資料４

平成２９年度　企業において育成すべき人材の知識・スキル及びカリキュラムに関する調査（中間報告）

平成２９年１２月

調査の概要

１．事業名

平成29年度企業において育成すべき人材の知識・スキル及びカリキュラムに関する調査

２．調査時期

平成29年11月～平成30年３月

３．調査内容

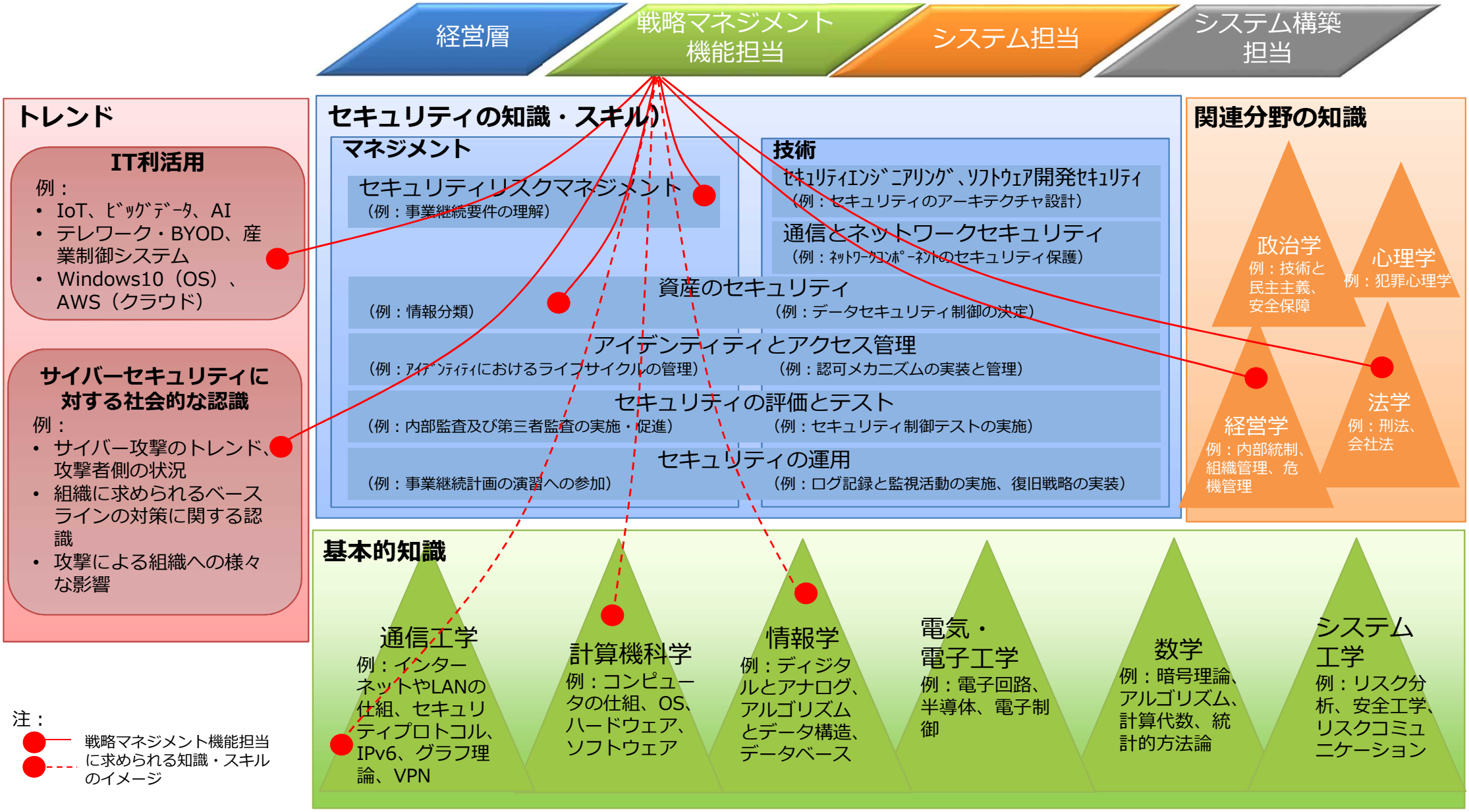
サイバーセキュリティ人材育成について、以下4点を明確化する

(1) 企業内のサイバーセキュリティに関する組織体制
(2) 組織体制における、各層の役割・人材像
(3) 必要とされる知識・スキル
(4) 知識・スキルを習得するための、モデルとなるカリキュラム

