資料26－5

令和３年度総務省サイバーセキュリティ関連予算概算要求について

令和２年10月

サイバーセキュリティタスクフォース事務局

令和3年度概算要求の状況（主要なサイバーセキュリティ関連予算（抜粋））

事業	令和２年度 予算額（円）	令和３年度 概算要求額（円）
サイバーセキュリティ統合知的・人材育成基盤の構築	**－**	**20.0億**
ナショナルサイバートレーニングセンターの強化	**15.0億**	**15.0億**
IoTの安心・安全かつ適正な利用環境の構築	**14.6億**の内数	**12.8億**の内数
サイバーセキュリティ情報共有推進事業	**3.6億**	**3.6億**
安全な無線通信サービスのための新世代暗号技術に関する研究開発	**－**	**132.2億**の内数
電波の有効利用のためのIoTマルウェア無害化/無機能化技術等に関する研究開発	**103.4億**の内数	**132.2億**の内数

サイバーセキュリティ統合知的・人材育成基盤の構築

■ サイバーセキュリティ情報を国内で収集・蓄積・分析・提供するとともに、社会全体でサイバーセキュリティ人材を育成するための共通基盤を情報通信研究機構（NICT）に構築し、産学の結節点として開放することで、サイバーセキュリティ対応能力の向上を図る。

（新規）【R３要求額：20.0億円】

STARDUST
サイバー攻撃誘因基盤

NICTER
サイバー攻撃観測網

各種外部情報

CYDER
実践的サイバー防御演習

サイバーコロッセオ
オリパラ関係者向けサイバー演習

民間が有する各種演習教材

成果展開

成果展開

教材変換インタフェースの開発・標準化

サイバー攻撃分析環境

情報

大規模集約データベース

情報

セキュリティ機器テスト環境

最新の攻撃情報（演習教材に反映）

相互補完

受講者の挙動（攻撃分析に活用）

演習教材提供環境

演習用大規模計算機環境

受講者挙動DB

AIを駆使した大規模横断分析＋付加価値の付与

根拠・背景等が
説明可能な国産セキュリティ情報

提供

政府機関・セキュリティ機関等

- マルウェア情報
- 指令サーバ情報
- 攻撃元IPアドレス情報
- 攻撃者/攻撃手法情報 等

コミュニティ形成による連携

人材育成事業者　教育機関　ICTベンダ

ナショナルサイバートレーニングセンターの強化

■ 巧妙化・複雑化するサイバー攻撃に対し、実践的な対処能力を持つセキュリティ人材を育成するため、平成29年4月より、情報通信研究機構（ＮＩＣＴ）の「ナショナルサイバートレーニングセンター」において演習等を実施。
※国立研究開発法人情報通信研究機構法の一部改正（平成28年法律第32号）により、NICTの業務として「サイバーセキュリティに関する演習その他の訓練を行うこと」が追加されたことに伴い、NICTにおいて実施しているもの。 【Ｒ３要求額：15.0億円】

CYDER Cyber Defense Exercise with Recurrence（サイダー）

国・地方公共団体・独法・重要インフラ事業者等を対象とした実践的サイバー防御演習

⇒ **年間100回**（全都道府県）、**計3,000名規模**で実施（元年度は延べ3,090名が受講）
令和３年度から**オンライン受講を本格開始**／高度な攻撃に対処可能な**攻防型演習を導入**

cyber colosseo（サイバーコロッセオ）

2020年東京大会関連組織のセキュリティ担当者等を対象とした実践的サイバー演習

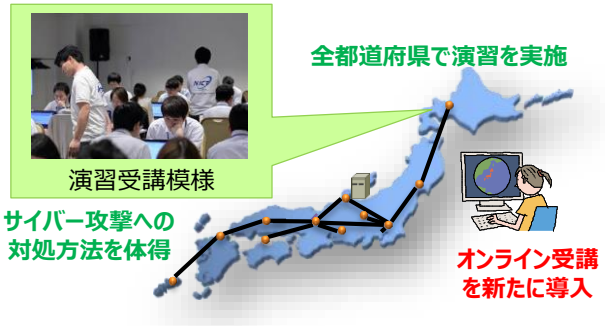
⇒ **令和元年度**は延べ**193名**が受講
令和２年度でセキュリティ担当者の育成を完了（令和３年度要求はなし。）

