別添１

IoT・5G セキュリティ総合対策（案）

令和元年〇月

サイバーセキュリティタスクフォース

目次

はじめに 3

Ⅰ　背景 4

（１）ICT 利活用の進展 4

（２）サイバーセキュリティリスクの増大や脅威の深刻化 4

Ⅱ　施策展開の枠組み 8

Ⅲ　情報通信サービス・ネットワークの個別分野のセキュリティに関する具体的施策 10

（１）IoT のセキュリティ対策 10

①　IoT 機器の設計・製造・販売段階での対策 11

②　IoT 機器の設置・運用・保守段階での対策 11

③　脆弱性等を有する IoT 機器の調査と注意喚起 12

④　サイバー攻撃に関する電気通信事業者間の情報共有 13

（２）5G のセキュリティ対策 13

①　ソフトウェア脆弱性への対応 13

②　ハードウェア脆弱性への対応 14

（３）クラウドサービスのセキュリティ対策 14

（４）スマートシティのセキュリティ対策 15

（５）トラストサービスの在り方の検討 16

（６）公衆無線 LAN のセキュリティ対策 17

（７）重要インフラとしての情報通信分野のセキュリティ対策 17

（８）地域の情報通信サービスのセキュリティの確保 18

Ⅳ　横断的施策 19

（１）研究開発の推進 19

①　基礎的・基盤的な研究開発等の推進 19

②　広域ネットワークスキャンの軽量化 20

③　ハードウェア脆弱性への対応【再掲】 21

④　スマートシティのセキュリティ対策【再掲】 21

⑤　衛星通信におけるセキュリティ技術の研究開発 22
⑥　AI を活用したサイバー攻撃検知・解析技術の研究開発 23
⑦　量子コンピュータ時代に向けた暗号の在り方の検討 23
⑧　重要インフラ等におけるサイバーセキュリティの確保 24
⑨　IoT 社会に対応したサイバー・フィジカル・セキュリティ対策 24

（２）人材育成・普及啓発の推進 24
①　実践的サイバー防御演習（CYDER）の実施 25
②　2020 東京大会に向けたサイバー演習の実施 25
③　若手セキュリティ人材の育成の促進 26
④　地域のセキュリティ人材育成 26

（３）国際連携の推進 28
①　ASEAN 各国との連携 28
②　国際的な ISAC 間連携 29
③　国際標準化の推進 29
④　サイバー空間における国際ルールを巡る議論への積極的参画 30

（４）情報共有・情報開示の促進 30
①　サイバー攻撃に関する電気通信事業者間の情報共有【再掲】 31
②　事業者間での情報共有を促進するための基盤の構築 31
③　サイバーセキュリティ対策に係る情報開示の促進 32
④　サイバーセキュリティ対策に係る投資の促進 33
⑤　国際的な ISAC 間連携【再掲】 33

Ⅴ　今後の進め方 35

はじめに

本タスクフォースでは、IoT 機器を踏み台としたサイバー攻撃等が深刻化している状況を踏まえ、2017 年（平成 29 年）10 月に「IoT セキュリティ総合対策」を取りまとめた。総務省では、その後、同総合対策に沿って取組を進め、2018 年（平成 30 年）７月に「IoT セキュリティ総合対策 プログレスレポート 2018」、2019 年(令和元年)５月に「IoT セキュリティ総合対策 プログレスレポート 2019」を策定・公表したところである。

「IoT セキュリティ総合対策」策定・公表後に、政府全体で新たな「サイバーセキュリティ戦略」(2018 年（平成 30 年）７月 27 日 閣議決定。以下同じ。）が策定されており、関係各府省庁は同戦略の下で連携して施策を展開する必要がある。また、IoT をはじめとする ICT の利活用が一層進展していく中で、今後、5G のサービスが開始することが予定されているほか、Society5.0 に向けた適切なデータ管理・流通の重要性やサプライチェーンリスクへの対応などの必要性が増大するなど、サイバーセキュリティリスクへの対策の一層の強化は急務となっている。

本文書は、今般、「IoT セキュリティ総合対策」策定・公表後の様々な状況変化などを踏まえつつ、IoT・5G 時代にふさわしいサイバーセキュリティ政策の在り方について検討し、「IoT・5G セキュリティ総合対策」として整理したものである。本文書を羅針盤として、総務省が関係各府省庁や地方公共団体及び民間企業等と連携し、我が国のサイバーセキュリティ政策に率先して取り組むことが期待される。

Ⅰ　背景

（１）ICT 利活用の進展

ICT（Information and Communications Technology：情報通信技術）によって、我が国の社会・経済は大きく変革を遂げてきた。人々の日々のコミュニケーションや情報収集、企業活動、購買行動、就労、余暇など、社会・経済のあらゆる場面で ICT の利活用が浸透している。令和の時代に入り、この流れは今後も加速していくことが想定される。このような変化をもたらした ICT の発展の態様については大きく以下の５つに大別することができる。

①ブロードバンド化（小容量通信から大容量通信へ）
②モバイル化（固定から移動へ）
③クラウド化（オンプレミス[1]からクラウドへ）
④IoT 化（人からモノへ）
⑤AI（人工知能）化（人から AI へ）

上記のような変化を通じ、ICT そのものの利便性の高まりと高付加価値化が進んだ結果、これまで我が国のデジタル経済は急速に発展してきた。さらに ICT を活用することで様々な分野・産業でのデータの収集・分析・活用が進み、当該分野・産業においても高付加価値化が進んでいるところである。

2020 年（令和２年）に 5G サービスが本格的に開始されることにより、このような流れはより一層加速していくことが予測され、我が国が目指すべき社会像としての Society5.0 の到来を迎え、今後、サイバー空間と実空間の一体化が一層進展していくことが想定される。

（２）サイバーセキュリティリスクの増大や脅威の深刻化

前述のとおり、社会・経済全体のあらゆる場面での ICT の利活用が水や空気のように浸透してきたところであるが、同時に必然的にサイバーセキュリティリスクも増大している状況である。

サイバーセキュリティリスクは、インシデントの影響度の大きさ×発生確率で表されるが、社会・経済の ICT への依存度が高まれば高まるほど、インシデントが発生した際の脅威や影響も飛躍的に増大し、またインシデントが発生する確率も高くなる。

[1] 自身が管理する設備内に情報システムを設置・運用する形態。

そのため、サイバーセキュリティの確保は、ICT の利活用による社会や経済の持続的・安定的な発展のために必要不可欠な取組となっている。

この点、本タスクフォースでは 2017 年（平成 29 年）10 月に、IoT 機器・システムのセキュリティの確保を主眼において「IoT セキュリティ総合対策」を策定・公表したが、直近で特に対策が必要となるサイバーセキュリティ上の留意事項としては以下のような点が挙げられる。

① 5G のサービス開始に伴う新たなリスク

今後サービスが開始される予定の 5G については、従来までの移動通信システムと比較して、①超高速、②超低遅延、③多数同時接続であるという特徴を有しており、IoT システムの基盤技術として、電気通信事業者のみならず、様々な主体や産業分野での利活用が期待されている。

他方、サイバーセキュリティの観点からは、5G のネットワークはネットワーク機能の仮想化・ソフトウェア化やモバイルエッジコンピューティング[2]（以下「MEC」という。）など、従来のネットワークとは構造等の点において異なる特徴を有することが想定されるから、その点を踏まえ、5G のネットワークのセキュリティ確保の在り方について検討する必要がある。

また、5G のサービス開始により、従来に比べて産業用途での IoT 機器の設置・運用が今後も増加していくことが想定されるため、IoT 機器のセキュリティの確保（脆弱性対策を含む）の重要性が今後さらに高まっていくことが想定される。

さらに、従来はインターネットから隔離された形で運用されていた産業機器やインフラなどが無線経由でインターネットに接続される可能性が高くなることから、IT 系（情報系）だけでなく、OT 系（制御系）のシステムのセキュリティ対策も今後より一層重要になることが想定される。

② サプライチェーンリスクの管理の重要性

今日では、サイバー空間と実空間の一体化の進展や、サプライチェーンのグローバル化の進展により、ソフトウェアやハードウェアのサプライチェーンなど、ICT の製品やサービスを製造・流通する過程において不正なプログラムや

[2] ネットワークのエッジ（ユーザの近く）でなされる通信処理や高度な演算・データ処理。

ファームウェアの組み込み、又は改ざんなどが行われるリスクへの対応[3]が求められている。

また、製品やサービスそのもののリスクだけではなく、委託等の契約関係がある関係者の間でサイバーセキュリティ対策が不十分な者が踏み台となって他者へのサイバー攻撃がなされ、被害が伝播する「被害のチェーン」が発生するおそれもある。

そのため昨今では、企業単体ではなく、サプライチェーン単位でのサイバーセキュリティ対策が求められている状況[4]であり、特に地域の中小企業では、人材を含めたリソース不足のため、サイバーセキュリティ対策が遅れている可能性があることから、対策の強化の取組が必要不可欠となっている。

