資料 33-２

ICT サイバーセキュリティ総合対策 2021
（案）

令和３年 XX 月

サイバーセキュリティタスクフォース

目次

はじめに

デジタル改革やデジタルトランスフォーメーションを通じたSociety5.0の実現に向けて、IoTや5Gをはじめとするの普及が進展しており、さらにサイバー空間があらゆる主体が参画する、いわば公共空間へと進化しつつある中で、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。

これまでサイバーセキュリティタスクフォース（座長　情報セキュリティ大学院大学学長　後藤厚宏）では、IoT・5Gの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を行ってきたところであり、2020年（令和２年）７月に「IoT・5Gセキュリティ総合対策2020」として提言を取りまとめたところである。同提言の策定後も、例えば、デジタル庁の設置を始めとするデジタル改革関連法案が成立するなど、サイバー空間を取り巻く多様な状況変化が見られているところであり、それに応じて、必要なサイバーセキュリティ対策もまた変化している。また、本年は政府におけるサイバーセキュリティに関する施策の基本的方針等を定める「サイバーセキュリティ戦略」の改定も予定されている。

本文書は、こうした状況の変化を踏まえつつ、同提言の策定後の議論を経て、必要な改定を行ったものである。改定に当たっては、ICT（情報通信技術）インフラやサービス全般のサイバーセキュリティ確保が、社会全体のデジタル改革・デジタル・トランスフォーメーションの実現、また、自由、公正、かつ安全なサイバー空間の実現のための前提として、極めて重要な政策課題であるとの考えの下、IoT・5Gにとどまらず、広くICTインフラ・サービス等に関する対策を盛り込むとともに、それを踏まえ、提言のタイトルについても、「ICT サイバーセキュリティ総合対策 2021」に改定したものである。本文書を羅針盤として、総務省が関係機関や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を期待する。

Ⅰ　改定に当たっての主要な政策課題

（１）昨年の「IoT・5G セキュリティ総合対策 2020」以降の状況変化

本タスクフォースでは、2020 年（令和２年）７月に、「IoT・5G セキュリティ総合対策 2020」を提言として公表したところであるが、その際、主要な政策課題として以下の４点を掲げたところである。

- ・COVID-19 への対応を受けたセキュリティ対策の推進
- ・5G の本格開始に伴うセキュリティ対策の強化
- ・サイバー攻撃に対する電気通信事業者のアクティブな対策の実現
- ・我が国のサイバーセキュリティ情報の収集・分析能力の向上に向けた産学官連携の加速

同提言の公表後も、COVID-19 の感染拡大防止のために人の移動が制限され、テレワーク活用等の社会のデジタル化が進展するなど、提言に記載した課題が継続する一方で、COVID-19 への対応において、行政サービスにおける様々な課題が明らかになり、真の行政のデジタル化の実現が求められ、政府においてはデジタル庁の設置に向けた議論が行われるようになった。また、我が国の様々な課題の解決と今後の経済成長に資する観点から、行政のデジタル化のみならず、国民による社会経済活動全般のデジタル化の推進、すなわち、社会全体のデジタル・トランスフォーメーション(DX)の推進が、「新たな日常」の原動力としてより一層重要な政策課題と認識されるようになった。

そして、政府においては、「デジタル社会の実現に向けた改革の基本方針」を決定したところであるが（令和２年 12 月 25 日閣議決定)、同閣議決定においては、デジタル社会のビジョンとして「デジタルの活用により、一人ひとりのニーズに合ったサービスを選ぶことができ、多様な幸せが実現できる社会」を掲げ、このような社会の実現に向けて、「誰一人取り残さない、人に優しいデジタル化」を目指し、行政を含む社会全体のデジタル改革や DX を強力に進めることとしている。

また、サイバーセキュリティ基本法に基づいて、我が国のサイバーセキュリティ施策の推進に当たっての基本的方針等を定める「サイバーセキュリティ戦略」についても、３年前に策定した現戦略の改定に向けて、現在サイバーセキュリティ戦略本部において検討が進められているところである。同戦略本部で議論された次期サイバーセキュリティ戦略の骨子[1]においては、サイバー空間があらゆる主体が参画する公共空間へと進化する中で、「誰一人取り残さない」サイバー

[1] https://www.nisc.go.jp/conference/cs/dai28/pdf/28shiryou01.pdf

セキュリティの確保（“Cybersecurity for All”）に向けた取組を進める必要があるとの考え方の下、「DX とサイバーセキュリティの同時推進」「公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保」「安全保障の観点からの取組強化」を通じて「自由、公正、かつ安全なサイバー空間」を確保するとの方向性が示されているところである。

これら閣議決定に定めるデジタル社会のビジョンやサイバーセキュリティ戦略本部が目指す「自由、公正、かつ安全なサイバー空間」の実現に当たって、IoT や５Ｇを含む ICT（情報通信技術）に係るインフラやサービスは、その基盤となるものである。したがって、社会全体のデジタル改革・DX 推進を進めるためには、国民一人ひとりがその基盤となる ICT を安心して活用できるよう、サイバーセキュリティを確保することが、いわば不可欠の前提としてますます重要になっている。

これまで本タスクフォースにおいては、上記「IoT・5G セキュリティ総合対策 2020」の公表後も、同提言に掲げた施策の進捗状況等の確認を行いつつ、新たな課題への対応や施策展開の加速化を図るための議論を継続して実施してきたところである。

以上のとおりの状況変化や昨年の提言の公表後の議論を踏まえて、「IoT・5G セキュリティ総合対策 2020」を改編し、新たな施策を盛り込む形で「ICT サイバーセキュリティ総合対策 2021」を策定することするものである。

なお、新たな提言を策定するに当たっては、「IoT・5G セキュリティ総合対策 2020」に掲げた施策の進捗状況を適切に把握し、それを踏まえた上で、新たな施策の方向性等を示していくことが適当である。こうした観点から「IoT・5G セキュリティ総合対策 2020」に掲げた施策の総務省における進捗状況について、別添において「プログレスレポート 2021」としてまとめている。

（２）状況変化等を踏まえた主要な政策課題

上記（１）の状況変化等を踏まえて、「ICT サイバーセキュリティ総合対策 2021」の策定に当たっては、社会全体のデジタル改革・DX を推進するに当たって、その前提として、国民が安心してデジタルを活用できる環境を整備する観点からサイバーセキュリティを確保すること、すなわち、「デジタル改革・DX 推進の前提としてのサイバーセキュリティの確保」が喫緊の政策課題であるという認識の下、そのための施策を重点的に推進していくことが適当である。

（３）主要な政策課題への対処のための施策の整理・分類

上記（２）で示した「社会全体のデジタル改革・DX 推進の前提としてのサイバーセキュリティの確保」という主要な政策課題に対処するために、総務省において重点的に推進すべき施策としては、大まかに次のとおり分類することができると考えられる。

①電気通信事業者における安全かつ信頼性の高いネットワークの確保のためのセキュリティ対策の推進

社会全体のデジタル改革や DX が進展すると、国民の生活や経済活動に必要な多くのやりとりが、電気通信事業者が設置しているネットワークを通じて、また、電気通信事業者が提供している電気通信サービスを利用して、行われることとなる。また、今後 5G の本格的な展開が見込まれ、電気通信事業者のネットワークやサービスは 5G が主流になっていく。そのため、今後、デジタル社会の実現に向けた改革を進め、国民一人ひとりが安全に安心してデジタルを活用していくためには、5G のセキュリティ対策の強化も含め、電気通信事業者のネットワークにおけるリスクの高まりに応じた適切なセキュリティ対策を講じ、電気通信事業者における安全かつ信頼性の高いネットワークを確保していくことが重要である。

②COVID-19 への対応を受けたセキュリティ対策の推進

総務省においては、2020 年（令和２年）７月の「IoT・5G セキュリティ総合対策 2020」策定・公表以降、COVID-19 への対応を受けたテレワークシステム等の ICT 利用の促進のためのセキュリティ対策を進めてきたところである。一方で、COVID-19 の感染拡大が続く中、特に中小企業等におけるテレワークの普及・定着にはいまだ課題もあるところであり、その対策の強化は急務である。また、ICT を安全・安心に利用するためのサイバーセキュリティの重要性は、COVID-19 後のいわゆるニューノーマルの社会においても同様であり、中期的な視点も視野も入れつつ、引き続き COVID-19 への対応を受けたセキュリティ対策に取り組むことが重要である。

③デジタル改革・DX 推進の基盤となるサービス等のセキュリティ対策の推進

社会全体のデジタル改革や DX は、IoT やクラウドサービス等のサービスの利用や、それらのサービスを組み合わせたユースケースであるスマートシティの構築・運営を通じて進展すると考えられる。今後、デジタル社会の実現に向けた改革を進め、ICT の活用を促進していくためには、このようなデジタル改革・DX 推進の基盤となるサービス等における課題に応じた適切なセキュリテ

ィ対策を講じ、これらのサービス等を国民一人ひとりが安心して利用できる安全な環境を整備していくことが重要である[2]。

④サイバーセキュリティ情報に関する産学官での連携・共有等の促進

デジタル改革・DX 推進の前提としてサイバーセキュリティを確保するためには、サイバー攻撃等に関する情報の収集・分析等を行い、有効な技術や知見を生み出すとともに、それらを関係者間で共有し、社会全体でのセキュリティ対策の底上げを図ることが有用である。そのため、産学官連携してのサイバー攻撃等に関する情報の収集・分析等や適切な共有・公表等を進めることが重要である。

なお、サイバーセキュリティの推進のための具体的な施策は多様であり、上記①～④の大まかな分類の中に、複数の具体的な施策が含まれる。また、具体的な施策としては、例えば、個別の ICT サービスやインフラなどに係る施策のほか、これら個別の ICT 分野での施策をより効果的に実施するための横断的な施策、例えば、国際連携の推進や、研究開発の推進、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、サイバーセキュリティに関する情報共有・情報開示の促進の観点からの取組などもある。

そのため、本提言では、総務省として取り組むべき具体的な施策について、まずは「Ⅱ　情報通信サービス・ネットワークの個別分野に関する具体的施策」と「Ⅲ　横断的施策」の２つの大項目に分けた上で、上記①～③についてはⅡに、また、上記④についてはⅢに、それぞれ中項目として記載し、さらに、個々の具体的な施策を各中項目の中の小項目として記載する形で整理を行っている。

（４）施策の推進・実施に当たっての基本的な考え方・主な留意点

具体的な施策の推進・実施に当たっては、以下のような基本的な考え方・観点に留意しつつ取り組むことが適当である。

①　サイバーセキュリティ戦略に定める５つの基本原則を踏まえた施策展開

上述の「サイバーセキュリティ戦略」においては、サイバー空間を「自由、公正、かつ安全な空間」とし、同法の目的に資するため、サイバーセキュリティに関する施策の立案及び実施に当たって従うべき基本原則として、従来から、「情報の自由な流通の確保」「法の支配」「開放性」「自律性」「多様な主体の連携」の５つの原則を定めている。サイバーセキュリティ戦略本部において現在議論が進められている次期サイバーセキュリティ戦略の骨子

[2] 「＜コラム＞ＤＸとサイバーセキュリティ」（P10）を参照。

（前述）においても、サイバー空間が、人々に豊かさや多様な価値実現の場をもたらし、今後の経済社会の持続的な発展の基盤となると同時に、自由主義、民主主義、文化発展を支える基盤になっていることを踏まえ、その取り巻く環境の急速な変化にもかかわらず、目指すべきサイバー空間に対する考え方はいささかも変わるものではないとして、これら５つの原則を堅持することとしている。

これら５つの原則の価値に軽重の差はなく、サイバーセキュリティに関する施策の推進・実施に当たっては、これら５つの原則のいずれもが等しく確保されているサイバー空間こそがサイバー空間のあるべき姿であるという点に留意しつつ、各施策を推進していくことが必要である。

また、前述のとおり、「次期サイバーセキュリティ戦略の骨子」において、「DX とサイバーセキュリティの同時推進」「公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保」「安全保障の観点からの取組強化」を進めるとの方向性が示されているところであり、これらの方向性も意識しながら個々の施策を推進・実施していくことが適当である。

② サービス・製品の提供側と利用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、サービス・製品の提供側と中小企業を含む利用側の双方の観点からのサイバーセキュリティ対策を推進する必要がある。なお、サービス・製品のソフトウェア化・複雑化等により、ユーザ自身が適切な対策を講じることが困難になりつつある現状を踏まえ、サービス・製品の提供側にはこれまで以上にユーザに寄り添った対策の実施が求められる一方で、利用するユーザにおいても、提供側等からのサポートも踏まえつつ、自らの責任で適切に措置を講じるよう努めることが適当であり、そうした利用側における施策も併せて推進していくことが必要である。

③ 各施策の粒度やタイムスパン等の違いに応じた施策展開

ICT に関するサイバーセキュリティの確保のための施策の中には、例えば、政府として企業向け・個人向けに講じるべき具体的な施策がある一方で、戦略や考え方の検討を深めるべき、いわば政策的な施策や課題があるほか、喫緊の課題として短期的に取り組むべき課題と、将来の動向を見据えつつ継続的・中長期的に取り組むべき課題があるなど、粒度やタイムスパン等の異なる多様な施策がある。本提言中にもこれらの施策が混在しているが、施策展開に当たっては、各施策の粒度やタイムスパン等の違いを認識した上で、

それに応じて取り組むことにより、サイバーセキュリティの確保・強化を総合的、かつ、有機的に進めていくことが重要である。

＜コラム＞ＤＸとサイバーセキュリティ

ICT・デジタル技術と多様なデータを用いて、企業のビジネスモデルや、国民の生活・行動様式を変革し、企業の競争力の向上による経済の持続的発展やユーザの利便性の向上に結びつけること、すなわち、デジタル・トランスフォーメーション（DX）の進展が見込まれている。

急速に進展する経済のグローバル化や社会経済構造の複雑化等に機動的かつ適切に対応していくためには、DX の推進が重要である一方で、デジタル化に伴うビジネスモデルや行動様式の変化、データの取扱いや ICT システムにおける不備・不具合によるデータの漏えい等により、円滑なサービス提供や業務遂行に支障が発生するリスクも生じ得ることとなる。

我が国の社会経済を取り巻くこうした環境変化の中で、DX を強力に推進することで強靭な社会経済システムを実現し、国民の便益を最大化するためには、これらの多様なリスクに適切に対処するためのサイバーセキュリティの確保が不可欠であり、DX とサイバーセキュリティの同時推進や、サイバーセキュリティを業務、製品・サービス等のシステムの企画・設計段階から確保する、いわゆるセキュリティ・バイ・デザインの考え方が今後ますます重要になっていくと考えられる。

Ⅱ　情報通信サービス・ネットワークの個別分野に関する具体的施策

１　電気通信事業者における安全かつ信頼性の高いネットワークの確保のためのセキュリティ対策の推進

社会全体のデジタル改革やDXが進展すると、国民の生活や経済活動に必要な多くのやりとりが、電気通信事業者が設置しているネットワークを通じて行われることとなる。

他方、電気通信事業者のネットワークについては、ネットワーク技術の進展に伴いソフトウェア化等が進むことにより、柔軟で効率的な運用が可能になる一方で、技術的な脆弱性が生じるリスクも増加している。また、電気通信事業者は、例えば、5G 構築のための知見などの技術優位性を保持するための技術情報や、営業秘密などの経営上の機微情報など、その有する情報・ノウハウが、安全保障上または経営戦略上の理由から狙われやすい傾向にあると考えられる。更に、ネットワーク機器の生産・流通プロセスやサービスの開発プロセス、データ管理プロセスのグローバル化やオープン化に伴う関係者の多様化の進展に伴い、ネットワーク機器内に脆弱性が存在するなどのサプライチェーンリスクも高まりつつある。

このほか、多数のマルウェアに感染したIoT機器（監視カメラ等）を踏み台にして特定のサーバ等に大規模なDDoS攻撃を仕掛ける事例が見られる中、NICTER[3]で観測したサイバー攻撃関連通信の約半数がIoT機器を狙ったものであることについて、これまでは、パスワード設定等に不備のあるIoT機器の利用者に対する注意喚起「NOTICE[4]」など、ユーザ側・端末機器側での対策を中心として措置を講じてきたが、今後、5Gの進展によりIoT機器の一層の増加が予想される中、現状の端末機器側での対応だけでは、端末の踏み台への悪用に適切に対応することが難しくなっていくことが予想される。

今後、デジタル社会の実現に向けた改革を進め、国民一人ひとりが安全に安心してデジタルを活用していくためには、このような電気通信事業者のネットワークにおけるリスクの高まりに応じた適切なセキュリティ対策を講じ、電気通信事業者における安全かつ信頼性の高いネットワークを確保してくことが重要である。

---

[3] 国立研究開発法人情報通信研究機構（NICT）が運用するサイバー攻撃観測網。

[4] National Operation Towards IoT Clean Environmentの略。国立研究開発法人情報通信研究機構（NICT）がサイバー攻撃に悪用されるおそれのある機器を調査し、電気通信事業者を通じた利用者への注意喚起を行う取組。

そのため、主に以下の３つの施策を推進していくことが適当である。
（１）安全かつ信頼性の高いネットワークの確保
（２）サイバー攻撃に対する電気通信事業者の積極的な対策の実現
（３）５Ｇの本格的な普及に向けたセキュリティ対策の強化

（１）安全かつ信頼性の高いネットワークの確保

①ガバナンス確保の在り方に関する検討

国民生活や経済活動に必要な多くのやりとりが電気通信事業者のネットワークを通じて行われており、電気通信事業者のネットワークに対して大規模なサイバー攻撃が発生すれば、大きな被害や社会的な影響を及ぼすリスクが高まっている。実際、電気通信事業者のネットワークがサイバー攻撃の標的となるインシデント事案も発生している。また、データ処理の委託や、他事業者との連携による電気通信サービスの提供、システムの高度化・ソフトウェア化等に伴い、委託先等からの情報漏えいや設定ミス等による内部からの情報漏えいのリスクも高まっている。

そのため、電気通信事業者のネットワークへのサイバー攻撃、委託先や内部からの情報漏えいといったリスクに対して適切かつ積極的な対策を講じることにより、ネットワークや電気通信サービスの安全・信頼性を確保し、ユーザが安心して ICT を利用できる環境を確保することが必要である。

具体的には、現状では、電気通信事業者のネットワークへのサイバー攻撃や脆弱性といったリスクの高まりに対する各電気通信事業者の対策の実施状況や、サイバー攻撃によるインシデントや通信事故の発生状況を十分には把握できていないことから、各事業者の取組が適切であるか否かの検証も困難である。そこで、まずは現状を把握すべく、総務省において、2021 年（令和３年）４月より、電気通信事業者に対してセキュリティ対策の取組状況に関する調査を実施しているところである。

また、同５月、総務省において、「電気通信事業ガバナンス検討会」が立ち上げられたところであり、デジタル変革時代における安心・安全で信頼できる通信サービス・ネットワークの確保を図るため、電気通信事業におけるサイバーセキュリティ対策とデータの取扱い等に係るガバナンス確保の在り方についての検討が行われていることから、今後、同検討会の中で、上記調査の結果を踏まえて、電気通信事業者による取組等の現状が、サイバー攻撃の複雑化・巧妙化や脆弱性の高まりといったリスクへの対策として適切であるか否かを検証していくことが適当である。

このほか、現在の IP ネットワークを構成する根幹技術である BGP や DNS に関しては、効果的な脆弱性対策の手法が検討されているが、広く電気通信事業者等に普及するには至っていない状況にあることから、これらについても、併せて普及方策等を検討することが適当である。

②通信事故の報告・検証制度の在り方の検討

現在、「情報通信審議会情報通信技術分科会 IP ネットワーク設備委員会」の下で開催されている「事故報告・検証制度等タスクフォース」において、通信サービス・ネットワークの安全・信頼性対策に関する PDCA サイクルについて、リスクマネジメントの考え方を踏まえ、デジタル社会における通信事故の防止や被害の拡大防止等という目的に向け、マルチステークホルダーにおける取組との連携・協力を推進し、通信事業者が引き続き主導的な役割を担うことができる環境整備の必要性が検討されている。

