



[小特集]

DX時代に求められる セキュリティ課題と対策

- 世界のセキュリティ法規と求められる管理・技術対策
- 生体認証をめぐる脅威と対策技術の研究動向
- サイバー攻撃の要因である「ぜい弱性」とは？
- ディープフェイク音声の脅威と対策について
- 暗号の安全性評価の重要性

2026年電子情報通信学会総合大会

ジュニア & 学生ポスターセッション 開催のご案内

同級生とは違う、一步先の発表体験

研究発表に挑戦してみませんか？電子情報通信学会では、総合大会において、ジュニア & 学生ポスターセッションを開催いたします。学会初心者の学生でも安心して研究成果を発表でき、自由に意見交換できる場です。詳細はHPからご確認ください。皆さまのご参加をお待ちしております。

日程

一般発表：2026年3月11日（水）

選奨発表：2026年3月12日（木）



開催場所

九州産業大学（福岡市）

1号館1階 エントランスホール

原稿提出締切

2026年 1月6日（火）17：00厳守



対象

小学生から博士前期課程の方

参加費

会 員：無料で発表可能です。

非会員：一般発表は参加費 3,000円（税込3,300円）が必要です。

選奨発表にはご参加いただけません。

一般社団法人
電子情報通信学会

〒105-0011 東京都港区芝公園 3 - 5 - 8

電話番号：03-3433-6691

ieice.org/jpn_r/activities/taikai/general/2026/ps



編集チームリーダー 木下雅之
Masayuki Kinoshita

DX 時代に求められる セキュリティ課題と対策

近年、私たちの社会は急速なデジタル化とともに、サイバー空間におけるリスクと隣り合わせの時代に突入しつつあります。DX（デジタルトランスフォーメーション）が進展し、IoT、AI、生体認証といった技術が社会基盤に深く組み込まれる中、それらを標的とするサイバー攻撃や情報改ざんの手法もまた高度化・多様化しています。セキュリティ対策は一部の専門領域にとどまるものではなく、あらゆる分野における不可欠な基盤となりつつあります。本小特集では、こうした現代的な脅威とそれに対抗するセキュリティ技術・制度について「セキュリティ法規」、「ぜい弱性」、「暗号」、「生体認証」、「ディープフェイク」の視点から多角的に掘り下げ、5件の解説記事を専門家の皆様に執筆頂きました。

初めに、セキュリティ法規の観点から、自動車及びコネクティッド・デジタル製品におけるサイバーセキュリティの法規要件と管理対策について紹介頂きます。次にサイバー攻撃の起点となるぜい弱性について取り上げ、その発生原因や攻撃例、そしてそれらへの対策について解説頂きます。また、私たちの身近で利用されているセキュリティ技術として、暗号化技術と生体認証について焦点を当てます。セキュリティ実現における中核的な技術の一つである暗号については、攻撃手法と安全性評価の重要性について解説頂きます。顔認証や指紋認証といった生体認証は利便性に優れ、PCやスマートフォンのロック解除や本人認証などに利用される一方、そのリスクと対策について御紹介頂きます。更に、AIの発展に伴い、新しい脅威として浮上しているディープフェイク音声に関する最新の研究成果や動向、課題について紹介頂きます。

小特集記事では、セキュリティの基礎的な知識と応用の両面に触れる解説記事をそろえており、初学者にも親しみやすい内容となっています。本小特集が、御覧の皆様のセキュリティ分野への関心を高めるきっかけになりましたら幸いです。

最後に、本小特集の発行にあたり、御執筆頂いた皆様、査読や校閲に御協力頂いた皆様、編集作業に御協力頂いた皆様へ感謝申し上げます。

小特集編集チーム

木下雅之、伊藤敬義、小南大智、中西孝行、松室堯之、村上靖宜



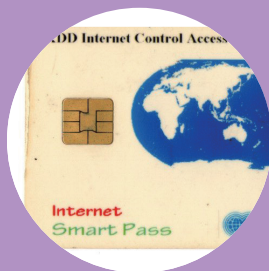
212



254



268



280

【小特集】

DX時代に求められる セキュリティ課題と対策

209

巻頭言

編集チームリーダー
木下雅之

217

— 解説 —

世界のセキュリティ法規と
求められる管理・技術対策
竹森敬祐

224

— 解説 —

生体認証をめぐる脅威と対策技術の研究動向
高田直幸

232

— 解説 —

サイバー攻撃の要因である「ぜい弱性」とは？
—— ぜい弱性がもたらすリスクと
ぜい弱性管理について ——

西村隆廣

239

— 解説 —

ディープフェイク音声の脅威と対策について
鵜木祐史

246

— 解説 —

暗号の安全性評価の重要性
國廣 昇

212	ー子どもに教えたい通信のしくみ：ジュニア会員向けページー 量子コンピュータのしくみとセキュリティへの影響 道後千尋／上村周作
254	ー開発物語ー SoftEther（前編） 登 大遊
262	ーこんなツール、使っていますー オープンソースの仮想マシン管理ツール 光来健一
268	ー街 plus 探訪ー 歴史とにぎわいが混在する街「福岡」 石田俊一
272	ー解説：技術と制度のおはなしー サイバーセキュリティ政策の現在と 通信ネットワークに対する取組みについて 梅城崇師
276	ー若者よ、世界に出よう！ー 私の留学 サンタさんのいる国へ 西尾美哉
280	ー私の研究者歴ー 研究とエンジニアリングの間で 大橋正良
289	ー巻末言ー 英文論文誌へ論文を投稿しよう！ 英文論文誌B編集委員長 長谷川 剛
290	編集後記



量子コンピュータのしくみとセキュリティへの影響

KDDI 総合研究所 道後千尋 Chihiro Dogo 上村周作 Shusaku Uemura

1. まえがき

量子コンピュータは、従来のコンピュータとは異なる原理に基づいて動作する新しい計算機です。近年、量子コンピュータに関する研究や開発が急速に進展しており、その活用に注目が集まっています。しかし、その仕組みや使い道については、まだ多くの人はなじんでいないと思います。

本記事では量子コンピュータの基本的な仕組みと、従来のコンピュータに対する優越性を解説します。また、量子コンピュータの使い道の一つとして、本号の特集であるセキュリティとの関係について解説します。

2. 量子コンピュータとは

皆さんが普段お使いのコンピュータのような従来のコンピュータでは、情報は0か1の値をとる「ビット」の集まりで表現されています。

このビットに対して、「論理積または論理和」、「論理否定の操作（ゲート）」を使って計算を行います。

スパコンを含む、今日の情報社会を形作るほとんど全てのコンピュータは、この仕組みで計算をしています。

1981年、物理学者のリチャード・ファインマンが「自然はニュートンの力学（古典力学）に従うのではなく、量子力学に従っている。その振舞いのシミュレーションをしたいなら、量子力学に基づく方法（計算機）を使った方がよいのではないか」と提唱し、これが量子コンピュータという概念の起源とされています。量子コンピュータは、従来のコンピュータにおけるビット表現や操作を量子力学の性質を利用して拡張した、「量子ビット」や「量子ゲート」から構成されます。

区別するため、量子力学が発見された際にそれ以前の力学が「古典力学」と呼ばれるようになったことに倣い、量子コンピュータ以前のコンピュータ、すなわち現在のコンピュータを「古典コンピュータ」と呼ぶことが

あります。

コンピュータに精通している方々の中には、古典コンピュータも実装では半導体を使っており、それは量子力学の性質を使った材料ではないか、とけげんに思う方もいらっしゃると思いますが、あくまでビットの表現方法（情報処理）に着目した命名であると理解頂いて、この記事内でも古典コンピュータと量子コンピュータと呼び分けます。

3. 量子コンピュータのビット表現

さて、では量子力学の性質を使ったビット表現とはどのようなものなのでしょうか？

本記事では詳しい数学記号の意味や式変形は教科書に譲り、図1の式のみを用いて量子力学と古典力学を対比させながら、量子ビットにつながる要素だけをかいつまんで説明します。

御存じのように、古典力学はニュートンの運動方程式 $ma = F$ を基礎として成り立っています。量子力学でもこれに当たる方程式があり、「シュレーディンガー方程式」と呼ばれています。図1の式1がシュレーディンガー方程式です。古典力学ではニュートンの運動方程式によって状態の時間変化（例、ばね振り子の運動）を記述できたように、量子力学ではシュレーディンガー方程式を使って量子の状態とその時間変化を記述することができます。任意の（一次元の）量子状態は、複素数の波動関数 $\Psi(x, t)$ で表されます。 Ψ は「プサイ」と読み、 x は空間上の位置、 t は時間を意味しています。波動関数 $\Psi(x, t)$ は、シュレーディンガー方程式に従って時間変化します。シュレーディンガー方程式に含まれる H は「ハミルトニアン」と呼ばれ、問題設定によって変わる項です。物理的には、系の全エネルギーを表しています。ここでは簡単に、波動関数 Ψ が量子の状態を表していて、シュレーディンガー方程式はその時間変化を決めていると思ってもらえれば十分です。

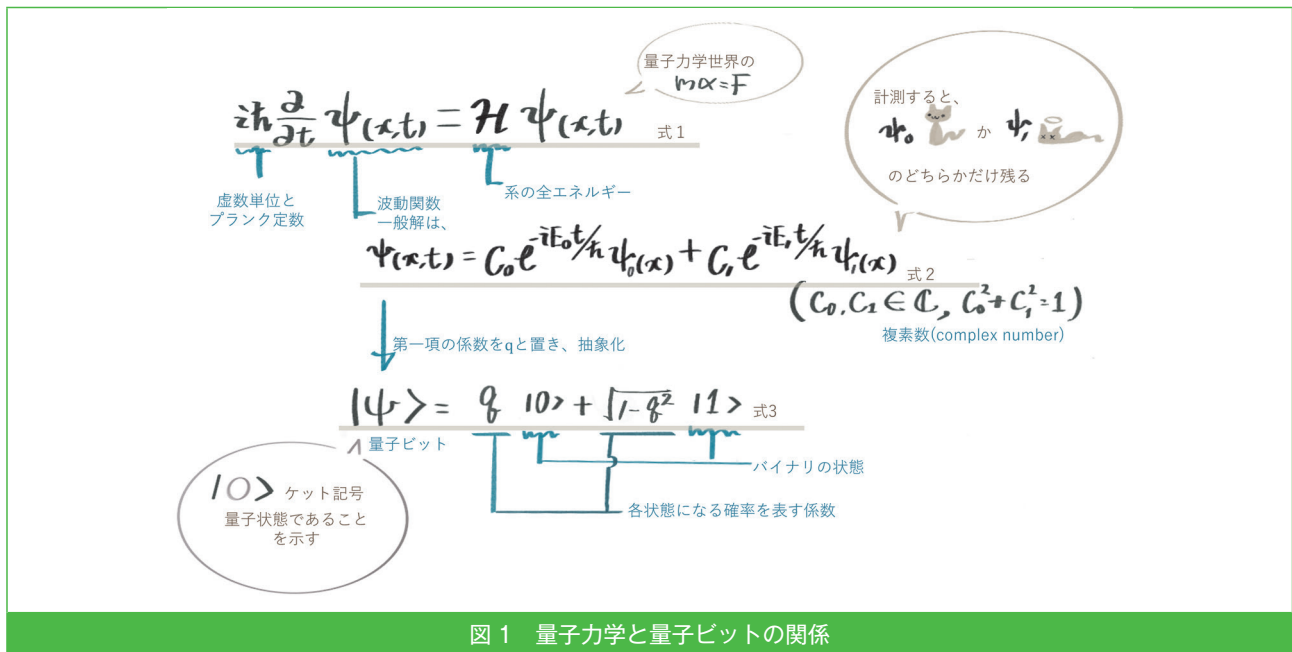


図1 量子力学と量子ビットの関係

量子の特有の性質として、状態の「重ね合わせ」があります。例えば、量子がエネルギー E_0 または E_1 を取る系（2準位）を考えると、シュレーディンガー方程式の一般解 Ψ として図1の式2が得られます。ここで、第一項（第二項）はエネルギーが E_0 (E_1) に確定している「古典的な」状態を表しており、特殊解に相当します。シュレーディンガー方程式は線形なので、その一般解は、特殊解を複素数 C_0, C_1 で重み付けた線形和になります。この量子状態 Ψ は測定（例えば、量子のエネルギー E を読み取る操作）されるまでは、 Ψ_0 と Ψ_1 と断言できないあいまいな状態です。このように二つの状態になる可能性のある状態のことを「重ね合わせ状態」と呼びます。しかし、一たび測定が行われると、 Ψ_0 か Ψ_1 かのいずれかの状態に収束（確定）し、エネルギーも E_0 か E_1 のいずれかになります。いずれに収束するかは、量子状態 Ψ が同じものであっても、測定のために異なり、その確率は係数 C_0 及び C_1 によって定まります。具体的には、 Ψ_0 となる確率は $P_0 = |C_0|^2$ です。観測結果は必ず Ψ_0 か Ψ_1 のどちらかの状態になる必要があるため、確率の合計、すなわち $|C_0|^2 + |C_1|^2$ でなければなりません。「状態を複素数倍して足し算したものも、実現可能な一つの状態である」、「しかし測定すると、どちらか一方にランダムに決まってしまう」ということは大変に不思議ですが、そのようなものも状態の仲間として認めないと、自然現象を説明できないことが実験で証明されています（例：二重スリット実験）。

量子力学では自然現象が波動関数で記述できることを認めてもらえたら、ここからはビットの話に入ります。

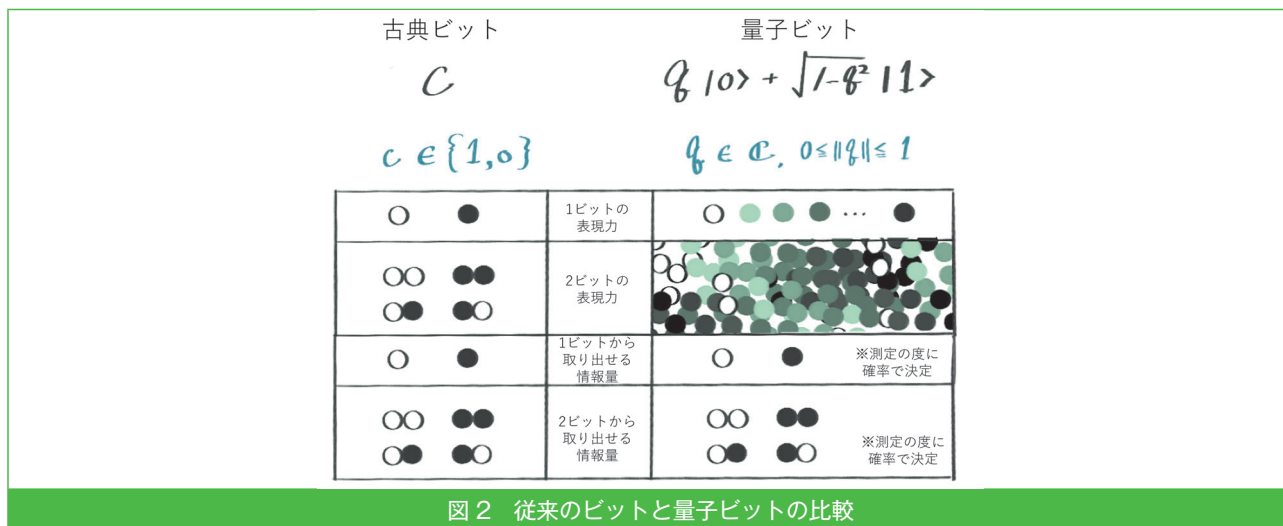
古典コンピュータでは、ビットの0と1は、コンデンサの電圧 V が高いか低いによって表現（実装）され

ています。

量子コンピュータでは、ビットの0と1は、量子の持つエネルギー E が高いか低いかで表現されます。古典コンピュータを実行する際にコンデンサの電圧の具体的な数値を気にしないように、量子コンピュータでも量子状態（波動関数）を抽象的に記載して扱います。高い方のエネルギーを E_1 、低い方のエネルギーを E_0 と書くことにし、対応する量子状態を $|1\rangle$ 、 $|0\rangle$ という記号で書くことにします。0と1をくくっている $| \rangle$ は「ケット」と読み、量子状態であることを示します。 C_0 と C_1 はまとめて複素数 q で表すことにすると、 $|1\rangle$ と $|0\rangle$ を重ね合わせた状態である $|\psi\rangle$ も、一つの量子が取り得る状態の一つです（図1、式3）。この $|\psi\rangle$ が量子コンピュータにおける“1ビット”であり、「量子ビット」と呼ばれるものです。従来のビットと計測される前の量子ビットの表現力の違いを、図2に示しました。重ね合わせの説明のとおり、計測によって読み出せる情報は古典ビットと同じ0か1になります。利点がないようにも思えますが、この点は4.で後述します。

ビットが用意できましたので、これを操作すれば演算が実行でき、コンピュータ（計算機）になります。

量子ビットに対する操作は「量子ゲート」と呼ばれます。量子ゲートの一部を、図3に示しました。例えば、 $|0\rangle$ を $|1\rangle$ に、 $|1\rangle$ を $|0\rangle$ に反転させるXゲート（古典コンピュータの論理否定に相当）というのがあります。また、完全に反転させるのではなく、中途半端に反転する、すなわち重ね合わせの重み q を変化させるRXゲートというのがあります。また、古典コンピュータにおける論理積や論理和のように、二つのビットを入力とするゲート（CNOTゲート）もあります。CNOTゲート



を行うと、以降は二つのビットが互いに影響し合う「量子もつれ状態」が作られます。量子もつれ状態となった二つの量子ビットは、図3の最下段右のように、片方の計測結果によって、もう片方の状態が決まるという興味深い性質を持ちます。このとき片方の量子ビットを操作するだけで、もつれの関係にあるほかの量子ビットに影響を与えることになり、並列計算（のようなもの）が実現できます。

量子コンピュータは、このように、従来の0と1の代わりに重ね合わせが可能な量子ビットを採用し、かつ量子力学特有のゲート操作を追加することで、古典コンピュータよりも多彩な情報の表現・操作を可能にするというアイデアに基づいています。実際に計算する際には、計算に必要なビット数分だけ量子を用意し、それらに計算に応じた適切な操作（ゲート）を加えることで状態を変化させていき、望む計算結果 $|\psi_i\rangle$ を高い確率（すなわち、大きな重み $|\mathbf{q}_i|^2$ で含む量子状態を作り出した上で、測定によって確定させることで計算が完了しま

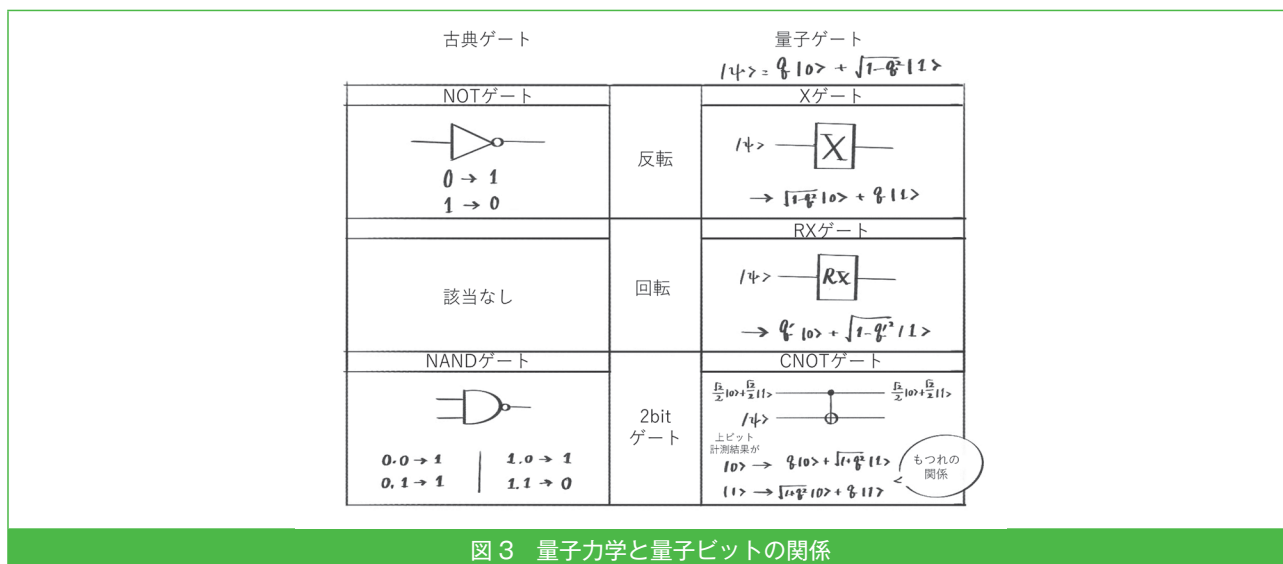
す。したがって、量子コンピュータを実用化するためには、量子を目標状態 $|\psi\rangle$ になるよう操作する技術（ハードウェア）と、量子ビットでの適切な表現及びゲート操作ができるアルゴリズム（ソフトウェア）の両方が必要とされており、現在はそのどちらも研究途上になっています。

4. 量子超越性とは

では古典コンピュータと全く異なる構成の量子コンピュータを開発するモチベーションはどこにあるのでしょうか？ 以下のとおり、量子ビットに特有な量子力学的性質を活用すると、古典コンピュータより有利に、すなわち高速に計算を進めることができます。

・重ね合わせ

従来のビットは0または1のいずれかの状態しか持つことができませんが、量子ビットは $|0\rangle$ と $|1\rangle$ の重ね合わせ状態を取ることができます。この重ね合わせ状態



のビットは、重ね合わせ状態を保ったまま操作することができ、操作後に新たな重ね合わせ状態を得ることができます。すなわち、複数の計算を並列することができます。この並列性が量子コンピュータは計算が速いと言われる理由の一つです。ただし、並列計算したものから、測定により（確率的に）取り出せるのは一つの状態のみです。答えの状態が持つ重み C が十分高くなるように量子状態をゲート操作（“誘導”）する手法は、「量子アルゴリズム」と呼ばれる重要な技術になっています。

・スケーラビリティ

量子ビット 1 個の量子状態は $|0\rangle, |1\rangle$ の重ね合わせで表され、2 個の量子状態は $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ で表されます。一般に N 量子ビットの量子状態は、 2^N 個の状態の重ね合わせとなります。このように、量子ビット数に対して指数関数的に並列計算の能力が向上します。

この性質を活用することで、同じ問題を 0/1 のビットで表現して古典コンピュータで解いたときより、はるかに早い時間で解けるような問題が幾つか見つかっています。古典コンピュータで数百年程度掛かるような問題を、量子コンピュータで実用的な時間内に解が出せる状態を「量子超越性」と呼びます。量子超越性が証明されている、または量子超越性が期待されている問題は、以下のものがあります。

・ランダムな量子回路からのサンプリング問題

Google が 2019 年に量子超越性を証明した問題です。古典コンピュータでは同じ計算を行うためには数千年掛かる計算を、量子コンピュータを使い約 200 秒で結果を得ることができました。この問題自体に実用性はなく、また古典にもより早く解くアルゴリズムがあるという指摘もありますが、この発表は量子コンピュータのマイルストーンとなっています。

・整数の素因数分解

アメリカの数学者ショアが 1994 年に「ショアのアルゴリズム」を提唱しました。これは多項式時間で素因数分解を行うアルゴリズムであり、古典のアルゴリズムの中で最も効率的とされる「数体ふるい法」が準指数時間で動作することに比べ、高速に実行できます。2019 年には IBM によって量子コンピュータ実機で実装され、15 を 3 と 5 に分解するという非常に小さなタスクですが、機能することが実証されています。

・量子力学に基づくシステム（分子の構造や化学反応など）のシミュレーション

量子ビットは量子状態を自然に表現できるため、量子力学に従って推移するシステムのシミュレーションの計算に、その効果が期待されています。これはファイマンの提案したアイデアそのものといえます。

・組合せ最適化問題

組合せ最適化問題は、解の候補が指数関数的に増加するため、古典的なアルゴリズムでは大規模な問題を解決することが困難である、と知られています。量子コンピュータにとっても難問ではありますが、効率的に解を探索する量子アルゴリズムが幾つか提案されています。

上記に挙げたように、現在量子コンピュータで実行できるアルゴリズムはごく限られた問題を高速に解くものです。汎用的な計算を行うコンピュータとして使うにはまだ遠く、現時点では量子コンピュータの長所を生かしつつ、古典コンピュータとハイブリッドで活用する研究が多くなされています。

5. 量子コンピュータとセキュリティ

量子コンピュータは様々な活用が見込まれる一方で、悪用によるセキュリティへの影響も懸念されています。具体的には、現在の暗号技術では量子コンピュータによって解読されてしまう、ということが明らかになっています。暗号は通信を行う際に意図した受信者以外には、送ったメッセージが読まれないようにするための技術のことで、スマートフォンなど多くの通信で用いられています。普段何気なく行っているチャットやインターネット検索が安心して使えるのも、暗号技術によって守られているためです。もし、そうしたプライバシーを守るための暗号が量子コンピュータによって解読されてしまうと、ほとんどの通信が盗み見られてしまう危険性ははらんでいます。個人間の通信はもちろんですが、企業間の通信もその例外ではなく、機密情報が漏えいするなど社会に大きな影響を与えてしまいます。

では実際に、量子コンピュータはどのようにして暗号を解読するのでしょうか？ 解読方法を説明する前に暗号について説明しておくと、「公開鍵暗号」と呼ばれる暗号技術では数学問題に基づいて暗号を構成します。公開鍵暗号方式の中でも広く一般に用いられている「RSA 暗号」と呼ばれる暗号方式では、素因数分解の困難性に基づいて暗号の安全性が担保されています。例えば、 211×491 を筆算などで計算することは大して難しいですが、逆に 103601 を素因数分解するのは難しいと感じるでしょう。RSA 暗号では、この難しさの違いに着目して暗号方式を設計しています。

暗号化を行うための鍵を生成する際には、二つの素数を掛け合わせて鍵を作ります。メッセージを送りたい送信者は、この鍵を用いて暗号化を行ってからメッセージを送ります。暗号化したメッセージを受け取った受信者は、鍵を作るときに用いた素数を使ってメッセージを復号します。したがって、攻撃者が不正にメッセージを解

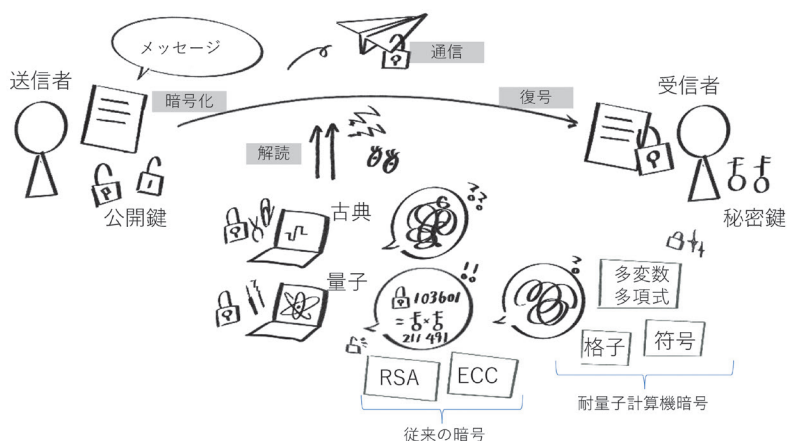


図 4 従来の暗号と耐量子計算機暗号

読しようとしたときには、暗号化するための鍵（二つの素数の積）を素因数分解して、その素数の情報を取得する必要があります。上記の例の 103601 では古典コンピュータですぐに素因数分解できますが、実際に用いられる素数はこれよりはるかに大きな桁数のものを用いるので、古典コンピュータには解読が非常に難しくなります。

前章で説明したように、量子コンピュータがあれば素因数分解を効率的に行うことができるので、量子コンピュータが実用されるようになると、RSA 暗号は安全ではなくなってしまいます。一般的な暗号方式として、RSA 暗号以外に「だ円曲線暗号」という方式もよく用いられていますが、この方式も量子コンピュータによって安全ではなくなることが知られています。

しかし量子コンピュータの登場によって暗号を用いる全ての通信が安全でなくなるか、というとそうではありません。現在、量子コンピュータに対しても耐性がある暗号の研究が進められており、既に実用化されつつあります。

このような暗号は「耐量子計算機暗号」と呼ばれ、これらの暗号を用いることで量子コンピュータが実用化されたとしても、安全に通信を行うことができると考えられています（図 4）。また、耐量子計算機暗号はそれぞれの方式が基づく数学問題に応じて「格子暗号」、「符号暗号」など幾つかの分類があります。例えば、格子暗号は数学における格子という構造をうまく利用した暗号方式の総称で、「LWE 暗号方式」や「NTRU 暗号方式」が知られています。格子は数学的には、所与の複数のベクトルの整数倍の和で表せるベクトル全体の集合のことで、これらの暗号方式は格子の「最短ベクトル問題」を解くことなどで、不正に解読されてしまいます。

最短ベクトル問題とは、文字どおり格子の中で最も短いベクトルを求める問題で、この問題は十分高い次元では答えの候補が極めて多くなるため、非常に難しい問題と考えられています。現在知られている量子アルゴリズムを用いても、この問題を多項式時間で解くことはできません。そのため、格子暗号を用いると量子コンピュータが実用化された時代でも安全にメッセージを送ることができると考えられています。

現在では格子暗号に限らず、多くの耐量子計算機暗号が提案されており、幾つかの手法は標準化もされています。今後、量子コンピュータが実用化されるまでに耐量子計算機暗号が広く用いられるようになることで、量子コンピュータが実用化された時代でも安心して通信を行えるようになることが期待されています。

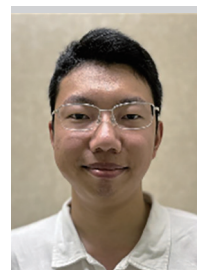
道後千尋

2017 東京理科大学大学院修士課程了。同年 KDDI 株式会社入社。2022 から KDDI 総合研究所で量子アルゴリズムを利用した数値最適化の研究に従事。



上村周作

2022 東大大学院修士課程了。同年 KDDI 株式会社入社。2023 から KDDI 総合研究所で完全準同形暗号の AI 応用や耐量子計算機暗号の研究に従事。



世界のセキュリティ法規と求められる管理・技術対策

竹森敬祐 Keisuke Takemori DNV ビジネス・アシュアランス・ジャパン

1 はじめに

製品ユーザをサイバー攻撃から保護することを目的として、2021年1月に国連欧州経済委員会 (UN/ECE) から自動車のサイバーセキュリティ (CS) 規則として UN Regulation No.155 (UN-R155)⁽¹⁾ が公表され、2022年頃から各国の法規として施行が始まった。2024年4月に英国から消費者向けコネクティッド製品を対象としたCS法規として Product Security and Telecommunications Infrastructure (PSTI)⁽²⁾ が、2024年12月に欧州連合 (EU) の執行機関である欧州委員会からデジタル製品に対してCS要件を課す Cyber Resilience Act (CRA)⁽³⁾ がそれぞれ発効され、各国で施行へと進みつつある。

これらの法規は、自動車、コネクティッド・デジタル製品の製造者が開発フェーズからCSに真摯に取り組み一定のCSレベルを確保すること、自動車やコネクティッド・デジタル製品としてサイバー攻撃への耐性を高めることや、ぜい弱性やインシデントへの迅速な対応を求めている。違反すると、生産・販売の停止や大きな違反金が課される可能性がある。これまで自主努力で進めていた技術的CS対策が、各国において法規化へと移行する中で、自動車、コネクティッド・デジタル製品の製造者にとって、組織の管理策として Cyber Security Management System (CSMS) の構築と技術的CS対策の理解は重要である。

本稿では、UN-R155、PSTI、CRAの三つのCS法規の要件を概観し、自動車やコネクティッド・デジタル製品の製造者が整備すべき管理策と、製品のCSを確保するために必要となる技術的CS対策の一例を紹介する。

以下、2. で三つの法規要件を概観する。3. で組織としてのルール・プロセスを整えて運用するためのCSMSの管理策を整理し、4. でCSリスク分析手法や暗号技術の一例を紹介する。最後に5. でまとめる。

2 法規要件の概説

自動車のCS規則であるUN-R155は、事業者としてCSMSを整備して、サイバー攻撃からの損害を防ぐための管理策と技術的CS対策を考慮した車両の開発・生産・保守を推進する。車両のCS耐性を確保することでサイバー攻撃からの損害を防ぐことができ、道路ユーザの安全やプライバシー保護などを達成する、学びの多い規則となっている。まず初めに、UN-R155の要件を整理する。その後、英国で施行された消費者向けコネクティッド製品のCS対応を求めるPSTIと、欧州委員会から発効されたコネクティッド・デジタル製品に対するCS対応を求めるCRAの要件を整理していく。

なお、誌面の都合上、全ての法規要件を解説できないことに御留意を頂きたい。詳細は、文献(1)～(3)に示した原文を参考にされたい。

2.1 UN-R155の要件

UN-R155の概形を表1に示す。UN-R155は、国連欧州経済委員会 (UN/ECE) の傘下にある自動車基準調

表1 UN-R155の概形

項目	内容
制定主体	国連欧州経済委員会 (UN/ECE) WP.29
公開日	2021年3月4日
施行日	2022年頃から順次、1958年協定加盟国で法規施行 ⁽⁴⁾
目的	車両の開発・生産・保守フェーズのCSMSの構築と車両のCS強化
対象	自動車、車載電子制御システム、これらと相互作用のある車両外コンポーネント
主要要件	Cyber Security Management System (CSMS)、車両CS型式

表2 UN-R155 7.2 節 CSMS 要件の概要

項目	要件の概要
7.2.2.1	開発・生産・生産後フェーズへの CSMS 適用
7.2.2.2	(a)組織としての CSMS の構築, ルールの整備 (b)リスク特定のプロセス (c)リスク評価, 対策導出のプロセス (e)テスト実施のプロセス (f)リスク評価を最新に保つプロセス (g)ぜい弱性や攻撃を監視し対応するプロセス (h)攻撃関連のデータを提供するプロセス
7.2.2.3	迅速にぜい弱性へ対応するプロセス
7.2.2.4	(a)ぜい弱性／サイバー攻撃を監視するプロセス (b)ぜい弱性／サイバー攻撃を分析するプロセス
7.2.2.5	CS に関する責任分担, サプライチェーン管理

和フォーラム (WP.29) 内の自動運転／CS 分科会で議論され、2021 年 3 月に公開された、自動車の型式認定を国際的に調和させるための「1958 年協定」⁽⁴⁾ に加盟する国において、2022 年頃から順次、自動車 CS 法規として施行が始まっている。車両並びに車載電子制御システム、及びそれらと相互作用のある車両外のコンポーネントを対象とした法規である。自動車製造者に課される法規であるが、要件の中に部品サプライヤの管理や技術文書の説明責任を課しており、部品サプライヤへも間接的に適用される。CS 要件としては、組織とルールを整えて、サイバー攻撃に対して車両の耐性を確保する CS 開発と生産を推進すること、及び生産後のぜい弱性・インシデントの監視と対応を推進する CSMS の構築と運用を求めている。また、CS リスク分析に基づく技術的 CS 対策を織り込んだ車両開発と生産を求めている。CSMS に関する要件の概要を表 2 に、CS 技術要件の概要を表 3 に示す。

UN-R155 7.2 節は、車両のライフサイクルとしての開発・生産・生産後フェーズに CSMS の管理策を適用することを求めている。CSMS とは、組織として CS ルールやプロセスを整え、役割と責任を割り当て、運用と監査による改善を推進する管理策である。開発フェーズに対して、リスクの特定・評価、対策の導出、実装した技術的 CS 対策のテストに関するプロセスの整備を求めている。また、生産後フェーズに対して、発覚するぜい弱性や車両へのサイバー攻撃を監視して対応を進めるプロセスや、監視の結果を開発フェーズにフィードバックすることでリスク評価を最新に保つプロセスの整備を求めている。ぜい弱性やサイバー攻撃の監視においては、原因や攻撃経路を分析する能力が求められ、迅速に対応するためのプロセスを整備する必要がある。UN-R155 は、車両製造者に課される規則であるが、その中には部品サプライヤとの CS に関する責任分担を定

表3 UN-R155 7.3 節 CS 技術要件の概要

項目	要件の概要
7.3.1	CSMS 適合証明書の取得
7.3.2	サプライヤ関連のリスクの特定と管理
7.3.3	リスク評価の実施
7.3.4	対策の実装
7.3.5	第三者製品から CS 影響を受けない車両対策
7.3.6	テストの実施
7.3.7	(a) 攻撃の検知と防止 (b) 監視能力のサポート (c) データフォレンジックの確保
7.3.8	コンセンサス規格に準拠した暗号技術の採用

めるサプライチェーン管理の要件があり、サプライチェーンにも間接的に適用される。車両製造者は、CSMS を適切に構築、運用できていることを、各国が定める認定機関、日本の場合は自動車技術総合機構に申請し、CSMS 試験を受審する⁽⁵⁾。合格すると、CSMS 適合証明書を取得できる。

UN-R155 7.3 節は、CS に関する車両等の型式認定⁽⁴⁾を取得するために、取得した CSMS 適合証明書に基づく CS 開発やサイバー攻撃監視を行うことを求めている。CS 開発においては、サプライヤ開発において特定されたリスクを把握し管理する必要がある。車両製造者としても、CS リスク評価に基づく設計を行い、対策の実装とテストが求められている。また、車両製造者の管理が及ばない第三者製品のぜい弱性に起因して、車両が CS 影響を受けない仕組みの実装も必要とされている。生産後フェーズである市場へ提供された車両に対するサイバー攻撃を監視・検知し、必要に応じて対策を図る必要がある^{(6), (7)}。採用する暗号技術は、各国の暗号評価プロジェクトなどが認めたコンセンサス規格に準拠した堅ろう性の高いものを選択しなければならない。こ

表4 PSTI の概形

項目	内容
制定主体	英国
施行日	2024 年 4 月 29 日
目的	コネクティッド製品の CS 強化
対象	消費者向けコネクティッド製品
主な要件	・コネクティッド製品への CS 要件の導入 ・ぜい弱性情報を受け付ける窓口の設置 ・サポート並びにサポート期間の公表

表5 CRAの概形

項目	内容
制定主体	欧州委員会
発効日	2024年12月11日
施行日	2026年9月11日 ぜい弱性の報告
目的	2027年12月11日 CRAの全体
対象	デジタル製品のCS強化
主な要件	・CSリスク分析に基づくCS設計・開発 ・ぜい弱性やインシデントの当局への報告 ・サポート並びにサポート期間の公表

れにより、サイバー攻撃に耐性のある車両が開発・生産され、新たなサイバー攻撃にも迅速に対処できることが期待される。

2.2 PSTIの要件

PSTIの概形を表4に示す。PSTIは、英国において2024年4月から施行された、インターネットに接続可能な消費者向け製品に対する技術的CS対策を要求する法規である。技術的CS対策として、製品ごとに異なるパスワードを設定するか、初回起動時にユーザーに変更させることなどを求めている。また、製品のぜい弱性の発見者から情報を受け取る窓口の設置や、セキュリティ更新プログラムの提供やそのサポート期間を公表することなどを製造者に求めている。UN-R155のようなCSリスク分析に基づく製品開発を明示的には求めておらず、表4に示す主な要件から構成されている。

2.3 CRAの要件

CRAの概形を表5に示す。CRAは、欧州委員会から2024年12月に発効された。欧州域の市場へこれまで提供されてきた（以降、上市と呼ぶ。）コネクティッド・デジタル製品に発覚するぜい弱性について、2026年9月から報告義務が課される。その後、2027年12月からCRAの全ての要件が施行される。対象は、デジタル要素を含むOS、ブラウザ、ネットワーク管理システムなどの製品や、これらを統合した製品である。なお、様々な製品に水平的に適用されるOS、ブラウザ、ネットワーク管理システムなどは、重要なデジタル製品に分類され、OS内の仮想実行環境やファイアウォールなどのCS製品については、重要なデジタル製品クラスIIに分類され、クラスごとに決められた適合性評価を受審する必要がある。CRAの主な要件として、CSリスク分析に基づくCS設計・開発、ぜい弱性やインシデントについて当局への報告、セキュリティ更新プログラ

表6 CRA 付属書 I Part 1 製品 CS 要件

項目	内容
(1)	リスクを踏まえたCS設計・開発・生産
(2)	(a)既知の悪用可能なぜい弱性がない状態での上市 (b)CSが確保された状態での上市 (c)ぜい弱性対応としてのソフトウェア（SW）更新の保証 (d)不正アクセスからの保護 (e)データに関する機密性の担保 (f)データに関する完全性の担保 (g)取り扱うデータの最小化 (h)DoS攻撃からの回復力、可用性の確保 (i)ほかの製品やネットワークへの悪影響の最小化 (j)攻撃対象領域を制限する設計・開発・生産 (k)損害の影響を低減する設計・開発・生産 (l)ログの記録と監視、オプトアウト機会の提供 (m)データや設定の削除機能の提供

表7 CRA 付属書 I Part 2 ぜい弱性対応の要件

項目	内容
(1)	ソフトウェア部品表（SBOM）の整備、ぜい弱性及びソフトウェアコンポーネントの特定
(2)	迅速なセキュリティ更新プログラムの提供
(3)	定期的なCSテストとレビューの実施
(4)	修正されるぜい弱性に関する情報の開示
(5)	ぜい弱性情報の開示に関する方針の策定と実施
(6)	ぜい弱性の報告を受け付ける窓口の公表
(7)	CSを確保した更新と自動的なSW更新の仕組み
(8)	更新プログラムの迅速かつ無料での提供

ムの提供やサポート期間の公表などがある。要件の詳細を、表6、7にまとめる。

CRAでは付属書I Part1に、製品に対するCS要件が列挙されている。CSリスク分析に基づくCS設計・開発・生産を行うこととされており、分析の結果から項目(2)の(a)～(m)の要件に対応する必要がある。例えば、(e)個人やその他のデータを保管、送信、処理において漏えいさせない機密性の担保、(f)個人やその他のデータ、コマンド、プログラムを勝手な操作や変更から保護する完全性の担保、(l)データや処理をログとして記録して活動を監視する機能と、監視や他者へのログ提供をユーザーが拒否するオプトアウトの機会の提供などを求めている。

CRAの付属書I Part2には、ぜい弱性対応の要件として表7の項目(1)から(8)が列挙されている。例えば、(1)ではソフトウェア部品表（SBOM: Software Bill of Materials）を整備して、ぜい弱性が含まれる製品やコンポーネントの特定や依存関係を把握できるようにすること、項目(5)では「Vulnerability Disclosure

表8 積極的に悪用されているぜい弱性の報告

期限	提出物	内容
24 時間以内	早期警告通知	・製品が利用されている国
72 時間以内	ぜい弱性通知	・製品に関する一般的な情報 ・エクスプロイト及びぜい弱性の一般的な性質 ・講じられた対策やユーザが講じることのできる対策に関する一般的な情報
対策が利用可能になった後 14 日以内	最終報告書	・深刻度を含むぜい弱性の説明 ・可能な場合、悪用者に関する情報 ・セキュリティ更新プログラムまたはほかの是正措置の詳細

