



01

## 暗号の安全性評価

盛合 志帆



03

## 格子暗号の実用化に向けて

— 解読実験の世界記録とその意義 —

青野 良範

06

## 暗号の安全性評価と CRYPTREC暗号リスト改定

ネットワークセキュリティ研究所 セキュリティ基盤研究室

07 宇宙天気ユーズーズフォーラム 開催報告

08 NICT Entrepreneurs' challenge 2 days  
「起業家甲子園」及び  
「情報通信ベンチャービジネスプラン発表会」の開催報告

09 受賞者紹介

11 情報バリアフリーのための  
ICT分野のサービス提供を支援します。  
チャレンジド向け通信・放送役務提供・開発推進助成金  
平成25年度公募

# 暗号の安全性評価



**盛合 志帆** (もりあい しほ)  
ネットワークセキュリティ研究所 セキュリティ基盤研究室長

1993年大学卒業。日本電信電話(株)、ソニー(株)を経て2012年、NICTに入所。  
暗号技術の設計および安全性評価に関する研究や国際標準化に従事。博士(工学)。

## 暗号の安全性評価の重要性

ネットワークの発展にともない、暗号技術は現代社会の根幹を支える技術となっています。暗号技術は、インターネットや携帯電話における通信の秘密保持のみならず、鉄道の自動改札システム、高速道路の自動料金収受システム、電子書籍などのコンテンツ配信、ブルーレイディスクの著作権保護、ICチップによるパスポート偽造防止などに用いられており、もはや暗号技術なしでは通信・交通・ビジネスの安全・安心な運用は考えられないと言っても過言ではないでしょう。

しかしながら、現在、社会で広く使われている暗号技術は、一度安全性が確認されれば永遠に安全であるというわけではなく、暗号解読技術の進歩により急激な安全性の低下が起ることもあります。このため、NICTネットワークセキュリティ研究所 セキュリティ基盤研究室では、日々進歩する暗号解読技術や計算機性能の向上を考慮に入れ、継続的に暗号技術の安全性評価の研究を行っています。

## 暗号の安全性指標

「暗号の安全性を評価する」とはいったいどのようにすればよいのでしょうか。暗号の安全性は、その暗号を最も効率のよいアルゴリズムで解読したときに必要な計算量を指標として定義されています。ある暗号の解読計算量が $2^k$ のオーダーであった場合、その暗号の安全性は $k$ ビットセキュリティであるといいます。例えば、暗号Aが $2^{112}$ 回の復号演算処理で鍵が見つかる場合、暗号Aの安全性は112ビットセキュリティとなります(図1)。暗号の安全性を評価するには、最も効率のよい解読アルゴリズムを見つけ、その方法で解読にどれくらいの手間が必要かを見積もればよいということになります。

米国標準技術研究所(National Institute of Standards and Technology: NIST)では暗号解読技術の進歩や計算機性能の向上を考慮に入れ、米国の政府調達において、何年にどれくらいのセキュリティレベルをもつ暗号技術を利用すべきかの指針を出しています。図2に2007年にNISTが発表した推奨鍵長・パラメータを示します。これによると、2011年以降は最低112ビットセキュリティの安全性指標をもつ暗号技術を利用すべきであり、このレベルと等価な共通鍵暗号は鍵長112ビット、RSAなど素因数分解問題に基づく公開鍵暗

日々進歩する解読技術や計算機能力を踏まえ  
暗号技術の安全性を評価することは重要な課題

**暗号の安全性指標**

その暗号を最も効率のよいアルゴリズムで  
解読したときに必要な解読計算量

解読計算量が  $2^k$  ⇒ その暗号の安全性は  $k$  ビット

例:  $2^{112}$  回の復号演算処理で鍵が見つかる場合  
その暗号の安全性は **112 ビットセキュリティ**

図1 暗号の安全性評価

		安全性指標に相当する鍵長・パラメータ (bit)				
		~2010年	2011~ 2030年	2031年~	2031年~	2031年~
<b>暗号の安全性指標</b>		<b>80 bit</b> セキュリティ	<b>112 bit</b> セキュリティ	<b>128 bit</b> セキュリティ	<b>192 bit</b> セキュリティ	<b>256 bit</b> セキュリティ
共通鍵暗号 (AESなど)		80	112	128	192	256
公開鍵暗号 デジタル署名	素因数分解問題に基づく方式 (RSAなど)	1024	2048	3072	7680	15360
	離散対数問題に基づく方式 (DSA, DHなど)	1024	2048	3072	7680	15360
	楕円曲線上の離散対数問題に基づく方式 (ECDSA, ECDHなど)	160	224	256	384	512
ハッシュ関数 (SHA-2など)		160	224	256	384	512

Recommendation for Key Management - Part 1: General (Revised), NIST SP 800-57, 2007.

図2 暗号の安全性指標

号は鍵長2048ビット、DSAなど離散対数問題に基づく公開鍵暗号は鍵長2048ビット、ECDSAなど楕円曲線上の離散対数問題に基づく公開鍵暗号は鍵長224ビット、ハッシュ関数はハッシュ長224ビットであることが示されています。なお、この指標は漸近的な計算量評価に基づきNISTが2007年に示したものであり、日々進歩する技術や実際の計算機実験による評価結果に基づいて変わっていきます。また、NIST以外のいくつかの国の研究機関等も指針を出しており、NISTとは異なる推奨鍵長・パラメータを示しているところもあります。

## セキュリティ基盤研究室でのこれまでの成果

セキュリティ基盤研究室でこれまで行ってきた暗号の安全性評価の1つに、現在最も広く使われている公開鍵暗号であるRSA暗号や楕円曲線暗号の評価があります。特に、1024ビットRSA暗号の解読は従来考えられていたよりも容易で、現在では、スーパーコンピュータを使うと1年程度で解けてしまうという評価を得ています(図3)。この評価結果は、我が国の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あるCRYPTREC (Cryptography Research and Evaluation Committees) を通じて公開され、誰もが参照できるようになっ

ています。当研究室では、電子政府推奨暗号リストの改訂のための暗号の安全性評価やCRYPTRECの事務局運営の面で貢献を行っています。詳細は本号p6で紹介します。

また、現在使われている暗号技術にとどまらず、クラウドコンピューティングにおいて、他に内容を一切知らせることなく計算作業などを託することができるよう、データを暗号化したまま種々のデータ処理を行うことが可能な次世代暗号の安全性評価も行っています。次世代暗号においてどのようなパラメータを選択すれば安全に利用できるかがわかるので、次世代暗号の実用化や標準化に役立ちます。次世代暗号の安全性評価に関して、当研究室では、これまでに、高度なプライバシー保護機能を実現する「ペアリング暗号」の解読で世界記録を達成しました(NICT NEWS 2012年9月号に掲載)。また、格子暗号の安全性評価でも世界記録を達成しております。詳細は本号p3-5で紹介します。

