挑戦する研究者たち
CHALLENGERS

阿部正幸

NTTセキュアプラットフォーム研究所
上席特別研究員

研究には「塞翁が馬」の視点と姿勢で臨む．影響を与え合える関係性の構築も研究活動である

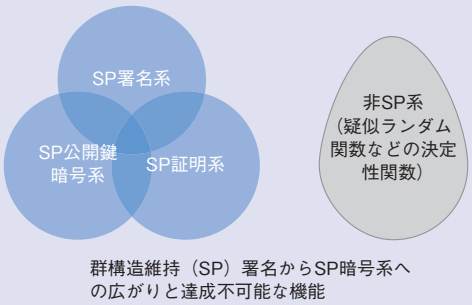
電子決済などの電子商取引や，ネット税務申告などの電子政府機能が普及しつつある現在，ネットワークやサービスの安全性についてはその重要性がますます高まっています．こうした中，現代暗号は安全性を保証する技術として活発に研究され発展しています．先導的研究を行い，革新的な技術を多数創出し実用化したことが評価され，2018年に情報通信および放送の進歩発展に著しい功績のあった方々に贈呈される前島密賞を受賞した阿部正幸NTTセキュアプラットフォーム研究所　上席特別研究員に，研究の進捗や研究者としてのあり方を伺いました．

「できない」ことを明らかにする

前回のインタビュー以来，手掛けている研究についてお聞かせください．

私が追究している大きなテーマは安全な暗号プロトコルの構成です．元の情報を暗号化したりデジタル署名を付けたりすることで必要な情報だけを必要な相手に安全に届ける，この手順のことを暗号プロトコルと言いますが，特に安全で効率的な暗号プロトコルへのアプローチが究極の目標です．一言で暗号プロトコルといっても，さまざまな要素が組み合わさって，幾重にも重なって構成されており，研究対象も基礎研究から応用研究まで，広い範囲に及びます．その中でも特に基礎となる部分は技術の進歩に沿ってチューンされていくことで変化していきます．まさに職人技的です．一方，基礎の上に積み重なっている技術は技術の進歩による変化を基礎の部分で吸収するので，これまでの技術や新しい技術を組み合わせることで対応できます．このような体系において，私は全体のバランスをかんがみて包括的な解と特化した問題に対する解の双方を求めるような取り組みを展開したいと考えています．

