2005 年度
情報セキュリティ推奨教育の
検討に関する調査報告書

NPO 日本ネットワークセキュリティ協会

2006 年 4 月 11 日

目次

JNSA **教育部会 情報セキュリティ推奨教育検討ワーキンググループメンバー**
（氏名横のカッコ内記載は、本報告書関連の保有資格略称）

ワーキンググループリーダー

持田 啓司	（SU）	セキュリティ・エデュケーション・アライアンス・ジャパン

本報告書執筆メンバー（所属企業名 50 音順）

櫻井 俊郎		株式会社 ＩＴサービス
齋藤 健司		株式会社 ＩＴサービス
佐々木 健美	（SU）	株式会社 インフォセック
関取 嘉浩	（CISA）	NRI セキュアテクノロジーズ株式会社
竹内 健治	（CISSP、CISA、GSLC）	NRI セキュアテクノロジーズ株式会社
大河内 智秀	（CISSP）	ＮＴＴコミュニケーションズ株式会社
副島 聡	（CISSP、CISA）	ＮＴＴコミュニケーションズ株式会社
滑川 愛恵	（CISSP）	ＮＴＴコミュニケーションズ株式会社
吉川 昌吾		エヌ・ティ・ティ・コムチェオ株式会社
荒木 淳		エヌ・ティ・ティ・コムチェオ株式会社
平井 健一	（SU、CSBM、CSPM、MCA）	株式会社 大塚商会
加藤 健司		クロス・ヘッド株式会社
河野 省二	（CISSP）	株式会社 ディアイティ
大西 克美		日本アイ・ビー・エム株式会社
鈴木 もなみ		日本アイ・ビー・エム株式会社
長谷川 長一	（CISSP）	日本ユニシス株式会社
松田 剛		株式会社 ヒューコム
馬場 重通		株式会社 フォーバル クリエーティブ
八城 美奈子		富士ゼロックス株式会社
古川 勝也		マイクロソフト株式会社
若林 勝広		マカフィー株式会社
与儀 大輔	（CISSP）	横河電機株式会社
佐々木 晴子	（CISSP）	横河電機株式会社

※ 上記資格名称（アルファベット順）

- CISA…… Certified Information Systems Auditor
- CISSP…… Certified Information Systems Security Professional
- CSBM…… SEA/J Certified Security Basic Master
- GSLC…… GIAC Security Leadership Certification
- CSPM…… SEA/J Certified Security Professional Master
- MCA…… MCA Security
- SU…… 情報セキュリティアドミニストレータ

著作権･引用について

1 始めに

情報セキュリティ推奨教育検討ワーキンググループ（以下、本ワーキング）は、NPO 日本ネットワークセキュリティ協会(JNSA)の教育部会に属し、2005 年度の単年度事業として国内における情報セキュリティ教育や資格の調査を行い、本報告書により情報セキュリティに携わる人材の効率的な育成のロードマップとして発表するものである。

詳細は後の章で述べていくが、人材に対する要求は組織において千差万別であり、画一的な教育体系を示すだけでは、時代に要求される情報セキュリティ人材の育成は困難である。本報告書は、一つの育成指標として参考にしていただきたい。

なお、本報告書をお読みいただいた皆様から、調査の方法や体系化の方法などについてご意見をいただければ、今後の再調査・体系化での改善も図れる上、当ワーキンググループにとっても励みとなるので、巻末の連絡先にお気付きの点をお知らせいただきたい。

2 報告書の目的

情報セキュリティ対策における人材育成の必要性は叫ばれているものの、現状の人材育成においては、製品導入に伴う操作教育や、短期的・場当たり的なものとなっている。このため、本来必要とされる組織全体を総括して各種対策を行うための人材配置を前提とした教育プログラムの提案ができているとは言い難い。

本ワーキングでは、組織の底辺から情報セキュリティ専門職種へ、それぞれの育成プロセスを示すことができる教育の在り方を検討し、人材育成による隙の無い組織構築のための教育プログラムを検討する。この中では、現状ある教育コースを用いて、現在必要と想定される職種別の人材育成フローの提案を行う。

また、情報セキュリティ専門職種の検討を通じて、日本に合った新たな組織デザインを試みることとする。

3 報告書の構成

本報告書は以下の 4 種類の検討内容で構成されている。

a. 情報セキュリティスキル項目検討
   情報セキュリティに関する業務を行ううえでの必要なスキル項目の検討を行い、大項目・中項目・小項目(キーワード)により整理し、リスト化する。
b. 対象教育コース(資格)調査・検討
   現段階で教育市場に存在する情報セキュリティ教育または資格について、そのカリキュラム内容を調査して、a.でまとめたスキル項目と対象範囲を比較検討する。
c. 職種別必要スキル項目検討
   情報セキュリティに関わる職種を分類するとともに、a.でまとめたスキル項目をもとにそれぞれの職種ごとに必要なスキル項目の検討を行う。
d. 職種別キャリアパス作成
   c.でまとめた職種別の必要スキル項目と、b.でまとめた対象教育コースのカリキュラム内容を確認し、職種別のレベルに応じて推奨する教育コースを研修ロードマップとして作成する。

この中で、a.は体系化の手法により様々な整理方法があるとともに、技術内容の進歩に伴い日々刻々と変わっていくものであること、また、b.の対象教育コースについても代表的な教育コースのみを選定しており、これが全てではないことを前提条件として承知いただきたい。

4 情報セキュリティスキル項目検討

（ア）作業内容

情報セキュリティに関する業務を行ううえでの必要なスキル項目の検討を行い、大分類・中分類・小分類・備考(キーワード)により整理しリスト化した。

（イ）参考資料

① 経済産業省教育研究会 カリキュラム　p15～29
http://www.meti.go.jp/policy/netsecurity/edu_report.html

② 情報処理技術者試験（情報セキュリティアドミニストレータ）スキル標準
http://www.jitec.jp/1_17skill/skill_00.html

③ IPA 情報セキュリティスキルマップ
http://www.ipa.go.jp/security/fy16/reports/skillmap/index.html

④ CISSP cbk
https://www.isc2.org/japan/
http://www.imslab.co.jp/service/CISSP/CISSP.html

（ウ）作業の詳細

IPA スキルマップを基にし、経済産業省教育研究会カリキュラム、情報処理技術者試験（情報セキュリティアドミニストレータ）スキル標準、IPA 情報セキュリティスキルマップ、CISSPcbk を参考に追加・整理し、詳細スキル項目まで作成した。

① SANS、CMU(カーネギーメロン大)など、他にもスキル項目の参考となるものは多いが、上記資料である程度の網羅性はまかなえるであろうことと、資料が増すほどに体系化における整理が煩雑となることから、今回は除外した。

② IPA スキルマップを基にした理由は、大分類の分け方が、業務や実施内容に偏らず技術項目で分類されており、本ワーキングにおける教育コースとのマッピングの際に整理しやすいとの理由からである。

③ 作成イメージ

スキルマップ	METI教育研究会	情報セキュアドスキル標準	CISSP cbk
AAAAAA	あああああ	aaaaaa	アクセスコントロー
	いいいいいい	bbbbbb	セキュリティ原則
CCCCCC	ううううう	cccccc	識別
	えええええ		バイオメトリク
	おおおおお	eeeeee	
FFFFFF	かかかかか	ffffff	承認
GGGGGG		gggggg	シングルサインオ
	くくくくく	hhhhhh	アクセス制御モデ
IIIIII	けけけけけ	iiiiii	
JJJJJJ	こここここ	jjjjjj	アクセス制御コン
	さささささ		アクセス制御手法
LLLLLL	しししししし	llllll	管理上の制御
MMMMMM		mmmmmm	物理的制御
NNNNNN		nnnnnn	論理的制御
OOOOOO	そそそそそ	oooooo	
	たたたたた	pppppp	アクセス制御監視
	ちちちちち	qqqqqq	アクセス制御に対
RRRRRR	つつつつつ		Teleconmmunications
SSSSSS		ssssss	Open System
TTTTTT	とととととと	tttttt	
UUUUUU	なななななな	uuuuuu	6.Presentation
	にににににに		5.Session layer
WWWWWW	ぬぬぬぬぬぬ	wwwwww	4.Transport
		xxxxxx	3.Network layer
YYYYYY	のののののの	yyyyyy	2.Data Link
ZZZZZZ	ははははは	zzzzzz	

スキル項目
あああああ
いいいいいい
ううううう
えええええ
おおおおお
かかかかか
きききききき
くくくくく
けけけけけ
こここここ
さささささ
しししししし
すすすすす
せせせせせ
そそそそそ
たたたたた
ちちちちち
つつつつつ
てててててて
とととととと
なななななな
にににににに
ぬぬぬぬぬぬ
ねねねねね
のののののの
ははははは

