

# 令和3年度 総務省科学技術関係予算概算要求 について

---

令和2年11月17日

総務省国際戦略局  
技術政策課

- ウィズコロナ/ポストコロナ時代において、ICTを最大限に活用した社会的課題の解決や経済的発展を目指し、令和2年8月に情報通信審議会より**戦略的に進めることとされたBeyond 5Gをはじめとする研究4領域**等の研究開発、国際標準化及び成果の迅速な社会実装を推進。
- ICT分野唯一の国立研究開発法人である情報通信研究機構（NICT）により、中長期的な視点から基礎的・基盤的研究開発を推進。

## 政府戦略等

**AI戦略2019**（令和元年6月11日 統合イノベーション戦略推進会議決定、  
令和2年6月22日 AI戦略実行会議フォローアップ）

**Beyond 5G推進戦略**（令和2年6月30日 総務省）

**量子技術イノベーション戦略**  
（令和2年1月21日 統合イノベーション戦略推進会議決定）

**サイバーセキュリティ戦略**（平成30年7月27日 閣議決定）

## 戦略領域

**AI**  
（脳情報通信  
・データ利活用）

**Beyond  
5Gの実現**

**量子情報  
通信**

**サイバー  
セキュリティ**



# 令和3年度総務省所管予算(案)における主な科学技術関係予算

2

- Beyond 5Gをはじめとした先端技術への戦略的投資を実施
- 具体的には、①Beyond 5G、②量子暗号通信、③AI(多言語翻訳)、④サイバーセキュリティ等の実現のための研究開発を推進。主な重点施策は次ページ以降のとおり。

単位：億円

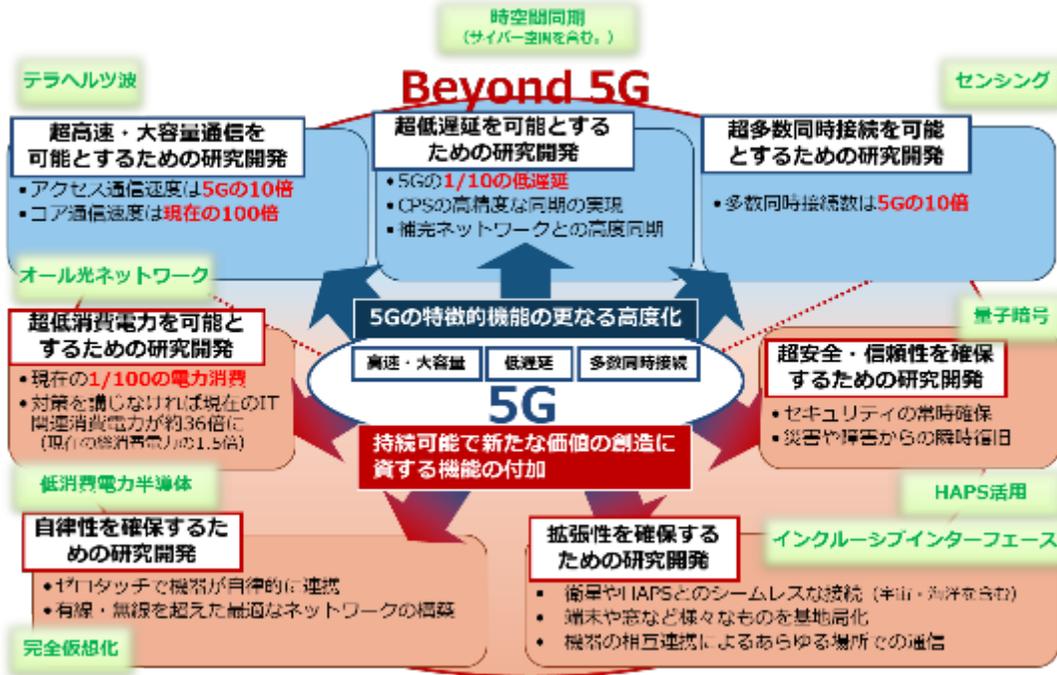
施策名	R2年度 予算額	R3年度 概算要求額	新規
Beyond 5G研究開発促進事業	-	50.0	○
国立研究開発法人情報通信研究機構施設整備費補助金	0.9	20.9	
新たな社会インフラを担う革新的光ネットワーク技術の研究開発	9.5	8.5	
仮想空間における電波模擬システム技術の高度化	30.1	40.0	
5G高度化等に向けた総合的・戦略的な国際標準化・知財活動の促進		6.2	○
戦略的情報通信研究開発推進事業	12.2	10.0	
電波資源拡大のための研究開発	103.4	132.2	
国立研究開発法人情報通信研究機構運営費交付金	279.4	283.4	
衛星通信における量子暗号技術の研究開発	3.4	5.0	
グローバル量子暗号通信網構築のための研究開発	14.4	14.5	
グローバル量子暗号通信網構築のための衛星量子暗号通信の研究開発	-	15.0	○
多言語翻訳技術の高度化に関する研究開発	14.0	14.0	
サイバーセキュリティ統合知的・人材育成基盤の構築	-	20.0	○

# 1. Beyond 5Gをはじめとした先端技術への戦略的投資

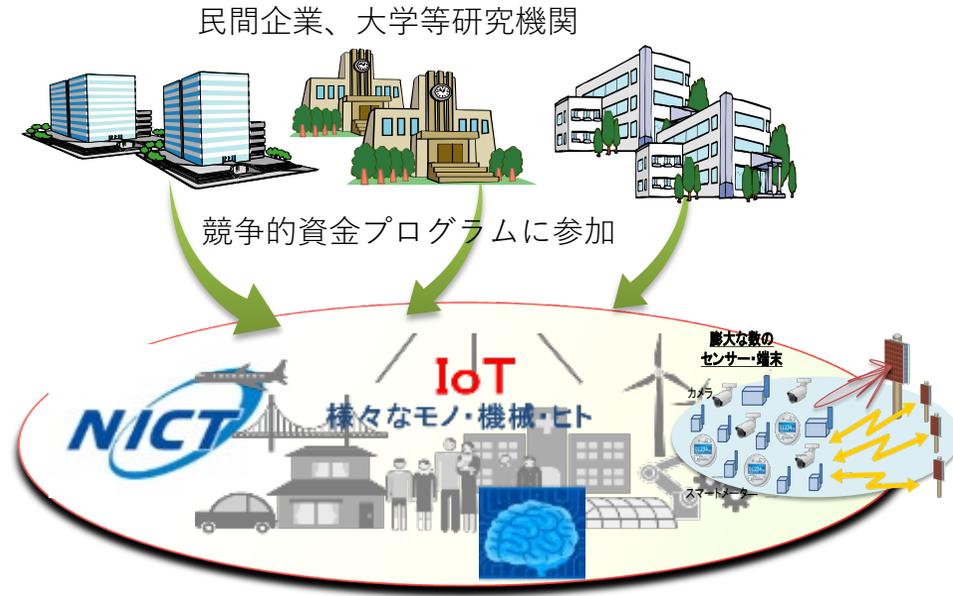
- ① Beyond 5G研究開発促進事業
- ② 国立研究開発法人情報通信研究機構施設整備費補助金