前回，2013年のインタビュー以降，大きく３つの研究を手掛けています．１番目は，群構造維持（SP）暗号系で



SP署名はさまざまな応用を持ち，その概念は公開鍵暗号や証明系へも広がった．一方，SPの概念が実現できない暗号機能があることも分かった．

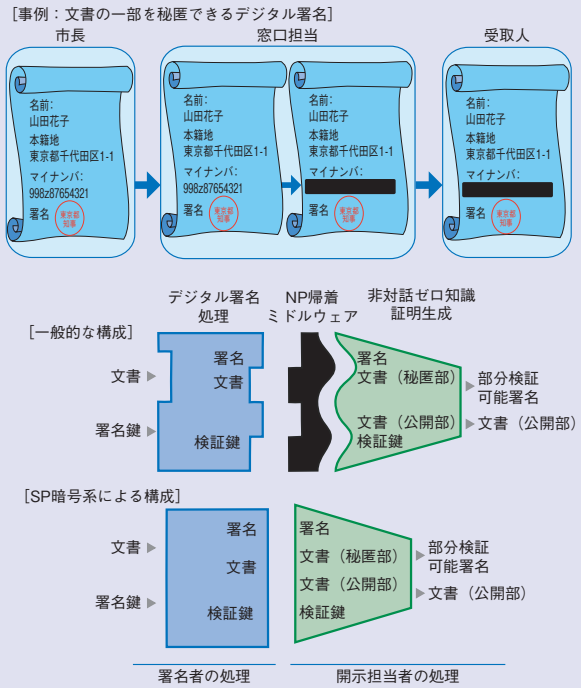


図１　群構造維持暗号系

実現不可能な関数があることの証明です（**図１**）．SP暗号系は，統一されたインタフェースを持つ複数の暗号技術を組み合わせて生成される安全性の高い暗号系で，広く応用されていますが，この概念が実現できない暗号機能があることが判明し，それを解明・証明することです．２番目は，構成不可能性を証明することです（**図２**）．SP暗号系で，複数の機能を組み合わせて高度な機能を構成する場合に，ある機能のインタフェースのみを用いたのでは，所望する機能の構成ができないことを証明するものです．そして，３番目はスマートコントラクトを用いた安全な情報売買の方式で，基礎から応用までを手掛けています（**図３**）．

SP暗号系は，2009年の終わりにその着想を得て，2013年はSPデジタル署名を開発し，実現に近づいてきたという時期でした．ドイツのカールスルーエ工科大学との共同研究により，高い安全性と相互接続性を両立するSPデジタル署名方式を世界で初めて開発しました．この成果は2017年８月に米国で開催された国際暗号学会主催のトップ会議 CRYPTO 2017 で発表しました[(1)]．その後，デジタル署名以外の暗号機能に関してもインタフェースを整えることを追究し続け，QA-NIZKと呼ばれる非対話証明系の開発にも取り組みました．

このプロセスを経て単にインタフェースを組み合わせるだけではなく，機能等を模索し，安全性が担保できない限界点，つまり「できない」ことを明らかにすることができました．この成果によって私たちは暗号分野で認知され，１つの研究分野を築くことができました．

