令和2年度「専修学校による地域産業中核的人材養成事業」

モデルカリキュラム

Society5.0 に対応した情報セキュリティ人材養成のモデルカリキュラム開発・実証事業

令和２年度「専修学校による地域産業中核的人材養成事業」

モデルカリキュラム

Society5.0 に対応した情報セキュリティ人材養成のモデルカリキュラム開発・実証事業

情報セキュリティモデル・カリキュラム 1

学科：コンピュータシステム基礎	担当講師：
科目名：ハードウェアの基本	授業回数：23 コマ（回）
科目概要：コンピュータを構成するハードウェアの基本について学ぶ。	
評価方法：	
前提知識：特になし。	

回数	学習項目	備考
1	コンピュータの種類と構成	
2	ハードウェアとは	
3	プロセッサの基本①種類と特徴	
4	プロセッサの基本②アーキテクチャ	
5	プロセッサの基本③制御装置・演算装置の役割	
6	プロセッサの基本④動作原理―演算の仕組み	
7	プロセッサの基本⑤動作原理―命令とアドレッシング	
8	プロセッサの基本⑥動作原理―割込み	
9	プロセッサの基本⑦クロック周波数、CPI、MIPS	
10	プロセッサの基本⑧高速化技術	
11	プロセッサの基本⑨並列処理	
12	プロセッサの基本⑩マルチプロセッサシステム	
13	メモリの基本①種類と特徴	
14	メモリの基本②主記憶装置	
15	メモリの基本③記憶階層	
16	メモリの基本④アクセス方式	
17	メモリの基本⑤メモリの容量と性能	
18	メモリの基本⑥記録媒体の種類と特徴	
19	バスの種類と特徴	
20	入出力インターフェイスの種類と特徴	
21	入力装置の種類と特徴	
22	出力装置の種類と特徴	
23	補助記憶装置の種類と特徴	

情報セキュリティモデル・カリキュラム 2

学科：コンピュータシステム基礎	担当講師：
科目名：ソフトウェアの基本	授業回数：11 コマ（回）
科目概要：コンピュータを構成するソフトウェアの基本について学ぶ。	
評価方法：	
前提知識：特になし。	

回数	学習項目	備考
1	ソフトウェアとは	
2	オペレーティングシステムの種類と特徴	
3	オペレーティングシステムの基本機能と構成	
4	オペレーティングシステムにおける管理の仕組み①（ジョブ管理、タスク管理、データ管理、入出力管理、記憶管理）	
5	オペレーティングシステムにおける管理の仕組み②（ネットワーク制御、運用管理、ユーザ管理、セキュリティ制御、障害管理）	
6	アプリケーションとは	
7	ミドルウェアの役割と機能	
8	ファイルシステムの種類と特徴	
9	開発ツールの種類と特徴、機能	
10	オープンソースソフトウェアの種類と特徴	
11	オープンソースソフトウェアの活用と最新動向	

情報セキュリティモデル・カリキュラム 3

学科：コンピュータシステム基礎	担当講師：
科目名：ネットワークの基本	授業回数：24 コマ（回）
科目概要：LAN やインターネット、TCP/IP など、ネットワークに関する基礎知識を習得する。	
評価方法：	
前提知識：特になし。	

回数	学習項目	備考
1	ネットワークの種類と特徴	
2	有線 LAN、無線 LAN の仕組み	
3	交換方式の種類と回線速度	
4	インターネットとは	
5	ネットワークアーキテクチャの考え方	
6	伝送方式と回線	
7	ネットワーク接続装置の種類と機能	
8	ネットワーク制御の仕組み	
9	TCP/IP の基本	
10	IP の役割と機能	
11	TCP と UDP の役割と機能	
12	アプリケーションプロトコルの役割と機能	
13	ネットワークの運用管理	
14	ネットワーク管理のためのツール	
15	ネットワーク仮想化の仕組み	
16	電子メールの仕組み	
17	Web の仕組み	
18	ファイル転送の仕組み	
19	検索エンジンの仕組み	
20	イントラネットとは	
21	エクストラネットとは	
22	代表的な通信サービス	
23	モバイル通信サービスの概要と現状	
24	モバイルシステムの機器と技術	

情報セキュリティモデル・カリキュラム 4

学科：コンピュータシステム基礎	担当講師：
科目名：データベースの基本	授業回数：14 コマ（回）
科目概要：データベースの種類や操作などの基本から活用・運用方法までの一連の知識を身につける。	
評価方法：	
前提知識：特になし。	

回数	学習項目	備考
1	データベースの種類と特徴	
2	データモデルの種類	
3	データ分析とは	
4	データベースの設計	
5	データの正規化	
6	代表的なデータ操作	
7	データベース管理システムの役割と機能	
8	トランザクション処理	
9	代表的なデータベース言語と SQL の基本	
10	データ定義言語の基本	
11	データ操作言語の基本	
12	データ制御言語の基本	
13	データベース活用の実際	
14	データベースの運用とデータ資源管理	

情報セキュリティモデル・カリキュラム 5

学科：コンピュータシステム基礎	担当講師：
科目名：プログラミング概要	授業回数：29 コマ（回）
科目概要：プログラミング言語の主な種類と特徴を概観する。	
評価方法：	
前提知識：特になし。	

回数	学習項目	備考
1	基本のプログラミング作法	
2	コーディング標準とは	
3	プログラムの構造	
4	プログラム言語のデータ型①整数型	
5	プログラム言語のデータ型②実数型	
6	プログラム言語のデータ型③論理型	
7	プログラム言語のデータ型④文字型	
8	プログラム言語のデータ型⑤抽象データ型	
9	プログラム言語のデータ型⑥構造型	
10	web プログラミングの基本①基本の仕組み	
11	web プログラミングの基本②プログラミング方法	
12	プログラム言語の歴史	
13	主な手続型言語の特徴	
14	主な手続型言語の記述方法①Fortran	
15	主な手続型言語の記述方法②COBOL	
16	主な手続型言語の記述方法③PL/I	
17	主な手続型言語の記述方法④Pascal	
18	主な手続型言語の記述方法⑤BASIC	
19	主な手続型言語の記述方法⑥C	
20	主なオブジェクト指向言語の特徴	
21	主なオブジェクト指向言語の記述方法①Java	
22	主なオブジェクト指向言語の記述方法②C++	
23	主なスクリプト言語の特徴	
24	主なスクリプト言語の記述方法①ECMAScript	
25	主なスクリプト言語の記述方法②Perl	
26	主なスクリプト言語の記述方法③PHP	
27	主なスクリプト言語の記述方法④Pyhon	
28	主なスクリプト言語の記述方法⑤Ruby	
29	共通言語基盤の特徴	

