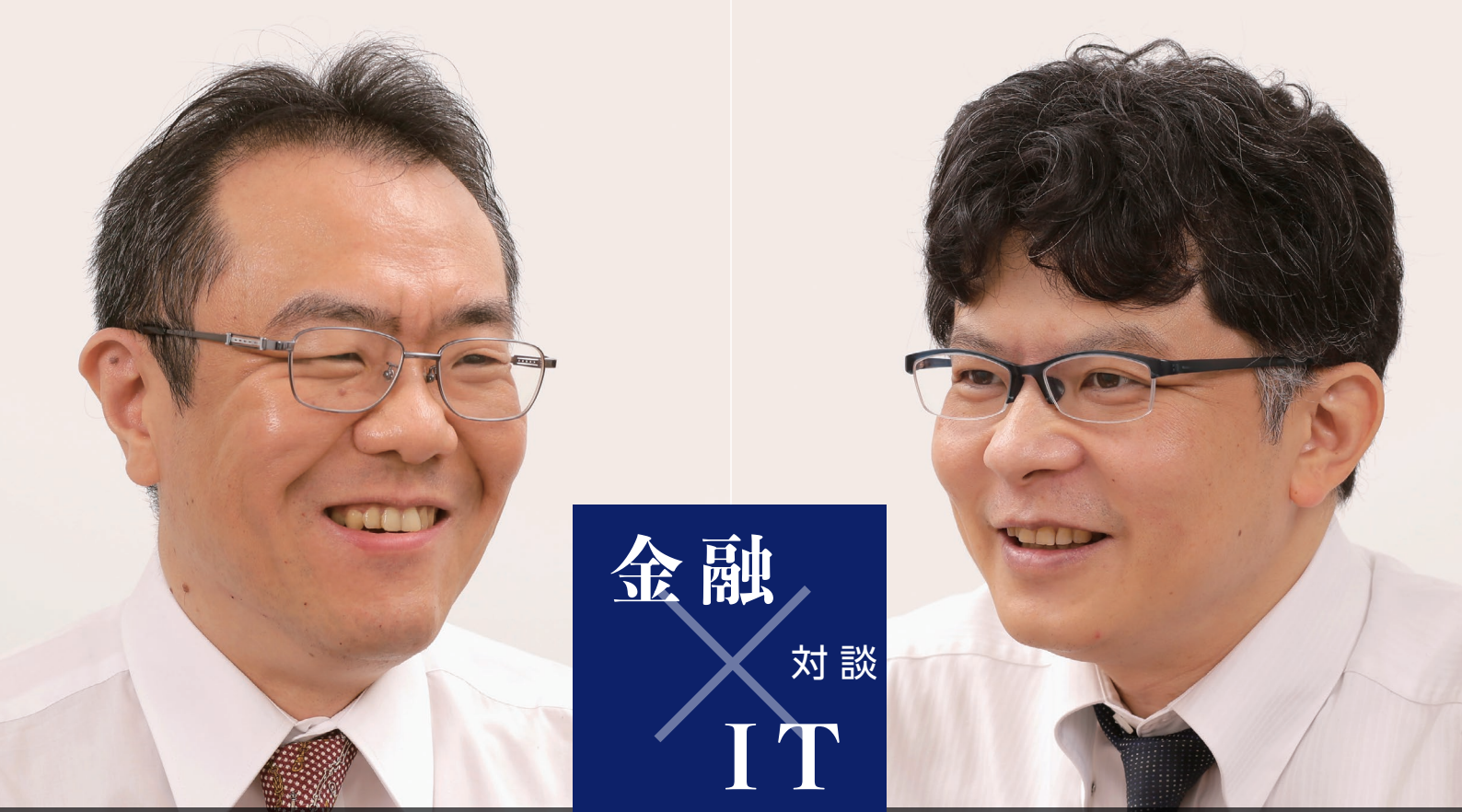


金融×IT 対談

花岡 悟一郎氏

産業技術総合研究所

サイバーフィジカルセキュリティ研究センター　首席研究員

Profile/Goichiro Hanaoka

1999年 日本学術振興会特別研究員（DC1）、2002年 同（PD）。2005年 産業技術総合研究所 入所。現在、同 サイバーフィジカルセキュリティ研究センター 首席研究員。博士（工学）。内閣府戦略的イノベーションプログラム（SIP）サブプログラムディレクター。平成30年度 科学技術分野の文部科学大臣表彰 科学技術賞（研究）他、受賞歴多数。