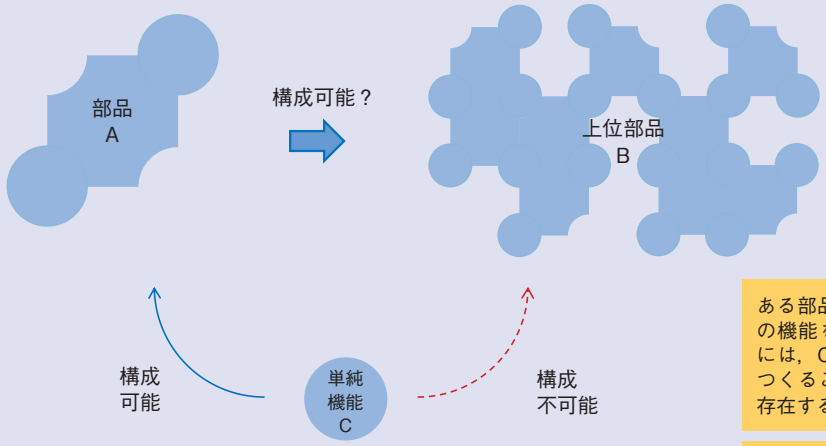


図 2　構成不可能性の証明

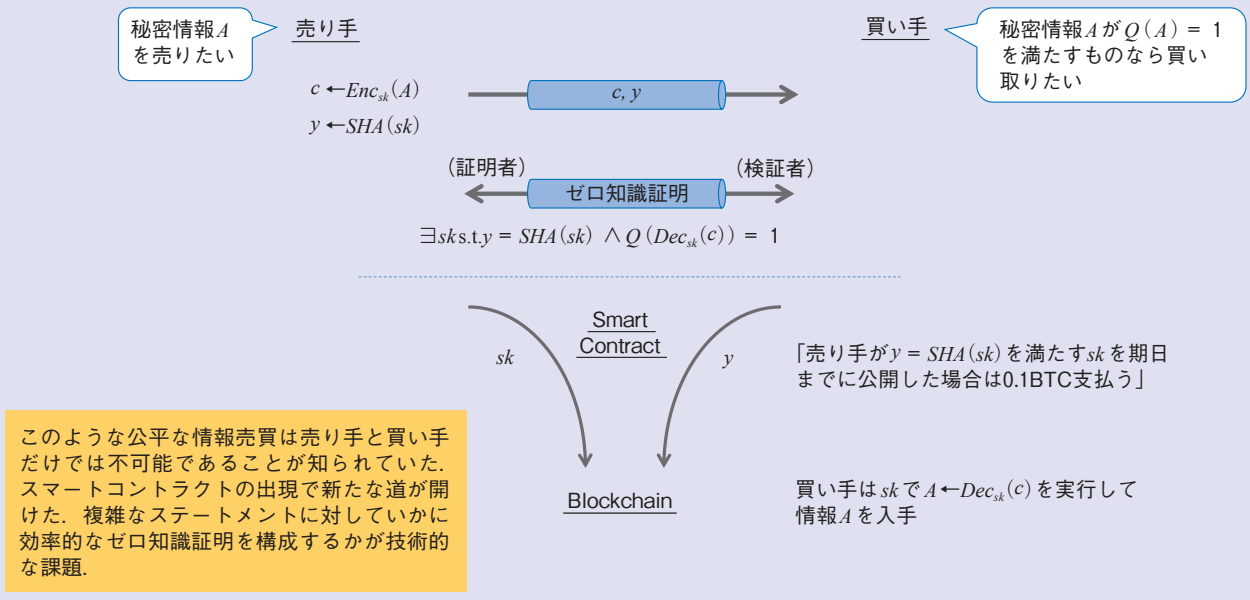


図 3　ブロックチェーン上のスマートコントラクトを用いた安全な情報売買

限界点や不可能性を証明することは重要なアプローチなのですね．

不可能性の証明は，一見すると生産的ではないように映るかもしれませんが，不可能性を知ることはとても意味のあることです．暗号系の研究はコンピュータの技術が変わると攻撃者の水準も変わります．これは安全性の概念が変わることを意味します．ごく簡単にいえば，基盤となるコンピュータの部分の安全性がその上に積み重なった技術に影響を与えないようにするためには，影響を与える限界点を把握する必要があります．不可能性の証明は，「ここから先は通行止め」と知らせる行為であり，さらに不可能の本質を知ることにつながり，組み立ての新しい方法を誘導する非常に有意義な研究なのです．

これを活かして追究し始めたのが非対話証明の言語拡張です．非対話証明は一方的に情報を送るだけで証明を完結させる技術です．デジタル署名とは違う暗号技術ですが，この分野でも限界点を追究しました．非対話証明の技術について，例えば，個人の年齢確認を行う場合には，生年月日を含む個人情報が記録された媒体（運転免許証やパスポート等）の提示を求められる場合がありますが，生年月日や個人情報は照会されたくないとき，年齢のみを提示できればこの問題は解消できます．これを可能にする技術がゼロ知識証明で，証明系といわれる暗号分野です．非対話証明暗号はSPと相性が良く，組み合わせて使われていました．そして，これらを組み合わせてもっと大きな事実を証明できないかと考えたのです．例えば，20歳以上で，自動車運転免許証を保持していて，社員2000人以上の企業に勤務している等，複合的な事実を証明するような証明系に拡張することを追究し始めました．ところがこれは難しいことが分かり，現在はそれが単に難しいだけなのか，不可能であるのかを明らかにすることに挑んでいます．

暗号系の研究はそれぞれの要求に合わせた安全性を考えていくことです．どこまでが暗号理論で守れるか，サーフェイスをしっかり示すのが仕事の１つで，新しい技術が生まれるたびに安全性の意味や使い方を検討します．スマートコントラクトはブロックチェーンを支える非対話証明の技術の応用で，自動化された契約行為を手助けします．当時の技術は非効率で，安全性が明確に示されていなかったのです．これらを追究しようとヨーロッパのポスドク（博士学位を取得した後，任期制の研究職に就いている人）とともに応用系，ブロックチェーンの分野に初めて挑み，デジタル情報の安全な売買の新しい方法を提案することができました．まだ検討すべきことがありますので継続して取り組んでいきたいと考えています．

