参考資料３

令和２年度総務省サイバーセキュリティ関係予算概算要求について

サイバーセキュリティタスクフォース事務局

令和元年 11月1日

令和2年度概算要求の状況（サイバーセキュリティ関連一部抜粋）

分類	事業（括弧内は実施内容）	令和元年度 予算額（円）	令和２年度 概算要求額（円）
IoT・５Ｇ	IoTの安心・安全かつ適正な利用環境の構築	**14.6億**の内数	**16.6億**の内数
人材育成	ナショナルサイバートレーニングセンターの構築	**14.9億**	**15.0億**
情報共有	サイバーセキュリティ情報共有推進事業	**3.4億**	**3.6億**
国際	諸外国におけるサイバーセキュリティ動向の調査研究	**0.5億**	**1.2億**の内数
トラスト	トラストサービスの制度化に係る調査研究	**－**	**1.2億**の内数
	電子署名の普及啓発等	**0.1億**	**1.2億**の内数
R&D	周波数有効利用のためのIoTワイヤレス高効率広域ネットワークスキャン技術の研究開発	**100.4億**の内数	**125.9億**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	**－**	**125.9億**の内数

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２年度は、令和元年度の取組を継続的に実施。5Gネットワークのセキュリティ確保については、元年度に構築を開始した仮想環境を拡充すると共に、サプライチェーンリスク対策のためのハードウェアの脆弱性の検証に取り組む。

当初予算額 （億円）

H30年度	R1年度	R2年度要求
–	14.6	16.6

① IoTセキュリティ対策の推進【455百万円】

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【735百万円】

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、サプライチェーン対策を含め、各構成要素におけるセキュリ ティを、総合的かつ継続的に担保する仕組みを整備する。（イメージ図中央）

③ 地域におけるIoTセキュリティ対策の強化【216百万円】

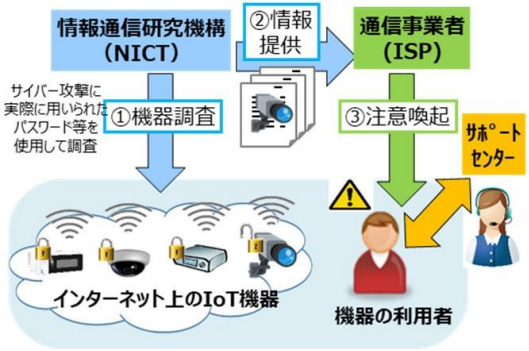
地域におけるセキュリティ対策強化のため、（ア）地域のIoTシステムのセキュリティ要件等のガイドライン化、（イ）地域のIoTセキュリティ人材を育成するための取組、及び（ウ）公衆無線LANのセキュリティ対策に関する周知啓発等を実施する。（イメージ図右）

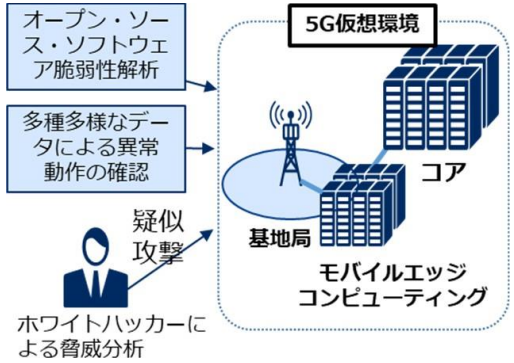
④ IoT利用環境の適正な運用及び整備等に資するガイドライン等策定【154百万円】

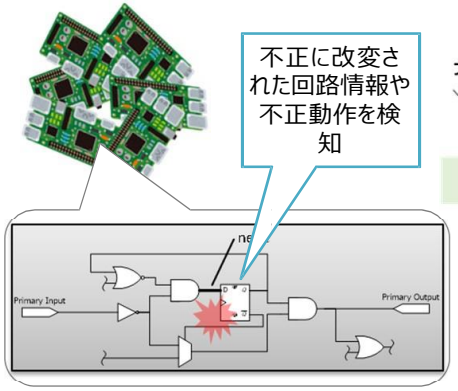
IoTサービスの適正な運用、整備等のため、多様な電波伝搬状況における電波の適正な利用に係るガイドライン等の策定を実施する。

