情報システムユーザースキル標準（UISS）
（14） セキュリティ
（研修ロードマップ）

2009. 03

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

独立行政法人　情報処理推進機構
経済産業省

１．研修コース群（体系図）---------- (14)-2

２．研修コース一覧---------- (14)-3

３．研修コースの内容---------- (14)-4

研修コース体系図（14）セキュリティ

＝当該領域研修コース　＝他の領域研修コース

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

研修コース一覧表（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（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)-5	
	情報セキュリティポリシ	○	○		6 時間	1 日間	(14)-6	
中級	セキュリティ技術中級	○	○		12 時間	2 日間	(14)-7	
	セキュリティ管理中級	○	○		12 時間	2 日間	(14)-8	
	セキュリティガイドライン	○	○		12 時間	2 日間	(14)-9	
上級	セキュリティ技術上級		○	○		3 日間	(14)-10	
	セキュリティ管理上級		○	○		3 日間	(14)-11	
	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	

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）

コース名 / 研修コースの内容	セキュリティ管理初級
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、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入門的な知識の修得を目的とする。 ○当コースでは、情報資産管理を対象として、情報資産保護とアクセスの重要性、不正アクセスから情報資産を守るためのアクセス管理方法、ネットワークセキュリティについてはウイルス対策についても学習する。
受講対象者	IS部門、または業務部門において、上司の指導の下、セキュリティを考慮したIS企画・導入、運用の管理に携わろうとする者
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	セキュリティ管理に関連する基本的な知識を活用し、上位者の指導の下で、セキュリティ管理規定に基づき業務に携わることができる。
関連知識	以下の事項の入門的な知識 ・情報システム安全対策基準、ISMS ・被害状況の調査方法、復旧時の考慮点、システム再編時の考慮点、事故の記録の記載事項に関する知識 ・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

コース名 / 研修コースの内容	情報セキュリティポリシ
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、情報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。 ○当コースでは、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。
受講対象者	IS部門、または業務部門において、上司の指導の下、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	・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。
関連知識	以下の事項の入門的な知識 ・脅威・脆弱性に関する知識 ・リスクの存在箇所・原因・種類 ・情報システム安全対策基準、ISMS

コース名 / 研修コースの内容	セキュリティ技術中級
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、情報システムについて、独力ですべてのセキュリティ設計、セキュリティ対策の採用ができる応用的な知識の修得を目的とする。 〇コース前半では、eラーニング形式によって、情報資産に対するセキュリティ対策とセキュリティ運用の考え方と、セキュリティ関連法規やセキュリティ対策を理解し、セキュリティ技術と製品の機能に関する技術的な知識を学習する。 後半では、講義形式、ワークショップ形式で、情報資産のリスクを評価し、安全対策を定め、セキュリティ技術を採択する方法を実践的に学習する。
受講対象者	IS部門、または業務部門において、すべて独力で、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、ワークショップ、eラーニング、
研修期間	標準日数 2 日（クラスルーム）、標準時間 12 時間 （eラーニング）
スキル修得目標	以下の業務について、すべて独力で実施することができる。 情報システムのセキュリティ対策に関する知識を活用し、技術チームメンバとして、情報システムのセキュリティの設計を実施する。 正確な調査情報を取得し、適切な方法論を用いて情報源および要求の把握を行う 現状の脅威に関する情報を網羅的に収集し、情報の改ざん、情報の漏洩、資源の浪費、資源の不正利用、人による過ちなどの分類項目で整理する。 識別されたリスクに対して、対策を決定し、対策が現状どの程度実施されているかどうか調査、整理する。
関連知識	以下の事項の応用的な知識 ・ISMS、コンピュータ不正アクセス対策基準、コンピュータウイルス対策基準、情報システム安全対策基準 ・定量的・定性的リスク評価方法、脅威・脆弱性に関する知識、リスクの存在箇所・原因・種類 ・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、・侵入検知システム、侵入監視サービス ・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）

コース名 / 研修コースの内容	セキュリティ管理中級
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、情報セキュリティについて、独力ですべての企画・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。 ○当コースでは、情報資産管理を対象として、情報資産保護とアクセスの重要性、不正アクセスから情報資産を守るためのアクセス管理方法、ネットワークセキュリティについてはウイルス対策についても学習する。
受講対象者	IS部門、または業務部門において、すべて独力で、セキュリティを考慮したIS企画・導入、運用の管理ができることを目指す者
研修方法	講義、ワークショップ、eラーニング、
研修期間	標準日数 2 日（クラスルーム）、標準時間 12 時間 （eラーニング）
スキル修得目標	セキュリティ管理に関連する基本的な知識を活用し、すべて独力で、セキュリティ管理規定に基づき業務に携わることができる。
関連知識	以下の事項の応用的な知識 ・情報システム安全対策基準、ISMS ・被害状況の調査方法、復旧時の考慮点、システム再編時の考慮点、事故の記録の記載事項に関する知識 ・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

コース名 / 研修コースの内容	セキュリティガイドライン
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、関連法規やガイドラインに従って、独力で全てのセキュリティ方針、セキュリティ基準の策定ができる応用的な知識の修得を目的とする。 〇前半では、eラーニング形式で、関連法規や、ガイドラインに関する知識修得ならびに、セキュリティポリシ、セキュリティ基準策定に関する知識を学習する。 〇後半では、講義形式、ワークショップ形式で、セキュリティポリシ策定方法、セキュリティ基準策定方法などについて検討し、その修得のための実績的な学習を行う。
受講対象者	IS部門、または業務部門において、すべて独力で、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、ワークショップ、eラーニング、
研修期間	標準日数 2 日（クラスルーム）、標準時間 12 時間 （eラーニング）
スキル修得目標	以下の業務について、すべて独力で実施することができる。 ・セキュリティに関する関連法規やガイドラインの知識を活用し、基本的なセキュリティポリシ策定、セキュリティ基準策定を実施する。 ・セキュリティポリシ策定、セキュリティ基準策定のための、情報資産の評価、脅威の認識、リスクの識別、対策の整理と調査、リスクの評価を実施する。
関連知識	以下の事項の応用的な知識 ・脅威・脆弱性に関する知識 ・リスクの存在箇所・原因・種類 ・情報セキュリティの国際標準（ISO17799、JISX58）、ISMS ・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、罰則の規程、対外説明の規定、例外の規定、規則更新の規定

