「サイバーセキュリティ2017（案）」に対する意見募集の結果の概要

- 実 施 方 法： NISCのWebページ及び電子政府の総合窓口（e-Gov）に掲載して公募
- 実 施 期 間： 2017年７月13日（木）～ ７月27日（木）
- 意 見 総 数： 15者から39件 【内訳：４企業・団体から延べ19件、11個人から延べ20件】

（１）修正意見： 全７件

- 主旨を踏まえて修正（全１件）
- 理由を付して原案どおりとすると回答（全６件）

（２）政策展開に係る意見： 全29件

- 今後の政策展開に係る意見については、当センターとしての考え方及び当該意見を今後の参考にする旨を回答

（３）賛同意見、その他意見： 全３件

注）提出された意見は必ずしも明確にこれらに分類されるものではないが、事務局で理解した区分にて計上している

- （参考）提出者名：

一般社団法人日本クラウドセキュリティアライアンス、日本オラクル株式会社、KPMGコンサルティング株式会社、
在日米国商工会議所、個人（11）

「サイバーセキュリティ 2017（案）」に対する意見募集の結果一覧

通し No.	提出者	該当箇所 ページ	該当箇所 章節項	概要	御意見に対する考え方及び修正	意見の種
1	在日米国商工会議所（ACCJ）	2	1.1	IoTシステムの設計、「ボット根絶」への動き、ガイドラインの発行、認証スキーム、脆弱性情報の普及など、セキュリティの概念を推進するための継続的なアプローチを歓迎するとともに、以下を提言します。 A）　IoTセキュリティに関する問題に備えるため、データの収集、保持、市民のプライバシーに対するビッグデータ分析に関する脅威、インフラと市民に対するIoTの完全性と可用性への脅威等、IoTセキュリティに関する意識啓発プログラムを設ける。 B）　被害につながる恐れのある、悪意のあるサイトへのアクセスを防止するために、コンピューティング性能が限られるIoT機器保護の自動機能を提供する安全なDNSサービスの使用を奨励する。 C）　IoTシステムを含む情報システムインフラ全体に焦点を当て、全府省庁に統一されたモデルとガイドラインを提供すべきである。システムインフラは、IoTデバイスからバックエンドシステムまで、データ分類に基づくエンドツーエンドのデータ転送を想定する必要があり、様々なタイプとレベルのサイバーセキュリティの問題を解決する「縦深防御」に基づいているべきだと考える。	IoTのサイバーセキュリティに関しては、ボット撲滅の推進や安全なIoTシステムの創出による国際競争力の強化に取り組んでいくこととしております。 また、政府機関等においては、統一基準群に基づき、サイバーセキュリティ対策を推進しているところです。その中で、ご意見については、施策の検討や実施の推進にあたって参考にさせていただきます。	政策展開に係る意見
2	KPMGコンサルティング株式会社	2	1.1（3）（イ）	以下のような表現にされてはいかがかと考えます。 「経済産業省において、IoTシステムの構成要素であるM2M機器等にも活用すべき制御システム向けのセキュリティに係る認証制度であるEDSA認証（2014年４月開始）について、普及・啓発を行うとともに、制御システム全体のセキュリティ評価・認証の仕組みを検討する。 理由： ISAsecureでは他機器も認証取得が増えつつありますが、国内のEDSA認証ではDCSコントローラが認証取得の中心になっております。 DCSコントローラは、プロセスデータの仲介者として間接的にIoTにデータを提供する存在にはなり得ますが、IoTの構成要素としてはあくまで黒子に徹する機器と見受けられます。 イメージの問題ですが、「EDSA認証の範囲は、もっと（DCS以外の）フィールド機器にも活用されるべき」であることを知らしめることを優先すべきと考えます。 （国内で、その他機器の認証取得意欲が低いのは、主に認証取得コストの問題だと思われますが、そのハードルを乗り越えるためにも経営層の意識改革と併せて動機付けが重要と考えます）	原案においては「M2M機器等」を制御システムの例示として記載しており、M2M機器がEDSA認証の対象であることは明らかであるため、原案のとおりとさせていただきます。	修正意見
3	在日米国商工会議所（ACCJ）	3	1.2	インシデントに備え次のような措置を取るよう産業界に奨励することを要望します。 A）　セキュリティ機能の現状に関する標準ベースの評価や、アーキテクチャ、ドキュメンテーション、問題点の特定とロードマップの作成といった、次世代のサイバーセキュリティに関するビジョン、戦略、ロードマップを組織レベルで作成し、複数年のセキュリティ計画とする。 B）　リスクや脅威の識別、ネットワークの監視、アーキテクチャ・アセスメント、積極的に高度な標的型攻撃を検知・対応するためのアセスメントを行うことおよびリアクティブなインシデント対応のため、先進的な手法に対する詳細なアセスメントやベンチマーキングを実施する。	現在サイバーセキュリティ経営ガイドラインの改定作業を実施しております。ご意見については、このようなガイドラインの見直しや施策の検討にあたって参考にさせていただきます。	政策展開に係る意見
4	個人（1）	3	1.2（1）（イ）	「1.2 セキュリティマインドを持った企業経営の推進」 「(1) 経営層の意識改革」に関して、「サイバーセキュリティ経営ガイドラインの普及を図る」ため、既存の他のガイドラインや基準の活用を図ってはどうかと考える。例えば既に企業等が導入している既存のガイドラインとサイバーセキュリティ経営ガイドラインとの項目レベルでの対応関係を整理し、当該ガイドラインの対応状況を把握、公表できるような仕組みを整えてはどうかと考える。	現在サイバーセキュリティ経営ガイドラインの改定作業を実施しております。ご意見については、このようなガイドラインの見直しや施策の検討にあたって参考にさせていただきます。	政策展開に係る意見
5	KPMGコンサルティング株式会社	・4 ・14	・1.2（3）（カ） ・2.2（3）（ク）	（「サイバーセキュリティ2017（案）」に盛り込むべき意見ではありませんが） 経済産業省は、演習コンテンツのブラッシュアップ等を目的として警察庁と連携されてはいかがかと存じます。 理由： 警察庁情報通信局情報技術解析課は平成27年度に大規模産業型制御システム模擬装置一式を調達導入済であり、攻撃対策としての緊急対処や実態解明の手法確立に活用されています。また、庁内で連携して警備局警備課では同年度から委託教養で現場捜査官の教育訓練を開始しています。 以下のような資料も公表されていますので、独自のノウハウを確立されている可能性が高いと思われます。 <https://www.npa.go.jp/policies/budget/review/h29/mogisouti_siryou.pdf>	「サイバーセキュリティ人材育成プログラム」（平成29年4月サイバーセキュリティ戦略本部決定）に基づき、各府省庁等と連携して演習等の取組を進めているところです。ご意見については、このような施策の推進にあたって参考にさせていただきます。	政策展開に係る意見
6	在日米国商工会議所（ACCJ）	5	1.3(2)（エ）	貿易障壁につながる国内規制の問題に関して、経済産業省および外務省が産業界とともに、他国に働きかける取組を行うことを歓迎します。	賛同意見として承りました。	賛同意見

