「IoT・5Gセキュリティ総合対策2020（案）」に対して提出された意見及びその意見に対するサイバーセキュリティタスクフォースの考え方（案）

資料25-1

項番	意見提出者	該当箇所	御意見の詳細	御意見に対する考え方
1	法人F（F5ネットワークスジャパン合同会社）	Ⅰ（1）IoT・5Gセキュリティ総合対策以降の状況変化と改定	(1) 電子署名について 悪意のある第三者の電子署名は排除していくべきだと考えます。 そのため 7ページ目「例えば、電子署名や」を「例えば、正当な認証局による信頼性の高い電子署名や」に変更いただき、その認識を明確にすることを提案いたします。	参考のご意見として承ります。 なお、当該記載は、あくまでサービスの種類として電子署名を示しているものであるため、修正は不要と考えます。
2	法人F（F5ネットワークスジャパン合同会社）	Ⅰ（1）IoT・5Gセキュリティ総合対策以降の状況変化と改定	(2) テレワークセキュリティについて テレワークのセキュリティ対策について利用企業側の視点で言及されていますが、施設側(サテライトオフィスなど共同利用型オフィス運営事業者)のセキュリティ実装の必要性も記載した方が良いと考えます。 例えば、5ページの「（1）テレワークの利用の増加への対応」や34ページの「（9）テレワークシステムのセキュリティ対策」の中に、「サテライトオフィスなど共同利用型オフィス運営事業者においても、施設内で利用される通信機器(Wi-Fiルータなど)やネットワークにつながる機器(複合機やネットワークカメラなど)」の選定や設定・運用について注意が必要である。」という内容の記述を加えることを提案いたします。	御指摘の点については、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、その対応が急務であるという観点から記載をしているものです。施設提供側の観点からの各種取組については、今後の取組の参考とすることが適当と考えます。なお、「（6）無線LANのセキュリティ対策」においては、施設提供側も含めたセキュリティ対策について記載しています。
3	法人J（アドイン）	Ⅰ（2）改定に当たっての主要な政策課題	Entity間及びEnd to Endの信頼性の確保による 安全 安心	御指摘の点については、今後の取組の参考とすることが適当と考えます。
4	法人J（アドイン）	Ⅰ（2）改定に当たっての主要な政策課題	Ⅰ（2）2）クラウドサービスの利用の進展を踏まえた対応 特に9ページセキュリティの確保～リテラシーの向上も重要である セキュリティ評価制度は、すでに世界的にあるモノでグローバルスタンダードが望まれる。 クラウドサービスと一般的にとあるがサービスによって全く違うモノである 本件も Entity間及びEnd to Endの信頼性の確保による 安全 安心	御指摘の点については、今後の取組の参考とすることが適当と考えます。
5	法人J（アドイン）	Ⅰ（2）改定に当たっての主要な政策課題	5G、L5G（日本独自）（他国は周波数共有など技術研究）、6G（バックボーン技術にも新技術が中国優勢） プロビジョニングの時にEntity間もしくはEnd to Endの信頼性を確保することよる 安全 安心	御指摘の点については、今後の取組の参考とすることが適当と考えます。
6	法人J（アドイン）	Ⅰ（2）改定に当たっての主要な政策課題	IoTデバイスに対しては、PKIや署名などを利用することは消費電力とCPUパワー上事実上使い物にならないと考えます。 物理的なハードウェア紛失や盗難また、サイドチャネル攻撃を除けば Entity間もしくはEnd to Endの信頼性を確保することよる 安全 安心	御指摘の点については、今後の取組の参考とすることが適当と考えます。

項番	意見提出者	該当箇所	御意見の詳細	御意見に対する考え方
7	法人K（アマゾンウェブサービスジャパン）	Ⅰ（2）改定に当たっての主要な政策課題	まず最初に、AWSは、総務省が「責任共有モデル」について言及いただいたことに感謝申し上げます。この「責任共有モデル」の概念は、官民双方においてクラウド技術採用を進めるために不可欠の概念といえます。 AWSは、クラウドサービスを利用する顧客の皆様が、サイバーセキュリティに関する知識を強化する必要があることに同意します。AWSといたしましても、顧客の皆様に向けてセキュリティのアウェアネスを高めるためのメッセージングに努めているところです 。 ただ、案文の9ページに記載されております「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」との記載は、いささかミスリーディングなのではないかと思われます。この文章を読んだ読者は、クラウド内のセキュリティ達成が困難なものであるとの感想を抱くかもしれません。実際は、クラウドにおけるセキュリティ確保のためのツールが多数用意されており、責任共有モデルと共に、最高度のセキュリティを確保するよう網羅されています（例えば、ある程度の規模のクラウド事業者を選択した場合、サービスの可用性や耐障害性を高めるために、複数の地域や拠点にサービスを冗長化する機能を利用することができます）。AWSの責任共有モデルの例でいえば、AWSがホストオペレーティングシステムと仮想化レイヤーから、サービスが運用されている施設の物理的なセキュリティに至るまでの要素を運用、管理及び制御することから、顧客の皆様の運用上の負担を軽減するのに役立ちます。そして顧客の皆様にはセキュアなアプリケーション等の設定管理を担っていただきます。またAWSは、顧客の皆様がアプリケーションレベルのセキュリティ策を実現するために役立つセキュリティツールやメカニズム及び暗号化ツールやベストプラクティスを紹介する様々なドキュメントを提供しております。加えて、AWSのパートナーからは、ネットワークセキュリティ、構成管理、アクセスコントロール、データ暗号化といったセキュリティ目的を達成するための数多くのツールや機能が提供されています。責任共有モデルのもとでは、コアビジネスにおけるクラウドサービスの利用にあたり、最も強いセキュリティ確保の要請と、最も要求度の高い顧客の皆様のニーズに応えるための、高度のデータアベイラビリティとセキュリティが用いられています。 よって、AWSとしましては、案文9ページの記述を次のように改訂することを提案します。 「責任共有モデルのもとにおいて、クラウドベンダーとユーザー（顧客）は、それぞれの役割を適切に果たすことで、クラウドに関するセキュリティリスクを最小化するために、共に協力すべきである。ユーザー（顧客）側は、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、クラウドベンダーから供給されるツールや対応策を用いてセキュリティリスクを最小化することに責任を持つべきである。またクラウドサービス提供者側においては、セキュリティに関する啓発活動や研修等を通じて役割を果たしていくべきである。」	頂いた御意見を参考に、責任共有モデルにおける利用者・調達者及びクラウドサービス提供者それぞれの役割が明確となるよう、追記しました。
8	法人L（ドキュサイン・ジャパン）	Ⅰ（2）改定に当たっての主要な政策課題	当事者型の電子署名(リモート署名を含むと考慮)やeシールでの対応をご検討いただくと共に、既に市場で普及している第三者型のクラウド電子署名サービスも1つのオプションとしてご検討頂きたい。第三者型のクラウド電子署名サービスでは、利用する企業を予め識別し、ユーザーがサービスを利用際には認証を要求しており、その認証を経たユーザーが送信(発行)する電子文書は信頼に足るものと言えると考えております。受信者は送信者のドメイン名等をログ情報で確認することもできますので、安全な形で電子文書の運用が可能ではないかと考えております。	2020年（令和2年）7月2日(木)に規制改革推進会議において取りまとめられた「規制改革推進に関する答申」の通り、所謂第三者型のクラウド電子署名サービスについては、総務省、法務省及び経済産業省において、電子署名法上の位置づけの明確化に向けた検討が行われているところであり、できるだけ早期に、その考え方をQ＆A等で明らかにし、広く周知を図ることとしています。
9	法人Q（ラック）	Ⅰ（2）改定に当たっての主要な政策課題	弊社は1995年に情報セキュリティ事業を立ち上げて以来、巧妙化、多様化するサイバー攻撃の最前線に立ってノウハウを蓄積してまいりました。昨今のIoT機器や5G等の通信基盤の発達には目を見張るものがあり、Society 5.0を目指し積極的に導入が推進されています。一方、ライフサイクルが長く、製造者や保守管理者がいなくなる場合もあるため、残留データや廃棄時の扱い等のセキュリティ上の新たな懸念があり、血液の動脈に対して静脈となる機能や役割も重要と感じております。その観点から、同対策の見直しに賛同するとともに、以下の意見を提出いたします。 意見１：p6「テレワークシステムのセキュリティに関するチェックリストの作成や相談窓口の拡充」について 実効的な体制を敷くためには、官や業界団体とともに、民間企業や情報安全確保支援士の活用が重要と考えます。	御指摘の点については、今後の取組の参考とすることが適当と考えます。
10	法人A（パロアルトネットワークス）	Ⅲ（1）IoTのセキュリティ対策	出荷時に問題がなかったとしても、その後ソフトウェアの不具合や脆弱性が発見される可能性は常に存在します。本総合対策案 P.20「Ⅱ 施策展開の枠組み ③時間軸を意識した施策展開」でも述べられているように、時間軸を意識した施策展開は重要です。ユーザがIoT機器の導入から利用終了までのライフサイクルを計画できるにはソフトウェアサポートの提供期間を知ることが必要なため、機器ベンダーによるサポート終了ポリシーの公開を行い、ユーザに周知することが必要と考えます。	御指摘の点については、今後の取組の参考とすることが適当と考えます。

項番	意見提出者	該当箇所	御意見の詳細	御意見に対する考え方
11	法人D（組込みシステム技術協会）	Ⅲ（1）IoTのセキュリティ対策	1.1. IoTのセキュリティ対策 IoTシステムの運用においては、OT-ITの両方の視点が必要と考える。NICTの取り組みとして、「NOTICE」の活動は有用と考える。しかしながら、あくまでも運用されたものに対する活動となり、運用前の設計におけるセキュリティ対策には繋がらないと考える。 セキュリティ対策においては、運用前の設計段階での対策が重要であり、セキュリティ・バイ・デザインを浸透させることが重要であると考える。特にOT側のエンジニアは、IoT活用のためのネットワークスキル経験が不足しており、セキュリティ対するノウハウ集積度も低く意識も低いと考える。OT技術者がIoTを活用していくためには、特に車載系では、クローズだったものが、ネットワーク利用によりコネクティッドとなったりと、今までネットワークを使ってこなかった技術者が多数のため、ネットワークスキルの向上とセキュリティに対する意識向上が必要であり、人材育成として急務であると考える。 OT側機器の脆弱性な部分として、ハードウェアの分解、ソフトウェアの解析に対する対策が重要となるため、OT側の開発段階時にセキュリティガイドラインの確立が急務であると考える。	御指摘の点については、今後の取組の参考とすることが適当と考えます。
12	法人D（組込みシステム技術協会）	Ⅲ（1）IoTのセキュリティ対策	総務省が発表した「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)」は有用である。NICTが活動している「NICTER」による活動も有用である。しかしながら、効力として「任意の認証」ではなく、強制力を持った認証にしなければ、ボット化の検知、対応、復旧が遅れることになりかねず、諸外国とのデータ競争にも負けてしまうと考える。	御指摘の点については、「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)」は強制規格である端末設備等規則の運用について明確化する観点から整理したものです。
13	法人D（組込みシステム技術協会）	Ⅲ（1）IoTのセキュリティ対策	1.6. 国際連携の推進 2016年に発生した「Mirai」では、保守ポートのtelnetを狙ったボット化を防ぐ取組みは重要になってくると考える。「Mirai」の問題では、保守ポートが空いていることが問題と考えられるが、最も重要になるのは、ボット化された事に気が付かなった点が挙げられる。本資料での提言通り、NICTの「NICTER」を活用した取組みは有用であり、今後も継続した活動を続けるべきと考える。	本総合対策の内容に賛同の御意見として承ります。
14	法人D（組込みシステム技術協会）	Ⅲ（1）IoTのセキュリティ対策	1.6.2. ボット化の対策 米国では、IoTデバイスがボット化してしまうことに対する対策として、2018年5月に商務省(DoC)、国土安全保障省(DHS)が報告書をまとめた。報告書に基づき、11月に「対ボットネット強靭化ロードマップ」を公開した。ボットネット撲滅活動を5つの取組みに分類した上で、官民が行うべき個別Workstream(タスク)として整理された。ロードマップの公表に合わせ、CSDE(The Council to Secure the Digital Economy)が表2に示す5つの取組み・タスクを示し、「国際アンチボットネットガイド」として公表し、官民の強いパートナシップを持った取組みを行っている。(参考文献6より引用) 本資料でも述べられている通り、産学官の連携のもと、積極的な活動を行い、ボット化対策を推進していくことが急務であると考える。	御指摘の点については、今後の取組の参考とすることが適当と考えます。
15	法人G（セキュアIoTプラットフォーム協議会）	Ⅲ（1）IoTのセキュリティ対策	【意見1】p22 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について アプリケーションがマイクロサービス化されることについてもセキュリティ対策の検討テーマとするべきである。 マイクロサービス化されることにより、変化に強く柔軟性に優れたアプリケーションが実現できるが、一方で、アプリケーション数は増加することになるため、結果として攻撃ポイントの増加にもつながる。これについては、アプリケーション開発者、DevOpsエンジニアも含めてセキュリティ対策を検討する必要がある。	御指摘の点については、特にクラウドコンピューティングの分野において、今後マイクロサービスの重要性は高まっていくと考えられます。そのため、Ⅲ（3）にあるクラウドサービスのセキュリティ対策に今後取り組んでいくにあたり、留意が必要な点と考えます。

