ISSN 1349-3531

NICT NEWS

独立行政法人
情報通信研究機構

2009
APR
NO.379
4

National Institute of Information and Communications Technology

情報通信セキュリティ研究センター特集

NiCT

巻頭インタビュー

4つのアプローチで進む 情報通信セキュリティ研究

安心・安全なネットワーク社会の実現を目指す

篠田　陽一
（しのだ　よういち）
情報通信セキュリティ研究センター
研究センター長

大学院修了後、東京工業大学助手、北陸先端科学技術大学院大学情報科学研究科助教授を経て、同大学院大学教授として現在に至る。2006年より情報通信研究機構情報通信セキュリティ研究センター長（兼務）、2007年より内閣官房情報セキュリティセンター補佐官（兼務）。博士（工学）。

情報通信セキュリティ研究センターが目指しているのは、情報通信技術による安心・安全なネットワーク社会の実現です。現在、4つのグループが未来を見すえた先進的な研究を進めています。

情報通信技術で安心・安全な社会を

――情報通信セキュリティ研究センターではどのような研究をされていますか。

篠田　「セキュリティ」というと、コンピュータウイルスやネットワークからの侵入といったイメージがありますが、私たちは「安心」とか「安全」というような広い意味でとらえています。情報通信と安心・安全技術の関係には2つの面があり、「情報通信による安心・安全技術の研究」と「情報通信のための安心・安全技術の研究」の2つの分野で研究を進めています。

「情報通信による安心・安全技術の研究」というのは、情報通信技術を使って、国民の生命や財産を守り、安心・安全な社会を作るためのもので、「防災・減災基盤技術グループ」が研究を行っています。「情報通信のための安心・安全技術の研究」とは、通信を暗号化したり、データの改ざんを追跡するといった研究で、「インシデント対策グループ」と「トレーサブルネットワークグループ」が研究を行っています。このほか、主に基礎理論を扱っている「セキュリティ基盤グループ」が、両方にまたがった活動をしています。

センターを構成する4つの研究グループ

――防災・減災基盤技術グループでは、どのような研究をしていますか。

篠田　情報通信技術はすべてのインフラのためのインフラ、「メタインフラ」といえます。電話をかけるにも、電気を分配するにも、交通機関を運行させるにも情報通信技術が使われています。災害が発生した場合に、非常時の通信システムなどを使って他のインフラをどのように支えていくかというのが、この研究の目的です。例えば電線が切れたり電源が落ちたりすると、交換機が動かなくなり、電話が通じなくなってしまいます。そのような時にどうやって通信網を再構築するかを研究しているわけです。「必要な情報を、必要な時に、必要な人あるいは場所に」というのがキャッチフレーズです。

――セキュリティ基盤グループでは暗号の研究をしているのですか。

篠田　暗号技術によって安心・安全な通信技術を確立することを目指しています。暗号というと、数学っぽい話に聞こえますが、それだけではなく、暗号そのものに新しい暗号をかける研究や、国の電子政府をサポートする研究など、いろいろなことをしています。

――今の暗号技術は安全なのでしょうか。

篠田　今使われている暗号システムが安全かどうかを検査することも仕事の1つです。そのほか、暗号を使ったいろいろなアプリケーションをシステムとして構築した時の安全性も検証しています。もちろん、他のグループへの技術提供も行っています。

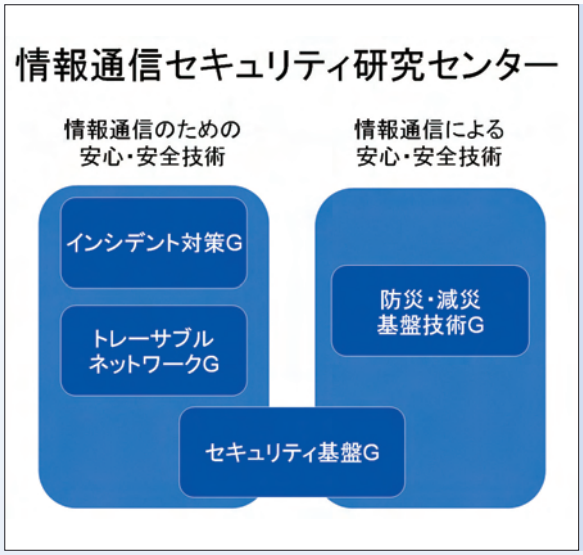
それから、携帯電話やパソコンなどの電子機器の漏えい電磁波を解析すると、その機器が今どんな動作をしているのかがわかってしまいます。これを防止する電磁波セキュリティ技術や物理セキュリティ技術も研究しています。

安心・安全なトラクタブルネットワークの実現へ

――インシデント対策とはどのような意味なのでしょうか。

篠田　インシデント対策というのは、金銭的な目的、または機密情報を盗む目的で実行されるサイバー攻撃を探知

し、解析し、改善に向けた対策をとることをいいます。インシデント対策グループでは、日本の広域で発生している実際の攻撃をリアルタイムで見て直接的な対処を行ったり、攻撃がどんな風に変わるかを予測したり、その予測に基づいた対策を研究するなど、サイバー攻撃に対する総合技術の研究開発をしています。ネットワーク上で観測・検知した攻撃をリアルタイムで自動分析し、可視化しているのが、最先端インシデント分析センター（nicter）です。



●情報通信セキュリティ研究センター4つの研究グループ

●最先端インシデント分析センターnicter

――トレーサブルネットワークグループはどのような研究をしていますか。

篠田　トレーサブルネットワークグループの目的は、時空を超えて問題の追跡をすることです。ドラマなどでよく電話を逆探知するシーンがありますね。あれは、空間を超えて相手を検出するということをしているわけです。現在の電話なら一瞬で逆探知できますが、インターネットに代表されるデータネットワークでは、今ひとつうまくいかないのです。トレーサブルネットワークグループでは、まずそこを克服して空間的に逆探知できるようにしようとしています。

