ISSN 0915-2318 平成2年3月5日第三種郵便物認可
令和5年5月1日発行　毎月1回1日発行　第35巻第5号（通巻410号）

NTT 技術ジャーナル

5 MAY 2023
Vol.35 No.5

特集

量子計算機時代を見据えた暗号研究の最前線

NTTデータ 先進技術特集

トップインタビュー

冨安　寛
NTTデータ　執行役員 技術革新統括本部長

グループ企業探訪

NTT EDX

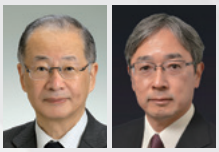
from NTT西日本

オープンイノベーションによる未来共創プログラム『Future-Build』で社会課題解決・未来社会創造に挑戦した6プロジェクトの成果報告

NTT
技術ジャーナル

5 MAY
2023
Vol. 35 No. 5

CONTENTS



NTT技術ジャーナルはWebで閲覧できます.
https://journal.ntt.co.jp/

本誌掲載内容についての
ご意見,ご要望,お問い合わせ先

日本電信電話株式会社
NTT技術ジャーナル事務局
E-mail　journal@ml.ntt.com

本誌ご購読のお申し込み,
お問い合わせ先

一般社団法人電気通信協会
ブックセンター
TEL (03)3288-0611
FAX (03)3288-0615
ホームページ　http://www.tta.or.jp/

企画編集
日本電信電話株式会社
〒100-8116　東京都千代田区大手町1-5-1
大手町ファーストスクエア　イーストタワー
NTTホームページ　URL https://group.ntt/jp/

発　行
一般社団法人電気通信協会
〒101-0003　東京都千代田区一ツ橋2-1-1如水会ビルディング6階
TEL (03)3288-0608　FAX (03)3288-0615
URL http://www.tta.or.jp/

/ト/ッ/プ/イ/ン/タ/ビ/ュ/ー/

View from the Top

NTTデータ
執行役員
技術革新統括本部長
冨安　寛

PROFILE：
1990年NTTデータ通信に入社．2007年NTTデータ 技術開発本部部長，2011年ソフトウエア工学推進センタ長，2015年技術革新統括本部 基盤システム事業本部 システム方式技術部長，2017年技術革新統括本部 システム技術本部長を経て，2020年6月より現職．

「今これをやらなきゃダメだ」という強い信念を持てるか．めざすはGlobal No.1の技術力の実現，お客さまへの提供価値の最大化

情報技術をもって新しい「仕組み」や「価値」を創造し，より豊かで調和のとれた社会の実現に貢献するNTTデータ．新中期経営計画では5戦略を携えて，投資と成長の好循環を確立し，Global 3rd Stageに向けた事業成長の実現をめざしています．この目標を技術面で率いる冨安寛NTTデータ技術革新統括本部長に具体的な技術戦略とトップとしての信条を伺いました．

技術部門のヘッドクォーター・技術革新統括本部を率いる

NTTデータの技術戦略についてお聞かせいただけますか．

NTTデータはここ数年で世界各国に19万人の社員を擁するまでに成長したグローバル企業です．2022年度から2025年度の新しい中期経営計画において，Global 3rd Stageの到達に向けて，ITサービスプロバイダとしてGlobalトップ5入りをめざして取り組んでいます．これまでGlobal 1st StageにおいてGlobalカバレッジを拡充し，Global 2nd Stageにてグローバルブランドの確立を図り，Global 3rd Stageでは，「変わらぬ信念，変える勇気」によってGlobalで質の伴った成長をめざしてきました．そして，Global 3rd Stageの到達に向けた新中期経営計画として，さまざまな人々をテクノロジでつなぐことで，未来に向けた価値をつくり，お客さまとともにサステナブルな社会の実現をめざして，「ITとConnectivity の融合による新たなサービスの創出」「Foresight起点のコンサルティング力の強化」「アセットベースのビジネスモデルへの進化」「先進技術活用力とシステム開発技術力の強化」「人材・組織力の最大化」の5戦略で臨んでいます．

私の率いる技術革新統括本部は米国や欧州に点在する技術部隊のヘッドクォーターの役割を担い，Global No.1の技術力の実現，お客さまへの提供価値の最大化を掲げた技術戦略により，先進技術の活用，お客さまの課題解決を実現する共創R&Dなどをとおして，今使える技術だけではなく今後普及していく技術の見極

め・活用することに，いち早くGlobal全体で取り組んでいます．特に，中期経営計画の5戦略においては「アセットベースのビジネスモデルの進化」と「先進技術活用力とシステム開発技術力の強化」に注力し，その実現に向けて技術注力領域を定めるとともに，高い生産性とデジタル時代にふさわしいアジリティを持つシステム開発を実現する技術を独自に開発してGlobal共通アセットとして提供し，そして，その価値を継続的に提供していくために技術力の高い人材の活用を進めています．

5戦略のうち，2つを担うとは大役ですね．ビジネスモデルの進化には注目が集まりそうです．

私たちのビジネスモデルは従来，お客さまのご要望に応じてシステムの開発を行うスタイルの，いわゆるSI（System Integration）でした．お客さまからのRFP（Request for Proposal：提案依頼書）を受けて提案する営業活動を行い，それぞれのRFPに対して，オーダーメイドとして一点もののシステム開発を中心に行ってきました．

この従来型SIから，これまで培ってきた顧客理解と高度な技術力でシステムをつくる力と，さまざまな企業システムや業界インフラを支え，人と企業・社会をつなぐ力を存分に発揮するために，アセットベースのSIへシフトします．

その背景にはIT人材の確保と，刻々と変化する環境やお客さまのご要望への迅速な対応という2つの課題があります．IT人材不足の解消については，従来型のSI業態のまま売上を拡充するためには大量の人材を抱えるプロジェクトを数多く実施しなくてはなりません．しかし，依然，IT人材の獲得競争は世界的に過熱している状況下にありますから，大量の人材が確保できるとは限りません．このため，「個別につくらない開発」の実現が重要になりますから，私たちはグローバルレベルでグループ内の技術や知見，経験などをアセット化して，それらをマルチリージョン，マルチインダストリで有効活用するスタイルをめざすことにしました．

迅速な対応については，デジタル技術の活用によってビジネススピードが急激に加速している中，従来型SIのスピード感ではそれについていけないため，アセットを活用して自ら提案し，発信するビジネスモデルへと進化させて，デジタル時代にふさわしいビジネスアジリティを備えて，お客さまへの提供価値を最大化していきます．

さて，アセットといってもさまざまなものがありますが，ここでは，業界や業務のフォーサイト，ベストプラクティス，ソフトウェア，自社ツール等の再利用可能なもののことです．そのうち，私たち技術革新統括本部はグローバル共通のテクノロジアセットの創出を担い，グローバルに技術注力領域を定めて，各領域で業界に依存しないテクノロジアセットを開発します．各領域での「売上規模拡大」「技術者数増加」「パートナーアライアンス強化によるエコシステムの実現」によって，Global No.1の技術力の獲得をめざし，その技術力を活かして，アセットベースのビジネスへの変革を加速させています．

技術開発活動をEGM領域に再構成

技術の活用力や開発技術力もさらに強化されるのですね．

これは私たちの技術をビジネスにつなげていくための非常に重要な戦略で，将来の競争力獲得に向けた先進技術の活用力と生産性の向上に向けたシステム開発技術力を強化するものです．まず，これらを技術の成熟度に応じてEGM（Emerging，Growth，Mainstream）の3つのフェーズに分けて，フェーズごとに技術獲得をめざす研究開発・技術開発活動に再構成しました．

Emergingフェーズは5年から10年後を想定した先進技術探索と，お客さまとともに新しい技術による価値創出を検討する共創R&Dを担います．そして，Growthフェーズでは3年から5年後の成長事業，技術注力領域を形成するための技術開発，テクノロジアセットの創出とビジネス検証に加えて技術者の育成も実施します．EmergingとGrowthフェーズにおいてはテクノロジアセットの整備を本格的に始動し，技術起点でグローバルビジネス拡大を実現していきます．また，新たな社会価値創出の重点施策テーマとして，IOWN（Innovative Optical and Wireless Network）については，要素技術の研究開発を推進するNTT研究所と連携し，研究成果をお客さまに展開・事業化できるように共通テストベッドの開発や，社会変革パートナーとの共創R&Dを実施するデジタルツイン共創プログラムも展開しています．

そして，Mainstreamフェーズでは現行の事業向けに技術注力領域でテクノロジアセットを開発し，グロー

バル戦略を統一して日本，米国，欧州３極での事業展開，デリバリーリソースの拡大，市場シェア拡大を推進します．主な技術注力領域としては，多様なクラウドサービスを活用したシステム開発を実施する「クラウド領域」，デジタル技術を活用したアジリティの高いシステム開発とさらなる生産性を追究する「ADM（Application Development and Management）領域」，従来の境界型の防御ではなく，ゼロトラストの考え方に基づくセキュリティサービスに注力する「サイバーセキュリティ領域」，そして，AI（人工知能）を利用したデータ分析と活用によって新たなビジネス価値の創出に挑む「D&I（Data & Intelligence）領域」の４領域があります．

技術革新統括本部の再編成はNTTデータのビジネス変革の旗印のようですね．

旗印というよりも「試金石」だと考えています．冒頭でもお話ししましたが，NTTデータは全世界に19万人の社員を擁する企業に成長しました．この成長過程ではM&Aを行っており，各社のビジネススタイルの違い，各国の商習慣やビジネスプロセスの違い，お客さまの特性やニーズの違いがあります．これらを共通化，場合によっては統合し，戦略的にNTTデータのアイデンティティを築いていくにあたって，各リージョンでそれぞれ異なるお客さまのニーズに適応できるよう調整していかなければなりません．これには相当な時間がかかることはいうまでもありませんが，ある意味で技術は世界共通ですから統一しやすいこともあり，技術戦略を先行して共有化したのです．

もちろん，初めてのことですから上手くいかないことも当然のごとくあります．そこで，事業計画に関してはスピード感を持って実行しつつ，必要に応じて修正するというやり方に変えて，各国の幹部とともに３カ月ごとにその実施状況により計画を見直しています．常に目を光らせて３カ月ごとに大修正ですから，私自身にも経過に一喜一憂するゆとりもありません．「夢中で取り組む」の繰り返しが後の「良かったな」につながっていくととらえて仕事をしています．

ところで，この見極めに際して，通常の指標に加えて，そのプロジェクトが「多忙な状況にあるのか」もポイントの１つとしています．「大変だ，大変だ」と言いながら全力で向き合ってきた仕事を後から振り返ってみたとき，「あれは面白かった．充実していた」と感じたことがあるかと思います．私自身にもそのような経験もあって，今まさに夢中になって取り組めているかどうかも見極めの際には考慮しています．

熱意を持って「人」を育てたい

本部長が仕事をする際に大切にしていらっしゃることを教えていただけますか．

私が入社したのは1990年です．研究開発の仕事からスタートし，画像認識の研究開発を10年程度続けてきました．しかし，手掛けていた画像認識は時代背景や将来性等のさまざまな判断から断念することとなり，金融システム関連の部署へと異動となりました．

この経験から得た教訓があります．それは，惰性でプロジェクトを継続してはいけない，タイムリーに撤退や軌道修正をかけるための強い信念を持つことが重要である，ということです．NTTデータはいまや19万人の社員を擁するグローバル企業ですから，惰性で仕事していてはこの19万人があらぬ方向へ進んでしまいます．だからこそ，NTTデータのグローバル一体化に向けた明快な技術戦略を世界各地の技術者と共有し，信念を持って変革を推し進めているのです．

それから，開発している技術はお客さまに受け入れられるものであるか，人気を集めそうなものであるかという目利きも重要です．フロントラインの社員がお客さまと直接コミュニケーションを図る中でつぶさに見た課題に対応できる技術を開発し，フロントラインの社員が「これで課題を解決できます」と自信を持ってお客さまに提案できるものをつくることが大事なのです．

ややもすると，技術者は現場からの距離が遠くなりがちで，その状況において自らの発想を起点にした開発に終始し，成果をお客さまに提案することがあります．こういうプロセスで開発したモノは残念ながらお客さまに受け入れられないことが多くなります．こうしたことから，私はタイムリーにフロントラインや現場の判断を大切にしたいと考えています．

現場や現場の方々の考えを大切にされるのですね．最後に，社内外の皆さんに一言お願いいたします．

私は熱意を持って「人」を育てようと努めています．人を育てるのに大切なのは，その人がどういう人であるか，どんなセンスを持つ人かを見極める力です．なぜならば，すべての人が同じタイミングやスピードで育つわけではありません．また，伸びる傾きも違えば，センスも違います．その人の個性に合った仕事を与えられるかどうかがトップの手腕だと考えています．育てたいと思うその人にとって難しすぎないか，簡単すぎないかといった点に合わせて個性を見極めることを常に念頭に置いています．

パートナーの皆さん．人材獲得は世界的にも熾烈な戦いを強いられています．マスコミではGAFA等のレイオフが報じられていることから，ICT人材はすでに飽和状態であると思

わるかもしれませんが，実体は違います．ICTの変化はめまぐるしく，そこに求められる人材像も変わってきており，それに対応できる人材獲得競争が起きているのです．また，さまざまなAIの登場から，将来的にコンピュータシステムはすべてAIにとって代わるのではないかと想像しがちですが，動かしているのは「人」ですし，コンピュータシステムやソフトウェアはこの先も必要です．だからこそ，今後も「人」が大切になります．私は社内の人だけではなく，パートナーの皆さんも責任を持って育てたいと考えていますので，ぜひ一緒に仕事をしていきましょう．

そして，お客さま．私たちの技術レベルの高い社員が皆様のご要望におこたえいたしますので，ぜひ私たちを採用してください．

最後に若い技術者の皆さんは「寝食を忘れる」という言葉のごとく，技術の勉強に没頭していただきたいですね．ソフトウェアやコンピュータシステムの技術は「使われてナンボ」ですから，チャンスがあれば若いうちに現場で経験を積んで，技術者として一回り大きくなってください．

（インタビュー：外川智恵/撮影：大野真也）

※インタビューは距離を取りながら，アクリル板越しに行いました．

インタビューを終えて

「冨安本部長はとても気取りのない方です」という評判どおり，インタビュー会場は5分に一度，笑いが起きるほど和気あいあいとした雰囲気に包まれました．というのも，冨安本部長は技術戦略やトップとしてのご方針を語る際，「第三者からはこんなふうに見えることもあるかもしれない」という客観的視点を添えて，ユーモアを織り交ぜながらお話をされるのです．客観的視点は時にクリティカルシンキング（批判的思考）であるため辛口に聞こえます．しかし，ユーモアを添えられて発せられるせいか耳障りではなく，誠実さを帯び，お話を伺った後もその発言の真意を反芻したくなりました．

そんな冨安本部長のご趣味は釣りで，「釣りは男性に孤独を感じさせない趣味だから」とか．おひとりの時間はどんなことをお考えになられているのか，冨安本部長が紹介してくださった一冊の本，『夜と霧』（V.E.フランクル 1945）に垣間見ました．「壮絶な人生を描きつつ，筆者は心理学者・精神科医として“頑張った”とか“戦い抜いた”だけではなく，冷静な視点で現状を分析し，記録を残しているんですよ」と冨安本部長．まさにウォームハートとクールヘッド．冨安本部長の絶妙なバランス感覚を感じたひと時でした．

NTTの研究所で獲得したスピリットを胸に，人類の発展に寄与するため「世界」に挑み続ける

東北大学　特別栄誉教授　中沢正隆博士
国立研究開発法人情報通信研究機構　主席研究員/NTTエレクトロニクス　フェロー　萩本和男氏

提供：国際科学技術財団

NTTの研究所に在籍されていた中沢正隆博士，萩本和男氏が，2023年Japan Prize（日本国際賞）を受賞されました．光信号を光のまま増幅する小型な光増幅器の実現と，それを利用した大容量の光通信システムへの貢献が評価されたものです．お二人は現在のグローバルなインターネット社会を支える基幹技術である「長距離・大容量光データ通信」への道を拓き，NTTが提唱するIOWN（Innovative Optical and Wireless Network）構想にも通ずる重要な業績を残されました．受賞を記念して，東北大学特別栄誉教授 中沢正隆博士と国立研究開発法人情報通信研究機構 主席研究員 萩本和男氏にお話を伺います．

中沢正隆博士
略歴：1980年日本電信電話公社入社．電気通信研究所，1984年マサチューセッツ工科大学客員研究員，1999年NTT R&Dフェロー，2001年東北大学電気通信研究所教授，2008年東北大学ディスティングイッシュトプロフェッサー（DP：卓越教授），2010年東北大学電気通信研究所長，2010年東北大学国際高等研究教育機構長，同先端融合シナジー研究所長，2011年国立大学付置研究所・センター長会議会長，2011年東北大学電気通信研究機構長，2018年同特任教授，2018年国立大学法人金沢大学理事（非常勤）（現在に至る），2022年東北大学災害科学国際研究所特任教授，DP．2023年東北大学特別栄誉教授（現在に至る）．
主な受賞歴：1989年桜井健二郎氏記念賞（萩本氏と共同），1994年電子情報通信学会業績賞(萩本氏と共同)，1997年科学技術庁長官賞（研究功績者賞），2002年 IEEE Daniel E. Noble Award，2005年OSA R. W. Wood Prize，2008年総務省志田林三郎賞，2009年産学官連携功労者表彰内閣総理大臣賞（萩本氏と共同），電子情報通信学会功績賞，2010年紫綬褒章，応用物理学会光・量子エレクトロニクス賞，IEEE Quantum Electronics Award，2013年日本学士院賞，2014年OSA Charles H. Townes Award，2015年藤原賞，河北文化賞など．

萩本和男氏
略歴：1980年日本電信電話公社入社．横須賀通信研究所研究員，1994年NTT伝送システム研究所グループリーダー，1998年NTT長距離通信事業本部担当部長，2000年NTT未来ねっと研究所研究部長，2005年同所所長，2009年NTT先端技術総合研究所所長，2013年NTTエレクトロニクス 代表取締役社長，2019年同社フェロー（現在に至る），2021年国立研究開発法人情報通信研究機構主席研究員（現在に至る）．
主な受賞歴：1989年桜井健二郎氏記念賞（中沢氏と共同），1991年IEE Oliver Lodge Premium，1994年高柳健次郎記念奨励賞，1994年電子情報通信学会業績賞(中沢氏と共同)，2006年電子情報通信学会業績賞，2007年前島密賞，2008年IEEE Fellow，2009年科学技術分野の文部科学大臣表彰科学技術賞，2009年産学官連携功労者表彰内閣総理大臣賞(中沢氏と共同)，2013年電子情報通信学会功績賞，2016年紫綬褒章．

エレクトロニクス・情報・通信分野において9年ぶり．日本人研究者の受賞

―Japan Prizeの受賞，おめでとうございます．受賞を知ってお二人ともとても驚かれたと伺いました．

中沢：大変嬉しく存じます．実は，自分が受賞したとはにわかに信じられませんでした．というのは，私はさまざまな賞の選考委員を務めていることもあり，2022年秋から冬のはじめあたりにJapan Prizeの事務局から電話があったということを聞いたときに，てっきり「選考委員になってください」という話だと思いました．

ところが，その後，Japan Prizeの理事長からご連絡をいただき「中沢博士が受賞されたのです．（賞を）お受けいただけますか？」と．本当に驚きました．受けるも何も受賞したことを信じられずに「本当ですか？大変うれしく思います」とお答えしました．萩本さんも同じだったのではないですか．

萩本：はい．Japan Prizeは非常に高名な方々が受賞されています．そのメンバーに私が加わってもよいのか，という驚きのほうが勝りました．連絡いただいたのは確か11月に入ったころだったと思います．実は，私もちょっとした行き違いがありまして，受賞の喜びを実感するまでに遠回りをしたのです．事務局側から，私がBeyond 5G研究開発促進事業プログラムディレクターを務めている情

提供：国際科学技術財団

報通信研究機構（NICT）宛にご連絡をいただき，在宅勤務だったので伝言をいただいても，よく分からず，「もしかしたら怪しい電話かもしれない」と警戒しながら，Japan Prizeに関するものだと分かるのに時間がかかりました．元東京大学総長の小宮山宏 国際科学技術財団理事長から改めてお電話いただけるとのことでしたので，中沢さんと同様に選考委員のお話かと思っておりました．しかし，「理事長からわざわざご連絡いただけるなんて，もしや…何かの受賞？」と一瞬よぎりましたが「ありえない話だ」と思っていました．

中沢：Japan Prizeを受賞するというのは，それくらい信じられない話なのですよ．Japan Prizeは分野検討委員会が翌々年の授賞対象となる２分野を決定し，毎年11月に発表します．同時に世界約15,000人以上の推薦人による推薦と，科学技術面での卓越性，社会への貢献度なども含めた総合的な審査が厳格に行われるのです．

また，過去に何度かノミネートしていただいたと耳にしたことがありますが，私たちは何かを受賞するために研究をしているわけではありませんから，ノミネートされたことも忘れていました．それ故，情報通信のかたちをグローバルに変えたことを評価されたことは何よりも嬉しいことです．

―お二人はどのようなご関係なのですか．そして，同じ分野の研究を手掛けることになったきっかけを教えていただけますでしょうか．

中沢：私たちは同じ年にNTT（当時電電公社）に，私は博士として，萩本さんは修士として入社しました．

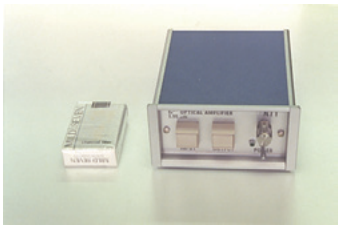
萩本：採用面接等の際に初めて顔を合わせて，実は同じ大学出身だと分かりました．学年が違い，顔を合わせたこともなかったのですが，それ以来懇意にさせていただいています．

中沢：新入社員研修後に私は茨城電気通信研究所（当時）に配属になり，光通信において光ファイバが切れた部分を特定する技術の研究を，そして，萩本さんは横須賀電気通信研究所（当時）で光ファイバを使った伝送システムの研究に取り組みました．

萩本：象徴的なのは受賞のきっかけとなったエルビウム添加ファイバ増幅器（EDFA：Erbium-Doped Optical Fiber Amplifier）について1989年に中沢さんと連名でOFC（光ファイバ通信国際会議）に報告した論文ですね（**図１**）．中沢さんのファイバ仲間から，半導体励起エルビウム添加ファイバ（EDF）で利得が取れるという話を聞き，1988年の年末から年始にかけてEDFを使って光増幅実験の準備を始めました．かなりの突貫工事です．OFCの締め切りまで，２週間ぐらいしかありませんでしたし，世界で初めてのファイバ増幅器による伝送実験でした．

半導体レーザ励起光増幅器の開発を中心とする光ファイバ網の長距離大容量化への顕著な貢献

―それではJapan Prizeを受賞された功績を伺います．授賞理由を拝見しますと，「半導体レーザ励起光増幅器の開発と実用化を中心に，波長分割多重伝送技術（WDM：Wavelength Division Multiplexing)や多値伝送技術（QAM：Quadrature Amplitude Modulation)，デジタルコヒーレント伝送技術など，一貫して光ファイバ通信網の伝送距離の長距離化および大容量化に対して多大な貢献をし，海底光ファイ



Prototype in 1989

・Paper:
M. Nakazawa, Y. Kimura, and K. Suzuki, “Efficient Er^{3+}−doped optical fiber amplifier pumped by a 1.48 μm InGaAsP laser diode,” Appl. Phys. Lett., vol. 54, pp. 295-297 (1989).

・Patent: JP2128337 “Optical fiber amplifier”

特徴：
・高速大容量
・低雑音
・低遅延
・小型高信頼

図１　世界で最初の半導体レーザ励起Erbium-Doped Fiber Amplifier（EDFA）

バ通信による大陸間通信や年々爆発的に増加するデータ量への対応など，グローバルなインターネット社会を支える基幹技術である長距離大容量光データ通信の道を拓いた」とあります．背景も含めて教えていただけますでしょうか．

中沢：1980年代，単一モードファイバによる光通信が実用化されたのですが，長距離通信においては，光ファイバ伝搬で減衰して弱くなった信号を電気的に元に戻して，再送信する中継器を数10 kmごとに設置する必要がありました．すなわち，光中継器では光信号を電気信号に変換・再生し，再度光信号に変換して元の信号強度で送信する方式が用いられていました．ところが，電気増幅器は扱える信号の帯域が狭く，信号が歪むこともあり，また光素子を含めた装置は大型になり消費電力も大きかったので，光信号をそのまま増幅する光増幅器の出現が期待されていました．これが実現すれば，小型で広帯域な信号の増幅が可能になります．

私と萩本さんは，その期待にこたえ，実用化が難しいといわれていた小型高効率広帯域の光増幅器EDFAを実現しました．この装置は筋が良かったのか，高速・大容量，低雑音，低遅延，小型・高信頼という優れた特徴を持っていました．

私は，EDFを励起するための光源として，波長1.48 μmのInGaAsP半導体レーザを用いる方法を世界で初めて提案しました．散乱・吸収等による光の減衰が0.2 dB/kmと小さく，光ファイバ通信での最低損失波長域である1.5 μm帯において，波長幅50 nm以上の広範囲にわたり12.5 dBの利得を得ることに成功しました．これにより，1.5 m四方程度の極めて大掛かりな励起光源を必要とする従来の光増幅器とは大きく違う，電池でも駆動できるわずか約10 cm四方の小型広帯域光増幅器をつくったのです．実用的な光通信システム構築への展望が開けたと評価をいただきました．

萩本：中沢さんの発明を基に，私は当該光増幅器を高出力化して1.8 Gbit/sの強度変調直接検波方式により212 kmの長距離伝送を成功させ，その実用性を世界で初めて実証しました．私たちの成果は代表的な光中継器として，開発から5年ほどで太平洋・大西洋横断光海底ケーブルなど世界を結ぶ幹線系長距離伝送網で採用されるなど，光通信システムの実用化を飛躍的に進展させたと評価をいただきました（**図2**）．

EDFAは多波長光信号も一括増幅できるため，WDMによる大容量化技術の開発も相まって，1990年代半ば以降光通信の利用が一気に進んだのです．私はこの技術の国際標準化を主導したことも評価されました．これまでほかの光増幅方式も開発されていますが，現在でも世界の主流はEDFAです．

こうして，私たちの業績が，世界中のインターネット上で利用する情報リソースの多様化・大容量化を可能にし，高速大容量な光通信システムが低価格で提供可能となったことで，さらにインターネットの爆発的な普及を後押したと評価をいただきました．

―私たちが現在，当たり前に使っているSNSやクラウドサービスなどの情報通信基盤の飛躍的な拡大を可能にした業績であると，Japan Prizeの授賞理由に謳われています．お二人のご苦労が実を結び，豊かな現代社会を築く，その一翼を担われたのですね．

中沢：私たちの仕事は縁の下の力持ちというか，一般的には通信はつながって当たり前と思われていますが，つながっていることは実は素晴らしいことなのです．受賞を機に光信号の伝送距離をどこまで延ばせるか，ファイバの切断場所の特定をどうするか，と格闘していた当時を思い出しました．

萩本：そうですね．当時，中継器をマンホールへ設置して実験していたことを思い出します．伝送実験のために中継器を設置している地下に潜るのですが，マンホールって空気が薄かったり，雨水が溜まっていたりして危険なんですよ．今後，運用していくにしても，長距離伝送により中継器の数を減らしていくことで，こういう危険な作業はないほうがいいと思いました．

―壮大なドラマが数々ありそうですが，EDFAにまつわるエピソードを少しだけ聞かせていただけませんか．

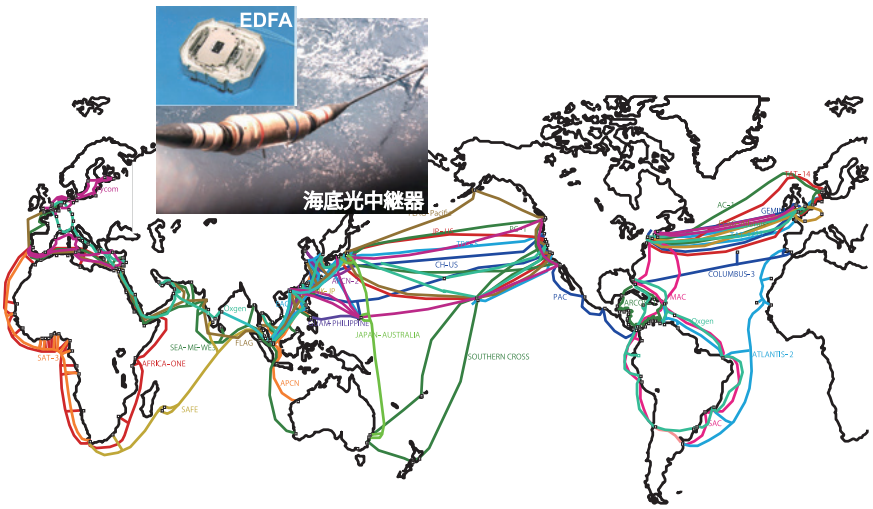


図2　国際海底光ケーブルネットワーク

中沢：光ファイバの破断点検出装置では光ファイバ中のレイリー散乱のレベルは非常に低いので，強い光パルスを入れる必要があるのですが，1980年当時はそれを実現できるハイパワーの半導体レーザはなかったのです．そこで，波長1.32 μmのYAG レーザ*1をNECのグループと一緒に開発し，FRLという現場試験を通じて光時間領域反射率計（OTDR）として技術資料にまとめ上げました．固体レーザが通信用測定装置として実用化されたのは，これが初めてではなかったでしょうか．単一モード光ファイバ伝送システムの中継器間隔は約80 km でしたので，探索距離としては片端から40 km見られればいいのですが，広いダイナミックレンジが必要だったので，さらにいい光源がないか探し始めたのです．

光ファイバ中では，最低損失波長の1.55 μm がパルスをもっとも遠くまで飛ばせるので，障害点探索距離も1.55 μm の高出力光源があれば最長の探索距離を実現できます．そこで，いろいろな固体レーザの発振波長を調べて，基底準位*2 $^4I_{15/2}$と上準位$^4I_{13/2}$との間に波長 1.55 μm の遷移線を持つエルビウムに行き着いたのです．入社２年後の1982年の春でした．早速，上司に「エルビウムレーザをつくりたい」と相談したところ，「それではやってみましょう」ということになりました．しかし，当時は米国でエルビウムの固体レーザを研究したことがあるという話がある程度で，誰も注目していませんでしたし，情報も論文も全くありませんでした．そこで，自分たちで一からつくることを決意し，Nd のリン酸系レーザロッドを手掛けていた保谷硝子に，「ぜひエルビウムレーザロッドを一緒につくってくれませんか」とお願いしたのです．保谷硝子の事業部長は「うちではやったことはないけれどやってみましょう」と快諾してくれました．あのとき，「これは難しいのでお断りします」ということになっていたら，その後のEDFAは実現していなかったかもしれません．

そして，EDFAの開発を通じて不思議だと思うことが２つありました．１つはエルビウムイオンがシリカガラスの中では光学活性であることです．普通はリン酸系やフッ化物系ガラスのような非発光（フォノン緩和）遷移が小さい材料で希土類はよく光りますが，エルビウムは例外的です．もう１つはシリカファイバでの波長 1.55 μm ラマン増幅の励起波長は 1.48 μm であり，エルビウムの擬似２準位的な励起波長も同じです．これは神のみぞ知るで，もし両者が異なっていたらEDFAの開発にはもっと時間がかかったか，開発されていなかったかもしれません．というのは，ラマン増幅とエルビウム増幅を同時に１つの研究室で研究していたのは世界中で私のグループしかなかったのです．

萩本：連絡をとっているといっても，茨城と横須賀に離れて研究活動をしていましたが，当時双方の研究指導をしていた島田禎晉さんから早く協力してシステム実験をするように指示され，1989 年にファイバ増幅器による最初の伝送実験に取り組みました．当時の励起レーザ出力が十分でなかったのと，安定性を増すために工夫する中で，条件を満たすEDFAを１本選んで，このファイバを２分割して使用することを考え，分割比を単なる２分割ではなく黄金比で切って巻き直すことに決めたところ，長いほうがパワーアンプ，短いほうがプリアンプに適していることが分かってきて，ただのファイバに見える素線が80 km のファイバ区間のロスを補って余りある増幅パワーを提供してくれるとは魔法のように感じました．

当時，光直接変調直接検波（IMDD）方式は，性能の向上に行き詰まり，コヒーレント光伝送方式との最後の決戦と思ったのが光直接増幅でした．1989年に成功した光ファイバ増幅中継実験は，やればやるほど感動的にEDFAのパフォーマンスは素晴らしかったことを今でも鮮明に覚えています．

光ファイバ増幅器が多くの波長を一括で歪みなく増幅でき，300台つないでも帯域が確保できるということで，多くの人の取り組みで，あっという間に太平洋横断を光ファイバ増幅だけで中継する検討が進んできました．NTTの陸上方式とほぼ同じタイミングで，信頼性を重視していた海底システムに導入するということをKDD（国際電信電話，当時）とAT&Tが判断したのには驚きました．人を感動させる研究をしたいと思っていましたが，自分が感動しました．

紆余曲折あってもめざすところへだんだんと近づいていく

―EDFAの誕生は，現在のグローバルなインターネット社会を支える基幹技術である「長距離・大容量光データ通信」への道を拓き，NTTが提唱するIOWN構想にもつながる功績です．こうした素晴らしい功績を遺す研究はどうすれば成し遂げられるのでしょうか．