③ Society5.0の実現に向けた適切なデータの流通・管理の重要性

Society5.0はサイバー空間と実空間を高度に融合させることにより、経済的発展と社会的発展の解決を両立する「人間中心の社会」であり、言い換えれば、サイバー空間と実空間の間でデータが循環して、相互に作用し、これを前提とした様々なサービスが提供され、人々の生活に浸透し、恩恵をもたらす社会である。

そのSociety5.0の実現の鍵となるのがデータであり、データの利活用・管理の利便性を高めるクラウドサービスの安全性の確保や、データ収集・分析を都市や地域の機能やサービスを効率化・高度化に生かすスマートシティのセキュリティの確保等の重要性が高まっている。また、データ流通の有効性を担保するための基盤として、ネット利用者の本人確認やデータの改ざん防止等の仕組みであるトラストサービスの必要性も高まっている。

また、経済のグローバル化が進展する今日においては、国内のみならず国際的なデータの移転も大幅に増加している[5]。この点、諸外国に目を転じてみれば、EUのGDPR（一般データ保護規則：General Data Preservation Rule)、米

[3] 例えば、2018年（平成30年）には、台湾のハードウェアメーカーのコンピュータにプリインストールされているユーティリティーツールが攻撃者に乗っ取られた結果、正規アップデートに見せ掛けてマルウェアが大量のユーザにインストールされた事例がある。

[4] 独立行政法人情報処理推進機構（以下「IPA」という。）が毎年公表している「情報セキュリティ10大脅威」において、2019年（令和元年）に公表されたものは初めて「サプライチェーンの弱点を悪用した攻撃の高まり」が10位以内にランクインした（４位)。

[5] 平成29年版情報通信白書によれば、各国企業における国外へのデータ提供状況について、企業向け国際アンケートにおいて、英国企業及びドイツ企業の約70%、米国企業の約60%、日本企業の約40%が現在越境のデータ提供を行っていると回答。

国の FISMA（連邦情報セキュリティマネジメント法：Federal Information Security Management Act)、中国のサイバーセキュリティ法など、各国の政府が企業などに対して国境を越えてデータを移転させないような法規制を導入している例も出始めているところである。

そのため、上述のような流れも認識しつつ、機密性（Confidentiality)・完全性（Integrity)・可用性（Availability)・真正性（Authenticity）等の確保の観点からの適切なデータの管理・流通の在り方、及びそれを実現するための手段等について検討する必要がある。

④ サイバーセキュリティにおける AI の利活用の重要性

社会・経済において AI の活用が進展していく中で、サイバーセキュリティ政策を進めていく上での AI の在り方についても検討が必要となっている。AI とサイバーセキュリティの関係については様々な議論があるが[6]、サイバー攻撃に対処する観点からは、まずは AI を利用したサイバーセキュリティ対策を促進していくことが重要である。

具体的には、年々複雑化・巧妙化するサイバー攻撃に対し、例えば、「予防」「検知」「対処」の各フェーズにおいて AI を活用した高効率かつ精緻な対策技術を確立するための研究開発を推進するなど、所要の施策を進める必要がある。

⑤ 大規模な量子コンピュータの実用化の可能性

近年研究が進みつつある量子コンピュータは、「量子ビット」を活用してこれまで難しかった大規模な並列演算を可能にし、新たな可能性を開く技術として期待されているが、一方で、サイバーセキュリティ上、新たな課題が生ずることも懸念されている。

具体的には、今後大規模な量子コンピュータが実用化された場合、現在様々な機会で利用されている公開鍵暗号の多くが解読可能になるおそれがある。大規模な量子コンピュータの実用化にはまだ時間がかかると予想されている[7]も

---

[6] なお、「サイバーセキュリティ 2019」（2019 年（令和元年）５月 23 日 サイバーセキュリティ戦略本部決定）では、AI とサイバーセキュリティの関係性について、「AI を利用した攻撃」「AI 自身による自律的な攻撃」「AI への攻撃」「AI を利用したセキュリティ対策」の４つの類型に分類がなされている。

[7] 米国の国立標準技術研究所（以下「NIST」という。）が 2016 年（平成 28 年）に公表したレポートによれば、数時間以内に鍵長が 2000 ビットの RSA（Rivest-Shamir-Adleman cryptosystem：巨大な素数同士をかけ合わせた整数を素因数分解するのが困難であることを利

のの、インターネット上で流通する様々な情報の機密性と完全性の確保等の観点から、量子コンピュータ時代を見据えた新たな推奨暗号の在り方について、現段階から検討を開始する必要がある。

⑥　大規模な国際イベント等の開催

大規模かつ非日常の国際イベントは最高度の注目を集めることから、サイバー攻撃の標的となるおそれがある。この点、2019 年（令和元年）には G20 やラグビーワールドカップ、2020 年（令和２年）には 2020 年東京オリンピック・パラリンピック競技大会（以下「2020 東京大会」という。）の開催が予定されている。

そのため、過去の経験も踏まえつつ、2020 東京大会に関係する重要なサービスを担う事業者のリスクマネジメントや対処体制の構築、訓練・演習の強化など、特に重要インフラ事業者、重要サービス事業者等において、これまで実施されてきた対策の一層の強化が求められる。

また、2020 東京大会が無事成功裏に終わったとしても、社会に対するサービスの提供を行うという「任務」[8]を担う重要インフラ事業者等にとっては、サイバー攻撃への対処態勢の強化は日常的に重要な課題であり、引き続き、平時・有事の対策を着実に実行することが求められる。

上記のような状況を踏まえ、昨今でサイバーセキュリティ対策は一層重要度を増していることから、2017 年（平成 29 年）10 月に策定・公表した「IoT セキュリティ総合対策」を発展的に改編する形で、IoT・5G 時代にふさわしいサイバーセキュリティ政策の在り方として、今般「IoT・5G セキュリティ総合対策」を策定することとしたものである。

Ⅱ　施策展開の枠組み

サイバーセキュリティ対策は広範な政策分野であり、その推進に当たっては

用した公開鍵暗号の一つ）を破る能力を持つ量子コンピュータが約 10 億ドルの予算で 2030 年までに実現する可能性があると予想している研究者もいる。

[8] 「サイバーセキュリティ戦略」では、サイバーセキュリティの基本的な在り方において、官民の自律的な取組を進めるにあたって求められる観点して①「サービス提供者の任務保証」、②「リスクマネジメント」、③「参加・連携・協働」の３つが挙げられている。このうち、①については、自らが遂行すべき業務やサービスを「任務」と捉え、これを着実に遂行するために必要となる能力及び資産の確保をすることを指し、一部の専門家に依存するのではなく、「任務」の遂行の観点から、その責任を有する者が主体的にサイバーセキュリティ確保に取り組む、こととされている。

各主体の適切な役割分担の下での連携・協働が必要である。この点、総務省に期待される役割は、まず情報通信サービス・ネットワークの、特に重点的に対応すべき個別分野のセキュリティの在り方について包括的な検討の上、関係府省庁や地方公共団体及び民間企業と連携しつつ、政策を実効的に推進していくことである。

さらに、当該分野での政策をより効果的に実施するための研究開発の推進や、情報通信サービス・ネットワークのユーザも含めた人材育成・普及啓発の推進、国際連携の推進、サイバーセキュリティに関する情報共有・情報開示の促進観点からの取組を並行して進めていく必要がある。

そのため、本文書では、総務省として取り組むべき具体的な施策について、「Ⅲ情報通信サービス・ネットワークの個別分野のセキュリティに関する具体的施策」と「Ⅳ　横断的施策」の「（１）研究開発の推進」、「（２）人材育成・普及啓発の推進」、「（３）国際連携の推進」、「（４）情報共有・情報開示の促進」という項目で整理を行っている。

なお、施策の検討・展開の際には、それぞれの取組において、例えば以下のような観点について留意しつつ、施策の有効性を確保する必要がある。

①　ネットワーク側とユーザ側の双方の観点からの施策展開

情報通信サービス・ネットワーク全体の安全性や信頼性を確保するためには、ネットワーク側とユーザ側の双方の視点でサイバーセキュリティ対策を推進するための施策を検討する必要がある。

②　情報通信サービス・ネットワークのレイヤー構造

情報通信サービス・ネットワークについては、機能に着目して構造的にサービス（データ流通）層、プラットフォーム層、ネットワーク層、機器層と分類が可能であるが、それぞれの層において留意すべき脅威とセキュリティ要件の在り方について検討する必要がある。

