

「新・情報セキュリティ人材育成プログラム(仮称)」
〈概要〉

2014年1月8日
普及啓発・人材育成専門委員会

新・情報セキュリティ人材育成プログラム(仮称)概要

1. はじめに

本プログラム策定までの経緯

「情報セキュリティ人材育成プログラム」(2011年)
(2011年度～2013年度及び中長期的な人材育成施策の方向性)

「情報セキュリティプログラムを踏まえた2012年度
以降の当面の課題等について」(2012年)
(人材育成施策の課題及び具体施策提言)



「新・情報セキュリティ人材育成
プログラム(仮称)」(2014年度～2016年度)



・「サイバーセキュリティ戦略」(2013年)
・IT総合戦略本部「創造的IT人材育成方針」(2013年)

2. 情報セキュリティ人材に関する現状と課題

(1)情報セキュリティリスクの深刻化

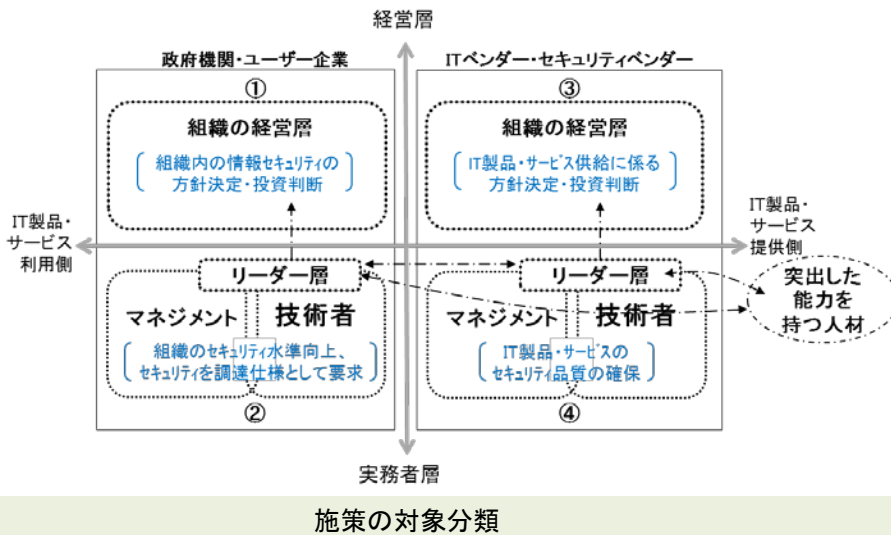
- 甚大化するリスク** 情報窃取のための標的型攻撃、重要インフラ機能障害を引き起こす攻撃等、サイバー攻撃が複雑・巧妙化。
- 拡散するリスク** あらゆるものがインターネットに接続されることにより、制御システム等もサイバー攻撃の対象に。
- グローバルリスク** 世界各国の情報通信技術利用拡大に伴い、国境のないサイバー空間では、リスクもボーダレスに拡大。

(2)情報セキュリティのスキルを有する人材の不足

- 情報セキュリティに従事する技術者約26.5万人のうち、約16万人が必要なスキルを満たしておらず質的に不足。加えて、潜在的に約8万人が量的に不足。(IPA試算)
- 急激に進む情報セキュリティリスクの深刻化への対応には、高度な専門性や突出した能力を有する人材も不可欠。
- グローバルリスクの拡大に伴い、活躍の場が国内・海外であることを問わず、グローバル水準の人材が必要。

(3) 施策の対象分類と検討すべき課題

リスクの深刻化と、一方で生じる人材不足に対処するためには、人材の育成・発掘(供給)だけでなくその雇用等(需要)にも施策を講じて「人材の好循環」を形成し、我が国の情報セキュリティレベルの向上をはかる必要がある。



- ◎「①利用側の経営層」は、情報セキュリティを経営戦略として認識し、「②利用側の実務者層」を適切な処遇で登用することが必要。【需要】
- ◎「②利用側の実務者」は、適切な情報セキュリティ対策を判断し、「④提供側の実務者層」に要求できる能力を身に付けることが必要。【供給】
- ◎「③提供側の経営層」は、必要なサービス・製品の開発・導入と、「④提供側の実務者層」を適切な処遇で登用することが必要。【需要】
- ◎「④提供側の実務者」は、利用側の顕在的・潜在的な要求に応えるレベルの能力を身に付けることが必要。【供給】
- ◎加えて、国全体のセキュリティレベル向上のため、牽引役として突出した能力を持つ人材が、各場面を行き来して活躍することが必要。【供給】

