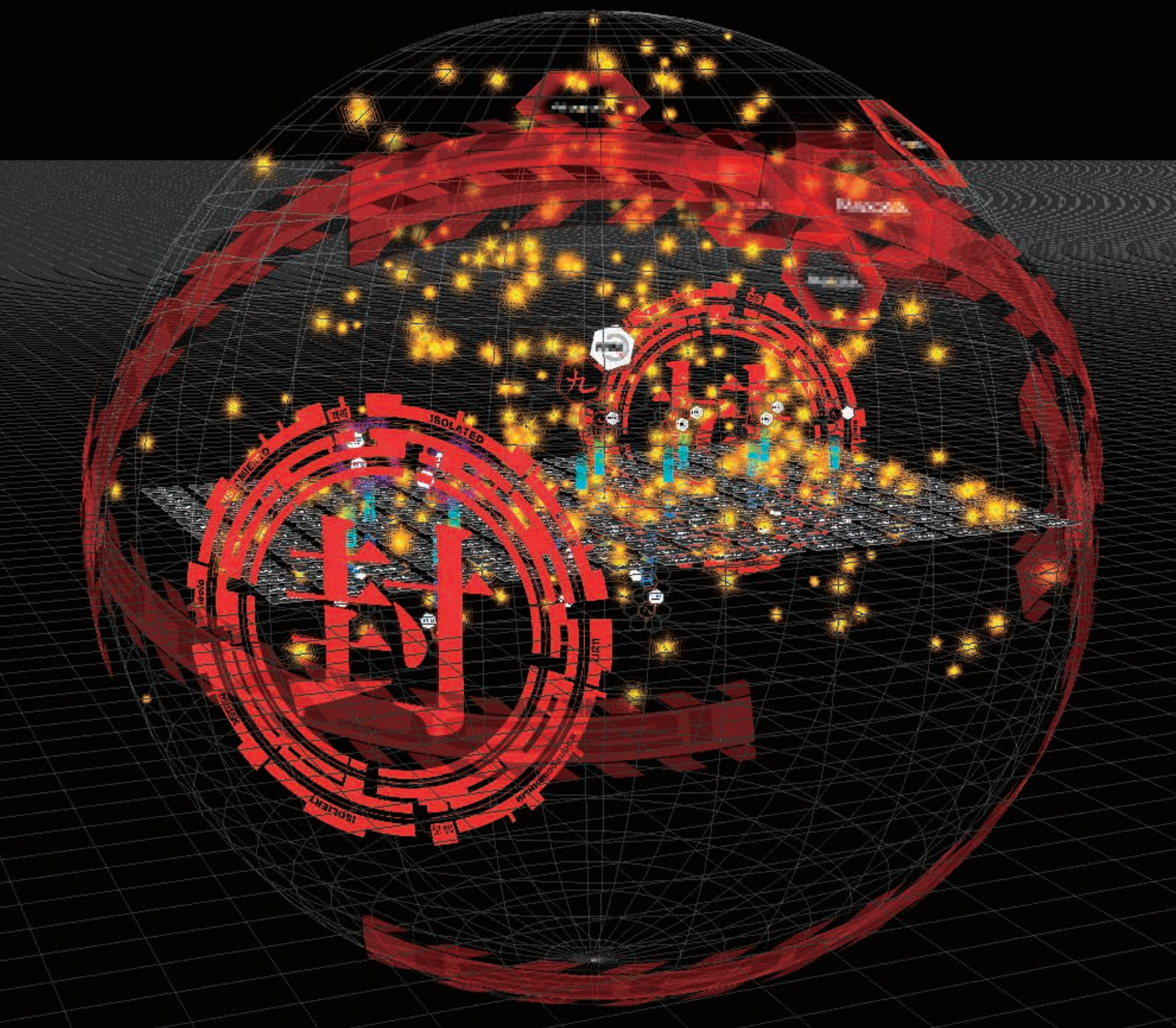
国立研究開発法人情報通信研究機構

NICT NEWS

2018
No.6
通巻 472

FEATURE

サイバーセキュリティの研究開発最前線



NICT NEWS 2018 No.6 通巻472
国立研究開発法人情報通信研究機構

CONTENTS

表紙写真「NIRVANA改の可視化画面例」
NIRVANA改の自動防御機能を用いて、セキュリティ機器やネットワーク機器に対してアクチュエーション（対策の実施命令）を行った結果、ネットワークセグメントがインターネットから遮断されている状況を可視化した画面。
中央の白色のパネルは組織内のネットワークセグメントに属するIPアドレスを、パネル外周の球体はセグメント外のネットワークを、黄色い光は遮断されセグメント内に封じ込められた通信を表す。
左上の写真は、サイバー攻撃の脅威を分析するNICTERオペレーションルーム。

INTERVIEW

熾烈なサイバー攻撃からいかにシステムを守るか！

サイバーセキュリティ研究室の目指しているものは？

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
サイバーセキュリティ研究室
室長

大学院博士課程後期修了後、2003年、独立行政法人通信総合研究所（現NICT）に入所。 2006年よりインシデント分析センターNICTERを核としたネットワークセキュリティの研究開発に従事。博士（工学）。

ますます激しさを増すサイバー攻撃。東京オリンピック・パラリンピックを2年後に控え、サイバーセキュリティ対策が注目されている。また、近年急速に普及が進んでいるIoT（モノのインターネット）機器への攻撃も課題である。

NICTのサイバーセキュリティ研究は、これらの脅威にどのように対処していこうとしているのか。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の井上大介に話を聞いた。

――サイバーセキュリティ研究室ではどのような研究を行っているのでしょうか。

井上　当研究室は、サイバー空間における実践的なセキュリティの研究をしています。現実社会で必要とされるセキュリティ技術とはどのようなものかを考え、世界の最先端技術に学びながら、日本独自のセキュリティ技術を構築すべく研究開発を進めています。

■国内最大のダークネットを観測するNICTER

――サイバーセキュリティのための様々なシステムを開発していますが、代表的なものについて説明をお願いします。

井上　我々が開発しているシステムを2次元平面上で分類してみます。（図　サイバーセキュリティ研究室研究マップ）縦軸は上がパッシブ、下がアクティブ、横軸は左がグローバル、右がローカルとなっています。

パッシブというのはサイバー攻撃を受動的に観測・分析することで、アクティブは能動的にこちらから働きかけるものです。

横軸は、サイバー攻撃に対する観測範囲の広さを示しています。グローバルではネットワーク広域を観測し、ローカルは組織の内部を観測します。

グローバルかつパッシブに分類されるのが、NICTER（ニクター）[*1]とDAEDALUS（ダイダロス）[*2]です。インシデント分析センターNICTERは、我々の研究開発の出発点というべきシステムで、ダークネットと呼ばれる約30万のIPアドレスに届く通信を観測・分析しています。

――ダークネットとは何でしょうか。

井上　インターネット上の未使用のIPアドレス群のことです。無差別型のサイバー攻撃では、攻撃の対象となる機器を探すための通信（スキャン）を送信します。このスキャンはインターネット全域に向けて送信されますので、組織や個人が使用中のIPアドレスだけでなく、未使用のIPアドレスであるダークネットにも届きます。なので、NICTERを使えば、無差別型サイバー攻撃の大局的な傾向を把握することができます。30万もの大規模なダークネットを観測しているのは日本国内ではNICTERだけです。

――攻撃は具体的にはどのようなものでしょうか？

井上　2017年のNICTERの観測データによると、一番多かったのは、TCP/23番ポートに対する攻撃で全体の3分の1以上を占めていました。このポートとはインターネット上でサービスを特定するための番号で、TCP/23番は1980年代に定められたTelnet（ユーザがネットワーク経由でサーバを操作できる通信プロトコル）向けのものですが、このポートを通してIoT機器に侵入してくるのです。

