情報システムユーザースキル標準
モデルカリキュラム

(14)セキュリティ　編

Ver.2.2

2009.3

経　　済　　産　　業　　省
独立行政法人情報処理推進機構(IPA)
社団法人日本情報システム・ユーザー協会
情報システムユーザースキル標準センター

もくじ　　はじめに

はじめに

１．モデルカリキュラムの主旨

情報システムユーザースキル標準 Ver.2.0(UISS Ver.2.0)の研修ロードマップは、情報システム部門の機能に対応した研修コースとして体系的に整理されています。

各研修コースは、研修を実施する際の「コースのねらい」や想定される「受講対象者」、研修に期待する「スキル修得目標」や研修内容と係わる「関連知識」などを定義しています(図１参照)。しかし、具体的な教育内容や教育方法については、各企業や受講者および研修の実施者がその状況に応じて柔軟に対応できることが望ましく、研修ロードマップでは規定していません。

コース名 / 研修コースの内容	セキュリティ技術初級
講座分類	□入門　■初級　□中級　□上級　□特論
コースのねらい	当コースは、セキュリティについて、指導の下または一定程度であれば独力でセキュリティに関する作業ができる基本的な知識を修得することを目的とする。 ○　当コースでは、ＩＳの構築・運用等におけるセキュリティの考え方、セキュリティ機能、および同機能の設計・運用等の業務の概要に関する基礎知識を学習する。
受講対象者	ＩＳ部門、または業務部門において、上位者の指導の下で、セキュリティを考慮したＩＳ構築、運用ができることを目指す者
研修方法	講義およびｅラーニング
研修期間	標準日数　1日（クラスルーム）、標準時間　6時間（ｅラーニング）
スキル修得目標	セキュリティの意義を理解できる。 セキュリティ関連業務における自らおよび他のメンバの役割分担を認識できる。 上位者の指導の下で、セキュリティ機能を設計・構築・運用に関する業務を担当することができる。
関連知識	以下の事項の入門的な知識 ・人的セキュリティ対策、技術的セキュリティ対策、物理的セキュリティ対策 ・セキュリティ要素技術（暗号化技術、認証技術、利用者確認、生体認証技術、公開鍵基盤、政府認証基盤、セキュアOS、アプリケーションセキュリティ、セキュアプログラミング等）

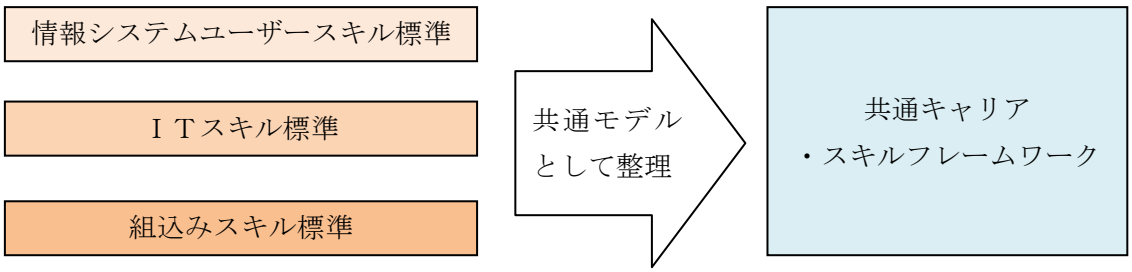
（図１）研修コース（セキュリティ　セキュリティ技術）の内容

本モデルカリキュラムは、研修ロードマップに従って研修コースを設計・実施する場合の参考情報として、またそれを受講する場合の参考情報として活用できるように整理しています。

２．共通キャリア・スキルフレームワークとの関係

共通キャリア・スキルフレームワークは、先行して策定・定義した情報システムユーザースキル標準をはじめ、IT スキル標準、組込みスキル標準の３つのスキル標準に共通したモデルとして整理されたもの(図２参照)です。

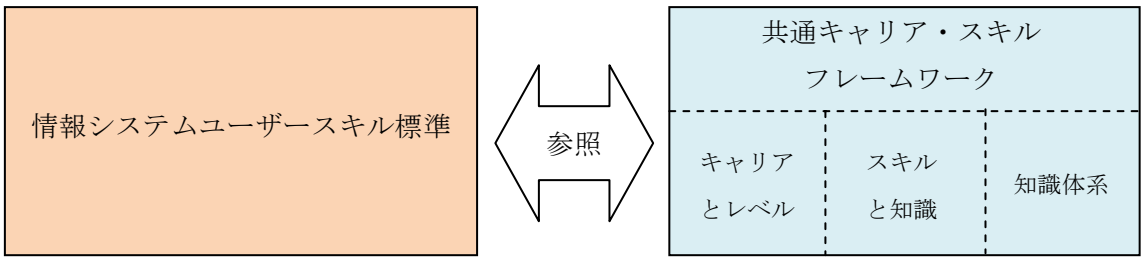
したがって、共通キャリア・スキルフレームワークは、3 つのスキル標準を共通化した高度 IT 人材に係わる人材像とその保有すべき能力や果たすべき役割について纏めた人材育成および評価の枠組みといえます。



（**図２**）３つのスキル標準と共通キャリア・スキルフレームワーク

共通モデルとして策定・定義した共通キャリア・スキルフレームワークと情報システムユーザースキル標準とは、相互に参照し合う関係となっています。

共通キャリア・スキルフレームワークは、３つのスキル標準に対して、①.キャリアとレベル、②.知識とスキル、③. 知識体系(BOK : Body of Knowledge)を共通のものとして体系化していますので、情報システムユーザースキル標準の研修コースごとに定義した知識項目を参照することで、共通キャリア・スキルフレームワークのスキル知識体系の知識項目と関連付けること（図 3 参照）が可能となります。



（**図３**）情報システムユーザースキル標準と共通キャリア・スキルフレームワーク

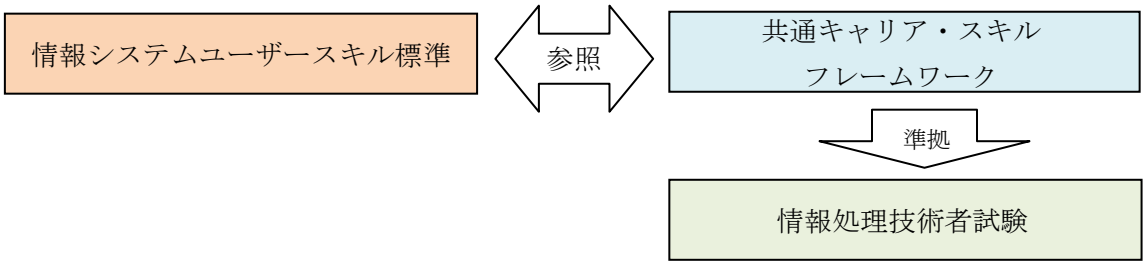
情報システムユーザースキル標準では、共通キャリア・スキルフレームワークの「キャリアとレベル」に準拠して、キャリアレベルを７段階のレベルで定義しています。

本モデルカリキュラムは、共通キャリア・スキルフレームワークを構成する「スキルと知識」および「知識体系」に基づき、知識分野や各研修コースで修得すべき関連知識を定義するほか、研修コースの編成等においても「スキルと知識」および「知識体系」を利用しています。

３．情報処理技術者試験との関係

情報処理技術者試験の体系は、原則として共通キャリア・スキルフレームワークに準拠して設計されています。したがって、情報処理技術者試験は、共通キャリア・スキルフレームワークに基づいた試験制度といえます。

本モデルカリキュラムは、共通キャリア・スキルフレームワークを参照していますので、それを介して情報処理技術者試験と関連付けされていることになります。したがって、知識体系だけでなく、試験制度のレベル区分にも準拠している(図４参照)といえます。



（**図４**）情報システムユーザースキル標準と情報処理技術者試験

第１章　本編の概要

１．セキュリティ

本モデルカリキュラムは、研修ロードマップに示した「セキュリティ」研修コースのシラバスをまとめたものです。

本モデルカリキュラムに基づく研修コースを履修することにより、情報システムユーザースキル標準のレベル２、レベル３およびレベル４に対応するセキュリティに必要な知識をそれぞれ効率的に習得することができます。

２．対象

本モデルカリキュラムは、情報システム部門に配属され、セキュリティ領域の業務に携わる人が必要とする知識とスキルを習得することを目的としており、以下の方々を対象人材として想定しています。

＜対象人材＞

1. 情報セキュリティを考慮した企画・導入・運用などの業務を担当または管理する方
2. 情報システムのセキュリティ設計やセキュリティ技術の実装など、セキュリティを直接構築・運用される方
3. セキュリティポリシやセキュリティ対策基準などのセキュリティ関連法規やガイドラインに基づいたセキュリティガイドライン等を策定する方　など

なお、これらの方々を対象とする研修(教育)場面は、企業の側面と個人の側面から想定しています。

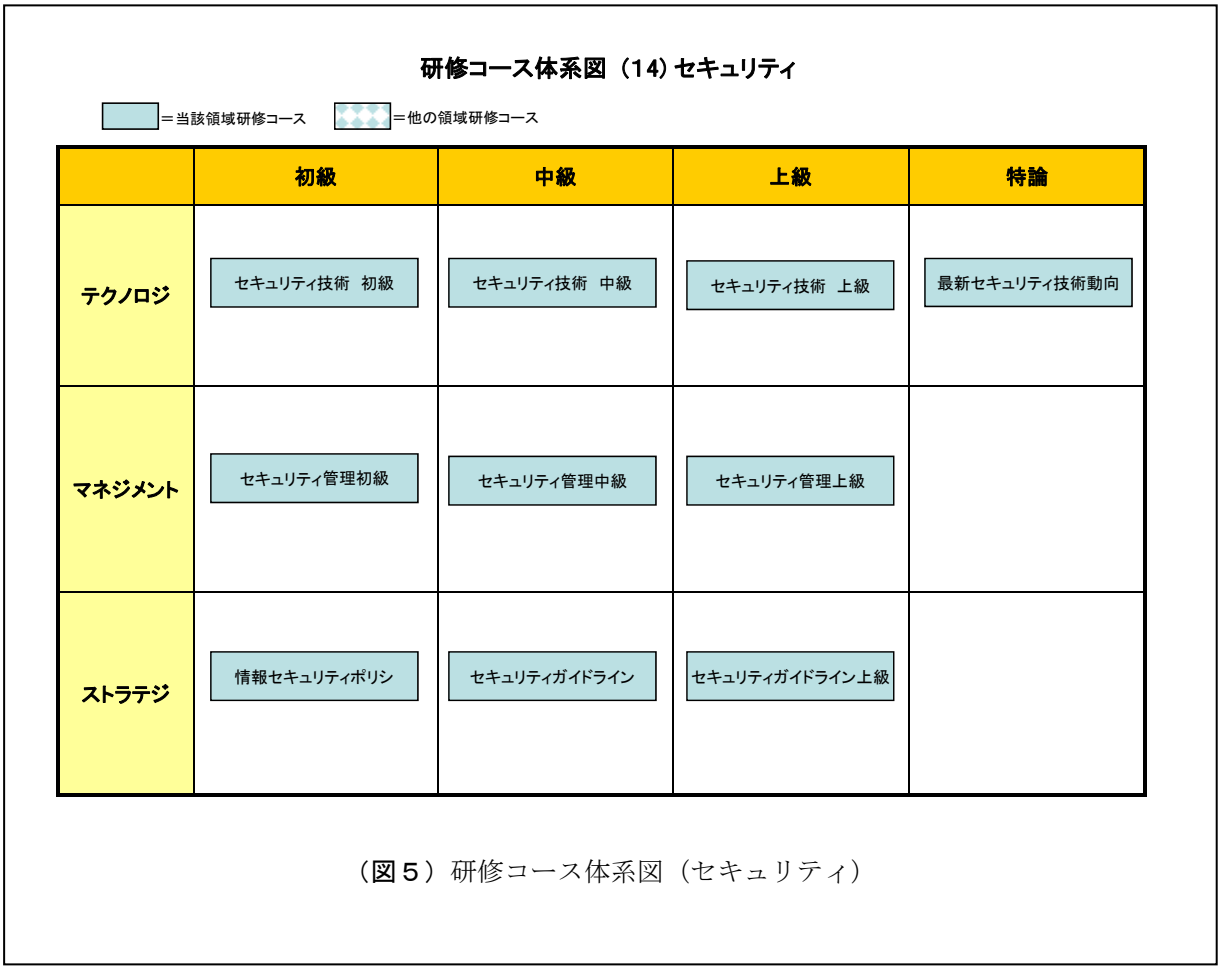
＜想定場面＞

1. 企業においては、キャリアチェンジなど人材育成戦略の一環として
2. 個人においては、キャリアアップの手段として

３．研修ロードマップとの関係

本モデルカリキュラムは、「セキュリティ」領域の研修コースをモデルカリキュラムとしてまとめたものです。したがって「セキュリティ」の研修コース体系図(図 5 参照)に規定された研修コースに対し、それぞれのシラバスを作成しています。

ただし、特別講義に分類した「最新セキュリティ技術動向」は、今後の動向という不確定要素を含むため、本モデルカリキュラムでは対象外としました。



（図５）研修コース体系図（セキュリティ）

セキュリティは、共通キャリア・スキルフレームワークの大分類ではテクノロジに区分されています。したがって、研修ロードマップに於いても「セキュリティ」の全体は、大分類としてはテクノロジに区分されます。

しかし、研修コースは、中分類の機能・役割に対応しており、その内容からテクノロジ系・マネジメント系・ストラテジ系という 3 つの分野(表 1 参照)で構成しています。

（表１）中分類と内容

分野	内容
テクノロジ系	セキュリティの設計、セキュリティ実装技術などの技術に関わる知識
マネジメント系	セキュリティの運用管理などに関わる知識
ストラテジ系	セキュリティポリシやガイドラインなどの関わる知識

研修ロードマップでは、講義・ワークショップ・ｅラーニングのコース区分、講義やワークショップの標準日数やｅラーニングの標準時間を研修コース一覧表(図６参照)に提示しています。

