「サイバーセキュリティ戦略」に基づき、2022年度に実施すべき施策に関する意見募集の結果の概要

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

■ 実施期間：令和３年（2021）年12月24日～令和４年（2022） １月28日（30日間）

■ 意見総数：14者から37件

【意見の種類】

・2022年度に実施すべき施策（サイバーセキュリティ2022）に関する意見：36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）：１件
- ・経済社会の活力の向上及び持続的発展：４件
- ・国民が安全で安心して暮らせるデジタル社会の実現：22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：４件
- ・推進体制：１件

・その他のご意見：１件

2022年度に実施すべき施策に関する意見募集の結果一覧

通しNo	該当箇所	御意見の要旨	御意見に対する主な考え方及び修正
1	総論	技術面・ソフト面・ハード面等の様々な観点から見たセキュリティ対策が重要である。	技術面、ソフト面、ハード面等、あらゆる観点を踏まえたサプライチェーン全体としてのセキュリティ対策が重要であるとのご意見と認識いたしました。ご意見については、サイバーセキュリティ政策を推進するにあたり、今後の参考とさせていただきます。
2	4．1．1　経営層の意識改革	重要インフラ事業者にはペネトレーションテストを義務化すべき。経営課題であることを直視することが可能となり、経営レベルでの対策が進むようになると考える。	重要インフラ事業者がその社会的責務を果たす観点から、経営層の意識改革を含め、組織的対策が実効的に進むよう取組を進める必要性があると認識しております。この認識に基づき、「重要インフラのサイバーセキュリティに係る行動計画（案）」において、組織統治の一部としてサイバーセキュリティを組み入れる方針を具体的に記載しております。ご意見については、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。
3	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	サプライチェーンの信頼性確保におけるサイバーセキュリティ対策のためのフレームワーク活用やガイドラインの策定・活用促進について、管理対象のサプライチェーン企業にフレームワーク等に則ったセキュリティ対策の実行を指示する場合は、対策実施後の監査まで行うスキームが必要と考える。	デジタル経営に向けた行動指針である「デジタルガバナンス・コード」において、DX認定の基準として、「サイバーセキュリティ経営ガイドライン等に基づき対策を行い、セキュリティ監査（内部監査を含む）を行っていること」が示されていると承知しております。ご意見について参考にさせていただき、インセンティブ付けも含めて、企業の取組促進を図ってまいります。
4	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	一定の基準を満たすセキュリティサービスのリスト化の取組について、リスト化するサービスには脆弱性診断サービスも含めるべきと考える。	IPAが実施する「情報セキュリティサービス基準適合サービスリスト」において、「脆弱性診断サービス」のリストも公開されていると承知しております。

2022年度に実施すべき施策に関する意見募集の結果一覧

通しNo	該当箇所	御意見の要旨	御意見に対する主な考え方及び修正
5	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	サプライチェーン全体のセキュリティ対策の必要性に対する認識が高まりつつある中で、積極的に取り組む企業に対する表彰やサプライヤーに対する税制優遇など具体的な施策を進めていただきたい。	DXに取り組む先進的な企業の選定・公表を行う「DX銘柄」の評価基準において、サイバーセキュリティ対策に関する項目が含められているほか、様々な民間団体でもサイバーセキュリティに特化した表彰等が行われていると承知しており、こうした取組を慫慂していくことが重要と考えております。 また、DX投資促進税制の対象となるDX企業認定制度において、サイバーセキュリティ対策についても認定基準に含められていると承知しております。 ご意見については、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。
6	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	国民の多くが利用しているSNSや、国や地方自治体のシステムを安心して利用できるよう、国産のシステムを構築してほしい。	政府機関における適切なセキュリティ水準が確保された信頼できるクラウドの利用促進のため、各政府機関は、クラウドサービスにおいて要機密情報を取り扱う場合は、原則として「ISMAPクラウドサービスリスト」に掲載されたクラウドサービスから調達することとしています。 ISMAPは、国際基準等を踏まえて策定した基準に基づき、各基準が適切に実施されているか監査するプロセスを経て、安全性が評価されたクラウドサービスを登録する制度です。 各政府機関は、ISMAPに登録されたクラウドサービスを基に、当該サービスが組み込まれる情報システムのリスク評価等を適切に実施した上で、ISMAPにおける統一的な基準に加え必要に応じて追加的な要求事項の設定を行い、実際の調達や運用を行っていくこととなります。ご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。
7	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	従来の「自分を守る」サイバーセキュリティから、インターネット全体の安全性を高める手法として、「自律分散型セキュリティ（AIS）基盤」の導入及び展開の提案。	ご意見については、今後の施策の検討や実施の推進に当たって、参考とさせていただきます。
8	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	海外からのインターネットを通じた攻撃に対し、日本国のインターネットを守るため、日本だけを隔離するような仕組みを検討すると共に、必要に応じて定期的な訓練等を検討すべきではないか。	サイバー空間は、場所や時間にとらわれず、国境を越えて、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、流通する場であるところ、こうした特徴を損なうことなく、サイバーセキュリティが確保される必要があると考えております。貴重なご意見として承ります。

