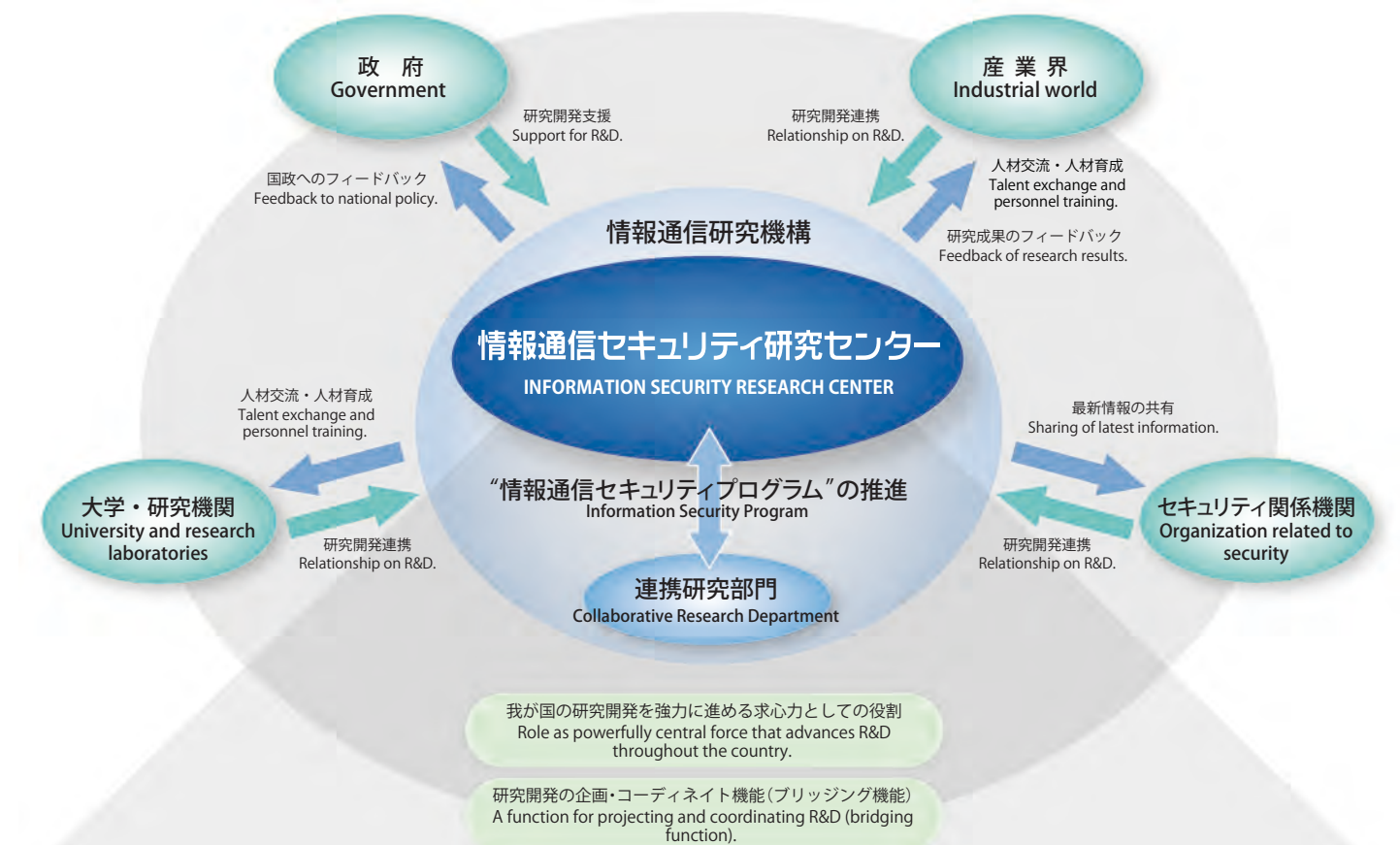


情報通信セキュリティ研究センターの組織  
Organization of the Information Security Research Center, NICT



情報通信セキュリティ研究センター INFORMATION SECURITY RESEARCH CENTER

**推進室**  
●セキュリティに関する研究テーマの総合調整  
●研究開発環境の整備の促進  
●外部機関などの連携の推進

**Project Promotion Office**  
●Overall coordination of security-related research themes  
●Creation and promotion of R&D environment  
●Promotion of collaborative relationship with external organizations etc.

