資料45－1

「ICTサイバーセキュリティ総合対策2023」（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）

■意見募集期間　：　令和5年7月7日（金）～同年7月26日（水）

■意見提出件数　：　17件（法人・団体：12件、個人：5件）

■意見提出者

	意見提出者
1	渋谷区
2	株式会社帝国データバンク
3	IssueHunt株式会社
4	楽天モバイル株式会社
5	一般社団法人デジタルトラスト協議会
6	セイコーソリューションズ株式会社
7	ソフトバンク株式会社
8	一般社団法人日本スマートフォンセキュリティ協会
9	MOTEX株式会社
10	日本電気株式会社
11	一般社団法人デジタルライフ推進協会
12	株式会社ラック
―	個人（5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（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	MOTEX株式会社	Ⅰ-2	「我が国全体として、地域や業種、事業規模を問わず、サイバー攻撃のリスクは引き続き高い状況にあると言える。」として、その事例が前段に掲載されておりますが、重要インフラを対象とした重大事案として「名古屋港（NUTS）のランサムウェア被害（2023年7月）」を追加してみてはいかがでしょうか。	御指摘を踏まえ、Ｐ9に追記をいたします。
2	個人C	Ⅰ-2	P7　一番上のグラフにおいて、「増加傾向」と記載されているが、2015年から2020年までは増加傾向であるが、それ以降は増加ではなく、平坦のように見える。増加傾向と示して重要である点を強調することは理解できなくはないですが、2020年から2022年までの傾向とその要因は適切に分析されるべきではないかとも思います。2020年の状況のみグラフ下に注記がされていることは認識していますが。 P7 下のグラフ 「令和4年におけるサイバー空間をめぐる脅威の情報等について」と記載されていますが「情報」は「情勢」の誤植かと思われます。次のグラフも同様。 P8 上のグラフ　有効回答が102件であり、2022年の被害は前のグラフから230件(114件＋116件)である。このため、有効回答が得られなかった件数が約半数の128件である。この128件も課題にすべきではないかと思います。(1)原因が不明がある。(2)原因を報告しない。(されない)点。前者は原因が明確になる対策が必要になるし、後者が適切な報告のルールとその制度が求められる。	Ｐ７下の図表の出典に関する御指摘について、貴見のとおり修正いたします。 他２点については、参考として承ります。
3	一般社団法人デジタルライフ推進協会	Ⅱ-1	一般社団法人デジタルライフ推進協会(DLPA)は利用者の利便性を守り、デジタルライフの健全な発展を推進する団体であり、主要家庭用ネットワーク機器メーカーが加盟し、ホームルーター等のセキュリティ向上を通して、安心安全な国内のホームネットワーク環境の提供を推進しております。 今回のICTサイバーセキュリティ総合対策2023の取りまとめについて、全面的な賛同の意を示したいと考えております。 当協会は「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」において報告させていただいた通り、DLPA推奨Wi-Fiルーターによるセキュリティ健全性の取り組みを進めており、JPCERT/CC様との連携と共に、NOTICEの整備・発展はこれらの取り組みを更に推進する上で、非常に重要な要素・情報になり得ると考えております。 p12における③メーカーやSIer等の幅広い関係者との連携による総合的な対処での取り組みの一環として、効率的・効果的かつ迅速な相互の技術的情報交換を目的としたNOTICEステアリングコミッティとの対話を要望・推進させていただくことで、国内ホームネットワーク環境の発展に寄与していきたいと考えております。	賛同の御意見として承ります。
4	株式会社ラック	Ⅱ-1-(1) その他関連項目	＜意見＞ IoTの真正性確保に関する技術開発・サービス開発の推進に関する取組の必要性について触れていただければと考えます。 ＜理由＞ 証明書が利用できる極一部のIoT機器を除き、大半のIoTは真正保証（身元保証）がなされておりません。よって、不正機器あるいは機器の不正操作の温床になるリスクがあると考えているためです。	御指摘の箇所については、「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」とりまとめに基づいて記述したものです。御意見については、参考として承ります。
5	一般社団法人日本スマートフォンセキュリティ協会	Ⅱ-1-(1) Ⅱ-1-(2)-イ Ⅱ-4-(1)-ア	複雑かつ巧妙化が進むサイバー攻撃や脆弱性に関する最新の動向などを踏まえ、今後取り組むべきサイバーセキュリティ分野の施策について「ICTサイバーセキュリティ総合対策2023」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指針にな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。 各種成果物を活用し、総合政策2023（案）の以下の部分の推進に具体的に貢献していく所存です。 P12 ②利用者への注意喚起等の実効性向上 ③メーカーやSIer等の幅広い関係者との連携による総合的な対処 →スマートフォン利用シーンに潜む脅威 Top10 2023*3による注意喚起を促進するとともに、IoTセキュリティチェックシート*1、スマートフォン利用ガイドライン対策チェックシートⅡ*2等によりIoTの利用における関係者の連携を促進。 