資料　31－3

「IoT・5Gセキュリティ総合対策2021（仮称）」の方向性（案）

2021年5月

サイバーセキュリティタスクフォース事務局

本タスクフォースにおけるこれまでの議論について

■ 過去５回のサイバーセキュリティタスクフォースにおいて、2020年（令和２年） ７月の「IoT・5Gセキュリティ総合対策2020」の策定・公表以降のサイバー攻撃をめぐる最近の動向や総務省におけるサイバーセキュリティ政策について御議論いただいてきたところ。

回　次	議　事　内　容
第26回 （R2.10.12）	✓ 「IoT・5Gセキュリティ総合対策2020」を踏まえた最近の取組状況
第27回 （R2.12.3）	✓ サイバー攻撃をめぐる最近の動向 ✓ 今後の検討課題について
第28回 （R3.2.8）	✓ サイバーセキュリティ統合知的・人材育成基盤について ✓ テレワークセキュリティガイドラインについて
第29回 （R3.3.9）	✓ スマートシティセキュリティガイドライン改定の方向性について ✓ 電気通信事業者のネットワークの安全・信頼性の確保に向けた取組について ✓ サイバー攻撃被害情報の共有と公表のあり方について ✓ サイバーセキュリティ分野における国際連携について
第30回 （R3.4.7）	✓ 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等について ✓ クラウドサービス利用時のセキュリティ向上に関する取組について ✓ 情報通信ネットワークの将来像とセキュリティ技術に関する標準化を巡る議論の動向について ✓ 「IoT・5Gセキュリティ総合対策2021（仮称）」の構成（案）について

「改定に当たっての主要な政策課題」について

- COVID-19感染症対応において、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るようになっている。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**重要な政策課題となっている**。

- 政府においても、「デジタル社会の実現に向けた改革の基本方針」を決定し（令和２年12月25日閣議決定)、**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、社会全体のデジタル改革・DX推進のためには、**国民一人ひとりが安心してその基盤となるデジタルを活用できるよう、サイバーセキュリティを確保することが前提**となる。

- こうした考えに基づき、「IoT・5G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推進の前提として**、国民が安心してデジタルを活用できる環境を整備するために**サイバーセキュリティを確保すること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としてはどうか**。

- 具体的には、次ページのとおりの構成（方向性）としてはどうか。

「IoT・5Gセキュリティ総合対策2021（仮称）」の方向性について

■ 本タスクフォースでの御議論や昨今のサイバーセキュリティの現状を踏まえ、「IoT・5Gセキュリティ総合対策2020」について、**「主要な政策課題」を改める**とともに、**各施策に関する記載について、対応する課題ごとにまとめながら内容を更新する**形で改定することとしてはどうか。

IoT・5Gセキュリティ総合対策2021（仮称）

【背景及び改定に当たっての主要な政策課題】
○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

【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
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
③５Ｇの本格的な普及に向けたセキュリティ対策の強化
（２）COVID-19への対応を受けたセキュリティ対策の推進
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
（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
①IoT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
（４）その他の具体的施策
①無線LANのセキュリティ対策
②放送分野のセキュリティ対策
③地域の情報通信サービスのセキュリティの確保

【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
①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
③その他の情報共有・情報開示の促進
（２）その他の横断的施策
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

別添：プログレスレポート2021（総合対策2020に掲げた各施策の進捗状況）

冒頭で、**総合対策2021全体に通底する背景・主要な政策課題を記載**することとしてはどうか。

各施策に関する記載については、本タスクフォースでの御議論や昨今のサイバーセキュリティの現状を踏まえ、**対応する課題ごとにまとめながら、施策内容の現行化及び新たな取組を追加**することとしてはどうか。

本日は、**「主要な政策課題」及び本タスクフォースで御議論いただいた施策の方向性について御議論**いただきたい。

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化や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、近年増加しつつある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などについて、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」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必要**ではないか。

