別紙１

「IoT・5G セキュリティ総合対策（案)」に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

（意見募集期間：令和元年６月 29 日～令和元年７月 18 日）

提出意見　：19 者

法人　　：６者（法人情報処理安全確保支援士会設立準備会、株式会社　LAC 、シスコシステムズ合同会社、パロアルトネットワークス（株)、一般社団法人　日本スマートフォンセキュリティ協会、華為技術日本株式会社）

個人　　：13 者（個人 A～M）

【総論】

意　見	考え方	提出意見を踏まえた案の修正の有無
意見１　目に見えない不正に対し、国の専門機関による調査を行い、結果を実名で公表して欲しい。また、法による厳しい罰則により、不正行為の抑止効果が得られるよう立法をお願いしたい。	考え方１	
○　サイバーセキュリティにおいて、ハードに起因するリスク、ソフトに起因するリスク、改ざん、不正アクセスなど様々な目に見えないリスクが存在する。悪意をもつ人、企業、組織、国などによる情報の漏えいや、インフラへの攻撃、テロなどから国民をも守るためには、目に見えない本来行われるべきではない不正に対し、国の高度な専門機関による調査を行い、結果を実名で公表して欲しい。また、法による厳しい罰則により、悪意をもつ人、企業、組織、国などどのような不正行為の実施者の場合に対しても、大きな痛みを伴うレベルの罰則を規定し厳しく運用することにより、不正行為の抑止効果が得られるよう、立法をお願いしたいと思います。 【個人 A】	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。	無
意見２　IoT・5G は軍事情報も含むと認識しているため、セキュリティを相当強化すべきである。	考え方２	
○　IoT・5G は軍事情報も含むと認識しているため、セキュリティを相当強化すべきと考える。具体的には、通信を伴う機器は日本国もしくはホワイト国に指定された国が設計・製造した機器を使う事を原則とし、対象国外で設計又は製造された機器，対象国外から輸入される機器に対しては、各輸出案件ごとの申請に加え、日本国の調査機関での分解調査を必須とすべきである。 【個人 B】	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。	無
意見３　韓国に特化したセキュリティが必要である。	考え方３	
○　韓国に特化したセキュリティ必要 【個人 C】	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。	無

意見４　今回の総合対策において取り上げた各分野について、IPA の ITSS＋のセキュリティ領域改善検討にあわせて、情報処理安全確保支援士を活用する制度設計を行い「国民の安心・安全の確保」のために有効な制度設計を行っていただきたい。	考え方４	
○　これまでは、パソコンやスマートデバイスといった「利用者の責任でセキュリティ対策を行う」ものがサイバーセキュリティの中心的な存在であったが、IoT は暮らしに溶け込む存在であり、利用者が意識することは困難である。また、それにあわせて急速に進展する５Ｇ技術によって、サイバーセキュリティ上の問題が拡散する速度そのものも劇的に向上している。これについて対策を講じることは喫緊の課題であり、今回こうして必要な対策について論じることは、国民の安心・安全を守るためにも極めて有意義であると考える。 一方、サイバーセキュリティがパソコン利用者等といった一部を対象としたものではなく、広くすべての国民の生活に影響する状況であるため、情報処理安全確保支援士の有効活用について積極的な取り組みを行うことにより、対策の有効性が増すものと考える。 Society5.0 以前の社会において重要とされてきた社会インフラについては、例えば有線通信に関する工事担任者制度や、無線通信に関する無線従事者資格制度といった「必置資格による安全の確保（=国民の安全・安心の確保)」が講じられている。これに対して Society5.0 以降の社会において重要となるサイバーセキュリティ分野に関しては、現状特に必置化措置が講じられておらず、人材の確保もなされていない。よって、時代に対応した必置化措置は、サイバーセキュリティ人材確保のための１案であり、その人材として情報処理安全確保支援士を積極活用することで、より安全・安心の確保に繋がると考える。 総務省においては、情報処理人材について「それぞれの分野における取組を通じて検討を進めていく」という段階は既に通り過ぎており、国民の安心・安全はすでに脅かされている状況であり、今回の総合対策において取り上げられた各分野について、現在ＩＰＡにおいて行われている ITSS＋のセキュリティ領域改善検討にあわせて、情報処理安全確保支援士を活用する制度設計を行っていただくことで「国民の安心・安全の確保」のために有効な制度設計を行っていただきたい。 【情報処理安全確保支援士会設立準備会】	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。	無