表9 CS に影響を及ぼす重大なインシデントの報告

期限	提出物	内容
24 時間以内	早期警告通知	・製品が利用されている国
72 時間以内	インシデント通知	・インシデントの一般的な情報、性質、初期評価の結果 ・講じられた対策やユーザが講じることのできる対策に関する一般的な情報
インシデント通知の提出後 1 カ月以内	最終報告書	・深刻度を含むインシデントの説明 ・脅威または根本原因 ・適用された／継続中の対策

Policy (VDP)」と呼ばれるぜい弱性情報の開示に関する方針を策定して運用することなどを求めている。

ここで、CRA の第 14 条には製造者の報告義務として、製造者は自ら認識した積極的に悪用されているぜい弱性、若しくは CS に影響を及ぼす重大なインシデントについて、迅速に当局へ報告しなければならないとされている。報告期限や内容について、表 8、9 にまとめる。

報告は、早期警告通知、ぜい弱性／インシデント通知、最終報告の 3 回となっている。早期警告通知は、自らぜい弱性を認識してから 24 時間以内とされており、製品を上市した国を事前に整理しておく必要がある。また、ぜい弱性／インシデント通知は、ぜい弱性／インシデントに関する性質やユーザが講じることのできる対策に関する情報を含む必要があり、72 時間以内に報告するには、ぜい弱性／インシデントの分析能力を適切に持つ必要がある。最終報告書には、根本原因や対策に関する情報が求められ、ここでも適切な分析能力を持つ必要がある。なお、報告に関する第 14 条は、2026 年 9 月 11 日から施行され、これまで欧州域へ上市して利用されている全てのデジタル製品が対象となる。

3 CSMS の構築の一例

UN-R155 では、組織として CS 対応を適切に推進するための CSMS の構築を求めている。これは、組織として体制とルールを整備し、誰が実施しても同様の結果を得られる業務フローを作成・運用し、監査によって継続的な改善を推進することである。

3.1 体制とルールの整備

図 1 に CSMS 構築のための体制とルール整備の一例を示す。人員、IT システム、文書などの情報セキュリティ管理は、Information Security Management System (ISMS) で推進し、これを組織運営の土台とする。この上に、製品の CS を実現するための CSMS を乗せるとよい。

製品・情報セキュリティに関する最高責任者は、製品・情報セキュリティ委員会を運営し、目的や方向性を示す最上位文書として基本方針を掲げ、これを実現するために何をどの程度達成するかを示す対策基準を策定

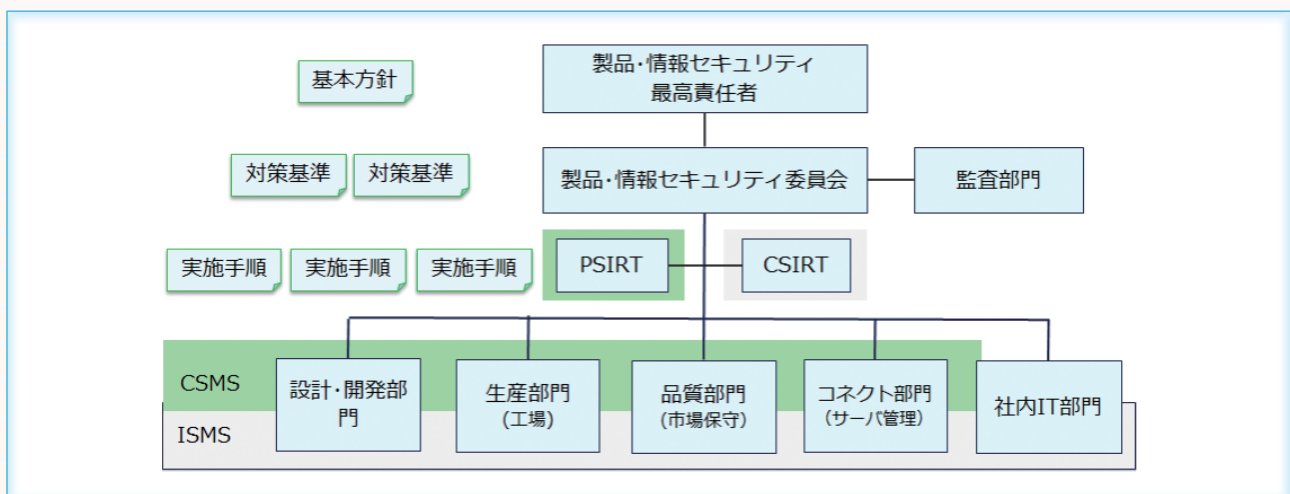


図1 体制とルールの整備の一例

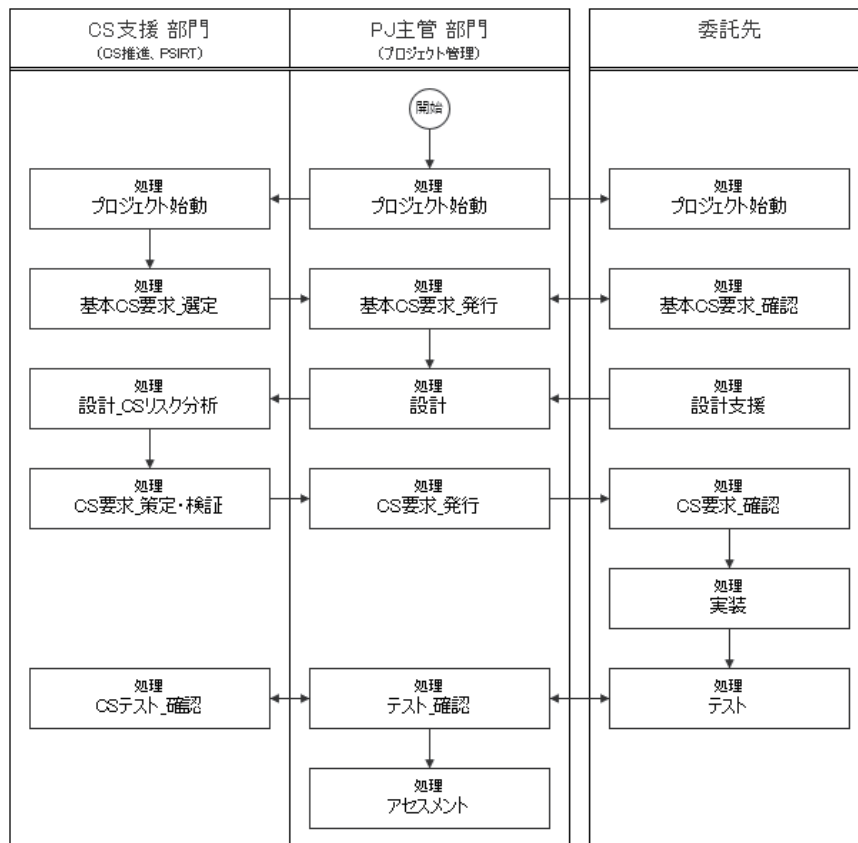


図2 業務フローの一例

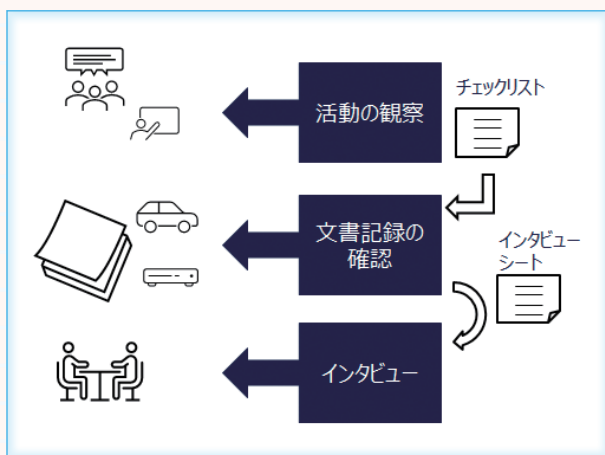


図3 監査活動の一例

し、周知する。CSMSの対象となる部門は、基本方針と対策基準を受けて、現場での対応を具体的な手順としてまとめた実施手順を策定し、その教育を推進する。また、製品に発覚するぜい弱性やインシデントへの対応として Product Security Incident Response Team (PSIRT) を設置して、組織間連携による迅速な対応を推進する。

3.2 業務フローの整備

図2に、実施手順の一つである製品のCS開発を進めるための業務フローの一例を示す。製品CS開発のプロ

ジェクトを主管する部門と、そこを支援する部門、委託先など連携先を明確にする。これにより、関係者の役割と業務の流れが分かるようになる。また、各業務の実施手順には、入力→処理→出力を定義するとよい。

3.3 監査による改善

図3に、CSMSに関わるルールの確認や運用を確認する監査活動の一例を示す。CSMSの機能の一つとしてルールが策定され適切に運用されていることを確認する監査部門を設けることもある。監査は、各部門の活動や、活動が記録された文書を確認する。また、各部門の担当者へのインタビューを通じて、CSMSが適切に運用されていることを確認する。結果は、適合、改善の機会、軽微な不適合、重大な不適合に分類して、改善活動を推進する。

4 技術的CS対策の一例

ここでは、製品CS開発において求められるCSリスク分析の流れ、CS開発活動が適切であることを確認する検証・テスト・アセスメント、そして技術的CS対策の基本となる暗号技術の一例を紹介する。

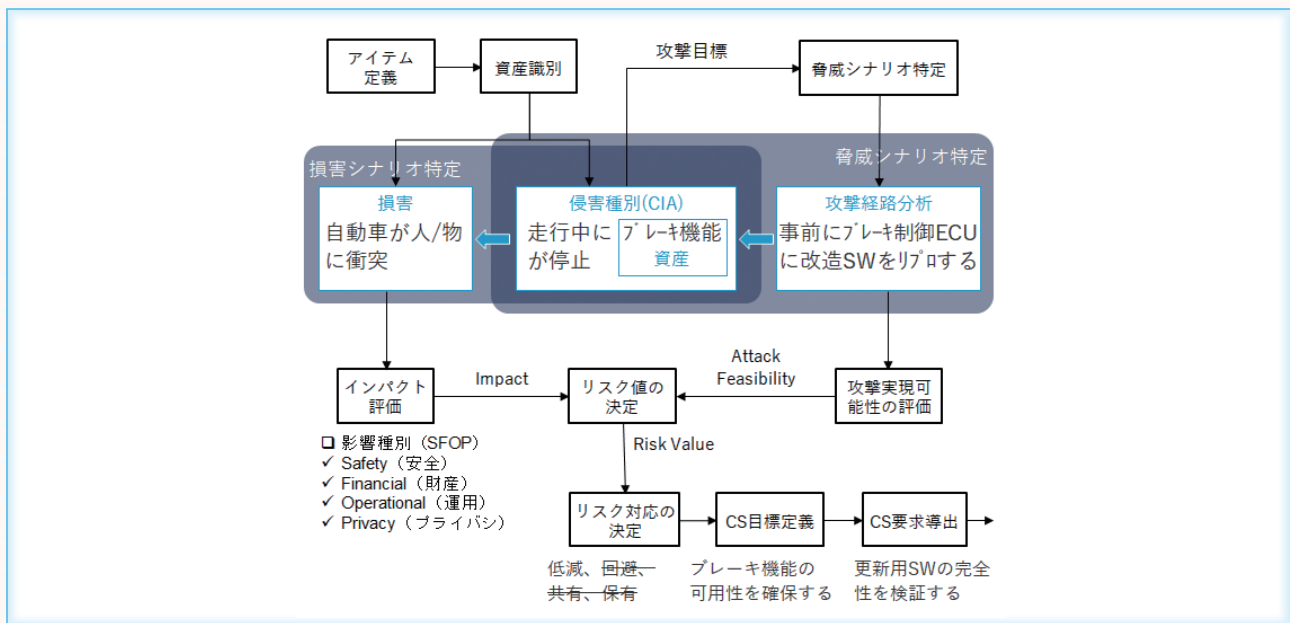


図4 CSリスク分析の流れ

4.1 CSリスク分析の手法

図4に、CSリスク分析の流れを示す。分析は、資産識別→損害シナリオ特定→インパクト評価→脅威シナリオ特定→攻撃経路分析→攻撃実現可能性評価→リスク値の決定→リスク対応の決定へと進む。リスク値を参考に対応として、低減：技術的CS対策などを図る、回避：リスクを含む機能を取り除くなど、共有：開発プロジェクトを保険に加入させるなど他者と共有する、保有：リスクが小さい場合、今は対応しないと判断するなどがある。

対応として低減を選択した場合は、CS目標定義→CS要求導出へと進む。図4では、ブレーキ機能の可用性を確保することをCS目標として、これを達成するためのCS要求として、更新用SWの完全性を検証することを導出している。その後も、システム設計を考慮した詳細なCSリスク分析を繰り返す段階的の詳細化を進めることで、製品の全体的な技術的CS対策から、ハードウェア／ソフトウェアの細部まで技術的CS対策を適切に施すことができる。

脅威シナリオ特定には幾つかの手法があるが、Microsoftが提唱する脅威のモデル化“STRIDE”⁽⁸⁾がよく知られている。資産識別、損害シナリオ特定、攻撃経路分析なども、様々な手法があるため、製品の特性に合わせた適切な手法を実施手順として整備しておくといよい。インパクト評価と攻撃実現可能性評価からリスク値を決定する指標には、CVSS v3⁽⁹⁾がある。こうした指標に基づき、リスク対応として、何らかの対策を図る“低減”，リスクを含む機能を排除するなどの“回避”，CS開発プロジェクトを保険に加入させるなど他者との“共有”，リスク値が極めて低いと判断して“保有”するなど、決定していく。低減と決定されると、攻撃実現可能性を低減させる対策としてのCS要求を導出する。

4.2 検証・テスト・アセスメント

開発プロジェクトの計画や、CSリスク分析の流れが適切に行われたことをチェックリストなどを用いて検証することで、設計レベルでのぜい弱性の混入を防ぐことができる。検証で用いるチェックリストの例を図5に

【チェックリスト】				
No.	対象	チェック項目	判定結果	判定理由
1	具体的な攻撃方法の列挙	脅威シナリオを実現する具体的な攻撃方法が攻撃経路として記されている。		
2		脅威シナリオごとに、考えられる攻撃経路が列挙されている。(一つの脅威シナリオに対して、複数の攻撃経路があり得る。)		
3		脅威シナリオと攻撃経路に矛盾はない。		

図5 検証で用いるチェックリストの一例

示しておく。製品の特性に合わせて、チェック項目を導出しておくといよい。設計後は、実装へと進み、CS 要求に基づく機能が仕様どおりに動作していることをテストを通じて確認する。最後に、一連の活動記録を第三者的な視点でレビューすることで、妥当性を判断するアセスメントを行うといよい。

4.3 暗号技術

情報セキュリティにおける機密性、完全性、可用性を確保するためには暗号技術の適用が一般的である。例えば、情報の機密性を担保するための暗号化や、完全性を確認するための署名・検証などがあり、これらを組み合わせてシステムの可用性を確保する。暗号技術には、十分な強度を有するアルゴリズムや「鍵長」を適用する必要がある。これら暗号アルゴリズムや鍵長については、CRYPTREC⁽⁶⁾やNIST SP-800⁽⁷⁾などで評価されており、参考にするといよい。

5 まとめ

本稿では、世界的に法規化が進む自動車やコネクティッド・デジタル製品を対象としたCS法規の要件を整理し、これを満たすための管理策や技術的CS対策の一例を概観した。自主的なCS開発・生産・保守を進めていた時代は終わり、自動車やコネクティッド・デジタル製品の製造者としてCS要件への対応が必須となってきている。CS法規に違反すると製品の生産や販売の停止や、大きな制裁金を課されることになるため、各種CS法規要件の把握と、CSMSの構築、技術的CS対策の理解に努める必要がある。

■ 文献

- (1) 国連欧州経済委員会自動車基準調和世界フォーラム (WP.29), “UN-R155.” <https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security>
- (2) 欧州委員会, “Cyber Resilience Act (CRA) .” <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847>
- (3) 英国, “Product Security and Telecommunications Infrastructure Act (PSTI) .” <https://www.legislation.gov.uk/ukpga/2022/46/part/1/enacted>
- (4) 国土交通省, “国連の車両等の型式認定相互承認協定 (1958 年協定) の概要.” <https://www.mlit.go.jp/common/000055228.pdf>
- (5) 自動車技術総合機構, “CSMS 試験.” <https://www.naltec.go.jp/publication/regulation/gtg5d20000000fht-att/ih31n00000008r8.pdf>
- (6) CRYPTREC, “電子政府推奨暗号の評価・監視.” <https://www.cryptrec.go.jp/>
- (7) NIST Computer security resource center, “SP 800 guidance.” <https://csrc.nist.gov/publications/sp800>
- (8) Microsoft, “脅威のモデル化 STRIDE.” <https://learn.microsoft.com/ja-jp/azure/security/develop/threat-modeling-tool-threats>
- (9) 情報処理推進機構, “共通脆弱性評価システム CVSS v3概説.” <https://www.ipa.go.jp/security/vuln/scap/cvssv3.html>

竹森敬祐

DNV ビジネス・アシュアランス・ジャパン株式会社。これまでインターネットセキュリティ、スマートフォンのセキュリティ&プライバシー、自動車セキュリティ、デジタル製品セキュリティに関する研究・開発や制度設計などに関わる。



生体認証をめぐる脅威と対策技術の研究動向

高田直幸 Naoyuki Takada セコム IS 研究所

1 はじめに

生体認証技術は「バイオメトリクス」とも呼ばれ、今日の私たちの生活に不可欠なものとなっている。PC やスマートフォンのロック解除やサインイン、公的サービスにおける本人確認、施設へのアクセスコントロールなど、様々な生活シーンで、顔認証や指紋認証、静脈認証といった生体認証技術が活用されている。利用者の「生体情報」を利用する生体認証技術は、従来のパスワードや暗証番号などの「記憶」に基づく認証や、IC カードなどの物理的なデバイスの「所持」に基づく認証に比べて、忘却や紛失のリスクが低く、利便性にも優れるとされ、広範な分野で実用化が進んでいる。

一方で、生体情報には変更が困難であるという本質的な性質があり、その漏えいや偽造、不正利用が深刻なセキュリティリスクを招く。このため、偽造生体情報への対策や、システム内に保持される生体情報の保護は、生体認証システムを安全かつ高い信頼性で運用するための最重要課題の一つとなる。更に近年、個人情報保護法や欧州一般データ保護規則（GDPR）、欧州 AI 法などの法整備が進み、生体情報及び生体認証技術の利活用においては、倫理的な妥当性やプライバシーへの配慮も不可欠となっている。

本稿では、生体認証技術／システムの基礎を説明した上で、生体認証をめぐる脅威と対策技術の研究を紹介する。特に、偽造生体情報による攻撃と「プレゼンテーションアタック検知」と呼ばれる対策技術、セキュリティのみならずプライバシーへの配慮において重要な技術となるテンプレート保護技術に焦点を当てる。

2 生体認証技術の基礎

生体認証は、人体の生物学的特徴に基づき、個人を識別・認証する技術である。この生体認証に用いられる生

物的特徴を「モダリティ」と呼ぶ。

2.1 生体認証のモダリティ

表 1 に代表的なモダリティを示す。生体認証のモダリティは、身体的特徴と行動的特徴に大別される。身体的特徴は人体の構造的な特徴に基づく「静的な」モダリティであるのに対し、行動的特徴は、個人特有の行動パターンや振る舞いによる「動的な」モダリティである。行動的特徴には環境や心理状態、身体の状態による影響が表れやすく、一般には身体的特徴の方が安定的で、高い識別精度を示す。その一方で、継続的に変化する行動的特徴の方が、生体情報の偽造や「なりすまし」への耐性が高いとされる。

複数のモダリティを組み合わせる認証方式も存在し、「マルチモーダル認証」と呼ばれる。マルチモーダル認証には、異なるモダリティの生体認証を順次実行する方式と、指紋と指静脈、掌紋と手のひら静脈といった、同時に取得可能な複数のモダリティを組み合わせる方式がある。このほか、高い精度を示す身体的特徴と、高い「なりすまし耐性」を示す行動的特徴を補完的に組み合わせるという考え方もある。

2.2 生体認証システムの構成

一般的な生体認証システムの構成を図 1 に示す。生体認証システムの多くは、「生体センサ」「特徴抽出部」「テンプレートデータベース」「照合部」から構成される。システムの動作は、ある人物の生体情報をシステムに「登録」するフェーズと、ある人物が生体情報を登録済みの人物であることを「認証」するフェーズに分けられる。

生体センサは、人物から生体情報を取得する役割を果たし、モダリティに合わせたセンサが利用される。例えば、指紋認証であれば、光学式、静電容量式、超音波式等の各種の指紋センサ、顔認証であれば、可視光カメラ

表 1 代表的な生体認証モダリティ

分類	モダリティ	解説	精度*
身体的特徴	指紋認証	手の指先の皮膚の凹凸パターン（隆線、汗腺など）を解析。手荒れや乾燥に影響を受けやすい	高
	顔認証	顔の画像特徴や目、鼻等の器官特徴を解析。照明や表情、年齢変化に影響を受けやすい	中～高
	虹彩認証	眼球の虹彩パターンを解析	高
	静脈認証（手のひら・手指）	手のひらや手指の血管パターンを近赤外線を読み取って解析。体表に露出せず偽造耐性がある	高
	耳介形状認証	耳の形状を解析。実用化事例は少ない	中
	DNA 認証	遺伝子情報を基に識別。精度は極めて高いが一卵性双生児は区別できない。即時認証には不向き	高
行動的特徴	筆跡認証（署名認証）	書字動作の軌跡や筆圧、速度などを解析	中
	キーストローク認証	キーボード入力のタイミング・強さなどを解析	低～中
	歩容認証（歩き方）	歩行時の動きや体重移動パターンを解析。遠隔からの認証用途に親和性が高い	中
	音声認証（行動的側面）	声のスペクトルや発話内容の癖（イントネーション、リズム）を解析	中
	タッチ動作認証	スマートフォンなどの操作パターン（スワイプ、タップ等）を解析	低～中

* 特定の製品／技術の精度ではなく一般的な傾向として記載。

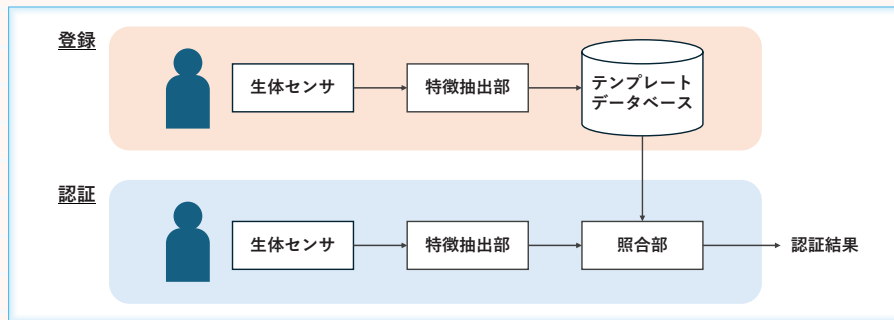


図 1 生体認証システムの構成

や、スマートフォンや PC にも搭載されている Depth カメラなど、多様なセンサが存在する。従来、生体情報の取得には、センサと生体を接触または近接させる必要があったが、近年のセンシング技術や、取得した生体情報からの特徴抽出処理の進化により、非接触や遠隔から取得できるモダリティが増えている。

特徴抽出部では、生体センサで取得した生体情報から個人の識別に用いる特徴が抽出され、システムが扱いやすい「特徴量」に変換される。登録フェーズで抽出された特徴量は、事後の認証フェーズで参照できるようデータベースに格納され、「テンプレート」と呼ばれる。特徴量の形式は、一般に、モダリティや認証アルゴリズムによって異なるが、指紋認証におけるマニューシャ特徴や、John G. Daugman 教授が特許化し、虹彩認証で利用されるアイリスコード等、広く認知されている形式も存在する。このほか、深層学習をはじめとする機械学習を活用して特徴量を算出する方式も、数多く研究されて

いる。

照合のプロセスでは、利用者の生体情報から算出した特徴量と、データベースに格納された登録人物のテンプレートとの類似度が算出される。類似度が所定の照合しきい値を超えた場合、認証対象者は登録人物と同一人物であると判定される。特徴量間の類似度の算出には、認証アルゴリズム独自の手法やコサイン類似度などが用いられる。

3

生体認証システムに対する脅威と攻撃手法

生体認証技術は、認証に個人特有の生体情報を用いるため、安全で便利であると考えられがちであるが、セキュリティの観点からは、生体認証特有の二つの大きな「ぜい弱性」がある。第 1 に、生体情報の一部は体表に露見しており、容易に詐取される。顔画像は誰でもカメラで撮影することができる。人が素手で物に触れれば、

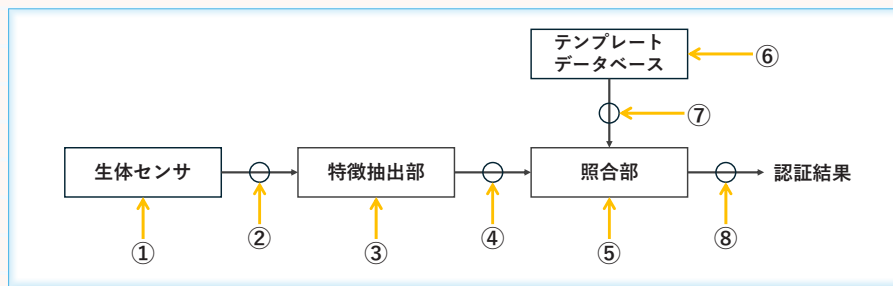


図2 生体認証システムの構成と攻撃のポイント

そこに指紋が残る。更に、センシング技術の発展により、非接触で取得できる生体情報も増えている。第2に、パスワードやICカード等の所持や記憶による認証手段とは異なり、生体情報は本質的に変更が困難である。例えば、個人の指紋画像が漏えいしたとしても、指紋の変更は容易ではない。これらのぜい弱性は、プレゼンテーションアタック (Presentation Attack) と呼ばれる偽造生体情報による攻撃につながる。

プレゼンテーションアタック以外にも、生体認証システムのぜい弱性を突いた攻撃が存在する。Rathaらは、生体認証システムにおける八つの攻撃ポイントを示した⁽¹⁾ (図2)。これらのポイントへの攻撃は、次の四つに分類される⁽²⁾。

(A) ユーザインタフェースへの攻撃

(B) 特徴抽出部、照合部などのモジュールへの攻撃

(C) モジュール間の通信路への攻撃

(D) テンプレートデータベースへの攻撃

代表的な攻撃と攻撃のポイントを上記の分類で整理したものを表2に示す⁽³⁾。本稿では、生体認証システム特有の攻撃として、ユーザインタフェースへの攻撃であるプレゼンテーションアタックと、テンプレートデータベースへの攻撃を取り上げ、対策を交えて詳説する。モジュールや通信路への攻撃は、一般的なITシステムと同様に、セキュアなソフトウェア実行環境 (TEE: Trusted Execution Environment) やコードサイニングの導入、通信路の暗号化やタイムスタンプ、チャレンジレスポンス方式の導入といった対策が有効に作用するため、本稿での対策の詳説は割愛する。

表2 生体認証システムへの代表的な攻撃 (文献(3)の表を一部改変)

番号	攻撃の種別	攻撃ポイント
1	プレゼンテーションアタック: 偽造生体情報の提示 (スプーフィング)	①
2	一卵性双生児や血縁者等の類似性の利用 (顔など)	①
3	正規ユーザから攻撃者への生体情報サンプルの提供 (正規ユーザと攻撃者との共謀)	①
4	ゼロ・エフォート試行: 攻撃者が正規ユーザになりすまして自身の生体情報を提示, 登録詐称	①
5	センサ上に残された残留生体情報の不正取得	①
6	センサや操作パネルの不正操作, 物理的な破壊	①
7	通信路を流れる正規ユーザの生体情報や特徴情報の傍受, 傍受した情報によるリプレイ攻撃	②, ④
8	生体情報/特徴量/テンプレートの継続的な改ざんによるヒル・クライミングアタック	②, ④, ⑦
9	マルウェアによる攻撃, トロイの木馬の注入	③, ⑤
10	多くのテンプレートと一致する偽造生体情報の推定, 提示 (ウルフ攻撃)	③, ⑤ (①, ②)
11	テンプレート情報の不正入手	⑥
12	テンプレートの改ざん, 攻撃者のテンプレートへの置換え	⑥
13	通信路からのテンプレート傍受, 傍受したテンプレートによるリプレイ攻撃	⑦
14	攻撃者のテンプレート注入	⑦
15	通信される認証結果の改ざん: 正規ユーザのアクセス拒否, 攻撃者のアクセス許可	⑧
16	サービス拒否攻撃: 通信路の切断/情報の改ざん/継続的なサンプル注入	②, ④, ⑦, ⑧

表3 主なプレゼンテーションアタック手法とその対策技術 (PAD)^{(5)~(10)}

モダリティ	攻撃手法
指紋	・ゼラチン、シリコン、ラテックス、木工用ボンド、粘土等による人工指紋の作成 ・3D プリンタでの指紋型の作成 ・他人の切断指や死者の指の利用
顔	・写真や動画の提示 ・顔写真を部分的にくり抜いて、お面として被って提示 ・シリコンや樹脂等による 3D マスクの作成、提示 ・ディープフェイク技術による顔画像や動画の作成、提示 ・一卵性双生児等によるなりすまし
虹彩	・虹彩画像の提示（赤外撮影に対応したプリンタでの印刷、モニタへの表示） ・虹彩画像の上にコンタクトレンズを載せて提示（眼球の湾曲再現） ・虹彩模様を印刷したカラーコンタクトレンズを装着して提示
静脈	・蠟（ろう）やシリコン樹脂、大根などの野菜による人工物の作成 ・赤外インクで静脈パターンを紙に印刷して提示
音声	・声真似：声色や話し方の真似 ・録音音声の再生 ・音声変換：正規ユーザの音声特徴を学習し、攻撃者の声質を変換して再生 ・音声合成：正規ユーザの音声特徴を学習し、任意テキストを合成して読み上げ

3.1 プレゼンテーションアタック

プレゼンテーションアタックは「なりすまし攻撃」とも呼ばれ、生体センサに対し偽造した人工物や映像等の情報を提示して、生体認証システムの誤動作を誘発する攻撃である。古くは、顔認証システムへの顔写真の提示など、単純なアプローチが主流であったが、松本らが、食品用のゼラチンを使用して偽造指紋を作成して攻撃を成功させて以降、プレゼンテーションアタックへの注目が高まった⁽⁴⁾。

2016年には、ISO/IEC30107 シリーズとして、プレゼンテーションアタック検知 (PAD: Presentation Attack Detection) の基本フレームワークや評価方法が国際標準化されている。近年では、生体認証技術やデバイスの PAD 性能の評価を、第三者となる品質保証機関に依頼し、国際標準で規定されたテスト手法・報告方法に従った評価として公表するケースもある。

表3に、指紋、顔、虹彩、静脈、音声のモダリティ別に、主なプレゼンテーションアタック手法とその対策技術 (PAD) を示す^{(5)~(10)}。ここに示した攻撃手法は、シリコン樹脂や印刷物などを使用して物理的な偽造生体を作成し、センサに提示するアプローチと、写真や映像などの偽造情報を生成して提示するアプローチに大別される。前者は3Dプリンティング等の成形技術の進化によって、後者はディープフェイク⁽⁷⁾をはじめとする生成AI研究の進化によって高度化しており、偽造生体情報のクオリティは日増しに高まっている。

対策技術となるPAD手法については、主にハードウェアによるものと、ソフトウェアによるものに大別される (表4)。ハードウェアによる手法の多くは、生体

の物理的な形質を直接計測することで生体検知を実現する。生成AIによる偽造情報生成攻撃に対しても効果的に作用すると期待できるが、専用のハードウェアを必要とし、適用できる場面が限定される。このため汎用的な技術として、ソフトウェアベースのPAD研究も盛んとなっている。

3.2 テンプレートデータベースへの攻撃

本攻撃は、大きくは攻撃者テンプレートの不正注入と、テンプレートの不正取得に分けられる。前者は攻撃者の生体情報による不正アクセスを企図したものである。後者の攻撃でテンプレートが不正取得されると、次の脅威につながり、より大きな影響が想定される。

- ・リプレイ攻撃での利用
- ・テンプレートの基になった生体情報の復元
- ・本来用途以外への不正転用

リプレイ攻撃とは、傍受した信号を再度通信路に流す攻撃である。通信路にぜい弱性がある場合、不正取得されたテンプレートによる攻撃は、深刻な脅威となる。

テンプレートから元の生体情報を復元する試みは、テンプレート復元攻撃 (template inversion attack) と呼ばれ、顔や指紋などのモダリティで多くの研究者が取り組んでいる。近年では、GANなどの生成AIを活用した研究が進み、クオリティの高い復元が実現されている⁽¹¹⁾。テンプレートからの顔画像の復元は、生体認証システムの利用者を特定されるプライバシーリスクにもつながる脅威となる。

本来用途以外への不正転用というのは、異なるシステム間のクロスマッチングを意味する。例えば、企業のア

表4 プレゼンテーションアタックの主な対策技術 (PAD) ^{(5)~(10)}

モダリティ	ハードウェアによる対策	ソフトウェアによる対策
指紋	・静電容量式センサの利用 (指表面の電位差の検知) ・型取り／印刷の解像度を超える高解像度での指紋センシング、微細特徴の利用	・発汗により指紋のコントラストが変化する現象の検知
顔	・Depth センサによる顔の 3D 形状の取得 ・マルチスペクトル／赤外線反射特性の観測による印刷物判別 ・カメラのピントを意図的にずらした画像からの立体判別 ・ランダムに表情や動作を指定するチャレンジ応答方式 ・光に対する縮瞳や視線の動きなどの眼球反応の観測	・瞬き検出 ・顔の血流による皮膚の微小な色変化からの心拍の検知
虹彩	・可視光照明制御による瞳孔の収縮反応の誘発、観測	・虹彩に映り込む環境光の反射、瞳孔と虹彩の境界線の解析 ・瞬き検出 ・光の変化や視線移動に対する瞳孔の動き、形状の解析
静脈	・マルチスペクトル撮像による差異の解析	・複数枚の静脈画像からの脈動、血流の観測
音声	・認証時にチャレンジ音／超音波を混入 (再生攻撃ではチャレンジ音が欠落／相違) ・ランダムに文章や数字列を提示するチャレンジ応答方式	・録音・再生機器固有の雑音、微小なエコー、量子化雑音の検知 ・音声変換や音声合成モデル特有のスペクトルの特徴の検知 ・話速やピッチの時間変動、間の取り方などのダイナミクスの精査 ・RNN, Transformer を応用した判別
共通	—————	・画像特徴の解析 - 雑音やコントラスト等の画像品質指標からの判別 - 印刷画像のモアレ、ドットパターン等の検出 - ディスプレイ映像に生じる輝度むらや反射光、モアレ、ドットパターン等の検出 - 微細特徴の欠落の検知 - CNN や Vision Transformer を応用した判別

クセスコントロール用のデータベースから不正取得した顔テンプレートを使って、街頭の防犯カメラ映像から当該人物を追跡したり、別のシステムに保管された個人の健康情報を検索したりといった、セキュリティやプライバシーの深刻な脅威につながる。

これらの脅威を回避する手段として注目されているのが次章で解説するテンプレート保護技術である。

4 テンプレート保護技術

これまで解説したとおり、生体認証システムにおけるテンプレートの流出は、リプレイ攻撃や、元の生体情報の復元、ほかのシステムデータとのクロスマッチングなど、深刻な脅威につながる。一般に、パスワードや暗証番号、IC カードなどの記憶や所持に基づく認証手段で漏えいや紛失が発生した場合には、危たい化した認証情報 (クレデンシャル) の無効化や更新という措置が取られるが、生体情報には変更が難しいという本質的な性質がある。テンプレート保護技術は、こうした問題を解決する技術として期待されている。

テンプレート保護技術の基本的なフレームワークは、ISO/IEC 24745:2022 で国際標準化されている。その

中で、テンプレート保護技術に求められる要件は、次の三つとされている。

- (1) 不可逆性 (Irreversibility) : テンプレートから元の生体情報の類推や復元ができないこと。
- (2) 更新可能性 (Renewability) : 同じ生体情報から異なるテンプレートデータを生成できること。(危たい化したテンプレートを無効化し新たなテンプレートに更新できること。)
- (3) リンク不可能性 (Unlinkability) : 異なる生体認証システム／データベースとのクロスマッチングに利用できないこと。

実運用の観点からは、上記三つの要件に加えて、テンプレート保護により認証精度が著しく劣化しないとする「精度の維持」を要件とする。本稿では、代表的なテンプレート保護技術として、特徴変換、バイオメトリック暗号、暗号化照合の三つのアプローチを解説する。

4.1 特徴変換 (Feature Transformation)

特徴変換アプローチでは、生体特徴に不可逆な変換を適用し、変換後の特徴をテンプレートとして照合に利用する。2001 年に Ratha らによって、キャンセルババイオメトリクス (Cancelable Biometrics) の名で、概念

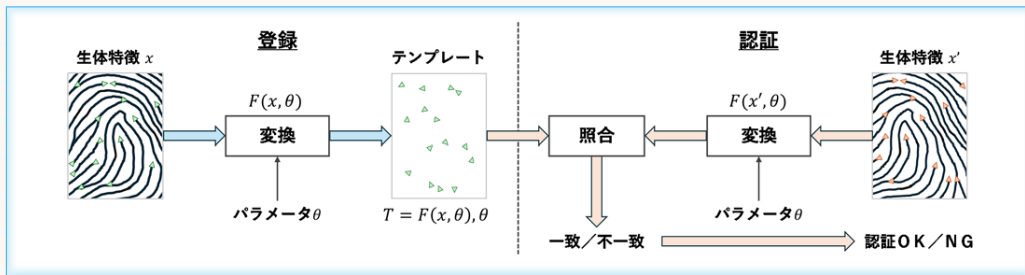


図3 特徴変換アプローチにおける登録と認証のフロー

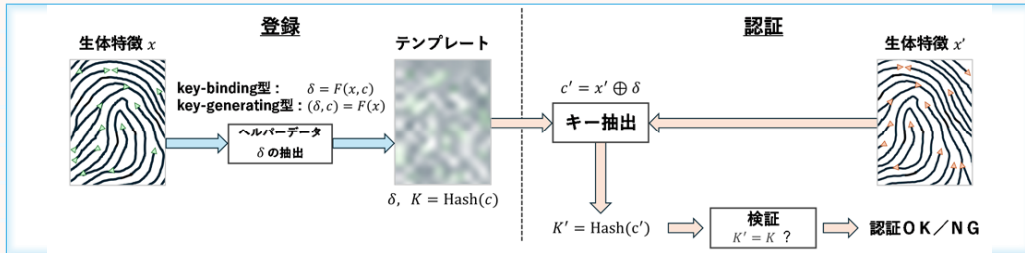


図4 バイオメトリック暗号を活用した生体認証システムの登録と認証のフロー

と基本アプローチが提案された⁽¹⁾。

図3に本アプローチで構成する生体認証システムの登録と認証のフローを示す。生体特徴 x を入力、 θ をパラメータとした変換関数 $F(x, \theta)$ によって生体特徴を変換し、変換した状態で照合を行う。 θ の変更によって生体特徴の変換結果を変更し、更新可能性とリンク不可能性を担保する。不可逆性は、変換関数の種別によって担保され、幾何的な変換やランダムプロジェクションなどの適用が研究されている^{(12), (13)}。

幾何的な変換の場合、変換後の特徴量同士の照合に、一般的な特徴量照合アルゴリズムも適用できる場合があり、システムへの導入負荷が低いメリットがある。一方で、変換アルゴリズムが単純であったり、パラメータ θ の漏えいがあったりすると、元の生体特徴や、元の生体特徴と同じ変換特徴が得られる生体特徴パターンを推定される危険性がある。 θ は登録時だけでなく、認証時にも必要となることから、厳格な管理が必要となる。また、変換後の特徴量類似度に着目し、遺伝的アルゴリズムで元の生体情報を探索する攻撃⁽¹⁴⁾ や、異なる変換パラメータで生成された複数のテンプレートから元の生体情報を再構成するARM (Attack via Record Multiplicity) 攻撃⁽¹⁵⁾ などが知られている。

4.2 バイオメトリック暗号 (Biometric Cryptosystems)

生体特徴は、個人内でも揺らぎがあるため、生体特徴そのものを、例えば暗号鍵のように安定的なデジタル情報として扱うことは困難である。そこで、特徴量を量子化して、誤り訂正符号を用いることで生体特徴の揺らぎを吸収し、更に暗号技術の知見を生かして不可逆性、更新可能性、リンク不可能性を実現する手法として、バ

イオメトリック暗号が研究されている。

図4に本アプローチで構成する生体認証システムの登録と認証のフローを示す。登録時は、生体特徴を使って、鍵 K を安全に封入したヘルパーデータを作成する。認証時は、ヘルパーデータと生体特徴から鍵を抽出する。認証は鍵の検証によって行う。

バイオメトリック暗号には、生体特徴とは独立に鍵 K を定める鍵結合型 (key-binding 型) と、生体特徴から鍵 K を生成する鍵生成型 (key-generating) がある。本稿では、鍵結合型と鍵生成型の代表的な手法として、Fuzzy Commitment⁽¹⁶⁾ と Fuzzy Extractor⁽¹⁷⁾ について解説する。鍵結合型でよく知られている手法として Fuzzy Vault⁽¹⁸⁾ もあるが、本稿では割愛する。

4.2.1 Fuzzy Commitment

Fuzzy Commitment は、生体特徴と誤り訂正符号を利用して作成したコミットメントから、鍵情報を安定的に抽出する方法である。

基本的なアイデアを以下に示す。ビット量子化された生体特徴 x と、ランダムに選択した誤り訂正可能な符号 c から、次式でヘルパーデータ δ を算出する。

$$\delta = x \oplus c$$

$\oplus$ はビットごとの排他的論理和演算を表す。今、個人内の揺らぎを含むビット量子化された生体特徴 x' が得られたとし、 x' と δ から次式で符号 c' を計算する。

$$c' = x' \oplus \delta$$

c' は、 x' と x の差異を c に反映したものとなるため、 x と x' の差異が許容範囲内にあれば、誤り訂正により符号 c' から符号 c が取得できる。しかるに、登録フェーズでは、生体特徴 x と符号 c から関数 $F(x, c)$ でヘルパー

データ δ と $K = \text{Hash}(c)$ を生成し、認証フェーズでは生体特徴 x' とヘルパーデータ δ から $K' = \text{Hash}(c')$ を生成して、 K' と K の一致判定で認証する仕組みが構築できる (図 4)。

生体特徴の揺らぎが大きい場合、安定的に鍵 K を抽出するためには、誤り訂正符号による訂正能力を高める必要があるが、誤り訂正能力を過度に高めると、他人受入れの発生による精度低下や、計算量の増大といった問題が生じる。このため、できるだけ安定的な生体特徴取得の実現が、Fuzzy Commitment 導入の課題となる。

