情報システムユーザースキル標準
モデルカリキュラム

(11)セキュリティ編

Ver.2.3

2010 年 3 月

独立行政法人情報処理推進機構(IPA)

（表紙うら）

＜**も　く　じ**＞

知識項目対応表

本編は、共通キャリア・スキルフレームワークの対象項目のうち、セキュリティ知識項目対応表（表１）に「◎＝主項目、○＝関連項目」としてマークした項目を扱っています。

（表１）セキュリティ知識対応項目表

共通キャリア・スキルフレームワーク					対応項目
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	○

シラバス設定コース

本編は、シラバス設定コース一覧表（表２)に記載されたコースのシラバスを掲載しています。

（表２）シラバス設定コース一覧表

コースレベル	番号	コース名	研修方法	コースのコマ数	記載ページ
テクノロジ系					
初級	11-T-01	セキュリティ技術初級	講義（含ミニ演習課題）	90 分×4（1 日間）	P.4
中級	11-T-02	セキュリティ技術中級	講義（含ミニ演習課題）	90 分×8（2 日間）	P.10
上級	11-T-03	セキュリティ技術上級	ワークショップ（含講義）	180 分×6（3 日間）	P.20
マネジメント系					
初級	11-M-01	セキュリティ管理初級	講義（含ミニ演習課題）	90 分×4（1 日間）	P.28
中級	11-M-02	セキュリティ管理中級	講義（含ミニ演習課題）	90 分×8（2 日間）	P.34
上級	11-M-03	セキュリティ管理上級	ワークショップ（含講義）	180 分×6（3 日間）	P.44
ストラテジ系					
初級	11-S-01	情報セキュリティポリシ	講義（含ミニ演習課題）	90 分×4（1 日間）	P.52
中級	11-S-01	セキュリティガイドライン	講義（含ミニ演習課題）	90 分×8（2 日間）	P.58
上級	11-S-03	セキュリティガイドライン上級	ワークショップ（含講義）	180 分×6（3 日間）	P.68

シラバス　1.（11-T-01）セキュリティ技術初級

1.1. コースシラバス

コースコード	11-T-01
コース名	セキュリティ技術初級
講座分類	初級
コース分野	テクノロジ
研修方法	講義（ミニ演習課題を含む）
受講前提	セキュリティに関して入門的な知識を修得していること
コース概要	・ 情報セキュリティについて、脆弱性や脅威を分析・評価し、それらのリスクの回避策や防止策に関する基本的な技術を学習する。 ・ 情報システム基盤や情報システム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または支援する基本的な方法について学習する。 ・ 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に実施できるセキュリティ技術の基礎知識を学習する。
コース目標	・ 上司の指導の下または一定であれば独力でセキュリティ要件を定義し、セキュリティ実装の計画から設計、構築、移行、運用するための技術的な基礎知識を修得する。 ・ セキュリティの観点から情報システム基盤や情報システム等の維持管理するための基本的な知識を修得する。 ・ 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修得する。
コースに対応する情報処理技術者試験	基本情報技術者試験 （セキュリティ領域）
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

コースのコマ構成		
回数	**コマタイトル**	**コマに対応する機能・役割定義**
第１回	暗号化技術と公開鍵基盤	140-01．セキュリティ方針の策定 140-03．セキュリティの分析
第２回	認証技術とセキュリティ技術の評価	140-01．セキュリティ方針の策定 140-03．セキュリティの分析
第３回	ネットワークのセキュリティ	140-01．セキュリティ方針の策定 140-03．セキュリティの分析
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	140-01．セキュリティ方針の策定 140-03．セキュリティの分析
備考		
・ ミニ演習課題は、基本情報技術者試験問題レベルが適切である。		

1.2. コマシラバス（1/4）

回数	第 1 回
コマタイトル	暗号化技術と公開鍵基盤
コマの学習目標	・ 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。
コマの学習内容	(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（Data Encryption Standard：データ暗号化標準） RSA（Rivest Shamir Adleman：人の名前）　など (3) 公開鍵基盤(PKI) 公開鍵証明書 CA（Certificate Authority：認証局） GPKI（Government Public Key Infrastructure ：政府認証基盤） BCA（Bridge Certificate Authority：ブリッジ認証局） SSL（Secure Socket Layer ：情報を暗号化した送受信プロトコル） など
時間の目安	90 分 （講義：80 分、ミニ演習課題：10 分）
その他	