さらに、時間を超えて問題の発生を追跡するという研究もしています。例えばウイルスの活動が発生した時、侵入した瞬間の状態など重要な瞬間を再現できるようになれば、同じ問題が発生しないように抑制することができます。

――2つのグループともサイバー攻撃対策を研究しているわけですね。

篠田　センター内では、2つを組み合わせて「トラクタブルネットワーク」という考え方を打ち出しています。ネットワークのようにたくさんのシステムを積み上げていくと、必ず不安定になって問題が発生します。そこで、問題が起きることは許容するけれど、問題を探知し、解析し、対策を取り、さらには問題の発生にまでさかのぼって解析し、再発を許さない。そうした機能を持つネットワークを作ろうという考え方がトラクタブルネットワークです。

「セキュリティ」は総合科学、だから面白い

――セキュリティ研究の特徴は、どのあたりにありますか。

篠田　セキュリティの研究はとても特殊です。ややこしいというか、面白いところなのですが、セキュリティの技術が完成すると、問題そのものがなくなってしまうという性質があります。また、セキュリティ技術そのものが他の技術、例えば情報通信に関する技術がないと成立しません。つまり、「セキュリティ」という単独の学問は存在せず、今までに研究開発されてきた他分野の知識を集めて仕立て直す、いわば総合科学なのです。暗号であれば数学ですし、データベース間の演算というような話であればデータベース技術や通信技術です。防災・減災の研究では、パニック時に人間がどの位の情報量を受け取ることができるかという問題を扱いますが、これは人間行動学や心理学、社会行動学の分野です。他にもハイパフォーマンスコンピューティング技術や「確率と推論」を扱うような人工知能分野の学問。このように、いろいろな研究分野を組み合わせて、総合的にセキュリティ研究を行っているのです。

――本日はありがとうございました。

安全なネットワーク環境を目指して

インシデント分析センター nicterの紹介

日本のインターネットを守るために

インターネットは今や、私たちの生活には欠かすことのできないツールとなっています。その一方でインターネットを経由したマルウェアの蔓延やそれに伴う情報漏えい、ユーザーをフィッシングサイトへと誘導する大量のスパムメール、Webサーバに対する情報改ざんやサービス不能攻撃など、様々なインシデント（セキュリティ事故）が日々発生しています。その対策は、ユーザーレベルではウイルス対策ソフトやパーソナルファイアウォール、企業などでは侵入検知システム（IDS）や侵入防止システム（IPS）などのセキュリティ技術が導入されています。これらの対策は局所的な「点」で守るセキュリティ技術で、各ユーザーや企業などの組織向けの対策です。しかし、社会インフラとしてインターネット全体を考えるとき、その安全性は点で守るだけでは十分とは言えません。

情報通信セキュリティ研究センターインシデント対策グループでは、日本のインターネットを守るための研究開発を目的に、ネットワークに対する攻撃を「点」ではなく「面」で観測する、インシデント分析センター nicter（Network Incident analysis Center for Tactical Emergency Response）の構築を行っています。

nicterの全体像

nicterは、広域のネットワーク攻撃の様子を観測・分析する「マクロ解析システム」、ネットワーク攻撃の原因であるマルウェアの解析を行う「ミクロ解析システム」及び攻撃の様子とその原因であるマルウェアを結び付けて原因を特定する「相関分析システム」で構成されています（図1）。

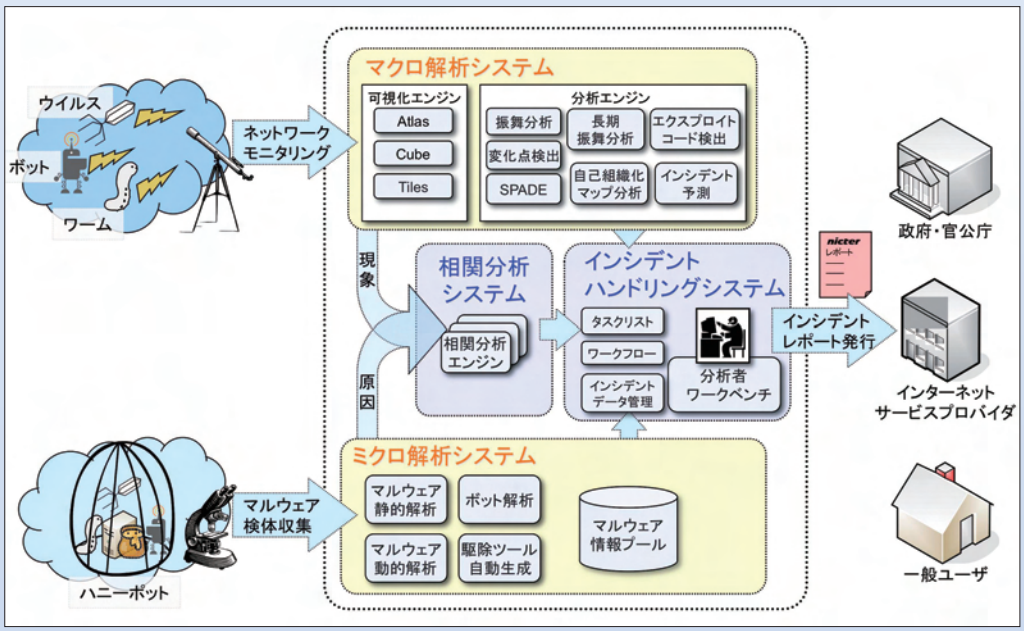
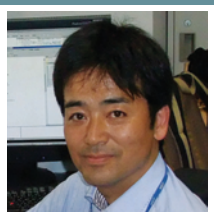