外園 康智

株式会社野村総合研究所

金融デジタルビジネスデザイン部　チーフリサーチャー

Profile/Yasunori Hokazono

2000年 野村総合研究所入社。企業向けデジタルコンサルティングおよび、言語処理・人工知能・暗号の研究とソリューション開発に従事。2018年・19年連続で、人工知能学会SWO研究会主催のナレッジグラフ推論チャレンジコンテストで最優秀賞受賞。2021年から23年 CRYPTREC（Cryptography Research and Evaluation Committees）高機能暗号委員。

AI時代の到来でプライバシー保護の問題がハイライトされる中、データを暗号化したまま計算できる「秘密計算」への社会の期待が高まっている。秘密計算はどのような社会ニーズに応えることができるのか。暗号理論研究の第一人者で暗号の社会実装にも尽力されている産業技術総合研究所の首席研究員、花岡悟一郎氏に語っていただいた。

暗号理論の研究はどのように発展してきたか

外園　花岡先生はこれまで三十年近く暗号理論の研究に携わり、これからも暗号の世界を背負っていかれるお立場にいらっしゃいます。まず、先生がこれまで暗号研究にどのように取り組んでいらっしゃったのかお話しいただけますか。

花岡　私が暗号の研究にかかわり始めたのは1997年で、大学院に進学してからです。幸運にも暗号への注目が急激に高まった時期でした。

　私がこの分野に入る直前くらいに、インターネットが一気に広まりました。それまで一般の人にとって情報通信と言えば電話をかけるくらいだったところにWindows 95が登場したのです。その結果、情報技術が広まり、ITバブルも発生しました。そういう時期でしたので、インターネット上の情報をどう守るのかにも関心が集まりました。

　暗号技術といえばどちらかというと政府機関や軍が機密情報を守るために使うものだったのが、一気に身近なものになりました。利用者の裾野が広がった分、暗号研究も急速に盛り上がってきたのです。

野村総合研究所　金融デジタルビジネスリサーチ部　©2024 Nomura Research Institute, Ltd. All rights reserved.

外園　暗号の方式が増え、かつ広く使われるようになったことで、国が設立した専門機関によって、暗号方式の選定や安全性評価が行われるようになりました。日本でもCRYPTRECがそうした責務を担っています。

花岡　そうですね。1993年には、三菱電機の松井充さんがアメリカの標準暗号だったDESを世界で初めて解読したというニュースもありました。そのようなこともあったため、DESの後継を選ばなければなくなり、非常に大きな話題となりました。私は学生時代に、DESの後継であるAESが選定されるプロセスをリアルタイムでつぶさに見ることができました。

外園　さらに、現在、一番普及している、RSA暗号でも事件がありました。

花岡　1998年には広く利用されていたRSA暗号の実装の一つに対してベル研究所のダニエル・ブライイヘンバッハーが選択暗号文攻撃（CCA）の適用可能性を示し、こうした攻撃への安全性を達成しないといけないという機運が高まりました。業界ではどうしたらCCA安全性を達成できるのかという研究が非常に盛りあがり、私はすっかりその魅力にとりつかれました。先端的な研究者が、全人類が使うべき公開鍵暗号の設計について侃々諤々議論し、ものすごい勢いで進歩していくのを間近で追いかけながら、自分もそれに近い領域の研究をいろいろやってみました。

外園　暗号を破るための研究と、安全性を向上させる研究の両輪のおかげで、暗号の安全性は高まり、インターネット上の商取引システムやメールなどのインフラになっているということですね。

花岡　そうです。一方で、私の学生時代が終わる頃には、共通鍵暗号も公開鍵暗号も基本的な部分は研究し尽くされた感じになってきました。そんな時、2001年に、マット・フランクリンとダン・ボネーという二人の研究者がIDベース暗号を提案します。私は「これは今後絶対重要になる」と感じました。IDベース暗号はまだ出てきたばかりでしたので、集中して勉強しました。

IDベース暗号とは、利用者の住所、氏名、メールアドレスなど公知の情報を公開鍵として利用する暗号方式で、その利便性から注目度が高まりました。IDベース暗号のように、従来の暗号技術にプラスアルファで何か高度な機能を持つ暗号技術の総称を高機能暗号と言います。

秘密計算の社会ニーズ

外園　従来の暗号は基本的には、二者ないし複数の主体が安全に通信するためにありますが、高機能暗号はそれを超えるものです。先生は、その中でも、データを暗号化したまま計算できる「秘密計算」の分野に取り組まれていらっしゃいます。この分野に取り組もうと思った動機を教えてください。

花岡　2001年頃から高機能暗号が急速にブームになり、多くの研究者から、いろいろな種類の高機能暗号が出てきました。私も含めて暗号研究者の多くは「これだけよいものなのだから、だまっていても社会でどんどん使われるだろう」と考えていたのではないかと思います。