意見５　ＩｏＴに関しては、各地方自治体での積極的な推進や、中山間地域での携帯電話通信網の補助事業を地方自治体が行っている状況を踏まえるべき。	考え方５	
○　（Ｐ３）　ＩｏＴに関しては、各地方自治体においても積極的な推進が行われていることや、中山間地域における携帯電話通信網の補助事業についても地方自治体が行っている状況を踏まえて　「…総務省が関係各府省庁や『地方自治体』及び民間企業等と連携し」と変更することが望ましい。 【情報処理安全確保支援士会設立準備会】	御指摘の地方公共団体との連携について、以下のとおり修正させていただきます。 （Ｐ３）「…総務省が関係各府省庁や地方公共団体及び民間企業等と連携し…」 （P35）「…内閣官房内閣サイバーセキュリティセンターや経済産業省をはじめとする関係府省庁や地方公共団体及び民間企業等との連携の下に進めていく必要がある。」	有
意見６　大規模な国際イベント等の開催において、事業者任せのリスクマネジメントではセキュリティ上の問題が生じることを排除できず、単に訓練・演習の強化のみの実施では、真に有用な知識を身に着けた人材であるかどうかの担保がなされない。	考え方６	
○　（Ｐ８）　大規模な国際イベント等の開催において、事業者任せのリスクマネジメントではセキュリティ上の問題が生じることを排除できない。また、単に訓練・演習の強化のみの実施では、真に有用な知識を身に着けた人材であるかどうかの担保がなされない。そういった課題を踏まえ「…これまで実施されてきた対策の一層の強化『及び ITSS+改善検討の活用、情報処理安全確保支援士の必置化を推進すること』が求められる。」と変更することが望ましい。 【情報処理安全確保支援士会設立準備会】	大規模な国際イベント等の開催に関連した取組や、訓練・演習を通じた人材育成の取組の在り方には様々な方向性が考えられることから、御指摘いただいた点なども踏まえながら取組を進めていくことが重要と考えます。	無
意見７　地方におけるセキュリティ人材の確保やセキュリティ対策の推進が求められていることや、地方行政に対する支援も総務省に期待される役割であることを踏まえるべき。	考え方７	
○　（Ｐ９）　サイバーセキュリティの主体として、地方分権の観点からも、地方におけるセキュリティ人材の確保やセキュリティ対策の推進が求められていることや、地方行政に対する支援も総務省に期待される役割であることを踏まえて　「関係府省庁や『地方自治体』及び民間企業と連携しつつ、政策を実行的に推進していくことである。」　と変更することが望ましい。 【情報処理安全確保支援士会設立準備会】	御指摘の地方公共団体との連携について、以下のとおり修正させていただきます。 （P9）「…関係府省庁や地方公共団体及び民間企業と連携しつつ、政策を実行的に推進していくことである。」	有
意見８　意見募集期間および表記に関する意見。	考え方８	
○ ・本件の意見募集期間を３０日未満としたのは、なぜですか？ ・６ページの脚注４の１行目「独立行政法人情報処理推進機構」は「独立行政法人情報処理推進機構（IPA)」と記載し、２３ページの脚注の４行目「独立行政法人情報処理推進機構（IPA)」は「IPA」と記載したらどうか。 ・６ページの脚注４の２行目「2019 年」は、「令和元年」と「平成 31 年」のどちらにあたるのですか？	御指摘を踏まえ、以下のように修正させていただきます。 （P4）「AI 化」→「AI（人工知能）化」 （P6）脚注４　「独立行政法人情報処理推進機構」→「独立行政法人情報処理推進機構（以下「IPA」とい	有

・８ページの１０行目「大会」は「2020 東京大会」と記載したほうがよいと思います。 ・１２ページの１７行目「国立研究開発邦人情報通信研究機構法」の法律番号を記載したほうがよいと思います。 ・１４ページの２行目「ネットワークのエッジ（基地局とコア網の間に設置）で通信処理や高度な演算・データ処理がなされるモバイルエッジコンピューティング（MEC)」は「MEC」と記載したほうがよいと思います。前段の５ページで略称を定義しているから。 ・２３ページの８行目「(人工知能)」は、初出の４ページで記載したほうがよいと思います。 ・２３ページの脚注の３行目「国立研究開発法人情報通信研究機構（NICT)」は「NICT」と記載したほうがよいと思います。前段の１２ページで略称を定義しているから。 【個人 D】	う。)」 （P6）脚注 4　「2019 年」→「2019 年（令和元年）に公表されたもので」 （P8）「大会」→「2020 東京大会」 （P12）「国立研究開発法人情報通信研究機構法」→「国立研究開発法人情報通信研究機構法（平成 11 年法律第 162 号)」 （P14）「モバイルエッジコンピューティング（MEC)」→「MEC」 （P23）「AI（人工知能)」→「AI」 （P23）「国立研究開発法人情報通信研究機構（NICT)」→「NICT」 （P23）脚注 「独立行政法人情報処理推進機構（IPA)」→ 「IPA」 なお、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。	

意見９　サイバーセキュリティ技術は日進月歩であり、新たに５Ｇへの対策を包含しつつ、セキュリティ総合対策が見直されることに賛同する。	考え方９	
○　弊社はインターネット黎明期の 1995 年に情報セキュリティ事業を立ち上げて以来、情報通信技術革命の進展に合わせて巧妙化、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。サイバーセキュリティ技術は日進月歩であり、新たに５Ｇへの対策を包含しつつ、セキュリティ総合対策が見直されることに賛同すると共に、以下の分野について、更なる対策の充実が必要であると考えております。 【株式会社　LAC】	本総合対策に賛同の御意見として承ります。	無
意見 10　総務省が IoT と 5G セキュリティに関する包括的なセキュリティ対策を策定することを歓迎する。	考え方 10	
○　総務省が IoT と 5G セキュリティに関する包括的なセキュリティ対策を策定することを歓迎します。キャパシティ・ビルディング、研究開発、国際的な取り組み、脅威インテリジェンスの共有を含む、今後注力すべき一連の活動として、既存の国際基準、ガイドライン、および協働の取り組みに沿った力強いテーマを持つこの文書を評価します。 また、日本政府が、国際的なリーダーとして、最近の G20 大阪サミットの準備と開催、それに、ラグビーワールドカップや東京 2020 オリンピック・パラリンピックを含む今後 1 年余りに予定される主要イベントへの準備を進めてきた経験とともに、この文書に列挙されている取り組みの多くを主導してきたその能力にこそ力の源泉があると認識しているものと認めるところです。 【シスコシステムズ合同会社】	本総合対策に賛同の御意見として承ります。	無