最近の傾向としては、IoT機器をターゲットとした攻撃が増えていることです。しかも年々、攻撃方法が巧みになっています。

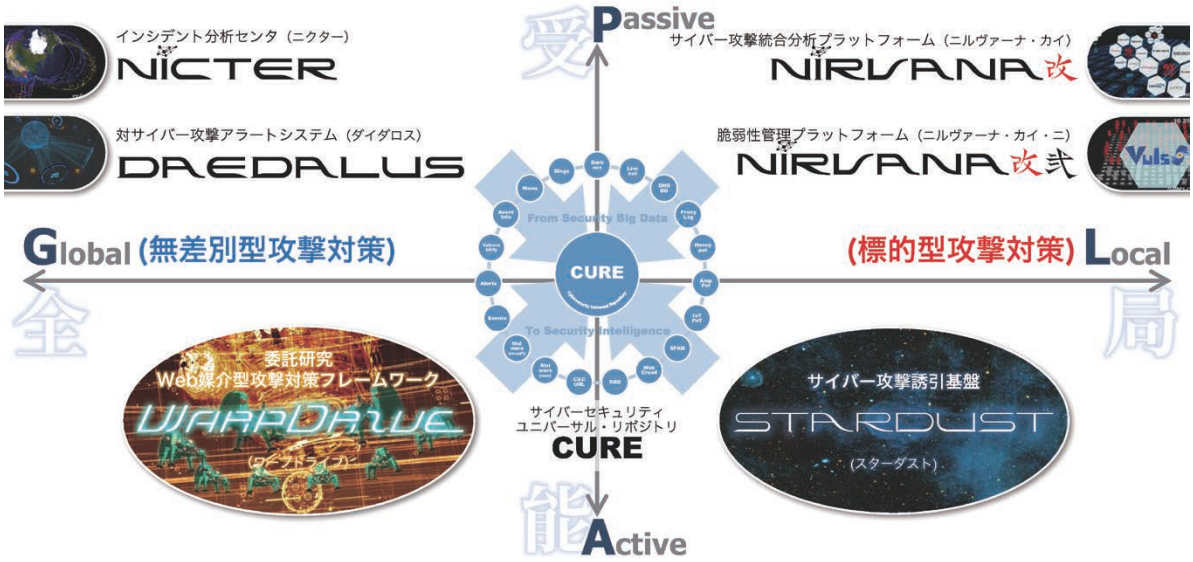


図　サイバーセキュリティ研究室研究マップ

2016年頃までは簡単なIDやパスワードによる侵入が大多数でしたが、2017年には、IoT機器の脆弱性（プログラムの不備）を利用する事例が増えてきました。さらに2018年には、IoT機器の背後にあるアンドロイド端末などに対する多段の攻撃も登場しています。

―― NICTERの観測情報はどのように活かされているのですか。

井上　JPCERTコーディネーションセンターやIPA（情報処理推進機構）、警察庁@policeなどのセキュリティ関連機関と情報共有を行っています。このほか、内閣サイバーセキュリティセンター（NISC）や東京オリンピック・パラリンピック競技大会組織委員会などとも協力しています。一般の方々向けには、NICTER Web（https://www.nicter.jp/）やNICTER Blog（https://blog.nicter.jp/）による情報発信も行っています。

■DAEDALUSとNIRVANA改／改弐

―― DAEDALUSは何をやっているのでしょうか。

井上　DAEDALUSは対サイバー攻撃アラートシステムです。NICTERの大規模ダークネット観測網で特定の組織からの通信を検出した場合、その組織にウイルス感染の疑いがあるということを知らせるアラートを送信します。現在、約600の地方自治体に無償でアラート情報を提供しています。また、DAEDALUSのテクノロジーは一般企業に技術移転され、既に商用のアラートサービスも始まっています。

―― NIRVANA改、NIRVANA改弐というシステムもありますね。

井上　NIRVANA改（ニルヴァーナ・カイ）[*3]は、サイバー攻撃統合分析プラットフォームです。標的型攻撃のようなローカルなサイバー攻撃に対処するため、組織のネットワークの末端にまでセンサーを設置してトラフィックを観測・分析・可視化します。また、各種セキュリティ機器からのアラートを集約し、トリアージ（対応の優先順位づけ）や、自動対処を可能にする組織内のセキュリティオペレーション支援ツールです。

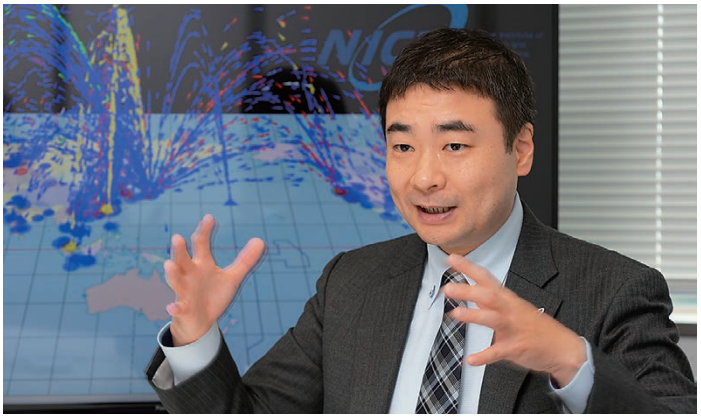
NIRVANA改弐（ニルヴァーナ・カイ・2）は、脆弱性管理プラットフォームです。組織のネットワークで稼働しているサーバ機器のOSやソフトウェアなどの構成を事前に把握しておき、新たな脆弱性が公表された際に、迅速な対応をとれるようにします。サーバ機器の脆弱性調査は国産のオープンソース脆弱性スキャナVuls（バルス）を使って行います。

NIRVANA改／NIRVANA改弐は、国内外の多くの企業のセキュリティ機器と連動が可能なように作られています。また、一般企業への技術移転を通して実社会への導入が進んでいます。

■SF漫画作品のキャラクターを起用したWarpDrive

アクティブかつグローバルの象限に位置するのが、ウェブ媒介型攻撃対策フレームワークWarpDrive（ワープドライブ）[*4]です。サイバー攻撃には、ウェブサイトを閲覧するだけでウイルス感染するものがあります。そこで、ユーザのウェブブラウザに攻撃観測用のセンサーを機能拡張としてインストールしていただき、ユーザのウェブアクセスを大規模収集します。また、ユーザが悪性サイトにアクセスしようとすると、そのブロックも行うアクチュエータの機能も持っています。

この機能拡張ソフトウェアのビジュアルとして、世界中で多くのファンを持つSF漫画作品『攻殻機動隊』のタチコマという人工知能のキャラクターを、攻殻機動隊REALIZE PROJECTと連携し、実装しました。タチコマがユーザとのコミュニケーション役を担うことで、多くの方々に親しみと実感を持って使っていただくためです。ユーザが増えればより多くのデータを集めることができ、悪性サイトの検知性能も向上します。2018年6月1日からユーザ参加型の実証実験を始めていますが、既に数千人のユーザにご利用いただいています。



■ STARDUSTとCURE

アクティブでローカルな象限には、サイバー攻撃誘引基盤STARDUST（スターダスト）があります。標的型攻撃では、ウイルス感染したコンピュータを踏み台として、攻撃者が組織内に侵入を試みるのですが、ウイルスのプログラムを解析するだけでは、攻撃の核心部分である人間の攻撃者による活動までは把握できませんでした。

そこで、組織を模倣したダミーのネットワーク環境を構築し、攻撃者をその環境内に能動的に誘引します。攻撃者にはダミーと分からないように環境を精巧に作り込んでいますので、ネットワーク環境内での攻撃者の挙動を長期観測することで、攻撃手法や意図を分析できます。

STARDUSTの成果として、攻撃者の実態が明らかになってきました。意外にも、大半の標的型攻撃は、マニュアル化されていると思われる類似の攻撃手法が用いられることが多く、攻撃者の技術力はそれほど高いものではありませんでした。これまで、セキュリティ業界の通説として語られていたような、高度なスキルをもった攻撃者が侵入を試みるようなケースは非常にまれであることが分かりました。このデータを基にして、リーズナブルな標的型攻撃対策技術の確立が期待できます。

最後に、研究マップの中央に位置しているのは、サイバーセキュリティ・ユニバーサル・リポジトリ（CURE）[*5]です。ここに、パッシブ・アクティブ・ローカル・グローバルの全方位の情報が集まってきます。集まったデータを相互に関係づけて分析する仕組みを研究開発しています。CUREで大量のデータを蓄積・分析することによって、分散したビッグデータから統合的なインテリジェンスの創出を目指しており、そのためには機械学習による自動分析技術が鍵になります。

■ NICTの役割

――国立の研究開発機関としてどのような役割を担っているのでしょうか。

井上　当研究室で研究開発した技術や、その結果得られたデータは、実社会に還元するのが基本です。そのため、産業界への技術移転や、セキュリティ関連機関との情報共有を進めています。例えば、国内で大規模なウイルス感染が発生した際には、研究室内の解析チームが原因追求に努め、関連機関と連携して注意喚起につなげるなどの活動も行っています。

――日本のセキュリティ技術は世界の中でどのくらいのレベルなのでしょうか。

井上　単純な比較はできないのですが、いわゆる失われた20年の間、セキュリティ技術の研究開発に関する投資は日本では非常に少なかったと言えます。その間、欧米では着実に研究開発が進み、現在のグローバルなセキュリティ産業につながっています。しかし、ここ数年で、日本企業も随分と意識が変わってきました。サイバー攻撃のニュースが毎日メディアをにぎわせ、企業の情報が大量に漏えいする事件が頻発し、日本企業のトップマネジメント層もセキュリティの重要性を十分認識するに至っています。何より、セキュリティをビジネスチャンスととらえる意識も高まっているように感じられます。

最近、セキュリティ自給率という言葉を使っています。これは、国産のセキュリティ製品が国内でどれくらい普及しているのかということですが、残念ながら日本製のセキュリティ製品で大きなシェアを占めているものは現時点では見当たりません。官公庁や国内企業の大部分は、海外製のセキュリティ製品で守られているのが実情です。内部のロジックを完全には把握できない、いわばブラックボックスで守られたセキュリティです。ナショナルセキュリティの観点からも、セキュリティ自給率を上げていかないといけないという問題意識を持っています。