コース名 / 研修コースの内容	セキュリティ技術上級
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、「セキュリティ設計」の後続コースとして、セキュリティ対策の採用に関連する改善や技術面での実践における課題の発見と解決を指導・管理できる高度かつ専門的な知識の修得を目的とする。 〇当コースでは、講義形式、ワークショップ形式で、セキュリティの設計において、特に強固なセキュリティが要求される場合や、複雑なシステム統合や特殊環境における考慮点について理解を深め、セキュリティ対策の採用を実践的に学習する。 検討する事例としては、インターネット接続において外部からの脅威の危険性が大きい情報システム、複雑で高度なアクセスコントロールが要求される情報システム、複雑で高度な物理的セキュリティが要求される情報システム、高度のプライバシ管理が要求される情報システム、高度の機密性が要求される情報システム、セキュリティ上の脆弱性が企業に多大な損害を与える情報システム、連続稼動のために変更、保守、障害回復に高度な設計が必要な情報システムなどを取り上げる。
受講対象者	IS部門、または業務部門においてセキュリティを考慮した IS 構築、運用の経験を有し、その指導または管理する立場を目指す者
研修方法	講義、ワークショップ
研修期間	標準日数 3 日（クラスルーム）
スキル修得目標	情報システムのセキュリティ対策に関する知識を活用し、指導または管理する立場で、情報システムのセキュリティを設計することができる。
関連知識	以下の事項の高度かつ専門的な知識 ・ISMS、コンピュータ不正アクセス対策基準、コンピュータウイルス対策基準、情報システム安全対策基準 ・定量的・定性的リスク評価方法、脅威・脆弱性に関する知識、リスクの存在箇所・原因・種類 ・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 ・侵入検知システム、侵入監視サービス ・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）

コース名 / 研修コースの内容	セキュリティ管理上級
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における課題の発見と解決を指導・管理できる高度かつ専門的な知識の修得を目的とする。 ○当コースでは、セキュリティポリシィを策定し、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ができる能力を身に着ける。
受講対象者	IS部門、または業務部門においてセキュリティを考慮した IS 構築、運用の経験を有し、その指導または管理する立場を目指す者
研修方法	講義、ワークショップ
研修期間	標準日数 3 日（クラスルーム）
スキル修得目標	セキュリティ管理について、指導または管理する立場で、情報資産に関するセキュリティ管理規定に基づく管理業務を実施することができる。
関連知識	以下の事項の高度かつ専門的な知識 ・情報システム安全対策基準、ISMS ・被害状況の調査方法、復旧時の考慮点、システム再編時の考慮点、事故の記録の記載事項に関する知識 ・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

コース名 / 研修コースの内容	セキュリティガイドライン上級
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、「セキュリティガイドライン」の後続コースとして、関連法規やガイドラインに従ったセキュリティ方針、セキュリティ基準策定における課題の発見と解決を指導・管理できる高度かつ専門的な知識を修得することを目的とする。 〇当コースでは、セキュリティポリシ策定、セキュリティ基準策定ならびにその見直しならびに指導を網羅的に行える知識、方法に関し学習する。 〇後半では、講義形式、ワークショップ形式で、網羅的なセキュリティポリシ策定方法、セキュリティ基準策定ならびにその見直しならびにその指導を行うスキルを修得するために実績的に学習する。
受講対象者	IS部門、または業務部門においてセキュリティを考慮した IS 構築、運用の経験を有し、その指導または管理する立場を目指す者
研修方法	講義、ワークショップ
研修期間	標準日数 3 日（クラスルーム）
スキル修得目標	以下の業務について。指導または管理する立場で実施することができる。 ・セキュリティ対策の取り組みを経営方針に反映させる。 ・個々の技術に依存せずに方針作成、指導する。 ・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、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、公開見直しに関し、方針、基準を策定する
関連知識	以下の事項の高度かつ専門的な知識 ・脅威・脆弱性に関する知識 ・リスクの存在箇所・原因・種類、・情報セキュリティの国際標準（ISO17799、JISX58）、ISMS ・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、罰則の規程、対外説明の規定、例外の規定、規則更新の規定

コース名 / 研修コースの内容	最新セキュリティ技術動向
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、日々変化していくITサービスを取りまく最新のセキュリティ技術動向を理解し、実際のビジネスで応用するための知識を修得することを目的とする。 ○当コースでは、国内外のIT動向やプラットフォーム・システム管理基盤・データベース・ネットワーク・分散コンピューティングシステムなどに関わる最新のセキュリティ技術の動向などについて学習する。 ○当コースは、必要に応じてテーマ毎に設定される。受講者は、自らのスキルの維持・向上を図るために必要に応じて選択し受講する。
受講対象者	IS にかかわる実務者もしくは、責任者またはリーダとして、セキュリティ技術に関する知識を深めたい者
研修方法	講義
研修期間	標準日数 1 日 （クラスルーム）
スキル修得目標	最新セキュリティ技術動向を網羅的かつ総括的に捉えることができる 最新セキュリティ技術情報を適切に分析・抽出し、文書化できる 最新セキュリティ技術情報を継続的に収集できる
関連知識	IT 動向 IT 動向調査手法