資料３

国立研究開発法人情報通信研究機構第６期中長期目標・中長期計画（案）　対比表

※サイバーセキュリティ関係のみ抜粋

第６期中長期目標 （令和８年２月２７日総務大臣指示）	第６期中長期計画（案） （令和８年３月２日認可申請）
Ⅰ．政策体系における法人の位置付け及び役割（ミッション） ［略］	
Ⅱ．中長期目標の期間 ［略］	
Ⅲ．研究開発の成果の最大化その他の業務の質の向上に関する事項 NICT は、中長期目標期間において、研究開発の成果の最大化その他の業務の質の向上のため、以下の取組を実施するものとする。 なお、１．～３．の取組に係る中長期計画及び年度計画の策定・変更に際しては、国の政策と連携し、Ⅰ.で示した政策体系における法人の位置付け及び役割（ミッション）を十分に踏まえて、検討するものとする。 また、評価に当たっては、２.（１）～（５）の各研究開発分野、３．①～⑥の各研究課題、４．を一定の事業のまとまりと捉え、各研究開発・取組の内容、段階等に応じて、別紙３から適切な評価軸及び指標を用いて実施する。また、１．については、これらの取組が我が国の重要政策の実現等にどのように貢献しているかという観点から、別紙３に基づき総合的な評価を実施する。	**Ⅰ　研究開発成果の最大化その他の業務の質の向上に関する目標を達成するためとるべき措置**
１．戦略的に推進すべき技術領域 我が国の重要政策の実現に不可欠な技術であり、産学官一体となり、横断的かつ戦略的な取組を強力に推進すべきものを「戦略領域」と位置付け、これら戦略領域において、NICTが民間投資や人材育成を活性化するための触媒となるべく、中長期的なビジョンを構想し、産学官で共有しながら、研究開発から社会実装までを連携して取り組んでいく産学官連携の中核・結節点としての役割を果たすものとする。	**１．戦略的に推進すべき技術領域** 我が国の重要政策の実現に不可欠な技術領域において、「２．重点的に推進すべき基礎的・基盤的研究開発等」、「３．イノベーションの基盤となる研究開発課題」及び「４．社会実装機能・外部連携機能等」の取組を通じて、中長期的なビジョンの下で研究開発から社会実装までを連携して取り組んでいく産学官連携の中核・結節点としての役割を果たすとともに、政府と密接に連携し、我が国の重要政策の実現に向けた取組を強力に推進する。
（１）AI・コミュニケーション ［略］	**１－１．AI・コミュニケーション** ［略］
（２）Beyond 5G ［略］	**１－２．Beyond 5G** ［略］
（３）量子情報通信 ［略］	**１－３．量子情報通信** ［略］

（４）サイバーセキュリティ 　デジタル化の進展により、国民生活・経済活動のデジタルサービスへの依存が一層高まっていく一方、質・量の両面でサイバー攻撃の脅威が増大し、国民生活や経済活動の基盤、ひいては国家及び国民の安全に深刻・致命的な被害を生じさせるおそれが現実のものとなっている。また、AI、量子技術等の新たな技術革新が続々と進む中、これらがサイバーセキュリティ分野にもたらす利便を最大限享受しつつ、それらのリスクに的確に対応することは喫緊の課題である。 　こうした昨今の情勢認識を踏まえ、NICTは、信頼できる公的機関として一次脅威情報を収集・分析・蓄積し、産学官との連携により演習等を通じたサイバー人材の育成や国産を核とした新技術・サービスの創出等の取組を進めていく必要がある。また、AIとサイバーセキュリティの融合のための研究開発を推進し、成果展開にも積極的に取り組むべきである。加えて、我が国の安全保障の観点から長期的・継続的に維持することが求められる暗号研究にも、継続的に取り組んでいくべきである。 　以上の認識の下、NICTは、サイバーセキュリティ研究開発の中核拠点として、我が国のサイバー対応能力を支える人材・技術に係るエコシステム形成に貢献するものとする。	**１－４．サイバーセキュリティ** 　機構が、サイバーセキュリティ研究開発の中核拠点として、我が国のサイバー対応能力を支える人材・技術に係るエコシステム形成に貢献するため、以下の事項を戦略的に推進する。 　