「ICTサイバーセキュリティ総合対策2021」（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

別紙１

■意見募集期間 ： 令和3年6月10日（木）～令和3年7月９日（金）

■意見提出件数 ： ９件（法人・団体：５者、個人：４者）

■意見提出者

	意見提出者
1	一般社団法人情報処理安全確保支援士会
2	KDDI株式会社
3	華為技術日本株式会社
4	ヴイエムウェア株式会社
5	BSA ザ・ソフトウェア・アライアンス
ー	個人（４者）

※いただいた御意見につきましては、原文を御意見ごとに分割して記載しております（ただし、本総合対策（案）と無関係と判断されるものは除いております）

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
1	一般社団法人情報処理安全確保支援士会	I. （３） 主要な政策課題への対処のための施策の整理・分類	［意見１］ P7（３）主要な政策課題への対処のための施策の整理・分類 各個別分野における政策課題への対策において、情報セキュリティ対策に関しては法律に根拠を持つ唯一の国家資格者である情報処理安全確保支援士の必置化を推進する観点での追記が必要である。これは、総務省が国民の安心・安全のために従前から行っている、無線局における無線従事者免許所持者の必置規定や電気通信事業者における電気通信主任技術者の必置規定と同様、高度な技術知識を要する分野において、その確実な履行を担保するためには無免許・無資格従事状態をこれ以上放置することは適切ではないとの観点からの指摘となる。そしてこられの業務について「アマチュア無線で十分に『無線の経験』があるから第1級アマチュア無線技士に第一種陸上特殊免許の範囲の業務をさせても問題ない」とはしていないにも関わらず、情報処理の分野については「経験」を基に従事を許可しているという点も、総務省の主張には大きな矛盾があることを指摘せざるを得ない。総務省が所管する免許制度は「必置主義」であるのに、経産省が所管する免許制度は「経験主義」でよしとするのであれば、その根拠について明確な見解を頂きたい。 総務省が所管する通信系の資格者必置措置についても、時代の要請に応じて資格体系等を整備・更新しつつその有効性を確保してきたという実績から鑑みても、サイバー空間の活用が急速に拡大、Society5.0として重要な社会基盤となりつつある現時点において、法律に根拠を持つ唯一の国家資格者である情報処理安全確保支援士の必置化については、総務省の国民に対する責任として積極的に検討・推進すべき課題であることを指摘したい。全体意見に記載したとおり、情報セキュリティ人材の重要性、という従来の表現では既に深刻な問題が生じており、現時点に置いてそれに取り組んでいないことは、まぎれもなく国民の安全確保に対する行政の怠慢であり、例えば情報処理安全確保支援士の活用について、内閣府のスーパーシティ構想においては言及されているが、総務省のスマートシティにおいては一言も触れられていないといった状況は、所管省庁が異なるという「縦割り」それのみを理由として、国民を危険に晒していると指摘せざるを得ない。デジタル庁の設置といったタイミングで、情報通信分野に関する資格者必置の推進については省庁を越えた検討を行い、それを踏まえた総合対策を講じる責任が総務省には存在していると考えている。	御意見については、参考として承ります。
2	一般社団法人情報処理安全確保支援士会	I. （３） 主要な政策課題への対処のための施策の整理・分類	それを踏まえて 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確保のためのセキュリティ対策の推進 …電気事業者のネットワークにおけるリスクの高まりに応じ「情報処理安全確保支援士といった国家資格者の必置を検討する等」といった適切なセキュリティ対策を講じ －とすることが、一般社団法人情報処理安全確保支援士会として必要であると考えている。	「Ｉ　改定に当たっての主要な政策課題」において、セキュリティ人材育成の推進に関しては、「横断的な施策」としてP8で言及されているため、御指摘をいただいた箇所については原案のとおりとします。
3	一般社団法人情報処理安全確保支援士会	I. （３） 主要な政策課題への対処のための施策の整理・分類	②ＣＯＶＩＤ－１９への対応を受けたセキュリティ対策の推進 …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、「例えば令和２年度に経済産業省が行った中小企業の情報セキュリティマネジメント指導業務における情報処理安全確保支援士会の活用といった事例を参考として、同様に総務省においても情報処理安全確保支援士を活用した」その対策の強化は急務である。 －とすることが、一般社団法人情報処理安全確保支援士会として必要であると考えている。	「Ｉ　改定に当たっての主要な政策課題」において、セキュリティ人材育成の推進に関しては、「横断的な施策」としてP8で言及されているため、御指摘をいただいた箇所については原案のとおりとします。
4	一般社団法人情報処理安全確保支援士会	I. （３） 主要な政策課題への対処のための施策の整理・分類	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 …デジタル改革・DX推進の基盤となるサービス等における「情報処理安全確保支援士の必置・活用の推進により実効性のある」課題に応じた適切なセキュリティ対策を講じ －とすることが、一般社団法人情報処理安全確保支援士会として必要であると考えている。	「Ｉ　改定に当たっての主要な政策課題」において、セキュリティ人材育成の推進に関しては、「横断的な施策」としてP8で言及されているため、御指摘をいただいた箇所については原案のとおりとします。
5	個人Ａ	II. 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確保のためのセキュリティ対策の推進	＞11頁 IoT機器の踏み台化には、適切なファームウェアのアップデートが一つの抵抗手段であるが、現在、日本における大手ICT機器メーカーでも、ファームウェアをTLSでの保護が行われた回線ではなく、巣のHTTPでの配布を行っている事業者が存在する（ヤマハ等。なんと、ヤマハは、大手有力ネットワーク機器メーカーなのに、HTTPSプロトコルでのファームウェア配布を行っていない。）。 この様な事態について、政府が施策を行い、無くしていくようにされたい。	御意見については、参考として承ります。

