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 Laboratory
Security Fundamentals Laboratory
Planning Office

Cybersecurity Research Institute
サイバーセキュリティ研究所

ごあいさつ

私たちの身の回りのモノ、そしてモノに搭載されているセンサーなどがネットワークにつながる IoT（Internet of Things）時代の利便性の陰で、IoT 機器のセキュリティ対策が喫緊の課題となっています。

さらに、IoT 機器から集約されたビッグデータの利活用にあたって、情報漏えいやプライバシーの問題などサイバーセキュリティが扱う課題は日々拡大しています。
国立研究開発法人情報通信研究機構（NICT）サイバーセキュリティ研究所では、直近に迫っている危機から到来する近未来の情報社会課題に対処すべく、サイバーセキュリティ技術の研究開発を進めています。

サイバーセキュリティ研究所が取り組む研究開発としては、サイバー攻撃に実践的に対抗する最先端のサイバーセキュリティ技術や、社会の安心安全を理論面から支える暗号技術などがあります。

サイバーセキュリティ技術

政府機関、地方公共団体、学術機関、企業、重要インフラ等におけるサイバー攻撃対処能力の向上を目指し、最先端の攻撃観測技術や分析技術等を研究開発します。また、サイバー攻撃に関連する情報を大規模に集約し、横断的分析や対策自動化等に向けた技術を確立します。さらに、研究開発成果の速やかな普及を目指します。

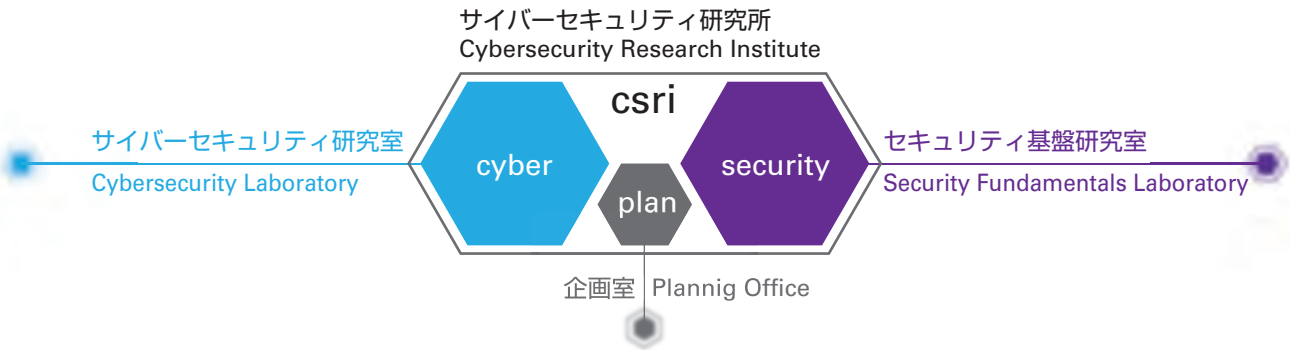
セキュリティ検証プラットフォーム構築活用技術

安全な環境下でのサイバー攻撃の再現や、新たに開発した防御技術の検証に不可欠な、セキュリティ検証プラットフォーム構築に関する技術の研究開発を行います。また、このプラットフォームを活用したサイバー演習等、セキュリティ分野の人材育成支援にも取り組みます。

