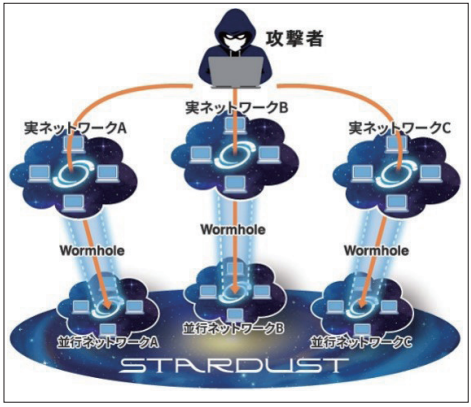

図 6 STARDUST のイメージ図

りました。

• CURE（キュア：Cybersecurity Universal RE – pository）

I これまで紹介してきたように、NICT では多種多様なセキュリティ情報を収集してきました。CURE はこれらの情報を一元的に集約して横断分析するセキュリティ情報融合基盤です（図 7）。CURE では、IP アドレスの過去の使用履歴や攻撃の関連性を簡単に把握できるデータベースが作成されており、従来は多くの時間を要したデータベースの照合が自動化され、1 つの IP アドレスに対する詳細な情報が即座に提供されます。

S さまざまな情報をつなぎ合わせることによってサイバー脅威の全体像が見えやすくなりますね。

I はい。さらに新機能も開発しています。本年 6 月には Watcher というカスタム通知機能について発表を行いました。

S Watcher とはどのような機能なのでしょうか。

I 組織の IP アドレスとかドメイン、メールアドレス、漏えい・流出してしまったファイルのハッシュなどを登録しておけば、CURE 内部で監視を行い、マッチすればアラートが届きます。DAEDALUS と同様の思想です。

S CURE はどの組織でも使えるのでしょうか。

I CYNEX の、Co-Nexus A と S の参画組織で希望があれば使えます。

S わかりました。CYNEX については後ほど伺い

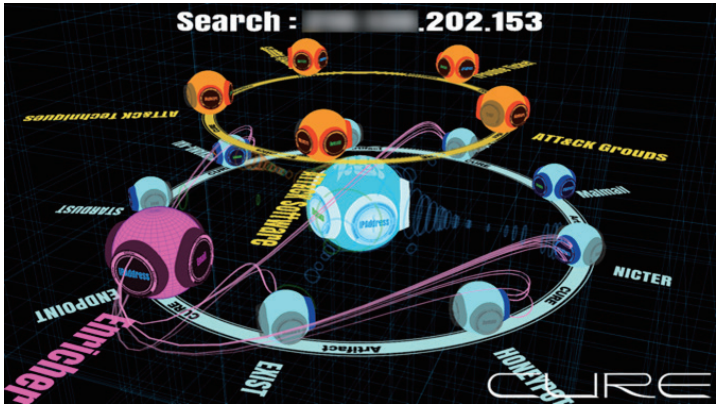

図 7 CURE では NICTER や STARDUST をはじめ多くの観測情報や分析情報を集約し、サイバー攻撃の全体像の解明や組織のセキュリティ向上に役立つ脅威情報の創出をめざす

サイバーセキュリティ研究所の所長に就任し、多忙な日々を送る井上氏だが、スケジュールの合間を縫ってインタビューにご協力いただいた

たいと思います。今回、各システムの開発の背景や経緯を説明いただくことで、それぞれのつながりがより鮮明に見えるようになり、非常に参考になりました。

システムの UI やネーミングに対するこだわり

S これまで説明いただいた各サービスは、サイバー空間を独創的に表現した UI（ユーザー・インターフェイス）を持っており、ネーミングセンスも独特に感じます。これらのこだわりについて教えてください。

I UI については、DAEDALUS がターニングポイントになっています。一般の人にもわかりやすいアラートの仕組みを可視化することが目的でした。デザインは私が担当し、OpenGL というグラフィック・ライブラリが使えるエンジニアと共に開発しました。そもそも凝ったデザインにしたつもりはないのですが、研究室でお披露目したところ全員から「ドン引き」されました（笑）。

S これまでの UI とは一線を画するまったく新しいものを見て、戸惑ったのかもしれません。

I ところが、2012 年の Interop で DAEDALUS を発表した際にはかなり話題になりました。YouTube に動画が投稿され、海外からも注目が集まりました。動画のコメントには「俺たちの知っている日本が帰ってきたぜ！」といった声も寄せられました。当時、日本の技術が海外向けに発信されることが少なくなっていたので、驚いた人が多かったのだと思います。