【IoT のセキュリティ対策】

意見 11　機器内部でのソフトウエアの改ざんやハードウエアの保守時での機器の交換時等に意図的に仕組まれたデバイスが混入する可能性があり、外部のポートからチェックするだけでは不十分である。	考え方 11	
○　IOT 機器に関しては NICT の NOTICE が不正アクセスを受ける可能性のあるポートを有する機器を保持する所有者に関して積極的な注意喚起を行うなどを行う予定ですが、機器内部でのソフトウエアの改ざんやハードウエアの保守時での機器の交換時等に意図的に仕組まれたデバイスが混入する可能性もあり、それらを外部のポートからチェックするだけでは不十分と思われる。特にインフラ系の公共システム（キャリアの通信設備含む）はその導入時、運用時でも定期的にチェックを行うことが肝要と思われる。 【個人 E】	御指摘の点については、今後の IoT・５Ｇのセキュリティ対策の取組の参考とすることが適当と考えます。	無

意見12　IoT 機器の設置・運用・保守段階での対策に対する追記案。	考え方12	
○　② IoT 機器の設置・運用・保守段階での対策 「IoT システム・サービス全体としてのセキュリティの確保に関しては、IoT 機器だけでなく、ネットワーク側での対処の在り方についても検討が必要である。この点で、IoT 機器の不正検知等のため、IoT 機器とインターネットの境界上にセキュアゲートウェイ（IoT セキュアゲートウェイ）を設置する取組が考えられる。本取組について、Ⅲ－（４）のスマートシティのセキュリティ対策の取組等を通じ、実際の導入を進める仕組みや方策について検討することが重要である。」 ・・・・の後（１２ページ）に、次のような文章を追記したほうが、今後に向けた更なる対応策や、その具体例が想定され、より良いように思えます。 ――――――――（追記文章案）―――――――― その他、脆弱性等を有する IoT 機器を利用、または IoT システムで高い安全性が求められる場合は、サービス利用者側の IOT 機器が直接通信回線（LTE, FTTH 等）から接続/ネットワークスキャンされないような仕組みや、サービス利用者側でもセキュリティ脅威に対して検知／対処可能な方策等、検討することが適当である。 具体的には、セキュアな（例：サービス提供事業者、または通信サービス事業者が提供／運用／管理するような）ホームゲートウェイ装置をサービス利用者側に設置し、IoT 機器とサービス提供者との接続時に、その装置を介し有線回線(例：FTTH 等)でアクセスすることでファイアウォール(Firewall)として利用するだけでなく、無線利用時の運用面の課題（例：IOT 機器が移動するカーモビリティ分野は利用環境変化で通信が途絶え誤検知／検知機能低下の症状発生）も極力回避できる方策の検討、更にはホームゲートウェイ装置自体のセキュリティ強度もシステム用途／脅威レベルに合わせ自動的に高めるような、AI とデータベース等を活用した検知・解析策／運用管理策等、検討していくことが望ましい。 【個人 F】	IoT セキュアゲートウェイの具体的な在り方については、御指摘を頂いた内容も含めて今後の取組の中で検討をしていくことが適当と考えます。	無
意見13　IoT 機器の不正検知等に関して、アプリケーションの識別および制御、防御、前述情報を含んだ通信ログの取得等までを含めるべきである。	考え方13	
○　3 章（1）2 の IoT 機器の不正検知等に関する記述ですが、昨今様々なアプリケーションを利用した不正アクセス等が発生しているため、アプリケーションの識別および制御。更に防御。また、前述情報を含んだ通信ログの取得等までの記載であった方がより具体的な施策と考えます。 【パロアルトネットワークス（株）】	御指摘のアプリケーションを利用した不正アクセス等に関する対処については、IoT セキュアゲートウェイに関連する今後の取組の中で検討していくことが適当と考えます。	無

意見 14　3 章（1）4 についても検知までが記載されているが、電気通信事業者による防御まで含めるべきである。	考え方 14	
○　3 章（1）4 についても検知までが明確に記載されていますが、電気通信事業者による防御までの記載であった方が具体的な施策と考えます。 【パロアルトネットワークス（株）】	御指摘の点について、ネットワークやプラットフォーム側による防御も重要と考えられるため、以下のように修正させていただきます。 （P12）「IoT システム・サービス全体としてのセキュリティの確保に関しては、IoT 機器だけでなく、ネットワークやプラットフォーム側での対処の在り方についても検討が必要である。この点で、IoT 機器の不正検知等のため、IoT 機器とインターネットの境界上にセキュアゲートウェイ（IoT セキュアゲートウェイ）を設置・運用し、ネットワークやプラットフォーム等での防御に活用する取組が考えられる。本取組について、Ⅲ－（４）のスマートシティのセキュリティ対策の取組等を通じ、実際の導入を進める仕組みや方策について検討することが重要である。」 （P16、P22）「IoT 機器の不正検知等のため、IoT 機器とインターネットの境界上にセキュアゲートウェイ（IoT セキュアゲートウェイ）を設置し、適切に運用する取組が考えられる。」	有
意見 15　製造業者における IoT 機器のセキュリティ・バイ・デザインの考え方を十分に浸透させるとともに、対策がとられた機器の市場への展開を促進させることが重要となる。	考え方 15	
○　Ⅲ情報通信サービス・ネットワークの個別分野のセキュリティに関する具体的施策 p11　(1)IoT のセキュリティ対策　①IoT 機器の設計・製造・販売段階での対策 ・意見内容 安心･安全な IoT を普及させるには、製造業者における IoT 機器のセキュリティ・バイ・デザインの考え方を十分に浸透させるとともに、対策がとられた機器の市場への展開を促進させることが重要となることについて、同意見です。 弊協会では、IoT 機器にも多く用いられている Android os を対象にサンプルコードの紹介、その背景にあるセキュリティ観点の留意事項、さらにセキュリティの理解を深めるための解説をまとめ、開発者の実践に役立つ「Android アプリのセキュア設計・セキュアコーディングガイド」を 2012 年 6 月から取りまとめ、誰でも利用使えるよう、HP で公開	本総合対策に賛同の御意見として承ります。 御提案の内容も参考にしつつ、IoT のセキュリティ対策に取り組むことが適当と考えます。	無