図1●nicterの全体像

【マクロ解析システム】

インターネット全体を見渡して、インターネットに何が起こっているかをリアルタイムに観測・分析を行います。国内複数の拠点に合計12万以上のIPアドレス群のセンサーを設置して観測しています。このセンサーはダークネットと呼ばれる、インターネット上で到達可能で、かつ未使用なIPアドレス空間に設置しています。未使用のIPアドレスにパケットが送信されることは、通常のインターネット利用では起こらないのですが、実際には相当数のパケットが到達しています。これらのパケットの多くは、ネットワークを経由してマル

●Profile●



大高 一弘
（おおたか かずひろ）
情報通信セキュリティ研究センター
インシデント対策グループ
研究マネージャー

1980年電波研究所（現NICT入所）。電離圏電波伝搬の研究、南極オーロラレーダ開発に従事。31次及び36次隊で南極越冬隊に参加。宇宙天気予報研究の後、現在はインシデント分析センターnicterの研究開発に従事。

ウェアを感染させることを目的に送信されています。観測されたパケットは、可視化エンジン（Atlas, Cube, Tiles）（図2～4）でリアルタイムにネットワーク攻撃の様子を直感的に分かりやすく表示し、観測することが可能になります。

【ミクロ解析システム】

ネットワーク攻撃の原因であるマルウェアの解析を行います。マルウェアの収集にはハニーポットやWebクローラ等を使用しています。収集されたマルウェアを自動的に解析しており、1日に約2000検体まで解析が可能です。ミクロ解析システムは静的解析エンジンと動的解析エンジンと呼ぶ2つの解析エンジンを用いて分析を行っています。

【静的解析エンジン】マルウェアの実行コードを逆アセンブルしてアセンブラレベルでマルウェアの持つ機能や特徴を詳細に解析します。得られたアセンブリコードから、マルウェアの実行コードに含まれるAPIのリストやアクセスに使用するメッセージの文字列など情報の抽出を行います。

【動的解析エンジン】マルウェアを実マシン上で実行させて、マルウェアが使用したAPIやネットワークアクセスなどの挙動を解析します。この動作を実ネットワーク環境で行うと、新たな感染活動やネットワーク攻撃を始めるため、完全に隔離した疑似ネットワーク環境を構築して解析を行っています。

最近のマルウェアは、実ネットワークと疑似ネットワークの識別を行っており、本来の感染活動・ネットワーク攻撃を開始しないことが多くなっています。マルウェアがチェックに用いているDNSやIRCなどの多数のダミーサーバを用意して実インターネットをエミュレートしています。

【相関分析システム】

nicterの最大の特徴は相関分析システムです。マクロ解析システムで観測されたスキャンを特徴ごとにプロファイリングし、ミクロ解析システムでマルウェアから抽出されたスキャンのプロファイルとの照合を行い、類似したプロファイルを持つマルウェアを候補として探し出していきます。このように、マクロ解析とミクロ解析の結果を融合することで、発生中のインシデントとその原因となるマルウェアの特定が可能となり、さらには特定されたマルウェアに応じた対策を導き出すことが可能となります。

より精度の高いインシデント対策へ

マクロ解析システムによるネットワーク観測とミクロ解析システムによるマルウェア解析の結果を突き合わせて、セキュリティインシデントの早期発見、原因究明、対策法の導出を目指すインシデント分析センターnicterについて紹介しました。

今後の研究開発では、より精度の高いインシデント対策の実時間での提供を目指していきます。

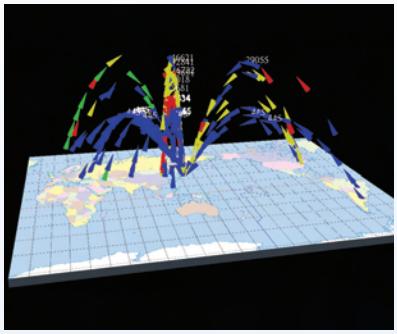


図2●Atlas
観測されたパケットのIPアドレスから国名を判別して、送信元の国の首都からあて先の国の首都にパケットが届く様子を世界地図上にリアルタイムに表示します。

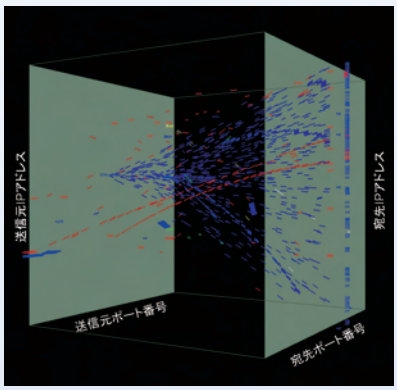


図3●Cube
観測されたパケットを、三次元にアニメーション表現する可視化エンジンです。立方体の平行する2面の片側の面を送信元、反対側の面をあて先として、縦軸はIPアドレス、横軸はポート番号で表現しています。観測されたパケットを送信元からあて先へ通過させることで、スキャンやバックスキャッタなどの様子が可視化され、現象を認識しやすくしています。

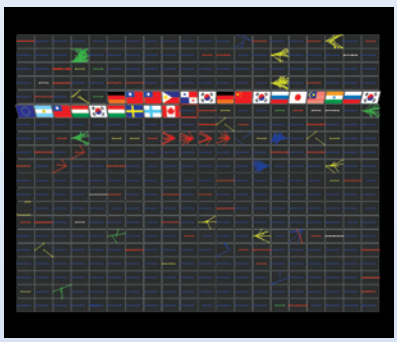
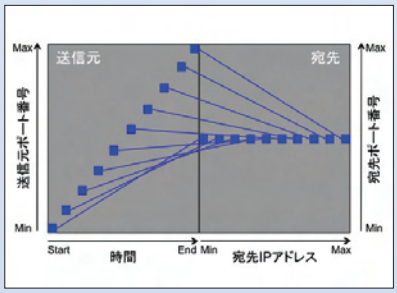