P16 （情報通信分野におけるSBOM導入の可能性の検討等） →セキュアコーディングガイド*4によるセキュアなアプリ開発を促進するとともに、モバイルアプリケーション開発10大チェックポイント*5により注意喚起を促し、今後、より安全な開発環境の実現に向けたアプリ開発ガイド(新)*6等を検討。 P45 【今後の取組】テレワークセキュリティガイドライン及びチェックリスト（設定解説資料を含む。）について、～(中略)～一層広く周知していく必要がある。 →スマートフォン利用ガイドライン及び対策チェックシートⅡ*2、スマートフォン利用シーンに潜む脅威Top10 2023*3については、テレワーク時にも活用できる項目があることからこれらを使って周知を促進。	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
			P51 ウ. こどもや高齢者等に向けた普及啓発 【今後の取組】 具体的には、こども向けの「e-ネットキャラバン」、高齢者向けの「デジタル活用支援推進事業」の実施において、～(中略)～サイバーセキュリティに関する講座の利活用に向けて検討することが適当である。 →こども向けには、セキュリティかるた*7を積極的に活用。IoTセキュリティチェックシート*1、スマートフォン利用ガイドライン及び対策チェックシートⅡ*2、スマートフォン利用シーンに潜む脅威 Top10 2023*3については、解説動画も作成しているころから高齢者を含む幅広い年齢層に向けたセキュリティの啓発に貢献。 成果物の概要 *1：IoTセキュリティチェックシート 一般企業がIoTを利用（導入）する際、セキュリティ面で考慮すべきことを網羅的にまとめたチェックシート。IoT導入のカギとなる「IT：情報システム系」と「OT:設備システム系」のコラボレーションを促進。 https://www.jssec.org/iot *2：スマートフォン利用ガイドライン及び対策チェックシートⅡ 「スマートフォン＆タブレット（以下スマートフォン）の業務利用に関するセキュリティガイドライン【 第二版 】」を 2014 年 3 月に発行。昨今の社会情勢や、NIST CSFを取り込み、初見でもすぐ理解できるよう「特性別／利用シーン別対策チェックシートⅡ」を2021年に策定。 https://www.jssec.org/dl/guidelines_checkSheet2_v1.0.pdf *3：スマートフォン利用シーンに潜む脅威 Top10 2023 スマートフォンを安全に利用するにあたっては、技術的対策で100%防ぐことは不可能であり、利用者一人一人がスマートフォン利用時の危険性を十分理解し、適切な判断を行うことが重要。そこで、利用者が分かりやすいよう「利用シーン」を合わせて、2022年の社会情勢を考慮して2023年に10大脅威としてとりまとめ。 https://www.jssec.org/news/news20230228.html *4：キュアコーディングガイド Androidアプリケーションのセキュリティを考慮した設計・開発のノウハウを集めたガイド。アプリケーション開発現場で「使う」ことを想定しサンプルコードセクション、サンプルコードの背景にあるセキュリティ観点の留意事項をまとめたルールブックセクション、さらにセキュリティの理解を深めるための話題をまとめたアドバンストセクションで構成。 https://www.jssec.org/dl/android_securecoding.pdf *5：モバイルアプリケーション開発 10大チェックポイント 2016 年のリリースから更新されていなかった「 OWASP Mobile Top 10プロジェクト」を再解釈し、スマートフォンアプリケーション開発者に向けて現状にあった「Mobile Top 10 」を選定。 https://www.jssec.org/mobile-apps-10checkpoint2023 *6：アプリ開発ガイド(新) スマートフォンアプリケーションの開発にあたって、不正な外部送信やその他の挙動を行わないようするためのガイドを今後検討予定。 *7：セキュリティかるた スマートフォンの利用が若年化している中、子どもたち自身が楽しみながら「危ないこと」に気づく力を身につけられるよう、小学校高学年から中学校1～2年生を対象にセキュリティかるたを作成(電子通信普及財団の助成金対象)。	
6	個人D	Ⅱ-1-(2)	DMARCの話が出ているが、元々総務省ではDKIMの推奨と推進を行なっていたはずである。 末端の電子メール利用者（一般的なISP等と契約し、その電子メールサービスを用いたメールの送受信を行なう者）にとっては、間違いなく、DKIMが最適な手段として機能する部分があり、その使用はSPF・DMARCの利用をするかどうかに関わらず、あるべきものであるはずであるが、なぜ、DKIMについてはこの文書のどこでも言及が無い様な事態となっているのか。 DKIMであれば、間違いなく、メールヘッダ中にDKIM-Signatureのエントリが示される事になり、それは末端の者にもとても有用な情報となるはずであるが、まず、DKIMについての導入を推進すべきと考える。（※技術的・仕様的に望ましいとなるものであるので、総務省等はそれに対抗出来ない。） DKIMはフェアであり、TLSによる電子メールの保護と同様に、全ての電子メールについて備わっているべきものであるが、総務省は、以前の姿勢を崩すでなく、DKIMについての推奨と推進を行なうようにされたい。（もちろん、TLSによる電子メールの送信・受信の保護についてもまだ対応を行なっていないISPや事業者があるのでこれも変わらずに。）	総務省においては、電子メールに関する効果的な脆弱性対策の手法として標準化されており、国際的にも実装が進みつつあるにも関わらず、我が国では導入が進んでいないDMARC等のネットワークセキュリティ技術について、導入に係る技術的課題等を調査し、具体的な課題解決策を検討していると承知しています。具体的には、昨年度からはDMARC等(SPF、DKIMを含む)のメール認証技術に係る技術的課題の調査・分析を行っており、得られた知見を踏まえ、今年度にはこれら技術の普及促進に向けたガイドライン案を作成し技術導入の普及啓発に取り組むものと承知しています。
