「サイバーセキュリティ戦略(案)」に対する意見募集の結果の概要

■ 実 施 方 法: NISCのWebページ及び電子政府の総合窓口(e-Gov)に掲載して公募を実施

■ 実 施 期 間: 2015年5月25日(月)～6月8日(月)

■ 意 見 総 数: 27者から83件

意見提出者の内訳 27者(個人:11、企業・団体:16)

83件(個人:30件、企業・団体:53件)

意見内容の内訳

・全体に係る意見:21件

・経済社会の活力の向上及び持続的発展に係る意見:25件

・国民が安全で安心して暮らせる社会の実現に係る意見:23件

・国際社会の平和・安定及び我が国の安全保障に係る意見:4件

・研究開発、人材育成・確保等に係る意見:10件

※日本年金機構の個人情報流出事案に係る意見は3件

＜参考＞

提出者名:(株)アズジェント、アーバーネットワークス(株)、NPO法人市民オンブズマン・ネットワーク行政、(一社)新経済連盟、ソフトバンクモバイル(株)、トレンドマイクロ(株)、日本オラクル(株)、NPO法人日本セキュリティ監査協会、(一社)日本電気制御機器工業会、NPO法人日本ネットワークセキュリティ協会、日本ユニシス(株)、Virtual Engineering Community、BSA | ザ・ソフトウェア・アライアンス、ファイア・アイ(株)、(株)MESSA、メリルリンチ日本証券(株)、個人(11)

「サイバーセキュリティ戦略（案）」に係る意見募集の結果一覧

27者　　83件

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
1	－	（株）アズジェント	5.2.3（1）ii. 被害の発生・拡大の防止	22	【意見内容】 ・訓練・演習に対する具体的な目標を如何に定めるか等の検討について記載してはどうか。 ・事態の早期把握のために、監視と監査を分離するのではなく、高い技術的調査も従来のセキュリティ監査に盛込むことを記載してはどうか 【理由】 政府や企業においては、ゲートウェイ・セキュリティ・ディバイス（FireWall、IDS/IPS、SandBOX 他）などを利用しSOCで監視を行っているが、これらのディフェンス・ラインで100%の防御は不可能であることは、世界的に周知の事実となっている。 侵入されてから被害が発見されるまで米国でも平均7か月というリサーチ結果にあるように、現状の焦点は発見・対策完了までの期間を短縮（潜伏期間中の早期発見）し、被害を最小限に抑えるフェール・セーフを如何に高い精度で、効率良く施せるかにある。 よって、ディフェンス・ラインの防御率を上げることは勿論であるが、侵入されてしまった後のフェール・セーフの仕組み作りを早急に進めることをガイドラインに組み込むべきである。	本戦略は、今後3年程度の基本的な施策の方向性を示すものであり、御指摘の内容については、今後の施策の実施に当たっての参考とします。 なお、5.2.3(1)に記載のとおり、本戦略においては「全ての政府機関等において、攻撃に直面することを前提とした多層的な対策を講ずる」旨を掲げており、御意見のように侵入されてしまった後のことも想定した対策についても推進して参ります。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
2	－	アーバーネットワークス（株）	5.2.2 重要インフラを守るための取組 5.2.3 政府機関を守る	18-23	重要な国家インフラは、例えば、金融、航空、鉄道、電力、ガス、水道などだけでなく、政府機関はすべて、攻撃者のターゲットになる可能性が高い。経験と統計では、DDoS攻撃やAPT攻撃は共に最も一般的な攻撃であることが示されている。 従って、日本政府は、さまざまな産業がサイバーの世界でさまざまな種類の攻撃から自分自身を守るための勧告を提唱する必要がある。 組織は、ビジネスの継続性、運用手順、災害復旧に対して、独自の要件を考慮し、そこに主要な構成要素としてのDDoS防御を含める必要がある。異なるDDoS防御の組み合わせは、Webプレゼンスにとって重要であり、組織のために必要である。同時に、それは、組織内に必要なベストプラクティス（最善の措置）を開発することでもある。 攻撃者らは非常に狡猾であるため、ここ数年では、攻撃の特定カテゴリとして、多くのAPT（Advanced Persistent Threat）攻撃と呼ばれる新しいタイプの攻撃が一般的になっている。 残念ながら、今日の企業は、予防セキュリティメカニズムに過度に依存している。予防措置が違反を検出する唯一の方法であってはならない。いわゆるサンドボックス機能を備えた違反検出システムは、多くの場合、完全なネットワークや組織が識別できるようなコンテキストデータ、完全な範囲を提供したり、問題となる攻撃も優先しない。また、それらは、ネットワーク全体からIOC	御指摘の内容については、政府機関、重要インフラ、企業等における今後の施策の検討に当たっての参考とします。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
			ための取組		（侵害指標）を相関分析したり、より高度な隠密攻撃に迅速に対応するために必要なネットワーク機能を提供していない。 重要インフラ組織は、内部へのAPT攻撃に対処するためのセキュリティ分析のアプローチを採用する必要がある。 セキュリティ分析の目標は、組織内のネットワークセグメントからすべての重要なトラフィックをキャプチャし、分析を完了することである。それは、フルパケットデータ解析を行うために設計されたビッグデータソリューションである。 我々は、さまざまな当事者がマルウェアやその他の高度な脅威の識別および無力化のために共同作業を行うことができ、日本国内のさまざまな組織から信頼できるセキュリティ専門家のプライベートソーシャルネットワークを構築することをお勧めする。これは、セキュリティ担当が効果的に、多くの場合、伝統的なセキュリティ防御では検出されない複雑な隠密攻撃に対抗するための実用的な情報を共有する場合に非常に有効である。	
3	－	NPO法人市民オンブズマン・ネットワーク行政	全般	－	【意見内容】 機密保護は国家として火急に絶対安全を完成させなければならない。 【理由】 同封のセキュリティを考え特許を取得した者は、イタリア人であるが、ガリレイガリレオの再来と云われる天才である。このソフトを破るには25億年かかると言われるものである。是非検討されることを進言します。 そして採用される事を希望します。国民のためです。これでセキュリティは万全です。	御指摘の内容については、今後の施策の検討に当たっての参考とします。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
4	－	（一社）新経済連盟	全般	－	情報セキュリティの意識向上が必要不可欠であり、そのために必要な官民の取り組みを提言として政府に提出している。今回の戦略案に記述として反映いただくとともに、施策の実行の参考にぜひしていただきたい。 http://jane.or.jp/topic/detail?topic_id=394 （提言概要） ・関係有識者のヒアリングの結果まとめ ・セキュリティに関するグローバル調査の解析結果を踏まえ、日本企業とグローバルでの意識の格差等を提示 ・以下具体的な政策提案項目 ①企業ボードメンバーによるセキュリティ対策に対する意識を向上し、当該対策に必要な経営資源を振り向けるようにする。 ②IT分野全般及びセキュリティに関する幅広い知見・技術と倫理観を持ったセキュリティ人材の養成と地位向上 ③企業や業種を超えたセキュリティ担当者間の情報共有の充実強化 ④社員へのセキュリティ教育を徹底するほか、一般社会のセキュリティ意識の向上と企業全体のセキュリティレベルの向上を図る。	今回のサイバーセキュリティ戦略においては、 5.1.2「セキュリティマインドを持った企業経営の推進」として ・企業におけるセキュリティに係る取組が市場等から正当に評価される仕組みの構築 ・経営層と実務者層との間のコミュニケーション支援を行う橋渡し人材層の育成 ・民民間・官民間における脅威・インシデント情報の共有・演習等実施の推進 等について記載しております。 5.4.1「人材の育成・確保」として ・他分野の知識も併せ持つハイブリッド型人材の育成促進 ・高等教育等における産学連携の推進・実践的演習の充実 ・国際的競技イベント等を通じたグローバル水準の高度人材の発掘・確保　　等について記載しております。 御提言の趣旨は、これらの方向性と合致するものであると考えます。また、これらの施策の推進にあたっては、経済界と政府との連携が重要であると考えております。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
5	－	ソフトバンクモバイル（株）	5.2.1（3）サイバー犯罪への対策	17-18	2105年4月17日、総務省にて意見募集が開始された「電気通信事業における個人情報に関するガイドライン及び解説の改正案」において、接続認証ログにおける保存の在り方が明確化されるところですが、本来、接続認証ログを含め通信履歴は、課金目的や苦情対応などの各通信事業者が業務を遂行する場合に限り、記録・保存することが可能な通信の秘密として保護されるべきものです。 よって、通信履歴の保存の見直しについては、必要性及び有効性を都度慎重に議論する必要があると考えます。仮に上述の目的や理由以外の必要性において通信履歴を保存する場合は、事前に十分な法的議論を経た上で、法令等の改正やガイドラインの整備といったステップを踏むべきです。 また、トラヒックが急増する昨今において、新たな目的のために通信履歴を保存することになれば、通信事業者に対し新たに多大なコスト負担・運用負荷がかかることは明白です。よって、本件に関しては、その必要性及び有効性が認められることを明確にし、国民の理解を得たうえで、議論をすべきと考えます。	御指摘の内容については、今後の施策の検討に当たっての参考とします。
6	1	トレンドマイクロ（株）	5.1.1(3)	10	【記載内容】 官民で連携しつつ、IoTシステムの構成要素であるM2M（Machine to Machine）機器やウェアラブル端末等の機器を含め、エネルギー分野、自動車分野、医療分野等におけるIoTシステムのセキュリティに係る総合的なガイドラインや基準の整備を行う。 【意見内容】 記載内容にそれが意識されているか不明であるが、将来的には管理者のわからない自律的に稼働し続けるIoT機器やハイジャックされ管理者からは制御不能IoT機器がネットワーク上に存在し、他社への攻撃や帯域を占有するなどの被害が想定される。そのような事案が発生した際に所定の手続きを経てそれら機器を排除できる手法についても検討するべきである。 【理由】 おもにISPなどがその実務にあたるとは思うが、発生から排除までに時間を要さずに行動する必要があるため、事前の取り決めが存在することが望ましい。	御指摘の内容については、5.1.1(3)の「関係者が連携しIoTシステムや、その構成要素である機器等の脆弱性を調査し、供給者への修正を促すとともに、利用者に着実に対策が行き届くような仕組み」を検討していく中で、参考とします。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