当該 PDCA サイクルの要である通信事故の報告・検証制度の今後の在り方については、環境変化に伴うリスクの量的・質的な変化等に対し、社会全体で対応可能な強靱性・実効性を確保するため、重大なリスクに関する OODA ループ[5]的な対応やリスク評価機能の強化の観点から、その見直しの検討が期待される。

（２）サイバー攻撃に対する電気通信事業者の積極的な対策の実現

IoT のセキュリティ対策としては、これまで端末側の対策として、電気通信事業法（昭和 59 年法律第 86 号）における端末設備等規則（昭和 60 年郵政省令第 31 号）へのセキュリティ要件の導入や、パスワード設定に不備のある IoT 機器やマルウェアに感染している機器の利用者への注意喚起といった取組を実施してきた。

しかしながら、IoT を狙った攻撃は依然として多く、また、今後、5G の進展により様々な産業で IoT 機器の利用が更に拡大することが予想される中、これまでの対策だけでは必ずしも十分ではないおそれがある。

[5] 「Observe（観察）」「Orient（状況判断、方向づけ）」「Decide（意思決定）」「Act（行動）」の 4 つのサイクルのこと。「PDCA」が計画（Plan）から始まるのに対して、OODA ループは状況等の観察（Observe）から始まる。

図１　IoT 機器を狙った攻撃の増加

（NICTER により１年間に観測されたサイバー攻撃回数）

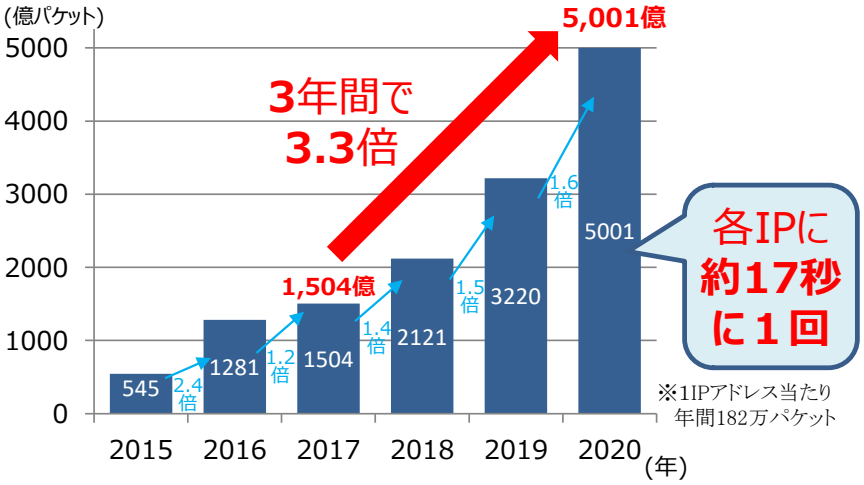
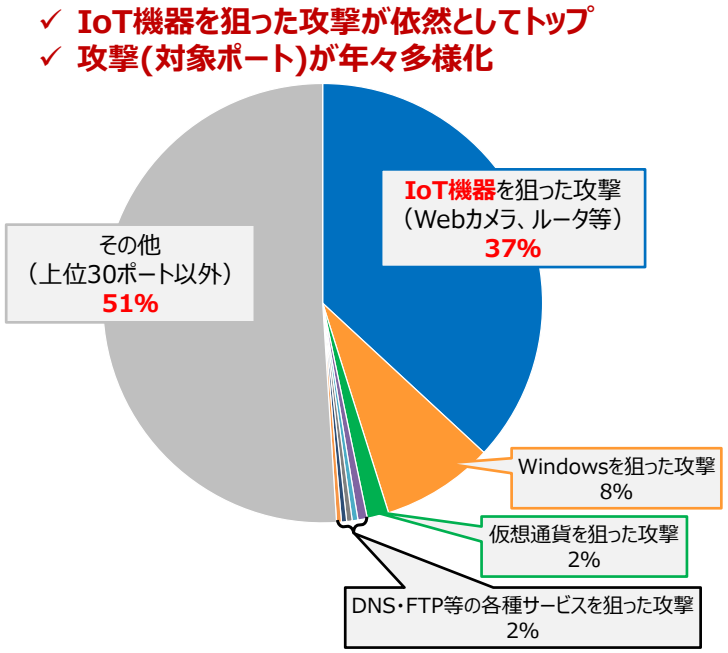


図２　IoT 機器を狙った攻撃の割合



※　NICTERで2020年に観測されたもの（調査目的の大規模スキャン通信を除く。）について、上位30ポートを分析したもの。なお、IoT機器を狙った攻撃は多様化しており、ポート番号だけでは分類しにくいものなど、「その他」に含まれているものもある。

そのような中、IoT のセキュリティ対策をより実効的なものにするためには、トラフィックが通過するネットワーク側でより機動的な対処を行う環境整備が必要と考えられる。

このため、ユーザ側で運用している情報通信機器や情報システムのセキュリティ対策と連動する形で、インターネット上で ISP が管理する情報通信ネッ

トワークにおいても高度かつ機動的な対処を実現するための方策の検討が必要である。

具体的には、電気通信事業者が自らトラフィックの流れ（フロー情報）を把握・分析して攻撃元の C&C サーバ（マルウェアに感染した端末に対して指令を与えるサーバ）を検知し、検知した C&C サーバに関する情報を電気通信事業者間で共有し、サイバー攻撃の予兆を捉えて早期に対処できるようにするため、通信の秘密に配慮した適切な対応を電気通信事業者が円滑に行うことが求められるところ、制度的な観点から対策の検討を行うことが重要である。なお、中長期的な課題として、通信の秘密の保護を図りつつ、より迅速なセキュリティ対策を実現するために、必要に応じ新たな視点からも検討を行うことが適当と考えられる。

また、フロー情報分析による C&C サーバ検知の手法について、現場での実証を行い、技術面・運用面での課題を検証し、検知の高度化を図るなど、新技術を活用した対策の高度化を促進することが適当である。

なお、脆弱性を有する IoT 機器を踏み台とするサイバー攻撃による被害の拡大を防止するためには、電気通信事業者間で攻撃元の情報を共有するなど、各電気通信事業者が協力・連携して対応することが重要であり、総務省においても引き続き電気通信事業者間の協力・連携を促進するための取組を進めていくことが必要である。

またこの点に関連して、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が設けられたところである。同制度を踏まえ、2019 年（平成 31 年）１月には、一般社団法人 ICT-ISAC[6]が認定協会としての認定を受けたところであり、総務省においては、本制度による取組の効果を向上させるため、今後ともこれらの取組への支援等に努めることが適当である。

---

[6] 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。

（３）5G の本格的な普及に向けたセキュリティ対策の強化

わが国では、2020 年（令和２年）より、携帯電話事業者が一般向け 5G サービスの提供を開始したほか、ローカル 5G[7]についても運用が始まりつつある。5G 通信ネットワークは、わが国の社会経済と国民生活を支える極めて重要な社会基盤であり、構築の段階から運用に至るまで、セキュリティ・バイ・デザインの考え方に基づき、安全性や信頼性の確保を進めることが適当である。

総務省では、こうした観点から、次に掲げるように、制度、技術、情報共有、市場、振興及び国際等の各種の政策手段を活用し、総合的に 5G のセキュリティ確保に取り組んでいる。

・5G の制度面におけるサプライチェーンリスク対策: 5G 周波数の割当てにおいてサプライチェーンリスク対策を条件化

・5G を念頭にした不正な機能や脆弱性の技術検証: 5G の商用の通信ネットワークを念頭に、システムに組み込まれた不正な機能や脆弱性を効率的に検出するための能力構築と技術開発を推進中。毎年度の取組を本 TF で報告するとともに、成果の一部を「5G ネットワーク構築におけるセキュリティに関する対策等の留意点（令和 2 年度版)」として公表し、周知・啓発

・5G セキュリティに関する民間ベースの情報共有: ICT-ISAC において「5G セキュリティ推進グループ」が活動推進中

・5G インフラ市場のオープン化とベンダー多様化: サプライチェーンリスク軽減に資するべく、5G ネットワーク機器のベンダー多様化のため、異なるベンダー間の 5G ネットワーク機器の相互接続規格「O-RAN[8]」の普及を進めており、O-RAN 準拠機器の相互接続性検証等の拠点である「OTIC[9]」の国内での具体化にむけて取組中

・安全性・信頼性等の確保された 5G の導入促進: サプライチェーンリスク対策を含む安全性・信頼性やオープン性等を満たす 5G ネットワーク機器を認定し、税制優遇措置によって通信事業者による当該機器の導入を促進

[7] 地域ニーズや個別ニーズに応じて様々な主体が利用可能な第５世代移動通信システム。

[8] モバイルネットワーク設備のオープン化等を推進することを目的に 2018 年２月に設立された団体 O-RAN アライアンス（Open Radio Access Network Alliance）において定められた規格。

[9] Open Test and Integration Center の略。携帯電話事業者や基地局ベンダー等が対象機器のオープンな規格への準拠を確認・試験するためのテストベッド。

・国際連携: G7 やプラハ会議等の多国間会合や各国との二国間会合を活用し、5G セキュリティ関連の意見交換や連携しての対外発信

こうした 5G セキュリティに関する既存の施策を着実に遂行し、わが国の基幹的重要インフラである 5G 通信ネットワークの安全性と信頼性を確実なものとすべきである。

加えて、5G においては、モバイルエッジコンピューティング（MEC）[10]の本格活用や、ネットワークの仮想化・ソフトウェア化によるリソースの動的制御やネットワークスライシング、ローカル 5G の一層の進展等により、例えば、スマートシティの構築の基盤として活用されるケースを含めて、これまでとは異なる多岐にわたるユースケースが想定されている。この際、ネットワークを整備・運用する電気通信事業者側におけるセキュリティ確保はもちろんのこと、5G の特性を活かして様々に利用しようとするユーザ側においても、ユースケースに応じて必要なセキュリティ対策を自ら行う必要がある。今後、5G の利用が本格化する中、政策の遂行にあたっては、こうした点も留意すべきである。

また、このような 5G セキュリティに関する既存施策を着実に実施すると共に、Beyond 5G・6G[11]を念頭に、サイバー空間に関する将来動向を把握し、新たな研究開発要素も含め、国として推進すべきセキュリティ面での取組を検討することが適当である。

例えば、現在、将来のサイバー空間のガバナンスやルール形成に向けた標準化等の国際的な議論が進められている。Beyond 5G・6G に向け、将来のサイバー空間のガバナンスに大きな影響を与え得る情報通信アーキテクチャをめぐる国際的な議論の一部においては、我が国が掲げる「自由、公正かつ安全なサイバー空間」とは異なる空間を指向する提案も行われている。こうした動向を主体的に把握し、サイバー空間のガバナンスやルールの形成に積極的に関与していくため、関係する国際的な議論の状況の調査及び国内における議論の活性化に資する取組を実施することが適当である。

[10] データ処理をクラウドなどのインターネット上のサーバで行うのではなく、基地局の近くに設置するサーバ（エッジサーバー）で処理することで、利用者への迅速な応答が可能となる技術。

[11] 5G の特長の更なる高度化に加えて、あらゆる機器が自律的に連携し、最適なネットワークを構築する自律性、地球上のどこでも通信を可能とする拡張性、セキュリティ・プライバシーが常に確保される超安全・信頼性、データ処理量の激増に対応できる超低消費電力、といった機能を実装した次世代の移動通信システム

２　COVID-19 への対応を受けたセキュリティ対策の推進

COVID-19 については、2021 年（令和３年）７月 14 日 15 時時点で世界全体での感染者数が約 1 億 8,775 万人、うち死亡者数が約 405 万人、同日 0 時時点で日本での感染者数が約 82.5 万人、うち死亡者数が 14,971 人にも及んでいる状況であり、世界全体として未曾有の事態に直面している。

我が国においては、2020 年（令和２年）２月以降、人の移動を抑制し、患者・感染者との接触機会を減らす観点から、テレワークや時差出勤の推進等を強力に推進してきた。その結果、様々な組織において、テレワークシステムを活用した在宅勤務やクラウド型の Web 会議システムを活用したミーティング、押印を省略した対面を前提としない手続の整備などが進んでいるところである。

しかしながら、COVID-19 の感染拡大が続く中、特に中小企業等におけるテレワークの普及・定着にはいまだ課題もあるところであり、その対策の強化は急務である。また、上記のような COVID-19 への対応における行動変容は、2021 年においても継続しており、また、感染拡大が終息に向かい又は終息を迎えた後も維持され、その結果、生き方・住み方・働き方をはじめとする人々の価値観や社会・コミュニティ・経済の在り方が大きく変わっていくと考えられる。

その際、時間や距離の壁を越えることを可能にする ICT の役割はこれまで以上に大きくなっていくと考えられ、同時にそのような ICT を安全・安心に利用するためのサイバーセキュリティの重要性が益々高まることが想定される。総務省においては、2020 年（令和２年）７月の「IoT・5G セキュリティ総合対策 2020」策定・公表以降、COVID-19 への対応を受けたセキュリティ対策を進めてきたところであるが、今後も引き続きこのような対策に取り組むことが重要である。

具体的には、COVID-19 への対応を受けたセキュリティ対策として、以下の２点を推進することが適当である。

（１）テレワークセキュリティの確保
（２）トラストサービスの制度化と普及促進

（１）テレワークセキュリティの確保

テレワークにおいては、インターネット経由でオフィスのネットワークへアクセスしたり、私用端末を利用したりすることも想定されることから、これらに対応したセキュリティ対策を実施する必要がある。実際に、テレワーク導入企業に対するアンケートでもセキュリティの確保が最大の課題とされている

[12]。

こうした状況を踏まえ、総務省では、「テレワークセキュリティガイドライン」や、セキュリティの専任担当がいない場合や、担当が専門的な仕組みを理解していない場合でも、最低限のセキュリティが確実に確保されることに焦点を絞った「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）」等を策定し、2021 年（令和３年）５月に最新のセキュリティ動向等を踏まえた改定を実施している。これらガイドライン類について、関係省庁や関連団体・企業等とも連携するとともに、オンラインコンテンツ(動画等)の活用も検討しつつ、テレワーク実施企業やテレワーク勤務者に広く周知していく必要がある。

また、コロナ後の対応も見据え、民間企業等におけるテレワークセキュリティの実態を引き続き調査するとともに、当該調査結果やセキュリティ動向等を踏まえつつ、テレワークセキュリティガイドラインの再改定の必要性を検討するほか、チェックリストについては、セキュリティに関するリテラシーが十分でない場合にも、その内容が適切に伝わるよう、記載内容の見直しや表現ぶりの改善を含めた検討を引き続き実施することが重要である。

（２）トラストサービスの制度化と普及促進

実空間とサイバー空間が高度に融合する Society5.0[13]の実現に向け、データを安心・安全に流通できる基盤の構築が不可欠であり、データの改ざんや送信元のなりすまし等を防止する仕組みであるトラストサービスの重要性が高まっている。

また、COVID-19 の感染拡大に伴い、テレワーク等の推進が求められ、あらゆるやり取りをデジタル完結する要請が高まる中、トラストサービスが重要な役割を果たすことがより一層期待されているところである。

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」を立ち上げ、我が国のトラストサービスの在り方に関する検討を行い、2020 年 2 月に最終取りまとめを提示してトラストサービスについて次の取組の方向性を示した。

---

[12] テレワークセキュリティに関する実態調査結果（2020 年度 2 次実態調査）
https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

[13] 狩猟社会、農耕社会、工業社会、情報社会に続く、人類史上５番目の新しい社会。新しい価値やサービスが次々と創出され、社会の主体たる人々に豊かさをもたらしていく。
（出典：未来投資戦略 2017（平成 29 年６月９日閣議決定））

① 電子データがある時刻に存在し、その時刻以降に改ざんされていないことを証明するタイムスタンプについては、国が信頼の置けるタイムスタンプサービス・事業者を認定する制度を創設することが適当。

② 電子データの発行元の組織を簡便に確認することができる e シールについては、信頼の置けるサービス・事業者に求められる技術上・運用上の基準を策定し、これに基づく民間の認定制度を創設することが適当。

③ リモート署名[14]については、民間団体において策定されるガイドライン等の精査等の取組を進めながら、電子署名法上の位置付けについて検討を行うことが適当。

当該提言を踏まえ、タイムスタンプについては、2020 年（令和２年）に「タイムスタンプ認定制度に関する検討会」を立ち上げ、現行の民間の認定制度である「タイムビジネス信頼・安心認定制度」が抱える課題や EU 等の国際的な制度との整合性等の観点から議論を行い、その結果を踏まえ、2021 年（令和３年）４月に「時刻認証業務の認定に関する規程（令和３年総務省告示第 146 号）」を公布、国による認定制度を整備した。

e シールについては、2020 年（令和２年）４月に「組織が発行するデータの信頼性を確保する制度に関する検討会」を立ち上げ、e シールの利用が有効なユースケースや我が国の e シールの在り方等について検討を行い、その結果を踏まえ、今後、我が国の e シールにおける信頼の置けるサービス・事業者に求められる技術上・運用上の基準等について整理した「e シールに係る指針」を作成し、2021 年（令和３年）６月に公表した。

電子署名については、回答書の公表を通じてリモート署名の電子署名法上の位置づけを示し、また、新しく登場したクラウド技術を活用した立会人型電子署名（利用者の指示に基づきサービス提供者自身の署名鍵による暗号化等を行う電子契約サービス）については電子署名法における取扱いが不明確であったことから、2020 年（令和２年）７月に「電子署名法２条１項に関する Q&A」を、同年９月には「電子署名法３条に関する Q&A」を公表する等、電子署名法上の電子署名の利便性の改善に向けた取組を実施した。

今後引き続きこれまでに整備した国による認定制度を適切かつ確実に運用するとともに、政府におけるデータ戦略、とりわけトラストサービスの基盤となる枠組みの創設に向けた検討の動向を踏まえ、e デリバリー（電子的な配達

[14] サービス提供事業者のサーバに利用者の署名鍵を設置・保管し、利用者がサーバにリモートでログインした上で自らの署名鍵で当該事業者のサーバ上で電子署名を行うこと。

証明付き内容証明郵便に相当)等トラストサービスのさらなる利用の拡大に向けた検討を行うことが適当である。

３　デジタル改革・DX 推進の基盤となるサービス等のセキュリティ対策の推進

社会全体のデジタル改革や DX は、IoT やクラウドサービス等のサービスの利用や、それらのサービスを組み合わせたユースケースであるスマートシティの構築・運営を通じて進展すると考えられる。

他方、(a)IoT については、NICTER で観測したサイバー攻撃関連通信の約半数が IoT 機器を狙ったものであること、(b)クラウドサービスについては、情報の漏えいやサービスの稼動停止といったインシデントが依然として発生していること、(c)スマートシティについては、特に様々なデータを連携させるに当たって、その運営に参加する多様な関係者に対してセキュリティの考え方やセキュリティ対策を徹底する必要があること、といったセキュリティ上の課題が存在する。

今後、デジタル社会の実現に向けた改革を進め、国民一人ひとりが安全に安心してデジタルを活用していくためには、このようなデジタル改革・DX 推進の基盤となるサービス等における課題に応じた適切なセキュリティ対策を講じ、これらのサービス等を安全に安心して利用できる環境を整備してくことが重要である。

そのため、以下の３つの施策を推進していくことが適当である。
（１）IoT のセキュリティ対策
（２）クラウドサービスの利用の進展を踏まえた対応
（３）スマートシティのセキュリティ対策

（１）IoT のセキュリティ対策

①　IoT 機器の設計・製造・販売段階での対策

IoT 機器の設計・製造・販売段階においては、製造事業者における 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、電気通信事業法の枠組みにおいて端末設備等規則を改正し、強制規格としての技術

基準が策定され、その運用の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、2020 年（令和２年）９月に第２版を公表しており、引き続き、当該技術基準の適切な運用を行っていくことが必要である。

また、こうした技術基準に加え、民間団体がセキュリティ要件のガイドラインを策定し、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）の仕組みを構築している。このような任意の認証（Certification）がより広範に普及するなど民間においても自主的な取組が進むことが期待される。

