「サイバーセキュリティ戦略」に基づき、2019年度に実施すべき施策に関する意見募集の結果の概要

■ 実施方法：NISCのWebページ、内閣官房のWebページ、電子政府の総合窓口（e-Gov）に掲載して公募

■ 実施期間：平成31年（2019年）１月24日（木）～２月25日（月）

■ 意見総数：24者から92件 【8企業・団体から延べ45件、16個人から延べ47件】

【意見の種類】

・2019年度に実施すべき施策（サイバーセキュリティ2019）に関する意見：87件

- ・経済社会の活力の向上及び持続的発展：27件
- ・国民が安全で安心して暮らせる社会の実現：21件
- ・国際社会の平和・安定及び我が国の安全保障への寄与：4件
- ・横断的施策：29件
- ・推進体制：6件

・その他の意見：５件

■ （参考）提出者名：

オフィスVG2、スプランクサービスジャパン合同会社、富士通クラウドテクノロジー株式会社、一般社団法人日本経済連合会産業技術本部、BSA | ザ・ソフトウェア・アライアンス、株式会社ラック、大日本印刷株式会社、匿名希望の団体、個人（12人）

2019年度に実施すべき施策に関する意見募集の結果一覧

通しNo	提出者	該当箇所	意見の要旨	主な考え方
1	個人 （4）	4．1．1　新たな価値創出を支えるサイバーセキュリティの推進	「5G（第5世代）」における構造では、「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）」の融合であり、「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」等に対し、融合される事で、サイバーセキュリティー対策が重要と、私は考えます。 クラウドコンピューティングとエッジコンピューティングに対し、無線LANにおける「Wi-Fi（ワイアーレスローカルエリアネットワーキング）」が、今後の構造に成ると、私は考えます。	先端技術を利活用したイノベーションを支えるサイバーセキュリティに関する賛同意見として承りました。内容については、今後の施策の検討や実施の推進に当たって参考とさせていただきます。
2	団体名匿名希望	4．1．1　新たな価値創出を支えるサイバーセキュリティの推進	企業の保有する情報について、情報の消去に関して明記し、使用済み情報の消去によりサイバー攻撃など有事の際のリスクの軽減を図ることができる。	個人情報保護法については、第19条において、「個人情報取扱事業者は、利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つとともに、利用する必要がなくなったときは、当該個人データを遅滞なく消去するよう努めなければならない。」と明記されております。 企業におけるサイバーセキュリティ対策に関しては、経営層の意識改革やサイバーセキュリティに対する投資の推進等を行うこととしており、引き続き、取組を推進してまいります。
3	個人 （7）	4．1．1　新たな価値創出を支えるサイバーセキュリティの推進	企業においては、サイバーセキュリティ対策が、潜在的損失リスクの低減に資すること、また、会社経営におけるリスク管理項目であることを、財務指標に組み込むとともに、監査項目に組み込むべきであると考える。	企業におけるサイバーセキュリティ対策に関しては、年次計画において「経営層の意識向上や民間企業における対策の促進に向けた取組を幅広く推進する」としており、サイバーセキュリティが経営リスクの一つとして認識されるよう、引き続き、取組を推進してまいります。
4	個人 （10）	4．1．1　新たな価値創出を支えるサイバーセキュリティの推進	（意見） 個人情報取扱事業者及びインターネットを収益プラットフォームとしている事業者については、情報処理安全確保支援士を常勤の取締役CISOとして必置化を義務とするべきである。 （理由） 「サイバーセキュリティ2018」において、戦略マネジメント層向けの理解促進等が記載されているが、理解の促進では実効性が無い。4.1.1(2)・(3)の実現にあたっても、経営的に発言権を持ち、判断できる知識を持つ有資格者のCISOを必置とすべきである。	情報処理安全確保支援士（登録セキスペ）制度は、平成29年4月に登録を開始し、2019年4月現在での登録者数は18，330人となったところ。また、登録開始から3年目となり、ある程度の運用実績も積み上がってきたことから、年次計画において「情報処理安全確保支援士制度の着実な実施に向けて必要な措置を講じる」としており、制度運用の更なる改善を検討する予定です。事業者等に対し登録セキスペの設置を強制する措置が適当か否かは慎重に議論する必要がありますが、御意見については、今後の検討にあたっての参考とさせていただきます。

2019年度に実施すべき施策に関する意見募集の結果一覧

通しNo	提出者	該当箇所	意見の要旨	主な考え方
5	スプランク サービス ジャパン合同会社	4．1．1　新たな価値創出を支えるサイバーセキュリティの推進	「サイバーセキュリティ投資へのインセンティブ」を明示化・視覚化するために、情報を共有しそれらを開示するための基盤システムが必要と考えます。	サイバーセキュリティに対する投資ののインセンティブとしては、平成30年よりコネクテッド・インダストリーズ税制等、一定のサイバーセキュリティ対策が講じられたデータ連携・利活用により生産性を向上させる取組についての税制措置を講じており、年次計画において「必要となるシステムやサイバーセキュリティ対策製品等の導入に対して税額控除等を措置するコネクテッド・インダストリーズ税制の活用を促す」などとされており、引き続きこのような取組の推進を図ってまいります。御意見については今後の取組の検討や実施にあたっての参考とさせていただきます。
6	株式会社ラック	4．1．1　新たな価値創出を支えるサイバーセキュリティの推進	各種施策の総合的な展開に当たっては、産官が適切な枠割り分担のもと密接に連携しつつ、「サイバーセキュリティ産業化」の視点をよりいっそう重視願いたい。	経済社会の活力の向上及び持続的発展に資するサイバーセキュリティに関する賛同意見として承りました。ご意見については、今後の施策の検討や実施の推進に当たって参考とさせていただきます。
7	株式会社ラック	4．1．1　新たな価値創出を支えるサイバーセキュリティの推進	スタートアップ支援事業について、「サイバーセキュリティ産業化」をも視野に実施願いたい。	経済社会の活力の向上及び持続的発展に資するサイバーセキュリティに関する賛同意見として承りました。ご意見については、今後の施策の検討や実施の推進に当たって参考とさせていただきます。
8	株式会社ラック	4．1．1　新たな価値創出を支えるサイバーセキュリティの推進	経営層の意識改革と合わせて、経営層自らが広くICTについて理解し一定の専門的知見を身につけられるよう「学び」の機会の創出その他の取組みを推進願いたい。	経営層の意識改革を目的として、年次計画において「経営層の意識向上や民間企業における対策の促進に向けた取組を幅広く推進する」としており、サイバーセキュリティが経営リスクの一つとして認識されるよう、引き続き、取組を推進してまいります。
9	株式会社ラック	4．1．1　新たな価値創出を支えるサイバーセキュリティの推進	サイバーセキュリティを十分認識した上で広くICTの利活用を推進している民間のCIOその他の有為な者の活動について、官民が連携し、ベストプラクティスとして共有・参照する取組みを検討願いたい。	平成31年3月に独立行政法人情報処理推進機構より、サイバーセキュリティ経営の実践をサポートするために、民間等の有意な取組事例を整理した「サイバーセキュリティ経営ガイドラインVer2.0実践のためのプラクティス集」を公表しました。今後も本プラクティスの拡充等の取組を推進してまいります。
10	大日本印刷株式会社	4．1．1　新たな価値創出を支えるサイバーセキュリティの推進	重要インフラ事業者や東証一部上場企業などから段階的に情報開示を義務化することが必要と考えます。	経済産業省・独立行政法人情報処理推進機構で公開しているサイバーセキュリティ経営ガイドラインにおいて、企業のサイバーセキュリティ対策に関する情報開示を促しているところです。また、年次計画において、経済産業省では、引き続きサイバーセキュリティ経営ガイドラインの普及促進を図るとともに、そのプラクティス集の充実を進めることとしており、総務省では「「サイバーセキュリティ対策情報開示の手引き」（仮称）を策定、公表し、その普及を図る。」としております。御意見については今後の取組の検討や実施に当たっての参考とさせていただきます。

