「次期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：令和3年（2021）年７月12日～8月10日（30日間）

■ 意見総数：24者から115件

【意見の種類】

・戦略本文に係るご意見：94件

- ・総論（策定の趣旨・背景、本戦略における基本的な理念、サイバー空間をとりまく課題認識 等）：19件
- ・経済社会の活力の向上及び持続的発展：20件
- ・国民が安全で安心して暮らせるデジタル社会の実現：32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：15件
- ・推進体制：4件

・「サイバーセキュリティ2021（2020年度年次報告・2021年度年次計画）（案）」のうちの2021年度年次計画（案）に係るご意見：19件

・その他のご意見：2件

「次期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

No	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
戦略本文に係る意見				
1	1～3（1．策定の趣旨・背景、2．本戦略における基本的な理念、3．サイバー空間をとりまく課題認識）	戦略本文に係る意見	脆弱性の存在するAI技術の適用によるリスクを追記するべきある。	ご指摘を踏まえ、「AI技術の様々なシステムへの活用」をリスク要因として追記いたしました。 （本文P.7　／226行目）
2	1～3（1．策定の趣旨・背景、2．本戦略における基本的な理念、3．サイバー空間をとりまく課題認識）	戦略本文に係る意見	ロシアのサイバー工作は技術力の劣勢を相殺するためである旨を注記するべきである。	ロシアが「軍事的及び政治的目的の達成に向けて影響力を行使するため」にサイバー攻撃等を行っているとみられるとの記載は、注釈45に示した既存の政策文書を参考に記載を行っております。
3	1～3（1．策定の趣旨・背景、2．本戦略における基本的な理念、3．サイバー空間をとりまく課題認識）	戦略本文に係る意見	「2.2　基本原則」に以下を追記してほしい。 「政治・経済・軍事・技術・法律・外交」 【理由】 他との整合性の観点	4.3.2（2）「サイバー攻撃に対する抑止力の向上」において、「サイバー空間における脅威について、平素から同盟国・同志国と連携し、政治・経済・技術・法律・外交その他の取り得る全ての有効な手段と能力を活用し」と包括的な手段・能力を活用する旨記載されており、原案のとおりとさせていただきます。
4	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	「4.3.2（2）①実効的な抑止のための対応」に以下を追記してほしい。 「政治・経済・軍事・技術・法律・外交」 【理由】 他との整合性の観点	No.3参照
5	1～3（1．策定の趣旨・背景、2．本戦略における基本的な理念、3．サイバー空間をとりまく課題認識）	戦略本文に係る意見	「3.サイバー空間をとりまく課題認識」に以下を追記してほしい。 「以下では、経済社会と国家安全保障をとりまく環境変化、国際情勢のそれぞれから、考慮すべきリスク要因を整理し、また、それらが具体的にどのように顕在化しているかについて示していく。」 【理由】 3．3を引き出すため。	ご指摘のとおり、経済社会活動への影響が結果として安全保障上のリスクにつながり得ると認識しております。脅威等の分析について3.3節全体に記載しておりますが、国家安全保障をとりまく環境変化については3.3.2国際情勢からみたリスクに記載しており、原案のとおりとさせて頂きます。
6	1～3（1．策定の趣旨・背景、2．本戦略における基本的な理念、3．サイバー空間をとりまく課題認識）	戦略本文に係る意見	「3.3 近年のサイバー空間における脅威の動向」に以下を追記してほしい。 「組織犯罪や国家の関与が疑われる攻撃が多く発生しており、海外では選挙に対する攻撃をはじめとする民主プロセスへの干渉や、サプライチェーンの弱点を悪用した大規模な攻撃、制御系システムを対象とした攻撃をはじめ広範な経済社会活動と国家安全保障に影響を与え得るインフラへの攻撃が猛威を奮っている。」	ご指摘を踏まえ、「経済社会活動』、ひいては国家安全保障』に影響を与え得る」と修文いたします。 （本文P.9　／270行目）

「次期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

No	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	1～3（1. 策定の趣旨・背景、2. 本戦略における基本的な理念、3. サイバー空間をとりまく課題認識）	戦略本文に係る意見	「3.3 近年のサイバー空間における脅威の動向」に以下を追記してほしい。 「こうしたサイバー攻撃により、生産活動の一時停止、サービス障害、金銭被害、個人情報窃取、機密情報窃取など、経済社会活動と国家安全保障に大きな影響が生じている。」	ご指摘を踏まえ、「経済社会活動』、ひいては国家安全保障』に大きな影響が生じ『得る状況となって』いる。」と修文いたします。 （本文P9. ／285行目）
8	1～3（1. 策定の趣旨・背景、2. 本戦略における基本的な理念、3. サイバー空間をとりまく課題認識）	戦略本文に係る意見	「デジタル社会の実現に向けた重点計画（2021年6月18日閣議決定）」において、「情報セキュリティの専門人材」として明確に位置づけされ、情報処理の促進に関する法律という国内法に根拠を持つ唯一の情報セキュリティ人材である「情報処理安全確保支援士」の必置化はもとより、活用にすら触れていないのは政府決定を無視した重大な瑕疵であると考える。	本戦略の編集方針（我が国のサイバーセキュリティ施策の方向性を示すものであり、一部を除き具体の施策や制度名について特定記載を行わない）から明示的な記載は行っておりませんが、情報処理安全確保支援士制度を念頭に、4.4.2(2)において「資格制度活用に向けた取組」を位置づけております。
9	1～3（1. 策定の趣旨・背景、2. 本戦略における基本的な理念、3. サイバー空間をとりまく課題認識）	戦略本文に係る意見	情報処理安全確保支援士の必置化を進めないことにより、情報セキュリティに関する専門性を想起させる低品質な民間資格の乱立を招いている。悪質な事業者及びそれにより認定された資格者による、情報セキュリティ対策としては不適切なサービスの提供が、情報セキュリティ人材全体の評価を低下させることもリスクとして考慮すべきである。	ご指摘の観点を含め、3.1(2)において「経済社会が抱える脆弱性の観点」で想定されるリスクとして、「人材不足・偏在」、また「企業組織や技術分野における人材不足がサイバーセキュリティに係る製品・サービス、技術を、過度に海外に依存する状況を招き得る」状況を位置づけております。
10	4. 1. 2 地域・中小企業におけるDX with Cybersecurityの推進	戦略本文に係る意見	情報処理安全確保支援士の登録状況において、首都圏への人材集中が著しい。これは、情報処理安全確保支援士に限らず全ての情報処理技術者において、高度情報処理技術者試験の合格者数を見ても、同じことが言える状況である。 つまり、デジタルトランスフォーメーションに取り組もうとしても、それに必要なサイバーセキュリティの強化を実現してくれる人材が、特に地方においては不足しているといった現状を認識し、その解消も戦略として定めるべきであると考える。	ご指摘の観点を含め、4.1.2において「人材の育成・マッチング（中略）が行われる場の形成の促進」を進めることを位置づけており、また、4.4.2(1)②において人材の活躍の観点から詳述して位置づけております。
11	4. 2. 3 経済社会基盤を支える各主体における取組①（政府機関等）	戦略本文に係る意見	「4.2.3 経済社会基盤を支える各主体における取組①（政府機関等）」に以下を追記してほしい。 国はこうした状況に対応したシステムの設計、運用・監視、インシデント対応、監査等について「情報処理安全確保支援士や高度情報処理技術者試験合格者といった免許・資格に根拠を持つ者による」体制・人材の在り方を検討する。	外部人材の採用については、情報処理安全確保支援士を含む資格の有無等についても総合的に勘案しつつ実施しているところです。 4.4.2(2)において「人材の活躍促進やマッチング促進の観点から、（中略）資格制度活用に向けた取組、自衛隊・警察も含む公的機関における専門人材確保の推進にもあわせて取り組む」と位置づけており、いただいたご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。

「次期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

No	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
12	4．1．3　新たな価値創出を支えるサプライチェーン等の信頼性確保に向けた基盤づくり	戦略本文に係る意見	セキュリティ製品・サービスの信頼性確保について、第三者による客観的な検証・評価が必要だという本書の記載には賛成である。しかし、それを行う人材の客観的な検証・評価に論及されていない点は画竜点睛を欠く。まずは現状法律で「情報セキュリティ専門人材」と定められた「情報処理安全確保支援士」を、これら検証・評価の仕組みの中心的な存在と位置づけ、充分に能力が担保された人材を確保することによる信頼性確保が重要であると考える。	ご指摘のとおり、検証を実施する者の信頼性確保の観点は重要であると考えており、4.1.3(3)において「検証ビジネスの市場形成に向け、国としても、検証事業者の信頼性を可視化する取組の検討に取り組む」と位置づけております。 なお、経済産業省が示している「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き　別冊3 検証人材の育成に向けた手引き」において、検証手法ごとの必要なスキル・知識が示されており、こうした要素を示すものとして資格制度の活用は重要であると認識しております。
13	4．1．4　誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着	戦略本文に係る意見	セキュリティ教育の担い手として〝自称〟経験者による誤った啓発活動を防止することも「正しい情報セキュリティ知識」を身に着ける為に必要である。例えば、情報人材が不足している地方自治体に対して総務省が人材派遣制度を提供しているが、派遣者リストにおける「情報セキュリティ」担当者に、ほとんど情報処理安全確保支援士がおらず、多くの素人が自らの経験に基づいて誤った内容を支援する、といったことが実際の弊害として発生している。	ご指摘のとおり、教育側へ正しい知識を涵養する観点から、セキュリティ教育が、正しい知識を有する担い手により行われることは重要であると認識しております。 ご指摘の取組はサイバーセキュリティに特化した取組ではございませんが、こうした取組を含め、ご意見として承り、今後の施策の推進に当たって参考にしてまいります。
14	4．2．1　国民・社会を守るためのサイバーセキュリティ環境の提供	戦略本文に係る意見	本戦略は情報セキュリティのCIA（＝confidentiality：機密性、integrity：完全性、availability：可用性）におけるCに力を入れて作られているように見受けられるが、情報セキュリティにとってIとAも同様に重要である。 国民が直接関与する政府・自治体のシステム関係部門の長、決裁サービス、金融機関といった分野の担当取締役においては情報処理安全確保支援士を優先的に必置化し、「情報処理におけるCIA安全が確保されないサービスが提供されることはない」といった「人的体制」を整えることに着手し、そのことを広く国民に周知することで、安心・安全を醸成することが最優先で着手すべきことであると考える。	「次期サイバーセキュリティ戦略」4.2.4(1)及び4.4.2(2)で言及しているとおり、「官民連携に基づく重要インフラ防護の推進」及び「資格制度活用に向けた取組」を推進してまいります。 具体的には、 ・「デジタルガバナンス・コード」において「望ましい取組」として「情報処理安全確保支援士の取得を会社として奨励」していることが位置づけられており、この活用促進に取り組んでまいります。 ・重要インフラ分野においては、「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版改定版）」において、従業インフラ事業者等は従業員に対して情報セキュリティに関連する十分な教育・トレーニングを実施する、特に、「情報処理安全確保支援士」等の資格取得等が期待される旨を記載しており、引き続き指針の整備・浸透に取り組んでまいります。 ・政府機関においては、有資格者を含む専門人材確保や、人材育成等に向けた専門職種ごとの資格等の整理を進めてまいります。