2022年度に実施すべき施策に関する意見募集の結果一覧

通しNo	該当箇所	御意見の要旨	御意見に対する主な考え方及び修正
9	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	ネットワーク上の行政警察の活動を積極的かつ各種不正な活動の新たな展開に応じて柔軟に実施可能とし、また治安維持のための組織犯罪活動の情報収集等を明示的に可能とする法令上の基礎付けが必要と考える。	サイバーセキュリティ2022の「2.1(3)(ス)」「3.2(2)(エ)」において、サイバー警察局及びサイバー特別捜査隊を設置し、サイバー空間の安全・安心の向上を図るとしています。ご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。
10	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	SNS等での個人情報、内容の流出・無断使用がないようにあらゆる手段を講じるべき。	我が国のサイバーセキュリティ戦略の基本的な理念である「自由、公正かつ安全なサイバー空間」を確保するため、今後も取り組んでまいります。貴重なご意見として承ります。
11	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	機器、ソフトウェア等のサプライチェーン構成要素における信頼性確保の仕組み構築について、特にインシデントの起因となりやすいエンドポイントの管理においては、リスクスコアを算定する仕組みの導入が有用と考えます。	サイバーセキュリティは、自らの機器・ソフトウェアにおける対策だけで完結するものではなく、サイバー空間を構成する様々な環境・要素が相互に支えあってこそ実現するものです。政府としても、サイバー空間を担う各主体がそれぞれ責任ある対応を果たせるような環境づくりを行うため、様々な施策を進めて参ります。貴重なご意見として承ります。
12	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	安心・安全なクラウドサービス利用環境構築のためのルール策定、対策パッケージ化について、クラウドサービスの設定不備は重大なインシデントにつながりかねないことから、設定のポリシー準拠状況の把握と違反時のリアルタイムでの対応が求められると考えます。	サイバーセキュリティ2022の「1.2(ケ)」において、総務省は、クラウドサービス利用者における設定不備を抑止・防止するための、クラウドサービス利用者、クラウドサービス事業者における実施すべき対策を整理した「クラウドサービス利用・提供における適切な設定のためのガイドライン」を2022年中に公表し、より安全・安心なクラウドサービスの利活用を促進することとしています。ご意見については、本施策の今後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。
13	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	サイバー攻撃への対処を実効たらしめる諸施策について、諸施策を検討する際には施策同士の関連を考慮し、特に導入する対策製品に関しては一貫して管理することが有用だと考えます。 サイバー攻撃が多様化するにつれ、単一の対策製品では防ぐことが難しく、またインシデント発生時の原因究明も困難になっています。	サイバーセキュリティにおいては、「セキュリティ・バイ・デザイン」の考え方が重要であり、施策全体を貫く方向性の一つとして、「デジタル改革を踏まえたデジタルトランスフォーメーションとサイバーセキュリティの同時推進」を掲げております。貴重なご意見として参考とさせていただきます。