2019年度に実施すべき施策に関する意見募集の結果一覧

通しNo	提出者	該当箇所	意見の要旨	主な考え方
11	個人 （13）	4．1．1　新たな価値創出を支えるサイバーセキュリティの推進	価値を創出するにはサイバーセキュリティを強化する必要があります。	新たな価値創出を支えるサイバーセキュリティへの賛同意見として承りました。内容については、今後の施策の検討や実施の推進に当たって参考とさせていただきます。
12	個人 （8）	4．1．2　多様なつながりから価値を生み出すサプライチェーンの実現	2018年度の戦略においては、「サプライチェーンにおける調達者が機器・サービス等の利用に際し、その信頼を確認できるよう、官民が連携して、信頼性が証明されている機器・サービス等のリストの作成と管理を行う仕組みの構築が必要である。」とされております。2019年度においては、具体的かつ現実的な計画作りを行い取り組むことが重要と考えます。	サプライチェーンにおけるサイバーセキュリティを確保できる仕組みの構築については、年次計画において「サプライチェーンの分野毎の要件を明確にしたうえでトラストリストを構築・確認する技術」等を確立することとしております。御意見については取組の実施や検討に当たって、参考とさせていただきます。
13	スプランク サービス ジャパン合同会社	4．1．2　多様なつながりから価値を生み出すサプライチェーンの実現	トレーサビリティの仕組みを確保するためには、期間を定めたログを記録する仕組みが必要と考えます。 セキュリティ装置だけではなく、ネットワークトラフィック、サーバー、端末までのトレーサビリティを確保するための期間を定めた「中央管理型ログ基盤」の仕組みが必要と考えます。	トレーサビリティ確保については、年次計画において、「業務データを安全に流通させるためのトレーサビリティ確保技術」等を開発することとしております。御意見については取組の実施や検討に当たって、参考とさせていただきます。
14	富士通クラウドテクノロジーズ株式会社（JASA/CAIS情報セキュリティ監査人補）	4．1．2　多様なつながりから価値を生み出すサプライチェーンの実現	サプライチェーンにつらなる中小企業がNIST SP800-171準拠性を低コストで得られるようにすべき。	サプライチェーンに連なる中小企業のサイバーセキュリティ対策については、2019年4月に策定した「サイバー・フィジカル・セキュリティ対策フレームワーク」ではNIST SP800-171との対応関係も示しているため、NIST SP800-171に準拠するセキュリティ対策要件を把握することが可能となっています。引き続き、中小企業等が実効的にこれらの対策要件を実装できるようにするための検討などを推進してまいります。御意見については取組の実施や検討に当たって、参考とさせていただきます。
15	（一社）日本経済団体連合会 産業技術本部	4．1．2　多様なつながりから価値を生み出すサプライチェーンの実現	「サプライチェーンにおける調達者が、信頼性が証明されている機器・サービス等のリストの作成と管理を行う仕組みの構築」を実施する際には、以下の2点に留意すべきである。 (1)現実的かつ分かりやすいものとすること (2)海外の取り組みも参考にすること	サプライチェーンにおけるサイバーセキュリティを確保できる仕組みの構築については、年次計画において「サプライチェーンの分野毎の要件を明確にしたうえでトラストリストを構築・確認する技術」等を確立することとしております。御意見については取組の実施や検討に当たって、参考とさせていただきます。

2019年度に実施すべき施策に関する意見募集の結果一覧

通しNo	提出者	該当箇所	意見の要旨	主な考え方
16	BSA｜ザ・ソフトウェア・アライアンス	4．1．2　多様なつながりから価値を生み出すサプライチェーンの実現	サプライチェーンへの脅威を低減し、悪意ある活動への防御を強化し、イノベーションと相互運用性を可能にするよう、洗練されたアプローチを優先的に採用することを推奨。サプライチェーンセキュリティへのアプローチが、裁量、相互運用性、協働、透明性、公平性、イノベーション、執行の各原則に従って策定されることを提案。	サプライチェーン対策については、2019年4月に策定した「サイバー・フィジカル・セキュリティ対策フレームワーク」の社会実装を推進するために、各産業分野におけるセキュリティ対策の検討を引き続き推進するとともに、データそのもののセキュリティ信頼性確保や、ソフトウェアのセキュリティ確保を実効的に行う確保するための具体的なセキュリティ対策管理手法等を検討してまいります。御意見については今後の取組の検討や実施の推進に当たっての参考とさせていただきます。
17	株式会社ラック	4．1．2　多様なつながりから価値を生み出すサプライチェーンの実現	中古品のリスクについて国民に対して広く普及・啓蒙する取り組みを推進願いたい。	国民一人一人がサイバーセキュリティに対する意識・理解を醸成し、サイバー空間における様々なリスクに対して対処できるよう、情報発信等の取組を推進しているところです。御意見については取組の実施や検討に当たって、参考とさせていただきます。
18	株式会社ラック	4．1．2　多様なつながりから価値を生み出すサプライチェーンの実現	ファームウェア書き換え、チップのすり替え等を防止する観点から、デバイスの製造者において、筐体の要所を複製が困難な封印等でシールするような仕組みを検討願いたい。	サプライチェーンにおけるサイバーセキュリティを確保できる仕組みの構築については、「4.1.2　多様なつながりから価値を生み出すサプライチェーンの実現」のとおり推進しているところです。御意見については取組の実施や検討に当たって、参考とさせていただきます。
19	株式会社ラック	4．1．2　多様なつながりから価値を生み出すサプライチェーンの実現	「サイバー・フィジカル・セキュリティ対策フレームワーク（案）」で示された「Society5.0」での新たなサプライチェーンにおいて、全体のセキュリティレベルを底上げし、中小企業を欠くべからざる構成要素とするため、中小企業におけるICT利活用と一体的なセキュリティ確保の取組みへの支援策を抜本的に強化願いたい。	中小企業におけるセキュリティ確保の取組については、年次計画において「SECURITY ACTION制度の拡大及びニーズに応じた制度の見直し」を通じて引き続き意識の向上を促す取組を実施してまいります。また、「サイバーセキュリティお助け隊に係る実証事業の全国実施」を通じて、中小企業に対する具体的な取組支援も実施してまいります。
20	（一社）情報通信ネットワーク産業協会	4．1．2　多様なつながりから価値を生み出すサプライチェーンの実現	「サプライチェーンにおける調達者が機器・サービス等の利用に際し、その信頼を確認できるよう、官民が連携して、信頼性が証明されている機器・サービス等のリストの作成と管理を行う仕組みの構築が必要である。」とされており、これをさらに具体的かつ現実的な計画に落とし込むことが重要	サプライチェーンにおけるサイバーセキュリティを確保できる仕組みの構築についての賛同意見として承りました。引き続き、取組を推進してまいります。
21	個人 （14）	4．1．2　多様なつながりから価値を生み出すサプライチェーンの実現	スパイ防止法など、法の面から実行できるサイバーセキュリティ強化の取組・仕組みづくりの実施もお願いいたします。国内ではファーウェイ問題に対しての危険意識が薄く、十分な議論も尽くされていないと思います。 日本企業、ひいては社会・国民の知的資産を守るため意識付けの為にも、法整備を含めた取組のご実施を強く希望いたします。	いわゆるスパイ防止法の必要性については様々な議論があるものと承知しておりますが、不正競争防止法に基づき、営業秘密の保護を図っているところであり、年次計画においても産業界及び関係省庁との連携により企業情報の漏えいの手口・被害実態等の情報共有を行うとするなど、各種取組を行っています。引き続き秘密の保護に努めてまいります。