■ そのため、**以下の３つの施策を推進していくこととしてはどうか**。

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
③５Ｇの本格的な普及に向けたセキュリティ対策の強化

具体的施策（１）①安全かつ信頼性の高いネットワークの確保

- 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。
- 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や脆弱性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。
- 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が行われる**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**、高まりつつあるサイバー攻撃や脆弱性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はないか**。
- なお、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はないか。

（参考）過去の会合における構成員からの御意見

- ✓ ISPあるいは電気通信事業者が最も大きな情報源を持っており、その情報に期待するということであると、その人たちにインセンティブを与えるような方法が必要。
- ✓ 安全な通信ネットワーク構築に関して、ユーザとして期待したい。

具体的施策（１）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、**端末側の対策として、これまで電気通信事業法**（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。
- 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、サイバー攻撃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**ではないか。
- 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はないか**。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ではないか。
- 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するとともに、**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こととしてはどうか**。

（参考）過去の会合における構成員からの御意見

- ✓ フロー情報分析を行って、本当にC&Cサーバを検知することができるのか、通信業界でもトライアルをさせていただけるのであればありがたい。いきなり通信を遮断するのではなく、C&Cサーバの検知が本当にできるのかということを、通信の秘密との関係や法的な課題や技術的な課題を整理するという所から始めさせていただけるのであれば、非常にありがたい。
- ✓ NICTとしては、電気通信事業者のフロー情報だけではなくて、例えばNICTでの色々な知的基盤が集まっているデータとのコリレーションなどを行うことによって、精度の高いC&Cサーバの検知などへの活用ができると良い。

具体的施策（１）③5Gの本格的な普及に向けたセキュリティ対策の強化

■ 総務省では、**5Gネットワークの安全性と信頼性の確保のため、制度、技術、情報共有、市場、振興及び国際等の様々な観点から政策に取り組んでいる**。

１）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

２）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。昨年度の取組の一部を本TFで報告するとともに、「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

３）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

４）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」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」の国内での具体化にむけて取組中

５）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

６）国際連携：G7やプラハ会議等の多国間・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

■ **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してはどうか**。

➢ 実施中の取組の例：将来のサイバー空間のガバナンスやルール形成に積極的に関与するための標準化等に関する取組の推進

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。

（参考）過去の会合における構成員からの御意見

✓ 日本においてもBeyond 5GやNew IPの話も含めて、国として推進すべきことを国（総務省）が中心になって整理をされて、その方向で進めていくというのが活性化につながる。

✓ Beyond5G、6Gに向けて、新たな研究開発要素も含めて、攻撃やそれに対する防御などを考えていく必要がある。

具体的施策（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）４月20日15時時点で世界全体での感染者数が約1億4,200万人、うち死亡者数が約303万人、同日0時時点で日本での感染者数が約53.7万、うち死亡者数が9,671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。

- **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、昨年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はないか**。

- 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点を推進することとしてはどうか**。

  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

具体的施策（２）①テレワークセキュリティの確保

- **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だけでなく、**感染症の拡大予防や、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**。
- 一方、テレワークの実施に当たっては、インターネットを利用したり、端末の持ち出しや私用端末の利用も想定されたりすること等から、組織内利用のみを想定していた従来のセキュリティ対策に加えて、テレワーク的な視点からもセキュリティ対策を実施する必要。実際に、テレワーク導入企業に対するアンケートでも、**セキュリティ確保が最大の課題**とされている。
- こうした状況を踏まえ、「**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を確実に確保していただく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）**」や**設定解説資料**を策定している。
- この状況を踏まえ、**次のような取組を進めていくこととしてはどうか**。
  - テレワークセキュリティガイドライン及び手引き（チェックリスト）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に広く周知**。
  - 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。
  - 手引き（チェックリスト）や設定解説資料については、**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**。
  - 勤務者（利用者）へ直接にセキュリティ対策の重要性の周知啓発を図っていくことも必要であり、「その他の具体的施策③利用者への普及啓発」の議論も踏まえ対応を実施。

