資料２－１

NISC National Information Security Center

「新・情報セキュリティ人材育成プログラム」関係施策の状況等について

「新・情報セキュリティ人材育成プログラム」の進捗状況について

■ 「新・情報セキュリティ人材育成プログラム」を踏まえ、各省庁等において、各種取り組みが推進されている。

■ 前回6月の専門委員会では、それぞれの施策の進捗状況にあわせ、専門委員会としても協力、もしくは実質的に関与して　いくべき施策を以下のように分けて示したところ。

■ 現在の進捗状況も踏まえ、今後専門委員会として取り扱っていく主な論点について検討を進める。

＜施策の推進方針＞

1.【関係省庁ですでに着手されており、引き続き着実に推進すべき施策】
○政府全体として整合性を持って進めていく観点から、専門委員会としても進捗状況等を適時把握し、必要に応じて助言。

2.【関係省庁の取組に対し、専門委員会としても協力していくべき施策】
○具体的な進め方について、専門委員会として積極的に意見を述べ、また助言等を実施。

3.【プロジェクト等の立ち上げから専門委員会として実質的に関与していくべき施策】
○必要な取組について、専門委員会として関係省庁に働きかける等により、施策を具体化。

「新・情報セキュリティ人材育成プログラム」の進捗状況について

1.【新プログラム策定前から関係省庁ですでに着手されている施策】
○政府全体として整合性を持って進めていく観点から、専門委員会としても進捗状況等を適時把握し、必要に応じて助言。

◇官公庁・企業等のサイバー攻撃等への対応能力向上に向けた実践的な訓練・演習の推進
（内閣官房、各府省庁）
・CYMATにおける省庁横断的な要員の研修（毎月）（内閣官房）：27年度概算要求　0.3億円
・実践的サイバー防御演習「CYDER」（総務省）　：27年度概算要求　4．5億円の内数

◇ enPitプログラムを通じた、複数の大学や大学院、産業界とが連携した実践的な高等教育の推進
（文部科学省）
・情報技術人材育成のための実践的教育ネットワーク事業：27年度概算要求　4．5億円

◇「セキュリティキャンプ」「サイバーレスキュー隊」等を通じた人材の発掘・育成（経済産業省）
・情報処理推進機構運営費交付金：27年度概算要求　36．1億円の内数

「新・情報セキュリティ人材育成プログラム」の進捗状況について

2.【関係省庁の取組に対し、専門委員会としても協力していくべき施策】
○具体的な進め方について、専門委員会として積極的に意見を述べ、また助言等を実施。

■ 企業等の経営戦略の一部としての情報セキュリティ対策の推進に係る施策

○経済団体等の場を活用して、企業等の経営層に対し、経営戦略の一部としての情報セキュリティ対策について意識啓発を実施（内閣官房）

・経団連において、国の基本問題検討委員会・情報通信委員会合同会合を開催、我が国におけるサイバーセキュリティの状況、最近の脅威等について、NISCから講演（本年10月1日）。

・新経連において、インターネットセキュリティWG第1回開催（本年6月4日）、海外機関と連携して会員企業への啓発やアンケート調査等を実施中。

○上場企業におけるサイバー攻撃によるインシデントの可能性等について、事業等のリスクとして投資家に開示することの可能性の検討（金融庁）

・金融庁において、SEC（米国証券取引委員会）、IOSCO（証券監督者国際機構）等海外機関の状況も注視しつつ検討が行われているところ。

■ 情報セキュリティに係る資格制度の在り方についての検討

○情報処理技術者試験の改善に係る検討の開始（経済産業省）

・新たな試験区分「情報セキュリティマネジメント試験」に関する検討がスタート。

・企業（とくにユーザー企業）内で、情報セキュリティポリシーの運用や調達に携わる人材の能力の底上げに資することを目指している。

「新・情報セキュリティ人材育成プログラム」の進捗状況について

■政府機関等における人材育成

○調達における情報セキュリティ要件の設定 （内閣官房、各府省庁）

・「政府機関の情報セキュリティ対策のための統一基準」において、情報システムの開発・運用等を外部委託する際に、従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）を確認することとした。

・調達における情報セキュリティ要件化について、政府が率先して取り組むことで、ベンダー側において情報セキュリティに対する投資意欲が喚起され、人材の登用・処遇向上が進むのでないか。

○サイバーセキュリティシリアスゲームに係る研究 （防衛省）

・日々高度化するサイバー攻撃に対し、防衛省・自衛隊職員のサイバーセキュリティに関する知識・経験レベルの底上げを目的に、体験型学習（シリアスゲーム）の手法を生かした、効果の高い学習教育・教育プログラムの整備に関する調査研究を計画している。

