資料１

国立研究開発法人情報通信研究機構の第５期中長期目標の変更案に対するサイバーセキュリティ戦略本部の意見（案）について

資料１－１　国立研究開発法人情報通信研究機構の第５期中長期目標の変更案に対するサイバーセキュリティ戦略本部の意見（案）の概要

資料１－２　国立研究開発法人情報通信研究機構の第５期中長期目標の変更案に対するサイバーセキュリティ戦略本部の意見（案）

資料１－３　国立研究開発法人情報通信研究機構の第５期中長期目標の変更案　新旧対照表

NICTの中長期目標変更案に対するサイバーセキュリティ戦略本部の意見（案）概要

■ 国立研究開発法人情報通信研究機構（NICT）法では、「（NICTの）中長期目標を定め、又は変更しようとするときは、あらかじめ、サイバーセキュリティ戦略本部の意見を聴かなければならない。」とされている。

■ NICT中長期目標の変更案における主な変更点等と、それに対する戦略本部意見（案）は以下のとおり。

総務大臣が策定するNICT中長期目標の変更案の概要

➢ NICT法改正により、IoT機器の調査業務に関して、下記のとおり変更。

・調査対象機器：「パスワード設定等に不備のあるIoT機器」から「サイバーセキュリティの確保のための措置を十分に講じていないと認められるIoT機器※」に拡大。

※脆弱性があるファームウェア等を搭載しているIoT機器、既にマルウェアに感染しているIoT機器

・助言・情報共有：従前の「電気通信事業者(インターネットサービスプロバイダー)」に加え、「IoT機器の管理者等※(に対する必要な助言及び情報提供）」に拡大。 ※IoT機器メーカー等

➢ これを踏まえ、同趣旨をNICT中長期目標案に記載。

サイバーセキュリティ戦略本部の意見（案）の概要

➢ 中長期目標の変更案は「サイバーセキュリティ戦略」にも整合し、内容は妥当。

➢ 以下の点を総務大臣に要請。

- 最新のサイバーセキュリティ攻撃の動向等を踏まえ、調査対象機器の適時の見直し
- IoT機器メーカー等への「セキュアバイデザイン、セキュアバイデフォルト原則」の趣旨も踏まえた積極的な助言や情報の提供

NICTが行うサイバー攻撃に悪用されるおそれのあるIoT機器の調査について、①令和５年度末に時限を迎えるID・パスワードに脆弱性があるIoT機器の調査を、令和６年度以降も継続的に実施を可能とするとともに、②調査の対象を拡充するための規定を整備する。あわせて、特定通信・放送開発事業実施円滑化法の廃止等を行う。

１．サイバーセキュリティ関連業務の規定の整備

（国立研究開発法人情報通信研究機構法の改正）

① ID・パスワードに脆弱性があるIoT機器の調査の継続的な実施

○ NICTが令和５年度末までに限り行うこととされているID・パスワードに脆弱性があるIoT機器の調査（特定アクセス行為）を、令和６年度以降も継続的に実施できることとする。

② 調査対象の拡充

○ NICTが行うIoT機器の調査等に係る業務について、その対象を拡充※するとともに、総務大臣が、サイバーセキュリティ戦略本部から意見を聴取した上で、NICTの中長期目標の策定等をする旨を規定する。

※ID・パスワードに脆弱性があるIoT機器に加えて、脆弱性があるファームウェア等を搭載しているIoT機器、既にマルウェアに感染しているIoT機器を新たに対象とする。