機構がこれまで推進してきたサイバー攻撃に関する一次脅威情報の収集・分析・蓄積を持続・発展させるとともに、それら情報に基づくサイバーセキュリティの基礎研究力を強化する。特に、AIとサイバーセキュリティの融合研究を加速し、AIによるセキュリティの高度化と、AI自身のセキュリティ検証・評価の両面から研究開発を推進する。 　量子計算機時代における安心・安全な情報基盤構築を推進するため、耐量子計算機暗号を含む暗号・認証技術及びプライバシー保護技術の研究開発を行うとともに、耐量子計算機暗号等の今後普及が見込まれる暗号技術等の安全性評価を行う。 　サイバー人材の育成のための演習その他の訓練や、産学官との連携を通じた国産のセキュリティ技術・サービス創出等のための取組を推進するとともに、日本の電気通信設備のセキュリティ向上に必要な助言及び情報の提供等を行うなど、サイバーセキュリティ研究開発の中核拠点として積極的な成果展開を行い、我が国のサイバー対応能力を支える人材・技術に関わるエコシステム形成に貢献する。
２．重点的に推進すべき基礎的・基盤的研究開発等 　我が国社会を支える情報通信分野の基礎的・基盤的な技術であり、中長期的な視点に立って研究開発等に取り組むべきものを「重点分野」とし、ICTを専門とする我が国唯一の公的研究機関として蓄積された技術力や知見・経験等を最大限活用する観点から、「電磁波先進技術」「革新的ネットワーク」「サイバーセキュリティ」「ユニバーサルコミュニケーション」「フロンティアサイエンス」の５分野を位置付けるものとする。そして、これら重点分野の研究開発等を通じて、「災害に強く、強靭な社会インフラの構築」「安全で、信頼できる情報通信環境の整備」「GX・DXを支える持続可能なICT基盤の構築」「DXを通じた効率化・合理化、新たな価値の創造」に貢献すべく、【重要度：高】として取り組むものとする。 　また、貢献目標に資する技術として、特に重点的に取り組むべきものを「重点課題」とし、重点分野ごとに設定するものとする。	**２．重点的に推進すべき基礎的・基盤的研究開発等** 　ICT を専門とする我が国唯一の公的研究機関として、我が国社会を支える情報通信分野の基礎的・基盤的な技術に関し、中長期的な視点に立って研究開発等に取り組む。
（１）電磁波先進技術分野 ［略］	**２－１．電磁波先進技術分野** ［略］
（２）革新的ネットワーク分野 ［略］	**２－２．革新的ネットワーク分野** ［略］

（３）サイバーセキュリティ分野 サイバー攻撃への対策は国を挙げて取り組むべき安全保障上の課題にもなっており、NICTに対する社会的要請が高まりつつあるとの認識の下、サイバー空間における脅威から社会システムや国民を守るために高度化が不可欠である基礎的・基盤的なサイバーセキュリティ技術は、特に「安全で、信頼できる情報通信環境の整備」に資することが期待されることから、以下の技術を重点課題として研究開発に取り組むとともに、研究開発成果の普及や社会実装を目指すものとする。とりわけ、重要電子計算機に対する不正な行為による被害の防止に関する法律（令和７年法律第42号）第71条第２項に基づき、重要電子計算機に対する特定不正行為による被害の防止に関する事項について、サイバー攻撃の観測・分析等の観点から関係者との連絡・協力に努める。 また、我が国の政府機関等にCYXROSSセンサー等の安全性・透明性を検証可能なセンサーを導入し、得られたサイバー脅威情報等を集約・分析・情報提供する活動をはじめ、こうした活動が研究開発をさらに推進するようなサイクルを確立することで、サイバーセキュリティ分野全体の継続的な能力向上に努めるものとする。併せて、これらの研究開発及び社会実装に関する体制の強化に向けた措置を講ずるものとする。 さらに、サイバーセキュリティ基本法（平成26年法律第104号）第31条第1項第2号その他の法令に基づく委託を受けた場合には、それら委託業務を確実に実施するとともに、各重点課題との相乗効果を得られるよう一体的に取り組むものとする。 ① サイバーセキュリティ技術 人間の社会活動の基盤となるインターネット上の脅威に適切に対処するため、我が国独自のサイバー脅威インテリジェンス基盤技術の確立を目指す。