中沢：EDFAのようなインパクトのある研究成果は稀ですし，研究は一山越えたらまた次の山と終わりはないものです．私たちの成果でいえば，エルビウムという素材と巡り会えた幸運やこの領域においてさまざまな研究者が飽くなき追究を

*1　YAG レーザ：イットリウム・アルミニウム・ガーネット（Yttrium Aluminum Garnet）を用いた固体レーザ．
*2　基底準位：電子の総エネルギーがもっとも低く安定な「基底状態」の電子配置の状態．

提供：国際科学技術財団

写真　授賞式の様子

続けてきた成果の上に成り立っていると思います．

また，「これをやったらいい」と最初から分かっているなら，皆がそれを手掛けるでしょう．しかし，それが分かりませんから，研究者は引き出しに知識を蓄えておくだけではなく，他の研究者とのつながりという引き出しも持っていて，素材や個々の成果，研究者の知識等を複合的に組み合わせて大きな成果を生み出しているのです．

萩本：私たちが成し遂げた1989年の伝送実験の成果を，島田さんがとても喜んでくださったのですが，私がOFCでの発表の準備をしていたら「発表は別の人に行ってもらいなさい」と言われました．理由を聞いたら，「あなたは報道発表やその後の対応でもっと忙しくなるから」と．そこで，自分で出した成果の発表を同僚に頼むことになったのです．今思えば，私が体力の限界だったことをかんがみての対応だったのかもしれません．

島田さんがその成果を光産業技術振興協会の桜井健二郎記念賞に，その年（1989年）に応募してくれたことから中沢先生とともに同賞を受賞することなったことが思い出深いです．その後も，研究から導入支援までいろいろつまずきながらも，先輩やコミュニティに支えられ，何とか目的を果たすことができ，Japan Prizeにつながったのだと思います．

加えて，エンジニアリングの観点からみると，成果物を世界に浸透させていくためには標準化や仲間づくりも重要ですから，時には自分の成果へのこだわりを捨てることも大切になります．国の支援も受け，各組織・各社の保有する知的財産を集約するドリームチームを結成できたことも成果につながったと感謝しています．組織を越えて協力することは，難しい一面もあります．しかし，海外に対抗していくためにも，日本の研究者も，日本の競争力を上げるだけではなく，社会全体への貢献や人類の発展をかんがみてまとまっていけたら，大きな成果を上げられると思います．

中沢：そのような観点でいうと，萩本さんは伝送装置，光増幅器の重要性をいち早く見抜いてシステムへ導入しようと他社と連携して築き上げました．そして標準化を主導する等，つながる力を存分に発揮されました．これは言葉にすると簡単だけれど，並大抵のことではないのですよ．

―いうまでもなく社会，人類の発展に研究者は大きく寄与しています．研究者にはどんな資質が求められるでしょうか．

中沢：人は生来，日々の生活をより良くしようと思って暮らしていると思いますが，それを生業にし，誇りを持ち，使命感を感じるのが研究者ではないでしょうか．そして，研究者には好奇心と情熱と強い意志が非常に重要ですね．

誰にも期待されていないとしても道を切り拓いていく，期待されていないときほどちゃんと頑張れるかが大事なんです．苦しいときでも自分の研究を楽しむくらいでないとダメなのです．というのは，メインストリートをずっと走っていたとしてもその研究が花開くとは限らないからなのです．

そして，本でできる勉強は年をとってもできるので，若いときにしかできない勉強をしておくことが大切だと思います．私は田舎で育ち，魚を捕ったり，アケビを採ったりと研究とは遠い世界に生きていました．中学生のころはプラモデルをつくるのが好きでしたし，真空管のラジオをつくったりもしていました．こうしたさまざまな経験が研究者の引き出しを満たしているように思いますし，伸びていくように思います．

萩本：その言葉どおり，中沢さんは光ファイバ向けのレーザを追究され，技術の発展に貢献されたことは並々ならぬ尊敬の念があります．東北大学の研究室にお邪魔したときも，当時のように実験をされていまして，中沢さんの熱意は本当にゆるぎない．70歳になったはずなのに20～30代のころと変わらない．すごいな．探求心というのは本当に変わらないのだと思いました．見習いたくても見習えないレベルです．

それを踏まえて，研究者というのは憧れや夢を持っていると言いましょうか，「こうなったらいい」と好奇心を持って臨む力があるのではないでしょうか．誰も登ったことのない高い山があったら登りたくなるような好奇心が大事ですね．そして，紆余曲折があってもその気持ちを持続できる人だと思います．自らの道程を振り返って感じますが，最初の気持ちを忘れなければ，紆余曲折があってもだんだんとめざすところへ近づいていきますし，少なくとも逆方向へ進むことはありません．

やったことのないことをするというのは成功への第一歩

ーNTTの研究所で培ったプリンシパルなスピリットをお聞かせいただけますでしょうか．

中沢：私たちが入社した当時はまだ電電公社でした．研究所はある意味の聖域で，各大学から優秀な研究者が集まり，さまざまな研究開発をされていたと思います．こうした環境で私たちは，米国のベル研究所等のような欧米の最高峰の研究所にどう打ち勝っていくかを念頭にいつも研究をしていました．

こうした中で，先輩方は非常に心が豊かでゆとりがありました．EDFAは当時の私の専門とは違うものでしたが，それでもEDFAの研究をしたいと申し出たときも「面白そうだ．やってみたら？」と，保谷硝子にも同行してくれたり，予算を工面してくれたりとサポートしていただきました．視野を広く持ち，サポーティブな姿勢で後進を支えるというスピリットは今でも私の中に生きていますし，今も海外の研究者たちと競争を続けています．

萩本：NTT研究所の初代所長，吉田五郎氏の言葉「知の泉を汲んで研究し実用化により世に恵を具体的に提供しよう」です．NTTは基礎研究から応用研究までさまざまな研究がなされており，世界的にみても非常に珍しいカバレッジの広い研究活動を展開し，他社と連携して実用化を図り，社会に貢献しています．CoE（Center of Excellence）という表現がありますが，河内正夫（元NTT先端技術総合研究所長）さんの言葉を借りれば，CoEの定義は，「二流の研究者が一流の成果を出せる組織」だそうです．

（今回はリモートにてインタビューを実施しました）

NTTがベースの技術をしっかりと再利用できるように確立しているのは重要な資産であり，価値の継承・発展を可能にする礎になります．その意味でも，先端技術は，デバイス・測定器・装置・サブシステムなどに形を変えて，実現手段を提供できることが，次世代につながる大事なステップになります．過去の技術がきっちりと蓄積されて，次の人がそれをベースに階段を登っていく，蓄積的な進歩こそが，これこそ位相整合がとれているという証左なのでしょう．

私自身も専門外ではアマチュアですが，一流の研究成果の上に新しいアイデアを重畳させることで成果を出せることもあります．私はこのスピリットで研究活動に臨んでいますし，光ファイバ通信領域でも同様に，後に続く研究者にCoEが受け継がれていくといいなと思います．

ー最後に後進の研究者の皆さんにエールをお願いいたします．

萩本：後進の研究者の皆さん，好奇心を胸に，長いトレンドを持って自分自身の研究に臨みましょう．また，組織を越えた仲間づくりは研究活動において非常に大切ですから学会にもぜひ出席してください．世の中にインパクトを与える研究活動に期待しています．

中沢：基礎研究をしている後進の研究者の皆さんに伝えたいのは，後追いはダメ．フロンティアスピリットを持って夢のある新しい研究をしていただきたいです．任されている研究があると思いますが，それとは別にやりたい研究を１つ持っているといいですね．研究の幅が広がりますし，やったことのないことをするというのは成功への第一歩なのです．（インタビュー：外川智恵）

特集

量子計算機時代を見据えた暗号研究の最前線

近年，暗号技術は単に情報を秘匿するというだけではなく，属性ベース暗号のような高機能暗号により，データの安全な利活用を支える技術としての役割も担うようになってきている．

また，昨今の量子技術の発展により，耐量子暗号や量子の特性を活かした新たな暗号技術の研究も進んでいる．

本特集では，NTTの暗号技術の研究者らによる論文をベースに，これらの最新暗号技術について紹介する．

Cryptography

現代暗号の発展と量子計算機時代の暗号研究に向けて

1976年から始まる現代暗号理論では，攻撃者を多項式時間チューリング機械とみなして安全性を考えていました．しかし，近年の汎用量子計算機の実現可能性はこのモデルを覆すインパクトを現代暗号にもたらしました．NTTの暗号研究は現代における情報システムの安全性を確立する技術を提供するとともに，量子計算機が普及した未来における応用の創出もテーマとしています．本稿では40年に及ぶNTTの暗号研究を概観し，現在の取り組みについて概説します．

阿部（あべ）　正幸（まさゆき）
NTT社会情報研究所

NTTの暗号研究を取り巻く状況

1982年の電電公社職員による銀行カード偽造事件に端を発したNTTの暗号研究は40周年を迎えました．発足当時わずか3名による暗号研究チームは，1992年に情報通信網研究所内で8名からなる正式な研究グループとなりました．これ以降，Webブラウザ Mosaicの登場（1993年）とともにインターネットが爆発的に普及してゆく時期と重なり，情報セキュリティの重要性が認識されて情報セキュリティプロジェクト（1999年）となり，さらにNTTセキュアプラットフォーム研究所（2012年）となりました．今日，情報セキュリティ技術はコモディティ化して日常生活を支えるものとなり，NTT社会情報研究所として広く暗号・情報セキュリティの研究に取り組んでいます．

ネットワークの高度化はさまざまな情報流通システムを可能とし，暗号も秘匿・認証という基本的な「守り」から，暗号通貨やクラウドコンピューティングなど新たな応用を創出する「攻め」へと適用範囲を拡大してきました．また，汎用量子計算機の実現可能性が高まり，現在実用化されている公開鍵暗号が急激に危殆化することが明らかになったことで，「守り」の利用でも新たな対応が迫られるようになりました．さらに将来を考えれば，汎用量子計算機を積極的に利用した暗号応用の創出と，それを支える基礎理論の確立が期待されるようになりました．

本稿では，暗号利用者と攻撃者の双方が現在利用できる計算機である，古典的な計算機を用いる「現代暗号」，攻撃者のみが量子計算機を用いる「耐量子暗号」，利用者も攻撃者も量子計算機を用いる「量子暗号」について（**図**），公開鍵暗号に関するトピックを中心に概観し，NTTの暗号理論研究とのかかわりについて述べます．もう1つの重要な研究トピックである共通鍵暗号については耐量子暗号の観点で述べることにします．

現代暗号理論の発展

安全で効率的な暗号は，あるクラスの問題を確率的チューリング機械で解

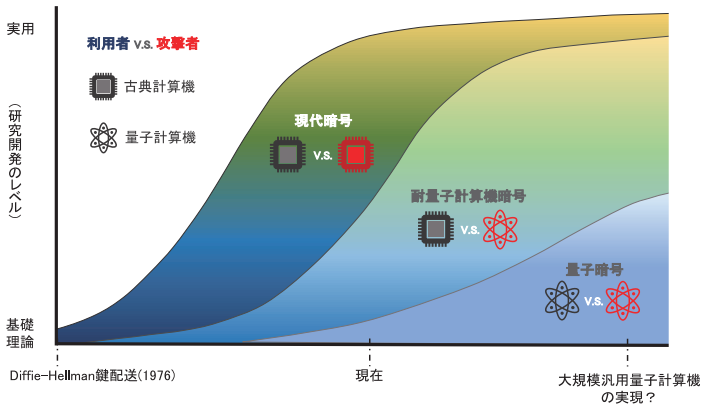


図　現代暗号・耐量子・量子 暗号の研究開発レベル

くことが平均的に難しいという計算量的な仮定に基づいて構成されます．攻撃者が利用できるアルゴリズムやハードウェアが進歩すると，個々の問題は以前より短い時間で解けるようになります．すると，その問題のクラスに基づく暗号では，安全性確保のためにより大きな公開鍵が必要となり，パフォーマンスが低下します．公開鍵暗号の先駆であるRSA暗号（1977年），Rabin暗号（1978年）やNTTが開発したデジタル署名方式ESIGN（1990年）は素因数分解問題の困難性を利用しています．開発当時，RSAの公開鍵は512ビットで安全と考えられていましたが，現在では3072ビット以上が推奨されています[(1)]．同じく先駆的な暗号技術であるDiffie-Hellman鍵配送（1976年），El Gamal暗号（1985年），DSA署名（1993年）は当初，乗法群上の離散対数問題を利用して構成されましたが，同じセキュリティレベルで公開鍵をより小さくできる楕円曲線上の離散対数問題に基づく構成（ECDSA署名など，2005年）に移行しました．

ネットワークの高度化によってクラウドコンピューティングのような高度な応用が出現し，暗号は基本的な秘匿・認証という守りの技術から，高度な情報流通サービスを構築するための攻めの技術へと発展してきました．楕円曲線上の群における双線形形写像（ペアリング）は，当初B. S. Kalisky Jr.によって安全な鍵生成に利用され（1987年），NTTの岡本龍明らによる楕円曲線暗号の安全性解析（MOV帰着，1991年）で広く知られました．その後，個人のIDを公開鍵にできるIDベース鍵交換（大岸聖史，境隆一，笠原正雄，2000年）やIDベース暗号（Dan Bonehら，2001年）で本格的に暗号に利用され，現在まで数多くの実用的な応用を創出しました．特に，それまで限定的だった非対話ゼロ知識証明の利用領域がペアリングの導入によって一気に拡大し（Jens Grothら，2008年），NTTでもペアリング群上でゼロ知識証明と署名などを自由に組み合わせて高度な機能を実現する群構造維持暗号系（阿部正幸ら，2009年）の研究が進展しました．ペアリングは，複雑なステートメントを短い証明書で効率的に検証できるComputationally Sound Proofという先進的な概念（Silvio Micali, 2000年）を，Zero-Knowledge Succinct Non-interactive Argument（zkSNARG）（Rosario Gennaroら，2012年）として実現することに大きく貢献しました．短い証明書はブロックチェーン上の応用に大変有効であるため，zkSNARGはWeb 3時代の基盤技術となることが期待され，C++のような高級言語で表現したステートメントをzkSNARGが扱いやすいNP完全な中間言語にコンパイルするフロントエンドの開発が進み，実用性が急速に向上しています．

暗号がさまざまな応用で利用されることや，暗号自体の高機能化に伴って，求められる安全性も高度化してきました．識別不可能性といった比較的単純な安全性に関しては，離散対数問題に基づくBlum-Micaliの疑似ランダム生成器（1982年）や素因数分解問題に基づくRabin暗号（1986年）のように，単一の困難性仮定への比較的単純な帰着による証明が示されてきました．しかし，攻撃者がより積極的に暗号システムの入出力に関与することを許した適応的選択暗号文攻撃に対する安全性（IND-CCA安全性，1991年）のような高度な安全性は，それを達成する暗号方式の構成も安全性証明も複雑になりました．Mihir Bellareらによる，ハッシュ関数を理想化して扱うランダムオラクルモデル（1993年）は，暗号の構成と安全性証明を単純化することに大きく貢献し，ランダムオラクルモデルが安全性の証明されたさまざまな暗号方式や応用が1990年代後半から2000年代に提案され，証明可能安全性のパラダイムが広まりました．NTTでは，IND-CCA安全な公開鍵暗号の一般的構成手法Fujisaki-Okamoto変換（FO変換，1998年），鍵カプセル化メカニズムPSEC-KEM（1999年），メッセージ回復型署名方式ECAOS（2008年）などがランダムオラクルモデルで安全性を証明できる方式として開発されました．一方，ランダムオラクルに基づかない効率的で証明可能安全な構成を追求する研究もさかんに行われました．

現在の計算機を対象として発展してきた暗号技術は，後述する量子計算機の登場以降の世界においても安全な暗号の構成に示唆を与えるものであり，暗号基礎理論として引き継がれていきます．

現代暗号から耐量子暗号へ

攻撃者が汎用量子計算機を実際に利用できるようになるまでにはまだ相当の時間がかかると考えられています．とはいえ，現時点で流通している情報の多くは収集され蓄積されているため，その将来的な安全性を確保するには，現在の暗号技術が汎用量子計算機を利用した未来の攻撃に耐える必要があります．耐量子計算機の安全な暗号の構成に用いる基本的な困難性仮定として，格子（Lattices）に基づく問題が有望視されています．格子問題の暗号への利用はAjtaiによる一方向性関数の構成（1996年）に始まり，その後，格子ベースで実用的な効率を持つNTRU暗号（1998年）が提案されています．デジタル署名については多変数多項式やハッシュ関数に基づく構成も耐量子安全性への有望な選択肢です．

2017年から開始されたNIST(米国国立標準技術研究所)によるPost-Quantum

Cryptography（PQC）Competitionで耐量子計算機安全な公開鍵暗号，デジタル署名の公募が行われ，2022年に最終候補が発表されたことから耐量子暗号は実用へと急速に近づきました．2024年には新たな標準となり，2030年までに現在の暗号に置き換えることが想定されています．NTTはNTRU暗号の提案元として，また，多数の候補の評価を行うかたちでNIST PQCコンペに貢献しています．量子計算機では重ね合わせ状態での演算が可能で攻撃者の計算原理が異なるため，安全性証明技法も量子計算機に合わせて再構築されてきました．前述のFO変換も量子状態で計算するハッシュ関数をモデル化した量子ランダムオラクルモデルで安全性が成り立つよう再検討され，NIST PQCコンペで採用された暗号方式CRYSTALS-KyberをIND-CCA安全とするために使われています．

格子は耐量子安全性の観点に加えて，高機能暗号を実現する基盤技術でもあります．特に，暗号化したまま平文の加算・乗算が可能である完全準同型暗号は，クラウドコンピューティングをはじめ，広範な応用を持つ強力な暗号技術です．NTTでは格子暗号の安全性解析や完全準同型暗号の研究（2013年～）に取り組んでいます．

ブロック暗号やハッシュ関数のような共通鍵暗号系の暗号技術については，内部構造を考慮しない汎用的な量子アルゴリズムを用いた鍵探索攻撃に対しては鍵長やブロック長を2～3倍にすることで安全性を維持できるため，整数論的仮定に基づく公開鍵暗号のような致命的な影響は受けないと考えられています．その一方で，よく知られた特定の構造に対して効果的な攻撃が示されているため，量子計算機による攻撃は共通鍵暗号にとっても新たなリスクです．本特集記事『量子計算機を用いた攻撃に対するハッシュ関数の安全性のより良い理解へ向けて』[2]では，量子計算機を用いた攻撃に対するハッシュ関数の安全性，特に，現在もっとも広く使われているハッシュ関数SHA-256やSHA-512を含むSHA-2の耐量子安全性について解説します．

耐量子安全なゼロ知識証明や暗号プロトコルの研究も進展していますが，直ちに現在の技術を代替する性能となるにはさらなる研究が必要です．例えば匿名電子投票では，従来の古典暗号技術で数kBの投票が，耐量子安全性の下では数100kBに増大してしまいます．これらは現在の暗号技術による情報流通システムの耐量子安全性への移行に不可欠な要素技術であり，早期の発展が期待されます．

そして量子暗号へ

近年のエッジデバイスの著しい計算能力向上はさまざまなアプリケーションを可能にしてきました．量子計算機が攻撃者だけでなく一般利用者にまで普及した未来では，どのような技術や応用があり得るでしょうか．量子物理学者のStephen Wiesnerは観測による量子状態の喪失を偽造不可能な量子マネーに応用するアイデアを1969年に述べています〔現在の暗号通貨や電子マネーの偽造防止は，取引台帳によるオンライン検証，暗号技術による事後検出，またはTEE（Trusted Execution Environment）の耐タンパー性などに拠っています〕．現在のデジタル技術では，情報が保管されていることを証明することはできても，消去されたことを証明することはできません．そのことが情報の廃棄を不確実にし，情報漏洩のリスクを生じています．本特集記事『秘密鍵を安全に貸与できる関数型暗号』[3]では，暗号の秘密鍵を消去したことを証明する研究を紹介します．量子計算機の話題が一般的になった現在，従来にない応用が模索されるだけでなく，基礎理論の確立をめざして量子物理，量子情報処理と暗号理論を融合する研究が行われています．本特集記事『新たな応用分野を切り拓く量子計算機向けアルゴリズム』[4]では，量子優位性，すなわち量子計算機の計算能力が現在の計算機を特定のタスクにおいて超えること，を示す研究を紹介します．

おわりに

NTT暗号研究を量子計算機の実現に関連して3つの分野に大別して概観しました．NTT社会情報研究所では基礎分野として今後も重要であり続ける暗号基礎理論から胸躍る遥か未来の応用まで多彩なテーマで暗号研究を進め，現在と将来の情報流通に貢献する技術を発信し続けます．

■参考文献

(1) https://www.cryptrec.go.jp/list.html
(2) 細山田：“量子計算機を用いた攻撃に対するハッシュ関数の安全性のより良い理解へ向けて，”NTT技術ジャーナル，Vol. 35，No. 5，pp.26-29，2023.
(3) 西巻：“秘密鍵を安全に貸与できる関数型暗号，”NTT技術ジャーナル，Vol. 35，No. 5，pp.19-21，2023.
(4) 山川：“新たな応用分野を切り拓く量子計算機向けアルゴリズム，”NTT技術ジャーナル，Vol. 35，No. 5，pp.22-25，2023.

阿部　正幸

暗号理論研究もその動機は目前のセキュリティリスクやこんな応用があったらいいという夢から始まっています．強固な理論を積み上げて，夢に届く技術を提供したいと思います．

◆問い合わせ先
NTT社会情報研究所
企画担当
E-mail　solab＠ml.ntt.com

秘密鍵を安全に貸与できる関数型暗号

「ないことを証明する」，この困難な命題を“悪魔の証明”などといいます．しかし量子のふるまいを利用すれば，関数型暗号における秘密鍵の消去，つまり「消去したこと」を証明できます．また量子のふるまいを利用することで秘密鍵の複製防止も可能となります．本稿では，2022年の国際暗号学会において発表した技術の概要と，実装された場合に期待されるイノベーションについて解説します．

西巻（にしまき）　陵（りょう）
NTT社会情報研究所

クラウド時代に対応する高機能暗号と秘密鍵

「1対多」の通信に活用される暗号のうち「公開鍵暗号」と呼ばれるものがあります．事前に鍵を共有しなくとも誰でもメッセージを暗号化でき，復号には秘密鍵を用います．現在，公開鍵暗号に高度なロジックを埋め込むさまざまな「インテリジェント暗号」が提案されています．よく知られているのが，ユーザの属性ごとに鍵のアクセス権限を設定できる「属性ベース暗号」です．例えば「人事部」「課長」という条件を組み込んで暗号化した場合，完全に同じ属性の鍵を持つ人だけが復号できます．条件に適合しない，あるいは部分適合の「人事部/係長」「営業部/課長」といった属性の鍵では復号できず，メッセージの秘匿性が守られます．

2023年1月に発表した論文『Functional Encryption with Secure Key Leasing』[(1)]に登場する「関数型暗号」は，インテリジェント暗号の中でもより強力なものとなります．属性ベース暗号では平文を得ることしかできないのに対し，関数型暗号では平文から特定の情報だけを復号して任意の計算結果を得ることができます．実用化されれば，難病患者の医療情報がストックされているデータベースから，患者のプライバシに触れることなく統計情報だけを計算するといったユースケースが可能になります．高機能な暗号はクラウド時代の情報セキュリティに大きな力を発揮すると期待されています．

これらの秘密鍵は既存のコンピュータでも生成できます．反面，いったん配布された鍵データのコピーを防ぐことはできません．ユーザが鍵の返却や削除を主張しても，複製した鍵を隠し持っていれば依然として暗号文を復号できます．そこで，関数型暗号の秘密鍵を量子力学の原理を使って「消去」および「コピー不可能」にできることを数学的に証明し，よりセキュアな鍵の貸与を提案しました（**図1**）．

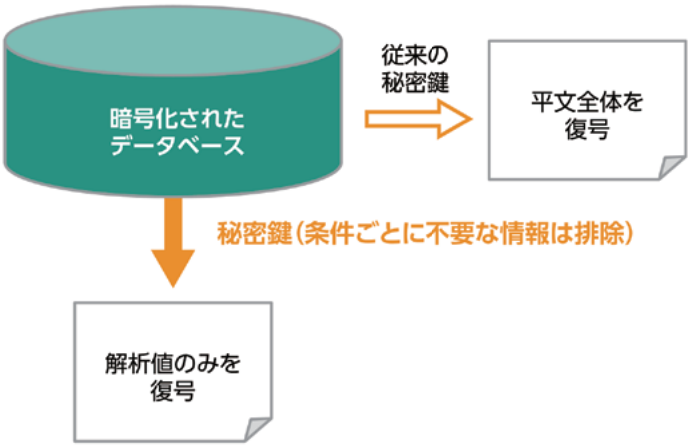


図1　高機能な関数型暗号

不確定性原理を利用し，「測定」で鍵を消去

前提として，鍵を貸与するホスト側も借り手のユーザも，共に量子計算機を使用していると仮定します．量子状態を保存できるメモリと，任意のアルゴリズムが実行できる量子計算機が実用化されており，ユーザに貸与する秘密鍵も量子の状態に変換して表現されています．この秘密鍵は重ね合わせ状態になっており，観測により状態が変化します．

このような秘密鍵を削除する方法は，まず量子ビットをなんらかのユニタリ変換*1で加工し，量子鍵を生成します．このとき計算基底（|0〉，|1〉）*2で測定すると鍵としての情報が残り，アダマール基底（|＋〉，|－〉）*3で測定すると鍵の情報が壊れるように設定します．

返却の時期が来たらユーザにアダマール基底で量子鍵を測定してもらいます．正しく観測されていれば不確定性原理によって鍵の情報は消去され，0か1で記述される古典情報だけが残ります．残った古典情報は消去の証拠として提出されます．

もし指定と異なる測定方法をとった場合，鍵の情報が残存しますから，返却したとは認められません．このように，状態を観測する方法を変えることで情報を部分的に消去し，鍵の機能を削除します（**図2**）．

秘密鍵が消えたことをどのように証明するのか，ないものを証明する「悪魔の証明」は可能なのか，これはとてもシンプルな方法です．秘密鍵を削除したときに，証拠として古典情報が提出されます．ホスト側はそれを確認した後，再度暗号文をユーザに送り，復号してもらいます．復号ができなければ鍵は存在しないと判断できます．つまり「復号失敗＝消去」と定義します．これを定式化するのです（**図3**）．

ノークローニングによるコピープロテクト

■秘密鍵のコピー防止

秘密鍵のコピー防止には量子の性質を利用します．自分自身が作成した量子状態は複製できますが，他人から与えられた未知の量子状態は「量子複製不可能定理（ノークローニング定理）」によって複製ができません．もし攻撃的なユーザが複製を試みたとしても2つの量子鍵のうちどちらかは正しい復号ができないのです．

しかもこの量子鍵は，鍵の機能を規定する情報を取り出すことができません．なぜなら前述したように，コピーしようと観測した瞬間に不確定性原理によって状態が変化し，鍵が消失するからです．測定せずに量子状態のまま置いておくしかありません．このような秘密鍵のコピープロテクトを定式化して証明しました．

暗号理論の安全性を，膨大な計算量から証明する「計算量的安全性」と，無限の計算能力を持った攻撃者にも解読されない「情報理論的安全性」に大別するならば，今回提案した手法は量子の性質と暗号理論の両方を利用するため前者の計算量的安全が保証されます（**図4**）．

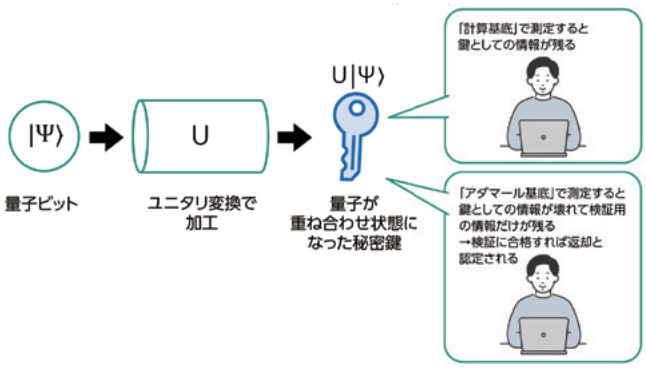


図2　量子秘密鍵の仕組み

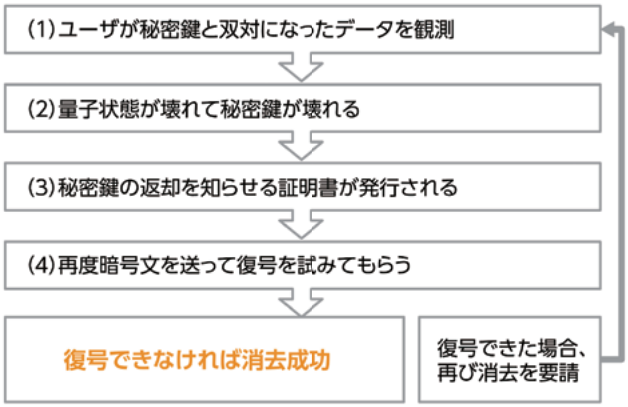


図3　量子秘密鍵の消去証明

＊1　ユニタリ変換：入力した量子ビットに演算を加えて変化させること．

＊2　計算基底：量子状態から情報を得るために行う基本的な測定．重ね合わせ状態になっている量子ビットは$|\Psi\rangle=\alpha|0\rangle+\beta|1\rangle$で表されますが，計算基底による測定を行うと，確率$|\alpha|^2$で測定値0を得て状態が|0〉になるか，あるいは確率$|\beta|^2$で1を得て状態が|1〉になります．

＊3　アダマール基底：量子状態が|＋〉か|－〉かを測定する．|0〉は|＋〉に，|1〉は|－〉に変換されます．

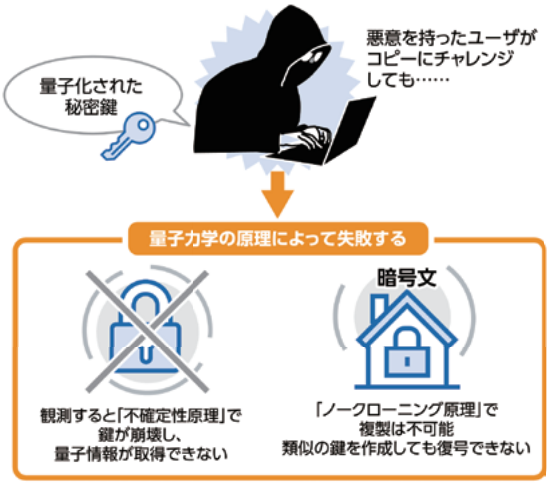


図 4　量子秘密鍵のコピープロテクト

■未来の量子社会に対応する暗号技術

現在，オンプレミス*4よりもクラウドが重視され，米国やカナダで公開されている量子計算機もクラウドサービスによって運用されています．このような 1 対多の通信環境においてより強力な暗号技術が求められています．

古典計算機でも鍵のデータを失効化する技術はいくつか提案されていますが，暗号文を生成するごとに秘密鍵をつくり直すタイプだと非効率で利便性に欠けます．また暗号文を一度全部更新するものだと元データの容量に比例してさまざまなコストが発生します．古いデータが残存するリスクも心配です．高機能暗号に量子力学を援用することで暗号化に伴うコストやリスクをスマートに解決できると考えました．

また，暗号化する手続きや具体的な技術へと発展させる理論など研究の範囲はまだまだ広がりそうです．

コンテンツサービスや忘れられる権利への展開

将来，今回の論文を軸としたものが国際標準となり，社会実装される可能性もゼロではないと思います．米国の国立標準技術研究所（NIST）などが次世代の暗号方式として選定すれば世界で標準化されるからです．

今回は秘密鍵に限定していますが，最終的にはプログラムの削除証明やコピー防止をめざしています．これらが実現した場合，企業の研究開発や情報管理，あるいはコンテンツサービスの提供方法なども変わるでしょう．顧客に量子鍵を渡してサービス利用期間中のみ有効とし，契約期間の満了と同時に鍵が無効化されるといったかたちで実装される可能性があります．第三者のサーバやクラウドサービスへの信頼性も高まりますし，著作権などのプロテクションもより強固になるでしょう．

また検索エンジンに残る古い暗号文を完全に抹消できれば，欧州連合（EU）が一般データ保護規則（GDPR）第17条に定めた「忘れられる権利（right to be forgotten）」にも応用できるかもしれません．今は「消しました」という相手の主張を信用するしかない状態ですが，量子力学を利用すれば新しい権利概念にも技術的に対応できる可能性があります（**図 5**）．

ただし，ある程度量子計算機が汎用化されて，一般的なユーザが使うようになれば，の話であり，現在のエラー訂正能力から考えると，もう少しエンジニアリングが発展しなければ実装はまだまだ先の話ではないかと思います．

さらに暗号技術は，いったんシステムが動き始めると世界規模となるため，更新は簡単ではありません．理論の構築から技術開発を経て社会実装に至るまではさまざまな要素が絡み合い，相応の時間を要すると考えています．

図 5　実装できるカテゴリ例

*4　オンプレミス：情報システムを使用者（企業など）自身が管理する設備内に導入，設置して運用すること．

■参考文献

(1)　https://link.springer.com/chapter/10.1007/978-3-031-22972-5_20

西巻　陵

古典計算機では実現が不可能な暗号機能を量子計算機の力によって実現できるようになります．今後量子計算機の力を利用した暗号技術は研究が進み応用が広がっていくことが期待されます．