２．信用基金の清算及び特定通信・放送開発事業実施円滑化法の廃止等

（・国立研究開発法人情報通信研究機構法の改正
・特定通信・放送開発事業実施円滑化法（NICTの業務特例を規定）の廃止）

○ NICTの信用基金を清算し、これに伴い、NICTの関連業務及び当該基金に係る業務を規定する特定通信・放送開発事業実施円滑化法を廃止する。

施行期日：令和６年４月１日（一部の規定を除く。）

（参考）国立研究開発法人　情報通信研究機構（NICT）の概要

■ 国立研究開発法人 情報通信研究機構（NICT※）は、ICT分野を専門とする我が国唯一の公的研究機関。
- 設立日：平成16年４月１日（旧（独）通信総合研究所（CRL）と旧通信・放送機構（TAO）が統合して発足）
- 役職員数： 理事長　徳田英幸(慶應義塾大学名誉教授)、理事５名、監事２名、職員1,329名（令和５年４月１日現在）
- 所在地： 小金井市 (本部)、横須賀市、神戸市、京都府精華町　（けいはんな）　等
- 令和５年度当初予算額：286.8億円（運営費交付金）（令和４年度当初予算額：282.5億円）

※　令和５年度は、第５期中長期計画期間（令和３年～令和７年）の３年目に当たる。

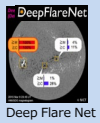
※ NICT: National Institute of Information and Communications Technology

重点研究分野 (NICT自らが研究開発を実施)

電磁波先進技術

・リモートセンシング
ゲリラ豪雨など突発的大気現象の早期捕捉


フェーズドアレイ気象レーダ



Deep Flare Net

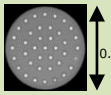
・宇宙環境
宇宙天気予報の提供

・時空標準
高精度な基準時刻の生成・分配供給


日本標準時システム

革新的ネットワーク

・フォトニックネットワーク
Beyond 5Gを支える大容量光ネットワーク



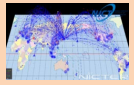
マルチコア光ファイバ

・次世代ワイヤレス
Beyond 5Gを実現する超高速・省電力・拡張空間の無線ネットワーク

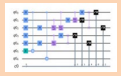

NTN（非地上系ネットワーク）

サイバーセキュリティ

・サイバーセキュリティ
多様化するサイバー攻撃に対応


NICTER

・暗号技術
耐量子計算機暗号など今後の利用が想定される次世代暗号


量子計算機を使った暗号解読

ユニバーサルコミュニケーション

・多言語コミュニケーション
自然な日本語に翻訳できる高精度な多言語翻訳


スマホアプリ

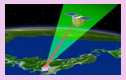

消防や警察でも活用
ライセンスによる
企業における製品普及

・社会知コミュニケーション
ユーザの興味や背景、コンテクストに応じた対話


対話ロボット

フロンティアサイエンス

・量子情報通信
量子鍵配送技術の国際標準化及び世界最高速の量子光源


光通信と量子鍵配送

・先端ICTデバイス
新型コロナウィルス対策に効果的な深紫外LED


深紫外光デバイス

・脳情報通信
脳情報通信による人間機能の拡張


脳機能全体のモデル化

我が国のICT産業の活性化、国際競争力確保に向けた取組

□Beyond 5Gの推進
- ◇先端的な研究開発を自主研究として実施
- ◇情報通信研究開発基金を活用した研究開発の支援・実施　等

□オープンイノベーション創出に向けた取組の強化
- ◇社会実装体制、産学官連携の強化
- ◇戦略的な標準化活動の推進
- ◇戦略的なICT人材の育成　等

□研究支援・事業振興業務
- ◇海外研究者の招へい
- ◇情報通信ベンチャー企業の事業化支援

機構法に基づく業務

□標準電波の発射、標準時の通報

□宇宙天気予報

□無線設備の機器の試験及び較正

資料１－２

国立研究開発法人情報通信研究機構の第５期中長期目標の変更案に対するサイバーセキュリティ戦略本部の意見（案）

令和６年１月〇日
サイバーセキュリティ戦略本部決定

今日の我が国の社会経済活動や国民生活においては、サイバー空間への依存度がますます高まっており、これまでシステムを積極的に利用してこなかった分野や組織においても、IoT 機器を含む情報システムの利用が拡大している。また、デジタル化による新たな技術・サービスの進展は、国民の利便性の向上につながり、特に急速に普及しつつある生成 AI は我が国の社会経済活動の持続的な発展につながり得るものとして大いに期待されている。

