資料７

国立研究開発法人情報通信研究機構の中長期目標の改正案に対する サイバーセキュリティ戦略本部の意見（案）

資料７－１　国立研究開発法人情報通信研究機構（NICT）の中長期目標の変更について

資料７－２　国立研究開発法人情報通信研究機構第４期中長期目標変更（案）　新旧対照表

資料７－３　国立研究開発法人情報通信研究機構の中長期目標の改正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７－１

国立研究開発法人情報通信研究機構（NICT）の中長期目標の変更について

平成３０年７月
総　　務　　省

国立研究開発法人情報通信研究機構法の一部改正について

● IoT機器などを悪用した**サイバー攻撃の深刻化**を踏まえ、国立研究開発法人情報通信研究機構（NICT）の業務に、**パスワード設定等に不備のあるIoT機器の調査**等を追加（**5年間の時限措置**）する等を内容とする**国立研究開発法人情報通信研究機構法の改正**を行うもの。

サイバー脅威の深刻化

・IoT機器の急激な増加に伴い、IoT機器を踏み台とするサイバー攻撃の脅威が顕在化。

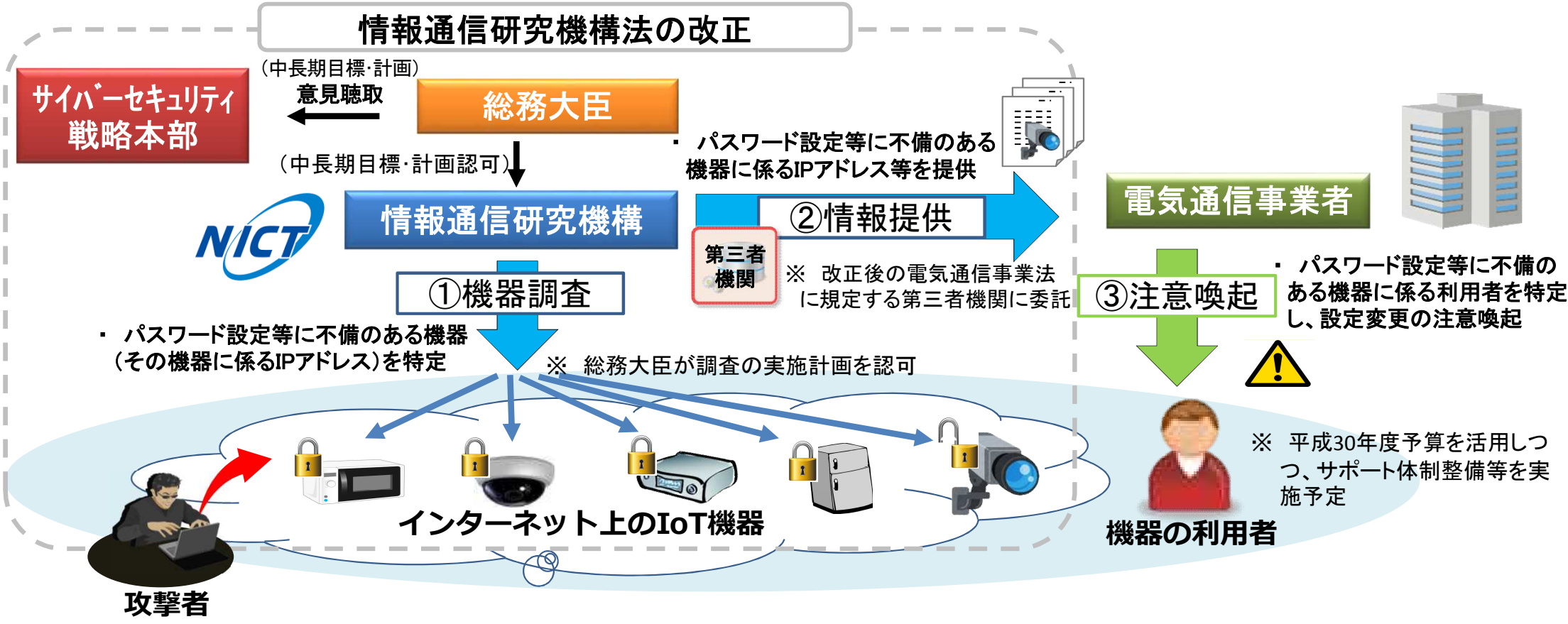
※IoT機器を狙った攻撃は全体の3分の2（2016年）

対策の必要性

・パスワード設定等に不備のあるIoT機器の実態を把握するため、調査機能の強化が急務。

体制の整備

・NICTに機器調査に係る業務を追加し、電気通信事業者と連携しつつ対策を推進（下図）。



パスワード設定等に不備のあるIoT機器の調査に係る中長期目標の変更案

- 国立研究開発法人情報通信研究機構法等の改正を踏まえ、NICTの**第4期中長期目標及び中長期計画を変更。**
- **パスワード設定等に不備のあるIoT機器の調査について、本中長期目標期間（平成28年度～32年度）に達成すべき目標を追加。**
- 本年８月中に総務大臣がNICTに目標を指示予定であり、これを踏まえNICTが計画の変更案を作成し、再度サイバーセキュリティ戦略本部に意見聴取した後、総務大臣が認可予定。

NICT第4期中長期目標（平成28年度～平成32年度）目次

主な変更箇所

「2．研究開発成果を最大化するための業務」に「（7）パスワード設定等に不備のあるIoT機器の調査」を追加。

（7）パスワード設定等に不備のあるIoT機器の調査