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
6	一般社団法人情報処理安全確保支援士会	II．１．（１） 安全かつ信頼性の高いネットワークの確保	［意見２］ P12（１）安全かつ信頼性の高いネットワークの確保 物理的な安全性と信頼性については、総務省がこれまで講じてきた無線従事者免許制度や電気通信主任技術者制度によって十分に担保されている。しかし一方で論理的なそれについては、無免許無資格で従事できる状況であり、物理的には資格が必要だが、論理的には資格が不要といった重大な矛盾が生じている。 総務省にはこの矛盾を解消すべく、安全かつ信頼性の高いネットワークを論理面でも確保するために、現状で唯一の国家資格者であり、定期的な研修により論理面でのセキュリティ対策について高い知見を法律によって保障されている情報処理安全確保支援士を総務省が所管する既存の必置制度に加えて、迅速に必置化し配置を行う必要があると考える。これを踏まえて ①ガバナンス確保の在り方に関する検討 …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とともに、「情報処理安全確保支援士の必置化によるリスク軽減の可能性」について取りまとめることが適当である。 －とすることが、一般社団法人情報処理安全確保支援士会として必要であると考えている。	セキュリティ人材の必要性や育成に関する施策は「Ⅲ　横断的施策」に言及されているため、御指摘をいただいた箇所においては原案のとおりとします。
7	ＫＤＤＩ株式会社	II．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	サイバー攻撃の予兆をとらえて早期に対処できるようにすることは重要だと考えます。様々な実現手法が想定されるため、広く、基礎的なところから検討を進めることが必要かと考えます。	本総合対策の内容に賛同の御意見として承ります。
8	華為技術日本株式会社	II．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 （３）5Gの本格的な普及に向けたセキュリティ対策の変化	（本文15ページ以下記述） 「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。」 （本文16ページ以下記述） 「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。（中略） 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」 （意見） 電気通信事業者の間で脆弱性情報等の情報の共有の取組が重要であることに同意する。 さらに、5Gシステムに組み込まれた不正な機能や脆弱性の検出に関する技術開発の取り組み、そのセキュリティ対策の民間への情報共有の取り組みに賛同する。 一方で、5G機器製造事業者が取るべきセキュリティ対策においても明確に言及することを提案する。例えば、本文第２章(2)③「脆弱性の検証手法等の確立と体制整備」で弊社が提案したグローバル標準・認証の基準を日本のセキュリティ対策に取り入れ、必要に応じて日本特有の要件を加えたうえで、電気通信事業者と5G機器製造事業者とが共通の検証基準を見据えて日本のセキュリティ対策に取り組み、リーダーシップを取ってその成果を国内外に発信することも重要であると考える。	本総合対策の内容に賛同の御意見として承りました。 なお、御意見については、参考として承ります。
9	ＫＤＤＩ株式会社	II．１．（３） 5G の本格的な普及に向けたセキュリティ対策の強化	今後5Gの重要性が高まることから、「5Gを念頭にした不正な機能や脆弱性の技術検証」において「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」をまとめて5G通信ネットワークの安全性と信頼性を確保する施策を推進することは非常に重要だと考えます。	本総合対策の内容に賛同の御意見として承ります。

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
10	一般社団法人情報処理安全確保支援士会	II. 2. COVID-19への対策を受けたセキュリティ対策の推進	[意見３] P18 2 COVID-19への対策を受けたセキュリティ対策の推進 COVID-19により、ニューノーマルという考え方が提唱され、急速にテレワークを促進する機運が醸成された。しかし、本書において指摘されているとおり、中小企業等におけるテレワークの普及・定着は、何をすればよいのかという支援を適切に実施できる体制が十分に整備されていなかったことにより大幅に立ち遅れ、これにより、大企業と中小企業等の格差をより一層拡大することとなった。また、地域のコミュニティ形成の一助となっているお稽古事といった生涯学習や、飲食店といった事業者にとっては特に深刻な影響が生じることとなった。こういった状況は、情報処理安全確保支援士を要件としたCISO又はCDOを都道府県及び政令市に必置化し、それらを中心として地域SECUNITYの構築に着手していれば避けることができた事態であったと考える。効果的な地域SECUNITY構築について、都道府県及び政令市に情報処理安全確保支援士を任命要件とするCISOやCDOの必置を推進し、地方公共団体と地域が一丸となったデジタル化推進を行うべきである、という提言を過去にもICTサイバーセキュリティ総合対策へのパブリックコメントにおいて行ったが、総務省においては、各自治体において適任者が担当している（事実そんなことになっていないのは明らかであるが）という現実逃避した見解を示すことにとどまり、本会の提言を考慮してこなかった。それどころか、資格を根拠として求めることなく「経験を評価して」CIO補やデジタル活用人材について税金を投じて支援するという、より現場に混乱を招く悪質な事業を推進し続けている。 そのことが、地域SECUNITY以前に、地域コミュニティの破壊を促進したことについて、総務省は猛省すべきであり、その反省を踏まえて過ちを繰り返すことなく、この際COVID-19危機を奇禍として、地方公共団体のデジタル化促進のために、地方自治体において「第三者の検証不可能な経験ではなく、情報処理技術者試験を根拠とした能力評価」と、それに基づく人事制度について直ちに導入に向けた調査・検討を開始すべきである。従前から総務省においては、情報処理技術者試験は経産省の管轄ということで、情報処理安全確保支援士について本書においても一言も触れないといった「国民を危険に晒す無用なこだわり」が見られていたが、「デジタル社会の実現に向けた重点計画（2021年6月18日閣議決定）」を踏まえ、国民に奉仕する一国家機関として今回こそはそのこだわりを捨て、国民の安心・安全の実現と、そのために必要なデジタル化推進のために必要な情報処理技術者活用について真剣に向き合ってほしいと一般社団法人情報処理安全確保支援士会としては考えている。 これを踏まえて （１）テレワークセキュリティの確保 …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。「加えて、都道府県及び政令市に情報処理安全確保支援士を任命要件としたCISO又はCDOを設置することを促進し、各地域においてデジタル化において必要な対策を迅速に講じることができるように制度設計を行う必要がある。」を追加すべきであると、一般社団法人情報処理安全確保支援士会としては考えている。	セキュリティ人材の必要性や育成に関する施策は「Ⅲ 横断的施策」に言及されているため、御指摘をいただいた箇所においては原案のとおりとします。
11	個人Ｂ	II. 2. COVID-19への対策を受けたセキュリティ対策の推進	・II-2にて「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。」と記載しているが、正確性に欠ける。 「感染者数」ではなく、「PCR検査陽性者数」であり、「死亡者数」もコロナが死因と限らず「死者がＰＣＲ検査陽性であれば、コロナ死」としているのだから、「死者のうちＰＣＲ検査が陽性であったもの」と訂正すべき。また、ＰＣＲ検査陽性者は必ずしもコロナ患者とは限らないことを明確に記載すべき。 また、現在の表現は、コロナが怖いという意識を植え付けようとしているがごとき表現になっているので、「コロナの危機は未曾有と言われているが、実際の患者数の推移やコロナを主因とする死亡者数を見ると、大げさに騒ぎ過ぎの感はある。とはいうものの、世界的にも日本においてもコロナを過剰に怖がっている状況からすると、テレワークの推進およびそのサイバーセキュリティ対策は必要であり・・・」にような表現に改めるべき。	御指摘をいただいた箇所の記載としては、事実として厚生労働省より公表されている数値を記載しているものとなるため、数値を更新し、以下の通り修正します。 「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。」
12	ＫＤＤＩ株式会社	II. 3. （1）IoTのセキュリティ対策	IoT機器の運用段階での対策として、IoT機器製造事業者、設置・運用する事業者等に注意喚起対象を広げていくことや注意喚起手法を検討することは非常に重要だと考えます。	本総合対策の内容に賛同の御意見として承ります。
13	ヴイエムウェア株式会社	II. 3. （1）IoTのセキュリティ対策	（「ICTサイバーセキュリティ総合対策2021（案）」P23中「・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。」との記載部分） ・意見内容 当該部分について「・ソフトウェア脆弱性等を有するIoT 機器（例 VPN 機器）を、国内外から提供される脅威インテリジェンスを活用して特定し、注意喚起を行う手法について検討を進める。」との変更を提案します。 （理由） サイバー攻撃は海外由来のものが国内由来に比べて圧倒的に多いことから、海外で収集された情報の活用が必須ですが（案）ではそのことが明確に示されていません。本総合対策として、国内にとどまらず海外からの情報収集を行うという「国内外から提供される脅威のインテリジェンス」の文言をあえて明記することで、その必要性を本総合対策の関係者に知らしめる必要があると考えます。	法に基づいてNICTが実施している業務の改善にかかる検討であるため、現行法に基づく記載としており、原案のとおりとさせていただくとともに、御意見については、参考として承ります。

