資料１

国立研究開発法人情報通信研究機構の第５期中長期計画（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１－１　国立研究開発法人情報通信研究機構の第５期中長期計画（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第５期中長期目標・中長期計画（案）　対比表

資料１－３　国立研究開発法人情報通信研究機構の第５期中長期計画（案）に対するサイバーセキュリティ戦略本部の意見（案）

国立研究開発法人情報通信研究機構の第５期中長期計画（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１－１

- 国立研究開発法人情報通信研究機構法（NICT法）の規定において、総務大臣が国立研究開発法人情報通信研究機構（NICT）の中長期計画を認可しようとするときは、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。
- 本年２月26日に総務大臣がNICTの第５期中長期目標（目標期間：令和３～７年度）を定め、NICTに指示したことを踏まえ、同年３月１日にNICTが総務大臣に中長期計画の認可申請を実施。
- 当該中長期計画においてNICTが実施する業務のうち、政府全体のサイバーセキュリティ戦略と整合的な形で実施される必要があるものについて、意見の求めがあった。

第５期中長期計画（案）の概要

✓ ５つの重点研究開発分野のうちの一つとして規定する「サイバーセキュリティ分野」のうち、次の研究開発等について、サイバーセキュリティ戦略本部の意見が求められている。

① **サイバーセキュリティに関する演習**
NICT法第14条第１項第７号に掲げる業務として、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

② **パスワード設定等に不備のあるIoT機器の調査**
NICT法附則第８条第２項に規定する業務として、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実施

戦略本部の意見の概要

- 「サイバーセキュリティに関する演習」は、サイバーセキュリティ**人材の育成のために重要な役割**を果たすもの
- 「パスワード設定等に不備のあるIoT機器の調査」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、示された**中長期計画案は**第５期中長期目標を踏襲したものであることから、サイバーセキュリティ戦略本部としては、**妥当な内容と判断**。

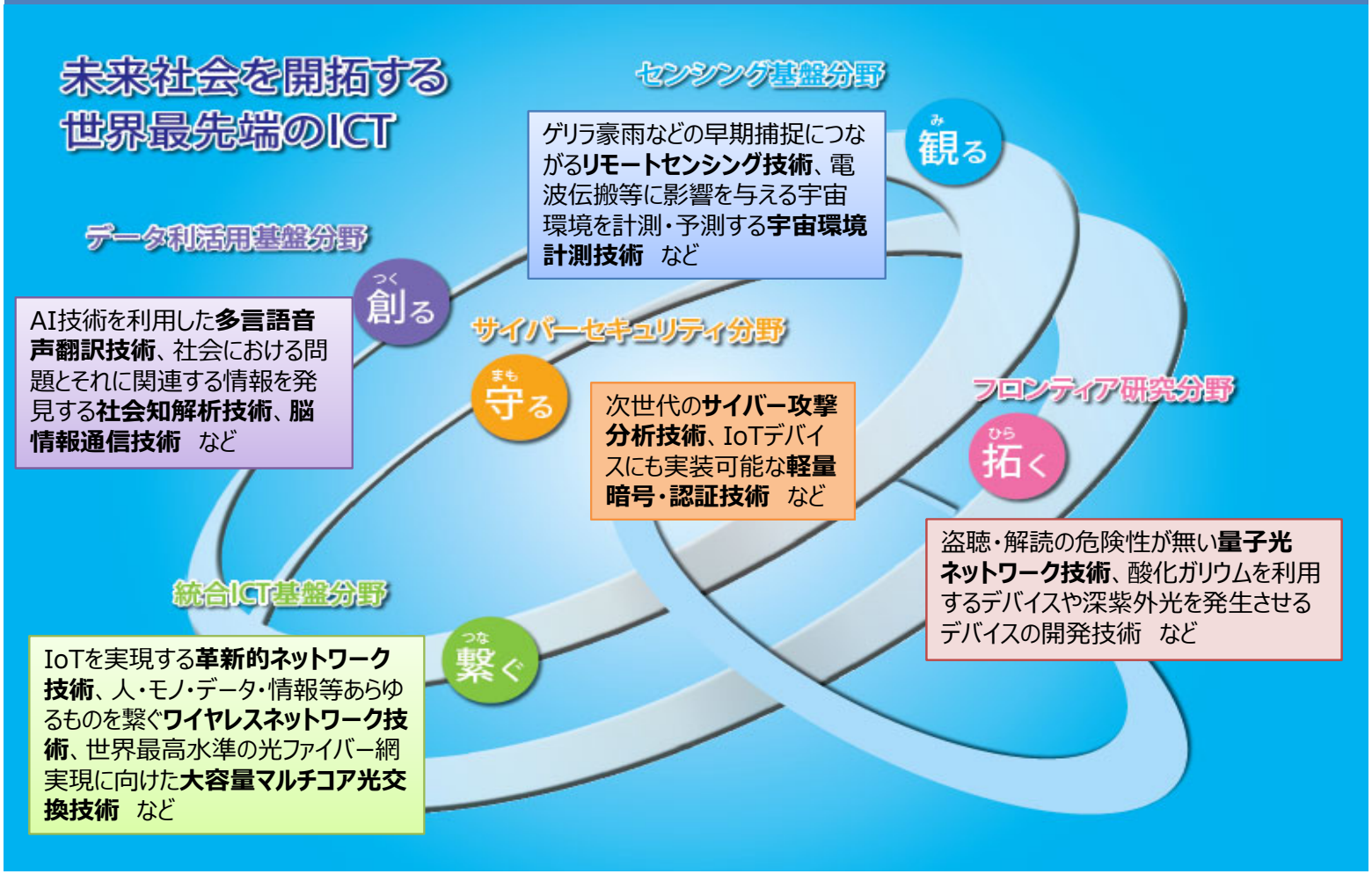
また、適切に業務運営が行われるよう、第５期中長期目標（案）に対する意見において要請した事項※の着実な実施を要請する。

