３．３．８ 例示⑧：社会人学び直し向け短期（２週間程度）集中コース

（１）概要

本カリキュラムの概要を次表に示す。

表 55　例示⑧概要

大学における情報セキュリティ教育のためのモデル・コア・カリキュラム　例示⑧		
社会人学び直し：短期（２週間程度）集中コース向け		
種別		科目シラバス
想定する受講者		情報セキュリティの学び直しをしたい現役IT技術者（30代中～後半）
受講者の知識・スキル		産業界で情報系業務に従事している技術者を想定する
育成する人材像		習得した情報セキュリティに関する実践的知識・経験を自らの業務に活かせる人材
到達目標	コア部分	下記テーマについて、業務遂行に必要な知識を習得する。 （テーマ例） ・組織における標的型攻撃対策 ・ソフトウェアの設計・開発段階におけるセキュリティ対策 ・情報セキュリティマネジメントと情報セキュリティ監査 ・CSIRT運営 ・デジタルフォレンジック
	コア以外を含むカリキュラム全体	（コア部分と同じ）
関連科目との関係		以下の領域のうち、当該コース内容を理解する上で必要なものについて基本的な知識を有することを前提とする（募集要項等で明示） ・コンピュータネットワーク（TCP/IP、無線LAN） ・コンピュータアーキテクチャ ・オペレーティングシステム（Windows及びUNIX系） ・プログラミング言語（C言語、アセンブラ）
実施方法		講義及び演習

（２）科目構成例

CSIRT 構築と運営を担う技術者の育成のため、CSIRT 構築の手引き、ネットワークと Web アプリケーションの検査、デジタルフォレンジックの演習を組み合わせた 9 日間の集中コースの例を表 56～表 58 に示す。それぞれのコースは単独でも受講できる内容としている。

(1) CSIRT 構築の手引き　(2 日間)

(2) ネットワークと Web セキュリティ技術演習　（3 日間）

(3) デジタルフォレンジック演習（4 日間）

表 56　科目構成例(1)：CSIRT 構築の手引き

コース内容	企業組織などでインシデント対応を担う企業内 CSIRT の基本的な役割と活動の考え方、企業を脅かす攻撃とその防御策について学ぶコース。セキュリティインシデント対応の基本的なプロセス、および対応時に用いられる技術について、解説と演習を通して習得するほか、組織内でのインシデント対応組織（CSIRT）の立上げと運用、および CSIRT 連携の進め方についてケーススタディを通して学ぶ。また、現実に起きている攻撃手法のデモや Web サーバのログ解析演習を通して、サイバー攻撃によるインシデントの実例について学ぶ。

回数	講義内容	解説
1～4 （1 日）	CSIRT 基礎と実践	• 企業におけるセキュリティリスクへの取組の基本、事故前提の活動、CSIRT の役割、CSIRT の活動例 • CSIRT ケーススタディ • CSIRT インシデントハンドリングの基本 • CSIRT インシデントハンドリングの基礎演習実
5～8 （1 日）	CSIRT 技術演習	• 導入解説、最近のサイバーセキュリティ動向、攻撃手法のデモ • 代表的な Web サーバ（Apache）のログの解説、ログ解析演習 1（URL デコード）、ログ解析演習 2（SQL インジェクション）と解説 • 攻撃手法のデモ（Gumblar またはシェル奪取）、ログ解析演習 3（ブルートフォース）、ログ解析演習 4（ディレクトリトラバーサル）と解説 • 攻撃手法のデモ（クロスサイトスクリプティング）、ログ解析演習 5（クロスサイトスクリプティング）と解説、IDS/IPS 概説、まとめ

