資料３－４

サイバーセキュリティ人材の育成に関する施策間連携ワーキンググループ
報告書
～「戦略マネジメント層」の育成・定着に向けて～

平成 30 年 5 月 31 日

サイバーセキュリティ人材の育成に関する施策間連携ワーキンググループ

目次

１　はじめに

（１）　経緯

これまで、内閣サイバーセキュリティセンター（NISC）では、「サイバーセキュリティ戦略」（平成 27 年９月閣議決定）を踏まえ、サイバーセキュリティ人材の需要（雇用）と供給（教育）を相応させ、好循環の形成を推進してきている。

具体的には、同戦略を踏まえ、サイバーセキュリティ戦略本部において「サイバーセキュリティ人材育成プログラム」（平成 29 年４月）を策定し、これまでにも各省庁において様々な施策が実施されているところ、個々の施策間の連携を強化することにより、より効果的な実施を図れたり、セキュリティ教育に関わる有限なリソースを効率的に活用できたりする可能性があるため、人材育成のモデルとなるカリキュラムの策定を含む、施策間連携の強化に取り組むことを示した。

また、「2020 年及びその後を見据えたサイバーセキュリティの在り方について－サイバーセキュリティ戦略中間レビュー－」（平成 29 年７月）を決定し、「サイバーセキュリティ人材育成プログラム」の内容のうち、急ぎ対応が必要と考えられる具体的な施策として、サイバーセキュリティにおける各人材層のモデル・カリキュラムの策定、人材育成に関する施策間の連携の取組を進めることを提示した。

こうした経緯を踏まえつつ、昨年６月、次期「サイバーセキュリティ戦略」の策定を念頭に、上記事項について本ワーキンググループでの検討を開始した。

（２）　本報告書の趣旨・位置づけ

本報告書は、本ワーキンググループで３回（平成 29 年６月、平成 29 年９月、平成 29 年 12 月）にわたり、以下の５つの内容を中心に検討を行った内容を取りまとめたものである。

① 企業において育成すべき各層別の人材像やキャリアパスの明確化
② セキュリティ人材育成の前提となる IT の基本的知識を明らかにするとともに、それを踏まえた各層別のカリキュラム（短期・中長期）の方向性を提示
③ 各層別のカリキュラムを意識した各省の人材育成施策に関する全体像を整理し、連携策の検討を推進
④ カリキュラムに基づく教材について、R&D を推進
⑤ 人材育成・確保に向けた産学官連携の在り方・具体的方策の明確化

なお、議論の過程においては、企業法制を反映した内容の整理をすべきとの意見もあっ

たが、企業の機関設計や機能分担は多様で変化しつつあり、サイバーセキュリティとの関連づけはなお考察を要することから、本報告書の記載については、企業におけるサイバーセキュリティ人材が担うべき機能を一般化して論じるものとする。

　また、本報告書の内容を踏まえ、「次期サイバーセキュリティ戦略」の関係する部分についての検討を深めていくこととする。

2　各層の役割・人材像

組織におけるサイバーセキュリティに関わる人材には、様々な役割の人材が存在し、一括りにすることは困難である。このため、企業等の組織内におけるサイバーセキュリティに関する体制のモデルを想定し、人材層に分けて検討を行った。

（1）　当初想定していた体制のモデル

各層の役割・人材像の検討において、当初想定していた企業等の組織におけるサイバーセキュリティに関する体制のモデルを次図に示す。

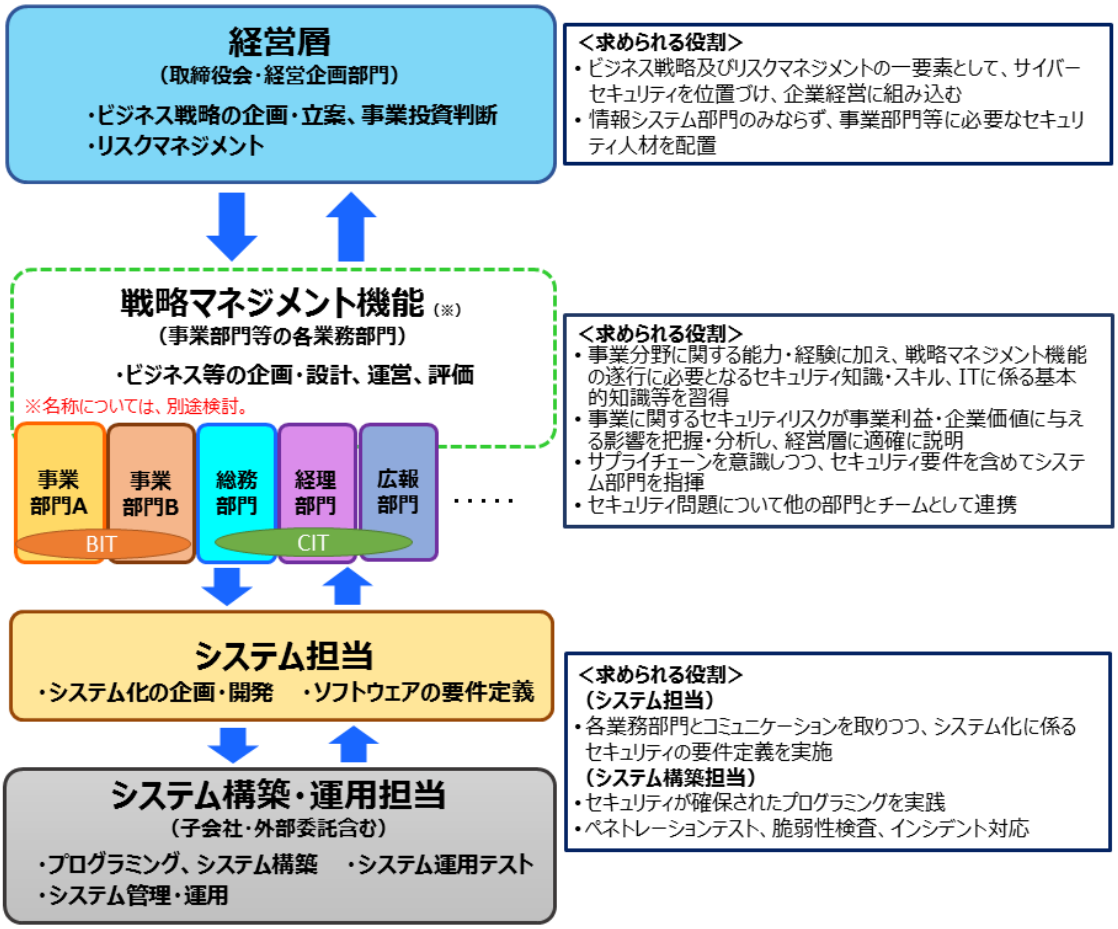


図１：想定する組織内の体制モデル

BIT：ビジネス IT、CIT：コーポレート IT

（2）　体制の検討

体制の検討に当たっては、

ａ　『産業横断サイバーセキュリティ人材育成検討会　第二期中間報告書』（産業横断サイバーセキュリティ人材育成検討会、2017 年 11 月）

b 『Cybersecurity Framework』（NIST、2014 年 2 月）

を参考とした。

a 産業横断サイバーセキュリティ人材育成検討会 第二期中間報告書

『産業横断サイバーセキュリティ人材育成検討会 第二期中間報告書』では、人材定義として、ゼネラリスト、エキスパート、スペシャリストの 3 類型に分類をしている。ゼネラリストは企業におけるラインマネジメントを行う人材であり、管理職となっていくキャリアパスが想定されている。これに対し、スペシャリストは専門的技術を持った人材であり、IT やセキュリティベンダー、情報子会社のキャリアパスが想定されている。その間にエキスパートという人材層が位置付けられており、自社事業とセキュリティ活動をよく知り、現場と経営をつなぐ人材であり、技術系企業の技師や技術職などのキャリアパスに類似するとしている。

図２：人材定義リファレンスに対する「エキスパート」の関係

出典：「産業横断サイバーセキュリティ人材育成検討会」 第二期中間報告書

また、同報告書において、セキュリティ人材のキャリアパスの検討に際して、「IT と事業の関係性」をもとに次の類型化を行っている。「IT ビジネス企業」においてはビジネス戦略の中核

において IT システム開発を伴うことが多く、DevOps[1]あるいは DevSecOps[2]などと呼ばれるように開発と運用とセキュリティ対策がサイクル的・同時並行的に行われていることが一般的である。その結果、こうした企業においては、セキュリティ人材のキャリアパスは、人事制度の中で確立されている可能性が高く、「伝統的な企業」におけるセキュリティ人材のキャリアパスとは大きく異なると想定されている。

表１：ユーザー企業の類型

IT ビジネス企業	ビジネス自体がインターネット上にある企業、または、IT を駆使してビジネスを行う企業 ● 業界：E-コマース、金融、各種クラウドサービス事業者等 ● サイバーセキュリティがビジネスに直結していることに自覚的であり、サイバーセキュリティに関して経営層の理解も高い。
伝統的な企業	ものづくり的な部分がビジネスの根幹である企業 ● 業界：電力、ガス、水道、石油、化学、自動車、航空、鉄道、その他製造メーカ等（多くの重要インフラ関連企業が含まれる。） ● 情報だけでなく、物理的なプラントや人などの安全（セーフティ）も含めたセキュリティ[3]。 ● サイバーセキュリティの重要性を認識しつつも、その優先度は必ずしも高くない。

※産業横断サイバーセキュリティ人材育成検討会　第二期中間報告書を参考に内閣サイバーセキュリティセンター作成

b　米国 NIST　Cybersecurity Framework

『Cybersecurity　Framework』は、重要インフラ事業者を主たる対象とし、サイバーセキュリティリスクを企業のリスクマネジメントプロセスの一つとして扱えるようにするためのフレームワークとして、米国 NIST が 2014 年 2 月に公表したものである。本フレームワークに示されている「企業内の情報と意思決定の流れ」によれば、①経営レベル、②ビジネス/プロセスレ

---

[1] Development（開発）、Operations（運用）を組合せた用語

[2] Development（開発）、Security（セキュリティ）、Operations（運用）を組合せた用語

[3] 物理的なプラント等における IT 化の進展により、サイバーセキュリティの問題が保安の問題につながるようなケースを想定

ベル、③実施/運用レベル、の情報と意思決定の流れがあるとされており、それぞれ、本検討において当初想定した①経営層、②戦略マネジメント機能、③システム担当及びシステム構築・運用担当、に相当するものと考えられる。

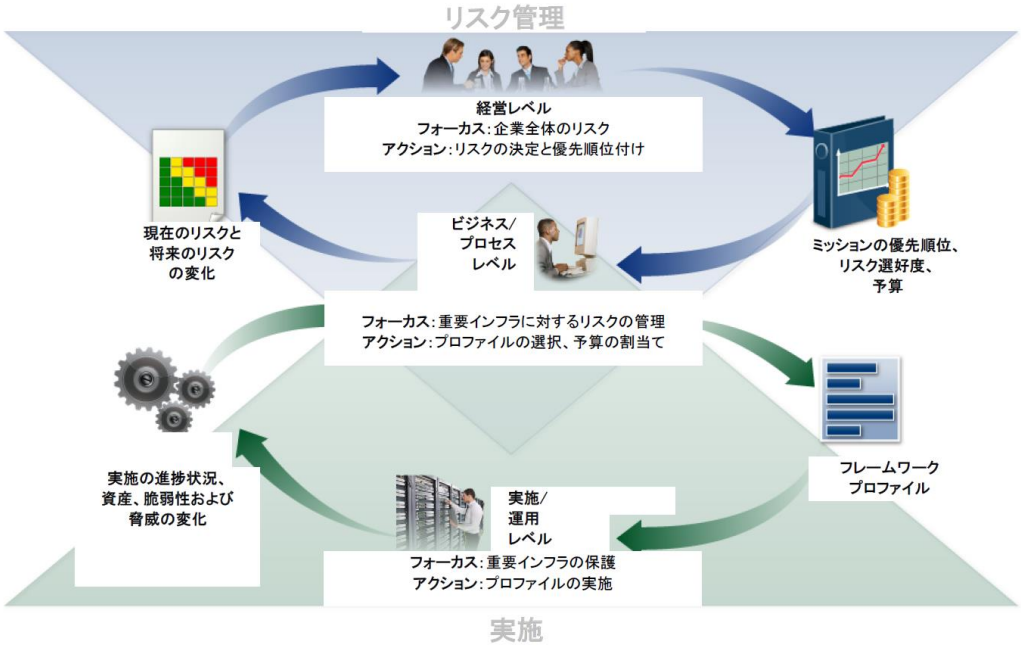


図３：NIST サイバーセキュリティフレームワークにおける企業内の情報と意思決定の流れ（概念図）

（３） 各層別の役割とキャリアパス

上記（２）を踏まえ、表１に示したユーザー企業の類型によって各層に求められる人材像が若干異なる可能性があることに留意する必要があるが、本検討においては、典型的なモデルとして、（１）で示した体制モデルを念頭に、

- 経営層
- 戦略マネジメント層
- 実務者層・技術者層（システム担当・システム構築担当を想定）

の３層で整理を行うこととする。その際には、「人」ではなく「機能」に着目して整理を行うこととする。

なお、経営層については、別途、セキュリティマインドを持った企業経営ＷＧにて検討を行ったため、本報告書については、その他の２層（戦略マネジメント層、実務者層・技術者層）についての検討について扱うものとする。

表１のうち、一般的に、IT ビジネス企業は、先端的な情報通信技術を積極的に取り入

れ、新たな価値創出を図ることが主なミッションとなっている。一方、伝統的な企業は、企業における基幹システムなどを円滑に運用し、事業継続を確保することが主なミッションとなる。近年の企業活動は多様化しているため、厳密に分類することは困難な場合もあるが、ここでの役割の想定については、IT ビジネス企業だけでなく、伝統的な企業についても対象として想定している。

a　戦略マネジメント層

＜求められる役割＞

1．通常時

① 経営戦略、事業戦略におけるサイバーセキュリティリスクを認識し、事業継続と価値創出に係るリスクマネジメントを中心となって支える役割を担う

② マネジメントの範囲におけるサイバーセキュリティリスクを認識し、そのリスクに対し、経営層の方針を踏まえた対策を立案、様々な役割を担う実務者・技術者を指揮し、経営者に報告する役割を担う

（具体的な役割のイメージ）
- ・事業影響が生じるサイバーセキュリティリスクの洗い出しの指示
- ・適切なセキュリティ対策への予算配分と対策の承認
- ・ベンダーの選定の判断
- ・外部委託先との契約時におけるセキュリティ対策の確認
- ・法令・諸制度対応の確認
- ・セキュリティルールの策定指示、確認
- ・事業継続や価値創出に関わるセキュリティ対策の状況や課題・対応策を経営層にわかりやすく報告

2．緊急時対応

① インシデントの事業影響についての推定

　システム担当等との情報共有をもとに、発生したインシデントの経営・事業に対する影響範囲と影響の内容について推定を行う

② 対策の立案、経営層への報告・協議、実務者層・技術者層の指揮

　経営・事業に対する影響を考慮しつつ、インシデントへの対応案を作成し、経営層による判断を支援するとともに、実務者層・技術者層を指揮し、対処の中核を担う

なお、戦略マネジメント層は、必ずしも一人でこれらの役割を担うことを想定しているわけではなく、経営戦略・事業戦略の遂行に向けて取り組む人材が、必要であればチームとなって上記に掲げる機能を全うすることを想定している。

＜想定されるキャリアパス＞

「戦略マネジメント層」を担う人材については、経営企画部門や事業部門等のマネジメントラインにおいて、キャリアパスを歩み、現時点でそれらの部門におけるマネジメントに携わっている人材を想定している。そういった人材が、様々な課題に対するマネジメントを行う中の一つの要素として、サイバーセキュリティ関連のリスクに起因する経営・事業上の脅威に対するマネジメントも行うことが期待される。なお、（一般的に伝統的な企業によく見られる傾向として、）事業部門等を含めたサイバーセキュリティのマネジメントに関し、IT 部門（情報システム部門）やリスクマネジメント部門が一括して担当するケースがある。その場合においては、少なくとも経営企画部門や各事業部門との緊密な連携・コミュニケーションや、それらの部門に対するガバナンスの確保が必要である。さらに、IT 部門（情報システム部門）やリスクマネジメント部門の当該人材は、その部門のみの経験ではなく、経営企画部門や事業部門の経験を有していることが望ましい。

b　実務者層・技術者層

システム企画や管理、構築、セキュリティの専門サービスを担う人材の役割等について、ユーザー企業は、産業横断サイバーセキュリティ人材育成検討会の第 1 期報告書等（別紙の参考 1 を参照）で、また、ベンダー企業は IPA（ITSS+）（別紙の参考 2 ）で過去に定義されたものがある。基本的にはそれらを参照することができるが、ここでは、戦略マネジメント層との関係で役割を記載することとする。

＜求められる役割＞

1．通常時

戦略マネジメント層の示す方針を踏まえ、システムの企画や管理、システム構築を担う立場として、サイバーセキュリティのリスクマネジメントを実践する役割を担う。具体的には、システムに関わるサイバーセキュリティリスクを把握し、セキュリティ対策（技術的な対策及びマネジメント策）を企画・構築・実施（管理・運用）する。その際、必要に応じて外部の業者に委託を行うことがあり、契約書の作成や履行確認などを行う。また、脆弱性に関わる情報等サイバーセキュリティ対策を行うために必要な情報を収集し、情報システムがサイバー攻撃

によって悪影響を受けないよう必要な対策を講じる。さらに、戦略マネジメント層に対して、リスクやセキュリティ対策など、サイバーセキュリティの実践に関わる内容について、説明を行うことが必要である。このため、戦略マネジメント層の示す方針を理解して取り組むことが期待される。

2. 緊急時対応

戦略マネジメント層の指揮の下、発生したインシデントのシステムに関わる影響範囲を特定する。また、インシデントに対するシステム面での技術的な対応案を作成し、戦略マネジメント層の指示の下で、外部ベンダーなどの外部関係者等も必要に応じて活用しつつ、関係者との連絡、調整や技術的な対処を実施する。