※中長期目標においてサイバーセキュリティ戦略本部から要請した事項
- 演習内容は、**実効性の高いものとするよう努め、適時に見直し**を行うこと
- 調査については、NICTの研究開発にフィードバックして**調査手法の高度化**に努めること
- 戦略等の改正がなされた場合は、当該改正内容を踏まえ、必要に応じて中長期目標の改正等の措置を講じること　　など

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。
- 役職員数：理事長　徳田英幸（慶應義塾大学客員教授）、理事５名、監事２名、職員1,187名　（R2.4.1現在）
- 令和２年度当初予算額：279.4億円
- 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

ＩＣＴ分野の基礎的・基盤的な研究開発



研究開発成果を最大化するための業務

- 技術実証と社会実証の一体的推進が可能なテストベッド構築・運用
- オープンイノベーション創出に向けた産学官連携等の取組
- 耐災害ＩＣＴの実現に向けた取組
- 戦略的な標準化活動の推進
- 研究開発成果の国際展開
- サイバーセキュリティに関する演習
- パスワード設定等に不備のあるIoT機器の調査

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

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
- ＩＣＴ人材の育成

サイバーセキュリティに関する演習（CYDER）

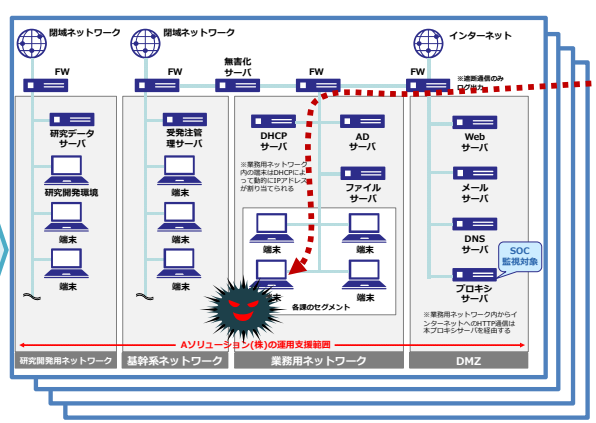
CYDER：CYber Defense Exercise with Recurrence

