「サイバーセキュリティ2016（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： 2016年６月13日（月）～ ６月27日（月）
- 意 見 総 数： 15者から90件 【内訳：４企業・団体から延べ26件、11個人から延べ64件】

（１）修正意見： 全53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40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13件）

（２）政策展開に係る意見： 全31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

（３）その他意見： 全６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：

NPO法人 日本ネットワークセキュリティ協会、一般社団法人全国銀行協会、一般社団法人電子情報技術産業協会、日本オラクル株式会社、個人（11）

「サイバーセキュリティ 2016（案）」に係る意見募集の結果一覧

通し No.	提出者	該当箇所		概要	御意見に対する考え方及び修正	意見の種類
		ページ	章節項			
1	個人（1）	―	全般	サイバーセキュリティは世界的情報戦の主軸であり、日本の防衛にも深く関わっていることから、サイバーセキュリティについて防衛省は深く関与するべき。また、日本独自のイントラが必要と感じられる。 なお、現在のサイバーセキュリティセンターの人事では、全ての問題に精通し管理できる人材が不足しており、サイバーセキュリティに関する責任者が必要である。	我が国の安全の確保については、防衛省や警察庁等を中心として対策を強化しているところであり、引続き検討してまいります。 また、内閣サイバーセキュリティセンターの人事に関する御意見につきましては、今後の体制・人員配置の検討に当たっての参考とさせていただきます。	その他
2	個人（2）	2	1.1.（3）（イ）	電気事業法の保安規制の対象として、スマートメーターのセキュリティガイドラインの他、電力制御システムに関するガイドラインも対象とすべきではないか。 ［理由］ JESCの民間規程としては、スマートメーターシステムセキュリティガイドラインと電力制御システムセキュリティガイドラインを、既に策定、承認済み。	御意見を踏まえ、以下のように修文いたします。 「経済産業省において、策定されたスマートメーターシステム及び電力制御システムに係るセキュリティガイドラインを電気事業法の保安規制に位置付ける。」	修正意見
3	個人（3）	―	2.1.（2）	インシデント発生時に必要な業務（フォレンジック、法的作業、委員会の設置など）を依頼可能な事務所・企業等のポータルを設置していただきたい。 ［理由］ インシデント発生時において、業者の検索・選択をする時間的余裕はないため、官公庁によって認定された対象を素早く検索できるようにしていただきたい。	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。	その他
4	個人（4）	2	1.1.（3）（イ）	当該ガイドライン及び経済産業省の規制は、電気事業者側のAルートを対象としたものであるため、「2.2 重要インフラを守るための取組」として記載した方が良いのではないか。	御意見を踏まえ、「2.2,（3）各分野の個別事情への支援」に掲載いたします。	修正意見

「サイバーセキュリティ 2016（案）」に係る意見募集の結果一覧

通し No.	提出者	該当箇所 ページ	該当箇所 章節項	概要	御意見に対する考え方及び修正	意見の種類
5	個人（5）	―	全般	次のような概念のセキュリティシステムを提案します。 【超セキュリティシステム】 世界最高にセキュリティレベルの高いIoTシステムを、日本国政府の中枢に1つは設置します（「超セキュリティシステム」）。超セキュリティシステムは、他のシステムのセキュリティ状態のチェックの主体になるとともに、壊滅的なサイバー攻撃に対抗する最後の砦ともなります。 【超セキュリティシステムのアーキテクチャ】 サイバー攻撃をするためのコンピュータウィルスなどを設計できないよう、CPUもメモリーも通信デバイスも、オペレーティングシステムも日本国政府独自のものであって、既存の汎用品とは設計思想が全く異なるものを用います。ただし、既存の情報処理システムとの通信のため、データは必ずブロックチェインに登録したデータだけを用います。	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。	その他
6	日本オラクル株式会社	16	2.3.（1）（チ）	「標的型攻撃に対する多重防御の取組を引き続き推進する。」を「標的型攻撃に対する多層防御の取組を引き続き推進する。」としてはどうか。 ［理由］ 当該施策は2.3（1）の多層な対策の一つとして言及しています（（1）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）。 また、「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」の中には「多重防御」という用語が使われていますが、本ガイドラインが参照・引用している資料の2014年6月以降では「多層防御」が使われているようです。 ・『高度標的型攻撃』対策に向けたシステム設計ガイド ・サイバーセキュリティ経営ガイドライン この用語の由来はNIST SP800-37 rev.1 『連邦政府情報システムに対するリスクマネジメントフレームワーク適用ガイド』（2010年版）におけるMultitier Organization-Wide Risk Managementであり、これが「組織全体の多層的なリスクマネジメント」と訳されて広く紹介されていることから、「多層防御」と称することが妥当かと考えます。	御意見につきましては、「サイバーセキュリティ戦略」において、「標的型攻撃に対する多重防御の取組を加速する」と記載しており、これに対応する施策となりますので、原案のとおりとさせていただきます。	修正意見