2022年度に実施すべき施策に関する意見募集の結果一覧

通しNo	該当箇所	御意見の要旨	御意見に対する主な考え方及び修正
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	海事に係るサイバーセキュリティ確保に資する具体的な施策を構築し、同分野において世界をリードして強化することを提案する。 海事に係る基本的なセキュリティガイドラインの策定、自律運航も見据えたICT技術を活用するにあたっての船舶で必要となるセキュリティ技術の研究(研究テーマ例：セキュリティテストの実証実験、セキュリティ監視等)、セキュリティ人材育成を支援するプログラムを準備するなど、海事に係るサイバーセキュリティの確保に資する具体的な施策を構築されることが望ましいと考える。	海運業は重要インフラ分野の「物流」に含まれており、「重要インフラのサイバーセキュリティに係る行動計画（案）」に基づき、障害対応体制の強化、安全基準等の整備及び浸透、情報共有体制の強化、リスクマネジメントの活用、防護基盤の強化の5つの取組を実施する等、様々な施策を推進しております。貴重なご意見として承ります。
15	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	ランサム攻撃対策として被害を受けた企業等が対応等について相談可能な態勢を整備することを提案する。捜査機関と連携しつつ、脅迫者との交渉を担ったり、データを暗号化されたのであればその解決を図ったり、また、サイバー保険と組み合わせることで、国民の生命や財産に係るよう事案が発生しても被害を極小する策を講じることも一つの方法ではないかと考える。	サイバーセキュリティ2022の「2.1(3)(コ)」において記載される、警察庁及び都道府県警察における様々な取組のほか、関係省庁において国民に寄り添った様々な取組を行っており、貴重なご意見として承り、施策の参考とさせていただきます。
16	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	サイバー空間におけるあらゆる本人認証において、多要素認証の実現を「国民・社会を守るためのサイバーセキュリティ環境提案」に盛り込むべきである。	多要素認証の重要性は様々に指摘をされ、各方面で導入も進んでいると認識しており、政府においても積極的に周知啓発を図っております。貴重なご意見として承り、サイバーセキュリティ政策を推進するにあたり、今後の参考とさせていただきます。

2022年度に実施すべき施策に関する意見募集の結果一覧

通しNo	該当箇所	御意見の要旨	御意見に対する主な考え方及び修正
17	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	民間の業者には徹底した情報管理と情報漏れ等の際には公共事業からの排除、刑事訴追等含めたペナルティが必要。また職員にも同様にペナルティが必要。	我が国が理念とするサイバー空間の基本原則は、「情報の自由な流通の確保」「法の支配」「開放性」「自律性」「多様な主体の連携」であり、貴重なご意見として承り、施策を進めて参ります。
18	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）	SNSやクラウドサービス及びサーバの国内管理を提供する国内企業の創設や、政府や行政機関が使用するシステム全般は、政府が責任をもって監視し、実現する道筋を作ってほしい。	No.6参照
19	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）	スパイ防止法と厳格な罰則の制定等のサイバーセキュリティ環境を守る法整備をお願いしたい。	サイバーセキュリティの確保において、情報の格付け、取扱制限の決定・明示、そしてサイバーセキュリティ組織・体制の確立は重要であり、防護対象（システム・情報等）の重要性に応じて、必要なセキュリティ対策を講じる必要があると認識しております。ご意見については、今後の施策の検討や実施に当たって、参考とさせていただきます。
20	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）	サイバー空間内の本人認証において、日本政府は米国政府に倣い、多要素認証の義務付け、及びWebAuthn/FIDO2規格の採用を呼びかけるべきである。	No.16参照
21	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）	半導体、各種機器、インフラ設備の生産、管理及び研究開発は日本人で構成されるべきであり、また諸外国を含めた政府・行政・教育機関・企業間の情報共有システムについては、同盟国・同志国等と強固な共有ができるような方針や対応をすべきと考える。	サイバーセキュリティを確保するためには、情報システムのライフサイクル全般を通じて様々な対策を行う必要があり、研究開発や製造段階におけるセキュリティの確保も重要と考えております。貴重なご意見として承ります。

