特別連載

ムーンショット・エフェクト——NTT研究所の技術レガシー

第11回　暗号技術

ノンフィクション作家の野地秩嘉（のじつねよし）氏より「ムーンショット・エフェクト——NTT研究所の技術レガシー」と題するNTT研究所の技術をテーマとした原稿をいただきました．連載第11回目は「暗号技術」です．本連載に掲載された記事は，中学生向けに新書として出版予定です（NTT技術ジャーナル事務局）．

■暗号とCISラボラトリー

NTT研究所のひとつCryptography and Information Security Laboratories（CISラボ）があるのはアメリカ，カリフォルニア州のサニーベールだ．シリコンバレーの一角にあり，パーム，AMDなどITベンチャーの本社がいくつもある町だ．

2019年に設立されたCISラボが研究しているのは暗号で，そのうち，暗号理論と仮想通貨等で利用されているブロックチェーンが対象である．社員数は49名で，うちCISラボの研究者は14名．設立されたばかりといってもいいのだけれど，暗号研究の分野ではすでに業績を上げている．

例として，次のふたつの賞が挙げられる．国際暗号研究学会（IACR）からは2020年4月にTest of Time Award，8月にはCrypto2020 Best Paper Awardを受賞した．さらに特許は10件を出願し，最難関の国際会議（Crypto，Eurocrypt）に採択されている論文数は世界一である．そして，現在活発に研究を行っているトップクラスの研究者の数も，例えばマサチューセッツ工科大学（MIT）などの一流大学や企業での暗号チームがそれぞれ4,5名程度であることに比べるとCISラボには7，8名以上が在籍している．

このように暗号の研究では世界トップレベルにある．

さて，所長の岡本龍明は「暗号とは何か」からレクチャーを始めた．

「辞書には，『秘密通信を行うための方法や装置に関する科学』と書いてあります．もともと暗号は軍事における使用がほとんどでした．それがインターネットの登場により，商用利用が進んだのです．インターネット自体は1969年に主として大学の間の通信技術として始まったわけですが，一般が使うようになったのは1990年代の中ごろ，みなさんもよくご存じのWindows 95が登場した頃からです」．

■ダダ漏れのインターネット

インターネットが一般化した頃，「データはダダ漏れが当たり前だったのです」と岡本は言った．

「データはネットワーク上を転々としながら，相手に届けられます．初期はセキュリティも考えずにデータは公開されたまま伝わっていきました．開封されたままの信書を裸のまま届けていたようなもので，誰でも簡単に見ることができましたし，改ざんされたり，すり替えられたりする危険がありました．そこでデータを暗号化してネットワーク上に載せるようになったのです」．

そうしてダダ漏れをなくすために暗号技術の商用化は始まった．

まず，暗号にはふたつの機能がある．

ひとつは秘匿する機能だ．データを簡単に見られないようにすること．

もうひとつは認証機能．送ったデータが正しいかどうか，送った相手が正しいかどうかを認証すること．

このふたつの機能を進化させることがデータのセキュリティを守り，個人のプライバシーを保護することにつながる．

■暗 号 理 論

暗号理論のなかでもCISラボの研究者が提唱した新しい概念の暗号が属性ベース暗号というもの．

岡本はこう解説する．

「従来の暗号方式は例えば人に見られたら困るものを暗号化して送り，受け取った側が復号機能を使って，暗号を元に戻すわけです．

一方で，例えば，暗号化したメールのなかからスパムメール（迷惑メール等）だけを削除して送るといったことがある場合，途中のサーバで暗号化されたものをいったん復号しなければなりません．そうしてメールの内容を確認し，スパムメールを検出，削除してから再び暗号化して，相手に送ることになる．つまりサーバという第三者が内容を見てしまうわけです．そうなると，暗号化の意味が損なわれ，暗号の安全性を確保するうえで，瑕疵（キズ）がついてしまう．