「サイバーセキュリティ 2016（案）」に係る意見募集の結果一覧

通し No.	提出者	該当箇所		概要	御意見に対する考え方及び修正	意見の種類
		ページ	章節項			
7	日本オラクル株式会社	34	用語解説	用語解説に「セキュリティ・バイ・デザイン」の追加を希望します。 ［理由］ 本文で「セキュリティ・バイ・デザイン」への言及が多いため、用語解説として説明を追加することにより、対象読者の理解が深まるため。	頂いたご意見の通り、用語解説に「セキュリティ・バイ・デザイン」を追加いたします。	修正意見
8	個人（6）	－	全般	本計画は2016年度の年次計画なのですから、2016年度が数ヶ月経過した現時点での作成は時期が遅いのではないのでしょうか。（たとえば、28頁の5.（ウ）に記載されている「伊勢志摩サミット」はすでに終了したものです）	サイバーセキュリティ2016の策定時期については、毎年度の年次報告における各府省庁の施策の評価も踏まえるとともに、意見募集のプロセスを経ることとしていることから、年次報告取りまとめ後になっているものです。策定時期の更なる前倒しについては、今後の検討課題として承ります。	その他
9	個人（6）	1	はじめに	1頁の第三段落の2行目「モノ」： 30頁の解説では「物」と記載されていますが、どちらが正しいのですか？	御意見を踏まえ、「モノ」に統一いたします。	修正意見
10	個人（6）	2	1.1.（3）他	2頁の（3）で「（イ）経済産業省・・・」のあとに「（ウ）厚生労働省・・・」が記載されていますが、記載の順番は建制順とするのが適当であると思います。（他の記載箇所についても同様）	施策の順番は「サイバーセキュリティ戦略」の記載等も参考に決定しておりますので、原案どおりといたします。	修正意見
11	個人（6）	3	1.1.（3）（イ）	3頁の（4）（イ）「IoT」： 「IoTシステム」と記載したほうが適当では？	当該施策につきましては、「システム」に含まれないものも対象としているため、原案どおりといたします。	修正意見
12	個人（6）	4	1.2.（3）（オ）他	4頁の（オ）の2行目「2020東京オリンピック」、15頁の（コ）「2020年東京オリンピック」、28頁の（ア）の3行目等「東京オリンピック」については、文言の統一化が必要です。	御意見を踏まえ、「2020年東京オリンピック・パラリンピック競技大会」に統一いたします。	修正意見
13	個人（6）	4	1.2.（3）（サ） 1.2.（3）（シ） 3.3.（2）（イ）	4頁の最終行「ICT-ISAC」、5頁の1行目「金融ISAC」、23頁の7行目「ISAC」について、「参考　用語解説」で解説してください。	御意見を踏まえ、「ISAC」を用語集に追加いたしました。	修正意見
14	個人（6）	6	1.3.（3）（カ） 1.3.（3）（キ）	6頁の（カ）の1行目、2行目「日本」と（キ）の1行目「我が国」は文言の統一化が必要です。	御意見を踏まえ、「我が国」に統一いたします。	修正意見

「サイバーセキュリティ 2016（案）」に係る意見募集の結果一覧

通し No.	提出者	該当箇所		概要	御意見に対する考え方及び修正	意見の種類
		ページ	章節項			
15	個人（6）	7	2.1.（1）（ケ）	7頁の（ケ）の1行目「高度化」： 反社会的なマルウェアに対しての形容詞としては不適当な文言だと思います。	マルウェアがより悪質に進化する様を表現するため、原案のとおりといたします。	修正意見
16	個人（6）	8	2.1.（2）（ア）	8頁の（2）（ア）の2行目等の「始め」： 他の記載箇所の「はじめ」との文言の統一化が必要です。	御意見を踏まえ、「はじめ」に統一いたします。	修正意見
17	個人（6）	9	2.1.（2）（カ）	9頁の3行目「7カ所」： 他の記載箇所での例にならって「7ヶ所」のほうが適当です。	「公用文の書き方」（昭和35年三訂版：文部省）P.264に基づき、「か所」で統一いたしました。	修正意見
18	個人（6）	9	2.1.（2）（カ）	9頁の3行目「フォーラム含む」：「フォーラムを含む」と記載するのが自然です。	御意見を踏まえ、「フォーラムを含む」に修正いたします。	修正意見
19	個人（6）	10	2.1.（3）（イ）	10頁の（3）（イ）の2行目「各都道府県警察」： 他の記載箇所と異なりここだけ「各」を記載したのはなぜですか？	御意見を踏まえ、「都道府県警察」に修正いたします。	修正意見
20	個人（6）	10	2.1.（3）（カ）	10頁の（3）（カ）の1行目「サイバーセキュリティ対策研究・研修センター」： 警察大学校のHPでは名称が「サイバーセキュリティ研究・研修センター」となっています。	御指摘誠にありがとうございます。警察大学校Webサイト上の記述を、「サイバーセキュリティ対策研究・研修センター」に修正いたしました。	修正意見
21	個人（6）	11	2.1.（3）（ク）	11頁の5行目「電気メータ」： 他の記載箇所での用例（スマートメーター）にあわせて「電気メーター」と記載するのが適当です。	御意見を踏まえ、「電気メーター」に修正いたします。	修正意見
22	個人（6）	11	2.1.（3）（コ） 3.2.（2）（イ）	11頁の（コ）の1行目「サイバー犯罪に関する条約」： 19頁の（1）（イ）の3行目等の「サイバー犯罪条約」とはおなじものを指しているのでしょうか？	御意見を踏まえ、「サイバー犯罪に関する条約」に修正いたします。	修正意見
23	個人（6）	14	1.1.（1）（ア） 2.3.（1）（ウ）	14頁の（ウ）の2行目「セキュリティ・バイ・デザイン」の定義は、初出の2頁の（1）（ア）の1行目で定義するのが適当です。	御意見を踏まえ、用語解説に「セキュリティ・バイ・デザイン」を追加します。	修正意見