「次期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

No	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
15	4．2　国民が安全で安心して暮らせるデジタル社会の実現	戦略本文に係る意見	国・地方公共団体・重要インフラ事業者においては、サイバーセキュリティの与える社会的インパクトの急速な拡大を踏まえて、組織の規模や性質、利用者（又は住民）の人数に応じて、情報処理安全確保支援士のCISO等上級職位への抜擢も含めた必置化を定め、それに伴う内部人材の抜擢や外部人材の登用を早急に進めるべきである。	No.14参照
16	4．2．2　デジタル庁を司令塔とするデジタル改革と一体となったサイバーセキュリティの確保	戦略本文に係る意見	「4.2.2 デジタル庁を司令塔とするデジタル改革と一体となったサイバーセキュリティの確保」に以下を追記してほしい。 準公共部門等の情報システムの整備及び管理の基本的な方針（以下「整備方針」という。）において、情報処理安全確保支援士の活用をはじめとしたサイバーセキュリティについても基本的な方針を示し、・・・	No.14参照
17	4．2．4　経済社会基盤を支える各主体における取組②（重要インフラ）	戦略本文に係る意見	「4.2.4経済社会基盤を支える各主体における取組②（重要インフラ）」に以下を追記してほしい。 ・重要インフラ事業者等のサイバーセキュリティに関し、基準の策定、演習及び訓練、「情報処理安全確保支援士の必置人数」、情報の共有その他 ・セキュリティ対策は組織一丸となって取り組むことが重要であるから、国は経営層「に情報処理安全確保支援士資格を持つ者をCISOとして必置することを求めることによって」リーダーシップが遺憾なく発揮できる体制の構築を図っていく。	No.14参照
18	4．4．2　人材の確保、育成、活躍促進	戦略本文に係る意見	情報処理安全確保支援士の活用 （民間から政府機関への採用の必須条件とするなど）	外部人材の採用については、情報処理安全確保支援士を含む資格の有無等についても総合的に勘案しつつ実施しているところです。 4.4.2(2)において「人材の活躍促進やマッチング促進の観点から、（中略）資格制度活用に向けた取組、自衛隊・警察も含む公的機関における専門人材確保の推進にもあわせて取り組む」と位置づけており、いただいたご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。

「次期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

No	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
19	1～3（1．策定の趣旨・背景、2．本戦略における基本的な理念、3．サイバー空間をとりまく課題認識）	戦略本文に係る意見	今後、法改正等により強制力が伴う非常事態宣言の発令あるいは都市封鎖法制が実現した際を見据え、クラウド事業者によるデータセンターへのアクセス権の確保について明確に担保してほしい。	クラウドサービスがサイバー空間において欠かせないインフラとなっていることを鑑みれば、クラウドサービスが安定的・継続的に提供されることについて、サイバーセキュリティに限らず、様々な観点から検討することは重要だと考えます。 ご意見いただいた内容については、仮定の話のため、直接的なお答えは難しいものの、コロナ禍においても、クラウドサービス提供者が、安定的にサービス提供を行うことも重要と考えます。 引き続き、利用者が安心してクラウドサービスに情報資産を委ねることができるように、日本社会全体における安心安全なクラウドサービス利用環境を構築すべく検討を進めて参ります。
20	1～3（1．策定の趣旨・背景、2．本戦略における基本的な理念、3．サイバー空間をとりまく課題認識）	戦略本文に係る意見	サイバーセキュリティ戦略が策定されることは誠に時宜を得たものであり、戦略の策定に賛同する。	賛同意見として承りました。
21	1～3（1．策定の趣旨・背景、2．本戦略における基本的な理念、3．サイバー空間をとりまく課題認識）	戦略本文に係る意見	利用者及び関係者は、サイバー攻撃の対象になり得る情報資産の存在、在り方や環境における利用の認識についても考える必要がある。	ご指摘の点を含め、3.1(2)において、「経済社会が抱える脆弱性の観点」からのリスクとして、「サイバーセキュリティに関するリテラシーの差異（中略）が攻撃者に狙われ得る弱点となる可能性がある」と位置づけております。
22	1～3（1．策定の趣旨・背景、2．本戦略における基本的な理念、3．サイバー空間をとりまく課題認識）	戦略本文に係る意見	総合行政ネットワーク（LGWAN）を利用しての通信については、VPNによる暗号化には頼らずに、自前での独自の暗号化を行っての通信を行ってほしい。 また、日本国における電気通信事業者が提供する電子メール役務について全てインターネット上等においてTLSでの保護が行われるようにしてほしい。	戦略案4.2.3の記載の通り、政府機関においては、情報システムの開発・構築段階も含めたあらゆるフェーズで対策を強化することとしており、個々のシステムの特性・要求に応じて最適なセキュリティ対策の導入を引き続き進めて参ります。
23	4．2．1　国民・社会を守るためのサイバーセキュリティ環境の提供	戦略本文に係る意見	「4.2.1　国民・社会を守るためのサイバーセキュリティ環境の提供」について ※御意見はNo.22と同意	No.22参照
24	4．目的達成のための施策	戦略本文に係る意見	「サイバーセキュリティー対策」が重要な構造。「検知（ディテクション）⇒分析（アナライズ）⇒対処（リアクションメソッド）」での「サイバーセキュリティー対策」が重要。	賛同意見として承りました。 本戦略（案）５．推進体制において「情報収集・分析機能に加え、サイバー攻撃の速やかな検知・分析・判断・対処を一体的サイクルとして行う機能の強化のため、所要の体制について検討する」こととしております。

「次期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

No	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
25	4. 目的達成のための施策	戦略本文に係る意見	従来の「境界型セキュリティ」の限界の認識を示されているので、3つの方向性においてDXとサイバーセキュリティの同時推進に「ゼロトラストセキュリティ」を追記してほしい。	ご指摘のとおり、従来の「境界型セキュリティ」の限界に関する認識を踏まえて施策の推進していくことが重要と考えており、具体的な取組も、既に戦略において位置づけております。 例えば、4.2.3において、「従来の『境界型セキュリティ』だけでは対処できないことも現実となりつつあることから、国はこうした状況に対応したシステムの設計、運用・監視、インシデント対応、監査等やそれを担う体制・人材の在り方を検討する」、「従来の「境界型セキュリティ」にとどまらない、常時診断・対応型のセキュリティアーキテクチャの実装に向けた技術検討と政府統一基準群の改定を行い、可能なところから率先して導入を進め、政府機関等における実装の拡大を進めていく」と記載しております。
26	4. 目的達成のための施策	戦略本文に係る意見	「リスクマネジメント」に係る取組強化について、セキュリティ自動化技術に基づく「サイバー衛生」によるリスク可視化を、「4（2）②」に追記してほしい。	ご指摘を踏まえ、自動化技術の活用等による効率的な防御について追記いたしました。（本文P.12　／379行目） なお、具体的な取組として例えば、4.2.3における「常時診断・対応型のセキュリティアーキテクチャの実装に向けた技術検討（中略）を行い、可能なところから率先して導入を進め、政府機関等における実装の拡大を進めていく」、4.4.1における「巧妙かつ複雑化したサイバー攻撃や今後本格普及するIoT等への未知の脅威に対応するため、（中略）AI技術による攻撃挙動解析の自動化技術に係る研究開発を実施する」「実際にAIを活用したセキュリティ製品やサービスの商用化が進んでいる。国は、AI技術に関する総合的な戦略等に基づき、AIを活用した民間のサイバー対策を引き続き後押しするとともに、『予防』『検知』『対処』の各フェーズにおいてAIを活用した高効率かつ精緻な対策技術の確立を推進していく」といった取組が挙げられる。
27	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	リスク可視化のための最も重要なサイバー自動化技術による「サイバー衛生力」の向上について追記してほしい。	ご指摘の点は、4.3.2(3)「サイバー空間の状況把握力の強化」において、「サイバー攻撃等を検知・調査・分析等するための技術の開発・活用等あらゆる有効な手段について幅広く検討を進める。」と包括的に記載されておりますが、別途のご指摘を踏まえ、4(2)②に、横断的な施策として、自動化技術の活用等による効率的な防御について追記いたしました。（本文P.12　／379行目）

「次期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

No	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
28	4. 目的達成のための施策	戦略本文に係る意見	「4.(2)公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保」に以下を追記してほしい。 官民連携体制によるナショナルサート 【理由】 官民連携を強調 ・ナショナルサートの名前を検討してほしい。一案として、National Cybersecurity Insident and Emergency Response Teamを提案します。	戦略案で言及しているナショナルサートは、政府機関のみならず、既存の情報共有体制や官民学を含めた国内外の関係者との連携も念頭に置いています。ご意見も参考に引き続き取り組んで参ります。
29	4. 2. 1 国民・社会を守るためのサイバーセキュリティ環境の提供	戦略本文に係る意見	「4.2.1(4)①包括的なサイバー防御の総合的な調整を担うナショナルサート機能等の強化」に以下を追記してほしい。 官民学連携によるナショナルサート 【理由】 官民連携を強調	No.28参照
30	4. 2. 6 多様な主体によるシームレスな情報共有・連携と東京大会に向けた取組から得られた知見等の活用	戦略本文に係る意見	「4.2.6(2)包括的なサイバー防御に資する情報共有・連携体制の整備」に以下を追記してほしい。 官民学連携によるナショナルサート 【理由】 官民連携を強調	No.28参照
31	4. 2. 7 大規模サイバー攻撃事態等への対処態勢の強化	戦略本文に係る意見	「4.2.7 大規模サイバー攻撃事態等への対処態勢の強化」に以下を追記してほしい。 国が一丸となったシームレスな対処態勢を官民学連携によるナショナルサートを核として強化する。 【理由】 官民連携を強調	No.28参照
32	5. 推進体制	戦略本文に係る意見	「5.推進体制（24行目～25行目）」に以下と修文するべきである。 官民学連携によるナショナルサート 【理由】 産と民は区別できない。	No.28参照
33	5. 推進体制	戦略本文に係る意見	「5.推進体制（9行目～10行目）」は以下と修文するべきである。 ~~産学官民~~官民学連携 【理由】 産と民は区別できない。	「全員参加による協働」の取組まで含め、本戦略全体を推進していくための内閣サイバーセキュリティセンターの役割として「産学官民連携」としております。ご意見も参考に引き続き取り組んで参ります。