したがって、本モデルカリキュラムにおいては、研修ロードマップに基づいた標準日数や標準時間を設定しています。

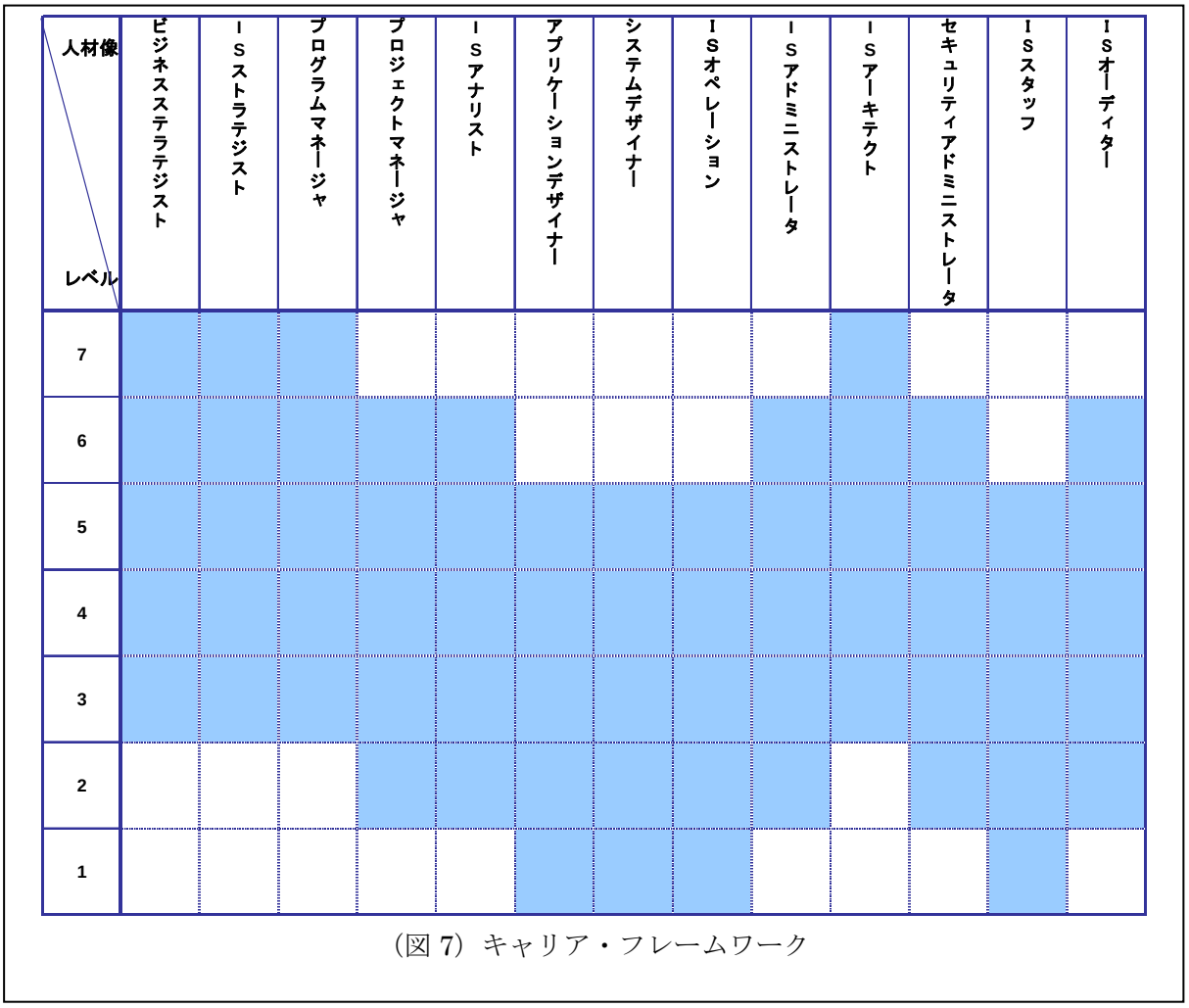
研修コース一覧（14）セキュリティ

分類	コース名	研修方法			研修期間		ページ	備　考（参照先）
		eラーニング	講義	ワークショップ	eラーニング（標準時間）	クラスルーム（標準日数）		
初級	セキュリティ技術初級	○	○		6時間	1日間	(14)-4	
	セキュリティ管理初級	○	○		6時間	1日間	(14)-7	
	セキュリティポリシ	○	○		6時間	1日間	(14)-10	
中級	セキュリティ技術中級	○	○	○	12時間	3日間	(14)-5	
	セキュリティ管理中級	○	○	○	12時間	3日間	(14)-8	
	セキュリティガイドライン	○	○	○	12時間	3日間	(14)- 11	
上級	セキュリティ技術上級		○	○		3日間	(14)-6	
	セキュリティ管理上級		○	○		3日間	(14)-9	
	セキュリティガイドライン上級		○	○		3日間	(14)-12	
特論	最新セキュリティ技術動向		○			1日間	(14)-13	

（図６）研修コース一覧表（セキュリティ）

４．レベルの定義

本モデルカリキュラムは、原則として情報システムユーザースキル標準のキャリア・フレームワーク(図７参照)のレベルに対応しています。



（図 7）キャリア・フレームワーク

研修ロードマップの「セキュリティ」に対応する人材像は「セキュリティアドミニストレータ」です。セキュリティアドミニストレータのキャリアレベルは「レベル２～６」で、レベル１の人材ではセキュリティアドミニストレータの業務を担当することは厳しいことを表しています。

しかし、情報システムに携わる者として必要な最低限の基礎的な知識として、レベル１が存在する他の人材像においてセキュリティの知識が必要となる場面があります。人材像に共通したレベルは、共通キャリア・スキルフレームワークで定義されています。そこで、本カリキュラムガイドでは、共通キャリア・スキルフレームワークのレベル定義に準拠するものとします。

なお、特別講座はレベルとは関係なく、最新技術動向やビジネス動向が変化する都度、該当するものを受講することが望ましいコースとして設定しています。

５．対応する情報処理技術者試験

本モデルカリキュラムのレベル定義は、共通キャリア・スキルフレームワークに準拠します。

したがって、情報処理技術者試験とは、共通キャリア・スキルフレームワークのレベルを通じて関連付けすることができます。

しかしながら、本モデルカリキュラムの内容は、情報システムユーザースキル標準に対する研修コースの情報に基づいていますので、ここで提供するすべての研修コースを履修しても、情報処理技術者試験の出題領域をすべて網羅しているとは限りません。情報処理技術者試験を受験する場合は、情報処理技術者スキル標準等で出題領域を確認するようにしてください。

（表２　講座区分、レベル、情報処理技術者試験の関係）

講座区分	レベル	情報処理技術者試験
入門講座	レベル１	IT パスポート試験
初級講座	レベル２	基本情報技術者試験
中級講座	レベル３	応用情報技術者試験
上級講座	レベル４	高度試験（情報セキュリティスペシャリスト試験）
特別講座	－	－

第２章　企業における活用方法

１．企業で活用する意義

本モデルカリキュラムでは、情報システム部門でセキュリティに関わる「情報セキュリティに関する知識とスキルが必要な企画・導入・運用などの業務を担当または管理される方」「情報システムのセキュリティ設計、セキュリティ技術の実装など、セキュリティを構築や運用される方」「セキュリティポリシやセキュリティ対策基準などのセキュリティ関連法規やガイドラインに基づいたセキュリティガイドライン等の策定をする方」を想定しています。

したがって、この情報を活用することにより、セキュリティ部門だけでなく、ＩＳ企画・ＩＳ導入・ＩＳ運用などに関わる人材へのセキュリティ研修として、限られた期間で体系的に行うことができます。また、研修コースの内容を確認することにより、効率的な実施計画を立案することもできます。

２．研修日数・時間

本モデルカリキュラムでは、講義中心の研修コースは 90 分単位のコマに分割し、4 コマから 8 コマで構成しています。したがって、半日研修の場合は 2 コマ、終日研修の場合は 4 コマを割り当てて実施します。また、ワークショップ中心の研修コースは 180 分単位のコマに分割し、6 コマで構成しています。したがって、終日研修の場合は 2 コマを割り当て、3 日間で実施します。

３．レベル

本モデルカリキュラムは、初級講座・中級講座・上級講座の研修コースごとの内容を定義し、情報として提供しています。

受講にあたり、同一レベルの講座はすべて受講することが望ましいのですが、ストラテジ系・マネジメント系・テクノロジ系と専門性が強い業務の場合には、該当する分野だけを受講するだけでも構いません。

４．中分類

セキュリティの大分類はテクノロジです。

しかし、ここで定義する研修コースは、中分類の機能・役割に対応しており、その内容によりストラテジ系・マネジメント系・テクノロジ系と 3 つの分野に区分しています。研修コースのレベルと分野の関係を表 3 に示します。

（表３）セキュリティの研修コース

	テクノロジ系	マネジメント系	ストラテジ系
初級講座	セキュリティ技術初級	セキュリティ管理初級	情報セキュリティポリシ
中級講座	セキュリティ技術中級	セキュリティ管理中級	セキュリティガイドライン
上級講座	セキュリティ技術上級	セキュリティ管理上級	セキュリティガイドライン上級

（注　入門講座は、「ＩＳ入門・カリキュラムガイド」をご覧ください。
本カリキュラムガイドには、特別講座の研修コースは紹介していません。

第３章　コース詳細

１．コース詳細の構成

本カリキュラムガイドは、研修コースごとに、以下の構成になっています。

１）コースシラバス
- 研修コースコード
- 研修コース名
- 研修ロードマップ
- 機能・役割定義
- 知識項目（ＢＯＫ）分野
- 知識項目（ＢＯＫ）分類
- レベル区分
- 受講前提
- 科目概要
- 学習目標概要
- 研修・教育方法
- 修得スキルの評価方法
- カリキュラム構成
- 情報処理技術者試験
- 備考

２）知識項目対応表

３）コマタイトル一覧
- 回数
- テーマ
- 学習目標

４）コマシラバス
- 研修コース名
- 回数
- テーマ
- 学習目標
- 学習内容
- 研修・教育方法
- 時間の目安
- 対応する機能・役割定義
- その他

２．研修コース一覧

なお、研修コース一覧(表５)に記載されている研修コースをシラバスとして策定しています。

（表５）研修コース一覧

レベル	番号	研修コース名	コマ数	ページ
テクノロジ系				
初級講座	T01	セキュリティ技術初級	90 分×4	P.14
中級講座	T02	セキュリティ技術中級	90 分×8	P.22
上級講座	T03	セキュリティ技術上級	180 分×6	P.34
マネジメント系				
初級講座	M01	セキュリティ管理初級	90 分×4	P.44
中級講座	M02	セキュリティ管理中級	90 分×8	P.52
上級講座	M03	セキュリティ管理上級	180 分×6	P.64
ストラテジ系				
初級講座	S01	情報セキュリティポリシ	90 分×4	P.74
中級講座	S02	セキュリティガイドライン	90 分×8	P.82
上級講座	S03	セキュリティガイドライン上級	180 分×6	P.94

1.（T01）セキュリティ技術初級

対応する機能役割定義

大項目		中項目	
大No.	大項目名（タスク）	No.	中項目名
73	IS 導入/ システムコンポーネントの分析・設計	1	システムコンポーネントの要件定義
		2	システムコンポーネントの設計
		3	アプリ分析・設計・開発への助言
74	IS 導入/ システムコンポーネントの開発	1	システムコンポーネントの構築
		2	システムコンポーネントのテスト
76	IS 導入/ IS の受入	1	システムテスト/システム化要件テスト
		2	ユーザー受入テスト
110	IS 運用	7	セキュリティ管理
140	セキュリティ	1	セキュリティ方針の策定
		4	セキュリティの見直し

1.1. 科目シラバス

研修コースコード	14－T－01
研修コース名	セキュリティ技術初級
研修ロードマップ	(14)セキュリティ
知識項目(BOK)分野	テクノロジ系　－　テクノロジ
知識項目(BOK)分類	【大分類】4. 技術要素 【中分類】11. セキュリティ
レベル区分	セキュリティのレベル 2 を目指す者
受講前提	セキュリティに関してレベル 1 程度以上のもの
科目概要	・ 情報セキュリティについて、上司の指導の下、脆弱性や脅威を分析・評価し、それらのリスクを回避・防止するため対象に求めるべきセキュリティ要件の定義、実装の計画から設計、構築、移行、運用、維持管理までを推進または支援する能力の修得を目的とする。 ・ 全ての情報資産に対する必要なセキュリティの企画・導入・運用を含む業務全般の実施できる技術的知識の修得を目的とする。
学習目標概要	・ セキュリティ要件を定義する知識を理解できる。 ・ セキュリティ実装の計画から設計、構築、移行、運用するための知識を理解できる。 ・ セキュリティの観点から情報システム基盤の維持管理するための知識を理解できる。 ・ ネットワークセキュリティ、データベースセキュリティ、アプリケーションセキュリティに関する知識を理解できる。
研修・教育方法	ワークショップ(演習課題を含む)
修得スキルの評価方法	以下の状況等を総合的に判断して評価する。 受講前・受講後の知識確認テスト 定量アンケート 受講レポート 演習課題の取り組み状況　など
カリキュラム構成	1 コマ 90 分　×　4 コマ （クラスルーム：標準日数 1 日）
情報処理技術者試験	基本情報技術者試験・セキュリティの一部
備考	

1.2. 知識項目対応表

◎＝主項目として扱う、○＝関連項目として扱う

共通キャリア・スキルフレームワーク					対象項目
分野	大分類		中分類		
テクノロジ系	1	基礎理論	1	基礎理論	
			2	アルゴリズムとプログラミング	
	2	コンピュータシステム	3	コンピュータ構成要素	
			4	システム構成要素	
			5	ソフトウェア	
			6	ハードウェア	
	3	技術要素	7	ヒューマンインターフェース	
			8	マルチメディア	
			9	データベース	
			10	ネットワーク	
			11	セキュリティ	◎
	4	開発技術	12	システム開発技術	
			13	ソフトウェア開発技術管理	
マネジメント系	5	プロジェクトマネジメント	14	プロジェクトマネジメント	
	6	サービスマネジメント	15	サービスマネジメント	
			16	システム監査	
ストラテジ系	7	システム戦略	17	システム戦略	
			18	システム企画	
	8	経営戦略	19	経営戦略マネジメント	
			20	技術戦略マネジメント	
			21	ビジネスインダストリ	
	9	企業と法務	22	企業活動	
			23	法務	

1.3. コマタイトル一覧

回数	テーマ	学習目標	参照先
第１回	暗号化技術と公開鍵基盤	・ セキュリティ技術の対象となる情報資産に対する物理的脅威、技術的脅威、人的脅威、脆弱性などを理解した上で、暗号化の種類や代表的な暗号方式の仕組み、およびその特徴を理解する。 ・ 公開鍵証明書や認証局など公開鍵基盤の仕組み、特徴、活用場面を理解する。	Ｐ．18
第２回	認証技術と セキュリティ技術の評価	・ 認証技術や利用者確認のために利用される技術の仕組み、特徴、どのような脅威を防止するためにどの技術を理解する。 ・ 情報資産の不正コピーや改ざんなどを防ぐ情報セキュリティ製品について、そのセキュリティ水準を知るためのセキュリティ技術評価の目的や考え方を理解する。	Ｐ．19
第３回	ネットワークの セキュリティ	・ ネットワークに対する不正アクセス、不正利用、サービスの妨害行為などの脅威について理解する。 ・ ネットワークセキュリティに対する対策の仕組み、実装方法、効果などを理解する。	Ｐ．20
第４回	データベースおよび アプリケーションの セキュリティ	・ データベースに対する不正アクセス、不正利用、破壊などの脅威に対する対策の仕組み、実装方法、効果などを理解する。 ・ Web アプリケーションに対する攻撃を抑制するアプリケーションセキュリティの対策の仕組み、実装方法、効果などを理解する。	Ｐ．21

1.4. コマシラバス（1/4）

研修コース名	セキュリティ技術初級
回数	第 1 回
テーマ	暗号化技術と公開鍵基盤
学習目標	・ セキュリティ技術の対象となる情報資産に対する物理的脅威、技術的脅威、人的脅威、脆弱性などを理解した上で、暗号化の種類や代表的な暗号方式の仕組み、およびその特徴を理解する。 ・ 公開鍵証明書や認証局など公開鍵基盤の仕組み、特徴、活用場面を理解する。
学習内容	(1) 脅威 事故、災害、故障、盗難、エラー、コンピュータ犯罪 情報漏えい、不正アクセス、不正侵入、盗聴、なりすまし 改ざん，DoS（Denial of Service：サービスの妨害）攻撃 ウイルス、ワーム、ソーシャルエンジニアリング　など (2) 暗号化技術 公開鍵暗号化方式 共通鍵暗号化方式 DES RSA　など (3) 公開鍵基盤(PKI) 公開鍵証明書 CA GPKI BCA SSL　など
研修・教育方法	講義(ミニ演習課題を含む)
時間の目安	90 分（演習課題を含む） （講義：80 分　　演習課題：10 分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】3. セキュリティの分析
その他	

1.4. コマシラバス（2/4）

研修コース名	セキュリティ技術初級
回数	第２回
テーマ	情報セキュリティ対策と技術情報
学習目標	・ 認証技術や利用者確認のために利用される技術の仕組み、特徴、どのような脅威を防止するためにどの技術を理解する。 ・ 情報資産の不正コピーや改ざんなどを防ぐ情報セキュリティ製品について、そのセキュリティ水準を知るためのセキュリティ技術評価の目的や考え方を理解する。
学習内容	(1) 認証技術 ディジタル署名 メッセージ認証 時刻認証 生体認証技術（指紋、静脈パターン、虹彩、顔） など (2) 利用者確認 ログイン コールバック IC カード PIN コード、 ワンタイムパスワード など (3) セキュリティ評価基準 評価方法 セキュリティ機能要件 セキュリティ保証要件 保証レベル ISO/IEC 15408 など
研修・教育方法	講義(ミニ演習課題を含む)
時間の目安	90 分（演習課題を含む） （講義：80 分　　演習課題：10 分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】3. セキュリティの分析
その他	