（エ）作業実施状況と作業途中での問題点

作業開始当初は、経済産業省教育研究会カリキュラムや CISSP cbk のスキル項目を基にして、別項目を参考に追加しようとしたが、技術項目で分けてあるわけでなく、職務による業務知識という観点で区分しているため、最終的に IPA スキルマップを基にすることとした。

具体的には、技術項目が複数箇所に記載されたり、業務内容としての記載のため複数の技術項目がひとまとめになってしまうなど、技術項目を探し出したり、教育内容をチェックしたりするには不向きであるという問題が発生したためである。

（オ）スキル項目リスト作成時の整理方法

IPA スキルマップを基にし、各種参考文献の技術項目等を追加整理しながら、情報セキュリティに必要な技術項目・実施項目等の体系化を行った。

概要は次のとおりである。

① 大分類「情報セキュリティマネジメント」に、中分類として「費用対効果」、「人員計画」、「教育・訓練」を追加

② 大分類に、「セキュリティアーキテクチャ」を追加
その中に中分類として、アプリケーションセキュリティに区分してあった、「システムライフサイクルセキュリティ」と「システム開発管理」を追加

③ 大分類「ネットワークインフラセキュリティ」に、中分類として「セキュアなインターネット、イントラネット、エクストラネット」を追加

④ 大分類「アプリケーションセキュリティ」に、全般の区分を追加
その中に中分類として、「アプリケーション環境とセキュリティ管理」「アプリケーションとシステムの脆弱性と脅威」「セキュリティ制御」を追加

⑤ 大分類「セキュアプログラミング技法」に、中分類として「プログラミング言語とツール」、「オブジェクト指向技術」、「データベースとデータウェア保管庫の脆弱性、リスク、防護」を追加

⑥ 大分類「セキュリティ運用」に、中分類として「物理セキュリティ」、「人的セキュリティ」、「リソース保護」を追加

⑦ 大分類「認証」に、中分類として「ID 管理と認証」、「効果的なパスワード管理」、「認可」「アクセス制御手法」「アクセス制御の管理」を追加

⑧ 大分類「暗号」に、中分類として「暗号に関する問題」、「暗号の代替」を追加

⑨ 大分類「電子署名」に、中分類として「メッセージダイジェストとその他のメッセージ完全性コード」を追加

⑩ 大分類「法令・規格」に、中分類として「主要法体系」「情報システム/インターネットの法的概念」を追加

⑪ 大分類に、「事業継続経営（BCM）」を追加
その中に中分類として、「アプリケーションセキュリティ」に区分してあった、「システムライフサイクルセキュリティ」と「システム開発管理」を追加

（カ）活用上の注意点

① スキル項目については、本ワーキング実施時に検討した内容であり、セキュリティ技術の進歩や、新たな脅威およびそれに対する対策手法は、日々変化していることを前提に活用いただきたい。

② 項目の整理方法については、本ワーキングでは技術内容に重点を置いて整理を行ったが、ある職種ごとの業務や必要スキルで整理した場合には、体系化の方法は違ってくるなど、視点によって体系化の仕方が変わることをご理解いただきたい。

（キ）スキル項目リスト

このスキル項目リストは、大分類・中分類・小分類・備考からなっているが、報告書本体には小分類までの掲載としているため、備考については別添の Excel シートを参照いただきたい。

大分類	中分類	小分類
情報セキュリティマネジメント	マネジメント技術	マネジメントプロセス
		マネジメントシステムの確立
		マネジメントシステムの導入･運用
		マネジメントシステムの監視･見直し
		マネジメントシステムの維持･改善
		情報セキュリティのドキュメント体系
	リスク分析技術	リスクの考え方
		リスクアセスメント手法
		情報資産の調査･評価
		脅威･脆弱性の調査
		リスク評価
		リスク対応
		リスク受容
		対策システムの検討･整理（リスクマネジメント方針）
	情報セキュリティポリシー	情報セキュリティポリシーとは
		情報セキュリティ組織（委員会）
		情報セキュリティポリシーの構成
		情報セキュリティ方針の策定
		基本方針
		物理的対策
		技術的対策 （情報システムに関する情報セキュリティ規程の作成）
		人的対策
		運用･管理対策 （情報システムの情報セキュリティ規程の作成）
		組織的対策（企業活動一般のセキュリティ規程の作成）
	費用対効果	単一損失予測、年次損失予測の計算、対策の選択、対策の評価、リスクの回避、低減、移転、受容
	人員計画	役割と責任、データオーナーとデータ管理者
	教育･訓練	利用者への啓発および教育訓練計画、利用者教育、セキュリティ技術者教育、教育方法（e-learning,OJT）、教育効果の測定
	情報セキュリティ監査	情報セキュリティ監査の目的（監査の種類）
		情報セキュリティ監査手法
		監査計画書
		監査報告書
	関連知識	情報セキュリティの関連制度
		情報セキュリティの標準化
		情報セキュリティの関連法規
		情報セキュリティ監査（内部監査、外部監査）

大分類	中分類	小分類
セキュリティアーキテクチャ	プラットフォームアーキテクチャー	コンピュータとネットワークの一般的な構成・アーキテクチャー・設計の原理
		アドレス指定：物理的，記号的
		メモリー空間との比較としてのアドレス空間
		ハードウェア，ファームウェア，ソフトウェアの違い
		マシンの種別（実，仮想，マルチ状態，マルチタスク，マルチユーザー）
		ネットワークプロトコルの機能（OSI参照モデル）
		運用状態
		リソースマネージャーの機能
		記憶装置の種類（1次記憶，2次記憶，実記憶，仮想記憶）
	セキュリティモデル	認定（Accreditation）と認証（Certification）
		クローズドシステムとオープンシステム
		監禁（Confinement），境界（Bounds），隔離（Isolation）
		制御：強制と任意
	評価基準の原則	IETFセキュリティアーキテクチャ（IPSec）
		ITSECのクラス，および必要な保証と機能
		オブジェクトとサブジェクト（目的と関係）
		参照モニターとカーネル（目的と機能）
		セキュリティモデル（Bell-LaPadula，Clark-Wilson，Biba）
		TCSECのクラスと必要な機能
	保護メカニズム	トークン，機能，ラベル（目的と機能）
		システムアーキテクチャーおよびシステム設計に関連する一般的な欠陥とセキュリティ問題
		隠れチャネル（メモリー，記憶装置，通信）
		初期状態と障害状態
		入力とパラメーターのチェック
		メンテナンスフックと特権プログラム（superzap/su）
		プログラミング（手法，コンパイラ，API（Application Programming Interface：アプリケーションプログラミングインターフェース），ライブラリーの問題）
		タイミング（TOC/TOU），状態変化，通信の切断
		電磁放射
	システムライフサイクルセキュリティ	安全なシステム/アプリケーションの開発のためのポリシー
		システムライフサイクルvsシステム開発ライフサイクル
		プロジェクトマネジメントの原則
		開発中の機密コードのセキュリティ
		さまざまなプラットフォームや開発方式のリスク
	システム開発管理	製品調達・導入
		セキュリティ計画
		設計段階におけるセキュリティ
		開発・要員計画
		テスト工程におけるセキュリティ
		運用段階でのセキュリティ
		外部委託管理

大分類	中分類	小分類
ネットワークインフラセキュリティ	ネットワーク設計技術	物理設計技術（物理設計時のセキュリティ対策）
		論理設計技術（論理設計時のセキュリティ対策）
		ルーティング制御（ルーティングによるセキュリティ対策）
		アドレス変換（アドレス変換によるセキュリティ対策）
		運用・管理
	セキュアなインターネット、イントラネット、エクストラネット	ゲートウェイとルータ
		TCP/IP
	ネットワークアクセスコントロール	パケットフィルタリング（アドレスとポート番号によるセキュリティ対策）
		MAC(Media Access Control)アドレスフィルタリング
		ポートベースVLAN（バーチャルLANによるセキュリティ対策）
	VPN(Virtual Private Network)	トンネリングプロトコル
		環境構築
		IPSecによるVPN装置（ファイアーウォール含）
		ルータによるVPN装置
		SSLによるVPN装置
	無線LAN	無線LANとパーソナルエリアネットワークの標準規格
		無線LANのセキュリティ問題と制御
		無線で接続するインターネットとWAN
		伝送技術
		認証・暗号化
		その他