それに対して，CISラボのブレント・ウォーターズという研究者は15年ほど前から属性ベース暗号（一般的には関数型暗号）という概念を考えだしました．先ほどの例でお話しすると，サーバにおいて暗号化されたデータを復号せず，暗号化したまま必要な情報だけを抽出して，スパムメールの検出・削除を可能とする技術です（**図**）」．

属性ベース暗号を使えばスパムメールの検出，削除だけでなく，自身の医療データや金融データのような，他人には絶対，知られたくないデータを安心して外部のサーバに保存したり送信したりすることができるようになる．

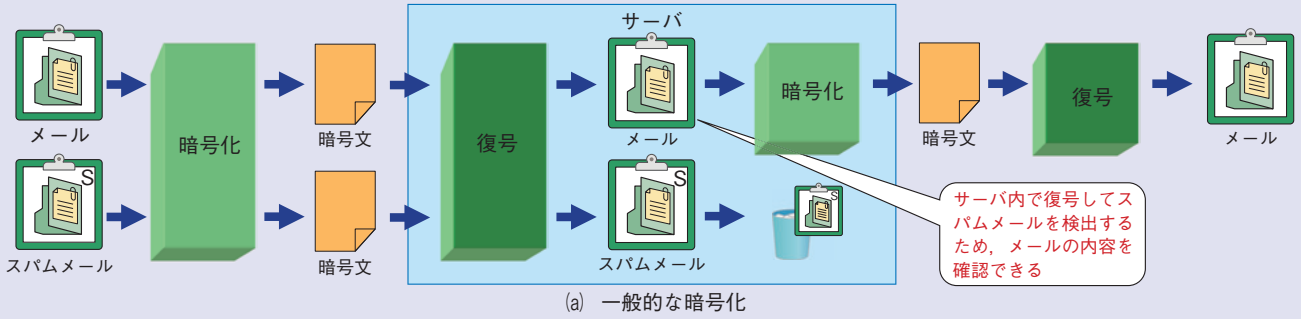
■ブロックチェーン技術

CISラボの研究テーマは暗号理論とブロックチェーンの２つであり，それぞれ７割，３割の比率で研究を進めている．ブロックチェーンに関してはジョージタウン大学でも研究を続けている松尾真一郎博士をリーダーに研究者４名が担当している．

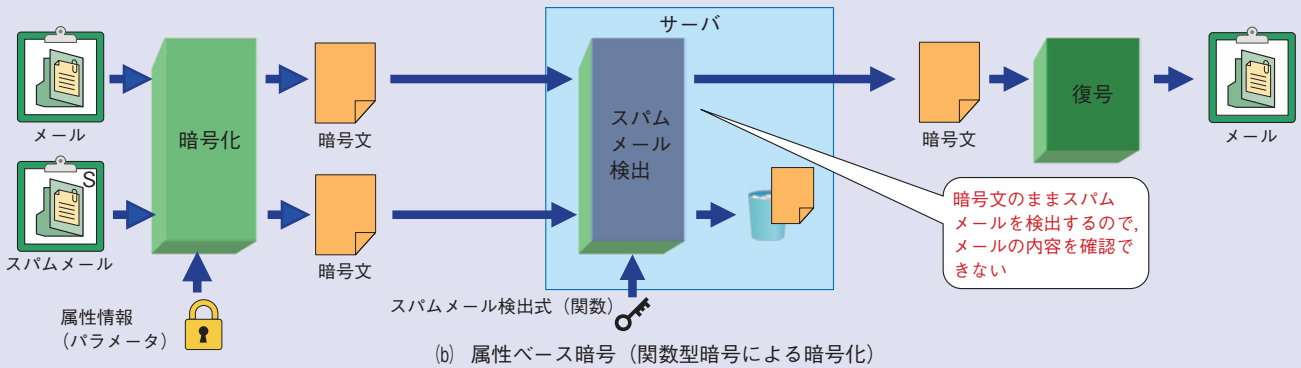
ブロックチェーンは暗号資産（仮想通貨）で使われている技術だ．そのため，スタートアップ企業（革新的技術で創業し急激に成長した企業），ベンチャー企業（革新的技術で創業した企業）を中心に研究者の奪い合いになっている．CISラボは基礎研究なので，岡本はブロックチェーン研究の場合，人材の確保に苦労していると苦笑した．