NICTが行っている暗号の安全性の評価結果は、我が国の電子政府システムをはじめ、世界中で広く利用されている暗号技術を安全に利用する際の適切な鍵長やパラメータを選択するための技術的根拠を与えており、極めて重要な貢献となっています。

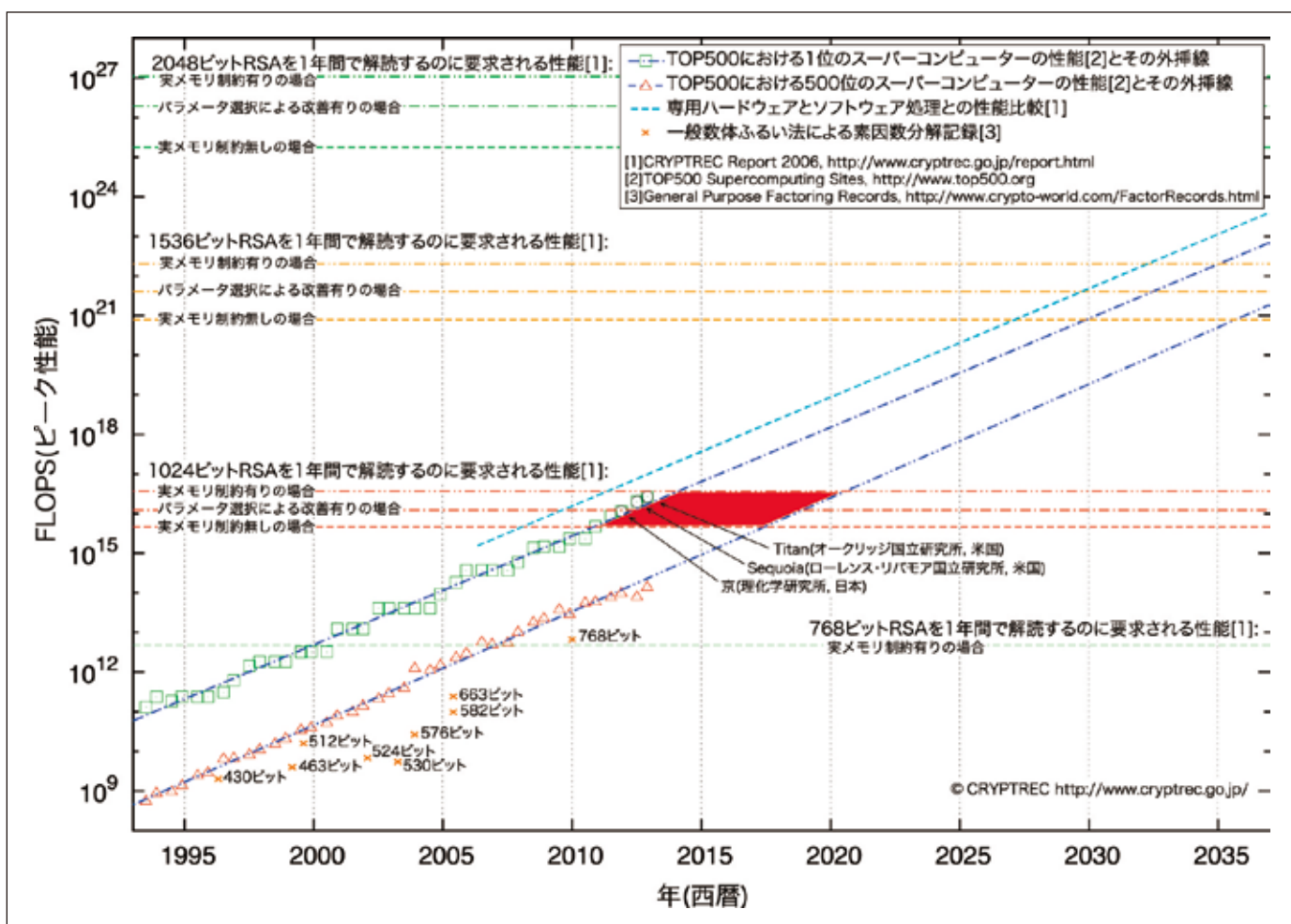


図3 RSA暗号の安全性評価

縦軸は計算機能力を表し、グラフの水平破線は下から順に768ビット、1024ビット、1536ビット、2048ビットのRSAを1年間で解読するのに要求される性能を示している。但し、この性能は実メモリ制約の有無により幅があり、例えば同じ1024ビットRSAについて複数の破線で表されている。一方、グラフの左下から右上にのびる線は年とともに推移する計算機性能の向上を示しており、スーパーコンピュータの演算処理速度のランキング上位500位を公表する「TOP500」における1位(□)および500位(△)のスーパーコンピュータの性能とその外挿線となっている。こちらも1位と500位で性能に幅がある。この水平線と斜め線が変わるところが赤く塗られているが、これが1024ビットRSAがスーパーコンピュータを用いて1年で解読される時期を表している。2013年現在、1024ビットRSAがスーパーコンピュータを用いて1年で解読される時期に入ってきたことがわかる。

# 格子暗号の実用化に向けて

## — 解読実験の世界記録とその意義 —



青野 良範 (あおの よしのり)  
ネットワークセキュリティ研究所 セキュリティ基盤研究室 研究員

大学院修了後、2011年、NICTに入所。公開鍵暗号の安全性評価に関する研究に従事。博士(理学)。

### はじめに

現代社会を支える公開鍵暗号技術として、主にRSA暗号と楕円曲線暗号が使われています。しかし、これら2種類の暗号は量子コンピュータを使うと簡単に解読されてしまうことが20年程前に数学的に証明されています。そのため、量子コンピュータを用いても(そしてもちろん普通のコンピュータでも)簡単に解読することのできない暗号方式を開発し、社会で運用していくための研究が進められています。このような、量子コンピュータでも通常のコンピュータでも解くことが難しい暗号は耐量子計算機暗号と呼ばれ、その候補としてさまざまなものが提案されています。

耐量子計算機暗号として新たに提案された暗号方式には、解読が難しいだけでなく、RSA暗号や楕円曲線暗号にはない様々な特徴、例えばクラウド・コンピューティングにおいて計算内容の機密保持に使える、大きな組織内での情報管理に向いている等の特徴を持っています。これらの暗号は、それぞれの特徴を活かして耐量子計算機暗号のデファクトスタンダードを狙っているため、さながら戦国時代のようになっています(図1)。

### 解読実験 — 暗号実用化のための基準作り —

提案された暗号方式の中で一番良いものはどれか、ということ誰かが納得する形で比較するため、統一された基準を作る必要があります。例えば、同じ暗号方式であれば、鍵長が長い(パラメータが大きい)方がより安全であることが直感的にわかりますが、異なる暗号方式の場合には鍵長による単純比較は行えません。