SecHack365（セックハック365）

25歳以下の若手セキュリティ人材の育成

⇒ **年間50名程度**の受講者を選定し、**１年間のトレーニング**コースを実施（元年度は45名が修了）
令和３年度も継続的に実施予定

新たな手法のサイバー攻撃にも対応できる演習プログラム・教育コンテンツを開発



実事案に対処可能な人材育成
CYDER

高度な攻撃に対処可能な人材育成
サイバーコロッセオ

ハイレベル層の人材育成
SecHack365

IoTの安心・安全かつ適正な利用環境の構築

■ 電波を用いるIoT機器が急増しサイバー攻撃の脅威も増大しているため、IoTに係るセキュリティ対策の強化や適正な利用環境の構築に向けたリテラシーの向上を図ることで、国民生活や社会経済活動の安心・安全の確保等を実現する。

■ 令和３年度は、現行計画に従って取組を継続。５Ｇネットワークのセキュリティ確保については、２年度までに構築した仮想環境を統合するとともに、サプライチェーンリスク対策のためのハードウェア脆弱性の検証対象を拡大。　【Ｒ３要求額：12.8億円の内数】

① IoTセキュリティ対策の推進

国内のインターネットに接続されたIoT機器を調査しサイバー攻撃に悪用されうる脆弱なIoT機器の利用者に注意喚起を行うプロジェクト「NOTICE」を実施する。（イメージ図左）

② 5Gネットワークのセキュリティ確保に向けた体制整備と周知・啓発

我が国の次世代の通信を担う基盤である5G（第5世代移動通信システム）について、ソフトウェア及びハードウェア両面の技術的検証を通じ、各構成要素におけるサプライチェーンリスク対策を含むセキュリティを、総合的かつ継続的に担保する仕組みを整備する。（イメージ図右）

③ 地域におけるIoTセキュリティ対策の強化

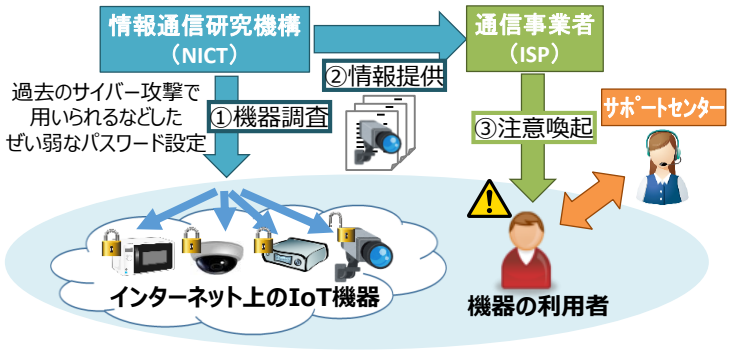
地域のコミュニティや企業、教育機関等と連携して、IoTセキュリティに関して活躍可能な人材を自立的に育成していくためのエコシステムの確立に向けた実証を行う。