一方で、こうしたサイバー空間の利用拡大、生成 AI などの新たな技術・サービスの普及に伴い、サイバー攻撃を受けるシステム側の侵入口（攻撃の端緒となる、いわゆる「セキュリティホール」）が増加しており、また、不十分なセキュリティ対策の結果としてシステム障害や情報漏えい等のインシデントにつながる可能性も増加するなど、サイバーリスクが高まっている。

こうした脅威等を踏まえ、「サイバーセキュリティ戦略」（令和３年９月 28 日閣議決定）では、IoT や 5G 等の新たな技術やサービスの実装における安全・安心の確保のため、安全な IoT システムを実現するための協働活動や指針策定、情報共有、国際標準化の推進、脆弱性対策への体制整備を実施することなどを盛り込んでいる。

今般、国立研究開発法人情報通信研究機構法の一部を改正する等の法律（令和５年法律第 87 号）を踏まえ、令和５年度まで実施されてきた「パスワード設定等に不備のある IoT 機器の調査」の調査対象を拡充し、令和６年度以降も実施される形で、今回の中長期目標の変更案に「IoT 機器のサイバーセキュリティ対策の促進」が追加されており、サイバーセキュリティの確保のための措置を十分に講じていないと認められる IoT 機器について、当該機器の管理者その他の関係者に対して必要な助言及び情報提供に関する業務を実施するとされ、その際には関係機関との連携を促進するものとされている。

こうした取組は、安全な IoT システムの構築に当たって重要な役割を果たすものであり、「サイバーセキュリティ戦略」が定める安全な IoT システムを実現するための協働活動や指針策定、情報共有にも資するもので「サイバーセキュリティ戦略」にも整合するものである。また、内閣官房内閣サイバーセキュリティセンター（以下「NISC」という。）が昨年 10 月に米国サイバーセキュリティ・インフラストラクチャー安全保障庁（CISA）等とともに共同署名に加わり公表した「セキュアバイデザイン、セキュアバイデフォルトに関する文書」が内容とする、「IoT 機器を含む IT 製品を対象とした、安全

性を確保した設計の実施」（セキュアバイデザイン）及び「ユーザー（顧客）が追加コストや手間を掛けることなく購入後すぐに安全にIT製品等を利用できること」（セキュアバイデフォルト）の両理念の具体化にも資するものである。

以上の考えに照らし、サイバーセキュリティ戦略本部としては、示された第５期中長期目標の変更案については妥当な内容であると判断する。

なお、NICTが、変更後の中長期目標を踏まえ適切に業務運営を行うよう、総務大臣に対し、以下の事項を要請する。

(1) 調査の実施について、以下の点に留意すること。

① 調査の内容は、対象となるIoT機器の実情や最新のサイバー攻撃の動向を踏まえたものとするほか、令和７年（2025年）日本国際博覧会（大阪・関西万博）等の大規模国際イベントも見据え、IoT機器を踏み台にした大規模なサイバー攻撃を防止するため、利用者に広範に注意喚起ができるよう、実効性の高いものとなるように努めるとともに、調査すべき機器の範囲について適時に見直しが行われること。

② 調査の実施に当たっては、既存の脆弱性関連制度と適切に連携しつつ、調査に関して十分な周知を行うとともに、IoT機器の利用者への影響等を十分考慮すること。また、適切なパスワード設定に加え、今般、新たに調査対象として拡充されるIoT機器の脆弱性等に対する有効なサイバーセキュリティ対策を講じることの必要性について関係者に周知活動を行うとともに、「セキュアバイデザイン、セキュアバイデフォルトに関する文書」の趣旨も踏まえ、利用者において安全なIoT機器の利用が実現されるよう、IoT機器メーカー、電気通信事業者等のセキュリティ関係者への積極的な助言や情報の提供が行われること。

③ 調査の結果については、適時、NICTにおける知見や研究開発にフィードバックして調査手法の高度化に努めるとともに、NISCをはじめとする関係省庁に対して必要に応じて情報共有を行うこと。

④ 調査を効果的かつ効率的に実施するため、必要な調査費用の確保や実施体制の充実に向けた検討を進めるとともに、既に流通しているIoT機器等については、利用者、製造事業者、電気通信事業者等の様々な主体が関係することから、これらの有機的連携が確保された取組につながるよう、NISCをはじめとする関係