――具体的にどのようにしようと考えていますか。

井上　NICTだけで全てをカバーすることはできませんので、産学と連携して研究開発を進めていきます。例えば、NICTのネットワーク自身をセキュリティ・テストベッド化し、我々の研究室はもちろん、外部の企業や大学が研究開発したセキュリティ技術も持ち込んで試験運用し、各種の評価を既に行っています。NICTの強みの一つは、膨大な量の実データを持っているということです。これを外部の研究者や技術者にも可能な限り活用していただこうと考えています。

――今後の展望についてお願いします。

井上　まずは、2020年の、東京オリンピック・パラリンピックを安全に乗り切ることです。国産のセキュリティ技術の向上と優秀なセキュリティ人材の育成に貢献し、目的を完遂したいと思います。

＊1　NICTER (Network Incident analysis Center for Tactical Emergency Response)

＊2　DAEDALUS (Direct Alert Environment for Darknet And Livenet Unified Security)

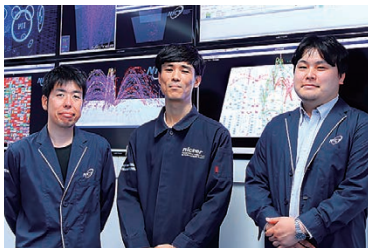
＊3　NIRVANA (NICTER Real-network Visual ANAlyzer)

＊4　WarpDrive (Web-based Attack Response with Practical and Deployable Research InitiatiVE)

＊5　CURE (Cybersecurity Universal Repository)

大規模観測が映し出すサイバー攻撃の現状

IoT時代に迫る脅威をとらえる研究開発



左から伊沢亮一、久保正樹、笠間貴弘

久保 正樹（くぼ まさき）
サイバーセキュリティ研究室
上席研究技術員
JPCERTコーディネーションセンターでセキュアコーディング、脆弱性ハンドリングに従事した後、2017年NICT入所。NICTER解析チームリーダー。

笠間 貴弘（かさま たかひろ）
サイバーセキュリティ研究室
主任研究員
大学院修了後、2011年NICT入所。NICTERプロジェクトをはじめ、サイバーセキュリティ関連技術の研究開発に従事。博士（工学）。

伊沢 亮一（いさわ りょういち）
サイバーセキュリティ研究室
主任研究員
セキュリティ系ベンチャー企業を経て、2012年NICT入所。OSカーネルモジュールや仮想化技術を用いたマルウェア解析など、サイバーセキュリティに関する研究に従事。博士（工学）。

NICTERプロジェクトでは、インターネット上で発生しているサイバー攻撃をリアルタイムに観測・分析する取組を10年以上にわたって実施しています。本稿では、それらの取組を通じて明らかになった近年のサイバー攻撃の状況について報告し、特にIoT機器を狙うサイバー攻撃に関する我々の研究開発の取組を紹介します。

■約30万アドレスによる大規模観測

NICTERプロジェクトでは、インターネット上の未使用のIPアドレス（ダークネット）に届く通信を観測することでサイバー攻撃の状況を把握しています。通常、ダークネットには何も通信が届かないはずですが、実際にはマルウェアに感染したコンピュータによる、次の攻撃先を探すための探索用の通信（スキャン）が大量に届いています。それらを大規模に観測・分析することで、マルウェアの感染拡大などの兆候をいち早く見つけ、対策につなげることができます。我々は現在、国内外の様々な組織と連携することで、世界最大規模となる約30万アドレスのダークネット観測を行っています（図1）。

■IoT機器を狙う攻撃活動の活発化

ここ数年、ダークネットで観測されるスキャンが増加しており、2017年には1 IPアドレス当たり約56万パケットものスキャンが観測されました。2017年に観測されたパケットを宛先ポート別にカウントしたグラフが図2です。グラフを見ると、23/TCP（Telnet）や22/TCP（SSH）を狙うパケットが多くを占めていることが分かります。近年、ユーザID/パスワード設定等に不備のあるIoT機器（主にWebカメラやWi-Fiルータなど）がマルウェア感染する事例が多数発生しており、我々の調査結果によってグラフの青色で塗られているもの（全体の半数以上）は全てそれらIoT機器を狙った攻撃活動であることが明らかになっています。また、感染は外国だけでなく日本国内でも発生しており、我々の観測・分析結果によって主に国内で販売・流通している機器（Wi-Fiルータ）がマルウェア感染し

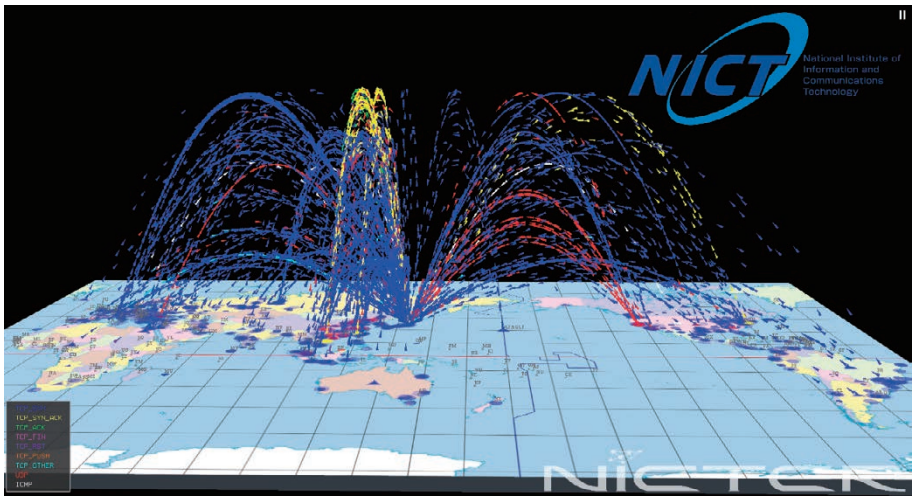


図1　NICTERダークネットに届く通信の様子（Atlasによる可視化）

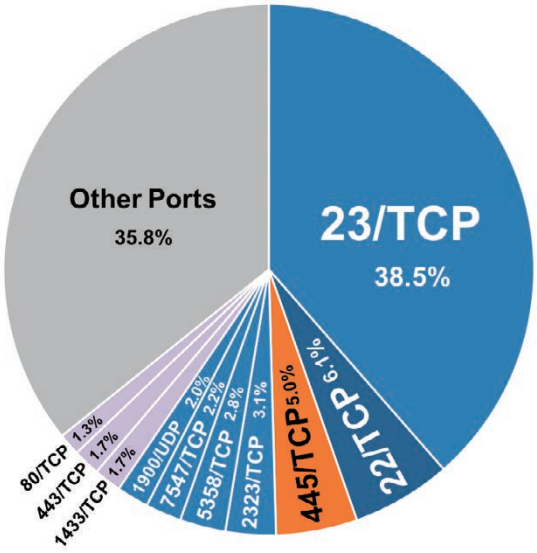


図2　ポート番号別の観測パケット数割合（2017年）

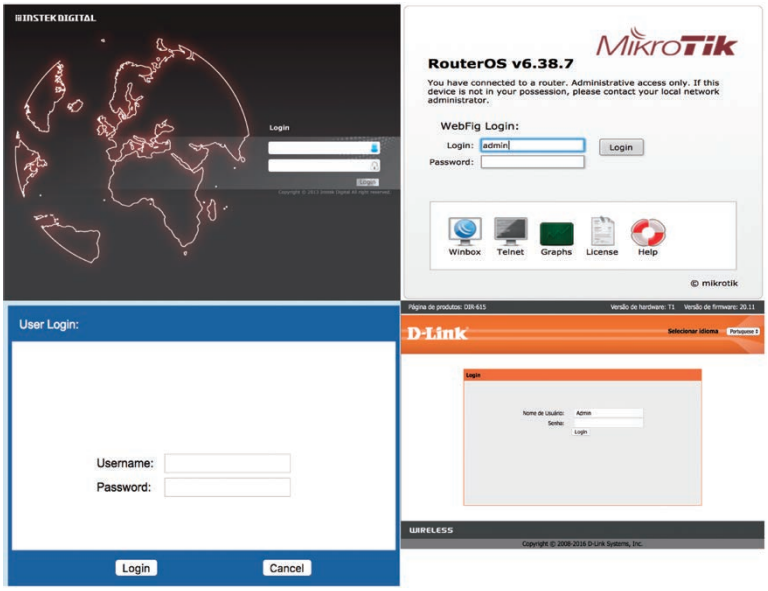


図3　IoT機器の管理用Webインターフェイスのログイン画面

ている事例も発見され、JPCERT/CCなどの関係組織への情報提供を行っています。

■感染IoT機器の自動分類

ダークネットで観測される攻撃元機器は既にマルウェアに感染している機器と考えられますが、観測したスキャン情報だけではそれらが本当にIoT機器なのか判別することは困難です。そこで、我々は攻撃元機器に対してこちらから能動的にアクセスを行い、得られたレスポンスから攻撃元機器の分類や自動判別を行う技術を研究開発しています。例えば、攻撃元機器に対してWebアクセスした際に、図3に示すような当該機器のログイン画面が見える場合があります。このログイン画面は機器によって異なり、収集したこれらの情報を基に各攻撃元機器を分類することで、大量にマルウェア感染が発生している機器を把握する取組を行っています。