情報セキュリティモデル・カリキュラム 6

学科：コンピュータシステム基礎	担当講師：
科目名：C と Java の基本技術	授業回数：24 コマ（回）
科目概要：C と Java のプログラム作成方法を習得する。	
評価方法：	
前提知識：「プログラミング概要」で学んだ知識。	

回数	学習項目	備考
1	C のプログラム作成①基本的なプログラム	
2	C のプログラム作成②数値計算	
3	C のプログラム作成③選択型プログラム	
4	C のプログラム作成④反復型プログラム	
5	C のプログラム作成⑤ビット演算	
6	C のプログラム作成⑥入力処理	
7	C のプログラム作成⑦配列	
8	C のプログラム作成⑧文字処理	
9	C のプログラム作成⑨ポインタ	
10	C のプログラム作成⑩関数	
11	C のプログラム作成⑪ライブラリ関数	
12	C のプログラム作成⑫記憶域クラス指定	
13	C のプログラム作成⑬構造体	
14	C のプログラム作成⑭ファイル処理	
15	Java のプログラム作成①基本的なプログラム	
16	Java のプログラム作成②数値計算	
17	Java のプログラム作成③選択型プログラム	
18	Java のプログラム作成④反復型プログラム	
19	Java のプログラム作成⑤クラスとインスタンス	
20	Java のプログラム作成⑥差分プログラム	
21	Java のプログラム作成⑦例外処理、並列処理	
22	Java のプログラム作成⑧コレクションと総称	
23	Java のプログラム作成⑨入れ子クラス	
24	Java のプログラム作成⑩列挙	

情報セキュリティモデル・カリキュラム 7

学科：コンピュータシステム基礎	担当講師：
科目名：Python 等の基本技術	授業回数：27 コマ（回）
科目概要：Python とアセンブリ言語（CASL Ⅱ）のプログラム作成方法を習得する。また、表計算ソフトの基本的な操作やマークアップ言語、UML の基本についても学習する。	
評価方法：	
前提知識：「プログラミング概要」で学んだ知識。	

回数	学習項目	備考
1	Python のプログラム作成①基本的なプログラム	
2	Python のプログラム作成②演算子を用いた式の表現	
3	Python のプログラム作成③要素を持つデータ型	
4	Python のプログラム作成④選択型プログラム	
5	Python のプログラム作成⑤反復型プログラム	
6	Python のプログラム作成⑥組み込み関数	
7	Python のプログラム作成⑦関数の定義	
8	Python のプログラム作成⑧クラスとオブジェクト	
9	Python のプログラム作成⑨変数及び関数の値の取り扱い	
10	Python のプログラム作成⑩ライブラリの活用	
11	アセンブリ言語（CASL Ⅱ）のプログラム作成①基本仕様	
12	アセンブリ言語（CASL Ⅱ）のプログラム作成②基本的なプログラム	
13	アセンブリ言語（CASL Ⅱ）のプログラム作成③算術演算、論理演算	
14	アセンブリ言語（CASL Ⅱ）のプログラム作成④選択と反復処理	
15	アセンブリ言語（CASL Ⅱ）のプログラム作成⑤シフト演算	
16	アセンブリ言語（CASL Ⅱ）のプログラム作成⑥表を使った処理	
17	アセンブリ言語（CASL Ⅱ）のプログラム作成⑦入出力処理	
18	アセンブリ言語（CASL Ⅱ）のプログラム作成⑧スタック	
19	表計算ソフトの活用①ワークシート、式	
20	表計算ソフトの活用②関数	
21	表計算ソフトの活用③マクロ	
22	表計算ソフトの活用④業務処理	
23	マークアップ言語の基本①HTML	
24	マークアップ言語の基本②XML	
25	マークアップ言語の基本③XHTML	
26	マークアップ言語の基本④スタイルシート	
27	UML の基本	

情報セキュリティモデル・カリキュラム 8

学科：コンピュータシステム基礎	担当講師：
科目名：システムの設計	授業回数：27 コマ（回）
科目概要：システムの構成に関する基本知識を得た上で、システムの要件定義～方式設計について学習する。	
評価方法：	
前提知識：特になし。	

回数	学習項目	備考
1	システム構成①集中処理と分散処理	
2	システム構成②様々な利用形態	
3	システム構成③主なシステム構成の種類と特徴	
4	ハイパフォーマンスコンピューティングとは	
5	クライアントサーバシステムとは	
6	Web システムの基本構成	
7	RAID とは	
8	信頼性設計の考え方	
9	システムの性能指標、キャパシティプランニング	
10	システム評価指標―RASIS、MTBF、MTTR、稼働率	
11	システムのコスト評価	
12	主なソフトウェア開発モデル	
13	システム要件定義①概要	
14	システム要件定義②システム化の目標と対象範囲	
15	システム要件定義③機能及び能力の定義	
16	システム要件定義④業務・組織及び利用者の要件	
17	システム要件定義④その他の要件	
18	システム要件定義⑤評価・レビュー手法	
19	システム方式設計①概要	
20	システム方式設計②設計の準備	
21	システム方式設計③ハードウェア・ソフトウェア・手作業の機能分割	
22	システム方式設計④ハードウェア	
23	システム方式設計⑤ソフトウェア	
24	システム方式設計⑥システム処理	
25	システム方式設計⑦データベース	
26	システム方式設計⑧システム結合テストの設計	
27	システム方式の評価・レビュー手法	