「サイバーセキュリティ 2017（案）」に対する意見募集の結果一覧

通し No.	提出者	該当箇所 ページ	該当箇所 章節項	概要	御意見に対する考え方及び修正	意見の種
7	在日米国商工会議所（ACCJ）	7	2.1	政府が国のサイバーセキュリティに関する助言と働きかけを行う窓口を一本化するよう要望します。 A）　窓口で得られる情報は、法規制、ガイドライン、経営レベルによる事業展開から効果的な実装事例、それにベストプラクティスと防御に関する消費者レベルのガイダンスをカバーする情報共有の原則のすべてが含まれている必要がある。 B）　窓口は、特に重要インフラの事業者向けに、検証されたツールやソリューション、それに対象となる問題に関する専門家への啓発と情報へのアクセスを提供する必要がある。 C）　システム管理者が自身を守るために必要な更新情報、掲示板、およびその他の情報を政府が窓口を通じて提供し、またユーザーがマルウェア攻撃から復旧するのを支援するため、業界を情報源として活用するよう提言する。	NISCにおいて、政府機関等、重要インフラ事業者等に加え、SNS等を通じて広く国民全体への注意喚起等の情報提供を実施しております。また、官民が連携し、迅速な集約・分析、効果的な対策の共有を行う情報連携体制を構築することを現在検討しております。ご意見ついては、このような施策の検討や実施の推進にあたって参考にさせていただきます。	政策展開に係る意見
8	一般社団法人日本クラウドセキュリティアライアンス	7	2.1(1)	2.1. 国民・社会を守るための取組 (1) 安全・安心なサイバー空間の利用環境の構築 ・欧米などでは既に医療・介護分野では遠隔医療・介護として自宅でのモニター・投薬などの体制が既に導入されているが、我が国での取り組みはこれからであるので、医療・介護・ヘルスケアの機器(体内埋め込み型・ウェアラブル含む)と医療・介護センターとの通信などに対する安全基準・接続時の認証の仕組みなどの整備が必要なのではないか?	2.2（イ）に記載のとおり、内閣官房及び重要インフラ所管省庁等が連携して、安全基準に関する施策を含む「重要インフラの情報セキュリティ対策に係る第４次行動計画」に基づく施策を進めることとしていますので、ご意見について参考にさせていただきます。なお、厚生労働省においては、医療機関等を対象とするサイバー攻撃の多様化・巧妙化、IoT等の新技術やサービス等の普及への対応等を目的に、2017年５月に「医療情報システムの安全管理に関するガイドライン」を第５版に改定し、情報セキュリティの確保に努めているところです。また、医療機関等からの通信方法についても、本ガイドラインにおいて示しております。	政策展開に係る意見
9	個人（1）	7	2.1(1)	「2.1国民・社会を守るための取組み」 「(1) 安全・安心なサイバー空間の利用環境の構築」に関して、仮想通貨・ブロックチェーンの安全な利用に関する記述がないが、金融庁などと連携した取り組みが必要ではないかと考える。加えて大学等における取組みに関する記述があるが、類似の組織としては病院・医療機関においてもシステムの重要性・脆弱性が指摘されており、厚労省等と連携した対策が必要ではないかと考える。	2.2（イ）に記載のとおり、内閣官房及び重要インフラ所管省庁等が連携して、安全基準に関する施策を含む「重要インフラの情報セキュリティ対策に係る第４次行動計画」に基づく施策を進めることとしていますので、ご意見について参考にさせていただきます。 なお、厚生労働省においては、「医療情報システムの安全管理に関するガイドライン（第５版）」（2017年５月）を策定するなど、情報セキュリティ確保に努めています。 また、金融庁においては、資金決済システムに関する制度的枠組みの整備などを行い、資金決済システムの安全性等の向上に努めているところです。	政策展開に係る意見
10	一般社団法人日本クラウドセキュリティアライアンス	7	2.1(1)	2.1. 国民・社会を守るための取組 (1) 安全・安心なサイバー空間の利用環境の構築 ・仮想通貨・電子マネーなど新しい決済インフラがサイバー空間で使えるようになってきている。その為の、決済端末・決済アプリなどのへの資金決済に関わる法整備と対策推進を明記するべき想定される脅威は、埋め込み型決済端末(いわゆるIoT)やスマホ内の決済アプリと残高管理を行うサーバもしくはブロックチェーン網に対しての安全対策基準やガイドラインの策定が必要であるブロックチェーン網は我が国だけの対応だけでは、対応しきれない問題でもあるが、各国と調整を行う主管がどこなのかを明らかにするだけでも意味があると思われる。	2.2（イ）に記載のとおり、内閣官房及び重要インフラ所管省庁等が連携して、安全基準に関する施策を含む「重要インフラの情報セキュリティ対策に係る第４次行動計画」に基づく施策を進めることとしていますので、ご意見について参考にさせていただきます。 なお、金融庁においては、資金決済システムに関する制度的枠組みの整備などを行い、資金決済システムの安全性等の向上に努めているところです。	政策展開に係る意見
11	在日米国商工会議所（ACCJ）	11	2.2	重要インフラを守るための取組に関して、以下のとおり意見を示します。 A）　政府が重要なサービスを全国レベルで把握するための枠組みを設けることを提言する。数の限られた大規模な企業が提供するクラウドサービスへの依存度が高まるにつれて、重要インフラや緊急救援サービスなど、特定の分野において、ひとつのプロバイダが大多数の消費者にとって単一の障害点になることがないよう監視する必要がある。このような単一の障害点については可視性が必要である。 B）　政府は、米国防総省の協力の枠組みをさらに活用し、米国防総省および国土安全保障省の専門家へのアクセスを得ることで取組を前進させることができる。	2.2に記載のとおり、情報通信分野を含めた重要インフラ事業者等については、サービスを安全かつ持続的に提供するため、内閣官房及び重要インフラ所管省庁等と連携し、「重要インフラの情報セキュリティ対策に係る第４次行動計画」に基づき、情報セキュリティ対策に取り組むこととしております。ご意見については、この行動計画に基づく施策を推進するにあたり、参考にさせていただきます。 なお、ご指摘の米国防総省の協力の枠組みが具体的に何を指すのか分かりかねますが、日米両政府は、2013年10月設置の日米サイバー防衛政策ワーキンググループ（CDPWG）を通じて、任務保障や重要インフラ防護におけるベストプラクティスの共有を含む取組を行っているほか、日米サイバー対話その他を通じ、DHS,DODその他政府機関と緊密な連携関係を築いています。	政策展開に係る意見
12	一般社団法人日本クラウドセキュリティアライアンス	14	2.2(3)	2.2. 重要インフラを守るための取組 (3) 各分野の個別事情への支援 非接触型/近傍通信型の決済システムが近年小売業等で導入が進んでいるが、中継機能を悪用したMITM(Man in the Middle)攻撃対策などの取り組みが必要である。資金決済法の監督官庁である金融庁主導の取り組みを明記する必要があるのではないか?	ご意見については、今後の施策の検討にあたって参考とさせていただきます。なお、金融庁においては、資金決済法及び前払式支払手段に関する事務ガイドライン等に基づき、情報セキュリティの確保を含めた、資金決済システムの安全性等の向上に努めているところです。	修正意見