項番	意見提出者	該当箇所	御意見の詳細	御意見に対する考え方
16	法人I（BSA ｜ザ・ソフトウェア・アライアンス）	Ⅲ（1）IoTのセキュリティ対策	IoTのセキュリティ対策を策定する上では、世界で進む同様の取り組みを考慮し、また、可能な限り、連携させることを奨めます。この緊急な課題に各国政府が着目する中、政策の分断のリスクが高まっています。IoTソリューションが本質的に相互連携・依存していることから、政策の分断は問題となります。IoTセキュリティへの政府のアプローチが形成されるにつれ、国内、又、国際的な政策が互いに相容れず、矛盾し、一貫性が無くなると、多国籍なテクノロジー企業は、最善のセキュリティ・ソリューションの提供を阻まれ、苦しむことになります。これはイノベーションや競争を抑制することにもなります。IoTセキュリティに関し相互運用性のあるアプローチをとることは、日本、ひいては、グローバル経済にとって不可欠です。 この点において、国際的に認められた規格を軸に、貴省がIoTのセキュリティ政策を策定することを奨めます。相互運用性を促進することに加え、産業界、政府、学識者間の合意に基づくことにより、継続的なセキュリティ成果を生むことが可能となります。合意に基づいた国際規格を代替することはできなくとも、IoT機器や部品の製造業者を指導する上では、産業界のベスト・プラクティスも参考となるでしょう。また、貴省はIoT機器に着目したセキュリティの検討を拡張し、ネットワークや通信インフラも活用し、IoT機器を保護する対策を考慮すべきです（例：安全な搭載、アクセスの方針、脅威監視、ドメイン・ネーム・サービス層のセキュリティ等）。 BSAは産業界の合意形成に向けた取り組みに関わっており、広く普及しているセキュリティに関するガイダンスを策定しました。例えば、BSAの『Framework for Secure Software』では、IoTソリューションや5Gを強化するソフトェアも含む、ソフトウェアのライフサイクルにおいてセキュリティを評価・促進する上で、エンタープライズ・ソフトウェア会社が実践しているベスト・プラクティスをまとめました。セキュリティへのアプローチを検討する上で、これらの資料を貴省が参照することを奨めます。また、20の主要なサイバーセキュリティとテクノロジー団体をまとめている、C2 Consensus on IoT Security Capabilitiesでは、市場が求めるセキュリティへの期待に応えるためにIoT機器が備えるべき重要な性能について、また、世界的にセキュリティの相互運用性を保つために、IoT機器製造者に向けたガイダンスをまとめています。 そして、対策案において触れているセキュリティ・バイ・デザインへのアプローチに関してですが、長期に亘りセキュリティを確保するには、ソフトウェア、ハードウェア、ファームウェア部品のライフサイクルにおける管理が大事であり、導入後の脆弱性への対応も求められているということを、ここに付け加えておきます。	御指摘の点については、今後の取組の参考とすることが適当と考えます。
17	法人I（BSA ｜ザ・ソフトウェア・アライアンス）	Ⅲ（1）IoTのセキュリティ対策	脆弱性は、研究者コミュニティにおける独立したセキュリティ専門家等により識別され、製品ベンダーに報告されます。このような協調的な脆弱性の公開（coordinated vulnerability disclosure、以下、「CVD」といいます）プログラム について、セキュリティの専門家はガイダンスと規格を策定し、この重要なニーズについて伝えています。このようなプログラムは全て国際的に認知されている ISO/IEC29147 や30111 と連動すべきです。 IoTのライフサイクルにおいて、セキュリティ成果を改善するには、政府は事業者が自主的に以下のようなCVDプロセスを確立するように奨励すべきです：（1）国際規格、特にISO/IEC29147と30111と連動している（2）人工的な軽減適時性等、非生産的な要件を避ける（3）IoTソリューションのライフサイクルにおける脆弱性管理に関する相対的なアプローチを反映している。	御指摘の点に関して、ここでいう「脆弱性等を有するIoT機器」の「脆弱性」は、例えば容易に推測されるパスワード等を設定しているような機器を指すもので、CVD等に類するものではありません。
18	法人Q（ラック）	Ⅲ（1）IoTのセキュリティ対策	意見5：p22「民間団体がセキュリティ要件のガイドラインを策定」について ガイドライン策定に際し、攻撃手法は対象国特有で無いことから、国際的な政策動向を踏まえることが重要と考えます。	御指摘の点については、民間団体がセキュリティ要件のガイドラインを策定する際には、国際的な政策動向だけではなく、国内での製品利用状況や強制規格との関係性等を幅広く勘案した上で検討が行われることが重要と考えます。
19	法人Q（ラック）	Ⅲ（1）IoTのセキュリティ対策	意見6：p24「NOTICE」について： 重要な活動であり、時限延長や法改正を要さない手法を組み合わせ、継続・深化されることが望ましいと考えます。	本総合対策の内容に賛同の御意見として承ります。
20	個人F	Ⅲ（1）IoTのセキュリティ対策	情報セキュリティ対策としては何からどんな情報をいかなるサービス環境下で守るのかという前提が必要です。その意味で、現在および近未来におけるユースケースを提示して技術を議論したほうが生産的ではないでしょうか。そのようなサービスの観点から、ネットワークと端末/サーバのあるべき姿を議論しなければなりませんが、ネットワークに依り過ぎた感があります。端末に関する議論が少ないと思います。IoTで示すもの、その基本ソフトウェアなどを明確に規定してからでないと議論が難しいと感じました。	御指摘の点については、今後の取組の参考とすることが適当と考えます。
21	法人B（ソリトンシステムズ）	Ⅲ（2）5Gのセキュリティ対策	(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・対策を検討することが必要だとする見解に賛成です。そして、これらの人材を育成するプログラムを推進することに賛成です。人材育成の現場で、バッファオーバーフロー、コマンドインジェクション、リモートからのシェルコマンド実行等のハッキングを基礎から学ぶコースはほとんどなく、その提供は喫緊の課題だと思います。	本総合対策の内容に賛同の御意見として承ります。

項番	意見提出者	該当箇所	御意見の詳細	御意見に対する考え方
22	法人C（インテル）	Ⅲ（2）5Gのセキュリティ対策	ソフトウェアとハードウェア両面で脆弱性検証を実施する際、定められた検証方法では技術的中立性が担保されるべきと考える。例えばハードウェアの脆弱性検証にはAIの活用が必要とあるが、技術的中立性を考慮すると、不正に改変された回路の検知や電子機器外部からの不正動作の検知ができれば、如何なる方法でも認められるべきである。加えて検証のプロセスは製造者や通信事業者に秘匿情報の開示が求めないことが担保されるべきである。	御指摘の点を踏まえ、該当施策について取り組むことが重要と考えます。
23	法人D（組込みシステム技術協会）	Ⅲ（2）5Gのセキュリティ対策	1.2. 5Gのセキュリティ対策 5Gの活用にあたって3つの視点でのセキュリティ対策が必要であると考える。また、「低遅延」「高速」「多様性」が謳われており、マルウェア感染拡大時のスピードが、従来のネットワークよりも各段に早くなると思われる。COVID-19の感染拡大にも類似するが、クラスターとならないための隔離方法、感染者の特定などネットワーク側からのアプローチが必要になると考える。特にM2Mでの感染拡大についての対策アプローチが必要になると考える。	御指摘の点を踏まえ、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を進めていくことが重要と考えます。
24	法人D（組込みシステム技術協会）	Ⅲ（2）5Gのセキュリティ対策	1.2.1. サプライチェーン 5Gの活用においては、大量のデータからAI(人工知能)を活用するための機械学習用のデータ収集をするニーズが多くなってくると想定される。活用分野として、運輸、公共サービスや農業など様々な業種に活用されることが予想されている。 例えば、データ収集には、センサーデバイスの活用が必須となってくる。センサーデバイスの調達の際には、セキュリティの観点では、調達先の企業の事業実態、所在地、過去の経歴(不祥事など)の観点で適切な評価が必要となると考える。 5Gを使ったセンサーによる製品やサービスの観点では、「センサーの不正操作を防げるか」「セキュリティ侵害を検知できるか」「不正なデータ流出がされないか」などの評価が必要になってくる。 2016年 米国セキュリティ会社が携帯電話のファームウェアに不正なプログラムがあることを発見したように、調達したものや利用されているものの不正を調査できるようなサプライチェーンルールの確立が必要だと考える。	5Gの本格開始に伴い、そのネットワークのセキュリティ確保の観点からは、サプライチェーンリスクへの対応を念頭に置きつつ、ハードウェア・ソフトウェアの両面において脆弱性の検証手法等を確立することが必要であると考えます。
25	法人D（組込みシステム技術協会）	Ⅲ（2）5Gのセキュリティ対策	1.2.2. データ 5Gの活用により、大量のデータを取得できることになる。大量に集まったデータは、厳しさが増す各種法令に基づくデータプライバシー基準に準拠しなければならない。 企業では、定期的なデータ価値の見直し、データのライフサイクルを管理し、「データをどのような方法で取得するか」「データをどこに保存するか」「司法管轄が異なり、データ保護に関する規定もことなる地域にデータを移動することがあるか」などをルール的に決め、データの収集ポイント、データの転送経路、最終的な保存先、さらに廃棄まで、一貫してデータを保護する必要が出てくる。	御指摘のとおり、関係法令に準拠して5Gを活用することが重要と考えます。
26	法人D（組込みシステム技術協会）	Ⅲ（2）5Gのセキュリティ対策	1.2.3. ネットワーク特性 5Gの「低遅延」「高速」「多様性」という特性を活かすことで、これまで現実的でなかったユースケースが実現可能となる。例えば、5Gの特性を活かす分野として、ヘルスケアが考えられる。高齢者などの生体情報をリアルタイムにモニタリングし、その値が正常レベルから逸脱したら介護者にアラートを知らせるなど仕組みを利用することで、介護にかかるコストを削減し、介護の質を高めるなどが可能となってくる。こういった利用方法では、悪意ある攻撃者が攻撃することで、「低遅延」の特性を妨害する事が考えられる。 「低遅延」を確保するために、定期的な遅延の測定、複数経路の確保、冗長化したネットワークを利用するなど、ネットワークの利用方法を考えることも必要となる。	御指摘の点を踏まえ、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を進めていくことが重要と考えます。
27	法人E（情報処理安全確保支援士会）	Ⅲ（2）5Gのセキュリティ対策	1　背景ー（2）―2 ・セキュリティ対策の実装の促進 「…実際に対策の実施を施すための制度的な措置や産業振興的な措置をとることが必要である。」という点について、制度的な措置をとるにあたり、これまで安定した通信環境を国民に提供することに貢献してきた、無線従事者制度や電気通信主任技術者制度といった国家資格所持者の必置措置を参考とし、情報セキュリティ分野における国家資格所持者である情報処理安全確保支援士の必置についても積極的に検討していただきたいと考えている。よって一般社団法人情報処理安全確保支援士会としては以下の内容に修正することが望ましいと考える。 「…実際に対策の実施を施すために『国家資格所持者の必置化といった』制度的な措置や、産業振興的な措置をとることが必要である。」	御指摘の点については、無線従事者制度や電気通信主任技術者制度といった国家資格所持者の設置のほかに、Ⅲ（2）③にあるように実際の対策を促すため、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など、規制的措置が重要と考えられるため、記載については原案どおりとさせていただきます。

項番	意見提出者	該当箇所	御意見の詳細	御意見に対する考え方
28	法人H（KDDI）	Ⅲ（2）5Gのセキュリティ対策	セキュアなSociety 5.0の実現に向け、安心・安全な国民生活や社会経済活動を支えるため、サイバーセキュリティの確保は官民で取り組むべき課題と考えます。 特に、あらゆる“モノ”がネットワークにつながる社会において、その基盤となる5Gネットワークにおける脆弱性の検証のための手法や体制を確立し、多様なステークホルダー間で情報を共有することは、非常に重要であると考えております。 当社は令和元年度より、総務省が実施する「5Gネットワークにおけるセキュリティ確保に向けたに調査・検討」プロジェクトに参加し、5Gにおけるセキュリティリスク分析や脆弱性の評価、5Gネットワーク構築のためのセキュリティガイドラインの策定等を行ってきました。引き続き、5Gセキュリティ確保のための取組を進めてまいります。 なお、25ページの3～4行目については、次のように修正した方が、文意が明確になると考えます。 「(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。」	本総合対策の内容に賛同の御意見として承ります。 また、御指摘を踏まえ、表現を以下のとおりといたします。 P25 「(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。」
29	法人I（BSA ｜ザ・ソフトウェア・アライアンス）	Ⅲ（2）5Gのセキュリティ対策	対策案では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関して記していますが、サプライヤーは、インフラやサービス改ざんを探知・軽減するために、ベンダー・サプライチェーンを認証するセキュリティ性能開発を強化しています。トラストアンカーやソフトウェア・イメージ・サイニングのような改ざんに防止技術は真正性やハードウェアの完全性を確実にします。対策案に記されているリスクに対応する上でも、これらの対策を取り入れ、産業界と協働することを推奨します。	御指摘の点も踏まえ、5Gの脆弱性の検証手法等の確立に向けた取組を進めていくことが重要と考えます。
30	法人I（BSA ｜ザ・ソフトウェア・アライアンス）	Ⅲ（2）5Gのセキュリティ対策	5Gネットワークの基盤として、革新的でソフトウェアで強化されたツールや技術は、5Gネットワークがどのように作用するか、そして、それをどのように守るかを根本的に作り変えます。 政府はセキュリティの課題に対応するために、ソフトウェアによって可能となるソリューションの導入を促進すべきです。特に、ネットワーク機能を仮想化する技術への投資、サイバーセキュリティを強化するための新たなソフトウェア・イノベーションの活用、そして、5Gの研究開発のセキュリティを優先させることは、5Gネットワークに関連するセキュリティの取り組みを強化することになります。これらは総務省が対策案で認識しているアプローチです。 この点で、我々はオープンスタンダード、又、オープンソース主導のアーキテクチャーを強調することを特に推奨いたします。無線アクセスネットワーク（RAN）技術は、セキュリティ課題に対応するためにソフトウェアを有効活用した一つの重要な事例となります。RAN市場は現在、ごく少数のベンダーが独占しており、そのうちのいくつかにはサプライチェーン上のリスク懸念があがっています。仮想無線アクセス・ネットワーク（V-RAN）やオープン無線アクセス・ネットワーク（O-RAN）によってRANを仮想化することは、競争を広げ、ネットワークのエッジにおけるセキュリティを前進させることになります。	御指摘の点も踏まえつつ、今後の5Gのセキュリティの在り方について検討していくことが重要と考えます。
31	法人I（BSA ｜ザ・ソフトウェア・アライアンス）	Ⅲ（2）5Gのセキュリティ対策	同様にソフトウェアを軸としたSDN（Software－Defined Networking）、ネットワーク・スライシング、NFV（Network Function Virtualization）のような技術はサイバーリスクを軽減する新たな機会をもたらします。政策立案者はガイダンスを策定し、研究開発に投資し、期待できるアプローチを試し、これらの新しい技術を新しいセキュリティ手法に適用することで、疑わしい通信を分離し、機密情報を保護し、ユーザーを認証し、その他のセキュリティ要件に対応すべきです。ゼロ・トラスト・アーキテクチャー（全領域の全アセットの間に明確な認証を設定）を導入するアプローチを採用し、完全性を確実にし（改ざんを継続的に監視し、軽減する信頼性の高い製品を採用）、完全な可視化を実現し（異常な動作や通信の探知を可能にする）、セグメンテーションを実施し（いかなるセキュリティー侵害の影響も最小限におさられるようにアセットのグループを適切に分割）、また効果的な脅威からの保護を採用（機械学習機能による防御的セキュリティ制御と継続的監視を提供）することで、安全な5Gセキュリティ環境を構築でき、運用を開始することができます。	御指摘の点について、5Gのセキュリティの検討にあたっては、SDN、NFVといった新たな技術が今後ネットワークレイヤーに導入されていくことを前提に取組を進めていくことが重要と考えます。