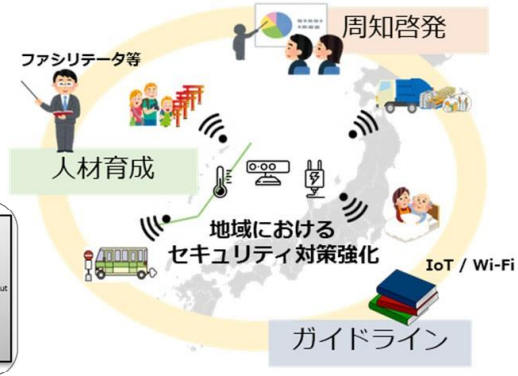
⑤ IPv6導入のためのガイドライン等策定【98百万円】

IoT機器の急増も背景にIPv4アドレスの枯渇が見込まれる中、IPv6化の推進の必要があり、大学・地方公共団体等の情報システムのIPv6化を促進するための調査・実証を通じてガイドライン等を作成し、IPv6導入のボトルネック解消に向けた環境整備を推進する。









ナショナルサイバートレーニングセンター

■ 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年度より、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。

【R２要求額：1,500百万円】

CYDER（サイダー）

国の行政機関・地公体・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、3,000名規模で実施（１日コース＆全都道府県で開催） 【1,156百万円】
令和２年度からは、攻防型の準上級コースを新設するとともにオンライン受講を開始予定

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

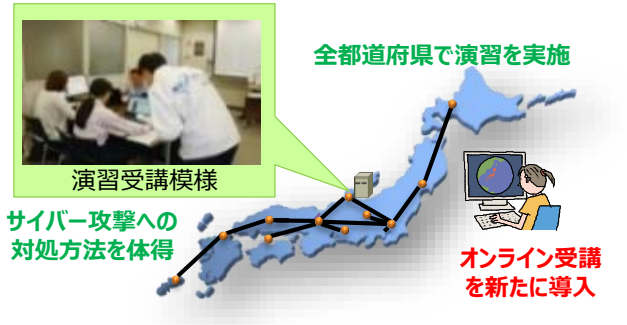
⇒ 平成29年度は延べ74名、平成30年度は延べ137名が受講 【173百万円】
今年度は最大400名規模で実施予定（令和２年度も大会直前まで実施予定）

SecHack365（セックハック365）

25歳以下の若手セキュリティイノベーターの育成

【157百万円】

⇒ 平成29年度は39名、平成30年度は46名が1年間のコースを修了
今年度は46名を受講者として選定し、令和２年度も50名程度を育成予定



実事案に対処可能な人材育成
CYDER

攻防側コースを新設
ノウハウを活用

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

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

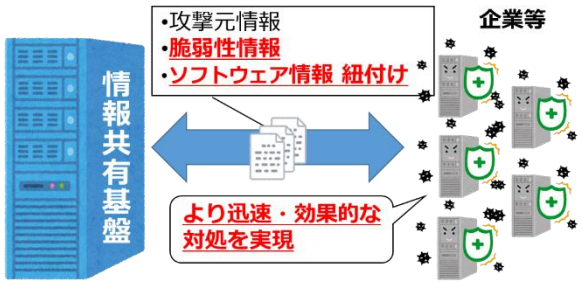
【これまでの取組・現状】
○平成29年度までは、情報共有の取組の推進を支援するため、情報共有基盤による機械処理可能な形式で攻撃者情報を共有する実証事業を実施。
○令和元年度は、①情報共有基盤を高度化し、攻撃者情報だけでなく、脆弱性情報とその影響を受けるソフトウェアの情報を共有する実証、②機械学習（AI）を活用し、多種多様な脆弱性情報の深刻度・信頼度を評価する技術の実証、③総合通信局を中心とした地域における情報共有体制の確立に向けた取組を実施。