「サイバーセキュリティ 2017（案）」に対する意見募集の結果一覧

通し No.	提出者	該当箇所 ページ	該当箇所 章節項	概要	御意見に対する考え方及び修正	意見の種
13	在日米国商工会議所（ACCJ）	15	2.3	政府機関を守るための取組について以下のとおり提言します。 A）　政府は、複数の府省庁にまたがるセキュリティオペレーションセンター（SOC）を集中化するところまで、セキュリティ運用のレベルを引き上げることを検討すべきである。 B）　政府の購買およびパートナーシップ慣行で、日本のサイバーセキュリティの需要に対応するために同様のアプリケーションや投資を示した事業者および提携企業を評価するべきである。 C)「各府省庁におけるクラウドサービス等の利用や対策の状況について調査」することに加えて、クラウドコンピューティングの標準化の現状と今後の方向性についても検討することが必要である。	統一基準群に則り、政府機関等における情報システムにおけるログの取得・管理及び適切な監視について政府機関等自らが措置を講じているところですが、いただいたご意見については、今後の施策の検討や実施の推進にあたって参考にさせていただきます。 なお、ご指摘のクラウドコンピューティングを含め、政府機関を守るための取組について検討する際は、ご指摘いただいた標準化の現状も踏まえて今後の方向性を検討してまいります。	政策展開に係る意見
14	日本オラクル株式会社	15	2.3(1)（ウ）	「また、各府省庁共通に取り組むべき事項については、」の前に「クラウドを利用する際のセキュリティ上の要件を整理し、統一基準群等の新たな規定として整理することを含む検討を行う。」を追記する。 【理由】 レガシーなオンプレミスのシステムと、クラウドのサービス利用につきましては、概念的には一致するセキュリティ管理策も、責任分解点、実施手順等に差異が生じるため、一般には分離して記述することが推奨されています。米国連邦政府のFedRAMPがその典型例かと思います。	ご指摘のクラウドを利用する際のセキュリティ上の要件については、2016年に改定した統一基準群において規定を強化しており、政府機関等の職員に対する研修においてクラウドサービス選定の際に考慮すべき点を説明するなど、意識の向上を図っているところです。ご意見を踏まえ、以下のように修文いたします。 「内閣官房において、2016年度に改定した統一基準群に基づき、クラウドを利用する際の意識向上を図るとともに、政府機関等の情報システムの調達におけるセキュリティ・バイ・デザインを推進するため、情報システムの調達仕様書の策定段階において適切に定めるべきセキュリティ対策要件について検討を行い、各府省庁におけるセキュリティ・バイ・デザインの取組を促進する。また、各府省庁共通的に取り組むべき事項については、規程への反映に向けた検討を行う。」	修正意見
15	日本オラクル株式会社	16	2.3(1)（タ）	「・・・標的型攻撃に対する多重防御の」を「・・・標的型攻撃に対する多層防御の」に改正する。 【理由】 「サイバーセキュリティ研究開発戦略」との文言統一です。 米国等の西側諸国では「多層防護（Multi-layered Defense）」ではなく「縦深防御（Defense-in-depth）」と記述するのが一般的ですが、国内では多層防御が多用されていますので上記を提案します。文中の「多重防御」という用語は日本国内では散見されますが、海外では類語がありません。	ご意見については、「サイバーセキュリティ戦略」（2015年９月４日閣議決定）において、「標的型攻撃に対する多重防御の取組を加速する」と記載しており、これに対応する施策となりますので、原案のとおりとさせていただきます。	修正意見