1.2. コマシラバス（2/4）

回数	第 2 回
コマタイトル	認証技術とセキュリティ技術の評価
コマの学習目標	・ 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。
コマの学習内容	(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（Integrated Circuit：集積回路）カード PIN（Personal identification number ：個人認証用のパスワード）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 ISO（International Organization for Standardization ：国際標準化機構） IEC（International Electrotechnical Commission ：国際電気標準会議）
時間の目安	90 分 （講義：80 分、ミニ演習課題：10 分）
その他	

1.2. コマシラバス（3/4）

回数	第3回
コマタイトル	ネットワークのセキュリティ
コマの学習目標	・ 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。
コマの学習内容	(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（Internet Protocol ：インターネットプロトコル）マスカレード VPN（Virtual Private Network：仮想私設網） WEP（Wired Equivalent Privacy：無線通信暗号化技術） WPA（Wi-Fi Protected Access ：無線 LAN の暗号化方式の規格）など
時間の目安	90 分 （講義：80 分、ミニ演習課題：10 分）
その他	

1.2. コマシラバス（4/4）

回数	第４回
コマタイトル	データベースおよびアプリケーションのセキュリティ
コマの学習目標	・ 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。
コマの学習内容	(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 バッファオーバーフロー攻撃 クロスサイトスクリプティング攻撃　など
時間の目安	90 分 （講義：80 分、ミニ演習課題：10 分）
その他	

シラバス　2.（11-T-02）**セキュリティ技術中級**

2.1. コースシラバス

コースコード	11-T-02
コース名	セキュリティ技術中級
講座分類	中級
コース分野	テクノロジ
研修方法	講義（ミニ演習課題を含む）
受講前提	セキュリティに関して基本的な知識を修得していること
コース概要	・ 「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ついて、脆弱性や脅威を分析・評価し、それらのリスクの回避策や防止策に関する応用的な技術を学習する。 ・ 情報システム基盤や情報システム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または支援する応用的な方法について学習する。 ・ 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に実施できるセキュリティ技術の応用知識を学習する。
コース目標	・ セキュリティ要件を定義し、独力で実践するための技術的な知識を修得する。 ・ セキュリティ実装の計画から設計、構築、移行、運用、維持管理までを独力で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。
コースに対応する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）
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

コースのコマ構成		
回数	**コマタイトル**	**コマに対応する機能・役割定義**
第1回	脅威と脆弱性	140-01. セキュリティ方針の策定 140-03. セキュリティの分析
第2回	暗号化技術と公開鍵基盤	140-01. セキュリティ方針の策定 140-03. セキュリティの分析
第3回	認証技術	140-01. セキュリティ方針の策定 140-03. セキュリティの分析
第4回	セキュリティ技術の評価	140-01. セキュリティ方針の策定 140-03. セキュリティの分析
第5回	セキュア OS と セキュアプログラミング	140-01. セキュリティ方針の策定 140-03. セキュリティの分析
第6回	ネットワークセキュリティ	140-01. セキュリティ方針の策定 140-03. セキュリティの分析
第7回	データベースセキュリティ	140-01. セキュリティ方針の策定 140-03. セキュリティの分析
第8回	Web アプリケーションセキュリティ	140-01. セキュリティ方針の策定 140-03. セキュリティの分析
備考		
・ ミニ演習課題は、応用情報技術者試験問題レベルが適切である。		

2.2. コマシラバス（1/8）

回数	第 1 回
コマタイトル	脅威と脆弱性
コマの学習目標	・ 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。
コマの学習内容	(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
時間の目安	90 分 （講義：80 分、ミニ演習課題：10 分）
その他	

2.2. コマシラバス（2/8）

回数	第 2 回
コマタイトル	暗号化技術と公開鍵基盤
コマの学習目標	・ 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、これらの知識をセキュリティ対策に応用する。
コマの学習内容	(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（Secure Multipurpose Internet Mail Extensions：電子メールの暗号化方式の標準） PGP（Pretty Good Privacy：暗号化ソフトウェア）など (2) 公開鍵基盤 公開鍵証明書 CA GPKI BCA SSL SET（Secure Electronic Transaction：インターネット上で安全にクレジット・カード決済を行うためのプロトコル） など
時間の目安	90 分 （講義：80 分、ミニ演習課題：10 分）
その他	