情報セキュリティモデル・カリキュラム 9

学科：コンピュータシステム基礎	担当講師：
科目名：ソフトウェアの設計	授業回数：25 コマ（回）
科目概要：ソフトウェアの要件定義～方式設計・詳細設計について学習する。また、システム、ソフトウェアの導入に向けたテストや導入後の管理等についても習得する。	
評価方法：	
前提知識：「システムの設計」で学んだ知識。	

回数	学習項目	備考
1	ソフトウェア要件定義（外部設計）①概要	
2	ソフトウェア要件定義（外部設計）②要件の確立	
3	ソフトウェア要件定義（外部設計）③評価・レビュー手法	
4	ソフトウェア要件定義（外部設計）④業務分析・要件定義の手法	
5	ソフトウェア方式設計（内部設計）①概要	
6	ソフトウェア方式設計（内部設計）②構造とコンポーネントの設計	
7	ソフトウェア方式設計（内部設計）③コンポーメント間インターフェイスの設計	
8	ソフトウェア方式設計（内部設計）④ソフトウェア結合テスト要件定義	
9	ソフトウェア詳細設計（プログラム設計）①概要	
10	ソフトウェア詳細設計（プログラム設計）②コンポーネントの詳細設計	
11	ソフトウェア詳細設計（プログラム設計）③インターフェイスの詳細設計	
12	ソフトウェア設計の評価・レビュー手法	
13	ソフトウェアの品質（ISO/IEC25010）	
14	ソフトウェア設計手法①プロセス中心設計、データ中心設計	
15	ソフトウェア設計手法②構造化設計、オブジェクト指向設計	
16	ソフトウェア構築①概要	
17	ソフトウェア構築②コーディング	
18	ソフトウェア構築③テスト・レビュー	
19	ソフトウェア結合・ソフトウェア適格性確認テスト	
20	システム結合・システム適格性確認テスト	
21	システム、ソフトウェア導入	
22	システム、ソフトウェア受け入れ支援	
23	保守のタスクと手順	
24	ソフトウェアの構成管理・変更管理	
25	開発環境の管理―開発ツールの整備、設計データの管理	

情報セキュリティモデル・カリキュラム 10

学科：セキュリティ基礎	担当講師：
科目名：セキュリティ概論①	授業回数：29 コマ（回）
科目概要：セキュリティに関する基本的な考え方から具体的な攻撃方法やセキュリティ技術を概観する。	
評価方法：	
前提知識：特になし。	

回数	学習項目	備考
1	セキュリティの必要性	
2	セキュリティ対策の歴史	
3	情報セキュリティの基本概念、定義	
4	情報資産に対するさまざまな脅威①脅威の種類	
5	情報資産に対するさまざまな脅威②被害事例	
6	主な外部リスク①概要	
7	主な外部リスク②マルウェア	
8	主な外部リスク③スパイウェア	
9	主な外部リスク④ランサムウェア	
10	主な内部リスク―脆弱性	
11	サイバー攻撃の変遷	
12	セキュリティ攻撃者の種類や動機	
13	ハッカーの現状とハクティビズム	
14	具体的な攻撃事例（個人対象）①インターネットバンキングやクレジットカード情報等の不正利用	
15	具体的な攻撃事例（個人対象）②ランサムウェアによる被害	
16	具体的な攻撃事例（個人対象）③ネット上の誹謗・中傷	
17	具体的な攻撃事例（個人対象）④スマートフォン、スマートフォンアプリを狙った攻撃	
18	具体的な攻撃事例（個人対象）⑤ウェブサービスへの不正ログイン	
19	具体的な攻撃事例（個人対象）⑥ウェブサービスからの個人情報の窃取	
20	具体的な攻撃事例（個人対象）⑦偽警告によるインターネット詐欺	
21	具体的な攻撃事例（組織・不特定多数対象）①標的型攻撃	
22	具体的な攻撃事例（組織・不特定多数対象）②制御システムへの攻撃	
23	具体的な攻撃事例（組織・不特定多数対象）③Web サイトの乗っ取りと改ざん	
24	具体的な攻撃事例（組織・不特定多数対象）④仮想通貨における問題	
25	主なセキュリティ技術①暗号技術	
26	主なセキュリティ技術②認証技術	
27	主なセキュリティ技術③利用者認証	
28	主なセキュリティ技術④生体認証技術	
29	主なセキュリティ技術⑤公開鍵基盤	

情報セキュリティモデル・カリキュラム 11

学科：セキュリティ基礎	担当講師：
科目名：セキュリティ概論②	授業回数：21 コマ（回）
科目概要：セキュリティ管理の概要とリスク別のセキュリティ対策の概要を学習する。	
評価方法：	
前提知識：「セキュリティ概論①」で学んだ知識。	

回数	学習項目	備考
1	セキュリティ管理に必要な事項①情報管理の枠組み（セキュリティポリシー等）	
2	セキュリティ管理に必要な事項②情報資産の概念とリスク	
3	セキュリティ管理に必要な事項③情報管理体制の基本	
4	人的セキュリティ対策①主なリスク（人的ミス、不正行為、ソーシャルエンジニアリングなど）	
5	人的セキュリティ対策②リスクへの対応（内部統制、プライバシーマーク）	
6	技術的セキュリティ対策①主なリスク（クラッキング、不正アクセス、情報漏えいなど）	
7	技術的セキュリティ対策②リスクへの対応（DMZ、検疫ネットワーク、SPF）	
8	技術的セキュリティ対策③リスクへの対応（URL フィルタリング、コンテンツフィルタリング）	
9	技術的セキュリティ対策④リスクへの対応（WPA2、SSID、ANY 接続拒否）	
10	技術的セキュリティ対策⑤リスクへの対応（電子透かし、ディジタルフォレンジックス）	
11	技術的セキュリティ対策⑥リスクへの対応（IDS/IPS）	
12	技術的セキュリティ対策⑦リスクへの対応（ファイアウォール、WAF）	
13	技術的セキュリティ対策⑧リスクへの対応（ホワイトリスト、ブラックリスト、フォールスポジティブ、フォールスネガティブ）	
14	技術的セキュリティ対策⑨リスクへの対応（SSL アクセラレータ、MDM、BYOD）	
15	技術的セキュリティ対策⑩リスクへの対応（コールバック、アクセス制御、DLP）	
16	技術的セキュリティ対策⑪リスクへの対応（SIEM、UTM、ビヘイビア法、パターンマッチング方式）	
17	技術的セキュリティ対策⑫主なセキュリティ製品	
18	物理的セキュリティ対策①主なリスク（侵入、盗難、水害など）	
19	物理的セキュリティ対策②リスクへの対応（RASIS、UPS）	
20	物理的セキュリティ対策③リスクへの対応（ミラーリング、クリアデスク、クリアスクリーン）	
21	物理的セキュリティ対策④リスクへの対応（シンクライアント、TPM）	