機構は、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（平成30年〇月〇日閣議決定）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、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。

（注1）フロンティア研究：より一層困難になる通信や情報処理における安全性確保等の課題を抜本的に解決し、豊かで安心・安全な未来社会を支えるICTの基礎となる新概念や新たな枠組みを形作ることを目指すもの。
（注2）テストベッド：新たな電気通信技術の開発・実証のための施設
（注3）オープンイノベーション：産学官連携等の幅広い連携による研究開発を行うことで新たな価値の創出に繋げるもの。

【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 National Institute of Information and Communications Technology

※NICT：National Institute of Information and Communications Technology

●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、常勤職員　423名（H30.4.1現在）

●平成30年度 予算額：281.4億円

●所在地：　本部　東京都小金井市
研究所等　神奈川県横須賀市、兵庫県神戸市、京都府相楽郡精華町(けいはんな)
大阪府吹田市、宮城県仙台市
技術センター　茨城県鹿嶋市、石川県能美市　等

●主な業務：

・情報通信分野の研究開発
- 突発的大気現象の早期補足、宇宙環境の計測・予測等を行う**センシング**(注1)**基盤分野**
- あらゆるものを繋ぐネットワーク、世界最高水準の光ファイバー網等を実現する**統合ICT基盤分野**
- 多言語での「おもてなし」、社会問題と関連する情報の発見、脳による価値判断の活用を実現する**データ利活用基盤分野**
- 次世代のサイバー攻撃分析技術でサイバー攻撃に対応する**サイバーセキュリティ分野**
- 量子光ネットワーク、新しいデバイス開発で省エネルギー社会に貢献する**フロンティア研究**(注2)**分野**

