2　サイバーセキュリティ技術
2　Cybersecurity Technology

2-1　サイバーセキュリティ研究室における研究開発
2-1　Overview of R&D Activities in Cybersecurity Laboratory

井上 大介　笠間 貴弘　高橋 健志
INOUE Daisuke, KASAMA Takahiro, and TAKAHASHI Takeshi

巧妙化・複雑化するサイバー攻撃に対抗するため、世界最先端のサイバー攻撃観測・分析・対策を可能にする技術基盤を構築し、実践的アプローチで社会課題の解決への貢献を目指す組織として、サイバーセキュリティ研究室は 2011 年に発足した。

2021 年から開始した第 5 期中長期計画においては、これまで 10 年以上にわたってサイバーセキュリティ研究室で実施してきた研究開発内容を更に発展させ、「データ駆動型サイバーセキュリティ技術」と「エマージングセキュリティ技術」の 2 つの研究の柱を立てて研究開発に取り組んでいる。本稿では、サイバーセキュリティ研究室の研究開発内容について概説する。

The cybersecurity laboratory was established in 2011 to research and develop countermeasure technologies against cyber-attacks and contribute to a safe and resilient society. In the 5th mid-and-long-term plan starting from 2021, the cybersecurity laboratory is further developing its research and development activities, which have been conducted over the past ten years, by establishing two research pillars: “data-driven cybersecurity technology” and “emerging security technology.” This paper outlines the research and development activities of the cybersecurity laboratory.

1　はじめに

日本初の商用インターネットサービスが開始された 1993 年から 30 年以上が経過し、もはやインターネットがない社会を想像することが難しいほどにインターネットは我々の社会の隅々にまで浸透している。その一方で、ICT 技術の発展に付随してサイバー攻撃の脅威も拡大の一途をたどっている。サイバー攻撃は悪意を持った人間が引き起こすものだが、そのためのツールとして使われるのがマルウェアと呼ばれる不正なプログラムである。

90 年代前半までマルウェアは愉快犯もしくは自己顕示を目的として作成・流布されることが多かったが、90 年代後半以降は金銭詐取を目的とした組織的な犯罪のツールとして利用され始め、高度化・巧妙化が急速に進んできた。これらのマルウェアに起因するサイバー攻撃に対抗するために、我々は長年、サイバー攻撃や標的型攻撃をリアルタイムで把握し適切な対応を実施するための観測・分析・対策技術の研究開発を進めてきた。一方、従来から継続するサイバー攻撃に加え、新たに社会に登場する ICT 技術に対する脅威も登場している。

そこで第 5 期中長期計画において、サイバーセキュリティ研究室では、無差別型攻撃や標的型攻撃をはじめとする多種多様なサイバー攻撃を観測する技術、状況把握を支える可視化技術、機械学習等の AI 技術を駆使した自動分析・自動対策技術の確立・高度化を進める「データ駆動型サイバーセキュリティ技術」と、新たに社会に登場する技術（IoT 機器、コネクテッドカー、Beyond 5G 等）やヒトに注目したユーザブルセキュリティに関するセキュリティ課題抽出や対策を進める「エマージングセキュリティ技術」の 2 つを研究開発の柱として研究開発を進めている。本稿では、この 2 つの軸に基づいて我々の研究テーマを紹介する。

2　データ駆動型サイバーセキュリティ技術の研究開発

我々はサイバー攻撃のトレンドの変化等に対応した技術開発を迅速に進めるため多種多様なサイバー攻撃

を観測する技術を開発している。これらの観測技術を通じて日々収集されるセキュリティビッグデータを基に、サイバー攻撃の状況把握のための可視化技術、AI技術を駆使した自動分析技術を研究開発し、得られた知見を活用した対策技術の展開につなげている。

2.1　無差別型攻撃対策

我々はインターネット上で発生する無差別型攻撃を観測・分析するシステムとしてNICTER（ニクター）の研究開発を推進している。NICTERでは世界最大規模の約30万アドレスの観測網を国内外に構築し、IoT機器の大規模感染をはじめとする新たな攻撃の兆候を迅速に発見可能なシステムを構築している。NICTER観測結果の詳細については「**2-2-1**　ダークネット観測システムNICTERの持続的進化とIoTマルウェアの隆盛」の記事を参照いただきたい。