大分類	中分類	小分類
アプリケーションセキュリティ 【全般】	アプリケーション環境とセキュリティ管理	環境のセキュリティ
		物理的、論理的、職務の分離
		実稼動環境と開発環境の分離
		キーパーソンとキー知識の保持
		プログラム／システム／エラーの取り扱いの文書化
		時間外運用のセキュリティと監視
		ソーシャルエンジニアリングの予防
	アプリケーションとシステムの脆弱性と脅威	脅威と脆弱性
	セキュリティ制御	アプリケーションベースのDoSの予防
		クッキー／ウェブサイトの操作（manipulation）のリスク
		アクティブXとJavaの制御
		機密データの暗号化防護
		ウェブベース（e.g. XML, SAML, SOAP, HTML）
		クライアントベース（e.g. Javaアプレット、アクティブX）
		サーバーベース
アプリケーションセキュリティ 【Web】	Webサーバに対する脅威	Webアプリケーションに対する攻撃
		DoS(Denial Of Service)／DDoS(Distributed Denial Of Service)攻撃
		ホームページの改竄
		情報送信時の情報漏洩
		プロキシサーバの不正利用
	Webサーバのセキュリティ対策	アカウントの設定
		ファイル／ディレクトリのアクセス権の設定
		ユーザ認証
		ファイアーウォール、侵入検知システム等の導入
	Webサーバの運用	Webコンテンツのアップロード
		セキュリティパッチの適用
		ログの収集と分析
		Webサーバの監視
		インシデント対策と体制
	Webアプリケーション設計	クロスサイトスクリプティング対策
		CGI(Common Gateway Interface)
		Webのセッション管理
	Webブラウザのセキュリティ	Webブラウザに対する脅威
		Webブラウザのセキュリティ対策
	Web関連プロトコルの基礎知識	HTTP(Hyper Text Transfer Protocol)
		SSL(Secure Socket Layer) /TLS(Transport Layer Security)
		SOAP(Simple Object Access Protocol)

大分類	中分類	小分類
アプリケーションセキュリティ 【電子メール】	メールサーバに対する脅威	第三者不正中継（Third-Party Relay）
		迷惑メール
		Spamメール（UCE/UBE）
		DoS(Denial Of Service)/DDoS(Distributed Denial Of Service)攻撃
		盗聴
		ユーザ情報の漏洩
		ウィルス
		代表的メールサーバアプリケーションの脆弱性
	メールサーバのセキュリティ対策	第三者不正中継（Third-Party Relay）対策
		迷惑メール対策
		Spamメール（UCE(Unsolicited Ccommercial E-mail)/UBE(Unsolicited Bulk E-mail)）対策
		ユーザ情報の漏洩
		代表的メールサーバアプリケーションの脆弱性対策
	メールクライアントのセキュリティ	盗聴対策
		ウィルス対策
	メールサーバの運用	セキュリティパッチの適用
		ログの収集と分析
		メールサーバの監視
		インシデント対策と体制
アプリケーションセキュリティ 【DNS(Domain Name System)】	DNSサーバに対する脅威	内部ネットワーク情報の漏洩
		TCP53番ポート（ゾーン転送）をついた攻撃
		DNSキャッシュ攻撃（ポジションキャッシュ）
		代表的DNSサーバアプリケーションの脆弱性対策
	DNSサーバセキュリティ対策と構成	内部ネットワークの隠蔽
		ゾーン転送対策
		DNSキャッシュ攻撃（ポジションキャッシュ）攻撃対策
	DNSサーバの運用	セキュリティパッチの適用
		ログの収集と分析
		メールサーバの監視
		インシデント対策と体制

大分類	中分類	小分類
OSセキュリティ 【Unix】	ログ管理	インシデント対応
		アクセスログの解析
		アクセスログの保管
	パッチ適用管理	適切なPatch適用状況と確認
	サービスの管理	サービスの制限とアクセス制御
		一般ユーザでのデーモンの起動
		ネットワークサービスとポート
		不要なサービスの削除
	ファイルシステム管理	ファイルシステム完全性検査
		バックアップとリストア
		暗号化ファイルシステム
		デフォルトのパーミッション設定
		パーミッション設定ミスの検出
		setuid/setgidビット
	アカウント管理	アカウント共有
		シャドウファイル
		強いパスワード/弱いパスワード
		グループポリシー
		ローカルセキュリティポリシー
		アカウントの概念及び権限の分散

大分類	中分類	小分類
OSセキュリティ【Windows】	構成･設定管理	Active Directory
		グループポリシー
		セキュリティテンプレート
		アクセスログの解析
		アクセスログの保管
		アカウント毎の証明書管理
	パッチ適用管理	Service Pack
		Hotfix (Patch, QFE)
		パッチ適用状況確認
		パッチの一括･一斉配布
		WindowsUpdate
	監査	ディレクトリアクセスの監査
		プロセス追跡の監査
		サービスの監査
		ファイルとフォルダの監査
		特権使用の監査
		アカウント監査
	ログ管理	インシデント対応
		イベントログ
		アクセスログの解析
		アクセスログの保管
	プロセス管理	ソフトウェア制限ポリシー
	サービス管理	ネットワークサービスとポート
		サービスのアクセス権
		不要なサービスの削除
	ファイルシステム管理	暗号化ファイル（EFS）
		アクセス制御リスト
		アクセス権の継承
		明示的な拒否権限
		NTFSセキュリティアクセス
	アカウント管理	強いパスワード/弱いパスワード
		証明書認証
		スマートカード認証
		ActiveDirectory
		ローカルアカウントとドメインアカウント
		アカウントの概念及び権限の分散
	ネットワーク保護	ポートフィルタ
		接続元･先の制限
		インターネット接続ファイアウィール
OSセキュリティ【TrustedOS】	強制アクセス制御の概念（MAC）	Auditログの特徴
		ファイル、プロセス、ユーザに対するセキュリティラベルの委任
		root特権の委任

大分類	中分類	小分類
ファイアーウォール	ファイアーウォールの導入･運用	ログ解析
		侵入検知装置ログとの違い
		DMZ等構成の設計
		フィルタリングルールの設計
	NAT(Network Address Translation)	StaticNAT
		DynamicNAT
		IPマスカレード
	ネットワークアクセスコントロール	Packet Filterling
		Circuit Level Gateway
		Application Level Gateway
		ステートフルインスペクション
侵入検知	侵入検知システムの導入･運用	運用体制とインシデント対応
		侵入検知システムの限界
		ログ解析
		ファイアーウォールログとの違い
	侵入検知システムの機能	管理コンソールへの告知（警告）
		防御機能　（TCPリセット/ルータ･ファイアーウォールでの遮断）
		受動ログ取得
		シグネチャ
		パターンマッチング方法
		プロミスキャスモード
	検出アルゴリズム	異常検出（統計異常ベース）
		不正検出（分析エンジン）
	検出方法	System Integrity Verifiers
		ログファイルモニター
		ネットワークモニタリング
	侵入検知システム	ホスト型
		ネットワーク型
		ハイブリッド型
		アプリケーションベースIDS
		ハニーポッド
		改竄検知

大分類	中分類	小分類
ウィルス	管理体制	報告告知体制
	感染後のポリシー	ウィルス検出ソフトの設置管理
		駆除方法と手順
	予防ポリシー	社内体制
		流行の傾向と予測
		他アプリケーションとの連携
		イントラネットの構築
		システム管理
		定義ファイル管理
		アンチウィルスソフトの配置
	発病	ウィルスの複合化
		バックドアの作成
		改竄
		情報発信
		外部攻撃
		メール発信
		破壊活動
	検出方法と駆除	予知検出
		メールに対するコンテンツフィルタ
		ウィルスの誤検知
		駆除方法
		スキャン方式の種類
		定義ファイル
		検出方法の種類
	感染	ウィルスの自己防衛機能
		脆弱点の利用
		兆候
		手段(媒体)
		経路
	種類	ウィルスの機能構成
		デマウィルス
		ジョークウィルス
		不必要なプログラム
		マクロウィルス
		トロイの木馬
		ワーム
		スクリプト
		ウィルス

大分類	中分類	小分類
セキュアプログラミング技法	プログラミング言語とツール	アセンブラ、コンパイラ、インタープリタ、クロスアセンブラ、クロスコンパイラ
		アプリケーションエラーハンドリング（ditチェック、入出力検証）
		トランザクション管理
		バックアップと冗長性の管理
		一時ファイル、一時オフィスのセキュリティ
		データ辞書
		チェックポイント/リスタート
		フィールドの初期設定と再利用
	Webアプリケーション	クロスサイトスクリプティング
		Webページとユーザ認証
		クエリストリングからの情報漏洩
		Webフォームの選択項目の危険性
		hiddenの危険性
	データベース	SQL引数のチェック
		スクリプトへのDBパスワードの埋め込み
		データベースとアクセス権限
	アプリケーション全般	パスワードの取り扱い
		入力値のチェック方法
		エラーメッセージからの情報漏洩
		ログ
		特権処理の局所化
		ソースコードチェックツール
		再利用と部品化
		モジュールの分割設計
		バッファーオーバーフロー
	XML(Extensible Markup Language)	XML署名
		XML暗号
		XMLアクセスコントロール
		SOAP(Simple Object Access Protocol)メッセージの取扱
	PHP(Hypertext Preprocessor)	危険な関数
		セキュリティホール
		サニタイジングの対策
	JAVA	危険なクラス
		カプセル化
		シリアル化と情報漏洩
		クラス継承となりすまし
		JAVAのアセーション
		synchronizedとレースコンディション
	Perl	ファイルオープン
		危険な関数
		Taintモード

