2023～2024年のモバイルICT社会トレンド総括

はじめに

前回の発刊から約2年が経過した。現在は5Gの普及拡大期であり、高速大容量通信の5Gを活用したさまざまな技術やサービスが世の中に普及している。これに伴いデジタルデータとして扱われる情報は日々増大し、組織、企業活動で収集・処理されるデータが急速に拡大している。モバイルデバイス1つで日常生活に必要なものが代用できる反面、プライバシー保護、サイバーセキュリティ対策も大きな社会課題となっている。

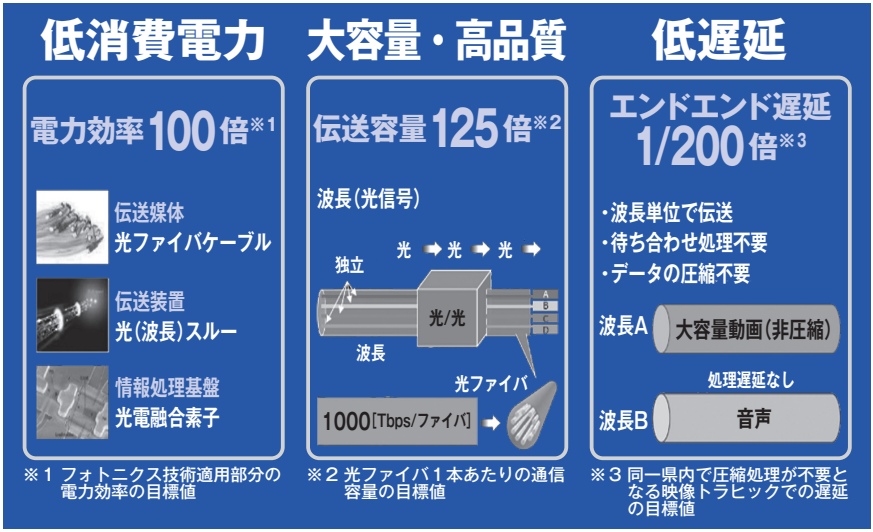
また2030年代に向けて6G[1]の研究開発も進められている。高速大容量、超低遅延などのモバイル通信技術は、現代社会の生活基盤としてなくてはならないものとなり、モバイルやICTを取り巻く環境は加速度的に変化をとげている。ここでは、そのような社会やサービス、技術の進化をめぐる2023年から2024年にかけての主な動きについて概観する。

1. 移動通信ネットワークのトレンド（IOWNと6G）

IOWN[2]（Innovative Optical and Wireless Network）は、NTTが提唱する次世代情報通信基盤であり、エレクトロニクス（電子）とフォトニクス（光）[3]の融合によって高効率な通信ネットワークを実現するという構想である。この構想は、光ファイバと無線技術を組み合わせることで、より高速で安定した通信を実現し、大容量のデータを効率的に転送することが可能となり、加えてエネルギー効率にも優れているという特徴がある。

少ない電力で環境に優しく、遠く離れた場所の様子をその場にいるかのように体験したり、ロボットや機械などと協働で作業したり、車の自動運転はもちろんのこと、空飛ぶ車の最適ルートをナビゲートするような未来のスマート社会の実現を目指している。

図表1●オールフォトニクス・ネットワークの目標性能



IOWNの特長の1つに、「低消費電力」がある。大規模なデータを処理しているにもかかわらず、消費電力が少ない。ネットワークから端末まで、電気通信を介さずに、できるだけ光のままで伝送する技術や、光電融合素子という新しいデバイスにより電気信号から光信号に置き換えるため、今までの100分の1まで消費電力を抑えることができる。これは3つある主要技術[2]の「オールフォトニクス・ネットワーク（APN）」(**図表1**）という技術である[4]。

今までは「経済成長（技術革新）」＝「莫大なエネルギーが必要」となることは当然と考えられてきたが、IOWNでは経済成長（技術革新）とともにエネルギー効率も図られる。また、エネルギーが消費されることで、環境に大きな影響を及ぼすという難しい課題もあったが、IOWN構想では通信技術の革新が持続可能な社会の実現にも貢献できる。