◆問い合わせ先

NTT 社会情報学研究所
企画担当
E-mail　solab @ ml.ntt.com

新たな応用分野を切り拓く量子計算機向けアルゴリズム

本稿では，量子計算機向けにNTTが考案した新しいアルゴリズムの論文（Verifiable Quantum Advantage without Structure）の概要を解説します．世界中で開発が進む量子計算機は，個別の問題を解くためのアルゴリズムの種類が現状では乏しく，このままでは応用先がごく限られる可能性があります．今回の新アルゴリズムは，この問題の突破口になり得るものです．「構造なしのNP探索問題」と呼ばれる種類の難問の1つを，量子計算機で超高速に回答できることを世界で初めて証明しました．量子計算機の新たな用途の発見につながる成果として，学会でも高く評価されています．

山川（やまかわ）　高志（たかし）

NTT社会情報研究所

はじめに

次世代の超高速計算機として期待される量子計算機には大きな課題があります．現状のままでは，使い道が狭い範囲に限られることです．

量子計算機の最大の利点は，現在の計算機と比べて超高速の計算が可能なことです．ただし，その恩恵を受けるには，量子計算機の仕組みを活かして効率的に計算するアルゴリズムが不可欠です．ところが，このアルゴリズムが決して豊富とはいえないのです．

実用に堪える量子計算機のハードウェアが登場するには，まだ5～10年単位の開発期間が必要とみられています．その間に，超高速性を理論で裏打ちできるアルゴリズムをたくさん見つけておかないと，極論すれば宝の持ち腐れになってしまうかもしれません．

今回NTTが考案したアルゴリズムは，この状況を一変させる可能性を秘めています．従来の常識では量子計算機の対象とされていなかった領域の問題を，超高速に解けることを世界で初めて証明したからです(1)．これまで研究者の間では，量子アルゴリズムが対象とする問題には何らかの構造が必要とされてきた*1のに対し，今回のアルゴリズムは構造がない問題を解くことができたのです．

構造がある問題を解く量子アルゴリズムの代表例は，インターネットの標準的な暗号を解ける方法として有名な「Shorのアルゴリズム」(2)でした．Shorのアルゴリズムが発表されたのは1994年なので，今回のアルゴリズムは約30年ぶりに登場した本質的に新しいアイデアといえます．

学会からも高い評価を受けています．成果を記述した論文は，理論計算機科学における最高峰の国際会議「IEEE Symposium on Foundations of Computer Science（FOCS）2022」に採択されました．Shorのアルゴリズムが発表されたのと同じ会議です．

さらに，量子計算理論の権威の1人，University of Texas at AustinのScott Aaronson教授は，量子力学に関する歴史的な議論で有名なソルベー会議の講演において，本件を最新のブレークスルーとして取り上げました(3)．科学分野の著名なオンライン媒体「Quanta Magazine」によれば，本件に刺激を受けた多くの研究者が，新しい用途の可能性について検討を始めたようです(4)．

検証可能性も満たす

今回の研究成果の位置付けを整理したのが**図1**です．「超高速」「構造なし」に加えて「検証可能」という性質を同時に満たせることが，開発したアルゴ

*1　後述のAaronson教授らは，量子アルゴリズムによって超高速化を図るには問題に構造が必要との予想を発表しています(3)．なお，この予想の対象が決定問題であるのに対し，NTTの成果は探索問題という違いがあります．

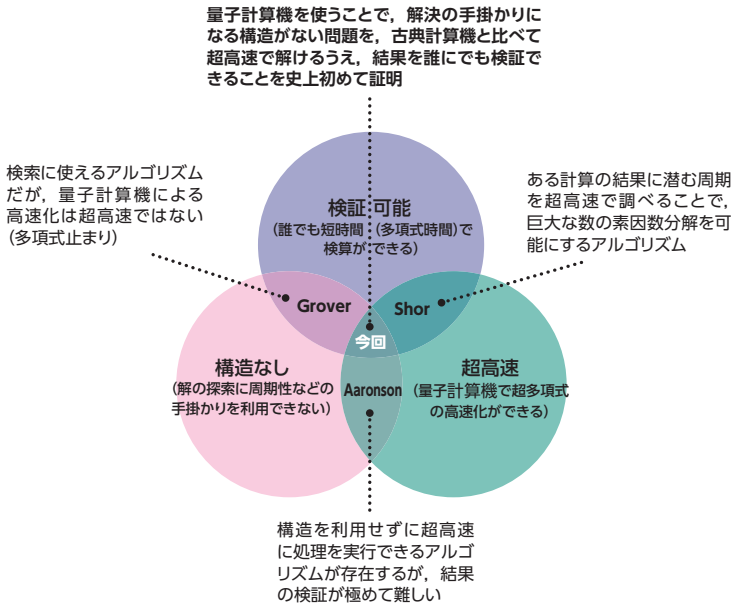


図1　開発した量子アルゴリズムの位置付け

リズムの重要な特徴です．

図が示すように，実は「構造なし」の問題を超高速に解けるアルゴリズムは従来もありました．例えば，前述のAaronson教授が提案した方法です[5]．ただしこれらのアルゴリズムには，検証可能性が欠けていました．

検証可能性とは，アルゴリズムが出した結果が正しいかどうかを簡単に確かめられることです．通常は，量子計算機ではなく従来型の計算機（量子計算機の分野では，古典計算機と呼ばれます）を使って，短時間で検証できることが求められます．ところが，既存のアルゴリズムは検証に極めて長い時間が必要で，出した答えが正解かどうかを事実上確かめられませんでした．これに対して，今回開発したアルゴリズムでは，結果の検証は短時間で済みます．

検証とは具体的にどういうことか，Shorのアルゴリズムを例に説明しましょう．Shorのアルゴリズムは，大きな桁の整数の素因数分解を対象にしています．例えば39,617を分解すると，答えは173×229になります．これが正解であることは，掛け算をすればすぐに確かめられます．数字の桁数が非常に大きくなると，素因数分解自体は古典計算機の手に負えなくなりますが，結果の検証は掛け算だけで済むため，古典計算機でも大して時間がかかりません．

このように検証が容易な（短時間*2で済む）問題は，NP（Non-deterministic Polynomial time）問題と呼ばれます．NTTが今回考案したアルゴリズムの対象もNP問題で，より細かくいえばNP探索問題とされるものです．

超多項式の高速性

図1には，構造のない問題を解けて，なおかつ検証可能性も満たす既存方式もあります．「Groverのアルゴリズム」と呼ばれるもので，量子計算機の教科書にも出てくる有名な手法です．この方式には，量子計算機に期待される「超高速性」が足りません．古典計算機のアルゴリズムに対して，せいぜい多項式で表せる高速化しか図れないのです*3．

今回開発したアルゴリズムやShorのアルゴリズムは，指数関数など，多項式を超えた数式で表せる大幅なスピードアップが可能です．例えば，インターネットの標準的な暗号が利用している2048ビットの整数を素因数分解するのは，古典計算機では何万年もかかるとされる難問です．ところが将来の大規模な量子計算機でShorのアルゴリズムを実行すれば，この問題を8時間で解けるという試算があります[6]．

ランダムな関数の入力を求める

では，Shorのアルゴリズムが利用している構造とは何なのでしょうか．

Shorのアルゴリズムは，ある数Nの素因数分解を，別の問題に置き換えて解いています．まずNと互いに素な自然数xを適当に選び，xのr乗（x^r）をNで割ったときの余りを計算します．ここで，rの値を変えていくと，**図2**(a)にあるように，余りの値は周期的に変化します．この周期が，問題に潜む構造といえます．

*2　ここでの短時間とは，多項式時間（polynomial time）のことを指します．多項式時間とは，問題の大きさ（例えば因数分解する数のビット数）nに対して，答えの計算時間がnの多項式〔nのx乗（xは非負の整数）の項を含む式〕で表せることを意味します．nが大きくなったときの値の増え方が，指数関数（定数のn乗）などと比べて緩やかです．

*3　Groverのアルゴリズムは，n個の候補から条件に合うものを選び出す検索問題が対象です．古典アルゴリズムでは平均n/2回，最大n回の問い合わせが必要なのに対し，Groverのアルゴリズムは$\sqrt{n}$回で済みます．両者を比べると高速化の度合いは二乗程度にとどまります．この程度の高速化では，量子計算機の誤り訂正のオーバヘッドなどで優位性が打ち消される可能性があります[3]．

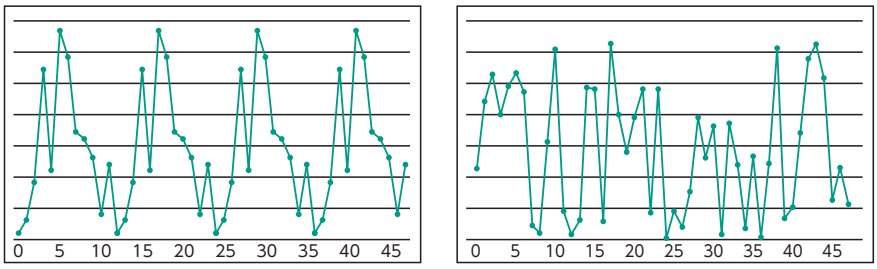
実はこの周期を求めることができれば，Nの因数は容易に計算できるのです．古典計算機では周期を求めるために非常に多くの計算が必要なのに対し，Shorのアルゴリズムは量子フーリエ変換という方式を使うことで超高速化を可能にしています．

今回のアルゴリズムが対象とする構造のない問題とは，解決にこのような手掛かりを利用できない問題のことです．量子アルゴリズムの開発では，しばしば処理の中身が分からない関数を対象に，出力から入力を推定する問題を取り上げます．この対象をブラックボックス，またはオラクル（神のお告げ）と呼びます．構造のない問題とは，オラクルの出力に規則性がみられない，すなわち入力に対してランダムな答（ただし同じ入力には同じ答）を返す問題ともいえます．

NTTはランダムなオラクルの具体例として，ハッシュ関数*4に注目しました．図2(b)に示すように，ハッシュ関数の入出力の間には規則がみられずランダムといえます．

ただし，ハッシュ関数は量子計算機による攻撃に対して安全なことが知られています．そこでNTTでは，2つの修正を施しました．オラクルへの入力として，ある制約を課したベクトルを利用することと，ベクトルの要素ごとに出力が1ビットのハッシュ関数を適用することです．前者は，入力するベクトルが，別の情報系列を変換した誤り訂正符号*5になっているという条件を加えました（**図3**）．

この構成で出力から入力を求める問題が，今回のアルゴリズムの対象です．これは構造のないNP探索問題といえます．古典計算機では解決に多大な処理が必要なのに対し，NTTが考案した量子アルゴリズムを使えば，処理量の増大に対して古典計算機と比較して指数関数的に高速に解を求められることを，数学的に示すことができました．そして出した答えの検証は，古典計算機でも簡単に実行できます．つまり，図1に示した3条件をすべて満たせるのです．



(a) 自然数の累乗の余り（周期性あり）　(b) ハッシュ関数の出力（周期性などの構造なし）

図2　構造の有無による関数の出力の違い

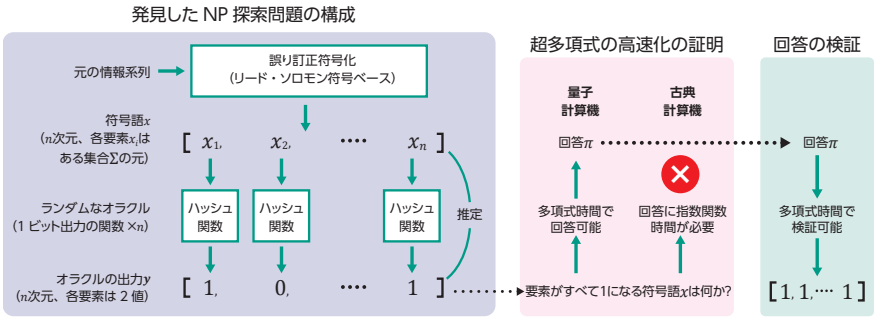


図3　対象とするNP探索問題と証明・検証の方法

次の目標は実用化

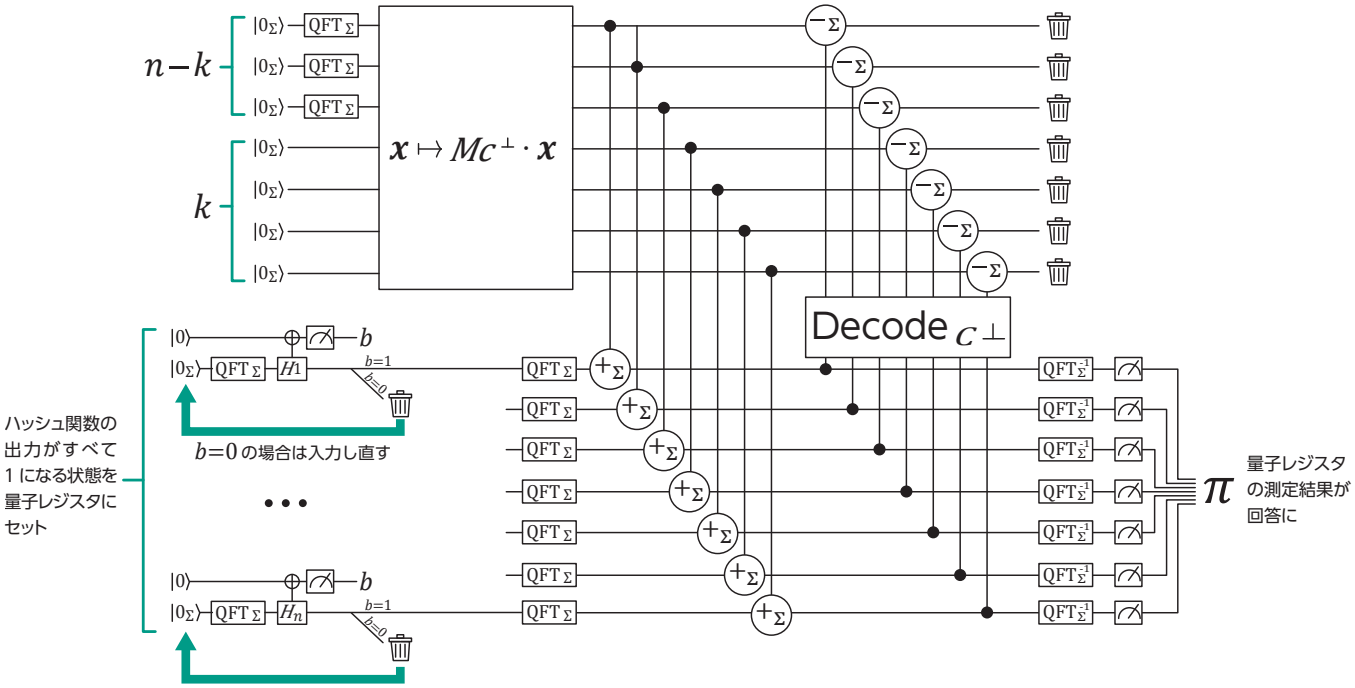
図4が，考案したアルゴリズムを示したものです．量子計算機では，アルゴリズムを量子ゲートと呼ばれる回路の組合せで表すことが普通で，この図もそれにならっています．本稿では詳細を説明できませんが，高速化のポイントの1つが図中の「QFT」で示される量子フーリエ変換にあるとはいえます．ただしShorのアルゴリズムとは異なり，出力の周期のような構造を見つけるために使っているのではありません．

では，このアルゴリズムはどのような用途の役に立つのでしょうか．実は，今回解いた問題はあくまでも量子計算機の可能性を探るためのもので，具体的な応用はありません．本成果が示した新たな方向で，現実的な問題を解くアルゴリズムを探ることは，NTTも含めた世界中の研究機関の大きな課題です．

Shorのアルゴリズムを開発した

*4　ハッシュ関数：入力した数値を別の数値に変換する関数．暗号分野で標準的に利用されるハッシュ関数「SHA-2」などの例があります．

*5　誤り訂正符号：伝えたい情報系列を冗長性のある情報系列に変換して，通信の途中で一部の情報が欠落しても元の情報を再現できるようにする技術．今回はFolded Reed Solomon codeと呼ばれる技術を利用しました．



x：符号語（$x \in C$）　C：符号（符号語全体の集合）　n：Cの長さ（xの次元数）　k：Cの階数　$|0_\Sigma\rangle$：Σ中の0に対応する状態　QFT$_\Sigma$：量子フーリエ変換
$C^\perp$：Cの双対符号　$n-k$：$C^\perp$の階数　$M_{C^\perp}$：最初の$n-k$列が$C^\perp$の基底ベクトルである任意の正則行列　H_i：i番目のハッシュ関数　b：量子ビットの測定結果
Decode$_{C^\perp}$：$C^\perp$の復号器　$+_\Sigma$：重ね合わせ状態の加算　$-_\Sigma$：重ね合わせ状態の減算　QFT$_\Sigma^{-1}$：量子フーリエ逆変換　π：回答（量子レジスタの測定結果）

図4　回答を計算する量子アルゴリズム

Peter Shorは，Daniel R. Simonsがある会議に投稿した論文が大きなヒントになったと振り返っています(7)．論文が示したアルゴリズムは非現実的な問題を対象にしたもので，プログラム委員会の一員だったShorの支持にもかかわらず，採択は却下されてしまいました．NTTの論文は幸いにも著名な国際会議で発表できました．論文を読んだ多くの研究者の中から，次なるShorのアルゴリズムが登場することを期待しています．

■参考文献

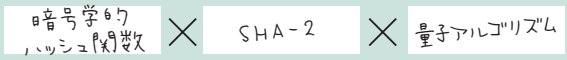
(1) T. Yamakawa and M. Zhandry：“Verifiable Quantum Advantage without Structure,” Proc. of FOCS 2022, pp. 69-74, Nov. 2022.
(2) S. Aaronson：“How Much Structure Is Needed for Huge Quantum Speedups?,” Sept. 2022. https://doi.org/10.48550/arXiv.2209.06930
(3) P. W. Shor：“Algorithms for Quantum Computation: Discrete Logarithms and Factoring,” Proc. of FOCS 1994, Nov. 1994.
(4) https://www.quantamagazine.org/quantum-algorithms-conquer-a-new-kind-of-problem-20220711/
(5) S. Aaronson：“BQP and the Polynomial Hierarchy,” Proc.of STOC 2010, Cambridge, U.S.A., pp. 141-150, June 2010.
(6) C. Gidney and M. Ekerå：“How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits,” Quantum, Vol. 5, p. 433, April 2021.
(7) P. W. Shor：“The Early Days of Quantum Computation,” Aug. 2022. https://doi.org/10.48550/arXiv.2208.09964

山川 高志

量子計算はまだ比較的新しい分野で，未解決問題の宝庫です．皆さんもこの分野の研究に取り組んでいただき，ぜひ私たちの提案したアルゴリズムの有用な応用を見つけてください．

◆問い合わせ先

NTT社会情報研究所
企画担当
E-mail　solab＠ml.ntt.com



量子計算機を用いた攻撃に対するハッシュ関数の安全性のより良い理解へ向けて

「SHA-2」は世界中で幅広く利用されている暗号学的ハッシュ関数です．量子計算機を悪用した攻撃の可能性が無視できなくなってきた昨今，量子計算機の出現がSHA-2の安全性にどのような影響を及ぼし得るのか，しっかりとした検証が必要です．研究を進めた結果，量子計算機を利用可能な世界では，SHA-2への衝突攻撃の攻撃可能段数が伸び得ることを世界で初めて示すことに成功しました．

ほそやまだ　あきのり
細山田　光倫

NTT社会情報研究所

SHA-2とは

大規模な汎用量子計算機が実用化されると，悪意のある攻撃者がそれを使って暗号技術を破ってしまうかもしれません．そうした攻撃に備えて，今のうちに，これまでの暗号技術がどこまで耐えられるのか，しっかりと検証しておく必要があります．

暗号技術の中でも「SHA-2」は重要なアルゴリズムで，普段PCやスマートフォンを使ってWebサイトを見る際にも使われ，高度情報化社会を裏から支えています．SHA-2は「(暗号学的) ハッシュ関数」の一種に分類される，NIST（米国国立標準技術研究所）標準の暗号技術です．ハッシュ関数は狭義の「暗号」ではないのですが，さまざまな別の暗号技術の一部に用いられたり，そのような暗号技術の安全性に深く関連していたりすることから，広義の「暗号技術」に含まれます*1．

狭義の暗号の主な役割は，メッセージを暗号化して内容を書くことです．当然ながら，(秘密鍵があれば) 暗号文を元のメッセージに戻せる必要があります．それに対してSHA-2のようなハッシュ関数hの役割は，メッセージMを入力してランダムな値h(M)を出力することであり，Mの内容を隠すことではありません．別々のメッセージMとM'のペアであってh (M) = h (M') を充たすようなものを「衝突」というのですが，安全なハッシュ関数とは，衝突を発見しようという攻撃に耐える（＝衝突耐性を持つ）ことが要請されます（**表1**）．

ここで与えられているのは，ハッシュ関数h*2のみです．攻撃者はとにかく何でも構わないので，h (M) = h (M') を充たすMとM'を見つければ「勝ち」です．その意味で衝突攻撃は「暗号文を解読する」のとは少し異なります．「暗号文を解読する」とは，(狭義の暗号で) 暗号化された暗号文が与えられて，元のメッセージを復元しようとする攻撃だからです．

なお，「衝突攻撃にどれだけ耐える

表1　狭義の暗号と暗号学的ハッシュ関数の違い

	狭義の暗号	暗号学的ハッシュ関数
機能	①メッセージを暗号化し，暗号文に変換する ②秘密鍵があれば暗号文を元のメッセージへ戻す	メッセージMを入力すると，ランダムな値h(M) を出力する
安全性	①暗号文から元のメッセージが推測できない ②その他，識別困難性など（詳細略）	①別々のメッセージMとM'であってh (M) = h(M') を充たすようなもの（これをhの衝突と呼ぶ）を見つけるのが非常に困難．衝突を見つけるという攻撃に対する耐性がある（＝「衝突耐性」） ②その他，原像計算困難性など（詳細略）

*1　実用的なハッシュ関数の設計は，主に（狭義の）共通鍵暗号の設計技術を流用することが多いことから，共通鍵暗号技術に含められます．

*2　より正確には，hを計算するアルゴリズム．

か」といっても限界があります．この限界を説明する重要な概念が「誕生日のパラドックス*3」です．この概念を応用すると，nビット出力のハッシュ関数の衝突を計算量$2^{n/2}$で発見できる，ということが分かります．誕生日攻撃は，ハッシュ関数がどれだけ安全でも適用できる汎用的な攻撃なのです．

ひるがえって，（古典計算機を用いた攻撃に対して）安全なハッシュ関数は，計算量$2^{n/2}$を掛けないと衝突が発見できないことが要請されます．例えば，とあるハッシュ関数の衝突を$2^{n/2}$未満の計算量で発見する専用攻撃の存在が分かった場合，その関数には特有の弱みがあって破られた，とみなされます．いわば，誕生日攻撃の計算量$2^{n/2}$は，特定のハッシュ関数を対象にした専用の攻撃が意味のある攻撃かどうかの判定基準になっているのです．

SHA-2の安全性指標

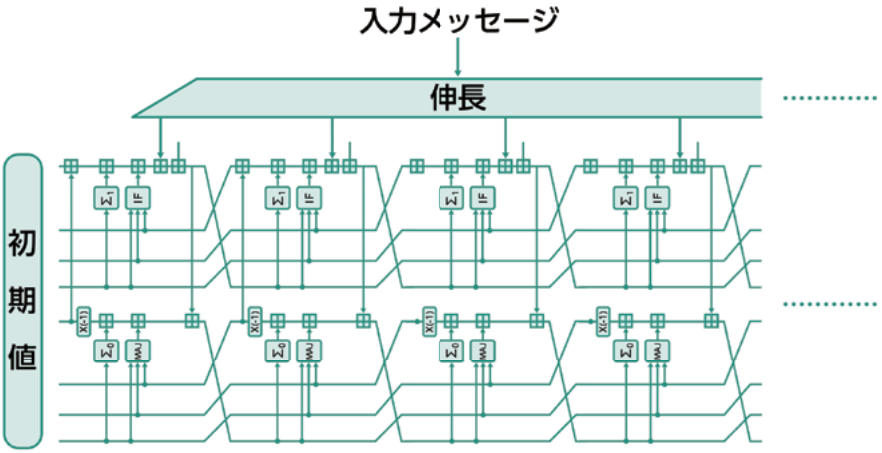
具体的には，SHA-2が出力を計算する仕組みは，次のとおりです．まず，入力されたデータが，大量の「メッセージブロック」の列に伸長されます．各メッセージブロックは，内部状態の値を更新させるのに使用されます．初期状態からスタートしてメッセージブロックを用いて内部状態を繰り返し何度も変化させることにより，最終の出力（ハッシュ値）が計算されます（**図1**）．

このように，SHA-2をはじめ，典型的なハッシュ関数の設計は，似たような処理を何段も繰り返し，一般にこの処理回数を減らせば減らすほど，安全性は弱まります．そのため，手掛かりが何もないような状況から何の予兆もなく天才的な攻撃方法が突然発見されるようなことは，滅多に起こりません．したがって，安全性を測る指標は「どこまで弱めれば破れてしまうか」という考えになります．

例えば，元のハッシュ関数が10回の処理を繰り返す構造をしていたとして（**図2**左），「この処理回数を6段まで減らせば$2^{n/2}$より小さい計算量で衝突が見つかってしまう」ということが分かるのであれば，その関数は6段まで破れてしまう，という言い方をします（図2右）．

また，本来の元の段数まで破られたとき，そのハッシュ関数は破れたことになりますが，元の段数に達していなくても，破られる段数が伸びれば「意味のある攻撃」とみなすことができます．

このように，その道のプロが注意深く設計したハッシュ関数が破れる際は，多くの場合，破れる段数が徐々に伸びていって，最終的に元の段数が破れる，という経過を多くの場合たどります．



※本来はさらに終了処理がありますが，ここでは割愛します．
なお，段関数の表現はMendelらの論文[1]によります．

図1　何段も更新を繰り返し，最終のハッシュ値を出力

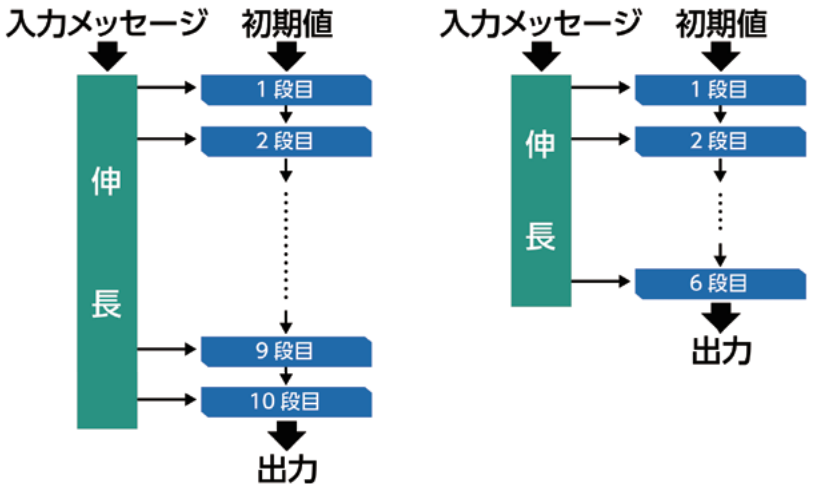


図2　元の段数が「10段」あるハッシュ関数への攻撃（左），
元の段数が「10段」あるハッシュ関数への，元の段数よりも少ない段数への攻撃（右）

*3　誕生日のパラドックス：ある人の誕生日は365通りあるはずだが，20人程度ランダムに人を集めて誕生日を聞くと，かなり高い確率で同じ日が誕生日のペアが見つかるというもの．

「世界中の研究者がよってたかって攻撃を試みたが，かなり弱めないと攻撃が成功しない」という事実が，ハッシュ関数の安全性を担保しているのです．

ハッシュ関数は量子計算機でも早々破れないのか

SHA-2のようなハッシュ関数は素因数分解のような綺麗な代数的構造を持たないため，量子計算機ができたからといってすぐに破れるようになることはないだろうと考えられてきました．唯一，汎用衝突攻撃*4の計算量が誕生日攻撃の$2^{n/2}$から$2^{n/3}$にまで落ちることは判明していました（＝BHTのアルゴリズム）．ただし，下げ幅がそれほど大きくないこともあり，「特段問題ないだろう，あるいはnが少し大きいハッシュ関数を使えば良いだろう」と受け止められてきました．

ところが研究を進めてみると，事態はそう単純ではありませんでした．まず，「AES-MMO」や「Whirlpool」といったハッシュ関数については，量子計算機によって1段多く破られることが分かりました（**表2**）．これまで堅牢であった暗号に対して，量子計算機は明らかに古典計算機よりも破る力があるのです[(2)]．

攻撃可能段数の伸びについては，「汎用衝突攻撃の計算量がさほど落ちない一方，特定のハッシュ関数をターゲットとした専用攻撃の計算量が落ちる幅はより大きくなることがあるため，専用攻撃の威力は相対的に高まる可能性がある」という考え方が根底にあります．例えば「グローバーのアルゴリズム」という量子アルゴリズムを使うと，専用攻撃によく使われる「差分解読法」の計算量は元の平方根程度まで落ちる可能性があることがすでに分かっていました[(3)]．一方，汎用衝突攻撃の計算量はBHTのアルゴリズムより下がらないことが証明されており，計算量が落ちる幅は元の平方根までには至りません（**表3**）．

これまでみてきたように，ハッシュ関数の（古典的な）安全性評価指標の1つは，段数をどこまで削れば破れるかということでした．そして特定の段数まで段数を削ったハッシュ関数への専用攻撃が有効かどうかは，その攻撃の計算量が汎用攻撃の計算量を下回っているかどうかで判定されていました．量子計算機が利用可能な世界では，攻撃成立の判定基準となるべき汎用攻撃の計算量がさほど変わらない一方，専用攻撃の計算量が相対的に下がるため，古典の世界よりも有効だと判定される専用攻撃の種類が増えると結論付けざるを得ないわけです．

量子計算機が利用可能な想定下で，そうした「基準」をどうとらえるべきかに着目した研究がない中で，7段AES-MMOや6段Whirlpoolへの衝突攻撃が，古典的には有効と判定されないにもかかわらず，量子計算機を利用可能な世界では有効と判定され，前述の着眼点の重要性を実証する具体例となりました．

量子計算機によるSHA-2への攻撃

ただし，AES-MMOやWhirlpoolといったハッシュ関数は，SHA-2と比べるとマイナーで，利用シーンもかなり限られています．そこで，現在もっとも広く使われているハッシュ関数であるSHA-2でも攻撃可能段数が伸びるのか，という疑問が自然と出てきます．これが今回の最大のテーマです．

そして実際に検討を重ねたところ，やはり段数が伸びるという結果が得られたのです．「SHA-2」は実は総称で，出力長が違ういくつかの関数が含まれているのですが，このうちのSHA-256やSHA-512について，古典的には有効でないが量子計算機のある世界では有効と判定される攻撃を見つけました[(4)]．

SHA-256は64段の処理を行っていますが，古典計算機を用いた場合，衝突耐性としては31段まで減らして弱めれば破られることが知られています．つまり，32回以上の処理が行われた際に衝突耐性を破るような攻撃は見つかっていませんでした．ところが，量子計算機が利用可能な世界では，38回程度でも衝突耐性が破れてしまうこと

表2　量子計算で破れる段数（AES-MMOとWhirlpool）

攻撃	元の段数	古典計算で破れる段数	量子計算で破れる段数
AES-MMO	10段	6段	7段
Whirlpool	10段	5段	6段

表3　汎用衝突攻撃と差分解読法と計算量の落ちる幅の違い

攻撃	古典	量子	スピードアップ
汎用衝突攻撃	$2^{\frac{n}{2}}$	$2^{\frac{n}{3}}$	元の平方根まで落ちない
差別解読法	T	$\sqrt{T}$	元の平方根まで落ちる

※正確には汎用衝突攻撃の計算量は計算モデルによって異なりますが，本稿では詳細は割愛します．

*4　汎用衝突攻撃：誕生日攻撃のように，どれだけ安全なハッシュ関数にも適用できる衝突攻撃．

表4　古典計算と量子計算で破れる段数の違い（SHA-256とSHA-512）

攻撃	元の段数	古典計算で破れる段数	量子計算で破れる段数
SHA-256	64段	31段	38段
SHA-512	80段	27段	39段

※古典攻撃で破れる段数は参考文献(5)，(6)を参照．

が分かったのです．つまり，量子計算機はSHA-2の安全性に影響を及ぼすといえるわけです．SHA-512についての結果も，基本的には同様です（**表4**）．

もちろん，この結果から直ちにSHA-2の衝突耐性が破られた，ということにはなりません．まだまだSHA-2は安全に使えます．しかしこの結果は，量子計算機はSHA-2の安全性にさほど影響を及ぼさないのではないかという従来の大雑把な見方は改めるべきだ，ということをはっきりと示しています．

今後の展開

ほんのわずかな期間で情報通信技術は急速な進化を遂げ，それに伴い，セキュリティの要となる暗号技術もしっかりと整備されてきました．その結果，誰もが利用できる世界中で共通の国際標準の暗号技術が打ち立てられています*5．これまでも何度となく，それまで用いられていた暗号技術の脆弱性が指摘され，早い段階でより強固な暗号を開発してきた歴史がありますが，量子計算機を想定した攻撃の研究については，まだまだ研究すべきことがたくさんあります．

社会で極めて重要な役割を果たしているSHA-2の安全性についてさえ，これまでよく分かっていなかったのですが，量子計算機が利用可能な世界では破れる段数が伸びると結論付けざるを得ないことが今回示されました．

今後も，未知の攻撃がないか探究を続けていく必要があります．こうした攻撃の研究で得た知見がフィードバックされれば，今後，より安全なハッシュ関数が設計されることになるでしょう．また，こうした攻撃の研究を公にすること自体が，もっと世の中の安全性を高めてゆくことにつながっていると思います．攻撃側もすでにこっそりと同じような研究をしているかもしれませんので，さらにその先を見越して，量子計算機による攻撃を想定し，それに十分耐えられる暗号をつくることがめざされます．どうしても日常生活の感覚とは異なる次元の問題ですから，なかなか実感がつかみにくいかもしれませんが，量子計算機が実用化される中では，こうした問題を攻撃者に先立って検討することが要請されます．

各暗号技術をターゲットとする専用の攻撃自体は，その暗号技術の内部構造をフルに利用しているため，他の研究への応用はあまり考えられません．しかし暗号技術の安全性は私たちの日常の暮らしと密接に関連していることから，広範に興味を持ってもらえるのではないかと期待しています．

*5　近年の量子計算機の急速な発展状況を受けて，NISTは耐量子暗号技術，特に公開鍵暗号（およびKEM）や電子署名の標準化作業に取り組んでおり，世界中から幅広い方式が集まっています．2023年1月の時点で選考はすでに一部が終わり，標準化されることが決定したものもあります．

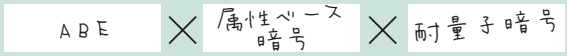
■参考文献

(1) F. Mendel, T. Nad, and M. Schläffer: "Finding SHA-2 Characteristics: Searching through a Minefield of Contradictions," ASIACRYPT 2011,Proc. of LNCS, Vol. 7073, pp. 288-307, 2011.
(2) A. Hosoyamada and Y. Sasaki: "Finding Hash Collisions with Quantum Computers by Using Differential Trails with Smaller Probability than Birthday Bound," EUROCRYPT 2020, Proc. of, Part II. LNCS, Vol. 12106, pp. 249-279, May 2020.
(3) M. Kaplan, G. Leurent, A. Leverrier, and M. N. Plasencia: "Quantum differential and linear cryptanalysis," IACR Trans. Symmetric Cryptol. 2016 (1) , pp. 71–94, 2016.
(4) A. Hosoyamada and Y. Sasaki: "Quantum Collision Attacks on Reduced SHA-256 and SHA-512," CRYPTO 2021, Proc. of, Part I. LNCS, Vol. 12825, pp. 616–646, 2021.
(5) F. Mendel, T. Nad, and M. Schläffer: "Improving Local Collisions: New Attacks on Reduced SHA-256," EUROCRYPT 2013, Proc.of LNCS, Vol. 7881, pp. 262-278, 2013.
(6) C. Dobraunig, M. Eichlseder, and F. Mendel: "Analysis of SHA-512/224 and SHA-512/256," ASIACRYPT 2015, Proc.of Part II. LNCS , Vol. 9453, pp.612-630, 2015.

