資料２

サイバーセキュリティ戦略（案）に関するパブリックコメントの主な結果一覧

意見のうち、パブリックコメントの対象となる案件についての意見のみ、意見の概要とこれらに対する考え方を掲載しています。

取りまとめの都合上、お寄せいただいた意見は適宜要約しております。

	意見の概要	意見に対する考え方（案）
	サイバーセキュリティ戦略全体に係る意見	
1	本戦略案が示す、巧妙化・深刻化するサイバー脅威への対応強化という方向性には全面的に賛同する。 　しかしながら、国際的な潮流を踏まえれば、我が国においても、目先の脅威への対処と並行して、デジタルインフラに対する国家としての主権を確立することが不可欠であると強く認識すべきである。 　この認識に基づき、以下の３つの方針を国家の基本原則として本戦略に明確に位置づけ、あらゆる施策の基盤とするべき。 １．統制可能性の確保 政府や重要インフラが扱う国民・企業の重要データは、日本の法制度と国家の意思決定の下で実質的に保護・管理されるべき。 ２．検証可能性の確保 デジタルインフラの信頼性は、提供事業者の自己申告に依存するのではなく、我が国が主体となって客観的に「検証」できる体制によって担保されるべき。クラウドサービス等が契約・法令・我が国のセキュリティ要件を遵守しているかを、ブラックボックス化させることなく継続的に確認できる仕組みを戦略の柱とすべき。 ３．戦略的選択肢の確保 特定の国や企業のプラットフォームへの過度な依存は、技術的・経済的なロックインを招き、将来的な国家の交渉力やレジリエンスを著しく低下させる。当面は海外の優れたサービスを活用しつつも、国産技術やオープン技術を基盤とした多様な選択肢を戦略的に育成・確保し、将来的にはそれらへの段階的な置き換えを目指すことを、国家安全保障の一環として明確に位置づけるべき。	ご意見として承ります。 　なお、我が国のサイバーセキュリティ分野における自律性確保に関しては、Ⅲ．３．「我が国のサイバー対応能力を支える人材・技術に係るエコシステム形成」において、「我が国は、デジタル技術・産業そのものも相当程度海外に依存しており、サイバーセキュリティ分野も同様である。安全保障の観点からも、我が国に基盤を持つ形での国内産業の育成や、技術力・開発力の向上等を通じた自律性の確保が求められる。」と述べた上で、海外の技術やサービスに過度に依存することなく、国産技術・サービスを核とした、技術、人材を育成する好循環のエコシステムの形成に向けた取組を進めることとしています。
2	戦略の中に「地域の生活基盤に根ざしたサイバーセキュリティ対策」や「一次産業者向けの支援制度・教育プログラムの整備」を明記し、地方の実情に即した施策を推進すべき。	ご意見として承ります。 　なお、Ⅲ．２．（２）②「地方公共団体におけるサイバーセキュリティ対策の強化」において、地方公共団体におけるサイバーセキュリティ対策の強化に関して、デジタル人材の確保・育成に対する支援に関して述べているほか、Ⅲ．２．（３）③「中小企業を始めとした個々の民間企業等における対策の強化」において、中小企業を始めとした個々の民間企業等における対策の強化に関して、地域金融機関、士業といった地域に根付いた主体との連携等の促進、中小企業等を含むサプライチェーン全体のサイバーセキュリティ強化を目的として設立された産業界主導のコンソーシアムを通じた普及展開活動の強化等に取り組む旨、記載しています。

3	官民連携や国際協調は重要だが、地域・中小事業者の視点が反映される仕組みが必要である。 　特に以下の点を重視すべき。 ・地域密着型業種への演習・支援体制の整備 ・脅威ハンティングにおける倫理的ガイドラインと文化的配慮 ・国際連携における地域の声の反映と価値観の共有 日本のサイバーセキュリティの「ブランド化」においても、「倫理性」「地域との共生」を前面に出すことが信頼形成につながる。	ご意見として承ります。
4	政府や国の機関に働く者が海外産のSNS等を使っている時点でセキュリティーは成り立たたず意識が弱すぎる。 早急な国産のそれらの開発普及と共に意識面でも徹底していくべき。	政府機関による情報発信等のためのSNS利用に際してのセキュリティ確保に関しては、政府統一基準において、その適正性の確保が図られているところです。
5	携帯基地局等通信インフラの中国製機器の排除を。バッテリーや整流器など、遠隔操作により停止できるつくりの様である。目立たない様攻撃をするとすれば、一番狙われやすいところ、各社へ確認をしてもらいたい。	ご意見として承ります。 なお、一般論として、重要インフラ事業者かつ基幹インフラ事業者でもある通信事業者は、関係法令等に基づく基準等を踏まえ、各事業者において必要なセキュリティ対策を講じることとなります。
6	サイバーセキュリティ戦略案の策定自体は、サイバー脅威の深刻化に対応する重要な一歩と評価する。私は賛成、反対の立場を明確に取らず、日常的に直面するインターネットウイルス、マルウェア、ランサムウェアなどの被害を減らすための具体的な対策を、政府・企業・個人レベルで徹底的に進めてほしいと願っている。	ご意見として承ります。サイバー空間に参画する各主体が、その主体自身の能力や社会に及ぼすリスクを踏まえ、適切な対策を講じられるよう、施策を推進してまいります。
7	システム開発における品質には法的なルールや規則がないに等しいため、日本で稼働している多くのWebサービスには、非常に多くの脆弱性が潜んでいると考えられる。 　明らかにシステムに欠陥があると判明しても罰則や指摘がないので、欠陥を抱えたままビジネスを展開することが可能になっている。 　そのため、絶対に満たすべき品質・セキュリティ要件を国が法で定めてくれれば、必然的に、サイバー攻撃に強いシステム・企業・日本が形作られていくと思う。 　一方で、能動的サイバー防御における攻撃者のサーバを無害化する件に関して、技術的にも法的（海外の）にも実現が可能なのか懸念している。ほぼ不可能ではないかと思われる。 　サイバー攻撃（脅威）も多種多様なため、すべてを守り切るのは不可能、もしくは非効率ではないか。 　様々な脅威から何を守護するのか、事前に定めている状態を目指してもらいたい。	政府機関等においては、政府統一基準に基づき必要な対策を行うこととされているほか、重要インフラ事業者等に対しては、各所管省庁の関係法令等に加え、新たなサイバーセキュリティ基本法に基づく「重要インフラ統一基準」に基づき、セキュリティ水準の引上げを図ることとされています。 　また、ベンダー、中小企業等を含めたサプライチェーン全体に関しては、リスク、能力、業態等も多様であるため、総合的なアプローチをとることとしています。 　アクセス・無害化措置については、サイバー対処能力強化法及び同整備法（2025年5月に国会で成立）に基づき実施するものです。そのための体制を早期に確立し、能力強化を図っていくこととしております。
8	「レジリエンスの向上」をより具体的に実行に移せるよう、以下のような具体的なアクションを加えてはどうか。 ・BCP/DR計画策定の徹底を重要インフラや政府機関等に推奨する ・復旧演習を定期的に行うことの重要性を戦略に盛り込む ・バックアップの高度化を図るため、ネットワークから隔離された「イミュータブル（変更不能）バックアップ」の導入などを推奨する	ご意見として承ります。 　本戦略案では、Ⅲ．２．(１)③「強靱な政府情報システムの構築と運用」において、政府機関等におけるインシデント発生時の早期復旧の確保等について述べているところです。また、現在の政府統一基準において、情報システムの運用継続計画の整備等に関して記述しているところです。 　その対策の在り方は組織・システム等によって様々なものが想定され、戦略において個別詳細に記述することは難しいと考えておりますが、社会全体のレジリエンスの向上に当たっては、個別組織の役割や被害を受けた際の影響の大きさ等を踏まえ、被害を受けた際の対応体制の整備や必要な準備をすることも重要であると考えられます。ご意見の観点も踏まえ必要な取組を進めてまいります。

9	情報資産を集積するストレージや機器に対する攻撃はサイバーセキュリティではないようにもみえるが、物理的な損失が電子情報の完全性に影響を及ぼすこともあることから、ディザスタリカバリのような冗長性やバックアップも、サイバーセキュリティの一要素として触れてもよいのではないか。 　地方自治体においては、自身の自治体だけでは物理的な制約が大きい。このため、複数の地方自治体をコーディネートし、相互に冗長性確保、バックアップをするといったことも将来必要になると考えられる。こういった活動の根拠としても、「物理的なセキュリティ」に触れても良いのではないかと考える。	ご意見として承ります。 　なお、「政府機関等の対策基準策定のためのガイドライン（令和７年版）」3.1.1(8)-2 において、「要保全情報若しくは要安定情報である電磁的記録のバックアップ又は重要な設計書のバックアップについて、災害や情報セキュリティインシデント等の危機的事象により生ずる業務上の支障を考慮し、適切な保管場所を選定すること。要保全情報又は要安定情報である電磁的記録のバックアップについて、危機的事象として情報システムや情報が破壊される情報セキュリティインシデントを想定する場合は、必要に応じて、（略）情報システムや情報とバックアップが同時に破壊されない保管場所を選定すること」としており、政府機関等のサイバーセキュリティ対策の基準を示す政府統一基準群において、こうした規定が既に整備されています。 　また、地方公共団体においても、クラウドサービスやデータセンターの利用により、遠隔地におけるバックアップを確保することは可能であると考えられます。
10	公共調達におけるセキュリティ製品・サービスの選定基準を、価格競争から、実際のセキュリティ効果と革新性を重視した評価体系へ移行すべき。	ご意見として承ります。 　なお、一般に、政府調達に当たっては、仕様等に必要なセキュリティ要件や求める機能等を記載したり、調達にあたって総合評価方式を採用すること等により、価格以外の要素を加味した調達は可能であると承知しています。
11	国家サイバー統括室が、どのようなインシデントに対してどのような法的根拠等により、どの程度関わることになるのか、被害組織や現場対応にあたる専門組織の負担軽減と効果的な官民間の情報共有のために何らかの形で基準等を作成し、公に示すべき。	効果的な官民間の情報共有等に向けて、いただいたご意見は今後の施策の参考とさせていただきます。
12	JPCERT/CCについては「民間団体」「専門機関」の表記があるが、JPCERT/CCを戦略上、どのような組織として位置付けているのか整理・明記いただきたい。 　このほか、各機関や活動を示す用語については、「サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会」にて事務局（警察庁、総務省、経済産業省、サイバーセキュリティ協議会事務局(NISC、JPCERT/CC)）でも検討されており、既に整理された成果物等と平仄をあわせるなど、適宜整理いただきたい。	ご指摘のあった、Ⅲ.1.(1)①「インシデント対処の高度化による被害の拡大・深刻化の防止」やⅢ.1.(2)①「官民間の双方向・能動的な情報共有と対策強化のサイクルの確立」においては、より専門的な分析等の専門機関としての役割を期待する文脈で「専門機関」と記載しています。一方、Ⅲ.1.(1)④では、幅広い民間団体・事業者等の組織が連携していく文脈であることを踏まえ「民間団体」としています。 　他にも、本戦略では、Ⅲ.2.(4)「全員参加によるサイバーセキュリティの向上」において「従前より、国、地方公共団体、民間団体を含めた様々なレベルの組織が普及啓発に取り組んできているが、各種の普及啓発が行き届きにくいことに留意しつつ･･･」と記述しており、この「民間団体」は、サイバーセキュリティに係る普及啓発に取り組む民間団体を幅広く念頭においていますが、Ⅲ.1.(1)①やⅢ.1.(2)①で述べられる「専門機関」も含まれ得るものです。 　仮に本戦略において（専門機関を含み得る）「民間団体」という字句を、全て「専門機関、（専門機関以外の）民間団体」と書き換えるのは、文章が煩瑣となりますので、ここでは原案の記述とさせていただきます。
13	本戦略（案）は、国家を背景とした高度なサイバー攻撃や社会全体のデジタル依存深化に伴うリスクを的確に整理しているが、同時に国家・社会に深刻な障害をもたらすEMP（電磁パルス）、高出力マイクロ波（HPM）、太陽フレア（GMD）等の電磁的広域障害リスクが十分に扱われていない。これらは、サイバー空間そのものの機能を停止させ得る「物理的サイバー攻撃」であり、サイバー防御能力を根本から低下させる点からも、戦略の中に正式に位置づける必要がある。	ご意見として承ります。