・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

・産学／地域／グローバル連携等、幅広いネットワークを活用したオープンイノベーション(注3)創出に向けた取組

・日本標準時の決定、標準電波の送信、電波の伝わり方の観測及び分析結果に基づく警報（宇宙天気予報）

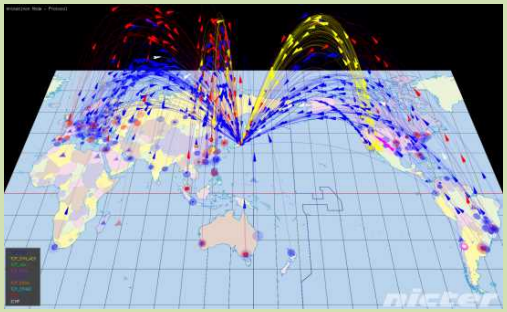
・民間、大学等が行う情報通信分野の研究開発の支援　など

（注1）センシング：電磁波を利用して人類を取り巻く様々な対象から様々な情報を取得・収集・可視化するための技術
（注2）フロンティア研究：より一層困難になる通信や情報処理における安全性確保等の課題を抜本的に解決し、豊かで安心・安全な未来社会を支えるICTの基礎となる新概念や新たな枠組みを形作ることを目指すもの。
（注3）オープンイノベーション：産学官連携等の幅広い連携による研究開発を行うことで新たな価値の創出に繋げるもの。

【参考】情報通信研究機構（NICT）におけるサイバーセキュリティ分野の研究開発

◆NICTER（ニクター）　【無差別型攻撃対策】

・ ダークネット（未使用ＩＰアドレス）への通信をセンサーで観測することで、**サイバー攻撃の地理的情報や攻撃量、攻撃手法等をリアルタイムに可視化**。
・ 本技術を応用して、地方公共団体情報システム機構（J-LIS）との協力により、**マルウェアに感染した自治体へDAEDALUSによるアラートを提供**。
・ ２０１７年11月時点で、**約600の自治体**に導入済み。



◆NIRVANA改（ニルヴァーナ・カイ）　【標的型攻撃対策】

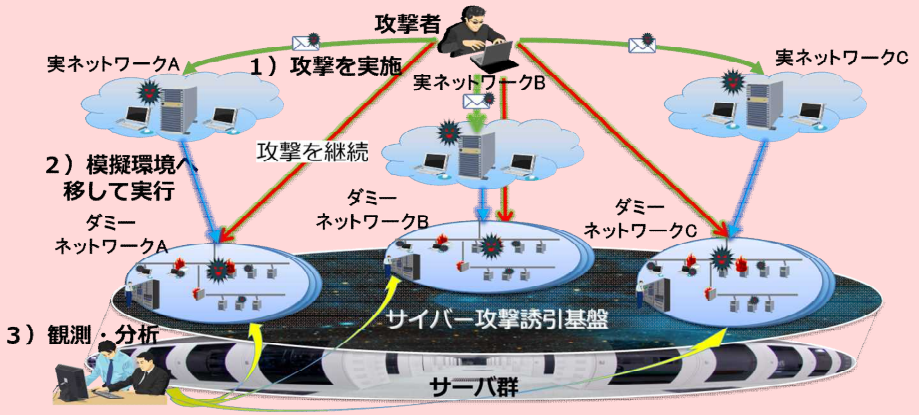
・ NICTERの技術を応用し、組織内にセンサーを設置して**組織内の通信状況をリアルタイムに可視化**するとともに、本技術について**2015年6月から技術移転開始**。
・ さらに、本技術と組み合わせ、**ネットワーク内での異常検知時に通信を自動遮断する技術**等を開発中。

◆WarpDrive（ワープドライブ）　【Web媒介型攻撃対策】

・ Web媒介型攻撃対策ソフトウェア「タチコマ・セキュリティ・エージェント（タチコマSA）」が、**Webブラウジングする際のURLやブラウザの内部挙動等のリアルタイムな収集**を行い、広大なWeb空間の観測網を構築。
・ **ユーザ群のマクロな挙動を分析し、新たな悪性Webサイトの出現など、Web空間での迅速な異常検知の実現を図る**。
・ 分析結果は大規模分析基盤からタチコマSAへ展開され、悪性Webサイトへのアクセスを自動的にブロックするとともに、ユーザに警告。