・Beyond 5G実現に必要な要素技術等の研究開発を行う競争的資金プログラムを実施するとともに、Beyond 5Gの研究開発に必要なテストベッド等の共用施設・設備をNICTに整備し、官民の叡智を結集したBeyond 5Gの研究開発を実施。

- ① 令和3年度概算要求・要望額：50.0億円（新規）
- ② 令和3年度概算要求・要望額：20.9億円（令和2年度予算額：0.9億円）



Beyond 5Gに必要なとされる研究開発事項



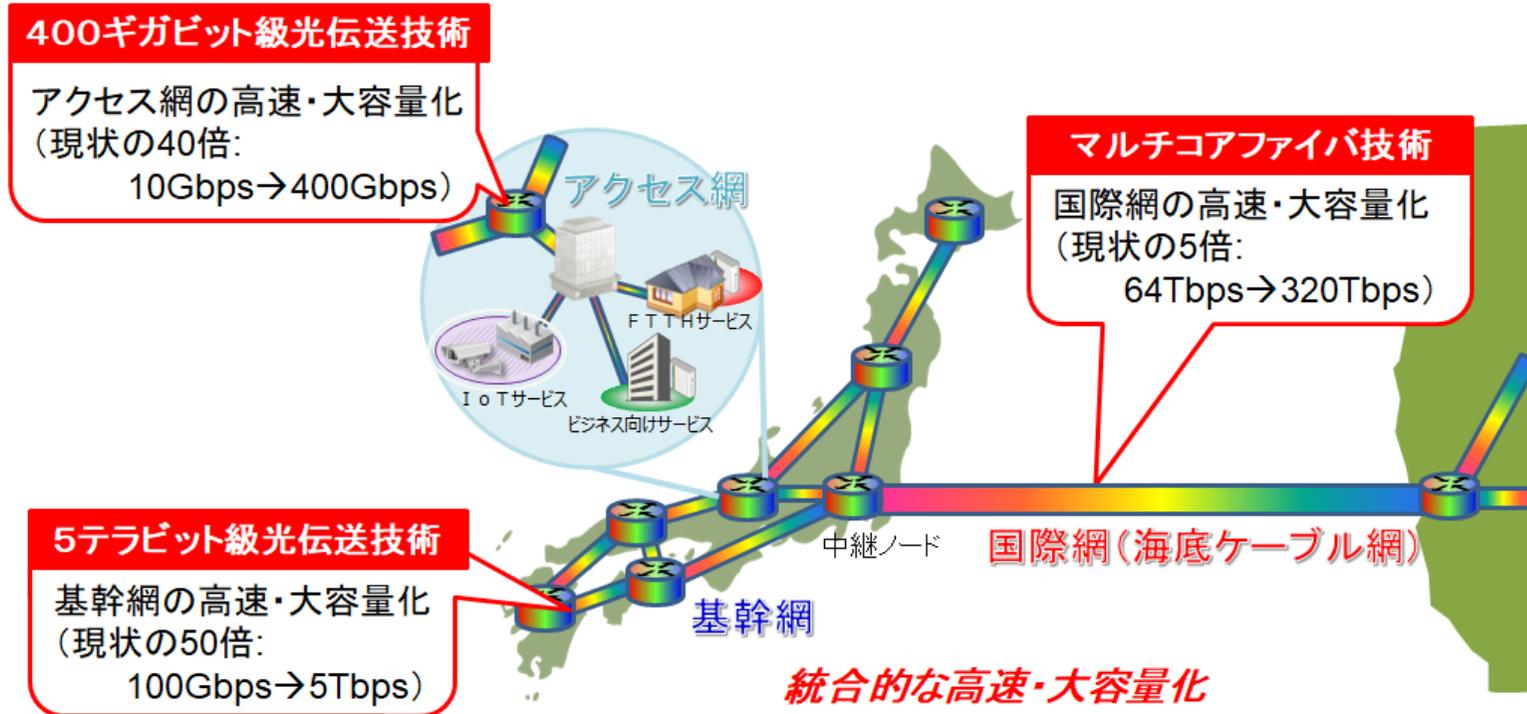
テストベッド等共用施設・設備を整備

# 1. Beyond 5Gをはじめとした先端技術への戦略的投資

## ③新たな社会インフラを担う革新的光ネットワーク技術の研究開発

- ・ Society5.0の実現に伴い光ネットワークに要求される通信容量の拡大、消費電力の削減を行うため、毎秒5テラビット級光伝送用信号処理技術等による革新的な光通信技術を確認し、IoT時代の新たな社会インフラを担う超高速・高信頼なネットワークの実現に寄与するとともに、我が国の国際競争力の強化に貢献する研究開発を実施

③令和3年度概算要求・要望額：8.5億円（令和2年度予算額：9.5億円）



# 1. Beyond 5Gをはじめとした先端技術への戦略的投資

## ④仮想空間における電波模擬システム技術の高度化

- ・今後新たに利用が想定される無線システムについて、実試験での検討に要する期間や費用の圧縮や、実環境では困難な大規模・複雑な検証を行うために、多様な無線システムを大規模かつ高精度で模擬可能な電波模擬システムの実現に向けた研究開発等を実施。

④令和3年度概算要求・要望額：40.0億円（令和2年度予算額：30.1億円）

- ・減衰・反射・回折などの電波伝搬を高精度に模擬
- ・既存無線システムとの干渉影響をリアルタイムに評価・判定



# 1. Beyond 5Gをはじめとした先端技術への戦略的投資

## ⑤5G高度化等に向けた総合的・戦略的な国際標準化・知財活動の促進

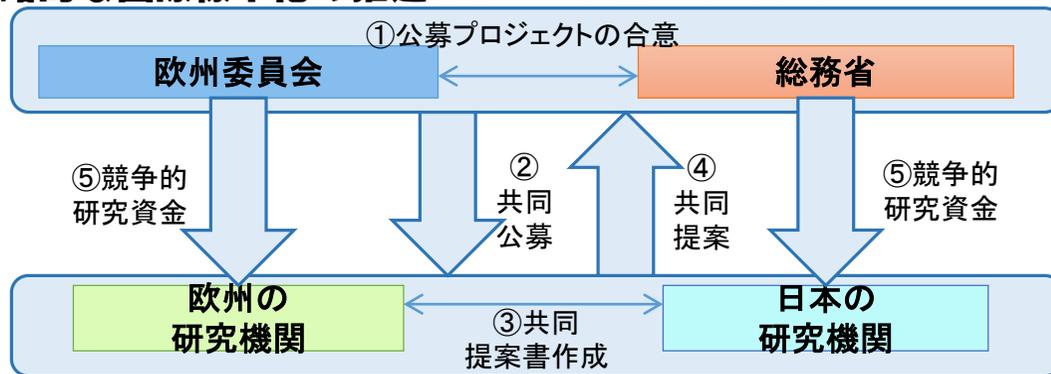
## ⑥戦略的情報通信研究開発推進事業（SCOPE）

- ICT分野における研究開発成果の国際標準化や実用化を加速し、イノベーションの創出や国際競争力の強化に資するため、外国の研究機関との国際共同研究開発を戦略的に実施するとともに、5Gの高度化等の推進に向けた国際標準化拠点等としての機能・体制を整備・活用することで、戦略的な国際標準化・知財活動を促進する。