NICTERによる観測・分析情報は、JPCERT/CC、IPA、@Police、国内大学等が参画組織であるSIGMON（定点観測友の会）、国内ISPによるDoS攻撃への迅速な対応と協調対処を行うワーキンググループ及び総務省・ISP・NICTが実施するNOTICEプロジェクトなどに情報共有を行っている。加えて、NICTER観測網を基に組織のマルウェア感染機器を検知しアラートを発報するDAEDALUS（ダイダロス）システムを定常運用し、地方自治体や政府関係組織へのアラート提供を行っている。

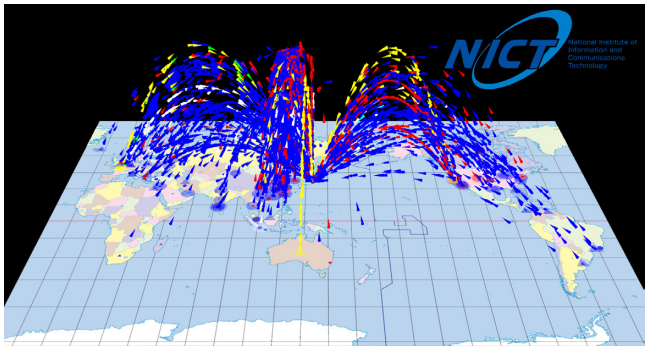

図1　インシデント分析センターNICTER

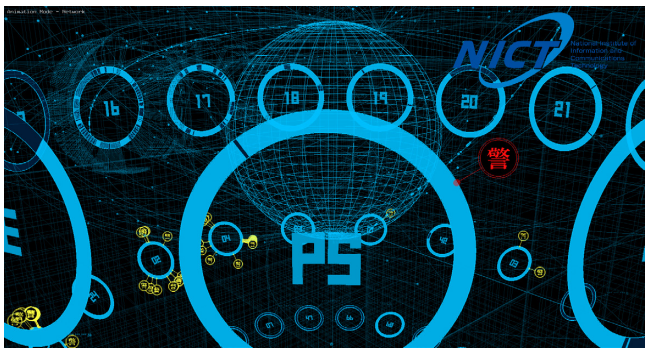

図2　対サイバー攻撃アラートシステムDAEDALUS

2.2　標的型攻撃対策

特定の組織を狙う標的型攻撃への対策技術の確立に向けて、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）の開発を進めている。NIRVANA改は組織内トラフィックのリアルタイム観測と分析機能に加え、各種セキュリティアプライアンス群からのアラート集約・可視化機能、アラート発生源へのドリルダウン機能、自動対策機能を備えたSIEM（Security Information and Event Management）システムである。我々はこのNIRVANA改をNICT CSIRT（Computer Security Incident Response Team）内に展開し、NICTの実ネットワークをテストベッドとした長期運用を通じてセキュリティオペレーション効率化のための改良や機能開発を実施している。

また、攻撃者による標的組織侵入後の攻撃活動を観測するために、実在する組織の環境を模擬したネットワーク内に標的型攻撃の攻撃者を誘引するための基盤であるSTARDUST（スターダスト）の研究開発を進めている。STARDUSTではNICTが保有する大規模サーバ群の上に仮想化技術を用いて実組織を模擬した「並行ネットワーク」を構築し、並行ネットワーク上の端末で標的型攻撃のマルウェアを実行したり標的型攻撃メールに記載された悪性URLにアクセスしたりすることで攻撃を発火させ、並行ネットワークに誘引した攻撃者の活動を観測することができる。STARDUSTの詳細については「**2-2-2**　攻撃者の行動を観測するためのサイバー攻撃誘引基盤STARDUST」の記事を参照いただきたい。

2.3　AI × サイバーセキュリティ

サイバーセキュリティ研究室では機械学習等のAI技術とサイバーセキュリティ技術を融合させた研究開発に取り組んでおり、独自に収集・蓄積したセキュリティビッグデータを用いた様々な研究活動を行っている。例えば、ダークネットトラフィックで観測されたスキャンパケットの同期性を分析することで、新たなマルウェア活動の発生を検知する技術（DARKTRACER）を開発している。そのほかにも、セキュリティアプライアンスが生成する大量のアラート情報を効果的にスクリーニングしセキュリティオペレーションを効率化する技術、JavaScriptの特徴を基にフィッシングサイトを高精度で検知する技術、多種多様なセキュリティ記事を入力として文書要約技術を用いてセキュリティキュレーション記事を自動生成する技術など、様々な研究開発を実施している。特にAI技術とサイバーセキュリティ分野の融合領域では国内外の研究組織との連携を積極的に進めながら研究開発を行っている。従来、AI技術を活用したセキュリティオペ