「サイバーセキュリティ 2016（案）」に係る意見募集の結果一覧

通し No.	提出者	該当箇所 ページ	該当箇所 章節項	概要	御意見に対する考え方及び修正	意見の種類
24	個人（6）	15	2.3.（1）（コ）	15頁の（コ）の「GSOCシステム」、「GSOCセンサー」については、30頁の「GSOC」の用語解説での記載が必要だと思います。	御意見を踏まえ、用語解説「GSOC」において「GSOCシステム」及び「GSOCセンサー」に係る記述を追記いたします。	修正意見
25	個人（6）	15	2.3.（1）（ス）	15頁の（ス）の6行目等の「インシデント・ハンドリング」： 他の箇所で記載の「インシデント対処」との違いは何ですか？	御指摘を踏まえ、「インシデント対処」で表記を統一いたします。	修正意見
26	個人（6）	15	2.3.（1）（ス） 2.3.（1）（ソ）	15頁の（ス）の最終行「NATIONAL CYBER EKIDEN」と16頁の2行目「NATIONAL 318(CYBER) EKIDEN」は違うものなのでしょうか？	御指摘を踏まえ、「NATIONAL 318(CYBER) EKIDEN」で統一いたします。	修正意見
27	個人（6）	16	2.3.（1）（タ）	16頁の4行目「フォレンジック調査」は「デジタルフォレンジック調査」のほうが適当だと思います。	御意見を踏まえ、「デジタルフォレンジック調査」に修正いたします。	修正意見
28	個人（6）	19	3.2.（ア）	19頁の「定点観測情報共有システム」と32頁の「TSUBAME」の解説の「定点観測システム」とはどちらが正しい名称なのでしょうか？	御意見を踏まえ、正式名称である「インターネット定点観測システム」に修正いたします。	修正意見
29	個人（6）	20	3.2.（2）（ア）	20頁（2）アの3行目「サイバーセキュリティ戦略」： 1頁で定義した略称の「戦略」で記載すべきところです。	ご意見を踏まえ、「はじめに」の内容を修正いたします。	修正意見
30	個人（6）	21	3.2.（4）（ア）	21頁の10行目「UNODC」：「参考 用語解説」で解説してください。	御意見を踏まえ、用語解説に「UNODC」を追加いたしました。	修正意見
31	個人（6）	21	3.2.（5）（ア）	21頁の（5）（ア）の3行目「わが国」： 他の記載箇所とあわせて「我が国」とすべきところです。	御意見を踏まえ、「我が国」に修正いたします。	修正意見
32	個人（6）	21	3.3.（イ） 5.（ウ）	21頁の3．3（イ）の「G7伊勢志摩サミット」と28頁の（ウ）の「伊勢志摩サミット」とについては、文言を統一化するのが適当であると思います。	御意見を踏まえ、「G7伊勢志摩サミット」に修正いたします。	修正意見
33	個人（6）	21	3.2.（4）（ア） 用語解説	21頁の「アジア・太平洋電気通信共同体」と29頁の「APT」の解説の「アジア太平洋電気通信共同体」とはどちらが正しい名称なのでしょうか？	御意見を踏まえ、「アジア・太平洋電気通信共同体」で統一いたします。	修正意見

「サイバーセキュリティ 2016（案）」に係る意見募集の結果一覧

通し No.	提出者	該当箇所 ページ	該当箇所 章節項	概要	御意見に対する考え方及び修正	意見の種類
34	個人（6）	29	用語解説	29頁の「CCRA」の解説の「CCに基づいた」の「CC」とは何を意味しているのですか？	御意見を踏まえ、用語解説に「CC」を追加いたしました。	修正意見
35	個人（6）	30	用語解説	29頁の「DDoS攻撃」： この用語は本文には記載が見当たりません。	御意見を踏まえ、削除いたします。	修正意見
36	個人（6）	30	用語解説 3.2.（1）（ウ）	30頁の「G8」： 本文に記載のある「G7」についても解説してください。	御意見を踏まえ、用語解説を「G7/G8」に修正いたします。	修正意見
37	個人（6）	30	用語解説	30頁の「G8」の解説の「8か国」： 他の記載箇所での例にならって「8ヶ国」のほうが適当です。	「か所」で統一いたしましたので、原案通りとさせていただきます。	修正意見
38	個人（6）	30	用語解説	30頁の「GSOC」： 本文での記載は「政府機関情報セキュリティ横断監視・即応調整チーム（GSOC）」なので、英語ではなく日本語の用語解説として記載したほうが適当です。	略称の用語解説という位置づけですので、原案通りとさせていただきます。	修正意見
39	個人（6）	31	用語解説	31頁の「JHAS」の解説の「SWGの略」は、「Sub Working Groupの略」を意味しているのでしょうか？	御意見を踏まえ、解説の1文目を、「Joint Interpretation Library（JIL）Hardware-related Attacks Subgroupの略」と修正いたします。	修正意見
40	個人（6）	31	用語解説	31頁の「JHAS」の解説の「作業部会」は「JIWG傘下の作業部会」のほうが適当と思います。	御意見を踏まえ、解説の2文目を、「欧州の認証機関、評価機関、スマートカードベンダ、ユーザーなどからなるJIWG傘下の検討部会。」と修正いたします。	修正意見
41	個人（6）	31	用語解説	31頁の「JIWG」の解説の「WGの略」は、「Working Groupの略」を意味しているのでしょうか？	御意見を踏まえ、解説の1文目を「Joint Interpretation Library（JIL） Working Groupの略。」と修正いたします。	修正意見
42	個人（6）	31	用語解説	31頁の「JTEMS」の解説の「検討部会」は「JIWG傘下の検討部会」のほうが適当と思います。	御意見を踏まえ、解説の2文目を、「カード端末セキュリティに関するJIWG傘下の検討部会」と修正いたします。	修正意見

「サイバーセキュリティ 2016（案）」に係る意見募集の結果一覧

通し No.	提出者	該当箇所		概要	御意見に対する考え方及び修正	意見の種類
		ページ	章節項			
43	個人（6）	31	用語解説	31頁の「NISC」と34頁の「内閣サイバーセキュリティセンター」の解説の記載内容は重複していますので、どちらかの記載は削除するのが適当です。	正式名称に加え、意図的に略称についても掲載したものですので、原案通りとさせていただきます。	修正意見
44	個人（6）	32	用語解説	32頁の「PP」の解説の「CCに従って」の「CC」とは何を意味しているのですか？	御意見を踏まえ、用語解説に「CC」を追加いたしました。	修正意見
45	個人（6）	32	用語解説	32頁の「機密性」: この用語は本文には記載が見当たりません。	機密性、完全性、可用性は情報セキュリティの三大要素であり、参考情報として記載しておりますので、原案通り掲載いたします。	修正意見
46	個人（6）	33	用語解説	33頁の「重要インフラ所管省庁」のうち、国土交通省の取組についての記載が本計画に記載されていないのはなぜですか？	2.2(ア)や2.2(1)(ア)において国土交通省も含めた重要インフラ所管省庁全てに共通する取組が記載されています。	修正意見
47	個人（6）	34	用語解説	34頁の「政府統一基準群」: 本文で記載されている用語は「統一基準群」です。	御意見を踏まえ、「統一基準群」で統一いたします。	修正意見
48	個人（6）	34	用語解説	34頁の「中央当局制度」: 本文で記載されている用語は「中央当局」です。	御意見を踏まえ、用語解説「中央当局制度」については削除いたします。	修正意見
49	個人（6）	39	用語解説	39頁の「リテラシー」の解説の「情報リテラシー」: 本文での用例「インターネットリテラシー」についての解説もお願いします。	御意見を踏まえ、用語解説「リテラシー」の例示を「インターネットリテラシー」に修正いたしました。	修正意見
50	個人（7）	－	2.1.(2) (シ)	BCPへの取組も含まれるのであれば、「2.1 国民・社会を守るための取組」ではなく「2.2 重要インフラを守るための取組」とした方が項目の整合性が取れるのではないかと思います。	御意見を踏まえ、「2.2, (3) 各分野の個別事情への支援」に掲載いたします。	修正意見
51	個人（8）	－	4.2.	情報セキュリティを学ぶことのできる大学が不足していると感じます。情報工学といった学部がある大学であっても情報セキュリティに特化した学部がある学校は少なく、国公立に限るとほんのわずかの学校でした情報セキュリティを学ぶことができません。給与の改善はもちろんですが、教育機関の充実なども必要だと考えます。	「サイバーセキュリティ人材育成総合強化方針」（平成28年3月サイバーセキュリティ戦略本部決定）において、「産学官が連携した教育の充実」の必要性について示し、高等専門学校や大学、大学院等での取組について推進するとしたところです。御意見も踏まえ、各種施策を推進してまいります。	政策展開に係る意見