- 国立研究開発法人情報通信研究機構法の改正（平成28年４月27日公布、５月31日施行）を受け、NICTは、**国の機関**、**指定法人**、**独立行政法人**、**地方公共団体**及び**重要インフラ事業者等**の情報システム担当者等を対象とした体験型の**実践的サイバー防御演習（CYDER）**を平成29年度から実施。
- 受講者は、**チーム単位で演習に参加。組織のネットワーク環境を模した大規模仮想LAN環境下で、実機の操作を伴って**サイバー攻撃によるインシデントの検知から対応、報告、回復までの**一連の対処方法を体験。**
- **全都道府県**において、年間**100回**・計**3,000名規模**で実施。
  ※平成29年度：年間100回・3,009名受講／平成30年度：年間107回・2,666名受講／令和元年度：年間105回・3,090名受講

演習のイメージ

我が国唯一の情報通信に関する公的研究機関である**NICTが有する最新のサイバー攻撃情報を活用**し、実際に起こりうるサイバー攻撃事例を再現した**最新の演習シナリオ**を用意。

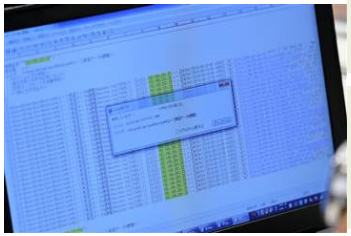
北陸StarBED技術センターの大規模高性能サーバ群を活用



擬似攻撃者

企業・自治体の**社内LANや端末を再現**した環境で演習を実施

受講チームごとに独立した演習環境を**構築**



演習模様 **専門指導員**による補助

チーム内での議論を通じた相互理解

本番同様のデータを使用した演習

インシデント（事案）対処能力の向上

令和２年度の実施状況

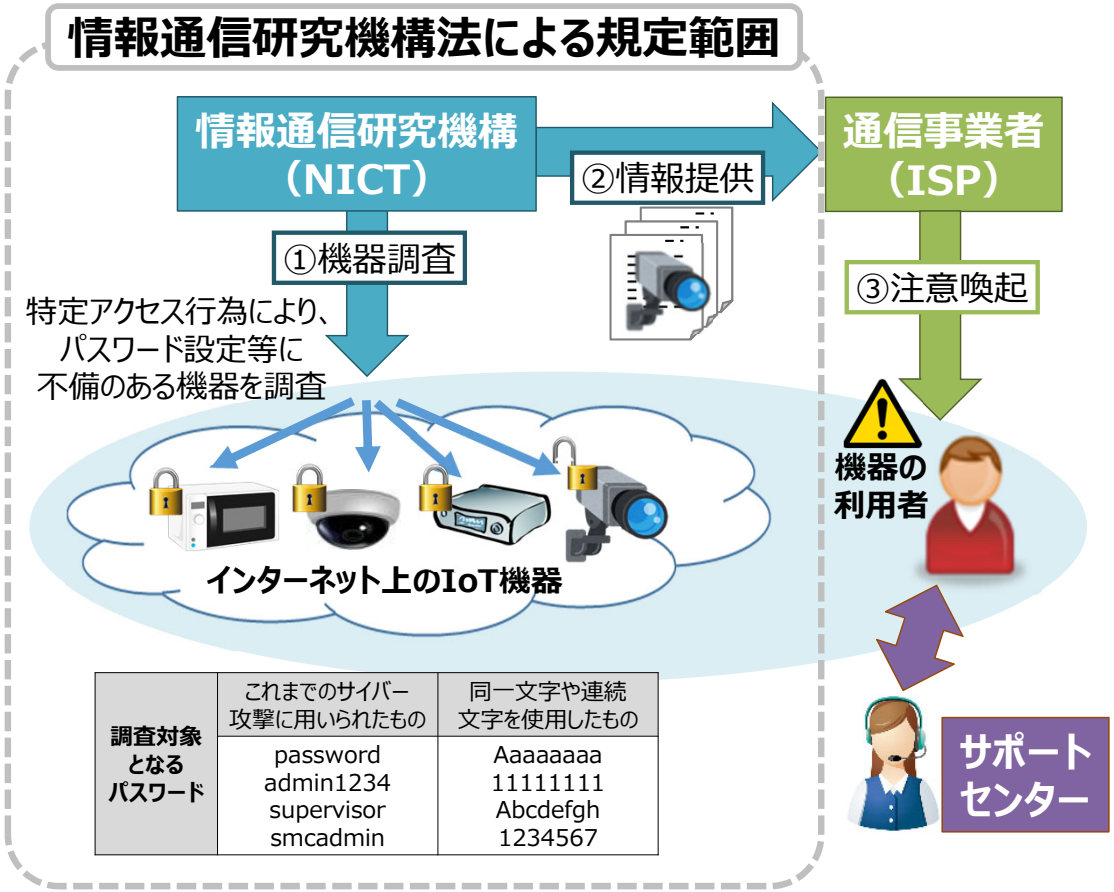
コース	受講対象組織	対象者	開催地	開催回数	実施時期
Aコース（初級）	全組織共通	システムの運用担当者（システムの利用者レベルを含む）	４７都道府県	７２回	８月～翌年２月
B-1コース（中級）	地方公共団体	セキュリティ管理業務を主導する立場の者	全国１１地域	１９回	10月～翌年２月
B-2コース（中級）	国の機関等、重要インフラ事業者等		東京・大阪・名古屋・福岡	１５回	１月～翌年２月