2022年度に実施すべき施策に関する意見募集の結果一覧

通しNo	該当箇所	御意見の要旨	御意見に対する主な考え方及び修正
22	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）	総務省によるIOT機器調査及び利用者への注意喚起（novice等）が実施されているが、各業界団体に対して業界各社の脆弱性情報を収集し、対策を促す様な仕組みを導入し、業界全体のセキュリティ対策を高める事を検討してはどうか。	サイバーセキュリティ2022の「2.1(1)(ス)」において、経済産業省告示に基づき、IPA（受付機関）とJPCERT/CC（調整機関）により運用されている脆弱性情報公表に係る制度を着実に実施するとともに、必要に応じ、「情報システム等の脆弱性情報の取扱いに関する研究会」での検討を踏まえた運用改善を図ることとしています。また、関係者との連携を図りつつ、「JVN」をはじめ、「JVNiPedia」（脆弱性対策情報データベース）や「MyJVN」（脆弱性対策情報共有フレームワーク）などを通じて、脆弱性関連情報をより確実に利用者に提供し、さらに、能動的な脆弱性の検出とその調整に関わる取組を行い、また、海外の調整機関や研究者とも連携し、国外で発見された脆弱性について、国内開発者との調整、啓発活動をJPCERT/CCにおいて実施することとしおります。ご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。
23	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）	経済安全保障推進法で検討されているところだが、スパイウェアを組み込まれるなどの調達リスクへの対応として、取引禁止先となっている主要国のリストを収集し、一般社団法人安全保障貿易センター等に委託して情報を取りまとめてリスト形式で公開しておく事で、日本企業が取引禁止先の製品の利用可否を判断しやすくするような事を検討してはどうか。	ご指摘のような各国の施策については、独立行政法人日本貿易振興機構（JETRO）でもわかりやすくウェブで情報発信する等、関係機関で様々な取組を進めているところであり、貴重なご意見として承ります。
24	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）	金融分野のオンライン化の進展等に伴い、年々複雑化・高度化するマネーロンダリング・テロ資金供与に繋がる不正送金、フィッシング詐欺等の金融犯罪に対抗するために、サイバーセキュリティ対策の強化が急務となっている。 サイバーセキュリティを確保しつつ、デジタル改革を推進していくためには、マイナンバーカードを利用した厳格な本人確認のもと、金融機関のログイン、登録口座等の重要情報の変更申請、一定金額以上の資金移動等に対応することを推進する。	政府としては、データの安全・安心な利活用の観点から、マイナポータルやマイナンバーカードの活用を推進して参ります。貴重なご意見として承ります。

2022年度に実施すべき施策に関する意見募集の結果一覧

通しNo	該当箇所	御意見の要旨	御意見に対する主な考え方及び修正
25	4．2．5　経済社会基盤を支える各主体における取組③（大学・教育研究機関等）	SINETのインターネットへの接続に大規模なゲートウエイを設置し、不正な通信を監視し、遮断し、またSINET内から出て行く通信についても必要な遮断を行えるような仕組みを導入し、またSINETの構築、運用及びセキュリティを担う専門機関を設置するなどして、体制強化も図るべきであると考える。	サイバーセキュリティ2022の「2.5(ウ)」より、国立情報学研究所（NII）において、引き続き国立大学法人等のインシデント対応体制を高度化するための支援（サイバー攻撃情報分析の機能追加を行いながら、引き続き情報提供を行うとともに、サイバーセキュリティに関する情報セキュリティ担当者向け・戦略マネジメント層向けの研修を行うことで、大学自体でインシデント対応が可能になる能力を身につける支援）を行うこととしております。 また、サイバーセキュリティ2022の「2.5(カ)」より、文部科学省において、文部科学省サイバーセキュリティ緊急対応支援チーム（M-CYMAT）の機能を引き続き強化し、サイバーセキュリティインシデント発生時における支援を行うこととしております。ご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。
26	4．2．7　大規模サイバー攻撃事態等への対処態勢の強化	サイバー攻撃に対し、防御のみならず、反撃並びに攻撃者に対して攻撃を無力化できるよう、法整備を進めてほしい。	サイバー攻撃に対しては、必要に応じて、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、様々な手段と能力を活用する必要があると認識しております。貴重なご意見として承ります。
27	4．2．7　大規模サイバー攻撃事態等への対処態勢の強化	緊張関係にある世界の中で国家（経済・軍事）安全保障面から大規模サイバー攻撃の拡大防止の注意喚起発信の体制構築と継続実行の施策を立ち上げていただきたい。主体はNISCで、注意喚起作成はIPAが実施し、公開発信はNISCのホームページが良いと考える。	例えば、NISCウェブサイトでは、「ストップ！ランサムウェア」としてランサムウェア特設ページを開設し、関係省庁の取組をまとめて情報発信しています。引き続きこのような取組を進めてい参ります。貴重なご意見として承ります。 https://security-portal.nisc.go.jp/stopransomware/
28	4．3．1「自由、公正かつ安全なサイバー空間」の確保	サイバー攻撃やその前兆となる活動への対抗措置や事前情報収集等の措置について、一定の範囲の者は正当化されるよう立法措置を講じることが必要と考える。特に電気通信事業法や有線電気通信法の通信の秘密侵害について、広範囲に必要な措置がとれるように明確に法律で正当化すべきと考える。	サイバーセキュリティ戦略の4.2.1(1)③では「利用者が安心して通信サービスを利用してサイバー空間において活動できるようにする観点から、必要に応じて関係法令に関する整理を行いながら、安全かつ信頼性の高い通信ネットワークを確保するための方策を検討する。」こととしております。いただいたご意見については、今後の施策の検討や実施の推進に当たって、参考とさせていただきます。