「次期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

No	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
34	4. 目的達成のための施策	戦略本文に係る意見	一般にトレーサビリティはプライバシーの保護などとトレードオフの関係にあるという認識が強い。トレーサビリティの語を、犯罪追跡可能性などの別の語で置き換えてほしい。	ご指摘の通り、トレーサビリティの確保にあたり、プライバシー保護等の考慮も重要であると考えております。ご指摘のような懸念も踏まえ、4.2.1において、「トレーサビリティの確保（中略）によって、サイバー犯罪の温床となっている要素・環境の改善を図る。その際、『情報の自由な流通の確保』の原則を踏まえて取組を進める。」と位置づけております。なお、「情報の自由な流通の確保」については、2.2(1)において、「プライバシーへの配慮を含め、情報の自由な流通で他者の権利・利益をみだりに害することがないようにしなければならないことも明確にされるべきである。」と位置づけております。
35	4. 目的達成のための施策	戦略本文に係る意見	現在、我が国においては、政府(NISC)と民間の専門組織が連携してナショナルサートの役割を担っている。ナショナルサートの枠組みの整備がこの分担を見直すことも視野に入れる場合には、国内外の関係者への丁寧な説明が必要であると考える。	今後とも、国内外に向けた丁寧な説明に努めて参ります。
36	4. 目的達成のための施策	戦略本文に係る意見	今時の戦略において対処調整センターとナショナルサート機能拡充はどのように関連しているのか。	国は、深刻なサイバー攻撃に対して、オールジャパンで力を合わせて対応することが求められる中、サイバーセキュリティ対処調整センターのような既存の情報共有体制間の連携を進めることを含め、サイバー攻撃に対し、情報収集・分析から政策立案・措置に至るまでの国全体として網羅的な対応が可能となるナショナルサートの枠組みを強化していくことを目指しています。
37	4．1　経済社会の活力の向上及び持続的発展	戦略本文に係る意見	官民がリアルタイムで脅威情報を共有するようなシステム(例えば、天気予報システムなど)の枠組みや法制の整備が必要と考える。	脅威情報の共有として、サイバーセキュリティ協議会の運営、脆弱性情報の共有としては情報セキュリティ早期警戒パートナーシップ等の取組があり、本戦略にも位置づけてございますが、更なる改善を含めたご意見として承ります。
38	4．1．1　経営層の意識改革	戦略本文に係る意見	経営層に求められる『プラス・セキュリティ』知識の体系化に加えて、コミュニケーションを行うセキュリティ専門家に要求される「事業・サービス等」に対する業務理解の向上についても、実現できる環境整備をお願いしたい。	ご指摘のとおり、セキュリティ専門家においても、事業・サービス等に対する業務理解の向上があわせて重要であることを認識しております。「サイバーセキュリティ体制構築・人材確保の手引き」においても、セキュリティ担当者に求められる知識・スキルとして「自社の業務プロセスへの理解」も位置づけられていると承知しており、これらの文書を含め、4.4.2(1)②に位置づけているとおり、「企業・組織内での機能構築（中略）に関するプラクティス実践の促進に向け、（中略）参考となる手引き資料の活用促進（中略）に取り組む」こととしております。

「次期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

No	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
39	4．1．2　地域・中小企業におけるDX with Cybersecurityの推進	戦略本文に係る意見	中小企業の「DX with Cybersecurity」を推進するためには、これまでにない品質の高いクラウドサービス（サプライチェーンリスク対策、脆弱性即応対策、リアルタイム監査等のリスクマネジメントを備えた）を提供する仕組みとロードマップを国民に示すと同時に、クラウドサービスの質を高めるための機能提供、もしくは利用者として参画する重要インフラ企業、セキュリティ専門企業の役割を周知していくことが必要と考える。	ご指摘の通り、中小企業においてクラウドサービスの利用が普及することが想定される中で、需要・供給両面から施策を推進することが重要と考えております。クラウドサービス提供に向けては、総務省において「クラウドサービス提供における情報セキュリティ対策ガイドライン」が策定されており、また、クラウドサービス利用に向けては、IPAにおいて「中小企業のためのクラウドサービス安全利用の手引き」が示されているなど、これらの活用促進に引き続き取り組んでまいります。 また、ご指摘の観点を含め、4.2.1(2)において、「利用者が安心してクラウドサービスに情報資産を委ねることができるよう国は、信頼性が高く、オープンかつ使いやすい高品質クラウドの整備を推進するとともに、政府機関や重要インフラ事業者等の利用者がクラウドサービスを利用する情報システムの設計及び開発の過程において考慮すべきサイバーセキュリティのルールを利用者、クラウドサービス事業者、システム受託事業者等の関係者と連携しながら策定する。」「国は政府情報システムのためのセキュリティ評価制度（ISMAP ）等の取組を活用したクラウドサービスの安全性の可視化の取組を政府機関等から民間にも広く展開し、一定のセキュリティが確保されたクラウドサービスの利用拡大を促進する。」と位置づけております。
40	4．1．2　地域・中小企業におけるDX with Cybersecurityの推進	戦略本文に係る意見	地域のDXにおける課題を集め、中央省庁に伝達する仕組を構築し、地域における課題の収集ときめ細やかな政策立案に活かせるよう期待する。	ご指摘の観点の重要性は認識しており、総務省及び経済産業省において、それぞれの地方局を通じた情報共有やニーズの吸い上げを図るとともに、4.1.3(1)に位置づけている「コンソーシアム」の取組の中で、地域におけるコミュニティ形成に関するワーキンググループを立ち上げており、地域ごとの課題を含めた課題収集・解決に向けた検討を行う体制を設けております。
41	4．1．2　地域・中小企業におけるDX with Cybersecurityの推進	戦略本文に係る意見	地域、中小企業という切り口だけではなく、製造業においてもDX化が進んでいるが、製造現場ではセキュリティ対策が十分にできていない。 IPAは、制御システムセキュリティガイドラインを出しているが、電力事業者以外は対策が進んでおらず、昨今の工場、製造現場におけるDX化を踏まえた制御システムへのリスク対応について政府から事業者に対策を求めるよう方策も検討してほしい。（工場向けのセキュリティガイドラインなど）	ご指摘のとおり、工場自動化等の動向を踏まえ、セキュリティ対策を推進することは重要であると考えており、4.2.1(1)②において、「国は（中略）工場の自動化（中略）等の新規分野に関するサイバーセキュリティの対策指針・行動規範の策定等を通じて、安心・安全を確保する」と位置づけております。

「次期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

No	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
42	4．1．2　地域・中小企業におけるDX with Cybersecurityの推進	戦略本文に係る意見	テレワークの普及によって、広く民間企業の間で、「ゼロトラストネットワーク」の活用が進んでいくことが予想される。 ゼロトラスト基盤の活用は、接続のための厳格な認証、許可の上に成り立っており、ゼロトラスト基盤の活用に向けた、本人、デバイス　などの認証の仕組み、基準、ガイドラインなど出すことも検討してほしい。	ご指摘のとおり、テレワークの普及等に応じて、ガイドラインや様々な解説資料等の整備を進めることが重要と考えており、4.4.3にその旨位置づけております。例えば、本年5月には、「テレワークセキュリティガイドライン」が改訂され、中小企業向けの手引き（チェックリスト）が整備されるなど、順次内容の充実が図られております。
43	4．1．2　地域・中小企業におけるDX with Cybersecurityの推進	戦略本文に係る意見	中小企業がデジタル化と同時にサイバーセキュリティ対策に取り組むには、セキュリティ人材・知見の不足などの課題を対処する必要があるとの見方に同意する。 その上で、廉価なクラウドサービスについて、政府と国内ITベンダーにおいて、利用者がコストメリットを享受できることに配慮しながら明確な運用ルール、セキュリティ基準を開発し、その上でサービス開発を促し、さらに、それらを踏まえて地域コミュニティの形成と「共助」を進めるべきと考える。	ご指摘の通り、中小企業においてクラウドサービスの利用が普及することが想定される中で、需要・供給両面から施策を推進することが重要と考えております。クラウドサービス提供に向けては、総務省において「クラウドサービス提供における情報セキュリティ対策ガイドライン」が策定されており、また、クラウドサービス利用に向けては、IPAにおいて「中小企業のためのクラウドサービス安全利用の手引き」が示されているなど、これらの活用促進に引き続き取り組んでまいります。
44	4．1．3　新たな価値創出を支えるサプライチェーン等の信頼性確保に向けた基盤づくり	戦略本文に係る意見	「4.1.3新たな価値創出を支えるサプライチェーン等の信頼性確保に向けた基盤づくり」を以下のように修文すべきである。 こうした観点から、信頼性確保の基盤づくりに取り組み、ひいては先端技術・イノベーションの社会実装に係る取組と相まって、世界の先端動向を適切に取り入れ且つ日本の独自技術の発展を促し、~~他国に依存しない~~日本発の製品・サービスの育成に取り組む。 【理由】 日本発の製品・サービス育成に賛同する。一方、他国の先端技術を一切排除し他国に依存せずゼロから自国開発することは現実的でないことは明らかである。	ご指摘を踏まえ、「他国に『過度に』依存しない」と修文いたします。 （本文P．17／538行目）
45	4．1．3　新たな価値創出を支えるサプライチェーン等の信頼性確保に向けた基盤づくり	戦略本文に係る意見	サプライチェーンの信頼性確保において、セキュリティ対策費を管理費として上乗せするなど、標準的な業務システムやサービスの提供を公共機能として構築し提供していくことを中長期的に実現していくことが重要と考える。	ご指摘の観点は重要であると考えており、ご意見として承ります。 なお、「情報サービス・ソフトウェア産業における下請適正取引等の推進のためのガイドライン」においては、「下請事業者が、個人情報保護等の法制度の変更やそのための情報セキュリティ等の強化に伴うコスト増に対応するため、単価の変更を行いたいと親事業者に求めたにも関わらず、十分に協議することなく下請代金の額を据え置いた場合」や、「サイバー攻撃は高度化多様化してきており、新たな制度や情勢に対応するための作業内容や費用は増大傾向にある」中で「こうした要素を考慮せずに、同じ下請金額で一方的に下請事業者に発注を行う場合」は、「買いたたきに該当するおそれがある」とされていると承知しております。

