情報セキュリティスキルアップ ハンドブック

～情報セキュリティマネジメント人材育成のために～

2015年9月

IPA 独立行政法人 情報処理推進機構
IT人材育成本部 HRDイニシアティブセンター

情報セキュリティスキルアップハンドブック

～情報セキュリティマネジメント人材育成のために～

目　次　　Contents

はじめに

本書は、情報セキュリティマネジメントの強化をねらいとして、一般企業での情報システムの利用部門（現場部門）において情報セキュリティマネジメントを推進する役割を担う人材に注目し、その役割と業務、必要なスキルと育成のための研修ロードマップを提供するものである。さらに、これらを利用する際の活用方法を記載している。本書の作成にあたっては、独立行政法人情報処理推進機構（IPA）が実施する「情報セキュリティマネジメント試験」で想定する対象者に準拠するとともに、IPAが公開する「ｉコンピテンシ ディクショナリ」[1] を参照した。

■本書における「情報セキュリティ管理者」の位置づけ

本書では、企業・組織における情報セキュリティ管理プロセスを「情報セキュリティマネジメント」と称し、現場部門でその推進の役割を担う人材を「情報セキュリティ管理者」と呼ぶ。具体的には、情報セキュリティに管理責任を持つ上位者からの指示を受けながら、各部門でのルールの理解やその徹底のために呼びかけをしたり、部門のセキュリティ状況を調査したりする現場部門の推進リーダである。既に多くの組織で、このような業務を担当する役割が置かれていると想定するが、本書ではそれを「情報セキュリティ管理者」と称する。

また、本書では情報セキュリティ管理者の各タスクに必要なスキルを洗い出して分類した。その際、情報セキュリティ管理者は、一般的なITスキル（ITパスポート試験相当[2] ）を保有していることを前提にした。

1　ｉコンピテンシ ディクショナリ　https://www.ipa.go.jp/jinzai/hrd/i_competency_dictionary/
2　IPA ITパスポート試験　https://www3.jitec.ipa.go.jp/JitesCbt/index.html

■本書の対象者

本書は、次のような方を対象としている。

① 経営者、最高情報セキュリティ責任者、情報セキュリティ推進組織、人材育成担当者、部門長などで、情報セキュリティ管理者を確保したい方

② 現場の情報セキュリティ管理者を育成したい方

③ 情報セキュリティ管理者としての業務をアサインされ、スキルアップしたいと思う方

④ 教育サービス事業者において、情報セキュリティ管理者の育成のための研修コースを企画したい方

⑤ 情報セキュリティベンダー、コンサルティング会社において、情報セキュリティ管理者の育成コンサルティングのフレームワークを検討したい方

■情報セキュリティ管理者育成の到達目標

本書では、情報セキュリティ管理者育成の到達目標を、以下のように想定している。

①組織のマネジメント層が、情報セキュリティ管理者の重要性を理解し、適切な人材にその業務を任せることができるようになること
②人材育成責任者や本人が、教育サービス事業者が提供する情報セキュリティ研修コースの受講判断ができるようになること
③情報セキュリティ管理者本人が、組織の最高情報セキュリティ責任者や情報セキュリティ推進組織と情報セキュリティについての会話ができるようになること

第１部

情報セキュリティ管理者の概要

第1章

情報セキュリティスキルアップハンドブック概要

1．背景と目的

近年、情報セキュリティ上のリスクが高度化・多様化している。また、どの業種においても情報の授受を伴って業務が遂行されており、幅広く情報セキュリティ分野の人材育成の強化が求められている。こうした状況を踏まえて、経済産業省では2012年度に「平成24年度情報セキュリティ対策推進事業（情報セキュリティ人材の育成指標等の策定事業）」を実施し、3スキル標準等の見直し案を検討した[3]。

独立行政法人情報処理推進機構（以下「IPA」という）は、経済産業省の前記事業による見直し案を受け、IT人材の育成において情報セキュリティを強化する場合に指標として参照することを目的に「情報セキュリティ強化対応スキル指標」を作成し公開[4]している。これは、情報セキュリティに関する職種・専門分野と、それに対応する業務（タスク）とスキルをｉ コンピテンシ ディクショナリから抜粋してコンパクトにまとめたものである。

一方、IT人材の市場動向を継続的に把握するためにIPAが毎年調査刊行する「IT人材白書2015」によると、情報セキュリティ上の関心事の第一位は「情報セキュリティマネジメント（運用・体制）」であった。また、内閣官房情報セキュリティセンター（現 内閣官房内閣サイバーセキュリティセンター）（NISC）における「普及啓発・人材育成専門委員会」での検討においても、事業部門の実務者（情報システムのユーザー）側の情報セキュリティリーダ層に関わる役割が注目[5]されている。

さらに、IPAでは、情報処理技術者試験に「情報セキュリティマネジメント試験」を創設し、2016年春から実施することになった。

本書は、このような流れを受け、現場の情報セキュリティ管理者の育成のための枠組みをまとめたものである。本書に含まれる情報セキュリティ管理者の役割、タスク、スキルは、情報処理技術者試験の「情報セキュリティマネジメント試験」で想定する対象者像に準拠した。

また、本書に含まれる各種の定義体を有効に活用する方法について、第3部「情報セキュリティスキルアップハンドブックの活用方法」に記載した。

---

3 経済産業省：平成24年度情報セキュリティ対策推進事業（情報セキュリティ人材の育成指標等の策定事業）のうち、事業報告書第1編（本編）PDFファイル
http://www.meti.go.jp/policy/it_policy/jinzai/index.html

4 IPA：情報セキュリティ強化対応スキル指標
http://www.ipa.go.jp/jinzai/hrd/security/index.html

5 内閣官房情報セキュリティセンター（NISC） 情報セキュリティ政策会議 第39回会合（平成26年5月19日）のうち、「新・情報セキュリティ人材育成プログラム」
http://www.nisc.go.jp/conference/seisaku/index.html#seisaku39

本書は情報セキュリティ管理者の育成を目的に、本人だけでなく経営者や最高情報セキュリティ責任者、部門長、教育サービス事業者、情報セキュリティベンダー、コンサルティング会社など、幅広い活用者を想定し、より多くの方々の参考になるよう作成した。想定される活用者と活用場面、及び本書の活用例の一覧を以下に示す。

表１　主な活用者と活用場面・活用例

活用者			活用場面	活用例
内部	経営者		情報セキュリティマネジメントを統括、推進する役割や業務を確認したい。	情報セキュリティを管理するための業務を洗い出し、自社の情報セキュリティ推進体制や、情報セキュリティ推進組織の位置づけを確認する際の参考とする。
	最高情報セキュリティ責任者		自社で行うべき事項と外部の情報セキュリティベンダーに依頼する事項を切り分けたい。	部門の情報セキュリティ推進に必要な業務（タスク）を確認し、外部の情報セキュリティベンダーに依頼する事項を切り分ける際の参考とする。
			自社独自の部門の情報セキュリティ管理者の役割や業務を定義したい。	組織の特性を考慮した情報セキュリティの管理を行うために、自社独自に定義すべき事項（役割と業務、タスク、スキル）を検討、定義する際の参考とする。
			部門の情報セキュリティ管理者のスキルレベルを確認したい。	業務遂行に必要なスキルを保有しているかを確認するための調査項目（スキル項目）を選定する際の参考とする。
		人材育成責任者	部門の情報セキュリティ管理者育成のために外部研修コースを選定したい。	部門の情報セキュリティ管理者に求められる研修コースを確認し、受講すべき研修コースを選定する際の参考とする。
			部門の情報セキュリティ管理者育成のための研修コースを自社内で作成したい。	自社独自の研修コースを作成するために、研修コースの学習内容に含めるべきスキルを確認する際の参考とする。
	部門長、管理職、所属長、マネージャー		部門の情報セキュリティ管理者を選出したい。	担当の人選にあたり、部門の情報セキュリティ管理者に必要な役割と業務、スキルを確認する際の参考とする。
	情報セキュリティ管理者		部門の情報セキュリティマネジメントを推進するために何が必要かを知りたい。	部門の情報セキュリティ管理者として業務遂行に必要なスキルを確認する際の参考とする。
			受講する研修コースを探したい。	スキルアップするために必要なスキルと研修コースがあるのかを確認する際の参考とする。
外部	教育サービス事業者		情報セキュリティ管理者育成のための研修コースを企画、作成したい。	本書の研修ロードマップに合わせ、研修コースを実装する際の参考とする。
	コンサルティング会社		情報セキュリティ管理者育成のコンサルティングフレームワークを作成したい。	情報セキュリティ管理者に必要な役割やタスク、スキルを利用する際の参考とする。

2. 情報セキュリティ管理者の重要性

情報セキュリティマネジメントの運用は、情報資産を取り扱うすべての従業員に関係する。さらに、部門独自の製品やサービスごとの情報資産の特定、セキュリティ対策、監査対応など、現場部門における独自対応も求められる。

情報セキュリティ管理者の役割は、情報セキュリティマネジメントについてしっかりと理解し、その運用を現場部門まで確実に浸透させ、部門の情報セキュリティマネジメントを推進してくことである。この役割は、現場部門で人、もの、情報を適切に管理し、情報セキュリティ事件や事故を発生させないためにも重要である。

また、万が一、セキュリティインシデントが発生した際には、組織のルールを順守させるように努め、関係部門とのコミュニケーションを図って、影響を最小限にとどめる役割も期待される。

3. 情報セキュリティスキルアップハンドブックの構成

本書は、以下の3部構成で作成されている。

■第1部 情報セキュリティ管理者の概要

「第1章 情報セキュリティスキルアップハンドブック概要」では、経営者、最高情報セキュリティ責任者、人材育成責任者、部門長、情報セキュリティ管理者などの企業内での活用者や教育サービス事業者が本書の内容を理解したうえで適切に活用できるように、背景と目的、本書の構成、ｉ コンピテンシ ディクショナリとの関係を説明している。