S 本当にカッコイイ UI です。前述の攻殻機動隊の作品中にそのまま登場したとしてもまったく違和感ありません。

I この可視化エンジンは、必要な情報をシンプルに表示しているだけで、無駄な装飾や関係ない情報は追加していません。機能美を追求した結果、日本的なデザインが生まれたのではないかと感じています。

S ネーミングの方はいかがですか。

I ネーミングのポイントは、システムの特徴が何かを徹底して考え抜くことです。そして、出てきた単語をうまく並べて、何かに近づけていきます。例えば、DAEDALUS の正式名称は、Direct Alert Environment for Darknet And Livenet Unified Security ですが、これはギリシャ神話に登場する有名な大工さんの名前になぞらえています。

S ネーミングの由来はとても興味深いお話です。

I さらに最も重要なのは、名前を普及させるフェーズです。同僚や上司の前で「ダイダロス」と言い続けます。最初は笑われるのですが、それでも続けていくと彼らの方から「ダイダロスの件だけど…」という風に使ってくれるようになるのです。

S ネーミングの決め方から普及にいたるまで、井上さんのメソッドがあるからこそ、次々と独創的なものが生まれるのですね。

I 余談ですが、ギリシャ神話に登場する神々の名は、セキュリティ製品で使われることが多くなり、徐々に難しくなってきています。

サイバーセキュリティの結節点をめざす CYNEX

S CYNEX（サイネックス：CYbersecurity NEXus）設立の背景・経緯について簡単にご紹介下さい。

I 設立の背景には、日本におけるサイバーセキュリティの自給率低迷という課題があります。日本

では、海外のセキュリティ技術を導入して運用することが主流となっています。専門家の中には、国内自給率が 1%以下との意見もあり、海外製品への過度な依存が国家安全保障の観点からも問題視されています。

S これまで私がインタビューしてきたセキュリティ専門家の中にも、同様の指摘をする方々がいらっしゃいました。

I その要因の 1 つに、日本国内のサイバーセキュリティのデータ不足が挙げられます。新しい攻撃に対応するための観測体制を整えるには長い時間がかかり、リアルタイムでのデータが不足しているため、研究開発や人材育成も進まないという「負のスパイラル」が発生しているのです。

S おっしゃるとおりです。

I このスパイラルを断ち切るためには、データを収集・分析し、国産製品を実データに基づいて検証・テストする仕組みが必要です。さらに、人材育成についても、海外の高額なプラットフォームに依存しており、大学や組織での育成が難しい現状があります。これらの課題を解決するために、NICT では国内でのデータ収集・分析・製品検証・人材育成を包括的に進める仕組みを構築しようとしています。

S それが CYNEX につながるのですね。

I はい。NICT 単独でサイバーセキュリティのすべてを担うのは難しいため、産官学の連携による結節点「NEXUS」を構築し、企業や政府、教育機関と協力しています。昨年 10 月に「CYNEX アライアンス」を立ち上げ、現在までに約 73 組織が参加しています。これにより、データ共有と人材育成を進める取り組みを強化しています。

S CYNEX の活動内容を簡単に教えてください。

I CYNEX ではプロジェクトを 4 つに分け、それぞれ「Co－Nexus A・S・E・C」の名称で活動を行っています（図 8）。「Co－Nexus A」は、サイバーセキュリティ情報の収集と解析者のコミュニティ醸成の支援。「Co－Nexus S」は、国産脅威情報の提供と高度 SOC 人材の育成プログラム。「Co－Nexus E」は、国産セキュリティ製品の検証やフィードバック。そして「Co－Nexus C」はサイバーセキュリティ演習のオープンプラットフォーム化となっています。

S 民間企業や教育機関から CYNEX に参加するとどんなメリットがありますか。

I CYNEX でもっとも人気なのが「Co－Nexus C」です。これは、サイバー演習用のハードウェア環境とコンテンツのセットで、大学や民間企業などで広く活用されています。セキュリティの専門家でない教員でも授業を行えるよう、サイバー演習用スライドや、その解説コメントなどが整備され

Co-Nexus A（Accumulation & Analysis）

NICTER・STARDUST・WarpDrive などの各種観測機構を活用し、サイバーセキュリティ情報の収集・蓄積を行う。また、国内解析者コミュニティを醸成し、共同分析の実現を目指す。

Co-Nexus S（Security Opreration & Sharing）

解析者と機械学習エンジンの連携で異種データの横断分析を行い、国産の脅威情報の生成と提供を行う。また、高度 SOC 人材育成プログラムを構築、SOC 人材の育成拠点を形成する。

Co-Nexus E（Evaluation）

NICT のネットワーク環境に国産セキュリティ製品のプロトタイプを導入し、長期運用を通じて機能検証と製品へのフィードバックを行い、国産セキュリティ製品の創出と普及を支援する。