■ 初等中等教育段階における情報教育の充実・教員の指導力向上

○初等中等教育段階からの情報教育の充実（文部科学省）

・情報セキュリティの基礎となる、情報通信技術の学習において、コンピューターの原理等についての理解を促すことが必要ではないか。

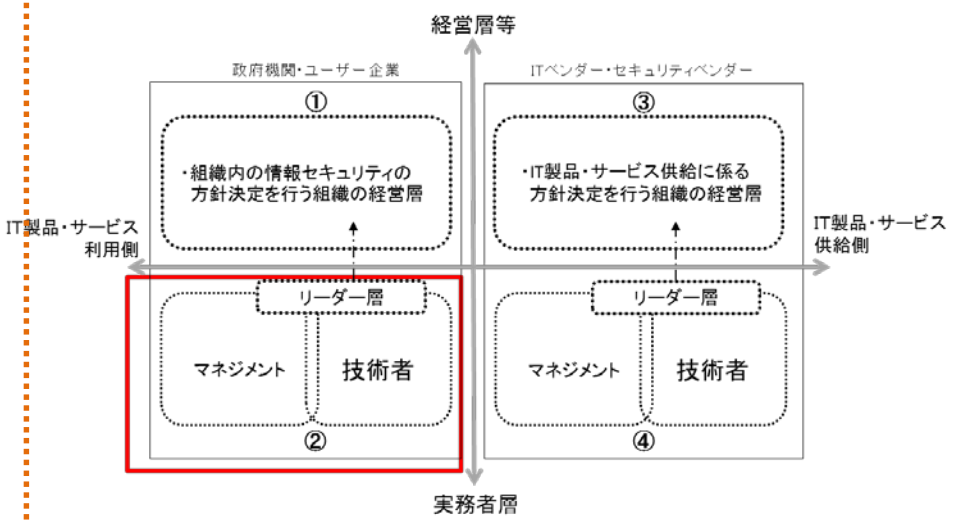
・英国等では、初等教育の段階からプログラミング教育の必修化が行われているが、こうした動向を踏まえつつ、プログラミング教育の在り方、子どもたちの関心の喚起、教員の指導力の向上に向けた検討が必要ではないか。

「新・情報セキュリティ人材育成プログラム」の進捗状況について

3.【プロジェクト等の立ち上げから専門委員会として実質的に関与していくべき施策】

○必要な取組について、専門委員会として関係省庁に働きかける等により、施策を具体化。

■ 経営層と実務者層の間をつなぐリーダー層の能力を育成する環境整備



○ユーザー側からの情報セキュリティに対する要求がない限り、提供するベンダー側の体制は強化されず、高度な人材の需要も喚起されない。

○ユーザー企業が組織として情報セキュリティの必要性を認識しない限り、正しい要求は行われにくい。経営層の意識を高めると同時に、実務者層とのコミュニケーションが円滑になることが重要。

○このため、ユーザー側の実務者層のリーダー層の育成が我が国のサイバーセキュリティの総合力を高めるために最も重要でないか。

○ユーザー側の実務者層のリーダー層を育成するための実践的な研修としてどのようなものが適切か？

【現在の取組】

・情報セキュリティ大学院大学では、情報セキュリティに加え、法とガバナンス、リスクマネージメント等の幅広いカリキュラムを実施

・・JUASの研修において、「IT投資対効果とその評価方法、実践モデル構築体験講座」「調達マネージメント実践講座」などのユーザー企業の実務者層のリーダー層を育成する研修等を実施

「新・情報セキュリティ人材育成プログラム」の進捗状況について

■ サイバー攻撃等のケースを基とした実践的な教材等の開発・事例共有の推進

・サイバー攻撃等に関する情報共有の枠組みとして、日本サイバー犯罪対策センター（JC3）、サイバー情報共有イニシアティブ(J-CSIP)、テレコム・アイザック推進会議（Telecom-ISAC Japan）等の枠組みがあるが、これら、国等に報告された事例や教訓等を死蔵させず、後の人材育成に活かすために共有する仕組みが作れないか。

・例えば、実際の事例を基にしたケースによるディスカッション形式での実践的な教育が行えないか。

・そのためにどのような課題があるか
- 事例の収集・配布にあたって、どのような検討が必要か（匿名化等）
- 収集、教材化、実際の教育はそれぞれどのような主体が担い、どのようなスキームで行っていくか
- 教材等を用いた教育をどのような形式で行っていけばよいか