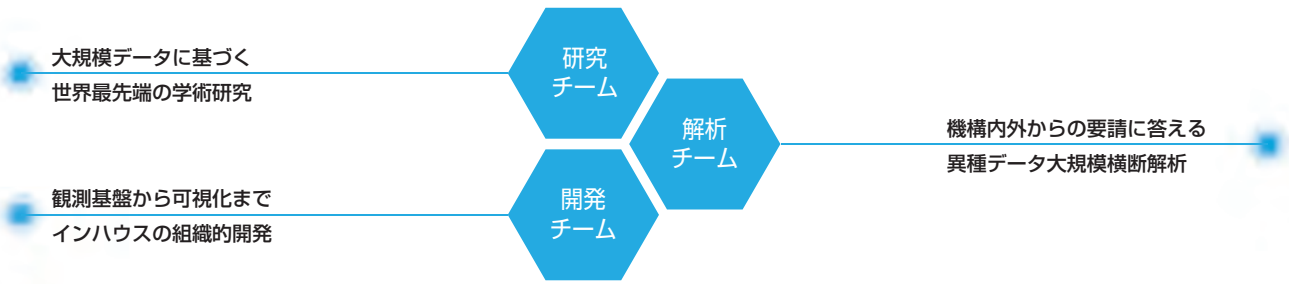
暗号技術

IoT の展開に伴って生じる新たな社会ニーズに対応するため、新たな機能を備えた機能性暗号技術の研究開発に取り組むほか、暗号技術の安全性評価を実施し、新たな暗号技術の普及・標準化及び安心・安全な ICT システムの維持・構築に貢献します。また、パーソナルデータの利活用を実現するためのプライバシー保護技術の研究開発や適切なプライバシー対策を技術支援する活動を推進します。

研究実施体制



サイバーセキュリティ研究室



1. 世界最大規模のサイバー攻撃観測網で収集したデータを集約・分析し、サイバー攻撃への対策の自動化を目指す研究開発
2. セキュリティ人材育成のためのサイバー演習等にも活用可能な可視化技術を含むセキュリティ・テストベッド技術の研究開発
3. 標的型攻撃を統合分析技術の実運用による、能動的・網羅的なサイバー攻撃観測技術を通して得られる膨大かつ網羅的なデータの分析・蓄積・共有技術の開発

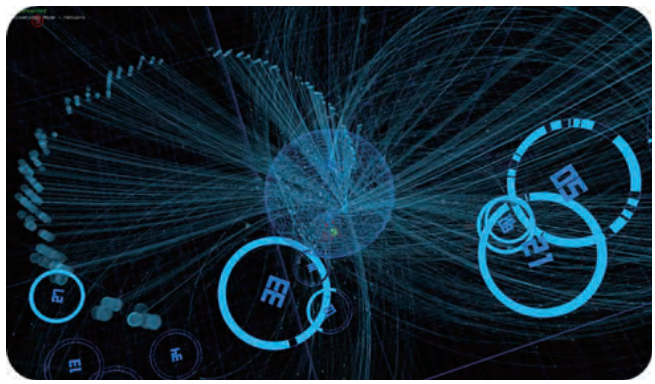
セキュリティ基盤研究室

1. IoT の展開に伴って生じる新たな社会ニーズに対応する、新たな機能を備えた機能性暗号技術の研究開発
2. 暗号技術の安全性評価による新たな暗号技術の普及・標準化及び安心・安全な ICT システムの維持・構築への貢献
3. パーソナルデータの利活用に向けた実用的なプライバシー保護技術の研究開発

Cybersecurity Laboratory
サイバーセキュリティー研究室

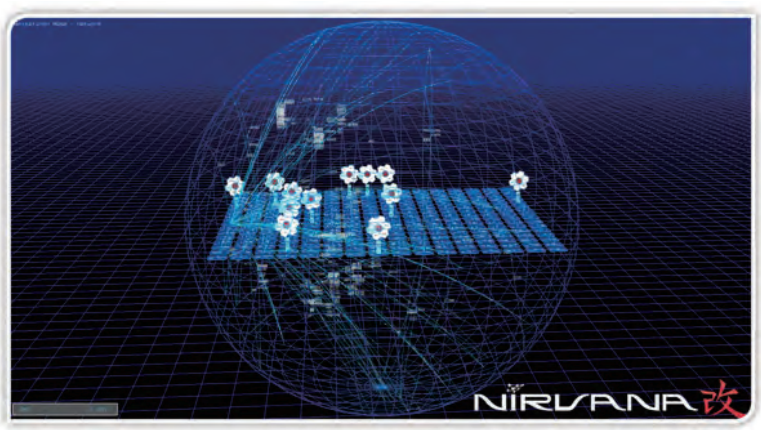
研究室概要

巧妙かつ複雑化したサイバー攻撃や普及する IoT 等への未知の脅威に対応するためのサイバーセキュリティ技術の研究開発を行っています。
また、無差別型攻撃や標的型攻撃等多様化したサイバー攻撃の情報を大量に集約･分析し、サイバー攻撃対策の自動化を目指す技術の研究開発を行います。さらに、研究開発成果を機構自らのサイバー攻撃分析能力の強化のために適用することにより、研究開発における技術検証を行い研究開発成果の速やかな普及を目指します。