Co-Nexus C（CYROP：Cyber Range Open Platform）

国内におけるセキュリティ人材育成のハードルを下げるため、演習シナリオや遠隔演習システムをオープン化し、教育機関や民間企業におけるセキュリティ人材育成事業の推進を行う。

図 8 CYNEX の活動内容：4 つの Co－Nexus

た教材が 70 種類以上も提供されています。この教材により、教員はスライドを使うだけで授業を進められることができ、コンテンツ作成の負担が軽減され、授業の質が向上しています。

S 確かに、教育機関などにとっては大きなメリットがありますね。

I また、「Co－Nexus S」では、CYNEX の解析チームの中で 2 年にわたって OJT コースを学んでいただいたり、「Co－Nexus E」では、企業が開発した製品に対して NICT のレッドチームが模擬攻撃を行いレポートの作成を行ったりしています。

S 説明を伺いましたが、CYNEX はとても「コスパ」が高いサービスだと感じました。もっと多くの組織に知れ渡ることを願っています。

日本のセキュリティ分野の国際競争力向上のために

S 本年 4 月、サイバーセキュリティ研究所の所長に就任されました。これまで研究者としてキャリアを歩んでこられて、今度は所長というマネジメント職に就かれました。何か違和感などはありますか。

I 所長就任以前から、サイバーセキュリティ研究室の室長を 13 年間務めていました。プレイングマネージャーとして働いていたので、所長に就任したといっても特に違和感はありません。強いていえば、出席すべき会議が圧倒的に増えたことでしょうか（笑）。

S 今後の目標などあれば教えてください。

I 学術の世界で 4 大セキュリティ会議の 1 つといわれる USENIX Security ※7 は、毎年 1000 人規模の参加者が集まる重要なカンファレンスです。今年の採択論文数は 2000 件以上の応募のうち 417 件（18.3%）で、日本からの採択はわずか 4 件に留まっています。一方で韓国は 16 件、中国は著者の半数以上を占める状況です。日本のセキュリティ研究は依然として世界への発信力が不足しており、今後は日本全体で研究力を高め、国際的に発信する流れを作ることが求められています。

S 論文数はその国の研究力を示す指標ともいわれます。論文数の低下にはさまざまな理由が考えられるとは思いますが、由々しき事態ですね。

I その意味において、CYNEX として日本のセキュリティ分野の強化に貢献していきたいと考えます。前述のように、政府や企業で使用されているセキュリティ機器やサービスの多くが海外製品に依存しており、国産製品の開発と導入が急務です。政府が国産製品を積極的に採用すれば、民間企業も国産セキュリティ製品を開発しやすくなります。また、大学との共同研究や人材育成を通じて、産官学が連携するエコシステムを構築することで、イノベーションを促進し、ひいては国際競争力の向上にもつながると考えているからです。

S 本日はありがとうございました。

※ 7 **USENIX Security**：https://www.usenix.org/conference/usenixsecurity24

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 2024.09

文＝日立システムズ

国際会議で発表された生成 AI に関するセキュリティリスクや活用の検討

【概要】：世界最大級のサイバーセキュリティ国際会議の 1 つ、BlackHat USA※1 では、生成 AI や大規模言語モデル（LLM）のセキュリティ対策への活用例や、AI のセキュリティリスクに関わる発表が数多くあった。また、政府主導で AI サイバーチャレンジ（AIxCC※2）が開催され、AI 開発と利用の促進のため企業と連携して取り組んでいる。

【内容】：2024 年 8 月開催の BlackHat USA では、120 ものサイバーセキュリティに関する研究成果が発表された。AI に関する講演が多く、脅威分析・自動化・規制・プライバシー・AI への攻撃など、話題は多岐にわたる。ここでは、研究者・ハッカーの視点から研究された内容を紹介する。また、BlackHat 後の DEFCON にて米国防総省の国防高等研究計画局（DARPA）の新技術研究開発の一環として開催された AI サイバーチャレンジ（AIxCC）の取り組みを紹介する。

・LLM を用いた脅威ハンティング

LLM の活用は、テキスト要約や SOC の分析自動化など多岐にわたるが、本研究は攻撃者が用いるマルウェアのファイル名／文字列／機械語を学習した LLM を用いて、攻撃者が使用する他のマルウェアやツールを見つけ出す手法が紹介された。従来は、マルウェアを解析した結果や、インシデント対応時の痕跡（IoC）など大量の情報を分析する必要があるが、LLM の活用で効率化を図ることができる。

