情報学を専門とする学科対象の

教育カリキュラム標準の策定及び提言

Cyber Security

目次

WG 構成

寺田真敏(委員長)	中央大学
上原哲太郎	立命館大学
大久保隆夫	情報セキュリティ大学院大学
菊池浩明	明治大学
齋藤孝道	明治大学
佐藤直	情報セキュリティ大学院大学
西垣正勝	静岡大学
平山敏弘	NPO 日本ネットワークセキュリティ協会

1. はじめに

情報専門学科カリキュラム標準 J17 では、サイバーセキュリティを側面別カリキュラム標準と位置付けている。本報告では、サイバーセキュリティ教育を取り巻く状況とともに、「一般教育レベル」「セキュリティ基礎レベル」「セキュリティ専門レベル」の 3 段階に分類した参考となるカリキュラムについて述べ、今後の取り組みを概説する。

2. サイバーセキュリティ教育を取り巻く状況

日本では IT 人材とサイバーセキュリティ人材の不足が指摘されており、2016 年 3 月に、内閣サイバーセキュリティセンターからも「サイバーセキュリティ人材育成総合強化方針」が発表されている状況にある。国内産業界においては、2015 年 2 月に経団連から「サイバーセキュリティ対策の強化に向けた提言」が公開され、産業界として具体的な取り組みを進めるため、翌 2015 年 6 月には「産業横断サイバーセキュリティ人材育成検討会」を発足させている。さらに、サイバーセキュリティにかかるインシデントに対処する体制であるシーサート(CSIRT)に求められる人材、セキュリティ知識分野(SecBoK)人材スキルマップの作成や産業サイバーセキュリティセンターの人材育成事業など、産業界で求められる人材を育成していくための様々な取り組みが行われている。このような状況を踏まえ、国内学術界においては、2016 年度理工系プロフェッショナル教育推進委託事業工学分野における理工系人材育成の在り方に関する調査研究において、「高等教育機関における情報セキュリティ教育実施のためのモデル・コア・カリキュラムの策定」が進められてきている。

J17 サイバーセキュリティ WG では、このような流れを受け、求められる人材像を明らかにすること、その人材に必要となるスキルを明らかにすること、スキルに関してレベル分けをすることが、ニーズを踏まえたカリキュラム作成などサイバーセキュリティ教育を進めるために有効であろうと考え調査を行った。

2.1. シーサート(CSIRT)に求められる人材

求められる人材像については、日本シーサート協議会が作成したシーサート(CSIRT)に求められる人材像を参考とした。シーサート(CSIRT: Computer Security Incident Response Team)は、サイバーセキュリティにかかるインシデントに対処するための組織の総称であり、インシデント関連情報、脆弱性情報、攻撃予兆情報を収集、分析し、対応方針や手順の策定などの活動を役割としている。国内シーサートの団体である日本シーサート協議会では、シーサートに求められる人材をその役割と共に明示しており(表 1)[1]、サイバーセキュリティ人材のベースとなるモデルとして、セキュリティ知識分野(SecBoK)人材スキルマップ

などで参照されている。

[1] CSIRT 人材の定義と確保

http://www.nca.gr.jp/activity/training-hr.html

表 1　シーサートに求められる人材

名称	役割
CSIRT 責任者、CSIRT 全体統括、コマンダー	自組織で起きているセキュリティインシデントの全体統制を行う。重大なインシデントに関しては CISO や経営層との情報連携を行う。また、CISO や経営者が意思決定する際の支援を行う。
連絡/調整担当、自組織外・自組織内連絡担当、IT 部門調整担当	社外窓口として、JPCERT/CC、NISC、警察、監督官庁、NCA、他 CSIRT 等との連絡窓口となり、情報連携を行う。 社内窓口として、IT 部門、法務、渉外、IT 部門、広報、各事業部等との連絡窓口となり、情報連携を行う。
トリアージ担当、優先順位選定担当	発生している事象に対して優先順位を決定する。被害がある場合の復旧優先順位や、拡散している場合にはどのシステムから停止していくべきか等の判断を行う。
インシデントマネジャー、インシデント管理担当	インシデントハンドラーに指示を出し、インシデントの対応状況を把握する。対応履歴を管理するとともにコマンダーへ状況を報告する。
インシデントハンドラー、インシデント処理担当	インシデントの処理を行う。セキュリティベンダーに処理を委託している場合には指示を出して連携し、管理を行う。状況はインシデントマネージャーに報告する。
ノーティフィケーション担当、組織内情報発信担当、自組織内調整・情報発信担当	自組織内を調整し、各関連部署への情報発信を行う。自組織システムに影響を及ぼす場合には IT 部門と調整を行う。
リサーチャー、情報収集担当	セキュリティイベント、脅威情報、脆弱性情報、攻撃者のプロファイル情報、国際情勢の把握、メ

名称	役割
	ディア情報などを収集し、キュレーターに引き渡す。単独機器の分析は行うが、相関的な分析はしない。
キュレーター、情報分析担当	リサーチャーの収集した情報を分析し、その情報を自組織に適用すべきかの選定を行う。リサーチャーと合わせて SOC(セキュリティオペレーションセンター)で実施することが多い。
セルフアセスメント担当、影響評価担当	自組織環境や情報資産の現状分析を行う。平常時の際にアセスメントを実施しておき、インシデント発生時にはアセスメント結果に基づいて影響範囲を特定する。
フォレンジック担当	システム的な鑑識、精密検査、解析、報告を行う。悪意のある者は証拠隠滅を図ることもあるため、証拠保全とともに、消されたデータを復活させ、足跡を追跡することも要求される。
インベスティゲーター､犯罪/不正調査担当	外部からの犯罪、内部犯罪の解決に向け調査する。セキュリティインシデントはシステム障害とは異なり、悪意のある者が存在する。通常の犯罪捜査と同様に、動機の確認や証拠の確保、次に起こる事象の推測などを詰めながら論理的に調査対象を絞っていくことが要求される。