しかし例えば、「世界一高速な解読プログラムを用いて、スーパーコンピュータ京でも解読に1年以上かかる」という安全性を同レベルに設定した上で、実際に利用する場合の暗号化速度の比較を行えば、異なる暗号方式同士でも優劣をつけることができます。実際には、解読プログラムもスーパーコンピュータも日々進化し続けているため、解読実験の結果から、スーパーコンピュータでの解読に1年以上かかるための数年後のパラメータはどれくらいで、このデータ量の下限は何バイトになっているという予測を行うことで、各暗号方式の安全性の比較評価を行うことができます(図2、3)。

耐量子計算機暗号の候補となっているいくつかの暗号方式に対して、このような評価を行うことにより、実用化の場

ごとに最適な方式を選ぶための基準作りを行うことができます。このたびセキュリティ基盤研究室では、候補のひとつである格子暗号の解読に現れる「最短ベクトル問題」の難しさの評価を行いましたので、以下に報告をします。

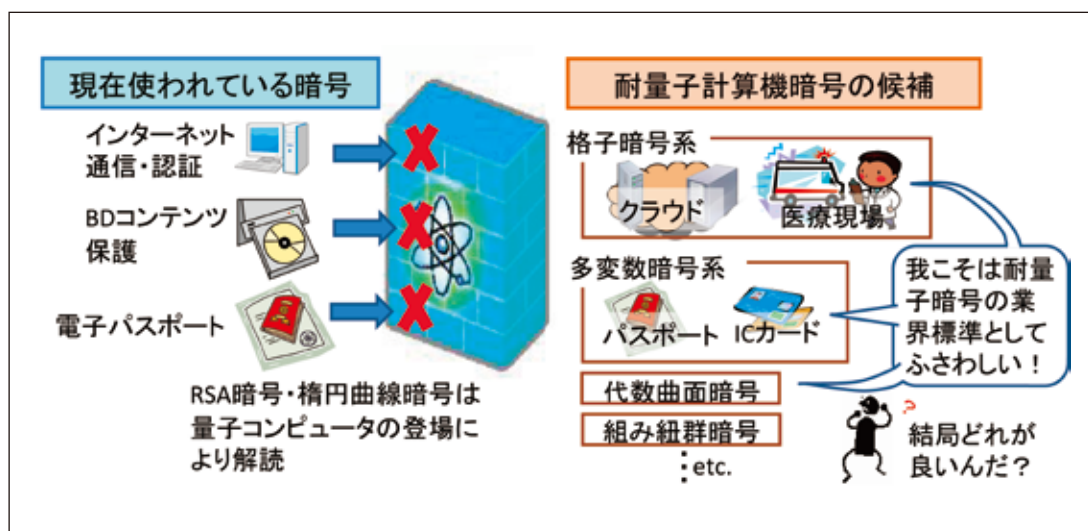


図1 耐量子計算機暗号の業界標準に向けて

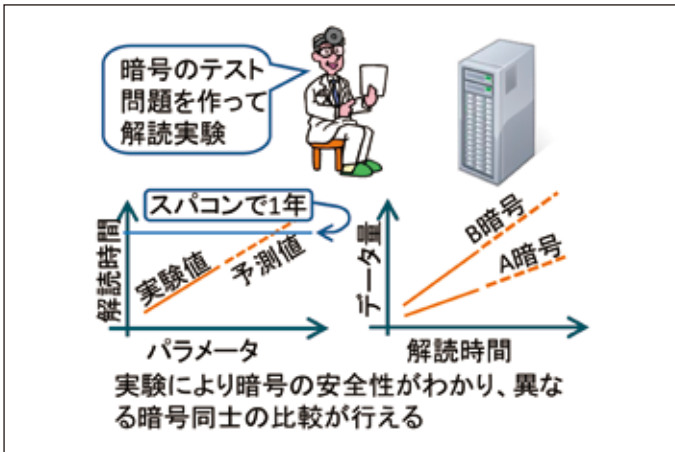


図2 解読実験による暗号の比較

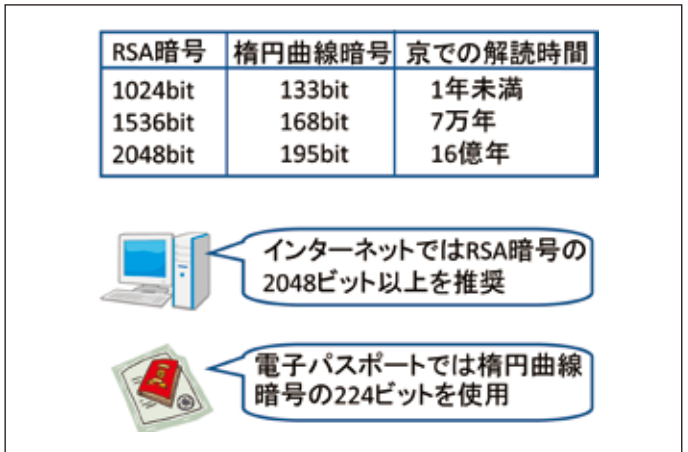


図3 解読実験による暗号の比較と実社会での応用

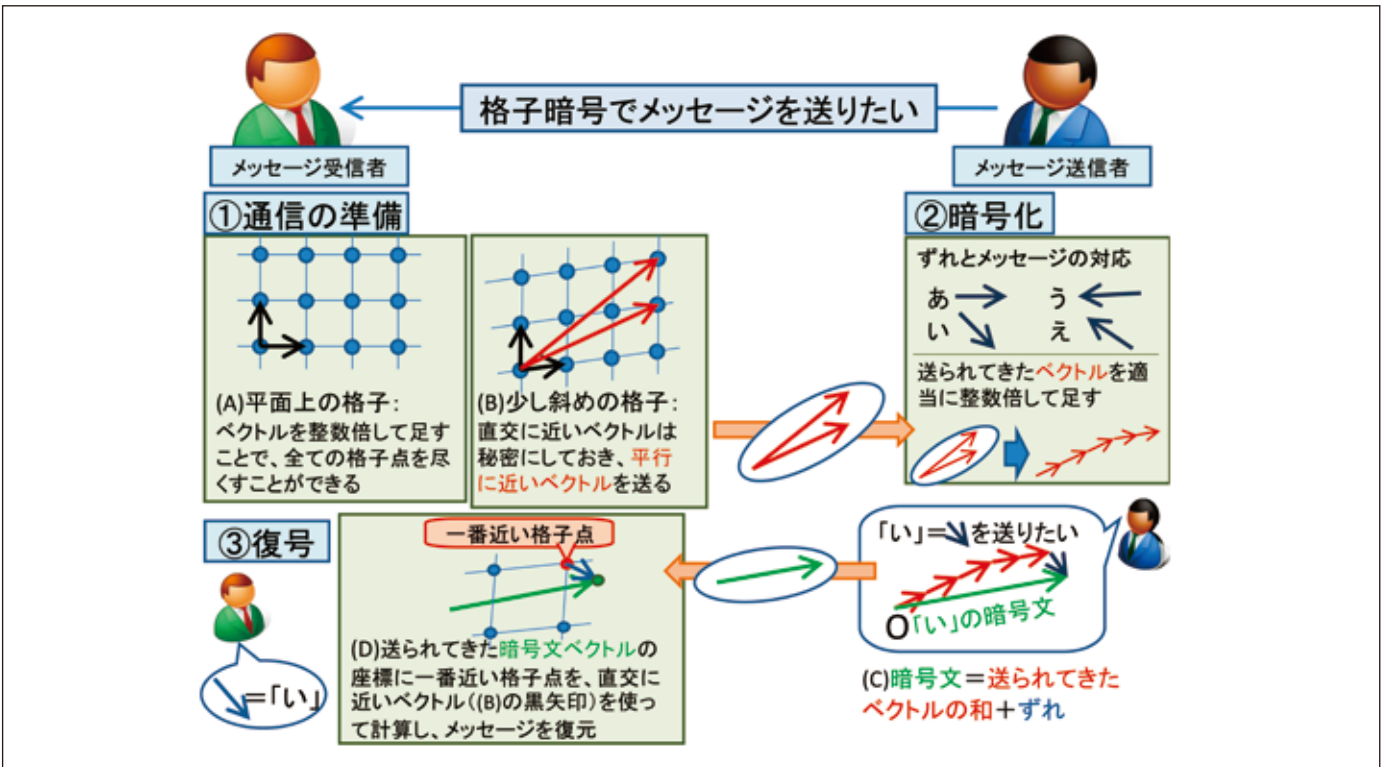


図4 格子暗号のイメージ

## 格子暗号

格子暗号の概念図を図4に示します。格子とは、図の(A)、(B)のように空間内に規則的に並んだ点の集合(図は2次元空間の例)であり、コンピュータの内部ではベクトルの集合(図中の黒矢印の組)として表現されます。このベクトルを適当に整数倍して足すことで、すべての格子点を網羅することができます。

格子暗号を用いた通信は、メッセージの送信者が受信者に対して通信処理の要求を出した後、①準備、②暗号文の生成・送信、③メッセージの復元の3ステップで行われます。

① 要求を受けた受信者はまず、図4(B)のような直交に近いベクトルの集合(黒)と、対応する少し斜めになっている格子(青)を生成します。このベクトルの集合(黒)を使うと暗号文を復号できるため、これは秘密情報としておきます。次に、斜めになっている格子の情報をメッセージ送信者に