なお、上記に示したこれらの役割は、企業の IT 活用状況、業種、規模によって若干変わってくることに注意すべきである。

また、実務者層・技術者層については、当該人材層に期待される機能を、経営戦略・事業戦略の観点から、他の専門人材と円滑にコミュニケーションをとりながら最も効果的・効率的にチームの一員として実践できることが重要であり、社内において人材を確保して育成する場合と、外部の事業者に属する専門人材を活用する場合の双方について、企業環境に適した人材育成・確保に向けた検討が必要である。

＜想定されるキャリアパス＞

実務者層・技術者層を担う人材については、いわゆるユーザー系の企業において社内で人材を確保する場合、一般的には次のようなキャリアパスが想定される。

1. 情報システム部門内での実践等を通じたスキル向上

情報システム部門内での OJT や、各種資格試験等の取得を通じて、業務に必要となるサイバーセキュリティ関連の知識・スキルを向上させていくキャリアパスである。自社内であまり経験する機会がなく、スキル向上が図りにくい分野については、外部の研修やトレーニング等を活用することも必要となる。

2. 情報システムベンダーや情報セキュリティサービスベンダーで経験を積んだ人材

ベンダーの立場で経験を積んだ上でユーザー企業に活躍の場を移すキャリアパスである。現状では国内において専門性の高い人材がベンダーに偏る傾向があり、こうしたキャリアパス

を経ている人材は少ないが、ユーザー企業における専門人材の必要性が意識されることで、今後、こうしたキャリアパスを持つ人材の比率が高まる可能性がある。

３　各層において求められる知識・スキルとモデルカリキュラム

（１）　知識・スキルの考え方

各人材層において求められる知識・スキルを検討するに当たって、経営層から実務者層・技術者層まで、それぞれの機能を全うするために必要な能力を明らかにする必要がある。そこで、ハーバード大学のロバート・L・カッツ教授の著作であり、人材のスキルに関する古典『Skills of an Effective Administrator』（Robert L. Katz、Harvard Business Review、1974 年９月号）について調査した。同文献において、３つのスキル（「テクニカル・スキル」（業務遂行能力）、「ヒューマン・スキル」（対人関係能力）、「コンセプチュアル・スキル」（概念化能力））の３種類を示している。この学説を紹介する『管理職に求められる「マネジメント」、管理職が執るべき行動の在り方について』（管理職のマネジメント能力に関する懇談会資料、内閣府人事局、2016 年）では、3 種類のスキルはそれぞれ次表のように整理されている。

表２：人材のスキルと定義

スキル名	定義	相対的な重要性
コンセプチュアル・スキル	企業を総合的にとらえることができる能力のこと。組織の諸機能がいかに相互に依存しあっているか、またその内のどれか１つが変化したとき、どのように全体の機能に影響が及ぶかを認識することであり、個別の事業が産業、地域社会、さらには国全体の政治的、社会的、経済的な力とどのように関係しているかを明確に描けることにまで及ぶ。	最上階層において特に重要
ヒューマン・スキル	グループの一員として手際よく仕事を行い、自分の率いるチーム内で力を合わせて努力する場を作り上げることや、グループ間で関係を構築すること。他人との対応能力であるヒューマン・スキルは、どの階層においても効果的管理を行うための基本となるもの。	すべての階層において重要
テクニカル・スキル	特定の活動、特に手法、プロセス、手順、あるいはテクニックと関わり合う活動を理解し、それに熟達していること。	下位階層において特に重要

カッツは同文献において、次図のように上位階層の管理者ほど「コンセプチュアル・スキル」が占める割合が高まり、下位層の実務者、専門人材ほど「テクニカル・スキル」が重要である

ことを示している。

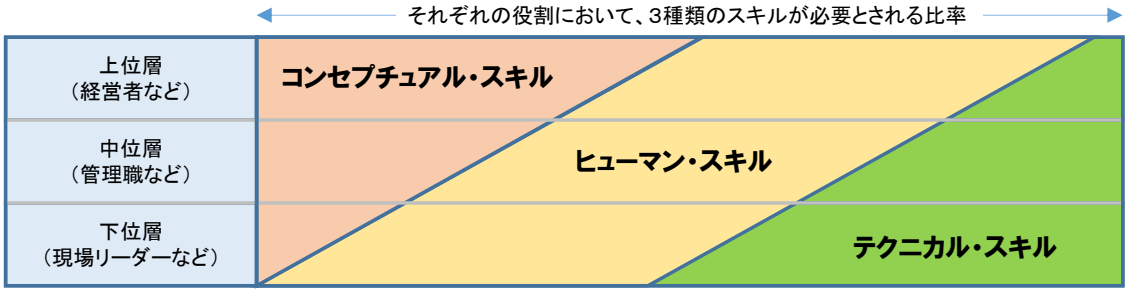


図４：管理者としての階層に応じて求められるスキルの相違

今回の検討における中核となる「戦略マネジメント層」は、このうち、中位層に位置付けられると考えられる。この層においては、経営層の視点をもってマネジメントを行い、経営層との円滑なコミュニケーションを行うために、「コンセプチュアル・スキル」が不可欠となる。一方で、現場の実務者や専門人材を動かすために「テクニカル・スキル」も求められる。

本報告書は、あくまでサイバーセキュリティ人材の知識・スキルにフォーカスをしているため、コンセプチュアルスキルやヒューマンスキルそのものの育成については論じることはなく、テクニカルスキルに特化した整理を行うこととする。特に戦略マネジメント担当においては、個別具体的なサイバーセキュリティに関する技術の詳細を身に付けるだけの時間的余裕もなく、そのような技術を活かせる役割ではないことが想定されるため、サイバーセキュリティに関するテクニカル・スキルをコンセプトとして、ないしは、コンセプチュアルスキルを発揮するのに最低限必要な形で、理解できるようにする工夫が必要である。

（２） 各層において求められる知識・スキルとモデルカリキュラム

a 戦略マネジメント層

1. 求められる知識・スキル

「戦略マネジメント層」を担う人材に相当する役割や専門分野として、比較的戦略マネジメント層に近いと考えられる人材像について定義されている内容を比較した結果を巻末の別紙の参考 4 に示す。「戦略マネジメント層」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、人間系など幅広い知識が必要であることが分かる。

また、ISO 31000:2009 が定めるリスクマネジメントプロセスや、事業戦略のためのプロセスを踏まえ、以下の図５にリスクマネジメント・事業戦略の一般的プロセス（左側）と、実体的な課題（右側）の関係を整理した。これは、企業が直面する様々な実体的課題に

関わる事業戦略とリスクマネジメントのプロセスを進めていく中で、サイバーセキュリティは、その一つの課題であることを示している。このため、サイバーセキュリティを実践するために、それに関連する必要な知識・スキルを整理するという考え方をとることにする。

このような考え方の下、戦略マネジメント層に求められるサイバーセキュリティに関連する知識・スキルを整理すると、

○事業継続を確保するためのリスクマネジメントに関しては、

① サイバーセキュリティに関するコミュニケーションや調整、実施体制とその運営に必要な知識・スキル
② サイバーセキュリティに関する法令やガイドライン、リスクマネジメントの手法に関する知識・スキル
③ サイバーセキュリティに関するリスクアセスメントを理解するために必要な知識・スキル
④ サイバーセキュリティリスクへの対応策（技術的な対応策、マネジメントによる対応策、それを提供する事業者を含む）に関する知識・スキル
⑤ サイバーセキュリティインシデントに関わる緊急時対応

が挙げられる。

また、

○新しい価値を創造するための事業戦略の推進に関しては、

① 事業に対する不正行為を想定するための知識・スキル
② セキュリティに対する顧客の期待を把握するために必要な知識・スキル
③ 事業計画において、サイバーセキュリティ投資、ランニングコスト等を適切に見積もり（費用対効果の分析などが想定される）、事業モデルに対して適切なセキュリティ対策の選定の判断に関わる知識・スキル

が挙げられる。これらの知識・スキルの分析に関する詳細については、別紙の参考４に詳細を示す。

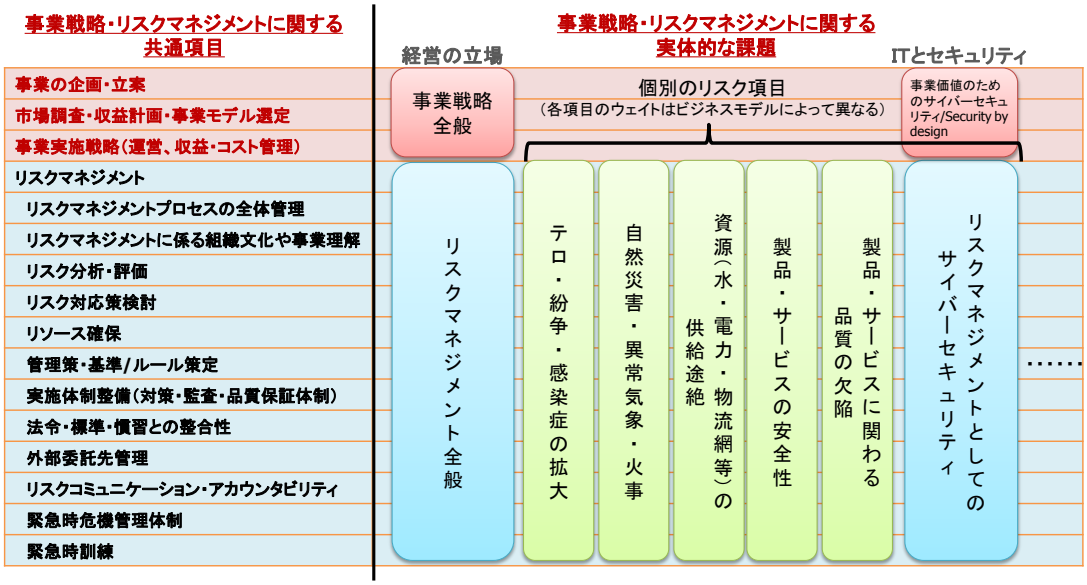


図 5：サイバーセキュリティを包含するリスクマネジメント機能の考え方

2. モデルカリキュラム

前項に示した知識・スキルを習得するためのモデルカリキュラムとして、戦略マネジメント層が受講することを想定した全 5 回のカリキュラム例を次表に示す。

表 3：戦略マネジメント層を担う人材育成のためのカリキュラム例

目的	企業等における事業戦略の企画・立案責任者が、事業戦略そのものに必要なサイバーセキュリティ対策を組み込む（例えば、セキュリティを考慮したビジネス設計や適切な外部委託）ために求められる、専門ベンダーとのコミュニケーションやリスク評価及び対応体制の構築のための知識・スキルを習得する。
前提知識・経験	企業等において事業やプロジェクトの管理経験を有する者。IT リテラシーは一般ユーザーレベルで可。企業経営に近い部署や業務の経験を有することが望ましい。

	スクーリング内容	説明	実施方法
第 1 回	サイバー空間を理解するための基礎知識 （基礎知識がある場合にはスキップしてもかまわない）	サイバーセキュリティの全体像を把握するとともに、サイバーセキュリティ上のリスクを理解するために必要となる、以下の基礎知識を理解することで、サイバーセキュリティの専門家とのコミュニケーションに必要なリテラシーを習得する。 (1) 人類と IT（腕木通信から 5 G、量子コンピューティングまで） (2) サイバー空間と社会（国家、政治、企業、テクノロジー、国民） (3) コンピュータ理論（OS を中心に）、情報通信ネットワーク理論 (4) インターネットの基本原理（ウェブ、電子メール、e コマース、クラウド） (5) サイバーセキュリティの要素技術（暗号と電子署名、認証、アクセス制御）	予習 2 時間 講義 90 分 宿題 2 時間
第 2 回	サイバー空間における脅威と対策	サイバー空間における主要な脅威を事業上のリスクとして適切に把握することができるよう、脅威及び脆弱性とその対策に関する以下の事項について学ぶ。 (1) 脅威の関係主体（利用者過失、犯罪組織等） (2) 不正・悪用の歴史・トレンドと考え方、犯罪心理 (3) 脅威と対策に関する情報収集の考え方と方法論・基本動作 (4) 脅威のトレンド（サイバーセキュリティに関わる過去の主要な事故やトラブル） (5) 脆弱性と対策（脆弱性の原理と対策方法、性能や利便性とのトレードオフ）	予習 2 時間 講義 90 分 （場合によっては、90×2 分） 宿題 2 時間

第3回	サイバーセキュリティに関連する法令・規格・諸制度	サイバーセキュリティ確保のために事業者が遵守すべき事項や、効果的な対策実現のために参照すべき制度等について学ぶ。 (1) 法令・規格・諸制度対応の考え方と方法論・基本動作 (2) 関連法令（不正アクセス禁止法、不正競争防止法、個人情報保護法、EU 一般データ保護規則（GDPR）等） (3) 規格・標準・ガイドライン（ISO 31000、ISO/IEC 27000 シリーズ、SP-800.171 等） (4) その他（クラウドサービスにおける約款、サイバーセキュリティ保険、インターネットの関係機関）	予習 2 時間 講義 90 分 宿題 2 時間
第4回	サイバーセキュリティに関連するリスクマネジメントの方法	リスクマネジメントを行う上でのサイバーセキュリティ分野の特殊性について認識した上で、リスクを許容レベル以下に抑制するための方法について、グループワークによる演習を通じて学ぶ。 (1) リスクマネジメントの基本的考え方と方法論・基本動作 (2) サイバーセキュリティリスクに関連するリスクの評価方法 (3) (2)で評価したリスクについての低減、回避、保有、移転の方法 (4) 体制構築（組織内での連絡・共有体制の整備・維持、外部専門家の活用等） (5) インシデント対応プロセス（異常検知、サービス停止の判断、復旧、メディア対応等）	予習 2 時間 講義 30 分＋ 演習 60 分 宿題 2 時間
第5回	企業価値向上とサイバーセキュリティ	事業において IT が担う役割が大きな企業ほど、サイバーセキュリティ対策を含めた形で適切にリスク管理されたサービスを提供することが企業価値の向上につながることを認識し、サイバーセキュリティ対策があらかじめ組み込まれた事業戦略を企画立案するための方法について、グループワークによる演習を通じて学ぶ。 (1) 企業価値とサイバーセキュリティの基本的考え方と方法論・基本動作 (2) 企業価値への影響を考慮した費用対効果分析に基づくサイバーセキュリティ投資の考え方 (3) セキュリティ品質とブランド戦略・顧客との信頼醸成 (4) セキュリティ対策の証明と情報発信	予習 2 時間 講義 30 分＋ 演習 60 分 宿題 2 時間

実施に当たっての条件を次に示す。

- 予習・宿題のボリュームが大きいことから、１～２日での集中開催は困難であり、週１回以上の間隔を開け、１～２か月での開催が適切である。各回の開催日を連続させないことで、受講者が学習した内容を記憶に定着させる効果が期待できる。
- 想定する受講者のポジションとして、自ら経営判断をする立場にはないが、経営者に対して説明したり、経営者が判断するための資料を作成したりする必要があり、経営課題について十分な認識を行う必要があることを想定する。
- １回目と２回目の講義においては、板書形式の講義は一切行わない。（必要な知識は予習で身に付けることを前提とする）講義においては、コンピュータとネットワークを実際に使い、手を動かし、目でみながら身に付けることを基本とする。
- ３回目～５回目の講義においても、板書形式の講義は一切行わない。（必要な知識は予習で身に付けることを前提とする）講義においては実際のケースを使いながら、ディスカッションないしは共同作業（演習）形式を中心として実施するものとする。
- 第１回の「サイバー空間を理解するための基礎知識」の講義では、サイバーセキュリティに関する脅威と対策の基本的事項を理解するために必要な情報技術に関する知識を集中的に学習させるものである。十分に知識がある場合はスキップをしてもかまわない。

なお、情報系の学習経験のない受講者を対象とする可能性が高いため、古典的な教科書に示されているコンピュータの原理などから入るのではなく、日常目にするサービスやアプリケーションの説明を導入とした上で、その原理を説明するなどの工夫が必要である。我が国では情報技術に関する基礎知識を大学等で習得している人材が少ないと見込まれることから、第 1 回講義で用いる教材に海外の類似内容のものを用いることはできず、今後新たに作成することが必要である。

- 第 2 回以降については、企業におけるリスクマネジメントについてある程度の経験を有することを前提に、サイバーセキュリティ固有の事情について説明するものである。

参考として、上記のモデルカリキュラムを体系的にまとめた図を以下に示す。

図 6 ：戦略マネジメント層におけるカリキュラムの体系

b　実務者層･技術者層

システム企画や管理、構築、セキュリティの専門サービスを担う人材の知識･スキル等について、ユーザー企業は、産業横断サイバーセキュリティ人材育成検討会の第 1 期報告書等で、また、ベンダー企業は IPA（ITSS+）で過去に定義されたものがある。また、カリキュラ

ムに関しては、『平成 28 年度理工系プロフェッショナル教育推進委託事業 工学分野における理工系人材育成の在り方に関する調査研究（情報セキュリティ人材育成に関する調査研究）成果報告書』において提示されたものがある。基本的にはそれらを参照することができるが、本項目においては、それらを整理したものを改めて提示することとする。

1. 求められる知識・スキル

ITSS＋及び SecBoK におけるシステム担当相当の専門分野・役割として、既に整理がなされている。詳細については別紙 7 ～10 の参考を参照。特に、経営層、戦略マネジメント層を支え、他の専門人材と円滑にコミュニケーションをとれる必要があるため、そのための知識・スキルや、新たな技術やシステム開発手法を積極的に活用するための知識・スキルが必要である。