そのために、多種多様なサイバー攻撃の観測・分析技術、様々な機関等から発信される脅威情報の大規模収集・分析技術及び脅威インテリジェンス生成技術等の研究開発を行うものとする。 また、新たな脅威に対処するため、Beyond 5G実現に向けたセキュリティ検証技術やローレイヤーのセキュリティ技術、人間に関するセキュリティを扱うユーザブルセキュリティや脳情報通信融合セキュリティといったヒューマン・センタード・サイバーセキュリティの研究開発を行うものとする。	**２－３．サイバーセキュリティ分野** サイバー攻撃への対策は国を挙げて取り組むべき安全保障上の課題にもなっており、機構に対する社会的要請が高まりつつあるとの認識の下、サイバー空間における脅威から社会システムや国民を守るために高度化が不可欠である基礎的・基盤的なサイバーセキュリティ技術として、以下の技術の研究開発に取り組むとともに、研究開発成果の普及や社会実装を目指す。特に、重要電子計算機に対する不正な行為による被害の防止に関する法律（令和７年法律第42号）第71条第２項に基づき、重要電子計算機に対する特定不正行為による被害の防止に関する事項について、サイバー攻撃の観測・分析等の観点から関係者との連絡・協力を積極的に行う。 また、我が国の政府機関等にCYXROSSセンサー等の安全性・透明性を検証可能なセンサーを導入し、得られたサイバー脅威情報等を集約・分析・情報提供するとともに、こうした活動が研究開発をさらに推進するようなサイクルを確立することで、サイバーセキュリティ分野全体の継続的な能力向上に努める。併せて、これらの研究開発及び社会実装に関する体制の強化に向けた措置を講ずる。 さらに、サイバーセキュリティ基本法（平成26年法律第104号）第31条第１項第２号その他の法令に基づく委託を受けた場合には、それら委託業務を確実に実施するとともに、各重点課題との相乗効果を得られるよう一体的に取り組む。 本分野は戦略的に推進すべき技術領域である「サイバーセキュリティ」に資する研究開発を牽引する役割を持つものとする。 **（１）サイバーセキュリティ技術** 社会・経済活動を支える情報通信基盤において高度化・多様化するサイバー脅威に適切に対応し、我が国の安全性の確保に資するため、脅威の実態把握を支える観測・分析・対策技術の研究開発を推進する。また、新たに社会に登場する技術に関するセキュリティ検証技術や、人間と情報技術の関係性から生じるセキュリティ・プライバシー上の脅威に対応するための基礎技術の研究開発を進める。 **（ア）サイバー脅威インテリジェンス基盤技術** 多種多様なサイバー攻撃を総合的に把握するため、無差別型攻撃や標的型攻撃を含む幅広い脅威に関する一次情報を、大規模かつ継続的に収集・蓄積するための基盤技術の研究開発を行う。また、多様な機関や情報源から発信される脅威情報を収集・整理し、攻撃観測データとの横断的な統合分析を通じて脅威動向を継続的に把握する技術の確立・高度化を進める。これらの取組により、独自の脅威インテリジェンス基盤を構築し、得られた技術や知見の社会実装を促進する。 **（イ）ヒューマン・センタード・サイバーセキュリティ技術** 人間がICTを利用する場面で生じるセキュリティ・プライバシー上の脅威に対応す

	るため、人間の行動特性や認知特性を踏まえたセキュリティ技術の研究開発を行う。具体的には、利用者が自然に安全な行動を取れる環境設計、人間の認知・行動に影響を及ぼす脅威の把握と対策など、心理学・認知科学・脳情報通信技術等と連携した研究開発を推進し、人を中心に据えた次世代のセキュリティを確立する。さらに、社会に新たに登場する技術に対するセキュリティ課題の抽出と対策に貢献するため、最新の通信機器、IoT機器、Beyond 5G等のエマージング技術に対応した脅威分析・セキュリティ検証技術を確立・高度化する。