ところが、実際は必ずしもそうはなりませんでした。10年くらい前からはそうした楽観的な考え方では駄目で、社会ニーズとのすり合わせこそが大事なのではないかと考えるようになりました。われわれが提供できそうなことと社会的ニーズをすり合わせた結果、一番役に立てそうなのが秘密計算の分野なのではないのかと考えたわけです。

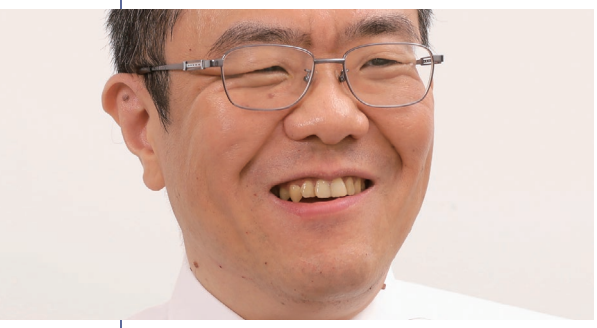
外園　研究と社会ニーズのギャップを埋めることが大事だということですね。先生が注目された秘密計算の社会ニーズとはどのようなものでしょうか。

花岡　ディープラーニングが登場し、世の中がAIで盛り上がり始めたときに、「AIを使ったら何でもできそうだけれども、本当にどんな情報も入れてしまって大丈夫なのか？」とAI利用に伴うプライバシー保護の問題がハイライトされるようになりました。そのおかげでAIを安全に利用するための暗号技術が世の中で注目されるようになりました。秘密計算は入力情報を隠したままデータ処理をする技術ですので、社会の期待が一気に高まったわけです。

外園　秘密計算の適用先はどのような分野でしょうか。

花岡　秘密計算の使い方は大きく分けて2つあると思います。

一つは、自分の個人情報を隠したまま分析にかけてもらい、その結果だけをもらうような使い方です。自



分の遺伝子情報を検査機関に隠したまま自分がどういう疾病リスクを持っているのか結果だけ返してもらう、というのは一例です。

企業が何を調べようとしているかを隠したまま、関連する情報を外部から得るというのも、この使い方にあたります。たとえば、企業が素晴らしいアイデアを思いつき、そのアイデアを進めていくにあたってそれに関連した情報等がどうなっているか知りたいと考えたとします。こうしたケースでは、質問をすることで自分のアイデアが伝わってしまう可能性があります。秘密計算を活用することで、アイデアを隠すことができるわけです。

外園　自分の情報を秘匿したまま、分析や検索の依頼ができますね。

花岡　もう一つの使い方は、複数の会社が互いに情報を出し合うと非常によいデータ分析ができる場合などに、互いに情報を見せ合うことなくデータ分析の結果だけ出す、というものです。A社はある人の行動履歴を持っている、B社はその人の保有資産がわかっている、といったケースでは、こうした秘密計算の使い方が有効です。

今述べた2つの使い方は、どちらも医療、金融、それから材料などの開発分野で、特に効果を発揮するのではないかと思います。

秘密計算の技術を直観的にわかりやすく説明するには

外園　先ほど、先生は社会ニーズに合わせて秘密計算に取り組んでいる、とおっしゃっていました。ただ、暗号化したまま計算できるというのは、一般の人たちには直観的にわかりづらいところがあるように思います。そのことは社会実装を進める上で障害となるのではないでしょうか。

花岡　おっしゃるように情報が隠されたまま計算できると言っても不思議に感じるという声をよく聞きます。

秘密計算には主に、秘密分散方式と準同型暗号方式などがあります。秘密分散に基づく計算の原理を簡単に説明すると次のようになります。

例えば8＋6を考えます。このとき、まず8は3と5に分けます。3だけを見ても、もう一方の5がわからない限り、もとの数字8は分かりません。また、6も2と4とに分けます。そして、3＋2、5＋4は別々に計算します。

つまり、もとの数字がわからないまま、2つの組にわけて計算をすることができます。最後にこの2つの計算結果を合わせると欲しかった14が出てきます。このように足し算は比較的簡単ですが、掛け算も工夫で可能となります。

このように秘密分散に基づく秘密計算では、秘密の情報を2つ以上に分割するのですが、（1）分割したときに、もう一方の情報がわからない限りもとの情報はわからない、（2）その状態のままどんどん計算ができる、という2つの原理でできているのです。

ここで問題なのは、こういった技術的説明を聞いてわかった気になったとしても、すぐにぜひ使いたいとまで思う人ばかりではないということです。「これなら自分の個人情報を預けても安心だ」とはならず、漠然としたどこか気持ち悪い感覚が残っている方が普通なのです。