図4●Tiles
観測されたパケットの送信元ホストごとの挙動を分析し、可視化するエンジンです。小さなタイル1つ1つが送信元ホストごとの挙動を表現しています。連続して観測し、最新の分析結果に随時更新していきます。タイルの片面は送信元の国旗を表示して、もう片面には送信元ホストが30秒間に送出したパケットの時刻、送信元／あて先ポート番号、あて先IPアドレスを用いて表現しています。1つのパケットは1本の線で表現しています。また、挙動を分析し、新しい挙動を検出するとアラートをあげてオペレータに通知しています。



暗号技術の安全性を測る

CRYPTRECのミッションとセキュリティ基盤グループの活動

セキュリティを確保するための基盤技術

情報通信ネットワークにおける、電子商取引、電子政府における電子認証、電子マネーの発展に伴い、情報の機密性と完全性（改ざんされないこと）の確保は安心・安全な社会基盤の構築において必要不可欠となっています。こうしたネットワーク環境においてセキュリティを確保するための基盤技術が暗号です。暗号はこれらの環境の至る所で要素技術として利用されており、オンラインショッピング、高速道路におけるETC、住民基本台帳カードを利用した役所での書類の申請、おサイフケータイ®、電子マネーといった我々の身近な場所で無意識のうちに使われています。

暗号の安全性評価

NICTセキュリティ基盤グループは暗号の解析手法の研究を行い、暗号技術の安全な設計手法や利用期限の指針として研究成果を社会へ還元しています。具体的な社会展開例の1つとしては、総務省をはじめとする各府省と連携して、暗号技術評価プロジェクト（CRYPTREC：http://www.cryptrec.go.jp）を運営しています。ここでは特に電子政府推奨暗号リスト（以下「リスト」という。）に登録されている暗号を監視し、安全性の経年劣化に伴い必要な技術的ガイダンスを報告しています。これは内閣府における「政府機関の情報セキュリティ対策のための統一基準（第4版）」にも反映されています。

また、現在様々なところで用いられている暗号の1つである公開鍵暗号RSAの危殆（完全に危ないわけではないが危機的状況）化についても予測を行っています。なお、RSAの安全性については、巨大な合成数の素因数分解（※補足参照）を行うのに必要な計算機資源を見積もることで予想できます。最も多く利用されている合成数である1024ビットの場合、計算機の最高性能が現状の伸び率で今後も向上すると仮定すると、早ければ2020年までに分解可能と予想されます（図1）。つまりRSAは、そう遠くない将来において1024ビットより大きい合成数を使う必要が出てきたのです。また、専用ハードウェアによる方法も注目されており、NICT連携研究部門による委託研究（素因数分解の困難性に基づく暗号の技術的評価に関する研究開発：富士通研究所）で、世界初の専用ハードウェアを開発しました。

このようにアルゴリズムの進歩と技術の進化が相乗効果を成し、暗号の安全性は日々低下していくことに注意しなければなりません。

暗号技術の利用期限と移行問題

暗号には安全に利用できる期限があ

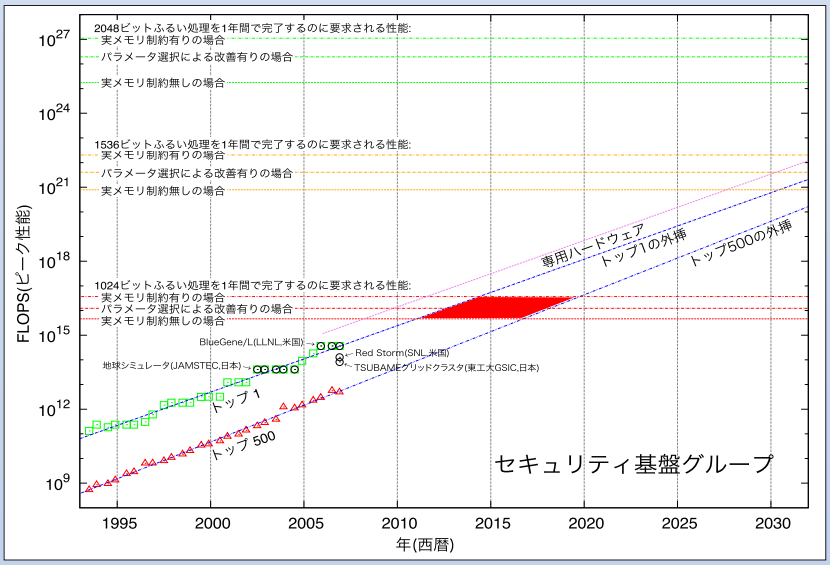


図1●1年間で篩（ふるい）処理を完了するのに要求される処理性能の予測

●Profile●

田中　秀磨
（たなか　ひでま）
情報通信セキュリティ研究センター
セキュリティ基盤グループ
主任研究員

大学院修了後、東京理科大学助手を経て2002年通信総合研究所（現NICT）に入所。現代暗号理論、情報セキュリティ、情報理論、符号理論などの研究に従事。博士（工学）。

り、それにより次の暗号への移行が必要になります。CRYPTRECの評価結果より、現在電子政府で使用されている公開鍵暗号RSA1024とハッシュ関数SHA-1はそれぞれRSA2048とSHA-256へ、2013年までに移行することとなっています（内閣官房情報セキュリティセンター「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針」）。これに伴い移行が必要なシステムは以下となっています。

