SEMINAR REPORT

最近の ICT 技術政策動向を含めた総務省の情報通信技術戦略について

総務省　大臣官房審議官
（国際技術、
サイバーセキュリティ担当）
近藤　玲子　氏

本日はこのような場で話題提供をさせていただく機会をいただき、ありがとうございます。私は総務省において情報通信関係の技術政策全般とサイバーセキュリティを担当しておりまして、政策動向や戦略について御紹介させていただきます。

全体像として総務省では技術政策を推進していくにあたり、特に研究開発だけではなく、国際競争力の強化、経済安全保障の確保といったようなことも念頭に、持続可能で強靭な社会の実現をしっかり意識をしながら、特に重点的な技術として Beyond 5G、AI、量子通信、サイバーセキュリティ、宇宙関係、こういった先端分野の研究開発を進めていく、それと知財、国際標準化活動を戦略的に推進していくことに取り組んでいます。本日は特にこの５つの分野についての取組を御説明するとともに、総務省と一体的に研究開発を進めていただいている情報通信研究機構（以下 NICT）のちょうど中長期目標の期間の区切りの年となるところ、次期の中長期目標期間に向けて今後どうしていくかについて議論をしておりますので、この点についても御紹介させていただきたいと思います。

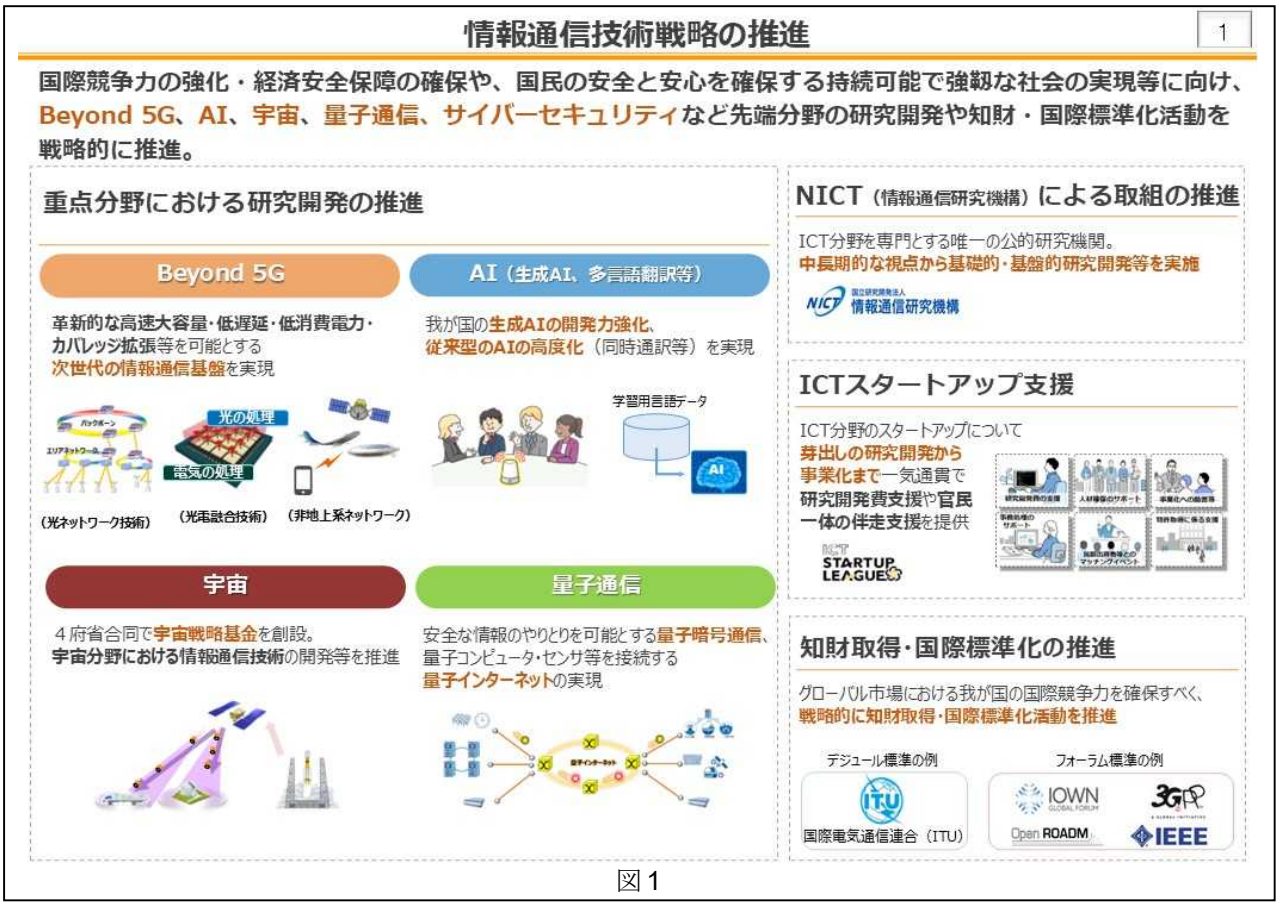


図１

AI に関する取り組み

AI は今までも何度かブームがあったと記憶されているかと思いますが、現在はディープラーニング技術の進歩ですとか、GPU が普及してマシンパワーが向上し、利用できるデジタルデータが増大したということで、第3次ブームと位置づけられているかと思います。特に膨大なテキストデータから学習をして高度な言語理解を実現する技術である LLM（大規模言語モデル）の登場によって AI に対し人間の言葉でいろいろ細かな指示を与えられるようになり、応用性が一気に広がって社会実装が進んでいる状況にあります。

図2

このLLMは、いろいろな課題に適用可能な汎用性を有していることと、今申し上げたように対話型で誰もが容易に扱っていけるということで、社会全体に非常に大きな影響を与える可能性があります。ホワイトカラーの仕事の多くが AI に代替されてしまうのではないかという指摘もありますが、企業の生産性を大きく向上させる面で非常に期待されています。インターネットと同様に社会の基盤技術の一つになる可能性を秘めているということで、日々新聞を見ても生成 AI に関する記事を見かけない日がないぐらい盛り上がっている分野になると思います。

図3

この LLM を応用して人と自然な会話をできるように特化したのが、ChatGPT に代表される対話型 AI サービスです。自然言語で操作ができるということで、普及スピードも格段に速くなっています。例えばフェイスブックではユーザー1 億人突破に 54 カ月かかったところ、ChatGPT ではリリースから僅か5日間でユーザーが 100 万人を突破し、2 カ月で 1 億人に到達したと言われています。海外でもビックテックを中心に LLM 開発の競争が進んでおり、国内でも多くの企業が開発に取り組んでいる状況になっています。LLM の応用分野はとても幅広く、文章の要約、翻訳、校正だけではなく、アイデア創出、コード生成、さらには役割を与えることで、例えば教育現場で学生の回答を評価したり、ソフトウエアの開発工程を自動化していくというようなこともできるようになってきています。

一方で、海外製の LLM として例えば ChatGPT-4 の場合であっても、英語と日本語では性能の差があるといったことが報告をされています。例えば、ChatGPT に対し日本語で「同じ単語が違う意味を持つ文章の例を教えて」と入力してみると、英語の「バンク」を挙げて、銀行と川岸と答えてしまうというのがありました。ただ、ChatGPT も日々進化をしていて、こういう場で御紹介するとしばらくすると直っているということも多く、日本語の性能はこれから追いついていくものと思います。

なお、日本の知識に特化した質問への応答については、日本語資源の学習効果が非常に顕著だという研究報告も行われています。こういう状況も踏まえ、NICT で高品質な日本語データの整備が重要ということで、2023 年度から LLM の学習言語データとして、日本語データの整備を行っています。NICT でウェブ上から収集した玉石混交の生データを基にクレンジングを行い、AI 学習に適した高品質な日本語データを整備し、国内の AI 開発企業などに提供しています。現状、最大で 22.9 テラバイトの日本語データを既に整備をしており、最大で 3110 億パラメータのモデルも試作をしています。これは、日本語の学習言語データとしては世界最大級のものです。こういう高品質な日本語データを国内の企業に提供することで、各企業が一からデータ集めをして、データクレンジングを行わなくてもよくなり、高性能な日本語 LLM の開発が促進されることが期待されています。

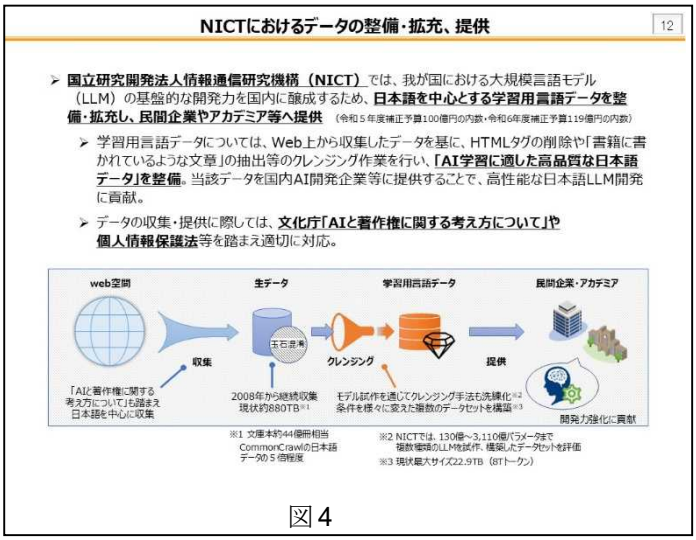


図4

生成 AI 登場により社会変革がいろいろ起きてきていますが、これに対応すべく、2023 年 5 月に「AI 戦略会議」が設置されました。政府における AI 戦略を検討し、AI の利用、それから AI のリスクへの対応、AI の開発力などに関する考え方を取りまとめた論点整理が公表されました。この中で AI 開発力については「開発に用いることのできる日本語を中心とするデータの整備・拡充を進めるべき」と挙げられております。総務省としてもしっかり取り組んでいくこととしております。