**インシデント対策グループ**  
●サイバー攻撃の情報収集・管理に関する研究  
●インシデントの分析・対策に関する研究

**Network Security Incident Response Group**  
●Research on monitoring and management of network event data  
●Research on analysis of and response to network incidents

**トレーサブルネットワークグループ**  
●サイバー攻撃を追跡可能なネットワークに関する研究  
●インシデントの再現ネットワーク技術に関する研究

**Traceable Secure Network Group**  
●Research on traceable network technologies against cyber attacks  
●Research on development of testbed for emulation of network incidents

**セキュリティ基盤グループ**  
●暗号技術・暗号プロトコルの研究  
●漏洩電磁波セキュリティ、サイドチャネル攻撃対策の研究  
●電子政府暗号の安全性の確保

**Security Fundamentals Group**  
●Research on cryptographic protocols and cipher technologies  
●Research on information security under electromagnetic threat and side-channel attacks  
●Establishment of secure ciphers for e-government

**防災・減災基盤技術グループ**  
●非常時における通信網の構築・確保に関する研究  
●防災・減災のためのユビキタス情報通信技術の研究

**Disaster Management and Mitigation Group**  
●Research on ensuring info-communications infrastructure in emergencies  
●Research on ubiquitous ICT for disaster management and mitigation



**NICT** 独立行政法人 情報通信研究機構

独立行政法人 情報通信研究機構  
情報通信セキュリティ研究センター  
〒184-8795 東京都小金井市貫井北町4-2-1 (小金井本部)  
TEL 042-327-7429  
URL <http://src.nict.go.jp/>

National Institute of Information and Communications Technology  
Information Security Research Center  
4-2-1, Nukui-Kitamachi, Koganei, Tokyo 184-8795, Japan (Koganei Headquarters)  
Phone +81 42 327 7429  
URL <http://src.nict.go.jp/index-e.html>

NICTIに関するお問合せは下記まで  
総合企画部 広報室  
Tel: 042-327-5392 Fax: 042-327-7587  
e-mail: [publicity@nict.go.jp](mailto:publicity@nict.go.jp)  
URL <http://www.nict.go.jp>

INFORMATION SECURITY RESEARCH CENTER

コミュニケーションの安心・安全をリードする研究開発拠点  
情報通信セキュリティ研究センター

情報通信セキュリティ研究センター

ごあいさつ  
Message

情報通信セキュリティ研究センター長  
篠田 陽一  
Executive Director,  
Information Security Research Center  
Yoichi SHINODA, Ph.D.



私たちの生活は、かつてないほど情報通信ネットワークへの依存度を高め、その利便性を大いに享受していますが、それと同時にさまざまなセキュリティ上の問題もクローズアップされています。

情報通信セキュリティ研究センターは、このような問題に対応していくため、情報通信研究機構(NICT)の第2期中期計画にともなう改組の一部として生まれた「安心・安全のためのICT」研究領域において、情報通信の、そして情報通信による安心・安全な生活をリードする研究開発拠点を形成すべく結成された研究センターです。

当センターの研究開発は、ふたつの大きな考え方のもとで進められています。ウイルスなどの悪意のあるソフトウェアに対応する技術や、時空を問わないトレスバック(発信元追跡)技術、そして情報を守るための暗号技術や電磁波技術を組み合わせることで、トラクタブル(扱い易い)なネットワークを実現していくという考え方、また、より便利な生活のためだけにICTを利用するのではなく、いざという時に生命や財産を救うためにも利用しようという、ICTによる防災・減災の考え方です。

私たちは、独立行政法人の組織としては唯一、情報通信における安心・安全を明示的に扱う研究ユニットとしての責任感・使命感のもと、ICTが便利さだけでなく、安心と安全をも意味するようになる日をめざして着実に研究開発を推進していきたいと考えています。

Our everyday life depends heavier on information networks than ever before, and we are enjoying conveniences brought by them more than ever. However, various issues in security have been recognized as well at the same time.

Our research center is the part of the "ICT for security and safety" research area which has been defined as a part of NICT's new 5-year mid-term research plan, to cope with such issues. We are intended to be the leader of research and development in establishing safe and secure life of people through information-communication technologies.

Our research and development are organized under two major goals. One is the realization of a secure and tractable network, through the use of next generation malware handling and traceback technologies. Another is the establishment of ICT that not only tolerates disasters, but also provides means to protect life and property of people under such conditions.

With the responsibility and mission brought by being the sole research unit within government agencies that explicitly handle safety and security in and by info-communication technologies, we would like to steadily conduct our research and development activities for the day that ICT not only means convenience, but also safety and security.

