「サイバーセキュリティ戦略」に基づき、2020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２年（2020年）１月30日（木）～２月28日（金）

■ 意見総数：13者から26件【７企業・団体から延べ17件、６個人から延べ９件】

【意見の種類】

・2020年度に実施すべき施策（サイバーセキュリティ2020）に関する意見：25件

- ・経済社会の活力の向上及び持続的発展：９件
- ・国民が安全で安心して暮らせる社会の実現：９件
- ・国際社会の平和・安定及び我が国の安全保障への寄与：１件
- ・横断的施策：６件
- ・推進体制：０件

・その他の意見：１件

■ （参考）提出者名：

一般社団法人コンピュータソフトウェア協会セキュリティ委員会、日本ヒューレット・パッカード株式会社、株式会社クロイツ、サウスプルーム株式会社、ヤフー株式会社、情報セキュリティ教育事業者連絡会(ISEPA)、日本ネットワークセキュリティ協会事業コンプライアンス部会、個人（６人）

2020年度に実施すべき施策に関する意見募集の結果一覧

通しNo	提出者	該当箇所	意見の要旨	主な考え方
1	一般社団法人コンピュータソフトウェア協会　セキュリティ委員会	4．1．1　新たな価値創出を支えるサイバーセキュリティの推進	セキュアコーディングの重要性の啓発、ISACでの情報連携および各プログラミング言語のセキュアコーディングガイドの整備が必要。	先端技術を利活用したイノベーションを支えるサイバーセキュリティに関する賛同意見として承りました。内容については、今後の施策の検討や実施の推進に当たって参考とさせていただきます。
2	個人（2）	4．1．1　新たな価値創出を支えるサイバーセキュリティの推進	サイバーセキュリティー対策における政策の提案＿1 「サイバーセキュリティー対策」が重要な構造と、私し個人は思います。 例えばですが、「センサー技術、ネットワーク技術、デバイス技術」から成る「CPS（サイバーフィジカルシステム）」の導入により、「ゼネコン（土木及び建築）、船舶、鉄道、航空機、自動車、産業機器、家電」等が融合される構造と、私は考えます。	先端技術を利活用したイノベーションを支えるサイバーセキュリティ対策の推進に関する賛同意見として承りました。内容については、今後の施策の検討や実施の推進に当たって参考とさせていただきます。
3	個人（2）	4．1．1　新たな価値創出を支えるサイバーセキュリティの推進	サイバーセキュリティー対策における政策の提案＿2 具体的には、「情報技術（IT）」及び「人工知能（AI）」での「回線（サーキット）」の事例、「サイバー空間（情報空間）」及び「フィジカル空間（物理空間）」での「回線（サーキット）」の事例が有ります。	先端技術を利活用したイノベーションを支えるサイバーセキュリティ対策の推進に関する賛同意見として承りました。内容については、今後の施策の検討や実施の推進に当たって参考とさせていただきます。
4	日本ヒューレット・パッカード株式会社	4．1．1　新たな価値創出を支えるサイバーセキュリティの推進	ユーザー識別（本人確認）や認証、認可、アクセス制御といったセキュリティ機能において、FIDO認証などの新しい標準化技術の活用を選択肢の一つとして考慮すべき	先端技術を利活用したイノベーションを支えるサイバーセキュリティに関する賛同意見として承りました。内容については、今後の施策の検討や実施の推進に当たって参考とさせていただきます。
5	一般社団法人コンピュータソフトウェア協会　セキュリティ委員会	4．1．2　多様なつながりから価値を生み出すサプライチェーンの実現	ソフトウェアで利用しているOSSが不明確であるといったサプライチェーン・リスクに対処するため、SBOMが作成できるシステムを安価に利用できるようなシステムの構築を望みます。	「サイバー・フィジカル・セキュリティ対策フレームワーク」に基づくセキュリティ対策の具体化・実装を推進するため設置されたタスクフォース（TF）のひとつ「ソフトウェアTF」において、ソフトウェア管理手法、脆弱性対応、OSS利活用等について検討しております。年次計画においても、ご指摘のOSSの活用に係るリスクを含めて適正なソフトウェア管理手法の在り方について検討を進めることとしています。
6	一般社団法人コンピュータソフトウェア協会　セキュリティ委員会	4．1．2　多様なつながりから価値を生み出すサプライチェーンの実現	中小企業へのPSIRT構築の支援およびソフトウェアの発注者にも開発におけるPSIRTの必要性を理解いただく啓発活動が必要。	サイバーセキュリティ戦略の中小企業の取組の推進に当たっての賛同意見として承りました。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。
7	株式会社クロイツ	4．1．2　多様なつながりから価値を生み出すサプライチェーンの実現	資金力の無い中小企業でも有効な対策を行うことが出来るようにもっと簡単に助成金、補助金が使えるようにしてほしい。また、現状のサイバー攻撃は対策ソフトだけで防ぐ事が難しく組織のルールや環境づくり、スタッフ研修と言った基礎的な事が重要です。そちらにも重点を置いた助成をした方が良い。	サイバーセキュリティ戦略における中小企業の取組の推進に当たっての賛同意見として承りました。 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、年次計画に基づき引き続き中小企業の取組を推進してまいります。
8	個人（6）	4．1．2　多様なつながりから価値を生み出すサプライチェーンの実現	中小企業のサーバやネットワークがほんとうにセキュリティ対策をしているのかの技術的調査と支援をすべき	サイバーセキュリティ戦略における中小企業の取組の推進に当たっての賛同意見として承りました。 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、年次計画に基づき引き続き中小企業の取組を推進してまいります。