◎政府認証基盤
◎地方公共団体組織認証基盤
◎公的個人認証サービス
◎商業登記に基づく電子認証制度
◎電子署名及び認証業務に関する法律

暗号の移行は多額の予算が必要な現実問題です。移行する間も業務を行い、移行後は前のデータとの互換性を保つ運用の必要もあります。今後は安全性だけでなく実装性や調達コストも暗号の選択基準となってくるでしょう。

（注：RSA2048とSHA-256は電子政府推奨暗号）

CRYPTRECの取り組みとセキュリティ基盤グループの貢献

現在のリストは2003年に策定されましたが、これを2008年から見直しを行い、2013年改訂を計画しています。2000年に策定を開始した時の要望は「安全な暗号の推奨」でした。約10年経過し、「システムを安全にする暗号の推奨」へと実用視点に変わり、多種多様な暗号選択が可能なことよりも実際に調達できる暗号を明確にすることが求められています。

このような要望にこたえるため、2008年度からリストの構造と運用から見直しています。この一環で2009年度は、前述の要望から実用性を強く要求した新規暗号公募を行います。理論的な安全性評価だけでなく、実装の安全性（耐サイドチャネル攻撃：消費電力や電磁波放射などデバイス動作時に生じる物理現象を利用した攻撃への耐性）が新たに評価項目に加わり、実用面での安全性にも配慮しています。

我が国のセキュリティを確立するために

NICTは公的研究機関であり、セキュリティ基盤グループには中立公平な立場から高度な技術的判断が求められています。したがって、我が国のセキュリティを確立するため、私たちの持つ能力を最大限に生かすことが使命であると考え、また私たちの研究活動が、我が国の技術を支える活動に貢献できるよう努力していきたいと考えています。

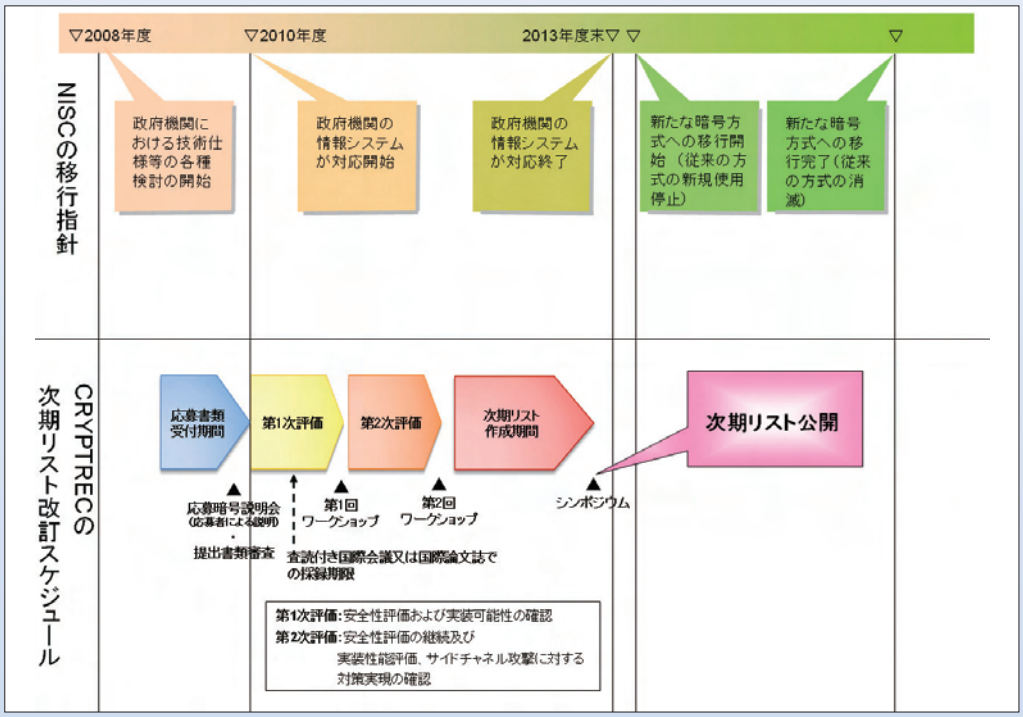


図2●CRYPTRECの電子政府推奨暗号リスト改訂とNISC（内閣官房情報セキュリティセンター）の移行指針スケジュール

※補足：暗号解読と素因数分解

一般に暗号解読は暗号文から鍵などの秘密情報を推定することで平文（暗号化される前の文）を得ることを思い浮かべますが、現代暗号は攻撃者にもっと有利な条件を与えて安全性を評価します。平文とそれに対応する暗号文を用いる条件（既知平文攻撃）や自由に選んだ平文に対応する暗号文を得ることができる条件（選択平文攻撃）などです。非現実的に思われるかもしれませんが、暗号化する鍵を公開する公開鍵暗号では、攻撃者は自由に平文と暗号文ペアを生成できますし、ICカードに記録された鍵を求める場合など攻撃例は多々あるのです。

理論的には鍵の総当たりを行えば必ず鍵を得ることができますが、最高性能の計算機でも実行できないくらい大きなサイズの鍵を設定することで安全性を確保します。そこで総当たりよりも効率的な解読法を開発し、最強の攻撃法の実行に必要な計算機資源（計算量やメモリ）で安全性を評価します。