2. モデルカリキュラム

『平成 28 年度理工系プロフェッショナル教育推進委託事業 工学分野における理工系人材育成の在り方に関する調査研究（情報セキュリティ人材育成に関する調査研究）成果報告書』（文部科学省（委託先：学校法人岩崎学園情報セキュリティ大学院大学）、2017 年 3 月）[4]において提示されているモデル・コア・カリキュラムのうち、例示⑤[5]及び有識者の御意見を踏まえて調整したものを次表に示す。

表 4：実務者のためのカリキュラム例

目的	企業等における IT 基盤の企画管理責任者が、必要なサイバーセキュリティ対策を組み込んだ（例えば、セキュリティを考慮したビジネス設計や適切な外部委託）事業計画を立案するために求められる、サイバーセキュリティの最新動向、リスクマネジメントの考え方及び対応体制の構築などに関する知識・スキルを習得する。		
前提知識・経験	企業等における情報システムや IT 基盤の運用実務経験者。情報セキュリティマネジメント試験に合格できる程度のサイバーセキュリティに関する知識を有することが望ましい。		
	講義内容	解説	実施方法

[4] http://www.mext.go.jp/component/a_menu/education/detail/__icsFiles/afieldfile/2017/06/19/1386824_001.pdf

[5] 成果報告書の p.93 例示⑤（情報セキュリティに関する単独の科目を対象とするもの）を参照。

第1回	情報セキュリティ基礎知識	情報セキュリティの基本的な概要を学び、現在社会が直面する情報セキュリティ課題と企業活動におけるセキュリティの重要性を理解するために実社会におけるサイバー攻撃の脅威と要因、及びサイバー攻撃対策に必要な考え方について学ぶ。サイバー攻撃への対策では、技術的・物理的な対策から人的・組織的対策まで総合的に取り組むことの重要性を学ぶ。	予習 2 時間 講義 90 分 宿題2時間
第2回	情報セキュリティを支える暗号技術の基礎と応用	暗号技術の基礎として、共通鍵暗号、ハッシュ関数、公開鍵暗号とその応用である電子署名とPKIについて学ぶ。	予習 2 時間 講義 90 分 宿題2時間
第3回	ネットワークを守る認証技術とシステム技術	不正なネットワーク接続を防御するための要素技術を学ぶ。「なりすまし」を防ぐために用いられる認証技術や「なりすまし対策」について紹介し、その効果を理解する。また、広く利用が普及している無線LANとスマートフォンのセキュリティ対策についても学ぶ。	予習 2 時間 講義 90 分 宿題2時間
第4回	企業の情報ネットワークシステムのセキュリティ	企業の情報ネットワークのセキュリティ課題と対応する防御技術としてネットワークの仮想化、侵入検知技術、セキュリティ管理業務と支援システムについて学ぶ。	予習 2 時間 講義 90 分 宿題2時間
第5回	ソフトウェアのセキュリティ課題と対策	ソフトウェアに潜む脆弱性について学ぶ。マルウェアの侵入の手口となるバッファオーバーフローを例に攻撃の仕組みやOSやシステム・ソフトウェアによる対策技術の概要について学ぶ。	予習 2 時間 講義 90 分 宿題2時間
第6回	情報セキュリティマネジメントのフレームワーク	情報セキュリティマネジメントにおける事故事例から情報セキュリティマネジメントの重要性とそのフレームワーク（PDCAサイクル）、インシデント対応時の基本的な考え方等について学ぶ。	予習 2 時間 講義 90 分 宿題2時間
第7回	情報セキュリティのリスクマネジメントとリスクコントロール	情報セキュリティマネジメントにおけるリスクマネジメント手法の概要を学びリスクの分析方法、リスクの評価方法、更にリスクコントロールについて事例をベースに学ぶ。	予習 2 時間 講義 90 分 宿題2時間
第8回	情報セキュリティの関わる法律と標準化動向の基礎知識	最新のセキュリティ関連の法律について焦点を当てサイバーセキュリティ基本法、不正アクセス禁止法などセキュリティに関係する主要な法律の内容について学ぶ。また情報セキュリティに関連する国際標準とガイドラインの概要とソフトローの役割について学ぶ。	予習 2 時間 講義 90 分 宿題2時間

実施に当たっての条件を次に示す。

- 予習・宿題のボリュームが大きいことから、２～３日での集中開催は困難であり、週１

回以上の間隔を開け、２～３か月での開催が適切である。

- 想定する受講者のポジションとして、企業の情報システムや IT 基盤の運用に関して豊富な実績を有する者が、それらのサイバーセキュリティ対策に関する企画・管理を担うために必要な知識・スキルを習得することを想定する。よって、戦略マネジメント層とは異なり、カリキュラムに IT の基礎に関する内容は含めていない。
- 本カリキュラムは、CSIRT においてインシデント対応の責任を有するような人材を対象としたものではない。こうした役割を兼ねる人材を対象とする場合は、インシデントレスポンスに関する演習等の時間をカリキュラムに追加することが考えられる。

表５：専門技術者のうち、セキュリティバイデザインを身に付ける人材育成のためのカリキュラム

目的	企業等における情報システムの構築担当者が、必要なサイバーセキュリティ対策を組み込んだ情報システムの設計・構築を行うために求められる、サイバーセキュリティの最新動向、リスクマネジメントの考え方及び対応体制の構築などに関する知識・スキルを習得する。
前提知識・経験	企業等における情報システムの構築実務経験者。情報セキュリティマネジメント試験に合格できる程度のサイバーセキュリティに関する知識を有することが望ましい。

	講義内容	解説	実施方法
第１回	情報セキュリティ基礎知識	情報セキュリティの基本的な概要を学び、現在社会が直面する情報セキュリティ課題と企業活動におけるセキュリティの重要性を理解するために実社会におけるサイバー攻撃の脅威と要因、及びサイバー攻撃対策に必要な考え方について学ぶ。サイバー攻撃への対策では、技術的・物理的な対策から人的・組織的対策まで総合的に取り組むことの重要性を学ぶ。	予習 2 時間 講義 90 分 宿題2時間
第２回	セキュリティ要件定義とセキュア開発	セキュリティバイデザインの考え方に基づく企画・設計段階での要件定義の方法、DevSecOpsの考え方、脆弱性を生じにくくするためのセキュアコーディング技術について学ぶ。	予習 2 時間 講義 90 分 宿題2時間
第３回	マルウェア感染及び不正侵入と対処	情報システムの脆弱性を悪用したマルウェア感染や不正侵入について、インシデントの過程においてどのような対策を講じれば影響を抑制できるか等の内容を講義と演習で学ぶ。	予習 2 時間 講義 30 分 ＋演習 60 分 宿題2時間
第４回	企業リスクとリスクマネジメント	情報システムの構築に関わるサイバーセキュリティ事象を対象とするリスクマネジメントについて、グループワークを通じて学ぶ。	予習 2 時間 講義 30 分 ＋演習 60 分 宿題2時間

実施に当たっての条件を次に示す。

- 予習・宿題のボリュームが大きいことから、２～３日での集中開催は困難であり、週１回以上の間隔を開け、２～３か月での開催が適切である。
- 想定する受講者のポジションとして、企業の情報システムや IT 基盤の構築に関して豊富な実績を有する者が、それらのサイバーセキュリティ対策に関する実務を担うために必要な知識・スキルを習得することを想定する。

４　各省庁等における人材育成施策と施策間連携の状況

各人材層を対象として、各省庁で行っている施策について、現状における全体像を整理した。

（１）　各省庁等における人材育成施策の全体像

各省庁等における人材育成施策の全体像は次図に示すとおり。各施策の詳細は別紙の参考４のとおり。

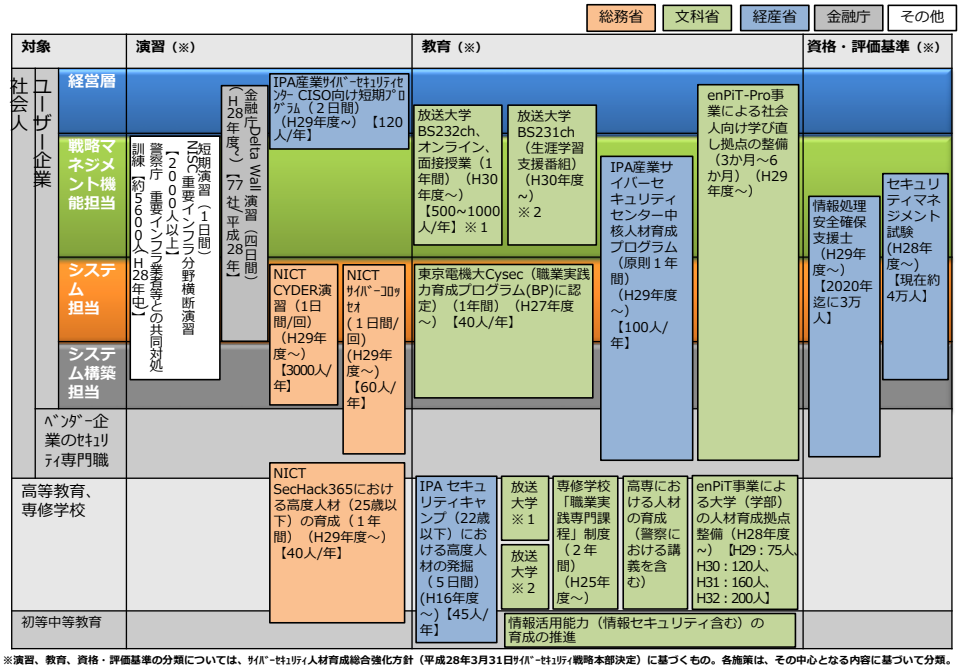


図７：各省庁の人材育成施策に関する全体像（イメージ）

（２）　施策間連携の状況

各施策間の連携について、その例を次に示す。

- enPiT 事業によるカリキュラムを高等専門学校生が受講
- SecHack365 やセキュリティキャンプへ、高等専門学校生が参加
- 警察における情報技術解析実務を踏まえたサイバーセキュリティ講義を高等専門学校にて実施
- 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の修了者は、「登録セキスペ」への登録に当たって、情報処理安全確保支援士試験を免除

５　各層の人材育成を進めていくための課題

（１）戦略マネジメント層

・　事業部門のサイバーセキュリティに対する意識が低い、あるいは、サイバーセキュリティは重要だが、具体的な対応は他の部門あるいはベンダーに任せているなどにより、サイバーセキュリティリスクに対し、サイバーセキュリティを考慮する機能が明確になっていない問題がある。

・　事業部門のマネジメント機能とサイバーセキュリティ対策が乖離していることがある。例えば、スピード感をもってシステムを構築し、セキュリティを組み込む必要があるが、それについてこられるベンダーがいないといった問題や、OT 部門で数十年のライフサイクルで運用するシステムに対して、突然 IT 並みのセキュリティレベルが必要と指摘され、ビジネスのプライオリティを乱されるなどの問題がある。このように、仮に経営層が事業部門においてセキュリティ対策を進めるということで推進したとしても、セキュリティ対策がビジネスのプロセス、セキュリティ意識、文化・慣習等に合わない問題がある。

・　事業部門の人材向けに適切なサイバーセキュリティ教材やプログラムが存在しない。

（２）実務者層・技術者層

・　経営層・戦略マネジメント層を支え、他の専門人材と円滑にコミュニケーションをとりながらチームの一員として対処ができる人材の育成が必要。

・　ビジネスイノベーションに不可欠な新たな情報通信技術やシステム開発手法を積極的に活用するためのサイバーセキュリティの知識・スキルの育成（IT ベンチャー向けのセキュリティ支援）が必要。

（３）戦略マネジメント層、実務者層・技術者層共通

・　需要と供給の好循環を産学官の連携の下、形成していくためには、需要サイド、供給サイドそれぞれについて見える化のための取組が重要。具体的には、需要に関しては、

　・　必要な人材規模の可能な範囲での把握

　・　企業におけるキャリアパスの明確化

　が必要である。

　また、供給に関しては、人材育成施策や各種教育プログラムについて、そのターゲットや将来のキャリアパスを含めて分かりやすく、一覧性をもって示していくことが必要である。

・　初等中等教育段階においては、小学校段階から必修としたプログラミング教育など、発達の段階に応じてコンピュータなどの情報技術の原理や仕組みなどを理解し、プログラミ

ング的思考といった論理的思考力を育てることが重要である。また、近年、若年層によるサイバー犯罪が発生していることから、情報モラル教育も重要な課題である。

・ さらに、IT やサイバーセキュリティに対して強い興味・関心を持つ若年層が、実践的に IT やサイバーセキュリティに関する能力を伸ばすことのできる環境が必要である。

６　人材育成に係る今後の施策の方向性

（１）　戦略マネジメント層に関わる施策の方向性

○組織における戦略マネジメント層の定着

・戦略マネジメント層がサイバーセキュリティの知識・スキルを身に付け、自らのマネジメントの中にサイバーセキュリティの項目を組み込んでいけるよう、経営層の理解と意識改革におけるテーマとしていく。

・具体的な戦略マネジメント層の活躍のイメージ（ロールモデル）を明確にするため、業種別の戦略マネジメント層の組織における位置づけ、機能の明確化、ベストプラクティスの共有について産業界と連携を図りつつ検討を行う。

・事業部門のマネジメントとセキュリティ対策が調和できるようなフレームワークの整備に取り組む。

○カリキュラム・教材開発と学び直しプログラムの推進

・これまで、事業部門の人材向けのサイバーセキュリティに関する適切な教材やプログラムが存在していなかったことから、経営・事業戦略の視点でセキュリティを実践するための知識・スキルを身に着けるための教材開発を推進するための試行的取組について検討する（最終的には、業種・業態に適した教材開発が行われることが望ましい）。また、こうした教材による学び直しプログラムの実践を指導者の発掘を含めて推進する。

（２）　実務者層・技術者層に関わる施策の方向性

○経営層・戦略マネジメント層を支える人材育成

産業界、教育機関及び研究機関が連携し、カリキュラムの検討・実施、継続的な見直しや、教育コンテンツの開発を進めるとともに、産業界のニーズに合った人材育成コースを提供できるようにする。また、資格・評価基準等によって知識と実践力を可視化していくことが重要である。その際、産業界との連携を図るものとする。

○クラウドや先端技術等の利用に係る人材育成

近年、製品やサービス等の開発においては、クラウドの活用や DevOps によるシステム開発、先端技術等の利用が急速なスピードで広がっている。このため、こうした新たな技術や開発手法に対応し、セキュリティ・バイ・デザインの考え方を基本としてセキュリティの知識・スキルを育成するための人材育成策を検討するとともに、相互に技術を高め合えるようなコミュニティの形成を推進する。

（３） 戦略マネジメント層、実務者層・技術者層共通の施策の方向性

○サイバーセキュリティ人材育成策の充実・強化と施策間連携の推進

今後の IT 利活用の広がりを踏まえれば、サイバーセキュリティ人材育成は引き続き重要な課題であるといえる。このため、産学官の連携を図りつつ、各省庁における人材育成施策の充実・強化を進めるとともに、各施策を効率的かつ効果的に推進するため、施策間の連携を推進する。

○人材育成の「見える化」の推進

米国 NIST による人材育成の見える化（ポータルサイト）[6]の取組を参考にしつつ、需要と供給の「見える化」、産学官連携の「見える化」等の取組を推進するためのツールの整備について検討を行う。ツールの例としては以下の通り。

（ツールの例）

・必要な人材規模・キャリアパスの明確化

・育成プログラムの適切な評価基準の策定及び評価に向けた検討

・カリキュラム・教材等が一覧になったポータルサイトの整備

○若年層（初等中等教育段階を含む）における教育の充実

- サイバーセキュリティや IT は若年層の教育が重要であるため、その基礎的な内容について、初等中等教育段階では、教育課程内で情報活用能力の育成に着実に取り組むとともに、教員の研修等に取り組む。
- さらに、教育課程外の地域や企業・団体等において、自由にサイバー関連ツール、機器を用いて興味を持って学べる機会が豊富に用意されるような環境整備を進めることが必要である。同時に、こうした自己実現の環境整備は、倫理教育と併せて実施することで、若年層による興味本位のサイバー犯罪などの防止に効果があると考えられる。

---

[6] http://cyberseek.org/

７　今後の取組

本取りまとめの内容を踏まえ、次期サイバーセキュリティ戦略の検討を進めるものとする。また、引き続き、産業界との緊密な連携の下、人材育成施策の検討を進めるとともに、各人材育成施策のさらなる連携の検討が行われるよう、本報告書の示した施策の方向性に示した実施状況については、サイバーセキュリティ戦略の年次報告等を通じてフォローアップを行う。

（別紙１）参考資料

参考１　各省庁の主な取組[7]

（１）総務省の取組

セキュリティ人材の育成（ナショナルサイバートレーニングセンター）

○　巧妙化・複合化するサイバー攻撃に対し、実践的な対処能力を持つセキュリティ人材を育成するため、平成29年４月に国立研究開発法人情報通信研究機構（NICT）に組織した「ナショナルサイバートレーニングセンター」において、下記取組を実施。

①　国の行政機関、地方公共団体、独立行政法人及び重要インフラ事業者等を対象とした実践的サイバー防御演習（CYDER）

②　2020年東京オリンピック・パラリンピック競技大会に向けた大会関連組織のセキュリティ担当者等を対象者とした実践的サイバー演習（サイバーコロッセオ）

③　若手セキュリティイノベーターの育成（SecHack365）

平成30年度予算　　15．1億円

実践的サイバー防御演習（CYDER）

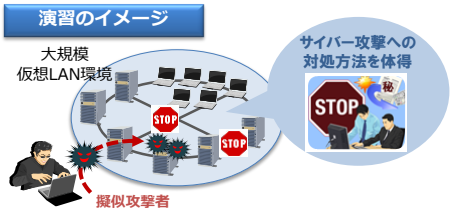
CYDER：CYber Defense Exercise with Recurrence

○　総務省は、NICTを通じて、**国の行政機関、地方公共団体、独立行政法人及び重要インフラ事業者等を対象**とした**実践的サイバー防御演習（CYDER）**を実施。