（参考）過去の会合における構成員からの御意見

- ✓ 2～3分のビデオのようなものをガイドラインの付録に付けて共有していただけるとありがたい。
- ✓ 中小企業への普及啓発として、中小企業に関連しているディストリビュータ等を巻き込んでガイドラインを普及できれば有用。
- ✓ 経営層の積極的な関与について、なぜセキュリティガイドラインが必要なのかについて根拠が薄いため、経営層が納得のいく根拠や理由を記述した方がよい。
- ✓ マニュアルを作ることは非常に重要であると思うが、仕様変更が頻繁になる箇所もあるので、マニュアルも追従して更新していくことが重要。
- ✓ WindowsXPや7、8の利用が多いことに対して、今後この手引きまたはガイドラインだけで対応していくのか、それとも別に何かやるのか等、改めて検討が必要。
- ✓ テレワークセキュリティガイドラインについて、他の省庁あるいは業界団体が出している同じようなドキュメント等とリンクするようにしたほうが良い。

具体的施策（２）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。
- **新型コロナウイルス感染拡大**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。
- 総務省は、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、**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、**令和３年４月に「時刻認証業務の認定に関する規程」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、**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、公表する**こととしている。
- **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については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。
- 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、**内閣官房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としてはどうか**。

具体的施策（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化や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で観測した攻撃通信の約半数が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必要**ではないか。
- そのため、**以下の３つの施策を推進していくこととしてはどうか**。
  ①IoT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

具体的施策（３）①IoTのセキュリティ対策

- IoT機器については、**NOTICE注意喚起**として、**サイバー攻撃を受けるおそれのある脆弱なIoT機器を調査して注意喚起**を行う取組みを2019年２月から実施している。（また、NICTER注意喚起として、既にマルウェアに感染しているIoT機器を検知して注意喚起を行う取組みを2019年６月から実施している。）
- NOTICE注意喚起では毎月約2000件（NICTER注意喚起では日々約200件）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減少していない**。この理由としては、(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、等が考えられる。
- 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、**次のような取組を進めていくこととしてはどうか**。
  - 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機器の利用者に対する注意喚起に加えて、IoT機器の**製造事業者**や、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って**いく。
  - **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。
- 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、**ネットワーク側でより機動的な対処を行うための環境整備**も推進することとしてはどうか。

（参考）過去の会合における構成員からの御意見

- ✓ NOTICEの注意喚起について、ハガキで総務省の名前を出す等、メディアへの活用を組み合わせて行うと、より効果がある。
- ✓ NOTICEに、VPNの脆弱性スキャンも加えてはどうか。
- ✓ NOTICEの調査対象の拡大を行い網羅性を高め、対象者を把握し訴求力の高い方法で注意喚起を行うことで、脆弱なIoT機器の撲滅を図ってはどうか。

具体的施策（３）②クラウドサービスの利用の進展を踏まえた対応

- 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一方、**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。
- また、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、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アセスメント等も活用し、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のではないか**。
- 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のではないか**。
- **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としてはどうか**。

（参考）過去の会合における構成員からの御意見

- ✓ 具体的にどういうことに注意して設定をしなくてはいけないか、といったことに深く入り込み、ベストプラクティスとしてまとめると設定のミス軽減が実現できると思う。
- ✓ セキュリティベンダによるアセスメントの利用普及が見込まれると各セキュリティベンダが投資しやすくなるので、そういった情報発信ができると良い。
- ✓ SaaSの利用に関するエンドユーザ向けの普及啓発も必要。
- ✓ クラウドサービス利用者の設定ミスの状況を鑑み、分かりやすい使い方というものに関してユーザとサービス提供者側の両方で色々努力しないとなかなかうまくいかない。提供者と利用者双方への対策検討が必要。

具体的施策（３）③スマートシティのセキュリティ対策

- **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。
- 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や、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 からの意見などを踏まえ、**2021年４月、「スマートシティセキュリティガイドライン（第2.0版）」の案が公表され、パブリックコメントが実施されているところ**である。
- 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、国内外に対してその普及を図ることが適当ではないか**。また、国内外のスマートシティセキュリティ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重要ではないか**。

