「サイバーセキュリティ2015（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
- 実 施 期 間： 2015年８月20日（木）～ ９月３日（木）
- 意 見 総 数： 30者から105件 【内訳：10企業・団体から延べ54件、20個人から延べ51件】

（１）賛同意見： 全３件

（２）修正意見： 全33件

- 表現の明確化や適正化などを求めるものについては、必要に応じて趣旨を踏まえて修正（全６件）
- 戦略で言及しているなどの理由で原案どおりとする意見については、理由を付して回答（全27件）

（３）政策展開に係る意見： 全66件

- 今後の政策展開に係る意見については、当センターとしての考え方及び当該意見を今後の参考にする旨を回答

（４）その他意見： 全3件

注）提出された意見は必ずしも明確にこれらに分類されるものではないが、事務局で理解した区分にて計上している

- （参考）提出者名：

イクシアコミュニケーションズ（株）、日本アイ・ビー・エム（株）、NPO法人 ウェブアクセシビリティ推進協会、日本オラクル（株）、（一社）日本オンラインゲーム協会、（株）ラック、BSA | ザ・ソフトウェア・アライアンス、（一社）新経済連盟、NPO法人 日本ネットワークセキュリティ協会、（一社）重要生活機器連携セキュリティ協議会、個人（20）

「サイバーセキュリティ2015（案）」に対する意見募集の結果

意見募集期間 ： 2015年8月20日（木）から同年9月3日（木）まで

30者　105件

通し番号	提出者	枝番	該当箇所		概要	意見の種類	御意見に対する考え方及び修正内容
			ページ	章節項			
1	個人（1）	－	－	2.2. (3)	社会保障番号制度のシステム導入は、区域分けをすると良いのではないか。 入札は全国8ブロックを2ブロックずつの4区画に分けて行い、4企業で社会保障番号制度を管理。 システムダウンさせたときのペナルティ料金を設定し、システム障害はアトサイト対応で翌日までの普及が必須条件。 [理由] ・社会保障番号制度のシステム導入で揉めているのと推察される。 ・ひとつの企業に絞るのはリスクが大きく、相互チェックにしたほうが良い。	その他	「社会保障番号制度のシステム導入」が具体的に何を指すのか明らかではないですが、具体的なシステム設計については本意見募集の対象外です。 なお、関連の入札については、意見招請等の所要の会計手続きを経て行うとともに、可用性やセキュリティの確保についても、十分に配慮した上で調達を行っています。
2	個人（2）	－	－	2.2. (3) 2.3.	インフラだけでなく業務プロセスにおけるセキュリティリスクを考慮して頂きたい。 例えば、マイナンバーを含むファイルを添付しメールで送信する事を禁止することや、マイナンバーを含むファイルは暗号化されている等の対策が必要。 また、業務システム開発時においても、システムの利用マニュアルを充実させ、業務プロセスにおけるセキュリティリスクを軽減するようにお願いしたい。 [理由] ・昨今、業務プロセスにおけるセキュリティリスクを考慮していないために、情報漏えい事件が発生している事象が多々見受けられる。	政策展開に係る意見	政府機関における業務プロセスにおけるセキュリティリスクを考慮した取組については、2.3. (1) (ツ)において更なる強化等を図ることとしております。また、特定個人情報の適正な取扱いに関するガイドライン(行政機関等・地方公共団体等編)においても御指摘いただいたセキュリティリスクを盛り込んでおりますが、今般さらに当ガイドラインの(別添)安全管理措置において、以下の事項等を追加し、運用面における対策を講ずるよう改正手続を進めております。 ・「情報漏えい等事案に対応」して、体制に加え、手順等を整備すること ・「不正アクセス等による被害の防止等に対応」して、個人番号利用事務において使用する情報システムについて、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行うこと ・「情報漏えい等の防止に対応」して、特定個人情報ファイルを機器又は電子媒体等に保存する必要がある場合、原則として、暗号化又はパスワードにより秘匿すること
3	個人（3）	－	P.28	4.2. (4) (イ)	「情報セキュリティマネジメント試験（仮称）」にも、現状の情報セキュリティスペシャリストと同程度の技術問題（午前1,2,午後1までが妥当か？）を用意し、その上で、セキュリティポリシーに関する問題を用意すべき。 それにより、情報セキュリティ対策を進めるうえでの基礎となる技術スキルが付き、ポリシー作成のスキルにも深みが出る。 基礎となる技術スキルが無くとも合格できるような、実用的でない資格にはしないでいただきたい。 [理由] ポリシーの作成に於いて必要なスキルは、システム開発経験、セキュリティ経験、ネットワーク経験、法務、等の専門的なテクニカルなスキルが基礎として求められるが、セキュリティの人材が不足していることから、セキュリティ前述の各種スキル・経験の無い人材がポリシー作成担当者として割り当てられ、運用に耐えられないポリシーや各種規定を作成してしまうことが見受けられる。	政策展開に係る意見	「情報セキュリティマネジメント試験（仮称）」では、組織のセキュリティポリシーの運用等に必要となる知識を問う内容とする予定ですが、より良い試験となるよう、引き続き検討してまいります。
4	個人（4）	－	－	1.1. 2.1.	IoTのセキュリティバイデザインの指針は既に公表されているのか、あるいはNISCがこれから策定するのか。この点を明確にしていただきたい。 また、既設のIoTシステムに対する見直しの方が重要であると考えられるが、この点はどうするのか？2020年に向けて最も脆弱となるシステムは、既設の長寿命のシステムである。	政策展開に係る意見	IoTのセキュリティに係る総合的なガイドラインを今後策定する予定です。 IoTについては、連携される既存システムを含めて、設計段階から脅威を考慮に入れる「セキュリティ・バイ・デザイン」を重視するとともに、経営層の意識改革による対策見直しの促進や、利用者へ注意喚起する仕組み等についても検討する方針です。
5	個人（5）	－	－	全般	各論に対する総論がなく、それぞれの省庁の取り組みが、サイバーセキュリティ戦略に対して必要十分なのかが理解できない。 それぞれの取り組みがサイバーセキュリティ戦略のどこに対応するものなのか、2015年度の目標値として十分なのかを示す資料を公表されたい。	その他	本案はサイバーセキュリティ戦略の体系に沿って2015年度に実施する施策を取りまとめたものであり、実施の主体を明確化しておくことは重要であると考えています。 今後、サイバーセキュリティ政策に係る新たな評価方針を策定、公表した上で、当該方針に基づき評価を毎年度実施し、取組が十分であるかどうかを確認しつつ、各種施策を推進していく予定です。

通し番号	提出者	枝番	該当箇所		概要	意見の種類	御意見に対する考え方及び修正内容
			ページ	章節項			
6	個人（6）	―	P.14	2.2.（3）（イ）	「情報提供ネットワークシステム等のマイナンバー関係システムについて、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が講じられたものとなるよう、管理・監督・支援等を行う。」とあるが、これは、個人番号利用事務等を含めた、マイナンバーを取り扱うすべてのシステムを対象としていると言う意味で、非常に賛成できる。NISCが中心となり、政府から一つもマイナンバーが漏れぬよう、対策されたい。	賛同意見	本案に賛同する御意見として承ります。 政府機関の対策についても万全を期すべく、各種施策を推進してまいります。
7	個人（7）	―	P.14	2.2.（3）（ウ）	マイナンバー制度の下で認証連携を行うに当たって、利便性の向上とセキュリティの確保がバランスの取れたものとなるよう、政府内及び官民での認証連携について、多要素認証等の認証方式や連携条件についての検討を行い、本年中を目途に取組方針を策定する。 この記載は、マイナンバー法に違反しているように読めるが内容如何。	その他	認証連携の方式は、現在検討しているところですが、当該記述の認証連携の方式については、マイナンバーそのものを利用することを前提としているものではありません。
8	個人（8）	―	P.15	2.2.（3）（カ）	制御システム全体のセキュリティ認証制度を確立するとあるが、具体的な内容如何。また、EDSA認証は重すぎるため、もっと軽い認証制度を国の補助の元に確立すべき。	政策展開に係る意見	CSSC（技術研究組合制御システムセキュリティセンター）において、「制御システム全体のセキュリティ認証制度」として、複数デバイスを組み合わせたシステムにおける認証制度であるSSA認証（System Security Assurance）の確立に向けた取組を実施しています。 また、認証制度にかかるニーズは、求めるセキュリティレベル等によっても異なることから、御意見の内容につきましては、今後の取組の検討に当たっての参考とさせていただきます。
9	個人（9）	―	―	全般	各府省庁が実施するとされている事柄について、内容に重複や抜け漏れ等がないように、NISCが横断的に内容を確認すべき。	政策展開に係る意見	本案は、NISCが横断的な調整を行い、各府省庁の重複排除や連携推進を行いつつ、2015年度に実施する施策を取りまとめたものです。今後もNISCが総合調整機能を果たし、全体最適化に努めてまいります。
10	個人（10）	―	P.25	4.1.（エ）	「2020年頃の実現を視野に」という文言は不要。 ［理由］ ・基盤技術の研究開発は、一定の期限を区切って行うというより、常日頃から積み重ねるものであって、成果が現れ次第、既存のネットワークに徐々に取り入れていけばよい。	修正意見	NICTにおいては、一つのマイルストーンとして2020年頃の実現を視野に新世代ネットワークの基盤技術の研究開発を推進しているところであるため、原案通りとさせていただきます。
11	イクシアコミュニケーションズ（株）	―	―	2.3.	標的型攻撃を含む外部からのネットワーク攻撃の脅威を検知・分析・防御するために、高度な専門知識を持つサイバーセキュリティの専門家育成が必要である。 防災訓練、避難訓練と同様に、サイバー攻撃をシミュレーションし、実際に次のアクションを判断・実行するための環境を提案する。	政策展開に係る意見	サイバー攻撃への対処に当たっては、御意見のとおり、座学のみならず、訓練・演習も重要と認識しており、2.3.（ス）において訓練・演習の実施を盛り込んでいるほか、体制整備や人材育成等を含め、多角的に取り組むこととしております。御意見については、これらの取組を推進するに当たり、参考とさせていただきます。
12	個人（11）	1	P.9	2.1.（2）（エ）	現在の利用規模が想定より小さいのであれば、現行の制度・システム自体に利活用を阻害する要因が存在するのでは、という観点からも検討をするべきではないか。	政策展開に係る意見	御意見の内容につきましては、今後の取組の検討に当たっての参考とさせていただきます。
13	個人（11）	2	P.11	2.1.（2）（ナ）	IPAや経済産業省の公式ページを日常的にチェックする人は少ないと思われる。より多くの国民に情報が届き、活用されるよう、普及・広報の方法は工夫されたい。	政策展開に係る意見	普及啓発活動においては、イベント・セミナーの開催やポスターの活用等も行っています。引き続き、国民の方々に広く知っていただけるように取り組んでいきます。
14	個人（11）	3	P.12	2.1.（3）（コ）	いわゆるサイバー刑法の運用については警察も当事者であるため、警察庁も関係機関として明記すべきではないか。 また、「適正な運用」の内容が不明確であるところ、証拠物品の取扱いに関する不祥事が発生している現状を鑑み、漏えい、改ざん、遺棄その他の証拠物品の不適切な取扱いの予防と事後検証を可能にする管理体制の構築が必須であり、そのために必要な検討を行うべきである。	修正意見	御意見を踏まえ、「検察当局及び都道府県警察において」と修文しました。なお、証拠物品に関する管理体制に関する御意見につきましては、今後の施策の検討に当たっての参考とさせていただきます。
15	個人（11）	4	P.15	2.3.	文書管理における電子データの取扱いの重要性が一層高まることに鑑み、公文書管理法の施行五年後の見直しにおいて、サイバーセキュリティの観点からの検討・検証を行えるよう、必要な情報収集や論点の整理などの準備をすべきではないか。	政策展開に係る意見	御意見の内容につきましては、今後の取組の検討に当たっての参考とさせていただきます。
16	個人（11）	5	P.15	2.3.（ア）	政府統一基準の次期改定の予定時期が決まっているのであれば、その時期を記載してはどうか。	修正意見	新たな脅威や課題については、いつ発生し、その課題への対応がどの程度必要となるかは判りません。よって、年次計画に改定時期を掲げることは馴染まないと考えており、原案のとおりとさせていただきます。
17	個人（11）	6	P.15 P.19	2.3.（1）（ウ） 3.1.（2）（ア）	今後調達されるシステムについてのみならず、現在調達中、および調達済みの情報システムや関連機器についてもサプライチェーン・リスクやトレーサビリティの調査をすべきではないか。	政策展開に係る意見	2.3.（1）（ウ）における「サプライチェーン・リスク」への対応は、システム調達時だけではなく、調達済みシステムの運用業務に係る外部委託の際にも適用されるものと考えております。御意見については、今後の取組の参考とさせていただきます。