項番	意見提出者	該当箇所	御意見の詳細	御意見に対する考え方
32	法人I（BSA ｜ザ・ソフトウェア・アライアンス）	Ⅲ（2）5Gのセキュリティ対策	様々な分野において5Gの導入が増すにつれ、一貫性のない、重複するガバナンスのリスクが生じます。5Gは以下の分野において不可欠なテクノロジーとなります：通信分野（5Gは超高信頼低遅延通信を提供します）、交通分野（5Gは高度な交通管理を可能とします）、医療分野（5Gが生命にかかわる医療機器や遠隔手術を支えます）、製造分野（5Gが遠隔操作での支援ロボットによりスマートマニュファクチャリングを可能とします）等。 前世代型の通信ネットワークが電気通信サービスに限定して規制することができたのに対し、5Gが依存する中核となるインフラ（例えばクラウドサービス）は多数の機能やクライアントに同時にサービス供給するため、従来の電気通信に限定した規制には適合しません。ガバナンスを成功させるには、分野や省庁をまたがった統一的なアプローチが必要です。そのようなガバナンスの仕組みは、柔軟性があり、5Gネットワーク特有の利用法や脅威に対応し、個別のコンプライアンス要件に合わせたリスクベースのアプローチを構築しなくてはいけません。統一性をもたらすためにも、貴省が他の省庁との連携を促進する効果的な仕組みを構築することを推奨します。	御指摘の点について、5Gのセキュリティの検討にあたっては、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や、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り、これらの点を踏まえ、関係省庁との連携を視野に入れつつ、Ⅲ（2）①にある、5Gの脆弱性の検証手法等確立と体制整備の取組を行うことが重要と考えます。 また、併せて、Ⅲ（2）②にあるとおり、様々なユースケースにおいて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取組が重要と考えます。
33	法人J（アドイン）	Ⅲ（2）5Gのセキュリティ対策	今後L5G研究会においてTAaaS (TrustAccess as a Service)の展開を提案する	御指摘の点については、今後の取組の参考とすることが適当と考えます。
34	法人N（楽天モバイル）	Ⅲ（2）5Gのセキュリティ対策	5Gは様々な分野でのサービス展開が期待されており、単なる通信サービスにとどまらない21世紀の基幹インフラとなるものです。こうした基幹インフラである5Gへの投資促進税制は、通信事業者のみならず、日本のあらゆる産業の利益につながるものであり、「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」の導入に賛同します。 全国5G事業者であるMNO4社間では、利益構造や利用ベンダー、建設予定数など大きく異なります。引き続き、全社の投資意欲が促進されるよう、公平に利用できる制度設計を行っていただきたいと考えます。 また「投資促進」という観点では、手続きや要件については、できるだけ簡便にしていただきたいと考えております。例えば、要件として、機器の安全・信頼性や安定供給性の観点は通信サービスを提供するうえで非常に重要ではありますが、通信事業者が直接証明することは難しく、「通信事業者が説明すべき事項」と「提供ベンダーが説明すべき事項」を適切に区分いただくことを要望します。	ご指摘の点については、安全・安全な5Gの投資を促進するため、「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」及び関係する税法に基づき、5Gの開発供給事業者と導入事業者が満たすべき具体的基準を今後明らかにすることが予定されています。
35	個人F	Ⅲ（2）5Gのセキュリティ対策	5G以降では、エンド・エンドでスライスを作り、種々のサービスを物理端末に提供することができます。この場合、スライス単独では従前の考え方でいいかもしれないが、複数スライスに属した端末におけるセキュリティはかなり様相の異なったものになります。例えば、クラウドで実装している種々のサービスを分け、契約書を取り交わすスライス、金銭の授受を行うスライス、電話・TV会議・チャットを行うスライスなどを構築することができます。各スライスはそれぞれの「セキュリティ・ガイドライン」が適用されるでしょう。その時、各スライスの終端の一つであるスマホのOSやミドルウェアとしてはいかなる機能が要求されるのかを研究面では詰めないといけないと思います。	御指摘の点も踏まえ、5Gの脆弱性の検証手法等の確立に向けた取組を進めていくことが重要と考えます。
36	法人A（パロアルトネットワークス）	Ⅲ（3）クラウドサービスのセキュリティ対策	P.27で「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」とあるように、クラウドの導入、リモートワークの急速な普及、IoTやモバイル端末の増加などにより、現在の組織ネットワークは単純な境界モデルでは防御できなくなってきています。場所にかかわらずすべてのリソースへのアクセスをセキュアにするゼロトラストモデルを早急に推し進めることが必要と考えます。	御指摘の点を踏まえ、クラウドサービスのセキュリティ対策の取組などを促進していくことが重要と考えます。
37	法人D（組込みシステム技術協会）	Ⅲ（3）クラウドサービスのセキュリティ対策	企業においても、通常はイントラシステム利用などオンプレ環境でデータの持ち出しが不可であることで、出社を余技なくされるケースも多々見受けられるため、積極的なクラウドシステムの活用など推進を企業に呼びかけていくことを推進頂けると良いと考える。	御指摘の点について、COVID-19への対応などを受けて今後クラウドサービスのニーズが増加していくことが想定されるため、セキュリティの確保を通じ、クラウドサービスの利用の加速化のための取組を実施することが重要と考えます。

項番	意見提出者	該当箇所	御意見の詳細	御意見に対する考え方
38	法人G（セキュアIoTプラットフォーム協議会）	Ⅲ（3）クラウドサービスのセキュリティ対策	【意見2】p26 （3）クラウドサービスのセキュリティ対策について クラウドサービス事業者が提供するセキュリティサービスだけでなくサードパーティのベンダーが提供するセキュリティ製品やセキュリティサービスも比較検討し、適切なセキュリティ対策を講じるべきである。 また、サイバー攻撃手法は、日々、高度化されているため、国内外の最新の攻撃手法について定期的に調査し、対応範囲、コスト、ユーザビリティ（利用者への影響）等を総合的に検討し対策を決定する必要がある。 なお、複数のクラウドサービスを使用する際には、同一領域のセキュリティサービスでも、 適用できるセキュリティポリシーなど、仕様に差があるため防御できる攻撃が異なるケースがある。 結果として、それがベンダー固有のリスクとなる可能性があることを考慮する必要がある。	御指摘の点については、今後の取組の参考とすることが適当と考えます。
39	法人I（BSA ｜ ザ・ソフトウェア・アライアンス）	Ⅲ（3）クラウドサービスのセキュリティ対策	27P III – (3) クラウドサービスのセキュリティ対策 対策案においては、「政府情報システムのためのセキュリティ評価制度（ISMAP）」の導入により、省庁間のクラウド導入を促進することが記されています。その中には、セキュリティを含むクラウド環境の管理責任がサービスの提供者と利用者・調達者間で分担されるという、共通認識である「責任共有モデル」が明記されています。また、対策案においては、サービスの提供者側だけでなく、利用者・調達者側のリテラシー向上の重要性についても触れています。クラウドサービスがIoTや5Gネットワークにますます不可欠となり、支えるアプリケーションやサービスが増えるにつれ、クラウド環境はより複雑でダイナミックになっていきます。クラウドサービス提供者は組込み型ID管理や脅威監視サービス等、顧客が自身のクラウド環境内で使う様々なセキュリティ・サービスを提供しています。また、IaaS（Infrastructure-as-a-Service）やSaaS（Software-as-a-Service）といった異なるクラウド・モデルによって役割や責任は変わります。 このことからも、クラウドの総合的なセキュリティ対策を策定する際には、このような多様な環境における役割や責任を慎重に区別し、この責任共有モデル下におけるのセキュリティへの意識向上が必要であることを強調しなくてはなりません。	御指摘を踏まえつつ、P27に記載のある通り、「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」が一般的であることを念頭に、利用者・調達者が自らと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」ことを検討することが重要と考えます。
40	法人P（在日米国商工会議所）	Ⅲ（3）クラウドサービスのセキュリティ対策	ACCJは、ISMAPをはじめとする政府の方針がクラウドにおけるセキュリティ確立に資するものと思料します。また「責任共有モデル」のもとでは、クラウドサービス提供者と利用者がそれぞれの管理権限に応じた責任分担を負うことにも同意いたします。ただし9頁に「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」とあるのは、誤解を招く恐れがあると思料します。クラウドと「責任共有モデル」を用いることでグローバルスタンダードに沿った総合的なセキュリティ対策が可能となるのであり、そのことをまずご指摘いただきたいと考えます。同時に、クラウドベンダー側においてユーザーのセキュリティのアウェアネスを高めるための情報提供をすることが望まれる等の建設的な表現をするべきであると考えます。	P11の「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」については、アンケート結果に基づく記載であるため、原案どおりとさせていただきます。 他方、頂いた御意見を参考に、責任共有モデルにおける利用者・調達者及びクラウドサービス提供者それぞれの役割が明確となるよう、追記しました。
41	法人Q（ラック）	Ⅲ（4）スマートシティのセキュリティ対策	意見7： p27 （4）スマートシティのセキュリティ対策 p42　5 スマートシティのセキュリティ対策【再掲】 上記対策は、サイバーセキュリティと想定外事象や事故に対するセーフティの両面が必要です。IoT機器単体のセキュリティ確保には限界があり、多様な関係者間や地域特性に沿った対策の考え方が必要と考えます。また、各国がISO等の国際標準化を進めていく中、我が国も積極的に標準策定に参画すべきと考えます。	御指摘の点については、現在、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・セーフティ分科会等の場において、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、明確化を図る取組が行われており、検討を踏まえつつ、スマートシティを推進する取組との連携を図り、地域やユースケースなどに応じたセキュリティ対策の実装を促進していくことが重要と考えます。併せて、これらの成果については諸外国と連携の上、国際標準化や必要に応じた国際的な議論の場への提案を検討するなど、諸外国との調和を意識して展開を図ることが重要と考えます。
42	法人D（組込みシステム技術協会）	Ⅲ（5）トラストサービスの制度化と普及促進	1.3. クラウドサービスのセキュリティ対策 DX(Digital Transformation)の推進においては、データが非常に重要な要素となり、ビジネスチャンスとなると考えられる。データ活用にあたっては、情報の漏えいや盗聴を未然に防ぐことや、漏えいに気付くことが必要になってくる。 データ活用には、C.I.Aの確保は勿論のこと、eシールやマイナンバーの活用、証明書の利用を促進し、データを扱う人や機器の真正性、データ自体の真正性を確保する認証方式の確立が必要となると考える。 企業においてクラウド利用にあたっては、データに対する漏えいや盗聴などを防ぐための認証や暗号化を利用するためのルールを確立するためのガイドライン化も必要となる。	御指摘の点を踏まえ、クラウドサービスのセキュリティ対策の取組やトラストサービスの制度化などを促進していくことが重要と考えます。