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
14	個人A	II．３．（１） IoTのセキュリティ対策	＞22頁 ＞23頁 電子メールの話が出てきているが、現在、日本の多くのISP等事業者は、電子メールについて、暗号化しての送受信両方を行えないようなメールサーバの運用を行っている。 ISP等事業者が自らのホームページ等で行っているような、認証局証明書の取得とそのメールサーバでの運用、及び対応したメールサーバソフトウェアの利用によって、電子メールのTLS保護（SMTPoverTLSやSTARTTLSによる。）が可能になり、それらが可能なサーバ間では、送受信両方のTLS保護が可能になるのであるが、ほとんどの事業者（NTTドコモやOCN等の超大手ICT事業者含む。超大手なのに、国民としては信じられない気分である。同社の有様は、悪事を企み、実行しているも同義であると考える。）がこの保護（送受信双方のTLSによる保護。（2020年あたりからやっと、相手側サーバが認証局証明書を導入している場合に、暗号化しての送信が可能になり始めた様であるが、自らのメールサーバではインターネット上の他メールサーバが暗号化のために用いるための認証局証明書を導入していない事がほとんどである。））に対応していない・対応しようとしていないので、政府は、ISP等事業者が、すみやかに（2021年中に！）、電子メールサーバにおいての認証局証明書の導入と電子メールの送受信双方の暗号化について行うように施策を行われたい。 というか、記載のある様な、ISP等の重要連絡電子メールについてもであるが、各種の行政が行う・行う事を予定している様な、重要な内容を含む電子メールの送受信についても、その送受信が暗号化されない、というのは、恐怖であり、また行政に既に差し支えが出ていると言えると考えるが（日本の、法定の、電気通信事業者であれば、電子メールの送受信のTLSによる保護が行われる状況が確率されているのであれば、この問題はかなり解決されると思われる。素の平文の電子メールがネットワーク上を行き来するのに比べて格段の保護が行われる事になるであろう。そのようにすべきであるはずである。全然なされていないが。総務省は何をやっているのか？悠長というか懈怠を発生させているのは間違いないであろう。（なお、国民としては、こんな状況では、行政が各種の重要な内容の書類を電子メールを用いて送受信するとする様な案について、賛成しにくいのである。当然の話であるが、全て、総務省のせいである事については、重く認識されたい。いつやるの？グーグル社のGmail等は相当前から対応を行っているのであるが。宿題はちゃんと早めに行われたい。2020年オリンピックの予定年でも2021年でも行われていなかったのであるが、いつやるのか？政府の責任は確実にあると認識されたい。））、政府は、事業者への監督・指示を行い、電気通信事業者が扱う電子メールについては、送受信ともにTLSによる保護が可能になるようにされたい。 当然であるが、この様な基本的な事について疎かにしている政府が、スマートシティなどと言うのは、片腹痛いものである。	御意見については、参考として承ります。
15	BSA ザ・ソフトウェア・アライアンス	II．３．（２） クラウドサービスの利用の進展を踏まえた対応	対策案に記載されているように、エンドユーザによる障害や設定ミスが発生しているものの、これらはオンプレミスや他の類似したサービスと重大な違いは無く、現在のクラウドで利用可能なセキュリティツールは、責任共有モデルと合わせ、最高レベルのセキュリティ実践を確保する包括的なものとなっています。 対策案の中で的確に認識されているように、クラウドコンピューティングは、コスト削減、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、といった多大な恩恵をもたらします。また、クラウドコンピューティングは、サイバーセキュリティの面でも大きく寄与します。日本がデジタル・ランスフォーメーションを実現し、これらのメリットを十分に活用するためには、政府においてクラウドコンピューティング・サービスが広く導入されることが不可欠であり、対策案で示されているように、このために、政府機関が調達するクラウドサービスのセキュリティを評価する「政府情報システムのためのセキュリティ評価制度」（ISMAP）が昨年開始されました。クラウドサービスプロバイダー（CSP）に対する基本的なセキュリティ要件を設定した、本制度の発足を支持する一方、公共部門における「クラウド・バイ・デフォルト原則」の実現という日本政府の目標を促進し、また、本格的なデジタル・トランスフォーメーションを可能にするサイバーセキュリティへの取り組みを支える上で、ISMAPの実施があまりにも煩雑で高額な費用を要していることに、我々は懸念を抱いています。 ISMAPには1,000以上の管理項目が掲載されているため、サービスを提供する企業やISMAP認証の取得を希望する企業には大きなコンプライアンス負担と法外なコストが課せられ、多くのCSPにとってISMAP認証の魅力が低下します。その結果、ISMAPクラウドサービスリストに登録され、日本の公共機関にサービスを提供できるCSPの数が不必要に制限される可能性があります。	御指摘の点については、クラウドサービス事業者の御意見を踏まえつつ、政府機関等における安全性の担保されたクラウドサービスの利用を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
16	BSA ザ・ソフトウェア・アライアンス	II. 3. （2）クラウドサービスの利用の進展を踏まえた対応	我々は、以下の点を考慮に入れ、政府が継続的に ISMAP の改善を検討することを奨めます。 • 様々なクラウドサービスのモデル（SaaS、IasS、PaaS）の特徴的な要件を考慮して、これらのサービスのリスクを管理するために最適化された必須のセキュリティ管理を定義することにより、現行の ISMAP をより柔軟で、実施しやすくすること。 • ISMAPを適用するにあたっては、中核となる基本的な管理策を対象とし、その他の追加の管理策については、実施される特定の状況下における必要に応じて適用されるようにし、広く採用されている国際規格、および調達側との間で締結された契約における追加要件に基づくこと。 • 国際的なクラウド・セキュリティのベスト・プラクティスに沿った、頻度を減らした監査スケジュール（例：三年に一度）を設定し、CSPと政府双方の監査作業を削減すること。毎年の監査では、CSP は連続して監査プロセスを実施しな くてはならず、常時、監査対応に追われることとなり、セキュリティ担当者の注意を不必要にそらすこととなります。調達省庁側にとっても、年度の契約更新の負荷が増すこととなります。 • 申請・登録の受付を、四半期ごとではなく、年間を通じて行うことができるようにすること。年に 4 回の申請・登録に限定されると、CSP にとっては、3ヶ月以上の遅れが生じる可能性があります。年間を通して継続的に申請・登録を行うことで、ISMAPは急速に進化するクラウドの技術に対応することが可能となります。 • ISMAP の開発プロセスと並行して、日本におけるクラウドサービスのためのIT 監査・ 認証要員の訓練・育成をするための手続を開発し、適切な人材を確保すること。 • クラウドサービスの責任共有モデル 3) を強調し、周知徹底させること。対策案において、責任共有モデルが認識されていることを我々は高く評価しており、政府機関全体において本モデルが理解されるよう、貴省が先導をとることを奨励します。ISMAPに責任共有の原則を明確に盛り込むことで、クラウドサービスのリスク管理をするための管理基準の設定と維持において、CSPと顧客との間とのクラウド運用に関する異なる責任が適切に認識されるようになります。また、自らが管理し、責任を負う環境の側面において、どの当事者が説明責任を負うのかを明確にすることができます。これにより、アクセス権を持たない顧客データやシステムに対して、CSP にセキュリティ要件や義務を課すという、セキュリティやプライバシーにとって逆効果をもたらすような状況を避けることができます。クラウド導入を成功させるには、クラウド利用者や調達者が、クラウド環境で安全なアプリケーションを開発し、必要に応じてサービス・ プロバイダーが提供するツールや対策を自らの責任で利用し、セキュリティ・リスク を最小限に抑えることが求められている、ということが理解されることが重要です。 3) https://cloudsecurityalliance.org/blog/2020/08/26/shared-responsibility-model-explained/ • 第三者による、国際的な認証および監査結果を、ISMAP の関連する管理基準および要件に準拠している証跡として認めること。これにより、実用的でない、現地監査の必要性が減ります。現地監査は、本目的以外では権限を持たない者による現場へのアクセスを要するため、データセンターを不必要な物理的セキュリティ・リスクにさらすことになります。 また、日本のデジタル・トランスフォーメーション（DX）という目標を支えるために、革新的で順応なセキュリティ・アプローチを可能にするようなクラウド・セキュリティ政策を採用することを強く推奨します。これにより、セキュリティへのリスク対応や回復力といった、クラウド技術が可能とする利点を効果的に活用することが可能となります。	御意見については、参考として承ります。
17	BSA ザ・ソフトウェア・アライアンス	II. 3. （2）クラウドサービスの利用の進展を踏まえた対応	この観点から、ISMAPの見直しに加え、「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」4）において、地方公共団体に対して、マイナンバー・データを管理する情報システムの物理的なネットワーク分離の実施を推奨するような、時代にそぐわないセキュリティアプローチを排除することを求めます。国民のプライバシーや個人情報を保護する意図を我々は十分に理解し、支持しますが、このような政策は、導入のための高額な費用を発生させ、当該データの想定通りの利用を可能にする、革新的なクラウドベースの技術やサービスを活用する上で大きな障害となります。また、ネットワーク分離は、逆にシステムの安全性を低下させる可能性があります。 4) https://www.soumu.go.jp/main_content/000726079.pdf 独立したネットワーク構築のためには、独立したサーバー、ルーター、スイッチ、管理ツールなど、ネットワークをサポートするために必要なインフラを構築する費用が必要となり、生産性や効率性が低下します。接続されたネットワークと分離されたネットワークやデバイスの間で情報を管理することは、時間を要するだけでなく、混乱やエラーも引き起こし、さらなるセキュリティリスクにつながる可能性があります。多くのクラウドサービスは、暗号化や厳格なアクセス管理システムなど、国際的に認められた機能を実装することで、世界水準のデータセキュリティを実現しています。5) BSA会員を含む多くのグローバルなCSPは、データ・セキュリティへの大規模な投資をしており、利用可能な機微個人情報のために、最も効果的なデータ・セキュリティを提供しています。これらの最高水準の安全なソリューションの使用を可能にすることを、日本政府が政策によって確かなものとすることが不可欠であると、我々は考えます。これらの最高水準のデータ・セキュリティ・ソリューションは、リスクベースで成果重視の手法を採用しています。 5) BSA International Cybersecurity Policy Framework https://bsacybersecurity.bsa.org/report-item/bsa-international-cybersecurity-policy-framework 採用されているのは、ゼロトラスト・セキュリティ・アーキテクチャー6)、高度なユーザーID管理とアクセス制限システム、常時接続の仮想プライベート・ネットワークや仮想ネットワーク・セグメンテーションなどのネットワーク制御、ネットワーク層に加えてデータ・ベース層での強力なデータ暗号化など、「多層防御」7）に基づいたセキュリティ・アプローチです。 6）Zero Trust Architecture, NIST SP-800-207 https://www.nist.gov/publications/zero-trust-architecture 7）NISTでは「多層防御（Defense-in-Depth）」は「人、技術、および業務遂行能力を統合して、組織内の階層およ びミッションごとに複数の調節可能な防壁を築く情報セキュリテ ィ戦略」と定義されています。 https://www.ipa.go.jp/files/000056415.pdf https://csrc.nist.gov/glossary/term/defense_in_depth	御意見については、参考として承ります。