2.2. セキュリティ知識分野(SecBoK)人材スキルマップ

人材に必要となるスキルについては、日本ネットワークセキュリティ協会が作成したセキュリティ知識分野(SecBoK)人材スキルマップを参考とした。セキュリティ知識分野(SecBoK)人材スキルマップでは、セキュリティ知識分野の項目を規定すると共に(表 2)、情報セキュリティサービスベンダにおける人材についてはセキュリティ専門会社が定義する職種と、ユーザ企業における人材については、シーサートに求められる人材との対応付けをしている[2]。この紐付けを利用することで、サイバーセキュリティ人材で必要となるセキュリティ知識分野の項目を概観できる。

[2] セキュリティ知識分野(SecBoK)人材スキルマップ 2017 年版

http://www.jnsa.org/result/2017/skillmap/index.html

表 2　セキュリティ知識分野(SecBoK)人材スキルマップの項目

分野	大項目	中項目	小項目
基礎	ICT 基礎	情報理論	情報理論に関する知識、一般的なエンコード技術の識別に関するスキル
		計算機ハードウェア	マイクロプロセッサに関する知識、マンマシンインタラクションの原理に関する知識、計算機アーキテクチャに適用される電子工学(回路ボード、プロセッサなど
		ネットワークインフラ	計算機ネットワークの基礎に関する知識、組織のLAN/WANの経路に関する知識、LAN と WAN の原理とコンセプトに関する知識、ネットワーク設計プロセスに関する知識など
		通信プロトコル・サービス	ネットワーク通信を提供するために、ネットワークサービスとプロトコルがどのように作用するかに関する知識、ネットワークアクセス、識別及びアクセス管理に関する知識など
		データ構造	データ管理とデータ標準化に関するポリシーと標準に関する知識、複雑なデータ構造に関する知識、データマイニングとデータウェアハウスの原理に関する知識など
		データベース	データベース理論に関する知識、データベース管理システム、問い合わせ言語、テーブル関係及びビューに関する知識、データベースシステムに関する知識など
		ナレッジマネジメント	ナレッジマッピング(ナレッジリポジトリのマップ)の実施に関するスキル、ナレッジマネジメント技術の利用に関するスキル
		アルゴリズムとプログラミング	計算機アルゴリズムに関する知識、計算機プログラミングの原則に関する知識、低レベル言語に関する知識、プログラミング言語の構造とロジックに関する知識など
		オペレーティングシステム	オペレーティングシステムに関する知識、サーバとクライアントの OS に関する知識、適用可能なシステム構成要素の識別、修正及び操作に関するスキルなど
		ソフトウェア	ソフトウェア工学に関する知識、ソフトウェアの構成と最適化に関するスキル、ソフトウェア設計ツール、手法及び技法に関する知識、ソフトウェアの品質保証プロセスに関する知識など

分野	大項目	中項目	小項目
		システム開発	システム開発のコンセプトに関するスキル、ソフトウェアのデバッグ原理に関する知識、ソフトウェアのデバッグの実施に関するスキル、デバッグ手続きとツールに関する知識など
		システム運用	システム運用のコンセプトに関するスキル、システム管理のコンセプトに関する知識、サーバ管理とシステム工学の理論、コンセプト及び手法に関する知識など
		エンタープライズアーキテクチャ	エンタープライズ IT アーキテクチャに関する知識､組織のエンタープライズ IT のゴールと目的に関する知識、情報技術のアーキテクチャコンセプトとフレームワークに関する知識など
		アプリケーションとサービス	仮想化技術と仮想マシンの開発と保守に関する知識、仮想マシンの利用に関するスキル、企業内メッセージングシステムと関連するソフトウェアに関する知識など
		その他	計算機の基本的操作に関するスキル、ディジタル著作権管理に関する知識、個人識別情報と PCIDSS に関する知識、ITSS レベル 2 程度の基礎的な IT リテラシー
	工学基礎		16 進データの読解に関するスキル､プロセス工学のコンセプトに関する知識、システムエンジニアリングプロセスに関する知識、全 5 レベルにおける CMMI に関する知識など
	ビジネス基礎		組織の評価と検証に関する要件に関する知識、組織のデータ資産のソース、特徴及び利用に関する知識、顧客組織の適用可能なビジネスプロセスと運用に関する知識など
セキュリティ基礎	総論		情報セキュリティシステム工学の原理に関する知識、機密性、完全性、可用性、認証及び否認防止に関連する情報保証の原理と組織要件に関する知識など
セキュリティガバナンス	総論		組織の企業情報セキュリティアーキテクチャシステムに関する知識、インテリジェンスの報告原理、方針、手続き及び手段、組織のリスク受容および/またはリスク管理のアプローチに関する知識
セキュリティマネジメント	総論		セキュリティマネジメントに関する知識、システムセキュリティの目的を反映したポリシーの作成に関するスキル、情報保証の原理と信条に基づくセキュリティ管理策の設計に関するスキルなど