② IoT 機器の運用段階での対策(脆弱性等のある IoT 機器の調査・注意喚起)

①の対策と並行して、既に設置されている IoT 機器についても、セキュリティを高めていくための対策を行う必要がある。

このため、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こと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（ISP）を通じて利用者への注意喚起を行うプロジェクト「NOTICE」を実施している。

また、2019 年（令和元年）６月より、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、ISP を通じて利用者へ注意喚起を行う取組（NICTER 注意喚起）も実施している。

NOTICE 注意喚起では毎月約 2,000 件(NICTER 注意喚起では日々約 200 件)の注意喚起情報を ISP に対して通知しているが、注意喚起対象件数については明確な減少傾向が見られない。この理由について、注意喚起情報を分析するとともに、ISP 及び ISP を通じた利用者並びに製造事業者等へのヒアリングを行うなどして検討を行ってきた。検討を通じて、(i)IoT の進展により新たな機器が取り付けられていること、(ii)機器の設定変更を伴うなど利用者による対策の難易度が比較的高いこと、(iii)ISP から利用者への通知方法について電子メールを中心に実施されており効果的な注意喚起ができていない可能性があること、(iv)回線契約者と IoT 機器管理者（保守者）が異なる場合もあり回線契約者本人の被害がないことも多く注意喚起による効果が期待できない可能性があること、等の複数の要因が重なっている状況が明

らかになりつつある。

また、現状の NOTICE では調査対象ポート等が限られているため、脆弱な状態にある IoT 機器を網羅的に調査できていないほか、NOTICE は特定の識別符号の入力可否を調査するものであることから、例えば、VPN 機器のソフトウェア脆弱性を悪用したサイバー攻撃が確認されているが、こうした VPN 機器を特定して注意喚起を行うといったことはできていない。

こうした状況を踏まえ、次の取組を進めていく必要がある。

・NOTICE や NICTER 注意喚起等の既存の取組を引き続き継続するとともに、NOTICE については、増減要因の詳細分析や http(https)を含めた調査対象ポートの拡大等の調査の詳細化・高度化を行う。

・各 ISP に対して電子メールだけでなく郵送・架電・往訪等による注意喚起の実施を強く働きかけるとともに、実際に注意喚起を受けた利用者へのヒアリング等を行うことで注意喚起効果の測定を図る。

・IoT 機器の利用者（回線契約者）に対する注意喚起に加えて、回線契約者と IoT 機器管理者が異なる状況に対応するため、IoT 機器を設置・運用する事業者（SIer 等）やマンションインターネット事業者等に対しても、積極的な注意喚起を行う。

・IoT 機器製造事業者との連携や、IoT 機器利用者への一般的な周知広報等を通じて、IoT 機器のセキュアな設定（パスワード設定、ファームウェア更新、サポート期限確認等）について周知啓発を進める。

・ソフトウェア脆弱性等を有する IoT 機器（例：VPN 機器）を特定し、注意喚起を行う手法について検討を進める。

これらの取組とあわせて、より実効的に IoT のセキュリティ対策を進める観点から、１－（２）に記載したとおりネットワーク側で機動的な対処を行うための環境整備も推進する必要がある。

なお、これらの取組については、多様なステークホルダーが IoT セキュリティの確保に取り組むことで実現するものであり、これを 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、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。この点、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はそうした趣旨を含む

ものであり、後述Ⅲ２（１）のとおり、引き続き ISO[15]/IEC[16]及び ITU-T[17]での国際標準化に向けた取組を推進していくことが適当である。

（２）クラウドサービスの利用の進展を踏まえた対応

組織における情報システムの構築や運用においてクラウドサービスを活用する場合、正しい選択を行えば、コスト削減に加えて、情報システムの迅速な整備、柔軟なリソースの増減、自動化された運用による高度な信頼性、災害対策、テレワーク環境の実現等に寄与する可能性が大きい[18]。

我が国においては、既に半数以上の企業が何らかのクラウドサービスを利用する状況であったが、COVID-19 への対応を受け、Web 会議システム等の爆発的に利用が進んでいるサービスも存在[19]するなど、今後クラウドサービスの利用の動きが加速していくことが想定される。

[15] 正式名称は国際標準化機構（International Organization for Standardization）。各国の代表的標準化機関から成る国際標準化機関。電気・通信及び電子技術分野を除く全産業分野（鉱工業、農業、医薬品等）に関する国際規格の作成を行っている。

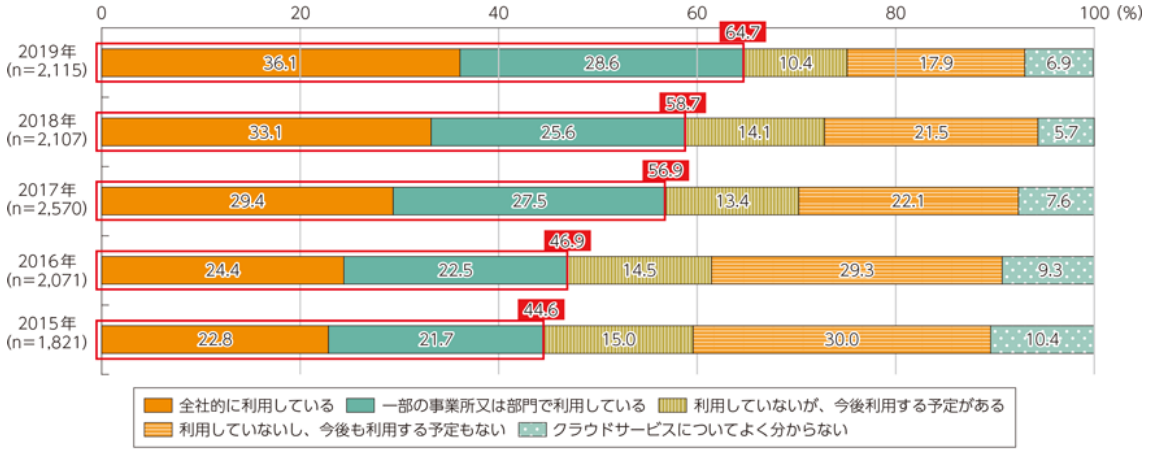
[16] 正式名称は国際電気標準会議（International Electrotechnical Commission）。各国の代表的標準化機関から成る国際標準化機関であり、電気及び電子技術分野の国際規格の作成を行っている。

[17] International Telecommunication Union Telecommunication Standardization Sector の略。国際連合の専門機関の一つである国際電気通信連合（ITU）の電気通信標準化部門。

[18] 「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」（平成 30 年６月７日各府省情報化統括責任者（CIO）連絡会議決定）によれば、クラウドサービスの利用のメリットとして、①効率性の向上、②セキュリティ水準の向上、③技術革新対応力、④柔軟性の向上、⑤可用性の向上の５つが挙げられている。

[19] 例えば、米国の Microsoft 社の発表によれば、同社の提供するチームコラボレーションサービス「Microsoft Teams」で実施される１日当たりの会議実行時間が 2020 年（令和２年）３月 31 日時点で、同年３月 16 日の９億分から 200%増（３倍）の 27 億分（4,500 万時間）に至ったとのことである。

図３　クラウドサービスを利用している企業の割合



（出典）令和2年版　情報通信白書

他方、クラウドサービスが重要な社会基盤となりつつある現在においても、セキュリティに対する不安やセキュリティ上の課題は依然として存在する。例えば、2019 年（令和元年）12 月には、自治体専用 IaaS サービスにおいてストレージ障害やデータアクセス障害が発生し、大多数の仮想 OS に影響が発生し、結果、多数の自治体の業務システムなどに長期間影響が出た。また、2021 年（令和３年）２月には、大手クラウドサービスの東京リージョンにおいて、冷却システムの電力喪失が原因でサービス障害が発生し、気象庁のウェブサイト等が一時閲覧できない状況となった。

クラウドサービスのセキュリティは一般的に「責任共有モデル」が採用されており、クラウドサービス事業者と利用者・調達者の共通の認識の下、それぞれの管理権限に応じた責任分担を行うものである。そのため、クラウドサービス事業者と利用者・調達者は、それぞれの役割を適切に果たすことで、クラウドサービスに関するセキュリティリスクを最小化するために、共に協力することが望ましい。特に、クラウドサービス事業者が、他事業者のクラウドサービスを調達・利用して自らのクラウドサービスを提供する場合、当該クラウドサービス事業者は、エンドユーザに対して提供者として責任を負いつつ、調達先のクラウドサービス事業者との関係では利用者・調達者としての責任を果たすことが求められる。

しかしながら、近年、エンドユーザがクラウドサービスを利用する際の設定ミスに起因する事故に加えて、こうした他事業者のクラウドサービスを調達・利用して自らのクラウドサービスを提供する事業者における設定ミスに起因する障害や情報漏えいといった事故が多発している。

この点、まず、利用者・調達者としてのクラウドサービス事業者は、自らの責任の下で、必要に応じてクラウド環境におけるセキュアなアプリケーション開発や、サービス提供者から供給されるツールや対応策、セキュリティ事業者によるクラウド監視のためのツールやアセスメント等も活用し、調達後も設定等を定期的に確認することで、設定ミスが起きるリスクを最小化することが求められる。

また、利用者・調達者としてのクラウドサービス事業者が適切に設定を行えるよう、調達先のクラウドサービス事業者（主に IaaS / PaaS 事業者が想定される）においては、利用者・調達者に対する情報提供やツールの提供といったサポートを提供することが求められる。

以上のとおり、クラウドサービス利用時の設定ミスを防止・軽減し、安全に安心してクラウドサービスを利用できる環境を整えるため、発生している設定ミスやそれに起因する事故、クラウドサービス事業者における取組状況等を把握しつつ、クラウドサービス事業者における上記のような取組を促す方策を検討していくことが適当である。

このほか、政府機関等が調達するクラウドサービスのセキュリティに関しては、2020 年（令和２年）６月、「政府情報システムのためのセキュリティ評価制度」（通称 ISMAP[20]: Information system Security Management and Assessment Program）が立ち上げられ、2021 年（令和３年）３月、第１弾の登録サービスリストが公開された。また、従前より民間団体等においては、クラウドサービスのセキュリティに関する認証等の取組もなされているところであり、このようなクラウドサービスのセキュリティの可視化の取組が着実に進んでいくことが望ましい。

[20] 詳細は ISMAP ポータルサイトを参照。
https://www.ismap.go.jp/

なお、付言すれば、クラウドサービスの利用の進展や、先述のテレワークの利用促進に伴って、これまで以上にそれぞれの組織においてオフィスの内外にまたがる通信やアクセスが増加し、境界の概念がなくなっていくなど、ネットワーク維持・管理の在り方や対応するセキュリティ対策の在り方も変化していくことが想定される。このようなICT利活用の進展に合わせたネットワークセキュリティモデル[21]も注目されている。今後、これまでとは異なったシステム・ネットワークの在り方が求められ、普及していく可能性もある中で、サービスの進展に対応したセキュリティ対策を引き続き検討していくことが求められる。

（３）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、「Society 5.0の先行実現の場」[22]である。

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することが想定され、常にサイバー攻撃の脅威にさらされるおそれがあるため、セキュリティの確保が重要な課題である。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が必要となることが想定される。加えて、スマートシティにおいて提供されるサービスや取り扱われるデータの安全性はその基盤となるスマートシティのセキュリティに大きく依存

---

[21] 米国標準技術研究所(NIST:National Institute of Standards and Technology)は「Draft(2nd) NIST Special Publication 800-207」において、「Zero Trust」のネットワークインフラについて、以下の前提を置いている。
・企業のプライベートネットワークは信頼できない
・ネットワーク上のデバイスは企業によって所有又は設定可能でない可能性がある
・内在的に信頼されているデバイスは存在しない
・全ての企業のリソースが企業の所有するインフラストラクチャ上に存在するわけではない
・企業の遠隔ユーザはローカルのネットワーク接続を信頼できない

その上で、「Zero Trust Architecture」が踏まえるべきコンセプトとして、
・あらゆる通信はネットワークの場所に関係なく保護される
・個々の企業のリソースへのアクセスは、接続単位で保証される
・ユーザ認証はアクセスが許可される前に動的かつ厳格に実施される
などを上げている。

[22] スマートシティについては、「統合イノベーション戦略2019」（令和元年６月21日閣議決定）において、「Society 5.0の先行実現の場としてのスマートシティの拡大・発展を図っていく必要がある」されている。

することとなるため、スマートシティがインフラとして社会に広く普及していくことに伴い、そのセキュリティの確保の重要性は一層高まっていく。

スマートシティのセキュリティ確保のため、総務省において、2020 年（令和２年）10 月、「スマートシティセキュリティガイドライン（第 1.0 版）」を策定・公表するとともに、その後も有識者やスマートシティの実現に取り組む自治体・事業者を交えた検討、スマートシティ官民連携プラットフォーム[23]のスマートシティセキュリティ・セーフティ分科会[24]からの意見などを踏まえ、2021 年（令和３年）６月、「スマートシティセキュリティガイドライン（第 2.0 版）」が公表されたところである[25]。

スマートシティの運営には多様な関係者が参加するため、スマートシティのセキュリティ確保のためには、スマートシティに内在するリスクやそれに対処する考え方について、多様な関係者間での共通認識の醸成が必要である。今後、各地でスマートシティの構築や活用が一層進んでいくことが期待される中、スマートシティのセキュリティ確保のため、総務省においては、「スマートシティセキュリティガイドライン（第 2.0 版）」について、あわせて作成されているチェックリストやガイドブックといったツールも利用しつつ、政府が実施するスマートシティ関連事業における要件として活用するなどにより、その普及を図るとともに、国際標準化も視野に、国際的に発信していくことが適当である。また、国内外のスマートシティセキュリティに関するベストプラクティスなども参考としながら、随時必要な見直しを行っていくことが適当である。

---

[23] 「統合イノベーション戦略 2019」等において、スマートシティの事業推進に当たり、官民の連携プラットフォームの構築を行うことが明記されたことを受け、内閣府、総務省、経済産業省、国土交通省が事務局となり、スマートシティの取組を官民連携で加速するため、企業、大学・研究機関、地方公共団体、関係府省等を会員とする「スマートシティ官民連携プラットフォーム」を設立。会員サポートとして、①事業支援、②分科会、③マッチング支援、④普及促進活動等を実施。2020 年（令和２年）４月末時点で 598 団体（オブザーバを含む）が参加。

[24] スマートシティ官民連携プラットフォームの下部の分科会の１つで、総務省、株式会社ラック、一般社団法人オープンガバメント・コンソーシアムが事務局となり、スマートシティにおいて実現される様々な機能・サービス・機器などについて、セキュリティやセーフティを確保しつつ、実装していくための方策について検討するために立ち上げたもの。

[25] 「スマートシティセキュリティガイドライン（第 2.0 版）」（案）に対する意見募集の結果及び「スマートシティセキュリティガイドライン（第 2.0 版）」の公表
https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00115.html

４　分野別の具体的施策

（１）無線 LAN のセキュリティ対策

無線 LAN は通信料等を気にすることなく高速な通信が利用可能な手段として家庭をはじめとして幅広く使われているほか、外出先で利用可能な公衆無線 LAN 環境についても、観光や防災などの観点から有効であることから官民を問わずその整備が進んでいる。一方で無線 LAN の利用に当たっては、適切なセキュリティ対策をとらなければ、無線 LAN 機器を踏み台にした攻撃や情報窃取が行われるおそれがある。

こうした状況を踏まえ、利便性と安全性のバランスに配慮しつつ、提供者は適切なセキュリティ対策をとった上で無線 LAN サービスを提供し、利用者に対してその説明責任を果たすこと、また、利用者は提供者からの情報を適切に読み取り、安全かつ便利なサービスを選択できるようになることが求められる。

このため、総務省においては、無線 LAN のセキュリティ対策に関して、利用者・提供者のそれぞれに向けたガイドラインを策定しているところ、この内容についてオンラインメディア等を活用して継続的な周知を実施する必要がある。

また、利用者に対するセキュリティ実態調査や提供者に対するセキュリティに配慮したサービスの提供状況調査等を行い、セキュリティ対策や対策意識の浸透状況を確認するとともに、必要に応じてガイドライン改定について検討を進めることが適当である。

（２）放送分野のセキュリティ対策

放送分野も、情報通信分野の一つとして、重要インフラに指定されている。放送分野においては、2020 年（令和２年）１月に公表した緊急提言において、「放送分野において、放送設備のサイバーセキュリティ確保に関する省令改正を速やかに実施することが必要」としているところである。

放送設備のサイバーセキュリティ確保に関する検討は、2019 年（令和元年）７月より情報通信審議会情報通信技術分科会放送システム委員会で行われ、同年 12 月に情報通信審議会から答申を受けた。当該答申を踏まえ、放送設備等のサイバーセキュリティ確保のため、放送法施行規則（昭和 25 年電波監理委員会規則第 10 号）等を改正する制度整備を実施し、2020 年（令和２年）３月に施行されたところである[26]。本制度改正によって、放送設備に関するサイバーセキュリティ対策の確保を技術基準に位置づけるとともに、放送設備に関する定期状況報告の際、サイバー事案に起因する事故報告を明記して報告を求めることとしており、引き続き、改正した制度を着実に運用していく必要がある。

（３）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、単独で十分なセキュリティ対策を取ることが難しかったり、セキュリティ対策の必要性を認識するに至らなかったりするケースが存在するおそれがある。したがって、地域レベルのセキュリティの質を向上させるためには、関係者間でのセキュリティに関する「共助」の関係が構築されることが望ましい。

このため、地域で情報通信サービスを提供している事業者を含む各種民間企業、行政機関、教育機関、関係団体等が、顔の見える関係の中で、セキュリティについて相互に啓発を行う体制やコミュニティを構築していくことが重要

[26] 具体的には、放送法施行規則において、放送設備等に対し、サイバーセキュリティの確保のために必要な措置が講じられていなければならない旨を新たに規定するとともに、放送法関係審査基準（平成 23 年総務省訓令第 30 号）において、以下の項目を審査項目として追加する制度改正を実施。

①放送本線系入力となる番組送出設備について、外部ネットワークから隔離するための措置
②放送設備に接続される監視・制御及び保守に使用される回線について、外部ネットワークからの不正接続対策を行うための措置
③設備の導入時及び運用・保守時におけるソフトウェアの点検について、不正プログラムによる被害を防止するため、放送設備のネットワークからの分離・遮断の措置及び不正プログラムの感染防止の措置
④放送設備に対する物理的なアクセス管理について、機密性が適切に配慮させるための措置
⑤放送設備の運用・保守に際して、業務を確実に実施するための組織体制の構築及び業務の実施に係る規程若しくは手順書の整備に関する措置

である。その上で、このような体制等において、イベント等の継続開催による地域のセキュリティ意識向上・人材育成や、国や専門家を招へいした情報提供が持続的・自発的に実施されることが望ましい。このような関係者間でのセキュリティに関する「共助」の関係を構築されたコミュニティ（以下「地域SECUNITY」という。）が形成されることで、地域におけるセキュリティ対策の質の向上が持続的に図られることが期待される。

そのため、引き続き「地域 SECUNITY」の構築に向け、各地域でのコミュニティ形成を推進することが必要である。

Ⅲ　横断的施策

１　サイバーセキュリティ情報に関する産学官での連携・共有等の促進

デジタル改革・DX 推進の前提としてサイバーセキュリティを確保するためには、サイバー攻撃等に関する情報の収集・分析等を行い、有効な技術や知見を生み出すとともに、それらを関係者間で共有し、社会全体でのセキュリティ対策の底上げを図ることが有用である。

他方、我が国のサイバーセキュリティ製品・サービスは、海外製品や海外由来の情報に大きく依存しており、国内のサイバー攻撃情報等の収集・分析等が十分にできていない。そのため、実データを用いた研究開発ができず、国産のセキュリティ技術が作れず、そのため国内のサイバー攻撃情報等の収集・分析等ができないというデータ負けのスパイラルに陥っている。

また、サイバー攻撃情報等の共有については、被害組織において、共有した情報を端緒に被害を受けたのが自組織であることが特定される懸念等があることから、適切に進んでいない状況にある。