2022年度に実施すべき施策に関する意見募集の結果一覧

通しNo	該当箇所	御意見の要旨	御意見に対する主な考え方及び修正
29	4．3．2　我が国の防御力・抑止力・状況把握力の強化	北朝鮮による電磁波攻撃やテンペストによる情報漏洩を防御するため、重要インフラの一部企業やクラウド事業者の一部のサービスに対して、傍受されないような対策を求める事が重要ではないか。	事業者はそれぞれ、自らが提供する事業の重要性に鑑み、様々なリスクを念頭にリスクアセスメントを行い、必要な対策を予め行っていく必要があると考えております。重要インフラについては、「重要インフラのサイバーセキュリティに係る行動計画（案）」に基づき、障害対応体制の強化、安全基準等の整備及び浸透、情報共有体制の強化、リスクマネジメントの活用、防護基盤の強化の５つの取組を実施することとしております。また、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べく、必要となる新たな技術開発を推進することとしております。ご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。
30	4．3．2　我が国の防御力・抑止力・状況把握力の強化	安全保障上の機密データを守るためにも、セキュリティクリアランスの仕組み以前に、国籍を正確に把握するなどの対応が必要と考えられる。	ご意見については、今後の施策の検討や実施の推進に当たって、参考とさせていただきます。
31	4．3．3　国際協力・連携	安心できる自由主義国の情報機関と緊密に連携し、安心できるシステム構築をしてほしい。	同盟国・同志国との緊密な連携は重要と認識しており、「自由、公正かつ安全なサイバー空間」を確保すべく、ご意見を踏まえ、引き続き取り組んでまいります。
32	4．4．2　人材の確保、育成、活躍促進	若年層だけでなく、シニア層についても、人材の育成・登用を進めてほしい。	サイバーセキュリティ分野における人材の確保、育成、活躍促進に向けて、対象を若年層に限らない各種取組を掲載しております。ご意見については、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。
33	4．4．2　人材の確保、育成、活躍促進	不登校児やひきこもりの人達の活用の検討をお願いしたい。	サイバーセキュリティ分野における人材の確保、育成、活躍促進に向けて、学歴等によらない多様な視点や優れた発想を取り入れることが重要と考えており、対象を学歴等で限定しない様々な人材育成施策を掲載しております。ご意見については、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。
34	4．4．2　人材の確保、育成、活躍促進	セキュリティクリアランスを行い、安心できる人材の活用と育成をしてほしい。	No.30参照

2022年度に実施すべき施策に関する意見募集の結果一覧

通しNo	該当箇所	御意見の要旨	御意見に対する主な考え方及び修正
35	4．4．2　人材の確保、育成、活躍促進	報酬に限度を設けず、公務員特別枠で優秀な人材を直接雇用すべき。	サイバーセキュリティ2022の「4.2(3)(イ)」において、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。具体的には、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、研修や演習の実施と並んで、適切な処遇の確保を進めております。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。
36	5．推進体制	我が国の防衛費は、GDP1%という枠がはめられているが、サイバー防衛力強化に使われる予算は、全く別枠として潤沢な予算を確保すべき。	サイバーセキュリティ政策の推進にあたっては、政府が毎年策定しているサイバーセキュリティ関係施策に関する予算重点化方針に沿って必要な予算の確保と執行を図っております。ご意見については、こうした方針を推進するにあたり、今後の参考とさせていただきます。
37	－	コロナ禍において、ワクチンに関するネガティブ情報等が削除されている状況は、極めて憂慮すべき。この様な言論統制はやってはならないし、自由を侵すこの様な行為は禁止すべき。	本意見募集と直接関係ないと考えられます。なお、政府としてご指摘のような事実は把握しておりませんが、サイバー空間の公共空間化が進展する状況において、言論の自由を守りつつ、我が国のサイバーセキュリティ戦略の基本的な理念である「自由、公正かつ安全なサイバー空間」の実現を図っていくことが重要と考えています。貴重なご意見として承ります。