「サイバーセキュリティ 2017（案）」に対する意見募集の結果一覧

通し No.	提出者	該当箇所 ページ	該当箇所 章節項	概要	御意見に対する考え方及び修正	意見の種
16	在日米国商工会議所（ACCJ）	18	3.1	我が国の安全の確保に関して、以下のとおり意見を示します。 A）　本戦略において、多岐にわたる政府機関が様々な役割、責任、義務を担っていることが明らかになっているが、これらの政府機関それぞれの役割を一般的に定義づけすると大変理解しやすくなる。今後出てくる新たな課題や動きについて、この一般的な定義があれば全体の戦略を再検討する必要なしに、どの機関が新たな課題に対応すべきか判断するうえで有効なガイドとなる。 B）　政府が、特定の産業が直面する主要な脅威を特定するための産業ベースのISAC（情報共有分析センター）を継続して発展させ、これらの脅威に対する防御および検出についてISAC加入者を啓発するよう要望する。	「サイバーセキュリティ戦略」（2015年９月４日閣議決定）では、「政府に限らず、重要インフラ事業者、企業、個人といったサイバー空間に関係する全てのステークホルダーが、サイバーセキュリティに係るビジョンを共有し、それぞれの役割や責務を果たし、また努力する必要がある。そして、政府はこれらのステークホルダーを適切な連携関係へと促す役割を担っている」としており、ご意見については、施策の検討や実施の推進にあたって参考にさせていただきます。	政策展開に係る意見
17	一般社団法人日本クラウドセキュリティアライアンス	20	3.2(3)	3.2. 国際社会の平和・安定 (3) サイバー空間を悪用した国際テロ組織の活動への対策 国際テロ組織の活動資金調達としてはサイバー空間が活用され始めている。サイバーテロ面だけではなく、テロ組織の資金源として我が国が標的になる事は容易に想定され、インターネットバンキング・仮想通貨・電子マネーなどに対する資金流出・域外決済/送金対策の言及が必要である。	インターネットバンキング、仮想通貨、電子マネー等を悪用した犯罪につきましては、「2.1 国民・社会を守るための取組 (3)サイバー犯罪への対策」(ア)及び(イ)に記載のとおり、警察庁において、産学官連携の促進や、対処態勢の強化に努めることとしています。ご意見については、このような施策の検討や実施の推進にあたって参考にさせていただきます。	修正意見
18	個人（1）	20	3.2（3）（イ）	「3.2国際社会の平和・安定」 「(3) サイバー空間を悪用した国際テロ組織の活動への対策」に関して、「国際テロ組織等の動向把握、攻撃の予兆等の早期把握」に加えて、昨今重要視されているのは、サイバー空間を利用した資金調達やマネーロンダリングへの対策である。これらについて、金融庁等との連携により取組む旨の記述が必要ではないかと考える。	サイバー空間を利用した資金調達等への対策につきましては、警察庁等において、金融機関等との共同対処協定の締結を推進し、インターネットバンキングに係る不正送金事犯対策を行うなど、所要の対策を推進しているところです。ご意見については施策の検討や実施の推進にあたって参考とさせていただきます。	修正意見
19	在日米国商工会議所（ACCJ）	21	3.3	政府がサイバーセキュリティの課題について国際的に取り組むことの必要性を盛り込んでいることを歓迎します。ACCJは、政府のこれらの取組に関し、特にASEANといったこの地域の国々において、技術専門家やキャパシティビルディング、トレーニング機会の提供などの分野で喜んで支援をする用意があります。	賛同意見として承りました。	賛同意見