４．進め方

(1) 文献調査（国内及び米国、欧州等）による情報収集・分析及び仮説の作成
(2) 仮説を基にしたヒアリング調査（10以上の企業）
(3) サイバーセキュリティ戦略本部及び関連会合（普及啓発・人材育成専門調査会、施策間連携ＷＧなど）等における有識者の議論の把握、整合性の確保

カリキュラムの考え方（イメージ･再掲）



「戦略マネジメント機能」に相当する人材層に期待される知識・スキル（調査結果）

「戦略マネジメント機能担当」に相当する人材層に期待される知識・スキルは、技術系にとどまらず、ビジネス系、社会系、人間系などに拡がっている。ただし、米国では技術系以外について、日本よりも幅広い知識・スキルを持つことが期待されている。

記号凡例（必要な知識・スキル／教育内容）◎＝高度、○＝中間、△＝初級、－＝不要、？＝不明			国内事例				米国事例※		
			産業横断「システム企画」担当職	ITSS+「情報リスクストラテジ」	ITSS+「情報セキュリティデザイン」	情セ大報告書例示⑤「単独科目」	NICE "Program Manager"	ブラウン大学エグゼクティブMBAプログラム	MIT Sloanスクール MBAプログラム
技術系	IT	システム構築	◎	－	◎	－	○	－	？
		運用・保守	－	－	－	○	△	－	？
		ハード・ソフト	？	－	－	－	○	－	？
		ネットワーク	◎	－	○	－	○	－	◎
		セキュリティ	◎	○	◎	○	◎	◎	◎
	OT（安全管理、プラント運用等）		－	－	－	－	△	－	？
	基礎	情報学・コンピュータ科学	？	？	？	－	－	－	◎
		工学基礎	？	？	？	－	－	－	◎
ビジネス系	マネジメント	プロジェクト	○	－	－	－	○	－	◎
		セキュリティ	○	◎	◎	△	◎	◎	◎
		クライシス	○	－	○	△	－	－	◎
		リスクセンス	？	？	？	？	○	◎	◎
	ガバナンス		◎	◎	○	－	○	◎	◎
	戦略	コンセプト	－	－	－	－	－	？	◎
		企画	◎＊	◎＊	◎＊	－	○	◎	◎
	ファイナンス		？	○	－	－	○	－	◎
社会系	国際関係		？	？	？	－	△	◎	◎
	経済学		？	？	？	－	－	－	◎
	法学		？	○	○	△	○	◎	◎
人間系	心理学・行動科学		？	？	？	－	－	◎	◎
	倫理		？	○	－	－	○	◎	◎
トレンド			？	○	○	－	○	◎	◎

＊：システム系の戦略・企画に限定

※：このほかカーネギーメロン大学について調査中

サイバーセキュリティ人材育成の取組に関する我が国における人材像の定義とカリキュラム（仮説）

「システム担当」「システム構築担当」といったいわゆるITエンジニアに相当するセキュリティ人材については、既に国内でもカリキュラムを含めて整理されているが、「戦略マネジメント機能担当」についてはそのような人材を端的にターゲットにするようなカリキュラムが存在しない。一方、米国では、MBAプログラムにおけるサイバーセキュリティコースをはじめとして具体的なカリキュラムが存在する。また、カリキュラムの内容も、単なる教科書的な「知識の詰め込み」ではなく、ビジネスにおいてサイバーセキュリティをどうフレーミングするのかの議論や、ケースに基づく意思決定の議論など、発想や意思決定における「考え方」に重きが置かれている。

人材分類	日本		米国	
	人材像等の定義例	カリキュラム例	人材像等の定義例	カリキュラム例
戦略マネジメント機能担当	● 産業横断検討会（第２期にて検討中） ● ITSS+（情報リスクストラテジ）	事例無し ● （IPA産業サイバーセキュリティセンター 中核人材育成プログラム？）	● NICE人材フレームワーク（プログラムマネージャ）	● MBAプログラムにおけるサイバーセキュリティコース
システム担当	● 産業横断検討会 ● SecBoK ● ITSS+（情報セキュリティアドミニストレーション等）	● 情セ大モデル・コア・カリキュラム ● enPiT 1/2/Pro ● 情報処理学会J07/J17 ● 情報処理安全確保支援士シラバス	● NICE人材フレームワーク（システムアドミニストレーション、システムアナリシス等）	● SANSコース(Managing Security Operations: Detection, Response, and Intelligence等） ● 大学等におけるインフォメーションシステム系プログラムにおける各種コース等
システム構築担当	● 産業横断検討会 ● SecBoK ● ITSS+（セキュア開発管理）	● 情セ大モデル・コア・カリキュラム ● enPiT 1/2/Pro ● 情報処理学会J07/J17 ● 情報処理安全確保支援士シラバス	● NICE人材フレームワーク（システムアーキテクチャ、ソフトウェアデベロップメント等）	● SANSコース(Web Application Pentesting Hands-On Immersion等） ● 大学等におけるソフトウェアエンジニアリング系プログラムにおける各種コース等

