「サイバーセキュリティ戦略（案）」等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：2018年６月７日（木）～６月21日（木）
- 意見総数：27者から97件【16企業・団体から延べ72件、11個人から延べ25件。】

【意見の種類】

・戦略本文に係る意見：66件

- ・総論（策定の趣旨・背景、サイバー空間に係る認識、本戦略の目的）：13件
- ・経済社会の活力の向上及び持続的発展：10件
- ・国民が安全で安心して暮らせる社会の実現：24件
- ・国際社会の平和・安定及び我が国の安全保障への寄与：7件
- ・横断的施策：9件
- ・推進体制3件

・政策展開（サイバーセキュリティ2018）に係る意見：29件

・その他の意見：2件

- （参考）提出者名：

株式会社ICS研究所、エムティインターナショナル株式会社、経団連産業技術本部、一般社団法人サイバーリスク情報センター公益財団法人笹川平和財団、在日米国商工会議所、一般社団法人新経済連盟、一般社団法人JPCERTコーディネーションセンター、次世代ICカードシステム研究会、石油化学工業協会、石油連盟、電気事業連合会、一般社団法人日本化学工業協会、特定非営利法人日本セキュリティ監査協会、特定非営利法人日本ネットワークセキュリティ協会、株式会社ラック、個人（11人）

「サイバーセキュリティ戦略（案）」等に関する意見募集の結果一覧

通しNo	提出者	該当箇所	御意見の種類	御意見の要旨	御意見に対する主な考え方及び修正
1	個人（1）	1～3（1. 策定の趣旨・背景、2. サイバー空間に係る認識、3. 本戦略の目的）	戦略本文に係る意見	プラットフォーム開発について、最も危険なのは賄賂などが未だにある国による開発である。国内ではなく、海外からの攻撃が問題となり、最初から海外視点を置かないと防御は難しい時代に入っているのではないか。	悪意ある主体や国家の関与が疑われる脅威について、本戦略(案)（2.2. サイバー空間における脅威の深刻化）において、「この空間は、場所・時間の制約を受けずに、悪意ある主体を含む全ての者が、新たな情報通信技術を悪用・濫用し、容易に活動できる場である。」、「国家の関与が疑われる大規模な事案も発生している。」と記載しています。 御意見も踏まえ、プラットフォームを含む情報インフラについて、その信頼性が揺らぐ懸念があることを明記することとし、本戦略(案)（2.2. サイバー空間における脅威の深刻化）において、以下のように追記することとします。 「さらに、一部の国が優越的な地位からサイバー空間を管理・統制することにより、情報インフラの信頼性が揺らぐ懸念もある。」
2	個人（2）	1～3（1. 策定の趣旨・背景、2. サイバー空間に係る認識、3. 本戦略の目的）	戦略本文に係る意見	電力および電気通信の重要インフラの業務継続が最も重要であることを記述されたい。	本戦略(案)（4.2.2 官民一体となった重要インフラの防護）に記載されている「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」において、重要インフラ分野の重要性については特に区別しておらず、電力及び電気通信に限らずどの分野も重要であると考えられるため、原案のとおりとします。
3	個人（2）	1～3（1. 策定の趣旨・背景、2. サイバー空間に係る認識、3. 本戦略の目的）	戦略本文に係る意見	サイバー空間は動的な脅威によって動的にリスクが変化する空間であるため、継続的監視に基づくリスクマネジメント（ISO27005）を適用する必要がある。	本戦略(案)（3.2. 目指すサイバーセキュリティの基本的な在り方）において、リスクマネジメントについて、「「リスクについて組織を指揮統制するための調整された活動」と定義」と記載しつつ、脚注37で「国際標準化機構（ISO）の定義」と明記しており、対応しておりますので、原案のとおりとします。
4	個人（2）	1～3（1. 策定の趣旨・背景、2. サイバー空間に係る認識、3. 本戦略の目的）	戦略本文に係る意見	電磁パルス脅威の記述を追加してほしい。	御指摘の「スーパーEMP兵器等による電磁パルス脅威」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、悪意ある主体や国家の関与が疑われる脅威について、本戦略(案)（2.2. サイバー空間における脅威の深刻化）において、「この空間は、場所・時間の制約を受けずに、悪意ある主体を含む全ての者が、新たな情報通信技術を悪用・濫用し、容易に活動できる場である。」、「国家の関与が疑われる大規模な事案も発生している。」と記載しており、原案のとおりとします。
5	次世代ICカードシステム研究会	1～3（1. 策定の趣旨・背景、2. サイバー空間に係る認識、3. 本戦略の目的）	戦略本文に係る意見	サイバー空間を構成するネットワークのセキュリティについては触れられていません。ネットワークセキュリティについて、もっと言及すべきではないか。	本戦略(案)（4.2. 国民が安全で安心して暮らせる社会の実現）において、「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」について記載しております。 御意見も踏まえ、この記載の前提となる認識として、同（2.2. サイバー空間における脅威の深刻化）においても、ネットワークセキュリティを含む情報インフラについて、その信頼性が揺らぐ懸念があることを明記することとし、以下のように追記することとします。 「さらに、一部の国が優越的な地位からサイバー空間を管理・統制することにより、情報インフラの信頼性が揺らぐ懸念もある。」
6	次世代ICカードシステム研究会	1～3（1. 策定の趣旨・背景、2. サイバー空間に係る認識、3. 本戦略の目的）	戦略本文に係る意見	秘匿性，完全性に係る社会への影響は多く記載されているものの，可用性といった今後のあるべきインフラについて十分な記載がありません。そのため，今後のサイバー空間の前提である環境のあるべき姿についても言及すべきではないか。 例えば，「2．2－（1）」の障害について，爆発的な利用によるインフラの飽和といったことも考えられるのではないか。	本戦略(案)（3.2. 目指すサイバーセキュリティの基本的な在り方）において、「信頼できるサイバー空間が自律的・持続的に進化・発展することを目指す」と記載しており、この記載は、「可用性といった今後のあるべきインフラ」についても包含しているため、原案のとおりとします。

「サイバーセキュリティ戦略（案）」等に関する意見募集の結果一覧

通しNo	提出者	該当箇所	御意見の種類	御意見の要旨	御意見に対する主な考え方及び修正
7	特定非営利法人日本セキュリティ監査協会	1～3（1. 策定の趣旨・背景、2. サイバー空間に係る認識、3. 本戦略の目的）	戦略本文に係る意見	法の支配に関し、「また、同様に、この空間では、既存の国際法が適用される。今後、サイバー空間が安全で信頼できる空間として持続的に発展していくためには、引き続き、既存の国際法の適用、規範の形成が不可欠である。」の部分について、サイバー空間に適用できる国際法はないとの諸説もあることから、「国際間においても、既存の国際法の枠組みの適用に加えて、より安全なサイバー空間形成のための規範の形成が不可欠である。」と修文すべき。	我が国は、サイバー空間にも既存の国際法が適用されるという立場を取っています。本戦略(案)（3.1. 基本的な立場の堅持）において、「引き続き、既存の国際法の適用、規範の形成が不可欠である。」と記載しており、御指摘の「より安全なサイバー空間形成のための規範の形成」についても包含していると考えられるため、原案のとおりとします。
8	特定非営利法人日本セキュリティ監査協会	1～3（1. 策定の趣旨・背景、2. サイバー空間に係る認識、3. 本戦略の目的）	戦略本文に係る意見	「サイバーセキュリティエコシステム」という言葉は、他の箇所で使用しない場合、該当の一文は削除した方がよい。	「サイバーセキュリティエコシステム」は、本戦略（案）（3.2.目指すサイバーセキュリティの基本的な在り方）に記載している「生物における免疫系のように、全ての主体が、サイバーセキュリティについて自らの役割を認識し、サイバーセキュリティに関する取組を自律的に行うこと」を象徴する用語であるため、原案のとおりとします。
9	特定非営利法人日本セキュリティ監査協会	1～3（1. 策定の趣旨・背景、2. サイバー空間に係る認識、3. 本戦略の目的）	戦略本文に係る意見	バングラディシュ中央銀行がハッキングを受け、約 8,100万ドルが不正送金。 ⇒「が不正送金」を「の不正送金」へ変更し、読みやすくすることを提案します。	御意見を踏まえ、以下のように修文することとします。 「バングラディシュ中央銀行がハッキングを受け、約8,100万ドルが不正送金された事案」
10	公益財団法人笹川平和財団	1～3（1. 策定の趣旨・背景、2. サイバー空間に係る認識、3. 本戦略の目的）	戦略本文に係る意見	基本法第2条では、サイバーセキュリティを「電磁的方法によって取り扱われる情報の漏洩等の安全管理に必要な措置ならびに情報システム及び情報ネットワークの安全性・信頼性の確保」と定義しているが、多様な主体の連携のため、国際的なサイバー空間の認識の動向を踏まえ、今後「サイバーセキュリティ」の対象は実空間も含むものとして幅広く考えていく必要がある。」	サイバー空間と実空間の一体化の進展を踏まえ、本戦略(案)（3.2.目指すサイバーセキュリティの基本的な在り方）において、「全ての主体が、サイバーセキュリティについて自らの役割を認識し、サイバーセキュリティに関する取組を自律的に行うことが求められる。」、「皆が力を合わせて取り組むこと、すなわち協働が求められる。」と記載しており、サイバーセキュリティに関する取組を幅広く進めることとしているため、原案のとおりとします。御意見の内容については、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。
11	株式会社ラック	1～3（1. 策定の趣旨・背景、2. サイバー空間に係る認識、3. 本戦略の目的）	戦略本文に係る意見	「サイバーセキュリティ戦略（案）」の趣旨等について、賛同いたします。	賛同意見として承りました。
12	経団連産業技術本部	1～3（1. 策定の趣旨・背景、2. サイバー空間に係る認識、3. 本戦略の目的）	政策展開（サイバーセキュリティ2018）に係る意見	経団連がこれまでの提言等において主張してきた重要事項の多くが盛り込まれており、全体として高く評価できる。	賛同意見として承りました。