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
18	BSA ザ・ソフトウェア・アライアンス	II．３．（２）クラウドサービスの利用の進展を踏まえた対応	また、ゼロトラスト・セキュリティ・アーキテクチャの考え方は、「暗黙の信頼ゾーン（implicit trust zone）」を可能な限り最小化することであるため、データを暗号化してオペレーターからも見えないようにしたり、システムの設計・開発段階で操作ミスをなくす努力をするなど、考え方に沿った様々なセキュリティ対策を行う必要があります。これらの対策は、一見するとサイバーセキュリティに直接関連してないように思えるかもしれませんが、ネットワークのセキュリティを含めたITシステム全体のセキュリティを確保する上で、非常に有効なアプローチとなります。 以上のことから、時代にそぐわない物理的なネットワーク分離やデータローカライゼーション要件を改め、現在の技術に合わせたセキュリティソリューションを採用し、成果重視のリスク管理制御に焦点を当て、「多層防御」の原則に基づいたベストプラクティスを採用し、安全なクラウドコンピューティングサービスの調達と利用を通じて政府業務をより効果的に推進させることを貴省に求めます。サイバーセキュリティのソリューションは、官民が連携し、市場主導型のソリューションを採用する時に最も効果を発揮します。8）BSAとBSA会員企業は、ISMAPの改善、また、意識向上のための教育プログラム提供など、貴省と協力し、官民双方で「クラウド・バイ・デフォルト原則」を推進していきたいと考えています。 8）https://bsacybersecurity.bsa.org/report-item/bsa-international-cybersecurity-policy-framework	御意見については、参考として承ります。
19	ヴイエムウェア株式会社	II．３．（２）クラウドサービスの利用の進展を踏まえた対応	（「ICTサイバーセキュリティ総合対策2021（案）」P26中「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。」との記載部分） ・意見内容 当該部分について「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が提供するマルチクラウドに対応した設定情報変更の可視化サービス及び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。」との変更を提案します。 （理由） 利用が進んでいるマルチクラウド環境においては、サービス提供者をまたいだ設定情報の管理が求められますが、当該サービス提供者をまたいだ設定情報の管理は各サービス提供者から個別に供給されるツールでは極めて困難です。そのため、セキュリティ事業者が提供する当該サービス提供者をまたいだ設定情報変更の可視化サービスの存在とその活用の必要性を本総合対策において明示する必要があると考えます。	いただいた御意見を踏まえ、該当箇所（P26）を以下の通り修正します。 「セキュリティ事業者が提供するマルチクラウドに対応した設定情報変更の可視化サービス及びセキュリティ事業者によるアセスメント等も活用し、」 →「セキュリティ事業者が提供するマルチクラウドに対応した設定情報変更の可視化サービス及びセキュリティ事業者による<u>クラウド監視のためのツールや</u>アセスメント等も活用し、」
20	ヴイエムウェア株式会社	II．３．（２）クラウドサービスの利用の進展を踏まえた対応	（「ICTサイバーセキュリティ総合対策2021（案）」P26中「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。」との記載部分） ・意見内容 当該部分について「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。なお、利用者・調達者としてのクラウドサービス事業者は、利用するクラウドサービスの構成、設定などが、事前に定義するポリシーに準拠して適切に設定されているかを定期的に確認する必要がある。」との変更を提案します。 （理由） クラウドサービスの利用にあたり、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事は本文に記載されている通りです。その継続的な対策として、構成や設定の確認作業は一度きりまたは何かイベントが生じた随時ではなく、構成や設定がポリシーに準拠しているかを"定期的に"確認することが極めて重要です。そのため、定期的に確認することの必要性および重要性を本総合対策において明示する必要があると考えます。	いただいた御意見で追記された文章は、「利用者・調達者としてのクラウドサービス事業者」において実施する事項のため、同ページに記載されている「利用者・調達者としてのクラウドサービス事業者」において実施する事項が記載された箇所に下記の通り追記いたします。 「～～～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。」 →「～～～アセスメント等も活用し、<u>調達後も設定等を定期的に確認することで、</u>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。」
21	ヴイエムウェア株式会社	II．３．（２）クラウドサービスの利用の進展を踏まえた対応	（「ICTサイバーセキュリティ総合対策2021（案）」P27中「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も注目されている。」との記載部分） ・意見内容 当該部分について「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。また、クラウドサービス間の連携を考慮したネットワークの検討、端末が接続する場所や接続するクラウドに応じ、必要に応じた動的なセキュリティを適用し柔軟性を確保する必要がある。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も注目されている。」との変更を提案します。 （理由） 複数のクラウドサービスの利用の拡大及びテレワークの拡大によって、前者に対してはクラウドサービス間の連携を考慮したネットワークセキュリティの検討及び、後者に対しては様々な利用形態及びネットワーク、アクセス可能なリソースに対応できる柔軟なセキュリティ確保の検討の重要性が「クラウドサービスの利用の進展を踏まえた対応」として今後ますます増大してきます。そのため、本総合対策においてはより幅広い視点として、それらを関係者に対して明示する必要があると考えます。	いただいた御意見の趣旨については、P27の注釈において言及されているため、原案のとおりとさせていただくとともに、御意見については、参考として承ります。