6	2	トレンドマイクロ（株）	5.1.2(1)	11	【記載内容】 CISO（Chief Information Security Officer）の機能が各企業の経営層に確実に位置付けられるよう、官民で連携して促す。 【意見内容】 CISOを育成する講座や教育コースなどの整備が求められる。 【理由】 CISOの定義やミッションは各社によって異なる。現状の日本にはCISOのあるべき姿やベストプラクティスが少なく、CISOがどのようにあるべきかを学ぶ場所も少ない。CISOという役職が形骸化しないために事例研究を含めた研究と成果のトランスファーが求められる。	御指摘のとおり、CISOを含む企業経営層に対する普及・啓発活動については重要と考えており、具体的な施策については年次計画の中で記載しています。
6	3	トレンドマイクロ（株）	5.1.2(2)	12	【意見内容】 以下の文言を追加する。 「政府は警察庁または防衛省において毎年数百名単位でサイバーセキュリティ専任者を採用し、育成に努めサイバー犯罪への対策、国家の安全の維持に努める。」 【理由】 今回の戦略案においてはセキュリティ技術者の出口・キャリアプランまで盛り込まれており、大いに期待できるところではある。しかしながらそのほとんどが民間の努力に期するものであり、現状を鑑みるに短期的に成功をもたらすとは考えにくい。よって、政府が率先してセキュリティ技術者育成のために機会を提供し、次代を担う世代がセキュリティで立身できる世界を実現するべきである。	御指摘のとおり、政府も含め官民をまたいだセキュリティ人材のキャリアパスの構築は重要な課題であると考えておりますので、「インターンシップ制度の充実を始めとしたマッチングに資する取組を推進する。」を「インターンシップ制度の充実を始めとしたマッチングに資する取組や、産学官横断的な人材のキャリアパス構築を推進する。」に修文します。 なお、「新・情報セキュリティ人材育成プログラム」（2014年５月 情報セキュリティ政策会議決定）において、「専門人材の育成・登用は、求められる人材像を社会に示し、情報セキュリティ人材に関する需要の呼び水にもなりうることから、政府として率先して進めることとする。」としているところです。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
6	4	トレンドマイクロ（株）	5.2.1(3)	17	【意見内容】 「このため、国は、サイバー空間の脅威に関する実態把握のための情報収集の強化やサイバー犯罪に係る捜査能力の向上、取締り体制及び取締りのための情報技術解析体制等の体制強化を進め、必要な人材育成や技術開発を着実に推進する。」の後に以下を追加する。 「そして、国は、国民に対してサイバー空間の脅威の啓発に努め、国民が被害通報・報告のしやすい環境の整備を推進する。」 【理由】 追跡の前段階としての、利用者からの被害通報が重要である。サイバー空間における少額被害など通報されることなく潜在しているマイクロ犯罪が多発している。これら犯罪を放置することが結果、犯罪者優位な状況を生み出す結果となっている事を広く国民に理解を求める必要があると考える。 被害情報が早期に共有されることで、類似犯罪発生時に利用者自らが危険を察知し、犯罪抑止につながる効果も期待できる。 サイバー犯罪に巻き込まれた疑いがあるときに、そのサービスを提供するプロバイダへ報告・相談することを呼びかけ、よいサイバー空間の習慣を実践する事が、世界中のデジタル社会に恩恵をもたらす結果となることを広く周知すべきである。	ご指摘いただきました、国民に対する啓発、国民が被害通報・報告のしやすい環境の整備につきましては、5.2.1(2)「国は、各種啓発主体と連携し、「サイバーセキュリティ月間」を始めとし、不正プログラムや不審なメールへの対処の方法等に係る普及啓発活動を推進する。」や「さらに、インターネット利用における悩みや不安に関する相談に応じられる人材を育成し、活動を促す取組についても、引き続き着実に推進する。」に含まれるものと考えており、原案のとおりとさせていただきます。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
6	5	トレンドマイクロ（株）	5.2.3(1) ii	22	【意見内容】 「また、政府機関で重大なインシデントが発生した場合における原因究明調査のための取組を強化し、分析結果を共有することによって被害の拡大防止を図るとともに、対策の改善に反映させる。」を以下のとおり修文する。 「また、各政府機関が有するCSIRTと普段から連携すると共に、政府機関で重大なインシデントが発生した場合における原因究明調査のための取組を強化し、分析結果を各政府機関のCSIRT共有することによって被害の拡大防止を図るとともに、対策の改善に反映させる。」 【理由】 既に中央省庁ではCSIRTが整備されていると思われ、CSIRT連携はインシデント発生時の連携だけでは円滑なコミュニケーションは図れない。そのため、定常時から連携体制を確認し合い、重大なインシデントに備えることが重要であるから。	御意見を踏まえ、「政府機関横断的な監視・即応機能及び各機関における事態の把握・対処機能の強化に取り組むとともに、インシデントの発生に備えた訓練・演習を実施し、対処要員の能力及び連携の強化を図る。」を「GSOCによる政府機関全体における検知・解析機能の強化、並びに各機関におけるインシデント対応を行うチーム（CSIRT）の体制及び事態の把握・対処機能の強化、インシデント発生時の情報提供の迅速化・高度化に取り組む。また、インシデントの発生に備えた訓練・演習を実施し、その教訓を施策に反映させるとともに、対処要員の能力・連携の強化及び各機関幹部による指揮の下での組織的対処の徹底を図る。」に修文します。
6	6	トレンドマイクロ（株）	5.4.1(1)	32	【意見内容】 「政府機関、研究者その他の関係者間で必要となる情報・データの共有」を以下のとおり修文する。 「政府機関、研究者その他の関係者間で連携の行いやすい形式で、必要となる情報・データの共有」 【理由】 データの共有においては、機械処理（コンピュータの取り扱い）がしやすく、連携可能な標準形式を策定しての配信が必要である。実例として、Excelのセル結合を使用し、再加工しなければ、機械に取り込みができないようなデータ形式での配信事例が見られる。このような機械処理しづらい形式でのビッグデータ共有は、生産性を低下させる恐れすらある。あらかじめデータ連係を想定した情報共有システムデータの設計が重要と言える。	御指摘を踏まえ、5.4.1(1)の「政府機関、研究者その他の関係者間で必要となる情報・データの共有」を「政府機関、研究者その他の関係者間で利用しやすい形式で必要となる情報・データの共有」に修文します。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
6	7	トレンドマイクロ（株）	5.4.2(2)	35	【記載内容】 このような素養としては、論理的思考力や情報通信技術、機器の基本的な仕組み等についての理解が必要であり、それらを初等中等教育段階から、児童生徒の発達段階に応じて培うことは不可欠である。 【意見内容】 User-Generated Contentsの作成に掛かるコストの低下により、利用者による十分な思慮が行われなかった情報発信の結果、自らまたは他人を傷つけるような事象が頻発している。自らの行動がどのような影響を及ぼす可能性があるのか、立ち止まって、考えるための教育機会の提供が必要である。その為の素養として、知的財産リテラシー、プライバシーポリシーなどを読み解く能力が必要と考える。具体的事案として、児童が自らの意思で投稿を行った動画や写真による児童ポルノへの悪用、他人のコンテンツの無断使用、反社会的行動を自らの意思でさらけ出すような行為、サービス提供内容の理解不十分による過剰な範囲での情報共有などがあげられる。サイバー空間上の自身の行動によって、世界中の人々を含め、他の方々すべてに影響を及ぼす可能性があることを初等中等教育段階から継続的な取り組みが必要であると考える。 【理由】 情報セキュリティ教育に加え、早期段階から知財教育を実施することが望ましい。	御指摘の内容は、5.4.2(2)の「初等中等教育段階から、児童生徒の発達段階に応じて、情報活用の実践力、情報の科学的な理解、情報社会に参画する態度を培う教育を一層推進し、情報セキュリティを含む情報モラルの理解等を促し、論理的思考力や情報通信技術、機器の基本的な仕組み等についての理解を促すようなものとなるよう取り組む。」の「情報モラルの理解等」に含まれていると考えています。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
7	1	日本オラクル（株）	5.1. 経済社会の活力の向上及び持続的発展	8	【意見内容】 「IoTシステムの提供するサービスの効用と比較してセキュリティリスクを許容し得る程度まで低減していくことが、今後の社会全体としての課題（チャレンジ）となる。」の後に次の段落として以下を追記する。 「また、IoTの活用の背景には、ネットワークを通じたサービスの利用を普及させるというネットワーク中心思想から、情報システム及びサービスの 中核であるデータを個人や部門の所有ではなく、エンタープライズ単位で、或いは関連企業等のステークホルダー、消費者などの拡大コミュニテイ内で 共有し、活用していくというデータ中心思想への転換がある。データ中心の情報システム及びサービスを円滑に動かすためには、データオーナー（data owner）の責任とマスタデータ管理が不可欠であるとともに、ネットワークセキュリティからデータセキュリティへの軸足の移動が必要とされる。クラウド 化の推進により、データセンタに膨大なデータが集約され、一回のサイバー攻撃で数百万件の個人情報等が漏洩する現状を考慮すると、データベースセ キュリティを含む多層のデータセキュリティを確保するのは急務である。」 【理由】 日本年金機構における大量の個人情報漏洩が社会問題化している現状に見られるように、最早、水際対策では高度サイバー攻撃を阻止できず、効果的 な内部対策の実現が求められている。	御指摘を踏まえ、5.1において、以下のとおり修文します。 「例えば、サイバー攻撃によりモノが意図しない動作をするよう遠隔操作されたり、ウェアラブル端末を通じて個人に関する情報が窃取されたりといった実空間に密着したリスクや、1回のサイバー攻撃で多くのステークホルダーが関与するデータベースから数百万、数千万件の個人情報等が流出するといった経済社会に重大な影響を及ぼすリスクは、こうしたサービスの信頼性や品質を根本的に損なう。」