◆STARDUST（スターダスト）　【標的型攻撃対策】

・ 高度かつ複雑なサイバー攻撃に対処するため、**政府や企業等の組織を模擬したネットワークに攻撃者を誘い込み**、**攻撃者の組織侵入後の詳細な挙動をリアルタイムに把握する**ことが可能な、高度で効率的なサイバー攻撃誘引基盤（STARDUST）を構築。



国立研究開発法人情報通信研究機構第４期中長期目標変更（案） 新旧対照表（※変更部分のみ）

資料７－２

（傍線部分は改正部分）

改　　正　　案	現　　行
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）	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）
１．（略）	１．（略）
２．　政策体系における機構の位置付けと役割（ミッション）	２．　政策体系における機構の位置付けと役割（ミッション）
（略）	（略）
加えて、国立研究開発法人情報通信研究機構法及び特定通信・放送開発事業実施円滑化法の一部を改正する等の法律（平成28年法律第32号）により、サイバーセキュリティ演習その他の訓練及びIoTの実現に資する新たな電気通信技術の開発等の促進に係る業務が、電気通信事業法及び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法律（平成30年法律第24号）により、パスワード設定等に不備のあるIoT機器の調査に係る業務が機構の業務の範囲に追加された。	加えて、国立研究開発法人情報通信研究機構法及び特定通信・放送開発事業実施円滑化法の一部を改正する等の法律（平成28年法律第32号）により、サイバーセキュリティ演習その他の訓練及びIoTの実現に資する新たな電気通信技術の開発等の促進に係る業務が機構の業務の範囲に追加された。
（略）	（略）
第二に、機構の研究開発成果を最大化するためには、研究開発業務の成果を実用化や標準化、社会実装等に導くための取組が不可欠であることから、社会経済全体のイノベーションの積極的創出につなげるため、テストベッド構築や産学官連携等の強化、標準化活動の推進、国際展開の強化、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機器の調査等に取り組むこと。	第二に、機構の研究開発成果を最大化するためには、研究開発業務の成果を実用化や標準化、社会実装等に導くための取組が不可欠であることから、社会経済全体のイノベーションの積極的創出につなげるため、テストベッド構築や産学官連携等の強化、標準化活動の推進、国際展開の強化、サイバーセキュリティに関する演習等に取り組むこと。
（略）	（略）
Ⅱ　（略）	Ⅱ　（略）

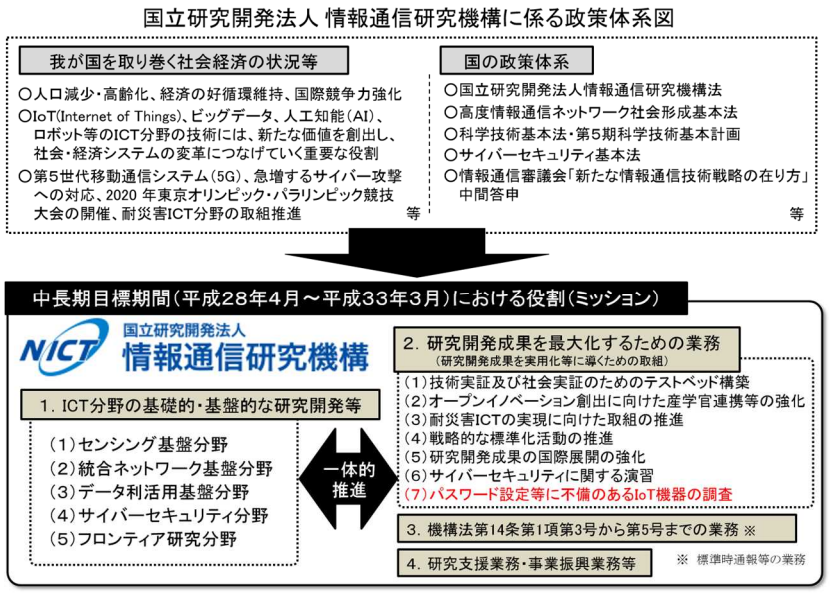
Ⅲ．　研究開発の成果の最大化その他の業務の質の向上に関する事項	Ⅲ．　研究開発の成果の最大化その他の業務の質の向上に関する事項
１．　（略）	１．　（略）
２．研究開発成果を最大化するための業務	２．研究開発成果を最大化するための業務
（１）　（略）	（１）技術実証及び社会実証のためのテストベッド構築 （略）
（２）　（略）	（２）オープンイノベーション創出に向けた産学官連携等の強化 （略）
（３）　（略）	（３）耐災害ＩＣＴの実現に向けた取組の推進 （略）
（４）　（略）	（４）戦略的な標準化活動の推進 （略）
（５）　（略）	（５）研究開発成果の国際展開の強化 （略）
（６）　（略）	（６）サイバーセキュリティに関する演習 （略）
（７）パスワード設定等に不備のあるIoT機器の調査 機構は、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（平成30年〇月〇日閣議決定）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、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。	

