資料１

国立研究開発法人情報通信研究機構の第6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)について

令和8年3月

国立研究開発法人情報通信研究機構の第６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（戦略本部）の意見を聴かなければならない。
- 本年２月27日に総務大臣がNICTの第６期中長期目標（目標期間：令和８～１２年度）を定め、NICTに指示したことを踏まえ、同年３月２日にNICTが総務大臣に中長期計画の認可申請を実施。
- 今般、NICTの第６期中長期計画を総務大臣が認可するにあたり、NICT法の規定に基づき、戦略本部に対して意見の求めがあった。

第６期中長期計画（案）の概要

- NICTの研究開発等の成果の普及展開業務のうち以下のものについて、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**
国の機関や地方公共団体、基幹インフラ事業者等の対処能力向上に貢献するため、最新のサイバー攻撃状況を踏まえた実践的な演習を実施
演習の実施に当たっては、全ての国の機関、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等についても、より多くの受講機会を確保できるよう配慮
（NICT法第14条第1項第7号イの業務：CYDER関連）

② **IoT機器のサイバーセキュリティ対策の促進**
IoT機器の対策に貢献するため、脆弱性を有する機器等の調査、ユーザやメーカー等に対する助言等（調査等）を実施
（NICT法第14条第1項第7号ロの業務：NOTICE関連）

戦略本部の意見（案）の概要

- 計画案は、**新たなサイバーセキュリティ戦略の内容を踏まえており、**戦略本部として**妥当な内容と判断。**
（戦略の主な関連記述）
  - 政府機関等だけでなく、重要インフラ事業者や地方公共団体等に向けた対処能力向上に資する実践的な演習の提供によるサイバー人材の育成・確保
  - IoT機器について各主体が適切な対策を講じられるよう、ユーザーやベンダーに対し助言等を行い、関係者が一丸となってサイバーセキュリティの確保に取り組む

- また、演習及び調査等に関する事項のほか、以下の旨が記載。戦略を踏まえており適当。
  - サイバー対処能力強化法※に基づく**サイバー攻撃の観測・分析等の観点**からの**関係者との連絡・協力**
  - サイバーセキュリティ基本法等に基づく**委託業務の確実な実施**
  - 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処能力を支える人材・技術に係るエコシステム形成に貢献**

※　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

国立研究開発法人 情報通信研究機構（NICT） 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**

NICT: **N**ational **I**nstitute of Information and **C**ommunications **T**echnology

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1,547名　（令和7年4月 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

- **情報通信分野の重要な研究開発**等に加え、**我が国の社会経済活動に必須な業務**（日本標準時の提供、標準電波の発射、宇宙天気予報等）を実施。
- NICTに**情報通信研究開発基金を設置し**、民間・大学等による**研究開発等を支援**。
- 本年度は第５期中長期目標期間（R3～R7）の最終年度。国立研究開発法人審議会等の意見も踏まえ、**第６期中長期目標（R8～R12）を策定**。

NICT運営費交付金等【令和８年度予算案】301.0億円
【令和７年度当初】　300.5億円

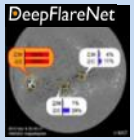
電磁波先進技術

・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

・宇宙環境
宇宙環境の監視・予測技術の高度化

・時空標準
高精度な原子時計の開発


フェーズドアレイ気象レーダ



Deep Flare Net

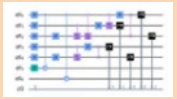

日本標準時システム

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

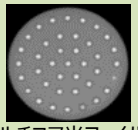

NICTER

・暗号技術
耐量子計算機暗号（PQC）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

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

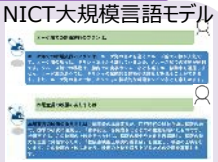

NTN（非地上系ネットワーク）

ユニバーサルコミュニケーション

・AI研究基盤
日本語を中心とした高品質・大規模データベース

・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

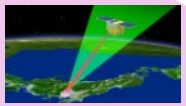
・社会知コミュニケーション
利用者の興味や背景、文脈に応じた対話


NICT大規模言語モデル


NICT提供スマホアプリ（ボイストラ）

フロンティアサイエンス

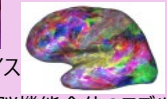
・量子情報通信
量子鍵配送（QKD）技術の国際標準化及び世界最高速の量子光源


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モデル化・拡張


脳機能全体のモデル化

分野横断的な研究開発等

・Beyond 5Gの推進
民間企業等の研究開発・標準化活動への支援
先端技術に関する自主研究の実施　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ICT人材　等