通し番号	提出者	枝番	該当箇所		概要	意見の種類	御意見に対する考え方及び修正内容
			ページ	章節項			
18	個人(11)	7	P.17	2.3. (1) (ツ)	政府統一基準群のみならず、各府省庁の関連する内部規則(行政文書管理規則、特定秘密保護規程など)それぞれについて、各種対策の強化に応じた改訂がなされるよう検討すべきではないか。	政策展開に係る意見	行政文書管理規則、特定秘密保護規程等の各府省庁の内部規則については、それぞれ個別の法令や基準等に基づき規定されており、各種対策の強化に応じた改定については、それらの法令等の改正等の際に行政機関間で連携することにより対応しております。御意見については、引き続き行政機関間の連携を図る上での参考とさせていただきます。
19	個人(11)	8	P.26	4.1. (2) (ア) 4.2. (1)	融合領域の研究促進にあたっては、同時に専門的な人材育成をも行うという観点から、法科大学院や公共政策大学院との連携も併せて推進対象として明示すべきではないか。	修正意見	御指摘の内容については、今後の取組の検討に当たっての参考とさせていただきます。
20	個人(11)	9	―	全般	英字略語については、初出のときに必ず正式名称を併記するとともに、全て用語解説で説明を加えるよう修正を求める。	修正意見	御指摘の点につきましては、用語解説に記載することとしています。
21	個人(11)	10	―	全般	各用語について、本文では表記を統一するよう修正を求める。例えば、「セキュリティ・バイ・デザイン」を「SBD」と略すことがある旨は用語解説を読まなければわからず、本文だけではこの二語が同一概念とわからない。	修正意見	御意見を踏まえ、「SBD」を「セキュリティ・バイ・デザイン」へ修正しました。
22	個人(11)	11	―	全般	各項目記載の検討事項について、審議会や有識者会議など、検討を行う会議体が確定している又は既に検討が始まっている場合は当該会議体名称を明記するよう修正を求める。(例:4.2.(ウ)の「産業構造審議会商務流通情報分科会情報経済小委員会IT人材WG」)	修正意見	本年次計画は、施策の内容を主として説明するものであり、また、施策の検討の場は複数の会議にまたがったり、都度見直されることなどもあることから、記載しない方針としています。そのため、御指摘の4.2.(ウ)につきましてもWG名を削除しました。なお、年次報告において、検討の場などを含めた取組実績を記載する予定です。
23	個人(12)	1	P.29	4.2. (4) (エ)	情報処理技術者試験の更新制度について、以前存在した「情報セキュリティ・アドミニストレータ」の扱いはどうするのか。 資格無効とするならば、同様に以前存在していた「第2種情報処理技術者」や「第1種情報処理技術者」も資格無効とすべき。 一方、資格更新対象となるのであれば、過去存在した他の時代遅れの資格も更新対象とすべき。また、「情報セキュリティ・アドミニストレータ」については、今回新規追加となる「情報セキュリティマネジメント」資格にアップデート可能なように制度設計願う。	政策展開に係る意見	情報処理技術者試験は、受験時点の知識・技能を認定する試験であり、合格した事実が無効になるということはありません。経済産業省において、サイバーセキュリティに従事する者の実践的な能力を適時適切に評価するための更新制度について、検討を行っております。なお、「情報セキュリティマネジメント」資格にアップデート可能なような制度設計は検討しておりません。
24	個人(12)	2	P.28	4.2. (4)	情報セキュリティ監査に係る資格として、「情報セキュリティ監査技術者試験」を新設してほしい。試験範囲にはISO27000シリーズやJISQ15001等を含めると良いと考える。 [理由] 情報セキュリティが企業の命運を決めるほど重要になっている昨今、情報セキュリティ監査に係る適切な資格が無い状況が続いている。ISMS審査員補資格は企業が30万円負担さえすれば、ほぼ誰でも取得でき、個人で取得するには不適切と考える。また、CISM(公認情報セキュリティマネージャー)もあるが、今一つメジャーではなく、受験費用も維持費用も高過ぎる。他にも情報セキュリティ関係の資格はあるが、どれも高額な費用がかかる。 会社法を改正し、上場企業には会計監査の他に情報セキュリティ監査も義務付けるべき時代が到来していると考える。	政策展開に係る意見	御指摘の内容については、今後の試験制度の見直し等施策の検討に当たっての参考とさせていただきます。
25	個人(13)	1	―	2.1. 1.3	行政として「脆弱性チェックをするように事業者に対して補助的に指導」するというよりも、民間コンテンツ制作事業者のサイバーセキュリティーの向上をさせるため、NISC等に属する国家公務員としてのハッカーないしは行政部門からの外部委託先機関が、民間事業者への行政サービスとして当該事業者のサイバー上のプログラムに対してハッキングを仕掛けるなどの直接的な施策を盛り込む必要があるかと思われます。 [理由] 事業者はサイバーセキュリティーに関する意識は高いものの、作成したプログラム等に対し外部からハッキングをさせるコスト負担が重く、このコスト増を敬遠してサイバーセキュリティーの脆弱性チェック無しにリリース(一般市場に販売)するケースが殆どです。民間のことは民間で対応が基本方針とは思いますが、これら(特に資本力のない中小規模事業者)を放置すると、セキュリティーホールのあるプログラムが社会の諸場面で浸透することになってしまうことが懸念されます。	政策展開に係る意見	サイバーセキュリティの確保については、一義的に事業者自らの責任で実施することとしています。 企業経営においてサイバーセキュリティ対策がやむを得ない「費用」ではなく、より積極的な経営への「投資」としてとらえられ、セキュリティが品質として保証されるよう、経営層の意識改革等が必要であると考えております。政府としましては、こうした考え方の下、各種施策を推進してまいります。

通し番号	提出者	枝番	該当箇所		概要	意見の種類	御意見に対する考え方及び修正内容
			ページ	章節項			
26	個人（13）	2	―	5.	海外での研究活動を行う中で、何らかのインシデントに巻き込まれる、ないしは海外で重要な機密を不意に得た場合、日本国民として日本政府のどことコンタクトをとり情報共有をはかるべきかわかりません。とりわけサイバーセキュリティーに関しては個人での対応に限られますので、私の手元の研究情報取得を懸念しています。	政策展開に係る意見	今後の施策の検討に当たっての参考とさせていただきます。なお、内閣官房及び法務省では国と国民の脅威に関する情報の提供を受け付けています。
27	日本アイ・ビー・エム（株）	1	P.3 P.4	1.2.（1）（イ） 1.2.（3）（ウ）	「サイバーセキュリティ経営ガイドライン」の策定に当たっては、民間の情報セキュリティ専門家の参画も求めるべきである 。 ［理由］ 民間には情報セキュリティの専門的な知見・経験を提供している事業者が多く存在しており、民間企業における情報セキュリティの実情や課題について精通している。「サイバーセキュリティ経営ガイドライン」の策定においては、これら事業者の意見も反映すべきと考えるため。	政策展開に係る意見	「サイバーセキュリティ経営ガイドライン」は、独立行政法人情報処理推進機構の「サイバーセキュリティリスクと企業経営に関する研究会」において産学官の有識者を集めて検討を進めているところです。よりよいガイドラインとなるよう引き続き検討してまいります。
28	日本アイ・ビー・エム（株）	2	P.3	1.2.（1）（イ）	「当該ガイドラインも含めた企業の取り組みについて、（中略）、同ガイドラインの内容や利活用のあり方も含めた指針の法制度化を、中小企業向けも含めて検討する。」に関し、企業向けのガイドライン策定は重要であるが、サイバー空間がグローバルであることに鑑み、国際的な議論を促進するとともに、必要に応じて日本がこれをリードしながら策定していくべきである。また、企業の取り組みの多様性を考慮して、民間企業にはあくまで「一つの指針」としての活用を促すべきであり、認証取得等を法的に義務付けることは避けるべきである。 ［理由］ 日本国内に限定するのではなく、グローバルな視点に立って世界にも役立つものとなるよう、「3．国際社会の平和・安定及びわが国の安全保障」に記載されているさまざまな国際協力の一環として作成すべきと考えるため。結果として、日本の企業にとってもより有用なものとなる。また、サイバーセキュリティの取り組みのレベルは、業態・企業により多様であるため、ガイドラインの遵守を義務付けることは避けるべきと考える。	政策展開に係る意見	御意見の内容については、今後の施策の検討に当たっての参考とさせていただきます。
29	日本アイ・ビー・エム（株）	3	P.4	1.2.（3）（イ）	「製品開発者が情報セキュリティ上の観点から配慮すべき事項」については、国際的なセキュリティ標準も踏まえて設定すべきである ［理由］ ソフトウェア製品や情報システムの開発段階におけるセキュリティ要件については、ISO／IECを始めとする国際的な標準があり、上記の「配慮すべき事項」はこれら先行する標準も踏まえて規定すべきと考えるため。	政策展開に係る意見	御指摘の通り、国際的なセキュリティ標準を踏まえた製品開発は重要と考えております。御意見の内容については、今後の施策の検討に当たっての参考とさせていただきます。
30	日本アイ・ビー・エム（株）	4	P.4	1.2.（3）（エ）	「発注者が把握できない多重の再委託の防止」に関して、そのための要件や防止策を検討するための研究会を設置してはどうか。 ［理由］ サプライチェーンは末端に行くにしたがって「発注者が把握できない」状況になりやすい。本戦略の目的を達成するため、サプライチェーン全体のセキュリティを向上させるための指針や具体策について、官民の協力により検討する協議体にて議論することが望ましいと考えるため。	政策展開に係る意見	御指摘のような課題については、現在経済産業省内で検討しているところです。御意見の内容については、今後の施策の検討に当たっての参考とさせていただきます。
31	日本アイ・ビー・エム（株）	5	P.5	1.3.（2）（ア）	「営業秘密官民フォーラム」が目的とする「最新の手口や被害実態などの情報の共有」については、既に同様の目的の協議体が複数存在する。民間企業に過度な負担とならないように、これら協議体の運営や整理統合を図るべきである。 ［理由］ 本項記載の目的には賛同するものの、各省が類似の目的で設置した協議体が増えるに従い、参加を求められる民間企業の負担は増大する。今後、手口の巧妙化、複雑さが増大することが見込まれるため、官民で情報共有を図る場の数を絞り、参加者が同じ情報を共有する方が効果的であると考えるため。	政策展開に係る意見	官民での情報共有等は重要である一方、御指摘のとおり、それが民間企業にとって過度の負担とならないようにすることも、重要であると考えます。御意見の内容については、こうした官民での取組の在り方に関する今後の検討に当たっての参考とさせていただきます。

