IPA
Information-technology Promotion Agency, Japan

15 情経第 1612 号

情報セキュリティスキルマップ構築の調査研究

2004 年 3 月

独立行政法人 情報処理推進機構

はじめに

高度情報通信社会における安全性・信頼性の向上において、情報セキュリティに関する技術、知識、分析能力等を有する人材を育成し、確保していくことが喫緊の課題となっている。平成 14 年度 IPA では、「情報セキュリティプロフェッショナル育成に関する調査研究」（以下「平成 14 年度調査」という）を実施し、企業、組織及び地方自治体等において情報セキュリティにたずさわる人材（＝ 情報セキュリティプロフェッショナル）の現状やその育成に関する問題点について調査を行った。

調査結果からは、企業、組織、自治体のいずれにおいても情報セキュリティの確保・維持に必要な人材の不足が認識されていること、情報セキュリティにたずさわる人材の育成・確保には困難が伴うこと、教育機関や組織内における情報セキュリティ教育の現状や成果と求める人材との間には「ミスマッチ」が存在すること、などが明らかになった。

加えて、平成 14 年度調査においては、上の調査結果を踏まえ、情報セキュリティプロフェッショナルに必要とされる知識を 16 項目の大分類と 400 以上の小分類に体系化した「情報セキュリティに関するスキルマップ」を作成した。このスキルマップは、主に情報セキュリティプロフェッショナルの「評価」と「教育」を目的とし、各組織の要求条件に応じたカスタマイズの上で活用可能とすることを目指すものである。

本調査研究では、平成 14 年度調査において作成した「情報セキュリティに関するスキルマップ」を、より広く利用し易いものとするため、時勢の変化や技術分野の進展に合わせたアップデートを行い「評価のものさし」としての完成を図ると共に、スキルマップの活用に向けた方策について検討を行った。加えて、情報セキュリティに関する個別の業務やタスクにおいて求められるスキルを整理した「スキルモデル」や利用者が自己のスキルのレベルをチェックするサンプルテストの検討を行った。

本調査研究の成果は、広く一般に向け公開し、わが国おける情報セキュリティ関連人材の育成において活用されることを目標とするものである。

－ 目　　次 －

1．調査研究の概要

本調査研究は、わが国における情報セキュリティ人材育成推進に寄与することを目的として、主に以下の 3 点について検討を行なった。

- 情報セキュリティに関する技術知識体系的に整理した「**情報セキュリティのためのスキルマップ**」のアップデート
- 情報セキュリティに関する個別の業務やタスクにおいて求められるスキルとそのレベルを整理した「**スキルモデル**」の策定
- 情報セキュリティに関する基本的な知識について、自己のレベルをセルフチェックできる問題と解答のリストである「**スキルレベルチェックテスト**」の策定

上記の検討にあたっては、特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）の教育部会スキルマップ検討ワーキンググループが調査研究活動を担当した（メンバを次ページ表 1-1 に示す）。

さらに、情報セキュリティ分野の有識者へのヒアリング調査ならびに情報セキュリティに関連する業務にたずさわっているエンジニアやコンサルタント等を対象としたグループインタビューを実施した。