送る必要がありますが、秘密情報のベクトルをそのまま送ってしまうと途中の盗聴者も暗号文を復元できてしまうため、暗号の意味がありません。そこで、同じ格子点を網羅するようなベクトルの集合で、暗号文の復元には使えないように変形したものを送ります。図4(B)の赤い2本のベクトルがそれで、ベクトル同士が互いに平行に近いときには、暗号文の復元には使えないことが知られています。

② メッセージ送信者はベクトルの集合を受け取ったのち、それらを適当に整数倍して足して座標を計算します。この座標は、受信者が生成した格子点のひとつになっています。この座標をさらに、送りたいメッセージの分だけずらして、受信者に送ります(図4(C))。このとき、ずれとメッセージの対応はあらかじめ決められているものとします。

③ 座標のデータを受け取った受信者は、送られてきた座標情報の一番近くにある格子点を計算で求め、ずれを計算し、そこからメッセージを復元します(図4(D))。

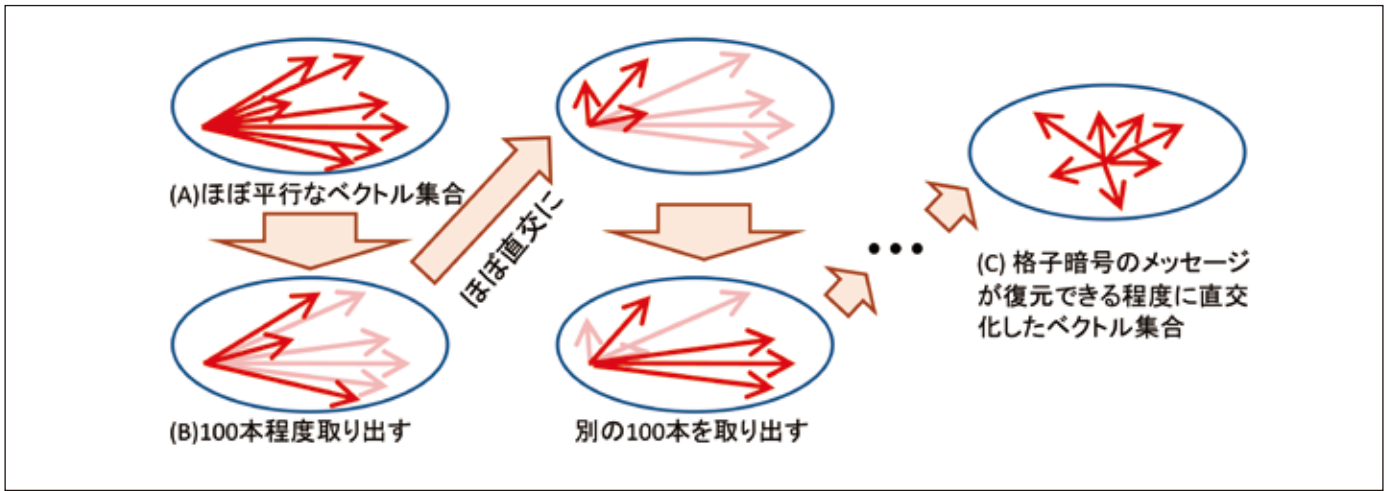


図5 ほぼ平行なベクトル集合を少しずつ直交化していくアルゴリズム

## 格子暗号の安全性

送信者が送った点の座標から、メッセージに対応するずれを計算するためには、座標に一番近い格子点を求める必要があります。この計算は、格子を表現するベクトル集合が図4 (B) の黒いベクトル集合のように互いにほぼ直交しているときには、高速に行えることが知られています。逆に、赤いベクトル集合のようにほぼ平行であるときには、計算は非常に時間がかかると予想されているため、盗聴者がほぼ平行なベクトル集合と暗号文の座標を手に入れても、その情報だけから暗号を解読することは難しく、格子暗号は安全であると考えられています。

反対に、もしも盗聴者がほぼ平行なベクトル集合からほぼ直交なベクトル集合を復元することができれば、どのような暗号文も解読できてしまうため、この復元が行えない程度のパラメータを取る必要があります。現在、ベクトルの本数が800本(800次元)程度であれば復元可能であることが実験により確認されており、今後もこの本数は上がり続けていくと考えられます。