3. 今後の取組方針

我が国の情報セキュリティの水準を高めるため、人材の「需要」と「供給」の好循環を形成する。

【需要】経営層の意識改革

- ・経営層の意識改革を促し、情報セキュリティを経営戦略として認識させるための取組を推進。情報セキュリティに対する投資意欲を喚起して人材の需要を創出。

【供給】人材の「量的拡大」と「質的向上」

- ・実務を担うボリュームゾーンに当たる既存のIT技術者に、情報セキュリティを必須能力として位置付ける。
- ・グローバル化する脅威に対応できる、高度な人材や突出した能力を有する人材を育成・発掘。

(1) 経営層の意識改革 【人材の需要側へのアプローチ】

① 経営戦略の一部としての情報セキュリティ対策の推進

- ▶ 組織全体のリスク管理の一環として情報セキュリティを事業継続に不可欠なものとして捉え、経営戦略の一部に位置づけていく。
- ▶ 情報セキュリティ対策や人材育成の重要性等について、経営層が集まるあらゆる機会をとらえて、経営戦略としての情報セキュリティに関する啓発活動を行っていく。
- ▶ 経営層がより一層、自社のセキュリティ対策に目を向けるための取組のひとつとして、米国の証券取引委員会(SEC)における取組を参考にしつつ、情報セキュリティに関連して起こりうる危険を事業等のリスクとして開示すること等について検討し結論を得る。

② 調達における情報セキュリティ要件の設定

- ▶ 製品・サービスの調達において、利用側が情報セキュリティを要件とすることは、提供側の意識改革につながると考えられ、情報セキュリティが経営に不可欠な基盤として再認識されることが期待されることから、政府調達で率先して取組をリードする。

(2) 必須能力としての情報セキュリティ 【人材の供給側へのアプローチ】

① 技術者に情報セキュリティを意識させるための取組

- ▶ システム設計・運用の要であり、情報セキュリティを実務として担当する人材のボリュームゾーンでもあるシステムエンジニア、プログラマー等のIT技術者に対し、企業内や教育機関等において、情報セキュリティスキルを向上させるための実践的な教育を実施。
- ▶ システムの設計段階から情報セキュリティ対策を織り込む「品質としてのセキュリティ」の必要性をベンダー、ユーザーの双方が共有し、情報セキュリティのスキルが不可欠である共通認識を形成。

② 情報セキュリティ能力の評価基準・資格等の整備

- ▶ 情報セキュリティ人材の能力を評価し、それを組織内での業務・処遇等に反映させていくため、情報セキュリティに関する資格試験やスキルを評価する基準、教育プログラムの整備等を政府として進めていく。
- ▶ 具体的には、スキル標準の改善・活用等を通じ必要とされる能力・知識を明確化。さらに、常に最新の情勢を踏まえた実践的な対処能力を評価・担保できる仕組みについて検討を進め、人材の能力の見える化を推進。

③ 情報セキュリティの実践的スキル向上のための取組

- ▶ 政府機関等が保有するサイバー攻撃の特徴的な事例を収集・分析してケースを作成。そのケースを題材として、技術者等が対処法(防御・攻撃方法も含む)について自ら考え、対策を検討できるような実践的な学習教材(教育プログラム・シミュレーター等)を政府関連機関、教育機関で作成・活用。
- ▶ 実際のサイバー攻撃を想定した仮想空間上での対応訓練等、国の研究機関等が保有している施設を活用。実際の運用環境に近い試験用プラットフォームを活用した演習・訓練により現場での対応力を強化。

(3) 高度な専門性及び突出した能力を有する人材の発掘・育成【人材の供給側へのアプローチ】

- ▶ 日々変化する新たな事案や高度な事案に対応し、情報セキュリティ分野を牽引するような高度な専門性を持った人材や、突出した能力を有する人材が不可欠。一方で、そのような人材を発掘・育成するためには、画一的な教材・教育プログラムだけではなく、テストベッドを用いた先端的な研究開発を通じた人材育成や、能力の開花に結び付く場を設ける等の成長支援が必要。

① 高度な専門性を持った情報セキュリティ人材育成のための高等教育の強化

- ▶ 「情報技術人材育成のための実践教育ネットワーク形成事業(enPiT)」等、複数の大学が連携して体制を整えるとともに、産学連携を進める。
- ▶ 大学・大学院で情報セキュリティに関する研究科等の設置を検討(経営学等の分野、海外の機関との連携も視野に)。
- ▶ 高専、専門学校等においては、ハードウェアとソフトウェアの基礎的な力をしっかりと身につけた上で、実践的な情報システムの開発能力を備える技術者の育成を行うとともに、必要な教員の充実等の場を整備。