6G（6Generation）は、次世代のモバイル通信技術であり、5Gの後継として開発が進められており、より高速・大容量なデータ転送、通信エリアの拡張、消費電力の低減・低コスト化、超低遅延、複数デバイスの同時接続などを可能にすることを目指している[1]。

6Gの革新的な技術の中で、特徴的なものは超低遅延化である。遅延が

1msec（ミリ秒）以下を実現すると、人体における神経の反応速度、すなわち脳で考えた情報を身体に反映させるまでの時間は約20msec[5]であるため、ネットワークが神経の反応速度を超えることになる。脳や身体の情報をネットワークに接続することにより、ネットワークで感覚を拡張することができるようになると考えられている[6]。

2. AI技術のトレンド

生成AIとAIエージェントの進展

アメリカのAI研究機関オープンAI（OpenAI）[7]が2022年11月に対話型生成AIサービス「ChatGPT[8]」を公開した。インターネットとスマートフォンさえあれば、世界のどこでもChatGPTが体験でき、世界中に大きな反響を呼ぶことになった。現在も改良が続けられており、2024年5月には「ChatGPT-4o[9]」をリリースしている。

生成AIの技術革新は目覚ましく、大規模言語モデル（LLM）[10]の進化により、大規模かつ高性能な言語モデルの開発が進んでいる。初期の言語モデルに比べ、近年の大規模言語モデルは桁違いに大きく、例えば、OpenAIのChatGPTでは、GPT-2で15億パラメータだったところ、GPT-3では1,750億パラメータにまで拡大した。モデルサイズが大きくなることで、より複雑な言語パターンを学習し、生成能力が向上しているといえる。また、質問者と会話する中で、GPT自身が学習していく強化学習という仕組みも採り入れている。今後は生成AIと技術革新の実装がより具体化していくであろう。

国産の技術としてはNTT版大規模言語モデル「tsuzumi」[11]なども開発されている。世界トップレベルの日本語処理性能を持ち、パラメータサイズはChatGPT-3の1,750億と比べて25分の1の70億と軽量であるため、学習やチューニングに必要となるコストを低減。更には視覚や聴覚といったマルチモーダルに対応し、特定の業界や企業・組織に特化したチューニングも可能となっている（特徴は**図表2**）。

また、AIコンステレーション[12]も特徴の1つである。環境負荷の低減だけでなく、AI同士を自律的に協調させることで、何でも知っている1つの巨

図表2●tsuzumiの特徴

軽　量	1GPU/1CPUで動作可能
カスタマイズ可能	産業・組織の専門知識を保有したAI
マルチモーダル	テキスト入力以外の多用なユースケース
日本語に強い	性能世界トップクラス・特に日本語は強い

大なLLMではなく専門性や個性を持った小さなLLMの集合知による、ハルシネーションリスク[13]の低減や高効率なAIを実現することを目指している。

AIエージェントについても少し触れておく。生成AIは、大量のデータから学習したパターンを基に、新たなコンテンツを生成する「一方向のAI」であるが、AIエージェントは複数のAIモデルやデバイスを組み合わせて自律的に管理し、周りの環境に応じて、意思決定と行動を行う「双方向のAI」である。例えば、スマートフォンの音声アシスタントやカスタマーサポートのチャットボット、自動運転車などがその一例である。AIエージェントは、業務の自動化やコスト削減、人的ミスの防止、24時間365日の安定稼働など、多くのメリットをもたらすことが期待されている。