■IoTマルウェアの分類

また、我々は実際のIoTマルウェアを捕獲し、その感染手法や目的を解明する技術の研究開発も行っています。IoTマルウェアは、MiraiやBashliteなどの著名なマルウェアに加え、近年では暗号通貨を採掘するIoTマルウェア（マイニングマルウェア）が増加しています。マイニングマルウェアをIoT機器に感染させ、暗号化通貨を採掘し、金銭を得るということが攻撃者の目的ですが、IoT機器1台で1日当たりに採掘できる暗号通貨の量はそれほど多くはありません。そこで、攻撃者は世界中に存在する大量のIoT機器を乗っ取ることで、得られる金銭を最大化しようとします。マイニングマルウェアの感染からIoT機器を守ることは、攻撃者の不正な資金調達を防ぐことにもつながります。

あるマルウェアを捕獲したときに、Miraiなのかマイニングマルウェアなのかといった種類がすぐに分かれば、その後のマルウェア解析を効率的に行うことができます。そこで我々はマルウェアを種類ごとに分類する手法を研究開発しています。分類を行う際に重要となるのが、あるマルウェアと別のマルウェアの類似度（似ている度合い）をいかにして計算するかですが、我々はマルウェアを構成する機械語に着目し、ある2つのマルウェアの機械語を比べたときに共通する命令部分が多ければ多いほど類似度を高くするようにしました。具体的には、機械語を逆アセンブルして得られた逆アセンブルコードから命令を抽出し、N-gramの組によって共通する命令列が多いほど類似度が高くなるように計算します。実際に、2,000個のマルウェア検体の類似度を計算し、2次元平面上にマッピングした結果が図4です。例えば、未知の検体（赤色の「＋」）のうち、Bashliteの近くにマッピングされている検体はBashliteの可能性が高いことが分かります。実際には、各マルウェア間の類似度を求めた後、機械学習手法を適用することで自動分類し、捕獲したマルウェアの種類を得ることができます。

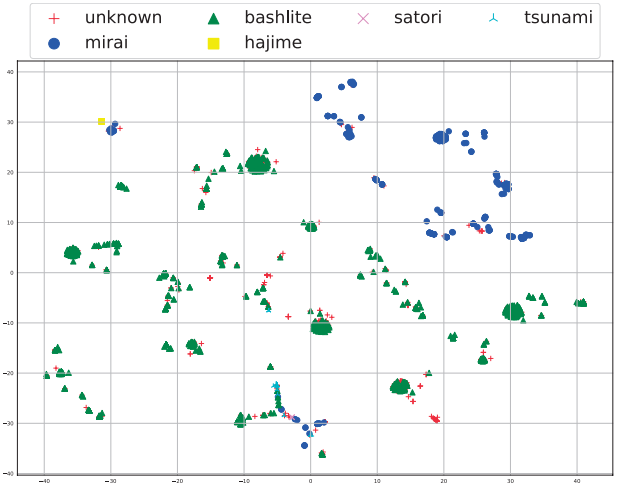


図4　類似度に基づいてマルウェアを分類した結果

■まとめ

インターネットにつながる機器が爆発的に増加するIoT時代を迎え、それらIoT機器を狙う攻撃活動も活発化しています。また、IoT機器が持つ様々な弱点を狙う攻撃が見られることから、攻撃自体がより複雑化してきています。我々は、こうしたIoT機器に対する脅威をいち早くとらえ、その実態を把握して対策に資するべく、これからもインターネットの観測・分析、新たな脅威をとらえるための研究開発を続けていきます。

NIRVANA改・NIRVANA改弐

次世代のセキュリティオペレーションの実現に向けて

鈴木 宏栄（すずき こうえい）
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
主任研究技術員
民間企業を経て、2009年NICT入所。NICTER、DAEDALUS、NIRVANA、NIRVANA改の研究開発に従事。

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
サイバーセキュリティ研究室
室長

サイバー攻撃対策は日々大量に発生するセキュリティアラートや脆弱性情報との終わりなき戦いとなっています。サイバーセキュリティ研究室は組織内のセキュリティオペレーションの効率化を目指し、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）」及び脆弱性管理プラットフォーム「NIRVANA改弐（ニルヴァーナカイ2）」の研究開発と社会展開を進めています。

■NIRVANA改

サイバー攻撃対策として多くの組織がファイアウォールや侵入検知システム、エンドホスト対策ソフトウェアなど、複数のセキュリティ対策製品を導入・運用しています。それらの対策製品は日々膨大なセキュリティアラートを生成し、その適切な処理には高い人的コストが発生します。

NIRVANA改は、セキュリティアラートの集中管理とトリアージによって、セキュリティオペレーションの効率化を図るサイバー攻撃統合分析プラットフォームです。NIRVANA改は言わば、リアルタイムかつグラフィカルなSIEM[*1]エンジンであり、1）アラート収集・分析、2）自動対処、3）トラフィック観測、4）リアルタイム可視化、の4つの機能を有しています（図1）。

アラート収集・分析機能

組織内に設置されたセキュリティ機器やエンドホスト対策ソフトウェアのアラート情報は、アラート情報収集システムによって集中管理され、NIRVANA改ユーザインターフェース経由で分析が可能です。オペレータはアラート情報を分類し、対処すべき優先順位を決定するトリアージを行います。

PC端末でマルウェア感染が発生した場合は、ホスト情報収集システムにより収集されるPC端末内の詳細情報により、マルウェアの特定、通信状況の確認などを迅速に行うことが可能です。さらに、ネットワーク系のセキュリティアラートとの関連付け

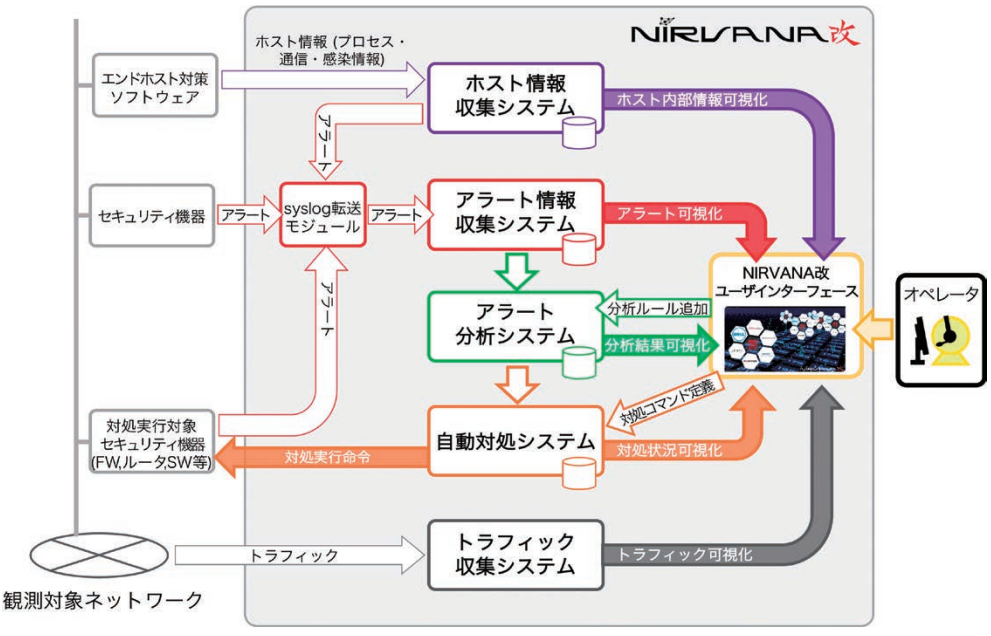


図1　NIRVANA改システム構成

図2　NIRVANA改の自動対処機能によるネットワーク遮断

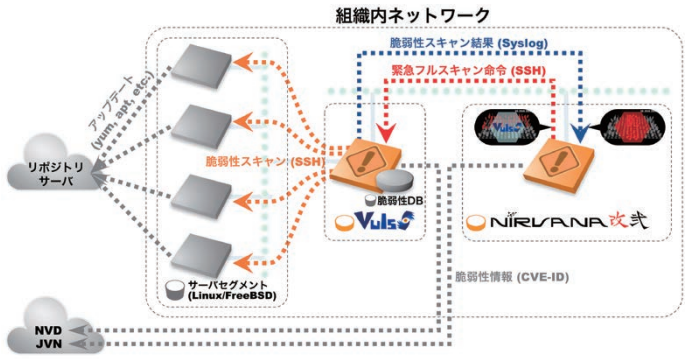


図3　NIRVANA改弐システム構成

もシームレスに行うことができ、原因特定に掛かる時間を大幅に短縮可能です。

アラート分析システムでは、オペレータが自由に設定可能な分析ルールにより、アラート情報収集システムのデータベースに蓄積されたアラート情報の中から、緊急に対処すべき重要なインシデントを自動抽出します。