4.2.2 Fuzzy Extractor

「鍵生成型」の本手法は、生体特徴 x から鍵 K とヘルパーデータ δ を生成する鍵生成関数 $\text{Gen}(x)$ と、揺らぎを含む生体特徴 x' とヘルパーデータ δ から、鍵 K' を生成する鍵再現関数 $\text{Rep}(x', \delta)$ の二つの関数で構成される。

典型的な実装では、 $\text{Gen}(x)$ は、誤り訂正符号 C の中から、 x に最近傍の符号語 $c \in C$ を選択し、次式で鍵 K と、ヘルパーデータ δ を生成する。

$$K = \text{Hash}(c), \delta = x \oplus c$$

$\text{Rep}(x', \delta)$ は、揺らぎを含む生体特徴 x' とヘルパーデータ δ から $c' = x' \oplus \delta$ を計算し、 c' を誤り訂正した上で、 $K' = \text{Hash}(c')$ を計算する。

両関数を活用することで、図 4 に示した認証の仕組みが構成できる。また、生体情報 x に由来して鍵生成ができることから、公開鍵暗号基盤 (PKI) やブロックチェーンの署名鍵生成への応用も検討されている。署名鍵生成に関しては、Fuzzy Signature など、より発展的なアプローチも研究されている^{(19), (20)}。

Fuzzy Commitment 同様に、特徴抽出や量子化に精度と工夫が求められるとともに、ヘルパーデータ δ から、生体特徴や鍵に関する情報が漏れないように設計することが重要となる。また、符号語 c が漏れいすると、 δ と c から元の生体特徴 x が復元できてしまうため、厳重な管理が必要となる。

4.3 暗号化照合 (Biometrics in encrypted domains)

「暗号化照合」は、生体特徴を暗号化したまま安全に照合するアプローチで、準同形暗号 (Homomorphic Encryption) を用いる方法や、セキュアマルチパーティ計算を用いる方法が広く研究されている。

準同形暗号とは、二つの暗号文 $\text{Enc}(m_1)$ と $\text{Enc}(m_2)$ を復号することなく、 $\text{Enc}(m_1 + m_2)$ や $\text{Enc}(m_1 \times m_2)$ などの演算ができる準同形性を有する暗号で、加算及び乗算の双方、及び組合せに準同形性を持つ完全準同型暗号 (FHE: Fully Homomorphic Encryption) と、加算

または乗算のいずれか一方にのみ準同形性を持つ部分準同形暗号 (PHE: Partially Homomorphic Encryption) がある。生体認証技術においては、生体特徴の類似度計算に積和演算が用いられることが多いことから FHE の活用が期待されたが、FHE には計算コストが極めて高いという課題がある。現在は、FHE の計算効率改善研究と、より軽量で実装が容易な PHE や、加算は無制限であるが乗算には回数制限がある somewhat 準同形暗号 (SHE: Somewhat Homomorphic Encryption) の活用研究が並行して進められている⁽²¹⁾。

準同形暗号で暗号化した生体特徴に対し、暗号化したまま照合演算を適用した場合、照合結果もまた暗号化された状態となる。照合結果を取り出すためには、これを復号する必要があるが、この復号処理をマルチパーティ計算で行うのが、セキュアマルチパーティ計算による暗号化照合アプローチである。代表的な手法としては、Shamir の秘密分散法を用いて準同形暗号の復号鍵を複数のパーティに分散し、各パーティで部分復号する方式がある。各パーティの部分復号結果を集約して Lagrange 補間等の手法で再構成することで、照合結果を復元する。この方式では、照合に関与するいずれのパーティも部分的な復号鍵しか保持しないため、完全な復号鍵が漏れいし、結果として生体特徴や照合結果が漏れいしてしまうリスクを低く抑えることができる。

5 今後の展望

本稿では、生体認証技術／システムに対する攻撃と、その対策技術として PAD と、テンプレート保護技術に焦点を当てて詳説した。

昨今、特殊詐欺やソーシャルエンジニアリングの温床として、映像や音声を紹介したりリモートコミュニケーションにおける「なりすまし」が社会的な問題となりつつあるが、本稿で解説した PAD 技術は、こうした「なりすまし」検知への応用も期待される。また、日本企業をはじめとした事業者を中心に、本稿で解説したテンプレート保護技術や、より発展させた技術を応用し、セキュリティやプライバシーに配慮した認証基盤の構築・実用化を進める動きもある。生体認証の持続的な発展には、本稿で紹介した技術を活用しつつ、プライバシー保護設計 (Privacy by Design) といった観点からの包括的な対応も必要となろう。

このほか、本稿では解説を割愛したが、FIDO や FIDO2 など、PC やスマートフォンに搭載された生体認証技術を活用した安全なオンライン認証基盤の標準化も進んでいる⁽²²⁾。スマートフォンの普及に伴って、オンラインの公的サービスや金融サービス等における生体認

証活用にも、一層の拍車がかかっている。

このように、今後も生体認証技術の活用は拡大していくことが予想される。生体認証技術の安全性を理解する上で、本稿の内容が一助となれば幸いである。

■ 文献

- (1) N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," IBM Syst. J., vol. 40, no. 3, pp. 614-634, Jan. 2001.
- (2) A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," EURASIP J. Adv. Signal Process, Article 113, March 2008.
- (3) W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "Security and accuracy of fingerprint-based biometrics: A review," Symmetry 11, no. 2: 141, Jan. 2019.
- (4) T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of artificial "Gummy" fingers on fingerprint systems," Proc. SPIE, vol. 4677, April 2002.
- (5) K. Karampidis, M. Rousouliotis, E. Linardos, and E. Kavallieratou, "A comprehensive survey of fingerprint presentation attack detection," J Surveill Secur Saf 2021;2:117-61, Oct. 2021.
- (6) L. Debiasi, C. Kauba, H. Hofbauer, B. Prommegger, and A. Uhl, "Presentation attacks and detection in finger- and hand-vein recognition," Proc. the Joint Austrian Computer Vision and Robotics Workshop 2020, pp.65-70, 2020.
- (7) T. T. Nguyen, Q. H. Nguyen, D. T. Nguyen, D. T. Nguyen, T. Huynh-The, S. Nahavandi, T. T. Nguyen, Q. Pham, and C. M. Nguyen, "Deep learning for deepfakes creation and detection: A survey," Computer Vision and Image Understanding, vol. 223, Aug. 2022.
- (8) D. Sharma and A. Selwal, "A survey on face presentation attack detection mechanisms: hitherto and future perspectives," Multimed Syst. Vol. 29, no. 3, pp. 1527-1577, March 2023.
- (9) C. B. Tan, M. H. A. Hijazi, N. Khamis, P. N. E. binti Nohuddin, Z. Zainol, F. Coenen, and A. Gani, "A survey on presentation attack detection for automatic speaker verification systems: state-of-the-art, taxonomy, issues and future direction," Multimedia Tools and Appl., vol. 80, pp. 32725-32762, Sept. 2021.
- (10) S. Marcel, J. Fierrez, and N. Evans, Handbook of biometric anti-spoofing: presentation attack detection and vulnerability assessment, Springer, 2023.
- (11) M. Gomez-Barrero and J. Galbally, "Reversing the irreversible: A survey on inverse biometrics," Comput. & Security, vol. 90, no. 2, Dec. 2019.
- (12) N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," IEEE Trans. Pattern Analysis and Machine Intell., vol. 29, no. 4, pp. 561-572, April 2007.
- (13) A. B. J. Teoh, A. Goh, and D. C. L. Ngo, "Random multispace quantization as an analytic mechanism for BioHashing of biometric and random identity inputs," IEEE Trans. Pattern Analysis and Machine Intell., vol. 28, no. 12, pp. 1892-1901, Dec. 2006.
- (14) X. Dong, Z. Jin, and A. T. B. Jin, "A genetic algorithm enabled similarity-based attack on cancellable biometrics," IEEE 10th International Conf. Biometrics Theory, Appl. and Syst.(BTAS), Sept. 2019.
- (15) C. Li and J. Hu, "Attacks via record multiplicity on cancelable biometrics templates," Special Issue: Security of new generation computing systems(NSS 2012), vol. 26, no. 8, pp. 1593-1605, June 2014.
- (16) A. Juels and M. Wattenberg, "A fuzzy commitment scheme," Proc. 6th ACM conf. Comput. and commun. security(CCS '99), Association for Comput. Mach., pp. 28-36, Nov. 1999.
- (17) Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: how to generate strong keys from biometrics and other noisy data," EUROCRYPT 2004, Springer Lecture Notes in Comput. Sci., vol.3027, pp.523-540, 2004.
- (18) A. Juels and M. Sudan, "A fuzzy vault scheme," Designs, Codes and Cryptography, vol. 38, no. 2, pp. 237-257, Feb. 2006.
- (19) K. Takahashi, T. Matsuda, T. Murakami, G. Hanaoka, M. Nishigaki, "Signature schemes with a fuzzy private key," International J. Inf. Security, vol. 18, pp. 581-617, Feb. 2019.
- (20) H. Higo, T. Isshiki, S. Otsuki, and K. Yasunaga, "Fuzzy signature with biometric-independent verification," International Conf. Biometrics Special Interest Group (BIOSIG), pp.1-6, Sept. 2023.
- (21) M. Yasuda, T. Shimoyama, J. Kogure, K. Yokoyama, and T. Koshiba, "Practical packing method in somewhat homomorphic encryption," International Workshop Data Privacy Management 2013, Springer Lecture Notes Comput. Sci., vol. 8247, pp. 34-50, Jan. 2014.
- (22) FIDO Alliance. <https://fidoalliance.org/>

高田直幸

1998 東北大・工・電気卒。2000 同大学院修士課程了。同年セコム株式会社入社。以来、生体認証、画像解析技術の研究に従事。2021～2023 バイオメトリクス研究専門委員会副委員長。現在、セコム株式会社IS研究所研究戦略部長。東京科学大技術経営専門職学位課程在学中。



サイバー攻撃の要因である「ぜい弱性」とは？

——ぜい弱性がもたらすリスクとぜい弱性管理について——

西村隆廣 Takahiro Nishimura NRI セキュアテクノロジーズ株式会社

1 はじめに

インターネットを利用するサービスが停止すれば、私たちは友人への連絡もままならず、「口コミ」評価の良い飲食店を見つけることも、その店を予約することも、これまで行ったことのない新しい店までたどり着くこともできなくなってしまうだろう。もちろんこれらに限らず企業や組織の業務においても、現代の我々の生活のあらゆる部分において、インターネットは必要不可欠なものとなっている。

サービス停止のみならず、企業の顧客データや個人情報漏えい、データの暗号化など、企業や個人に限らず社会にも大きな影響を及ぼすサイバー攻撃は、ニュースなどでも多く取り上げられている。多くの人が「ソフトウェアのぜい弱性を狙った攻撃」などという言葉を目にした経験があるのではないだろうか。漠然と「ぜい弱性」という言葉を聞いたことがある方は多く、何となく理解しているかもしれないが、詳しく理解している方は少ないと思われる。サイバー攻撃発生の要因の一つとなるぜい弱性について、発生する原因や攻撃例、企業や組織における対策方法を中心に解説していく。

2 ソフトウェアのぜい弱性とは

ぜい弱性とは、システムやソフトウェアなどのセキュリティ上の欠陥のことを指す。その欠陥は不正アクセスやコンピュータウイルスなどのサイバー攻撃により、甚大な被害をもたらす原因の一つとされている。ぜい弱性は英語では Vulnerability と言い、攻撃の受けやすさ、被害の遭いやすさなどを意味する。コンピュータ用語ではなく、人の状態などに対しても使われる言葉である。

似たような言葉として「セキュリティホール」もあるが、こちらはシステムやソフトウェアの開発段階における設計ミスや、プログラムコードの書き間違いなどに

よって発生するセキュリティ上の欠陥を指す。対してぜい弱性は、管理態勢や人的ミスなども含めたシステム環境全体における欠陥を指す。つまり、セキュリティホールはぜい弱性の一種であり、不具合や設計ミスが原因で発生する欠陥のみを指している。

システム上の欠陥については「バグ」という言葉も一般的ではないだろうか。こちらはセキュリティにかかわらず、システムやソフトウェアが正常に動作しない場合に使用される言葉である。このバグも、ただ単に機能が想定どおりの動きをしない場合だけでなく、セキュリティに影響がある場合にはぜい弱性と呼ばれる。バグは想定どおりの動きをしているかどうかテスト段階で見つけることは難しくないのだが、ぜい弱性やセキュリティホールは通常の使い方をする分には問題が発生しないため、開発側が気づきにくいと言われている（図 1）。

3 ソフトウェアぜい弱性が発生する原因

ぜい弱性が発生する原因とは何か、その発生原因を対策すれば、ぜい弱性によって引き起こされるサイバー攻撃を防ぐことができるのではないだろうか。ぜい弱性の主な発生原因は以下のようなものが挙げられる。

- ・開発段階における設計ミス
- ・プログラムコードの書き間違い
- ・OS や基幹システムの更新に伴い発生する欠陥
- ・使用しているソフトウェアの設計、または更新に伴い発生する欠陥
- ・OS やソフトウェアのアップデートや修正パッチの未適用
- ・運用や設定のミス
- ・新たなサイバー攻撃手法の登場により、従来正常であった状態がぜい弱性となるケース

これら全てを含め漏れなく対応ができていれば、ぜい弱性の発生を防ぐことができるかもしれない。しかし、

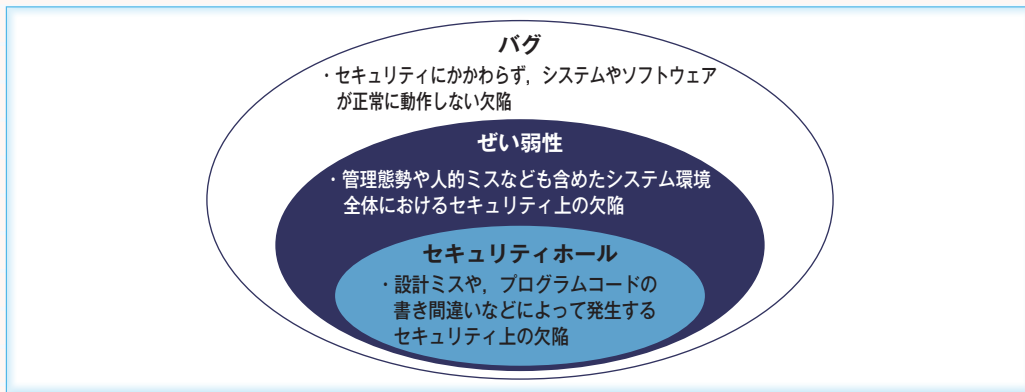


図1 ぜい弱性、セキュリティホール、バグの関係図

サイバー攻撃の進化によって日々新たな攻撃手法が生み出され続けており、想定し得ないことがぜい弱性として見つかるなど事前の対策は非常に難しい。

既に見つかったぜい弱性については、OS やソフトウェアのアップデート、修正パッチを早期に適用することにより、サイバー攻撃の被害に遭う可能性を低くすることが可能である。個人であればアップデートや修正パッチを即適用することはそう負担が掛からないことかもしれない。しかし、企業や組織などで様々なシステムを利用していればいるほど、アップデートや修正パッチによりほかのシステムに影響がないか入念な確認が必要のため、大きな負担となる。そのためぜい弱性が放置されてしまい、放置されたぜい弱性を突かれてサイバー攻撃の被害に遭う企業や組織も少なくない。

4 ソフトウェアぜい弱性がもたらす影響と攻撃例

サイバー攻撃の多くはぜい弱性を悪用して行われており、ぜい弱性を放置することでサイバー攻撃の被害に遭う可能性は高まり、事業活動に甚大な影響を及ぼすこととなる。本章では、具体的な攻撃例について解説する。

4.1 マルウェア感染

マルウェアとは、不正かつ有害な動作を行う意図で作成されたコンピュータウイルス、トロイの木馬、ワーム、スパイウェアなどを含む、悪意のあるソフトウェアや悪質なコードの総称である。

ぜい弱性を放置することで、マルウェアに感染する可能性が高まることは確実である。PC がマルウェアに感染すると、勝手に外部と接続して操作されたり、PC 内のファイルが破壊や暗号化されたり、外部へ持ち出されるなどの被害に遭う。企業や組織にとっては業務に支障をきたすばかりでなく、存続も危ぶまれるような大きな損害額となる可能性もある。

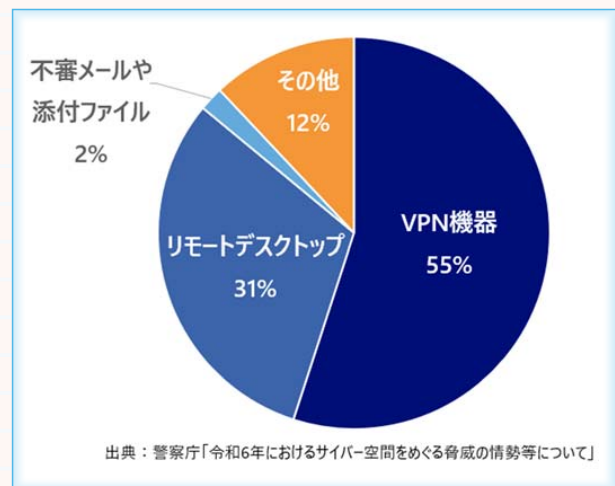


図2 ランサムウェア感染経路

昨今のマルウェアの多くはOS やソフトウェアのぜい弱性を利用して感染するため、ぜい弱性を解消するためのアップデートやパッチの適用は極めて重要である。

4.2 不正侵入

ここでいう不正侵入とは、攻撃者による直接的な端末やサーバへの不正侵入を伴う侵害を指す。侵害の影響度が高いことから、ランサムウェアを用いた侵害が国内外で非常に注目されており、警察庁は「ランサムウェア被害において、VPN やリモートデスクトップ用の機器からの侵入が、全体の感染経路の8割以上を占める状況である」と報告^{*1}している（図2）。

ランサムウェアの攻撃者は、VPN などのぜい弱性のある機器を攻撃の足掛かりとして企業や組織のネットワークに侵入する。そしてドキュメントファイルなどを「人質」として暗号化し、復号のために被害者に金銭を要求する。攻撃を受けた企業や組織は、被害拡大を防止

*1 警察庁「令和6年におけるサイバー空間をめぐる脅威の情勢等について」

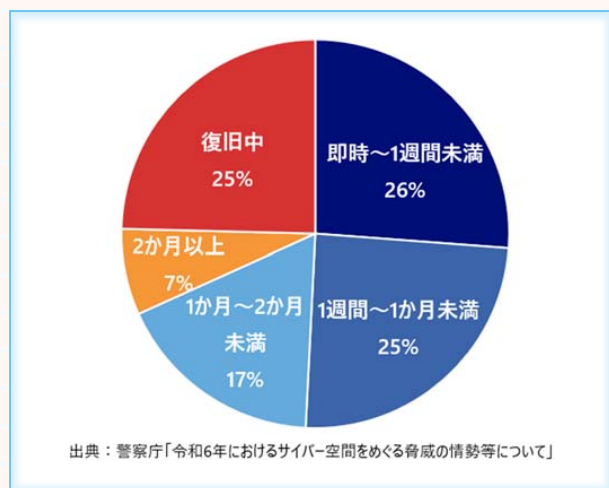


図3 ランサムウェア被害の復旧等に要した期間

するためにシステムを停止せざるを得なくなる場合や、業務の継続に影響が及ぶ場合がある。そのため企業や組織は自分たちが使用している機器を把握し、ぜい弱性やアップデートに関する情報を確認し、ぜい弱性を放置することなくアップデートやパッチの適用を確実に実施することが重要である。システム保守を外部委託している場合は、ぜい弱性の対処が保守契約に含まれているかを確認し、その対処が適切に実施されていることを確認することも重要である。

4.3 データの盗聴

ここでいうデータの盗聴とは、企業が公開しているWebサイトなどにおいてデータが盗まれることを指す。Webサイトにおいて後述の4.5.1のSQLインジェクションのぜい弱性がある場合、Webサイト上の入力フォームに不正な文字列を挿入することで、不正にデータベースにアクセスすることができてしまう。そのためデータベース内の個人情報などが盗まれ、情報漏えいの被害につながる。

Webアプリケーションのぜい弱性診断を行い、見つかったぜい弱性に対策を施すことでこの被害を未然に防ぐことが可能である。

4.4 システムの停止

ぜい弱性を突かれてシステムに不正侵入された場合、調査や復旧までの間、システムやサービスを停止せざるを得ない状況に追い込まれる場合も少なくない。ランサムウェアによる企業のシステム停止のニュースは記憶に新しいのではないだろうか。その企業が提供する動画配信サービスは、復旧までに実に2か月もの時間を要した。同社は被害拡大防止のためにサーバをシャットダウンしたが、攻撃者により遠隔からシャットダウンしたサーバを起動されるという執ような攻撃を受けた。その

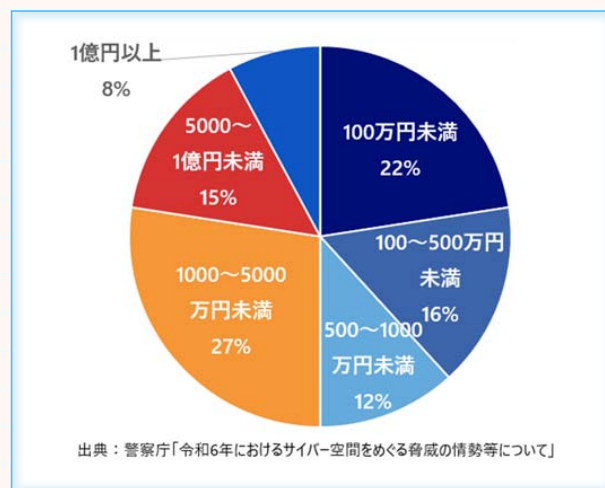


図4 ランサムウェア被害の復旧等に要した費用

ためサーバの電源ケーブルや通信ケーブルを物理的に抜線したことで、データセンタ内のサーバ全てが使用不可となったことを公表している。犯行グループが発表した声明をみると、ここまで被害が大きくなった原因は仮想化基盤のぜい弱性であったと言われている。

企業や組織において、システム停止が発生すれば信頼の失墜のみならず、機会損失などの被害も甚大となる(図3、4)。

4.5 Webサイトの改ざん

Webサイトの改ざんとは、文字どおりWebサイトが悪意のある何者かによって管理者の意図しない何らかの内容に書き換えられてしまうことや、Webサイト上に悪意のあるファイルなどを埋め込まれてしまうことを指す。最悪の場合、改ざんされたサイトを閲覧した人のPCにマルウェアを感染させてしまうなど、自らが加害者になってしまう可能性もある。Webサイトの改ざんの原因となるぜい弱性を利用した攻撃として、主に以下の三つがある(表1)。

4.5.1 SQLインジェクション

Webアプリケーションのぜい弱性を利用し、Webサイト上の入力フォームにSQL文を注入(インジェクション)することで、データベースに保存されたデータを不正に読み取ったり、改ざんしたりする攻撃である。決済を伴うECサイトや会員登録を行うポータルサイトなど、SQLサーバを利用するサイトが標的となる。

この攻撃の対策としては、プレースホルダの利用、エスケープ処理、Webアプリケーションのバージョンを最新に保つこと、WAF(Web Application Firewall)の導入などがある^{*2}。

表 1 Web サイトのぜい弱性を突いたサイバー攻撃

名称	手法	対象
SQL インジェクション	Web サイト上の入力フォームに SQL 文を注入（インジェクション）し、データベースに保存されたデータへの不正アクセスや改ざんなどを行う	決済を伴う EC サイトや、会員登録を行うポータルサイトなど
クロスサイト・スクリプティング	不正な JavaScript や HTML などを含んだ URL をクリックさせ、偽ページなどを表示させる	アンケートサイトやサイト内検索、ブログ、掲示板など
クロスサイト・リクエストフォージェリ	悪意のある URL をユーザにクリックさせ、第三者がユーザになりすまし不正な操作を行う	ログインを必要とする、オンラインバンキング、SNS、EC サイトなど

4.5.2 クロスサイト・スクリプティング

Web アプリケーションのぜい弱性を利用し、不正な JavaScript や HTML などを含んだ URL をクリックさせることで、ユーザの Web ブラウザに偽ページなどを表示させる攻撃である。アンケートサイトやサイト内検索、ブログ、掲示板などといったユーザからの入力内容を基に Web ページを生成するサイトなどが標的となる。

この攻撃の対策としては、サニタイジング（スクリプトの無害化）、入力値の制限、WAF の導入などがある^{*2}。

4.5.3 クロスサイト・リクエストフォージェリ

Web アプリケーションのセッション管理のぜい弱性を利用し、悪意のある URL をユーザにクリックさせることで、第三者がユーザになりすまして不正な操作を行う攻撃である。ログインを必要とするオンラインバンキング、SNS、EC サイトなどが標的となる。

この攻撃の対策としては、トークンの利用、リクエストヘッダの確認などがある^{*2}。

これら Web サイトの改ざんに関わる攻撃は、全て 4.3 のデータの盗聴の対策と同様である。すなわち Web アプリケーションのぜい弱性診断を行い、見つかったぜい弱性に対策を施すことでサイバー攻撃の被害を未然に防ぐことが可能である。

5

ぜい弱性情報の収集・活用、確認・対策方法

私たちが日々の業務や生活の中で使用する様々なシステムは、一つのシステムの中で多数のソフトウェアが稼働している。ぜい弱性がもたらすサイバー攻撃の被害をできるだけ防ぐためには、自組織が利用するシステムに内在するソフトウェアを全て把握し、それらのぜい弱性情報を入手し、その情報を評価した上で、ぜい弱性への対応を行う必要がある。その一連のプロセスを「ぜい弱性管理」と呼ぶ。ぜい弱性管理を行うことで自組織のセキュリティが向上するばかりでなく、セキュリティ対策状況が可視化され、万が一サイバー攻撃被害に遭ったと

しても、その対処を効率的に行うことができるようになる。その結果、被害を最小限に抑えることが期待できる。

5.1 ぜい弱性情報の収集

ぜい弱性は主に、ソフトウェアの開発ベンダなどのホワイトハッカーが探したり、攻撃者が実際に悪用したりすることで見つかる。こうして見つかったぜい弱性の情報は、公開データベースに登録されることが多い。主要なデータソースは以下のとおりである（表 2）。

5.1.1 JPCERT/CC

JPCERT/CC（一般社団法人 JPCERT コーディネーションセンター）^{*3} は日本におけるコンピュータセキュリティインシデントへの対応を行う組織である。国内外のセキュリティ関連情報を収集し、セキュリティアドバイザリーやぜい弱性情報、注意喚起を公開している。

5.1.2 IPA

IPA（独立行政法人情報処理推進機構）^{*4} は日本の IT 国家戦略を技術面・人材面から支えるために設立された独立行政法人である。本機構の所管官庁は経済産業省であり、セキュリティインシデントへの対応支援、ぜい弱性情報の収集と公開、セキュリティ意識の向上を図るための啓発活動などを実施している。JPCERT/CC とともに日本国内における情報セキュリティの中心的な役割として機能している。

5.1.3 JVN

JVN（JP Vendor Status Notes）^{*5} は経済産業省告示「ソフトウェア等脆弱性関連情報取扱基準」を受けて、日本国内の製品開発者のぜい弱性対応状況を公開するサイトである。JPCERT/CC と IPA により共同で運営さ

^{*2} これらは具体的な実装方法の説明となるため、本解説では割愛する。

^{*3} JPCERT/CC (<https://www.jpcert.or.jp/>)

^{*4} 独立行政法人情報処理推進機構：IPA (<https://www.ipa.go.jp/>)

^{*5} Japan Vulnerability Notes (<https://jvn.jp/>)

表 2 ぜい弱性情報の主要なデータソース

名称	概要
JPCERT/CC (一般社団法人 JPCERT コーディネーションセンター)	日本国内の情報セキュリティインシデントに対応するための民間のコンピュータセキュリティインシデント対応チーム (CSIRT)
IPA (Information-technology Promotion Agency, Japan: 独立行政法人 情報処理推進機構)	日本政府 (所轄官庁は経済産業省) が設立した情報セキュリティや IT 人材育成の推進を担う独立行政法人
JVN (Japan Vulnerability Notes)	JPCERT/CC と IPA が共同運営する日本で使用されているソフトウェアなどのぜい弱性関連情報とその対策情報を提供するポータルサイト
JVN iPedia	IPA が運営する国内外問わず日々公開されるぜい弱性対策情報を、JVN, JPCERT/CC, NVD などと情報と連携して、収集・蓄積することを目的としたぜい弱性情報データベース
NVD (National Vulnerability Database)	NIST (米国国立標準技術研究所) が運営するぜい弱性情報データベース
Exploit Database	OffSec 社が運営する実際に確認されたセキュリティぜい弱性を利用した攻撃コード (Exploit) や対策方法を収集・公開しているオープンな情報共有データベース
OWASP (Open Web Application Security Project)	Web アプリケーションやソフトウェアのセキュリティを向上させることを目的とした米国の非営利団体で、Web アプリケーションのセキュリティに関するガイドラインやツール、フレームワークを無償で提供

れている。

5.1.4 JVN iPedia

JVN iPedia^{*6} はぜい弱性情報データベースである。JVN が新たなセキュリティ情報をいち早く提供するプラットフォームであるのに対し、JVN iPedia は日々発見されるぜい弱性対策情報を蓄積し、アーカイブ機能や検索機能を実装して幅広く利用することを目的としている。

5.1.5 NVD

NVD (National Vulnerability Database)^{*7} は NIST (米国国立標準技術研究所) によって管理されているぜい弱性情報データベースである。世界で最も広く利用されているぜい弱性情報のソースである。

5.1.6 Exploit Database

Exploit Database^{*8} はセキュリティに関する教育やテストなどを提供する OffSec 社が、実際に使用可能なぜい弱性のエクスプロイトコードや攻撃手法を収集したオンラインデータベースである。セキュリティ研究者が新たに発見されたぜい弱性の悪用方法を共有するためのプラットフォームで、システムのセキュリティ検証を行う際の実践的なリソースとして利用されている。

5.1.7 OWASP

OWASP (Open Web Application Security Project)^{*9} は Web アプリケーションのセキュリティに関する包括的な情報、ガイドライン、ツール、リソース

を提供しており、セキュリティ対策の基準として開発者やセキュリティ専門家に広く活用されている。

これら信頼性のある情報源から収集した、ぜい弱性情報について、主に以下が確認ポイントとなる。

- CVE 識別子 (ぜい弱性に割り当てられる一意の ID)
- ぜい弱性の概要
- 影響を受ける製品／バージョン
- CVSS スコア (ぜい弱性の深刻度)
- 修正情報 (アップデートやパッチなどの対応策)

5.2 ぜい弱性情報の活用

収集したぜい弱性情報から、自組織内で影響を受ける可能性のあるシステムやアプリケーションを特定する必要がある。次にそのぜい弱性が自組織に与えるリスクを評価し、優先して対応すべきか否かといった対応方針を決定する。

ぜい弱性情報は毎日多数公開されており、その全ての情報を収集してリスクを評価することは大変労力のいる仕事である。リスクを評価して対応優先度を決定するに

*6 ぜい弱性対策情報データベース: JVN iPedia (<https://jvndb.jvn.jp/>)

*7 NIST National Vulnerability Database (<https://nvd.nist.gov/vuln>)

*8 Exploit Database (<https://www.exploit-db.com/>)

*9 Open Web Application Security Project: OWASP (<https://owasp.org/>)

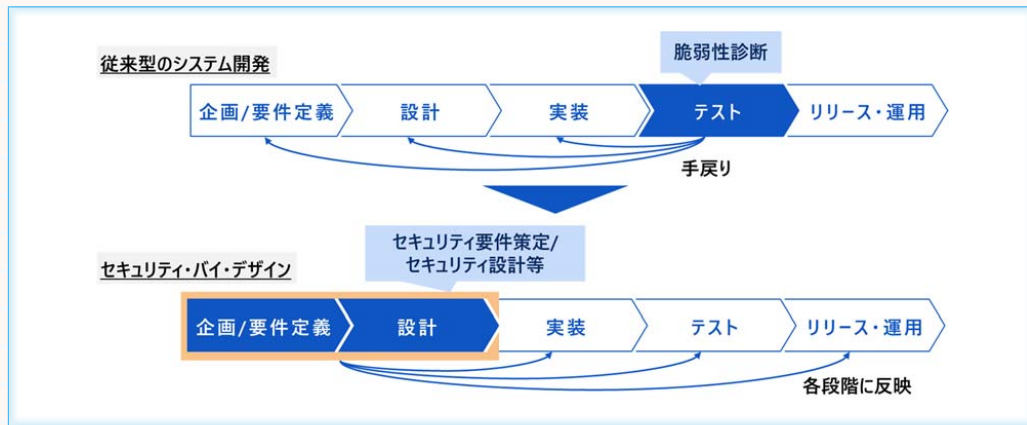


図5 セキュリティ・バイ・デザイン推進による安全性向上のイメージ

は高度な専門的知識も必要となるため、ぜい弱性管理においては外部の専門家を利用する企業や組織も少なくない。

5.3 ソフトウェアのぜい弱性の確認

日々新たな攻撃が生まれているため、自組織が利用するソフトウェアにぜい弱性が潜んでいないか、定期的な確認も必要である。

ぜい弱性を確認する方法には、ソースコード解析、ぜい弱性スキャン、ペネトレーションテストなどがある。しかし、専門知識を要するため自組織のみで実施するハードルは高く、こちらも外部の専門家による実施が一般的である。

5.4 ソフトウェアのぜい弱性の対策

常に新しいぜい弱性情報を収集し、自組織に影響のあるぜい弱性を見つけ、それを評価し、対応方針を決め、対応を実施する。また、自組織が利用するシステムに内在するソフトウェアにぜい弱性が潜んでいないか、定期的に確認して対応を実施する。ソフトウェアのぜい弱性の対策としてできることは、ぜい弱性管理プロセスの整備と、そのプロセスにのっとった継続的な対応を地道に行うことである。言葉にするのは簡単だが、多くの企業や組織にとって、これらに漏れなく対応するスキルを持ち合わせた人材、予算の確保などは非常に困難であろうと思われる。

ぜい弱性を完全になくすことはできないが、ぜい弱性を減らす方法として「セキュリティ・バイ・デザイン」という考え方がある。次章でその考え方について解説する。

6 セキュリティ・バイ・デザイン

システムやソフトウェア、製品の開発初期段階からセキュリティを考慮し、設計プロセスに組み込む考え方、



図6 ぜい弱性修正コストのイメージ

セキュリティ・バイ・デザインについて解説する。

セキュリティ・バイ・デザインという概念は新しいものではなく、2000年頃には登場していたと言われている。従来はリリース前のぜい弱性診断を軸としてセキュリティ対策を行うことが主流だった。しかし、リリース直前や運用中に見つかったぜい弱性を修正するには、システム全体を再設計することが必要な場合もあるため、相当なコストや時間を要することもある。そのため、ぜい弱性診断によってぜい弱性が発見されても、緊急度の高いぜい弱性は修正するが、コストやリリースまでの時間の制約から、低リスクのぜい弱性は修正しないケースが多いのが実態である。

こうした状況を防ぐため、セキュリティ・バイ・デザインを採用することで、企画・設計段階で検出可能なぜい弱性が存在しない状態にすることが可能となる（図5）。大幅なコスト削減効果を望むことができ（図6）、従来見過ごされていた低リスクのぜい弱性や、リスクを受容していた比較的风险の高いぜい弱性にまで対策が施され、セキュリティ品質が向上する。

近年のDX（デジタルトランスフォーメーション）やデジタルビジネスの進展に伴い、セキュリティ・バイ・デザインの重要性が改めて認識されており、デジタル庁が2022年に「政府情報システムにおけるセキュリティ・バイ・デザインガイドライン^{*10}」を発行している。

2024年には、金融庁が公表した「金融分野における

2.3.4.3. セキュリティ・バイ・デザイン
基本的な対応事項
①金融商品・サービスの企画・設計段階から、セキュリティ要件を組み込む「セキュリティ・バイ・デザイン」を実践すること。サービス全体の流れの中で、重要なサードパーティも含めてリスクを検証し対策を講ずること。 ②自組織にシステムを提供する重要なサードパーティにおいて、セキュリティ・バイ・デザインを実施できる体制となっているかを確認すること。
対応が望ましい事項
a. セキュリティ・バイ・デザインにかかる管理プロセスを、以下の点も考慮のうえ、整備し、運用すること。 ・セキュアコーディングに係る基準を策定し、実施すること。 ・データの機密性、アクセス管理、イベントログ取得等のセキュリティ要求事項を明確化していること。 ・セキュリティ技術・アーキテクチャーに係る設計標準を策定すること。 ・アプリケーションソフトウェアのリリース前及びリリース後定期的に、アプリケーションのぜい弱性診断を実施すること。 ・システムへのぜい弱性の混入及び作込みを未然に防止し、早期に検知するツール（ソースコード解析ツール等）を活用すること。

図7 金融庁が公表した「金融分野におけるサイバーセキュリティに関するガイドライン」の要件

サイバーセキュリティに関するガイドライン^{*11}」においても、セキュリティ・バイ・デザインの対応が要件の一つとして盛り込まれている（図7）。本要件では企画・設計段階だけではなく、開発・運用工程における事項も挙げられている。本ガイドの要件に準拠するためには、システム開発のライフサイクル全体でセキュリティ対策を考慮していく必要があると考えられる。

セキュリティ・バイ・デザインは概念であり、決まった型はなく、企業や組織によって対応策は様々で大きく異なることもある。まずは小さな取組みからでも、セキュリティ・バイ・デザインを実施して頂きたい。

7 おわりに

残念ながら、ぜい弱性を完全になくすことはできない。なぜなら技術の進歩、攻撃手法の進化、意図しない操作などとともに、新たなぜい弱性が常に発見されるためである。

しかし、ぜい弱性を放置すればその分セキュリティリスクは高まり、事業継続の危機はもちろん、社会的混乱を及ぼす可能性もある。ぜい弱性対策の重要性を理解し、万が一サイバー攻撃の標的となったとしても、被害を最小限に食い止めることができるようにぜい弱性に挑んで頂きたい。

西村隆廣

2002 野村総合研究所に入社。2009 NRI セキュアテクノロジーズに出向後、セキュリティコンサルティング業務に従事。セキュリティ戦略の企画・評価・マネジメント、サイバーセキュリティ態勢整備、サイバーセキュリティ分野の先進的な事業開発等を担当。



※10 デジタル庁（https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/7e3e30b9/20240131_resources_standard_guidelines_guidelines_01.pdf）

※11 金融庁（<https://www.fsa.go.jp/news/r6/sonota/20241004/18.pdf>）

ディープフェイク音声の脅威と対策について

鵜木 祐史 Masashi Unoki 北陸先端科学技術大学院大学

1 はじめに

情報通信技術や AI（人工知能）技術の急激な発展により、我々を取り巻くマルチメディア情報通信の利用形態が劇的に変化し、それと同時に社会的脅威も急激に高まっている。これらの技術は我々の生活に様々な面でメリットをもたらす生活を豊かにする一方で、個人情報の漏えいによる悪用といったリスクにさらされている。

例えば、音声メディアに焦点を当ててみると、10 数年前までは、違法コピー・違法配信が主たる社会問題であり、近い将来、デジタルフォレンジクス（デジタル機器に残された情報を収集・解析し、証拠として活用する技術）における音声改ざん等が問題になると予想されていた⁽¹⁾。しかし、近年では、図 1 に示すように、深層学習ベースの音声合成技術で制作された偽物の合成音声（以後、「ディープフェイク音声」と呼ぶ）による「なりすまし」といった社会的脅威が急激に高まっている⁽²⁾。そのため、音声メディアを安心安全に利用するための仕組みや、音声に含まれるプライバシー情報をディープフェイクのような攻撃から守る革新的技術の確立が喫緊の課題になっている。

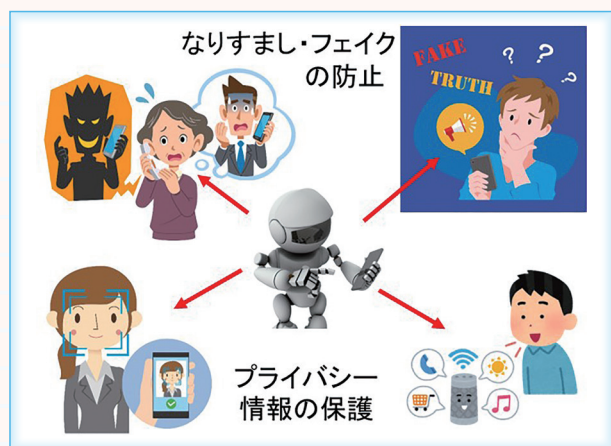


図 1 音声セキュリティの課題

本稿では、ディープフェイク音声による脅威を紹介し、その対策と課題を概説する。また、最新の研究成果を紹介し、現在の動向と残された課題を検討する。

2 音声合成技術の歴史の概観と現在の展開

音声合成技術は、元々フェイク音声を作成するために開発されたわけではない。音声合成技術が目指すゴールは、「福祉応用」など豊かな人間社会形成の一助になることである。例えば、将来何かの理由（病気等による発話器官の障がいなど）でしゃべれなくなったとしても、発話内容をテキストで打ち込むことで、自分の声でその内容を機械にしゃべらせることができるようになることである。その結果、QoL（Quality of Life）の向上にもつながり、皆ハッピーになるというわけである。ところが最近の展開をみるとそうでもないような気がしている。

音声合成技術の研究は、コンピュータの発展とともに進歩してきた。詳細な歴史の説明は専門書に譲るが（全体を俯瞰し、AI 音声合成技術までを含む教科書が見当たらないため、ウィキペディアの音声合成⁽³⁾を参照して頂きたい。）、れい明期の頃は機械方式で合成音声の実現を試み、人間の発話生成機構や機能をまねる形で検討されてきた。その後、ボコーダが発明され、波形接続・音声素片合成形式、統計的手法（HMM: Hidden Markov Model 音声合成）、そして深層学習ベース音声合成技術へと発展した。深層学習ベースと一くくりにしているが、波形生成モデル WaveNet やエンドツーエンド方式の音声合成器、ニューラルボコーダの登場など、その発展スピードは急激である。現在は、大規模音声発話データを活用して学習することで、自然で高品質の合成音声を提供できるようになり、図 2 に示すような応用展開に至っている。

最近の深層学習ベースの音声合成技術では、本人の大規模音声発話データがあれば、本人そっくりの自然な音



図2 深層学習ベース音声合成技術の応用先

声を合成できるところまで来た。現在はそれを、本人の少数音声発話データから実現できるところまで競争が激化しているところである。その結果、本人のデジタル分身を作る技術（例えば、小池百合子都知事の広報キャラクター、AI ゆりこ 2.0⁽⁴⁾）やサイバー空間でのアバター音声合成、更には故人の声の復活（AI 故人⁽⁵⁾）という話にまで展開されている。