今後、デジタル社会の実現に向けた改革を進め、国民一人ひとりが安全に安心してデジタルを活用していくためには、産学官連携してのサイバー攻撃等に関する情報の収集・分析等や適切な共有・公表等を進め、社会全体でのセキュリティ対策の底上げを図ることが重要である。

そのため、主に以下の２つの施策を推進していくことが適当である。

（１）我が国のサイバーセキュリティ情報の収集・分析能力の向上に向けた産学官連携の加速

（２）サイバー攻撃被害情報の適切な共有及び公表の促進

（１）我が国のサイバーセキュリティ情報の収集・分析能力の向上に向けた産学官連携の加速

サイバーセキュリティは国家の基幹を守るもので、国際競争力の強化のほか、安全保障の観点からもサイバーセキュリティ産業の強化は必須である。

そのため、NICT は、情報通信技術を専門とする我が国唯一の国立研究開発法人であり、サイバーセキュリティに関する国内トップレベルの研究開発等を

実施している。NICT が有するこれらの技術・ノウハウ[27]や情報を中核として、NICT において、我が国のサイバーセキュリティ情報の収集・分析とサイバーセキュリティ人材の育成における産学の結節点となる「サイバーセキュリティ統合知的・人材育成基盤」（CYNEX）を構築中である。なお、この CYNEX の取組は、後述２（３）①の人材育成に関する取組と一体的に実施しているものである。

この CYNEX では、得られた情報の効果的な共有と適切な管理、育成人材の質の担保やスキルアップの階層化等にも留意しつつ、早期の本格稼働に向けてシステム基盤構築・運営環境整備を引き続き進める必要がある。また、その計画・進捗については、サイバーセキュリティタスクフォースの議論と一体で進めることが適当と考えることから、本タスクフォースに適宜報告をし、方向性について最新のセキュリティ動向等を踏まえた議論を深めていく必要がある。

また、NICT は、CYNEX が産学官の組織にとって利用したいと思える環境となるよう関係者との密な意見交換を行い必要な改善を施すとともに、利用する全ての組織にとっての拠り所となるコミュニティの形成を積極的に図ることが求められる。

（２）サイバー攻撃被害情報の適切な共有及び公表の促進

大手民間企業等を対象としたサイバー攻撃が多発している中、攻撃被害を受けた組織が、サイバー攻撃に関する情報を外部専門機関等に共有することは、攻撃者の手口等を分析し、第三者における新たな被害の発生を未然に防止することができるため、社会的に望ましい。しかし、被害組織においては、共有した情報を端緒に被害を受けたのが自組織であることが特定されて二次被害が発生する懸念があることや、いかなる情報をどのようなタイミングで外部専門機関等に共有すれば良いのかが判然としないことなどから、外部専門機関等への情報共有が適切に進んでいない。

また、サイバー攻撃に対する注意喚起等を促進する見地から、攻撃被害を受けた組織は被害事実を速やかに一般に向けて公表すべきであるとする指摘もあるが、被害事実の公表は、被害組織にとって現に発生した被害を軽減することには繋がらず、逆に社会的な批判等の二次被害が発生する可能性が高いことから、積極的には行われない。

[27] 世界的にも有数の規模を誇るサイバー攻撃観測網（NICTER）や、模擬的な企業ネットワーク上でマルウェア解析が可能なシステム（STARDUST）を保有し、また、研究開発だけでなく、実践的サイバー防御演習（CYDER）により NICT による人材育成を実施している。

こうした状況を踏まえ、サイバー攻撃の被害を受けた場合に、いかなる情報をどのようなタイミングで外部専門機関等に提供すれば、自組織に不都合が発生する状況を避けつつ社会的に求められる情報共有ができるのかをまとめた、ガイダンスを作成・発信していくことが適当である。

更に、被害情報の公表がサイバー攻撃に対する注意喚起等を促進するとの見地も踏まえ、サイバー攻撃の被害を受けたことを公表した組織に対する適切な評価や支援の在り方等について、社会的なコンセンサスを作っていくための方策の検討を進めることが適当である。その際、過去の対応事例等をいわばケーススタディとして示すことも含め、情報共有や公表のインセンティブを高める、あるいは、抵抗感を低減させるための方策の検討を併せて行っていくことが適当である。

（３）その他の情報共有・情報開示の促進

①　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。

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。

②　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、こうした取組を更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。

この点、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。

その後、民間において、本手引き等を踏まえ、企業のサイバーセキュリティ対策情報の開示状況を調査・公表したり、それを踏まえて一定の企業を表彰する取組が登場しており、総務省においては引き続き、これらの取組への必要な支援等、産業界全体における情報開示の取組を促進していくことが重要である。

２　ICT サイバーセキュリティに係る横断的施策

（１）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。

2019 年（令和元年）６月に開催された G20 大阪サミットでは、我が国主導の下デジタル経済に関する議論が行われ、データ・フリー・フロー・ウィズ・トラスト（DFFT：信頼性のある自由なデータ流通）の概念が合意された。データの自由な流通を促進するため、サイバーセキュリティをはじめとする課題に対処することが必要であり、我が国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。

また、国際標準化に向けた議論の場をはじめとする国際場裡においては、サイバー空間のルール形成に大きな影響を及ぼし得るインターネットのアーキテクチャに関し、既存の秩序と相容れないおそれのある提案も行われている。これは、「自由、公正かつ安全なサイバー空間」の実現を目指す我が国にとっての大きな課題である。こうした動向を的確に把握しつつ、国内外の多様な主体と協力しながら適切に対処するための連携体制を構築していく

必要がある。

さらに、国内企業のサイバーセキュリティ分野における国際競争力の持続的な向上を図る観点から、官民一体となった情報の収集、分析等を通じて、国際的に展開し得るビジネス案件の形成力の強化を図ることが重要である。

① ASEAN 各国をはじめとするインド太平洋地域等との連携

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(AJCCBC)における実践的サイバー防御演習「CYDER[28]」等の実施を通じ、2022 年（令和４年）までに 700 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引き続き進める必要がある。同時に、AJCCBC における研修内容の発展を図る観点から、オンライン環境で受講可能なプログラムを拡充しつつ、有志国との第三者連携や国内企業との連携の強化を図ることが重要である。

また、日・ASEAN サイバーセキュリティ政策会議、日 ASEAN デジタル大臣会合及び高級実務者会合、ISP 向け日 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サイバー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 におけるサイバー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」や「グローバル ICT インフラの構築の促進に向けた諸外国との戦略的連携の推進」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を促進するほか、情報の自由な流通の確保、法の支配、開放性、自律性、多様な主体の連携といったサイバーセキュリティ戦略上の基本原則の実現・浸透を図る必要がある。

加えて、「自由で開かれたインド太平洋（FOIP）」構想等の政府戦略を踏まえつつ、各国との連携を強化することが重要である。

② 国際的な ISAC 間連携

サイバー攻撃は国境を越えて行われるため、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

[28] 「CYDER」の詳細は P41 参照。

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、2019 年（令和元年）11 月に一般社団法人 ICT-ISAC と米国の IT-ISAC との間でサイバーセキュリティ上の脅威に対する情報共有体制の一層の強化を目的として締結された覚書に基づき、国際連携ワークショップの開催等を通じて、一般社団法人 ICT-ISAC と米国の ICT 分野の ISAC との連携を更に強化し、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。また、ISAC 間の連携など、脅威情報等の国際的な共有を進めるための取組を米国に加えて他の国・地域等へ拡大することも重要である。

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など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、前述の「自由、公正かつ安全なサイバー空間」という基本的な理念に必ずしも整合的でない動きが見られる現状も踏まえつつ、我が国として注力すべき分野や具体的な課題等について調査を行うとともに、積極的な対処のために必要な連携体制の強化に向けて取り組んでいく必要がある。

さらに、Ⅱ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)[29]やICANN(Internet Corporation for Assigned Names and Numbers)[30]、IGF（Internet Governance Forum）[31]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、NOTICE、DAEDALUS[32]等のIoTセキュリティ対策をはじめとしたⅡ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、相手国の状況に応じて国際連携の場で共有をし、各国の取組につながるよう働きかけるとともに、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。総務省は、イスラエル・国家サイバー総局との間で2018年（平成30年）11月に締結した覚書に基づき人材育成協力を推進しており、引き続きこうした取組を拡大することが重要である。

（２）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、インターネットをはじめとするネットワークに接続される機器の更なる増加に伴い、サイバー攻撃の対象が拡大するとともに、AIの進展やサプライチェーンの複雑化等により、

[29] インターネットに関連した標準、教育、政策に関してリーダシップを発揮するために設立された非営利団体。140以上の組織メンバーと80,000人の個人会員によって構成される 。

[30] ドメイン名やIPアドレスなどのインターネットの重要資源の世界的な管理・調整を行う組織 。マルチステークホルダーによる参画のもと、運営されている。

[31] インターネットに関する公共政策課題について、マルチステークホルダー（政府、民間部門、技術・学術コミュニティ、市民社会等）が対話を行う場として国連が設置しているフォーラム。

[32] Direct Alert Environment for Darknet And Livenet Unified Securityの略。NICTが有するサイバー攻撃観測網を活用したアラートシステム。

攻撃手法・能力が巧妙化・大規模化していくことが想定される。そのため、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。

また、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」（令和元年５月 23 日サイバーセキュリティ戦略本部報告）においては、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、「サプライチェーンリスクの増大」、「サイバーセキュリティ自給率の低迷」、「研究・技術開発に資するデータの活用」、「先端技術開発に伴う新たなリスクの出現」、「産学官連携強化の必要」、「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。加えて、「次期サイバーセキュリティ戦略の骨子」において、AI 技術の進展や量子技術の進展など中長期的な技術トレンドを視野に入れた研究開発を進めること、「AI 戦略 2021」において、年々複雑化・巧妙化するサイバー攻撃に対する「予防」「検知」「対処」の各フェーズに AI を活用して高効率かつ精緻な対策技術を確立することとしている。

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。

なお、その際、マルウェアの解析や攻撃者の振る舞いの分析に加え、未知の攻撃に先回りして対抗するために従来の施策の振り返りや効果測定の手法、攻撃者の動機の分析の検討なども一つの研究要素となり得ることに留意することが適当である。

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。

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 IoT 機器のセキュリティ対策技術の研究開発の推進

脆弱な IoT 機器のセキュリティ対策として、IoT マルウェアを無害化・無機能化する技術を確立すべく、2020 年度（令和２年度）～2022 年度（令和４年度）までの３年間を実施期間とし、「電波の有効利用のための IoT マルウェアの無害化/無機能化技術等に関する研究開発」に取り組んでいる。

本研究開発を通じ、AI 技術を駆使した IoT マルウェアの挙動検知及び駆除技術、マルウェアに感染した IoT 機器を無害化・無機能化する技術の開発に取り組む必要がある。

③ 脆弱性の検証手法等の確立と体制整備

総務省では、5G のネットワークやその構成要素及びサービスについて、ソフトウェア・ハードウェアの両面から技術的検証を行うことを通じ、5G のネットワークのセキュリティを確保する仕組みや体制を整備するための取組を実施している。

引き続きこれらの取組を進め、脆弱性の検証手法等の確立と体制整備を着実に図っていくことが適当である。

④ 衛星通信におけるセキュリティ技術の研究開発

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。

⑤ 暗号技術に関する安全性評価と研究開発の推進

総務省等においては、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 CRYPTREC[33]を実施しており、この中で NICT は暗号技術の安全性評価において重要な役割を果たしている。

[33] Cryptography Research and Evaluation Committees の略。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。

総務省及びNICTにおいては、量子コンピュータが現代暗号に及ぼす影響の把握に務めるとともに、2022年度（令和４年度）末を目途とする電子政府推奨暗号リスト（CRYPTREC暗号リスト）の改定に向けた検討を継続することが必要である。また、耐量子計算機暗号（PQC）の標準化や実装状況のフォローを行いつつ、耐量子計算機暗号に関するガイドラインを策定し、暗号技術利用者に対する理解増進に努めるとともに、今後利用が拡大すると想定されるIoT機器等に用いられる「軽量暗号」や、暗号状態で情報処理が可能な「高機能暗号」についてもガイドラインを作成することが重要である。

加えて、暗号技術に関する研究開発として、2021年度（令和３年度）から４年間の研究開発期間で「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」において、5G等のための超高速・大容量に対応した共通鍵暗号方式技術や5G等のための耐量子計算機暗号の機能付加技術等の研究開発に取り組むこととしており、これを着実に実施していくことが必要である。

⑥　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、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、IoT機器のセキュリティを保証する技術、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。

今後、上記の研究開発を本格化するとともに、製造・ビル等の分野における実証実験を開始するなど、本取組を着実に進めることが重要である。

（３）人材育成・普及啓発の推進

これまで、総務省は、NICTの「ナショナルサイバートレーニングセンター」を通じて、実務者層・技術者層及び若年層を対象とした次の人材育成施策を実施してきたところであり、引き続き NICT において着実に取り組んでいく必要がある。

１）　国の機関、地方公共団体、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（CYDER[34]）
２）　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

[34] CYber Defense Exercise with Recurrenceの略。

ロッセオ[35]）（2020 年度（令和２年度）で必要な人材育成を完了）

３）　若手セキュリティイノベーターの育成（SecHack365）

また、これらの取組に加え、組織の戦略マネジメント層や ICT 環境構築技術者・開発者等も含む人材育成を産学官が連携して行うための仕組みや、地域におけるセキュリティ能力向上のための人材育成の仕組みについても検討を進める必要がある。

さらに、利用者が安全に ICT を利用するためには、利用者一人ひとりがサイバーセキュリティ上の脅威を認識し、それを回避するための適切な対策を把握し、実践することが重要である。そのため、利用者の現在の認識を踏まえた普及啓発にも取り組んでいくことが必要である。

①　人材育成オープンプラットフォームの構築

②の実践的サイバー防御演習（CYDER）等により人材育成を行っているものの、人材育成を全て国で実施することは困難であるため、民間事業者や教育機関等における自立的な人材育成が求められる。しかしながら、演習用の環境構築やシナリオ開発には高度な知識や技術力、そして基盤となる計算機環境が必要であり民間企業・教育機関のみでは十分に対応できていない。

こうした課題に対応するため、サイバーセキュリティの人材育成に関し、演習の実施に関する様々な要素（データセット、教材、演習用ミドルウェア、計算機リソースなど）を総合的にカバーする、オープン型の新たな人材育成プラットフォームや、産学官の連携によって当該プラットフォームを積極的に活用するためのコミュニティの支援が必要であり、前述１（１）の CYNEX の取組を進めていく必要がある。

②　実践的サイバー防御演習（CYDER）の実施

総務省は NICT を通じ、行政機関等の実際のネットワーク環境を模した大規模仮想 LAN 環境を構築の上、国の機関等 、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）を実施している。また、CYDER で使用する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ものを提供している。

[35] 2020 年東京オリンピック・パラリンピック競技大会に向けた大会関連組織のセキュリティ担当者等を対象者とした実践的サイバー演習。

サイバー攻撃は年々増加していることから、社会全体としてサイバーセキュリティ対応力を強化することは急務であり、実際のインシデント発生時に対応を行う情報システム担当者等に対する人材育成の取組は特に重要である。防災訓練と同様に定期的に演習を経験することで実対応時の能力向上を図るよう、CYDER による人材育成を引き続き実施する必要がある。

特に、地方公共団体には未受講の団体もあることから、そのような団体が我が国におけるサイバーセキュリティ対策上の穴とならないよう、受講の促進を図っていく必要がある。また、地理的・時間的要因等により CYDER が受講できない者への対応として、オンライン演習についても積極的に進めていく必要がある。なお、オンライン演習の実施に当たっては、集合演習に比べて十分な演習効果が発揮されるように必要に応じて改善を行っていくことも必要である。

なお、サイバーコロッセオについては、2020 年度（令和２年度）で必要な人材育成を完了しているが、東京大会における対応状況も踏まえ、必要に応じてその成果を CYDER や CYNEX の取組に反映していくことが適当である。

③　若手セキュリティ人材の育成の促進

総務省は NICT を通じ、25 歳以下の若手 ICT 人材を対象として、新たなセキュリティ対処技術を生み出しうる最先端のセキュリティ人材（セキュリティイノベーター）を育成する「SecHack365」を 2017 年度（平成 29 年度）から実施している。

この取組は、NICT の持つサイバーセキュリティの研究資産を活用しながら、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・開発を、第一線で活躍する研究者・技術者が１年かけて継続的かつ本格的に指導することが特徴であり、我が国における高度セキュリティ人材の育成のため、引き続き、本取組を進める必要がある。

④　地域における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。サイバー攻撃は地理的な距離に関係なく、弱いところがターゲットとな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。

地域においては、セキュリティに関する雇用の受け皿がないことから、若年層がセキュリティ人材を目指さず、地域におけるセキュリティ人材が更に不足するという悪循環がある。そのため、地域においてセキュリティを地場産業化しようとしている民間企業等と総務省が連携し、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ことについて、その有効性をモデル事業により検証を行うとともに、その成果をモデル事業対象地域以外に横展開して活用できるように進めていく必要がある。

⑤　利用者への普及啓発

利用者が安全に ICT を利用するためには、高齢者を含む利用者一人ひとりがサイバーセキュリティ上の脅威を認識し、それを回避するための適切な対策を把握し、実践することが重要である。総務省において、まず利用者の現在の認識を把握するため、サイバーセキュリティに関する意識調査を実施したところ、メール内のリンク先の URL の確認といった基礎的な対策が必ずしも実施されていない実態や、多要素認証の導入について面倒と感じる利用者が多いといった利用者の意識が明らかとなった[36]。

利用者における脅威の認識と対策の実践を促すため、意識調査の結果明らかになった利用者の認識を踏まえた普及啓発施策に取り組んでいくことが適当である。

具体的には、まず、フィッシング被害防止のため、メールや SMS の送信元やリンク先 URL をよく確認することの重要性を周知するとともに、ISP や携帯電話事業者に対して、フィッシング被害防止に向けた十分な対策の実施を働きかけることが適当である。また、ウェブサイト運営者等に対して、多要素認証について使い勝手の良い方法の工夫を働きかけることや、特にキャッスレス決済サービスやオンラインショッピングサイトで多要素認証の導入に対するニーズが高いことを関係者に共有していくことが適当である。

マルウェア感染防止のためには、OS のアップデートやルータ等のファームウェアアップデートの必要性について周知するとともに、ISP や携帯事業者によるマルウェア感染等の被害防止のためのセキュリティ対策が引

[36] 「サイバーセキュリティに関するインターネット利用者の意識調査結果について」（令和３年４月７日　第 30 回サイバーセキュリティタスクフォース資料 30-1）

き続き必要である。また、利用者の端末がサイバー攻撃の踏み台になるケースについては、ユーザ自身のこととして捉えづらいため、NOTICE 等の事業者側の取組を引き続き推進することが重要である。

周知の具体的な手法・媒体については、オンラインでの周知に注力しつつ、テレビやラジオ等のメディアも含め、利用者に広くリーチ可能な効果的な周知手法を検討すべきである。

また、総務省 Web サイトを通じた情報発信についても積極的に進めていく必要があることから、「国民のための情報セキュリティサイト」についても、最新のサイバーセキュリティ動向を踏まえた内容の見直し等を進めていくことが重要である。

Ⅳ　今後の進め方

「ICT サイバーセキュリティ総合対策 2021」は、昨今のサイバー空間を取り巻く多様な環境変化や状況変化等を踏まえて、社会全体のデジタル改革・DX の推進の前提としてのサイバーセキュリティの確保が主要課題であるとの認識の下で、当該主要課題への対処のために講じるべき施策を取りまとめたものである。総務省においては、今後、本提言を踏まえて「自由、公正、かつ安全なサイバー空間」の実現を下支えする ICT インフラやサービスのサイバーセキュリティの確保を図る観点から、各施策を具体的に推進していくべきである。なお、施策の推進に際しては、サイバー空間を取り巻く環境等が常に変化し続けていることを踏まえて、そうした変化に柔軟に対応しつつ、取り組んでいくことが必要である。