「次期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

No	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
46	4．1．3　新たな価値創出を支えるサプライチェーン等の信頼性確保に向けた基盤づくり	戦略本文に係る意見	中小企業がコンソーシアムを活用することは難しく、中小企業を「任務保証」の当事者とするには、コンソーシアムの取組を支援することではなく、品質の高いクラウドサービスを積極的に利用して頂くことが重要と考える。	4.1.2に記載しているとおり、両面の取組の推進が重要であると考えております。
47	4．1．3　新たな価値創出を支えるサプライチェーン等の信頼性確保に向けた基盤づくり	戦略本文に係る意見	「他国に依存しない日本発の製品・サービス」について、製品・サービスの内容よりも今後は持ってるデータが勝負になり得ることが考えられるため、「日本独自の攻撃実態などのデータとその取り組み」についても重要と考える。	ご指摘の観点の重要性は認識しており、4.1.3(4)において、「サイバーセキュリティに関する情報を国内で収集・蓄積・分析・提供していくための知的基盤を構築し、安全保障の観点から情報管理に留意しつつ、産学官の結節点として、当該情報を産官学の様々な主体に効果的に共有する」ことを位置づけており、この中で、国産の脅威情報の蓄積・提供が期待されます。
48	4．1．3　新たな価値創出を支えるサプライチェーン等の信頼性確保に向けた基盤づくり	戦略本文に係る意見	中小企業に「任務保証」を当事者意識とするため、（1）サプライチェーンの信頼性確保、の施策として[4.1.2]に記述のある「中小企業へ普及させようとしているクラウドサービス」に、CDMのようなリスクマネジメントを可能とした仕組みを積極的に取り入れることを検討してほしい 。 ※）CDM：Continuos Diagnostic and Mitigation	4.1.2においては、「今後は、中小企業に広くクラウドサービスの利用が普及することも一つの重要な選択肢となると想定される」と記載しております。 なお、CDMについては、4.2.3において「常時診断・対応型のセキュリティアーキテクチャの実装に向けた技術検討と政府統一基準群の改定を行い、可能なところから率先して導入を進め、政府機関等における実装の拡大を進めていく」と位置づけており、戦略の推進に当たって参考にしてまいりたいと思います。
49	4．1．4　誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着	戦略本文に係る意見	子供向けのサイバーセキュリティ教育が最重要と考える。 子供向けのサイバーセキュリティに関する注意事項の啓発ではなく、義務教育とする計画を早急に立てていただきたい。	ご指摘のとおり、サイバーセキュリティに関するリテラシーを身につけてもらうことは重要であると考えており、子供向けにサイバーセキュリティを含む情報モラルに関する教育等を推進していくことについて、本戦略にも位置づけております。 なお、義務教育という観点では、新しい学習指導要領において、技術・家庭科（技術分野）の中でセキュリティを含む内容が位置づけられており、また、情報モラルに関する指導を充実させるための動画教材の充実等に引き続き取り組んでまいります。
50	4．1．4　誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着	戦略本文に係る意見	GIGAスクール構想において、教員が情報端末を活用する授業術を学ぶ機会がない。新型コロナウイルスの感染拡大に伴い、迅速な対応が求められており、学校外の人材の積極的に活用するなど、情報端末を活用した授業術の獲得方策を検討してほしい。	ご指摘のとおり教師のICT活用に対する支援の重要性を認識しており、4.1.4において教師の日常的なICT活用の支援等を行う支援員等の配置等について記載しております。
51	4．1．4　誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着	戦略本文に係る意見	不適切な情報技術の利用を防ぐために、リテラシーを高めると同時に情報モラルや情報法に係る最低限の学びを行うために、NPO団体や弁護士など外部人材の協力を得て、正しくICTを活用する人材の育成に努めることが必要と考える。	ご指摘のとおり様々な地域の担い手と連携して取組を進めていくことが重要と認識しており、4.1.4にその旨を位置づけております。施策の具体化に向けて、ご意見として承ります。

「次期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

No	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
52	4．1．4　誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着	戦略本文に係る意見	情報教育を既存の教育機関のみによって実現することは難しく、情報教育を行う機関や組織の設立・運営について、自治体が中心となって推進する計画を全国横断的に立案・実現していくことも必要と考える。	ご指摘のとおり既存の教育機関のみに取組を委ねるのではなく、必要な支援を実施していくことが重要と考えており、ご意見として承り、関係省庁に伝達させていただきます。
53	4．1．4　誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着	戦略本文に係る意見	外国勢力からのデマ・偽情報・フェイクニュース(いわゆる影響工作)などを随時検知し、国民に啓発を行う体制の構築の具体化が必要である。	ご意見として承り、関係省庁に伝達させていただきます。 なお、偽情報の問題に対しては、多様なステークホルダーによる多面的な議論が行われ、プラットフォーム事業者、ファクトチェック機関、メディアなど関係者間の協力が進められることが必要であると認識しております。
54	4．2．1　国民・社会を守るためのサイバーセキュリティ環境の提供	戦略本文に係る意見	・安全保障関連の記述との関係から、特に価値観を共有しない国（中国、ロシア、北朝鮮）出身の民間企業のサービスに対する規律の強化が必要である ・「利用者保護」の定義については、いわゆる「ネット弱者」である未成年者等の保護も含まれると理解している一方で、そうしたネット弱者の保護の観点からの安全・安心の確保についても記述すべきである	特定の国に関連することのみを理由として、特定の企業が提供するサービスについて何等かの規制をする考えは政府としてはありません。他方、サイバー空間の公共空間化やサプライチェーンの深化を踏まえれば、サイバー空間を構成する機器、ソフトウェア、データ、サービス等のサプライチェーンの構成要素における信頼性は極めて重要であると認識しており、例えば戦略案4.2.1(1)①では、これらの構成要素における信頼の確保を図るための仕組みの構築や、トレーサビリティの確保等を記載しています。 また、高齢者や若年層も含め多くの国民が利用するサービスについても、サプライチェーン管理を含めたサイバーセキュリティ対策が重要と認識しており、その旨戦略案4.2.1(1)③に記載しています。 また、戦略案4.2.1(5)では、現在認知されているサイバー攻撃の多くが国民の個人情報や国際競争力の源泉となる知的財産に関する情報を目的としていることを踏まえ、経済安全保障の観点を含めた対策についても記載しています。 頂いたご意見も参考に、引き続きサイバー空間の信頼性確保に取り組んで参ります。
55	4．2．1　国民・社会を守るためのサイバーセキュリティ環境の提供	戦略本文に係る意見	米国大統領令でも触れている、ソフトウエアサプライチェーンセキュリティの強化を参考に、以下の内容を追加検討してはどうか。 「政府が使用するソフトウエアは、極めて重要でソフトウエア開発の透明性確保が大切。セキュアなソフトウエア開発のガイドラインとガイドライン適合の成果物提示、信頼できるソースコードのサプライチェーン、ソフトウエア部品表SBOM（Software Bill Of Materials）の提示、脆弱性開示プログラムへの参画、ソフトウエアセキュリティ向上に向け政府の購買力の活用、ソフトウエアラベリング（認証ラベル）検討等。（原文参照をしてください）」	ご指摘の通り、ソフトウェアの信頼性確保は極めて重要であり、戦略案4.2.1(1)①では、ソフトウェアのサプライチェーンの構成要素における信頼の確保を図るための仕組みの構築やトレーサビリティの確保等について記載しています。ご意見も参考に引き続き取り組んで参ります。

「次期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

No	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
56	4．2．1　国民・社会を守るためのサイバーセキュリティ環境の提供	戦略本文に係る意見	米国大統領令でも触れている、政府システムの調査と修復の能力向上を参考に、以下の内容を追加検討してはどうか。「イベントログの収集と提供による官民相互活用及び保存ログ種別・保存期間・保護方法・暗号化方法などの要件明確化。（原文を参照してください）」	ご指摘の通り、セキュリティ対策の向上にはイベントログの効果的な収集・分析・活用が重要であり、例えば国においては、戦略案4.2.3に記載の通り、従来の「境界型セキュリティ」にとどまらない、常時診断・対応型のセキュリティアーキテクチャーの実装に向けた技術検討等を行うこととしています。 また、戦略案4.2.1(3)においても、ログの重要性に鑑みて、ログの保存の在り方について、関係するガイドラインを踏まえ関係事業者における適切な取組を推進することとしています。 ご意見も参考に引き続き取り組んで参ります。
57	4．2．1　国民・社会を守るためのサイバーセキュリティ環境の提供	戦略本文に係る意見	インシデント発生時には国及び重要インフラ事業者が、IaaS提供事業者のみではなく、PaaS及びSaaS提供事業者とも【正確な】情報共有ができるフレームワークの構築をお願いしたい。	クラウドサービスのインシデントは多くの利用者に影響を与えかねず、また様々なサービスが相互に連関・連鎖しているため、影響が拡大していくことも考えられます。そうした観点から、戦略案4.2.1(2)では、安心安全なクラウドサービス利用環境の構築に係る取組について記載しており、ご意見も参考に、検討を進めて参ります。
58	4．2．2　デジタル庁を司令塔とするデジタル改革と一体となったサイバーセキュリティの確保	戦略本文に係る意見	「ISMAP制度の継続的な見直し」にあたっては、以下の点にご配慮してほしい。 ・監査自体にとても時間と労力がかかり、費用・時間共に企業側の負担が膨大である。 ・申請、登録の機会が年に4回と限られるため、申請、登録を常時受け付ける等のプロセスに変更してほしい。	ISMAPは、常時申請を受け付けた上で、登録の可否を決定するISMAP運営委員会を四半期に一回、定期的に開催することとしておりますが、必要に応じてISMAP運営委員会を臨時開催し、登録の可否を決定する場合もあります。御意見につきましては、今後の施策の検討や実施に当たって、参考とさせていただきます。
59	4．2．1　国民・社会を守るためのサイバーセキュリティ環境の提供	戦略本文に係る意見	セキュリティ産業は、サービスとして客観的な品質基準が整備されていない未成熟なレベルにあると考えます。そのため、セキュリティ環境の整備とともに産業として成立させるための計画や支援も必要と考える。	ご指摘の通り、セキュリティ産業の育成は重要な課題であるとの認識のもと、戦略案4.1.3(3)ではセキュリティ製品・サービスの信頼性確保や、日本発の製品・サービスの育成について記載しております。
60	4．2．1　国民・社会を守るためのサイバーセキュリティ環境の提供	戦略本文に係る意見	サイバー犯罪への対策に関しては、既存の警察・消防組織と連携しつつ、例えば横断的な全国規模でラストワンマイルを担当する組織の確立が有効と考える。	例えば戦略案4.2.1(3)では、サイバー防犯に係るボランティア等の関係機関・団体と連携し、広報啓発等を推進する等を記載しており、引き続き国民一人一人の皆様にも行き届く対策を心掛けて参ります。