分野	大項目	中項目	小項目
ネットワークセキュリティ	総論		ネットワーク通信のセキュア化に関するスキル、何がネットワーク攻撃及び脅威と脆弱性の双方への関係を構成するかに関する知識、脆弱性とシステム内の設定情報に基づくシステム的なセキュリティ問題を識別する能力など
	トラフィック解析		ネットワークトラフィック解析手法に関する知識、パケットレベル解析に関する知識、適切なツールを用いたパケットレベル解析の実施に関するスキルなど
	侵入検知		IDS ツールとアプリケーションに関する知識、IDS のハードウェアとソフトウェアの種類に関する知識、侵入検知技術によるホストならびにネットワークベースの侵入の検知に関するスキルなど
	脆弱性診断		脆弱性診断に関する基礎知識、ペネトレーションテストの原理、ツール及び技術に関する知識、警告、アドバイザリ及び報告書から得られる既知の脆弱性に関する知識など
	フィルタリング		ウェブフィルタリング技術に関する知識
	アクセス制御		ポリシーベースとリスクに適応できるアクセス制御に関する知識、ホスト／ネットワークのアクセス制御に関する知識など
	VPN		VPN セキュリティに関する知識、VPN 装置と暗号化の利用に関するスキル
	深層防御		深層防御の原理とネットワークセキュリティアーキテクチャに関する知識
システムセキュリティ	総論		アプリケーションの脆弱性に関する知識、システムとアプリケーションのセキュリティ上の脅威と脆弱性に関する知識、システムとアプリケーションのセキュリティ上の脅威と脆弱性など
セキュアシステム設計・構築	総論		ソフトウェアのセキュリティとユーザビリティを含む、システムライフサイクルマネジメントの原理に関する知識、セキュアな構成管理技術に関する知識、特定したセキュリティリスクについての対策の設計に関するスキルなど
	セキュアプログラミング		ソフトウェア開発に適用するための情報保証の原理と手法に関する知識、セキュアコーディング技術に関する知識、ソフトウェア関連の情報技術のセキュリティに関する原理と手法に関する知識など

分野	大項目	中項目	小項目
	テスト		ソフトウェアリリースにおける品質保証プロセスへのブラックボックスセキュリティテストツールの統合に関するスキル、セキュアテスト計画の設計に関するスキルなど
セキュリティ運用	総論		運用上のセキュリティに関する知識、新興の情報技術と情報セキュリティ技術に関する知識、システム診断ツールと障害識別技法に関する知識など
	インシデント対応		インシデントのカテゴリ、インシデントレスポンス及び応答のタイムラインに関する知識、インシデントレスポンスとハンドリングの方法論に関する知識など
	その他		内部不正の検出、報告、検出ツール及び法規制に関する知識と経験、セキュアな取得に関する知識、セキュリティイベント(事象)の相関ツールに関する知識
暗号・認証・電子署名	総論		暗号化アルゴリズムに関する知識、暗号に関する知識、暗号化手法に関する知識、アクセス時の認証手法に関する知識、一方向性ハッシュ関数(に関するスキル
サイバー攻撃手法	総論		現在及び新興の脅威/攻撃手法に関する知識、攻撃者に悪用される可能性のある新興のコンピュータベースの技術に関する知識、一般的な攻撃ステージに関する知識など
	マルウェア		マルウェアの取扱いに関するスキル、マルウェアからのネットワークの保護に関するスキル、マルウェア解析のコンセプトと手法に関する知識、マルウェア解析ツールに関する知識
	その他		正常な動作に見せかける振る舞いに関するスキル、ソーシャルエンジニアリング技術の利用に関するスキル、Windows または Unix/Linux 環境におけるハッキング手法に関する知識など
デジタルフォレンジクス	総論		デジタルフォレンジクス用データの処理に関する基本コンセプトと実践に関する知識、標準の運用手続きまたは国内標準に基づいて証拠の完全性を維持するスキルなど
法・制度・標準	総論		業界標準かつ組織的に受け入れられる解析原理と手法に関する知識、プライバシー影響評価(PIA)に関する知識、システム設計に関係するシステムソフトウェアならびに組織設計標準など

2.3. スキルに関するレベル分け

スキルに関するレベル分けについては、平成 28 年度理工系プロフェッショナル教育推進委託事業 工学分野における理工系人材育成の在り方に関する調査研究(情報セキュリティ人材育成)[3]などを参考にして、3 段階の分類を利用することとした(表 3)。

表 3　スキルに関するレベル分け

レベル		内容
一般教育レベル		一般教養としての情報セキュリティに関する知識を備え、適切な判断ができる人材を対象とするもの
専門レベル	〈基礎〉 セキュリティ基礎	情報セキュリティに関する基礎的な知識・経験と意識を身につけたい人材を対象とするもの
	〈応用〉 セキュリティ専門	習得した知識・実践的経験を自らの専門分野のセキュリティ対策に活かせる人材を対象とするもの

[3] 平成 28 年度理工系プロフェッショナル教育推進委託事業 工学分野における理工系人材育成の在り方に関する調査研究(情報セキュリティ人材育成に関する調査研究)
http://www.mext.go.jp/a_menu/koutou/sangaku2/1387701.htm

3.　サイバーセキュリティのカリキュラム作成の支援

サイバーセキュリティを側面別カリキュラム標準と位置付けていることから、サイバーセキュリティのカリキュラム作成に参考となるよう調査結果をまとめた。

3.1. 各情報専門教育との対応

カリキュラムモデルにまず必要となるのは、教えるべき知識項目の整理である。そこで、サイバーセキュリティのカリキュラム作成の際に参考となる、セキュリティ知識分野(SecBoK)人材スキルマップにおける各情報専門教育がカバーする範囲と表 3 の専門レベルを対象としたレベル分けを整理した(表 4)。なお、専門レベルの前提知識の項目については、ICT 基礎として分類している。