３・４　（略）

Ⅳ～Ⅵ　（略）

別紙１

国立研究開発法人情報通信研究機構に係る政策体系図



別紙２

国立研究開発法人情報通信研究機構の評価軸等

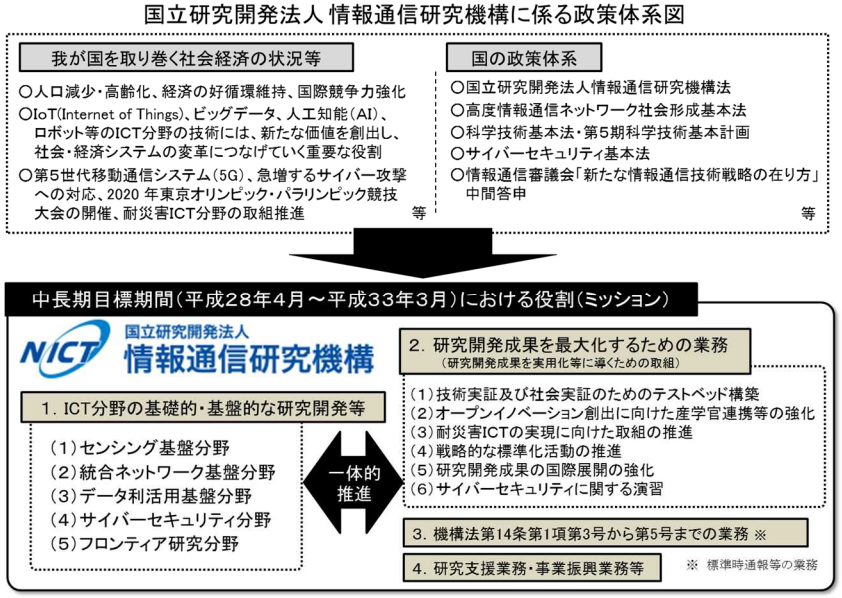
項目	評価軸	指標
１．　（略）	（略）	（略）
２．研究開発成果を最大化するための業務	●ハイレベルな研究開発を行うためのテストベッドが構築されているか。	●研究開発成果を最大化するための取組成果（評価指標）

３・４　（略）

Ⅳ～Ⅵ　（略）

別紙１

国立研究開発法人情報通信研究機構に係る政策体系図



別紙２

国立研究開発法人情報通信研究機構の評価軸等

項目	評価軸	指標
１．　（略）	（略）	（略）
２．研究開発成果を最大化するための業務	●ハイレベルな研究開発を行うためのテストベッドが構築されているか。	●研究開発成果を最大化するための取組成果（評価指標）

