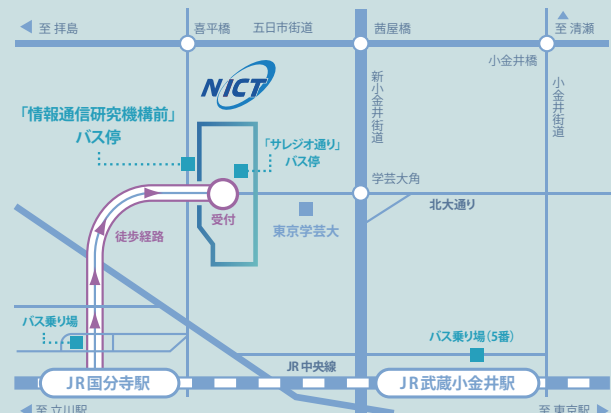




〒184-8795
東京都小金井市貫井北町4-2-1
URL: <https://www.nict.go.jp/>

サイバーセキュリティ研究所
E-mail: cyber-info@ml.nict.go.jp
URL: <https://csri.nict.go.jp/>

NICTに関するお問い合わせは広報部まで
TEL: 042-327-5392 FAX: 042-327-7587
E-mail: publicity@nict.go.jp



国立研究開発法人情報通信研究機構

サイバーセキュリティ研究所

CYBERSECURITY RESEARCH INSTITUTE

Cybersecurity Laboratory
Security Fundamentals Laboratory
Cybersecurity Nexus
National Cyber Training Center
National Cyber Observation Center
General Planning Office



サイバーセキュリティ研究開発の 世界的中核拠点をめざして

Towards a Global Center of Excellence
for Cybersecurity R&D

巧 妙化・複雑化するサイバー攻撃への対策は国を挙げた喫緊の課題となっており、サイバーセキュリティ分野でのNICTに対する社会的要請が高まりつつあります。サイバーセキュリティ研究所では、多種多様なサイバー攻撃から我が国を守るため、NICTの中立性を活かし、産学との緊密な連携によりサイバーセキュリティ研究開発の世界的中核拠点を目指します。また、政府の方針を踏まえ、サイバーセキュリティに関する演習、サイバーセキュリティ産学官連携拠点形成、IoT機器のサイバーセキュリティ対策の促進などの業務を実施します。

N ICTでは、サイバー攻撃に関連した情報を大規模に収集・蓄積し、横断分析する技術の研究開発を進めてきました。令和3年4月からの第5期中長期計画では、これらの技術の高度化を進めるとともに、サイバーセキュリティ情報を分析する国内解析者コミュニティを形成し、社会全体でサイバーセキュリティ人材を育成するための共通基盤を開放することで、日本のサイバーセキュリティの対処能力向上を目指します。また、安心・安全なサイバー空間の実現には、セキュリティやプライバシーを確保した上で、データを安全に利活用する技術が欠かせません。さらに、大規模量子コンピュータが実現すると、現在使われている暗号技術の安全性が脅かされるという懸念もあります。耐量子計算機暗号などの量子コンピュータ時代に対応する新たな暗号技術、並びに、電子政府システム等において現在広く使用されている暗号技術の安全性評価を行ってまいります。

サイバーセキュリティ研究所 研究所長
井上大介



Cybersecurity Laboratory

サイバーセキュリティ研究室

OUTLINE

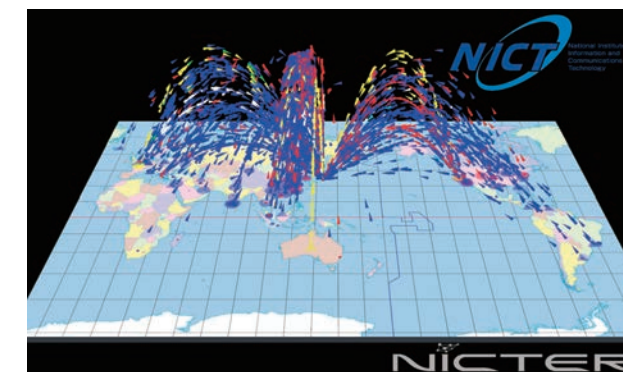
サイバー攻撃対処能力の絶え間ない向上と多様化するサイバー攻撃の対処に貢献するため、『データ駆動型サイバーセキュリティ技術』と『エマージングセキュリティ技術』の2つの柱を軸に研究開発を行っています。特に、巧妙化・複雑化するサイバー攻撃に対応した攻撃観測・分析・可視化・対策技術、大規模集約された多種多様なサイバー攻撃に関する情報の横断分析技術、新たなネットワーク環境等のセキュリティ向上のための検証技術の研究開発に取り組むとともに、研究開発成果の普及や社会実装を目指します。