このような展開が今後どこまで広がるのか予想もつかないが、一つだけ言えることは、これらの技術が悪用されることにより、なりすましといった社会問題を増しかねないことである。今後は、倫理観をもってこれらの技術を使わなければならないのかもしれない。

3 なりすまし音声の脅威

2015年9月、音声科学のトップカンファレンスの一つである Interspeech 2015 のスペシャルセッションにおいて、ASVspoof チャレンジ⁽⁶⁾ が初めて開催された。このチャレンジでは、図3のように、音声合成技術や音声変換技術による音声なりすまし、あるいは収録

音声（本人に同意なく盗聴された音声）と本物の声を判別するアルゴリズムの開発を通じて、なりすまし攻撃とその対策を独立に評価することを狙いとした。これまでに5回（ASVspoof2015, ASVspoof2017, ASVspoof2019, ASVspoof2021, ASVspoof2024）開催され、なりすまし音声対応やシステムの攻撃耐性の強化が検討されてきた。

ASVspoof2015 で最も驚いたのは、なりすまし音声の検出性能にうんぬんする前に、話者認証システムが当時の合成音声によって突破されたことであった。これは過度に評価されたこともあったかもしれないが、音声合成によるなりすまし攻撃が非常に脅威と感じた最初のきっかけでもあった。当然ながら回を増すごとに、合成音声の品質も向上し、なりすまし音声も巧妙化されている印象を持った。

このようなチャレンジにより、学術的にはなりすまし攻撃やその脅威への対策は練られているものの、現実的には下記のようななりすまし音声による詐欺事件やオンライン選挙活動被害の実例も起こっている。

- ・ AI を悪用した音声詐欺が世界で増加⁽⁷⁾

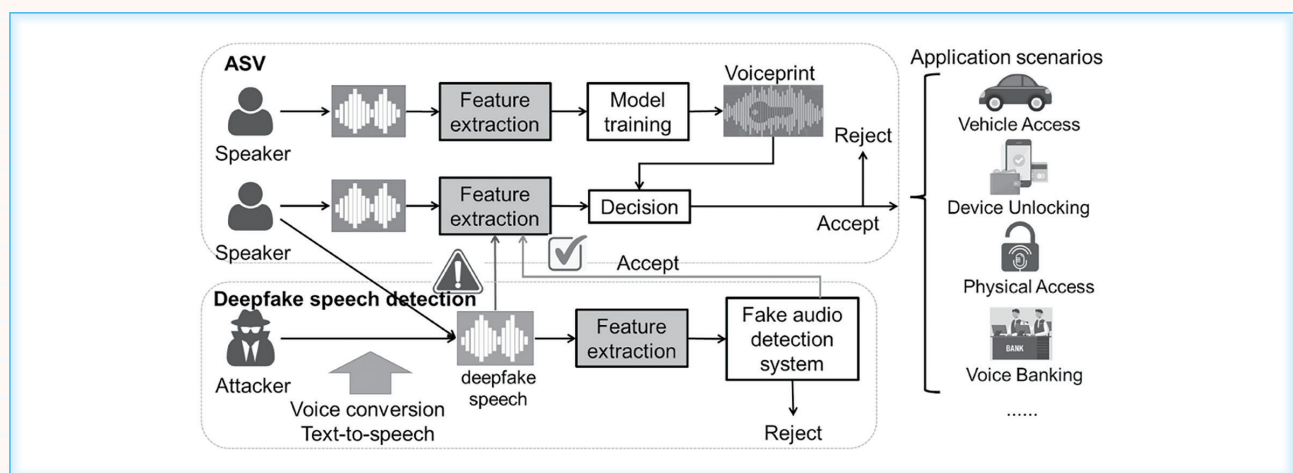


図3 なりすまし音声の対策

- ・「AI 音声を詐欺に悪用 3 秒の素材で親族らになりすまし」⁽⁸⁾
- ・前澤友作氏や堀江貴文氏に（声まで）なりすました詐欺広告⁽⁹⁾
- ・ディープフェイクボイスによるなりすまし（AI 音声によるなりすまし詐欺）⁽¹⁰⁾
- ・「AI で音声など無断生成 声優らがルール作りを訴え啓発動画」⁽¹¹⁾
- ・「生成 AI が『オレオレ詐欺』を助長？ 技術革新が犯罪を高度に」⁽¹²⁾
- ・「バイデン大統領の AI『なりすまし音声』、男を起訴 罰金 9 億円も」⁽¹³⁾

これらは氷山の一角に過ぎず、現実的にはもっと多くの事件が起こっている可能性がある。また、今後はもっと複雑で大きな社会問題を引き起こす可能性もある。

4 ディープフェイク音声への対応

4.1 チャレンジ

ディープフェイク音声検出に限定した最初のチャレンジは ADD 2022 (Audio Deepfake Synthesis Detection 2022) である⁽¹⁴⁾。これは、IEEE ICASSP 2022 信号処理グランドチャレンジの一環として開催された。

ADD 2022 では、人間の音声パターンを正確に模倣できるディープフェイク生成技術の高度化に焦点を当てている。これにより、検出システムにとって本物の音声とディープフェイク音声の区別が非常に困難なものになっている。第 2 回チャレンジ (ADD 2023)⁽¹⁵⁾ も開催されており、世界中の研究者がディープフェイク音声検出のための革新的技術の開発を目指している*。

ディープフェイク音声検出に関するほかの調査報告

として、Chen ら⁽¹⁶⁾ や Wang ら⁽¹⁷⁾ の報告がある。Chen らは、新しい音声合成方法が絶えず登場しているため、検出モデルが様々なディープフェイク音声に共通するパターンを特定しながら、新しい音声合成技術によってもたらされる変動に、耐性を持つことが難しくなっていることを指摘している。Wang らは、ディープフェイクの制作者がその検出を回避するために敵対的攻撃を使用する可能性があり、ディープフェイク音声検出が雑音に対して頑健でなければならないと指摘している。

Yi らは、ADD 2023 の調査を通じて、ディープフェイクスピーチ検出のためのラベル付きデータセットの入手が困難であり、真正サンプルとディープフェイクサンプルの分布が不均衡となり、ディープフェイク音声の検出性能が最適化されない可能性があることを示した⁽¹⁸⁾。また、ディープフェイク合成音声検出モデルでは、短い発話箇所でも正確な予測を行うため、より多くのコンテキスト情報を必要とする。そのため、これらの知見はディープフェイク音声の制作者による悪用につながる可能性がある。このような課題に対処するためには、ディープフェイク合成音声検出の継続的な研究開発が必要である。

4.2 データベース

ディープフェイク音声検出のための主要なデータベースは、図 4 に示すように、ASVspoof 2019/2021 と ADD 2022/2023 である。

ASVspoof 2019 は、なりすまし対策の比較評価プ

* ASVspoof は様々な種類のなりすましを対象にしているが、ADD は音声合成によるなりすましに限定している。

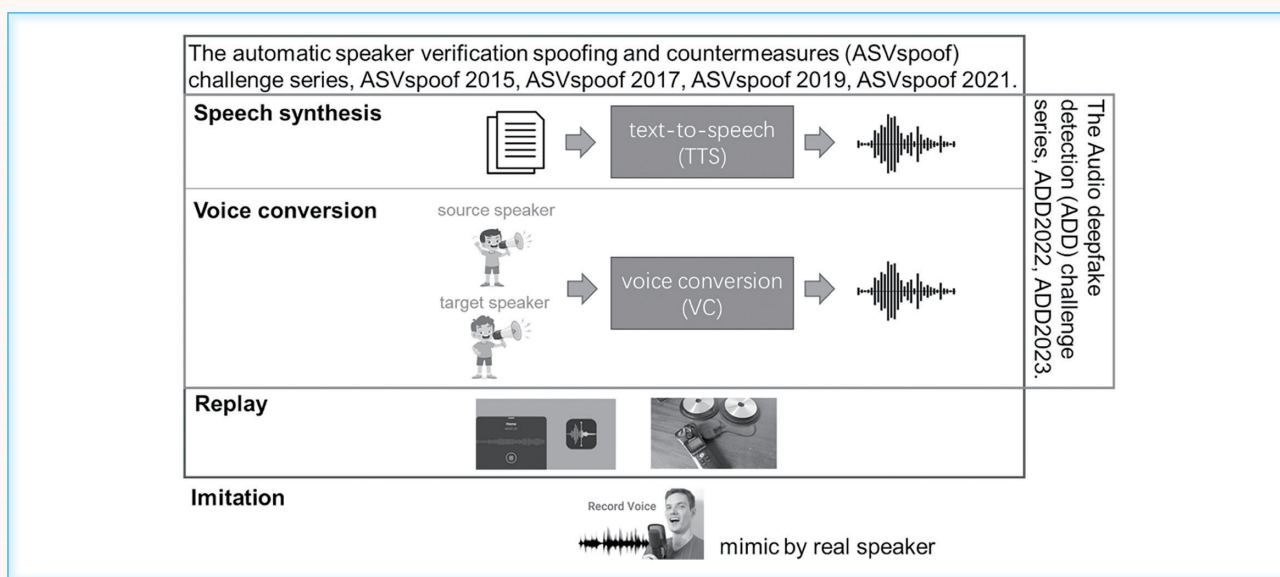


図 4 ディープフェイク音声データベース

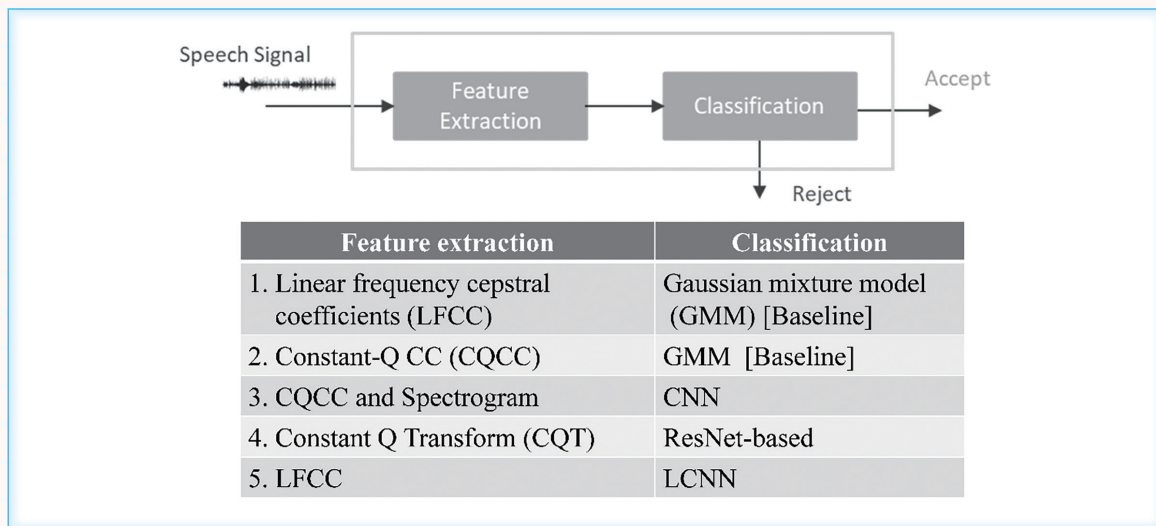


図5 代表的なディープフェイク音声検出の概要

ラットホームを作成するために使用されたものであり、正規の音声信号と偽装された音声信号の標準化されたデータセットが含まれている⁽¹⁹⁾。ASVspoof 2019は、なりすましの種類を論理アクセス（音声変換及びテキスト音声合成）と物理アクセス（様々な環境におけるリプレイ攻撃）の二つのシナリオに再概念化されている^{(19), (20)}。

ASVspoof 2021には、オンライン音声データに対するなりすまし音声検出の頑健性を評価するために、ディープフェイク音声という別のシナリオが追加されている⁽³⁾。

ADD データセットは、ディープフェイク音声の検出と分析に使用されている。ADD 2022には、低品質フェイク音声検出 (LF)、部分的フェイク音声検出 (PF)、音声フェイクゲーム (FG) の三つのトラックがある。LF 音声検出は、実世界の雑音の中で完全に偽の発話を識別することに重点を置いている。PF 音声検出は、部分的に偽の音声を識別することを対象とする。FG 音声検出は、生成と検出の二つのタスクから成る敵対的ゲームである⁽¹⁴⁾。

ADD 2023では、三つのサブ課題（FG、操作領域の位置、ディープフェイクアルゴリズムの認識）を通じて、部分的な偽音声の区間と偽音声の発生源を特定することを課題としている⁽¹⁵⁾。

4.3 最新の方法

ディープフェイク音声検出で利用される特徴量は、短時間・長時間特徴量、プロソディの特徴量、及び最先端の検出技術で利用されるディープ特徴量に分類される。

音声信号の短時間フーリエ変換 (STFT) から得られる短時間スペクトル特徴には、対数振幅スペクトルや線形予測符号化など、大きさや位相に基づく特徴がある。

定Q変換 (CQT)、ヒルベルト変換、ウェーブレット変換などの長時間スペクトル特徴は、時間周波数パターンを分析するために使用される⁽¹⁸⁾。特に、両スペクトル特徴において、ケプストラムベースの特徴として、固有周波数ケプストラム係数 (LFCC)、メル周波数ケプストラム係数 (MFCC)、CQT ベースのケプストラム係数 (CQCC) が使用されている。

韻律の特徴には、基本周波数 (F0)、継続時間、パワー変化、話速など、より長い音声区間が含まれる。このような手作業で作成された特徴量はロバストであるが、バイアスに悩まされることもある。

ディープニューラルネットワーク (DNN) を介して学習されるディープ特徴は、学習可能なスペクトル、教師あり埋込み、及び自己教師あり埋込み特徴に分類される⁽¹⁸⁾。広く使用されている DNN には、Wav2vec や HuBERT がある。Zaman ら⁽²¹⁾ はこれらの要素を組み合わせ、オーディオ分類で一般的に使用される深層学習アーキテクチャによって既存のモデルを分類している。更に、スタンドアロンの深層学習モデルは、サポートベクターマシン (SVM) や K 近傍法 (KNN) といった従来の分類器と組み合わせることも可能である。

4.4 結果と限界

上述した代表的なディープフェイク音声検出の概要を図5に示す。ADD 2022/2023 チャレンジで提案された数多くの検出器の性能評価については、トラックごとに評価されランク付けされている。評価尺度は原則、等価エラー率 (EER) が利用され、この値が限りなく 0 に近づくことを狙いとしている。いずれも高い検出性能を達成しているところがあるが、十分に満足のものではなく、それぞれのトラックで個別に今後の課題が述べられている状況である^{(14), (15)}。

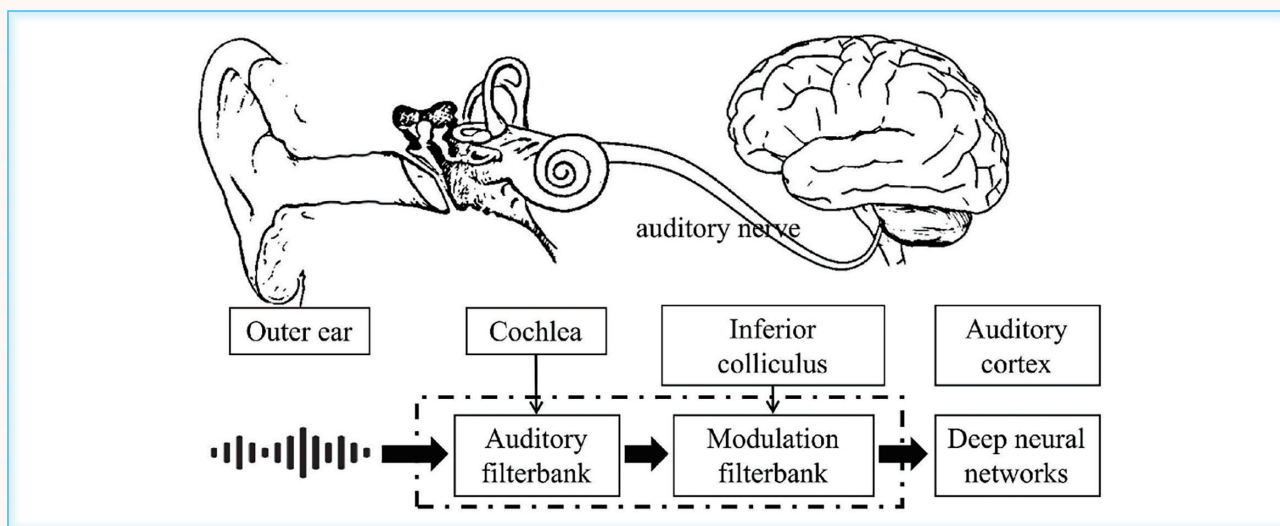


図 6 聴覚のスペクトル変調・時間変調分析の概要

ディープフェイク音声検出において多くの特徴抽出技術法が実装されているが、まだ幾つかの欠点が残されている。従来の音響特徴のほとんどは、話者の個人性や言語情報などの一般的な情報を抽出するように設計されているため、真正音声と音声合成で作られた偽音声を区別する識別力が限られている。更に、フロントエンドの特徴抽出手法は、入力音声の雑音（ノイズ）やばらつきの影響を受けやすく、特に録音条件や背景雑音が変化する実世界のデータを扱う場合、性能が低下する可能性がある。

これらの特徴のほとんどは、本物と偽物の音声の違いを視覚化したり、なぜそのような違いが生じるのかを説明したりするために使用できるものにはなっていない。また、ADD では合成音声＝ディープフェイク音声と限定しているが、ASVspoof では合成音声以外のフェイクを対象にしていることにも注意しておきたい。

5 人間の聴知覚メカニズムに基づく方法

筆者らのグループでは、上述の問題から、本物と偽物を判別する仕組みまで言及できるように、図 6 に示すメカニズムから説明可能な人間の聴知覚メカニズムに基づくディープフェイク検出法を検討した。

- ・聴覚フィルタバンクを利用した音の時間周波数分析とそのスペクトル変調・時間変調（STM）表現を利用したディープフェイク音声検出法⁽²²⁾
- ・音声のプロソディに関わる基本周波数の時間変動でみられるジッター・シマーを音響特徴としたディープフェイク音声検出法⁽²³⁾
- ・聴知覚の主な違いとして音色評価に関わる特徴（シャープネス、ラフネス、ブライトネス、ハードネスなど 8 種類）を利用したディープフェイク音

声検出法⁽²⁴⁾

- ・フェイク音声を病理音声の一つと解釈した場合の知覚評価に関わる特徴（ジッター・シマー、声帯音源対雑音比など）を利用したディープフェイク音声検出法⁽²⁵⁾

いずれの方法も ADD 2022/2023 や ASVspoof 2019/2021 のデータベースを対象に EER で評価した。検出性能だけみると、いずれの方法もこれらのチャレンジで提案された最新の方法の検出精度には負けてしまうが、聴知覚に関する音響特徴の段階で、本物と偽物の違いをおおむね説明できるという大きな利点を有する。これらの音響特徴の次元は深層学習をベースとする検出法の特徴の次元に比べて大幅に低くなることから深層学習ベースの識別器に整合し難いところも問題である。

一方で、ADD や ASVspoof では、ディープフェイク音声、なりすまし音声を対象に議論していたが、両方で考慮されていない、なりすまし音声もある。それは、人間による「ものまね音声」（Imitated speech）である。我々は、ものまね音声をどれだけ人間が正確に弁別できるか、22 人の大学院生を対象に 20 人の話者を対象とするものまね音声検出実験を行った。ここでは、実験参加者は 20 人の話者を学習し、その話者識別率が 90 % を超えるまで学習を行わせた。2 人がこの作業でギブアップし、話者識別率 90 % を超えた 20 人の学生がものまね音声検出実験に進んだ。その結果、検出精度は 70.1 % であった⁽²⁶⁾。

この結果に対し、典型的なディープフェイク検出器（特徴としてメルスペクトルを利用）では、検出精度が 51 % であったのに対し、聴知覚に関係する音色指標を利用したところ検出精度が 62 % であった。人間の検出能力にはまだ追い付いていないが、前述したように聴知覚メカニズムを考慮する検出方法の優位性を確認できる。

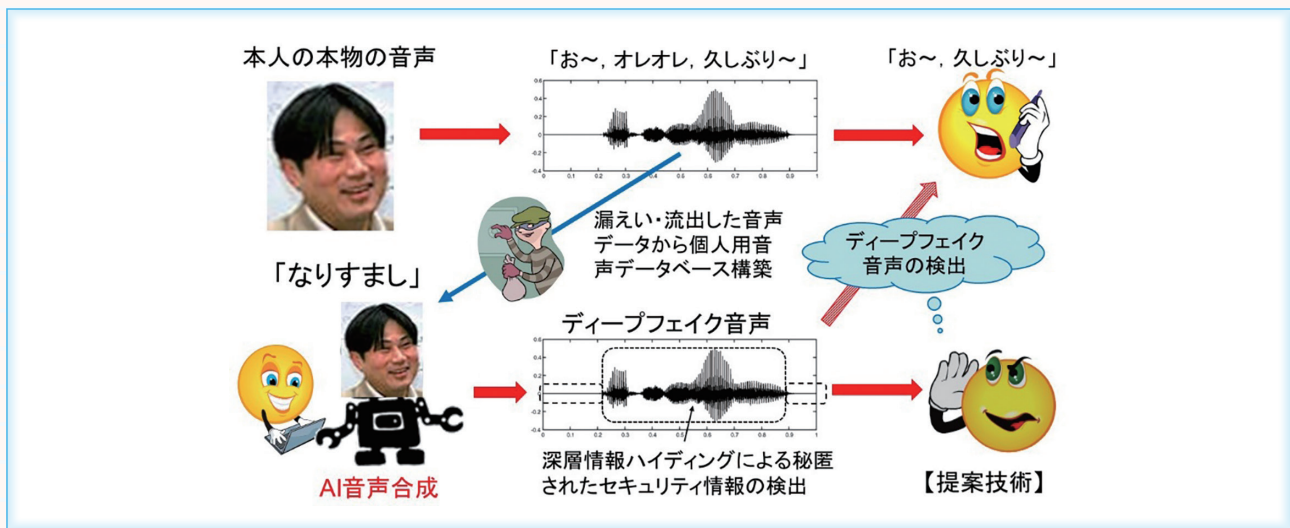


図7 ディープフェイク合成音声の検出

6 今後の展開

前述したように ADD 2022/2023 では、「深層学習ベースの音声合成で作成されたもの＝ディープフェイク音声」として検出対象とした。ASVspoof は音声合成のほか、音声変換や収録音声（リプレイ攻撃）をなりすまし音声の対象とした。いずれも重要な課題を検討するためのシナリオに沿ったものである。しかし、この方針でいくと、元々、利用目的のあった音声合成が全て「悪」として捉えられてしまうことになる。

筆者がこれまでに力を入れて取り組んできたマルチメディアセキュリティの一つである「音声情報ハイディング技術」の立場からすると、むしろ安全な合成音声を利用するならば、「合成音声マーク」のような安全装置を合成音声に秘匿しておくことがよいのではないかと考える。例えば、図7に示すように、ネットを流通するようなデジタル音声（あるいは合成音声）に事前に秘密情報を秘匿しておき、それが悪意ある操作を受けることで、秘密情報が壊され、それを検出器で確認することで改ざんの有無を確認できる。また、データの真正性を担保したい場合は、同様に秘密情報を秘匿しておき、それをもって正しい利用である宣言をすれば、ディープフェイク音声のような攻撃に対しては一定の防御策になり得るものと考ええる。

既にこのようなアプローチもみられるようで、深層学習ベースの音声合成器に知覚不可能で頑健な音声情報ハイディング技術を組み込むことが、今後のなりすまし音声に対する大きな防御策になるものと予想する。

7 おわりに

本稿では、ディープフェイク音声といった音声なりす

ましによる脅威を紹介し、その対策と課題を概説した。また、最新の研究成果を紹介するとともに、筆者の取り組みと現在の動向、残された課題を紹介した。

■ 文献（サイト閲覧日は2025年6月16日）

- (1) 鶴木祐史, “聴覚特性に基づいた音響情報ハイディング技術,” 信学FR誌, vol. 13, no. 4, pp. 284-293, April 2020.
- (2) J. Yamagishi, X. Wang, M. Todisco, M. Sahidullah, J. Patino, A. Nautsch, X. Liu, K. A. Lee, T. Kinnunen, N. Evans, and H. Delgado, “ASVspoof 2021: accelerating progress in spoofed and deepfake speech detection,” Proc. Workshop Automatic Speaker Verification and Spoofing Countermeasures Challenge, Sept. 2021.
- (3) <https://ja.wikipedia.org/wiki/%E9%9F%B3%E5%A3%B0%E5%90%88%E6%88%90>
- (4) 毎日新聞, “小池知事そっくり「AI ゆりこ 2.0」新動画公開 11カ月ぶり更新,” June 1, 2025. <https://mainichi.jp/articles/20250530/k00/00m/040/323000c>
- (5) 日経ビジネス, “AIで故人を再現、倫理的に許される?,” June 12, 2025. <https://business.nikkei.com/atcl/gen/19/00648/060900008/>
- (6) Automatic speaker verification and spoofing countermeasures challenge (ASVspoof). <https://www.asvspoof.org/>
- (7) マカフィー PR Times, “AI（人工知能）を悪用した音声詐欺が世界で増加中,” May 17, 2013. <https://prtimes.jp/main/html/rd/p/000000032.000033447.html>
- (8) 日本経済新聞, “AI 音声詐欺に悪用 3秒の素材で親族らになりすまし,” Sept. 11, 2023. <https://www.nikkei.com/article/DGXZQOUE104850Q3A710C2000000/>
- (9) FNN プライムオンライン, “動画と声で「堀江貴文」「前澤友作」かたる投資勧誘,” April 1, 2024. <https://www.fnn.jp/articles/-/685739?display=full>
- (10) CNN, “AI生成のクローン音声使ったなりすまし詐欺,” Sept. 19, 2024. <https://www.cnn.co.jp/tech/35224072.html>

- (11) NHK, “AIで音声など無断生成 声優らがルール作りを訴え啓発動画,” Oct. 21, 2024. <https://www3.nhk.or.jp/news/html/20241021/k10014615291000.html>
- (12) 日経BOOK PLUS, “生成AIが「オレオレ詐欺」を助長? 技術革新が犯罪を高度に,” Jan. 22. <https://bookplus.nikkei.com/atcl/column/011400459/011400002/>
- (13) 朝日新聞, “バイデン大統領のAI「なりすまし音声」、男を起訴 罰金9億円も,” May 24, 2025. <https://www.asahi.com/articles/ASS5S03CSS5SBQBQ0GLM.html>
- (14) J. Yi, R. Fu, J. Tao, S. Nie, H. Ma, C. Wang, T. Wang, Z. Tian, Y. Bai, C. Fan, S. Liang, S. Wang, S. Zhang, X. Yan, L. Xu, Z. Wen, H. Li, Z. Lian, and B. Liu, “ADD 2022: the first audio deep synthesis detection challenge,” Proc. ICASSP2022, pp. 9216–9220, Feb. 2022.
- (15) J. Yi, J. Tao, R. Fu, X. Yan, C. Wang, T. Wang, C. Y. Zhang, X. Zhang, Y. Zhao, Y. Ren, L. Xu, J. Zhou, H. Gu, Z. Wen, S. Liang, Z. Lian, S. Nie, and H. Li, “ADD 2023: the second audio deepfake detection challenge,” Proc. IJCAI2023 Workshop on Deepfake Audio Detection and Analysis, pp. 125–130, May 2023.
- (16) T. Chen, A. Kumar, P. Nagarsheth, G. Sivaraman, and E. Houry, “Generalization of audio deepfake detection,” Proc. Odyssey, pp. 132–137, Nov. 2020.
- (17) R. Wang, F. J-Xu, Y. Huang, and Q. Guo, “Deepsonar: Towards effective and robust detection of ai-synthesized fake voices,” Proc. 28th ACM international conf. multimedia, pp. 1207–1216, May 2020.
- (18) J. Yi, C. Wang, J. Tao, X. Zhang, C. Y. Zhang, and Y. Zhao, “Audio deepfake detection: A survey,” ArXiv Preprint, ArXiv:2308.14970, Aug. 2023.
- (19) M. Todisco, X. Wang, V. Vestman, M. Sahidullah, H. Delgado, A. Nautsch, J. Yamagishi, N. Evans, T. Kinnunen, and K. A. Lee, “ASVspoof2019: Future horizons in spoofed and fake audio detection,” arXiv preprint arXiv:1904.05441, April 2019.
- (20) X. Wang, J. Yamagishi, M. Todisco, H. Delgado, et al., “ASVspoof2019: A large-scale public database of synthesized, converted and replayed speech,” Comput. Speech & Language, vol. 64, no. 2, p. 101114, May 2020.
- (21) K. Zaman, M. Sah, C. Direkoglu, and M. Unoki, “A survey of audio classification using deep learning,” IEEE Access, vol. 11, pp. 106620–106649, Sept. 2023.
- (22) H. Cheng, C. O. Mawalim, K. Li, L. Wang, and M. Unoki, “Analysis of spectro-temporal modulation representation for deep-fake speech detection,” Proc. APSIPA ASC 2023, pp. 1822–1829, Nov. 2023.
- (23) K. Li, X. Lu, M. Akagi, and M. Unoki, “Contributions of jitter and shimmer in the voice for fake audio detection,” IEEE Access, vol. 11, pp. 84689–84698, Aug. 2023.
- (24) A. Chaiwongyen, N. Songsriboonsit, S. Duangpummet, J. Karnjana, W. Kongprawechnon, and M. Unoki, “Contribution of timbre and shimmer features to deepfake speech detection,” Proc. APSIPA2022, pp. 97–103, Nov. 2022.
- (25) A. Chaiwongyen, s. Duangpummet, J. Karnjana, W. Kongprawechnon, and M. Unoki, “Potential of speech-pathological features for deepfake speech detection,” IEEE Access, vol. 12, pp. 121958–121970, Aug. 2024.
- (26) K. Zaman, I. J. A. M. Samiul, K. Li, Y. Uezu, S. Kidani, and M. Unoki, “Ability of human auditory perception to distinguish human imitated speech,” IEEE Access, vol. 13, pp. 6225–6236, Jan. 2025.

鵜木祐史 (正員:フェロー)

北陸先端大・先端科学技術研究科・教授, 生体機能・感覚研究センター長。専門は聴覚科学・音声科学・音信号処理。1999 北陸先端大・情報科学・博士後期課程了。博士(情報科学)。2023-2025 日本音響学会副会長。2025 EMM 研究会委員長。現在, 音声情報ハイディング技術を利用した音声なりすまし対策の課題に鋭意取り組んでいるところである。



暗号の安全性評価の重要性

國廣 昇 Noboru Kunihiro 筑波大学

1 あなたの暗号は安全ですか？

身の回りを見渡してみると、世の中には暗号があふれていることが分かる。インターネットバンキングは既に広く利用されており、オンラインストアによって、クレジットカードを用いた商取引が一般的になっている。これらのサービスを安全に利用するためには、当然、安全性が担保されていなければならない。しかし、広く認識されているとおり、我々の周りには多くの脅威があふれている。これらの脅威の詳細な内容については、情報処理推進機構（IPA）が毎年公表している「情報セキュリティ 10 大脅威」⁽¹⁾などを参照されたい。2025 年 6 月現在でも、証券会社のインターネット取引への不正アクセス・不正取引が問題になっており、それを受けて、多くのサービスで多要素認証の必須化などの対策が進んでいる。その際、その対策が本当に有効であるか、安全であるかの厳密な評価が必要となる。せっかく対策を施しても、安全でなければ、意味がない。たとえ高度な暗号を使って安全な通信路を設けたとしても、暗号とは関係ないところで安全性が破られることも多い。セキュリティ技術は、一番弱いところが狙われるため、穴を埋め

ることが重要である。そのような状況ではあるものの、セキュリティの基盤となる暗号技術がぜい弱であれば、その暗号技術によって立つセキュリティシステムもぜい弱なものとなる。セキュリティシステムの構築において、使用している暗号は「当然安全である」という前提で議論することになる。

ケルクロフスの原理というものが知られている。「攻撃者は仕組みを知っている」という前提で対策をすべきである、という原理である。そのため、暗号方式自体を隠すことにより安全性を担保しようとすることは、この原理の下では許容されない。

秘匿通信を考えてみよう（図 1）。ケルクロフスの原理の下では、暗号化及び復号のアルゴリズムを公開することになる。復号する権限を持つ者だけが所有する復号鍵のみを隠すことにより、安全性が保証されなくてはならない。この枠組みにおいては、暗号化鍵は必ずしも秘密にする必要はないことに注意されたい。復号鍵は秘密にしなければならないため、暗号化鍵と復号鍵が同一である場合には、暗号化鍵も秘密にしなければならない。そのため、暗号化鍵と復号鍵は、送信者と受信者の共通の秘密となる。この方式は、「共通鍵暗号」や「対称暗

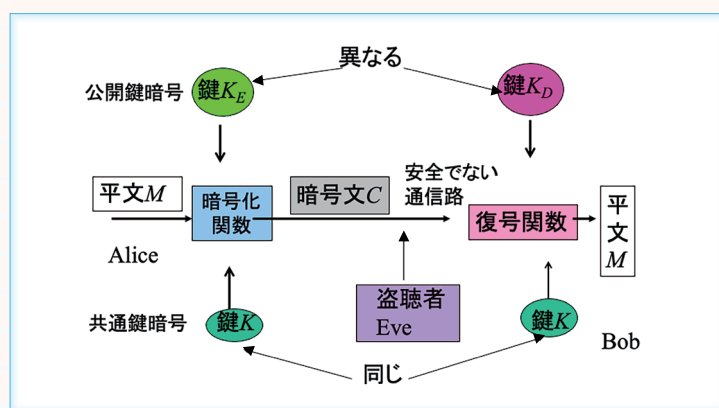


図 1 公開鍵暗号と共通鍵暗号

号」と呼ばれることが多い。暗号化鍵と復号鍵が異なる場合には、暗号化鍵を秘密にせず、公開しても問題ない。更に、利便性のために、積極的に暗号化鍵を公開することが多い。そのため、「公開鍵暗号」と呼ばれる。

暗号化鍵で暗号化し、復号鍵で復号処理をすると平文が復元されるため、暗号化鍵と復号鍵の間には強い関係がある。そのため、公開されている暗号化鍵を利用すると、その関係性を用いて復号鍵が分かってしまうかもしれない。公開鍵を公開しても復号鍵が分からないようにするために、何らかの数学的な困難な問題（RSA 暗号*においては素因数分解問題、ElGamal 暗号においては離散対数問題）の困難さを仮定し、その仮定の下で安全性が担保されることになる。ここで、適切な設定（RSA 暗号においては、2,048 bit の合成数を利用するなど）を行うことにより、現実的な時間では解読できないようにすることが重要である。適切な鍵長の設定については、CRYPTREC 暗号技術報告書⁽²⁾などを参照されたい。

2 暗号の安全性評価

暗号の安全性評価において、攻撃者は、公開されている情報や通信を盗聴することによって得られる情報は自由に使ってよい。まずは、このように受動的に得られる情報のみを使った攻撃を考える。

現在広く利用されている RSA 暗号⁽³⁾は素因数分解の困難さに安全性の根拠を置いている。素因数分解は、 $15=3\times 5$ というように、合成数が与えられたときに、素数の積に分解するものである。合成数が小さい場合には、2、3、5 と小さい順に素数で割り切れるかを確認することにより、容易に素因数分解を行うことが可能である。しかし、この単純な方法では、大きい合成数の場

合には、膨大な計算時間が必要である。それでは、もっと効率的なアルゴリズムではどうであろうか？ 素因数分解は、古くから研究されているが、現在のところ、素因数分解を行う多項式時間アルゴリズムは知られていない。その一方で、現在知られている最適なアルゴリズムは、指数関数時間を必要とせず、多項式時間と指数関数時間の間に属する準指数関数時間というクラスに属している。2025 年 6 月現在で、素因数分解された最も大きな RSA 型の合成数（同じサイズの二つの異なる素数の積）は、RSA-250 という 250 桁・829 bit の合成数である。図 2 に RSA-250 の素因数分解を示す。RSA 型の合成数の場合、これより大きい合成数は、依然、素因数分解はされていない。

この攻撃では、RSA 暗号を真正面から解読する場合を考えている。つまり、公開されている情報のみから暗号を解読する状況である。これ以降では、攻撃者は、公開されている情報だけでなく、様々な副次的な情報を入手できる状況を考え、「サイドチャネル攻撃」として総称される攻撃を取り上げる。この攻撃では、例えば、消費電力などの物理的な何らかの量を観測し、その情報を用いることによって、秘密情報を復元することがゴールとなる。

以降の説明のために、教科書的な RSA 暗号を簡単に説明する。

鍵生成：

Step1: n ビットの異なる素数 p, q を生成。 $N=pq$ を計算。

Step2: $ed\equiv 1 \pmod{(p-1)(q-1)}$ となる e, d を設定

暗号化鍵を (N, e) 、復号鍵を d とする。

暗号化：平文を m として、暗号文 $C=m^e \bmod N$ を計算する。

復号：暗号文を C として、平文 $m=C^d \bmod N$ を計算する。

* 提案者 3 人 Rivest, Shamir, Adleman の頭文字から名付けられた。

RSA-250=

```
21403246502407449612644230728393335630086147151447550177977549
20881418023447140136643345519095804679610992851872470914587687
39626192155736304745477052080511905649310668769159001975940569
3457452230589325976697471681738069364894699871578494975937497937
=
641352894770715802787901901705773890848250147429434472081168596
32024532344630238623598752668347708737661925585694639798853367
×
333720275949781565562260106053551142279407603447675546667845209
87023841729210037080257448673296881877565718986258036932062711
```

図 2 RSA-250 の素因数分解

RSA 暗号の復号処理は、二乗計算と乗算計算により、実現される。この計算を実現する最も基本的な計算法は、「バイナリー法」（若しくは「Square-and-Multiply 法」）と呼ばれる方法である。秘密のべき指数（RSA 暗号においては、秘密鍵 d ）を 2 進数展開した上で、上位ビットから値を読んでいき、

1. ビットが 1 であるときには、二乗演算（Square）をした上で乗算演算（Multiply）を行い、
2. ビットが 0 であるときには、二乗演算（Square）を行う、

ことにより行われる。

「単純電力解析」と呼ばれる攻撃を説明する。復号処理中の電力波形を観測することにより、二乗演算と乗算演算の区別ができる状況を考える。多くの場合、二乗演算と乗算演算は、異なる処理であるため、原理的にもこの二つの演算は区別可能である。この観測により、二乗演算と乗算演算がどの順番で行われたかの演算系列を知ることができる。更に、この演算系列を基に秘密鍵を復元することが可能である。これは、秘密鍵の各ビットが 0 であるのか、1 であるのかによって行う演算が異なること、そして、それを攻撃者が識別可能であることから攻撃に成功する⁽⁴⁾。

3 ダメな ATM の事例

暗号の安全性を評価する際に、仕様どおりであれば安全であるが、仕様どおりに実装をしないために、想定よりも弱くなってしまうことがある。このような実装を用いたために、秘密情報に依存した挙動が観測されることにより、ぜい弱性が生じることがある。多くの人になじみのある銀行 ATM での認証を基に、説明をしたい。

ATM では、通常キャッシュカードと 4 桁の暗証番号を用いた認証が行われる。（なお、キャッシュカードは所持情報、暗証番号は知識情報による認証であるため、多要素認証とみなすことができる。）キャッシュカードを ATM に挿入した上で、4 桁の暗証番号を入力し、暗証番号が事前に設定したものと一致すれば、正しい利用者であると確認され、現金の引出し等の処理が行われる。一致しない場合には、単に認証エラーであることを返す（図 3）。暗証番号を適切に設定した上で、たまたま、暗証番号を当てられてしまう確率は、 $1/10,000$ であり、十分小さい確率である。そのため、高々 10,000 回、平均でも 5,000 回程度の繰返しで暗証番号を当てることができる。多くの場合、3 回暗証番号の入力を間違えると、取引が停止されるため、適切に暗証番号が設定されていれば、3 回以内に暗証番号が当たる確率は極めて小さく、安全であるとみなすことができる。しか

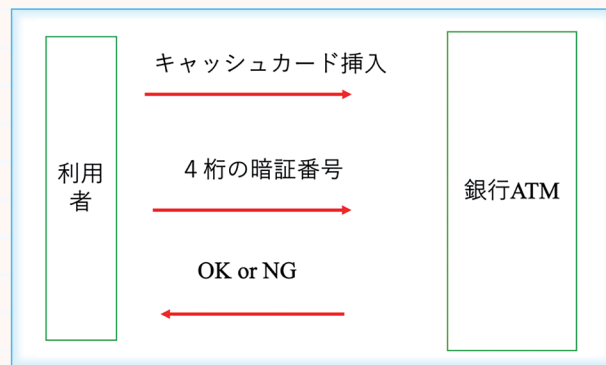


図 3 通常の銀行 ATM の認証

し、暗証番号を適切に設定していない場合（例えば、1234 などの簡単なものや誕生日に設定するなど。）は、当然、安全性は保証されない。

以下の二つの少し変わった（ダメな）ATM を考えてみる。いずれも、サイドチャネル攻撃とみなすことができる攻撃により、安全性が損なわれる。

一つ目は「おせっかい」な ATM である。この ATM は、暗証番号を間違えた場合、単に間違えていることを伝えるだけでなく、4 桁の暗証番号を入力し終えた段階で、何桁目を間違えているかのエラーメッセージを返してくれるものである。このような状況は考えにくいかもしれないが、利用者からの苦情（間違えた場合でも、ヒントを教えるべきであるなど。）や（間違った）利便性の向上を理由として、このようなシステムを導入してしまうということがあるかもしれない。この ATM の場合では、エラーメッセージを利用することで、高々 10 回の暗証番号の入力で認証に成功してしまう。正しい実装の場合は平均 5,000 回程度必要であったものが、格段に減少しており、ぜい弱性が生じている。この ATM の教訓としては、エラーが生じた（暗証番号が事前に設定したものと異なる）場合、エラーが生じている事実だけを伝えるべきであり、暗証番号のヒントとなり得る情報を与えてはならないということである。この ATM の例では、いかにもヒントになりそうな情報をエラーメッセージとして回答しているが、ヒントになりそうもないが、本来不要なエラーメッセージを回答してしまうために、ぜい弱性が生じた例がある。PKCS #1 v1.5 に対する Bleichenbacher によるミリオンメッセージ攻撃が、その代表例である。

二つ目の例は「せっかちな」ATM である。この ATM は、4 桁全ての暗証番号の入力を待たずに、暗証番号を間違えた段階で、エラーが生じたことを報告するものである。暗証番号を 1 桁でも間違えた段階で、既に、この試行は失敗することが確定しており、このタイミングでエラーを返しても、認証システムとしては表面上何も問題はない。それどころか、認証に要するトータ