# コミュニケーションの安心・安全をリードする研究開発拠点

## Leading R&D activities in safety and security for and by info-communication technologies



**インシデント分析センター"nicter"**  
ネットワーク上の攻撃の検知とその原因となり得るウイルス等の解析により、インシデントを迅速かつ正確に検知し、対策を導出する研究開発を行うためのインシデント分析センターです。

**Incident analysis center "nicter ; network incident analysis center for tactical emergency response"**  
A center for developing quick and accurate incident detection and response technologies by analyzing computer viruses and worms.



**リアルタイムモニタリングシステム**  
ネットワーク上におけるトラフィックや攻撃をリアルタイムでモニタするシステムです。

**Real-time monitoring system**  
A system for monitoring network traffic and ongoing cyber attacks in real time.



**インシデント分析システム**  
収集したイベントデータを用いてインシデントの発生を自動的に検知するシステムです。

**Incident analysis system**  
A system for detecting occurrence of incident from monitored event data.



**モニタ表示画像情報漏洩評価システム**  
コンピュータから放出電磁波として漏洩する表示情報を評価する装置です。

**Evaluation system for display information leakage**  
A system for evaluating the display information leakage from computers through electromagnetic emanation.



**高出力電磁波照射システム**  
高出力電磁波を照射するシステムです。

**High-power microwave system**  
A system for radiating intentional high power electromagnetic wave.



**サイドチャネル解析評価システム**  
暗号モジュールのサイドチャネル信号を解析するシステムです。

**Side-channel signal analyzing system**  
A system for analyzing the side-channel signal observable from cryptographic modules.

**Technologies to monitor and manage network event data**  
We are researching monitoring method of network event data and management technologies of captured data to detect cyber attacks.

**Event analysis technology**  
We are researching incident detection technologies by analyzing behavior of computer viruses and monitored event data.

**Cyber attacks response technologies**  
We are researching contingency plans against incidents detected by event analysis.

**イベント収集・管理技術**  
サイバー攻撃の発生を検知するため、ネットワーク上の様々な事象（イベント）に関するデータを収集・管理する技術について研究しています。

**イベント分析技術**  
収集したイベントデータの分析から、ウイルスの挙動やインシデントの発生を検知する技術について研究しています。

**サイバー攻撃対策技術**  
イベントがインシデントと検知された後の緊急対策について研究しています。

**サイバー攻撃によるネットワークインシデントの分析・対策技術**  
Detection and Prevention of Network Incidents Caused by Cyber Attacks

**サイバー攻撃の発生・拡大を追跡・予測可能とする技術**  
Technologies to provide Networks with Traceability and Predictability against Emergence and Proliferation of Cyber Attacks

**トレーサブルネットワーク技術**  
ネットワーク上におけるサイバー攻撃・不正アクセスへの対策として、発信元追跡技術について研究しています。

**再現ネットワーク技術**  
ネットワーク上におけるウイルスの挙動解析や発信元追跡の精度や実用性を評価する再現ネットワーク技術の研究を行っています。

**セキュア・オーバーレイ技術**  
インターネット上にセキュアなネットワークを重畳することにより安全な通信基盤を確立する方法の研究を行っています。

**Traceable network technologies**  
We are researching technologies to detect and reveal the source of cyber attacks and security incidents.

**Testbed for emulation of cyber attacks**  
We are developing testbed ( i.e. network for experiment ) for analyzing behavior of computer viruses and worms and validating the effectiveness and feasibility of our traceback system.

**Secure overlay technologies**  
We are researching the overlay network system over Internet for secure information transmission and communication.

**Research on design and analysis of authentication and cryptographic protocol**  
We investigate the secure ubiquitous network methodologies such as applications of formal methods in verification of security protocols, design and analysis of new anonymous authentication protocols, and lightweight public-key cryptosystems and infrastructure.

**Research on analysis and evaluation of crypto algorithms**  
We analyze and evaluate the security of crypto algorithms against various attack methods. We also develop provable secure constructions of crypto algorithms.