項番	意見提出者	該当箇所	御意見の詳細	御意見に対する考え方
43	法人D（組込みシステム技術協会）	Ⅲ（5）トラストサービスの制度化と普及促進	1.7.3. 人為的ミスの改善 日本国内で発生するセキュリティインシデントを見る限り、「人為的ミスが」多いことが挙げられる。IPA 10大脅威2020(参考文献7)の報告もある通り、Top3はいずれも「人為的ミス」が多いと報告されている。諸外国に比べて、メールなどの誤送信、記憶媒体の紛失などと人為的なミスが多いことが分かる。各企業での取り組みはしているものの、セキュリティ意識が低いために発生するミスとなっており、ネットワーク活用において悪用されない仕組み作りも必要となると考える。特に真正性を確保できる仕組みつくりにおいて、個人が特定できる仕組みや個人しか利用できない仕組み作りなどが必要になると考える。	御指摘の点については、今後の取組の参考とすることが適当と考えます。
44	法人I（BSA ｜ ザ・ソフトウェア・アライアンス）	Ⅲ（5）トラストサービスの制度化と普及促進	貴省がテレワークや時差出勤を促進し、社員が請求書や押印や印刷等の処理のために事務所に通わずに済むよう、文書や業務のデジタル化を進めていることを歓迎します。この点で、タイムスタンプ、リモート署名、eシールを含むトラストサービスを促進し、また、これらのサービスを認証する公的枠組みの検討は大変重要となります。また、電子署名及び認証業務に関する法律が、民間においてクラウドサービスが広く普及していなかった2000年に制定されていることを踏まえ、本法を更新されることを奨めます。日本政府は、関連する基準適合の要件が現代の技術を利用できるようにし、民間企業が文書を認証するのにデジタル署名や電子タイムスタンプを全面的に活用をできるようにすべきです。COVID-19を受けての緊急事態宣言時には、リモート署名やタイムスタンプが認証の公式な法的手段として認められていなかったことから、勤務者が事務所に通わざるをえない事態となりました。 対策案においては、二年以内にトラストサービスに関する認定制度、認定基準、また現行法上の位置づけの検討が進むと記されておりますが、その検討過程においては、民間も積極的に関与させ、本取り組みを加速化させることを奨めます。社会において、これらのサービスが広く普及するには、誰もが、どのような端末からも、簡単にアクセスし、使用できるようにし、又、省庁内においても、本サービスが広く導入されるようにすべきです。また、これらのサービス導入を促進するために、様々な活用事例を政府から提示し、遠隔を軸とした活動の主要基盤となるクラウドサービスの積極的な導入も引き続き促進することを奨励します。	御指摘の点については、現在、総務省において、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、e シールについても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、民間の有識者にも参加頂く形で具体的な認定制度の創設に向けた検討を行っているところです。
45	法人J（アドイン）	Ⅲ（5）トラストサービスの制度化と普及促進	認定制度や認証制度および勇往集権的プラットフォームの展開は世界の潮流から外れている 全てがだめではないがマーケットトレンドとテクノロジートレンドから情勢を判断し枠組みを行わないと世界から取り残されてしまう。	2020年（令和2年）2月に取りまとめられた「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とりまとめ」にも記載のあるとおり、トラストサービスについて、今後の技術進歩やサービス展開の動向、国際的な議論の状況等を踏まえて、その信頼性を確保するための仕組みの在り方について、随時見直しを図ることが重要と考えます。
46	法人L（ドキュサイン・ジャパン）	Ⅲ（5）トラストサービスの制度化と普及促進	左記サービスの認定制度の確立や法制度上での位置づけを明確化頂くことは、是非促進して頂きたいと考えております。 一方、実際に利用されるユーザーの視点で、柔軟なサービス形態の検討を是非お願いします。 例えば、タイムスタンプには存在証明と長期保管といった2つの目的がありますが、各々の利用目的に沿った利用方法の例示で、eシールの対象業務の明示、リモート署名時における本人確認方法の柔軟性(海外ではリモートで本人確認を実施し、その場で電子証明書を発行するサービスもあります)など、実際に利用されるユーザーがメリットをより感じることができるような建付けをお願いいたします。 また、クラウド型サービスでは、独自の方式で既に同等のサービスを提供し普及しているものもございます。市場での認知度を踏まえ、認定された枠組み以外のサービスに関しましても、是非オプションとして継続的に利用できるようご検討頂きたい。	2020年（令和2年）2月に取りまとめられた「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とりまとめ」にも記載のあるとおり、トラストサービスについて、今後の技術進歩やサービス展開の動向、国際的な議論の状況等を踏まえて、その信頼性を確保するための仕組みの在り方について、随時見直しを図ることが重要と考えます。
47	法人N（楽天モバイル）	Ⅲ（5）トラストサービスの制度化と普及促進	紙の書類のデジタル化や業務そのもののデジタル化の更なる促進に強く賛同いたします。トラストサービスを認定するような公的枠組みの構築に加え、「押印仕分け」等で押印が不要なものについては法律上必須ではないという解釈をガイドライン等で明確化する等、普及を加速していただくよう要望いたします。	本総合対策の内容に賛同の御意見として承ります。なお、2020年（令和2年）6月19日（金）に、内閣府、法務省及び経済産業省が「押印についてのQ＆A」を公表しており、当該Q&Aにおいては、商慣行として押印が定着している民間事業者間の商取引等について、民間事業者による押印廃止の取組が進むよう、押印に関する民事基本法上の規定の意味や、押印を廃止した場合の懸念点に応える考え方等が示されています。
48	法人O（セールスフォース・ドットコム）	Ⅲ（5）トラストサービスの制度化と普及促進	現行の電子署名法に基づく電磁的記録の法廷での証拠能力を得るには、特定認証業務事業者の提供するPKIを使用するトラストサービスを使用した電子署名を要するが、eシールの使用範囲として例示されている領収書や請求書等の経理書類等の電磁的記録について法廷での証拠能力を必要とする場合は、従来の特定認証業務を介した電子署名を必要とすると言う理解で正しいか、お伺いしたい。また同時にP.30で言及されているタイムスタンプサービス事業者の認定制度と電子署名法との関係について、是非明確な整理をお願いしたい。 また、最近ではタイムスタンピングのみで法廷での証拠能力があると言及しているサービス等が存在し、若干の法解釈の混乱も見られるため、電子署名法に関し政府による抜本的な見直しおよび周知が必要と考えられる。	電子的な文書については、電子署名法3条に推定効に関する規定があり、本人による一定の電子署名（参考：電子署名法3条「本人による電子署名（これを行うために必要な符号及び物件を適正に管理することにより、本人だけが行うこととなるものに限る）」）が付された場合にのみ、推定効が働くこととされています。なお、タイムスタンプについては個別の法律によらない認定制度、eシールについては民間の認定制度の創設を目指して検討しているところです。

項番	意見提出者	該当箇所	御意見の詳細	御意見に対する考え方
49	法人P（在日米国商工会議所）	Ⅲ（5）トラストサービスの制度化と普及促進	在日米国商工会議所（ACCJ）は電子的な方法による文書の真性担保の必要性があるとの指摘について賛同します。電子署名法は2000年に作られた法律でもあり、リモート型ないしクラウド型の署名押印に対応していません。コロナ危機においては、リモート型署名押印が使えないために出社せざるを得ない人もいたといわれています。今日クラウドサービスが普及してきている事情に照らし、電子署名法改正や公的解釈によってリモート型の署名押印が法律上も真性担保の方式として認知されることを要望します。ACCJが「新型コロナウイルスの影響に対処するための緊急財政対策に関する共同声明」で述べましたとおり、紙ベースの文化から電子的な方法に移行することは、感染症を含めた様々なリスクを防止し、効率性を向上させるものと考えます。加えて、ACCJとしましては、リモート型のサイン等が単に便利さや効率性を向上させるだけでなく、適切に運用されれば偽造などを防ぐためのセキュアな方法でもあることを指摘したく存じます。	本総合対策の内容に賛同の御意見として承ると共に、ご指摘の点については、今後の取組みの参考とすることが適当と考えます。また、リモート型ないしクラウド型の電子署名については、今後電子署名法上の位置づけを明確化することが重要と考えます。
50	法人Q（ラック）	Ⅲ（5）トラストサービスの制度化と普及促進	意見2：p7「トラストサービス」について 真正性証明の推進に賛成するとともに、EUのeIDAS等の国際的な電子取引制度との互換性が確保されることが望ましいと考えます。	本総合対策の内容に賛同の御意見として承ります。
51	個人F	Ⅲ（5）トラストサービスの制度化と普及促進	図2のeシールに関しては、契約書等の授受に関わります。紙の契約書に関しては、従来は収入印紙が必要で、公正証書や会社の定款をつくるときには公証役場の世話になります。この部分を単純の電子化したのでは、年間2兆円近くあった印税が取れなくなります。ただでさえ税収増が難しい現在、単純にeシールを導入したのでは、国益に反します。印紙税をしっかり徴収できるシステムを作らなければならないと思います。そのためのセキュリティはどうあるべきかも考えなければならないでしょう。Everything over IPではなく、専用のスライス上に構築したほうが抜本的な設計ができるでしょう。単純に国外の技術や制度を導入するのではなく、日本の経済システムに合せた改修を経て導入する施策を望みたい。	御指摘の点も踏まえ、トラストサービスの制度化と普及促進について取り組むことが重要と考えます。
52	法人D（組込みシステム技術協会）	Ⅲ（6）無線LANのセキュリティ対策	1.5. 無線LANのセキュリティ対策 総務省での公衆無線LANに関わる調査結果などから、利用者の無線LANに対するセキュリティ意識が低いように見受けられる。 無線LANについては、利用者がセキュリティ意識を持って対応することが求められるので、利用者に対するセキュリティ意識を向上させるための啓発やガイドラインなどを展開し、意識を高めることが必要と考える。	本総合対策の内容に賛同の御意見として承ります。
53	法人D（組込みシステム技術協会）	Ⅲ（6）無線LANのセキュリティ対策	1.5.1. 訪日外国人と日本人の意識の違い 2015年に総務省で行った公衆無線LAN利用に係る調査結果から見て、日本国内の利用者のセキュリティ意識はあることが伺える。 しかしながら、実際に対策を実施している統計を見ると、対策が実施されていない事が分かる。Wi-Fi利用にあたっての脆弱性に対する認知度が高いものの、実際の実施率が低くなっていることが伺える。 実際の対策についても、OSアップデートは一定数対策されているが、公衆無線LAN利用時の基本的な対策の実施率が低いことが伺える。 COVID-19の拡大に伴い、無線LANの利用がリモートワークで活用されている中で、個人で利用する際の無線LANセキュリティ対策は必須となってくると考えられ、利用者に対するセキュリティ意識向上のための啓発が急務となっているため、電波利用の観点などから、積極的なセキュリティ対策の啓発活動をしていくべきと考える。	本総合対策の内容に賛同の御意見として承ります。

項番	意見提出者	該当箇所	御意見の詳細	御意見に対する考え方
54	法人E（情報処理安全確保支援士会）	Ⅲ（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	（指摘事項2） 「…実際の業務やシステム構成に応じた活用しやすいものにしていく必要がある。」「…紙の書類のデジタル化や業務そのもののデジタル化のさらなる促進が必要である」「…トラストサービスの活用を推進することが考えられる。」といった認識については異論はない。しかし、中小企業にリスクを取らせて取り組ませる前に、政府CIOが定めた「デジタル・ガバメント実現のためのグランドデザイン」に記載している「ユーザー体験志向」にもあるとおり、まずは身近な存在であり、総務省が所管している地方自治体でこれらの取り組みを行いその事例（具体的な実現方法や課題、それに対する対応等）を、地域の範として中小企業が参考にできる状況とすることが重要ではないかと考える。 よって、一般社団法人情報処理安全確保支援士会としては本頁の内容に以下を追加することが望ましいと考える。 「加えて、中小企業向け施策と並行して、各地方自治体が中小企業の取り組みの参考となるように、自治行政局を中心として、各地方自治体におけるテレワークの推進、業務のデジタル化、トラストサービスの活用といった取り組みに早急に着手する。また、その際に各自治体に勤務している高度情報処理技術者資格所持者等を臨時の異動や兼務辞令を用いて柔軟に活用することを各自治体に対して要請し、各自治体において専門性を持った人材が迅速にこれらの取り組みを行えるように後押しするとともに、それらの取り組みに対して地方自治体職員が出前講義といった方式で、地域の中小企業が安心できる特定企業や特定製品の営業行為が無い方式で、高い頻度での説明会や相談会を開くといった取り組みの実施についても検討する。」	御指摘の点について、業務のデジタル化やトラストサービスの活用状況やニーズを踏まえつつ、必要な検討を進めていくことが重要であるため、記載については原案どおりとさせていただきます。
55	法人E（情報処理安全確保支援士会）	Ⅲ（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	（指摘事項3） 地方自治法234条の3において法定長期継続契約として定めてられいる「電気通信役務」であるが、いわゆるパブリッククラウドの活用においては、電気通信役務と見做されないため、自治体の負担するセキュリティ装置やサーバといった情報インフラのコストは「最大負荷時」を想定して調達しなければならないという現状がある。一年のうち数度しかない業務（例：住民税の当初賦課業務）のために、膨大な余剰リソースを確保せざるを得ない現状は大きな無駄となっている。 よって、一般社団法人情報処理安全確保支援士会としては指摘事項2に続いて 「また、その際に地方自治法234条の3に定めた法定長期継続契約の「電気通信役務」の範囲を、パブリッククラウドサービスの契約も適用内となるよう法改正の作業に着手するとともに、パブリッククラウドを用いた従量課金型のシステム導入について各自治体に対して積極的に働きかけを行う。そのために、県及び政令市の職員において『政府情報システムのためのセキュリティ評価制度（ISMAP）』監査機関登録規則に定められた業務執行責任者の要件を満たす有資格者の有無を調査し、有資格者については自治体におけるパブリッククラウド推進の責任者として、各自治体における情報システムの調達に関する管理監督職に任用する制度を試験的に開始し、あわせて地方自治体の実態に即したパブリッククラウド活用の方向性を検討するそれら職員の合議体の立ち上げについて検討する。その際、パブリッククラウドの利用とあわせ、情報セキュリティについても十分に考慮する必要がある事から、同様に各自治体における情報処理安全確保支援士の登録実態調査を実施し、より多面的な角度から有効な議論ができるように同合議体への参加を検討するものとする。」 という記述を追加することが適当であると考える。	御指摘の点について、地方公共団体におけるパブリッククラウドの利用については、そのセキュリティの確保の在り方を含め、今後も具体的な検討が必要と考えており、記載については原案どおりとさせていただきます。
56	法人G（セキュアIoTプラットフォーム協議会）	Ⅲ（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	【意見3】p31 （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について マルウェアとC&Cサーバー間の暗号化通信が増加していることから通信ログを取得するにあたり、必要に応じて通信内容を復号しログ取得を行うことを検討する必要がある。	御指摘の点については、今後の取組の参考とすることが適当と考えます。
57	法人I（BSA ｜ ザ・ソフトウェア・アライアンス）	Ⅲ（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	31P III-(7)重要インフラとしての情報通信分野のセキュリティ対策 　また我々は、貴省において「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」（以下、「ガイドライン」といいます）の更新に向けた検討がされていることを歓迎します。業務における利便性をさらに向上させ、政府のクラウド・バイ・デフォルト方針やデジタル手続法を反映し、地方公共団体におけるテレワークを促進させる目的で本検討がなされる時、本ガイドラインにおいては、クラウドサービス事業者（CSP）が、リージョナル又グローバルなインフラを活用してデータを蓄積・処理できるよう、データセンターの場所ではなく、CSPが準拠法に従い、データを安全かつ適切に扱うことに焦点をあてた改正をして頂くことを希望します。また、クラウドサービスを最大限活かし、より良いデジタル・サービスを市民に提供するために、物理的なネットワーク分離に関する記載をガイドラインから削除する、もしくは、分離の範囲を狭めることを推奨します。	御指摘の点について、まずデータセンターの所在については、住民情報等の機密性の高い情報を蓄積する場合は、日本の法令の範囲内で運用できるデータセンターを選択する必要がありますが、オープンデータ、環境計測値等の機密性の低い情報をクラウドサービスに蓄積する場合は、どの国の法令が適用されるのかを確認し、リスク等を考慮した上でデータセンターの所在を選択することがガイドライン上で許容されています。 また、ネットワーク分離については、総務省において本年5月22日に公表した「自治体情報セキュリティ対策の見直しについて」を踏まえ、所要の見直しを行うこと、とされております。