○　**受講者は、組織のネットワーク環境を模した大規模仮想LAN環境下で、実機の操作を伴って**サイバー攻撃によるインシデントの検知から対応、報告、回復までの**一連の対処方法を体験**。

○　平成29年度は、**全国で100回開催**し、**計3,009名が受講**。

演習のイメージ




CYDER演習風景（大手町）

- NICT北陸StarBED技術センターに設置された大規模高性能サーバー群を活用し、行政機関等の実際のネットワークを模した大規模仮想LAN環境を構築。
- NICTの有する技術的知見を活用し、サイバー攻撃に係る我が国固有の傾向等を徹底分析し、現実のサイバー攻撃事例を再現した最新の演習シナリオを用意。

平成30年度の実施計画

コース	受講対象組織	開催地	開催回数	受講予定者数
Aコース（初級）	（全組織共通）	47都道府県	60回	1,800名
B-1コース（中級）	地方公共団体向け	全国11地域	20回	600名
B-2コース（中級）	国の行政機関等向け	東京	10回	300名
B-3コース（中級）（新設）	重要インフラ事業者（※）向け	東京	10回	300名
				計3,000名

（※）情報通信、金融、航空、鉄道、電力、ガス、医療、水道、物流、化学、クレジット、石油、地方公共団体の13分野

7　関係機関より提供

東京2020オリンピック・パラリンピック競技大会に向けた実践的サイバー演習（サイバーコロッセオ）

○ 近年さらに高度化・多様化するサイバー攻撃に備え、東京2020オリンピック・パラリンピック競技大会の適切な運営を確保することを目的として、**大会関連組織のセキュリティ担当者等を対象とした、**高度な攻撃に対処可能な人材の育成を行う**実践的サイバー演習「サイバーコロッセオ」を平成30年2月から本格的に実施**。

○ サイバーコロッセオは、**NICTが実施主体となり**、大規模演習環境及び長年のサイバーセキュリティ研究による知見を活かした、**実際の機器やソフトウエアの操作を伴う「実践的なトレーニング」を実施**。

イメージ図

東京2020オリンピック・パラリンピック競技大会のサイバーセキュリティを確保

■ 大規模演習環境を用いて、東京大会の公式サイト、大会運営システム等ネットワーク環境を忠実に再現した、仮想のネットワーク環境を構築。

■ 仮想のネットワーク環境上で、東京大会時に想定されるサイバー攻撃を擬似的に発生させ、攻撃・防御手法の検証及び訓練を実施。

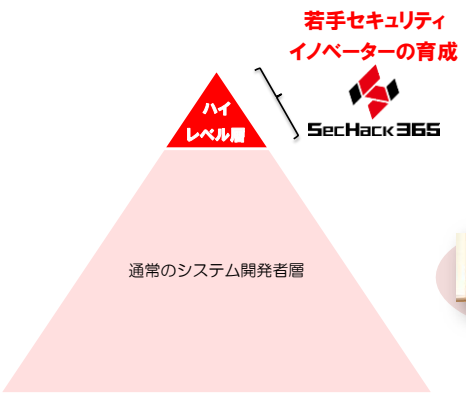
若手セキュリティイノベータの育成（SecHack365（セックハックサンロクゴ））

○ **未来のサイバーセキュリティ研究者・起業家の創出に向けて**、NICTの持つサイバーセキュリティの研究資産を活用し、**若年層のICT人材を対象に**実際のサイバー攻撃関連データに基づいた**セキュリティ技術の研究・開発を、第一線で活躍する研究者・技術者が1年かけて継続的かつ本格的に指導**。

○ 対象者は、日本国内に居住する**25歳以下の若手ICT人材**（平成29年度は受講者として47名を選定。）

○ 受講者は、NICTの有する遠隔開発環境（NONSTOP（※））を活用し、**年中どこからでも遠隔開発実習を行うことが可能**。また、**集合イベントとして、座学講座（研究倫理）やハッカソン等を実施**。

（※） NONSTOP(NICTER Open Network Security Test-out Platform)では、NICTの長年にわたるサイバーセキュリティ研究によって得られた膨大なセキュリティ関連データを活用することができ、NONSTOP内に整備された様々な研究開発・解析用ツール類と、他では触れることのできない貴重なデータを用いて研究・開発に取り組むことが可能。



■ 遠隔開発実習、座学講座、ハッカソン等の組合せによる総合的な人材育成プログラム。

（２）文部科学省の取組

Society 5.0に対応した高度技術人材育成事業

平成30年度予算額　12億円　（平成29年度予算額：９億円）

背景・課題

◆ 第４次産業革命の進展による産業構造の変化に伴い、**付加価値を生み出す競争力の源泉が、「モノ」や「カネ」から、「ヒト(人材)」・「データ」である経済システムに移行。**

◆あらゆる産業でITとの組み合わせが進行する中で我が国の国際競争力を強化し、持続的な経済成長を実現させるには、**ITを駆使しながら創造性や付加価値を発揮し、我が国の成長を支える産業基盤の強化とともに、新たな産業を創出する人材の育成が急務。**

産学連携による実践的な教育ネットワークを形成し、Society 5.0の実現に向けて人材不足が深刻化しているサイバーセキュリティ人材やデータサイエンティスト、科学技術を社会実装できる人材といった、大学等における産業界のニーズに応じた人材を育成する取組を支援。

（資料）IT人材の最新動向と将来推計に関する調査結果（平成28年6月経済産業省）

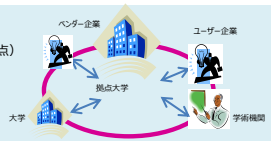
事業の取組内容

取組１　成長分野を支える情報技術人材の育成拠点の形成(enPiT)　８億円【継続】

産学連携による課題解決型学習(PBL)等の実践的な教育の推進により、大学における情報技術人材の育成強化を目指す。
※PBL：Project Based Learning の略

取組１-①　学部学生に対する実践的教育の推進(enPiTⅡ)　５億円
（運営拠点：１拠点、分野別中核拠点：４拠点）
・大学間連携により、PBL中心の実践的な教育を実施
・教育ネットワークを構築し、開発した教育方法や知見を全国に普及
・産業界と協力な連携体制を構築
※enPiT（エンピット）：Education Network for Practical Information Technologiesの略

取組１-②　IT技術者の学び直しの推進(enPiT-Pro)　３億円（５拠点）
・大学が有する最新の研究の知見に基づき、情報科学分野を中心とする高度な教育(演習・理論等)を提供
・拠点大学を中心とした産学教育ネットワークを構築し、短期の実践的な学び直しプログラムを開発・実践
・セキュリティ等の特に人材不足が深刻な分野の学び直し推進

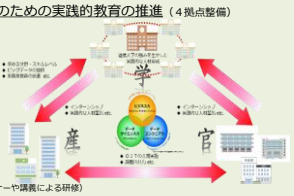


取組２　未来価値創造人材育成プログラム　４億円　【新規】
高い専門性と俯瞰的知識を身に付けたより実践的でハイブリッドな人材の育成強化を目指す。

取組２-① 超スマート社会の実現に向けたデータサイエンティスト育成事業
３億円【新規】

産官学による実践的な教育ネットワークを構築し、文系理系を問わず様々な分野へ数理科学の応用展開を図り、それぞれの応用分野でデータから価値を創出し、ビジネス課題に答えを出す人材(データサイエンティスト)を育成する。

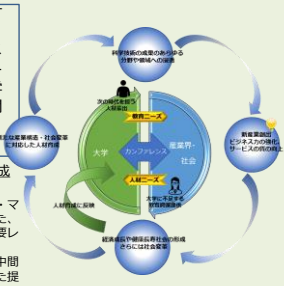
◆データサイエンティスト育成のための実践的教育の推進（４拠点整備）
・産業界や地方公共団体と強力な連携体制を構築し、必要となるビッグデータの提供、実課題によるPBL（共同研究）やインターンシップ等からなる教育プログラムを開発・実践
・データサイエンスを学ぶ必要に駆られた社会人の学び直しの場を提供し、産官ともに人材不足の中で、Off-JTの産官共同実施の機会やコミュニティ形成を醸成
※Off-JT：Off-the-Job Training（職場外でのセミナーや講義による研修）



取組２-② 科学技術の社会実装教育エコシステム拠点の形成　１億円【新規】

産学共同で科学技術の社会実装に資する教育のエコシステム拠点を形成し、工学分野における主専攻・副専攻（メジャー・マイナー）、ダブルメジャーといった高度専門人材育成に必要な学部・大学院連結プログラムの先導的開発に向けたフィージビリティスタディを実施する。

◆社会実装教育の実現に不可欠なモデル作成
（運営拠点：１拠点、拠点大学：３拠点整備）
・学部と大学院の連結教育プログラム（メジャー・マイナー、ダブルメジャー）の先導的開発に向けた、現状把握、今後の展望、ターゲット、社会の需要レベルなどの明確化
・「大学における工学系教育の在り方について（中間まとめ）」等の有識者会議等で取りまとめられた提言内容を踏まえた取組を実施。



情報セキュリティ人材の育成

平成30年度予算額：4億円（平成29年度予算額：2.4億円）
((独)国立高等専門学校機構運営費交付金 特別教育研究経費の内数)

１．課題・背景

あらゆるものがインターネットに接続され、ITを活用したサービスが拡大する中、情報セキュリティ人材の育成が急務となっている。IoT機器を理解し、設計段階からセキュア（安全に）設計ができる人材、稼働しているクラウド環境を管理・監視できる人材の養成が必要。

２．取組概要

（１）高知高専、石川高専などにおいて**企業と連携した情報セキュリティのスキルセット（到達目標）の構築、教材開発を行う**とともに、**情報セキュリティの教育実践と到達度評価**を行う。

（２）情報セキュリティに関する知識やスキルの習得に加え、**高い倫理観やITリテラシーを習得**する教材・教育プログラムの展開と、社会ニーズを踏まえた実践的な演習環境の高度化を図る等、教育環境を加速度的に整備することにより、**情報セキュリティ人材の質的向上と量的拡大を図る**。

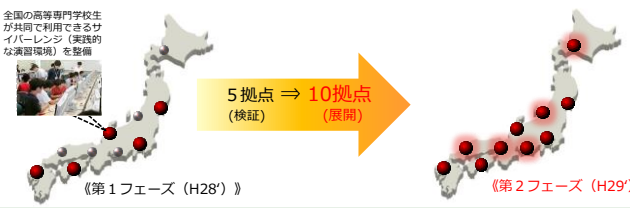
「セキュリティ演習拠点」の整備

◇「情報セキュリティ人材」の演習拠点を全国10ヶ所に整備し、全国の高専からアクセスを可能としたサイバーレンジ（実践的な演習環境）を提供

○第１フェーズ：平成28年度に整備した先行５拠点（一関、木更津、石川、高知、佐世保）において、「情報セキュリティ人材」の育成に必要な教育実践を検証し、理想的な環境整備と実効性のある教育方法を確立。

○第２フェーズ：第１フェーズで構築したものを基に、全高専を補完するため、後発５拠点（旭川、小山、岐阜、松江、熊本）の教育環境整備を実施し、全国10ヶ所で「情報セキュリティ人材」の発掘・育成を強力に実行。

※ 日々進化しているサイバー攻撃技術にも対応するため、定期的な環境更新（アップデート）が必要。



【拠点整備・環境更新の年次計画イメージ】
◎ 拠点整備 ⇒ 平成28年度、29年度の2カ年で整備
◎ 環境更新 ⇒ 平成30年度から４年周期で更新

	H28’	H29’	H30’	H31’	H32’	H33’
拠点整備	5拠点	5拠点				
環境更新（ソフトウェア中心）			3拠点	2拠点	3拠点	2拠点

専門学校における職業教育の充実

「職業実践専門課程」の文部科学大臣認定制度

平成23年1月　中央教育審議会「今後の学校におけるキャリア教育・職業教育の在り方について」答申

○　職業教育を通じて、自立した職業人を育成し、社会・職業へ円滑に移行させること、また、学生・生徒の多様な職業教育ニーズや様々な職業・業種の人材需要にこたえていくことが求められており、このような職業教育の重要性を踏まえた高等教育を展開していくことが必要。
○　高等教育における職業教育を充実させるための方策の一つとして、職業実践的な教育のための新たな枠組みを整備。
⇒　新たな学校種の制度を創設するという方策とともに、既存の高等教育機関において新たな枠組みの趣旨をいかしていく方策も検討。

平成25年7月「専修学校の質保証・向上に関する調査研究協力者会議」報告

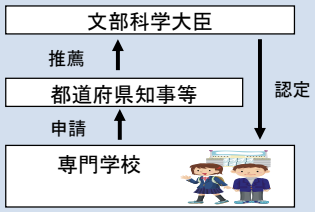
「新たな枠組み」の趣旨を専修学校の専門課程においていかしていく先導的試行として、企業等との密接な連携により、最新の実務の知識等を身につけられるよう教育課程を編成し、より実践的な職業教育の質の確保に組織的に取り組む専門課程を文部科学大臣が「職業実践専門課程」として認定する。

⇒平成25年8月　「専修学校の専門課程における職業実践専門課程の認定に関する規程(文部科学省告示第133号)」を公布・施行
⇒平成26年3月31日　「職業実践専門課程」を文部科学大臣が認定し、官報で告示。 4月から認定された学科がスタート

平成29年3月　これからの専修学校教育の振興のあり方について（報告）

職業実践専門課程は、**教育の高度化と改革を目指す専門学校の取組の枠組**として位置づけることが必要。

認定要件等



－認 定 要 件－

企業等との「組織的連携」　取組の「見える化」

○　修業年限が2年以上
○　企業等と連携体制を確保して、授業科目等の教育課程を編成
○　企業等と連携して、演習・実習等を実施
○　総授業時数が1700時間以上または総単位数が62単位以上
○　企業等と連携して、教員に対し、実務に関する研修を組織的に実施
○　企業等と連携して、学校関係者評価と情報公開を実施

情報セキュリティ，情報モラルに関する教育について

学習指導要領における主な記述

小・中学校学習指導要領　（平成29年3月31日公示）

総則

（小・中学校）　第1章　第2
2(1) 各学校においては，児童（生徒）の発達の段階を考慮し，言語能力，情報活用能力（情報モラルを含む。），問題発見・解決能力等の学習の基盤となる資質・能力を育成していくことができるよう，各教科等の特質を生かし，教科等横断的な視点から教育課程の編成を図るものとする。

社会

（小学校）　第2章　第2節
3(4)ア　アの(ア)の「放送，新聞などの産業」については，それらの中から選択して取り上げること。その際，情報を有効に活用することについて，情報の送り手と受け手の立場から多角的に考え，受け手として正しく判断することや送り手として責任をもつことが大切であることに気付くようにすること。

（中学校）　第2章　第2節　第3
2(2) 情報の収集，処理や発表などに当たっては，学校図書館や地域の公共施設などを活用するとともに，コンピュータや情報通信ネットワークなどの情報手段を積極的に活用し，指導に生かすことで，生徒が主体的に調べ分かろうとして学習に取り組めるようにすること。その際，課題の追究や解決の見通しをもって生徒が主体的に情報手段を活用できるようにするとともに，情報モラルの指導にも留意すること。

【技術・家庭】

（中学校）　第2章　第8節　第2
2D(1)ア 情報の表現，記録，計算，通信の特性等の原理・法則と，情報のデジタル化や処理の自動化，システム化，情報セキュリティ等に関わる基礎的な技術の仕組み及び情報モラルの必要性について理解すること。

イ 技術に込められた問題解決の工夫について考えること。

3(4)ア (1)については，情報のデジタル化の方法と情報の量，著作権を含めた知的財産権，発信した情報に対する責任，及び社会におけるサイバーセキュリティが重要であることについても扱うこと。

道徳

（小・中学校）　第3章　第3
2(6) 児童（生徒）の発達の段階や特性等を考慮し，第2に示す内容との関連を踏まえつつ，情報モラルに関する指導を充実すること。

高等学校学習指導要領　（平成30年3月30日公示）

総則

第1章　第2款
2(1) 各学校においては，生徒の発達の段階を考慮し，言語能力，情報活用能力（情報モラルを含む。），問題発見・解決能力等の学習の基盤となる資質・能力を育成していくことができるよう，各教科・科目等の特質を生かし，教科等横断的な視点から教育課程の編成を図るものとする。

地理・歴史

第2章　第2節　第3款
2(4) 情報の収集，処理や発表などに当たっては，学校図書館や地域の公共施設などを活用するとともに，コンピュータや情報通信ネットワークなどの情報手段を積極的に活用し，指導に生かすことで，生徒が主体的に学習に取り組めるようにすること。その際，課題の追究や解決の見通しをもって生徒が主体的に情報手段を活用できるようにするとともに，情報モラルの指導にも留意すること。

公民

第2章　第3節　第2款　第1
3(3)カ(キ) アの(エ)については，(ア)から(ウ)までのそれぞれの事項と関連させて取り扱い，情報に関する責任や，利便性及び安全性を多面的・多角的に考察していくことを通して，情報モラルを含む情報の妥当性や信頼性を踏まえた公正な判断力を身に付けることができるよう指導すること。その際，防災情報の受信，発信などにも触れること。

第2章　第3節　第3款
2(4) 情報の収集，処理や発表などに当たっては，学校図書館や地域の公共施設などを活用するとともに，コンピュータや情報通信ネットワークなどの情報手段を積極的に活用し，指導に生かすことで，生徒が主体的に学習に取り組めるようにすること。その際，課題の追究や解決の見通しをもって生徒が主体的に情報手段を活用できるようにするとともに，情報モラルの指導にも配慮すること。

情報

第2章　第10節
第2款　第1　情報Ⅰ
2(1)ア(イ) 情報に関する法規や制度，情報セキュリティの重要性，情報社会における個人の責任及び情報モラルについて理解すること。
イ(イ) 情報に関する法規や制度及びマナーの意義，情報社会において個人の果たす役割や責任，情報モラルなどについて，それらの背景を科学的に捉え，考察すること。
第3款
2(1) 各科目の指導においては，情報の信頼性や信憑性を見極めたり確保したりする能力の育成を図るとともに，知的財産や個人情報の保護と活用をはじめ，科学的な理解に基づく情報モラルの育成を図ること。