「次期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

No	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
61	4．2．1　国民・社会を守るためのサイバーセキュリティ環境の提供	戦略本文に係る意見	以下の取り組みの推進に期待している。 「国は中小企業、海外拠点、取引先等、サプライチェーン全体を俯瞰し、発生するリスクを自身でコントロールできるよう、サプライチェーン内での情報共有や報告、適切な公表等を推進する産業界主導の取組を支援する。」	昨今のサイバー空間の情勢を踏まえれば、サプライチェーン全体でセキュリティを確保する重要性はますます高まっていると認識しており、今後もご期待に沿えるように検討を進めて参ります。
62	4．2．1　国民・社会を守るためのサイバーセキュリティ環境の提供	戦略本文に係る意見	「国は政府情報システムのためのセキュリティ評価制度（ISMAP）等の取組を活用したクラウドサービスの安全性の可視化の取組を政府機関等から民間にも広く展開し、一定のセキュリティが確保されたクラウドサービスの利用拡大を促進する」にあたり、民間での活用方針について、今後具体的な内容を示してほしい。	具体的なスケジュールは定まっていませんが、まずは政府機関における運用を進め、運用状況を踏まえながら、将来的には民間における利用も推奨していくことを検討しています。
63	4．2．1　国民・社会を守るためのサイバーセキュリティ環境の提供	戦略本文に係る意見	海賊行為による著作権侵害等については、警察庁又は文化庁に職務としてその整理を行わせるようにしてほしい。	国は、サイバー空間を悪用する犯罪者の摘発を推進するとともに、事業者への働きかけ等を行うことにより、官民が連携してサイバー犯罪対策を推進して参ります。
64	4．2．2　デジタル庁を司令塔とするデジタル改革と一体となったサイバーセキュリティの確保	戦略本文に係る意見	ISMAP 制度の民間での活用方針について、今後具体的な内容を示してほしい。	具体的なスケジュールは定まっていませんが、まずは政府機関における運用を進め、運用状況を踏まえながら、将来的には民間における利用も推奨していくことを検討しています。
65	4．2．2　デジタル庁を司令塔とするデジタル改革と一体となったサイバーセキュリティの確保	戦略本文に係る意見	NISCは必要があればデジタル庁にも指導を行い、国のサイバーセキュリティが適切に確保されるようにしてほしい。	デジタル庁とNISCの関連性について一例を挙げれば、 デジタル庁が作成する情報システムの整備・管理の基本的な方針において、サイバーセキュリティに関する基本的な方針を示すこととし、当該部分については、サイバーセキュリティ戦略本部と緊密に連携して作成することとしています。 また、デジタル庁にセキュリティの専門チームを置き、デジタル庁が整備・運用するシステムを中心とする検証・監査を実施するとともに、内閣サイバーセキュリティセンター（NISC）がその体制を強化しつつ、デジタル庁が整備・運用するシステムを含めて国の行政機関等のシステムに対するセキュリティ監査等を行って参ります。 これらにより、国民の重要な情報資産を保護して参ります。

「次期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

No	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
66	4．2．3　経済社会基盤を支える各主体における取組①（政府機関等）	戦略本文に係る意見	国は情報システムの設計・開発段階から講じておくべきセキュリティ対策として、DevSecOpsに基づくクラウドサービス等の継続監視を追記してほしい。	戦略案4.2.3では、「情報システムの開発・構築段階も含めたあらゆるフェーズでの対策を強化していく」と記載しております。また、デジタル・ガバメント推進標準ガイドライン（各府省情報化統括責任者（CIO）連絡会議決定）においても、要件定義・設計開発・運用等の各段階においてセキュリティ対策を適切に行うこととしており、クラウドサービスについてもこうした対策検討の対象となっています。なお、特にご指摘の政府情報システムが利用するクラウドサービスに関しては、各政府機関において適切なリスク評価、リスク管理を行うとともに、セキュリティ評価制度（ISMAP）において統一的なセキュリティ要求基準が適切に実施されているか、継続的に確認しております。 ご意見も参考に引き続き取り組んで参ります。
67	4．2．3　経済社会基盤を支える各主体における取組①（政府機関等）	戦略本文に係る意見	政府統一基準群の改定と運用やクラウド監視に対応したGSOC機能強化の検討にあたっては、IaaSのみではなく、PaaS及びSaaSクラウドサービス提供事業者にもヒアリング・協議を行ってほしい。	ご意見も参考に、引き続き検討を進めて参ります。
68	4．2．4　経済社会基盤を支える各主体における取組②（重要インフラ）	戦略本文に係る意見	令和3年4月30日、内閣官房、個人情報保護委員会、金融庁、総務省は、「政府機関・地方公共団体等における業務でのLINE利用状況調査を踏まえた今後のLINEサービス等の利用の際の考え方（ガイドライン）」を策定・公表したが、同ガイドラインを一般化（SNS等の民間サービス全般を対象）する方向性の記述を求める。特に、当該SNS等事業者が外国の事業者である場合には、データの保管場所が日本国外にあるケースが多く、その場合、同国の法令に基づくガバメントアクセスが深刻なセキュリティ・リスクとなる可能性があることから、本次期サイバーセキュリティ戦略においても、上記対応について明記していただきたい。	例えば、「地方公共団体における情報セキュリティポリシーに関するガイドライン（令和2年12月版）」では、「8.4クラウドサービスの利用」において、「情報セキュリティ管理者は、クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用されるリスクを評価して委託先を選定し、必要に応じて委託事業の実施場所及び契約に定める準拠法・裁判管轄を指定しなければならない。」とあり、ご指摘の観点も含めて適切なサービスを選定することとしております。戦略案4.2.4(2)にも、同ガイドラインに基づくセキュリティ対策が着実に実施されるよう記載されているところ、ご意見も参考に引き続き取り組んで参ります。
69	4．2．4　経済社会基盤を支える各主体における取組②（重要インフラ）	戦略本文に係る意見	「4.2.4（1）官民連携に基づく重要インフラ防護の推進」に以下を追記してほしい。 国民生活及び社会経済活動、さらに国家安全保障の基盤である重要インフラサービス・・・	国民生活及び社会経済活動の基盤である重要インフラサービスの安全かつ持続的な提供の確保は、我が国の安全保障上も重要であることはご指摘の通りであり、その観点から例えば戦略案4.3.2(1)では重要インフラの任務保証の重要性等を記載しています。 また、安全保障の観点からの任務保証の重要性や対策については、戦略案4.3.2(1)①において記載しております。 ご意見も参考に引き続き取り組んで参ります。

「次期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

No	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	4．2．4　経済社会基盤を支える各主体における取組②（重要インフラ）	戦略本文に係る意見	「4.2.4　経済社会基盤を支える各主体における取組②（重要インフラ）」について 重要インフラ防護にあたり、必要に応じて、国及び重要インフラ事業者が、IaaS提供事業者のみではなく、PaaS及びSaaS提供事業者とも【正確な】情報共有ができるフレームワークの構築をお願いしたい。	クラウドサービスのインシデントは多くの利用者に影響を与えかねず、また様々なサービスが相互に連関・連鎖しているため、影響が拡大していくことも考えられます。そうした観点から、戦略案4.2.1(2)では、安心安全なクラウドサービス利用環境の構築に係る取組について記載しており、ご意見も参考に、検討を進めて参ります。
71	4．2．4　経済社会基盤を支える各主体における取組②（重要インフラ）	戦略本文に係る意見	「4.2.4　経済社会基盤を支える各主体における取組②（重要インフラ）」に記載の文書「重要インフラ事業者等による情報収集を円滑にするための横断的な情報共有体制の一層の充実」について ※御意見はNo.70と同意	No.70参照
72	4．2．4　経済社会基盤を支える各主体における取組②（重要インフラ）	戦略本文に係る意見	地方公共団体に対する支援について、地方公共団体が内製化（商用パッケージの組み合わせやカスタマイズ）をできる仕組みが必要と考える。	戦略案4.2.4(2)のとおり、地方公共団体情報システムの標準化、行政手続のオンライン化等、必要な諸制度の整備を推進し、地方公共団体において適切なセキュリティが確保されつつ、新たな時代の要請にも柔軟に対応できるように、検討を進めて参ります。
73	4．2．4　経済社会基盤を支える各主体における取組②（重要インフラ）	戦略本文に係る意見	データ所在場所についての問題から、「クラウド・バイ・デフォルト」については不適切であると考える。最低、行政機関が使用し、データが所在するようにするのは、国内リージョン内限定、等の制限を行うべきであると考える。	例えば、「政府情報システムにおけるクラウドサービスの利用に係る基本方針（2021 年（令和3 年）3 月30 日、各府省情報化統括責任者（CIO）連絡会議決定）」においては、SaaSの選定に際しては、「我が国の法律及び締結された条約が適用される国内データセンタと我が国に裁判管轄権があるクラウドサービスを採用候補とするものとする」等、ご指摘の点も踏まえた取組を行っています。
74	4．2．6　多様な主体によるシームレスな情報共有・連携と東京大会に向けた取組から得られた知見等の活用	戦略本文に係る意見	「4.2.6(1)分野・課題ごとに応じた情報共有・連携の推進」に以下を追記してほしい。 セプターやISACを含む・・ 【理由】 NISCのセプターがまず日本での情報共有の中心のため。	情報共有は、セプター、ISACといった様々な既存の枠組みの充実・強化と、そうした様々な情報共有の枠組みの相互連携が重要であり、ご意見も踏まえ、「セプター」についても記載させていただくとともに、引き続き情報連携の充実に取り組んで参ります。 （本文P.27　／918行目）
75	4．2．6　多様な主体によるシームレスな情報共有・連携と東京大会に向けた取組から得られた知見等の活用	戦略本文に係る意見	ナショナルサートに関連する記述で、4.2.1と4.2.6で記述が異なるのはどのような理由か。	4.2.6(2)にも「国内外の関係者との連絡調整について十分な技術的能力及び専門的な知識経験を有する専門機関」を追記する方向で検討させていただきます。 （本文P.28　／925行目）