③　時間軸を意識した施策展開

IoT 機器のライフサイクル、人材育成のスパンなど、施策の効果の発現に関する時間軸を意識した政策立案を行う必要がある。

④　政策バリューチェーンの構築

例えば、研究開発の成果を情報通信サービス・ネットワークの個別分野の施策に反映しつつ、その成果について国際的な展開を図る、また、情報通信サービス・ネットワークの個別分野のセキュリティに関する施策と人材育成の施策を連携させて、地域のサイバーセキュリティ確保を一体的に推進するなど、個別施策を有機的に連携させ、横断的で一貫性のある施策展開を図る必要がある。

Ⅲ　情報通信サービス・ネットワークの個別分野のセキュリティに関する具体的施策

総務省においてセキュリティの確保に取り組むべき情報通信サービス・ネットワークの個別分野としては、以下のような分野が考えられる。

まず、今後の 5G サービスの開始を迎え、IoT 及び 5G のセキュリティ対策は重要な政策課題となっており、既に始まっている取組と合わせて重点的に取り組んでいく必要がある。

また、Society5.0 の実現に向けたデータ流通や管理の需要性が増している中で、クラウドサービスの安全性の確保やスマートシティのセキュリティの確保も必要性が高まっているほか、データ流通の有効性を担保するための基盤としてのトラストサービスの在り方の検討も必要となっている。

さらに、昨今ではサプライチェーンの弱いところを狙った攻撃が散見されることから、我が国の情報通信サービス・ネットワーク全体のセキュリティの確保のため、地域の情報通信サービス・ネットワークのセキュリティ強化も必要である。

その上で、2020 東京大会及びその後を見据え、公衆無線 LAN のセキュリティの確保や、重要インフラ分野・重要サービス分野としての情報通信分野のセキュリティの確保などにも取り組む必要がある。

なお、具体的施策の検討・実施に当たっては、前述（Ⅱ）の①～④の観点などに留意する必要がある。

（１）IoT のセキュリティ対策

IoT 機器の脆弱性については、IoT 機器の①設計・製造・販売（輸入を含む。）段階、②設置・運用・保守段階において適切な対策をとる必要がある。

また、既にインターネットに接続されて設置・運用されている IoT 機器が多数あることが想定されることから、IoT 機器の脆弱性等の調査を実施するとと

もに、利用者への注意喚起や情報共有の取組等を推進する必要がある。

① IoT 機器の設計・製造・販売段階での対策

設計・製造・販売段階においては、製造業者における IoT 機器のセキュリティ・バイ・デザインの考え方を十分に浸透させるとともに、対策がとられた機器の市場への展開を促進させることが重要となる。

この点、IoT 機器に関する基本的なセキュリティ対策については、電気通信事業法（昭和 59 年法律第 86 号）の枠組みにおいて端末設備等規則（昭和 60 年郵政省令第 31 号）を改正し、強制規格としての技術基準が策定[9]されている（2019 年（平成 31 年）３月１日公布、2020（令和２年）年４月１日施行)。また、当該改正後の同規則の各規定等に係る端末機器の基準認証に関する運用について明確化を図る観点から、総務省において 2019 年（平成 31 年）４月に「電気通信事業法に基づく端末機器の基準認証に関するガイドライン（第１版)」を策定・公表している。今後は、当該技術基準の運用開始に向けた準備を進めることが必要である。

また、IoT 機器に関するセキュリティ対策の上乗せ部分については、民間団体がセキュリティ要件のガイドラインを策定し、さらに当該要件に適合した IoT 機器に対して適合していることを示すマークを付す認証（Certification）制度の構築の準備を進めていることから、このような民間の任意の認証（Certification）制度の普及が期待される。

② IoT 機器の設置・運用・保守段階での対策

機器の性格上セキュリティ対策を取ることが困難なものや海外製品など、流通する IoT 機器の中から、脆弱性を有する IoT 機器を完全に排除することは困難であることから、機器の設置・運用・保守段階（ネットワークへの接続時又は接続後）において、脆弱性を有する機器が存在することを前提として、セキュアな IoT システム構築を実現する仕組みが重要である。

また、IoT 機器は広範な利用者が利用することが想定されており、利用者によっては、IoT 機器やセキュリティに関する知識が十分に無いことが想定され

[9] インターネットプロトコルを使用し、電気通信回線設備を介して接続することにより、電気通信の送受信に係る機能を操作することが可能な端末設備について、最低限のセキュリティ対策として、①アクセス制御機能、②アクセス制御の際に使用する ID/パスワードの適切な設定を促す等の機能、③ファームウェアの更新機能、又は①～③と同等以上の機能を具備することを求めている。なお、PC やスマートフォン等、利用者が随時かつ容易に任意のソフトウェアを導入することが可能な機器については本対策の対象外とされている。

る。したがって、例えば、IoT 機器の設置後に新たな脆弱性が発見された場合に、当該 IoT 機器の製造業者によって脆弱性のパッチがユーザサポートの一環として提供されるなど、各種事業者の側において対策が実施される仕組みの構築が重要である。

IoT システム・サービス全体としてのセキュリティの確保に関しては、IoT 機器だけでなく、ネットワークやプラットフォーム側での対処の在り方についても検討が必要である。この点で、IoT 機器の不正検知等のため、IoT 機器とインターネットの境界上にセキュアゲートウェイ（IoT セキュアゲートウェイ）を設置・運用し、ネットワークやプラットフォーム等での防御に活用する取組が考えられる。本取組について、Ⅲ－（４）のスマートシティのセキュリティ対策の取組等を通じ、実際の導入を進める仕組みや方策について検討することが重要である。

③　脆弱性等を有する IoT 機器の調査と注意喚起

前述の①、②の対策については、実効性を発揮するまでに一定程度の時間を有することから、まずは既に設置されている IoT 機器に関する脆弱性等の有無の調査を実施し、必要な対応を速やかに実施する必要がある。

この点、国立研究開発法人情報通信研究機構（以下「NICT」という。）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５年間の時限措置として追加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（平成 11 年法律第 162 号）の改正を実施し、2019 年（平成 31 年）２月より、NICT が IoT 機器を調査し、電気通信事業者を通じて利用者への注意喚起を行うプロジェクト「NOTICE[10]」を開始したところであり、引き続き、本プロジェクトの着実な実施を通じ、既に現在設置されている IoT 機器のセキュリティ対策を進めることが必要である。

また、「NOTICE」の取組に加えて、既にマルウェアに感染している IoT 機器を NICT の「NICTER」プロジェクトで得られた情報を基に特定し、電気通信事業者を通じて利用者へ注意喚起を行う取組を実施することも必要である。

さらに上述の取組の実施にあたり、専用のサポートセンターを設置し、行政相談窓口や消費生活センター等と連携しつつ、ウェブサイトや電話による問合せ対応を通じて利用者に適切な IoT 機器のセキュリティ対策を案内することも必要である。

10　National Operation Toward IoT Clean Environment の略。

加えて、これらの取組については、IoT 機器のセキュリティ対策のベストプラクティスとして、Ⅳ－（３）の国際連携の推進などの取組を通じ、海外各国に対して発信し、各国の取組につながるよう働きかけることが重要である。

④　サイバー攻撃に関する電気通信事業者間の情報共有

脆弱性を有する IoT 機器が踏み台となったことが確認された際、被害の拡大を防止するため、ISP による、当該 ISP の利用者の端末と C&C サーバ[11]の間の通信を遮断する等の取組が必要である。

この点、総務省では、2018 年（平成 30 年）５月の改正電気通信事業法において、電気通信事業者が「送信型対電気通信設備サイバー攻撃」への対応を共同して行うため、攻撃の送信元情報の共有や C&C サーバの調査研究等の業務を行う第三者機関(認定送信型対電気通信設備サイバー攻撃対処協会。以下「認定協会」という。）を総務大臣が認定する制度を創設し、2019 年（平成 31 年）１月に一般社団法人 ICT-ISAC[12]が認定されたところである。

今後は認定協会の活動について、マルウェアに感染している可能性の高い IoT 端末等や C&C サーバであると疑われる機器の検知や利用者への注意喚起等の電気通信事業者が行う対策に向け、円滑な実施のための支援を行うなどの取組を促進することが重要である。

また、こうした認定協会の活動や「NOTICE」の実施状況も踏まえ、電気通信事業者等が協力してサイバー攻撃への対処を行う際の基盤となる効果的な情報共有の在り方について引き続き検討することが重要である。

（２）5G のセキュリティ対策

①　ソフトウェア脆弱性への対応

今後サービスが開始される予定の 5G については、従来までの移動通信システムと比較して、①超高速、②超低遅延、③多数同時接続であるという特徴を有しており、IoT システムの基盤技術として、電気通信事業者のみならず、様々

11　ボットネットや感染コンピュータのネットワークに対し、不正なコマンドを遠隔で頻繁に送信するために利用されるサーバのこと。Command and Control サーバの略。