「サイバーセキュリティ戦略（案）」等に関する意見募集の結果一覧

通しNo	提出者	該当箇所	御意見の種類	御意見の要旨	御意見に対する主な考え方及び修正
13	電気事業連合会	1～3（1. 策定の趣旨・背景、2. サイバー空間に係る認識、3. 本戦略の目的）	戦略本文に係る意見	下記のとおり修正してはどうか。 【修正案】 3.2. (2)3つの観点 ①サービス提供者の任務保証 …すなわち、これは、サイバーセキュリティに関する取組そのものを目的化するのではなく、各々の組織の経営層・幹部が、「任務」に該当する業務やサービスを見定めて、その安全かつ持続的な提供、万が一の事態における事業継続や緊急時対応に関する責任を全うするという考え方である。 【理由】 「安全かつ持続的な提供に関する責任」だけでなく、万が一の事象も起こりうるとの前提の下で、緊急時の早期・適切な対応といった趣旨を織り込むべきではないか。	本戦略(案)（3.2. 目指すサイバーセキュリティの基本的な在り方）において記載している「安全かつ持続的な提供」は、御指摘の「万が一の事態における事業継続や緊急時対応」を包含すると考えられ、また、「4.2.2(1)① リスクマネジメントの推進」において、「事業継続計画及び緊急時対応計画を策定することが重要である」と記載をしているため、原案のとおりとします。 御意見の内容については、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。
14	在日米国商工議会所（The American Chamber of Commerce in Japan）	1～3（1. 策定の趣旨・背景、2. サイバー空間に係る認識、3. 本戦略の目的）	戦略本文に係る意見	サイバー空間は容易に国境を超え多大な効果をもたらします。しかしその一方で、サイバーセキュリティ対策は予測がつかない対策を強いられます。したがって、以下の下線部分の文を盛り込むことにより、サイバー空間の拡がりを表すべき。 ⑤ 多様な主体の連携 サイバー空間は、国、地方公共団体、重要インフラ事業者、サイバー関連事業者その他の事業者、教育研究機関、個人などの多様な主体が活動することにより構築される多次元的な世界である。更にはサイバー空間上では国外の利害関係者とも容易につながり、サイバー空間の拡がりを特定することは極めて難しい。	本戦略(案)（1. 策定の趣旨・背景）において、「こうした発展を遂げた空間は、場所や時間の制約にとらわれず、国境を越えて、量・質ともに多種多様な情報・データを自由に生成・共有・分析することが可能な場であり、流通する場でもある。（中略）新たな価値を生み出していく可能性がある。」、同（4.3. 国際社会の平和・安定及び我が国の安全保障への寄与）において、「サイバー攻撃は容易に国境を越え、（中略）、サイバー空間の安全・安定の確保のためには、（中略）国際協力・連携を進める必要がある。」と記載しています。 このように、御指摘の「サイバー空間上では国外の利害関係者とも容易につながり、サイバー空間の拡がりを特定することは極めて難しい」に対応した記載となっているため、原案のとおりとします。 御意見の内容については、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。
15	株式会社ICS研究所　代表取締役社長 村上正志	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	戦略本文に係る意見	そのリスクを大きくする脆弱性情報を部品個体単位で即時確認できるトレーサビリティ管理環境を構築しこれを維持する必要がある 重要インフラや製造業や施設設備のHSE（Health, Safety & Environment）を脅かす要因の一つであるサイバーリスクへの対策も投資である。：HSE&Securityという言葉を追加記入した方が良いセキュリティ認証CSMSの導入やEDSA認証取得の制御製品で制御システム構築することを保険契約条件に入れることを推進して行くとさらに加速すると考えます。それも企業経営では投資になります。	いただいた御意見は、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。 なお、以下のとおり本戦略（案）に記載しております。 ・トレーサビリティについては、本戦略（案）（4.1.2(2) 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）において、「トレーサビリティ を確認するための仕組みと、創出された信頼そのものに対する攻撃を検知・防御するための仕組みを検討する」と記載しています。 ・重要インフラ等の安全性については、本戦略（案）（4.2. 国民が安全で安心して暮らせる社会の実現）において、「業務やサービスが安全かつ持続的に提供されるよう、サイバーセキュリティの基本的な在り方で掲げた「任務保証」の考え方に基づく取組を推進していく」と記載しています。 ・サイバーセキュリティ保険については、本戦略（案）（4.1.1(2) サイバーセキュリティに対する投資の推進）において、サイバーセキュリティ対策の実施状況に応じて、適切に保険料が算定される仕組みにより、リスクへの備えに対するコストが明確になっていくため、投資が進めやすくなる可能性があることを踏まえ、「官民が連携してサイバーセキュリティにおける保険の活用を推進するための方策について検討を行う」と記載しています。 ・サイバーセキュリティに関する取組についての情報公開については、本戦略（案）4.1.1(2)（サイバーセキュリティに対する投資の推進）において、「投資家が企業経営層のサイバーセキュリティに関する取組を評価できるような仕組みづくりを進めていく」と記載しています。

「サイバーセキュリティ戦略（案）」等に関する意見募集の結果一覧

通しNo	提出者	該当箇所	御意見の種類	御意見の要旨	御意見に対する主な考え方及び修正
16	個人（2）	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	戦略本文に係る意見	次のように修文されたい。 「その際には、サイバーセキュリティに係るリスクは企業が直面する様々なリスクの1つであるが、動的なリスクであるため、従来の静的なリスクマネジメントに加えて、継続的監視に基づく動的なリスクマネジメントを組み入れていくことが重要である。」	リスクマネジメントについては、本戦略（案）（3.2(2)② リスクマネジメント）において、「リスクの特定・分析・評価という個別の活動を指すのではなく、組織を指揮統制して、組織が有する有限の資源を適切に分配し、リスクに対応していく一連の活動の全体を意味している」としております。 御指摘の「動的なリスクマネジメント」との点についても、その主旨は含まれていると考えていることから、原案のとおりとしますが、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。
17	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	戦略本文に係る意見	経営そのもののDX対応が喫緊の課題である現状を踏まえ、将来的には、経営層が広くICTに係る専門的知見を有し、ICT利活用「戦略マネジメント」の一環としてサイバーセキュリティを取扱うべきものと考える。 【修文案】 具体的には、経営層は、デジタルトランスフォーメーション（DX）の進展を十分認識し、取締役会等を通じたサイバーセキュリティに関する積極的な関与が期待されるとともに、リスクマネジメントのために必要となるサイバーセキュリティに関する一定の知識・能力を身につけることが求められる。その際、中短期的視点において、経営層に深い技術的な知識やスキルを期待することは必ずしも現実的ではない。このため、経営戦略、事業戦略におけるサイバーセキュリティのリスクを認識し、経営層の方針を踏まえた対策を立案し、実務者・技術者を指導できる人材（いわゆる「戦略マネジメント層」）を確保することが重要である。	デジタルトランスフォーメーションの進展の観点については、本戦略（案）（4.1.1(1) 経営層の意識改革）の箇所において、「サイバー空間の利用が急速に進展する中、自由であるがゆえに常に脅威が潜んでいるという認識に立って、そのための備えをすることが必須」としており、御指摘の観点も、重要と考えています。 また、将来的に経営層が広くICTに係る専門的知見を有するべきとの点については、現状では、経営層がサイバーセキュリティに関する一定の知識・能力を身につけることが必要ではあるものの、即座に深い技術的な知識やスキルを求めることは現実的ではないと考えているため、原案の記載ぶりとしておりますが、御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。
18	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	政策展開（サイバーセキュリティ2018）に係る意見	民間のCIOその他の有為な者の活動について、ベストプラクティスとして共有・参照する取組みを検討いただきたい。	サイバーセキュリティ2018（案）の1.1.(2)サイバーセキュリティに対する投資の推進において、「経済産業省において、「サイバーセキュリティ経営ガイドライン」の実践的な定着を図るために、具体的な対策事例や情報共有活動事例等を示すプラクティスを作成する。また、企業がどの程度サイバーセキュリティ対策を実施するかの目安として活用できる可視化ツールを作成する」と記載しており、これに基づく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。
19	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	政策展開（サイバーセキュリティ2018）に係る意見	民間企業等における投資へのインセンティブ付与のため、より一般的・汎用的なサイバーセキュリティ対策に必要なシステム構築、サービス利用等の促進に係る税制優遇措置を講じていただきたい。	サイバーセキュリティ2018（案）の1.1(2)サイバーセキュリティに対する投資の推進において、「総務省及び経済産業省において、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、それに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ことで、事業者のセキュリティ対策の強化と生産性向上を同時に促進する。」との取組を盛り込むこととし、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。
20	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	政策展開（サイバーセキュリティ2018）に係る意見	関係機関による当該「モノやサービス等」の先導的な導入を促進する仕組みについて検討いただきたい。	サイバーセキュリティ2018（案）の2.3(3)先端技術の活用による先取り対応への挑戦において、「内閣官房において、近年普及してきた情報システムの基盤の中でサイバー攻撃による高い耐性を有するものについて、これらの情報技術を、政府機関等において活用できる可能性について検証する」との取組を盛り込むこととし、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。
21	特定非営利法人日本セキュリティ監査協会	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	政策展開（サイバーセキュリティ2018）に係る意見	研究開発に当たっては、サイバーセキュリティ人材のひっ迫等を考慮し、サイバーセキュリティに関する知見の蓄積及び利活用或いは次世代への継承を狙いとする自動化等の技術開発も視野に入れる。	サイバーセキュリティ2018（案）の4.2.(1)実践的な研究開発の推進では、例えば「文部科学省において、理化学研究所革新知能統合研究センター（AIPセンター）を通じ、革新的な人工知能基盤技術の構築と、サイバーセキュリティを含む社会的課題の解決に向けた応用研究等を進めていく」等の取組を盛り込むこととし、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。