【R２要求額：359百万円】

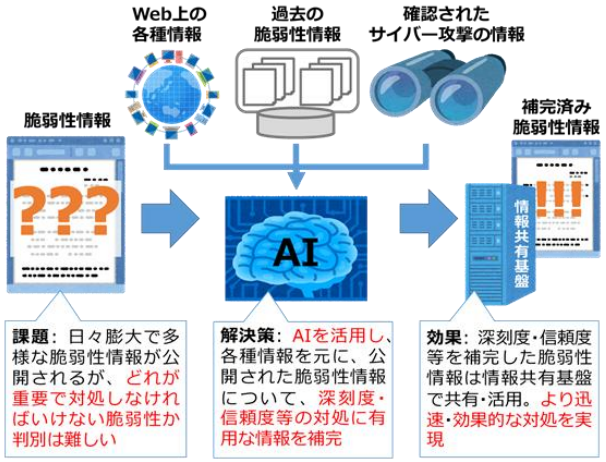
【目標・成果イメージ】
○以下により、サイバー攻撃による被害の甚大化を防ぎ、情報通信インフラをはじめとする我が国社会・経済の強靱性を向上させる。
・通信事業者や放送事業者をはじめとする産業界における関係者間の情報共有促進によるサイバーセキュリティ対策の強化
・総合通信局を中心とした地域の情報共有体制の構築

①情報共有基盤の高度化【180百万円】

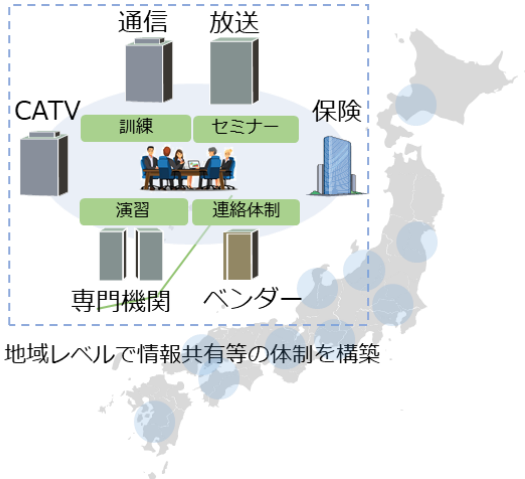
	既存	高度化
攻撃元情報	○	○
脆弱性情報	×	○＋評価
ソフトウェア情報 紐付け	×	○



②深刻度・信頼度評価の高精度化【124百万円】



③総通局を中心とした情報共有体制【55百万円】



地域レベルで情報共有等の体制を構築

トラストサービスの制度化に係る調査研究

- Society5.0実現に向け、社会全体のデジタル化が進む中、電子データの改ざんや送信元のなりすまし等を防止し、その正当性を担保するトラストサービスの重要性が高まっている。
- 安心・安全なデータ流通を支える基盤となるトラストサービス（タイムスタンプ、eシール等）の在り方について検討を行い、2019年中を目途に結論を得て、速やかに制度化の検討を実施

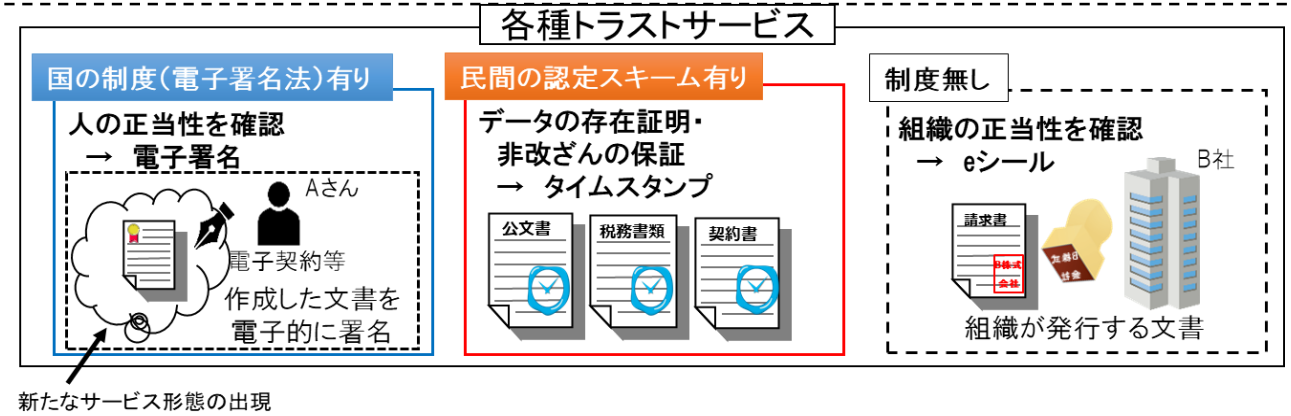
  ※「デジタル時代の新たなＩＴ政策大綱」、「成長戦略フォローアップ」等にも記載あり。
- EUにおいては、トラストサービスを包括的に規定するe-IDAS規則が発効（2016年）している状況も踏まえ、我が国においても、国際的相互運用性等を踏まえた形でトラストサービスの制度的枠組みを構築するため、欧米等におけるトラストサービスの活用事例や認定・審査基準等に関する調査研究を行う。