「サイバーセキュリティ 2016（案）」に係る意見募集の結果一覧

通し No.	提出者	該当箇所		概要	御意見に対する考え方及び修正	意見の種類
		ページ	章節項			
52	個人（8）	－	2.1.	「Tor」などのp2p技術を用いた匿名でのインターネットの閲覧や投稿に関する記述がないこと疑問に思いました。この技術を用いて、サイバー犯罪などが行われた際に事後追跡可能性がとても低くなってしまうことは非常に問題であると考えます。この点についての加筆をお願いします。	事後追跡可能性に関する取組につきましては、2.1.(1)（ス）、2.1.(3)（サ）に記載の取組をはじめ、警察庁や総務省等において今後も適切に取り組んでまいります。	政策展開に係る意見
53	個人（8）	5	1.3.（1）（ア） 2.1.（3）（エ）	サイバーセキュリティの産業化は今後、日本において非常に重要であり、サイバーセキュリティを行う企業やサイバーボランティアに対して法律などを含む特例の策定などが必要だと考えます。	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。	政策展開に係る意見
54	個人（8）	5	1.3.（1）（エ）	著作権法において、セキュリティ目的の特例措置が認められた上で、企業との利用規約に対しても効力のある法律が策定される必要があると考えます。また、一般人がリバースエンジニアリングで脆弱性が発見した場合などに、その情報を報告することのできる機関も必要だと考えます。	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。	政策展開に係る意見
55	個人（9）	2	1.1.（1）（ア）	IoTに係るセキュリティ確保について記載された内容にて、「セキュリティ・バイ・デザイン」が強調されていることが読み取れるが、少々唐突に言葉が登場している感がある。IoTにおけるセキュリティ・バイ・デザインを強調する理由について少し触れた方がよいのではないか。 例えば、以下のような文章を挟み込んではどうか。「社会の重要なインフラを担う可能性のあるIoTにおいては、強固で、漏れのないセキュリティ確保が必要となる。この実現のためには、設計段階からのセキュリティの作り込みや、その意識の醸成が重要となる。」等。	「セキュリティ・バイ・デザイン」の必要性については、サイバーセキュリティ戦略に記載しておりますので、原案通りとさせていただきます。	修正意見
56	個人（9）	2	1.1.（3）（ア）	「IoTセキュリティガイドラインをとりまとめ、普及に努める」とあるが、セイバーセキュリティ2015と変わらず、ガイドラインの作成についてや、具体的な進め方が記載されていないため、記載するとよい。	「IoTセキュリティガイドライン」は、平成28年７月５日に決定し、今後本ガイドラインの事業者等への普及を行っていくため、原案どおりとさせていただきます。	修正意見
57	個人（9）	10	2.1.（3）（エ）	「サイバー空間におけるボランティア活動」の具体例を記載いただきたい。	御意見を踏まえ、「警察庁において、サイバー空間における犯罪被害防止のための教育等のボランティア活動の促進を図るため、サイバー防犯ボランティアの結成を促すとともに活動の支援を強化することにより、安全で安心なインターネット空間の醸成に向けた取組を推進する。」に修正いたします。	修正意見

「サイバーセキュリティ 2016（案）」に係る意見募集の結果一覧

通し No.	提出者	該当箇所		概要	御意見に対する考え方及び修正	意見の種類
		ページ	章節項			
58	個人（9）	11	2.1.（3）（ク）	サイバー犯罪に的確に対処するため、情報技術解析部門をひとつの組織とするなど一元化することで資源を有効に使うことは検討しないのか。情報セキュリティに係る人材はIT人材の中でも特に少ないとされているため、効果的かつ効率的な解析のために集中化することは一つの選択肢であると考える。	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。	政策展開に係る意見
59	個人（9）	14	2.3	2015年6月発生の日本年金機構における個人情報流出事案を受けて、2015年8月にNISCから厚生労働省に対し、勧告の中で個人情報等の重要情報を含む情報システムの分離を行うことを求めているが、同様の措置を政府機関に展開するための施策は検討しないのか。政府機関においては、日本年金機構が有する個人情報と同様の個人情報を大量に扱っており、厚生労働省に当該措置を求めるのであれば、政府機関全体に求めることも検討すべきと考える。	御指摘の、個人情報等の重要情報を含む情報システムの分離を政府機関に展開するための施策については、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の規定を見直し・強化することにより対応する予定です。	政策展開に係る意見
60	個人（9）	14	2.3	政府機関全体を通じて、府省庁等各機関でサイバーセキュリティ人材を個別に確保することが、常態的に難しい状況にあると思料するが、例えば内閣官房が主導して以下のような取組を行うことは検討しないのか。 ・各政府機関に派遣するためのサイバーセキュリティに係る専門的な人材を一元的に雇用する。 （例えば、内閣官房が主導して、上記のための取組（組織・体制の整備等）を行う。） ・各政府機関には、上記で採用した専門的な人材を派遣し、サイバーセキュリティに係る専門的な事務を行ってもらう。 ・当該人材は定期的に政府機関を異動することで、複数の政府機関におけるサイバーセキュリティ対策の取組状況の認識等から政府機関のサイバーセキュリティ対策水準向上への寄与を期待する。	御指摘の課題については、「サイバーセキュリティ人材育成総合強化方針」（平成28年3月31日サイバーセキュリティ戦略本部決定）第2章2.（3）において、セキュリティ・ITに一定の専門性を有する人材の育成のため、「将来的に、一部の人材を総務省行政管理局等で採用・一括管理し、各府省庁等に派遣する枠組みを検討する。（各府省庁の人材育成に目途が立った段階での実施に向け検討）」という方針が示されており、検討が行われているところです。	政策展開に係る意見