## 最先端アルゴリズムによる解読実験

我々は暗号の解読実験を行うため、ベクトル集合の復元を行う最新のアルゴリズムを改良しました。ほぼ平行なベクトル集合からもとの集合を復元する計算は、一気に全てのベクトルを扱おうとすると非常に大変なものとなります。そのため最新のアルゴリズムでは、図5のようにベクトル集合の中から100本程度取り出してそれらをほぼ直交なベクトル集合に直し、もとの集合に戻してまた別の100本を処理する、という操作を繰り返すことで全体を少しずつ直交に近づける計算を行っています。

一般に、ベクトル集合が平行に近いときには、ベクトルは長く(図5 (A))、直交に近いときには短い(図5 (C))という特徴があります。そのため、与えられたベクトル集合を変形してなるべく短いベクトルを求める問題が暗号の安全性評価

に深く関わっています。この問題は最短ベクトル問題と呼ばれ、格子暗号解読コンテストである格子最短ベクトル問題チャレンジ(TU Darmstadt lattice challenge)\*では世界中の研究者がこの問題を解くためにしのぎを削っています。既存の研究では、取り出すベクトルの本数が固定値であったため計算中に無駄な箇所があったのですが、我々は取り出す本数の最適値を自動的に計算する手法を確立し、アルゴリズムを改良しました。コンテストにおいて825次元の問題を解き、新たな世界記録を樹立することができました。

## 将来の展望

現在、格子暗号の安全性評価に使われているアルゴリズムはメモリの使用が極端に少ないものが主流です。一方、アルゴリズム理論では「時間-空間計算量トレードオフ」と呼ばれるメモリ使用量を増やして計算を高速化する手法(図6)があるため、それを用いて高速化したアルゴリズムでの再評価を行いたいと考えています。また、ベクトルの集合を直交化させるアルゴリズムは、格子暗号以外の評価にも応用できることが知られているため、それらの解読実験も行いたいと考えています。

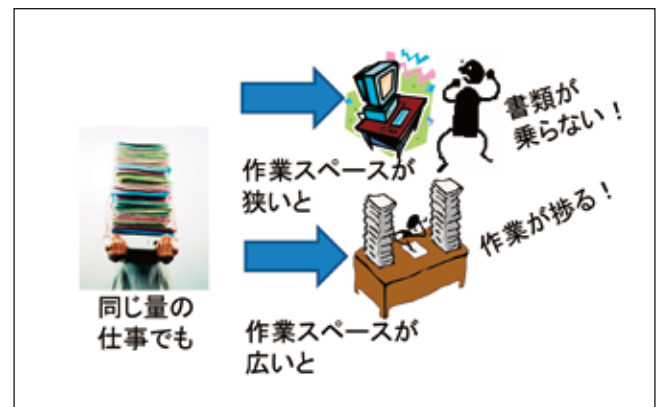


図6 時間-空間計算量のトレードオフ

\* 格子最短ベクトル問題チャレンジ(TU Darmstadt Lattice Challenge)  
ドイツのダルムシュタット工科大学が2008年より主催している、格子の最短ベクトル問題のコンテスト。この問題の難しさを検証するため、500次元から2000次元までのチャレンジ問題が25次元刻みで出題されており、この分野の著名な研究者がより大きな次元、より短いベクトルの探索を目指してしのぎを削っている。

# 暗号の安全性評価と CRYPTREC暗号リスト改定

ネットワークセキュリティ研究所 セキュリティ基盤研究室

## CRYPTRECへの貢献

CRYPTRECとはCryptography Research and Evaluation Committeesの略であり、我が国の電子政府における調達のために参照すべき暗号のリスト（電子政府推奨暗号リスト）に掲載されている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は、総務省及び経済産業省が共同で運営する暗号技術検討会と、NICT及び情報処理推進機構（IPA）が共同で運営する3つの下部委員会で構成されています。その中でセキュリティ基盤研究室はこれまで電子政府推奨暗号リストに掲載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助言を行うという役割を担ってきました。2003年に発表された電子政府推奨暗号リストが、近年の技術動向等を踏まえて改定され、2013年3月に総務省及び経済産業省からCRYPTREC暗号リストとして発表されました。セキュリティ基盤研究室は、この改定作業に暗号安全性評価及び事務局運営の面で貢献しました。

## CRYPTREC暗号リスト改定

電子政府推奨暗号リストは、2003年に10年間安心して利用できるという観点で選定されましたが、(1) 10年が経過したこと、(2) 暗号解析技術・計算機の発展により安全性の低下が進んだこと、(3) 暗号が利用されるシーンが広がったことから、2013年に新たに「電子政府推奨暗号リスト」を改定した「CRYPTREC暗号リスト」が作成されました\*。CRYPTREC暗号リストは安全性だけでなく、調達容易性、国産暗号の普及促進といった様々な視点で検討され、「電子政府推奨暗号リスト」、「推奨候補暗号リスト」、「運用監視暗号リスト」から構成されています。電子政府推奨暗号リスト及び推奨候補暗号リストには安全性及び実装性能が確認された暗号技術が掲載されています。特に、電子政府推奨暗号リストには、CRYPTRECにて調達が容易である等と判断されたものが掲載されています（図1）。また、運用監視暗号リストにはハッシュ関数SHA-1など実際に解読されるリスクが高まるなど推奨すべき状態ではなくなった暗号技術が掲載されています。