「第2章 情報セキュリティ管理者の役割と業務」では、本書で想定する企業の情報セキュリティ推進体制と情報セキュリティ管理者の役割と業務（タスク）を説明している。

「第3章 情報セキュリティ管理者に求められるスキル」では、情報セキュリティ管理者が第2章で定義されたタスクを実行する際に求められるスキルについて説明している。

■第2部 研修ロードマップ

「第1章 研修コース体系」では、情報セキュリティ管理者に必要なスキルを修得するための研修コース体系を説明している。

「第2章 研修コース内容」では、研修コース体系で示した各研修コースの内容例を示している。

■第3部 情報セキュリティスキルアップハンドブックの活用方法

「第1章 活用方法の概要」では、組織・企業や教育サービス事業者などが本書を活用する目的や活用方法について説明している。

「第2章 活用例」では、代表的な活用例について、活用手順や活用時のポイントなどについて説明している。

■添付資料

「タスクとスキル項目の対応表」では、第1部で説明する情報セキュリティ管理者のタスクと、タスクに対応するスキルカテゴリ、主なスキル項目を表で示している。

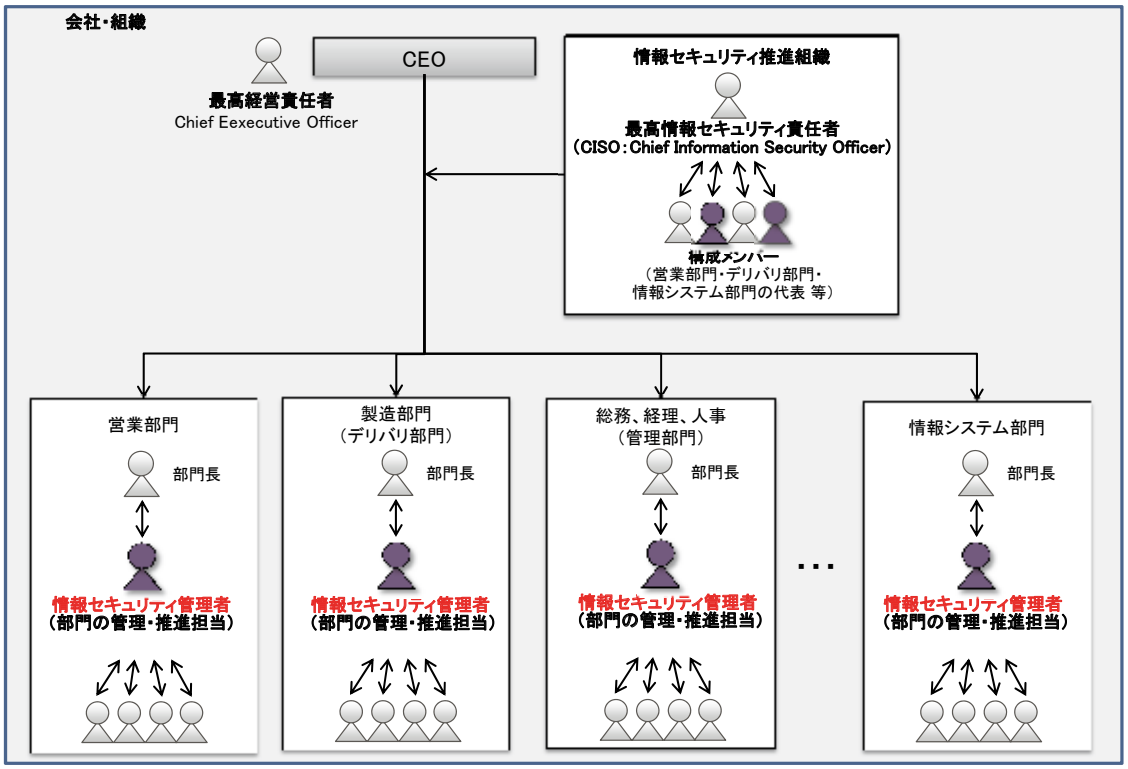
「研修コースとスキル項目の対応表」では、第2部の各研修モデルと「第1部 第3章 情報セキュリティ管理者に求められるスキル」で説明するスキルとの対応を表で示している。

第2章

情報セキュリティ管理者の役割と業務

1. 情報セキュリティの推進体制例と情報セキュリティ管理者

本書では、企業の情報セキュリティ対策の推進体制例として、「図１ 情報セキュリティの推進体制」にある組織体制を想定している。



※情報セキュリティ管理者（部門の管理・推進担当）は、部門長の兼務や複数の担当者が担当する場合もある
※情報システム部門は情報セキュリティ推進組織の役割を担う場合もあるが、上図ではユーザ部門の中の1部門として捉えている

図１　情報セキュリティの推進体制例

■情報セキュリティ推進組織

企業の情報セキュリティ戦略の立案や推進などを行う、全社の情報セキュリティを管理、推進する組織。最高情報セキュリティ責任者や営業部門、デリバリ部門、情報システム部門など、各部門の代表者などから構成される。

■最高情報セキュリティ責任者（CISO：Chief Information Security Officer）

企業の情報セキュリティ戦略の立案や推進などを行う、全社の情報セキュリティの統括責任者。

■部門長

部門の情報セキュリティの責任者。

■情報セキュリティ管理者

情報セキュリティ推進組織が策定した情報セキュリティ戦略に基づき、部門内の情報セキュリティマネジメントを推進する担当者。情報セキュリティ管理者は、部門長が兼務したり、部門のメンバが複数人で担当したりする場合もある。

2. 情報セキュリティ管理者の役割と業務

情報セキュリティ管理者の役割と業務を示す。この役割と業務は参照モデルであり、実際に組織内で役割定義などとして活用する際は、部門の状況や作業の分担状況などによって、組織ごとに調整し適用することを前提としている。

表2　情報セキュリティ管理者の業務と役割、期待する技術水準の定義

対象者像	情報システムの利用部門にあって、情報セキュリティリーダとして、部門の業務遂行に必要な情報セキュリティ対策や組織が定めた情報セキュリティ諸規程（情報セキュリティポリシを含む組織内諸規程）の目的・内容を適切に理解し、情報及び情報システムを安全に活用するために、情報セキュリティが確保された状況を実現し、維持・改善する者
業務と役割	情報システムの利用部門において情報セキュリティが確保された状況を実現し、維持・改善するために、次の業務と役割を果たす。 ➢ 部門における情報資産の情報セキュリティを維持するために必要な業務を遂行する。 ➢ 部門の情報資産を特定し、情報セキュリティリスクアセスメントを行い、リスク対応策をまとめる。 ➢ 部門の情報資産に関する情報セキュリティ対策及び情報セキュリティ継続の要求事項を明確にする。 ➢ 情報システムの調達に際して、利用部門として必要となる情報セキュリティ要求事項を明確にする。また、業務の外部委託に際して、情報セキュリティ対策の要求事項を契約で明確化し、その実施状況を確認する。 ➢ 部門における情報セキュリティを確実に運用する。 ➢ 部門のメンバの情報セキュリティ意識、コンプライアンスを向上させ、内部不正などの情報セキュリティインシデントの発生を未然に防止する。 ➢ 情報セキュリティインシデントの発生又はそのおそれがあるときに、情報セキュリティ諸規程、法令・ガイドライン・規格などに基づいて、適切に対処する。 ➢ 部門又は組織全体における情報セキュリティに関する意見・問題点について担当部署に提起する。
期待する技術水準	情報システムの利用部門において情報セキュリティが確保された状況を実現し、維持・改善するために、次の知識・実践能力が要求される。 ✓ 部門の情報セキュリティマネジメントの一部を独力で遂行できる。 ✓ 情報セキュリティインシデントの発生又はそのおそれがあるときに、情報セキュリティリーダとして適切に対処できる。 ✓ 情報技術全般に関する基本的な用語・内容を理解できる。 ✓ 情報セキュリティ技術や情報セキュリティ諸規程に関する基本的な知識を持ち、情報セキュリティ機関、他の企業などから動向や事例を収集し、部門の環境への適用の必要性を評価できる。
レベル対応	共通キャリア・スキルフレームワークのレベル2に相当

3. 情報セキュリティ管理者に求められる業務（タスク）

情報セキュリティ管理者に求められる業務（タスク）は、前節の定義をもとに、ｉコンピテンシ ディクショナリのタスク中分類[6]から独自に抽出、整理し、参照モデルとして定義した。実際の活用にあたっては、各組織で情報セキュリティ管理者として求められる範囲や部門の状況、役割の分担状況などをもとに、調整し適用してほしい。

情報セキュリティ管理者は、表中にある当該タスク（中分類）のすべてを担当するわけではなく、その中の情報セキュリティマネジメントに関する部分であることにも留意する。例えば「システム化要件定義」については、それに含まれるすべてのタスクを主体的に担当するわけではなく、上位者の指示のもとで現場の「情報セキュリティについての要求事項をまとめるタスク」を実行することを想定している。

表３　ｉコンピテンシ ディクショナリにおける情報セキュリティ管理者のタスク

タスク大分類	タスク中分類
システム企画立案	情報セキュリティ要件定義
システム要件定義・方式設計	システム化要件定義
IT運用コントロール	IT運用管理
	情報セキュリティ管理
システム運用管理	セキュリティ障害管理
資産管理・評価	資産管理規定の策定
	資産管理プロセスの実施
事業継続マネジメント	事業継続計画の策定
情報セキュリティマネジメント	情報セキュリティ戦略と方針の策定
	情報セキュリティの運用
	情報セキュリティの見直し
契約管理	契約締結管理
コンプライアンス	管理方針と体制
	実施と評価
調達・委託	委託業務管理

6　ｉコンピテンシ ディクショナリ2015v2版にある「タスクプロフィール×タスク対応表」では、情報セキュリティマネジメントの担当するタスクをタスク小分類まで示しているので、そちらも参照のこと。
http://www.ipa.go.jp/jinzai/hrd/i_competency_dictionary/index.html

第3章

情報セキュリティ管理者に求められるスキル

本章では、部門の情報セキュリティマネジメントを推進するために、情報セキュリティ管理者が保有すべきスキルについて説明する。前節で示した各タスクに対して、必要なスキルをi　コンピテンシ　ディクショナリ[7]のスキルデータから抽出し整理した。抽出したスキル項目は、スキルカテゴリという単位で本書独自に分類整理し、育成カリキュラムと結びつけるようにした。スキルを導出したプロセスを以下に図示する。

スキル項目に含まれる知識項目の詳細については、必要に応じて、ｉコンピテンシ ディクショナリを参照して定義することを想定している。

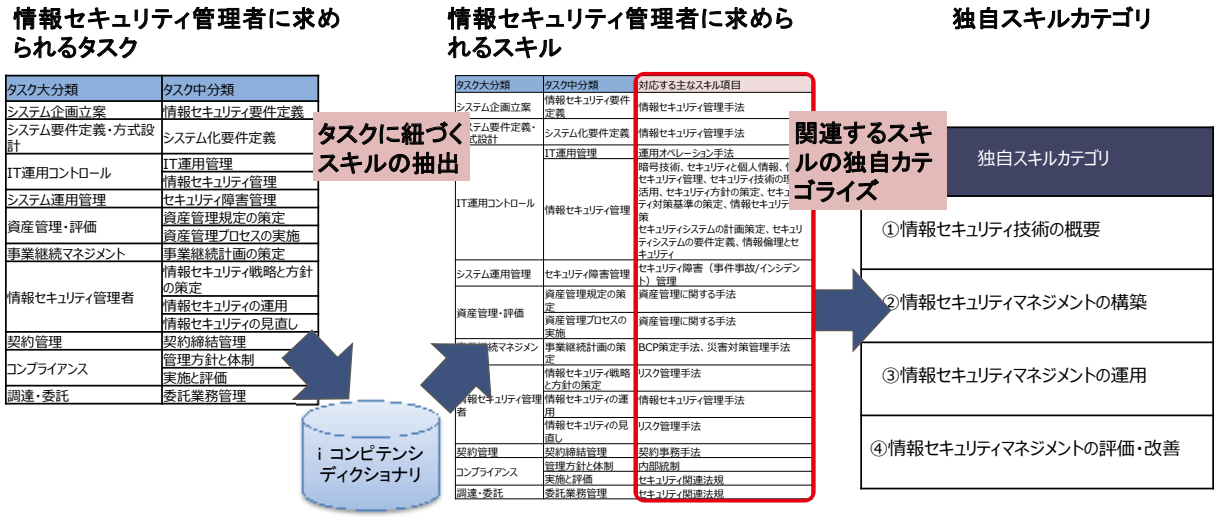


図２　スキル導出のプロセス

本書で定義したスキルカテゴリは、①「情報セキュリティ技術の概要」②「情報セキュリティマネジメントの構築」③「情報セキュリティマネジメントの運用」④「情報セキュリティマネジメントの評価・改善」の4つである。このスキルカテゴリは独自のもので、「情報セキュリティ強化対応スキル指標」の分類にあるスキルカテゴリ（メソドロジ、テクノロジ、関連知識、ITヒューマンスキル）の分類とは同一ではないので注意する。以下、次の節で詳説する。