パスワード設定等に不備のあるIoT機器の調査（NOTICE）

NOTICE: National Operation Towards Iot Clean Environment

- 国立研究開発法人情報通信研究機構法の改正（平成30年５月23日公布、11月１日施行）を受け、NICTは、**パスワード設定等に不備があり、サイバー攻撃に悪用されるおそれのあるIoT機器の調査（NOTICE）**を平成31年２月より実施。
- NICTが実施した調査結果については、インターネット・サービス・プロバイダ（ISP）へ通知を行い、ISPにおいて利用者を特定した上で当該利用者に対して注意喚起を実施。

調査の実施イメージ



調査対象となるパスワード	これまでのサイバー攻撃に用いられたもの	同一文字や連続文字を使用したもの
	password admin1234 supervisor smcadmin	Aaaaaaaa 11111111 Abcdefgh 1234567

調査の実施結果（令和２年末時点）

注意喚起対象としてISPへ通知したもの*

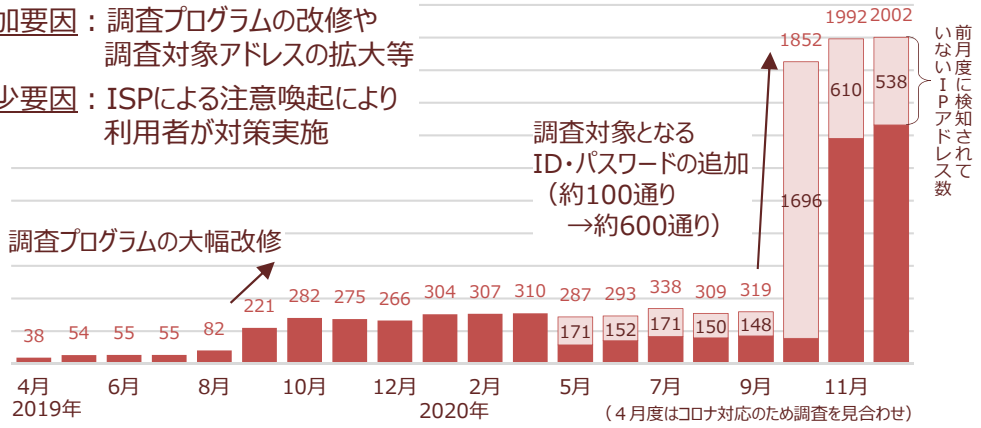
2,002件（2020年12月度分）

（参考）2020年度の累積件数：7,392件（2019年度：2,249件）
ID・パスワードが入力可能だったもの：8.6万件

*) 特定のID・パスワードによりログインできるかという調査をおおむね月に1回実施し、ログインでき、注意喚起対象となったもの（ユニークIPアドレス数）

増加要因：調査プログラムの改修や調査対象アドレスの拡大等

減少要因：ISPによる注意喚起により利用者が対策実施



（参考）国立研究開発法人情報通信研究機構法

国立研究開発法人情報通信研究機構法（平成11年法律第162号）

第十四条　**機構は**、第四条の目的を達成するため、**次の業務を行う**。
一　情報の電磁的流通及び電波の利用に関する技術の調査、研究及び開発を行うこと。
二～六　［略］
→サイバーセキュリティに関する演習（CYDER）
七　第一号に掲げる業務に係る成果の普及として**サイバーセキュリティ(略)に関する演習その他の訓練を行うこと**。
八　前号に掲げるもののほか、第一号、第二号及び第六号に掲げる業務に係る成果の普及を行うこと。
九～十三　［略］

＜附則第８条第２項＞
→パスワード設定等に不備のあるIoT機器の調査（NOTICE）
２　機構は、第十四条及び前項に規定する業務のほか、**平成三十六年三月三十一日までの間、次に掲げる業務を行う**。
一　特定アクセス行為を行い、通信履歴等の電磁的記録を作成すること。
二　特定アクセス行為に係る電気通信の送信先の電気通信設備が次のイ又はロに掲げる者の電気通信設備であるときは、当該イ又はロに定める者に対し、通信履歴等の電磁的記録を証拠として当該電気通信設備又は当該電気通信設備に電気通信回線を介して接続された他の電気通信設備を送信先又は送信元とする送信型対電気通信設備サイバー攻撃のおそれへの対処を求める通知を行うこと。
イ　電気通信事業者　当該電気通信事業者
ロ　電気通信事業者（略）の利用者　当該電気通信事業者
三　前二号に掲げる業務に附帯する業務を行うこと。

＜附則第８条第６項において準用する第23条＞
第二十三条　総務大臣は、通則法第三十五条の四第一項の規定により中長期目標（第十四条第一項第七号に掲げる業務及びこれに附帯する業務並びに附則第八条第二項に規定する業務に係る部分に限る。）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。
