「ICTサイバーセキュリティ政策の中期重点方針」（案）に対して提出された意見及び
その意見に対するICTサイバーセキュリティ政策分科会の考え方

■意見募集期間　：　令和6年7月2日（火）～同年7月19日（金）

■意見提出件数　：　17件（法人・団体：4件、個人：13件）

■意見提出者

	意見提出者
1	株式会社ラック
2	一般社団法人日本スマートフォンセキュリティ協会
3	ニューリジェンセキュリティ株式会社
4	楽天モバイル株式会社
ー	個人（13件）

※頂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

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	個人	1章 1	・該当箇所 冊子4頁 第１章 サイバーセキュリティを巡る情勢と対応の方向性 １．サイバーセキュリティを巡る情勢 ・意見 「Society5.0」という語が出てきているが、その言葉は一般社会において一般的な語ではない。 日本政府はその言葉を使いたいようであるが、都度、（脚注等で）説明を行うようにされたい。 （その方が振り返り等を行う際も有用であるはずであろう。）	御意見については、参考として承ります。
2	個人	1章 1-(1)-イ	・該当箇所 冊子6頁 第１章 サイバーセキュリティを巡る情勢と対応の方向性 １．サイバーセキュリティを巡る情勢 （１）サイバー攻撃の最近の動向 イ その他のサイバー攻撃の状況 ・意見 「VPN機器」という記述があるが、「VPN機器」が指す対象はどうも自明性に欠けるように思われる。 登録通信事業者が各一般家庭や事業者事務所に設置するような光ファイバー関係機器、またケーブルテレビ等における同様の機器等についてもVPN機器というような名称を用いているのかどうか、そういう所が気になるのであるが（それらについての範囲も気になる。ONUは入るのか、HGWも含むのか、そういう境界についてもはっきり認識しておきたいものである。加えて言うと、仮想化されたソフトウェア的なものについてはどうであるのか、などの疑問もある。）、そのような疑念が技術的知見のある者等からすると生じうるのではないかというような可能性がありうるような場合においては（あるはずと考える。）、その指し示すものについて、脚注等で提示を行って、記述する内容についての正確さ・適切さを確保するようにしていただきたい。	御意見については、参考として承ります。
3	個人	2章 1	交通、上下水道、エネルギー関係は重要なインフラですが、なぜここでは重要インフラとして記載がないのでしょうか？	はじめに（p1）に示したとおり、本重点方針（案）は、 ・重要インフラ分野におけるサイバーセキュリティ対策強化 ・サイバーセキュリティの基盤となる人材育成及び研究開発 ・サイバーセキュリティの確保に向けた国際連携及び普及啓発 に関し、総務省が今後中長期的に取り組むべきサイバーセキュリティ施策の方向性について取りまとめたものです。 そのため、本重点方針（案）においては、総務省の所管する通信、放送、自治体、データ流通基盤について取りまとめることとし、総務省の所管でない交通、上下水道、エネルギー関係については取りまとめの対象外としております。
4	個人	2章 1-(3)	第２章 ＩＣＴサイバーセキュリティ政策の中期重点方針の（３）自治体に関し、 減少傾向（１９９４年に３３０万人いた自治体の職員は２０２３年に２８０万人にまで減少）にある自治体職員に新たな役割を追加することは行政運営の崩壊を招く恐れがある。 また災害やその他公共サービスの維持が優先されることから、新たなスキルや知識の習得にも大きな課題があると思われる。 その解決策として、各自治体においてセキュリティ人材の人件費を計画し、即戦力となりうる外部人材を積極的に採用（常勤／非常勤）を行い、民間技術者の活用したICTサイバーセキュリティの推進が有効と考えられる。 各人材の得意な領域を担うことでの官民連携したセキュリティ対策の実行こそ、国が行うICTサイバーセキュリティの根幹と思われます。 また、採用対象となる人材はセキュリティクリアランス等、十分な人物評価を行うことが求められると考えられる。	御意見については、参考として承ります。
5	ニューリジェンセキュリティ株式会社	2章 1-(4)	p32 ーーー引用ーーー さらに、クラウドボットネットを利用したサイバー攻撃の増加等、クラウドサービスを取り巻く国内外のセキュリティの最新動向の把握に継続して取り組み必要に応じて対策を講じていくことが求められる。 ーーー意見ーーー クラウドボットネットについては、昨今様々なクラウドサービスからの攻撃を実際に検知しています。クラウド基盤を活用することからIPレンジによる制御が効きにく、また攻撃者によるIPアドレスの変更が容易なため、防御が困難です。 クラウド事業者による悪性ボット作成者に対する対処を求めたいと考えます。 また、クラウドストレージサービスに配置したファイルをC&Cとするマルウェアも存在するため、これらの検知と対応をクラウドサービス事業者と取り組む必要もあると考えます。	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
