「サイバーセキュリティ人材育成総合強化方針（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３月９日（水）～ ３月18日（金）
- 意 見 総 数：　25者から84件 【内訳：５企業・団体から延べ28件、20個人から延べ56件】

意見内容の内訳：

○１．人材の需要と供給の好循環の形成　１件

○２．経済社会の変化に対応した経営戦略　17件

〔内訳：(1)「経営層」の意識改革　10件、　・(2)「橋渡し人材層」の育成　６件、　・第２章全体、その他　１件〕

○３．産学官が連携した人材育成の循環システムの構築　41件

内訳：・(1)求められる人材像の明示　６件、　・(2)産学官が連携した学校教育の充実　６件、
・(3)演習環境の整備　４件、　・(4)資格・評価基準等の能力の可視化　14件
・(5)突出した能力を有した人材の発掘・確保　３件、　・第３章全体、その他　８件

○全体、その他　25件

意見を踏まえた修正：　全6件

- （参考）提出者名：

産業横断サイバーセキュリティ人材育成検討会、シスコシステムズ合同会社、東京商工会議所、
一般社団法人日本クレジット協会、NPO法人日本ネットワークセキュリティ協会、個人（20）

「サイバーセキュリティ人材育成総合強化方針（案）」に対する意見募集の結果一覧

25者　84件

番号	枝番	提出者	該当箇所		概要	御意見に対する考え方及び修正
			ページ	章節項		
1	―	個人（1）	1	はじめに	現状認識をより詳しく述べてほしい。 例えば、「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人材ワーキンググループ（第１回）」の配布資料4-1「IT人材を巡る現状について」P.10の記述「情報システム産業では、1990年代以降主にユーザ企業の業務効率化案件等を受託開発するビジネスモデルを形成して来たが、2000年代後半から協力会社を中心として労働環境の悪化が相次ぎ受託開発ビジネスの限界に直面。丸投げ委託、多重下請けと人月ビジネスの横行等により、業界全体の魅力が低下した。」などを参考にすべきではないか。	本方針は、「サイバーセキュリティ戦略」を踏まえ、平成28年度以降の人材育成に係る各種施策の強化方針をまとめることを目的としたものです。御指摘のように、IT分野の労働環境の向上は重要な課題と認識しています。このため本方針においても「能力を可視化した上で、産業界やセキュリティ関連業務を行う独立行政法人を含め政府関係機関等において業務に従事する者にその能力や実績に見合った適正な処遇を実現していくことも重要」であると記載しているところです。
2	1	個人（2）	3	Ⅰ.2.(1)	「サイバーセキュリティ経営ガイドライン」の作成・普及だけでなく、NISCやIPA等でも経営者向けコンテンツを充実させてほしい。 また、首都圏だけでなく地方都市でのセミナー開催も検討願いたい。	御指摘のとおり、経営層向けコンテンツの充実は重要であると考えており、本方針においても「企業等がサイバーセキュリティ対策に取り組んでいることをステークホルダー等に情報発信する方策等について検討」することとしています。 また、地方都市でのサイバーセキュリティに係るセミナーの充実についても重要と考えております。今後の取組の参考とさせていただきます。
3	2	個人（2）	4	Ⅰ.2.(2)	「橋渡し人材層」の定義が曖昧、あるいは役割が細分化できていない。ビジョンの提示は経営者の責務であり、対策の実施は実務者の役割である。 セキュリティは、IT分野だけでも、アプリケーション、ネットワーク、データベース等の上位レイヤから下位レイヤまで多岐に渡る知識が必要であり、経営学や法律等の分野も1人でカバーするのは現実的に困難である。 一方、コミュニケーションやマネジメント能力を重視するのであれば、ITコーディネーターやITストラテジストがセキュリティの知識を多少習得すれば対処可能と思われる。 この層に本当に求められる能力やスキルが何かを今一度検討してほしい。	御指摘のとおり「橋渡し人材層」に求められる能力やスキルの整理は必要であると考えます。このため、本方針においては、まず人材育成施策において目標とする人材像をの明確化について検討を進めることとしております。また、スキルにつきましても「ITを利活用する技術者等がサイバーセキュリティに関する知識や技能を習得することをめざし、独立行政法人情報処理推進機構（IPA）が整備するITスキル標準の中に必要なスキルを取りまとめ、その普及を促進する。」としているところです。 なお、御意見も踏まえ、「橋渡し人材層」の役割の説明を「経営層の示す経営方針に基づくサイバーセキュリティ対策を実践し、実務課題を踏まえた経営戦略を提示し、さらに、組織内の関係部局間の総合調整や実務者層をまとめリードすることができる」に修文しています。
4	3	個人（2）	8	Ⅰ.3.(3)	産学官の連携は、官製政策ではなく、WGや調査会以外の団体企業からも意見聴取する等、産学の意見も十分取り入れた上で進めていただきたい。 とりわけCSSCは、毎年同じようなシナリオが使い回しされ、内容的にも実践的な演習とは呼べないようである。 もっと国民・企業に還元されるよう、民営化も含めて運営の改善をお願いしたい。	サイバーセキュリティに関する施策を推進するに際し、産業界や大学等の関係者の意見を踏まえることが重要と考えております。このため、産学官の多様な主体が参加可能な「情報セキュリティ社会推進協議会産学官人材育成WG」も活用し、情報共有を行っていくこととしています。 なお、演習環境の整備についても拡充することとしています。
5	4	個人（2）	9	Ⅰ.3.(4)	情報セキュリティスペシャリストの更新制化等を検討しているようであるが、前述のとおりセキュリティは多岐に渡る知識が必要である。本来は、他のIPA高度試験でも同様の挑戦が望まれるはずであるが、年2回しか実施しない試験を更新制とするのはナンセンスである。 また、企業活動がグローバル化している中、国内でしか通用しない資格制度は全く有用でなく、セキュリティスペシャリストだけでなく、IPAの試験全般の見直しが必要である。 情報処理安全確保支援士が免許のような資格でないならば、英語資格のTOEICやTOEFLのようにスコア制で可視化するのも良いのではないか。	御意見については、今後、情報処理安全確保支援士制度のあり方を検討する際の参考とさせていただきます。
6	5	個人（2）	10	Ⅰ.3.(5)	将来期待される人材を表彰するだけでなく、学生であれば給付型奨学金を付与すること等も検討してはどうか。 海外では国を挙げて人材を育成しているところもある中、発掘だけでは不十分である。	サイバーセキュリティに係る人材の育成・確保に際し、環境整備が重要であると考えます。そのため、本方針においても「その能力や実績に見合った適正な処遇を実現していくことも重要であり、産学官が連携して適性処遇の推進やキャリアパス等の整備を検討していく。」としているところです。
7	―	個人（3）	9	Ⅰ.3.(4)	現状案では、「情報処理安全確保支援士」は認知度の低い意味のない資格になると思われる。このため、同資格の認知向上のためマークの作成。官公庁職員への資格取得の奨励策、イメージ向上のための名称の検討、色々なスキル認証試験や知識認定試験も実施し認証されたものを登記簿に標記できるようにする等の改善策について検討すべきでないか。	御意見については、今後、情報処理安全確保支援士制度の詳細設計や普及策等を検討する際の参考とさせていただきます。