２　総務大臣は、通則法第三十五条の五第一項の規定による**中長期計画**（**第十四条第一項第七号に掲げる業務**及びこれに附帯する業務並びに**附則第八条第二項に規定する業務**に係る部分に限る。）**の認可をしようとするとき**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**。

資料１－２

国立研究開発法人情報通信研究機構第５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５期中長期目標 （令和３年２月26日総務大臣指示）	第５期中長期計画（案） （令和３年３月１日認可申請）
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	１．重点研究開発分野の研究開発等
（１）電磁波先進技術分野 ［略］	１－１．電磁波先進技術分野 ［略］
（２）革新的ネットワーク分野 ［略］	１－２．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 我が国において、これまでにない価値の創造や社会システムの変革等をもたらす新たなイノベーション力を強化するためには、「社会（生命・財産・情報）を守る」能力として、急増するサイバー攻撃から社会システム等を守るサイバーセキュリティ分野の技術の高度化が不可欠となっていることから、【重要度：高】として、以下の研究開発等に取り組むとともに、標準化、研究開発成果の普及や社会実装を目指すものとする。 また、急増するサイバー攻撃への対策は国を挙げた喫緊の課題となっており、サイバーセキュリティ分野でのNICTに対する社会的要請が高まりつつあることから、研究開発等やその成果普及等に関する体制の強化に向けた措置を講ずるものとする。	１－３．サイバーセキュリティ分野 我が国において、これまでにない価値の創造や社会システムの変革等をもたらす新たなイノベーション力を強化するためには、「社会（生命・財産・情報）を守る」能力として、急増するサイバー攻撃から社会システム等を守るサイバーセキュリティ分野の技術の高度化が不可欠となっていることから、以下の研究開発等に取り組むとともに、標準化、研究開発成果の普及や社会実装を目指す。 また、急増するサイバー攻撃への対策は国を挙げた喫緊の課題となっており、サイバーセキュリティ分野での機構に対する社会的要請が高まりつつあることから、研究開発等やその成果普及等に関する体制の強化に向けた措置を講ずる。
①　サイバーセキュリティ技術 サイバー攻撃対処能力の絶え間ない向上と多様化するサイバー攻撃の対処に貢献するため、巧妙化・複雑化するサイバー攻撃に対応した攻撃観測・分析・可視化・対策技術、大規模集約された攻撃に関する多種多様な情報の横断分析技術、新たなネットワーク環境等のセキュリティ向上のための検証技術の研究開発を実施する。	（１）サイバーセキュリティ技術 サイバー攻撃対処能力の絶え間ない向上と多様化するサイバー攻撃の対処に貢献するため、巧妙化・複雑化するサイバー攻撃に対応した攻撃観測・分析・可視化・対策技術、大規模集約された多種多様なサイバー攻撃に関する情報の横断分析技術、新たなネットワーク環境等のセキュリティ向上のための検証技術の研究開発を実施する。 （ア）データ駆動型サイバーセキュリティ技術 無差別型攻撃や標的型攻撃をはじめとする巧妙化・複雑化するサイバー攻撃を複数の側面から観測する技術、状況把握を支える可視化技術、機械学習等のAI技術を駆使した自動分析・自動対策技術の確立・高度化を進める。また、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、横断分析する技術についても確立・高度化を進める。 サイバー攻撃のトレンドの変化等に対応した技術開発を迅速に進める体制を