・研究支援・事業振興業務
海外研究者の招へい　等

・GPAI東京専門家支援センター

サイバーセキュリティに関する演習（CYDER：CYber Defense Exercise with Recurrence）

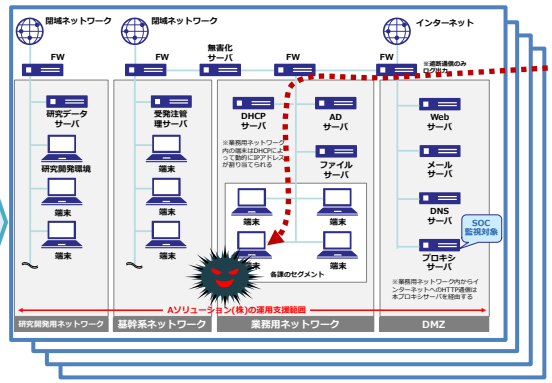
- 総務省は、平成29年度から、NICTにおいて、**国の機関**、**指定法人**、**独立行政法人**、**地方公共団体**及び**重要インフラ事業者等**の情報システム担当者等を対象とした体験型の**実践的サイバー防御演習**(**CYDER**)を実施。
- 受講者は、**チーム単位で演習に参加。組織のネットワーク環境を模した大規模仮想LAN環境下で、実機の操作を伴って、**外部のセキュリティ事業者の支援を受けることを前提としてサイバー攻撃によるインシデントの検知から対応、報告、回復までの**一連の対処方法を体験。**
- **全都道府県**において、年間**100回・計3,000名規模**で実施(集合コース)。令和６年度は106回・**4,225名**が受講。

※ H29年度:100回・3,009名、H30年度:107回・2,666名、R元年度:105回・3,090名、R2年度:106回・2,648名、R3年度: 105回・2,454名、R4年度: 108回・3,327名、 R5年度: 110回・3,742名、R6年度: 106回・4,225人

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**

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７年度の実施状況

コース名		実施方法	レベル	受講想定者（習得内容）	受講想定組織	実施地	実施回数	実施期間
CYDER	A	集合形式	初級	システムに携わり始めた者 (事案発生時の対応の流れ)	全組織共通	４７都道府県	７８回	７月～翌年１月
	B-1		中級	システム管理者・運用者 (主体的な事案対応・ｾｷｭﾘﾃｨ管理)	地方公共団体	全国８地域	１０回	10月～11月
	B-2				地方公共団体以外	東京・大阪・名古屋	１３回	翌年１月
	C		準上級	セキュリティ専門担当者 (初動分析を含む主体的な事案対応)	全組織共通	東京・大阪	５回	11月～翌年１月
プレCYDER		オンライン形式	-	全ての情報システム担当者 (最低限必要となる知識の習得と最新化)	全組織共通	(受講者職場等)	-	1期：５月～８月 2期：９月～11月 3期：11月～翌年１月