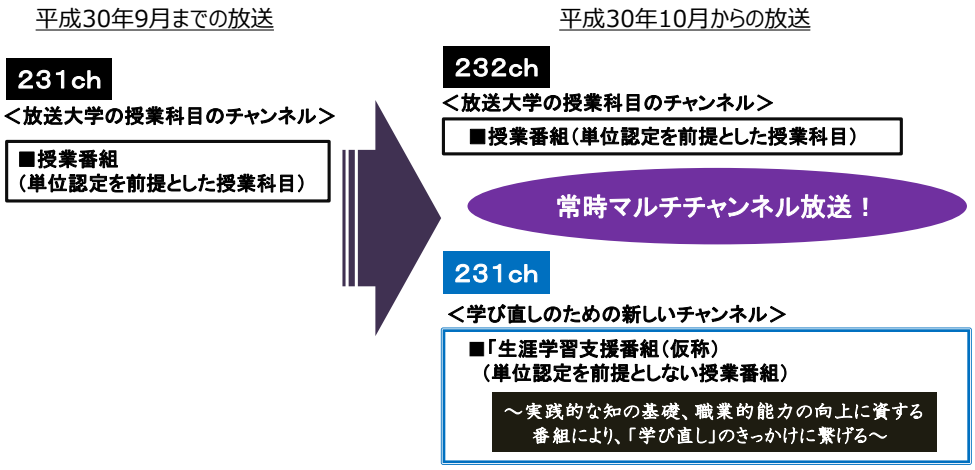
情報セキュリティ、情報モラル教育の充実に向けて

○新学習指導要領の趣旨の普及
○新学習指導要領の趣旨の実現に向けた情報教育及びICT活用の推進に関する調査研究
○新学習指導要領に対応した高等学校情報科担当教員の指導力向上
情報科担当教員を対象とした都道府県等の研修で活用できる教員研修用教材（研修テキスト）を作成・配布
（データサイエンスやサイバーセキュリティなど最新の情報技術に関する知識や指導方法、企業との連携の進め方等を再習得するための研修について、各都道府県教育委員会等の計画的な実施を支援）

○児童生徒向け啓発資料の作成・配布
『ちょっと待って！スマホ時代のキミたちへ』
○授業に活用できる動画教材や手引書等の作成
『情報社会の新たな問題を考えるための教材～安全なインターネットの使い方を考える～』
『情報モラル実践事例集2015』
○情報モラル教育に関するセミナーの実施

2018年10月から 放送大学 はマルチチャンネル放送！

**放送大学はこれまで、単位認定を前提とした授業科目に対応した番組を放送してきました。
これに加え、人生100年時代における社会人の多様な学び直しや生涯学習のニーズに応え、
単位認定を前提としない、様々な学びの機会を提供するチャンネルをお届けします。**



（３）経済産業省の取組

商務情報政策局 サイバーセキュリティ課
03-3501-1253

産業系サイバーセキュリティ推進事業

平成30年度予算額 19.1億円（11.7億円）

事業の内容

事業目的・概要

- 近年、企業や個人の情報を狙ったサイバー攻撃にとどまらず、プラントやインフラそのものの停止を狙い、制御システムまで含めた社会システム全体を標的とするサイバー攻撃のリスクが高まっています。（※制御システム：工場やプラントの機械や設備などのコントロールを行うために用いられるシステムのこと）
- 国家として、安全・安心な社会を築くためには、重要インフラや我が国経済・社会の基盤を支える産業における、サイバー攻撃に対する防護力を強化することが必須です。
- そのため、（独）情報処理推進機構（IPA）に29年4月に設立した「産業サイバーセキュリティセンター（Industrial Cyber Security Center of Excellence）」において、模擬プラントを用いた演習を通じて、官民の共同によりサイバーセキュリティ対策の中核となる人材を育成します。また、実際の制御システム等の安全性検証等により、産業のサイバーセキュリティ対策のノウハウを創出します。

成果目標

- 模擬プラント等を活用し、重要インフラ事業者等において、サイバーセキュリティの総合的な戦略立案を担う人材を毎年100人程度育成します。

条件（対象者、対象行為、補助率等）

国 → 交付金 → （独）情報処理推進機構

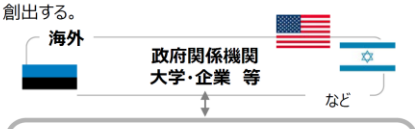
事業イメージ

模擬プラントを用いた演習等を通じた人材育成

- 情報系システムから制御系システムまでを想定した模擬プラントを設置。専門家と共に安全性・信頼性の検証や早期復旧の演習を行う。
- 最新の攻撃情報の調査・分析結果に応じてプログラムのアップデート等を実施。
- 海外との連携も積極的に実施。

実際のシステムの安全性・信頼性検証等

- 社会インフラ等で活用されている実際の制御システムやIoT機器の安全性・信頼性を検証。
- あらゆる攻撃可能性を検証し、必要な対策立案を行うことで、業界全体で活用可能なサイバーセキュリティ対策のノウハウを創出する。



IPA 産業サイバーセキュリティセンター
Industrial Cyber Security Center of Excellence（ICSCoE）

国内大学・研究機関 等

独立行政法人情報処理推進機構（IPA）運営費交付金

平成30年度予算額 49.0億円（45.4億円）

事業の内容

事業目的・概要

- 独立行政法人情報処理推進機構（IPA）が行う業務に必要な運営費を交付し、以下の事業を行います。

（１）ITが社会各層に浸透したことに伴う情報セキュリティ対策の強化

重要インフラや企業等に対するサイバー攻撃に関する情報などの収集・評価・分析を行うとともに、対策方法の提案・普及を通じて、被害の未然防止や低減を図ります。

（２）高度なIT人材の発掘・育成・支援とIT人材の裾野の拡大

未踏IT人材発掘・育成事業の実施及び拡充等を通じて高度なIT技術を有する人材への支援を強化するとともに、このような人材の起業・事業化に向けた支援を強化します。また、試験制度の着実な実施・普及等によりIT人材の裾野の拡大に取り組みます。

（３）社会基盤としてのＩＴ技術の実装支援に向けた取組

国民・企業が、IT技術の進化に伴う利益を有効かつ安全に享受できるよう、常に最先端の技術動向の調査分析を行い、それらを役立つ形で発信します。

成果目標

- 国家資格「情報処理安全確保支援士」について、2020年までに3万人超の有資格者の確保を目指すという政府目標に貢献します。
- 未踏IT人材発掘・育成事業等を通じ、チャレンジ精神溢れ将来の起業へとつながる人材を年間 100名輩出することを目指すという政府目標に貢献します。

条件（対象者、対象行為、補助率等）

国 → 交付金 → 情報処理推進機構（IPA）

事業イメージ

（１）ITが社会各層に浸透したことに伴う情報セキュリティ対策の強化

- サイバー攻撃に関する情報収集、対処方法の提示

重要インフラ等におけるサイバー攻撃に関する情報収集・情報共有のほか、サイバー攻撃に対する注意喚起を発出します。

（２）高度なIT人材の育成・支援とIT人材の裾野の拡大

- 未踏IT人材発掘・育成事業の実施及び拡充

突出した才能を持つITクリエータを発掘・育成します。また、産業界をリードするIT等のトップ人材を創出するため、起業・事業化支援の人材育成プログラムを創設し、日本の将来を切り拓いていくIT人材の発掘・育成を強化します。


（未踏人材発掘・育成事業）

- セキュリティ・キャンプ

若手のセキュリティ人材に対し、第一線の技術者が最新のノウハウ等を伝授します。

（３）社会基盤としてのIT技術の実装支援に向けた取組

- 最先端のＩＴ技術の動向に関する情報収集・発信等

AIをはじめとした最先端のIT技術の動向を情報収集・調査・分析しつつ、国民・企業の役に立つ形で発信します。

- ＩＴに関するタスクとスキルの体系化

ITを利活用するビジネスに求められる業務（タスク）と、それを支えるIT人材の能力や素養（スキル）を体系化します。

情報処理安全確保支援士試験　免除対象者一覧

- 産業構造審議会試験ＷＧ中間とりまとめを踏まえ、**試験合格者と同等以上の能力を有する者及び試験の全部又は一部を免除する者を指定**。
- 国等においてサイバーセキュリティの実務に一定期間以上従事している者については知識・能力を有する者であり試験を全部免除。また、大学等で情報セキュリティを学んでいる者については、学校で習得した知識に相当する部分を一部免除（午前Ⅱ）。若手の情報セキュリティ分野への誘導を促す。

対象者	試験免除	要件	制度実施時期
内閣情報調査室、警察庁、防衛省、IPA情報処理安全確保支援士試験委員で所定の事務を行った者	全部	指定ポストで2年以上勤務。各機関の長が推薦する者を経済産業大臣が認定	警察庁、防衛省職員は平成29年4月7日から実施。その他は、平成29年9月29日からの実施。
IPA 産業サイバーセキュリティセンターの講習修了者	全部	修了証により全部試験免除を申請した者	平成29年9月29日に関係告示を公布・施行。第1期生から対象。
大学院、大学、専門学校（4年制）の情報セキュリティ学科等を修了した者	午前Ⅱ	認定に必要となる履修学科をすべて修了した者（最終学年の者に限る）であって受験申込みをする者	平成29年9月29日に関係告示を公布・施行。 対応の早い学校については来年4月に入学した者から対象となる見込み。
支援士試験・高度試験の合格者又は午前Ⅰで所定の成績であった者	午前Ⅰ	過去2年間の合格者等に限る	法施行時に開始。
旧SC、SV試験合格者	全部	合格者	法施行時に開始。

（４）金融庁の取組

金融庁の施策例

金融分野のサイバーセキュリティ対策強化

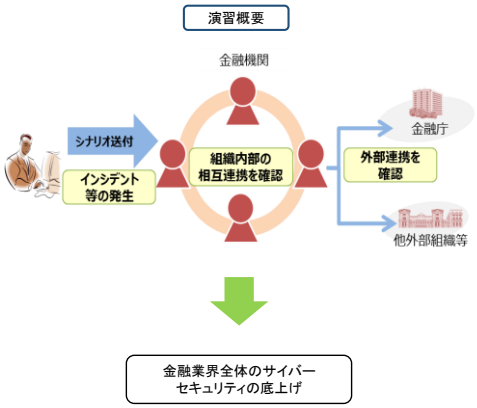
○ 金融業界横断的なサイバーセキュリティ演習の実施

平成３０年度当初予算：0.5億円（平成29年度当初予算：0.5億円）

事業概要

- 金融分野におけるサイバー攻撃の高度化が進む中、サイバーセキュリティの確保は、金融システム全体の安定のため喫緊の課題。
- 「金融分野におけるサイバーセキュリティ強化に向けた取組方針」（27年７月公表）に基づき、金融業界全体のインシデント対応能力の更なる向上を図るため、平成29年度、２回目の「金融業界横断的な演習」（Delta Wall Ⅱ）を実施。
  （参考）平成29年度演習においては、中小金融機関の底上げを目的に、参加金融機関の参加枠および対象業態を拡充のうえ、約100先が参加（前回は77先）。
- サイバー攻撃へ的確に対応するためには、演習を通じて、現在の対応態勢が十分であるかを確認するなど、PDCAサイクルを回しつつ、対応能力を向上させることが有効。
- 金融分野のサイバーセキュリティ強化には、官民が一体になって取り組んでいくことが重要であり、平成３０年度も、引き続き演習を実施予定。

（注）本演習は、金融庁と参加金融機関の双方で負担（28年度、29年度）

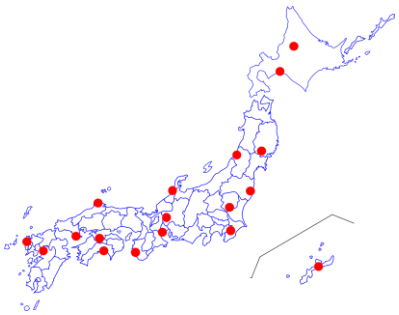


（５）警察庁の取組

警察の施策例

警察における情報技術解析実務を踏まえたサイバーセキュリティ講義

警察庁では、(独)国立高等専門学校機構と連携し、高等専門学校へのサイバーセキュリティ講義を推進。
学生のサイバーセキュリティ分野に対する興味・理解を促進し、人材育成とそれに伴う社会全体の対処能力向上に努めている。



(独)国立高等専門学校機構の情報セキュリティ人材育成プログラムに参加する18の高等専門学校を対象に実施予定。

※ 平成28年度は木更津、高知及び沖縄高専にて、平成29年度は苫小牧及び小山高専にて試行実施。

(例)

平成29年12月15日苫小牧工業高等専門学校(警察庁及び北海道警察情報通信部)

学生参加型のデモ実演

捜査支援を模擬した実習

平成29年12月26日小山工業高等専門学校(警察庁及び東京都警察情報通信部)

基調講演

捜査支援を模擬したCTF

参考２　実務者層・技術者層に相当する役割・専門分野（主にユーザー企業）

文献	役割・専門分野名称	業務内容
産業横断検討会 *1	ISMS 担当	情報システム部門におけるサイバーセキュリティ機能を担う。 （詳細な内容は、*1 において人材定義リファレンスにおける機能との対応表として定義されている）
	システム企画担当	
	サイバーセキュリティ事件・事故担当	
	セキュリティ設計担当	
	構築系サイバーセキュリティ担当	
	運用系サイバーセキュリティ担当	
	CSIRT 担当	
	SOC 担当	
	基幹システム構築担当	
	基幹システム運用担当	
	WEB サービス担当	
	業務アプリケーション担当	
	インフラ担当	
	サーバ担当	
	DB 担当	
	ネットワーク担当	
	サポート・教育担当	
	ヘルプデスク担当	
SecBoK *2	ＩＴ企画部門	社内のＩＴ利用に関する企画・立案を行う。必要に応じて、ＩＴの利用状況の調査・分析等を行う。
	ＩＴシステム部門	社内のＩＴプロジェクトを推進するとともに、アプリケーションシステムの設計、構築、運用、保守等を担当する。
NCA *3	ソリューションアナリスト	自組織の事業計画に合わせてセキュリティ戦略を策定する。現在の状況とあるべき姿の Fit&Gap 分析からリスク評価を行い、ソリューションマップを作成して導入を推進する。

文献	役割・専門分野名称	業務内容
		導入されたソリューションの有効性を確認し、経営層と情報共有を行い、改善計画に反映する。
	リサーチャー	セキュリティイベント、脅威情報、脆弱性情報、攻撃者のプロファイル情報、国際情勢の把握、メディア情報などを収集し、キュレーターに引き渡す。単独機器の分析は行うが、相関的な分析はしない。
	キュレーター	リサーチャーの収集した情報を分析し、その情報を自組織に適用すべきかの選定を行う。リサーチャーと合わせて SOC（セキュリティオペレーションセンター）で実施することが多い。
	脆弱性診断士	OS、ネットワーク、ミドルウェア、アプリケーションが安全かどうかの検査を行い、診断結果の評価を行う。
	セルフアセスメント担当	自組織環境や情報資産の現状分析を行う。平常時の際にアセスメントを実施しておき、インシデント発生時にはアセスメント結果に基づいて影響範囲を特定する。
	インシデントマネージャー	インシデントハンドラーに指示を出し、インシデントの対応状況を把握する。対応履歴を管理するとともにコマンダーへ状況を報告する。
	インシデントハンドラー	インシデントの処理を行う。セキュリティベンダーに処理を委託している場合には指示を出して連携し、管理を行う。状況はインシデントマネージャーに報告する。
NICE 人材フレームワーク *4	情報システムセキュリティ管理者	プログラム、組織、システム等におけるサイバーセキュリティ対策に責任を負う。
	IT プロジェクトマネージャー	情報技術関連プロジェクトを直接管理する。
	セキュアソフトウェア査定者	新規または既存のコンピュータアプリケーション、ソフトウェア、または特殊ユーティリティプログラムのセキュリティを分析し、実用的な結果を提供する。
	システムセキュリティアナリスト	システムセキュリティの統合、テスト、運用、保守の分析と開発を担当する。
	サイバー防衛インシデント対応者	ネットワーク環境またはエンクレーブ内のサイバーインシデントを調査、分析、および対応する。
	脆弱性診断アナリスト	ネットワーク環境内のシステムとネットワークの評価を実施し、それらのシステム/ネットワークが受け入れ可能な構成、特殊又はローカルなポリシーから逸脱している場所を特定する。既知の脆弱性に対する多層防御アーキテクチャの有効性を評価する。

*1：産業横断サイバーセキュリティ人材育成検討会 第一期最終報告書，産業横断サイバーセキュリティ人材育成検討会，2016 年 9 月.

*2：セキュリティ知識分野（SecBoK）人材スキルマップ 2017 年版，JNSA 教育部会，2017 年 9 月.

*3：CSIRT 人材の定義と確保 Ver.1.5，日本コンピュータセキュリティインシデント対応チーム協議会，2017 年 3 月.

*4 ： Cyber-risk Oversight (Director's Handbook Series), National Association of Corporate Directors (NACD), 2017 年.