表 57　科目構成例(2)：ネットワークと Web セキュリティ技術演習

コース内容	Web サーバ、メールサーバ等の設置・運用に際して必要となる基礎的なセキュリティ技術の習得を狙いとして、検査ツールを利用したサーバに対するポートスキャン検査演習と脆弱性検査演習を行うとともに、発見された脆弱性を是正するための対策演習を行い、結果を報告書にまとめる演習を実施する。Web サーバの構築や運用に必要となる Web アプリケーションセキュリティ検査の知識及び技術を習得し、独力で Web アプリケーションセキュリティ検査を実施し、その結果に応じて必要な対処を提案できる基礎スキルを身につけることを狙いとする。具体的には、脆弱性を持つ Web サーバが設置された環境を利用し、主要な検査項目の演習を集中して行うとともに、対策の提案を含む検査結果報告書をまとめる演習を実施する。

回数	講義内容	解説
1～4 （1 日）	ネットワークセキュリティ技術	• オリエンテーション • ネットワークセキュリティ検査の概要 • ポートスキャン検査演習（nmap） • 脆弱性検査ツールの使用方法と脆弱性検査演習（Nessus） • 発見された脆弱性への対策演習と効果の確認 • 検査結果報告書作成と発表 • まとめ
5～12 （2 日）	Web アプリケーション検査	• オリエンテーション • Web アプリケーション検査の流れ • 入力パラメータの事前調査演習 • 入力検査演習 • セッション検査演習 • 強制ブラウジング検査演習 • 脆弱性対策の概説 • 検査結果報告書の作成とまとめ

表 58　科目構成例(3)：デジタルフォレンジック演習

コース内容	インシデント発生後の対処に必要となるデジタルフォレンジック技術の基礎を習得することを狙いとする。具体的には、デジタルフォレンジックの基礎知識・技術の解説、Windows 端末の解析で共通的に実施される基本的な作業に関する解説と実習、企業におけるインシデントを想定した本格的な解析演習を集中して行うとともに、結果を報告書にまとめる演習を実施する。

回数	講義内容	解説
1～4 （1日）	デジタルフォレジックの基礎	• オリエンテーション • デジタルフォレンジックとは • デジタルフォレンジックに必要な知識と作業の流れ • 各種オープンソース解析ツールの使い方
5～8 （1日）	予備演習：Windows パソコン利用者が行った操作を知り、その痕跡を調査	• ファイルシステムのタイムスタンプ • レジストリ • イベントログ • Web アクセス履歴 • USB デバイス接続履歴、等
9～16 （2日）	解析演習：ある企業からの情報漏えいの原因、影響範囲等を解析	• 情報漏えいの原因となった不正アクセス等の解析 • 情報漏えい経路の解析 • 不正アクセスに伴う影響範囲の解析、等 • 解析結果報告書の作成 • 振り返り：解析対象パソコンで起きていたことの解説

（3）適用条件

期間は必要な講義・演習数等に応じて調整することになる。

（4）産業界で用いられる指標等との対応

本カリキュラムで受講可能な科目と産業界で用いられるスキル分類との対応関係を次表に示す。

表 59　産業界で用いられる指標との対応（例示⑧）

記号凡例： ◎=演習を伴う実践的専門教育 〇=座学中心の専門教育 ◇=基礎的/入門的教育 ★=状況に応じてケースバイケース ※=習得済が受講の前提 緑色は[産]*及び[情]*で求めているスキル 水色縦線は[産]*のみで求めているスキル			iコンピテンショナリディクショナリのスキル分類												
			メソドロジ					テクノロジ							関連知識
			戦略	企画	実装	利活用	支援活動	システム	開発	保守・運用	非機能要件	組込み・計測・制御	共通技術	
SecBoK2016 知識項目	基礎	工学基礎									※	※	※	
		ICT 基礎		※	※			※	※	※	※	※	※	
		ビジネス基礎	※		※	※	※							※
	セキュリティ専門分野	セキュリティ基礎									※			
		セキュリティガバナンス					★							
		セキュリティマネジメント	★			★	★				★			
		ネットワークセキュリティ						★			★			
		システムセキュリティ		★				★	★		★			
		セキュアシステム設計・構築		★	★			★	★		★			
		セキュリティ運用			★	★	★	★		★	★			
		暗号・認証・電子署名									★			
		サイバー攻撃手法									★			
		デジタルフォレンジック									★			
		法・制度・標準				★	★				★			★