大分類	中分類	小分類
セキュアプログラミング技法(続き)	VB/ASP	Requestへのアクセス
		仮想パスのマッピング
		セッションタイムアウト
	C/C++	危険な関数
		文字列処理の際の危険
		サブシェルの呼び出し
		メモリリーク
		C++デストラクタ
	Unix	シンボリックリンクの悪用
		PATH変数/子プロセスのすり替え
		setuid
		forkの利用
		レースコンディション
		coreファイルから情報漏洩
		安全なパス名
		テンポラリファイルからの情報漏洩
	コンパイラ・仮想マシン	最適化による脆弱化
		動作オプションによるオーバーフロー防止
		出力コードの特性
	Windows	安全なパス名
		プロセス間通信
		プロセス間通信オブジェクトのアクセス権
		特権の管理
		偽装アカウント
		制限アカウント
		レジストリ管理・アクセス権
		テンポラリファイルからの情報漏洩
		プロセス、スレッドのアクセス権
		NTFS(New Technology File System)ストリーム
		NTFSのセキュリティ機能
	オブジェクト指向技術	オブジェクト、クラス、メッセージ
		CORBA (Common Object Request Broker Architecture)
		DCOM (Distributed Component Object Model)
		EJB (Java Beans and Enterprise Java Beans)
		SOAP (Simple Object Access Protocol)
		カプセル化
		オブジェクト再利用のリスク

大分類	中分類	小分類
セキュアプログラミング技法（続き）	データベースとデータウェア保管庫の脆弱性、リスク、防護	データベースの種類
		データベースとアプリケーションのインターフェース
		データベース、データマート、データ倉庫
		メタデータ
		DBMS (Database Management Systems)
		ユーザーと管理者のためのアクセス制御（職務の分離）
		バックアップと復旧
		エラーの取り扱い
		効率的処理
		錠の管理
		ACIDテスト
		保管された情報の防護vs移動中の情報の防護
		データベースの完全性のリスク／管理
		SQL(Structured Query Language)

大分類	中分類	小分類
セキュリティ運用	物理セキュリティ	脅威の種類
		脅威の根源
		脆弱性
		建物、敷地、境界の保安組織
		システムセキュリティ戦略
		トレーニング
		物理的なセキュリティ手順
		環境規制
		物理的な防御
		設備サポートシステム
		物理アクセス制御
	人的セキュリティ	雇用方針、雇用慣行、経歴調査、人物調査、雇用契約、入社時および退社時の手続き、職務内容説明、役割と責任、職務の分離、職責の分離、定期配置転換
		組織構造におけるセキュリティ上の役割(加えて実施責任者の業務やプロフェッショナリティに言及)、関係するサードパーティ、責任の明確化、証拠収集と証拠保全、倫理規程、プロフェッショナリティ、プライバシーポリシ、最小特権の原則、職務分離、ローテーション
	リソース保護	制御種別
		制御手法
		媒体管理
		IT資産管理
	定常運用時のセキュリティ確保	問題管理(不測事態対応計画)
		構成管理
		事前設定
		モニタリング
		セキュリティホール対策
		(パッチマネジメント管理)
		定常作業
		ユーザ対応等
	異常時対応	異常検知
		原因究明・トラブルシューティング
		システム復旧
		緊急時対応
	運用関連情報(脆弱性情報・対策情報・攻撃情報・被害情報)	情報源の種類と特徴
		脆弱性情報の意味と分析

大分類	中分類	小分類
セキュリティプロトコル	アプリケーション層	PGP(Pretty Good Privacy)
		S/MIME(Secure Multipurpose Internet Mail Extensions)
		SSH(Secure SHell)
	トランスポート層	SSL(Secure Socket Layer)/TLS(Transport Layer Security)
		Socks
	ネットワーク層	IPSec
		IPinIP
	データリンク層	L2TP(Layer2 Tunneling Protocol)
		PPTP(Point-to-Point Tunneling Protocol)
		L2F(Layer 2 Forwarding protocol)
		MPLS(Multi-Protocol Label Switch)
		MPOA(Multi-Protocol Over ATM)
認証	ID管理と認証	ID管理およびビジネスプロセスとの整合
	パスワード認証	固定パスワード
		ワンタイムパスワード
		パスワードの暗号化
	バイオメトリック認証	指紋
		音声
		虹彩
		網膜
		手の大きさ
		ペンの速度、筆圧
		顔認証
		DNA
		行動パターン
	認証デバイス	ICカード
		USBトークン
		耐クローン
		耐タンパ
	認証プロトコル	AKE(Authenticated Key Exchange)
		Kerberos
		RADIUS
		SSH(Secure SHell)
	Web認証	Cookie
		SSL(Secure Socket Layer)認証
	システム認証	サーバ間認証
	シングルサインオン	アクセス制御
		セッション管理
		ログ管理
		構成

大分類	中分類	小分類
アクセス制御	効果的なパスワード管理	種類
		強度
		発行
		使用
		管理
	認可	Trusted Authority - LDAP, ADなど
		匿名アクセス - ヌル認可
		権限委譲 (Delegation)
		擬人化 (Impersonation)
	アクセス制御手法	制御スキーム
		制御の種類
		導入
	アクセス制御の管理	アクセス制御の管理手法

大分類	中分類	小分類
PKI(Public Key Infrastructure)	PKIの利用	セキュアタイムスタンプ
		公証
		電子CP(コマーシャルペーパ)
		認可機関
		権限管理とPKIとの統合
		アプリケーションでの利用
		利用方法の規格化
	証明書と認証	証明書の構造と意味
		証明書の有効性検証
		証明書のフォーマット
		OID(オブジェクト識別子)
		ポリシー機関
		認証機関と登録機関
		鍵と証明書のライフサイクル管理
		属性証明書
	証明書失効	CRL(証明書失効リスト)
		ARL(認証機関失効リスト)
		OCSP(オンライン証明書ステータスプロトコル)
	信頼モデル	認証機関の階層構造
		相互認証
		ブリッジCA
		認証パスの構築
		認証パスの有効性確認
		インターオペラビリティ
	契約モデル	クローズモデル
		ネットワークモデル
		オープンモデル
	記述とデータ方式	ASN.1とBER(Basic Encoding Rules)、DER(Distinguished Encoding Rules)、PEM(Privacy Enhanced Mail)
		Base64エンコーディング
	規格	公開鍵証明書の規格(RFC3280、X.509)
		PKCS(Public Key Cryptography Standards)
		CRLの規格
		証明書とCRLの配布点
		CMP(Certificate Management Protocol)
		属性証明書の規格
	公開リポジトリ	ディレクトリサーバの利用
	認証局(CA)の構築と運用	認証局の運用形態
		認証局の構築
		秘密鍵管理(HSMN、アクセラレータ)
		認証局運用規程
		証明書ポリシー
	法的枠組み	電子署名及び認証業務に関する法律（電子署名・認証法）

大分類	中分類	小分類
PKI(Public Key Infrastructure)（続き）	PKIの要素技術	認証機関
		証明書ﾘﾎﾟｼﾞﾄﾘ
		証明書失効
		鍵のバックアップと回復
		自動鍵更新
		鍵履歴
		相互認証
		否認防止のサポート
		タイムスタンプ
	PKIが提供するサービス	認証
		データの完全性
		データの秘匿性

大分類	中分類	小分類
暗号	公開鍵暗号	公開鍵暗号の原理
		公開鍵暗号で実現できる機能
		公開鍵暗号のアルゴリズム
		Diffie-Hellman鍵配送
		楕円曲線上の演算を利用した暗号法
	共通鍵暗号	共通鍵暗号の原理
		共通鍵暗号のアルゴリズム
		非同期式ストリーム暗号
		同期式ストリーム暗号
	ハッシュ関数	ハッシュ関数の原理
		ハッシュ関数の構成法
		専用ハッシュ関数
	暗号用乱数	暗号用乱数の原理
		真性乱数
		擬似乱数
	鍵管理	鍵共有方式
		鍵生成方式
		(公開鍵暗号方式の) 秘密鍵の保管方法
		共有鍵の保管方式
		秘密情報分散保管法
		鍵管理サーバ方式
		KPS(Key Predistribution System)方式
		鍵の正しい保管と配布
		紛失鍵の復旧と廃止
		鍵強度とサイズ
		キーエスクローと鍵の複数者による管理
	ゼロ知識証明	ゼロ知識証明の原理
		ゼロ知識証明プロトコル
		ゼロ知識証明の応用
	その他の暗号方式	MAC(Message Authentication Code)
		量子暗号
		秘密分散(Secret Sharing)
	暗号解読・強度評価	暗号解読と強度評価
		暗号解読と暗号攻撃
		全数探索型攻撃法
		ショートカット法
		サイドチャネル攻撃法
		鍵の発見のためのソーシャルエンジニアリングやその他の非技術的手法
		暗号技術評価プロジェクト (CRYPTREC)
	暗号に関する問題	国際的使用と輸出
		法執行機関の関与
	暗号の代替	ステガノグラフィー
		ウォーターメーキング