「サイバーセキュリティ 2017（案）」に対する意見募集の結果一覧

通し No.	提出者	該当箇所 ページ	該当箇所 章節項	概要	御意見に対する考え方及び修正	意見の種
20	個人（2）	24	4	「4. 横断的施策」について ・東日本大震災において津波、原子力災害における避難警報、勧告、報告、報道においてリスクコミュニケーションに関する多くの問題が生じ、初動時の対応や風評被害による禍根を残す結果となっている。 　これを踏まえ、サイバーテロ等のシビア・インシデントへの特に初動時におけるリスクコミュニケーションについて、警戒レベル等の段階を明確化し、各段階における対応基準を策定し、レベルの判断～報告～情報提供～情報伝達等のコミュニケーションフローを整備することで国民の混乱を最小化し適切な行動を喚起することで被害の局所化・早期に事態の終息化を図る、という戦略的な視点が必要である。	2.2(2)(ア)に記載のとおり、効果的かつ迅速な情報共有の実現のための取組のひとつとして、重要インフラサービス障害等に係る深刻度判断基準の導入に向けた検討を進めることとしています。ご意見については、このような施策の検討や実施の推進にあたって参考にさせていただきます。	政策展開に係る意見
21	在日米国商工会議所（ACCJ）	24	4.1	政府は、政府機関や企業のサイバーセキュリティの成熟度の向上や、研究開発への投資に対してインセンティブを提供すべきであると考えます。 これには、望ましい活動や成果を促進するための助成金も含まれます。	サイバーセキュリティ研究開発戦略に基づく技術開発に取り組んでまいります。その中で、ご意見については、関係省庁とも連携の上、施策の検討や実施の推進にあたって参考にさせていただきます。	政策展開に係る意見
22	個人（2）	25	4.2	「4.2. 人材の育成・確保」について ・上記のような非常事態における適切な行動を実行できるように教育・訓練を行う必要がある。特に情報提供の際に末端で情報伝達における重要な役割を担うべき報道機関の記者や教育機関の教職員等の関係者、問合せ窓口となる可能性の高い自治体職員、通信事業者やクラウドサービス提供者、システム販売会社、電気店等の従事者については、提供された情報を正しく理解し、憶測や風評に左右されず、的確に他者への情報伝達を可能とするための教育・訓練が重要と思われる。	「2020年及びその後を見据えたサイバーセキュリティの在り方について－サイバーセキュリティ戦略中間レビュー－」（2017年7月13日サイバーセキュリティ戦略本部決定）において、「サイバー攻撃発生時や危険度の高い脆弱性が判明した時などに状況や対策についての情報発信や相談対応をより迅速に行えるよう関係機関の連携を図りつつ取組を強化する」こととしています。ご意見については、このような施策の検討や実施の推進にあたって参考にさせていただきます。	政策展開に係る意見
23	在日米国商工会議所（ACCJ）	25	4.2	人材の育成・確保に関して、以下のとおり提言します。 A）　複数の政府機関や教育機関が、日本におけるサイバーセキュリティの能力を育成、開発、強化するために使用できるクラウドベースのサイバーレンジ施設を構築し、継続的な更新を支援する。この施設は、複数の機関が演習や研修を行うための共通のプラットフォームとして利用できる。 B）　スキルマッピングや雇用、教育、研修に対するアカウンタビリティを含む国の安全保障に関わるサイバーセキュリティのカリキュラムを提供する養成機関を設けること。そしてそれには主要な研究成果や研修教材が利用されること。 C）　都道府県においてサイバーセキュリティCoEとして選定されている大学や熟練した人材へのアクセスを確実に確保すること。これによって都道府県や地域の企業に研修のための拠点ならびにリエゾンセンターを提供することになる。 D）　業界横断的にインシデント対応を効果的にリードできるサイバーセキュリティの専門家を増やすために継続的に取り組むこと。 