⑤令和3年度概算要求・要望額：6.2億円（新規）

⑥令和3年度概算要求・要望額：10.0億円の内数（令和2年度予算額：12.2億円の内数）

### 戦略的な国際標準化の推進（例：日EU国際共同研究）



### 外国機関との国際共同研究のテーマ例

- ・5G（無線、ネットワーク、アプリ）
- ・ICTロボット
- ・光ネットワーク
- ・スマートシティ
- ・IoT社会インフラ
- ・eHealth 等

### これまでの成果

#### 研究成果

国際標準獲得 (H25-R1)	24件
論文 (H25-R1)	290本以上

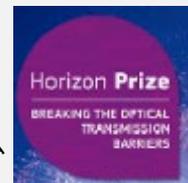
#### プライズ獲得

**SAFARI**  
(2014-2017 光通信領域)  
「再構成可能なインフラのための  
スケラブル・フレキシブル  
光通信」

#### Horizon Prize

<受賞概要>

- ・光伝送技術
- ・PHOTONMAPチーム
- ・賞金50万ユーロ



#### 成果の事業化



(2017-2019 ICTロボット)

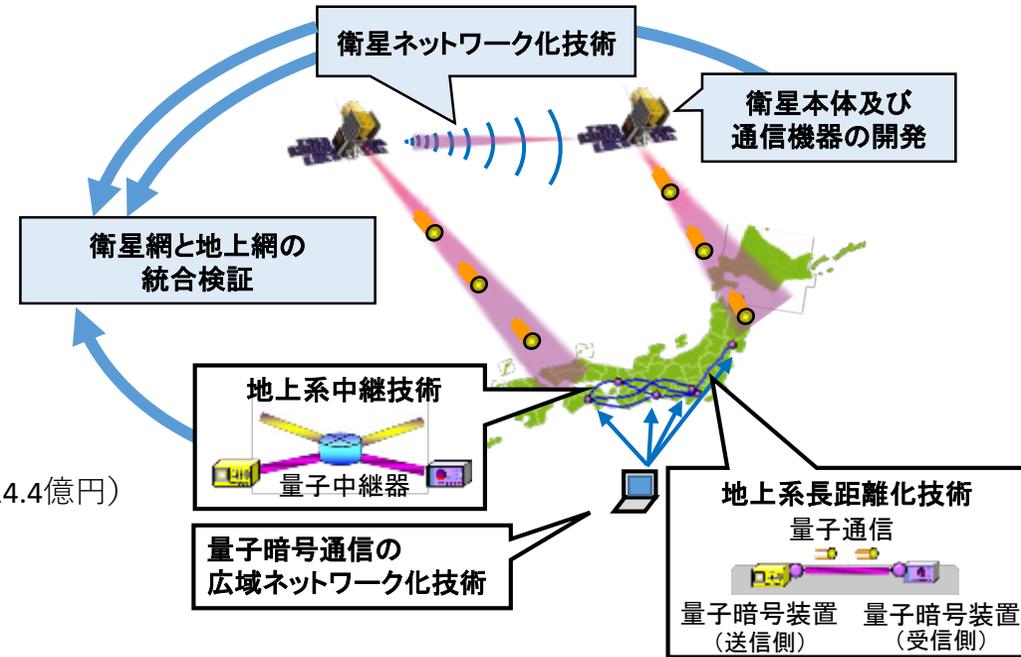
「高齢者支援に資する  
文化知覚ロボット環境システムの研究開発」

## 2. 量子暗号通信の実現

- ①グローバル量子暗号通信網構築のための研究開発
- ②グローバル量子暗号通信網構築のための衛星量子暗号通信の研究開発

・現代暗号の安全性の破綻が懸念されている量子コンピュータ時代において、国家間や国内重要機関間の機密情報のやりとりを安全に実行可能とするため、グローバル規模での量子暗号通信網の実現に向けた研究開発の実施。

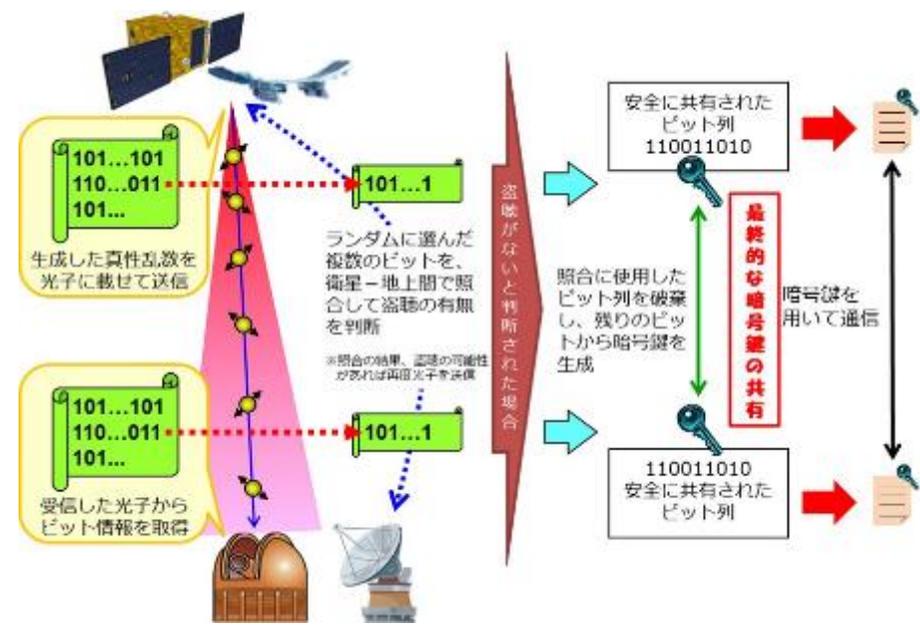
- ①令和3年度概算要求・要望額：14.5億円（令和2年度予算額：14.4億円）
- ②令和3年度概算要求・要望額：15.0億円（新規）