2.2. コマシラバス（3/8）

回数	第 3 回
コマタイトル	認証技術
コマの学習目標	・ 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理解し、これらの知識をセキュリティ対策に応用する。
コマの学習内容	(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（オープン・ネットワーク用の認証と暗号化システム）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
時間の目安	90 分 （講義：80 分、ミニ演習課題：10 分）
その他	

2.2. コマシラバス（4/8）

回数	第４回
コマタイトル	セキュリティの評価
コマの学習目標	・ 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、これらの知識をセキュリティ対策に応用する。
コマの学習内容	(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：セキュリティの国際基準） ST（Security Target：セキュリティ設計仕様書） CEM （Common Evaluation Methodology ：共通評価方法論） EAL（Evaluation Assurance Level：評価保証レベル） など
時間の目安	90 分 （講義：80 分、ミニ演習課題：10 分）
その他	

2.2. コマシラバス（5/8）

回数	第５回
コマタイトル	セキュア OS とセキュアプログラミング
コマの学習目標	・ 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、効果などの知識を理解し、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理解し、これらの知識をセキュリティ対策に応用する。
コマの学習内容	(1) セキュア OS MAC（Message Authentication Code：データ認証方式） 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
時間の目安	90 分 （講義：80 分、ミニ演習課題：10 分）
その他	

2.2. コマシラバス（6/8）

回数	第6回
コマタイトル	ネットワークセキュリティ
コマの学習目標	・ 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、効果などの知識を理解し、これらの知識をセキュリティ対策に応用する。
コマの学習内容	(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（Service Set Identifier ：無線 LAN のアクセスポイントを識別するための名前） WEP WPA MAC アドレス フィルタリング ハニーポット　など
時間の目安	90 分 （講義：80 分、ミニ演習課題：10 分）
その他	

2.2. コマシラバス（7/8）

回数	第 7 回
コマタイトル	データベースセキュリティ
コマの学習目標	・ 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、効果などの知識を理解し、これらの知識をセキュリティ対策に応用する。
コマの学習内容	(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（Structured Query Language ：データベースを操作するための共通言語） インジェクション　など
時間の目安	90 分 （講義：80 分　演習課題：10 分）
その他	

2.2. コマシラバス（8/8）

回数	第 8 回
コマタイトル	Web アプリケーションセキュリティ
コマの学習目標	・ 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、効果などの知識を理解し、これらの知識をセキュリティ対策に応用する。
コマの学習内容	(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
時間の目安	90 分 （講義：80 分　演習課題：10 分）
その他	

シラバス　3.（11-T-03）セキュリティ技術上級

3.1. コースシラバス

コースコード	11-T-03
コース名	セキュリティ技術上級
講座分類	上級
コース分野	テクノロジ
研修方法	ワークショップ（講義を含む）
受講前提	セキュリティに関して実践的な知識を修得していること
コース概要	・ 「セキュリティ技術中級」の後続コースとして、情報セキュリティについて、脆弱性や脅威を分析・評価し、それらのリスクの回避策や防止策に関する高度な技術を学習する。 ・ 情報システム基盤や情報システム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または支援する高度な方法について学習する。 ・ 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に実施できるセキュリティ技術の高度な知識を学習する。
コース目標	・ セキュリティ要件を定義し、実践するための高度な知識の学習を通じて、セキュリティに関する技術を指導する知識を修得する。 ・ 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実践的技術の学習を通じて、後進育成できる知識を修得する。 ・ 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できるスキルを修得する。
コースに対応する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
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

コースのコマ構成		
回数	**コマタイトル**	**コマに対応する機能・役割定義**
第１回	情報システムの脆弱性・脅威分析	140-01．セキュリティ方針の策定 140-03．セキュリティの分析
第２回	セキュリティ要件定義	140-01．セキュリティ方針の策定 140-03．セキュリティの分析
第３回	セキュリティ機能の設計	140-01．セキュリティ方針の策定 140-03．セキュリティの分析
第４回	セキュリティ実装技術 (セキュアプログラミング)	140-01．セキュリティ方針の策定 140-03．セキュリティの分析
第５回	セキュリティ実装技術 （ネットワーク）	140-01．セキュリティ方針の策定 140-02．セキュリティ基準の策定
第６回	セキュリティ機能の 本番移行	140-01．セキュリティ方針の策定 140-02．セキュリティ基準の策定
備考		
・ 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。		