「サイバーセキュリティ戦略（案）」等に関する意見募集の結果一覧

通しNo	提出者	該当箇所	御意見の種類	御意見の要旨	御意見に対する主な考え方及び修正
22	経団連産業技術本部	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	政策展開（サイバーセキュリティ2018）に係る意見	ヒト・情報・技術・カネといったサイバーセキュリティ対策強化に必須のリソースを確保することが重要である。	賛同意見として承りました。 御意見の内容については、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。
23	日本ネットワークセキュリティ協会	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	政策展開（サイバーセキュリティ2018）に係る意見	投資促進のためにも、有価証券報告書でのリスク記載を義務化するなどの施策も、税制優遇などと合わせて施策として組み入れていただきたい。	サイバーセキュリティ2018（案）の1.1(1)経営層の意識改革において、「経済産業省において、取締役会のサイバーセキュリティへの関与を促すとともに、投資家に対するサイバーセキュリティの啓発を行う観点から、上場企業において行われる「取締役会の実効性評価」の評価項目について、サイバーセキュリティへの経営層の関与をその評価項目として組み込むことを促進する」との取組を盛り込むこととし、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	在日米国商工議会所（The American Chamber of Commerce in Japan）	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	政策展開（サイバーセキュリティ2018）に係る意見	セキュリティ・バイ・デザインによって、日本のモノやサービスの信頼性向上や海外展開の推進に寄与することとなると考えます。 国際競争の高まりや真正性や信頼性の検証が困難になるという理由のもとに、国外製品が排除されたり、または不当に扱われたりすることのないよう御配慮を要望します。	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	個人（3）	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	戦略本文に係る意見	市場の評価を受けて経営者を規律付けするために有価証券報告書等の開示情報を充実させることが適当である。	本戦略（案）（4.1.1(2) サイバーセキュリティに対する投資の推進）において、「投資家が企業経営層のサイバーセキュリティに関する取組を評価できるような仕組みづくりを進めていく」と記載しており、これに基づく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。
26	個人（3）	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	戦略本文に係る意見	CEO後継者に求める素養として、サイバーセキュリティに関するナレッジや経験を例示するなどの方策が考えられる。	本戦略（案）（4.1.1(2) サイバーセキュリティに対する投資の推進）において、「投資家が企業経営層のサイバーセキュリティに関する取組を評価できるような仕組みづくりを進めていく」と記載しており、これに基づく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。
27	個人（4）	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	政策展開（サイバーセキュリティ2018）に係る意見	中小企業の取組の促進に関して、サイバーセキュリティ相談窓口の設置、情報処理安全確保支援士等のインシデント発生時の専門家派遣制度の活用を盛り込み、インシデントに対応出来る環境を整備すべき	サイバーセキュリティ2018（案）の1.1(2)サイバーセキュリティに対する投資の推進において、「経済産業省において、中小企業のサイバーセキュリティ対策の促進を図るため、身近な相談窓口の整備等の支援体制の強化を検討するとともに、サイバーセキュリティ保険の普及を図る」との取組を盛り込むこととし、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。
28	特定非営利法人日本セキュリティ監査協会	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	戦略本文に係る意見	常用漢字外なので「拡がる」を「広がる」に修正した方がいいのではないか	御指摘を踏まえ、「サプライチェーンがグローバルに広がる中で」と修正することとします。
29	特定非営利法人日本セキュリティ監査協会	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	戦略本文に係る意見	(3)中小企業の取組の促進の第一文の根拠が不明確なので、 「大企業に比較して経営基盤が脆い中小企業の場合、サイバー攻撃による金銭的な損害や信用の低下による経営的打撃から回復することができにくい。」と修文してはどうか。	本戦略（案）の策定に当たっては「サイバーセキュリティ人材の育成に関する施策間連携ワーキンググループ報告書」（平成30年5月31日）の内容を反映しているところ、同報告書（P23）において、より詳細に「中小企業は、大企業に比べて経営基盤が必ずしも盤石ではないため、サイバー攻撃により、金銭的な損害や信用の低下を招いてしまった場合、経営に与えるインパクトが極めて大きい」と記載しており、原案のとおりとします。

「サイバーセキュリティ戦略（案）」等に関する意見募集の結果一覧

通しNo	提出者	該当箇所	御意見の種類	御意見の要旨	御意見に対する主な考え方及び修正
30	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	戦略本文に係る意見	国民生活の保護等の視点からサプライチェーンの中に中古品取引も含めて考えるべき。 【修文案】 サイバー空間と実空間の一体化が加速的に進展する中、「Society5.0」の実現に向けて、グローバルな規模で、これまで取引がなかった異なる業種の企業間取引が生まれたり、中古品等の個人間取引が急速に拡大したりしている。	多様なつながりの一つの形態に個人間取引も含まれ得るところ、本戦略（案）（4.1.2(2) 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）において、「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」としており、ご指摘の「中古品等の個人間取引」の観点についても、その主旨は含まれていると考えていることから、原案のとおりとしますが、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。
31	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	政策展開（サイバーセキュリティ2018）に係る意見	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進めていただきたい。	いただいた御意見は、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。 なお、サイバーセキュリティ2018（案）の4.3全員参加による協働において、「内閣官房において、行動計画に基づき、NISCが中核的役割を担いつつ、各府省庁や民間の取組主体と協力して、「サイバーセキュリティ月間」をはじめとし、サイバーセキュリティに関する各種イベント等の開催や情報発信等を通じ普及啓発活動を進める」との取組を進めています。
32	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	政策展開（サイバーセキュリティ2018）に係る意見	Logisticレイヤーにおける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いただきたい。	いただいた御意見は、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。 なお、サイバーセキュリティ2018（案）の1.2.(2)サプライチェーンにおける機器・サービスのサイバーセキュリティを確認できる仕組の構築において、「内閣府において、戦略的イノベーション創造プログラム（SIP）第2期「IoT社会に対応したサイバー・フィジカル・セキュリティ」により、セキュアなSociety 5.0の実現に向けて、様々なIoT機器を守り、社会全体の安全・安心を確立するため、中小企業を含むサプライチェーン全体を守ることに活用できる、『サイバー・フィジカル・セキュリティ対策基盤』の研究開発及びその社会実装を推進する。本プロジェクトでは、IoT機器のセキュリティを保証する技術、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、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、サイバー・フィジカル空間を跨った不正なデータを検知・防御する技術等を開発する。」との取組を進めています。
33	在日米国商工議会所（The American Chamber of Commerce in Japan）	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	政策展開（サイバーセキュリティ2018）に係る意見	ブロックチェーン技術をめぐるセキュリティについても考慮に入れた戦略を検討することが経済社会の活力向上に一層資するものと考えます。	本戦略（案）（4.4.2(1) 実践的な研究開発の推進）において、「AI、ブロックチェーンなどの先進的な技術を用いたサイバーセキュリティ確保の技術（中略）について重点的に取り組む」こととしており、これに基づく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。
34	エムティインターナショナル株式会社	4．1．3　安全なIoTシステムの構築	戦略本文に係る意見	安全なIoTシステムの構築の原点は、プログラム対策の安全性の担保である。 データ生成の実態確認の為にプログラムテストが必須である。完全なプログラム開発とはコンパイルアップ時点でSyntaxチェックに加えSemanticsチェックも完了していることである。データ生成の完全性を担保するシナリオ関数技術が必須である。	本戦略（案）（4.1.3 安全なIoTシステムの構築）において、「官民が連携して、安全なIoTシステムの構築に取り組む」と記載しており、これに基づく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。
35	次世代ICカードシステム研究会	4．1．3　安全なIoTシステムの構築	戦略本文に係る意見	IoT機器のライフサイクルとして、「提供・購入」、「設定・展開」についても言及すべきではないか。	本戦略（案）（4.1.3(2) 脆弱性対策に係る体制の整備）において、「ライフサイクル」には、いただいた御意見の主旨も含んでおり、例えば具体的な取組の一つである総務省の「IoTセキュリティ総合対策」では、設計・製造、販売(輸入を含む。)、設置、運用・保守、利用の段階に分けて、取組を整理しております。引き続き安全なIoTシステムの構築に向けた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。