大分類	中分類	小分類
電子署名	電子署名の利用	コードサイニング
		XML(Extensible Markup Language)署名(規格、利用)
	電子署名の要素技術	電子署名署名に利用される暗号アルゴリズム
		電子署名に利用されるハッシュ関数
	電子署名の仕組み	署名作成方法
		署名検証方法
		メッセージダイジェスト
		デジタル封筒
	電子署名の利点	秘密鍵利用による本人性の保証
		ハッシュ関数の利用
		署名検証の容易さ
	メッセージダイジェストとその他のメッセージ完全性コード	チェックサム
		ハッシュ機能とメッセージダイジェスト
不正アクセス手法	遠隔不正侵入･操作	バッファーオーバーフローを悪用した攻撃
		Format String Bug
		Frame Pointer Error
		Spyware
		不正アクセスの隠蔽（ログ改竄）
		バックドア
		なりすまし
		トロイの木馬
		ロジック爆弾
	サービスの停止	メール爆弾
		DoS(Denial Of Service)攻撃
		DDoS(Distributed Denial Of Service)攻撃
	盗聴行為	Sniffing
		WireTAP
		無線ＬＡＮ（802.11系）の傍受
		アナログ無線の傍受
	偵察行為	TCP(Transmission Control Protocol)スキャン
		UDP(User Datagram Protocol)スキャン
	情報収集	パスワードクラック
	古典的不正アクセス技法	ソーシャルエンジニアリング
		ピギーバック
		スーパーザップ
		スキャベンジング
		サラミ

大分類	中分類	小分類
法令･規格	基準･指針･ガイドライン等	情報システム安全対策基準
		コンピュータウィルス対策基準
		コンピュータ不正アクセス対策基準
		システム監査基準
		ソフトウェア管理ガイドライン
		情報通信ネットワーク安全･信頼性基準
		情報システム安全対策指針
		行政情報システムの安全対策指針
		情報セキュリティポリシーに関するガイドライン
		情報セキュリティ監査制度関連基準･ガイドライン
		情報セキュリティマネジメントシステム(ISMS)認証基準
	主要法体系	法的要件の認識、法体系の種類、コモンロー、Civil or Code法、国際的相違、国際的協力
	情報システム/インターネットの法的概念	内部者の不正使用、ホワイトカラー/金融詐欺、産業スパイ、ハッカー、児童ポルノ、ストーカー、組織的犯罪、テロリスト、ソーシャルエンジニアリング
		知的財産、特許、登録商標
		デューケアとデューディリジェンスの概念
		プライバシー
		国際的原則
		規制問題
		自主規制
		従業員監視
		知的財産権管理
		営業機密管理
		コンテンツ管理
		倫理規定
	法令	電子署名及び認証業務に関する法律(電子署名･認証法)
		特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律（プロバイダー責任法）
		不正アクセス行為の禁止等に関する法律
		電子商取引に関する準則
		個人情報の保護に関する法律（個人情報保護法）
		著作権法
		高度情報通信ネットワーク社会形成基本法(IT基本法)
	国際標準規格	ISO(国際標準化機構)/IEC(国際電気標準会議)セキュリティ関連規格
		IETF(Internet Engineering Task Force)セキュリティ関連規格
		ITU(国際電気通信連合)セキュリティ関連規格
		FIPS(連邦政府情報処理規格)140
	国際ガイドライン	OECD(経済協力開発機構)セキュリティ関連ガイドライン
		欧州連合「個人データ処理に係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令」
		欧州評議会「サイバー犯罪条約」

大分類	中分類	小分類
事業継続経営（BCM：Business Continuity Management）	プロジェクト範囲の整備と計画	事業組織分析
		リソース要件
	事業影響度分析	脅威分析
		緊急時の分析
		クリティカル事業機能
		第三者および、ネットワーク化された関係
	リスク評価（Risk Assessment）	―――――
	事業継続と復旧の戦略	事業体の優先順位
	計画の設計と策定	緊急対応
		人員への通知
		バックアップと遠隔地保管
		連絡
		電気・ガス・水道
		ロジスティクスと補給品
		環境保護
		文書
		事業継続と再開の計画
	導入（導入前の準備）	訓練
		テストと評価
		復旧手順
	復元	主要拠点の復旧
		調達
		データ復旧
		主要拠点への再配置
	フィードバックと計画の管理	復旧後の報告
		再検討と進化の計画
		計画管理
		連絡
	文化の醸成	―――――
	計画の維持管理	―――――
	監査	―――――
	危機管理計画（CMP: Crisis Management Plan）	情報収集
		エスカレーションポリシ
		インシデント対応マニュアル
		インシデント対応
		コンピュータ証拠
		証拠収集と証拠保全
		組織内のインシデントレスポンスチーム
		災害時復旧計画、事業継続計画
		事後報告

大分類	中分類	小分類
事業継続経営（BCM：Business Continuity Management）（続き）	事業継続計画（BCP: Business Continuity Plan）	――――
	ディザスタリカバリ計画（DRP: Disaster Recovery Plan）	――――
	ガイドライン	経済産業省「事業継続計画策定ガイドライン」
		内閣府「事業継続ガイドライン　第一版」
		BCI「Good Practice Guideline 2005」
		BSI「PAS56」
その他	不正コピー防止	不正コピー対策
		権利管理技術（DRM）の要素技術
		権利記述言語の標準化
		法的要件
	電子透かし	電子透かしの基本概念
		電子透かしの方式
		電子透かしの応用形態

5 対象教育コース(資格)調査・検討

（ア）作業目的

現調査段階で教育市場に存在する情報セキュリティ教育または資格について、そのカリキュラム内容を調査して、スキル項目と対象範囲を比較検討する。

（イ）参考資料

① 経済産業省教育研究会　教育制度および資格認定制度の現状　p7～12
http://www.meti.go.jp/policy/netsecurity/edu_report.html

② ITSS ユーザー協会 資料(ITSS とベンダー試験の関係)
http://www.itssug.org/docs/isv/isvmap10.zip

（ウ）作業の詳細

教育コース内容の対象としている教育範囲を明確にするため、スキル項目と比較して教育実施内容を調査した。

① 今回取り上げる教育コースは、本 WG 参加メンバーに関係するコースならびに、市場において広く知られているものを調査対象とした。

② 作成イメージ

スキル項目リスト

スキル項目
あああああああ
いいいいいいい
ううううううう
えええええええ
おおおおおおお
かかかかかかか
きききききききき
くくくくくく
けけけけけけ
こここここここ
さささささささ
しししししししし
すすすすすすす
せせせせせせ
そそそそそそ
たたたたたた
ちちちちちち
つつつつつつ
てててててて

教育コース調査

A社 aコース	A社 bコース	A社 cコース	B社 dコース	B社 eコース	C社 fコース
○		○	○		○
○		○	○		○
○		○			○
			○		
○		○	○	○	
○		○	○		
					○
	○		○		
○	○		○		○
○	○				
○	○		○		○
○	○		○		
			○		
	○		○	○	○
○		○			○
○	○	○		○	○
○	○			○	○
	○	○	○		○
			○		

（エ）活用上の注意点

① 本ワーキングでは、スキル項目ごとの解説分量(ページ数)までは比較をしていないため、実際のコース検討の際には、テキスト内容等の確認をお勧めする。

② 現存する全ての教育コースを抽出したわけではないが、掲載されていないコースの場合には、スキル項目とカリキュラムをチェックすることで、教育対象範囲を確認することが出来る。

（オ）教育コース一覧

報告書本体にはコース名・対象資格・受講形式・教育提供機関までを掲載しているため、コースごとのスキル項目別対応状況は、別添の Excel シートを参照いただきたい。