・Copilot への攻撃手法

Microsoft 社が提供する生成 AI プラットフォームである Copilot が学習したデータに含まれる社内 DB などの機密情報が盗み出される手法が紹介された。根本的な原因は、従来のクラウド環境と同様の設定不備やぜい弱性によるものであり、初期状態で脆弱な設定の項目もあった。生成 AI サービス提供する際には、Secure by Design / Default の概念に沿って、セキュリティを開発プロセスに盛り込み、導入時に安全な設定を行うことが必要となる。

・DAPRA が開催する AI サイバーチャレンジ（AIxCC）

DARPA は、技術革新を加速させるために「報奨金付きチャレンジプログラム」を開催しているが、今回は AI サイバーチャレンジ（以下、AIxCC）を実施した。DEFCON では、AIxCC の準決勝が行われ、上位 7 チームがそれぞれ賞金 200 万ドル（約 2.9 億円）を獲得し、来年度の決勝へと駒を進めた。ただし、開発したシステムをオープンソフトウェア（OSS）として寄贈することが必須の条件となっている。本チャレンジの開催は、既成概念にとらわれない思考の推奨や、幅広い層の参加を促すといった公益につながる一方で、DARPA にとっても経済的メリット（参加チームが費やす時間が賞金額を上回る）があるという。AIxCC の目的は、AI システムの開発を支援することで、イノベーションを加速させ、大手 AI 企業（Anthropic、Google、Microsoft、OpenAI）やオープンソースコミュニティが連携することで、重要インフラやソフトウェアサプライチェーンのセキュリティ対策を行うことにある。この背景には、アメリカにおける他国との AI に懸念、例えば、AI 技術の分断化等の対立、といった安全保障上の懸念が関わっていると推察できる。

BlackHat や DEFCON で発表された生成 AI・LLM の最新情報を収集するとともに、国内外の AI に関わる政策方針にも注目していく。

［情報源］

※ 1 https://www.blackhat.com/us-24/briefings/schedule/

※ 2 https://www.darpa.mil/news-events/2024-08-11

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

2. Web データ収集編

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。前号より「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。

前回は、環境準備編として、OSINT（Open - Source Intelligence）や OPSEC（Operational Security）の概念や、OSINT 調査を実行する環境を準備しました。

今回は、Web データ収集編として、Google Dorks と Web アーカイブサイトなど、Web のデータを調査する方法を紹介します。

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. Web ブラウザーを用いた情報収集

2.1 Google を用いた情報収集

2.1.1 Google Dorks

Google Dorks（Google Hacking）は、特殊な演算子を使用してインターネット上の特定の隠された情報を検索する技術です。Google 検索では、検索の絞り込みまたは検索ターゲットの指定に使用できる複数の検索演算子がサポートされているため、これらの演算子を用いて情報収集する方法を説明します。

表 1 に Google Dorks で用いる演算子の一例を示します。完全一致（AND）や部分一致（OR）で検索する方法はすでにご存じかもしれませんが、ファイル拡張子の指定や検索する Web サイトの制限、URL に含まれる文字列などの条件を組み合わせることができます。図 1 に Google Dorks を用いた検索例を示します。セキュリティというワードが Web ページに含まれている中で、特定のドメインに絞り込み、拡張子 pdf/xlsx/docx のファイルを検索しています。このように Google Dorks を活用することで膨大な情報から特定の情報を絞り込むことができます。

表 1 Google Dorks で用いる演算子の一例

演算子	機能	例
“[文字列]”	指定した文字列を完全一致で含むサイト検索	“Cyber Security”
[文字列1] or [文字列2]	文字列1か文字列2を含むサイトを検索	CVE-2017-11822 or CVE-2017-0199
-[文字列]	文字列を除外した結果を検索	“CVE-2017-0199” -Emotet
site	特定のサイトに結果を制限させる	site:hitachi-systems.com
filetype:[拡張子]	ファイル拡張子を持つ結果のみを検索	filetype:pdf site:hitachi-systems.com
cache:[url]	最新のサイトのキャッシュを検索	cache:hitachi-systems.com
intitle:[文字列]	タイトルに文字列を含むサイトを検索	intitle:"Cyber Security"
inurl:[文字列]	URLに文字列が含まれるサイトを検索	inurl:security site:hitachi-systems.com
intext:[文字列]	特定の文字列が含まれるサイトを検索	intext:"CSF 2.0"