【Ｒ２要求額：50百万円（新規）】

【具体的な調査研究事項】

➢ 各種トラストサービスの制度化にあたり、国際的相互運用性も踏まえつつ、省令等の具体的な運用の技術基準を定める上で、以下に掲げる内容の調査研究を行い、安心・安全なデータ流通の確保及び各種手続きの電子化による社会経済の効率化に寄与する。

① 欧米等他国における各種トラストサービスの活用事例や、実際の認定及び審査に係る基準及び運用状況の調査、他国制度との相互運用性を確保する上での技術的・制度的課題の調査
② 民間における各種トラストサービスの活用事例及び利用ニーズの調査
③ 各種トラストサービス事業者の主要サービスに係る技術・運用面の動向の調査
④ 上記①～③を踏まえた、トラストサービスの制度化の検討



電子署名の普及啓発等

① 電子署名法に基づく**普及啓発活動を実施**するとともに、電子署名等のサービスを組み合わせることで実現可能な**データの送達等の完全性を保証する仕組み**（電子書留）や、**データを送受信するモノの正当性を確認する仕組み**（モノの認証）等に関して、長期的な観点から、海外（欧米）の先進事例や国内外での需要の調査を実施。

② 情報セキュリティに関する周知啓発等を行うため、**情報セキュリティに関する新たな動向の調査や「国民のための情報セキュリティサイト」の維持管理を実施**。

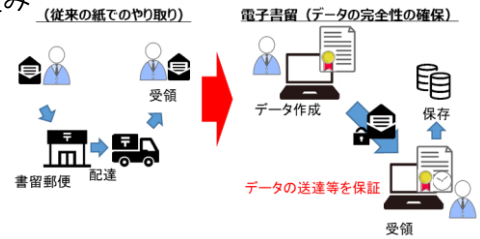
【R２要求額：18百万円】

① 電子署名等に関する調査及び普及啓発

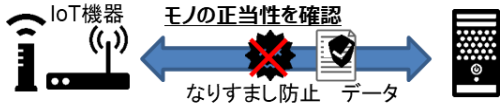
電子署名等のサービスに係る普及啓発活動を実施。

また、IoT機器等の発する膨大なデータの流通及びその活用が見込まれるSociety5.0では、データの信頼性の確保が必要となるため、電子署名等のサービスの組合せにより実現可能なデータの送達等の完全性を保証する仕組みや、データを送受信するモノの正当性を確認する仕組みについて、長期的な観点から、海外の先進事例や国内外での需要の調査を実施。