アドバンスト・サイバーセキュリティ技術

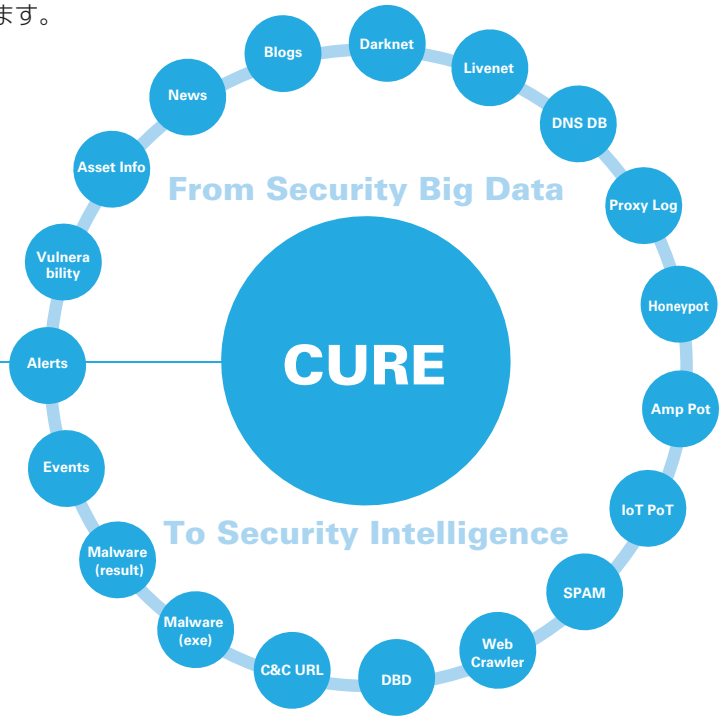
政府や重要インフラを狙うサイバー攻撃への対処能力を向上させるため、能動的・網羅的な観測技術、機械学習等を応用した分析支援や複数情報源を横断解析する分析技術に加え、可視化駆動によるセキュリティ・オペレーション技術、IoT 機器向けセキュリティ技術等の研究開発を行っています。



サイバーセキュリティ・ユニバーサル・リポジトリ技術

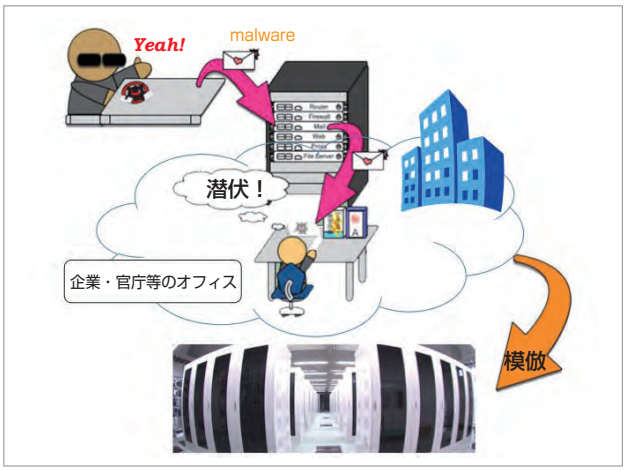
サイバーセキュリティ関連情報を大規模集約し、安全かつ利便性の高いリモート情報共有を可能とするサイバーセキュリティ・ユニバーサル・リポジトリを構築し、これに基づく自動対策技術の研究開発を行っています。また、この技術を用いたセミ・オープン研究基盤を構築し、セキュリティ人材育成に貢献します。

サイバーセキュリティ・ユニバーサル・リポジトリ
CURE（Cybersecurity Universal Repository）



セキュリティ検証プラットフォーム構築活用技術

サイバーセキュリティ技術の研究開発を効率的に行うために、サイバー攻撃の安全な環境下での再現や新たな防御技術の検証等を実施可能な検証プラットフォームの構築を行い、その活用のための模擬環境・模擬情報活用技術及びセキュリティ・テストベッド技術の研究開発を行っています。



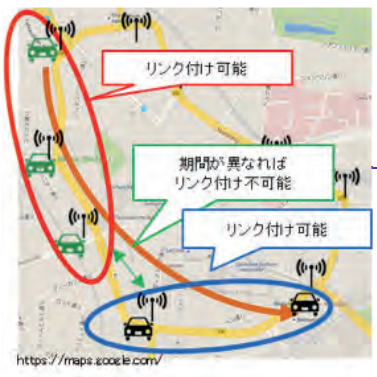
Security Fundamentals Laboratory
セキュリティ基盤研究室