図 1 Google Dorks の検索例

Google Dorks は OSINT 調査だけではなく、攻撃者によっても悪用されます。図 2 に示すのは Google Dorks のデータベースが用意された Web サイトであり、ぜい弱性のあるサーバーやファイルを検索するための検索例がまとまっています。攻撃者はインターネット上からぜい弱性のある組織や Web サイトを調査するために Google Dorks を悪用します。防御側もこれらの技術を用いることで組織が公開すべきではない情報が誤って外部から閲覧可能な状態になっていないかを確認できます。最近は、外部アタックサーフェス管理（EASM、External Attack Surface Management）と呼ばれる言葉も出てきています※ 1。EASM は、インターネットに面している内部ビジネス資産を特定し、攻撃者に悪用される可能性のあるぜい弱性、パブリッククラウドの誤設定、漏えいした認証情報、その他の外部情報やプロセスを監視するプロセスを指します。EASM を活用するメリットとして、「リスクの軽減」、「コンプライアンスの維持」、「ぜい弱性の管理」、「クラウドでの安全な運用」などが挙げられます。

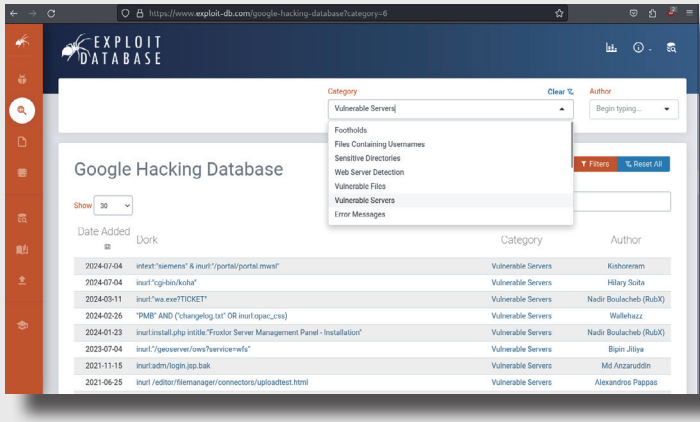

図 2　Google Hacking Database（https://www.exploit-db.com/google-hacking-database）

その他にも、Google Dorks をまとめた DorkSearch.com※ 2 や、図 3 のように Google の検索フォームで組み合わせて検索する手法を GUI 上で検索条件を設定できる Web サイトも存在します。皆さんもいろいろと検索を試して結果を確認してみて下さい。

図 3　Google Advanced Search (https://www.google.com/advanced_search)

※ 1 https://www.rapid7.com/ja/fundamentals/external-attack-surface-management-easm/
※ 2 https://dorkserch.com/

2.1.2 Google Alerts

Google Dorks でさまざまな条件を用いて検索できることを説明しました。条件に一致した検索結果を自動で通知したい場合、Google Alerts をお勧めします。Google Alerts を使用するには Google アカウントが必要ですが、ログインすると図 4 のように検索条件に該当した結果を指定したメールアドレスに通知させることができます。これにより、自組織のドメインで機密情報などを含むファイルが外部から閲覧可能になっていないかを監視し、アラートを飛ばすことが可能となります。

図 4　Google Alerts（https://www.google.com/alerts）と検索条件の設定例

2.2 Web アーカイブ

Google Dorks を用いてさまざまな情報を検索できることがわかりましたが、すでに Web サイトが閉じて検索結果を取得できない場合があります。この場合に、Web アーカイブを調査することで過去にさかのぼって Web サイトの情報を確認できます。Web アーカイブを用いる理由として、他にも以下に挙げる理由が考えられます。

- Web サイトに直接アクセスしたくない（またはアクセスできない）場合
- Web ブラウザーからアクセスできる Web サイトのアーカイブを保存したい場合
- Web サイトが以前の時点でどのようになっていたかを確認したい場合

2.2.1 Web Archives

Google では、Web キャッシュ機能があり過去の Web サイトをキャッシュで確認することが過去にはできました。現在、Web キャッシュ機能がなくなったため Web ブラウザー上ではデフォルトでキャッシュが確認できなくなりましたが、アドオンである「Web Archives」を用いることで Web サイトのキャッシュを Web ブラウザーから確認できます。「Web Archives」はさまざまな Web ブラウザー用にプラグインを用意されていますが、本稿では Firefox のアドオンを用います。次の URL（https://addons.mozilla.org/ja/firefox/addon/view-page-archive/）にアクセスし、図 5 にしたがって Firefox に「Web Archives」を設定します。