14	人材基盤の構築、産学官連携の強化、高度な技術への対応に重点を置くことは、長年の労働力問題を解決し、日本の国際競争力を強化するための重要な一歩である。これらのイニシアティブを強く支持する。 　同時に、戦略の影響をさらに高めるには、日本の取り組みを国際的に認められた枠組みや資格とより明確に連携させることが重要であると考える。 　具体的には、日本のサイバーセキュリティ人材基盤を開発する際に、NIST NICEフレームワークなど広く採用されている国際モデルに対応付けし、日本の役割定義、スキルレベル、国際分類との対応関係を明確に公表することをお勧めする。また、CISA、CISM、CRISC、CGEIT、CDPSEといった国際的に認められた認証を枠組み内の関連役割と能力レベルに結びつけることで、実務者にとってのスキルの可視化が明確になり、より構造的なキャリアパスが支援される。	賛同意見として承りました。 　後段の海外の枠組みとの連携・対応関係の明確化については、今後の施策の参考とさせていただきます。
15	本案は、他国の脅威に対して、日本がサイバー領域における攻撃主体となることを宣言するものとなっている。 　政府はサイバーによる被害を無くすことにこそ努力すべきである。 本案でも繰り返し言及されている自由、公正かつ安全なサイバー空間は、東アジアにおいて敵対しあうのではなく、平和的な関係の中に維持されるべきである。 　サイバー領域において、人々が国境を越えた自由なコミュニケーションを実践できるような基盤を構築することや民主主義の基盤をなす検閲されずに自由に自らの思想・信条を伝えることを保障すること、通信の秘密をグローバルに保障することである。軍事的緊張をなくしていくことを目指し、軍事に依存しない外交や国際関係を構築し、国家や国家を後ろ盾とするサイバー攻撃の動機を失なわせることであり、これこそが政府がまず第一に取り組むべきサイバーセキュリティの戦略的な課題である。 　本案は、攻撃のリスクを軽減する最も本質的で基本的な国家の責任に背を向けるものであって、到底受け入れがたい。	アクセス・無害化措置や通信情報の利用は、サイバー対処能力強化法等（2025年5月に国会で成立）に基づき、実施するものです。その立法に際しても、過去の関連する経緯等を十分に精査した上、通信の秘密に十分に配慮を行うものとなっており、今般、国会においてご審議をいただいて成立しております。なお、通信情報の利用やアクセス・無害化措置については、独立機関として設置されるサイバー通信情報監理委員会における事前承認や検査等を始めとする、これら関係法の仕組み等によって適正な執行が図られることとなります。また、アクセス・無害化措置は、国際法上許容される範囲内で実施するものであり、こうした点も、本戦略で述べているところです。 　また、サイバー分野における同盟国・同志国等との効果的な国際連携及び国際協調は極めて重要であることから、特に、アクセス・無害化措置やパブリック・アトリビューション等、能動的な防御・抑止に係る各種措置の検討、実施に際しては、同盟国・同志国等と必要な情報を共有し、共同して対応を図るなど適切に連携するとともに、国際的な枠組み・ルール形成等のための多国間の議論にも積極的に貢献することとしています。
16	・本案は、国家あるいは国家を後ろ盾とする国外の国・地域に起点をもつサイバー攻撃を主要な脅威と位置づけた上で、サイバーセキュリティの国家戦略を策定しようというものと理解するが、それを解決するための外交的な取り組みの位置付けがほとんどない。 ・政府がサイバー空間においてなすべき第一の責務は、サイバー領域において、人々が国境を越えた自由なコミュニケーションを実践できるような基盤を構築することや民主主義の基盤をなす検閲されずに自由に自らの思想・信条を伝えることを保障すること、通信の秘密をグローバルに保障することであるが、本案は、このような責任を回避するものであって、到底受け入れがたい。	アクセス・無害化措置は、サイバー対処能力強化法等（2025年5月に国会で成立）に基づき、実施するものです。その立法に際しても、過去の関連する経緯等を十分に精査した上、今般、国会においてご審議をいただいて成立しております。なお、アクセス・無害化措置については、独立機関として設置されるサイバー通信情報監理委員会における事前承認や検査等を始めとする、これら関係法の仕組み等によって適正な執行が図られることとなります。さらに、アクセス・無害化措置は、国際法上許容される範囲内で実施するものであり、こうした点も、本戦略で述べているところです。 　また、サイバー分野における同盟国・同志国等との効果的な国際連携及び国際協調は極めて重要であることから、特に、アクセス・無害化措置やパブリック・アトリビューション等、能動的な防御・抑止に係る各種措置の検討、実施に際しては、同盟国・同志国等と必要な情報を共有し、共同して対応を図るなど適切に連携するとともに、国際的な枠組み・ルール形成等のための多国間の議論にも積極的に貢献することとしています。

17	・本案は、日本もまた攻撃者となることを通じて、優位にたつことを意図している。本案は日本の攻撃手法について一切沈黙しているが、これは問題であり、明らかにすべきである。 ・攻撃が実害となってしまうケースの多くは、適切なセキュリティの設定・管理がなされていなかったなどによるものである。これらは、私たち市民一人ひとりの場合も、企業や団体の場合も、対処可能な対策であり、政府が国家安全保障や、ましてや軍事的な政策の一環として軽々に位置付けるべきものではない。 ・日本のサイバー攻撃はサイバー攻撃の応酬という事態を招く。日本のサイバー攻撃は相手による反撃の動機を刺激し、攻撃の応酬から実空間における軍事的な緊張へと、戦争を誘引するきっかけになりかねない ・本案には通信の秘密やプライバシー・個人情報の権利についてはほとんど実質的な言及も関心ももたれていない。 ・本案は、憲法9条や国際法に反して、日本のサイバー攻撃をもっぱら加速化させ、 人々のサイバー・セキュリティをより一層脆弱にするものと言わざるをえず、反対である。	アクセス・無害化措置は、サイバー対処能力強化法等（2025年5月に国会で成立）に基づき、実施するものです。その立法に際しても、過去の関連する経緯等を十分に精査した上、今般、国会においてご審議をいただいて成立しております。なお、アクセス・無害化措置については、独立機関として設置されるサイバー通信情報監理委員会における事前承認や検査等を始めとする、これら関係法の仕組み等によって適正な執行が図られることとなります。さらに、アクセス・無害化措置は、国際法上許容される範囲内で実施するものであり、こうした点も、本戦略で述べているところです。 　また、サイバー分野における同盟国・同志国等との効果的な国際連携及び国際協調は極めて重要であることから、特に、アクセス・無害化措置やパブリック・アトリビューション等、能動的な防御・抑止に係る各種措置の検討、実施に際しては、同盟国・同志国等と必要な情報を共有し、共同して対応を図るなど適切に連携するとともに、国際的な枠組み・ルール形成等のための多国間の議論にも積極的に貢献することとしています。
18	今回取りまとめていただいた、サイバーセキュリティ戦略について、賛同する。 　今後、本戦略を踏まえた具体的な施策を有意義・有効なものとしていくことが重要と考えており、これらの施策の実施にあたっては政府機関が主導し、牽引いただくことを期待する。	賛同意見として承りました。
19	本案のI.に関係して、我が国に対するサイバー空間上における影響工作（インフォメーション・オペレーション）をサイバー攻撃の一つとしてとらえ、デジタルプラットフォーム事業者への対応義務を含めた、総合的な対策を政府として検討すべき。	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。
20	サイバーセキュリティ政策における主要課題――特に人材育成、組織能力の強化、産学官連携の促進といったテーマは、長く議論され続けており、依然として克服すべき課題として残っているように見受けられる。この点は、行政が取り組んでこられた努力の不足を意味するものではなく、むしろ“本質的で構造的な課題であるがゆえに、繰り返し取り上げられる”という性質によるものと理解している。 　そのため、今回の戦略においても、過去の施策がどの部分で一定の成果を挙げ、どの部分が構造的な課題として残り続けているのかが、もう少し示されると、戦略の必要性や重点領域の明確化に大きく寄与するものと考える。 　特に、「なぜこれらの課題が依然として解消しきれていないのか」について、制度面・人材市場・産業構造・技術変化といった複合的な視点から整理されると、現実的な道筋がより描きやすくなると感じる。	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。 　ご指摘の通り、本戦略が掲げる事項は、これまでのサイバーセキュリティ戦略においても課題として取り上げ、その都度、解決に取り組んでまいりましたが、依然として解消できていないものが存在します。 　今後、本戦略を踏まえた年次計画・年次報告等においても分析と評価を行うこと等を検討して参ります。
21	本戦略案では、民間の重要インフラ事業者へのサイバーセキュリティ強化策の推進が主に示されているが、政府機関自身も重要インフラの一部であることを明記し、まず政府機関が率先して政府システムの調達投資・強化を行い、その成果を民間重要インフラ事業者へ製品開発事業者やSI事業者を通じて普及させる仕組みを盛り込むべき。	ご意見として承ります。なお、本戦略Ⅲ．２．（２）「重要インフラ事業者・地方公共団体等におけるサイバーセキュリティ対策の強化」における「重要インフラ事業者」は、サイバーセキュリティ基本法における「重要社会基盤事業者」を指しておりますが、政府機関も「重要社会基盤事業者」に含まれています。ただし、政府機関等においては、本戦略案においては、個別に項立て（Ⅲ．２．（１））をして、そのサイバーセキュリティ対策の強化に関して述べています。
22	「自由、公正かつ安全なサイバー空間」を確保するため、日々新たに発案される攻撃手法に逐次対応する後手の防御ではなく、防御側が主体となって能動的な適応型のサイバーセキュリティ体制の構築をワン・ジャパンで目指す方針について賛同する。	賛同意見として承りました。また、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。

23	文章全体について。「ひいては」が多用されており、与えたいであろう印象を与えられてないのではないか。「ひいては」は一度使用すればそれ以降自明であると考えるが、多用されており、文章全体が間延びしている。 　また、殊更強調したい箇所で使用すべきかと思うが多用されていることから強調が薄まっている印象を受ける。 　そのため初出の箇所以外で使用するのは止めるべき。	本戦略では、サイバー攻撃が及ぼす国家安全保障への影響に関する言及において「ひいては」という用語を使用しています。この理由は、サイバー攻撃がまず国民生活や経済活動等に直接的な影響を与え、それが結果的に国家安全保障にも影響を及ぼす、という論理構成を明確にするためです。論理構成を明確にするため、このような用語を用いていることから、原案維持とさせていただきます。
24	大学等においては、学問の自由と自律性を尊重したセキュリティ文化の醸成が必要である。 中小企業には「信頼の循環」を軸とした共助圏の形成を支援すべきである。 個人への啓発では、感情に訴えるストーリーテリングや「顔の見える支援」が有効である。	ご意見として承りました。 　なお、大学等については、Ⅲ．２．（２）③「大学等におけるサイバーセキュリティ対策の強化」において「学問の自由の精神に基づき各構成主体の独立性が尊重される文化を持つため、組織全体としての画一的な情報セキュリティ対策を適用することに困難が伴う。」ことを踏まえ、「国は大学等による自律的な取組を支援するべく、サイバーセキュリティ対策や体制整備等に関する助言・情報共有、研修・訓練の実施、事案発生時の助言等の支援を行う。」と記載しております。 　また、中小企業等については、Ⅲ．２．（３）③「中小企業を始めとした個々の民間企業等における対策の強化」において「「自助」・「共助」・「公助」を組み合わせた施策を一層強化する必要がある。」と記載しております。

	意見の概要	意見に対する考え方（案）
	サイバー空間を巡る情勢認識に係る意見	
25	7頁15行目の段落に関して、20行目に「サイバー対応に必要な人材・技術を我が国で持続的に産み出していく環境形成が急務である。」とあるが、具体的な緊迫度合いを示せるよう具体的な起源を示す方が良い。	緊迫度合いについては、３．「我が国のサイバー対応能力を支える人材・技術に係るエコシステム形成」の冒頭で「我が国では、その人材の不足が長らく指摘されている。戦略的にサイバーセキュリティ人材を育成・確保しなければ、人材不足からサイバーセキュリティの確保が一層困難となる事態も懸念される。」ことや、「我が国は、デジタル技術・産業そのものも相当程度海外に依存しており、サイバーセキュリティ分野も同様である」旨の記載しています。 　その上で、人材・技術面の課題の「起源」は複合的な要因が長期的に影響した結果とも考えられ、具体的な記載はここでは行わないこととします。
26	4頁 35行目の「同国は有事に備え重要インフラ等の機能妨害・機能破壊も視野」について、有事は加害ではなく、被害と結びつく言葉であり、有事に備えるのは被害を被る側であり、加害する側が、有事に備えるという記述は、拝読していて違和感を覚えた。 　有事を見据え、狙って、対してなどの記載に変更するべき。	ご意見を踏まえ、「同国は有事**<u>を見据え</u>**、重要インフラ等の機能妨害・機能破壊も視野に入れたサイバー攻撃キャンペーンを行っている」と技術的な修正をすることといたします。