2019年度に実施すべき施策に関する意見募集の結果一覧

通しNo	提出者	該当箇所	意見の要旨	主な考え方
22	個人 （2）	4．1．3　安全なIoTシステムの構築	電気用品（PSEマーク）や携帯電話（技適マーク）のように国内において利用可能なIoT機器の認証制度を制定・実施すべきと考える。	官民が連携して、安全なIoTシステムの構築に取り組む必要があるという認識の下、取組を進めており、今後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。
23	個人 （4）	4．1．3　安全なIoTシステムの構築	「5G（第5世代）」におけるサイバーセキュリティ対策には種類がある。IoT機器を接続すると、「サテライト、クラウド、エッジ」等のシステムに対し、サイバーセキュリティー対策が重要と、私は考えます。	先端技術を利活用したイノベーションを支えるサイバーセキュリティに関する賛同意見として承りました。内容については、今後の施策の検討や実施の推進に当たって参考とさせていただきます。
24	BSA｜ザ・ソフトウェア・アライアンス	4．1．3　安全なIoTシステムの構築	IoTセキュリティ基準は、当該基準が世界中における同様の取組みと継続的に整合性を保っていることが重要。IoT機器は、機能、能力及びリスクに関して極めて幅広い多様性があることを考慮し、IoTセキュリティ基準は、リスクベースで柔軟性を有するものであることが重要。	安全なIoTシステムの構築に関する賛同意見として承りました。内容については、今後の施策の検討や実施の推進に当たって参考とさせていただきます。
25	株式会社ラック	4．1．3　安全なIoTシステムの構築	IoTを中核とする「Society5.0」実現のためには、安全保障の観点から、「サイバーセキュリティ産業化」をも視野に、国主導により、トラストチェーンインフラ国産化に向けた取組みに早急に着手願いたい。	国産のサイバーセキュリティ製品・サービスに関しては、年次計画において、「内閣官房において、研究・技術開発に資する産学官連携による体制構築の検討を含め、国産のサイバーセキュリティ製品・サービスの育成も見据えた、我が国のサイバーセキュリティの研究・技術開発に関する取組方針を取りまとめると共に、関係機関との連携の下、施策を推進する。」としております。御意見については今後の取組の検討や実施の推進に当たっての参考とさせていただきます。
26	個人 （13）	4．1．3　安全なIoTシステムの構築	国内企業（可能であれば政府が支援をする形）で進めて欲しい	安全なIoTシステム構築に向けて、サイバーセキュリティの体系の整備や脆弱性対策に係る体制の整備を行うこととしております。内容については、今後の施策の検討や実施の推進に当たって参考とさせていただきます。
27	個人 （16）	4．1．3　安全なIoTシステムの構築	初期のままの利用を制限すること。誰でも利用するそのことを踏まえ、アクセシビリティにすること。設定が困難または面倒あったりなどがあると脆弱性になる。業界へ積極的な対策の後押しと一般（多様な）への啓発をすること。	サイバーセキュリティ戦略（平成30年7月27日閣議決定）では、官民が連携して、IoT機器の脆弱性について、設計・製造、運用、そして破棄までのライフサイクルを見通したサイバーセキュリティ対策や、ネットワーク上の脆弱なIoT機器の対策等のための体制整備が必要であるとされており、今後の施策の実施や検討に当たって、参考とさせていただきます。
28	個人 （1）	4．2．1　国民・社会を守るための取組	某大型掲示板はじめとするネットでの荒らし、煽り、ネガティブキャンペーンといった書き込みの厳罰化をお願いします。 もしそういう事を書き込んだら2度と書き込めないようにして下さい。	ご指摘の書き込みが具体的に何を指すのか必ずしも明確ではないと考えられますが、今後も、サイバーセキュリティ戦略（平成30年7月27日閣議決定）に基づき、国民が安全で安心して暮らせる社会の実現のため、サイバー犯罪への対策を推進していきます。

2019年度に実施すべき施策に関する意見募集の結果一覧

通しNo	提出者	該当箇所	意見の要旨	主な考え方
29	個人 (11)	4．2．1　国民・社会を守るための取組	国家機密だけではなく企業秘密に関してもカバーするスパイ防止法を制定し、内部からのセキュリティ破壊者（侵入者）、情報漏洩者に対する罰則を厳罰化し、不法活動の防止を図るべきと考える。	いわゆるスパイ防止法の必要性については様々な議論があるものと承知しておりますが、特定秘密保護法や不正競争防止法に基づき、特定秘密や営業秘密の保護を図っているところであり、引き続き秘密の保護に努めてまいります。
30	（一社）日本経済団体連合会 産業技術本部	4．2．1　国民・社会を守るための取組	政府が、情報インフラ等の信頼性を評価するための検証や政府調達における運用改善等について検討し対策を進める際、海外の取組も参考にし、現実的かつ分かりやすいものとすべきである。	政府では、サプライチェーン・リスク対策として、IT調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せを行い、年次計画において、政府の重要業務に係る情報システム・機器・役務等の調達におけるサイバーセキュリティ上の深刻な悪影響を軽減するための取組を開始したところです。円滑な調達が行われるよう、頂いた御意見も参考に関係省庁と連携して取り組んで参ります。
31	株式会社ラック	4．2．1　国民・社会を守るための取組	研究者やセキュリティベンダー等がマルウェア解析やセキュリティ事業を安心して実施できるよう、いわゆるコンピュータ・ウイルスに関する罪の成立条件を具体的かつ網羅的に提示願いたい。	いわゆるコンピュータ・ウイルスに関する罪については、その構成要件は法律に明示されており、その考え方についても法務省ウェブサイト（http://www.moj.go.jp/content/000076666.pdf）で公表しております。
32	（一社）情報通信ネットワーク産業協会	4．2．1　国民・社会を守るための取組	海外の事例も踏まえ、日本に新たな機器セキュリティ検証・評価の仕組みを構築することが、今後の日本の情報通信インフラおよび日本経済の発展のために重要と考える。	政府では、サプライチェーン・リスク対策として、IT調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せを行い、年次計画において、政府の重要業務に係る情報システム・機器・役務等の調達におけるサイバーセキュリティ上の深刻な悪影響を軽減するための取組を開始したところです。また、産学官が連携した、サプライチェーンリスクに対応するための技術検証体制の整備に向けた取組など、サイバーセキュリティの研究・技術開発を政府一体となって進めてまいります。
33	個人 (13)	4．2．1　国民・社会を守るための取組	5G通信インフラへの注目が集まる中、日本は、国民や社会を守るために、中国産や影響力を行使されている企業を選定対象外とすべきである。	特定の国や企業を対象としたものではありませんが、政府では、サプライチェーン・リスク対策として、IT調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せを行い、年次計画において、政府の重要業務に係る情報システム・機器・役務等の調達におけるサイバーセキュリティ上の深刻な悪影響を軽減するための取組を開始したところです。

