岡本龍明　フェロー　NTT Research, Inc. CIS Lab　所長

世界トップの暗号研究所をめざして

ICTによってあらゆるビジネス活動が展開される現代において，セキュリティ対策の要ともいえる暗号技術はますます信頼性・確実性への期待が高まっています．暗号，ブロックチェーンの世界的権威が集結するNTT Research, Inc.のCryptography and Information Security Laboratories（CIS研）で陣頭指揮を執る岡本龍明フェローに，研究所の進捗とトップレベルの研究者としての心構えを伺いました．

米国だからできる「暗号のドリームチーム」結成

●現在なさっているお仕事を教えてください．

NTT Research, Inc.のCryptography and Information Security Laboratories（CIS研）所長として，マネジメントを中心に仕事をしています．前回，本コーナーに登場させていただいたときは１人の研究者としてお話をさせていただきましたが，今回はマネジメントをする立場から，CIS研で手掛ける暗号，ブロックチェーンといったテーマについて，NTT Research, Inc.はどのような研究所かも含めてお話しさせていただきます．

NTT Research, Inc.の開設は2019年7月ですが，それ以前から準備を行っていました．まさにゼロからのスタートで，開設前の半年は特に人集めや体制づくりに集中的に取り組んでいました．立ち上げに先立ち，2018年に，そこで働かないかとお声掛けをいただいたとき，私は自らが手掛けている暗号という研究分野において，日本ではできない，米国でなければできないことをしたいと思いました．そのためにまずは人材の獲得ですが，シリコンバレーは世界各国から著名で優秀な人材が多く集まり，活動しています．こうしたことから，地の利を活かし，世界トップの暗号研究所を設立して，そこに世界で活躍している人を集め，いわゆる暗号分野におけるドリームチームをつくることを目標に，現在でも尽力しています．

●ドリームチーム結成にはどのような構想がおありだったのでしょうか．

何を研究分野に据えるか．これは戦略的に重要な課題です．私は研究テーマとして，コアな暗号理論，そして，ブロックチェーンの2つを選択し，それぞれを7割，3割の比率で推進することにしました．テーマを絞り込んだ2018年の暮れごろから優秀な研究者の獲得に動き出し，2020年2月現在で10名が在籍しています．暗号分野はBrent Waters博士をリーダーに優秀な研究者6名が，ブロックチェーン分野はジョージタウン大学で研究をされている松尾真一郎博士をリーダーに優秀な研究者4名が担当しています．ただ，ブロックチェーン分野は，スタートアップ，ベンチャーを中心にビジネス分野に活躍する場が多く，どうしてもそちらへ人材が偏ってしまうため，基礎研究を手掛けようという人が少なく，人材の確保に若干苦労しています．

研究所は開設しましたが，採用活動は継続しており，3月より暗号分野で新たにトップレベルの研究者が入所する予定で，今後も長期的な視野を持って優秀な人材を確保しようと考えています．優秀な研究者の場合は声をかけてもすぐに移籍できるという状況にない方も多く，例えば，大学で働いておられる方の場合，好意的に移籍を考えてくださってもすぐに退職して入所できるような環境にはありません．各研究者の状況をかんがみつつ，大学で働きながら研究所に所属して働いてもらうなどして，環境が整い次第，軸足を研究所に移してもらえるように配慮しています．

今は世界のどこにいてもリモートで働ける時代ではありますが，私たちの仲間は徐々に各々が環境を整えてシリコ

ンバレーのこの地に集結し始めています．NTT Research, Inc.も2020年夏で設立１年目を迎え，昨年よりずいぶん進化してきており，私の構想の実現に向けて着々と進んでいます．