参考３ 実務者層・技術者層に相当する役割・専門分野（主にベンダー企業）

文献	役割・専門分野名称	業務内容
ITSS+ *1	情報セキュリティデザイン	「セキュリティバイデザイン」の観点から情報システムのセキュリティを担保するためのアーキテクチャやポリシーの設計を行うとともに、これを実現するために必要な組織、ルール、プロセス等の整備・構築を支援する。
	情報セキュリティアドミニストレーション	組織としての情報セキュリティ戦略やポリシーを具体的な計画や手順に落とし込むとともに、対策の立案や実施（指示・統括）、その見直し等を通じて、自組織または受託先における情報セキュリティ対策の具体化や実施を統括する。また、利用者に対する情報セキュリティ啓発や教育の計画を立案・推進する。
	情報セキュリティアナリシス	情報セキュリティ対策の現状に関するアセスメントを実施し、あるべき姿とのギャップ分析をもとにリスクを評価した上で、自組織または受託先の事業計画に合わせて導入すべきソリューションを検討する。導入されたソリューションの有効性を確認し、改善計画に反映する。
	セキュア開発管理	情報システムや製品に関するリスク対応の観点に基づき、機能安全を含む情報セキュリティの側面から、企画・開発・製造・保守などにわたる情報セキュリティライフサイクルを統括し、対策の実施に関する責任をもつ。
	脆弱性診断	ネットワーク、OS、ミドルウェア、アプリケーションがセキュアプログラミングされているかどうかの検査を行い、診断結果の評価を行う。
	CSIRT キュレーション	情報セキュリティインシデントへの対策検討を目的として、セキュリティイベント、脅威や脆弱性情報、攻撃者のプロファイル、国際情勢、メディア動向等に関する情報を収集し、自組織または受託先に適用すべきかの選定を行う。
	インシデントハンドリング	自組織または受託先におけるセキュリティインシデント発生直後の初動対応（被害拡大防止策の実施）や被害からの復旧に関する処理を行う。セキュリティベンダーに処理

文献	役割・専門分野名称	業務内容
		を委託している場合には指示を出して連携する。情報セキュリティインシデントへの対応状況を管理し、CSIRT コマンドのタスクを担当する者へ報告する。
	サイバー防衛インシデント対応者	ネットワーク環境またはエンクレーブ内のサイバーインシデントを調査、分析、および対応する。
	脆弱性診断アナリスト	ネットワーク環境内のシステムとネットワークの評価を実施し、それらのシステム/ネットワークが受け入れ可能な構成、特殊又はローカルなポリシーから逸脱している場所を特定する。既知の脆弱性に対する多層防御アーキテクチャの有効性を評価する。

*1：ITSS＋，独立行政法人情報処理推進機構（IPA），2017 年 4 月.

参考４　各省庁の人材育成施策に関する全体像の整理

各省庁の人材育成施策に関する全体像の整理

				育成対象																					形式		教育内容					基礎知識		
				組織							学び直しを含む					学生																		
						民間企業																												
コード	実施主体	名称	年齢	自治体	独立行政法人		重要インフラ事業者	高等教育機関	その他	詳細	経営層	戦略マネジメント機能担当	システム担当	システム構築担当	ベンダー企業のセキュリティ専門職	小中高校生	高専生	大学生	大学院生（非社会人）	その他	詳細	連携	人数 ※年間の平均値	期間（時間） ※1人・1社/1年間当たり	座学、講義（試験を含む）	演習	技術（防御）	技術（攻撃）	ビジネス	マネジメント	オペレーション	計算機科学	システム管理	マネジメント
1-3	（独）NICT	SecHack365	～25					✓	✓							✓	✓	✓	✓	✓	25歳以下であれば社会人も排除しない	2-3	40	1840（概算）	✓	✓	✓	✓	✓			✓		
2-3	（独）国立高等専門学校機構	高等専門学校における情報セキュリティ人材の育成	15～22					✓									✓					1-1 1-3 2-4 3-3 5-2			✓	✓	✓	✓						
2-4	東北大学（文部科学省補助事業）	enPiT事業による大学（学部）の人材育成拠点整備	20～22					✓										✓				2-3	200	105～150	✓	✓	✓	✓				✓		
3-3	（独）IPA	セキュリティキャンプ	～22					✓	✓							✓		✓				2-3	80	40	✓	✓	✓	✓	✓			✓		
5-2	警察庁、管区警察局、東京都・北海道警察情報通信部 ※警察庁はH28,29のみ	警察における情報技術解析実務を踏まえたサイバーセキュリティ講義	～22					✓									✓					2-3	【H28・29試行実績】28 【H30見込み】100	【H28・29試行実績】9 【H30見込み】6	✓	✓	✓	✓						
2-7	放送大学	BS232ch、オンライン、面接授業		✓	✓	✓	✓	✓			✓	✓					✓	✓	✓				750（想定）	920（概算）	✓		✓	✓		✓	✓			
2-8	放送大学	BS231ch		✓	✓	✓	✓	✓			✓	✓					✓	✓	✓					1	✓									
3-5	（独）IPA産業サイバーセキュリティセンター	CISO向け短期プログラム	40～			✓	✓				✓	✓								✓	CISO,CISO補助者		90	20	✓	✓				✓	✓			✓
4-1	金融庁	Delta Wall 演習				✓	✓				✓	✓	✓										1200	4		✓				✓	✓			
5-1	都道府県警察、管区警察局（都道府県情報通信部）	共同対処訓練 ※ 各回の目的に応じて参加組織、育成対象等は異なる。		✓	✓	✓	✓	✓	✓	オリパラ関係機関等	✓	✓	✓	✓						✓	インフラ運用担当者等		5600	3	✓	✓	✓	✓			✓		✓	
2-2	情報セキュリティ大学院大学（文部科学省補助事業）	enPiT-Pro事業による社会人学び直し拠点整備		✓	✓	✓	✓				✓	✓	✓	✓	✓								35（メインコース） 200（クイックコース）	120（メインコース） 60（クイックコース）	✓	✓	✓	✓		✓	✓	✓	✓	✓
6-1	NISC	重要インフラ分野横断演習		✓	✓		✓					✓	✓	✓									2000	8		✓					✓			
3-4	（独）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	30前後			✓	✓					✓	✓		✓					✓	将来のCISO候補生	3-1	80	1840	✓	✓	✓	✓		✓	✓	✓	✓	
3-2	（独）IPA	セキュリティマネジメント試験		✓	✓	✓	✓	✓				✓	✓	✓				✓	✓				24410	試験 3	✓					✓	✓		✓	✓
3-1	（独）IPA	情報処理安全確保支援士		✓	✓	✓	✓	✓				✓	✓	✓	✓			✓	✓			3-4	6994	試験 5	✓		✓	✓		✓	✓	✓	✓	
1-1	（独）NICT	CYDER演習		✓	✓	✓	✓						✓	✓								2-3	3000	9	✓	✓					✓	✓	✓	
2-1	東京電機大学大学院（文部科学大臣認定制度）	Cysec（職業実践力育成プログラム（BP）に認定）		✓	✓	✓	✓				✓		✓	✓					✓	✓	ICTシステム管理者等		40	135	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
1-2	（独）NICT	サイバーコロッセオ							✓	オリパラ組織委員会等			✓	✓	✓								60	初級 9 準上級 16	✓	✓	✓	✓			✓	✓	✓	
2-5	文部科学省	専修学校職業実践専門課程	18～					✓																	✓	✓	（各専修学校の教育内容による）							
2-6	文部科学省	情報モラル教育・情報教育の推進	～18						✓	小・中・高等学校						✓									✓	✓								

参考５　戦略マネジメント層に相当する人材層に期待される知識・スキル

分類			国内事例				米国事例	
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			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」	東京電機大 CySec 情報セキュリティマネジメントとガバナンス	NICE 人材フレームワーク "Program Manager"	MIT スローン校 MBA コース “Cybersecurity”
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　　※：受講の前提知識

*1：ITSS＋，独立行政法人情報処理推進機構（IPA），2017 年 4 月.

*2：平成 28 年度理工系プロフェッショナル教育推進委託事業 工学分野における理工系人材育成の在り方に関する調査研究（情報セキュリティ人材育成に関する調査研究）成果報告書，文部科学省（委託先：学校法人岩崎学園情報セキュリティ大学院大学），2017 年 3 月.

*3：東京電機大学国際化サイバーセキュリティ学特別コース（CySec）[5MG]情報セキュリティマネジメントとガバナンス, 2017 年度

*4：Special Publication 800-181 National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, NIST, 2017 年 8 月.

*5：MBA コース 2017 年春期科目“Cybersecurity”, MIT Sloan school.

参考 6　すべての企業において戦略マネジメント層を担う人材に求められる知識・スキル

プロセス（ISO 31000 項目抜粋）			サイバーセキュリティ関連スキル（①～⑤は対応する講義回）	外部委託先に求める役割	ITSS+専門分野
リスクマネジメント	コミュニケーション及び協議	異なる領域の専門知識の収集	・サイバーセキュリティに関する脅威や対策一般についての情報収集に関するスキル② ・専門家とのサイバーセキュリティに関するコミュニケーションスキル④	（外部委託を想定しない）	・情報リスクストラテジ ・CSIRT リエゾン
		多様なステークホルダの見解の考慮	・ユーザーがシステムやサービスに求める機能要件の理解①	（外部委託を想定しない）	
		組織内外との継続的協議	・同業他社のセキュリティレベルについて情報収集し、自社レベルと比較できるスキル（①～⑤の総合力） ・関係する部署や外部機関の把握、関係構築及び維持に関するスキル ・持続的な連絡体制の構築・維持に関するスキル④	（外部委託を想定しない）	

プロセス（ISO 31000 項目抜粋）			サイバーセキュリティ関連スキル （①～⑤は対応する講義回）	外部委託先に求める役割	ITSS+専門分野
	組織の状況の確定	考慮すべき外部要因の確定	・サイバーセキュリティの関連法令・規格・ガイドライン等の理解③	（外部委託を想定しない）	・情報リスクストラテジ
		考慮すべき内部要因の確定	・組織におけるビジネスモデル、ビジネス上のプライオリティ、経営層の関心事項並びに IT 利活用状況の理解	（外部委託を想定しない）	
		リスクマネジメントプロセスの全体管理・調整	・サイバーセキュリティに関連したリスクマネジメントの手法に関する理解④ ・サイバーセキュリティ対策実施に伴う組織内調整に関するスキル④	（外部委託を想定しない）	
		リスクに関する許容レベルの設定	・サイバーセキュリティリスクが組織にもたらす影響についての理解④	（外部委託を想定しない）	
	リスクアセスメント	リスクの特定	・組織の目的についての理解 ・組織のビジネスモデル及びそれを実現するための仕組みの理解 ・サイバーセキュリティをとりまく最新の脅威についての理解②	・リサーチャー	・情報セキュリティアナリシス
		リスクの分析	・脅威、脆弱性、対策の有効性についての理解② ・業務プロセスの分析と標準化に関するスキル ・リスク分析のフレームワークに関する理解④	・ソリューションアナリスト ・脆弱性診断士	
		リスクの評価	・脅威が組織にどのような影響を及ぼすかの評価に関するスキル②	・ソリューションアナリスト ・コンサルタント	
	リスク対応	リスク対応策の選定	・選択し得る対策についての情報収集に関するスキル② ・対策についての費用対効果も含めた評価に関するスキル⑤ ・関連法令・規格・ガイドライン等との整合性確保に関するスキル③	・ソリューションアナリスト ・キュレーター	・情報リスクストラテジ ・情報セキュリティデザイン ・CSIRT キュレーション

プロセス（ISO 31000 項目抜粋）			サイバーセキュリティ関連スキル （①～⑤は対応する講義回）	外部委託先に求める役割	ITSS+専門分野
		対応計画の準備及び実践	・対策が有効に機能する環境や条件についての理解②	（外部委託を想定しない）	
			・自社要員にて行うべき対応と外部委託が可能な対応の違いについての理解	（外部委託を想定しない）	
			・外部委託先において対策を遵守させるための実践に関するスキル	（外部委託を想定しない）	
	意思決定への適用*	記録を通じた明示	・意思決定者が理解できるようにリスクを可視化するスキル④	（外部委託を想定しない）	・情報リスクストラテジ
	アカウンタビリティ*	役割及び責任の明確化	・サイバーセキュリティ対策を担う要員の役割定義に関するスキル④	（外部委託を想定しない）	
リスクマネジメント	モニタリング及びレビュー	リスクの監視	・監視結果からインシデントの発生可能性を判断するスキル②	・ソリューションアナリスト	・情報セキュリティアナリシス
		リスクの変化や新リスクの検出	・サイバーセキュリティ分野を対象とするリスクセンス ・サイバーセキュリティのトピックスの収集に関するスキル②	・リサーチャー	
		リスクマネジメントの監査	・ルールの遵守状況についての監査に関するスキル④	・情報セキュリティ監査人	・情報セキュリティ監査
	継続的改善*	組織のパフォーマンス到達目標を用いた改善	・モニタリング結果に基づく改善可能箇所の検出に関するスキル ・改善案の策定と組織内合意形成に関するスキル④	・コンサルタント	・情報リスクストラテジ
	統治体制への統合*	組織の方針への反映	・事業リスクの一部としてサイバーセキュリティに関するリスクを包括的に管理するためのスキル④⑤	（外部委託を想定しない）	
	緊急時対応への事前の備え	対応手順の策定及び準備	・インシデント対応手順に反映すべき内容についての理解④	・コンサルタント	・CSIRT コマンド ・CSIRT キュレーション
		緊急時実行組織の整備	・組織に求められる CSIRT の要件に関する理解④	（外部委託を想定しない）	

プロセス（ISO 31000 項目抜粋）			サイバーセキュリティ関連スキル （①～⑤は対応する講義回）	外部委託先に求める役割	ITSS+専門分野
		緊急時対策及び復旧対策の評価	・インシデント対応の実績の把握と評価を行うスキル④	・ソリューションアナリスト	

＊：ISO 31000 にて「高度リスクマネジメント」に定義されているプロセス

参考７　IT ビジネス企業において戦略マネジメント層を担う人材に求められる知識・スキル

プロセス		サイバーセキュリティ関連スキル （①～⑤は対応する講義回）	外部委託先に求める役割	ITSS+専門分野
事業戦略	事業の企画・立案	・企画している事業に対し、犯罪者や不正を意図する者がどのような行為を企てるかを想定するスキル② ・企画している事業を遂行する上での影響が見込まれるサイバーセキュリティ関連リスクの洗い出し、影響評価に関するスキル④	・コンサルタント	・情報リスクストラテジ
	市場調査（顧客ニーズ調査、需要予測、競合分析等）	・需要等を踏まえたサイバーセキュリティ関連リスクの定量的評価に関するスキル④ ・サイバーセキュリティに関する市場ニーズの把握に関するスキル⑤ ・競合企業におけるサイバーセキュリティ対策の実施状況の調査、推定に関するスキル	・コンサルタント	・情報リスクストラテジ
	収益計画策定（マネタイズモデル、収益予測、投資計画等）	・事業計画に応じたサイバーセキュリティ対策の初期投資、ランニングコスト等の概算に関するスキル⑤	・コンサルタント	・情報リスクストラテジ
	事業モデル策定（実施体制、内部化・外部化、パートナー選定、連携計画等）	・事業の実施モデルに応じたサイバーセキュリティ対策の選定に関するスキル②	・コンサルタント ・ソリューションアナリスト	・情報セキュリティアドミニストレーション
	事業実施戦略策定（実現方式・運用方針等）	・実現方式に応じた適切なサイバーセキュリティ対策の選定に関するスキル② ・対策を通じたリスクの低減、移転等の効果の評価に関するスキル④	・コンサルタント ・ソリューションアナリスト	・情報セキュリティアドミニストレーション

		・サイバーセキュリティ対策の費用対効果分析に関するスキル⑤		

参考８　システム担当に求められる知識･スキル：ITSS+におけるシステム担当人材に求められる知識･スキル（『ITSS＋』（独立行政法人情報処理推進機構（IPA），2017 年４月）より抜粋）

スキル項目コード	スキルカテゴリ	スキル分類	スキル項目	情報セキュリティデザイン	情報セキュリティアドミニストレーション	情報セキュリティアナリシス
S110010060	メソドロジ	（戦略）　市場機会の評価と選定	最新技術動向把握の手法	◎		
S110050030			技術開発計画	○		
S110050040			技術開発戦略の立案	○		
S110060010		（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	◎	○	
S110060030			ソリューションビジネス	◎	○	
S110060040			業務プロセス	◎	○	
S110060050			現行システムの調査・分析手法	◎	○	
S110060060			事業戦略の把握・分析の手法	◎	○	
S110060070			情報システム戦略	◎	○	
S110080010		（戦略）　業務動向把握手法	業務動向の把握手法	◎	◎	
S120010010		（企画）　システム企画立案手法	システム化計画	◎		
S120010020			システム企画立案手法	◎	○	
S120010030			ソリューション提案手法		○	
S120010040			技術問題解決手法	◎		
S120010050			調達計画・実施	◎		
S120020020		（企画）　セールス事務管理手法	契約事務手法		○	

スキル項目コード	スキルカテゴリ	スキル分類	スキル項目	情報セキュリティデザイン	情報セキュリティアドミニストレーション	情報セキュリティアナリシス
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） 非機能要件設計手法	プラットフォーム要件定義手法	◎		
S120040020			システム基盤の非機能要件設計	◎		
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チャ設計手法	◎		
S130010030			インダストリパッケージ設計・開発手法	◎		
S130010040			インフラストラクチャアーキテクチャ設計手法	◎		○
S130010050			データアーキテクチャ設計手法	◎		
S130020010		（実装） ソフトウェアエンジニアリング手法	セキュリティ実装手法	◎		
S130020020			ソフトウェアデザイン手法	◎		
S130020030			ソフトウェアのモデリング手法	◎		
S130020040			ソフトウェア開発手法	◎		○
S130020050			ソフトウェア製作手法	◎		○
S130020060			ソフトウェア設計の表記手法	◎		
S130020090			ソフトウェア設計手法	◎		
S130060010		（実装） 業務パッケージ活用手法	業務パッケージ適用手法		◎	
S130060020			業務パッケージ導入手法		◎	
S130090010		（実装） 見積り手法	規模の見積手法	◎		
S140020020			サービス移行手法			○
S140040010		（利活用） サービスの運用	サービスの運用手法		○	○
S140040020			システム運用管理手法		○	○