E）　認定機関が重要な評価作業（侵入テスト、インシデント対応、レッドチームアセスメント等）を行うため査定者を設ける枠組みを活用すること。 F）　日本の高等教育においてサイバーセキュリティを学ぶ学生によりよい内容のトレーニングを提供できるよう、産官学連携に取り組むこと。 G）　主要政府機関、重要インフラ産業、および日本にとって重要な産業のパートナー間で、コンピュータのインシデント対応に関する全国規模の演習の実施を検討すること。 H）　エグゼクティブレベル、ミドルレベル、スタッフレベルの年間トレーニングのために、重要インフラを含むサイバートレーニングシナリオ（フィジカルおよび非対称戦の両方を含む）のためのテーブルトップエクササイズ（TTX）を開発すること。	産学官連携や全国規模のサイバー演習等、「サイバーセキュリティ2017（案）」に既に記載している各施策に基づき、取組を進めてまいります。ご意見については、このような施策の検討や実施の推進にあたって参考にさせていただきます。	政策展開に係る意見
24	個人（3）	25	4.2(1)（ウ）	「4. 横断的施策⇒4.2. 人材の育成・確保⇒(1)高等教育段階や職業能力開発における社会ニーズに合った人材の育成」での「(ウ)ハイブリッド型人材の育成」では、T型人材を廃止しH型人材の導入をする事だと思います。(ア)T型人材とは、専門性を一つ持ち幅広く繋げる事です。(イ)H型人材とは、専門性を二つ持ち幅広く繋げる事です。要約すれば、H型人材を目指すという事は、多様性創造力の天才を作り出す事なので、同じ所に約3年以上は居座らず、内閣府の職員は、官公庁の職員を退職して、ITネットワーク部門以外での別の専門性を極めて頂きたいです。例えば事例が挙げられます。IT部門から介護部門に行く等です。飲食部門から化学部門に行く等です。スポーツ部門から法学部門に行く等です。官公庁職員からホームレスに行く等です。具体的には、無職も多様性です。	あらゆる産業でITとの組み合わせが進行する中で、情報系学部だけでなく、情報系学部以外においても、サイバーセキュリティの知識・能力を身につけることは必要であると考えております。このように、高等教育段階においては、一つの専門性を高めていく人材育成（T型人材）のみならず、複数の専門性を高めていく人材育成（H型人材）も必要と考えております。	政策展開に係る意見
25	個人（3）	26	4.2(3)（ウ）	「4. 横断的施策⇒4.2. 人材の育成・確保⇒(3)突出した能力を有しグローバルに活躍できる人材の発掘・育成・確保」での「(ウ)独創的なアイディア・技術を有する人材の発掘・育成」では、「持続的改革と創造的改革」に異なりがあります。現在の日本国が認識している「グラーバル及びイノベーション」とは、持続的改革です。本物のイノベーションとは、「創造的破壊（スクラップアンドビルドアップ）」事なので、定義を明確にするべきです。	サイバーセキュリティ人材の育成については、「サイバーセキュリティ人材育成プログラム」（平成29年4月サイバーセキュリティ戦略本部決定）等に基づき、取組を進めているところです。ご意見については、このような施策の検討や実施の推進にあたって参考にさせていただきます。	政策展開に係る意見
26	個人（1）	26	4.2（4）	「4.2人材の育成・確保」 「(4) 人材が将来にわたって活躍し続けるための環境整備」に関して、優秀な人材確保に重要なことは、活躍し続けたいと思う処遇であると考えるが、この点についての記述がない。優秀な人材が高待遇で国内の民間企業や海外の企業・研究機関等に流れている現状に対抗し、防衛省、警察庁の人材高度化を図るための処遇面での施策が必要と考える。	政府機関におけるセキュリティ人材の確保・育成については、「サイバーセキュリティ人材育成総合強化方針」（平成28年3月31日サイバーセキュリティ戦略本部決定）等に基づき、取組を進めているところです。ご意見については、このような施策の検討や実施の推進にあたって参考にさせていただきます。	政策展開に係る意見