省庁との連携を行うこと。

(2) 変更後の中長期目標を踏まえた調査の実施状況については、年次報告において毎年度の実績をサイバーセキュリティ戦略本部に報告すること。また、NISC からの求めに応じて適宜報告を行うこと。

(3) 次期サイバーセキュリティ戦略の策定等において、調査に関係する重要な改正がなされた場合は、その改正内容を踏まえ、必要に応じ、中長期目標の変更等の必要な措置を講じること。

以上

資料１－３

国立研究開発法人情報通信研究機構の中長期目標（第５期）の変更案　新旧対照表

（※国立研究開発法人情報通信研究機構法の一部を改正する等の法律による改正後の国立研究開発法人情報通信研究機構法第14条第１項第７号に掲げる業務又はこれに附帯する部分のみに係る変更部分のみ）

（傍線部分は変更部分）

Page	変更案	現行
7,8	**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** **１．重点研究開発分野の研究開発等** **（３）サイバーセキュリティ分野** **①・②　（略）** **③　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等のサイバー攻撃への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の方針を踏まえ、NICT法第14条第１項第７号イ（令和５年度までは第14条第１項第７号）の規定に基づき、最新のサイバー攻撃に関する知見を踏まえた実践的な演習を実施するほか、若手セキュリティ人材の育成を行う。 **④　（略）** **⑤　パスワード設定等に不備のあるIoT機器の調査（令和５年度まで）** 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の方針を踏まえ、国立研究開発法人情報通信研究機構法の一部を改正する等の法律（令和５年法律第87号）による改正前のNICT法附則第８条第２項の規定に基づき、パスワード設定等に不備のあるIoT機器の調査及び電気通信事業者への情報提供に関する業務を、令和６年３月31日まで実施する。その際、関係機関と連携を図るとともに、本調査の重要性等を踏まえ、情報の安全管理に留意しつつ、広範な調査を行うことができるよう配慮する。 **⑥　IoT機器のサイバーセキュリティ対策の促進（令和６年度以降）** 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の方針を踏まえ、NICT法第14条第１項第７号ロの規定に基づき、サイバーセキュリティの確保のための措置を十分に講じていないと認められるIoT機器について、当該機器の管理者その他の関係者に対して必要な助言及び情報提供に関する業務（同法第18条の規定に基づくパスワード設定等に不備のあるIoT機器の調査及び電気通信事業者への情報提供に関する業務を含む。）を実施する。その際、本業務の重要性等を踏まえ、情報の安全管理に留意しつつ、関係機関と連携を促進するものとする。	**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** **１．重点研究開発分野の研究開発等** **（３）サイバーセキュリティ分野** **①・②　（同左）** **③　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等のサイバー攻撃への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の方針を踏まえ、NICT法第14条第１項第７号の規定に基づき、最新のサイバー攻撃に関する知見を踏まえた実践的な演習を実施するほか、若手セキュリティ人材の育成を行う。 **④　（同左）** **⑤　パスワード設定等に不備のあるIoT機器の調査** 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の方針を踏まえ、NICT法附則第８条第２項の規定に基づき、パスワード設定等に不備のあるIoT機器の調査及び電気通信事業者への情報提供に関する業務を、令和６年３月31日まで実施する。その際、関係機関と連携を図るとともに、本調査の重要性等を踏まえ、情報の安全管理に留意しつつ、広範な調査を行うことができるよう配慮する。 ［新設］