戦略的に大きな課題に挑む

●暗号分野の研究ではどのような目標を立てていますか．

従来型の暗号方式は，人に見られたら困るようなものを金庫の中に入れて（暗号化）送り，受け取り側が鍵を使って金庫から出す（復号化）という概念でした．ところが，例えば，暗号化されたメールの中からスパムメールを削除して受信しようとした場合，途中のサーバでスパムメールを検出・削除する必要がありますが，このためにサーバにおいて暗号メールを復号して（鍵を開ける），メールの内容を確認し，検出・削除の処理を行った後再度暗号化する（金庫に入れて鍵をかける）ことになります．つまりサーバ（第三者）が金庫の合鍵を持っていることになり，送信側と受信側の間における暗号化の意味が，この部分で損なわれることになります．逆にいえば，暗号の安全性を確保するうえで，用途をはじめとして各種の制約がある，ということになります．

これに対して，当研究所のWatersは，15年ほど前に属性ベース暗号(ABE)（より一般的には関数型暗号）という概念を世界に先駆けて発表しました（**図１**）．これにより，先ほどの例では，サーバにおいて暗号化されたデータを復号することなく，必要な情報だけを抽出することができるようになり，その情報を基にスパムメールの検出・削除が可能となります．

こうした新しい概念の暗号が登場してくる中，私たちは現在，標準的な仮定の下で安全性が証明された高度な機能を持った暗号方式の実現を目標に，①弱い安全性から望ましい安全性への変換方式，②さまざまな暗号プロトコルの設計，安全性証明，③LWE（Learning with Errors）仮定に基づく暗号方式，などの研究を進めています．

ここで，私たちの取り組みの一端を紹介します．選択暗号文安全性（IND-CCA）は，構成が易しい選択平文安全性（IND-CPA）よりもレベルの高い安全性で，もっとも強い暗号のクラスです．上で述べた属性ベース暗号(ABE)

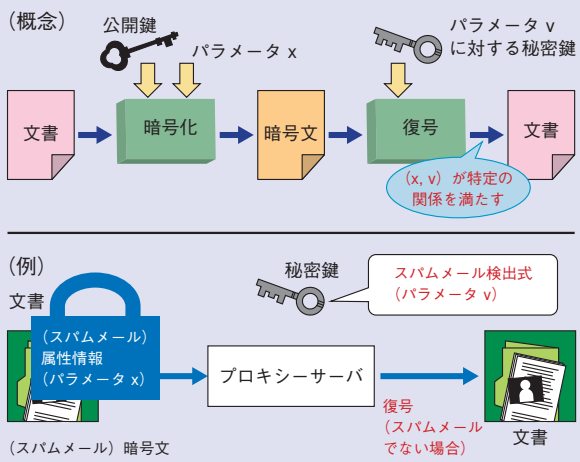

図１　属性ベース暗号（関数型暗号）

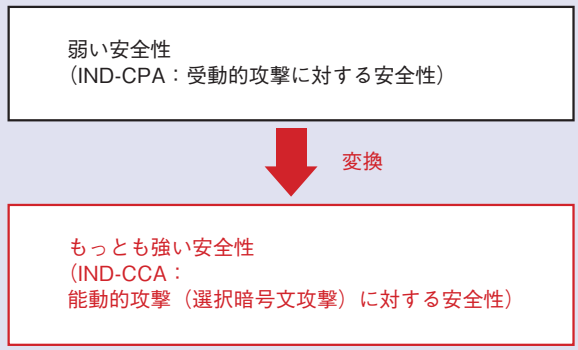

図２　弱い安全性から望ましい安全性への変換

において，最近，私たちはどのようなIND-CPA安全なABEも，hinting PRGと呼ばれる新たな手法を用いることでIND-CCA安全なABEに変換できることを示しました．これを受けて，数論の手法を用いてより高速でコンパクトなhinting PRGの実現，さらに，一般的な関数型暗号や再ランダム化暗号に対しても適用できるIND-CCA変換方法の実現をめざしています（**図２**）．

LWE仮定は，耐量子安全性や格子のワースト問題との関連など，暗号における優れた仮定として広く認められており，また，新たな暗号機能をつくる手法としても多くの結果を生み出してきました．ここで，私たちはLWE仮定に基づく暗号を実現する新たな野心的な目標を持ってい