情報セキュリティモデル・カリキュラム 12

学科：セキュリティ基礎	担当講師：
科目名：セキュリティ概論③	授業回数：19 コマ（回）
科目概要：利用者ができるセキュリティ対策と実際の情報漏洩の事例について学ぶとともに、セキュリティの実装技術やセキュリティ関連情報の収集方法を知る。	
評価方法：	
前提知識：特になし。	

回数	学習項目	備考
1	利用者のセキュリティ対策①基本的な対策	
2	利用者のセキュリティ対策②web サイト閲覧、ショッピングサイト	
3	利用者のセキュリティ対策③ネットオークション、インターネットバンキング	
4	利用者のセキュリティ対策④クラウドサービス、オンラインゲーム	
5	利用者のセキュリティ対策⑤SNS	
6	利用者のセキュリティ対策⑥電子メール	
7	利用者のセキュリティ対策⑦各種情報機器	
8	利用者のセキュリティ対策⑧コンピュータリテラシー	
9	情報漏洩の事例と対策①Twitter アカウント情報流出、Web ブラウザに保存された情報流出など	
10	情報漏洩の事例と対策②日本語入力ソフトによる情報流出、中国サイトへの情報流出など	
11	セキュリティ実装技術①セキュアプロトコル	
12	セキュリティ実装技術②認証プロトコル	
13	セキュリティに関する法整備	
14	セキュリティ関連情報の収集方法①Google Hacking の利用方法	
15	セキュリティ関連情報の収集方法②SHODAN の利用方法	
16	セキュリティ関連情報の収集方法③機密情報の収集	
17	セキュリティ関連情報の収集方法④Web サイトの安全性確認方法	
18	セキュリティ関連情報の収集方法⑤脆弱性検索サイト	
19	求められるセキュリティ人材像	

情報セキュリティモデル・カリキュラム 13

学科：セキュリティ基礎	担当講師：
科目名：ネットワークセキュリティ概論	授業回数：31 コマ（回）
科目概要：ネットワークセキュリティを構成するファイアウォールや VPN 等の技術について学習する。また、IoT についての基本知識を習得する。	
評価方法：	
前提知識：特になし。	

回数	学習項目	備考
1	イントラネットの構成	
2	ファイアウォールの仕組み①概要	
3	ファイアウォールの仕組み②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、プライベートアドレス	
4	ファイアウォールの仕組み③ネットワークアドレス変換（NAT）	
5	ファイアウォールの仕組み④DMZ	
6	ファイアウォールの仕組み⑤ファイアウォールの弱点	
7	ファイアウォールの仕組み⑥パーソナルファイアウォール	
8	IDS・IPS の仕組み①種類	
9	IDS・IPS の仕組み②検知方法と動作	
10	プロキシサーバの仕組み	
11	WAF（Web アプリケーションファイアウォール）の仕組み	
12	VPN の仕組み①概要	
13	VPN の仕組み②トンネリング、カプセル化	
14	VPN の仕組み③VPN の種類とプロトコル	
15	VPN の仕組み④IPsec	
16	ネットワークスキャン①ドメイン情報の取得	
17	ネットワークスキャン②ホストへのスキャン	
18	ネットワークスキャン③パスワードの奪取	
19	ネットワークセキュリティの最新事情―ゼロトラストセキュリティ	
20	IoT の概要と現状	
21	IoT のアーキテクチャ	
22	IoT セキュリティの課題①セーフティ、セキュリティ	
23	IoT セキュリティの課題②プライバシー（ネットワークカメラなど）	
24	IoT に関するインシデント事例	
25	IoT に対する脅威分析	
26	IoT セキュリティ―機器設計と利用者による対策	
27	IoT に関する各種ガイドライン	
28	IoT セキュリティの最新動向	
29	スマートフォンのセキュリティ①概要	
30	スマートフォンのセキュリティ②最新動向	
31	セキュリティへの AI の活用	

情報セキュリティモデル・カリキュラム 14

学科：セキュリティ基礎	担当講師：
科目名：暗号・認証・電子署名	授業回数：18 コマ（回）
科目概要：暗号技術についての概要を把握し、PKI 実装等の基本知識を身に付ける。	
評価方法：	
前提知識：特になし。	

回数	学習項目	備考
1	暗号技術の種類と特徴	
2	共通鍵暗号①ブロック暗号	
3	共通鍵暗号②ストリーム暗号	
4	共通鍵暗号③ハッシュ関数	
5	共通鍵暗号④暗号技術の標準化の動向	
6	公開鍵暗号①概要と経緯	
7	公開鍵暗号②RSA 暗号	
8	公開鍵暗号③デジタル署名	
9	公開鍵暗号④相手認証の必要性と技術	
10	公開鍵暗号⑤課題（正当性保障、量子計算機）	
11	認証技術の種類と特徴	
12	公開鍵基盤 PKI の仕組み	
13	信頼モデルの種類と特徴	
14	PKI の応用①SSL/TLS	
15	PKI の応用②タイムスタンプサービス	
16	利用者認証技術の種類と特徴	
17	プライバシー保護技術①匿名化	
18	プライバシー保護技術②秘密計算（ISO/IEC 19592-2:2017）	