身近になるAI技術

昨今、ネットショッピングを利用して買い物をしている方は多い。コロナ禍以降、オンラインでの商品注文や購買について急速に増加、定着した消費行動（**図表4**）であるが、例えば、eコマース[14]のWebサイトで顧客が商品をカートに入れたり、買い物リストに保管したりすると、高度なアルゴリズムに基づいて追加のレコメンドの表示や、欲しい品物を検索していると類似商品を提案された経験はお持ちであろう。「なんで自分が探している商品を知っているのか？」と不思議に思うこともあったと思う。このアルゴリズムは、類似の商品を購入した他の顧客と比較し、適切なレコメンドを行うようプログラムされているAI技術で、自分が探している情報を先回りして提供してくれる。

このようにAIを活用した製品レコメンデーションは、オンラインショッピングでは以前から一般的だが、さらに生成AIが加わることで、カスタマイズされた表現や商品説明をつけられるようになり、プロセス全体で「パーソナルな特別感」が増す。生成AIでターゲットを絞り込み、価格や商品メッセージでパーソナライズ感を出すことで、よりユーザーの嗜好や性格に合わせたコンテンツの生成が可能となる。これはほんの一例であるが、現在では、創作活動（音楽、アート、文章）、教育、医療、エンターテインメントなど、さまざまな分野で生成AI技術が応用拡大され、生成AI技術の進化はますます重要性を増していくと考える。

弊所でも2023年度より生成AIに関して調査を開始した。利用と認知についても若年層、男性の利用や認知が高く、10代男性においては「よく利用している」「利用したことがある」で5割を超えている。20代男性でも約4割と高く、若年層ほどChatGPT（生成AI）を利活用していることが判明している。また聞いたことがあるまで含めると全体で6割超の人が聞いたことがあると回答し、社会全体にかなり浸透していることが明らかとなった（**図表3**）。

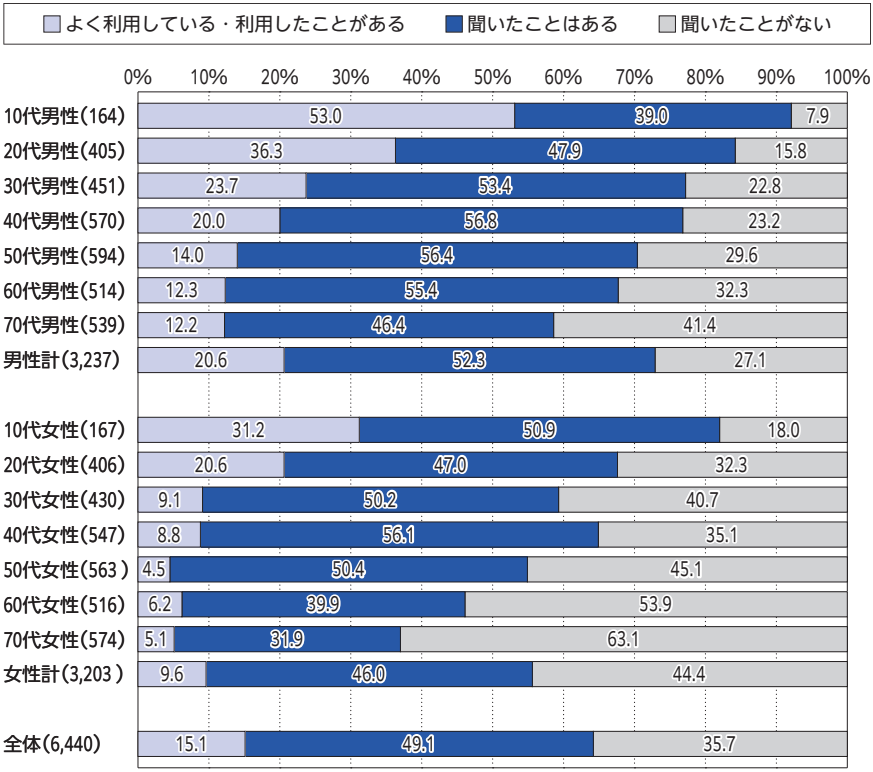
生成AIを含むAI技術には多くの可能性がある一方で、いくつかの重要な課題もある。