項番	意見提出者	該当箇所	御意見の詳細	御意見に対する考え方
58	法人I（BSA ｜ザ・ソフトウェア・アライアンス）	Ⅲ（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	また、地方公共団体の自主性を認め、各々の要件に合わせて商業的に交渉されたクラウドサービス契約に基づいて、最良のITソリューションと情報セキュリティへのアプローチが実現できるようにすることを強く奨めます。また、これに加え、地方公共団体間で積極的にベスト・プラクティスの共有がされることを奨めます。可動性、サービスの選択性、自主性を可能とする柔軟なガイダンスにより、市民を効率的に支援する上で必要なシステムを、地方公共団体が最適に選択することが可能となります。	御指摘の点については、地方公共団体においてセキュリティが確保された形でクラウドサービスの利用ができるよう、今後も検討を行うことが重要と考えております。
59	法人E（情報処理安全確保支援士会）	Ⅲ（8）地域の情報通信サービスのセキュリティの確保	3 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ー（8） 「地域SECUNITY」を構築することの重要性については賛同する。しかし、実施主体が明確でないことや、特に地方自治体においては、「地域SECUNITY」に関与することが想定されている情報政策部門の管理監督者について任命要件が無く、他参加者である民間事業者等と異なり、必ずしもICTに関する知見がある職員が担当者として配置されていないことや、定期異動により地域コミュニティを醸成するために十分な期間が取れないことなどから、顔の見える関係が構築できないといった課題がある。 現状も、各県警が主体として開催しているサイバー犯罪に対する年1回の情報交換会において、県及び政令市の職員、重要インフラ事業者が会合を行うといった取り組みがなされているが、地方自治体以外の組織からの参加者は高度情報処理技術者であるのに対し、自治体職員はそうではなく、単に同会が実施する「プロモーション・セミナー・演習」へ参加することが目的となっており、コミュニティの成立には程遠い状況である。 よって、「地域SECUNITY」のリーダーシップを取るべき県及び政令市については、情報セキュリティの知見がある職員を同施策の担当者として配置すること、また、配置に際しては一定期間の留任を明記し、地方自治体を中心とした「地域SECUNITY」の構築について、必要な人事施策を行うように、自治行政局が中心となって地方自治体に対して働きかけを行う必要があると考える。同時に、「地域SECUNITY」の長期的かつ持続的な発展を見据え、地域の情報セキュリティ人材が運営の主体となり、地方自治体の専門人材の不足を補うことができるよう、地域在住の情報処理安全確保支援士といった情報セキュリティに関する国家資格所持者又は資格者団体に「地域SECUNITY」活動の一部又は全部を委託することも視野に入れた制度設計についても検討すべきである。 よって、一般社団法人情報処理安全確保支援士会としては（8）の末尾に以下の内容を追加することを提言する。 「更に、これら施策の主体となるべき県及び政令市に対して、情報処理安全確保支援士等の情報セキュリティに関する知見を有する職員を、コミュニティ醸成の業務を行うため、自治行政局が主体となり一定の任命要件、職位及び期間を定め配置する働きかけを行っていくことも同時に実施する必要がある。あわせて、「地域SECUNITY」の自律的かつ継続的な発展を実現するため、情報セキュリティに関する国家資格であり一定の知見が担保されている、地域在住の情報処理安全確保支援士又は情報処理安全確保支援士により構成された団体に対して、業務の全部または一部の委託を行うことについても、制度設計において考慮すべきである。」	御指摘の点については、「地域SECUNITY」の中心となり得る団体（総合通信局、経済産業局、地方自治体、民間団体等）は、地域特性によって様々な場合が考えられ、一律に同一の要件を設定することは適切でないことから、記載については原案どおりとさせていただきます。
60	法人D（組込みシステム技術協会）	Ⅲ（9）テレワークシステムのセキュリティ対策	1.4. テレワークシステムのセキュリティ対策 COVID-19の拡大に伴い、企業におけるテレワーク活用が多くなってきており、情報セキュリティ対策は非常に重要な要素となっている。「テレワークセキュリティガイドライン（第4版）」にもあるが、「ルール」「人」「技術」のバランスが取れた対策の実施が望まれるが、COVID-19拡大に伴って、改めて日本国内におけるIT化の推進が遅れていることが露呈したと考える。 特に経営層のセキュリティに対する考えの甘さやITインフラ設備の遅れなどで、ネットワーク活用におけるルール化がなされていないなど、経営対策としてのセキュリティ対策の遅れが目だったように感じられる。 IT化の推進においては、本資料のeシールなどの活用を積極的に推進し、真正性を担保できる国産の認証基盤の構築やペーパーレス化の推進が必要と考える。 本資料の「データ負けのスパイラル」でも述べられているが、テレワークツールの活用においても、海外製のツールしか使われていないのが現状であり、データ流出は起きている前提での改善施策を検討した方が良いと考える。少なからず、中小企業向けにはどんなツールを利用することが望ましいのかを選定可能なガイドラインなどを作成するなどの活動が望ましいと考える。	本総合対策の内容に賛同の御意見として承ります。

項番	意見提出者	該当箇所	御意見の詳細	御意見に対する考え方
61	法人E（情報処理安全確保支援士会）	Ⅲ（9）テレワークシステムのセキュリティ対策	【総論】 Society5.0の実現に向けた取り組みが進められる中、COVID-19により改めて情報通信に係るリスクや課題といったものが明らかにされた。それらで得られた知見を基に、迅速に総合対策を定めることは非常に有意義な取り組みであると評価する。しかし、具体的な取り組みついて、一般社団法人情報処理安全確保支援士会として、社会全体の情報セキュリティの向上といった観点から、いくつかの提言を行いたい。 1　背景一（2）―1 1）テレワークの利用の増加への対応 （指摘事項1） 「…中小企業等がテレワーク環境下におけるセキュリティ対策を容易に強化できるようにするため、テレワークシステムのセキュリティに関するチェックリストの作成や相談窓口の拡充などの実践的な支援に取り組んでいくことが必要である。」とあるが、既にIPA（独立行政法人情報処理推進機構）が「中小企業の情報セキュリティ対策ガイドライン第3版」を作成しており、その中に情報セキュリティ自社診断といったチェックリストも存在している。また、中小企業を対象に情報処理安全確保支援士による情報セキュリティポリシー作成支援事業も実施された実績があり、改めて総務省が異なる取り組みを行うよりは、IPA（独立行政法人情報処理推進機構）と連携して中小企業を対象とした情報セキュリティ強化の取り組みを推進するほうがより効果的であると思われる。よってこの部分については「…中小企業等がテレワーク環境下におけるセキュリティ対策を容易に強化できるようにするため、『IPA（独立行政法人情報処理推進機構）等の関係機関と連携して』テレワークシステムのセキュリティに関するチェックリストの作成や相談窓口の拡充などの実践的な支援に取り組んでいくことが必要である。」と変更することで、より中小企業にとって便利でありなおかつ、専門的知見を活かした有効な対策が実施できると一般社団法人情報処理安全確保支援士会では考えている。	本総合対策の内容に賛同の御意見として承ります。 テレワークに関する御指摘の点については、作成するチェックリストはテレワークセキュリティガイドラインを補足するものでテレワーク利用の観点に着目したものですが、その内容については国内外の各種ガイドラインの整合を図っていくことが重要と考えます。
62	法人A（パロアルトネットワークス）	Ⅲ（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	「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環境整備をすすめる」という点に賛同致します。有害通信を判別するためには、一定程度の通信内容の分析が必要であり、本文書で提言されている通り「通信の秘密」の解釈に対して早急に整理が必要と考えます。	本総合対策の内容に賛同の御意見として承ります。
63	法人M（テレコムサービス協会）	Ⅲ（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	②サイバー攻撃検知や防御に関して電気通信事業者の果たす役割が大きいことは十分理解しておりC＆Cサーバを検知し、サイバー攻撃の指令通信の遮断等対策を実施できるような環境整備の検討は是非引続き進めて頂きたいところですが、電気通信事業者の多くは経営資源や人的資源に乏しくサイバー攻撃検知や防御に関して十分な対応を取ることが出来ません。助成金の交付や税制優遇による物的支援に合わせ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に認定した第三者機関等による技術・人材支援の検討も必要と考えます。またサイバー攻撃への電気事業者の切断等の対応ですが、電気通信事業者が実施できるようにする法環境の整備については、この報告書に触れられていますが、電気通信事業者が万が一、実施したらサイバー攻撃者から逆に訴えられるといった電気通信事業者が加害者扱いされてしまった場合ことが記載されていません。そういった揉め事を解決する為の行政レベルの調停機能の検討や電気通信事業者・サービス提供事業者に関する攻撃に対する免責の検討なども含め第三者機関等による支援策の検討も要望します。	御指摘の点については、今後の取組の参考とすることが適当と考えます。
64	法人O（セールスフォース・ドットコム）	Ⅲ（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	（P.16 (4)「具体的には、ISP が自ら C&C サーバ 15を検知し、サイバー攻撃の 指令通信遮断等の対策を実施するための方策や、新技術を活用した対策の高度化を促進」 P.36「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、」について） 大変良い試みと考えられるが、現在でも、誤ったレビュテーション情報によって、問題の無いウェブサイト等がブロックされてしまい、サービスが利用できなくなる事象がしばしば発生している。そのため、当該方策の制度的・技術的な観点からの検討には、前述のような一般サイトがC＆Cと見做され誤ったブロックが発生した場合の迅速な解除対応プロセスについても初期から合わせて検討対象としていただきたい。	御指摘の点については、今後の取組の参考とすることが適当と考えます。