② AI×サイバーセキュリティ技術 AI技術を活用し、セキュリティ対策に有用な情報をリアルタイムに導出する「AI for Security（AIを活用したサイバーセキュリティ確保）」技術の研究開発を行うものとする。また、AIモデルやAI搭載システムへの攻撃に対する安全性を検証・評価し、こうした安全性の観点を中心に信頼性の高いAI技術を構築する「Security for AI（AIに係る安全性確保）」技術の研究開発を行うものとする。さらに、当該研究分野の国際競争力強化のため、積極的に国際連携を推進する。	**（２）AI×サイバーセキュリティ技術** AIを活用してサイバー攻撃の検知・分析・対応を高度化し、システム全体の安全性を強化する「AI for Security（AIを活用したサイバーセキュリティ確保）」技術の研究開発を行う。また、AIモデルやAI搭載システムへの攻撃に対する安全性を検証・評価し、こうした安全性の観点を中心に信頼性の高いAI技術を構築する「Security for AI（AIに係る安全性確保）」技術の研究開発を行う。さらに、当該研究分野の国際競争力強化のため、積極的に国際連携を推進する。 **（ア）AI 駆動型サイバーセキュリティ技術の高度化** 高度化･多様化するサイバー攻撃や未知の脆弱性に対処するため､AI 技術を活用し、サイバー防御においても攻撃兆候の検知・分析の高度化やマルウェアの挙動解析・機能分析の効率化を図る。さらに、ソフトウェアに内在する脆弱性の早期発見等に AI を活用し、セキュリティ対応の高度化・自動化を可能とする技術の確立を目指す。 **（イ）AI 技術の安全性・信頼性向上** AI モデルに対する敵対的攻撃や悪用等のリスクに対応するため、安全性・信頼性を体系的に検証・評価する技術の研究開発を行う。また、AI 搭載システムに対して、AI の実装・運用に起因する誤動作や不正利用等の悪用リスクに着目し、その安全性について検証・評価を行う。 **（ウ）AI×サイバーセキュリティ技術に関するグローバル連携体制の構築** AI×サイバーセキュリティ分野における国際的な研究動向や脅威情報を迅速に把握し、研究成果の高度化及び国際競争力の強化を図るため、海外の研究機関、大学、国際プロジェクト等との連携を推進する。国際共同研究や人材交流を通じて国際的に通用する研究成果の創出を目指すとともに、国際的な標準化、ルール形成及び知識基盤への貢献を視野に入れた研究開発を推進する。
③ 次世代暗号・プライバシー保護技術 量子コンピュータ時代に安全に利用できる暗号基盤技術の確立を目指し、現代暗号に加え、耐量子計算機暗号を含む次世代暗号技術の研究開発及び安全な	**（３）次世代暗号・プライバシー保護技術** 情報インフラの発展にともない、情報のセキュリティやプライバシーの確保を推進するため、耐量子計算機暗号を含む暗号・認証技術、プライバシー保護技術の研究開

データ利活用を促進するプライバシー保護技術等の研究開発を行うものとする。また、安心・安全な国民生活に貢献するために、耐量子計算機暗号に係る安全性評価等を喫緊の課題とし、国内外の状況変化に柔軟に対応して着実に実施するとともに、我が国の電子政府推奨暗号リストの維持・管理を行うものとする。	発を行う。また、社会で普及している暗号技術、耐量子計算機暗号等の今後普及が見込まれる暗号技術及び暗号を利用するプロトコルの安全性評価を実施し、国民生活を支える情報インフラの堅牢化を推進する。 **（ア）安全なデータ利活用技術** データ利活用の恩恵を誰もが享受できるように、耐量子計算機暗号等の次世代暗号技術を軸に、データ利活用と安全性を両立させる暗号・認証技術やプライバシー保護技術に基づいたセキュリティ基盤技術の研究開発を行う。加えて、それらの応用技術について社会実装に向けた研究開発及び実証実験などを行うことを通じて、量子計算機時代における安心・安全な情報基盤構築を促進する。 **（イ）量子計算機時代に向けた暗号技術の安全性評価** 量子計算機時代に対応した安全な暗号技術基盤の確立を目指し、電子政府システム等で使用される暗号技術に加え、耐量子計算機暗号、軽量暗号、さらには世界的に広く利用される実システムの暗号プロトコルを対象とした安全性評価に関する研究開発を行う。