通し番号	提出者	枝番	該当箇所		概要	意見の種類	御意見に対する考え方及び修正内容
			ページ	章節項			
32	個人(14)	1	P.3 P.26	1.1.(4)(ア) 4.1.(3)(エ)	「経済産業省において、．．．システムの品質、安全性、効率を向上、両立させるための革新的、先端的技術の基礎研究に取り組む。」の施策には、「情報セキュリティ研究開発戦略(改訂版)(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」で記述されている「脆弱性を作り込まないソフトウェア開発技術」は含まれているとの認識で合っているか。当該技術は、攻撃者優位のAPT攻撃環境を逆転する革新技術であるため、産学官の英知を結集したオールジャパン態勢で最優先案件として予算化および実施してほしい。 [理由] APT攻撃を完全に防御するためには、数学的に脆弱性を含まないことが証明されたソフトウェア開発技術に基づくIoTシステムのOS、通信プロトコルおよびアプリケーションの開発が必要である。	政策展開に係る意見	御認識のとおり、本施策には「脆弱性を作り込まないソフトウェア開発技術」も含まれています。
33	個人(14)	2	P.16	2.3.(1)(ク)	内閣官房による各府省庁の情報システムの公開された脆弱性等への対応やサイバー攻撃に係る対策の実施状況の調査周期をリアルタイムのAPT攻撃に対して実効性を挙げるために現行の1年から短縮化されたい。 [理由] 現状のサイバー防御技術ではAPT攻撃を完全に防御できないため、情報セキュリティリスク管理を適時に行うために情報資産の脆弱性やセキュリティ設定の継続的監視が必要である。米国の連邦政府および米軍では、APT攻撃に対応するためにリアルタイムのセキュリティ常時監視が導入されている。	政策展開に係る意見	「政府機関の情報セキュリティ対策のための統一基準の策定と運用等に関する指針」(平成26年5月19日付け情報セキュリティ政策会議決定)の2-2に示すとおり、各府省庁における対策の実施状況の点検は、各府省庁の責任において実施することを原則としており、内閣官房における点検は、政府機関全体として更に効果的かつ効率的に実施する観点から実施しているものです。内閣官房では、今後、サイバーセキュリティ基本法に基づき、各府省庁のセキュリティポリシーの運用状況について、PDCAサイクルが機能しているかなどのマネジメント監査を行うことにより確認していくこととしているところであり、御意見については、今後の取組の検討に当たっての参考とさせていただきます。
34	個人(14)	3	P.19	3.1.(1)(エ)	「防衛省情報通信基盤(DII)のクローズ系及びネットワーク監視器材に最新技術を適用していく。」を次のとおり修文する。 「防衛省情報通信基盤(DII)のクローズ系及びネットワーク監視器材に情報資産の脆弱性及びセキュリティ設定の継続的監視ができるセキュリティ常時監視技術を適用していく。」 [理由] APT攻撃に対する実効性のある技術として最新技術という表現では、具体的に何をするのか分からないため、最新技術として実効性の高い技術を(オ)および(カ)の表現と同様レベルで明示的に表現すべきである。	修正意見	御意見を踏まえ、以下のように修文しました。 「防衛省情報通信基盤(DII)のクローズ系及びネットワーク監視器材に常続監視等を強化するための最新技術を適用していく。」
35	個人(14)	4	P.25	4.1.(ウ) 4.1.(1)	総務省の「ネットワークの各構成要素における最適な情報セキュリティ設定の自動的導出」を目標とした「ネットワーク全体におけるリスク評価・検証技術の研究開発」は、現在のセキュリティ常時監視の基盤技術であるSCAPに代わる技術を開発することですか。現行SCAPは、情報セキュリティポリシーに基づくOSおよびアプリケーション毎のセキュリティ設定のベースラインを事前作成することを前提としてリスク評価・検証を行うセキュリティ自動化技術である。APT攻撃に対する実効性のある当面の対策を行うためには、対策の適時性の観点から現行SCAPに基づくセキュリティ常時監視ソリューションの活用も検討すべきである。また、当該施策を実現するための「ネットワーク全体におけるリスク評価・検証技術の研究開発」の具体記述を、「4.1.1(1)サイバー攻撃の検知・防御能力の向上」の具体施策にSCAPとの関係も含めて明示的に表現すべきである。 [理由] 「ネットワーク全体におけるリスク評価・検証技術の研究開発」が「4.1.(1)サイバー攻撃の検知・防御能力の向上」のどの具体施策に対応しているのかわかりにくい。	政策展開に係る意見	4.1.(ウ)は、4.1.(1)に該当するものではないため、原案どおりとします。なお、御意見の内容については、今後の取組の検討に当たっての参考とさせていただきます。

通し番号	提出者	枝番	該当箇所		概要	意見の種類	御意見に対する考え方及び修正内容
			ページ	章節項			
36	個人（14）	5	P.27	4.1.（5）（ア）	戦略的イノベーション創造プログラム（SIP）新規課題候補「重要インフラ等におけるサイバーセキュリティの確保」の「運用時における機器装置のセキュリティ確認技術」は、重要インフラ等の制御システムのセキュリティ常時監視を実現するための基盤技術であるため、本来、重要インフラの情報セキュリティ対策の責任箇所であるNISCが主導すべきであり、「情報セキュリティ技術開発戦略」で取り挙げるべき最優先技術の1つである。したがって、「4.1.（5）関係機関との連携」での具体記述だけではなく、「「サイバーセキュリティ2015（案）」の概要について」の記述と同様に「4.1. 研究開発の推進」の方針記述（イ）として「戦略的イノベーション創造プログラム（SIP）の枠組み等によりAPT攻撃に実効性のある基盤技術および革新技術の研究開発を推進する。」を明示的に記述すべきである。 ［理由］ APT攻撃に対する実効性のある当面の技術は、セキュリティ常時監視技術である。また、APT攻撃を完全に防御する革新技術の1つは、システムの強靱化のために脆弱性を作り込まないソフトウェア開発技術である。情報セキュリティ技術開発の有効性を高めるために、技術開発投資については、各省集約方式ではなくNISCが技術開発目標を明確にして投資優先度を決めるべきである。	修正意見	各施策の並びは「サイバーセキュリティ戦略」の記載箇所と対応をさせる構成としており、記載順序等が施策の優先度を示すものではない、原文のままとします。 なお、御意見の内容については、今後の取組の検討に当たっての参考とさせていただきます。
37	NPO法人ウェブアクセシビリティ推進協会	―	P.14他	2.2.（3）（ウ）他全般	サイバーセキュリティの確保は極めて重要であるが、システムを利用する障害者・高齢者等に対する情報アクセシビリティの確保に留意する旨、言及されたい。 2.2.（3）（ウ）を次のように変更するように提案する。 「利便性の向上とセキュリティの確保がバランスの取れたものとなるよう、<u>また、アクセシビリティが確保されたものとなるよう</u>」 ［理由］ ・セキュリティの確保ばかりを重視した結果、利便性に大きな影響を及ぼすという事象は、十分に起こり得る。特に、高齢者や障害者などは、一般の人々よりも利便性の低下の影響を受けやすく、利用不可能という状況に陥るような場合はセキュリティの確保施策について一考する必要があると考える。 ・2011年に改正された「障害者基本法」、政府が2013年度から2017年度に講ずる施策として定めた「第3次障害者基本計画」においても、行政情報のバリアフリー化、取り分けウェブアクセシビリティの向上が明確に規定されている。 ・例えば今回の意見募集において、電子メールにより意見を提出する場合、送付先メールアドレスが画像で表示されセキュリティが確保されているが、音声読み上げソフトを利用する視覚障害者は送付先が把握できない。また、「電子政府の総合窓口（e-Gov）」では、「いたずらによる機械的な意見提出を防ぐため」として画像認証が用いられており、同様に視覚障害者は独力で意見を提出することができない。 ・上記のメールアドレスの画像においては全角の文字を用いたり、画像認証とともに音声認証や問合せ先のリンクを用意することによって、セキュリティを確保しながらアクセシビリティが確保できる。セキュリティの向上に取組む際は、アクセシビリティの確保にも留意されたい。 ・マイナンバー制度における官民連携の認証連携で利用者による入力が求められるとしたら、アクセシビリティが確保されていなければ障害者・高齢者などの一部の国民だけが排除される恐れがある。	修正意見	2.2.(3)（ウ)については、「アクセシビリティ」は「利便性」に含まれるものと考えておりますので原案通りとします。また、その他施策についても、障害者基本法等を踏まえて実施してまいります。
38	個人（15）	―	―	全般	サイバー分野での役割は世界情勢で重要な位置づけにあるため、想定外の事が起きたとしても何らかの対策により、国民の生命・財産が守られるような仕組みをお願いします。	政策展開に係る意見	御意見の内容については、本計画の「2. 国民が安全で安心して暮らせる社会の実現」や「3.1. 我が国の安全の確保」等に記載している施策をはじめ、各種施策を着実に推進することにより、万全を期していきたいと考えております。
39	個人（16）	1	P.28	4.2.（2）（イ）	教育に携わる全ての関係者が情報セキュリティに関する基本的な知識を含む情報技術に関する指導力の向上を目指した取組を進めるに当たり、指導主事、リーダー的教員等には、ITパスポート試験、情報セキュリティマネジメント試験など国家試験の合格を必要事項としてはどうか。 また、教育機関で育成する人材のレベルの明確化と併せて、教員にとって必要となるスキルや教員向けの教材等は、ITパスポート試験、情報セキュリティマネジメント試験などの合格を必要条件にするなど、国家試験を活用してはどうか。	政策展開に係る意見	いただいた御意見も参考にしながら、教員等の指導力向上の取り組みについて検討してまいります。