少し別の切り口で、AI の進展を語っていく中でよく言及される、「AI が果たして人間の脳を実現できるのか、特に感情部分について、人間の感情は外部から観察できる形になり得るのか」といった観点から行っている研究開発について、少し御紹介したいと思います。こちら、NICT では脳の情報処理を外側から観測をすることで、人工的に脳を再現するモデルである人工脳の構築を研究しています。

基礎研究だったこの技術を活用し、現在ではいろいろな機関と組んで実装を進めています。例えば、テレビ広告（CM）の事前評価を行うものが既に商用化されています。仮想的な人工脳に CM の案を見せて、視聴者がどのように感じるかをシミュレーションし、それをうまく微調整することでマーケティングに活用するといったことが行われています。実際に NTT データに技術移転しており「NeuroAI/D-Planner」というサービス名で商用展開が行われています。テレビ広告とかウェブデザインとかポスターとか、人に与える印象を AI が事前に評価するというサービスとして活用が進んでいるのです。2021 年から延べ 200 件以上の提供実績があると聞いています。図 5 右下にも書かれていますが、例えば NTT ドコモでは CM を製作する際に、人工脳が示してくれる好感度がどう変化するかを見て、好感度の高いほうに全体のストーリーとか構図を変えたり、起用する女性の洋服の色を変えるなど、そういうことが行われていると聞いています。

図 5

今日は詳細を御説明しませんが、実はこの脳情報通信技術の応用分野は広くなっています。既に NICT ではスポーツのトレーニング等で気持ち的に恐怖を乗り越えられる血流を促すイメージトレーニング、それから歩行訓練、高所恐怖症の解消など、様々な分野での実用化に向けた研究開発を行っておりますので、御紹介をさせていただきました。

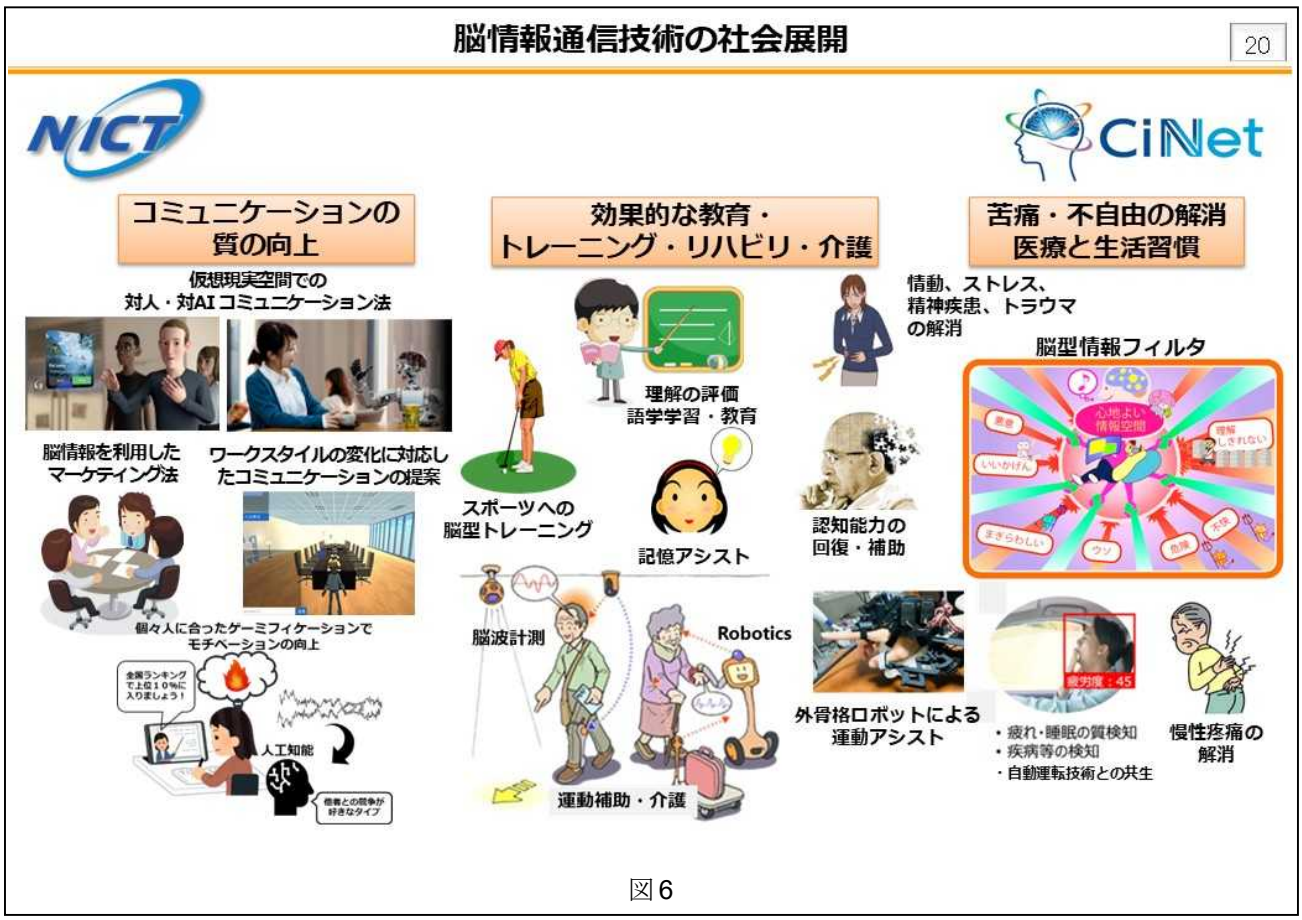


図 6

Beyond 5G に関する取り組み

Beyond 5G についてお話をしたいと思います。今年 1 月の日経新聞に掲載された内容ですが、国際エネルギー機関の推計では、OpenAI の ChatGPT が 1 回のクエリ、問合せに回答する消費電力量が 2.9 ワット時になっているということで、これは Google 検索の約 10 倍に相当しています。この AI による膨大な計算量を支えるために、データセンターの消費電力量が大きく増えており、2022 年に約 460 テラワット時だった消費電力量が、2026 年には 620 から 1,050 テラワット時に達するというような報道がなされています。この 1,000 テラワット時は、日本国内の年間消費電力に匹敵する規模と言われており、日本でもデータセンターの需要と電力需要が急増しているという状況にあります。

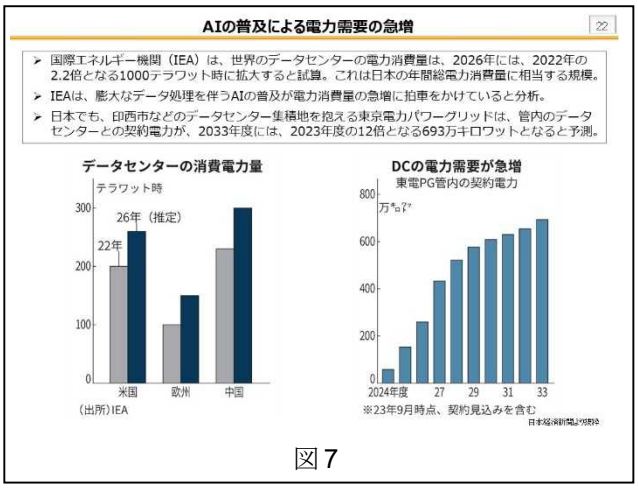


図 7

この電力需要をどうしていくのかも考えつつ、今後の生成 AI がどうなっていくのかについて、総務省でも関係者の方々と議論し考え方を整理していますが、今後の AI について開発や利活用が益々社会課題の解決に使われるのは間違いない一方、この電力消費が膨大な状況において、大規模な AI を作り続けてよいのか、また、一つの大規模な LLM に頼った場合に偽・誤情報を組み入れられたらどうするのか、そういったことを考えると AI のリスクは実際に存在します。一部の国では AI は危険ゆえ規制しなければといった議論もありますが、リスクを抑制しながらイノベーションを加速化していくということを考えると、一極集中的な巨大な汎用 AI に頼って全てを解決するのではなく、個別分野に特化し小型で分散化した AI 同士を連携させることにより、電力消費量も抑えつつ、安全安心な AI の利活用を促進していけるインフラ整備に取り組んでいこうと、総務省としては考えているところです。

図 8 は昨年 5 月の経済財政諮問会議で総務大臣がプレゼンした資料の抜粋になります。細かいところはさておき、一番下の 3 行を見ていただければと思います。現在多大な電力を消費するデータセンターが首都圏と近畿圏の大都市に集中していますが、データセンター間を超低遅延で接続できるオール光ネットワークで接続することで、今まではデータセンターにできるだけ利用者は近いところにいたいというのがありましたが、距離の制約を緩和して大都市周辺に集中しているデータセンターの分散化を図っていくことを目指すインフラ整備となります。