ルの時間を考えると、この実装の方が有用であると考えて、このような実装をしてしまうことがあるかもしれない。この例では、明示的に、一つ目の例のようにどのようなエラーが生じたかを返しているわけではなく、単に、エラーが生じたことだけを返していることに注意されたい。しかし、どのタイミングでエラーが返されるかの情報を利用して、何桁目でエラーが生じたかの情報を得ることができる。この情報を用いることにより、5,000回よりもずっと少ない回数で暗証番号を当てることができる。まず、1桁目が0であると予想し、ここでエラーが出れば、0ではないことが確定する。次の試行では1桁目を1としてみる。エラーが生じなければ、1桁目の正しい値が確定する。次いで2桁目の入力をして、全ての桁を確定していく。この単純な方法により、高々37回の試行回数で暗証番号の復元に成功する。間違いが生じたタイミングでエラーを出力しなくても、何桁目でエラーが生じたかにより、エラーを出力するまでの時間がごく僅かに異なる場合も同様の攻撃が可能である。

ここで示した例は極端なものであり、このようなATMは当然のことながら存在しない。ここで示した攻撃は、秘密の情報を推測する際に、正解であるか不正解であるかの条件分岐により挙動が異なり、そのことを外部から観測可能であることを原因として成立する。つまり、安全性を担保するためには、秘密の情報に依存した情報を一切、漏らさないことが必要となる。

この種の攻撃を防ぐ技術として、「定数時間実装」が知られている。どのような入力（この場合は、暗証番号などの秘密情報）に対しても、計算時間が一定となるというものであり、(少なくとも計算時間からは、)何も情報が漏れず、安全性が担保されるというものである。

これまで説明してきたように暗号技術の安全性を考える場合には、様々な状況下での安全性を考慮する必要がある。安全性評価においては、使える道具は何でも使ってよい。これ以降では、RSA暗号の安全性評価において、単に素因数分解の困難さを評価するという教科書的な評価だけでなく、攻撃者にとって有利な状況下でのRSA暗号の安全性について考える。4.以降では、これまでに筆者が行ってきた誤り訂正符号、格子理論、量子アルゴリズムといった数理的な手法を用いた解析を紹介する。

具体的には、

1. RSA 秘密鍵の各ビットが漏えいする場合の安全性評価 (4.)
2. RSA 秘密鍵 d が小さいときの攻撃 (5.)
3. 量子計算機を用いた場合の RSA 暗号の安全性評価 (6.)

を詳しく説明する。

4

RSA 暗号の秘密鍵が誤り付きで漏えいする場合の攻撃

RSA 暗号の安全性は巨大な合成数の素因数分解の困難さに基づいているが、これは単に「素因数分解を経由して RSA 暗号を破ることは難しい」ということにすぎない。攻撃者にとって有利なヒントが与えられた場合に、どの程度安全性が低下するかの評価が重要となる。ここでは、秘密鍵の部分情報が得られたときに、鍵全体を復元する攻撃を考える。

何らかの物理的な攻撃により、RSA 暗号の秘密鍵 (p, q, d, d_p, d_q) に関連した値が観測される状況を考える。サイドチャネル情報として、正しい秘密鍵の値に小さなエラーが乗った情報が得られる状況である。このような状況として、「Coldboot 攻撃」⁽⁵⁾ などがある。ここでは、RSA 暗号の秘密鍵の各ビットが独立に漏えいする状況を想定する。まず、離散的な漏えいについて考える。これまでの研究では、秘密鍵の各ビットが独立に、

- ・確率 δ で消失するモデル⁽⁶⁾
- ・確率 ϵ でビット反転するモデル
- ・非対称な確率でビット反転するモデル
- ・確率 δ で消失しかつ確率 ϵ でビット反転するモデル⁽⁷⁾

などが検討されている。

より現実的な環境下での物理的な攻撃として、連続量のデータが得られるという状況も考えられている。観測値 y が、対応する正しい秘密鍵ビットに依存した確率分布に従うというモデルが提案されている^{(8), (9)}。具体的には、秘密鍵のビットが0のときには確率密度関数 $f_0(y)$ 、ビットが1のときには確率密度関数 $f_1(y)$ に従って、実数値が観測される状況を考えている。このような誤り付きの連続量のデータから、

(1) RSA 暗号の秘密鍵を復元する効率的なアルゴリズムを提案すること、

(2) 攻撃に成功するための条件を導出すること、

が研究のゴールとなる。攻撃の成功条件の記述として、文献 (8), (9) では、微分エントロピー (Differential Entropy) と カルバック・ライブラー情報量 (KL-divergence) などの連続量に関する情報量を測る概念を用いている。ここで、カルバック・ライブラー情報量は二つの確率密度関数の間の距離とみなすことができる量である。

文献 (8), (9) の成果を簡単に説明する。 f_0 と f_1 に関する事前知識の程度により、四つのタイプに分類して、それぞれに対して有効なアルゴリズムを提案している。これらのタイプに共通するフレームワークとして、Tree-Based Approach⁽⁶⁾ を用いている。このフレームワー

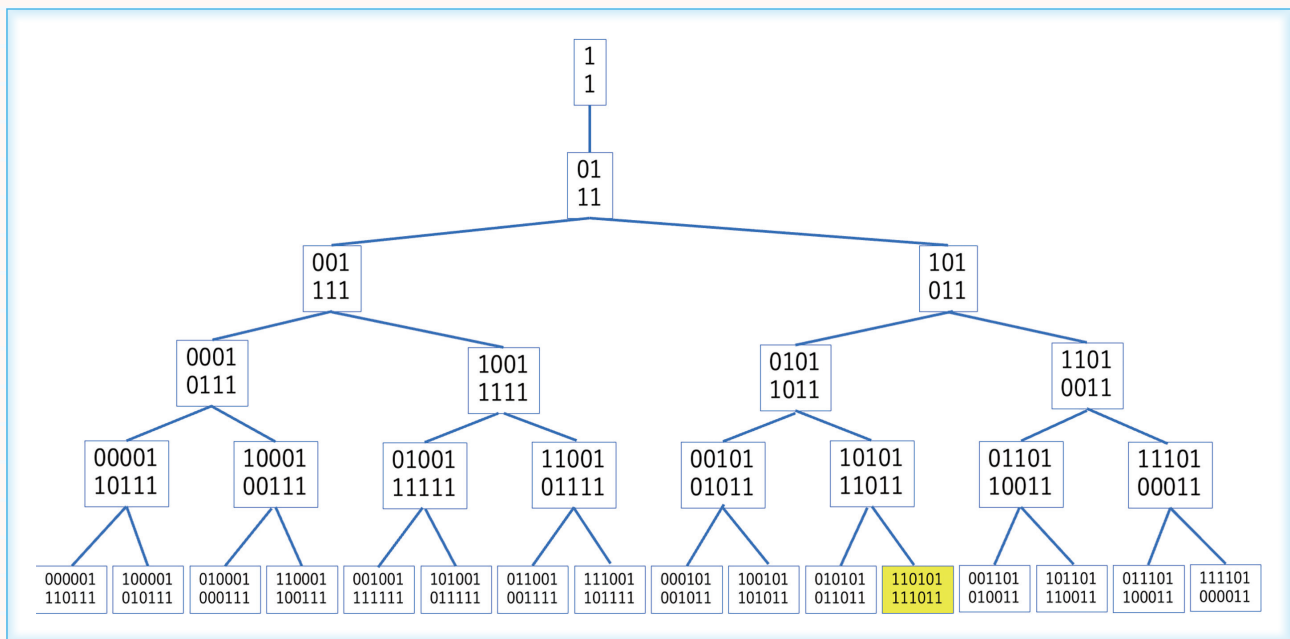


図4 Tree-Based Approach

($N=3127(=53 \times 59)$ であり、 p と q の情報だけを用いている。黄色い葉が正しい p (=110101)と q (=111011)に対応している。)

クでは、秘密鍵を $\text{slice}(i) := (p[i], q[i], d[i + \tau(k)], d_p[i + \tau(k_p)], d_q[i + \tau(k_q)])$ のように表現している。秘密鍵の $\text{slice}(i-1)$ までの部分情報を知っていると仮定すると、秘密鍵の各ビット間には五つの変数に対して四つの制約条件が存在するため、これにより二つの候補ビット列が生成される。Tree-Based Approach では、二分木(図4)を用いて、 $\text{slice}(i)$ を表現することになる。公開鍵が定まると二分木全体が一意に定まり、一つの葉が正しい秘密鍵に対応する。(図4中で、黄色くマークされている葉。)ここで、葉の総数は 2^{m^2} となる。鍵復元アルゴリズムでは、適切なルールを設定した上で、観測された系列と木により管理される候補系列に基づき、それぞれのノードを捨てるか残すかを決定している。

具体的なアルゴリズムは、Expansion(拡張) and Pruning(枝刈り)戦略を用いる。各フェーズで、 L 個のノードそれぞれに対して 2^L 個のノードを生成し、 $L \cdot 2^L$ 個のノードを得るExpansionフェーズと、その中からスコア関数の上位 L 個を残すPruningフェーズを $n/2t$ 回繰り返すことになる。

このアルゴリズムにおいて、スコア関数をどのように設定するかが重要である。1個の観測系列 y と多くの候補系列 x_i に対して、 $\arg\max \text{Score}(x_i, y)$ を計算することで、最ももらしい秘密鍵を推定する。

以下、四つの状況のうち三つについて簡単に整理する。

状況1: f_0 と f_1 が完全に分かっている場合

スコア関数として対数ゆう度比を用いる。このスコア関数がうまく機能する直感的な理由は、正しくない候補

x に対するスコアの期待値が0であるのに対し、正しい候補 x に対するスコアの期待値が正であるためである。

状況2: f_0 と f_1 の近似が分かっている場合

現実には正確な漏えい分布が分からないという問題に対処するため、まず分布 f_0 と f_1 を推定し、推定した分布を用いてスコア関数を設定することにする。成功条件は、正確な分布を知っている場合と比較して、推定のずれによる情報損が加わる形(KL Divergenceにより評価される)で悪化することになる。

状況4: f_0 と f_1 に関する情報が何もない場合

漏えい分布の知識を一切使用せずに計算可能な関数をスコア関数として用いる。これは、共通鍵暗号に対する差分電力解析で用いられる技術と類似している。

5 秘密鍵が小さいときの攻撃

RSA暗号では、秘密鍵 d を小さく設定することは実装上意味を持つ。復号処理は、 $C^d \bmod N$ で行われるため、 d が小さければ、復号時間を短くすることが可能である。

RSA暗号の秘密鍵が非常に小さいときには、容易に解読可能である。例えば、 d が1,000以下と設定されている場合には、高々1,000回の試行で解読が可能である。複数の暗号文が得られているときに、その復号結果が常に意味を持つ場合、正しい鍵であると判定できる。また、正しい d が与えられたときに、 $ed-1$ は、 $(p-1)(q-1)$ の倍数であることを利用して、 N の素因数分解が可能である。

逆に、秘密鍵 d が非常に大きい場合、公開鍵のみから d を求めることは素因数分解と同じ計算量が必要であることが知られている。そのため、秘密鍵 d の大きさが、その間に属している場合、つまり、 d がそれほど小さくなく、大きくもない場合の安全性に興味がある。

秘密鍵 d が $N^{0.25}$ よりも小さいときには、連分数展開を用いることにより、素因数分解できることが1990年にWienerにより提案されている。この d の限界は、1999年にBonehとDurfeeにより、 $N^{0.292}$ にまで拡張されている⁽¹⁰⁾。この攻撃は、格子理論に基づくアルゴリズムであり、多項式時間で動作する格子簡約アルゴリズム、LLL (Lenstra-Lenstra-Lovasz) アルゴリズムをサブルーチンとして用いている。

格子理論に関する問題として最も代表的な問題は、最短ベクトル問題である。この問題は、 m 本の線形独立なベクトルが与えられたときに、このベクトルの整数結合のうちで非自明な最も短いベクトルを求める問題である。(0ベクトルが自明な最短ベクトルである。) この問題は、次元が大きい場合には、現実的な計算時間で解くことができないことが知られている。最短ベクトルを求めることが困難であることを利用して、暗号の構成に用いられている。その一方で、最短ではないが、そこそこ短いベクトルを求めることは現実的な時間で可能である。暗号の解読問題を、そこそこ短いベクトルを求めることに帰着することによって一連の攻撃は設計されている。この分野全般の解説として、文献(11)などがある。

解読問題 (RSA 暗号の秘密鍵 p と q を求めること) は、Small Inverse Problem として定式化されている。RSA 暗号の鍵設定 $ed \equiv 1 \pmod{(p-1)(q-1)}$ は、ある自然数 k が存在して、 $ed-1 = k(p-1)(q-1)$ と記述できる。更に、 $k(N+1-(p+q))+1 \equiv 0 \pmod{e}$ と変形可能である。 $f(x,y) = x(A+y)+1$ とおくと、 $f(x,y) \equiv 0 \pmod{e}$ の解の一つは $(x,y) = (k, -(p+q))$ となる。細かい係数を無視すると、 $k < e^\delta$, $p+q < N^{1/2} \approx e^\alpha$ の範囲で解 $(k, -(p+q))$ を求める問題と考えることができる。 $p+q$ を求めることができれば、 $pq=N$ であるため、二次方程式 $x^2-(p+q)x+N=0$ と解くことによって、 p と q を求めること (素因数分解) が可能である。

多項式時間で Small Inverse Problem の解を求めることができるための解の上限を導出することにより、解読できるための条件を定めることが可能である。 $\alpha = 1/2$ の場合、 $\delta < 0.292$ のときに多項式時間で解けることが示されている。

RSA 暗号における低指数べき攻撃の限界 $d < N^{0.292}$ は、提案当時は、0.292という値は不自然であり、限界が更新されることが予想されていた。しかし、その提案から25年以上たつが、いまだ更新されていないという

のが現状である。筆者らは、0.292は、 $1-1/\sqrt{2}$ であり、ある意味自然であるという考えに基づき、適切に限定したクラスにおいては、この0.292が最適であることを示している⁽¹²⁾。もちろん、このクラスに属さないアルゴリズムが、この限界を破る可能性は残されている。

6

量子計算機を用いた場合の RSA 暗号の安全性評価

古典計算機を用いた場合、素因数分解は多項式時間で解くことはできないと強く信じられている。RSA 暗号において、現在標準的に用いられている公開鍵 N は2,048 bit に設定されているが、このアルゴリズムの計算量評価及び解読実験の結果を踏まえて設定されている。

量子 Turing 機械上では、RSA 暗号、だ円曲線暗号といった現在広く使われている公開鍵暗号方式を多項式時間で破ることが可能である。1994年に提案されたショアのアルゴリズム⁽¹³⁾により素因数分解や離散対数問題の効率的な解法が可能になるためである。

量子計算の歴史としては、1985年にDeutschによる量子 Turing 機械の導入をきっかけとし、1994年にSimonのアルゴリズム (周期関数の位数発見)、そしてShorのアルゴリズムが提案されている。更に、1996年にはGroverのアルゴリズム (探索問題) が提案されている。このアルゴリズムは、共通鍵暗号の秘密鍵探索やハッシュ関数の衝突発見に利用される。Shorのアルゴリズムは理論的な拡張が進み、可換群上での隠れ部分群問題 (素因数分解や離散対数問題を含むより広いクラスの問題) を解くことが可能であることが知られている。

Shorの素因数分解アルゴリズムの戦略は、ターゲットとする合成数 N に対して、 N と互いに素な自然数 a を選び、 $a^r \bmod N = 1$ となる自然数 r (位数) を求めることにある。 r を求めることができれば、古典的な計算により (一定の確率で) N の因数を多項式時間で見つけることが可能である。Shorのアルゴリズム全体の計算時間のオーダーは $\log N$ の多項式であることが知られているが、現代暗号に対する実際の影響を考えると、素因数分解に要する詳細なリソース評価が必要である。

素因数分解回路 (図5) の主要なステップは以下のとおりである。

Step 1: 初期状態 $|0\rangle^m \otimes |1\rangle$ を準備する。ここで $m = 2\log N + 1$ と設定する。

Step 2: 第1レジスタ (先頭 m -qubit) にアダマール変換を施し、均一な重ね合わせ状態を作る。

Step 3: べき乗剰余を適用し、重ね合わせの各状態に対して $|x\rangle \rightarrow |a^x \bmod N\rangle$ と変換する。

Step 4: 第1レジスタに逆量子フーリエ変換を作用さ

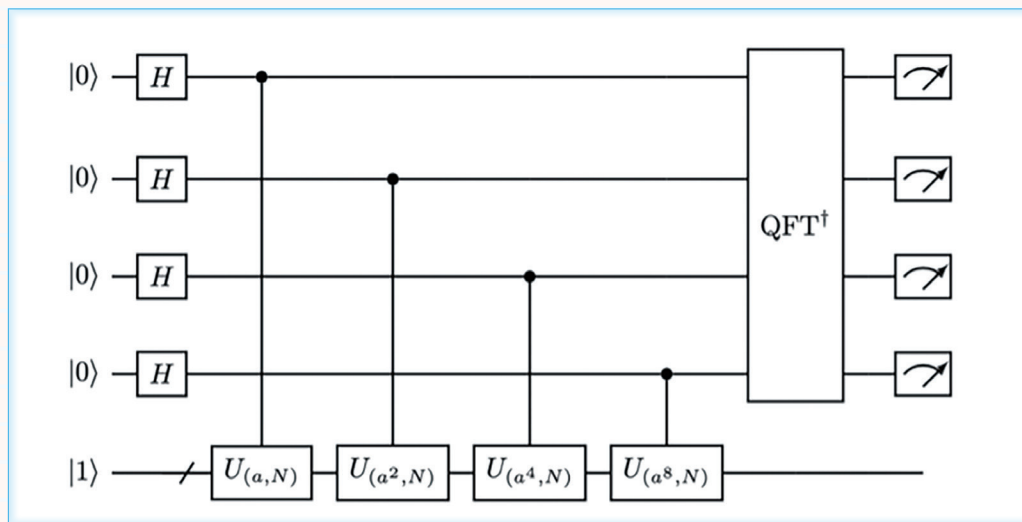


図5 Shorの素因数分解アルゴリズム

せる。

Step 5: 第1レジスタを観測する。

量子計算パートはここで終了である。量子計算回路構成において、 $|y\rangle \rightarrow |by \bmod N\rangle$ という、量子的に格納されている y という値を、古典的に定められた b 倍を行い、同じく古典的に定まっている値 N で割り算した余りを求める演算の実装が重要となる。

次は古典計算パートである。観測により得られた値を連分数展開することにより、 r を復元し、この r の値を用いて素因数分解を行う。

前述のように、Shor アルゴリズムは量子パートと古典パートに分かれる。量子パートの核となるべき乗剰余演算は、更に幾つかの小さい演算に分割され、標準的には、加算回路にまで分解される。

加算回路の構成法として、様々な回路構成が知られており、古典計算の足し算を可逆化したもの、一般化 Toffoli ゲートを用いたもの、量子フーリエ変換を用いた量子加算などの構成法が知られている。どの加算を用いるかによって、量子ビット数、回路サイズ、回路深さなどの量子的なリソースが異なる。全てに優れた方法は存在せず、少ない量子ビット数で動作する回路構成は、回路サイズ、回路深さが大きくなる傾向がある。

文献(14)では、量子誤りが一切ないという理想的な状況下でのリソース評価が与えられている。2,048 bit の合成数の素因数分解を行うには、4,000~6,000 程度の量子ビット、 10^{11} ~ 10^{13} 程度の量子ゲートが必要である。その後の研究の進展により、量子誤りがある状況下でのリソースの評価や、より効率的な量子回路の構成が提案されている。

量子計算機に対しても安全な耐量子計算機暗号の研究・開発が世界中で進んでいる。例えば、米国 NIST では、標準化プロジェクトが進んでおり、既に三つの標準

化文書が公開されている。日本でも、耐量子計算機暗号への移行に向けて準備が進められている。移行を円滑に進めるためにも、RSA 暗号など現在利用されている方式に対する安全性をできるだけ正確に理解することが必要となる。

7 まとめ

本稿では、主に RSA 暗号に対する様々な安全性評価について紹介した。特に、教科書的ではない攻撃手法について詳しく説明を行った。5., 6. における発展した内容を理解したい場合には、文献(15)などの書籍を参照されたい。本稿により、暗号の安全性評価の重要性について一層理解が深まることを期待する。

文献

- (1) 情報処理推進機構, “情報セキュリティ 10 大脅威.” <https://www.ipa.go.jp/security/10threats/index.html>
- (2) CRYPTREC 暗号技術評価委員会報告. https://www.cryptrec.go.jp/eval_cmte.html
- (3) R. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” Commun. ACM, vol. 21, no.2, pp. 120–126, 1978.
- (4) P. Kocher, “Differential power analysis,” Proc. CRYPTO99, pp. 388–397, Dec. 1999.
- (5) J. A. Halderman, S. D. Schoen, N. Heninger, W. Clarkson, W. Paul, J. A. Calandrino, A. J. Feldman, J. Appelbaum, and E. W. Felten, “Lest we remember: cold-boot attacks on encryption keys,” Proc. 17th USENIX Security Symposium, 2008.
- (6) N. Heninger and H. Shacham, “Reconstructing RSA private keys from random key bits,” Proc. CRYPTO2009, 2009.
- (7) N. Kunihiro, N. Shinohara, and T. Izu, “Recovering RSA secret keys from noisy key bits

- with erasures and errors,” IEICE Trans. Fundamentals, vol. E97-A, no.6, pp. 1273-1284, June 2014.
- (8) N. Kunihiro and J. Honda, “RSA meets DPA: recovering RSA secret keys from noisy analog data,” Proc. CHES2014, LNCS 8731, pp. 261-278, June 2014.
- (9) N. Kunihiro and Y. Takahashi, “Improved key recovery algorithms from noisy RSA secret keys with analog noise,” Proc. CT-RSA2017, LNCS 10159, pp. 328-343, Jan. 2017.
- (10) D. Boneh and G. Durfee, “Cryptanalysis of RSA with private key d less than $N^{0.292}$,” IEEE Trans. Inf. Theory, vol. 46, no. 4, pp. 1339-1349, July 2000.
- (11) 國廣 昇, “格子理論を用いた暗号解読の最近の研究動向,” 信学 FR 誌, vol. 5, no. 1, pp. 42-55, July 2011.
- (12) N. Kunihiro, N. Shinohara, and T. Izu, “A unified framework for small secret exponent attack on RSA,” IEICE Trans. Fundamentals, vol. E97-A, no. 6, pp. 1285-1295, June 2014.
- (13) P. Shor, “Algorithms for quantum computation: Discrete logarithms and factoring,” Proc. 35th

Annual Symposium on Foundations of Comput. Sci., pp. 124-134, Nov. 1994.

- (14) N. Kunihiro, “Exact analyses of computational time for factoring in quantum computers,” IEICE Trans. Fundamentals, vol. E88-A, no. 1, pp. 105-111, Jan. 2005.
- (15) 國廣 昇, 安田雅哉, 水木敬明, 高安 敦, 高島克幸, 米山一樹, 大原一真, 江村恵太, 暗号の理論と技術 量子時代のセキュリティ理解のために, 國廣 昇 (編), 講談社, 東京, 2024.

國廣 昇 (正員: フェロー)

筑波大システム情報系教授。1996 東大大学院工学系研究科修士課程了。同年、日本電信電話株式会社入社。2001 博士 (工学)。電通大、東大を経て、現職。一貫して、暗号理論、特に公開鍵暗号の安全性評価に従事。編著書に、「暗号の理論と技術 量子時代のセキュリティ理解のために」(講談社, 2024-05)、「データサイエンス はじめの一步」(講談社, 2024-08) などがある。



筑波大学 登 大遊 Daiyuu Nobori

1. 概要

SoftEther VPN は、オープンソースの複数プラットフォーム及び複数 VPN プロトコル対応 VPN ソフトウェアである。SoftEther VPN は、Windows, Linux, Mac, FreeBSD 及び Solaris 上で動作する。2025 年 11 月末日時点で、全世界の 1,000 万台以上のサーバにインストールされた実績を有する。ユーザのうち約 9 割は、海外である。ソフトウェア VPN として、それなりに人気がある。このようなシステムに密接に関連した通信ソフトウェアの開発は、正攻法では高額なコストが掛かり、限られた時間内で品質の高いコードを作るとは困難である。個人開発においては、コストを低減し必要な予算を確保すると同時に、自らの技術力を形成・蓄積する必要がある。また、個人利用可能な各種の資源を最大限に活用する必要がある。そして、良質なソフトウェアを作るためには、開発・試験環境を整える必要がある。特に、ネットワークに関連するシステムソフトウェアを開発する際には、自由な実験用ネットワークが必要である。また、特に重要な工夫は、いきなり目的ソフトウェアの開発を開始するのではなく、言わば「遊び目的」のサーバやシステム、ネットワークを組んでみて、それを使って楽しんでみることで技術力を自然に形成するとともに、その過程で必要なソフトウェアを作る、という流れで開発を行うことである。

本稿では、筆者の学生時代の「SoftEther VPN 開発物語」として、れい明期、特に最初のベータ版を開発して初公開するよりも以前に行った、問題解決の過程を述べる。また、2003 年当時は、こういうことは学生でなければむしろ困難であった。だが、近時は組織内の社会人でも、組織の資源、環境、設備を十分に活用して、同様の技術開発を行うことを許容・黙認する試行錯誤環境が、大企業や行政等の日本型組織にも形成され始めている。筆者

は、社会人がこれらを活用することによって様々な新たなシステムソフトウェアが開発され、よって日本の IT 技術立国が実現されると考えている。そこで、今後、日本の多組織で同時並行的に生じると予想する IT 技術革新現象についても述べる。

2. はじめに

SoftEther VPN (図 1, 2) は、多数の OS 上で多種の VPN プロトコルを統合的に利用でき、C 言語で 30 万行以上の規模を有する、それなりに内部構造が複雑で多機能な通信システムソフトウェアである^{(1), (2)}。このようなシステムソフトウェアの開発で、通常苦勞する課題は、次の 3 点である。

課題 (1)：OS に密接に関連するか、または OS の内部で組み込まれて動作するコード (システムコールの性質を十分に理解しないと設計や記述できないプログラムやカーネルモードのデバイスドライバ等) を実装する必要がある。OS の知識を必要とし、高い性能の実現やセキュリティ耐性の確立、不具合時のデバッグも大変である。これらに要する知識をどのようにして修得すればよいかが、問題となる。

課題 (2)：開発及び動作検証の段階においては、複数台のコンピュータと実験用のリアルなコンピュータネットワークを必要とする。これらの環境をどのようにして実現すればよいかが、問題となる。

課題 (3)：品質向上においては、机上負荷試験のみに頼ることなく、様々なユーザにリアルに利用してもらい、多様な環境と用途における動作テスト (バグのあぶり出し) が必要である。どのようにしてできるだけ変な用途、異様な負荷のある用途に利用してもらえばよいかが、問題となる。

これらの課題 (1), (2), (3) に含まれる各種問題は、⑦コストの問題と④技術の問題とに分けることができる。⑦コストの問題とは、開発環境等の物的資源と、設計・開発・テストに必要な専門能力等

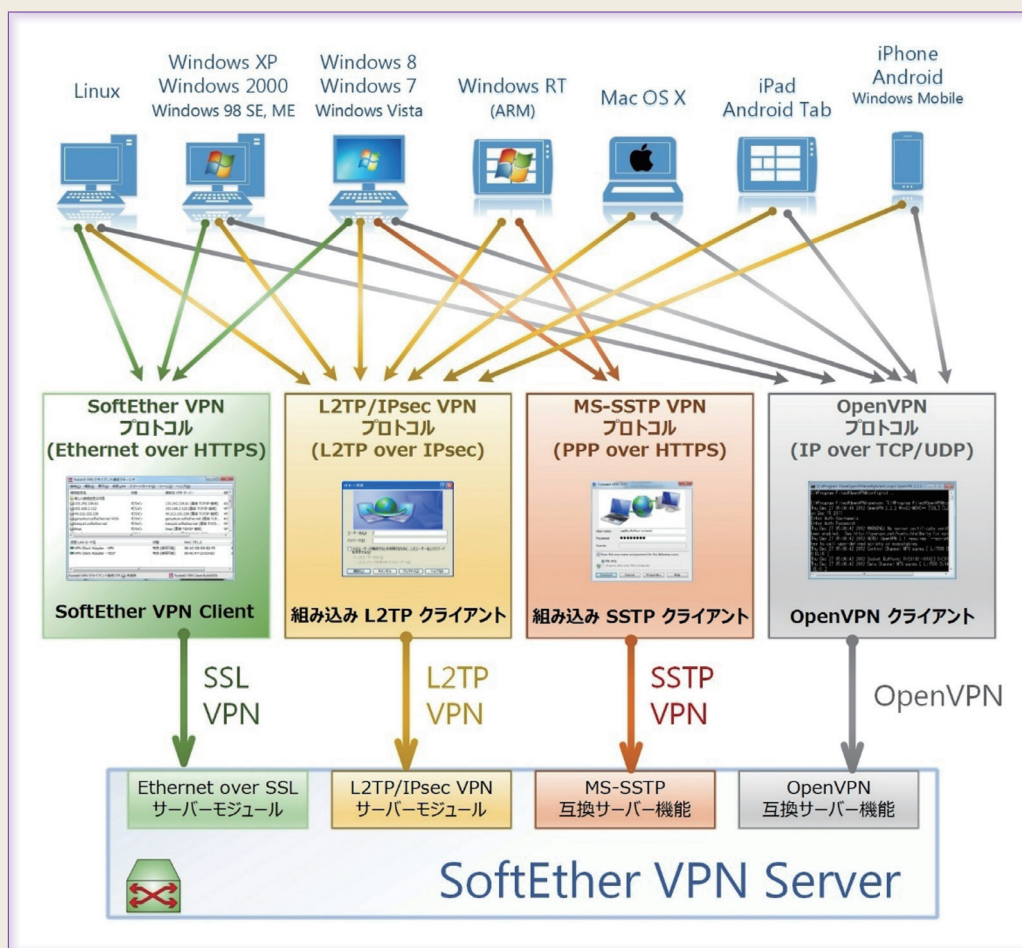


図 1 SoftEther VPN の複数 VPN プロトコルへの対応

の人的資源を、資本が乏しい個人レベルでどのように確保すればよいのか、という資源獲得の問題であり、そもそもの技術研究の最低限度のスタート地点に立つために必要なブートストラップ的問題である。④技術の問題とは、⑦の条件を充足したと仮定して、いまだ誰も作ったことがない水準の技術研究を、どのように行えばよいかという問題である。この二つの問題は、密接に関連している。「大企業の正攻法」では、⑦の問題をひとまず外注的な金銭投資で解決することが多いが、④は金銭では調達困難であるため、結局、④の壁に直面することとなる。そこで、⑦の段階から大企業の正攻法を避け、後述のように個人的かつ小規模な創造的工夫をする方が、④も同時に解決できるという利点が生じる場合がある。以下、筆者が行った手法を述べる。

3. ⑦コスト(資源)の問題の解決

通常の企業で見られるソフトウェア開発の正攻法では、課題(1)を解決するため、専門家にコンサルティングや開発委託を頼むことが多いが、そう

すると、膨大なコストが掛かる。また、課題(2)を解決するためには、本格的なラボ環境を構築する必要が生じ、やはり、膨大なコストが掛かる。課題(3)は複雑で広範なテスト環境を再現し、「テスター」と呼ばれる人員を雇用する必要がある、同様に、膨大なコストが掛かる。このように、ソフトウェアの開発は通常、膨大なコストが掛かる。通信システムソフトウェアは特に高度複雑であるため、そのコストは膨大となる。

このような通信システムソフトウェアの開発コストを捻出することは、大企業においては可能かもしれないが、個人では大変である。更に、SoftEther VPNを開発した2003年7月、筆者は同年4月に筑波大学(当時の第三学群情報科学類)に入学した直後(大学1年生)だったので、収入を有する通常の社会人よりも資金力に相当程度劣り、正攻法ではほとんど開発が不可能な状況に置かれていた。

この場合、まず、コストを引き下げて開発を完遂する工夫が必要となる。課題(1)については、専門家に頼んで仕事をしてもらうのではなく、やはり、自らが勉強をして技術・知識を身に付け、自ら

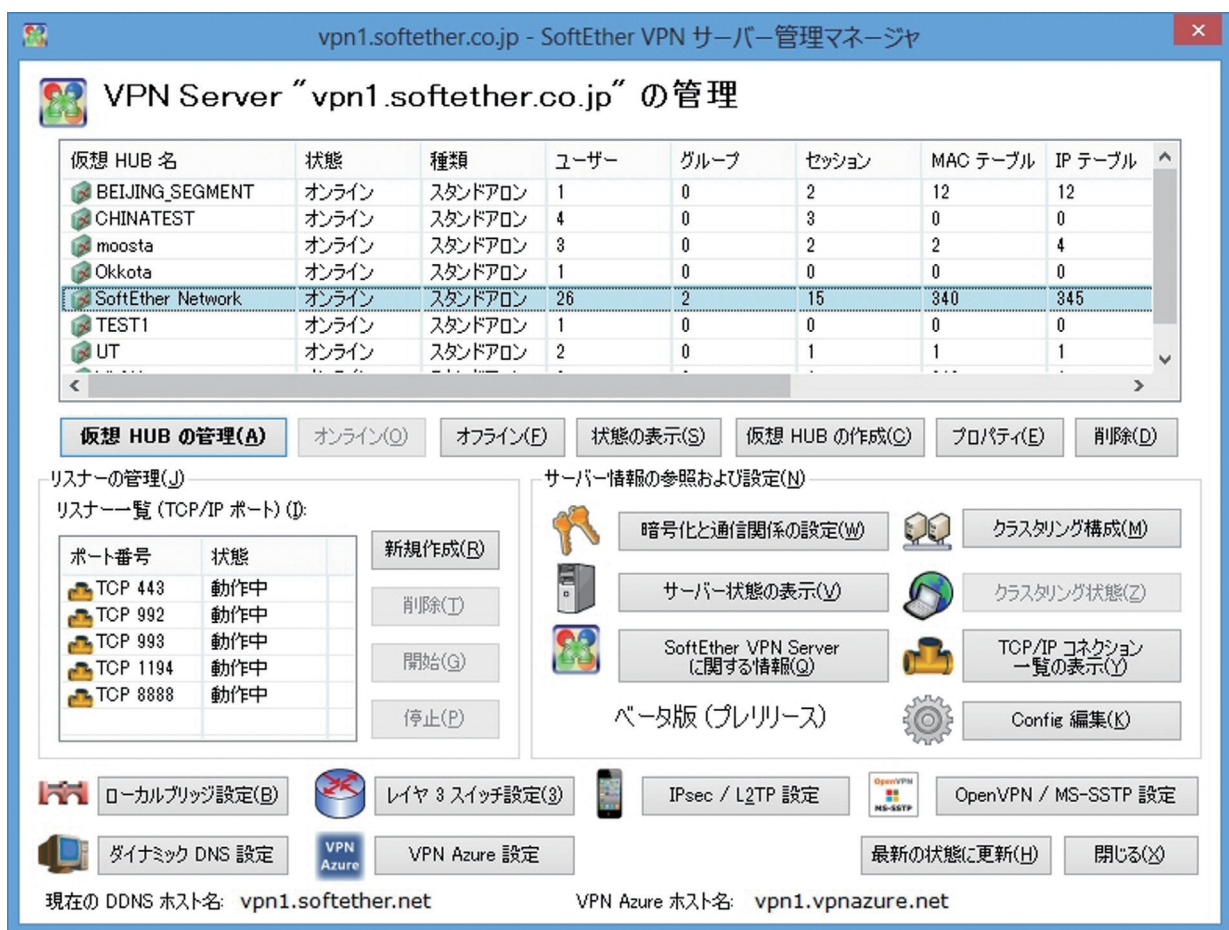


図2 SoftEther VPN Server の実行画面

が専門家となることで、解決する必要がある。この際、勉強には、ある程度の苦行が伴うが、コストを下げる必要性から人に頼めないの、自ら率先して行わざるを得ない状況となり、それなりに進捗するから、解決できる。課題(2)についても同様に、技術・知識を身に付けることにより、できるだけ安価な最低限度、かつ、効果的・快適に利用できる自分専用のラボ環境を作ることによって解決できる。課題(3)については、更なる一工夫が必要である。多様な環境を用意してテスターに依頼してテストにかけるのは、コストが掛かる。そうではなく、インターネット上で、「ベータテスター」と呼ばれる試作ソフトウェアの早期ユーザを募る工夫が有効である⁽³⁾。そうすれば、コストをほとんど掛けずに、様々なユーザの千差万別の環境で、豊富なバグを発見してもらうことができる。

上記のとおり、課題(1)、(2)においては、自らが勉強をして専門知識を身に付けるというフェーズを経ることで、コストを大幅に下げることができる。専門知識を習得し自らの技術水準を向上させる

ことはもちろん、複雑なソフトウェアを問題なく実装するためにも必要なことである。同時に、開発に掛けるコストを軽減させ、手持ちの資金力で開発を現実化するためにも、必要なことである。自ら技術力を高めれば、外注と比較して、開発コストが1桁も2桁も下がるのである。

このようにして、開発に必要なコストを下げるのができたとしても、そのコストは決してゼロにはならない。確かに、学生時代に課題(1)の解決のための独習を行う際は、大学授業の合間(または、最中?)に、様々な技術的試行錯誤を行う際は、自らの身体・頭脳を用いて行うので、目に見えるコストは余り掛からないかもしれない。簡単なアプリケーションであれば、ほとんど自らの身体・頭脳の消費コスト(すなわち、生活費)のみでプログラミングが可能である。だが、SoftEther VPNのような通信システムソフトウェアを作る場合は、課題(2)のハードウェアや通信環境が、それなりに必要となる。そのための資源を、個人レベルでどのように獲得するかが、問題となる。



図3 「IPA 未踏ソフト」の予算で自宅にデータセンターを
建立 (2003年7月)

そこで、頼ったのは、国と大学である。まず、国について述べる。経済産業省の施策で、当時、「未踏ソフトウェア創造事業」(「未踏ソフト」)という国主導のソフトウェア開発事業が存在していた。これは、現在も「未踏人材発掘・育成事業」として名称を変えて存在している。未踏ソフトは、国の予算で、IPA(独立行政法人情報処理推進機構)が運営していて、大学生等がターゲットであった。これに応募し、うまいことプレゼンをやって採択されると、最大で300万円(実際には、間接経費的な管理費用が途中で控除されるので、正味200万円くらいが活用できる)の委託契約を獲得できる。その予算の範囲内で、開発者は生活費に充ててもよいし、ハードウェア等の外部支払い経費に充ててもよい。筆者は、ありがたいことに未踏ソフトに採択され、委託契約金を用いて、多数のサーバやネットワークカード、Hub、ルータ、開発用のソフトウェアライセンス(MSDNというマイクロソフト社の開発用ライセンス)、グローバルIPアドレス8個×2本のぜいたくなインターネット接続回線などを調達できた。これらを自宅の学生アパートの部屋に並べるための金属棚も買ってもらった。これらの「官給品」のおかげで、自宅があたかも小規模なデータセンターのようになったのである(図3)。この自宅のデータセンター化は、極めて高い効用を発揮した。これについては、重要な点があるので、後に詳述する。

個人レベルでも応募することができ、100~200万円くらいの支援が受けられる予算は、日本のIT人材育成のために、大変重要である。2003年当時は、IPA未踏事業がほとんど唯一の広く知られた予



図4 筑波大学の地下にある光ファイバや電力水道を通す等のための全長14 kmもの巨大な地下通路

算であった。現代社会ではこのようなものは大変良いことであるとされており、国においては経済産業省以外にも、総務省等のほかの省庁に同様な人材育成予算がある。地方でも、また公益的な法人にも、そういう予算がある。インターネットで調べると、すぐに見つかるであろう。

次に、大学の活用について述べる。SoftEther VPNの開発が可能となったのは、筑波大学の人材(IT好事家=こうずか=的な教授陣)と環境によるものが大きい。まず、前述の国の未踏ソフト事業の話は、大学の先生からの助言で初めて知って応募したものである。いよいよ、SoftEther VPNの開発を開始した後、OSに関する概念的な知識や、プログラミングに関する技法などの入り口については、大学の「好事家先生」のところに、頻繁に通って習得した。当時、大学には大体午前3時ぐらいまで好事家先生が残っていて、コンピュータをいじって何かやっているという雰囲気であった。我々学生も、やはり好事家であるから、毎日、大体午後9時ぐらいから、大学の地下の「共同溝」と呼ばれる、光ファイバ等が大量に敷設されている「巨大地下帝国」(図4)をくまなく探検して、泥まみれになった後に、午前2時ぐらいに地上にまた戻ってくるのであるが、たいていは地下の巨大構造物や機械設備などを一べつした後、地上に戻ると、今度はOSに関する話が聞きたくなるので、好事家先生のところへ行くと、好事家先生はまだパソコンをいじっているの、OSの話が聞けるのである。この手法の繰り返しにより、一般的な大学授業で習うよりも、質的にも量的にも豊富な知識を、短期間で習得することが可能となった。



図5 筑波大学の「第2シリコンバレー」(古いコンピュータや周辺機器の廃棄場所)で、学生たちによる勉強用物品のリサイクルの様子。

そして、物質面においても、大学は必要な物品・資源の「穀倉宝庫」でもある。実のところ、IPA 未踏ソフトの予算があっても、その執行はそれなりに大変であり、事前に計画を立てていない物品を購入することは手間であった。確かに、国の予算は、大きなサーバ等の必ず必要になることがあらかじめ判明している物品の購入には利用しやすいが、通信システムソフトウェアの開発を進める際には、どうしても、臨機応変に消耗品レベルの細やかな部品等(ネットワークカード、スイッチング Hub、壊れてもよいハードディスクなど)を調達する必要もある。これらの物品は、中古品や廃棄されたジャンク品のような品質であってもよく、何とか使えばよいのであるが、国の予算でこれらの調達をしようとすると極めて煩雑となり現実的でない。

さて、幸運なことに、筑波大学には年に2回、夏と冬に「第2シリコンバレー」というような地区が形成される。第2シリコンバレーとは、筆者が勝手に名付けたものであるが、大学の工学系棟の「ビルの谷間」に各研究室から廃棄される古いコンピュータや周辺機器が積まれる、要するに「不要物品廃棄祭り」のことである。不要な機材群が「どんど焼き」のように山積みされるのである(図5)。これらは数日間野ざらし・雨ざらしにされ、放っておくとすぐに壊れて無価値になり、最後には大学が産廃業者にお金を払って引き取ってもらい、粉碎される運命にある。ここで、大学の昔からの伝統的慣習として、これらの廃棄される物品を、それらが雨、風にさらされて壊れて無価値になる前に、学生たちがいち早く、めばしいものを救護してリサイク

ルし、自らの技術的研鑽のために自由に活用するという「古き良き風習」が、いまだ現存しているのである。これについて、大学当局も、長年、慣行としてこのような学生による廃棄物品拾得をおおらかに認識・認容してきたのである。