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	ヴイエムウェア株式会社	II．３．（３） スマートシティのセキュリティ対策	（「ICTサイバーセキュリティ総合対策2021（案）」P28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、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（令和３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手続が実施されたところである。」との記載部分） ・意見内容 当該部分について「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（令和３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手続を経て、同年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）」が公表されたところである。」との変更を提案します。 （理由） パブリックコメントを経て最終版である「スマートシティセキュリティガイドライン（第 2.0版）」が公表されているため、その事実を記載することを提案します。	いただいた御意見を踏まえ、該当箇所（P27）を以下の通り修正します。 「2021 年（令和３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手続が実施されたところである。」 →「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。」
23	個人 A	II．４．（１） 無線LANのセキュリティ対策	＞29頁 無線LANの安全性確保も重要であるが、無線LANを使わない形でのネットワーク運用を行えるようにしておくのも良いと考える。 NTTが提供するフレッツ・クロスでは、無線LANを有さないHGW一体型ONUの提供が存在しない状況であるが、無線LAN機能が機器に含まれているとどうしても危険性が生じるので、そもそもその様な機能の無い機器が運用出来るようにされたい。	御意見については、参考として承ります。
24	一般社団法人情報処理安全確保支援士会	II．４．（３） 地域の情報通信サービスのセキュリティ確保	[意見４] P30（３）地域の情報通信サービスのセキュリティ確保 現在総務省において「地方自治体情報システムの標準化及びガバメントクラウドへの集約化」という誤った施策が遂行されている。これにより情報通信技術者の東京集約が一層促進され、地域で情報通信サービスを提供している事業者においては、地方自治体情報システムという公共事業の消滅に備えて、事業撤退や大手事業者への業務統合が検討されている状況であり、地域の情報通信産業におけるエコシステムの崩壊という、地域SECUNITYの推進と真逆の施策が同じ総務省で実施されているという奇妙な状況となっている。これについては、内閣府が開設したデジタル改革共創ＰＦにおいても同様の危険性が指摘されているが、標準化の方法論は政治的な取り組みであり、情報工学的な観点では誤ったものである点が多々存在しているが、これらについての議論は総務省において無視されている。それが故に、単に地方に大きな損害を与え、なおかつ標準化で企図した効果は何も得られずに終わるのではないかと、高度情報処理技術者の団体である情報処理安全確保支援士会としては懸念を抱いている。 内閣府と連携し、デジタル改革共創ＰＦに投稿されている標準化やガバメントクラウドに対する懸念論を直ちに確認し、現在の「自治体の実態を把握しておらず情報工学面での危険性を指摘できない自称学識経験者・無資格無免許で十分な情報工学の見識を有していない自治体出身の自称経験者・利害関係者であるベンダー」からなる「自治体システム標準化検討会」については直ちに解散し、デジタル改革共創ＰＦにおいて懸念論を提示している高度情報処理技術者資格を所持する自治体職員を中心として標準化関連業務の再編成を行い、早急に正すべきは正していただきたいと考えている。こういった状況で、地域SECUNITYの構築が自発的に実施されることは困難である。例えば情報処理安全確保支援士の登録状況を見ても、極端に三大経済圏に偏っており、地方における人材不足は深刻である。よって、標準化やガバメントクラウドの構築といった取り組みを利用して、地方自治体のＤＸ推進を一種の大規模公共事業と位置づけ、それをトリガーとした能動的な地域SECUNITY構築が必要であり、そのためには特に多数の住民に直接接している政令市を皮切りとして、情報処理安全確保支援士の抜擢体制を整備し、標準化の早急な仕切り直しが必要であることを総務省においては認識していただきたい。 この考えに基づき 「このため、地域で…」以下について このため、第一段階として２０政令市、次に全ての都道府県において情報処理安全確保支援士を任命要件とする内部抜擢を中心としたCDO又はCISO設置の制度化を推進するとともに、総務省を中心としたウォーターフォールな標準化から、住民に一番近いところにいる地方自治体職員によるアジャイルな標準化へと取り組みの見直しを行う。この取り組みを通じて、地方自治体が中心となり、地域の各種民間企業、教育機関、関係団体等が、顔の見える関係の中で、セキュリティを踏まえたデジタル化推進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。そのうえで、このような体制等において、SNS等を活用した地域のセキュリティ意識向上・人材育成や、地方の顔である政令市及び都道府県による情報提供が持続的・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及びデジタル化に関する「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及びデジタル化の持続的な推進が期待される。 －というものに差し替えることが望ましいと、一般社団法人情報処理安全確保支援士会としては考えている。	セキュリティ人材の必要性や育成に関する施策は「Ⅲ　横断的施策」に言及されているため、御指摘をいただいた箇所においては原案のとおりとします。
25	BSA ザ・ソフトウェア・アライアンス	III．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推進の前提として安全なサイバー環境を構築するためには、産学官連携によるサイバー攻撃等に関する情報の収集・分析を促進することが有用であるとする、貴省の見解を、我々は全面的に支持します。自主的なデータ共有の取り決めを促進することは、社会全体のセキュリティ対策のレベルを高めることに貢献します。また、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、ISAC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。また、サイバーセキュリティの強化は、導入されている技術が国内か海外のものかによって左右されるものではありません。 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し、また、生産国に関係なく利用可能な最良のセキュリティ技術を確実に採用することに注力することを奨めます。これにより、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り、日本が国際的にサイバーセキュリティでリーダーシップを発揮できなくなる事態を回避することができます。	御意見については、参考として承ります。