7	日本電気株式会社	Ⅱ-1-(2) Ⅱ-4	●p.13及びp.43について OSやソフトウェア、機器等の更新を実施することに対する意識啓発も対策に含めるのがよいと考えます。 文書冒頭に記載されている2022年10月に病院で発生したインシデントを含め、VPN等でネットワークの安全性は確保されていたものの、更新を実施していなかったことに起因してインシデントが発生したという事例が数多くあります。	御意見については、参考として承ります。なお、P78（付録４）には、「ファームウェアの更新、新しい機器への買い換え等を含めて利用者によるIoT機器の適切な管理を推進するための周知啓発を強化する」旨を記載しており、脆弱性等のあるIoT機器によって生じうる不利益・リスクと、その対応策について、分かりやすく伝える工夫をすることを含めて、総合的なIoTボットネット対策に取り組んでいただきたいと考えております。

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
8	日本電気株式会社	Ⅱ-1-(2)-ア	悪性Webサイト情報の収集・分析について、同様の施策がJC3（日本サイバー犯罪対策センター）でも2023年3月より実施されています。 この取組みとも連携し、より多くの情報を収集して分析することで、より効果が見込まれると考えます。 JC3　ScamAdviser(SAGICHECK)への協力 https://www.jc3.or.jp/news/2023/20230301-488.html	ご指摘のとおり、悪性Webサイトへの対策のためには、多くの情報を収集して分析することが重要であり、御意見については、参考として承ります。
9	楽天モバイル株式会社	Ⅱ-1-(2)-ア	「RPKI、DNSSEC、DMARC等のネットワークセキュリティ技術については、国内ISP等における導入状況や各ネットワークセキュリティ技術導入に係る技術的課題の調査・分析を継続するとともに、得られた知見を踏まえたネットワークセキュリティ技術等の普及促進に向けたガイドライン案を作成し、技術導入の普及啓発に取り組む」（P14）とする本報告書案に賛同いたします。 楽天グループではDMARC等の実装を推進しており、今後もこうしたサイバーセキュリティ対策に積極的に取り組んでまいります。 （https://corp.rakuten.co.jp/security/anti-fraud/）	賛同の御意見として承ります。
10	IssueHunt株式会社	Ⅱ-1-(2)-ア	積極的なサイバーセキュリティ対策を進めるためには、電気通信事業者が自社の製品やサービスに対する脆弱性を事前に検知し、対策することが重要である。ICT サイバーセキュリティ総合対策 2023にて今後の取組として挙げられている対応は必須であるものの、日々複雑且つ高度化していくサイバー攻撃において、自社、関係団体及び関係事業者のみで網羅することは困難である。そのため、2010年代から米国や欧州で普及している「バグバウンティ（脆弱性報奨金制度）」を取り入れ、電気通信業者が自社の製品やサービスに対する調査案件を公開し、セキュリティ研究者などの国内外の第三者と連携することで常時攻撃者側の視点に立った対策を講じることが効果的であると考える。	御意見については、参考として承ります。
11	楽天モバイル株式会社	Ⅱ-1-(2)-イ	「アプリ事業者以外の第三者によるスマートフォンアプリの挙動の技術的な解析可能性についての検証を行うことが適当」（P16）とする本報告書案に賛同いたします。 アプリ事業者以外の第三者によるスマートフォンアプリの挙動の技術的な解析を進めるためには、安全なソフトウェア開発を行うための体制・プロセスを整えた上で、アプリ事業者が外部の研究者と良好な関係性を築くための枠組みを整えることが肝要と考えます。 こうした考えの下、当社においては、脆弱性情報の扱い等について定める「ソフトウエア製品等の脆弱性関連情報に関する取扱規程（平成29年経済産業省告示第19号）」の遵守に加え、外部の研究者の協力の下「脆弱性開示プログラム（Vulnerability Disclosure Program）」を整備し、その運用に努めているところです。	御意見については、参考として承ります。なお、P17の御指摘の箇所については、我が国としては「自由、公正かつ安全なサイバー空間」の確保を基本的な考え方としているところ、こうした考え方とは必ずしも整合的ではない提案に対しては、「自由、公正かつ安全なサイバー空間」を支えるネットワークや技術の特性及び普及状況を念頭に置きつつ、国際的な議論に対応することが求められる趣旨で記述したものです。