（教材作成のイメージ）

○実際に事案対応に当たった組織において、事案の発生段階から収束までを時系列的にまとめた事例集を作成。

○各教育機関等において、事例を基に、例えば、インシデント発生の連絡を受けた初期段階、追加調査の段階に分け、想定される事象や次の調査内容の検討、応急処置の検討について実際に行った行動と比較し議論していくのはどうか。

○また、事例としては、公開情報としての取り扱いのしやすさから、まずは政府や独立行政法人における事案のうち秘匿性の低いものから取り組んでいってはどうか。

○また、実際に教える側、生徒の側から、事例集としてどのような情報を盛り込むべきかの改善点をフィードバックするために、例えば、文部科学省が実施しているenPITのカリキュラムの中でケーススタディを盛り込むのはどうか。

「新・情報セキュリティ人材育成プログラム」の進捗状況について

■ 情報セキュリティ人材のスキルモデルの作成

- **これまでの委員会で、それぞれの人材がどのようなスキルセットが求められるのかを明確にすべきとの指摘があった。**
- **IPAでは情報セキュリティ人材について、職種モデルを設定し、そのミッションや活動内容、求められるスキル等について整理しているが、これを参考にそれぞれの人材育成に活用していってはどうか。**

職種コード	職種	専門分野	解説
HS-030-010	セキュリティアドミニストレータ	情報セキュリティアドミニストレータ	【ミッション】 全社の情報資産へのセキュリティにおける社内外からの脅威やリスクへの対応に責任を持ち、特に情報セキュリティ戦略やポリシー・ルール策定等を推進する。 【活動内容】 ・セキュリティ方針の策定・セキュリティ基準の策定・セキュリティの分析・セキュリティの見直し ●事業戦略策定 ・情報セキュリティ戦略の策定 ●セキュリティ ・セキュリティ方針の策定 ※平成24年度に「情報セキュリティ人材の育成指標等の策定事業」（経済産業省）によって検討されたスキル標準等の見直し案の方針を受けて作成した UISS視点の人材モデル。
HS-040-010	セキュリティアドミニストレータ	ISセキュリティアドミニストレータ	【ミッション】 全社の情報資産へのセキュリティにおける社内外からの脅威やリスクへの対応に責任を持ち、特にIS戦略と情報セキュリティ戦略との相互連携を図る。情報セキュリティ戦略やポリシーを企画・計画に落とし込み、実装（ないしはその指示）・提供・維持・管理を行う。 【活動内容】 セキュリティの活動領域として以下を実施する。 ● IT基盤構築・維持・管理 ・品質統制フレームワークの運営　（各プロジェクトに対するガバナンスの実施） ・ IS導入計画の策定 ●セキュリティ ・セキュリティ基準の策定 ・セキュリティ事故と対応の分析 ・セキュリティ対応の見直し ※平成24年度に「情報セキュリティ人材の育成指標等の策定事業」（経済産業省）によって検討されたスキル標準等の見直し案の方針を受けて作成した UISS視点の人材モデル。
HS-050-010	セキュリティアドミニストレータ	インシデントハンドラ	【ミッション】 全社の情報資産へのセキュリティにおける社内外からの脅威やリスクへの対応に責任を持ち、特に情報セキュリティインシデントについて、インシデントの発生を検知・受付し、適切に判断・対応することで、被害を極少化する。 【活動内容】 セキュリティの活動領域として以下を実施する。 ●IS運用 ・セキュリティ管理 ※平成24年度に「情報セキュリティ人材の育成指標等の策定事業」（経済産業省）によって検討されたスキル標準等の見直し案の方針を受けて作成した UISS視点の人材モデル。

