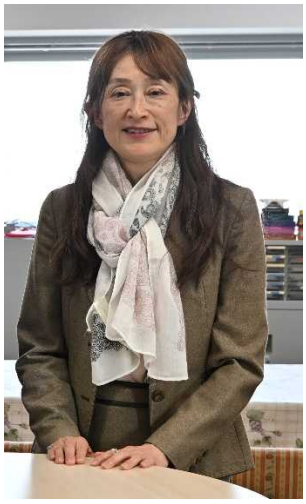
SCAT LINE テレコム技術の未来を拓く情報誌

INTERVIEW

# 大阪大学大学院工学研究科　宮地充子教授インタビュー



## 数学理論を活用して、量子計算機に対して安全な暗号基盤の実現を

情報セキュリティは、私たちの安心で安全なデジタル生活を支える重要な要素です。このうち、暗号技術は、情報セキュリティの基盤技術で、オンラインショッピング、コミュニケーションアプリなど、日常生活に深くかかわっています。そんな中、最近は量子コンピュータの開発が進展し、従来の暗号が解読される可能性が高まっています。そこで楕円曲線暗号の第一人者であり、ISO/IEC における数多くの国際規格のエディターを務めるなど、情報セキュリティ分野の発展に貢献されている宮地先生に、最近の暗号技術の動向と高度 IT 人材の教育プログラムについて、お話を伺いました。

## ID ベース暗号を応用して、ユーザビリティの高い安全な公開鍵暗号を開発する

**■研究者の道に入った経緯について教えてください。**

パナソニックの研究所で配属されたのが、セキュリティを研究していた部署でした。当時，世界的にも最先端の公開鍵認証局の日本の中での立ち上げのプロジェクトが始まり、その委員として参画し、公開鍵暗号を担当しました。委員会活動をするなかで、尊敬する先生よりお誘いがあり、大学に赴任することになりました。

**■研究が大きく飛躍したきっかけを教えてください。**

もともと海外に行きたいと思っていました。2001 年に文科省の在外研究員の申請に採択されて、カリフォルニア大学デービス校（UCD）に行くことになりました。ちょうどアメリカ同時多発テロが発生したときでした。UCD では以下のような研究ができました。

一般的に、セキュリティは何らかの安全性の前提が必要です。例えば、鍵は盗まれないというような前提を置いて、データを暗号化したり、署名を付けたりします。では、鍵が盗まれてしまったときにどうするかという議論がちょうどスタートしたところでした。鍵が漏洩して、全部の暗号文、あるいは全部のメッセージが偽造されてしまったら暗号の意味がない。それを防ごうという研究が始まりました。

一般的に鍵が漏洩すると、過去に作ったデータが見えてしまうとか、過去に作ったデータが偽造されることが問題となります。UCD では、そのような問題を防ぐ研究が始まっていました。解決策は、１つの鍵を持ち続けるのではなく、鍵を変化させていくことです。今使っている鍵が漏洩しても、過去に使った鍵を復元できないようにすることで、昔のデータは復号できないという考え方です。これが、前方秘匿性（Forward Secrecy）と呼ばれる概念です。その署名アルゴリズムや公開鍵暗号を作る研究が動いていました。また、過去の方向だけではなく、未来の方向においても安全にしたいと考えました。自分が持つ鍵を、携帯電話と、自宅 PC とに分けて入れ、両方が漏れない限り、未来の暗号文も未来の秘密鍵も漏洩しないようにして、安全性を高める研究に取り組みました。

**■そのような研究で工夫されたことはありますか。**

多くの人が使えるように利便性を確保する工夫が必要でした。例えば、鍵はある期間だけ使って全部捨てた場合にも、新たに相手に暗号化してもらうことを考えると、相手も自分もお互いに鍵が捨てられてしまっていては、どのように暗号化をしてよいか分からなくなってしまいます。復号化に必要な鍵は毎回変