例えば、データや情報の収集・分析・提示において、ある方向に偏った見方や評価によるバイアスが生成されるコンテンツに反映されることがある。これにより、特定の組織や個人に対する偏見や差別を助長したり、情報が偏重するリスクがある。

また、フェイクニュース、ディープフェイク[15]、スパム[16]生成などの悪意ある用途にも利用されるリスクもあり、倫理的な使用を確保するためのガイドラインや規制が必要であったり、生成AIが既存の作品を模倣、または直接使用することで、著作権侵害、知的財産権の問題や個人情報、プライバシー侵害のリスクなど、さまざまな課題も表面化している。これらの課題に対処するためには、技術的な解決策の開発、倫理的なガイドラインの策定、法的な規制の整備など、社会全体での議論と協力が必要となる。

AI技術が進化した将来、AIによって専門的な知識やタスクなどが自動化

図表3●性年代別 ChatGPTの認知と利用［調査対象：全国・15～79歳男女・n=6,440］



出典：2024年一般向けモバイル動向調査

されるため、人が持つ創造力や感性が重要視される。AIは革新的なツールであることは間違いないが、万能ではない。過去の事象を基にした分析には長けているが創造的な思考や直感的な判断、感情やニュアンスを理解することは苦手とされている。「新しいものの創造」や、「常識を超えた発想」「リーダーシップ」というのはAIからは出てこないため、AIが苦手とされる発想、創造を人がすることでAIとの分業、差別化を図り、AIによって効率化された時間を有効に使うことで生産性もさらに向上すると考える。

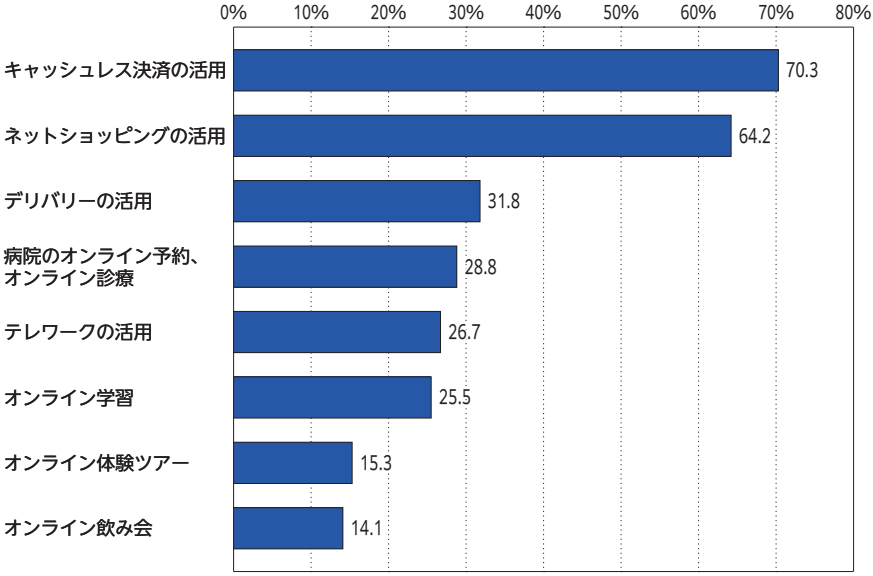
3. フィンテック（FinTech）のトレンド

コロナ禍により定着したこと

フィンテック（FinTech）[17]とは、金融（Finance）と技術（Technology）を組み合わせた造語で、テクノロジーを活用して提供される革新的な金融サービスや製品を指す。フィンテックの主な分野・サービスには「デジタルバンキング」「キャッシュレス決済」「オンライン取引」「ブロックチェーン[18]」「仮想通貨（暗号資産）[19]」「RegTech[20]（規制技術）」などがあり、フィンテックの発展は金融業界における効率性の向上、コスト削減、地域経済の活性化などで大きな変化をもたらしている。

2023年の弊所の調査によるとキャッシュレス決済の活用について、コロナ禍前と比べて約7割の人から生活に定着したという回答を得ている（**図表4**）。しかも若年層からシニアの年代別に見ても7割前後の人がキャッシュレス決済を活用しているという結果となっている[21]。コロナ禍によって大