1. **電子書留**：送信・受信の正当性や送受信される**データの完全性の確保**を実現する仕組み

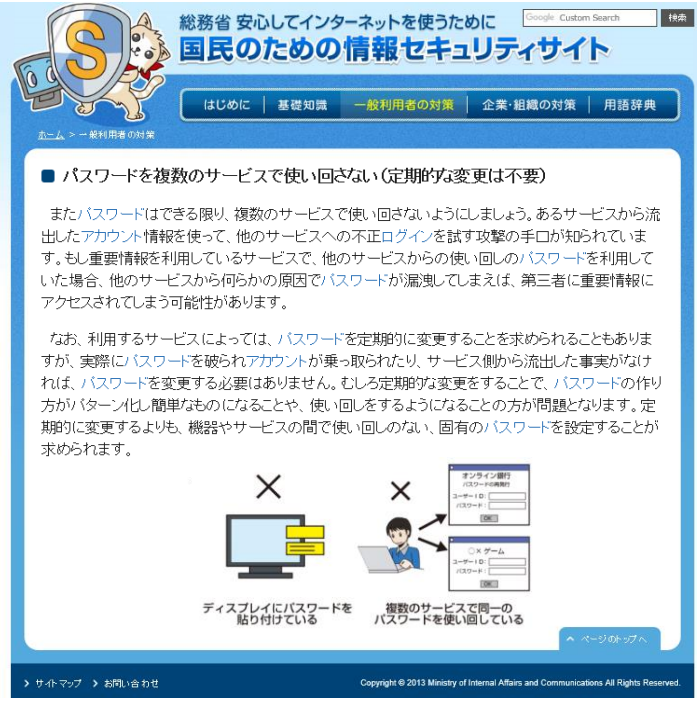


2. **モノの認証**：IoT機器等の各種センサーから送信されるデータのなりすまし防止等のため、**モノの正当性**を確認する仕組み



② 最新の情報セキュリティ動向の調査等

インターネットサービスにおける情報セキュリティに関する動向等の調査を行うとともに、調査内容を踏まえ、ウェブページを活用した利用者への普及啓発活動等を行う。



諸外国におけるサイバーセキュリティ動向の調査研究

■ 近年、政府機関、重要インフラ事業者、IoT機器等へのサイバー攻撃の事案が多数発生しており、サイバー攻撃に対する国家の強靭性を確保する観点から、諸外国におけるサイバーセキュリティ動向の調査研究を行うことにより、国際動向を踏まえた我が国におけるサイバーセキュリティ政策の立案・遂行を図る。

目的

【R2年度要求額：47百万円】

通信・放送インフラへの攻撃やIoT機器を狙ったボットの増加等、サイバーセキュリティの脅威は増大するおそれがある。次に挙げるサイバーセキュリティ動向を迅速かつ的確に把握し、効果的な国際協力・連携を推進する。

実施内容

① 諸外国におけるサイバーセキュリティ政策の動向調査
近年脅威が高まっているサプライチェーンリスクに係る政策動向について欧米諸国を中心に調査する。セキュリティ対策は政府の取組のみでは不十分であり、民間の協力が不可欠であることから、政府の実施するサイバーセキュリティ政策に対する民間企業・研究機関等の反応についても合わせて調査する。

② 各国ISPによるサイバーセキュリティ対策の動向調査
脅威情報を共有することがセキュリティ対策として有効であることから、個別のISPによる取組及び各国におけるISP連携のあり方等について調査する。特に、米国におけるISP間の情報共有に関する最新の取組や成功事例について調査する。

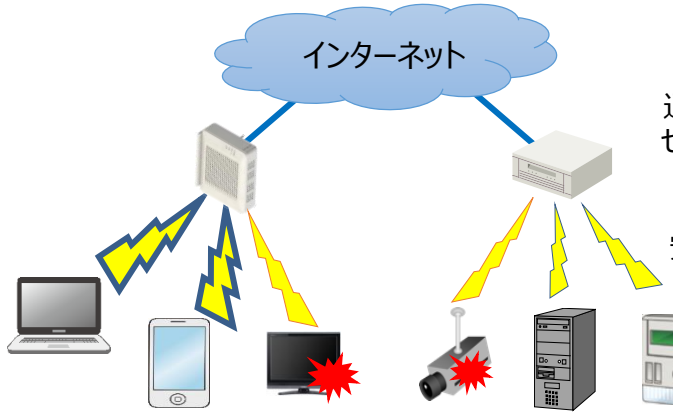
③ 各国におけるサイバーセキュリティ技術開発の動向調査
各国の技術開発動向を把握した上で我が国のサイバーセキュリティ技術開発を推進すべく、特に、サイバーセキュリティ分野の先進的技術を開発する企業・研究機関が多数存在する米国における、ACD（Active Cyber Defense：脅威に対する積極的防護策）等の最新技術開発動向について調査する。

周波数有効利用のためのIoTワイヤレス高効率広域ネットワークスキャン技術の研究開発

■ 近年、IoT機器を狙ったサイバー攻撃は著しく増加傾向にあり、脆弱なIoT機器への対策が喫緊の課題である。脆弱なIoT機器が無線LAN等に接続されている場合、通信を阻害することなくセキュリティを高める必要がある。このため、ワイヤレスIoT機器の周波数の利用状況の自動推定による広域ネットワークスキャン技術、広域ネットワークスキャンの無線通信量軽減技術等を開発し、周波数の有効利用を図る。

【背景・課題】
・2018年に世界で流通しているＩoT機器は約307億台。
・NICTのNICTERで観測したサイバー攻撃のうち、2018年では約半数がIoT機器を狙ったもの。
・脆弱なIoT機器のセキュリティ対策のため、膨大なIoT機器に対して広域ネットワークスキャンを実施する必要がある。