- ③衛星通信における量子暗号技術の研究開発

・世界的な人工衛星等の産業利用に向けた活動の活発化による衛星利用の需要拡大に対応するため、また、衛星通信に対する脅威となりつつあるサイバー攻撃を防ぎ、安全な衛星通信ネットワークの構築を可能とするため、高秘匿な衛星通信に資する技術の研究開発を実施するとともに、国際標準の獲得等による我が国の国際競争力の向上を実施。

- ③令和3年度概算要求・要望額：5.0億円（令和2年度予算額：3.4億円）



### 3. AIによる多言語翻訳技術の高度化

#### ○多言語翻訳技術の高度化に関する研究開発

- ・総務省では、世界の「言葉の壁」を解消し、グローバルで自由な交流を実現するため、「グローバルコミュニケーション計画2025」を推進し、2025年大阪・関西万博を見据え、AIにより会話の文脈や話者の意図を補完した実用レベルの「同時通訳」を実現するための研究開発を実施。

令和3年度概算要求・要望額：14.0億円（令和2年度予算額：14.0億円）

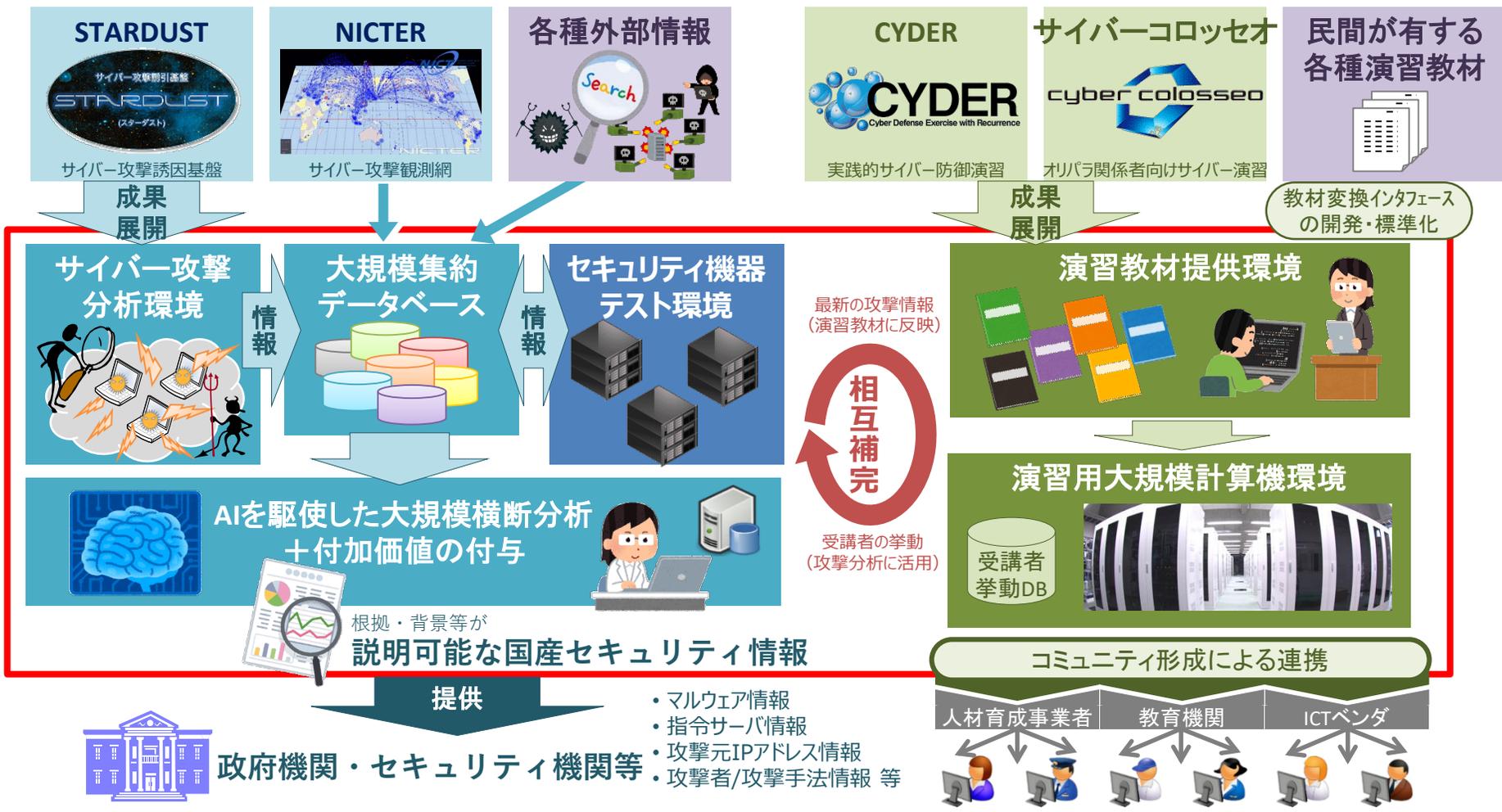


# 4. デジタル化の進展に合わせたサイバーセキュリティの確保

## ○サイバーセキュリティ統合知的・人材育成基盤の構築

・サイバーセキュリティ情報を国内で収集・蓄積・分析・提供するとともに、社会全体でサイバーセキュリティ人材を育成するための共通基盤を国立研究開発法人情報通信研究機構（NICT）に構築し、産学の結節点として開放することで、我が国全体のサイバーセキュリティ対応能力を強化。