	意見の概要	意見に対する考え方（案）
	国が要となる防御・抑止と体制・基盤の整備に係る意見	
27	15頁1行目の1段落に関して、10行目の「高度な情報収集・分析能力を担う体制・基盤・人材等を総合的に整備する。」を、「高度な情報収集・分析能力を担う体制・基盤・人材等を、地位・待遇・スキルアップ等を含め総合的に整備する。」とする方が良い。すでに通信系企業等でセキュリティに関わる人材は多く存在しているが、「GAFA予備校」と呼ばれる問題で顕著であるように、高度人材は外資系企業へ流出している。現時点で我が国の企業に勤務する人材の地位・待遇改善措置をしない限りは我が国のセキュリティが改善することはない。	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。
28	・この戦略（案）が、昨今の緊迫する国際情勢や国内の脅威に対し、従来の枠組みから一歩進め、「国家安全保障政策」としてサイバーセキュリティを位置づけられた方向性は、非常に時宜を得たものだと考えている ・「防御」の考え方を一歩進め、「侵入はあり得る」という前提に立ち、ネットワークの「内部」を守る「ゼロトラスト・アーキテクチャ」の考え方をより分かりやすく明示することを提案する ・サーバー間や端末間の通信も適切に制御・監視する「マイクロセグメンテーション」のような対策を、重要インフラや政府機関のシステムにおいて推奨してはどうか ・「認証（アイデンティティ）」や「ネットワーク内部（横展開）」の監視・制御にも目を向けていく考え方を普及させるべき	ご意見として承ります。 　なお、ご指摘の、内部に侵入されていることを前提とした対策については、現在の政府統一基準において、内部に侵入した攻撃の早期検知・対処や、外部との不正通信の検知・対処等の対策（内部対策及び出口対策）、「ゼロトラストアーキテクチャ」の考え方に基づき実装する場合の対策等も記載しているほか、デジタル社会推進標準ガイドライン群においても、ゼロトラストアーキテクチャを適用するためのガイドラインを策定し公表しているところです。 　こうした政府統一基準群やデジタル社会推進標準ガイドライン等の継続的な見直し等を含め、政府機関等のセキュリティ対策水準の向上重要インフラ事業者等のセキュリティ対策の強化の必要性については、Ⅲ．２．「幅広い主体による社会全体のサイバーセキュリティ及びレジリエンスの向上」で述べているところです。ご意見の観点も踏まえ、引き続き、セキュリティ対策水準の向上を図ってまいります。
29	アクセス・無害化措置に関して、対象国の国内法や国際法に抵触する恐れがないかについての法解釈を明示すべきではないか。 　ただし、他国への抑止力のためにあえてグレーゾーンにするために明記しないのであれば、それは一考の余地がある。	アクセス・無害化措置は、サイバー対処能力強化法及び同整備法（2025年5月に国会で成立）に基づき、実施するものです。同整備法により改正された警察官職務執行法では、処置の対象たる電子計算機が国内に設置されていると認める相当な理由がない場合には、警察庁の警察官のみが処置をできることとし、あらかじめ、警察庁長官を通じて、外務大臣と協議しなければならないと規定されていることに加え、通信防護措置をとるべき旨を命ぜられ、警察と共同して当該通信防護措置を実施する自衛隊の部隊等は、警察官職務執行法を準用し、あらかじめ、防衛大臣を通じて、外務大臣と協議しなければならないと規定されており、国際法上許容される範囲内で実施することとなります。
30	能動的サイバー防御で官民連携や通信情報の収集を行い目的を実現することとしているが、サイバーセキュリティの研究に関する情報の収集も対象にすることを検討すべき。 　そのための窓口を設けることや、有益な情報を収集するためのバウンティ制度の設立も検討すべき。	Ⅲ．１．（１）①「インシデント対処の高度化による被害の拡大・深刻化の防止」で述べているとおり、国家サイバー統括室は、インシデントの迅速かつ的確な把握・分析・評価や被害防止に向けた情報発信等を行うこととしているほか、同②「通信情報を含むサイバーセキュリティ関連情報の集約、効果的な分析と活用」で述べているように、被害の防止に資する分析に有用なあらゆるサイバーセキュリティ関連情報を集約していくこととしています。したがって、一般論として言えば、サイバー攻撃の拡大防止に資する情報であれば、国家サイバー統括室における集約の対象となると考えられます。 バウンティ制度に関しては、ご意見として承ります。

31	サイバー脅威に対する抑止の一つとして、サンクション（制裁）についても言及すべきではないか。国内に対する根拠の提示だけでなく、外部に対する意思表示と抑止に効果があるのではないか。	本戦略のⅢ．１．（１）③「国際的なルール形成の推進」において、国際連合憲章を始めとする国際法は、サイバー空間において適用されること、及び、サイバー空間における国家による国際違法行為は当該国家の国家責任を伴い、被害国は、一定の場合には、当該責任を有する国家に対して均衡性のある対抗措置及びその他合法的な対応をとることが可能である旨、記載しています。また、Ⅲ．１．（１）①「同盟国・同志国等との情報・運用面での協力の強化」において、悪意あるサイバー活動の抑止に向けては、パブリック・アトリビューションの実施等とともに、外交面での対応を含め、同盟国・同志国等との間で緊密に連携して推進する旨言及しています。
32	攻撃アクターに関するインテリジェンスの収集を行うこととその有用性についても言及をすべきではないか。	Ⅲ．２．（１）②において記載しているように、サイバー攻撃への的確な対処のために、様々な形で収集された分析に有用なあらゆる情報を国家サイバー統括室に集約し、攻撃の検知や攻撃傾向の分析のみならず、攻撃側の意図や目的等についても分析を行うこととしております。
33	攻撃者に継続的にコストを負わせることに対する言及について、より明確に示してもよいのではないか。	平素から攻撃者側に継続的にコストを負わせることについては、我が国の総合的な防衛体制の強化に資するものであり、これを目指していくものとして、本戦略の複数の個所で言及しております。また、その手法としては、サイバー対処能力強化法等に基づく措置のみならず、あらゆる選択肢を、関係府省庁との緊密な連携を確保しつつ、国家サイバー統括室の総合調整の下で検討し、実施していくこととしています。
34	国際的な脅威情報共有の枠組みへの関与と、国内の新協議会の役割について、その方針を明確にすべき。 　具体的にはセキュリティ業界のCTA（Cyber Threat Alliance）のように、政府の影響からの独立性を重視する民間主導の枠組みが存在し、国が直接これらに加盟し、脅威の痕跡情報、標的型の攻撃キャンペーンや攻撃者などのコンテキスト情報を取得することは、その枠組みの性質上、制約が伴うと考えられる。 　このため、国際的な脅威情報については、欧米主要国等の同志国との連携を通じて情報共有を図りつつ、国内の官民情報共有においては、「新協議会」をNeed to Shareの中核的なプラットフォームとして明確に位置づけ、その機能強化を急ぐべきである。	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。
35	どのようなものを「大規模インシデント」と指定するのか、他の事案認定の枠組みとの整理を行いつつ、基準等を示すべき。	大規模インシデント時における関係機関等と連携した効果的な対処に向けて、いただいたご意見については今後の施策の参考とさせていただきます。
36	情報通信分析において、「潜在的被害の発見」とあるが、「把握」だけでなく、被害を認知できていない被害組織への通知や支援等に係る調整まで行うべき。	ご意見として承ります。 　なお、サイバー対処能力強化法においては、整理・分析した情報の関係組織への提供について規定されている（第16、38、40～42及び45条）ところ、政府としては、これに基づき、必要に応じた適切な情報共有を実施して参ります。
37	官民での情報共有に関して、「適切な情報の取扱いを確保」とあるが、今後、国側から民間側に情報を提供する場合における、機微情報のデグレードや官民間でどのように効果的に脅威情報を取り扱うかなど、官民間における脅威情報の取扱いに係るガイダンス整備等をすべき。	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。

38	アクセス・無害化措置などにより攻撃の影響を低減することが中心に記載されているが、これに加えて、「攻撃者を特定し、刑事捜査・逮捕・起訴にまでつなげること」を可能にする国際的な枠組みの整備方針も明記していただきたい。	国際的な連携の必要性については、Ⅲ．１．（３）「国際連携の推進・強化」及びⅢ．２．（５）「サイバー犯罪への対策を通じたサイバー空間の安全・安心の確保」に御指摘の内容も含まれているものと考えます。
39	能動的サイバー防御（アクセス・無害化措置等）の実施について、発動判断プロセスと運用手順をガイドラインとして明文化する方針を戦略に追記いただきたい。具体的には、1. 発動権限を持つ組織・役職、2. 発動判断の条件（被害規模・継続性・国家関与の蓋然性等）、3. 関係省庁・機関間の連携・承認フロー、4. 事後検証と説明責任のプロセスを整理し、戦略本部のもとで運用ガイドを策定することを提案する。	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。
40	本案のIII １．（１）②に関係して、能動的サイバー防御(ACD)の実行にあたって、政府は着実な情報保全がなされている形で平時から効率的に民間のITインフラに対する攻撃データ等の収集・活用を行うべき。	Ⅲ．１．（１）②「通信情報を含むサイバーセキュリティ関連情報の集約、効果的な分析と活用」で述べているとおり、サイバー対処能力強化法に基づく基幹インフラ事業者等によるインシデント報告を含む被害報告を含め、分析に有用なあらゆる情報を国家サイバー統括室に集約してまいります。
41	日本が戦略の第一の柱として、深刻化するサイバー脅威に対する防御・抑止を優先されていることを高く評価する。 　そのうえで、オンラインにおける国家活動に関する国際的なルール作りを支持する以上に、日本がパブリック・アトリビューションと抑止効果を通じて、これらのルールをどのように維持できるかに比重を置けば、戦略の強化につながるものと考える。戦略は、パブリック・アトリビューションの重要性と、実施に当たっての国際協力の必要性を正しく認識されているが、アトリビューションに含めるべき情報、特にサイバーインシデントによる国際ルール（規範または法律）の違反が発生したかどうかも強調すべき。さらに、ルールが確立され、悪意のあるサイバーインシデントによる違反が発生した時点で、将来のインシデントを抑止する上で意味のある結果が課されることも、戦略で明確にすべき。サイバー防御の改善と、サイバー空間における悪意のある主体の継続的な関与のみに重点的に取り組むだけでは、オンラインにおける敵対者の抑止には不十分であり、効果的なサイバー抑止には意味のある結果が必要である。	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。
42	今般のサイバーセキュリティ戦略案は、国家レベルでのサイバー脅威インテリジェンスプログラムの構築を指向するものであり、歓迎する。 　収集・分析した情報を民間企業に提供し、活用することに言及があるが、今後、収集・分析した情報をどのように活用するか（例えばインテリジェンス駆動型の脅威検知・監視、インシデントレスポンス、レッドチーミング（TLPT）、戦略立案）について、具体的な検討が必要である。	賛同意見として承りました。なお、提供された情報の民間企業等における活用の在り方は、一般的に、当該民間企業等においても必要な検討が行われることが期待されます。
43	アクセス・無害化措置や通信情報の分析・活用は、国家安全保障上の必要性は理解できるが、国民のプライバシーや表現の自由とのバランスが重要である。 　以下の原則を明記すべきである。 ・第三者的監視・評価制度の整備 ・国民への説明責任と対話の場の整備 ・情報共有原則の明文化（Need to Share / Need to Know） ・国際連携における倫理的基準の共有 ・地域・民間との信頼形成	通信情報の利用やアクセス・無害化措置導入を規定した「サイバー対処能力強化法」等において、通信情報の利用やアクセス・無害化措置については、独立機関である「サイバー通信情報監理委員会」が事前承認や検査等を行うこと（サイバー対処能力強化法第48条）となっており、同委員会は、その所掌事務の処理状況について、国会に報告するとともに、その概要を公表することになっております（同法第61条）。そのほか、これらの法において措置の適正確保のための所要の規律が定められていること等から、ご指摘の「整備」はすでになされているものと考えます。