2019年度に実施すべき施策に関する意見募集の結果一覧

通しNo	提出者	該当箇所	意見の要旨	主な考え方
34	個人 （6）	4．2．2　官民一体となった重要インフラの防護	重要インフラを担う企業（下位請負含む）に対してはエンドポイントセキュリティを徹底させる事が必要と感じる。	ご指摘のエンドポイントセキュリティについては、「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第5版）」（平成30年4月4日サイバーセキュリティ戦略本部決定）等に基づき、「マルウェアからの保護」、「運用ソフトウェアの管理」、「技術的脆弱性管理」等を求める取組を進めており、年次計画では、2章2.2 (1)(ア)において、「各分野の安全基準等の整備・浸透を促進する。」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。
35	個人 （10）	4．2．2　官民一体となった重要インフラの防護	IPAの実施する情報処理技術者試験の所持者と工程を関連付けて、特に官公庁及び自治体、金融、生活インフラ系企業のシステム構築については、無免許無資格者による作業を早急に法により禁止すべきである。 経済産業省においては、直ちに義務化に向けた法制度検討、資格取得支援制度の拡充を実施すべきである。	自治体・金融機関等の重要インフラ事業者等におけるシステム構築については、「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第5版）」（平成30年4月4日サイバーセキュリティ戦略本部決定）において、情報セキュリティ要件を踏まえた情報システムの取得について定める等、適切な対応を求めており、年次計画では、2章2.2 (1)(ア)において、「各分野の「安全基準」等の整備・浸透を促進する。」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。
36	個人 （10）	4．2．2　官民一体となった重要インフラの防護	地方公共団体のうち、県及び政令市においては、IPA高度資格とITSSスキルマップに対応した情報系人事施策の実施について着手すべきである。	地方公共団体等における人材育成については、「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」（平成29年4月18日サイバーセキュリティ戦略本部決定、平成30年7月25日サイバーセキュリティ戦略本部改定）等に基づき、必要なセキュリティ人材像の定義、情報セキュリティに係る訓練・演習、資格取得等の具体的な人材育成策を推進しているところです。年次計画では、総務省による地方公共団体向けの取組等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。
37	個人 （10）	4．2．2　官民一体となった重要インフラの防護	官公庁・生活インフラ企業・県及び政令市については、情報処理安全確保支援士のCISOを必置化すべき。	県及び政令市を含む重要インフラ事業者等における人材育成については、「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」（平成29年4月18日サイバーセキュリティ戦略本部決定、平成30年7月25日サイバーセキュリティ戦略本部改定）等に基づき、必要なセキュリティ人材像の定義、情報セキュリティに係る訓練・演習、資格取得等の具体的な人材育成策を推進しているところです。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。

2019年度に実施すべき施策に関する意見募集の結果一覧

通しNo	提出者	該当箇所	意見の要旨	主な考え方
38	富士通クラウドテクノロジーズ株式会社（JASA/CAIS情報セキュリティ監査人補）	4．2．2　官民一体となった重要インフラの防護	クラウドサービスについては、国内外でルール化が進む中、重要インフラの防護という観点から、「国策クラウド」を作った方がいいのではないか。	国内外の法令や評価制度等について、国際動向も踏まえた望ましいデータ管理（クラウドサービスを含む）の在り方について、「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第5版）等の改定」の検討を進めており、年次計画においても1章1.1 (2)において「「データ管理の在り方」を同指針に追加するとともに所要の修正を行う改定を実施し、改定後の指針については、従来と同様、関係省庁等が連携し、各重要インフラ分野の安全基準等への反映を通じて事業者へ浸透させる取組を促進していく。」としているところです。 御意見については、このような施策の検討や実施の推進に当たって参考にさせていただきます。
39	個人 （10）	4．2．3　政府機関等におけるセキュリティ強化・充実	「Society5.0以前」の社会インフラでは、各工程について厳密な資格制度が設けられている。同様に、「Society5.0」において、重要な社会インフラとなる情報システム及び通信について、IPAの実施する情報処理技術者試験の所持者と工程を関連付けて、特に官公庁及び自治体、金融、生活インフラ系企業のシステム構築については、無免許無資格者による作業を早急に法により禁止すべき。	官公庁等の調達においては、必要に応じ、システム構築を確実に実施できるように資格要件を定めるなどして、適切に対応を行っているところです。 権利制限に関する制度をシステム構築に適用することの適否については慎重に議論する必要はありますが、いただいた御意見は、今後の施策の実施や検討に当たって参考とさせていただきます。
40	スプランクサービス ジャパン合同会社	4．2．3　政府機関等におけるセキュリティ強化・充実	我が国においても、中枢、末端に至るセイバーセキュリティ情報を採取、分析することで日本政府における監視体制が確立できるものと考える。 このため、各府省庁の端末におけるリアルタイム情報収集・分析による、決められた時間内にアラートを発することのできる監視の仕組みが必要と考える。	端末、サーバ、通信回線等の監視及び監視するイベント情報の効率的活用について現行の統一基準群に記載しております。 また、年次計画において、情報提供の迅速化・高度化に資するため、情報収集・分析機能強化等の検討を行うこととしています。 いただいた御意見は、施策の実施や検討に当たって、参考とさせていただきます。
41	個人 （11）	4．2．3　政府機関等におけるセキュリティ強化・充実	政府機関等の内部にスパイが潜入していた場合を考え、スパイ防止法を制定し、内部からのセキュリティ破壊者（侵入者）に対する罰則を厳罰化すべき。	年次計画において、引き続き、統一基準群に定めた内部からの不正操作を防止するための措置や情報システムが不正操作等されていないことの検証を行うために必要なログを取得する規定等に基づいて取組を行ってまいります。 いただいた御意見は、今後の施策の実施や検討に当たって、参考とさせていただきます。

2019年度に実施すべき施策に関する意見募集の結果一覧

通しNo	提出者	該当箇所	意見の要旨	主な考え方
42	BSA｜ザ・ソフトウェア・アライアンス	4．2．3　政府機関等におけるセキュリティ強化・充実	サイバーセキュリティ戦略は、政府機関でのクラウド推進の重要性を認識。政府のメッセージの一貫性を保ち、関係政府機関等の誤解を生まないよう、クラウドに関する過去のガイダンスの一部の再検討を要望。特に、政府統一基準のうちクラウドがリスクを高めているような記載（4.1.4）及び物理的ネットワーク分離がセキュリティ上解決策であるとの推奨（5.2.1（2）a項）を懸念。 「政府情報システムにおけるクラウドサービスの利用に関する基本方針」における「クラウド・バイ・デフォルト原則」を評価。経済産業省と総務省によるクラウドサービス安全性評価の取組が、当該方針に適合し、世界的に他の政府機関クラウド安全性評価及び認証スキームと相互運用可能で、国際的に認められた標準に適合するよう要望。	年次計画において、引き続き、政府機関におけるクラウドサービスの利用状況を適宜調査し、課題等の把握に努めてまいります。 いただいた御意見は、今後の施策の実施や検討に当たって参考とさせていただきます。
43	個人 （15）	4．2．3　政府機関等におけるセキュリティ強化・充実	サイバー攻撃等に対し安全保障上のグランドデザインについて、まずは我が国の中枢機能のセキュリティ強化、充実を、最もはじめに重点的になすべき。 世代を超えたオールジャパンで取り組んで頂きたい。	年次計画において、政府機関等における情報システムのセキュリティ対策の進捗状況の把握や、取組の促進に向けて必要な支援を行うなど、政府機関等全体としての情報セキュリティ水準の維持・向上を図るべく必要な施策を進めてまいります。 いただいた御意見は、今後の施策の実施や検討に当たって参考とさせていただきます。
44	個人 （16）	4．2．3　政府機関等におけるセキュリティ強化・充実	高度な攻撃が可能になればリスクが高まるため、 専任担当と、研修、緊急時など、実際のリスクの軽減と対処を積極的に出来る体制を作ること。	政府機関等において発生した情報セキュリティインシデントに対処する体制として、各政府機関等にCSIRTを設置しています。また、政府一体となった対応が必要となる情報セキュリティインシデントに対する機動的な支援体制として、内閣サイバーセキュリティセンターに情報セキュリティ緊急支援チーム（CYMAT）を設置しています。なお、各政府機関等のCSIRT要員及びCYMAT要員の能力及び技能の向上に向けた研修等を実施しております。 御意見を踏まえ、年次計画において、引き続き、CSIRT及びCYMATに対して研修等の実施を盛り込み、体制の強化を行ってまいります。
45	株式会社ラック	4．2．5　2020年東京大会とその後を見据えた取組	「サイバーセキュリティ対処調整センター」において、関連情報を民間の知見をも活用しつつ幅広く収集・分析する等の取組みを推進してほしい。	年次計画において、対処態勢の整備の取組を実施することとしております。サイバーセキュリティ対処調整センターの情報共有システムには、サイバーセキュリティ関係機関や重要サービス事業者等並びにCTI情報を提供してくださる事業者の方々が参加し、民間の方々の知見が活用できる仕組みになっております。今後は、その仕組みを有効に働かせることが肝要と考えております。 御意見については今後の取組の検討や実施の推進に当たっての参考とさせていただきます。