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
26	個人Ｂ	III．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	・被害情報の開示・共有については、被害を受けた企業が情報公開を躊躇するのは理解できる一方、そういう被害情報が共有されないと、対策が遅れてしまうというのは、納得できるところ。現状は、個人情報が流出した可能性がある場合のみ公表されている感じなので、個人情報の流出ありなしに関わらず、サイバー攻撃を受けた場合は、報告を義務付け、公表については、企業が特定されない程度の情報（どの産業分野で、どのような攻撃を受けたかなど）を公的機関が速やかに実施すべき。	御意見については、参考として承ります。
27	ＫＤＤＩ株式会社	III．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確保に向けサイバー攻撃情報等を収集・分析し活用する必要があり、社会全体でセキュリティ対策を底上げするためには産官学で連携するコミュニティ形成を推進することは大変重要であると考えます。	本総合対策の内容に賛同の御意見として承ります。
28	ヴイエムウェア株式会社	III．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	（「ICTサイバーセキュリティ総合対策2021（案）」P33中「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。」との記載部分） ・意見内容 当該部分について「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、国内外を問わずサイバーセキュリティ製品やサイバーセキュリティの情報を有効に取り入れることで、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。」との変更を提案します。 （理由） 国内の関係情報はもとより、海外企業製品や情報を積極的に取り入れ、NICTのソースをより広げることを本総合対策で明示することで、関係者にその必要性を知らしめ「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」につながると考えます。	本取組は、国産のサイバーセキュリティ情報を生む取組であり、原案どおりとさせていただくとともに、御意見については、参考として承ります。
29	ＫＤＤＩ株式会社	III．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	サイバー攻撃被害情報の適切な共有及び公表の促進のための検討を進めていくことは重要と考えます。	本総合対策の内容に賛同の御意見として承ります。
30	華為技術日本株式会社	III．２．（２） 研究開発の推進	（本文40ページ以下記述） 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。 （意見） 技術的検証を通じて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に賛同する。特に5Gネットワーク機器の検証は国際的な協調の元に行い、オープンな第三者機関による検証・認証の仕組みの導入を推進すべきである。 例えば、欧州では欧州委員会の元で欧州共通の5Gセキュリティ認証の仕組みが検討されており、それに呼応してGSMAは3GPP標準と協調したNESAS（Network Equipment Security Assurance Scheme）を運用している。さらにNESASを拡張して欧州の5Gセキュリティ標準とすることも検討されている。 これら5Gセキュリティのグローバル標準・認証の動向を注視しながら、日本にも5Gセキュリティのグローバル標準・認証仕組みを導入し、外部専門機関による実用機器の検証試験、セキュリティ認証制度の導入を提案する。これは、日本企業によるソリューションのグローバル展開の促進にも寄与するものと考える。	本総合対策の内容に賛同の御意見として承りますした。 なお、御意見については、参考として承ります。