表 4　各情報専門教育との対応とレベル分け

分野｜大項目｜中項目	CS	IS	CE	SE	IT	GE	CyS ICT 基礎	CyS セキュリティ基礎	CyS セキュリティ専門
基礎|ICT 基礎|情報理論	●			●	●	●	●		
基礎|ICT 基礎|計算機ハードウェア	●	●		▲	●		●		
基礎|ICT 基礎|ネットワークインフラ	●	●		▲	●	●	●		
基礎|ICT 基礎|通信プロトコル・サービス	●	●		▲	●	●	●		
基礎|ICT 基礎|データ構造	●	●		▲	▲		●		
基礎|ICT 基礎|データベース	●	●		▲	●	●	●		
基礎|ICT 基礎|ナレッジマネジメント	●	●		▲	▲	●	●		
基礎|ICT 基礎|アルゴリズムとプログラミング	●			●	●	●	●		
基礎|ICT 基礎|オペレーティングシステム	●	●		▲	●	●	●		
基礎|ICT 基礎|ソフトウェア	●	●		●	●	●	●		
基礎|ICT 基礎|システム開発	●			●	●	●	●		
基礎|ICT 基礎|システム運用	▲	●		▲	●	●	●		
基礎|ICT 基礎|エンタープライズアーキテクチャ	▲	●		×	●		●		
基礎|ICT 基礎|アプリケーションとサービス	●			▲	●		●		
基礎|ICT 基礎|その他	▲	●		▲	●	●	●		
基礎|工学基礎|	●			●		●	●		
基礎|ビジネス基礎|	×	●		▲	▲				
セキュリティ基礎|総論|	●	●	●	●	●	●		●	
セキュリティガバナンス|総論|		●	▲	▲	●				●
セキュリティマネジメント|総論|	▲	●	●	▲	●				●
ネットワークセキュリティ|総論|	●		●	▲	●	●		●	
ネットワークセキュリティ|トラフィック解析|	▲		▲	▲	●				●
ネットワークセキュリティ|侵入検知|	▲		▲	▲	●				●

分野｜大項目｜中項目	CS	IS	CE	SE	IT	GE	CyS ICT 基礎	CyS セキュリティ基礎	CyS セキュリティ専門
ネットワークセキュリティ｜脆弱性診断｜	▲		▲	●	●				●
ネットワークセキュリティ｜フィルタリング｜	▲		●	▲	●			●	
ネットワークセキュリティ｜アクセス制御｜	▲		●	▲	●			●	
ネットワークセキュリティ｜VPN｜	▲		●	▲	●			●	
ネットワークセキュリティ｜深層防御｜	▲		×	▲	▲				●
システムセキュリティ｜総論｜	▲		●	●	●	●		●	
セキュアシステム設計・構築｜総論｜	●		×	●	●				●
セキュアシステム設計・構築｜セキュアプログラミング｜	●		×	●	●			▲	●
セキュアシステム設計・構築｜テスト｜	●		×	●	●				●
セキュリティ運用｜総論｜	▲		●	▲	●				●
セキュリティ運用｜インシデント対応｜	▲		●	×	●				●
セキュリティ運用｜その他｜	×	●	▲	×	▲				●
暗号・認証・電子署名｜総論｜	●		●	●	●			●	
サイバー攻撃手法｜総論｜	●		●	●	●			▲	●
サイバー攻撃手法｜マルウェア｜	●		●	▲	●			▲	●
サイバー攻撃手法｜その他｜	▲		×	▲	●				●
デジタルフォレンジクス｜総論｜	●		▲	×	●				●
法・制度・標準｜総論｜	▲		●	▲	▲				●

●：実施すべき

▲：実施すると良い

×：実施の必要はない

3.2. モデル・コア・カリキュラム

サイバーセキュリティのカリキュラム作成において参考となるモデルカリキュラムについては、平成 28 年度理工系プロフェッショナル教育推進委託事業 工学分野における理工

系人材育成の在り方に関する調査研究(情報セキュリティ人材育成)[3]のモデル・コア・カリキュラムを一般教育、セキュリティ基礎、セキュリティ専門レベル分けをし、整理し直した(表 5)。詳細については、参考情報を参照のこと。

表 5　モデル・コア・カリキュラム：レベルによる分類

レベル		モデル・コア・カリキュラム
一般教育		例示①：一般教養としての情報セキュリティに関する講義を対象とするもの
セキュリティ基礎		例示②：学士課程卒業後就職を予定している理工系学生等を対象とするもの
		例示③：情報セキュリティを専門とする学科等を対象とするもの
セキュリティ専門	学生	例示④：修士課程に進学予定の情報系学士課程の学生を対象とするもの
		例示⑤：情報セキュリティに関する単独の科目を対象とするもの
		例示⑥：専門とは別に情報セキュリティを学ぶコース等を対象とするもの
		例示⑦：情報セキュリティを専門とする専攻等を対象とするもの
	社会人学生	例示⑧：社会人学び直し向け短期(2 週間程度)集中コース
		例示⑨：社会人学び直し向け中期(3～6 ヶ月程度)コース
		例示⑩：社会人学び直し向け長期(1 年程度)コース