番号	枝番	提出者	該当箇所		概要	御意見に対する考え方及び修正
			ページ	章節項		
8	―	個人(4)	全体	全体	実際の分析や脆弱性診断ができるセキュリティ人材は、現在の日本でマニアックな存在として認識されてしまっている。これを改善する事も重要である。教育機関を作っても応募したいと思わせる国民の意識改革がないと、人材の裾野は広がらないと思う。 TVドラマに取り上げられることで科捜研に関する見方が各段に変わったのと同様に、もっとサイバー分野で働く人材が国民にポジティブに捉えられる環境作り、世論作りも欠かせないのではないか。橋渡し人材層にせよ、セキュリテイそのもに携わる人材にせよ。まだまだ日の目を見ない仕事という印象が国民の間にはあると思われる。 自分の出向先勤務地のロシアは、サイバーセキュリティの先進国で、セキュリティ人材のベースとなるソフトウェア人材育成が非常に進んでおり、既に欧州へソフトウェア人材の輸出国となっている。逆に自動車等のモノづくりが日本よりも苦手なので人材をサイバー用に集めやすいのかも知れない。人口も日本と変わらないこの国の人材育成の事例は日本の方針を決めていくのに参考になるのではないか。	サイバーセキュリティに関する関心・理解度・対応力について広く国民に浸透させるため平成21年度から「情報セキュリティ月間」(現「サイバーセキュリティ月間」)を設け、国民に親しみやすいメディアを活用する等普及啓発活動に取り組むなどしているところです。また、サイバーセキュリティは我が国のみならず世界各国で共通の課題と考えておりますので、海外での取組等も参考にしつつ取組を進めていくこととしています。
9	―	個人(5)	9	Ⅰ.3.(4)	新しい資格区分「情報処理安全確保支援士」を創設するに際し、名称独占だけでなく業務独占資格としての機能を盛り込んでほしい。 人材確保を目的とするのであれば、アメとムチに倣い、ある程度のインセンティブを資格保持者に与えるのが効果的ではないかと。 現実的な提案としては、一定の規模以上またはn人以上の個人情報を取り扱う企業に必置とするような形態が望ましい。	御意見については、今後、情報処理安全確保支援士制度のあり方を検討する際の参考とさせていただきます。
10	―	個人(6)	9	Ⅰ.3.(4)	情報処理安全確保支援士制度の設立は基本的に賛成。ただし、現状の制度設計では魅力が全くない。 (1)守秘義務(罰則付き)や更新義務が課せられるにも関わらず、登録者の権利的なものが一切ない(名称独占は取得者にとって権利にもメリットにもならない)。 (2)名称がわかりにくく、センスがない。 取得者に魅力のある制度とすることが、全体のレベルの向上につながると思う。例えば企業のセキュリティ監査権の独占化や監査証明書発行の独占化等の検討をするべき。 現状のままでは、情報処理技術者試験と同様に意味のない制度になってしまう。	御意見については、今後、情報処理安全確保支援士制度のあり方を検討する際の参考とさせていただきます。 また、(2)の名称に関する御意見については、今後、情報処理安全確保支援士制度の普及策等を検討する際の参考とさせていただきます。
11	1	個人(7)	全体	全体	人材育成におけるキャリアパスにおいて、学校や大学教育からのステップの観点が不足していると感る。 昨今は、小学生でさえスマホを持つ時代であり、すでにサイバーセキュリティを意識していかなければならない環境である。 また大学生は卒業後、社会人として活躍していくが、セキュリティ関連の教育が十分ではない企業もある。また、学生生活の中でも、研究内容や論文など保護すべき情報が多々あるため、一定レベルのセキュリティ教育が必要であると思う。	御指摘のとおり、サイバーセキュリティに関する素養はすべての人にとって必要なものとなりつつあります。本方針においても「理論・基礎の習得について大学等の段階から行われることが期待される」と記載しているところです。 また、初等中等教育段階における教育の充実については、「サイバーセキュリティ戦略」の記載に基づき、引き続き取り組んでいきます。また、サイバーセキュリティに関する関心・理解度・対応力について広く国民に浸透させるため平成21年度から「情報セキュリティ月間」(現「サイバーセキュリティ月間」)を設け国民に親しみやすいメディアを活用する等普及啓発活動に取り組むなどしているところです。
12	2	個人(7)	3	Ⅰ.2.(1)	サイバーセキュリティ経営ガイドラインは非常に有効であり、普及させ、達成度を確認する仕組みが必要であると思う。 PDCAや考え方など、ISMSの概念に重なる部分が非常に多く、企業にとってはISMSよりは馴染みやすいと思う。例えば、J-SOXと同じように監査項目としてもよいと考えている。	「サイバーセキュリティ経営ガイドライン」の普及も含め、サイバーセキュリティに関する取組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ための方策について取り組むこととしています。今後の取組の参考とさせていただきます。
13	―	個人(8)	全体	全体	企業のセキュリティに対する意識やCISSP等有資格者人材への注目度は上がってきたものの、行政施策等に対する企業姿勢は形式的なものが多い。 セキュリティ有資格の育成体系や人材の増加数等の調査等がされておらず、行政・企業や行政で、現在のスキルや資格保有者を把握できていない。 行政・企業から有資格者に声がからないケースがあり、現状あまり登用・活用されていない。個人で資格やスキルの維持に取り組まざるを得ず、負担が大きい。 スキルの高い実務者がいても、管理者の理解が得られず対策ができないケースが多い。 高資格者への育成支援・助成(行政主導の資格奨励)、資格者の待遇面優遇等が必要と考える。	本方針においては、サイバーセキュリティに関する取組が、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ための方策について取り組む等によって、「経営層」の意識改革を促し、人材の需要を喚起するとともに、産学官が連携した人材の育成の循環システムを構築することとしております。 また、「能力を可視化した上で、産業界やセキュリティ関連業務を行う独立行政法人を含め政府関係機関等において業務に従事する者にその能力や実績に見合った適正な処遇を実現していくことも重要であり、産学官が連携して適性処遇の推進やキャリアパス等の整備を検討していく。」と修文し、能力や実績に見合った適切な処遇を実現する旨記載することとします。
14	1	団体(1)	3	Ⅰ.2.(1)	「企業等がサイバーセキュリティ対策に取り組んでいることをステークホルダー等に情報発信する方策等について検討」に基本的には賛同するが、一過性のものではなく、2020年以降も見据えた中長期の取組みが必要である。	御指摘のとおり、人材育成は短期的に結果がでるものではなく、また、あらゆるモノがインターネットにつながり、サイバー空間への脅威が深刻化する中で、経済社会の変化に対応して社会で活躍できる人材育成に係る取組を推進していきます。