（参考）過去の会合における構成員からの御意見

- ✓ スマートシティセキュリティガイドラインをどういう形で進めていき、誰のために発信するかというのを、もう少しクリアにした方が良い。
- ✓ スマートシティセキュリティガイドラインについて、参加組織のどの部門にこれを読んで有効に使うようなセキュリティ人材がいれば良いのかというのを考えていく必要がある。
- ✓ スマートシティでは、それぞれの個別ルール自体が不整合であるがゆえの色々なインシデントまがいなことが起こるのではないか。

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対策は、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必要**ではないか。

- そのため、**以下の２つの施策を推進していくこととしてはどうか**。
  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

横断的施策（１）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、**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**。
- **情報通信研究機構**（**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**として、**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。
  - 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。
  - 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。
- このNICTとNICTが有する技術・ノウハウを中核として、我が国のサイバーセキュリティ情報収集・分析とサイバーセキュリティ人材育成の**産学の結節点となる基盤**※（**CYNEX**）を構築中である。（※サイバーセキュリティ統合知的・人材育成基盤）
- **CYNEX**について、得られた情報の効果的な共有方法、安全保障の観点からの情報管理、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、**早期の本格稼働を目標とした基盤構築を引き続き推進**していくべきではないか。また、その**計画・進捗について本ＴＦに適宜報告**をし、**方向性について更に議論を深める**べきではないか。
- また、**利用対象となる産学が利用しやすいものとなるよう**関係者との意見交換を積極的に行うとともに、**積極的なコミュニティ形成を図っていくべき**ではないか。

（参考）過去の会合における構成員からの御意見

- ✓ 人材育成という観点で、ユーザ企業の担当者がNICTの取組にあるようなコミュニティに参加したり、交流できる機会があれば、知識や状況の理解にもつながる。
- ✓ 安全保障の観点から、NICTで別途通常より厳密な情報管理と資格審査の仕組みを作らなければならない。
- ✓ セキュリティベンダにとってインセンティブが明確となるようにしてほしい。
- ✓ セキュリティ産業を成長させるための具体的なスコープを明確にしてほしい。
- ✓ 中堅企業の人材育成の観点から、スキルアップの階層化などができると良い。
- ✓ STARDUSTのセミオープン化について、得られた情報、知見というものを効率的に伝えていく手段を検討するべき。
- ✓ NICTの人材育成施策について、セキュリティ教育のクオリティをどう担保していくかという課題があるので、サーティファイされた教材など、質の保証が今後大事になってくる。

横断的施策（１）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。
- 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・発信していくこととしてはどうか**。
- 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としてはどうか**。

（参考）過去の会合における構成員からの御意見

- ✓ サイバー攻撃の被害者は、単に第三者のセキュリティ対策のためというだけでは、情報共有や公表には踏み切れない。情報共有や公表をした瞬間に、被害者だったはずの者がステークホルダにとっての加害者になったり、社会的な悪者のように捉えられたりすることもある。被害者を取り巻くステークホルダとしてのあるべき振る舞いについて社会的なコンセンサスを得ていく取組につなげてほしい。
- ✓ サイバー攻撃の被害者からの情報共有・情報公開が進むには、情報共有や公表のプロセスの整理に加え、（被害者が社会的な悪者のように捉えられないような）社会的コンセンサスをいかに作るのか重要であり、そのための広報活動にコストを割いてもらいたい。
- ✓ サイバー攻撃の被害者向けに、情報共有や公表に関するなんらかのフォーマットやガイドラインがあってほしいし、それを広く周知してほしい。被害者が更に叩かれるようでは、情報共有や公表のインセンティブはなかなか上がらない。

横断的施策（２）②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、**利用者ひとり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。
- **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としてはどうか**。
- 具体的には、**以下の方向で取り組むこととしてはどうか**。
  - 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。
  - 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。
  - マルウェア感染防止のため、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を継続すること。
  - 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。
- 広く利用者に対して行う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、既存のメディアも含め、利用者に広くリーチ可能な効果的な周知手法を検討することとしてはどうか**。