調査事例①（ITSS+で定義される専門分野「情報リスクストラテジ」）

専門分野名	**情報リスクストラテジ**	想定業務	経営課題
		レベル範囲	レベル４～７
定義	自組織または受託先における業務遂行の妨げとなる情報リスクを認識し、その影響を抑制するための、組織体制の整備や各種ルール整備等を含む情報セキュリティ戦略やポリシーの策定等を推進する。自組織または受託先内の情報セキュリティ対策関連業務全体を俯瞰し、アウトソース等を含むリソース配分の判断・決定を行う。		
必要な知識・スキル（抜粋）	IT系	・セキュリティの基礎技術（情報保証、セキュリティアーキテクチャ、プラットフォームセキュリティ、暗号技術、保証・信用・信頼のメカニズム）に関する知識・スキル ・セキュリティの構築技術（方針・基準・計画の策定、要件定義、情報セキュリティ管理、情報セキュリティ分析、セキュリティの見直し）に関する知識・スキル ・システム企画立案手法、ソリューション提案手法に関する知識・スキル ・ソフトウェアエンジニアリング手法（セキュリティ実装、セキュリティ品質）に関する知識・スキル ・サポートセンター基盤技術（インシデント管理システム等）に関する知識・スキル	
	ビジネス系	・市場機会の評価と選定（ビジネス環境分析、経営管理システム、経営戦略手法）に関する知識・スキル ・システム戦略立案手法（システム活用推進・評価、業務プロセス、事業戦略・分析、情報システム戦略）に関する知識・スキル ・コンサルティング手法に関する知識・スキル ・業務動向把握手法に関する知識・スキル ・リスクマネジメント手法に関する知識・スキル ・ITガバナンス、内部統制に関する知識・スキル ・事業継続計画（BCP策定、災害対策管理）に関する知識・スキル ・チェンジマネジメント手法（協働の管理、ビジネスソリューション変更管理、業界固有の要件・事例）に関する知識・スキル ・システムアーキテクティング技術（システム要件定義、障害時運用方式、災害対策）に関する知識・スキル ・ビジネスインダストリ（エンジニアリングシステム、ビジネスシステム、産業機器、民生機器）に関する知識・スキル ・企業活動（経営・組織論、会計・財務、情報セキュリティ監査、ビジネスプロセスマネジメント）に関する知識・スキル ・標準化に関する知識・スキル	
	社会系人間系	・技術者の社会的責任と倫理に関する知識 ・情報倫理に関する知識 ・セキュリティ関連法規及びその他の法律・ガイドライン・技術者倫理に関する知識・スキル	

調査事例②（NICEで定義される役割「プログラムマネージャー」）

役割名	**プログラムマネージャー** **Program Manager**	カテゴリ	監督・統制
		専門領域	調達及びプログラム/プロジェクトの管理
定義	プログラムの主導、調整、コミュニケーション、統合を担い、全体の責任を負う。機関や企業における優先度との整合性を確保する。		
必要な知識・スキル（抜粋）	IT系	• コンピュータネットワークのコンセプトとプロトコル、及びネットワークセキュリティ手法に関する知識 • サイバーセキュリティとプライバシーの原理に関する知識 • サイバー脅威と脆弱性に関する知識 • 情報技術のアーキテクチャコンセプトとフレームワークに関する知識 • ソフトウェアのセキュリティとユーザビリティを含む、システムライフサイクルマネジメントの原理に関する知識 • セキュリティ、ガバナンス、調達及び管理に関するクラウドベースのナレッジマネジメント技術とコンセプトに関する知識	
	ビジネス系	• リスクマネジメントプロセスに関する知識、リスクマネジメントフレームワークの要件に関する知識 • サイバーセキュリティの失効がもたらす運用上のインパクトの特定に関する知識 • リソースマネジメントの原理と技法に関する知識 • 組織のエンタープライズITのゴールと目的に関する知識 • サプライチェーンのリスクマネジメントに関する実践（NIST SP 800-161）に関する知識 • 組織のコアビジネスとミッションのプロセスに関する知識 • IT調達要件に関する知識 • システムの目標に関して、システムパフォーマンスの手段や指標、及びパフォーマンスの向上または是正に必要となるアクションの特定に関するスキル • 連携先を含む企業全体にわたって情報に関するニーズとインテリジェンスの収集要件を解釈、追跡及び優先順位づけるスキル • サプライチェーンのリスクマネジメント標準の適用に関する能力 • 開発を監督し、ライフサイクルコストの見積を更新する能力 • 供給者及び/又は製品の信頼性を評価/確保する能力 • 調達プロセスを通じてセキュリティが確実に実践されるようにする能力	
	社会系 人間系	• サイバーセキュリティとプライバシーに関連する、法律、規制、方針及び倫理に関する知識 • 暗号及びその他のセキュリティ技術に関する輸出入規制に関する知識	