② 最先端の分野で活躍する突出した人材の発掘及び更なる能力向上

- ▶ 最先端の分野で活躍する突出した能力を持つ人材は、通常の教育による育成が難しい。その能力に着目した発掘や、切磋琢磨して能力の開花に結び付く場を設けることが重要。このため以下のような取組を実施。
 - ・ 将来のIT産業の担い手になり得る優れた若い人材の発掘と育成のため、IT業界の第一線で活躍中のトップエンジニアを講師として招聘し、情報セキュリティなどに関する高度な教育プログラムである「セキュリティキャンプ」事業
 - ・ IT技術を駆使してイノベーションを創出することのできる独創的なアイデアと技術を有するとともに、これらを活用する優れた能力を持つ、突出した若い逸材(スーパークリエータ)を発掘育成することを目的とした「未踏事業」
 - ・ チームに分かれて主催者の用意する課題をクリアしながら得点を競う競技イベントである「SECCON」の開催

(4) グローバル水準を超える人材の育成

- ▶ 企業の活動を始めとするあらゆる分野において、国内のみならずグローバル水準で見てもリードできる人材が必要。
- ▶ グローバル水準の人材が各高等教育機関で育成されるとともに、企業等において積極的に雇用されるよう取組を推進。
- ▶ グローバル水準の人材育成に向けては、できるだけ多くの国際的な体験や情報共有の場が必要。このため、各国機関との緊密な連携、世界トップクラスの専門家が集まる国際会議の誘致、留学支援等を通じて研鑽を積む場を増やしていくことが有効。
- ▶ また、国内で行われている競技イベント等を国際レベルで実施することも検討。

(5)政府機関等における人材育成

①政府機関における人材育成

- ▶政府機関等においても、その情報及び情報システムに係る情報セキュリティ水準の一層の向上を図るため、システム担当者の能力の底上げや幹部の情報セキュリティに対する理解の増進は引き続き着実に取り組む。
- ▶採用及び人事ローテーションにおける特別の配慮や、官民の人事交流等による外部の優秀な人材の有効活用等に引き続き積極的に取り組んでいく。
- ▶情報セキュリティセンターの機能強化に合わせ、インシデント情報の集約、技術動向の分析が可能な内部人材の育成を進める。
- ▶情報システム担当者のみでなく、職員全員の意識や能力の向上のため、研修・訓練を実施。
- ▶将来的には、海外のように情報セキュリティの専門家が、政府、民間企業、研究機関、教育機関の各機関で経験を積みつつ、総合的なセキュリティ人材としてのスキルを上達していくようなキャリアパスが形成されることが望まれる。

②重要インフラ事業者等における人材育成

- ▶「分野横断型演習」や「セプター訓練」の実施及び改善を図るとともに、重要インフラ事業者等における組織内CSIRT等の設置や、重要インフラ事業者等を対象としたワークショップ等を開催するなど、情報セキュリティリスクに対応できる職員の育成等を通じて、職員の情報セキュリティ意識の啓発と能力の底上げ等の取組を推進。

(6)横断的課題

①初等中等教育段階における情報通信に関する基礎学力に関する教育の充実

- ▶初等中等教育段階において、情報通信技術に関する教育の充実。今後さらに、情報処理に必要な論理的な思考力やITの原理についての理解を促すようなものとなることを期待する。また、このような思考力や理解を確認する内容を含む試験についても検討が進むことを期待する。

②高等教育段階における実践的能力を高める演習の強化

- ▶高等教育段階において、情報系技術者として必要な実践的能力をより一層高める演習の強化が望まれる。

③情報セキュリティ人材のキャリアパスの提示

- ▶情報セキュリティの専門家だけでなく、IT技術者全体において、情報セキュリティの知識を習得することを前提とした人材の育成、キャリアパスの提示が必要。

ご議論いただきたい点

「新・人材育成プログラム(仮称)」に関し、特にご議論いただきたいと考えている点は以下のとおり。

全体的な方向性について

○プログラム全体の構成や方向性について、具体的に修正すべき点や不足している点はないか。

推進方策について（具体性が不足していると考えられる点）

○経営層の意識改革に向け、現在挙げている取組の他に考えられる具体策はないか。

○人材の能力の「見える化」のために、現在挙げている取組(スキル標準の改善・活用、能力評価の仕組みの検討)に加えて具体的に必要な取組はないか。

○グローバル化する脅威に対応できる人材の育成に向け、我が国が取り組まなければならない具体策は何か。

○高等教育段階の学生の実践的能力をより一層強化する具体的対策は何か。

○高等教育機関等で情報セキュリティが教えられる人材を育てていくため、具体的にどのような取組が必要か。

フォローアップ及び成果指標について

○本プログラムの目標、成果指標として具体的にどのような指標が考えられるか。

例えば、情報セキュリティ人材の不足感については企業へのアンケート形式で調査が行われているが、代替されるべき指標はないか。

情報処理技術者試験の受験者数、合格者数は、指標として適切か。

○上記指標を設定する場合、具体的にどのような計測手法・データ取得方法が考えられるか。