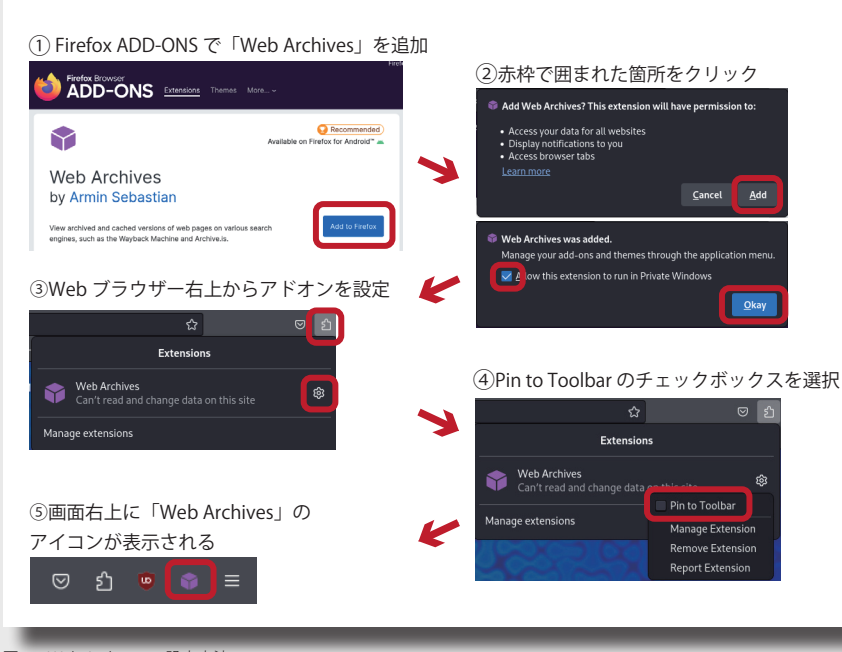

図 5：Web Archives の設定方法

図 6 に「Web Archive」の使用例を示します。Web ブラウザー上で検索した結果のキャッシュを確認したい場合、検索結果のリンク上で右クリックし、「Web Archives」を選択します。すると、いくつかの検索エンジンが右側に表示されますが、今回は Google のアイコンをクリックします。すると、図 7 に示すように Web サイトのキャッシュが表示されます。「Web Archives」では、Google の他に Yandex や Bing などのキャッシュも確認できます。一番上の「All Search Engines」をクリックするとすべてのエンジンのキャッシュがタブで表示されるため、結果を比較してみてください。

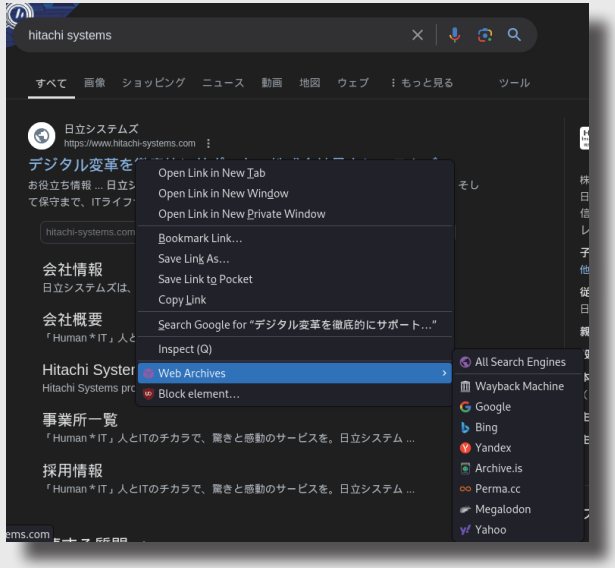

図 6 Web Archives の使い方

図 7 検索した Web サイトの Web Archives でのキャッシュ

2.2.2 Wayback Machine

「Web Archive」を用いて検索エンジンでの検索結果からキャッシュを検索する方法を説明しましたが、独自に Web アーカイブを取得してデータベース化してくれている Web サイトが存在します。今回は、図 8 に示す「Wayback Machine」を紹介します。図 9 は「Wayback Machine」で hitachi-systems.com のアーカイブを検索した結果です。カレンダー形式で Web アーカイブが保存されている日が確認できます。この中から、確認したい日付をクリックすることで当時の Web サイトを確認することができます。