筆者たちも大学1年生のときに、早速この廃棄祭りで多数の Intel や 3Com 社のネットワークカードやスイッチング Hub、ルータ、液晶モニタ、キーボード等を取得した。これらは個人でリサイクルする場合もあるし、複数人の学生たちが共同で多数ストックしていることもある。このようにして、必要なジャンク機材が、必要に応じてすぐに利用できる状態になっていた。通信システムソフトウェアのプログラミングやデバッグを進める上では、こういった細やかな物品を必要とするたびに、直ちにそれが手元で用意できるかどうか、命運を定める。いちいち秋葉原に買いに行ったり、あるいは納入業者に注文する事務的手間の時間的蓄積が、開発・デバッグ作業中の希少な我々の頭脳のメモリ・キャッシュからの忘却を引き起こさせ、大いなる損失を発生させる。これを予防するために必須の手元の豊富なジャンク機器ストックをほとんどコストを掛けず実現する場として、学生の視点に立つて適切に配慮がなされた、廃棄コンピュータ機材の山を提供する大学環境は、極めて重要である。

4. ①技術の問題の解決

通常の正攻法で、⑦コストの問題を解決したとしても、それは単にスタート地点に立てたというだけであって、未解決問題を解決する新たなソフトウェアを作ることは困難である。開発主体自らによる①技術的試行錯誤による能力形成が必要である。だが、いったん大企業の正攻法で⑦を解決してしまったならば、技術的側面において主体的試行錯誤をする必要がないという行動様式が身に付いてしまい、①がなかなか形成されないという問題がある。

筆者の場合、前述の方法で様々な多様な資源を組み合わせる方法で、⑦を解決したが、その際の試行錯誤と、⑦で入手した各種資源が中古・廃品等であるという「失敗許容性」も相まって、①技術習得が自然に進んでいった。以下、詳しく述べる。

SoftEther VPN の開発は、期間が限られており、迅速性が求められているプロジェクトであった。「IPA 未踏ソフト事業」の期間中に一応完成させな

なければならないが、実質的に9か月間しか時間がなかった。そのうち、プログラミングに費やせる期間は、せいぜい6か月間であった。そこで、通常、人が10年程度かけて習得するプロセスを、どのようにして6か月間で習得するかが、問題であった。

ここで、大企業的な正攻法では、机上での学習やプログラミングの研修やコンサルを受けたり、仕様書を書いて何らかのラボを構築してもらったり、きちんとした仕組みを構築してテストや品質向上のための業務フローを整えたりするであろう。だが、そのような正攻法の方法によって開発することができるシステムソフトウェアの水準は、低いレベルにとどまるのである。我々が開発しなければならないシステムソフトウェアは、作り方が誰もまだ分からないような部類のものであるから、机上や研修、コンサル等では、決して教えてもらうことかできない。(教えることができる者は存在しない。)どのようなラボ環境があれば開発可能かが、事前に不明であるということになる。この場合、計画主義的環境構築は、むしろ、開発者の能力を制約する。テストや品質向上を制度的に行うと、一見、品質が向上するように見えて管理的満足感が得られるが、それは形式的なものであり、実質的な品質向上は実現されない。多様な環境で思ってもみない用途をされたり、負荷を掛けられたりした際に、未発見の低品質な部分のバグが、馬脚を現わすことになる。大企業でも長期間掛かるような問題を、個人開発において同等の手法を採用したとして、到底、事業期間の9か月で解決することはできない。

そこで、筆者は、前述の課題(1)、(2)、(3)の技術的側面を実現するために、上記のような正攻法プロセスを採ることはしなかった。それは、正攻法プロセスを知らなかったためである。恐らく正攻法を知っていれば、つい、うっかりと、誤って、それに従ってしまい、SoftEther VPNなどは、絶対に9か月間では一応の完成すら覚つかなかったに相違ない。だが、幸運にも、筆者は上記のような一般的・企業のソフトウェア・エンジニアリング手法を全く知らなかったし、大学で会った先生方も、誰一人として、そういうことをやれ、と言ってこなかったのである。要するに自らも、大学の先生方も、皆、素人的だったのである。そこで何をすればよいかよく分からなかったから、筆者はひとまず、遊びのつもりで前述のIPA未踏ソフト事業の委託金で、自宅にデータセンターもどきのネットワーク環境を作る

ことにしたのである。

「自宅サーバや自宅データセンターの建立」というものは、2025年の現代においては、文化的な、大変立派な行為と認識されていると言ってよい。「自宅サーバ」とか「逸般の誤家庭」という検索キーワードで調べてみるとよい。これは、小さい頃にお世話になったプロバイダやクラウドサービス事業者からの独立を果たし、一人前の大人を自覚する、「元服」に匹敵する儀式である。そして、今も昔も、コンピュータやネットワークが異様にできる大学生たちの主要な技術力蓄積手段である。最近では、インターネットバックボーン(「BGP」と呼ばれる通信の仕組み)の設備を自宅に設置したり、クラウドサービスを自作したりする大学生や社会人好事家も増加している。だが、これは、自宅に物理的に機材を設置する手法であるので、規模が大きくなると、自宅では物理的に限界が生じる。そこで、自宅サーバ群を大学のネットワークセンターや研究科のサーバールーム、企業、行政機関の電算室等の隅に、いよいよ、こっそりと、移転することにするのである。そして、そこから、だんだんとサーバ類が増殖していくのである。

筆者は、最近13の行政機関(主に市町村)を巡回してヒアリングをさせて頂いたが、だいたい半分くらいの市のIT能力の獲得方法は、20年以上前から行政機関の庁舎に「こっそりと自前サーバを建立し、そこで勉強する」というものであった。(更に、こっそりSoftEtherを使って自宅から行政機関にリモートログインしていた人も点在した。)そういった勉強方法を怠らずに励行してきた職員がいる行政機関は、それが継続して知識が蓄積され、20年たって、ITに関して先進的な立派な組織能力を身に付けておられ、そういった職員個人も、20年たった今はITのトップレベルの管理者になって組織を支えておられるのである。

IT能力、ひいてはシステムソフトウェア技術革新能力は、このようにして国家的に形成される。IT技術立国において、必須の正常な過程である。後述するように、COBOLも、インターネットも、実はノイマン形コンピュータも、公務員や行政の研究所の研究者が職場環境を改良しようとして発明している。UNIXは電話会社職員が遊びで発明している。Googleの大規模検索エンジンシステムが、大学のサーバールームの片隅から、このようにして成長していったことは大変有名である^{(4),(5)}。近時、日本の

大学、企業、行政機関においても、この米国手法を見倣って、自宅サーバや自宅データセンターの限界を突破するため、サーバやネットワーク機器の持込みを許容ないし奨励するところが見られる。この傾向がこのまま継続、発展すれば、日本からも UNIX や Google や Amazon、Microsoft などに匹敵する立派なシステムソフトウェアを生み出す豊富な人材が増え、日本の IT 立国は実現されるであろう。

さて、話を筆者の自宅データセンターに戻すと、当初は環境に大きな制約があった。大学の近くの自宅のアパート（月額 2.9 万円くらい）は、AC100V、15A のコンセントが僅か 2 本しかなかった。そこに IPA の予算で購入した複数のサーバを置いて、電源を入れた後に電子レンジを使うと、ブレーカーがすぐに落ち、大いなる苦難を味わった。そこで、IPA の委託開発を確実に遂行する目的のため、電子レンジは、一大決心して捨ててしまった。（真実は、祖父から送られてきたほうれん草の冷凍物を電子レンジに入れてふたを閉じた後、これを忘れて数日たち、装置全体が回復不能な状態に陥ったことが原因である。）これにより、ようやく IPA の官給サーバは一応電源を入れられるようになった。しかし、次に更なる電力不足が発生した。筆者のアパート室には IPA のお金で確保した、余っている光ファイバ回線やグローバル IP アドレスが多数あるらしい、といううわさが学生間で流れ、同級の数人の大学生などが Web サーバを次々に持ち込んできたのである。ここで筆者が大変悩まされたことは、電力問題だけではない。

当時のサーバには、まず必ず CD-ROM ドライブ（DVD-ROM ではない）が付いていたのであるが、サーバ管理者（つまり、所有者の学生）が夜中に SSH から eject コマンドを実行し、CD-ROM トレイを遠隔で、無意味に何度も出し入れして、モータ音を鳴らし、夜中に筆者を大いに困惑させるのである。このことを耳にして愉快に思った別の者は、模倣をしようとして、その者の持込みサーバで同様に eject コマンドを実行したが、その者の哀れなサーバには、スリム・タイプの CD-ROM ドライブしか付いておらず、一度排出されればトレイは外から指で押さなければ元に戻らない。そこで、筆者はその都度、指で押し戻してあげた。

ちなみにそれらの Web サーバの一つには、いつの間にか筑波大学園祭の公式 Web サイト (<https://sohosai.com/>) の電子申請システムなども稼動す

るようになっていたらしい。要するに、IPA のお金で調達した金属ラックや、IPA のお金で調達したグローバル IP アドレス回線に、IPA の SoftEtherVPN の開発プロジェクトとは全然無関係のホストが、多数稼動している状態となったのである。これらは、副次的効果として、サーバ持ち込み学生たちの IT 技術能力向上に、極めて役立っていた。現在、それらの人材は皆、習得した技術を活用し、社会的に大変有益な効用を生み出しているようであるから、IPA が法律で掲げる「情報処理の促進」という立派な役割を、間接的に果たしていると言えるのである。したがって、そういう当時の受益学生たちは、今からでも IPA に 3 回程度頭を下げるべきである。

ところでこの大変適当な手法では、そのうちに B フレッツで引ける IP アドレス 8 個×2 本=16 個を超えるグローバル IP アドレスを割り当てることができない、という重大な限界に、誰もがうすうすと気づくのである。すなわち、前述の「元服」を経て自宅データセンターを構築したものの、結局上流プロバイダの IP バックボーンの一部として支配下にある以上、それを超えるものは決して作れない、ということに気づくのである。そこで、この制限から脱却するために、近時の自宅データセンター好事家たちは、AS 番号と多数個の IPv4 アドレスの直接の割当を受け、前述のとおり、BGP と呼ばれるバックボーン領域に手を染めることが流行している。このようにネットワーク的自律運営を果たして初めて、我々日本人も、AWS や Google、Microsoft を超えるクラウドサービスやインターネットサービスに関わる通信システムソフトウェアの開発を開始することができる。

筆者は自宅ネットワークや自宅サーバのレベルから芽生え、自然に成長し、いよいよ大学・企業・官庁のサーバールの隅を占拠していった、同時に、自前クラウドや自前インターネットバックボーンに手を伸ばすというような IT 人材育成法が、歴史的にみると正攻法であると考え、現在の若手人材をみると、こういった正攻法の普及・増加が見える。この手法が IT における国富論と言える。これにより、日本の技術水準は今後ますます向上し、やがて、全世界で利用される日本製のシステムソフトウェア群やクラウドサービス群、AI 群が相次いで多数誕生し、ついに日本の「デジタル敗戦」は挽回され、IT 立国は実現される。これにより、日本の国際競争力は復活し、収益や雇用はもちろん、社

会福祉の問題すら解決できる可能性がある。

後編では、前記⑦で入手した資源群で、本来目的のプログラミングをすることをしばらく懈怠（けたい）し、自宅データセンターの自作をして単に遊んでいたことが、結果的に、短期間での④技術形成につながった点から述べる。（後編に続く）

文献

- (1) 登 大遊, “SoftEther による Ethernet の仮想化とトンネリング通信,” 情処学第 45 回プログラミングシンポジウム論文誌, pp.147-158, Jan. 2004.
- (2) 登 大遊, 新城 靖, 佐藤 聡, “SoftEther VPN Server: マルチプロトコル対応のクロスプラットフォームなオープンソース VPN サーバ,” コンピュータソフトウェア, vol. 32, no. 4, pp. 3-30, Nov. 2015.
- (3) パスカル・ザカリー, 闘うプログラマー 上巻, pp.208, 日経 BP, 東京, 1994.

- (4) SolarWinds Worldwide, LLC., “Before Google became Google: the original setup at Stanford University,” March 2009. <https://www.pingdom.com/blog/original-google-setup-at-stanford-university/>
- (5) Gigazine, “Google の初代サーバを間近から詳細に撮影した写真いろいろ,” Feb. 2007. https://gigazine.net/news/20070226_google/

登 大遊

1984 兵庫県生まれ。ソフトウェア技術者兼経営者。ソフトイーサ株式会社代表取締役。専門は VPN（仮想プライベートネットワーク）などの通信技術を含めたシステムソフトウェア。2017-03 筑波大学大学院システム情報工学研究科博士後期課程了。博士（工学）。2022-04 筑波大客員教授。





オープンソースの 仮想マシン管理ツール

九州工業大学 光来健一 Kenichi Kourai

1 はじめに

計算機やネットワークで仮想化技術が広く使われるようになり、仮想マシン（VM）もずいぶん身近な存在になった。無償で利用できる VirtualBox や、2024 年 11 月に無償化された VMware Workstation（または Fusion）を使ったことがある方も多いだろう。ユーザーに VM を提供する Infrastructure as a Service (IaaS) クラウドを利用している方は少ないだろうが、それ以外の多くのクラウドでも、内部では VM を使ってサービスを提供するのが一般的である。最近は VM ではなくコンテナが使われることが増えているが、クラウドではコンテナを VM の中で動かしていることも多い。

VM は計算機のリソース（CPU、メモリ、ディスク、ネットワークなど）を、仮想化することによって作られる仮想的な計算機である。VM には様々な OS をインストールすることができる。例えば、Windows 10 から使えるようになった Windows Subsystem for Linux 2 (WSL2) は VM を使って Linux を動作させており、Windows 上でシームレスに Linux のアプリケーションを動かすことができるようになっている。古くは Windows 7 において「XP モード」と呼ばれる互換モードが提供されていたが、このモードは VM を使って一つ前のバージョンの OS である Windows XP を動作させ、その上で Windows XP のアプリケーションを動作させていた。

また、VM は必要なときに必要なだけ作成することができる。クラウドではアクセスが増えたときにはサービスを提供する VM を増やし、アクセスが減ると VM も減らすという仕組みが採用されている。このような柔軟な対応は物理的な計算機では難しい。この特徴を利用すると、ネットワークを用いた様々な実験に VM を活用することができる。例えば、分散コンピューティングなどにおいて、ネットワークに多数の計算機を接続して実

験を行いたい場合、VM であれば簡単に必要な台数を用意でき、複数のホストにまたがっていても一元的な管理を行うことができる。物理的な計算機を用いて実験を行う前の検証に VM を利用することもできる。

本稿では、Linux のデファクトスタンダードの仮想化ソフトウェアである Kernel-based Virtual Machine (KVM) と、その VM を管理するための三つのオープンソースのツールを紹介する。

2 KVM

KVM は 2005 年にイスラエルのスタートアップの Qumranet 社によって開発された仮想化ソフトウェアである。KVM は Intel や AMD の CPU が提供する仮想化支援機構を用いて、VM 内の OS（以降、「ゲスト OS」と呼ぶ）を改変せずに動作させることを可能にした。2007 年に Linux カーネル 2.6.20 にマージされた後、2008 年には Red Hat 社に買収され、現在に至るまで活発に開発が続けられている。KVM は「ハイパバイザ」とも呼ばれ、VM にリソースを分配したり、VM 間の隔離を行ったりしている。KVM は「タイプ II」と呼ばれる種類のハイパバイザであり、既存の OS（ゲスト OS に対して「ホスト OS」と呼ばれる）の上（一部

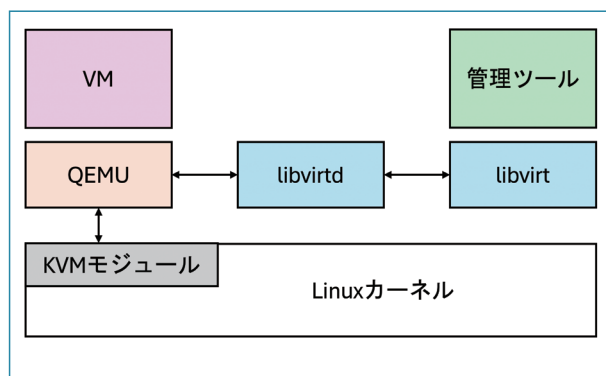


図1 KVM を用いる仮想化システム

の機能はホスト OS の中で実行される。そのため、タイプ I と呼ばれる、ハードウェアの上で直接動作するハイパバイザと比べて利用しやすいという特徴がある。

KVM を用いる仮想化システムのアーキテクチャは図 1 のようになっている。ホスト上で動作している Linux カーネルの中で KVM モジュールが動作する。カーネルの上ではデバイスエミュレータの QEMU (「きゅーえむ」と読むことが多い) が動作し、KVM モジュールを呼び出しながら動作する。QEMU は VM に提供される仮想ディスクや仮想 NIC などの仮想デバイスのエミュレーションを行う。VM の実行は KVM モジュールと QEMU だけで行うことができるが、VM を管理するために libvirt デーモン (libvirtd)⁽¹⁾ が用いられることが多い。libvirtd は KVM だけでなく、Xen や VirtualBox など、多数の仮想化ソフトウェアに対応している。更に、VM の管理だけでなく、コンテナの管理を行うこともできる。libvirtd を利用する管理ツールは libvirt ライブラリを用いて作成される。本稿で紹介する virt-manager, virsh, OpenStack 以外にも様々な VM 管理ツールが作成されている。

Ubuntu 25.04 において KVM を使うには qemu-kvm パッケージをインストールし、kvm-ok コマンドで KVM が利用できるようになったことを確認する。また、libvirt を使うために libvirt-daemon-system パッケージをインストールする。これらのパッケージをインストールすると、依存関係のある必要なパッケージが全てインストールされる。

3 virt-manager

仮想マシンマネージャ (virt-manager)⁽²⁾ は Red Hat 社によって開発された VM を管理するためのグラフィカルツールである。virt-manager を実行すると図 2 のように、起動中及び停止中の VM の一覧が表示される。virt-manager を使うことで、VM の作成、起動、停止などの基本操作に加えて、クローンの作成、スナップショットの作成、マイグレーションなどを簡単な操作で行うことができる。この管理ツールを使うには virt-manager パッケージをインストールする。本稿では Ubuntu 25.04 でインストールされる virt-manager 5.0.0 を対象とするが、ほかのバージョンでも基本的な操作方法は同じである。

3.1 VM の作成

VM を作成するには、まず、ゲスト OS をインストールするために用いる ISO イメージをダウンロードする。Ubuntu をインストールする場合には Ubuntu の公式サ

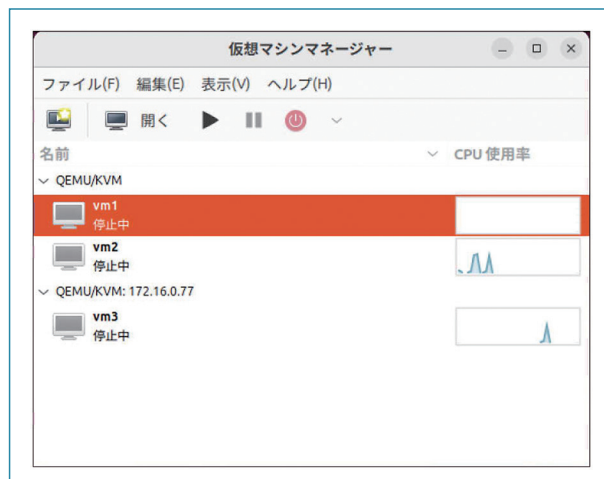


図2 virt-manager の画面

イトからダウンロードすることができるが、日本国内のミラーサイトを使う方が短時間でダウンロードが完了する。ダウンロードした ISO イメージを virt-manager で利用できるようにするために、virt-manager のイメージ格納用ディレクトリに配置する。

この ISO イメージを使って VM を作成するには、virt-manager の VM 作成ボタンをクリックしてローカルメディアからのインストールを選択する。一覧から ISO イメージを選択し、割り当てる仮想 CPU 数とメモリ量を指定する。ホストの CPU コア数やメモリ量、同時に起動する VM の数などを考慮して割当を決定する。後で変更することもできるため、取りあえずはデフォルトの値のままでも構わない。

次に、仮想ディスクのサイズを設定する。このサイズはインストールするゲスト OS に合わせて調整する必要がある。例えば、Ubuntu Desktop をインストールするには Ubuntu Server よりも大きな仮想ディスクが必要になる。仮想ディスクはホスト上にファイルとして作成され、ファイルの見掛け上の大きさは仮想ディスクのサイズと同じになる。しかし、実際には仮想ディスクに書き込まれたデータの分しかホストのディスクは使用されない。そのため、仮想ディスクのサイズは大きめに設定しておくといよい。

最後に、仮想ネットワークの設定を行う。VM はデフォルトで NAT 接続されるため、VM の中から外部のネットワークにアクセスすることしかできない。外部のネットワークから VM にアクセスできるようにしたい場合は、ブリッジ接続を行う必要がある。そのために、bridge-utils パッケージをインストールし、netplan の設定ファイルを作成してネットワークブリッジ (br0 等) の設定を行う。ブリッジの設定は Ubuntu のグラフィカルな設定ツールでは行うことができないため、コマンドラインで行う必要がある。ブリッジが作成されていれ

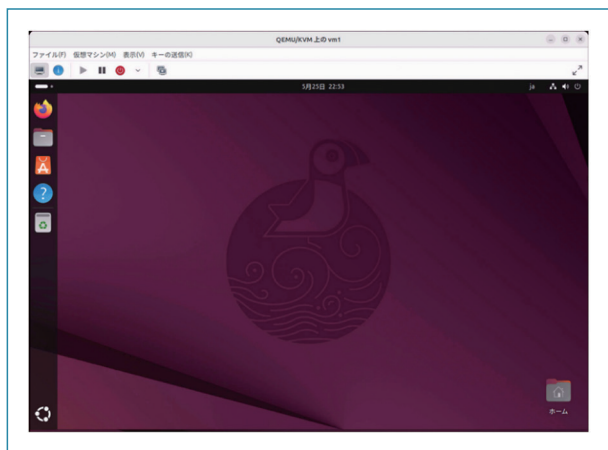


図3 VMのグラフィカルな画面

ば、ネットワークの設定の際にブリッジデバイスを選択することができる。

このようにして作成したVMを起動すると、ISOイメージを用いてUbuntuのインストーラが実行される。その後は通常のインストール作業を行い、再起動すると図3のようにVM内でUbuntuが起動する。VMを停止させる際にはVM内でシャットダウンを行えばよいが、virt-managerの電源ボタンから[シャットダウン]を選択しても正常にシャットダウンが行われる。VMが応答しなくなった場合には[強制的に電源OFF]を選択することで停止させることができるが、データが失われるおそれがある。

3.2 様々なVMの管理

ネットワークの実験を行うには複数のVMが必要になることが多いが、それぞれのVMを一から作成してゲストOSをインストールするのはかなりの手間が掛かる。VMの作成を容易にするために、virt-managerではVMのクローンを作成することができる。VMが停止している状態でVMのメニューにある[複製...]を選択すれば、同じ状態のVMのクローンが作られる。ただし、ホスト名や静的IPアドレスも同じになるため、複製したVMを起動した後でこれらを変更する必要がある。

VMを用いて仮想ルータを作成するには、VMに仮想NICを追加する必要がある。VMの仮想ハードウェアに変更を加えるには、VMが停止している状態で図4のようにVMの仮想ハードウェアの一覧を表示し、新しい仮想NICを追加する。VMを起動すると、追加した仮想NICが見えるようになっている。この仮想NICを別のネットワークに接続するには、別のネットワークブリッジ（例えばbr1）を作成しておき、それを仮想NICの接続先とする。

virt-managerはリモートホストのVMを管理するこ

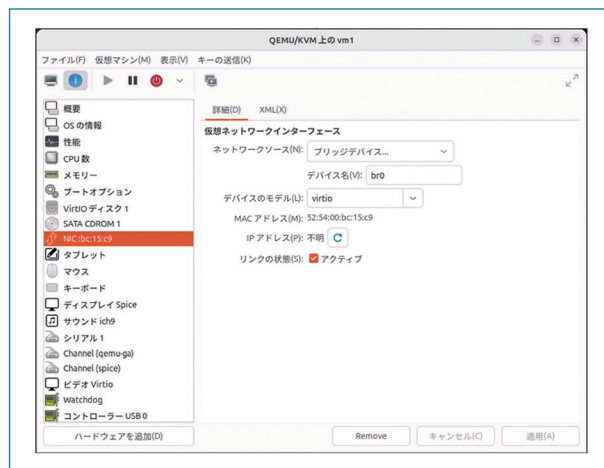


図4 VMの仮想ハードウェア

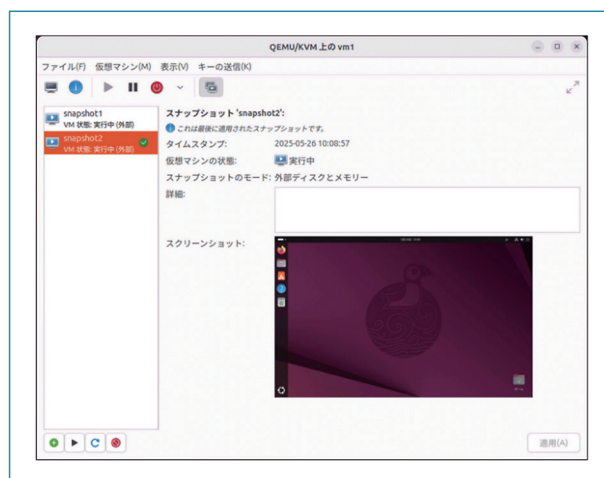


図5 VMのスナップショットの管理

ともできる。リモートホストにはSSHで接続するため、リモートホストにはopenssh-serverパッケージをインストールし、ローカルホストにはssh-askpassパッケージをインストールする。そして、virt-managerのメニューにある[接続を追加...]を選択し、リモートホストのユーザ名とホスト名を入力する。ユーザ名はデフォルトではrootになっているが、rootでSSHログインできるように設定するとセキュリティが低下するため、一般ユーザに変えた方がよい。リモートホストに接続すると、リモートホストに存在するVMの一覧も表示されるようになる。例えば、図2のvm3はリモートホストのVMである。以降はローカルホストで動いているVMと同様に管理を行うことができる。この機能はvirt-managerが利用しているlibvirtライブラリがSSH経由でリモートホストのlibvirtdに接続することでシームレスに実現されている。

virt-managerはVMの状態をスナップショットとして保存しておき、後で必要になったときに復元することができる。例えば、VMへのゲストOSのインストール

直後にスナップショットを保存しておき、VM の設定がおかしくなってしまったときに簡単に初期状態に戻す、といった使い方ができる。VM のスナップショットボタンをクリックすると図 5 のような管理画面が表示されるので、スナップショットに分かりやすい名前をつけて保存する。必要になったときには戻したいスナップショットを選択して状態の復元を行う。

この機能を応用したのが VM のマイグレーションである。マイグレーション元のホストで VM の状態を保存し、それをマイグレーション先のホストにネットワーク経由で転送して VM の状態を復元する。スナップショットと異なるのは、VM を動かしたまま、状態の保存・転送を行うことができる点である。マイグレーション中に VM が変更した状態は再送することで、マイグレーション先において完全な状態を復元することができる。リモート管理を行う場合と同様に、マイグレーション先のホストへの接続を追加しておいてから、VM のメニューにある [移行...] を選択し、マイグレーションを実行する。しばらくするとマイグレーションが完了し、マイグレーション先のホストで VM が再開される。

VM マイグレーションでは基本的に CPU やメモリなどの VM の状態だけが転送され、仮想ディスクの転送は行われない。そのため、仮想ディスクはネットワークファイルシステム (NFS 等) を用いてホスト間で共有しておく必要がある。NFS サーバでは nfs-kernel-server パッケージをインストールし、VM の仮想ディスクを配置する。それをマイグレーション元とマイグレーション先の両方のホストのイメージ格納用ディレクトリにマウントして共有する。スナップショットを保存した後の VM はマイグレーションに失敗するようであるため、マイグレーション機能を利用する場合にはスナップショット機能は使わないようにする必要がある。

4 virsh

virsh は VM を管理するためのコマンドラインツールであり、グラフィカルツールが使えないサーバでも SSH ログインして利用することができる。また、VM の管理を行うシェルスクリプトの中で用いることもできる。virsh は libvirt-daemon-system パッケージをインストールする際に同時にインストールされる。virsh のコマンドの幾つかを表 1 に示す。

例えば、VM を起動するには virsh start コマンドを用いる。virt-manager とは異なり、VM のグラフィカルな画面を表示させることはできないため、ゲスト OS の起動メッセージやログインプロンプトなどを表示させたい場合は、virsh console コマンドを用いて VM のシ

表 1 virsh のコマンドの例

コマンド名	機能
list	VM 一覧を表示する。起動していない VM も表示するには --all オプションをつける。
start	VM を起動する。
shutdown	ゲスト OS をシャットダウンして VM を停止する。
destroy	VM の電源を切る。
dumpxml	VM の設定を XML 形式で表示する。
edit	XML 形式の VM の設定を編集する。
save	VM の状態をファイルに保存する。
restore	VM の状態をファイルから復元する。
migrate	VM を指定したホストにマイグレーションする。

リアルコンソールに接続する。virsh start コマンドに --console オプションを指定してもよい。VM 内のメッセージがシリアルコンソールに出力されるようにするには、VM 内のゲスト OS にシリアルコンソールを使うための設定を行う必要がある。起動した VM を停止する際には virsh shutdown コマンドを用い、ゲスト OS が正常にシャットダウンされるようにする。

virsh を用いると、virt-manager ではサポートされていない、きめ細かい VM の管理を行うことができる。virt-manager では起動中の VM を停止させずに行うライブマイグレーションのみがサポートされているが、virsh migrate コマンドを使えば、ほかにも様々な方法でマイグレーションを行うことができる。例えば、マイグレーションを最速で完了させるために、VM を一時停止させてからマイグレーションを行うことができる。更には、起動していない VM に対してもオフラインマイグレーションを行うことができる。また、マイグレーションでの状態転送方法として TCP によるダイレクト接続と SSH トンネルだけでなく、TLS を用いたりデータを圧縮したりすることができる。virsh migrate-setspeed コマンドを用いることで VM マイグレーションの際の最大ネットワーク帯域を制限することもできる。

virsh migrate コマンドに --copy-storage-all オプションをつけることで、VM の状態だけでなく仮想ディスクも転送することができる。この機能を用いると、仮想ディスクを共有していないホスト間でもマイグレーションを行うことができる。ただし、一般に仮想ディスクのサイズは VM のメモリのサイズよりも大きいため、VM マイグレーションに長い時間が掛かる。マイグレーション先にあらかじめベースとなる仮想ディスクをコピーしておけば、--copy-storage-inc オプションをつけてマイグレーションを行うことで、差分だけを高速に転送する

```

virt-install ¥
  --name vm2 ¥
  --vcpus 2 ¥
  --ram 4096 ¥
  --disk size=25 ¥
  --network bridge=br0 ¥
  --location ubuntu-25.04-server.iso ¥
  --graphics none ¥
  --extra-args 'console=ttyS0,115200n8 serial'

```

図6 コマンドを用いた VM の作成

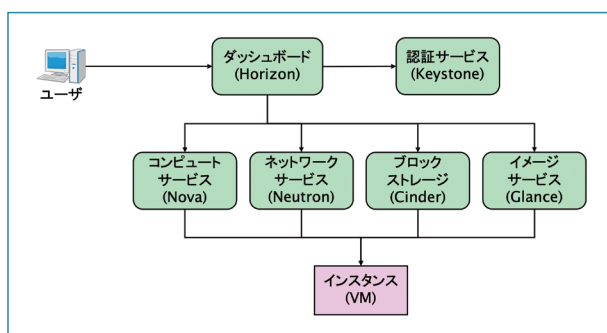


図7 OpenStack の構成

こともできる。

コマンドラインで VM を作成してゲスト OS のインストールを行うには、virt-install コマンドを利用する。このコマンドは virt-install パッケージでインストールする。virt-install は virt-manager が VM の作成及びゲスト OS のインストールを行う際に内部で利用されている。virt-install は図 6 のように多くのオプションを指定して実行する。この例では、2 個の仮想 CPU、4,096

MB のメモリ、25 GByte のディスクを割り当て、ネットワークにはブリッジ接続を用いるようにした VM を作成する。その後、指定した ISO イメージからシリアルコンソールを用いてゲスト OS をインストールする。

5 OpenStack

OpenStack⁽³⁾ は VM 管理ツールの範疇を超えた巨大なクラウド基盤ソフトウェアであるが、virt-manager や virsh と同様に libvirt を用いて VM の管理を行っているため、ここで簡単に紹介する。OpenStack は IaaS クラウドを構築するためのオープンソース・ソフトウェアであり、サーバ、ストレージ、ネットワークなどを統合的に管理して、VM やストレージをユーザに提供する。商用の Amazon EC2 や S3 の影響を強く受けており、プライベートクラウドを構築する際になどに用いられている。OpenStack は 2010 年に Rackspace Hosting 社と NASA の共同プロジェクトとして開発が始まり、2012 年に設立された OpenStack Foundation によって管理されてきた。2020 年には名称を Open Infrastructure Foundation (OpenInfra Foundation) に変更し、2025 年 3 月には Linux Foundation のメンバーとなった。500 以上の企業が開発に参加しているのが特徴である。

OpenStack を構成する主要コンポーネントは図 7 のようになっている。ダッシュボード (Horizon) はユーザに Web ベースのグラフィカルインタフェースを提供しており、インスタンス (VM) やストレージ、ネットワークの管理などを行うことができる。コンピュートサービス (Nova) はインスタンスにリソースを割り当てて起動する。このサービスは libvirt を用いて VM の管

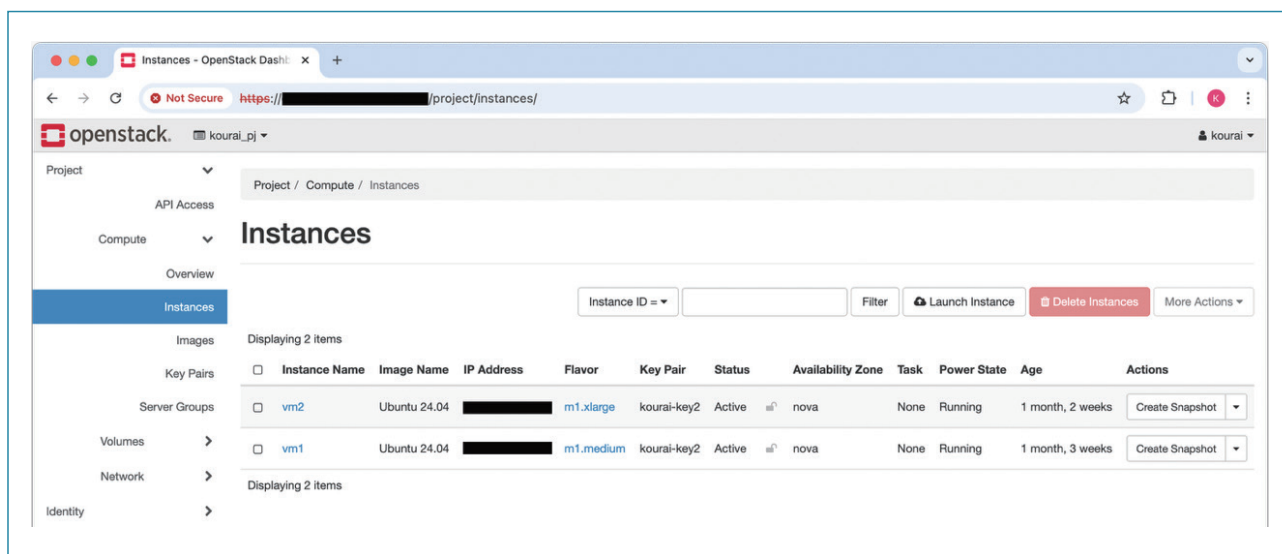


図8 OpenStack のダッシュボード

理を行っている。イメージサービス (Glance) はインスタンスのイメージ (仮想ディスクのテンプレート) を管理する。ネットワークサービス (Neutron) はネットワーク機能を提供し、ネットワークを仮想的に分割してインスタンスをネットワークに接続する。ルータ、ファイアウォール、ロードバランサなどの機能も提供する。認証サービス (Keystone) はダッシュボードや API にアクセスする際のユーザ認証の機能を提供する。

ダッシュボードにログインすると、図 8 のようにインスタンスの一覧が表示される。グラフィカルな画面を使ってそれぞれのインスタンスにアクセスすることもできるが、基本的には SSH でログインして利用する。ログインに必要な公開鍵認証のキーペアは事前に作成して秘密鍵をダウンロードしておき、インスタンス作成時に公開鍵を指定する。パスワード認証を無効にしておくことができるため、VM 作成直後のセキュリティを強化することができる。

インスタンスを作成する際には、登録されているインスタンス・タイプの中から必要な仮想 CPU 数やメモリ量を持ったものを選択する。インスタンス・タイプは管理者が自由に登録することができる。更に、登録されているイメージの中から利用したいゲスト OS を選択する。イメージも管理者が自由に登録することができ、Ubuntu の場合は Ubuntu のサイト上でクラウドイメージが提供されている。作成した VM を起動すると、ゲスト OS のインストールを行うことなく、指定したイメージから直接、仮想ディスクが作成され、すぐに VM が利用可能になる。

6 おわりに

本稿では、Linux 上で KVM を用いて VM を管理するためのツールである virt-manager と virsh、及びクラウド基盤ソフトウェアの OpenStack を紹介した。virt-manager はグラフィカルツールであり、VM の管理を容易に行うことができる。よりきめ細かい管理を行いたい場合や、サーバで VM の管理を行う場合には virsh を使うことができる。複数のユーザで VM を使いたい場合には OpenStack を導入すると便利である。筆者は大学院の講義で OpenStack を用いて VM を使った演習を行わせている。本稿が Linux で VM を使う際の一助となれば幸いである。

文献

- (1) Red Hat, Inc., “libvirt: the virtualization API.” <https://libvirt.org/>
- (2) Red Hat, Inc., “Virtual machine manager.” <https://virt-manager.org/>
- (3) OpenInfra Foundation, “OpenStack: open source cloud computing infrastructure.” <https://www.openstack.org/>

光来健一

2002 東大大学院理学系研究科情報科学専攻博士課程了。博士 (理学)。同年から NTT 未来ねっと研究所研究員。2003 東工大・情報理工・助手, 2008 九工大・情報工・准教授, 2018 同教授。オペレーティングシステムや仮想化に関する研究に従事。



歴史とにぎわいが混在する街 「福岡」

街plus
探訪



九州産業大学 石田俊一 Toshikazu Ishida

1 はじめに

福岡市は九州北部に位置しアジアに近い地理的特性から、古くから国際交流の拠点として発展してきました。2025年5月時点の推計人口は約165万人で、全国の政令指定都市の中でも人口増加率が高く、活気ある都市として注目されています⁽¹⁾。その背景には「天神ビッグバン」や「博多コネクティッド」といった大規模再開発があり、都市機能の高度化と魅力的な街づくりが進行中で、地価の上昇、若者や企業の流入が続いています。古代から続く歴史と伝統を大切にしながらも、先進的な都市づくりを進める福岡は、今後も発展を続ける注目の都市だと言えます。また福岡には、もつ鍋や水炊き、豚骨ラーメンなど多くのおいしいものが存在し、文化として地域に根付いています。

今回は福岡市の紹介とともに、福岡市の中でも2025年電子情報通信学会総合大会の開催会場である、九州産業大学が位置する福岡市東区に注目した歴史や文化について紹介するとともに、筆者の好きな豚骨ラーメンに注目した食文化についても紹介します。

2 福岡市の成り立ち

福岡市の歴史は、古代から「博多」として知られた地域から始まります⁽²⁾。博多は8世紀には既に文献に登場し、大陸との交易の拠点として栄えました。特に中世には、商人たちによる「自治都市」として発展し、国際貿易港としての地位を確立しました。しかし、戦乱によって博多の街は幾度も焼失し、そのたびに復興を遂げてきました。

江戸時代初頭に入ると、関ヶ原の戦いの功績により「筑前国」を与えられた黒田長政が、1601年に那珂川の西側に福岡城（図1）を築き、その周辺に城下町を整備しました。この新たな町は、黒田氏の先祖の地「備前福岡」（現・岡山県瀬戸内市）にちなんで「福岡」と

名付けられました。こうして、那珂川を挟んで東に商人の町「博多」、西に武士の町「福岡」という二つの異なる性格を持つ町が並立する形が生まれました。

明治時代に入り、廃藩置県により福岡藩は福岡県となり、1876年には福岡と博多が正式に統合されました。市制施行にあたっては、市名を「福岡」とするか「博多」とするかで激しい議論が交わされ、最終的には市議会が1票差で「福岡市」と決定しました。

その後、福岡市は周辺の町村を次々と編入し、1972年には政令指定都市に昇格、現在では九州最大の都市として、行政・経済・文化の中心地となっています。博多の名は今も駅名や地名、祭り（「博多祇園山笠」）などに残り、福岡市の歴史的・文化的アイデンティティの一部として息づいています⁽³⁾。

3 福岡城の歴史

福岡の地名の発祥は先に述べたとおり、福岡城と関係が深いことから、ここでは福岡城について紹介します。

福岡城は江戸時代初期の1601年、黒田長政によって築かれました⁽⁴⁾。彼は関ヶ原の戦いの功績により筑前52万石を与えられ、父・黒田如水（官兵衛）の助言を受けて、博多の西にある福崎の丘陵地に新たな城を築くことを決意しました。福岡城は平山城（ひらやまじろ）として設計され、築城には7年を要し1607年



図1 福岡城跡



図2 多聞櫓

に完成しました。福岡城は本丸、二の丸、三の丸から成り、大小47の櫓と10の城門を備えた大規模な城郭で、総面積は約47万 m^2 、石垣の総延長は約6kmに及びます。特に「多聞櫓（たもんやぐら）」（図2）は現存する重要文化財であり、城の象徴的存在です。江戸時代を通じて、福岡城は黒田氏の居城として機能し、福岡藩の政治・軍事の中心地となり、城下町も整備され、福岡は九州の主要都市として発展しました。

幕末には第11代藩主・黒田長濤によって大規模な城の改修が行われました。明治維新後、1871年の廃藩置県により福岡藩は廃止され、福岡城も廃城となりました。多くの建造物は解体され、城跡は公園や公共施設として再利用されました。その後、福岡城は「舞鶴城」と呼ばれたこともあり、城跡は「舞鶴公園」として整備され、市民の憩いの場となっています。

20世紀以降、福岡城跡の保存と整備が進められ、2014年には「福岡城跡整備基本計画」が策定されました。天守閣は現存しませんが、天守台や石垣、櫓などの遺構が残り、歴史的景観の復元が進んでいます⁽⁴⁾。また、城内には平安時代の迎賓館「鴻臚館（こうろかん）」の遺跡も発見され、古代から近世にかけての歴史が交差する貴重な場所となっています。現在、福岡城跡は歴史教育や観光の拠点としても重要な役割を果たし、春には「福岡城さくらまつり」などのイベントも開催され、多くの人々に親しまれています。