3.3. 既存カリキュラム

サイバーセキュリティのカリキュラム作成において、既存カリキュラムも参考になると考え、表 6 に示す視点から整理をした。詳細については、参考情報を参照のこと。

表 6　既存カリキュラムの整理テンプレート

テンプレート名	概要
レベル分類	既存カリキュラムのレベルを一般教育、セキュリティ基礎、セキュリティ専門に分類する。
属性項目	既存カリキュラムの具体的なカリキュラムの例示として、属性項目のテンプレートに沿って例示する。

表 7　レベル分類テンプレート

レベル	授業科目名	学部/学科	想定対象年度	単位数	講義/演習	必修/選択	備考
一般教育	情報セキュリティ論	商学部	学部 3,4 年	2 単位	講義	選択	
	：	：	：	：	：	：	
セキュリティ基礎	情報セキュリティ技術	理工学部	修士 1 年	2 単位	講義	選択	
	：	：	：	：	：	：	
セキュリティ専門	暗号理論	理工学部	修士 1 年	2 単位	講義	選択	
	：	：	：	：	：	：	

表 8　属性項目テンプレート

項目	内容
大学名	○○大学
レベル	セキュリティ基礎
授業科目名	ネットワークセキュリティ
学部/学科	△△学部
想定対象年度	修士 1 年
単位数	2 単位
講義/演習	講義
必修/選択	必修
目的	ネットワークにおける脅威の理解およびネットワークセキュリティ基礎技術の習得
授業の概要	セキュアな情報システムを構成するにあたって念頭に置くべき、基本的なネットワークセキュリティを習得する。
授業計画と内容	1 イントロダクション、ネットワーク社会に潜む危険の認識 2 ネットワークアーキテクチャとセキュリティ 3 TCP/IP とセキュリティ(1)特別な意味を持つ IP アドレス 4 TCP/IP とセキュリティ(2)経路制御 ：

4.　おわりに

本報告では、サイバーセキュリティ教育を取り巻く状況、サイバーセキュリティのカリ

キュラム作成の支援について概説した。特に、サイバーセキュリティ教育を取り巻く状況として、産業界を中心に、求められる人材像を明らかにすること、その人材に必要となるスキルを明らかにすることが、シーサートに求められる人材、セキュリティ知識分野(SecBoK)人材スキルマップという形で具体化されている。今後の取り組みとしては、サイバーセキュリティのカリキュラム作成の支援と、シーサートに求められる人材、セキュリティ知識分野(SecBoK)人材スキルマップのような具体的な事例との繋がり作っていくことで、情報学を専門とする学科対象の教育カリキュラムと産業界との繋がりを作っていくことである。

5. 参考情報

5.1. モデル・コア・カリキュラム

モデル・コア・カリキュラムの付録では、レベル分けしたモデル・コア・カリキュラムの概要を紹介する。

付表 1　モデル・コア・カリキュラム：レベルによる分類

レベル		モデル・コア・カリキュラム	カリキュラムの概要
一般教育		例示①：一般教養としての情報セキュリティに関する講義を対象とするもの	付表 2
セキュリティ基礎		例示②：学士課程卒業後就職を予定している理工系学生等を対象とするもの	付表 3
		例示③：情報セキュリティを専門とする学科等を対象とするもの	付表 4
セキュリティ専門	学生	例示④：修士課程に進学予定の情報系学士課程の学生を対象とするもの	付表 5
		例示⑤：情報セキュリティに関する単独の科目を対象とするもの	付表 6
		例示⑥：専門とは別に情報セキュリティを学ぶコース等を対象とするもの	付表 7
		例示⑦：情報セキュリティを専門とする専攻等を対象とするもの	付表 8
	社会人	例示⑧：社会人学び直し向け短期(2 週間程度)	付表 9

	学生	集中コース	
		例示⑨：社会人学び直し向け中期(3～6 ヶ月程度)コース	付表 10
		例示⑩：社会人学び直し向け長期(1 年程度)コース	付表 11

付表 2　一般教育レベル

例示①：一般教養としての情報セキュリティに関する講義を対象とするもの

情報セキュリティリテラシー教育向け		
種別		科目シラバス
想定する受講者		学士課程の新入生(1 年次・学部問わず)
受講者の知識･スキル		普通科高校卒業程度の知識・スキルを想定する
育成する人材像		日常の社会生活を営む上で必要となる情報セキュリティに関する知識を備え、適切な判断ができる人材
到達目標	コア部分	以下の 5 点について理解する。 ①情報セキュリティをなぜ考える必要があるか ②情報倫理と著作権に関して遵守すべき事項 ③代表的な脅威がもたらす影響と対策のための技術や仕組み ④情報セキュリティに関する法律や制度 ⑤情報社会においてセキュリティとして留意すべきこと
	コア以外を含むカリキュラム全体	(コア部分と同じ内容の詳細化)
関連科目との関係		・本科目受講に先立って受講しておくべき科目はなし ・リテラシー科目として以下の①②のいずれかの指定を推奨： ①全学生必修 ②情報処理関連の演習または情報セキュリティ専門科目の受講には本科目の単位取得を要件とする
実施方法		講義または e ラーニング教材自習