PROJECTS

データ駆動型サイバーセキュリティ技術

サイバー攻撃のトレンドの変化等に対応するための実践的なサイバーセキュリティ技術の研究開発を行っています。具体的には、無差別型攻撃や標的型攻撃をはじめとする巧妙化・複雑化するサイバー攻撃を複数の側面から観測する技術、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・高度化に取り組んでいます。また、開発した技術や収集した攻撃データ、得られた知見は積極的な社会展開を進めています。

サイバー攻撃観測・分析システム「NICTER」



インターネット上で発生するサイバー攻撃通信を捉え世界地図上で可視化している様子

エマージングセキュリティ技術

新たに社会に登場する技術のセキュリティに関する課題抽出や対策に貢献するため、最新の通信機器、5G / Beyond 5G、コネクテッドカー等のエマージング技術に対応したセキュリティ検証技術の研究開発を行っています。また、人間（ユーザ）の行動様式やメンタルモデル、意思決定プロセスを分析し、ユーザビリティを損ねることなく高いセキュリティを実現するためのユーザブルセキュリティの研究開発にも取り組んでいます。

対サイバー攻撃アラートシステム「DAEDALUS」



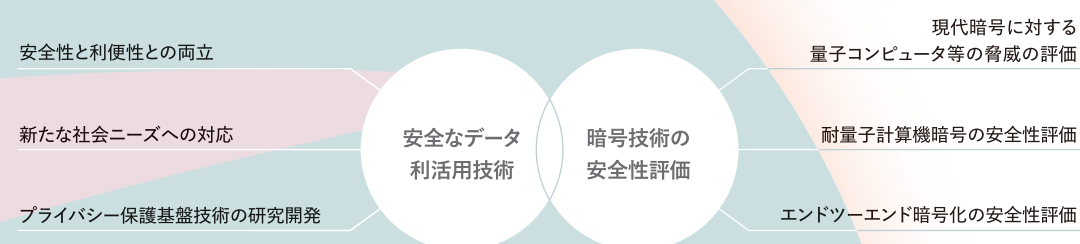
マルウェア（不正プログラム）に感染した機器を検知しアラートが発報されている様子

Security Fundamentals Laboratory

セキュリティ基盤研究室

OUTLINE

セキュリティ基盤研究室では、世界最先端の暗号技術を核に、セキュリティとプライバシー確保の観点で、人々の生活や経済活動を支える様々なシステムの安全な運用に寄与する研究開発を行っています。

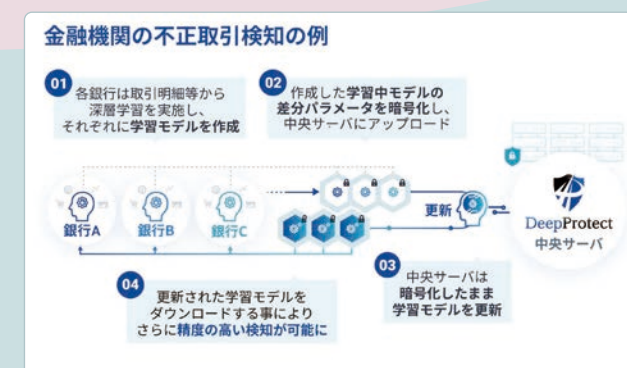


PROJECTS

安全なデータ利活用技術

データの提供・収集・保管・解析・展開の各段階における、セキュリティやプライバシーを確保するため、匿名認証等のアクセス制御技術、秘匿計算等のプライバシー保護解析技術等の研究開発を行っています。これらを用いて組織横断的な連携を含む金融やヘルスケアデータ等の利活用を促進し、関連技術の普及に努めるとともに、安全なテレワーク等の社会的な課題解決に貢献していきます。

DeepProtect プライバシー保護連合学習システム

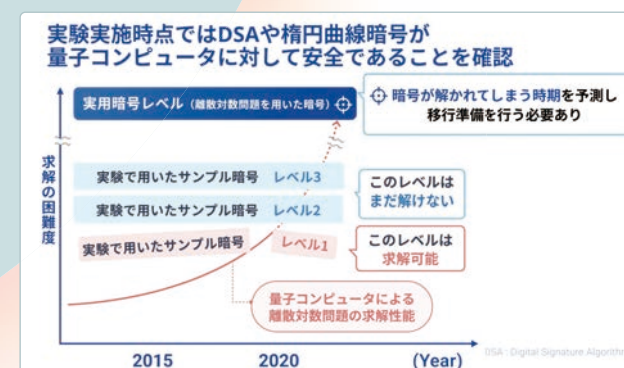


個人情報など機密性の高いデータを開示せずに、複数組織で共同のデータ解析を可能にするDeepProtect

暗号技術の安全性評価

暗号技術の適切な実装と安全な運用に貢献するため、暗号基盤技術の研究開発を行っています。具体的には量子コンピュータ時代にも安全に利用できる、耐量子計算機暗号として世界標準となることが予想されている格子暗号、多変数公開鍵暗号等や、現在広く使用されているRSA暗号、楕円曲線暗号等の安全性評価に関する研究開発に取り組んでいます。またその成果を基に電子政府システム等において使用される暗号技術の安全性評価を行っています。