細山田　光倫

複雑に入り組んだハッシュ関数アルゴリズムの性質を調べ，攻撃の糸口をつかむといった作業は，パズルを解くプロセスと似ています．パズルが好きな方は，ぜひ，こうした暗号攻撃の研究に関心を持ってもらいたいと思います．

◆問い合わせ先
NTT社会情報研究所
企画担当
E-mail　solab＠ml.ntt.com



暗号とアクセス制御を組み合わせる革新的な属性ベース暗号（ABE）技術の最新動向

NTT Research, Inc. において取り組んでいる，暗号技術と属性によるアクセス制御を組み込んだ属性ベース暗号「ABE」に関する研究の論文を解説します．ABEはオフライン環境でも設定された属性に基づいて復号可能なデータを制御できる画期的な技術です．高効率なスキームや耐量子暗号への対応など，最新の技術動向を紹介するとともに，技術の普及に向けた活動についても紹介します．

Yannis Rouselakis

後藤（ごとう）　隆（たかし）

NTT Research, Inc.

はじめに

誰もがセキュアなデータにアクセスした経験があるでしょう．その場合，パスワードと，おそらく，別に生成されたパスワードとは異なるセキュリティコードを入力する必要があります．これらが認証されればセキュアなサーバによって，データが送信されます．

この流れの裏では，もっとさまざまなことが起きています．例えばパスワードは，通常，鍵導出関数によって鍵に変換されます．公開鍵とそれに対応する秘密鍵のペアは，今日の一般的なセキュリティモデルである公開鍵暗号（PKE：Public Key Encryption）の中核を成すものです．しかし，それだけではありません．2004年，2人の暗号技術者が，従来のPKEを一般化した形式で，ユーザのポリシーや属性に基づいてデータを共有する方法を発表しました．属性ベース暗号（ABE：Attribute-Based Encryption）と呼ばれるこのアプローチは，専門家がその可能性の探求を続けている段階であるにもかかわらず，商用利用が始まっています．業界のリーダーたちは新たな用途を見出し，暗号技術者は最適化された，より安全な暗号化構造を構築しています．

従来のデータセキュリティに加えて，ABEは継続的な研究成果の下，新たなデータセキュリティの手法として浮上しています．研究成果には，ABEの効率の良い実装に関する論文と，量子計算機に対して安全と思われるABEに関する論文という，NTTが関係する2つの論文が含まれます．暗号理論に裏打ちされ，ABEの魅力的なアプリケーションの数も増えてきています．

歴史と定義

Amit Sahai博士とBrent Waters博士は，暗号研究に関する国際会議「Crypto 2005」において，論文の一部として，ABEを初めて発表しました．SahaiとWatersは，IDベース暗号（IBE：Identity-Based Encryption）と呼ばれる以前の方式に基づき，アイデンティティを記述的な属性の集合ととらえることを提案しました．この新鮮な発想が，新たな可能性を生み出したのです．

従来の暗号は，特定の者をターゲットにして，「全」か「無」かのアクセスを提供するものでした．それに対して，ABEはより詳細なアクセス制御を組み込み，ユーザのポリシーや属性に基づいて暗号化されたデータ（暗号文）を共有することができます．ユーザが属性「X」の秘密鍵を要求した場合，暗号機関では，このユーザが本当に属性「X」を持つか，持つ資格があることを検証します．この検証を行うのは，従来の認証システムです．データを復号化する際には，ユーザの属性が暗号文に数学的に組み込まれたポリシー（条件式）に合致しているか，「暗号処理の内側」で行われ，暗号文の復号は，ユーザ鍵の属性が条件式と一致する場合にのみ行われます．

SahaiとWatersは，共著の論文の中で，大学の学科長が採用委員会メン

バ向けの文書を暗号化したいという仮想のケースを用いて，ABEの説明を行いました．この場合，ABEは，「採用委員会」「教員」「学問の専門性」といった属性から構成されるアイデンティティを暗号化することになり，すべての属性を含むアイデンティティを持つユーザであれば，文書を復号化することができます．

この論文によって，より柔軟で，きめ細かな暗号化モデルという考え方が根付いたのです．この論文は，2020年までに何千回も引用されるようになり，同年，国際暗号学会（IACR）のTest of Time Awardも受賞しています．2019年にNTT Research, Inc.に入社したWatersは，2022年，岡本龍明フェローの後任として，NTT Research, Inc. Cryptography and Information Security Laboratories（CIS研）のDirectorに就任しました．

最近の論文

ときが経つとともに，さまざまな特性を持つABEの方式が研究されてきています．これらの多くの方式を1つの方式としてまとめることができるでしょうか．

これを成し遂げたのが，ルール大学ボーフムのDoreen Riepel博士とNTT ResearchのHoeteck Wee博士の共著の論文『FABEO：Fast Attribute-Based Encryption with Optimal Security』です（Riepelは，CIS研で研究インターンシップに参加しながら，本研究の一部を完成させました）．両博士は，汎用版のABEの可能性を示すと同時に，他の大多数のABEアルゴリズムよりも優れた性能を実現しました．FABEOの4つの特性を紹介します．

■表現力（Expressiveness）

選択したポリシーと属性で，条件を多様に表現できます．想像し得るあらゆるポリシーを実現するのが，ABEの黄金律であるモノトーンスパンプログラムと呼ばれる技術で，秘密を複数に分割し，再分配し，共有することができます．モノトーンスパンプログラムとは任意のブール式，例えば“（A OR B）AND（C AND（X OR Y））”のようなものです．以前の方式ではORのみ，ANDのみ，ORのANDのみ，などの使用の制限がありました．本特性は，4つの特性の中でもっとも重要な特性といえ，ABEがより実用的に利用できるようになっています．

■無制限なサイズ（No limits on size）

鍵や暗号文に付加するポリシーと属性のサイズの制限がありません．最初のABE方式では，Sahai，Watersの共著の論文の例を挙げると，「採用委員会」「教員」「専門性」という属性を含めることができますが，属性の数が3つなど一定の上限を超えると，安全性に欠けていました．この特性は，表現力に関係するもので，10，20，あるいは，それ以上の数の属性を持つことができます．

■大領域の属性（Large attribute universe）

好みの属性を使用することができます．最初の方式では特定の属性のみが使用可能でしたが，この特性によって，ランダムな文字列，名前，日付と時刻，その場でつくった単語など，何でも属性として使用することができます．より細かなアクセス制限が可能となります．

■適応的安全性（Adaptive security）

この特性は実質的に，私たちが証明できるもっとも強いセキュリティの概念を満たしています．適応的安全性では，仮想の攻撃者の能力を高めることで，結果として自分たちの方式がより強いということを証明できます．例えば，攻撃者は複数の秘密鍵を要求し，暗号文の内部に深く入り込み，秘密鍵について学んだことに応じて適応することができる能力を持つと想定します．これは現実世界の脅威のシナリオによく似ています．

これらの特性を実現することに加えて，RiepelとWeeは，FABEOシステムを非常に効率的に設計し，双線形ペアリング楕円曲線に正確に当てはめました．これまでの楕円曲線の構築においては，いくつかの操作の相対的な速さを考慮していないことが問題でした．楕円曲線は数学者の創造物です．暗号技術者は，楕円曲線という道具箱に何が入っているかはあまりコントロールできませんが，道具を選び，その使い方を決めることはできます．

最近の別の論文『Decentralized Multi-Authority ABE for DNFs from LWE』では，NTT Researchの Pratish Datta 博　士，Ilan

Komargodski博士，Brent Waters博士が量子計算機の脅威に言及しています．著者らの成果は，耐量子の計算難度が高いともっとも広く信じられている誤差を伴う学習（LWE：Learning With Errors）仮定から，分散型のマルチオーソリティMA-ABEを初めて構築したことです．また，本方式は，自動定理証明に有用なDNF（Disjunctive Normal Form）式で表されるアクセスポリシーをサポートしています．

暗号システムの安全性を証明するには，特定の数学的予想が必要です．今後の目標は，量子の世界で通用するシステムを構築することで，ノイズの下で線形方程式を解く問題であるLWEは，そのような予想の1つです．著者らはLWEから最初のMA-ABEを構築する過程で別のものを達成しました．それが，以前の方式で使用していた非常に非効率な変換を必要としない，最初の暗号文ポリシー（CP：Ciphertext Policy）シングルオーソリティABEです（注：ABEは，条件がデータに埋め込まれたCPと，条件が鍵に埋め込まれたキーポリシーのいずれかの形態をとります）．

著者らが，マルチオーソリティではなくシングルオーソリティのABEを最初に構築したのは，それがマルチオーソリティ化のために必要だったからです．LWEから構築したこれまでのCP ABE方式では，普遍的な回路ベースの変換を使用していましたが，これは，MA-ABEの設定で使用するには非効率的で非実用的なものでした．シングルオーソリティCP ABEの構築では，複数の秘密鍵を集める共謀を防ぎ，ポリシーを少数のパラメータで符号化しなければならない，という2つの課題をクリアする必要があり，しかも，現状の変換技術を使用せずにそれを実現する必要がありました．

これらの課題を克服するため，2つの技術を改良しました．1つは再構成係数が小さく線形独立性が保証された新しい線形非単調秘密分散方式（LSSS）の設計です．LSSSは秘密パラメータをエンコードするためにさまざまな暗号構造で採用されている線形代数手法です．もう1つは，LSSSの性質を利用し既存の構成と証明方法をLWEに適応させることです．LWE仮定を用いることで実用的な暗号化方式を構築し，2つの課題の克服に成功しました．

シングルオーソリティを経てマルチオーソリティのCP ABEに移行するには，さらに2つの課題を克服する必要がありました．秘密鍵の共謀を回避し続けるために，鍵どうしを結びつける公開ランダム性を用いて実現しました．そして，1つのオーソリティで鍵を生成するための条件として，セットアップと鍵生成アルゴリズムにおいてモジュール性を実現する必要がありました．そうでなければ，マルチオーソリティとはいえません．シングルオーソリティの設計時にこの2つの課題を特に意識して設計したため，自然にマルチオーソリティに拡張することができました．

なおマルチオーソリティは，以下に述べる方式を考えるうえで自然な方法と考えられています．例えば，職業と国籍（例，「医学博士」と「アメリカ人」）に基づいて暗号化を行いたい場合，性質の異なる2つの属性を持つことになります．病院や大学の誰かが，あなたが医師であるかどうかを確認することはできますが，国籍を確認するには，政府当局の助けが必要です．これらの機関を組み合わせ，すべてをチェックする（さらに，機密データを共有する）ことができる集権センタを配置することは非現実的です．そのためマルチオーソリティの仕組みが必要になります．

勢いを増すABE

前述の両論文は，ABEの進化を支えています．FABEO論文は，最適な機能を網羅したABEの構築が可能であり，より実用可能性が高まりました．LWEからMA-ABEを構築した論文は，耐量子ABEの大規模な実用化に一歩近づいた技術です．実際，NTT Researchの技術推進チームは，この論文の耐量子ABEの初期実装をすでに終え問題のない動作を確認していますが，今後はより高速で効率的な実装に取り組んでいきます．

NTT Researchは，基礎研究を重視する一方で，開発した研究コンセプトの製品化を支援する「技術推進チーム」を設置しています．本チームは，ABEがヘルスケア，医療，金融，教育，政府などの分野におけるセキュリティやプライバシのニーズに対応できると考え，NTTの事業会社と協議を重ね

てきました．2021年，NTTは，シドニー工科大学（UTS）と，UTSの内部システムをよりセキュアにすることを目的としたABEの概念実証プラットフォームの構築を含む契約を締結したと発表しました．また，ABE暗号方式は，ETSI（European Telecommunications Standards Institute）による標準化の支援を得ています．

2022年，NTT Researchは，2週間にわたるABEハッカソンを開催し，世界中から5つのNTT関連チームが集まりました．優勝したベルギーのNTTチームは，ロゴ，顔，ナンバープレートなど人物を特定できる情報を含む画像のパーツやGPS情報を含むメタデータにABEを適用するという新たな手法のデモンストレーションを行いました．同チームは，スキャンした医療文書やテストの回答など，写真画像のみならず個人情報保護の対象となる他の画像にも同様にABEを適用できる可能性があることを示しました．

他のデモは，残りの4カ国のNTTチームが作成したもので，以下のユースケースが紹介されました．

- 金融（インド）：銀行システムを，単一の要素に基づいてアクセスを許可または拒否する役割ベースのアクセス制御（RBAC）システムから，ABEを使用した，より繊細な制御へと移行
- 公共交通機関（イタリア）：ローマの新交通サービスにABEを導入し，チケット購入と物理的アクセス制御を支援
- 通信（日本）：ABEを使用した，プライバシが保護された通話ソリューションの導入により，適切な場所にいる，適切な役職のスタッフや，緊急通話の必要があるスタッフが，従業員の個人携帯番号に電話をかけることができる
- 個人データ（ルーマニア）：ABEを使用して，自動車の電子センサ上でセキュアなIoT（Internet of Things）プロトコルを実現し，自動車のオーナーがデータの収益化オプションを制御できる

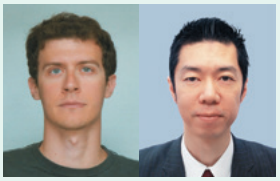
同ハッカソンでは，アクセスが容易で，HTTPエンドポイントの役割を果たし，鍵を使用して暗号化，復号化を行い，ソリューションをすばやく試作することができるWebツール「ABE Resolver」が利用できることも確認されました．

今後の展開

Watersによると，ABEは，長年にわたりさまざまな結果をもたらしてきました．まず，アプリケーション単体としてのABEがあります．さらに，他の暗号システムを構築するためのコンポーネントとしてのABEがあり，研究コミュニティにも大きな影響を与えてきています．第三に，ABEの「精神と概念」があり，関数暗号など他の暗号技術に影響を与えています．

ABEそのものについては，ユースケースは急増しています．開発ツールへのアクセスが容易なことも，このトレンドを後押ししています．今後，さまざまな状況で商品化が行われるでしょう．ほとんどの用途に最適で，非常に高速な，ABEのベースバージョンが登場すると思われます．また属性を秘匿可能なABE，耐量子セキュリティ，そして付加機能を持つものなど複数のABEが登場すると思われます．

ポスト量子環境の到来には何年もかかるかもしれませんが，この分野における私たちの活動は，私たちがABEの長期的な展望をどう見ているかを示す良い指標となると考えています．この革新的な暗号化手法の背景には20年近い歴史があり，私たちは，さらに長く耐えられるソリューションを準備していきます．



（左から）Yannis Rouselakis/
後藤　隆

NTT Research, Inc.は，暗号技術のほか，Quantum Computing，Bio Digital Twinなどの基礎研究にフォーカスしたアメリカ・カリフォルニアにある海外研究所です．NTT Research, Inc.の現実をアップグレードする，Upgrade Realityを実現する研究活動にぜひご期待ください．

◆問い合わせ先
NTT Research, Inc.
Technology Promotion Team
E-mail　tech_promotion @ ntt-research.com

主役登場

古典計算機では不可能な暗号技術を実現する量子力学の力

西巻　陵
NTT社会情報研究所
特別研究員

暗号技術が達成する安全性は大きく分けて２種類あります．１つが情報理論的安全性であり，無限大の計算能力があっても破られることがない安全性です．もう１つは計算量的安全性であり，現在の計算機では破ることが難しいとされている安全性です．可能ならば情報理論的安全性を達成できるほうがもちろん望ましいです．しかし，公開鍵暗号に代表されるように多くの暗号技術において情報理論的安全性を達成することは不可能です．また，情報理論的安全性を達成できる暗号技術であっても，効率が非常に悪いことがほとんどです．ここでは，情報秘匿のための暗号の話だけに焦点を当てます．

１つの妥協点として考えられたものが，暗号文を消去することで消去した後は，無限大の計算能力をもってしても暗号を解読することができない消去証明可能暗号と呼ばれる暗号技術です．つまり，暗号文が消去される以前は計算量的安全性を達成し，消去後は情報理論的安全性を達成しています．仮に計算機の能力が将来飛躍的に向上するか，あるいは全く新しい革命的なアルゴリズムが生まれたとしても，暗号文を消去さえすればどうやっても解読できないので現実的な折衷案といえます．

問題はそのような暗号文の消去が実現できるかということです．これは古典計算機では不可能な暗号技術であり，量子計算機を利用することで初めて実現可能になります．量子力学の不確定性原理は，ある物理量Ａと別の物理量Ｂ（代表的なものは位置と運動量）について２つを同じくらいの正確さで測定することはできない，という原理です．これを応用することで，暗号文の消去（つまり含まれていた平文の情報消去）を実現することができます．消去証明可能暗号では，平文から量子状態の暗号文を生成します．平文の情報（仮にＸとする）に関する正確さが一定以上下がるような情報量（仮にＹとする）を，量子状態の暗号文から観測させることによって暗号文を消去することが可能になります．暗号文を生成したときに付加的に生成される検証用の情報を使って，情報量Ｙをチェックすることで暗号文を確かに消去したことを確認できます．量子状態の観測は不可逆的な操作なので，観測を行うと元の量子状態の暗号文は復元できません．このように量子力学の原理を応用することで古典計算機では実現できない高い安全性を持つ暗号技術を実現できます．

最近の私の研究で，このような消去証明可能な公開鍵暗号方式やさらに公開鍵暗号の発展形である関数型暗号について消去証明可能な方式を設計しました．古典計算機では実現不可能な暗号技術として，ほかには暗号文がコピー不可能な暗号などもあります．私はこの量子力学の強大な力に魅せられ，消去証明可能暗号をはじめとする古典計算機では実現不可能な暗号技術の実現のために研究に取り組んでいます．

特集

NTTデータ 先進技術特集

本特集では，2023年１月24～25日にNTTデータが実施したイベント「NTT DATA Innovation Conference 2023」で紹介した技術のほか，NTTデータの先進技術を紹介する．

NTT DATA Advanced

Technologies

顧客との共創に向けたグローバルでの先進技術の取り組み

古川（ふるかわ） 洋（ひろし）[†1]
Pietro Scarpino[†2]
Theresa Kushner[†3]
NTTデータ[†1]
NTT DATA Italia[†2]
NTT DATA Services[†3]

2023年1月24～25日にNTTデータが実施したイベント「NTT DATA Innovation Conference 2023」において，技術革新統括本部 技術開発本部イノベーションセンタ（イノベーションセンタ）のセンタ長と，イノベーションセンタ欧州および北米拠点の責任者が，グローバルでの先進技術に関する取り組みや，その成果を基にした顧客との共創R&D活動について発表を行いました．本稿では，各講演の概要をとおしてイノベーションセンタの取り組みを紹介します．

イノベーションセンタの位置付けと役割（講演者：イノベーションセンタ センタ長　古川 洋）

NTTデータが2022年4月に発表した新中期経営計画の5つの柱のうち，イノベーションセンタでは，「先進技術活用力」と「システム開発技術力の強化」を担当しています．

私たちの目標は，世界中から高度な先進技術を獲得し，先進技術を基に革新的なお客さまと共創R&D（研究開発）を実行することです．イノベーション活動の加速に向け，世界6カ国にイノベーションセンタの拠点を立ち上げました（**図1**）．各拠点において先進技術の成熟度を検証し，検証した技術が顧客事例として事業価値を生み出すかどうかを確認します．この取り組みにあたっては，それぞれの拠点が持つ特性を活かし，最大限効率化を図ることが重要です．また，イノベーションセンタ全体としての統合性を保つため，グローバルに点在する各イノベーションセンタが適用する活動プロセスを標準化することが必要だと考えています．

イノベーションセンタ　欧州拠点の取り組み（講演者：イノベーションセンタ 欧州拠点 責任者　Pietro Scarpino）

欧州では，特に量子コンピューティングと産業分野におけるメタバースに焦点を置いて活動を行っています．また，「変革（Transform）」，「専門性（Specialize）」，そして「つなぐ力（Glue）」という3つの戦略の柱を掲げています．

まず，「変革」について，私たちは，積極的な提案活動によりイノベーションによる価値創造を実現しようとしています．具体的には，人間中心のアプローチを使ってイノベーションを起こし，真にビジネスにつながる提案を行っています．次に「専門性」ですが，先進技術を提案する際には，お客さまの業界や個々のニーズを把握しておく必要があること，また，導入のメリットを理解いただけるよう，専門的に対応することを意識して進めています．「つなぐ力」については，私たちは，これまでお客さまとの共創に向けてたくさんの方々とワークショップを行い，技術によってビジネスを変革する方法を議論してきました．こうした活動では，各イノベーションセンタの拠点間における連携も必要です．さらに，スタートアップや研究機関とも連携を進めており，お客さまに私たちのケイパビリティ（能力や強み）を提示しています．つまり，私たちイノベーションセンタを活用いただくことで，さまざまな連携が進み，ビジネス上のひらめきを生み出すことができるのです．

これらを実現するための4つの要素があります．まず，革新的なソリューションを構築する「高度な専門性を持つ技術人財（テック・アドバイザリー）」です．テック・アドバイザリーは，「変革を起こす環境（Innovation space）」にて，お客さまのニーズを理解し，私たちが提供できる価値を示します．私たちは進め方も重要であると考えており，単にイノベーションの場を提供したり，技術力を示したりするのではなく，実用的なアプローチによりビジネスへの

図1　イノベーションセンタの方針と拠点

影響を及ぼしていきたいと考えています．また，システム部門など一部の部門だけではなく，関連する各部門の関与を促し，社内における組織間の壁を解消することも重要であるため，活動の初期段階から各部門のメンバを参画させ，関係を構築します．このように，十分に関係構築を行ったうえでお客さまと議論を重ね，先進技術を基に私たちの価値を提案し，ビジネスをこれまでとは異なるかたちで推進していきます．

「The space」は，先進技術を紹介することを目的とした新しいコンセプトのショールームです（**図2**）．お客さまだけでなく，同僚などさまざまなステークホルダが最先端の技術を体験することができます．「The space」では，欧州拠点の技術に加え，イノベーションセンタの他地域の拠点が取り組む技術も体験していただくことができます．私たちは，設立から9カ月でお客さま（主に経営幹部層）向けのイベントを90件以上開催しました．先進技術がどう未来につながるかを知っていただくためのもので，200人以上の方に参加いただき，すでに30件以上の共創の機会が生まれています．この取り組みには，10カ国以上がかかわっており，活動をとおしてグローバルなつながりを構築することができました．

私たちは，さまざまな企業や研究機関とパートナーシップ構想を進めており，技術系企業では，NVIDIAと戦略的パートナーシップを締結しました．こうしたパートナーシップを活用してデジタルツインや産業分野におけるメタバースの専門家である彼らとともにソリューション開発を行っています．私たちは，お客さまへの共同提案を開始しており，複数の活動をともに行う予定です．そのほかにも，メディア企業とパートナーシップを結び，活動を行っています．

次に，産業分野のメタバースに関して進行中の事例を紹介します．私たちは，公共，メディア，エネルギー，製造業，通信などさまざまな分野で活動を行っています．活動の基本にデジタルツインのコンセプトがあり，デジタルのレプリカ（複製）を作成しています．物理的なもの（物体や実体）と仮想的に作成したレプリカを組み合わせることにより，いろいろなユースケースが生まれます．

ある事例では，お客さまから，データセンタのレプリカを作成し，デバイスのデータをすべて統合したいという要望をいただきました．仮想的に作成したシステムをモニタリングすることで，物理的な振る舞いのシミュレーションを行いたいというものでした．私たちは，プラットフォームを使って，3Dの仮想的なレプリカをつくり，データセンタにあるすべてのものを双方向にシミュレーションすることを実現しました．本レプリカでは，細かな構成

図 2　「The space」の様子

部品までデジタル化されているので，詳細まで確認することができます．

イノベーションセンタ 北米拠点の取り組み（講演者：イノベーションセンタ 北米拠点 責任者 Theresa Kushner）

私たちは，世界中からイノベーションの創出が期待される人財を集めて先進技術の可能性を検証しています．5～10年後に主流となるであろう技術を特定し，お客さまとの共創をとおして，現在および将来の問題に対する解決の糸口を見出そうとしています．また，スタートアップや研究機関との関係性を強化することによって，技術的な強みを獲得しています．

北米では，イノベーションプログラムを実行しています（**図 3**）．このプログラムでは，まず見込み顧客に対するイノベーション活動の入り口として，「ブリーフィングセンタ」を活用します．次に，「イノベーションスタジオ」において，既存の課題や技術を検討しながらお客さまのニーズを特定していきます．イノベーションセンタでは，問題解決に必要となる先進技術を検証し，検証で得られた知見を基に実証実験を実施し，MVP（Minimum Viable Product：お客さまに価値を提供できる最小限の製品・サービス）の作成までを一気通貫で行います．さらに，後続のデリバリーセンタが，製品開発，お客さまへの提供を担当します．非常にシンプルなモデルですが，私たちイノベーションセンタでは，このように包括的な活動を行っています．

私たちが活動を行っているイノベーションスタジオとイノベーションセンタについて，少し詳しく紹介します．

イノベーションスタジオでは，お客さまが中心となって活動を行います．ここでは，日々の業務から離れ，自身の問題の解決や，将来必要となることに対して集中して取り組むことができます．また，先進技術を使った課題の解決方法を検討することができます．机上でMVPを作成するようなこともあれば，自分たちの環境を模した仮想的な空間，例えば都市を模した空間に実際に入っていただくことで，没入感を得たり，これから活用しようとする先進技術を事前に体験したりすることもできます．

また，イノベーションセンタでは，先進技術を網羅的に検証し，技術の成熟度を判定することで取り組むテーマを決定しています．特定した技術について，どの拠点が取り組むべきかについても戦略的に検討します．そして，グローバルの拠点間で協力し，先進技術をお客さまのビジネス価値へと変換していくのです．私たちは，グローバルにおける技術戦略を設定し，それらを基に活動を進め，最終的に革新的なお客さまとの共創をめざしています．

北米では，特に「デジタルヒューマ

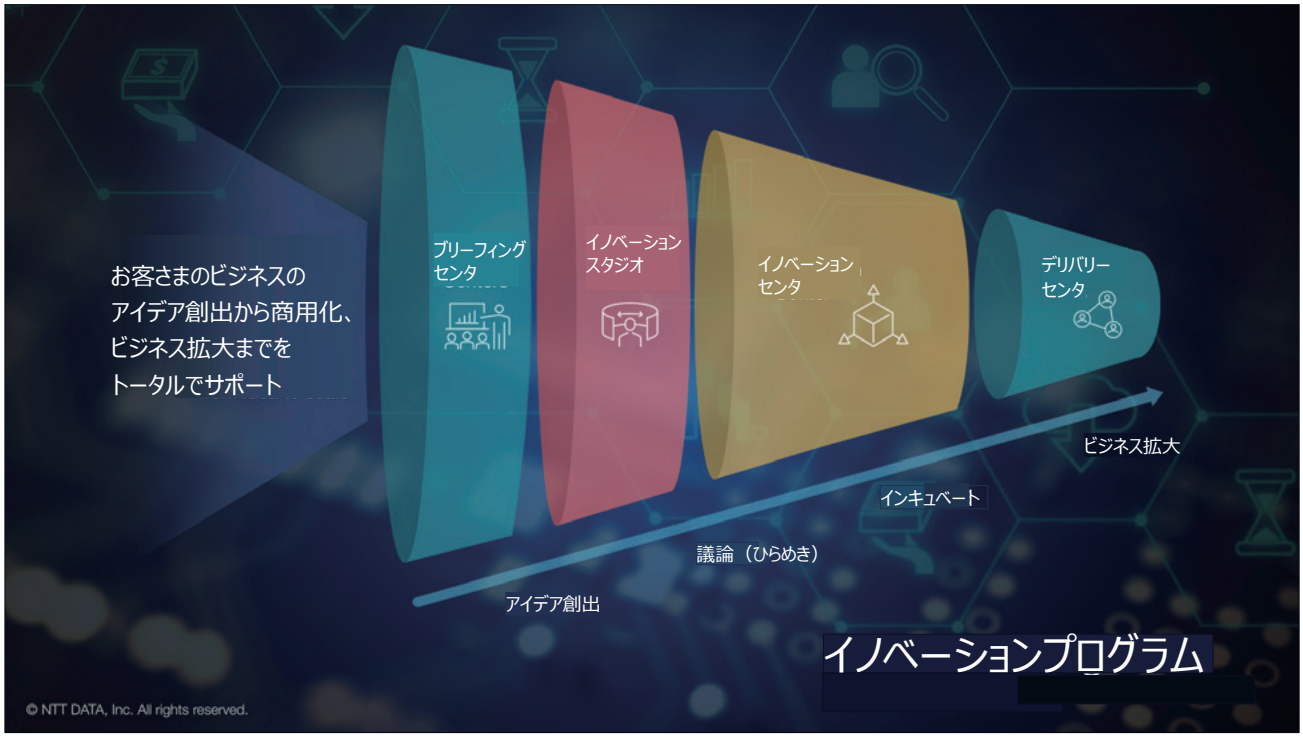


図3　イノベーションプログラム

ン」と「スマートスペース（知的空間）」の分野に注力し，活動を行っています．

デジタルヒューマン分野については，人間の姿をした3Dキャラクターに関する取り組みなどを行っています．最初に，アバターの作成，ボイスクローニング，可視化のプラットフォームなど，技術を構成する要素を特定し，技術評価を行います．私たちの拠点には，技術的な専門性に加え，価格，コスト，保守などの観点からお客さまに最適な提案が行える人財がそろっています．デジタルヒューマンを活用することで，人手不足の解消や，人件費の削減が実現できると考えています．また，デジタルヒューマンの事例としては，アパレル業界大手のお客さまと一緒に，仮想的な洋服の試着に関する取り組みを進めています．

スマートスペースについても同様に取り組みを進めています．スマートスペースとは，効率的かつ効果的な管理のために，ネットワーク化され，かつセンサを備えた物理的な環境であり，大きな空間だけでなく，店舗や工場といった小さな空間でも実現可能な仕組みです．例えば，ある地域の非常事態における対処方法を検討したい場合，シミュレーションを行うことが重要となりますが，その際，センサを利用するとともに，スマートスペースのケイパビリティを統合するのです．スマートスペースの事例としては，国際空港内にある公共交通を対象として，輸送ハブの動きをリアルタイムで収集して情報提供するといった取り組みを行いました．

私たちは，デジタルヒューマンとスマートスペースの組合せも有効だと考えています．スマートスペース上にメタバース空間があり，そこでアバターがガイドとなることで双方向のやり取りが生まれます．