12　ISAC は Information Sharing and Analysis Center の略で、サイバーセキュリティに関する情報収集や、収集した情報の分析等を行う組織を指し、分析した情報は ISAC に参加する会員間で共有され、各々のセキュリティ対策等に役立てられる。通信分野では、2002 年（平成 14 年）に他分野に先立ち、「Telecom-ISAC」が設立され、その後、会員企業を ISP 事業者、放送事業者、ICT ベンダー及びセキュリティベンダー等に拡大する形で、一般財団法人日本データ通信協会から独立し、「ICT-ISAC」として一般社団法人化。

な主体や産業分野での利活用が期待されている。

一方、5G のネットワークに関しては、ネットワーク機能の仮想化・ソフトウェア化が進むことから、新たなサイバーセキュリティ上の課題が懸念される。また、新たにネットワークのエッジ（ユーザの近く）で通信処理や高度な演算・データ処理がなされる MEC が利用されることから、ネットワークインフラとしての機能維持のためには、基地局やコア網のみならず、MEC も含めた各構成要素（デバイス、クラウド、アプリケーション等）全体を考慮したセキュリティの確保が必要不可欠である。

そのため、5G を利用したシステム全体の各構成要素におけるソフトウェア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し、ガイドライン等によって対策の共有等を図ることを通じ、5G を構築・活用する重要インフラ事業者等への周知・啓発を図ることが必要である。

また、5G のセキュリティの確保は、国際的にも重要な政策課題であることから、作成したガイドライン等について国際機関等への提案も視野に入れるなど、諸外国との連携を図ることが期待される。

② ハードウェア脆弱性への対応

機器のセキュリティについては、機器にインストールされているソフトウェアだけでなく、集積回路の設計工程において、ハードウェア脆弱性が存在する可能性が指摘されている。

そのため、総務省では、2017 年度（平成 29 年度）より、戦略的情報通信研究開発推進事業（SCOPE）において、ハードウェア脆弱性の検知技術の研究開発を実施し、膨大な数の回路設計図をビッグデータとして収集・蓄積しつつ、脆弱性が存在する可能性のあるチップを、AI を活用して類型化し、ハードウェア脆弱性を発見するための研究開発を実施してきたところである。

5G の時代を見据え、サプライチェーンリスクへの対応の観点から、ソフトウェアやファームウェアに対する対策と合わせて、引き続き、ビッグデータや AI を活用しつつハードウェアに組み込まれるおそれのある脆弱性を検出する技術の研究開発等を推進することが必要である。

（３）クラウドサービスのセキュリティ対策

ICT の利活用が社会全体として進展する中、インターネット上のリソースを臨機応変に活用するクラウドサービスは、サービスアプリケーションから多様な

IoT プラットフォームまで、様々な ICT ソリューションを支えており、データの利活用・管理における中核のサービスとなっている。

その中で、我が国の政府においても「政府情報システムにおけるクラウドサービスの利用に係る基本方針」(2018 年（平成 30 年）６月７日 CIO 連絡会議決定）を定め、情報システム調達に際しては、コスト削減や柔軟なリソースの増減等の観点から、クラウドサービスの利用を第一候補として検討を行う旨の方向性が示されているところである。

この点、諸外国では、2010 年代に政府が情報システム調達においてクラウドファーストを掲げ、その後間もなく、政府が主導してクラウドサービスの安全性を評価する制度を構築・運用している事例があり、2018 年（平成 30 年）に上述のクラウド・バイ・デフォルト原則を採用した我が国においても、安全性評価の制度の検討が必要な段階に到達している。

そのため、総務省と経済産業省において、クラウドサービスの安全性評価に関する検討を行うことを目的として、2018 年（平成 30 年）８月より、「クラウドサービスの安全性評価に関する検討会」を開催し、2019 年（平成 31 年）３月に制度の枠組みが示されたところである。

本枠組みを踏まえつつ、官民双方が一層安全・安心にクラウドサービスを採用し、継続的に利用していくため、クラウドサービスの安全性評価制度について、引き続き、総務省において、経済産業省と連携しつつ、2020 年（令和２年）の制度の開始を目指して、評価基準や制度の確立に向けた検討を進めることが必要である。

（４）スマートシティのセキュリティ対策

スマートシティは、先進的技術の活用により、都市や地域の機能やサービスを効率化・高度化し、各種の課題の解決を図るとともに、快適性や利便性を含めた新たな価値を創出する取組であり、Society5.0 の先行的な実現の場である。

この点、総務省では、都市に設置されたセンサーから収集・生成・蓄積・解析されるデータを活用し、その解析結果を都市経営の課題解決などに活用するデータ利活用型スマートシティ事業を 2017 年度（平成 29 年度）から実施しているところである。なお、今後は政府のスマートシティに係る各事業の連携や分野間のデータ連携等を協力推進していくため、関係本部・省庁で連携[13]していくこ

[13] 統合イノベーション戦略推進会議（第４回）(2019 年（平成 31 年）３月 29 日)「府省連携したスマートシティ事業の推進について」

ととされている。

他方、スマートシティでは、インターネットに接続するセンサー・カメラ等が散在し、多様なデータが流通しているため、常にサイバー攻撃のリスクにさらされるおそれがある。また、様々なデータが共通プラットフォーム上で流通する中で、データの真正性の確保や適切なデータ流通の管理の仕組みの構築等も必要である。さらに、システムとしてのスマートシティの構築・運用には多様な主体が関わることから、システム全体としてのセキュリティの在り方について多様な関係者間で一定の共通認識の醸成が必要である。

そのため、スマートシティ上の様々なユースケース（分野）やアーキテクチャ、相互運用性などを踏まえつつ、スマートシティに求められるセキュリティ要件について検討を行い、明確化を図る必要がある。

また、スマートシティの取組は国際的にもEUの研究開発プロジェクトHorizon 2020やNISTが主導するGCTC（Global City Teams Challenge[14]）プロジェクトでも展開されており、総務省ではEUと連携した、スマートシティ分野のセキュリティ・プライバシ保護を含む日EU共同研究（Fed4IoT[15]）を2018年（平成30年）から実施している。

そのため、上述の成果については諸外国と連携の上、国際標準化や必要に応じた国際的な議論の場への提案を検討するなど、諸外国との調和を意識して展開を図ることが重要である。

さらに、スマートシティのシステムでは、多種多様なIoT機器が活用されることが想定されることから、そのセキュリティの確保に当たっては、IoT機器そのもののセキュリティの強化だけでなく、ネットワークの側でIoT機器の不正検知等を実施するための仕組みが有効であり、実際の運用に関して、Ⅲ－（１）－②のIoT機器とインターネットの境界上にセキュアゲートウェイを設置し、適切に運用する取組との連携の在り方も検討することが重要である。

（５）トラストサービスの在り方の検討

Society5.0の実現に向けて、サイバー空間の自由で安心・安全なデータの流通を実現するためには、データの信頼性を確保する仕組みとして、データの改ざんや送信元のなりすまし等を防止するトラストサービスが不可欠である。

---

[14] https://pages.nist.gov/GCTC/

[15] スマートシティアプリケーションに拡張性と相互運用性をもたらす仮想IoT-クラウド連携基盤の研究開発（Fed4IoT）

そのため、総務省では、「プラットフォームサービスに関する研究会」の下に「トラストサービス検討ワーキンググループ」を設置し、2019 年（平成 31 年）１月から、以下のようなトラストサービスに関する現状や課題について検討を行っている。

１）人の正当性を確認できる仕組み（電子署名）
２）組織の正当性を確認できる仕組み（組織を対象とする認証、ウェブサイト認証）
３）IoT 機器等のモノの正当性を確認できる仕組み
４）データの存在証明・非改ざんの保証の仕組み（タイムスタンプ）
５）データの送達等を保証する仕組み（e デリバリー）

一方、EU においては 2016 年（平成 28 年）７月に発効した eIDAS（electronic Identification and Authentication Services）規則により、電子署名、タイムスタンプ、e シール等のトラストサービスについて包括的に規定している状況である。

そのため、国際的な相互運用性の確保の観点からも、引き続き、同ワーキンググループにおいて、制度的課題等について整理を行い、トラストサービスの在り方について 2019 年（令和元年）中を目途に結論が得られるよう、検討を進めることが必要である。

（６）公衆無線 LAN のセキュリティ対策

公衆無線 LAN については、2020 年東京大会に向けて、観光や防災の観点から、その普及が進んでいるところである。他方、多くの公衆無線 LAN のサービスにおいて、依然としてサイバーセキュリティに対する配慮に欠けるものも多く、これらのサービスを踏み台にした攻撃や情報漏洩などのインシデントが発生するおそれもある。

そのため、公衆無線 LAN の利用者や提供者向けの公衆無線 LAN の利用の手引きの普及を図るなど、利用者・提供者において必要となるセキュリティ対策に関する周知啓発の充実を図ることが重要である。