3.2. コマシラバス（1/6）

回数	第 1 回
コマタイトル	情報システムの脆弱性・脅威分析
コマの学習目標	・ 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。
コマの学習内容	――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
時間の目安	180 分 （講義：60 分、ワークショップ：120 分）
その他	

3.2. コマシラバス（2/6）

回数	第 2 回
コマタイトル	セキュリティ要件定義
コマの学習目標	・ 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。
コマの学習内容	――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
時間の目安	180 分 （講義：60 分、ワークショップ：120 分）
その他	

3.2. コマシラバス（3/6）

回数	第3回
コマタイトル	セキュリティ機能の設計
コマの学習目標	・ 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。
コマの学習内容	――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
時間の目安	180 分 （講義：60 分、ワークショップ：120 分）
その他	

3.2. コマシラバス（4/6）

回数	第４回
コマタイトル	セキュリティ実装技術（セキュアプログラミング）
コマの学習目標	・ 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。
コマの学習内容	――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
時間の目安	180 分 （講義：60 分、ワークショップ：120 分）
その他	

3.2. コマシラバス（5/6）

回数	第５回
コマタイトル	セキュリティ実装技術（ネットワーク）
コマの学習目標	・ 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。
コマの学習内容	――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（Virtual LAN：バーチャル LAN） 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
時間の目安	180 分 （講義：60 分、ワークショップ：120 分）
その他	

3.2. コマシラバス（6/6）

回数	第 6 回
コマタイトル	セキュリティ機能の本番移行
コマの学習目標	・ 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。
コマの学習内容	――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
時間の目安	180 分 （講義：60 分、ワークショップ：120 分）
その他	

シラバス　4.（11-M-01）セキュリティ管理初級

4.1. コースシラバス

コースコード	11-M-01
コース名	セキュリティ管理初級
講座分類	初級
コース分野	マネジメント
研修方法	講義（ミニ演習課題を含む）
受講前提	セキュリティに関して入門的な知識を修得していること
コース概要	・ 情報セキュリティマネジメントについて、上司の指導の下、企画・導入･運用を含むセキュリティ業務全般の管理ができる基本的な知識を学習する。 ・ 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に関連する知識を学習する。
コース目標	・ 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知識を修得する。 ・ 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知識を修得する。 ・ 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知識を修得する。 ・ 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知識を修得する。
コースに対応する情報処理技術者試験	基本情報技術者試験 （セキュリティ）
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

コースのコマ構成		
回数	**コマタイトル**	**コマに対応する機能・役割定義**
第1回	セキュリティ技術	140-03. セキュリティの分析
第2回	情報セキュリティ対策と技術情報	140-03. セキュリティの分析
第3回	セキュリティ事故の初動処理	140-03. セキュリティの分析
第4回	セキュリティ対策の見直し	140-01. セキュリティ方針の策定 140-03. セキュリティの分析
備考		
・ ミニ演習課題は、基本情報技術者試験問題レベルが適切である。 ・ 次の共通キャリア・スキルフレームワークにも対応する。 【大項目】9. 企業と法務－【中項目】23. 法務		

4.2. コマシラバス（1/4）

回数	第1回
コマタイトル	セキュリティ技術
コマの学習目標	・ 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。
コマの学習内容	(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 認証サーバ、NAT、IP マスカレード VPN、WEP、WPA、IDS、IPS (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
時間の目安	90 分 （講義：80 分、ミニ演習課題：10 分）
その他	

4.2. コマシラバス（2/4）

回数	第 2 回
コマタイトル	情報セキュリティ対策と技術情報
コマの学習目標	・ 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。
コマの学習内容	(1) 人的セキュリティ対策 情報セキュリティポリシ 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（Reliability Availability Serviceability Integrity Security：システムの信頼性評価指標） 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 など
時間の目安	90 分 （講義：80 分、ミニ演習課題：10 分）
その他	

4.2. コマシラバス（3/4）

回数	第3回
コマタイトル	セキュリティ事故の初動処理
コマの学習目標	・ 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。
コマの学習内容	(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
時間の目安	90 分 （講義：80 分、ミニ演習課題：10 分）
その他	