2019年度に実施すべき施策に関する意見募集の結果一覧

通しNo	提出者	該当箇所	意見の要旨	主な考え方
46	個人 （11）	4．2．6　従来の枠を超えた情報共有・連携体制の構築	大規模サイバー攻撃等を防ぐために、諸外国の諜報機関（CIA、MI6等）のような体制を整備し、水面下の情報を確実に収集し、それを生かせる様にすべき。	引き続き諸外国の様々な機関とも連携して、情報収集に努めてまいります。
47	株式会社ラック	4．2．6　従来の枠を超えた情報共有・連携体制の構築	内閣官房が中心となり構築する情報共有体制における情報共有を促進する観点から、当該情報共有に貢献した参加者が適切に評価され、また適切に保護される環境の整備を加速願いたい。	2018年12月に改正されたサイバーセキュリティ基本法に基づき、2019年4月1日に、官民の多様な主体が連携してサイバーセキュリティに関する情報共有を行い、サイバー攻撃による被害の発生及び被害の拡大を防ぐための「サイバーセキュリティ協議会」が組織されました。 同協議会については、年次計画においても、実際の運用の経験や各主体の意見を丁寧に踏まえ、必要に応じて運用ルールやシステムを不断に見直すこととしており、頂いた御意見は、同協議会における情報共有促進のための参考とさせていただきます。
48	個人 （6）	4．2．7　大規模サイバー攻撃事態等への対処態勢の強化	大規模サイバー攻撃事態等への対処態勢強化として、まず入念なリスクの洗い出しとリスクの解消や低減を最優先で行って欲しい。	「4.2.7　大規模サイバー攻撃事態等への対処態勢の強化」では、あらゆる対策を行ったうえで、万が一、事態が発生してしまった場合に備えた施策・取組を記載しています。ご指摘のとおり、まずは事態が発生しないような取組が重要であることから、「4.2.2　官民一体となった重要インフラの防護」、「4.2.3　政府機関等におけるセキュリティ対策の強化・充実」及び「4.2.5　2020年東京大会とその後を見据えた取組」に対応するものとして、年次計画において重要インフラ事業者等におけるリスクマネジメントの推進、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・デザインの推進、2020年東京大会の安全に対する脅威及びリスクの分析、評価等の取組を行っているところです。ご意見については、取組の実施や検討に当たって、参考とさせていただきます。
49	富士通クラウドテクノロジーズ株式会社（JASA/CAIS情報セキュリティ監査人補）	4．3．2　我が国の防御力・抑止力・状況把握力の強化	自衛隊のサイバー防衛隊に日本企業に所属する日本国籍所有者だけが資格を有する予備自衛官制度を作り、民間企業のセキュリティ人材をそれに任命するのが妥当と考える。	防衛省における民間のセキュリティ人材の活用策については、不断に検討してまいります。
50	個人 （15）	4．3．2　我が国の防御力・抑止力・状況把握力の強化	サイバーセキュリティについて、安全保障上も危機感をもって、グランドデザインをし、官民一体、オールジャパンで総力をあげて取り組んでいただきたい。その先導役を果たしていただくことを切に希望する。	サイバーセキュリティ戦略（平成30年7月27日閣議決定）に基づき、国民・社会を守るための取り組みや重要インフラ防護、政府機関のセキュリティ強化、我が国の防御力、抑止力、状況把握の強化等の取り組みを内閣サイバーセキュリティセンターが中心となり官民一体となって進めてまいります。ご指摘の点についても今後の取組の検討や実施の推進に当たって参考とさせていただきます。

2019年度に実施すべき施策に関する意見募集の結果一覧

通しNo	提出者	該当箇所	意見の要旨	主な考え方
51	BSA｜ザ・ソフトウェア・アライアンス	4．3．3　国際協力・連携	多くの国々が未だ新たなサイバーセキュリティ法の策定・施行の初期段階にある東南アジア地域に注力した国際的キャパシティ・ビルディング支援活動を維持し拡大するよう希望。	内閣官房、警察庁、総務省、外務省、経済産業省、その他関係府省庁・機関が相互に連携、情報共有を行い、ASEAN加盟国をはじめとする各国における能力構築支援に積極的に取り組んでいます。ご指摘の点についても参考とさせていただき、年次計画において「関係府省庁・機関が相互に連携、情報共有を行い、各国における効果的な能力構築支援に積極的に取り組む」としております。
52	株式会社ラック	4．3．3　国際協力・連携	アジア太平洋地域におけるサイバーセキュリティ人”才”の育成支援事業については、国内外で実績のある手法を活用しつつ、「サイバーセキュリティ産業化」をも視野に推進願いたい。	内閣官房、警察庁、総務省、外務省、経済産業省、その他関係府省庁・機関が相互に連携、情報共有を行い、ASEAN加盟国をはじめとする各国における能力構築支援に積極的に取り組んでいます。ご指摘の点についても参考とさせていただき、年次計画において「関係府省庁・機関が相互に連携、情報共有を行い、各国における効果的な能力構築支援に積極的に取り組む」としております。 総務省では、日ASEANサイバーセキュリティ能力構築センター（AJCCBC）に関しては、ASEAN各国の政府機関及び重要インフラ事業者のサイバーセキュリティ担当者等を集め、実践的サイバー防御演習（CYDER）をはじめとするサイバー演習を提供しています。今後とも、民間企業と連携しつつ、ASEAN域内のサイバーセキュリティ能力向上の充実に努めてまいります。 経済産業省は、「サイバーセキュリティ産業化」としては、ベトナム、バングラデシュ、カンボジア、ラオス、ミャンマーといったASEAN地域において、サイバー攻撃に強い電力制御システム（SCADA）の導入に向け、現地の電力企業への支援に取り組んでいます。
53	個人 （3）	4．4．1　人材育成・確保	IPA主催の資格試験の時期を4月・10月から、7月・1月への変更を検討してほしい。	情報処理技術者試験及び情報処理安全確保支援士試験につきましては、年間合計約50万人が受験する試験となっています。受験者の混乱を避ける観点から、試験の実施期日の変更については、慎重に検討する必要があります。御意見については、今後の検討にあたっての参考とさせていただきます。
54	個人 （3）	4．4．1　人材育成・確保	IPA主催のセキュリティマネジメント試験をCBT対応としてほしい。	情報セキュリティマネジメント試験の午後試験においては、1つの事例に対し、複数の質問を設ける出題形式をとっており、CBTになじまない試験となっております。御意見については、今後の検討にあたっての参考とさせていただきます。
55	個人 （6）	4．4．1　人材育成・確保	態勢強化としては、ホワイトハッカーなどの技術者の育成は第一に挙げられる事が多いが、啓蒙や教育が大きな力となる。国民の意識から対処態勢の意識が欲しい。	国民一人一人がサイバーセキュリティに対する意識・理解を醸成し、サイバー空間における様々なリスクに対して対処できるよう、全員参加による協働に向けた取組を推進しているところです。御意見については取組の実施や検討に当たって、参考とさせていただきます。