7　本書のスキル項目はｉコンピテンシ ディクショナリ2015v2版で、情報セキュリティマネジメント試験とスキルの対応表を提供しているので、そちらも参照のこと。
http://www.ipa.go.jp/jinzai/hrd/i_competency_dictionary/index.html

表４　スキルカテゴリー覧

独自スキルカテゴリ
①情報セキュリティ技術の概要
②情報セキュリティマネジメントの構築
③情報セキュリティマネジメントの運用
④情報セキュリティマネジメントの評価・改善

1.「情報セキュリティ技術の概要」カテゴリに関するスキル

「情報セキュリティ技術の概要」カテゴリでは、部門の情報セキュリティマネジメントを推進するうえで求められる「技術の概要」に関するスキルを整理した。

「情報セキュリティ技術の概要」カテゴリは、さらに「IT基礎技術の概要」「セキュリティ技術の概要」「情報セキュリティ管理技術の概要」「インフラセキュリティ技術の概要」の4つのスキルカテゴリ（詳細）に分類した。

「情報セキュリティ技術の概要」カテゴリに求められるスキルは、以下のとおりである。

表５　「情報セキュリティ技術の概要」カテゴリに求められるスキル

独自スキルカテゴリ		i コンピテンシ ディクショナリ	
スキルカテゴリ	スキルカテゴリ（詳細）	スキル分類	スキル項目
①情報セキュリティ技術の概要	IT基礎技術の概要	(共通技術) IT基礎	コンピュータシステムの構成
			システムの構成
			システムの評価指標
	セキュリティ技術の概要	(非機能要件) セキュリティの基礎技術	情報セキュリティ
			暗号技術
			セキュリティと個人情報
		(非機能要件) セキュリティの構築技術	コンピュータ・フォレンジクス（証拠保全追跡）
		(非機能要件) セキュリティの利用技術	情報セキュリティ管理
	情報セキュリティ管理技術の概要	(支援活動) リスクマネジメント手法	リスク管理手法
			情報セキュリティ管理手法
	インフラセキュリティ技術の概要	(非機能要件) セキュリティの基礎技術	アプリケーションセキュリティ
			情報プラットフォームのセキュリティ技術
			ネットワークのセキュリティリスク
			セキュリティ技術の理解と活用

2.「情報セキュリティマネジメントの構築」カテゴリに関するスキル

「情報セキュリティマネジメントの構築」カテゴリには、部門の情報セキュリティマネジメントを推進するうえで求められる「構築」に関するスキルを整理した。

「情報セキュリティマネジメントの構築」カテゴリは、さらに「ISMS構築」「情報セキュリティシステムの構築」「法規の導入」の3つのスキルカテゴリ（詳細）に分類した。

「情報セキュリティマネジメントの構築」カテゴリに求められるスキルは、以下のとおりである。

表6　情報セキュリティマネジメントの構築に求められるスキル

独自スキルカテゴリ		iコンピテンシ ディクショナリ	
スキルカテゴリ	スキルカテゴリ（詳細）	スキル分類	スキル項目
情報セキュリティマネジメントの構築	ISMS構築	(支援活動) ITガバナンス	内部統制
		(支援活動) 事業継続計画	BCP策定手法
			災害対策管理手法
		(支援活動) 資産管理手法	資産管理に関する手法
		(非機能要件) セキュリティの基礎技術	情報保証と情報セキュリティ
		(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
			セキュリティ対策基準の策定
			情報セキュリティ対策
	情報セキュリティシステムの構築	(非機能要件) セキュリティの構築技術	セキュリティシステムの計画策定
			セキュリティシステムの要件定義
	法規の導入	(企画) セールス事務管理手法	契約事務手法
		法規・基準・標準	セキュリティ関連法規

3.「情報セキュリティマネジメントの運用」カテゴリに関するスキル

「情報セキュリティマネジメントの運用」カテゴリには、部門の情報セキュリティマネジメントを推進するうえで求められる「運用」に関するスキルを整理した。

「情報セキュリティマネジメントの運用」カテゴリに求められるスキルは、以下のとおりである。

表7 「情報セキュリティマネジメントの運用」カテゴリに求められるスキル

独自スキルカテゴリ		iコンピテンシ ディクショナリ	
スキルカテゴリ	スキルカテゴリ（詳細）	スキル分類	スキル項目
情報セキュリティマネジメントの運用	— （同左）	（非機能要件） セキュリティの基礎技術	情報倫理とセキュリティ
		（非機能要件） セキュリティの構築技術	情報セキュリティ対策
		（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
			システム運用・保守技術（セキュリティ）
			セキュリティ障害 （事件事故/インシデント）管理

4．「情報セキュリティマネジメントの評価・改善」カテゴリに関するスキル

「情報セキュリティマネジメントの評価・改善」カテゴリには、部門の情報セキュリティマネジメントを推進するうえで求められる「評価・改善」に関するスキルを整理した。

「情報セキュリティマネジメントの評価・改善」カテゴリは、さらに「評価基準」「評価・改善」の2つのスキルカテゴリ（詳細）に分類した。

「情報セキュリティマネジメントの評価・改善」カテゴリに求められるスキルは、以下のとおりである。

表8　「情報セキュリティマネジメントの評価・改善」カテゴリに求められるスキル

独自スキルカテゴリ		i コンピテンシ ディクショナリ	
スキルカテゴリ	スキルカテゴリ（詳細）	スキル分類	スキル項目
情報セキュリティマネジメントの評価・改善	評価基準	(非機能要件) セキュリティの基礎技術	保証、信用、信頼のメカニズム
		(非機能要件) セキュリティの利用技術	セキュリティ技術評価
	評価・改善	(非機能要件) セキュリティの利用技術	情報セキュリティ監査の実施・支援
			セキュリティの分析
			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)

第２部

研修ロードマップ

第1章

研修コース体系

情報セキュリティ管理者に必要なスキルを修得できる研修コースを、本書のスキルカテゴリ単位で整理し、研修コース体系を作成した。研修コースの受講対象者は、一般的なITスキル（ITパスポート試験相当）を保有していることを前提とした。

この研修コース体系は、部門の情報セキュリティマネジメントをこれから担当する人向けの「初級（R0～R1）」コースと、現在活躍している人向けの「中級（R2～R3）」コースとで構成した。「中級（R2～R3）」には、より実践的なケーススタディを盛り込むことで、スキルの定着と部門の情報セキュリティマネジメント実務での実践力強化を狙っている。

本章の研修コース体系、及び研修コースは、参照モデルとして作成しており、研修コース内容は例示である。企業の実状にあわせて、研修コースをカスタマイズした上で活用してほしい。

研修コース体系図

情報セキュリティ管理者の実務能力向上のために必要となる研修コースを、スキルカテゴリごとかつスキルレベルごと、及び受講順がわかるように、研修コース体系として図示する。

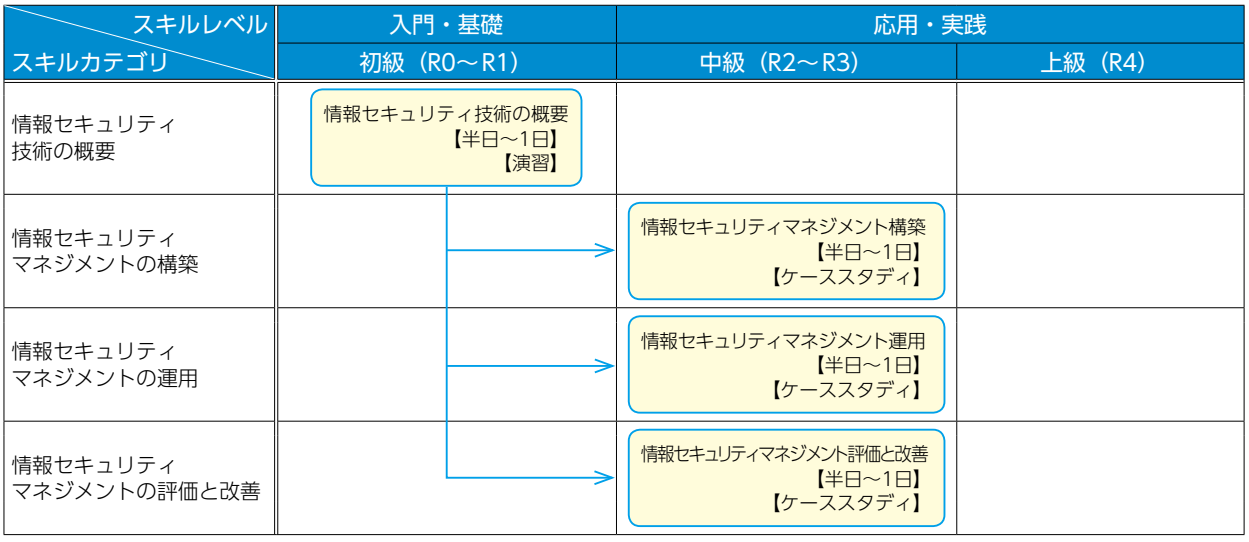


図３　研修コース体系図

※この研修コース体系は、現場の情報セキュリティ管理者の育成に特に重要となるスキルを優先的に研修コースとして設定した。そのため、システム開発やシステム運用が主となるタスク領域は、研修コースの内容に含んでいない。各社でのコースの設計・実装においては、現場のニーズや保有する製品・サービス、事業内容に合わせ、タスクを起点に検討することを推奨する。

【スキルレベル】

各コースは以下のスキルレベルの受講者を対象として想定している。

■初級（R0～R1）

情報セキュリティマネジメントを学習する人、実際にこれから担当する人

■中級（R2～R3）

現在、部門の情報セキュリティ管理を担当しており、主体的に作業を行える人

■上級（R4）

全社的な視点で、情報セキュリティ対策を推進し、より実践的な業務、及び全社推進における改善提言を行える人

表９　スキルレベルの判断基準例（参考）[8]

ランク	診断基準
R4	他者を指導できる、又はその経験あり
R3	独力で実施できる、又はその経験あり
R2	サポートがあれば実施できる、又はその経験あり
R1	トレーニングを受けた程度の知識あり
R0	知識、経験なし

【研修コースの構成】

研修コースは、説明と演習、又はケーススタディから構成した。

■初級（R0～R1）

初級は、情報セキュリティ管理者として活動するために必要な情報セキュリティに関する基礎知識の修得を目的とし、コースを設計した。初級のコースは、説明と演習から構成した。

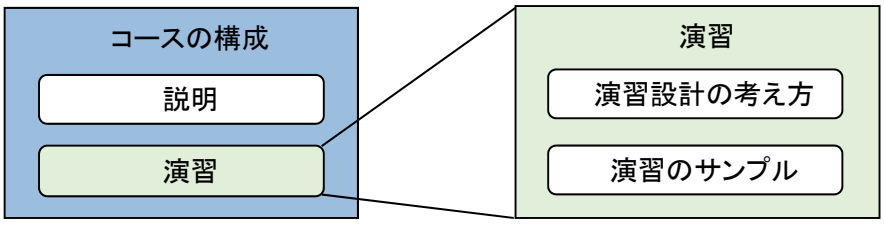


図４　初級のコース構成

8　「ｉコンピテンシ・ディクショナリ（試用版）」のタスク評価の診断基準例をもとに独自で作成。

■中級（R2～R3）

中級は、部門の情報セキュリティマネジメントの実務で、研修内容をすぐに活用できるように、より実践的なケーススタディを盛り込んだコースを設計した。中級のコースは、説明とケーススタディから構成した。ケーススタディは、グループワークを想定している。