項番	意見提出者	該当箇所	御意見の詳細	御意見に対する考え方
65	法人Q（ラック）	Ⅲ（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	意見3： p16「情報通信ネットワークにおいても高度化かつ機動的な対処を実現」 p35 （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 高度かつ機動的であることに加え、従来の受動的なサイバー攻撃対策の延長線上ではない、能動的な対策が必要と考えます。	本総合対策の内容に賛同の御意見として承ります。
66	法人Q（ラック）	Ⅲ（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	意見4：p16「ISPが自らC&Cサーバを検知」について C＆Cサーバの検知には、セキュリティベンダの保有するブラックリストの活用も有用と考えます。また、検知だけでなく、C&Cサーバを遮断する等の対策も重要と考えます。	本総合対策の内容に賛同の御意見として承ると共に、ご指摘の点については、今後の取組みの参考とすることが適当と考えます。
67	法人A（パロアルトネットワークス）	Ⅳ（1）研究開発の推進	日本が「サイバーセキュリティ自給率」が低く、サイバーセキュリティの国産産業育成が喫緊の課題であることは同意致します。一方で欧米諸国とは違う観点や分野でのアプローチも一案ではないかと考えます。 また、各種公的機関が観測した実データを大規模に集積する仕組みについては、そういったデータを送信できる仕組みに対応できる機器のみ(主に国産製品)が選定可能となり、ベンダーロックインにつながることを懸念しております。	本総合対策の内容に賛同の御意見として承ります。 また、御指摘の点については、サイバーセキュリティ統合知的基盤の構築を通した、国際的に通用するエンジニアの育成や国産セキュリティ技術・産業の育成によって、我が国がグローバルレベルの情報共有などの国際的なサイバーセキュリティの向上へ貢献をしていくことが重要と考えますので、その点を本文中において明確化します。
68	法人B（ソリトンシステムズ）	Ⅳ（1）研究開発の推進	我が国のサイバーセキュリティ自給率を高めることに賛成です。「データ負けのスパイラル」は指摘の通りだと同意します。一方で、日本にはセキュリティクリアランス制度が準備されておらず官民連携が深まらないことも理由の一つだと感じます。本施策は、国家安全保障の枠組みと表裏一体の施策と考えます。産官学それぞれの立場を尊重しつつ効率的に取り組めるよう制度も重要です。取組の1）、2）、3）、4）、は速やかに取り組むべき課題ですし、そのような活動に貢献できる機会があれば積極的に関わりたいと希望します。	本総合対策の内容に賛同の御意見として承ります。
69	法人C（インテル）	Ⅳ（1）研究開発の推進	サイバーセキュリティに関する国内の人材と国産事業の育成のために、関連する実データを共有・共用できるオープン・プラットフォームを構築する事はデータの秘匿性を確保するという条件を満たす限り適切な対策と考える。しかしながらData Free Flow with Trust (DFFT)の政策に基づけば、本プラットフォームは国内事業者だけでなく海外事業者にもオープンにされるべきであり、グローバルな環境にすることで最も効果的に活用されるものと考える。	本総合対策の内容に賛同の御意見として承ります。
70	法人C（インテル）	Ⅳ（1）研究開発の推進	IoTの普及により、機能レベルに集中していたセキュリティに関わる概念を大きく広げる必要がある。製品またはシステムの期待される機能を継続させるために、製品のライフサイクルに基づくサプライチェーンを含むフェーズ（開発・製造・輸送・設置・運用・アップデート・リサイクル・廃棄など）に応じた脅威と主たる責任主体を明確にしたセキュリティ対策が重要と考える。施策ごとに対象フェーズを定義することで責任主体と対策を明確にできる。	本総合対策の内容に賛同の御意見として承ります。
71	法人C（インテル）	Ⅳ（1）研究開発の推進	商用化には未だ数年かかるとは言われているが、ポスト量子コンピューティングを見据え、現在使用中の公開鍵暗号の安全性に関する検討を進めることは重要と考える。一方、量子コンピュータは通信傍受やハッカーから個人情報を保護する上に大きな役割を果たすといわれている。よって、量子コンピューティングから現在の暗号を保護する観点とともに量子コンピュータによる新たな暗号を導入するという両者の観点で検討が進められることを期待する。	本総合対策の内容に賛同の御意見として承ります。 なお、量子暗号についてはⅣ－（1）－⑥に、耐量子計算機暗号についてはⅣ－（1）－⑦にそれぞれ記載をしています。
72	法人D（組込みシステム技術協会）	Ⅳ（1）研究開発の推進	また、OT側の開発においては、特に外部調達するハードウェアやソフトウェアなど調達基準やサプライチェーンの確立やルールが必須であり、経済産業省が推進しているCPSF(Cyber Security Phisical Framework)の活用と本活動の連携が必須になると考える。	御指摘の点について、関係府省庁等と連携して取り組むことが重要と考えます。
73	法人D（組込みシステム技術協会）	Ⅳ（1）研究開発の推進	1.8. AIの積極的な活用 本資料にも述べられている通り、セキュリティ対策においては、機械学習などAIの活用は有用であると考える。AI自体もセキュリティや安全面での課題も多くある。攻撃者にとっては、AIであっても解析できるだけのスキルを持っていると想定され、AI自体のセキュリティに対する取組みも急務であると考える。	ご指摘の点も踏まえ、研究開発を進めるに際しては、AIの専門家も取り込むかたちで、取組を進めていくことが重要と考えます。
74	法人G（セキュアIoTプラットフォーム協議会）	Ⅳ（1）研究開発の推進	【意見4】p38 1）実データを大規模に集約・蓄積する仕組みについて 実データの蓄積後、“データの理解”と“データの準備”が必要となる。 トラフィックデータやログデータなどは、非構造化データまたは半構造化データであるため、並べられたデータからその意味を理解し、分析に必要なデータのみを抽出し、外れ値や欠損値への対処、数値データのスケーリング処理や名寄せなど、必要に応じて、加工変換処理を実施する必要がある。	御指摘の点を踏まえ、該当施策について取り組むことが重要と考えます。

項番	意見提出者	該当箇所	御意見の詳細	御意見に対する考え方
75	法人G（セキュアIoTプラットフォーム協議会）	Ⅳ（1）研究開発の推進	【意見5】p38 2）実データを定常的・組織的に分析する仕組みについて セキュリティの知見をもつデータサイエンティストの育成が必要である。	御指摘の点を踏まえ、該当施策について取り組むことが重要と考えます。
76	法人G（セキュアIoTプラットフォーム協議会）	Ⅳ（1）研究開発の推進	【意見6】p38 3）実データで国産製品を運用・検証する仕組みについて サイバーセキュリティの防御性能について、海外製品とのベンチマークを実施するべきである。特に分析結果の比較においては、精度、正確さだけでなく、偽陽性率、偽陰性率の差の明確化と発生理由を調査考察することが重要である。	御指摘の点を踏まえ、該当施策について取り組むことが重要と考えます。
77	法人K（アマゾンウェブサービスジャパン）	Ⅳ（1）研究開発の推進	AWSは、日本がセキュリティに関する情報共有のために国境を越えたデータ流通を促進するためのリーダーシップを発揮することについて支持いたします。またAWSは、サイバーセキュリティとデータ保護の分野において、日本がリードすることを期待します。データフリーフローウィズトラスト（DFFT）の概念のもと、日本政府がサイバーセキュリティに関する情報を共有し、国際的に連携を図ることについて、AWSはサポートさせていただきたいと考えます。この国際連携の観点からは、AWSとしましては、総務省に対し、案文が「サイバーセキュリティ自給率」に言及していることについて再考をお願いしたいところです。焦点を当てるべきは、グローバル基準に則ったセキュリティの実現にあり、日本の産業界は国際的なセキュリティのコミュニティにおいて力を発揮することができるはずです。日本産のセキュリティ製品やサービスにこだわるよりも、総務省はグローバルレベルの情報共有や国際的に通用するエンジニアの育成に力を入れるべきです。日本産のセキュリティ製品やサービスにこだわることは、日本固有のセキュリティモデルにつながりかねず、国際社会でリーダーシップを発揮しようとする日本政府の目的に反し、国益にとってもマイナスになりかねないと危惧します。	御指摘の点については、サイバーセキュリティ統合知的基盤の構築を通した、国際的に通用するエンジニアの育成や国産セキュリティ技術・産業の育成によって、我が国がグローバルレベルの情報共有などの国際的なサイバーセキュリティの向上へ貢献をしていくことが重要と考えますので、その点を本文中において明確化します。
78	法人N（楽天モバイル）	Ⅳ（1）研究開発の推進	弊社はルーラルエリアや山岳地帯等のカバーと災害時の非常用通信手段を実現するために小型衛星を用いた通信技術を適用したフレキシブルなサービスを考えております。陸上、海上、空域等あらゆる場所の多地点から、大容量かつ低コストで、通信の信頼性（可用性）が要求される様々なデータの流通を目指していることから、衛星通信におけるセキュリティ技術の研究開発の取り組みに賛同します。	本総合対策の内容に賛同の御意見として承ります。
79	法人P（在日米国商工会議所）	Ⅳ（1）研究開発の推進	現在の案文は、日本製のセキュリティ製品が少ないことへの懸念が示されています。しかし、製品がどこで作られたかというよりも、グローバルに通用するセキュリティ知識や技術を養成することに重きが置かれるべきです。また日本はそうした人材を育成できるだけの可能性があり、人材育成環境を整えることを優先課題とすべきです。これには、例えば米国とシンガポールの間で結成された合同サイバーセキュリティワーキングループの下で検討されているCyber Technical Assistance Program(CTAP)のような、民間と連携した取組みが考えられます。そのために総務省がセキュリティに関するグローバルな情報共有の仕組みを実現することにリーダーシップを発揮することに期待します。「国産」にこだわることで、セキュリティのフレームワーク等がガラパゴス化する恐れを危惧します。そもそもセキュリティ上の脅威はグローバルなものであり、製品がつくられた場所について重視することは実務的でもないと考えます。	御指摘の点については、サイバーセキュリティ統合知的基盤の構築を通した、国際的に通用するエンジニアの育成や国産セキュリティ技術・産業の育成によって、我が国がグローバルレベルの情報共有などの国際的なセキュリティへ貢献をしていくことが重要と考えますので、その点を本文中において明確化します。
80	法人D（組込みシステム技術協会）	Ⅳ（2）人材育成・普及啓発の推進	1.7. 人材育成・普及啓発の推進 本資料にある通り、日本ではセキュリティ対応ができる人材は不足している。本資料でも述べられている通り、日本のセキュリティ技術者は不足していると考える。ただ、充足していると回答したものでは、諸外国に比べてセキュリティに対する意識が低いのが目立っていると考える。	本総合対策の内容に賛同の御意見として承ります。

項番	意見提出者	該当箇所	御意見の詳細	御意見に対する考え方
81	法人D（組込みシステム技術協会）	Ⅳ（2）人材育成・普及啓発の推進	1.7.2. セキュリティ技術者の育成 本資料で述べられている通り、実践的サイバー防御演習(CYDER)などの活用を積極的に行ってCEH(Certified Ethical Hacker)を育成していく事は非常に重要なことである。ただし、現状の国内の動向を見る限り、適切なポジションやキャリアパスがないのが現状である。時間や予算についてもセキュリティ技術者のポジションを明確にし、必要となるスキル要件の定義を行った上で積極的な育成をしていくことが必要であると考える。 一方、セキュリティ人材の育成を行っているが、実際に対策をしているが、実際の業務に必要なスキルを整理せずに教育を実施していると回答しているものもある。闇雲に教育をしたところで、正しいスキルを身に付く分けではないため、実践のために必要となるスキル標準定義を行い、必要となるスキル体系化と教育カリキュラムの展開が必要と考える。 2017年に起きた「Wi-Fi WPA2の問題」は、SNS上に広がった。SNSで拡散されたことで、センセーショナルな報道となったが、誰しもが使うWi-Fiだっただけに初報が大きく取り上げられすぎたことも挙げられる。実際にIPAから報告あった内容を見る限りでは、盗聴範囲が限られていており、適切な対策をすることで対策できる内容であったことも伺える。SNS上で拡散される情報を正しく見極め、正しい対策ができる技術者の育成も必要となると考える。	本総合対策の内容に賛同の御意見として承ります。 また、人材育成に関するご指摘の点については、関係省庁とも連携した上で今後の取組の参考とすることが適当と考えます。
82	法人E（情報処理安全確保支援士会）	Ⅳ（2）人材育成・普及啓発の推進	4　横断的施策ー（2）－5 「…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…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。」とあるが、セキュリティファシリテーターに求められる技術的知識及び能力が明確となっておらず、情報セキュリティ人材の確保が緊急に求められる現状認識から考えると、セキュリティファシリテーターの能力要件が明確となっていない状態から人材育成方法を検討するのではなく、現在IPA（独立行政法人情報処理推進機構）が所管している「情報処理安全確保支援士制度、情報セキュリティマネジメント試験、情報セキュリティプレゼンター制度」といった情報セキュリティ人材に関する既存の制度と連携していくことで、二重投資の無駄なくかつ迅速な人材確保が実現できる。セキュリティファシリテーターについて総務省が改めて要件を定めることは「Ⅱ－4　政策バリューチェーンの構築」で言及されている「関係府省庁の実施する個別施策との有機的な連携を図り、横断的で一貫性のある施策展開を図る必要がある。」との内容とも矛盾しており、同時に「経産省所管のセキュリティ人材施策」「総務省所管のセキュリティ人材施策」が乱立することは、利用者である国民の目から見ても混乱をもたらす可能性のみが高まり、情報セキュリティの実現に対して、有用性よりも弊害の方が大きいのではないかと懸念される。 よって一般社団法人情報処理安全確保支援士会としては以下の内容に修正することが望ましいと考える。 「…人材が必要となることから『IPA（独立行政法人情報処理推進機構）で実施されている情報セキュリティ人材の育成施策等他省庁や他政府機関と連携しながら』総務省においてこうした人材の育成『及び確保』を支援する方法について検討するとともに、既に各地方自治体において情報処理安全確保支援士登録をしている職員を迅速に調査し、そういった「地域に既にあるリソースを活用すること」についても早急に対応していく必要がある。」 また、一般社団法人情報処理安全確保支援士会としても、国内で唯一の情報セキュリティに関する国家資格に基づく士業団体として、地方におけるセミナー活動等も企画しており、これら地域の課題について、それぞれの地域特性にあわせて積極的に貢献していきたいと考えている。	御指摘の点については、既存の取組を含め、関係府省庁や独立行政法人等と密接に連携して取り組むことが適当と考えます。
83	法人M（テレコムサービス協会）	Ⅳ（2）人材育成・普及啓発の推進	IoT・5Gセキュリティ総合対策2020は、今後さらに増えていくサイバーセキュリティ攻撃に際し、備えを講じるものであり、基本的に賛同します。 また総務省様の調べで、日本では諸外国と比べ、セキュリティ対策に従事する人材が約88%不足となっており、足らない人材については、電気通信事業者へ期待する面は大きいと思えます。しかしながら、セキュリティ面の人材育成やそもそもセキュリティ対策人材確保が高額で高止まりとなっており、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だけでは、どうしても、インセンティブが弱いと言わざる得ません。 以上から、以下の3点について、提案、意見をさせて頂きます。 ①セキュリティ人材確保・育成のための助成金の交付 ・税制優遇とは関係無く、システム費用の補填でもなく、1人あたりのセキュリティ人材の育成や委託に関し、一定の助成金を与えるというもの。 ・電気通信事業者以外にも、その人材を確保・委託する企業にも、支出される。 ・セキュリティ対策人材の増加が見込まれ、安価に提供・確保出来るようになる。	御指摘の点について、実務者層の育成の観点からは、実践的サイバー防御演習（CYDER）がこれまで実施されてきております。その上で、本総合対策にも盛り込まれているとおり、戦略を立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や、環境構築技術者・開発者層など幅広い層の育成に関しては、オープン型人材育成プラットフォームを活用し、民間による体系化された人材育成の取組を積極的促進することが重要と考えます。