	意見の概要	意見に対する考え方（案）
	官民連携エコシステムの形成及び横断的な対策の強化に係る意見	
44	・新たな官民連携の組織体は「give and take」の概念を念頭に、情報収集・提供、インシデント対応支援、リスクコミュニケーションなどの機能をもつ組織とするべき。また、定期的な会合やワークショップを開催し、参加企業間の情報や意見交換を促進するとともに、官民との人材交流を行い、信頼関係の構築を図るべき。 ・組織設置にあたっては、米国の共同サイバー防衛連携（JCDC）、英国のインダストリー100（i100）、豪州のサイバー脅威情報共有 (CTIS)など参考とするべき。	ご意見として承ります。サイバー対処能力強化法第45条第1項に基づく協議会については、Ⅲ．１．（２）①「官民間の双方向・能動的な情報共有と対策強化のサイクルの確立」で述べている内容を踏まえつつ、現在作成が進められている同法第３条第1項に基づく重要電子計算機に対する特定不正行為による被害の防止のための基本的な方針（基本方針）等も踏まえ、その具体的なあり方を検討してまいります。
45	・民間へ提供する情報（以下例示参照）は経営層の意識決定に有用な情報提供を実施するべき。 - 攻撃者の主体、目的、背景 - 攻撃の緊急度、重要度 - 攻撃の被害想定、波及効果 - 初期対応や中長期の対応 ・セキュリティ・クリアランス制度の適切な設計や運用を求めるとともに、情報提供においても十分に活用すべき。	賛同意見として承りました。Ⅲ．１．（２）①「官民間の双方向・能動的な情報共有と対策強化のサイクルの確立」で述べている通り、民間事業者への情報提供においては、構成員から汲み取ったニーズも踏まえ、国だからこそ取得できる情報を活用した分析を行い、この分析を踏まえた脅威情報等を構成員に積極的に提供してまいります。また、情報の機微性に鑑みて、必要に応じて、セキュリティ・クリアランス制度を活用した構成員への提供を行う予定です。
46	本年10月にDDoS攻撃・ランサムウェア報告様式の統一がされ、今後報告窓口の一元化をシステム整備も含めて検討されているが、運用面も含めて、リアル性や効率性も含めて早急に進めるべきである。	今後、システム整備を進め新法の報告義務施行（公布から１年６月後以内）に併せ実施予定です。
47	「新協議会」の設立に関して、サイバー脅威情報を機密度に応じて段階的に共有できる枠組みや、民間が参加しやすいガバナンス設計を希望する。また、対応を支援するサイバーセキュリティ企業も枠組みに入れることを検討いただきたい。	ご意見として承ります。なお、Ⅲ．１．（２）①「官民間の双方向・能動的な情報共有と対策強化のサイクルの確立」でも述べるとおり、特に機微度の高い脅威情報等については、必要に応じて、セキュリティ・クリアランス制度を活用して構成員へ提供することや、新協議会の構成員以外の者に対しても、秘密を含まない情報の提供を行う予定です。また、新協議会には、セキュリティベンダーに構成員として参加しいただくことを想定しております。
48	サイバーインシデント発生時・平時の情報共有時の「統一連絡窓口」（例：分野別CSIRT、ワンストップの相談窓口など）について、それぞれの窓口の担当範囲（相談内容／対象業種／緊急度など）を戦略の中で整理し、図表などで分かりやすく提示していただきたい。	ご意見として承ります。 現在、Ⅲ．１．（１）①「インシデント対処の高度化による被害の拡大・深刻化の防止」に記載しているように、「被害組織が対処活動に集中できるよう、国は、被害組織からのインシデント報告にかかる負担の軽減を目指し、サイバー対処能力強化法に基づく報告も含めた報告様式の一元化とともに、報告先の一元化に向けて所要の調整を進める。」状況にありますが、報告先の一元化が完了次第、その周知徹底に取り組んでまいります。
49	脅威ハンティングの取組対象を、「一般の民間企業」に対しても段階的に拡大していく方針を明記していただきたい。また、日本政府主導の脅威インテリジェンス・プラットフォームを構築する等、規模や業種を問わず多くの企業が脅威情報を閲覧・共有できるようにすることを検討していただきたい。	Ⅲ．１．（２）②「官民における脅威ハンティングの実施拡大」でも述べているとおり、脅威ハンティングが浸透していない我が国の現状に鑑み、脅威ハンティングの普及を促進する必要があると考えておりますが、特に、高度脅威アクターの標的となる政府機関、独立行政法人、サイバー安全保障を確保する上で重要な民間事業者等における脅威ハンティングの必要性が高いと考えております。また、脅威ハンティングの実施は組織間の情報等の共有がその有効性を高めるため、官民間の情報共有の推進が重要になると考えており、その点も留意しながら各種施策を講じていきたいと思います。
50	現状の記載では、演習の主な対象が政府機関や重要インフラ事業者に限定されている印象があるため、参加企業の業種・規模を問わず、インシデント対応能力の向上を図るための、段階別・レベル別の演習メニュー等を整備し、「官民・業種横断」で参加できる仕組みの構築を戦略に位置付けていただきたい。	ご意見として承ります。なお、例えば、国立研究開発法人情報通信研究機構（NICT）が実施する実践的サイバー防御演習「CYDER」は、主な受講対象を国の機関や地方公共団体、重要インフラ事業者等としつつも、一般の民間企業等からの受講も可能としております。

51	Ⅲ．１．（２）①「官民間の双方向・能動的な情報共有と対策強化のサイクルの確立」の「国家サイバー統括室の総合調整の下、内閣府が、平素及び事案発生時における脅威情報等の相互共有等を行う。」の個所について「国家サイバー統括室の総合調整の下、内閣府が、平素及び事案発生時における脅威情報等の相互共有等を行うと共に、サイバーセキュリティ対策に関係する多様な機器の構成部品の出所やそのサプライチェーンの情報を調査収集分析するため、新協議会による機器製造にかかわる事業者からのヒアリングを積極的に実施する。」との修正を提案する。	ご意見として承ります。
52	巧妙化・高度化するサイバー攻撃に対し、国全体として対処能力を高めるためには、官民連携の強化が不可欠である。 　重要インフラ事業者が被害防止のための対策を実施できるようにするため、政府機関にて整理・分析された情報、政府機関でしか知り得ない情報などを、それを必要とする重要インフラ事業者に対して、迅速に展開いただくことを期待する。	賛同意見として承りました。Ⅲ．１．（２）①「官民間の双方向・能動的な情報共有と対策強化のサイクルの確立」で述べている通り、民間事業者への情報提供においては、構成員から汲み取ったニーズも踏まえ、国だからこそ取得できる情報を活用した分析を行い、この分析を踏まえた脅威情報等を構成員に積極的に提供してまいります。
53	Ⅲ．１．（２）１およびⅢ．３.（2）に関係して、サイバー対処能力強化法及び同整備法における官民連携については、民から官へのインシデントの報告や官から民へのサイバーセキュリティ関連情報の提供等、官民における情報(データ)の流通が大きな柱の一つである。それら流通するデータは安全保障に関するデータであるため、国産事業者が中心となり我が国の司法管轄権の及ぶ範囲にデータが留まるような制度及び情報通信基盤の下で扱われなければならないと考える。 　我が国の国産事業者が中心となり、国内にデータがとどまる形でサイバー脅威情報の官民における活用サイクルができる制度を作るべき。 　加えて、官民における積極的な情報の流通がなされ、そのような情報を基にした政府におけるアクセス・無害化オペレーションの高度化のために、民間事業者がNCOをはじめとする政府機関への情報提供を行うインセンティブを感じるような制度設計が必須であると考える。	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。

	意見の概要	意見に対する考え方（案）
	国際連携の推進・強化に係る意見	
54	インド太平洋地域等への支援において、政府の能力構築支援（ODA等）と日本企業のビジネス展開支援を一体的に推進する「官民連携パッケージ」を更に具体化し、日本の国益と国際協調を両立させる取り組みを強化してほしい。	ご意見として承ります。 Ⅲ．１．（３）②「インド太平洋地域におけるサイバー安全保障分野の対応能力向上の支援・推進」に記載しているとおり、インド太平洋地域を始めとする諸外国への能力構築支援については、同盟国・同志国、国際機関、産学といった多様な主体と連携し、重層的かつオールジャパンで戦略的に進めてまいります。
55	NCOが被害組織や専門組織等から提供を受けた情報を同盟国・同志国等と共有する際の、同意取得や匿名性確保等の具体的な配慮事項や、運用指針が決まっているかご教示いただきたい。	お問合せの運用指針等について、政府の対応に関する詳細についてのお答えは差し控えさせていただきます。

	意見の概要	意見に対する考え方（案）
	政府機関等のサイバーセキュリティ対策強化に係る意見	
56	「サイバーセキュリティ基本法」第２６条に定める監査に関して、「指定法人」については、特別法で運用される認可法人も対象とすべきである。 特に、下記の法人については取り扱う情報の機密性、社会インフラとしての重要性、安全保障の観点から必須と考えられる。 ・日本銀行 ・預金保険機構 ・農水産業協同組合貯金保険機構 ・原子力損害賠償・廃炉等支援機構 ・電力広域的運営推進機関 ・使用済燃料再処理・廃炉推進機構	「サイバーセキュリティ基本法」第26条第１項第２号に基づく監査は、政府機関・独立行政法人・指定法人に対して行われるものであり、この「指定法人」は、サイバーセキュリティ基本法第13条に基づき、特殊法人・認可法人のうち当該法人においてサイバーセキュリティが確保されない場合に生ずる国民生活又は経済活動への影響を勘案して、当該法人におけるサイバーセキュリティの確保のために講ずる施策の一層の充実を図る必要がある法人としてサイバーセキュリティ戦略本部が指定しているものとなります。 　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。
57	ガバメントクラウド等のクラウド基盤を国民生活の最重要インフラと位置づけ、GSOC等による優先的な監視・防御対象であることを戦略本文に明記すべき。また、クラウド特有の脅威に対応するため、CSPM等の継続的な監視・評価の仕組みを整備し、調達要件において国産の運用自動化技術を積極的に評価・活用すべき。	ご意見として承ります。 　なお、ご指摘のようなクラウド基盤も含む、デジタル庁が整備・運用する国民に対するサービスの基盤システム、各府省庁が共通で利用するシステム等の重要な政府情報システムについて、Ⅲ．２．（１）③「強靱な政府情報システムの構築と運用」に記載のとおり、システムの強靭性確保とサイバーセキュリティ強化に取り組んでまいります。また、Ⅲ．２．（１）①イ「ISMAPの継続的な見直し」に記載のとおり、クラウドサービスの進展等を踏まえ、ISMAP制度の継続的な見直し等を実施してまいります。
58	既に多くの団体（業界団体、学会、標準化団体など）が様々なセキュリティ基準やガイドラインを公開しており、「どれを参照すべきか分かりにくい」という課題があるなか、政府主導で基準の統合・整理を進める方針を明記していただきたい。	ご意見として承ります。 　なお、一般に、サイバーセキュリティの動向は非常に早く、また業種・業態も様々であり、リスクも多様であることから、政府がすべての基準やガイドラインを統合・整理することは必ずしも適切ではないと考えられます。他方、必要に応じて、政府において策定すべきと考えられる分野等の基準やガイドライン等については、すでに一部整備を行っているものもあるところ、必要に応じて対応を検討してまいります。
59	現在記載されている、「政府統一基準群の継続的な見直し」および「重要インフラ統一基準」を新たに定める方針に賛同する。 　その際、過去に策定されている類似のガイドライン等を参考にし、さらに最新の状況に即した内容に更新した内容として記載することを望む。 　例えばIPAが策定した「重要情報を扱うシステムの要求策定ガイド」は、2024年以降更新されておらず、改定の時期になってきていると思われるが、このガイドでは「計算途上のデータ暗号化」について「特殊なハードウェアやソフトウェアに限定されるなど、現時点では課題があります」と記載されているが、実態は変化してきており、「計算途上のデータ暗号化」は引き続き重要な技術要件として位置づけられる可能性がある。	賛同意見として承りました。 　なお、いただいたご意見を踏まえ、Ⅲ．２．（２）「重要インフラ事業者・地方公共団体等におけるサイバーセキュリティ対策の強化」において、「重要インフラ統一基準の作成は、**現行制度や国際・技術・脅威の動向等を踏まえ、**2026年度に行う。」と一部追記することといたします。

60	クラウドサービスのセキュリティ評価制度 ISMAP について、単なる「継続的な見直し」に留めず、1. 審査・更新プロセスの迅速化と柔軟化、2. 最新クラウド技術への追随、3. FedRAMP 等海外制度との相互参照・相互承認の検討といった「俊敏性向上策」を戦略レベルで明示いただきたい。	ISMAP については、本戦略において「クラウドサービスの進展とともに、政府機関等によりクラウド上で取り扱われる情報は質・量共に多様化しているところ、これらの状況に適切に対応するため、国は、取り扱う情報により求めるセキュリティ水準の合理化を図る、最新のセキュリティ対策の柔軟な導入を可能とするなどの制度の見直しを実施する」と記載したうえで、クラウドサービスは日々進展していること等から、ISMAPの運用状況、海外の取組、国際規格の改定等を踏まえて、国は、制度の継続的な見直しを実施するとしているところです。
61	AI 活用による検知・分析の高度化について、SOAR と組み合わせた AI-SOAR の段階的導入計画と、MTTD／MTTR、自動化率、誤検知削減率等の KPI を戦略本文に明記いただきたい。例えば「〇年度までに主要府省庁の SOC で SOAR を本格稼働」「重大インシデントの MTTR を△%短縮」といった形で、具体的な成果指標を設定されることを提案する。	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。
62	サプライチェーン・リスクの一環として、セキュリティ製品・サービスのベンダー M&A リスク への備えを明示いただきたい。具体的には、1. 特定製品に依存しない「能力・性能要件ベース」の調達、2. 複数ベンダー併用や代替製品候補の事前検討、3. 主要セキュリティ製品についての乗り換え・終了時対応方針の整理等を、調達方針に組み込むことを提案する。	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。
63	Ⅲ．２．（１）①ウ 「政府機関等における機密性の高い情報の取扱いの検討」に関して、今後民間への情報・意見聴取を実施する際には、ガバメントクラウドを提供するIaaS事業者だけでなく業態等が大きく異なるSaaS事業者も重要なステークホルダーの一つとして情報・意見を提供できる機会をいただきたい。 Ⅲ．２．（１）①エ「政府機関等のIT調達等におけるサプライチェーン・リスクの軽減」に関して、政府機関等に採用いただいているクラウドサービス事業者も重要なステークホルダーの一つとして情報・意見を提供できる機会をいただけると幸い。	ご意見として承ります。
64	Ⅲ．２．（１）③「強靱な政府情報システムの構築と運用」に関して、非常に堅牢なサービスとしてISMSやSOC2等の国際規格を取得し、ISMAPに登録したクラウドサービスについても、強靭な政府情報システムの構築のためにご活用いただけることを期待する。	ご意見として承ります。
65	本案のⅢ. 2（１）１ やⅢ. 2.（2）に関係して、政府のITシステム調達契約について、システム構築時や運用受託契約中にサイバーセキュリティインシデントが発生した際は、受託事業者ではなく、政府がインシデントレスポンス（IR）を行うベンダーを選定する契約制度にすべき。また、特定社会基盤事業者についても、同様の運用とすることが望ましい旨のガイドラインを策定すべき。	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。
66	本案のⅢ. 2（１）１ やⅢ. 2.（2）に関係して、政府調達契約に係るインシデントレスポンス(IR)において、政府が信頼できるサイバーセキュリティ事業者及びサイバーセキュリティサービスの双方を認定する制度を作成し、政府調達契約に係るセキュリティインシデントの際は、当該認定事業者及び認定サービスの中から選定する制度を創設すべき。また、特定社会基盤事業者についても、同様の運用とすることが望ましい旨のガイドラインを策定すべき。	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。
67	本案のⅢ. ２．（１）に関係して、政府においては民間企業における先進的な技術やナレッジを使って政府機関のサイバーセキュリティ防御を実現することを求めると同時に、実務において得られる知見を国内のサイバーインテリジェンスコミュニティ育成のために活用されたい。	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。
68	Ⅲ. ２．（1） 政府機関等におけるサイバーセキュリティ対策の強化　p22　行2について、 「政府機関等においては、自身が巧妙化・高度化するサイバー攻撃の標的」は、「重要インフラである政府機関等においては、自身が巧妙化・高度化するサイバー攻撃の標的」とすべき。	特に当該記載をせずとも文意がとおるため、原案のままとします。
69	ガバメントクラウドは、サービス開始時から現在まで、事実上、米系クラウドサービス事業者の寡占状態にあるが、地政学的リスクは大きく変動しており、NCOは、サイバーセキュリティ政策の司令塔として、情報のCIAだけでなく、我が国の（自治体を含む）政府機能の継続性や、戦略的自律性の観点も踏まえ、デジタル庁に対し適切に牽制機能を発揮すべきである。	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。 なお、ガバメントクラウドに係る施策は、一義的にはデジタル庁で立案・実施されるものですが、NCOも、政府全体におけるサイバーセキュリティ確保に係る施策の総合調整の観点等から、必要な対応を行って参ります。