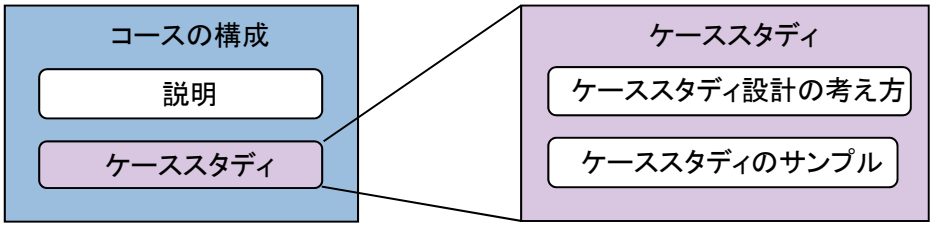


図５　中級のコース構成

第2章

研修コース内容

1. 「情報セキュリティ技術の概要」コース

◆コース概要	
コース名	情報セキュリティ技術の概要
スキルカテゴリ	情報セキュリティ技術の概要
スキルレベル	初級
コース形態	集合研修、又はCBT（Computer Based Testing）（説明と個人演習）
研修期間の目安	半日～1日
コース概要	情報セキュリティから見た情報システムの構成、情報セキュリティ技術の概要、情報セキュリティの管理方法について、情報セキュリティマネジメントの観点から、演習を通じて学習する。
学習目標	・情報セキュリティに関する技術概要を理解する。 ・情報セキュリティの管理方法の概要を修得する。
受講対象者	これから部門内の情報セキュリティ管理を担当する人。 （情報セキュリティ管理者のR1を目指す人）
前提知識	業務でPCを利用しており、自PCの環境をセットアップできる。又は、同等の知識を有すること。
コースの構成例	第1章　IT技術の概要 情報セキュリティを理解するために必須となるIT技術の概要を把握する。 ・コンピュータシステムの構成（インターネット、Webシステム、クライアント・サーバシステム、信頼性の向上とシステム構成） ・インフラセキュリティ（ネットワークセキュリティ、サーバセキュリティ、アプリケーションのセキュリティ） 第2章　情報セキュリティ技術の概要 情報セキュリティで利用されている代表的な技術の概要を把握する。 ・情報セキュリティの目的（脅威、守るべき情報資産、機密性、完全性、可用性など、情報セキュリティ対策） ・情報セキュリティに対する脅威と対策技術（情報セキュリティ技術の役割、ウイルス対策、不正アクセス対策、暗号技術、証明書、認証技術、セキュアOSなど） 第3章　情報セキュリティの管理 情報セキュリティに欠かせない管理作業として、情報のライフサイクルの理解、守るべき情報資産とリスクの概要、情報セキュリティマネジメントシステムの概要を理解する。 ・情報セキュリティポリシ ・情報セキュリティ管理者の位置づけ、役割、業務（全社推進体制と部門責任者の役割、会議体と部門の情報セキュリティ管理者の役割、部門の対策、部門のPDCAサイクル） ・リスクアセスメントの概要（情報セキュリティに対する脅威、脆弱性、評価方法の種類と特徴、リスク、リスク対策の種別（低減、回避、移転、保有）、情報セキュリティ対策の種別（技術的対策、物理的対策、人的対策）、情報セキュリティポリシ及び規程類の体系と部門ルール、監査への対応） 演習「自部門の情報セキュリティ対策」 部門の情報セキュリティ対策の状況を把握する。
研修修了後の取得スキル項目	コンピュータシステムの構成、システムの構成、情報セキュリティ、暗号技術、セキュリティと個人情報、リスク管理手法、情報セキュリティ管理、ネットワークのセキュリティリスク、セキュリティ技術の理解と活用、情報プラットフォームのセキュリティ、情報セキュリティ管理手法

◆演習の解説

（1）演習設計の考え方

設定の主旨	情報セキュリティ管理者の役割を初めて担うには、担当部門の情報セキュリティ対策の現状把握が欠かせない。演習は、情報セキュリティマネジメント及びそれらを取り巻く環境を把握することを目的としている。
演習	自部門の情報セキュリティ対策
目的	自部門の情報セキュリティ対策がどのような脅威に対応するかについて演習を通じて理解する。
何を考えさせるか	自部門に施されている情報セキュリティ対策には何があるか。 各情報セキュリティ対策が防ごうとしている脅威は何か。
対応するスキル項目との関係	暗号技術、セキュリティと個人情報、情報セキュリティ管理、ネットワークのセキュリティリスク、セキュリティ技術の理解と活用、情報プラットフォームのセキュリティ、情報セキュリティ管理手法

（2）演習のサンプル

設問	自部門で実施されている情報セキュリティ対策とその対策が防ごうとしている脅威について列挙しなさい。
解答の観点	・情報セキュリティ対策（ウイルス対策、ファイアウォール、入退室管理、サーバルーム、お客様との会議スペース、暗号技術、証明書、認証技術、情報セキュリティ規程、情報資産管理台帳など） ・機密性、完全性、可用性の観点から脅威を列挙（ウイルス感染、ハッキング、盗難、紛失、災害、システムトラブル、ネットワークトラブルなど）

2.「情報セキュリティマネジメント構築」コース

◆コース概要	
コース名	情報セキュリティマネジメント構築
スキルカテゴリ	情報セキュリティマネジメントの構築
スキルレベル	中級
コース形態	集合研修（説明とケーススタディ）
研修期間の目安	半日～1日
コース概要	部門の情報セキュリティマネジメントを構築するための基準や、情報資産の調査、リスクアセスメントの概要、管理台帳の作成、部門ルールの策定について、部門の情報セキュリティマネジメントの観点から、ケーススタディを通じて修得する。
学習目標	・部門の情報セキュリティマネジメントを構築する。 ・情報セキュリティに関連する法的な対応を導入する。
受講対象者	現在部門内の情報セキュリティ管理を担当しており、主体的に作業を行えることを目指す人。（情報セキュリティ管理者のR2、R3を目指す人）
前提知識	「情報セキュリティマネジメントの技術概要」コースを修了していること。又は同等の知識を有すること。
コースの構成例	第1章　部門の情報セキュリティマネジメントの構築 部門の情報セキュリティマネジメントの位置づけや体制、構築の対象とプロセスを理解する。 ・情報セキュリティ対策の基本（対策の基準ISO15408など、機密性、完全性、可用性、情報セキュリティのPDCAなど） ・情報セキュリティ規程の体系と部門ルール（ポリシ、スタンダード、プロシージャ、部門ルール） 第2章　情報資産の調査と分類、管理台帳 部門内での守るべき情報資産をどう洗い出すのかと、どう分類し、どのように台帳管理するのかについて修得する。 ・守るべき情報資産の洗い出し（書類、データ、媒体、PC、システムなど） ・情報資産の分類（分類区分の設計、公開、秘密、重要、関係者外秘密など） 第3章　リスクアセスメントの実施 部門の情報資産に対して、どのようにリスクアセスメントを実施するのかを修得する。 ・リスクアセスメントの流れ（脅威、脆弱性、リスク算出、評価） ・アプローチ方法と例（ベースライン、非形式、詳細、組合せ） ・情報セキュリティ対策（物理的対策の代表的種類、人的・組織的対策の代表的種類、技術的対策の代表的種類） ケーススタディ1「情報資産の洗い出しとリスクアセスメント」 情報資産の洗い出しの実際と管理台帳の設計について修得する。 ・法的観点の配慮（個人情報保護法の概要、契約（委託契約など）、不正アクセス禁止法の概要） ケーススタディ2「委託先の情報セキュリティ管理（法的対応）」 部門の情報セキュリティ対策として法的な対応について修得する。 第4章　部門の情報セキュリティ規程の導入・年間計画の策定 部門の情報セキュリティ対策の計画と導入をどのように進めるかを修得する。 ・情報セキュリティマネジメントの具体的な業務 ・管理台帳の作成（資産名、管理者、機密レベル、持ち出し日時、記入要領など） ・部門ルールの作成と周知 ・年間スケジュールの策定（情報セキュリティのPDCA、教育と周知、監査対応、マネジメントレビュー、状況報告、改善報告） ケーススタディ3「部門ルールの作成と管理台帳の設計」 部門への情報セキュリティルールの導入方法について修得する。
研修修了後の 取得スキル項目	資産管理に関する手法、情報保障と情報セキュリティ、情報セキュリティ方針の策定、セキュリティ対策基準の策定、契約事務手法、セキュリティ関連法規

◆ケーススタディの解説

ケーススタディ1：「情報資産の洗い出しとリスクアセスメント」の解説

（1）ケーススタディ設計の考え方

設定の主旨	部門の情報セキュリティマネジメントを構築する場合に欠かせないのが「部門の情報資産を洗い出すことと、リスクアセスメントすること」である。部門情報の洗い出しとリスクアセスメントの進め方を身につけるために、ひとつのケースとして掲げてある。
ケース	情報資産の洗い出しとリスクアセスメント
目的	情報資産をどう捉えるか、リスクアセスメントをどうすべきかについてケーススタディを通じて修得する。
何を考えさせるか	自部門の情報資産の洗い出し方法 リスクアセスメント方法に従ったリスクの算出方法
対応するスキル項目との関係	資産管理に関する手法、セキュリティ方針の策定

（2）ケーススタディのサンプル

状況	営業部門では、自社のみならずお客様の個人情報や秘密情報を取り扱っている。 情報セキュリティ規程には、情報資産を洗い出し、リスクアセスメントを行い、管理すべき情報資産を決定する旨が記載されている。 情報セキュリティ推進室から担当部門の情報資産の洗い出しとリスクアセスメントについて指示を受けた。 取扱い情報には、カタログや契約書、見積書、製品開発情報などが紙媒体と共有サーバ上に格納されている。 お客様へはモバイル機器でのプレゼン、USBによる情報の授受なども行われている。また、個人所有のスマートフォンによる討議結果の記録なども行われている状況である。
環境	自社内の組織体制と役割定義（推進部門、IT部門、部門内責任者） 自社情報セキュリティ規程 (情報資産とリスクアセスメントに関連する記載部分) (情報の機密レベル：公開、社外秘、重要など) 自社の個人情報保護規程（個人情報の特定と管理に関する部分） 主要業務の情報の流れ（お客様⇔部門⇔関連部門など）
設問	情報セキュリティ管理者として、本依頼が担当部門にされたと想定し、以下の設問について検討し、その結果を発表しなさい。 設問1：部門で取り扱われている情報資産を列挙しなさい。 設問2：洗い出した各情報資産について、脅威と脆弱性を列挙しなさい。 設問3：カタログ、契約書（紙媒体）、見積書（USB）について、指示されたリスクアセスメント方法に従って、リスクを算出しなさい。
解答の観点	設問1：(以下の観点から、業務で使用している情報資産を列挙する。) ・書類、データ、個人情報、秘密情報など ・紙媒体、電子記憶媒体、PC、システムなど ・個人が職場に持ち込むスマートフォン、電子記憶媒体など 設問2：(以下の観点で主要な脅威と脆弱性を列挙する。) ・機密性、完全性、可用性の観点から脅威を列挙（ウイルス感染、ハッキング、盗難、紛失、災害、システムトラブル、ネットワークトラブル、外部者の侵入など） ・脆弱性（パッチ未適用、新種のウイルス出現、新たな攻撃手法、入退室管理の不徹底、鍵管理の不徹底など） 設問3：(以下の観点でリスク値を算出する。) ・情報資産の重要度、機密性、完全性、可用性