1.4. コマシラバス（3/4）

研修コース名	セキュリティ技術初級
回数	第3回
テーマ	セキュリティ事故の初動処理
学習目標	・ ネットワークに対する不正アクセス、不正利用、サービスの妨害行為などの脅威について理解する。 ・ ネットワークセキュリティに対する対策の仕組み、実装方法、効果などを理解する。
学習内容	(1) ネットワークセキュリティ ファイアウォール，パケットフィルタリング IDS（Intrusion Detection System：侵入検知システム） IPS（Intrusion Protection System：侵入防止システム） 認証サーバ NAT（Network Address Translation：ネットワークアドレス変換)， IP マスカレード VPN（Virtual Private Network：仮想私設網） WEP（Wired Equivalent Privacy） WPA（Wi-Fi Protected Access）など
研修・教育方法	講義(ミニ演習課題を含む)
時間の目安	90 分（演習課題を含む） （講義：80　演習課題：10 分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】3. セキュリティの分析
その他	

1.4. コマシラバス（4/4）

研修コース名	セキュリティ技術初級
回数	第4回
テーマ	データベースおよびアプリケーションのセキュリティ
学習目標	・ データベースに対する不正アクセス、不正利用、破壊などの脅威に対する対策の仕組み、実装方法、効果などを理解する。 ・ Web アプリケーションに対する攻撃を抑制するアプリケーションセキュリティの対策の仕組み、実装方法、効果などを理解する。
学習内容	(1) データベースのセキュリティ 不正利用 不正アクセス 破壊 暗号化 利用者認証 データベースアクセス制御 ログの取得 アカウント管理 パスワード管理 外部媒体の利用制御 不正アクセス検知 (2) Web アプリケーションのセキュリティ Web システムのセキュリティ対策 セキュアプログラミング バッファオーバフロー攻撃 クロスサイトスクリプティング攻撃　など
研修・教育方法	講義(ミニ演習課題を含む)
時間の目安	90 分（演習課題を含む） （講義：80　演習課題：10 分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】4. セキュリティの見直し
その他	

2. （T02）セキュリティ技術中級

対応する機能役割定義

大項目		中項目	
大No.	大項目名（タスク）	No.	中項目名
73	IS 導入/ システムコンポーネントの分析・設計	1	システムコンポーネントの要件定義
		2	システムコンポーネントの設計
		3	アプリ分析・設計・開発への助言
74	IS 導入/ システムコンポーネントの開発	1	システムコンポーネントの構築
		2	システムコンポーネントのテスト
76	IS 導入/ IS の受入	1	システムテスト/システム化要件テスト
		2	ユーザー受入テスト
140	セキュリティ	1	セキュリティ方針の策定
		4	セキュリティの見直し

2.1. 科目シラバス

研修コースコード	14－T－02
研修コース名	セキュリティ技術中級
研修ロードマップ	(14)セキュリティ
知識項目(BOK)分野	テクノロジ系　－　テクノロジ
知識項目(BOK)分類	【大分類】4. 技術要素 【中分類】11. セキュリティ
レベル区分	セキュリティのレベル 3 を目指す者
受講前提	セキュリティに関してレベル 2 程度以上のもの
科目概要	・ 「セキュリティ技術初級」の後続コースとして、情報セキュリティに関する脆弱性や脅威を分析・評価し、それらのリスクを回避・防止するため対象に求めるべきセキュリティ要件の定義、実装の計画から設計、構築、移行、運用、維持管理までを推進または支援する応用的能力の修得を目的とする。 ・ 全ての情報資産に対する必要なセキュリティの企画・導入・運用を含む業務全般の実施や指導・管理などを応用できる技術的知識の修得を目的とする。
学習目標概要	・ セキュリティ要件を定義する知識を修得し、応用できる。 ・ セキュリティ実装の計画から設計、構築、移行、運用、維持管理までを推進または支援する応用的能力の修得し、応用できる。 ・ セキュア OS、セキュアプログラミング、データベースセキュリティ、ネットワークセキュリティ、アプリケーションセキュリティに関する知識を修得し、応用できる。
研修・教育方法	ワークショップ(演習課題を含む)
修得スキルの評価方法	以下の状況等を総合的に判断して評価する。 受講前・受講後の知識確認テスト 定量アンケート 受講レポート 演習課題の取り組み状況　など
カリキュラム構成	1 コマ 90 分　×　8 コマ （クラスルーム：標準日数 2 日）
情報処理技術者試験	応用情報処理技術者試験・セキュリティ領域の一部
備考	

2.2. 知識項目対応表

◎＝主項目として扱う、○＝関連項目として扱う

共通キャリア・スキルフレームワーク					対象項目
分野	大分類		中分類		
テクノロジ系	1	基礎理論	1	基礎理論	
			2	アルゴリズムとプログラミング	
	2	コンピュータシステム	3	コンピュータ構成要素	
			4	システム構成要素	
			5	ソフトウェア	
			6	ハードウェア	
	3	技術要素	7	ヒューマンインターフェース	
			8	マルチメディア	
			9	データベース	
			10	ネットワーク	
			11	セキュリティ	◎
	4	開発技術	12	システム開発技術	
			13	ソフトウェア開発技術管理	
マネジメント系	5	プロジェクトマネジメント	14	プロジェクトマネジメント	
	6	サービスマネジメント	15	サービスマネジメント	
			16	システム監査	
ストラテジ系	7	システム戦略	17	システム戦略	
			18	システム企画	
	8	経営戦略	19	経営戦略マネジメント	
			20	技術戦略マネジメント	
			21	ビジネスインダストリ	
	9	企業と法務	22	企業活動	
			23	法務	

2.3. コマタイトル一覧

回数	テーマ	学習目標	参照先
第１回	脅威と脆弱性	・ セキュリティ技術の対象となる情報資産に対する物理的脅威、技術的脅威、人的脅威、脆弱性などを理解しこれらの知識をセキュリティ対策に応用する。	P．26
第２回	暗号化技術と公開鍵基盤	・ 暗号化の種類や代表的な暗号方式の仕組み、およびその特徴、公開鍵証明書や認証局など公開鍵基盤の仕組み、特徴、活用場面を理解し、応用する。	P．27
第３回	認証技術	・ 認証技術や利用者確認のために利用される技術の仕組み、特徴、どのような脅威を防止するためにどの技術が用いられるかの知識を修得し、応用する。	P．28
第４回	セキュリティ技術の評価	・ 情報資産の不正コピーや改ざんなどを防ぐ情報セキュリティ製品について、そのセキュリティ水準を知るためのセキュリティ技術評価の目的や考え方、適用方法を理解する。	P．29
第５回	セキュア OS とセキュアプログラミング	・ システムの開発、運用におけるセキュアプログラミングやセキュリティを強化した OS であるセキュア OS の仕組み、実装技術、効果などの知識を修得し、応用する。	P．30
第６回	ネットワークセキュリティ	・ ネットワークに対する不正アクセス、不正利用、サービスの妨害行為などの脅威に対する対策の仕組み、実装方法、効果などの知識を修得し、応用する。	P．31
第７回	データベースセキュリティ	・ データベースに対する不正アクセス、不正利用、破壊などの脅威に対する対策の仕組み、実装方法、効果などの知識を修得し、応用する。	P．32
第８回	Web アプリケーションセキュリティ	・ Web アプリケーションに対する攻撃を抑制するアプリケーションセキュリティの対策の仕組み、実装方法、効果などの知識を修得し、応用する。	P．33

2.4. コマシラバス（1/8）

研修コース名	セキュリティ技術中級
回数	第 1 回
テーマ	脅威と脆弱性
学習目標	・ セキュリティ技術の対象となる情報資産に対する物理的脅威、技術的脅威、人的脅威、脆弱性などを理解しこれらの知識をセキュリティ対策に応用する。
学習内容	(1) 脅威 事故災害 故障 盗難 エラー コンピュータ犯罪 情報漏えい 不正アクセス 不正侵入 盗聴 なりすまし 改ざん DoS 攻撃 ウイルス ワーム ソーシャルエンジニアリング　など (2) 脆弱性 バグ セキュリティホール 人為的脆弱性　など
研修・教育方法	講義(ミニ演習課題を含む)
時間の目安	90 分（演習課題を含む） （講義：80 分　演習課題：10 分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】
その他	

2.4. コマシラバス（2/8）

研修コース名	セキュリティ技術中級
回数	第２回
テーマ	暗号化技術と公開鍵基盤
学習目標	・ 暗号化の種類や代表的な暗号方式の仕組みおよびその特徴、公開鍵証明書や認証局など公開鍵基盤の仕組み、特徴、活用場面を理解し、応用する。
学習内容	(1) 暗号化技術 公開鍵暗号化方式 通鍵暗号化方式 公開鍵 秘密鍵 DES RSA 楕円暗号方式 S/MIME PGP など (2) 公開鍵基盤(PKI) 公開鍵証明書 CA GPKI BCA SSL SET など
研修・教育方法	講義(ミニ演習課題を含む)
時間の目安	90 分（演習課題を含む） （講義：80 分　　演習課題：10 分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】3. セキュリティの分析
その他	

2.4. コマシラバス（3/8）

研修コース名	セキュリティ技術中級
回数	第3回
テーマ	認証技術
学習目標	・ 認証技術や利用者確認のために利用される技術の仕組み、特徴、どのような脅威を防止するためにどの技術が用いられるかの知識を修得し、応用する。
学習内容	(1) 認証技術 ディジタル認証、ディジタル署名、メッセージ認証 時刻認証、チャレンジレスポンス認証　など (2) 利用者確認 ログイン、コールバック、アクセス管理、IC カード PIN コード、Kerberos 方式、ワンタイムパスワード シングルサインオン　など (3) 生体認証技術 指紋認証、静脈パターン認証、虹彩認証 声紋認証、顔認証、網膜認証、 本人拒否率、他人受入率　など
研修・教育方法	講義(ミニ演習課題を含む)
時間の目安	90 分（演習課題を含む） （講義：80 分　演習課題：10 分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】3. セキュリティの分析
その他	

2.4. コマシラバス（4/8）

研修コース名	セキュリティ技術中級
回数	第４回
テーマ	情報セキュリティ対策
学習目標	・ 情報資産の不正コピーや改ざんなどを防ぐ情報セキュリティ製品について、そのセキュリティ水準を知るためのセキュリティ技術評価の目的や考え方、適用方法を理解し、応用する。
学習内容	(1) セキュリティ評価基準 評価方法 セキュリティ機能要件 セキュリティ保証要件 保証レベル　など (2) ISO/IEC 15408 CC（Common Criteria：コモンクライテリア） ST（Security Target：セキュリティターゲット） CEM （Common Methodology for Information Technology Security Evaluation） EAL（Evaluation Assurance Level：評価保証レベル） など
研修・教育方法	講義(ミニ演習課題を含む)
時間の目安	90 分（演習課題を含む） （講義：80 分　　演習課題：10 分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】3. セキュリティの分析
その他	

2.4. コマシラバス（5/8）

研修コース名	セキュリティ技術中級
回数	第5回
テーマ	セキュア OS とセキュアプログラミング
学習目標	・ セキュリティを強化した OS であるセキュア OS の仕組み、実装技術、効果などの知識を修得し、応用する。 ・ システムの開発、運用におけるセキュアプログラミングに関する知識を修得し、応用する。
学習内容	(1) セキュア OS MAC 最小権限 トランスデッド OS など (2) セキュアプログラミング プログラム言語 ウェブアプリケーション開発 ソフトウェア脆弱性対策技術 など
研修・教育方法	講義(ミニ演習課題を含む)
時間の目安	90 分（演習課題を含む） （講義：80 分 演習課題：10 分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】3. セキュリティの分析
その他	

2.4. コマシラバス（6/8）

研修コース名	セキュリティ技術中級
回数	第 6 回
テーマ	ネットワークセキュリティ
学習目標	・ ネットワークに対する不正アクセス、不正利用、サービスの妨害行為などの脅威に対する対策の仕組み、実装方法、果などの知識を修得し、応用する。
学習内容	(1)　ネットワークセキュリティ 関門ルータ ファイアウォール パケットフィルタリング アプリケーションゲートウェイ方式 IDS IPS 認証サーバ NAT IP マスカレード VPN セキュリティ監視 SSID WEP WPA MAC アドレス フィルタリング ハニーポット　など
研修・教育方法	講義(ミニ演習課題を含む)
時間の目安	90 分（演習課題を含む） （講義：80 分　演習課題：10 分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】4. セキュリティの見直し
その他	

2.4. コマシラバス（7/8）

研修コース名	セキュリティ技術中級
回数	第 7 回
テーマ	データベースセキュリティ
学習目標	・ データベースに対する不正アクセス、不正利用、破壊などの脅威に対する対策の仕組み、実装方法、効果などの知識を修得し、応用する。
学習内容	(1) データベースセキュリティ 暗号化 利用者認証 データベースアクセス制御 データベースバックアップ ログの取得 アカウント管理 パスワード管理 外部媒体の利用制御 不正アクセス検知 SQL インジェクション　など
研修・教育方法	講義(ミニ演習課題を含む)
時間の目安	90 分（演習課題を含む） （講義：80 分　演習課題：10 分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】3. セキュリティの分析
その他	

2.4. コマシラバス（8/8）

研修コース名	セキュリティ技術中級
回数	第８回
テーマ	Web アプリケーションセキュリティ
学習目標	・ Web アプリケーションに対する攻撃を抑制するアプリケーションセキュリティの対策の仕組み、実装方法、効果などの知識を修得し、応用する。
学習内容	(1) Web アプリケーションセキュリティ Web システムのセキュリティ対策 セキュアプログラミング バッファオーバーフロー攻撃 クロスサイトスクリプティング攻撃 SQL インジェクション攻撃 スパム対策 ウイルス対策　など
研修・教育方法	講義(ミニ演習課題を含む)
時間の目安	90 分（演習課題を含む） （講義：80 分　演習課題：10 分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】4. セキュリティの見直し
その他	

3. （T03）セキュリティ技術上級

対応する機能役割定義

大項目		中項目	
大No.	大項目名（タスク）	No.	中項目名
30	IT 基盤構築・維持・管理	1	IT 戦略の策定
		4	IT 基盤整備（標準作成）
140	セキュリティ	1	セキュリティ方針の策定
		2	セキュリティ基準の策定
		3	セキュリティの分析
		4	セキュリティの見直し

3.1. 科目シラバス

研修コースコード	14－T－03
研修コース名	セキュリティ技術上級
研修ロードマップ	(14)セキュリティ
知識項目(BOK)分野	テクノロジ系　－　テクノロジ
知識項目(BOK)分類	【大分類】4. 技術要素 【中分類】11. セキュリティ
レベル区分	セキュリティのレベル 4 を目指す者
受講前提	セキュリティに関してレベル 3 程度以上のもの
科目概要	・ 「セキュリティ技術中級」の後続コースとして、情報システム基盤の構築・運用において、情報セキュリティに関する脆弱性や脅威を分析・評価し、それらのリスクを回避・防止するための対象（情報システム基盤、情報システム、セキュリティ機能等）に求めるべきセキュリティ要件の定義、実装の計画から、設計、構築、移行、運用、維持管理までを推進又は支援できる知識を修得する。
学習目標概要	・ セキュリティ要件が実現するセキュリティ対策の目標と範囲など、セキュリティ要求仕様として提示することができる。 ・ セキュリティ要件を実現するアーキテクチャとして、ハードウェア、ネットワーク、ソフトウェアのそれぞれに対し、実施するセキュリティ機能の実装方式を設計し、実装することができる。 ・ 個別の情報システムまたはセキュリティ機能の開発プロジェトもしくはセキュアな開発プロジェクト環境の整備を含むプロジェクト管理を技術的側面から支援することができる。
研修・教育方法	ワークショップ(演習課題を含む)
修得スキルの評価方法	以下の状況等を総合的に判断して評価する。 受講前・受講後の知識確認テスト 定量アンケート 受講レポート 演習課題の取り組み状況　など
カリキュラム構成	1 コマ 180 分　×　6 コマ （クラスルーム：標準日数 3 日）
情報処理技術者試験	情報セキュリティスペシャリスト試験の一部
備考	