私たちは，このような活動をとおして，NTTデータの一員として，またグローバルなイノベータとして将来に向けて貢献していきたいと考えています．

（左から）古川　洋/
Pietro Scarpino /
Theresa Kushner

イノベーションセンタでは，先進的なお客さまとの共創R&Dをめざし，グローバル拠点横断で技術検証や提案活動を行っています．私たちの活動に興味を持たれた方がいらっしゃいましたら，ぜひお問い合わせください．

◆問い合わせ先
NTTデータ
イノベーションセンタ
E-mail　ic_pr＠kits.nttdata.co.jp

ウェルビーイング × ITで実現する新しい未来

ウェルビーイングに関する取り組みは，国内外の経済界や政府系機関など，さまざまなステークホルダーが関心を持ち，ポストSDGs（持続可能な開発目標）として高い注目を集めています．本稿では，ITを用いたウェルビーイング支援に関する考え方やシステム開発方法論について軽く触れた後に，NTTデータが開発しているウェルビーイングテクノロジについて，その技術の中身から適用イメージまで紹介します．

野村（のむら）　雄司（ゆうじ）　片岡（かたおか）　紘平（こうへい）

NTTデータ

ウェルビーイングとは

WHO（世界保健機関）は，「健康とは，病気ではないとか，弱っていないということではなく，肉体的にも，精神的にも，そして社会的にも，すべてが満たされた状態にあることをいいます」と，当該機関の憲章として掲げています．ウェルビーイングという言葉に明確な定義*1はありませんが，ここに出てくる「肉体的にも，精神的にも，そして社会的にも」良い状態（ウェルビーイング）が分かりやすい解釈かと思います．

ウェルビーイングは，各人によって大きく異なります．また，同一人物においても，日々，時々刻々と変化します．こういったウェルビーイングは，一見とらえどころがないように思えますが，心理学などの分野において尺度化され，人々のウェルビーイングを測定する取り組みがなされてきました．

*1　英語の原文にはWell-Beingという言葉が明記されています．

ウェルビーイングを測定することにより，ウェルビーイングが向上するための手立てが検討できるようになります．

社会の動向と私たちの取り組み

2000年代後半にGDPなどの経済指標では測れない人々の生活の豊かさを可視化する取り組みが始まり，これに続くかたちで，OECD（経済協力開発機構）が加盟国の生活の状況を測定する，「How's life?」という調査を始め，これらが各国の政策決定に大きく寄与し始めています．また，SDGs（持続可能な開発目標）の3番目のゴール，「Good Health and Well-being」としても，ウェルビーイングは注目を集めています．

日本においても，2021年には「政府の各種の基本計画等について，ウェルビーイング に関するKPIを設定する」ことが政策に上がり，2022年はウェルビーイング元年とまでいわれるほど，国内にも浸透してきています．社会が株主資本主義からステークホルダー資本主義に変わりつつある昨今，社会全体として，利益を追求するだけでなくあらゆるステークホルダーに向き合わなければいけない時代になってきています．そのため企業においても，株主や従業員だけでなく，企業活動に関係する生活者や地球環境等のあらゆるステークホルダーを豊かにする必要性が高まってきています．つまり，ウェルビーイングが経営の中心になってきているといっても過言ではないでしょう．

別の潮流として，内閣府は新たな社会“Society 5.0”，デジタル田園都市構想を掲げ，サイバー空間とフィジカル空間を融合させた社会づくりに取り組んでいます．ITが人々や社会に果たす役割は大きくなっています（**図1**）．このように高度なIT社会化の素地ができているため，ITはウェルビーイング領域にも染み出し，むしろITがウェルビーイング領域をリードしていくべきだと考えています．このような背景から，NTTデータはウェルビーイング×ITを社会やビジネスの成長の鍵ととらえ，ITを活用した人々のウェルビーイングの実現をめざしています．

ウェルビーイングテクノロジによる支援

これまでNTTデータは，自然言語処理などをはじめとするAI（人工知能）開発の実績を積んできました．加えて，近年より一層注目が高まっているAIガバナンスの観点も踏まえたシステムの開発にも注力しています．本稿で紹介するウェルビーイングテクノロジは，これらの実績や取り組みを高度に組み合わせた技術です．

■対象とするウェルビーイング

前述のとおり，ウェルビーイングはあいまいで一元的な定義はありませんが，個人が主観的に感じるものである“主観的ウェルビーイング”，これを下支えするように“生活満足度”がある[*2]と考えています．主観的ウェルビーイングは，ポジティブ感情や達成感など，心理的な状態や認知に関連します．一方，生活満足度は，文字どおり，賃金や職場，公共サービスなど自身の生活に直接的にかかわる満足度です．

この主観的ウェルビーイングは，時間変化に伴って日々移り行くもので，このような日々の生活に密接にかかわるものを持続的ウェルビーイングと呼んでいます[*3]．私たちは，このもっとも身近な，持続的ウェルビーイングを支援するテクノロジを開発しています．

■ウェルビーイング支援のフレームワーク

日常生活におけるユーザの持続的ウェルビーイングの遷移イメージを**図2**に示します．日常の気持ちの浮き沈みに伴って，4つの状態を遷移します．この持続的ウェルビーイングの遷移に合わせて，ウェルビーイングの持

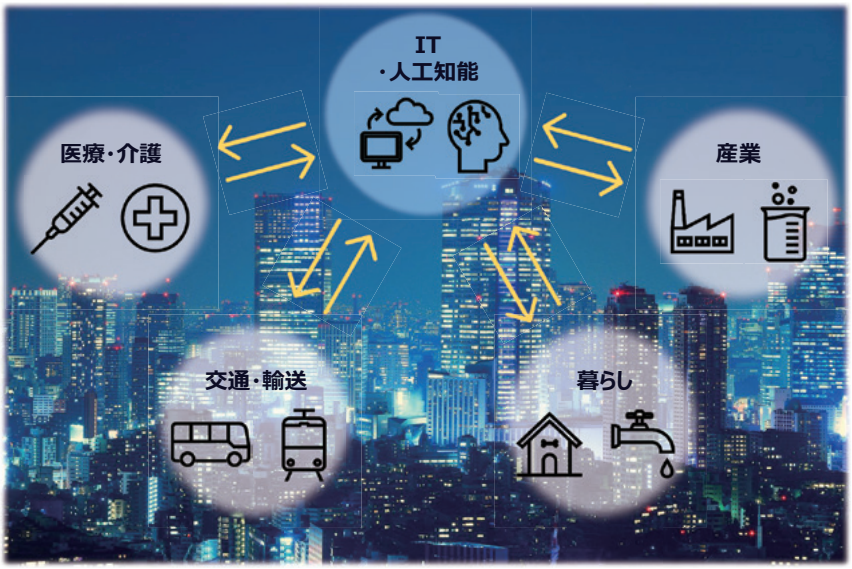


図1　ITが人々や社会に果たす役割の拡大

*2　主観的ウェルビーイングと同階層に位置付ける考え方もあります．
*3　このほかに，快楽主義的ウェルビーイングと医学的ウェルビーイングがありますが，本稿では割愛します．

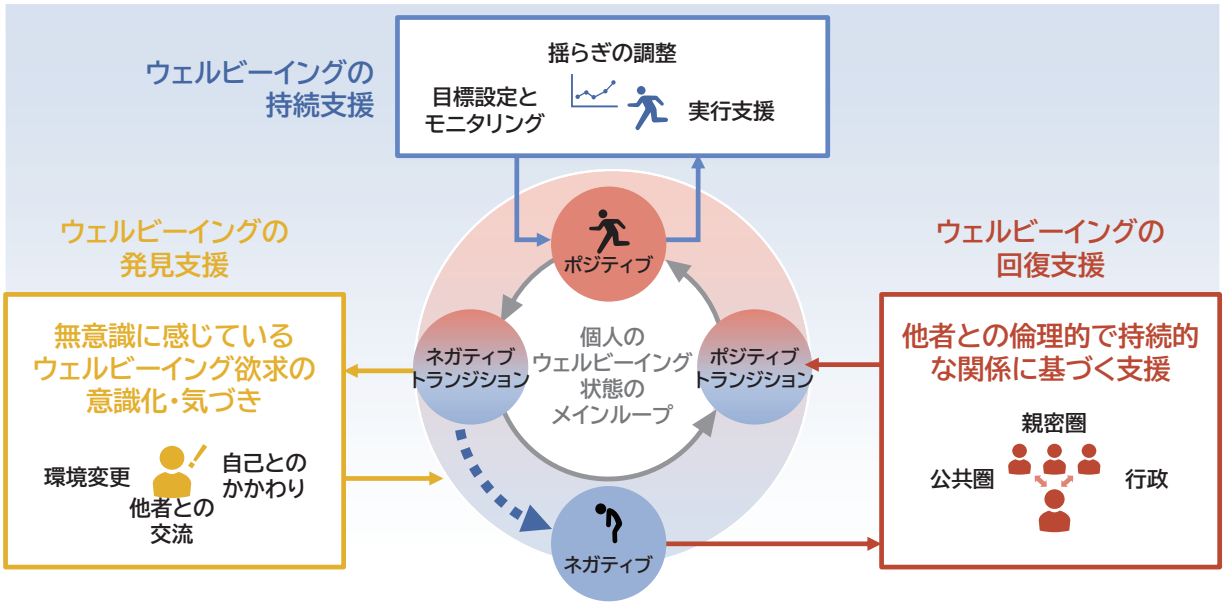


図2　持続的ウェルビーイングの遷移イメージ

続支援，発見支援，回復支援の３つの支援ができると考えています．この中でも，私たちは持続支援を中心に据えて，ウェルビーイングテクノロジの開発に取り組んでいます．**図３**に私たちが開発しているウェルビーイングテクノロジの支援フレームワークを示します．

「ユーザ理解技術」はユーザの性格・価値観，趣味趣向，行動習慣を，大規模言語モデルをはじめとするAIを用いて推定します．従前からNTTデータは自然言語処理をはじめとするAIのビジネス適用に注力していました．これに心理学的な知見を取り込み，「ユーザ理解技術」を開発しています（**図４**）．想定しているインプットデータは，ユーザのSNSや，コンテンツ閲覧履歴，ウェアラブル端末などのバイタルデータなどであり，多様なデータを用います．これらのデータには，ユーザの性格・価値観，趣味趣向，行動習慣が反映されていると考えられますので，これらのデータを使ってそれぞれの価値観を推定します．

「施策最適化技術」はユーザの価値観を理解したうえで，ウェルビーイング向上施策のレコメンドを行うものです．施策の内容のみに基づいたレコメンドを行うだけではなく，その提示方法や，抽象度，選択可能性を総合的に最適化していきます．提示方法の側面からの最適化は，施策を提示するタイミング，メッセージの送り方，その文面，行動のハードルの高さを調整します．残りの抽象度と選択可能性は，行動選択におけるユーザの自律性にかかわる重要な側面です．施策の抽象度と選択可能性を適切にコントロールすることで，システムが提案したものを脊髄反射的に選ぶ（または，選ばせる）のではなく，ユーザが自律的に選択・

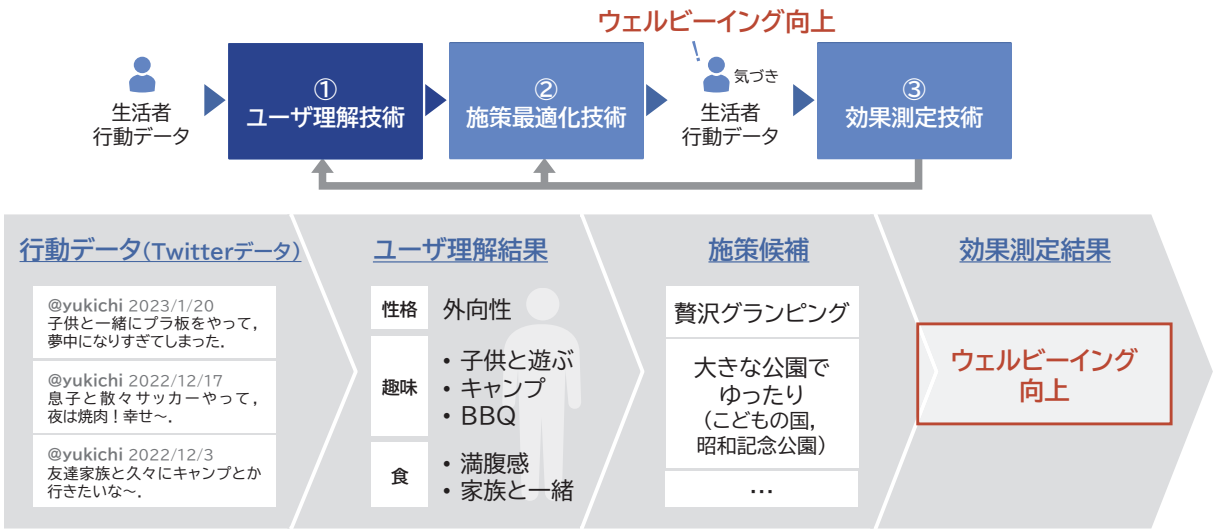


図３　ウェルビーイングテクノロジの支援フレームワーク

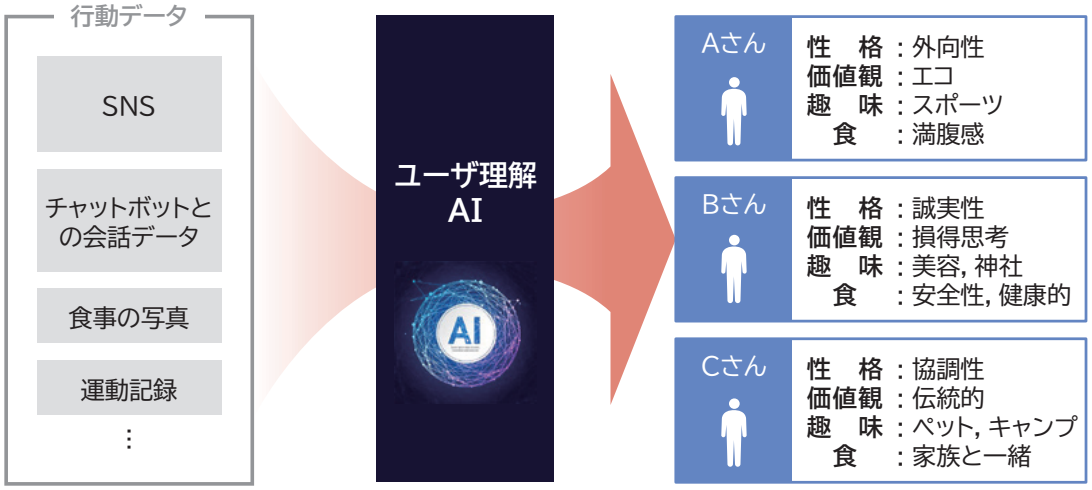


図４　ユーザ理解技術

行動したという感覚を持てるようにします．

「効果測定技術」は，ウェルビーイング支援施策を実施した結果，ユーザの状態がどのように変化したかの効果を測定するための技術です．ここでは，主観的ウェルビーイング指標と，その下位指標となるウェルビーイングの構成要因に関する測定を行います．測定において，従来から行われているユーザのアンケート結果の分析だけでなく，実際にその行動を行ったのかを分析する行動履歴分析，さらには，ユーザの日記の分析やウェアラブル端末から収集される睡眠の分析などを多面的に実施します．主観的ウェルビーイング指標の測定内容は，大別して認知的満足度と，感情の２つがあり，これらの測定のためにアンケートも実施します．このとき，行動のプロセス自体に対する評価も併せて取得します．例えば，健康のために歩く内容の施策を提示した場合，その結果の満足度は10点満点で，プロセスとしては，「歩くこと自体楽しかった」など，総合点数と一緒に，どのようなプロセスが重要なファクターであったかを把握することが重要です．その他，自社サービス利用による効果に直結する指標などがあれば，それが評価できるようなアンケートを作成する，もしくは，データ（数値，画像，テキストなど）をモニタリングするような機能をユーザインタフェースに追加実装し，定量化します．

以上の３技術のループを回すことで，継続的にユーザの持続的ウェルビーイングを支援します．

■ウェルビーイング支援時に気を付けるべきこと

前述のとおり，ウェルビーイングテクノロジの技術的な側面を紹介してきましたが，技術と表裏一体になっているのが，倫理の問題です．NTTデータは法令遵守だけではなく，より広域な倫理的な観点も考慮したAIガバナンスに積極的に取り組んでいます．ウェルビーイングテクノロジが偏見（バイアス）や不平等を生むことがないよう，また，社会に受容されることを考慮しながら，専門チームと協力して開発に取り組んでいます．

ウェルビーイングの要因は，個人によって異なるということを常に念頭に置いておく必要があります．ウェルビーイングを押し付けられることは，他者から杓子定規な基準があてがわれてしまうことであり，逆にウェルビーイングが損なわれてしまいます．

併せて，ユーザの自律性を奪うような技術であってはいけません．テクノロジが何かを強制したり，制限したりすることは，人がウェルビーイングな状態であるための重要な要因である“自律性”が損なわれてしまいます．上記は一般的に気を付けるべきことを挙げましたが，これ以外にも個々のサービス特有の検討が必要になります．

ChatGPTをはじめとする生成系AIが，非AIエンジニアの層にまで急速に普及しており，今後，AI関連のウェルビーイング支援技術の開発がさらに加速することが予想されます．このような状況では，“安全で有効なサービスの提供のためには，プライバシとセキュリティ，ユーザエクスペリエンス，信頼性，エビデンスに基づいたアプローチ，倫理的配慮，そして継続的改善を心掛けることが必要でしょう”[*4]．

今後の展開

政府のSociety 5.0の取り組みやスマートフォン・ウェアラブル端末の普及，AI技術の加速度的発展など，ITがさらに活用されていく社会へ移行していくことが想定されます．本稿の主題である，ウェルビーイング×ITを省みると，瞑想支援などのウェルビーイング要因を支援する個々のサービスはあるものの，人々のウェルビーイングを包括的に支援する技術というのは，いまだ世間に出回っていません．

昨今注目されている，生成系AI，対話エージェントは，ウェルビーイング支援を提供するにあたって最適なパートナーになる可能性を秘めています．このような最新の技術を積極的に取り入れながら，ユーザの日常の生活に寄り添い支援するウェルビーイングテクノロジの開発に取り組み，個々人がウェルビーイングでいられる社会の実現に向けて，NTTデータも貢献していきます．

（左から）野村　雄司／ 片岡　紘平

個人のウェルビーイングを制度や仕組み，人だけで支援し続けることは，現実的ではありません．そこで活躍するのがAIをはじめとするITであると著者らは考えています．AIによるウェルビーイング支援という世界は，もう目の前に来ています．

◆問い合わせ先
NTTデータ
技術革新統括本部 システム技術本部
データ＆インテリジェンス技術部
TEL　050-5546-8097
E-mail　dioffering-contact@kits.nttdata.co.jp

＊4　“”の中の文は，「テクノロジを用いて人々のウェルビーイングを支援するときに何を気を付けなければならないか」をChatGPTに質問したときの回答を要約したものです．

高まる“デジタルアイデンティティ”の重要性とNTTデータの取り組み

「デジタルアイデンティティ」という言葉を耳にしたことはあるでしょうか．「認証」「ID管理」といったキーワードを連想する方もいらっしゃるかと思います．NTTデータでは，この「デジタルアイデンティティ」を，企業のサイバーセキュリティの中心に位置する重要な要素であるととらえ，これまでさまざまなお客さまの課題を解決に導いてきました．本稿では，その方法論の一部を紹介します．

宍戸（ししど）　りさ
NTTデータ

MDRへの着目とデジタルアイデンティティの重要性

NTTデータでは，これまで自社や国内外グループ会社内のセキュリティ環境を整備してきた経験や，お客さまへのご支援実績をとおして得られた知見を活かし，「MDR（Managed Detection and Response）」を軸にこれからの市場を牽引していこうとしています．MDRとは，ITリソース全般の監視と，トラブルが起きた際には対応・復旧までを行うセキュリティの専門家によるサービスの総称です[(1)]．MDRが重要視される背景には，コロナ禍の影響や，世の中のオンライン化の流れ，そしてそれらに伴うサイバーセキュリティのトレンドの変化の中でも，特に「ゼロトラスト」という概念が定着してきたという点があると考えています．ゼロトラストとは，Microsoft社が「never trust, always verify」と提唱しているとおり[(2)]，ネットワークの境界で強固にリソースを保護する（つまり会社であれば，社内からのアクセスは安全，社外からのアクセスは危険と一律に判断する）のではなく，すべての通信を信用せず，アクセス可否を都度判断する，境界を突破されることを前提にした考え方のことを言います．ゼロトラストな世界では，過去にNTT技術ジャーナルにて紹介[(3)]したNIST（National Institute of Standards and Technology：米国国立標準技術研究所）が提唱するサイバーセキュリティフレームワークのうち，「特定（Identify）」「対応（Respond）」「復旧（Recover）」が特に重要となります．MDRはこれらをまとめて実現するソリューションです．

NTTデータでは，**図1**に示す9つの分野に分けてMDRをとらえています．

9つそれぞれの要素で，どのようにセキュリティ強度を向上させるかを総合的に考えていくことになりますが，

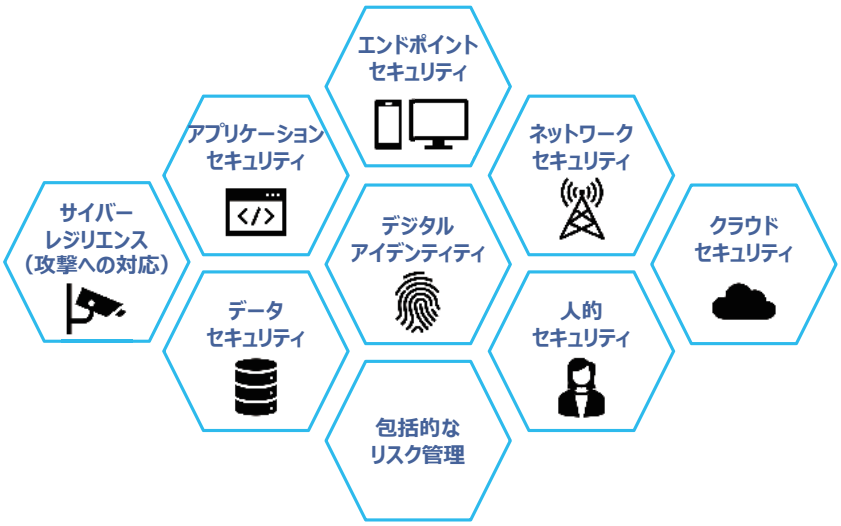


図1　MDRを構成する要素

その中心に位置するのが，「ID管理」や「アクセス制御」「認証」といったキーワードで語られることの多い「デジタルアイデンティティ」という分野です．

MDRにおいてデジタルアイデンティティが中心となる理由はいくつかありますが，もっとも大きな理由は，物理的な人間の存在と，その人が使うさまざまなネットワークやシステムをつなぐ役割を果たすのが「デジタルアイデンティティ」であり，「あなたは誰？」「あなたは本当に本人？」という点をまず確認し保証することが，ゼロトラストな世界を実現するためには必要になるため，ということだと考えています．

企業はデジタルアイデンティティについてまず何を考えるべきか

企業が，ゼロトラストというキーワードで自社内を見つめ直すとき，またはデジタルアイデンティティにまつわる何らかの課題を解決しようとするとき，まずは何が必要になるでしょうか．

私たちがお客さまのデジタルアイデンティティにまつわる課題解決を支援させていただく際には，「課題の全体像整理」のフェーズ（**図2**の赤字部分）を重要視しています．それは，お客さまに見えている課題は氷山の一角であることが多いこと，またそれを解決するだけでは根本的な改善にならなかったり，見えている課題に着手して検討を進めるうちに，それに絡む，より優先度の高いテーマが見つかったりするケースがあるためです．特にデジタルアイデンティティの分野には，「これをこうしておけば大丈夫」というベストプラクティスが少なく，お客さまの状況に合わせてソリューションを選定し，カスタマイズをしたうえで実装していくことが必要な要件も多いため，ゴールまでの最適解を見つけるのは簡単ではありません．

課題を整理するために，NISTやISO（International Organization for Standardization：国際標準化機構）は国際的なガイドラインやフレームワークを定義しています（**表**）．

これらは，日本国内はもちろん，世界で多くの組織や専門家が参考にしている情報です．しかし，実務的な観点で考えると不足する点があるのでは，と私たちは考えています．NTTデータでは，主に企業内部のデジタルアイデンティティの課題整理のためのフレームワークを策定し，多くのお客さまへのコンサルティングを行っていますので，その概要を紹介します．

デジタルアイデンティティについて考えるべき9つの観点

企業のデジタルアイデンティティについて俯瞰するためには，**図3**に吹き出しで示す9つの観点が必要となります．これらをサイバー空間ではなく，企業内の物理的な環境に置き換えた例が**図4**になります．

順番に9つの観点の内容を説明します．

■身元確認（Proofing）

物理的な「その人」をシステムが理解できるように，電子的な「ID＝Identity」に紐付けること．よく「本人確認」という言葉を耳にしますが，身元確認と，後に示す「当人認証」の2つを実施して初めて，本当の意味での「本人確認」ができたといえます[6]．

■ライフサイクルマネジメント（Life-cycle Management）

電子的なIDが生成されてから破棄されるまでの一連の状態と，その遷移を管理すること．ISO/IEC 24760ではこの観点についてモデルとともに説明されています．

企業では，人事イベントや，改姓，組織名変更などと連動してアカウントの状態が正しく変遷しているかが主な確認ポイントとなります．2023年1月25日にIPA（情報処理推進機構）により発表された組織向けの「情報セキュリティ10大脅威2023（IPA10大脅威）」[7]

表　NIST SP800-63 [4] とISO/IEC 24760 [5] の概要

NIST SP800-63	“Digital Identity Guideline” システムへの要求事項として，デジタルアイデンティティに関する保証レベルを定義しているガイドライン
ISO/IEC 24760	“IT Security and Privacy -A framework for identity management-” デジタルアイデンティティの管理（特に状態変化）に主眼をおき，用語や概念を定義している

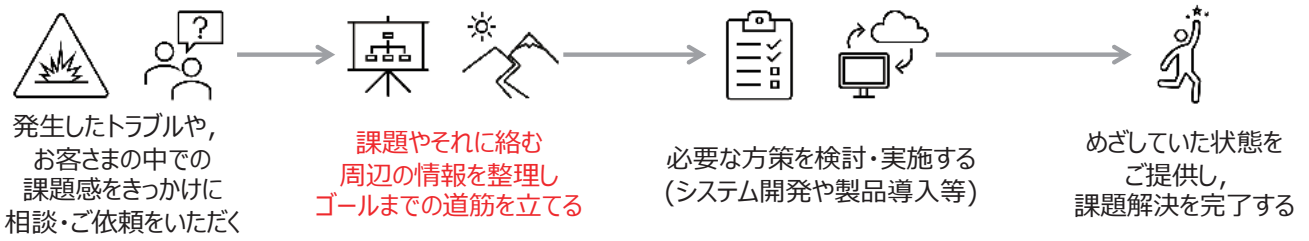


図2　問題解決支援の流れ

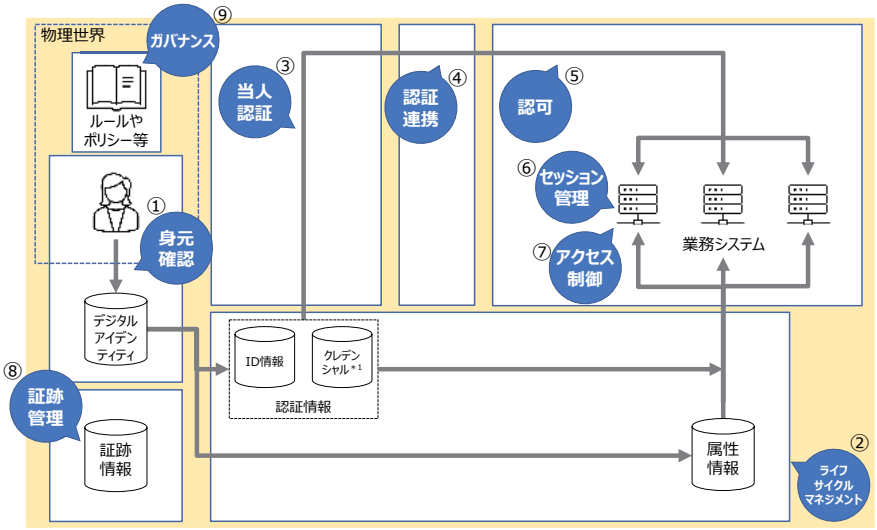


図 3　NTTデータで整理したデジタルアイデンティティの課題整理のためのフレームワーク

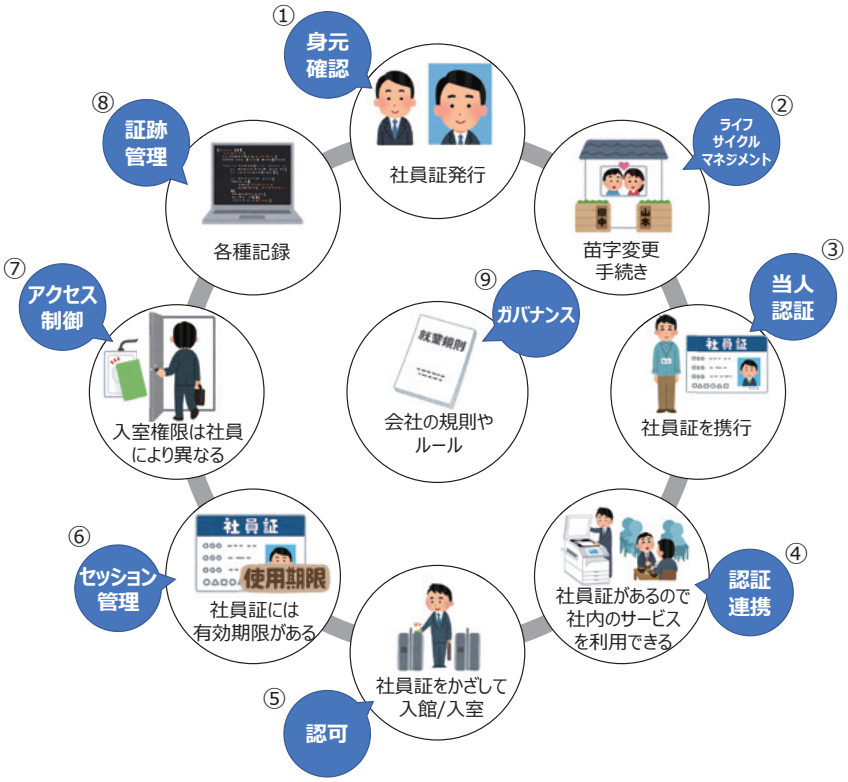


図 4　企業内の物理的な環境におけるデジタルアイデンティティの観点の例

では，脅威第 4 位に選定された「内部不正による情報漏えい」への対策で，「従業員の異動や離職に伴う不要な利用者IDなどは直ちに削除する」べきであると言及されています．

■当人認証（Authentication）

電子的なIDが，持ち主本人によって使用されたかを判定すること．一般的に，認証の 3 要素と呼ばれる「知識」「所持」「生体」のいずれかの情報，またはそれらの組合せで判定します．

始業のために端末にログオンするとき，各システムにサインインするとき，機微な情報の取り扱いがあるシステムを利用するとき，どのような認証情報を使っているでしょうか．IPA10大脅威で指摘されているように，認証情報を窃取・悪用される危険性について十分に検討されているでしょうか．

当人認証については，セキュリティ強度と利便性のバランスなどについてもよく話題に上ります．これまでは，セキュリティ強度を上げようとすると利便性が下がる，両者はトレードオフの関係であるといわれてきました．ですが最近は「パスワードレス認証*2」や「WebAuthn*3」などに代表されるような「セキュリティ強度も利便性もどちらも高い」方法を取ることができるようになってきています．

■認証連携（Federation）

他のシステムで実施した当人認証の結果を受け入れ，自システムで再度当人認証をせずにアクセスを許可すること．認証連携するために，複数サービス間でのSSO（Single Sign On）を実現するケースもあります．

■認可（Authorization）

システムが当人認証の結果を確認し，自らへのアクセスを許可すること．各業務システム側で実施するのか，認証基盤やID管理をするシステム側で実施するのかなどの観点があります．

■セッション管理（Session Management）

当人認証，認証連携，認可をした状態をどの程度の時間保持するかを，要件に沿って決めること．分かりやすい

---

*1　クレデンシャル：パスワードや電子署名，資格証明書など，当人利用であることを確認するために，ユーザ自身が示すことができる情報群のこと．

*2　パスワードレス認証：認証の3要素のうちパスワードに代表される「知識」情報を使わずに当人認証を行う方法．パスワードの漏えいの危険性や，パスワードを覚えなければいけないユーザの負担感を下げることが期待されます．

*3　WebAuthn：Webサービスにおいてパスワードレス認証を実現するための認証技術の仕様の1つ．

判断基準として，機微な情報の取り扱いがあるかどうかという点があります．離席している間，他の作業をしている間，無操作のまま30分経過した後など，どの程度の時間「その情報がその人（例えば離席している間になりすましが発生することも考慮に入れる必要があります）に見える状態になっていて大丈夫か」をシステムごとに整理していきます．