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
7	2	日本オラクル（株）	5.2.3 、i.インシデントの未然防止	22	【意見内容】 「また、サプライチェーン・リスクへの対応を始めとした情報システムの企画・設計段階からセキュリティの確保を盛り込むための取組を推進する。」に以下のとおり追記、修文する。 「また、サプライチェーン・リスクへの対応を始めとし、データの保全を念頭にした情報システムの企画・設計段階からセキュリティの確保を盛り込むための取組を推進する。」 【理由】 サイバー空間で懸念される現実の脅威は、例えば、個人情報を含む機密情報の窃取、データの改ざんなどを起点として、サイバー空間を含む人間社会 全体に問題が波及する。つまり、起点となるデータの保全こそが最大の課題になる。そのため、情報システムの企画・設計段階から、データのライフサ イクルに焦点に当て、データの保全を念頭においたセキュリティの確保が最低限必須の要件となる。	御指摘のとおり、情報システムの企画・設計段階からデータ保全を念頭に置くことは重要であると考えています。他方、企画・設計段階から念頭に置くべき事項は必ずしもデータ保全に限られるものではないため、原案のとおりとします。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
7	3	日本オラクル（株）	5.4.1(4) 国際連携による研究開発の強化	33	【意見内容】 「同時に、様々な国際標準化の取組が行われている中で、セキュリティ技術に関する国際標準の策定・普及や相互承認の枠組み作りを進めていく。」を以下のとおり修文する。 「同時に、さまざまな国際標準化の取り組みの中で、セキュリティ技術を中心とした要素技術、システムインテグレーション技術など幅広い視野に立った国際標準の策定・普及や相互承認の枠組み作りを進めていく。」 【理由】 IoTまでを視野に入れたサイバーセキュリティを考えるとき、単なるセキュリティ技術に関する国際標準の策定・普及や相互承認の枠組み作りでは 片落ちになる懸念がある。例えば、クラウドコンピューティング環境を前提とするIoTの場合では、インターネットにつながる機器がクラウドサービ ス使用者となり、現在想定されているクラウドコンピューティングのモデルを一歩進化させねば対応が難しいと考えられる。このような状況も踏まえた 上で、国際標準の策定を行わねばならない。そのためには、セキュリティに関する標準化技術者のみならず、幅広い標準化技術者の参画が必須となろ う。「4.5　多様な主体の連携」に「サイバーセキュリティに係るビジョンを共有し、それぞれの役割や責務を果たし、また努力する必要が ある。そして、政府はこれらのステークホルダーを適切な連携関係へと促す役割を担っている。」とあるが、この考え方は、堅牢で柔軟なサイバーセ キュリティを実現するための国際標準化にとって極めて重要なカギとなる。	御指摘の趣旨を踏まえ、セキュリティに資する幅広い技術等という観点から、5.4.1(4)の「セキュリティ技術に関する国際標準」を「セキュリティ技術を中心とした様々な国際標準」に修正します。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
8	1	NPO法人日本セキュリティ監査協会	5.1.2 セキュリティマインドを持った企業経営の推進	11	【意見内容】 「セキュリティ人材の育成、組織能力の向上等を図ることが必要となってくる。」の後に以下を追記する。 「加えて、企業と政府、企業相互ならびに企業と利用者間の信頼を醸成するために、経営者が情報セキュリティ管理に関する説明責任を果たすことが求められる。」 【理由】 経営者の意識改革のためには、重要な情報を扱っている企業の経営者自身が説明責任を果たす責務を負うことが必要となる。意識改革の啓発活動において、説明責任を果たすことを明確にしておくとともに、そのためには自社の情報セキュリティ対策が適切に行われていることを確認する必要がある。特に、重要な情報を扱う民間企業においては、第三者として独立した専門家による監査に基づく保証を得ることが重要である。	御指摘のとおり、経営者による的確な認識と説明は重要であり、5.1.2(1)に「サイバーセキュリティを経営上の重要課題として取り組んでいることが市場や出資者といったステークホルダーから正当に評価される仕組みや資金調達等の財務面で有利となる仕組みの構築、認識醸成」と記載しており、この中に御指摘の考え方も含まれていると考えており、原案のとおりとします。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
8	2	NPO法人日本セキュリティ監査協会	5.1.2 (1) 経営層の意識改革	11,12	【意見内容】 「ステークホルダーから正当に評価される仕組みや資金調達等の財務面で有利となる仕組みの構築、認識醸成のための官民が一体となった啓発活動を実施する。」の後に次の段落として以下を追記する。 「また、情報セキュリティ管理が適切に行われていることを情報セキュリティ監査で確認し、その結果の公開等を通じて、情報を取り扱う主体としての説明責任を果たすことを促す。特に、大量の個人情報を取り扱う事業主体、重要インフラ事業者およびオリンピック・パラリンピックにおいて中核的な役割を担う主体においては、開催の前年度までに保証型情報セキュリティ監査を行い、第三者の保証を得ることとする。」 【理由】 経営者の意識改革のためには、重要な情報を扱っている企業の経営者自身が説明責任を果たす責務を負うことが必要となる。意識改革の啓発活動において、説明責任を果たすことを明確にしておくとともに、そのためには自社の情報セキュリティ対策が適切に行われていることを確認する必要がある。特に、重要な情報を扱う民間企業においては、第三者として独立した専門家による監査に基づく保証を得ることが重要である。	御指摘のとおり、経営者による的確な認識と説明は重要であり、5.1.2(1)に「サイバーセキュリティを経営上の重要課題として取り組んでいることが市場や出資者といったステークホルダーから正当に評価される仕組みや資金調達等の財務面で有利となる仕組みの構築、認識醸成」と記載しており、この中に御指摘の考え方も含まれていると考えており、原案のとおりとします。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
8	3	NPO法人日本セキュリティ監査協会	5.2.3　政府機関を守るための取組	21	【意見内容】 「新たに直面した脅威・課題についても基準に逐次反映することによって対応してきたところである。」の後に以下を追記する。 「環境変化が急激であることからこれを加速し、基準等に準拠した情報セキュリティ対策が実施できていることについて、確認を行い、国民の信頼をより高めるようにしていく。」 【理由】 政府の情報セキュリティ対策に関する国民の信頼をより得ると共に、情報セキュリティ監査の結果をより有効に活用することが望ましいため。	御指摘の内容については、5.2.3に「政府機関等においては、既に顕在化している脅威や課題はもとより、未知の脅威等に直面した場合であっても柔軟かつ迅速に対応できるよう、従来から推進している対策に万全を期すことを前提としつつ、先々を見据えて以下の事項について重点的に取り組むとともに、政府機関における統一的な基準を始めとした規程に適時反映し、監査や平素からの教育などの取組によりその徹底を図る。」と、5.2.3(2)に「定期的な自己点検や第三者的視点からのマネジメント監査を始めとした点検の実施を通じて、政府機関等における対策強化のための体制・制度の検証・改善に取り組む」とそれぞれ記述しており、これに含まれると考えることから、原案のとおりとします。 なお、御指摘の「新たに直面した脅威・課題についても基準に逐次反映することによって対応してきた」については、政府機関等におけるこれまでの取組の概要として記述しています。
8	4	NPO法人日本セキュリティ監査協会	5.2.3（1）攻撃を前提とした情報システムの防御力の強化	23	【意見内容】 新たにⅳ項として以下を追記する。 「ⅳ. 信頼の確立　政府機関は国民の安全を守る立場であり、また、国民生活に重大な影響を与える可能性のある情報を国民から預託されている立場である。このため、国民の十分な信頼と期待に応える必要があり、実施している情報セキュリティ管理について、国民への説明責任を果たす必要がある。これまでも、情報セキュリティ監査等を行い、情報セキュリティ管理について報告書を公開するなど国民への説明に努めてきた。更に、新たな体制に基づきより厳密な監査を行うこととしている。今後、情報セキュリティ管理の責任者のコミットメントが果たされているかを検証する助言型監査を行うと共に、2020年までに重要な情報を取り扱う組織を対象に保証型監査を実施し、信頼の確立を図る。」 【理由】 政府の情報セキュリティ対策に関する国民の信頼をより得ると共に、情報セキュリティ監査の結果をより有効に活用することが望ましいため。	5.2.3(1)の「攻撃を前提とした情報システムの防御力の強化・多層的な対策の推進」は、サイバー攻撃への対処に関する施策を記載するパートとしており、原案のとおりとします。 なお、情報セキュリティ監査に関しては、5.2.3(2)において「定期的な自己点検や第三者的視点からのマネジメント監査を始めとした点検の実施を通じて、政府機関等における対策強化のための体制・制度の検証・改善に取り組む」としているところであり、御意見については当該施策の検討に当たっての参考とします。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
9	1	（一社）日本電気制御機器工業会	全般	－	文章の至るところに「官民」連携という文言がありますが、「産学」の文言が入っておりませんが、なぜでしょうか。	「官民」と記載している場合は、官庁と民間組織（産学を含む）を指して用いていますが、「産学官」と記載した方がより文意が通じやすい箇所について、「官民」の記載を「産学官」に修文します。
9	2	（一社）日本電気制御機器工業会	全般	－	各戦略におけるスケジュールをある程度、明確にされてはいかがでしょうか。	本戦略は、今後3年程度の基本的な施策の方向性を示すものであり、各年度に実施する具体的な施策の内容については、別途、年次計画を作成し推進していく旨、7.に記載しています。
9	3	（一社）日本電気制御機器工業会	5.2. 国民が安全で安心して暮らせる社会の実現	23	政府及び重要インフラ企業に対し、監査を徹底していく旨の内容が提示されています。そこで、各団体の制御システムセキュリティに関する取り組みを記載してはどうでしょうか。	本戦略では、重要インフラ企業に対する監査を徹底していく旨の内容は記載しておりませんが、制御系システムのセキュリティについては、その重要性を認識し、国際標準に即した第三者認証制度の活用等について記載しています。
10	－	NPO法人日本ネットワークセキュリティ協会	全般	－	官民を問わず、様々なサイバーセキュリティインシデントが頻発している昨今、さらに様々なIT新技術の利用が急拡大している現在、政府としてのサイバーセキュリティ戦略改定は大きな意味を持つものと考えます。新戦略に賛同すると同時に、サイバーセキュリティ業界の団体として、また、民間のサイバーセキュリティ向上をになう一翼として、日本のサイバー空間の安全、安心に今後とも様々な形で協力いたしていく所存です。とりわけ、民間企業においては、IT現場のセキュリティ能力向上や、情報交流、インシデント対応能力向上などが大きな課題となっており、こうした面でも政府と情報交換しながら、積極的に取り組みを進めたいと考えます。	本案に賛同する御意見として承ります。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