3.2. 知識項目対応表

◎＝主項目として扱う、○＝関連項目として扱う

共通キャリア・スキルフレームワーク					対象項目
分野	大分類		中分類		
テクノロジ系	1	基礎理論	1	基礎理論	
			2	アルゴリズムとプログラミング	
	2	コンピュータシステム	3	コンピュータ構成要素	
			4	システム構成要素	
			5	ソフトウェア	
			6	ハードウェア	
	3	技術要素	7	ヒューマンインターフェース	
			8	マルチメディア	
			9	データベース	
			10	ネットワーク	
			11	セキュリティ	◎
	4	開発技術	12	システム開発技術	
			13	ソフトウェア開発技術管理	
マネジメント系	5	プロジェクトマネジメント	14	プロジェクトマネジメント	
	6	サービスマネジメント	15	サービスマネジメント	
			16	システム監査	
ストラテジ系	7	システム戦略	17	システム戦略	
			18	システム企画	
	8	経営戦略	19	経営戦略マネジメント	
			20	技術戦略マネジメント	
			21	ビジネスインダストリ	
	9	企業と法務	22	企業活動	
			23	法務	

3.3. コマタイトル一覧

回数	テーマ	学習目標	参照先
第１回	情報システムの 脆弱性・脅威分析	・ 情報資産の価値をセキュリティの観点から明確にすることができる。 ・ 特定したリスクについて、リスクが発現する確率およびリスクが発現した場合の影響の大きさを定量的または定性的に把握することでリスクの値を算定することができる。	P．38
第２回	セキュリティ要件定義	・ 優先度の高いリスクへの対応を中心に、開発対象システムの問題点を定義できる。 ・ 要求事項から、開発対象システムにおけるセキュリティ要件を決定することができる。 ・ セキュリティ要件が実現するセキュリティ対策の目標と範囲などを定義できる。	P．39
第３回	セキュリティ機能 の設計	・ セキュリティ要件を実現するアーキテクチャとして、ハードウェア、ネットワーク、ソフトウェアのそれぞれに対し、実施するセキュリティ機能の実装方式の定義できる。 ・ 必要な実装の設計を行うことができる。	P．40
第４回	セキュリティ実装技術 (セキュアプログラミング)	・ ソフトウェアに対し、セキュリティ要件定義上必要な実装を行うことができる。 ・ セキュアプログラミングに関する知識（プログラム言語、ウェブアプリケーション開発、ソフトウェア脆弱性対策技術など）の手法を用いることができる。	P．41
第５回	セキュリティ実装技術 （ネットワーク）	・ ネットワークに対し、セキュリティ要件定義上必要な実装を行うことができる。 ・ ネットワーク実装においては、ファイアウォール、侵入検知システム、認証 VLAN、検疫ネットワークなどのセキュリティ対策装置の採用を検討することができる。	P．42
第６回	セキュリティ機能の 本番移行	・ 企業の情報セキュリティポリシに準拠した、開発対象システムの導入計画の作成および導入、受け入れを支援することができる。 ・ 利用者側に対するサポートの範囲を決定し、利用者に対する教育訓練の計画と実施を管理することができる。	P．43

3.4. コマシラバス（1/6）

研修コース名	セキュリティ技術上級
回数	第1回
テーマ	情報システムの脆弱性・脅威分析
学習目標	・ 情報資産の価値をセキュリティの観点から明確にすることができる。 ・ 特定したリスクについて、リスクが発現する確率およびリスクが発現した場合の影響の大きさを定量的または定性的に把握することでリスクの値を算定することができる。
学習内容	――講義―― (1) 情報資産の評価 情報資産の識別方法、情報資産の評価方法　など (2) リスクの特定 脅威の分析、脆弱性の分析、リスクの存在箇所、 リスクの発生時期、リスクの原因　など (3) リスクの算定 定量的リスク評価方法、定性的リスク評価方法 リスク対策のコスト、リスクの許容　など (4) リスクの評価 リスク基準、リスク対応の優先順位　など (5) リスク対策の選択 抑止、予防、検知、回復 最適化（低減）、回避、移転、保有 物理的、管理的、人的、技術的 ――ワークショップ―― ケースの (1) 情報資産の評価 (2) リスク評価とリスク対策の選択
研修・教育方法	ワークショップ（講義を含む・クラスルーム）
時間の目安	180分（演習課題を含む） （講義：60分　　演習課題：120分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】1. セキュリティ方針の策定
その他	ケースに使用するモデル企業は、文書または図解で提示し、第1回から第6回まで、通しで利用できるものが望ましい。

3.4. コマシラバス（2/6）

研修コース名	セキュリティ技術上級
回数	第２回
テーマ	セキュリティ要件定義
学習目標	・ 優先度の高いリスクへの対応を中心に、開発対象システムの問題点を定義できる。 ・ 要求事項から、開発対象システムにおけるセキュリティ要件を決定し、セキュリティアーキテクチャを設計することができる。 ・ セキュリティ要件が実現するセキュリティ対策の目標と範囲などを定義できる。
学習内容	――講義―― (1) セキュリティ要件定義のための情報収集・分析 アプリケーション調査・分析 ネットワークアーキテクチャ調査・分析 業務上の機能要求および性能要求 (2) セキュリティアーキテクチャの設計 システムアーキテクチャの選択 ハードウェア構成、ソフトウェア構成 ネットワーク構成、システム化範囲 アーキテクチャの候補、信頼性設計 物理的対策、人的対策、管理的対策、技術的対策 (3) セキュリティ要件の定義 運用上の要求、保守上の要求、システム移行時の要求 データベースへの要求、ネットワークへの要求　など ――ワークショップ―― ケースの (1) セキュリティアーキテクチャの検討 (2) セキュリティ要件の定義
研修・教育方法	ワークショップ（講義を含む・クラスルーム）
時間の目安	180 分（演習課題を含む） （講義：60 分　　演習課題：120 分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】1. セキュリティ方針の策定
その他	ケースに使用するモデル企業は、文書または図解で提示し、第１回から第６回まで、通しで利用できるものが望ましい。

3.4. コマシラバス（3/6）

研修コース名	セキュリティ技術上級
回数	第3回
テーマ	セキュリティ機能の設計
学習目標	・ セキュリティ要件を実現するアーキテクチャとして、ハードウェア、ネットワーク、ソフトウェアのそれぞれに対し、実施するセキュリティ機能の実装方式の定義できる。 ・ 必要な実装の設計を行うことができる。
学習内容	――講義―― (1). セキュリティ実装方式の決定と評価 詳細機能フロー システム方式の選択 ハードウェア構成 ソフトウェア構成 ネットワーク構成 (2) セキュリティ実装の設計 サブシステムの機能仕様とインタフェース設計 データモデルの設計 外部設計 ネットワークシステムの設計　など ――ワークショップ―― (1) セキュリティ実装方式の検討 (2) セキュリティ実装の設計
研修・教育方法	ワークショップ（講義を含む・クラスルーム）
時間の目安	180分（演習課題を含む） （講義：60分　　演習課題：120分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】1. セキュリティ方針の策定
その他	ケースに使用するモデル企業は、文書または図解で提示し、第1回から第6回まで、通しで利用できるものが望ましい。

3.4. コマシラバス（4/6）

研修コース名	セキュリティ技術上級
回数	第4回
テーマ	セキュリティ技術（セキュアプログラミング）
学習目標	・ ソフトウェアに対し、セキュリティ要件定義上必要な実装を行うことができる。 ・ ソフトウェア実装においては、セキュアプログラミングに関する知識（プログラム言語、ウェブアプリケーション開発、ソフトウェア脆弱性対策技術など）の手法を用いることができる。
学習内容	――講義―― (1) セキュリティ機能の実装 ソフトウェアコンポーネント設計 入出力設計 物理データ設計 部品化と再利用 内部設計 デザインレビュー プログラム設計 モジュール仕様 テスト仕様 プログラミング（C++、Java、Perl など） セキュアプログラミング ソフトウェア開発ツール システムテスト　など ――ワークショップ―― (1) 情報セキュリティ機能の実装 (2) セキュアプログラミング
研修・教育方法	ワークショップ（講義を含む・クラスルーム）
時間の目安	180 分（演習課題を含む） （講義：60 分　　演習課題：120 分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】1. セキュリティ方針の策定
その他	ケースに使用するモデル企業は、文書または図解で提示し、第 1 回から第 6 回まで、通しで利用できるものが望ましい。

3.4. コマシラバス（5/6）

研修コース名	セキュリティ技術上級
回数	第5回
テーマ	セキュリティの実装（ネットワーク）
学習目標	・ ネットワークに対し、セキュリティ要件定義上必要な実装を行うことができる。 ・ ネットワーク実装においては、ファイアウォール、侵入検知システム、認証 VLAN、検疫ネットワークなどのセキュリティ対策装置の採用を検討することができる。
学習内容	――講義―― (1)　ネットワークのセキュリティ実装 プロトコルの決定 トポロジの決定 ネットワーク機器の選定 ファイアウォール 侵入検知システム 認証 VLAN 検疫ネットワーク　など ――ワークショップ―― (1)　ネットワークセキュリティ実装
研修・教育方法	ワークショップ（講義を含む・クラスルーム）
時間の目安	180 分（演習課題を含む） （講義：60 分　　演習課題：120 分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】2. セキュリティ基準の策定
その他	ケースに使用するモデル企業は、文書または図解で提示し、第 1 回から第 6 回まで、通しで利用できるものが望ましい。

3.4. コマシラバス（6/6）

研修コース名	セキュリティ技術上級
回数	第 6 回
テーマ	セキュリティ機能の本番移行
学習目標	・ 企業の情報セキュリティポリシに準拠した、開発対象システムの導入計画の作成および導入、受け入れを支援することができる。 ・ 利用者側に対するサポートの範囲を決定し、具体的なメニューを提示し、利用者に対する教育訓練の計画と実施を管理することができる。
学習内容	――講義―― (1)　開発対象システムの本番移行 事前の段取り、立会い、媒体の安全な移送 (2)　開発対象システムの受け入れ検査支援 システムテスト、システム化要件テスト 受け入れレビュー、受け入れ検査 (3)　運用担当者の教育・訓練及び支援 教育計画の立案、ヘルプデスク (4)　システム利用者対応 利用者セキュリティ管理 利用者教育、利用者からの相談 ――ワークショップ―― (1)　運用担当者の教育計画
研修・教育方法	ワークショップ（講義を含む・クラスルーム）
時間の目安	180 分（演習課題を含む） （講義：60 分　　演習課題：120 分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】2. セキュリティ基準の策定
その他	ケースに使用するモデル企業は、文書または図解で提示し、第 1 回から第 6 回まで、通しで利用できるものが望ましい。

4.（M01）セキュリティ管理初級

対応する機能役割定義

大項目		中項目	
大No.	大項目名（タスク）	No.	中項目名
100	IS 保守	1	保守計画
		2	保守の実施
		4	リリース管理
		7	セキュリティ管理
140	セキュリティ	1	セキュリティ方針の策定
		3	セキュリティの分析
		4	セキュリティの見直し

4.1. 科目シラバス

研修コースコード	14－M－01
研修コース名	セキュリティ管理初級
研修ロードマップ	(14)セキュリティ
知識項目(BOK)分野	テクノロジ系　－　マネジメント
知識項目(BOK)分類	【大分類】4. 技術要素 【中分類】11. セキュリティ
レベル区分	セキュリティのレベル 2 を目指す者
受講前提	セキュリティに関してレベル 1 程度以上のもの
科目概要	・ 情報セキュリティについて、上司の指導の下、企画・導入・運用を含む業務全般の管理ができる知識の修得を目的とする。 ・ 情報システムを開発する上で必要な情報セキュリティに関する技術を理解し､セキュリティの分析やセキュリティ対策の見直し知識を学習する。
学習目標概要	・ 情報システムを開発する上で必要な情報セキュリティに関する技術を理解し、担当業務に適用できる。 ・ 人的､技術的､物理的なセキュリティの側面から情報セキュリティ対策を検討し、担当する事項に適用できる。 ・ セキュリティ事故や事件などを通じてセキュリティを分析する手順を理解し、担当業務に適用できる。 ・ 新たなリスクの整理と分析を行い､情報セキュリティ対策の見直しを理解し、担当業務に適用できる
研修・教育方法	ワークショップ(演習課題を含む)
修得スキルの評価方法	以下の状況等を総合的に判断して評価する。 受講前・受講後の知識確認テスト 定量アンケート 受講レポート 演習課題の取り組み状況　など
カリキュラム構成	1 コマ 90 分　×　4 コマ （クラスルーム：標準日数 1 日）
情報処理技術者試験	基本情報技術者試験・セキュリティの一部
備考	（次のＢＯＫも対応） 【大分類】9. 企業と法務 【中分類】23. 法務

4.2. 知識項目対応表

◎＝主項目として扱う、○＝関連項目として扱う

共通キャリア・スキルフレームワーク					対象項目
分野	大分類		中分類		
テクノロジ系	1	基礎理論	1	基礎理論	
			2	アルゴリズムとプログラミング	
	2	コンピュータシステム	3	コンピュータ構成要素	
			4	システム構成要素	
			5	ソフトウェア	
			6	ハードウェア	
	3	技術要素	7	ヒューマンインターフェース	
			8	マルチメディア	
			9	データベース	
			10	ネットワーク	
			11	セキュリティ	◎
	4	開発技術	12	システム開発技術	
			13	ソフトウェア開発技術管理	
マネジメント系	5	プロジェクトマネジメント	14	プロジェクトマネジメント	
	6	サービスマネジメント	15	サービスマネジメント	
			16	システム監査	
ストラテジ系	7	システム戦略	17	システム戦略	
			18	システム企画	
	8	経営戦略	19	経営戦略マネジメント	
			20	技術戦略マネジメント	
			21	ビジネスインダストリ	
	9	企業と法務	22	企業活動	
			23	法務	○

4.3. コマタイトル一覧

回数	テーマ	学習目標	参照先
第１回	セキュリティ技術	・ 情報セキュリティ管理に必要な情報セキュリティ技術の基本的な考え方を理解する。 ・ セキュリティ管理の立場から、ネットワークやデータベースに実装するセキュリティ対策のあらましを理解する。	P．48
第２回	情報セキュリティ対策と技術情報	・ セキュリティ管理の立場から、人的、技術的、物理的セキュリティの側面から、情報セキュリティ技術を理解する。 ・ 最新のセキュリティ技術情報を収集し、社内システムの適用評価を理解する。 ・ セキュリティ管理の立場から、セキュリティ技術評価の基本的な考え方を理解する。	P．49
第３回	セキュリティの分析	・ 侵入検査を継続的に実施し、セキュリティポリシの遵守状況を評価することを理解する。 ・ 事故発生時における被害拡大防止、証拠保存、および事故原因の特定や再発防止策を検討・実施とシステムを復旧する知識を理解する。 ・ 事故などのセキュリティ評価情報を、セキュリティの見直しに利用することを理解する。	P．50
第４回	セキュリティの見直し	・ セキュリティ管理の立場から、運用上や技術上の問題から影響を受けるセキュリティを特定し、セキュリティ対策の更新体制を整備し、セキュリティ対策を更新することを理解する。 ・ 継続的にセキュリティ対策の見直しを行う必要性を理解する。	P．51