併せて、電子政府推奨暗号リストを制定するCRYPTRECの暗号技術評価委員会事務局として、CRYPTREC暗号リスト掲載暗号の継続的な状況監視を行うとともに、将来的にリスト掲載候補となる暗号技術の安全性評価を行う。現代暗号については、従来型の計算機及び量子計算機を用いた安全性評価を行う。また、特に対応が急務となっている、格子暗号や多変数多項式暗号を含む耐量子計算機暗号の安全性評価を推進する。以上の研究開発・安全性評価に当たっては、世界最先端の評価技術を通じて、国内外の標準化動向を踏まえながら、各種暗号技術の妥当性及び安全性を検証することにより、安心・安全な暗号基盤の普及及び持続的な運用に貢献する。
④ サイバーセキュリティに関する演習 国の機関や地方公共団体、重要インフラ事業者等のサイバー攻撃対処能力の向上に貢献するため、サイバーセキュリティ戦略等の政府方針を踏まえ、NICT法第14条第1項第7号イの規定に基づき、最新のサイバー攻撃に関する知見や社会的ニーズを踏まえた実践的なサイバー演習を、高い受講効果が得られるよう開発・提供する。また、NICTにおけるサイバーセキュリティ研究や本演習を通じて得られた知見等を活用し、若手セキュリティ人材の育成を行うものとする。	**（4）サイバーセキュリティに関する演習** 国の機関や地方公共団体、基幹インフラ事業者等のサイバー攻撃への対処能力の向上に貢献するため、国からの補助等を受けた場合には、その予算の範囲内で、サイバーセキュリティ戦略等の政府の方針を踏まえ、機構法第14条第１項第７号イの規定に基づき、機構の有する技術的知見を活用して、最新のサイバー攻撃状況を踏まえた実践的なサイバーセキュリティ演習を実施する。演習の実施に当たっては、サイバーセキュリティ基本法第13条及び第14条の規定を踏まえ、全ての国の行政機関、独立行政法人及び指定法人並びに地方公共団体及び基幹インフラ事業者等の受講機会を確保するとともに、重要インフラ事業者及びその組織する団体についても、より多くの受講機会を確保できるよう配慮する。また、地理的条件により受講機会が失われることを最小限とするよう、集合演習を全国で実施するほか、オンライン演習を効果的に実施して、未受講となる組織・団体や基礎的な知識習得が必要な組織・団体に対して積極的な参加を促す。併せて、最新のサイバー攻撃情報を踏まえた演習内容の高度化、オンライン演習における学習定着率の向上等、演習効果の最大化に取り組む。さらに、

⑤ サイバーセキュリティ産学官連携の推進 我が国のサイバー攻撃対処能力とセキュリティ自給率の向上[1]に貢献するため、サイバーセキュリティ分野の産学官連携拠点において、国内外の組織との実効的な連携等を通じ、サイバー攻撃情報等の大規模な収集・分析・共有やサイバー攻撃観測技術・ノウハウ等の共有、国産セキュリティ製品の評価と開発元へのフィードバックによる製品・サービス開発の加速化等に取り組むものとする。 また、各産業分野の特性に応じたサイバー攻撃対処能力の構築に貢献するため、より高度な対処能力構築といった観点にも留意しつつ、NICTにおけるサイバーセキュリティ研究の知見等を活用し、演習基盤の開放により産学官における自律的な人材育成を支援するものとする。	機構におけるサイバーセキュリティ研究と演習業務で得られた知見等を活用し、若手セキュリティ人材の育成を行う。 **（５）サイバーセキュリティ産学官連携の推進** 我が国のサイバー攻撃対処能力とサイバーセキュリティ自給率の向上に貢献するため、サイバーセキュリティ分野の産学官連携拠点において、国内外の組織との実効的な連携等を通じ、サイバー攻撃情報等の大規模な収集・分析・共有やサイバー攻撃観測技術・ノウハウ等の共有、民間による国産セキュリティ製品・サービス開発を加速させるための製品・技術の検証評価、演習基盤の開放、産学官における人材育成の支援の取組を行う。 **（ア）サイバー攻撃情報等の大規模な収集・分析・共有** （１）の研究開発成果展開や独自の情報収集基盤による大規模なサイバー攻撃情報の収集を基礎に、国内の組織との連携による技術、情報共有を通じてサイバー攻撃の共同分析を行う。