11	1	日本ユニシス(株)	全般	－	過去に策定された戦略との関係が不明なので、例えば平成25年に策定された「サイバーセキュリティ戦略2013」との関連性や継続性について1章で補足を付記していただきたい(過去の戦略とは変化があった部分や、捨てる部分、継続する部分についてなど)。	今回の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(平成26年法律第104号)に基づき、閣議決定文書として策定されることとなっており、これまでの情報セキュリティ政策会議で策定していた戦略とは位置付け・内容ともに異なるものです。なお、個別の施策については、年次計画に記載することとします。
11	2	日本ユニシス(株)	2.2.サイバー空間における脅威の深刻化	2	「場所・時間の制約を受けず誰もが容易に参加できるサイバー空間は、悪意ある攻撃者に対し、防御側と比べて非対称な優位性を与えている。」における「非対称な優位性」の意味が判らないので補足を付記していただきたい。	御指摘の「非対称な優位性」とは、例えば、攻撃者は世界中の任意の場所から任意のタイミングで任意の手段で攻撃できることに対して、防御側は世界中のどこからどのような方法で来るかわからない攻撃に対して常にセキュリティを確保し続けなければならないため、取組の負荷やコスト、影響度等において攻撃側に非対称な優位性があることを指しますが、ここでは基本的な考え方のみ列記しており、個々の具体的な内容は記載していないことから、原案のとおりとします。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
11	3	日本ユニシス(株)	5.目的達成のための施策	7	【意見内容】 「4章 基本原則」の「4.5. 多様な主体の連携」において、「国民の表現の自由とプライバシーの保護を共存させ」とのあるべき姿が記述されていることに鑑み、5章の「目的達成のための施策」のどこかに「プライバシー・バイ・デザインの考え方を推進する」旨を追記してはいかがでしょうか。 【理由】 5.1.1(1)において「セキュリティ・バイ・デザインの推進」が記述されています。 今後の連接融合情報社会においては、パーソナルデータやマイナンバー情報を扱うことが飛躍的に増大するので、セキュリティ・バイ・デザインと並び、プライバシー・バイ・デザインの概念が必須となります。	サイバーセキュリティに係る施策を推進する中で、プライバシー保護の観点は非常に重要であると認識しておりますが、本戦略の「5. 目的達成のための施策」では、サイバーセキュリティに係る施策を示すことを目的としているため、「プライバシー・バイ・デザイン」の推進を掲げることは馴染まないものと考えます。尚、施策の推進に当たっては「4.1情報の自由な流通の確保」で記載している通り、「所要の規律とプライバシーの確保の適正なバランスについて十分な吟味を行うべきである」という基本原則に従うことも明示しております。
11	4	日本ユニシス(株)	5.1.1.(3) IoTシステムのセキュリティに係る制度整備	10	「官民で連携しつつ、IoTシステムの構成要素であるM2M(Machine to Machine)機器やウェアラブル端末等の機器を含め、エネルギー分野、自動車分野、医療分野等におけるIoTシステムのセキュリティに係る総合的なガイドラインや基準の整備を行う。」とありますが、「官民で連携しつつ」の対応策として、ウエアラブルデバイスセキュリティの対策ガイドを検討・策定している(社)日本スマートフォンセキュリティ協会等を活用してはいかがでしょうか。	御指摘の内容については、今後の施策の検討に当たっての参考とします。
11	5	日本ユニシス(株)	5.1.3.(2) 公正なビジネス環境の整備	14	「セキュリティを理由に国際的な貿易のルールに不適切な影響を及ぼす措置に対しては、国際的な連携の下、厳格に対処する。」における「セキュリティを理由に国際的な貿易のルールに不適切な影響を及ぼす措置」の意味が判り難いので具体例を追記していただきたい。	ここでは一般論として記載しており、特定の例を挙げることは適切でないと考えるため、原案のとおりとします。
11	6	日本ユニシス(株)	5.2. 国民が安全で安心して暮らせる社会の実現	15	「残存リスクの情報も添えて経営者層に対し総合的な判断を受ける機能保証(任務保証)の取組が必要である。」における「機能保障(任務保障)の取組」の意味が判り難いので、具体的に記述していただきたい。	御指摘を踏まえ、より文意が通じやすいよう、御指摘の箇所について、「残存リスクの情報も添えて経営者層に対し提供し総合的な判断を受ける「機能保証(任務保証)」の考え方に基づく取組が必要である。」と修文します。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
11	7	日本ユニシス(株)	5.2.3政府機関を守るための取組	21	実際にインシデントが発生してしまった場合にどう対応するかについての指針が必要に思われます。例えば、インシデント発生時の被害状況公開の指針、被害者からの問い合わせへどんな情報を提供するかなどの指針など。	インシデント発生時の対応については重要であると考えており、5.2.3(1)において対応方針を記載しているところです。御指摘の内容については、今後の施策の検討に当たっての参考とします。
11	8	日本ユニシス(株)	5.4.1　研究開発の推進	32	【意見内容】 長期的な視野に立って、老若男女のあらゆる利用者が、そのリテラシーの高低にかかわらず、いつでもどこでも、ストレスなく使いこなせるセキュリティ対策技術の研究開発推進を追記してはいかがでしょうか。 【理由】 現在のインターネット利用環境においては、一般利用者が使用する端末機器のセキュリティ確保において相当なリテラシーが要求され、普通の利用者にはあまりに実現困難な対策が多くあります。そのため、一般利用者のリテラシーに係わらず適正なセキュリティ確保が実現できるような対策手法の研究開発の推進が望まれます。	御指摘の点については、5.4.1(1)「サイバーセキュリティの研究開発は社会的なニーズを踏まえ実用化されることが重要であり、研究成果の社会還元の推進が重要である。」に含まれるものと考えており、原案のとおりとします。 なお、「情報セキュリティ研究開発戦略(改定版)」(2014年7月 情報セキュリティ政策会議決定)において、利用者の視点を踏まえた研究開発について記載しています。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
11	9	日本ユニシス（株）	全般（連接融合情報社会の適切な維持のため、比較的実行が容易な物理テロ対策の追記について）	－	【意見内容】 例えば民間のクラウド・データセンター等に対する、郵便による炭疽菌の送り付けや火炎瓶等の発火物持参による突入など、比較的簡単に実行が可能な物理テロへの備えは、大規模（地震）災害対策と同様に必須と考えます。 しかしながら、ISO27000ベースの規程や日本国内の各省庁が制定しているセキュリティ基準やガイドラインには物理テロ攻撃を想定した対策要件が記述されておらず、また民間企業にはその対策に係る知見がありません。 連接融合情報社会の適切な維持のためには、サイバーセキュリティと並んで比較的実行が容易な物理テロによる情報システム破壊への適切な防御施策が望まれます。これにより、グローバルな性質を持つサイバー空間の平和と安定に寄与できます。	御指摘の内容については、今後の施策の検討に当たっての参考とします。 なお、サイバーセキュリティの観点からも重大な事象については、サイバーセキュリティ戦略本部は、必要に応じて重大テロ対策本部などの危機管理の体制との連携や、国家安全保障会議との緊密な連携等により対応していきます。
12	1	Virtual Engineering Community	全般	－	制御システムでは、現場の安全基準と対策があり、それに「制御システムセキュリティ対策」が加わったリスクアセスメントが求められると考えます。 日本の各産業別特異性も考慮した制御システムセキュリティアセッサ制度の実現と、認定試験及び普及啓発活動を実施していく民間機関創設の必要性を感じております。	制御システムのセキュリティに係る評価・認証制度等への取組については、5.1.3(3)において、「制御装置等を含むIoTシステムのセキュリティに係る国際的な標準規格や評価・認証制度の国際的な相互承認への枠組み作りについて、産学官が一体となり、国際的議論を主導していくほか、我が国のベストプラクティスの国際的な共有・展開を図る。」と記載しています。 御指摘の内容については、今後の施策の検討に当たっての参考とします。
12	2	Virtual Engineering Community	全般	－	制御システムを対象にしたペネトレーションテストする場合は、現場の安全対策を施した上で実施されなければならない為、かなりのコストと時間が必要となります。 できるだけコストと時間をかけないで安全に実施効果を出す技術的検討も事前検討に含めておくことになると思います。	制御システムを含むIoTシステム全体としてのセキュリティ確保のための対策として、5.1.1(4)において、「テスト環境の構築や、システム全体の脅威分析・リスク評価手法の開発、ICチップを含むハードウェアの真正性の検証等、社会科学的な研究も含め、IoTシステムにおける対策検討等に必要な技術開発・実証事業を行う。」と記載しています。具体的な施策については年次計画の中で記載します。 御指摘の内容については、今後の施策の検討に当たっての参考とします。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
12	3	Virtual Engineering Community	5.2.2 重要インフラを守るための取組	18-21	重要インフラ事業者の内部監査、外部監査の実施について 内部監査や外部監査を実施するに、監査範囲・監査項目・監査基準・監査方法の定義と内容設定が必要となります。アセットオーナー対象とサプライヤ対象の監査チェックシートを活用してはいかがでしょうか。	御指摘の内容については、今後の施策の検討に当たっての参考とします。
12	4	Virtual Engineering Community	5.4.2 人材の育成・確保	34-36	e-learning教育ビデオ講座やゲーム形式でインシデント疑似体験ができるトレーニングの活用、制御システムセキュリティ対策のセキュアなアセットオーナー管理者やセキュアな制御システムエンジニアリング設計技術者やセキュアな制御製品開発技術者を目指す方々が自分の実力がどこにあるかを見る目安となる模擬試験の実施などによる制御システムセキュリティ対策の人材教育が重要と考えます。	実践的演習や能力の可視化の重要性や取組について、5.4.2(1)、5.4.2(4)、5.4.2(5)で記載しており、御指摘の内容については、今後の施策の検討に当たっての参考とします。 なお、具体的な施策については年次計画の中で記載します。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