項番	意見提出者	該当箇所	御意見の詳細	御意見に対する考え方
84	法人A（パロアルトネットワークス）	Ⅳ（3）国際連携の推進	ICT-ISACの連携をはじめとする、各業界分野のISAC間での連携による脅威情報等の国際的な共有は非常に重要であり必要不可欠と考えます。 ISAC間での連携が進みつつある一方で、国内セキュリティ事業者と海外セキュリティ事業者間での脅威情報共有や連携においても更なる連携が必要と考えます。 一例として、米国のNPO法人でCyber Threat Alliance (CTA)と呼ばれるセキュリティベンダー間で未知の脅威情報を共有し、セキュリティ業界全体として早期の攻撃対策を推進する組織がございます。本書17ページ目、図9、世界セキュリティアプライアンス製品市場ベンダー別シェアに記載の上位4社が加盟する組織で、業界内においては競合する会社同士で脅威情報を共有しております。 日本からも昨年数社が加盟されましたが、こういった国際的なアライアンスへ国内セキュリティ事業者が多く参加し、国内外の脅威情報を収集、共有していくことで、データ負けのスパイラルから抜け日本のサイバー攻撃への対処能力向上に役立つと考えます。 日本のセキュリティ事業者への、こうした組織へ加盟するインセンティブや、推進も必要と考えます。	御指摘の点も踏まえつつ、ISAC連携をはじめとする民間事業者間の情報連携について促進していくことが適当と考えます。
85	法人C（インテル）	Ⅳ（3）国際連携の推進	サイバーセキュリティ対策はグローバルな課題であるため、ISO/IEC JTC-1などの国際標準化活動への参画および国際標準の関連規則への適用を推進していくことが重要と考える。国際標準化活動への積極的な貢献は、国内での取組みを国際標準に反映させることができるだけでなく、国内の人材や国産事業の育成にもつながる。さらには国際標準化動向を常時把握する上でも重要である。国際標準化活動に参画することにより、どの標準を国内の規則に用いるべきか、国際的なハーモナイゼーションを図りつつ国内の関連規則を策定するために準拠すべき最新の国際標準は何かを理解することができると考える。 また、国際連携の推進に関しては、安全なサイバー・フィジカルシステムを世界に構築することを目指し、今後も日本政府がDFFT政策のもと国際的な議論をリードすることを期待する。	本総合対策の内容に賛同の御意見として承ります。
86	法人D（組込みシステム技術協会）	Ⅳ（3）国際連携の推進	国際情勢として、米国、欧州など主要国でのサイバーセキュリティに対する法案、ガイドラインが策定、施行されている状況であり、日本としても国際的な連携や活動が必要になっていると考えられ、各国の動向に合わせた取組みが必要である。	御指摘の点も踏まえつつ、国際連携の推進を図ることが重要と考えます。
87	法人D（組込みシステム技術協会）	Ⅳ（3）国際連携の推進	1.6.1. 日本の現状 NRI Secure Insight 2019によると、国内で参考としているセキュリティガイドラインの多くが、ISO27000シリーズになっている。特筆すべきは、フレームワーク・ガイドラインを利用していないのが3割あることである。米国のNISTや欧州のENISAなどの動向を踏まえると、国際情勢に合わせたフレームワーク・ガイドライン利用をしていくことが急務であると考える。諸外国の動向として、業界特有の規制などが数多く存在しており、GDPRを始めとしたデータの取り扱い方など海外でのビジネスを展開するにあたっては、IEC62443などの国際規格の対応などを推進していくことが必要と考えられる。	御指摘の点については、今後の取組の参考とすることが適当と考えます。
88	法人I（BSA ｜ ザ・ソフトウェア・アライアンス）	Ⅳ（3）国際連携の推進	サイバーセキュリティの脅威は性質上、グローバルであり、国境によって隔てられているわけではありません。効果的な分析と調査のためには、サイバー攻撃に有効な脅威情報が広く可視化されていなくてはなりません。可視化は様々な情報源から可能となります。対策案に記載されている、オプンソースな情報（OSINT）（IV(1)①）やISAC（III(1)③、IV（3）②）のような特定分野ごとの情報共有や分析センターのような選択肢に加え、顧客のインストール先、発表されている脆弱性、脅威を共有するネットワーク等から得ることも可能です。意義ある分析のために脅威情報を集めることは、脅威の調査が実施される場所には関係しません。日本国内のベンダーは海外の事業者同様、日本の情報源だけでなく、世界中の情報源から脅威情報を得て、研究することができます。国内と海外ベンダー間の脅威情報共有の取り決めは、有効な脅威データを集め、国内の能力開発を可能とし、対策案に記されている「データ負けのスパイラル」を防ぐことができます。BSA会員企業の多くはそのような情報共有の取り決めを促進しています。貴省が情報共有を強化し、エンジニアをグローバルな規模で育成することを奨めます。日本特有のサイバーセキュリティ・モデルが世界と相容れなくなることは、日本が国際的にサイバーセキュリティをリードすることを妨げることになります。	御意見頂いた「貴省が情報共有を強化し、エンジニアをグローバルな規模で育成することを奨めます。」について、本総合対策の内容に賛同の御意見として承ります。
89	法人P（在日米国商工会議所）	Ⅳ（3）国際連携の推進	ACCJは総務省が国際連携の推進に向けてセキュリティへの取組みを強化することを支持します。また情報共有促進のためには国際的なデータ流通が不可欠であることにも同意します。日本政府が掲げるDFFTの精神は、国際的なセキュリティコミュニティにおける情報共有において重要な役割を果たすものと期待します。	本総合対策の内容に賛同の御意見として承ります。

項番	意見提出者	該当箇所	御意見の詳細	御意見に対する考え方
90	法人A（パロアルトネットワークス）	Ⅳ（4）情報共有・情報開示の促進	国内サイバー攻撃関連情報が収集できないことが日本のサイバーセキュリティにおける大きな課題であることに同意致します。 日本におけるサイバー攻撃関連情報が少ない大きな要因は、海外のセキュリティ製品が多いこと以上に、国内外問わず自組織から脅威及び脅威分析に不可欠なデータを含め自組織外にデータを共有しない考え方と、国内でのサイバー攻撃関連情報の公表、共有の仕組み等が課題と考えます。 ガイドラインの整備が進みつつあるクラウドの利活用の更なる推進と併せ、脅威に関するデータやサイバー攻撃情報の公表、共有の仕組みと報告におけるインセンティブ等の整備も併せて取り組むべきと考えます。	本総合対策の内容に賛同の御意見として承ります。
91	法人D（組込みシステム技術協会）	Ⅳ（4）情報共有・情報開示の促進	1.7.1. 経営層の育成・普及啓発 セキュリティ対策にあたっては、諸外国のようにトップダウンでの対策が取れていないと考える。日本の場合、自社/他者でのセキュリティインシデントや内部監査などでの指摘による他者からの指摘が発端となっている。自発的な取組みとなっておらず、経営課題としてのセキュリティ対策の意識が低いの現状である。国内においては、セキュリティ対策が後ろ向きなイメージとなっており、積極的な対応を行っているとはいえない状況である。また、諸外国の動向を踏まえると、セキュリティ対策がされていない機器の受け入れが難しくなってくると予想されるため、経営課題としてのセキュリティ対策の意識向上のための育成や啓発活動が急務であると考える。	本総合対策の内容に賛同の御意見として承ります。
92	法人G（セキュアIoTプラットフォーム協議会）	Ⅳ（4）情報共有・情報開示の促進	【意見7】p50 （4）情報共有・情報開示の促進について 国内外の各種機関との情報共有・情報開示にあたっては、APIを使用し、セキュアにオンラインで完結する仕組みを構築するべきである。	御指摘の点については、今後の取組の参考とすることが適当と考えます。
93	法人A（パロアルトネットワークス）	—	サイバーセキュリティ人材育成を含め日本のサイバー攻撃への自律的な対処能力を高める為の取組みに賛同致します。 日本でのセキュリティ製品そのものの開発に主眼をおくのではなく、現在セキュリティ事業者間で主流である海外のセキュリティ製品も有効に活用しながら、本書38ページ目①サイバーセキュリティ統合知的基盤の構築に記載の仕組みを通して国内脅威情報の収集、共有と人材育成に主眼をおくことで、日本独自の演習環境や演習教材の整備、開発を含めた日本の自律的なサイバー攻撃への能力向上を計るのが実現性高く効率が良いと考えます。	本総合対策の内容に賛同の御意見として承ります。
94	法人D（組込みシステム技術協会）	—	総括として、NICT(国立研究開発法人情報通信研究機構)の取り組みや総務省「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)」を軸にした、IT側観点の提言となっており、IoTにおけるOT側の視点を入れたIoT全体のシステムでの対策方法が取れるように取組みを継続頂ければと考える。ボット化対策や人材育成の部分についても、NICTの取り組みを軸にした積極的な活動を継続頂ければ考える。	御指摘の点については、今後の取組の参考とすることが適当と考えます。

項番	意見提出者	該当箇所	御意見の詳細	御意見に対する考え方
95	法人I（BSA ｜ザ・ソフトウェア・アライアンス）	―	はじめに BSAは国際市場において、世界のソフトウェア産業を代表する主唱者です。BSAの会員はソフトウェアが実現するイノベーションの第一線で活躍する企業で構成されており、5Gネットワーク・インフラやサービスを基盤とする、クラウド・コンピューティング、IoT（Internet of Things）、人工知能（AI）やその他の製品やサービスを通じて、世界の経済成長を加速化しています。データ駆動型の製品やサービスのグローバル・リーダーとして、また、サイバーセキュリティを促進する立場として、BSAは『Cybersecurity Agenda』を策定し、世界中の政府に向けて、サイバーセキュリティ上の優先政策課題の解決にソフトウェアを活用すること、強靭な官民連携や広範囲な国際協力を通して、相互運用性を保ちながら、サイバーセキュリティ強化への取り組みを拡大することを提言しました。BSAは特に、以下の点における官民連携を強く支持します。 ・業界標準を活用し、重要なセキュリティ情報を把握するための新たなツールを開発し、セキュリティに関する研究と脆弱性開示を強化することで、安全なソフトウェアのエコステムを促進する。 ・相互運用性があり、リスクベースのサプライチェーン・セキュリティ政策を支持し、5Gとソフトウェアのサプライチェーンを強化し、政府調達においてサイバーセキュリティを優先し、サプライチェーンの安全性を強化するための連携的な取り組みを促進する。 ・国際規格の策定を支持し、セキュリティに関する国際法を連動させ、グローバルな規範に関する取り決めを促進することで、サイバーセキュリティ活動に関する国際的な合意形成を進める。 ・STEM（科学・技術・工学・数学）教育を受けられる機会を増やし、サイバーセキュリティ分野のキャリア形成に向けた新たな道を開き、テクノロジー技能を持つ働き手を強化することで、21世紀型のサイバーセキュリティ労働力開発をする。 ・デジタル・トランスフォメーションを受け入れ、革新的なクラウド・セキュリティ・ソリューションを促進し、最先端技術の可能性を活用し、新たに出現するリスクに対抗するためのイノベーティヴな連携を育むことで、サイバーセキュリティを前進させる。 上記の優先事項は、本対策案と一致しております。貴省が、労働力と人材開発、研究開発、官民連携、国際協力、国際規格、またセキュリティ・バイ・デザインの重要性を認識していることを我々は高く評価しています。	本総合対策の内容に賛同の御意見として承ります。
96	法人I（BSA ｜ザ・ソフトウェア・アライアンス）	―	また、この機会に、日本政府が今回の世界的パンデミックにおいて、懸命に対応されていることに感謝を述べさせて頂きます。BSA会員企業は世界中の政府を支援するために、救済と援助のための様々な取り組み を始めています。エンタープライズ向けのソフトウェア企業は、教育者や事業者に向けてアドバイスや無償のリソースを提供し、緊急な医療研究のためのスーパーコンピューティングやアナリィテクス・ツールを運用し、緊急資金を寄付するなど、この難題に共に立ち向かうために連携をとっております。 この取り組みの一環として、BSAは『対応と回復に向けたアジェンダ』（以下、「アジェンダ」といいます）を策定し、強靭で包括的なリモート・エコノミー（遠隔環境での経済活動）の構築のための提言をしました。アジェンダでは、強固なサイバーセキュリティの実践、強靭なインシデント対応力の支援、また、パンデミックからの回復期においては、5Gネットワークを含む、ユニバーサルで手頃で安全な高速インターネット・アクセス、そして、クラウドサービスへの責任ある移行を推進することを政府に求めています。 上記の見解は貴省の対策案とも一致しており、加えて、以下の意見を述べさせて頂くことで、日本政府がCOVID-19からの回復においてセキュリティをさらに強化し、日本経済の回復力を強化し、2021年の東京オリンピック・パラリンピック競技大会に備えることに貢献したく考えています。	本総合対策の内容に賛同の御意見として承ります。
97	法人M（テレコムサービス協会）	―	③サイバーセキュリティ攻撃に関する補償の相互扶助制度・保険の創設 ・昨今、サイバーセキュリティ攻撃を対象にした損保会社が中心に、サイバーセキュリティ保険が流行っております。しかし、保険料は、損保会社の裁量に一任され、高額なものとなっております。 ・サイバーセキュリティ攻撃は、増加の一途を辿っており、自社だけで、その保険料を賄うのも、限界があります。よって、複数社で、相互で補償し合う保険制度を国が音頭を取り、実施出来ないか、という提案になります。これは、どうしても、損保会社達が仕切ると高額となり、入りたくても入れない企業様がいると思われるからです。 ご検討の程、お願いいたします。	御指摘の点については、サイバーセキュリティリスクの減少のためのセキュリティ対策をとりつつ、有事の際に備えてサイバーセキュリティリスクを移転する仕組みとしてのサイバーセキュリティ保険の双方を検討することが重要と考えます。その上、サイバーセキュリティ保険については、損害保険会社によって既に提供されているところですが、一定のセキュリティ対策をとっていることを示すことで保険料が減免になる例も存在します。