しております(日本語の他、英語、中国語にも対応)。毎年 Android os の版の改正に応じて見直しも行っていますので、セキュリティ・バイ・デザインに基づく IoT 機器の設計に積極的な活用を望みます。 〈参考〉 『Android アプリのセキュア設計・セキュアコーディングガイド』 ・日本語版 https://www.jssec.org/dl/android_securecoding/ ・英語版 https://www.jssec.org/dl/android_securecoding_en/ ・簡体字版(公益財団法人電気通信普及財団の助成金により作成) https://www.jssec.org/dl/android_securecoding_cn/1_introduction.html 【一般社団法人　日本スマートフォンセキュリティ協会】		
意見 16　セキュアゲートウェイについて IoT エッジデバイスのエラー情報も SOC（セキュリティ・オペレーション・センター）に通知できるような仕組みも重要である。	考え方 16	
○　Ⅲ 情報通信サービス・ネットワークの個別分野のセキュリティに関する具体的施策 －（1）IoT のセキュリティ対策 －② IoT 機器の設置・運用・保守段階での対策 （及び参照記載のある P16、P22 の該当部分） （意見） 「IoT 機器の不正検知等のため、IoT 機器とインターネットの境界上にセキュアゲートウェイ（IoT セキュアゲートウェイ）を設置する取組が考えられる。」の部分について、「設置する」を「設置し、適切に運用する」とすべきと考えます。セキュアゲートウェイは攻撃を検知する良いセンサーにもなりえますので、ゲートウェイ本体の異常検知の通知だけでなく、IoT エッジデバイスのエラー情報も SOC（セキュリティ・オペレーション・センター）に通知できるような仕組みも重要と考えております。 【株式会社　LAC】	御指摘を踏まえ、以下のように修正させていただきます。 （P12）「IoT システム・サービス全体としてのセキュリティの確保に関しては、IoT 機器だけでなく、ネットワークやプラットフォーム側での対処の在り方についても検討が必要である。この点で、IoT 機器の不正検知等のため、IoT 機器とインターネットの境界上にセキュアゲートウェイ（IoT セキュアゲートウェイ）を設置・運用し、ネットワークやプラットフォーム等での防御に活用する取組が考えられる。本取組について、Ⅲ－（４）のスマートシティのセキュリティ対策の取組等を通じ、実際の導入を進める仕組みや方策について検討することが重要である。」 （P16、P22）「IoT 機器の不正検知等のため、IoT 機器とインターネットの境界上にセキュアゲートウェイ（IoT セキュアゲートウェイ）を設置し、適切に運用する取組が考えられる。」	有

意見 17　IoT のセキュリティ要件については、海外で見られる他の取り組みとの間で整合性を有する、と明示的に述べるべき。またブロッキングについては、悪意があるとみられる IoT の動作をブロックする際に緊急の通信がブロックされてしまった場合責任を問われる可能性があるため、通信事業者は懸念を有することになる。	考え方 17	
○　1. 文書 12 ページ: 今後の IoT 認証システムへの言及と、コンプライアンスを課す可能性を指し示す言及があります。ここでは、理想的には、米国、オーストラリア、英国、ドイツなど、IoT のベースライン セキュリティ要件を確立するために、海外で見られる他の取り組みとの間で整合性を有する、と明示的に述べることができるのではと考えます。シスコは、IoT 機器が、理想的には、攻撃されたり、攻撃の一部として使用されたりするのを検知するネットワークの機能を促進する基準の適用をサポートしなければならない場面に最低限必要な機能についてアドバイスを行うことができます。これらの機能には、一意のデバイス識別子と暗号化機能が含まれます。 2. 既に展開されている IoT 機器のセキュリティ保護について様々な言及があります。異常な振る舞いを示す IoT 機器が迅速に特定されることが確実に行われる必要があることに同意します。と考えます。シスコのエンジニアは、機器メーカーが、IoT 機器がどう動作するかを標準化した方法で宣言できる よう、IETF の標準である “MUD（Manufacturer Usage Description” (https://developer.cisco.com/site/mud/)の開発を主導してきました。これにより、ネットワークの力を活用して、機器の可視性と制御を確立し、感染を検出して悪意のある動作をブロックすることができます。 3. 感染した機器からの通信をブロックする必要性への言及もあります。これは、上記のポイント 2 のように、機器がどのように動作するかについての詳細情報がある場合、より簡単に行うことができます。ブロッキングについてありうる懸念としては、例えば米国でみられるように、悪意があるとみられる IoT の動作をブロックする際に緊急の通信がブロックされてしまった場合責任を問われる可能性があるため、通信事業者は懸念を有することになります。 また、文書には、スマートシティや公共 Wi-Fi など、シスコが知見を提供できる多くの分野が含まれており、総務省とのより深い協力に向けた意見交換を希望しています。 安全なデジタル経済の基盤のもとで、日本の国と国民、そしてパートナー企業が、経済的な潜在力を発揮できるようシスコがその一助となるうえで、日本政府との継続的なパートナーシップを希望しています。 【シスコシステムズ合同会社】	P11 にあるとおり、IoT 機器に関する基本的なセキュリティ対策については、電気通信事業法（昭和 59 年法律第 86 号）の枠組みにおいて端末設備等規則（昭和 60 年郵政省令第 31 号）を改正し、強制規格としての技術基準が既に策定されている（2019 年（平成 31 年）３月１日公布、2020（令和２年）年４月１日施行）ところです。また、IoT 機器に関するセキュリティ対策の上乗せ部分に該当する要件については、民間団体がセキュリティ要件のガイドラインを策定し、さらに当該要件に適合した IoT 機器に対して適合していることを示すマークを付す認証（Certification）制度の構築の準備を進めているものであり、あくまで任意の規格としての普及が期待されるものです。 その上で、御指摘の IoT に関する海外で見られる他の取組との整合性の点については、P29 にあるように、現状の取組としても「IoT セキュリティガイドライン」を国際標準に反映する等の取組を行っており、まずはこれらの取組を通じ、IoT のセキュリティ対策について国際的な議論との調和を図っていくことが適当と考えます。 頂いた御意見を踏まえ、引き続き、総務省においても民間企業と連携してサイバーセキュリティ政策を推進することが適当であると考えます。	無