令和3年度概算要求・要望額：20.0億円（新規）



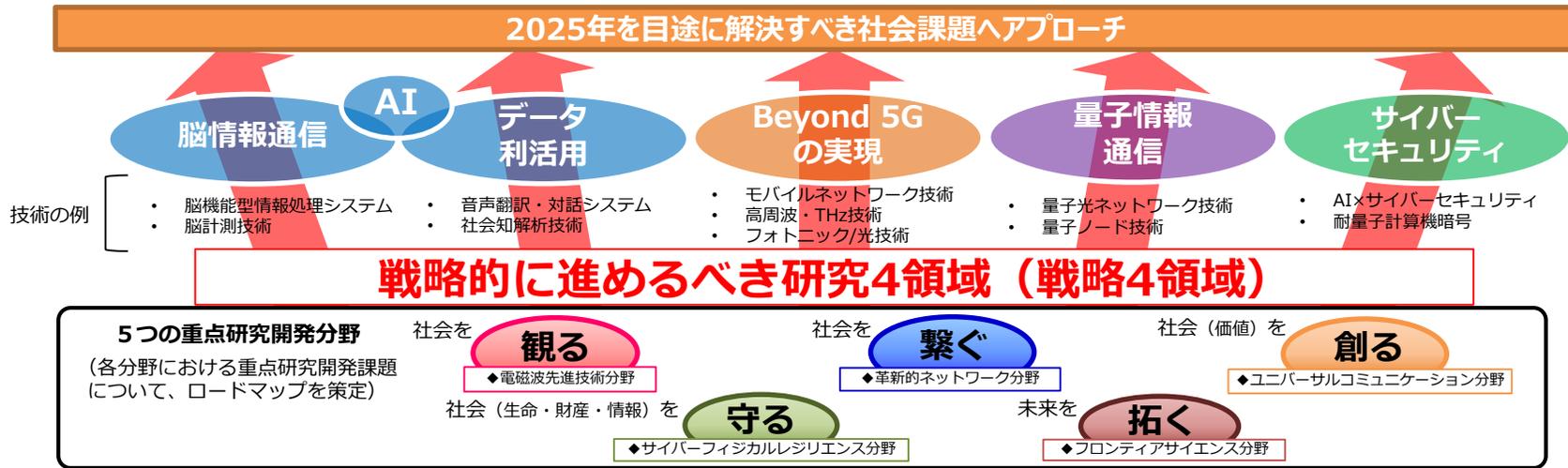
# 参考資料

# Beyond 5G時代における新たなICT技術戦略（概要）

■ Society5.0の実現やグローバル展開に向けたICT技術戦略を推進するため、次期科学技術基本計画（R3年度～）や国立研究開発法人情報通信研究機構（NICT）次期中長期計画（R3年度～）等を見据え、ICT分野で我が国が重点的に取り組む研究開発や推進方策等の戦略をとりまとめ

## 重点戦略・・・どの研究開発分野・課題にfocusするか

- ▶ Beyond 5G 推進戦略等の政府戦略やSociety5.0の早期実現に向けた次世代のICT基盤に必要な先端技術等の観点から、**戦略的に推進すべき研究領域を特定**
- ▶ 近年の社会情勢・ニーズ・技術動向等を踏まえ、**国が主導して推進すべき重点研究開発課題を特定**（51件（うち戦略4領域の対象30件））
- ▶ 宇宙基本計画など政府の重要政策に鑑み、宇宙分野等の我が国の経済成長や産業基盤の強化に資する取組を推進



## 推進戦略・・・研究開発をどのような体制で推進し、成果をどう社会にdeployするか

### 研究開発環境の整備

- ▶ 戦略4領域において国際ハブ化等の役割を担う**研究拠点化**を推進
- ▶ B5G時代における研究開発環境として**次世代テストベッドの構築**
- ▶ 電波の開放等（テラヘルツ波等）の政策と連携した研究開発の推進
- ▶ 上記の取組を活用した産学連携による**B5G研究開発プラットフォーム**の構築 等

### 研究開発スキームの強化

- ▶ **NICT/企業間の連携ラボ**等新たなスキームの導入
- ▶ 研究開発プロジェクト戦略策定等に資する**技術動向等の調査・分析機能の新設**
- ▶ シーズ創出につながる基礎・基盤的な創発研究から、スタートアップ等の社会実装に至る**総合研究開発プログラムの創設**
- ▶ **NICT発ベンチャー創出・育成**に向けた支援体制強化
- ▶ 研究開発支援やプロジェクト運用改善について検討 等

## 標準化戦略・・・戦略的ツールとして標準化活動を強化

### 標準化の推進

- ▶ 知財を含め標準化を戦略的に推進する拠点機能（**Beyond 5G知財・標準化戦略センター(仮称)**）の整備、標準化・知財動向の調査・分析機能の強化
- ▶ 研究開発段階から戦略的パートナーとの標準化活動を推進する**国際共同研究の強化**
- ▶ **OSS開発・実装試験環境としてのテストベッドの活用、オープンインターフェース化**を推進する異ベンダー機器間の**相互接続試験環境の整備**
- ▶ 若手、ユーザ企業、知財の専門家等を含む**チームによる標準化活動の支援**

### 人材育成等

- ▶ 魅力ある研究環境の提供等による**中長期的な研究開発を担う人材の確保**
- ▶ 組織を越えた人材交流の推進等**流動性/ダイバーシティの確保を通じた人材育成** 等

- ▶ 実績のある人材の活用、活動機会やインセンティブの拡大による若手育成等**標準化人材の確保・育成** 等

# Beyond 5G 推進戦略の全体像

- **Beyond 5G推進戦略**は、
  - ①2030年代に期待されるInclusive、Sustainable、Dependableな社会を目指した**Society 5.0実現のための取組**。
  - ②Society 5.0からバックキャストして行う**コロナに対する緊急対応策**かつ**コロナ後の成長戦略を見据えた対応策**。
- 本戦略に基づく**先行的取組**については、大阪・関西万博が開催される**2025年をマイルストーンとして世界に示す**。

## 基本方針

### グローバル・ファースト

- **国内市場をグローバル市場の一部と捉える**とともに、**我が国に世界から人材等が集まるようにする**といった双方向性も目指す。

### イノベーションを生むITシステムの構築

- **多様なプレイヤーによる自由でオープンな取組**を積極的に促す制度設計が基本。

### リソースの集中的投入

- 我が国のプレイヤーが**グローバルな協働に効果的に参画**できるようになるために必要性の高い施策へ一定期間集中的にリソースを投入。

政府と民間が一丸となって、国際連携の下で戦略的に取り組む

### 研究開発戦略

先端技術への集中投資と、大胆な電波開放等による

**世界最高レベルの研究開発環境の実現**

2025年頃から順次要素技術を確立

### 知財・標準化戦略

戦略的オープン化・デファクト化の促進と、海外の戦略的パートナーとの連携等による  
**ゲームチェンジの実現**  
〔サプライチェーンリスクの低減と市場参入機会の創出〕

Beyond 5G必須特許シェア10%以上

### 展開戦略

5G・光ファイバ網の社会全体への展開と、5Gソリューションの実証を通じた産業・公的利用の促進等による

**Beyond 5G readyな環境の実現**

2030年度に44兆円の付加価値創出

**Beyond 5Gの早期かつ円滑な導入**

**Beyond 5Gにおける国際競争力強化**

インフラ市場シェア3割程度  
デバイス・ソリューション市場でも持続的プレゼンス

**産学官の連携により強力かつ積極的に推進**

## Beyond 5G推進コンソーシアム

- ①各戦略に基づき実施される具体的な取組の共有、②国内外の企業・大学等による実証プロジェクトの立ち上げ支援、③国際会議の開催

- **第5期科学技術基本計画**の下、科学技術イノベーションを創出するため、新型コロナウイルス感染症への対応も踏まえた、今後において重点的に取り組むべき施策をとりまとめ、策定。
- 総務省の関連では、**Beyond 5G、AI、量子技術及び衛星等のICT分野の研究開発**のほか、**新型コロナウイルス感染症の対応（第Ⅱ部）**では殺菌用深紫外LED、情報通信ネットワークの整備等に関する記述も盛り込まれている。