13	1	BSA｜ザ・ソフトウェア・アライアンス	5.1.1 (1) 安全な IoT システムを活用した新規事業の振興	9	【意見内容】 当該箇所については、「IoT システムに係る新たな事業を成功させるためには、競争力の源泉となる高いレベルでのセキュリティ品質の実現が不可欠である。このため、システムの企画・設計段階からセキュリティの確保を盛り込むセキュリティ・バイ・デザイン（Security By Design）の考え方を推進する。そして、IoT事業者は、この考え方を、既存システムのアップグレードやレガシーインフラへのつなぎこみの際にも考慮すべきである。具体的には、「IoT システムに係る事業について、セキュリティ・バイ・デザインの考え方に基づき所要のセキュリティ対策を業態横断的に推進し、メリハリをもって、積極的に新規事業の振興を図る。」との方針を記載すべきと考えます。 【理由】 セキュリティ・バイ・デザインを推進していくべきことについては賛同しますが、現実には、既存のシステムがセキュリティ・バイ・デザインの考え方に基づいた新システムに完全に入れ替わるまでには、長い時間を要します。このため、完全に新システムに移行するまでの間、既存のシステムのアップグレードやレガシーインフラへのつなぎこみの際にも、セキュリティを確保していく方策について考える必要があります。	御指摘を踏まえ、「このため、システムの企画・設計段階からセキュリティの確保を盛り込むセキュリティ・バイ・デザイン（Security By Design）の考え方を推進する。」を「このため、連接される既存システムを含めて、IoTシステム全体の企画・設計段階からセキュリティの確保を盛り込むセキュリティ・バイ・デザイン（Security By Design）の考え方を推進する。」に修文します。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
13	2	BSA｜ザ・ソフトウェア・アライアンス	5.1.1 (2) IoTシステムのセキュリティに係る体系及び体制の整備 (3)IoTシステムのセキュリティに係る制度整備	9,10	日本政府が、セキュリティー般、特にIoTに依存する部分について、そのルールを、事業者にとってより明確になるよう取り組まれることを歓迎します。また、民間部門と十分な協議のもとルールを策定するとの本戦略のアプローチに賛同します。日本政府においては、適切なサイバーセキュリティ政策及び当該政策を実施するための正しい制度的枠組を策定すべく、引き続き取り組んでいただけるようお願い致します。この際、サイバーセキュリティに関する体系・体制・制度整備は、以下の重要な原則（以下「推奨基本原則」という。）に基づき策定されるべきと考えます。 （ア）リスク・ベースかつ優先順位をつける （イ）技術中立性 （ウ）実行可能であること （エ）柔軟性 （オ）プライバシー及び市民の自由の尊重 以上に加えて、（ア）不必要で不合理な要求事項の策定を避け、事業者が自らが最も直面し得るリスクを低減できるように、幅広く、最も効果的な最先端のサイバーセキュリティソリューションを開発し、採用できるようにし、（イ） 業界が参加して国を超えて承認された、国際的認知のある標準を採用し、（ウ）最先端の製品及びサービスは、複数の異なる国に存在する研究開発拠点の国際的な協力のもと開発されるものであるから、現地で生まれた技術を優先する政策を回避することも非常に重要であり、これらを政策として採用するよう政府に対し要望致します。	IoTシステムのセキュリティに係る体系・体制の整備、制度整備について、産学官が連携して取り組んでいくことは重要であり、御指摘の内容については、各種ガイドラインの策定等、今後の施策の検討に当たっての参考とします。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
13	3	BSA｜ザ・ソフトウェア・アライアンス	5.1.2 （1）経営層の意識改革	11	事業者及び団体におけるサイバーセキュリティ対策の採用を促進する政府の取組みに賛同します。堅牢なサイバーセキュリティの確保は、我が国の経済社会の活力の向上及び持続的発展のために必要であることにとどまらず、海外における競争力の向上にも役立つものであるため、その点追記すべきと考えます。即ち、堅牢なサイバーセキュリティの確保は、消費者及び投資家双方の信頼を獲得し維持するものだからです。	本案に賛同する御意見として承ります。
13	4	BSA｜ザ・ソフトウェア・アライアンス	5.1.2（3）組織能力の向上	12	ガイドラインの策定や第三者認証の活用にあたっては、前記の推奨基本原則を考慮するよう要望致します。 また、本戦略は、サイバーセキュリティに関する懸念に対応する上で情報共有が重要であること及びこれを達成するためには官民協働が促進されるべきことを指摘しており、これに賛同します。	御指摘の内容については、今後の施策（ガイドラインの策定や第三者認証の活用等）の検討に当たって参考とします。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
13	5	BSA｜ザ・ソフトウェア・アライアンス	5.1.3(1) サイバーセキュリティ関連産業の振興(13頁)	13	サイバーセキュリティ分野におけるベンチャー企業等の活性化のため、政府系ファンドの活用によるベンチャー企業同士の国際的な交流を含む共同研究開発等の促進、公的研究機関とベンチャー企業との共同研究開発の促進等の取組が挙げられていますが、国家プロジェクトの予算が終了した後も持続可能なビジネスにするためにはどのようにすればよいのかというビジョンも提示すべきと考えます。従って、国内外の民間企業及び公的研究機関においてどのような実証実験及び事業が展開されているかの調査を行い、その結果を有効活用するような取組を本戦略に加えるべきであると考えます。	IoT産業等の関連産業の成長に伴い、今後、コンサルティングや人材育成ビジネスを含むサイバーセキュリティ関連産業に対する需要が一層増加することが見込まれることから、サイバーセキュリティ産業がこうした需要を捉え、成長産業となるよう、国内外で大規模に活躍できる企業の育成やベンチャー企業の育成等によりこれを振興していくことが重要であると考えており、御指摘の内容については、今後の施策の実施に当たっての参考とします。
13	6	BSA｜ザ・ソフトウェア・アライアンス	5.1.3(2) 公正なビジネス環境の整備	14	セキュリティを理由に国際的な貿易のルールに不適切な影響を及ぼす措置に対して、国際的な連携の下、厳格に対処することは非常に重要であり、これを強く支持します。 企業は、技術革新や消費者のニーズへの合致等、その目的に応じて、最適かつ最善のテクノロジーを使用することができなければなりません。また、インターネット関連サービスを提供する企業は、物理的なインフラを自国や自身の地域に保有する必要がないにもかかわらず、多くの国がそのような要件を課そうとしており、これにより企業に不必要なコストと負担を強いている問題があります。企業は、サービスをその国向けに変更したり、サービスを展開する国ごとに高コストのデータセンターを設置することを求められるべきではないと考えます。同様の関心を有する国と連携し、日本政府がこの問題に積極的に対応されることを要望致します。	本案に賛同する御意見として承ります。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
13	7	BSA｜ザ・ソフトウェア・アライアンス	5.1.3(3) 我が国企業の国際展開のための環境整備	14	【意見内容】 国際標準や評価認証制度の策定・関与が大変重要であることについて賛同致しますが、その取組においては、推奨基本原則に基づき牽引していただけるよう要望します。 また、サプライチェーン・リスクへのセキュリティ対策の協力を推進していくことは非常に重要な取組みであり、その際、ASEAN諸国のみに注力するのではなく、米国やEUなど同じ目標を持つ他の地域の政府ともパートナーシップを結んでいくことを要望します。 【理由】 「国際的なルールや規範の形成」「国際的な信頼醸成措置」「世界各国との協力・連携」等の箇所でも挙げられている事項ですが、このことは、サプライチェーン・リスクへのセキュリティ対策についても同様に行っていくことが有益であると考えます。これにより、本分野においても、より広範な国際協力体制の構築が可能となり、日本企業が世界のサプライチェーン要件を満たすことを確実なものとするからです。	御指摘のとおり、ASEAN加盟国のみならず、北米や欧州等との協力・連携を推進することが重要と認識しており、5.3.3において、その旨を記載しています。
13	8	BSA｜ザ・ソフトウェア・アライアンス	5.2.1(1)安全・安心なサイバー空間の利用環境の構築	15,16	調査を行った結果、ソフトウェアの不正利用とサイバーセキュリティの脅威との間に相関関係があることが分かりました。 管理を行うということは一見簡単なことのようですが、現実には、多くの事業者において、適正なソフトウェアライセンスのみの使用を命じる方針を採用するという、最初の第一歩が行われていません。 政府に対し、セキュリティリスクを減じるために、官民において、ソフトウェア資産管理のベストプラクティスを示し、これを共有することを要望します。	御指摘のとおり、安全・安心なサイバー空間の利用環境の構築を図る上でプラクティスの共有は重要と認識しており、一般利用者等への普及啓発に取り組む旨、5.2.1(1)においても記載しているところです。御指摘の内容は、今後の普及啓発施策検討に当たっての参考とさせて頂きます。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
13	9	BSA｜ザ・ソフトウェア・アライアンス	5.2.1(1)安全・安心なサイバー空間の利用環境の構築	15,16	マルウェアに感染したネットワークが構成するボットへの先手的な対応の検討は具体的なものである必要があると考えます。これには、法的・制度的に未整備の部分についての検討を含み、また、対応策について、民間の知見を充分に活用されることを期待します。日本においても、米国事例も参考に、より柔軟な制度を検討していくことが有益であると考えます。 さらに、警察、検察、裁判所等がサイバー犯罪に対して知見を蓄えることが有益であると考えます。この点、米国のNational Computer Forensic Instituteの活動が参考となります。また、人材面でも、官民の人材交流をさらに活性化することで、グローバルなサイバー犯罪に対応できる人材を育てていくことが肝要です。	御指摘のとおり、サイバー犯罪対策に関する制度の整備や人材の育成は重要と認識しており、5.2.1(3)や5.4.2(3)において、その旨を記載しています。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