情報セキュリティモデル・カリキュラム 15

学科：セキュリティ基礎	担当講師：
科目名：生体認証技術	授業回数：17 コマ（回）
科目概要：暗号技術において利用が進んでいる生体認証技術について、技術的な特徴から利用の事例までを学習する。	
評価方法：	
前提知識：「暗号・認証・電子署名」で学んだ知識。	

回数	学習項目	備考
1	生体認証技術①種類と特徴	
2	生体認証技術②利用の経緯	
3	生体認証技術③身体計測によるもの	
4	生体認証技術④行動計測によるもの	
5	生体認証技術⑤導入における課題―誤作動対応、構築コスト、安全性	
6	生体認証技術⑥PKI との関係	
7	生体認証技術⑦偽造等の脆弱性対応（キャンセラブルバイオメトリクス）	
8	生体認証技術⑧プライバシーとの関係	
9	生体認証技術⑨パスワードモデルとの比較	
10	生体認証技術⑩サーバ認証モデルとクライアント認証モデル	
11	生体認証技術⑪IC カードとの連携	
12	生体認証技術⑫認証の誤差	
13	生体認証技術⑬標準化の動向	
14	生体認証技術⑭利用事例	
15	生体認証技術⑮新たな応用分野―ターゲティング広告、ヘルスケアなど	
16	生体認証技術⑯FIDO	
17	最新技術の動向	

情報セキュリティモデル・カリキュラム 16

学科：セキュリティ基礎	担当講師：
科目名：セキュリティ運用	授業回数：28 コマ（回）
科目概要：組織としてセキュリティを運用する上で求められるリスクマネジメントの考え方や手法、情報セキュリティに関する規程や ISMS の構築に関する基礎知識を習得する。	
評価方法：	
前提知識：基本的なセキュリティ技術に関する知識。	

回数	学習項目	備考
1	情報セキュリティ管理の考え方	
2	リスクマネジメント基礎―ISO31000	
3	リスク分析と評価①情報資産の調査方法	
4	リスク分析と評価②情報資産の分類方法	
5	リスク分析と評価③情報資産に対するリスクの種類	
6	リスク分析と評価④リスクアセスメント	
7	リスク分析と評価⑤リスク対応	
8	緊急時対応	
9	情報セキュリティに関する組織内規程①セキュリティポリシーの構成	
10	情報セキュリティに関する組織内規程②セキュリティポリシーの策定手順	
11	情報セキュリティに関する組織内規程③セキュリティポリシーの周知、教育	
12	情報セキュリティに関する組織内規程④秘密情報管理規程	
13	情報セキュリティに関する組織内規程⑤セキュリティインシデント対応規程	
14	情報セキュリティに関する組織内規程⑥SNS ガイドライン	
15	情報セキュリティに関する組織内規程⑦運用の実際	
16	情報セキュリティマネジメントシステム（ISMS）の基本①構築方法	
17	情報セキュリティマネジメントシステム（ISMS）の基本②運用方法	
18	情報セキュリティマネジメントシステム（ISMS）の基本②主な規格	
19	情報セキュリティ組織機関の役割と活動①社内組織	
20	情報セキュリティ組織・機関の役割と活動②公的機関	
21	情報セキュリティ組織・機関の役割と活動③民間組織	
22	セキュリティ技術の評価―CC(ISO/IEC 15408)の概要	
23	セキュリティテスト手法①概要	
24	セキュリティテスト手法②脆弱性検査の概要	
25	セキュリティテスト手法③Web サイトの脆弱性検査	
26	セキュリティテスト手法④脆弱性検査ツール	
27	セキュリティテスト手法⑤侵入検知ツール	
28	セキュリティテスト手法⑥Web サイトの侵入検知	

情報セキュリティモデル・カリキュラム 17

学科：セキュリティ基礎	担当講師：
科目名：セキュリティ関連法規・法令	授業回数：20 コマ（回）
科目概要：サイバーセキュリティ基本法や個人情報保護法、取引を行う上での守秘契約など、セキュリティを取り巻く法律について学習する。	
評価方法：	
前提知識：特になし。	

回数	学習項目	備考
1	知的財産権	
2	サイバーセキュリティ基本法の目的と概要	
3	日本におけるサイバーセキュリティ体制―サイバーセキュリティ戦略本部、NISC（内閣サイバーセキュリティセンター）	
4	サイバーセキュリティ基本法改正のポイントと背景	
5	サイバーセキュリティ戦略の具体的内容	
6	不正アクセス禁止法	
7	個人情報保護法①個人情報、プライバシーとは	
8	個人情報保護法②個人情報の取り扱いに関する規定	
9	JIS Q 15001：2017 個人情報保護マネジメントシステム―要求事項―	
10	個人情報に関する国際標準	
11	マイナンバー法	
12	刑法（ウイルス作成罪など）	
13	電子署名及び認証業務に関する法律	
14	その他のセキュリティ関連法（プロバイダ責任制限法、特定電子メール法など）	
15	取引関連法規①外部委託契約	
16	取引関連法規②守秘契約	
17	取引関連法規③ライセンス契約	
18	取引関連法規④ソフトウェア開発契約	
19	IT 基本法	
20	その他の法律（電気通信事業法、e-文書法など）	

情報セキュリティモデル・カリキュラム 18

学科：セキュリティ基礎	担当講師：
科目名：セキュリティ関連基準	授業回数：16 コマ（回）
科目概要：セキュリティ関連の各種基準やガイドライン、規格について。また、情報に関する倫理やコンプライアンス等についても学習する。	
評価方法：	
前提知識：特になし。	