通し番号	提出者	枝番	該当箇所		概要	意見の種類	御意見に対する考え方及び修正内容
			ページ	章節項			
40	個人(16)	2	P.28	4.2. (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＞ ・情報処理技術者試験をベースとした「アジア共通統一試験」のITパスポート試験を日本国内でも実施してはどうか。 ・IPAが「アジア共通統一試験」のITパスポート試験のスコア、上位合格者を明確化し表彰することによって、ITを利活用しているユーザー企業におけるIT人材が適切に評価されるのではないか。 ・スコア競技会、イベント的にITパスポート試験を実施することで、学生やITを利活用しているユーザー企業における社会人などがハイスコアを目指せることで、合格後の継続教育に繋がっていくのではないか。	政策展開に係る意見	御意見の内容につきましては、今後の施策の検討に当たっての参考とさせていただきます。
41	個人(16)	3	P.28	4.2. (4)	＜人材が将来にわたって活躍し続けるための環境整備＞ ・「ここからセキュリティ！」のポータルサイトにウェブバナーから、ITパスポートや情報処理技術者試験試験とリンクさせてはどうか。 ・情報セキュリティサポーターの認定について、ITパスポートなど国家試験の合格を必要条件としてはどうか。 ・「情報セキュリティ月間」において、ITパスポート試験の公式キャラクターとタイアップや、ウェブバナーからiパス試験とリンクさせてはどうか。情報セキュリティに係わる基本的な知識の向上、国家試験の周知、普及に繋がるのではないか。 ・IPAでは、ITパスポートの公式キャラクターも出てきたところである。今後は、ITパスポートの公式キャラクターを起用して、YouTubeや電車内の動画広告など、国家試験の広報活動に起用してはどうか。	政策展開に係る意見	いただいた御意見を踏まえ、今後検討してまいります。なお、情報セキュリティサポーターは、セキュリティ対策推進協議会（SPREAD）が実施している制度であり、政府の管轄外であるため、お答えすることはできません。
42	個人(16)	4	P.28	4.2. (4) (イ)	＜情報セキュリティマネジメント試験について＞ ・日曜日に5時間程度拘束されての受験は、受験者に過大な負担となる。ITパスポートと同様に小問、中問からなる半日程度で終えられる出題形式としてはどうか。 ・情報セキュリティマネジメント試験の合格者については、登録型のアドオン資格とすることが資格者の母数を確保する上で望ましいのではないか。 ・情報セキュリティマネジメント試験の合格者に対しても、継続的な学習と新しい知識を身に付けてもらえることが望ましいと思う。合格者における資格の更新制を推奨するため、CBT方式を目指した試験としてはどうか。	政策展開に係る意見	御意見の内容につきましては、今後の試験の検討に当たっての参考とさせていただきます。
43	個人(17)	1	―	1.1.	1.1節の「安全なIoTシステムの創出」で示されている、IoTシステムの提供側の観点での施策は重要なものと考えます。ここに示されるように、まずは、安全なIoTシステムを創出することが第一ではありますが、今後想定される社会インフラとしてのIoTシステムに対する利用者の広がりを考えると、IoTシステムの利用側の観点での施策の検討も必要ではないかと考えます。	政策展開に係る意見	IoTの利用者側視点での対応については、「2.1. 国民・社会を守るための取組」における、事業者への働きかけや利用者への普及啓発の中で取り組んでいきます。
44	個人(17)	2	―	2.1. (1)	2.2節(1)において、「安全・安心なサイバー空間の利用環境の構築」のための施策が示されています。この中に組み込みソフトウェアやスマートフォンについての施策も示されており、IoTシステムについても考慮されていると思いますが、将来のIoTシステムを見据えた利用環境はどうあるべきかという観点（利用側の観点）からの検討も、IoTシステム自体の安全性（提供側の観点）と合わせて、今後考えてゆくべき事項であると考えます。	政策展開に係る意見	御意見の内容につきましては、今後の取組の検討に当たっての参考とさせていただきます。
45	個人(18)	―	P.3	1.1. (4)	検討対象に「組込み向けハイパーバイザーを用いたセキュリティ向上の仕組み」を加えて欲しい。また、ガイドラインの提示および評価認証制度においても、対象として「組込み向けハイパーバイザーを用いたセキュリティ向上の仕組み」を加えて欲しい。 [理由] 組込み向けシステムに多く搭載されている代表的なプロセッサIPであるARM/MIPS/INTEL等において、OS環境の仮想化・分離をハードウェア側で支援する機能がサポートされるようになっている。組込み向けプロセッサにおいてもアクセス制御および完全仮想化を利用するハイパーバイザーが開発され、システム機能を実現する部分とは独立に（分離された環境で）動作するモジュールにより安全な起動・安全なファームウェア更新の実現に利用されている現状がある。 これらの状況を踏まえ、IoTシステムのセキュリティに係る技術開発・実装において、セキュリティの向上に組込み向けハイパーバイザーを用いるケースについても、利用可能な技術としての検討ならびにガイドライン提示のための調査対象に加えるべきであると考える。	政策展開に係る意見	頂いた御意見については、産官学の役割分担も踏まえて行われる領域と考えておりますが、政府としてもIoTシステムのセキュリティに係る技術開発・実証の施策を進めてまいります。

通し番号	提出者	枝番	該当箇所		概要	意見の種類	御意見に対する考え方及び修正内容
			ページ	章節項			
46	日本オラクル(株)	1	P.8	2.1.(1)(ア)	提案として、以下のとおり修正(下線部を追記)。 (ア) 内閣官房において、事業者のセキュリティ・バイ・デザインに対する取組を促すとともに、各府省庁等において、多層防御の構成がとれる仕組みに改善する等、こうした考え方に基づく取組が行われるよう働きかけを行う。 [理由] 「多層防御」も含めて情報漏えいや改ざんを阻止するといった対策を検討することが重要であると考えます。	修正意見	本方針においては、特段例示はしていませんが、多重的な防御の仕組みに関する重要性については、認識しており、「高度サイバー攻撃対処のためのリスク評価等のガイドライン」(平成26年6月)でそれらを実現する際に採るべき手法について示されています。
47	日本オラクル(株)	2	P.17	2.3.(1)(ツ)	提案として、以下のとおり修正(下線部を追記)。 (ツ) 内閣官房において、(中略)、機密性・完全性の高い情報を管理するデータベースに対する不正なア クセス等による情報漏えいや改ざん等について、多層防御により阻止する等の対策を含め、政府統一基準を始めとした規程への反映に向けた検討を行う。 [理由] 「多層防御」も含めて情報漏えいや改ざんを阻止するといった対策を検討することが重要であると考えます。	修正意見	御意見につきましては、「「高度サイバー攻撃対処のためのリスク評価等のガイドライン」の運用等を通じて標的型攻撃に対する多重防御の取組の加速を図るとともに、個人情報や機微な情報を始めとした機密性・完全性の高い情報に焦点を当てた政府機関における情報管理の更なる強化に向けて、取り扱う情報の性質や量に応じた情報システムの分離」とされている部分に「多重防御の取組の加速を図るとともに」と記載しておりますので、原案のとおりとさせていただきます。
48	日本オラクル(株)	3	P.17	2.3.(1)	提案として、以下の施策を追加。 (ト) 各府省庁におけるアイデンティティ管理・アクセス制御の厳正化を推進するとともに、属性ベースアクセス制御(ABAC)等のベストプラクティスの導入を促進する。 [理由] アイデンティティ管理やアクセス 制御はセキュリティ対策の中で極めて重要な事項の 一つです。政府機関を守るための取組として加える必要があると考えます。	修正意見	2.3.(1)(ツ)において「政府機関における情報管理の更なる強化に向けて検討を行う」旨を盛り込んでいるところであり、御意見の内容については、今後の検討に当たっての参考とさせていただきます。
49	(一社)日本オンラインゲーム協会	1	P.3	1.2.(1)(ア)	オンラインゲーム業界の特性を踏まえ、エンターテイメント業界や、コンシューマー・データ配信サービス事業者にとって、著しく不利益となるようなことがないよう攻撃の程度、範囲、影響の開示の範囲を限定的にしていただきたい。 [理由] アプリなどのコンシューマー・データ配信サービスは、法人間サービスと比較すると、攻撃される頻度が高くなりやすく、単純にサイバー攻撃が発生した場合の想定リスク金額を契約書に基づいて計算し開示するといったガイドラインとなった場合には、他業界と比較して著しくリスクが高いように見える可能性がある。	政策展開に係る意見	情報開示の可能性及び関連する仕組みの検討にあたっては、開示による企業の負担等も考慮し、関係者の意見も聞きながら、検討を進めてまいります。
50	(一社)日本オンラインゲーム協会	2	P.4	1.2.(3)(オ)	CSIRTの設立や連携について、税制上の優遇や斡旋も含めて、各種業界団体などと意見交換しながら進めていただきたい。 [理由] ゲーム業界やエンターテイメント業界では中小企業やベンチャーも多く、組織内CSIRTについては窓口のみで、外部業者と連携を取る動きしかできないと思われる。そのため、特に中小企業や各種業界団体に対しての(設立した場合に対しての)税制上の優遇や斡旋を行う形でないと、絵に描いた餅に感じる。	政策展開に係る意見	CSIRTの設立促進・支援、普及・連携促進に当たっては、関係者の意見も聞きながら進めてまいります。
51	(一社)日本オンラインゲーム協会	3	P.6	1.3.(1)(エ)	リバースエンジニアリングを行うことができる主体、範囲、目的を限定的に定め、厳格な条件を満たすもの以外は、利用規約どおりリバースエンジニアリングを禁ずるという内容にしていただきたい。 [理由] 本年の8月5日に、あるオンラインゲームにおけるシナリオやキャラクターがリバースエンジニアリングされ、ネットに開示されるトラブルが発生した。セキュリティ目的だけにリバースエンジニアリングをした場合においても、別の目的にも使用したり、流出したりする可能性がある。	政策展開に係る意見	いただいた御意見の視点も含め、セキュリティ目的のリバースエンジニアリングに関する適法性の明確化に関する措置について検討してまいります。