自動対処機能

自動対処システムは、アラート分析システムにより導出されたインシデントに対して、通信遮断などの対策を定義し、自動実行（あるいは手動実行）することができます。対処実行対象機器への実行コマンドは、対処対象機器が持つインターフェースに合わせて、柔軟に定義が可能です。

トラフィック観測機能

トラフィック観測システムは、組織のネットワークからポートミラーリングやネットワークタップによってトラフィックを収集します。収集されたトラフィックは、リアルタイムにユーザインターフェース上で可視化され、オペレータによるネットワークの迅速な現状把握を助けます。

リアルタイム可視化機能

NIRVANA改のユーザインターフェースでは、リアルタイムの3Dビジュアライゼーションによって、一連のセキュリティオペレーション（セキュリティアラートの分析から、トリアージ、自動対処まで）を迅速かつ効率的に行うことを可能にします（図2）。

■NIRVANA改弐

サイバー攻撃による被害を「予防」するためには、OSやソフトウェアの欠陥である「脆弱性」への対処が必要不可欠です。しかし、従来の脆弱性管理は人手に頼る部分が多く、高い人的コストを要するため、

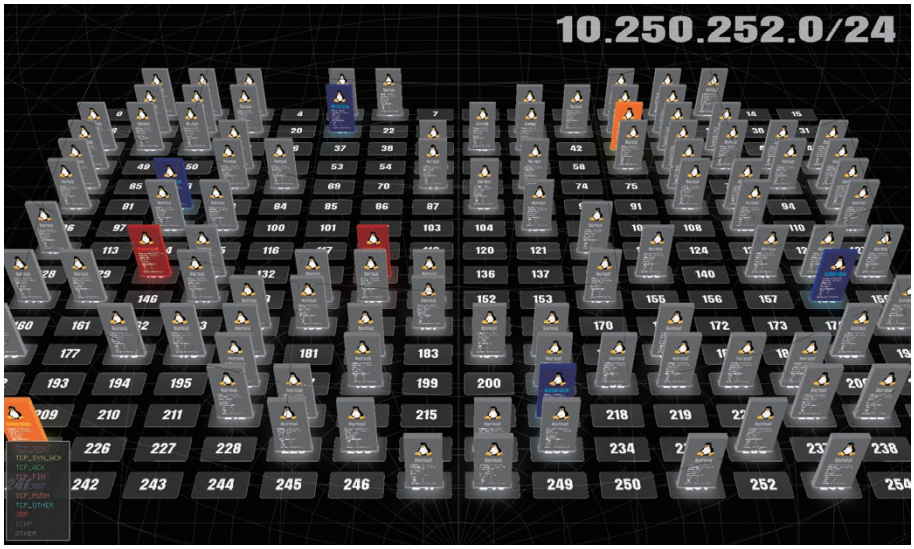


図4　NIRVANA改弐によるサーバ機器の脆弱性対応状況の全体俯瞰

組織のセキュリティ向上の障壁になっていました。

NIRVANA改弐は、国産の脆弱性スキャナ「Vuls*2」と連動し、組織内の脆弱性の統合的な管理を可能にする脆弱性管理プラットフォームです。Vulsはエージェントレスの脆弱性スキャナであり、組織内のLinux/FreeBSD系サーバに定期的に接続し、各サーバの脆弱性スキャンを行います。脆弱性スキャンの結果は、NIRVANA改弐によってリアルタイムに可視化されます（図3）。

NIRVANA改弐のユーザインターフェースでは、組織内のサーバ機器はモノリスで表現され、脆弱性の重大度に応じてモノリスの色が変化します。オペレータは、サーバ機器の脆弱性対応状況の全体俯瞰（図4）が可能となります。影響範囲の広い脆弱性が公表された場合には、NIRVANA改弐の自動対処機能を用いて、Vulsに緊急フルスキャン命令を送ることができ、脆弱性を保有するサーバ機器を能動的に検知できます。

組織内のサーバに脆弱性が発見された場合、オペレータはNIRVANA改弐から外部の脆弱性情報にアクセスし、脆弱性の詳細情報を確認することも可能です。また、組織のセキュリティポリシーに従って、サーバのアップデートを行うなど、迅速かつ効率的な脆弱性管理が可能となり、組織のセキュリティ向上や人的コストの低減が期待できます。

■今後の展望

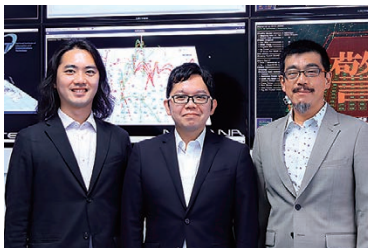
NIRVANA改は、民間企業への技術移転を通じて社会展開を進めており、日本国内の導入事例は着実に増加しています。今後は、セキュリティオペレーションの現場からのフィードバックを基にNIRVANA改及びNIRVANA改弐の更なる高度化を進め、社会のセキュリティ向上に貢献していきます。

＊1　Security Information and Event Management：セキュリティ情報イベント管理の略称。セキュリティ機器やソフトウェアが出力するイベント情報を一元的に保管して管理し、脅威となる事象を把握するテクノロジーのこと。

＊2　Vuls：フューチャー株式会社（代表取締役会長兼社長 グループCEO: 金丸 恭文）により開発された国産OSS脆弱性スキャナ。

サイバー攻撃誘引基盤STARDUST

攻撃者を誘い込み、攻撃活動の実態を明らかに



左から遠峰隆史、津田侑、金谷延幸

津田 侑（つだ ゆう）
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
研究員
2013年に大学院博士後期課程単位取得認定退学後、同年NICT入所。標的型攻撃対策やセキュリティオペレーション、サイバー模擬戦（CTF）に関する研究に従事。博士（情報学）。

遠峰 隆史（とおみね たかし）
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
有期研究技術員
2012年に大学院後期博士課程単位取得退学後，大学研究員を経て2013年NICT入所。ネットワーク運用やインターネット、標的型攻撃対策に関する研究に従事。

金谷 延幸（かなや のぶゆき）
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
主任研究員
大学院修士課程修了後、民間研究所でのセキュリティ研究の経験を活かして、2013年NICT入所、標的型攻撃対策の研究に従事。

標的型攻撃は特定の組織を狙ったサイバー攻撃で、社会的な問題となっています。一方で、NICTERのような無差別型攻撃の観測では、標的型攻撃の様子をとらえることは困難です。そこで、標的型攻撃の攻撃者を誘い込み、彼らの活動を密かに観測するための基盤の研究開発を進めています。

■標的型攻撃対策の研究の難しさ

サイバー攻撃はコンピュータネットワークを介して被害を及ぼす行為を指しますが、その中でも社会的に大きな影響を与えているものが「標的型攻撃」です。標的型攻撃は読んで字のごとく、企業や官公庁等の特定の組織に狙いを定めて実行されるサイバー攻撃です。攻撃者は標的となる組織の特性を調査し、その特性に合わせた攻撃手法で組織内のネットワークに侵入します。そして、攻撃者の目的（機密情報の窃取等）を達成するまで長期間にわたって活動を進めます。

日本国内でも標的型攻撃による大規模な被害が発生しています。2015年6月に公になった日本年金機構から125万件もの個人情報が流出した一連の事件は、「Blue Termite（ブルーターマイト）」と呼称される攻撃によるもので、日本の組織が標的とされていました。また、この攻撃では「Emdivi（エムディヴィ）」と呼ばれるマルウェアが用いられていました。攻撃者は日本語で作成されたメールにこのEmdiviを添付することで標的組織内に侵入し、指令サーバを介して標的組織内で様々な攻撃活動をしていました。

このような攻撃の全体像は、メディア上の情報やセキュリティ企業によるマルウェアの解析結果を蓄積することで大まかに把握できます。しかし、このような情報源には攻撃の実態が詳細に記載されることはほとんどありません。実際に標的となった組織内で攻撃者がどのような手順・手段で攻撃を進めたのか、ネットワーク内のシステムにどのようなログが残されたのかといった攻撃の痕跡は、対策技術の研究開発に必須となりますが、このような情報は被害組織の機密情報も多く含むことから公開されません。