4.4. コマシラバス（1/4）

研修コース名	セキュリティ管理初級
回数	第 1 回
テーマ	セキュリティ技術
学習目標	・ 情報セキュリティ管理に必要な情報セキュリティ技術の基本的な考え方を理解する。 ・ セキュリティ管理の立場から、ネットワーク、データベースに実装するセキュリティ対策のあらましを理解する。
学習内容	(1) 暗号化技術 公開鍵暗号化方式、共通鍵暗号化方式、DES、RSA　など (2) 認証技術 ディジタル署名、メッセージ認証、時刻認証　など (3) 利用者確認 ログイン、コールバック、IC カード、PIN コード、 ワンタイムパスワード　など (4) 生体認証技術 指紋、静脈パターン、虹彩、認証、顔　など (5) 公開鍵基盤(PKI) 公開鍵証明書、CA、GPKI、BCA、SSL　など (6) ネットワークセキュリティ ファイアウォール、パケットフィルタリング、IDS、IPS 認証サーバ、NAT、IP マスカレー、VPN、WEP、WPA (7) データベースセキュリティ 暗号化、利用者認証、データベースアクセス制御 ログの取得、アカウント管理、パスワード管理、 外部媒体の利用制御、不正アクセス検知、など
研修・教育方法	講義(ミニ演習課題を含む)
時間の目安	90 分（演習課題を含む） （講義：80 分　　演習課題：10 分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】3. セキュリティの分析
その他	

4.4. コマシラバス（2/4）

研修コース名	セキュリティ管理初級
回数	第２回
テーマ	情報セキュリティ対策と技術情報
学習目標	・ セキュリティ管理の立場から、人的、技術的、物理的セキュリティの側面から、情報セキュリティ技術を理解する。 ・ 最新のセキュリティ技術情報を収集し、社内システムの適用評価を理解する。 ・ セキュリティ管理の立場から、セキュリティ技術評価の基本的な考え方を理解する。
学習内容	(1) 人的セキュリティ対策 情報セキュリティポリシ、社内規定、 情報セキュリティ教育、パスワード管理、など (2) 技術的セキュリティ対策 クラッキング対策、暗号処理、ファイアウォール コンピュータウイルス対策、OS アップデート ネットワーク監視、アクセス制御、侵入検知、など (3) 物理的セキュリティ対策 RASIS、施錠管理、入退室管理 RAS 技術、耐震耐火設備、監視カメラ、 など (4) セキュリティ技術評価 評価方法、セキュリティ機能要件、 セキュリティ保証要件、保障レベル ISO/IEC 15408
研修・教育方法	講義(ミニ演習課題を含む)
時間の目安	90 分（演習課題を含む） （講義：80 分　　演習課題：10 分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】3. セキュリティの分析
その他	

4.4. コマシラバス（3/4）

研修コース名	セキュリティ管理初級
回数	第3回
テーマ	セキュリティ事故の初動処理
学習目標	・ 侵入検査を継続的に実施し、セキュリティポリシの遵守状況を評価することを理解する。 ・ 事故発生時における被害拡大防止、証拠保存、および事故原因の特定や再発防止策を検討・実施とシステムを復旧する知識を理解する。 ・ 事故などのセキュリティ評価情報を、セキュリティの見直しに利用することを理解する
学習内容	(1) 事故の検知 ログの取得、不正侵入、セキュリティ違反　など (2) 初動処理 緊急時対応マニュアル 事故の連絡と説明、処置の優先順位、被害拡大の防止策 証拠保存のタイミング　など (3) 事故の分析 被害と影響の調査 操作記録 アクセス記録 事故原因の特定　など (4) 復旧処理 復旧処置 事故の記録　など (5) 再発防止 再発防止策の検討と実施 システム再構築　など
研修・教育方法	講義(ミニ演習課題を含む)
時間の目安	90分（演習課題を含む） （講義：80分　演習課題：10分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】3. セキュリティの分析
その他	

4.4. コマシラバス（4/4）

研修コース名	セキュリティ管理初級
回数	第４回
テーマ	セキュリティ対策の見直し
学習目標	・ セキュリティ管理の立場から、運用上や技術上の問題から影響を受けるセキュリティを特定し、セキュリティ対策の更新体制を整備し、セキュリティ対策を更新することを理解する。 ・ 継続的にセキュリティ対策の見直しを行う必要性を理解する。
学習内容	(1) 技術情報の収集と評価 セキュリティホール、パッチ (2) 運用上の問題点整理と分析 利用者アンケートとヒアリング情報 (3) 技術上の問題点整理と分析 問題点の分析 (4) 体制構築 セキュリティ対策更新体制 (5) 更新手続き 情報セキュリティ監査 (6) 継続的見直し
研修・教育方法	講義(ミニ演習課題を含む)
時間の目安	90 分（演習課題を含む） （講義：80 分　演習課題：10 分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】4. セキュリティの見直し
その他	

5.（M02）セキュリティ管理中級

対応する機能役割定義

大項目		中項目	
大No.	大項目名（タスク）	No.	中項目名
30	IT 基盤構築・維持・管理	5	品質統制フレームワークの運営
40	IS 戦略実行マネジメント	1	IS 戦略実現上のリスクへの対応
		2	コントロールフレームワークの維持・管理
100	IS 保守	1	保守計画
		2	保守の実施
110	IS 運用	4	リリース管理
		7	セキュリティ管理
140	セキュリティ	1	セキュリティ方針の策定
		2	セキュリティ基準の策定
		4	セキュリティの見直し

5.1. 科目シラバス

研修コースコード	14－M－02
研修コース名	セキュリティ管理中級
研修ロードマップ	(14)セキュリティ
知識項目(BOK)分野	テクノロジ系　－　マネジメント
知識項目(BOK)分類	【大分類】4. 技術要素 【中分類】11. セキュリティ
レベル区分	セキュリティのレベル 3 を目指す者
受講前提	セキュリティに関してレベル 2 程度以上のもの
科目概要	・ 「セキュリティ管理初級」の後続コースとして、全ての情報資産に必要なセキュリティの企画・導入・運用を含む業務全般の実施や指導・管理などを応用できる知識の修得を目的とする。 ・ セキュリティポリシを運用する観点から、セキュリティ管理システムを導入・構築し、運用管理や問題発生時の処置、さらにセキュリティポリシそのものを見直しなどに応用する。
学習目標概要	・ セキュリティ基本方針やセキュリティ対策基準等に従って、組織等に適切な運用の指導およびその状況を管理することができる。 ・ セキュリティ事故を検知した際、緊急対応の規定に従った適切な初動処理、その被害状況や範囲、事故原因等を特定し、再発防策を施して事故を復旧させることができる ・ 最新の脅威や事故の情報を収集し、新たなリスクの整理と分析を行って情報セキュリティポリシを見直すことができる。
研修・教育方法	ワークショップ(演習課題を含む)
修得スキルの評価方法	以下の状況等を総合的に判断して評価する。 受講前・受講後の知識確認テスト 定量アンケート 受講レポート 演習課題の取り組み状況　など
カリキュラム構成	1 コマ 90 分　×　8 コマ （クラスルーム：標準日数 2 日）
情報処理技術者試験	応用情報処理技術者試験・セキュリティ領域の一部
備考	（次のＢＯＫも対応） 【大分類】9. 企業と法務 【中分類】23. 法務

5.2. 知識項目対応表

◎＝主項目として扱う、○＝関連項目として扱う

共通キャリア・スキルフレームワーク					対象項目
分野	大分類		中分類		
テクノロジ系	1	基礎理論	1	基礎理論	
			2	アルゴリズムとプログラミング	
	2	コンピュータシステム	3	コンピュータ構成要素	
			4	システム構成要素	
			5	ソフトウェア	
			6	ハードウェア	
	3	技術要素	7	ヒューマンインターフェース	
			8	マルチメディア	
			9	データベース	
			10	ネットワーク	
			11	セキュリティ	◎
	4	開発技術	12	システム開発技術	
			13	ソフトウェア開発技術管理	
マネジメント系	5	プロジェクトマネジメント	14	プロジェクトマネジメント	
	6	サービスマネジメント	15	サービスマネジメント	
			16	システム監査	
ストラテジ系	7	システム戦略	17	システム戦略	
			18	システム企画	
	8	経営戦略	19	経営戦略マネジメント	
			20	技術戦略マネジメント	
			21	ビジネスインダストリ	
	9	企業と法務	22	企業活動	○
			23	法務	○

5.3. コマタイトル一覧

回数	テーマ	学習目標	参照先
第１回	情報セキュリティの技術	・ 情報セキュリティに関する技術の種類、仕組み、特徴などを理解し、この技術を使用してセキュリティ管理に応用する。	Ｐ．56
第２回	情報セキュリティ対策	・ 人的、技術的、物理的セキュリティの側面から、情報セキュリティ技術を理解し、セキュリティ管理に応用する。	Ｐ．57
第３回	セキュリティ実装技術	・ システム開発や運用におけるセキュリティ対策やセキュリティ実装の仕組み、技術、効果を修得し、セキュリティ管理に応用する。	Ｐ．58
第４回	セキュリティ事故の初動処理	・ セキュリティ違反を発見するツールを駆使し、継続的に監視できる知識を応用する。 ・ 事故発生時における被害拡大防止、証拠保存など緊急対応の規定を理解し、応用する。	Ｐ．59
第５回	セキュリティ事故の分析と復旧	・ 事故の損害と影響を評価し、事故原因を特定できる知識を理解し、応用する。 ・ 再発防止策を検討・実施し、システムを復旧する知識を応用する。	Ｐ．60
第６回	セキュリティの評価（評価基準）	・ 侵入検査を継続的に実施し、セキュリティポリシの遵守状況を評価する知識を修得する。 ・ セキュリティの評価情報を、セキュリティ対策の見直しに利用する知識を応用する。	Ｐ．61
第７回	問題点の整理と分析	・ 運用上や技術上の問題から影響を受けるセキュリティを特定し、分析できる。 ・ 最新のセキュリティ技術情報を収集し、社内システムの適用を評価することができる。	Ｐ．62
第８回	セキュリティ対策の更新	・ セキュリティ対策の更新体制を整備し、ポリシを更新する知識を応用する。 ・ 継続的にセキュリティ対策の見直しを行う知識を修得し、応用する。	Ｐ．63

5.4. コマシラバス（1/8）

研修コース名	セキュリティ管理中級
回数	第 1 回
テーマ	情報セキュリティの技術
学習目標	・ セキュリティ管理の対象となる情報セキュリティに関する技術の種類、仕組み、特徴などを理解し、この技術を使用してセキュリティ管理に応用する。
学習内容	(1) 暗号化技術 公開鍵暗号化方式、共通鍵暗号化方式、公開鍵、秘密鍵 DES、RSA、楕円暗号方式、S/MIME、PGP など (2) 認証技術 ディジタル認証、ディジタル署名、メッセージ認証 時刻認証、チャレンジレスポンス認証 など (3) 利用者確認 ログイン、コールバック、アクセス管理、IC カード PIN コード、Kerberos 方式、ワンタイムパスワード シングルサインオン など (4) 生体認証技術 指紋認証、静脈パターン認証、虹彩認証 声紋認証、顔認証、網膜認証、 本人拒否率、他人受入率 など (5) 公開鍵基盤(PKI) 公開鍵証明書、CA、GPKI、BCA、SSL、SET など
研修・教育方法	講義(ミニ演習課題を含む)
時間の目安	90 分（演習課題を含む） （講義：80 分　　演習課題：10 分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】3. セキュリティの分析
その他	

5.4. コマシラバス（2/8）

研修コース名	セキュリティ管理中級
回数	第２回
テーマ	情報セキュリティ対策
学習目標	・ 人的セキュリティ、技術的セキュリティ、物理的セキュリティの側面から、情報セキュリティ技術を理解し、セキュリティ管理に応用する。
学習内容	(1) 人的セキュリティ対策 情報セキュリティポリシ、社内規定、 情報セキュリティ教育、情報セキュリティ訓練 情報セキュリティ啓蒙　事件事故への対処マニュアル パスワード管理、セキュリティ担当者、内部統制　など (2) 技術的セキュリティ対策 クラッキング対策、暗号処理、ファイアウォール コンピュータウイルス対策、OS アップデート ネットワーク監視、ネットワークアクセス権の設定 アクセス制御、侵入検知、電子透かし　など (3) 物理的セキュリティ対策 RASIS RAS 技術、耐震耐火設備、UPS、二重化技術 ミラーリング、ハウジングセキュリティ、監視カメラ 施錠管理、入退室管理　など
研修・教育方法	講義(ミニ演習課題を含む)
時間の目安	90 分（演習課題を含む） （講義：80 分　　演習課題：10 分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】3. セキュリティの分析
その他	

5.4. コマシラバス（3/8）

研修コース名	セキュリティ管理中級
回数	第3回
テーマ	セキュリティ実装技術
学習目標	・ システム開発や運用におけるセキュリティ対策の仕組み、技術、効果を修得し、セキュリティ管理に応用する。 ・ ネットワーク、データベース、アプリケーションへの実装を修得し、セキュリティ管理に応用する。
学習内容	(1) セキュアOS MAC 最小権限、トランスデッドOS など (2) ネットワークセキュリティ 関門ルータ、ファイアウォール、 パケットフィルタリング、 アプリケーションゲートウェイ方式 IDS、IPS、認証サーバ、NAT、IPマスカレード VPN、セキュリティ監視、SSID、WEP、WPA MACアドレス、フィルタリング、ハニーポット など (3) データベースセキュリティ 暗号化、利用者認証、データベースアクセス制御 データベースバックアップ、ログの取得、 アカウント管理、パスワード管理、外部媒体の利用制御 不正アクセス検知、SQL、インジェクション など (4) アプリケーションセキュリティ Webシステムのセキュリティ対策、 セキュアプログラミング、バッファオーバーフロー攻撃 クロスサイトスクリプティング攻撃、SQL インジェクション攻撃、スパム対策、ウイルス対策 など
研修・教育方法	講義(ミニ演習課題を含む)
時間の目安	90分（演習課題を含む） （講義：80分 演習課題：10分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】3. セキュリティの分析
その他	

5.4. コマシラバス（4/8）

研修コース名	セキュリティ管理中級
回数	第４回
テーマ	セキュリティ事故の初動処理
学習目標	・ セキュリティ管理の立場からセキュリティ違反を発見するツールを駆使し、継続的に監視できる知識を応用する。 ・ セキュリティ管理の立場から事故発生時における被害拡大防止、証拠保存など緊急対応の規定を理解し、応用する。
学習内容	(1)　事故の検知 ログファイル、システムログ、システムエラーログ アラーム記録 トラフィックパターン分析 システム整合性 侵入検知システム 侵入監視サービス　など (2)　初動処理 緊急時対応マニュアル 事故の連絡と説明 処置の優先順位 被害拡大の防止策 証拠保存のタイミング　など
研修・教育方法	講義(ミニ演習課題を含む)
時間の目安	90 分（演習課題を含む） （講義：80 分　演習課題：10 分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】3. セキュリティの分析
その他	

5.4. コマシラバス（5/8）

研修コース名	セキュリティ管理中級
回数	第５回
テーマ	セキュリティ事故の分析と復旧
学習目標	・ 事故の損害と影響を評価し、事故原因を特定できる知識を理解し、応用する。 ・ セキュリティ管理の立場から再発防止策を検討・実施し、システムを復旧する知識を応用する。
学習内容	(1) 事故の分析 被害状況の調査方法 ネットワーク機器の設定チェック トランザクションログのチェック 事故原因の調査方法 事故原因の追及手順 セキュリティ情報 操作記録 アクセス記録 範囲と損害 コンピュータフォレンジックス　など (2) 復旧処理 復旧処置 事故の記録　など (3) 再発防止 再発防止策の検討と実施 システム再構築　など
研修・教育方法	講義(ミニ演習課題を含む)
時間の目安	90 分（演習課題を含む） （講義：80 分　演習課題：10 分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】3. セキュリティの分析
その他	