「サイバーセキュリティ 2017（案）」に対する意見募集の結果一覧

通し No.	提出者	該当箇所 ページ	該当箇所 章節項	概要	御意見に対する考え方及び修正	意見の種
27	個人（4）	26	4.2（4）（イ）	・情報セキュリティマネジメント試験の活用促進について 情報セキュリティマネジメント試験を「情報処理安全活用推進士」略称「登録シスアド」という名称独占による国家資格として創設してはどうか。 シスアドを略称に推す理由として「セキマネ」は発音しずらく、ユーザー側の試験区分として50万人程度の合格者数と一般企業においても知名度があった「シスアド」の名称を復活させた方がユーザー企業や一般企業に向けた普及が一気に進むと思われるためである。	情報セキュリティマネジメント試験は「サイバーセキュリティ人材育成プログラム」（平成29年4月サイバーセキュリティ戦略本部決定）等に基づき、取組を進めているところです。ご意見については、このような施策の検討や実施の推進にあたって参考にさせていただきます。	政策展開に係る意見
28	個人（4）	26	4.2（4）（ウ）	・第４次産業革命に対応したIT人材育成とITスキル標準の改定について 全ての社会人がITリテラシーを標準装備することの必要性が課題となっており、厚労省においても来年度、社会人へ向けたIT基礎力を身に付ける職業訓練を概算要求するようであるが、職業訓練の出口としてITパスポートの合格を必須科目としてはどうか。 ITリテラシーを標準装備させるならば、ITパスポートも国家資格化してはどうか。 企業内において合格者数の不足人数分だけ、障害者雇用納付金の制度を模してお金を独法IPAなどへ納付させる仕組みを制度化してはどうか。 納付されたお金はテレワークやクラウドソーシングなどを行っている企業への助成や補助金として活用できる仕組みにすることでITリテラシーの標準装備とIT利活用による働き方改革が推進されていくのではないか。	第４次産業革命に対応したIT人材力の強化については、第８回未来投資会議（平成29年５月12日開催）における厚生労働大臣提出資料において、社会人の基礎的ITリテラシーの習得機会の拡充について、関連予算を平成30年度概算要求に盛り込むとされており、現在、検討中です。 なお、ITパスポート試験は、情報技術に関する基礎的知識を問う国家試験であり、今後ITを本格的に学ぶための導入部分に当たるものと考えております。従って、ITパスポートを国家資格化する予定はありません。ご意見の内容については、このような施策の検討にあたって参考にさせていただきます。	政策展開に係る意見
29	個人（5）	27	4.2（4）（エ）	前回のサイバーセキュリティ2016では（4）-（エ）に 情報処理安全確保支援士制度を「行政機関等における人材登用で当該制度を積極的に活用する方策を検討する。」と記載されていたが、今回のサイバーセキュリティ2017（案）では活用に対する具体的な方策が述べられていない。 「経済産業省において、情報セキュリティに係る最新の知識・技能を備えた専門人材の国家資格として2016年に開始した情報処理安全確保支援士（登録セキスペ）制度の着実な実施に向けて必要な措置を講じる。 さらに総務省において、地方公共団体におけるサイバーセキュリティを担う人材を確保するために情報処理安全確保支援士等を専門部署に人材登用するように方策を検討する。」 と記述していただきたい。	情報処理安全確保支援士制度については、行政機関のみならず、民間にも幅広く制度を普及させることが必要なことから記述を変更したものです。また、一定以上の能力や経験を有する者については、情報処理安全確保支援士の資格が取得しやすくする等により、活躍しやすい職場環境を整えているところです。 地方公共団体における情報セキュリティに関わる人材の知識・技能の確保については、各団体の情報セキュリティポリシー等で具体的に定めております。総務省としては、地方公共団体の情報セキュリティポリシー策定について、ガイドラインを示し方向性について技術的助言する役割を担いますが、特定の認定制度を主眼に置くものではございません。すなわち、情報セキュリティ人材の知識・技能の確保には、新規雇用や外部からの支援の調達、職員への研修など 種々の方法があり、かつ知識・技能の測定や認定方法にも複数あり、当該制度が唯一の方法ではないことから、当該資格保有者の登用を主たる対応方法とする方針を打ち出すことは難しいところです。ご意見の内容については、今後の施策の検討にあたって参考にさせていただきます。	修正意見
30	在日米国商工会議所（ACCJ）	27	4.2（4）（エ）	・情報処理安全確保支援士制度について 最新の知識を身に付けるために必要なWeb講習、集合研修の受講料を個人の負担とするならば、独占業務や必置などの厚遇措置が講じられていない中…費用対効果の面から考えて、コスパが悪過ぎる。 Web講習、集合研修の受講料を見直すなど…負担軽減策を講じてはどうか。とりわけ、障害者手帳を有する者における支援士のWeb講習や集合研修の受講料は、手帳のコピーを提出して確認が取れたならば、各種ある減額制度に準じた措置を講じる合理的配慮を願いたい。	情報処理安全確保支援士が行う業務の観点から、最新のサイバーセキュリティの知識・技能を維持する必要があり、講習が法律で義務付けられているところです。受講料については、IPAにおいて実費を勘案して設定したものであり、ご理解をお願いします。なお、常に運営の効率化を念頭におき、受講者の負担を低減できるよう努力してまいります。	政策展開に係る意見
31	個人（6）	27	4.2.（4）（エ）	4.2.（4）エとして先に創設された情報処理安全確保支援士制度についての言及があるが「制度の普及に向けた必要な措置」、「当制度普及のため、企業や団体への周知等を積極的に行う」との曖昧な記載にとどまっており、他の項の施策に対して安全確保支援士がどう活用されていくのか定義されていない。情報処理安全確保支援士制度はサイバーセキュリティ対策の推進のために整備された制度と理解しているが、当「サイバーセキュリティ2017(案)」の他の項の具体的な取り組みと紐づいていない。官庁内の担当組織や担当者による縦割りでの制度普及やサイバーセキュリティ施策の立案のみでなく、既存の制度や取り組みを複合的に関連させた取り組みが必要と考えます。 「1.経済社会の活力の向上及び持続的発展」の項であれば、制度整備や経営層の意識改革、人材育成等において情報処理安全確保支援士制度との関連を付けた施策を実施するべきと考える。 例えば ・一定以上規模の組織であれば情報処理安全確保支援士を必置化 ・情報処理安全確保支援士の配置企業を企業別に公開（現在は支援士の登録企業が公開されているが、人に対する登録有無であり、企業としての配置状況は読み取れない。1企業に何人配置しているか、従業員や資本金に対する配置比率等に応じたランキング等、制度活用を推進するための具体的な取り組みが必要） ・各取り組みの中での情報処理安全確保支援士の活用指針を定義等	情報処理安全確保支援士の設置等の義務的措置を設けることについては、社会的な効果と企業の負担等の影響等を総合的に考慮する必要があり、現時点で具体的な措置を規定することは困難ですが、ご意見の内容については、今後の施策の検討にあたって参考とさせていただきます。	政策展開に係る意見
32	個人（7）	27	4.2（4）（エ）	情報処理安全確保支援士の扱いについて、周知されていない実情があるにせよ、扱いが簡略すぎる。 高額な研修会費用を考えると、先行きが明確にあたえられていなければ、登録を行う人数は増えないと思われる。 将来的な位置づけや、差し当たって支援士同士で情報交換が行えるような組織の立ち上げなど、支援士になろうと考える人がメリットと感じるような施策は取れないものだろうか。	情報処理安全確保支援士制度の周知については、企業や教育機関を重点におきつつ、引き続き適切に実施してまいります。 支援士の情報交換が行える組織については、支援士の数等を勘案し、必要な時期に検討を行うこととします。	政策展開に係る意見