2020年度に実施すべき施策に関する意見募集の結果一覧

通しNo	提出者	該当箇所	意見の要旨	主な考え方
9	日本ヒューレット・パッカード株式会社	4．1．3　安全なIoTシステムの構築	安全なIoTシステム構築のためには多層的な観点での防御が必要と考えております。既にIoTシステムに関するサイバーセキュリティはIoT推進コンソーシアムにより「IoTセキュリティガイドライン」として公開されていると理解しております。今後はこれらの対策に加え、AIを用いたIoTデバイス属性の特定や不正端末の識別、防御といった観点も重要となる	ご指摘の通り、サイバーセキュリティへのAIの活用は重要な観点であると考えます。いただいた御意見は今後の検討の参考とさせていただきます。
10	サウスプルーム株式会社	4．2．1　国民・社会を守るための取組	クラウドのような外部組織でのデータ管理が中心の現在では、サーバそのものがハッキングされれば、企業、団体及び個人がセキュリティ対策を行ったとしても、他と通信する過程で全てのデータが抜き取られてしまう。 政府若しくは政府の関連団体がハッキングされている事実を掌握した上で、該当企業、団体への指導警告を徹底し、対策を取らせ、少しでも被害を縮小する方向に舵をとらなければならない。	我が国のサイバーセキュリティの確保に当たっては、サイバー攻撃対策が重要と考えております。 これまでもサイバー攻撃の被害を受けていることを把握した場合には、JPCERT/CCに情報提供し、JPCERT/CCを通じて被害を受けた組織・機関等に対して情報提供・注意喚起を行ってきておりますが、ご指摘についても今後のこうした取組に際して参考とさせていただきます。
11	日本ヒューレット・パッカード株式会社	4．2．1　国民・社会を守るための取組	政府機関の情報システムや国民向けサービスにおける認証機能の実装において、標準化技術であるFIDO認証を一つの選択肢として考慮すべきである。	多様な認証方式があると認識しているところ、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。
12	日本ヒューレット・パッカード株式会社	4．2．1　国民・社会を守るための取組	各企業・団体に対し、「サイバーセキュリティ保険」の必要性・緊急性の更なる啓発と普及が必要である	ご指摘のとおり、サイバーセキュリティ保険の利用拡大に向けた更なる啓発と普及が重要と考えており、年次計画においては、サイバーセキュリティお助け隊の取組や、Security　Action制度との連携により、サイバーセキュリティ保険の活用や普及・啓発に向けた取組を進めることとしています。いただいたご意見は今後の取組の参考とさせていただきます。
13	サウスプルーム株式会社	4．2．2　官民一体となった重要インフラの防護	政府機関等からガイドラインの発行ができれば、ハッキングに対応する企業も増え、状況が改善することが考えられる。 公的な組織・団体が、ハッキングを受けたサーバの情報を入手し、被害サーバの管理企業や団体等に通知ないし指導できれば、被害サーバの管理企業や団体はその事実に向き合い対策しなければならなくなるだろう。 日本国内で年間5万台以上のサーバがハッキングされ、管理者権限を奪われていて、ほとんどがその事実に気づいていないことから、様々な情報が流出し国としても大きな損失を出しているという点にどのように対策するか検討していただくことが重要である。	我が国のサイバーセキュリティの確保に当たっては、それぞれの組織・機関が主体的にセキュリティ対策に取り組むことが重要であると考えております。 NISCとしては、これまでもこうした取組を支援すべく、様々な取組を行っていますが、ご指摘についても今後の施策を検討・実施する際に参考とさせていただきます。
14	ヤフー株式会社	4．2．2　官民一体となった重要インフラの防護	セキュリティクリアランス制度が無い状況が、官民連携と国際連携の両面において足枷になる恐れがあるため、セキュリティクリアランス制度の早期創設の検討を望む	頂いた御意見については、今後のサイバーセキュリティ政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。