研究室概要

IoT の展開に伴って生じる新たな社会ニーズに対応するため、新たな機能を備えた機能性暗号技術や軽量暗号・認証技術の研究開発を行っています。
また、暗号技術の安全性評価を実施し、新たな暗号技術の普及・標準化に貢献するとともに、安心・安全な ICT システムの維持・構築に貢献します。さらに、パーソナルデータの利活用に貢献するためのプライバシー保護技術の研究開発を行い、適切なプライバシー対策を技術面から支援します。

機能性暗号技術

従来の暗号技術が有する暗号化や認証の機能に加え、今後新たに生じる社会ニーズに対応する新たな機能を備えた暗号技術である機能性暗号技術の研究開発を行います。具体的には、暗号化したまま検索が可能な暗号方式、匿名性をコントロール可能な認証方式、効率的でセキュアな鍵の無効化や更新方式等の研究開発を行います。
また、コスト、リソース、消費電力等に制約のある IoT デバイスにも実装可能な軽量暗号・認証技術に関する研究開発を行います。



- 路車間通信においてプライバシー保護を実現する軽量グループ署名

暗号技術の安全性評価

日々進化する暗号技術に対する脅威に対抗するため、電子政府システムをはじめ国民生活を支える様々なシステムで利用されている暗号方式やプロトコルの安全性評価を継続して実施し、システムの安全性維持に貢献します。
また、今後の利用が想定される新たな暗号技術に対しても安全性評価を実施し、その普及・標準化及び ICT システムの長期にわたる信頼性確保に貢献します。

格子暗号の安全性評価　TU Darmstadt Lattice Challenge
https://www.latticechallenge.org/

CRYPTREC（クリプトレック）

Cryptography Research and Evaluation Committees の略で、電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクトです。　CRYPTREC Web サイト http://cryptrec.go.jp/

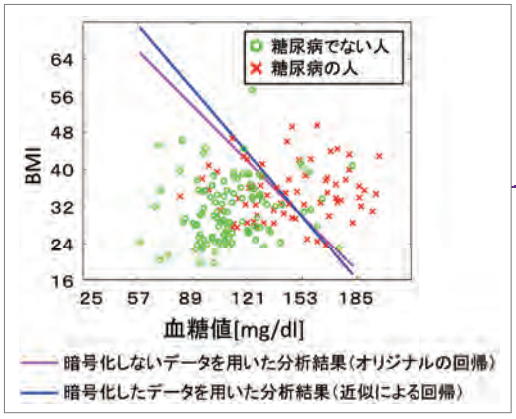
CRYPTREC 体制

暗号技術検討会
事務局：総務省、経済産業省

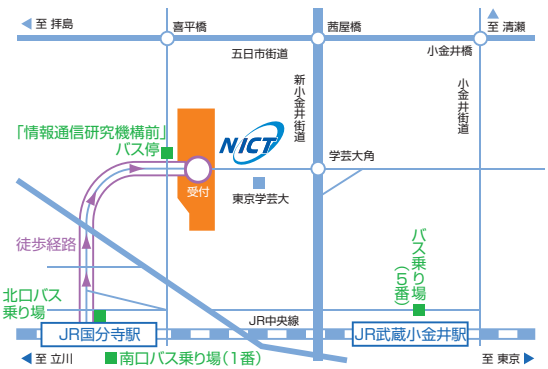
暗号技術評価委員会 事務局：NICT、IPA	暗号技術活用委員会 事務局：IPA、NICT
暗号技術の安全性 / 実装評価を中心とした技術的な検討課題を担当	セキュリテイ対策の推進、暗号技術の利用促進及び産業化を中心とした暗号利用に関する検討課題を担当

プライバシー保護技術

個人情報及びプライバシーの保護を図りつつ、パーソナルデータの利活用に貢献するために、準同型暗号や代理再暗号化技術等を活用し、データを暗号化したまま様々な解析を可能とする技術等の研究開発を行っています。また、パーソナルデータ利活用におけるプライバシー保護を技術支援するため、ポータル機能の構築等の活動を行います。



暗号化したままデータを分類できるビッグデータ向け解析技術



国立研究開発法人
情報通信研究機構
National Institute of Information and Communications Technology

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

サイバーセキュリティ研究所
Tel:(042)327-5807
E-mail:cyber-info@ml.nict.go.jp
URL:http://www.nict.go.jp/csri/

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

2017.02