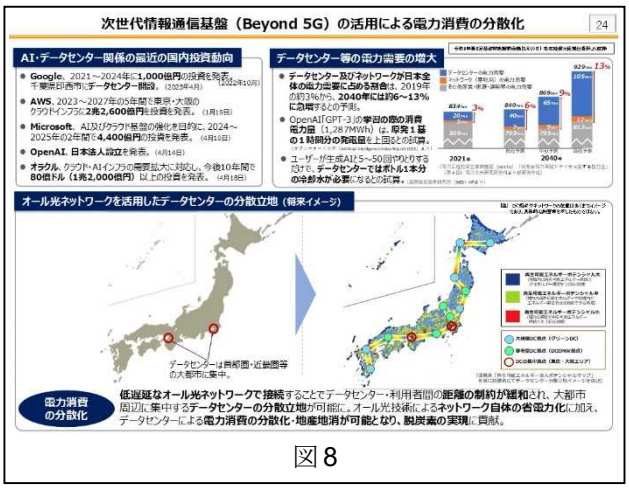


図 8

データセンターを分散化させることで、電力消費の分散化も可能になります。そして各所のデータセンターに小型・分散化した AI を活用していくといった世界を描きながら、この技術開発の支援スキームとして、総務省では次世代情報通信基盤「Beyond 5G」を早期に実現するため NICT に研究開発基金を設置しました。これを活用することで、民間企業や大学における研究開発や国際標準化を支援しています。

図 9

図 10 が 2030 年代の AI 社会を支える次世代情報通信基盤のイメージです。今までお話ししたような個別分野に特化をした小規模で分散化した多くの AI を駆動するデータセンターを連動、連携させ、そこに自動車、ドローン、ロボット、あとはセンサーを備えたいろいろなもの、そういう多様なユーザーともものとを場所を問わずにつなぐことができるインフラをつくっていこうと考えています。その主な構成要素となるのが、データセンターなどの計算資源、オール光ネットワーク、宇宙や成層圏を活用した非地上系ネットワーク、無線ネットワークであると想定をしています。

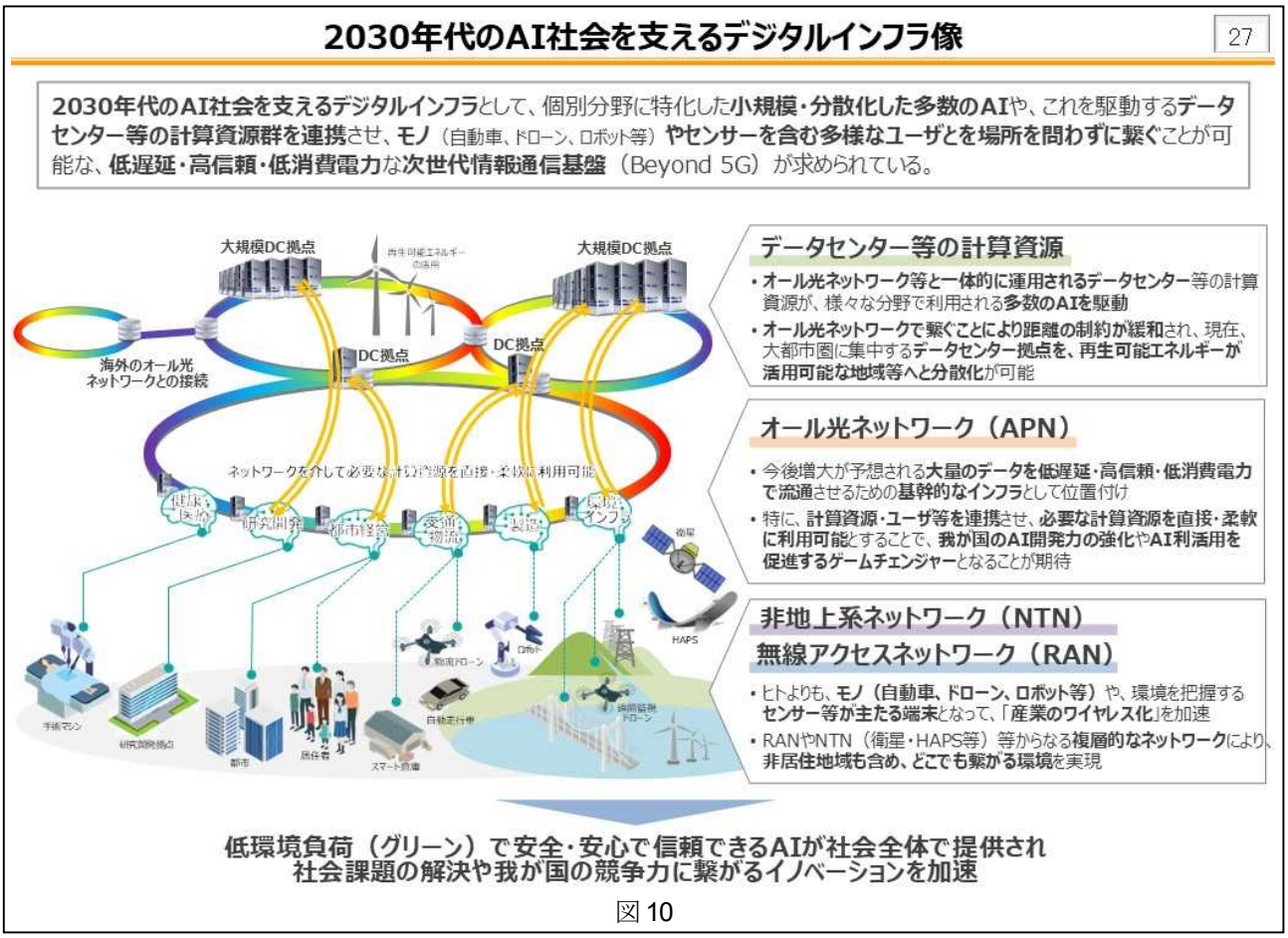


図 10

それぞれについて戦略的に取り組もうということで、先ずデータセンターといった計算資源については、先に申し上げたようにオール光ネットワークと一体的に運用し、様々な分野で利用される多くの AI を駆動するイメージになります。オール光ネットワークでつなぐことで距離の制約が緩和されて、現在、大都市に集中するデータセンター拠点を再生可能エネルギーも使える地域へと分散していくことが可能になると思います。

つぎに、真ん中のオール光ネットワーク（APN）については今後ますます AI 等を使ってデータが増えていくのですが、そういった大量のデータを低遅延・高信頼・低消費電力で流通させるための基幹的なインフラとしてこの APN が重要になっていきます。地理的に分散した計算資源とユーザーと結びつけていくということで、いろいろなところで AI を開発することができるようになりますし、利活用も促すものと捉えています。

そして、最近存在感が増している非地上系ネットワーク（NTN）についても、無線アクセスネットワークと合わせて、人を結ぶだけではなく自動車、ドローン、ロボットといったものとか、それと環境を把握するセンサーなど様々なものが今後端末になって結ばれていくと考えています。ワイヤレスの世界が進んでいる中で、NTN は HAPS、衛星などといった非地上系ネットワークを組み合わせて複層的なネットワークで人が住んでないところでも通信できるような世界を実現していこうと取り組んでいます。

ちなみにこういった話については、2023 年に開催された「G7 群馬高崎デジタル・技術大臣会合」でも閣僚宣言が行われたときに Beyond 5G/6G 時代の将来ネットワークに関する G7 ビジョンということで承認をされ、世界にもこういったネットワークが重要だということがしっかり発信されました。

なお、総務省でも昨年 8 月に Beyond 5G の実現を一層推進していくということで、特にこの AI の爆発的な普及といった環境変化を踏まえ、新たな戦略をまとめています。