「サイバーセキュリティ 2016（案）」に係る意見募集の結果一覧

通し No.	提出者	該当箇所		概要	御意見に対する考え方及び修正	意見の種類
		ページ	章節項			
61	個人（10）	5	1.3.（3）	今後『世界最先端IT国家創造宣言』に基づき、紙文書の電子化、ペーパーレス化が急速に発展すると想定する中で、日本における電子化のアプリケーションや電子署名に関するトラストリストを作成すべきと考えます。また、国際化を検討する中においては少なくともEUのEUのeIDAS（Electronic identification and trust services.）との相互運用性を確保すべきと考えます。 そのために、定期的、逐次的に欧州の動向を把握し、かつ必要に応じて提言を実施できる環境を整えておくようにすべきです。内容としては、「1.3.（3）我が国企業の国際展開のための環境整備」に追加が望ましいと考えます。 なお「トラストサービス」とは以下の電子サービスと指します。 1.電子署名、タイムスタンプなどのサービスに関連する証明書の生成、検証、照合 2.ウェブサイト認証の為の証明書の生成、検証、照合 3.これらのサービスに関連する電子署名、シール、又は証明書の保存 トラストリストの作成に関しては、国による実施が想定いたしますが、業務によっては、一部民間企業への委託も考慮できるものと考えます。	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。	政策展開に係る意見
62	一般社団法人全国銀行協会	3	1.2.（1）（ア）	投資家へのリスク開示の内容・範囲・周期・方法は、上場企業にとって過度の負担とならないものであることが望ましい。	内閣官房において、セキュリティマインドを持った企業経営WGを開催し、サイバーセキュリティへの対処状況についての情報発信の在り方について検討しております。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。	政策展開に係る意見
63	一般社団法人全国銀行協会	3	1.2.（1）（ウ）	企業のサイバーセキュリティ対策への取組を評価する場合、優良企業の対応負荷が増えないよう、国内外の既存の各種基準やガイドラインを活用いただきたい。	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。	政策展開に係る意見
64	一般社団法人全国銀行協会	4	1.2.（3）（ウ）	再委託管理については、委託先事業者の独立性を要求する労働者派遣法との整合性を明確にしていただきたい。 また、委託先事業者におけるセキュリティ対策の状況を確認するための標準的な様式が整備されることが望ましい。	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。	政策展開に係る意見

「サイバーセキュリティ 2016（案）」に係る意見募集の結果一覧

通し No.	提出者	該当箇所		概要	御意見に対する考え方及び修正	意見の種類
		ページ	章節項			
65	一般社団法人全国銀行協会	7	2.1.（1）（カ）	脆弱性情報の配信では、国内外におけるセキュリティ情報交換の方式に関する議論に準拠していただきたい。	脆弱性情報の配信においては、社会的なニーズに応じた標準的な記述形式の採用についても検討したいと考えています。	政策展開に係る意見
66	一般社団法人全国銀行協会	7	2.1.（1）（コ）	JPCERT/CCが解析したマルウェア検体情報の共有に際しては、情報提供源の秘匿に十分な注意が払われる必要がある。	経済産業省およびJPCERT/CCは、情報提供者がJPCERT/CCに対する信頼のもとに情報提供を行っている点を十分に認識しており、統計情報として活用する場合も含めて提供元に関する情報の秘匿化等について配慮しつつ、共有先等の認識についても考慮しながら、共有の要否や内容について判断・実施しております。	政策展開に係る意見
67	一般社団法人全国銀行協会	11	2.2.（オ）他	政府による演習・訓練の並立に際しては、目的および想定される参加者の棲み分けを相互に調整して明示いただきたい。	御指摘の事項は重要であると考えており、演習・訓練を実施するに当たっては、関係機関間で調整をしてまいります。	修正意見
68	一般社団法人全国銀行協会	12	2.2.（2）（カ）	重要インフラ事業者等が保有するシステムに対する脆弱性試験は、その必要性は理解できるが、実施方法については、事業者の負担、事業への影響が最小限になるよう、ご配慮をいただきたい。既に事業者で試験を実施している場合は、その結果を参照すること等も検討いただきたい。	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。	政策展開に係る意見
69	一般社団法人電子情報技術産業協会	－	全般	サイバーセキュリティ2016（案）の各項目について、主語が府各省庁の記載となり、対応する組織が明確でわかりやすい表現となっているが、サイバーセキュリティ2016全体として、どの組織がどのような役割を担っているかの組織視点での全体が俯瞰できる構成概要がまとまっているとよい。 ［理由］ 「サイバーセキュリティ2016（案）」の概要資料と、「サイバーセキュリティ2016（案）」をつなげる各組織視点での構成概要がないが、全体が俯瞰できる構成概要がまとまっていると、より理解しやすいため。	サイバーセキュリティ2016の各項目については、施策の実施主体を明確にする観点から、各省庁を主語とした記述にしています。他方、全般的に、複数省庁が連携して取り組む施策が多くなっていることも踏まえ、概要資料については、組織ごとにまとめたものとはせず、サイバーセキュリティ戦略の項目ごとにまとめた形としています。御意見については、今後、より分かり易い資料とするためのものとして承ります。	その他

