「サイバーセキュリティ人材育成プログラム（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：　2017年３月13日（月）～ ３月24日（金）
- 意 見 総 数：　15者から69件【内訳：2企業・団体から延べ13件、13個人から延べ56件。】

意見内容の内訳：

１．本プログラムの趣旨・位置づけ等に関わる意見	8件
２．本プログラムの状況の認識に関わる意見	3件
３．今後の具体的な取組に関わる意見	17件
４．資格制度に関わる意見	6件
５．その他意見	35件

意見を踏まえた修正：　全3件

注）提出された意見等は必ずしもこれらに分類されるわけではないが、事務局で理解した区分にて計上している。

意見募集に対して寄せられたご意見の概要及びご意見に対する考え方

※ご意見の全体像が分かるように、代表的な意見を例として抽出し、その趣旨を踏まえて編集・整理しております。

番号	具体的な意見内容	ご意見に対する考え方
1	○本プログラムの趣旨・位置づけ等に関わる意見 （意見の例） ・サイバーセキュリティ人材育成プログラムに賛同する ・情報セキュリティとサイバーセキュリティ、そしてセーフティなどのマッピング、サイバーセキュリティ人材の定義、人材育成の方向性を明確にすべき ・いつまでに、何を達成できるのかが不明。希望の持てるプランを提示いただきたい ・誰を対象にしているのかが不明。研究者・開発者や官僚の育成の観点が非常に乏しく、文書のスコープが狭すぎる ・サイバーセキュリティを経済活動の一環として捉えており、国家安全保障や治安活動を含めた視点に乏しい ・民にできる部分は民が担うよう、積極的に官から民への移行を支援すべき ・サイバーセキュリティを社内向け（守り）と社外向け（攻め）を明確に分けて考えることが重要である	本プログラムは、企業をはじめとする社会で活躍できるサイバーセキュリティに関連する人材育成の方向性を示すことにより、安全な経済社会の活動基盤としてのサイバー空間の形成に向けた環境整備を図るものです。こうした中で、ビジネスにおけるイノベーションの担い手となりうる研究者や開発者も対象とし、高度人材として記載しております。また、サイバー攻撃は、国民生活や国際社会が危機にさらされる原因となりうるとしており、こうした脅威に対処できることも人材育成の目的としております。さらに、若年層の教育も含め、サイバーセキュリティ向上へのモチベーションを持つような人材育成に取り組むことが重要であることを位置づけております。今後、サイバーセキュリティをとりまく状況や課題については、フォローを行い、適時、必要に応じて本プログラムの見直しを検討することとしております。その中で、本プログラムの趣旨・位置づけや、状況の認識等に関し、いただいた御意見を参考にさせていただきます。
2	○本プログラムの状況の認識に関わる意見 （意見の例） ・「サイバーセキュリティ人材育成の取組については一定の成果があったといえる」とあるが、エビデンスを提示いただきたい ・情報処理技術者というよりも、社会人や学生などにおいて、ITリテラシーが不足していることが問題である ・セキュリティを「投資」と考える場合、リターンを求めないリスク低減や製品・サービスの付加価値向上、ひいては競争力向上や企業価値向上を図るために必要不可欠なものが重要である	
3	○今後の具体的な取組に関わる意見 （意見の例） ・業務の規模と内容に応じて、必要なスキル（資格）を持つ人材を一定数必置とし、さらに不作為によるインシデント発生時には経営層への罰則も検討すべき ・欧州でも話題になっているように、セキュリティベンダーによるビジネスのための偏向したデータを政府がそのまま利用している。攻撃を明確にした上で、顕在化の可能性、社会的影響の大きさを検討し、何をする人材がどの程度必要かを明確にすべき ・サイバーセキュリティに特化した教育だけではなく、基礎分野の教育についても支援・強化をすべき ・日本国内の独自の認定制度に基づく官中心の人材育成ではなく、国際的に認定されている民間資格や教育プログラムも積極的に取り入れるべき ・セキュリティ対策の有効性評価は、実務部門から独立したリスク管理部門や専門知識を持った経営者が行うべき ・サイバーセキュリティを投資として考えよというのであれば、投資効果を適切に判断できる基準を示すべき ・各所・各層におけるサイバーセキュリティ人材に求められる「素養」の具体化、サイバーセキュリティ人材の新たな活躍の場への流動性を高める方策の検討を行うべき ・情報通信の基礎知識保有者として無線従事者や工事担当者の人材活用や従来の技術をカリキュラムに取り入れる議論をすべき ・セキュリティの自動化に関する技術や知見をもった人材育成に力を入れるべき ・サイバーリスクへの対応には、クラウドへの理解や語学の能力も必要 ・「産学官からなる実務者のワーキンググループ」では、産学官の各活動の相互連携や重複排除の観点が重要 ・セキュリティ技術のイノベーション、ビジネスイノベーションは、一企業が自らの予算では対応不可能なので、国としての積極的な支援をお願いしたい ・産学連携による人材育成の推進（寄附講座等の産学連携活動）も盛り込んでほしい ・初等教育に関しては、大学まで含めたトータルでの教育体系を考慮すべき ・教える側の人材育成の課題解決が必要である ・経営層の意識改革は、政府からの働きかけが重要である	需要と供給の好循環を形成するため、NISCが中心となって、産学官の連携を図るためのネットワークの強化や、モデルとなるカリキュラムの策定をはじめ、各施策間の連携に向けた取組を推進することとしております。具体的には、サイバーセキュリティ人材に関する施策間連携ワーキンググループ等を通じて、関係府省庁や産業界、大学等とも連携し、今後の具体的な取組を推進してまいります。こうした今後の活動の中で、いただいた御意見を参考とさせていただきます。
4	○資格制度に関わる意見 （意見の例） ・2020年までに3万人を確保するため、受験機会を増やしたり、同レベルの民間資格の保有者に情報処理安全確保支援士の資格を付与することを検討すべき。また、資格保有者に対するインセンティブを増やすことを検討すべき ・情報セキュリティシステムアドミニストレータの合格者を活用すべき。例えば、情報処理安全確保管理士などを創設し、情報セキュリティシステムアドミニストレータ合格者をみなし合格者とすべき ・情報システムの利用部門への普及を促す観点から、「情報セキュリティマネジメント試験」について、「情報処理安全活用推進士」等とした名称独占の国家資格を創出すべき ・情報処理安全確保支援士の配置を義務化し、一定数配置した場合には税制優遇を与えるなどの制度整備により、サイバーセキュリティ人材育成に係るメリット・デメリットを定義すべき ・情報処理安全確保支援士に関する試験免除の制度を改善すべき	
5	○その他の意見 （意見の例） ・eDiscoveryは訴訟対応であり、サイバーセキュリティとは別の領域である ・技術的修正に関する意見（西暦による表記を年号によるものにすべき等）	・本プログラムでは、セキュリティの範囲が広がっていることを解説しております。その観点で、その他の意見につきましても、今後の取組の参考とさせていただきます。 ・技術的修正に関する御意見の一部については、それを踏まえて本文の修正をさせていただいております。