回数	学習項目	備考
1	情報セキュリティに関する基準①コンピュータウイルス対策基準	
2	情報セキュリティに関する基準②コンピュータ不正アクセス対策基準	
3	情報セキュリティに関する基準③ソフトウェア等脆弱性関連情報取扱基準	
4	情報セキュリティに関する基準④サイバーセキュリティ経営ガイドライン	
5	情報セキュリティに関する基準⑤中小企業の情報セキュリティ対策ガイドライン	
6	情報セキュリティに関する基準⑥コンシューマ向け IoT セキュリティガイド	
7	情報セキュリティに関する基準⑦IoT セキュリティガイドライン	
8	情報セキュリティに関する基準⑧サイバーフィジカルセキュリティ対策フレームワーク	
9	情報セキュリティに関する基準⑨スマートフォン安全安心強化戦略	
10	情報セキュリティに関する基準⑩ソーシャルメディアガイドライン	
11	標準、規格①概要	
12	標準、規格②JIS	
13	標準、規格③IS	
14	法を取り巻く情報倫理、モラル	
15	企業のコンプライアンス	
16	セキュリティ関連の政策動向	

情報セキュリティモデル・カリキュラム 19

学科：情報セキュリティの設計と構築	担当講師：
科目名：システムセキュリティ構築①	授業回数：23 コマ（回）
科目概要：OS、データベース、web システムに関するセキュリティ上の必須知識を学習する。	
評価方法：	
前提知識：「セキュリティ基礎」で学んだ知識。	

回数	学習項目	備考
1	OS 関連のセキュリティ①概要	
2	OS 関連のセキュリティ②アクセス管理	
3	OS 関連のセキュリティ③システム管理	
4	OS 関連のセキュリティ④Windows	
5	OS 関連のセキュリティ⑤Linux	
6	OS 関連のセキュリティ⑥スマートフォン	
7	データベースセキュリティ①概要	
8	データベースセキュリティ②アクセス管理	
9	データベースセキュリティ③ロール	
10	データベースセキュリティ④Oracle のセキュリティ	
11	Web システムのセキュリティ①概要	
12	Web システムのセキュリティ②HTTP	
13	Web システムのセキュリティ③セッションハイジャック	
14	Web システムのセキュリティ④セッションフィクセーション	
15	Web システムのセキュリティ⑤SQL インジェクション	
16	Web システムのセキュリティ⑥クロスサイトスクリプティング（XSS）	
17	Web システムのセキュリティ⑦クロスサイトリクエストフォージェリ（CSRF）	
18	Web システムのセキュリティ⑧ディレクトリトラバーサル	
19	Web システムのセキュリティ⑨OS コマンドインジェクション	
20	Web システムのセキュリティ⑩バッファオーバフロー（BOF）	
21	Web システムのセキュリティ⑪クリックジャッキング	
22	Web システムのセキュリティ⑫ HTTP ヘッダインジェクション	
23	Web システムのセキュリティ⑬メールヘッダインジェクション	

情報セキュリティモデル・カリキュラム 20

学科：情報セキュリティの設計と構築	担当講師：
科目名：システムセキュリティ構築②	授業回数：20 コマ（回）
科目概要：メール、DNS システムに関するセキュリティ上の必須知識を学習する。また、情報ハインディング技術について一通り習得する。	
評価方法：	
前提知識：「セキュリティ基礎」で学んだ知識。	

回数	学習項目	備考
1	メールシステムのセキュリティ①概要	
2	メールシステムのセキュリティ② SMTP、POP のセキュリティ	
3	メールシステムのセキュリティ③S/MIME、PGP	
4	メールシステムのセキュリティ④送信ドメイン認証（SPF、DKIM、DMARC）	
5	メールシステムのセキュリティ⑤フィルタリング	
6	メールシステムのセキュリティ⑥OP25B	
7	メールシステムのセキュリティ⑦Web メール	
8	DNS システムのセキュリティ①概要	
9	DNS システムのセキュリティ②DNS キャッシュポイズニング	
10	DNS システムのセキュリティ③DDoS 攻撃	
11	DNS システムのセキュリティ④その他	
12	情報ハインディング技術①電子透かし―機能と用途	
13	情報ハインディング技術②電子透かし―原理	
14	情報ハインディング技術③電子透かし―技術要件	
15	情報ハインディング技術④電子透かし―関連する法制度	
16	情報ハインディング技術⑤電子透かし―実用例	
17	情報ハインディング技術⑥ステガノグラフィ―機能と用途	
18	情報ハインディング技術⑦ステガノグラフィ―原理	
19	情報ハインディング技術⑧ステガノグラフィ―技術要件	
20	情報ハインディング技術⑨ステガノグラフィ―実用例	

情報セキュリティモデル・カリキュラム 21

学科：情報セキュリティの設計と構築	担当講師：
科目名：セキュアなシステム設計・開発①	授業回数：16 コマ（回）
科目概要：セキュアなシステムを設計・開発する上で必要な考え方や知識について、CC(ISO/IEC 15408)をベースに学習する。	
評価方法：	
前提知識：「セキュリティ基礎」で学んだ知識。	

回数	学習項目	備考
1	セキュアな情報システムとは	
2	セキュリティアーキテクチャの考え方	
3	セキュアな設計のステップ	
4	セキュリティドメインの概念とドメイン分離の実現方法	
5	自己保護の概念と実現方法	
6	非バイパス性の概念と実現方法	
7	セキュアな初期化の概念と実現方法	
8	CC(ISO/IEC 15408)の概要	
9	セキュリティの設計①ST 概説・セキュリティ課題定義	
10	セキュリティの設計②セキュリティ対策方針・セキュリティ要件	
11	セキュリティの設計③CC(ISO/IEC 15408)セキュリティ機能コンポーネント	
12	セキュリティの実装①CC(ISO/IEC 15408)セキュリティ保証コンポーネント・ADV クラス	
13	セキュリティの実装②CC(ISO/IEC 15408)セキュリティ保証コンポーネント・AGD クラス	
14	セキュリティの実装③CC(ISO/IEC 15408)セキュリティ保証コンポーネント・ALC クラス	
15	セキュリティの実装④CC(ISO/IEC 15408)セキュリティ保証コンポーネント・ATE クラス	
16	IT セキュリティ評価及び認証制度と暗号モジュール試験及び認証制度	