通し番号	提出者	枝番	該当箇所		概要	意見の種類	御意見に対する考え方及び修正内容
			ページ	章節項			
52	（一社）日本オンラインゲーム協会	4	P.8	2.1.（1）（ウ）	業界特性によっては適用が困難なコーディングルールを決められると開発側での制約になる可能性があるため、範囲や程度について各種業界団体などと意見交換しながら進めていただきたい。 ［理由］ IPAにおいて整備したコーディングスタンダードの高信頼化は、現状IPAで提供しているセキュリティに関するコーディングルールや心得のようなものと推測する。そのままであれば問題ないが、業界特性によっては適用が困難なコーディングルールを決められると開発側での制約になる可能性がある。	政策展開に係る意見	IPAにおいて整備したコーディングスタンダードは、ソースコードの標準化や品質の均一化を進めることを目的として、組織やグループ内のコーディングルールを決める際の参考となるような注意事項やノウハウを整理したものです。そのため、これらの取組等は、開発者である民間企業の制約にはならないと考えています。また、コーディングスタンダードの整備にあたっては、産学の知見を集結して注意事項やノウハウを整理していますが、御指摘の点も踏まえ今後検討を進めてまいります。
53	（一社）日本オンラインゲーム協会	5	P.10	2.1.（2）（ウ）	現行の情報セキュリティ教育ではインターネットは危ないという内容を青少年に教えるものが多いが、インターネットの有用性と危険性を半々で教える公平なものにしていただきたい。「危ないから触らない」という回避ではなく、「どうすれば安全か」という適切な利用指導を中心にすべきと考えます。 ［理由］ 今後の子どもたちの時代の世界はインターネットの活用力と、実際の仕事の能力が密接につながるため、「危ないから触らない」という回避ではなく、「どうすれば安全か」という適切な利用指導を中心にすべきと考える。	政策展開に係る意見	利用者の普及啓発については、頂いた御意見も参考に、「2.1.(2)サイバー空間利用者の取組の促進」の施策等で進めてまいります。 なお、「新・情報セキュリティ普及啓発プログラム」の「初等中等教育層に向けた取組」において、学校現場等での指導にあたって、脅威に関する知識だけでなく、最新の製品・サービス等の動向を踏まえ、何をすればよいのかという具体策も併せて提供することの必要性についても記載しています。
54	（一社）日本オンラインゲーム協会	6	P.12	2.1.（3）（サ）	サイバー犯罪の捜査に支障をきたさない枠組みもあわせて検討すべきではないでしょうか。 ［理由］ サービス運営しているスマートフォンゲームにおいて不正アクセス事件が発生し、捜査機関が被疑者特定のためゲームに接続した際に使用されたキャリア側へ通信履歴の開示を求めたが、ゲーム接続認証にはSSL通信を使用しており、秘匿性の高い通信であるとキャリア側に判断されたため通信履歴は保存されておらず、追跡調査が行えなかった事案があった。 「電気通信事業における個人情報保護に関するガイドライン」によれば、システムの安全性の確保やその他業務の遂行に必要な場合、通信履歴を記録し保存することができる、とされている。但し、通信履歴を記録するかどうかは事業者の任意であるため、通信履歴を保存していなかった場合、上記のような問題が発生してしまう。	政策展開に係る意見	サイバーセキュリティ戦略5.2.1 （3）において、「サイバー犯罪に対する事後追跡可能性を確保するため（中略）適切な取組を推進する。」としており、御意見の内容につきましては、今後の施策の検討に当たっての参考とさせていただきます。
55	（一社）日本オンラインゲーム協会	7	P.12	2.1.（3）（サ）	サーバ管理の会社が外国法人である場合や、サーバの設置場所が国外にある場合においてのガイドラインおよびサイバーセキュリティ基本法などの法の適用範囲を明確化していただきたい。具体的には、サーバ管理の会社が外国法人である場合や、サーバの設置場所が国外にある場合は、適用となるのかなどについても記載をしていただきたい。	政策展開に係る意見	「電気通信事業における個人情報保護に関するガイドライン」は、一般的に、日本国内に拠点を設置して電気通信事業を行う者が適用対象になると考えられます。
56	（株）ラック	1	P.2	1.1.（3）	ドローンや自動車IoT関連について国土交通省の関与が必要です。すでにドローンに関する法律的整理が進んでいますが、一方で、自律飛行によるスパイ活動を行う、あるいは直接的な人的被害を引き起こすドローンの開発が進んでいます。自動車については車載器やOBDインターフェースから攻撃される事例が相次いでおり、何らかの対応が必要です。 農林水産業でIoTの利用が増えています。その整理に農林水産省の関与が必要です。現在のラジコンヘリコプターによる農薬散布だけでなく、ドローンを用いた病虫害検査、ピンポイント農薬散布などが自律飛行で行われる準備が始まっています。電子百葉箱や土壌の定点観測の結果の自動収集も始まっています。里山管理として害獣の動態把握等にIoTセンサーは活用されています。水産物の流通管理のために個々に電子タグを取り付けて、消費者に付加価値情報の提供を行う取り組みも行われています。これらの活動を妨害したり、誤った情報を注入することで、高濃度な残留農薬を含む農作物が流通させたり、農林水産物の市場経済を混乱させることが出来ます。	政策展開に係る意見	御指摘のとおり、各分野において関係府省庁が参画することは重要であり、1.1.(1)や1.1.(2)で示したように、内閣官房が各府省庁に働きかけを行ってまいります。
57	（株）ラック	2	P.2	1.1.（3）（ク）	IPAのソフトウェア等脆弱性関連情報取扱基準において脆弱性は「不正アクセス等の攻撃によりその機能や性能を損なう原因となり得る安全上の問題箇所」と定義されているが、これに「人の生命、身体または財産を侵害する原因となり得る安全上の問題箇所」を加える必要があります。また、人の生命、身体または財産に対する攻撃について、全体的に見直す必要があります。	政策展開に係る意見	御指摘の点は、不正アクセス等の攻撃によりその機能や性能を損なうことによって生じるものに含まれると考えております。今後の施策の検討に当たっての参考とさせていただきます。

通し番号	提出者	枝番	該当箇所		概要	意見の種類	御意見に対する考え方及び修正内容
			ページ	章節項			
58	(株)ラック	3	P.3	1.1.(4)	医療機器に対する案がありません。厚生労働省が適切かどうかは分かりませんが、薬剤注入型ウェアラブルデバイスが不正アクセスによって異常な動作を引き起こされた場合や、センサー型ウェアラブルデバイスからのセンシティブな医療情報の流出などに関するリスク評価をするためにも、医療機器特有の技術開発が必要です。	政策展開に係る意見	御指摘の点の必要性も含め、1.1(3)(エ)の検討を進めてまいります。
59	(株)ラック	4	P.3	1.1.(4)(カ)	有人運転の自動車に限らず、IoTデバイスが物理的かつ自律的に移動するという考えが必要です。ドローン、掃除ロボット、自動運転する自動車などが、プログラムのバグあるいは不正攻撃によって引き起こされる問題を最小限にするための取り組みが必要です。問題は引き起こされることが前提です。	政策展開に係る意見	御指摘のとおり、IoTシステムには移動する構成要素もあり、1.1.(4)の各施策をはじめとしたIoTのセキュリティ確保に向けた取組はその視点も踏まえて進めてまいります。
60	(株)ラック	5	P.11	2.1.(2)(チ)	(ここの場所での指摘が良いかどうか分かりませんが)標的型攻撃の訓練だけでなく、IoTデバイスへの攻撃に対する訓練の研究を始める必要があります。情報漏洩だけでなく、物理動作を伴うIoTデバイスに攻撃を受けた場合にどのような対応が可能であるのかを示せるようにする必要があります。	政策展開に係る意見	御意見の内容につきましては、今後の取組の検討に当たっての参考とさせていただきます。
61	(株)ラック	6	P.25	4.1.(1)	※施策の追加 侵入検知が間に合わない場合に備えて、危険な作動を予防するシステムも必要です。IoTデバイスの表面上のコントロールまでは攻撃されることを前提とし、最後のモータやエンジンを動作させる部分のリミッターのようなものを検討する必要があります。侵入を伴わない攻撃や、プログラムバグによる想定外動作にも対応しなければなりません。	政策展開に係る意見	IoTシステムを介して実空間とサイバー空間が融合するという特性も踏まえ、セキュリティに関する取組はは、御指摘のような点も含めて進めてまいります。
62	BSA｜ザ・ソフトウェア・アライアンス	1	―	全般	＜官民連携＞ サイバーセキュリティの体制が効果的であるためには、国内及び世界の民間団体との協力が、明確な役割として組み込まれている必要があります。この点、グローバルなソフトウェア、IT企業は、最先端のソフトウェア・ソリューションや、企業向けベストプラクティスを開発する豊富な経験を有しております。 日本政府は、現在、業界ごとのサイバーセキュリティ・ガイドラインを策定していますが、私たちは、その過程において、官民連携を活用すること、及び国際調和を達成するために国際基準を採用することを強く要望します。内閣官房内閣サイバーセキュリティセンター(NISC)が本計画案を完成し、実行し、日本のサイバーセキュリティを高めるために各政府機関・団体の責任範囲について取り決める際、民間団体が必要に応じた役割を十分に担うことができるよう要望します。	政策展開に係る意見	サイバーセキュリティ政策の推進にあたっては、民間団体の御意見等も踏まえつつ、産学官民が連携し、推進するよう努めてまいります。具体的な役割等については、御意見も踏まえ、今後検討してまいります。
63	BSA｜ザ・ソフトウェア・アライアンス	2	―	全般	＜サイバーセキュリティに関する国際的アプローチ＞ どのような国又は政府であっても、単独でサイバーセキュリティリスクを解決することはできません。非政府組織や国際的な連携先と協働することは、サイバーセキュリティの効果的なアプローチにおける欠かせない要素です。国際市場において成長し続けられるよう日本企業の競争力を維持しつつ、サイバースペースにおける安全確保の運用効率を高めるためには、国内ポリシーを策定する際に、グローバルな視点を持つことが重要です。 従って、日本政府においては、地域間及びグローバルでの情報共有及び保護を最大化するために、国際的、自主的かつ市場主導の基準を活用することを強く求めます。	政策展開に係る意見	サイバーセキュリティに関する基準については、御指摘の国際性や自主性、市場の観点は重要であると考えています。御意見の内容について、今後の施策の検討に当たっての参考とさせていただきます。