スキル項目コード	スキルカテゴリ	スキル分類	スキル項目	情報セキュリティデザイン	情報セキュリティアドミニストレーション	情報セキュリティアナリシス
S140040040			運用オペレーション手法		○	
S140040050			運用支援ツール手法		○	○
S150010010		（支援活動） 品質マネジメント手法	テスト技術・手法	◎		○
S150010020			テストのマネジメント手法	◎		○
S150010030			品質レビュー手法	◎		
S150010040			検査のマネジメント手法	◎		○
S150010050			品質マネジメント手法	◎		○
S150010060			品質に関する基礎	◎		○
S150010070			セキュリティ品質に関する手法	◎	◎	◎
S150010080			ユーザービリティ品質に関する手法	◎		
S150010090			セーフティ品質に関する手法	◎		
S150010100			法的権利・法的責任のマネジメント手法	◎		
S150010110			品質要求分析手法	◎		○
S150010120			品質マネジメントシステム構築手法	◎		
S150010130			品質改善に関する手法			○
S150010140			品質管理に関する手法	◎		○
S150010150			品質計画に関する手法			○
S150010160			品質保証に関する手法	◎		○
S150010170			品質測定・評価手法	◎		○
S150010180			品質分析・評価手法	◎		○
S150030010		（支援活動） リスクマネジメント手法	リスク管理手法	○	◎	○
S150030020			情報セキュリティ管理手法	◎	◎	○
S150040010		（支援活動） IT ガバナンス	IT ガバナンス手法	○	◎	
S150040020			内部統制	○	◎	○
S150070010		（支援活動） ファシリティマネジメント手法	ファシリティマネジメント		○	
S150080010		（支援活動） 事業継続計画	BCP 策定手法		◎	

スキル項目コード	スキルカテゴリ	スキル分類	スキル項目	情報セキュリティデザイン	情報セキュリティアドミニストレーション	情報セキュリティアナリシス
S150080020			災害対策管理手法		◎	
S150100010		（支援活動） 標準化・再利用手法	ソフトウェア開発プロセスの標準化手法	◎		
S150100020			ソフトウェアエンジニアリングの標準化手法	◎		
S150120050		（支援活動） 情報セキュリティ	リスク分析手法	◎	◎	◎
S150120060			情報セキュリティポリシー策定手法	○	◎	◎
S150130010		（支援活動） チェンジマネジメント手法	協働の管理手法	◎		
S150130020			ビジネスソリューション変更管理手法	◎		
S150130030			ソリューション価値測定手法	◎		
S210010010	テクノロジ	（システム） ソフトウェアの基礎技術	ソフトウェア工学			○
S210010020			ソフトウェアの標準化			○
S210010030			ソフトウェアエンジニアリングツール・開発技術			○
S210010040			ソフトウェア構築の基礎知識			○
S210010100			オープンソースソフトウェア			○
S210010110			テスティング			○
S210010120			ソフトウェア品質			○
S210020010		（システム） ソフトウェアの構築技術	システム開発の概念と方法論			○
S210020020			システム開発のアプローチ			○
S210020030			ソフトウェア要件定義			○
S210020040			ソフトウェア方式設計・ソフトウェア詳細設計			○
S210020050			アプリケーション方式設計手法			○
S210020070			リアルタイムシステム設計			○
S210020080			ソフトウェア開発のフォールトトレランス			○
S210020090			ソフトウェア構築			○

スキル項目コード	スキルカテゴリ	スキル分類	スキル項目	情報セキュリティデザイン	情報セキュリティアドミニストレーション	情報セキュリティアナリシス
S210020100			ソフトウェア結合・ソフトウェア適格性確認テスト			○
S210020110			受入れ支援			○
S210020140			構築品質			◎
S210020150			テスティングツール			◎
S210020160			セキュアプログラミング技法	◎		◎
S210020170			セキュアプログラミング技法（データベース）	◎		◎
S210030030		（システム） ソフトウェアの利用技術	ソフトウェアの進化や保守			○
S210160010		（システム） ネットワークの基礎技術	ネットワーク	○	○	○
S210160020			ネットワークコンピューティング	○	○	○
S210160030			ネットワークシステムの技術動向	○	○	○
S210160040			ネットワーク標準	○	○	○
S210160050			ネットワーク方式	○	○	○
S210160060			通信プロトコル	○	○	○
S210160070			データ通信と制御		○	○
S210180010		（システム） ネットワークの利用技術	ネットワーク管理	○	○	
S210180020			ネットワーク応用	○	○	
S210180030			ネットワーク製品知識	○	○	
S210180040			業界固有のセキュリティ要件、事例	◎	○	○
S210180050			ネットワークシステムの評価	○	○	○
S210180060			テレコミュニケーション	○		
S210190010		（システム） クラウドコンピューティングの基礎技術	クラウドコンピューティング基礎	◎	○	○
S210200010			クラウドデータベース技術	◎		
S210200020			クラウド構築技術	◎		
S210200030			クラウドアプリケーション実装技術	◎		
S210200040			仮想マシンゲストのセキュリティ		○	○

スキル項目コード	スキルカテゴリ	スキル分類	スキル項目	情報セキュリティデザイン	情報セキュリティアドミニストレーション	情報セキュリティアナリシス
S210210010		（システム） クラウドコンピューティングの利用技術	インタークラウド技術		○	○
S210210020			クラウドコンピューティング利用	◎	○	○
S210210030			クラウドシステムの監視技術	◎	○	○
S220010010		（開発） システムアーキテクティング技術	システム要件定義	◎	○	○
S220010020			システムインテグレーションとアーキテクチャ	◎	○	○
S220010030			アプリケーション共通基盤要件定義手法	◎		○
S220010040			アプリケーション共通基盤設計手法	◎		
S220010050			IT 基盤構築プロセス	◎		○
S220010060			システム間連携技術	◎		
S220010070			システム方式設計	◎		
S220010100			オブジェクト指向技術	○		
S220020010		（開発） システム開発管理技術	開発プロセス・手法	○		
S220020020			開発環境管理	○		
S230020080			システムの監視			◎
S230020090			稼働状況管理			◎
S230030050		（保守・運用） システム保守・運用・評価	アプリケーションシステムの受け入れ			○
S230030060			システム運用管理要件定義	○		
S230030070			システム運用管理設計	○		
S230030080			システム運用方式技法	○	○	○
S230030090			システムの投資評価技法	○		
S230030100			システム管理計画	○	○	○
S230030110			システム管理技術	○	○	○
S230030120			システム保守基準	○		○
S230030140			システム管理製品		○	○
S230030150			運用管理ソフト製品		○	○

スキル項目コード	スキルカテゴリ	スキル分類	スキル項目	情報セキュリティデザイン	情報セキュリティアドミニストレーション	情報セキュリティアナリシス
S230030170			運用システムの改善		○	○
S230030180			運用に関するシステム評価		○	○
S230030190			性能管理		○	
S230030200			障害時運用方式	○	○	
S230030210			災害対策	○	○	
S230030230			保守技術			○
S230030240			メンテナンス			○
S230060040			信頼性、可用性、保守性	○	○	
S230060050			耐震安全確保	○	○	
S230060060			物理ネットワーク（通信ネットワーク）の設計	○	○	
S230060070			防災防犯設備設計	○	○	
S230060100			品質管理の知識	○	○	
S230070010		（保守・運用）　サポートセンター基盤技術	インシデント管理システム	○	○	
S240010010		非機能要件（可用性、性能・拡張性）	非機能要件の基礎	○		○
S240010020			負荷分散と可用性の設計	○		
S240010030			システム信頼性、性能設計	○		
S240010040			高信頼性システムの設計	○		
S240010050			データベースシステムの信頼性設計	○		
S240020010		（非機能要件）　セキュリティの基礎技術	情報セキュリティ	◎	◎	◎
S240020020			情報保証と情報セキュリティ	◎	◎	◎
S240020030			情報倫理とセキュリティ	◎	◎	○
S240020040			セキュリティ・アーキテクチャ技術	◎	○	○
S240020050			アプリケーションセキュリティ	◎	◎	◎
S240020060			情報プラットフォームのセキュリティ技術	◎	◎	◎
S240020070			ネットワークのセキュリティリスク	◎	◎	◎

スキル項目コード	スキルカテゴリ	スキル分類	スキル項目	情報セキュリティデザイン	情報セキュリティアドミニストレーション	情報セキュリティアナリシス
S240020080			暗号技術	◎	○	○
S240020090			セキュリティと個人情報	◎	◎	◎
S240020100			保証、信用、信頼のメカニズム	◎	○	
S240020110			セキュリティ技術の理解と活用	◎	◎	◎
S240030010		（非機能要件）　セキュリティの構築技術	セキュリティ方針の策定	○	◎	○
S240030020			セキュリティ対策基準の策定	○	◎	○
S240030030			情報セキュリティ対策	◎	◎	○
S240030040			セキュリティ実装技術	◎	◎	○
S240030050			セキュリティシステムの計画策定		◎	○
S240030060			セキュリティシステムの要件定義	◎	◎	○
S240030070			セキュリティシステムの設計	◎	◎	○
S240030080			セキュリティシステムの実装、検査	◎	◎	○
S240030090			コンピュータ・フォレンジクス（証拠保全追跡）		○	○
S240040010		（非機能要件）　セキュリティの利用技術	セキュリティシステムの運用管理	○	◎	○
S240040020			セキュリティシステム導入支援		◎	○
S240040030			システム運用・保守技術（セキュリティ）	○	◎	◎
S240040040			セキュリティ障害（事件事故/インシデント）管理	○	◎	◎
S240040050			情報セキュリティ管理	○	◎	○
S240040060			情報セキュリティ監査の実施・支援	○	◎	○
S240040070			セキュリティ技術評価	○	◎	◎
S240040080			セキュリティの分析	○	◎	◎
S240040090			セキュリティの見直し（セキュリティシステムの評価と改善）	○	◎	○
S240040100			コンテンツセキュリティ技術		◎	○
S310020050	関連知識	企業活動	情報セキュリティ監査			○

スキル項目コード	スキルカテゴリ	スキル分類	スキル項目	情報セキュリティデザイン	情報セキュリティアドミニストレーション	情報セキュリティアナリシス
S310020060			ビジネスプロセスマネジメント	○		
S310030010		法規・基準・標準	セキュリティ関連法規	○	◎	○
S310030020			その他の法律・ガイドライン・技術者倫理	○	◎	○
S310030050			標準化関連	◎		

参考９　システム担当に求められる知識・スキル：SecBoK2017 におけるシステム担当人材に求められる知識・スキル（『セキュリティ知識分野（SecBoK）人材スキルマップ 2017 年版』（JNSA 教育部会, 2017 年９月）より抜粋）

分野	大項目	中項目	小項目
基礎	ICT 基礎	データ構造	適切な情報基盤がもつ性質及び機能に関する知識
		システム開発	システム開発のコンセプトに関するスキル
		システム運用	システム運用のコンセプトに関するスキル
		エンタープライズアーキテクチャ	エンタープライズ IT アーキテクチャに関する知識
			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
	工学基礎		技術トレンドデータの妥当性を決定する能力
	ビジネス基礎		関連する情報構造の状態と機能に関する知識
			組織のコアビジネスとミッションの原理に関する知識
			サプライチェーンリスクの削減のための輸出管理規制と責任機関に関する知識
セキュリティ基礎	総論		機密性、完全性、可用性、認証及び否認防止に関連する情報保証の原理と組織要件に関する知識
			サイバーセキュリティ問題に関する外部組織と学術機関に関する知識
セキュリティマネジメント	総論		IT サプライチェーンのセキュリティ/リスクマネジメントのポリシー、要求事項および手続きに関する知識
ネットワークセキュリティ	脆弱性診断		コンピュータネットワーク防御（CND）と脆弱性評価ツール（オープンソースツールとその能力を含む）に関する知識

システムセキュリティ	総論		システムとアプリケーションのセキュリティ上の脅威と脆弱性（例： バッファオーバフロー、モバイルコード、クロスサイトスクリプティング、PL/SQL 及びインジェクション、競合状態、隠れチャネル、リプレイ、リターン指向攻撃、悪意のあるコード）に関する知識
セキュアシステム設計・構築	総論		安全、パフォーマンスおよび信頼性の観点から局所固有となるシステムの要件（例： 標準的な IT を使えない重要インフラシステム）に関する知識
セキュリティ運用	総論		新興の情報技術と情報セキュリティ技術に関する知識
			リスク脅威の評価に関する知識
サイバー攻撃手法	総論		攻撃者に悪用される可能性のある新興のコンピュータベースの技術に関する知識
法・制度・標準	総論		技術トレンドを識別するために有用な業界の指標に関する知識
			活動に影響を及ぼす技術的及び法的なトレンドの追跡と解析に関するスキル
			実施する作業に関する適用法、行政機関のガイドラインおよび/または行政/犯罪に関する法的ガイドラインおよび手続きに関する知識
			重要インフラに影響を及ぼす作業に関連する法律、ポリシー、手続きまたはガバナンスに関する知識

参考 10 システム構築担当に求められる知識・スキル：ITSS+におけるシステム構築・運用に求められる知識・スキル（『ITSS＋』（独立行政法人情報処理推進機構（IPA），2017 年４月）より抜粋）

スキル項目コード	スキルカテゴリ	スキル分類	スキル項目	セキュア開発管理	脆弱性診断	CSIRT キュレーション	インシデントハンドリング
S110010060	メソドロジ	（戦略） 市場機会の評価と選定	最新技術動向把握の手法	◎		◎	
S110050010		（戦略） 製品・サービス開発戦略	顧客環境分析手法	○			
S110050020			製品開発戦略手法	○			
S110050030			技術開発計画	○			
S110050040			技術開発戦略の立案	○			
S110060010		（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	◎			
S110060030			ソリューションビジネス	◎			

スキル項目コード	スキルカテゴリ	スキル分類	スキル項目	セキュア開発管理	脆弱性診断	CSIRT キュレーション	インシデントハンドリング
S110060040			業務プロセス	◎			
S110060050			現行システムの調査・分析手法	◎			
S110060060			事業戦略の把握・分析の手法	◎			
S110060070			情報システム戦略	◎			
S110080010		（戦略） 業務動向把握手法	業務動向の把握手法			◎	
S120010020		（企画） システム企画立案手法	システム企画立案手法	○			
S120010030			ソリューション提案手法	○			
S120010040			技術問題解決手法	◎			
S120020020			契約事務手法	○			
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） 非機能要件設計手法	プラットフォーム要件定義手法	◎		○	
S120040020			システム基盤の非機能要件設計	◎		○	
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チャ設計手法	○			
S130010030			インダストリパッケージ設計・開発手法	○			
S130010040			インフラストラクチャアーキテクチャ設計手法	○		○	
S130010050			データアーキテクチャ設計手法	○			
S130020010		（実装） ソフトウェアエンジニアリング手法	セキュリティ実装手法	◎			
S130020020			ソフトウェアデザイン手法	◎			
S130020030			ソフトウェアのモデリング手法	◎			
S130020040			ソフトウェア開発手法	◎			
S130020050			ソフトウェア製作手法	◎			

スキル項目コード	スキルカテゴリ	スキル分類	スキル項目	セキュア開発管理	脆弱性診断	CSIRT キュレーション	インシデントハンドリング
S130020060			ソフトウェア設計の表記手法	◎			
S130020070			開発プロセス設定手法	◎			
S130020080			開発環境設計手法	◎			
S130020090			ソフトウェア設計手法	◎			
S130060010		（実装） 業務パッケージ活用手法	業務パッケージ適用手法			◎	
S130060020			業務パッケージ導入手法			◎	
S130100010		（実装） プロジェクトマネジメント手法	プロジェクトマネジメント	◎			
S130100020			プロジェクト統合マネジメント	◎			
S130100030			プロジェクトコストマネジメント	◎			
S130100040			プロジェクトコミュニケーションマネジメント	◎			
S130100050			プロジェクトスコープマネジメント	◎			
S130100060			プロジェクトステークホルダマネジメント	◎			
S130100070			プロジェクトタイムマネジメント	◎			
S130100080			プロジェクトリスクマネジメント	◎			
S130100090			プロジェクト資源マネジメント	◎			
S130100100			プロジェクト調達マネジメント	◎			
S130100110			プロジェクト品質マネジメント	◎			
S140020010		（利活用） サービスの設計・移行	サービスの設計手法	○			
S140020020			サービス移行手法	○		○	
S140030010		（利活用） サービスマネジメントプロセス	サービス提供プロセス遂行手法	○			
S140030020			解決プロセス遂行手法	○			
S140030030			統合的制御プロセス遂行手法	○			
S140030040			関係プロセス遂行手法	○			
S140040010		（利活用） サービスの運用	サービスの運用手法			○	○
S140040020			システム運用管理手法			○	○

スキル項目コード	スキルカテゴリ	スキル分類	スキル項目	セキュア開発管理	脆弱性診断	CSIRT キュレーション	インシデントハンドリング
S140040050			運用支援ツール手法			○	○
S150010010		（支援活動） 品質マネジメント手法	テスト技術・手法	◎	◎	○	
S150010020			テストのマネジメント手法	◎	◎	○	
S150010030			品質レビュー手法	◎			
S150010040			検査のマネジメント手法	◎	◎	○	
S150010050			品質マネジメント手法	◎	○	○	
S150010060			品質に関する基礎	◎	○	○	
S150010070			セキュリティ品質に関する手法	◎	○	◎	
S150010080			ユーザービリティ品質に関する手法	◎			
S150010090			セーフティ品質に関する手法	◎			
S150010100			法的権利・法的責任のマネジメント手法	◎			
S150010110			品質要求分析手法	◎	○	○	
S150010120			品質マネジメントシステム構築手法	◎			
S150010130			品質改善に関する手法	◎	○	○	
S150010140			品質管理に関する手法	◎	○	○	
S150010150			品質計画に関する手法	◎	○	○	
S150010160			品質保証に関する手法	◎	○	○	
S150010170			品質測定・評価手法	◎	○	○	
S150010180			品質分析・評価手法	◎	○	○	
S150030010		（支援活動） リスクマネジメント手法	リスク管理手法	◎	○	○	
S150030020			情報セキュリティ管理手法	◎	○	○	
S150100010		（支援活動） 標準化・再利用手法	ソフトウェア開発プロセスの標準化手法	◎			
S150100020			ソフトウェアエンジニアリングの標準化手法	◎			
S150120050		（支援活動） 情報セキュリティ	リスク分析手法	◎	◎	◎	
S150120060			情報セキュリティポリシー策定手法	○		○	
S210010010	テクノロジ		ソフトウェア工学	◎			