4 福岡市東区の成り立ちと神社

2025年電子情報通信学会総合大会が開催される九州産業大学が位置する福岡市東区は、古代から現代に至るまで多様な歴史と文化が息づく地域です。特に、筥崎宮（はこぎきぐう）、名島神社（なじまじんじゃ）、産土根神社（うぶすねじんじゃ）、綿津見神社（わたすみじんじゃ）といった神社は、地域の精神的支柱として重要な役割を果たしてきました。



図3 筥崎宮（上：鳥居，下：境内）

筥崎宮（図3）は、921年に創建されたとされ、日本三大八幡宮の一つに数えられます。主祭神は応神天皇で、神功皇后と玉依姫命も祀られています。鎌倉時代の元寇では「神風」が吹いたとされ、厄除・勝運の神として信仰を集めました⁽⁵⁾。また、豊臣秀吉や黒田長政など歴史的な武将も参拝し、福岡の発展に深く関わってきました。



図4 名島神社（上：鳥居，下：境内）



図5 綿津見神社の絶景スポット

名島神社（図4）はかつての名島城跡に鎮座し、地域の守護神として親しまれています。名島城は1588年、小早川隆景が豊臣秀吉の命で築城したもので、福岡城築城に伴い廃城となりましたが、その跡地は現在公園として整備され、歴史を今に伝えています⁽⁶⁾。

産土根神社は、地域の産土神（うぶすながみ）を祀る古社で、地元住民の生活と密接に結び付いてきました。詳細な創建時期は不明ですが、古くから信仰の場として、地域の安寧と繁栄を祈る祭祀が続けられています⁽⁷⁾。

綿津見神社は、福岡市東区三苫に鎮座する海の守護神、綿津見神（わたつみのかみ）を祀る神社です。古くから海上安全や漁業繁栄を祈願する場として信仰されてきました。境内には平安時代後期から南北朝時代にかけての仏像群が安置されており、市の有形文化財に指定されています。神社は玄界灘を望む高台にあり、夕日の美しい絶景スポットとしても知られています⁽⁸⁾（図5）。

近年の東区は、福岡市の都市化とともに急速に発展しています。箱崎や香椎エリアでは再開発が進み、大

学や研究機関の集積、交通インフラの整備が進行中です。特に九州大学箱崎キャンパス跡地の再開発は、商業・住宅・文化施設の融合を目指す大規模プロジェクトとして注目されています。また、歴史的町並みの保存にも注力しており、旧唐津街道沿いの町家や名島橋などが文化財として登録されるなど、歴史と現代が共存する街づくりが進められています。

5 九州産業大学

2025年の総合大会の会場となる九州産業大学（図6）は、1960年に「九州商科大学」として創立され、1963年に現在の名称へと改称された福岡市東区に位置する私立大学です。創立者・中村治四郎の理念「産学一如（産業と大学の一体化）」の下、実践的な教育を重視し、商学部から始まった学びの場は、現在では9学部21学科、大学院5研究科を擁する総合大学へと発展しました。

大学は2020年に創立60周年を迎え、2030年に向けた中期計画を策定。「文理芸融合のグローバル総合大学」を目指し、教育・研究・国際化・地域貢献など8分野にわたる改革を進めています。特に注目すべきは、キャンパス整備の一環として進められている「学美（まなび）の丘」構想です。これは、学生の学びと交流を促進するための新たな空間づくりで、2025年度までに複数の施設改修や新設が進められています。例えば、正門周辺や体育館周辺の駐車場・駐輪場の再整備、学習支援施設の拡充などが進行中です。更に、九州産業大学の立地条件も大きな魅力の一つです。JR「九産大前」駅から徒歩ですぐというアクセスの良さに加え、JR「博多」駅から電車で約15分、福岡市中心部である天神エリアへ乗換えなしでアクセス可能、福岡空港へも電車で約30分以内と、国内外の移動にもスムーズで、「都市型キャンパス」としての利便性を備えています。



図6 九州産業大学



図7 博多ラーメン（左）と久留米ラーメン（右）

また、大学周辺には福岡名物で、筆者の好物である豚骨ラーメンを提供する店舗が徒歩圏内に9軒以上あります。福岡県では300軒以上のラーメン店がしのぎを削っています。こってりとしたスープに細麺が絡む本場の味を、授業の合間や放課後に気軽に楽しめるのは、福岡ならではの特権です。

6 豚骨ラーメンの歴史や種類について

豚骨ラーメンは、豚の骨を長時間煮込んで作る白濁スープが特徴のラーメンで、福岡県久留米市が発祥だと言われています。その後、福岡市の博多や長浜でも独自の進化を遂げ、現在では「久留米ラーメン」「博多ラーメン」「長浜ラーメン」として知られています（図7）。

久留米ラーメンは1937年に誕生し、白濁スープは偶然の産物として1947年に生まれました。濃厚で「こく」があり、スープは「呼び戻し」製法で継ぎ足しされるのが特徴です。

長浜ラーメンは、漁港の市場労働者向けに素早く提供するため、極細麺と博多ラーメンよりあっさりしたスープが特徴です。「替え玉」文化も長浜ラーメンから始まったと言われています。

そのほか、しょう油やみその香りを追加して風味を出した「豚骨醤油ラーメン」や「味噌豚骨ラーメン」など、豚骨ベースのラーメンの種類は豊富です。これらの違いは、地域の食文化や歴史に根差しており、豚骨ラーメンの奥深さを物語っています。更に各店で使用する麺にも個性があり、同じ麺でもゆで方の違いによる麺の硬さでも味が変わります。選べる麺の硬さは店や豚骨ラーメンの種類によっても異なりますが、「硬め＞普通＞やわ」と選ぶことができ、更に店によっては「バリカタ」「ハリガネ」「粉落とし」など、より硬い麺のゆで方もあります。

「豚骨ラーメンは臭いが…」と思われる方もいら

っしゃると思います。実際に筆者も食べる前は思っていました。しかし、一度食べると価値観ががらっと変わる経験をする事間違いなしです。あっさりしていて癖が少ないラーメンを希望の方は博多ラーメンから、こくがありインパクトを求める方は久留米ラーメンから試してみることをお勧めします。福岡以外でも、近年全国各地で豚骨ラーメンを提供する店は見受けられますが、「激戦区」福岡で是非食べて頂き、深い歴史をかみ締めてみてはいかがでしょうか。福岡にお越しの際はお試し下さい。

■文献（サイト閲覧日は2025年5月29日）

- (1) 福岡市役所, “福岡市.” <https://www.city.fukuoka.lg.jp/soki/tokeichosa/shisei/toukei/jinkou/jinnkousokuhou.html>
- (2) 福岡市博物館市史編さん室, “福岡市史.” <https://www.city.fukuoka.lg.jp/shishi/>
- (3) 福岡市経済観光文化局, “福岡市歴史文化情報データベース.” https://bunkazai.city.fukuoka.lg.jp/cultural_datas/
- (4) article.bespes-jt.com, “福岡城について.” <https://article.bespes-jt.com/ja/article/fukuoka-castle>
- (5) 宮崎宮, “宮崎宮の歴史.” <https://www.hakozakigu.or.jp/history/>
- (6) 名島神社, “由緒・歴史-【公式】福岡市東区名島にある名島神社.” <https://najima-jinja.com/about/history>
- (7) 山崎好裕, 近代経済社会の形成と顕幽二元論の成立：産須那神概念を媒介に、福岡大学先端経済研究センター, 福岡市, 2021.
- (8) 福岡市経済観光文化局, “福岡市の文化財.” <https://bunkazai.city.fukuoka.lg.jp>

石田俊一（正員）

九州産業大学理工学部情報科学科准教授。平15愛媛大・理・数理卒。平15同大学院修士課程了。平21九大大学院システム情報科学府了。平21北九州大基盤教育センター助教。平22九州産業大基礎教育センター講師。平26同准教授。平29同大学理工学部情報科学科准教授。情報学基礎理論、セルオートマトンに関する研究に従事。博士（理学）。



サイバーセキュリティ政策の現在と 通信ネットワークに対する取組みについて

総務省サイバーセキュリティ統括官室

梅城崇師 Takanori Umeki

1 はじめに～サイバーセキュリティをとりまく状況～

デジタル化の進展により、私たちの生活や経済活動のあらゆる側面が通信ネットワークに支えられている。社会インフラの多くもネットワークにつながっており、利便性の一方で、サイバー攻撃の脅威に日常的にさらされている。

実際に国立研究開発法人情報通信研究機構（NICT: National Institute of Information and Communications Technology）の観測⁽¹⁾によれば、2024年に観測されたサイバー攻撃関連通信はIPアドレス一つ当たり約242万パケットに達し、約13秒に1回攻撃が届いている計算となる。これは2014年の約20倍に当たり、増加傾向が顕著である。

また、サイバー攻撃は巧妙化・深刻化しており、単なるWebサイトの改ざんや情報漏えいにとどまらず、社会インフラに影響する事例も相次いでいる。米国の石油パイプライン企業のほか、国内でも医療機関や港湾施設での業務停止など、実社会への影響が生じている。

更に、国家主体の関与が疑われる高度なサイバー活動も顕在化している。ウクライナ侵略時にはインフラ侵入や情報操作が行われたとされ、2023年には米軍施設や重要インフラに対する長期的な侵入事例が報告されている。

加えて、政府関係機関等への不正アクセスなど、機微情報の窃取を目的としたサイバー攻撃も後を絶たない。

このように、量・質の両面でサイバー攻撃の脅威は増大しているのが現状である。

2 政府におけるサイバーセキュリティ対策

我が国における政府のサイバーセキュリティ対策の歴史は、2000年にまで遡る。当時、急速に普及していたインターネットを背景に、2000年1月には中央省庁

のホームページが相次いで改ざんされる被害が発生した。政府として情報セキュリティの強化を一丸となって実施することが求められ、翌月には「内閣官房情報セキュリティ対策推進室」が設置され、政府としての取組みが始動した。

その後、2014年、我が国のセキュリティ対策について画期的な節目となる「サイバーセキュリティ基本法」が成立した。同法に基づいて「サイバーセキュリティ戦略本部」及び「内閣サイバーセキュリティセンター」が設置され、組織体制が法律上の根拠を持って体系的に整備された。また、「サイバーセキュリティ戦略」が政府として最高意思決定手続きである閣議決定文書として策定されることとなった。なお、法令で「サイバーセキュリティ」という用語が用いられたのもこの法律が初めてである。

そして2025年5月、昨今のサイバー攻撃の脅威の増大に対応するため、「サイバー対処能力強化法及び同整備法」が新たに成立した⁽²⁾。この法律は、いわゆる能動的サイバー防御（ACD: Active Cyber Defense）の実現を目的としており、国民生活や経済活動の基盤並びに国家及び国民の安全を、サイバー攻撃から守るための新たな防御体制を整備するものである。具体的には、重要なインフラを担う事業者と政府との間の情報連携を強化するとともに、攻撃サーバなどを検知するため通信情報の活用が法的に認められた。サイバー攻撃の全容を把握することが可能となり、攻撃サーバの無害化なども法的に実施できることとなった（図1）。

能動的サイバー防御は、攻撃を未然に防ぎ被害を最小限に抑える新たな対応策である。これにより、我が国のサイバーセキュリティ政策は新たな段階に入り、進化する脅威に対して柔軟かつ迅速に対応できる体制が整いつつある。

「能動的サイバー防御」NEW 3ポイント!

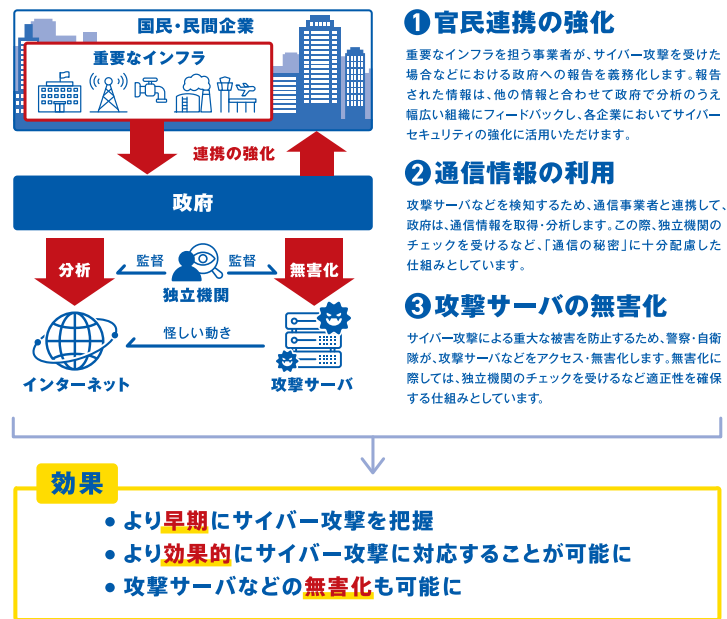


図 1 能動的サイバー防御の概要

(出典：内閣官房「サイバー安全保障に関する取組」リーフレット資料から抜粋)

3 総務省におけるサイバーセキュリティ対策

3.1 サイバーセキュリティにおける総務省の役割

こうした政府全体のサイバーセキュリティ対策の中で、総務省は、情報通信ネットワークを所管する立場として重要な役割を担っている。

情報通信は、機能停止すれば国民生活や経済社会に甚大な影響を及ぼす「重要インフラ」を構成する15分野（金融、電力等）の一つに位置付けられているが、ほかの分野とは異なる特性を有している。すなわち、情報通信が、サイバー攻撃が日々飛び交う「サイバー空間」そ

のものであり、その安全を確保することが、ほかの重要インフラ分野のみならず、国民全体の安全にも直結するという点である。

総務省では、こうした情報通信、ひいてはその利用者をサイバー攻撃から防御するため、情報通信分野を専門とする我が国唯一の国立研究開発法人であり、サイバー攻撃に関する観測・分析を長年にわたり実施し、高度な技術力等を有するNICTと緊密に連携するとともに、そのほかの関係機関とも協力して、多様な取組みを推進している（図2）。以下に具体的な取組みの一部を紹介する。

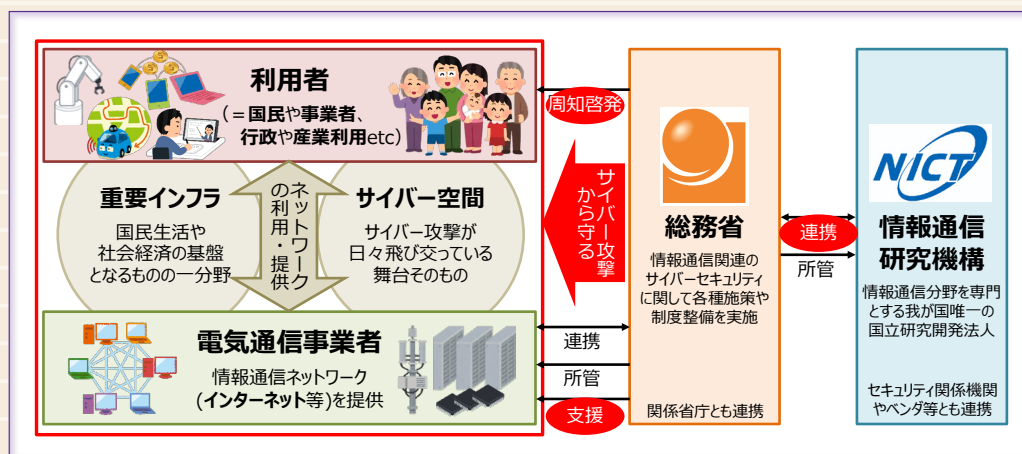


図2 サイバーセキュリティにおける総務省の役割

3.2 DDoS 攻撃対策—ネットワークに根差す脅威への対応

近年、様々な機器がインターネットに接続されるようになり（これらは一般に IoT（Internet of Things）機器と呼ばれる。）、セキュリティ対策の甘い IoT 機器を踏み台にした攻撃が多く発生している。総務省では、IoT 機器を用いた攻撃の中でも特に、標的となるサーバ等に処理能力を超える大量の通信を送りつけることで、当該サーバを利用不能にする攻撃である DDoS 攻撃（分散型サービス不能攻撃：Distributed Denial of Service attack）対策に取り組んでいる。

DDoS 攻撃は、標的に大量の通信を送りつけるため、標的だけでなくネットワーク全体の速度低下を引き起こし、標的以外のほかの利用者にも影響を及ぼし得ること、そして、標的に大量の通信を送りつけること自体が攻撃手法であるため、標的側のみでの対応が困難な場合もあり、ネットワーク側での対策が求められることがある。

そのため、総務省では、電気通信事業者等と連携し、DDoS 攻撃手法に着目した二つの側面から対策を講じている（図3）。

3.2.1 C&C サーバへの対策

攻撃者は、大量の IoT 機器に対し、自身の身元を隠すため、直接指令を出さずに、C&C（Command & Control）サーバと呼ばれる中継サーバを介して攻撃を行う。この C&C サーバを封じ込めることが、効果的な対策となる。

そのため、複数の電気通信事業者と協力して、電気通信事業者が自身のネットワーク管理のために利用するフロー情報（IP アドレスやパケット数などに関する情報）

を分析して C&C サーバを検知し対策に活用するための実証事業を 2022 年から進めている。

3.2.2 ぜい弱な IoT 機器への対策（NOTICE プロジェクト）

サイバー攻撃に悪用されるおそれのある、ぜい弱な IoT 機器についても対策を行っている。

具体的には、高度な技術を有する NICT において、国内の IoT 機器を調査して、既にマルウェアに感染したものやファームウェアにぜい弱性があるもの、そして容易に推測され得る ID・パスワードを利用しているものを特定している。また、特定した IoT 機器の利用者に対して、電気通信事業者を通じて注意喚起を行い、セキュリティ対策を促している。この一連の取組みを「NOTICE（National Operation Towards IoT Clean Environment）」プロジェクトと呼び推進している。

なお、この NOTICE プロジェクトを実施するためには、実際に容易に推測され得る ID・パスワードを、調査対象の機器に入力して結果を確認するという行為が必要である。これを一般に行うと不正アクセス禁止法に抵触することから、NICT が総務大臣の監督の範囲でのみ、これを行うことができるよう、2018 年に関連法の改正を行った上で実施している。

3.3 電気通信事業者への支援

インターネットは、歴史的に、信頼できる相手との接続を前提としてきた経緯があり、そこで用いられている通信プロトコルには、構造的なぜい弱性が残されている。これにより、通信経路の乗っ取りや、送信元を偽装した「なりすましメール」などの問題が生じやすい状況にある。

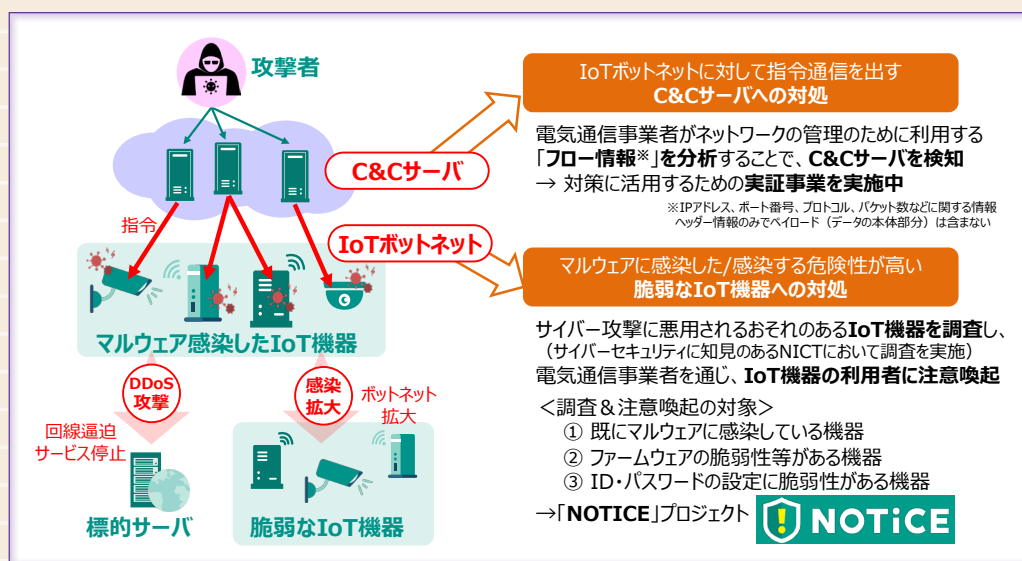


図3 IoT 機器を悪用したサイバー攻撃（DDoS 攻撃等）への対策

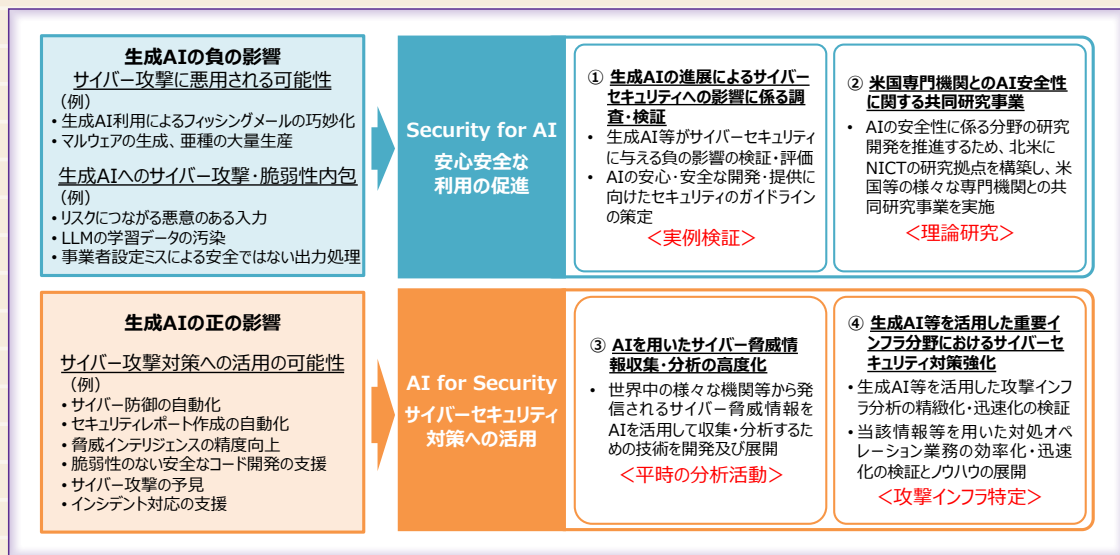


図4 AIとサイバーセキュリティ

これに対し、電子認証技術を活用することで安全性を高めるための新たなプロトコル（DMARC、DNSSEC、RPKI）が、国際的に標準化されてきており、技術的な基盤は整いつつある。しかしながら、導入に掛かるコストや技術的なノウハウの不足といった課題から、国内での導入は必ずしも十分に進んでいないのが現状である。

このため、総務省では技術ガイドラインの策定や、設定方法に関する講習などを通じて、電気通信事業者等に対して、こうしたプロトコルの導入を後押ししている。

3.4 通信利用者への支援

通信の利用者自身の安全を確保することも極めて重要な課題である。総務省では、無線 LAN やテレワークのセキュリティに関するガイドラインを 2004 年から整備している。その後も、技術進展や脅威の変化に応じて継続的に見直すなど、早い段階から利用者視点でのセキュリティ対策に取り組んできた。

特に、コロナ禍に伴い急速に普及が進んだテレワークに関しては、専門的な知見を持つ人材に限られる中小企業でも、現実的かつ確実なセキュリティ対策を実践することが必要である。そのため、チェックリスト形式の手引きや設定マニュアルを整備し、現場の負担を軽減しつつ安全なテレワーク環境の構築を支援している。

3.5 AI 技術への対応

昨今の AI 技術の進展は、サイバーセキュリティの在り方にも大きな変化をもたらしている。生成 AI のサイバー攻撃への悪用といった新たなリスクが顕在化している一方で、年々増加するサイバーセキュリティ対策業務の負荷軽減に生成 AI（人工知能）等の利活用が期待されている。

こうした状況を踏まえ、総務省では、AI に起因するリスクを最小限に抑えるための「Security for AI」と、AI を積極的にセキュリティ対策に活用する「AI for Security」の双方に取り組んでいる（図 4）。

4 おわりに

社会のあらゆる活動が通信ネットワークに依存する中、その安全性を確保することは国民生活と経済活動を支える基盤として極めて重要である。総務省としても、情報通信ネットワークの所管官庁として、関係機関と連携しながら不断の対応を続けていく。また、進展する技術と脅威の変化を的確に捉え、柔軟かつ実効的なサイバーセキュリティ政策の実現にこれからも不断に取り組んでいく。

■ 文献

- (1) 国立研究開発法人情報通信研究機構，“プレスリリース，NICTER 観測レポート 2024 の公開.” <https://www.nict.go.jp/press/2025/02/13-1.html>
- (2) 内閣官房，“リーフレット，サイバー安全保障に関する取組.” https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/

梅城崇師

2007-04 総務省採用。総務省において通信・放送・電波行政に従事し、内閣官房内閣サイバーセキュリティセンター、デジタル大臣秘書官を経て、2024-10 総務省サイバーセキュリティ統括官室にて統括補佐、2025-07 から同室企画官としてサイバーセキュリティ政策に従事。



私の留学 サンタさんのいる国へ

若者よ、
世界に
出よう！



オウル大学大学院 西尾美哉 Miya Nishio

1 はじめに

フィンランドにあるオウル大大学院 Wireless Communications Engineering（無線通信工学）に在学中の西尾美哉です。2024年9月から留学を開始し、現在、修士課程1年目を終えたところです。

留学先として若干メジャーではないフィンランドをなぜ選んだか、留学前に得た少ない現地情報からフィンランドに入ったため、実際に現地で感じた戸惑い、楽しみなど、まだまだ学びの真っ只中ですが、母国から一歩踏み出したからこそ得られたことをつづてみます。

2 留学までの流れ

学部時代は日本で工学部に所属していましたが、無線通信とは関係ない分野を学んでいました。（卒論はAIの応用についてです。）大学院への進学は考えていたものの、どのような分野に進みたいかの決断ができていなかった学部3年の終わりに、大学の教授から勧められたスイス・ジュネーブにある国際電気通信連合（ITU）という国連組織で半年のインターンシップを行いました。

そこで初めて通信の分野、特に通信の標準化について知ることになり、大学院では無線通信を学ぶことを決意しました。

元々ヨーロッパで一度は勉強してみたいという思いがあったため、そしてオウル大は無線通信に強いという教授からのアドバイスもあり、フィンランドへの留学を決めました。

ビザ取得は至ってシンプルで早く、レジデンスもPSOASというフィンランドの会社が学生用にアパートを管理しているため、特に問題なく予約することができました。ジュネーブでのインターンの際には、トラブルで一度『家なき子』ならぬ、「家ナシ子」状態になっていたため、取りあえず屋根のあるところに住むことがで

き一安心でした（図1）。

フィンランドのオウルには7月に到着、早めに引越しや手続きを開始しました。8月末の学期開始直前に来る学生も多いのですが、日本国籍保持者にはシェンゲン協定加盟国における「3か月のビザ免除」が適用されるため、早めに渡航し、余裕を持って引越しすることをお勧めします。

先にスムーズにアパートを借りることができたと思いましたが、小さな町であるオウルも、7、8月になるとレジデンスの取り合いのような状況になってしまうそうです。

3 大学生活

大学のカリキュラムとしては1年目に座学、夏休み



図1 現在住んでいるアパート。3人でのシェアですが、共有はキッチンのみで冷蔵庫も3人分あり、色分けされています。

中にインターン、2年目に残りの座学と修論で構成されています。

無線通信の分野を学ぶことが初めての私にとって、アンテナ、無線チャネルなど、学部で学ぶべきことを補いながら講義を理解していくことはとても大変です。コロナ禍の際の大学の対応として、2、3年前の授業の録画を視聴することが可能であったため、授業に出席した後、録画を視聴して復習をすることの繰り返しでした。

また、ジュネーブでのインターンから帰国した後、日本の標準化団体で手伝いをする機会を頂き、標準化会合に出席するために1〜2か月に1回は外国に渡航しています。仕事を続けながら、慣れない地で、初めての分野の学問に取り組む1年目は、本当に「毎日が大変」の連続でした。

四苦八苦の日々とは言え、「海外で学ぶこと＝オウル大」の良いところは大きく三つあると強く感じています。

まずは、授業が常に「グローバルな視点」であることです。

例えば、どの授業でも教授は通信の標準について話します。通信はどうしてもグローバルな活動になるので、技術者、そして研究者だとしても、ITUや3GPPでできていく「標準」を意識しながら活動を進める必要がある、ということを教わります。特に、標準化活動に携わっている私にとって、学んでいることがどのように仕事とつながっていくのかが分かり、大変興味深いと感じています。

次に、手厚いキャリアサポートがあることです。

海外からの学生も多いことから、大学・大学院卒業後の就職活動に手厚いサポートがあります。数か月に1回はキャリアイベントがあり、担当の教授との面談を通して今後の仕事についての考えも聞かれます。

また、このようなサポートがあるからこそ、学生が仕事をしていることに対して寛容であり、そのことで私も現在の生活を乗り切れていることが大きいと感じています。

そして最後に、企業との連携が強いことです。

Nokiaのプレゼンスが大きく、キャリアイベント以外でも企業との連携講義やイベントも多いです。講義でも企業の方が担当することもあり、常に、インダストリーのことを考える機会が与えられます。

何のために勉強、何のために研究していくのか、ということがはっきり分かるため、モチベーションにもなりますし、自分の中で、どのように学問を進めるべきかの明確化にもつながっています。

4 学問以外での大学生活

さて、勉強以外でも学びが十分あります。

北欧では学科別に色が違うオーバーオール（つなぎ、図2）を着る文化があり、学生イベントに参加するたびにパッチ（ワッペン）をもらうことができます。そのたびにそのパッチをオーバーオールに縫いつけていきます。

イベントは様々ですが、特に衝撃的だったのが、「WCOK」というイベントで、Kyykkäという昔ながらのスポーツゲームを行います（図3）。

Kyykkäは二つのチームに分かれて、テニスコートより一回り小さい場所で、Karttu（野球のバットみたいなもの）を投げて、真ん中に置いてある20個ほどのKyykkäs（木のブロック）に当て、相手の陣地に入れるというゲームです。Kyykkäsも縦横20cmないので、Karttuをゴルフクラブのように振り回し、地面に滑らせながらKyykkäsを当てる必要があります。私も経験のために投げてみましたが、なかなか正確に投げられませんでした。

友人のチームが参加していたので、3月に、まだ凍っている大学の駐車場で震えながら観戦しました。そこで



図2 オーバーオール（つなぎ）



図3 Kykkä ゲーム

衝撃的なのが、何とプレーヤも観客も片手に缶コーヒーを持っていると思いきや、朝9時から片手にビールでのゲーム参加。

どのチームもプレーしなくてはならない「暗黙の」学生ルールもあり、結局は私もプレーをすることになりましたが、ゲーム中に人が振り回す Karttu に当てられないように走り回るばかりで、(残念ながら?) ビールを飲んでいる暇はありませんでした。

慣れないゲームへの飛び入りでしたが、日照時間の少ない極寒の中で気軽にスポーツを楽しむ、「これぞフィンランドの学生生活」に参加したことで、気候と環境によって人の生活様式も大きく影響を受けることが体感できました。

これから留学される方には、是非、地元の学生のコミュニティに積極的に参加して頂くことをお勧めします。勇気も必要ですし、驚くことも多いですが、「郷に入っては郷に従え」は楽しみを倍増させる方法の一つだと確信しています。

余談ですが、パッチはイベント以外でも観光地などで売られています。フィンランドには41か所の国立公園があり、各公園でパッチが売られているため、スタンプラリー好きの私は、それを全て制覇することに現在挑戦中です。

5 太陽「いすぎ」・「いなさすぎ」問題



オウルは北緯 65 度に位置しているため、冬は寒く、太陽が出ません。

11 月頃から太陽の沈みが早くなり、12 月には日の出が 10 時頃、日の入りが 14 時半頃で、太陽が上がっても 1 日中夕方みたいな空です。

そんなときに見ることができるのがオーロラだ! と思い、フィンランドを更に北上、素晴らしいグラスドームのホテルを予約し、夜中ずっと星空を観察するという事に冬の間に何回か挑戦しましたが、運悪く、なかなかオーロラを見ることができませんでした。

しかし、3 月のある日の夜、小腹が空いてオウルの近所のスーパーに買い物に出たら、今までに一度もはつきりと見たことがなかった、鮮明な青緑のオーロラを目にしました(図4)。写真では伝えられないほどの大きさで、金魚が泳ぐような穏やかな動きで空を横切っていました。寒くて外に立ち止まっていられないはずが、口をポカーンと開けたまま 5 分、10 分、見ほれてしまいました。

その後、どうしてもまた見たい! という欲望で今までの旅行よりも更に北上し、2泊しましたが、見る事ができませんでした…。

現在は 6 月。冬とは逆で今度は太陽が沈みません。



図4 3月，オウル市内で見たオーロラ

先日、日の出が3時，日の入りが23時半でした。夜といっても大変明るい夜です（図5）。

それでも日の入りは更に遅れる予定で，ピークは6月20日頃と言われております。

明るくて明るくて，うれしいものの，ちょっとは暗くてもいいかなと…。

太陽で気分が翻弄される毎日です。



図5 6月上旬，23時47分の様子

オウルはそんな印象が特に強く感じられる場所でありながら，テクノロジーをしっかりと学べる場所でもあります。学問が大変でも，仕事が大変でも，学生生活にびっくりしながらも，太陽が昇り続けていたり，1日中真っ暗でも，オウルで学べてよかったと思いながら，残りの留学期間にはもっと大きな学びと発見を期待してやみません。

6 サンタさんとムーミンに抱かれて

サンタさんの村があり，ちょっとシニカルで自然の中で繰り広げられる妖精ムーミンのストーリーを生んだフィンランドの地。「自然」と「人々の生活」と「フェアリーテール」が不思議と違和感なく織りなされているような気がしています。

西尾美哉

2024 東大・工卒。学部在学中 ITU でのインターンシップに参加したことから国際標準化活動に興味を持ち，2025 現在はオウル大大学院 Wireless Communications Engineering（無線通信工学）修士課程に在籍中。学業を続けながら引き続き，ITU の活動や電気通信技術委員会（TTC）における標準化会合の出席とサポートなどの仕事にも携わっている。



研究とエンジニアリングの間で

大橋正良 (正員：フェロー)

1983 京大大学院了。同年国際電信電話株式会社 (現KDDI) 入社。KDDI 研究所にて主として移動体衛星通信、符号理論、セキュリティの研究に従事。その後、第3世代移動通信システムの研究開発・標準化、ユビキタス・センサネットワークの研究開発に従事。KDDI 研究所執行役員を経て、2008 ATR メディア情報科学研究所所長。2011 ATR 適応コミュニケーション研究所所長。2013 福岡大工学部電子情報工学科教授。2024 同名誉教授／ATR 適応コミュニケーション研究所連携研究員／(株) オプテージ社外監査役。工博。電子情報通信学会、情報処理学会、IEEE ライフメンバー。電子情報通信学会において、2008 USN 研究会専門委員長、2013 B-plus 編集委員長、2016 IT 研究会専門委員長、2019 基礎・境界ソサイエティ副会長、2021 同会長、2024 同編集長、2025 企画理事を歴任。1990 年度本会学術奨励賞受賞。



福岡大学名誉教授
大橋正良
Masayoshi Ohashi



1. はじめに

B-plus では従前「私の技術者歴」と「私の研究者歴」の二本立てで掲載がされていたが、最近では「私の研究者歴」に統一されたと伺った。自分は若干の研究歴もあったが、振り返ってみれば圧倒的に通信エンジニアとしてのキャリアを歩んできたんだな、と感じる。

私は恐らくほかの方々、特にこの研究を追求してきました、という生粋の研究者の方々に比べ、多様な経歴を歩んできたと思う。本稿では大学時代から現在に至るまでの私のキャリアについて、エピソードも交えて紹介したい。

結論から言えば、自分が歩んできたキャリアは、主として企業や社会の要請に応じて柔軟にテーマを変えてきていたが、それは、今から思えば自分の信念で研究を貫くのと裏腹に、時代が動くとともに移り変わるものだった。



2. 1980年代: 衛星通信と符号理論

学生時代私は、京都大学工学部電気第2工学科において木村磐根教授の下で、卒業研究として宇宙プラズマの観測結果を解析した。修士課程では宇治キャンパスの加藤研究室に所属したが、実質松本紘助教授(当時)に就き、宇宙プラズマの計算機シミュレーションを行った。今では超小規模になるが、

当時は名古屋大学プラズマ研究センター(プラ研)にしばしば籠って、16 MByteのメモリを駆使してバッチジョブを繰り返し、最後に二次元のプラズマ波伝搬を首尾良くシミュレートできた。これで無事修士論文が完成し、松本先生はその後この結果を論文にして下さった。

その後、KDD(国際電信電話株式会社、現KDDI)に入社した。博士課程への意図がないことを松本先生に告げると同社を推薦して頂いた。初めKDD 茨城衛星通信所に配属された(図1)。同通信所は日本の衛星通信発祥の地として知られており、当時、山口衛星通信所と並び、衛星を介した日本の



図1 当時の KDD 茨城衛星通信所

国際ゲートウェイの役割を担い、運用／保守合わせ当時 100 名程度のエンジニアが従事していた。その頃会社には新入社員は 2, 3 年現場で経験を積み、というポリシーがあり、結果的に私は約 2 年間、管理・保全・運用など一通りの業務を経験させて頂いた。研究所で研究を始めたい気持ちも大きかったが、思えば貴重な運用経験を積んだ。今でもきっと衛星通信のオペレーションはできると思う。

1984 年に東京・恵比寿にあった KDD 研究所に移った。所属は衛星通信研究室で、移動衛星通信を所轄し、平田康夫氏が室長だった。当時は海事衛星通信サービスを提供していたインマルサットがデジタルシステムに移行するフェーズで、それに向けた研究開発が行われていた。私は誤り訂正符号化の研究をやればどうかと言われ、安田豊氏の下で衛星通信に適した誤り訂正符号化・復号技術の研究をさせて頂いた。安田氏はそれまでも畳込み符号化／パンクチャド復号の提案等の実績を持たれ、大きな刺激を受けてきた。

研究内容としては、当時衛星通信には畳込み符号化／ビタビ復号に必要な応じてリードソロモン符号を接続した方式が主に検討されていた。それでそれに代わる方式の候補として畳込み符号化／逐次復号方式をテーマとして薦められ、本研究にしばらく取り組んだ。逐次復号では、符号によって構成される木（通常 2 分木）を基に受信側で蓋然性の高い枝（受信語と相関の高い符号語）を探索する必要がある。この枝が明確に判別できるよう符号器の長さに対応する拘束長と呼ばれるパラメータを長くする必

要があり、ビタビ復号のような最ゆう復号の適用は事実上不可能であった。そのため、ヒューリスティックに最ゆうに近い特性を得られるようなアルゴリズムを工夫するとともに、復号特性を左右する列距離関数特性に優れた畳込み符号の構成と探索アルゴリズムも検討し、高符号化率符号も含め良い符号を探索できた。復号においてもスタックを活用して有望な候補のみを伸長させ、ほかの枝をリアルタイムに削って連続的に復号するアルゴリズムを考案した⁽¹⁾。

当時研究所では、それまでハードウェアはベンダに試作を依頼し、それを用いて性能を評価するのがごく一般的だったが、当時、画像符号化グループを中心としてハードウェア化／ASIC^{*1}化が積極的に進められつつあった。その流れの中で、自分の研究テーマも良い方式ならそれを ASIC 化せよ、と（簡単に）言われた。右も左も分からぬ研究者にいきなり ASIC 作れ、と言われても無理な話で、ベンダに飛び込んで設計ツールを買い求めたいと聞いても、「あんたこれで何個量産するつもりですか？ 目論見もなくやっても意味ないですよ」と追い返された。

どうしようと思っていた中、FPGA^{*2}という手があると教えられた。ちょうど代表格の XILINX が世に出てきて数年後のことだった。開発環境をそろえ、一から論理設計を学び、回路図を設計して

- * 1 Application Specific Integrated Circuit: 特定用途用半導体。
- * 2 Field Programmable Gate Array: プログラム可能な論理回路デバイス。

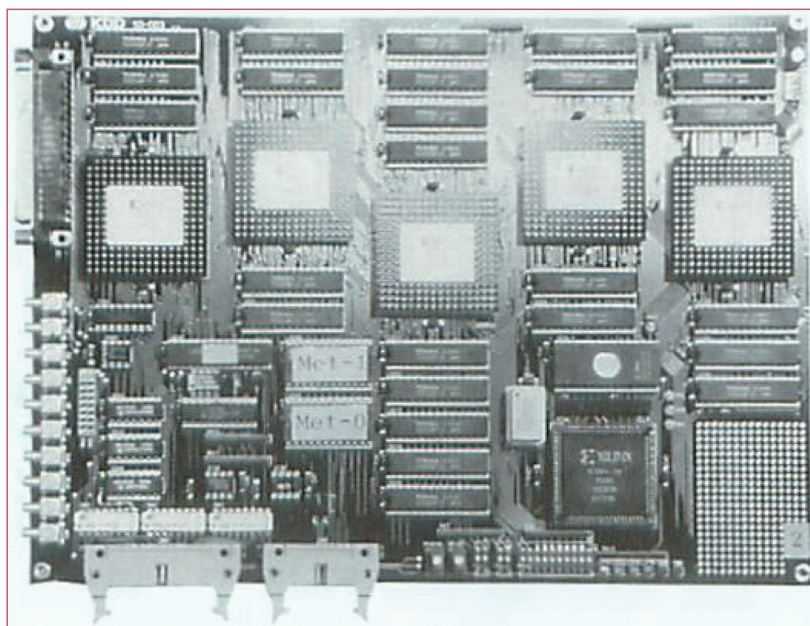


図 2 逐次復号 FPGA ボード

ROMに焼いてはロジックアナライザで動作を検証するデバッグの毎日だった。少なくとも周辺で独自にFPGAハードを設計製作していたのは自分たち以外いなかった。結果数多くの困難に出会いながらも、ほぼ1年余りで逐次復号ボードが完成した(図2)。復号速度は64 kbit/s程度しか出なかったが、実現できた符号化利得は特に高符号化率において他の方式を凌駕していた⁽²⁾。今振り返れば、木構造を基にゆう度の高いシーケンスをリアルタイムで連続的に出力し続けるのは、一種の推論エンジンだったと思う。

ハードウェア化も一息ついた段階で、今では当たり前であるが、誤り訂正後のシンボルの確度を出力できないかということ考えた。当時幾つかの試みが報告されていたが、有効性は十分ではなかった。そのような中BCJRアルゴリズム⁽³⁾に注目し、これを利用して事後確率最大化復号(MAP)を行えばシンボル確度を出せるかもしれないと考えて評価していったところ、伝送路の事前分布さえ分かれば、かなり良い精度でシンボル確度を出せることが判明し、論文となった⁽⁴⁾。復号時の確度を利用するのはその後のターボ符号、LDPC符号の復号でも重要な一構成要素であり、符号理論の発展にも僅かに貢献できたか、と感じている。