RSAは暗号文を生成するためにしか使えない鍵を公開し（公開鍵）、復号する鍵はユーザーが秘密に管理しています（秘密鍵）。公開鍵に含まれる、ある合成数の素因数分解ができてしまうと秘密鍵がばれてしまいます。その結果、暗号文を復号されたり、公開鍵暗号を利用した電子署名の偽造をされたりします。したがって、最高性能の計算機でも素因数分解が実行できないくらい大きな合成数が必要になります。RSA1024の合成数は1024ビット（10の300乗程度）という大きい数なのですが、素因数分解アルゴリズムの向上と計算機能力の進化で徐々に安全性が低下しています。

災害時の情報収集に役立つICT

災害時はまず情報収集から

災害が発生すると、何よりもまず情報収集が必要です。本稿では、災害時の情報収集にICTを活用することを目指したNICTの取り組みの一端をご紹介します。

携帯電話端末による情報収集

携帯電話端末は、今日最も普及しているICT機器であり、誰でもどんな場合でも持ち歩いている可能性が高いことから、災害時にも活用が期待されます。ただし災害時には電話が通じにくくなりがちなため、電話機として使うことは困難かもしれません。したがって、災害時にも途切れないネットワーク技術の確立が重要と言えますが、発想を変えて、電話機以外の使い方で情報収集に活用する技術を確立するというアプローチのほうが、より直ちに災害時に役立つと考えられます。

災害時に自治体の職員等が被害状況の現地調査を行う場合、紙地図やカメラなどを携行して歩きますが、作業効率が悪く、また災害対応に追われている中で限られた人数で網羅的に調査を行うことは困難です。そこでNICTでは総務省消防庁消防大学校消防研究センターと連携して、誰もが持ち歩いている携帯電話端末のカメラ機能や測位機能を駆使して、市民が協力して被害状況の調査を行うためのアプリケーション開発を進めています。収集した被害状況は、通信ができない場合でも端末のメモリーに情報を蓄積して対策本部に持ち込む使い方もできるようにし、また測位は基地局を使わずGPSのみで自立的にできる機能を目指しています。20~60歳代の市民に操作してもらう実証実験を昨年から繰り返して実施し、より使いやすいアプリケーションを目指して改良を進めています。

またNICTは、総務省消防庁や科学警察研究所等と連携して、科学技術振興調整費による共同プロジェクト「電子タグを利用した測位と安全・安心の確保」（研究代表機関：東京大学空間情報科学研究センター）に参加し、地下街などGPSによる測位が困難なエリアにおける補完的な位置把握手段として、電子タグ（RFID）を壁などに設置しておき、持ち歩き端末を使ってそのIDを受信することで、自らの位置を把握して防災や防犯に役立てる技術の確立を進めています。その中でNICTは、ブルートゥースとRFIDリーダを搭載した携帯電話端末を使い、壁などに設置されたブルートゥースデバイスから発信されるアドレスを手掛かりにして自らの位置を把握し、同じく壁などに設置されたパッシブ（無電源）型RFIDを「電子貼り紙」として、メッセージを現場に書き置きする手段とする開発を進めています（図1）。これは大規模災害時の現場での安否情報交換や建物の応急危険度判定結果等への応用を想定しています。現時点では、携帯電話端末と一体的に使用できるリーダの制約のため、読み取り専用のRFIDを使用しており、書き込みはネット上のサーバに行うことで仮想的に実現し

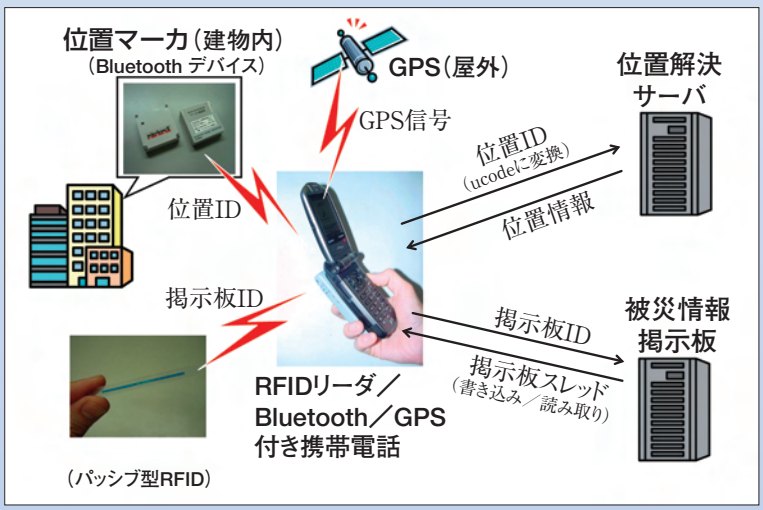


図1●ブルートゥースとRFIDリーダを搭載した携帯電話端末による測位と「電子貼り紙」の概念

●Profile●

滝澤 修
（たきざわ おさむ）
情報通信セキュリティ研究センター
防災・減災基盤技術グループ
グループリーダー

大学院修士課程修了後、1987年に郵政省電波研究所（現NICT）入所。2000年から非常時防災通信及びコンテンツセキュリティの研究開発に従事。2006年より現職。2008年よりセキュリティ基盤グループリーダー兼務。博士（工学）。防災士。

ていますが、我々が可搬型パソコンを用いて既に実現している、書き込み可能なＲＦＩＤに対して直接オフラインで読み書きする機能（本誌２００４年11月号参照）を携帯電話端末でも実現することが、ネットへのアクセスが保証されない災害時の利用には不可欠と考えており、引き続き改良を進めています。

これらの開発成果は、対象機種が限定されるものの、携帯電話キャリアのアプリケーションサーバに登録して希望者によるダウンロードを可能にし、防災防犯ボランティア等を手始めの対象者として、広く提供していく計画です。