番号	枝番	提出者	該当箇所		概要	御意見に対する考え方及び修正
			ページ	章節項		
15	2	団体(1)	6	Ⅰ.3.(1)	「経営等他分野の知識を併せ持つ『ハイブリッド型人材』」について、確かに橋渡し人材として経営などの知識は必要であるが、それ以前に、サイバーセキュリティに係る人材は、企業の機密情報や個人情報、さらには重要インフラに接する機会が多いため、技術面の知識のみならず、守秘義務の順守など、高い倫理規範や行動規範が求められる。人材育成にあたって加えるべき留意点である。	サイバーセキュリティに係る人材には、技術面の知識のみならず高い倫理観も同時に求められることは御指摘のとおりです。 「3. 産官学が連携した人材育成の循環システムの構築」の部分に「サイバーセキュリティ人材においては、技術的な能力のみならず、高い倫理観も同時に身に付ける必要がある。」旨を追加します。
16	3	団体(1)	6	Ⅰ.3.(2)	「理論・基礎の習得について大学等の段階から行われることが期待される」とある。高度な専門的知識の習得については大学等の段階からであることは当然であるが、インターネットの仕組みや利用にあたってのルールやマナー、脅威の種類や対処方法についての基礎的な知識は、小・中学校からの早期教育が必要である。	御指摘のとおり、サイバーセキュリティに関する素養はすべての人にとって必要なものとなりつつあります。本方針においても「理論・基礎の習得について大学等の段階から行われることが期待される」と記載しているところです。 また、初等中等教育段階における教育の充実については、「サイバーセキュリティ戦略」の記載に基づき、引き続き取り組んでいきます。また、サイバーセキュリティに関する関心・理解度・対応力について広く国民に浸透させるため平成21年度から「情報セキュリティ月間」(現「サイバーセキュリティ月間」)を設け国民に親しみやすいメディアを活用する等普及啓発活動に取り組むなどしているところです。
17	4	団体(1)	9	Ⅰ.3.(4)	「情報処理安全確保支援士」、「情報セキュリティマネジメント試験」について、人材育成の一つの目標として新たな資格・評価基準ができることは大いに意味のあることであり、歓迎する。 ただし、情報処理安全確保支援士は、業務独占がなく、士業として独立できるメリットが少ない。「能力に見合った適正な処遇を実現していくことも重要」との記載もあるが、有資格者本人のキャリアパスとしても有益で、かつ中小・小規模事業者にとっても有益な人材として活躍できるような制度設計が望まれる。	御意見については、今後、情報処理安全確保支援士制度のあり方を検討する際の参考とさせていただきます。
18	1	団体(2)	全体	全体	「リカレント教育」は、言葉の定義が様々なようであるので、ここでは分かりやすく「社会人教育」としてよいのではないか。	「サイバーセキュリティ戦略」(平成27年9月閣議決定)において「リカレント教育」という言葉を用いていることから、本戦略でも表記を合わせています。なお御指摘も踏まえ「リカレント教育」について注釈を追加しています。
19	2	団体(2)	全体	全体	「橋渡し人材層」の必要性を取り上げる背景説明が必要ではないか。一般的に、日本企業の経営幹部はサイバーセキュリティに関する知識や経験を持たないまま就任し、それらを短い任期で習熟することを期待しにくいという、日本独特の背景をどこかで簡単に補足するとよいと考える。	「橋渡し人材層」の必要性については、まず「「経営層」の意識改革」において「社会の変化をより多くの企業経営層が的確に捉え、危機意識を持ってリスクマネジメントに当たることが必要である。」と経営層がサイバーセキュリティに係る取組を経営戦略の一環として積極的に取り組むよう意識改革を促すこととした上で「経営層が直接、サイバーセキュリティの専門的な知見を有する実務者層一人一人とコミュニケーションをとっていくことは難しい。このため、経営層の示す経営方針に基づくサイバーセキュリティ対策を実践し、実務課題を踏まえた経営戦略を提示し、さらに、組織内の関係部局間の総合調整や実務者層をまとめリードすることができる橋渡し人材層が必要であり、その育成を推進する。」としているところです。
20	3	団体(2)	5	Ⅰ.3.	「産学官が連携した人材育成の循環システムの構築」について、特に今すぐ必要な人材は、サイバーセキュリティ人材の必要性を身をもって実感し、人材育成エコシステムの中で常に牽引、先導するような発言力・影響力のある人であり、実際にそのような人が中心となって施策を推進すべき。	人材育成の循環システムを形成するためには、それぞれの取組・施策をつなげる取組が必要であり、御指摘のシステムを牽引・先導するような人材も含め産学官の多様な主体が参加可能な「情報セキュリティ社会推進協議会産学官人材育成WG」で検討を進めてまいります。
21	4	団体(2)	5	Ⅰ.3.(1)	「求められる人材像の明示」について、人材育成の実効性を考えると、教える側の人材(教員等)の確保・育成・維持が極めて重要で急務な課題であり、方針に追記すべき。 具体的な課題として、(1)若年層へのリテラシー教育からトップガン人材の育成まで様々な観点で一貫した方針に則って教える人材、(2)教える側の人材が活躍できる場・キャリアパス・社会的システム、(3)教える側の人材を育てる効果的な方法(例えば、イスラエルやエストニアのようなサイバー先進国で十分な実地経験を積み日本に合った指導者教育プログラムの構築に反映するような施策を検討) などの必要性が挙げられる。	御指摘のとおり、教える側の人材(教員等)の確保等は重要であると考えています。「サイバーセキュリティ戦略」(平成27年9月閣議決定)においても「教員の情報通信技術を活用した指導力向上を目指した研修等の改善・充実を進める。」と記載しています。この取組の中で、産業界側の御協力による教える側の人材確保の動きもあることから、本方針においても「企業からの寄附講座の開設や講師派遣等が進みつつあるが、さらに、産業界と連携した教育プログラムの開発等を行い、地域における教育機関なども含め、共有化することが重要となる。」と記載しているところです。
22	5	団体(2)	5	Ⅰ.3.(1)	「橋渡し人材層」は、新たな職種の人材として経営者層と実務者層の間に採用・配置するだけではなく、経営者への橋渡し機能を担うことができるように既存の実務者層(主に管理職)を育成するケースもあり得ると考える。	本方針において、「橋渡し人材層」は、新たな職種の人材として採用・配置するだけでなく、「実際に実務者として組織内の業務経験を積む必要があり、実務者層をまとめ指揮できるリーダー的な役割を担うことが期待される」として、実務経験者がなることも想定しています。
23	6	団体(2)	6	Ⅰ.3.(1)	人材を育成するにあたり推進する4つの施策として、「産学官が連携した教育の充実、演習環境の整備、資格・評価基準等の能力の可視化、突出した人材の発掘・確保の各種施策」とあるが、この他に、セキュリティに関する脅威やリスク、対策等に関する情報を収集・共有する活動に積極的に参加することも人材育成は重要である。このような活動は社外の組織やコミュニティで行われていることが多く、経営層が積極的に促すことが必要である。	御指摘のとおり「セキュリティに関する脅威やリスク、対策等に関する情報を収集・共有する活動に積極的に参加する」は重要であることから、Ⅰ 2.(1)に「危機意識を持ってリスクマネジメントにあたることが必要である。」との一文を追加します。