2019年度に実施すべき施策に関する意見募集の結果一覧

通しNo	提出者	該当箇所	意見の要旨	主な考え方
56	オフィスVG2	4．4．1　人材育成・確保	「情報処理安全確保支援士(登録セキスペ)」の役割と位置付けについて明記して欲しい。例えば、今度実施される「NOTICE」に関して、一定の権限を課してその実施を代行出来る様にしてもよいのではないか。もちろん、そのための法整備は必要であり、すぐにというわけにはいかないと思うが、国が設けた資格故に、一定の役割と権限を付与して然るものと考える。	情報処理安全確保支援士（登録セキスペ）制度は、平成29年4月に登録を開始し、2019年4月現在での登録者数は18，330人となったところ。また、登録開始から3年目となり、ある程度の運用実績も積み上がってきたことから、年次計画において「情報処理安全確保支援士制度の着実な実施に向けて必要な措置を講じる」としており、制度運用の更なる改善を検討する予定です。御意見については、今後の検討にあたっての参考とさせていただきます。
57	個人 (10)	4．4．1　人材育成・確保	有資格者による組織強化に直ちに着手すべきである。支援士としてスキルが担保されている人材を直ちにCISOに就け、これらの業界に対して異動の抑制を要請するとともに、それらに対するより高度な研修を実施するほうが有効性が高いと考える。 よって、官公庁については、情報処理安全確保支援士のCISOを必置化すべき。	官公庁においても、体制の整備を図っているほか、人材育成の観点から、情報システム統一研修（総務省主催）を実施しています。 CISOについては、各府省庁において、職歴・保有資格等を勘案し任命しているものと承知しており、頂いた意見については、今後の体制整備・人材育成の参考とさせていただきます。
58	個人 (10)	4．4．1　人材育成・確保	資格者が高く評価されるようになるはずであるし、そうすれば企業もそこにお金を投じる動機付けにもなる。一方で、官公庁も人材確保の観点から、制度でもって民間の取り組みを刺激するような取り組みが必要であると考える。 よって、IPAの資格者、上級ベンダー資格取得者に対して一定の処遇とすることについて法制化すべき。	官公庁においては、一定の業務経験と研修の修了（特定の資格による代替可）を要件としてスキル認定を与え、その者が専門性・特殊性の高い業務に従事した際には、一定の給与上の評価をしています。御意見については、今後の検討にあたっての参考とさせていただきます。 情報処理技術者試験などの試験合格者に一定の処遇を与えるか否かは、民間企業などが自社の業務内容に応じて判断すべき事項であると考えております。
59	個人 (11)	4．4．1　人材育成・確保	基礎的ITリテラシーの標準装備へ向けて、ITパスポート試験の受験を業種を問わず全てのビジネスパーソン、学生たちへ奨励してはどうか。	ITパスポート試験は、ITを利活用するすべての社会人が備えておくべきITに関する基礎的な知識が証明できる国家試験であり、いただきましたご意見のとおり、普及に努めてまいります。
60	個人 (11)	4．4．1　人材育成・確保	ITパスポート試験を合否制からスコア制へと変更して、ITリテラシースタンダード（ITLS）1 級、2級などを認定する方式に改めてはどうか。	ITパスポート試験については、既にスコア表示にも対応しております。また、当該試験は、ITを利活用するすべての社会人が備えておくべきITに関する基礎的な知識が証明できる国家試験であり、これに満たないITLS2級を認定する意義は認められないことから、検討する予定はありません。ご意見については今後の取組の検討や実施の推進に当たっての参考とさせていただきます。
61	個人 (11)	4．4．1　人材育成・確保	情報セキュリティマネジメント試験を改組して「情報システムアドミニストレータ試験」を新たに創設してはどうか。	情報セキュリティマネジメント試験は、情報セキュリティを担う人材の育成・確保を目的に、情報セキュリティマネジメントに関する基本的なスキルを認定する試験として、平成28年4月から開始しされました。いわゆる情報システムアドミニストレータとは、主旨がことなるものであり、情報セキュリティマネジメント試験の改組を検討する予定はありません。

2019年度に実施すべき施策に関する意見募集の結果一覧

通しNo	提出者	該当箇所	意見の要旨	主な考え方
62	個人 (11)	4．4．1　人材育成・確保	情報システムアドミニストレータ試験については、以下のとおりにしてはどうか。 ・略号：ID　午前試験⇒80問、120分 ・情報セキュリティに関する出題×25問 ・FE試験よりテクノロジ、マネジメント、ストラテジ、各10問 ・iパスの公開問題よりAI、ビッグデータ、IoTから25問 午後試験⇒120分 ・情報セキュリティマネジメントに関する出題×2問（各20点） ・シスアド的なスキルを問うための中問×4題を出題（各15点）	情報セキュリティマネジメント試験は、情報セキュリティを担う人材の育成・確保を目的に、情報セキュリティマネジメントに関する基本的なスキルを認定する試験として、平成２８年４月から開始しされました。いわゆる情報システムアドミニストレータとは、主旨がことなるものであり、情報セキュリティマネジメント試験の改組を検討する予定はありません。
63	BSA｜ザ・ソフトウェア・アライアンス	4．4．1　人材育成・確保	サイバーセキュリティ人材育成が優先課題。現在の人材における不均衡に対処するため、多くの女子学生がサイバーセキュリティを含むコンピューターサイエンス教育の道を進むインセンティブ付与は特に重要。	イノベーションを推進する観点から、人材の多様性の確保を推進していくことへの賛同意見として承りました。
64	株式会社ラック	4．4．1　人材育成・確保	大規模災害の被災地の復興支援と人材定着に向け 、セキュリティ人〝才〟育成をベースとするICT利活用事業を実施願いたい。	イノベーションを推進する観点からも人材の多様性の確保に取り組んでいくこととしております。
65	株式会社ラック	4．4．1　人材育成・確保	人材の流動性・地位の向上、安定的な雇用機会の創出並びにキャリアパス及び適切な処遇の確保に向けた所要のスキルの明確化、素養を含む保持スキルの「見える化」、キャリアパスの例示その他の取組みを総合的に推進願いたい。	産学官が連携して人材の需要や人材育成施策に関する情報共有等の連携を図りつつ、人材育成・確保を強化するとともに、人材の多様性の確保を推進していくことが重要としております。御意見については今後の取組の検討や実施の推進に当たっての参考とさせていただきます。
66	株式会社ラック	4．4．1　人材育成・確保	各地において情報リテラシー・モラルに関する普及啓発に取組む者に対する財政的・人的支援の強化、インセンティブ付与策を検討願いたい。	情報リテラシー・モラルに関する普及啓発については、年次計画において「文部科学省において、ネットモラルキャラバン隊を通じ、スマートフォン等によるインターネット上のマナーや家庭でのルールづくりの重要性の普及啓発を実施する。」としております。御意見については取組の実施や検討に当たって、参考とさせていただきます。
67	株式会社ラック	4．4．1　人材育成・確保	若年層に対する情報モラル教育の一環として、普及・啓発を強化願いたい。 かかる指導層を確保するため、特にサイバーセキュリティに関する法制度に関するものについてもよりいっそう盛り込んでいただきたい。	若年層に対する普及啓発に寄与する教員に関する取組として、年次計画において「独立行政法人教職員支援機構と連携し、新学習指導要領の趣旨を踏まえ、情報通信技術を活用した指導や情報モラルに関する指導力の向上を図るため、各地域で情報教育の中核的な役割を担う教員等を対象とした研修を実施する。」としております。御意見については取組の実施や検討に当たって、参考とさせていただきます。