昨年11月に千葉県のつくばエクスプレス・東武鉄道流山おおたかの森駅周辺において、プロジェクト参加機関が合同でフィールド実験を実施し、その際に国土地理院がRFID付き基準点（4級相当）を多数設置しました。その１つが記念碑として駅前の歩道に残されていますので、機会があればNICT等の機関名が刻まれた基準点を探してみてください。

レスキューロボットによる情報収集

災害やテロが発生した際に、救助隊員らが危険で入れない建物内を探査する手段として、遠隔操縦ロボットが期待されています。ＮＩＣＴは、独立行政法人新エネルギー・産業技術総合開発機構（ＮＥＤＯ）による「戦略的先端ロボット要素技術開発プロジェクト」に参加し、閉鎖空間内で複数の高速移動体から安定した複数映像、計測データ、行動指令データを伝送するための通信技術の研究開発を担当しています（研究代表機関：国際レスキューシステム研究機構）。遠隔操縦するロボットの通信手段としては無線が適していますが、閉鎖空間内で複数映像を安定して送るためには多くの課題があります。一方、有線では被災現場のような不整地ではケーブルの存在が行動の制約となる問題があります。そこで我々は折衷案として、無線アクセスポイントが数十m間隔で数珠つなぎになっている１本の通信ケーブルを、まず1台のロボット（図2）が中枢神経のように探査空間内に奥深く敷設していき、それを命綱として、各アクセスポイントの周囲で複数のロボットが無線制御で探査活動をする、という有線・無線ハイブリッド通信方式の確立を目指しています。同プロジェクトは、現役の消防隊員と共に仙台市及び神戸市の地下街において繰り返し実証実験を行って、問題点の洗い出しと改良を進めてきました。これまでに７００ｍ（ほぼ1駅分）の距離の地下街で遠隔操縦できるところまで達成しています。昨年末に行われたＮＥＤＯによるステージゲート（絞り込み評価）の結果、ＮＩＣＴが参加している開発チームのみが「通過」と判定され、実用化に向けてあと２年間の継続が認められました。これは、ＮＩＣＴの有線・無線ハイブリッド通信方式を含め、実戦を想定した現実的な開発コンセプトが高く評価された結果と考えています。このプロジェクトでは２０１５年ごろの実戦配備を目指しています。

図2●国際レスキューシステム研究機構等と共同開発中の通信ケーブル敷設ロボット

「使える防災減災技術」の確立を目指す

このように我々の研究開発に一貫している特徴は、通常の通信手段が駄目になっても、限られた機能を駆使して、何とかして災害時に役立つようにするための、「すぐ使える泥臭い技術」の積み重ねを目指していることです。防災減災は、巨費を投じてトップダウン的な最先端システムを１つ開発すれば実現できるというような生易しい対象ではありません。災害時には「ガラス細工のような最先端技術」でなく「生き残っているローテク」が支持されます。ローテクとはいえ、生き残らせる（技術のサバイバビリティを高める）ための泥臭い工夫は、最先端技術の研究開発とは違った難しさがあるため、防災関連機関やメーカーでもなかなか手掛けられないという現実があり、結局は我々のようなＩＣＴ分野の公的研究機関が防災関係者と密接に連携しながら手掛けるしかない状況なのです。防災・減災基盤技術グループは、防災という出口を看板に掲げている（前身の時代も含めて）ＮＩＣＴで唯一の研究グループとして、「使える防災減災技術」の確立を目指す責任があると考えています。

ドップラーライダーで風の動きを観測
都市スケールの大気現象を解析し、生活に役立てたい

電磁波計測研究センター　環境情報センシング・ネットワークグループ
岩井　宏徳

都市部の風を観測し環境問題解決に役立てる

「地面にドップラーライダーを設置し、都市スケールの大気現象、主に風の動きを観測しています」と語るのは、電磁波計測研究センター環境情報センシング・ネットワークグループの岩井研究員です。

ドップラーライダーとは、レーザーを照射して大気中のちり（エアロゾル）などの移動速度を計測し、風の動きを検知する装置です。ドップラーライダーは電波を利用するレーダーと異なり、ビルが密集している都市部の地表面近くでも観測ができます。また、都市部でのスケールの小さな大気現象を詳細に観測できるため、都市部の天気予報の精度向上や大気汚染・ヒートアイランドなどの環境問題解決に役立てられます。レーザーには、人間の目に入っても障害が起きないアイセーフの近赤外線レーザーが利用されています。

地道な観測から様々な成果が

岩井研究員は、観測技術と解析技術の研究を担当しており、これまでにも様々な観測実験と観測結果を解析してきました。山形県では農作物に被害を与える「清川だし」と呼ばれる特徴的な強風の発生メカニズムを突き止めるために観測を行い、発生源周辺の3次元的な風の動きを計測しました。また、本部（小金井）での観測結果から、東京上空に飛来した黄砂の空間分布と流れの可視化にも成功しています。

2台のドップラーライダーを使用した仙台空港での観測では、海から吹く風が水平ロール渦と呼ばれる渦を発生させていることを明らかにしました。

「2台のドップラーライダーで観測することによって、1台では把握できない、風の流れを三次元的に、かつ詳細にとらえることができました」（岩井研究員）。ドップラーライダーは、機器そのものが高価で日本に数台しかない上に、移動が簡単ではないため、複数台を使用した観測は世界でも数例しか行われていません。

「将来はドップラーライダーのネットワークを設置して、ビル風やゲリラ豪雨、大気汚染など、都市部特有の大気現象や気象現象を観測したい」と語る岩井研究員は、大学在学中は宇宙プラズマに関する研究を行っており、NICTにおいても4年間宇宙天気予報に関する研究に従事してきました。「気象学については3年前の異動後から取り組み始めたばかり」とのことですが、「現場に行ってデータを取ることは自分に合っている」と、気象研究の楽しさも語ってくれました。