（現況と経緯）

- 新型コロナウイルス感染症や世界各地での大規模災害等の前例のない非連続な変化により、我が国のデジタル化の遅れ、スピード感や危機感の不足が露呈
- **国家間の覇権争いの中核が進行技術によるイノベーションに大きくシフト**する中で、我が国の科学技術・イノベーションの工場が喫緊の課題
- 人文・社会科学の知も融合した**総合知により真の「Society 5.0」を実現**するための戦略的な科学技術・イノベーション政策が必要

デジタル化の加速・イノベーションの創出・研究力の強化 が必要



## 具体的に取り組むべき施策の柱（Society5.0の具体化）

- i) 新型コロナウイルス感染症への対応と持続的かつ強靱な社会・経済構造の構築
- ii) イノベーションの創出（Beyond 5G等）
- iii) 研究力の強化
- iv) 主要分野の戦略的な取組（AI, 量子技術等の基盤技術、拠点の整備等）

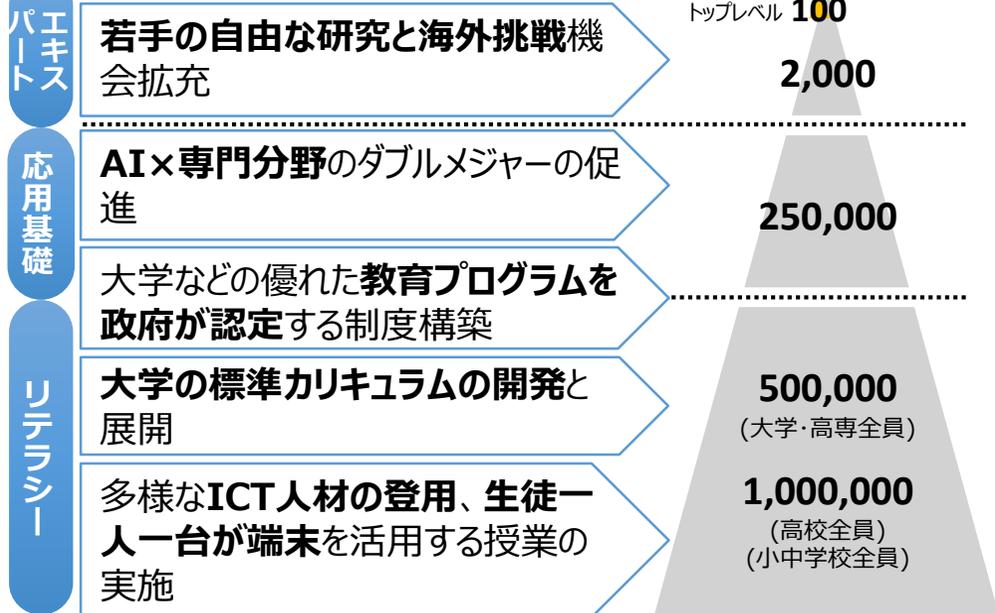
- Society 5.0は、科学技術イノベーションの活用を通じて人間中心の社会を実現する壮大な構想。  
**AIはその鍵となる基盤技術**
  - 「人間中心のAI社会原則」\*に基づき、実現すべき未来のビジョンを共有した上で、**AIの社会実装を推進するための戦略を策定**
- \*統合イノベーション戦略推進会議決定（平成31年3月）

## 人材育成

- ◆ 持続可能な社会の柱の1つとして、優先して議論

主な取り組み

2025年目標（人 / 年）



## 研究開発

- ◆ AI 研究開発ネットワークの構築
- ◆ AI 中核研究プログラムの立ち上げ



AIの基盤的・融合的な中核研究プログラムの立ち上げ

基礎理論

コンピューティング・デバイス

高品質かつ信頼できる AI

AIのシステムコンポーネント

## 社会実装

### ◆重点5分野におけるA Iの社会実装で世界をリード

健康・医療



農業



国土強靱化



交通インフラ・物流



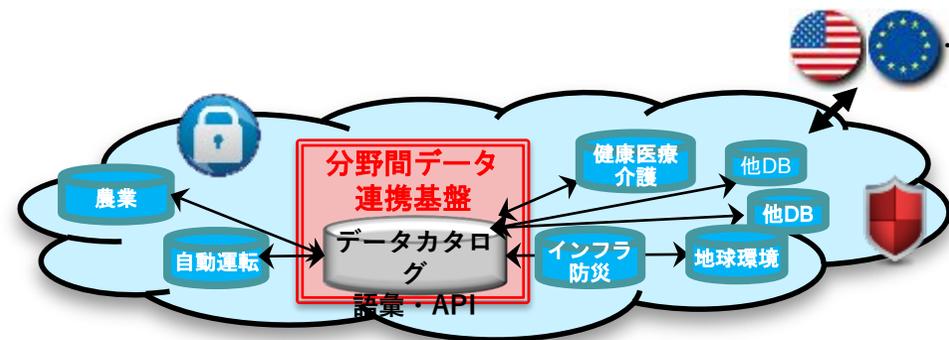
地方創生(スマートシティ)



## データ・トラスト・セキュリティ

### ◆次世代のA Iデータ関連インフラの構築と国際連携

- 重点5分野におけるデータ連携基盤の本格稼働
- 欧米等と相互認証可能なトラストデータ連携基盤の構築
- A I活用によるサイバー攻撃対策技術の確立



トラスト（信頼性）の課題：過去のデータで不適切な判断



# AI戦略2019 フォローアップ

統合イノベーション戦略推進会議（第7回）（R2.6.26）資料を一部変更

- ✓ 昨年6月に策定した「AI戦略2019」の実施初年度として、各府省庁等が関連する取組を鋭意実施。
- ✓ 取組の8割強は、計画通りに進捗。
- ✓ 新型コロナウイルス感染症拡大に直面し、よりデジタル社会の深化が不可欠。  
→AIの研究開発・社会実装、それらを支える情報通信環境の整備等の強化・充実が必要。

（参考）2019年度内を期限とした取組の進捗状況

	取組数	計画通り	未了/ 一部未了	進捗率
教育改革	31	27	4	87%
研究開発	16	11	5	69%
社会実装	26	24	2	92%
データ関連基盤	9	8	1	89%
デジガバ・中小	3	3	0	100%
倫理・その他	4	4	0	100%
Total	89	77	12	87%