69-2	3. （2） 幅広い主体による社会全体のサイバーセキュリティ及びレジリエンスの向上、 p8　行15-20について、 「政府機関等が範となり、強固な対策を実践していくとともに、重要インフラ事業者・地方公共団体はもちろんのこと」は、 「政府機関等が範となり、調達投資を含め強固な対策を率先して実践し、開発ソフトウエアや企画ガイドなどの成果を製品開発事業者やSI事業者を通じて普及させる仕組みを構築し、政府機関等や重要インフラ事業者・地方公共団体はもちろんのこと」とすべき。	政府機関等における強固な対策に関しては、Ⅲ．２．（１）③「強靱な政府情報システムの構築と運用」において、「各政府機関等においては、政府統一基準群やデジタル社会推進標準ガイドライン等を踏まえつつ、自らの業務、情報システムの特性等を踏まえたリスク分析・評価を行い、企画から運用まで一貫したセキュリティ対策を実施する考え方（セキュリティ・バイ・デザイン）を徹底し、適切なセキュリティ水準が確保された情報システムを構築する」旨等を述べています。また、政府においては、政府機関等におけるセキュリティ対策やシステム企画・整備・運用において活用される、政府統一基準群やデジタル社会推進標準ガイドライン等のドキュメントを整備し、一般に公表をしているところです。

	意見の概要	意見に対する考え方（案）
	重要インフラ事業者・地方公共団体等のサイバーセキュリティ対策に係る意見	
70	暗号資産業界のセキュリティを国家レベルの課題として位置付け、各種の施策の対象とすべきである。暗号資産業界について、戦略案には具体的な施策の記載がないが、同業界は北朝鮮の核開発の資金源となっており（戦略案5頁）、政府機関や重要インフラ事業者とは異なる文脈で、セキュリティレベルの抜本的な向上が必要である。NCOは、サイバーセキュリティ政策の司令塔として、同庁（特にその施策の有効性）に対し適切に牽制機能を発揮すべきである。	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。 　なお、ご指摘のとおり、暗号資産業界に係るサイバーセキュリティ確保に関する監督は、一義的には金融庁で実施されるものですが、NCOも政府全体におけるサイバーセキュリティ確保に係る施策の総合調整の観点等から、必要な対応を行って参ります。
71	サイバーセキュリティに関して、事業者同士では話が進みやすいが、国の地方機関や県などではなかなか話が通じない難しさを感じる。 　指導していくべき公的機関で専門的知識が乏しい方々がこの分野を担当されている現状はいかがなものか。せめて、ITパスポートや基本情報処理技術者の保持者に担当させられないか。	外局や地方支分部局を含む政府機関等における人材面の取組については、Ⅲ．２．（１）④「政府機関等におけるサイバーセキュリティ人材の育成・確保と体制の強化」で述べているとおり、各府省庁において必要な体制整備、研修や演習の実施、資格取得の促進等に着実に取り組むこととしております。また、地方公共団体に関しては、Ⅲ．２．（２）②「地方公共団体におけるサイバーセキュリティ対策の強化」で述べているとおり、デジタル人材の確保・育成に対する支援及び人員体制構築に必要な研修プログラムの活用推進等、人材面を含め地方公共団体のセキュリティ基盤の強化のための更なる取組を進めることとしています。こうした取組を通じ、適切な人材育成・確保に努めてまいります。 いずれにしましても、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。
72	都道府県単位で運用されている自治体セキュリティクラウドについて、国が共通基盤を整備し、小規模自治体を含む全国の自治体が安価に利用できる仕組みを検討してはいかがか。	ご意見として承ります。 　なお、Ⅲ．２．（２）②「地方公共団体におけるサイバーセキュリティ対策の強化」で述べているとおり、本戦略では、地方公共団体の自治体情報セキュリティクラウドの更新に向けた財政的な支援も含む取組や、地方公共団体の情報システムに内在する脆弱性等を診断するシステムの構築等の取組を行っていくこととしており、国は、地方公共団体において適切にサイバーセキュリティ対策が実行されるよう、国と地方の役割分担を踏まえつつ必要な支援を実施していきます。
73	Ⅲ．２．（２）①ア「重要インフラ統一基準の作成とこれに基づく取組」「重要インフラ事業者等におけるサイバーセキュリティの確保に関して国の行政機関が実施すべき施策について具体的かつ統一的な基準（以下「重要インフラ統一基準」という。）を新たに定める。」の箇所について「重要インフラ事業者等におけるサイバーセキュリティの確保に関して国の行政機関が実施すべき施策について具体的かつ統一的な基準（以下「重要インフラ統一基準」という。）を新たに定めると共に、当該サイバーセキュリティの確保に関わる機器に対する認証基準を明示し、基幹インフラ制度における届出を行おうとする基幹インフラ事業者が導入等計画策定の段階から当該ベースラインを徹底することを実現する」との修正を提案する。	ご意見として承ります。

74	Ⅲ．２．（２）②「全ての地方公共団体が確実にサプライチェーン・リスク対策を含むサイバーセキュリティ対策を実施できるような新たな仕組みの構築を検討する。」の箇所について「全ての地方公共団体が確実にサプライチェーン・リスク対策を含むサイバーセキュリティ対策を実施できるような新たな仕組みの構築を検討すると共に、当該サプライチェーン・リスク対策が十分に確保された機器に対する認証基準を明示し、すべての地方公共団体において適切にサイバーセキュリティ対策が実行されるよう必要な支援を実施する。」との修正を提案する。	ご意見として承ります。 　セキュリティ機器やセキュリティサービスの審査については、既に経済産業省において実施されているところであり（JC-STAR等）、「地方公共団体の情報セキュリティポリシーに関するガイドライン」においても、地方公共団体における当該制度の活用により、サプライチェーン・リスク対策を適切に講じるよう求めております。 　なお、サプライチェーン・リスク対策を含む新しいサイバーセキュリティ対策の仕組みについては、更なる対策の強化や実効性の確保に向けて検討を進めてまいります。
75	重要インフラ事業者・地方公共団体・中小企業等に対する対策について、一律の水準を求めるのではなく、セキュリティ成熟度に応じた段階的導入モデル を明示いただきたい。具体的には、 フェーズ１：EDR 導入（端末での即時検知・隔離） フェーズ２：XDR による横断的監視・相関分析 フェーズ３：AI-SOAR によるインシデント対応の自動化 というロードマップを提示し、フェーズごとに技術支援・財政支援・人材育成策を紐付けることを提案する。	ご意見として承ります。
76	Ⅲ．２．（２）①ア「重要インフラ統一基準の作成とこれに基づく取組」およびⅢ．２．（２）①イ「重要インフラ防護範囲の在り方」に関して、重要インフラ事業者等に対してサービスを提供するSaaS事業者等も重要なステークホルダーの一つとして情報・意見を提供できる機会をいただきたい。	ご意見として承ります。
77	本案のⅢ ２．（２）１に関係して、特定社会基盤事業分野への追加が検討されている病院分野において、高度なサイバーセキュリティサービス／製品を調達あるいはサイバーセキュリティ対策をアウトソーシングできるように複数病院で共同調達できるような仕組みを作るべき	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。
78	本案のⅢ ２．（２）２に関係して、地方公共団体において、高度なサイバーセキュリティサービス／製品を調達あるいはサイバーセキュリティ対策をアウトソーシングできるよう、一定程度の地域ごとで共同調達できるような仕組みを作るべき	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。 　なお、すでに自治体情報セキュリティクラウド等について、複数団体による共同調達が実施されております。

	意見の概要	意見に対する考え方（案）
	ベンダー、中小企業を含む民間企業等のサイバーセキュリティ対策に係る意見	
79	SBOMやJC-STAR制度の導入は、技術的・人的リソースに乏しい事業者にとって高いハードルである。 　制度の普及と同時に、以下のような支援策が必要である。 ・地域商工会・NPO等と連携した「サイバーセキュリティお助け隊」の拡充 ・ひな形・テンプレートの提供による実務負担の軽減 ・地域別・業種別のリスク評価と対策ガイドラインの提示 　これにより、形式的な遵守ではなく、実質的なセキュリティ向上が期待できる。	賛同意見として承りました。なお、ご指摘の点については、Ⅲ．２．（３）③「中小企業を始めとした個々の民間企業等における対策の強化」において「サイバーセキュリティお助け隊サービスの利用改善に向けた見直し」、「サプライチェーンにおけるリスクに応じて各企業が取るべきセキュリティ対策の水準を可視化・確認する制度の活用促進にむけたガイドライン等の整備・規程類のひな形の提示」、「サプライチェーンにおけるリスクに応じて各企業が取るべきセキュリティ対策の水準を可視化・確認する制度の仕組みの整備」を記載しております。
80	SI企業がユーザー企業に納入しているソフトウェア、システムに関して、運用を止めてでも、利用しているOS、OSSの脆弱性が発覚したらすぐにアップデートする、させることを国として強制してほしい。IT業界に長らく勤めているものとしては、現場が脆弱性対策をしようと試みてもユーザー企業、およびその仲介のSI企業が全く耳を貸さない。モダナイズを進めるより脆弱性をすぐに修正するための対応、また対応を怠っていたSI企業を法的に罰するような施策を強く求める。	一般に、ソフトウェア脆弱性への対応は、当該脆弱性のパッチを当てる等の手法以外にも様々なリスク回避・軽減手法が考え得ること、当該脆弱性がもたらすリスクやパッチ当て作業に伴う影響は、システムによって多様であるため、あらゆる脆弱性に関して、全てのシステムに対して運用を停止してアップデートすることを一律に義務化・強制することは、必ずしも適当ではないと考えられます。 　その一方で、今般成立したサイバー対処能力強化法においては、基幹インフラ事業者に対するソフトウェア等脆弱性に係る国からの是正措置要請が規定されたところであり、基幹インフラ事業者に対する必要な措置が認められれば、国は対応を求めることとなると考えられます。 　また、基幹インフラ事業者以外の事業者においても、リスクを踏まえて緊急の対応が必要な脆弱性については、速やかな対応が求められることはいうまでもなく、必要な対応が速やかに図られるよう、国としては、関係団体とも連携の上、ガイドラインの整備や普及啓発活動を含め、様々な施策を推進していきます。
81	経営層執行側、投資家間のコミュニケーションの円滑化を図り、サイバーセキュリティに関する重要情報の正確かつタイムリーな開示（適時開示）を行うことを念頭に、有価証券報告書への記載義務を検討する。また、コーポレートガバナンスコードにサイバーセキュリティに関する方策を明確に記載すべきである。 　米国では2023年に上場企業に対し、①サイバーセキュリティのリスク管理と戦略、ガバナンスに関する一定の情報をForm 10-K（年次報告書）において開示すること、および②顧客情報への不正アクセス等のサイバーセキュリティ・インシデントが発生した場合、当該インシデントを重要と判断した時点から原則４営業日以内に Form 8-K（臨時報告書）で開示することを義務化した。わが国においてもこうした事例を参考に速やかに取り組むべきである。	ご意見として承りました。
82	世界のサイバーセキュリティ保険市場は年々拡大し、2024年度では200億ドルを超えると想定されている。しかし、わが国のサイバーセキュリティ保険市場は約300億円の規模と言われ、市場規模が小さく、かつ日本企業のサイバー保険加入率は7.8%と欧米に比べ低い。サイバー保険は新たな分野であるため、各保険会社だけではデータが不足している状況である。政府主導でデータ集約、分析、ルール作りをして、サイバー保険によるリスク評価の枠組みとしての選択肢を作るべきである。 　サイバーセキュリティ評価、サイバー保険、有価証券報告書など一体として運用すべきである。	ご意見として承りました。