ケーススタディ2：「委託先の情報セキュリティ管理（法的対応）」の解説

（1）ケーススタディの設計の考え方

設定の主旨	情報セキュリティに関する法的対応について、個人情報を含む委託契約を具体例としながら、業務への導入方法を身につけるために、ひとつのケースとして掲げてある。
ケース	委託先の情報セキュリティ管理（法的対応）
目的	委託先の情報セキュリティ管理をどう捉えるか、その対応をどうすべきかについてケーススタディを通じ修得する。
何を考えさせるか	委託する内容と情報セキュリティの関係 委託契約における情報セキュリティ事項への記載項目 委託先への周知方法
対応するスキル項目との関係	契約事務手法

（2）ケーススタディのサンプル

状況	お客様企業（O社）から受託した案件であるが、一部の業務の再委託（I社）を条件に受注した。お客様からの委託要件には、個人情報を含むため、情報セキュリティ対策を徹底することが求められている。具体的には、情報セキュリティ管理者の設置と誓約書、従業者全員からの誓約書、委託先の管理、情報セキュリティ対策状況の中間報告、及び最終報告を求められている。最終報告では、残存情報の完全な消去とその証明書も求められている。なお委託先企業は、2年前に当社が発行した入館IDカードを紛失した経緯がある。
環境	自社内の組織体制と役割定義（推進部門、IT部門、法務、総務） 自社情報セキュリティ規程（委託に関連する記載部分） 自社の個人情報保護規程（再委託関連などの該当部分） 委託契約の情報セキュリティに関する項目（契約書の該当条項） 情報セキュリティの管理や損害賠償に関する条項は標準契約書として存在するが、委託先への管理者設置、誓約書の提出、廃棄証明書の提出及び監査は含まれていない。 委託先の組織体制と情報セキュリティ環境（委託先部門の環境）
設問	情報セキュリティ管理者として、本受注案件が担当部門で発生したと想定し、以下の設問について検討し、その結果を発表しなさい。 設問1：お客様企業（O社）からの本案件の情報セキュリティ要件を整理しなさい。 設問2：委託先（I社）へ指示すべき事項を列挙しなさい。 設問3：委託先（I社）への契約の条項として追加すべき項目を列挙しなさい。
解答の観点	設問1：（以下の観点で要件を洗い出す。） ・個人情報について（利用目的、再委託、個人情報の取得など） ・情報セキュリティ管理者の設置と誓約書の提出 ・業務従業者からの誓約書の提出 ・情報セキュリティ対策状況の把握と報告 ・取扱い情報の管理と廃棄の管理、廃棄証明の提出 設問2：（以下の観点でI社へ支持すべき事項を列挙する。） ・I社の業務従業者からの誓約書の取得 ・I社の情報セキュリティ管理者の設置と誓約書の提出 ・委託業務に関する情報管理の方法（台帳管理など）の確立 ・業務実施に関するI社への情報セキュリティ監査の実施 ・業務終了時のI社からの廃棄証明書の提出 設問3：（以下の観点で追加条項を列挙する。） ・情報セキュリティ管理者の設置 ・情報セキュリティ管理者及び業務従事者の誓約書の提出 ・廃棄証明書の提出 ・情報セキュリティ監査への対応

ケーススタディ３：「部門ルールの作成と管理台帳の設計」の解説

（1）ケーススタディ３の設計の考え方

設定の主旨	部門の情報セキュリティマネジメントを構築する場合に、情報セキュリティ規程から自部門にあわせたルールや管理台帳を作成することが必須である。部門情報の洗い出しと管理方法を身につけるために、ひとつのケースとして掲げてある。
ケース	部門への情報セキュリティルールの実装
目的	全社共通の情報セキュリティ規程をどう捉えるか、その規程をどう実装すべきかについてケーススタディを通じ修得する。
何を考えさせるか	情報セキュリティ規程の求めている要件 部門内業務の流れと情報セキュリティ規程の対象とする情報資産 情報セキュリティ規程に従った記録 情報のライフサイクルに従った情報の原本、コピー、配布、消去の管理（情報のトレーサビリティの確保）
対応するスキル項目との関係	セキュリティ方針の策定、セキュリティ対策基準の策定、情報セキュリティ対策

（2）ケーススタディのサンプル

状況	市場調査サービス部門では、お客様から秘密情報をいただき、市場の調査を実施、報告している。情報セキュリティ規程では、お客様の秘密情報の管理に関して規定されており、その規程を調査業務へ適用する指示を受けた。 また、本部門ではUSBの持ち出しも承認があれば可能としている。
環境	自社内の組織体制と役割定義（推進部門、IT部門、法務、総務） 自社情報セキュリティ規程（該当秘密情報の取扱いについての記載部分） お客様との情報の受渡し規約 調査業務の概要（作業概要、業務フロー、お客様、社内共同作業部門）
設問	情報セキュリティ担当者として、本情報セキュリティ規程を担当部門に導入すると想定し、以下の設問について検討し、結果を発表しなさい。 設問1：お客様から入手したUSB媒体上の秘密情報のライフサイクルを洗い出しなさい。 設問2：お客様から入手した秘密情報の管理台帳とUSB媒体の持ち出し管理台帳に必要な項目を列挙しなさい。 設問3：秘密情報とUSBの管理の取扱いについて、部門の従業員に対する周知項目と周知方法を列挙しなさい。
解答の観点	設問1：（以下の観点で情報のライフサイクルを洗い出す。） ・原本、配布、バックアップ、他部門への送付、消去、お客様への送付、持ち出し、返却など 設問2：（以下の観点で主要な管理台帳の項目を列挙する。） ・秘密情報の管理台帳（情報資産名、管理者、機密レベル、取得日時、確認日時、確認者、廃棄日時） ・USBの管理台帳（情報資産名、管理者、持ち出し者名、持ち出し日時、承認者、返却者、返却日時、記録情報の消去確認、承認者） 設問3：（以下の観点で周知項目と周知方法を検討する。） ・周知項目（管理台帳名、管理責任者、設置場所/格納場所、記入ルール、承認者） ・周知方法（説明会、部門の会議、メール/回覧、部門ホームページ、張り紙など）

3.「情報セキュリティマネジメント運用」コース

◆コース概要	
コース名	情報セキュリティマネジメント運用
スキルカテゴリ	情報セキュリティマネジメントの運用
スキルレベル	中級
コース形態	集合研修（説明とケーススタディ）
研修期間の目安	半日～1日
コース概要	部門の情報セキュリティマネジメントの運用に必要な項目とインシデントへの具体的な対応方法について、部門の情報セキュリティマネジメントの観点から、ケーススタディを通して修得する。
学習目標	・情報セキュリティマネジメントの運用について理解する。 ・自部門内のインシデントに対応できる。
受講対象者	現在部門内の情報セキュリティ管理を担当しており、主体的に作業を行えることを目指す人。（情報セキュリティ管理者のR2、R3を目指す人）
前提知識	「情報セキュリティマネジメントの技術概要」コースを修了していること。又は同等の知識を有すること。
コースの構成例	第1章　部門の情報セキュリティマネジメント運用の概要 部門の情報セキュリティを維持するために欠かせない作業について理解する。 ・情報セキュリティ環境変化の把握（新たな業務、新たなオフィス、人材の異動、情報機器の新規購入や廃棄、ネットワークの変更、サーバやOSの変更、インシデント、パッチ適用、新たな脅威の出現など） ・部門で対応すべき事項（情報資産の棚卸し、部門ルールの更新、管理台帳の確認と見直し、情報環境の更新、従業員への教育や周知） 第2章　インシデントへの対応 部門担当者として重要となるインシデントへの対応について、部門の状況やインシデントの種類に従った適切な行動を修得する。 ・インシデントの種別ごとの対応（ウイルス感染、ハッキング、情報の不正持ち出し、紛失、火災、水害、盗難、サーバ障害など） ・インシデント時の初動と対策の強化（インシデントごとの初動と対策例、お客様を含むステークフォルダーへの対応） ・インシデントの報告（対象情報、時刻と事象、判断事項、再発防止） ケーススタディ4「インシデント発生への対応」 ケースを通じて、インシデントへの対応方法とインシデントの準備や訓練が重要なことを修得する。
研修修了後の 取得スキル項目	情報倫理とセキュリティ、セキュリティ障害（事件事故/インシデント）管理

◆ケーススタディの解説

ケーススタディ4：「インシデント発生への対応」の解説

（1）ケーススタディ設計の考え方

設定の主旨	部門の情報セキュリティマネジメントを運用する場合に、インシデントの種類に応じた状況の把握と判断、初動が重要である。インシデントの種別に応じた対処方法を身につけるために、ひとつのケースとして掲げてある。
ケース	インシデント発生への対応
目的	組織の中でインシデントをどう捉えるか、その対応をどうすべきかについてケーススタディを通じ修得する。
何を考えさせるか	インシデントの判断 緊急的対応（適切な初動対処、推進部門への早期報告、指示の実施） 緊急対応後の措置（推進部門、IT部門、法務、総務などとの連携） インシデント報告（インシデントの経緯：時間と状況変化の記録）
対応するスキル項目との関係	セキュリティ障害（事件事故/インシデント）管理

（2）ケーススタディのサンプル

状況	インシデントの発生 営業部門のAさんが、お客様情報や見積書などが格納された携帯端末を、お客様先懇親会から帰宅する途中電車内で眠ってしまい紛失してしまった。Aさんは、気づいた直後駅員さんへ届け出た。その5分後に部門の情報セキュリティ管理者のSさんへ報告した。
環境	組織体制と役割定義（推進部門、IT部門、法務、総務） 情報セキュリティ規程（該当インシデントの記載部分） 携帯端末の利用環境（シンクライアント化されていない端末）
設問	情報セキュリティ管理者として、本インシデントが担当部門で発生したと想定し、以下の設問について検討し、結果を発表しなさい。 設問1：Aさんから報告を受けた時点で、緊急的な対応（初動）としてどのような対処を行うべきかを列挙しなさい。 設問2：緊急対応後の対処として、お客様への対応、情報セキュリティの規程、対象部門の従業員などへの観点から、どのような対処を行うかを検討しなさい。 設問3：本インシデントについてお客様へ報告に伺うには、どのような内容を報告すべきかを検討しなさい。
解答の観点	設問1：（以下の観点で情報セキュリティの初動を列挙する。） ・社外への対応（駅、警察） ・社内への対応（情報セキュリティ推進室、総務、IT部門） ・技術的対応（マシンロック、位置情報検出など可能であれば） 設問2：（以下の観点で対応を検討する。） ・社内への対応（インシデント報告、推進室、IT部門、総務、法務） ・情報セキュリティ対策の見直し（情報の授受方法、携帯端末の取扱い、従業員への周知/教育） ・社外への対応（お客様、警察） 設問3：（以下の観点で報告内容をまとめる。） ・発生状況 ・格納情報（該当のお客様のみの情報） ・時間的経緯 ・再発防止策