5.4. コマシラバス（6/8）

研修コース名	セキュリティ管理中級
回数	第6回
テーマ	セキュリティの評価
学習目標	・ 侵入検査を継続的に実施し、セキュリティポリシの遵守状況を評価する知識を修得する。 ・ セキュリティ管理の立場からセキュリティの評価情報を、セキュリティの見直しに利用する知識を応用する。 ・
学習内容	(1) セキュリティポリシ遵守状況 セキュリティ侵犯テスト 継続実施 不備発見時の対応 (2) 侵入検査サービス (3) セキュリティ強化策 セキュリティ勧告 セキュリティホール情報 パッチ情報 (4) セキュリティ技術評価 評価方法、セキュリティ機能要件、 セキュリティ保証要件、保障レベル ISO/IEC 15408 CC、CEM、ST、CEM、EAL
研修・教育方法	講義(ミニ演習課題を含む)
時間の目安	90分（演習課題を含む） （講義：80分　演習課題：10分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】3. セキュリティの分析
その他	

5.4. コマシラバス（7/8）

研修コース名	セキュリティ管理中級
回数	第 7 回
テーマ	新たなリスクの整理と分析
学習目標	・ セキュリティ管理に運用上や技術上の問題から影響を受けるセキュリティを特定し、分析できる。 ・ 最新のセキュリティ技術情報を収集し、社内システムの適用を評価することができる。新たなリスクにより影響を受けるセキュリティの箇所を識別でき、整理することができる。
学習内容	(1) 技術情報の収集と評価 セキュリティ情報の収集 セキュリティ技術情報の収集 評価基準 適用の判断（費用対効果） (2) 運用上の問題点整理と分析 利用者アンケートとヒアリング情報 セキュリティ違反状況 問題点分析 利用者の反発、非現実的なルール、など (3) 技術上の問題点整理と分析 問題点の分析 新技術導入による影響 (4) 見直し項目の整理
研修・教育方法	講義(ミニ演習課題を含む)
時間の目安	90 分（演習課題を含む） （講義：80 分　演習課題：10 分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】4. セキュリティの見直し
その他	

5.4. コマシラバス（8/8）

研修コース名	セキュリティ管理中級
回数	第８回
テーマ	情報セキュリティ対策の更新
学習目標	・ セキュリティ対策の更新体制を整備し、対策を更新する知識を応用する。 ・ セキュリティ管理の立場から、継続的にセキュリティ対策の見直しを行う知識を修得し、応用する。
学習内容	(1) 体制構築 対策更新体制 (2) 更新準備 新たなリスク 指摘事項 改善勧告 (3) セキュリティシステムの再構築 機能設計 実装 運用 管理 (4) 更新手続き 情報セキュリティ監査 (5) 継続的見直し
研修・教育方法	講義(ミニ演習課題を含む)
時間の目安	90 分（演習課題を含む） （講義：80 分　演習課題：10 分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】4. セキュリティの見直し
その他	

6. （M03）セキュリティ管理上級

対応する機能役割定義

大項目		中項目	
大No.	大項目名（タスク）	No.	中項目名
30	IT 基盤構築・維持・管理	5	品質統制フレームワークの運営
100	IS 保守	1	保守計画
		2	保守の実施
140	セキュリティ	1	セキュリティ方針の策定
		2	セキュリティ基準の策定
		3	セキュリティの分析
		4	セキュリティの見直し

6.1. 科目シラバス

研修コースコード	14－M－03
研修コース名	セキュリティ管理上級
研修ロードマップ	(14)セキュリティ
知識項目(BOK)分野	テクノロジ系　－　マネジメント
知識項目(BOK)分類	【大分類】4. 技術要素 【中分類】11. セキュリティ
レベル区分	セキュリティのレベル 4 を目指す者
受講前提	セキュリティに関してレベル 3 程度以上のもの
科目概要	・ 「セキュリティ管理中級」の後続コースとして、全ての情報資産に対する必要なセキュリティの企画・導入・運用を含む業務全般の実施や指導・管理できる高度かつ専門的な知識の修得を目的とする。 ・ セキュリティポリシを運用する観点から、管理システムを導入・構築し、運用管理、そして、問題発生時の改善処置の実施やセキュリティポリシそのものを見直す能力を身に着ける。
学習目標概要	・ セキュリティ基本方針やセキュリティ対策基準等に従って、自ら遵守し、また、組織等に適切に運用することができる。 ・ セキュリティ事故を検知した際、緊急対応の規定に従った適切な初動処理、その被害状況や範囲、事故原因等を特定し、再発防策を施して事故か復旧させることができる ・ 最新の脅威や事故の情報を収集し、新たなリスクの整理と分析を行って情報セキュリティポリシを見直し、セキュリティポリシを再構築する工程を管理することができる。
研修・教育方法	ワークショップ(演習課題を含む)
修得スキルの評価方法	以下の状況等を総合的に判断して評価する。 受講前・受講後の知識確認テスト 定量アンケート 受講レポート 演習課題の取り組み状況　など
カリキュラム構成	1 コマ 180 分　×　6 コマ （クラスルーム：標準日数 3 日）
情報処理技術者試験	情報セキュリティスペシャリスト試験の一部
備考	（次のＢＯＫも対応） 【大分類】9. 企業と法務 【中分類】23. 法務

6.2. 知識項目対応表

◎＝主項目として扱う、○＝関連項目として扱う

共通キャリア・スキルフレームワーク					対象項目
分野	大分類		中分類		
テクノロジ系	1	基礎理論	1	基礎理論	
			2	アルゴリズムとプログラミング	
	2	コンピュータシステム	3	コンピュータ構成要素	
			4	システム構成要素	
			5	ソフトウェア	
			6	ハードウェア	
	3	技術要素	7	ヒューマンインターフェース	
			8	マルチメディア	
			9	データベース	
			10	ネットワーク	
			11	セキュリティ	◎
	4	開発技術	12	システム開発技術	
			13	ソフトウェア開発技術管理	
マネジメント系	5	プロジェクトマネジメント	14	プロジェクトマネジメント	
	6	サービスマネジメント	15	サービスマネジメント	
			16	システム監査	
ストラテジ系	7	システム戦略	17	システム戦略	
			18	システム企画	
	8	経営戦略	19	経営戦略マネジメント	
			20	技術戦略マネジメント	
			21	ビジネスインダストリ	
	9	企業と法務	22	企業活動	
			23	法務	○

6.3. コマタイトル一覧

回数	テーマ	学習目標	参照先
第１回	情報セキュリティ管理	・ 情報セキュリティ基本方針や各種セキュリティ規定などを含め、情報セキュリティマネジメントシステムを理解し、運用管理できる。 ・ 情報セキュリティを実現するために必要なセキュリティ実装技術を理解し、活用状況を管理できる。	P．68
第２回	事故対応	・ セキュリティの実施状況管理において、事故を検知した場合、規定に基づく初動処置を行い、被害を最小限に食い止め、復旧することができる。 ・ 初動処置後、事故の分析を行い、再発防止策を策定することができる。	P．69
第３回	セキュリティの評価	・ 侵入検査を継続的に実施し、セキュリティポリシの遵守状況を評価することができる。 ・ 侵入検査で不備のある場合は、速やかに対策を行うことができる。 ・ セキュリティの評価情報を、セキュリティの見直しに利用することができる。	P．70
第４回	最新情報と問題点の分析と評価	・ セキュリティ管理の立場から最新のセキュリティ技術情報を収集し、社内システムの適用を評価することができる。 ・ ポリシ実施上の問題点の収集、整理、新たに導入した技術により影響を受けるポリシの箇所を識別し、整理することができる。	P．71
第５回	新たなリスクの整理と分析	・ セキュリティ管理の立場から新たなリスクにより影響を受けるセキュリティポリシの箇所を識別でき、整理することができる。 ・ 整理された問題点について、セキュリティポリシ変更に対する分析ができ、ポリシの見直し箇所をすべて特定することができる。	P．72
第６回	セキュリティポリシの更新	・ セキュリティポリシの更新体制を整備することができる。 ・ 分析結果からポリシ変更部分について、再確認し、セキュリティポリシを更新できる。 ・ セキュリティ管理の立場から継続的にセキュリティポリシの見直しを行うことができる。	P．73

6.4. コマシラバス（1/6）

研修コース名	セキュリティ管理上級
回数	第 1 回
テーマ	情報セキュリティ管理
学習目標	・ 情報セキュリティ基本方針や各種セキュリティ規定などを含め、情報セキュリティマネジメントシステムを理解し、運用管理できる。 ・ 情報セキュリティを実現するために必要なセキュリティ実装技術を理解し、活用状況を管理できる。
学習内容	――講義―― (1)　情報セキュリティポリシ 情報セキュリティ基本方針 情報セキュリティ対策基準 情報セキュリティに関する規定　など (2)　情報セキュリティマネジメントシステム ISMS 適合評価制度 ISMS 認証 ――ワークショップ―― ケースの (1)　情報セキュリティポリシの理解 （ポリシ策定を一部含む） (2)　セキュリティの実施状況管理
研修・教育方法	ワークショップ（講義を含む・クラスルーム）
時間の目安	180 分（演習課題を含む） （講義：60 分　　演習課題：120 分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】1. セキュリティ方針の策定
その他	ケースに使用するモデル企業は、文書または図解で提示し、第 1 回から第 6 回まで、通しで利用できるものが望ましい。

6.4. コマシラバス（2/6）

研修コース名	セキュリティ管理上級
回数	第２回
テーマ	事故対応
学習目標	・ セキュリティの実施状況管理において、事故を検知した場合、規定に基づく初動処置を行い、被害を最小限に食い止め、復旧することができる。 ・ 初動処置後、事故の分析を行い、再発防止策を策定することができる。
学習内容	――講義―― (1)　事故の検知 ログファイル、システム整合性 侵入検知システム、侵入監視サービス　など (2)　初動処理 緊急時対応マニュアル、処置の優先順位 被害拡大の防止策、証拠保存のタイミング　など (3)　分析 被害状況、事故状況、コンピュータフォレンジックス　など (4)　復旧 復旧処置、システムの再構築、事故の記録 (5)　再発防止策 再発防止策、システムの再構築 ――ワークショップ―― ケースの (1)　事故の検地と初動処置 (2)　事故の分析と復旧 (3)　再発防止策
研修・教育方法	ワークショップ（講義を含む・クラスルーム）
時間の目安	180 分（演習課題を含む） （講義：60 分　　演習課題：120 分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】3. セキュリティの分析
その他	ケースに使用するモデル企業は、文書または図解で提示し、第１回から第６回まで、通しで利用できるものが望ましい。

6.4. コマシラバス（3/6）

研修コース名	セキュリティ管理上級
回数	第3回
テーマ	セキュリティの評価
学習目標	・ 侵入検査を継続的に実施し、セキュリティポリシの遵守状況を評価することができる。 ・ 侵入検査で不備のある場合は、速やかに対策を行うことができる。 ・ セキュリティの評価情報を、セキュリティの見直しに利用することができる。
学習内容	ーー講義ーー (1) セキュリティ技術評価 セキュリティ機能要件 セキュリティ保証要件 ISO/IEC 15408 (2) 侵入検査サービス (3) セキュリティ強化策 (4) セキュリティ管理の継続実施 ーーワークショップーー (1) セキュリティ評価 (2) 見直し事項の整理
研修・教育方法	ワークショップ（講義を含む・クラスルーム）
時間の目安	180分（演習課題を含む） （講義：60分　　演習課題：120分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】3. セキュリティの分析
その他	ケースに使用するモデル企業は、文書または図解で提示し、第1回から第6回まで、通しで利用できるものが望ましい。

6.4. コマシラバス（4/6）

研修コース名	セキュリティ管理上級
回数	第4回
テーマ	最新情報と問題点の分析と評価
学習目標	・ セキュリティ管理の立場から最新のセキュリティ技術情報を収集し、社内システムの適用を評価することができる。 ・ ポリシ実施上の問題点を収集、整理することができる。 ・ 新たに導入した技術により、影響を受けるセキュリティポリシの箇所を識別し、整理することができる。
学習内容	――講義―― (1) 技術情報の収集と評価 技術情報 (2) 運用上の問題点整理 利用者アンケートとヒアリング情報 セキュリティ違反状況 問題点の分析・整理 (3) 技術上の問題点整理 問題点の分析・整理 ――ワークショップ―― (1) 運用上の問題点とその解決策案 (2) 技術上の問題点とその解決策案
研修・教育方法	ワークショップ（講義を含む・クラスルーム）
時間の目安	180分（演習課題を含む） （講義：60分　　演習課題：120分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】4. セキュリティ対策の見直し
その他	ケースに使用するモデル企業は、文書または図解で提示し、第1回から第6回まで、通しで利用できるものが望ましい。

6.4. コマシラバス（5/6）

研修コース名	セキュリティ管理上級
回数	第5回
テーマ	新たなリスクの整理と分析
学習目標	・ セキュリティ管理の立場から新たなリスクにより影響を受けるセキュリティポリシの箇所を識別し、整理することができる。 ・ 整理された問題点について、セキュリティポリシ変更に対する分析ができ、ポリシの見直し箇所をすべて特定することができる。
学習内容	――講義―― (1) 最新情報の収集 最近のセキュリティ事例（JPERT/CC、IPA　など） 最新セキュリティ対策情報 (2) 事例によるリスク評価 (3) ポリシの見直し 最新情報からの見直し 事例からの見直し (4) 見直し項目の整理 ――ワークショップ―― (1) ポリシの見直し (2) 見直し項目の整理
研修・教育方法	ワークショップ（講義を含む・クラスルーム）
時間の目安	180分（演習課題を含む） （講義：60分　　演習課題：120分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】4. セキュリティ対策の見直し
その他	ケースに使用するモデル企業は、文書または図解で提示し、第1回から第6回まで、通しで利用できるものが望ましい。

6.4. コマシラバス（6/6）

研修コース名	セキュリティ管理上級
回数	第6回
テーマ	情報セキュリティポリシの更新
学習目標	・ セキュリティポリシの更新体制を整備することができる。 ・ 分析結果からポリシ変更部分について再確認し、セキュリティポリシを更新できる。 ・ セキュリティ管理の立場から継続的にセキュリティポリシの見直しを行うことができる。
学習内容	――講義―― (1) 体制構築 ポリシ更新体制 (2) 更新箇所の検証 リスクの再分析 リスクの再評価 (3) ギャップ分析 現行箇所と更新箇所 (4) 更新手続き (5) 継続的見直し ――ワークショップ―― (1) ポリシ更新体制の構築 (2) 変更箇所のギャップ分析 (3) 継続的活動の構築
研修・教育方法	ワークショップ（講義を含む・クラスルーム）
時間の目安	180分（演習課題を含む） （講義：60分　　演習課題：120分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】4. セキュリティ対策の見直し
その他	ケースに使用するモデル企業は、文書または図解で提示し、第1回から第6回まで、通しで利用できるものが望ましい。