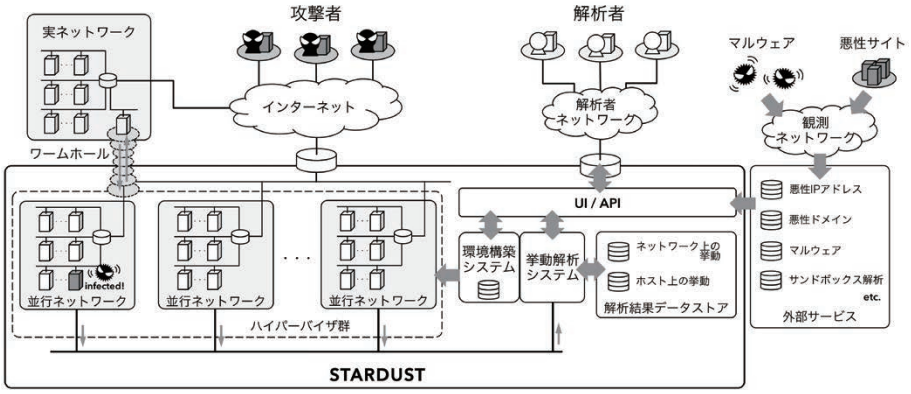


図1　STARDUSTの構成図

■攻撃者の活動が観測可能な基盤「STARDUST」

そこで我々は、標的型攻撃に関するデータを収集するために、攻撃者の活動を観測するための基盤「STARDUST（スターダスト）」を研究開発しています（図1）。STARDUSTは、攻撃者の誘引先となる組織のICT環境を高精細に模擬した「並行ネットワーク」を自動構築できます。並行ネットワーク上の端末で、標的型攻撃に利用されたマルウェアを実行することで実際の指令サーバとの接続を確立し、攻撃者を誘引します。

誘引した攻撃者に長居させるために、STARDUSTには文書ファイルやメール、Webブラウザのブックマーク、ユーザ情報などを設置する機能があり、これにより並行ネットワークが実際に利用されている

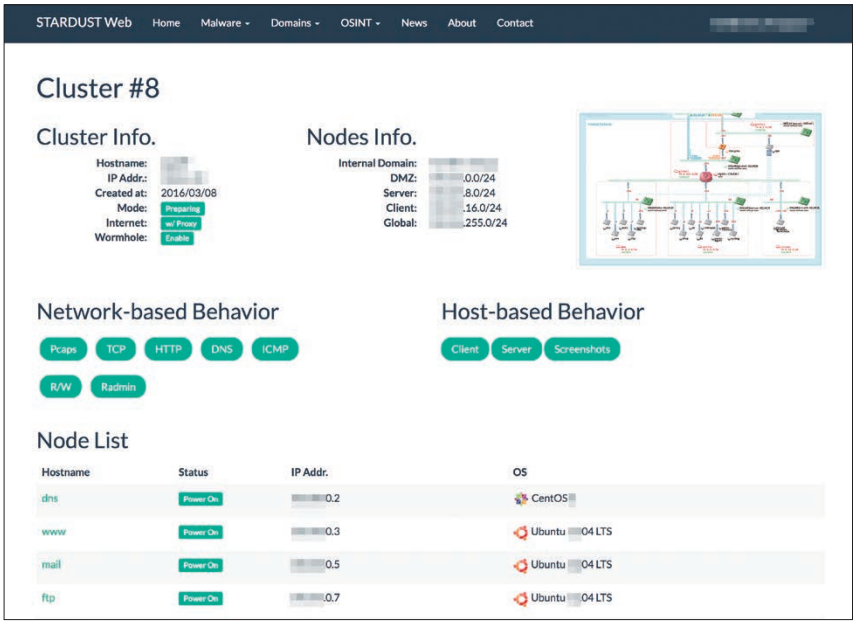


図2　STARDUSTのWebインタフェース

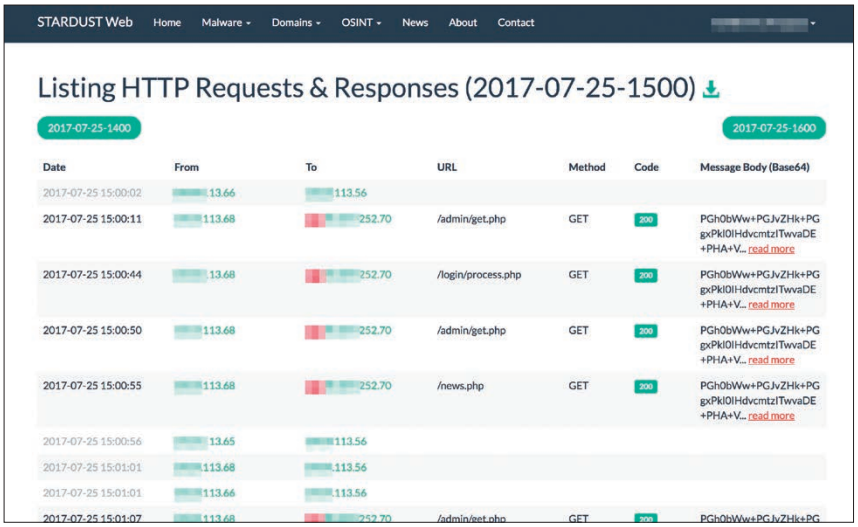


図3　STARDUSTで取得したHTTP通信（指令サーバとマルウェア間のやりとりを含む）

かのような錯覚を与えることができます。また、「ワームホール」を利用することで、攻撃者が標的にした組織のネットワークを実際に介して指令サーバに接続できます。これらにより、攻撃者に対してあたかも攻撃が成功したかのように思わせることができます。

攻撃者が並行ネットワーク上の端末を探索したときの痕跡は、端末内またはネットワーク上の通信から取得できます。STARDUSTでは、観測していることが攻撃者に気付かれないようにステルス性の高い方式を採用しています。取得したデータは、リアルタイムにWebインタフェースから参照できます（図2、3）。また、取得したデータに基づいて、観測しながら各端末を操作することも可能です。

■分かってきた攻撃者の実態

これまで、NICTサイバーセキュリティ研究室では、様々な標的型攻撃関連のマルウェアを用いて攻撃者を誘引してきました。本稿では、その中でも「DragonOK（ドラゴンオーケイ）」と呼ばれる攻撃グループから得られた活動の一例を紹介します（図4）。

これらは、誘引された攻撃者が実際に並行ネットワーク上の1端末で実行したOS標準搭載のコマンドです。これらのコマンドは組織内のネットワーク管理者が利用するもので、一般の職員が利用することはほとんどありません。この結果から、攻撃者はこのようなコマンドを利用して組織内のネットワークを探索していくことが分かりました。ここで15行目のコマンドに注目してください。攻撃者は「whomai」というコマンドの実行を試みていますが、OSにはこのようなコマンドはありません。次の行で「whoami」、「whoami /group」と続けて正しいコマンド実行やオプションを付与した実行をしているため、これは攻撃者の入力ミスと考えられます。この結果から、攻撃者は攻撃活動を自動で実行しているのではなく、手作業で実行している可能性がうかがえます。

```
1  net view
2  systeminfo
3  whoami
4  tasklist
5  dir c:¥users¥nito¥desktop¥
6  dir "c:¥program files¥"
7  dir d:¥
8  dir c:¥users¥nito¥
9  dir c:¥users¥nito¥documents¥
10 dir c:¥users¥nito¥downloads¥
11 dir "c:¥Program Files (x86)¥"
12 netstat -an
13 dir c:¥users¥nito¥documents¥Credential
14 ipconfig /all
15 whomai /groups | find /i "level"
16 whoami
17 whoami /groups
18 net group
19 net view
20 arp -a
21 netstat -ano
22 ping ***.***.8.4 -n 1 （プロキシサーバのIPアドレス）
23 tasklist
24 netstat -an
25 net view
26 tracert
27 net view ¥¥win05
```

図4　攻撃活動の一例

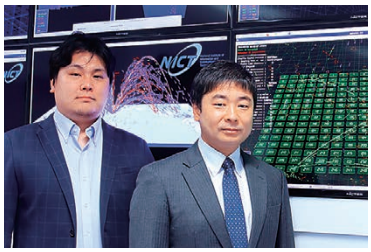
このように、攻撃者を実際に誘引し、その活動を観測することで攻撃活動の実態が見えてきました。このような実際のデータを蓄積していくことで標的型攻撃の知見が得られ、さらにはデータの様々な活用が見込まれます。

■今後の展望

昨年5月のSTARDUSTの公開から利用者を徐々に拡大し、今では企業や大学等の様々な組織で活用されています。並行して、NICT内においても実際の標的型攻撃をSTARDUSTに誘引し解析しながらデータを収集しています。ここで収集できたデータは攻撃のシミュレーションではなく、実際の攻撃者の観測から得られた貴重な情報です。そのため、このデータに基づいたサイバー攻撃演習のシナリオを生成することで、リアリティのある演習を行えると考えています。また、データセット化することによって今後の研究開発につながるものと期待できます。

Web媒介型攻撃対策「WarpDrive」の取組
ユーザ参加型によるWeb攻撃対策の実現に向けて

山田 明（やまだ あきら）
株式会社KDDI総合研究所
大学院修了後、2000年KDDI株式会社に入社、KDDI研究所（現KDDI総合研究所）にて、ネットワークセキュリティ、侵入検知システム、DDoS攻撃対策に関する研究開発に従事。博士（情報科学）。