「サイバーセキュリティ戦略（案）」等に関する意見募集の結果一覧

通しNo	提出者	該当箇所	御意見の種類	御意見の要旨	御意見に対する主な考え方及び修正
36	株式会社ラック	4．1．3　安全なIoTシステムの構築	政策展開（サイバーセキュリティ2018）に係る意見	グローバルなサイバー攻撃等のリスクを回避する観点から、一定の要件が保証されないIoT機器の国内販売を禁ずる措置を検討いただきたい。	サイバーセキュリティ2018（案）の1.3(1)IoTシステムにおけるセキュリティの体系の整備と国際標準化、(2) 脆弱性対策に係る体制の整備の取組の中で、必要なサイバーセキュリティの要件を整理し、その要件を満たすIoT機器の利用を推奨することや、国際標準化に向けた取組を推進する等、安全なIoTシステムの構築に向け取組を進めて参ります。
37	株式会社ラック	4．1．3　安全なIoTシステムの構築	政策展開（サイバーセキュリティ2018）に係る意見	サイバー攻撃の情報共有に当たって、ベンダや関係者から開示された情報の取り扱いに十分留意するよう検討いただきたい。	サイバーセキュリティ2018（案）の2.6(1)多様な主体の情報共有・連携の推進において、「国の行政機関、重要インフラ事業者、サイバー関連事業者等官民の多様な主体が相互に連携し、サイバーセキュリティに関する施策の推進に係る協議を行うための協議会の創設に向けて検討を進める。」としており、これに基づく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。
38	在日米国商工議会所（The American Chamber of Commerce in Japan）	4．1．3　安全なIoTシステムの構築	政策展開（サイバーセキュリティ2018）に係る意見	日本独自の基準や規制を設定するのではなく、国際標準の採用を推奨する。	賛同意見として承りました。 サイバーセキュリティ2018（案）の1.3.(1)IoTシステムにおけるセキュリティの体系の整備と国際標準化の、「安全なIoTシステムを実現するために求められるサイバーセキュリティに関する基本的な要素等の国際標準化に向けた取組」に盛り込むこととし、国際標準との整合性を取るべく推進して参ります。
39	個人（2）	4．2．1　国民・社会を守るための取組	戦略本文に係る意見	積極的サイバー防御については、本来、毛沢東によれば攻勢防御であり、「報復の抑止」としてのサイバー攻撃能力を含めた定義にすべきである。	「積極的サイバー防御」は、サイバー攻撃に対して能動的に防御していく取組のことであり、必ずしも「報復の抑止」までを考慮したものではありませんが、御意見として承ります。
40	特定非営利法人日本セキュリティ監査協会	4．2．1　国民・社会を守るための取組	戦略本文に係る意見	下記下線部分の追記を提案します さらに、国民が仮想通貨を…引き続き議論を主導していく。 一方で、2022年の成人年齢の引き下げ等を見据えて、新たな技術に対する国民のサイバーセキュリティリテラシーの向上のため、産学官の連携をより一層強化し、サービスの提供事業者が利用者教育を行うなどの幅広い施策を検討する。	本戦略（案）（4.4.3 全員参加による協働）において、「産学官民の関係者が円滑かつ効果的に活動し、有機的に連携」、「サイバーセキュリティについての教育を推進する」と記載しており、原案のとおりとします。
41	株式会社ラック	4．2．1　国民・社会を守るための取組	戦略本文に係る意見	民間事業者等が安心して解析等の業務に従事できるよう、サイバーセキュリティに関する法令解釈を明確化する旨を記述されたい。	「いわゆるコンピュータ・ウイルスに関する罪」については、既に法務省等が考え方を公表しています。サイバーセキュリティをめぐる環境の変化を踏まえると、サイバーセキュリティに関する法令解釈を網羅的に明示することは困難と思われ、前述のとおり既に主なものについては公表されていることから、原案のとおりとします。 一方で、官民連携によるサイバー犯罪対策を推進するためには、研究者や民間事業者等が法令に則った上で安心してサイバーセキュリティ事業に従事できることが重要であるため、官民連携の推進に当たって参考とさせていただきます。
42	日本ネットワークセキュリティ協会	4．2．1　国民・社会を守るための取組	戦略本文に係る意見	サイバーセキュリティ事業従事者逮捕事案等の発生を受け、ICTの利用促進を阻害しない適切な取締りについて記述されたい。	ICTの利用促進を阻害しないという点については、戦略本文（3．本戦略の目的）において、基本的な理念（「自由、公正かつ安全なサイバー空間」を目指す）や基本原則（③開放性、④自律性）として考え方を記載しております。 本戦略（案）は、上記考え方を踏まえた上での取組として記載していることから、原案のとおりとします。

「サイバーセキュリティ戦略（案）」等に関する意見募集の結果一覧

通しNo	提出者	該当箇所	御意見の種類	御意見の要旨	御意見に対する主な考え方及び修正
43	公益財団法人笹川平和財団	4．2．2　官民一体となった重要インフラの防護	戦略本文に係る意見	官民連携の更なる強化が必要であること、 その際、重要インフラ事業者における連絡担当者には、関連資格保有者にセキュリティクリアランスを施した上で充てることが望ましく、また、そのような枠組みによる事業者の負担軽減も必要であるため、4.2.2（1）に⑥として以下の文章を追加すべき。 「⑥官民連携の更なる強化 　サイバー攻撃への迅速な対応を行うため、重要インフラ事業者における連絡担当者の指定（既存の国家資格保持者等を活用）及び重要インフラ事業者から内閣サイバーセキュリティセンターへのインシデントの報告の義務化を検討する。その際、報告の義務化に伴う重要インフラ事業者の負担軽減のため税制優遇等の助成措置についても併せて検討する。」	「官民連携の強化」は重要なポイントであるため、本戦略（案）において様々な個所に記載しております。 インシデント報告を促進することにより官民連携を強化することについては、御意見を踏まえ、同（4.2.6(2) 情報共有・連携の新たな段階へ）において、以下のように修文することとします。 「サイバーセキュリティインシデント等に係る、自ら保有する情報を積極的に提供する主体が評価される環境を整備していく。」 また、「報告の義務化に伴う重要インフラ事業者の負担軽減のため税制優遇等の助成措置」については、今後の取組の参考とさせていただきます。
44	石油化学工業協会	4．2．2　官民一体となった重要インフラの防護	戦略本文に係る意見	「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」でも「相互依存性等を踏まえた重要インフラ事業者等のクラス分け」が示されており、分野ごとに差異があることは理解されている。「サイバーセキュリティに関する意識や取組の進捗に温度差がある」ことを、一概に解決すべき「課題」と決めつけるべきではない。	「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」において、「相互依存性等を踏まえた重要インフラ事業者等のクラス分け」を記載しており、分野ごとの取組について差異があることは御認識のとおりですが、趣旨は、一部の重要インフラ事業者等による先導的取組について、更に強化・推進していくとともに、他の重要インフラ分野に広めていく、ということであり、全体的な底上げを行っていくということです。 したがって、分野ごとの取組について差異があることを課題として捉え、その課題を解決するために全体的なセキュリティレベルの底上げを行っていく、という記載は適切と考えておりますので、原案のとおりとします。
45	石油化学工業協会	4．2．2　官民一体となった重要インフラの防護	政策展開（サイバーセキュリティ2018）に係る意見	「安全等を維持する観点から、サイバーセキュリティ対策を関係法令等における保安規制として位置付けるなど、制度的枠組みを適切に改善していく」との記述がある。 　重要インフラ事業者は「サイバーセキュリティ基本法」に則って自主的に取組んできているところである。法制化の検討に際しては、初めから法制化ありきの対応ではなく、法益や対象業種の特性を踏まえて必要性や在り方を慎重に検討することが大前提である。対象となる事業者へのサイバー攻撃による障害の影響の大きさと、これに対応するための事業者の負担に十分に配慮されたい。	「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」に盛り込まれている内容であり、原案のとおりとします。 なお、サイバーセキュリティの完全性・可用性・機密性をどのように位置付けていくかについては、関係法令等の目的によって当然異なりますので、その目的に照らして、妥当な位置付けとなるように考えており、そのような意味で、「適切に改善」していくとしています。
46	個人（5）	4．2．2　官民一体となった重要インフラの防護	戦略本文に係る意見	「4.2.2　官民一体となった重要インフラの防護」項目にて『重要インフラ分野ごとに、サイバーセキュリティに関する意識や取組の進捗に温度差があるという課題がある。』との指摘に賛同する。 「（2）安全基準等の改善・浸透」にて、より具体的に情報セキュリティの国家資格である「情報処理安全確保支援士」を必置とする事を提案する。 重要インフラ事業者について、企業間格差を是正するためにも関係法令等における保安規制として導入することを強く要望し提案する。 「地方公共団体のセキュリティ強化・充実」においても 前述の通り国家資格である「情報処理安全確保支援士」の有資格者の配置を要件として盛り込むことを提案したい。	本戦略（案）は、今後３年程度の基本的な施策の方向性を示したものであり、個別具体的な取組を記載することは考えておりませんが、「情報処理安全確保支援士」に関する提案については、今後の取組の参考とさせていただきます。 また、「関係法令等における保安規制として導入する」ことについては、本戦略（案）（4.2.2(2)② 安全基準等の改善・浸透）において、「安全等を維持する観点から、サイバーセキュリティ対策を関係法令等における保安規制として位置付けるなど、制度的枠組みを適切に改善していく」と記載しています。