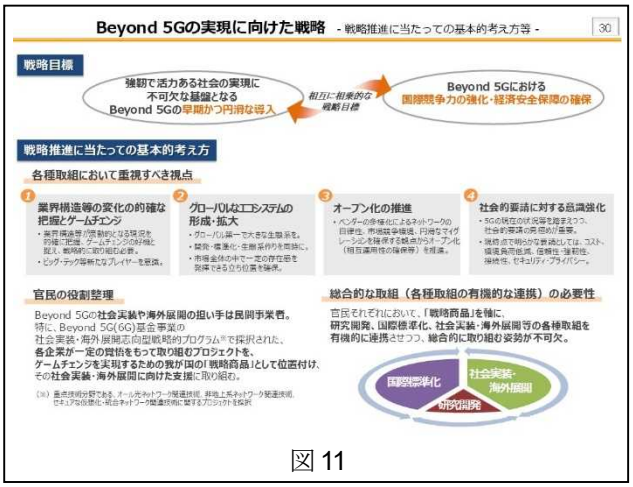


図 11

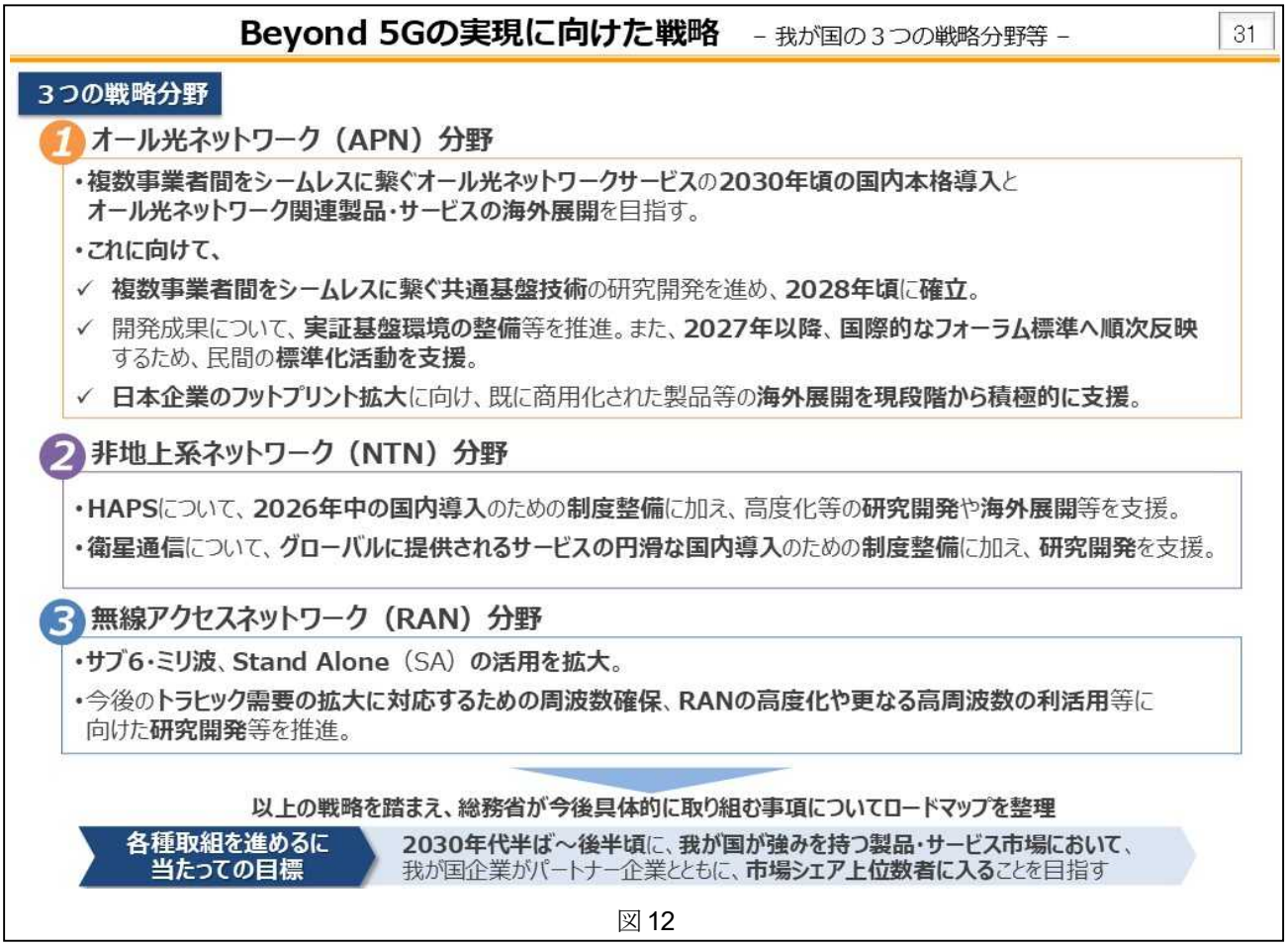


図 12

戦略の目標としましては、Beyond 5G の早期かつ円滑な導入に合わせ、この Beyond 5G を使い、国際競争力を強化していくことも相互に相乗効果のある目標として挙げています。4 点重視すべき視点を挙げていますが、変化が激しい ICT 分野において、産業構造もどんどん変わる昨今、それをしっかり把握していこうと考えています。国内にとどまらず、国外をきちんと見てグローバルファーストの立ち位置を確保していく。それとガラパゴスにならないよう、相互運用性の確保といったオープン化を推進する。そして、コスト、環境負荷の低減、信頼性、セキュリティといった社会的要請にアンテナを高くして対応していこうと考えています。

その上で民間事業者の役割ですが、とかく研究開発プロジェクトは研究開発で終わってしまうパターンも現実には結構ありますが、Beyond 5G についてはそうではなく、社会実装、海外展開を絶対に行う覚悟を持って取り組んでくださる方を総務省は支援します。また、こうした各企業が取り組むプロジェクトを「戦略商品」と位置づけ、総務省としては、その社会実装、海外展開に向けた支援に取り組んでいます。

図 12 では、戦略的に取り組む分野である APN、NTN、RAN の分野を挙げています。少し細かい目標も入れましたが、APN 分野については一つの事業者だけでなく、複数事業者間をつなぐネットワークサービスを 2030 年ぐらいには国内に導入し、海外にも展開する。それから、複数事業者間をシームレスにつないでいくためには共通の基盤技術を開発しないといけないので、これは 2028 年頃を目指す。併せて実証環境についても、予算を獲得し進めていくべく取り組んでいます。

また、NTN の関係では、HAPS については 2026 年中に国内導入するための各種制度整備や、研究開発支援を行っていきます。また、衛星通信についても制度整備、研究開発支援を進めていくこととしています。

RAN の分野では、高い周波数帯をしっかり活用していくことや、5G の Stand Alone についての活用拡大、それと今後のトヒック需要拡大に対応するため、さらに高いほうの周波数帯の確保、研究開発も行っていこうとしています。

量子に関する取り組み

量子技術は大きく 3 種類あります。まず 1 つがスパコンの能力を超える計算力を持って、今まで計算できなかったものが計算できるようになる量子コンピュータ分野です。それから量子を使うことによりセンサーの精度が向上することで、今まで見えなかったものが見えるようになる量子センシング・計測分野があります。そしてまさに総務省が担当、推進する部分になりますが、量子の性格として、盗聴されると中身が変わるということで盗聴を検知できます。これにより暗号鍵を安全に伝送することができるようになります。これが量子暗号通信で、私たちはこの量子暗号通信の早期実装を目指して様々な支援を行っています。

量子暗号通信の中身に入る前に、現在の暗号通信とその課題についてお話したいと思います。今、私たちが使っている暗号方式は、現行の計算機、およびもう少し先の計算機までを含めた能力では解析にスパコンを使っても膨大な時間を要し、そんなに時間がかかるゆえ解析が現実的ではないということで解読できない、という前提で今の暗号方式は使われています。但し、量子コンピュータが登場してきて、その卓越した計算力により既存の暗号方式が現実的な時間で、例えば 100 日ぐらいで破られてしまうことが判ってきました。最近言われるのは、今は破られないけれども取りあえずデータを取っておき、計算資源が高速化されたときに、「Harvest Now」と言いますが、後で解読するというようなことも指摘されており、暗号が危殆化する危険が高まってきています。

これに対抗する技術として、国際戦略局でも取組みを進めている量子暗号通信あるいは量子鍵配送と、耐量子計算機暗号（PQC）が世界各国で取り組まれているということになります。

まず量子暗号通信の仕組みについて説明します。量子状態の光が観測されると状態が変化することが分かっています。これを使うと暗号鍵が盗聴されたかどうかが受信側で判別できますので、盗聴された暗号鍵は捨てるということで安全性が確保されます。ただ、この方式は光子を扱うということで、一対向で 1 億円程とか、非常に高額な専用装置がまだ必要となるという状況にあります。

図 14

図 13

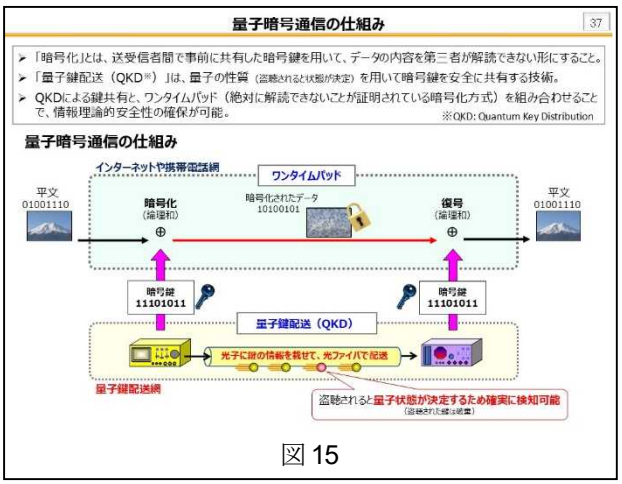


図 15

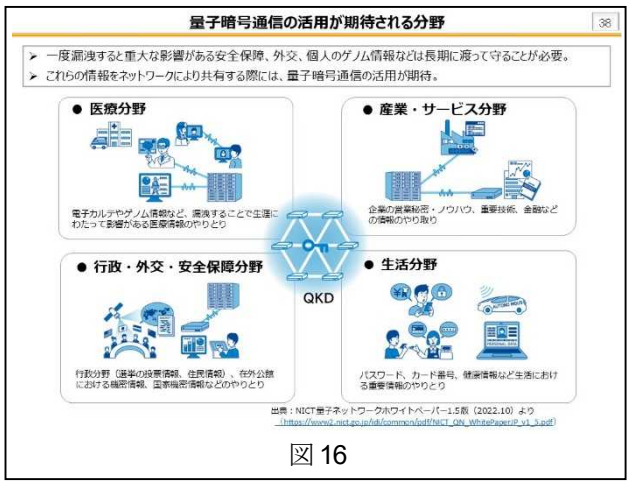


図 16

もう一つは、PQC と呼ばれる耐量子計算機暗号です。これは一言で言うと、量子コンピュータが得意としない、例えば格子問題のような数学問題を用いた暗号方式となります。ソフトウエア的に解決をしていくので、ユーザー1 人当たりという観点であればコストは安くなるというメリットもあるのですが、そういう仕組みにつくり直さないといけないということで、いろいろなものの今使っている暗号方式を全部変えていく必要がある、また全面移行に時間がかかるというデメリットもあります。

こうした中で、PQC なのか、量子暗号通信なのかは保有しているシステムに応じ、どちらが適正なのかをそれぞれで考えながら入れていくことになります。量子暗号通信は、絶対に解読できないということが既に証明されているワンタイムパッドという暗号方式で暗号化されたデータ自体はインターネットで送ります。暗号化に使った鍵を量子にて鍵配送ネットワークで送るということを行い、この鍵は仮に盗まれてもすぐに気づくことが出来るので、もし見られてしまった場合はもう一回鍵を送り直すことで鍵の安全性を共有します。

このワンタイムパッド方式については昔からある暗号方式で、絶対に安全なのですが、その鍵をどうやって相手に届けるかが課題でした。今はアタッシェケースに入れて持っていくとか、そういう世界ですが、この量子鍵配送を使うことによって絶対に解読できないこのワンタイムパッドの暗号鍵を光で送ることができるようになる。これにより、情報理論的安全性が確保されるというものになっています。