4.2. コマシラバス（4/4）

回数	第４回
コマタイトル	セキュリティ対策の見直し
コマの学習目標	・ 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。
コマの学習内容	(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
時間の目安	90 分 （講義：80 分、ミニ演習課題：10 分）
その他	

シラバス　5.（11-M-02）セキュリティ管理中級

5.1. コースシラバス

コースコード	11-M-02
コース名	セキュリティ管理中級
講座分類	中級
コース分野	マネジメント
研修方法	講義（ミニ演習課題を含む）
受講前提	セキュリティに関して基本的な知識を修得していること
コース概要	・ 「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を学習する。 ・ 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できる知識を学習する。
コース目標	・ 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業務に適用できる知識を修得する。 ・ 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知識を修得する。 ・ 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知識を修得する。 ・ 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知識を修得する。
コースに対応する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）
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

コースのコマ構成		
回数	**コマタイトル**	**コマに対応する機能・役割定義**
第１回	情報セキュリティの技術	140-03．セキュリティの分析
第２回	情報セキュリティ対策	140-03．セキュリティの分析
第３回	セキュリティ実装技術	140-03．セキュリティの分析
第４回	セキュリティ事故の初動処理	140-03．セキュリティの分析
第５回	セキュリティ事故の分析と復旧	140-03．セキュリティの分析
第６回	セキュリティの評価（評価基準）	140-03．セキュリティの分析
第７回	問題点の整理と分析	140-04．セキュリティの見直し
第８回	セキュリティ対策の更新	140-04．セキュリティの見直し
備考		
・ ミニ演習課題は、応用情報技術者試験問題レベルが適切である。 ・ 次の共通キャリア・スキルフレームワークにも対応する。 【大項目】9．企業と法務－【中項目】23．法務		

5.2. コマシラバス（1/8）

回数	第 1 回
コマタイトル	情報セキュリティの技術
コマの学習目標	・ 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。
コマの学習内容	(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（Pretty Good Privacy ：暗号技術を利用するアプリケーション・ソフト　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
時間の目安	90 分 （講義：80 分、ミニ演習課題：10 分）
その他	

5.2. コマシラバス（2/8）

回数	第 2 回
コマタイトル	情報セキュリティ対策
コマの学習目標	・ 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。
コマの学習内容	(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（Remote Access Service ：ダイヤルアップ接続通信機器）技術 耐震耐火設備、二重化技術 UPS（uninterruptible power supply：無停電装置） 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
時間の目安	90 分 （講義：80 分、ミニ演習課題：10 分）
その他	

5.2. コマシラバス（3/8）

回数	第3回
コマタイトル	セキュリティ実装技術
コマの学習目標	・ 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。
コマの学習内容	(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、IP マスカレード NAT（Network Address Translation ：IP アドレス変換方式）、 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
時間の目安	90 分 （講義：80 分、ミニ演習課題：10 分）
その他	

5.2. コマシラバス（4/8）

回数	第４回
コマタイトル	セキュリティ事故の初動処理
コマの学習目標	・ 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。
コマの学習内容	(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
時間の目安	90 分 （講義：80 分、ミニ演習課題：10 分）
その他	

5.2. コマシラバス（5/8）

回数	第５回
コマタイトル	セキュリティ事故の分析と復旧
コマの学習目標	・ 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。
コマの学習内容	(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
時間の目安	90 分 （講義：80 分、ミニ演習課題：10 分）
その他	

5.2. コマシラバス（6/8）

回数	第6回
コマタイトル	セキュリティの評価
コマの学習目標	・ 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。
コマの学習内容	(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、EAL
時間の目安	90 分 （講義：80 分、ミニ演習課題：10 分）
その他	

5.2. コマシラバス（7/8）

回数	第 7 回
コマタイトル	新たなリスクの整理と分析
コマの学習目標	・ 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。
コマの学習内容	(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
時間の目安	90 分 （講義：80 分、ミニ演習課題：10 分）
その他	

5.2. コマシラバス（8/8）

回数	第 8 回
コマタイトル	情報セキュリティ対策の更新
コマの学習目標	・ 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。
コマの学習内容	(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
時間の目安	90 分 （講義：80 分、ミニ演習課題：10 分）
その他	