その際、Ⅲ－（８）の地域の情報通信サービスのセキュリティの確保の取組で構築する連絡体制を活用し、効果的な周知啓発を図ることが重要である。

（７）重要インフラとしての情報通信分野のセキュリティ対策

情報通信分野は、「重要インフラの情報セキュリティに係る第４次行動計画」

（平成 29 年４月 18 日サイバーセキュリティ戦略本部決定　平成 30 年７月 25 日サイバーセキュリティ戦略本部改定。以下「第４次行動計画」という。）において、特にその機能が停止又は低下した場合に国民生活・社会経済活動に多大なる影響を及ぼしかねないサービスとして重要インフラの 14 分野の１つに指定されている。

第４次行動計画を踏まえ、重要インフラ各分野に横断的な指針として「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第５版）」（平成 30 年４月サイバーセキュリティ戦略本部決定　令和元年５月サイバーセキュリティ戦略本部改定）が定められており、同指針を踏まえ、官民で連携して、安全基準等の整備及び浸透の取組が進められている。

この点、電気通信においては、各年の取組として、「電気通信事故検証会議」等の枠組みを通じ、電気通信事故の分析・検証等を行うとともに、事故再発防止のため、「情報通信ネットワーク・安全信頼性基準」等の見直しの必要性について検討を行っている。

また、2018 年度（平成 30 年度）には、前述のⅢ－（１）－④のとおり、「送信型対電気通信設備サイバー攻撃」に関する送信元情報の共有や C&C サーバの調査研究等を行う第三者機関として認定協会を総務大臣が認定する制度を創設した。さらに本制度改正に関連して、「送信型対電気通信設備サイバー攻撃」が原因である電気通信事故の発生状況を把握する観点から当該事故の報告を求めるため、電気通信事業報告規則を改正する制度整備が行われている。

以上のような取組も踏まえつつ、引き続き、必要に応じて情報通信分野のセキュリティ対策に関する制度的枠組みの改善等に向けた取組が行われることが期待される。

（８）地域の情報通信サービスのセキュリティの確保

我が国の情報通信サービス・ネットワークの安全性や信頼性の確保の観点からは、全国規模や首都圏でサービスを提供している事業者だけでなく、地域単位で情報通信サービスを提供している事業者におけるサイバーセキュリティの確保も重要な課題である。

他方、地域においては、首都圏と比較してサイバーセキュリティに関する情報格差が存在するほか、経営リソースの不足等の理由により、セキュリティ対策が十分でないケースが存在するおそれがある。

そのため、業界団体やセキュリティ関係機関等と連携しつつ、地域の事業者の

サイバーセキュリティ対策の質の向上に向けた連絡体制を構築することが必要である。

なお、当該施策の展開に当たっては、Ⅲ－（６）の公衆無線 LAN のセキュリティの確保やⅣ－（２）－①の実践的サイバー防御演習（CYDER）の実施、Ⅳ－（２）－④の地域のセキュリティ人材育成の取組等との連携を図り、効果的に地域の情報通信サービスのセキュリティ対策の質の向上を図ることが重要である。

Ⅳ　横断的施策

（１）研究開発の推進

サイバー空間における攻撃の態様は常に変化しており、これに対応するには、政府が支援する産学官連携による研究開発の成果を即座に反映した最新のサイバーセキュリティ対策を実施していくことが有効である。

この点、サイバーセキュリティに関する研究開発は重要な政策課題とされており、サイバーセキュリティ戦略において、高いレベルのセキュリティ品質を備えた安全・安心な製品やサービスを提供していくことは、我が国の産業の成長、国際競争力の向上を目指していく上で不可欠である旨や、実践的なサイバーセキュリティの研究開発が必要である旨が示されている。

また、同戦略期間中における政府の取組の具体化及び強化を図る目的で策定された「サイバーセキュリティ研究・技術開発取組方針」（2019 年（令和元年）５月 23 日サイバーセキュリティ戦略本部報告）によれば、我が国のサイバーセキュリティの研究・技術開発において取り組むべき課題として、（１）サプライチェーンリスクの増大、（２）サイバーセキュリティ自給率の低迷、（３）研究・技術開発に資するデータの活用、（４）先端技術開発に伴う新たなリスクの出現、（５）産学官連携強化の必要、（６）国際標準化強化の必要、の６点が指摘されているところである。

したがって、総務省においても、上述の課題認識の下、NICT や民間企業等と連携しつつ、研究開発の成果が民間企業等への技術移転によって広く普及し、社会実装が進むことを視野に入れながら、サイバーセキュリティ対策に係る研究開発を効果的に推進する必要がある。

①　基礎的・基盤的な研究開発等の推進

これまで NICT では、中長期計画に基づき、サイバーセキュリティ分野の基

礎的・基盤的な研究開発等を実施しているところである。

例えば、巧妙化・複雑化するサイバー攻撃や標的型攻撃に対応するため、模擬環境や模擬情報を用いて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を可能にするサイバー攻撃誘引基盤「STARDUST」（スターダスト）を活用し、攻撃活動の早期収集や未知の標的型攻撃等を迅速に検知する技術等の研究開発を行っている。

また、暗号技術分野においては、現在利用されている暗号技術及び今後の利用が想定される暗号技術の安全性評価、量子コンピュータ時代に向けた格子理論に基づく新たな公開鍵暗号の開発、プライバシーの保護に資する暗号化したままデータを解析する技術等の研究開発が行われている。

その中で、インターネット上で起こる大規模攻撃への迅速な対応を目指したサイバー攻撃観測・分析・対策システムを用いて、ダークネットや各種ハニーポットによるサイバー攻撃の大規模観測及びその原因（マルウェア）等の分析を実施する「NICTER」プロジェクトが実施されている。同プロジェクトで得られるマルウェアに感染している機器に係る情報を、電気通信事業者に提供することで、Ⅲ－（１）－③の脆弱性等を有する IoT 機器の調査と注意喚起と連携し、IoT 機器のセキュリティ対策を推進することが必要である。

このような基礎的・基盤的な研究開発については、その研究開発の成果が民間企業等への技術移転によって広く普及し、社会実装が進むことが求められることから、引き続き、社会全体のサイバーセキュリティ対策の質の向上に資するよう、基礎的・基盤的な研究開発等を推進することが必要である。

② 広域ネットワークスキャンの軽量化

IoT 機器を狙ったサイバー攻撃は依然として多く、脆弱な IoT 機器のセキュリティ対策は喫緊の課題である。他方、IoT 機器の対策のためには、インターネットに接続している IoT 機器に対して広域的なネットワークスキャンを実施する必要がある。

他方、IoT 機器が増大している中で広域ネットワークスキャンを行うと、それに係る通信量も膨大になるおそれがあることから、通信量の抑制と精度の向上を両立するような効率的な広域ネットワークスキャンの実現が必要となる。

そのため、総務省では、通信量の抑制と精度の向上を実現する効率的な広域ネットワークスキャンの実現を目的として、2018 年度（平成 30 年度）～2020 年度（令和２年度）までの３年間を実施期間とし、「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」に取り組むこととしている。

本研究開発を通じ、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の開発と広域ネットワークスキャンの無線通信量軽減技術の開発に取り組む必要がある。

また、本研究開発の成果については、Ⅲ－（１）－③の IoT 機器の脆弱性調査に活用し、当該調査の効率化を図ることが重要である。

③　ハードウェア脆弱性への対応【再掲】

機器のセキュリティについては、機器にインストールされているソフトウェアだけでなく、集積回路の設計工程において、ハードウェア脆弱性が存在する可能性が指摘されている。

そのため、総務省では、2017 年度（平成 29 年度）より、戦略的情報通信研究開発推進事業（SCOPE）において、ハードウェア脆弱性の検知技術の研究開発を実施し、膨大な数の回路設計図をビッグデータとして収集・蓄積しつつ、脆弱性が存在する可能性のあるチップを、AI を活用して類型化し、ハードウェア脆弱性を発見するための研究開発を実施してきたところである。

5G の時代を見据え、サプライチェーンリスクへの対応の観点から、ソフトウェアやファームウェアに対する対策と合わせて、引き続き、ビッグデータや AI を活用しつつハードウェアに組み込まれるおそれのある脆弱性を検出する技術の研究開発等を推進する必要がある。

④　スマートシティのセキュリティ対策【再掲】

スマートシティは、先進的技術の活用により、都市や地域の機能やサービスを効率化・高度化し、各種の課題の解決を図るとともに、快適性や利便性を含めた新たな価値を創出する取組であり、Society5.0 の先行的な実現の場である。

この点、総務省では、都市に設置されたセンサーから収集・生成・蓄積・解析されるデータを活用し、その解析結果を都市経営の課題解決などに活用するデータ利活用型スマートシティ事業を 2017 年度（平成 29 年度）から実施しているところである。なお、今後は政府のスマートシティに係る各事業の連携や