4.「情報セキュリティマネジメント評価と改善」コース

◆コース概要	
コース名	情報セキュリティマネジメント評価と改善
スキルカテゴリ	情報セキュリティマネジメントの評価と改善
スキルレベル	中級
コース形態	集合研修（説明とケーススタディ）
研修期間の目安	半日～1日
コース概要	情報セキュリティの評価の基準や部門の情報セキュリティ監査への対応、特に不適合への対応方法について、部門の情報セキュリティマネジメントの観点から、ケーススタディを通じて修得する。
学習目標	・情報セキュリティの評価と改善方法を理解する。 ・具体的な改善施策、再発防止策を立案する。
受講対象者	現在部門内の情報セキュリティ管理を担当しており、主体的に作業を行えることを目指す人。（情報セキュリティ管理者のR2、R3を目指す人）
前提知識	「情報セキュリティマネジメントの技術概要」コースを修了していること。又は同等の知識を有すること。
コースの構成例	第1章　情報セキュリティの評価 情報セキュリティの評価の参照基準について概要を把握する。 ・情報セキュリティ評価の基準（社内の情報セキュリティ規程、ISO15408の概要など） ・各種情報セキュリティ基準の活用場面（部門ルールの作成、情報セキュリティマネジメントシステムの構築、情報セキュリティ監査） 第2章　情報セキュリティ監査への対応と改善 部門の情報セキュリティ管理者に必要とされる監査へ対応や不適合への対応について修得する。 ・情報セキュリティの評価活動の分類（内部監査、外部の監査、審査） ・情報セキュリティ監査で問われること（情報セキュリティ対策の実施状況とそのエビデンス（証跡）、不適合事項への対応状況、環境の変化、新たな脅威への対応状況） ・情報セキュリティ監査への対応（エビデンスの準備、ヒアリングへの対応） ・不適合への対応（情報セキュリティ施策の改善、再発防止策の立案実施） ケーススタディ5「不適合への対応」 ケースを通じて、不適合の是正処置と再発防止策を策定できる。
研修修了後の 取得スキル項目	セキュリティ技術評価、情報セキュリティ監査の実施・支援、セキュリティの分析、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）

◆ケーススタディの解説

ケーススタディ5：「不適合への対応」の解説

（1）ケーススタディ設計の考え方

設定の主旨	部門の情報セキュリティを評価改善するには、情報セキュリティ事故や情報セキュリティ監査からの改善指示などに適切に対応する必要がある。不適合への処置と再発防止の施策策定の方法を身につけるために、ひとつのケースとして掲げてある。
ケース	不適合への対応
目的	情報セキュリティ監査の不適合をどう捉えるか、その対応をどうすべきか、再発防止策をどうするのかについてケーススタディを通じ修得する
何を考えさせるか	情報セキュリティ監査の不適合の理解 不適合への対処（脆弱な箇所を防ぐための対策） 再発防止策（再発を防止するための対策） 不適合対策の報告（実施内容と計画、承認）
対応するスキル項目との関係	情報セキュリティ監査の実施・支援、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）

（2）ケーススタディのサンプル

状況	監査部門の長は、最近の情報セキュリティ事故・事件などの報道から、情報セキュリティ監査を徹底し、情報セキュリティ対策の周知と改善を行うことにした。 その結果、製品の発送部門では、誤記で廃棄する納品書が秘密書類の廃棄箱ではなく、ゴミ箱に捨てられているのが散見され、書類の廃棄規程が順守されていないことが指摘された。 監査では不適合とその是正を指示されたが、情報セキュリティ規程には、秘密書類の廃棄に関する記載はある。しかし、記載ミスの書類の取扱いについては明確に対象とは記載されていなかった。
環境	組織体制と役割定義（推進部門、IT部門、法務、総務） 情報セキュリティ規程（該当インシデントの記載部分） 情報セキュリティ監査規程（不適合への対処部分） 不適合報告書（不適合に関する記載部分）
設問	情報セキュリティ管理者として、本不適合が担当部門で発生したと想定し、以下の設問について検討し、結果を発表しなさい。 設問1：是正処置として、何をどう対処するか検討し、まとめなさい。 設問2：再発防止策として、何をどう対処するか検討し、まとめなさい。 設問3：是正処置及び再発防止策の内容や実施について、協力してもらう部門と依頼内容を列挙しなさい。
解答の観点	設問1：（以下の観点で是正処置を検討する。） ・誤記資料を含めた廃棄対処の明確化 ・廃棄の承認ルールの作成又は見直し 設問2：（以下の観点で再発防止策を検討する。） ・従業員への教育又は周知 ・部門承認者不在時の処置の明確化 ・プリンタ周りへの周知の掲示 設問3：（以下の観点で協力依頼部門を検討する。） ・情報セキュリティ規程類の改定（推進室、監査部門） ・従業員への周知教育（推進室、研修部門、監査部門） ・代理の部門承認者（部門長） ・プリンタ周りへの掲示（総務、推進室）

第３部

情報セキュリティスキルアップ
ハンドブックの活用方法

第1章 活用方法の概要

従来、部門の情報セキュリティ管理者について、共通の業務・役割の定義はなかった。そのため、情報セキュリティ管理者に相当する役割や業務内容を自社で定義し、育成することは大変な作業であった。

本書に記載されている「業務（タスク）やスキル、研修コース体系、研修コース」を参照すれば、情報セキュリティ管理者の確保、育成を効率的に行うことが可能になる。

本書の第1部、第2部では、参照モデルとして、以下の4項目を定義した。

・情報セキュリティ管理者が担う役割と業務内容（以下「役割定義」という。）
・情報セキュリティ管理者の業務（タスク）（以下「タスク定義」という。）
・情報セキュリティ管理者に必要なスキル（以下「スキル定義」という。）
・研修ロードマップ（研修コース体系、研修コース）（以下「研修ロードマップ」という。）

これらの参照モデルは、企業・組織の経営者、最高情報セキュリティ責任者、人材育成責任者、情報セキュリティ管理者自身などを対象とし、幅広く活用していただくことをねらっている。活用主体による代表的な例を以下に示す。

表10　主な活用者と活用場面・活用例

活用者			活用場面	活用例	主な参照先	
					章・節	参照モデル
内部	経営者		情報セキュリティマネジメントを統括、推進する役割や業務を確認したい。	情報セキュリティを管理するための業務を洗い出し、自社の情報セキュリティ推進体制や、情報セキュリティ推進組織の位置づけを確認する際の参考とする。	・第1部 第2章の2	・役割と業務
	最高情報セキュリティ責任者		自社で行うべき事項と外部の情報セキュリティベンダーに依頼する事項を切り分けたい。	部門の情報セキュリティ推進に必要な業務（タスク）を確認し、外部の情報セキュリティベンダーに依頼する事項を切り分ける際の参考とする。	・第1部 第2章の3	・タスク定義
			自社独自の部門の情報セキュリティ管理者の役割や業務を定義したい。	組織の特性を考慮した情報セキュリティの管理を行うために、自社独自に定義すべき事項（役割と業務、タスク、スキル）を検討、定義する際の参考とする。	・第1部 第2章の2 ・第1部 第2章の3 ・第1部 第3章 ・第3部 第3章の1	・役割と業務 ・タスク定義 ・スキル定義
			部門の情報セキュリティ管理者のスキルレベルを確認したい。	業務遂行に必要なスキルを保有しているかを確認するための調査項目（スキル項目）を選定する際の参考とする。	・第1部 第2章の3 ・第1部 第3章 ・第3部 第3章の2	・タスク定義 ・スキル定義
		人材育成責任者	部門の情報セキュリティ管理者育成のために外部研修コースを選定したい。	部門の情報セキュリティ管理者に求められる研修コースを確認し、受講すべき研修コースを選定する際の参考とする。	・第2部 第1章 ・第2部 第2章 ・第3部 第3章の3	・研修ロードマップ
			部門の情報セキュリティ管理者育成のための研修コースを自社内で作成したい。	自社独自の研修コースを作成するために、研修コースの学習内容に含めるべきスキルを確認する際の参考とする。	・第1部 第3章 ・第2部 第1章 ・第2部 第2章 ・第3部 第3章の4	・スキル定義 ・研修ロードマップ
	部門長、管理職、所属長、マネージャー		部門の情報セキュリティ管理者を選出したい。	担当の人選にあたり、部門の情報セキュリティ管理者に必要な役割と業務、スキルを確認する際の参考とする。	・第1部 第2章の2 ・第1部 第2章の3 ・第1部 第3章	・役割と業務 ・タスク定義 ・スキル定義
	情報セキュリティ管理者		部門の情報セキュリティマネジメントを推進するために何が必要かを知りたい。	部門の情報セキュリティ管理者として業務遂行に必要なスキルを確認する際の参考とする。	・第1部 第2章の3 ・第1部 第3章	・タスク定義 ・スキル定義
			受講する研修コースを探したい。	スキルアップするために必要なスキルと研修コースがあるのかを確認する際の参考とする。	・第2部 第1章 ・第2部 第2章	・研修ロードマップ
外部	教育サービス事業者		情報セキュリティ管理者育成のための研修コースを企画、作成したい。	本書の研修ロードマップに合わせ、研修コースを実装する際の参考とする。	・第1部 第3章 ・第2部 第1章 ・第2部 第2章 ・第3部 第3章の5	・スキル定義 ・研修ロードマップ
	コンサルティング会社		情報セキュリティ管理者育成のコンサルティングフレームワークを作成したい。	情報セキュリティ管理者に必要な役割やタスク、スキルを利用する際の参考とする。	・第1部 第2章の2 ・第1部 第2章の3 ・第1部 第3章	・役割と業務 ・タスク定義 ・スキル定義

第2章 本書の活用例

本章では、前述の4つの参照モデルの代表的な活用例を説明する。インプットとなる参照モデル、実施のメリット、活用の手順と実施時のポイント、留意点を下記に整理した。

【活用例】

■活用例A：自社の情報セキュリティ管理者の業務（タスク）とスキルを定義する

■活用例B：情報セキュリティ管理者のスキルレベルを確認する

■活用例C：教育サービス事業者の研修を選定する

■活用例D：自社内で研修コースを作成する

■活用例E：教育サービスを提供する

【活用手順の概要】

各活用例の手順について、概要を以下の表に示した。

表11　活用手順の概要

活用例	インプット	活用手順	アウトプット
A	・本書の役割定義、タスク定義、スキル定義 ・ｉ コンピテンシ ディクショナリ	・推進体制と役割分担の確認 ・役割定義 ・タスクの整理 ・スキルの整理	・自社の情報セキュリティ管理者の役割定義、タスク定義、スキル定義
B	・タスク定義 ・スキル定義 ・ｉ コンピテンシ ディクショナリ	・業務（タスク）とスキルの確認 ・スキルレベルの調査 ・スキルレベルの分析と評価	・部門の情報セキュリティ管理者のスキルレベル分析結果
C	・研修ロードマップ	・研修コース企画 ・外部研修の調査 ・選定・　受講対象者の選抜	・情報セキュリティ管理者の育成計画（研修コース体系、研修コース一覧など）
D	・スキル定義 ・研修ロードマップ	・研修コース企画 ・研修コース設計 ・研修コース開発	・情報セキュリティ管理者の育成計画（研修コース体系、研修コース一覧など）
E	・スキル定義 ・研修ロードマップ	・調査・　分析 ・研修コース企画 ・研修コース設計 ・研修コース開発	・研修コース体系 ・研修コース

活用例Ａ：自社の情報セキュリティ管理者の業務（タスク）とスキルを定義する

企業・組織は、それぞれの情報セキュリティ推進体制にあわせて、個別に業務内容と必要なスキルを明らかにする必要がある。そのうえで、現在の役割分担とその差異から、育成計画や人員計画を立て、部門の情報セキュリティマネジメントを推進することが理想的なアプローチである。しかし、情報セキュリティ管理者の役割や業務内容を定義し、自社で育成していくことは大変な作業となる。そのため、本書を参照し、自社の実情や実績にあわせて定義をカスタマイズすることで、作業負荷の軽減を図ることができる。