	●機構内外の利用者にとりテストベッドが有益な技術実証・社会実証につながっているか。 ●取組がオープンイノベーション創出につながっているか。 ●取組が耐災害ＩＣＴ分野の産学官連携につながっているか。 ●取組が標準化につながっているか。 ●取組が研究開発成果の国際的普及や日本企業の国際競争力強化につながっているか。 ●取組が最新のサイバー攻撃に対応できるものとして適切に実施されたか。 ●取組が 機器のサイバーセキュリティ対策の一環として計画に従って着実に実施されたか。	●機構内外によるテストベッドの利用結果（評価指標） ●機構内外によるテストベッドの利用件数（モニタリング指標） ●産学官連携等の活動状況（評価指標） ●標準や国内制度の成立寄与状況（評価指標） ●標準化や国内制度化の寄与件数（モニタリング指標） ●国際展開の活動状況（評価指標） ●演習の実施回数又は参加人数（モニタリング指標） ●調査したIoT機器数（モニタリング指標） ●IoT機器調査に関する業務の実施状況（評価指標） 等
３．　（略）	（略）	（略）

	●機構内外の利用者にとりテストベッドが有益な技術実証・社会実証につながっているか。 ●取組がオープンイノベーション創出につながっているか。 ●取組が耐災害ＩＣＴ分野の産学官連携につながっているか。 ●取組が標準化につながっているか。 ●取組が研究開発成果の国際的普及や日本企業の国際競争力強化につながっているか。 ●取組が最新のサイバー攻撃に対応できるものとして適切に実施されたか。	●機構内外によるテストベッドの利用結果（評価指標） ●機構内外によるテストベッドの利用件数（モニタリング指標） ●産学官連携等の活動状況（評価指標） ●標準や国内制度の成立寄与状況（評価指標） ●標準化や国内制度化の寄与件数（モニタリング指標） ●国際展開の活動状況（評価指標） ●演習の実施回数又は参加人数（モニタリング指標） 等
３．　（略）	（略）	（略）

資料７－３

国立研究開発法人情報通信研究機構の中長期目標の改正案に対する サイバーセキュリティ戦略本部の意見（案）

年　月　日
サイバーセキュリティ戦略本部決定

サイバー空間と実空間の一体化が進展する中、AI や IoT などの技術・サービスが人々に多くの恩恵をもたらす可能性がある一方で、こうした技術・サービスが制御できなければ新たな脅威を生むおそれが常に内在している。また、IoT 機器が攻撃等により意図しない作動をし、様々な業務・機能・サービスに障害が生じた場合、国民の安全・安心を脅かす事態が生じるおそれもある。

こうした脅威に対応し、サイバーセキュリティ対策の抜本的な強化を図るため、サイバーセキュリティ基本法（平成 26 年法律第 104 号）第 25 条第１項第１号に基づき作成した案（平成 30 年７月〇日サイバーセキュリティ戦略本部決定）を踏まえ、同法第 12 条第５項において準用する同条第３項の規定に基づき、閣議決定予定のサイバーセキュリティ戦略（以下「戦略」という。）における重要な観点の一つである「参加・連携・協働」、すなわち、情報共有や個人と組織間の相互連携・協働を含む、各々が平時から講じる基本的な取組が重要である。電気通信事業法及び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法律（平成 30 年法律第 24 号）により、国立研究開発法人情報通信研究機構（以下「NICT」という。）が行うこととされた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（以下「調査」という。）に関する業務については、平時から講じる基本的な取組を促進するにあたって重要な役割を果たすものである。

その実施に当たっては、戦略を踏まえ、安全な IoT システムの構築に向けて、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とともに、「未来投資戦略 2018」（平成 30 年６月 15 日閣議決定）を踏まえ、データの高度利活用・流通の促進に寄与することが求められる。

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中長期目標の改正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、平成 32 年（2020 年）東京オリンピック・パラリンピ

ック競技大会も見据え、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、パスワード設定等に不備のある機器に係る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、適時に見直しが行われること

② 調査の実施にあたっては、調査に関して十分な周知を行うとともに、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の必要性について周知活動を行うこと

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、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。）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に努めること

(2) 改正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) 戦略等について、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、中長期目標の改正等の必要な措置を講じること

以上