番号	枝番	提出者	該当箇所		概要	御意見に対する考え方及び修正
			ページ	章節項		
24	7	団体(2)	6	Ⅰ.3.(2)	産学または産学官連携による人材育成活動や民間の人材育成事業（研修等）のうち、国が指定するものへの参加者（受講者）に対して支援金を支給し、教育を受ける側の負担を軽減できる仕組みがあるとよい。	今後、必要となるサイバーセキュリティに係る人材の確保が可能となるように、人材の裾野を拡大し、その能力の底上げを図ることが重要と考えます。このため各取組に対し、積極的に関与・参加を促すことを含め推進してまいります。
25	8	団体(2)	7	Ⅰ.3.(3)	「演習環境の整備」は、NICTのCYDER、CSSCのテストベッド等の特定の環境の整備ではなく、重要インフラ事業者や個別企業、大学等がそれぞれの環境で柔軟に演習・訓練ができる環境の整備、仕組みづくりの方が重要と思う。	本方針では具体的な施策の事例としてNICT等を取り上げているところですが、企業、大学等がそれぞれの環境で柔軟に演習・訓練ができる環境の整備、仕組みづくりに産学官が連携して取組むことも重要であり、関係者が情報共有しつつ推進していきます。
26	9	団体(2)	7	Ⅰ.3.(3)	3.(3)冒頭の四角枠内に記載された2種類の演習については、例えば「高な技術的演習」、「組織的総合演習」とそれぞれタイトルをつけるとよいと思う。 また、本文中「組織横断的な調整能力や発生した事態に対するマネジメント能力等」とあるが、もう少し具体的に、例えば「大規模なサイバー攻撃を受けたと想定した緊急ケース等における組織横断の調整やマネジメントから成る実践的な総合演習（交通や電力等、業界共通のシナリオを適用することも有効）」と記述するとよいのではないか。	御提案ありがとうございます。本方針では、具体的な事業の内容と整合性を図る必要があり、原文の記述のままとします。また、具体的な実施内容については参考とさせていただきます。
27	10	団体(2)	9	Ⅰ.3.(4)	今春「情報処理安全確保支援士」と「情報セキュリティマネジメント試験」の2種類の資格・評価基準が新設されたが、情報セキュリティ関連業務は多岐にわたるため、これだけでは実務をカバーするには十分とは言えないと思う。「情報処理安全確保支援士」の試験だけでは、セキュリティサービスや技術を提供する立場に求められる実践的な技術力や業務能力を適切に測ることができない懸念があると思われる。	御意見については、今後、情報処理安全確保支援士制度のあり方を検討する際の参考とさせていただきます。
28	11	団体(2)	5	Ⅰ.3.	「グローバルかつ高度なサイバー攻撃等に対応し、サイバーセキュリティに係る突出した能力を有した人材の発掘・確保にも努める。」とあるが、「発掘」といういい方に違和感がある。突出した人材は一朝一夕に出来上がるものではないため、基礎からある程度のレベルの教育を行った上で、あるレベルからは、本人が「自走」できる仕組み作りをする必要がある。 また、「自走」を支援するものとして仲間がいた方がよいので、「自走できる人たちのコミュニティづくりを産学官で推進する」ということも掲げてはどうか。さらに、このコミュニティは国境を越えた広がりであることがよい。	「発掘」の表現は「サイバーセキュリティ戦略」においても同じ表現を使用しておりますので、そのままとしています。また、御指摘のとおり、能力を持った人材同士が切磋琢磨できる環境整備が必要であり、本方針においても「突出した能力を持つ人材が海外のハイレベルなコンテストや演習に参加することを促すことや、我が国に海外の有能な人材が魅力を感じられるような場（国際的なコンテストや実践的な演習環境）を整備していくとともに、民間団体における同種の取組を積極的に支援していく。」と記載しているところです。
29	12	団体(2)	全体	全体	人材育成のエコシステムに連動したプロフェッショナル・キャリアパスを具体的に準備することは、現時点難しいかもしれない。その場合、P.11「図2：社会で活躍する人材の育成」は、あくまでも人材育成におけるイメージであり、また一例であるということを強調してほしい。 そして、新たな章として「3.(6) 情報セキュリティ／サイバーセキュリティ・プロフェッショナルのキャリアパス／キャリアモデル」といったものを追加し、今回の方針を発行した後も、引き続き当領域におけるイメージやケースの具体化を行ない、それらの実現に向けた検討を並行して推進する強い意思表示をといった本文中に盛り込んでほしい。近い将来に向けたキャリアパス思考の要諦・エッセンスになるのではないか。	御指摘のとおり、本方針で示した人材育成の循環システムは一つの例に過ぎないため、「図2：社会で活躍できる人材の育成（イメージ）」と修正します。また、人材育成は短期的に結果がでるものではなく、また、あらゆるモノがインターネットにつながり、サイバー空間への脅威が深刻化する中で、経済社会の変化に対応して社会で活躍できる人材育成に係る取組を推進していきます。
30	1	個人（9）	全体	全体	方針案が策定されたことについては素直に評価している。昨今報道されるように人材の量（人数の目標）だけが先行することで、質が確保できずにサイバーセキュリティ担当という名の素人が粗製濫造されるような事態を危惧している。 方針から具体的な人材育成計画に落とし込み、真に日本に役立つ人材が育成されることを期待する。 また、方針の策定にあたり、韓国などすでに育成計画が日本より進んでいる国の事例に倣うことが可能か、ご検討いただきたい。	賛同意見として承ります。今後の取組の参考とさせていただきます。
31	2	個人（9）	全体	全体	スケジュールについて、全体的に方針と実態が見合っていない印象を受ける。仮に4年後の平成32年の東京オリンピックを一つのターゲットとするのであれば、前年度である平成31年度までに一定の育成成果を出すことを考えると、そこまでのロードマップが方針から読み取れず、また直近の人材像の策定に約1年かけるというスケジュール感から考えても、間に合うようには思えない。 現実的かつ具体的なロードマップを打ち出してほしい。	本方針は、「サイバーセキュリティ戦略」を踏まえ、人材育成に係る各種施策で強化するとともに、各施策の円滑な連携を促進するために取りまとめたものであり、各種施策については、本方針に基づきそれぞれ順次進めていきます。

番号	枝番	提出者	該当箇所		概要	御意見に対する考え方及び修正
			ページ	章節項		
32	3	個人（9）	8	Ⅰ．3．(4)	特に実務者を対象とした、より実践的な資格が整備されることを期待する。 現在、国内の代表的な関連資格はIPAと考えているが、座学に比重が置かれており、実務上のスキルには直結しないのが現状である。自分も取得しているが、一定の効果はあると考えるものの、やはり「サイバーセキュリティに携わる者の常識として知っておく内容」の域を出ていないという印象を持っている。ここは海外よりも大きく遅れており、SANSやOffensive Security等、同分野の資格を参考に、より効果の高い資格の整備を期待する。	御意見については、今後、情報処理安全確保支援士制度のあり方を検討する際の参考とさせていただきます。
33	4	個人（9）	12	Ⅱ．	安全なサイバー空間の実現のために、雇用やキャリアパスの整備が必要という主張に賛同する。サイバーセキュリティの人材に関して具体的なキャリアパスが見えないことが、人材の量・質ともに充実しない遠因であると考えている。民間企業が大きく関わる点ではあるが、育成と同時に雇用やキャリアスタートができるよう制度を策定してほしい。	賛同意見として承ります。今後の取組の参考とさせていただきます。
34	―	個人（10）	4	Ⅰ．2．(2)	橋渡し人材の育成については、（中心となる数人を除き）本職との草鞋を履く形で集め、集めた講演者が集まって能動的にスライドを調整する形を取りながら、地方ごとの特色に合わせた形で微調整した上で、内容にお墨付きを与え、現在の経営者のマインドを汲み取り、負担を与えないタイミングで、システムをデザインしてはどうか。	本方針における「橋渡し人材層」は、経営層の示す経営方針に基づくサイバーセキュリティ対策を実践し、実務課題を踏まえた経営戦略を提示し、さらに、組織内の関係部局間の総合調整や実務者層をまとめリードすることができる人材としており、産学官連携してその育成を推進していきます。
35	1	個人（11）	3	Ⅰ．2．(1)	サイバーセキュリティを投資とするのであれば、それに伴う収益なり、メリットを明確にすべきである。	投資の考え方については、「サイバーセキュリティ戦略」において「高いレベルのセキュリティ品質が確保された製品・サービスを市場に投入し、新たなビジネスを創出する経営判断に当たり、サイバーセキュリティに関する素養が企業経営層の必須能力となりつつある。こうした社会の変化をより多くの企業経営層が的確に認識し、セキュリティ対策はやむを得ない「費用」ではなく、より積極的な経営への「投資」であるとの認識を醸成していくことは、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。」と示しており、本方針も同戦略を踏まえたものとなっています。
36	2	個人（11）	全体	全体	「サイバーセキュリティ経営ガイドライン」P.2に「大企業及び中小企業（小規模事業者を除く）のうち、IT に関するシステムやサービス等を供給する企業及び経営戦略上 IT の利活用が不可欠である企業を想定している。」、「ただし、企業の規模やビジネスモデルによっては、本ガイドラインの適用が必ずしもセキュリティ対策として適切ではないケースもありうる。」とあり、全ての組織・企業を想定した本方針の書き方には違和感がある。	「経営ガイドライン」につきましては、普及に取り組みつつ、利用者の御意見も踏まえ適宜見直しを進めていきます。 また、中小事業体への啓発と事業の推進については重要と考えており、御指摘も踏まえ取り組んでいきます。
37	3	個人（11）	全体	全体	サイバーセキュリティは他の情報基礎分野の延長の上に成り立つ。短期的な知識習得も現時点では必要かもしれないが、サイバーを広く捉え、偏りのない、長期的な人材育成策を盛り込んでほしい。	御指摘のとおり、人材育成は短期的に結果がでるものではなく長期的なものであり、また、あらゆるモノがインターネットにつながり、サイバー空間への脅威が深刻化する中で、経済社会の変化に対応して社会で活躍できる人材育成に係る取組を推進していきます。
38	4	個人（11）	8	Ⅰ．3．(4)	「サイバーセキュリティに従事する者の能力の可視化に資する資格・評価基準の整備」について、すでに国際的な資格や高度な知識体系が複数確立されており、それらの活用や支援を優先すべきである。	御指摘の懸念もあり、現在ある各種資格等の活用も含め、サイバーセキュリティに従事する者の能力の可視化に資する資格・評価基準の整備に取り組んでいるところです。
39	5	個人（11）	全体	全体	サイバーセキュリティは、攻撃の脅威の上に需要が成り立つものであり、本施策が適切に機能することにより、需要が低下することも視野に入れる必要があるのではないか。	経済社会の変化に対応するため、産学官が連携して人材育成の循環システムを構築する必要があり今後取組を推進していく上での参考とします。
40	6	個人（11）	全体	全体	効率化の視点が抜けていないか。今の人材消費・職人型のサイバーセキュリティ対策には限界がある。少ない人材を効率的に活用するための分析ツールや解析手法などの作成支援を盛り込むべきではないか。	本方針に基づく各施策の進捗確認及び評価を行いつつ推進することとしています。、なお、御指摘の点については、人材育成の循環システムを今後取組を推進していく上での参考とします。
41	―	個人（12）	全体	全体	マルウェアやサイバー攻撃を完全に防ぐことができたとしても、個人情報や営業機密はセキュリティソフト会社やOS、SNSの海外サーバーに知られることなく蓄積されている。クラウド型のセキュリティソフトや、OS、SNSのサーバーが海外にある場合は、日本の法規が及ばず、不当に営業機密等を収集される可能性がある。このようなサービス利用に対しても監査できる人材を育成してほしい。	本方針では明示的に示していませんが、サイバーセキュリティの監査人材も必要であると考えており、現行の「新・情報セキュリティ人材育成プログラム」において「情報セキュリティ監査等を行う人材の育成、資格制度の適切な活用等も必要となる。こうした人材の育成は企業等の経営層の意識啓発のみならず、我が国の情報セキュリティ水準の向上にも資すると考えられることから、監査等を実施する者の常日頃からのスキルアップ（最新の情報の提供など）、行動規範の確立、監査制度の整備充実について引き続き取り組む。」と記載しています。