●Profile●

岩井　宏徳
（いわい　ひろのり）
電磁波計測研究センター
環境情報センシング・
ネットワークグループ　研究員

大学院修了後、2001年通信総合研究所（現NICT）に入所。宇宙天気予報に関する研究に従事し、現在は主にドップラーライダーに関する研究に従事。

情報通信セキュリティ研究センター 推進室　研究マネージャー　奥山 利幸

CRYPTREC シンポジウム 2009
～電子政府推奨暗号リスト改訂に向けて～

総務省をはじめとする各府省と連携して運営を行っている暗号技術評価プロジェクト（CRYPTREC）では、2013年度に予定している電子政府推奨暗号リストの改訂に向け、2009年度より新たな暗号の公募を実施します。本公募について広く周知するため、２月18日（水）虎ノ門パストラルホテルにおいて、NICT及び情報処理推進機構（IPA）の主催、総務省及び経済産業省の共催により、シンポジウムを開催しました。

本シンポジウムでは、電子政府推奨暗号リストの重要性や、暗号リスト改訂の進め方に関する講演のほか、今後の暗号技術研究に関するパネルディスカッションも行われました。関連企業、大学、官庁、公的機関などから約230名の参加者があり、非常に盛況でした。

会場の様子

NICT 情報通信セキュリティシンポジウム
～今後の情報セキュリティを読む～

情報セキュリティ政策会議において定められた２月２日の「情報セキュリティの日」の関連行事として、２月 26 日（木）虎ノ門パストラルホテルにおいて、NICT の主催、情報セキュリティ政策会議、総務省及び関連学会の後援により、シンポジウムを開催しました。

本シンポジウムでは、情報通信セキュリティの専門家による講演及びパネルディスカッションを通して、情報通信セキュリティの最新動向について理解を深めていただくとともに、今後の情報通信セキュリティ技術を展望する機会となることを目的として、第１部では「アイデンティティ管理技術の現状と今後を読む」、第２部では「ネットワークセキュリティ技術の今後を読む」をテーマに、それぞれ３つの講演及びパネルディスカッションが行われました。パネルディスカッションでは参加者からも多数の質問や意見が出るなど、非常に活発な議論が行われ、大変盛況でした。

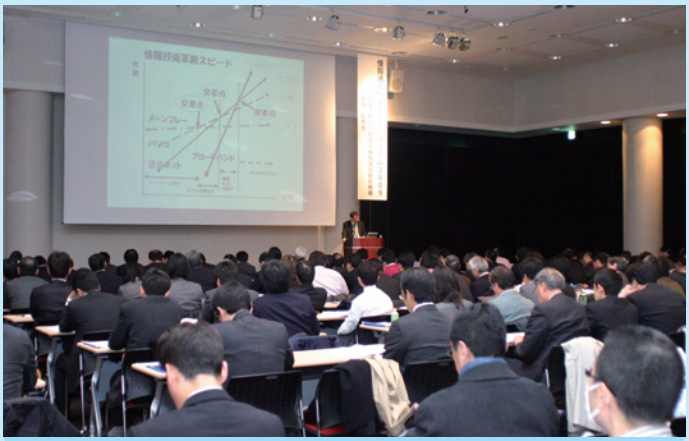
パネルディスカッションの様子

情報通信ベンチャーフォーラム2009開催報告

情報通信振興部門 創業支援グループ　マネージャー　吉野 浩史

独立行政法人情報通信研究機構では、情報通信ベンチャー支援の一環として、情報通信分野におけるベンチャーの起業促進とベンチャー企業経営・ビジネス展開の活性化を目的として、毎年、情報通信ベンチャー関係者の方々を対象としたイベント「情報通信ベンチャーフォーラム」を開催しています。

本年度は、平成21年2月20日にベルサール飯田橋において、「ICTベンチャービジネスの展望～起業から成長へのフェーズを探る」を基調テーマに、情報通信の専門家による基調講演と情報通信ベンチャーの若手経営者4名によるリレー講演を実施しました。



会場（ベルサール飯田橋）の様子

当日は、約200名の参加者があり、講演プログラム終了後に開催した情報交流会では、講演者と参加者の方々による活発な意見交換と交流が行われました。

	講　師	演　題
基調講演	**中島　洋 氏** 株式会社MM総研所長、 国際大学グローバル・コミュニケーション・センター主幹研究員／教授	情報通信の新潮流と未来市場
リレー講演	**伊藤 健吾 氏** 株式会社メタキャスト代表取締役社長&CEO	体験共有がソーシャルメディアを変える： Social Lifestreaming Service ～2009年はセマンティックがキーワード!?
	上村　崇 氏 株式会社ALBERT代表取締役社長	独自のレコメンド技術で世界を目指すICTベンチャー
	田中 泰生 氏 芸者東京エンターテインメント株式会社代表取締役CEO	20年で任天堂とアップルとディズニーを抜こうと思ってるハイテクエンタメ会社社長大いに語る
	妹尾 賢俊 氏 maneo株式会社代表取締役	ソーシャルレンディング： Web2.0金融～世界の状況と日本～

※参考URL http://www.venture.nict.go.jp/ezp/index.php/venture/nict_2/node_20835/2009/node_25315

読者の皆さまへ

次号は、計測技術で生存環境の安心・安全を目指す、電磁波計測研究センターを特集します。

NICT NEWS 2009年4月 No.379

編集発行
独立行政法人情報通信研究機構 総合企画部 広報室
NICT NEWS 掲載URL http://www.nict.go.jp/news/nict-news.html

編集協力　財団法人日本宇宙フォーラム

〒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/