7.（S01）情報セキュリティポリシ

対応する機能役割定義

大項目		中項目	
大No.	大項目名（タスク）	No.	中項目名
140	セキュリティ	1	セキュリティ方針の策定
		2	セキュリティ基準の策定

7.1. 科目シラバス

研修コースコード	14－S－01
研修コース名	情報セキュリティポリシ
研修ロードマップ	(14)セキュリティ
知識項目(BOK)分野	テクノロジ系　ー　ストラテジ
知識項目(BOK)分類	【大分類】4. 技術要素 【中分類】11. セキュリティ
レベル区分	セキュリティのレベル 2 を目指す者
受講前提	レベル 1 程度以上のもの
科目概要	・ セキュリティについて、上位者の指導の下または一定程度であれば独力でセキュリティ対策に関する作業ができる基本的な知識の修得を目的とする。 ・ IS 導入や IS 運用等におけるセキュリティの考え方、セキュリティ機能、情報セキュリティポリシ策定等の業務の概要に関する基礎知識を学習する。
学習目標概要	・ 情報セキュリティの目的、考え方、重要性、および情報セキュリティ管理の目的、考え方を理解できる。 ・ 情報資産に対する脅威や脆弱性などの種類、リスク分析と評価の手順を理解できる。 ・ 情報セキュリティポリシの目的や考え方を、および情報セキュリティマネジメントシステム、セキュリティに対する他の基準、セキュリティ機関の役割を理解できる。 ・
研修・教育方法	講義(ミニ演習課題を含む)
修得スキルの評価方法	以下の状況等を総合的に判断して評価する。 受講前・受講後の知識確認テスト 定量アンケート 受講レポート 演習課題の取り組み状況　など
カリキュラム構成	1 コマ 90 分　×　4 コマ （クラスルーム：標準日数 1 日）
情報処理技術者試験	基本情報技術者試験　セキュリティの一部
備考	（次のＢＯＫにも対応） 【大分類】9. 企業と法務 【中分類】23. 法務

7.2. 知識項目対応表

◎＝主項目として扱う、○＝関連項目として扱う

共通キャリア・スキルフレームワーク					対象項目
分野	大分類		中分類		
テクノロジ系	1	基礎理論	1	基礎理論	
			2	アルゴリズムとプログラミング	
	2	コンピュータシステム	3	コンピュータ構成要素	
			4	システム構成要素	
			5	ソフトウェア	
			6	ハードウェア	
	3	技術要素	7	ヒューマンインターフェース	
			8	マルチメディア	
			9	データベース	
			10	ネットワーク	
			11	セキュリティ	◎
	4	開発技術	12	システム開発技術	
			13	ソフトウェア開発技術管理	
マネジメント系	5	プロジェクトマネジメント	14	プロジェクトマネジメント	
	6	サービスマネジメント	15	サービスマネジメント	
			16	システム監査	
ストラテジ系	7	システム戦略	17	システム戦略	
			18	システム企画	
	8	経営戦略	19	経営戦略マネジメント	
			20	技術戦略マネジメント	
			21	ビジネスインダストリ	
	9	企業と法務	22	企業活動	
			23	法務	○

7.3. コマタイトル一覧

回数	テーマ	学習目標	参照先
第１回	情報セキュリティ管理と情報資産	・ 情報セキュリティの目的、考え方、重要性および情報セキュリティ管理の考え方を理解できる。 ・ 企業の情報資産を識別し、資産の重要度や致命度を評価する知識を理解できる。 ・ 情報資産に対する脅威や脆弱性を理解できる。	P．78
第２回	リスク分析と評価	・ 代表的なリスク分析手順を理解できる。 ・ 情報資産を保護する手段としてのリスク分析や、リスクの発生頻度や被害の大きさから、リスクを評価する方法を理解できる。 ・ リスク評価に基づき、情報セキュリティ対策や緊急時計画を検討することを理解できる。	P．79
第３回	情報セキュリティポリシ	・ 情報セキュリティポリシの目的、考え方および情報セキュリティポリシに従った組織運営を理解できる。 ・ 情報セキュリティマネジメントシステムの目的や仕組みを理解できる。 ・ セキュリティ機関の役割を理解できる。	P．80
第４回	セキュリティに関する社内規定	・ セキュリティの観点から検討した社内の規定や情報システムの規定について、どのようなものがあるかを理解できる ・ 各種規定とセキュリティポリシとの整合性があることを理解できる。	P．81

7.4. コマシラバス（1/4）

研修コース名	情報セキュリティポリシ
回数	第 1 回
テーマ	情報セキュリティ管理と情報資産
学習目標	・ 情報セキュリティの目的、考え方、重要性および情報セキュリティ管理の考え方を理解できる。 ・ 企業の情報資産を識別し、資産の重要度や致命度を評価する知識を理解できる。 ・ 情報資産に対する脅威や脆弱性を理解できる。
学習内容	(1) 情報セキュリティ 目的、考え方、重要性 情報の機密性、完全性、可用性 情報システムの信頼性 否認防止性、責任追跡性、真正性　など (2) 情報セキュリティ管理 目的、考え方、保護対象(情報資産) (3) 脅威 事故、災害、故障、盗難、エラー、コンピュータ犯罪 情報漏えい、不正アクセス、不正侵入、盗聴 なりすまし、改ざん、DoS 攻撃、ウイルス、ワーム ソーシャルエンジニアリング　など 物理的脅威・技術的脅威・人的脅威の区分 (4) 脆弱性 欠陥、不徹底、未整備、不備　など バグ、セキュリティホール、など
研修・教育方法	講義(ミニ演習課題を含む)
時間の目安	90 分（演習課題を含む） （講義：80 分　演習課題：10 分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】1. セキュリティ方針の策定
その他	

7.4. コマシラバス（2/4）

研修コース名	情報セキュリティポリシ
回数	第２回
テーマ	リスク分析と評価
学習目標	・ 代表的なリスク分析手順を理解できる。 ・ 情報資産を保護する手段としてのリスク分析や、リスクの発生頻度や被害の大きさから、リスクを評価する方法を理解できる。 ・ リスク評価に基づき、情報セキュリティ対策や緊急時計画を検討することを理解できる。
学習内容	(1) 情報資産の分類 機密性、完全性、可用性 重要度 致命度 (2) リスク評価 発生頻度と損害の大きさ リスクの種類 財産損失、収益の喪失 ペリル、ハザード、モラルハザード (1) リスク対策 リスクコントロール、リスクヘッジ リスクファイナンス、情報化保険 リスク回避、リスク移転、リスク保有、リスク最適化 リスク分離、リスク集中
研修・教育方法	講義(ミニ演習課題を含む)
時間の目安	90 分（演習課題を含む） （講義：80 分　演習課題：10 分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】1. セキュリティ方針の策定
その他	

7.4. コマシラバス（3/4）

研修コース名	情報セキュリティポリシ
回数	第3回
テーマ	情報セキュリティポリシ
学習目標	・ 情報セキュリティポリシの目的、考え方および情報セキュリティポリシに従った組織運営を理解できる。 ・ 情報セキュリティマネジメントシステムの目的や仕組みを理解できる。 ・ セキュリティ機関の役割を理解できる。
学習内容	(1) 情報セキュリティポリシ 情報セキュリティ基本方針 情報セキュリティ対策基準 (2) 情報セキュリティマネジメンシステム 目的と仕組み（維持・改善） ISMS 適合評価制度 ISMS 認定 ISO/IEC 17799 （IJS Q 27002） ISO/IEC 27001 (3) セキュリティ機関 役割 IPA セキュリティセンター JPCERT/CC
研修・教育方法	講義(ミニ演習課題を含む)
時間の目安	90 分（演習課題を含む） （講義：80 分 演習課題：10 分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】2. セキュリティ基準の策定
その他	

7.4. コマシラバス（4/4）

研修コース名	情報セキュリティポリシ
回数	第4回
テーマ	セキュリティに関する社内規定
学習目標	・ セキュリティの観点から検討した社内の規定や情報システムの規定について、どのようなものがあるかを理解できる ・ 各種規定とセキュリティポリシとの整合性があることを理解できる。
学習内容	(1) 情報セキュリティポリシの階層 情報セキュリティ基本方針 情報セキュリティ対策基準 各種社内のセキュリティ関連規定 (2) セキュリティ関連規定 雇用契約/職務規定 機密管理規定 文書管理規定 情報管理規定 プライバシポリシ セキュリティ教育の規定 罰則の規定 対外説明の規定 例外の規定 規則変更の規定 承認手続き　など
研修・教育方法	講義(ミニ演習課題を含む)
時間の目安	90分（演習課題を含む） （講義：80分　演習課題：10分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】2. セキュリティ基準の策定
その他	

8. （S02）セキュリティガイドライン

対応する機能役割定義

大項目		中項目	
大No.	大項目名（タスク）	No.	中項目名
140	セキュリティ	1	セキュリティ方針の策定
		4	セキュリティの見直し

8.1. 科目シラバス

研修コースコード	14－S－02
研修コース名	セキュリティガイドライン
研修ロードマップ	(14)セキュリティ
知識項目(BOK)分野	テクノロジ系　－　ストラテジ
知識項目(BOK)分類	【大分類】4. 技術要素 【中分類】11. セキュリティ
レベル区分	セキュリティのレベル 3 を目指す者
受講前提	セキュリティに関してレベル 2 程度以上のもの
科目概要	・ 「セキュリティポリシ」の後続コースとして、情報セキュリティ基本方針や情報セキュリティ対策基準の策定に関連する仕組みや手法およびそれらを応用できる知識の修得を目的とする。 ・ 情報セキュリティ基本方針や情報セキュリティ対策基準の策定に関連する知識を修得し、情報セキュリティ基本方針や情報セキュリティ対策基準の策定に応用する。
学習目標概要	・ 情報セキュリティの目的、考え方、重要性、および情報セキュリティ管理の目的、考え方を理解し、応用する。 ・ 情報資産に対する脅威や脆弱性などの種類、リスク分析と評価の手順を修得し、応用する。 ・ 情報セキュリティポリシの目的、考え方を修得し、応用する。 ・ 情報セキュリティマネジメントシステムやセキュリティに対する他の基準の考え方、セキュリティ機関の役割を修得し、応用する。
研修・教育方法	講義(ミニ演習課題を含む)
修得スキルの評価方法	以下の状況等を総合的に判断して評価する。 受講前・受講後の知識確認テスト 定量アンケート 受講レポート 演習課題の取り組み状況　など
カリキュラム構成	1 コマ 90 分　×　8 コマ （クラスルーム：標準日数 2 日）
情報処理技術者試験	応用情報技術者試験　セキュリティの一部
備考	（次のＢＯＫも対応） 【大分類】9. 企業と法務 【中分類】23. 法務

8.2. 知識項目対応表

◎＝主項目として扱う、○＝関連項目として扱う

共通キャリア・スキルフレームワーク					対象項目
分野	大分類		中分類		
テクノロジ系	1	基礎理論	1	基礎理論	
			2	アルゴリズムとプログラミング	
	2	コンピュータシステム	3	コンピュータ構成要素	
			4	システム構成要素	
			5	ソフトウェア	
			6	ハードウェア	
	3	技術要素	7	ヒューマンインターフェース	
			8	マルチメディア	
			9	データベース	
			10	ネットワーク	
			11	セキュリティ	◎
	4	開発技術	12	システム開発技術	
			13	ソフトウェア開発技術管理	
マネジメント系	5	プロジェクトマネジメント	14	プロジェクトマネジメント	
	6	サービスマネジメント	15	サービスマネジメント	
			16	システム監査	
ストラテジ系	7	システム戦略	17	システム戦略	
			18	システム企画	
	8	経営戦略	19	経営戦略マネジメント	
			20	技術戦略マネジメント	
			21	ビジネスインダストリ	
	9	企業と法務	22	企業活動	
			23	法務	○

8.3. コマタイトル一覧

回数	テーマ	学習目標	参照先
第１回	情報セキュリティの目的と情報セキュリティ管理	・ 情報セキュリティの目的、考え方、重要性を理解し、応用する。 ・ 情報セキュリティ管理の考え方を修得し、応用する。	Ｐ．86
第２回	情報資産	・ 企業の情報資産を識別し、資産の重要度や致命度を評価する知識を理解し、応用する。 ・ 情報資産に対する脅威や脆弱性を理解し、応用する。	Ｐ．87
第３回	リスク分析と評価	・ 代表的なリスク分析手法を理解し、情報資産を調査する手法を修得し、応用する。 ・ 情報資産を保護する手段として、リスク分析・評価を行う手順を修得し、応用する。	Ｐ．88
第４回	リスク対策	・ リスクの発生頻度や被害の大きさから、リスクを評価する知識を理解し、応用する。 ・ リスク評価に基づき、情報セキュリティ対策や緊急時計画を理解し、応用する。	Ｐ．89
第５回	情報セキュリティポリシ	・ 情報セキュリティポリシの目的、考え方を理解し、応用する。 ・ 情報セキュリティポリシに従った組織運営を理解し、応用する。	Ｐ．90
第６回	企業活動一般のセキュリティ規定	・ セキュリティの観点から社内規定を策定する知識を修得し、応用する。 ・ 策定した社内規定と、セキュリティポリシの整合性を確認する知識を修得し、応用する。	Ｐ．91
第７回	情報システムのセキュリティ規定	・ セキュリティの観点から情報システム運用やネットワーク利用、セキュリティ管理などの情報システムのセキュリティ規定などを策定する知識を修得し、応用する。	Ｐ．92
第８回	情報セキュリティマネジメントシステム	・ 緊急時・災害時の対応を理解し、応用できる。 ・ 情報セキュリティマネジメントシステムの仕組みやセキュリティ機関の役割を理解し、応用できる。	Ｐ．93

8.4. コマシラバス（1/8）

研修コース名	セキュリティガイドライン
回数	第1回
テーマ	情報セキュリティの目的と情報セキュリティ管理
学習目標	・ 情報セキュリティの目的、考え方、重要性を理解し、応用する。 ・ 情報セキュリティ管理の考え方を修得し、応用する。
学習内容	(1) 情報セキュリティ 目的と考え方 重要性 情報の機密性、完全性、可用性 情報システムの信頼性 否認防止性、責任追跡性、真正性　など (2) 情報システムのセキュリティに関するガイドライン(OECD) (3) 情報セキュリティ管理 目的と考え方 保護対象 物理的資産 人的資産 管理的資産 サービス 無形資産　など
研修・教育方法	講義(ミニ演習課題を含む)
時間の目安	90分（演習課題を含む） （講義：70分　演習課題：20分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】1. セキュリティ方針の策定
その他	

8.4. コマシラバス（2/8）

研修コース名	セキュリティガイドライン
回数	第２回
テーマ	情報資産
学習目標	・ 企業の情報資産を識別し、資産の重要度や致命度を評価する知識を理解し、応用する。 ・ 情報資産に対する脅威や脆弱性を理解し、応用する。
学習内容	(1) 情報資産 物理的資産 人的資産 管理的資産 サービス 無形資産　など (2) 脅威 事故、災害、故障、盗難、エラー、コンピュータ犯罪 情報漏えい、不正アクセス、不正侵入、盗聴 なりすまし、改ざん、DoS 攻撃、ウイルス、ワーム ソーシャルエンジニアリング　など 物理的脅威・技術的脅威・人的脅威の区分 (3) 脆弱性 欠陥、不徹底、未整備、不備　など バグ、セキュリティホール、など
研修・教育方法	講義(ミニ演習課題を含む)
時間の目安	90 分（演習課題を含む） （講義：70 分　演習課題：20 分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】1. セキュリティ方針の策定
その他	

8.4. コマシラバス（3/8）

研修コース名	セキュリティガイドライン
回数	第3回
テーマ	リスク分析と評価
学習目標	・ 代表的なリスク分析手法を理解し、情報資産を調査する手法を修得し、応用する。 ・ 情報資産を保護する手段として、リスク分析・評価を行う手順を修得し、応用する。
学習内容	(1) リスク分析手法 定量的リスク分析 定性的リスク分析 JRAM（JIPDEC Risk Analysis Method） (2) 情報資産の分類 機密性、完全性、可用性 重要度 致命度 (3) リスク評価 発生頻度と損害の大きさ リスクの種類 財産損失、収益の喪失 ペリル ハザード モラルハザード 年間予想損失額 得点法 コスト要因
研修・教育方法	講義(ミニ演習課題を含む)
時間の目安	90分（演習課題を含む） （講義：70分　演習課題：20分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】1. セキュリティ方針の策定
その他	