では、この量子暗号通信が実際にどういう場で使われるかですが、やはり一度漏えいしてしまうと、重大な悪影響があると想定される情報のやり取りでの活用が先ずはあるであろうということで、医療分野である電子カルテ、ゲノム情報などが対象になるでしょう。それと外交、安全保障分野での国家機密情報や企業の営業秘密、金融情報のやり取り、そういったところで使われていくものと考えています。

量子コンピュータの開発が非常に加速化している中で、現行の暗号通信の危殆化が懸念されており、世界各国で量子暗号通信の導入に向けた動きが進展しています。諸外国の状況としては、中国では既に約 80 都市をカバーする総延長 1 万キロ以上の量子暗号通信ネットワークが構築されていると言われています。韓国でもソウル、釜山間 490 キロメートルのネットワークがあります。それからロシアでは研究機関間を結ぶ 160 キロのテストベッドがあるということです。欧州では全域で量子暗号通信ネットワークを整備するということが既に決定されていて、調達手続も始まっています。日本では量子暗号通信の課題について、種々の実証を行っていく東京 QKD ネットワーク（テストベッド）を NICT が構築をしており、このテストベッドの上でいろいろな信頼性の試験などを行っています。運用の蓄積も 2010 年からの立ち上げ以来、実際に世界で最も長い運用実績となっています。総務省としては 2030 年までに量子暗号通信網の社会実装と国際競争力強化を目指し、研究開発の支援および国際標準化について NICT としっかり推進していきたいと考えている分野になります。

図 17

宇宙通信に関する取り組み

宇宙産業はとても伸びており、モルガン・スタンレーによると世界の宇宙市場、2040 年には 1 兆ドル超の市場規模になると言われています。日本政府も、宇宙基本計画の中で宇宙産業を日本経済における成長産業に位置づけようということで、2020 年に 4.0 兆円の市場規模を、2030 年代の早い時期に 2 倍の 8.0 兆円に拡大していくことを掲げています。

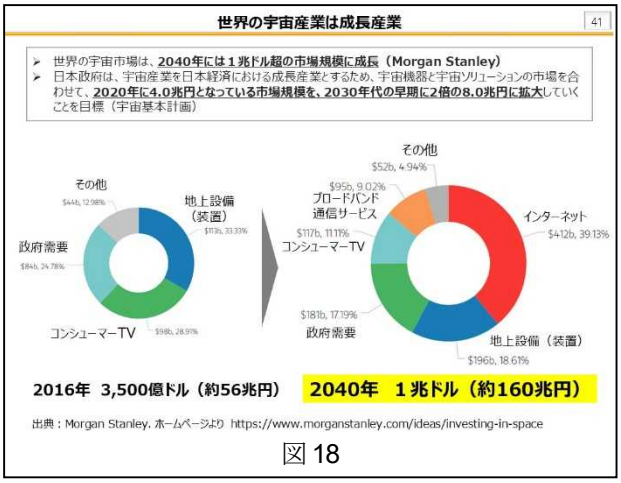


図 18

宇宙における活動領域が拡大していく中で、この通信インフラ・サービスの重要性が高まってきており、世界的に業界構造が変わってきています。まず使われるデータとして、地球の観測衛星が取る衛星画像や各種観測データなど宇宙空間でのデータ需要が大きく増えていて、高速大容量伝送が必要になってきています。これに伴い、最近 LEO と呼ばれる低軌道衛星コンステレーションが台頭してきていて通信事業に大きな影響が出てきています。また、スマホと通信衛星の直接通信も今年中には実現ということで、地上の通信網と NTN との融合への期待が高まっています。あとは、低軌道のコンステレーションの台頭を受けて、今まで別々に使われていた静止衛星事業者、非静止衛星事業者、携帯電話事業者の統合、協業が世界中で進展してきている状況にあります。この衛星通信は、離島、山間部などの電波が届かない、ケーブルが引けないといったところの通信インフラとして、また災害が発生した際のバックアップとしても大変重要な役割を担っています。

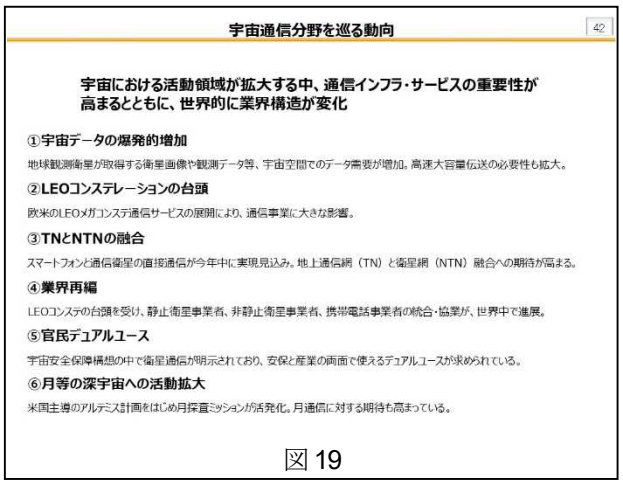


図 19

図 20 の右下の図にあるように、衛星通信分野の市場規模は、2035 年には 2180 億ドルぐらいになるだろうという予測もされています。

図 20

こうした中で宇宙分野での研究開発をしっかりと行っていくため、国の予算は年度単位になっていますが、単年度で切れてしまうと長期的に取り組めないであろうということで、複数年度にわたりこの分野で民間企業や大学が大胆に研究開発に取り組めるよう新たな基金を創設する運びになりました。

2023 年 11 月に経済対策、いわゆる補正予算が組まれる際、宇宙分野について複数年度にわたり先端技術開発、技術実証、商業化を支援するため JAXA に 10 年間の「宇宙戦略基金」を設置し、速やかに総額 1 兆円規模の支援を行うことを目指すことが明記されました。

図 21

これを踏まえ 2023 年度補正予算で、宇宙戦略基金が JAXA に造成されました。これは、実際には内閣府と総務省、経産省、文科省が一緒に取り組んでいます。

総務省もこの宇宙戦略基金を活用し、量子暗号通信の衛星版があると外国ともより安全な通信ができるようになるということで、衛星量子暗号通信技術の開発、衛星コンステレーション構築のための技術の実証、月面の水資源探査に向けたセンサー関係の研究開発などを宇宙戦略基金で推進していくこととしています。なお、2024 年度も補正予算を確保し、衛星間での光通信技術の開発にも取り組んでいます。

宇宙戦略基金 技術開発テーマ（令和５年度補正・総務省分）一覧

45

➢ 令和５年度補正予算にてJAXAに造成された宇宙戦略基金（総務省分：240億円）を活用し、今後10年で取り組むべき技術開発のうち、宇宙分野での計画や資金ニーズが顕在化しており、速やかに支援に着手すべき技術開発の内容を、当面の 事業実施に必要となる支援規模、期間等とあわせ、技術開発テーマとして設定。

※このほか、令和５年度補正予算の内訳としては本基金事業の管理費（７億円程度）を含む。

衛星等

衛星量子暗号の通信技術の開発・実証

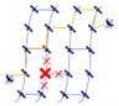
距離に依らない堅牢なセキュリティ環境を実現する量子暗号通信網の構築に向けた衛星搭載用の通信機器 及び地上局設備の開発・実証

支援規模：145億円/１件程度
支援期間：５年間程度

衛星コンステレーションの構築に必要な通信技術の実装支援

大容量リアルタイム通信が可能な衛星間光通信におけるキー技術として、相互運用性、高速性、安定性等を備えたネットワークに必要な光ルータ等の技術開発

支援規模：19億円/１件程度
支援期間：３年間程度



探査等

月面水資源探査技術

センシングによる効率的な月面水資源探査に向けた、小型軽量なセンサを搭載した小型衛星の開発・実証

支援規模：64億円/１件程度
支援期間：４年間程度

月-地球間通信システム開発・実証FS

月-地球間における大容量かつ高精度捕捉等が可能な通信アンテナの開発に向けた基本設計、高品質・高信頼性のモバイル通信環境の実現可能性の調査

支援規模：５億円/１件程度
支援期間：１年間程度

図 22

宇宙戦略基金 技術開発テーマ（令和６年度補正・総務省分）一覧

46

①衛星光通信を活用したデータ中継サービスの実現に向けた研究開発・実証

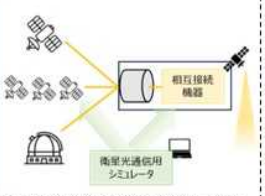
支援総額　　：235億円
採択予定件数　　：１件
最長支援期間(SG※1)　：５年程度※2(3年目)

【概要】
我が国の事業者による光通信を利用した軌道間のデータ中継サービスの商用提供の開始に向けた、静止軌道と低軌道等との間における衛星光通信技術(データ中継)の確立、ネットワークの制御及び監視が可能なシステムの開発並びにこれらを一体とした実証を行う。

②衛星光通信の導入・活用拡大に向けた端末間相互接続技術等の開発

支援総額　　：(A)25億円、(B)５億円
採択予定件数　　：(A)１件程度、(B)１件程度
（A、Bを同一の事業者が実施することも可）
最長支援期間(SG※1)　：３年（１年目）

【概要】
衛星光通信の導入・活用拡大に向けた(A)衛星光通信端末の相互接続の確保に関する技術及び(B)光通信を行う衛星間の捕捉・追尾や衛星姿勢等の計算を支援するソフトウェア等の開発等を行う。