【実施内容】
ワイヤレスIoT機器の通信を阻害しない、より効率的なスキャンを実現するため、①周波数の利用状況の自動推定による広域ネットワークスキャン技術、②広域ネットワークスキャンの無線通信量軽減技術等を開発する。
令和２年度は、令和元年度までに開発した各技術を統合し、テストベッドや実ネットワークを用いた実証実験を行い、広域ネットワークスキャンに係る通信量の削減効果について総合評価を行う。



ワイヤレスIoT機器の
通信を阻害することなく、
セキュリティ対策が必要な
ワイヤレスIoT機器を
特定することで、
安全なICT基盤を実現

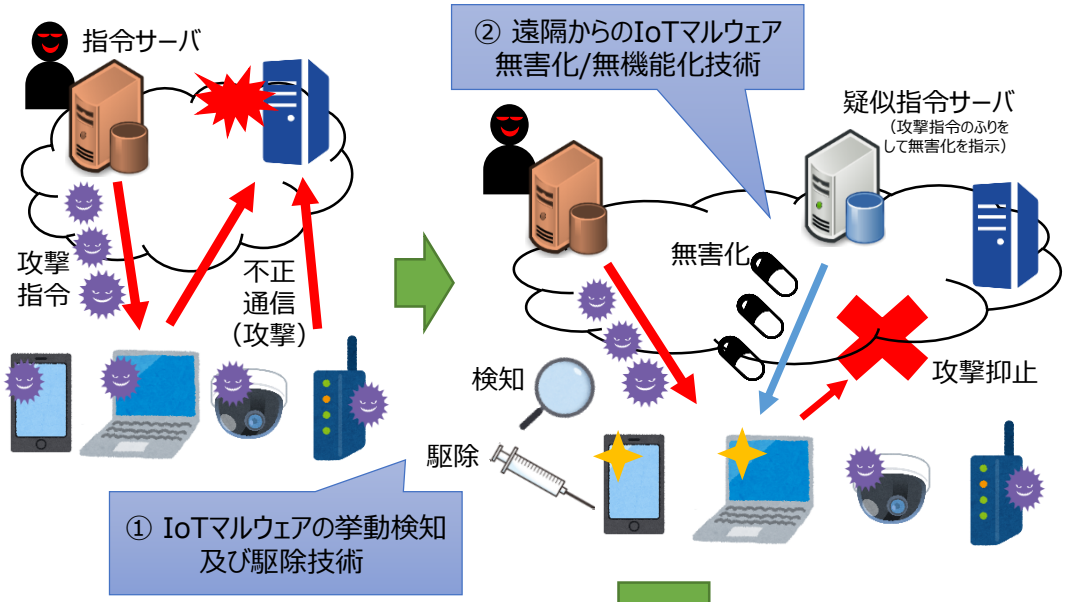
目標	周波数の利用状況の自動推定による広域ネットワークスキャン技術、広域ネットワークスキャンの無線通信量軽減技術等を令和２年度までに開発し、令和３年度までに本技術の実用化を目指す。
対象周波数帯	UHF帯
実施期間	平成30年度～令和２年度　（３カ年）
令和２年度要求額	12,588百万円の内数

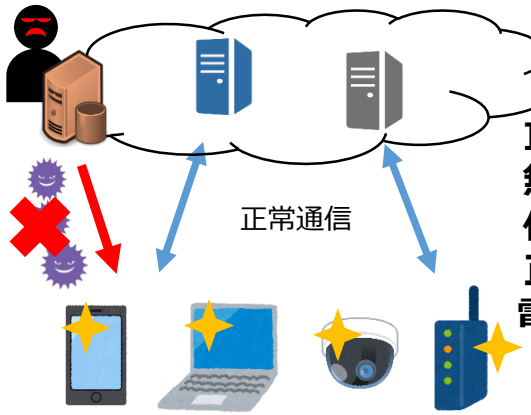
電波の有効利用のためのIoTマルウェア無害化/無機能化技術等に関する研究開発

■ 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、IoT機器が急速に増加しており（令和2年に世界で約400億台と予測）、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通信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機器が、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機器による不正通信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正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2年度は、各技術の基本方式の設計やプロトタイプの開発を行い、基礎技術の確立を目指す。





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年度までに実用化を目指す。マルウェアに感染したIoT機器からのサイバー攻撃を抑止し、無線リソースひっ迫を低減することで、安心・安全なIoT社会を実現する。
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２年度要求額	12,588百万円の内数