## 2019年度の進捗（進捗のあった主な取組）

- G I G Aスクール構想の前倒し実施、数理・データサイエンス・A I 教育プログラム認定制度（リテラシーレベル）検討
- 「人工知能研究開発ネットワーク」を設立、3月末時点で104の機関が参画
- 医療画像診断支援やスマート農業、インフラデータプラットフォーム構築
- スマートシティ共通アーキテクチャ構築
- G20 AI原則や各省庁のAIガイドラインの策定

**進捗遅れの挽回、新たな課題や新型コロナウイルス感染症拡大への対応、等**

## 2020年度に実施する主な取組

- G I G Aスクール構想の加速、認定制度（応用基礎）の検討、社会人リカレント教育の拡充
- AIの信頼性確保や、人文・社会科学と数理・情報科学との融合に関する研究開発
- ものづくり現場の暗黙知（経験や勘）の伝承・効率的活用を支え、生産性を向上させるAI技術の開発
- 5Gや光ファイバ等のAI利活用に向けたネットワーク基盤の高度化、計算資源の増強
- 自治体でのAIサービスの標準化、自治体行政へのAI・RPA※1の実装
- 責任あるAIやイノベーション等の推進に向け、GPAI※2等における国際連携の強化

※1 RPA : Robotic Process Automation、 ※2 GPAI : Global Partnership on AI

- 量子技術は、将来の経済・社会に変革をもたらす、また、安全保障の観点からも重要な基盤技術であり、米欧中では、本分野の研究開発を戦略的かつ積極的に展開
- 我が国においても「量子技術イノベーション」を明確に位置づけ、日本の強みを活かし、重点的な研究開発や産業化・事業化を促進。量子コンピュータのソフトウェア開発や量子暗号などで、世界トップを目指す

## ＜量子技術イノベーション創出に向けた重点推進項目＞

### I 重点領域の設定

- ✓ 世界に先駆けて「量子技術イノベーションを実現」



- ✓ 「主要技術領域」、「量子融合イノベーション領域」を設定し、ロードマップを策定

例：量子コンピュータ、量子通信・暗号、量子AI、量子セキュリティ

- ✓ 研究開発支援を大幅に強化し、企業等からの投資を呼び込み

### II 量子拠点の形成

- ✓ 国内外から人や投資を呼び込む「顔の見える」拠点が不可欠



- ✓ 「量子技術イノベーション拠点(国際ハブ)」を形成（5拠点以上）

例：量子ソフトウェア拠点、量子慣性センサ拠点、量子セキュリティ拠点

- ✓ 基礎研究から技術実証、人材育成まで一貫通貫で実施

### III 国際協力の推進

- ✓ 産業・安全保障の観点から、欧米との国際連携が極めて重要



- ✓ 量子技術に関する多国間・二国間の協力枠組みを早期に整備

令和元年12月に日米欧3極による政府間シンポジウムを日本で初開催

- ✓ 特定の国を念頭に安全保障貿易管理を徹底・強化

上記の取組を含め、量子技術イノベーションの実現に向けて、5つの戦略を提示

技術開発戦略

国際戦略

産業・イノベーション戦略

知財・国際標準化戦略

人材戦略

中長期的

戦略期間(2018~2021年(3年間))

## 1 策定の趣旨・背景

1. サイバー空間がもたらすパラダイムシフト(サイバー空間では、創意工夫で活動を飛躍的に拡張できる。人類がこれまでに経験したことのないSociety5.0へのパラダイムシフト)
2. 2015年以降の状況変化(サイバー空間と実空間の一体化の進展に伴う脅威の深刻化、2020年東京大会等を見据えた新たな戦略の必要性)

## 2 サイバー空間に係る認識

1. サイバー空間がもたらす恩恵
    - 人工知能(AI)、IoT<sup>※</sup>などサイバー空間における知見や技術、サービスが社会に定着し、既存構造を覆すイノベーションを牽引。**様々な分野で当然に利用**され、人々に豊かさをもたらしている。
  2. サイバー空間における脅威の深刻化
    - 技術等を**制御できなくなるおそれは常に内在**。IoT、重要インフラ、サプライチェーンを狙った攻撃等により、国家の関与が疑われる事案も含め、多大な経済的・社会的な損失が生ずる可能性は拡大
- ※: Internet of Thingsの略

## 3 本戦略の目的

1. **基本的な立場の堅持**
  - 基本法の目的(2) 基本的な理念(「自由、公正かつ安全なサイバー空間」)
  - 基本原則(情報の自由な流通の確保、法の支配、開放性、自律性、多様な主体の連携)
2. 目指すサイバーセキュリティの基本的な在り方
  - 目指す姿(**持続的発展のためのサイバーセキュリティ(「サイバーセキュリティエコシステム」)の推進**)
  - 主な観点(①サービス提供者の**任務保証**、②**リスクマネジメント**、③**参加・連携・協働**)