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
31	一般社団法人 情報処理安全 確保支援士会	全般	サイバー空間を取り巻く多様な状況変化がみられていることを前提として、ICTサイバーセキュリティ総合対策について「必要な改定を行った」とあるが、情報セキュリティのＣＩＡ（=機密性（Confidentiality）、完全性（Integrity）、可用性（Availability））という観点から状況を確認してみると、例えばコロナ対策に関する各種アプリケーションにおける不具合、金融機関における大規模システム障害、頻発するマルチペイメントサービスの障害による決済不能や不正な財産の窃取といった、安心・安全とは程遠いと言わざるを得ない状況であり、改定の必要性には同意できるが、今回の改定で十分にこれらの状況に対応できるものに達しているとは到底認めることはできない。一般社団法人情報処理安全確保支援士会としては、サイバー空間及び広く情報通信に係る安全確保を支援することにより、国民の安心・安全なサイバー空間利用を促進するために設立された、法的根拠を持つ国家資格者の団体として、過去のパブリックコメントにおいて何度も「情報処理安全確保支援士の必置・活用」を提言してきた。 にもかかわらず、今回の改定においても「情報処理安全確保支援士」という言葉は用いられておらず、産官学における「自主的な情報セキュリティ人材の確保・育成」に関する取り組みに依存した極めて投げやり且つ国民に対して無責任な内容となっており、総務省においてサイバー空間の取り巻く状況が極めて危険な状況となりつつあり、これを回避するために、漠然とした人材ではなく、法的に情報セキュリティに関する能力が担保された現状唯一の国家資格者である「情報処理安全確保支援士」を明記し、その必置化や活用といったことについて未だ一切言及していないことは本総合対策の実効性を失わせる極めて重大な瑕疵であると言わざるを得ない。加えて、過去当会が提出したパブリックコメントへの意見に対し、『情報セキュリティ人材という存在に求められる能力には様々なものがあり、また、情報セキュリティに関する資格も複数存在するため、情報処理安全確保支援士とは明記できない』といった趣旨の見解表明を繰り返しているが、総務省が情報セキュリティに対しこういった無責任な姿勢を取り続けることで、現に悪意ある事業者による詐欺行為を助長し、それによる被害発生も確認されており、情報セキュリティ人材の資格名を明記しないことによって生じている国民に対する損害について、総務省において深刻に捉え、それを基に各種情報セキュリティ関連施策を講じてほしいと考えている。具体的には、情報セキュリティ人材の必要性を各種文書等で掲げつつも、最低要件となる資格名を記載しないことにより、民間事業者による「情報セキュリティ人材を想起させる名称のサムライ商法の乱立」が既に生じており、こういったサムライ商法のセミナーで費用をだまし取られるといった自己完結型の被害のみならず、十分な能力を持たない自主認定資格を提示してコンサルを行う「自称情報セキュリティの専門家」によるUTM（＝Unified Threat Management：統合脅威管理）等ネットワーク機器の誤設定や、不当に高額なネットワークセキュリティ機器の中小事業者への販売、不安をあおり高額なルータ設定確認料金を徴収するといった実効性のない情報セキュリティコンサルティングといった被害を確認することができる。単に「情報セキュリティ人材の育成・確保」と総務省がとらえていることも、サイバー空間を取り巻く多様な状況変化に伴って生じている現実空間を取り巻く悪質な状況変化であり、情報セキュリティ人材という抽象的な表現ではなく、現状唯一の国内法に根拠を持ち倫理規定が定められた国家資格者であり、情報セキュリティに関する継続的学習を法により義務付けられている情報処理安全確保支援士を、情報セキュリティ人材というあいまいな表現と置換し、なおかつより専門性が求められる分野については、例えば「情報処理安全確保支援士であって脆弱性診断の経験を有する者」という形で、情報処理安全確保支援士という具体的資格名に言及しつつ、必要な人材像を明確に提示する責任を、国民の安心・安全を守るべき総務省は痛感し、各種文書の作成にあたる必要があることを厳しく踏まえて行政施策の検討に当たってほしい。そして何よりも「デジタル社会の実現に向けた重点計画（2021年6月18日閣議決定）」において、情報処理安全確保支援士は「情報セキュリティの専門人材」として明確に位置づけられており、その他の資格や情報セキュリティ専門人材といたものは、日本国政府の決定として存在しないことが確認されたわけであるから、日本国政府の一機関である総務省としては、従前のようにごまかしの見解を表明することの社会への負の影響をこそ厳しく認識して、政府機関として一貫した方針に従い「情報セキュリティ人材」という用語については「情報処理安全確保支援士」と明記することを徹底していただきたい。 この考え方に基づき、以下提言する。	御意見については、参考として承ります。
32	一般社団法人 情報処理安全 確保支援士会	全般	【追加提言】 現在総務省において、地方及び地方自治体の情報化を推進するため、民間からCIO補を採用することについて交付金を支給するという施策を行っていたり、情報化推進人材派遣事業を行っていたりするが、この多くは地方のデジタル化にとって有害である。有害と断じる最大の理由として、これら施策における従事者にIPAの資格取得を要件としておらず、自己申告の経験で評価することが可能となっていることである。それにより、十分に能力がある人間ではなく、例えば首長の縁故でCIO補として採用されている事例が多く存在し、これらは単に現場に混乱をもたらすだけで、デジタル化の推進にはむしろ大きな阻害要因となっている。そもそも、デジタル化についてわからないから外部人材を頼るのであり、これらの経験が十分なものか判断する能力がないのに、経験を評価する仕組みにしているという制度設計そのものに無理があるということ想定する能力が総務省の担当者にはなかったのか、もし考慮漏れだったとしたならば、その地方軽視の姿勢について猛省を促したい。いずれにせよ、この混乱状態から一刻も早く「健全化」を果たすため、わずかな経験を針小棒大に騙る応募者又は縁故採用者への対抗策として、CIO補人材であれば「情報処理安全確保支援士・ITストラテジスト合格者」を必須要件として提示することに早急に取り組んでいただきたい。またあわせて、地方自治体には情報化人材がいないことを前提として制度が設計されてしまっているため、CIO補のポジションが委託として固定され、これら資格を既に所持している職員が飛び級できないといった弊害も生じている。自治体によっては、外部委託者に対して技術的な訓練を自治体職員が行うといった笑えない状況も生じている。総務省は自治体に対して、毎年度様々な照会を実施しているが、IPA資格取得状況に関する照会を実施したことはなく、つまりは総務省の地方自治体における情報化人材への意識というのは「騙りを認める」程度のもの、という認識を持たざるを得ない状況である。もし今回のDX推進に関して、人材育成・確保を重視するのであれば、まずは現状の確認が重要であり、そのためには「情報人材が不足していると思いますか」という主観を聞くアンケートではなく、実際の高度情報処理人材の配置状況を調査する必要があるのではないか。その調査結果を踏まえ、例えば高度情報処理技術者に限定した経験者採用を推進している熊本市や、情報処理安全確保支援士会の理事を輩出している広島市といった、既に十分に情報処理安全確保支援士及び高度情報処理技術者試験合格者が在籍している都道府県及び政令市の人事部門に対しては、DXに対応するための人事制度として、デジタル改革共創ＰＦにおいて提言されている既存の高度情報処理資格試験合格者及び情報処理安全確保支援士を中心とした飛び級・抜擢制度のモデルケースとなる取組をデジタル庁設立と合わせて着手することを依頼するとともに、一部自治体で散見される縁故採用や現場経験のない元コンサルタントの騙り経歴で業務に従事している無資格無免許者と、高度情報処理技術者資格を有する有能な既存職員の交代を指示することが、地方の安心・安全及びSociety5.0時代の地方振興を行うために最優先で取り組むべき行政課題であるということを一般社団法人情報処理安全確保支援士会として指摘させていただきたい。	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。 御意見については、参考として承ります。