12	個人B	Ⅱ-1-(2)-エ	＞国際場裡における議論に効果的に対応していくためには、これら技術のメカニズムや効果、国内外の普及状況等を踏まえた関与が求められる。 本稿意見者には全く理解し難い文章だ。そもそも「我が国が掲げる「自由、公正かつ安全なサイバー空間」の在り方と必ずしも整合的ではないと考えられる国際標準の提案」は、具体的に何を示しているのか？脚注に詳述すべきである。 まず記載した上での検討となるが、文頭で「我が国が掲げる「自由、公正かつ安全なサイバー空間」の在り方と必ずしも整合的ではない」と言っているにも関わらず、結論が「国際場裡における議論に効果的に対応」となっているため、文章全体の意味が通らなくなっている。一体全体何を優先したいのか。もうすこし整理願う。	
13	株式会社ラック	Ⅱ-1-(2)-オ	＜意見＞ スマートシティセキュリティガイドラインの更新維持と、各地域の調査・相談対応の団体設立につながるような活動が実現できればと考えます（スマートシティISACのような形） ＜理由＞ 各地域で推進されているスマートシティの取組について情報共有の場が少なく、また意見や事例提出がしやすい環境が少ないと感じているためです。	御意見については、参考として承ります。なお、P19において、スマートシティ官民連携プラットフォームのセキュリティ・セーフティ分科会において、セキュリティ対策の先進事例について官民で情報共有を行った旨を記述しており、関係者間においてこうした情報共有の取組が引き続き進められることを期待しています。
14	日本電気株式会社	Ⅱ-1-(3)	トラストサービスの普及に当たっては、何よりも国や総務省による制度化が重要と考えます。運用状況を踏まえた適切な制度見直しを含め、認定制度の早期実現が望ましいと考えます。	御意見については、参考として承ります。なお、eシールについては、P23に記述したとおり、「引き続き、我が国のeシールサービスの状況等に関する情報収集を行いつつ、民間サービスの信頼性を評価する基準策定及び適合性評価の実現に向けた、国による認定制度の創設を含めて検討を進めていくことが適当である」としており、これを踏まえて必要な対応を進めていただきたいと考えております。

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
15	セイコーソリューションズ株式会社	Ⅱ-1-(3)	デジタル技術を便利に使うことで、Society5.0社会を実現するには、本報告書案記載の通り、トラストサービスが重要な役割を果たすこととなると考えます。 サイバーセキュリティ総合対策として、トラストを確保する枠組みの実現において、以下の提言をさせていただきます。 ■ｅシールの国による認定制度の早期創設 当社のタイムスタンプ認定制度における経験から、 ① トラストサービスは、基盤サービスであることから、実際の利用者への価値訴求が難しい。 利用者は、利便性・効率性やコストには敏感ですが、データの信頼性が保証できない場合の将来のセキュリティ事故対策には意識が低い。 ② 民間による認定制度では、基盤としての通用性が低く、利用者が安心してご利用いただく判断が難しい。 これらのことは、折角のDX気運にもかかわらず、エビデンスは紙面・対面で済ましてしまう可能性が高いことを意味します。 デジタルによる生成から保管までの一貫処理が途絶え、Society5.0社会は、画餅になってしまう可能性すらあります。 この危惧を打破し、流通する情報のデータ化において、一貫してデータそのものの信頼性を確保するためには、仕組みとして発出元が特定できることと完全性を保証することで法的な効力をもつ公的な制度を創設することであると考えます。	御意見については、参考として承ります。なお、eシールについては、P23に記述したとおり、「引き続き、我が国のeシールサービスの状況等に関する情報収集を行いつつ、民間サービスの信頼性を評価する基準策定及び適合性評価の実現に向けた、国による認定制度の創設を含めて検討を進めていくことが適当である」としており、これを踏まえて必要な対応を進めていただきたいと考えております。
16	一般社団法人　デジタルトラスト協議会	Ⅱ-1-(3)	令和５年（2023年） ７月４日 サイバーセキュリティ戦略本部にてまとめられた「サイバーセキュリティ2023」では、CS戦略の方向性として、「デジタル改革を踏まえたデジタルトランスフォーメーションとサイバーセキュリティの同時推進」が挙げられています。 御省から発出される「ICTサイバーセキュリティ総合対策2023」にトラストサービスの普及に関する記述を織り込まれる意義は大きく、デジタルの利便性を享受し、様々な分野でDXを実現するには21-23ページに記載の通りデジタルデータの信頼性を確保する「トラストサービス」の普及に向けた取組を一層推進することが肝要であると思料致します。 政府におけるデータ戦略、とりわけトラストを確保する枠組みの実現に向けて以下の推進を提言させていただきます。 ■包括的なトラスト基盤の創設 令和3年４月にデータ戦略タスクフォースの下に設置され、内閣官房 情報通信技術（IT）総合戦略室にて開催された「トラストに関するワーキングチーム」の検討では、データのトラストの枠組み検討の主な論点として、以下の６点が示されました。 論点１：包括的なトラスト基盤の創設 論点２：国(又は、民間機関)による認定制度の創設 論点３：認定の公的効果 論点４：各種トラストサービスのクオリファイドサービスの認定基準、特定サービスの基準の策定 論点５：クオリファイドサービスをトラステッドリストとして公表 論点６：国際的な相互承認 DFFTの文脈で、国際的に信頼ある自由なデータ流通の必要性が高まっています。国際競争力を維持する上で、わが国においてトラストを確保する枠組みの整備が重要であり、上記論点を踏まえた包括的なトラスト基盤の速やかな創設が求められていると考えます。 ■国(又は、民間機関)による認定制度の創設と各種トラストサービスのクオリファイドサービスの認定基準、特定サービスの基準の策定 現在、国によるトラストサービスの認定は電子署名、タイムスタンプにとどまっていますが、「ICTサイバーセキュリティ総合対策2023」でお示しいただいたｅシール、eデリバリーに加え、リモート署名、リモートｅシールに関しても認定制度の創出に向け検討を加速すべきと考えます。認定の基準となる技術・運用基準は国際的な標準技術に従っていることが求められ、各トラストサービスの共通した要件と、個別要件から組み立てが可能であり、関係省庁を横断、連携した取り組みにより効率化、スピードアップが図れると考えます。 ■認定の公的効果の法制化 「トラストサービス」は、市場における電子取引の信頼性を高め、官民のオンラインサービス、電子ビジネス、電子商取引の有効性を高める「産業基盤」であるため、さまざまな法省令・告示・ガイドラインから援用される「統一した規則」を設定し、法的効果を与えることが望ましいと考えます。 ■クオリファイドサービスをトラステッドリストとして公表 サイバー空間と実空間が高度に融合したSociety5.0では、マシンtoマシンでのデータ流通が国内外で加速することが想定されます。流通するデータのトラストを自動的に高速で検証でき、後段に自動連係できる仕組みが求められます。 利用者視点から、利用しているアプリケーションが、安心できるサービスであるのか、提供されたデジタルデータが安心できるサービスによるものであったのか、を確認する手段が現時点ではありません。 「統一した規則」では、機械的に、トラストサービスであること・あったことを国内外の利用者が確認できるトラストアンカーの開示と国際間での接続を含む運用を制度として盛り込むべきであります。国による検討の場を早急に設置し、そのあり方の検討に着手する必要があると考えます。 ■国際的な相互運用の早期実現 トラストサービスは、時空間を超越するデジタル社会の基盤であることから、上記DFFT文脈からもトラストサービスの国際相互運用が求められると考えます。 国連の国際商取引法委員会では、国境を越えて商取引を行うにあたって、やりとりされる情報の確からしさの根拠を共通認識とすべく、トラストサービスの	御意見については、参考として承ります。なお、トラストサービスについては、P22に記述したとおり、「今後とも、政府におけるデータ戦略、とりわけトラストを確保する枠組みの実現に向けた検討の動向を踏まえながら、各種トラストサービスの普及に向けた取組を推進することが求められる」としており、これを踏まえて必要な対応を進めていただきたいと考えております。

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
			モデル法を採択しています。（UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services (2022)） このことは、国として国際的に通用する仕組みを整備し、海外の基盤と相互承認することがデジタル社会における商取引では、共通認識となることを示しているものと考えます。我が国においても、経済安全保障促進の観点から国の主導で推進されることを期待します。	
17	株式会社帝国データバンク	Ⅱ-1-(3)	以下、本文から引用 【今後の取組】 今後とも、政府におけるデータ戦略、とりわけトラストを確保する枠組みの実現に向けた検討の動向を踏まえながら、各種トラストサービスの普及に向けた取組を推進することが求められる。具体的には、タイムスタンプについて、国による認定制度を適切に運用するとともに、必要に応じて制度の見直し等を検討する必要がある。また、eシールについて、引き続き、我が国のeシールサービスの状況等に関する情報収集を行いつつ、民間サービスの信頼性を評価する基準策定及び適合性評価の実現に向けた、国による認定制度の創設を含めて検討を進めていくことが適当である。さらに、eデリバリー等データ流通の信頼性の確保に向けた検討を行うことが適当である。 上記取組に賛同します。 特に、eシールに関する「民間サービスの信頼性を評価する基準策定及び適合性評価の実現に向けた国による認定制度の創設」が重要と認識しています。 以下で挙げる基準について、適合性評価が公表されることは利用者、検証者にとって必要不可欠であり、当該適合性評価を行う機関を認定（或いは監督など）は「電子署名及び認証業務に関する法律（平成12年法律第102号）」や「時刻認証業務の認定に関する規程（令和３年総務省告示第146号）」のように国による認定が適当と考えます。 (1)eシール用電子証明書を発行する電子認証局に関する基準 (2)eシール用電子証明書プロファイルに関する基準 (3)リモートeシールサービス提供に関する基準 また、eデリバリー等データ流通の信頼性の確保に向けた検討も同様に必要と認識しています。eデリバリーが安全、簡便に利用できる環境構築は、我が国のDXの推進には不可欠と認識しています。なおeデリバリーは、送信側・受信側の認証を含めてサービス間連携が重要とも想定しています。	賛同の御意見として承ります。なお、eシールについては、P23に記述したとおり、「引き続き、我が国のeシールサービスの状況等に関する情報収集を行いつつ、民間サービスの信頼性を評価する基準策定及び適合性評価の実現に向けた、国による認定制度の創設を含めて検討を進めていくことが適当である」としており、これを踏まえて必要な対応を進めていただきたいと考えております。