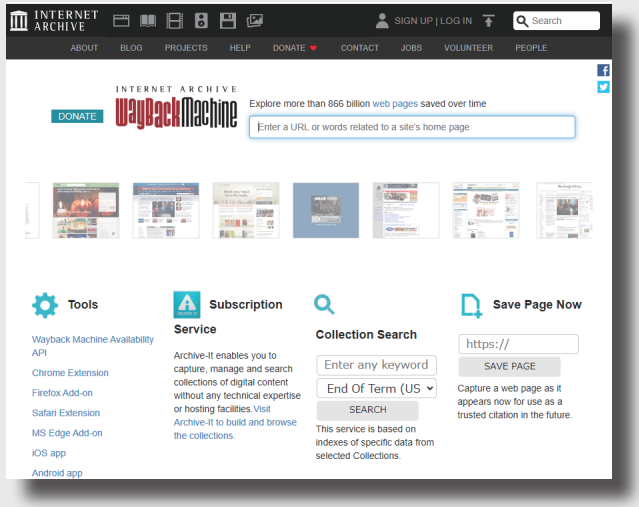

図 8 Wayback Machine（https://archive.org/）

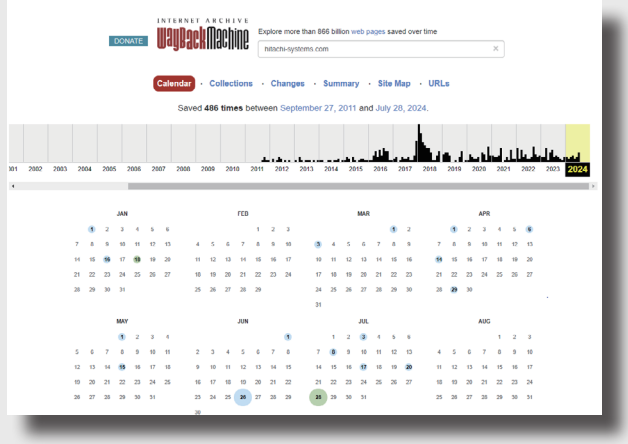

図 9 Web アーカイブの取得回数と日時

「Wayback Machine」では、2 つの Web アーカイブから結果を比較することもできます。図 10 のように【Changes】のタブをクリック後、2 つの日付を選択して【Compare】とすると、結果を横並びにして比較することもできます。現在と過去で Web サイトの構成や表示の変更が可視化されて比較しやすくできます。

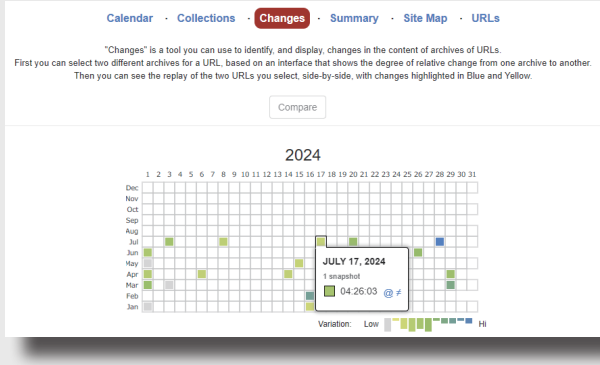

図 10 Web アーカイブの比較（左：2024/7/28、右：2011/9/27）

国立国会図書館のインターネット資料収集保存事業では、世界各国の Web アーカイブサイトを紹介してくれています（次ページ 図 11）。「Wayback Machine」以外にもさまざまな Web サイトがあるため、Web アーカイブを検索する際には、複数の Web サイトで検索すると結果を取得できる可能性が高まります。

図 11 国立国会図書館 インターネット資料収集保存事業（世界の Web アーカイブ）
（https://warp.ndl.go.jp/contents/reccommend/world_wa/index.html）

2.2.3 urlscan.io

urlscan.io（図 12）は、Web サイトをスキャンしてさまざまな情報を表示してくれるオンラインサービスです。調査したい URL を検索することで、urlscan.io が代わりにアクセスしてスキャンを行い、IP アドレスや HTTP レスポンスの情報を確認することができます。例えば、自組織にフィッシングを疑う不審なメールが届いた場合、直接アクセスするのではなく、urlscan.io の Public Scan を実施することで、Web サイトの画面やレスポンス情報を確認し、それらの情報を深堀して分析するなどに urlscan.io は活用できます。

図 12 urlscan.io のトップ画面

図 13 には、フィッシングサイトが疑われる URL をスキャンした結果を示します。右上に Web サイトの画面キャプチャーが表示されていますが、Google の検索サイトが表示されています。フィッシングサイトは、urlscan.io やその他オンラインスキャンサービスからのアクセスには、分析を妨害させるためにフィッシングサイトとは無関係な Google などへリダイレクトを行うことが多いため、このような結果になっています。また、表示された IP アドレスなどは外部サービスと連携されており、VirusTotal や Censys のページへ飛んで更なる情報を取得することも可能です。