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
33	BSA ザ・ソフトウェア・アライアンス	全般	BSA は、政府やグローバル市場において、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、クラウドコンピューティング、モノのインターネット（IoT）、人工知能（AI）、また、その他の新たなイノベーションをもたらす製品やサービスなど、世界経済の成長を促進するソフトウェアを活用した技術革新の最前線にいます。また、BSAの会員は、現在、業界全体で使用されているソフトウェア・セキュリティのベスト・プラクティスの多くを開拓した、セキュリティのリーダーでもあります。 BSAは、昨年、「IoT・5G セキュリティ総合対策 2020（案）」2) に対して意見書を提出しており、貴省が引き続き、日本のデジタル・トランスフォーメーションを推進し、国民が様々なデジタルサービスを安全に利用できる環境を整備することに重点を置き、サイバーセキュリティの向上に向けて取り組まれていることを高く評価しています。 １）BSA の活動には、Adobe, Altium, Amazon Web Services, Atlassian, Autodesk, Aveva, Bentley Systems, Box, Cisco, CNC/Mastercam, Dassault, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Nikon, Okta, Oracle, PTC, Rockwell, Salesforce, ServiceNow, Siemens Industry Software Inc., Slack, Splunk, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, Workday, Zoomが会員企業として参加しています。詳しくはウェブサイト（http://bsa.or.jp）をご覧ください。 2） https://bsa.or.jp/wp-content/uploads/20200626j.pdf また、IoT、5G、クラウドベースのサービスなどの技術を安全に導入・利用するためのハイレベルなガイドラインの策定や、テレワークの重要性を認識されていること、国際的なサイバーセキュリティ・コミュニティと緊密に連携してクラウドベースの技術活用に取り組まれていることを支持します。「自由、公正、かつ安全なサイバー空間」の実現に向けて、ICTに係るインフラやサービスのサイバーセキュリティを確保するという貴省の目標を支援するため、以下、意見を述べさせて頂きます。	本総合対策の内容に賛同の御意見として承ります。
34	BSA ザ・ソフトウェア・アライアンス	全般	上記意見が、「対策案」を最終的に確定する上で有効であれば幸いです。データ・フリー・フロー・ウィズ・トラスト（DFFT）を推進するために、貴省がサイバーセキュリティに関し、国際的なリーダーシップを発揮することを我々は支援します。また、日本のデジタルトランスフォーメーションを推進するために、貴省と協力してサイバーセキュリティを強化していくことを期待しています。本意見に関して、ご質問がある場合又はより詳細に議論をされたい場合には是非ご連絡下さい。	本総合対策の内容に賛同の御意見として承ります。
35	個人C	全般	サイバーセキュリティーを政府および各部局や民間企業で高めることに異議はない。しかし伝え聞くデジタル庁の創出を聞くが、このサイバーセキュリティ法が十分整った後の話しだろうと思える。 現在の政府行政の進め方は、プライオリティの検討不十分も甚だしく、しかも人気取り担当役員の属人的性癖もあるのだろが、やたら印鑑を廃止する等、我が国の歴史から生まれた美習といえるべきものを破壊する所業だと感じる。	御意見については、参考として承ります。
36	個人D	全般	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（NewRadio）」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ゲエッジ）」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。	御意見については、参考として承ります。