えても、相手が暗号化するときの鍵は毎回変わると不便です。自分で復号化するときの秘密鍵は変化しても、相手が暗号化するときの公開鍵は固定する必要があります。
当時はうまくいかず、実現できない状況でした。しかし、転機がありました。ちょうど、ID ベース暗号が実現されたのです。ID ベース暗号は昔からセキュリティ研究者が作りたいと思っていた暗号です。通常、暗号化する鍵は、乱数でランダムです。その鍵で暗号化したデータを相手に送るのですが、単にランダムな鍵では幾つかの鍵がある場合に正しく相手本人のものかどうか分からなくなる問題が発生します。そこで本人と分かるような住所、名前、電話番号といったデータを暗号鍵に使うのが ID ベース暗号です。
ID が暗号化に利用する鍵となります。復号する鍵は秘密に自分が持っておきます。暗号化する鍵は公開された ID を使って、それを復号化する秘密鍵をもとめるという考え方ですが、そもそも公開されたデータから秘密鍵を計算できたら、暗号を解読されてしまいます。だから、このような ID ベース暗号の実現には高度なテクニックが必要で、ID ベース暗号が実現できない状況が続いていました。それが作れることになり、そのアイデアを応用することで、先述の、鍵が漏洩しても、過去のデータの解読はできず、また未来のデータも分からなくするために復号する鍵は更新し、一方で暗号化する鍵は固定できるようになりました。

## プライバシーを保護して不特定多数の人が利活用できる分散データベースを

**■その後、どのような研究に取り組まれているのでしょうか。**
大阪大学に来てちょうど 10 年になりました。楕円曲線の研究や共通鍵暗号の解読、また演算アルゴリズムの高速化、ブロックチェーンの研究、プライバシ、さらには AI セキュリティなど、研究室に 40 人弱の学生がいますので、情報セキュリティ分野を幅広く研究しています。情報セキュリティ分野は総合科学と呼ばれ、社会の変化や新たな技術の提案に沿って、新しい研究分野を切り開いてきました。例えば、AI セキュリティなども近年のトピックスです。
私は今、オープンサイエンスの実現に向け、データを安全に保護するための研究をしています。従来における研究内容の共有は、特定の人の間のやりとりが通常でした。決まった人に向けて暗号化しておくことで済んでいたのです。しかし、最近は、不特定多数の人がデータを使うようになってきました。例えば、AI を利用して回答を得るときは、様々な情報源から収集されるデータを利活用します。そのときに、データ保持者が自分のプライバシー情報を制御できる枠組みが必要です。データ保持者が自らプライバシー情報を保護しながら、AI で利活用できるようにする研究に取り込んでいるところです。

## 量子コンピュータの登場を見越して、利便性が高い耐量子暗号を目指す

**■耐量子暗号の研究にも取り組まれていますね。**
量子コンピュータが実用化されると、社会基盤となっている現在の暗号が解読される可能性があります。データを今収集し、将来解読する「harvest now, decrypt later」という脅威を最近よく聞きます。このような脅威に対応するために、耐量子暗号の研究にも取り組んでいます。
企業によっては、従来の暗号でなく、耐量子暗号に変えていく動きがあります。既に耐量子暗号に変えているところもあります。耐量子暗号では、安全性を担保するため鍵のビット長を大きくなります。但し、ビット長を大きくすると、その分暗号化処理の計算時間がかかります。暗号化処理を高速化する研究も重要になっています。
一方で、監視カメラやセンサーなどの IoT 機器は、多くの場所で日常的に使われ、これからももっと増えるものと思います。こちらも、暗号が解読されデータが偽造されてしまったら意味がありませんのでデータ保護は必須です。しかしながら、これらの機器は、消費電力の観点から、鍵のビット長があまりに大きい暗号を使えません。安全性と計算量のバランスが必要になります。耐量子暗号のような暗号を小さいセンサーに載せても意味がありません。センサーの電池がすぐに消耗してしまいます。この様に、用途に見合った暗号も求められます。