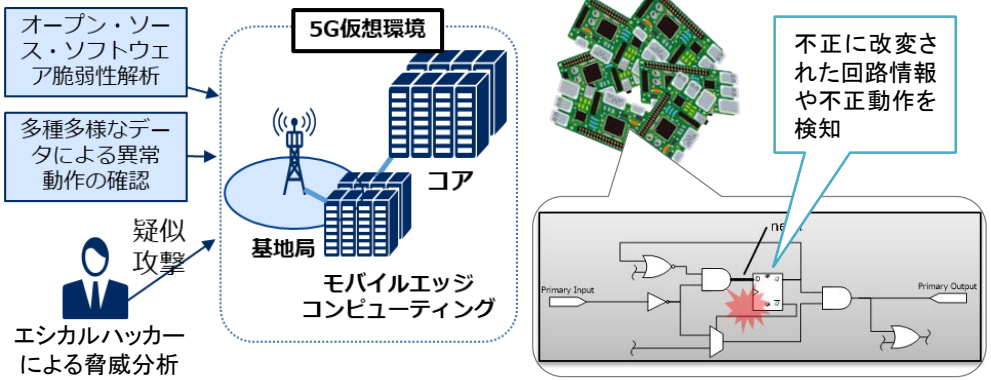
④ 無線LANのセキュリティ対策の強化

無線LANを安心・安全に利用するため、利用者・提供者双方におけるセキュリティ対策状況調査やガイドライン策定を行うとともに、周知・啓発活動を推進する。

⑤ IPv6導入のためのガイドライン等策定

IPv6導入のボトルネックとなっているシステム・アプリケーション側のIPv6化を推進するため、特にIPv6化の知見が不足している大学・中小企業等の情報システムのIPv6化に係る調査・実証を通じて導入ガイドライン等を策定し、IPv6化の環境整備を推進する。





サイバーセキュリティ情報共有推進事業

①重要インフラ事業者等がサイバー攻撃情報を共有するための情報共有基盤において、脆弱性情報を新たな共有対象とするとともに、ソフトウェア資産情報と組み合わせることで、迅速かつ効果的な対処を実現
②日々公開される多種多様な脆弱性情報について、AIを活用した高精度な深刻度・信頼度評価を行い、結果を情報共有基盤で共有することにより、迅速かつ効果的な対処を実現
③総合通信局を中心として所管事業者等との情報共有等を実施する体制を構築

【R３要求額：359百万円】

【これまでの取組・現状】

○平成29年度までは、情報共有の取組の推進を支援するため、情報共有基盤による機械処理可能な形式で攻撃者情報を共有する実証事業を実施。

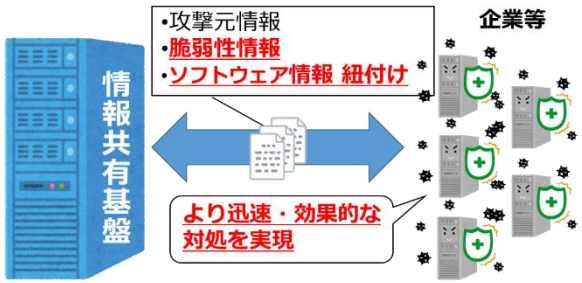
○令和元年度及び２年度は、①情報共有基盤を高度化し、攻撃者情報だけでなく、脆弱性情報とその影響を受けるソフトウェアの情報を共有する実証、②機械学習（AI）を活用し、多種多様な脆弱性情報の深刻度・信頼度を評価する技術の実証、及び①、②の連携のための検証を実施するとともに、③総合通信局を中心とした地域における情報共有体制の確立に向けた取組を実施。

【目標・成果イメージ】

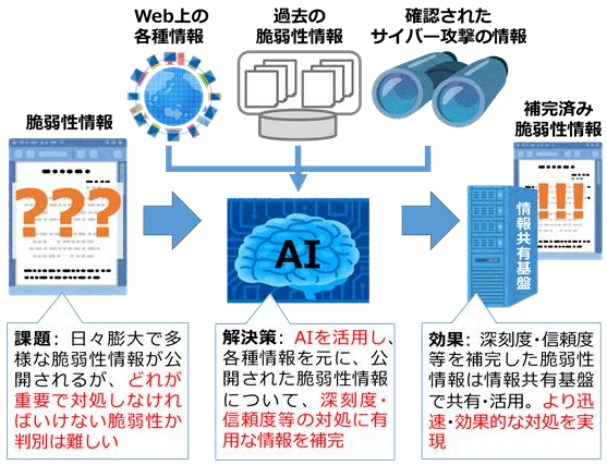
○以下により、サイバー攻撃による被害の甚大化を防ぎ、情報通信インフラをはじめとする我が国社会・経済の強靭性を向上させる。
- 通信事業者や放送事業者をはじめとする産業界における関係者間の情報共有促進によるサイバーセキュリティ対策の強化
- 総合通信局を中心とした地域の情報共有体制の構築