通し番号	提出者	枝番	該当箇所		概要	意見の種類	御意見に対する考え方及び修正内容
			ページ	章節項			
64	BSA｜ザ・ソフトウェア・アライアンス	3	―	全般	＜情報共有＞ サイバーセキュリティに対する脅威、脆弱性、インシデントといった情報につき、影響を受ける者と攻撃からの防御手段を開発する者が共有できるようにすることは大変重要です。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、本計画案を最終化する際、日本政府が上記の原則を考慮するよう求めます。 (1) 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 (2) 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 (3) 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 (4) 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 (5) 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及びその他の状況に対する賠償保険が提供されるようにすること。 (6) 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	政策展開に係る意見	御意見の内容につきましては、今後の取組の検討に当たっての参考とさせていただきます。
65	BSA｜ザ・ソフトウェア・アライアンス	4	P.2	1.1. (3)	IoTシステムのセキュリティに係る制度整備に関しては、脅威モデルを定義することなくして、開発側が脅威を軽減することは不可能であるため、(3)に記載される全ての項目は、各省により軽減すべき脅威モデルを定義した上で実行されるべきです。従って、「各省により、下記各項目において軽減すべき脅威モデルを定義した上で」との文言を、(ア)の項目が始まる前に追加して記載するのが良いと考えます。	修正意見	御意見の内容につきましては、今後の取組の検討に当たっての参考とさせていただきます。
66	BSA｜ザ・ソフトウェア・アライアンス	5	P.2	1.1. (3) (ア)	以下のように修正（下線部を追記）することを要望します。 「経済産業省において、軽減すべき脅威モデルを定義した上で、IoT及びサイバーフィジカルシステムへの脅威シナリオ及び攻撃についての国際的なベストプラクティス及び評価を参考にしつつ、IPAを通じて、IoTシステムに含まれる機器等に関して、攻撃事例や利用形態を基に整理を行い、国際的かつ自主的基準に基づいた総合的なガイドラインの確立に向け、脅威分析とセキュリティ対策の明確化を図る。また、その際には、製品開発側にも調査を行い、脅威軽減に向けた努力に関する背景知識を得るものとする。」 ［理由］ 日本政府が国内向け独自基準を策定するのではなく、国際的、自主的かつ市場主導的な基準を活用することを強く求めます。サイバー脅威がグローバルなものであることを鑑みれば、効果的なサイバーセキュリティ戦略は、その効果を確実にするために国際的な視点が必要です。	修正意見	国際的な視点を参考にしつつ取り組むことは重要であると考えております。御指摘の内容につきましては、今後の施策の検討に当たっての参考とさせていただきます。
67	BSA｜ザ・ソフトウェア・アライアンス	6	P.2	1.1. (3) (イ)	以下のように修正（下線部を追記）することを要望します。 「総務省において、軽減すべき脅威モデルを定義した上で、国際的なベストプラクティス及び評価を参考にしつつ、IoTシステムに関する横断的な取組の1つとして、ウェアラブル端末等のM2M機器の運用の実装上のセキュリティに係る横断的なガイドライン策定の検討を実施する。」 ［理由］ 国際的な経験が有益であることは同様です。	修正意見	御意見を踏まえ、以下のとおり修文致します。 「総務省において、国際的な動向も踏まえ、IoTシステムに関する横断的な取組の1つとして、M2M機器の運用の実装上のセキュリティに係る横断的なガイドライン策定の検討を実施する。」
68	BSA｜ザ・ソフトウェア・アライアンス	7	P.2	1.1. (3) (ウ)	以下のように修正（下線部を追記）することを要望します。 「経済産業省において、軽減すべき脅威モデルを定義した上で、国際的なベストプラクティス及び評価を参考にしつつ、エネルギー分野におけるIoTのセキュリティガイドラインとして、スマートメーターのセキュリティの評価技術・手順の実証を行う。」	修正意見	スマートメーターのセキュリティ評価については、資源エネルギー庁に設置されたセキュリティ検討ワーキンググループの報告書（2015年7月）に示された、国際基準も踏まえた対策要件を参考に検討しておりますが、脅威等については今後の動向を踏まえて検討を行う必要があり、本計画においては原案のとおりとさせて頂きます。

通し番号	提出者	枝番	該当箇所		概要	意見の種類	御意見に対する考え方及び修正内容
			ページ	章節項			
69	BSA｜ザ・ソフトウェア・アライアンス	8	P.2	1.1. (3) (エ)	以下のように修正（下線部を追記）することを要望します。 「厚生労働省において、軽減すべき脅威モデルを定義した上で、国際的なベストプラクティス及び評価を参考にしつつ、医薬医療機器法上の医療機器のサイバーセキュリティについて検討を進める。」	修正意見	御指摘の点も参考にしつつ、1.1.(3)（エ)の検討を進めてまいります。なお、今後検討を行う範囲・方向性が限定されないよう、修正は行わないことといたします。
70	BSA｜ザ・ソフトウェア・アライアンス	9	P.3	1.1. (4) (ウ)	以下のように修正することを要望します。 「経済産業省において、世界的でスケーラブルな認証制度及び基準に則した制御システムのテスト環境を用い、システム全体の脅威分析、リスク評価を行う技術を開発し、評価・認証制度やサイバー演習へと活用する。その際には、Common Criteriaのような国際的アプローチを採用し、世界の知見を活用するとともに、世界規模での脅威低減に貢献できるようにする。また、IoTの分野毎に求められる異なる評価、脅威モデルの定義及び認証制度に留意するものとする。」 ［理由］ 日本が国際的、自主的で、かつマルチステークホルダープロセスを通じて開発された認証制度を採用することを強く求めます。そして、そのような基準の一つが世界の共通基準（Common Criteria）であり、これを採用するのが本件においても有益と思われます。また、IoTの分野毎(例えば、ウェアラブル機器、原子力施設等)に求められる評価・認証制度に留意し、それぞれ異なったアプローチにより開発することが重要です。	修正意見	評価・認証制度や演習の実施にあたっては、国際的な動向を参考にしておりますが、共通基準の採用にあたっては、今後の動向を踏まえて検討を行う必要があり、本計画においては原案どおりとさせていただきます。
71	BSA｜ザ・ソフトウェア・アライアンス	10	P.3	1.1. (4)	下記施策を追加することを要望します。 「経済産業省において、国際的IoTコンソーシアムにより開発された事業モデル及び利用事例を実現するIoTアーキテクチャに基づいた実用的なセキュリティフレームワークに関する調査を実施し、これら国際的IoTコンソーシアムとの共同実証実験の実施について検討する。」 ［理由］ 本計画案には、この経済産業省の重要な取組みが盛り込まれていません。世界的な競争力を実現するには、日本の産業界がIoT分野における専門知識を有する国際的なIoTコンソーシアムと連携し協働することが重要です。	修正意見	IoTの推進やセキュリティ対策の推進にあたり、国際的な視点は重要と考えており、御指摘の内容につきましては、今後の施策の検討に当たっての参考とさせていただきます。
72	BSA｜ザ・ソフトウェア・アライアンス	11	P.4	1.2. (3) (エ)	以下のように修正することを要望します。 「経済産業省において、情報システム開発・運用に係るサプライチェーン全体のセキュリティ向上のため、情報システム開発・運用に係る取引の適正化を図るための制度整備を行う。」 ［理由］ 現在の世界規模の供給モデルの中で、多重の再委託を禁止することは不可能であり、一社に全ての清算を要求することは現実的でないことから、本記載について懸念を有します。コスト削減効果と効率を高めるために必要な委託と再委託から生じるサプライチェーンリスクの管理については、リスクベースアプローチを採用するべきです。	修正意見	本案における制度整備は、多重の再委託を禁止することを念頭においたものではなく、サプライチェーンのセキュリティのガバナンスを強化することを念頭においたものです。 なお、懸念が発生する表現を避ける観点から、趣旨については変更ありませんが、頂いたご意見の通り、表現を修正します。
73	BSA｜ザ・ソフトウェア・アライアンス	12	P.6	1.3. (1)	下記施策を追加することを要望します。 「経済産業省において、2020年の東京オリンピック・パラリンピック及びそれ以降に向け、日本のサイバーセキュリティの進展を妨げているセキュリティにおける障害について理解し、効率的で革新的なサービスと製品によりこれらの障害を克服するため、民間との対話及び連携を推進する。」 ［理由］ 2020年に開催する東京オリンピック・パラリンピックを控え、日本ではサイバーセキュリティに関する関心と懸念が高まっています。しかし、これらの懸念は、未だ、日本のサイバーセキュリティに係る課題を革新的な製品とサービスにより解決していくために業界と活発な議論を行うまでには至っていません。サイバーセキュリティ問題に適切に取組むためには、政府が、官民連携の構築と強化を促進し、リードしていく必要があります。	修正意見	御意見の内容につきましては、今後の取組の検討に当たっての参考とさせていただきます。