2019年度に実施すべき施策に関する意見募集の結果一覧

通しNo	提出者	該当箇所	意見の要旨	主な考え方
68	株式会社ラック	4．4．1　人材育成・確保	わが国のセキュリティ若手人材が海外の有為な若手人材との交流等を通じて国際感覚を身に着けるための実践的機会の創出	我が国のセキュリティ若手人材が海外の若手人材との交流等ができる実践的な機会については、NPO日本ネットワークセキュリティ協会が実施する「SECCON国際CTF大会」に対し、経済産業大臣賞を交付することで支援をしており、年次計画においても、「「CTF」に対する後援等を通じて、普及・広報の支援を行う。」とし、引き続き支援を行う予定です。御意見については取組の実施や検討に当たって、参考とさせていただきます。
69	大日本印刷株式会社	4．4．1　人材育成・確保	情報処理安全確保支援士（登録セキスペ）制度において、「技能検定」も導入し、「事態対処可能なサイバーセキュリティ技術者育成」が必要と考えます。	情報処理安全確保支援士（登録セキスペ）制度は、平成29年4月に登録を開始し、2019年4月現在での登録者数は18，330人となったところ。また、登録開始から3年目となり、ある程度の運用実績も積み上がってきたことから、年次計画において「情報処理安全確保支援士制度の着実な実施に向けて必要な措置を講じる」としており、制度運用の更なる改善を検討する予定です。御意見については、今後の検討にあたっての参考とさせていただきます。
70	大日本印刷株式会社	4．4．1　人材育成・確保	登録セキスペの人数に応じたポイント制度を導入し、登録人数に応じた税制優遇措置、サイバーセキュリティ保険の減額などの具体的インセンティブが必要	情報処理安全確保支援士（登録セキスペ）制度は、平成29年4月に登録を開始し、2019年4月現在での登録者数は18，330人となったところ。また、登録開始から3年目となり、ある程度の運用実績も積み上がってきたことから、年次計画において「情報処理安全確保支援士制度の着実な実施に向けて必要な措置を講じる」としており、制度運用の更なる改善を検討する予定です。御意見については、今後の検討にあたっての参考とさせていただきます。
71	大日本印刷株式会社	4．4．1　人材育成・確保	緊急の有事対応を想定しサイバーセキュリティ人材データベース構築、また、当該人材を育成・確保するための認定講習、認定講習機関の登録制度などの仕組みが必要	防衛省における民間のセキュリティ人材の活用策については、不断に検討していくとともに、人材育成・確保に係る各種取組を進めてまいります。
72	個人（16）	4．4．1　人材育成・確保	戦略的に質の担保をしその向上とその維持。各分野をつなげる役割やそれらの人材などが足かせにならないように	御意見の趣旨が必ずしも明確ではないと考えられますが、御意見として承ります。
73	個人（7）	4．4．2　研究開発の推進	事業者での調達に関する調達システムおよび調達システムを構成する個別の IT/ICT機器の要求技術仕様を検討・推奨、システムを各IT/ICT機器の安全性を検証するための検証技術仕様とその検証環境、ならびに実機を用いた検証を実施する産官学の組織を創設すべき	サイバー攻撃の脅威を踏まえた実践的なサイバーセキュリティの研究開発が必要であるとの認識の下、システムに組み込まれている機器やソフトウェアについて検証できる手段を確保することが重要としており、年次計画において「内閣官房において、関係府省と連携し、国産技術の確保・育成のための取組や、政府調達における活用も可能な、産学官連携による、サプライチェーンリスクに対応するための技術検証体制の整備に向けた取組を進める。」として、引き続き、取組を推進してまいります。

2019年度に実施すべき施策に関する意見募集の結果一覧

通しNo	提出者	該当箇所	意見の要旨	主な考え方
74	個人 （8）	4．4．2　研究開発の推進	「政府機関や重要インフラ事業者等が提供するサービスの全体の基盤となる信頼できる情報インフラについて、国際海底ケーブル等のインフラ設備の防護の強化を含めた整備を促進する。このため、信頼性を評価するための検証や政府調達における運用改善等について検討し、対策を進める。」とされております。2019年度においては、具体的かつ現実的な計画の策定をし取り組むことが重要と考えます。 日本に新たな予断の無い機器セキュリティ検証・評価の仕組みを構築することが、今後の日本の情報通信インフラおよび日本経済と社会の発展のために重要と考えます	サイバー攻撃の脅威を踏まえた実践的なサイバーセキュリティの研究開発が必要であるとの認識の下、システムに組み込まれている機器やソフトウェアについて検証できる手段を確保することが重要としており、年次計画において「内閣官房において、関係府省と連携し、国産技術の確保・育成のための取組や、政府調達における活用も可能な、産学官連携による、サプライチェーンリスクに対応するための技術検証体制の整備に向けた取組を進める。」として、引き続き、取組を推進してまいります。
75	個人 （12）	4．4．2　研究開発の推進	情報通信機器の安全性を，社会体制，地理的，経済的な要因とは独立して，技術的に検証する必要性が，今後ますます重要になると考えられる．通信機器に関するソフトウェア・ハードウェアセキュリティの専門家からなる検討委員会を発足させ，そこでの検討結果を結果をうけ，機器単位で安全性の認証をおこなう機構を発足させることを提言する．	サイバー攻撃の脅威を踏まえた実践的なサイバーセキュリティの研究開発が必要であるとの認識の下、システムに組み込まれている機器やソフトウェアについて検証できる手段を確保することが重要としており、年次計画において「内閣官房において、関係府省と連携し、国産技術の確保・育成のための取組や、政府調達における活用も可能な、産学官連携による、サプライチェーンリスクに対応するための技術検証体制の整備に向けた取組を進める。」として、引き続き、取組を推進してまいります。
76	株式会社ラック	4．4．2　研究開発の推進	いわゆるセーフハーバールール（例：登録セキスペその他の資格保持者が研究その他の適正な業務を遂行する際に免責される等）の導入を検討願いたい。	情報処理安全確保支援士（登録セキスペ）制度は、平成29年4月に登録を開始し、2019年4月現在での登録者数は18，330人となったところ。また、登録開始から3年目となり、ある程度の運用実績も積み上がってきたことから、年次計画において「情報処理安全確保支援士制度の着実な実施に向けて必要な措置を講じる」としており、制度運用の更なる改善を検討する予定です。また、ご指摘の「いわゆるセーフハーバールール」が具体的に何を指すのか必ずしも明確ではないと考えられますが、例えば、不正指令電磁的記録作成等罪（刑法168条の2）については，「実行の用に供する目的」や「正当な理由がない」ものであることが要件とされ、これらの要件を満たさない場合には、処罰の対象とされないところです。また、不正アクセス行為の禁止等に関する法律第2条第4項においては、アクセス管理者の承諾を得て行う行為は不正アクセス行為に当たらないとされており、同行為は処罰の対象とされないところです。
77	株式会社ラック	4．4．2　研究開発の推進	AI時代におけるサイバーセキュリティ確保の観点から大きな脅威となる各種課題についての研究開発を推進願いたい。	サイバー空間におけるイノベーションの進展とそれに値するサイバー攻撃の脅威を踏まえた実践的なサイバーセキュリティ研究開発を進めることとしております。御意見については取組の実施や検討に当たって、参考とさせていただきます。