【5G のセキュリティ対策】

意見 18　セキュリティーにおいては、機材の性能、機材のソフトウェア、人によるリスクを抑えなければならない。	考え方 18	
○　５Ｇセキュリティーに関して。 セキュリティーとは、 １機材の性能によるもの ２機材のソフトウェアによるもの ３人によるもの セキュリティーを語る上では、この３つを抑えないといけません。これは常識です。　１　２　に関しては、それぞれのプロが対策を講じるでしょうが、３によるものに関して、日本政府は全く考慮していないに等しい。 中国には、国家情報法なるものがある限り、中国国籍の中国人、その多国籍の中国人を、これにかかわらせること自体が、セキュリティーホールになります。すでに、総務省に、その中国の息のかかった人が入り込んでるようで、まったくもって信用ができない。即刻改善を。 【個人 G】	御指摘の点については、今後の 5G のセキュリティ対策の取組の参考とすることが適当と考えます。	無
意見 19　国民の健康への懸念があるため 5G 導入の中止を要望する。	考え方 19	
○　5G 導入の中止を要望します。 ベルギー・ブリュッセルにて、国民の健康が懸念されることから、導入が一時停止されています。それ以外にもアメリカ・カナダ・イタリアなどの諸外国（G20 参加国も含む）も電磁波に関する対策をしています。 それに引き換え日本は、電磁波に関する議論は一切されておらず、メディアにも取り上げられていません。 国民に知らされていないだけで、電磁波被害は数多く存在しています。 ベルギーの方の言葉を借りるなら、日本人も電磁波被害を実験するモルモットではありません。 安全だと仰るならまず第一に電磁波の存在を知らしめてから導入の議論をしていただくようお願い致します。 【個人 H】	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」として整理したものです。 なお、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、本年５月に必要な制度整備がなされたところです。 今後とも、国民の皆様への周知など必要な取組がなされることが適当と考えます。	無

意見 20　５G 機器に関して、全ての機器に対する包括的なソフトウエア、ハードウエアのチェックが不可欠と思われる。	考え方 20	
○　５G に関しては５G 機器に関しては尚のこと、昨今いろいろ言われているようなセキュリティ問題が存在しているようなので全ての機器に対する包括的なソフトウエア、ハードウエアのチェックが不可欠と思われる。それら機器をチェックする公的な組織の組成も必要で、そこでの認証、承認が得られた機器こそが各キャリアが安心して使用できるものとなる。 【個人 E】	御指摘の点については、今後の５G のセキュリティ対策の取組の参考とすることが適当と考えます。	無
意見 21　情報抜き取りチップ等、意図的な機器への仕込み排除についてもあげるべき。	考え方 21	
○　・機器の脆弱性は課題に挙げてても、情報抜き取りチップ等、意図的な機器への仕込み排除についてもあげるべき。 【個人 I】	御指摘の点については、P14 にあるとおり、機器のセキュリティについて、機器にインストールされているソフトウェアだけでなく、集積回路の設計工程においてハードウェア脆弱性が存在する可能性が指摘されていることから、ビッグデータや AI を活用しつつハードウェアに組み込まれるおそれのある脆弱性を検出する技術の研究開発等を推進することが適当と考えます。	無
意見 22　5G セキュリティを総合的かつ継続的に担保する仕組みの整備、および、重要インフラ事業者等への周知・啓発を行うことに賛同する。	考え方 22	
○　5G セキュリティを総合的かつ継続的に担保する仕組みの整備、および、重要インフラ事業者等への周知・啓発を行うことに賛同します。 欧州諸国などにおけるセキュリティ担保の仕組みを参考しつつ、さらに、連携するとすることで、効率的で速やかに IoT システムおよび 5G システムに関するサイバーセキュリティ対策の仕組みを、我が国において、設計・構築・運用することが必要かつ重要であると考えます。産官学による国内でのマルチステークホルダによる体制の確立を行い、さらに、グローバルな連携・協調を同時に進めることが重要であると考えます。特に、個別機器およびシステムのサイバーセキュリティ対策の評価(＝アセスメント)を実現する体制の構築が重要であると考えます。 【個人 J】	本総合対策に賛同の御意見として承ります。	無