「サイバーセキュリティ戦略（案）」等に関する意見募集の結果一覧

通しNo	提出者	該当箇所	御意見の種類	御意見の要旨	御意見に対する主な考え方及び修正
47	石油連盟	4．2．2　官民一体となった重要インフラの防護	戦略本文に係る意見	電力、ガス、石油の3分野以外で制御系システムを利用している分野における当事者意識を高め、関係全分野での対策を推進する目標に鑑み以下の通り修文すべき。 「電力、ガス、石油分野等の重要インフラ事業者の中には、サービス提供のために制御系システムを用いている事業者がある。この制御系システムに不具合が生じると通常のサービスが提供できなくなり、国民生活に大きな支障が生じるおそれがある。」	御意見を踏まえ、「4.2.2(1)⑤ 制御系システムのセキュリティ対策」において、以下のように修文することとします。 「電力、ガス、石油分野等の重要インフラ事業者の中には、サービス提供のために制御系システムを利用している事業者がある。サイバー攻撃等により制御系システムに大きな影響が生じると通常のサービスが提供できなくなり、国民生活に大きな支障が生じるおそれがある。」
48	一般社団法人日本化学工業協会	4．2．2　官民一体となった重要インフラの防護	戦略本文に係る意見	重要インフラサービスを安全かつ持続的に供給する「任務保証」については、同じサービス障害が発生した場合でも重要インフラ分野ごとにその影響は異なる。 サイバーセキュリティに関する全体的な底上げを行う際にも、分野ごとの特性を考慮した対応が必要である。	「分野ごとの特性を考慮した対応」については、本戦略（案）（4.2.2(1)② 安全基準等の改善・浸透）において、「業務の内容、組織の規模、システムの使用期間、国際競争力への影響等を考慮して安全基準等を改善する取組を継続的に推進する。」と記載をしており、既にその要素は盛り込んでいます。
49	電気事業連合会	4．2．2　官民一体となった重要インフラの防護	戦略本文に係る意見	【修正案】 重要インフラの防護については、「任務保証」の考え方に基づき、重要インフラサービスを安全かつ持続的に提供するために、・・・ 【理由】 第4次行動計画では、「『機能保証』とは、各関係主体が重要インフラサービスの防護や機能維持を確約することではなく、各関係主体が重要インフラサービスの防護や機能維持のためのプロセスについて責任を持って請け合うことを意図している。」とあり、「機能保証」という表現を「任務保証」という表現に変更する際に、「重要インフラサービスの防護や機能維持を確約することではない」ということは抜け落ちないようにしてもらいたい。 「安全かつ持続的な提供に関する責任」だけでなく、万が一の事象も起こりうるとの前提の下で、緊急時の早期・適切な対応といった趣旨を織り込むべきではないか。	御意見を踏まえ、本戦略（案）（4.2.2 官民一体となった重要インフラの防護）について、以下のように修文することとします。 「重要インフラの防護については、「任務保証」の考え方を踏まえ、重要インフラサービスの安全かつ持続的な提供を実現するため、「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」（以下「行動計画」という。）の5つの施策群に基づいた取組を推進してきた。」
50	電気事業連合会	4．2．2　官民一体となった重要インフラの防護	戦略本文に係る意見	【修正案】 （注釈部分） 47 「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」では「機能保証」としていたが、趣旨は「重要インフラサービスの防護や機能維持を確約することではなく、重要インフラ事業者等が果たすべき役割を確実に遂行することが重要」ということであり、ここで言う「任務保証」と同じ趣旨である。 【理由】 第4次行動計画では、「『機能保証』とは、各関係主体が重要インフラサービスの防護や機能維持を確約することではなく、各関係主体が重要インフラサービスの防護や機能維持のためのプロセスについて責任を持って請け合うことを意図している。」とあり、「機能保証」という表現を「任務保証」という表現に変更する際に、「重要インフラサービスの防護や機能維持を確約することではない」ということは抜け落ちないようにしてもらいたい。 「安全かつ持続的な提供に関する責任」だけでなく、万が一の事象も起こりうるとの前提の下で、緊急時の早期・適切な対応といった趣旨を織り込むべきではないか。	御意見を踏まえ、本戦略（案）（4.2.2 官民一体となった重要インフラの防護）について、以下のように修文することとします。 「重要インフラの防護については、「任務保証」の考え方を踏まえ、重要インフラサービスの安全かつ持続的な提供を実現するため、「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」（以下「行動計画」という。）の5つの施策群に基づいた取組を推進してきた。」 なお、本戦略（案）の脚注46には、「任務保証」の考え方の基となる「2015年戦略」の「機能保証（任務保証）」を記載することとし、以下のとおり修文することとします。 「「2015年戦略」では「機能保証（任務保証）」としていたが、趣旨は「重要インフラ事業者等が果たすべき役割を確実に遂行することが重要」ということであり、ここで言う「任務保証」と同じ趣旨である。」

「サイバーセキュリティ戦略（案）」等に関する意見募集の結果一覧

通しNo	提出者	該当箇所	御意見の種類	御意見の要旨	御意見に対する主な考え方及び修正
51	電気事業連合会	4．2．2　官民一体となった重要インフラの防護	戦略本文に係る意見	『このような課題を解決するため、経営資源が限られ、サイバーセキュリティに十分な資源を割り当てることが難しい重要インフラ事業者等におけるセキュリティ対策モデルに関する検討を含め、…』とあるが、具体的にどのような取組みか、本戦略上どこに反映されているのか。	この記載の趣旨は、「サイバーセキュリティに関する全体的な底上げを行う必要がある」ということであり、「サイバーセキュリティに十分な資源を割り当てることが難しい重要インフラ事業者等におけるセキュリティ対策のモデルに関する検討」は、「全体的な底上げ」の一例として挙げているものです。具体的な取組については、関係主体で検討していく必要があると考えています。
52	電気事業連合会	4．2．2　官民一体となった重要インフラの防護	戦略本文に係る意見	【修正案】 ①リスクマネジメントの推進 重要インフラサービスは、サイバー攻撃発生時であっても安全かつ持続的に提供されることが望まれている。提供できるようにする必要がある。このため、重要インフラ事業者等は、事前のセキュリティ対策を講じるだけでなく、横断的かつ複合的なリスクを念頭に置いたリスクアセスメントの結果を踏まえ、「任務保証」の考え方に基づき、万が一の事態において、早期かつ適切に対応するため、を踏まえた事業継続計画及び緊急時対応計画を策定することが重要である。 【理由】 サイバー攻撃発生時に「安全かつ持続的に提供できるようにする必要がある」というのは、この戦略の中で記載されている「リスクを完全に除去することは不可能である」との内容にはそぐわない。	重要インフラは他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり、その機能が停止、低下又は利用不可能な状態に陥った場合に、我が国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるものであることから、そのような事態に陥らないようにするためにも、そのサービスの安全かつ持続的な提供は必要であるため、原案のとおりとします。 また、「事業継続計画及び緊急時対応計画」自体が「万が一の事態において、早期かつ適切に対応するため」のものであるため、この部分についても原案のとおりとします。
53	電気事業連合会	4．2．2　官民一体となった重要インフラの防護	戦略本文に係る意見	【修正案】 (1)行動計画に基づく主な取組 ⑤制御系システムのセキュリティ対策 電力、ガス、石油分野等では、サービスを提供するために制御系システムを利用しているため、サイバー攻撃により制御系~~この~~システムに大きな影響が~~不具合が~~生じると通常のサービスが提供できなくなり、国民生活に大きな支障が出るおそれがある。制御系システムの特性を踏まえたセキュリティ対策が十分に行われ、サービスが安全かつ持続的に提供できるよう、官民一体となって、制御系システムに関する人材育成を推進するとともに~~し~~、タイムリーに脅威情報の収集・分析・展開等を行っていく。 【理由】 1つの制御系システムが不具合を起こした場合にサービス影響が必ず発生するように誤解を招きかねない表現であるため、表現を見直した。 二文目は主語が不明確であり、本節のタイトルから「官民一体となって」という言葉を入れた。また、情報の収集・分析・展開は官庁からもタイムリーに提供されることを期待して言葉を補った。	御意見を踏まえ、本戦略（案）（4.2.2(1)⑤ 制御系システムのセキュリティ対策）について、以下のように修文することとします。 「電力、ガス、石油分野等の重要インフラ事業者の中には、サービス提供のために制御系システムを利用している事業者がある。サイバー攻撃等により制御系システムに大きな影響が生じると通常のサービスが提供できなくなり、国民生活に大きな支障が生じるおそれがある。制御系システムの特性を踏まえたセキュリティ対策が十分に行われ、サービスが安全かつ持続的に提供できるよう、官民一体となって、制御系システムに関する人材育成を推進するとともに、適時、脅威情報の収集・分析・展開等を行っていく。」
54	一般社団法人日本化学工業協会	4．2．2　官民一体となった重要インフラの防護	政策展開（サイバーセキュリティ2018）に係る意見	「サイバーセキュリティ対策を関係法令等における保安規制として位置付けるなど」の部分を削除していただきたい。 はじめから規則や法規制ありきの対応ではなく、法益や対象業種の特性を踏まえて必要性や在り方を慎重に検討することが大前提であると考える。	御指摘の箇所については、「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」に盛り込まれている内容であり、原案のとおりとします。 なお、サイバーセキュリティの完全性・可用性・機密性をどのように位置付けていくかについては、関係法令等の目的によって当然異なりますので、その目的に照らして、妥当な位置付けとなるように考えており、そのような意味で、「適切に改善」していくとしています。