2020年度に実施すべき施策に関する意見募集の結果一覧

通しNo	提出者	該当箇所	意見の要旨	主な考え方
15	個人（4）	4．2．3　政府機関等におけるセキュリティ強化・充実	省庁および地方公共団体から発注・委託する場合において委託先に求めるべき情報のセキュリティ基準を欧米NIST SP800-171等にならい強化することを提案するとともに、日本の組織では、最高情報責任者等「組織の上級職員」が依然として不在および極度に不足している状況であることから、人材の育成とそのスキル認定、およびその必要性の理解が急務である。	省庁に関しては、政府機関等の情報セキュリティ対策のための統一基準群（平成30年度）においては、政府機関の外部委託に係る規定を載せており、外部委託先における情報セキュリティ対策の実施を求めております。引き続き、この取組を推進していきます。 また、地方公共団体に関しては、「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」において、外部委託先における情報セキュリティ対策の実施等を求めています。 御意見については、このような施策の検討や実施の推進に当たって参考にさせていただきます。
16	サウスプルーム株式会社	4．2．3　政府機関等におけるセキュリティ強化・充実	日本で情報流出が無差別に発生している現実を踏まえて、公共及び主要インフラのセキュリティ状況を正確に把握し、PDCAのサイクルを実施することをお願いします。	政府機関においては、最新のサイバーセキュリティ状況を政府統一基準群に反映し、これに基づいた各機関の情報セキュリティ監査の他、サイバーセキュリティ本部による監査により、セキュリティ状況を把握し、その結果に応じた、セキュリティ対策の改善を実施しています。 また、情報通信、電力、金融等14分野の重要インフラについては、サイバーセキュリティ対策に関する「行動計画」を策定し、安全基準の指針の整備、官民での情報共有の促進、演習による対処能力の向上等の取組を実施しています。 引き続き、関係機関が密接に連携し、サイバーセキュリティを確保できるよう、これらの取組を進めてまいります。
17	個人（5）	4．2．4　大学等における安全・安心な教育・研究環境の確保	私立大学についても，国立大学と同様に，情報セキュリティの計画（ロードマップ）や進捗状況／実施状況を文科省に報告させる仕組みを導入するべきと考える。	ご指摘の箇所については、元文科高第59号『大学等におけるサイバーセキュリティ対策等の強化について（通知）』（令和元年5月24日付）において、私立を含めた大学等に対し「サイバーセキュリティ対策等基本計画」の策定を求めており、フォローアップを行う上での参考とさせていただきます。
18	サウスプルーム株式会社	4．2．6　従来の枠を超えた情報共有・連携体制の構築	中国ブラックマーケットのハッカー達に好きなようにハッキングされている現状を脱却するためには、中国ブラックマーケットのリアルタイムな情報を入手し、その情報を即時分析し、対策する必要がある。	我が国のサイバーセキュリティの確保に当たっては、ご指摘のように様々な情報を収集し、必要に応じて民間とも情報共有することが重要と考えております。 これまでもこうした観点から様々な取組みを行ってきていますが、ご指摘についても今後の施策の検討や実施に当たっての参考とさせていただきます。
19	サウスプルーム株式会社	4．3．2　我が国の防御力・抑止力・状況把握力の強化	政府機関主導でホワイトハッカーの育成及び採用を精励し、また検証の現場にそのホワイトハッカーを人員として配置し、攻撃の再現、ハッカー目線の見識から分析し対策を講じる必要があります。	サイバーセキュリティ戦略において、突出した能力を有しグローバルに活躍できる人材の発掘・育成・確保も引き続き行っていく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。