分野間のデータ連携等を協力推進していくため、関係本部・省庁で連携[16]していくこととされている。

他方、スマートシティでは、インターネットに接続するセンサー・カメラ等が散在し、多様なデータが流通しているため、常にサイバー攻撃のリスクにさらされるおそれがある。また、様々なデータが共通プラットフォーム上で流通する中で、データの真正性の確保や適切なデータ流通の管理の仕組みの構築等も必要である。さらに、システムとしてのスマートシティの構築・運用には多様な主体が関わることから、システム全体としてのセキュリティの在り方について多様な関係者間で一定の共通認識の醸成が必要である。

そのため、スマートシティ上の様々なユースケース（分野）やアーキテクチャ、相互運用性などを踏まえつつ、スマートシティに求められるセキュリティ要件について検討を行い、明確化を図る必要がある。

また、スマートシティの取組は国際的にも EU の研究開発プロジェクト Horizon 2020 や NIST が主導する GCTC（Global City Teams Challenge）プロジェクトでも展開されており、総務省では EU と連携した、スマートシティ分野のセキュリティ・プライバシ保護を含む日 EU 共同研究（Fed4IoT）を 2018 年（平成 30 年）から実施している。

そのため、上述の成果については諸外国と連携の上、国際標準化や必要に応じた国際的な議論の場への提案を検討するなど、諸外国との調和を意識して展開を図ることが重要である。

さらに、スマートシティのシステムでは、多種多様な IoT 機器が活用されることが想定されることから、そのセキュリティの確保に当たっては、IoT 機器そのもののセキュリティの強化だけでなく、ネットワークの側で IoT 機器の不正検知等を実施するための仕組みが有効であり、実際の運用に関して、Ⅱ－（１）－②の IoT 機器とインターネットの境界上にセキュアゲートウェイを設置し、適切に運用する取組との連携の在り方も検討することが重要である。

⑤　衛星通信におけるセキュリティ技術の研究開発

近年、世界的な宇宙分野における人工衛星等の産業利用に向けた活動が活発化しており、商社や自動車製造など、これまで宇宙ビジネスに関わったことがない非宇宙系であった業界がその動きを牽引している。また、衛星コンステレ

[16]　統合イノベーション戦略推進会議（第４回）（2019 年（平成 31 年）３月 29 日）「府省連携したスマートシティ事業の推進について」

ーションによるグローバルな地球観測や衛星通信網の構築に関する計画が進められており、今後一層の衛星利用の需要拡大が見込まれる状況にある。

一方、衛星通信に対する第三者による通信内容の盗聴や改ざん、制御の乗っ取りといったサイバー攻撃が脅威となりつつあり、より一層の衛星通信のセキュリティ強化が求められる。

そのため、総務省では、安全な衛星通信ネットワークの構築を可能とし、盗聴や改ざんが極めて困難な量子暗号通信を超小型衛星に活用するための技術の確立に向け、2018 年度（平成 30 年度）から５年間の研究開発期間で「衛星通信における量子暗号技術の研究開発」に取り組んでおり、引き続き、本研究開発を継続して実施する必要がある。

⑥　AI を活用したサイバー攻撃検知・解析技術の研究開発

日々、数多く発生するサイバー攻撃に対して、AI を活用することにより、サイバー攻撃の検知・解析を自動化し、多様なサイバー攻撃に対する迅速なサイバーセキュリティ対策を講ずることが可能となる。

そのため、今後、AI を活用したサイバー攻撃検知・解析技術の研究開発にも取り組む必要がある。具体的には、様々な手法により収集したサイバー攻撃情報を、機械学習を用いて分析することにより、マルウェアの攻撃挙動の解析を自動化するとともに、攻撃の初期挙動の特徴分析や影響度評価を行い、関連組織で共有できる早期警戒情報を導出する技術等を開発する必要がある。

⑦　量子コンピュータ時代に向けた暗号の在り方の検討

①のとおり、暗号技術分野については、NICT において、現在利用されている暗号技術及び今後の利用が想定される暗号技術の安全性評価、量子コンピュータ時代に向けた格子理論に基づく新たな公開鍵暗号の開発、プライバシーの保護に資する暗号化したままデータを解析する技術等の研究開発を行っている。

その上で、今後、大規模な量子コンピュータの実用化による暗号の危殆化の可能性を踏まえた検討が必要であることから、CRYPTREC[17]の「暗号技術検討会」の下に「量子コンピュータ時代に向けた暗号の在り方検討タスクフォース」を

[17]　Cryptography Research and Evaluation Committees の略であり、電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクト。総務省及び経済産業省が共同で運営する「暗号技術検討会」と、NICT 及び IPA が共同で運営する「暗号技術評価委員会」及び「暗号技術活用委員会」で構成される。

設置し、次期電子政府推奨暗号リストの要件、その他新たな暗号技術の動向を踏まえた検討を行う必要がある。

⑧　重要インフラ等におけるサイバーセキュリティの確保

戦略的イノベーション創造プログラム（以下「SIP」という。）の第１期課題（2015 年度（平成 27 年度）～2019 年度（令和元年度））である「重要インフラ等におけるサイバーセキュリティの確保」について、内閣府、経済産業省等と連携して研究開発と実証を進めている。

本課題では、2020 東京大会の安心・安全な開催に向けて重要インフラ等におけるサイバーセキュリティを確保するため、制御・通信機器の真贋判定技術及び動作監視・解析技術等の開発に取り組んでおり、最終年度である 2019 年度（令和元年度）において、幅広い分野に横展開するための技術開発及び社会実装を進める必要がある。

⑨　IoT 社会に対応したサイバー・フィジカル・セキュリティ対策

SIP の第２期（2018 年度（平成 30 年度）～2022 年度（令和４年度））では、新たな研究課題として「IoT 社会に対応したサイバー・フィジカル・セキュリティ」を設定し、内閣府、経済産業省等と連携して取組を開始している。

本課題では、IoT 機器のセキュリティを保証する技術、サプライチェーンの分野毎の要件を明確にしたうえでトラストリストを構築・確認する技術、業務データを安全に流通させるためのトレーサビリティ確保技術、サイバー・フィジカル空間を跨った不正なデータを検知･防御する技術等の開発に取り組んでいる。

そのため、上記の研究開発を本格化するとともに、実証実験に向けた準備を着実に進めることが重要である。

（２）人材育成・普及啓発の推進

サイバーセキュリティ人材の育成は重要な政策課題とされており、サイバーセキュリティ戦略においては、組織における経営層、戦略マネジメント層、実務者層・技術者層といった各人材層の育成・確保や、若年層における教育の充実、中小企業関係の取組等について、具体的な方向性が示されているところである。

これまで、総務省の施策としては、特に実務者層・技術者層及び若年層を対象に、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、

１） 国の行政機関・地方公共団体及び重要インフラ事業者などを対象とした実践的サイバー防御演習（CYDER）

２） 2020 年東京大会の適切な運営に向けたセキュリティ人材の育成（サイバーコロッセオ）

３） 若手セキュリティエンジニアの育成（SecHack365）

の取組を行っているところであり、引き続き、これらの取組を継続して進めるとともに、サイバーセキュリティの知識・スキルが十分でない中小企業向けの人材育成の取組を実施する必要がある。

① 実践的サイバー防御演習（CYDER）の実施

総務省は NICT を通じ、NICT の北陸 StarBED 技術センターに設置された大規模高性能サーバ群を活用し、行政機関等の実際のネットワークを模した大規模仮想 LAN 環境を構築の上、国の行政機関、地方公共団体、独立行政法人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）を実施している。

また、演習シナリオについては、NICT の有する技術的知見を活用し、サイバー攻撃の傾向を分析し、現実のサイバー攻撃事例を再現した最新のシナリオを提供している。

そのため、演習の取組を継続的に進めつつ、NICT が実施している基礎的・基盤的な研究開発の研究成果も活用しつつ、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・教育コンテンツの開発を継続的に行う必要がある。

また、特に受講実績の少ない地方公共団体の受講機会拡大を図るため、開催方法等の工夫を行うなど、運営方法についても継続的に見直しを進めることが重要である。

その上で、Ⅲ－（８）の地域の情報通信サービスのセキュリティの確保の取組と連携し、CYDER の適切な周知広報がなされることが期待される。

② 2020 東京大会に向けたサイバー演習の実施

総務省は NICT を通じ、2020 東京大会の適切な運営の確保を目的として、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「サイバーコロッセオ」を 2016 年（平成 28 年）より実施している。

本演習においては、大規模クラウド環境を用いて、公式サイト、大会運営システムや、社会インフラの情報システム等を模擬したシステムを構築し、当該システムを活用して、大会開催時を想定したサイバー攻撃を模擬し、大会組織委員会のサイバーセキュリティの担当者を中心に、攻撃側と防御側の手法の検証及び訓練を行っている。

また、2018 年（平成 30 年）より講義形式でサイバーセキュリティ関係の知識や技能を学ぶコロッセオカレッジを開設したほか、実機演習についても演習シナリオのレベル分けを増やすなど、必要に応じて見直しを実施している。