＊[産] 産業横断サイバーセキュリティ人材育成検討会「人材定義リファレンスに基づくスキルマッピング」が求めるスキル
[情] 情報処理安全確保支援士試験シラバスにおける要求される知識に対応するスキル

（５）実施上の工夫点

これまで社会人向け講座等を実施していない大学等で行う場合、まず短期のものから開始することが現実的と考えられる。実施方法の詳細については４．２．５に示す。

３．３．９ 例示⑨：社会人学び直し向け中期（３～６ヶ月程度）コース

（１）概要

本カリキュラムの概要を次表に示す。

表 60　例示⑨概要

大学における情報セキュリティ教育のためのモデル・コア・カリキュラム　例示⑨		
社会人学び直し：中期（３～6ヶ月程度）コース向け		
種別		科目シラバス
想定する受講者		情報セキュリティの学び直しをしたい現役IT技術者（30代中～後半）
受講者の知識・スキル		産業界で情報系業務に従事している技術者を想定する
育成する人材像		習得した情報セキュリティに関する実践的知識・経験を自らの業務に活かせる人材
到達目標	コア部分	下記の複数テーマに関する業務遂行に必要な知識を習得し、複合的な領域で構成される業務や脅威への対策に関する能力を得る。 （テーマ例） ・組織における標的型攻撃対策 ・ソフトウェアの設計・開発段階におけるセキュリティ対策 ・情報セキュリティマネジメントと情報セキュリティ監査 ・CSIRT運営 ・デジタルフォレンジック
	コア以外を含むカリキュラム全体	（コア部分と同じ）
関連科目との関係		以下の領域のうち、当該コース内容を理解する上で必要なものについて基本的な知識を有することを前提とする（募集要項等で明示） ・コンピュータネットワーク（TCP/IP、無線LAN） ・コンピュータアーキテクチャ ・オペレーティングシステム（Windows及びUNIX系） ・プログラミング言語（C言語、アセンブラ）
実施方法		講義及び演習

（２）科目構成例

企業の CSIRT 組織の構築および CSIRT のチームメンバ人材の育成を想定した科目構成例を表 61 に示す。この構成例では、座学主体の基礎講義 3 科目、応用科目 2 科目とハンズオン主体の演習科目（社会人学び直し向け短期集中コースの科目例と同じ）を 3～6 か月程度で学ぶことにより、受講する社会人が所属する企業の CSIRT の中核メンバとして活動するために役立つ能力を得ること目標としている。基礎講義と応用講義は、それぞれ 1 コマ（90 分）ずつの開講を予定しているが、演習科目は、演習の効率面から、2 日から 3 日程度の単位で集中開講とすることが望ましい。

表 61　科目構成例

科目	講義名・コマ数	解説
基礎講義 1	セキュアシステム構成論・15 コマ（各 90 分）	• 情報セキュリティ概論 • さまざまな事例から見るシステムの脆弱性 • 情報システムに到達する不正経路という視点で「セキュアな情報システムとは何か」ついて考察 • セキュリティポリシーという視点で、情報システム全体の構成要素について見ていくことで、セキュアなシステムをどのように構成するか整理する
基礎講義 2	セキュアプログラミングとセキュア OS・15 コマ（各 90 分）	• ソフトウェアの脆弱性 • 設計レベルの問題と実装レベルの問題 • バッファオーバーフロー攻撃の仕組みと防御策 • Web アプリケーションの脆弱性 • 隔離実行、サンドボックス • セキュア OS とアクセス制御
基礎講義 3	ネットワークシステム設計・運用管理・15 コマ（各 90 分）	• ネットワーク設計のための理論（待ち行列理論、トラヒック理論、グラフ理論、信頼性理論） • ネットワークサービス • VLAN と VPN • 企業ネットワーク構築と運用管理の概要 • ネットワークセキュリティ対策技術 • 仮想ネットワーク技術とクラウド、SDN
基礎講義 4	インターネットテクノロジ・15 コマ（各 90 分）	• インターネットの生い立ちと発展の経緯、標準化 • ネットワークアーキテクチャ、ネットワークトポロジ、ネットワークの分類 • LAN 技術（イーサネット、衝突制御、誤り制御、フロー制御） • 無線 LAN、ダイヤルアップ接続 • IP アドレス、アドレス変換、アドレス解決、IPv4 パケット • ルーティング • TCP と UDP、再送制御、輻輳制御 • DHCP、DNS、FTP