「サイバーセキュリティ 2016（案）」に係る意見募集の結果一覧

通し No.	提出者	該当箇所		概要	御意見に対する考え方及び修正	意見の種類
		ページ	章節項			
70	一般社団法人電子情報技術産業協会	－	全般	ビッグデータやクラウドの活用促進による国内の産業が活性化できる方向の取組みに関しても盛り込んでいただきたい。 ［理由］ ビッグデータやクラウドの活用に関しては、適切なセキュリティ対策が分からないため、安全方向に倒してしまうという現状があり、極端な例では、一切情報を提供しない、クラウド接続禁止といったセキュリティ対策になってしまう場合もある。「適切なセキュリティ対策が取られていれば、情報提供やクラウド活用をしてもよい」という認識を持っていただくことが、国内産業の活性化につながると考えるため。	御指摘の点については重要と考えており、4.1.(2)（イ)の取組等において検討を進めてまいります。	政策展開に係る意見
71	一般社団法人電子情報技術産業協会	2	1.1.（1）（ア）	セキュリティ・バイ・デザインの考えにおいて、IoTシステム／IoTデバイス自体のアップデート等継続的なセキュリティ維持管理機能を盛り込む旨配慮いただきたい。 ［理由］ 家電や自動車、組み込み機器、各種センサなどのIoTシステム／IoTデバイスは、10年を超えて利用されることがあり、耐用年数も相応の期間が考慮されており、長期の利用に耐えられる必要があるため。	御指摘のとおり、セキュリティ・バイ・デザインの考え方は、IoTシステムのライフサイクル（企画・設計・開発・運用・廃棄）に関して、企画・設計段階から情報セキュリティの観点を意識し、その際に必要となる調達仕様にセキュリティ要件を適切に組み込むこととしています。	政策展開に係る意見
72	一般社団法人電子情報技術産業協会	2	1.1.（3）（ア）	IPA 公開文書との役割や位置づけ等も整理の上で、IoTセキュリティガイドラインの普及に努めると、読者は理解が整理されて良い。 ［理由］ 「IoTセキュリティガイドライン」もIPAと連携しつつ取りまとめられたものであり、IPAにおいても5月に「IoT 開発におけるセキュリティ設計の手引き」を公開しており具体的な脅威分析もされている。 IoTセキュリティガイドライン以外にもこの分野の公開文書は諸々あるので、他ガイドとの役割や位置づけや想定読者などを大上段で整理されると、読者としても整理して読み分けしやすくなり、「IoTセキュリティガイドライン」のより一層の普及になると考えるため。	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。	政策展開に係る意見

「サイバーセキュリティ 2016（案）」に係る意見募集の結果一覧

通し No.	提出者	該当箇所		概要	御意見に対する考え方及び修正	意見の種類
		ページ	章節項			
73	一般社団法人電子情報技術産業協会	2	1.1.（3）（ウ）	使用者のヘルスケア情報を収集・管理するウェアラブル端末やサービスが存在している。取り扱う情報の機微度は医療情報より低いと考えられるものの、パーソナルデータの一つとして取扱いに配慮するよう記載していただきたい。 ［理由］ 医療機器だけでなく、ヘルスケア情報を収集・管理するウェアラブル端末やサービスの取り扱う情報についても配慮が必要であると考えるため。	策定予定のガイドライン（1.1.（3）（ウ））は、医療機器のサイバーセキュリティに関するものとなります。御指摘のサービス等で取り扱われる情報の扱いについては、一般的なIoT機器のセキュリティ対策に関する御意見として、今後の施策の参考とさせていただきます。	政策展開に係る意見
74	一般社団法人電子情報技術産業協会	2	1.1.（3）（カ）	「これまで対象としていなかった案件」について、具体的な例示の記載があるとよい。また、「能動的な」について、具体例の記載があるとよい。 ［理由］ ・案件が何を指しているかが不明である。具体的な例示があると、ここで述べたい内容の理解が深まるため。 ・現在の対応が受動的であり、その改善のために能動的な対応をご検討されていると思うが、能動的な対応の内容が不明瞭である。具体例があると、ここで述べたい内容の理解が深まるため。	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。	修正意見
75	一般社団法人電子情報技術産業協会	3	1.2.（1）（イ）	経営層の意識改革のため、説明会だけでなく他にも具体的な施策を交えて、より一層の支援をお願いする。 ［理由］ IoTセキュリティガイドラインに記載あるように、経営者がIoTセキュリティにコミットすることが、IoT普及の点でも肝要と考えるため。	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。	政策展開に係る意見
76	一般社団法人電子情報技術産業協会	3	1.2.（2）（ア）	「橋渡し人材層」の活躍が、今後のサイバーセキュリティ対策の推進に大変重要な役割になってくると考えるが、社会的に認知される職種等の定義が必要である。 ［理由］ 国内において、真のセキュリティエバンジェリストとなり得る人材が、「橋渡し人材層」と考えますが、推進する方法の開発等のみでは、活躍が認知されない懸念があるため。	「サイバーセキュリティ人材育成総合強化方針」（平成28年3月サイバーセキュリティ戦略本部決定）において、「「橋渡し人材」の育成」の必要性について示したところです。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。	政策展開に係る意見