また、「ICT サイバーセキュリティ総合対策 2021」の推進に当たっては、社会全体のデジタル改革・DX 推進の主体となる多様なステークホルダーの理解と連携の下で効果的に進めていくことが必要である。こうした観点から、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との間で、本提言及び提言の目的・狙い、ビジョンの共有を図り、取組の強化を図っていくことが望ましい。

別添　プログレスレポート 2021

「IoT・5G セキュリティ総合対策 2020」に掲げた施策の進捗状況は以下のとおりである。

項番	総合対策2020の本文	進捗状況（※令和3年6月1日時点）
Ⅲ　情報通信サービス・ネットワークの個別分野に関する具体的施策		
（１）IoTのセキュリティ対策		
①　IoT機器の設計・製造・販売段階での対策		
1	IoT機器の設計・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、電気通信事業法の枠組みにおいて端末設備等規則を改正し、強制規格としての技術基準が策定 されている（2019年（平成31年）３月１日公布、2020年（令和２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、当該技術基準の適切な運用を行っていくことが必要である。 また、こうした技術基準に加え、民間団体がセキュリティ要件のガイドラインを策定し、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）の仕組みを構築している。このような任意の認証（Certification）がより広範に普及するなど民間においても自主的な取組が進むことが期待される。	・電気通信事業法の枠組みにおいて「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２版）」も活用して、当該技術基準の適切な運用を行っている。 ・民間の任意の認証（Certification）制度として、一般社団法人重要生活機器連携セキュリティ協議会（CCDS）において、IoT機器のセキュリティ要件を定め認証プログラムを実施している。
②　脆弱性等を有するIoT機器の調査及び注意喚起		
2	①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要することから、既に設置されているIoT機器のセキュリティ対策に関しては別に対応を行う必要がある。 この対策については、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こと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（ISP）を通じて利用者への注意喚起を行うプロジェクト「NOTICE 」を実施している。 また、2019年（令和元年）６月より、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、ISPを通じて利用者へ注意喚起を行う取組も実施している。 これらの注意喚起の取組について引き続き実施し、取組に参加するISPの拡大を図っていくとともに、各ISPにおいて架電や往訪も含めた有効な注意喚起手法についてベストプラクティスの共有を行っていくことが必要である。また、総務省においても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、Web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が必要である。そして、こうしたIoT機器の利用者に対する注意喚起に加えて、IoT機器の製造事業者や、法人向けIoT機器を念頭としてIoT機器を設置・運用する事業者（SIer等）に対しても、脆弱な状態にあるIoT機器を増やさないような注意喚起等を行っていく必要がある。 さらに、緊急提言にもあるように、国内の重要施設に設置されているIoT機器について、利用事業者名や用途がインターネット上から容易に判別できることなどによって攻撃を受けやすい状態に置かれていないか調査を行い、問題のある機器の所有者・運用者等に対策の実施を促していく取組を、東京大会までに実施する必要がある。 なお、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。	・総務省及びNICTは、インターネットサービスプロバイダ（以下「ISP」という。）と連携し、2019年（平成31年）２月から、ID・パスワード設定等が脆弱なためサイバー攻撃に悪用されるおそれのあるIoT機器の調査及び当該機器の利用者への注意喚起を行う取組「NOTICE」を実施している。おおむね月に１回の頻度で調査を行っており、2020年度（令和２年度）は12,804件を注意喚起対象としてISPへ通知した。 ・また、2019年（令和元年）６月からは、NICTのNICTERプロジェクトで得られた情報を基に、既にマルウェアに感染しているIoT機器の利用者に対し、ISPが注意喚起を行う取組（NICTER注意喚起）を実施している。注意喚起対象となるものは日々ISPへ通知しており、2020年度末（令和２年度末）までの１日平均で約190件を通知している。 ・これらの取組状況については、次のURLにて公表している。 https://notice.go.jp/status
③　サイバー攻撃に関する電気通信事業者間の情報共有		
3	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など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。	・2019年（平成31年）２月より、「NOTICE」プロジェクトにおいて、電気通信事業者間の情報共有の結節点となる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。）の機能を活用し、認定協会経由でパスワード設定等に不備のあるIoT機器に関する情報をISPに通知しているところである。 ・また、2021年（令和３年）２月から７月にかけて、海外の捜査当局から警察庁に対して提供された国内のEmotetに感染している機器に関する情報を認定協会経由でISPに通知し、当該情報に記載されている機器の利用者に対して注意喚起を実施した。 ・更に、2020年（令和２年）２月に、一般社団法人ICT-ISACにおいて広く5Gセキュリティに係る情報共有を進めることを目的とした「5Gセキュリティ推進グループ」が立ち上げられたところ、当該グループにおいて、ローカル5Gを提供する事業者やローカル5Gを利用する主体にとって参考となる、ローカル5Gのセキュリティガイドラインの作成に着手した。

（2）5Gのセキュリティ対策		
① 脆弱性の検証手法等の確立と体制整備		
4	5Gのネットワークに関しては、仮想化・ソフトウェア化が進むことから、サプライチェーンリスクを含む新たなサイバーセキュリティ上の課題が懸念される。そのため、5Gのネットワークやその構成要素及びサービスについて、ソフトウェア・ハードウェアの両面から技術的検証を行うことを通じ、5Gのネットワークのセキュリティを確保する仕組みや体制を整備することが必要である。 具体的には、まず、ソフトウェアを中心としたネットワークの脆弱性については、5Gの通信インフラとしての機能保証のため、ソフトウェアにより構成される部分を含め、ネットワーク全体のセキュリティを確保する必要がある。 そのため、5Gの仮想環境を構築し、(a)オープンソースソフトウェア等の解析、(b)多種多様なパターンのデータ入力による異常動作確認（ファジング）、(c)エシカルハッカーによる脆弱性調査・脅威分析を実施し、対策を検討することが必要である。 一方、ハードウェアの脆弱性については、5G等のネットワークを構成するハードウェア上に故意に組み込まれた不正なチップによって生じるセキュリティ上の課題に対応するため、AIを活用し(a)回路情報から不正に改変された回路を検知する技術や、(b)電子機器外部で観測される情報から不正動作を検知する技術を開発し、対策を検証することが必要である。 また、上記の検証結果を踏まえつつ、5G等のネットワーク上での運用面の課題等についても検討する必要がある。 その上で、技術移転などを含めて前述のような脆弱性検出技術の成果を活用し、関連する脅威の分析の視点を踏まえつつ、システムや利用者に対するインパクト分析を実施し、必要なセキュリティ対策を検討することが必要である。また、このような検証・分析の取組において、5Gの事業者・運用者やベンダー等が協力して実施する体制を構築することが必要である。	・5G については、携帯電話事業者による全国向け 5G サービスと、地域の企業や自治体等の様々な主体が自らの建物や敷地内でスポット的に柔軟にネットワークを構築し利用可能とするローカル 5G の取組が開始されている。 ・総務省において、2019 年度（令和元年度）より、5G ネットワークにおけるソフトウェアの脆弱性に対応するための調査検討を実施している。2020 年度（令和 2 年度）は、5G の通信インフラとしての機能保証のため、ソフトウェアにより構成される部分を含め、ネットワーク全体のセキュリティを確保する必要があることから、5G 仮想環境の対象を、コアネットワークのみならず、モバイルエッジコンピューティング（MEC)まで拡張し、オープンソースソフトウェア等の解析、多種多様なパターンのデータ入力による異常動作確認（ファジング）、エシカルハッカーによる脆弱性調査、脅威分析の実施に向けて取り組んだ。 ・ハードウェア脆弱性への対応は、外部から調達した設計ツールや設計部品を用いたチップの安全性を担保するために、設計・製造におけるチップの脆弱性検知手法の調査検討を実施しており、令和 2 年度は標準的なベンチマーク回路等を用いて、不正回路の種類及びその機能を明確化し、不正回路を検知する技術の開発を行った。加えて、回路情報が入手できないチップの安全性を担保するために、市販の組込みマイコン等、比較的簡易な電子機器の動作のもと、電子機器の外部から観測される情報を用いて、不正動作を検知する技術の開発を行った。 ・引き続き、ハードウェアチップの脆弱性検知手法の確立を目的として、ハードウェアチップの回路情報を用いて不正回路を検知する技術及び電子機器の外部から観測される情報を用いて不正動作を検知する技術の改良及び基礎的な検証を実施する。
② 5Gの脆弱性情報や脅威情報等の共有の枠組みの構築		
5	4Gまでの従来の移動通信システムでは電気通信事業者がネットワークの運用を行っていたが、5Gの時代では、ローカル5Gについて、従来は通信サービスのユーザとしての位置づけであった様々な企業や自治体等がネットワークの運用者として関わっていくこととなる。 また、ネットワークの用途も、超低遅延や多数同時接続などの特長を活かした様々な産業用途が期待されているため、リスクや脅威の在り方も多様なものが想定される。 このため、5Gのセキュリティを確保していく上では、①の脆弱性の検証と合わせ、5Gのネットワークを運用している事業者・運用者やベンダー、利用者等の間での脆弱性情報や脅威情報、さらにこれらの対処の在り方に関する情報の共有の取組が重要である。 この点、5Gとそのセキュリティに関する情報共有などを定期的に実施して5Gのセキュリティの啓発を進めるとともに、ローカル5Gを含む5Gの運用者が5Gサービスを提供する場合のサイバーセキュリティ上の懸念や脅威に関する問い合わせに対して助言を行うことを目的とし、2020年（令和２年）２月に一般社団法人ICT-ISACにおいて「5Gセキュリティ推進グループ」が設立されたところである。 上記のような民間での取組を踏まえつつ、引き続き、5Gのセキュリティの確保に向け、情報共有の取組を促進することが必要である。	・一般社団法人ICT-ISACの5Gセキュリティ推進グループにおいて、ローカル5Gを含む5Gの運用者に対する助言を行うための枠組を構築し、ローカル5G免許を取得した事業者への参画の働きかけを実施した。 ・一般社団法人ICT-ISACの5Gセキュリティ推進グループにおいて、ローカル5Gを提供する事業者やローカル5Gを利用する主体にとって参考となる、ローカル5Gのセキュリティガイドラインの作成に着手した。
③ 5Gのセキュリティ対策の促進のための政策的措置		
6	5Gのセキュリティ確保のためには、①、②の取組に加え、実際のネットワークにおいて対策の実装が進むことが必要である。この点、5Gのセキュリティの確保については、サイバーセキュリティ基本法（平成26年法律第104号）第６条及び第７条の趣旨を踏まえ、電気通信事業者その他の5Gのネットワークの運用者が自ら積極的かつ自主的に確保すべきものであり、国としてはこのような自主的な取組を支援するような振興的措置を取ることが望ましい。その上で、特に必要な部分については、法令等に基づき規律が課されることが望ましい。 この点、5Gの安全性・信頼性を確保しつつその適切な開発供給及び導入を促進するため、全国5G及びローカル5Gの導入事業者に対する税制優遇措置や導入事業者及び開発供給事業者に対する金融支援の実施を盛り込んだ「特定高度情報通信技術活用システムの開発供給及び導入の促進に関する法律」が2020年（令和２年）５月に成立したところであり、今後、税制優遇及び金融支援措置が積極的に活用されるよう、その早期施行に向け必要な準備を進めることが必要である。 また、5Gのセキュリティを確保するため、全国5Gでは、携帯電話事業者に対して第５世代移動通信システムの導入のための特定基地局の開設計画の認定の際に、サプライチェーンリスク対応を含む十分なサイバーセキュリティ対策を講ずることを条件として付しているほか、ローカル5Gでは、ローカル5G導入に関するガイドラインにおいて、サプライチェーンリスク対応を含む十分なサイバーセキュリティ対策を講じる旨を明記するとともに、ローカル5Gの免許時の条件として付すこととしている。 このような産業振興的な枠組み、制度的な枠組みの両面から5Gのセキュリティ確保に向けた取組を進める必要がある。	・安全性・信頼性の確保等を図るための指針を含む、特定高度情報通信技術活用システムの開発供給及び導入の促進に関する法律及びその下位法令が施行され、これに基づき、開発供給計画及び導入計画を認定し、①全国キャリアの高度な送受信装置等の前倒し整備や、②ローカル5Gの送受信装置等の設備投資に向けた動きが進展している。 ・また、5G のサイバーセキュリティを確保するため、全国 5G では、携帯電話事業者に対して第 5 世代移動通信システムの導入のための特定基地局の開設計画の認定の際に、サプライチェーンリスク対応を含む十分なサイバーセキュリティ対策を講ずることを条件として付した。ローカル 5G では、ローカル 5G 導入に関するガイドラインにおいて、サプライチェーンリスク対応を含む十分なサイバーセキュリティ対策を講じる旨を明記するとともに、ローカル 5G の免許時の条件として付している。 ・このような産業振興的な枠組み、制度的な枠組みの両面から 5G のセキュリティ確保を推し進めている。

（3）クラウドサービスのセキュリティ対策		
7	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りつつある。また、COVID-19への対応において、クラウド型のWeb会議システムなどの利用も増大しており、今後社会・経済の様々な分野で利用が加速していくことが想定される。 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」（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。 このような状況を踏まえ、現在、政府機関等の情報システムにおけるクラウドサービスの調達に関しては、「政府情報システムのためのセキュリティ評価制度」（通称 ISMAP: Information system Security Management and Assessment Program）について、2020年度（令和２年度）中に各省庁において制度の利用開始ができるよう立ち上げが進められているが、本取組を着実に実施する必要がある。 また、クラウドサービスのセキュリティについては、既存の様々な認証・認定制度が存在し、サービスにおける対策の可視化の取組がなされており、クラウドが普及していく時代においては、利用者・調達者の側においてこのような既存の認証・認定制度を参照していくことが期待される。他方、クラウドサービスを活用した情報システムについては、クラウドサービスの提供者と利用者・調達者による「責任共有モデル」が採用されることが一般的であることを念頭に、利用者・調達者が自ら採るべき対策についても認識をした上でサービス利用を行う必要があることから、利用者・調達者の側のリテラシー向上に向けた取組を進めることが重要である。 なお、付言すれば、クラウドサービスの利用やテレワークの普及の進展などを念頭に、それぞれの組織においてオフィスの内外をまたがるアクセスが増加し、境界の概念がなくなっていくなど、ネットワーク維持・管理の在り方や対応するセキュリティ対策の在り方も今後徐々に変化していくことが想定される。このような新たな時代のネットワークセキュリティの在り方について、継続的に調査・検討し、必要に応じて政策に反映していくことが重要である。	・2020年（令和２年） ６月、「政府情報システムのためのセキュリティ評価制度」（通称 ISMAP: Information system Security Management and Assessment Program）が立ち上げられ、2021年（令和３年） ３月に第１弾として10サービス、同年６月に第２弾として４サービスがISMAPに登録され、ISMAPポータルサイト上のクラウドサービスリストに掲載された。 ・「クラウドサービス提供における情報セキュリティ対策ガイドライン（第2版）」を、中小を含む全てのクラウドサービス事業者がより利用しやすくなるよう、全体の構成見直しや責任共有モデルの考え方、管理策の見直しなどを含む改定を検討し、「クラウドサービス提供における情報セキュリティ対策ガイドライン（第3版）」（案）を作成し、2021年（令和３年） ７月に当ガイドライン（案）に対する意見募集を開始した。（当ガイドラインの改定版は2021年度（令和３年度）中に公表予定。）
（4）スマートシティのセキュリティ対策		
8	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、「Society 5.0の先行実現の場」 である。 この点、総務省では、都市や地域が抱える様々な課題の解決や地域活性化・地方創生を目的として、ICTを活用した分野横断的なスマートシティ型の街づくりに取り組む「データ利活用型スマートシティ推進事業」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 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することが想定され、常にサイバー攻撃の脅威にさらされるおそれがあるため、IoT機器の監視を行うセキュアゲートウェイの在り方についての検討が重要である。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が必要となることが想定される。また、スマートシティには多様な主体が関わることが想定されるため、システム全体としてのセキュリティのPDCAサイクルや、平時・有事のセキュリティ確保の体制としてのSOC又はCSIRTの在り方についても検討が必要となることが想定される。 以上を踏まえ、スマートシティのセキュリティ確保の在り方について、多様な関係者間で一定の共通認識の醸成が必要である。具体的には、スマートシティ官民連携プラットフォーム のスマートシティセキュリティ・セーフティ分科会 など、官民の検討の場において、スマートシティのセキュリティ確保の観点から留意すべき要件やチェックすべき事項などについて検討を行い、明確化を図ることが必要である。またその際は、スマートシティを推進する取組との連携を図り、セキュリティ対策の実装を促進していくことが重要である。 なお、スマートシティは、地域におけるIoTや5G、クラウドサービスのユースケースとしての側面もあり、（１）のIoTのセキュリティ対策や、（２）の5Gのセキュリティ対策、（３）のクラウドサービスのセキュリティ対策の取組等の連携を図ることが重要であるほか、（８）の地域の情報通信サービスのセキュリティの確保やⅣ－（２）－⑤の地域のセキュリティ人材育成の取組など、地域のセキュリティ強化の取組と連携を図ることも重要である。 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	・スマートシティ官民連携プラットフォームのスマートシティのセキュリティ・セーフティ分科会の活動において、スマートシティにおけるセキュリティの在り方について議論・意見交換を行った。 ・2020年（令和２年）10月、スマートシティのセキュリティの在り方について整理した「スマートシティセキュリティガイドライン（第1.0版）」を公表した。 ・その後、総務省が実施したスマートシティセキュリティの取組実態調査や、スマートシティのセキュリティ・セーフティ分科会や各種有識者会合における意見を踏まえ、「スマートシティセキュリティガイドライン（第1.0版）」の改定を検討し、2021年（令和３年） ６月に「スマートシティセキュリティガイドライン（第2.0版）」として公表した。