図表4●新型コロナウイルス感染拡大前と比較して生活で定着したと思うこと
（2023年2月調査）[調査対象：全国・15～79歳男女・n=6,151]



きく普及し、そして生活に定着したフィンテック技術の1つといえる。

ポイントサービスの定着、進展

デジタル技術の進化によって使いやすく、貯めやすくなった「ポイントサービス」は、日本での始まりもかなり古く、最初は紙のスタンプカード、1980年代後半には大手家電量販店がバーコードを読み取って管理するポイントカードを発行したといわれている。現在ではキャッシュバックといわれるように、通貨と同様な感覚で扱われている。ポイントサービスについては、かなり前から存在はしていたが、プラスティックカードやスタンプカードなどが主流で商品購入時にレジに出して、ポイントやスタンプを押してもらう一手間二手間をかけないと付与されなかった、また、財布の中にポイントカードが山のようにたまって散乱し、どこのポイントカードかわからなくなった経験もあると思う。それが今ではスマホの決済アプリなどに付属されているので、キャッシュレス決済と同時にポイントも付与され、その場でポイントを利用して商品も購入できる。そのため、顧客エンゲージメントを高め、ロイヤルティを構築することに利用されている。

また、ポイントサービス市場も年々拡大している。昨今の動きとしてはポイント事業について新たな業種の参入による競争激化、ポイント経済圏のボーダーレス化が大きなトレンドとなっている。公共交通機関の金融サービスへの参入、eコマース分野での連携などさまざまな業種、分野に影響を与えている。今後、フィンテックの中でも「ポイント投資」「株・NISAなどの投資アプリ」「銀行口座アプリの進化」といった資産形成系サービスの動きにも注目していきたい。

4. サイバーセキュリティの動向

社会経済活動のデジタル化が加速度的に進む中、サイバーセキュリティの確保は社会的課題の重要項目の1つである。近年のサイバー攻撃は巧妙かつ多様化し、生活のさまざまな場面において身近なリスクとなっている。

また、「攻撃の匿名化」や「サイバー犯罪のビジネス化」に伴い、特定の組織や企業を狙った「ランサムウェア攻撃[22]」や「標的型攻撃[23]」が主流

となっている、近年のサイバー攻撃の動向については、社会のデジタル化と切り離せないことは明確であり、組織、企業のみならず、個人に対しても攻撃の対象となっていることから、サイバーセキュリティについても触れておきたい。

ランサムウェア攻撃・標的型攻撃の増加

ランサムウェアは、身代金を要求するコンピュータウイルスの一種で、主にメールやWebサイト経由で感染する悪質なソフトウェアである。

2021年以降、新型コロナ禍の拡大に伴い、リモート環境を狙ったランサムウェアによるサイバー攻撃・被害が急増している。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2024［組織］」では、「ランサムウェアによる被害」が1位[24]となっている。ランサムウェアについては「最新ソフトウェアのアップデート」「不審なリンクをクリックしない」「不審なメールの添付ファイルを開かない」「信頼できないWebサイトのファイルをダウンロードしない」などの対処策はあるものの、常に新種が出現するため、イタチごっこ的な側面があり、完璧な防衛は困難である。ただし適切な対策を講じることで、被害を最小限に抑えることができることは間違いない。

最近の動向として、二重恐喝という手口も増加している。まず企業などのネットワークに侵入し、暗号化を解除してほしければ身代金を支払うように要求する。さらに、盗み出した情報を暴露されたくなければ削除料を支払えと、追加で身代金を要求するので、慎重かつ毅然とした対応が必要である。

標的型攻撃は、特定の企業や個人などをターゲットにし、メールやWebサイトからウイルス・マルウェアを感染させるサイバー攻撃である。標的型攻撃メール（スピアフィッシングメール[25]）も巧妙化が進み、実在する取引先のドメインを偽装したりするので、不審なメールの場合はリンクや添付ファイルを開く前に送信元のドメインや本文内容などを慎重に確認しなければならない。