付表 3　セキュリティ基礎レベル

例示②：学士課程卒業後就職を予定している理工系学生等を対象とするもの

就職を予定している学士課程在籍者を対象とする情報セキュリティ分野の実践講座向け

種別		科目シラバス
想定する受講者		学士課程で卒業を予定しており､セキュリティに関する知識を得たいと考える 3～4 年次在籍者(理工系学生や IT 技術の利用者となる学生)
受講者の知識･スキル		理工系教養科目＋情報リテラシー教育を想定する
育成する人材像		産業界で必要となる情報セキュリティ分野に関する基礎的な知識を身につけた人材(セキュリティ分野への就職は前提としない)
到達目標	コア部分	受講者の志望業界で求められる次のような情報セキュリティに関する 知見を習得し、実務に活用できるようにする。 (例 1)工学系(非情報): 制御システムのセキュリティ対策技術 (例 2)保健医療福祉系：個人・機微情報の管理手法 (例 3)芸術系：作品の脆弱性対策及び著作権保護
	コア以外を含むカリキュラム全体	(コア部分に同じ)
関連科目との関係		本科目受講に先立って受講しておくべき科目を設定しないが、受講する学生の前提知識に応じて、以下の内容に関する教育を推奨する。 ①情報とデジタルデータの概念 ②コンピュータとして総称することが可能な機器の概念
実施方法		講義及び演習

付表 4　セキュリティ基礎レベル

例示③：情報セキュリティを専門とする学科等を対象とするもの

情報セキュリティ分野を専門とする学科向け		
種別		カリキュラム
想定する受講者		情報セキュリティを専門とする学科の学生(1～4 年次)
受講者の知識･スキル		普通科高校卒業程度の知識・スキルを想定する。
育成する人材像		情報セキュリティに関する基礎的な知識経験と意識を身につけた人材 (セキュリティ分野への就職は前提としない)
到	コア部分	情報セキュリティ上の主要な脅威と対策について理解すると

達 目 標		ともに、情報セキュリティ分野の代表的な要素技術について、演習等を通じてそれぞれの原理と活用方法を習得する。
	コア以外を含むカリキュラム全体	（コア部分に同じ）
関連科目との関係		学科内で体系的に整備する。
実施方法		講義及び演習、卒業論文

付表 5　セキュリティ専門レベル

例示④：修士課程に進学予定の情報系学士課程の学生を対象とするもの

進学予定の情報系学士課程在籍者を対象とする情報セキュリティ分野の実践講座向け		
種別		科目シラバス
想定する受講者		修士課程でセキュリティを学びたいと考える学士課程 3～4 年次在籍者
受講者の知識･スキル		理工系教養科目＋情報リテラシー教育を想定する
育成する人材像		情報セキュリティを本格的に学ぶ上で必要となる基盤的知識を習得した人材
到 達 目 標	コア部分	情報セキュリティ分野の要素技術(網羅的でなく部分的でよい)の習得を通じて対策の重要性と脅威に応じた対策方法について理解する。
	コア以外を含むカリキュラム全体	（コア部分に同じ）
関連科目との関係		・本科目受講に先立って受講しておくべき科目を設定しないが、受講する学生の前提知識に応じて、以下の内容に関する教育を推奨する。 ①情報とデジタルデータの概念 ②コンピュータとして総称することが可能な機器の概念
実施方法		講義及び演習

付表 6　セキュリティ専門レベル

例示⑤：情報セキュリティに関する単独の科目を対象とするもの

修士課程在籍者を対象とする情報セキュリティ分野の単独科目向け	
種別	科目シラバス

想定する受講者		情報セキュリティ以外の分野を専攻する修士課程在籍者等
受講者の知識･スキル		理系大学卒業程度の知識・スキルを想定する
育成する人材像		情報セキュリティに関する基本的な知識を備えた人材 (セキュリティ分野への就職は前提としない)
到達目標	コア部分	情報セキュリティに関する基本的な知識を備えた人材 (セキュリティ分野への就職は前提としない)
	コア以外を含むカリキュラム全体	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､主要な脅威とその対策に関する技術的背景知識を通じて理解する。
関連科目との関係		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理解する。
実施方法		・修士課程において前提とする科目等はなし。

付表 7　セキュリティ専門レベル

例示⑥：専門とは別に情報セキュリティを学ぶコース等を対象とするもの

修士課程在籍者を対象とする情報セキュリティ専門講座等向け		
種別		科目シラバス
想定する受講者		専門とは別に情報セキュリティを学ぼうと考える修士課程在籍者等
受講者の知識･スキル		理系大学卒業程度の知識・スキルを想定する
育成する人材像		習得した知識実践的経験を自らの専門分野のセキュリティ対策に活かせる人材
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理解する。
関連科目との関係		以下について十分な知識を有することを前提とする。 ・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

付表 8　セキュリティ専門レベル

例示⑦：情報セキュリティを専門とする専攻等を対象とするもの

情報セキュリティを専門とする専攻科向け		
種別		カリキュラム
想定する受講者		情報セキュリティを専門とする専攻科の学生
受講者の知識･スキル		理系大学卒業程度の知識・スキルを想定する
育成する人材像		情報セキュリティに関する専門的な知識と実践的な経験及び意識を備えた人材とし､セキュリティの専門性をある程度発揮できる環境への就職等を想定する
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		専攻内で体系的に整備する。
実施方法		講義及び演習、修士論文

付表 9　セキュリティ専門レベル

例示⑧：社会人学び直し向け短期(2 週間程度)集中コース

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	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)