人との連鎖が研究成果につながる

研究活動を充実させるために心掛けていらっしゃることはありますか．

暗号プロトコルの研究分野は，かつては比較的小さなコミュニティで，研究対象も限られていました．しかし，セキュリティが一般的な概念となって研究のすそ野もかなり広がったため，学会でも隣のセッションで隣接する分野について議論されていることが十分に理解できないこともあります．

こうしたときに助けになるのは，アンテナを高くすることや過去の論文の共同執筆者や友人，知人の存在です．情報収集や研究を自分だけで成し遂げるのは大変ですが，友人や知人等との交流から新しい情報に触れることができます．

前述のスマートコントラクトの研究はまさにその事例です．その分野で良い成果を上げたかつての研究仲間であるポスドクとの会話が発端となり，私はスマートコントラクトを追究し，価値ある報告をすることができました．彼との出会いはスペインで開かれた学会でした．当時，まだ学生だった彼が学会で，私が過去に手掛けていた研究テーマについて発表していたのです．とても興味深い発表でしたから私は彼に「良い発表ですね！」と声をかけひとしきり

話をしました．そのときはそれで終わったのですが，数年後に突然「大学院を卒業するのであなたの下で研究をしたい」とのコンタクトがあり，彼との研究活動が始まりました．おそらく直接話したことが一度もなければ実現していなかったでしょう．「人となり」を知っていたからこそだと思います．

こうした経験からも人のネットワークは研究者にとって死活的な問題だと考え，友人や知人との関係はとても大切にしています．学会等，機会があれば積極的に出かけてさまざまな人と知り合って，研究につなげています．長い間続けてきたので，友人や知人も現在では権威あるポストについている方が多くなり，彼らが指導している学生などとのつながりも生まれ，新しい研究活動が生まれるという良い循環ができています．人との連鎖が研究につながっていくことが本当にうれしいです．

充実したつながりが研究に良い影響を与えるのですね．どんな研究者の周りに人は集まるのでしょうか．

自分の知らないことを知っていて，それを多く持っている研究者の周りには自然と人が集まってきます．自らがそのような人材であることはもちろん大切ですが，これに加えて研究活動はある意味で寝食を共にする間柄でもありますから，特にフィーリングの合う方とのつながりがあればもっと良いと思っています．

若い方々はもう少し計画的に研究者どうしがつながっていくのかもしれませんが，私は研究者の「人」の部分とのつながりを大切にしたいのです．なぜなら，研究は私にとっては生活の一部ですし，人生の大半を費やしてきたのが研究活動です．それを自分が大切にしていることから切り離すことはしたくないですね．

また，研究は基本的にアウトプットを求められますから，それを創出するためにもインプットが重要となります．人とのつながりや余暇等，何からインプットするかは人それぞれですが，私は世界中の人とのつながりから得ています．これを研究活動と連動させることができるこの環境をとても幸せだと思っています．

ところが，2020年は新型コロナウイルスの感染拡大によって，人とのつながり構築を実行できませんでした．過去では，東日本大震災のときにも同様に人との連鎖が中断しました．当時は私のグループに入る予定だったポスドクが震災によって来日を躊躇したのです．この状況も，日本の安全性を来日予定のポスドクたちに伝えることで徐々に解消されましたが，今回の新型コロナウイルスの感染拡大はそのときと状況が違います．私たちも海外に赴くことができないし，海外の研究者の来日も難しいのです．日本に住んでいる外国籍の研究者はいても，これを機に来日しようという研究者は限りなく少ないのです．既知の仲をリモートでつなぎ，彼らの紹介で新しい出会いもありますが，予期せぬ出会いが自然発生的には起こり得ないのが残念です．