6	個人	全体	５ページの１行「当たり」と、同１３行「あたり」とは、どちらかに字句を統一したほうがよい。	御指摘を踏まえ、「当たり」に統一いたしました。
7	個人	全体	本件の「意見提出が30日未満の場合その理由」は何ですか？	行政手続法上、同法第39条第１項の規定により「命令等制定機関」が「命令等を定めようとする場合」に、「意見の提出のための期間」を定めて意見の公募を行わなければならないとされており、同条第３項の規定により、「第一項の規定により定める意見提出期間」は、「公示の日から起算して三十日以上」でなければならないとされております。 今回意見募集の対象とされている「ICTサイバーセキュリティ政策の中期重点方針」（案）は同法第２条第８号規定の「命令等」に該当せず、本パブリックコメントは、同法第39条第１項の適用を受けて行うものではないため、意見提出期間を30日以上と規定する同条第３項が適用されないため、30日以上としておりません。
8	個人	全体	１１ページの１８行「更に」と、１２ページの３行「さらに」とは、どちらかに字句を統一したほうがよい。	「新しい「公用文作成の要領」に向けて（報告）」（令和３年３月12日文化審議会国語分科会公表）に基づき、接続詞の「さらに」は仮名書きに、副詞の「更に」は漢字に、それぞれ記載を統一しております。
9	個人	全体	３ページの最下行の３行上「とりまとめ」と、５２ページの５行「取りまとめ」とは、どちらかに字句を統一したほうがよい。	御指摘を踏まえ、「取りまとめ」に統一いたしました。
10	個人	全体	１０ページの５行「ハマス等」は「ハマス」の誤記ではないか？	御指摘を踏まえ、「ハマス」に修正いたしました。
11	株式会社ラック	全体	御省が昨年8月に「ITCサイバーセキュリティ総合対策2023」を取りまとめられ、弊社としても、その後の動きを注視しておりました。 本年2月より、ICT サイバーセキュリティ政策分科会を開催され、サイバー攻撃の巧妙化・深刻化や厳しさを増す安全保障情勢、生成 AI 等の新たな技術・サービスの急速な普及、サプライチェーンの多様化・複雑化などの動向を踏まえ、御省が新たに「中長期的に取り組むべきサイバーセキュリティ施策の中期重点方針」を示されたことは、誠に時期を得たものであり、報告内容につきまして、賛同致します。 今後も弊社は、同方針を踏まえつつ、ASEAN諸国との連携をはじめ、ITとサイバーセキュリティの力で、社会的課題に立ち向かい、国の発展を支え、人々の暮らしを守ってまいります	賛同の御意見として承ります。
12	個人	全体	案P5において「Web カメラ」との記載があるが、2023 年の「情報通信ネットワークにおけるサイバーセキュリティ対策分科会とりまとめ」では同趣旨と思われる文脈で「ネットワークカメラ」として記載されている 用語を統一するか使い分けについてお示しいただきたい	御指摘を踏まえ、「ネットワークカメラ」に修正いたしました。
13	一般社団法人日本スマートフォンセキュリティ協会	全体	一般社団法人日本スマートフォンセキュリティ協会(JSSEC、会長　佐々木 良一)より、意見提出させていただきます。 複雑かつ巧妙化が進むサイバー攻撃や厳しさを増す安全保障情勢、生成AIの急速な普及などを踏まえ、サイバーセキュリティ分野における今後取り組むべき方向性について「ICT サイバーセキュリティ政策の中期重点方針」として取りまとめたことにより、関係機関や民間企業等が連携し、我が国のサイバーセキュリティの維持向上に具体的に取り組めるものと認識しております。 JSSECでは、サイバーフィジカルの融合が進んでいく中、人とサイバー空間の橋渡しとなるスマートフォンについて、セキュリティの重要性に関して普及・啓発を行っております。 利用シーンに潜む脅威とその対策、アプリ開発に関する実施規範や安全なコーディングのためのガイド等の各種成果物を活用し、P24「・スマートフォンアプリのセキュリティ対策の推進」、P25「・ネットワークセキュリティ認証技術の導入促進」に具体的に貢献していく所存です。	賛同の御意見として承ります。
14	ニューリジェンセキュリティ株式会社	全体	ニューリジェンセキュリティ株式会社はクラウドセキュリティサービスの提供を通じて、生活の中で高い重要度を占めるデジタルサービスの安全を守り、安心してデジタルテクノロジーを活用できる社会の実現に取り組んでいます。 この度取りまとめいただいた「ICT サイバーセキュリティ政策の中期重点方針」により、官民の連携が求められるセキュリティを推進するための基盤になるものと考え賛同致します。	賛同の御意見として承ります。
15	楽天モバイル株式会社	全体	本報告書（案）P35「２．サイバー攻撃対処能力の向上と新技術への対応」の「（１）我が国のサイバー攻撃対処能力の向上」２段落目の５行目に誤記があるよう見受けられますので、当該箇所について次のように修正をお願いいたします。 「環境構築には高度な技術力と相応の費用を要するに加え、ことから、民間企業・教育機関等のみでは十分に対応できないため」（※「、ことから」の削除）	御指摘を踏まえ、「、ことから」を削除いたしました。