通し番号	提出者	枝番	該当箇所		概要	意見の種類	御意見に対する考え方及び修正内容
			ページ	章節項			
74	BSA｜ザ・ソフトウェア・アライアンス	13	P.13	2.2.(1)(ウ)	日本政府が、サイバーセキュリティ上の懸念を解決するために情報共有が重要であることを十分に認識されていることは大変素晴らしいことですが、本記載のままですと、重要インフラ分野以外において、任意・匿名ではなく、強制的な情報共有の対象となるようにも読み得るため、任意・匿名であることを明確化すべきと考えます。即ち、流動的な脅威環境においては、パートナーシップ、信頼及びインセンティブの上に成り立つ情報共有が最も効果的であり、企業等がサイバーリスクを管理する上で最も良く機能すると考えます。また、情報共有に関して適切な賠償責任の制限が提供されることは非常に重要です。	修正意見	本案は、サイバーセキュリティ戦略に基づくもので、同戦略の5.2.2 (1)において「重要インフラ防護の範囲等の不断の見直し」としているとおり、重要インフラ分野以外においても必要な範囲において重要インフラと同様の取組を行っていくべき旨を記載しているものです。
75	BSA｜ザ・ソフトウェア・アライアンス	14	P.16	2.3.(1)(オ) 2.3.(1)(カ)	経済産業省において、政府調達推進のために又は暗号化モジュールに関し、評価及び認証手続の改善又は試験及び認証制度の普及を図る旨記載されています。これらの試験、評価及び認証手続についても上記同様、各政府機関において試験済みや認証済みの製品の迅速な展開が可能となるよう、国際的なベストプラクティス及び基準に則したものとしていただけるよう要望します。 [理由] BSAは、日本政府が、政府機関の保護のために、世界的なベストプラクティス及び国際基準を採用すべきであると考えており、最新の脅威から防御するために世界中から最も優れた技術を日本において展開することを困難とするような日本独自の基準を策定することがないよう要望します。	政策展開に係る意見	IPAで運営している暗号モジュールの試験及び認証制度では、国際標準ISO/IEC19790の一致規格であるJIS X 19790を暗号モジュールセキュリティ要求事項として採用しております。
76	(一社)新経済連盟	1	P.5	1.3.(1)(イ)	クラウドセキュリティガイドラインの普及促進にあたって既存のガイドラインと連携して進めていただきたい。 [理由] 大学や研究機関等で既に作成・普及促進をしているため、これらの動きと連携した方がより速やかな対応ができるため。	政策展開に係る意見	御意見の内容につきましては、今後の取組の検討に当たっての参考とさせていただきます。
77	(一社)新経済連盟	2	P.20	3.2.(1) 3.3.	国際的なサイバーセキュリティ政策について、我が国政府が民間の自主的取組を尊重した方向性を主体的に示していくべきことを明記すべき。 [理由] 民間によるサイバーセキュリティ確保に向けた活動が委縮しないようにするため。	政策展開に係る意見	方向性については「サイバーセキュリティ戦略」において、自律性の尊重を基本原則として掲げているとおり、国際的なサイバーセキュリティ政策においても、民間の自主的取組を十分に尊重して実施してまいります。
78	(一社)新経済連盟	3	P.21	3.2.(2)	我が国政府が特定のセキュリティ手法やセキュリティ技術を民間事業者に課すことがないようにすべき。 [理由] 民間の対応に柔軟性がなくなり、日本特有のガラパゴス的な対応になる可能性があるため。	政策展開に係る意見	御指摘の点については、「サイバーセキュリティ戦略」において、自律性の尊重を基本原則として掲げているとおり、民間の自主的取組を十分に尊重して実施してまいります。
79	(一社)新経済連盟	4	P.27	4.2.	政府による民間の自主的取組みの尊重と支援について追記すべき。 [理由] 人材育成策も民間との協同で実施しているものが含まれているように、技術の進展が早いサイバーセキュリティ上の課題については、政府機関主導だけではなく、民間の自主的な取組みを尊重し、政府がそれらを支援することにより、柔軟性を確保でき効率的であるため。	政策展開に係る意見	上述のとおり、自主的取組みの尊重については「サイバーセキュリティ戦略」において基本原則として掲げています。なお、本年次計画は、同戦略に基づき主に政府が取り組む施策を取りまとめたものですが、4.2.(ア)で示した「新・人材育成プログラム」において、産学官が連携して取り組むことの重要性等について記載しています。
80	(一社)新経済連盟	5	P.28	4.2.(2)(ア)	①教育委員会や各機関の職員、先生方にセキュリティのリスクマネジメントを国全体で徹底的に教育して頂きたい。 ②産学連携で協力して推進して頂きたい。 [理由] 初等中等教育機関や教育委員会の職員、先生方の情報セキュリティに対するモラルが高いとは言えない。例えばUSBキーを無くした場合も特段処罰があるわけでもなく、新たなセキュリティ対策を講じる事もなく穏便に処理されていると考えられるため。	政策展開に係る意見	いただいた御意見も参考にしながら、教員等の指導力向上の取り組みについて検討してまいります。

通し番号	提出者	枝番	該当箇所		概要	意見の種類	御意見に対する考え方及び修正内容
			ページ	章節項			
81	（一社）日本電気制御機器工業会	―	P.3	1.2.（1）（イ）	“1.2. セキュリティマインドを持った企業経営の推進”に記載があるサイバーセキュリティ経営ガイドラインについて、日本電気制御機器工業会　制御システムセキュリティ研究会では、制御システムセキュリティの必要性を強く感じておりますが、企業若しくは経営者へ理解して頂くことは難しく、政府が計画されているサイバーセキュリティ経営ガイドラインの策定・普及に賛同いたします。 “また、当該ガイドラインも含めた企業の取り組みについて、第三者認証等によりステークホルダー等から客観的に評価される仕組みを検討する”との記載がありますが、第三者認証は既存の制度の活用と独立した制度を構築する2つの手法があるかと思いますが、どちらがより普及しやすいのか検討をしていただくことを希望します。	賛同意見	御賛同意見として承ります。より良いガイドラインとなるよう検討を進めてまいります。
82	NPO法人日本ネットワークセキュリティ協会	1	P.2	1.1.（3）	IoTをシステムとして考えた場合、それらを統括するサービスサイトが持つ、情報配信、デバイス全体またはグループの制御や調整、ソフトウエア、ファームウエアの配信、データの収集といった機能が侵害されることによるリスクは非常に大きなものがあります。このようなサイトは非常に多数のデバイスに影響を与えうるため、一般のサイトに比べて遙かにリスクが高いと思われ、こうしたサービスに関するリスク評価の考え方やセキュリティガイドラインも併せて整備していく必要があると考えます。	政策展開に係る意見	IoTシステムの特性も踏まえ、御意見の内容につきましては、今後の取組の検討に当たっての参考とさせていただきます。
83	NPO法人日本ネットワークセキュリティ協会	2	P.8	1.1.（4）	IoT機器への近年の攻撃傾向を見ると、事前に機器やソフトウエアをリバースエンジニアリングすることで、必要な情報を得ている場合が多数を占めています。単純なプログラムの難読化といった方法が破られてしまうことも多く、こうしたリバースエンジニアリング対策、とりわけファームウエアやアプリケーションのリバースエンジニアリングを防止するための標準的な技術開発が重要であると考えます。こうした内容の施策として検討いただければと考えます。	政策展開に係る意見	御意見の内容につきましては、IoTシステムに限ったものではありませんが、産学官の役割分担も考慮しながら、今後の取組の検討に当たっての参考とさせていただきます。
84	NPO法人日本ネットワークセキュリティ協会	3	P.4	1.2.（3）	情報システムのセキュリティは、その開発～運用にいたる作業にたずさわるすべての人が、その持ち場でのセキュリティに気を配れなければ維持することは困難です。セキュリティ専門家の数をどれだけ増やしても、IT全体のボリュームに対してセキュリティ専門家が受け持てる範囲には限度があります。従って、一般の情報システム関連業務の従事者全体について、セキュリティ意識、知識の底上げを図る必要があると考えます。このための施策として、こうした人材におけるスキルマップに関連するセキュリティ知識を必須要件として組み込み、またそれを評価する仕組みが必要です。こうした施策も是非盛り込んでいただきたいと考えます。	政策展開に係る意見	4.2.(ア)で示した「新・人材育成プログラム」において、情報通信技術者に対し、情報システムのセキュリティのスキル向上させていくための取組がある旨記載しております。
85	NPO法人日本ネットワークセキュリティ協会	4	P.5	1.3.（1）	すべてのサイバー攻撃の被害を完全に防ぎきること(リスクをゼロにすること)は困難です。また、頻度は非常に低いが壊滅的な被害をもたらすようなインシデントも存在し、これらに対しての技術的な対応がコスト対効果の面から十分にとれない場合も考えられます。このようなケースに対しての損害補填を目的とした保険制度、ビジネスの強化も必要と考えます。	政策展開に係る意見	「サイバーセキュリティ戦略」において「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。」旨を記載しております。今後の関連産業の振興において、御指摘の内容につきましては、今後の取組の検討に当たっての参考とさせていただきます。
86	NPO法人日本ネットワークセキュリティ協会	5	P.8	2.1.（2）（エ）	昨今の標的型攻撃やフィッシングにおける詐称メール対策として、メール電子署名の普及促進に必要な、サービスや製品への実装や利用の簡素化を後押しするような施策を検討していただければと考えます。	政策展開に係る意見	御意見の内容につきましては、今後の取組の検討に当たっての参考とさせていただきます。
87	NPO法人日本ネットワークセキュリティ協会	6	P.26	4.2.（4）	我が国のセキュリティ人材の国際化推進の観点からも、既存の、また今後整備される資格制度と既に世界的に広まっていて評価の高い資格、認証制度(たとえばCISSP,CISMなど)との内容互換、相互認証の制度化を行うべきと考えます。新たな国産資格が生まれるたびに、こうした資格取得者がそれを取得、維持するのでは極めて非効率であり、既存の国際資格取得者には、同等の国内資格が付与される枠組み整備をお願いします。	政策展開に係る意見	御意見の内容については、今後の試験制度等の検討に当たっての参考とさせていただきます。
88	NPO法人日本ネットワークセキュリティ協会	7	P.30	5.（イ）	国際的に重要なイベントに際して、関連施設、サービス、重要インフラ以外の一般企業が社会混乱や対応力の分散などを狙って攻撃される可能性の検討も行う必要があります。特に、大きなイベント時期には専門家がそちらに取られ、一般企業で専門家の協力が得られにくくなる可能性もあるため、あらかじめこうした事態に備える体制作りを一般企業が推進できるような施策も併せて検討していただければと考えます。	政策展開に係る意見	御指摘の点については認識しており、そうした点も踏まえて検討してまいります。