外園　原理的には、情報を分割したまま計算するから外に情報が洩れないのは分かっても何か腑に落ちないわけですね。

花岡　そうです。私は高機能暗号の社会実装を自分に与えられたミッションだと思っています。何か新しい技術を世に出したいと考えたときには、技術が優れていることも重要ですが、それに劣らず「使ってみたい」と思ってもらえるような上手な説明をすることも重要だと考えています。

そして暗号についてよい説明手法を考えること自体を新しい研究領域として取り組んでおります。先ほど説明した秘密計算の理屈については、「視覚秘密分散」という手法を用いて視覚的に表す説明方法を検討しました。視覚秘密分散を用いると、1枚ずつ見ると何の意味も持たない2枚の画像が、重ね合わせると秘密の画像が浮かび上がります。

外園　2枚のシートから、NRIのロゴが浮かび上がる仕組みを作っていただきました。

花岡　以前は、企業に秘密計算の技術を紹介しに行っても、多くの方が狐につままれたような顔をされてい

野村総合研究所　金融デジタルビジネスリサーチ部　©2024 Nomura Research Institute, Ltd. All rights reserved.

ました。ですが、視覚秘密分散を営業ツールとして使うようになってからは、かなり手応えを感じられるようになりました。

われわれは、この手法をさらに発展させて、視覚的な秘密計算を実現し、それをわかりやすいユースケースシナリオで使って見せるショートストーリーの動画を作成しました[1]。

外園　私も拝見しました。ストーリーと解説の動画では、マッチングしたペアの数だけわかり、それ以外の情報が一切漏れない仕組みが視覚的に説明されていました。

視覚秘密分散は、言葉で説明してもわかりにくいので、ぜひこの動画を見ていただきたいです。

人間の「情報を出したい」という欲求に応える高機能暗号

外園　政府は目指すべき未来社会の姿としてSociety 5.0を掲げています。安全な社会を構築していく上で暗号はその基盤になり得るのではないかと思います。

先生は、暗号の社会実装に尽力されています。今後、高機能暗号の技術がさらに進化していくと、社会はどのような恩恵を受けられると考えていらっしゃいますか。

花岡　セキュリティ技術と言えば、これまでは自分の情報を「いかに守るか」という文脈で語られることが多かったと思います。しかし、そうした傾向は、徐々に、自分の情報を「いかに出すか」に力点が移ってきているところではないかと思っています。

「情報を守りたい」という人間の欲求の裏には「情報を出したい」という欲求もおそらくあるはずです。高機能暗号を利用することで、出したい情報や出しても構わない情報だけを出して、守りたい情報はしっかり守る、という絶妙なバランスを取れるようになるのではないかと思います。

外園　「情報を出したい」という人間の欲求を満たすには、一方でうまく暗号で守られている必要があるということですね。

花岡　そうです。

そうした「情報を出したい」という欲求は人間の私利私欲だけではないと思います。人間は群れ社会でずっと生きてきたので、おそらく本能的に、自分の持っている情報を他の人に使ってもらえれば嬉しいと感じるのだと思います。そうした本能を抑圧されない世の中はどうなっているのか見てみたいです。

外園　AIが学習するコンテンツはインターネット上では、すでに枯渇しつつあります。個人や企業内の誰かが情報を出していかないと、AIはこれ以上賢くならないわけです。そういう意味でも、コントロールしながら情報を出すことができる秘密計算などの暗号技術は大事だと思います。

最後に、先生がたが研究された暗号を社会実装していく上で、そうした技術を利用する企業側に何か期待することはありますか。

花岡　われわれが暗号技術について利用者である企業の方にお話しさせていただく際に、各企業に暗号担当のインターフェイスとして専門家である「ソリューション・アーキテクト」ともいうべき方がいらっしゃると非常によいなと思っています。

外園　ソリューション・アーキテクトは、システム設計ができ、かつ暗号技術もある程度わかっている必要があります。両方の専門性を持つとなるとなかなか厳しいですが、そうした人材の育成は企業の暗号技術の利用を促進する上でカギを握りそうですね。

花岡　私はそうした分野を横断したソリューション・アーキテクトの果たす役割は今後ますます重要になると思っています。ただ、われわれが押し付けるような話ではないです。各企業にそういう人を置く重要性を認識していただけるよう、技術を提供するわれわれ暗号研究者ががんばらなければいけない、と強く感じています。

外園　暗号はすでに社会にとって重要なインフラですが、さらに、先進的な暗号技術によって、よりスマートな社会になることが期待できそうです。

本日は貴重なお話をありがとうございました。

（文中敬称略）

1) PRIVATE MATCHING -視覚化された秘密計算-
https://www.youtube.com/watch?v=vikGJEIU5UU
PRIVATE MATCHING -視覚化された秘密計算-（解説編）【産総研公式】
https://www.youtube.com/watch?v=kIY0kVBIh_g