番号	枝番	提出者	該当箇所		概要	御意見に対する考え方及び修正
			ページ	章節項		
42	―	個人（13）	全体	全体	一部の突出した人材の育成も大事とは思うが、セキュリティ人材のすそ野を広げるためには、セキュリティのジェネラリストの育成も必要。 若きセキュリティ人材の目指すキャリアパスが、必ずしも世界に通用するトップクラスの人材とは限らず、複数のキャリアパスの可能性が広がることも若年層を引き込むキーとなるのではないか。天才にしかたどり着けないスペシャリストだけではなく、今現在日本のセキュリティを支えている無名のエンジニア達がクローズアップされ身近な存在であることがわかるような取り組みを期待する。 米国と異なり、日本では、新卒者は配属されるまでは何を担当できるかわからないの企業・行政組織が多いのではないか。人材を登用する側の改革といった協力も必要不可欠である。 また、米国で一部取組が始まっているように、セキュリティ人材を会社の根幹を守る重要な人材として投資し、評価するといった制度を導入した企業へのインセンティブを設けることはできないか。	本方針においては、技術面で優れたサイバーセキュリティの人材だけでなく、経営層と実務者とをつなぐ「橋渡し人材層」の育成も重要と考えております。このため「経営層の示す経営方針に基づくサイバーセキュリティ対策を実践し、実務課題を踏まえた経営戦略を提示し、さらに、組織内の関係部局間の総合調整や実務者層をまとめリードすることができる橋渡し人材層が必要であり、その育成を推進する。」と記載しています。 また、「「経営層」の意識改革」において「社会の変化をより多くの企業経営層が的確に捉え、危機意識を持ってリスクマネジメントに当たることが必要である。」と記載しており、経営層がサイバーセキュリティに係る取組を経営戦略の一環として積極的に取り組むよう意識改革を促していきます。
43	1	個人（14）	全体	全体	対象とすべき「サイバーセキュリティ人材」についての具体的な定義が記載されていない。これはP.1の「サイバーセキュリティを専門とする人材のみならず、ユーザー企業等も含めた幅広い立場でのサイバーセキュリティに係る人材」を対象とする方針案であると理解してよいか。	本方針は、社会で活躍できる人材の育成に向け、サイバーセキュリティを専門とする人材のみならず、ユーザー企業等も含めた幅広い立場でのサイバーセキュリティに係る人材育成に向けた各種施策を加速させていくための方針を示したものです。
44	2	個人（14）	2	Ⅰ．1.	「連接融合情報社会」なる用語は「サイバーセキュリティ戦略」以降にNISCにおいて発せられる文書等でよく拝見しているが、一般的に用いられる用語として定着しているとは考えられない。もう少し一般の主婦が一見して理解できるような平易な用語に改めていただけると、サイバーセキュリティ戦略の普及啓発につながるのではないか。	本方針は「サイバーセキュリティ戦略」の方針の下、人材育成に向けた各種施策を加速させていくための方針ですので同じ用語を使用しています。 また、普及啓発については、サイバーセキュリティに関する関心・理解度・対応力について広く国民に浸透させるため平成21年度から「情報セキュリティ月間」（現「サイバーセキュリティ月間」）を設け国民に親しみやすいメディアを活用する等普及啓発活動に取り組むなどしているところです。
45	3	個人（14）	3	Ⅰ．2.（1）	情報セキュリティ対策は積極的な経営への投資という表現が用いられている。経営層に、情報セキュリティ対策に対するポジティブな印象を与えるためにこのような表現を用いたと思われるが、対策に係るのはあくまで費用であり、情報セキュリティ対策を実施するから利益が大幅に向上するというものではない。また「投資」であるならば、一定のところで利益を回収しなければならないという反動が発生することも十分考えられ、本来NISCが求める戦略とは異なると考えられる。「投資」という用語を用いると、一般の経営者（それもよく分かっていない経営者）に誤読される恐れがあるのではないかと懸念し、もう少し慎重な用語の用い方をお願いしたい。	「サイバーセキュリティ戦略」において「高いレベルのセキュリティ品質が確保された製品・サービスを市場に投入し、新たなビジネスを創出する経営判断に当たり、サイバーセキュリティに関する素養が企業経営層の必須能力となりつつある。こうした社会の変化をより多くの企業経営層が的確に認識し、セキュリティ対策はやむを得ない「費用」ではなく、より積極的な経営への「投資」であるとの認識を醸成していくことは、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。」と示しており、本方針も同戦略を踏まえたものとなっています。
46	4	個人（14）	3	Ⅰ．2.（1）	「サイバーセキュリティ経営ガイドライン」について、内容としてガイドラインの中身が非常に理解しづらく、また中小企業には負担が重い内容となっており、地方の中小規模かつ情報セキュリティを専業としていない事業体の情報セキュリティ担当者からは非常に守りづらいものであるという意見がある。また、当該ガイドラインを遵守しておれば安全であるというわけにはいかないのがサイバーセキュリティに係る事案である。したがって、当該ガイドラインをただ普及させていくのではなく、何が最も重要なのか、ITリスクをどう考えていくのかという点になるべく心を砕いていただき、経済産業省とうまく連携して攻撃から守られていない中小事業体への啓発と事業の推進を行っていただきたい。	「経営ガイドライン」につきましては、普及に取り組みつつ、利用者の御意見も踏まえ適宜見直しを進めていきます。 また、中小事業体への啓発と事業の推進については重要と考えており、御指摘も踏まえ取り組んでいきます。
47	5	個人（14）	3	Ⅰ．2.（1）	「企業等がサイバーセキュリティ対策に取り組んでいることをステークホルダー等に情報発信する方策等」は、有価証券報告書等の文書に含めるような報告書等を作成させる予定があるということか。現在検討している具体的な方法を教えてほしい。また、そもそもこのような行為について、企業側がなぜそれを実施していかねばならないのか（実施していく負担を当該企業が負わなければならないのか）について、根拠となる法令等や参考にされている諸外国の制度等があれば教授願う。	「企業等がサイバーセキュリティ対策に取り組んでいることをステークホルダー等に情報発信する方策等」につきましては現在検討中であり、御意見も踏まえ取り組んでいきます。
48	6	個人（14）	4	Ⅰ．2.（2）	「橋渡し人材層」について、「経営層の示す経営方針に基づくサイバーセキュリティ対策を実践すること、実務課題を踏まえた経営戦略を提示すること、さらに、実務者層をまとめ、リードすることができることが必要である。」という記載があり、加えて「「機能保証（任務保証）」の考え方に基づく取組が求められる」というような形で橋渡し人材層に求められる要件が定義されている。ここに記載されている橋渡し人材層は、前後の文脈から見て”サイバーセキュリティ対策の実務対応者（主に技術者集団）のトップ”を想定し、その者に経営層と話すことのできるだけのマネジメント能力を求めていると理解しているが、その理解で間違いないか。	御意見のような人材も含め「経営層の示す経営方針に基づくサイバーセキュリティ対策を実践し、実務課題を踏まえた経営戦略を提示し、さらに、組織内の関係部局間の総合調整や実務者層をまとめリードすることができる」人材と定義しています。