13	10	BSA｜ザ・ソフトウェア・アライアンス	5.2.2(2)効果的かつ迅速な情報共有の実現	19	サイバー攻撃は、民間か政府機関かを問わず、また、国を超えてなされるため、情報共有に関する政策は、官民で又は民間企業・政府機関のそれぞれの間での情報共有を促進するものとすべきです。この観点から、政策決定者に対し、有効なサイバー脅威情報共有のために以下の6つの基本原則を推奨しています。 （ア）適切な目標を定めた政策を通じて、情報の共有及び受領に対する法律又は規制上の潜在的影響を明示的に限定することにより、民間機関が、国内及び海外において、サイバー脅威の指標に関する情報を他の民間機関又は政府と自発的に情報共有できる権限を付与すること （イ）サイバー脅威の指標を適時に共有することを妨げずに、サイバー脅威情報の共有により影響を受ける者のプライバシーを保護する適切な政策を策定すること （ウ）関連するサイバー脅威の情報を民間部門と共有する権限を政府機関に付与し促進すること、及び当該情報共有の期間を早めること（自動メカニズムによる場合を含む） （エ）民間機関による政府及び民間双方との間の情報共有を促進すること、共有される情報について義務づけられる契約上の条件を最小限にすること、並びに、影響を受ける当事者が適切な取引上の合意を締結できるような柔軟性を提供すること （オ）官民の情報共有のための民間のポータルを構築すること、及びこれらの情報共有に対する賠償保険が提供されるようにすること。 （カ）共有されたサイバー脅威の情報は、受領者によりサイバーセキュリティ促進にのみ用いられ、その他の目的に用いられず、及び、政府と情報を共有した場合にはその情報はサイバーセキュリティ促進又は限定された法の執行にのみ用いられることを保証すること	御指摘の内容については、今後の施策の検討に当たっての参考とします。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
13	11	BSA｜ザ・ソフトウェア・アライアンス	5.3 国際社会の平和・安定及び我が国の安全保障	24	サイバー空間がグローバルな空間であること、サイバー攻撃が容易に国境を越えて行われ得ることから、同盟国及び同様の立場に立ついわゆる有志国・機関との間の脅威情報の共有や人材育成等における協力・連携の積極的な推進が不可欠であり、また、その他の国とも信頼醸成を進めていくことが重要であるとの指摘につき賛同し、政府及び民間の双方のレベルで緊密な連携が進められるよう、確実な推進を望みます。	本案に賛同する御意見として承ります。
14	－	ファイア・アイ（株）	全般	－	【意見内容】 サイバー脅威に対して効果的な防御のために、基本的な基盤となる戦略的方針を構築するべきであり、この方針には、攻撃者の攻撃ライフサイクルを念頭に、シグネチャーに依存しないプロアクティブな方法をもってして、攻撃を検知し、防御する手法も含まれるべきです。 これらの新しい技術の導入と政府のセキュリティ防御の必要性の周知をすすめるために、担当職員、調達担当職員の皆様への研修や教育も含まれるようにしなければなりません。 この研修や教育には、高度なサイバー攻撃を行う攻撃者によって使用されるツール、戦術や手法に重点を置いて進化しているサイバー脅威を含める必要があります。 これは、担当職員の方が業務にあたる上で、最新の脅威状況に照らし合わせて、必要な決定事項を標準化することを可能とし、高度な攻撃者に対抗するセキュリティ対策をすすめます。 また、従来の調達手順に乗っ取らない、脅威の変化に対応できる新しいサイバーセキュリティ機能の、迅速かつ柔軟な取得を可能にする調達プロセスの確立もまた重要な課題であり支援するべきです。 高度なサイバー脅威から防御するための対策を導入することは、重要です。	御指摘の内容については、今後の施策の検討に当たっての参考とします。 なお、プロアクティブな対処の重要性については、「情報セキュリティ研究開発戦略（改定版）」（2014年7月 情報セキュリティ政策会議決定）にも記載しているところであり、本戦略においては5.4.1(1)の「実態を踏まえた検知・防御能力の向上」の中で認識しています。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
15	－	（株）MESSA	全般	－	メール添付のファイルを開封する必要がある業務では、業務を行うクライアントを十分に管理する必要があると思います。GoogleのGMailなどでは、1つのアカウントに紐付けて数個のPOP3もしくはIMAPサーバーからメールを受信することが可能です。開封する必要があるファイル（Wordファイル、PDFファイルなど）はブラウザで見ることが可能です。クライアントのパソコン上にファイルをダウンロードしてから開く事よりリスクを軽減できるはずです。適応型の防御は必要だと思います。コストをかけないで、現状のシステムをリスクが少ない方向へシフトするのは大事だと思います。	御指摘の内容については、今後の施策の検討に当たっての参考とします。
16	1	メリルリンチ日本証券（株）	5.1.2(1) 経営層の意識改革	11	経営層の意識改革については重要と考えるが、経営責任については法整備進めて経営に求める責任を明確にすることが望まれる。	御指摘の内容については、今後の施策の検討に当たっての参考とします。
16	2	メリルリンチ日本証券（株）	5.2.2(3) 各分野の個別事情への支援	20	各分野の個別事情への支援については期待したい。また、各分野リスクレベルにあったコントロール要件が設定することが望まれる。電気・ガスなどライフラインに係る業種のコントロール要件と、金融機関に求めるコントロール要件は相違するはず。	本案に賛同する御意見として承ります。なお、重要インフラの各分野における安全基準等は各分野におけるサービスの特性や社会環境等に応じて当然に異なるものであると考えます。
16	3	メリルリンチ日本証券（株）	6. 推進体制	37	情報共有について関係各所の連携強化を図ることは必要だが、障害原因のシステム名、ベンダー名など特有な情報に対しての情報共有について一定のルールを策定して運用することが大切と考える。 また、年金保険機構の問題などを考慮して、早期の限定的な情報共有のルール策定も必要。	情報の共有に当たっては、効果的な情報を迅速に共有していく必要があると認識しており、御指摘の内容については、今後の施策の検討に当たっての参考とします。
16	4	メリルリンチ日本証券（株）	－	－	事務所を独立した場所に設けるなど物理的な情報隔壁への対応も必要である。	御指摘の内容については、今後の施策の検討に当たっての参考とします。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
17	－	個人（1）	全般	－	方針に経済性を意識して含めることも検討する必要があるのではないかと考えました。 ・サイバーセキュリティを公的な安全保障とするのであれば、公的サービスの提供と税の徴収を行いサイバースペースの治安維持に関する一定程度の責任を政府がもつことを明確にする ・この税の徴収を大規模なバグバウンティープログラムや民間企業との人材流動性向上（中途採用）にあてるなど競争性のあるモデルを政府主導で立案 ・日本独自の技術開発ではなく、米国からライセンス生産モデルなどを日本企業でもできるようサイバーセキュリティ製品にもあてはめて、日本企業による独自カスタマイズを日本企業が推進できるようにする ・IoTの安全は製品だけでなくバックエンドとAPIによるAPI経済圏支配が標準化のドミナントを起こすと推測される。よって単にセキュリティを組み込むだけでなく、相互接続プログラムのアジャイル化とAPIファーストの経済圏を日本スタンダードにすることを世界No1企業を有する日本の自動車業界等と連携して狙う ・上述のAPI経済のリードから得られるデータ基盤が次世代の競争力になる など、後手ではなく先手をとるなら経済的なモデルを成り立たせる意気込みを追加されるのがよいのではと思いました。	御指摘のとおり、サイバーセキュリティを考える上で、我が国の「経済社会の活力の向上及び持続的発展」も重要であると認識しており、5.1にその旨を掲げています。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
18	－	個人（2）	5.1.1安全なIoTシステムの創出(2)IoTシステムのセキュリティに係る体系及び体制の整備,(3)IoTシステムのセキュリティに係る制度整備	9,10	IoTとして定義した各種機器は「今後」接続されるモノだけではなく、「すでに接続されている」モノが多数ある。 旧来のセキュアではないモノを安全な状態にするための解決策を開発することができれば新しいビジネスとして世界中に展開することも可能であり、産業育成の観点からも意義があると思われるので、慎重に対応する必要がある一方で、今後登場する新しい製品やサービスにおけるセキュリティ強度は一定の基準が必要であり、機能の更新を行うことのできる仕組みが必須であり、標準化と基準の制定とを常に対で提供する必要がある。 もし2020年により安全な環境を実現したいのであれば、速やかに開発および評価の基準とそれらを実現するための標準の策定を行い、事業者および個人を含め、一定のセキュリティを実現することのできないモノの販売や購入、利用の規制も視野に入れる必要があると思われる。 自由であることと、無秩序であることとは同義ではないので、運用と技術開発による新しいサイバーセキュリティの実現の検討をお願いいたします。	御指摘のIoTシステムのセキュリティに係る総合的なガイドラインや基準の整備については、5.1.1(3)において掲げています。具体的な施策については年次計画の中で記載します。 また、5.2.2(3)において、「制御系システム等の調達、運用には高度な専門性が必要とされることから、セキュリティ要件への適合を客観的に判断することが可能である国際標準に即した第三者認証制度の活用を進めていく。」と記載しています。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
19	1	個人（3）	5.1.1安全なIoTシステムの創出 (2)IoTシステムのセキュリティに係る体系及び体制の整備,(3)IoTシステムのセキュリティに係る制度整備	15	サイバー空間の中にも、実社会にあるような以下の観点が必要ではないか ・防犯 ・犯罪者の確保と訴追 ・流れてくる情報の遮断、情報の分析、発信元・有害情報の広がりの特定 ・犯罪発生時の機動的な対応、被害者保護 ・サイバー犯罪者予備軍の監視 現在は、民間人技術者が、国内外の犯罪者の軍隊に近い組織と戦っている現状です。 相手の攻撃手法が、想像を超える量で増えていますし、特定しきれないです。 技術は、オープンな技術を用いるのではなく、クローズドな技術にし、警察国防の技術のように扱い、犯罪者が抜け穴を見つけない施策が必要かと思います。 民間が、技術開発するとどうしても、情報が洩れます。	御指摘のとおり、サイバー空間における防犯、サイバー犯罪対策の強化は極めて重要であると考えています。このため、5.2.1(3)で、サイバー空間の脅威に関する実態把握のための情報収集の強化やサイバー犯罪に係る捜査能力の向上、取締り体制及び取締りのための情報技術解析体制の強化、人材育成や技術開発の着実な推進について記載しています。また、サイバー犯罪に対する事後追跡可能性を確保するため、通信履歴の保存の在り方について、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。 また、クローズドな技術に関しては、5.4.1.(3)において、「また、安全保障の観点等から国として維持することが不可欠な技術もある。このため、公的研究機関や大学等の適切な研究機関において、研究開発を促す環境の整備を着実に進めていく。」と記載しています。