「次期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

No	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
76	4．2．7　大規模サイバー攻撃事態等への対処態勢の強化	戦略本文に係る意見	「4.2.7大規模サイバー攻撃事態等への対処態勢の強化」を以下のように修文すべきである。 更に、国及び各主体は官民連携の取組において座学での教育や机上訓練の実施に加え、サイバーレンジといった模擬空間を活用したより実践的な訓練の実施等を通じてセキュリティ人材を育成及び活用することで、大規模サイバー攻撃事態等への対処を強化する。 【理由】 即戦力になりうる人材の育成には、より実践的な環境での訓練が必要であることは明らかな一方、教育現場では未だに座学や机上演習等に終始するケースが散見される。	訓練対象者のレベルやニーズに応じて、サイバーレンジといった模擬空間を活用した訓練も行われており、今後もより実践的な訓練を広く導入していくなど、ご意見も参考に引き続き検討を進めて参ります。
77	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	戦略本文に係る意見	中国、ロシア、北朝鮮といった国への言及がある一方で、こうした国出身の企業が脅威となり得ることについての記述がない。	特定の国に関連することのみを理由として、特定の企業が提供するサービスについて何らかの規制をする考えは政府としてはありません。他方、サイバー空間の公共空間化やサプライチェーンの深化を踏まえれば、サイバー空間を構成する機器、ソフトウェア、データ、サービス等のサプライチェーンの構成要素における信頼性は極めて重要であると認識しており、例えば4.2.1(1)①では、これらの構成要素における信頼の確保を図るための仕組みの構築や、トレーサビリティの確保等を記載しています。 また、戦略案4.2.1(5)では、現在認知されているサイバー攻撃の多くが国民の個人情報や国際競争力の源泉となる知的財産に関する情報を目的としていることを踏まえ、経済安全保障の観点を含めた対策についても記載しています。
78	4．4．1　研究開発の推進	戦略本文に係る意見	現在のAIのセキュリティの課題としての、学習データのバイアス、プロセスの不可視性、アルゴリズム固有の脆弱性等を明示して、研究の方向性を追記してほしい。	ご指摘を踏まえ、考え得る脅威について、注釈に追記いたしました。 （本文P.38　／1280行目）
79	4．4．1　研究開発の推進	戦略本文に係る意見	「4.4.2②量子技術の進展を見据えた対応」を以下のように修文すべきである。 以上のほか、「Beyond 5G」をはじめとした様々な技術トレンドを中長期的な視点から捉え、特にクラウドの安全利用促進のための具体的な可視化・監視技術（＊1）の検討やリビング・テストベッドの活用推進等を通じ、国として推進すべき技術課題の検討を不断に行っていく。 ＊1　基礎的な技術研究、政府、自治体によって有効に監視・運用するため具体的には次の三点が想定される。（1）クラウドの運用・可視化方法、（2）エンドツーエンドの通信の可視化、監視方法、（3）利用者端末の状態監視	ご指摘を含む技術の重要性は認識しており、4.2.1(1)において「利用者が安心してクラウドサービスに情報資産を委ねることができるよう、国は、信頼性が高く、オープンかつ使いやすい高品質クラウドの整備を推進する」ことを位置づけております。

「次期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

No	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
			【理由】 5GやAI、量子コンピュータ等の利用が促進に際し、データ通信量の増大は膨大なものとなり外部クラウドサービスの利用が必須となり、当該外部クラウドサービスの可視化や監視技術は、組織単位での運用負荷を軽減するため必ず隔離すしなければならない共通の技術です。それに関して本サイバーセキュリティ戦略で明示がない。	
80	4．4．1　研究開発の推進	戦略本文に係る意見	国産サイバーセキュリティ産業の育成にあたっては純国産産業の育成のみならず、海外の先端サイバーセキュリティ技術を国産企業で成熟させるというビジネスも考えられる。このようなビジネスマッチングを視野に入れた市場展開を推進していただくことをお願いしたい。	ご指摘の観点もサイバーセキュリティに係る先端技術・イノベーション活動を活性化させていくために重要であると考えており、4.1.3(3)において、「国産セキュリティ製品・サービスのグローバル展開に向けて、国際標準化に向けた取組や海外展示会への出展支援等を引き続き推進する」と位置づけております。ご意見として承り、戦略の推進に当たって参考にしてまいりたいと思います。
81	4．4．1　研究開発の推進	戦略本文に係る意見	実践的な研究開発テーマとして、NISTが提唱しているサイバーセキュリティフレームワークの発展を取り上げることをお願いしたい。	具体かつ個別の研究課題に関するご意見と承知いたしましたが、4.1.3(1)や4.2.1(1)に位置づけている各種フレームワークの策定等に向けて参考にしてまいりたいと思います。
82	4．4．2　人材の確保、育成、活躍促進	戦略本文に係る意見	情報処理技術者試験の在り方を抜本的に再検討し、2年後を目途に、新方式への移行が検討されている。抜本的に再検討するのであれば、名称独占型の国家資格として技術者個人の職業的地位を保障すべきではないか。	ご意見として承りました。個別政策の運用に関する論点でありますので、所管省庁に伝達させていただきます。
83	4．4．2　人材の確保、育成、活躍促進	戦略本文に係る意見	重度障がい者にとって就労につながるITスキルの証明であるCBT方式のITパスポート試験，基本情報技術者試験，情報セキュリティマネジメント試験の受験において「障害者差別解消法に基づいた合理的配慮」を国家の責務として講じてもらいたい。	ご意見として承りました。個別政策の運用に関する論点でありますので、所管省庁に伝達させていただきます。
84	4．4．2　人材の確保、育成、活躍促進	戦略本文に係る意見	【ITコーディネータの再定義】 経済産業省の推進資格としての位置付けではなく、その認定試験等の実施を独立行政法人情報処理推進機構IPAが行う、情報処理技術者試験に加えることを提案する。	ご意見として承りました。個別政策の運用に関する論点でありますので、所管省庁に伝達させていただきます。

「次期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

No	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
85	4．4．2　人材の確保、育成、活躍促進	戦略本文に係る意見	政府や行政機関で、従来の処遇を超えた特別措置を適用して、優秀なエンジニアを採用できるように環境整備をお願いしたい。	高度専門人材確保のための方策や活用の在り方については、引き続き関係各所において検討を進めて参ります。4.2.2(3)において「各府省庁において人材確保・育成計画を作成し、『サイバーセキュリティ・情報化審議官』等による司令塔機能の下、定員の増加による体制整備、研修や演習の実施、適切な処遇の確保についても着実に取り組む」「高度なサイバー犯罪や安全保障への対応等を行うため、外部の高度専門人材を活用する」ことなどを位置づけており、いただいたご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。
86	4．4．2　人材の確保、育成、活躍促進	戦略本文に係る意見	政府や行政機関で、従来の処遇を超えた特別措置を適用して、優秀なエンジニアを採用できるように環境整備をお願いしたい。 【理由】 サイバーセキュリティ人材育成においては、常に最新の情報やインフラ技術に接する環境の整備が不可欠であるが、人材育成において最新の環境を維持して育成することは単一組織では負荷が大きすぎることから、その整備（共用環境の整備）及び育成する人材のレベル分けについて本サイバーセキュリティ戦略を受けて、今後改めて検討する必要がある。	ご指摘のとおり訓練環境の提供は重要であると考えており、4.4.2(2)において「社会全体でサイバーセキュリティ人材を育成するための共通基盤を構築し、教育機関・教育事業者による演習事業実施が可能となるよう、講師の質の担保等に留意しつつ、産学に開放する」と位置づけております。
87	4．4．2　人材の確保、育成、活躍促進	戦略本文に係る意見	巧妙化・複雑化する脅威への対処にあたっては、業種や業務に関わらず、あらゆる角度から組織内のセキュリティ意識を隅々までいきわたらせることが重要と考える。そのため、これまでは業種に視点が置かれたISACなどが組織されてきたが、、総務、経理、製造、物流、経営等の業務視点から見た情報共有の仕組み作りが必要と考える。	業務視点で情報共有の仕組みを構築することには一定の課題があると考えられますが、4.1.3(1)に位置づけているとおり、昨年、産業界が一体となって中小企業を含むサプライチェーン全体でサイバーセキュリティ対策を推進することを目的とした「サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）」が立ち上げられるなどの動きもあり、目的に応じて様々な仕組みを活用いただくことが重要と考えております。