83	国が中小企業向けの集団的防御プラットフォームのような仕組みを設け、安価なツールを導入するだけで脅威監視、分析、対処等の支援を受けられるようにしてはいかがか。	ご意見として承ります。 　中小企業に関しては、Ⅲ．２．（３）③で述べるように、人材・予算等の十分なリソース確保が困難といった課題があるという認識の下、「自助」「共助」「公助」の考え方を組み合わせつつ、「公助」の取組としてサイバーセキュリティお助け隊サービスを始めとした外部専門家の支援を得られる仕組みの整備や、基幹インフラ事業者のサプライチェーンに属する中小企業等からの情報収集・統合・分析・還元による「集団的防御」の枠組みの導入を進める等の取組により、中小企業のサイバーセキュリティ対策の支援に取り組んでまいります。
84	人的・技術的リソースの不足が顕著である中小企業や地方自治体への支援として、「共通SOC基盤」や「簡易ゼロトラスト導入支援」などの、現場レベルでの即応力向上策を講じていただきたい。	中小企業に関しては、Ⅲ．２．（３）③で述べるように、人材・予算等の十分なリソース確保が困難といった課題があるという認識の下、「自助」「共助」「公助」の考え方を組み合わせどのような支援が必要であるかも検討しつつ、「公助」の取組としてサイバーセキュリティお助け隊サービスを始めとした外部専門家の支援を得られる仕組みの整備や、基幹インフラ事業者のサプライチェーンに属する中小企業等からの情報収集・統合・分析・還元による「集団的防御」の枠組みの導入を進める等の取組により、サイバーセキュリティ対策の支援に取り組んでまいります。 　また、地方公共団体については、自治体情報セキュリティクラウドのの更新に向けた財政的な支援も含む取組や、地方公共団体の情報システムに内在する脆弱性等を診断するシステムの構築等の取組等を含め、国は、地方公共団体において適切にサイバーセキュリティ対策が実行されるよう、国と地方の役割分担を踏まえつつ必要な支援を実施していきます。
85	政府が推進するサイバーセキュリティ施策・指針については、クラウド環境に限定せず、ハイブリッド環境やオンプレミス環境も視野に入れ、具体的な方策を明確化すべき。 　また、一般企業における導入を実効的に促進するため、JC-STAR制度の活用に加え、基準を満たした場合の税優遇措置などのインセンティブ施策や、一定の水準を満たさない場合の罰則規定の整備といった、費用捻出が難しい企業を後押しする多角的な方策の検討が必要。	ご意見として承ります。 　なお、政府のサイバーセキュリティ施策やガイドライン等は、必ずしもクラウド環境のみに限定したものではありません。 　また、「JC-STAR」制度については、更なる制度構築を進め、ガイドライン・補助金等各種施策と組み合わせつつ、政府機関・地方公共団体・重要インフラ事業者・産業界等、社会全体で活用を促進することとしています。
86	中小企業のセキュリティ対策強化のため、セキュリティ投資に対する税制優遇、補助金などの具体的な公的支援策（インセンティブ）を戦略的に組み込み、公助を強化すべき。	中小企業のセキュリティ対策の推進に向けては、政府・業界団体・支援組織等が連携して行ってきた「自助」・「共助」・「公助」を組み合わせた施策を一層強化する必要があるとしているところです。 　「公助」に関する施策の在り方を含め、引き続き必要な施策を検討してまいります。

87	経済産業省が進めている2026年度運用開始予定の「サプライチェーンにおけるリスクに応じたセキュリティ対策の水準を可視化・確認する制度」について、既存のセキュリティ認証制度（ISMAP或いは、ISMS、国際規格等）との連携・相互活用を最大限検討し、ベンダー側の多重審査や対応負担の増加を回避すべき。	ご意見については、今後の制度設計についての検討の参考とさせていただきます。
88	中小企業に対して、インシデント対応（スポット支援）に加え、安価で信頼性の高い国産MSSやMDRの導入を支援する新たな公助の枠組み（例：「継続モニタリング支援モデル」）を検討いただきたい。	中小企業に関しては、Ⅲ．２．（３）③「中小企業を始めとした個々の民間企業等における対策の強化」で述べているように、人材・予算等の十分なリソース確保が困難といった課題があるという認識の下、「自助」「共助」「公助」の考え方を組み合わせどのような支援が必要であるかも検討しつつ、「公助」の取組としてサイバーセキュリティお助け隊サービスを始めとした外部専門家の支援を得られる仕組みの整備や、基幹インフラ事業者のサプライチェーンに属する中小企業等からの情報収集・統合・分析・還元による「集団的防御」の枠組みの導入を進める等の取組により、サイバーセキュリティ対策の支援に取り組んでまいります。
89	「全員参加によるサイバーセキュリティの向上」の理念に賛同する。その実現のため、中小企業のリソース不足に対応するための専門家派遣制度や、業界団体を通じた教育・支援体制への政府支援の拡充をお願いしたい。	賛同意見として承りました。Ⅲ．２．（３）③「中小企業を始めとした個々の民間企業等における対策の強化」でも述べている通り、セキュリティの外部専門家による支援を容易に探索・依頼できるような仕組みの整備・活用促進等を通じた「公助」を推進してまいります。
90	一定規模以上、または特定分野の企業・団体に対して、重大サイバーインシデントの政府機関への報告を「実質的に義務に近い形」で求める制度（報告対象・期限・報告先の明確化）を導入すべき。 　また、定期的なセキュリティチェック（自己点検・外部監査など）の実施と、その結果を踏まえた改善計画策定を求める仕組みを検討すべき。 　加えて、攻撃の手口や実施事項等の事例を政府主導でプラットフォーム上で日本企業に公開するような仕組み検討すべき	ご意見として承ります。なお、今般成立したサイバー対処能力強化法においては、基幹インフラ事業者は、特定重要電子計算機のインシデント情報やその原因となり得る事象を認知したときは、事業所管大臣及び内閣総理大臣に報告することが義務づけられております。 　また、例えば、Ⅲ．１．（２）①「官民間の双方向・能動的な情報共有と対策強化のサイクルの確立」において、サイバーセキュリティの最前線に立つ実務者層が、経営層の理解の下で実効性の高い対策を講じられるよう、国は技術的な脅威の動向や具体的な攻撃手法、対応方法といった実践的な情報を積極的に提供することを記載しています。
91	「サプライチェーン強化に向けたセキュリティ対策評価制度」★４以上の構築・運用につき、以下をご教示いただきたい。 １．【認定機関】当該制度に係る認定・評価を実施する主体はどの機関を想定されているか。政府機関、独立行政法人、民間の第三者認証機関、業界団体等のいずれか、または複数併存となるか。 ２．【義務の有無】本制度の認定取得は原則任意との理解でよいか。あるいは、重要インフラ・重要産業や一定規模（例：従業員数・売上・資産規模等）以上の事業者に対して取得を義務付ける想定であるか。一定の義務付けが想定される場合は、義務付け対象の業界・条件等、また経過措置、適用開始時期、不適合時の対応（罰則・発注制限の有無）などの想定をご教示いただきたい。 ３．【制度運用】 当該基準・制度は、政府統一基準に規定の上、政府調達における入札参加資格・技術要件等として導入することを想定しているか。（要は政府案件の入札時には認定を必須とするなど） 他方、民民の取引・委託契約においては、本認定制度の活用を「義務」、「推奨」、「任意」のいずれに位置付けるのか、方針をご教示いただきたい。	経済産業省及び内閣サイバーセキュリティセンター（現国家サイバー統括室）が2025年４月に公表している「サプライチェーン強化に向けたセキュリティ対策評価制度構築に向けた中間とりまとめ」において、以下の方向性が示されています。引き続き政府において検討を進め、今後、「サプライチェーン強化に向けたセキュリティ対策評価制度」の具体的な内容や運用方針について「制度構築方針（案）」として取りまとめる予定です。 1.【認定機関】について、★４については、認定機関から認定を受けた評価機関による第三者評価スキームを想定している。 2.【義務の有無】及び3.【制度運用】 について、制度が効果的と想定される業界等については、優先的に制度活用を促進していく。そのために、例えば、中小企業の情報セキュリティガイドラインへの追記や、 業界毎の特性を踏まえた導入促進、政府調達での参照や重要インフラ事業者等での活用推奨等について検討を進める。

92	Ⅲ．２．（１）①エ「政府機関等のIT調達等におけるサプライチェーン・リスクの軽減」の「そのような環境変化の下にあってもサプライチェーン・リスクを十分に軽減できるよう、関連制度との調和を図りつつ」の箇所について「そのような環境変化の下にあってもサプライチェーン・リスクを十分に軽減できるよう、サイバーセキュリティ成熟度モデル認証（CMMC: Cybersecurity Maturity Model Certification）やNIST SP800-171など各国で既に確立されている手法を参考にした上で、わが国独自の認証モデルを確立し、関連制度との調和を図りつつ」との修正を提案する。	ご意見として承ります。 なお、ご指摘いただいた制度を含め、諸外国の制度を参考にしながら、今後も我が国の制度の適切な運用に努めて参ります。
93	Ⅲ．２．（３）③「セキュアバイデザイン原則等に基づくベンダー等における責任あるサイバーセキュリティ対策の取組の推進」「社会全体で促進に取り組んでいくとともに、我が国が主導する形での諸外国との制度調和に向けた活動に取り組んでいく。」の箇所について「社会全体で促進に取り組んでいくとともに、我が国が主導する形での諸外国との制度調和に向けた活動及び、ISMS （ISO 27001）やBCMS （ISO 22301）など既に確立されている諸制度及び規格との制度調和に向けた活動に取り組んでいく。」との修正を提案する。	ご意見については、今後の制度設計についての検討の参考とさせていただきます。
94	サプライチェーン全体のセキュリティ確保にあたり、ゼロトラスト・アーキテクチャの成熟度評価 を導入し、各組織の到達度を戦略本部が定期的に評価・フォローアップする仕組みを提案する。例えば、1. 多要素認証の適用率、2. デバイス／ネットワークの分離・可視化状況、3. 特権アクセス管理の実装状況等を指標化し、「ゼロトラスト成熟度レベル」として整理・公表することを検討いただきたい。	ご意見として承ります。
95	本案のⅢ．２．（１）１ やⅢ．２．（３）に関係して、令和4年10月に経済産業省と公正取引委員会は「サプライチェーン全体のサイバーセキュリティ向上のための 取引先とのパートナーシップの構築に向けて」を公表したが、特に特定社会基盤事業者や政府調達において、下請法におけるサプライチェーンへの適法な支援／要請がどのようなものであるかより具体的で明確にすべき。	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。
96	日本が包括的なマルチステークホルダー関与を通じて、社会全体のサイバーセキュリティおよびレジリエンスの強化に注力されていることを高く評価している。社会のサイバーセキュリティ体制を強化するためには、重要インフラ事業者、地方公共団体、民間企業の技術的および政策的欠陥を理解し、緩和する努力が不可欠であると考えている。 エコシステムのセキュリティを強化するために、リスクベースのサイバーセキュリティ国際標準などを活用した重要インフラ保護の取り組みを強く支持する。 サプライチェーン全体の保護は極めて重要である。民間部門と連携してセキュアバイデザイン原則を通じて透明性および説明責任を促進する取り組みを歓迎する。 実践的なガイドライン、テンプレート、支援サービスで中小企業等を支援することは、セキュリティエコシステムのギャップを解消する鍵となる。既存のベストプラクティスを強化するために、日本が他国や国際標準化団体によって開発された資源や枠組みを活用し、中小企業等のサイバーセキュリティを支援することを期待する。 日本と提携して、重要インフラを保護するサイバーセキュリティ取り組みを推進することを期待する。 そして、政府、産業界、学界、および市民社会の間の積極的な協力は、社会のあらゆる部分においてセキュリティを実現する基礎となる。これには、デジタル影響力の脅威に対するレジリエンスが含まれる。	基本的に、戦略案への賛同意見として承りました。