■アクセス制御（Access Control）

各システムが，アクセスしてきたユーザの情報を基にアクセスを許可または拒否（または再度当人認証を要求）すること．IPA10大脅威の第４位「内部不正による情報漏えい」の攻撃手口の１つに「アクセス権限の悪用」が挙げられており，「必要以上に高いアクセス権限が付与されている場合，より重要度の高い情報が窃取」されるおそれがあると述べられています．企業内のシステムにおけるアクセス制御は，ロール（役職などの役割）や属性（アクセス元IPアドレスなどの特徴）の情報を使って行うのが一般的です．各システム側でどのような要件を定めているか，また認証基盤やID管理をするシステムが存在する場合は必要なロールや属性をどのように管理しているかなどについて確認をしていきます．

■証跡管理（Accounting）

利用状況やシステムへのアクセス履歴などを取得・管理すること．「重要情報へのアクセス履歴や利用者の操作履歴などのログ，証跡を記録し，監視すること」は，IPA10大脅威でも重要な対策として挙げられています．昨今ではクラウドサービスの利用が増えていますが，製品によっては社内で規定された期間よりも短いログの保存期間しか保証されないケースもあるため，定期的にエクスポートして別途保管するといった処理が必要になる場合もあります．

また，証跡管理は監査を実施するうえでも重要です．適切なID情報の管理をすることはもちろん必要ですが，定期的な監査を実施し，運用が適切に回っているのかを確認することが求められています．

■ガバナンス（Governance）

デジタルアイデンティティに絡む全要素を企業で正しく運用していくために必要な規程を作成・管理したり，棚卸を実施すること．企業においてガバナンスの維持は非常に重要です．ここまで述べてきた８つの観点について，社内規程やポリシーはあるでしょうか．そしてそれらは適切なタイミングで見直され，現場ではそれに従った運用がなされているでしょうか．

NTTデータが提供できる価値

本稿では，デジタルアイデンティティの重要性，またデジタルアイデンティティについて考えるべき９つの観点を軸にその内容について紹介してきました．NTTデータでは，NISTやISOが定義している既存の標準を参考にしながら，デジタルアイデンティティ全体の課題を体系的かつ網羅的に整理するフレームワークを独自に整備し，それに基づくコンサルティングと，ソリューションの提案を多数実施してきています．冒頭でも述べたとおり，デジタルアイデンティティは社内のセキュリティを考えるうえで避けては通れないテーマであり，土台となる部分です．「デジタルトランスフォーメーション（DX）」「クラウドシフト」「リモート化」など，さまざまなキーワードが流行する中，社内のセキュリティをどのように向上させ，時代に合うかたちにしていくかを考えるとき，ぜひ「デジタルアイデンティティ」を中心に考えてみていただければと思います．全体像を整理する中で，例えば「うちの会社には実はこんなITリソースがあったのか」「明文化されていないがこんな通信経路もあり得てしまう」など，デジタルアイデンティティ以外の課題が見えてくるといった副次的な効果もあり，社内システム全体を見つめ直すきっかけになると，NTTデータは考えています．

■参考文献

(1) https://www.gartner.com/smarterwithgartner/gartner-top-technologies-for-security-in-2017
(2) https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview
(3) from NTTデータ：“NTTデータが取り組むゼロトラスト業務環境，” NTT技術ジャーナル，Vol.33, No.9, pp.58-62, 2021.
(4) https://pages.nist.gov/800-63-4/
(5) https://www.iso.org/standard/77582.html
(6) https://www.meti.go.jp/press/2020/04/20200417002/20200417002.html
(7) https://www.ipa.go.jp/security/vuln/10threats2023.html

宍戸 りさ

セキュリティは，業種，業態，規模，国内外を問わず世の中共通のテーマであると考えています．セキュリティと一言でいっても非常に多くの要素を含んでいますが，「デジタルアイデンティティ」という切り口で考えたことのある人は案外少ないのではないでしょうか．本稿で，デジタルアイデンティティという分野の深みを垣間見ていただければと思います．

◆問い合わせ先
NTTデータ
技術革新統括本部 システム技術本部
サイバーセキュリティ技術部
TEL 050-5546-2556
E-mail Risa.Shishido＠nttdata.com

Low-Code Platformで変わるソフトウェア開発の高速化

近年，LCP（Low-Code Platform：ローコードプラットフォーム）と呼ばれるソフトウェア開発手法が注目を集めています．本稿では，LCPが持つ機能の解説や，これまでのソフトウェア開発の歴史におけるLCPの立ち位置，従来の手法と比較してLCPが優れている点，LCPの注意事項，LCPの事例やLCPが実現する未来について解説します．

島倉（しまくら）　優人（ゆうと）
NTTデータ

LCPとは

LCPとは，設計・製造・テスト・運用といったソフトウェアのライフサイクル全体をサポートするソフトウェア開発プラットフォームのことです．ソフトウェア開発と一言で表しても，その中で実施することは「開発環境を用意する」「本番運用環境を用意する」「設計書を基にソースコードを書く」「ソースコードを実行可能なソフトウェアに変換する」「ソフトウェアを開発・本番運用環境で実行する」「ソフトウェアを監視・分析する」，など多岐にわたります．LCPは**図1**に示すように大きく5種類の機能を提供しており，各工程を自動化して高い生産性を実現できます．

①　各種環境PaaS[*1]提供

ソフトウェア実行のためには，典型的な例として次のハードウェアを用意する必要があります．

- ソフトウェアを実行するためのサーバ
- データを蓄積するためのデータベース
- インターネットに公開するためのネットワーク

また，開発環境，テスト環境，本番環境など複数環境を用意することが一般的です．LCPでは利用開始と同時にソフトウェアを開発・実行できる環境が提供されます．さらに，モバイルなどのデジタル技術を容易に利用できる製品もあります．

②　視覚的なモデリング

LCPでは，GUI操作により，視覚的に画面・データ・ロジックなどをモデリング（設計）します．ドラッグ&ドロップによるGUI操作を中心としており，特定プログラミング言語の知識に依存せずにソフトウェアをモデリング可能です．自動化技術によりコーディング量を極限まで減らすことで高生産性を実現しています．

③　マーケットプレイス

LCPではソフトウェアのテンプレートや，画面・ロジックのテンプレート，さらには，細かな部品などの共有・再利用を行うためのリポジトリが提供されることが多いです．これによりソフトウェアを1からつくる必要がなく，

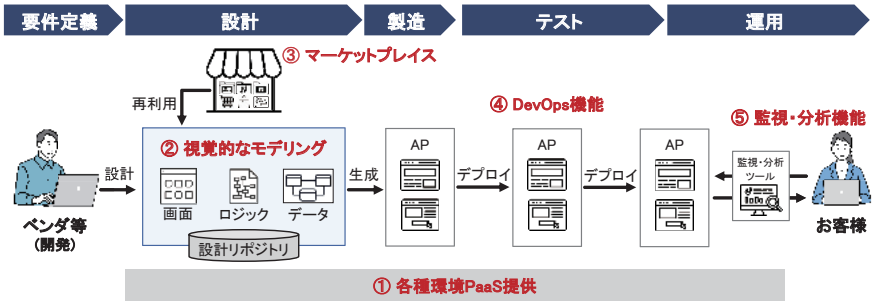


図1　LCPの機能と構成要素

*1　PaaS（Platform as a Service）：クラウド上のプラットフォームを利用できるサービスのこと．

「車輪の再発明」を防いで生産性向上を実現します．

④　DevOps*2機能

モデリング情報からすぐに実行可能なソフトウェアを生成し，LCP内のソフトウェア実行環境に配置・実行する機能が提供されます．この機能により作成したソフトウェアをすぐにリリースできるようになり，リリースまでのリードタイムを短縮できます．

⑤　監視・分析機能

①から④の機能でソフトウェアを実行したら，そのソフトウェアが期待どおりに動作しているかをモニタリングする必要があります．LCPではこの機能も提供され，利用状況をリアルタイムで確認できます．ソフトウェアへのアクセス状況，エラーの発生状況などに加えて，パフォーマンスやユーザエクスペリエンスを分析できる機能を持った製品もあります．

以上の説明のように，LCPはソフトウェアライフサイクル全体に対して機能を提供しており，これによりソフトウェア開発の高速化を実現できます．ただ，LCPが登場する前からもソフトウェア開発高速化の取り組みはされてきました．以降では，従来の手法とLCPが異なる点について説明します．

ソフトウェア開発の歴史からみるLCP

プログラミングの歴史は1940年以前までさかのぼり，コンピュータが直接解釈できる機械言語が登場したことが始まりです．機械言語は二進数で表現されており，人間が理解し使いこなすことはとても難しいものです．その後，アセンブリ言語，C/Javaのようなプログラミング言語が登場しました．なかでもC/Javaのような高級言語は機械言語と比較して自然言語に近いものになっており，機械言語の複雑さが隠蔽され，人間が理解しやすくなりました．人間が理解しやすくなったことで，生産性や保守性が向上しました．その後，さらに視覚的なモデリングによるビジュアル開発ができる機能を備えたLCPが登場し，より人間が直感的に理解しやすくなりました．**図2**に示すように，LCPはビジュアル言語であるともいえます．これにより，これまでの開発言語と比べてより高い生産性や保守性の向上を実現できます．

図3に示すように，プログラミング言語の進化と並行して，手でプログラミングすることから脱却する技術も登場しました．進化の流れは大きく2種類あり，「開発自動化」と「パッケージ（PKG）製品活用」です．

開発自動化は，CASEツール*3による開発，MDA*4によるモデル記述

*2　DevOps：DevelopmentとOperationsを組み合わせた造語．開発者と運用者が連携してソフトウェアが提供する価値をエンドユーザへ迅速に届ける手法のこと．

*3　CASE（Computer Aided Software Engineering）ツール：1980年代から1990年代にかけて多く利用された，ソフトウェア設計の可視化や設計データからソースコードを自動生成するソフトウェア開発支援ツールのこと．

*4　MDA（Model Driven Architecture）：業務のフローや機能などを抽象化したモデルを最初に作成して開発を進める手法のこと．このモデルからソースコードを生成する．

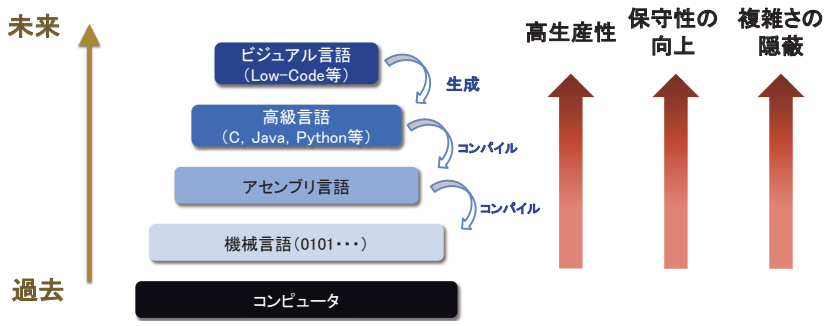


図2　プログラミング言語の進化

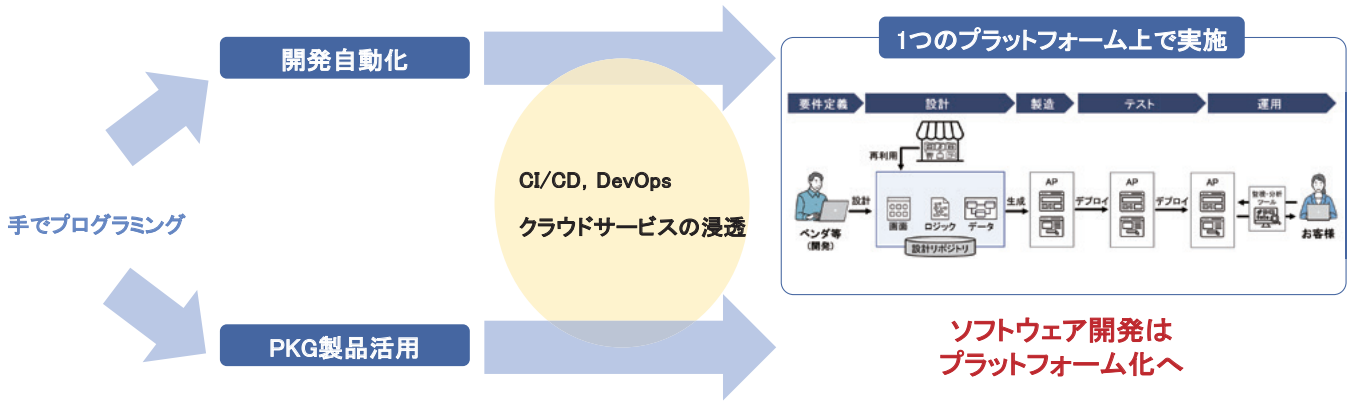


図3　ソフトウェア開発手法の生産性向上・高速化の変遷

などが挙げられます．PKG製品活用は，特定業務の効率化のためのPKG製品を活用するというものです．いずれもソフトウェア開発の「自動化」と「標準化・再利用」であるといえ，生産性向上・高速化は進化と発展を遂げてきました．

そして近年，CI/CD*5，DevOps，クラウドサービスなどさまざまな技術が登場し，自動化の対象領域が拡大しました．いろいろな自動化技術を採用することで生産性向上を期待できますが，それぞれの技術を導入するためのコストがかかってしまいます．そこで，ソフトウェア開発をプラットフォーム化し，１つのプラットフォーム上で複数の自動化技術を利用しながら開発できるかたちに進化しました．LCPはこれに該当します．

プラットフォーム化したことによるメリットとして，**図４**に示すように，これまでのソフトウェア開発自動化手法よりも多くの工程に適用できるようになったことが挙げられます．ソフトウェア開発自動化手法はこれまで「ソースコード生成特化型」と「統合環境型」の２種類がありましたが，それぞれ課題がありました．ソースコード生成特化型は設計情報からソースコードを生成することに特化したものであり，自動生成されたソースコードからソフトウェアを実行する手法は別途検討する必要がありました．また，統合環境型はソフトウェアの設計を開始する段階で利用でき，実行可能なソフトウェアを生成してくれる製品もありますが，ソフトウェアの実行環境は別に用意する必要があるなど適用工程は限定的でした．

LCPはプラットフォーム型として提供されることで，システムライフサイクル全般に対して自動化を適用できるようになり，これまでの手法よりも生産性の向上や開発の高速化を実現できるようになりました．

LCPが実現する未来

近年はVUCA*6時代であり，何が起こるかの予測が難しい世の中においては変化に素早く対応する必要があります．そのため，ソフトウェア開発には高いアジリティが求められます．LCPは，ソフトウェア開発ライフサイクルの一連の流れの自動化を提供しますので，アジリティを高めることができます．結果，世の中の変化に追従できる超高速開発の実現に寄与します．

また，近年はDX（デジタルトランスフォーメーション）の推進を実現するために，ソフトウェア開発のニーズが爆発的に増加していて，IT人財のニーズも高まっています．このIT人財は高いIT技術力だけではなく，問題や課題を正確に把握し解決策をソフトウェア設計まで落とし込む力，ステークホルダーを巻き込んでソフトウェア開発を推進するプロジェクトマネジメント力など幅広い力が求められます．従来の開発では複数の技術を組み合わせる必要がありましたが，LCPでは採用したLCP製品のことだけを学べば最低限のソフトウェアを開発できます．そのため複数の技術や，それらを組み合わせる方法を学ぶことと比較すると，習熟難易度が下がります．近年のIT人財のニーズの高まりに伴い高度なスキルを持ったIT人財の確保は難しくなっていますが，習熟が比較的容易であるLCPを活用することで，既存人財のリスキリングも実現できます．

習熟が容易であることから，従来ソフトウェア開発を外部に委託していた企業において，ソフトウェア開発を自社で行う，いわゆるソフトウェア開発内製化にも向いています．内製開発ではステークホルダー間のコミュニケーションや意思決定を自社内で完結できるため，開発のスピードアップに伴う

*5　CI/CD（Continuous Integration / Continuous Delivery）：ソフトウェアのビルド（生成）やテスト，デプロイ（配置）などを自動化し，これらを継続的に実施する手法のこと．

*6　VUCA：Volatility，Uncertainty，Complexity，Ambiguityの4単語の頭文字を並べたもの．不安定，不確実，複雑，あいまいで予想どおりにいかない社会情勢のこと．

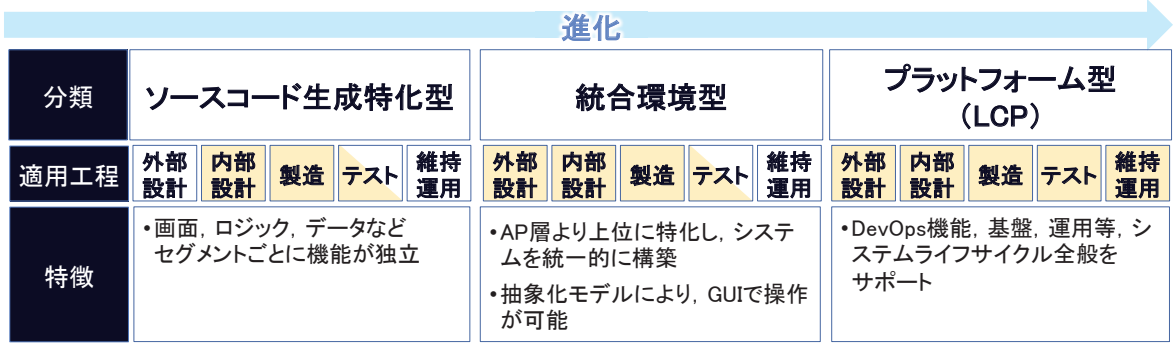


図４　ソフトウェア開発自動化手法の進化

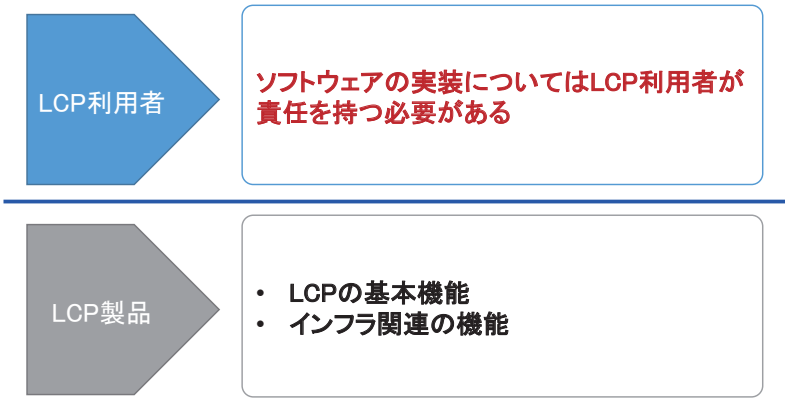


図5　LCPの責任共有モデルのイメージ

アジリティの向上が期待できます．

ここで，ソフトウェア開発内製化の具体的な事例を紹介します．NTT東日本において，内製開発を推進する経営的背景が増していました．そこで，NTTデータサポートの下，社員をLCP人財へリスキリングする取り組みを行いました．現在では，その人財が主体となって内製開発をできるようになっています．経営層による緊急情報把握が3日程かかっているという経営課題がありましたが，危機管理の仕組みの刷新と合わせて内製開発による迅速化，コスト最適化を達成しました．

LCPの注意事項

前述の説明だけですとLCPは夢のようなツールに見えてきますが，使い方を誤るとさまざまな問題が発生する可能性があります．

① 求められる品質が高い場合は，品質保証ストーリーも高度になる

LCPを用いることで，ソフトウェア開発のための技術のハードルが下がり，「どうつくるか」，ではなく，「何をつくるか」に注力できるため，ITベンダのようなプロの技術者だけではなく，ビジネス部門の担当者がソフトウェア開発に携わる，いわゆる市民開発者も利用すると考えられます．例えば，市民開発者が社内のミッションクリティカルなソフトウェアの開発を実装することを考えます．ミッションクリティカルである場合は求められるソフトウェア品質のレベルも高くなり，高度な品質保証ストーリーが必要になります．これはソフトウェアプロセスの有識者が必要になり，市民開発者だけでは困難になります．

② シャドーITの増加やITガバナンスの低下

LCPでは簡単にソフトウェアをつくれることから，企業のIT部門が把握していないものが存在してしまう，いわゆるシャドーITの発生リスクが高まります．その問題を解決するためには，IT部門による統制が必要です．

③ LCP製品のFit&Gap

近年LCPの市場は急速に成長しており，200を超える多種多様なLCP製品・サービスが登場しています．各製品にはそれぞれ特徴があるため，目的や用途に応じて適切な製品を選定する必要があります．

④ LCP製品との責任共有モデルの理解

クラウドサービスでは責任共有モデルを理解したうえで利用することが重要ですが，LCPについても同様です．**図5**に示すように，LCPでは，ソフトウェアの実装に関する問題は利用者責任となることが多いです．例えば，本来はユーザ認証による権限設定をする必要があったが忘れてしまいセキュリティインシデントが発生した場合，ソフトウェアの実装方法が起因の問題となりますのでLCP利用者側の責任となります．利用する製品が担保する仕様について理解をし，それ以外のところは利用者自身で問題が発生しないかを確認する必要があります．

今後の展望

LCPの利用には利点がある反面，注意しなければならない点もあることをご理解いただけたかと思いますが，昨今の時代背景を踏まえると導入を推進すべきソリューションであると考えます．NTTデータでは，LCPの導入障壁を払拭する手法を確立し，先見の事業変革をお客さまとともに実現します．

■参考文献

⑴ https://www.nttdata.com/jp/ja/data-insight/2022/1018/
⑵ https://www.nttdata.com/jp/ja/data-insight/2019/0304/
⑶ https://www.nttdata.com/jp/ja/data-insight/2021/0818/

島倉　優人

「これまで経験がないけど，リスキリングでソフトウェア開発に携わりたい」「今よりも高い生産性でソフトウェア開発をやりたい」と考えられている方，ぜひLCPを検討してください．NTTデータでは，さまざまなLCP製品を取り扱っています．連絡をお待ちしています．

◆問い合わせ先

NTTデータ
技術革新統括本部 システム技術本部 ADM技術部
E-mail　adm_contact @ kits.nttdata.co.jp

挑戦する研究者たち
CHALLENGERS

亀岡弘和

NTTコミュニケーション科学基礎研究所
上席特別研究員

科学技術は先達が少しずつ積み上げてきた成果．それをさらに良くするのが，今を生きる私たち研究者の使命である

「アニメのキャラクターの声が想像と違った」「言い淀みがひどいのでスピーチに自信が持てない」「病気や怪我などで失ってしまった自分の声を取り戻したい」等，発話にまつわるさまざまな思いや不自由さがあります．コミュニケーションにおけるさまざまな制約をAI（人工知能）の機械学習や信号処理の力により取り除き，あらゆる人が不自由なく快適にコミュニケーションを行える環境の実現をめざして本分野の最前線で活躍するNTTコミュニケーション科学基礎研究所 亀岡弘和上席特別研究員に研究の進捗と研究活動の醍醐味を伺いました．

コミュニケーション機能を拡張するメディア情景分析・生成技術を追究

2度目のご登場ですね．手掛けている研究について教えていただけますでしょうか．

私たちの日ごろのコミュニケーションにおいては，障がいや加齢などによる物理的な制約，外国語の会話などにおける能力的な制約，緊張状態などの心理的な制約などが伴い，思いどおりに話せないことがあると思います．私が取り組んでいるのは，そうしたコミュニケーションにおけるさまざまなかたちの障壁や制約を克服するための信号処理・機械学習技術の開発です．

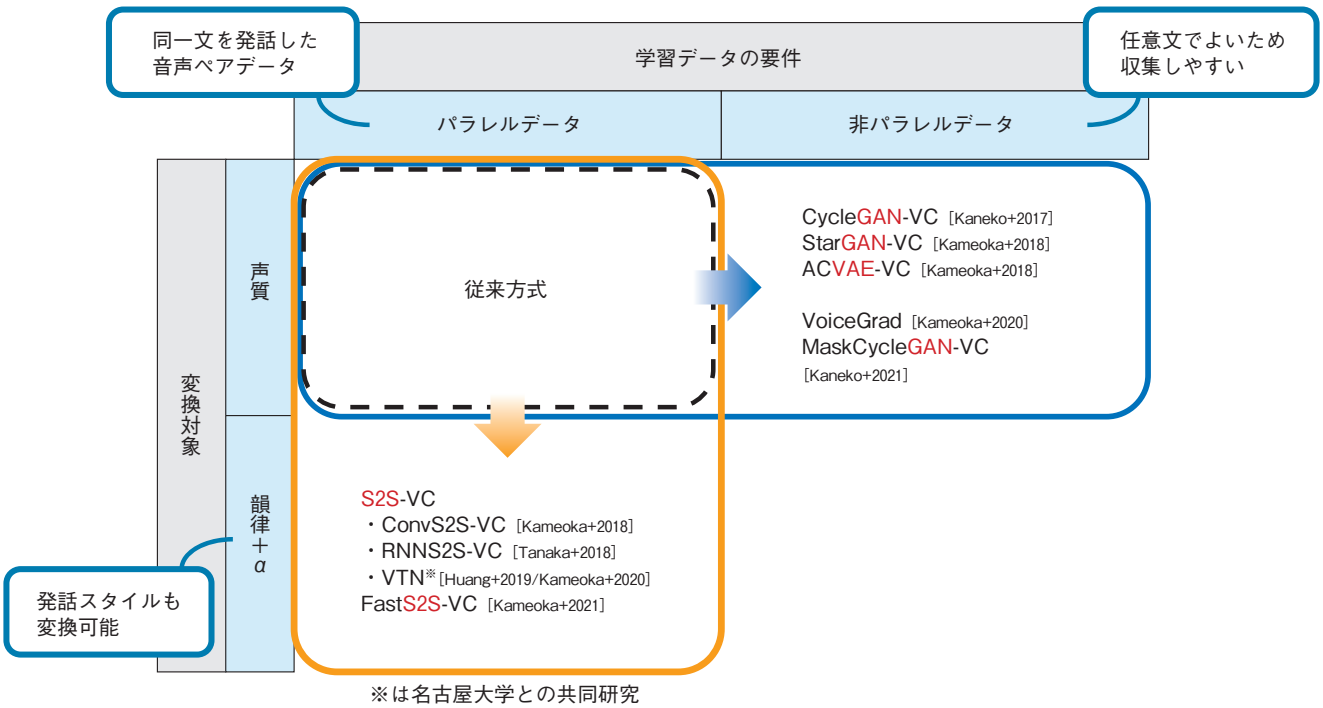
コミュニケーションには発信者と受信者が存在しますが，それぞれが望む表現でメッセージを受け渡しできるようにするため，発信者から送信される信号を状況に適した表現にリアルタイム変換するシステムの構築をめざしています．このようなシステムを実現するうえで今のところ核となると考えられるのが音源分離技術と音声変換技術で，前者が受信者側の聴覚機能を補完する技術に相当し，後者が発信者側の発声機能を補完する技術に相当します．音源分離は前回お話しした「外界音を対象とした要素分解」に該当し，混合音に含まれる複数の音を分離抽出し，残響や雑音を取

り除いたりすることで対象音を強調することが目的になります．音声変換についても前回少しだけ触れましたが，発話内容を保持したまま音声の特徴を所望のものに変えることが目的になります．

さらに，音だけでなく動画像やテキストなどの多種のメディアを有効活用した新たなコミュニケーション方式の可能性を模索しています．例えば，顔に合った音声を生成したり，声に合った顔画像を生成したりすることで，コミュニケーションに広がりを与えられないかということを考えています．

前回，さらに追究したいとお話しされていた高い品質と自然性を意識した音声生成についてはいかがですか．

前回も少しだけ触れましたが，これまで音声変換にかかわる基礎技術およびその周辺技術を多く開発してきました．私たちが音声変換の研究に着手したのは2016年ごろだったのですが，当時主流となっていた従来方式では，同一の文章を発話した音声ペアを用い，同じ音素を発している時刻が合うように一方の音声を時間伸縮したうえで，音声変換器，つまり元音声の特徴を目標音声の特徴に変換する変換則を学習するアプローチがとられていました．このような同一の文章を発話した音声ペアのデータをパラレルデータと言います．もちろん，パラレルデータを多く集められる条件ではこのアプローチは有効なのですが，例えば目標音声が特定の有名人の声の場合など，パラレルデータを容易に取得できない場面も多々あります．そこで，当時機械学習やコンピュータビジョンなどの分野ですでに脚光を浴びていた変分自己符号化器（VAE：Variational Autoencoder）や敵対的生成ネットワーク（GAN：Generative Adversarial Network）といった深層生成モデルに目を付け，任意の文章を発話した元音声および目標音声のサンプルからでも音声変換器を学習することが可能な非パラレル音声変換手法を考案しました（**図1**）．これらの手法は学習にパラレルデータを必要としないので，音声変換の利用場面を大きく



※は名古屋大学との共同研究

図1　深層生成モデルによる柔軟な音声変換の実現

広げることが期待されます．

また，当時のほとんどの従来方式では，変換対象の音声特徴が声質に限られており，抑揚やリズムなどの発話スタイルを変換するまでには至りませんでした．そこで私たちは声質だけでなく発話スタイルも変換できるような方式を創り出したいと考え，当時すでに機械翻訳や音声認識，テキスト音声合成などで多大な効果が示されていた系列変換（S2S：Sequence-to-Sequence）学習と呼ぶ枠組に着目しました．S2S学習は，長期依存関係をとらえながらあるベクトル系列から（異なる長さの）別のベクトル系列に変換するニューラルネットワークモデルを学習する枠組です．ポイントは注意（Attention）機構と呼ぶモデル構造にあり，これにより変換元と変換先の音声特徴量系列の要素間の対応付け規則とともに要素間の変換則を学習することが可能になります．当時S2S学習アプローチを音声変換に適用する試みは私たちが知る限りほとんどなされていなかったのですが，これをいち早く試したところ，期待していたとおり声質以外にも抑揚や発話リズムも柔軟に変換できるようになることが実験を通じて分かり，同僚たちと興奮したのを覚えています．

現在の音声変換の最先端手法は，ほぼ例外なく，元音声からメルスペクトルと呼ぶ音声特徴量ベクトルの系列を抽出して変換するステップと，変換したメルスペクトルの系列から音声波形を生成するステップからなります．前述のVAE，GAN，S2S学習に基づく手法はいずれも特徴量変換を行う前段のステップに相当する技術でしたが，後段のステップを波形生成と言い，ニューラルネットワークで表現した場合の波形生成器をニューラルボコーダと言います．音声研究に詳しい方であればご存じかもしれませんが，WaveNetと呼ぶ高品質波形生成法が2016年にDeepMindから発表され，以降多くの研究者により盛んに高速化，高品質化，学習効率向上の研究が行われています．これまで私たちは特徴量変換技術の研究をメインに進めてきましたが，最近は波形生成の高品質化と低遅延化のための研究にも力を入れ始めているところです．

以上のそれぞれの成果はICASSPやInterspeechなどの国際会議やIEEE Transactions on Audio, Speech, and Language Processingなどの学術論文誌に採録され，これまでのところ合計で1000回以上引用されています．私たちの最近のアクティビティも徐々に認知されてきていると感じます．

音声変換・音源分離技術の高精度化・効率化・柔軟化のための機械学習基盤の構築

コミュニケーションに悩む人には朗報ですね．具体的な応用先を聞かせていただけますか．

まず音声変換技術に関してですが，これまで実験的に良い感触が得られた応用先としては，話者変換以外ですと，英語の訛りの変換，ささやき声の変換，電気喉頭音声の変換，感情表現変換，言い淀みの変換などがあります．英語の訛りの変換は，話し手の英語を聴き手にとって聴き取りやすい訛りに変換することで，会話を円滑化するのに役立つと考えています．例えば，日本人にとっては（もちろん人によってですが）いわゆる日本語訛りの発音の方がネイティブな発音よりも聴き取りやすい場合もあるかと思いますので，あえて訛りを付与するといったような使い方も考えられます．ささやき声の変換は，ささやき声を自然発声風の音声に変換することを目的としたタスクです．例えば１人で電車内や喫茶店にいて声を発するのがはばかられるような場面で電話やオンラインミーティングをしたい場合があると思いますが，これが実現できると，周囲に声を聞かれないようにささやき声で話しても，相手側には普通の声として届けられるようになります．電気喉頭音声の変換は，電気喉頭音声を健常な音声に変換することを目的としたタスクです．電気喉頭音声は，喉頭摘出手術などで声帯を失ってしまった発声障がい者が電気式人工咽頭を用いて発した音声で，抑揚に乏しく機械的な音声になってしまいがちですが，音声変換技術によりそういった音声を健常者のような音声に変換することが可能になります．ほかにも発話スタイルを変化させることで感情表現も変換することも，「あー」や「えーと」などのような言い淀みやフィラー

を自動的に省略して発話全体を流暢にすることもある程度可能であることが分かってきました．これらの音声サンプルはデモサイトで聴くことができますので，ご興味がある方はぜひアクセスしてみてください[(1)〜(3)]．また，音声分離については，前述のVAEを音源信号のモデル化に用いた多チャネル音源分離法を以前提案し，その高速化と高精度化に向けた検討を行ってきました．これまで多チャネル音源分離の研究分野ではせいぜい5音源程度の混合信号しか扱われていませんでしたが，私たちが提案した手法により18音源もの混合信号を高精度に分離できることを実証し，世界でも例をみないレベルの性能を達成することができたと考えています．こちらの音声サンプルもデモサイトで聴くことができますので，ぜひアクセスしてみてください[(4)]．