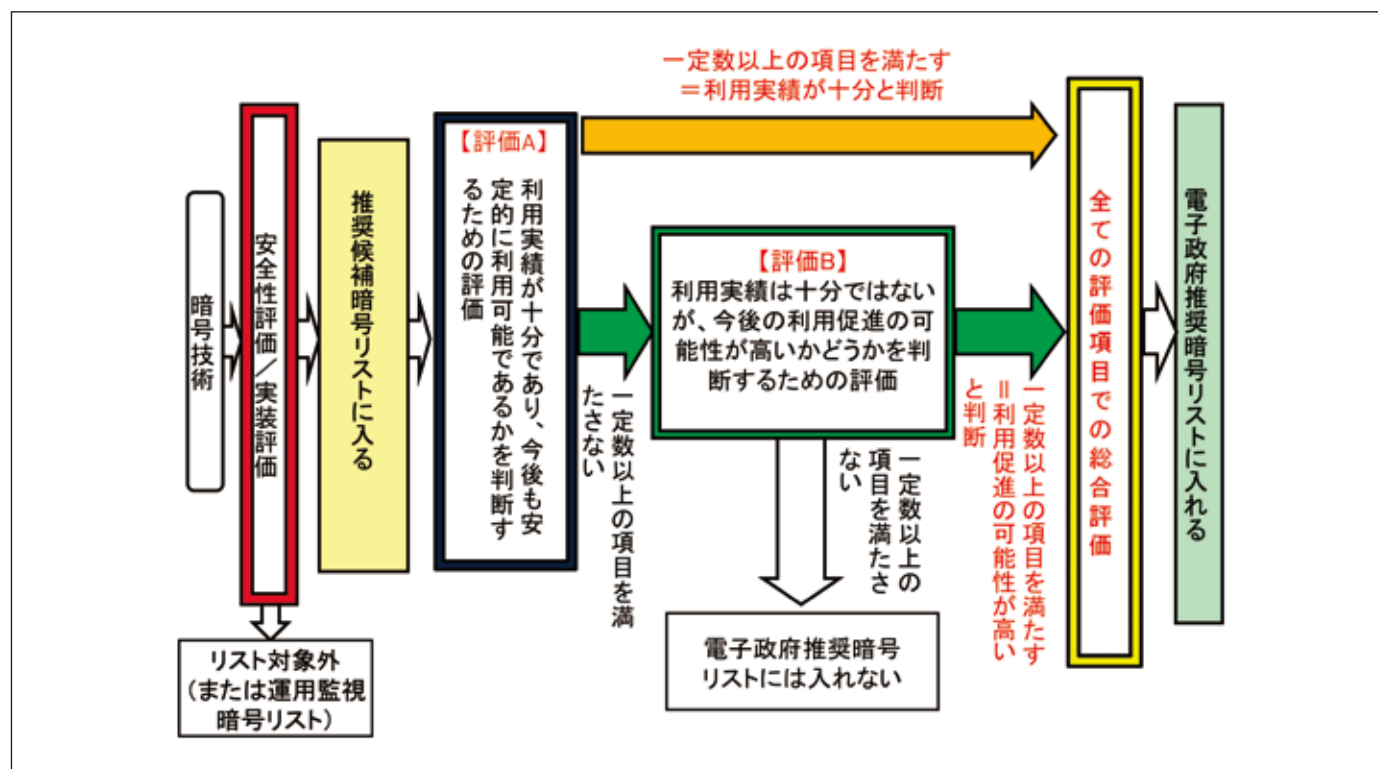


図1 リストの改訂プロセス

\* 電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）  
[http://www.soumu.go.jp/main\\_content/000206523.pdf](http://www.soumu.go.jp/main_content/000206523.pdf)

# 宇宙天気ユーザーズフォーラム 開催報告

電磁波計測研究所 宇宙環境インフォマティクス研究室 石井 守

2013年2月26日にNICT本部研究本館4階国際会議室において、宇宙天気ユーザーズフォーラムを開催しました。参加者は官公庁、大学および研究機関、航空関係者および衛星運用関係者を中心に90名を超え、ほぼ満席となる盛況でした。

熊谷博NICT理事の挨拶で幕を開けたフォーラムは2部構成となっており、第1部では、現在の宇宙天気の概況の説明およびNICTの行う宇宙天気の取り組みについて、石井守NICT宇宙環境インフォマティクス研究室長が講演を行いました。第2部では、宇宙天気関連の近年のトピックスについて、人工衛星に対する宇宙天気の影響として九州工業大学の趙孟佑教授、近年導入が進められている測位衛星を用いた航空航法に対する宇宙天気の影響について電子航法研究所の斎藤享氏、また太陽活動が活発な時に流れる巨大地電流の影響が変電所などに与える影響について気象庁地磁気観測所の源泰拓氏にご講演いただきました。

講演後の総合討論では参加者から活発な質問・コメントをいただきました。特に航空関係では、近年GPSをはじめとする衛星測位情報の航空航法への利用が進んでいますが、電離圏の変動がその誤差の大きな原因となっていることから、宇宙天気情報の重要性がICAO（国際民間航空機関）においても検討されており、本フォーラムにおいても活発な質疑が交わされました。また、これまでわが国ではあまり影響がないとされていた地電流の電力施設への影響についても、今後の研究の進展によっては再検討が必要であるとの結果に多くの聴衆が強い関心を示していました。

フォーラム終了後には、NICTで宇宙天気予報会議を行っている予報室等の見学会を開催し、30名以上の方が参加されました。参加者の多くが日頃から宇宙天気予報情報を電子メールなどで受け取っていることから、「実際に予報を行っている現場を見ることができて良かった」という声を多くいただきました。また、参加者のアンケートでは、それぞれの講演について「分かりやすかった」、「十分理解できた」という回答とともに具体的な感想やコメントをいただくことができ、NICTの宇宙天気予報に対する関心の高さと期待を知るものとなりました。また、NICTの提供している宇宙天気情報についても、実利用の例をご教示いただくとともに、多くのご要望をいただきましたので、今後の改善に生かしていきたいと思っております。



講演の様様



宇宙天気予報室見学の様様



# NICT Entrepreneurs' challenge 2 days 「起業家甲子園」及び 「情報通信ベンチャービジネスプラン発表会」の開催報告

NICTでは、ICTを活用した事業を志す全国の高等専門学校生、大学生、大学院生などの次世代の人材の発掘・育成、及びICT分野の地域発ベンチャー企業の事業拡大等のサポートを実施しています。

その一環として、学生や若手がビジネスプランを競い合う「起業家甲子園」及び全国の有望ベンチャー企業がビジネスプランを競い、資金調達・販路拡大などのビジネスマッチングを促進する「情報通信ベンチャービジネスプラン発表会」を開催しました。

## 「第2回起業家甲子園」

2013年3月7日(木)

全国から選抜された9チームによるプレゼンテーションが行われ、最優秀賞、審査委員特別賞、さらに、13の協賛企業が提供するインターンシップ参加権などの「特別賞」が授与されました。交流会では、協賛企業・関係者など100名程度が参加し、活発な交流が行われました。

### 最優秀賞

電気通信大学大学院「チーム☆ひとりのできるもん(代表 堀内公平氏)」  
『技術者の独学文化を変えるコードリーディングプラットフォーム“CodeLibrary”』

オープンソース(OSS)のコードを読んで、すきま時間に自身の技術力を向上させられる、ソーシャルコードリーディングプラットフォーム。基本的にアプリを無料で提供し、プラットフォーム上でのユーザ間のコードにまつわるノウハウの売買の-marginが売り上げとなる。



会場の様子

### 審査委員特別賞

沖縄工業高等専門学校「ShinBunet(代表 兼城駿一郎氏)」  
『ShinBunet』

インターネットを使えないという方の情報格差(デジタルデバインド)を解決するため、気になった新聞記事に手をかざすだけで自動的にインターネット上から関連情報が収集され、iPadに表示されるシステム。iPadに表示する際、紙媒体の新聞のような形で広告を埋め込むことによる収益化を目指す。また、「どの記事に関して新聞購読者は関連情報を欲しているのか」というデータも収集することができるため、このデータを利用した別のビジネスに繋げることも可能である。



受賞後の記念撮影

## 「平成24年度(第15回)情報通信ベンチャービジネスプラン発表会」

2013年3月8日(金)

前日開催した起業家甲子園の最優秀チームによるプレゼンテーション、NICT社会還元促進部門によるNICTの知財・技術移転の取り組みの紹介の後、ベンチャー企業8社によるプレゼンテーションが行われ、大賞及び今年から新設した聴講者の投票によるオーディエンス賞が授与されました。当日は200名程度が参加し、プログラム終了後の情報交流会では、活発な意見交換や商談が行われました。