教育コース識別番号	教育コース名	対象資格	教育形式			教育提供機関（照会先）
			座学	実機演習	ワークショップ	
①	情報セキュリティ入門	――――――	○			横河電機
②	情報セキュリティ実践講座(基礎編)	――――――	○		○	インフォセック
③	情報セキュリティ実践講座(応用編)	――――――	○		○	インフォセック
④	セキュリティーの基礎	――――――	○			IBM
⑤	暗号とデジタル署名入門	――――――	○	○		IBM
⑥	個人情報保護-基礎から対策まで	――――――	○		○	IBM
⑦	はじめようセキュリティー	――――――	○	○		IBM
⑧	セキュリティー実践編	――――――	○	○		IBM
⑨	Ciscoセキュリティー実習	――――――	○	○		IBM
⑩	セキュリティーの基礎〔CD-ROM教材〕	――――――	○			IBM
⑪	NetScreenによるセキュリティー構築実習	――――――	○	○		IBM（提供：ﾅｸｼｰｼﾞｬﾊﾟﾝ）
⑫	BS7799/ISMS準拠-情報セキュリティポリシー策定法	――――――	○			IBM（提供：アイセス）
⑬	BS7799/ISMS準拠-情報セキュリティポリシー策定演習	――――――	○		○	IBM（提供：IPｲﾉﾍﾞｰｼｮﾝｽﾞ）
⑭	身近な事例で学ぶ情報セキュリティ入門	――――――	○			大塚商会
⑮	攻撃手法から学ぶネットワークセキュリティ	――――――	○	○		大塚商会
⑯	迫り来る危機！個人情報保護対策	――――――	○			大塚商会
⑰	VirusScan	――――――	○	○		マカフィー
⑱	ePolicy Orchestrator	――――――	○	○		マカフィー
⑲	WebShield	――――――	○	○		マカフィー
⑳	IntrsuShield	――――――	○	○		マカフィー
㉑	FoundStone	――――――	○	○		マカフィー
㉒	アルティメット･ハッキング･イントロダクション	――――――	○	○		マカフィー
㉓	アルティメット･ハッキング	――――――	○	○		マカフィー
㉔	アルティメット･ハッキング･エキスパート	――――――	○	○		マカフィー
㉕	インシデントレスポンスとフォレンジックス	――――――	○	○		マカフィー
㉖	SEA/J情報セキュリティ技術認定基礎コース	CSBM(Certified Security Basic Master)	○			SEA/J認定校
㉗	SEA/J情報セキュリティ技術認定応用コーステクニカル編	CSPM(Certified Security Professional Master) of Technical	○	○		SEA/J認定校
㉘	SEA/J情報セキュリティ技術認定応用コースマネジメント編	CSPM(Certified Security Professional Master) of Management	○		○	SEA/J認定校

教育コース識別番号	教育コース名	対象資格	教育形式			教育提供機関(照会先)
			座学	実機演習	ワークショップ	
㉙	ドットコムセキュリティ情報セキュリティ啓発コース(1時間)	――――――	○			エヌ・ティ・ティ・コムチェオ
㉚	ドットコムセキュリティ情報セキュリティ入門コース(半日)	――――――	○			エヌ・ティ・ティ・コムチェオ
㉛	ドットコムセキュリティ情報セキュリティ基本コース(1日)	――――――	○		○	エヌ・ティ・ティ・コムチェオ
㉜	ドットコムセキュリティ情報セキュリティ推進者教育コース(3日)	――――――	○		○	エヌ・ティ・ティ・コムチェオ
㉝	SANS Security Essentilals (SEC 401)	GSEC	○	○		NRIセキュアテクノロジーズ
㉞	SANS Firewalls, Perimeter Protection and VPNs (SEC 502)	GCFW	○	○		NRIセキュアテクノロジーズ
㉟	SANS Hacker Techniques, exploits and Incident Handling (SEC 504)	GCIH	○	○		NRIセキュアテクノロジーズ
㊱	SANS Auditing Networks, Perimeters and Systems (AUD 507)	GSNA	○	○		NRIセキュアテクノロジーズ
㊲	SANS System Forensics, Investigation and Response (SEC 508)	GCFA	○	○		NRIセキュアテクノロジーズ
㊳	SANS Security Leadership Essentials (MGT 512)	GSLC	○		○	NRIセキュアテクノロジーズ
㊴	SANS +S™ Training Program for the CISSP® Certification Exam (MGT 414)	CISSP	○			NRIセキュアテクノロジーズ
㊵	(ISC)2公式 CISSP® 10ドメインレビューセミナー	CISSP	○			ISC2
㊶	Comptia Security+	Comptia Security+ (SY0-101)	○			CompTIAトレーニングパートナー
㊷	MCA Security	MCA Security (M10-400)	○			MCAトレーニングセンター
㊸	CISA レビューコース	CISA	○			ISACA
㊹	公認情報セキュリティマネージャー(CISM)レビューコース	CISM	○			ISACA
㊺	情報セキュリティアドミニストレータ	情報セキュリティアドミニストレータ(SU)	○			
㊻	テクニカルエンジニア(情報セキュリティ)	テクニカルエンジニア(情報セキュリティ)(SV)	○			

6 職種別必要スキル項目検討

（ア）作業内容

情報セキュリティに関わる職種を選定・分類するとともに、前記 4 の情報セキュリティスキル項目をもとに、それぞれの職種ごとに必要なスキル項目の検討を行った。

① 代表的な職種の選定

IT の提供者、組織のトップ、利用者の 3 つの観点で職種を洗い出し、次の 7 職種を代表的な職種として選定した。

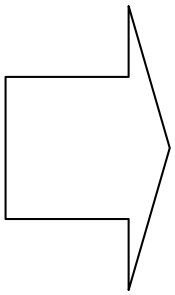
1. IT の提供者として次の 5 職種を選定した。
   設計、NW/SYSTEM 構築、アプリ開発、ポリシー構築、運用
2. 利用者については、組織において情報を活用する全ての人材を対象とした。
3. 組織のトップとして、CISO を役員レベルで想定した。

② 必要スキルの表示方法

実装あるいは対応を実施する者は◎、知識として必要な場合は○、業務に直接影響ない場合は×を表示した。

③ 作成イメージ

スキル項目
ああああああ
いいいいいい
ううううううう
えええええええ
おおおおおお
かかかかかか
きききききき
くくくくくく
けけけけけけ
ここここここ
さささささささ
ししししししし
すすすすすす
せせせせせせ
そそそそそそ
たたたたたた
ちちちちちち
つつつつつつ



職種 A	職種 B	職種 C	職種 D	職種 E
○	◎	○	×	×
○	◎	×	○	×
○	◎	×	○	×
◎	◎	×	○	×
○	○	×	◎	○
○	○	×	◎	×
◎	○	×	○	×
◎	◎	×	○	×
○	◎	×	○	×
○	◎	×	○	×
○	◎	○	○	×
○	×	○	×	○
◎	×	○	×	○
◎	×	○	×	○
○	×	○	×	◎
○	×	○	×	◎
○	×	○	×	○
◎	×	○	×	○

（イ）活用上の注意点

① 職種は代表的なものであり、組織によって複数職種を兼務していたり、対象者がいない職種がある場合が想定される。
このため、各組織ごとに対象となる職種に漏れがないか確認し、漏れている職種は配置する必要がある。

② 実際の業務と対象職種をかぶせてみることで、漏れているセキュリティ対策が確認できる。

③ セキュリティ人材以外が実装するものも考えられるため、スキル項目に掲載されている項目に責任を持つものがいるか確認し、漏れている項目は担当を決めるなどする必要がある。

（ウ）職種別必要スキル項目一覧

報告書本体には中分類までを掲載しているため、小分類、備考および職種別のコメントは、別添の Excel シートを参照いただきたい。

大分類	中分類	職種						
		設計	NW/SYSTEM構築	アプリ開発	ポリシー構築	運用	利用者	CISO
情報セキュリティマネジメント	マネジメント技術	×	×	×	◎	○	○	◎
	リスク分析技術	×	×	×	◎	○	○	◎
	情報セキュリティポリシー	×	×	×	◎	○	○	◎
	費用対効果	×	×	×	○	×	×	◎
	人員計画	×	×	×	◎	×	○	◎
	教育･訓練	×	×	×	○	×	×	◎
	情報セキュリティ監査	○	×	×	◎	○	×	◎
	関連知識	○	○	×	◎	○	×	◎
セキュリティアーキテクチャ	プラットフォームアーキテクチャー	◎	◎	◎	○	◎	○	○
	セキュリティモデル	◎	○	○	○	×	○	○
	評価基準の原則	◎	○	○	○	×	×	○
	保護メカニズム	◎	○	○	○	×	○	○
	システムライフサイクルセキュリティ	◎	◎	◎	○	○	×	◎
	システム開発管理	◎	◎	◎	○	○	×	◎
ネットワークインフラセキュリティ	ネットワーク設計技術	○	◎	×	○	◎	×	○
	セキュアなインターネット、イントラネット、エクストラネット	◎	◎	◎	○	◎	×	○
	ネットワークアクセスコントロール	○	◎	×	○	◎	×	○
	VPN(Virtual Private Network)	○	◎	○	○	○	○	○
	無線LAN	◎	◎	×	○	○	×	○
アプリケーションセキュリティ【全般】	アプリケーション環境とセキュリティ管理	○	○	◎	○	○	○	◎
	アプリケーションとシステムの脆弱性と脅威	○	◎	◎	○	◎	×	○
	セキュリティ制御	○	◎	◎	○	○	○	○
アプリケーションセキュリティ【Web】	Webサーバに対する脅威	○	◎	◎	○	◎	○	○
	Webサーバのセキュリティ対策	◎	◎	○	○	◎	×	○
	Webサーバの運用	○	○	○	○	◎	×	○
	Webアプリケーション設計	○	○	◎	○	◎	×	○
	Webブラウザのセキュリティ	○	○	○	○	◎	○	○
	Web関連プロトコルの基礎知識	○	◎	◎	○	◎	○	○
アプリケーションセキュリティ【電子メール】	メールサーバに対する脅威	○	◎	○	○	◎	○	○
	メールサーバのセキュリティ対策	◎	◎	○	○	◎	×	○
	メールクライアントのセキュリティ	○	◎	×	○	◎	○	○
	メールサーバの運用	○	○	×	○	◎	×	○
アプリケーションセキュリティ【DNS(Domain Name System)】	DNSサーバに対する脅威	○	◎	○	○	◎	×	○
	DNSサーバセキュリティ対策と構成	◎	◎	○	○	◎	×	○
	DNSサーバの運用	○	○	×	○	◎	×	○