	整え、開発した技術や得られたデータの社会展開を進める。また、開発した観測・分析技術は、（３）から（５）までの取組に適用することにより技術検証を行うとともに、当該取組からのフィードバックを受け、有用性を高めていく。 （イ）エマージングセキュリティ技術 新たに社会に登場する技術のセキュリティに関する課題抽出や対策に貢献するため、最新の通信機器、IoT機器、コネクテッドカー等のエマージング技術に対応したセキュリティ検証技術を確立する。具体的には、エマージング技術のネットワーク接続試験環境構築、実機を用いた脅威分析や攻撃シナリオの評価等により、個々のエマージング技術のセキュリティ課題を抽出し対策につなげる。また、これらの知見を通じ、今後世の中に登場するBeyond 5G等の新たなネットワーク環境におけるセキュリティ課題や検証手法を明確化する。
②　暗号技術 社会の持続的発展において欠くことの出来ない情報のセキュリティやプライバシーの確保を確かなものとするため、耐量子計算機暗号等を含む新たな暗号・認証技術やプライバシー保護技術の研究開発を実施するものとする。その安全性評価を行うとともに、安全な情報利活用を推進し、国民生活を支える様々なシステムへの普及を図るものとする。	（２）暗号技術 社会の持続的発展において欠くことの出来ない情報のセキュリティやプライバシーの確保を確かなものとするため、耐量子計算機暗号等を含む新たな暗号・認証技術やプライバシー保護技術の研究開発を実施し、その安全性評価を行うとともに、安全な情報利活用を推進し、国民生活を支える様々なシステムへの普及を図る。 （ア）安全なデータ利活用技術 データの提供・収集・保管・解析・展開の各段階におけるセキュリティやプライバシーを確保するため、匿名認証や検索可能暗号等のアクセス制御技術、秘匿計算等のプライバシー保護解析技術等の研究開発を行う。これらを用いて組織横断的な連携を含むデータ利活用を促進するとともに、安全なテレワーク等の社会的な課題解決に貢献する。 （イ）量子コンピュータ時代に向けた暗号技術の安全性評価 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、耐量子計算機暗号を含む新たな暗号技術及び電子政府システム等において使用される暗号技術の安全性評価に関する研究開発を実施する。具体的には、将来的には耐量子計算機暗号として世界標準となることが予想される格子暗号、多変数公開鍵暗号等や、現在広く使用されているRSA暗号、楕円曲線暗号等の安全性評価について取り組み、世界最先端の評価技術によって国民生活を支える様々なシステムの安全な運用に貢献する。
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。	（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、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の受講機会を確保するとともに、重要社会基盤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、オンライン演習を拡大していくこととし、未受講となる組織・団体に対して積極的な参加を促す。あわせて、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、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。
④　サイバーセキュリティ産学官連携拠点形成 我が国のサイバー攻撃対処能力の絶え間ない向上に貢献するため、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、横断的に分析し、実践的な脅威情報の生成・関係機関との共有等を行うための基盤を構築する。また、当該基盤を活用し、国産セキュリティ技術を事業者が検証できる環境を構築するとともに、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に取り組む。加えて、社会全体でのセキュリティ人材の持続的供給のため、演習で得た知見等を積極的に活用するための基盤を構築し、民間等における自律的な人材育成の支援を行う。これらの取組により、我が国のサイバーセキュリティに関する情報分析・人材育成等の中核拠点を形成する。	（４）サイバーセキュリティ産学官連携拠点形成 我が国のサイバーセキュリティ対処能力の絶え間ない向上に貢献し、社会全体でセキュリティ人材を持続的に育成していくため、サイバーセキュリティに関する情報分析・人材育成等の産学官連携の中核的拠点を形成する。 具体的には、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ための基盤を構築するとともに、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。あわせて、当該基盤を活用し、国産セキュリティ技術を機器製造事業者や運用事業者が検証できる環境を構築する。 また、上記の取組を通じて、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。さらに、これら取組で得た最新のサイバーセキュリティ関連情報に（３）の演習で得た知見等をあわせ、これを活用した人材育成演習を民間や教育機関等が実施可能とするための基盤を構築し、民間等における自律的な人材育成の支援を行う。 加えて、これら取組について、産学官の関係者が円滑かつ自主的に参画できるような枠組みを整備し、参画機関からの要望やフィードバックを反映しつつ基盤を構築し、参画機関の協力を得て運営する。
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。	（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、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、機構法附則第８条第２項の規定に基づき、機構の有する技術的知見を活用して、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、総務省や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、調査手法や情報の安全管理に留意しつつ、より広範かつより高度な調査を行うことができるよう配慮する。