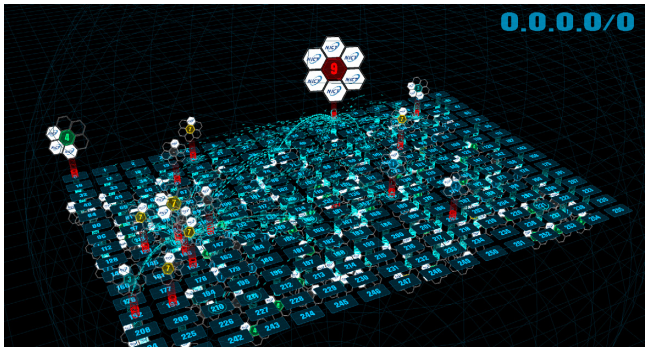

図 3　サイバー攻撃統合分析プラットフォーム NIRVANA 改

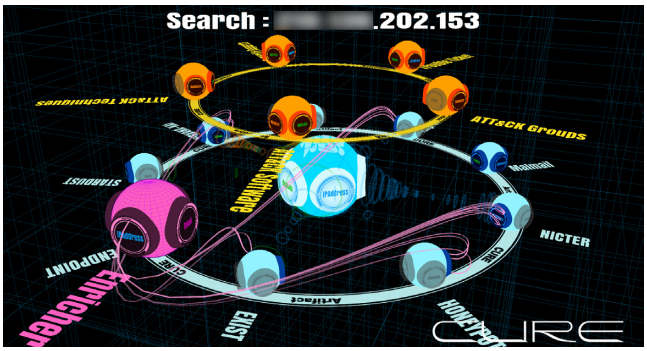

図 4　セキュリティ情報融合基盤 CURE

レーションの自動化技術の研究開発に注力してきたが、それらの技術が社会で広く利用されるためには、AI そのものに対する信頼性の構築が必要不可欠である。そのため近年では、AI そのもののセキュリティや、その判定結果に対する解釈可能性などを担保するための研究開発にも取り組んでいる。AI を活用した取組については「2-2-3　AI 技術を用いたデータ駆動型サイバーセキュリティ」の記事を参照いただきたい。

2.4　セキュリティ情報融合基盤 CURE

前述した、NICTER や NIRVANA 改、STARDUST をはじめとする各種サイバー攻撃観測システムで収集された情報は、セキュリティ情報融合基盤 CURE（キュア）に集約される。CURE は、サイバー攻撃観測情報を格納する Artifact レイヤ、自然言語で記述される分析情報を格納する Semantics レイヤ、2 つのレイヤに格納されたデータに対して付加的な情報を与えるデータエンリッチメントの仕組みとして Enricher の機能を備えている。CURE による情報集約と横断分析によって異なるサイバー攻撃間の関連性や類似性を特定し、サイバー攻撃の実態把握の精度向上と質の高い脅威情報の生成が行える。CURE の詳細については「2-2-4　セキュリティ情報融合基盤 CURE」の記事を参照いただきたい。

3　エマージングセキュリティ技術の研究開発

新たな技術が社会に登場する時、そこには新たな脅威が潜んでいる。IoT、クラウド、コネクテッドカー、自動運転、5G・Beyond 5G、VR・AR、生成 AI 等々、我々はこれらのエマージング技術に対して攻撃者側の視点を持ってセキュリティの脅威分析やセキュリティ検証技術・対策技術の研究開発を進めることで、攻撃者に先んじたセキュリティ対策の実現を目指している。