## 4 目的達成のための施策

経済社会の活力の向上及び持続的発展	国民が安全で安心して暮らせる社会の実現	国際社会の平和・安定及び我が国の安全保障への寄与
<ol style="list-style-type: none"> <li>新たな価値創出を支えるサイバーセキュリティの推進               <ul style="list-style-type: none"> <li>＜施策例＞ <b>経営層の意識改革の促進(「費用」から「投資」へ)</b></li> <li>投資に向けたインセンティブ創出(情報発信・開示による市場の評価、保険の活用)</li> <li>セキュリティ・バイ・デザインに基づくサイバーセキュリティビジネスの強化</li> </ul> </li> <li>多様なつながりから価値を生み出すサプライチェーンの実現               <ul style="list-style-type: none"> <li>＜施策例＞ <b>中小企業を含めたサプライチェーン(機器・データ・サービス等の供給網)におけるサイバーセキュリティ対策指針の策定</b></li> </ul> </li> <li>安全なIoTシステムの構築               <ul style="list-style-type: none"> <li>＜施策例＞ IoTシステムにおけるセキュリティの体系の整備と国際標準化</li> <li><b>IoT機器の脆弱性対策モデルの構築・国際発信</b></li> </ul> </li> </ol>	<ol style="list-style-type: none"> <li>国民・社会を守るための取組               <ul style="list-style-type: none"> <li>＜施策例＞ 脅威に対する事前の防御(<b>積極的サイバー防御</b>)策の構築</li> <li>サイバー犯罪への対策</li> </ul> </li> <li>官民一体となった重要インフラの防護               <ul style="list-style-type: none"> <li>＜施策例＞ 安全基準等の改善・浸透(サイバーセキュリティ対策の<b>関係法令等における保安規制としての位置付け</b>)</li> <li>地方公共団体のセキュリティ強化・充実</li> </ul> </li> <li>政府機関等におけるセキュリティ強化・充実               <ul style="list-style-type: none"> <li>＜施策例＞ <b>情報システムの状態のリアルタイム管理の強化</b></li> <li>先端技術の活用による先取り対応への挑戦</li> </ul> </li> <li>大学等における安全・安心な教育・研究環境の確保               <ul style="list-style-type: none"> <li>＜施策例＞ <b>大学等の多様性を踏まえた対策の推進</b></li> </ul> </li> <li>2020年東京大会とその後を見据えた取組               <ul style="list-style-type: none"> <li>＜施策例＞ <b>サイバーセキュリティ対処調整センターの構築の推進</b></li> <li>成果のレガシーとしての活用</li> </ul> </li> <li>従来の枠を超えた情報共有・連携体制の構築               <ul style="list-style-type: none"> <li>＜施策例＞ <b>多様な主体の情報共有・連携の推進</b></li> </ul> </li> <li>大規模サイバー攻撃事態等への対処態勢の強化               <ul style="list-style-type: none"> <li>＜施策例＞ <b>サイバー空間と実空間の双方の危機管理に臨むための大規模サイバー攻撃事態等への対処態勢の強化</b></li> </ul> </li> </ol>	<ol style="list-style-type: none"> <li>自由、公正かつ安全なサイバー空間の堅持               <ul style="list-style-type: none"> <li>＜施策例＞ <b>自由、公正かつ安全なサイバー空間の理念の発信</b></li> <li>サイバー空間における法の支配の推進</li> </ul> </li> <li>我が国の防御力・抑止力・状況把握力の強化               <ul style="list-style-type: none"> <li>＜施策例＞ <b>国家の強靱性の確保</b></li> <li>(①任務保証、②我が国の先端技術・防衛関連技術の防護、③サイバー空間を悪用したテロ組織の活動への対策)</li> <li>サイバー攻撃に対する<b>抑止力の向上</b></li> <li>(①実効的な抑止のための対応、②信頼醸成措置)</li> <li>サイバー空間の<b>状況把握の強化</b></li> <li>(①関係機関の能力向上、②脅威情報連携)</li> </ul> </li> <li>国際協力・連携               <ul style="list-style-type: none"> <li>＜施策例＞ <b>知見の共有・政策調整</b></li> <li>事故対応等に係る国際連携の強化</li> <li>能力構築支援</li> </ul> </li> </ol>

### 横断的施策

- 人材育成・確保** <施策例> **戦略マネジメント層の育成・定着**、実務者層・技術者層の育成(高度人材含む)、人材育成基盤の整備、**政府人材**の確保・育成の強化、国際連携の推進
- 研究開発の推進** <施策例> 実践的な研究開発の推進(**検知・防御等の能力向上**、**不正プログラム等の技術的検証**を行うための体制整備)、**AI等**中長期的な技術・社会の進化を視野に入れた対応
- 全員参加による協働** <施策例> サイバーセキュリティの普及啓発に向けた**アクションプランの策定**、**国民への情報発信**(サイバーセキュリティ月間の充実等)、サイバーセキュリティ教育の推進

## 5 推進体制

本戦略の実現に向け、サイバーセキュリティ戦略本部の下、**内閣サイバーセキュリティセンターを中心に関係機関の一層の能力強化**を図るとともに、同センターが、各府省庁間の総合調整、産学官民連携の促進の要となる主導的役割を担う。**施策が着実かつ効果的に実施されるよう必要な予算の確保と執行を図る。** 等

# IoT・5Gセキュリティ総合対策2020の概要

- サイバーセキュリティタスクフォースにおけるこれまでの短期的・中長期的な観点の議論、「我が国のサイバーセキュリティ強化に向け速やかに取り組むべき事項 [緊急提言]」※<sup>1</sup>の内容、さらには新型コロナウイルス感染症への対応等を踏まえつつ、「IoT・5Gセキュリティ総合対策」※<sup>2</sup>について、必要な改定を行い、「IoT・5Gセキュリティ総合対策2020」として2020年7月に公表。

## ● 改定に当たっての主要な政策課題

### 1 COVID-19 への対応を受けたセキュリティ対策の推進

- テレワークシステムのセキュリティに関するチェックリストの作成や相談対応体制の拡充など、特に中小企業を念頭においたテレワークセキュリティの確保のための実践的な対策を推進する。
- ネット上で業務・手続を完結可能とするため、電子署名やeシールなどのトラストサービスの制度化や普及促進を図るとともに、制度・手続・慣習の見直しを進める。

### 2 5G の本格開始に伴うセキュリティ対策の強化

- 5Gネットワークの脆弱性及び脅威の検証・分析のための手法や体制の確立
- 関係者間のリスク・脅威情報の共有の促進
- 規制・振興両面でのセキュリティ対策の実装の促進など

セキュリティ・  
バイ・デザインの  
観点で推進

### 3 サイバー攻撃に対する電気通信事業者のアクティブな対策の実現

巧妙化・多様化するサイバー攻撃に対処するため、電気通信事業者における積極的なサイバーセキュリティ対策（C&Cサーバの能動的な検知や攻撃指令通信の遮断等）を迅速かつ効果的に実施可能とするため、通信の秘密の保護を図りつつ、一層のサイバーセキュリティを確保する方策について検討を行う。

### 4 我が国のサイバーセキュリティ情報の収集・分析能力の向上に向けた産学官連携の加速

我が国におけるセキュリティ製品・サービスの海外依存や慢性的な人材不足から脱却するため、サイバーセキュリティ情報を国内で収集・蓄積（生成）・提供するとともに、社会全体でサイバーセキュリティ人材を育成するための共通基盤を構築し、産学官連携の結節点とするための体制の構築を図る。

## ● IoT・5Gセキュリティ総合対策2020の枠組み

### 重点的に対応すべき情報通信サービス・ネットワークの個別分野等に関する具体的施策

- ✓ IoT、5G、クラウドサービス、スマートシティ、テレワークシステムのセキュリティ
- ✓ トラストサービスの制度化と普及促進 など

具体的施策間  
でも連携

連携

連携

連携

#### 研究開発

- ✓ 統合知的基盤
- ✓ ハードウェア脆弱性
- ✓ AI
- ✓ 暗号

など

#### 人材育成 普及啓発

- ✓ 人材育成基盤
- ✓ サイバー演習
- ✓ 地域の人材育成

など

#### 情報共有 情報開示

- ✓ 情報共有基盤
- ✓ 情報開示の促進

など

連携

### 国際連携

- ✓ ASEAN各国や欧米諸国等との連携
- ✓ 国際標準化

など

※<sup>1</sup> 2020年東京大会に向けた対処として短期的な観点から早急に取り組むべき事項を整理した結果を「我が国のサイバーセキュリティ強化に向け速やかに取り組むべき事項 [緊急提言]」として2020年1月に公表。

※<sup>2</sup> IoT・5G時代にふさわしいサイバーセキュリティ政策の在り方について検討した結果を「IoT・5Gセキュリティ総合対策」として2019年8月に公表。