19	2	個人（3）	5.1.1安全なIoTシステムの創出 (2)IoTシステムのセキュリティに係る体系及び体制の整備,(3)IoTシステムのセキュリティに係る制度整備	15	以下の観点での監視も必要かと思います。 ・犯罪者予備軍、犯罪者及びその団体、利用者の保護観点での閲覧サイトの監視 ・流れてくるパケットの監視、犯罪者予備軍のシステムの監視 ・送金やクレジットカード決済のお金の流れの重点的な監視 サイバー交番の設置により、有害サイトの通知、被害の相談連絡ができるようにし、利用者の安心を担保する必要もあります。 サイバー空間でも、国民の生命財産を保護し、世界で一番治安のよい国を目指していただけることを切に望みます。	御指摘のとおり、悪意あるサイバー犯罪の実態を把握し、法令に従って適切に取り締まるとともに、サイバー空間において今後起こり得る新たな手口にも対処できるようにするため、犯罪対処能力・捜査能力の向上が不可欠であると認識しており、5.2.1(3)でその旨を記載しています。 また、利用者の安全・安心を担保するため、情報セキュリティ安心相談窓口や違法・有害サイトの届出窓口等で対応できる人材の育成を進めるべく、5.2.1(2)で、インターネット利用における悩みや不安に関する相談に応じられる人材を育成し、活動を促す取組についても、引き続き着実に推進することとしています。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
20	1	個人（4）	5.4.2 人材の育成・確保 （1）高等教育段階や職業能力開発における社会ニーズに合った人材の育成	34	【意見内容】 「このため、大学院、大学、高等専門学校等の高等教育機関においては、サイバーセキュリティに係る理論・基礎の習得と演習を通じた実践力の強化が求められる。」は文章の趣旨が曖昧です。文章をより明確にすべきです。 【理由】 「実践力の強化が求められる」の主体は誰でしょうか？学生なのか、教職員・研究者なのか。それともカリキュラムや設備、セキュリティポリシといった体制なのか。それらの全てのことなのか。文意がよく理解できません。	御指摘のとおり本文の趣旨が分かりにくいことから、「実践力の強化が求められる。」を「実践力の強化に向けた取組を推進する。」に修文します。
20	2	個人（4）	5.4.2 人材の育成・確保 （3）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	35	【意見内容】 「また、例えばサイバー攻撃に対する対処法（防御手段、攻撃方法も含む）の研究を通じ、自ら考え、対策を検討できる能力の育成を推進する。」の後に、例えば、「育成する人材には、能力を発揮するにあたってプロフェッショナルとしての中立性を維持し、公益に反する欺瞞的な行動を自制できるだけの高い倫理観を付与する」といった文章を追加する。 【理由】 「5.4.2 人材の育成・確保」の節のどこにも「高い倫理観の醸成」が触れられないのは看過できません。「グローバルに活躍できる人材」の育成を目指すなら、育成した人材が「Code of Ethics」を遵守することは必須です（日本はここが特に弱い）。さもなければ、以前に発生した研究不正と同じような状況が発生し、サイバーセキュリティの分野においても国際的な信用を失うことになります。また、人材が公正な視点を失えば、例えば、「世界に通用する技術・ポリシ」ではなく、「自分や自組織に都合の良い技術・ポリシ」が採用され、結果として国内の技術・セキュリティ水準、更には国際競争力が低下する原因となります。	御指摘を踏まえ、5.4.2柱書の最後に「なお、こうした人材においては、技術的な能力のみならず、高い倫理観も同時に身に着ける必要がある。」と追記します。 なお、初等中等教育段階から児童の発達段階に応じて情報セキュリティを含む情報モラルの理解を促すこととしており、5.4.2(2)で「初等中等教育段階から、児童生徒の発達段階に応じて、情報活用の実践力、情報の科学的な理解、情報社会に参画する態度を培う教育を一層推進し、情報セキュリティを含む情報モラルの理解等を促し、論理的思考力や情報通信技術、機器の基本的な仕組み等についての理解を促すようなものとなるよう取り組む。」と記載しています。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
21	－	個人（5）	5.4.1（3）サイバーセキュリティのコア技術の保持	33	【意見内容】 「研究開発を促す環境の整備を着実に進めていく。」に以下を追記、修文。 「研究開発を促す環境の整備を着実に進めていくとともに、その研究成果を国や公的研究機関が積極的に活用することによってセキュリティ産業育成のための初期マーケットを創造することが必要である。」 【理由】 国家プロジェクトの研究成果を産業化するためには、新しいものを積極的に活用して初期マーケットを創出することが重要である。セキュリティは国防と同じで、国は率先してその市場を作り出すべきである。	研究成果の産業化等の社会還元の推進は重要と考えます。そのため、5.4.1(1)で「サイバーセキュリティの研究開発は社会的なニーズを踏まえ実用化されることが重要であり、研究成果の社会還元の推進が重要である。」と記載するとともに、関係者間での必要となる情報・データの共有に向けた取組を推進することとしており、原案のとおりとします。 また、5.1.3(1)において「サイバーセキュリティ関連産業の振興」として「研究開発成果を活用したベンチャー企業の育成」等に取り組むこととしています。
22	－	個人（6）	5.2.3 政府機関を守るための取組	21-23	政府機関又は政府機関から委任・委託を受け業務を行う特殊法人は、監査法人による金融監査と同様に、セキュリティ監査を行うように義務づけるようにお願い致します。	御意見を踏まえ、5.2.3に「(4)」として、以下のとおり追加いたします。 (4) 監視対象の拡大等による総合的な対策強化 政府機関全体としてのサイバーセキュリティを強化するため、独立行政法人や、府省庁と一体となり公的業務を行う特殊法人等における対策の総合的な強化を図る。 具体的には、当該法人におけるインシデント対処能力の向上や所管省庁による当該法人への監査の強化等を図るほか、当該法人におけるサイバーセキュリティに関する取組について、法人の特性等を踏まえつつ、政府機関の取組（上記(1)から(3)まで）に準じて推進する。とりわけ、当該法人について、公平な受益者の負担に留意しつつ段階的にGSOCの監視対象に追加するほか、サイバーセキュリティ戦略本部がNISCに実施させる監査及び原因究明調査の対象とする等の施策を推進する。また、本対策強化に際しては、専門的知見を有する関係法人との連携体制の整備を図ることを含め、所要の法改正について速やかに検討を行い、必要に応じて措置する。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
23	1	個人（7）	5.1.1 安全なIoTシステムの創出 (1)安全なIoTシステムの創出	9	【意見内容】 「このため、システムの企画・設計段階からセキュリティの確保を盛り込むセキュリティ・バイ・デザイン（Security By Design）の考え方を推進する。」の後に以下を追記する。 「製品設計においては、ハードウェア機能とソフトウェア機能およびそれらの協調によるセキュリティ性能を重視する。」を追記する。 【理由】 セキュリティ・バイ・デザインの具現には、製品のセキュリティ性能を付加価値として市場が認める必要があるため。	御指摘の製品のセキュリティ性能を付加価値として市場が認めることについては、5.1.2(3)に、企業における製品・サービスの関係者がセキュリティ・バイ・デザインを共通の価値として認識することを促していく旨を記載しており、この中に御指摘の考え方も含まれているものと考えることから、原案のとおりとします。
23	2	個人（7）	5.1.1 安全なIoTシステムの創出 (4)IoTシステムのセキュリティに係る技術開発・実証	11	【意見内容】 「このため、テスト環境の構築や、システム全体の脅威分析・リスク評価手法の開発、ICチップを含むハードウェアの真正性の検証等、」に追記し、以下のとおり修文する。 「このため、テスト環境の構築や、システム全体の脅威分析・リスク評価手法の開発、ICチップを含むハードウェアの真正性の検証やセキュリティ性能の定量評価等、」 【理由】 ハードウェアセキュリティを担うICチップについて、真正性の検証のみならず、そのセキュリティ性能を定量的に評価する手法も技術開発が必要であるため。	御指摘のセキュリティ性能の定量評価につきましては、5.1.1(4)の「ICチップを含むハードウェアの真正性の検証等」に含まれる内容であると考えており、原案のとおりとします。
23	3	個人（7）	5.1.3 セキュリティに係るビジネス環境の整備	14	【意見内容】 脚注8「機器やシステムの設計・製造・調達・設置・運用段階におけるリスクであって、これらの段階においてウィルスを含む悪意のあるプログラムを埋め込まれるなどのリスクを含む。」に追記し、以下のとおり修文する。 「ICチップおよびその応用機器やシステムの設計・製造・調達・設置・運用段階におけるリスクであって、これらの段階においてウィルスを含む悪意のあるプログラムを埋め込まれるなどのリスクを含む。」 【理由】 米国・欧州ではセキュリティ機能を有するICチップの改竄が潜在的リスクとして既に社会課題となっているため。	御指摘を踏まえ、脚注8の「機器」を、「機器（ICチップを含む。）」に修文します。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
23	4	個人（7）	5.3.2 国際社会の平和・安定 (5)国際的な人材育成	29	【意見内容】 「このため、このような人材には、サイバーセキュリティに関する十分な知識とともに、各国の社会・経済・文化等の状況についての理解も求められる。」に追記し、以下のとおり修文する。 「このため、このような人材には、サイバーセキュリティおよびハードウェアセキュリティに関する十分な知識とともに、各国の社会・経済・文化等の状況についての理解も求められる。」 【理由】 国際的な人材育成においては、サイバーセキュリティはもちろん、セキュリティ機能を有するICチップとその応用制御機器等のハードウェアについても十分に理解している人材が必要であるため。	御指摘のハードウェアのセキュリティに関する知識は、サイバーセキュリティに関する知識に含まれると考えており、原案のとおりとします。
23	5	個人（7）	5.4.1 研究開発の推進 (3)サイバーセキュリティのコア技術の保持	33	【意見内容】 「特に、コア技術を育む基礎研究については、暗号研究のように、直ちにビジネスにつながらないものの、経営力、事業開発力のある者との連携により、新たな産業創出の種となるものであり、また、安全保障の観点等から国として維持することが不可欠な技術もある。」の後に以下を追記する。 「国際的な市場競争力の高いセキュリティ機能・性能を具体化するハードウェアセキュリティ技術の研究も極めて重要である。」 【理由】 サイバーセキュリティ技術の研究開発において、わが国が国際的に先導的な立場にあるために、通信ネットワークなどの基本機能を担う日本製ハードウェアにおけるセキュリティ性能を十分に高め、国際市場に広く流通する必要があるため。	御指摘を踏まえ、5.4.1において以下のとおり修文します。 「さらに、サイバー攻撃は日々進化し高度化・複雑化しており、その変化に対処していくため、ネットワーク、ハードウェア、ソフトウェア等の幅広い分野において、創意と工夫に満ちたサイバーセキュリティ技術を生み出すための充実した研究開発の推進が不可欠である。」