加えて今までは、標的型攻撃メールが侵入の大多数だったが、2023年頃からVPNなどネットワークの外部接点（ルーターやVPNなどインターネッ

ト境界に設置された装置）における弱点を悪用した「ネットワーク貫通型」攻撃や、マルウェアなどの不正ツールを極力使用せず、セキュリティツールやOSに組み込まれた既存の機能を悪用する「環境寄生型（Living Off the Land）」と呼ばれる攻撃[26]が増加している。また、侵入を防ぐ防衛的な対策はもちろん必要であるが、サイバー攻撃に遭遇し、ウイルス感染した直後の対処策も重要となってくる。何か不測の事態が起こった時にパニックを起こさずに冷静かつ、的確に対処することが望ましい。例えば自分のPCがウイルス感染した時にどのように行動したらよいか、最初に何をするのかなど、事前シミュレーションも重要な対策の1つであるので、事前事後の両面の対応策を準備してほしい。

インターネットとサイバーセキュリティの知識や、利用方法に応じたサイバーセキュリティ対策については、総務省HP「国民のためのサイバーセキュリティサイト」[27]などにわかりやすくまとめてある。

生成AIがサイバーセキュリティに及ぼす影響

サイバーセキュリティの動向の1つとして、生成AIがサイバーセキュリティに及ぼす影響を気にされている方もいると思う。想定されるのは、クレジットカード番号やアカウント情報などの重要情報を盗み出すフィッシング詐欺などに、犯罪グループが生成AIを利用するというケースが想定される。以下に生成AIを利用した事例を紹介する。

①フィッシング詐欺となりすまし

生成AIを用いて、リアルなメールやメッセージを作成し、なりすますケースでは、従来のフィッシング攻撃よりも巧妙に見えるメッセージが送信される。また、ビジネスメール詐欺などでは、社長や上司のなりすましを行い、社内の従業員から資金をだまし取るケースもある。

②ディープフェイク[15]技術の悪用

生成AIを用いて、合成動画や音声を作成する技術を悪用することで、有名人やビジネスリーダーになりすまし投資詐欺をさせるケースもある。

③セキュリティテストと攻撃シミュレーション（防衛手段）

一方で防衛手段として、生成AIをサイバーセキュリティ対策に活用することも考えられる。生成AIを用いることで、セキュリティテストや攻撃シミュレーションを行うことが可能となる。これにより、脆弱性を特定し、対策を講じることができるため、対策強化にもつながる。

サイバーセキュリティについては、ハード・ソフト面でのさまざまな対策が必要となってくる、しかしながら、新種のウイルスや新型の攻撃など、日々進化していることもあり、ツールやソフトウェアだけで対応できないことも想定されるため、最後は企業や個人が、セキュリティ意識を高い水準で維持することが、最も重要な対策ではないかと思っている。

5. おわりに

ICT技術におけるトレンドは相互に関連しており、1つひとつの技術の進歩が別の技術の発展を後押しするという連鎖反応を起こしている。ビッグデータの処理にはクラウドが必要であり、クラウド上での処理はAIと連携して高度な予測モデルを構築し、ビッグデータとクラウドと連携して、IoTデバイスからのデータをリアルタイムで処理している。ビッグデータ、クラウド、AI、IoTなどの技術はサイバー攻撃の脅威を増加させ、サイバーセキュリティは、これらの技術の進歩に対する対策として重要となる。など、すべてのトレンドが結びついてモバイルICTの未来を形成していくと考える。

注

1 6G：docomo business Watch　6G通信とは？ いつから何が実現するのかを解説
https://www.ntt.com/bizon/6g.html
NTT技術ジャーナル記事 特集「5G evolution & 6Gに向けたNTTドコモの取り組み」
https://journal.ntt.co.jp/article/15175