シラバス　6.（11-M-03）セキュリティ管理上級

6.1. コースシラバス

コースコード	11-M-03
コース名	セキュリティ管理上級
講座分類	上級
コース分野	マネジメント
研修方法	ワークショップ（講義を含む）
受講前提	セキュリティに関して実践的知識を有するもの
コース概要	・ 「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を学習する。 ・ 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高度な内容を学習する。
コース目標	・ 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学習を通じて、セキュリティ管理に関する指導する知識を修得する。 ・ セキュリティ事故を検知した際、緊急時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、さらに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学習を通じて、後進育成できる知識を修得する。 ・ 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できるスキルを修得する。
コースに対応する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
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

コースのコマ構成		
回数	**コマタイトル**	**コマに対応する機能・役割定義**
第1回	情報セキュリティ管理	140-01. セキュリティ方針の策定
第2回	事故対応	140-03. セキュリティの分析
第3回	セキュリティの評価	140-03. セキュリティの分析
第4回	最新情報と問題点の分析と評価	140-04. セキュリティの見直し
第5回	新たなリスクの整理と分析	140-04. セキュリティの見直し
第6回	セキュリティポリシの更新	140-04. セキュリティの見直し

備考

・ 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。
・ 次の共通キャリア・スキルフレームワークにも対応する。
【大項目】9. 企業と法務－【中項目】23. 法務

6.2. コマシラバス（1/6）

回数	第 1 回
コマタイトル	情報セキュリティ管理
コマの学習目標	・ 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。
コマの学習内容	――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
時間の目安	180 分 （講義：60 分、ワークショップ：120 分）
その他	

6.2. コマシラバス（2/6）

回数	第 2 回
コマタイトル	事故対応
コマの学習目標	・ 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。
コマの学習内容	――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、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　など
時間の目安	180 分 （講義：60 分、ワークショップ：120 分）
その他	

6.2. コマシラバス（3/6）

回数	第3回
コマタイトル	セキュリティの評価
コマの学習目標	・ 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。
コマの学習内容	――講義―― (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 ――ワークショップ―― (1) セキュリティ評価 (2) 見直し事項の整理
時間の目安	180 分 （講義：60 分、ワークショップ：120 分）
その他	

6.2. コマシラバス（4/6）

回数	第４回
コマタイトル	最新情報と問題点の分析と評価
コマの学習目標	・ 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。
コマの学習内容	――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
時間の目安	180 分 （講義：60 分、ワークショップ：120 分）
その他	

6.2. コマシラバス（5/6）

回数	第５回
コマタイトル	新たなリスクの整理と分析
コマの学習目標	・ 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。
コマの学習内容	――講義―― (1) 最新情報の収集 最近のセキュリティ事例（JPCERT/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
時間の目安	180 分 （講義：60 分、ワークショップ：120 分）
その他	JPCERT/CC（Japan Computer Emergency Response Team /Coordination Center：JPCERT コーディネーションセンター) IPA（Information-technology Promotion Agency, Japan ：独立行政法人情報処理推進機構

6.2. コマシラバス（6/6）

回数	第 6 回
コマタイトル	セキュリティポリシの更新
コマの学習目標	・ 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。
コマの学習内容	――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
時間の目安	180 分 （講義：60 分、ワークショップ：120 分）
その他	

シラバス　7.（11-S-01）情報セキュリティポリシ

7.1. コースシラバス

コースコード	11-S-01
コース名	情報セキュリティポリシ
講座分類	初級
コース分野	ストラテジ
研修方法	講義(ミニ演習課題を含む)
受講前提	セキュリティに関して入門的な知識を修得していること
コース概要	・ 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ポリシに関する作業ができる基本的な知識を学習する。 ・ 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。
コース目標	・ 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目的、考え方などの知識を修得する。 ・ 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などの知識を修得する。 ・ 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などの知識を修得する。
コースに対応する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
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

コースのコマ構成		
回数	**コマタイトル**	**コマに対応する機能・役割定義**
第１回	情報セキュリティ管理と情報資産	140-01．セキュリティ方針の策定
第２回	リスク分析と評価	140-01．セキュリティ方針の策定
第３回	情報セキュリティポリシ	140-02．セキュリティ基準の策定
第４回	セキュリティに関する社内規定	140-02．セキュリティ基準の策定