従来の手法と提案された手法を比較しながら聴いてみると，この技術の素晴らしさが良く分かりますね．

ありがとうございます．さらにこれらの検討に加えて，音以外のメディアを活用しながら音声を生成・制御したり音声を活用して音以外の信号を生成・制御したりするクロスモーダル信号生成の研究にも取り組んでいます．例えば顔に合った音声の生成や声に合った顔画像生成などです（**図2**）．この取り組みでは，音声コミュニケーションをより豊かにすることだけなく，コミュニケーション機能拡張において直感的な制御を可能にすることをめざしています．

具体的な取り組みの一例として，音声のみから話者の顔を予測し，予測した顔を画像として出力するクロスモーダル顔画像生成や，声質変換において目標声質を（話者IDの代わりに）顔画像により指定することができるクロスモーダル声質変換などの検討を行いました．これらのデモンストレーションを，NTTコミュニケーション科学基礎研究所（CS研）オープンハウスで実演したところ好評を博し，各種メディアで取り上げていただきました．

また，音声のみから話者のアクションユニット（顔面筋パラメータ）系列を推定する新たな試みも行いました．私たちの知る限りこのような試みはほかになかったため，どの程度の精度を達成できるかは全くの未知数でしたが，実験を通じてこれがある程度可能であることを明らかにしました．また，音声から推定したアクションユニット系列を用いて顔画像変換を行うことで，声に合わせて静止顔画像の表情を動かすことができるようになります（**図3**）．今後これをさらに高精度化しうまく活用すれば，自分の話し方や声質が会話相手にどのような印象を与えているかを視覚的にフィードバックできるようになり，プレゼンテーション能力やコールセンターなどの接客能力の向上を支援することに役立つかもしれません．

これらの取り組みについてもそれぞれデモサイトを用意していますので，ご興味のある方はアクセスしてみてください[(5)，(6)]．

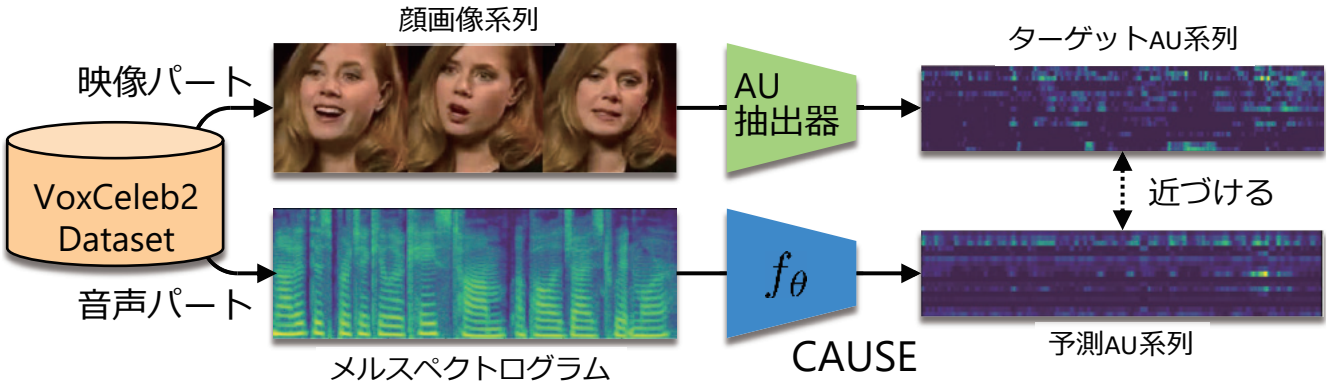
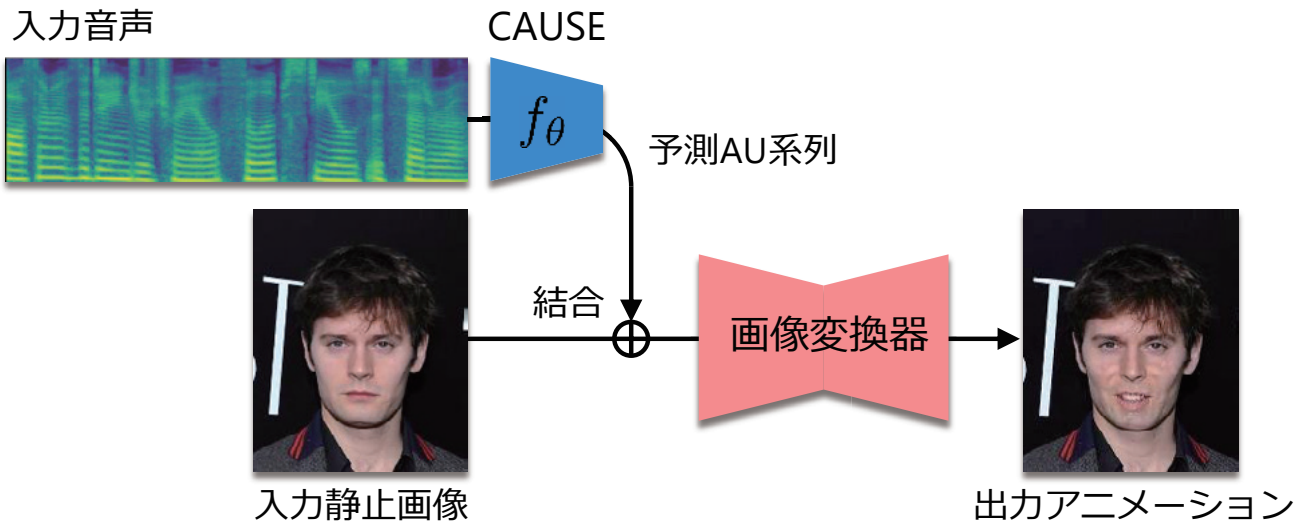


図2　クロスモーダルアクションユニット系列推定器（CAUSE：Crossmodal Action Unit Sequence Estimator）の学習



※　顔画像はVoxCeleb2 Dataset [Chung+2018*]，CelebA Dataset [Liu+2015*]のものを使用

Z. Liu, P. Luo, X. Wang, and X. Tang: "Deep Learning Face Attributes in the Wild," in Proc. ICCV, pp. 3730-3738, 2015.
J. S. Chung, A. Nagrani, and A. Zisserman: "VoxCeleb2: Deep Speaker Recognition," in Proc. Interspeech, pp. 1086-1090, 2018.

図３　CAUSEと顔画像変換器を用いた音声からの顔表情制御

素人発想・玄人実行に努める

研究者として大切にされてきたことを教えてください．

金出武雄先生の著書のタイトルにある「素人発想，玄人実行」は，普段から私が研究者として心掛けていることの１つです．専門的な知識が増えてくるとつい「研究のための研究」に陥り，重箱の隅をつついたような研究テーマを設定してしまいがちになります．それはそれで重要な研究テーマに発展し得る場合もあると思うのですが，１つひとつの研究テーマに対して，素直に面白いと思えるかどうか，本当に世の中の役に立つのかどうか，をできるだけ冷静に自問自答するようにしています．例えばコミュニケーション機能拡張の研究においては，日常生活の中で，普段あまり意識しないような違和感や不自由さはないか，それらを解決するための打開策はないか，ということを常日頃考えています．今，人工知能（AI）や機械学習の分野は発展がものすごく速い激動の時代に入っていますので，常に最新のトレンドや研究動向を追うことはもちろん大切ですが，一度冷静になり，自分の中にある「内なる声」に耳を傾けることも大切だと思っています．

そして最近，AIの研究をやっていて改めて実感するのは，当たり前のことですが，できるだけ多く手を動かすこと，つまりコーディングと実験をできるだけ多く行うことの大切さです．もともと私は１つひとつの問題に対し，じっくりと仮説と理論を立て，定式化したうえでその解法を編み出す研究スタイルが得意なほうでしたが，深層学習やニューラルネットワークを用いた研究では，それとは対照的に，実験による仮説検証を速いスピードでとにかく何回も何回も繰り返すことが重要であると感じています．ニューラルネットワークの挙動は必ずしも直感どおりではなく，生物を相手にしているような感覚がすることがあり，触れれば触れるほど感覚が身に付いてくると感じるので，今は必ず１日１回はコーディングと実験を欠かさず行うようにしています．深層学習ではニューラルネットワークに学習サン

プルをたくさん入力して，学習データに合った振る舞いを学ばせていくわけですが，その訓練プログラムをコーディングしている自分自身が，たくさんのコーディングと実験をとおしてニューラルネットワークの振る舞いを学んでいっている感覚がして，とても新鮮で面白いです．

今後はどのようなことに取り組まれますか．また，後進の研究者にも一言お願いいたします．

まず，感性語による要望にこたえるような音声変換です．例えば「可愛い声」「優しい声」「堂々とした声」にしたい，といったような要望があったときに，それにこたえるような音声変換です．これまで扱ってきた音声変換では変換目標の音声特徴は一意に定義しやすいものでしたが，これらの例からも分かるように感性語の定義は曖昧で人によって異なります．このように定義が曖昧で主観的であるような感性語をいかにして定量化できるかが鍵になりますが，現在その課題に同僚と一緒に取り組み始めています．

また，この音声変換システムの実用化を想定したとき，他人の声になりすます等により悪用される可能性は否めません．今後は，音声変換システムの悪用防止のための研究も視野に入れています．

それから，実用化に向けてはホワイトボックス化したモデルをつくる必要性も感じています．音声変換の例でいえば，リアルタイムに音声を変換するシステムを実際に使用する場合，想定外な変換が行われないように保証する必要があります．変換のされ方によっては話し手の意図に反した印象を相手に与えかねない可能性があるからです．ニューラルネットワークは，学習データに合った振る舞いを学習する能力は非常に長けている一方で，内部がブラックボックス的であるがゆえに，学習データにないデータが入力されたときの振る舞いをなかなか予見することができず，制御するのが必ずしも簡単ではありません．したがって，音声変換モデルを安心して利用できるようにするためのモデル構造や制御メカニズムの研究も今後必要になると考えています．

最後に，後進の研究者の皆さんに向けてですが，研究者の使命は「世の中を良くする」ことだと思っています．皆で協力し，常に便利さや快適さを追究する人間の隠れた欲求にこたえるために知恵を絞り，人が安心・安全に，幸せに生きていける世の中にしていってもらいたいと思います．

研究をしていると辛いことも多いと思います．月並みな言葉かもしれませんが，ネガティブな面ばかりに目を向けず，研究を楽しむことが大事だと思います．今NTT研究所ではリモート勤務の方が多くなっていると思いますが，そういう方々は特に，雑談目的でもいいのでオンラインミーティングを頻繁に開いて同僚や先輩とコミュニケーションを図る場をたくさん設けるよう意識してみてください．話をしているうちに楽しくなってきて，刺激も得られると思います．そして，研究者どうし，相互のリスペクトも忘れずにいたいですね．私は学生と一緒に研究することも多く，論文原稿をチェックする機会がありますが，時折，提案技術の優位性を主張したいがために従来技術を必要以上におとしめるような記述を目にします．しかし，科学技術は先達が英知を結集して少しずつ積み上げてきたものであって，それをさらに良くしようとするのが研究者の仕事です．だからこそ，良いところを見つけ，さらに良くしようという視点で先行研究を眺め，研究に臨んでいただきたいです．

■参考文献

⑴ https://www.kecl.ntt.co.jp/people/kameoka.hirokazu/Demos/s2s-vc/index.html
⑵ https://www.kecl.ntt.co.jp/people/kameoka.hirokazu/Demos/acvae-vc3/index.html
⑶ https://www.kecl.ntt.co.jp/people/kameoka.hirokazu/Demos/stargan-vc2/index.html
⑷ https://www.kecl.ntt.co.jp/people/kameoka.hirokazu/Demos/mvae-ss/index.html
⑸ https://www.kecl.ntt.co.jp/people/kameoka.hirokazu/Demos/crossmodal-vc/index.html
⑹ https://www.kecl.ntt.co.jp/people/kameoka.hirokazu/Demos/cause/index.html

挑戦する
研究開発者たち
CHALLENGERS

成瀬友麻 / 小川香菜子

NTTビジネスソリューションズ
バリューデザイン部　コアソリューション部門
マネージドIT担当

サービス開発は社会にとって「未来」や「希望」．災害大国・日本の課題解決に臨む

日本は地理的な位置や地形，気象などの自然的条件から災害が発生しやすく，災害大国と呼ばれています．自治体においてはこうした災害に対して住民の安全確保，インフラ等への影響の極小化や復旧をはじめとする防災（減災）・災害対策に取り組んでいます．このような自治体の取り組みをサポートするNTTビジネスソリューションズ バリューデザイン部コアソリューション部門の成瀬友麻氏と小川香菜子氏に，自治体の災害対策を支援する新サービス開発の背景，開発に向けた取り組み，そして，サービス開発者としての姿勢を伺いました．

災害発生時に自治体が抱える課題にこたえる新サービス「Spectee Pro for elgana」

現在，手掛けているサービス開発の背景・概要をお聞かせいただけますか．

（成瀬）日本は災害大国として知られ，私たちは阪神・淡路大震災，東日本大震災等，多くの人の命を奪う大きな自然災害を経験しています．こうした災害への対応は，1961年（昭和36年）に制定された災害対策基本法の下，国の防災計画「防災基本計画」，指定公共機関の「防災業務計画」，地方自治体の「地域防災計画」等が作成され，国や自治体を挙げて実施されています．災害対策基本法は，東日本大震災をはじめとしたさまざまな災害を教訓に，2011年から2019年の8年間で大幅な改正が行われ，自治体には災害時と平常時それぞれにおいて役割が与えられました．災害時の対応には情報の収集，発信と広報の円滑な対応に加えて，住民等の円滑かつ安全な避難の確保，被災者保護対策の改善等が盛り込まれました．

実際の災害発生時には，自治体では現場の状況を把握して，その結果を被災状況に応じた復旧作業や住民周知などの災害対応に活用することになるため，被災状況把握は急

務となります．実際の災害発生時において，この状況把握は主として現地へ自治体職員を派遣して調査することになり，非常に手間取るとともに，被災現地と災害対策本部等との間の情報共有は，電話やメールなどで行われることが多く，的確な情報の伝達・集約が困難となっていました．

こうした自治体共通の課題を解決するために，「Spectee Pro for elgana」というサービスを開発しました（**図1**）．このサービスは，SNSや河川・道路カメラ，人工衛星データなどを基にAI（人工知能）で災害時の被害のシミュレーションや予測などさまざまな角度からの情報を“可視化”した地図画面上に，現地のスマートフォン等のGPSによる位置情報を基に，撮影した画像と作成した文章を重畳表示し，チャットや電話等により現地との間でセキュアなコミュニケーションを図ることで，的確な情報収集を可能とするものです．さらに，基本的に被災現地に駆け付けて状況把握や救済活動を担当している消防団員に依頼して被災状況を送信してもらうことで，自治体職員が現地に向かう時間と労力も削減できます．

2023年2月に名古屋市様と，このサービスを利用して都度更新される災害情報をリアルタイムに確認できる利便性と効果，サービスの有用性や改善点を検証しました．災害時における情報収集の利便性が高まるという定性的な効果が確認できたとともに，「市町村で災害対策に役立つサービスである」といった名古屋市役所職員の方よりコメントもいただきました．

技術開発と立ち位置を異にするサービス開発

どのようなプロセスでサービス開発を行っているのか聞かせてください．

（成瀬）一般的にサービス開発は，新しい技術やプロダクトを市場のニーズに対応させてサービスにつなげていく「プロダクトアウト」のアプローチと，市場の課題やニーズに対応していくために必要な技術やプロダクトを探したり，新規開発したりすることでサービスにつなげていく「マーケットイン」のアプローチがあります．研究所の成果等新技術のサービス化は「プロダクトアウト」となりますが，私たちはお客さまに近い立場にいるので「マーケットイン」でサービス開発を行っています．

サービス開発は，いずれのアプローチにおいても，サービスコンセプト企画，サービスアイデアとビジネスモデル検討，市場調査，実現方法検討，オペレーション・営業チャネル検討，事業性判断といったプロセスを経て，サービスとして市場にローンチされます．

「Spectee Pro for elgana」の開発においては，防災・災害対策に着目して自治体等のお客さまにヒアリングを行い，前述のように被災状況の把握に課題を抱えている自治体が多いことを確認しました（市場調査）．課題を掘り下げていくと被災現地との間のコミュニケーションを工夫することで対応できることに気付きました（サービスコンセプト，サービスアイデア・ビジネスモデル）．実現方法検討にあたってはコミュニケーションという意味で，NTT西日本グループ開発のセキュリティの高さを特長に，180万ID以上の導入実績のある（2023年1月時点），ビジネス

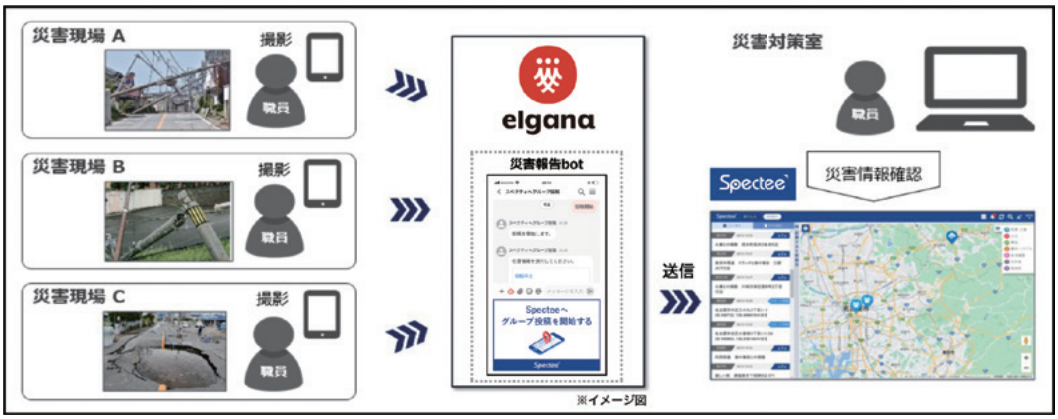


図1　サービス概要イメージ

チャットツール「elgana」に着目しました．

そして，NTT西日本グループのオープンイノベーション施設「QUINTBRIDGE(クイントブリッジ)」で2022年に開催された，「elgana」の連携パートナーについてのビジネス共創ピッチプログラム「Business Match-up For Next Value」にて採択された「株式会社Spectee（スペクティ）」と連携を開始しました(1)．これがきっかけで，AIリアルタイム危機管理サービスで，災害や事故などのリスク情報をリアルタイムに配信するほか，SNSや河川・道路カメラ，人工衛星データなどを基にAIで災害時の被害のシミュレーションや予測などさまざまな角度から被害状況を“可視化”する，スペクティ社の「Spectee Pro」を知り，「elgana」と「Spectee Pro」をAPI（Application Programming Interface）連携させることで，「Spectee Pro」の地図上に，「elgana」で撮影した画像と作成した文章を投稿し，画面上に仕組みを新たに構築することとしました（**図2**，**3**）．

（小川）サービスは，ある意で味研究成果や開発技術の事業への出口であり，逆に技術に関係なく市場から収入を得る入口です．事業に直結するサービス開発であるがゆえに，単なる需要予測や事業収支のみならず，将来的に抱える事業リスクも考慮のうえ事業化を判断する必要があります．サービスが厳しい競争環境下にあるときは，他社の戦力やサービスの相違等も考慮した戦略も立てていく必要があります．このためには市場調査とその分析には特に注力することになり，PoC（Proof of Concept）においても市場における許容性，必要度，お客さまへのインパクト等の検証も重要なものとなります．このように，サービス開発は技術開発とその立ち位置を少し異にするものです．

サービス開発の醍醐味はお客さまの喜びの声を聞くこと

サービス開発を手掛ける際に大切にしていることを教えてください．

（成瀬）サービス開発の醍醐味はお客さまの喜びの声です．私たちは常にお客さまのリアルな声を大切にしながらサービス開発に臨んでいるのですが，課題解決につながった等，お客さまからの声を直接伺えることが何よりも嬉しいです．社会の課題解決に私たちのサービスを役立てていただくために，お客さまの視点を常に意識する必要があり，そのために次の点に配意しながらサービス開発に取り組んでいます．

（小川）私は，サービス開発プロセスの中で技術に近い分野を担当しているのですが，同じようなものを複数つく

図2　利用シーン（災害発生時）

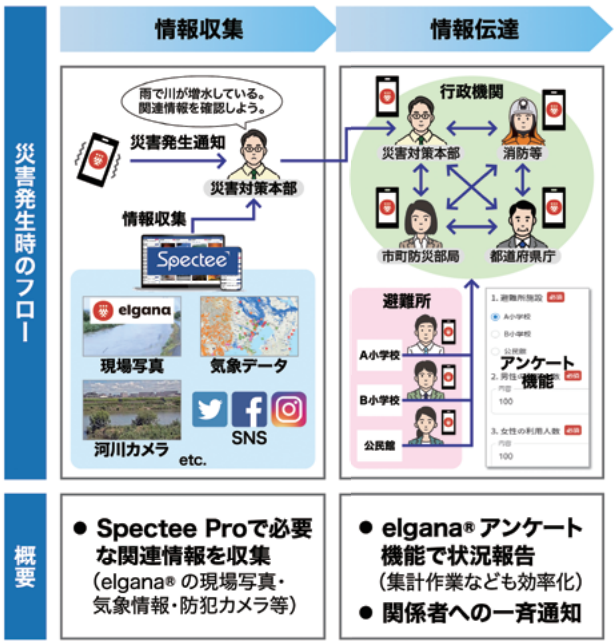


図3　利用シーン（情報収集～情報伝達）

らないこと，特注品をつくらないことです．同じようなものを複数つくるということは，社内においてカニバリゼーションを発生させ，営業担当が何をお客さまにお届けすればいいのかという判断をくるわせるばかりではなく，その先のお客さまも惑わせてしまいます．そして，開発内容も重複してくるので開発投資の重複にもつながり，お客さまへの提供価格高騰に直結します．そこで，サービスの開発にあたっては，複数のお客さまへの提供機能・価値の最大公約数を意識し，それをコストミニマムで実現することを心掛けています．ただ，どうしてもお客さま固有の部分への対応が必要な部分も出てくるので，その場合はパラメータの設定変更やカスタマイズ，サービスの外側での機能開発によるインテグレーションにより対応していくように考えています．

また，自身の関係する技術に深く入り込むほど，視野が狭くなってくると感じることがあります．サービス開発では検討対象が広範にわたっているため，広い視野と高い視座が必要となるのですが，これに逆行してしまうことになるので，開発の早い段階から市場やオペレーションに近い視点を反映していくために，営業やオペレーションに関係する各部署に相談に行きます．さらに自分でつくったモノを営業と一緒に売りに行き，お客さまの声を直接伺ったこともあります．

（成瀬）「我が社のサービスは最高だ」と自負することは良いのですが，それだけになってしまうのは非常に危険です．「独りよがり」になってしまうと，時代に乗り遅れ，他社に太刀打ちできないサービスが出来上がってしまうことがあるからです．世界を見渡し，自らの考えが世の中にマッチしているのかは常に検証する必要があると思っています．お客さまと直接お会いしている営業部隊にサービスの有用性の高さを確認する等，出口戦略も見据えてサービス開発をすることを心掛けています．

加えて「鳥の目，虫の目，魚の目」で見ることも重要です．俯瞰的な視野で物事を中長期的にとらえることや，今まさに現場が抱える課題は何かをつぶさにとらえる視点等，これらを同時に持てるように心掛けています．

サービス開発にかける熱意が伝わってきました．では最後に，サービス開発者にとって重要なスキル，サービス開発者としての思いを教えてください．

（成瀬）サービス開発者は社会にとっての「未来」だと考えています．幅広い視点で社会を見通せる力が一番大切だと思います．そして，調整力も重要です．サービス開発という立場には，お客さまをはじめ営業，企画，オペレーション等多くのステークホルダーがいます．お客さまはもちろんですが，意見が食い違う関係各所とうまく調整して進めていかないことには，サービスを世に出すことはできません．その意味で調整力は大切だと考えています．そして，最後にスピード感です．時に技術開発担当者には申し訳ないなと思いつつ，市場においていかれないように「速く仕上げてほしい」等と無理を言ってしまうこともあります．市場は待ってくれませんし，サービスが市場に出たところが出発点なので，こういった事情を理解・認識していただけるよう調整しています．

私は２人の子育てをしつつ，残業も出張もしながら働いています．子育てをしながらだと，どちらかをあきらめないといけないと思いがちですが，私はそうはしたくないですね．仕事もプライベートも双方100の力で臨みたいのです．将来的には新規ビジネスを生み出し，それが市場で認められた結果，開発者としていわゆるバイネーム人材になりたいというのがサービス開発者としての思いであり，憧れでもあります．

（小川）仕事でいわゆる無茶ぶりをされても，「できない」「やらない」と言わないことです．まずはどうやってそれを実現できるだろうかと考えることを大切にしています．また，「５分でできることは５分でやる」という姿勢も重要です．頼まれたことを，今忙しいからと後回しにすることはあると思いますが，中身が５分でできることならすぐに対応してやってしまうことです．

サービス開発者は社会にとって「希望」であると私は考えています．これからも仕事とプライベートに150×150の全力で臨んでいきたいと思います．

（成瀬）出来上がったサービスは我が子のように愛おしいんですよ．１社でも多くのお客さまに喜んでいただくために，ファースト案件をめざして，これからもサービス開発に臨みます．

■参考文献

⑴ from NTT西日本：“オープンイノベーションによる未来共創プログラム『Future-Build』で社会課題解決・未来社会創造に挑戦した６プロジェクトの成果報告，” NTT技術ジャーナル，Vol.35，No,5，pp. 72-73，2023.

明日のトップランナー

NTTコミュニケーション科学基礎研究所

安　謙太郎 特別研究員

触覚提示の端緒を開く，非電力・磁力による「マグネタクト技術」

ヒューマンコンピュータインタラクションの研究領域では，人がコンピュータを快適に利用するためのさまざまな研究が行われています．NTTではその取り組みの一環として，通信トラフィックの増大による大容量電力消費や地球温暖化といった課題に向けた非電気的デバイスの実現に向けた研究開発を行っています．今回は，電気を使うことなく磁力によって触覚提示を行う「マグネタクト技術」について，安謙太郎特別研究員にお話を聞きました．

◆PROFILE：2013年慶應義塾大学大学院メディアデザイン研究科博士後期課程修了．2013年～2016年シンガポール国立大学（NUS：National University of Singapore）にてResearch Fellow．2016年日本電信電話株式会社入社．2019年より特別研究員．ヒューマンコンピュータインタラクション（HCI：Human Computer Interaction）領域における触覚情報提示技術の研究に従事．

磁力を用いて凹凸感を提示する「マグネタクト技術」

◆ご研究されている「マグネタクト技術」はどのようなものでしょうか．

私はNTT入社以降，マグネットシートを使った触覚情報提示技術を研究しています．マグネットシートとは一般的に売られているごく普通のシート状の磁石で，ビデオテープやカセットテープにも使われる磁性材料を樹脂と混ぜて平たくしたものであるため，強い磁場を近づけるとS極とN極の磁場パタンを書き込むことが可能です．この性質を利用して，磁場パタンを書き込んだマグネットシートどうしを重ねてすり合わせると，シート間に磁力の引力と斥力が発生し，平面どうしであるにもかかわらずシート間にボコボコとした凹凸感を発生させることができます．この技術をMagnet（磁石）とTactile（触覚）を組み合わせ「マグネタクト」と名付けました．

マグネタクト技術には従来技術と比較して「電力を必要としない」という大きな強みがあります．私はNTT入社以前にシンガポール国立大学（NUS：National University of Singapore）で3年間研究員として働いており，そこで当時の同僚で現在は東京電機大学准教授の勝本雄一朗氏と一緒に研究していた「Bump Ahead」の技術がマグネタクト技術にも応用されています．このBump Aheadは，S極とN極のフェライト磁石が交互に敷き詰められている板の上で，4つの磁石を内蔵させたデバイスをスライドさせることにより，磁力の引力と斥力による「ボコボコ」とした非常に強い力触覚を発生させることができます．またデバイスに内蔵された4つの磁石を45度回転させることによって，磁力の総和を変化させ触覚の有無を一瞬で切り替えることも可能です（**図1**）．このデバイスが開発される以前は，磁力を操作するために電磁石に電流を流す手法が一般的であり，強い磁場を生み出すための大量の電力やコイルの過熱などさまざまな課題がありました．そうした中で，電磁石を使用せずに磁石を回転させるだけで触覚のオンオフを即座に切り替えられるというBump Aheadの技術が，従来の課題を解決できたのは大きな研究目標の達成でした．

◆磁力によって凹凸感を発生させる「マグネタクト技術」はどのように生まれたのでしょうか．

Bump Aheadの技術には，敷き詰めたフェライト磁石の部分に大きな課題が残っていました．例えば直径20 mm・厚さ5 mmのフェライト磁石を40 x 40 cmの広さに敷き詰める場合，合計で400個の磁石が必要になり，さらに重さは約3 kgと気軽に持ち運ぶことが難しくなってしまいます．また400個の磁石を敷き詰めている間にも磁石は引き寄せ合うため，一瞬の気の緩みで連鎖的にすべての磁石がくっついてしまうという悲劇も技術実装の際に何度か体験しました．

このままでは実際に世の中で使われることは難しいと考え，より簡単にBump Aheadの技術の課題を解決し実現する方法を考えていました．ある日，研究室に行くとたまたまマグネットシートの上にネオジム磁石が置いてあり，当時研究に取り入れたばかりのマグネットビューアという磁場を可視化できるシートでこれを観察してみたところ，マグネットシートの磁場が上に置いてあ

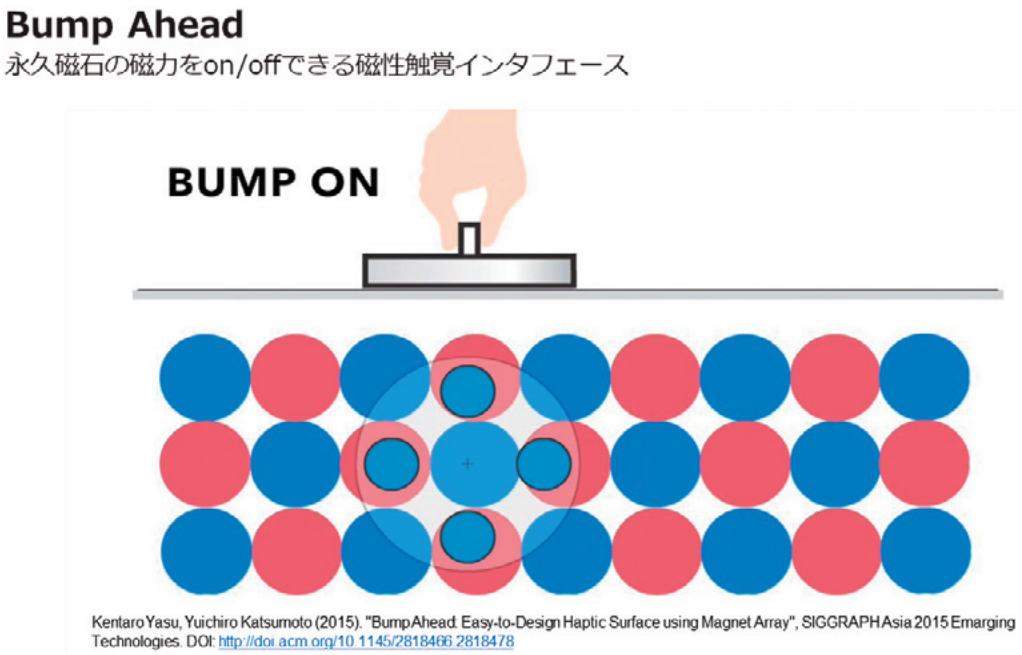


図1　Bump Aheadの技術

るネオジム磁石によって書き換わっていることに気が付きました．しかしマグネットシートはフェライト磁石に比べ磁力が非常に弱く，すり合わせないと凹凸感が感じられないため，当初はあまり実用的ではないと判断しており研究には至りませんでした．その後NTTへ入社してから「磁場パタンを簡単に書き換えるのであれば，すり合わせたときの感触を計算で予測して多様に変えられるのではないか」「磁場を書き換えることによりさまざまな応用が可能になるのではないか」と考えを改めて研究を進め，完成したのが「マグネティックプロッター」です．

マグネティックプロッターはマグネットシート上の磁場を書き換える装置です．「磁場パタンが簡単に書き換えられるのであれば，機械を使って詳細なパタンを書き込めるのではないか」という着想を得て研究を開始しました．小型のネオジム磁石を家庭用のプロッティングマシン（紙にペンで図形を書くことができる装置）に取り付けることで，マグネットシートに詳細な磁場パタンを着磁して，2枚のマグネットシートをこすり合わせたときのボコボコ感を磁場パタンによって制御することができます．もちろんネオジム磁石を手に持ち磁場パタンを書き込むこともできるのですが，機械を用いることで高い精度で詳細な磁場パタンを作成可能です．**図2**で示しているように，書き込む磁場の間隔や組み合わせを変えることによって凹凸感を変化させることもできます．

またこの技術が完成した翌年には，マグネティックプロッターを使い触覚インタフェースをつくる方法についての研究を行いました．マグネティックプロッターを使って詳細な磁場パタンを書き込んだマグネットシートを，タブレット型端末などのタッチスクリーンに貼り付けることで，クリック感のあるボタンやスイッチをつくる手法です．これらの研究の成果提供をする際に，改めてマグネットシートを用いた触覚技術が大きな可能性を秘めていることを認識し，その技術全般に「マグネタクト」という名前を付けました．