「サイバーセキュリティ戦略（案）」等に関する意見募集の結果一覧

通しNo	提出者	該当箇所	御意見の種類	御意見の要旨	御意見に対する主な考え方及び修正
55	エムティインターナショナル株式会社	4．2．3　政府機関等におけるセキュリティ強化・充実	戦略本文に係る意見	政府機関等におけるセキュリティ強化・充実について、プログラム構造の欠陥対策を第1義で対策を考えなければ外壁対策では不可能である。今回のテーマ全てがプログラム問題であることを認識すべき。	OSも含めたソフトウェアの攻撃耐性を向上させる取組も重要と考えますが、昨今のサイバー攻撃の状況を鑑みれば、本戦略（案）（4.2.3(1)① 情報システムの防御能力の向上と状態の把握）に記載したように、IT資産管理、アカウント管理の徹底及び事案発生時の情報漏えいを防ぐためのデータ保護など、多層的な防御の取組を推進することとしているため、原案のとおりとします。
56	個人（2）	4．2．3　政府機関等におけるセキュリティ強化・充実	戦略本文に係る意見	表現を適正化するべき。 「ITの資産管理の自動化」について、「情報システムの状態をリアルタイムに把握し」という表現は少しあいまいな表現であるため、「情報システムの脆弱性、セキュリティ設定等をリアルタイムに把握し」に修文されたい。	情報システムの防御能力のために、情報システムを構成する機器やソフトウェアに関わる様々な項目を迅速に把握することを想定しており、全体を捉えた記載としているため、原案のとおりとします。
57	個人（2）	4．2．3　政府機関等におけるセキュリティ強化・充実	戦略本文に係る意見	表現を適正化するべき。 「効率的な情報システムの状態の把握」について、同様に「情報システムの脆弱性、セキュリティ設定等のリアルタイムの把握」に修文されたい。	情報システムの防御能力のために、情報システムを構成する機器やソフトウェアに関わる様々な項目を迅速に把握することを想定しており、全体を捉えた記載としているため、原案のとおりとします。
58	電気事業連合会	4．2．4　大学等における安全・安心な教育・研究環境の確保	戦略本文に係る意見	大学等の位置づけを国際関係などと関連させて取り扱うべき。	大学等は、国民に対する直接的な関わりが強いことから、本戦略（案）（4.2. 国民が安全で安心して暮らせる社会の実現）に盛り込んでおり、原案のとおりとします。
59	特定非営利法人日本セキュリティ監査協会	4．2．5　2020年東京大会とその後を見据えた取組	戦略本文に係る意見	表現の見直し。 「次により」を後ろに持ってきた方が読みやすいとの意見。	御意見を踏まえ、以下のように修文することとします。 「このため、以下のとおり、2020年東京大会のサイバーセキュリティの確保及びその後を見据えた施策を推進する。」
60	一般社団法人JPCERTコーディネーションセンター	4．2．5　2020年東京大会とその後を見据えた取組	戦略本文に係る意見	将来的に、「サイバーセキュリティ対処調整センター」を「サイバー攻撃等に対してオールジャパンで力を合わせて対処するための調整役・調整窓口（ナショナルCSIRT）として活用」するとの方針が記載されていることについての意見。 NISCとJPCERT/CCが、いわゆる「ナショナルCSIRT」の機能を分担して担ってきたものを新組織の所掌とすることは、国内外における混乱は必至であり、どのような役割分担を担う方針なのか、また、国内、国外に対してどのような説明を行うのか明らかしてほしいというもの。	「サイバーセキュリティ対処調整センター」をナショナルCSIRTとして活用するため具体的な活用の方法、役割・業務については、今後、2020年東京大会に向けて対処態勢を確立していく過程で、既存の枠組が実施する国際連携・国内調整に混乱が生じないように、関係省庁・関係機関と調整を進めてまいります。
61	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	政策展開（サイバーセキュリティ2018）に係る意見	オリパラの際のサイバーセキュリティ対処調整センターの運用については、民間のセキュリティベンダーを含む関係機関等との協力関係を構築強化すべき。当社も可能な限り協力する。	東京大会を見据え、貴社を含む多くの民間セキュリティベンダーとの協力関係を強化していきたいと考えております。
62	電気事業連合会	4．2．5　2020年東京大会とその後を見据えた取組	戦略本文に係る意見	重要サービス事業者という文言が使用されているが、重要インフラ事業者の誤記ではないか。	重要サービス事業者には「重要インフラ事業者」に含まれる事業者もあれば、含まれない事業者もあります。以前から、2020年東京大会の開催・運営に重要なサービスを提供している事業者を「重要サービス事業者」と呼称しているところ、ここでもその意味で使用しており、誤記ではないため、原案のとおりとします。

「サイバーセキュリティ戦略（案）」等に関する意見募集の結果一覧

通しNo	提出者	該当箇所	御意見の種類	御意見の要旨	御意見に対する主な考え方及び修正
63	公益財団法人笹川平和財団	4．2．6　従来の枠を超えた情報共有・連携体制の構築	戦略本文に係る意見	情報共有について、各主体単独で対応困難なものについて、政府が主導的にサイバーセキュリティの実務を担っていく必要がある旨を追記すべき。	本戦略（案）（4.2.6 従来の枠を超えた情報共有・連携体制の構築）において記載されている「新たな役割」の中には、ケースに応じて政府が主導的に対応を行うことも含んでいるため、原案のとおりとします。
64	公益財団法人笹川平和財団	4．2．6　従来の枠を超えた情報共有・連携体制の構築	戦略本文に係る意見	情報共有について、日本版AISを構築するため、内閣官房内閣サイバーセキュリティセンターがサイバー脅威情報共有システムの技術使用を定める旨を追記すべき。	「日本版AIS」を含め、先進的な情報共有システムの推進が必要であるとの観点から、本戦略（案）（4.2.6(2) 情報共有・連携の新たな段階へ）に「寄せられる情報に対して、処理の自動化を推進するなどして、適切かつ迅速な分析や、各々の主体が真に必要とする情報の共有を実現していく。」と記載しているため、原案のとおりとします。
65	一般社団法人JPCERTコーディネーションセンター	4．2．6　従来の枠を超えた情報共有・連携体制の構築	戦略本文に係る意見	「従来の枠」が判然とせず、官民関係や業界区分が無くなるように読むことができ、それは不適切と考えられるため、官民や業界といった従来の枠を踏まえつつ新たな段階の情報共有の姿を検討し、環境造成や意見醸成に努める旨の記述に変更すべき。	サイバーセキュリティのための情報共有・連携の枠組みにおいては、例えば、所管省庁を同じくする複数の業界が情報共有体制を構築する動きが見られるなど、新しい連携が生まれつつあります。「官民や業界といった従来の枠を超えて」との記載は、官民関係や業界区分を前提としつつも、それに囚われない新しい動きの推進等を想定したものであり、趣旨としては明確と考えますので、原案のとおりとします。 御意見の内容については、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。
66	公益財団法人笹川平和財団	4．3．1　自由、公正かつ安全なサイバー空間の堅持	戦略本文に係る意見	IoT通信プロトコル等サイバー空間における国際標準の策定において主導的な立場を確保する旨を記載すべき。	本戦略（案）（4.1.3(1) IoTシステムにおけるサイバーセキュリティの体系の整備と国際標準化）において、「官民が連携の下、安全なIoTシステムを実現するために求められるサイバーセキュリティに関する基本的な要素等の国際標準化に向けた取組を推進する」と記載されており、これに基づく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。
67	特定非営利法人日本セキュリティ監査協会	4．3．1　自由、公正かつ安全なサイバー空間の堅持	戦略本文に係る意見	「既存の枠組みの存在」が何を想定しているのかが理解できるように「各種の国際条約等を踏まえた既存の枠組み」と修正すべき。	「既存の枠組み」の中には国際条約の他、国内法、国際的な協力に係る取組、政府の関与のあり方やルール形成のプロセス等が含まれますので、原案のとおりとし、御意見の内容については、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。
68	個人（2）	4．3．2　我が国の防御力・抑止力・状況把握力の強化	戦略本文に係る意見	「均衡性のある対抗措置」に基づく「サイバー攻撃能力」による「報復の抑止」を明示すべき。	本戦略（案）（4.3.2(2)① 実行的な抑止のための対応）において、「我が国は、悪意ある主体の行動を抑止し、国民の安全・権利を保障するため、国家の関与が疑われるものも含め、我が国の安全保障を脅かすようなサイバー空間における脅威について、同盟国・有志国とも連携し、脅威に応じて、政治・経済・技術・法律・外交その他の取り得るすべての有効な手段と能力を活用し、断固たる対応をとる。」と記載しており、原案のとおりとします。
69	公益財団法人笹川平和財団	4．3．2　我が国の防御力・抑止力・状況把握力の強化	戦略本文に係る意見	関係機関の情報収集に関する法的要件の見直しの検討についても検討を進めるべき。	本戦略（案）（4.1.3 安全なIoTシステムの構築）において、「プライバシーの問題などの共通課題やそれぞれの取組について、全体像が俯瞰できる形で可視化するとともに、情報共有を行うための仕組みを構築する」と、また、「ネットワーク上の脆弱なIoT機器の対策については、パスワード設定に不備のある機器の調査・特定を行い、電気通信事業者において当該機器の利用者への注意喚起を円滑に行えるよう、所要の制度整備を着実に進める」と記載されており、これらに基づく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。