スキル項目コード	スキルカテゴリ	スキル分類	スキル項目	セキュア開発管理	脆弱性診断	CSIRT キュレーション	インシデントハンドリング
S210010020		（システム） ソフトウェアの基礎技術	ソフトウェアの標準化	◎			
S210010030			ソフトウェアエンジニアリングツール・開発技術	◎			
S210010040			ソフトウェア構築の基礎知識	◎			
S210010050			ソフトウェア設計の基礎知識	◎			
S210010060			プログラミング基礎技術	◎			
S210010070			プログラミング	◎			
S210010080			プログラム言語	◎			
S210010090			その他の言語	◎			
S210010100			オープンソースソフトウェア	◎			
S210010110			テスティング	◎			
S210010120			ソフトウェア品質	◎			
S210020010		（システム） ソフトウェアの構築技術	システム開発の概念と方法論	◎			
S210020020			システム開発のアプローチ	◎			
S210020030			ソフトウェア要件定義	◎			
S210020040			ソフトウェア方式設計・ソフトウェア詳細設計	◎			
S210020050			アプリケーション方式設計手法	◎			
S210020060			アプリケーション設計	◎			
S210020070			リアルタイムシステム設計	◎			
S210020080			ソフトウェア開発のフォールトトレランス	◎			
S210020090			ソフトウェア構築	◎			
S210020100			ソフトウェア結合・ソフトウェア適格性確認テスト	◎			
S210020110			受入れ支援	◎			
S210020120			開発ツール	◎	○		
S210020130			再利用のための構築	◎			

スキル項目コード	スキルカテゴリ	スキル分類	スキル項目	セキュア開発管理	脆弱性診断	CSIRT キュレーション	インシデントハンドリング
S210020140			構築品質	◎	◎	○	
S210020150			テスティングツール	◎	◎		
S210020160			セキュアプログラミング技法	◎	◎		
S210020170			セキュアプログラミング技法（データベース）	◎	◎		
S210030010		（システム） ソフトウェアの利用技術	アプリケーション計画	○			
S210030020			既存ソフトウェアの把握技法	○			
S210030030			ソフトウェアの進化や保守	○			
S210030040			業務パッケージ最新動向	○			
S210030050			インテリジェントシステム	○			
S210040010		（システム） Web システムの基礎技術	Web システムとその技術	○			
S210040020			サーバ技術	○			
S210040030			インターネットアプリケーション基盤技術	○			
S210040040			アプリケーションサービス	○			
S210040050			アプリケーション実行方式	○			
S210050010		（システム） Web システムの構築技術	Web アプリケーション技術	○			
S210050020			分散コンピューティング開発環境	○			
S210060010		（システム） Web システムの基礎技術	Web システムとその技術	○			
S210070010		（システム） データベースの基礎技術	データベース	○			
S210070020			リレーショナルモデル	○			
S210070030			データベース方式	○			
S210070040			データ操作	○			
S210070050			トランザクション処理	○			
S210070060			SQL	○			
S210070070			情報管理	○			
S210080010		（システム） データベースの構築技術	データベースの要件定義	○			
S210080020			データベース設計	○			

スキル項目コード	スキルカテゴリ	スキル分類	スキル項目	セキュア開発管理	脆弱性診断	CSIRT キュレーション	インシデントハンドリング
S210080030			データベースマネジメントシステム（DBMS）の選定・導入	○			
S210080040			データベースシステムの受け入れ	○			
S210080050			データベースマネジメントシステム（DBMS）への実装とテスト	○			
S210080060			データベース開発における重要技術	○			
S210090010		（システム） データベースの利用技術	データのオペレーション管理技術	○			
S210090020			データのセキュリティ管理技術	○			
S210090030			データベースシステム管理	○			
S210090040			データベース運用技術	○			
S210090050			データベース運用設計	○			
S210090060			データアクセスサービス設計技術	○			
S210090070			データクオリティ管理技術	○			
S210090080			データと情報の管理	○			
S210090090			データベース応用	○			
S210090100			データベース関連製品の利用技術	○			
S210090110			データベースの周辺技術	○			
S210090120			データベース診断技術とチューニング技術	○			
S210090130			データ移行	○			
S210090140			データ移行設計	○			
S210090150			データ統合サービス設計技術	○			
S210090160			マスタデータ管理技術	○			
S210090170			ドキュメントとコンテンツ管理技術	○			
S210090180			情報製品の設計技術	○			
S210090190			データ照会・加工・クレンジング技術	○			
S210090200			データマイニングツールの利用技術	○			
S210100010		（システム） プラットフォームの基礎技術	オペレーティングシステム	○			
S210100020			ミドルウェア	○			

スキル項目コード	スキルカテゴリ	スキル分類	スキル項目	セキュア開発管理	脆弱性診断	CSIRT キュレーション	インシデントハンドリング
S210100030			プラットフォーム技術	○			
S210110010		（システム） プラットフォームの構築技術	IT アーキテクチャ（ソフトウェア）	○			
S210110020			プラットフォーム実装技術	○			
S210110030			共通基盤としてのプラットフォーム設計構築	○			
S210120010		（システム） プラットフォームの利用技術	システムプラットフォームの受け入れ	○			
S210120020			システム診断技術と障害対策技術	○			
S210120030			プラットフォームシステム管理	○			
S210120040			製品知識（プラットフォーム）	○			
S210130010		（システム） ハードウェアの基礎技術	ハードウェア	○			
S210140010		（システム） ハードウェアの構築技術	IT アーキテクチャ（ハードウェア）	○			
S210160010		（システム） ネットワークの基礎技術	ネットワーク	○		○	
S210160020			ネットワークコンピューティング	○		○	
S210160030			ネットワークシステムの技術動向	○		○	
S210160040			ネットワーク標準	○		○	
S210160050			ネットワーク方式	○		○	
S210160060			通信プロトコル	○		○	
S210160070			データ通信と制御			○	
S210180010		（システム） ネットワークの利用技術	ネットワーク管理			○	
S210180020			ネットワーク応用			○	
S210180030			ネットワーク製品知識			○	
S210180040			業界固有のセキュリティ要件、事例	○		○	
S210180050			ネットワークシステムの評価			○	
S210190010		（システム） クラウドコンピューティングの基礎技術	クラウドコンピューティング基礎	○		○	
S210200010			クラウドデータベース技術	○			

スキル項目コード	スキルカテゴリ	スキル分類	スキル項目	セキュア開発管理	脆弱性診断	CSIRT キュレーション	インシデントハンドリング
S210200020		（システム） クラウドコンピューティングの構築技術	クラウド構築技術	○			
S210200030			クラウドアプリケーション実装技術	○			
S210200040			仮想マシンゲストのセキュリティ	○	○	○	○
S210210010		（システム） クラウドコンピューティングの利用技術	インタークラウド技術	○		○	
S210210020			クラウドコンピューティング利用	○		○	
S210210030			クラウドシステムの監視技術	○		○	
S220010010		（開発） システムアーキテクティング技術	システム要件定義	◎		○	
S220010020			システムインテグレーションとアーキテクチャ	◎		○	
S220010030			アプリケーション共通基盤要件定義手法	◎		○	
S220010040			アプリケーション共通基盤設計手法	◎			
S220010050			IT 基盤構築プロセス	◎		○	
S220010060			システム間連携技術	◎			
S220010070			システム方式設計	◎			
S220010080			システム結合・システム適格性確認テスト	◎			
S220010090			導入	◎			
S220010100			オブジェクト指向技術	◎			
S220010110			ファイルシステム	◎			
S220010120			フレームワーク要素技術	◎			
S220020010		（開発） システム開発管理技術	開発プロセス・手法	◎			
S220020020			開発環境管理	◎			
S220020030			知的財産適用管理	◎			
S220020040			構成管理・変更管理	◎			
S230020080		（保守・運用） IT サービスオペレーション技術	システムの監視			○	○
S230020090			稼働状況管理			○	
S230030010			移行設計	◎		○	

スキル項目コード	スキルカテゴリ	スキル分類	スキル項目	セキュア開発管理	脆弱性診断	CSIRT キュレーション	インシデントハンドリング
S230030020		（保守・運用） システム保守・運用・評価	移行	◎		○	
S230030030			プラットフォーム移行設計	◎		○	
S230030040			プラットフォーム移行	◎		○	
S230030050			アプリケーションシステムの受け入れ	◎		○	
S230030060			システム運用管理要件定義	◎			
S230030070			システム運用管理設計	◎			
S230030080			システム運用方式技法	◎		○	○
S230030090			システムの投資評価技法	◎			
S230030100			システム管理計画	◎		○	○
S230030110			システム管理技術	◎		○	○
S230030120			システム保守基準	◎		○	
S230030130			運行管理	○		○	
S230030140			システム管理製品	○		○	○
S230030150			運用管理ソフト製品			○	○
S230030160			運用システムの構築			○	
S230030170			運用システムの改善			○	○
S230030180			運用に関するシステム評価			○	○
S230030190			性能管理	○		○	
S230030200			障害時運用方式	○		○	○
S230030210			災害対策	○		○	○
S230030220			構成管理	○		○	
S230030230			保守技術	○		○	
S230030240			メンテナンス	○		○	
S230030250			保守・廃棄			○	
S230060040		（保守・運用） ファシリティ設計技術	信頼性、可用性、保守性			○	
S230060050			耐震安全確保			○	
S230060060			物理ネットワーク（通信ネットワーク）の設計			○	

スキル項目コード	スキルカテゴリ	スキル分類	スキル項目	セキュア開発管理	脆弱性診断	CSIRT キュレーション	インシデントハンドリング
S230060070			防災防犯設備設計			○	
S230060100			品質管理の知識			○	
S230070010		（保守・運用） サポートセンター基盤技術	インシデント管理システム	○		○	○
S240010010		非機能要件（可用性、性能・拡張性）	非機能要件の基礎	○		○	
S240010020			負荷分散と可用性の設計	○		○	
S240010030			システム信頼性、性能設計	○		○	
S240010040			高信頼性システムの設計	○			
S240010050			データベースシステムの信頼性設計	○			
S240020010		（非機能要件） セキュリティの基礎技術	情報セキュリティ	◎	◎	◎	◎
S240020020			情報保証と情報セキュリティ	◎	○	◎	○
S240020030			情報倫理とセキュリティ	○	○	○	○
S240020040			セキュリティ・アーキテクチャ技術	◎	○	◎	
S240020050			アプリケーションセキュリティ	◎	◎	◎	○
S240020060			情報プラットフォームのセキュリティ技術	◎	◎	◎	○
S240020070			ネットワークのセキュリティリスク	◎	◎	◎	○
S240020080			暗号技術	○	◎	◎	○
S240020090			セキュリティと個人情報	◎	○	◎	○
S240020100			保証、信用、信頼のメカニズム	○		○	○
S240020110			セキュリティ技術の理解と活用	◎	○	◎	○
S240030010		（非機能要件） セキュリティの構築技術	セキュリティ方針の策定	◎		○	○
S240030020			セキュリティ対策基準の策定	◎	○	○	○
S240030030			情報セキュリティ対策	◎	○	○	○
S240030040			セキュリティ実装技術	◎	◎	◎	
S240030050			セキュリティシステムの計画策定	◎	○	◎	○
S240030060			セキュリティシステムの要件定義	◎	○	◎	○
S240030070			セキュリティシステムの設計	◎	○	◎	
S240030080			セキュリティシステムの実装、検査	◎	◎	◎	

スキル項目コード	スキルカテゴリ	スキル分類	スキル項目	セキュア開発管理	脆弱性診断	CSIRT キュレーション	インシデントハンドリング
S240030090			コンピュータ・フォレンジクス（証拠保全追跡）	○	○	○	○
S240040010		（非機能要件） セキュリティの利用技術	セキュリティシステムの運用管理	○	○	◎	◎
S240040020			セキュリティシステム導入支援	○	○	◎	
S240040030			システム運用・保守技術（セキュリティ）	○	○	◎	○
S240040040			セキュリティ障害（事件事故/インシデント）管理	○	○	◎	◎
S240040050			情報セキュリティ管理	○	○	◎	○
S240040060			情報セキュリティ監査の実施・支援	○	○	○	○
S240040070			セキュリティ技術評価	○	○	◎	○
S240040080			セキュリティの分析	○	○	◎	○
S240040090			セキュリティの見直し（セキュリティシステムの評価と改善）	○	○	◎	○
S240040100			コンテンツセキュリティ技術	○	○	◎	○
S310020050	関連知識	企業活動	情報セキュリティ監査	○		○	○
S310030010		法規・基準・標準	セキュリティ関連法規	○		○	
S310030020			その他の法律・ガイドライン・技術者倫理	○		○	
S310030030			知的財産権	○			
S310030040			労働関連・取引関連法規	◎			
S310030050			標準化関連	◎		◎	

参考 11　システム構築担当に求められる知識･スキル：SecBoK2017 における IT システム部門に求められる知識･スキル（『セキュリティ知識分野（SecBoK）人材スキルマップ 2017 年版』（JNSA 教育部会, 2017 年 9 月）より抜粋）

分野	大項目	中項目	小項目
基礎	ICT 基礎	ネットワークインフラ	通信方式（例： Bluetooth、RFID、赤外線通信、Wi-Fi、ポケットベル、携帯電話、衛星受信アンテナ）および好ましくない情報の通信を可能とする、またはインストールされたシステムの正しい運用を妨げるジャミング技術に関する知識
		通信プロトコル・サービス	ネットワークプロトコル（例： TCP/IP、DHCP）およびディレクトリサービス（例；DNS）に関する知識
			ネットワークを通じてトラフィックがどのように流れるか（例： TCP/IP、OSI、ITIL）に関する知識
			VoIP に関する知識
		システム開発	システム開発のコンセプトに関するスキル
		システム運用	システム運用のコンセプトに関するスキル
			データバックアップ、バックアップの種類（フル、インクリメンタル）及び復元コンセプトとツールに関する知識
	工学基礎		全 5 レベルにおける CMMI に関する知識
セキュリティ基礎	総論		機密性、完全性、可用性、認証及び否認防止に関連する情報保証の原理と組織要件に関する知識
セキュリティマネジメント	総論		コンピュータネットワーク防御（CND）のポリシー、手続きおよび規制に関する知識
ネットワークセキュリティ	総論		ネットワーク通信のセキュア化に関するスキル
			何がネットワーク攻撃及び脅威と脆弱性の双方への関係を構成するかに関する知識
			トポロジー、プロトコル、構成要素及び原理を含むネットワークセキュリティアーキテクチャのコンセプト（例：深層防御のアプリケーション）に関する知識
	トラフィック解析		ネットワークトラフィック解析手法に関する知識
			パケットレベル解析に関する知識
	侵入検知		IDS ツールとアプリケーションに関する知識
			IDS のハードウェアとソフトウェアの種類に関する知識
			センサのチューニングに関するスキル
	フィルタリング		ウェブフィルタリング技術に関する知識
			ホスト／ネットワークのアクセス制御（例：アクセス制御リスト）に関する知識

	アクセス制御		ホスト／ネットワークアクセス制御（例： アクセス制御リスト）の適用に関するスキル
	VPN		VPN セキュリティに関する知識
			VPN 装置と暗号化の利用に関するスキル
システムセキュリティ	総論		システムとアプリケーションのセキュリティ上の脅威と脆弱性（例： バッファオーバフロー、モバイルコード、クロスサイトスクリプティング、PL/SQL 及びインジェクション、競合状態、隠れチャネル、リプレイ、リターン指向攻撃、悪意のあるコード）に関する知識
セキュリティ運用	インシデント対応		インシデントレスポンスとハンドリングの方法論に関する知識
			インシデントハンドリング手法の利用に関するスキル
			インシデントに関連したネットワークセキュリティの報告のためのプロセスに関する知識
サイバー攻撃手法	マルウェア		マルウェアからのネットワークの保護に関するスキル

（別紙２）サイバーセキュリティ人材の育成に関する施策間連携ワーキンググループ
委員名簿及び開催実績

＜委員＞

主査	後藤　厚宏	情報セキュリティ大学院大学　学長
委員	荒金　陽助	産業横断サイバーセキュリティ人材育成検討会 （CRIC CSF）事務局
委員	衛藤　将史	国立研究開発法人　情報通信研究機構 ナショナルサイバートレーニングセンター サイバートレーニング研究室　室長
委員	岸本　誠一	独立行政法人　国立高等専門学校機構 高知工業高等専門学校 副校長・専攻科長・ソーシャルデザイン工学科　教授
委員	曽根　秀昭	東北大学　教授
委員	田口　聡	独立行政法人　情報処理推進機構 HRD イニシアティブセンター　企画グループ　研究員

（五十音順、敬称略）

＜開催実績＞

第１回　平成 29 年６月 26 日

・各施策の取組について

・セキュリティ人材育成の基本的な認識と今後の取組の方向性

・平成 28 年企業のサイバーセキュリティ対策に関する調査報告

第２回　平成 29 年９月 14 日

・サイバーセキュリティ人材育成の検討の方向性について

・有識者からのプレゼンテーション

第３回　平成 29 年 12 月 27 日

・検討事項について

・各層別の人材像とキャリアパス及びカリキュラムの方向性について

・各省庁の人材育成施策の連携策の検討及び教材の R&D の推進について

・産学官連携の在り方と具体的方策について

第４回　平成 30 年４月 18 日

（セキュリティマインドを持った企業経営ワーキンググループと合同開催）

・サイバーセキュリティ人材育成に関する方向性について

－セキュリティマインドを持った企業経営ワーキンググループ報告書

－サイバーセキュリティ人材の育成に関する施策間連携ワーキンググループ報告書