（５）トラストサービスの制度化と普及促進		
9	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。 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」を開催し、2019年（平成31年）１月から、トラストサービスに関する現状や課題について検討を実施し、2020年（令和２年）２月に同研究会最終報告書の取りまとめがなされ、一定のサービス提供の実態又は具体的なニーズの見込みがあり、利用者がより安心して利用できる環境の構築に向けた課題が顕在化しているタイムスタンプ、ｅシール及びリモート署名について、以下のとおり、今後の取組の方向性が示された。 １）タイムスタンプについては、技術やサービス内容が確立されており、一般財団法人日本データ通信協会による民間の認定制度が14年間運用されてきたが、国の信頼性の裏付けがないことや、国際的な通用性への懸念が更なる普及を妨げている一因となっていることを踏まえ、国が信頼の置けるタイムスタンプサービス・事業者を認定する制度を創設することが適当である。 ２）ｅシールについては、新しいサービスであり、その導入促進のためには利用者が安心して利用するため、信頼のおけるサービス・事業者に求められる技術上・運用上の基準の提示や、それを満たすサービス・事業者について利用者に情報提供する仕組みが重要である一方、サービス内容や提供するための技術などが確立されていないことから、国が一定程度関与しつつ、信頼の置けるサービス・事業者に求められる技術上・運用上の基準を策定し、これに基づく民間の認定制度を創設することが適当である。 ３）今後利用拡大が期待されるリモート署名については、ガイドラインが民間団体において策定されたことを踏まえ、利用者によるリモート署名の円滑な利用を図るため、当該民間のガイドラインの策定・公表や自主的な適合性評価の仕組みの整備を受け、主務省（総務省、経済産業省、法務省）において、当該ガイドライン等の精査や当該ガイドライン及び適合性評価の仕組みの運用状況のモニタリングなどの取組を進めながら、リモート署名の電子署名法上の位置づけについて速やかに明確化することが適当である。 これを受け、上述の方向性に合わせ、トラストサービスの制度的な枠組みの形成に向けた取組を一層加速する必要がある。 ・ タイムスタンプについて、2020年度（令和２年度）中に国による認定制度の整備を行う。 ・ ｅシールについて、国が関与して策定した基準に基づく民間の認定制度の創設に向け、2021年度（令和３年度）までに認定基準等の整備を行う。 ・ リモート署名について、技術や運用の動向も踏まえ検討を行い、2021年度（令和３年度）までに電子署名法上の位置づけを明確化する。 また、COVID-19への対応において、請求書や押印手続、印刷など紙の書類の処理の必要性がテレワークの実施の阻害要因になっているケースがあり、企業間の様々なやり取りの電子化やオンラインでの完結が求められる中、トラストサービスはその実現に必要不可欠なものであるため、可能な限り前倒しを検討することが求められる。 なお、これら制度の具体化と併せて、実際の利用の場面でトラストサービスの各種業法等における位置づけを明確化していくことが重要であることを踏まえ、各種法令・ガイドライン等との関係で有効な手段として認められるトラストサービスの要件を明示するよう、法令・制度を所管する関係府省庁への働きかけを行っていくことも重要である。	・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については、2020年（令和2年）２月に公表された「プラットフォームサービスに関する研究会トラストサービス検討ワーキング グループ最終取りまとめ」において示された方針に基づき、タイムスタンプ・eシール・電子署名のそれぞれについて検討を行ってきた。 ・タイムスタンプについては、2020年（令和２年）３月に「タイムスタンプ認定制度に関する検討会」を立ち上げ、現行の民間の認定制度である「タイムビジネス信頼・安心認定制度」が抱える課題やEU等の国際的な制度との整合性等の観点から同年３月の第１回会合以来、翌年３月まで合計11回にわたり議論を行い、2021年（令和３年）３月に最終取りまとめを提示した。その結果を踏まえ、同年４月に「時刻認証業務の認定に関する規程（令和3年総務省告示第146号）」を公布、国による認定制度を整備した。 ・eシールについては、2020年（令和２年）４月に「組織が発行するデータの信頼性を確保する制度に関する検討会」を立ち上げた。まずは同年４月に第１回会合を開催して以来、翌年３月まで合計11回にわたり、eシールの利用が有効と考えられるユースケースについて事業者へのヒアリングや広く一般を対象に提案募集等を実施し、その結果を踏まえつつ、実証等を通じて整理した技術的基準等についても参考にしながら、我が国におけるeシールの在り方等について検討を行った。2021年度においても継続して検討を行い、その結果を踏まえ、我が国のeシールにおける信頼の置けるサービス・事業者に求められる技術上・運用上の基準等について整理した「eシールに係る指針」を作成し、2021年（令和３年）６月に公表した。 ・電子署名については、回答書の公表を通じてリモート署名の電子署名法上の位置づけを示し、また、新しく登場したクラウド技術を活用した立会人型電子署名（利用者の指示に基づきサービス提供者自身の署名鍵による暗号化等を行う電子契約サービス）については電子署名法における取扱いが不明確であったことから、同年７月に「電子署名法２条１項に関するQ＆A」を、同年９月には「電子署名法３条に関するQ&A」を公表する等、電子署名法上の電子署名の利便性の改善に向けた取組を実施した。
（６）無線LANのセキュリティ対策		
10	無線LANは通信料等を気にすることなく高速な通信が利用可能な手段として家庭をはじめとして幅広く使われているほか、外出先で利用可能な公衆無線LAN環境についても、観光や防災などの観点から有効であることから官民を問わずその整備が進んでいる。一方で無線LANの利用に当たっては、適切なセキュリティ対策をとらなければ、無線LAN機器を踏み台にした攻撃や情報窃取が行われるおそれがある。 総務省においては、無線LANのセキュリティ対策に関して、利用者・提供者のそれぞれに向けたガイドラインを策定し、緊急提言を踏まえ、2020年（令和２年）５月に改定を行っている。東京大会に向けて多くの利用が見込まれるホテル・観光機関や病院、そしてICTの利活用が急速に進んでいる学校等に対してガイドラインの内容を周知していくなど、安全・安心に無線LANを利用できる環境の整備に向けて、利用者・提供者の双方に対するセキュリティ対策に関する周知啓発を図っていく必要がある。	・無線LANの利用者・提供者向けのセキュリティに関するガイドラインとして2020年（令和２年）５月に改定を行った「Wi-Fi利用者向け簡易マニュアル」及び「Wi-Fi提供者向け セキュリティ対策の手引き」について総務省Webサイトを通じて周知を行った。 ・無線LANのセキュリティに関する利用者意識調査と提供者状況調査を実施した。結果については、ガイドライン類と併せて、次のURLにて公表している。 https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/ ・無線LANの利用者のセキュリティ対策に関する周知啓発の一環として、オンライン動画講座を2021年（令和３年）２月12日から同年３月24日にかけて開講した。これは、有識者が公衆無線LAN利用時のリスクや適切なセキュリティ対策等を動画全11回により紹介するもので、3,161名が受講登録を行った。また、若年層を含む利用者への周知を目的として、20秒程度の動画コンテンツ（全５種）を作成し、SNSを通じて、2021年（令和３年）２月12日から同年３月23日にかけて、216万インプレッション （3.3万クリック） の動画配信（広告）を行った。

（7）重要インフラとしての情報通信分野等のセキュリティ対策

11

情報通信分野及び地方公共団体分野は、「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　令和２年１月30日サイバーセキュリティ戦略本部最終改定。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、又は利用不可能となった場合に国民生活・社会経済活動に多大なる影響を及ぼしかねないものとして重要インフラに指定されている。

第４次行動計画を踏まえ、重要インフラ各分野の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４日サイバーセキュリティ戦略本部決定　令和元年５月23日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に向けた取組が進められている。

この点、まず情報通信分野のうち、電気通信分野においては、事故再発防止のため、「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、「情報通信ネットワーク・安全信頼性基準（昭和62年郵政省告示第73号）」等の見直しの必要性について検討を行っている。

さらに、情報通信審議会情報通信技術分科会IPネットワーク設備委員会においては、2019年（令和元年）６月から2020年（令和２年）３月にかけて「IoTの普及に対応した電気通信設備に係る技術的条件」について検討が行われた。具体的には、通信ネットワークの本格的なソフトウェア化・仮想化の進展に対応した技術基準等の在り方や災害に強い通信インフラの維持・管理方策について検討が行われ、その検討結果については、2020年（令和２年）３月に情報通信審議会から一部答申を受けたところである。

当該答申を踏まえ、総務省においては、令和元年房総半島台風等による通信被害を踏まえ市町村役場をカバーする固定通信局舎及び携帯電話基地局について24時間以上の停電を考慮した予備電源を確保することなど電気通信事業者における停電対策の強化等に関する制度整備を行うため、情報通信ネットワーク安全・信頼性基準の改正に向けた手続を行っており、2020年（令和２年）６月末までの制度化を予定している。今後は、改正後の制度を着実に運用していくとともに、引き続き委員会を開催し、電気通信設備の安全・信頼性確保に向け必要な検討が進められていくことが期待される。

また、2018年度（平成30年度）には、前述の（１）－③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（昭和63年郵政省令第46号）を改正する制度整備が行われている。

今後は、当該事故に関する情報を含むサイバー攻撃を起因とする電気通信事故に関する情報、それらの情報を踏まえた再発防止に向けた教訓等及び情報通信ネットワーク安全・信頼性基準等に関する内閣官房内閣サイバーセキュリティセンターや電気通信事業者との間の情報共有の在り方等、情報通信ネットワークの安全・信頼性対策とサイバーセキュリティ対策との更なる連携強化を図ることが期待される。

加えて、放送分野においては、2020年（令和２年）１月に公表した緊急提言において、「放送分野において、放送設備のサイバーセキュリティ確保に関する省令改正を速やかに実施することが必要」としているところであるが、2019年（令和元年）７月より情報通信審議会情報通信技術分科会放送システム委員会で放送設備のサイバーセキュリティ確保に関する検討を開始し、同年12月に情報通信審議会から答申を受けたところである。

当該答申を踏まえ、放送設備等のサイバーセキュリティ確保のため、放送法施行規則（昭和25年電波監理委員会規則第10号）等を改正する制度整備を実施し、2020年（令和２年）３月に施行されたところである。本制度改正によって、放送設備に関するサイバーセキュリティ対策の確保を技術基準に位置づけるとともに、放送設備に関する定期状況報告の際、サイバー事案に起因する事故報告を明記して報告を求めることとしており、今後は改正した制度を着実に運用していく必要がある。

また、地方公共団体分野においては、2015年（平成27年）のいわゆる「三層の対策」により、インシデント数の大幅な減少を実現するなど、短期間で自治体の情報セキュリティ対策の抜本的強化したところであるが、2019年（令和元年）12月より、三層の対策の効果や課題、新たな時代の要請を踏まえ、効率性・利便性を向上させた新たな自治体情報セキュリティ対策について検討を開始したところである。

なお、緊急提言においては、情報通信分野の取組に関し、サイバーセキュリティ対策や事故報告についての法令への位置づけ、分野ごとの所管省庁や業界団体によるガイドラインや基準の策定を通じてサイバーセキュリティ対策を実効的に進めていく取組について、あらゆる機会を通じて周知し、対応の強化を呼びかけていくことが必要としたところであり、今後も安全基準等の整備及び浸透の取組などを積極的に推進していくことが期待される。

【情報通信分野】

・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　令和２年１月30日サイバーセキュリティ戦略本部最終改定。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、又は利用不可能となった場合に国民生活・社会経済活動に多大なる影響を及ぼしかねないものとして重要インフラに指定されている。第４次行動計画を踏まえ、重要インフラ各分野の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４日サイバーセキュリティ戦略本部決定　令和元年５月23日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に向けた取組が進められている。情報通信分野のうち、電気通信分野においては、情報通信審議会情報通信技術分科会IPネットワーク設備委員会において、2019年（令和元年）６月から2020年（令和２年）３月にかけて「IoTの普及に対応した電気通信設備に係る技術的条件」について検討が行われた。具体的には、通信ネットワークの本格的なソフトウェア化・仮想化の進展に対応した技術基準等の在り方や災害に強い通信インフラの維持・管理方策について検討が行われ、その検討結果については、2020年（令和２年）３月に情報通信審議会から一部答申を受けたところである。当該答申を踏まえ、総務省においては、令和元年房総半島台風等による通信被害を踏まえ市町村役場をカバーする固定通信局舎及び携帯電話基地局について24時間以上の停電を考慮した予備電源を確保することなど電気通信事業者における停電対策の強化等に関する制度整備を行うため、情報通信ネットワーク安全・信頼性基準を2020年（令和２年）６月に改正した。今後は、改正後の制度を着実に運用していくとともに、引き続き委員会を開催し、電気通信設備の安全・信頼性確保に向け必要な検討が進められていくことが期待される。

・また、2018年度（平成30年度）には、「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（昭和63年郵政省令第46号）を改正する制度整備が行われ、2019年度には８件、2020年度（第３四半期まで）には12件の報告が行われている。今後は、電気通信事故の再発防止や被害軽減等のため、「電気通信事故検証会議」等の取組みを通じ、当該事故に関する情報を含むサイバー攻撃を起因とする電気通信事故に関する情報、それらの情報を踏まえた再発防止に向けた教訓等及び情報通信ネットワーク安全・信頼性基準等に関する内閣官房内閣サイバーセキュリティセンターや電気通信事業者との間の情報共有の在り方等、情報通信ネットワークの安全・信頼性対策とサイバーセキュリティ対策との更なる連携強化を図ることが期待される。

【放送分野】

・2020年（令和２年）３月に改正した制度を着実に運用するため、各放送事業者に対して放送設備に係るサイバーセキュリティ対策の自己点検の実施を要請した。また、放送局の再免許の際には、各事業者のサイバーセキュリティ対策を確認した。

【地方公共団体分野】

・「三層の対策」の効果や課題、行政手続のオンライン化の推進など新たな時代の要請を踏まえ、効率性・利便性を向上させた新たな自治体情報セキュリティ対策の検討を行い、令和２年12月に「地方公共団体における情報セキュリティポリシーに関するガイドライン」の改定を行った。

（8）地域の情報通信サービスのセキュリティの確保

12

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、単独で十分なセキュリティ対策を取ることが難しかったり、セキュリティ対策の必要性を認識するに至らなかったりするケースが存在するおそれがある。したがって、地域レベルのセキュリティの質を向上させるためには、関係者間でのセキュリティに関する「共助」の関係が構築されることが望ましい。

このため、地域で情報通信サービスを提供している事業者を含む各種民間企業、行政機関、教育機関、関係団体等が、顔の見える関係の中で、セキュリティについて相互に啓発を行う体制やコミュニティを構築していくことが重要である。その上で、このような体制等において、イベント等の継続開催による地域のセキュリティ意識向上・人材育成や、国や専門家を招へいした情報提供が持続的・自発的に実施されることが望ましい。このような関係者間でのセキュリティに関する「共助」の関係を構築されたコミュニティ（以下「地域SECUNITY」という。）が形成されることで、地域におけるセキュリティ対策の質の向上が持続的に図られることが期待される。

また、このような自律的に活動している「地域SECUNITY」が発展していく中で、「地域SECUNITY」同士が地域の枠を越えて情報共有や連携を行うことで、コミュニティとしての活動の活性化や新たな価値創造につながることが期待される。また、将来的には、各地域におけるセキュリティのニーズとシーズのビジネスマッチング、共同研究による地域発のセキュリティソリューションの開発など地域一体となった課題解決がなされていくことも期待される。

そのため、まずは、「地域SECUNITY」の構築に向け、関係府省庁と連携し、各地において地域単位でのコミュニティ構築を支援することが必要である。その際、国においては、地域の自主性を尊重しつつ、例えばコミュニティの成功事例のプロモーションや、セミナー・演習の実施に当たっての専門家の斡旋などの側面支援に注力していくことが重要である。

なお、当該施策の展開に当たっては、（６）の無線LANのセキュリティ対策やⅣ－（２）－②の実践的サイバー防御演習（CYDER）の実施、Ⅳ－（２）－⑤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、効果的に地域のセキュリティ対策の質の向上を図ることが重要である。

・「地域SECUNITY」に該当するコミュニティとして、関東地域において「関東サイバーセキュリティ連絡会」（2021年（令和３年）３月に立ち上げ）、北陸地域において「北陸サイバーセキュリティ連絡会」（2020年（令和２年）３月に立ち上げ）、東海地域において「東海サイバーセキュリティ連絡会」（2020年（令和２年）８月に立ち上げ）、中国地域において「中国地域サイバーセキュリティ連絡会」（2020年（令和２年）10月に立ち上げ）、四国地域において「地域SECUNITY形成促進事業／関係者会議」（2020年（令和２年）11月に立ち上げ）を立ち上げた。

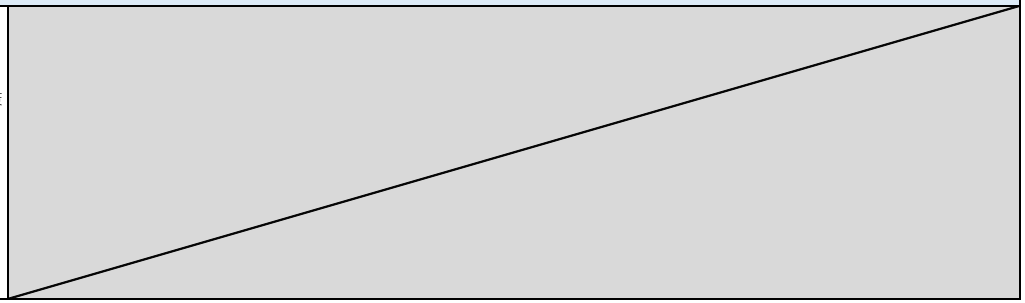
・各地域の「地域SECUNITY」を通じ、地域の情報通信サービスを提供している事業者を含む関連事業者・団体におけるセキュリティ意識啓発・対応能力向上のためのセミナーやサイバーインシデント対応演習を実施し、「地域SECUNITY」におけるサイバーセキュリティに関する共助の取組の推進を行った。

（9）テレワークシステムのセキュリティ対策		
13	テレワークは、時間や場所を有効に活用でき柔軟な働き方を実現するものであるとともに、COVID-19への対応という観点や、災害発生時も含めた業務継続という観点からも有効かつ重要なものである。中長期的な観点から、我が国においては少子高齢化に伴う生産年齢人口の減少への対処が要請されており、そのためにもテレワークの利活用を検討する必要がある。一方で、テレワークの実施に当たっては、職場環境に閉じたLANではなくインターネット経由での業務を前提とする必要があること、また、通常と異なる勤務環境やシステムを利用する場合も多いことから、適切なセキュリティ対策を採ることが必要である。また、企業間においてWeb会議システムを利用するケースにおいても同様に適切なセキュリティ対策を採ることが必要である。 このため総務省では、企業等がテレワークを実施する際のセキュリティ上の不安を払拭し、安心してテレワークを導入・活用するための指針として、2018年（平成30年）４月に「テレワークセキュリティガイドライン（第４版）」を作成している。さらに、COVID-19への対応等のため中小企業等においてもテレワークの導入が拡大する中で、当該ガイドラインをより具体的で分かりやすくした、実践的な内容のチェックリスト等が有用であり、総務省において早期に策定を行う必要がある。企業等においては、このようなガイドラインやチェックリスト等を活用することで、これからテレワーク環境を導入しようとする場合には適切なセキュリティ対策を採り、既にテレワーク環境を導入している場合にはセキュリティ対策の自己点検等を行うことが重要である。 また、COVID-19への緊急対応のため多くの企業では準備期間が十分とれずにテレワークを導入・導入検討していると想定されるが、特に中小企業等においては十分なセキュリティ知識を有した担当者がいない場合が多いと想定されるため、テレワーク導入時及び導入後においてセキュリティ対策の専門家が相談を受け付ける体制を提供する必要がある。 こうした取組と併せて、中小企業等のテレワークセキュリティに関する実態把握のための調査を行い、実際の業務やシステム構成に応じた活用しやすい取組としていくなど、セキュリティを確保したテレワーク環境を実現するための適切な支援策を講じていく必要がある。	・総務省では従来から「テレワークセキュリティガイドライン」を策定し、セキュリティ対策の考え方を示してきてたが、テレワークを取り巻く環境やセキュリティ動向の変化に対応するため2021年（令和３年）５月に全面的に改定を行った。 ・テレワークセキュリティガイドラインを補完するものとして、セキュリティの専任担当がいないような中小企業等においても、テレワークを 実施する際に最低限のセキュリティを確実に確保してもらうための「中小企業等担当者向けテレワークセキュリティの手引き(チェックリスト)」も2020年（令和２年）９月に初版を策定し、テレワークセキュリティガイドラインの改定と合わせて第２版に改定を行った。 ・企業等におけるテレワークに関するセキュリティ等の実態を把握するための調査をWebアンケートにより実施した。結果については、ガイドライン類と併せて、次のURLにて公表している。 https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/ ・テレワークセキュリティに関して、セキュリティの専門家に無料で相談できる窓口を2020年（令和２年）７月14日から2021年（令和３年）３月30日まで開設し、136件（内、自治体等25件、民間企業111件）の相談対応を実施した。
（10）電気通信事業者による高度かつ機動的なサイバー攻撃対策の実現		
14	サイバー攻撃はその定義からして、電気通信事業者のネットワークを経由し、ユーザに対してなされるものであり、サイバー攻撃の検知や防御等に関して電気通信事業者の果たす役割が大きい。 例えば、これまでIoT機器のセキュリティ対策については、IoT機器の技術基準の策定・運用やIoT機器の利用者向けの注意喚起など、端末側でのセキュリティ対策が中心であったが、今後は、より効率的かつ総合的なセキュリティ対策の実現のため、注意喚起等の取組と併せて、電気通信事業者が、個々の感染端末に指示を出すC&Cサーバに直接対処するといった、通信ネットワーク側における積極的なサイバー攻撃対策を推進することが期待される。 このため、IoTのセキュリティ対策を含め、様々な分野において、海外における動向（制度、実施状況等）も参考としながら、ユーザ側で運用している情報通信機器や情報システムのセキュリティ対策と連動する形で、インターネット上でISPが管理する情報通信ネットワークにおいても高度かつ機動的な対処を実現するための方策の検討が必要である。 具体的には、電気通信事業者が自らC&Cサーバを検知し、サイバー攻撃の指令通信の遮断等の対策を実施できるような環境整備に向け、通信の秘密に配慮した適切な対応を電気通信事業者が円滑に行うことが求められるところ、制度的な観点から対策の検討を行うことが重要である。なお、中長期的な課題として、通信の秘密の保護を図りつつ、より迅速なセキュリティ対策を実現するために、必要に応じ新たな視点からも検討を行うことが適当と考えられる。 また、技術的な課題解決のための取組も重要である。例えば、利用者のPCやIoT機器などがマルウェアに感染した場合に当該PCや機器に対して指令を与えるC&Cサーバの探索については、通信の秘密等の制度的観点に配慮しつつ、AIを活用して検知の高度化を図るなど、新技術を活用した対策の高度化を促進する必要がある。 さらに、これらの取組について、実際に通信ネットワークを活用して情報システムを運用しているユーザ企業向けの対策との連携を含め、関係府省庁とも連携して取組を推進していくことが重要である。	・電気通信事業者のネットワークへのサイバー攻撃等のリスクの深刻化を踏まえ、各電気通信事業者の対策の実施状況を把握すべく、2021年（令和３年）４月より、電気通信事業者に対してセキュリティ対策の取組状況等に関する調査を実施しているところである。 ・同年５月に、電気通信事業者におけるサイバーセキュリティ対策とデータの取扱い等に係るガバナンス確保の在り方についての検討を行う「電気通信事業ガバナンス検討会」を立ち上げたところ、本検討会において、上記調査の結果を踏まえ、既存の制度に基づく電気通信事業者による取組等の現状が、高まりつつあるサイバー攻撃等のリスクへの対策として適切であるか否かを検証していくこととしている。 ・また、電気通信事業者自らによるC&Cサーバの検知に関して検討を進めてきたところであり、今後、本文Ⅱ１（２）にあるとおり、電気通信事業者が自らC&Cサーバを検知し、検知したC&Cサーバに関する情報を電気通信事業者間で共有し、サイバー攻撃の予兆を捉えて早期に対処できるようにするため、制度的な観点から対策の検討を行う。