調査事例③（MITスローンスクールMBA科目「サイバーセキュリティ」）

大学名等	MIT（マサチューセッツ工科大学）スローンスクールMBAコース	
科目名	**サイバーセキュリティ**（2017年春期開講、12週）	
概要	サイバーセキュリティに関する総合的なアプローチを提供する。脅威、運用及び影響の原因と挙動に焦点を置くとともに、技術、経済、政治及び戦略の観点からのソリューション戦略を扱う。	
講義テーマ（同大学シラバスより抜粋）	**パート1：コンテクスト、コンセプト、論点**（サイバーセキュリティの概要を示す。多面的な視点から、脅威、意図、能力、不確実性を含む多様性にフォーカスする。）	
	1 導入＝コンテクスト、意味、インパクト、不確実性	脅威としてのサイバーセキュリティに関するフレーミング
	2 新しいグローバルチャレンジ＝我々は何を知っていて、何を知らないか	グローバルな変化と新たなルール、サイバー環境と実環境との相違
	3 サイバースペース＝インターネットアーキテクチャとセキュリティの複雑性	レイヤー毎の官民アクターの行動を含むアーキテクチャのレビュー
	4 サイバー脅威を扱う国際機関	FIRST, IMPACT, ITUなどの国際機関の役割と課題
	パート2：比較展望－場面と条件（サイバーセキュリティの地政学、政治学及び経済学的な「実態」について説明する。新興の活動にともなう新しいマーケットに関する内容を含む。ケーススタディ、データとその測定、関係者とその損得について考察する。）	
	5 ナショナルセキュリティ＝サイバー脅威とサイバー戦争の可能性	国家安全保障におけるサイバーセキュリティの位置付け
	6 障害ポイントと制御範囲	ケーススタディによる制御ポイントの分析
	7 サイバーセキュリティに関する保険と他の原則	サイバーセキュリティに関する対策と保険による保護、その可能性と課題
	8 サイバーセキュリティにおける経営の役割：TJXの事例におけるサイバーセーフティ分析	新規事業による新たなサイバーセキュリティ上の脅威とその対処についての事例毎の分析
	パート3：政策対応＝戦略と意味（国内・国際的な方針について、変化し続けるサイバーエコロジーにおける代替ソリューション戦略を含めて、公式・非公式の内容を扱う。）	
	9 方針と予想＝コンピュータサイエンスからの視点	コンピュータサイエンスの観点に基づくツール、プロセス、意思決定
	10 マルウェアと脆弱性に関する市場	マルウェアに関する市場、アクターと収益構造
	11 組織のサイバーセキュリティ文化の役割についての理解	メトリクス、サービス、アクター、関心を踏まえたサイバーセキュリティ政策
	12 もうひとつの未来：次は何か？	地政学、国際政治学等を踏まえたインターネットとサイバー領域

今後の予定

1. 企業ヒアリング調査

- 文献調査及び本WGの議論をもとに、適切と考えられる国内企業（10社程度）を選定の上、サイバーセキュリティに関する役割の設定と任用、育成の取組等について聴き取り調査を行う。
- 調査対象企業は以下の２類型の双方を含むように選定する。

  類型１：ITが事業の柱であり、IT戦略が事業の成否そのものに関わってくる企業
  （例：金融、情報通信、新電力、ネット系サービス等）

  類型２：ITを使ってはいるが、それが事業の中核にはなっていない業界の企業
  （例：製造業、建設業等）

2. 結果のとりまとめ

- 文献調査及び企業ヒアリング調査、本WGをはじめとする関連会議等での議論の結果を踏まえ、以下の４点について今後の政策に資するようとりまとめを行う。
  ① 企業内のサイバーセキュリティに関する組織体制
  ② 組織体制における、各層の役割、人材像
  ③ 必要とされる知識・スキル
  ④ 知識・スキルを習得するための、モデルとなるカリキュラム