③衛星光通信の実装を見据えた衛星バス及び光通信端末の開発及び製造に関するフィージビリティスタディ

支援総額　　：４億円
採択予定件数　　：２件程度
最長支援期間(SG※1)　：２年（１年目）

【概要】
2030年代以降を見据え、衛星光通信において使用する衛星バス及び光通信端末の国際競争力確保のために必要となる技術的要件・国際競争力確保の要件を調査・検討し、産業基盤を構築する方策を検討する。

④国際競争力ある通信ペイロードに関する技術の開発・実証

支援総額　　：58億円
採択予定件数　　：１件程度
最長支援期間(SG※1)　：５年程度（２年目）

【概要】
国際競争力の観点で優位性を有する通信ペイロードの基盤技術の獲得・製造能力の自律性を確保を目指し、衛星機能の柔軟性の確保等の需要に対応する国際競争力ある通信ペイロードに関する技術の開発・実証を行う。

⑤衛星通信と地上ネットワークの統合運用の実現に向けた周波数共用技術等の開発・実証

支援総額　　：110億円
採択予定件数　　：１件
最長支援期間(SG※1)　：５年程度※2(３年目)

【概要】
我が国の事業者がコントロール可能な衛星通信と地上ネットワークの統合運用の実現に向けた、周波数共用技術の開発及び実証を行う。

※１ SG（ステージゲート評価）の時期はいずれも目安であり、事業計画等によって時期の変更があり得る。
※２ ステージゲート評価等を踏まえ、支援総額の範囲内でさらに必要な期間（１年程度）を追加することが可能。

図 23

サイバーセキュリティに関する取り組み

次は、サイバーセキュリティの分野です。インターネットがつながり非常に便利になって、インターネットを使い成長がより一層進んでいるところですが、この成長を支えているインターネットに忍び込み、そして悪いことをする、というのが非常に増えていて、その被害も深刻化しています。攻撃手法としては、2000 年頃はネットがつながり、みんなが使い慣れてきたときに、少し自分のネットワークの知識をひけらかしてやろうというのでシステムに入り込んでみたり、また DDoS 攻撃をしてみたりなど、とにかく自分はすごいぞというのをひけらかすような攻撃からスタートをしていました。

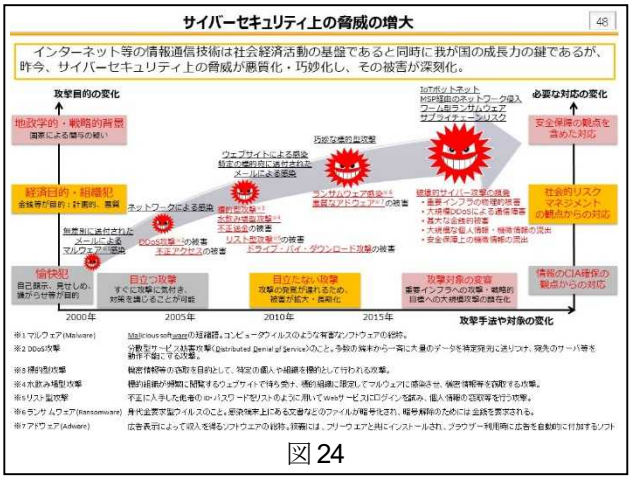


図 24

2010 年頃から機密情報を窃取することを目的とした攻撃が始まります。普段皆さんもメールに関する訓練をされていると思いますが、一見業務上のメールと信じてしまうようなものが来る、しかし実はそこにマルウェアが仕組まれていて添付ファイルを開けたら感染する、感染しても何も気づかず、そしていつの間にかどんどん情報が漏えいしている、という、本人は気づかない、目立たない攻撃が増えてきています。この目立たない攻撃は大量に機密情報が流出してしまった後に、誰かが流出しているよと言って初めて気づくということで、被害が拡大したり、長期化するものとなっています。またその間に感染端末上の文章などのファイルが暗号化されて、暗号解除のために金銭を要求される。いわゆる身の代金要求型（ランサムウェア）の被害が増加してきています。最近では重要インフラの物理的な被害とか、それから大規模な DDoS 攻撃による通信障害、ほかに莫大な金銭被害を与えるもの、また個人情報、機微情報を大規模に流出してしまうもの、さらには安全保障系のところが被害に会うなど、破壊的なサイバー攻撃も頻発するようになってきています。

国内の事例で言えば、病院がランサムウェアによる攻撃を受け電子カルテが暗号化されてしまい、予約が受け付けられないだけではなく、外来の診療ができなくなったり、手術が停止してしまった事例がありました。それから自動車部品のメーカーへのサイバー攻撃により、自動車会社が国内全工場の稼働を一旦停止しなければいけないという事例もありました。また港でランサムウェア攻撃を受けて、コンテナの搬入が停止してしまった事例もありました。このように企業、組織、個人の活動に非常に重大な影響を与える事案が出てきている状況にあります。

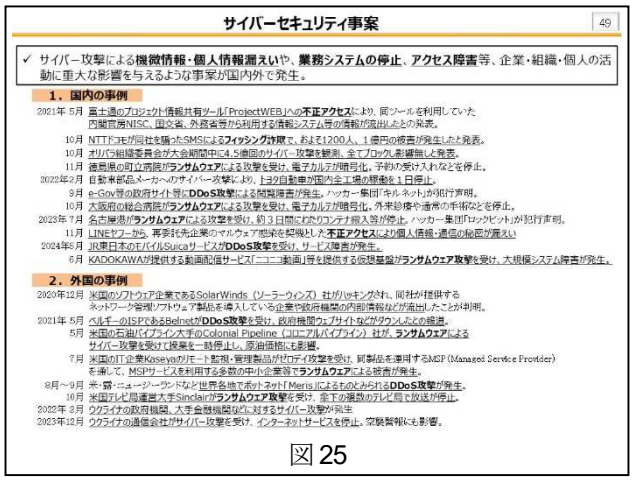


図 25

ここでまた NICT の取組になりますが、10 年ほど前から NICTER というサイバー攻撃観測網を運用しており、その規模がどんどん大きくなっています。今ではこの NICTER は約 30 万の未使用の IP アドレスを利用し、インターネット上にこの未使用アドレスをセンサーとして設置をすることで、攻撃者が攻撃対象の探索（スキャンと呼ばる）を行う通信を 24 時間大規模に観測しています。仕組みとしては、このセンサーは外部に何もサービスを提供していないので、本来は、外部から通信パケットが来るわけはないのですが、攻撃者がどこか脆弱性がないかと探すスキャンをするときの不特定多数の IP アドレスに対し無差別に送信する送信パケットを観測する、という仕組みになります。

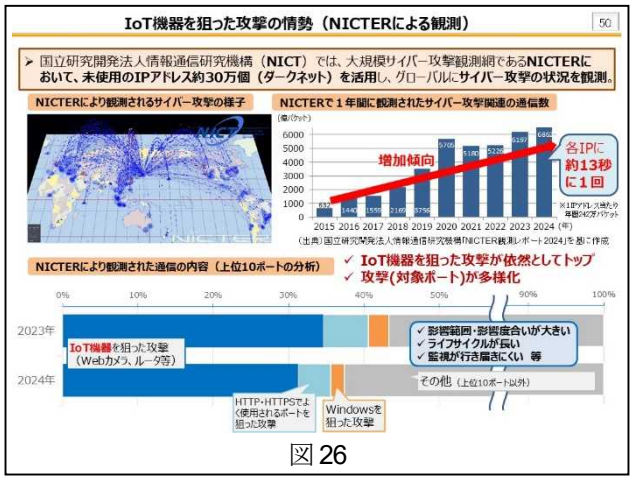


図 26

図 26 の右側のグラフ「NICTER で 1 年間に観測されたサイバー攻撃関連の通信数」ですが、これはサイバー攻撃そのものではありません。踏み台とかボットとか聞かれたことがあると思いますが、サイバーセキュリティ対策が十分ではない機器が、遠くにいる攻撃者からこいつは脆弱だから使ってやれと乗っ取られ、ロボットみたいに使われて攻撃をしてくるというものになります。そういう攻撃関連通信、踏み台になってしまったところから飛んでくる通信が非常に増えてきており、その中身が、どういう種類のパケットなのかを見てみると、IoT 機器を狙ったものが依然としてトップを占めます。これは即ち、サイバー攻撃が行われるときは脆弱な機器が狙われることを意味します。その脆弱な機器 IoT 機器が踏み台になって例えば重要なインフラなどへの攻撃が行われるので、この IoT 機器の脆弱性をなく

していく取組を行うことが非常に重要になるのです。

これまでも総務省、NICT で IoT の脆弱性を調べ、簡単に破られてしまう ID やパスワードが設定されている機器を見つけ、所有者に注意喚起を行うというプロジェクトを行ってきて、ID・パスワードに脆弱性のある IoT 機器が少なくなってきたかと思いきや、未だ 10 年以上前の機種が 4 割も世の中に存在することが見えていまして、まだまだ今後も継続していかなければいけません。またここ数年の傾向として、単に ID・パスワードが緩いというだけではない、例えばファームウェアに脆弱性があるというような攻撃も発生してきています。またマルウェアの活動も依然として活発です。サイバー攻撃関連の通信の対策はいろいろ行ってきていますが、5 年前と比較して 3 倍増加しているという観測もなされています。

利用者の意識に関する課題もあります。例えば Wi-Fi ルータの利用者向けのアンケートでは、約 58%の利用者が Wi-Fi ルータのセキュリティを意識していないと答えています。まだまだ利用者の意識も十分ではありません。なお、法人利用者については、監督、管理責任の所在が曖昧といった適切な管理体制がとられていないという報告も行われています。サイバーセキュリティの課題は提起されて久しいものの、周知啓発をどんなにやってもまだまだ足りないと感じているところです。