情報セキュリティモデル・カリキュラム 22

学科：情報セキュリティの設計と構築	担当講師：
科目名：セキュアなシステム設計・開発②	授業回数：17 コマ（回）
科目概要：働き方改革、コロナウイルスの流行に伴いテレワークの普及など変化するネットワーク環境に対し、求められるゼロトラストセキュリティの考え方について学習する。	
評価方法：	
前提知識：「セキュアなシステム設計・開発①」で学んだ知識。	

回数	学習項目	備考
1	ゼロトラストセキュリティ①with コロナ、after コロナのセキュリティ課題	
2	ゼロトラストセキュリティ②境界型とゼロトラストの違い	
3	ゼロトラストセキュリティ③境界型の歴史	
4	ゼロトラストセキュリティ④境界型の弱点	
5	ゼロトラストセキュリティ⑤ゼロトラストのコンポーネント群	
6	ゼロトラストセキュリティ⑥クラウド（IaaS、PaaS、SaaS）	
7	ゼロトラストセキュリティ⑦MDM	
8	ゼロトラストセキュリティ⑧EDR	
9	ゼロトラストセキュリティ⑨SOC	
10	ゼロトラストセキュリティ⑩SIG	
11	ゼロトラストセキュリティ⑪CASB	
12	ゼロトラストセキュリティ⑫SASE	
13	ゼロトラストセキュリティ⑬実装プロセス	
14	ゼロトラストセキュリティ⑭事例―Google	
15	ゼロトラストセキュリティ⑮事例―Microsoft	
16	ゼロトラストセキュリティ⑯事例―PagerDuty	
17	ゼロトラストセキュリティ⑰課題	

情報セキュリティモデル・カリキュラム 23

学科：情報セキュリティの設計と構築	担当講師：
科目名：セキュアなネットワーク設計	授業回数：28 コマ（回）
科目概要：セキュアプロトコルや ISO/IEC19790、セキュアプログラミングに関する知識、技術を学習する。ネットワーク構成事例についても紹介する。	
評価方法：	
前提知識：「セキュリティ基礎」で学んだ知識。	

回数	学習項目	備考
1	セキュリティ原則	
2	セキュアプロトコルの基本要素と概念	
3	暗号系プロトコル：Diffie-Hellman 鍵共有	
4	ネットワーク系プロトコル①Ipsec	
5	ネットワーク系プロトコル②SSL/TLS	
6	アプリケーション系プロトコル①電子投票	
7	アプリケーション系プロトコル②電子入札	
8	認証プロトコル①SAML	
9	認証プロトコル②Oauth	
10	認証プロトコル③FIDO	
11	耐タンパ性とは	
12	暗号処理①処理速度向上	
13	暗号処理②ユーザーインターフェース	
14	暗号モジュールの評価と試験・認証制度	
15	ISO/IEC19790①暗号モジュールの仕様、暗号モジュールのインタフェース	
16	ISO/IEC19790②役割・サービス及び認証、ソフトウェア・ファームウェアセキュリティ、動作環境	
17	ISO/IEC19790③物理セキュリティ、非侵襲セキュリティ	
18	ISO/IEC19790④Sensitive Security Parameter 管理、自己テスト	
19	ISO/IEC19790⑤ライフサイクル保証、その他の攻撃への対処	
20	セキュアプログラミング①脆弱性	
21	セキュアプログラミング②設計原則・実装原則	
22	セキュアプログラミング③脅威モデリング	
23	セキュアプログラミング④開発プロセス	
24	セキュアプログラミング⑤必要なセキュリティ機能	
25	ネットワーク構成事例①公開サーバー群をファイアウォールの外に置く場合	
26	ネットワーク構成事例②公開サーバー群をファイアウォールの中に置く構成	
27	ネットワーク構成事例③公開サーバーをファイアウォールの別ポートに設置する場合	
28	ネットワーク構成事例④ファイアウォールによって公開サーバー群を挟む構成	

情報セキュリティモデル・カリキュラム 24

学科：情報セキュリティの設計と構築	担当講師：
科目名：サイバー攻撃手法	授業回数：22 コマ（回）
科目概要：サイバー攻撃に関する詳細な攻撃手法について学習する。	
評価方法：	
前提知識：「セキュリティ基礎」で学んだ知識。	

回数	学習項目	備考
1	サイバー攻撃対策の考え方	
2	サイバー攻撃対策の種類①入口・出口対策	
3	サイバー攻撃対策の種類②多層防御	
4	マルウェアの動作内容と種類	
5	マルウェアへの対策	
6	不正アクセスの攻撃手法	
7	不正アクセスへの対策	
8	アプリケーションに対する攻撃手法	
9	アプリケーションへの攻撃対策	
10	主な攻撃手法①辞書攻撃、総当たり攻撃、パスワードリスト攻撃	
11	主な攻撃手法②クロスサイトスクリプティング、クロスサイトリクエストフォージェリ、クリックジャッキング	
12	主な攻撃手法③ドライブバイダウンロード、SQL インジェクション、ディレクトリトラバーサル	
13	主な攻撃手法④レインボーテーブル、サイドチャネル攻撃、ディレクトリリスティング、OS コマンドインジェクション	
14	主な攻撃手法⑤中間者攻撃、MITB 攻撃、第三者中継	
15	主な攻撃手法⑥DNS キャッシュポイズニング、DNS 水責め攻撃、IP スプーフィング	
16	主な攻撃手法⑦セッションハイジャック、セッション ID 固定化攻撃、リプレイ攻撃	
17	主な攻撃手法⑧DoS 攻撃、DDoS 攻撃、EDoS 攻撃、電子メール爆弾	
18	主な攻撃手法⑨標的型攻撃、APT、水飲み場型攻撃	
19	主な攻撃手法⑩フィッシング、ワンクリック詐欺、スミッシング	
20	主な攻撃手法⑪ゼロデイ攻撃、サイドチャネル攻撃	
21	主な攻撃手法⑫テンペスト攻撃、ポートスキャン	
22	主な攻撃手法⑬ダウングレード攻撃、フットプリンティング、SEO ポイズニング	