解析者コミュニティ活動などの連携活動による参画組織間の信頼関係の醸成を進め、情報流通を活性化する。 **（イ）サイバー攻撃観測技術・ノウハウ等の共有** 多種多様なサイバーセキュリティ関連情報を大規模集約した上で、横断的かつ多角的に分析し、実践的かつ説明可能な脅威情報を生成するとともに、収集した実データ及び生成された脅威情報を必要とする関係機関に継続的に提供する。この活動に参画組織の人材を受け入れ、サイバーセキュリティ関連情報を多角的に解析する能力を有する高度セキュリティ人材の育成を行う。 **（ウ）民間による国産セキュリティ製品・サービスの開発を加速させるための製品・技術の検証評価** 国産セキュリティ技術を検証できる環境を独自に構築し、国産セキュリティ技術や製品、サービスの検証・評価を実施するとともに、そのフィードバックを行うことで、製品やサービスの開発を支援する。また、最新のサイバー攻撃の知見に基づく検証手法の定式化、その継続的な更新を含めた製品検証の持続的な枠組作りを進める。 **（エ）演習基盤の開放による産学官における自律的な人材育成の支援** 各産業分野の特性に応じたサイバー攻撃対処能力の構築に貢献するため、より高度な対処能力構築といった観点にも留意しつつ、最新のサイバーセキュリティ関連情報やこれまでの機構における演習業務で得た知見等を活用した、民間企業や教育機関等が自ら人材育成演習を実施可能とする基盤を運用・開放し、民間企業等における自律

[1] サイバーセキュリティ分野における技術や人材を過度に海外へ依存することなく我が国独自に安定的に確保できるようにすること。

	的な人材育成の支援を行う。加えて、重要インフラ事業者、基幹インフラ事業者の業種向けの教材作成を強化し、高度演習に資する基盤を構築・運用する。
⑥ IoT機器のサイバーセキュリティ対策の促進 IoT機器のサイバーセキュリティ対策に貢献するため、サイバーセキュリティ戦略等の政府方針を踏まえ、NICT法第14条第1項第7号ロの規定に基づき、脆弱性を有する機器やマルウェア感染機器の調査を実施し、ユーザーやメーカー等の関係者に対して、必要な助言及び情報提供を行うものとする。また、独自のセンサーの開発等、IoT機器のサイバーセキュリティ向上の研究開発を行うものとする。	**（６）IoT 機器のサイバーセキュリティ対策の促進** IoT機器のサイバーセキュリティ対策に貢献するため、国からの補助等を受けた場合には、その予算の範囲内で、サイバーセキュリティ戦略等の政府方針を踏まえ、機構法第14条第１項第７号ロの規定に基づき、機構の有する技術的知見を活用して、脆弱性を有する機器やマルウェア感染機器の調査を実施し、ユーザーやメーカー等の関係者に対して、必要な助言及び情報提供を行う。本事業の推進に当たっては、機構法第18条の規定に基づき特定アクセス行為等を実施するとともに、内閣官房国家サイバー統括室、総務省、電気通信事業者及び関係団体等と密に連携する。 また、国からの補助等を受けた場合には、機構の有する技術的知見を活用して、独自のセンサーの開発等、IoT機器のサイバーセキュリティ向上の研究開発を行う。
（４）ユニバーサルコミュニケーション分野 ［略］	**２－４．ユニバーサルコミュニケーション分野** ［略］
（５）フロンティアサイエンス分野 ［略］	**２－５．フロンティアサイエンス分野** ［略］
３．イノベーションの基盤となる研究開発課題 ［略］	**３．イノベーションの基盤となる研究開発課題** ［略］
４．社会実装機能・外部連携機能等 NICTの研究開発成果を民間企業や大学等に橋渡しするための「社会実装機能」及び NICTが有する施設・設備や蓄積された知見等を活用して民間企業等のイノベーションを促進するための「外部連携機能」の充実・強化を図るものとする。 その際には、上記Ⅰ．１．で示した2030年代に目指すべき社会像の実現に資するよう、グローバルな視座から関連技術や人材育成・活用等のトレンドを把握・分析することで、イノベーション創出の方向性を明らかにするとともに、その実現に向けた実践的な行動計画を設計するものとする。