**暗号・認証プロトコルの設計・評価技術**  
形式的手法に基づく暗号プロトコルの安全性評価手法の開発や、新しい匿名認証プロトコルの提案・評価を行っています。また、ユビキタスネットワーク社会を考慮した公開鍵暗号の軽量化について研究を行うことで、安心・安全なネットワーク社会の基盤を構築しています。

**暗号アルゴリズムの安全性評価**  
暗号アルゴリズムを解析し、様々な攻撃手法に対する安全性を評価しています。安全性を証明できる構成手法の開発を行っています。

**暗号・認証技術の研究開発**  
Research on Cryptology and Authentication

# INFORMATION SECURITY RESEARCH CENTER

## 情報通信セキュリティ研究センター

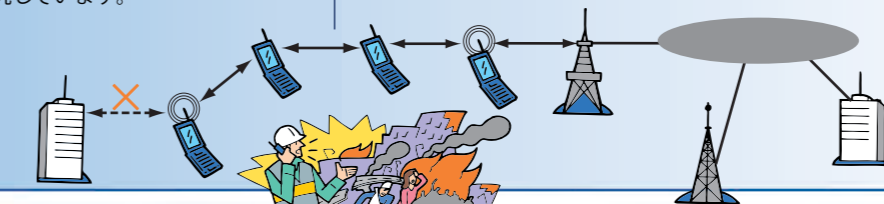
**災害に強いネットワーク構築技術の研究**  
Research on Emergency Communications Networks

**非常時におけるアドホックネットワーク形成技術**  
災害時に移動端末間の一時的・自律的なネットワーク接続を確立し、基地局を介さずとも通信を確保するための技術について研究しています。

**災害時のネットワーク制御基盤技術の研究**  
災害時の通信需要の増加により起こる輻輳に対しても多くの通信ができるための様々な制御技術について研究しています。

**Research on ad hoc network configuration technologies for emergency communications**  
We are researching ad hoc network technologies that enable communication by establishing temporary and autonomous connection among mobile terminals without base stations at the time of disaster.

**Research on network-control fundamental technologies during disasters**  
We are researching network-control technologies so that many people can use communication networks even in congested situations caused by rapid increases of call demands during disasters.



**Research on evaluation and countermeasures against the information leakage caused by electromagnetic emanation.**  
We study evaluation and countermeasures against the information leakage caused by electromagnetic emanation from electronic devices.

**Research on side-channel analysis and countermeasures**  
We gather and analyze the side-channel signals coming from various cryptographic modules and develop the effective countermeasures against the potential side-channel attacks.

**Research on security of signal and data processing against malicious electromagnetic radiation.**  
We study security problems of signal and data processing on information systems against malicious electromagnetic radiation and develop the effective countermeasures.

**放出電磁波による漏洩情報評価・対策技術**  
情報機器から放出される電磁波に起因する情報漏洩問題に対して、漏洩する情報量の定量的な評価方法および対策技術について研究しています。

**サイドチャネル解析と対策技術**  
暗号モジュールのサイドチャネル解析に対して、観測する信号の評価と暗号解析について研究するとともに、その対策技術について研究しています。

**侵入電磁波に対する情報セキュリティ評価・対策技術**  
情報機器への電磁波照射による回路の故障や誤動作について解析し、侵入電磁波とデータ改変の評価およびその対策技術について研究しています。

**電磁波に関する情報セキュリティ**  
Research on Information Security under Electromagnetics Threat

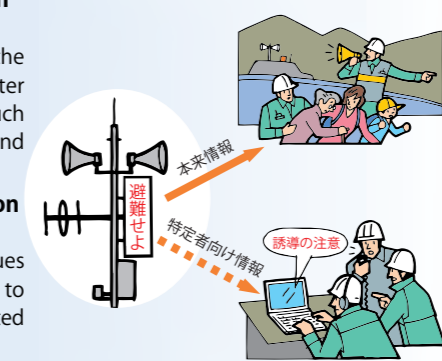
**災害時の情報収集・伝達を支援するICTシステムの研究**  
Research on the ICT for Information Gathering and Delivery in Disaster Situation

**ユビキタスデバイスを用いた被災地情報収集・共有技術の研究**  
災害情報授受用に工夫したRFID（電子タグ）、センサー、マイクロサーバ等の小型デバイスを多数配置して、防災・減災に役立つ情報を正確に授受し共有する技術について研究しています。

**災害時に応用可能な情報多重化技術の研究**  
災害時の限られた通信容量を最大限に生かすため、本体情報に付加情報をアプリケーションレベルで重畳し、伝送可能情報量を増やす情報多重化技術について研究しています。

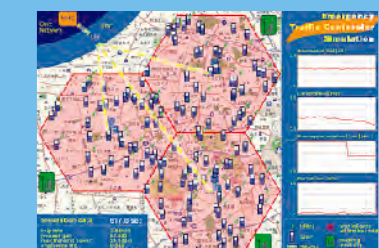
**Research on information gathering / sharing technology for disaster prevention and mitigation using ubiquitous devices**  
We are conducting research and development of the technology to receive, deliver and share the disaster information correctly by using many small devices, such as RFID (Radio Frequency Identification tag), sensors and microcomputers.