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	楽天モバイル株式会社	全体	「生成AIをはじめとするAI技術の急速な普及に伴い、サイバーセキュリティ分野においても、AIを起因とした新たなリスク（AIの脆弱性を狙ったサイバー攻撃、AIの不適切な利用によるセキュリティリスクやAIを悪用したサイバー攻撃等）が指摘されている」（P42）と記載あるところ、当社はこの現状を深刻に受けとめております。AIに起因するセキュリティリスクを可能な限り回避・低減するため、「今後の取組の方向性」に記載あるとおり、「Security for AI」および「AI for Security」の取組が必要であるとの方向性に賛同いたします。 AIに起因する新たなセキュリティリスクに対処するため、当社においては、最新の動向を継続的に把握し、関係機関と連携して多層防御等の対策を講じることが重要であるとの認識の下、業界全体のセキュリティレベル向上に寄与すべく、継続的に把握している海外を含めた最新のAI技術動向に関する知見について、当社が所属するサイバーセキュリティ関連の業界団体に積極的に共有しております。 また、「『AIセキュリティ情報発信ポータル』の更新等を通じて、AIセキュリティに関する情報の的確かつ分かりやすい発信に取り組むことが必要である」（同）と記載あるところ、当社では、「利用者」である一般のお客様に安全にサービスをご利用いただけるよう、情報セキュリティに関する啓発活動の一環として、当社のWebサイト上に情報セキュリティポータルを開設して情報提供しております。 (参考: https://network.mobile.rakuten.co.jp/guide/security/) 今後当該ポータルにAIセキュリティに関する情報等を追加掲載していくことで、一般のお客様へ最新のAIセキュリティに関する情報をお届けし、より安全にサービスをご利用いただけるよう努めてまいります。	賛同の御意見として承ります。
17	個人	その他	昨今、日本のITを牽引するような企業ですら、サイバー攻撃の被害に遭っている。生成AIの普及により、こういった被害はどんどん拡大していくだろう。日本政府として、一流のホワイトハッカーなどの人材を役所に入れないといけないと思う。これまでのような、年功序列の報酬体系ではなく、一流の人材に見合った特別な待遇を用意すべきである。	御意見については、参考として承ります。
18	個人	その他	政府、企業、個人がサイバー攻撃に遭い金銭を要求される、個人情報が流出する等の被害があってはならないのでサイバーセキュリティ強化を早急にやるべき 年間報酬1000万円？2000万円などの高額報酬を渡してホワイトハッカーを雇うべき 義務教育でホワイトハッカー育成もやるべき	御意見については、参考として承ります。
19	個人	その他	サイバーセキュリティを疎かにするのは日本の国益や安全を損なうので徹底的に強化すべき 企業内部に入り込みウイルスを仕込んだりする者(産業スパイ)等を法律で罰せられる様にすべきなのと、そういった輩を企業内部に入れないよう対策すべき	御意見については、参考として承ります。