彼は言った．

「当研究所のブロックチェーン研究のゴールは『プロ



⑷　一般的な暗号化



⑸　属性ベース暗号（関数型暗号による暗号化）

図　属性ベース暗号（関数型暗号）

グラム可能で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こと』．今のところはそのための基盤的な研究にフォーカスを当てています．

現在，ビットコインのような仮想通貨やブロックチェーンが大きな話題になっています．そのせいもあって，『誰でも共有可能な公開帳簿』がすぐにも普及すると考えている人が少なくないようです．しかし，誰もが簡単に使える共通の帳簿づくりにはまだまだ時間がかかります．長期にわたる基礎的，理論的な研究開発が必要なのです．

また，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，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．そうなると，CISラボはもっと多くの方に協力していただかなくてはならないと思っています」．

■毎日の研究と受賞の意義について

では，暗号とブロックチェーンの「研究」とはいったい，どういった作業になるのだろうか．この場合の研究とは実験のような手を動かすことではないだろう．それは「考える」ことだ．

すると，それはつまり，沈思黙考する毎日なのか．そういうことならば何も研究所まで行かなくとも，自宅で学術論文を読んだり，窓を開けて雲の流れを見つめて，ひらめきが下りてくるのを待っていたりしてもいいのではないか…．

「いやいや，そうではありませんよ」．

岡本は言った．

「確かに研究のアイデアは机に向かわなくとも出てきます．通勤電車のなかでも，散歩している途中でも，何かしら考えているのが研究者ですから．私が思うに，研究者として必要なのはディスカッションです．先ほども申し上げましたが，当研究所のブロックチェーン研究者は数学，量子力学，ITと専門が分かれています．専門が違う人間たちが対面し，集まって話すことがとても重要だと思っています．幸い，アメリカはワクチン接種が進んで，ロックダウンもなくなりました．生身で話しながら研究が進むのを楽しむ毎日が戻ってくるのも近々のことでしょう」．

冒頭に触れたが，CISラボは設立してわずか3年足らずなのに，受賞歴もあり特許も獲得している．暗号の基礎研究機関としてはすでに世界トップと言っていい．それは岡本の研究所マネジメントが優れているからなのか．

「いえいえ，そんなことはありません．ただ，この分野はとてもオープンな分野です．誰が何をやっているかがすぐにわかりますし，評価される世界でもあります．

受賞したうちのひとつ，Test of Time Awardの受賞論文はブレント・ウォーターズが15年前に発表した論文です．属性ベース暗号の概念を世の中に提示したもので，世界でもトップクラスの引用件数を誇る論文です．15年の間にさまざまな論文に引用され，また実用されて使われるようになりました．時代を経て認められた論文です．この賞は，学会でもこうした研究成果を大切に評価しようとしてきている証拠なんです．つまり，未来で高く評価されるような成果をめざして研究は進展していくのです」．

暗号研究，ブロックチェーン研究は難解と思われがちだが，関わっている研究者たちにとっては謎解きのような楽しさがあるのではないか．毎日，謎解きに挑戦している彼らの仕事は未来へ向かってボールを投げるようなものだろう．

野地秩嘉（のじつねよし）
1957年東京都生まれ．早稲田大学商学部卒業後，出版社勤務を経てノンフィクション作家に．日本文藝家協会会員．人物ルポルタージュをはじめ，食や美術，海外文化などの分野で活躍中．著書は『高倉健インタヴューズ』『キャンティ物語』『サービスの達人たち』『ニューヨーク美術案内』など多数．『トヨタ物語』『トヨタに学ぶカイゼンのヒント』がベストセラーに．『TOKYOオリンピック物語』でミズノスポーツライター賞優秀賞受賞．近著は『日本人とインド人』（翻訳　プレジデント社），『新TOKYOオリンピック・パラリンピック物語』（KADOKAWAから7月14日発売予定）．