18	渋谷区	Ⅱ-1-(3)	Eシール活用による自治体の請求・支払い義務のDX化について ○自治体の請求・支払業務の現状 ・通知当の行政文書における公印押印の省略、事業者・個人への押印省略などは浸透してきたが、請求書等の請求・支払いにかかる書類は現在も社印等の押印を求める状況が続いている。（2018　JAL　架空請求事件も影響あり。） ・一方、自治体における電子契約の導入は、導入済み、導入検証中を含めると、全自治体の10%以上※１となっており、契約事務のDX化は急速活着実に進んでいる。 ※令和５年７月現在の弁護士ドットコムのクラウドサイン導入自治体数、GMOグローバルサインのGMOサインの導入・導入検討数から推定したもの（両社の発表記事から計算） ○提案 ・電子契約とeシールの組み合わせにより、自治体・事業者間の請求・支払義務を電子化し、飛躍的な効率化を実現する。 ・ポイント 自治体がeシールを利用（事業者側の負担軽減）、 どのような財務会計システムにも対応可能 ○効果 ・請求・支払い事務における請求書(紙）の削減、封入、郵送、返信（郵送）など、自治体、事業者双方の事務の軽減に大きなメリットがある。(社会全体の効率化) ・自治体においては、経常事務の削減により、住民サービスに多くの職員を従事させることができ、本来の住民サービスの質を向上させることができる。社会全体のペーパーレス化に貢献し、SDGsを進展させることができる。 ○貴職への要望 ・Eシールについては、セキュリティレベルにおいて議論があるのは承知しているが、自治体が国内において使用するレベルであれば、EU策定レベルと同等レベルのものでなくても十分ではないかと考える。 ・自治体におけるDXは、現在進行中であり、その流れを加速させるうえでも、用途に合ったセキュリティレベルのeシールを導入するなど、早々の開始をお願いしたい。	御意見については、参考として承ります。なお、eシールについては、P23に記述したとおり、「引き続き、我が国のeシールサービスの状況等に関する情報収集を行いつつ、民間サービスの信頼性を評価する基準策定及び適合性評価の実現に向けた、国による認定制度の創設を含めて検討を進めていくことが適当である」としており、これを踏まえ必要な対応を進めていただきたいと考えております。
19	IssueHunt株式会社	Ⅱ-1-(3)-エ	クラウドサービスの設定不備に起因する情報漏えいや障害といった事故を防ぐためには、特定の人物や事業者に依存せず、多くの関係者と連携する枠組みを作ることが効果的と考える。特に昨今普及しているクラウドサービスにおいては、サイバー攻撃の手法が日々進化しており、限られた人的リソースの中で情報収集や分析、対策を講じることは困難である。そのため、米国や欧州で普及している「バグバウンティ（脆弱性報奨金制度）」を取り入れ、自社の製品やサービスに対する調査案件を公開し、セキュリティ研究者などの第三者と連携することで、”監視の目を増やす”対策を常時取り入れる仕組みを作ることが効果的であると考える。	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
20	MOTEX株式会社	Ⅱ-2-(1)	「演習の実施に必要となる幅広い要素（データセット、演習用ミドルウェア、計算機リソース等）を総合的にカバーする」とありますが、ログ監視・分析やインシデント対応等の人材育成に主眼を置いていると認識しています。これら人員以外に、セキュリティマネジメントにおいて必要となる「セキュリティ戦略・企画、セキュリティリスクの評価・監査を行う人材の育成」についても検討いただきたいと考えます。	CYNEX Co-Nexus Cでは、NICTが構築・整備している演習基盤をオープン化することで、産学官連携による人材育成を推進しており、御意見については、参考として承ります。
21	個人B	Ⅱ-2-(1)	＞また、我が国のサイバーセキュリティ人材は質的にも量的にも不足しており、人材育成を全て国で実施することは困難であるため、 人材育成はむしろ国家が先陣きって対応すべきと本稿意見者は考える。本稿意見者のこの解釈と後述３１ページの説明は合致している。しかしながらここで「人材育成を全て国で実施することは困難」と言い切ってしまっているため、後述３１ページの説明と続かなくなっている。 ここは、次の段落と合わせて、 －－－－－－－－－－－－－－－－－－－－－－－－－－－－ また、我が国のサイバーセキュリティ人材は質的にも量的にも不足している。人材不足解消には、民間事業者や教育機関等における自立的な人材育成がまず求められるものの、演習用の環境構築やシナリオ開発には高度な知識や技術力、そして基盤となる計算機環境が必要であり、民間企業・教育機関のみでは十分に対応できていない。 （中略） 国内でのサイバーセキュリティ情報生成や、人材育成を加速するエコシステムの構築が必要である。困難を承知で国家が先陣を切ってこれを実施する。 －－－－－－－－－－－－－－－－－－－－－－－－－－－－ というような文章であれば違和感ない。	「ICTサイバーセキュリティ総合対策2023（案）」P24では、「人材育成を全て国で実施することは困難である」と記載しており、人材育成の一部を国が実施することの実現可能性や必要性は否定していません。したがって、当該記載は、P31における「総務省は、NICTの「ナショナルサイバートレーニングセンター」を通じて、サイバーセキュリティ人材育成の取組（CYDER、CIDLE、SecHack365）を積極的に推進している。また、地域のコミュニティや企業、教育機関等と連携して、サイバーセキュリティ人材を自立的に育成していくためのエコシステムの確立に向けた実証を行っている。」との記載とは矛盾しないと考えております。