ます．ここでは，まず疑似ランダム関数（PRF）を難読化する新たな概念とその応用を考え，次にLWE仮定から証拠暗号をつくるための方法を示します．そこへの中間段階として，制限付きPRFを実現し，このような流れの中で，LWEベースのABEの適応的安全性を実現する新たな手法と限界を明らかにしようとしています．

●ブロックチェーン分野ではいかがでしょうか．

ブロックチェーンにおける研究開発の大きなゴールである「プログラム可能な共有された帳簿を利用したアプリケーションを誰もが自由につくることができるような状態を実現する」ための基盤的な研究にフォーカスを当てています（**図 3**）．

昨今，ビットコインやブロックチェーンが大きな話題となりましたから，あたかも広く普及する時期がまもなくやってくるようにも思えるかもしれません．しかし，実際にこうしたゴールを達成するのは非常に大きなチャレンジで，長期にわたる基礎的，理論的な研究開発が必要です．このため，セキュアかつよりスケーラブルな分散合意アルゴリズムの研究，プログラム可能な帳簿のための安全なプログラミング環境を実現するための研究，そして，ブロックチェーン上での情報処理を行う際のプライバシ保護の実現のための研究に取り組んでいます．

ブロックチェーンの理論研究はさまざまな異なる性質が絶妙に組み合わさっているため，異なる専門性を持った研究者でチームを構成する必要があります．さらに，ブロックチェーンは戦略的に研究を展開しなくてはなりません．前述のとおり，人材がベンチャーやスタートアップに流れてしまうので優秀な人材の確保が難しく，チームがまだ立ち上がったばかりということもあり，より人材を強化する必要性を感じています．現在は，暗号プロトコルの安全性，ソフトエンジニアリング，形式検証，ゲーム理論，経済学の専門性を持つ研究者で組織しており，さらに異なる専門性を持つ研究者の採用をめざしています．

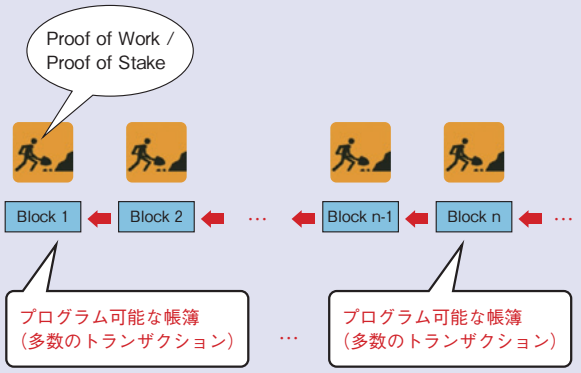

図 3　ブロックチェーンによるプログラム可能な公開帳簿

研究者としての業績を上げる以外にアピールする術はない

●優秀な人材を見極める際，どこをご覧になっているのでしょうか．あるいは，応募者の立場からどうアピールすべきかを教えていただけますでしょうか．

研究者の場合は特にアピールする必要はないと思っています．その分野のプロフェッショナルの研究者が集う学会では優秀な研究者どうしが評価し合っています．例えば，暗号チームのWatersは世界トップの研究者であり，彼は，中堅，若手などそれぞれのレイヤで優秀な研究者をよく知っています．現在のメンバーも彼の推薦による研究者が入所しています．設立して半年の間，噂を聞きつけて売り込んでくる研究者もいるのですが，基本的には自薦ではなく，研究分野で卓越した業績や能力を持つ人を採用するつもりです．ブロックチェーンチームの松尾もこの分野の優秀な人材には詳しく，彼の推薦により研究者を迎え入れています．まだ学生でこれから博士号を取ろうとしているような若い研究者であっても，優秀な人はその研究成果のどこかに光るものがありますから，そういう人材を探し当てることは可能です．つまり，自分の研究者としての業績を上げる以外にアピールする術はないと思います．