（参考）過去の会合における構成員からの御意見

- ✓ 専門用語や技術用語を使って書いているので分かりにくいというケースがよく見られるので、やっていただきたい方にサンプル的にでも読んでいただいて、できるかどうかを確認するなどをしていくべき。
- ✓ 周知啓発の媒体として、インスタグラムを利用するなどの工夫をしても良い。
- ✓ SNSなどでリーチできない対象への啓発として、テレビやラジオ、新聞、雑誌等も活用すると良い。
- ✓ 昨今の情勢を鑑みて、スマートフォンアプリに関する意識調査も行うべき。
- ✓ 感染しないことが一番であるが、実際のところ扱っているのは現場の社員であるため、そのあたりに対してもエンドユーザへの啓発が必要。Twitter等のSNSも活用して、エンドユーザ向けに分かるような形で啓発を進めていくのが良い。
- ✓ オンラインによる教育等が進んできているため、オンライン向けのコンテンツの開発や試行錯誤をしていく必要がある。
- ✓ ユーザに対する教育あるいは啓発にも限界があるため、ユーザを信じない形でリソースアクセスの環境を提供するということについては、ゼロトラストあるいはAlways verifyという考え方に対する研究開発をしていくことが良い。

横断的施策（２）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、政府間及び民間組織間での国際連携が不可欠である。これを踏まえ、主に以下の観点から、一層の連携を推進することとしてはどうか。

【二国間・多国間連携】

各国・地域とのICT政策対話やサイバー協議等の場及び政策担当者間での意見交換の機会を通じて、引き続き国際的な信頼醸成を図る。また、NICTが運用するDAEDALUS等、サイバー攻撃等の脅威の低減に資する取組については、引き続き積極的に海外の政府機関等に対して連携を働きかけることとし、サイバー空間全体の安全・安心の向上への寄与を目指す。

【民間組織間の国際連携の促進】

サイバーセキュリティに係る脆弱性や脅威等に関する情報の国際的な共有等を通じたICT分野のISAC間の国際連携を引き続き促進する。特に、米国に加えて、欧州、豪州等における関係情報共有組織とICT-ISACとの連携を後押しする。

【ASEAN諸国等に対する能力構築支援】

アジア地域、特にASEAN諸国に対する能力構築支援は、サイバー空間全体の安全・安心の向上や「自由で開かれたインド太平洋戦略（FOIP）」を踏まえた地政学的観点から重要であることを踏まえ、我が国主導で設立された日ASEANサイバーセキュリティ能力構築センター（AJCCBC）におけるサイバー防御演習をより充実させるうえで、欧米との第三者連携を推進するとともに、国内企業との連携の強化を図る。

【サイバー空間のガバナンスやルール形成に積極的に関与するための標準化等に関する取組の推進】

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。

【サイバーセキュリティ関係企業の海外展開支援】

我が国企業の国際競争力の持続的な向上を図るうえで、官民一体となった情報収集・分析等を通じたビジネス案件の形成力の強化が不可欠であることを踏まえ、サイバーセキュリティ分野における民間企業の海外展開を支援するための市場調査等を実施する。

（参考）過去の会合における構成員からの御意見

- ✓ 人材育成や演習の研修などの基盤を提供したりするというのは、1つの国際連携として重要な取組になると思っているので、ぜひとも進めていただきたい。
- ✓ 日本の民間サイバーセキュリティ企業として、是非、海外企業や政府組織との連携ができるチャンスを広げていただきたい。具体的には、ASEANに対する民間企業の支援の欧米への拡充、AJCCBCにおける技術支援など。
- ✓ JASPERの活用などの海外機関との連携については、NICTだけでなく、関連するステークホルダーで連携していくことが重要。
- ✓ 海外同士の事業者団体と協定を結んで日本のNOTICE方式を輸出するというか、広めていくような方法を考えることも良い。
- ✓ 上級レベルの研究者を作るプログラムとして、国外の大学、研究機関等との、トップレベルでの学術的な、または研究開発的な連携というのも入ると良い。