**■耐量子暗号が普及するには、利便性の向上が重要ですね。**
耐量子暗号を導入したために、今まで便利に使っていた機能が消えてしまうのではないかといった課題があります。従来の暗号方式で広く使用されている機能として、秘密計算（データを暗号化したまま加算しても、その計算結果を復号した値は、暗号化前のデータの計算結果と一致すること）があります。例えば、AI システムに暗号化したままデータを入力して、内部で足したり引いたりしても、復号化したら元の計算結果と一致するようにしたい。ここで、耐量子暗号にも、秘密計算できる方式はあるのですが、現状、演算回数に限界があるのです。耐量子暗号の世界においては、復号化した値が 2 や 3 などに明確に決まるのではなく、2.3 だから 2 とか、2.8 だから 3 など、曖昧な値から判断します。それゆえノイズが大きくなると、それぞれ 2.8 とか 3.1 などになって、どちらが 3 か分からなくなります。演算を重ねるごとにノイズが増えていくので、演算回数は例えば 10 回等に制限されてしまいます。いろいろな数学を使って、このような制約をなくす、等々、耐量子暗号の利便性を向上する研究に取り組んでいます。

## サイバー攻撃から社会を守る高度 IT 人材を育成する

**■高度 IT 人材の育成を目指す教育プログラム（enPiT）にも取り組まれています。**
enPiT は、数学やアルゴリズム、暗号や情報セキュリティの基盤技術から、情報セキュリティガバナンスや法制度、セキュリティ脅威の分析から、マネジメントまでカバーし、社会システムにセキュリティ技術を適用できる深い知識の獲得と現場知識の涵養を目指した教育プログラムです。（図１）　学部生向け、大学院生向け、社会人向けの３つのコースを用意しました。

私は、もともと教えるのがとても好きです。北陸先端大学院大学に在籍していたときは、公開演習形式で無償のサマースクールを運営しました。北陸先端大学院大学は学部がないので、様々な学生のバックボーンの学生が研究室に配属されます。授業だけでは必要な基盤技術をとてもカバーすることができません。そこで、事前知識なしに、集中的に座学と演習を学ぶような講義と演習を実施しようと思ったのです。せっかく教えるなら、学外の学生も受け入れるようにすると社会貢献にも繋がるなと考え、サマースクールを開講するようになりました。手探りのサマースクールでしたが、教えた学生がティーチング・アシスタントになって順調に回転するようになりました。

そして、大阪大学に移り、サマースクールの運用を考えるようになりました。自分の研究を通じた社会貢献にもなる無償のサマースクールですが、「受講者はお金を払ってもよい講義を受講するので、大切なのは無償ではなく、よい講義を提供できることでは？」という助言を頂き、有償の教育コースを開始するようになりました。そしてサマースクールはそのコースの１つの演習として提供するようになりました。民間の教育プログラムと比べると圧倒的に安いのですが、それでも下手な講義では受講者が来なくなります。講義の質を高めることができて、今ではよかったと思っています。