「次期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

No	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
88	4．4．2　人材の確保、育成、活躍促進	戦略本文に係る意見	DXw/CSに必要な人材確保・育成のための環境整備や共通基盤の構築等、理念や取り組みについて異論はない。 そのうえで、これらはセキュリティに関する一般的な知識を備えた人材の増員や育成には有益であるが、未知の問題へ対応し自ら解決策を見出せるような人材の発掘、その先の進路を活性化するものではないように思える。特に十代未満の若年層を対象に、自発的な興味を促せるような仕組みが必要かと思う（例えば「鳥人間コンテスト」や大学、高専対象の「ロボコン」のような類のもの）。	ご指摘のとおり若年層を含めた優秀な人材の育成・確保の視点は重要であると認識しており、4.4.2(2)において「実務者層・技術者層の育成に向けては、（中略）若年層向けのプログラム（中略）の実施（中略）など、官民で取組の推進が行われてきているところ、近年の脅威動向に対応するとともに、男女や学歴等によらない多様な視点や優れた発想を取り入れつつ、これら実践的な対処能力を持つ人材の育成に向けた取組を一層強化し、コンテンツの開発・改善を図っていく」と位置づけております。
89	4．4．2　人材の確保、育成、活躍促進	戦略本文に係る意見	「プラス・セキュリティ」知識については、サプライチェーンや業種・業界における連携・共有ができる分類のあり方の検討や、それら分類に対応した人材育成プログラムの整備、IT研修等を実施している企業における提供プログラムに対するラベリング等、エコシステムとなるよう推進してほしい。	ご意見として承り、戦略の推進に当たって参考にしてまいりたいと思います。また、引き続きご理解・ご協力をお願いいたします。
90	4．4．3　全員参加による協働、普及啓発	戦略本文に係る意見	中央省庁の政策の伝達と地域・地方の実態を相互に連携する仕組みづくりが急務だと考える。特に地域・地方のラストワンマイルにいるICT利用者に啓発情報や注意喚起、犯罪予防などを行う地域内の仕組みづくりや役割を担う人材の育成、組織の形成やその支援が必要と考える。	ご指摘のとおり、様々な関係者がお互いの役割分担の下で連携・協働することが重要であると考えており、本戦略に位置づけております。特に、犯罪対策としては、4.2.1(3)に「人材育成等の観点から、官民が連携したサイバー犯罪対策を推進するとともに、国民一人一人の自主的な対策を促進し、サイバー犯罪の被害を防止するため、サイバー防犯に係るボランティア等の関係機関・団体と連携し、広報啓発等を推進する」と位置づけております。
91	4．4．3　全員参加による協働、普及啓発	戦略本文に係る意見	カウンターインテリジェンスに係る人材の育成を政府レベルで検討する必要があると考える。	4.3.2(3)「サイバー空間の状況把握力の強化」において、関係機関における、「高度な分析能力を有する人材の育成・確保等について幅広く検討を進める」こと、「サイバーカウンターインテリジェンスに係る取組を進める」と記載しており、原案のとおりとさせていただき、いただいたご意見については今後の取組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。
92	5．推進体制	戦略本文に係る意見	省庁間の縦割りを廃し、政策の整合性を向上させる観点から、総務省・経済産業省のサイバーセキュリティ政策関係部署はNISCに統合すべきである。	本戦略（案）5．推進体制において「公的機関が限られたリソースを有効活用しつつその役割を果たせるよう、関係機関の一層の対応能力強化・連携強化を図る。その中で、内閣サイバーセキュリティセンターは、本部の事務局として、各府省庁間の総合調整及び産学官民連携の促進の要となる主導的役割を担う。」としております。ご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。

「次期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

No	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
93	5. 推進体制	戦略本文に係る意見	「サイバーセキュリティ2021」（案）を見て、関係機関において様々な施策が実行されていることを理解できた。 デジタル庁発足以降に、国・国民・社会を守るという観点と、各政府機関・団体・組織を守るという観点で、それぞれの司令塔となるべき組織とその施策について、今後さらに踏み込んだ戦略が示されることを期待している。	賛同意見として承りました。 ご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。
94	4．3．1 「自由、公正かつ安全なサイバー空間」の確保	戦略本文に係る意見	以下の取組みの推進に期待している。 「G20 大阪首脳宣言においてデジタル経済における「信頼性のある自由なデータ流通（Data Free Flow with Trust: DFFT）」を促進する必要性が確認されたこと、「プラハ提案」において 5Gセキュリティにおけるトラストの重要性が言及されたこと等に見られるように同盟国・同志国等と連携した国際的な取組に向けた動きが進展している。また我が国が目指す「自由、公正かつ安全なサイバー空間」の秩序形成に向けては、インターネット・ガバナンス・フォーラム等インターネット・ガバナンスに関するマルチステークホルダー・アプローチでの枠組みも発展してきている。」 「引き続き国際社会に対して我が国の基本理念を発信し、我が国の基本理念に沿う新たな国際ルールの策定に積極的に貢献するとともに、こうした国際社会のルール形成及びその運用が、国際社会の平和と安定及び我が国の安全保障に資するものとなるよう、あらゆる取組を行っていく。」	ご指摘のとおり、4.3.1(2)「サイバー空間におけるルール形成」において、「G20 大阪首脳宣言においてデジタル経済における「信頼性のある自由なデータ流通（Data Free Flow with Trust: DFFT）」を促進する必要性が確認されたこと、「プラハ提案」において5Gセキュリティにおけるトラストの重要性が言及されたこと等に見られるように同盟国・同志国等と連携した国際的な取組に向けた動きが推進している。また、我が国が目指す「自由、公正かつ安全なサイバー空間」の秩序形成に向けては、インターネット・ガバナンス・フォーラム等インターネット・ガバナンスに関するマルチステークホルダー・アプローチでの枠組みも発展してきている」、「引き続き国際社会に対して我が国の基本理念を発信し、我が国の基本理念に沿う新たな国際ルールの策定に積極的に貢献するとともに、こうした国際社会のルール形成及びその運用が、国際社会の平和と安定及び我が国の安全保障に資するものとなるよう、あらゆる取組を行っていく」と記載されており、賛同のご意見として承ります。

「次期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

No	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
サイバーセキュリティ2021に係る意見				
95	1～3（1. 策定の趣旨・背景、2. 本戦略における基本的な理念、3. サイバー空間をとりまく課題認識）	サイバーセキュリティ2021（2020年度年次報告・2021年度年次計画）（案）」のうちの2021年度年次計画（案）に係る意見	「1.2.2.3 経済社会基盤を支える各主体における情勢②（重要インフラ）」に以下を追記してほしい。 このように、クラウドサービスは利便性が高い反面、障害等の発生により重要インフラ事業者等が提供するサービスに影響が生じることから、外部サービスであるクラウドサービスを利用するに当たっては、利用契約で担保されている内容を踏まえつつ、適切な防御措置が必要であることを示す結果となった。加えてマルチクラウド環境利用時について、複数のクラウド環境を統合的に管理する必要性がさらに高まることが容易に想定される。 【理由】 マルチクラウド環境の利用が増加する中、今後必要となる防護措置を明示する必要があるため。	当該箇所は、2020 年度、国内外において重要インフラ分野等で発生したサイバーセキュリティインシデントについてファクトベースで記述したものであり、将来に向けた予測等には触れていません。なお、クラウドサービス利用時の予防措置に関しましては、次期サイバーセキュリティ戦略案4.2.1(2)新たなサイバーセキュリティの担い手との協調において、「政府機関や重要インフラ事業者等がクラウドサービスを用いた情報システムを設計及び開発する過程において考慮すべきサイバーセキュリティのルールを、クラウド利用者やクラウドサービス事業者、システム受託事業者等の関係者と連携しながら策定する」こととしております。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。
96	4. 1. 1 経営層の意識改革	サイバーセキュリティ2021（2020年度年次報告・2021年度年次計画）（案）」のうちの2021年度年次計画（案）に係る意見	サイバーセキュリティ経営ガイドライン実施状況の可視化ツールVer.1.0の可視化された状況の取扱いやその活用に関して、関係者間でコンセンサスが取れるように配慮した形で推進していただくようお願いしたい。	御意見については、今後の施策の推進に当たって参考とさせていただくべく、所管省庁にも伝達させていただきます。
97	4. 1. 1 経営層の意識改革	サイバーセキュリティ2021（2020年度年次報告・2021年度年次計画）（案）」のうちの2021年度年次計画（案）に係る意見	取締役会の実効性評価や、企業がDXの取り組みを推進する上でのサイバーセキュリティの重要性の周知を含め、サイバーセキュリティ経営の普及・実践の促進を期待したい。	賛同意見として承りました。
98	4. 1. 2 地域・中小企業におけるDX with Cybersecurityの推進	サイバーセキュリティ2021（2020年度年次報告・2021年度年次計画）（案）」のうちの2021年度年次計画（案）に係る意見	クラウドサービス事業者に対する方策検討のみではなく、利用者やSIパートナー側もクラウドサービスの「責任共有モデル」を十分理解するとともに、クラウドサービス事業者が発信する情報の理解促進や技術的スキル向上を促すよう、国からアドバイスをお願いしたい。	次期サイバーセキュリティ戦略（案）4.(2)①において、「あらゆる組織が、サイバー空間を提供・構成する主体として、自らが遂行すべき業務や製品・サービスからエンドユーザに至るサプライチェーン全体の信頼確保を『任務』と捉えること」を「任務保証」として求めております。 また、ご指摘のとおりクラウドサービス利用者の理解も重要であると考えており、サイバーセキュリティ2021の1.2(ケ)において、「クラウドサービス利用者やクラウドサービス事業者における、クラウドサービス利用時の設定ミスの防止・軽減に資するための方策を検討する」こととしています。御意見についてはこうした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。