2 IOWN構想とは？ その社会的背景と目的
https://www.rd.ntt/iown/0001.html

3 フォトニクス：光の性質を応用する装置・技術についての工学。

4 オールフォトニクス・ネットワークとはなにか
https://www.rd.ntt/iown/0002.html

5 叶内・水澤「実地医家に必要な新しい検査と重要な検査項目」『日本内科学会雑誌』第97巻第12号,

2008年12月

6 NTTドコモ　ホワイトペーパー「5Gの高度化と6G」
https://www.docomo.ne.jp/binary/pdf/corporate/technology/whitepaper_6g/DOCOMO_6G_White_PaperJP_20211108.pdf

7 OpenAI：アメリカのサンフランシスコに拠点を置く、人工知能（AI）の開発および普及を目的とした非営利研究機関。テキスト生成系AIの「ChatGPT」を開発。https://openai.com/ja-JP/

8 ChatGPT：人間との対話に近い自然な文章を生成するAIチャットサービス。

9 ChatGPT-4o：ChatGPTの最新モデルであるGPT-4o（Omni、オムニ）。従来のモデルよりも回答精度がはるかに向上、音声会話もできる。
https://openai.com/index/hello-gpt-4o/

10 大規模言語モデル：大量のデータとディープラーニング技術によって構築された言語モデル。

11 NTT版大規模言語モデル「tsuzumi」
https://www.rd.ntt/research/LLM_tsuzumi.html

12 AIコンステレーション：NTTニュースリリース「NTTとSakana AI、サステナブルな生成AI社会に向けたAIコンステレーション研究で連携」
https://group.ntt/jp/newsrelease/2023/11/13/231113b.html

13 ハルシネーションリスク：AIが事実と異なる不正確な回答を生成すること。

14 eコマース：Electronic Commerce（エレクトロニック・コマース）」の略。インターネット上で商品やサービスの売買を行う取引のこと。

15 ディープフェイク：「ディープラーニング」と「フェイク」を組み合わせた造語。AIを用いて、人物の動画や音声を人工的に合成する処理技術。

16 スパム：受け取り手が望んでいない、要求していない通信を大量に送信することをいう。一般的には電子メール（スパムメール）のことをいう。最近では、X、Instagram、FacebookといったSNSのメッセージを使ったスパムもある。

17 FinTech：金融（Finance）と技術（Technology）を掛け合わせた造語。銀行や証券、保険などの金融分野に、IT技術を組み合わせることで生まれた新しいサービスや事業領域。

18 ブロックチェーン：ブロックと呼ばれる単位でデータを管理し、鎖（チェーン）のように連結して保管する技術、仕組みを指す。金融取引履歴などで利用される技術。

19 仮想通貨：インターネットを通じて不特定多数の間で商品などの対価として使用できる通貨。代表的なものとしてビットコイン、イーサリアムなどがある。

20 RegTech：規制（Regulation）と技術（Technology）を組み合わせた造語。主に新しいITを活用して複雑化・高度化が進む金融規制に対応する金融ITソリューションを指す。

21 NTTドコモ　モバイル社会研究所　調査研究レポート「7割が『キャッシュレス決済』生活で定着」
https://www.moba-ken.jp/project/lifestyle/20231127.html

22 ランサムウェア攻撃：身代金を要求するコンピュータウイルスの一種、主にメールやWebサイト経由で感染する。

23 標的型攻撃：特定の企業や組織をターゲットにし、メールやWebサイトからウイルスなどを感染させるサイバー攻撃。

24 独立行政法人情報処理推進機構（IPA） 情報セキュリティ 10大脅威 2024
https://www.ipa.go.jp/security/10threats/10threats2024.html

25 スピアフィッシング：特定の組織や人物を狙って偽の電子メールを送信し、個人情報などを収集する標的型フィッシング攻撃。

26 環境寄生型攻撃：マルウェアや悪性プログラムを利用せず、セキュリティツールやOSに組み込まれた既存の機能などを悪用する攻撃。

27 国民のためのサイバーセキュリティサイト
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/