目 標		・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

付表 10　セキュリティ専門レベル

例示⑨：社会人学び直し向け中期(3～6ヶ月程度)コース

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

付表 11　セキュリティ専門レベル

例示⑩：社会人学び直し向け長期(1 年程度)コース

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

5.2. 既存カリキュラム

既存カリキュラムの付録では、一般大学と専門大学を対象に調査した事例を例示する。調査は、シラバス掲載 URL を利用した調査とヒアリング調査とを併用した。

(1)中央大学

(a)シラバス掲載 URL

http://syllabus.chuo-u.ac.jp/syllabus

(b)レベルによる分類

付表 12　中央大学：レベルによる分類

レベル	授業科目名	学部/学科	想定対象年度	単位数	講義/演習	必修/選択	備考
一般教育	インターネット&情報セキュリティ論	学部間共通科目	学部 1 年	2 単位	演習		付表 13
	情報セキュリティ論／情報技術と社会システム	総合政策学部	学部 2 年	2 単位	講義		
セキュリティ基礎	情報セキュリティ論	商学部	学部 3,4 年	2 単位	講義		付表 14
	プログラム演習 V (情報セキュリティ技術論)	商学部	学部 3,4 年	2 単位	演習		
	情報セキュリティ基礎	理工学部	学部 3 年	2 単位	講義		
	情報セキュリティ技術	理工学研究科博士課程前期課程	修士 1 年	2 単位	講義		
	電子社会と情報セキュリティ	理工学研究科博士課程前期課程	修士 1 年	2 単位	講義	選択	
	情報セキュリティ法制	理工学研究科博士課程前期課程	修士 1 年	2 単位	講義		
	ネットワークセキュリティ	理工学研究科博士課程前期課程	修士 1 年	2 単位	講義	選択	
セキュリティ専門	－	－	－	－	－	－	－

(c)カリキュラムの概要

付表 13　中央大学：一般教育レベル：インターネット&情報セキュリティ論

項目	内容

項目	内容
大学名	中央大学
レベル	一般教育レベル
授業科目名	インターネット&情報セキュリティ論
学部/学科	学部間共通科目
想定対象年度	学部 1 年
単位数	2 単位
講義/演習	演習
必修/選択	
目的	現代の情報通信技術の発達とインターネットの普及は便利で快適な社会を実現しているがその一方で今まで存在しなかった問題を発生させている。この授業では、現代のインターネット社会に対応する技術、倫理について必要な知識を身につけ、適切な対応ができるようにすることを目標とする。
授業の概要	インターネットに代表される情報通信技術(ICT)の急速な発達と普及は私達の日常を大きく変えている。他方、現在の社会において ICT を利用するということは、様々な制約を理解し、あるいはいろいろな面での危険性を理解しなければ、しばしば予期しない問題を生じたり、思ってもいないトラブルに巻き込まれたり、自分や他人を不快な状況を発生させるようになっています。この講義ではこのような現実をふまえ、現代社会を生きる上で必要不可欠となる情報社会の問題点とそれに対応することを目標として、技術的側面と倫理的な側面の両面についての理論的な背景、現実の問題の実例の解説し、具体的対処法あるいはそれらに対応するのに必要な心構えについて講義し、実習を行います。情報や情報システムを活用して、実り多い大学生活とするために、これらの事柄について理解し、注意を払い無用なトラブルに巻き込まれないよう、適切な行動を心掛けることを期待したい。
授業計画と内容	1 現代の情報環境と ICT の問題点 キーワード まず初めに 2 ネットワーを知ろう キーワード ネットの基礎を学ぼう 3 ネットワーを知ろう その 2 キーワード ネット技術を使ってみよう 4 クラウド型ビジネスと個人情報保護 キーワード なぜタダなのか 5 クラウド型ビジネスの実際 キーワード 作って学ぼう 6 クラウド型ビジネスの実際 その 2 キーワード javascript を知ろう 7 クラウド型ビジネスの実際 その 3 キーワード Monaca でアプリ作り 8 クラウド型ビジネスの実際 その 4 キーワード タダより高いものはない 9 情報倫理入門 I-1 自己決定と自己責任 キーワード 情報と倫理 10 情報倫理入門 I-2 自己決定と自己責任 キーワード 情報倫理と私 11 IoT の現状 キーワード 世界は変わるか 12 人工知能と機械学習 キーワード コンピュータは人を超えるか 13 人工知能と機械学習 その 2 キーワード コンピュータも間違える 14 情報倫理入門 II 社会と企業 キーワード 情報倫理と企業 15 情報倫理入門 II-2 社会と企業 キーワード 社会と情報倫理

付表 14　中央大学：セキュリティ基礎レベル：情報セキュリティ論

項目	内容
大学名	中央大学
レベル	セキュリティ基礎
授業科目名	情報セキュリティ論
学部/学科	商学部
想定対象年度	学部 3,4 年
単位数	2 単位

項目	内容
講義/演習	講義
必修/選択	
目的	企業等の組織の一員になれば、必ず対応が求められる情報セキュリティ維持のための活動、規定等を、その背景、理由とともに理解することを目標とします。
授業の概要	企業活動において、情報の重要性はますます増してきています。従来からの文書類の情報とともに、IT の進展、ネットワークの拡大に伴い電子化された情報を有効に活用することが求められてきています。また個人の生活においても、ネットワークが各家庭に広くいきわたっている現在、やはり情報の収集、発信が重要な要素になってきています。これらの情報は、正しい内容であり、必要なときに適時に活用でき、また必要な情報が網羅されてこそ、その価値があります。と同時に、その情報は正当な権限を持つ関係者のみが利用することができ、権限の無い者には、秘匿されていることが必要で、その環境が整ってこそ、関係者が安心して情報を活用することができます。本講座では、企業活動および個人生活を行う人、更には企業などの組織で情報および情報セキュリティの管理を行う人に向けて、情報セキュリティの実務的な観点を紹介します。
授業計画と内容	1 情報セキュリティ論ガイダンス 2 情報セキュリティとは 3 情報システムを巡る動向と情報セキュリティ 4 情報システムの脅威と対策の基本 5 情報セキュリティ対策のポイント 6 企業における情報セキュリティ対策 7 情報セキュリティにおける PDCA サイクルと監査 8 情報セキュリティ対策の技術 9 クラウドと情報セキュリティ 10 リスクマネジメントとリスク分析 11 個人情報保護 12 事業継続計画 13 我が国の情報セキュリティを巡る施策 14 本年度の主要な情報セキュリティ事故 15 まとめ