「サイバーセキュリティ 2016（案）」に係る意見募集の結果一覧

通し No.	提出者	該当箇所		概要	御意見に対する考え方及び修正	意見の種類
		ページ	章節項			
77	一般社団法人電子情報技術産業協会	4	1.2.（3）（ウ）	民間企業においてはそのビジネス戦略上、特定分野の業務を関係会社に移管することにより、企業グループ全体として経営資源の最適配分を図る事業構造をとっている場合が少なくない。このような場合において、各企業はグループ内での統一的なサプライチェーン全体のセキュリティ対策を実施しており、本項が指摘するリスクの高い丸投げ下請けや発注者が把握できない多重の再委託とは本質的に異なるものである。政府にはこのような企業経営の実態も勘案の上、サプライチェーン全体のセキュリティ向上に資する適切な制度整備をお願いしたい。 ［理由］ 企業経営上の観点から、グループ会社と役割分担を行っている企業の実態を理解して頂くことで、効率的かつ効果的なサプライチェーン全体のセキュリティ向上策の検討を行って頂きたいため。	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。	政策展開に係る意見
78	一般社団法人電子情報技術産業協会	4	1.2.（3）（ク）	「金融庁において、金融業界横断的なサイバーセキュリティ演習を実施する」とあるが、具体的な方式についてお考えがあれば盛り込まれてはどうか。 1.2.（3）（カ）「経済産業省において、重要インフラ企業等に対する標的型攻撃への対処能力向上のため、模擬システム等を用いた実践的なサイバー演習を行う」と同様の記述にするのが良いと考える。 ［理由］ 具体的な方法の記載があると理解が深まるため。	御意見を踏まえ、以下のように修文いたします。 「金融庁において、参加金融機関および金融業界全体のセキュリティレベルの底上げを図るため、攻撃の実例分析を踏まえた金融業界横断的なサイバーセキュリティ演習を実施する」	修正意見
79	一般社団法人電子情報技術産業協会	7	2.1.（1）（エ）	ソフトウェアは、アプリケーション、ミドルウェア、OSを一般的にイメージするが、ハードウェアに対するファームウェアも含めているのかどうかが不明瞭。ファームウェアについても言及すべきと考える。 ［理由］ ファームウェアも対象に含まれていることが明確になるため。	IPAにおいては、組込みシステム（ハードウェアに対するファームウェアも含む）についても、利用者への品質説明力の強化を図っていることから、今後も、安全性・信頼性等の向上に努めてまいります。御指摘を踏まえ、「情報処理システム等」を「情報処理システムや組込みシステム等」に修正いたします。	修正意見

「サイバーセキュリティ 2016（案）」に係る意見募集の結果一覧

通し No.	提出者	該当箇所		概要	御意見に対する考え方及び修正	意見の種類
		ページ	章節項			
80	一般社団法人電子情報技術産業協会	14	2.3.（1）（ウ）	サプライチェーン・リスクへの対応は、各府省・調達毎に対応方法や対応レベルが異なる性格のものではないと考える。従って、各府省・各調達案権において個別判断となる部分を極小化し、政府全体で統一的な判断基準を整備して欲しい。 ［理由］ 政府各機関の共通的な事項については、統一基準群において以前より統一的な判断基準が整備されていることと思われるが、より運用を徹底して頂き、各府省間の偏りを無くすことで、応札事業者が要求されている基準を満たしているかどうかの判断がしやすくなり、様々な事業者の応札参加機会の拡大に繋がることが期待されるため。	サプライチェーン・リスクへの対応は、調達ごとに対応方法や対応レベルが必ずしも一致しないと考えますが、御指摘と同様の課題を解決するために、内閣サイバーセキュリティセンターでは、「外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書」や、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」を整備しております。	政策展開に係る意見
81	一般社団法人電子情報技術産業協会	16	2.3.（2）（エ）	「内閣官房及び各府省庁」が対象となっているが、民間企業においても同様の働きかけを行うことをご配慮いただきたい。 ［理由］ 情報セキュリティ対策は官民挙げて対応すべきと考えるが、必要となる人材像も共通する部分も多いと想定される為、教育資料の民間への提供等官民協調した取組みがあると考えるため。	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。	政策展開に係る意見
82	個人（11）		1.2.（1）	ITを利活用しているユーザー企業はもとより、中小企業における「経営層」の意識改革を促していくには、セキュリティ人材の育成における指標となり得る国家試験「情報処理技術者試験」のITパスポート試験、情報セキュリティマネジメント試験を従前よりの能力認定だけの試験制度ではなく、名称独占などの法的根拠による「権威」を持たせてはどうか。	ITパスポート試験及び情報セキュリティマネジメント試験は、ITの利活用者のIT基礎力や情報セキュリティ管理能力の向上を目指した試験であり、学生から社会人までITを利活用する全ての方向けの「能力評価試験」として活用していただくことを目的としています。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。	政策展開に係る意見

「サイバーセキュリティ 2016（案）」に係る意見募集の結果一覧

通し No.	提出者	該当箇所 ページ	該当箇所 章節項	概要	御意見に対する考え方及び修正	意見の種類
83	個人（11）		4.2.（4）	・名称独占による法的根拠を持つ「情報処理安全確保支援士」の制度に倣って、ITを利活用する側の「ITパスポート試験」、「情報セキュリティマネジメント試験」においても「情報処理業務活用推進士」、「情報処理安全活用推進士」等の名称独占を付与した「国家資格」を創設してはどうか。 ・ITを利活用している全ての企業人に対して、ITスキルや情報セキュリティ知識の証明となるITパスポート試験の合格を外部ネットワークに接続する情報処理端末機を業務で扱う上でのパスポートにしてはどうか。	前項のとおり、ITパスポート試験は、特定の業務に関する資格の付与を目的とした資格試験ではなく、ITを利活用する全ての方が必要とする能力評価試験であることを目的としています。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。	政策展開に係る意見
84	個人（11）	26	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。	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。	政策展開に係る意見
85	個人（11）		4.2.（3）	・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。	・日本国内での実施につきましては、需要の規模、コスト、受益者負担の程度等の観点から検討させていただきます。 ・アジア共通統一試験は、日本の情報処理技術者試験をベースに海外で実施しているものあり、受験者に日本人は含まれておりません。なお、アジア共通統一試験のスコア上位合格者の表彰はすでに取り組んでおります。 【ご参考】成績優秀者情報のページURL http://www.itpec.org/jp/statsandresults/high-score-passers.html ・競技会やイベント等への活用につきましては、今後の普及方策を検討する際の参考とさせていただきます。	政策展開に係る意見