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
24	－	個人（8）	－	－	マイナンバー制度ネットワーク構築について。もっとも重要なことは、セキュリティ対策です。導入時初期にあっては「送受信分離・人介在システム」としてください。 私の意見は、新規なものではなく、たとえば学校では「成績」「給与」「汎用」のように、はっきり独立のLANが構築されていました。また成績LANは昔はフロッピーディスクで教員から提出される形式でした。最近はすべてネットで、処理するところに、運用上の不備が生じています。なぜ不備が発生するかといいますと、この20年間を振り返っても、コンピュータの性能が、ハード・ソフト両面で1000倍以上向上したからです。 私は、今後も、この技術革新は続くと思います（専用化・並列化・物性的・材料・製造技術など）。したがって、私が述べた、一見、陳腐な意見でも、担当者、責任者、利用者に、簡単、明確、明瞭に、その運用の要点を説明・納得できるようにしておくべきだと思います。その延長上に、さらなる自動化があると思います。	御指摘のとおり、マイナンバー制度におけるセキュリティの確保が重要であると認識しており、5.2.2(3)において以下のとおり修文します。 「マイナンバー法における個人番号利用事務において使用するシステムについて、インターネットから独立する等の高いセキュリティ対策を踏まえたシステム構築や運用体制整備を含めて検討の上、必要な措置を講ずるとともに、関係機関が連携し専門的・技術的知見を有する監視・監督体制を整備する。」
25	1	個人（9）	２．２　サイバー空間における脅威の深刻化	2	【意見内容】 サイバー脅威の認識として、論理攻撃が中心でネットワーク阻止攻撃としての電磁パルス(ElectroMagnetic Pulse: EMP)脅威が挙げられていないため、次の記述を追加されたい。「さらに、サイバー空間に巨大な脅威を及ぼす蓋然性の高いEMP脅威としては、①人工的EMP攻撃、特に小型の超EMP核兵器を用いた高々度電磁パルスによる電力網および電子機器の破壊、並びに②太陽活動がもたらす巨大な磁気嵐による電力網の破壊がある。」 【理由】 EMP脅威について、国家指導者が十分に認識し、政府機関および電力網を中心とした重要インフラのシステム防護のための態勢を優先的に整備する必要がある。	御指摘のEMP（電磁パルス）による脅威については認識しておりますが、当該箇所については、脅威を網羅的に挙げることとしていないため、原案のとおりとします。 なお、「情報セキュリティ研究開発戦略（改定版）」（2014年7月 情報セキュリティ政策会議決定）P.27 6.(1)①にEMP（電磁パルス）による脅威について記載しています。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
25	2	個人（9）	3. 目的（3）戦略において目指す日本の姿	4	【意見内容】 「実空間と融合したサイバー空間を活用していくためには、利便性の裏に潜む脅威に的確に対処できることが必要不可欠であり、高付加価値を創出するための「投資」が必要となる。」を以下のとおり修文する。 「実空間と融合したサイバー空間を活用していくためには、利便性の裏に潜む脅威に的確に対処できることが必要不可欠であり、高付加価値を創出するための「セキュリティ投資」が必要となる。」 【理由】 「投資」の意味がわかりにくい。	御指摘の箇所については、一般概念としての「投資」を記載していることから、原案のとおりとします。なお、セキュリティに関する投資の考え方については5.1に記載しています。
25	3	個人（9）	５．１．１（１）安全なIoTシステムを活用した新規事業の振興 ５．１．１（４）IoT システムのセキュリティに係る技術開発・実証	9,10	【意見内容】 情報システムよりも高い品質をIoTシステムに要求する場合、数学的に脆弱でないことを保証できる革新的なソフトウェア構築技術によりOS、通信プロトコル、アプリケーション等のソフトウェアをゼロから開発すべきである。米国のDARPAは、脆弱性のない高い保証された組み込みシステム構築技術開発のためのHigh Assurance Cyber Military System(HACMS)プログラムを産官学で推進している。 【理由】 情報システムでは、セキュリティ・バイ・デザインによる脆弱性の低減は普通の考え方であるが、この考え方を導入しても統計的品質管理の基づくソフトウェア開発方法である限り脆弱性をゼロにすることはできない。ソフトウェアの脆弱性をゼロにするためには、従来のソフトウェア構築技術と異なる革新的なソフトウェア構築技術を開発する必要がある。	5.1.1(4)において、「IoTシステムの構成要素の特徴を加味した情報通信技術の開発・実証事業を行う。」と記載しており、御指摘の内容については、今後の施策の検討に当たっての参考とします。 なお、脆弱性を作りこまないためのソフトウェア開発技術の必要性については、「情報セキュリティ研究開発戦略（改定版）」（2014年7月 情報セキュリティ政策会議決定）P.32 6.(2)の「⑦ソフトウェアの安全性確保」に記載しています。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
25	4	個人（9）	5．2　国民が安全で安心して暮らせる社会の実現	15	【意見内容】 「リスクを分析し、協議し、残存リスクの情報も添えて経営者層に対し総合的な判断を受ける機能保証（任務保証）の取組が必要である。」の後に、以下のとおりサイバー空間に巨大な影響を及ぼす蓋然性の高い人工的EMP脅威に関する記述を追加する。 「さらに、サイバー空間に巨大な影響を及ぼす人工的EMP脅威に対応するために、政府機関および電力網を中心とした重要インフラの具体的な防護の取組が必要である。」 【理由】 EMP脅威について、国家指導者が十分に認識し、政府機関および電力網を中心とした重要インフラのシステム防護のための態勢を優先的に整備する必要がある。	御指摘のEMP（電磁パルス）による脅威については認識しておりますが、当該箇所については、脅威を網羅的に挙げることとしていないため、原案のとおりとします。 なお、「情報セキュリティ研究開発戦略（改定版）」（2014年7月 情報セキュリティ政策会議決定）P.27 6.(1)①にEMP（電磁パルス）による脅威について記載しています。
25	5	個人（9）	5．2．3（1）ii. 被害の発生・拡大の防止	22	【意見内容】 「政府機関横断的な監視・即応機能及び各機関における事態の把握・対処機能の強化に取り組むとともに、」を以下のとおり修文する。 「迅速なセキュリティリスク管理を行うために各機関における情報システムのセキュリティ状態（脅威、情報資産の脆弱性およびセキュリティ設定の脆弱性）の常時監視および任務保証のリスク評価／可視化並びに政府機関横断的なリスク評価／可視化に取り組むとともに、」 【理由】 APT攻撃は、作文的な対策では対応できないため実効性のある対策を導入すべきである。今回の社会保険機構のようなAPT攻撃事案発生時に政府機関トップの適時および適切な状況認識と判断支援をするためにリアルタイムなセキュリティリスク管理の仕組みを政府機関および関連機関が導入すべきである。そうしなければ、情報セキュリティ予算は国家予算の無駄遣いになる。	ご指摘の内容については、5.2.3(1) ii .の「GSOCによる政府機関全体における検知・解析機能の強化、並びに各機関におけるインシデント対応を行うチーム（CSIRT）の体制及び事態の把握・対処機能の強化、インシデント発生時の情報提供の迅速化・高度化に取り組む」、5.2.3(2)の「リスク評価に基づく組織的な情報システムの対策・管理の推進」、6.の「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高度な情報分析・集約・共有機能を有する体制を整備する」に含まれていると考えています。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
25	6	個人（9）	5.3.1 我が国の安全の確保	25	【意見内容】 「こうした認識を多様な関係主体間で共有した上で、これまでの連携を一層強固にし、切れ目のない重層的・多層的な防護を実現する。」を以下のとおり修文する。 「こうした認識を多様な関係主体間で共有した上で、これまでの連携を一層強固にし、各主体がリアルタイムのセキュリティリスク管理ができる態勢を実現する。」 【理由】 国家を主体としたゼロデイ脆弱性を用いたAPT攻撃に対して、現状の防御技術による政府や重要インフラ等が有している社会システムに重層的・多層的な防護を行っても完全な防護は不可能である。したがって、現状の防御技術を前提とした場合、サイバー攻撃に対してリアルタイムのセキュリティリスク管理のできるセキュリティ常時監視および任務保証のリスク評価／可視化が必要である。	御指摘の内容については、5.3.1において、「様々な主体によるサイバー攻撃の兆候を含む状況を早期に認識・把握し、問題点を検知して対応する能力の一層の向上を図っていく」と記載しておりますが、ご指摘を踏まえ、以下の通り修文します。 「様々な主体によるサイバー攻撃の兆候を含む状況を早期に認識・把握し、問題点を検知して迅速に対応する能力の一層の向上を図っていく」
25	7	個人（9）	5．3．1（3）政府機関・社会システムの防護	26	【意見内容】 「防衛当局である防衛省・自衛隊においては、自らが保有するネットワーク・インフラの防護を引き続き強化するとともに、上記の社会システムに対するサイバー攻撃も、任務遂行上の大きな阻害要因となる可能性を踏まえ、自衛隊の任務保証に関連する主体と連携を深化させていく。」を以下のとおり修文する。 「防衛当局である防衛省・自衛隊においては、自らが保有するネットワーク・インフラのリアルタイムなセキュリティリスク管理態勢を整備するとともに、上記の社会システムに対するサイバー攻撃も、任務遂行上の大きな阻害要因となる可能性を踏まえ、自衛隊の任務保証に関連する主体にもセキュリティリスク管理態勢を義務づける調達制度に深化させる。」 【理由】 APT攻撃は、作文的な対策では対応できないため実効性のある対策を導入すべきである。今回の社会保険機構のようなAPT攻撃事案発生時に政府機関トップの適時および適切な状況認識と判断支援をするためにリアルタイムなセキュリティリスク管理の仕組みを政府機関および関連機関が導入すべきである。そうしなければ、情報セキュリティ予算は国家予算の無駄遣いになる。	防衛省・自衛隊のネットワークは現在24時間体制で実施しており、リアルタイムでのセキュリティ監視体制を敷いています。 また、自衛隊の任務保証に関連する主体とは、御意見も踏まえ、連携を深化させていきます。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
25	8	個人（9）	5．4．1（1）サイバー攻撃の検知・防御能力の向上	32	【意見内容】 「また、政府が推進する研究開発プロジェクトにおいて、研究開発の企画段階からサイバーセキュリティを組み込むなど、防御能力の向上を進める。」を以下のとおり修文する。 「また、政府が推進する研究開発プロジェクトとして、脆弱性のないソフトウェア構築技術開発に取り組むなど、防御能力の革新的向上を進める。」 【理由】 国家を主体としたゼロデイ脆弱性を用いたAPT攻撃に対する防御能力の向上には、サイバー攻撃に対する強靭性向上と脆弱性のないソフトウェア構築技術の開発の2つのアプローチがある。前者については、本戦略案においても挙げられているが、後者については挙げられていない。攻撃者優位のサイバー空間の状況を変えるためには、政府の推進する研究プロジェクとして、APT攻撃を不可能にする革新技術としての「脆弱性のないソフトウェア構築技術開発」に取り組むべきである。特に、無人機、自動走行自動車、ロボット等の人命に係わるIoTシステムのソフトウェア開発には必須である。米国のDARPAは、脆弱性のない高い保証された組み込みシステム構築技術開発のためのHigh Assurance Cyber Military System(HACMS)プログラムを産官学で推進している。	御指摘の内容は、研究開発プロジェクトにシステムの企画・設計段階からセキュリティの確保を盛り込むことの重要性を述べているものであり、趣旨が異なること、またソフトウェアの脆弱性に関する課題に限らないことから、原案のとおりとします。 なお、脆弱性を作りこまないためのソフトウェア開発技術の必要性については、「情報セキュリティ研究開発戦略（改定版）」（2014年7月 情報セキュリティ政策会議決定）P.32 6.(2)の⑦ソフトウェアの安全性確保に記載しています。
26	1	個人（10）	全般	－	【意見内容】 一昨年策定された現戦略においては、特定省及びその所管法人色の濃さを感じさせ、各省の関連白書の一部抜粋と見まがう部分も散見されたが、今回の戦略では、各省間でのバランスが取れ、かつ相互に整合し総合された内容になっており、全省庁的な取組を示す戦略になっている。法的根拠（サイバーセキュリティ基本法）に基づくNISC殿のリーダーシップに拠るものと理解する。 【理由】 本文全般をサーベイしての率直な感想である。	本案に賛同する御意見として承ります。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
26	2	個人（10）	5.2.1(3)サイバー犯罪への対策	17,18	【意見内容】 サイバー犯罪に係る現状及び見通しを踏まえた、現行法制の必要十分性の検証による現法令の見直し・強化、要すれば新たな法制度の整備を行うことを明確に謳うべきと考える。 【理由】 原案では、「法令に従って適切に取り締まる」こと、「犯罪対処能力・捜査能力の向上」が不可欠としているが、新たな法整備どころか、現法令の見直し・強化にすら踏み込んでいないように見える。	本戦略は、今後3年程度の基本的な施策の方向性を示すものであり、その施策の実現に当たり必要がある場合には、法制度の整備等についても検討します。
26	3	個人（10）	5.2.2(2)効果的かつ迅速な情報共有の実現	19,20	【意見内容】 「情報源の秘匿」や「共有範囲の設定など適切な加工を行う」だけでは真に有意な情報の収集は困難であることから、現実的な対応としては、カルテル等におけるリニエンシー制度並みとは行かないまでも、有意な（提供主体にとっては不利な）情報を提供した場合の提供者への具体的なインセンティブを提示し、法的に担保すべき（その旨を記載すべき）である。 【理由】 真に有意な情報（提供側にとっては不利な情報）を民間企業等の側から本気で得ようとする場合、民間企業等にとって具体的かつ法的に担保されたメリットが必要である。	本戦略は、今後3年程度の基本的な施策の方向性を示すものであり、その施策の実現に当たり必要がある場合には、法的な担保等についても検討します。
27	1	個人（11）	「5.1.2(3) 組織能力の向上」 「5.2.2重要インフラを守るための取組」	12,18	セキュリティ要件への適合を国際標準に即した第三者認証制度の活用を進める場合、CC（Common Criteria）、JCMVPといった既存の第三者評価制度も、積極的に活用することを明記していただきたい。例えば、IoTのPP（Protection Profile）を作成することで、既存のCC評価フレームワークを活用することができると考えます。	本戦略は、今後3年程度の基本的な施策の方向性を示すものであり、第三者認証制度の活用の際には、当然のことながら、国際標準や既存の制度の活用も踏まえたものとします。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
27	2	個人（１１）	「5.2.3(1)i インシデントの未然防止」	22	送信ドメイン認証（DKIM等）や暗号技術を利用したS/MIME等の対策を積極的に推進していただきたい。	御指摘の内容については、従来から取り組んでいるところであり、今後も引き続き推進していきます。
27	3	個人（１１）	「5.1.1(4) IoTシステムのセキュリティに係る技術開発・実証」 「5.4.1(3)サイバーセキュリティのコア技術の保持」	10	安全なIoTシステム」を計測する「安全性評価技術」の研究開発や評価体制の強化を継続的に推進していただきたい。例えば、暗号技術であれば、直ちにビジネスにつながらない「安全性評価技術=解読技術」の研究開発に対する支援や客観的に安全性を評価する体制（CRYPTREC）を維持していただきたい。	御指摘の内容に関し、5.4.1(3)において、「コア技術を育む基礎研究については、暗号研究のように、直ちにビジネスにつながらないものの、経営力、事業開発力のある者との連携により、新たな産業創出の種となるものであり、また、安全保障の観点等から国として維持することが不可欠な技術もある。このため、公的研究機関や大学等の適切な研究機関において、研究開発を促す環境の整備を着実に進めていく」としています。 また、暗号化技術の安全性評価体制（CRYPTREC）の維持については、「情報セキュリティ研究開発戦略（改定版）」（2014年7月 情報セキュリティ政策会議決定）の6⑫暗号技術　などで記載しており、引き続き推進することとしています。
27	4	個人（１１）	「5.2.1(2)サイバー空間利用者の取組の促進」	16	本サイバーセキュリティ戦略を推進する上で、サイバー空間における民間事業者・団体や、地方公共団体、公的機関の自らを特定するための基本情報（WebサイトのURL、英字名称など）に対して、国民がいつでもアクセス可能な情報基盤の整備を進めていただきたい。 そのため、5.2.1(2)に、「また、民間事業者・団体や、地方公共団体、公的機関が、自らWebサイトアドレス、法人番号等の基本的な情報を国民に提供可能とする基盤の整備を推進する。」と追加していただくことを提案します。	御指摘の内容については、普及啓発などの今後の施策の検討に当たっての参考とします。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
27	5	個人（１１）	「6. 推進体制」について	37	サイバーセキュリティ戦略本部の位置付け・役割を明確に位置付けていただきたい。 分野ISACやC-CERT、JPCERT/CC、警察・防衛省を含めたインシデント情報の共有体制も明示していただきたい。	御指摘のサイバーセキュリティ戦略本部の位置付けや役割については、サイバーセキュリティ基本法（平成26年法律第104号）に定められています。 また、本戦略は、今後3年程度の基本的な施策の方向性を示すものであり、個別の組織や団体の役割や関係性を記載するものではないため、原案のとおりとします。