意見 23　MEC の説明について、MEC の特徴は、サーバの物理的な配置場所にあることを考慮し、物理的な配置場所について言及すべき。	考え方 23	
○　5 ページ　「① 5G のサービス開始に伴う新たなリスク」への意見 脚注に「ネットワークのエッジ（基地局とコア網の間に設置）で通信処理や高度な演算・データ処理がなされること。」と MEC が説明されています。しかしながら、総務省の別資料 http://www.soumu.go.jp/main_content/000593247.pdf の 12 〈http://www.soumu.go.jp/main_content/000593247.pdf の 12〉 ページに説明されているように、MEC は「クラウド上でサービス提供を行っていたサーバをユーザの近くに配置する」と一般的に知られています。つまり、MEC の特徴は情報処理機能であるサーバの物理的な配置場所にあり、通信機能である「コア網」の後置に MEC サーバが配置されます。セキュリティの観点からは、安全なデータセンター内設置か、電柱上などの屋外設置かなど、物理的な配置場所は重要な考慮点になりますので、当該脚注は上記別資料の説明内容に合致させた方が良いと考えます。 【華為技術日本株式会社】	御指摘を踏まえ、以下のように修正させていただきます。 （P5）脚注：「ネットワークのエッジ（ユーザの近く）でなされる通信処理や高度な演算・データ処理。」	有
意見 24　5G セキュリティを総合的かつ継続的に担保する仕組みの整備、および、重要インフラ事業者等への周知・啓発を行うことに賛同する。「5G」という言葉が通信インフラを意味するのか、アプリケーション・情報処理も含めたサービス全体を意味するのかが不明確である。さらに、「ネットワークインフラ」の定義の明確化が必要である。	考え方 24	
○　13 ページ　「(2)5G のセキュリティ対策」への意見 5G セキュリティを総合的かつ継続的に担保する仕組みの整備、および、重要インフラ事業者等への周知・啓発を行うことに賛同します。 既に欧州諸国では同様のセキュリティ担保の仕組みがあります。それらを参考とすることで、効率的に国際協調のとれた 5G セキュリティ対策の仕組みを日本に構築できると考えます。弊社は、欧州諸国におけるセキュリティ対策構築に深く関わってきており、情報提供等で日本の取り組みの一助になればと考えています。 なお、文中に、「ネットワークインフラとしての機能維持のためには、基地局やコア網のみならず、MEC も含めた各構成要素（デバイス、クラウド、アプリケーション等）全体を考慮したセキュリティの確保が必要不可欠である。」とあります。この文章からは、「ネットワークインフラ」が通信機能だけではなくクラウドやアプリケーションなどの情報処理機能もその構成要素として含むように読めます。これは「5G の各構成要素におけるソフトウェアを含むセキュリティを総合的かつ継続的に担保する仕組みを整備し」という文章でも同様であり、「5G」という言葉が通信インフラを意味するのか、アプリケーション・情報処理も含めたサービス全体を意味するのかが不明確です。 9 ページにも記載されているように「アプリケーション層、	本総合対策に賛同の御意見として承ります。 なお、御指摘の「ネットワークインフラ」については、基本的にはネットワーク層を指す概念として認識しております。また、「5G」については、ネットワーク層、機器層を指す概念として認識しております。御指摘を踏まえ、以下のように修正させていただきます。 （P14）「…5G を利用したシステム全体の各構成要素におけるソフトウェアを含むセキュリティを総合的かつ継続的に担保する仕組みを整備し…」 また、用語の統一性を確保する観点から、本総合対策の前に策定・公表された「IoT セキュリティ総合対策」と表現ぶりを合わせ、以下のように	有

プラットフォーム層、ネットワーク層、端末層と分類が可能であるが、それぞれの層において留意すべき脅威とセキュリティ要件の在り方について検討する必要」があるため、「ネットワークインフラ」の定義の明確化が必要と考えます。 【華為技術日本株式会社】	修正させていただきます。 （P9）「…サービス（データ流通）層、プラットフォーム層、ネットワーク層、機器層と分類が可能であるが、それぞれの層において留意すべき脅威とセキュリティ要件の在り方について検討する必要…」	
意見 25　安価に脆弱性を発見する技術が重要であり、ハードウェア脆弱性に対する対策を引き続き研究開発することが必要である。	考え方 25	
○　Ⅲ 情報通信サービス・ネットワークの個別分野のセキュリティに関する具体的施策 － (2) 5G のセキュリティ対策 － ② ハードウェア脆弱性への対応 （及び再掲されている P19 の関連部分） （意見） 高速・低遅延な５Ｇの普及に伴い、多種多様な機器がネットワークに接続されることが想定されますが、これら機器のセキュリティについては、大量生産を前提としたハードウェアによる実装となることが考えられます。この場合、製造者以外による脆弱性の発見は、例えば電子顕微鏡による回路の把握が必要等、高額かつ困難となります。このため、安価に脆弱性を発見する技術が重要であり、ハードウェア脆弱性に対する対策を引き続き研究開発することが必要と考えます。 【株式会社　LAC】	本総合対策に賛同の御意見として承ります。	無
意見 26　5G セキュリティを総合的かつ継続的に担保する仕組みの整備、および、重要インフラ事業者等への周知・啓発を行うことに賛同する。	考え方 26	
○　5G セキュリティを総合的かつ継続的に担保する仕組みの整備、および、重要インフラ事業者等への周知・啓発を行うことに賛同します。グローバルな視点が必要な通信の特性を鑑みて、日本が独自にセキュリティを担保するシステムとはせずに欧米先進各国との協調や共有を重視した取り組みをおこなうべきです。 【個人 K】	本総合対策に賛同の御意見として承ります。	無

【トラストサービスの在り方の検討】

意見 27　トラストサービスについて、目的外利用を検知阻止する仕組みやデータの廃棄を証明する仕組みついても検討が必要である。	考え方 27	
○　（Ｐ１７） トラストサービスについて、目的外利用を検知阻止する仕組みやデータの廃棄を証明する仕組みついても検討が必要であると考える。よって 「６）データ送達後の目的外利用検知阻止やデータ破棄を証明する仕組み」 を追加することが望ましい。 【情報処理安全確保支援士会設立準備会】	御指摘の点については、将来的な課題として、今後のトラストサービスの検討の在り方の取組の参考とすることが適当と考えます。	無

【クラウドサービスのセキュリティ対策】

意見 28　クラウド利用における記載では、クラウドサービスの継続利用に基づき、安全評価においてもリアルタイムで継続的に実施されるべきであると考える。	考え方 28	
○　3 章（3）のクラウド利用における記載では、クラウドサービスの継続利用に基づき、安全評価においてもリアルタイムで継続的に実施されるべきであると考えます。 【パロアルトネットワークス（株)】	御指摘の点については、今後のクラウドサービスのセキュリティ対策の取組において参考とすることが適当と考えます。	無