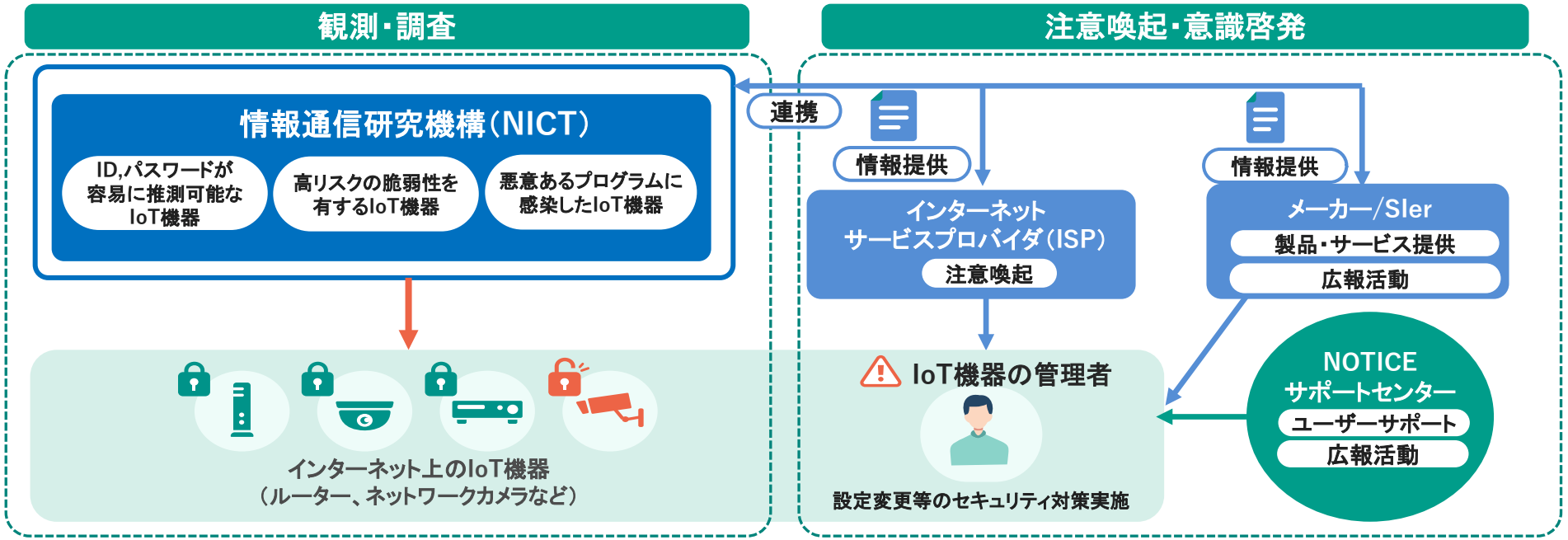
IoT機器のサイバーセキュリティ対策の促進（NOTICEプロジェクト）

NOTICE: National Operation Towards Iot Clean Environment

みんなで守る、IoT。 NOTiCE

サイバー攻撃のトレンドに対応するため、令和５年度NICT法改正により**連携組織**や調査対象となる**脆弱性の種類**を拡大

- NICTがインターネットを観測・調査し、**悪意あるプログラム（マルウェア）に感染した踏み台IoT機器や、今後感染する危険性が高い脆弱なIoT機器を発見**
- 電気通信事業者（ISP）やIoT機器メーカー等と連携し、当該機器等の**管理者に注意喚起・意識啓発**を行い対応を促すことで、**IoTボットネットによるサイバー攻撃（DDoS攻撃）の発生と被害を軽減**



令和7年11月の結果

IoT機器観測総数	マルウェアに感染したIoT機器検知数	高リスク脆弱性を有するIoT機器	ID, パスワードが容易に推測可能なIoT機器
月 1.17 億件	最大 424 件/日	月 2,592 件	月 14,002 件

（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）

（業務の範囲）

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］

七　第一号に掲げる業務に係る成果の普及として、次の業務を行うこと。

イ　サイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。ロにおいて同じ。）に関する**演習その他の訓練を行うこと**。　→ **サイバーセキュリティに関する演習（CYDER）**

ロ　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電気通信設備の管理者その他の関係者に対して**必要な助言及び情報の提供を行うこと**。　→ **IoT機器のサイバーセキュリティ対策の促進（NOTICE）**

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］

十四　前各号に掲げる業務に附帯する業務を行うこと。

2　［略］

3　機構は、前二項の業務のほか、サイバーセキュリティ基本法第三十一条第一項（第二号に係る部分に限る。）の規定による事務を行う。

（中長期目標等に関するサイバーセキュリティ戦略本部の意見の聴取）

第二十一条　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。**