	意見の概要	意見に対する考え方（案）
	全員参加によるサイバーセキュリティ向上に係る意見	
97	防衛省、経産省、デジタル庁などの大臣クラスが公開イベントなどで危機的な状態を国民に告知するべき。国として国民の危機感を煽ることはいかがかと思うし、SNSのフェイクニュースなどの懸念もあるが、その対応もサイバーセキュリティの実務の一環と考え、継続的に国として告知を行うべき。 　サイバー以外の危機的な状況についての国民とのコミュニケーションと合わせて、長期での国民への情報発信計画が必要だと思う。	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。なお、「サイバー空間における脅威の実態について、国民の認識と理解を得ることの必要性」については、「Ⅱ３．サイバー空間を取り巻く課題認識及び施策の方向性」において、本戦略に基づき施策を推進するに当たっての留意点として述べられております。 　また、いただいたご意見を踏まえて、Ⅲ２．（４）「全員参加によるサイバーセキュリティの向上」において、以下下線の文言を追加することとします。 「これまで国は、ウェブサイトやSNSでの情報発信、講習会等の開催、ハンドブック・教材等のコンテンツの整備のほか、サイバーセキュリティ月間の取組を推進し、関係者が連携・協働する仕組みを下支えしてきた。国は、引き続きこの役割を担いつつ、環境や多様なニーズに合わせて各コンテンツを適切にアップデートし、より広くその情報が届くように関係者との連携を拡大・強化していく。**その際、様々な主体の対策や行動が促進されるように、厳しさを増すサイバー空間を取り巻く情勢等に関する情報発信も念頭に置く。**」
98	サイバーセキュリティのリテラシー向上や人材育成・確保の視点から初等教育段階から中等教育までセキュリティ教育をすべき。また民間人材を活用し、生徒の教育レベルの向上や教える側である教員の知識向上を行うべき。 　セキュリティ人材の即戦力、さらにはトップ人材を広げるためには高専、大学、大学院の人材において質、量を広げる必要がある。例えば、豪州で導入しているサイバーアカデミーを参考にサイバーセキュリティを専門に学べる仕組みを検討してはどうか。	本戦略において、「数理・データサイエンス・AI教育プログラム認定制度」を通じた大学や高等専門学校におけるサイバーセキュリティを含む数理・データサイエンス・AI教育の強化や、「セキュリティ・キャンプ」等の若年層を対象とした高度な技術教育プログラムの推進を図ることとしていますが、いただいたご意見も踏まえ、引き続き施策の在り方を検討して参ります。
99	「情報セキュリティを含む情報教育の充実」については、官民連携の活用を通じて、現実に何が起きているのかを実感できる学びを提供し、サイバーセキュリティに関するリテラシーの向上につなげていただきたい。	賛同意見として承りました。いただいたご意見も参考としながら、実効性のあるリテラシー向上が図られるよう、Ⅲ．２．（４）　「全員参加によるサイバーセキュリティの向上」で述べているとおり、関係者との連携を拡大・強化しながら、コンテンツの整備等を進めてまいります。

	意見の概要	意見に対する考え方（案）
	サイバー犯罪への対策を通じたサイバー空間の安全・安心の確保に係る意見	
100	詐欺による不正送金被害について「自己責任である」という考え方もあるが、現状の脅威は以下のような背景から、個人の責任に帰すことには限界がある。 自己責任論の限界と政策的介入の必要性がある。 ・国をまたぐ組織的な犯罪者グループの関与: 高度な技術と組織力を持つ国際的な犯罪者集団が背景におり、その摘発や被害回復は一国の捜査機関だけでは困難	御指摘のとおり、サイバー犯罪は、手口の高度化や国際化が進んでいることから、このような現状を踏まえ、引き続き、サイバー犯罪への対策を通じたサイバー空間の安全・安心の確保に努めてまいります。
101	金融機関へのインセンティブ政策の導入を検討すべき。 我が国においても、金融機関に対して詐欺被害の補償を求める政策誘導が議論されるべきである。	ご意見として承ります。金融機関による詐欺被害の補償制度がサイバーセキュリティの確保と直接関係するかは必ずしも明確ではありませんが、重要インフラ事業者かつ基幹インフラ事業者でもある金融機関のサイバーセキュリティ対策は当然重要であり、金融庁を通じて必要な対応を行ってまいります。

	意見の概要	意見に対する考え方（案）
	サイバー対応能力を支える人材に係る意見	
102	政府機関等、重要インフラ事業者および一定規模以上の一般企業に対して、「情報処理安全確保支援士」をサイバーセキュリティに関する主要部署（経営企画、システム開発・運用、CSIRT、内部監査等）に所要人数を配置することを義務付けるべき。	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。なお、情報処理安全確保支援士の活用促進に関しては、Ⅲ．３．（１）　②「サイバーセキュリティ人材の育成に資する教育や演習・訓練の更なる充実」において、「国家資格である情報処理安全確保支援士については、資格更新時の負担軽減を図りつつ、中小企業のセキュリティ対策支援を含め、活用促進に向けた取組を進める」と記載しております。
103	サイバー分野は、単なる技術習得ではなく、技術者の「独自の視点」「美意識」「倫理観」が成果に直結する領域である。よって、以下の視点を追加すべきである。 ・技術者の「署名性（signature）」を尊重する教育・評価制度の構築 ・自由度と倫理性を両立する育成環境の整備 ・地域の若者や非正規技術者へのアクセス機会の拡充 官民交流における創造性の尊重とリスク管理の両立	ご意見として承りました。
104	たとえば情報処理安全確保支援士を、現行の宅地建物取引士相当に格上げし、中小企業基本法に相当しない大企業には、会社法上の関連会社単位で１名以上の常勤を義務付けというのはどうだろうか。 　なお、中小企業基本法に相当する中小企業についても情報処理安全確保支援士の１名以上の常勤が望ましいが、こちらは規模の多寡によって差があることから、商工会議所での１名以上常駐を定義し、必要に応じて管下の中小企業基本法に相当する中小企業を支援するという方策を提案したい。	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。なお、情報処理安全確保支援士の活用促進に関しては、Ⅲ．３．（１）　②「サイバーセキュリティ人材の育成に資する教育や演習・訓練の更なる充実」において、「国家資格である情報処理安全確保支援士については、資格更新時の負担軽減を図りつつ、中小企業のセキュリティ対策支援を含め、活用促進に向けた取組を進める」と記載しております。
105	本戦略においては「人材・技術のエコシステム形成」の項に「人材育成と並行した業務効率化・標準化支援」という観点を明記し、国が積極的に推進いただきたいと考えている。	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。 　なお、サイバーセキュリティ対策に関する作業効率化に関しては、例えば、Ⅲ．１．（１）①「インシデント対処の高度化による被害の拡大・深刻化の防止」に記載しているように、「被害組織が対処活動に集中できるよう、国は、被害組織からのインシデント報告にかかる負担の軽減を目指し、サイバー対処能力強化法に基づく報告も含めた報告様式の一元化とともに、報告先の一元化に向けて所要の調整を進める。」こととしているほか、基幹インフラ事業者による国へのインシデント報告等のための情報共有基盤の整備を行うこととしています。 　また、Ⅲ．２．（３）「ベンダー、中小企業等を含めたサプライチェーン全体のサイバーセキュリティ及びレジリエンスの確保」において、サプライチェーンにおけるリスクに応じて各企業が取るべきセキュリティ対策の水準を可視化・確認する制度の活用促進にむけたガイドライン等の整備・規程類のひな形の提示等を述べているところですが、こうした取組を含め、民間企業等において、サイバーセキュリティ対策が効率的に実施できるような取組を推進して参ります。

106	本戦略案に強く賛同する。 　特に「全員参加によるサイバーセキュリティ」および「人材／技術のエコシステム形成」という理念は、極めて重要であり、我が国の安全保障の根幹を支えるものと考える。 　しかしながら、現場のリアリティを見れば、この美しい理念が「技術者中心の発想」に留まる限り、社会全体のレジリエンスは決して高まらない。 　「文系セキュリティ人材」の明確な定義と政策上の位置付けを行ってもらいたい。 　技術者以外のリスク、法務、教育、監査担当をサイバー人材フレームワークの正式な領域として明示し、研修、育成、資格制度の対象に含めるべき。 「委託先管理・リスク評価・教育運用」を担う文系セキュリティ実務者への支援策を新設してもらいたい。 　本戦略が掲げる「サプライチェーン全体のレジリエンス確保」（新たなサイバーセキュリティ戦略（案）の概要）は、実務的には「取引先チェック」「契約条項」「再委託確認」「台帳更新」などの非技術業務の上に成り立っている。 　これを支えるツール、SaaS、ガイドライン整備への支援を求める。 「セキュリティDX」の文脈に文系セキュリティのDXを含めてもらいたい。 　本戦略案が強調するAI、量子、能動防御も重要であるが、Excelとメールに依存した旧来運用を脱却し、リスク評価を自動化・共有できる環境整備こそ、官民一体の防御基盤の礎となる。 官民連携エコシステムの中に「2線部門」を組み込んでもらいたい。 　現在の想定ではCSIRTやSOCが中心だが、実際に各組織で「防御・抑止の起点」となるのはリスク、セキュリティ、コンプライアンス部門である。 　彼らを巻き込んだ研修、演習、協議会こそ、能動的防御を支える真のエコシステムである。	賛同意見として承りました。 　なお、Ⅲ．３．（１）①で述べている「人材フレームワーク」においては、意思決定・戦略策定、法務、教育・訓練、監査等の技術的な役割以外についても、人材像として広く定義しており、本フレームワークを軸として、研修等の様々な育成施策を包括的に一層充実させる想定です。 　また、「専門的なセキュリティスキルを有していない人材」に関する学習機会の提供としては、例えばⅢ．３．（１）②「サイバーセキュリティ人材の育成に資する教育や演習・訓練の更なる充実」において、「専門的なセキュリティスキルを有していない人材についても組織内外のセキュリティの専門家と協働する上で必要な知識を習得したプラス・セキュリティ人材となれるような学習機会の充実化を図る。」と記載しております。 　ほか、本戦略において、マネジメント層がサイバーセキュリティ確保に関して必要な認識・理解をしていることが、企業等におけるサイバーセキュリティ向上に大きな影響を与えることを踏まえ、例えば、Ⅲ．.２．（３）②「サプライチェーンを通じたサイバーセキュリティ及びレジリエンスの確保」において、「サプライチェーン全体でのサイバーセキュリティ及びレジリエンス確保に向け、単なるシステム管理の問題ではなく、包括的なリスク管理の問題として、サイバーセキュリティに係る視点を企業経営に取り入れる必要性がある。そのため、国は、経営者の意識改革や企業の行動変容をより強力に促し、各企業がセキュアな製品調達や取引先選定を行うための環境整備に取り組む。」と記述しているほか、Ⅲ．１．（２）①「官民間の双方向・能動的な情報共有と対策強化のサイクルの確立」において「官民間の複層的な対話の継続的な実施が重要である。実務者層から経営層まで参加し、必要に応じて個別または分野横断的に異なる階層で行うなど、多角的な視点から対話に取り組む」と述べています。
107	33頁30行目の段落に関して、33行目の「人材フレームワークを軸に、様々な施策を有機的に連携させながら効率的・効果的な人材育成を進める。」を「人材フレームワークを軸に、待遇改善や我が国の企業への就労促進策などをはじめとした様々な施策を有機的に連携させながら効率的・効果的な人材育成を進める。」とする方が良い。高度スキルを持った人材は我が国の企業では待遇が低く定着しないためである。	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。
108	サイバーセキュリティの人材強化における産官学の共通認識をするためにも、諸外国の事例や国内の動きを参考に、政府主導で人材定義の可視化および教育機関との連携をする必要がある。 　取り組みにあたっては、欧米諸国の事例を参考にすべきである。	人材フレームワークについては、NCOにおいて現在サイバーセキュリティ人材フレームワークに関する検討会での議論も踏まえ具体的な検討を進めています。諸外国の人材フレームワークの動向等も踏まえて、引き続き具体的な取組を検討してまいります。
109	若年層のみを主な対象とする現行の方針を見直し、就職氷河期世代やホスト氷河期世代を含む中堅層を戦略的な人材として位置づけ直すとともに、ＳＥＳや派遣、請負に偏った産業構造を是正しなければ、国家として必要なサイバー防御力と人材基盤を確保できないのではないかという問題意識をお伝えし、改善をご検討いただきたい	本戦略における人材の育成は、Ⅲ．３．（１）②「サイバーセキュリティ人材の育成に資する教育や演習・訓練の更なる充実」でも「初等中等教育段階から高等教育、職業訓練、社会人の能力開発、高度専門人材の育成に至るまで、体系的かつ継続的な学びの環境整備が求められる」と述べるとおり、若年層のみを対象としておりません。特定の年齢層に限らないトレーニング等の機会の提供を含め、多様な学びの機会が継続的に提供され、それらを通じて得た知識・技能がキャリア形成や活躍の場につながるよう、各種教育・訓練制度を俯瞰しながら、改善を進めてまいります。