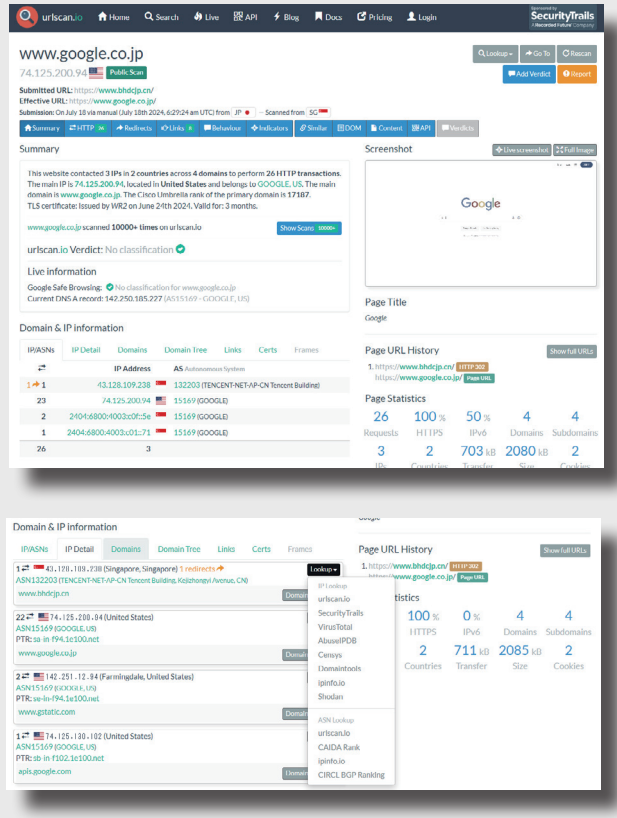

図 13　不審な URL をスキャンした結果

3. クラウドストレージバケットの調査

クラウドストレージバケットは、コンテンツを公開する目的で作成されるものなので、多くの場合公開されています。中には、非公開や限定公開をしたつもりが一般公開されている場合もあり、この場合は情報漏えいにつながる恐れがあります。図 14 に示す「Grayhatwarfare」は、Amazon や Microsoft のクラウドなどのストレージバケットをインデックス化して結果を検索可能にする Web サイトです。バケットの他にも短縮リンクのデータベースもあります。

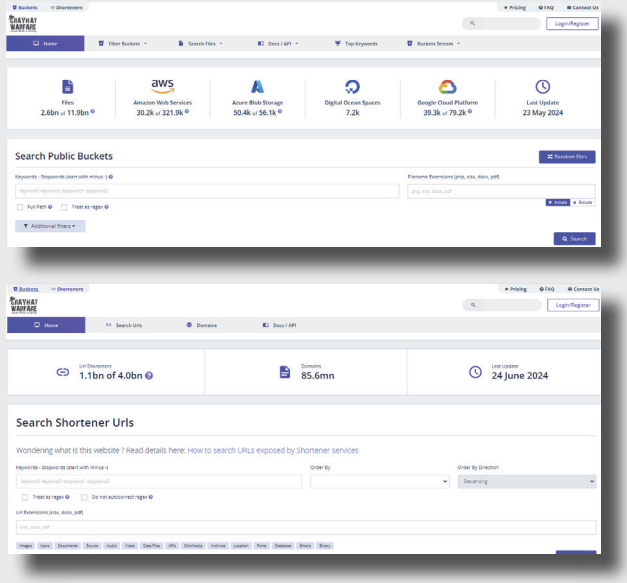

図 14「Grayhatwarfare」（https://buckets.grayhatwarfare.com/）の検索画面

キーワードに「security」、ファイル拡張子に「pdf」を指定してクラウドストレージバケットで検索した結果を図 15（次ページ）に示します。ファイル拡張子を指定するには無料アカウントが必要なため、事前に登録を実施しています。検索結果は、6687 件ですが、有償アカウントだと 3 万 3917 件結果が表示されるようになります。実際に検索結果からファイルの閲覧やダウンロードをするには、機密情報やマルウェアが含まれる場合や、卑わいな画像や児童ポルノが含まれる場合があるため注意が必要です。国の法令によってはダウンロードして保存することが違反する場合もあるため、実際にファイルをダウンロードする際には法令部門などとの調整が必要となります。

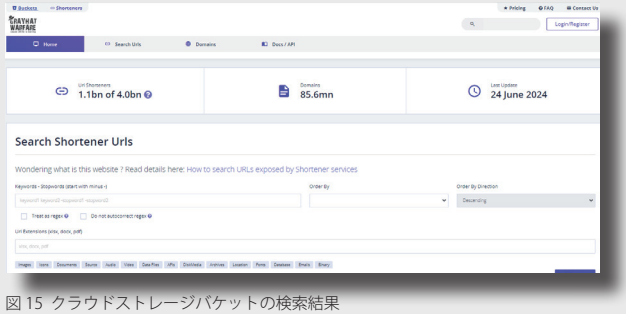

図 15 クラウドストレージバケットの検索結果

5. おわりに

今回はここまでとなります。今回は、OSINT 体験「Web データ収集編」として、Web ブラウザーを用いた情報収集手法と、クラウドストレージの調査サイトを紹介しました。次回は「Web ／インフラ調査」を紹介します。

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.64

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