◆「マグネタクト技術」を世の中に発信する取り組みについて教えてください．

2019年にマグネタクト技術を成果提供してから，さまざまなかたちで世の中の人に使ってもらう方法を検討してきました．2020年には「Magnetact Idea Session」という，クリエイターの方々と一緒にマグネタクトの使い道を考えるワークショップを開催しました．さまざまなアイデアが出る中で，日本を代表するクリエイターの1人である石川将也氏が「磁石シートと紙を組み合わせて動物のような紙工作に動きを与える」というアイデアを提案してくれました．私が提供したマグネタクトの技術は磁力によって触覚を提示するものでしたが，それだけでなく磁石シートと厚紙を紙でつなぎ合わせて「動き」の領域に技術を発展させることができたのです．このアイデアは私の研究テーマであった「知識・経験・設備・環境のない人でも動くものをつくれるようにする」を叶えるもので，非常に嬉しいものでした．そこから短い期間に石川さんが中心となり，福永紙工という紙製品製造のスペシャリストの協力を得て，2021年にこれは「マグ

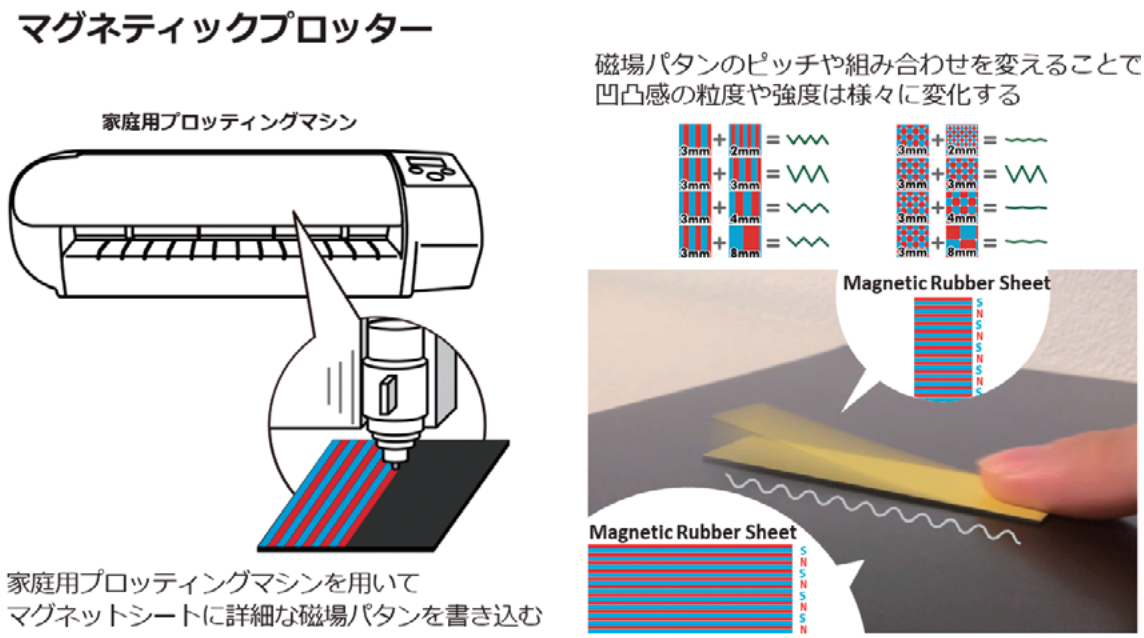


図２　マグネティックプロッターの技術と触覚提示の組み合わせ例

ネタクトアニマル」として製品化されています．そして製品化以降はオンライン，オフライン問わずさまざまな場所でワークショップが開催され，多くの方に磁石の不思議さと動くものをつくる楽しさを提供し続けています．

また最近では「マグネシェイプ」という技術を開発しています．これは磁場パタンが書き込まれたマグネットシートの磁力が磁石を内蔵したピンを上下させるというものです．非常にシンプルな構成ながら，非電気的に文字やアニメーションを表示することができます（**図3**）．

新たな「つくり方」を創出し多くの人に価値を届けていく

◆今後のご研究のビジョンを教えてください．

私の研究領域であるヒューマンコンピューターインタラクション（HCI：Human Computer Interaction）では，人間とコンピュータの相互作用や人間にとって使いやすいインタフェースなどが日々研究されています．その中で私の技術は電力も機械も必要としないため，一見コンピュータとは関連のない技術に思えるでしょう．しかし例えばマグネタクトアニマルの「紙の形状や紙に貼り付けるパーツなどによって動きを設計する」という作業手順は，コンピュータを用いたプログラミングにとても似ています．このマグネタクトアニマルをはじめとした磁性技術は，コンピュータの作業概念を，コンピュータを使用することなく体験・学習できる装置として大いに役立つと考えています．また現在のコンピュータは電力で動くものが大半ですが，数値計算・論理演算・入力した情報に基づいた出力を実現する手段は，必ずしも半導体と電流だけではありません．実際に世界へ目を向けると，粘菌やDNAを使った情報処理技術や，物体や流体の物理的特性に計算を行わせる仕組みがさかんに研究されており，HCI研究領域でも「programmable matter」または「programmable material」と呼ばれる非電気的デバイスを用いて形状や色や動きなどをプログラミングする試みが数多く提案されています．私が研究している磁性材料を用いた磁場制御・情報提示技術も，既存の「コンピュータ」という概念を拡張して，多くの人にものをつくる手段を与えていくのではないかと考えています．

◆研究開発を進めるうえで，大切にされている考え方を教えてください．

私の好きな曲で椎名林檎さんの『ありあまる富』の一節に「価値は生命に従ってついている」という言葉があります．この歌詞の意味するところを「何を奪われても新しいものを生み出す力こそが人間の強さだ」と解釈すれば，新しいものを生み出していくことへの大きな励みになります．また私自身がつくったものを人に見せて世の中に発信するだけではなく「新しいつくり方を創出する」というところに注力し，多くの人に新しいつくり方でおもしろいものを生み出してほしいと願っています．

そして研究では新規性や目新しさが求められることが多くありますが，最先端の道具や材料にこだわりすぎると高価すぎて誰にも使えないものや本当に必要な人に届かない技術が完成してしまいます．そうならないために，研究を進めるときには「誰がどこで使うのか」「今までできなかったことは何か」といったことを常に意識して取り組まなければならないと思います．私の研究

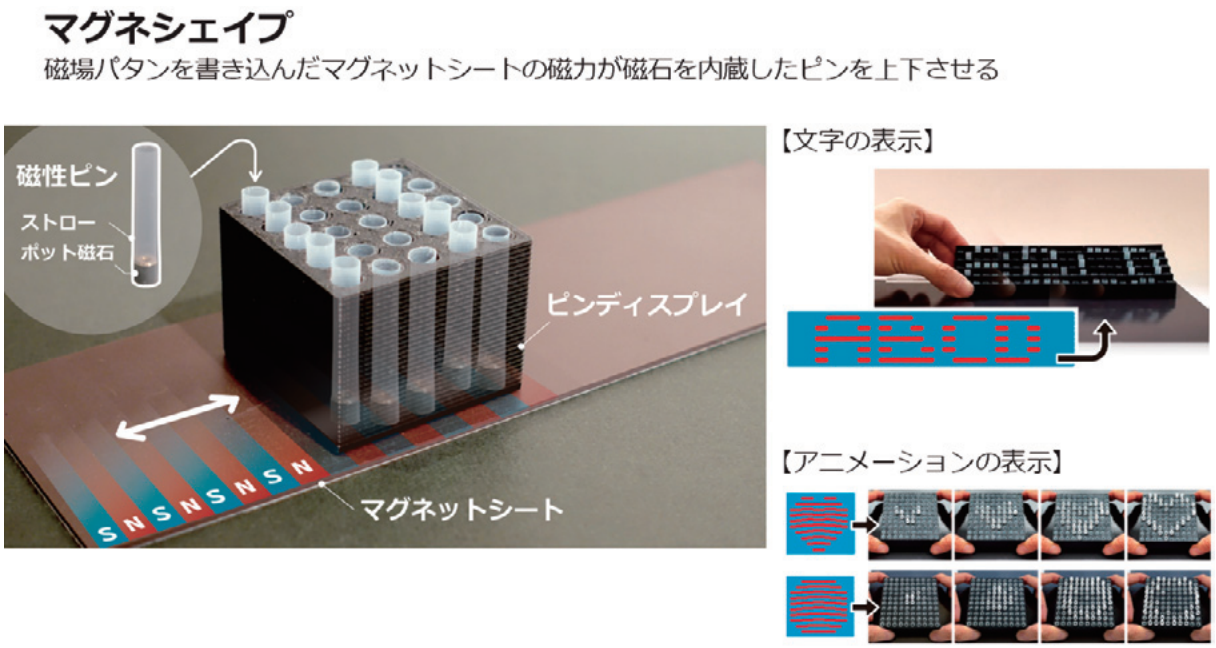


図 3　マグネシェイプの技術と情報表示例

であれば，ホームセンターやスーパーなどへ行って一般の方が手に入りやすい素材をチェックし，その素材を使った新たなつくり方はないだろうかということを常に考えています．今後も技術が必要とされているところから目をそらすことなく，研究に邁進していきたいと考えています．

◆最後に，研究者・学生・ビジネスパートナーの方々へメッセージをお願いします．

私の所属するNTTコミュニケーション科学基礎研究所の感覚インタフェース研究グループでは，メンバーが各々独立して独自のテーマに取り組んでいます．これまで私も磁性材料による力場提示を使った研究を自分の判断に基づいて行ってきており，テーマ設定や発表する学会などをほとんど自分の意志で決めることができたのは幸運だったと思います．企業で研究を行う場合には，事業の中でその研究がどのような意味を持ち，短期的にどのような利益につながるのかといった視点は重要だと思います．しかしNTTで研究テーマを決める際には，会社の利益に直結するような短期的視点より，長期的かつ戦略的視点が求められるため，非常に研究のしがいがある環境だと感じています．また論文執筆以外に自分で進めた研究の特許申請・デモ制作・映像制作・事業化なども執り行う必要がありますが，NTTでは事務・知財・事業化推進などのサポートや，理解ある上司と同僚のおかげで研究をうまく進められていることに感謝しています．

そしてこれからも研究を進めていく中で，論文を発表することはゴールではなく，むしろスタートととらえて取り組んでいきたいと考えています．確かに発表論文数は研究者評価の1つの指標として使われてきましたし，学生は一定数の論文を発表することが卒業要件に必要かもしれません．しかし私は，自分の技術が誰かに使われて初めて大きな喜びを感じることができる人間です．そのため，技術をより多くの人に簡単に使えるかたちで提供する努力を続け，マグネタクトアニマルのように私が考えつかなかったようなものが誕生する瞬間を楽しみにしています．もし私の技術を使ってみたい，という方がいらっしゃいましたらぜひコンタクトいただけますと幸いです．

（今回はリモートにてインタビューを実施しました）

株式会社NTT EDX

https://www.nttedx.co.jp/

ICTで学びを新たなステージへ導くパイオニア

NTT EDXは，出版社，書店，高等教育機関等と連携して学修者本位の教育の実現をめざした，「電子教科書・教材配信サービス」を展開している．「ICTで学びを新たなステージへ」というビジョンを掲げて高等教育の高度化・教育のDX（デジタルトランスフォーメーション）をめざす思いを金山直博社長に伺った．

NTT EDX　金山直博社長

電子教科書・教材配信サービスで高等教育の高度化，教育のDXをめざす

◆設立の背景と会社の概要について教えてください．

平成30年の中央教育審議会で出された「2040年に向けた高等教育のグランドデザイン」において，高等教育のあり方とそのプロセスの可視化に関する方針が提示された後，コロナ禍をきっかけとして大学においてリモートベースの講義が一般化してきました．この動きに呼応してNTT西日本が，大日本印刷との協業により，大学に向けて電子図書館，電子教科書といったソリューションを提供してきました．

当時は，丸善雄松堂や大学生協等が独自のプラットフォームにより同様なソリューションを提供していたのですが，利用者の立場からみるとViewerがプラットフォームごとに異なる，出版・書店業界としても扱える電子書籍等がプラットフォームに依存するといった課題がありました．教育の質を高める，電子化による大学や出版業界のDX（デジタルトランスフォーメーション）といった社会課題は共通なので，NTTグループとして，これまでの取り組みにより得られた知見をベースにプラットフォームの統合をはじめとして社会課題の解決を目的に，大日本印刷とNTT東日本の参画を受けて3社により，2021年10月にNTT EDX（エディックス）が設立されました．社名はEducation × DXに由来し，「ICTで学びを新たなステージへ」を企業ビジョンとして，会社の登記地である大阪，本社のある東京の2カ所で，事業運営をしています．

◆具体的にどのような事業展開をしているのでしょうか．

学修者本位の教育の実現をめざした，電子教科書・教材配信サービスを展開しています（**図1**）．紙ベースの書籍の場合，基本的に，出版社等で作成された書籍は，流通網により書店等を経由して読者の手に渡ります．電子書籍の場合は，書店を通じて購入した電子書籍がViewerを通じて利用者に届けられます．NTT EDXの電子教科書・教材配信サービスは高等教育機関をターゲットとして特化されたものです．

基本的なサービスメニューとして，出版社から電子化の許諾が得られた教科書を仕入れ，書店等を通じて教員や学生に販売する「電子教科書取次サービス」，および，購入された電子教科書がViewerを通じて閲覧できるようにする「電子教科書・教材配信プラットフォーム」を提供しています．また，大学等における教育では，教科書ではなく教員が作成した教材が利用されることもありますが，この場合も電子教科書同様にこのプラットフォームにより配信が可能です．この場合の電子教材作成をサポートする「オリジナル教科書・教材制作サービス」も提供しています．さらに，各教科書等へのアクセス状況やマーカーを引いたり，メモをしたりといった学修ログデータも収集しているため，それらを学生の履修状況の把握から講義等における指導へフィードバック，売れ筋教科書の調査といったマーケティングに活用可能な「学修データ利活用サービス」も提供しています．

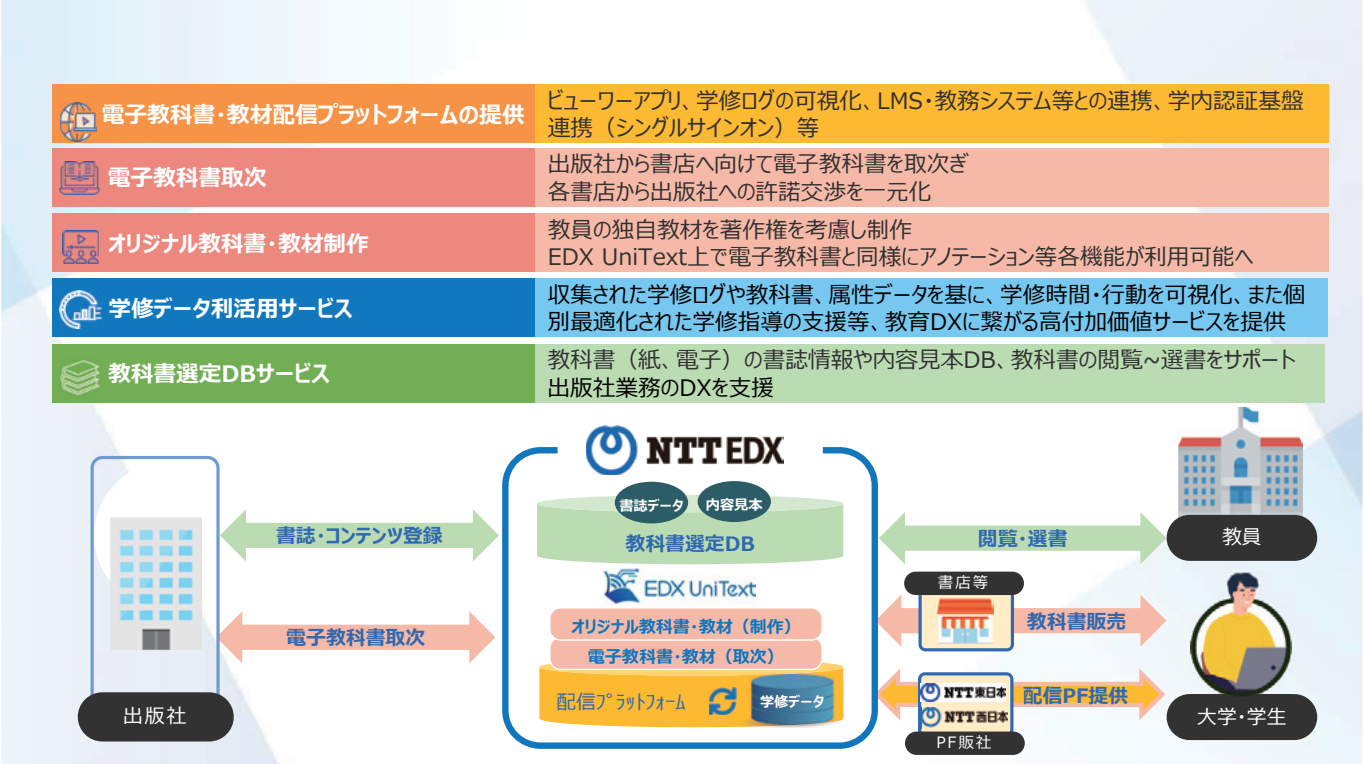


図1　事業概要

市場のパイオニアとして，学生の質の向上や日本がめざしている教育のあり方に貢献

◆事業を取り巻く環境はどのような状況でしょうか．

文部科学省の施策である「GIGAスクール構想」では，小中学校等における施策の推進にあたって補助金等の手当てがなされているのに対して，「2040年に向けた高等教育のグランドデザイン」において高等教育の高度化の方針が提示されてはいるものの，個々の施策については大学の自主性に委ねられているものが多く，当然ですがこの施策向けの補助金等の手当てはほぼありません．少子化の中で特に私立大学では教育の高度化ツールとしてのみならず，大学の魅力，付加価値のアピールの材料として電子教科書配信プラットフォームを活用しているところもありますが，講義の方針等は各教員に委ねられているところがほとんどで，補助金もない中で大学全体としての動きは一部のものとなっています．

一方，配信プラットフォームサービスを提供している競合他社もありますが，対象サービスの違いやそれぞれの強みと弱みには違いがあり，全国でオープンにサービスを展開しているNTT EDXとは現在のところ緩やかなすみ分けができている状況です．

日本国内には大学が約800，学生が約300万人，教員が約19万人で，あるコンサルティング会社の試算では大学・高等教育機関における教科書関連市場は約500億円となっています．その中でNTT EDXでは，現在約150大学，約16万のアクティブユーザにご利用いただいており，スタートラインに近い市場の中で，まさにパイオニア的な存在です．

◆今後の展望についてお聞かせください．

会社設立1年半でもあり，走り出したばかりの市場で足場を築いていくためにもサービスの安定運用は必須であり，そのうえで電子教科書・教材配信サービスの付加価値をご理解いただきながらお客さまを増やしていくことが重要です．ビジネス的な観点から，まずは30～40%のシェア獲得が1つの目標となります．

大学の教員のミッションが研究と教育であり，教員によりその比重も異なります．一方で，大学における教育の方向性のカギを握るのは教員であり，教育と研究の比重によってもこうしたサービスの受け止め方も異なります．サービスの利用により講義の効率化も期待でき，研究にしても教育にしても忙しい教員にとってこれは大きな付加価値になります．教員とのディスカッションをとおして理解をいただくとともに，新しい付加価値に向けた機能追加等も今後行っていきます．

そして，さまざまな方と連携しながら，この教育の世界で，学生の質の向上や日本がめざしている教育のあり方というところに，いかに貢献できるかといった意識を持って事業を進めていきたいと思っています．

異文化の融合を進めてビジネスを前進

企画部　部長
藤田 英隆　さん

企画部
田中 友基　さん

◆担当されている業務について教えてください.

企画部なので，基本的には経営企画，総務，財務といったコーポレート業務がメインですが，設立間もない少人数の会社でもあるので，サービス企画から営業を担当してくれているNTT西日本・東日本の法人営業部門の方々への支援等ほとんどすべての業務にかかわっています.

メインビジネスが電子教科書・教材配信サービスで，扱い商品が電子メディアではありますが，その商流をはじめ基本的には出版業界のビジネスがベースとなっています．NTTグループ側からみると，出版業界は未知の世界ですが，逆に大日本印刷側からみても同様だと思います．同じことに対してそれぞれの業界で異なる用語を使うこともよくあります．社内の会議においても，それぞれの立場からの意見の相違の調整に苦労する中で，よく確認してみると実質的な相違はほとんどなかった，というようなこともあります.

コーポレート業務においてその違いが如実に表れてくるのが契約です．契約の相手先として出版業界がメインで，逆にお客さまは大学であり，対応していただく教員によってもそのスタイルが千差万別です．当社はその立場上，契約においてはどうしても「従」側の立場になることが多いので，NTTグループが契約相手の場合はともかく，それぞれの業界の商慣習が反映された契約書になってしまいます．つまり，契約書がダブルスタンダード，トリプルスタンダードな状況になっています．また，NTT EDXはNTTグループと大日本印刷の出資により，社員がそれぞれからの出向者で構成されており，その出向形態の相違から総務・人事的な業務でもダブルスタンダードが発生しています.

こうしたダブルスタンダードな状態について抜本的に見直しをかけるには相手方との力関係や少人数でパワー不足のところもあるので時間がかかるとは思いますが，それぞれのいいところ取りや，デファクト的なものを活用しつつ標準化を進めていきたいと思います.

◆今後の展望について教えてください.

とにかくお客さまを増やしていくことで，ビジネスが成立し，社会課題解決への貢献にもつながるので，現段階においてはそれが第一優先です．NTT西日本・東日本の法人営業部門が実際の営業部隊として活動してくれるので，そこへの支援に注力していきます．そのために販売キットやツールの充実はもちろんですが，やっと運用が軌道に乗ってきたホームページをさらにブラッシュアップして，1つのチャネルとしてそこに誘導してもらうような仕組みを構築していきます（**図2**）.

一方で，新ビジネスとして大学教員のオリジナル教科書・教材制作サービスは，著作権マネジメントも行うことで幅が広がり，それをベースとして大学内への「電子教科書・教材配信サービス」の拡大も期待できるので，これに関する検討も進めたいと思います.

こうした活動を行う中で少しずつダブルスタンダードの解消にも取り組みたいと思います.

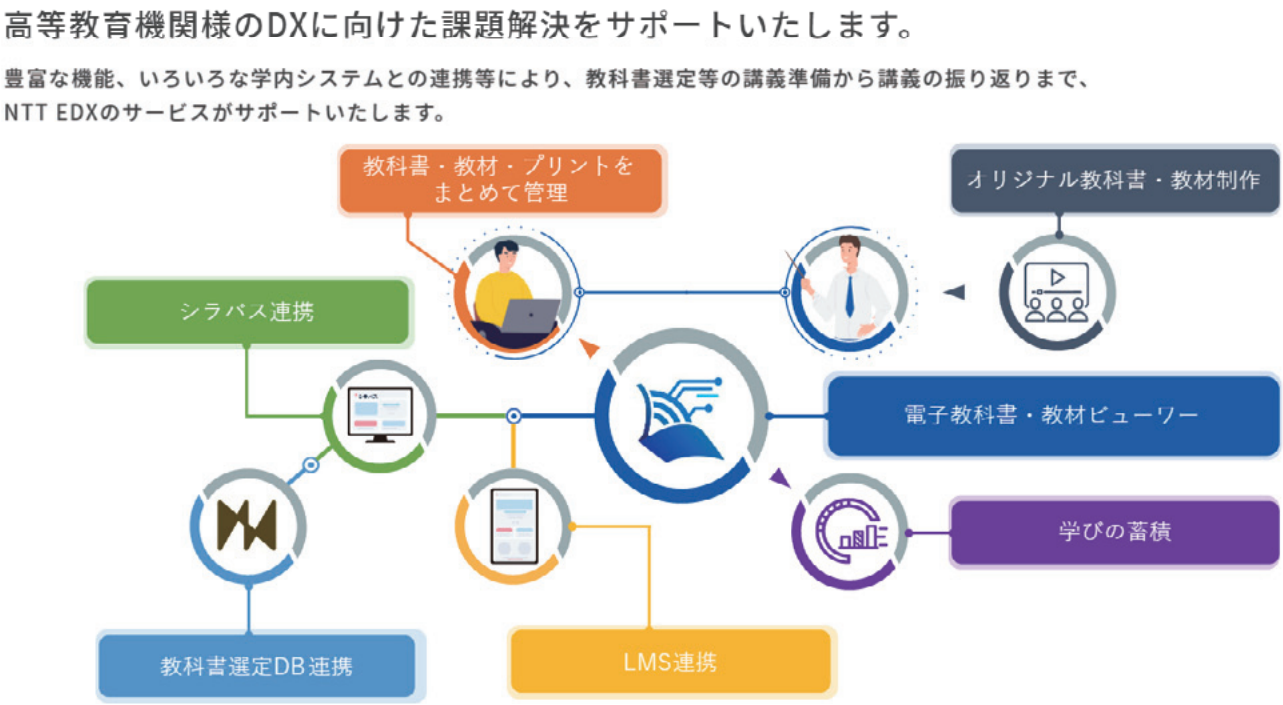


図2　NTT EDXのサービス概要

NTT EDX ア・ラ・カルト

■文化の違い

NTTグループと大日本印刷，異なる業界で仕事の作法どころか，それぞれの文化も異なっているそうです．これまで当たり前だと思っていたことが，そうではなかったことがままあるとのこと．業界用語はもちろんですが，普段何気なく使っている言葉の違いもあるようで，ある会議の中の議論が半分以上分からなかったなどということもあったそうです．言葉は文化そのものですからね．こうした文化のちょっとした違いにも社員の皆さんはいい刺激を受けて，これが会社も個人も今後の発展につながるのではないかと信じてやまないようです．

■第1回目の集合会議・イベントをめざして

少人数の会社ですが，東京と大阪にロケーションが離れていることもあり，さらに会社設立がコロナ禍の真っただ中でリモートワークになっていたこともあり，少人数であるにもかかわらずいまだに全員で顔を合わせたことがないそうです．リモートワークが社会に浸透してきて，NTT EDXもWeb会議等をかなり活用しているとのことですが，会議の取り組み方や働き方については親会社含め三者三様でありWeb会議ではどうも調子が出ないこともあるようです．コロナ禍も落ち着いてきていることもあり，そろそろ全員集合の会議・イベントを始めようかとしているところで，その企画を募集中とか．

オープンイノベーションによる未来共創プログラム『Future-Build』で社会課題解決・未来社会創造に挑戦した6プロジェクトの成果報告

NTT西日本では，オープンイノベーション施設「QUINTBRIDGE」の取り組みとして，2022年8月より未来共創プログラム『Future-Build For Well-being society』を開始し，オープンイノベーションによる社会課題解決や未来社会の創造に取り組んできました．100件を超える応募の中から，採択された10社とともに2023年3月28日に実証実験の成果を発表しました．ここでは，その様子を紹介します．

はじめに

2022年3月に大阪・京橋に開業したオープンイノベーション施設「QUINTBRIDGE（クイントブリッジ）*」は，法人会員が670組織，個人会員が1万人で，毎日200～300名が利用する施設です．10代から80代までの多種多様な会員層とともに「業界・地域課題の解決」と「未来社会の創造」に向けて，さまざまなパートナーと共創による新規事業開発に日々トライしています．

今回紹介する未来共創プログラム『Future-Build For Well-being society』は，NTT西日本とさまざまなプロダクト・アイデアを持つスタートアップが，新規事業検討を短期集中（約6カ月）で実施し，プロジェクトの継続可否を判断するというスピード感あふれる内容です．100件を超える国内外の応募の中から採択された10社とともに，健康，生活，環境，経済の4領域6テーマで「つながりでウェルビーイングを実感できる社会の実現」に向けて検討された成果を，2023年3月28日にQUINTBRIDGEにて報告しました．

未来共創プログラム『Future-Build』成果報告会概要

NTT西日本と採択パートナーが，約6カ月間でアイデア検討，フィールド検証，事業化検討を実施した内容の発表を行いました（**写真1**）．森林正彰NTT西日本代表取締役社長も含めた社内審査員および外部有識者による審査により，①ネクストステージ（事業性検証のフェーズ），②さらなるコンセプトの深掘り・技術再検討が必要なプロジェクト，③検討終了のプロジェクトが発表されました．各プロジェクトの概要を**表**に示します．

審査結果

審査の結果は以下のとおりです．

① ネクストステージ（事業性検証のフェーズ）
- 『ARを活用した「まちの賑わい」の創出』
- 『地球環境に配慮した次世代型農業支援サービス』

② さらなるコンセプトの深掘り・技術再検討が必要なプロジェクト
- 『安価な設備の故障予知診断システムの開発』
- 『自然関連情報視える化サービス』

③ 検討終了のプロジェクト
- 『医療・ヘルスデータ活用による心身のウェルビーイング』
- 『リアルタイムな遠隔操作によるマルチタスクロボッ

写真1　プロジェクト参加メンバー

表　プロジェクトの概要

領域	募集テーマ	採択パートナー	プロジェクト名
健康	医療・ヘルスデータ活用による心身のウェルビーイング	株式会社スポルツ	医療・ヘルスデータ活用による心身のウェルビーイング
		株式会社Enjoydream Holdings	
		Being	
		528株式会社	
生活	“まち”の魅力創出と賑わいをデジタルとリアルとのデータ連携で加速するまちづくり	株式会社ビープリッジ	ARを活用した「まちの賑わい」の創出
経済	ロボットや業務自動化による労働力・人材不足の解消	アダワープジャパン株式会社	リアルタイムな遠隔操作によるマルチタスクロボットオペレーションの実現
		広島商船高等専門学校	安価な設備の故障予知診断システムの開発
環境	海洋資源を活用した炭素吸収・測定ビジネス	株式会社イノカ	自然関連情報視える化サービス
	化学肥料や農薬を抑制したネイチャーポジティブな環境再生型農業	NTTコムウェア	地球環境に配慮した次世代型農業支援サービス
		株式会社エムスクエア・ラボ	

＊「QUINTBRIDGE（クイントブリッジ）」は，NTT西日本が運営するオープンイノベーション施設です．西日本・大阪 京橋から企業・スタートアップ・自治体・大学等のパートナーとともに，「業界・地域課題の解決」と「未来社会の創造」をめざし，つながりでWell-beingを実感できる社会を実現していきます（https://www.quintbridge.jp/）．
本号p.60「挑戦する研究開発者たち」コーナーの「Spectee Pro for elgana」もQUINTBRIDGE発の案件です（https://www.nttbizsol.jp/newsrelease/20230420150000891.html?_ga=2.110555845.1398530464.1682054802-632719628.1681865600）．

写真２　NTT西日本　イノベーション戦略室　事業開発担当シニアマネジャー　藤森　敬基

写真３　プレゼンテーションの様子

写真４　NTT西日本　イノベーション戦略室　事業開発担当シニアマネジャー　駒　寿浩

写真５　プレゼンテーションの模様

トオペレーションの実現』

それでは，ネクストステージに進む２テーマの発表内容を紹介します．

ARを活用した「まちの賑わい」の創出

『ARを活用した「まちの賑わい」の創出』のプロジェクトは採択パートナーである株式会社ビーブリッジとともに発表しました．

NTT西日本本社や京阪モールの壁面など，今まで活用されてこなかった場所にキャラクターやアート，広告のAR（Augmented Reality）を映し出すことで新たな人流を発生させる取り組みを発表しました．

実証実験の結果，物理的な限界があったイベントや広告において新たな提供エリアを広げ，「今後も活用を継続したい」といった声がまちづくり事業者からあがっていました．審査員からは，事業化した先の未来をどうみているのか，どういったところでビジネスとして成立させるのか，AR実用させるというところの「勝ち筋」への質問等が活発に行われました（**写真２，３**）．

地球環境に配慮した次世代型農業支援サービス

『地球環境に配慮した次世代型農業支援サービス』のプロジェクトは採択パートナーであるNTTコムウェア，株式会社エムスクエア・ラボと協力パートナーである株式会社ジャパンバイオファームとともに発表しました．

農業の化学肥料や農薬が与える環境への負荷の改善に向けて，自然にやさしい環境配慮型の農業を広めるための有機農業ついて発表されていました．

実際につくられた有機野菜は，収量良し，きれい（病害虫なし），そして美味しく色艶も問題なしという結果になり，実際に出荷し完売することもできたそうです．また，日本のみならず海外にも展開をしたいという，熱の入ったプレゼンテーションをしていただきました．審査員からは，事業性検証という次のフェーズに進むための検討材料を真剣に伺う質問がなされました（**写真４，５**）．

今後の展開

ネクストステージに進むプロジェクト，再検討を実施するプロジェクトについては事業化に向けた活動を進めていきます．

本プログラム[(1)～(4)]は，初年度の成果や課題を踏まえてバージョンアップして次年度も開催できるように検討していきます．今後の活動にぜひご期待ください．

本イベントに関する結果や外部審査員からのコメント・総評については，参考文献⑸よりご覧ください．

■参考文献

⑴　https://www.quintbridge.jp/program/2022_future-build/
⑵　https://www.ntt-west.co.jp/news/2211/221129a.html
⑶　https://www.ntt-west.co.jp/news/2212/221215a.html
⑷　https://www.ntt-west.co.jp/news/2302/230206a.html
⑸　https://www.ntt-west.co.jp/news/2303/230331a.html

◆問い合わせ先

NTT西日本
イノベーション戦略室
E-mail　innovationstrategy_pr-ml@west.ntt.co.jp