「次期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

No	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
99	4．1．2　地域・中小企業におけるDX with Cybersecurityの推進	サイバーセキュリティ2021（2020年度年次報告・2021年度年次計画）（案）」のうちの2021年度年次計画（案）に係る意見	「別添1 2021 年度のサイバーセキュリティ関連施策 1.2 地域・中小企業における DX with Cybersecurity の推進」について ※御意見はNo.98と同意	No.98参照
100	4．1．2　地域・中小企業におけるDX with Cybersecurityの推進	サイバーセキュリティ2021（2020年度年次報告・2021年度年次計画）（案）」のうちの2021年度年次計画（案）に係る意見	「別添1 2021 年度のサイバーセキュリティ関連施策 1.2 地域・中小企業における DX with Cybersecurity の推進　（ケ）総務省施策」について ※御意見はNo.98と同意	No.98参照
101	4．1．4　誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着	サイバーセキュリティ2021（2020年度年次報告・2021年度年次計画）（案）」のうちの2021年度年次計画（案）に係る意見	「2.2.1.4 誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着」について No.98の意見に加え、クラウドに限らず、システム導入後は、設備投資だけでなく、社員やシステム運用者への教育に対する投資も必要であることを記載してほしい。	No.98参照
102	4．1．2　地域・中小企業におけるDX with Cybersecurityの推進	サイバーセキュリティ2021（2020年度年次報告・2021年度年次計画）（案）」のうちの2021年度年次計画（案）に係る意見	クラウドサービス利用時の設定ミス等による事故防止・軽減に資するための方策の検討について、政府が利用するクラウドサービスに対するペネトレーションテストの義務化や利用方法の普及促進に向けた一層の働きかけが必要と考える。	ご指摘のとおりクラウドサービス利用者の理解は重要であると考えており、サイバーセキュリティ2021の1.2(ケ)において、「クラウドサービス利用者やクラウドサービス事業者における、クラウドサービス利用時の設定ミスの防止・軽減に資するための方策を検討する」こととしています。なお、内閣官房においては、国の行政機関の情報システムにおけるセキュリティ対策の点検・改善を行うためのペネトレーションテストを通じて、クラウド利用型のシステムを含めて引き続き問題点の改善に向けた助言等を行うこととしています。御意見についてはこうした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。
103	4．1．2　地域・中小企業におけるDX with Cybersecurityの推進	サイバーセキュリティ2021（2020年度年次報告・2021年度年次計画）（案）」のうちの2021年度年次計画（案）に係る意見	サイバーセキュリティ対策に対する意識啓発や情報セキュリティへの投資、民間のお助け隊サービスの普及支援の推進について、中小企業に加え、（サプライチェーンの一部である）大企業も共助として取り組む形の施策の推進をお願いしたい。	昨年、産業界が一体となってサプライチェーン全体で~~の~~サイバーセキュリティ対策を推進することを目的として立ち上げられた「サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）」において、大企業も含む様々な業界・経済団体会員として加わっており、サイバーセキュリティ2021の1.2(エ)において、「SC3等の活動を通じて、中小企業のサイバーセキュリティ対策に対策に対する意識啓発を推進」することとしており、サイバーセキュリティお助け隊サービスの利用推奨を行うなどの取組を進めてまいります。御意見についてはこうした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。

「次期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

No	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
104	4．1．3　新たな価値創出を支えるサプライチェーン等の信頼性確保に向けた基盤づくり	サイバーセキュリティ2021（2020年度年次報告・2021年度年次計画）（案）」のうちの2021年度年次計画（案）に係る意見	トラスト基盤整備等の普及促進の検討について、特に中小企業等に向けては、財務省とも連携し、税制優遇措置等の検討や、普及啓発に向けた新たな枠組み等の検討が必要と考える。	ご指摘のとおりトラストサービスの基盤等の中小企業等への普及促進の観点は非常に重要であると考えております。今後の政策の検討に向けて、ご意見として承ります。
105	4．2　国民が安全で安心して暮らせるデジタル社会の実現	サイバーセキュリティ2021（2020年度年次報告・2021年度年次計画）（案）」のうちの2021年度年次計画（案）に係る意見	対策を進めるにあたっては、セキュリティのみではなく、リスク評価に基づいたセーフティの観点も踏まえて検討する必要がある。その中で、特に緊急性を要するインシデントが発生した場合は、関係箇所との迅速な合意形成及び執行のプロセスが必要である。	サイバーセキュリティ2021の2.2.1国民・社会を守るためのサイバーセキュリティ環境の提供において、「国は、深刻なサイバー攻撃に対して、オールジャパンで力を合わせて、適宜適切な情報把握・分析から事案対処までに至るインシデント対応及びその後の再発防止や改善に向けたルール作り等の政策措置の展開を一体的に推進する包括的なサイバー防御策について、関係主体との連携も図りつつ、持ち得る全ての能力と手段を活用して展開する。そのために必要な、包括的なサイバー防御の総合的に調整を担うナショナルサート機能等の強化及び包括的なサイバー防御を着実に実施していくための環境整備について検討を推進する」とあるところ、フィジカル面での被害状況に応じた国としての対応とサイバー防御策を一体として検討しており、今後ともサイバーセキュリティとセーフティの観点も含めて取り組んで参ります。
106	4．2．1　国民・社会を守るためのサイバーセキュリティ環境の提供	サイバーセキュリティ2021（2020年度年次報告・2021年度年次計画）（案）」のうちの2021年度年次計画（案）に係る意見	「別添1 2021 年度のサイバーセキュリティ関連施策 2.1 安全・安心なサイバー空間の利用環境の構築」（以降の再掲施策も同様）について ※御意見はNo.58と同意	No.58参照
107	4．2．1　国民・社会を守るためのサイバーセキュリティ環境の提供	サイバーセキュリティ2021（2020年度年次報告・2021年度年次計画）（案）」のうちの2021年度年次計画（案）に係る意見	クラウドサービスのサイバーセキュリティのルール策定及びグローバルな連携にあたっては、IaaS提供事業者のみではなく、PaaSやSaaS提供事業者ともヒアリングを実施する等の確実な連携をお願いしたい。	クラウドサービスがサイバー空間において欠かせないインフラとなっていることを鑑み、利用者が安心してクラウドサービスに情報資産を委ねることができるように、御意見も参考に、国としてもサービス形態にかかわらず、社会全体における安心安全なクラウドサービス利用環境を構築すべく検討を進めて参ります。
108	4．2．1　国民・社会を守るためのサイバーセキュリティ環境の提供	サイバーセキュリティ2021（2020年度年次報告・2021年度年次計画）（案）」のうちの2021年度年次計画（案）に係る意見	なりすましメールへの対策として、特に中小企業等における送信ドメイン認証技術の更なる普及促進を図るため、経済産業省・財務省とも連携し、税制優遇措置や、サプライチェーントップからの積極的活用推奨等の検討をお願いしたい。	国としても送信ドメイン認証技術の普及は「なりすましメール」への技術的対策の一つとして重要だと認識しており、引き続き普及に向けた周知、広報を行って参ります。

「次期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

No	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
109	4．2．1　国民・社会を守るためのサイバーセキュリティ環境の提供	サイバーセキュリティ2021（2020年度年次報告・2021年度年次計画）（案）」のうちの2021年度年次計画（案）に係る意見	全行政機関（国・独立行政法人・国特別法人・地方公共団体系も含む）の使用するメールアドレスについて、全て送受信ともにTLSによる暗号化通信で保護されるようにすべきである。	政府機関においては、情報システムの開発・構築段階も含めたあらゆるフェーズで対策を強化することとしており、個々のシステムの特性・要求に応じて最適なセキュリティ対策の導入を引き続き進めて参ります。
110	4．2．3　経済社会基盤を支える各主体における取組①（政府機関等）	サイバーセキュリティ2021（2020年度年次報告・2021年度年次計画）（案）」のうちの2021年度年次計画（案）に係る意見	「別添1 2021 年度のサイバーセキュリティ関連施策 2.3 経済社会基盤を支える各主体における取組①（政府機関等）（シ）内閣官房施策」について ※御意見はNo.59と同意	いただいた御意見については、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。
111	4．3．3　国際協力・連携	サイバーセキュリティ2021（2020年度年次報告・2021年度年次計画）（案）」のうちの2021年度年次計画（案）に係る意見	サイバー攻撃の起点はアジア太平洋地域やアフリカ等の地域に限定されず、その他欧州、北米、南米等の様々な地域になっている状況を踏まえ、TSUBAMEセンサーの効率的な運用も含め、対象地域の拡大を期待したい。 また、攻撃起点のうち、サイバー後進国のインフラ自体が攻撃のインフラとなり、各国のCSIRT関連機関と情報連携やインシデント対応調整がより一層求められていると考えられ、今後もより一層JPCERT/CCの取り組みをより深化させ、日本の国益に沿う調整期間としての役割を期待したい。	ご指摘の点はご意見をいただいております3.3(2)(ウ)において、「JPCERT/CCと各参加国関係機関等との間での共同解析やマルウェア解析連携との連動等の取組を進める。」「アジア太平洋地域以外への観測点の拡大を進める」こととしております。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参考とさせていただきます。
112	4．4　横断的施策	サイバーセキュリティ2021（2020年度年次報告・2021年度年次計画）（案）」のうちの2021年度年次計画（案）に係る意見	情報共有体制に関する考え方は、粒度は異なれど次期戦略本文や2021年度年次計画の至る所に散見されるため、横断的施策の一つとして新たに加えるべきである。	分野や主体等の特性に応じた情報共有体制も重要であることから、分けて記載させていただいております。 ご指摘のとおり、情報共有にあたっては、分野横断的に集約・分析し、関係主体と共有する仕組み等による官民・分野横断的な情報共有体制の強化が必要と考えており、国全体としての情報共有体制としては、サイバーセキュリティ2021の2.2.1国民・社会を守るためのサイバーセキュリティ環境の提供において示しているとおり、国は、深刻なサイバー攻撃に対して、オールジャパンで力を合わせて、適宜適切な情報把握・分析から事案対処までに至るインシデント対応及びその後の再発防止や改善に向けたルール作り等の政策措置の展開を一体的に推進する包括的なサイバー防御策について、関係主体との連携も図りつつ、持ち得る全ての能力と手段を活用して展開し、そのために必要な、包括的なサイバー防御の総合的に調整を担うナショナルサート機能等の強化及び包括的なサイバー防御を着実に実施していくための環境整備について検討を推進してまいります。

「次期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

No	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
113	-	サイバーセキュリティ2021（2020年度年次報告・2021年度年次計画）（案）」のうちの2021年度年次計画（案）に係る意見	デジタル庁発足後、デジタル庁はどのセキュリティ施策で関わっていくのか決まっていれば記載をお願いしたい。	現在情報通信技術（IT）総合戦略室が取り組んでいる施策につきましては、引き続きデジタル庁が取り組むこととなります。例えば、2.2(ア)「国、地方公共団体、準公共部門等の情報システムの整備や管理について、サイバーセキュリティを含む基本方針の策定及びその実装の推進」や、2.3(ツ)「常時診断・対応型のセキュリティアーキテクチャの実装に向けた、収集すべきデータ項目や分析方法等に関する実証研究の実施」が該当します。
無関係、その他				
114	-	無関係、その他	日本システムアドミニストレータ連絡会の紹介。	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。
115	-	無関係、その他	日本のセキュリティソフト「AppGuard（アップガード）」の採用をお願いしたい。	戦略案4.2.3の記載の通り、政府機関においては、情報システムの開発・構築段階も含めたあらゆるフェーズで対策を強化するとともに、例えば、従来の「境界型セキュリティ」にとどまらない、常時診断・対応型のセキュリティアーキテクチャの実装に向けた技術検討等、個々のシステムの特性・要求に応じて最適なセキュリティ対策の導入を引き続き進めて参ります。