項番	意見提出者	該当箇所	御意見の詳細	御意見に対する考え方
98	法人I（BSA ｜ザ・ソフトウェア・アライアンス）	―	BSAは、上記が対策案をまとめるに参考となることを願います。データ・フリー・フロー・ウィズ・トラスト（DFFT）を支えるために貴省がサイバーセキュリティにおいて、リーダーシップを発揮するのを我々は支援します。また、今後は、政策提言に関して意見募集をする際は、長めの期間を設けることを奨励します。19日間ではなく60日間であれば、対策案を検討・分析し、高い関心を持つ利害関係者間で調整し、我々の立場や提案をまとめ、思慮深く、建設的な提言を、政策策定においてすることが可能となります。また、BSAは現在、セキュリティ政策において世界中の政府を支援するために、IoTや5Gのセキュリティに関する指針を策定しております。本意見に関してご質問等があれば、いつでもご連絡下さい。	本件について意見募集期間を20日間としておりますが、本総合対策は、行政手続法（平成5年法律第88号）第39条第1項において、「案及び関連資料をあらかじめ公示し、意見提出期間等を定めて広く一般の意見を求めなければならない」と規定されている「命令等」に該当しないことから、任意の意見公募として実施しているものであり、その期間についても既存の同種の文書の任意の意見公募の例を参考にして定めたものです。
99	法人J（アドイン）	―	状況変化とは、CNS（Communication Network Security）として考えた場合Networkの増大にと多様性があります。 個別固有の留意事項はわかりますが、暗号学的、数学的、学術的及び市中解決策で、抜け落ちていた「信頼関係」の担保を忘れています。利用者と提供者、通信するEntity間（必ず2点です）このことを確実に行えばかなりの本対策で言うSecurity対策の解決baseになります。	御指摘の点については、今後の取組の参考とすることが適当と考えます。
100	法人J（アドイン）	―	防御、駆除、ワクチン、監査も必要条件ではあるが十分条件ではない	御指摘の点については、今後の取組の参考とすることが適当と考えます。
101	法人J（アドイン）	―	日本発のArchitectureはあります。 今現在利用されているほぼ全てのベースは、欧米と中国が先導しています。 アメリカのように利用者がNISTを動かし枠組みを決めていくなど 日本では利用者の望みが国が決めてくれればそれに従うではリテラシーの向上は望めません。自主性がないから技術も追いつかず施策も後手後手になります。 最後に添付にNISTとも進めている日本発のArchitectureとProtocolを添付します。 USでは、原丈人様が発起人の一人です。 日本では、辻井重男先生に監修をお願いし、藤原洋様にもご協力をお願いしています。	御指摘の点については、今後の取組の参考とすることが適当と考えます。
102	法人K（アマゾンウェブサービスジャパン）	―	全般的なコメント AWSは、総務省が提言するテレワークの推進及び国際的なサイバーセキュリティのコミュニティにおける国際協力を深めて行くという方向性に賛同し、サポートさせていただきたいと考えています。とりわけ、コロナ危機を経たのち、政策におけるサイバーセキュリティの重要性は増しています。AWSは、各府省情報化統括責任者（CIO）連絡会議が決定した「政府情報システムにおけるクラウドサービスの利用に係る基本方針」（2018（平成30）年6月7日）について、政府諸機関に対し情報システムにおけるクラウドサービスの利活用について有益なガイドを示すものであることから、強くサポートします。AWSは、クラウドのコスト削減効果、サポート、機能性及び内在する高いセキュリティを認めたうえで、政府情報システムにおいてデフォルトでクラウドサービスを採用することを促すCIO連絡会議の「クラウドバイデフォルト」原則を支持いたします。AWSは、総務省サイバーセキュリティ統括官室が、引き続きグローバルなセキュリティ基準や監査基準に合致したセキュリティ政策を推進することを希望いたします。またAWSは、各種組織がIoT、5G及び各種クラウドサービスを安全且つセキュアに用いるためのハイレベルのガイドラインを作成するという、総務省の方針にも賛成いたします。AWSは、総務省がサイバースペースと物理スペースをつなぐデバイスやシステムに多様なリスクがあり得ることを想定し、ハイレベルのガイドを策定されることに感謝申し上げます。これまで、AWSは日本政府に対し、AWSのグローバルなクラウドに関する実務経験を共有することで、ISMAP（政府情報システムのためのセキュリティ評価制度）の策定に協力して参りました。AWSとしましては、総務省がクラウドサービスのセキュリティの評価を行うための技術的側面を評価する第三者監査及び国際的に認められた産業界におけるセキュリティ標準の価値を、今後も認識していただくことを希望いたします。またAWSは、総務省が引き続き、弊社のグローバルな顧客の皆様へのサービス提供を通じて蓄積した経験を踏まえたインプットを重視し、より良い政策形成に臨まれますことを希望いたします。また、AWSは、総務省がISO27001やSOCレポート等の既存の産業界リードによるリスク管理や信頼性確保のためのメカニズムをリソースとして活かした形で、民間企業がガイドラインやフレームワークを運用できるよう柔軟性をもって対応いただくようお願いしたいと考えます。	本総合対策の内容に賛同の御意見として承ります。 御意見を踏まえ、本総合対策に盛り込まれた施策に取り組んでいくことが重要と考えます。

項番	意見提出者	該当箇所	御意見の詳細	御意見に対する考え方
103	個人A	―	「サイバーセキュリティー対策」が重要な構造と、私し個人は思います。例えばですが、「センサー技術、ネットワーク技術、デバイス技術」から成る「CPS（サイバーフィジカルシステム）」の導入により、「ゼネコン（土木及び建築）、船舶、鉄道、航空機、自動車、産業機器、家電」等が融合される構造と、私は考えます。具体的には、「電波規格（エレクトロリカルウェーブスペック）」及び「通信規格（トランスミッションスペック）」での「回線（サーキット）」の事例が有ります。（ア）「通信衛星回線（サテライトシステム）」における「トランスポンダー（中継器）」から成る「ファンクションコード（チャンネルコード及びソースコード）」のポート通信での「DFS（ダイナミックフレカンシーセレクション）」の構造。（イ）「電話回線（テレコミュニケーション）」における基地局制御サーバーから成る「SIP サーバー（セッションイニテーションプロトコル）」の構造。（ウ）「インターネット回線（ブロードバンド）」におけるISPサーバーから成る「DNSサーバー（ドメインネイムシステム）」の構造。（エ）「テレビ回線（ブロードキャスト）」における「通信衛星回線、電話回線、インターネット回線」の構造。具体的には、「方式（システムスペック）」での「回線（サーキット）」の事例が有ります。（ア）「3G（第3世代）」における「GPS（グローバルポジショニングシステム）」から成る「3GPP方式（GSM方式及びW-CDMA方式）」の構造。（イ）「4G（第4世代）」における「LTE方式（ロングタームエボリューション）」から成る「Wi-Fi（ワイアーレスローカルエリアネットワーキング）」の構造。（ウ）「5G（第5世代）」での「NR（New Radio）」における「MCA方式（マルチチャンネルアクセス）」から成る「DFS（ダイナミックフレカンシーセレクション）」の構造。具体的には、「情報技術（IT）」及び「人工知能（AI）」での「回線（サーキット）」の事例が有ります。（ア）クラウドコンピューティングでは、「ビッグデータ（BD）」から成る「データーベース（DB）」の導入により、ITネットワークの構造。例えばですが、ファイアーウォールにおける強化では、ルーターとスイッチを挟み込む様に導入する事で、「クラウド側（プロバイダー側）←ルーター⇔ファイアーウォール⇔スイッチ→エッジ側（ユーザー側）」を融合する事で、ハードウェアーの強化の構造。（イ）エッジコンピューティングでは、Web上における「URL（ユニフォームリソースロケーター）」での「HTML（ハイパーテキストマークアップラングエッジ）」から成る「API（アプリケーションプログラミングインタフェース）」に導入により、「HTTP 通信（ハイパーテキストトランスファープロトコル）」における暗号化によるソフトウェアーでの「HTTPS（HTTP over SSL/TLS）」の融合により、AIネットワークの構造。具体的には、「サイバー空間（情報空間）」及び「フィジカル空間（物理空間）」での「回線（サーキット）」の事例が有ります。（ア）「サイバー空間（情報空間）」では、「SDN/NFV」における「仮想化サーバー（メールサーバー、Web サーバー、FTP サーバー、ファイルサーバー）」から成る「リレーポイント（中継点）」での「VPN（バーチャルプライベートネットワーク）」が主流な構造。（イ）「フィジカル空間（物理空間）」では、「AP（アクセスポイント）」が主流な構造。要約すると、「ボット（機械における自動的に実行する状態）」による「DoS攻撃」及び「DDoS攻撃」でのマルウェアーにおける「C＆Cサーバー（コマンド及びコントロール）」では、「LG-WAN（ローカルガーブメントワイドエリアネットワーク）」を導入した「EC（電子商取引）」の場合では、クラウドコンピューティング及びエッジコンピーティングにおける「NTP（ネットワークタイムプロトコル）」の場合では、「検知（ディテクション）⇒分析（アナライズ）⇒対処（リアクションメソッド）」での「サイバーセキュリティー対策」が重要と、私は考えます。	御指摘の点については、今後の取組の参考とすることが適当と考えます。
104	個人C	―	今や、戦争や侵略は銃や大砲、ミサイル、化学兵器ではなく、国に送り込まれた工作員がさも日本人として偽名で政治家やマスコミ、国の中枢機関、企業に潜り込み、世論をミスリードし、日本国を危うくしており、さらにサイバー攻撃などあらゆる手段を使って乗っ取りを推進しています。我々もあらゆる手段で日本国と日本人を守らなければなりません。サイバーセキュリティーに関しても、ある一定以上のレベルを企業に義務付けるなど、法整備も必要であると思います。仮想敵国の真の目的を知り、守るために、先手を打って行きましょう。	御指摘の点については、今後の取組の参考とすることが適当と考えます。
105	個人D	―	1：NETクラウド互換ソフトの開発 2：NETクラウドOFFLINE使用の強制（やらせるのではなく、規制） 3:NETインフラシステム教育 対策に於ける改善効果 1：外部流出及び、外注による不当予算削減及び、評価適正。 2：OFFLINEによりウイルス感染リスク減少及び、リモートシャットダウン。 3:システムを理解していない為、余計な対策絵御行い、システムERRを引き起こすを排除。	御指摘の点については、今後の取組の参考とすることが適当と考えます。
106	個人E	―	ソフトバンク子会社の日本コンピュータービジョンから納品した中国共産党企業センスシステムの顔認識や検温システムを総務省、文科省、農水省は危機管理ができていない。センスシステムはアメリカから金融制裁企業に指定されており、又は、日本コンピュータービジョンはセンスシステムに約十億ドルの投資をしている企業である。もともとソフトバンクは中国共産党関連企業ですよ。様々なデータが中国共産党に流れている可能性があり、地頭が悪いとしか言いようがない。こんなことをしているとアメリカから制裁措置をとられるよ。	御指摘の点については、今後の取組の参考とすることが適当と考えます。
107	個人（多数）	その他	なお、意見公募の締切り（令和2年6月25日（木）17時）以降に「5Gの健康被害」や「5Gの中止」等に関する御意見が多数寄せられました。（御意見の詳細については省略）	本報告書は、IoT・5G 時代にふさわしいサイバーセキュリティ政策の在り方について検討し、「IoT・5G セキュリティ総合対策2020」として整理したものです。 我が国では、無線局から発射される電波について、これまでの科学的知見や国際的ガイドラインを基に、人体に影響を及ぼさない十分な安全率を考慮した安全基準（電波防護指針）を定め、携帯電話端末の製造や携帯電話基地局の設置等にあたっては、電波防護指針を基にした規制値を遵守するよう法令で規定されています。 5G システムで使用予定の6GHz 以上の周波数帯についても、総務省情報通信審議会一部答申「高周波領域における電波防護指針の在り方」（平成 30 年 9 月 12 日）を踏まえ、令和元年5月に必要な制度整備がなされたところです。 総務省においては、電波の安全性について、今後とも研究や検証を進めるとともに、国民の皆様へのわかりやすい周知など、引き続き必要な取組を行っていくこととなっております。