備考

・ ミニ演習課題は、基本情報技術者試験問題レベルが適切である。

・ 次の共通キャリア・スキルフレームワークにも対応する。

【大項目】9．企業と法務－【中項目】23．法務

7.2. コマシラバス（1/4）

回数	第 1 回
コマタイトル	情報セキュリティ管理と情報資産
コマの学習目標	・ 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。
コマの学習内容	(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
時間の目安	90 分 （講義：80 分、ミニ演習課題：10 分）
その他	

7.2. コマシラバス（2/4）

回数	第 2 回
コマタイトル	リスク分析と評価
コマの学習目標	・ 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。
コマの学習内容	(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 (3) 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
時間の目安	90 分 （講義：80 分、ミニ演習課題：10 分）
その他	

7.2. コマシラバス（3/4）

回数	第3回
コマタイトル	情報セキュリティポリシ
コマの学習目標	・ 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。
コマの学習内容	(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(Information Security Management System ：情報セキュリティマネジメントシステム）適合評価制度 ISMS 認定 ISO/IEC 17799 （JIS 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
時間の目安	90 分 （講義：80 分、ミニ演習課題：10 分）
その他	

7.2. コマシラバス（4/4）

回数	第４回
コマタイトル	セキュリティに関する社内規定
コマの学習目標	・ 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。
コマの学習内容	(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
時間の目安	90 分 （講義：80 分、ミニ演習課題：10 分）
その他	

シラバス　8.（11-S-02）セキュリティガイドライン

8.1. コースシラバス

コースコード	11-S-02
コース名	セキュリティガイドライン
講座分類	中級
コース分野	ストラテジ
研修方法	講義(ミニ演習課題を含む)
受講前提	セキュリティに関して基本的な知識を修得していること
コース概要	・ 「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を学習する。 ・ 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。
コース目標	・ 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目的、考え方を理解し、応用する知識を修得する。 ・ 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、応用する知識を修得する。 ・ 情報セキュリティポリシの目的、考え方を修得し、応用する知識を修得する。 ・ 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、応用する知識を修得する。
コースに対応する情報処理技術者試験	応用情報技術者試験 （セキュリティ領域）
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

コースのコマ構成		
回数	**コマタイトル**	**コマに対応する機能・役割定義**
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	140-01．セキュリティ方針の策定
第２回	情報資産	140-01．セキュリティ方針の策定
第３回	リスク分析と評価	140-01．セキュリティ方針の策定
第４回	リスク対策	140-01．セキュリティ方針の策定
第５回	情報セキュリティポリシ	140-01．セキュリティ方針の策定
第６回	企業活動一般のセキュリティ規定	140-02．セキュリティ基準の策定
第７回	情報システムのセキュリティ規定	140-02．セキュリティ基準の策定
第８回	情報セキュリティ マネジメントシステム	140-02．セキュリティ基準の策定
備考		
・ ミニ演習課題は、応用情報技術者試験問題レベルが適切である。 ・ 次の共通キャリア・スキルフレームワークにも対応する。 【大項目】9．企業と法務－【中項目】23．法務		

8.4. コマシラバス（1/8）

回数	第 1 回
コマタイトル	情報セキュリティの目的と情報セキュリティ管理
コマの学習目標	・ 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。
コマの学習内容	(1) 情報セキュリティ 目的と考え方 重要性 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
時間の目安	90 分 （講義：70 分、ミニ演習課題：20 分）
その他	

8.4. コマシラバス（2/8）

回数	第 2 回
コマタイトル	情報資産
コマの学習目標	・ 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。
コマの学習内容	(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
時間の目安	90 分 （講義：70 分、ミニ演習課題：20 分）
その他	

8.4. コマシラバス（3/8）

回数	第3回
コマタイトル	リスク分析と評価
コマの学習目標	・ 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。
コマの学習内容	(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 ：JIPDEC が開発した定性的リスク分析方法論） (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
時間の目安	90 分 （講義：70 分、ミニ演習課題：20 分）
その他	

8.4. コマシラバス（4/8）

回数	第４回
コマタイトル	リスク対策
コマの学習目標	・ 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。
コマの学習内容	(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
時間の目安	90 分 （講義：70 分、ミニ演習課題：20 分）
その他	