大分類	中分類	職種						
		設計	NW/SYSTEM構築	アプリ開発	ポリシー構築	運用	利用者	CISO
OSセキュリティ【Unix】	ログ管理	○	○	×	○	◎	×	○
	パッチ適用管理	○	○	×	○	◎	○	○
	サービスの管理	○	◎	×	○	◎	×	○
	ファイルシステム管理	○	◎	×	○	◎	×	○
	アカウント管理	◎	◎	×	○	◎	×	○
OSセキュリティ【Windows】	構成・設定管理	○	◎	×	○	◎	×	○
	パッチ適用管理	○	○	×	○	◎	○	○
	監査	◎	○	×	○	◎	×	○
	ログ管理	◎	○	×	○	◎	×	○
	プロセス管理	○	○	×	○	◎	×	○
	サービス管理	○	◎	×	○	◎	○	○
	ファイルシステム管理	○	◎	×	○	◎	×	○
	アカウント管理	◎	◎	×	○	◎	○	○
	ネットワーク保護	○	◎	×	○	◎	○	○
OSセキュリティ【TrustedOS】	強制アクセス制御の概念（MAC）	○	◎	×	○	○	×	○
ファイアーウォール	ファイアーウォールの導入・運用	○	◎	×	○	◎	×	○
	NAT(Network Address Translation)	○	◎	×	○	◎	×	○
	ネットワークアクセスコントロール	○	◎	×	○	◎	×	○
侵入検知	侵入検知システムの導入・運用	◎	◎	×	○	◎	×	◎
	侵入検知システムの機能	○	◎	×	○	◎	×	○
	検出アルゴリズム	○	◎	×	○	◎	×	○
	検出方法	○	◎	×	○	◎	×	○
	侵入検知システム	○	○	×	○	◎	×	○
ウィルス	管理体制	○	○	×	○	○	○	◎
	感染後のポリシー	○	○	×	○	◎	○	○
	予防ポリシー	○	○	×	○	◎	○	◎
	発病	○	○	×	○	◎	◎	○
	検出方法と駆除	○	◎	×	○	◎	○	○
	感染	○	○	×	○	◎	◎	○
	種類	○	○	○	○	◎	○	○

大分類	中分類	職種						
		設計	NW/SYSTEM構築	アプリ開発	ポリシー構築	運用	利用者	CISO
セキュアプログラミング技法	プログラミング言語とツール	○	○	◎	×	×	×	×
	Webアプリケーション	○	○	◎	○	○	×	○
	データベース	○	○	◎	○	○	×	○
	アプリケーション全般	○	○	◎	○	○	×	○
	XML(Extensible Markup Language)	○	○	◎	×	×	×	○
	PHP(Hypertext Preprocessor)	×	○	◎	×	×	×	○
	JAVA	×	○	◎	×	×	×	○
	Perl	×	○	◎	×	×	×	○
	VB/ASP	×	○	◎	×	×	×	○
	C/C++	×	○	◎	×	×	×	○
	Unix	◎	◎	◎	×	◎	×	○
	コンパイラ･仮想マシン	×	○	◎	×	×	×	○
	Windows	◎	○	◎	×	◎	×	○
	オブジェクト指向技術	○	○	◎	×	×	×	○
	データベースとデータウェア保管庫の脆弱性、リスク、防護	○	○	◎	○	○	×	○
セキュリティ運用	物理セキュリティ	×	○	○	○	○	○	◎
	人的セキュリティ	×	×	×	◎	○	○	◎
	リソース保護	○	○	○	○	◎	○	◎
	定常運用時のセキュリティ確保	○	○	○	○	◎	○	◎
	異常時対応	○	○	×	○	◎	×	○
	運用関連情報（脆弱性情報･対策情報･攻撃情報･被害情報）	○	◎	◎	○	◎	×	○
セキュリティプロトコル	アプリケーション層	◎	◎	◎	○	◎	○	○
	トランスポート層	◎	◎	◎	○	◎	○	○
	ネットワーク層	◎	◎	◎	○	◎	○	○
	データリンク層	◎	◎	◎	○	◎	○	○
認証	ID管理と認証	◎	○	×	○	◎	×	◎
	パスワード認証	◎	◎	○	○	◎	○	○
	バイオメトリック認証	◎	◎	○	○	◎	○	○
	認証デバイス	◎	◎	○	○	◎	○	○
	認証プロトコル	◎	◎	○	○	◎	×	○
	Web認証	◎	◎	○	○	◎	○	○
	システム認証	◎	◎	○	○	◎	×	○
	シングルサインオン	◎	◎	○	○	◎	×	○
アクセス制御	効果的なパスワード管理	◎	○	○	○	◎	○	◎
	認可	◎	◎	○	○	○	○	○
	アクセス制御手法	◎	○	○	○	○	×	○
	アクセス制御の管理	◎	◎	×	○	◎	×	○

大分類	中分類	職種						
		設計	NW/SYSTEM構築	アプリ開発	ポリシー構築	運用	利用者	CISO
PKI(Public Key Infrastructure)	PKIの利用	○	○	○	○	○	○	○
	証明書と認証	◎	◎	×	○	○	×	○
	証明書失効	◎	◎	×	○	◎	×	○
	信頼モデル	◎	◎	×	○	◎	×	○
	契約モデル	◎	○	×	○	○	×	○
	記述とデータ方式	◎	○	○	○	○	×	○
	規格	◎	○	○	○	○	×	○
	公開ﾘﾎﾟｼﾞﾄﾘ	◎	○	×	○	○	×	○
	認証局(CA)の構築と運用	◎	◎	×	○	◎	×	○
	法的枠組み	○	○	×	○	○	×	◎
	PKIの要素技術	◎	◎	○	○	○	×	○
	PKIが提供するサービス	◎	◎	○	○	○	○	○
暗号	公開鍵暗号	◎	◎	○	○	○	×	○
	共通鍵暗号	◎	◎	○	○	○	×	○
	ハッシュ関数	◎	◎	○	○	○	×	○
	暗号用乱数	○	○	○	○	○	×	○
	鍵管理	○	◎	○	○	○	×	○
	ゼロ知識証明	○	○	○	○	○	×	○
	その他の暗号方式	○	○	○	○	○	×	○
	暗号解読･強度評価	◎	○	○	○	○	×	○
	暗号に関する問題	○	○	○	○	○	○	◎
	暗号の代替	○	○	○	○	○	×	○
電子署名	電子署名の利用	○	○	◎	○	○	○	○
	電子署名の要素技術	○	◎	○	○	○	×	○
	電子署名の仕組み	○	◎	○	○	○	×	○
	電子署名の利点	○	○	○	○	○	○	○
	ﾒｯｾｰｼﾞﾀﾞｲｼﾞｪｽﾄとその他のﾒｯｾｰｼﾞ完全性ｺｰﾄﾞ	○	◎	○	○	○	×	○
不正アクセス手法	遠隔不正侵入･操作	○	○	○	○	○	×	○
	サービスの停止	○	○	○	○	○	○	○
	盗聴行為	○	○	○	○	○	○	○
	偵察行為	○	○	○	○	○	×	○
	情報収集	○	○	○	○	○	○	○
	古典的不正アクセス技法	○	○	○	○	○	○	○