通し番号	提出者	枝番	該当箇所		概要	意見の種類	御意見に対する考え方及び修正内容
			ページ	章節項			
89	個人(19)	1	P.2	1.1. (3) (ウ) 2.2. (3)	スマートメーターはその設置拒否が可能なようにしていただきたい。これについてセキュリティを確保するのは非常に難しいものである。(現状、WIMAX等の回線(勿論電力会社所有の設備ではない)を暗号化せずに通信がなされているという状況であるが、こんな無茶苦茶な事がまかり通る様であれば絶対に設置強制は不許可であろう。)また、個人の選択の権利を害するのは非常に良くない事である。エネルギー政策的に言うと、スマートメーターではなく電力供給側にバッファを設けてエネルギーの調整を行うべきものであるので、そもそもスマートメーターとは必要があるものではない。徒に機器を高性能化させ機能を増やしてもセキュリティ不安を発生させ国民の安全を危機に晒すだけなので、この政策は即刻見直しが必要である。	政策展開に係る意見	スマートメーターの設置そのものや電力政策の是非については、本案の意見募集の対象外です。 なお、スマートメーターの通信内容については、資源エネルギー庁に設置されたセキュリティ検討ワーキンググループの報告書(2015年7月)において、暗号化等のセキュリティ対策が盛り込まれています。
90	個人(19)	2	―	―	脆弱性の作り込みに関しては人的要素が最重要となる。これについて、国内SIerには悪質な業者が多数存在し、大手も含め実の所関わりを持っていない業者はほぼ存在しないと言える状況であるが、これらによって作り込まれる脆弱性とその修正のおろそかさは大量かつ大規模なものであるので(省庁系のサイトも多数これにより問題が作り込まれている)、即刻正常化を図っていただきたい。悪質な業者の排除は日本にとって良い事であるのはもちろん、国際社会に対しての責務でもある。	政策展開に係る意見	御意見の内容については、今後の施策の検討に当たっての参考とさせていただきます。
91	個人(19)	3	―	2.3.他	セキュリティについてはまずは「定型的なチェック」を行うべきである。サイトデザインはセキュリティ基準を満たしているか(不要なJavaScriptの排除、高強度のSSL通信が可能)等も行わずに「第三者認証等」などという事は言うべきではない。これらに反したgo.jpのサイトが一つも無くなった状態にしてから事にあたっていただきたい。また、Windowsの利用を中止にしていただきたい。業務は当然Linuxで行えるはずのものであるが、省庁から率先して業務でのWindows利用をやめていただきたい。問題発祥の源である。	政策展開に係る意見	御意見の内容については、今後の施策の検討に当たっての参考とさせていただきます。
92	個人(19)	4	―	―	クラウドについてはその利用を一考するようにしていただきたい。不要にクラウドを連呼している事態が散見される。外部にデータを置く事はセキュリティ的に望ましいものではないという原則を再度認識するよう注意をうながしていただきたい。	政策展開に係る意見	御意見の内容については、今後の施策の検討に当たっての参考とさせていただきます。
93	個人(20)	―	―	全般	しっかりと日本の国益を守るサイバーセキュリティ対策をして欲しいです。 国民の生命・財産も。効果的な取り組みをして欲しいです。	政策展開に係る意見	本計画に記載している施策を始め、「サイバーセキュリティ戦略」に基づくサイバーセキュリティ政策を着実に推進することにより、我が国の国益の確保し、国民の生命や財産を保護するよう努めてまいります。
94	(一社)重要生活機器連携セキュリティ協議会	1	―	全般	＜全般の印象＞ サイバーセキュリティ2015では、技術的対策の観点だけでなく、企業経営レベルでの対応から一般利用者への啓発、意識底上げまで幅広く対応すべきプレーヤーをカバーしており、弊協議会の考えと一致していて非常に賛同できる内容と考えます。また、各省庁が何を行うべきかを具体的に示す形式は、具体的で分かりやすいものと評価いたします。	賛同意見	賛同意見として承ります。「はじめに」にも記載のとおり、今後3年程度の基本的な施策の方向性を示す「サイバーセキュリティ戦略」の体系に沿った形で2015年度に実施する具体的な取組を記載しています。

通し番号	提出者	枝番	該当箇所		概要	意見の種類	御意見に対する考え方及び修正内容
			ページ	章節項			
95	（一社）重要生活機器連携セキュリティ協議会	2	―	1.1.（4）（イ） 1.1.（4）（エ）他	＜「IoTシステム」という用語について＞ 1.1.（4）（イ）、1.1.（4）（エ）等において、単に「IoTシステム」とすべてを一括りにするのではなく、例えば、以下のように対象を区別できる様に明記すべきであると考えます。 案1：「IoTシステム（重要インフラ・産業向け制御システム）」と「IoTシステム（一般利用者向けシステム）」 案2：「産業向けIoT制御システム」と「一般利用者向けIoTシステム」 なお、1.1.（4）（イ）、（エ）において、「IoTシステム」を「産業向けIoTシステムおよび一般利用者向けIoTシステム」と修正する。 ［理由］ 「IoT」という単語は様々な用途・分野の様々なシステム形態まで包含した非常に曖昧な用語となっています。昨年NISCより出された情報セキュリティ研究開発戦略で反映いただいたように、社会インフラ（重要インフラ）やプラントの安定稼働を担うシステムと、家電や自動車、在宅医療健康機器、HEMS等の日常生活を支える機器（生活機器）やそれらと連携するスマートフォン等のモバイルデバイスなど一般利用者が管理する形の機器群で構成されるシステムは、同じ「IoT」でも明らかにそのセキュリティの性格は違うものと感じています。 また、今年度の米国で開催されたセキュリティイベントDEFCON23では、ICS（Industrial Control System、いわゆる産業向け制御システム）と、一般利用者が扱うつながる家電やホームルータ・ホームセキュリティ製品などの機器類（これをIoTと称していた）を対象とした議論は区別されていました。これは、訓練されたシステム保守・管理者の管理の下で運用される社会システム・プラントシステムのICSと、セキュリティ管理の意識や知識の低い一般利用者が管理する生活機器のIoTシステムは区別されていることが伺えます。	修正意見	「サイバーセキュリティ戦略」で定義した「IoTシステム」は、産業向けも一般利用者向けも含めあらゆるモノがネットワークに接続されるものであることから、少なくとも本年次計画の施策において分けて記載することは適当でないものと考えます。なお、施策を具体的に推進するに当たっては、御意見の内容も参考させていただきます。
96	（一社）重要生活機器連携セキュリティ協議会	3	P.2	1.1.（3）（カ）	＜EDSA認証について＞ 「IoTシステムの構成要素であるM2M機器等のセキュリティに係る認証制度であるEDSA認証」を「産業向けIoTシステムの要素であるM2M機器等の認証制度であるEDSA認証」に修正されてはどうか。 ［理由］ EDSA認証は、よく読めば最後に「制御システム全体のセキュリティ認証制度を確立する」とあり、産業向け制御システム（ICS）の領域と読めますが、IoTと言われる機器全般にEDSA認証を適用して普及啓発していく、と誤解して読めました。 EDSA認証は、その仕様にもある通り「産業向け制御システム」を対象とした認証制度であり、管理体制下で運用されるシステムであることが前提となっています。一般利用者向けIoTシステムの認証制度は、EDSA認証は参考としつつも、別途検討が必要と考えており、同(3)-(ア)で記載されているIPA殿の取り組みがその検討基盤となることを期待しています。	修正意見	御意見を踏まえ、「IoTシステムの構成要素であるM2M機器等のセキュリティに係る認証制度であるEDSA認証」を「IoTシステムの構成要素であるM2M機器等の制御システム向けのセキュリティに係る認証制度であるEDSA認証」と修正します。
97	（一社）重要生活機器連携セキュリティ協議会	4	P.2	1.1.（3）（カ）	上記に加えて、以下を追加しては如何でしょうか。 「（どこかの組織）を通じ、一般利用者向けIoTシステムの構成要素である生　活機器等のセキュリティ に係る認証制度を確立する。」	修正意見	御意見の内容につきましては、今後の取組の検討に当たっての参考とさせていただきます。
98	（一社）重要生活機器連携セキュリティ協議会	5	P.2	1.1.（3）（キ）	以下を追加しては如何でしょうか。 「（どこかの組織）を通じ、インターネット上の公開情報を分析し、国内の一般利用者向けIoTシステム等で外部から悪用されてしまう危険性のあるシステムの脆弱性や設定の状況について、そのシステムの製造組織に対して情報を提供する。」	修正意見	セキュリティ関連機関（JPCERT/CCなど）が、例えばインターネット上に接続されたデバイスを検索するサービスやインターネット定点観測システムなどのデータを活用し、IoT 機器等の管理者に対してインシデント未然防止の観点で接続先に改善依頼を行い、必要に応じて製造ベンダへの改善の提案等を行っております。御意見の内容につきましては、今後の取組の検討に当たっての参考とさせていただきます。
99	（一社）重要生活機器連携セキュリティ協議会	6	P.3	1.1.（4）（ウ）	以下を追加しては如何でしょうか。 「（どこかの組織）において、一般利用者向けIoTシステムのテスト環境を用いシステム全体の脅威分 析、リスク評価を行う技術を開発し、評価・認証制度やサイバー演習へと活用する。」	修正意見	御意見の内容につきましては、今後の取組の検討に当たっての参考とさせていただきます。

通し番号	提出者	枝番	該当箇所		概要	意見の種類	御意見に対する考え方及び修正内容
			ページ	章節項			
100	（一社）重要生活機器連携セキュリティ協議会	7	P.3	1.1.（4）（エ）	以下を追加しては如何でしょうか。 「・・・・脅威分析及びリスク評価を行う。さらに脆弱性検証システムの開発を行う。」	修正意見	御意見の内容につきましては、今後の取組の検討に当たっての参考とさせていただきます。
101	（一社）重要生活機器連携セキュリティ協議会	8	P.3	1.1.（4）（オ）	原案に対し、以下の文言を追加しては如何でしょうか。 「アタック（攻撃）手法の調査・研究」	修正意見	御意見の内容につきまして、今後の取組の検討に当たっての参考とさせていただきます。
102	（一社）重要生活機器連携セキュリティ協議会	9	P.3	1.1.（4）（カ）	原案に対し、以下のように文言（下線部）を追加しては如何でしょうか。 「経済産業省において、自動車のセキュリティ確立に向けて、自動車業界関係者等と制御システム及びインフォテイメントシステムといった車載器等に関するセキュリティ上の課題と対策について情報交換を行い、解決に向けた方向性を得るとともに研究開発を推進する。」	修正意見	自動車のシステム変化に鑑み、自動車のセキュリティに求められる要件について引き続き検討していきます。
103	（一社）重要生活機器連携セキュリティ協議会	10	P.4	1.2.（3）（キ）	原案のあとに以下を追加しては如何でしょうか。 「・・・実践的なサイバー演習を行う。さらに、（どこかの組織において）一般利用者向けIoTシステム（例えば大量のホームゲートウェイ等）へのサイバー攻撃を想定した模擬システムを構築し、それを用いた実践的サイバー演習を行う。」	修正意見	御意見の内容につきましては、今後の取組の検討に当たっての参考とさせていただきます。
104	（一社）重要生活機器連携セキュリティ協議会	11	P.25	4.1.（エ）	原案に対し、以下の文言（下線部）を追加しては如何でしょうか。 「総務省において、NICTを通じ、2020年頃の実現を視野に、ユーザーからの要求に応じた最適な品質やセキュリティ・耐災害性等に優れた新世代ネットワークの基盤技術、及びIoT機器と通信ネットワークとが連携したIoTシステムにおける攻撃技術と防御技術の研究開発を推進する。」	修正意見	御意見の内容につきましては、今後の取組の検討に当たっての参考とさせていただきます。
105	（一社）重要生活機器連携セキュリティ協議会	12	P.25	4.1.（1）（エ）	原案に対し以下を追加しては如何でしょうか。 「（どこかの組織を通じて）、一般利用者向けIoTシステムの挙動を解析し、サイバー攻撃を検知する技術開発や、ホワイトリスト技術に関する研究を行う。」	修正意見	御意見の内容につきましては、今後の取組の検討に当たっての参考とさせていただきます。