番号	枝番	提出者	該当箇所		概要	御意見に対する考え方及び修正
			ページ	章節項		
49	7	個人（14）	4	Ⅰ.2.(2)	サイバーセキュリティ専業企業等の一部の企業と監査部門を除く大多数の企業では、ITのサービスや運用を担う実務担当者の大多数は、マネジメント能力を保有していたとしても情報セキュリティに関する事象を経営層に橋渡しすることのできるキャリアパスが形成されていないため、実施することが非常に難しい。平時の状況が現場担当者に任せきりでインシデント発生時に現場責任者のみが対応を迫られるなど、組織の権限と責任が十分に執行されていない状況が多々見受けられる。橋渡し人材層の理想は理解できるが、実現には実務担当者の働きが経営層に十分認識され、必要な権限が的確な統制の下で与えられ、キャリアパスがあってはじめて可能と考えている。P4に「コミュニケーションをとりやすくするためのツール」や「マネジメント能力を高めるための演習」という表現もあるが、これらの手段の前に前提として適切な対応を促すべきではないか。この点をきちんと議論していただきたい。	「企業等がサイバーセキュリティ対策に取り組んでいることをステークホルダー等に情報発信する方策等」につきましては現在検討中であり、御意見も踏まえ取り組んでいきます。
50	8	個人（14）	5	Ⅰ.3.	「リカレント教育」について、実現の「原資」をどのように考えているか。個々人の負担であればさほど人数は増えないと思われ、企業負担であれば企業によってばらつきがあり、最もサイバーセキュリティ対策が弱いといえる中小事業体等では人材育成が進まないという状況に陥る。	今後、必要となるサイバーセキュリティに係る人材の確保が可能となるように、人材の裾野を拡大し、その能力の底上げを図ることが重要と考えます。このため各取組に対し、積極的に関与・参加を促すことを含め推進してまいります。
51	9	個人（14）	5	Ⅰ.3.	現状で実施されている社会人リカレント教育の大多数は首都圏(東京都や横浜市等)を含めた地点が中心で、地方都市では講座受講の選択肢が非常に限定されている。人材育成の橋渡し人材層を増やしていくために、これらについてはどのような具体的な対策を検討されているか。	サイバーセキュリティに係る教育の機会が首都圏に集中しているとした指摘があると認識しております。そのため、本方針においては「産業界と連携した教育プログラムの開発等を行い、地域における教育機関なども含め、共有化することが重要となる。」としているところです。
52	10	個人（14）	5	Ⅰ.3.(1)	「『求められる人材像』を明確にすることが必要である」との表現があり、「平成28年度中にまとめる」とあるが、そもそも当方針案の策定の際に先に検討しておくべきではないか。人材像が明確ではないのに育成方針を定めるというのは順序が逆と考える。	人材像については、P.5 Ⅰ.3.(1)に記載のように「新・情報セキュリティ人材育成プログラム」での定義を基にしています。なお、今後も改善が必要なため「『求められる人材像』を明確にすることが必要である」としています。御指摘を踏まえ今後取り組んでいきます。
53	11	個人（14）	6	Ⅰ.3.(2)	職業人を育てるために学部・大学院（enPiT）・専門学校・高等専門学校等の取組が記載されているが、教育現場においてこれらの教育を担う者が圧倒的に不足しているのが現状。寄付講座や社会人実務者による講座などの記載事項もあるが、それでは方針案の人材育成は不可能であると思われる。教育を担う者をどう増やしていくのか、その対策についてこの方針案に盛り込んでいただきたい。	産学官が連携した教育については大学等の取組の効果等について検証しつつ必要に応じて改善・推進を図ることとしています。御意見も踏まえ取り組んでいきます。
54	12	個人（14）	8	Ⅰ.3.(3)	国立情報学研究所が演習環境を整備するという表現があるが、私立大学等は含まれないのか。	国立大学法人及び大学共同利用機関法人が、国立情報学研究所と連携して、所属機関の技術職員を対象に実施する研修事業の内容について記載しておりますので、私立大学は含まれておりません。
55	13	個人（14）	9	Ⅰ.3.(4)	「情報処理安全確保支援士」は、まず名称が適切でない。士である以上、士業として成立させるという認識をNISC及び経済産業省は持っているのか。いろいろな資料を見ても、どのような職務を担わせるのか明確でなく、士業として成立しうるものではない。これを創設させるならば、まずこれらの職務職能と士業としてのキャリアが形成可能かをきちんと検討してほしい。登録簿についても、実際の運用時に誰も登録していなかったり活用が進まなかったりということもあり得る。現在、経済産業省が整備しているシステム監査台帳制度や情報セキュリティ監査台帳制度などの活用状況を精査しているか。また、これらの既存の台帳制度との住み分けどのように設定するのか。様々な制度を新規で作ることは、いたずらに民間企業（特に規模の小さい事業体）の負荷を増大させるだけで、本質的な目的（情報セキュリティ対策の質的向上）に寄与しない。	御意見については、今後、情報処理安全確保支援士制度等のあり方を検討する際の参考とさせていただきます。 また、職務の明確化に関する御意見については、今後、情報処理安全確保支援士制度の普及策等を検討する際の参考とさせていただきます。
56	14	個人（14）	9	Ⅰ.3.(4)	IPAがITスキル標準の中に必要なスキルを取りまとめるとあるが、「情報セキュリティマネジメント試験」実施の前に行うべきではないか。	ITエンジニアを対象とし、既に整備されているITスキル標準のさらなる充実を図ることを記述しています。
57	15	個人（14）	10	Ⅰ.3.(5)	若年層対応としてセキュリティ・キャンプや、未踏ITなどが取り上げられている。受講後のキャリアの追跡状況は行われているか。また、彼らが突出した技能を持ちつつも体系的に学ぶことのできる場を提供することも彼らのその後のキャリアにおいて必要だと考えている。そのような場は整備されているか。	有能な人材が活躍できる環境整備は重要と考えます。このため、本方針においては「能力を可視化した上で、産業界やセキュリティ関連業務を行う独立行政法人を含め政府関係機関等において業務に従事する者にその能力や実績に見合った適正な処遇を実現していくことも重要であり、産学官が連携して適性処遇の推進やキャリアパス等の整備を検討していく。」と記載しております。 また、体系的に学ぶことができる場として、例えば、一定のサイバーセキュリティに係る業務を含めて勤務経験の後、大学院等の教育機関でサイバーセキュリティのみならず、経営や法律等の他分野の専門知識を身に付ける集中的かつ体系的な学習の機会が与えられる、リカレント教育の充実等を推進することとしています。