【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】

意見 29　情報通信ネットワーク・安全信頼性基準等の見直しについては、電気通信事業者でサイバー攻撃と判断した場合において、C&C 通信等の不正な通信の遮断までを検討していただきたい。	考え方 29	
○　3 章（7）情報通信ネットワーク・安全信頼性基準等の見直しについては、電気通信事業者において、一定条件下において合法的に取得したトラフィック分析においてサイバー攻撃と判断した場合において C&C 通信等の不正な通信の遮断までを検討していただきたいと考えます。 【パロアルトネットワークス（株)】	これまで総務省において数次にわたり、巧妙化・複雑化するサイバー攻撃に対して電気通信事業者が適正な対処を講ずることが出来るよう検討を行うことを目的として「電気通信事業におけるサイバー攻撃への適正な対処のあり方に関する研究会」を開催し、電気通信事業者が通信の秘密等に配慮した適切な対応を行うことが可能となるよう、法的な整理について検討をしてきたところです。同研究会第二次取りまとめ（平成 27 年９月）において、C&C サーバ等との通信の遮断に関する有効な同意についての考え方が整理されています。	無

【地域の情報通信サービスのセキュリティの確保】

意見 30　そもそもサイバーセキュリティ人材がいなければ、連絡体制内の質を確保することができず、十分なセキュリティ対策を講じることは不可能である。	考え方 30	
○　（Ｐ１８） （８）地域の情報通信サービスのセキュリティの確保 地域においてサイバーセキュリティに関する情報格差が存在することを是正するためには、地域の事業者のサイバーセキュリティ対策の質の向上に向けた連絡体制を構築することも有益ではあると考えるが、そもそもサイバーセキュリティ人材がいなければ、連絡体制内の質を確保することができず、十分なセキュリティ対策を講じることは不可能である。よって、 「そのため、『情報処理安全確保支援士を中心とした、組織内 CSIRT を構築するなどし、業界団体やセキュリティ関連機関等と連携しつつ、』地域の事業者の…」 と変更することが望ましい。 【情報処理安全確保支援士会設立準備会】	地域の情報通信サービスのセキュリティの確保に関しては、御指摘いただいた点なども踏まえながら取組を進めていくことが適当と考えます。	無

【人材育成・普及啓発の推進】

意見 31　人材不足の対応の方法として、SIEM、SOAR 等のツールを利活用した動的な対応や中小企業、一般ユーザが少ない負担で適用できるシェアリング型のセキュリティ基盤、サービス等を政府、自治体および電気通信事業者にて検討をいただきたい。	考え方 31	
○　4 章（2）人材不足の対応の方法として SIEM（Security Information and Event Management）、SOAR（Security Orchestration, Automation and Response）等のツールを利活用した動的な対応や中小企業、一般ユーザが少ない負担で適用できるシェアリング型のセキュリティ基盤、サービス等を政府、自治体および電気通信事業者にて検討をいただきたいと考えます。 【パロアルトネットワークス（株）】	御指摘の点については、今後の人材育成・普及啓発の推進の取組において参考とすることが適当と考えます。	無
意見 32　サイバーセキュリティに関する人材育成は、ＩＰＡの情報処理安全確保支援士制度を中心としたものに統合すべきである。	考え方 32	
○　（Ｐ９） サイバーセキュリティに関する人材育成は、全体意見に記載したとおりＩＰＡの情報処理安全確保支援士制度を中心としたものに統合すべきである。よって「３　時間軸を意識した施策展開」について「ＩｏＴ機器のライフサイクル、『情報処理安全確保支援士等、サイバーセキュリティに関する有資格者の活用を軸とした』人材育成のスパンなど」 と変更することが望ましい。 【情報処理安全確保支援士会設立準備会】	御指摘の人材育成の点については、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必要であると考えます。	無

意見 33　地域のセキュリティ人材育成について､記載されている対策が必要であることについて強く同意する。ただし、地域でのセキュリティ人材のシェアリング についてはＩＰＡと連携して行うべきである。	考え方 33	
○　４　地域のセキュリティ人材育成 記載されている課題について、総務省の認識は非常に適切なものであり、課題に対する対策が必要であることについて、本会も強く同意している。しかし、それに対する施策の一部については、国民の安心・安全といった観点からいくつかの課題を指摘するとともに、本会から提言を行いたい。なお、これらの取組については、IoT 及び 5G の展開速度からも「今後の取り組みを通じて検証する段階」ではなく、確かな施策として直ちに実施する必要がると考えている。こういった観点から ２）地域でのセキュリティ人材のシェアリング サイバーセキュリティの専門家に関する得意分野や知識レベルで細分化したデータベースは既にＩＰＡが提供しており、更に総務省が類似のサービスを提供することは利用者に無用の混乱を与えることから、この取り組みについてはＩＰＡと連携して行うべきである。よって 「…細分化してデータベース化した上で､『IPA が提供する情報処理安全確保支援士検索サービスも活用し､』必要とする中小企業等」と変更することが望ましい。 【情報処理安全確保支援士会設立準備会】	御指摘の人材育成の点については、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。	無
意見 34　地域における人材エコシステムの形成について、高等教育機関と連携することが望ましい。	考え方 34	
○　（Ｐ２７－２８） ３）地域における人材エコシステムの形成 具体的に、高度なセキュリティ人材に関して明確な目標設定がされていないことから 「高等教育機関と連携することにより､『情報処理安全確保支援士などの』高度なセキュリティ人材の輩出」 と変更することが望ましい。 【情報処理安全確保支援士会設立準備会】	地域における人材エコシステムの形成に関しては、御指摘いただいた点なども踏まえながら取組を進めていくことが重要と考えます。	無
意見 35　通信も含む ICT 系(情報通信系)と OT 系の両方の視点が持てる人材が育成できるよう両者のコラボレーションが非常に重要である。	考え方 35	
○　P26 (2)人材育成･普及啓発の推進　④地域のセキュリティ人材育成　1)研修機会の不足 P27 同　1)地域のセキュリティリーダーの育成（地域の多様なステークホルダーについて） ・意見内容 今回の案のとおり、地方においてサイバーセキティに関して学ぶ機会は少なく、弊協会においても、活動を通じてご縁があった中部の愛知や岐阜から、セミナーなどの開催は少ない、IoT セキュリティのことを聞く相手もいない、といった意見を承っております。 また、地域の多様なステークホルダーを巻き込むためのノウハウも盛り込むことが必要ということについても同意見です。特に、p5　23 行目にあるように「IT 系(情報系)だけでなく、OT 系(制御系)のシステムのセキュリティ対策も今後一層重要になる」とあるよう、通信も含む ICT 系(情報通信系)と OT 系の両方の視点が持てる人材が育成できるよう両者のコラボレーションが非常に重要なると考えます。	御指摘いただいた内容を踏まえつつ、今後も ICT 系、OT 系人材等の相互理解の醸成に取り組んでいくことが適当と考えます。	無