企業・組織における情報セキュリティ管理者の役割、タスク、スキルを定義するメリットは、以下のとおりである。

・組織力の強化
　－企業・組織が持つべき情報セキュリティマネジメント機能・役割の可視化
　－組織ごとに求められるタスク、スキルの可視化
　－組織の特徴を取り込むことによる実効性の向上
・人材育成計画の立案
　－組織・部門に最適化した育成計画の検討

情報セキュリティ管理者の役割やタスク、スキルを、企業・組織における現状に合わせ、自社のモデルとして再定義を行う。再定義にあたり、本書の第１部に記載の「情報セキュリティ管理者の役割と業務」「情報セキュリティ管理者に求められる業務（タスク）」「情報セキュリティ管理者に求められるスキル」をリファレンスとして活用できる。

企業・組織ごとに情報セキュリティ管理者の役割やタスク、スキルを定義する場合の手順と作業のポイント・留意点を以下に示す。

図６　活用例Ａの活用手順

手順１　推進体制と役割分担の確認

現状の情報セキュリティ管理の推進体制や役割分担を確認する。

確認すべき主なポイント

・情報セキュリティ管理体制とその取り組み範囲
・情報セキュリティの技術面の実行・支援の体制
・ISMSなどの既存のマネジメントシステムの取り組み状況
・個人情報保護などの既存のセキュリティ関連の取り組み状況

・部門が独自に保有する製品やサービス

留意点

部門の情報セキュリティマネジメントの推進に携わる方には、高度なセキュリティ技術を求めないこと。そのため、他の組織や専門技術者からの支援を受けることが可能かどうかを十分に確認することに留意する。

手順２　役割定義

「第1部 第2章 情報セキュリティ管理者の役割と業務」に記載の「役割と業務」を参照し、自社に求められる役割と業務の再定義を行う。

役割と業務の再定義は、自社の情報セキュリティマネジメント業務の実情と照らし合わせ、役割と業務の追加・削除を行うこと、また組織独自のルールや用語の表現などの内容修正を行うことである。

考慮すべき主なポイント

・手順１で整理した推進体制と役割分担をもとに、上位者や推進組織及び専門技術者との関わりを示す

・部門の情報セキュリティ管理者への指揮命令系統を考慮する

・部門の情報セキュリティ管理者として実行できる権限を考慮する

・具体的な業務や行動を意識し再定義を行う

留意点

部門の情報セキュリティ管理者が実行しない業務がある場合は、役割や業務から削除する形で再定義を行う。そして、削除した役割や業務については、推進組織や専門技術者が担当し、全体として情報セキュリティマネジメントの実行に抜け漏れがないことの確認を行う必要がある。また、業務の内容とその責任範囲に矛盾がないこともあわせて確認することが必要である。

手順３　タスクの整理

「第１部 第２章 情報セキュリティ管理者の役割と業務」に記載の「情報セキュリティ管理者に求められる業務（タスク）」を参照し、自社に求められるタスクの再定義を行う。

タスクの再定義は、部門の情報セキュリティ管理者に求められるタスクの追加、削除のほか、組織独自ルールや用語表現などの内容修正を行うことである。部門の情報セキュリティ管理者に求められるタスクを追加する場合は、ｉ コンピテンシ ディクショナリを参照することで、効率的に追加作業を進めることが可能である。

考慮すべき主なポイント

・「情報セキュリティ管理者に求められる業務（タスク）」が示すタスクの業務内容を正しく理解する

・上記をもとに、現状と将来を踏まえたタスクを再定義する

・必要なタスクが既存のタスク一覧に存在しなければ追加し、抜け漏れをなくす

・特に、組織や部門独自のタスクを含める

留意点

タスクを再定義する際は、部門の情報セキュリティに関するタスクを対象として再定義を行う。推進組織や専門技術者など、他の役割が主務として担うタスクとは重複しないことが求められる。例えば、全社の情報セキュリティポリシ作成のタスクや、情報システムの開発に関わるタスク、情報システムの運用に関わるタスクなどである。

手順4　スキルの整理

「第1部 第3章　情報セキュリティ管理者に求められるスキル」に記載のスキルを参照し、自社に求められるスキルの再定義を行う。スキルの再定義は、部門の情報セキュリティ管理者に求められるスキルの追加、削除のほか、組織独自ルールや用語表現などの内容修正を行うことである。部門の情報セキュリティ管理者に求められるスキルを追加する場合には、ｉ コンピテンシ ディクショナリを参照することで、効率的に追加作業を進めることができる。

考慮すべき主なポイント

・「情報セキュリティ管理者に求められるスキル」が示すスキルの内容を正しく理解する
・上記をもとに、現状と将来を踏まえたスキルを再定義する
・ｉ コンピテンシ ディクショナリを活用した場合は、タスクと連係したスキルを特定する
・対応した資格がある場合は、試験内容のシラバスを確認し、スキルを特定する

留意点

再定義したスキルは、スキルカテゴリで分類し、育成計画の検討や教育プログラムの選定に使いやすい形にまとめることが求められる。さらに、手順3、4で再定義したタスクとスキルの関係性を整理することで、情報セキュリティ管理者の業務と、求められるスキルが関連づけられる

活用例Ｂ：情報セキュリティ管理者のスキルレベルを確認する

部門の情報セキュリティマネジメントを推進するには、業務遂行のためのスキルレベルを把握し、教育・訓練を行う必要がある。推進者の教育・訓練を行うためには、部門の情報セキュリティマネジメントの構築、運用、評価と改善が正常に遂行できるスキルがあるか、また、その体制が整っているかを明らかにする必要がある。

本書を参照して情報セキュリティマネジメントに必要なタスク、スキルを確認し、そのタスクとスキルのレベルを調査することで、情報セキュリティの実情を可視化できる。これにより、教育・訓練などの処置を検討することが可能となる。

自社の情報セキュリティ管理者のスキルレベルを把握することのメリットは、以下のとおりである。

・組織力の強化
　－情報セキュリティのスキルレベルの可視化
　－要員選択の客観性の担保
・人材育成計画の立案

－情報セキュリティ管理者の現状と強化ポイントの明確化
－経験、スキルを得るための教育企画への提言

情報セキュリティ管理者のスキルレベルの確認にあたっては、本書の第1部に記載の「情報セキュリティ管理者に求められる業務（タスク）」や「情報セキュリティ管理者に求められるスキル」をリファレンスとして活用できる。

情報セキュリティ管理者のスキルレベルを確認する場合の手順と作業のポイント・留意点を以下に示す。

図７　活用例Ｂの活用手順

手順１　業務（タスク）、スキルの確認

部門の情報セキュリティ管理者に求められる業務（タスク）とスキルを確認する。

確認すべき主なポイント

・業務（タスク）とスキルの内容を確認する
・理想とするスキルレベル（あるべき姿）を設定する
・現在の育成の取り組み状況とその対象となる業務（タスク）、スキルの関係性を確認する

留意点

スキルレベルを評価・分析するためには、理想とするスキルレベル（あるべき姿）を想定しておくことが重要である。スキルレベルを評価する前に「どの程度の要員が必要なのか」「どのレベルまでを目指すのか」「どういった育成の施策を行ってきているのか」など、現状と将来を見据えることが重要となる。

手順2　スキルレベルの調査

スキルレベルの調査では、部門の情報セキュリティ管理者に求められるタスクとスキルの現状を調査する。調査にあたっては、タスク遂行の実績と保有スキルを調査するための、調査票を用意し、部門の情報セキュリティ管理者に対して調査を行う。

考慮すべき主なポイント

・評価・分析を行いやすくするため、スキルレベルの調査結果は定量的データとして測定・収集する
・i コンピテンシ ディクショナリに記載されている「評価の診断基準例」などを参考とする
・スポットの調査ではなく、継続的にスキルレベルを調査する
・調査結果のデータは履歴管理できる形式とする

留意点

部門の情報セキュリティ管理は、部門長にマネジメント責任がある場合が多い。そのため、スキルレベル調査においては、部門の情報セキュリティ管理者だけではなく、部門長も含めた範囲でスキルレベルの調査を行うかを検討する必要がある。

手順3　スキルレベルの分析と評価

部門の情報セキュリティの情報セキュリティ管理者が保有する現状のスキルレベルを可視化し、分析し評価を行う。スキルレベルの分析と評価では、全社・部門ごとの分析、あるべき姿とのギャップ分析などを行い、人材の確保や育成における課題を抽出し、評価することである。

考慮すべき主なポイント

・分析を行う前に、どのような傾向となり、どのような対策が必要となるかの仮説を設定しておく
・仮説をもとに部門別や年度別、タスク別など様々な視点で分析を行い、仮説の検証を行う
・あるべき姿とのギャップ分析を行い、強化ポイントを明確にする
・結果の考察を行い教育企画への提言を行う

留意点

部門の情報セキュリティ管理者は、組織構成の変更や所属の異動により変更が発生することが想定される。これにより、経年変化を分析・評価した場合、スキルレベルが下がることがあることを認知する必要がある。

活用例Ｃ：教育サービス事業者の研修を選定する

部門の情報セキュリティマネジメントを推進するには、情報セキュリティ管理者の育成が重要である。育成手段のひとつに、研修コースの受講がある。育成に必要な研修は企業・組織によって異なるため、自社に必要な研修を洗い出し、自社の情報セキュリティ管理者育成の研修ロードマップを明確にすることが求められる。

自社の情報セキュリティ管理者育成に必要な研修は、教育サービス事業者の研修を選定する方法がある。

教育サービス事業者の研修を選定するメリットは以下のとおりである。

・既存の研修が利用できる
　－研修コース開発にかかるコストの削減
・情報セキュリティの標準的な知識と対処方法を学習できる

教育サービス事業者の研修を選定する場合の手順と作業のポイント・留意点を以下に示す。

図８　活用例Ｃの活用手順

手順１　研修コース企画

本書の研修ロードマップと情報セキュリティ管理者のスキルレベル分析の結果などから、現在の情報セキュリティ管理者に不足しているスキル、今後強化していきたいスキル、自社に必要な研修などを確認し、外部研修コースの調達基準を調査し、決定する。

確認すべき主なポイント

・予算
・育成目標
・研修の必要性と目的
・強化すべきスキル
・研修修了後の達成目標
・研修内容
・自社のコース体系
・外部研修コースの調達基準

手順２　外部研修の調査・選定

外部研修コースの調達基準と一致する外部研修があるかを調査し、自社の育成計画に合致する研修を選定する。選定した研修をもとに、自社の情報セキュリティ管理者育成の研修コース体系や研修一覧に反映する。

確認すべき主なポイント

・教育サービス事業者のコース調査（費用、カリキュラム、講師など）
・研修の開催方法の検討（教育サービス事業者の定期開催、一社向け個別開催）
・開催スケジュール
・育成計画

手順３　受講対象者の選抜

企画内容、研修コース体系、コース一覧をもとに、受講対象者の選抜方法、募集方法を検討し、受講対象者を決定する。

確認すべき主なポイント

・対象者の選定方法
　－CISO（情報セキュリティ推進組織）からの指名、現場からの推薦などを考慮する
　－新任の場合は、受講を必須にするような仕組みにする
・対象者の募集方法
・受講結果評価や受講履歴の保存の方法