科目	講義名・コマ数	解説
		• WWW、電子メール、P2P ファイル交換 • セキュリティプロトコル（IPsec、SSL） • 監視・管理（ICMP、SNMP） • IPv6（IPv6 パケット、IPv4 からの移行） • IP 電話（SIP、音声品質） • QoS（Intserv、Diffserv、キューイング） • マルチキャスト
演習	CSIRT 構築と運営 （詳細は表 56～表 58 参照）	• CSIRT 構築の手引き (2 日間・8 コマ・各 90 分) • ネットワークと Web セキュリティ技術演習 （3 日間・12 コマ・各 90 分） • デジタルフォレンジック演習（4 日間・16 コマ・各 90 分）
応用講義 1	ハッキングとマルウェア・15 コマ（各 90 分）	• 偵察とソーシャルエンジニアリング • スキャンと脆弱性識別 • システムハッキング • トロイの木馬，バックドア，ウィルス，ワーム • スニッファ • マルウェアの概要と作成 • マルウェア解析環境構築、マルウェア収集、表層解析 • アセンブラの基礎とプログラミング • バイナリファイルの構成 • 動的解析、静的解析、アンチ解析技術
応用講義 2	組織行動と情報セキュリティ・15 コマ（各 90 分）	• 組織の定義と組織行動論の枠組み • モチベーションと組織への貢献 • 組織コミットメントと組織の成果 • 集団のダイナミクス • リーダーシップの役割 • 組織文化の概念と機能、形成と変革 • 組織学習：不完全な組織学習をもたらす要因 • 意思決定のバイアス • 意思決定の課題と改善 • 危機管理組織のマネジメント

科目	講義名・コマ数	解説
		• 企業事故･不正行動の事例研究 • 組織変革の立案と策定

（３）適用条件

期間は必要な講義・演習数等に応じて調整することになる。

（４）産業界で用いられる指標等との対応

例示⑧に準じる。

（５）実施上の工夫点

本カリキュラムは、情報セキュリティ分野に関するさまざまな領域の専門的知識を備えた人材を多数擁する高等教育機関での実施を前提とする。

上記の基礎講義や応用講義をコンパクトに実施する場合は、例示⑤で示した科目構成例（１）を活用することも検討に値する。

３．３．１０ 例示⑩：社会人学び直し向け長期（１年程度）コース

（１）概要

本カリキュラムの概要を次表に示す。

表 62　例示⑩概要

大学における情報セキュリティ教育のためのモデル・コア・カリキュラム　例示⑩		
社会人学び直し：長期（１年程度）コース向け		
種別		カリキュラム
想定する受講者		情報セキュリティの学び直しをしたい現役IT技術者（30代中～後半）
受講者の知識・スキル		産業界で情報系業務に従事している技術者を想定する
育成する人材像		習得した情報セキュリティに関する実践的知識・経験を自らの業務に活かせる人材
到達目標	コア部分	産業界で技術者として活躍する際に知っておくべき情報セキュリティの考え方について、脅威の特徴や対策に用いられる要素技術に関する専門的内容を座学と演習の組み合わせを通じて体系的に理解する。
	コア以外を含むカリキュラム全体	コア部分の知識の種類を拡張した形で、より幅広い脅威や対策技術について体系的に理解する。
関連科目との関係		以下の領域について基本的な知識を有することを前提とする（募集要項等で明示） ・コンピュータネットワーク（TCP/IP、無線LAN） ・コンピュータアーキテクチャ ・オペレーティングシステム（Windows及びUNIX系） ・プログラミング言語（C言語、アセンブラ）
実施方法		講義及び演習