8.4. コマシラバス（4/8）

研修コース名	セキュリティガイドライン
回数	第4回
テーマ	リスク対策
学習目標	・ リスクの発生頻度や被害の大きさから、リスクを評価する知識を理解し、応用する。 ・ リスク評価に基づき、情報セキュリティ対策や緊急時計画を理解し、応用する。
学習内容	(1) リスク対策 リスクコントロール リスクヘッジ リスクファイナンス 情報化保険 リスク回避 リスク移転 リスク保有 リスク最適化 リスク分離 リスク集中 (2) 緊急事態 緊急事態の区分 緊急時計画 (3) バックアップ対策 (4) 復旧計画
研修・教育方法	講義(ミニ演習課題を含む)
時間の目安	90分（演習課題を含む） （講義：70分　演習課題：20分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】1. セキュリティ方針の策定
その他	

8.4. コマシラバス（5/8）

研修コース名	セキュリティガイドライン
回数	第5回
テーマ	情報セキュリティポリシ
学習目標	・ 情報セキュリティポリシの目的、考え方を理解し、応用する。 ・ 情報セキュリティポリシに従った組織運営を理解し、応用する。
学習内容	(1) 情報セキュリティ基本方針 目的 範囲 達成レベル 情報セキュリティに関する責任者 経営者・従業員の遵守事項 情報セキュリティ活動の実施体制 (2) 情報セキュリティポリシ関連事項 マネジメントレビュ リスクアセスメント インシデント管理 事業継続管理 セキュリティ教育・研修 コンプライアンス セキュリティ対応組織
研修・教育方法	講義(ミニ演習課題を含む)
時間の目安	90分（演習課題を含む） （講義：70分　演習課題：20分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】2. セキュリティ基準の策定
その他	

8.4. コマシラバス（6/8）

研修コース名	セキュリティガイドライン
回数	第 6 回
テーマ	企業活動一般のセキュリティ規定
学習目標	・ セキュリティの観点から社内規定を策定する知識を修得し、応用する。 ・ 策定した社内規定と、セキュリティポリシの整合性を確認する知識を修得し、応用する。
学習内容	(1) 企業活動一般のセキュリティ規定 雇用契約/職務規定 機密管理規定 機密区分、機密保護 脅迫、恐喝、侵入、窃盗、産業スパイ、無線電波傍受 横領、背任 ID、パスワードの流出、データ保護 文書管理規定 情報管理規定 プライバシポリシ セキュリティ教育の規定 罰則の規定 対外説明の規定 例外の規定 規則変更の規定 承認手続き　など (2) セキュリティポリシとの整合性
研修・教育方法	講義(ミニ演習課題を含む)
時間の目安	90 分（演習課題を含む） （講義：70 分　演習課題：20 分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】2. セキュリティ基準の策定
その他	

8.4. コマシラバス（7/8）

研修コース名	セキュリティガイドライン
回数	第 7 回
テーマ	情報システムのセキュリティ規定
学習目標	・ セキュリティの観点から情報システム運用やネットワーク利用、セキュリティ管理などの情報システムのセキュリティ規定などを策定する知識を修得し、応用する。
学習内容	(1) 情報システムのセキュリティ規定 インターネット利用規定 インターネット向け公開サーバ設置および管理規定 社内サーバおよびクライアントの設置および管理規定 リモートアクセスポイントの設置および管理規定 アプリケーションインストール規定 データ管理の規定 コンピュータウイルス対策運用規定 情報セキュリティ監査の規定 情報システム管理者の規定 システム開発の規定 (2) セキュリティポリシとの整合性
研修・教育方法	講義(ミニ演習課題を含む)
時間の目安	90 分（演習課題を含む） （講義：70 分　演習課題：20 分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】2. セキュリティ基準の策定
その他	

8.4. コマシラバス（8/8）

研修コース名	セキュリティガイドライン
回数	第８回
テーマ	情報セキュリティマネジメントシステム
学習目標	・ 緊急時・災害時の対応に関するガイドラインを理解し、応用できる。 ・ 情報セキュリティマネジメントシステムの仕組みを理解し、応用できる。 ・ セキュリティ機関の役割を理解し、応用できる。
学習内容	(1) 緊急時・災害時の規定 緊急時対応の規定 災害時対応の規定 他のガイドラインとの整合性 (2) 情報セキュリティマネジメンシステム 目的 仕組み（維持・改善） ISMS 適合評価制度 ISMS 認定 ISO/IEC 17799 （IJS Q 27002） ISO/IEC 27001 (3) セキュリティ機関 役割 IPA セキュリティセンター JPCERT/CC
研修・教育方法	講義(ミニ演習課題を含む)
時間の目安	90 分（演習課題を含む） （講義：70 分 演習課題：20 分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】2. セキュリティ基準の策定
その他	

9.（S03）セキュリティガイドライン上級

対応する機能役割定義

大項目		中項目	
大No.	大項目名（タスク）	No.	中項目名
140	セキュリティ	1	セキュリティ方針の策定
		2	セキュリティ基準の策定
		4	セキュリティの見直し

9.1. 科目シラバス

研修コースコード	14－S－03
研修コース名	セキュリティガイドライン上級
研修ロードマップ	(14)セキュリティ
知識項目(BOK)分野	テクノロジ系　－　ストラテジ
知識項目(BOK)分類	【大分類】4. 技術要素 【中分類】11. セキュリティ
レベル区分	セキュリティのレベル 4 を目指す者
受講前提	セキュリティに関してレベル 3 程度以上のもの
科目概要	・ 「セキュリティガイドライン」の後続コースとして、セキュリティ関連法規およびセキュリティガイドラインの理解を深め、自社のセキュリティ基本方針やセキュリティ対策基準に基づき、現状の課題を解決するセキュリティの各種規定の策定について、高度かつ専門的な知識の修得を目的とする。 ・ 情報セキュリティ基本方針や情報セキュリティ対策基準、各種セキュリティに関する規定の策定に関連し、応用できる知識を深める。
学習目標概要	・ セキュリティ関連法規およびセキュリティガイドラインの知識を修得し、応用できる。 ・ 情報セキュリティ基本方針を策定および評価することができる。 ・ 情報セキュリティ対策基準を策定および評価することができる。 ・ 情報セキュリティポリシに基づいたセキュリティ関連の各種規定を策定および評価することができる。
研修・教育方法	ワークショップ(演習課題を含む)
修得スキルの評価方法	以下の状況等を総合的に判断して評価する。 受講前・受講後の知識確認テスト 定量アンケート 受講レポート 演習課題の取り組み状況　など
カリキュラム構成	1 コマ 180 分　×　6 コマ （クラスルーム：標準日数 3 日）
情報処理技術者試験	情報セキュリティスペシャリスト試験の一部
備考	（次のＢＯＫも対応） 【大分類】9. 企業と法務 【中分類】23. 法務

9.2. 知識項目対応表

◎＝主項目として扱う、○＝関連項目として扱う

共通キャリア・スキルフレームワーク					対象項目
分野	大分類		中分類		
テクノロジ系	1	基礎理論	1	基礎理論	
			2	アルゴリズムとプログラミング	
	2	コンピュータシステム	3	コンピュータ構成要素	
			4	システム構成要素	
			5	ソフトウェア	
			6	ハードウェア	
	3	技術要素	7	ヒューマンインターフェース	
			8	マルチメディア	
			9	データベース	
			10	ネットワーク	
			11	セキュリティ	◎
	4	開発技術	12	システム開発技術	
			13	ソフトウェア開発技術管理	
マネジメント系	5	プロジェクトマネジメント	14	プロジェクトマネジメント	
	6	サービスマネジメント	15	サービスマネジメント	
			16	システム監査	
ストラテジ系	7	システム戦略	17	システム戦略	
			18	システム企画	
	8	経営戦略	19	経営戦略マネジメント	
			20	技術戦略マネジメント	
			21	ビジネスインダストリ	
	9	企業と法務	22	企業活動	
			23	法務	○

9.3. コマタイトル一覧

回数	テーマ	学習目標	参照先
第１回	情報資産の評価と リスクの認識	・ 企業の情報資産を識別し、資産の重要度や致命度を評価し、整理することができる。 ・ 社会における一般的なリスクの情報を幅広く収集し、整理することができる。	P．98
第２回	リスクの識別と対策	・ 情報資産のリスクを識別し、発生しうる時期や場所、その原因や要因等について整理することができる。 ・ 識別されたリスクに対して対策を検討し、決定することができる。	P．99
第３回	リスク評価	・ 整理されたリスクの発生確率やその損害額を算定することができる。 ・ 各リスクに対して、リスク対策コストを算定し、リスク発生時の損害額と対策コストのバランスを考慮することができる。 ・ 残存リスクを評価することができる。	P．100
第４回	情報セキュリティ 基本方針	・ セキュリティ対策の目的、適用範囲、達成レベル、対策基準の方針を策定できる。 ・ 情報セキュリティの責任者、経営者・従業員の遵守事項、組織または実施体制、運用、罰則、公開、見直しになど、基本方針に盛り込むことができる。	P．101
第５回	企業活動一般の セキュリティ規定	・ 企業の規則体系に合わせ、セキュリティの観点から社内規定を策定することができる。 ・ 策定した社内規定と、セキュリティポリシの整合性を確認することができる。	P．102
第６回	情報システムの セキュリティ規定	・ 企業の規則体系に合わせ、セキュリティの観点から情報システム運用規定、ネットワーク利用規定、業務規定、セキュリティ管理規定などを策定することができる。 ・ 策定した情報システム規定と、セキュリティポリシの整合性を確認することができる。	P．103

9.4. コマシラバス（1/6）

研修コース名	セキュリティガイドライン上級
回数	第 1 回
テーマ	情報資産の評価とリスクの認識
学習目標	・ 企業の情報資産を識別し、資産の重要度や致命度を評価し、整理することができる。 ・ 社会における一般的なリスクの情報を幅広く収集し、整理することができる。
学習内容	――講義―― (1) 情報資産 物理的資産、ソフトウェア資産、データ資産　など (2) 情報セキュリティ管理 考え方の整理、管理対象　など (3) 脅威 物理的脅威、技術的脅威、人的脅威　など (4) 脆弱性 欠陥、不徹底、未整備、不備　など ――ワークショップ―― ケースの (1) 情報資産のリストアップ (2) 脅威と脆弱性のリストアップ
研修・教育方法	ワークショップ（講義を含む・クラスルーム）
時間の目安	180 分（演習課題を含む） （講義：60 分　　演習課題：120 分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】1. セキュリティ方針の策定
その他	ケースに使用するモデル企業は、文書または図解で提示し、第 1 回から第 6 回まで、通しで利用できるものが望ましい。

9.4. コマシラバス（2/6）

研修コース名	セキュリティガイドライン上級
回数	第２回
テーマ	リスクの識別と対策
学習目標	・ 情報資産のリスクが識別し、発生しうる時期や場所、その原因や要因等について整理することができる。 ・ 識別されたリスクに対して対策を検討し、決定することができる。
学習内容	――講義―― (1) リスクの識別 リスクの存在箇所 リスクの発生時期 リスクの原因 (2) リスク対策 抑止、予防、検知、回復 最適化(低減)、回避、移転、保有 物理的対策、人的対策、管理的対策、技術的対策 (3) リスクの調査 現状のリスク調査　など ――ワークショップ―― ケースの (1) リスクの識別 (2) リスク対策 (3) リスクの調査
研修・教育方法	ワークショップ（講義を含む・クラスルーム）
時間の目安	180 分（演習課題を含む） （講義：60 分　　演習課題：120 分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】1. セキュリティ方針の策定
その他	ケースに使用するモデル企業は、文書または図解で提示し、第１回から第６回まで、通しで利用できるものが望ましい。

9.4. コマシラバス（3/6）

研修コース名	セキュリティガイドライン上級
回数	第3回
テーマ	リスク評価
学習目標	・ 整理されたリスクの発生確率やその損害額を算定することができる。 ・ 各リスクに対して、リスク対策とコストを算定し、リスク発生時の損害額と対策コストのバランスを考慮することができる。 ・ 残存リスクを評価することができる。
学習内容	――講義―― (1). リスク算定 定量的分析と定性的分析 発現確率 影響度 リスク値の計算 (2) リスク評価 損害コスト リスク軽減の対策コスト 残存リスク リスクの許容 優先順位　など ――ワークショップ―― (1). リスク算定 (2) リスク評価
研修・教育方法	ワークショップ（講義を含む・クラスルーム）
時間の目安	180分（演習課題を含む） （講義：60分　　演習課題：120分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】1. セキュリティ方針の策定
その他	ケースに使用するモデル企業は、文書または図解で提示し、第1回から第6回まで、通しで利用できるものが望ましい。

9.4. コマシラバス（4/6）

研修コース名	セキュリティガイドライン上級
回数	第4回
テーマ	情報セキュリティ基本方針
学習目標	・ リスク評価の結果に基づき、セキュリティ対策の目的、適用範囲、達成レベル、対策基準の方針を策定できる。 ・ 情報セキュリティの責任者、経営者・従業員の遵守事項、組織または実施体制、運用、罰則、公開、見直しになど、基本方針に盛り込むことができる。
学習内容	ーー講義ーー (1) 情報セキュリティ基本方針 目的 範囲 達成レベル 情報セキュリティの責任者 経営者/従業員の遵守事項 情報セキュリティ活動の実施体制　など (2) 方針のテンプレート (3) 承認手続き ーーワークショップーー (1) 情報セキュリティ基本方針の策定
研修・教育方法	ワークショップ（講義を含む・クラスルーム）
時間の目安	180分（演習課題を含む） （講義：60分　　演習課題：120分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】1. セキュリティ方針の策定
その他	ケースに使用するモデル企業は、文書または図解で提示し、第1回から第6回まで、通しで利用できるものが望ましい。

9.4. コマシラバス（5/6）

研修コース名	セキュリティガイドライン上級
回数	第5回
テーマ	企業活動一般のセキュリティ規定
学習目標	・ 企業の規則体系に合わせ、セキュリティの観点から社内規定を策定することができる。 ・ 策定した社内規定と、セキュリティポリシの整合性を確認することができる。
学習内容	――講義―― (1) 企業活動一般のセキュリティ規定 雇用契約/職務規定 機密/文書/情報管理規定 セキュリティ教育の規定 罰則の規定 対外説明の規定 例外の規定 規則変更の規定 承認手続き　など ――ワークショップ―― (1) 企業一般のセキュリティ規定
研修・教育方法	ワークショップ（講義を含む・クラスルーム）
時間の目安	180分（演習課題を含む） （講義：60分　　演習課題：120分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】2. セキュリティ基準の策定
その他	ケースに使用するモデル企業は、文書または図解で提示し、第1回から第6回まで、通しで利用できるものが望ましい。

9.4. コマシラバス（6/6）

研修コース名	情報セキュリティポリシ策定上級
回数	第6回
テーマ	情報システムのセキュリティ規定
学習目標	・ 企業の規則体系に合わせ、セキュリティの観点から情報システム運用規定、ネットワーク利用規定、業務規定、セキュリティ管理規定などを策定することができる。 ・ 策定した情報システム規定と、セキュリティポリシの整合性を確認することができる。
学習内容	――講義―― (1) 情報システムのセキュリティ規定 インターネット利用規定 インターネット向け公開サーバ設置および管理規定 社内サーバおよびクライアントの設置および管理規定 リモートアクセスポイントの設置および管理規定 アプリケーションインストール規定 データ管理の規定 コンピュータウイルス対策運用規定 緊急時対応の規定 災害時対応の規定 情報セキュリティ監査の規定 情報システム管理者の規定 システム開発の規定 ――ワークショップ―― (1) 情報システムのセキュリティ規定
研修・教育方法	ワークショップ（講義を含む・クラスルーム）
時間の目安	180分（演習課題を含む） （講義：60分　　演習課題：120分）
対応する機能・役割定義	【大分類】14. セキュリティ 【中分類】2. セキュリティ基準の策定
その他	ケースに使用するモデル企業は、文書または図解で提示し、第1回から第6回まで、通しで利用できるものが望ましい。