●研究の課題やテーマを探すときに意識していらっしゃることはありますか．

私は自分の研究分野において，もっとも重要と思われる課題をテーマにしたいと思っています．その研究分野の方向性を決めるようなテーマであり，自分にとって興味が持てることなどを基本にしています．いろいろな人と共同研究しながらディスカッションをすると，お互いに新たなテーマが見つかることがあります．その際も，仮に誰かがおもしろいと評価しても，自分自身がそれを重要だと思えないことはテーマにしたくありません．ただ，これにもさまざまな場合があって，最初はそれほど重要だと思われな

かったことが後々発展して，中心的なテーマになることもあります．見極めは難しいこともありますが，基本的には優秀な研究者というのは良いセンスを持っていて，それをベースに選択できることが多いように思います．

10年前のインタビューでもお答えしたかと思いますが，一言でいうとこれらは研究者としてのテイストです．テイストは芸術でいえば審美眼のようなもので，研究を進めていく先に待っているのは実り豊かな場所であるか，荒野であるかを見定めるある種の勘です．

どこにいようとも，物まねではなくオリジナルをめざして

●今後はどこをめざしていきますか．

チームとしては自他ともに認める世界トップレベルの研究者集団をめざします．今でも結構トップに近いと思っていますが，これを確実なものにしたいと思います．そして，大きな賞を受賞するなど，各研究者の業績の証となるものを得るようにもしたいと思っています．暗号は計算機科学の分野ですので，残念ながらノーベル賞の対象ではありませんが，計算科学のノーベル賞と謳われているチューリング賞の受賞などが1つの目標となります．「NTT Research, Inc.は世界的な権威のある賞を受賞した研究者が在籍している研究所」であるといった，社会的な分かりやすさを追求する意味でも獲得したいですね．

個人としては，ライフワーク的に取り組んでいるものはあります．今の世の中，複雑なものがあふれていますよね．例えば，生命体はとても複雑です．また，宇宙もビッグバン直後の単純な姿から複雑なかたちに進化してきたことが知られています．こうした世の中で複雑だといわれている物事に対して，統一的な見方というものをある種の科学としてとらえたい．30年以上前から複雑系という研究分野はあるのですが，この延長線上で理論的にきちんとしたものを打ち出したいと思っています．私は今67歳です．マネジメントの仕事はこれからそれほど長くできるとは思っていませんが，研究者としての仕事はもう少し長く現役で続けていきたいと思っています．

●若い研究者の皆さんに一言お願いいたします．

日本の外で仕事をしていて「日本は少し縮んでいるな」というイメージがあります．1980年代はバブルでもありましたから，ジャパンアズナンバーワンともいわれていましたが，日本は今，世界の中で存在感が少なくなったように感じます．IT業界においてGAFAのような企業は，NTTの研究開発費の10倍あまりの研究開発費をかけています．こうした状況下では，従来日本（企業）が成功したようなやり方を繰り返していては，その存在感をあまりアピールできないのではないでしょうか．現在，日本においてもっとも成功したIT企業も世界においては存在感がありません．ではどうしたら存在感を示せるのか．今私たちは，日本にいては小さなサークルをぐるぐると回っているだけにすぎないという意識を持って，NTT Research, Inc. などの試みを通じて，世界へ向けての取り組みを行っています．こうした意識で視点を世界に向けて行動すると良いと思います．重要なのは物まねではなくてオリジナルな何かを生み出すことです．日本のベンチャー企業はどこか他人の物まねをしているところが多いのではないかと感じます．誰とも違う自分独自のものを生み出すという気概を持つと良いでしょうね．この時代，東京（もしくは地方）にいてもネットでつながっていますから，シリコンバレーでできることはできるはずです．視点を世界に向けて，日本にいてもこれは誰にも負けないという気概でオリジナルな発想を生み出していただきたいですね．