「サイバーセキュリティ戦略（案）」等に関する意見募集の結果一覧

通しNo	提出者	該当箇所	御意見の種類	御意見の要旨	御意見に対する主な考え方及び修正
70	特定非営利法人日本セキュリティ監査協会	4．3．2　我が国の防御力・抑止力・状況把握力の強化	戦略本文に係る意見	「カウンターサイバーインテリジェンス」について括弧や注釈などで意味を記載すべき。	御意見を踏まえ、以下のように注釈を追加します。 「情報通信技術を用いた外国の敵意ある諜報活動に対抗する情報防衛活動」
71	電気事業連合会	4．3．2　我が国の防御力・抑止力・状況把握力の強化	戦略本文に係る意見	国内の脅威情報共有（政府機関、地方公共団体、サイバー関連事業者、重要インフラ事業者、教育研究機関など）推進について記載すべき。	本戦略（案）（4.2.6 従来の枠を超えた情報共有・連携体制の構築）の箇所において、「官と民、業界、国内外といった枠を超えた情報の共有・連携を推進していく」と記載されており、これに基づく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。
72	次世代ICカードシステム研究会	4．3．3　国際協力・連携	戦略本文に係る意見	「国際標準」、「デジュール標準」、「デファクト標準」といった検討の場についても配慮すべき。	本戦略（案）（4.1.3(1) IoTシステムにおけるサイバーセキュリティの体系の整備と国際標準化）の箇所において、「官民が連携の下、安全なIoTシステムを実現するために求められるサイバーセキュリティに関する基本的な要素等の国際標準化に向けた取組を推進する」と記載されており、これに基づく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。
73	個人（6）	4．4．1　人材育成・確保	戦略本文に係る意見	おそらく、サイバー犯罪が出来るほどのプロは、中々居ない 日本の現場では”卑怯な奴は俺が捕まえる”と努力されています。これらの方は、日本のエライ方ではなく、庶民です。 国として、ある程度、身分保障が有っても、良いのではないか。	本戦略（案）（4.4.1人材育成・確保）において、「教育等を通じ、資格・評価基準等によって可視化された確かな知識と実践力を備えた人材が、適切な処遇を受け、更に実務経験を積み重ねることにより、人材の需要と供給が相応されるといった好循環の形成が必要である。」と記載しており、これに基づく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。
74	個人（7）	4．4．1　人材育成・確保	政策展開（サイバーセキュリティ2018）に係る意見	戦略マネジメント層の育成において、ITパスポート試験を必要な前提知識にしてはどうか。	サイバーセキュリティ2018（案）の4.1.(1)戦略マネジメント層の育成・定着において、「内閣官房において、戦略マネジメント層を担う人材の育成に向けて、必要な知識・スキルを身に着けるための試行的取組について検討する」との取組を盛り込むこととし、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。
75	個人（7）	4．4．1　人材育成・確保	政策展開（サイバーセキュリティ2018）に係る意見	情報処理の促進に関する法律を改正して、情報セキュリティマネジメント試験を「情報処理安全管理推進士」、登録システムアドミニストレータ試験（登録シスアド）を創設してはどうか。	サイバーセキュリティ2018（案）の4.1.(2)実務者層・技術者層の育成において、情報処理安全確保支援士制度や情報セキュリティマネジメント試験の普及を図ることとしており、これら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。
76	個人（7）	4．4．1　人材育成・確保	政策展開（サイバーセキュリティ2018）に係る意見	ITパスポート試験を合否制からスコア制によるITリテラシースタンダード1級、2級などを認定する方式に改めてはどうか。	サイバーセキュリティ2018（案）の4.1.(2)実務者層・技術者層の育成において、ITパスポート試験を含む情報処理技術者試験全般について、「内閣官房及び経済産業省において、情報セキュリティ人材を含めた高度IT人材の育成強化のため、情報セキュリティ分野を含めた各種情報分野の人材スキルを測る情報処理技術者試験について一層の周知及び普及を図る」との取組を盛り込むこととしました。 試験方式の変更については、現時点では検討しておりませんが、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。
77	個人（7）	4．4．1　人材育成・確保	政策展開（サイバーセキュリティ2018）に係る意見	ITパスポート試験について、従前にあった中問をペーパー方式で90分程度の試験として新たに新設してはどうか。	サイバーセキュリティ2018（案）の4.1(2)実務者層・技術者層の育成において、ITパスポート試験を含む情報処理技術者試験全般について、「内閣官房及び経済産業省において、情報セキュリティ人材を含めた高度IT人材の育成強化のため、情報セキュリティ分野を含めた各種情報分野の人材スキルを測る情報処理技術者試験について一層の周知及び普及を図る」との取組を盛り込むこととしました。 試験方式の変更については、現時点では検討しておりませんが、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。

「サイバーセキュリティ戦略（案）」等に関する意見募集の結果一覧

通しNo	提出者	該当箇所	御意見の種類	御意見の要旨	御意見に対する主な考え方及び修正
78	個人（7）	4．4．1　人材育成・確保	政策展開（サイバーセキュリティ2018）に係る意見	各省庁の全職員等について、ITパスポートの受験を義務化すべき。	政府の職員は、ITのスキルを向上させるため、総務省が実施している「情報システム統一研修」を受講することができますが、この研修の中には、ITパスポート試験のレベルと同等と位置付けられるよう用意された「情報システム入門」コースが含まれております。 これらの「情報システム統一研修」については、政府部内育成の専門人材である「橋渡し人材」を育成するために、政府機関における統一的な方針である「サイバーセキュリティ人材育成総合強化方針」等に基づき、役職に応じた段階的な受講を原則とするなどの取組を進めています。 いただいた御意見は、上記の取組の実施や推進に当たっての参考とさせていただきます。
79	公益財団法人笹川平和財団	4．4．1　人材育成・確保	戦略本文に係る意見	民間の高度専門人材の採用拡大を検討する。	人材育成のカリキュラムについては、「サイバーセキュリティ人材の育成に関する施策間連携ワーキンググループ報告書」（平成30年5月）において、NICEのプログラムを含む事例に基づくモデルカリキュラムを例示しています。 また、各府省庁における人材確保・育成については、本戦略（案）（4.4.1(4) 各府省庁におけるセキュリティ人材の確保・育成の強化）に「各府省庁におけるセキュリティ人材の着実な確保・育成を継続して進めていく」と記載しており、具体的には、「サイバーセキュリティ人材育成総合強化方針」に基づき、各府省庁において情報セキュリティ・ITに関する専門的知識・経験を有する者を任期付職員として積極的に採用するなどの取組を進めています。いただいた御意見は、これらの取組の実施や推進に当たって参考とさせていただきます。
80	一般社団法人サイバーリスク情報センター産業横断サイバーセキュリティ人材育成検討会	4．4．1　人材育成・確保	戦略本文に係る意見	戦略案の主旨について賛同。 以下の点を補強することで、戦略の影響力および効果が更に高まる。 1．産学官、各業界、各業界、産業横断などの多様な連携を促進することが肝要。 2．信頼の輪に基づく民間の主体的かつ持続的な活動を促進することで、迅速かつ柔軟な対応の実現とその実効性を高めることに繋がる。 3．セキュリティ人材育成を継続的に推進すること自体が大きな課題。我が国の産業構造・業務形態・人事慣行などの実状を踏まえたセキュリティ人材への多様なニーズに答えることを考慮すべき。 4．セキュリティ人材に少ない日本の経営層を支えるセキュリティ統括人材（戦略マネジメント層に該当）は重要な存在。	賛同の御意見として承りました。 「1．持続的かつ効果的な協調体制を構築・発展させるために、産学官、各業界、業界横断などの多様な連携を促進することが肝要。」と、「2．信頼の輪に基づき、民間（産業界）の主体的かつ持続的な活動（特に事例・ノウハウの共有など）を促進することで、迅速かつ柔軟な対応の実現とその実効性を高めることに繋がる。」につきまして、本戦略（案）（4.4.1 人材育成・確保）において、「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・確保を強化していく」と記載しており、これに基づく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。 「3．全ての施策を支えるセキュリティ人材育成を継続的に推進すること自体が大きな課題。また、我が国の産業構造・業務形態・人事慣行などの実状を踏まえた、セキュリティ人材への多様なニーズにこと得ることを考慮すべき。」につきまして、戦略マネジメント層、実務者層・技術者層、あるいは突出した能力を有しグローバルに活躍できる人材の育成について記載しており、御意見の主旨も踏まえて取組を進めてまいります。 「4．特にセキュリティの専門家が少ない日本の経営層を支えるセキュリティ統括人材（戦略マネジメント層に該当）の存在は、より重要なものと位置付け」につきまして、本戦略（案）（4.4.1(1) 戦略マネジメント層の育成・定着）において「サイバーセキュリティに係るリスクを認識し、事業継続と価値創出に係るリスクマネジメントを中心となって支える立場」として「戦略マネジメント層」を位置付け、経営層の理解の促進と、その定着を図ってまいります。