IoT 機器の脆弱性を利用されたサイバー攻撃にどう対処するというときに、2 つのアプローチがあります。1 つはそもそもこの踏み台となりボット化される IoT 機器に指令を出してくる大本の（悪い）コマンド&コントロールサーバを検知し、対処を行うというもの。それと 2 つ目は、ボットになり、ウイルスに感染した IoT 機器、これから感染してしまうかもしれない弱い機器について、どこにそういった機器があるかを検出し注意喚起をしていくもの、この 2 つの面から対策を行っていかなければなりません。

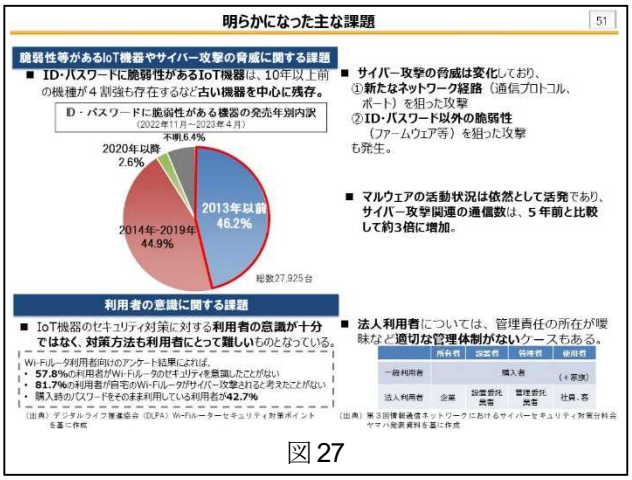


図 27

まず 1 つ目についてですが、総務省では、通信事業者でフロー情報と呼ばれる、IP アドレスといったようなヘッダーの情報（中身ではなく機械的な情報）を分析することで、ボット化した IoT 機器に攻撃指令を行う可能性のあるコマンド&コントロールサーバについて攻撃が実際に出される前に検知をし、攻撃の対策に活用していくという実証事業を進めています。

実際にコマンド&コントロールサーバは、攻撃を出す前に自分の部下となったボットへ「生きているか」みたいな感じで度々通信するのです。そういったところを捉えて、未然にコマンド&コントロールサーバを見つけていくことを実証で行っています。

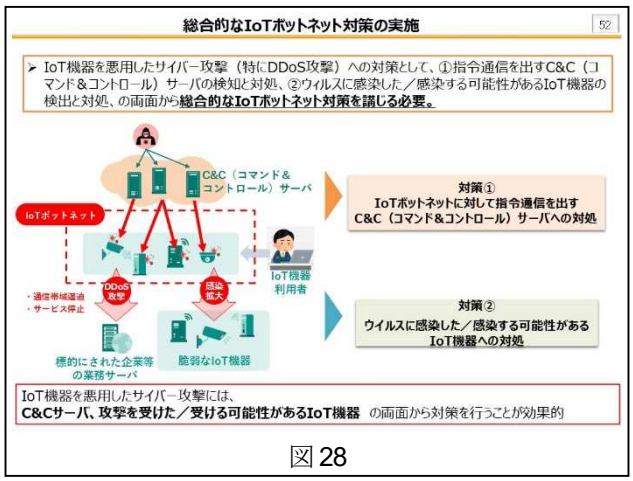


図 28

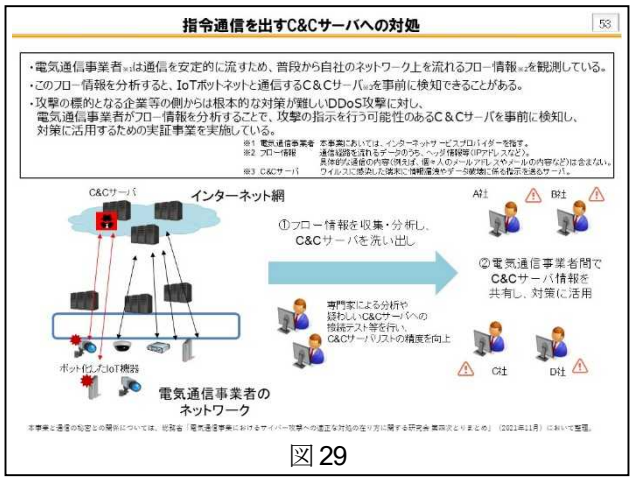


図 29

2 つ目については NOTICE と呼ばれるプロジェクトで、NICT が、容易に推測されるような ID・パスワードを設定している機器をスキャンして調べていったり、ファームウェアが脆弱になっている IoT 機器を見つけたり、マルウェアに実際に感染してしまっている IoT 機器などを観測して、ISP や機器メーカーと協力し脆弱な IoT 機器の所有者に注意喚起をする取組を行っています。

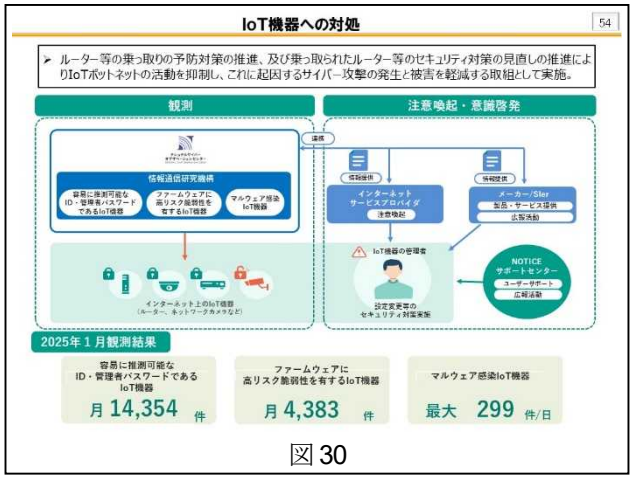


図 30

今年1月の観測では、容易に推測できるID、管理者パスワードを設定しているIoT機器が14,000件以上見つかっています。マルウェアに感染しているIoT機器は一日で最大約300件検出をされているということで、日々いろいろな攻撃が行われています。

こうした国内の多くのIoT機器が、所有者が全く気づかないうちにDDoS攻撃の発生源、ボットになってしまっているということで、総務省としても普及啓発を推すべく「推定しにくいパスワードを設定してください」や「ソフトウエアを更新してください」、「IoT機器の利用していない機能を停止してください」などといったことをうったえています。

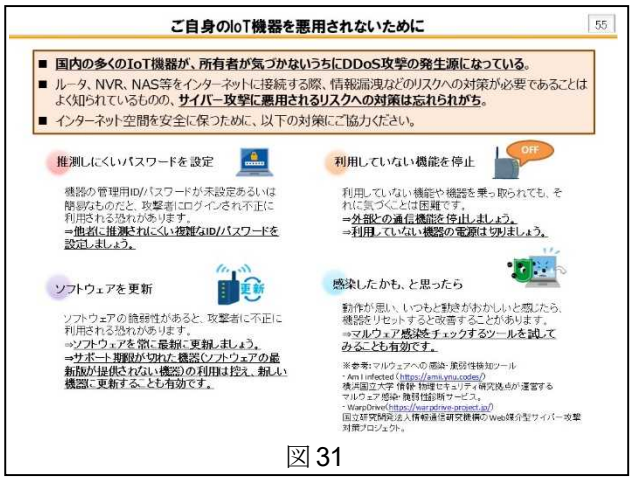


図31

イメージ的には家の戸締まりの話と同じで、「窓を開け過ぎないで」や、「目が行き届かない窓を開けたら誰か入ってきますよ」というレベルのことなので、通信においてもボットは止めてくださいという、そういった意識啓発を行っています。

我が国においては、サイバーセキュリティ人材が少ないと言われています。日本と海外を比べると、セキュリティ対策に従事する人材が少ないと感じている割合が日本はかなり多くなっています。やはりセキュリティへの投資はコストになると言う経営者の方がまだ多く、なかなかそこのセキュリティ対策がなされないのですが、これからはセキュリティ対策は投資だと考えられなければいけないと思います。これももう数年前から言われていますが、まだまだ進んでいないというのが現状です。なお、各社においてセキュリティ人材の育成は喫緊の課題だといったアンケート結果もあります。

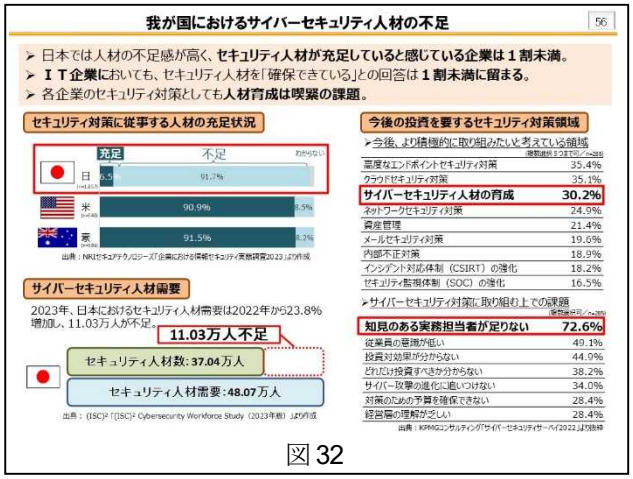


図32

こうした状況を捉え、総務省では2017年からNICTで演習を行っています。国の機関、指定法人、独立行政法人、自治体、重要インフラ事業者の情報システム担当者を対象として、体験型の実践的なサイバー防御演習（CYDER）を行っています。

この演習では、受講者はチーム単位で作業します。これは企業で情報システム室などはチームでサイバー攻撃に対応してきていますので、同じようにチームで演習に参加をしてもらい、その組織のネットワーク環境を模擬した大規模な仮想のLANの環境をつくって、その中で実機の操作を行いながら、「ここで攻撃を受けました」、「そこのログを取ります」、そして外部のセキュリティ業者やベンダーに連絡して対策を施す、というような一連の流れを体験していただいています。