Ⅳ　横断的施策		
（１）研究開発の推進		
15	サイバー空間における攻撃の態様は常に変化しており、インターネットをはじめとするネットワークに接続される機器の更なる増加に伴い、サイバー攻撃の対象が拡大するとともに、AIの進展やサプライチェーンの複雑化等により、攻撃手法・能力が巧妙化・大規模化していくことが想定される。そのため、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」（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、「サプライチェーンリスクの増大」、「サイバーセキュリティ自給率の低迷」、「研究・技術開発に資するデータの活用」、「先端技術開発に伴う新たなリスクの出現」、「産学官連携強化の必要」、「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。特に、膨大化するサイバー攻撃に関する情報を高効率かつ有効に活用するためのサイバー攻撃観測技術等の高度化やサイバーセキュリティ情報を国内で収集・蓄積（生成）・提供するためのシステム基盤の構築、量子計算機時代等を見据えた安全に利用できる暗号基盤技術の確立、5G等の新たなネットワーク環境の進展を踏まえたセキュリティ検証技術の確立等について重点的に取り組む必要がある。 なお、サイバーセキュリティが社会経済活動のインフラとなりつつある現状を考慮し、研究開発を進めるに際して、サイバーセキュリティ技術の研究者だけでなく、法制度やAI等の専門家も取り込む形で、社会システム全体の中での位置づけを踏まえた実証等の取組を進めていく必要がある。また、国際標準化や国際連携についても積極的に進めることが求められる。	
①　サイバーセキュリティ統合知的基盤の構築		
16	我が国のサイバーセキュリティは、海外製品や海外サービスへの依存度が高い状況にある。そのため、国内のデータが海外に流出して分析される一方、我が国は海外で生成された脅威情報を高額で購入することでセキュリティ対策を講じてきた状況である。この状況を別の側面から見ると、実データの不足が、良質な国産のセキュリティ技術の創出・普及を阻害し、それが更に実データの不足をもたらすという「データ負けのスパイラル」に陥っていることが考えられる。 このため、我が国の企業の国際競争力強化はもちろんのこと、グローバルレベルの情報共有へのより一層の貢献や国際的に通用するエンジニアの効果的な育成、政府機関や重要インフラ事業者等のサービスを支えるセキュリティ技術が過度に海外に依存する状況の回避・脱却などの観点から、コア技術の開発・運用を中心に、国産技術・産業の育成を進めていくことが重要であり、我が国において、以下の取組を進める必要がある。なお、その際、我が国において必要なサイバーセキュリティ関連情報の収集・分析等を実施できるように仕組みを整えながらも、グローバルな協力・連携も含め、国際的なサイバーセキュリティの向上に貢献するという視点が重要である。 １）実データを大規模に集約・蓄積する仕組み 　具体的には産学官が連携して、各種公的機関等が観測した情報やインターネット上の公開情報（OSINT）を大規模に集約して蓄積する仕組みが考えられる。 ２）実データを定常的・組織的に分析する仕組み 　具体的には攻撃ツールや手法を並列かつリアルタイムに観測・解析する環境を構築するとともに、本環境を活用した高度解析者の結集・育成を行う仕組みが考えられる。 ３）実データで国産製品を運用・検証する仕組み 　具体的には国産製品のプロトタイプ群を長期運用・機能検証できる環境を構築するとともに、本環境を活用したSOC人材の育成を行う仕組みが考えられる。 ４）実データから脅威情報を生成・共有する仕組み 　具体的には１）～３）で収集した実データを用い、AIを駆使した大規模横断分析を行い、日本独自の脅威情報を生成し、信頼性の高い、説明可能かつ即時的なセキュリティ情報を関連機関で共有することが考えられる。 以上の取組を自律的に実施する仕組み・体制を構築し、国内でサイバーセキュリティ情報を収集・蓄積（生成）・提供する環境が必要である。	・NICTの「サイバーセキュリティネクサス（CYNEX）」を通じて、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（サイバーセキュリティ統合知的・人材育成基盤）の構築を開始した。

	② 基礎的・基盤的な研究開発等の推進	
17	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機能的な公開鍵暗号の研究開発、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）－②の脆弱性等を有するIoT機器の調査及び注意喚起と連携し、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。	・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。 ・サイバーセキュリティ技術については、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・模擬情報を用いたサイバー攻撃誘引基盤「STARDUST」の高度化を進めるとともに、標的型攻撃の解析結果について、関係機関との情報共有を行った。加えて、サイバーセキュリティ関連情報を大規模集約し、安全かつ利便性の高いリモート情報共有を可能とする「CURE」（キュア）を開発・実装するとともに、NICT内における集約データ間の突合分析を含む試験運用を行った。 ・また、暗号技術分野については、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を行った。 ・引き続き、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く。
	③ IoT機器のセキュリティ対策技術の研究開発の推進	
18	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。 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。一方で、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）－②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。 さらに、増加し続けるIoTマルウェアを無害化・無機能化する技術を確立すべく、2020年度（令和２年度）～2022年度（令和４年度）までの３年間を実施期間とし、「電波の有効利用のためのIoTマルウェアの無害化/無機能化技術等に関する研究開発」に取り組むこととしている。 本研究開発を通じ、AI技術を駆使したIoTマルウェアの挙動検知及び駆除技術、マルウェアに感染したIoT機器を無害化・無機能化する技術の開発に取り組む必要がある。	・既存の広域ネットワークスキャン技術は、IoT機器が接続されたネットワークに対して網羅的に行うものであるため、IoT機器が増加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。このため、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指して、2018年度（平成30年度）から「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」に取組む、2020年度（令和２年度）に終了した。本研究開発の成果は、ITU-T 勧告Q.4062の標準化に寄与するなど IoT試験の効率的実施に寄与するのみならず、安定したネットワーク・機器制御情報などの伝送や遅延耐性のあるアプリケーションの効率的配信にも活用できると期待される。 ・また、引き続き、IoTマルウェアの挙動検知及び駆除技術、マルウェアに感染したIoT機器を無害化・無機能化する技術の開発を目的とした「電波の有効利用のためのIoTマルウェアの無害化/無機能化技術等に関する研究開発」は取組みを進める。

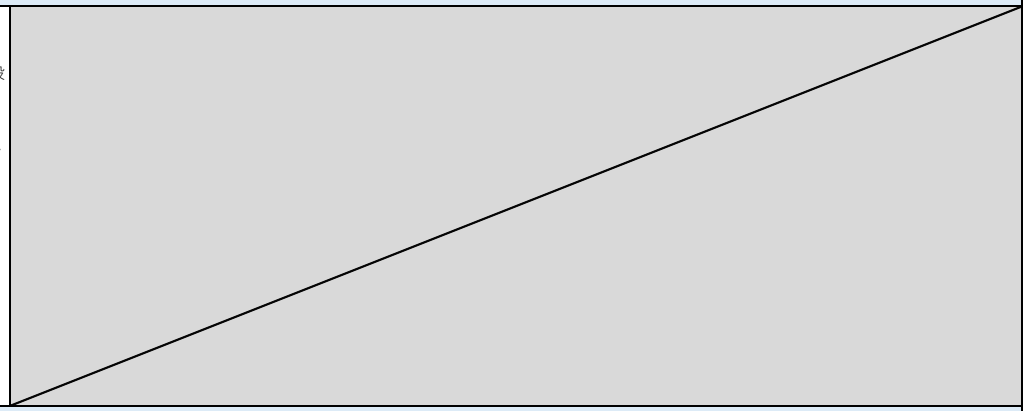
	④　脆弱性の検証手法等の確立と体制整備【再掲】	
19	5Gのネットワークに関しては、仮想化・ソフトウェア化が進むことから、サプライチェーンリスクを含む新たなサイバーセキュリティ上の課題が懸念される。そのため、5Gのネットワークやその構成要素及びサービスについて、ソフトウェア・ハードウェアの両面から技術的検証を行うことを通じ、5Gのネットワークのセキュリティを確保する仕組みや体制を整備することが必要である。 具体的には、まず、ソフトウェアを中心としたネットワークの脆弱性については、5Gの通信インフラとしての機能保証のため、ソフトウェアにより構成される部分を含め、ネットワーク全体のセキュリティを確保する必要がある。 そのため、5Gの仮想環境を構築し、(a)オープンソースソフトウェア等の解析、(b)多種多様なパターンのデータ入力による異常動作確認（ファジング）、(c)エシカルハッカーによる脆弱性調査・脅威分析を実施し、対策を検討することが必要である。 一方、ハードウェアの脆弱性については、5G等のネットワークを構成するハードウェア上に故意に組み込まれた不正なチップによって生じるセキュリティ上の課題に対応するため、AIを活用し(a)回路情報から不正に改変された回路を検知する技術や、(b)電子機器外部で観測される情報から不正動作を検知する技術を開発し、対策を検証することが必要である。 また、上記の検証結果を踏まえつつ、5G等のネットワーク上での運用面の課題等についても検討する必要がある。 その上で、技術移転などを含めて前述のような脆弱性検出技術の成果を活用し、関連する脅威の分析の視点を踏まえつつ、システムや利用者に対するインパクト分析を実施し、必要なセキュリティ対策を検討することが必要である。また、このような検証・分析の取組において、5Gの事業者・運用者やベンダー等が協力して実施する体制を構築することが必要である。	【Ⅲ(2)①の再掲】 ・5G については、携帯電話事業者による全国向け 5G サービスと、地域の企業や自治体等の様々な主体が自らの建物や敷地内でスポット的に柔軟にネットワークを構築し利用可能とするローカル 5G の取組が開始されている。 ・総務省において、2019 年度（令和元年度）より、5G ネットワークにおけるソフトウェアの脆弱性に対応するための調査検討を実施している。2020 年度（令和 2 年度）は、5G の通信インフラとしての機能保証のため、ソフトウェアにより構成される部分を含め、ネットワーク全体のセキュリティを確保する必要があることから、5G 仮想環境の対象を、コアネットワークのみならず、モバイルエッジコンピューティング（MEC)まで拡張し、オープンソースソフトウェア等の解析、多種多様なパターンのデータ入力による異常動作確認（ファジング）、エシカルハッカーによる脆弱性調査、脅威分析の実施に向けて取り組んだ。 ・ハードウェア脆弱性への対応は、外部から調達した設計ツールや設計部品を用いたチップの安全性を担保するために、設計・製造におけるチップの脆弱性検知手法の調査検討を実施しており、令和 2 年度は標準的なベンチマーク回路等を用いて、不正回路の種類及びその機能を明確化し、不正回路を検知する技術の開発を行った。加えて、回路情報が入手できないチップの安全性を担保するために、市販の組込みマイコン等、比較的簡易な電子機器の動作のもと、電子機器の外部から観測される情報を用いて、不正動作を検知する技術の開発を行った。 ・引き続き、ハードウェアチップの脆弱性検知手法の確立を目的として、ハードウェアチップの回路情報を用いて不正回路を検知する技術及び電子機器の外部から観測される情報を用いて不正動作を検知する技術の改良及び基礎的な検証を実施する。
	⑤　スマートシティのセキュリティ対策【再掲】	
20	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、「Society 5.0の先行実現の場」である。 この点、総務省では、都市や地域が抱える様々な課題の解決や地域活性化・地方創生を目的として、ICTを活用した分野横断的なスマートシティ型の街づくりに取り組む「データ利活用型スマートシティ推進事業」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することが想定され、常にサイバー攻撃の脅威にさらされるおそれがあるため、IoT機器の監視を行うセキュアゲートウェイの在り方についての検討が重要である。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が必要となることが想定される。また、スマートシティには多様な主体が関わることが想定されるため、システム全体としてのセキュリティのPDCAサイクルや、平時・有事のセキュリティ確保の体制としてのSOC又はCSIRTの在り方についても検討が必要となることが想定される。 以上を踏まえ、スマートシティのセキュリティ確保の在り方について、多様な関係者間で一定の共通認識の醸成が必要である。具体的には、スマートシティ官民連携プラットフォームのスマートシティセキュリティ・セーフティ分科会など、官民の検討の場において、スマートシティのセキュリティ確保の観点から留意すべき要件やチェックすべき事項などについて検討を行い、明確化を図ることが必要である。またその際は、スマートシティを推進する取組との連携を図り、セキュリティ対策の実装を促進していくことが重要である。 なお、スマートシティは、地域におけるIoTや5G、クラウドサービスのユースケースとしての側面もあり、Ⅲ－（１）のIoTのセキュリティ対策や、Ⅲ－（２）の5Gのセキュリティ対策、Ⅲ－（３）のクラウドサービスのセキュリティ対策の取組等の連携を図ることが重要であるほか、Ⅲ－（８）の地域の情報通信サービスのセキュリティの確保や（２）－⑤の地域のセキュリティ人材育成の取組など、地域のセキュリティ強化の取組と連携を図ることも重要である。 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	【Ⅲ(4)の再掲】 ・スマートシティ官民連携プラットフォームのスマートシティのセキュリティ・セーフティ分科会の活動において、スマートシティにおけるセキュリティの在り方について議論・意見交換を行った。 ・2020年（令和２年）10月、スマートシティのセキュリティの在り方について整理した「スマートシティセキュリティガイドライン（第1.0版）」を公表した。 ・その後、総務省が実施したスマートシティセキュリティの取組実態調査や、スマートシティのセキュリティ・セーフティ分科会や各種有識者会合における意見を踏まえ、「スマートシティセキュリティガイドライン（第1.0版）」の改定を検討し、2021年（令和３年）６月に「スマートシティセキュリティガイドライン（第2.0版）」として公表した。
	⑥　衛星通信におけるセキュリティ技術の研究開発	
21	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。	・「衛星通信における量子暗号技術の研究開発」において令和２年度は装置の試作等を実施。 ・引き続き2021年度（令和３年度）は国際宇宙ステーション（ISS）における実証に向けた装置の製作及び機能検証等を実施予定。

	⑦　量子コンピュータ時代に向けた暗号の在り方の検討	
22	総務省及び経済産業省は共同で、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CRYPTREC を実施している。この中で、NICT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等の役割を担っており、2022年度（令和４年度）末を目途とする電子政府推奨暗号リスト（CRYPTREC暗号リスト）の改定の検討においても積極的にその役割を果たしていく必要がある。 また、今後、大規模な量子コンピュータの実用化により、現在の公開鍵暗号（RSA暗号や楕円曲線暗号）が将来的に解読されるおそれがある こと等を踏まえ、2019年度（令和元年度）からCRYPTREC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」を設置し、量子コンピュータ時代の推奨暗号の在り方について検討を実施している。2019年度（令和元年度）の検討においては、CRYPTREC暗号リストとは別に「耐量子計算機暗号（PQC）」に関するガイドラインを作成することが適当とされているほか、今後利用が拡大すると想定されるIoT機器等に用いられる「軽量暗号」や、暗号状態で情報処理が可能な「高機能暗号」についてもガイドラインを作成することが適当とされたところである。 総務省等においては、量子コンピュータの開発状況や耐量子計算機暗号（PQC）の標準化状況のフォロー等を行うため、引き続き同タスクフォースでの検討を継続するとともに、CRYPTREC暗号リストの改定と並行して耐量子計算機暗号等に関するガイドラインの検討を行っていくことが重要である。	・CRYPTRECを通じてCRYPTREC暗号リストに掲載された暗号技術の監視、安全性及び信頼性の確保のための調査、研究、基準の作成等を行った。 ・また、社会ニーズを見据え、暗号を安全に利活用するための取組などについて検討した。また、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設置し、量子コンピュータや新たな暗号技術の動向等を踏まえ、我が国の暗号の在り方と課題についての議論や、次期CRYPTREC暗号リストが満たすべき条件の整理を進めた。
	⑧　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	
23	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、製造・ビル等の分野における実証実験を開始し、本取組を着実に進めることが重要である。	・戦略的イノベーション創造プログラム（SIP）第2期「IoT社会に対応したサイバー・フィジカル・セキュリティ」においては、『サイバー・フィジカル・セキュリティ対策基盤』の研究開発及びその社会実装を推進すべく、IoTシステム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等について研究開発を実施した。 ・引き続き研究開発を行うとともに、ビル等の分野における実証実験等を通じて要素技術を確立する。
	（2）人材育成・普及啓発の推進	
24	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、総務省は、NICTの「ナショナルサイバートレーニングセンター」を通じて、実務者層・技術者層及び若年層を対象とした次の人材育成施策を実施しており、引き続き取り組んでいく必要がある。 １）　国の機関、地方公共団体、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（CYDER） ２）　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）　若手セキュリティイノベーターの育成（SecHack365） また、これらの取組に加え、組織の戦略マネジメント層やICT環境構築技術者・開発者等も含む人材育成を産学官が連携して行うための仕組みや、地域におけるセキュリティ能力向上のための人材育成の仕組みについても検討を進める必要がある。	