110	政府機関や民間企業が学生等を一定期間受け入れ、実際のログ分析や運用業務を通じて訓練する「実務即応型訓練制度」を導入・政策支援し、即戦力人材の育成を加速させる等の取り組みを検討すべき。	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。
111	「人材フレームワーク」の整備方針を支持する。特に、産業界の実務スキルと教育機関の専門知識を接続する仕組みを設けることで、即戦力となる人材育成に繋がると考える。	賛同意見として承りました。
112	本戦略が示す「国産技術・サービスを核としたエコシステム形成」は日本のサイバー主権を確立するうえで不可欠。産学官連携による研究開発支援や、スタートアップ企業への資金的・制度的支援の拡大を期待する。	賛同意見として承りました。
113	人材の早急な確保については情報処理安全確保支援士を企業（大・中小規模問わず）に必置または専属支援士を義務付け、情報処理安全確保支援士の独占業務を策定すべきと提言する。	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。なお、情報処理安全確保支援士の活用促進に関しては、Ⅲ.3．（1）　②において、「国家資格である情報処理安全確保支援士については、資格更新時の負担軽減を図りつつ、中小企業のセキュリティ対策支援を含め、活用促進に向けた取組を進める」と記載しております。
114	高度な人材・技術の力強いエコシステムを構築し、国のサイバーレジリエンスを強化するという日本のビジョンを強く支持する。産学官の連携を通じた優れたサイバー人材の育成は、複雑化するサイバー脅威に対応する上で不可欠である。 イノベーションを促進し、新たな技術やサービスを創出することの重要性を認識している。相互運用性と国際標準への準拠は、セキュリティとレジリエンスを確保する上で不可欠であり、日本が最先端のセキュリティソリューションを活用されることや、国内企業が国際的に成功することを可能にすると考えている。 人工知能や量子技術は、機会とともに課題ももたらす。安全な開発ガイドラインや、敵対的なAIやAIを悪用したサイバー攻撃に対抗する施策など、AIの安全性とセキュリティに関する日本の積極的な姿勢を歓迎する。 また、2035年までに耐量子計算機暗号（PQC）に移行する目標を設定されたロードマップも評価しており、円滑かつ安全な実装を支援するために専門知識を提供している。 　日本が量子暗号通信（QKD）技術の継続的な研究開発に関心を示されていることを支持しているが、現在の限界を踏まえほとんどの組織が耐量子を実現する主要な手段としてPQCを実装する必要性を強調することが重要である。	基本的に、戦略案への賛同意見として承りました。

	意見の概要	意見に対する考え方（案）
	サイバー対応能力を支える技術開発等に係る意見	
115	米国との関税交渉の条件である米国への投資の一部を日本からの米国サイバーセキュリティ企業、事業へ投資し、その成果を日本のサイバーセキュリティの戦略に効果的に活用する。 　既に政府、企業は多くの米国企業のサイバーセキュリティ製品、サービスを活用している。国産が望ましいと言う意見は分かるが、現実的には米国の技術活用が必須であり、米国との関係の一環としてサイバーセキュリティに関わる技術の推進を共同で行う案は検討しても良いのではないか。	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。 　なお、一般論としては、サイバーセキュリティ分野における技術・サービスに係るエコシステム形成に関して、Ⅲ．３．（２）　において「我が国の国際競争力の確保や、安全保障上の懸念が生じないことを前提として、必要に応じ、国際連携の下、推進していく。」と記載しており、必要な国際連携をすべて排除しているものではありません。
116	33頁17行目の段落に関して、18行目の「研究開発・開発支援・実証の実施・拡充や、それらを通じた技術情報等の活用、スタートアップ支援等」を「研究開発・開発支援・実証の実施・拡充や、それらを通じた技術情報等の活用、事業支援等」とする方が良い。スタートアップはさまざまな目論見で見栄えの良い実績を出すことができる場合もあるが、既存の企業が新たにチャレンジしている事例も同じく存在している。	ご指摘の「スタートアップ支援等」は例示であり、サイバーセキュリティ産業の育成のための施策は、スタートアップ向けの施策のみに限定しているものではありません。本戦略では、サイバーセキュリティサービス提供事業者が正当に評価される仕組みの整備や、我が国のサイバーセキュリティ製品・サービス提供事業者の海外進出等に資する施策を推進・検討についても記述しているように、既存企業も対象となる施策も組み合わせて推進していきます。
117	「サイバーセキュリティサービス提供事業者が正当に評価される仕組みの整備」について、サービスの「セキュリティ効果」や「品質」を定量的に評価するための統一的かつ客観的な評価指標の策定を急ぐべき。	ご意見については、今後の制度設計についての検討の参考とさせていただきます。
118	政府調達において、国内サポート体制やクラウドネイティブな運用自動化技術の有無を評価項目に加え、優れた国産技術を有するスタートアップや中堅企業が採用されるインセンティブ設計を導入してはどうか。	ご意見として承ります。
119	AI防御技術やクラウドセキュリティ等の新興領域において、日本発の技術がデファクトスタンダードや国際標準として採用されるよう、政府による戦略策定と民間企業の参画支援を強化してほしい。	ご意見として承ります。 　政府として、企業や研究機関等とも積極的に連携し、基礎研究を含むサイバーセキュリティ分野の技術開発、社会実装や国際標準化に向けた取組を引き続き推進してまいります。

	意見の概要	意見に対する考え方（案）
	新技術への対応に係る意見	
121	AI や量子技術への対応は、技術的な先手だけでなく、「人間中心設計」「説明可能性」「社会的受容性」などの視点が不可欠。 　とくにAI for SecurityやSecurity for AIの取組においては、「住民が安心して使えるか」「説明が理解できるか」「誤操作が防げるか」といった設計思想を重視すべきである。 　技術は人間のためにあるものであり、制度設計においても「人間性を尊重する設計思想」が根幹に据えられるべきである。	ご意見として承りました。なお、Ⅲ．３．（３）①「AI技術の進展及び普及に伴う対応・取組」において「AI がサイバーセキュリティにもたらすメリットを最大限に享受しつつ、負の側面を最小化するために、国際的な動向及び技術の進展、サイバー攻撃の動向等を踏まえ、研究開発、ガイドラインの整備等のルール形成、社会実装、人材育成等の様々なアプローチを総合的に推進する。」と記載しております。
122	複数の量子コンピューター開発企業より、2029年までには誤り耐性を持つ量子コンピューターが市場投入される可能性は限りなく高く、RSA暗号をはじめとした公開鍵暗号が破られるリスクは更に高まる。2020年代には更に激甚化するサイバー攻撃から守る手段を社会に導入することが必要であり、そのためにはPQCを導入するのが最も現実的な解である。 現在、国家サイバー統括室で進めているPQC導入ガイドラインを本年12月末までに作り上げ、まずは国が指定した重要インフラからPQCへの移行にむけて、官民協力のもと導入を開始すべきである。 　サイバー空間における脆弱性はIoTによって繋がるサイバー社会において、末端のエッジデバイスと国民、企業をつなげるレガシーな有線システム（個別拠点に引き込んだ光ファイバーケーブルを電子情報に変換するルーターやテレビなどを繋ぐセットボックス）は中国で製造・輸入された安価な製品が多く、サイバー攻撃の起点となる可能性が最も高いと考えられ、社会基盤のみならず、個別住宅を含むエッジ対策も、1日も早く国家サイバー統括室において検討を開始するべきである。	ご意見として承りました。 　ご指摘のIoT機器のセキュリティ対策については、本戦略においても一定のセキュリティ水準を満たすIoT製品を認証する「JC-STAR」制度等、ベンダー等における責任あるサイバーセキュリティ対策の取組の推進等を掲げているところであり、引き続き関係省庁とも連携して、必要な対策の推進を行っていきます。 　なお、Ⅲ．３．（３）②「量子技術の進展に伴う対応・取組」において、「**ただし、情報の重要性や暗号技術の利用状況等を把握した上で、どのように移行を進めるかを検討し、適切に判断する必要がある。例えば、特に機微な情報や保護期間が非常に長期となることが想定されている情報等を扱う場合等においては、より早期に移行を行うことも含め、情報システムごとに適切に検討を行うこととする。**」との脚注を記載することといたします。
123	現在、内閣府及び経済産業省において、経済安全保障推進法の改正の議論が進行している。上記の通り基盤インフラ強化においてPQCの導入を加えるべきであるとともに、先端技術の官民技術開発協力の対象として対量子計算暗号技術の開発を含めた我が国の情報インフラ強化技術開発をその対象に明示すべきである。 　開発あるいは導入した耐量子計算機暗号の有効性を確かめるには、「防御技術」を検証する「攻撃技術」が必要となり、攻撃技術も官民の技術協力に加えるべきである。しかし、本件については国家の機微情報に該当する可能性が高く、取り扱いには十分な配慮が必要であると考えている。	ご意見として承りました。 　また、Ⅲ．３．（２）「新たな技術・サービスを生み出すためのエコシステムの形成」や（３）「先端技術に対する対応・取組」で述べているとおり、サイバーセキュリティ分野の技術開発等の取組の推進に加え、先端技術がサイバーセキュリティや国家安全保障等にもたらす影響を踏まえ、必要な取組を推進してまいります。
124	重要技術およびサイバーセキュリティに関する国際連携において、わが国が「信頼に足るインフラ保有国」として位置づけられるため、PQC標準策定から実装までの全体プロセスに能動的に参加するべきである。 　わが国はセキュリティ・クリアランス制度の実施およびサイバー情報空間の保護なしには国際インテリジェンスコミュニティーの仲間入りができないことを自覚すべきである。	Ⅲ．１．（３）③「国際的なルール形成の推進」で述べているとおり、国際的なルールの形成等に向けて対応を進めてまいります。 　また、Ⅲ．１．（３）①「同盟国・同志国等との情報・運用面での協力の強化」で述べているとおり、必要な情報保全措置を徹底した上で、情報等を的確に共有し、我が国のサイバー分析・対処能力向上に資する情報協力を進めてまいります。
125	AIや量子技術などの先端分野で国際的なルール形成に積極的に参画する姿勢を支持する。	賛同意見として承りました。
126	政府機関等におけるPQCへの移行について、原則として2035年までを目指し、2026 年度に工程表（ロードマップ）を策定するとの方針を支持する。 　将来に向けたサイバーセキュリティ確保のため、政府機関をはじめ、重要インフラ事業者、民間事業者などでの対応が円滑に進むよう、政府としても適切に後押しをしていただきたい。	賛同意見として承りました。

127	本案のIII ３．（３）２に関係して、耐量子計算機暗号（PQC）や量子暗号通信（QKD）等の暗号技術において、政府が民間に先んじて活用・導入すべき。	ご意見として承りました 　なお、Ⅲ．３．（３）②「量子技術の進展に伴う対応・取組」でも述べているとおり、「政府機関等における PQC への移行について、原則として、2035 年までに行うことを目指し、政府機関等における暗号技術の利用状況等も踏まえ、関係府省庁の連携の下、2026 年度に工程表（ロードマップ）を策定し、我が国における円滑な移行を推進」してまいります。

	意見の概要	意見に対する考え方（案）
	その他	
128	戦略的サイバー防御などと言って他国・自国のサーバアクセスを正当化している様だが、それは攻撃であり侵害でもある。国内外サーバの監視は思想信条の自由、通信の秘密を侵害するもので、まともな方策とは思えず、削るべき。 やるべきなのは セキュリティホールを作らない為の IT 企業へのプログラム検証の義務付けや、セキュリティアップデートの無償化、ファイアウォールの義務化などである。 　EU による AI 規制法への準拠が必要である。 　また、社会的な犯罪に対しては、SNS での書き込みに ヒューマン・チェック（いわゆる「ロボットではありません」の確認）を義務化して、自動書き込みや社会扇動、不正な広告などを抑止する必要があると思う。	通信情報の利用や、アクセス・無害化措置は、サイバー対処能力強化法等（2025年5月に国会で成立）に基づき、実施するものです。その立法に際しても、過去の関連する経緯等を十分に精査した上、通信の秘密に十分に配慮を行うものとなっており、今般、国会においてご審議をいただいて成立しております。なお、通信情報の利用やアクセス・無害化措置については、独立機関として設置されるサイバー通信情報監理委員会における事前承認や検査等を始めとする、これら関係法の仕組み等によって適正な執行が図られることとなります。また、アクセス・無害化措置は、国際法上許容される範囲内で実施するものであり、こうした点も、本戦略で述べているところです。 　そのほか、本戦略は、官民連携・国際連携の下、幅広い主体による適切な対策の実施を含め、総合的に対策を実施することとしています。
129	この案には、個別の国からの具体的なサイバー攻撃について言及があるが、これだけでは、日本がサイバー攻撃を受けている全体像が見えない。アメリカや西側諸国も攻撃を行なっている可能性への言及がないため、脅威の根拠そのものが信用できる情報源によれていないと考える。 　むしろ、日本政府が取り組むべき基本的な課題は、地政学的な脅威を取り除くような外交努力である。この外交努力についての言及や考察が、この案にはまったくない。	本戦略において記述しているサイバー攻撃の国家的な利用が行われているとみられる事例は、我が国を取り巻く安全保障環境において特に注目すべき国・地域の関与に関するものとしています。また、「外交努力についての言及や考察が、この案にはまったくありません。」との点については、Ⅲ．１．（３）「同盟国・同志国等との情報・運用面での協力の強化」において、「国際的に主導できる能力を構築するとともに、外交面での対応を含め、同盟国・同志国等との間で緊密に連携して推進する。」と述べているところです。
130	反対。国会でとりあげてほしい。	サイバーセキュリティ戦略は、サイバーセキュリティ基本法に基づき政府において策定することとされているものです。なお、閣議決定後は、国会に報告することとされています。
131	国家ゼロトラスト基盤（National Zero Trust Base：NZTB）の整備を提案する。NZTBは、既存のインターネットの上に重ねる「安全通信層」であり、個人認証・暗号通信・経路検証を常時行う仕組みを持つ。通信内容を検閲するのではなく、通信の正当性を証明することで、自由と安全の両立を図ることを目的とする。この構想は、国民の通信を国家が監視するものではなく、攻撃者の匿名性と無責任性を減じるための共通防御層の整備である。	ご意見として承ります。