①情報共有基盤の高度化

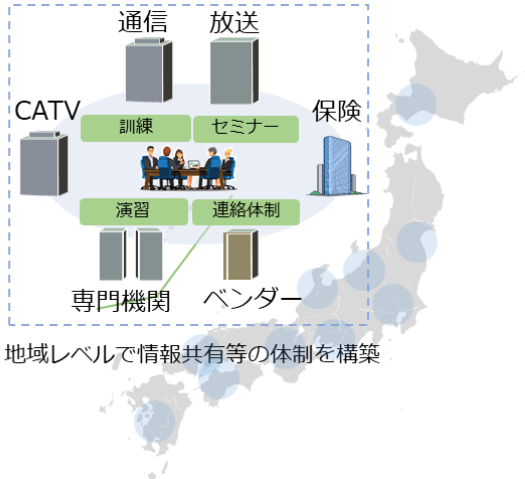
	既存	高度化
攻撃元情報	○	○
脆弱性情報	×	○＋評価
ソフトウェア情報 紐付け	×	○



②深刻度・信頼度評価の高精度化



③総通局を中心とした情報共有体制



地域レベルで情報共有等の体制を構築

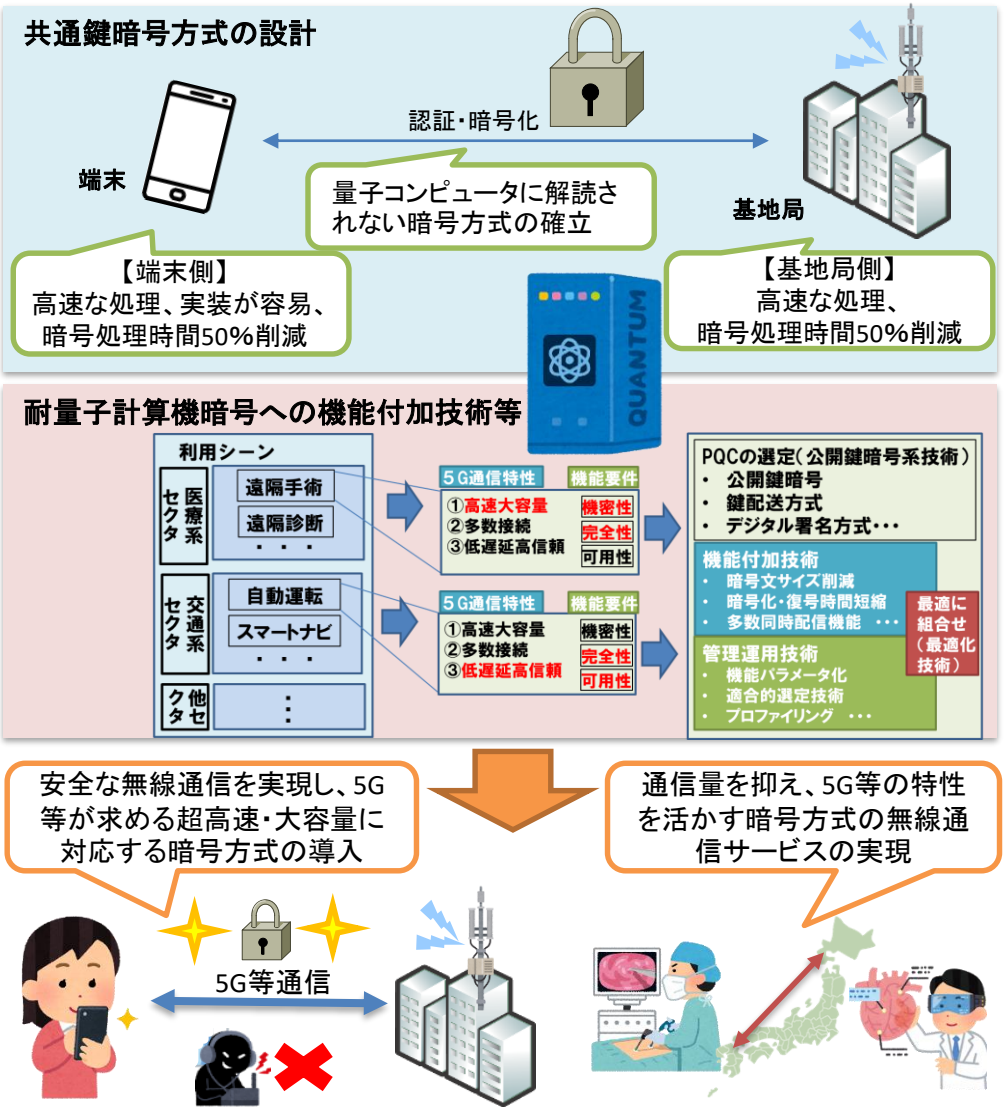
安全な無線通信サービスのための新世代暗号技術に関する研究開発

■ 5G等の高度化において、大規模量子コンピュータ等に解読されないよう、①ＬＴＥと同等の安全性を確保しつつ、超高速・大容量に対応した共通鍵暗号方式、②5G等の特性を損なわないよう、5G等のユースケースに応じた耐量子計算機暗号（PQC）への機能付加技術等を確立することで、無線通信リソースの効率的な利用環境を提供することにより、無線リソースのひっ迫を抑止し電波の有効利用を図る。

【背景・課題】
・大規模量子コンピュータ等が実用化されると、共通鍵暗号方式においては、ＬＴＥと同等の安全性を確保するためには鍵長を増加する必要があるが、スマートフォン等の限られた情報処理能力の中で5G等が求める高速・大容量に対応した暗号方式の設計が課題である。
・また、公開鍵暗号方式においては、高速な解読が可能となるため、PQCへの移行が必要である。今後、複数の暗号方式が採用される予定であるが、5G等のユースケースに応じて最適化し、スマートフォン等の計算資源や通信量を抑えるようにPQCへの機能付加等が必要である。

【実施内容】
大規模量子コンピュータ等に解読されないよう、①ＬＴＥと同等の安全性を確保するために鍵長を倍にしつつ、超高速・大容量に対応できる共通鍵暗号方式、②5G等のユースケースに応じ、通信データ量を抑え、PQCへの機能付加技術等を確立し、無線通信の効率的な利用環境を提供することにより、電波の有効利用を図る。

目標	超高速・大容量に対応する共通鍵暗号方式及びPQCへの機能付加技術等を令和６年までに開発するとともに、ISOや3GPP等の標準化団体に提案し、標準化策定に寄与することを目指す。
対象周波数帯	5G等のバンド：3.6GHz～4.6GHz、27.00GHz～29.50GHz、100GHz超の高い周波数帯
実施期間	令和３年度～令和６年度　（４カ年）
令和３年度要求額	132.2億円の内数