22	個人C	Ⅱ-2-(2)-ウ	P29「これらの研究開発の成果については、例えば、標的型攻撃観測技術の高度化では、並行ネットワーク構築機能の強化を進めたサイバー攻撃誘引基盤（STARDUST）の外部利用を推進し、10以上の機関に利活用されるなど社会実装および成果展開を推進した。」と記載されている。この記載内容は、昨年の総合対策記載の内容と全く同じである。10以上の機関がもっと増加したのか、継続して使用されていてその課題は等の記載があるとよりよいのではないかと思います。さらに、「今後の取組」の記載内容が1年前とまったく変わっていないことは、いかがなものかと思ってしまいます。	ご指摘のうち【現状】に係る記載は、NICTにおける研究開発の社会実装及び成果展開の状況の一例として、サイバー攻撃誘因基盤（STARDUST）の外部利用の現状を記載したものです。 ご指摘のうち【今後の取組】に係る記載は、NICTにおいて、ICTを取り巻く諸課題やサイバー攻撃の状況を踏まえ、研究開発を推進・牽引することが引き続き求められており、その旨記載したものです。
23	個人C	Ⅱ-2-(3)-ア	P32「CYDERを受講した地方公共団体の数は順調に拡大しているものの、未受講の団体が依然として存在することから、未受講団体がサイバーセキュリティを確保する上での弱点とならないように、引き続き、地方公共団体に対し、CYDERの受講促進を図ることが必要である。」と記載されている。本記載は昨年とまったく同じである。せめて、全体の地方公共団体数と受講済み団体数のトレンドを示し、未受講がどれくらい減っているのかどうかなど見える化が必要ではないかと思えます。	ご指摘の記載は、現時点においてもなお、地方公共団体に対してCYDERの受講促進を図ることが必要であり、その旨記載したものです。地方公共団体のCYDER受講状況に係る詳細データは、CYDERを効率的、効果的に実施する観点から取り扱うことが適当であると考えております。
24	個人C	Ⅱ-2-(3)-ア	P32「CYDERは、これまで、主に国の機関等及び地方公共団体を対象として実施されてきた。他方、近年、病院等の重要インフラ事業者がサイバー攻撃を受け、その運営に大きな支障を生じさせる事案が相次いでおり、その要因として、当該事業者の人的能力の不足も挙げられている。重要インフラ事業者の機能不全が社会経済活動に与える影響を踏まえ、こうした事案に対応するため、重要インフラ事業者に対するCYDERの提供を拡大することが求められる。」と記載されている。非常に賛成でもあり、いまさら感も感じます。CYDERは病院も含めて重要インフラ及びそれに関する事業体、団体で実施される必要があると思います。	賛同の御意見として承ります。
25	MOTEX株式会社	Ⅱ-2-(3)-エ	【現状】にて沖縄県での事業内容が掲載されており、セキュリティ事業に携わる者としてこの活動に賛同いたします。今後、沖縄県以外の各地域への拡大を期待します。	賛同の御意見として承ります。
26	個人B	Ⅱ-4-(2)-ウ	文部科学省が出てくるものの、こども家庭庁の記載が一切見当たらない。こども家庭庁は一切関与しないということか確認させてほしい。	FMMCが実施している「e-ネットキャラバン」は、現状においては、こども家庭庁との連携は行っていないと承知しております。
27	ソフトバンク株式会社	Ⅱ-4-(2)-ウ	P.51【今後の取組】に対する意見 サイバーセキュリティ上のリスクの高まりに伴い、特に注力すべき普及啓発対象としてこどもや高齢者が挙げられていますが、スマートフォンやインターネットを使いこなしている層もセキュリティに関する意識・対策が十分とは考えにくく、こどもや高齢者に限らず、普及啓発は等しく全年齢層を対象として強化すべきです。この点、本取りまとめ案に記載のデジタル活用支援推進事業の利活用は有効な方策の一つであり、警察庁等関係省庁とも連携し、早期にサイバーセキュリティに関する講座を同事業の対象として追加すべきと考えます。	御意見については、参考として承ります。なお、デジタル活用支援推進事業においては、総務省・内閣官房で連携し、サイバーセキュリティの普及啓発の観点から講座教材を作成し、講習会を行いました。今後、サイバーセキュリティに関する講座の利活用に向けて検討してまいります。

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
28	MOTEX株式会社	Ⅱ-1-(2)-エ	「大手自動車メーカーが利用するSaaSサービス」とありますが、クラウドサービス詳細は公開されていないため「大手自動車メーカーが利用するクラウドサービス」が適切かと考えます。	御指摘を踏まえ「大手自動車メーカーが利用するSaaSサービス」を「大手自動車メーカーが利用するクラウドサービス」に修正いたします。
29	個人A	全体	・６ページの５行「あたって」と、１５ページの最下行の６行上「当たって」とは、どちらかに字句を統一したほうがよい。 ・１２ページの１７行「更に、」と、１５ページの最下行の９行上「さらに、」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、Ｐ６の５行目の「あたって」を「当たって」に、P12の17行目の「更に、」を「さらに、」に修正いたします。