（２）科目構成例

表 63　科目構成例（仮）

学年	講義	演習等
理論系	暗号理論、暗号・認証と社会制度、アルゴリズム基礎、数論基礎、計算代数、統計的方法論	
技術系	暗号プロトコル、インターネットテクノロジ、不正アクセス技法、ネットワークシステム設計・運用管理、セキュアシステム構成論、情報デバイス技術、情報システム構成論、オペレーティングシステム、セキュアプログラミングとセキュアOS、ソフトウェア構成論、ペネトレーション技法、統計的リスク管理、個人識別とプライバシー保護	プログラミング実習、 セキュアシステム実習、 ネットワークセキュリティ技術演習、 Webアプリケーションと脆弱性対策演習、 デジタルフォレンジック演習
マネジメント系	情報セキュリティマネジメントシステム、セキュリティシステム監査、セキュリティ管理と経営、リスクマネジメント、組織行動と情報セキュリティ、セキュア法制と情報倫理、法学基礎、知的財産制度、国際標	インシデント対応とCSIRT基礎演習、 組織経営とセキュリティマネジメント演習、 事業継続マネジメント演習

	準とガイドライン、セキュリティの法律実務、リスクの経済学、マスメディアとリスク管理	
その他	情報セキュリティ特別講義	情報セキュリティ輪講

（３）適用条件

受講者のニーズや大学側のポテンシャルに応じて、期間やカリキュラム内容を削減する可能性について考慮することが望ましい。

（４）産業界で用いられる指標等との対応

本カリキュラムで受講可能な科目と産業界で用いられるスキル分類との対応関係を次表に示す。

表 64　産業界で用いられる指標との対応（例示⑩）

記号凡例： ◎=演習を伴う実践的専門教育 〇=座学中心の専門教育 ◇=基礎的/入門的教育 ★=状況に応じてケースバイケース ※=習得済が受講の前提 緑色は[産]*及び[情]*で求めているスキル 水色縦線は[産]*のみで求めているスキル			iコンピテンショナリディクショナリのスキル分類												
			メソドロジ					テクノロジ							関連知識
			戦略	企画	実装	利活用	支援活動	システム	開発	保守・運用	非機能要件	組込み・計測・制御	共通技術	
SecBoK2016 知識項目	基礎	工学基礎									※	※	※	
		ICT 基礎		※	※			※	※	※	※	※	※	
		ビジネス基礎	※		※	※	※							※
	セキュリティ専門分野	セキュリティ基礎									※			
		セキュリティガバナンス					★							
		セキュリティマネジメント	★			★	★				★			
		ネットワークセキュリティ						★			★			
		システムセキュリティ		★				★	★		★			
		セキュアシステム設計・構築		★	★			★	★		★			
		セキュリティ運用			★	★	★	★		★	★			
		暗号・認証・電子署名									★			
		サイバー攻撃手法									★			
		デジタルフォレンジック									★			
		法・制度・標準				★	★				★			★

＊［産］産業横断サイバーセキュリティ人材育成検討会「人材定義リファレンスに基づくスキルマッピング」が求めるスキル
［情］情報処理安全確保支援士試験シラバスにおける要求される知識に対応するスキル

（５）実施上の工夫点

社会人にとっては受講負荷が大きいため、修士課程と同レベルの内容を課す場合であっても負荷軽減について配慮することが望ましい。また、講義内容等を理解する上で必要となる基盤技術に関する知識は受講者において偏りがあるのが一般的であるので、以下のような工夫を行うこと

が求められる。

- 予め受講者を対象にアンケートを実施し、下記の各技術に関する経験や理解度などを尋ねる：
  ーコンピュータの構造、オペレーティングシステムの機能、ソフトウェアの動作原理
  ーTCP/IP に基づく通信原理、ルータ、スイッチ等の役割、無線 LAN の仕組み
  ープログラミング言語、アセンブラ言語による開発経験
- 講義を実施する際の受講者との会話を通じて内容を調整する（少人数での実施の場合）