8.4. コマシラバス（5/8）

回数	第５回
コマタイトル	情報セキュリティポリシ
コマの学習目標	・ 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。
コマの学習内容	(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
時間の目安	90 分 （講義：70 分、ミニ演習課題：20 分）
その他	

8.4. コマシラバス（6/8）

回数	第 6 回
コマタイトル	企業活動一般のセキュリティ規定
コマの学習目標	・ 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。
コマの学習内容	(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
時間の目安	90 分 （講義：70 分、ミニ演習課題：20 分）
その他	

8.4. コマシラバス（7/8）

回数	第 7 回
コマタイトル	情報システムのセキュリティ規定
コマの学習目標	・ 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。
コマの学習内容	(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
時間の目安	90 分 （講義：70 分、ミニ演習課題：20 分）
その他	

8.4. コマシラバス（8/8）

回数	第８回
コマタイトル	情報セキュリティマネジメントシステム
コマの学習目標	・ 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。
コマの学習内容	(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 （JIS 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
時間の目安	90 分 （講義：70 分、ミニ演習課題：20 分）
その他	

シラバス　9.（11-S-03）セキュリティガイドライン上級

9.1. コースシラバス

コースコード	11-S-03
コース名	セキュリティガイドライン上級
講座分類	上級
コース分野	ストラテジ
研修方法	ワークショップ（講義を含む）
受講前提	セキュリティガイドラインに関して実践的な知識を修得していること
コース概要	・ 「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を学習する。 ・ 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、より実践的に応用できる知識を学習する。
コース目標	・ 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学習を通じて、セキュリティガイドラインに関する指導方法の知識を修得する。 ・ 情報セキュリティ基本方針を策定および評価する学習を通じて、後進育成できる知識を修得する。 ・ 情報セキュリティ対策基準を策定および評価する学習を通じて、後進育成できる知識を修得する。 ・ 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学習を通じて、後進育成できる知識を修得する。
コースに対応する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
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

コースのコマ構成		
回数	**コマタイトル**	**コマに対応する機能・役割定義**
第１回	情報資産の評価とリスクの認識	140-01．セキュリティ方針の策定
第２回	リスクの識別と対策	140-03．セキュリティの分析
第３回	リスク評価	140-03．セキュリティの分析
第４回	情報セキュリティ基本方針	140-04．セキュリティの見直し
第５回	企業活動一般のセキュリティ規定	140-04．セキュリティの見直し
第６回	情報システムのセキュリティ規定	140-04．セキュリティの見直し
備考		
・ 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。 ・ 次の共通キャリア・スキルフレームワークにも対応する。 【大項目】9．企業と法務－【中項目】23．法務		

9.4. コマシラバス（1/6）

回数	第 1 回
コマタイトル	情報資産の評価とリスクの認識
コマの学習目標	・ 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。
コマの学習内容	――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
時間の目安	180 分 （講義：60 分、ワークショップ：120 分）
その他	

9.4. コマシラバス（2/6）

回数	第 2 回
コマタイトル	リスクの識別と対策
コマの学習目標	・ 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。
コマの学習内容	――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
時間の目安	180 分 （講義：60 分、ワークショップ：120 分）
その他	

9.4. コマシラバス（3/6）

回数	第3回
コマタイトル	リスク評価
コマの学習目標	・ 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。
コマの学習内容	――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
時間の目安	180 分 （講義：60 分、ワークショップ：120 分）
その他	

9.4. コマシラバス（4/6）

回数	第４回
コマタイトル	情報セキュリティ基本方針
コマの学習目標	・ 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、見直しなど、基本方針に盛り込むことができる。
コマの学習内容	――講義―― (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 ――ワークショップ―― (1) 情報セキュリティ基本方針の策定
時間の目安	180 分 （講義：60 分、ワークショップ：120 分）
その他	

9.4. コマシラバス（5/6）

回数	第5回
コマタイトル	企業活動一般のセキュリティ規定
コマの学習目標	・ 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。
コマの学習内容	――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
時間の目安	180 分 （講義：60 分、ワークショップ：120 分）
その他	

9.4. コマシラバス（6/6）

回数	第6回
コマタイトル	情報システムのセキュリティ規定
コマの学習目標	・ 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。
コマの学習内容	――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
時間の目安	180 分 （講義：60 分、ワークショップ：120 分）
その他	