(2)情報セキュリティ大学院大学

(a)シラバス掲載 URL

http://www.iisec.ac.jp/education/curriculum/

(b)レベルによる分類

付表 15　情報セキュリティ大学院大学：レベルによる分類

レベル	授業科目名	学部/学科	想定対象年度	単位数	講義/演習	必修/選択	備考
一般教育	－	－	－	－	－	－	－
セキュリティ基礎	－	－	－	－	－	－	－
セキュリティ専門	情報セキュリティ輪講 I		修士 1 年	2 単位		必修	
	情報セキュリティ特別講義		修士 1 年	2 単位		必修	

レベル	授業科目名	学部/学科	想定対象年度	単位数	講義/演習	必修/選択	備考
	暗号・認証と社会制度		修士1年	2単位		選択	
	暗号プロトコル		修士1年	2単位		選択	
	暗号理論		修士1年	2単位		選択	
	個人識別とプライバシー保護		修士1年	2単位		選択	付表16
	不正アクセス技法		修士1年	2単位		選択	
	セキュアシステム構成論		修士1年	2単位		選択	
	セキュアプログラミングとセキュアOS		修士1年	2単位		選択	
	セキュアシステム実習		修士1年	2単位		選択	
	情報セキュリティマネジメントシステム		修士1年	2単位		選択	
	セキュリティシステム監査		修士1年	2単位		選択	
	セキュリティ管理と経営		修士1年	2単位		選択	
	リスクマネジメント		修士1年	2単位		選択	
	組織行動と情報セキュリティ		修士1年	2単位			
	セキュア法制と情報倫理		修士1年	2単位		選択	
	セキュリティの法律実務		修士1年	2単位		選択	
	統計的リスク管理		修士1年	2単位		選択	
	リスクの経済学		修士1年	2単位		選択	
	マスメディアとリスク管理		修士1年	2単位		選択	
	特設講義(セキュリティ監査)		修士1年	2単位		選択	
	特設講義(情報セキュリティ運用リテラシーⅠ・Ⅱ)		修士1年	2単位		選択	
	特設講義(ハッキングとマルウェア解析)		修士1年	2単位		選択	
	特設講義(IoTセキュリティ特論)		修士1年	2単位		選択	
	特設講義(サイバー・インテリジェンス)		修士1年	2単位		選択	
	特設実習(セキュリティ実践Ⅰ)		修士1年	2単位		選択	

レベル	授業科目名	学部/学科	想定対象年度	単位数	講義/演習	必修/選択	備考
	特設実習(セキュリティ実践Ⅱ)		修士1年	2単位		選択	
	情報セキュリティ輪講Ⅱ		修士2年	2単位		選択	
	特設実習(Windowsセキュリティ)		修士2年	2単位		選択	

(c)カリキュラムの概要

付表 16　情報セキュリティ大学院大学

セキュリティ専門レベル：個人識別とプライバシー保護

項目	内容
大学名	情報セキュリティ大学院大学
レベル	専門レベル(＝セキュリティ専門)
授業科目名	個人識別とプライバシー保護
学部/学科	
想定対象年度	修士1年
単位数	2単位
講義/演習	
必修/選択	選択
目的	個人識別とプライバシーに関わるインターネット社会の諸課題について、技術面と法律面の両面から対応する基本能力を身につける。
授業の概要	本講義では、最初に個人識別と本人認証の原理を技術の面からに解説し、それをベースにインターネット社会における本人認証の仕組みと利用における技術的・法的課題について、具体的事例を通して学ぶ。次に、個人識別や本人認証技術と深い関係を持つプライバシー保護の問題について、法律的な視点と技術的な観点から問題点を理解する。最後に、講義の内容を基礎として演習を行い、受講者の理解を深めると同時に具体的事案に対する対応力を養うこととする。
授業計画と内容	本講義は、リレー講義形式と演習(計15回)で実施する。また、以下の(1)と(2)の各講義は、適宜、織り交ぜて行う。(3)の演習は、15回講義の最後の3回にて行う。 (1)　技術面 （ア）　個人識別と本人認証の技術の概要 （イ）　パスワード、PKI、バイオメトリック他 （ウ）　認証基盤、電子申請・電子申告、電子商取引等 （エ）　アイデンついて管理とID連携 （オ）　認可連携と属性交換 （カ）　クラウドサービスに向けた技術動向 （キ）　ビッグデータサービスにおけるプラバシー保護技術の動向 (2)　法律面 （ア）　プライバシーの語源と空間的・時間的展開 （イ）　人格権的保護と財産権的保護 （ウ）　個人データの保護とプライバシーの保護 （エ）　CESS型理解とPASS型理解 （オ）　ケース・スタディ (3)　演習 （ア）　演習課題の提示と説明・解説

項目	内容
	（イ） 受講生による相互発表、討議 （ウ） 受講生による相互発表、討議