### 大賞

株式会社GClue(代表取締役 佐々木陽氏)  
『iOS連携ハードプラットフォーム』

オープンソースハードウェアとして開発したiOS連携ハードウェアを軸にしたプラットフォームを構築し、開発されたiOS連携の作品集をオープンソース及びオープンソースハードウェアとして公開したり、そのキット販売やキット作成講座などを展開する。最初のターゲットは、iOS連携玩具とし、Open Source Omocha(oSo)としてiPhoneと連携可能なDIY玩具市場の開拓を目標とする。



発表の様様



会場の様子

### オーディエンス賞

株式会社リーボ(代表取締役CEO 松尾龍馬氏)  
『超小型電気自動車向けカーシェアシステム“こてかけ”の提供』

新しいモビリティとして注目されている超小型電気自動車(1~2人乗り)向けに、独自開発したカーシェアリングシステム。このシステムの特徴は、(1)スマートフォンアプリ内で会員登録、免許証認証、車両予約、料金支払い等、必要な手続きを全て完結することができる。(2)ステーション間でのワンウェイ利用に対応している。(3)導入先に合わせ、スマートフォンアプリ、車載ディスプレイに観光ルート案内やご当地音声ガイドなどの機能を付加してカスタマイズ提供することができる。の3点。



表彰後の記念撮影

# Awards

◆受賞者紹介◆

## 受賞者 ● 松尾 真一郎 (まつお しんいちろう)

ネットワークセキュリティ研究所 セキュリティアーキテクチャ研究室 室長

共同受賞者: 宮崎 邦彦 (株式会社日立製作所)  
大塚 玲 (独立行政法人産業技術総合研究所)

◎受賞日: 2012/3/19

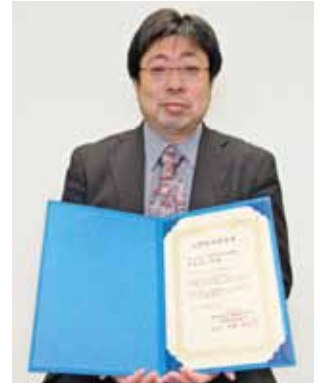
◎受賞名: 国際規格開発賞

◎受賞内容: ISO/IEC JTC1において、ISO/IEC 29128 (First Edition) Verification of Cryptographic Protocols のコエディタとして編集を行い、ISOの発行を完了させたため

◎団体名: 一般社団法人情報処理学会

◎受賞のコメント:

このたび、セキュリティ技術の安全性検証方法をISO/IEC JTC1において標準化を完了させることができました。私たちがネットワークを利用する時、様々なセキュリティ技術を使いますが、その技術が本当に自分たちを守ってくれるかどうかを検証する必要があります。この標準はその検証の物差しとなります。この標準化をサポートしてくださった皆様に感謝するとともに、今後のNICTの研究成果の普及に役立てていきたいと思っております。



## 受賞者 ● Ganesh Gowrishankar (ガネッシュ ゴウリシャンカー) 未来ICT研究所 脳情報通信研究室 専門研究員

共同受賞者: Chenguang Yang, Sami Haddadin, Sven Parusel, Alin Albu-Schäeffer and Etienne Burdet

◎受賞日: 2012/5/17

◎受賞名: 2011 King-Sun Fu Memorial IEEE Transactions on Robotics Best Paper Award

◎受賞内容: IEEE Transactions on Roboticsの趣意に沿った最も優れた論文(年間1本)に贈られる賞であり、技術面、獨創性、潜在的効果、プレゼンテーションの明瞭さ、応用への実地的意義の点で優れていたため

◎団体名: IEEE Robotics and Automation Society

◎受賞のコメント:

人間の運動能力を支える神経計算過程の理解を、ロボットの柔軟な制御と学習に役立てることを目指してきました。ロボティクスと神経科学を統合することは、これらの研究分野を大きく進展させると信じます。今回の最優秀論文賞は、ロボティクス分野では世界で最も権威のある賞です。人間が自らの運動システムを環境に適応させる仕組みを解明し、それをロボットの制御に応用し、人間と同様の優れた運動知性を実現することに成功しました。



## 受賞者 ● 成瀬 誠 (なるせ まこと)

光ネットワーク研究所 フォトニックネットワークシステム研究室 主任研究員

共同受賞者: 豎 直也 (東京大学大学院)  
関根 陽子、大八木 康之、  
法元 盛久 (大日本印刷株式会社)  
松本 勉 (横浜国立大学大学院)  
大津 元一 (東京大学大学院)

◎受賞日: 2012/7/24

◎受賞名: 第26回(2012年度)獨創性を拓く  
先端技術大賞  
優秀賞(フジサンケイ ビジネスアイ賞)

◎受賞内容: ナノ寸法の光を用いたナノフォトニックセキュリティの研究開発

◎団体名: フジサンケイ ビジネスアイ

◎受賞のコメント:

このような伝統と名誉ある賞をいただくことができ関連各位に深く御礼申し上げます。受賞対象の研究は、近接場光という「小さな光」を用いた光システムの原理と実現に関する内容です。システム設計、ナノ構造作製、近接場光分析、性能評価をNICT、東京大学、大日本印刷株式会社、横浜国立大学が共同で行いました。授賞式は高円宮妃殿下ご臨席のもと行われ、パネル展示説明という光栄に預かりました。今後ご指導のほどよろしくお願い申し上げます。



左から2番目が成瀬誠

## 受賞者 ● 児島 史秀 (こじま ふみひで)

ワイヤレスネットワーク研究所 スマートワイヤレス研究室 主任研究員

◎受賞日: 2012/7/31

◎受賞名: The IEEE Standards Association acknowledge with appreciation

◎受賞内容: IEEE 802.15.4eタスクグループにおいて、スマートメータ等に有効な省電力MAC仕様の提案を行い標準規格に収録された実績をはじめ、同タスクグループにおける標準化活動において多大なる寄与を行ったため

◎団体名: IEEE-SA

◎受賞のコメント:


本業績は、国内ガス会社・メータメーカにより切望されたスマートメータ用省電力無線技術を、NICTの貢献により国際標準規格として策定したもので、国内通信技術の発展に寄与するというNICTの本分からも、その高い意義を実感すると同時に、本受賞に対し大変光栄に感じております。当該技術分野は現在、標準化後の普及化フェーズにありますが、今後の発展に対し、NICTとして適切な寄与を行っていききたいと思っております。



**受賞者 ● 伊沢 亮一** (いさわ りょういち) ネットワーク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

◎受賞日: 2012/9/5  
 ◎受賞名: FIT2011 ヤングリサーチャー賞  
 ◎受賞内容: 論文「One-Time Password Authentication Scheme to Solve Stolen Verifier Problem」が優秀であると認められたため  
 ◎団体名: 情報科学技術フォーラム運営委員会