若い研究者を励ます言葉は自分への励ましでもある

暗号分野の先駆者として，この分野の発展をどのように眺めていらっしゃいますか．

暗号分野の研究は1970年からの積み重ねによって成熟してきました．若い研究者の参入によって多岐にわたる研究に取り組まれてきた結果，すそ野がとても広くなりました．技術が成熟する過程は核となる部分のみが高く積み上がるのではなく，シーツをつまみ上げるようにすそ野が形成されて進んでいくのではないかと思います．多くの研究者がさまざまな可能性を模索することが横への広がり，最先端を追究していくことが縦の伸びです．その形状は崩れることがないというのが研究の成熟を表現しているのではないでしょうか．

暗号分野もかつては結構なスピード感で新しいアイデアが発表されていましたが，すそ野が広がった今では周辺領域も十分に踏まえたうえで論ずる必要があります．さらに，

当初はページ数にして10ページ前後の論文でも受け入れられてきましたが，最近では，30ページ，40ページは当たり前になってきたので書き上げるのも大変です．一方で，すそ野が広がり，隣の研究者のしていることが分からないほどに発展してきたというのは，研究者それぞれの頑張りを意味しているし，この分野でオンリーワンになれる可能性が高いことを意味していて喜ばしいと思います．

ただ，どのような研究分野においても，基礎となる部分の技術改革が起きるとそれまでの研究がリセットされる可能性をはらんでいます．例えば，通信ネットワークのクロスバ交換機がデジタル交換機に置き換わり，それがルータに置き換わるといった具合に，過去の技術が全く別の概念の技術に置き換わっています．暗号分野でも基礎に近い分野は同様のことが起きています．暗号と密接なかかわりのあるコンピュータも，真空管から発展して量子コンピュータの時代が視野に入ってきました．従来の数学的な暗号を破れる量子コンピュータに対応する暗号を構築しなければならない時代が来ています．これに伴い，研究者は全く新しい技術を習得しなければならないのです．一方で，私が追究している暗号プロトコルは応用分野も視野に入る位置にありますからこれまでの知見を活かせると考えています．

研究者としてのあり方と，後輩の研究者の皆さんへアドバイスをお願いいたします．

研究者とは野生生物のように，それぞれが全く違う個性を持ってそれぞれに意味や役割があり，研究コミュニティというエコシステムを確立させる存在だと思います．研究者の特性が画一化されていたらインスパイヤされないでしょうし，新しいものも生まれないのではないでしょうか．別の言い方をすれば，研究者どうしの刺激（専門性や成果）によって各研究者が準備していた何か（研究）に火が付く，影響を与え合う存在だとも思います．

若い研究者の皆さんには知識をギブアンドテイクしたときはすぐに借りを返そうとせず，短いスパン，狭い視野で考えず，物事を判断する際には拙速にならず，時間をかけることも忘れないようにしていただきたいです．私の好きな故事である「塞翁が馬」の解釈は，さまざまあると思いますが，私は「ロングスパンで物事を考えよ」という意味だと思います．時間的に長い目で物事を見て，横のつながりを広く持って物事を判断していけたらいいと思います．

技術革新によって自分が積み上げてきたことがリセットされる，世代交代が起きることは正直なところ，不安を感じることもあると思います．NTTの上席特別研究員は次世代を育成し，機会を与えることも仕事の１つなのですが，後進がどんどんと成果を上げて，つながりを築いていくことはとても喜ばしく思います．一方で，上席特別研究員には１人の研究者としての活躍も求められていますから，活躍する若い研究者が発表する成果もキャッチアップしていかなければいけません．若い研究者の活躍を目の当たりにして，「私はこの先，本当についていけるのだろうか」と不安になることもありますが，若い研究者と直接対決ではなくても，私の手掛ける研究分野とニーズと興味がうまく合致してくれたら，不安を乗り越えて活動していけるだろうと思います．私自身が若い研究者を励ます言葉は自分への励ましだと思っています．これからも，今の立場に胡坐をかくことなく常に挑み続けていたいです．

■参考文献

⑴ https://www.ntt.co.jp/news2017/1707/170727a.html