2020年度に実施すべき施策に関する意見募集の結果一覧

通しNo	提出者	該当箇所	意見の要旨	主な考え方
20	個人（1）	4．4．1　人材育成・確保	公的な職場においては、セキュリティチームも当然必要だが、その基盤となる人材も育てるべきではないか。そのためにも、公務員の採用方法に関して現場が必要だと感じる人材を雇用するための制度や、人材を育成するための職場環境が必要ではないか。	サイバーセキュリティ戦略における人材育成・確保の推進に当たっての賛同意見として承りました。同戦略においては、産学官が連携して人材の需要や人材育成施策に関する情報共有等の連携を図りつつ、人材育成・確保を強化するとともに、人材の多様性の確保を推進していくことが重要としております。 政府機関においても、常勤・非常勤を問わず、様々な方法により即戦力の高度専門人材の確保に取り組んでいるほか、部内育成の専門人材の確保・育成に向け、有為な人材の確保や研修等に積極的に取り組んでいるところであり、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。
21	個人（3）	4．4．1　人材育成・確保	ITの質を向上させるためにも、良い人材をこちらの意思で正職員として雇える様制度を整えて頂きたい。	サイバーセキュリティ戦略における人材育成・確保の推進に当たっての賛同意見として承りました。同戦略においては、産学官が連携して人材の需要や人材育成施策に関する情報共有等の連携を図りつつ、人材育成・確保を強化するとともに、人材の多様性の確保を推進していくことが重要としております。御意見については、今後の取組の検討や実施の推進に当たっての参考とさせていただきます。
22	情報セキュリティ教育事業者連絡会(ISEPA)	4．4．1　人材育成・確保	「セキュリティ業務の整理」と「人材のセキュリティスキル見える化」による実効性のある政策実行を望みます。	サイバーセキュリティ戦略において、産学官が連携して人材の需要や人材育成施策に関する情報共有等の連携を図りつつ、人材育成・確保を強化するとともに、人材の多様性の確保を推進していくことが重要としております。ご指摘いただいた点も踏まえ、年次計画においては、特に、産業サイバーセキュリティ研究会WG2において、御指摘の「セキュリティ業務の整理」と「人材のセキュリティスキル見える化」をITSS＋（セキュリティ領域）の改定等により進めることとしています。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。
23	日本ネットワークセキュリティ協会事業コンプライアンス部会	4．4．1　人材育成・確保	法令に抵触しないよう過度に意識するあまり、競争力が海外に比べて劣っている懸念もあり、こうした委縮効果が生じないような環境整備を求める。	NISCにおいては、事業者が適切にサイバーセキュリティ対策を講じる上で、不正アクセス禁止法を含め参照すべき関係法令をQ&A方式で解説する「サイバーセキュリティ関係法令Q&Aハンドブック」を作成し、NISCウェブサイトで公表（※）するなど環境整備を図ったところです。 （※）https://www.nisc.go.jp/security-site/files/law_handbook.pdf
24	個人（2）	4．4．2　研究開発の推進	「サイバーセキュリティー対策」における構造では、「科学技術（サイエンステクノロジー）」の「詳細（ディタイル）」を明確に導入する事が望ましい。	先端技術を利活用したイノベーションを支えるサイバーセキュリティ対策の推進に関する賛同意見として承りました。内容については、今後の施策の検討や実施の推進に当たって参考とさせていただきます。
25	日本ヒューレット・パッカード株式会社	4．4．2　研究開発の推進	市場にはすでにNIST SP800-193に準拠したICT機器などが販売されている状況にあります。すでに利用可能状態にある技術をどう利活用していくかという次のフェーズを本格検討すべき時期に来ており、「研究・技術開発」のみならず「実用化、利活用」を念頭に置いた施策をご検討いただくのが相当である	サイバーセキュリティ研究・技術開発取組方針において、社会実装までのプロセスを念頭に置きつつ取組を進めることが重要としております。御意見については、今後の取組の検討や実施の推進に当たっての参考とさせていただきます。

2020年度に実施すべき施策に関する意見募集の結果一覧

通しNo	提出者	該当箇所	意見の要旨	主な考え方
26	個人（2）	－	・社会構造が古い為に新しく改革し向上による概略案 ・教育内容の改正による具体案 ・女性社会進出での改正による具体案 ・外国人 高度人材での導入で社会水準の向上 による具体案 ・「ガバナンス（政治統治）」構造の改正による具体案 ・生活水準 で の基準 による詳細案 ・官公庁が考案した無駄な政策の廃止による詳細案	本意見募集と直接関係ないと考えられますが、ご意見として承ります。