◎受賞のコメント:  
 本賞を受賞できたことを大変嬉しく思っております。FIT2011ではクライアントとサーバが安全に相互認証するためのワンタイムパスワード認証方式を提案しました。提案方式の特徴は、攻撃者がサーバおよび通信路から情報を盗用してなりすましを行う『ハイブリッドセフト攻撃』に対して耐性があることで、この点を評価いただきました。本研究を行うにあたり有益なご議論をいただいた方々に感謝しております。




**受賞者 ● 藤枝 美穂** (ふじえだ みほ)<sup>\*i</sup> **熊谷 基弘** (くまがい もとひろ)<sup>\*i</sup> **蜂須 英和** (はちす ひでかず)<sup>\*ii</sup> **李 瑛** (り いん)<sup>\*i</sup> **井戸 哲也** (いど てつや)<sup>\*iii</sup> **長野 重夫** (ながの しげお)<sup>\*i</sup> **井戸 哲也** (いど てつや)<sup>\*iii</sup>

<sup>\*i</sup> 電磁波計測研究所 時空標準研究室 主任研究員 <sup>\*ii</sup> 電磁波計測研究所 時空標準研究室 研究員 <sup>\*iii</sup> 経営企画部 企画戦略室 プランニングマネージャー

共同受賞者: 山口 敦史 (Physikalisch-Technische Bundesanstalt) 高野 哲至 (東京大学) 高本 将男 (東京大学) 香取 秀俊 (東京大学)

◎受賞日: 2012/9/11  
 ◎受賞名: 応用物理学会論文賞 (優秀論文賞)  
 ◎受賞内容: Sr-光格子時計におけるNICT-東大リンク実験の論文「Applied Physics Express Vol4 082203(2011)」が優れていたため  
 ◎団体名: 公益社団法人応用物理学会

◎受賞のコメント:  
 近年より高精度な光周波数標準による秒の再定義が求められていますが複数の光周波数標準の値が本当に一致しているのか確認する手段がないため、未だ実施には至っていません。本論文では、光ファイバ経由での比較手段を確立し確かに値が $10^{-16}$ という不確かさで一致することを示しました。全員の力を合わせ、数回の徹夜を経て得た結果が認められ大変光栄です。光テストベッドJGN2plusの利用をはじめご支援いただいた皆様に感謝致します。




左から熊谷基弘、山口敦史、井戸哲也、蜂須英和、藤枝美穂、李瑛

**受賞者 ● 岡本 拓磨** (おかもと たくま) ユニバーサルコミュニケーション研究所 多感覚・評価研究室 研究員

◎受賞日: 2012/9/20  
 ◎受賞名: 栗屋潔学術奨励賞  
 ◎受賞内容: 「多チャンネルスピーカアレイによる音響ブライバシーエリア形成のマスクに関する検討」が優秀な講演と認められたため  
 ◎団体名: 一般社団法人日本音響学会


◎受賞のコメント:  
 今回受賞した栗屋潔学術奨励賞は、今回の発表だけでなく、これまでの研究発表を総合的に評価して若手研究者に贈られます。今回の受賞を励みにし、今後もよい研究をしていきます。多数のスピーカを用いて、音声が聞こえるエリアと全く聞き取れないエリアを形成する方法を提案しました。今後はこの方法をスピーチブライバシーだけでなく、様々な位置で異なる音が聞こえるような超臨場感音響通信技術として発展させていければと思います。



**受賞者 ● 佐々木 謙介** (ささき けんすけ) 電磁波計測研究所 電磁環境研究室 研究員

◎受賞日: 2012/9/20  
 ◎受賞名: 電気学会優秀論文発表賞  
 ◎受賞内容: 平成23年度の電気学会 基礎・材料・共通部門における発表(著者: 佐々木謙介・和氣加奈子・渡邊聡一)が優秀論文発表として評価されたため  
 ◎団体名: 一般社団法人電気学会

◎受賞のコメント:  
 この度、私どもの電磁界理論分野における研究発表が評価され、優秀論文発表賞をいただきました。本研究ではこれまで評価が困難と考えられていたミリ波帯での人体へのばく露評価技術について提案・検討致しました。本研究を進めるにあたりまして日頃よりご支援・ご助言いただきました電磁環境研究室及び、関係者の皆様に感謝申し上げます。



# 情報バリアフリーのための ICT分野のサービス提供を支援します。

## チャレンジド向け通信・放送役務提供・開発推進助成金 平成25年度公募

公募期間：平成25年3月12日(火)～4月15日(月)

### ◇ 対象事業

身体上の障害のため通信・放送役務を利用するのに支障のある人が当該通信・放送役務を円滑に利用できるようにするためのもので、身体障害者(以下「チャレンジド」という)の利便の増進に著しく寄与する通信・放送役務を提供し、又は開発する業務

### ◇ 助成期間

単年度

### ◇ 助成率

2分の1

助成金は、助成対象経費として妥当であると判断された経費に対して支払われるもので、助成対象経費の2分の1を限度額とします。

### ◇ 対象者

民間企業等

\*対象者自身が自らサービスを提供することが必要です。

### ◇ 対象事業者の要件

- (1) 助成対象事業を的確に遂行するに足る能力を有すること。
- (2) 助成対象事業に係る資金調達に自己のみによっては困難であること。
- (3) 助成対象事業を的確に遂行するのに必要な経費のうち、自己負担分の調達に関して十分な能力を有すること。
- (4) 助成対象事業に係る経理その他の事務についての確な管理体制及び処理能力を有すること。

身体上の障害のため通信・放送役務を利用するのに支障のある人がこれを円滑に利用できるよう、通信・放送役務の提供又は開発を行う民間企業等に対して、必要な資金の一部を助成します。  
募集要項は、<http://www.nict.go.jp/press/2013/03/12-1.html> をご覧ください。

事業者(申請者)

公募

申請

助成金  
交付

NICT

(独) 情報通信研究機構

評価委員会  
(外部有識者)

### ◇ お問い合わせ先

産業振興部門 情報バリアフリー推進室

E-mail: kakusa@ml.nict.go.jp

URL:

[http://www2.nict.go.jp/ict\\_promotion/barrier-free/104/](http://www2.nict.go.jp/ict_promotion/barrier-free/104/)

読者の皆さまへ

次号は、光周波数標準の先がけとなるストロンチウム光格子時計や新たな研究プロジェクトについて取り上げます。

**NICT NEWS** 2013年3月 No. 426

ISSN 1349-3531 (Print)  
ISSN 2187-4042 (Online)

編集発行

独立行政法人情報通信研究機構 広報部

NICT NEWS 掲載URL <http://www.nict.go.jp/data/nict-news/>

〒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](mailto:publicity@nict.go.jp)

URL: <http://www.nict.go.jp/>