この後、伝送信号処理グループに配属された。何をやっていいのかよく分からない部分もあったが、当時セキュリティをやれと言われ、何か貢献できることはないかと考えていた。後に述べる欧州標準第2世代移動通信システムGSM(Global System for Mobile communications)とのインタワークの検討の中でSIM的なものを活用すべきと、1995年にICカードを用い、Kerberosタイプの分散認証スキームに基づき、認証の後にアプリケーションを提供する仕組みを試作した⁽⁵⁾。ちょうどWindows 95にTCP/IPが標準で搭載が始められた頃で、インターネット上で安全にサービスを提供しようとの意図で開発を進めた。当時スマートカードを製造販売していたGemplus社からドライバ等の面からもサポートを受けた。見掛けも良く、これは役に立つだろうとSmart Passと名前を付け商標も取ったが、社内では評価を得るも、実際には鳴かず飛ばずの結果となった(図3)。今マイナンバーカードが国民に与えられて認証が必須になったのを見るに、世の中は変わったと思う。

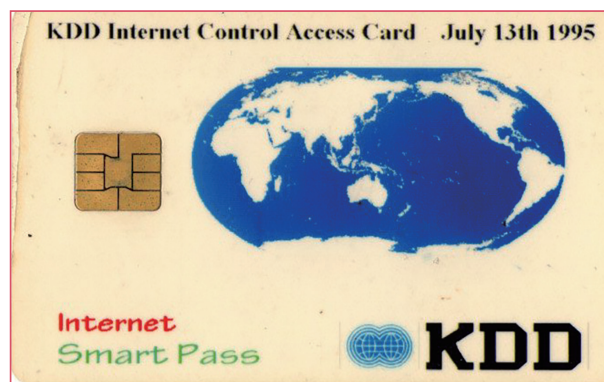


図3 Internet Smart Pass



3. 移動衛星通信のフィールドエンジニア

1980年代から90年代にかけ、衛星通信研究室では次世代のデジタル移動通信システム実現に向けたフィールドトライアルが活発に行われていた。海事衛星通信ではスタンダードBシステムの導入に向けた評価として「東海大学丸II世号」を用いて幾度か船舶通信実験が行われた。私は通信所従事経験もあったせいか、主に山口衛星通信所にて陸側のオペレーションを担当した。船舶から発せられるCW搬送波(クリーンキャリア)を準同期検波してA-D出力をリアルタイムでデータとして取り込み、海上伝搬路の特性を取得していた。

ある大しけの日、船が左右に40°ぐらい傾き、船側のメンバがほぼ全員船酔いでダウンしていた際、オシロスコープを見ていると観測信号が急にゆっくりと右回転を始め、そのうち止まり、今度は左回転を始めて止まり、これが繰り返される現象を観測した。何だと思って船側と話をすると、それは船の傾きと同期していた。ドップラーだ。衛星を介して陸側で船の傾きが観測されたのが実に面白かった。

当時、国では技術試験衛星「きく5号」(ETS-V)を用いた衛星通信実験が活発に行われており、我々もこれに参加し、イベントの都度、機材を一式現場に運びアンテナも設置して、実証実験/デモを続けた。これを通じ機材の梱包・開梱が実に手際良く行えるようになった。また、本経験を通じてエンドのPCや通信端末からベースバンド/RF/アンテナまで全て通じて設置・運用できる能力も身に付いた。電気通信大学に行かれた唐沢好男先生らとも御一緒にセスナ機にアンテナを設置し、主に大阪・八尾空港を使って試験飛行を繰り返し、航空通信伝搬データを取得した。

KDDがJALと共同で実施した航空衛星通信実験⁽⁶⁾にも協力した。幾度か太平洋路線のJAL機に

搭乗し、通信実験を行った。ファクシミリやデータ伝送は研究所側の担当だったが、当時 OSI プロトコルが実際に使われていたことを覚えている。エピソードを一つ挙げると、世界からメンバを集めた JAL のミーティングが東京の帝国ホテルであり、茨城衛星通信所を介して太平洋飛行中の JAL 機とリアルタイムで通話する企画があった。私は茨城衛星通信所で中継業務を担当した。ところが前日のリハーサルがごとく失敗、成田駐機の機材も米国に飛んで行ってしまった。衛星折り返しも地上折り返しも問題ないのに、地上—衛星の中継で失敗する。茨城が原因なのは明らかだった。徹夜のデバッグを覚悟したが、通信所の若手の技術者が私の説明を聞いて思わず衛星系と地上系をつなぐ某社手作りの RS232C コードを抜いて中を開けたところ、はんだが 1 か所取れていた！ はんだをつけ直して接続 OK となり、航空機帰路の本番も（私にとっては劇的に）社長とパイロットとが無事会話ができた。当時、航空衛星通信はまだ実用化されていなかったため、会場からはそのデモの真偽を疑う声もあった、と伺った。



4. 1990年代から2000年はじめ： 第3世代移動通信(3G)の開発と標準化

KDD は当時、国際通信事業者であり、中継業務が専担であったことから、エンドユーザを獲得することは同社の悲願であった。その一環として、KDD は日本テレコムと共同で PHS^{*3} の実証実験を実施することとなり、他社と比較して小規模ながら 1993 年に札幌で実証実験を行った。私もチームメンバと一緒に札幌駅付近で基地局設置とシステム運用を含め実験を数か月実施した。その甲斐もあってか、KDD も最終的にアステルグループの一員として参加できることになったのは良いニュースだった。

そうしているうちに 1990 年代後半に入り、日本として世界をリードして第 3 世代移動通信 (3G) を提案・標準化していこう、という気運が高まった。私はほかの多くの無線の研究者・技術者とは異なり、サービス／ネットワークの視点で検討・標準化に従事した。

初期は電波産業会 (ARIB) で 3G (当時は「FPLMTS」と呼ばれた) のサービス検討に携わった。久保田主査から幾度も 3G らしいサービスを考

え出して下さい、と言われていたものの、誰も余り提案できるものはなかったと記憶している。それはある種当たり前で、当時は貴重な通信資源をビジネス用途以外に浪費するのは誰も考えられなかったからである。

その後、情報通信技術委員会 (TTC) で 3G ネットワークの検討に携わることとなった。NTT / ドコモは当時 IN (Intelligent Network) を基盤にした 3G ネットワーク実現を狙っており、その協力を KDD にも期待していたが、IN 自身が将来なく消えていった。無線分野の ITU-R のようには注目されていなかったものの、私自身はここを基盤に ITU-T SG11 における IMT-2000 標準化作業に寄与し、ネットワーク標準のため、特にハイレベルポリシーの面から日本寄書を積極的に提出し、世界初の IMT-2000 ネットワーク標準 ITU-T Q.1701⁽⁷⁾ の策定に寄与することができた。

そうした中、3G の標準化体制の検討にも関わらせて頂き、現在の 3GPP と 3GPP2 の標準規格策定体制が創設された。私自身は TTC において、当時、国内ネットワーク標準は唯一規格しか認められてこなかった中、欧州標準 GSM ベースの 3GPP 網と米国標準 ANSI ベースの 3GPP2 網の併存が不可避な IMT-2000 網標準スキームの枠組み作りに取り組んだ。KDD が DDI と合併する中で、私は 3GPP2 において TSG-N (ネットワーク) に参加するとともに、後に作られた TSG-S (サービス) セキュリティ WG の副議長を数年務めた。TSG-N においては、当時 3GPP にはあったものの、3GPP2 ネットワークでは規定されていなかった SIM (UIM) の標準化を行うべく、小職名にて TTC から標準案を提出した。初め採択されなかったが、後に中国からの要請を受け、本案ベースで検討が進み、最終的に C.S0023⁽⁸⁾ として標準化された。CDG (CDMA Development Group) からも感謝の楯を頂戴した。

3G 標準化が一段落する中、欧州では次世代システムを検討するフォーラム WWRF (Wireless World Research Forum)⁽⁹⁾ が創設されるなど次世代システムへの指向も高まり、日本においても mITF (mobile IT Forum) が設置された。そこで多くのメンバが次世代無線システムの議論に参加する中、私はサービスプラットフォーム WG の主査に着任した。

WWRF が次世代ビジョンの白書をいち早くリリースしてきており、日本としても自分たちのビジョンを固める必要があるとして、mITF では国内事業者・国内外ベンダを集め 1 年半ほど定期的に検討

* 3 Personal Handy-phone System: 第2世代デジタルコードレス電話

Service Platform Reference Model : Advanced Service

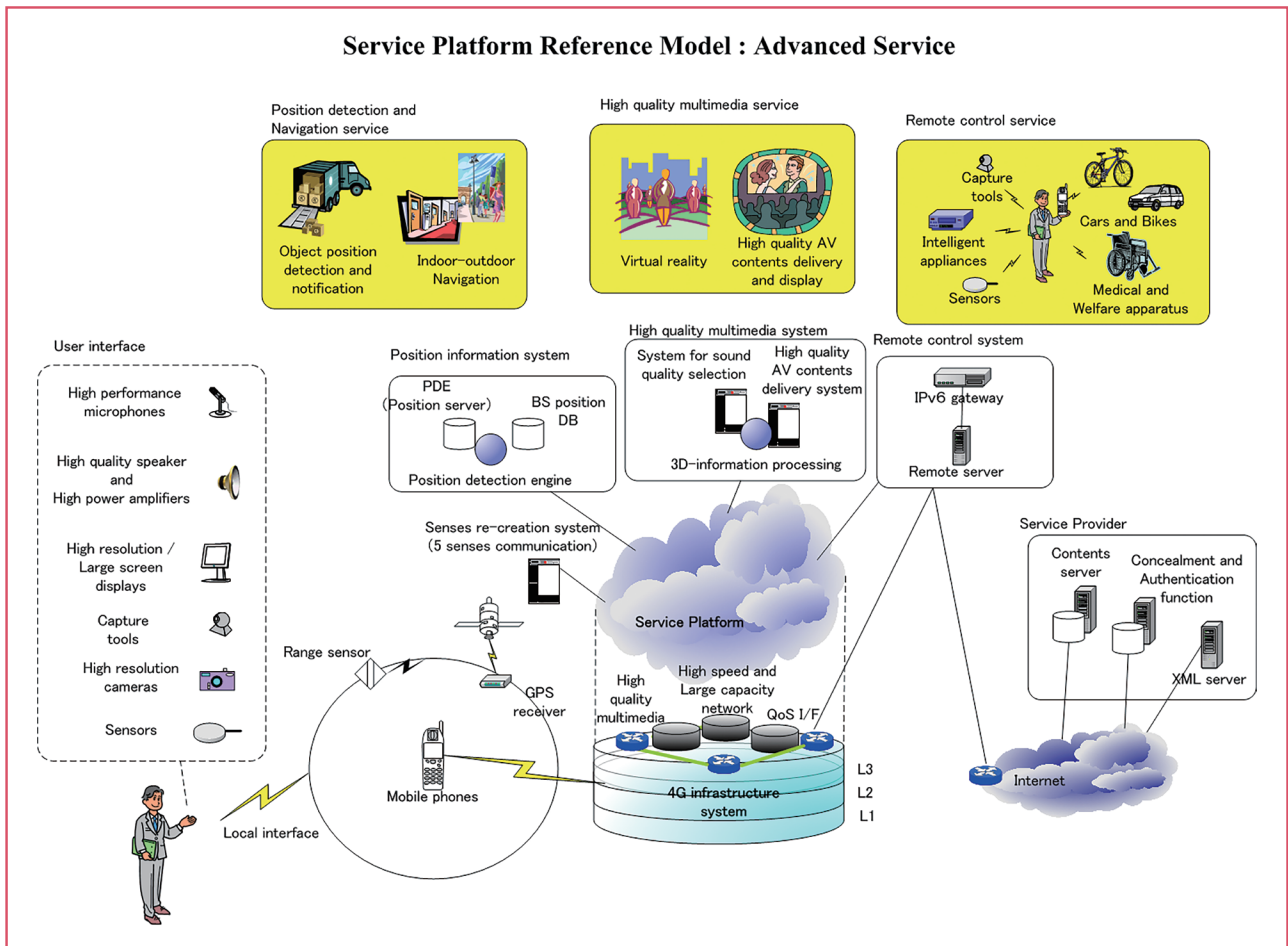


図4 mITFにおけるサービスプラットフォーム概要図(2003年)

会を続け、2003年に無線／ネットワーク／サービスを通じ自分たちの次世代通信システムのビジョンを策定した。これは「Flying Carpet」と名付けられた⁽¹⁰⁾。図が複雑だということで簡略化されたが、当時自分がドラフトして提出した次世代モバイルシステムを図4に示す。この図から見て分かるとおり、端末には高度なディスプレイ・カメラ・マイク・センサが具備されるとともに、ネットワークの背後ではGPSによる位置情報ベース・高精度マルチメディア・リモート制御サービスなどが花開く構図が描き出されており、4Gの無線インタフェースもさることながら、端末とサーバ側で極度に機能が発達することを予想していた。まだスマートホンもクラウドという言葉もない時代に実に良い予測ができたものと認識している。これは自分というより、優秀なエキスパートのメンバの方々の集合知の結実だと考えている。

書き遅れたが、1990年代にはKDDでの研究開発として、GSMと第2世代日本標準PDC(Personal Digital Cellular)間のローミングシステムの研究開発にも取り組んだ。第2世代移動通信システムの「日本孤立化」の状況に鑑み、端末はそれぞれの

端末を使いながらも、何とかして両者をシステム側でインタワークできないかというのが動機であった。システム側で、GSMのプロトコルスタックとPDCのプロトコルスタックを連携するシステムを検討して試作を行った。インタワークにはモビリティインタワーク・認証インタワークをはじめ、一部サービスインタワークまでもグループで検討した⁽¹¹⁾。3Gが開始され、本検討が実用化されることはなかったが、エンドユーザを持たない中継通信事業者が一国のモバイルシステムの孤立を避けるべく提起した、ある意味「KDD & 日本」らしい研究開発だったと認識している。



5. 2000年代: ユビキタスネットワーク(IoTの萌芽)

第3世代モバイルが立ち上がった後、私はユビキタスネットワークの研究開発に軸足を移した。現在では考えられないが、当時、日本は「e-Japan構想」の名の下に光ファイバ網が整備され、3Gシステムがいち早く立ち上がり、多くのベンダから各種の携帯端末がリリースされ、その結果、世界の中で

2000年代の総務省によるユビキタス関連研究開発ロードマップ

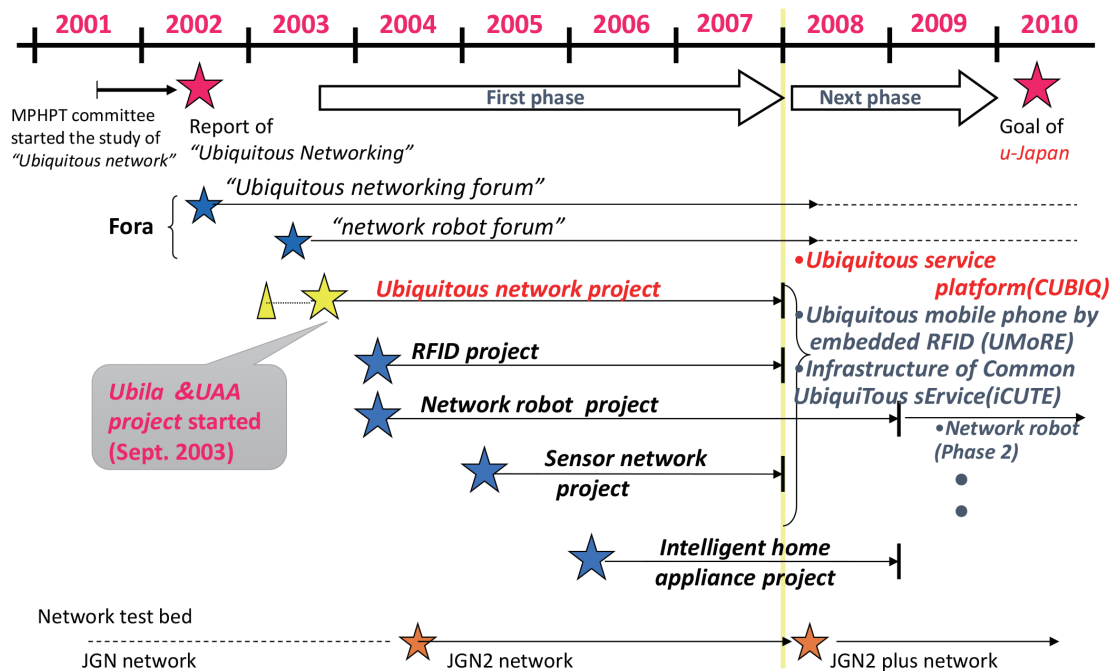


図5 2000年代のユビキタス関連研究ロードマップ

は最も ICT 分野における先進国だった。

総務省では、e-Japan そしてそれに次ぐ「u-Japan」の実現を目指し各種のプロジェクトが打ち出された。概略を図5に示す。その中で私はユビキタスネットワークプロジェクトの一つ「Ubila プロジェクト (2003-2007)」⁽¹²⁾に従事し、最終的に責任者となった。これは東大／慶大／九工大／NEC／富士通／KDDI／KDDI 研による大規模なプロジェクトで、産学官連携により、どこでも何でもつながる、を指向したプロジェクトだった。このコンセプト図を図6に示す。(この構図はかなりコピーされ、結構いろいろなところで今でも使い続けられている。)

Ubila プロジェクトの特徴は実空間指向であり、社会で生活する人々の情報・状況 (コンテキスト) をセンシングし、それをネットワーク側でうまく処理して、最終的には人々の暮らしに寄与することを目指していた。大学を中心にデモ環境の空間を充実させるとともに、プロモーションビデオの製作、実証実験の実施など多彩な活動を行った。製作された2本のビデオはユビキタスネットワークの将来像を描く面白いストーリーとして評判を呼んだ。

KDDI は「ケータイ de ライフログ」という名で、携帯を活用し人々の日常の行動をライフログとして情報収集・活用を図るシステムの試作・実証を行う

など、技術主導からサービス主導への転換を図っていった。早くにこれを栃木の農業高校に働き掛け、生徒の農作業をロギングする実証を試みたが、校長先生が「これからの農業は絶対こうなっていくます」とおっしゃっていたのが興味深い。

その後、私は「けいはんな」(関西文化学術研究都市)の国際電気通信基礎技術研究所 (ATR) に出向となったが、Ubila 後継プロジェクトとして、同じく何にでもつながるオープンプラットフォーム「CUBIQ プロジェクト (2008-2012)」を担うこととなった。このフィーチャーの実現に幾つもの技術提案が出されたが、有力な提案として、Web プロトコルの考えに基づいた RESTful なアプローチが有効であろうと、これをベースに多くの相互接続・デモを実施していった。例えば、「ららぽーと柏の葉」において、今、何が一番ホットなのかをセンシングして、サイネージや携帯端末に提示するデモを行った。当時、RESTful なアプローチは日本では我々が主たるプラクティスとしていたが、世界においても IoT の接続はあちこちでこの考え方ベースで行うのが当たり前となっていた。我々のアプローチは全く間違っていなかったことを認識した。KDDI としては、ドングルで接続する形の RFID リーダ付き携帯の試作が行われた。

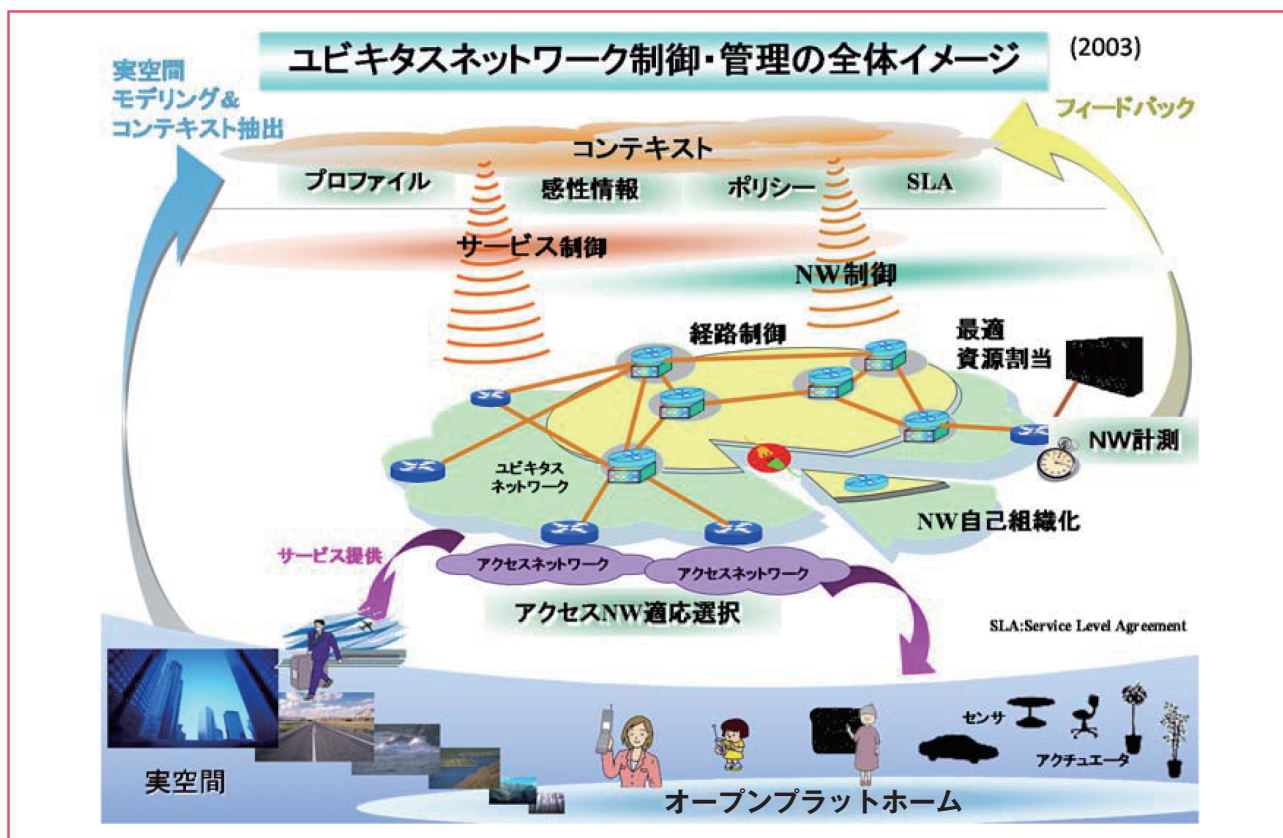


図6 Ubila Project の概要



6. B-plusの思い出

おそらく2006年頃だったと思う。通信ソサイエティで新しい雑誌を刊行するので手伝ってほしいと要請され、発刊準備チームに加わった。当時、酒井善則先生が編集長を担当され、才覚あるソサイエティメンバの方々によって次々に内容・企画が検討されていった。2007年創刊号が刊行された。率直にうれしかった。ただ課題としては、B-plusは「特定の収入源なきコストセンター」だったことだ。これが各種努力されて学会の収支を支えられている方々からは批判も受けたことがあった。(今なら自分もそう思う。)

2012年度からは前任の故山崎克之先生から要請を受け編集委員長を担当した。雑誌の方向感をどうするかも試行錯誤の部分もあったが、学会での他の企画との差別化から、特に若手の研究者やエンジニア・在学の学生に訴求できる内容にしていこうとの方向感が固まっていた時代だった。当時から活躍頂いていた関屋大雄先生が今期まで編集委員長を担われ、引き続き良質の記事が継続して執筆されているのをとてもうれしく思うし、これからもB-plusが続けられることを切に願っている。



7. SITA学会の基礎・境界ソサイエティへの迎え入れ

情報理論とその応用学会(SITA学会)は1978年から研究会として発足し、1986年から独立した学会として活動を始め、数多くの傑出した研究者を輩出してきた。毎年開催される「SITAシンポジウム」も2024年で第47回を迎える歴史あるシンポジウムであり、小生も第8回から参加してきた。一方、基礎・境界ソサイエティにも情報理論研究会(IT研究会)が長く存在しており、ある種同じスコープを持つ組織が並存していた。

2008年度から2年間、私は同ソサイエティで事業担当副会長を担当した。当時会長の小林欣吾教授は若手研究者が二組織の運営管理を行うのは大変な重荷なのでマージを図りたい、との意向を表明され、私がその任を負うこととなった。当時SITA学会側の会長は山本博資教授で、山本先生は、SITA学会が任意団体の弱みである、会長が運営に無限責任を持つ点を危惧され、Legal bodyに所属するのが正しい姿だとおっしゃっておられた。SITA学会ー基礎・境界ソサイエティ間の幾度かのキャッチボールを経て基礎・境界ソサイエティ側は準備を整え、後はSITA学会側の解散決議に委ねられた。

2009年12月、湯田温泉（山口市）で開催されたSITA総会場で、賛否が議論される中、僅差で解散、電子情報通信学会への移行が決議されるに至った。ある種感銘を受けた。その後基礎・境界ソサイエティにおいてSITAサブソサイエティとして活動が開始され、関係各位の御尽力で組織・制度が充実されていった。この経緯は小林先生の記事に詳しい⁽¹³⁾。

私は、会長が無限責任を負うのは全く間違っている、との山本先生の御意見に賛成ながらも、実際にそんなことはなかろうと高をくくっていた面もあった。しかしながら、その後のコロナ禍で実際に国際会議の開催が不可能になる事態が発生し、あながち起きないはずの話ではなかったことを自覚することとなる。間違ったことはしていなかった、と思っている。



8. 2010年代から現在： 医療応用とIoT実用化

ATRにおける活動の一つとして、京大医学部・古川壽亮教授と一緒にCBT（Cognitive Behavior Therapy, 認知行動療法）の研究開発に取り組んだ。CBTとはうつ病患者に対して、薬物投与ではなく、患者自身に自己観照してもらい、自分の行動を棚卸しして、それを医者と共に共有していくことで治療を図る仕組みである。当時、ほとんどの患者は紙に自分の行動を記していたが、古川教授と話し合う中で、“今時、それ、スマホだよな”と連携し、ライフログの知見も生かし同システムの試作・実証に京都大学／国立精神・神経医療研究センター（堀越勝部長）／ATRで取組み、「こころアプリ」としてリリースされた⁽¹⁴⁾。大学に移ることになり、本検討から自分は外れたものの、ATRメンバがサーバ構築運用も含め研究を継続し、全国のおよそ100人の被験者の1年以上のライフログを取得・分析できるに至った。最終的には開発ソフトウェアは製薬メーカーにライセンスされた。今、メンタルな分野のIoT研究開発が活発化している中、先駆的かつ有益な研究開発になったと認識しており、その活動は現在でも継続している⁽¹⁵⁾。情報通信研究機構（NICT）からは継続的に援助を賜った。

2013年には福岡大学に移り、学生に対する教育が大きな仕事となった。IoTをやろうと思った。昔に比べて、Raspberry Piをはじめとする端末の価格、センサの価格、通信料金、クラウドの維持費用など随分安くなり、大学でも比較的楽に調達でき

る。そこで学生に対しては、実装・接続に重きを置き、センサや通信機器類を各種与え、接続して動作させてみる、といろいろと試みさせた。

そうしているうちに福岡県直方市から、IoTの研究開発と一緒に取り組んでほしいとの要請を受けた。一級河川の遠賀川が流れる直方市では2、3年に一度洪水被害が生じており、それに対処するため、特に注意すべきポイントでの水位監視及び「樋門（ひもん）」と呼ばれるこれまで人手で行っていた水門のモータによるリモート開閉制御の研究開発だった。申請したところ総務省戦略的情報通信研究開発推進事業（SCOPE）に採択された。主要な市街地をカバーするため、LPWA（Low Power Wide Area）と呼ばれる920 MHz帯の無線アクセスを用いることとし、市役所で直接データを得られるよう基地局を市役所屋上に設置した。不達のエリアには簡易な中継器を小学校の屋上に設置することで対処できた。後は必要とされる水位センサを試作して配備していった。2年で20か所余りでの水位計測センサの設置が行えた。加えてLPWAを介しての樋門制御にも成功した。学生も意欲的に取り組んでもらった。2023年には大雨が直方市を襲ったが、システムはほとんど問題なく状況を伝え続けた。プロジェクト完了後も、問題なく稼働し市民に情報提供を続けている。本件はSCOPE研究開発奨励賞を受賞した⁽¹⁶⁾。



9. Gabor レーダ検討ほか

数年前、九州大学・香田徹教授（現名誉教授）から要請を受け、それまで九州大学・實松豊准教授（現教授）と一緒に取り組んでいたGaborスキームを活用したレーダの研究に参加させてもらった。GaborスキームはOFDMと同様、時間・周波数の両領域で信号を多重化する。OFDMのようにサブキャリア間の直交性は成立しないものの、時間軸上でのオペレーションと周波数軸でのオペレーションを双対に取り扱うことが可能である。これを用いて、レーダの要件である遅延・ドップラー推定をうまく交互に行えないかとの課題に取り組んでいる⁽¹⁷⁾。

2024年3月、福岡大学を退職した。依然として同学の非常勤講師は継続しているが、6月から新たに通信事業者の（株）オプテージで社外監査役として働き始めた。監査業務は自分にとって全くの新規領域であるが、日々学んでいる段階である。



10. おわりに：若手技術者／研究者へのメッセージ

これまでの技術者歴を記させて頂いた。我ながらいろいろなことをやってきたものだ、と率直に実感する。まあ、アイデンティティの欠如というか自分はこれをやるぞ、という固い意志より、今、世で求められていくもの、世の変わり目に沿ったものとはこれだ、という流れでずっと自分が対処してきたように感じる。やってみるものだ。

■文献

- (1) 大橋正良, 平田康夫, “連続復号を可能とするスタックアルゴリズム型逐次復号法,” 信学論 (A), vol. J69-A, pp. 1586-1593, 1986.
- (2) 大橋正良, 鈴木利則, “小型スタック逐次復号ボードの試作,” 第15回情報理論とその応用シンポジウム (SITA'92), pp. 29-32, Sept. 1992.
- (3) L. Bahl, J. Cocke, F. Jelinek, and J. Raviv, “Optimal decoding of linear codes for minimizing symbol error rate,” IEEE Trans. Inf. Theory, vol. IT-20, no. 2, pp. 284-287, March 1974.
- (4) 大橋正良, 安田 豊, “ビット誤り率を最小化する畳込み符号の復号アルゴリズムとその応用,” 信学論 (A), vol. J75-A, pp. 1233-1239, 1992.
- (5) 鈴木利則, 大橋正良, “ICカードを用いた分散処理型認証システムの開発,” 信学技報 (交換システム; 情報ネットワーク; 通信方式), SSE94-108, IN94-76, CS94-107, pp. 105-110, 1994.
- (6) https://www.jstage.jst.go.jp/article/jinnvib/98/0/98_KJ00004997676/_pdf
- (7) 例えば TTC, <https://www.ttc.or.jp/application/files/8315/5434/1370/JT-Q1701v1.pdf>
- (8) http://www.3gpp2.org/Public_html/Specs/C.S0023-D_v2.0_R-UIM_20111231.pdf
- (9) <https://wwrf.ch/>
- (10) https://docbox.etsi.org/Workshop/2006/2006_GSC11/GSC11_RT_Joint_Session/gsc11_joint_16%20ARIB%20Activities%20on%20IMT-2000%20and%20IMT-Advanced.pdf
- (11) A. Yamaguchi, S. Ota, Y. Ito, M. Ohashi, and F. Watanabe, “Inter-system mobility and service management in GSM/PDC roaming,” Globecom '97, pp. 694-698, Nov. 1997.
- (12) 大橋正良, 徳田英幸, 尾家祐二, 森川博之, 桐葉佳明, 加藤正文, 長谷川 亨, “ユビキタスネットワーク制御・管理技術 (Ubila),” 信学誌, vol. 91, no. 7, pp. 569-582, July 2008,
- (13) https://www.jstage.jst.go.jp/article/essfr/5/1/5_1_6/_pdf
- (14) <https://www.life2bits.com/kokoro/>
- (15) <https://rezitore.com/>
- (16) <https://www.advantech.com/ja-jp/resources/news/ictinnovationforum2024>
- (17) 大橋正良, “[招待講演] 離散ガウス波形による2次元 BPSK 信号の性能評価,” 信学技報 (IT 研), IT2020-24, Nov. 2020.

英文論文誌へ論文を投稿しよう！

英文論文誌 B 編集委員長 長谷川 剛
Go Hasegawa

電子情報通信学会通信ソサイエティの英文論文誌 (IEICE Transactions on Communications) では、将来の通信分野の発展に向けて、新たな潮流を示す研究提案を発信すべく、「ポジションペーパー」を募集しております。とりわけ、既存の技術的枠組みにとらわれない自由な発想や挑戦的な視点に基づいた研究の芽を積極的に取り上げ、次世代の通信研究の方向性を照らすことを目指しています。

ポジションペーパーでは、以下のような特徴を持つ論文を歓迎します。

- ・通信分野に対する新しい見方や思考法、あるいはこれまでにないパラダイムの提示
- ・従来技術の延長ではなく、本質的に新しい方式や構成の提案
- ・現段階では技術的に成熟していないが、将来の技術革新へとつながる可能性を秘めた独創的なアイデア
- ・世界最高水準の数値性能、あるいは従来とは異なる視点によって実現された実証結果や試作事例の報告

ポジションペーパーは、網羅的な実験評価や完成度の高さが必ずしも求められるわけではなく、むしろ独自性、先進性、問題提起力といった観点が重視されます。特に、既存の技術に対する問題意識を明確に示し、それを乗り越えるための構想を提示するような論文に大きな期待が寄せられています。学術的成熟に至る前段階の研究であっても、ほかの研究者との議論や新たな視点の共有につながるものであれば、論文としての価値は極めて高いものと考えています。

また、各分野の第一線で活躍されている研究者による「招待サーベイ論文」も、本論文誌の柱の一つとして位置付けています。これは、特定分野における近年の研究動向、技術的課題、今後の展望を包括的に整理し、分野全体の発展に向けた知的基盤として機能することを目指すものです。研究を始めたばかりの学生、若手研究者や異分野の読者にとっても有益な導入となり、俯瞰的かつ中立的な観点から分野の再整理を行う貴重な機会となります。

現在、招待サーベイの対象として検討しているトピックは以下のような分野です。

- ・B5G/6G の実現に向けたネットワーク運用自動化技術
- ・マルチコアファイバネットワーク技術
- ・次世代ネットワークアーキテクチャのフォワードینگ技術
- ・AI を活用したネットワーク技術／AI のためのネットワーク技術

これらは今後の通信技術において中核的な役割を担うテーマであり、各分野における基盤の理解の深化、研究の加速化、政策との連携など多方面にわたる波及効果が期待されます。なお、上記に限らず、注目すべきトピックやサーベイ執筆候補者についての御提案も歓迎しております。産学連携、国際動向、地域特性などを考慮した提案も積極的に検討致します。

併せて、英文論文誌 B では特集とは別に、通信分野全般にわたる一般論文も常時受け付けています。通信理論、ネットワーク制御、移動通信、無線伝送、光通信、IoT、センサネットワーク、量子通信、AI の通信応用、ネットワークセキュリティなど、多様な研究分野を対象としており、投稿時期にかかわらず柔軟に受理・審査を行っております。

本誌は、国際的な論文データベースである IEEE Xplore にも収録されており、英文による発表を通じて、世界中の研究者・実務者との知的交流が可能です。また、掲載論文はオープンアクセスになるため、成果の社会的インパクトをより広く伝えたい著者にとっても、有意義な選択肢となっています。

IEICE Transactions on Communications は、単なる論文の蓄積の場ではなく、通信技術の未来像を議論し形成していく場である、と私たちは考えています。構想段階のアイデアから完成度の高い実証研究まで、全ての段階にある挑戦的な研究を歓迎し、柔軟な視点から評価する姿勢を大切にしています。

革新的なアイデア、俯瞰的な知見、そして熱意に満ちた挑戦をお持ちの皆様の御投稿を、編集委員会一同、心からお待ちしております。

NEXT ISSUE

2026 年春号（第 76 号）2026 年 3 月 1 日発行

小特集 統計学・数学関連

ジュニア会員向けページ：統計の基礎、平均、標準偏差、95% 信頼区間

私の研究者歴：菊間信良

若者よ、世界に出よう！：留学の意味と成功への道
街 plus 探訪：ベナン

……他、御期待下さい

Editors Note

執筆者の皆様にはお忙しい中御対応頂き感謝申し上げます。
小特集記事では、セキュリティの基礎的な知識と応用の両面に触れる解説記事がそろっております。御覧の皆様のセキュリティ分野への関心を高めるきっかけになりましたら幸いです。
(M.K.)

今回の小特集では、日常的に使うようになった生体認証技術を取り上げました。指紋認証や顔認証の便利さの裏にあるセキュリティの仕組みに興味を持つきっかけになれば幸いです。
(T.M.)

仮想マシン KVM は、OS など基盤ソフトウェア研究に欠かせないツールです。積極的に活用し、是非我が国から優れた研究成果を発信して下さい。「若者よ、世界に出よう！」では、フィンランド留学の楽しい日々が語られています。小国ながら存在感の大きい北欧の国の力強さを感じて下さい。「子どもに教えたい通信の仕組み」では、多くの方が「理解したい（が難しい!）」と感じる量子コンピュータを分かりやすく紹介しています。今号も楽しい記事が盛りだくさんです。
(S.Y.)

セキュリティ特集号の編集委員を担当することになり、まず頭に浮かんだのが地域の「パパ友」です。そのつながりで執筆依頼を快諾頂くことができました。業務や専門とは異なる人とのつながりを、今後も大切にしていきたいと思っています。
(T.I.)

B-plus は技術に関する記事以外にもおもしろい記事が満載です。一つの記事が運命を変えてしまうかもしれません。読者の皆さんが楽しい未来へ導かれることを願っています。
(M.O.)



2025 年冬号（第 75 号）
2025 年 12 月 1 日 発行

EDITORIAL COMMITTEE

編集委員長 山口実靖

編集副委員長 山本 嶺 橘 拓至

編集委員

飯田大輔	伊藤敬義	伊藤暢彦	上野貴弘
金友 大	木下雅之	古川剛志	小南大智
櫻井利昭	沢田健介	立神光洋	道後千尋
中西孝行	中野雄介	中村光貴	長谷川直輝
羽多野一磨	早馬道也	東野武史	干川尚人
松田一孝	松室亮之	水野 修	山下泰輝

本誌の愛称は「B-plus」、正式名称は「通信ソサイエティマガジン」、
「IEICE Communications Society Magazine」です。
本誌掲載論文を文献引用する際は、邦文略称「信学通誌」、英文略称
「IEICE Commun. Mag.」を用いて下さい。

通信ソサイエティマガジン B-plus へのお問い合わせ

- ☐ ご意見、ご要望：b-plus@ieice.org
- ☐ ホームページ ▶ <https://www.ieice.org/~cs-edit/magazine/index.html>
- ☐ B-plus 冊子体購入のお申込みはこちら ▶ https://www.ieice.org/~cs-edit/magazine/order_y.html.utf8

複写される方へ

一般社団法人電子情報通信学会は、本誌に掲載された著作物の複写複製に関する権利を一般社団法人学術著作権協会に委託しております。複写複製を御希望の方は、一般社団法人学術著作権協会 (<https://www.jaacc.org>) が提供している複製利用許諾システムを通じて申請して下さい。

なお、複写以外の許諾（著作物の転載、翻訳等）に関しては、委託しておりませんので、直接本会へお問い合わせ下さい。

〈問合せ先〉 一般社団法人電子情報通信学会
TEL (03) 3433-6691 FAX (03) 3433-6659
著作物利用許諾申請： <https://www.ieice.org/jpn/copyright/tensai.html>

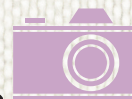
発行人／白石 智
発行所／一般社団法人 電子情報通信学会 通信ソサイエティ
〒105-0011 東京都港区芝公園 3-5-8 機械振興会館
Tel：03-3433-6691（代表） 振替：00120-0-35300

制 作／株式会社 太平印刷社
東京都品川区東品川 1-6-16

© Copyright 2025 IEICE. All rights reserved.

75
The photograph,
Communication can be seen.

通信がみえる一枚の写真



KDDI 新宿ビルアンデルセンモニュメント

道後千尋（KDDI 総合研究所）



表面：左から愚か者、太陽、風車夫、風船、魔女



表面中央：風車夫をモチーフにしたレリーフ



裏面：左から道化師、小さな宮殿、プリマドンナ、中国の宮殿、踊り子

新宿駅から徒歩 5 分、KDDI 新宿ビルの正面玄関前に設置された記念碑。デンマークを代表する童話作家アンデルセンが作製した切り絵をモチーフに、彫刻家ヤン・プール氏がデザインを手掛けています。

この記念碑は、1974 年に国際電信電話（KDD）本社ビルとして竣工した際に、デンマークの大北電信会社（グレート・ノーザン・テレグラフ社）から寄贈されました。同社は 1871 年に長崎～上海、長崎～

ウラジオストク間に日本初の国際海底電信線を建設し、国際通信の幕開けとなりました。アンデルセン童話には「大きなうみへび」という、大西洋横断海底電信ケーブルを題材とした話もあり、通信の歴史に思い馳せられる装飾となっています。

どなたでも御覧になれる場所にございますので、近隣にお越しの際は是非お立ち寄り下さいませ。



写真を募集致します

マガジン編集委員会では、「通信がみえる一枚の写真」をテーマに写真（電子ファイル（jpeg）あるいはプリント）、タイトル、説明文（約 300 字）を募集致します。詳細は、通信ソサイエティマガジン HP（<http://www.ieice.org/~cs-edit/magazine/ieice/photo.html>）を御参照下さい。

送り先：

【郵 送】〒105-0011 東京都港区芝公園 3-5-8 機械振興会館内 電子情報通信学会 通信ソサイエティマガジン担当

【メール】b-plus@ieice.org までお送り下さい。

未来60年賞チャレンジコンテスト 最終ステージ開催

～未来への扉を開く、挑戦者たちの舞台～

総合大会会場：九州産業大学 1号館 S201
 2026年3月10日（火）10時開始（予定）

未来60年賞チャレンジコンテストの最終ステージは8名のファイナリストが未来を見据えた独創的で挑戦的な取り組みをアピールし競いあう場です。若手研究者や技術者が、自らの情熱とアイデアをもって挑み、未踏の領域への新たな可能性を切り拓きます。その姿は、まさに次代の科学技術を担う「挑戦者たちの舞台」と言えるでしょう。

本ステージでは、ファイナリストたちが研究成果やプロジェクトのビジョンをプレゼンテーションし、審査員や来場者の前で熱い議論を繰り広げます。未来を変える一步が生まれる瞬間を、ぜひ会場で体感してください。

なお、未来60年賞チャレンジコンテスト最終ステージは総合大会会場で開催されます。無料で聴講いただけますが、総合大会の他セッションを聴講される場合は、別途、聴講参加申込みが必要となります。詳細は、総合大会オフィシャルホームページをご確認ください。



同世代の挑戦が
見られるなんて、
絶対に見逃せないね！

未来を変える研究って、
ワクワクするね。
現地で聴講しよう！



未来60年賞



総合大会

問合せ先：電子情報通信学会 未来60年賞事務局：mirai60@ml.ieice.org