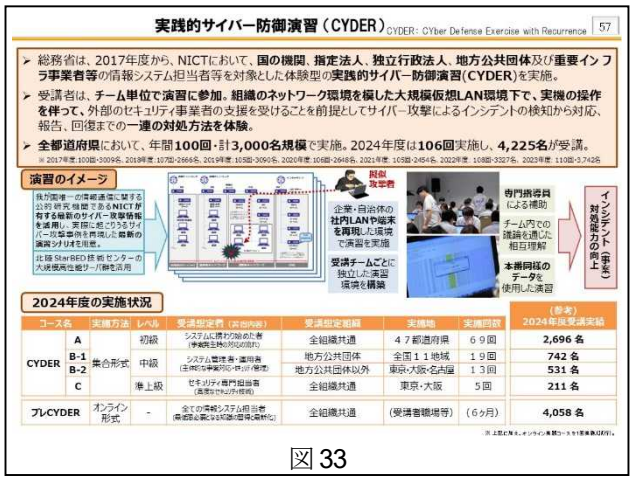


図33

このサイバー攻撃に対する対応はエスカレーションと言いますが、報告をいかに素早く行っていくかが非常に重要なので、それを体験していただくことを行っています。これまで全都道府県で年間100回、合計1年当たり参加者3,000名規模で実施してきています。2024年度は年間106回、4,000名以上に受講をしていただいています。

あとはトップクラスの若手人材を育成することを目的として、25歳以下の若手を対象としたSecHack365というプログラムもNICTで提供しています。

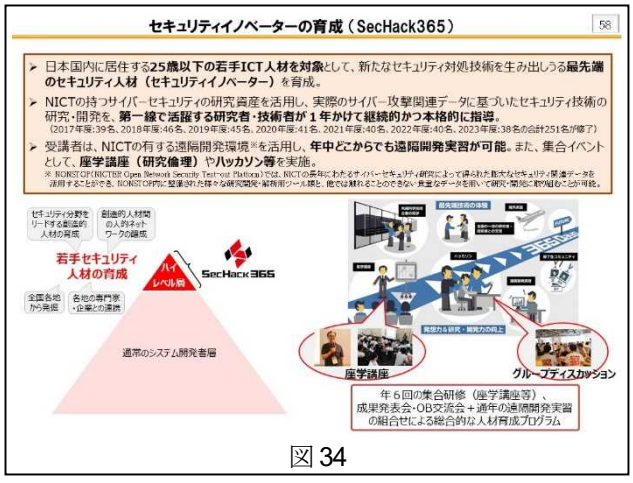


図34

これは NICT の様々な知見、および豊富なデータを活用し、実際のサイバー攻撃関連のデータに基づいたセキュリティ技術の研究や開発を、第一線で活躍する NICT の研究者と技術者が 1 年間伴走支援をし、指導していくものです。2017 年度に開始してから 24 年度まで合計で 328 名が今まで修了しています。24 年度は 39 名参加しました。実際、小学生の方が参加したときもありました。修了生はいろいろな場面で活躍されています。例えば、大学院の修士課程 2 年のときに参加してくださった修了生は、そのときの成果物のゲームを基に起業して、その後国立大学の学長特別補佐として大学での起業支援を行ったり、本を出版したりされています。このように活動の幅を広げている方もおられ、総務省としても、これからもこうした若手人材の育成に力を入れていきたいと思っております。

NICT 次期中長期目標・計画策定に向けた議論

NICT は 5 年ごとに中長期の目標・計画を定め、これに沿って研究開発を行っていますが、ちょうど令和 8 年度から次期中長期の時期に入ります。第 6 期の期間に入るということで、今、情報通信審議会の技術戦略委員会において、NICT が取り組むべき重点的研究分野、それと成果展開の推進方策などについて議論をいただいています。

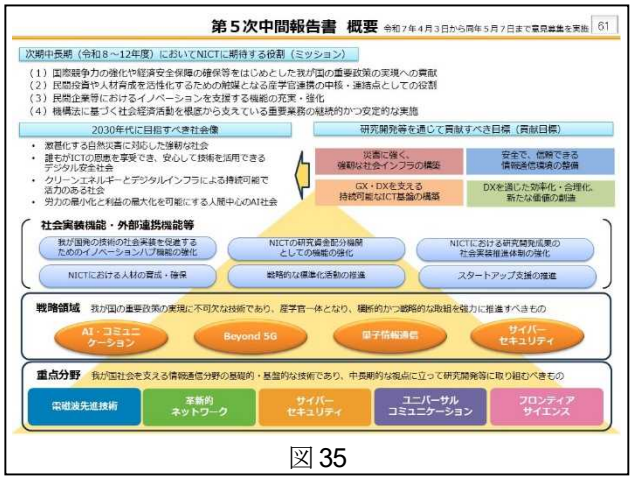


図 35

なお、図 35 の通り報告書案がまとまってきていまして、5 月 7 日まで意見募集を行っていたものになります。令和 8 年度から 5 年間の次期中長期に NICT に期待するミッションが、上に 4 点書かれています。1 点目が、国際競争力の強化や経済安保の確保といった日本の重要政策を実現するための貢献を行うこと。2 点目としては、民間投資や人材育成を活性化する触媒としての役割、産学官連携の中核・連結点としての役割を果たすということ。3 点目が、民間企業におけるイノベーションを支援する機能の充実・強化をしていくこと。そして 4 点目として、NICT 法に基づく社会経済活動を支えている種々の重要業務の継続的かつ安定的な実施、こういったミッションがまとめられています。

戦略領域はもともと前期より AI、Beyond 5G、量子情報通信、サイバーセキュリティの 4 つとなっていますが、これらの分野について考えると AI やサイバーセキュリティについては社会的な重要性がさらに増大してきているということ、また Beyond 5G や量子情報通信については、今、社会実装に向けて重要な局面にあるということで、引き続きこれらの分野をしっかり進めていくというのが基本的な考え方になっています。

図 36

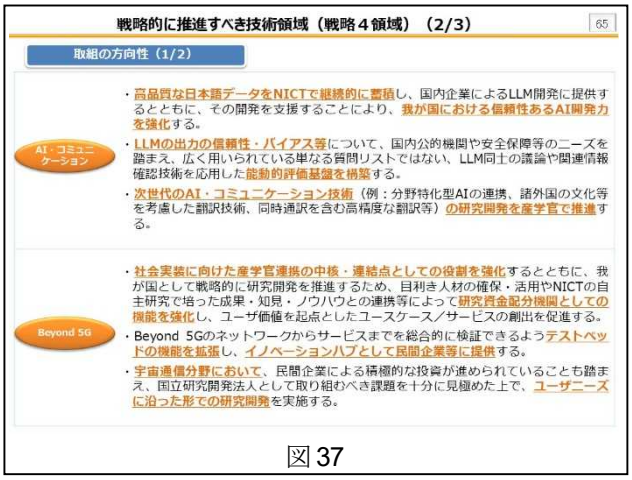


図 37

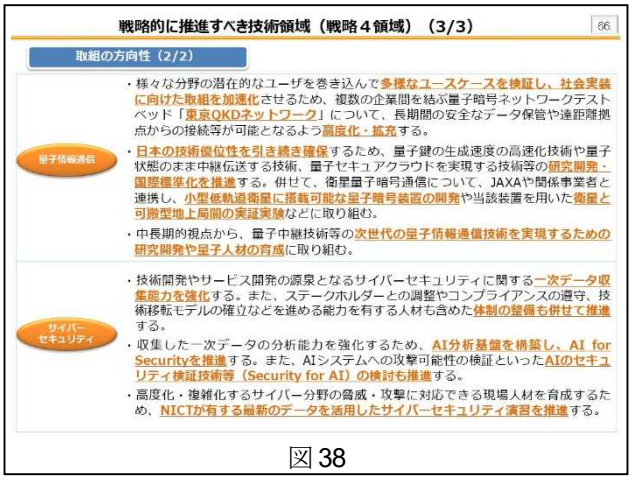


図 38

図 39

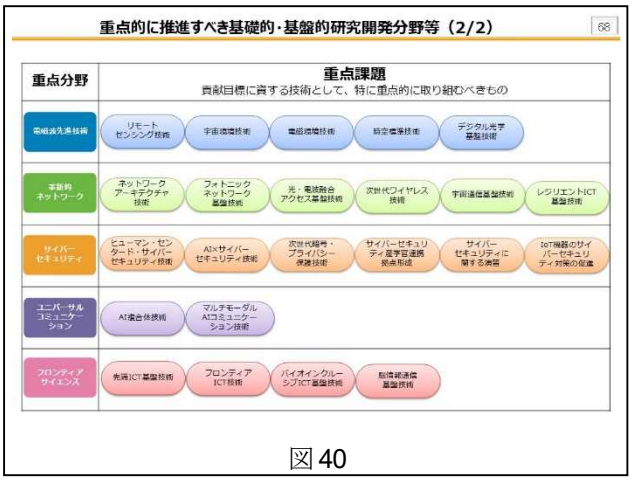


図 40

これから NICT は社会実装に特に力を入れていくので、今後 NICT が持っているテストベッドをもっと沢山の人が使いたくなるものにする、や、Beyond 5G 基金におけるファンディングエージェンシーとしての機能を強化していく、あるいは技術シーズとニーズの橋渡しとして、大学と企業との連携をさらに進める、他は人材育成、技術移転関係、標準化活動、スタートアップの支援、等々を着実に進めて研究開発成果が確実に社会実装されていくことを、しっかり行っていくことを目指し計画をまとめているところです。

以上､最近の技術政策の取組を御紹介させていただきました。