30	個人C	全体	今回、非常に重要なICTサイバーセキュリティ総合対策2023を取り纏め得られ、コメントを出す機会をいただきありがとうございます。複雑、巧妙になっているサイバー攻撃に対してどのような観点で向きあえばいいかの指針になるものだと認識しています。 昨年のICTサイバーセキュリティ総合対策2022からの形式上は、更新であるため、更新箇所がわかるようにWordの変更履歴版も同時に公開されるといいのではないかと思いました。これにより、今までも総合対策を参照している方々が、どのような変化があるのかがよりわかりやすくなるのではないかと思います。	ICTサイバーセキュリティ総合対策2023は、ICTサイバーセキュリティ総合対策2022策定後のサイバーセキュリティタスクフォースにおける議論を踏まえて、新たにとりまとめたものであるため、変更履歴の公表等は実施しておりません。
31	個人A	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？	今回の意見募集については、その対象である「ICTサイバーセキュリティ総合対策2023」（案）が行政手続法第２条第８号規定の「命令等」に該当しないため、同法第39条第１項及び同条第３項が適用されないこと等も踏まえて、期間を設定したものです。
32	個人E	はじめに	「審議会等の整理合理化に関する基本的計画」（平成11年４月27日閣議決定）別紙４「懇談会等行政運営上の会合の開催に関する指針」においては、「懇談会等に関するいかなる文書においても、当該懇談会等を『設置する』等の恒常的な組織であるとの誤解を招く表現を用いないものとする。」とされているところ、本案P4等において「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」を「設置し」た旨が記載されているのは、不適当である。	御指摘を踏まえ、Ｐ４、P12、P46、P63の「設置」を「開催」に修正いたします。
33	個人C	付録３	3つめ、4つめのURLの記載が適切でなく、クリックしても適切なファイルが開かない。 P59 記載されているURLとリンクされているURLとが異なる。このためクリックしても適切なファイルが開かない。 (表示)～867112.pdf (リンク)～000690267.pdf	御意見を踏まえ、URLを修正いたします。
34	個人A	付録４	９２ページの第５回の議事内容欄の２行「取りまとめ骨子（案）ついて」は「とりまとめ骨子（案）について」の誤記か？	御意見を踏まえ、「とりまとめ骨子（案）について」に修正いたします。
35	日本電気株式会社	付録４の 2-(2)-② 2-(4)-③	●p.73及びp.79について 利用者への注意喚起はあくまでルータやIoT機器に注目した記載となっていますが、内容自体はID・パスワードの設定等やソフトウェアの更新など、PC等にも適用される一般的なものと思われます。そのため、利用者の意識が向きにくいルータやIoT機器の対策がシステム全体においてどのような位置づけ・優先度なのか、言及されるべきかと思います。システムインテグレーター等との連携についても、注意喚起によって、顧客(エンドユーザ)が納得して実施できることが重要となりますので、同様の情報展開が求められると思われます。	御意見については、参考として承ります。なお、利用者への注意喚起については、P78に記述したとおり、「・・・利用者によるIoT機器の適切な管理を推進するための周知啓発を更に強化する。その際、脆弱性等のあるIoT機器が、利用者本人やネットワーク全体に対して、どのような不利益・リスクを生じさせるのか、また、その対応策について分かりやすく伝わるよう工夫する」としており、これを踏まえて必要な対応を進めていただきたいと考えております。
36	個人C	付録４の1-(2)	P66　図のタイトルは慣例に従い図の下に記載したほうがいいかと思います。	付録４中の図のタイトルについては、統一的に図の上に記載しています。
37	日本電気株式会社	付録４の1-(3)	ID・パスワードの脆弱性を除く、リモートコード実行やコマンドインジェクション等のファームウェアをはじめとする様々なソフトウェアの脆弱性について、それらがそもそも発現しにくいようにする取り組みについて言及するのがよいと考えます。具体的には、セキュリティ・バイ・デザインに基づいたソフトウェアの開発について言及するのがよいと考えます。IoT機器においては、後からの対策としてファームウェア更新が用意されたとしても、実際に更新されない場合が多いです。そのため、そもそも脆弱性が出荷後に発現しにくくなるような取り組みについても言及するのがよいと考えます。セキュリティの観点からIoT機器に付加価値を付けるような取り組みにつながるような記載があるとよいと考えます。	御意見については、参考として承ります。なお、本とりまとめ案は、主にNOTICEをはじめとする既にインターネットに接続されたIoT機器のセキュリティ対策等について検討を行ったものでありますが、P67に記述したとおり、「端末（IoT機器）側の対策については、開発・製造といった段階でも適切なセキュリティ対策が講じられることが望ましい・・・」旨や、P79に記述したとおり、「ISP 及びメーカー等の関係者が連携し、ファームウェアの自動更新等、利用者が意識せずにIoT 機器を適切に管理可能な製品・サービスの普及に取り組む」旨についても言及しているところです。
38	MOTEX株式会社	付録４の1-(3)	「PCやスマートフォンにおけるOSのアップデート等や、クラウドサービス（SaaS）等」とありますが、IoT機器が利用するクラウドサービスはSaaS以外にもPaaSなども想定されるため、「PCやスマートフォンにおけるOSのアップデート等や、クラウドサービス等」が適切かと考えます。	御指摘の箇所については、セキュリティ対策において適切な役割分担が行われている例を具体的に列挙するために記載したものです。