情報セキュリティモデル・カリキュラム 25

学科：情報セキュリティの設計と構築	担当講師：
科目名：サイバー攻撃対策	授業回数：17 コマ（回）
科目概要：実際の構築環境も想定しながら、サイバー攻撃に対する防御手法について学習する。後半では、具体的なケーススタディも行う。	
評価方法：	
前提知識：「サイバー攻撃手法」で学んだ知識。	

回数	学習項目	備考
1	主な防御手法①ファイアウォール	
2	主な防御手法②次世代ファイアウォール	
3	主な防御手法③IDS/IPS	
4	主な防御手法④エンドポイント	
5	主な防御手法⑤フィルタリング	
6	主な防御手法⑥WAF	
7	主な防御手法⑦DLP	
8	主な防御手法⑧UTM・SIEM	
9	さまざまなセキュリティ製品とセキュリティサービス	
10	サイバー攻撃ケーススタディ①情報漏洩	
11	サイバー攻撃ケーススタディ②脆弱性	
12	サイバー攻撃ケーススタディ③認証	
13	サイバー攻撃ケーススタディ④マルウェア	
14	サイバー攻撃ケーススタディ⑤フィッシング	
15	サイバー攻撃ケーススタディ⑥インターネットバンキング	
16	サイバー攻撃ケーススタディ⑦スマートフォン	
17	サイバー攻撃ケーススタディ⑧最新事例	

情報セキュリティモデル・カリキュラム 26

学科：情報セキュリティの設計と構築	担当講師：
科目名：セキュリティマネジメント	授業回数：25 コマ（回）
科目概要：ISMS の構築・運用について ISO/IEC27002 に沿って学習する。また、世界標準として浸透しつつある NIST サイバーセキュリティフレームワークの内容も把握する。	
評価方法：	
前提知識：「セキュリティ基礎」で学んだ知識。	

回数	学習項目	備考
1	情報セキュリティマネジメントの背景・用語	
2	リスクマネジメントの基本	
3	ISO31000 の概要	
4	情報セキュリティリスクのアセスメント手順	
5	ISO/IEC27001①概要	
6	ISO/IEC27001②組織の状況	
7	ISO/IEC27001③リーダーシップ	
8	ISO/IEC27001④計画	
9	ISO/IEC27001⑤支援	
10	ISO/IEC27001⑥運用	
11	ISO/IEC27001⑦パフォーマンス評価	
12	ISO/IEC27001⑧改善	
13	ISO/IEC27002①概要	
14	ISO/IEC27002②情報セキュリティ方針	
15	ISO/IEC27002③組織	
16	ISO/IEC27002④資産管理	
17	ISO/IEC27002⑤人的管理	
18	ISO/IEC27002⑥技術的管理	
19	ISO/IEC27002⑦物理的管理	
20	ISO/IEC27002⑧事業継続管理とコンプライアンス	
21	ISMS 適合性評価制度と情報セキュリティ監査制度	
22	セキュリティマネジメントの世界標準①NIST サイバーセキュリティフレームワーク	
23	セキュリティマネジメントの世界標準②NIST SP800	
24	セキュリティマネジメントの世界標準③NIST FIPS	
25	セキュリティマネジメント事例紹介	

情報セキュリティモデル・カリキュラム 27

学科：情報セキュリティの設計と構築	担当講師：
科目名：セキュアなシステム運用	授業回数：29 コマ（回）
科目概要：ファイアウォール等技術の運用上の注意点を押さえるとともに、セキュリティ監査・評価の要点及びデジタルフォレンジックの考え方から実践・応用的な知識を習得する。	
評価方法：	
前提知識：「セキュリティ基礎」「サイバー攻撃対策」「セキュリティマネジメント」で学んだ知識。	

回数	学習項目	備考
1	ファイアウォールの運用	
2	IDS/IPS の運用	
3	アンチウイルスソフトウェアの運用	
4	WAF の運用	
5	セキュリティ監査の体制	
6	セキュリティ監査の基準	
7	セキュリティ監査の技術・方法	
8	セキュリティ評価①概要	
9	セキュリティ評価②自己点検	
10	セキュリティ評価③情報セキュリティ対策ベンチマーク	
11	プライバシー影響評価（PIA）の実施手順	
12	インシデント対応の考え方	
13	インシデント対応の基本的なプロセス	
14	デジタルフォレンジックの概要と経緯	
15	デジタルフォレンジックの適用範囲と事例	
16	デジタルフォレンジックのプロセス	
17	デジタルフォレンジック運用上の注意点	
18	デジタルフォレンジックの実践①ネットワークからのデータ収集	
19	デジタルフォレンジックの実践②コンピュータからのデータ収集	
20	デジタルフォレンジックの実践③データ復元	
21	デジタルフォレンジックの実践④データ分析の基本	
22	デジタルフォレンジックの実践⑤ネットワークトラフィックの分析	
23	デジタルフォレンジックの実践⑥アプリケーションの分析	
24	デジタルフォレンジックの実践⑦オペレーティングシステムの分析	
25	デジタルフォレンジックの実践⑧ファイルシステムの分析	
26	デジタルフォレンジックの実践⑨スマートフォンのフォレンジック	
27	デジタルフォレンジックの応用①マルウェア解析	
28	デジタルフォレンジックの応用②脅威ハンティング	
29	デジタルフォレンジックの法的な有効性と事例	

令和２年度「専修学校による地域産業中核的人材養成事業」
Society5.0に対応した情報セキュリティ人材養成のモデルカリキュラム開発・実証事業

モデルカリキュラム

令和３年２月

一般社団法人全国専門学校情報教育協会
〒164-0003　東京都中野区東中野1-57-8　辻沢ビル3F
電話：03-5332-5081　FAX　03-5332-5083