「サイバーセキュリティ戦略（案）」等に関する意見募集の結果一覧

通しNo	提出者	該当箇所	御意見の種類	御意見の要旨	御意見に対する主な考え方及び修正
81	株式会社ラック	4．4．1　人材育成・確保	政策展開（サイバーセキュリティ2018）に係る意見	・民間主導での、雇用機会、キャリアパス創出、適切な処遇が確保されることが重要。 ・短期で成果を上げるため、民間で既に行われているキャリアパスの明確化等の取組を参照する等、関係する主体との連携を推進してほしい。	人材の需要（キャリアパスや雇用機会）につきましては、「サイバーセキュリティ人材の育成に関する施策間連携ワーキンググループ報告書」（平成30年5月）（2．（3）　各層別の役割とキャリアパス）において「戦略マネジメント層」と「実務者層・技術者層」について想定されるキャリアパスを記載しており、一般の民間企業での参考としていただくことで、キャリアパスや雇用機会の創出の促進を図っております。 また、同報告書では、産業サイバー人材育成検討会の第1期報告書やIPA（ITSS+）での人材定義を紹介し、同様の取組の連係を図っております。 御意見の内容については、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	株式会社ラック	4．4．1　人材育成・確保	政策展開（サイバーセキュリティ2018）に係る意見	先般制度化された登録セキスペについて、個人や民間企業等の資格取得・保持への更なるインセンティブ付与策を検討いただきたい。	サイバーセキュリティ2018（案）の4.1(2)実務者層・技術者層の育成において、「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）制度の着実な実施と当該制度の普及のため、企業や団体への周知等を積極的に行う」との取組を盛り込むこととし、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。
83	株式会社ラック	4．4．1　人材育成・確保	政策展開（サイバーセキュリティ2018）に係る意見	若年層に対する情報モラル教育の一環として、関連法令に係る普及啓発の強化、教員養成課程や教員の研修への盛り込み、各地で普及啓発に取り組む者へのインセンティブ付与策を検討していただきたい。	サイバーセキュリティ2018（案）の4.1(3)人材育成基盤の基盤、4.3.全員参加による協働において、「文部科学省において、独立行政法人教職員支援機構と連携し、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」及び、「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」との取組をもりこむこととしました。 御意見の内容については、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。
84	株式会社ラック	4．4．1　人材育成・確保	政策展開（サイバーセキュリティ2018）に係る意見	高度なサイバーセキュリティ技術を持つ人材となることが期待される若年層向け環境整備に係る民主導の取り組みについて、各主体のよりいっそう積極的な関与を促進いただきたい。	サイバーセキュリティ2018（案）の4.1(3)人材育成基盤の基盤及びにおいて、「文部科学省において、新学習指導要領の実施を見据え、児童生徒の発達の段階に応じた、プログラミング的思考や情報セキュリティ、情報モラル等を含めた情報活用能力を培う教育を一層推進する」及び「総務省において、NICTに組織した「ナショナルサイバートレーニングセンター」における「SecHack365」の取組を通じて、若年層のICT人材を対象に、高度なセキュリティ技術を本格的に指導し、セキュリティイノベーターの育成に取り組む」との取組を盛り込むこととし、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。
85	個人（3）	4．4．1　人材育成・確保	戦略本文に係る意見	リボルビングドアなど官民交流の仕組みを作ることが人材不足を解消する一つの方法であると考える。	本戦略（案）（4.4.1 人材育成・確保）において、「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・確保を強化していく」と記載しており、これに基づく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。
86	一般社団法人新経済連盟	4．4．1　人材育成・確保	戦略本文に係る意見	国内の人材育成で、海外の知見を取り入れる旨の記載が必要。	本戦略（案）（4.4.1(5) 国際連携の推進）において、「我が国のサイバーセキュリティ人材の育成においても、国内で完結するのではなく、可能な限りグローバルな規模で切磋琢磨できるようにするべきである」及び「海外の人材育成を行う組織との間で様々な連携を促すための仕組み作りを主要国との連携の下で進める」と記載しており、国内での人材育成に海外からの知見を積極的に取り入れるという趣旨についても包含しているため、原案のとおりとします。

「サイバーセキュリティ戦略（案）」等に関する意見募集の結果一覧

通しNo	提出者	該当箇所	御意見の種類	御意見の要旨	御意見に対する主な考え方及び修正
87	個人（8）	4．4．1　人材育成・確保	戦略本文に係る意見	横断的施策に関して組織間のバラつきを埋めるため情報処理安全確保支援士制度を核とした専門人材の活用プラットフォームを構築することが必要と考える。	情報処理安全確保支援士制度においては、登録者の氏名、連絡先、得意分野・スキル等をウェブ上で公開することで、企業による活用の促進を図っています。今後も当該制度の普及に向け、企業や団体への周知を積極的に行うこととしており、御指摘の点も、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。
88	個人（2）	4．4．2　研究開発の推進	戦略本文に係る意見	現状の攻撃者優位から防御者優位の状況に転換するための重要な基盤技術の1つとして、帰属特定技術の研究開発を推進する必要がある。	本戦略（案）（4.4.2(1) 実践的な研究開発の推進）において、「トレーサビリティ（追跡可能性）の確保とこれらに対する攻撃の検知・防御に関する研究開発を進める」と記載しており、これに基づく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。
89	公益財団法人笹川平和財団	4．4．2　研究開発の推進	戦略本文に係る意見	サイバーセキュリティ産業の育成については、政府の重要な横断的施策として特記することが望ましいため、「4.4.2. サイバーセキュリティ産業の育成」として政府による研究機関のACE指定等の創設やサイバーセキュリティ産業育成の国家戦略特区の設定の検討に関する文章を追加すべき。	本戦略（案）（4.1.1(3) 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ビジネスの強化）において、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ビジネスの強化のための各種の施策を推進する旨、また同（4.4.1(5) 国際連携の推進）において、海外の人材育成を行う組織との間での様々な連携を促すための仕組み作りを推進する旨を記載しており、これらに基づく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。
90	株式会社ラック	4．4．2　研究開発の推進	政策展開（サイバーセキュリティ2018）に係る意見	いわゆるコンピュータ・ウイルスに関する罪の成立要件を具体的かつ網羅的にお示しいただきたい。 また、同罪、不正アクセス禁止法その他の関係法令について、いわゆるセーフハーバールールの導入を検討いただきたい。	サイバーセキュリティ2018（案）の1.1(1)経営層の意識改革において、「内閣官房において、企業が積極的なサイバーセキュリティ対策を講じる上で事業者が特に認識しておくべき関係法令集の作成を念頭に、その体制について検討を行う」との取組を盛り込むこととし、制度上の課題に関する調査・研究を推進していきます。
91	個人（9）	4．4．3　全員参加による協働	戦略本文に係る意見	「サイバーセキュリティ教育」の定義が曖昧な上、「情報モラル教育」の“一部”としてしまうと、“悪さをしない”ということだけに限定されるのではないか。 あらためて、情報安全を確保するという意味での“サイバーセキュリティ”を明確にすべき。そろそろ、積極的な“セキュリティマインド”を醸成するという意味での「サイバーセキュリティ教育」を前面に押し出すべき。 せめて、「情報モラル教育及びサイバーセキュリティ教育」としていただきたい。	本戦略（案）では、「自由、公正かつ安全なサイバー空間」を目指す上で、サーバーセキュリティに関する国民一人一人の理解を幅広い観点から促していくことを意図しております。御意見も踏まえ、主旨を明確にするため、以下のように修文することとします。 「学校教育での情報活用能力の育成を通じて、サイバーセキュリティについての教育を推進する。」

「サイバーセキュリティ戦略（案）」等に関する意見募集の結果一覧

通しNo	提出者	該当箇所	御意見の種類	御意見の要旨	御意見に対する主な考え方及び修正
92	公益財団法人笹川平和財団	5. 推進体制	戦略本文に係る意見	中長期的には、 ・内閣サイバーセキュリティセンターを発展的に機能強化しサイバーセキュリティ庁として独立の機関とすべき。同庁への各府省の監督、サイバー攻撃の検知・収集・分析、サイバー攻撃に対処するための指揮命令及び予算要求の権限付与等について検討すべき。 ・インターネット利用者に対するサイバーセキュリティ対策賦課金の導入についても検討するべき。 【理由】 ・国家支援のサイバー攻撃や所属不明の大規模サイバー攻撃など高度・大規模なサイバー攻撃の対処まで民間の自主的な取り組みに任される ・様々な行政機関が分散的にサイバーセキュリティの人材育成・産業育成を実施している	本戦略(案)（5. 推進体制）において、「内閣サイバーセキュリティセンターを中心に関係機関の一層の能力強化を図る」に記載しており、内閣サイバーセキュリティセンター及び関係機関の能力強化及び必要な予算の確保を図っていくこととしており、今後の取組の参考とさせていただきます。 なお、御意見も踏まえ、必要な予算の確保に関する趣旨を明確にするため、以下のように修文することとします。 「各府省庁の施策が着実かつ効果的に実施されるよう、経費の見積もり方針を定め、政府としての必要な予算の確保と執行を図る。」
93	次世代ICカードシステム研究会	5. 推進体制	戦略本文に係る意見	今回の戦略では「個人・組織による平時からの対策と連携」として民間の協力が求められており、本戦略の全体のロードマップについてもお示し頂きたい。	本戦略（案）（3.2. 目指すサイバーセキュリティの基本的な在り方）において、「3つの観点（中略）からサイバーセキュリティに関する官民の取組を推進することとし、サイバー空間における安全・安心と経済発展を両立させ、信頼できるサイバー空間が自律的・持続的に進化・発展することを目指す」と記載し、3年間の諸施策の目標及び実施方針を明確にしています。 また、それを達成するための具体的な施策についても、本戦略（案）（5. 推進体制）において「各年度の年次計画を作成する」と記載しているように、各年度の年次計画において明らかにすることとしています。
94	経団連産業技術本部	5. 推進体制	政策展開（サイバーセキュリティ2018）に係る意見	内閣サイバーセキュリティセンターのリーダーシップの下、これらの施策が着実に実行に移されるとともに、2020年の東京オリンピック・パラリンピックに向け、政党・省庁・業界・組織・地域等の壁を越えて、Society 5.0の実現に不可欠なサイバーセキュリティ強化に向けた取り組みが進展することを期待する。	賛同意見として承りました。
95	電気事業連合会	5. 推進体制	戦略本文に係る意見	下記のとおり修正してはどうか。 【修正案】 また、本部は、本戦略で示された方向性に基づき、各府省庁の施策が効果的に実施されるよう、実行費用の見積もり方針を定め、政府としての最適な予算の確保と執行を図る。 【理由】 国の姿勢は「やむを得ない経費」との意識が表れているのではないか。	サイバーセキュリティ基本法第25条で、本部の事務について「関係行政機関の経費の見積りの方針（中略）の作成」等とされていることを踏まえて記載しており、御指摘の「やむを得ない経費」という趣旨ではないため、原案のとおりとします。
96	個人（10）	–	不明	日中韓3カ国きょう情報通信相会合がおかしい。日本人の個人情報を中国に売り渡す動きではないか。	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。

「サイバーセキュリティ戦略（案）」等に関する意見募集の結果一覧

通しNo	提出者	該当箇所	御意見の種類	御意見の要旨	御意見に対する主な考え方及び修正
97	個人（11）	–	不明	・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、御意見として承ります。