番号	枝番	提出者	該当箇所		概要	御意見に対する考え方及び修正
			ページ	章節項		
58	16	個人(14)	全体	全体	方針案全体を通じ、地方における人材育成の方向性が盛り込まれていない。地方や事業体の大小に限らず狙われているため、弱い部分を作らない方針案が求められている。政府としては特に地方の人材育成についてもう少し検討してほしい。	地方における人材育成についても重要であると考えています。そのため、本方針においては「産業界と連携した教育プログラムの開発等を行い、地域における教育機関なども含め、共有化することが重要となる。」としているところです。
59	1	団体(3)	3	Ⅰ.2.(1)	「サイバーセキュリティ経営ガイドライン」の普及を「経営層」に推進するとあるが、「経営層」の定義の精査が必要ではないか。	企業の規模やビジネスモデルによって、「経営層」の捉え方が異なるため、定義をすることは難しいと考えます。
60	2	団体(3)	3	Ⅰ.2.(1)	我が国の民間企業では、実例に乏しいため、政府や民間に近い業務を行っている独立行政法人等政府所管の組織で率先して適用することで、実際の取り組み方の例を示すことができれば民間の参考になる。これらの組織においても情報セキュリティに関わる人材の処遇やキャリアパスは確立されているといえず、そうした面でも手本となっていただければと考える。	政府人材等の育成についても引き続き取り組んでいきます。
61	3	団体(3)	4	Ⅰ.2.(2)	どのような人材を選んで教育し、経営層を支えるためにどのような体制を作っていくのかまで踏み込んでほしい。また、経済や経営学部などやビジネススクールなどとの連携が必要だと考えるが、具体的な施策があれば、言及してほしい。	本方針においては、例えば、「橋渡し人材層」においては、「サイバーセキュリティの知識だけでなく、経営等他分野の知識を併せ持つ「ハイブリッド型人材」(複合型人材)が求められる。」とした上で、各種施策について記載しているところです。
62	4	団体(3)	4	Ⅰ.2.(2)	「そのため、経営層と実務層との間の…コンテンツを平成28年6月を目途に作成する」の内容は、橋渡し人材の「育成」ではなく「支援」と思われる。現状を考えると、支援より育成に重点をおいた施策が必要。	橋渡し人材層の育成には、企業等組織の中の実践が必要となることから、共通的なツールの提供を考えているものです。
63	5	団体(3)	5	Ⅰ.3.	産学官で人材が循環しやすくする制度作りの検討をお願いしたい。	御指摘の点については、人材育成の循環システムを今後検討していく上での参考とします。
64	6	団体(3)	5	Ⅰ.3.(1)	企業における人材育成は、何らかの実務経験者に対して実施することがほとんどである。そのため、最終的な人材像だけでなく、最適の候補者像と施すべき教育をセットで提示する必要がある。	サイバーセキュリティに関する施策を推進するに際し、産業界や大学等の関係者の意見を踏まえることが重要と考えております。このため、産学官の多様な主体が参加可能な「情報セキュリティ社会推進協議会産学官人材育成WG」も活用し、情報共有を行っていくこととしています。
65	7	団体(3)	6	Ⅰ.3.(2)	P.6に「企業からの寄付講座の開設や講師派遣等が進みつつある」とあるが、各企業・講師のモチベーションの上に成り立っている部分もあるため、国としても産学連携がよりスムーズかつ活発になる対策の検討をお願いしたい。	サイバーセキュリティに関する施策を推進するに際し、産業界や大学等の関係者の意見を踏まえることが重要と考えております。このため、産学官の多様な主体が参加可能な「情報セキュリティ社会推進協議会産学官人材育成WG」も活用し、情報共有を行っていくこととしています。 今後、必要となるサイバーセキュリティに係る人材の確保が可能となるように、人材の裾野を拡大し、その能力の底上げを図ることが重要と考えます。このため各取組に対し、積極的に関与・参加を促すことを含め推進してまいります。
66	8	団体(3)	8	Ⅰ.3.(4)	資格は国際的にも認知されるものにするべきであり、ISO/IEC17024に沿ったものにする必要があると考える。	御意見については、今後、情報処理安全確保支援士制度を運用していく上での参考とさせていただきます。
67	9	団体(3)	9	Ⅰ.3.(5)	突出した能力を有した人材は、育成だけでなく、永続的に働ける場を維持・拡大する環境を政策に含めていただくことを期待する。	御指摘の点については、人材育成の循環システムを今後検討していく上での参考とします。
68	―	企業(1)	全体	全体	サイバーセキュリティのための人材不足の解決に産学官が深く協力してあたることが重要と考えており、民間企業が提供する教育プログラムも活用願う。	サイバーセキュリティに関する施策を推進するに際し、産業界や大学等の関係者の意見を踏まえることが重要と考えております。このため、産学官の多様な主体が参加可能な「情報セキュリティ社会推進協議会産学官人材育成WG」も活用し、情報共有を行っていくこととしています。
69	1	個人(15)	2	Ⅰ.2.	サイバーセキュリティを費用ではなく投資と考えるというのは理想であるが、現状利益に結びつかず、投資対効果が図りにくい。 「サイバーセキュリティ経営ガイドライン」にも記載されているが、経営層が意識を変えリーダーシップをとることが何より重要と考える。説明会やセミナーに加え、影響力の高い産学官の人物とメディアを使った広報・啓発活動を行うなどをぜひ盛り込んでいただきたい。	「サイバーセキュリティ戦略」において「社会の変化をより多くの企業経営層が的確に認識し、セキュリティ対策はやむを得ない「費用」ではなく、より積極的な経営への「投資」であるとの認識を醸成していくことは、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。」と示しており、本方針も同戦略を踏まえたものとなっています。 そのため、「サイバーセキュリティ経営ガイドライン」の普及も含め、サイバーセキュリティに関する取組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ための方策について取り組むこととしています。 今後の取組の参考とさせていただきます。