来年に開催される 2020 東京大会の円滑な実施に向け、大会事務局等と連携しつつ、引き続き本演習の取組を着実に実施する必要がある。

③　若手セキュリティ人材の育成の促進

総務省では NICT を通じ、未来のサイバーセキュリティ研究者・起業家の創出に向けて、サイバーセキュリティ分野の第一線で活躍する研究者・技術者が 25 歳以下の若手 ICT 人材に対し、実際のサイバー攻撃関連データに基づいたセキュリティ技術の研究・開発について、１年かけて継続的かつ本格的に指導する「SecHack365」を 2017 年（平成 29 年）から実施している。

我が国のサイバーセキュリティの確保に向け、セキュリティイノベーターの育成を推進するため、引き続き、本取組を進める必要がある。

④　地域のセキュリティ人材育成

サイバーセキュリティ人材の育成は重要な政策課題となっているが、特に地域においては人材の確保が一層厳しい状況にある。昨今のサイバー攻撃は地理的な距離に関係なく、弱いところをターゲットとする傾向にあることから、セキュリティ人材の裾野を広げ、地域のセキュリティ人材を底上げすることが必要である。

そのため、本タスクフォースの下に、サイバーセキュリティ人材の育成に関する課題を整理し、その在り方について検討を行うことを目的とする「サイバーセキュリティ人材育成分科会」を 2018 年（平成 30 年）12 月に設置し、2019 年（平成 31 年）６月に第一次取りまとめがなされたところである。

具体的には、地域のサイバーセキュリティに関し、以下の三つの課題が存在する。

１）研修機会の不足

サイバーセキュリティに関する研修や気づきを得る機会は、都市部に集中しており、地域での研修機会が少ない状況にある。

２）組織体制の不足

地域の中小企業等では、CISO や CSIRT 等の体制が整っていない場合が多く、特に規模が小さい組織ほど、サイバーセキュリティ体制が整っていない状況にある。

３）就業機会の不足

サイバーセキュリティ関連企業においても人材は不足しており、地域や中小企業向けのビジネスには十分に手が回っていない状況にある。また地域においてはサイバーセキュリティに関する雇用の受け皿がなく、地域の人材が地元に根付かない状況にある。

上記の課題認識を踏まえ、以下の施策に取り組む必要がある。

１）地域のセキュリティリーダーの育成

地域の中小企業等にサイバーセキュリティに関する気づきを与えるためのコミュニティ活動を活性化するため、地域でリーダーとなる人材を育成するためのカリキュラムの体系化や研修コンテンツの作成を行うモデル事業を実施する必要がある。

なお、カリキュラムや研修コンテンツの検討にあたっては、サイバーセキュリティだけでなく、中小企業等の経営層の関心を惹く内容を含め、地域の多様なステークホルダーを巻き込むためのノウハウも盛り込むことが必要である。

２）地域でのセキュリティ人材のシェアリング

サイバーセキュリティの専門家や専門組織を、得意分野や知識レベルで細分化してデータベース化した上で、必要とする中小企業等とのマッチングや複数の中小企業等間でのシェアリングのモデル事業を実施することが必要である。

その際、監査やリスクマネジメント経験のあるシニア人材、U・I ターン人材、セカンドキャリアを地域への貢献に活かそうとする人材、産休・育休からキャリア復帰を目指す女性人材などの活用が期待される。

３）地域における人材エコシステムの形成

地域の民間企業等と連携し、民間による雇用の受け皿創出の動きに合わせ、就業の場の確保と就業につながる研修を一体的に行うことを通じて、地域における人材エコシステムの形成を図るためのモデル事業を実施することが必要である。

さらに、高等教育機関と連携することにより、高度なセキュリティ人材の輩出や、下請的な業務にとどまらないハイエンドなサイバーセキュリティビジネスの地場産業化を通じて、より高次のエコシステムの形成が期待される。

（３）国際連携の推進

サイバー空間は国境を越えて利用される領域であり、サイバーセキュリティの確保のためには国際連携の推進が必要不可欠である。そのため、米国をはじめとする G7 各国を中心に、二国間及び多国間の枠組みの中で本分野における情報共有や国際的なルール作り（サイバー空間における国際法の適用関係の明確化や国際規範の具体化）を多様なルートで進めつつ、情報通信サービス・ネットワーク分野の具体的な施策、研究開発、人材育成・普及啓発、情報共有・情報開示の取組などを進めていく必要がある。

特に 2019 年（令和元年）には、G20 が我が国で開催されたが、我が国としては、サイバーセキュリティ分野における国際協調に向けて今後も主導的な役割を果たしていくことが求められる。その際、サイバーセキュリティの確保を理由とする情報の自由な流通を阻害する動きに対しては、データの越境流通の円滑化がサイバー空間の健全な発展に不可欠であることを踏まえて対応していく必要がある。

①　ASEAN 各国との連携

アジア地域においては引き続き ASEAN 各国との協力関係の強化が必要である。具体的には、日 ASEAN サイバーセキュリティ能力構築センターにおける実践的サイバー防御演習「CYDER」等の実施を通じ、４年間（2018 年（平成 30 年）～2021 年（令和３年））で 650 人程度を目標として ASEAN のセキュリティ人材の育成支援を進める必要がある。

また、日・ASEAN サイバーセキュリティ政策会議、日 ASEAN 情報通信大臣会合及び高級実務者会合、ISP を対象とする日 ASEAN 情報セキュリティワークショップ等の定期的な開催により、我が国及び ASEAN におけるサイバーセキュ

リティの脅威をめぐる状況や IoT セキュリティ対策に関する情報交換を行うほか、ASEAN 側のニーズを踏まえつつ、ASEAN における IoT セキュリティ強化に向けた施策の導入・促進のための協力を推進することが重要である。

さらに「ICT 国際競争力強化パッケージ支援事業」等の取組を通じ、我が国における ICT の知見やノウハウを含めた成功事例の海外展開の促進を図る必要がある。

② 国際的な ISAC 間連携

サイバー攻撃には国境が存在しないため、サイバーセキュリティ対策においては、脅威情報（攻撃情報）等の国際的な共有を行うことにより、国際レベルで早期の攻撃挙動等の把握が必要不可欠である。そのため、国内の産業分野ごとに設立されるサイバーセキュリティに関する脅威情報等を共有・分析する組織である ISAC（Information Sharing and Analysis Center）において、国際的な ISAC 間等の連携を引き続き促進していく必要がある。

具体的には、国際連携ワークショップの開催等を通じて、日本の ICT-ISAC と米国の ICT 分野の ISAC との連携をさらに強化し、通信事業者、放送事業者、IoT 機器ベンダー、セキュリティベンダー等が、脅威情報やインシデント情報等を自動的に共有し、サイバーセキュリティ対策に活用することを促進することが重要である。

③ 国際標準化の推進

IoT セキュリティに係る国際標準化が ISO/IEC 及び ITU-T で議論されているところであり、関係府省庁の連携において、こうした活動に積極的に貢献していくことが重要である。具体的には、2016 年（平成 28 年）７月に IoT 推進コンソーシアムの IoT セキュリティワーキンググループにおいて策定された IoT セキュリティガイドラインを国際標準に反映する等の取組を進めることが重要である。

また、サイバーセキュリティ分野の国際標準化動向について、現状を把握しつつ、我が国として注力すべき分野について調査を行う必要がある。

さらに、Ⅲの情報通信サービス・ネットワーク分野の具体的施策について、必要に応じて国際連携の場で共有するとともに、国際標準化等の可能性について継続的に検討することが重要である。

④　サイバー空間における国際ルールを巡る議論への積極的参画

サイバー空間における国際ルール等のあり方については、国連をはじめ、G7 や G20、二国間協議等の政府が主体となる場だけでなく、ISOC（Internet Society)や ICANN(Internet Corporation for Assigned Names and Numbers)、IGF（Internet Governance Forum）等のマルチステークホルダーによる場を含め、様々なチャネルを通じて議論が進められてきている。

狭義のインターネットガバナンスのあり方について、物理的な伝送網の上に構築されたパケット伝送網については、「自律・分散・協調」を基本原則として民間主体のマルチステークホルダーによる運営が行われている。しかし、更にその上位に位置するデータ・情報流通層においては、情報の自由な流通（オープンエコノミーの確保)、個人データの越境流通、国際連携によるサイバーセキュリティの確保、サイバー空間における安全保障の確保などの様々な議論が行われているところであり、こうした議論に我が国として積極的に参画していく必要がある。

その際、サイバー空間におけるルール整備は基本的にリアル空間と同等の規制が適用されるものであり、かつ領域ごとの議論は既存の国際ルールに準拠することを基礎として議論が進められることが期待される。

さらに、Ⅲの情報通信サービス・ネットワーク分野の具体的施策について、必要に応じて国際連携の場で共有をし、海外からのフィードバックを得て施策の改善につなげる取組を継続的に進めることが重要である。