**Research on information multiplexing contribution for disaster mitigation**  
We are researching information multiplexing techniques on an application layer which is expected to contribute to the increase of message capacity calmly under the limited resources of communication at the time of emergency.



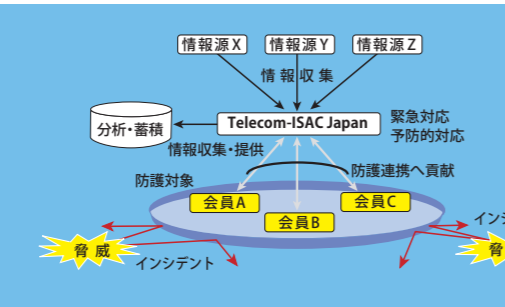
**輻輳対策技術シミュレーションシステム**  
災害時の通信の輻輳に対する様々な制御技術の研究するためのネットワークシミュレーションシステムです。

**A network simulation system for congestion-control technologies**  
A network simulation system to research on network-control technologies in congested situations during disasters.



**RFIDの防災応用**  
RFID（電子タグ）を位置情報の発信源や被災地情報の共有手段として用いる研究をしています。

**RFID system for use in disaster relief as positioning source and emergency message boards**  
We have developing systems that uses radio frequency identification (RFID) tags both as the source of location information and as data storage units to record messages or information in disaster situations.



**財団法人日本データ通信協会 Telecom-ISAC Japan**  
通信サービスの提供を妨げる各種インシデントを収集・分析し、その分析結果をインターネットサービスプロバイダ等からなる会員間で共有することにより、インシデントに対する強固な情報通信基盤の提供を目指すための組織です。

**Nippon Information Communication Association Telecom-ISAC Japan (Telecom Information Sharing and Analysis Center Japan)**  
Telecom-ISAC Japan was founded to help build up a solid telecommunication infrastructure by collection and analysis of security incidents, e.g. security attacks and security accidents, and by sharing this information with ISP members.



**CRYPTREC (クリプトレック：暗号技術検討会及び暗号技術監視委員会の総称)**  
暗号技術の評価し、安全な暗号技術を電子政府推奨暗号リストにまとめ、その安全性および信頼性を監視する委員会です。CRYPTREC統一WEBサイト <http://www.cryptrec.jp/>

**CRYPTREC (Cryptography Research and Evaluation Committees)**  
CRYPTREC evaluated cryptographic techniques, established the e-government cipher list out of secure cryptographic techniques, and monitors its security and reliability. <http://www.cryptrec.jp/>

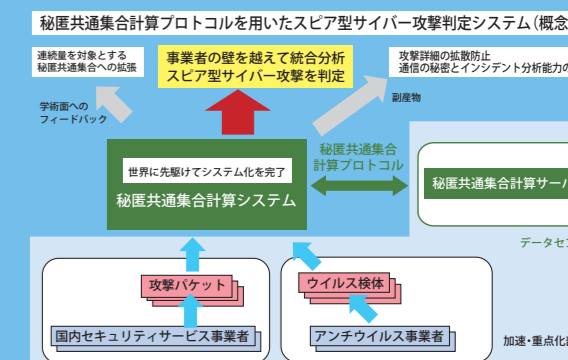
**VM Nebula**  
PCエミュレータと仮想ネットワーク (VLAN) を用いて、インターネット上の攻撃への対策技術を検証するための装置です。

A simulation system for Internet security using PC emulators (virtual machines) and virtual LANs for virtualizing the Internet and targets.



**秘匿共通集合計算プロトコル**  
暗号関連技術を使い、複数の組織が有する情報を、互いに開示することなく、解析する技術を開発しています。

**Privacy-preserving computations**  
Cryptographic techniques which enable us to analyze the sensitive information stored among organizations have been developed.



**災害対応ロボット間通信用アドホックネットワーク**  
被災者探索を行うロボット群の通信・制御手段として、ロボット間のアドホックネットワークを使用した通信技術のシミュレーションと実機を使った検証を行っています。

**Inter-robot ad hoc network for disaster management**  
Novel ad hoc network technology for rescue robots' communication and control has been developed on network simulator and real rescue robot system.