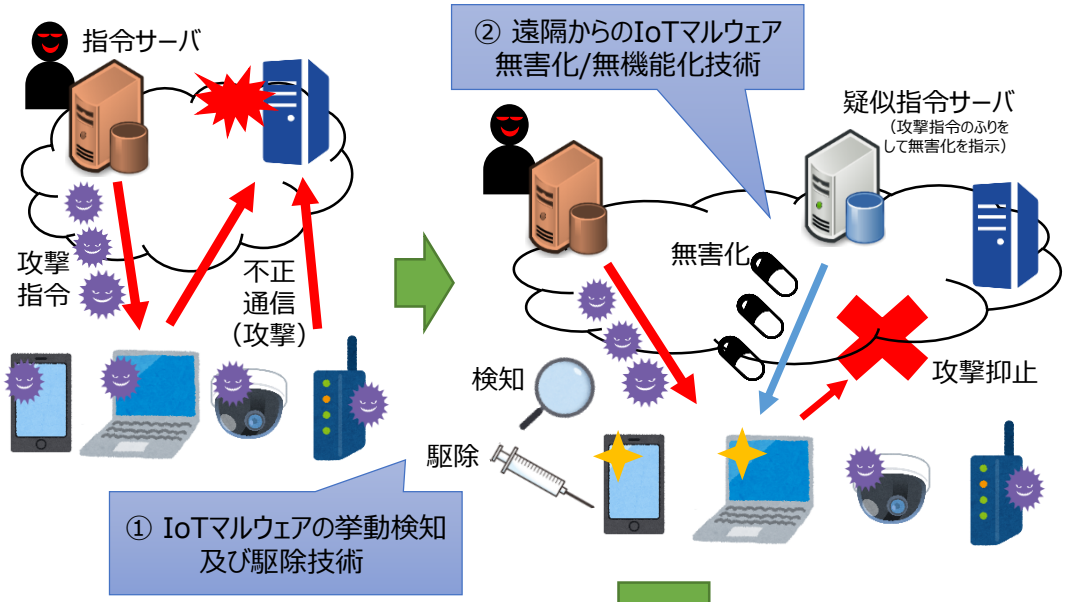


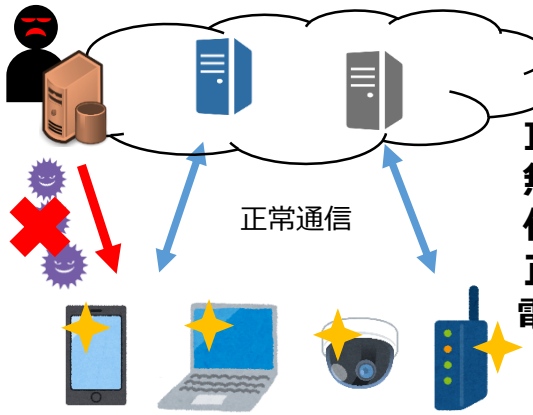
電波の有効利用のためのIoTマルウェア無害化/無機能化技術等に関する研究開発

■ IoTの普及により、無線ネットワークに接続されるIoT機器が急速に増加している。これらがマルウェアに感染すると、大量の不正通信を発生させ、無線リソースをひっ迫させるおそれがある。そのため、マルウェアに起因する不正な無線通信を抑止することを目的として、IoT機器に感染するマルウェアを無害化/無機能化する技術等を研究開発し、電波の有効利用を図る。

【背景・課題】
- 近年、センサーなどのIoT機器が急速に増加しており、これらがマルウェアに感染すると無線ネットワークに大量の不要な電波を発生させることから、無線リソースのひっ迫が懸念される。
- 多くのIoT機器は、メモリー等のリソースの制約等により十分なセキュリティ対策が行われないまま運用されている中、マルウェアに感染したIoT機器による不要な電波の発射を抑止することが喫緊の課題となっている。

【実施内容】
マルウェアに感染した不要な無線通信を抑止するため、①IoTマルウェアの挙動検知及び駆除技術、②遠隔からのIoTマルウェア無害化及び無機能化技術の研究開発を実施する。令和３年度は、令和２年度に設計・開発した基本方式やプロトタイプに関し、改良及び評価・機能改善を行う。





IoTマルウェアを無害化/無機能化することで、不正通信を抑止し電波の有効利用を実現

目標	マルウェアの攻撃挙動の解析を自動化し早期警戒情報として導出する技術、IoT機器に感染したマルウェアを無害化/無機能化する技術を令和４年度までに開発し、令和５年度までの実用化を目指す。マルウェアに感染したIoT機器からの不要な電波を抑止し、無線リソースひっ迫を低減することで、電波の有効活用を図る。
対象周波数帯	IoT機器の通信として利用される無線システムの周波数帯 （700MHz/800MHz帯、900MHz帯、920MHz帯、1.5MHz帯、1.7MHz帯、2GHz帯、2.3GHz帯、2.4GHz帯、2.5GHz帯、2.6GHz帯、3.4GHz帯、4GHz帯、4.5GHz帯、5GHz帯）
実施期間	令和２年度～令和４年度　（３カ年）
令和３年度要求額	132.2億円の内数