現在使用されている暗号の危殆化時期を予測する



NICTは量子コンピュータ実機での離散対数問題の求解実験に世界で初めて成功

Cybersecurity Nexus

サイバーセキュリティネクサス

OUTLINE

CYNEX (Cybersecurity Nexus : サイネックス) はこれまでNICTが収集してきたサイバー攻撃等の膨大なデータ、研究開発成果や人材育成の知見を活用し、サイバーセキュリティに関する産学官の巨大な『結節点』となる先端的基盤の構築を目指して新たに組織化されました。サイバーセキュリティ情報を国内で収集・蓄積・分析・提供するとともに、社会全体でサイバーセキュリティ人材を育成するための共通基盤を開放することで、日本のサイバーセキュリティの対応能力向上を目指します。

PROJECTS

CYNEXの活動内容：4つのCo-Nexus

CYNEXでは4つのサブプロジェクト『Co-Nexus』を並行して推進します。



WarpDrive (Web媒介型攻撃対策技術の実用化に向けた研究開発)



攻撃観測網への参加ユーザー募集中

サイバー攻撃は多様化・巧妙化を続け、Webサイトを閲覧するだけでマルウェアに感染するWeb媒介型攻撃による被害が後を絶ちません。CYNEX Co-NexusAのWarpDriveプロジェクトでは、アニメ「攻殻機動隊SAC_2045」シリーズに登場するキャラクター「タチコマ」をモチーフに開発した、Web媒介型攻撃対策ソフトウェア「タチコマ・セキュリティ・エージェント」を無償配布し、ユーザ参加型の攻撃観測網を構築することによって、攻撃の実態解明や攻撃対策の展開を目指しています。

National Cyber Training Center

ナショナルサイバートレーニングセンター

OUTLINE

我が国全体として、多様化・悪質化するサイバー攻撃に対抗し社会の安全を守っていくためには、その担い手となるサイバーセキュリティ人材の育成を一層加速していく必要があります。このような背景を踏まえ、平成29年度総務省予算の成立を受け、NICTは、長年のサイバーセキュリティに関する研究で得られた技術的知見等を最大限に活用することにより実践的なサイバートレーニングを企画・推進する組織である「ナショナルサイバートレーニングセンター」を、平成29年4月1日付けで設置しました。

PROJECTS

ナショナルサイバートレーニングセンターは、以下3つの事業を推進しております。



実践的サイバー防御演習 サイダー CYDER

国の機関、地方公共団体及び重要インフラ事業者等を対象に、組織のネットワーク環境を模擬した環境で、実践的な防御演習を行うことができるプログラムを提供することにより、数千人規模でセキュリティオペレーターを育成。



実践サイバー演習 リブシィ RPCI

NICTが持つ大規模演習環境を活用且つCYDERの演習ノウハウを活かした、リアリティを高めたインシデントハンドリング演習。公的機関初の情報処理安全確保支援士向け特定講習として提供。



若手セキュリティオペレーター育成 セックハック サンロクゴ SecHack365

セキュリティの様々な課題にアイデアで切り込める人材（セキュリティオペレーター）の育成を目的とした、25歳以下のICT人材向けプログラム。NICTの長年の研究開発のノウハウや環境を活かし1年をかけて本格的に指導を行う。

National Cyber Observation Center

ナショナルサイバー オブザベーション センター

OUTLINE

ナショナルサイバーオブザベーションセンターは、NOTICEプロジェクトにおける調査を担う組織として、日本国内のインターネット空間に対して広域スキャンを実施しサイバー攻撃に悪用されるおそれのあるIoT機器を探索します。発見した脆弱なIoT機器の情報はインターネットサービスプロバイダや機器メーカー等に対して提供され、機器利用者等への注意喚起や対処を通じて、インターネットの安全・安全に役立てられています。

PROJECTS

NOTICE

NOTICE(National Operation Towards IoT Clean Environment)は、インターネットに接続されるルーターやネットワークカメラ等のIoT機器のセキュリティ対策を向上させることで、IoT機器の乗っ取りやボットネットの活動の抑制を目指すプロジェクトです。総務省・NICT・インターネットサービスプロバイダ(ISP)が連携し、「サイバー攻撃に悪用されている、またはその危険性があるIoT機器の観測」及び「危険性があるIoT機器のセキュリティ対策」を推進しています。