留意点

一社向け個別開催の場合は、自社における情報セキュリティ規程や情報環境にあわせたケースの変更など、研修内容のカスタマイズが可能な場合があり、自社の育成目標に近い、効果的な育成が可能となる。

活用例Ｄ：自社内で研修コースを作成する

部門の情報セキュリティマネジメントを推進するには、情報セキュリティ管理者の育成が重要である。育成手段としては、研修コースの受講がある。育成に必要な研修は、企業・組織によって異なるため、自社に必要な研修を洗い出し、自社の情報セキュリティ管理者育成の研修ロードマップを明確にすることが求められる。

自社の情報セキュリティ管理者育成に必要な研修は、自社内で研修コースを作成する方法がある。

自社内で研修コースを作成するメリットは以下のとおりである。

・自社に合致した研修内容で情報セキュリティ管理者の育成が可能となる
　－自社内の環境に応じた具体的な操作方法なども教育できる

自社内で研修コースを作成する場合の手順と作業のポイント・留意点を以下に示す。

図９　活用例Ｄの活用手順

手順１　研修コース企画

本書の研修ロードマップと情報セキュリティ管理者のスキルレベル分析の結果などから、現在の情報セキュリティ管理者に不足しているスキル、今後強化していきたいスキル、自社に必要な研修などを確認し、研修コース体系の検討と新規で作成するコースを洗い出す。新規で作成するコースは、本書の研修コース内容を参考にし、コース概要などを決める。

確認すべき主なポイント

・予算
・育成目標
・研修の必要性と目的
・強化すべきスキル
・研修修了後の達成目標
・研修内容
・自社の研修コース体系
・新規で開発するコースの選定とコース企画
　－コース体系、コース名、スキルカテゴリ、スキルレベル、コース形態、期間、コース概要、学習目標、受講対象者、前提知識、演習環境など
・開発体制、開発スケジュール、提供時期、教材開発スキル

手順2　研修コース設計

新規コースはコース企画をもとに、コース設計（概要設計、構成設計、詳細設計）を行う。研修コース設計は、本書のタスク定義とスキル定義を参考にする。新規作成する研修コースは、自社の情報セキュリティ管理者の研修コース体系や研修一覧に反映する。

確認すべき主なポイント

・研修のリソース（講師、教室、環境など）
・構成設計（目次）
・詳細設計
・タイムテーブル
・演習・ケーススタディ設計
・学習目標を達成するために必要なタスク、スキルを参考にした設計

手順3　研修コース開発

各社の開発プロセスに準ずる。

留意点

研修コース企画、研修コース設計においては、自社で実現可能かどうかを考慮する。教材作成スキルが不足している場合は、外部発注して作成することも可能である。

活用例Ｅ：教育サービスを提供する

教育サービス事業者は、市場のニーズにあった研修コースの提供が求められる。本書は、情報セキュリティ管理者が担うタスクとスキルが定義されているため、情報セキュリティ管理者に必要なスキル修得のための研修コースを効率よく提供できる。

教育サービス事業者が教育サービスを提供するメリットは以下のとおりである。

・情報セキュリティ管理者に必要なスキル調査を簡素化できる
・標準の研修コース体系に沿ったコース提供が可能になる

教育サービスを提供する場合の手順と作業のポイント・留意点を以下に示す。

図10　活用例Ｅの活用手順

手順１　調査・分析

本書の確認、及び市場動向、技術動向、他社動向、顧客ニーズ、現状の調査、分析を行う。

確認すべき主なポイント

・市場動向調査
・技術動向調査
・顧客ニーズ調査・分析
・他社動向調査
・現状分析

手順２　研修コース企画

市場調査、ニーズ調査・分析などの結果や本書の研修ロードマップから、ビジネスプランを作成し、研修コース体系を作成する。新規に研修コースを作成する場合は、本書の研修コース内容を参考にし、コース概要などを決める。

確認すべき主なポイント

・ビジネスプラン
・研修コース体系
・新規で開発するコースの選定とコース企画
　－コース体系、コース名、スキルカテゴリ、スキルレベル、コース形態、期間、コース概要、学習

目標、受講対象者、前提知識、演習環境など

・開発体制、開発スケジュール、提供時期、教材開発スキル

・コース価格

手順３　研修コース設計

新規コースはコース企画をもとに、コース設計（概要設計、構成設計、詳細設計）を行う。研修コース設計は、本書のタスク定義とスキル定義を参考にする。新規作成する研修コースは、情報セキュリティ管理者の研修コース体系や研修一覧に反映する。

確認すべき主なポイント

・研修のリソース（講師、教室、環境など）

・構成設計（目次）

・詳細設計

・タイムテーブル

・演習・ケーススタディ設計

・学習目標を達成するために必要なタスク、スキルを参考にした設計

手順４　研修コース開発

各社の開発プロセスに準ずる。

留意点

研修ロードマップでは、研修コースのコース形態や期間、コース構成などに幅を持たせており、教育サービス事業者がより実践的な研修コースを開発できるように、教育サービス事業者の強みを活かして最適化できるようにしている。

添　付　資　料

添付 1：タスクとスキル項目の対応表

添付 2：研修コースとスキル項目の対応表

■添付1：タスクとスキル項目の対応表

タスク大分類	タスク中分類	スキルカテゴリ（独自）	スキルカテゴリ（詳細）	対応する主なスキル項目（i コンピテンシ ディクショナリ）
システム企画立案	情報セキュリティ要件定義	情報セキュリティ技術の概要	情報セキュリティ管理技術の概要	情報セキュリティ管理手法
システム要件定義・方式設計	システム化要件定義	情報セキュリティ技術の概要	情報セキュリティ管理技術の概要	情報セキュリティ管理手法
IT運用コントロール	IT運用管理	情報セキュリティ技術の概要	セキュリティ技術の概要	運用オペレーション手法
	情報セキュリティ管理	情報セキュリティ技術の概要	セキュリティ技術の概要	暗号技術、セキュリティと個人情報、情報セキュリティ管理
		情報セキュリティ技術の概要	インフラセキュリティ技術の概要	セキュリティ技術の理解と活用
		情報セキュリティマネジメントの構築	ISMS構築	セキュリティ方針の策定、セキュリティ対策基準の策定、情報セキュリティ対策
		情報セキュリティマネジメントの構築	情報セキュリティシステムの構築	セキュリティシステムの計画策定、セキュリティシステムの要件定義
		情報セキュリティマネジメントの運用	—	情報倫理とセキュリティ
システム運用管理	セキュリティ障害管理	情報セキュリティマネジメントの運用	—	セキュリティ障害（事件事故/インシデント）管理
資産管理・評価	資産管理規定の策定	情報セキュリティマネジメントの構築	ISMS構築	資産管理に関する手法
	資産管理プロセスの実施	情報セキュリティマネジメントの構築	ISMS構築	資産管理に関する手法
事業継続マネジメント	事業継続計画の策定	情報セキュリティマネジメントの構築	ISMS構築	BCP策定手法、災害対策管理手法
情報セキュリティマネジメント	情報セキュリティ戦略と方針の策定	情報セキュリティ技術の概要	情報セキュリティ管理技術の概要	リスク管理手法
		情報セキュリティ技術の概要	情報セキュリティ管理技術の概要	情報セキュリティ管理手法
	情報セキュリティの運用	情報セキュリティ技術の概要	情報セキュリティ管理技術の概要	情報セキュリティ管理手法
	情報セキュリティの見直し	情報セキュリティ技術の概要	情報セキュリティ管理技術の概要	情報セキュリティ管理手法
		情報セキュリティ技術の概要	情報セキュリティ管理技術の概要	リスク管理手法
契約管理	契約締結管理	情報セキュリティマネジメントの構築	法規の導入	契約事務手法
コンプライアンス	管理方針と体制	情報セキュリティマネジメントの構築	ISMS構築	内部統制
		情報セキュリティマネジメントの構築	法規の導入	セキュリティ関連法規
	実施と評価	情報セキュリティマネジメントの構築	ISMS構築	内部統制
調達・委託	委託業務管理	情報セキュリティマネジメントの構築	法規の導入	セキュリティ関連法規

■添付2：研修コースとスキル項目の対応表

スキルカテゴリ（独自）		i コンピテンシ ディクショナリ		研修コース			
				初級	中級		
スキル カテゴリ（独自）	スキル カテゴリ（独自・詳細）	スキル分類	スキル項目	情報セキュリティマネジメントの技術概要	情報セキュリティマネジメント構築	情報セキュリティマネジメント運用	情報セキュリティマネジメント評価と改善
情報セキュリティ技術の概要	IT基礎技術の概要	(共通技術) IT基礎	コンピュータシステムの構成	○			
			システムの構成	○			
			システムの評価指標				
	セキュリティ技術の概要	(非機能要件) セキュリティの基礎技術	情報セキュリティ	○			
			暗号技術	○			
			セキュリティと個人情報	○			
		(非機能要件) セキュリティの構築技術	コンピュータ・フォレンジクス（証拠保全追跡）				
		(非機能要件) セキュリティの利用技術	情報セキュリティ管理	○			
	情報セキュリティ管理技術の概要	(支援活動) リスクマネジメント手法	リスク管理手法	○			
			情報セキュリティ管理手法	○			
	インフラセキュリティ技術の概要	(非機能要件) セキュリティの基礎技術	アプリケーションセキュリティ				
			情報プラットフォームのセキュリティ技術	○			
			ネットワークのセキュリティリスク	○			
			セキュリティ技術の理解と活用	○			
		(利活用) サービスの運用	システム運用管理手法				
情報セキュリティマネジメントの構築	ISMS構築	(支援活動) ITガバナンス	内部統制				
		(支援活動) 資産管理手法	資産管理に関する手法		○		
		(支援活動) 事業継続計画	BCP策定手法				
			災害対策管理手法				
		(非機能要件) セキュリティの基礎技術	情報保証と情報セキュリティ		○		
			セキュリティ方針の策定		○		
			セキュリティ対策基準の策定		○		
			情報セキュリティ対策				
	情報セキュリティシステムの構築	(非機能要件) セキュリティの構築技術	セキュリティシステムの計画策定				
			セキュリティシステムの要件定義				
	法規の導入	(企画) セールス事務管理手法	契約事務手法		○		
		法規・基準・標準	セキュリティ関連法規		○		
情報セキュリティマネジメントの運用		(非機能要件) セキュリティの基礎技術	情報倫理とセキュリティ			○	
		(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				
			システム運用・保守技術（セキュリティ）				
			セキュリティ障害（事件事故/インシデント）管理			○	
情報セキュリティマネジメントの評価・改善	評価基準	(非機能要件) セキュリティの基礎技術	保証、信用、信頼のメカニズム				
		(非機能要件) セキュリティの利用技術	セキュリティ技術評価				○
	評価・改善	(非機能要件) セキュリティの利用技術	情報セキュリティ監査の実施・支援				○
			セキュリティの分析				○
			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）				○

情報セキュリティスキルアップハンドブック
～情報セキュリティマネジメント人材育成のために～

2015年 9月15日　初版第1刷発行

発行　　独立行政法人情報処理推進機構　IT人材育成本部　HRDイニシアティブセンター
所在地　〒113-6591 東京都文京区本駒込 2-28-8　文京グリーンコート　センターオフィス15階
電話　　03-5978-7544
http://www.ipa.go.jp/jinzai/hrd/index.html

ISBN978-4-905318-33-0

9784905318330

1923055009264

ISBN978-4-905318-33-0
C3055　¥926E

定価　1,000円(税込)

IPA