そのためには、まずは、セキュリティ啓発が必要で、OT 系の技術者の多くが持つ「今まで閉じた世界を前提に考える文化」に対して、ICT 系技術者が持つ「Io 時代にはどこかで繋がっている前提と考える文化」を啓発していくことが必須です（セキュリティ文化の形成）。 そこで、JSSEC では、一般企業が IoT を導入する時に検討すべき事項を、誰もが容易に網羅的に俯瞰できるようにし、検討した経緯が見える化でき、ICT 側、OT 側、さらには構築ベンダー側の担当者が共通認識を持てるように「IoT セキュリティチェックシート」を作成いたしました。ICT・OT を理解する新たな人材の育成に、この「IoT セキュリティチェックシート」が大きく貢献するものと考えており、p27 の 18 行目の下に以下のような記述を追加することが適当と考えます。 「また、OT 系のシステムのセキュリティ対策の重要性を鑑み、民間団体等におけるサイバーセキュリティの啓発と、ICT 系人材と OT 系人材が相互協力できる機会の創設が期待される。」 〈参考〉 IoT セキュリティチェックシート https://www.jssec.org/iot 【一般社団法人　日本スマートフォンセキュリティ協会】		

【国際連携の推進】

意見 36　誰が攻撃してくるのか十分想定してから対策を考えるべきではないか。	考え方 36	
○　・仮想敵国(攻撃者)が誰かという視点が欠けているために、国際連携の推進なんかも謳われています。誰が攻撃してくるのか十分想定してから対策を考えるべきでは？ 【個人 I】	御指摘の点については、今後の国際連携の推進の取組の参考とすることが適当と考えます。	無
意見 37　IoT 機器のエラーログ等の運用面についても国際標準化が必要と考える。	考え方 37	
○　「IoT セキュリティガイドラインを国際標準に反映する等の取り組み」の部分について、「IoT セキュリティガイドライン」を「IoT セキュリティガイドラインや IoT 機器のエラーログ等の運用面」とすべきと考えます。IoT 機器のエラーログ等のセキュリティに関する運用周りを標準化しない場合、コストが指数関数的に増大することから、その国際標準化が必要と考えております。 【株式会社　LAC】	御指摘の点も踏まえつつ、国際連携の推進の取組を進めていくことが適当と考えます。	無

【その他】

意見 38　日本の侵略を狙っている国を関わらせてはいけない。	考え方 38	
○　とにかく、これだけは。中国や韓国等、反日教育を行なっている国、日本の侵略を狙っている国を関わらせてはいけない。 【個人 L】	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。	無
意見 39　官公庁の職員の約 30 パーセントを解雇すれば日本は良く成る。	考え方 39	
○　「総務省サイバーセキュリティ統括官室」が提唱している内容では、サイバーセキュリティー対策では、「国家主権（官公庁)」の職員の約 30 パーセンを「リストラ（整理解雇)」し、「リストラ（整理解雇)」した「国家主権（官公庁)」の職員を、「ホームレス（路上生活者)」に促せば、高度化が図れる構造と、私は考えます、例えばですが、「国家主権（官公庁)」の職員は、「ルーチンワーカー（単純労働者)」の「事務系（クラーク及びビロー)」と思いますので、「国家主権（官公庁)」の職員の「事務系（クラーク及びビロー)」を廃止し、「高度専門性（エキスパート)」及び「専門性（スペシャリスト)」を導入すれば、「解決（ソリューション)」する事と、私は考えます。具体的には、「方法論（メソッド)」では、量子コンピューターが高度化すると、IoT 機器に接続された「5G（第 5 世代)」が導入される事により、「人工知能（AI)」における「AI 量子コンピューター」のサイバーセキュリティー対策でのセキュリティー人材が必要と、私は思います。要約すると、低レベルな「国家主権（官公庁)」の職員の約 30 パーセントを「リストラ（整理解雇)」し、「路上生活者（ホームレス)」に促せば、日本は良く成ると、私は考えます。サイバーセキュリティー対策におけるセキュリティー人材を、日本国で、育成する事は、財政コストが無駄なので、「外国人高度人材（高度外国人人材)」における「大学院修士号及びそれと同等の経歴を持つ者（マスター以上)」を導入すれば、「解決（ソリューション)」する事と、私は考えます。要するに、私から見れば、低レベルな総務省も、他人事では無く、総務省の職員の約 30 パーセントを「リストラ（整理解雇)」し、「ホームレス（路上生活者)」に促す事で、日本国は良く成る構造と、私は考えます。 【個人 M】	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。	無