大分類	中分類	職種						
		設計	NW/SYSTEM構築	アプリ開発	ポリシー構築	運用	利用者	CISO
法令･規格	基準･指針･ガイドライン等	◎	○	○	◎	◎	○	◎
	主要法体系	○	○	○	○	○	○	◎
	情報システム/インターネットの法的概念	○	○	○	○	○	○	◎
	法令	◎	×	×	◎	○	×	◎
	国際標準規格	○	○	○	○	○	×	◎
	国際ガイドライン	○	×	×	○	○	×	◎
事業継続経営（BCM：Business Continuity Management)	プロジェクト範囲の整備と計画	○	×	×	○	×	×	◎
	事業影響度分析	○	×	×	◎	○	○	◎
	リスク評価（Risk Assessment)	○	×	×	◎	○	×	◎
	事業継続と復旧の戦略	○	×	×	◎	○	×	◎
	計画の設計と策定	○	×	×	◎	◎	×	◎
	導入（導入前の準備）	○	×	×	○	○	×	◎
	復元	○	×	×	○	◎	×	◎
	フィードバックと計画の管理	○	×	×	◎	◎	×	◎
	文化の醸成	×	×	×	○	○	×	◎
	計画の維持管理	×	×	×	○	○	×	◎
	監査	×	×	×	○	○	×	◎
	危機管理計画（CMP: Crisis Management Plan)	○	○	○	◎	◎	×	◎
	事業継続計画（BCP: Business Continuity Plan)	×	×	×	×	○	×	◎
	ディザスタリカバリ計画（DRP: Disaster Recovery Plan)	×	×	×	×	○	×	◎
	ガイドライン	×	×	×	×	○	×	◎
その他	不正コピー防止	◎	◎	◎	○	○	○	◎
	電子透かし	○	◎	○	○	○	×	○

7 職種別キャリアパス作成

（ア）作業内容

職種別の必要スキル項目と、対象教育コースのカリキュラム内容を確認し、職種別のレベルに応じて推奨する教育コースを研修ロードマップとして作成した。

（イ）作業の詳細

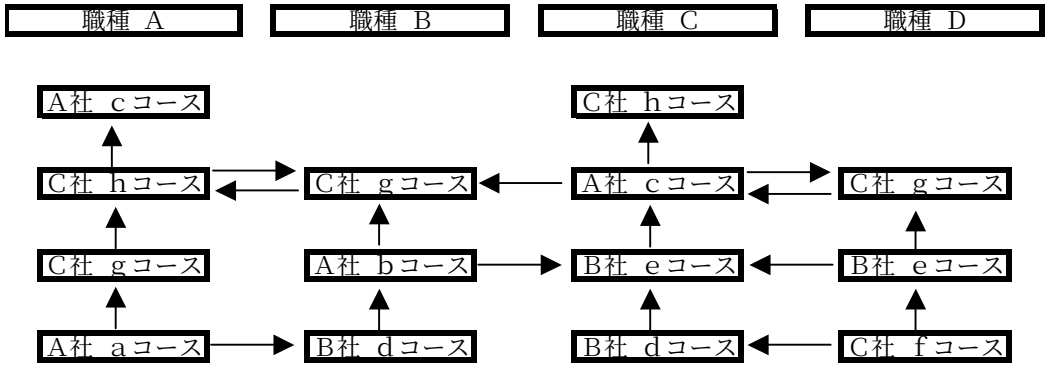
職種ごとの人材育成ロードマップを明確にするため、職種別の必要スキル項目に対して、調査した教育コースの内容の網羅性を検討し、想定する職種別の育成過程として、レベル別に教育コースを組み込んだ。

① 職種別の必要スキル項目と、教育コースの該当項目が近いほど、推奨する教育コースとして考える。

② 教育コースの内容が同等であれば、知識を与える座学コースを基礎とし、実機演習やワークショップを伴うコースを応用と位置づけた。

③ 作成イメージ

職種別研修ロードマップ



（ウ）活用上の注意点

① 個人スキルの面での活用
同一職種内でのスキルアップだけでなく、キャリアチェンジの際の教育検討にも活用することができる。

② 組織面での活用
セキュリティ対策を考えた人事異動の際の参考にすることができる。

③ 職種は代表的なものであり、各組織ごとの組織体制や職務分担によって必要教育コースは変わることに注意する必要がある。

④ 教育コースによりロードマップを示しているが、各教育コースを受講すればその職種になれるものではなく、実際は教育コースで学習したスキルを活用することによりキャリアは形成されることを理解する必要がある。

（エ）職種別キャリアパス

前記「5 対象教育コース(資格)調査・検討」の「（オ）教育コース一覧」に記載してある教育コース識別番号を基に、対象職種別ごとの教育コース受講後想定レベルを確認いただきたい。

職種別 受講後想定レベル	① 設計	② NW/SYSTEM構築	③ アプリ開発	④ ポリシー構築	⑤ 運用	⑥ 利用者	⑦ CISO
ハイレベル	㊱	㉞㉟㊲	㉟㊲	㊱	㉞㉟㊱㊲		
↑	㉝㊳	㉝㊳	㉝㊳	⑬㉝㊳	㉝㊳		⑬㉝㊳
	㊴㊵	㊴㊵	㊴㊵	⑫ ㊴ ㊵ ㊸ ㊹	㉕㊴㊵		⑫ ㉕ ㊴ ㊵ ㊸㊹
	⑤ ⑧ ⑮ ㉗ ㊻	⑤ ⑧ ⑨ ⑪ ⑮ ⑱ ⑲ ⑳ ㉑㉔㉗㊻	⑤ ⑧ ㉔ ㉗ ㊻	③ ⑧ ⑮ ⑱ ⑲ ⑳ ㉑ ㉔ ㉘㉜㊺㊻	③ ⑧ ⑨ ⑪ ⑮ ⑰ ⑱ ⑲ ⑳ ㉑ ㉔ ㉗ ㉜㊻	③㊼	③ ㉑ ㉔ ㉘ ㉜㊺
	⑥㉖㊶	⑥ ㉒ ㉓ ㉖ ㊶	⑥ ㉒ ㉓ ㉖ ㊶	② ⑥ ㉒ ㉓ ㉖㊶	② ⑥ ㉒ ㉓ ㉖㊶㊷	② ⑥ ⑦ ⑭ ㉖㊶	② ⑥ ⑭ ㉒ ㉓㉖㊶
↓ エントリーレベル	①④⑩	①④⑩	①④⑩	①④⑩	① ④ ⑩ ㉙ ㉚㉛	① ④ ⑩ ⑯ ㉙㉚㉛	① ④ ⑩ ㉙ ㉚㉛

8 最後に

（ア）報告書添付物

本報告書の各項目の説明においても触れているが、報告書に関する詳細資料として、Excel ファイルにより「スキル項目(兼)職種別必要スキル」「教育コース一覧」「教育コース内容チェックリスト」「職種別対応教育コースロードマップ」を収録している。適宜内容をご確認いただきたい。

（イ）人材育成におけるその他の必要事項

本ワーキングの調査では人材育成のロードマップを示すことを目的として調査検討を行ってきた。スキルセットとしての知識の継承であるこれらの教育コースは、昨今の組織や社会を取り巻く環境の中で、広範となり高度化してきている情報セキュリティ技術を知識として後進に継承し、新たな防衛および対策技術を培うには重要な要素である。

しかし、本ワーキングで調査検討した教育コースの実施により組織の人材を効率的に育成しただけでは、故意や過失での情報セキュリティインシデントによる危険や損害から組織を守ることはできない。

多くの組織において意識やモラルを高め、セキュリティインシデントを防止するために、正社員化や賞罰規程の導入などが行われたが、組織管理の視点で長期的に見るとほとんど影響しないといわれている。逆に組織成立要件である、意思疎通・貢献意欲・共通目的の三つを継続的に高めることが、組織体として重要となる。

つまり、人材育成においてはスキルセットとマインドセットの両立が重要であり、組織における個人のモチベーションを高く保ち続けるということが、情報セキュリティインシデントを未然に防ぐ重要なポイントといえる。

本ワーキングで調査検討した教育コースについては、あくまでもスキルセットを効率的に取得していくためのロードマップである。

マインドセットの強化については、本ワーキングの主目的ではないため調査検討の対象からは外したが、組織ロイヤルティ、モラルといった面で重要であり、各組織でスキルセットの向上と同様にマインドセットを高める仕組みが取り入れられるよう、メソッドを確立いただきたい。

（ウ）組織デザインの検討

今後は、各組織単位で現状の組織体制に合わせて情報セキュリティ人材の配置を考えるのではなく、情報セキュリティ対策として考えた場合のあるべき姿に対する組織体制を検討し、その組織における情報セキュリティ人材の適正配置を検討する必要もあるだろうと考える。

現状のヒエラルキーのもとで情報セキュリティ対策を検討した場合、他の事業や組織の論理が優先され、本来必要とされるべき情報セキュリティ対策が行えないというジレンマがある。このため、視点を変えて組織を見つめなおす必要もあるというのが本ワーキングでのメンバーの一致する意見でもあった。

最後になるが、組織体制の見直しも含めて情報セキュリティ人材を配置する際の参考としていただければと思い、PeopleCMM や経営組織論の文献等を参考にしつつ、本ワーキングの調査検討にあたったことを、ここに記して締めくくることとする。

NPO 日本ネットワークセキュリティ協会

情報セキュリティ推奨教育検討ワーキンググループ