（４）情報共有・情報開示の促進

ICT の利活用が進展した現在では、サイバー攻撃を行う側が圧倒的に優位な状況にあり、サイバー攻撃を受ける側はサイバーセキュリティを協調領域と捉え、平時・有事において協力をして取り組むことが求められる。

この点で、サイバーセキュリティ基本法の一部を改正する法律（2019 年（令和元年）４月施行)によって、新たにサイバーセキュリティ協議会が創設され、官民を含めた多様な主体がサイバーセキュリティに関する情報を迅速に共有することにより、サイバー攻撃による被害を予防し、被害の拡大を防ぐための体制が構築されているところである。その他の情報共有体制も含め、脆弱性情報やサイバー攻撃に関する脅威情報のほか、サイバーセキュリティ対策に関する情報等の共有を促進し、各主体のサイバーセキュリティ対策の質を向上させることが重要である。

また、企業や組織の活動において ICT の利活用が前提となっている現在、サイバーセキュリティリスクの認識やその対策についてステークホルダーに適切な開示を行うことは、ステークホルダーへの説明責任を果たし、円滑な関係を維持する上で重要な取組となっている。

さらに、サイバーセキュリティ対策の情報開示を促進することにより、民間企業の経営層が自社の対策について認識をし、さらに他社との比較によって対策の質の向上に取り組むことが期待される。また、社内や取引先・委託先への啓蒙・啓発にも寄与するなど、情報開示は各主体のサイバーセキュリティ対策の質の向上に寄与することも期待される。

① サイバー攻撃に関する電気通信事業者間の情報共有【再掲】

脆弱性を有する IoT 機器が踏み台となったことが確認された際、被害の拡大を防止するため、ISP による、当該 ISP の利用者の端末と C&C サーバの間の通信を遮断する等の取組が必要である。

この点、総務省では、2018 年（平成 30 年）５月の改正電気通信事業法において、電気通信事業者が「送信型対電気通信設備サイバー攻撃」への対応を共同して行うため、攻撃の送信元情報の共有や C&C サーバの調査研究等の業務を行う第三者機関(認定送信型対電気通信設備サイバー攻撃対処協会。以下「認定協会」という。）を総務大臣が認定する制度を創設し、2019 年（平成 31 年）１月に一般社団法人 ICT-ISAC が認定されたところである。

今後は認定協会の活動について、マルウェアに感染している可能性の高い IoT 端末等や C&C サーバであると疑われる機器の検知や利用者への注意喚起等の電気通信事業者が行う対策に向け、円滑な実施のための支援を行うなど、取組を促進することが重要である。

また、こうした認定協会の活動や「NOTICE」の実施状況も踏まえ、電気通信事業者等が協力してサイバー攻撃への対処を行う際の基盤となる効果的な情報共有の在り方について引き続き検討することが重要である。

② 事業者間での情報共有を促進するための基盤の構築

事業者間の情報共有を促進するためには、解析・対処能力が事業者間で一様ではないことを踏まえ、情報共有の目的・利点・手順、必要とされる情報を明確化するとともに、平時・有時などの状況に応じた提供すべき情報の範囲、提供先の範囲等を明確化することが重要である。また、単に各事業者の情報を共

有するだけではなく、効果的かつ効率的に実施することが重要であり、将来的には、共有された情報に基づき、サイバー攻撃に応じた自動防御を目指すことも考えられる。

総務省では、2016 年度（平成 28 年度）及び 2017 年度（平成 29 年度）に、ICT-ISAC と連携し、サイバー攻撃に関する情報を収集・分析・配布する情報共有基盤の試行運用を行う実証事業を行い、その成果として、ICT-ISAC において、「脅威情報の情報共有基盤　利用ガイドライン」を策定しており、引き続き、同ガイドラインの普及を図ることが重要である。

また、同情報共有基盤については、米国国土安全保障省（DHS）が運営する自動情報共有システム（AIS）と連携しており、このような海外との連携の取組も促進することが重要である。

さらに、事業者においてより迅速なサイバーセキュリティ対策を促進するため、サイバー攻撃に関する情報に加え、脆弱性情報を活用し、当該脆弱性の影響を受けるソフトウェアと紐付けた形で情報を配布する仕組みの検討を行うとともに、機械学習を活用したサイバー攻撃に関する情報の分析及び対策の自動化に向けた検討を実施するなど、サイバーセキュリティの更なる強化に資する情報共有基盤の構築を促進することが必要である。

③　サイバーセキュリティ対策に係る情報開示の促進

民間企業においては、複雑・巧妙化するサイバー攻撃に対する対策強化を進める動きが見られるようになってきており、こうした取組をさらに促進するためには、サイバーセキュリティ対策を講じている企業が、その対策の在り様について適切に開示をし、様々なステークホルダーから評価される仕組みを構築していくことが求められる。

このような状況を踏まえ、2017 年（平成 29 年）12 月より本タスクフォースの下に「情報開示分科会」を設置し、民間企業の情報開示の促進に向けた議論を実施してきたところであり、2018 年（平成 30 年）６月に報告書を公表したところである。

当該報告書を受け、まずは、民間企業のサイバーセキュリティ対策の自主的な情報開示を促進する観点から、2019 年（令和元年）６月に、民間企業の実際の開示事例等を盛り込んだ「サイバーセキュリティ対策情報開示の手引き」が策定・公表されたところである。

今後は民間企業の情報開示を促進するため、本手引きを策定して普及を図る

とともに、必要に応じて手引きの見直し等の検討を行うことが重要である。

④　サイバーセキュリティ対策に係る投資の促進

上述のとおり、情報開示の促進を通じて民間企業におけるサイバーセキュリティ対策の質の向上が進むことが期待されるが、併せて、民間企業のサイバーセキュリティ対策に関する投資が促進されるような環境整備（インセンティブの付与を含む）が必要である。

この点、一定のサイバーセキュリティ対策が講じられたデータ連携・利活用により、生産性を向上させる取組について、それに必要となるシステムや、センサー・ロボット等の導入を支援する税制措置（コネクテッド・インダストリーズ税制[18]）が 2018 年（平成 30 年）に創設され、2020 年（令和２年）までの３年間の適用期間で運用されているところである。

そのため、当該税制措置の活用状況を把握・分析しつつ、必要に応じ、企業のニーズ等を反映したサイバーセキュリティ対策に係る投資の促進のための政策支援の在り方について検討を行うことが期待される。

⑤　国際的な ISAC 間連携【再掲】

サイバー攻撃には国境が存在しないため、サイバーセキュリティ対策においては、脅威情報（攻撃情報）等の国際的な共有を行うことにより、国際レベルで早期の攻撃挙動等の把握が必要不可欠である。そのため、国内の産業分野ごとに設立されるサイバーセキュリティに関する脅威情報等を共有・分析する組織である ISAC（Information Sharing and Analysis Center）において、国際的な ISAC 間等の連携を引き続き促進していく必要がある。

具体的には、国際連携ワークショップの開催等を通じて、日本の ICT-ISAC と米国の ICT 分野の ISAC との連携をさらに強化し、通信事業者、放送事業者、IoT 機器ベンダー、セキュリティベンダー等が、脅威情報やインシデント情報

[18]　当該税制を利用しようとする事業者は、生産性向上特別措置法（平成 30 年法律第 25 号）に基づき、データの安全管理の方法や、その内容の適正性及びその運用について担保する情報処理安全確保支援士（登録セキスペ）等を記載することとしている「革新的データ産業活用計画」を作成し、主務大臣に提出し、「生産性向上特別措置法第二十九条の規定に基づく生産性の向上に特に資するものとして主務大臣が定める基準」（平成 30 年内閣府、総務省、財務省、文部科学省、厚生労働省、農林水産省、経済産業省、国土交通省、環境省告示第２号）に適合することについてその確認を受け、その認定を受けることにより、同計画に基づき取得又は制作するソフトウェア、器具用品、機械装置に対して特別償却 30％又は税額控除３％（平均給与等支給額の対前年度増加率が３％以上となる場合は５％）を措置することとしている。

等を自動的に共有し、サイバーセキュリティ対策に活用することを促進することが重要である。

Ⅴ　今後の進め方

「IoT・5G セキュリティ総合対策」の推進に際しては、定期的に検証を行い、進捗状況を把握するとともに、本分野における技術革新や最新のサイバー攻撃の態様を踏まえ、必要に応じて随時見直しを行っていくことが望ましい。また、対策の推進に際しては、内閣官房内閣サイバーセキュリティセンターや経済産業省をはじめとする関係府省庁や地方公共団体及び民間企業等との連携の下に進めていく必要がある。

「IoT・5G セキュリティ総合対策」の推進は、2020 年東京大会の成功に向けても必須である。重要インフラの防御対策強化の観点を含め、関係するステークホルダーの連携によるビジョンの共有と取組の強化が不可欠である。