「サイバーセキュリティ 2017（案）」に対する意見募集の結果一覧

通しNo.	提出者	該当箇所 ページ	該当箇所 章節項	概要	御意見に対する考え方及び修正	意見の種
33	個人（2）	28	5	「5. 推進体制」について ・現状認識として、仮想通貨や自動運転技術等の急速な進歩・普及に伴い、これまで住み分けられていたサイバー空間と現実世界との境界線があいまいになりつつある。このためサイバーテロによる、社会経済への深刻なダメージが生じるリスクが急速に高まっている。 このような現状を踏まえ、大規模なサイバーテロ等の非常事態における、金融システム、電子商取引、通信・インターネット、クラウドサービス等の利用制限や利用停止措置等の緊急措置について、法制度の整備が必要である。	ご指摘の法制度の整備が具体的に何を指すのかが分かりかねますが、近年のサイバー攻撃の激化などサイバー空間における脅威がますます高まる状況にあり、特定の高度な技術を有する者のみがサイバーセキュリティの対処を行う形態ではもはや対応は困難であると認識しております。ご意見については、今後の施策の検討や実施の推進にあたって参考にさせていただきます。	政策展開に係る意見
34	個人（3）	―	―	全体の企画構造の素案を確認したのですが、厳密には、「企画（プラン）」して頂きたいです。（ア）「試作化（トライアルプロダクション）」⇒「量産化（メスプロダクション）」⇒「製品化（メイドプロダクション）」です。（イ）「戦略（ストラテジー）」、「作戦（オペレーション）」、「戦術（タクテック」）、「兵站（ロジステック）」を厳密化する事です。具体的には、「製品化（メイドプロダクション）」するには、人材の確保から来る1世代20年とし「約2世代（約40年）」が掛かると考えます。私は現在で中高年なので、約40年先の未来では新構造を使うことなく他界していると考えます。文学とは、作品を出せば1世代で終わります。科学とは、自分の世代で成し遂げられ無い功績を、次の世代に託す事に意味があります。	「サイバーセキュリティ2017（案）」とは直接関係がないと考えられますが、ご意見として承ります。	政策展開に係る意見
35	個人（8）	―	―	「組織的なストーキング、及び嫌がらせ行為・集団によるストーカー」と呼ばれる集団犯罪で、私たちに行われている組織的なストーキング、及び嫌がらせ行為は、相手が見知らぬ第三者の集団であり、集団の一人または複数人がかわるがわる、毎日、執拗な嫌がらせを行ってきます。 相手を特定できず、共謀していることの証明が難しいため、現在のストーカー規正法では対処できません。ネット内でもハッキングや工作、サブリミナルが溢れています。 テクノロジー犯罪、集団ストーキング犯罪は海外で明らかにされていると同時に、取り締まりが行われています。なぜ日本は野放しなのですか？	ネット上のつきまとい行為や誹謗中傷等につきましては、犯罪を構成する場合は、警察庁等において厳正な取締りを推進することとしており、引き続き、取組を推進してまいります。	その他
36	個人（9）	―	―	地方において情報格差を感じる。地方の空白をもう少し埋めていただける機会があるとよい。資料を拝見しあらゆる施策で対応されることが良く理解できるが、首都圏一局集中に感じられる。地理的条件や経済的な条件で地方の中小企業や個人等に地方とのギャップの解消がむずかしい。「サイバー交番」的に、より地域に密着した、ミニ研究施設、個人であっも気軽に相談可能な施設が望まれる。	2.1(2)（セ）に記載のとおり、IPAを通じ、「情報セキュリティ安心相談窓口」、「標的型サイバー攻撃の特別相談窓口」によって、サイバーセキュリティ対策の相談を受け付ける体制を充実させ、一般国民や中小企業等の十分な対策を講じることが困難な組織の取組を支援してまいります。	政策展開に係る意見
37	一般社団法人日本クラウドセキュリティアライアンス	―	―	全般的に、内閣官房・経産省・総務省・警察庁・防衛省以外の他省庁の記述が粗い印象を受ける。政府一体となった取り組みに省庁間の温度差が見受けられるのはよろしくないと思われる。特に重要インフラに関してはエネルギーと通信分野の対策は見えてくるのだが、お金(金融)と健康(医療・ヘルスケア)分野に関しては取り組みが不十分な印象を受ける。	「2.2 重要インフラを守るための取組」に記載した各種施策については、各重要インフラ分野を対象としており、金融分野及び医療分野が除かれることはありません。今後も、「重要インフラの情報セキュリティ対策に係る第4次行動計画」に基づいた施策を推進してまいります。	政策展開に係る意見
38	個人（10）	―	―	ますますサイバー的な危険性はこれからも多くなってくると思います。 専門的な分野の育成には賛成致します。 また、国防としての位置付けなも、最前線的な意味合いも含まれると思っています。 日本は多分研究されれば他国に負けないくらいの見識などもあるはず、大いにこう言った方の意見も取り入れ、未然に防ぐ事の可能な分野として、独自の開発にも着手していただきたいと思っています。	サイバーセキュリティ研究開発戦略に基づく取組を進めていく中で、ご意見については、施策の検討や実施の推進にあたって参考にさせていただきます。	政策展開に係る意見
39	個人（11）	―	―	IoTの企図する第四次産業革命の担い手は、これまでITの蓄積のない中小企業や農業法人、スタートアップ企業等であり、経営者の意識高く臨んでも、今日の高度なサイバー攻撃に対抗できる経営資源は持ち合わせていない。 ここ数年、各省庁から大量の基準やガイダンスがばらまかれているが、小規模な組織がこれらの一つ一つに個別に対応できるわけはなく、その実効性は担保されていない。 一方、国が進めるデジタルガバメントにおいても、これらの業者の多くはそのサプライチェーン上も重要な取引先であり、政府調達におけるガバナンスの対象でもある。 米国ではFedRAMPの枠組みで政府機関がクラウド上にセキュアなサービスを構築し、シェアする取り組みが始まっている。我が国でも政府調達基準のナショナルクラウドを確立し、中小企業等にも安くセキュアなインフラを使わせられるようなエコシステムが必要。 守れないルールを乱立させるより、使えるインフラを生み出すエコシステムを構築するのが早道。人材不足も解消する。	「2020年及びその後を見据えたサイバーセキュリティの在り方について－サイバーセキュリティ戦略中間レビュー－」（2017年7月13日サイバーセキュリティ戦略本部決定）において「中小企業等においては、サイバーセキュリティ対策に使えるリソースに限界があることから、外部の能力や知見を活用しつつ、効率的に進める方策の検討が必要である。特に、クラウドサービスの活用等、中小企業のセキュリティを実質的に高めるための取組を行う」としており、ご意見については、このような施策の検討や実施の推進にあたって参考にさせていただきます。	政策展開に係る意見