別紙３

NICTの評価軸等

III. 1. 重点研究開発分野の研究開発等

項目	評価軸	指標
(3)サイバーセキュリティ分野	• 研究開発等の取組・成果の科学的意義（独創性、革新性、先導性、発展性等）が十分に大きなものであるか。 • 研究開発等の取組・成果が社会課題・政策課題の解決につながるものであり、または、それらが社会的価値の創出に十分に貢献するものであるか。 • 研究開発等の成果を社会実装につなげる取組（技術シーズを実用化・事業化	【評価指標】 • 具体的な研究開発成果 • 研究開発成果の移転及び利用の状況 • 共同研究や産学官連携の状況 • データベース等の研究開発成果の公表状況 • （個別の研究開発課題における）標準や国内制度の成立寄与状況 • IoT 機器調査に関する業務の実施状況（「パスワード設定等に不備のある IoT 機器の調査」の評価時に使用）（令和５年度まで） • IoT 機器のサイバーセキュリティ対策の促進に関する業務の実施状況（「IoT 機器のサイバーセキュリティ対策の促進」の評価時に使用）（令和６年度以降） 【モニタリング指標】 • 査読付き論文数 • 招待講演数 • 論文の合計被引用数 • 研究開発成果の移転及び利用に向けた活動件数（実施許諾件数等） • 報道発表や展示会出展等の取組件数 • 共同研究件数 • （個別の研究開発課題における）標準化や国内制度化の寄与件数 • 演習の実施回数又は参加人数（「サイバーセキュリティに関する演習」の評価時に使用）

NICTの評価軸等

III. 1. 重点研究開発分野の研究開発等

項目	評価軸	指標
(3)サイバーセキュリティ分野	• 研究開発等の取組・成果の科学的意義（独創性、革新性、先導性、発展性等）が十分に大きなものであるか。 • 研究開発等の取組・成果が社会課題・政策課題の解決につながるものであり、または、それらが社会的価値の創出に十分に貢献するものであるか。 • 研究開発等の成果を社会実装につなげる取組（技術シーズを実用化・事業化	【評価指標】 • 具体的な研究開発成果 • 研究開発成果の移転及び利用の状況 • 共同研究や産学官連携の状況 • データベース等の研究開発成果の公表状況 • （個別の研究開発課題における）標準や国内制度の成立寄与状況 • IoT 機器調査に関する業務の実施状況（「パスワード設定等に不備のある IoT 機器の調査」の評価時に使用） • ［新設］ 【モニタリング指標】 • 査読付き論文数 • 招待講演数 • 論文の合計被引用数 • 研究開発成果の移転及び利用に向けた活動件数（実施許諾件数等） • 報道発表や展示会出展等の取組件数 • 共同研究件数 • （個別の研究開発課題における）標準化や国内制度化の寄与件数 • 演習の実施回数又は参加人数（「サイバーセキュリティに関する演習」の評価時に使用）

Page	変更案			現行		
		に導く等）が十分であるか。 • 取組が ICT 人材の需要に対応できるものとして適切に実施されたか。（「サイバーセキュリティに関する演習」及び「サイバーセキュリティ産学官連携拠点形成」の評価時に使用） • 取組が我が国全体のサイバーセキュリティ対応能力強化に貢献するものとして計画に従って着実に実施されたか。	• 構築した基盤環境の外部による利用回数、もしくは利用者数（「サイバーセキュリティ産学官連携拠点形成」の評価時に使用） • 民間企業が開発した人材育成コンテンツ数（「サイバーセキュリティ産学官連携拠点形成」の評価時に使用） • 調査した IoT 機器数（「パスワード設定等に不備のある IoT 機器の調査」の評価時に使用）（令和５年度まで） • IoT 機器の調査に基づく通知件数（「IoT 機器のサイバーセキュリティ対策の促進」の評価時に使用）（令和６年度以降）		に導く等）が十分であるか。 • 取組が ICT 人材の需要に対応できるものとして適切に実施されたか。（「サイバーセキュリティに関する演習」及び「サイバーセキュリティ産学官連携拠点形成」の評価時に使用） • 取組が我が国全体のサイバーセキュリティ対応能力強化に貢献するものとして計画に従って着実に実施されたか。	• 構築した基盤環境の外部による利用回数、もしくは利用者数（「サイバーセキュリティ産学官連携拠点形成」の評価時に使用） • 民間企業が開発した人材育成コンテンツ数（「サイバーセキュリティ産学官連携拠点形成」の評価時に使用） • 調査した IoT 機器数（「パスワード設定等に不備のある IoT 機器の調査」の評価時に使用） • ［新設］