2019年度に実施すべき施策に関する意見募集の結果一覧

通しNo	提出者	該当箇所	意見の要旨	主な考え方
78	個人 （6）	4．4．3　全員参加による協働	事件があれば一部を高らかに報道させてしまう事が、国民にとっては最大の防御力・抑止力・状況把握力の強化に繋がると感じる。AC（公共広告機構）を上手く利用しても良いと思う。	国民一人一人がサイバーセキュリティに対する意識・理解を醸成し、サイバー空間における様々なリスクに対して対処できるよう情報発信等の取組を推進しているところです。御意見については取組の実施や検討に当たって、参考とさせていただきます。
79	株式会社ラック	4．4．3　全員参加による協働	「全員参加による協働」推進の観点から一定の意義・有益性が認められるものについて、一般ユーザがスマートフォン等で簡便に利用できるようアプリ化・ツール化する取組みを推進願いたい。	「サイバーセキュリティ意識・行動強化プログラム」（平成31年1月24日サイバーセキュリティ戦略本部決定）においてポータルサイトによる取組の見える化及び連携推進を掲げているところ、御意見踏まえ、年次計画において、「内閣官房において、関係機関と連携し、人材育成や普及啓発に関する官民の様々な取組みを集約するポータルサイトを構築し、対象となる層や伝達手法の見える化及び連携を推進するための検討を行う。」と記載いたしました。
80	株式会社ラック	4．4．3　全員参加による協働	網羅的・一覧性をもってサイバーセキュリティに関する普及啓発・支援ポータルに掲載される等、当該コンテンツの流通・利活用を促進願いたい。	「サイバーセキュリティ意識・行動強化プログラム」（平成31年1月24日サイバーセキュリティ戦略本部決定）においてポータルサイトによる取組の見える化及び連携推進を掲げているところ、御意見踏まえ、年次計画において、「内閣官房において、関係機関と連携し、人材育成や普及啓発に関する官民の様々な取組みを集約するポータルサイトを構築し、対象となる層や伝達手法の見える化及び連携を推進するための検討を行う。」と記載いたしました。
81	個人 （16）	4．4．3　全員参加による協働	障害者や高齢者なども全員参加による協働が出来るようにアクセシビリティにすること	国民一人一人がサイバーセキュリティに対する意識・理解を醸成し、サイバー空間における様々なリスクに対して対処できるようにするため、全員参加による協働に向けて国民一人一人を対象とした取組を記載しているところです。内容については、今後の施策の検討や実施の推進に当たって参考とさせていただきます。
82	個人 （6）	5．推進体制	サイバー空間の維持管理はもはや民間企業だけで担えるものでは無い。守るための取り組みとして最善のものは法整備であり、急務である。これらは旧来の商法や刑法を改革していかねばならない。	ご指摘の「法整備」が具体的に何を指すのか必ずしも明確ではないと考えられますが、サイバーセキュリティ基本法の一部を改正する法律（平成30年法律第91号）などが成立しており、それに基づく取組を進めております。
83	個人 （4）	5．推進体制	「内閣官房内閣サイバーセキュリティーセンター（NISC）」を昇格させ「内閣サイバーセキュリティー庁」を導入する事が望ましい。 「5G（第5世代）」の構造では「NR(New Radio)」の導入であり、「6G（第6世代）」の構造では「NA(New Audio)」の導入であると思う。「情報技術（IT）」の分野でのITネットワークだけでは無く、「人工知能（AI）」の分野でのAIネットワークに対しても、サイバーセキュリティ対策が必要と思う。	サイバーセキュリティ政策については、サイバーセキュリティ基本法に基づき、関係省庁の大臣を本部員とする「サイバーセキュリティ戦略本部」の下、戦略を定め、対策を進めています。また、内閣サイバーセキュリティセンターはサイバーセキュリティ戦略本部の事務局を担っており、関係府省庁の総合調整等を行っております。なお、平成28年、平成30年にはサイバーセキュリティ基本法の法改正が成立するなど、必要な体制整備を行っています。 御意見につきましては、サイバー空間に係る認識として「AIの劇的な進化」も盛り込んだサイバーセキュリティ戦略（平成30年7月27日閣議決定）の実施状況や、改正法の施行状況を注視していくべきと考えています。

2019年度に実施すべき施策に関する意見募集の結果一覧

通しNo	提出者	該当箇所	意見の要旨	主な考え方
84	BSA｜ザ・ソフトウェア・アライアンス	5. 推進体制	BSA会員企業は、サイバーセキュリティ戦略の実施に重大な関心を有しており、日本のコネクテッド・エコノミー全体のセキュリティを向上させる効果的なアプローチを策定するため、NISCに協力させていただきたいと考えています。	サイバーセキュリティ戦略の推進に当たっての賛同意見として承りました。今後の施策の実施や検討に当たって、参考とさせていただきます。
85	BSA｜ザ・ソフトウェア・アライアンス	5. 推進体制	BSAの提唱するインターナショナル・サイバーセキュリティ・ポリシーフレームワークの原則（①国際的に認められた技術標準との整合性、②リスクベース、結果重視、技術中立的であること、③市場主導のメカニズムを信頼すること、④イノベーションを促進するよう柔軟で適応可能であること、⑤官民連携、⑥プライバシー保護を重視すること）に基礎を置くよう提言。	サイバーセキュリティ戦略（平成30年7月27日閣議決定）の基本原則には、「情報の自由な流通の確保」、「自律性」、「多様な主体の連携」が盛り込まれており、また、同戦略には、サイバーセキュリティの取組を進めるに当たって求められる観点として、「リスクマネジメント」が盛り込まれており、これらに基づいた取組を進めております。頂いた御意見については、今後の施策の実施や検討に当たって、参考とさせていただきます。
86	BSA｜ザ・ソフトウェア・アライアンス	5. 推進体制	BSAは、サイバーセキュリティにおけるNISCのリーダーシップに敬意を表するとともに、NISCが協力的なマルチステークホルダー・アプローチを取られていることについて感謝します。サイバーセキュリティ戦略に基づき2019年度に実施すべき施策の検討においてBSA及び会員企業の本意見が有用なものであること、また、本取組みについて引き続きNISCと協力していけることを願っております。ご質問やご意見があればいつでもご連絡下さい。	サイバーセキュリティ戦略（平成30年7月27日閣議決定）の推進に関する賛同意見として承りました。今後の施策の実施や検討に当たって、参考とさせていただきます。
87	個人（16）	5. 推進体制	用語が色々わからない。 規模や官民や立場や個人や組織に寄らずというのを整理し強調したほうが良い	ご指摘の用語が具体的に何を指すのか必ずしも明確ではないと考えられますが、サイバーセキュリティ戦略（平成30年7月27日閣議決定）の推進に当たって、参考とさせて頂きます。
88	個人（9）	－	サイバーセキュリティ担当大臣の発言が、病人の気持ちを考えていない内容であり、問題である。	本意見募集と直接関係ないと考えられますが、ご意見として承ります。
89	個人（4）	－	・社会構造が古い為に新しく改革し向上による概略案 ・教育内容の改正による具体案 ・女性社会進出での改正による具体案 ・外国人高度人材での導入で社会水準の向上による具体案 ・「ガバナンス（政治統治）」構造の改正による具体案 ・生活水準での基準による詳細案 ・官公庁が考案した無駄な政策の廃止による詳細案」	本意見募集と直接関係ないと考えられますが、ご意見として承ります。

2019年度に実施すべき施策に関する意見募集の結果一覧

通しNo	提出者	該当箇所	意見の要旨	主な考え方
90	個人 （5）	-	20年前に仕事中の事故で、建設用の重機に右足をひかれ切断に至った。当時の重機の運転手を処罰して欲しい。警察も頼りにならないので国の力を貸して欲しい。	本意見募集と直接関係ないと考えられますが、ご意見として承ります。
91	個人 （13）	-	学生に中共スパイが混じっているようにも思える。学校存続のために変な補助金目当てで外国人留学生を日本の税金を使って無料招待するより、日本国民学生の学費ローンとも呼ばれる奨学金制度を何とかしてほしい。	本意見募集と直接関係ないと考えられますが、御意見として承ります。
92	個人 （16）	-	学問というより数学のようにそれを前提とした利用、それを推進するための基礎研究、抽象的でわかりがたいことを伝える工夫。日常（アナログ）の延長ではない。	御意見の趣旨が必ずしも明確ではないと考えられますが、今後も、サイバーセキュリティ戦略（平成30年７月27日閣議決定）に基づく取組を推進していきます。