（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］	１－４．ユニバーサルコミュニケーション分野 ［略］ １－５．フロンティアサイエンス分野 ［略］

資料１－３

国立研究開発法人情報通信研究機構の第５期中長期計画（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３年３月●日
サイバーセキュリティ戦略本部決定

ますます複雑化・巧妙化するサイバー攻撃に対応し、サイバーセキュリティ対策の抜本的な強化を図るためには、サイバーセキュリティ戦略（平成30年７月27日閣議決定）等を踏まえ、関係機関の知見を活用していくことが必要である。

国立研究開発法人情報通信研究機構法（平成11年法律第162号）第14条第１項第７号に掲げる業務として、国立研究開発法人情報通信研究機構（以下「NICT」という。）が行うサイバーセキュリティに関する演習については、サイバーセキュリティ基本法（平成26年法律第104号）第13条及び第14条に定める演習として、サイバーセキュリティ人材の育成のために重要な役割を果たすものである。
その実施に当たっては、サイバーセキュリティ戦略を踏まえ、複雑化・巧妙化するサイバー攻撃に対応し、かつ、組織や企業のニーズに対応した人材の育成に努めることが求められる。

また、国立研究開発法人情報通信研究機構法附則第８条第２項に規定する業務として、NICTが行うパスワード設定等に不備のあるIoT機器の調査（以下「IoT機器調査」という。）については、IoT機器に対するサイバー攻撃等の深刻化に対応し、ネットワークの安全・信頼性を確保する観点から重要な役割を果たすものである。
その実施に当たっては、サイバーセキュリティ戦略を踏まえ、産官学民及び民間企業相互間の連携と役割分担の下で進めることが求められる。

以上の「国立研究開発法人情報通信研究機構の第５期中長期目標案に対するサイバーセキュリティ戦略本部の意見」（令和３年２月９日サイバーセキュリティ戦略本部決定。以下「戦略本部意見」という。）でも示した考えに照らし、サイバーセキュリティ戦略本部としては、示された中長期計画案については、妥当な内容である、と判断する。

なお、NICTが、この中長期計画を踏まえ適切に業務運営を行うよう、総務大臣に対しては、引き続き戦略本部意見に記載の事項を着実に実施するよう要請する。

以上