3.1　5G セキュリティ

5G の商用利用が開始され、「超高速大容量」「高信頼・低遅延」「多数同時接続」の特徴を持ったネットワークが普及し始めている。5G ネットワークでは多種多様なデバイスがつながり、自動運転や遠隔医療からスマート農業・スマートファクトリ、高精細映像制作など様々なサービスの実現が期待されている。しかしその一方で、新技術の導入によりこれまでの環境では想定していなかった新たなセキュリティ脅威の懸念が考えられる。そこで我々は、5G セキュリティ検証用テストベッドの整備を行い、5G 環境におけるセキュリティ脅威の検討とモデリング分析、緩和策等の技術の研究開発を実施している。5G セキュリティに関する取組の詳細については「2-3-1　5G ネットワークにおけるセキュリティ確保に向けた取組」の記事を参照いただきたい。

3.2　ローレイヤセキュリティ

IoT 機器の普及やサプライチェーンリスクの高まりによって、ある機器に脆弱性（ぜいじゃく）や意図的に仕込まれたバックドア（外部から侵入可能な裏口）が存在しないか検証する技術の重要性が高まっている。そこで我々は、ファームウェアやカーネルモジュールから FPGA（Field-Programmable Gate Array）、IC チップ、センサデバイスのようなハードウェアにより近い領域（ローレイヤ）のセキュリティ技術の研究開発に取り組んでいる。また、ウェアラブルデバイスからコネクテッドカーなども対象に、物理的なセンサの誤データ入力への耐性に関するセキュリティ検証技術の研究開発を実施している。ローレイヤセキュリティに関する取組の詳細については「2-3-2　Low Layer セキュリティに関する研究活動の紹介」の記事を参照いただきたい。

3.3　ユーザブルセキュリティ

セキュリティの課題を考える上でシステムやサービス等に関わる人間の視点を無視することはできない。我々は、ユーザがシステムやサービス等を利用する際に、セキュリティが確保されつつ、ユーザにとっての

効果、効率及び満足度を損なわずに本来の目標を達成する「ユーザブルセキュリティ」の研究開発を推進している。一概に人間といっても立場や状況・役割によって様々なセキュリティ課題が存在する。例えば、開発者（プログラマ）が脆弱性を作り込まずにシステムやサービスを効率的に実装するためにはどうすれば良いか、一般ユーザが適切なセキュリティ対策を実施するために必要なサポートは何か、ユーザにセキュリティ上の望ましい行動を取らせるにはどのような手法が有効か、など人間とコンピュータの関係におけるセキュリティ課題は多岐にわたる。我々のユーザブルセキュリティ関する取組の詳細については「2-3-3　ユーザブルセキュリティ」の記事を参照いただきたい。

4　おわりに

サイバー攻撃は基本的に攻撃者有利の戦いであるため、サイバー攻撃への対処能力向上のためには技術的な観点のみならず様々な観点からの研究開発が重要である。そのため、サイバーセキュリティ研究室ではサイバーセキュリティを専門とする研究者だけでなく、機械学習等の AI 技術やネットワーク技術、ハードウェア技術、心理学や社会学など多様なバックグラウンドを持つ研究者・技術者によるチームを構築し研究開発を推進している。また、サイバー攻撃は国境を越えてくることから日本国内のみならず世界的な連携が必要不可欠である。我々は国立研究開発法人である NICT の中立性・公共性を活かし、国内外の大学や民間企業とも幅広い研究協力関係を築くことでサイバーセキュリティ分野の世界的な研究拠点を目指している。

井上 大介（いのうえ だいすけ）
サイバーセキュリティ研究所
研究所長
博士（工学）
サイバーセキュリティ、情報セキュリティ、セキュリティ可視化
【受賞歴】
2018 年　前島密賞
2016 年　産学官連携功労者表彰 総務大臣賞
2009 年　科学技術分野の文部科学大臣表彰（科学技術賞）

笠間 貴弘（かさま たかひろ）
サイバーセキュリティ研究所
サイバーセキュリティ研究室
室長
博士（工学）
サイバーセキュリティ
【受賞歴】
2022 年　電子情報通信学会 ICSS 2022 年度研究賞
2019 年　NDSS2019 Distinguished Paper Award
2011 年　情報処理学会 2011 年度山下記念研究賞

高橋 健志（たかはし たけし）
サイバーセキュリティ研究所
シニアマネージャー
博士（国際情報通信学）
サイバーセキュリティ、人工知能
【受賞歴】
2020 年　The 19th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, Best Paper Award
2018 年　コンピュータセキュリティシンポジウム 2018（CSS2018）最優秀論文賞
2012 年　日本 ITU 協会賞（奨励賞）