左から笠間貴弘、井上大介

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
主任研究員

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
サイバーセキュリティ研究室
室長

Webブラウザを媒介にしたマルウェア感染が深刻な被害を及ぼしている一方、その実態を把握して対策することが課題になっています。攻撃Webサイトは、観測を避けて攻撃コードを隠蔽することや、非常に短い時間で活動をやめてしまうことがあります。この課題を解決するためにユーザ参加による攻撃観測・対策の仕組みを研究開発しました。この仕組みでは、ユーザ端末のWebブラウザ履歴を集めることによって観測を実現します。さらに、多くのユーザ参加を促すために、攻殻機動隊REALIZE PROJECTと連携した実証実験を開始しました。この取組によって、攻撃実態が解明されつつあります。

■Webブラウザを媒介した攻撃が観測できない

サイバー攻撃の感染経路は、Webブラウザを媒介にしたものが主流になっています。サイバー攻撃の観測では、ハニーポットによる受動的な観測と、クローラによる能動的な観測がされてきました。しかしながら、このWeb媒介型攻撃は、ユーザ端末において発生するため、それらによる観測が困難でした。攻撃コードが埋め込まれているWebサイトを網羅的に発見することが難しいため実態がつかめず、クローラによる接続を識別して攻撃コードを隠蔽する仕組みが観測を難しくしていました。

■ユーザ参加型によるWeb媒介型攻撃対策

そこで我々は、ユーザ参加によるWeb媒介型攻撃対策「WarpDrive[*1]」の研究開発を行いました。WarpDriveでは、一般ユーザの参加によって観測環境を構築する点が特徴です。図1にWarpDriveのシステム構成を示します。システムは、ブラウザセンサと分析基盤からなります。観測に協力していただくユーザには、端末のWebブラウザにブラウザセンサと呼ばれるソフトウェアをインストールしていただきます。このセンサからの分析基盤に情報を集めることによって、ユーザ端末において発生している攻撃の実態把握を実現します。そして、把握した実態に基づいて攻撃サイトをテイクダウンしたり、ユーザが攻撃サイト

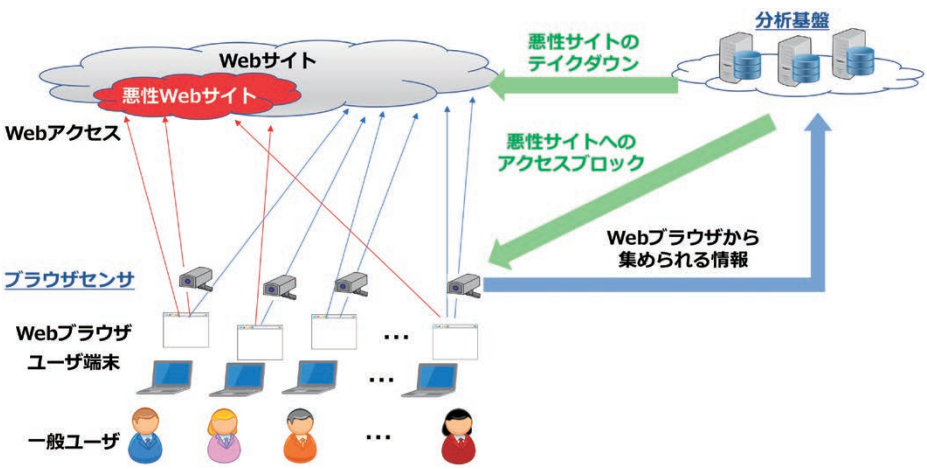


図1　ユーザ参加型によるWeb攻撃対策

にアクセスしてしまった場合、それをブロックして被害を未然に防いだりします。より多くのユーザ参加によって、攻撃の全体把握及び検知・防御の性能が上がっていきます。

図2　Web閲覧履歴の可視化

■攻殻機動隊 REALIZE PROJECTとの連携による実証実験

ユーザ参加型の攻撃観測を大規模に展開するために、攻殻機動隊 REALIZE PROJECTと連携して、実証実験を開始しました。アニメ「攻殻機動隊S.A.C.」シリーズに登場するキャラクター「タチコマ」を起用したブラウザセンサ「タチコマ・セキュリティ・エージェント（以下、タチコマSA）」を開発しました。タチコマは、アニメにおいて主人公たちを強力にサポートする高度な人工知能（AI）を搭載しているキャラクターです。タチコマSAでは、攻撃観測及び防御などのセキュリティ機能に加えて、攻殻機動隊のコンテンツや同作をモチーフにしたWeb空間の可視化等も体験できます（図2、3）。

2018年6月1日に実証実験を開始して、約3か月間で5,000人を越すユーザに登録していただくことができ、毎日約15億件のブラウザ履歴を収集しています。また、タチコマSAによって悪性サイトへのアクセスをブロックした事例が1日平均11.7件、詳細分析の結果、悪性度が高いと判断されたURLが1日平均140.1件集まってきています。本研究プロジェクトでは、表のように攻撃サイトのURLが短時間で変化していく様子を観測できました。これは、Rig Exploit Kitという攻撃ツールのURL変化の様子です。

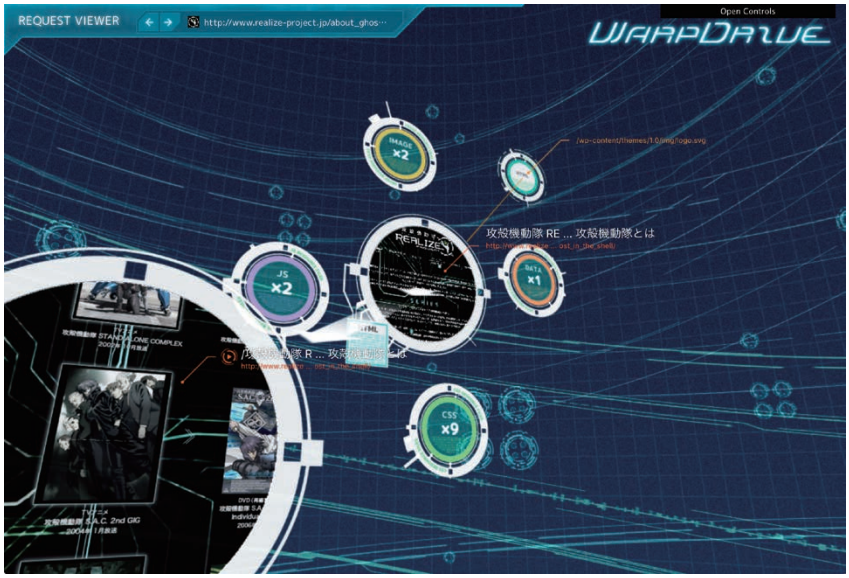


図3　Webコンテンツの可視化

表　悪性サイト（Rig Exploit Kit）のURL変化（2018年8月7日）

悪性サイトURL	開始	終了	継続	回数
http://aaa.aaa.213.226?MjczMDQ<略>	01:33:27	05:40:53	4.1	7
http://bbb.bbb.124.190?NTM2NTE<略>	07:56:01	14:20:56	6.4	10
http://ccc.ccc.213.216?MTc1NTg<略>	16:43:38	20:34:27	3.8	8
http://ddd.ddd.120.59?NDY2MTg<略>	20:54:58	22:47:59	1.9	5
…	…	…	…	…

■WarpDriveの今後

現在、WarpDriveでは、実証実験を行っており、貴重なデータが順次集まってきています。今後、この収集データを活用したWeb媒介型攻撃の更なる実態把握並びに、この実証実験環境を利用したユーザ環境のセキュリティ改善を検討しています。さらに、この研究開発によって得られた知見や技術の実用化を目指していきます。また、タチコマSAは、実証実験の期間中にポータルサイト*2からダウンロード・インストールできます。ご興味のある方は、是非ご参加ください。

*1 WarpDrive（Web-based Attack Response with Practical and Deployable Research InitiatiVE）

*2 https://warpdrive-project.jp

マルチパラメータ・フェーズドアレイ気象レーダを用いた実証実験の開始

～NICTプレスリリースより～

内閣府のSIP「レジリエントな防災・減災機能の強化」の施策として、NICTをはじめとする研究グループは世界初の実用型「マルチパラメータ・フェーズドアレイ気象レーダ（MP-PAWR）」を開発し、これを用いた実証実験を2018年7月から開始しました。MP-PAWRは雨雲の高速三次元観測と雨量の高精度観測の双方を実現する新型気象レーダで、レーダを中心とする半径 60 km の範囲の領域で地上付近から上空まで30秒間隔で連続的に観測することで、急激に発達する積乱雲による降雨を監視します。観測データは国立研究開発法人防災科学技術研究所の気象予測モデルに組み込まれ、30分先までの豪雨予測情報として、市民や自治体防災担当者などの2,000 人のモニターへ提供されます。