また、産学官をはじめとしたすべての人々の「知」の結節点となるよう、過去から現在に至る研究開発の動向や社会的受容性等に関する知見の集積・共有を図るものとする。	**４．社会実装機能・外部連携機能等** 機構の研究開発成果を民間企業や大学等に橋渡しするための「社会実装機能」及び機構が有する施設・設備や蓄積された知見等を活用して民間企業等のイノベーションを促進するための「外部連携機能」の充実・強化を図る。 その際には、2030年代に目指すべき社会像の実現に向け、グローバルな視座から最新の技術、市場・ニーズ、標準化、人材育成・活用等のトレンドを把握・分析することで、イノベーション創出の方向性を明らかにするとともに、その実現に向けた実践的な行動計画を設計する。 また、国内外の公的情報資源との連携を段階的に推進し、研究者や市民が安心して活用できる参加型の知的基盤を形成する。その実現に向け、透明性と説明可能性を備えた情報整理・参照支援の仕組みを段階的に整備する。
（１）我が国発の技術の社会実装を促進するためのイノベーションハブ機能の強化 ［略］	**４－１．我が国発の技術の社会実装を促進するためのイノベーションハブ機能の強化** ［略］

（２）研究資金配分機関としての機能の強化 ［略］	**４－２．研究資金配分機関としての機能の強化** ［略］
（３）NICTにおける研究開発成果の社会実装推進体制の強化 ［略］	**４－３．研究開発成果の社会実装推進体制の強化** ［略］
（４）戦略的な標準化活動の推進 ［略］	**４－４．戦略的な標準化活動の推進** ［略］
（５）積極的かつ戦略的な国際連携の推進 ［略］	**４－５．積極的かつ戦略的な国際連携の推進** ［略］
（６）国土強靭化に向けた取組の推進 ［略］	**４－６．国土強靭化に向けた取組の推進** ［略］
（７）ICT人材育成の強化 我が国の国際競争力の強化のため、国として戦略的に取り組むべきICT研究開発分野において、NICTの研究成果等を活用した人材育成プログラムを若手技術者、教育指導者等へ提供し、新たな分野を切り拓くことのできる専門性の高い人材育成に取り組むものとする。 また、産学官連携による共同研究等を通じた専門人材の強化、連携大学院協定等によるNICTの職員の大学院・大学での研究・教育活動への従事、国内外の研究者や学生の受け入れ等を推進し、一層深刻化するICT人材不足の解消にも貢献するものとする。	**４－７．ICT人材育成の強化** 我が国のICT分野における国際競争力の強化や我が国の将来を担う人材の育成等のため、サイバーセキュリティ技術、量子情報通信技術等の技術分野において、機構の研究成果を活用した人材育成プログラムを策定・提供する。 また、産学官連携による共同研究等を通じて、幅広い視野や高い技術力を有する専門人材の強化に貢献する。さらに、連携大学院制度に基づく大学等との連携協定等を活用して機構の研究者を大学等へ派遣することにより、大学等におけるICT人材育成に寄与するとともに、国内外の研究者や大学院生等を機構の研究開発へ受け入れることにより、先端的な研究開発を担う人材を育成する。
（８）研究支援業務・事業振興業務等 ［略］	**４－８．研究支援業務・事業振興業務等** ［略］ **４－９．その他の業務** ［略］
５．NICT法第14条第１項第３号から第５号までの業務 ［略］	**５．機構法第14条第１項第３号から第５号までの業務** ［略］
Ⅳ．業務運営の効率化に関する事項 ［略］	**Ⅱ　業務運営の効率化に関する目標を達成するためとるべき措置** ［略］

Ⅴ．財務内容の改善に関する事項 ［略］	**Ⅲ　予算計画（人件費の見積もりを含む。）、収支計画及び資金計画** ［略］ **Ⅳ　短期借入金の限度額** ［略］ **Ⅴ　不要財産又は不要財産となることが見込まれる財産がある場合には、当該財産の処分に関する計画** ［略］ **Ⅵ　前号に規定する財産以外の重要な財産を譲渡し、又は担保に供しようとするときは、その計画** ［略］ **Ⅶ　剰余金の使途** ［略］
Ⅵ．その他業務運営に関する重要事項 ［略］	**Ⅷ　その他主務省令で定める業務運営に関する事項** ［略］