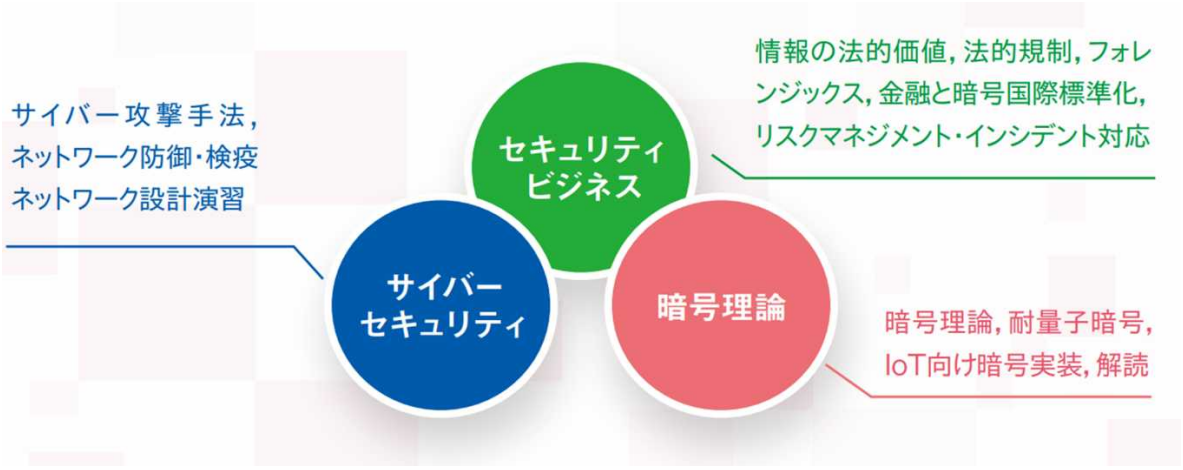



図１　教育プログラム enPiT のコースコンセプト

## 学会発表や論文投稿に SCAT 助成を活用する

**■研究費助成を受けて頂いて 20 年経ちましたが、SCAT の助成はどのようにお役に立ったでしょうか。**

申請書を書くときは、自分がこれから取り組む研究について熟考します。そのことが新しい研究トピックを見つける機会になりました。採択されたとき、「がんばろう」と意欲が湧いたことを覚えています。

また、助成金は、学会発表や論文投稿で役立ちました。あと、学生を学会発表に連れて行くこともできました。最近は、論文のオープンアクセスの費用の負担が高くなっていますので、この面でもとても助かりました。

**■数ある助成の中から、どのような理由で SCAT を選んだのでしょうか。**

大学に赴任してからというもの、毎年助成金を獲得する必要に迫られています。助成金は、助成対象の分野が異なると、採択されません。助成を受けた先生方を調べ、同じ分野の先生が受けていれば、大丈夫だと判断しています。そうしてセキュリティ分野の先生が採択されている SCAT を選択しました。

**■助成仕様で改善してほしいことはありますか。**

助成金の使用期間を柔軟に変更できるとよいかと思います。研究は長期的に続くので、助成期間が終わってから論文が採択され掲載されることもあります。その経費にも助成金を使えるとよいと思います。期間内に使うように求められると、助成で実施した研究の公表にかかる経費が期間後になることが多く、謝辞の記載も入れたいので、期間のフレキシビリティがあるとよいかと思います。

**■今後の助成活動に対する要望はありますか。**

助成金とともに、研究者が繋がる機会があるとよいかと思います。コロナ以前は、表彰式があり、初めてお会いする研究者の方々といろいろとお話しができました。その、助成後の例えば 10 年後に再び以前の皆様とお会いする場があるとうれしいです。助成時の研究内容とは変化しているでしょうが、どのように研究が花開いていったかのお話を伺うことは大切だと思います。さらに、そこで知り合った人との共同研究のきっかけになるかもしれません。

また、審査員と対話してコメントをいただく場があれば幸いです。採択されなかった場合にはフィードバックもできます。なお、採択された場合は、成果発表会を開くとよいと思います。審査員の方々からフィードバックをいただいたり、他の研究者の話を聞くこともできるので楽しいと考えます。

**プロフィール**

大阪大学大学院理学研究科修士課程修了後、パナソニック株式会社を経て、1998 年北陸先端科学技術大学院大学准教授、2007 年同教授、2002-03 年カリフォルニア大学デービス校客員研究員、2015 年大阪大学大学院 教授、2016 年から 2023 年独立行政法人 情報処理推進機構 監事、2024 年大阪大学大学院 栄誉教授、現在に至る。2000 年より ISO/IEC JTC1/SC27 でエディター、2017-2021 年より「成長分野を支える情報技術人材の育成拠点の形成（enPiT）情報セキュリティプロ人材育成短期集中プログラム」大阪大学拠点の代表を務めた。