「サイバーセキュリティ 2016（案）」に係る意見募集の結果一覧

通し No.	提出者	該当箇所 ページ	該当箇所 章節項	概要	御意見に対する考え方及び修正	意見の種類
86	個人（11）		4.2.（4）	・「情報処理安全確保支援士」は、情報セキュリティマネジメント試験の合格者からのキャリアパスとなるよう難易度を考慮した試験制度として設計してはどうか。 （午前1試験の免除あるいは、午前試験は2つに分けず実施されていた情報セキュリティアドミニストレータ試験の午前試験と同等レベルの出題としてはどうか。午後試験は、技術者テクニカル側人材とマネジメント人材の両方が問題を選択できるように均等に出題してはどうか。） ・情報セキュリティスペシャリスト試験と同等のレベルでは難易度が高く、中小企業へ人材が拡がらないと思う。 ・支援士3万人を確保するために旧制度（情報セキュリティアドミニストレータ、テクニカルエンジニア情報セキュリティ）の合格者を認定するのは、知識が旧過ぎるため見直してほしい。 ・情報セキュリティマネジメント試験の合格者が講習を受講することで情報処理安全確保支援士となるに必要な知識や技能を身に付けられるよう制度設計してはどうか。 ・ITパスポート試験の出題、シラバスを見直して、中分類において『セキュリティマネジメント』を設けてはどうか。 情報セキュリティにおける出題割合を更に引き上げて、出題数の内訳で30問程度の出題としてはどうか。 ・情報セキュリティマネジメント試験の普及については、初音ミクとコラボレーションして広報活動に起用してはどうか。	・「情報処理安全確保支援士」（以下、「支援士」という。）につきましては、安全な情報システムを設計、開発、運用するために必要な情報セキュリティに関する知識・技能を身に付けた人材を対象としておりますので、資格試験の難易度は、「情報セキュリティスペシャリスト試験」と同等レベルが必要であると考えており、同試験をベースとして資格試験を創設する予定です。また、支援士には定期的な講習受講を義務付け、支援士として必要な知識・技能の維持を図ることとしております。 ・支援士制度では、旧制度（情報セキュリティアドミニストレータ、テクニカルエンジニア情報セキュリティ）の合格者及び情報セキュリティスペシャリスト試験合格者を支援士となる資格を有する者とする予定でおりますが、合格から一定年数を経過している者につきましては、登録後速やかな講習を義務付けることにより、知識の最新化を図ることとしております。 ・ITパスポート試験は、ITを利活用する全ての方が必要とする能力評価試験はであり、情報セキュリティ分野の能力評価試験としては、平成28年度から「情報セキュリティマネジメント試験」を開始いたしました。 ・コラボレーションにつきまして、今後の普及活動の検討にあたって参考とさせていただきます。	政策展開に係る意見

「サイバーセキュリティ 2016（案）」に係る意見募集の結果一覧

通し No.	提出者	該当箇所		概要	御意見に対する考え方及び修正	意見の種類
		ページ	章節項			
87	NPO日本ネットワークセキュリティ協会	1	はじめに	「はじめに」を見ると、「本書は戦略に基づく2期目の年次計画であり、政府が2016年度に実施する具体的な取組を戦略の体系に沿って示したものである。」とあります。つまり、サイバーセキュリティ戦略をもとに、年度ごとの戦略を立てて、それをもとに各府省庁が翌年度向けに予算取りをするという仕組みであるべきと考えられます。 しかし、本書の内容は各府省庁が昨年度に予算取りしてある施策を列挙したもののように見受けられます。サイバーセキュリティが我が国の最重要課題の一つとなり、内閣サイバーセキュリティセンターの強化が求められている現状であれば、NISCが主体となり、サイバーセキュリティ戦略をもとに各府省庁の施策を効果的に統制し、そののち各府省庁にて予算取りを行い、施策を実施するという流れにすべきと考えます。 このパブコメに関してもよりよいアイデアを拾い出す仕組みとして活用できる機会として頂ければ幸いです。	各府省庁の予算取りについては、サイバーセキュリティ関係施策に関る予算重点化方針に基づき予算要求を行っております。2017年度の予算重点化方針につきましては、サイバーセキュリティ戦略や2015年度の評価結果、今回のパブリックコメントで寄せられた御意見を参考に、現在作成しているところです。御意見の内容につきましては、今後のパブリックコメントの活用方法を検討するに当たっての参考とさせていただきます。	その他
88	NPO日本ネットワークセキュリティ協会	3	1.1.（4）	全般的に見て、視点が、個々の機器の重要度が高いシステムのみに偏っている印象を受けます。IoTに関しては、ハードウエア開発が極めて容易になっている現状を踏まえ、ベンチャー企業等、今後IoTをビジネスチャンスととらえて参入してくる企業も念頭にした、セキュアなプラットホーム開発、提供（たとえば、汎用的なIoT用のソフトウエアフレームワークの開発など）にも力点をおくべきと考えます。IoTに関する研究開発については、こうした視点も取り入れていく必要があります。	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。	政策展開に係る意見
89	NPO日本ネットワークセキュリティ協会	3	1.2.	経営層に関する議論び視点が、大企業に偏っている印象を受けます。実際、侵害を受ける可能性があるシステムの総数から言えば、中小企業の比率が極めて高いため、現実的には「経営層の意識」があっても、人材、費用などの制約から対応が難しい場合が少なくありません。経営層に対する意識改革に加え、こうした現実問題を解消していくための支援策についても考える必要があります。たとえば、中小企業がそのITを共同運用するための組合制度の推進とこうした組合への制度的な支援といったことが考えられます。日本の物作りの中心であり、先端技術を少なからず保有する中小企業の経営層の意識を変えるためには、こうした施策を並行して進めていくことが不可欠です。	内閣官房において、セキュリティマインドを持った企業経営WGを開催し、中小企業の視点を含めた企業経営の考え方について検討しております。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。	政策展開に係る意見

「サイバーセキュリティ 2016（案）」に係る意見募集の結果一覧

通し No.	提出者	該当箇所		概要	御意見に対する考え方及び修正	意見の種類
		ページ	章節項			
90	NPO日本ネットワークセキュリティ協会	26	4.2.（4）	人材育成を考えるにあたり、この項目は非常に重要と考えます。キャリアパスのモデリングに加え、有能な人材が広く民間企業に採用されるような施策、たとえば、組織のセキュリティマネジメントにおける人材モデルなどの普及、啓発を進めていく必要があると考えます。こうした人材が、広く民間に分布することで、セキュリティ事業者とそのユーザである企業、組織とのよりスムーズな連携が期待でき、セキュリティビジネスの拡大にもつながります。	人材の需要と供給のバランスを相応させ、好循環の形成を促進することは重要だと考えております。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。	政策展開に係る意見