「職種×スキル対応表」には、職種・専門分野別に求められるスキルが詳しく定義されており、育成の参考にすることができるようになっている。

コード	スキルカテゴリ	スキル分類	スキル項目	ITSS	情報セキュリティ人材					
				ITスペシャリスト	コンサルタント	ITアーキテクト	セキュリティアドミニストレータ	ISセキュリティアドミニストレータ	インシデントハンドラ	セキュリティマネージャ
				セキュリティ	情報リスクマネジメント	セキュリティアーキテクチャ	情報セキュリティアドミニストレータ	ISセキュリティアドミニストレータ	インシデントハンドラ	組込みセキュリティ
				HI-060-060	HS-010-010	HS-020-010	HS-030-010	HS-040-010	HS-050-010	HS-060-010
S110060010	メソドロジ	（戦略）　システム戦略立案手法	システム化戦略手法		◎	◎		◎		
S110060020			システム活用促進・評価		◎	◎		◎		
S110060070			情報システム戦略		◎	◎		◎		
S120010020			システム企画立案手法		◎	◎		◎		
S120030010		（企画）　要求分析手法	要求の抽出手法			◎				
S120030020			要求の整理手法							
S120030030			要求の仕様化手法			◎				
S120030040			要求の評価手法			◎				
S120030050			要件定義			◎				
S120040010		（企画）　非機能要件設定手法	プラットフォーム要件定義手			◎				
S130010010		（実装）　アーキテクチャ設計手法	アーキテクチャ設計手法			◎				◎
S130010020			アプリケーションアーキテク			◎				
S130010030			インダストリパッケージ設計・開			◎				
S130010040			インフラストラクチャアーキテクチャ設計			◎				◎
S130010050			データアーキテクチャ設計手法			◎				
S150010030			検査のマネジメント手法	◎		◎				
S150010040			品質マネジメント手法	◎		◎		◎		
S150010050			品質マネジメントシステム構築手法			◎		◎		
S150010070			品質管理に関する手法	◎		◎				
S150010090			品質保証に関する手法	◎		◎		◎		
S150010100			品質測定・評価手法	◎		◎				
S150030020			情報セキュリティ管理手法		◎	◎	◎	◎		

例）ISセキュリティアドミニストレータ想定スキル

出典：IPA情報セキュリティ強化対応スキル指標より抜粋

「新・情報セキュリティ人材育成プログラム」の進捗状況について

■ 企業等の経営戦略の一部としての情報セキュリティ対策の推進に係る施策

○上場企業におけるサイバー攻撃によるインシデントの可能性等について、事業等のリスクとして投資家に開示することの可能性に係る調査（現在NISCで委託調査を検討中）

・2011年10月に米国証券取引委員会（SEC）は、サイバーセキュリティに関するリスクを年次報告書「FORM10-K（外国企業の場合はFORM20-F）」に記述することを示したガイドラインを発行した。

・開示のあり方については、SECや証券監督者国際機構（IOSCO）等でも引き続き検討が行われているところ。

・我が国の企業においても、米国でも上場している企業を始めとして、サイバーセキュリティに関するリスクを有価証券報告書に記載する例が増加している。

・NISCにおいて、日経平均株価225銘柄から任意に数十社をサンプル抽出し、有価証券報告書の「事業等のリスク」の記載状況を調べたところ、多くの企業でサイバーセキュリティに関するリスクが記載されていた。また、金融やインフラ事業者は記載している企業が多く、繊維、製紙等素材産業では記載している企業が少ない傾向にあるとの仮説を得た。

・今後、有価証券報告書におけるリスクの記載状況をもう少し詳細に調査・分析し、経営戦略の一部として認識・対策が進むよう検討していく。

「新・情報セキュリティ人材育成プログラム」の進捗状況について

■ 産学が連携した人材育成の取組

○情報セキュリティ人材の育成に向け、企業と連携して寄付講座や大学院プログラム等を開設する大学も出始めている。（各大学の報道発表資料等をもとにNISC調べ）

【情報セキュリティ大学院大学】
株式会社NTTドコモ、NTTナレッジ・スクウェア株式会社が運営する大規模公開オンライン講座（MOOC）提供サイト「gacco（ガッコ）」において、NTTセキュアプラットフォーム研究所が制作協力して、情報セキュリティの基礎技術となる暗号技術、システムやネットワークのセキュリティ技術、さらに、それらを取り巻く法制度まで情報セキュリティの全体を幅広く学べる入門講座である「情報セキュリティ『超』入門」を開講予定。

【東京電機大学】
サイバーセキュリティ技術領域のみの教育でなく、法律・経済・外交・心理・倫理等の知識も有し、経営、監査等も先導可能な高度サイバーセキュリティ専門家の育成を目指した「国際化サイバーセキュリティ特別コース」を設立（平成26年度文部科学省「高度人材養成のための社会人学び直し大学院プログラム」）。

【北陸先端科学技術大学院大学】
日本電気株式会社（NEC）と連携し、サイバーセキュリティ人材を育成するためのサイバーレンジ（サイバー空間の演習場）を構築する技術を研究開発するとともに、これを用いた教育プログラム（演習環境、教材、カリキュラム）の設計および開発を行なう寄付講座を開設。

【早稲田大学】
日本電信電話株式会社（NTT）と連携し、学部学生向けに大学で実施されているコンピュータサイエンスの基礎的な知識の育成に加えて、日々高度化するサイバー攻撃の現場を踏まえ研究開発を推進しているNTTの観点からサイバー攻撃対策の土台となる教育を実施。さらに大学院では、実践的な演習を交えた教育を通じて新たなサイバー攻撃対策手法を創出できる傑出した人材を発掘・育成する寄付講座を開設。