番号	枝番	提出者	該当箇所		概要	御意見に対する考え方及び修正
			ページ	章節項		
70	2	個人（15）	5	Ⅰ.3.	ユーザ企業においてもセキュリティ人材を確保し、活用する仕組みは必要であるが、専門性が認められないとキャリアを積むことは難しい。企業では、様々な業務経験を積む意味で異動ローテーションがある。そのような環境で、変化の激しいセキュリティの専門キャリアを積み育成することは非常に難しい。 専門家からの知識の吸収やセキュリティ領域でキャリアや経験を積むこと視野に入れ、ユーザ企業も含めた、産学官のセキュリティ人材交流をより増やして欲しい。 情報処理安全確保支援士及び情報セキュリティマネジメント試験については是非推進してほしい。適正処遇の推進についても期待したい。	産学官のセキュリティ人材交流や情報共有は重要と考えております。また、能力に応じた適正処遇は重要であり、本方針においても「能力を可視化した上で、産業界やセキュリティ関連業務を行う独立行政法人を含め政府関係機関等において業務に従事する者にその能力や実績に見合った適正な処遇を実現していくことも重要であり、産学官が連携して適性処遇の推進やキャリアパス等の整備を検討していく。」としているところです。
71	1	個人（16）	6	Ⅰ.3.(2)	サイバー攻撃のような複雑で未知の問題に対応する人材を育てるには、従来の学校教育を改革し、正解のない問題の解決策やリスクの回避方法を考えさせ議論させるような能力開発を行う必要がある。文部科学省にも協力させて、サイバーテロ対策など社会の複雑な問題に対応する能力を身につけられる実践的な教育を学校で実施してほしい。	例えばenPiTにおいて複数の大学と産業界による全国的なネットワークを形成し実際の課題に基づく課題解決型学習等の実践的な教育を推進しているところですが、御意見につきましては、今後の取組の参考とさせていただきます。
72	2	個人（16）	全体	全体	サイバーテロに備えるには、コンピュータ技術に関する知識だけでなく、日本や世界各国の法律・時事問題・文化・産業構造など、背景にある問題や法制度に関する幅広い知識が必要。サイバーセキュリティ人材の育成にあたっては、IT技術だけでなく、そうした幅広い教養を習得させてほしい。	サイバーセキュリティの知識だけでなく、経営等他分野の知識を併せ持つ「ハイブリッド型人材」の育成は重要であり、本方針においてもその旨記載しております。
73	3	個人（16）	全体	全体	日本の企業の多くは人手不足の状態にあり、サイバーセキュリティ人材を社内で全て育成するのは難しい。 セキュリティの監査やコンサルを行う公的機関をつくる等して、サイバーセキュリティ業務を社外にアウトソースできる仕組みをつくり、各企業の負担を減らす工夫が必要。	本方針においても産学官が連携した人材の循環システムの構築について記載しており、サイバーセキュリティに人材育成について産学官が密接に連携していくことが重要だと考えています。
74	4	個人（16）	全体	全体	企業の多くは、海外に事業拠点を展開し、製品を世界中に輸出している。セキュリティ人材育成の施策は、海外で採用・育成する現地人も対象にすべき。 海外の大学や教育省などに働きかけをして、日本品質のセキュリティ人材の育成を進めてもらう必要がある。	今後の取組の参考とさせていただきます。
75	5	個人（16）	全体	全体	優秀な人材を集めるには、スキルを習得してその職種に就くことで得られる報酬が大きくなければならない。 建物の診断や健康診断の業務を国家資格を有する者に限定しているのと同じように、サイバーセキュリティ業務についても国家資格保有者に限定する等して、セキュリティ技術者の雇用や所得水準を保障する制度も必要。	能力に応じた適正処遇は重要であり、本方針においても「能力を可視化した上で、産業界やセキュリティ関連業務を行う独立行政法人を含め政府関係機関等において業務に従事する者にその能力や実績に見合った適正な処遇を実現していくことも重要であり、産学官が連携して適性処遇の推進やキャリアパス等の整備を検討していく。」としているところです。
76	6	個人（16）	全体	全体	サイバーセキュリティ対策に関する法制度を立案・決定・実行する国会議員や官公庁職員がサイバーセキュリティの脅威や対策について理解していなければ、産業や生活を守るサイバーセキュリティ対策の法制度は整備できない。 サイバーセキュリティ教育は、学生や企業の社員だけでなく、国会議員や行政職員にも実施すべき。	御指摘のとおり、サイバーセキュリティ対策はあらゆる人に必要な素養になっていると認識しております。また、サイバーセキュリティに関する関心・理解度・対応力について広く国民に浸透させるため平成21年度から「情報セキュリティ月間」（現「サイバーセキュリティ月間」）を設け国民に親しみやすいメディアを活用する等普及啓発活動に取り組むなどしているところです。
77	－	個人（17）	5	Ⅰ.3.	「リカレント学習の充実」に賛同する。 サイバーセキュリティに求められる人材は、自身の対応が社会にどう影響するかを感じるセンサーを持つことが必要であり、他分野の企業人・実務家との大学院における交流は、多角的な視点やコミュニケーション能力を身に付ける良い機会である。同時に、こうした交流や実習の際、自身がこれまで修得した専門知識を、相手に啓蒙することで双方のシナジーを生む。 一方、リカレントより前の基礎トレーニング段階では、多種多様な攻撃手法の研究・実践を自由かつ十分に行える空間が必要であり、法律による制約的な特性から開放された場やルールを作るべきである。	サイバーセキュリティの知識だけでなく、経営等他分野の知識を併せ持つ「ハイブリッド型人材」の育成は重要であり、本方針においてもその旨記載しております。
78	－	個人（18）	全体	全体	経済産業省認定の国家資格、IPA「情報処理技術者試験」のうち、「ITパスポート試験(IP)」と「情報セキュリティマネジメント試験(SG)」の品質向上と普及率向上のプロジェクトを実施してほしい。	御指摘の点については、現状においても取り組んでいるところですが、今後も引き続き同取組に努めてまいります。

番号	枝番	提出者	該当箇所		概要	御意見に対する考え方及び修正
			ページ	章節項		
79	―	個人（19）	5	Ⅰ.3.	人材の需要と供給の循環サイクルが有効に機能するためには、報酬やコストの負担についてある程度の議論や想定が必要と考えている。 雇用サイド（ユーザ企業）において、人材が流動的にサイクルするには給与・福利厚生が競争的であることが必要であるが、日本の企業文化では他の職務に比べて高い報酬を実現するのはそう簡単ではない。採用のモチベーションを上げる議論が必要。逆に、うまく機能すれば、人材共有も自ずからついてくると思われる。 供給サイドにおいては、コストである教育費を個人、企業、国のいずれが負担すべきものか。将来高額報酬を得ることが期待できなければ個人負担はありえず、企業や国が負担するのであれば、このサイクルのどこでコストが回収されるかを考える必要がある。 人材流動のサイクルではなくスキルセットのサイクルであれば、個々の企業が従業員を産学で教育するということで、企業がコストを負担するのは理にかなっているが、もはやより良い教育内容を提供するための議論だけでよい気がしている。 また、「橋渡し人材」はとても良い概念であり、この人材のサイクルの議論を深めていただきたい。特に外部採用については、有効に機能するための方法論や企業風土の分析・研究が必要である。	人材育成の循環システムを形成するためには、それぞれの取組・施策をつなげる取組が必要であり、産学官の多様な主体が参加可能な「情報セキュリティ会推進協議会産学官人材育成WG」も活用し、情報共有を行っていくこととしています。 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。
80	1	個人（20）	3	Ⅰ.2.(1)	IPAより先頃公表された「2015年度 中小企業における情報セキュリティ対策に関する実態調査」によれば、日本における企業の8割以上を占める中小企業の多くは、情報セキュリティ担当者が不在で社内外の相談窓口もない。中小企業における「経営層」の意識改革を促していくために、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について、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。	御意見については、今後、情報処理技術者試験制度等のあり方を検討する際の参考とさせていただきます。
81	2	個人（20）	6	Ⅰ.3.(2)	「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がそのスコアや上位合格者を示し表彰することにより、ユーザー企業のIT人材が適切に評価されるのではないか。また、競技会やイベント的に試験を実施することで、学生やユーザー企業の合格後の継続教育に繋がっていくのではないか。	御意見については、今後、情報処理技術者試験制度等のあり方を検討する際の参考とさせていただきます。 なお、ITパスポート試験については、国内においても実施しているところです。
82	3	個人（20）	8	Ⅰ.3.(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パスポート試験、情報セキュリティマネジメント試験についても、「情報処理業務活用推進者」、「情報処理安全活用推進者」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スキルや情報セキュリティに係わる知識を身に付けている企業人が充足していおらず、ITパスポート試験の合格が全ての企業人の必須スキルとなるよう推奨してはどうか。 「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。情報セキュリティスペシャリスト試験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。 3万人を確保するために旧制度の合格者を認定することには反対。	御意見については、今後、情報処理技術者試験制度、情報処理安全確保支援士制度のあり方を検討する際の参考とさせていただきます。 なお、ITパスポート試験については、御指摘のとおり全ての社会人が備えるべきITリテラシーとして推奨しているところですが、今後も引き続き、その普及に努めてまいります。
83	1	団体(4)	8	Ⅰ.3.(4)	世界規模でサイバー攻撃が行われている現状を踏まえ、日本国独自の資格のみで能力の可視化を行うのではなく、ISACAのCISM、(ISC)2のCISSP、SANSのGIAC 等のグローバルスタンダードな資格も追加してはどうか。	御意見については、今後、情報処理安全確保支援士制度等のあり方を検討する際の参考とさせていただきます。
84	2	団体(4)	8	Ⅰ.3.(4)	「情報処理安全確保支援士」になるための要件や、設置要件の有無等を明確にしていただきたい。また、制度設計にあたって、事業者にとって過度な負担とならないようご配慮いただきたい。	御意見については、今後、情報処理安全確保支援士制度の普及策等を検討する際の参考とさせていただきます。