	①　人材育成オープンプラットフォームの構築	
25	②の実践的サイバー防御演習（CYDER）の実施等を通じた人材育成を行っているものの、我が国全体としてはサイバーセキュリティ人材のニーズはあるが育成が不十分な状況である。特に、戦略を立ててシステムベンダと共働しつつ組織のセキュリティ対策を先導できる人材が不足しているほか、環境構築技術者・開発者層のセキュリティ知識の不足により、本来防げるはずのセキュリティインシデントが発生している。 このような人材育成を全て国で実施することは困難であるため、特に民間事業者において大学等の教育機関を巻き込みながら自立的に育成を行うことが求められるが、演習用の環境構築やシナリオ開発には高度な知識や技術力、そして基盤となる計算機環境が必要であり民間企業・教育機関のみでは十分に対応できていない。また、このような不十分な国内基盤を背景として、既存の民間演習事業においても、海外の演習教材に依存し、日本特有の事例が反映できない状況である。 こうした課題に対応するため、サイバーセキュリティの人材育成に関し、演習の実施に関する様々な要素（データセット、教材、演習用ミドルウェア、計算機リソースなど）を総合的にカバーする、オープン型の新たな人材育成プラットフォームや、産学官の連携によって当該プラットフォームを積極的に活用するためのコミュニティの支援が必要である。	・NICTの「サイバーセキュリティネクサス（CYNEX）」を通じて、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（サイバーセキュリティ統合知的・人材育成基盤）の構築を開始した。
	②　実践的サイバー防御演習（CYDER）の実施	
26	総務省はNICTを通じ、行政機関等の実際のネットワーク環境を模した大規模仮想LAN環境を構築の上、国の機関等 、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）を実施している。また、CYDERで使用する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ものを提供している。 サイバー攻撃は年々増加していることから、社会全体としてサイバーセキュリティ対応力を強化することは急務であり、実際のインシデント発生時に対応を行う情報システム担当者等に対する人材育成の取組は特に重要である。防災訓練と同様に定期的に演習を経験することで実対応時の能力向上を図るよう、CYDERによる人材育成を引き続き実施する必要がある。 また、地方公共団体には未受講の団体もあり、そのような団体が我が国におけるサイバーセキュリティ対策上の穴とならないよう、2020年（令和２年）１月に公表した緊急提言を踏まえ、総務省と都道府県が緊密に連携し、都道府県ごとに受講計画を策定するなどの取組により受講の促進を図っていく必要がある。 NICTにおいても、開催日程や開催場所の工夫などの運営面の継続的見直しによって受講機会を拡大するとともに、地理的な要因等により未受講となっている地方公共団体を主な対象として、オンラインでの受講を可能とする演習環境の整備を早期に実施することが求められる。	・実践的サイバー防御演習「CYDER」は、2017年度（平成29年度）から、NICTのナショナルサイバートレーニングセンターを通じて実施している。 ・2020年度（令和２年度）は、演習を106回実施し、計2,648名が受講した。 ・地方公共団体（1,788団体）においては、2019年度（令和元年度）までの未受講団体は844団体であったが、2020年度（令和２年度）にはこのうち257団体が受講したことから、残る未受講団体は587団体である。
	③　東京大会に向けたサイバー演習の実施	
27	総務省はNICTを通じ、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2017年度（平成29年度）から実施している。 本演習においては、大規模演習環境を用いて、東京大会の公式サイト、大会運営システム等ネットワーク環境を再現した、演習環境（仮想ネットワーク環境）を構築し、東京2020大会時に想定されるサイバー攻撃を擬似的に発生させ、本格的な攻防型演習等を実施している。さらに、実機演習を補完する形で、2018年度（平成30年度）からは講義演習形式により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ている。 2021年（令和３年）に延期された東京大会の円滑な実施に向け、大会組織委員会と緊密な連携を図りながら、引き続き本取組を着実に実施する必要がある。	・2020年東京大会に向けた実践的サイバー演習「サイバーコロッセオ」は、2017年度（平成29年度）から、NICTのナショナルサイバートレーニングセンターを通じて実施し、2020年度（令和２年度）で目標とする人材育成を完了した。 ・2020年度（令和２年度）は、実機演習を行う「コロッセオ演習」において延べ168名が受講し、2017年度（平成29年度）からの合計で延べ571名が受講した。また、講義形式により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」において延べ378名が受講し、2018年度（平成30年度）からの合計で1,717名が受講した。
	④　若手セキュリティ人材の育成の促進	
28	総務省はNICTを通じ、25歳以下の若手ICT人材を対象として、既存ツールを単にユーザとして利用するだけではなく、自ら手を動かしてセキュリティに関わる新たなモノづくりができる人材（セキュリティイノベーター）の育成施策「SecHack365」を2017年度（平成29年度）から実施している。 この取組は、NICTの持つサイバーセキュリティの研究資産を活用しながら、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・開発を、第一線で活躍する研究者・技術者が１年かけて継続的かつ本格的に指導することが特徴である。NICTの有する遠隔開発環境を活用し、年中どこからでも遠隔開発実習が可能であり、こうしたオンライン環境に加え集合研修等を行うことで高度な人材育成を実施している。 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。	・25歳以下の若手ICT人材を対象として、新たなセキュリティ対処技術を生み出しうる最先端のセキュリティ人材（セキュリティイノベーター）を育成する取組である「SecHack365」は、2017年度（平成29年度）から、NICTのナショナルサイバートレーニングセンターを通じて実施している。 ・2020年度（令和２年度）は41名が修了し、2017年度（平成29年度）からの合計で171名が修了している。

	⑤　地域のセキュリティ人材育成	
29	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。サイバー攻撃は地理的な距離に関係なく、弱いところがターゲットとな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。 2019年度（令和元年度）に実施したモデル事業において、地域の中小企業等の多くは、セキュリティ対策に関する問題意識が強くなく、その必要性をそもそも認識していない場合が多いという結果が判明しており、地域の中小企業等においてサイバーセキュリティに関する気づきを得ていただくための活動が必要である。このような活動を地域において自立的かつ継続的に行うためには、地域のセキュリティリーダー（セキュリティファシリテーター）となる人材の育成や、自らセキュリティに関する問題意識を持って活躍しようとしている人材が必要となることから、総務省においてこうした人材の育成を支援する方法について検討していく必要がある。 また、地域においては、セキュリティに関する雇用の受け皿がないことから、若年層がセキュリティ人材を目指さず、地域におけるセキュリティ人材が更に不足するという悪循環がある。そのため、地域においてセキュリティを地場産業化しようとしている民間企業等と総務省が連携し、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ことについて、その有効性の検討を行う必要がある。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。 総務省においては、モデル事業の実施等を通じてこれら地域人材の育成に関する取組を引き続き実施し、その成果はモデル事業対象地域以外でも横展開して活用できるように進めていく必要がある。	・地域コミュニティにおいて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するためのエコシステムを目指し、エコシステム構築に必要となる育成カリキュラム等の育成モデルを構築するための実証事業を沖縄県にて実施した。 ・地域のセキュリティリーダー（セキュリティファシリテーター）となる人材については、2019年度（令和元年度）の実施結果を踏まえ、自立的な人材育成に適した方策について検討している。
	（3）国際連携の推進	
30	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。 2019年（令和元年）６月に開催されたG20大阪サミットでは、我が国主導の下デジタル経済に関する議論が行われ、データ・フリー・フロー・ウィズ・トラスト（DFFT：信頼性のある自由なデータ流通）の概念が合意された。データの自由な流通を促進するため、サイバーセキュリティをはじめとする課題に対処することが必要であり、我が国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各国をはじめとするインド太平洋地域等との連携	
31	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）～2022年（令和４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デジタル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サイバー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におけるサイバー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。 加えて、「自由で開かれたインド太平洋（FOIP）」構想等の政府戦略を踏まえつつ、各国との連携を強化することが重要である。	・2018年（平成30年）９月にタイのバンコクに設立した「日ASEANサイバーセキュリティ能力構築センター（AJCCBC：ASEAN Japan Cybersecurity Capacity Building Centre）」において、ASEAN各国の政府機関及び重要インフラ事業者のサイバーセキュリティ担当者を対象に実践的サイバー防御演習（CYDER）、デジタルフォレンジック演習及びマルウェア解析演習を定期的かつ継続的に実施しており、これまでに500名以上が参加した。また、同センターではASEAN各国から選抜された若手技術者・学生がサイバー攻撃対処能力を競う「Cyber SEA Game」も開催しており、直近では2020年（令和２年）12月に実施した。さらに、AJCCBCの取組を円滑に進めるため、プロジェクト・ステアリング・コミッティーの構成員として必要な支援・助言を行っている。新型コロナウイルス感染症の影響でセンターの施設において演習等を実施することが困難となったため、既存の演習等についてオンラインで実施可能となるようプログラムを改編し、2021年6月よりオンラインでの提供を開始した。また、サイバーセキュリティに係る基礎的な知識を教授するための自己学習コースやCTF（Capture The Flag）形式の実践的解析演習コースといった教材を新たにオンラインで提供し、ASEAN各国に利用いただいた。 ・一方、2020年（令和２年）10月にオンラインで開催された「第13回日・ASEANサイバーセキュリティ政策会議」では、直近１年間の各国のセキュリティ政策について意見交換を行ったほか、サイバーインシデントへの対処協力、重要インフラ防護の実践事例の共有及びサイバーセキュリティ人材の育成等の協力活動の確認・評価を行った。 ・2021年（令和３年）１月にオンラインで開催された「第1回日ASEANデジタル大臣会合及び第1回日ASEANデジタル高級実務者会合」では、今後１年間の日ASEAN間の協力・連携施策について、サイバーセキュリティを含めたICT分野における更なる連携の実現に向けた「ICTワークプラン2021」がとりまとめられた。 ・2021年（令和３年）１月にオンラインで開催された「第11回ISP向け日ASEAN情報セキュリティワークショップ」では、日本及びASEANのISP間で、サイバーセキュリティに関する最新動向、自組織の課題、取組や計画等についての情報共有等を行った。同ワークショップの枠組みを用いて、恒常的な情報共有や意見交換等を可能とするオンライン上の基盤を構築し、その活用を図っている。 ・他方、2020年度にBYOD（Bring Your Own Device）セキュリティ対策ソリューションの実証実験をマレーシアの大学にて実施した。実証実験終了後の2021年３月に、マレーシアサイバーセキュリティ庁と共催で、本実証実験の説明やその他企業が自社の製品を紹介しつつサイバーセキュリティ対策について説明するウェビナーを実施し、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展開を図った。
	② 国際的なISAC間連携	
32	サイバー攻撃は国境を越えて行われるため、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、2019年（令和元年）11月に一般社団法人ICT-ISACと米国のIT-ISACとの間でサイバーセキュリティ上の脅威に対する情報共有体制の一層の強化を目的として締結された覚書に基づき、国際連携ワークショップの開催等を通じて、一般社団法人ICT-ISACと米国のICT分野のISACとの連携を更に強化し、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。また、こうした取組を国際的に拡大することも重要である。	・2021年（令和３年）４月にオンラインで開催された「第５回ISAC国際連携ワークショップ」が、総務省、米国国土安全保障省、日米のISAC代表者等の参加のもと開催され、日米ISAC間での情報共有を促進するための具体的方策について議論した。 ・豪州や欧州のISAC関連組織と日本のISACとの連携も深めるべく、ワークショップ等の開催に向けて総務省が中心となって調整を進めている。
	③ 国際標準化の推進	
33	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など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。	・国内関係機関と連携し、我が国からISO/IEC JTC1 SC27及びITU-T SG17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」をベースとした勧告・標準の策定に向けて寄与文書を入力するなど、国際標準化の議論に参加・貢献した。2020年（令和２年）８月から９月及び2021年（令和３年）4月にオンラインで開催されたITU-T SG17会合では、IoTシステムのためのセキュリティ管理策に関する勧告案について議論が実施された。 ・また、ISO/IEC JTC1 SC27会合でも、IoTにおけるセキュリティ及びプライバシーのためのガイドラインの策定に向けた議論が実施された。 ・さらに、ITU-T SG17会合においては、「自由、公正かつ安全なサイバー空間」という我が国のサイバーセキュリティ戦略上の基本的な理念に必ずしも整合的でない標準化に向けた提案に対しては、有志国と連携しつつ見直し等を促す対応を行った。

	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	
34	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、NOTICE等のIoTセキュリティ対策をはじめとした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、相手国の状況に応じて国際連携の場で共有をし、各国の取組につながるよう働きかけるとともに、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。総務省は、イスラエル・国家サイバー総局との間で2018年（平成30年）11月に締結した覚書に基づき人材育成協力を推進しており、引き続きこうした取組を拡大することが重要である。	・二国間協議については、2020年（令和２年）９月にオンラインで行われた「インターネットエコノミーに関する日米政策協力対話」、同年10月にオンラインで行われた「日EU・ICT戦略ワークショップ」、同年12月にオンラインで行われた「日ベトナムICT共同作業部会」、同年12月にオンラインで行われた「日中韓サイバー協議」、2021年（令和３年）２月にオンラインで行われた「日EU・ICT政策対話」、同年３月にオンラインで行われた「日独ICT政策対話」、同年４月にオンラインで行われた「日EU・ICT戦略ワークショップ」、同年５月にオンラインで行われた「日独サイバー協議」、「日米サイバー協議（課長級）」などを通じて、各国とサイバーセキュリティ政策の共有等を行い、関係強化及び信頼醸成に取り組んだ。 ・また、2018年（平成30年）11月にイスラエル国家サイバー総局との間で締結したサイバーセキュリティ分野における協力覚書に基づき、両国間で政策の情報交換を継続するとともに、人材育成に関してSecHack365修了生が2021年（令和３年）４月に開催されたサイバーテックグローバル2021に登壇するなど協力を深化させた。 ・対サイバー攻撃アラートシステム（DAEDALUS）によるアラートの提供について欧州等の国々に呼びかけ、提供を希望する国との連携を図っている。
（４）情報共有・情報開示の促進		
35	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（平成31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。さらに、民間の取組としては、サイバー攻撃や事故への事前の対処、及び、障害発生時の事案対処や復旧に関する情報などについて事業者間で共有することを目的としたISACがいくつかの業界で立ち上げられており、緊急提言おいて、他の重要インフラ分野等でのISACの立ち上げの促進や国際間を含むISAC間の連携を促進することの必要性について指摘したところである。 以上を踏まえつつ、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、更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】	
36	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など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（認定協会）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。	・2019年（平成31年）２月より、「NOTICE」プロジェクトにおいて、電気通信事業者間の情報共有の結節点となる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。）の機能を活用し、認定協会経由でパスワード設定等に不備のあるIoT機器に関する情報をISPに通知しているところである。 ・また、2021年（令和３年）２月から７月にかけて、海外の捜査当局から警察庁に対して提供された国内のEmotetに感染している機器に関する情報を認定協会経由でISPに通知し、当該情報に記載されている機器の利用者に対して注意喚起を実施した。 ・更に、2020年（令和２年）２月に、一般社団法人ICT-ISACにおいて広く5Gセキュリティに係る情報共有を進めることを目的とした「5Gセキュリティ推進グループ」が立ち上げられたところ、当該グループにおいて、ローカル5Gを提供する事業者やローカル5Gを利用する主体にとって参考となる、ローカル5Gのセキュリティガイドラインの作成に着手した。

	② 事業者間での情報共有を促進するための基盤の構築	
37	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、情報共有の内容や範囲に配慮しつつ、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。	・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のため、総務省において、2019 年度（令和元年度）から、脆弱性情報をその影響を受けるソフトウェアと紐付けた形で配布する仕組みの検討を実施するとともに、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している。 ・2020 年度（令和 2 年度）は、IPA にて公表される脆弱性情報等をSTIX 形式にて情報共有基盤上で共有し資産管理ツール上で紐付けを行うとともに、機械学習によって評価された深刻度評価情報の統合に向けた実証試験を行った。

	③　サイバーセキュリティ対策に係る情報開示の促進	
38	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、こうした取組を更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。 この点、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。引き続き、民間企業の情報開示を促進するため、本手引きの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。 なお、2019年度（令和元年度）においては、企業等において様々なインシデントが発生していたところであり、発生後にどのように対応し公表をしていくかという点も含め、サイバーセキュリティ対策に関する情報開示は引き続き重要な課題である。 今後は、各企業に加え、マスメディア・格付機関など、企業による情報開示をステークホルダーに伝達する主体を含めた産業界全体における情報開示の取組を促進していくことが重要である。	・一般社団法人日本IT団体連盟に設置されたサイバーセキュリティ委員会の企業評価分科会にオブザーバとして参加し、「サイバーセキュリティ対策情報開示の手引き」等に基づき、必要に応じて助言を行った。当該分科会は、日経225を対象に開示情報から各社のサイバーセキュリティの取組姿勢に関する調査を行い、2020年（令和２年）11月に調査結果を公表した。
	④　サイバーセキュリティ対策に係る投資の促進	
39	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、全国5G及びローカル5Gについては、サイバーセキュリティ等を確保しつつその適切な開発供給及び導入を促進するため、全国5G及びローカル5Gの導入事業者に対する税制優遇措置や導入事業者及び開発供給事業者に対する金融支援の実施を盛り込んだ「特定高度情報通信技術活用システムの開発供給及び導入の促進に関する法律」が2020年（令和２年）５月に成立したところであり、今後、税制優遇及び金融支援措置が積極的に活用されるよう、その早期施行に向け必要な準備を進めることが必要である。	・既述のとおり、安全性・信頼性の確保等を図るための指針を含む、特定高度情報通信技術活用システムの開発供給及び導入の促進に関する法律及びその下位法令が施行され、これに基づき、開発供給計画及び導入計画を認定し、①全国キャリアの高度な送受信装置等の前倒し整備や、②ローカル5Gの送受信装置等の設備投資に向けた動きが進展している。
	⑤　国際的なISAC間連携【再掲】	
40	サイバー攻撃は国境を越えて行われるため、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、2019年（令和元年）11月に一般社団法人ICT-ISACと米国のIT-ISACとの間でサイバーセキュリティ上の脅威に対する情報共有体制の一層の強化を目的として締結された覚書に基づき、国際連携ワークショップの開催等を通じて、一般社団法人ICT-ISACと米国のICT分野のISACとの連携を更に強化し、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。また、こうした取組を国際的に拡大することも重要である。	【Ⅳ(4)⑤の再掲】 ・二国間協議については、2020年（令和２年）９月にオンラインで行われた「インターネットエコノミーに関する日米政策協力対話」、同年10月にオンラインで行われた「日EU・ICT戦略ワークショップ」、同年12月にオンラインで行われた「日ベトナムICT共同作業部会」、同年12月にオンラインで行われた「日中韓サイバー協議」、2021年（令和３年）２月にオンラインで行われた「日EU・ICT政策対話」、同年３月にオンラインで行われた「日独ICT政策対話」、同年４月にオンラインで行われた「日EU・ICT戦略ワークショップ」、同年５月にオンラインで行われた「日独サイバー協議」、「日米サイバー協議（課長級）」などを通じて、各国とサイバーセキュリティ政策の共有等を行い、関係強化及び信頼醸成に取り組んだ。 ・また、2018年（平成30年）11月にイスラエル国家サイバー総局との間で締結したサイバーセキュリティ分野における協力覚書に基づき、両国間で政策の情報交換を継続するとともに、人材育成に関してSecHack365修了生が2021年（令和３年）４月に開催されたサイバーテックグローバル2021に登壇するなど協力を深化させた。 ・対サイバー攻撃アラートシステム（DAEDALUS）によるアラートの提供について欧州等の国々に呼びかけ、提供を希望する国との連携を図っている。
	⑥　5Gの脆弱性情報や脅威情報等の共有の枠組みの構築【再掲】	
41	4Gまでの従来の移動通信システムでは電気通信事業者がネットワークの運用を行っていたが、5Gの時代では、ローカル5Gについて、従来は通信サービスのユーザとしての位置づけであった様々な企業や自治体等がネットワークの運用者として関わっていくこととなる。 また、ネットワークの用途も、超低遅延や多数同時接続などの特長を活かした様々な産業用途が期待されているため、リスクや脅威の在り方も多様なものが想定される。 このため、5Gのセキュリティを確保していく上では、Ⅲ－（２）－①の脆弱性の検証と合わせ、5Gのネットワークを運用している事業者・運用者やベンダー、利用者等の間での脆弱性情報や脅威情報、さらにこれらの対処の在り方に関する情報の共有の取組が重要である。 この点、5Gとそのセキュリティに関する情報共有などを定期的に実施して5Gのセキュリティの啓発を進めるとともに、ローカル5Gを含む5Gの運用者が5Gサービスを提供する場合のサイバーセキュリティ上の懸念や脅威に関する問い合わせに対して助言を行うことを目的とし、2020年（令和２年）２月に一般社団法人ICT-ISACにおいて「5Gセキュリティ推進グループ」が設立されたところである。 上記のような民間での取組を踏まえつつ、引き続き、5Gのセキュリティの確保に向け、情報共有の取組を促進することが必要である。	【Ⅲ(2)②の再掲】 ・一般社団法人ICT-ISACの5Gセキュリティ推進グループにおいて、ローカル5Gを含む5Gの運用者に対する助言を行うための枠組を構築し、ローカル5G免許を取得した事業者への参画の働きかけを実施した。 ・一般社団法人ICT-ISACの5Gセキュリティ推進グループにおいて、ローカル5Gを提供する事業者やローカル5Gを利用する主体にとって参考となる、ローカル5Gのセキュリティガイドラインの作成に着手した。