図1　MP-PAWR アンテナ部（埼玉大学建設工学科3号館屋上）

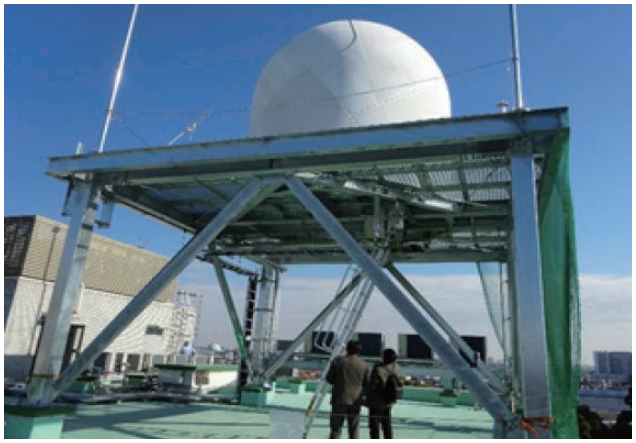


図2　埼玉大学に設置のMP-PAWR

マルチパラメータ・フェーズドアレイ気象レーダ（MP-PAWR）とは

MP-PAWRは、水平・垂直偏波の電波を利用することで高精度の観測を実現する機能（MP：Multi Parameter）を備えた高速三次元観測可能なフェーズドアレイ気象レーダ（PAWR：Phased Array Weather Radar）です。雨粒は小さなものはほぼ球形ですが、大きくなるにつれ落下時の空気の抵抗により横にひしゃげた楕円体（鏡餅のような形状）になり、水平・垂直偏波での散乱・伝搬特性が異なるため、この違いを使うことで雨の種類（霧雨と大粒の雷雨など）を識別、降水強度推定の高精度化が可能になります。PAWRは同時に複数方向観測可能なDBF（Digital Beam Forming）による鋭い受信ビームと広角の送信ビームを組み合わせ、これらの送信・受信ビームを仰角方向に高速電子走査します。瞬時に鉛直断面の降水観測を行い、方位方向にはレーダアンテナの機械的な回転（一周30秒）を行うことで、高速三次元観測を実現しています。

図3　埼玉大学を中心とした半径60Km圏内の高速3次元観測範囲
国土地理院の電子地形図（タイル）にレーダ観測範囲を追記して掲載

■関連プレスリリース

- **世界初の実用型「マルチパラメータ・フェーズドアレイ気象レーダ（MP-PAWR(エムピーパー)）」を用いた実証実験の開始について**
  （2018年7月19日付け　http://www.nict.go.jp/press/2018/07/19-1.html）

Webカメラなどの IoT 機器に感染するマルウェア解析に挑む

伊沢 亮一（いさわ りょういち）

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 主任研究員　博士（工学）

安全なインターネット社会を実現したいという想いを抱きつつ、NICTに入所する2012年以前からマルウェア解析の研究をしていました。当時はWindowsに感染するマルウェアが特に猛威をふるっており、Windowsマルウェアが研究の対象でした。私はプログラムの機械語に興味をもっていたこともあり、マルウェアのバイナリ（プログラム）を構成する機械語から悪意ある振る舞いを自動で推定する方法や機械語を基に、マルウェア分類などの研究開発に大学院の研究室メンバーとともに取り組みました。2013年を境にWebカメラやホームルータなどのIoT機器に感染するマルウェア（IoTマルウェア）が徐々に増加し、現在ではWindowsマルウェアに並ぶ脅威となりました。そのため、主な研究対象をWindowsマルウェアからIoTマルウェアに移行し、マルウェア解析の研究に取り組んでいます。

研究の対象をWindowsマルウェアからIoTマルウェアに移行したのですが、WindowsとIoT機器とではいくつかの違いがあり、その違いに苦労しました。例えば、Windowsが動作するPCのCPU（中央演算処理装置）はIntel x86_64というCPUアーキテクチャで、Windowsマルウェアも Intel x86_64の機械語で構成されています。一方、IoT機器にはARMやMIPSなど種々のアーキテクチャのCPUが採用されており、動作するCPUアーキテクチャによってIoTマルウェアの機械語が異なります。そこで、ARMやMIPSの機械語を勉強するところから始め、機械語を基にしたIoTマルウェアの分類手法を研究開発しました。解析対象のマルウェアを分類することにより、類似するマルウェアが事前に分かるため、本分類手法は解析の支援として役立ちます。本手法については、本誌P5「IoTマルウェアの分類」の節でも紹介していますのでご参照ください。

本分類手法は異なるCPUアーキテクチャで動作するマルウェアをひとまとめに扱うことができません。今後は機械語の差異を吸収する方法を考え、CPUアーキテクチャを越えたマルウェア分類に取り組む予定です。捕獲したIoTマルウェア全てを分類することで全体の傾向が把握しやすくなる見込みです。これらの分類を基にIoTマルウェアの脅威に迅速に対応するための研究を進めていきます。

■経歴

2004年　徳島大学工学部知能情報工学科卒業
2006年　徳島大学大学院博士前期課程を修了し、セキュリティ系ベンチャー企業に入社すると同時に神戸大学大学院博士後期課程に進学
2012年　神戸大学大学院博士後期課程を修了し、博士（工学）を取得。同年、NICT入所
2018年　現職

■受賞歴など

- Best Paper Award (The 13th Asia Joint Conference on Information Security)
- FIT2011 ヤングリサーチャー賞

■一問一答

Q：最近はまっていることは？
A：最近になって哲学に関する本を（自宅で）読むようになりました。哲学的な問題を解くために思考する過程が、自身の研究にも役立ちそうな気がしています。

Q：生まれ変わったら？
A：猫になって、肉球がある幸せに浸ります。飽きたら窓際でゴロゴロします。外を見て鳥がいたら「ケケケ」と本能的にクラッキングすると思いますが、このときの猫の気持ちが分かるのが楽しみです。

Q：研究者志望の学生さんにひとこと
A：（研究者になることに不安がある方向けですが）論文執筆が苦でないのであれば研究者として食べていけると思います。

新連載「NICTのチャレンジャー」では、様々なものに挑むNICT職員の横顔をご紹介していきます。

みんなで作る世界一の自動翻訳
翻訳バンク

1億文の翻訳データの集積を目指して、企業等からのデータのご提供をお待ちしております

NICTでは翻訳の高精度化に必要な翻訳データの集積に取り組むとともに、2017年6月からニューラル機械翻訳技術の導入等を進めております。しかしながら、翻訳技術を活用する分野によっては翻訳データが足りないことが課題となっていました。

総務省とNICTは、自動翻訳システムの様々な分野への対応や高精度化を進めるため、オール・ジャパン体制で翻訳データを集積する『翻訳バンク』を2017年9月から運用しています。

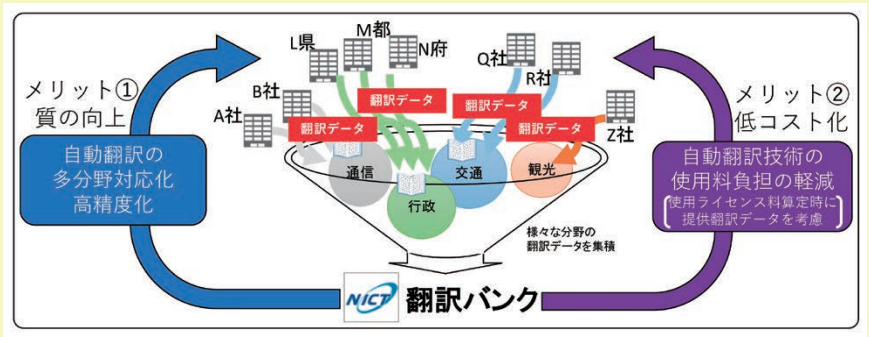
翻訳データとは、原文とそれが様々な言語に翻訳された訳文の対を集めたものです。企業などには技術資料やマニュアルなどの翻訳データが眠っているのではないでしょうか。

NICTはデータを提供していただく方に対し、NICTの自動翻訳技術のライセンス料の負担を軽減する仕組みを用意しました。

ご提供いただけるデータ、若しくはご興味のある方は下記までご連絡ください。
e-mail：h-bank@ml.nict.go.jp

自動翻訳技術のライセンスにご関心がある場合は、下記の問い合わせ先にご連絡ください。
e-mail：textra-info@khn.nict.go.jp

【翻訳バンクURL】http://h-bank.nict.go.jp/



NICT NEWS 2018 No.6 通巻 472
編集発行：国立研究開発法人情報通信研究機構 広報部
発行日：平成30（2018）年11月（隔月刊）

〒184-8795 東京都小金井市貫井北町4-2-1
TEL: 042-327-5392 FAX: 042-327-7587
E-mail: publicity@nict.go.jp

URL: http://www.nict.go.jp/
@NICT_Publicity
#NICT

定期購読のお申込みはQRコード、Webまたは E-mailにて承っております。
ISSN 1349-3531 (Print)
ISSN 2187-4042 (Online)

R70 (再生紙を使用)