図 1-1 に本調査研究の全体概要を示す。

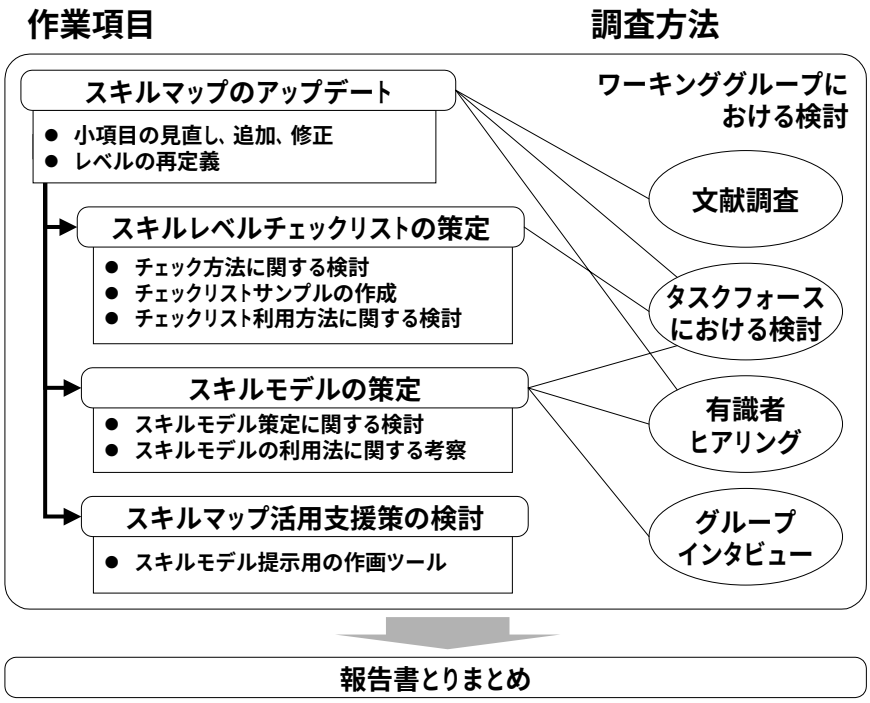


図 1-1　本調査研究の全体概要

表 1-1　NPO 日本ネットワークセキュリティ協会（JNSA）
教育部会スキルマップ検討ワーキンググループ　メンバー

No.	氏名	所属	TF メンバ[1]
1	小杉　聖一	NEC ソフト	○
2	佐藤　由佳子	NTT コミュニケーションズ	
3	小松　伸久	TIS	
4	園田　道夫	アイ・ティ・フロンティア	
5	岩切　裕一	アイセス	
6	米川　敦	アイタック	○
7	長谷川長一	アライドテレシス	
8	小林　忍	アライドテレシス	
9	大久保　祐子	アライドテレシス	○
10	佐藤　友治	インターネット総合研究所	
11	林　簡	インフォセック	
12	杉谷　郁夫	グローバルエース	
13	黒坪　則之	クロスヘッド	○
14	池野　修一	セコム IS 研究所	
15	近藤　弓末	ソニー	○
16	河野　省二	ディアイティ	
17	安田　直義	ディアイティ	○
18	松田　剛	ヒューコム	○
19	舘岡　均	横河電機	○
20	塚本　克治	工学院大学	
21	伏見　諭	情報数理研究所	
22	佐藤　憲一	大塚商会	
23	宇崎　俊	中央青山監査法人	
24	佐々木　良一	東京電機大学	
25	若林　勝広	日本ネットワークアソシエイツ	○
26	冨田　高樹	富士総合研究所	○
27	佐久間　敦	富士総合研究所	○

[1] TF(タスクフォース)メンバ)：「２．２．２ スキルマップの構築作業について」参照

２．「情報セキュリティのためのスキルマップ」の構築

本調査研究では、情報セキュリティプロフェッショナルの育成の推進に資することを目的として、「情報セキュリティのためのスキルマップ」（＝ 以下、単に「スキルマップ」と呼ぶ）の構築について検討を行った。

本章では、スキルマップの構築に関して、以下の項目について述べる。

1. 「情報セキュリティのためのスキルマップ」について
2. スキルマップのアップデートについて
3. 2003 年度版スキルマップの概要と見直しの論点
4. 2003 年度版スキルマップの詳細
5. スキルマップの活用方法に関する考察

２．１ 「情報セキュリティのためのスキルマップ」について

２．１．１ スキルマップ構築の背景・経緯

情報処理推進機構（IPA）は、2002 年度「セキュリティ対策研究開発等事業」の一環として「情報セキュリティプロフェッショナル育成に関する調査研究」を実施した[2]。

同調査研究では、企業や地方自治体における情報セキュリティにたずさわる人材の育成の状況、大学、専門学校等の情報セキュリティ教育の現状について把握するために、表 2-1 に示す調査を行った。

これらの各調査から、情報セキュリティにたずさわる人材育成に関して、以下のような問題や課題が存在している状況がうかがえる。

（1）不足する情報セキュリティ人材と遅れる人材の確保

情報システム関連の製品やサービスを開発、提供する「ベンダ企業」、それらの製品・サービスを自社の情報システムやネットワークに導入し、運用する「ユーザ企業」のいずれにおいても、過半数の企業が情報セキュリティにたずさわる人材の不足感を感じている。

その一方で、ともに積極的な増員を予定している企業それほど多くは無く、特にユーザ企業において情報セキュリティの専門人材を採用、確保しようとする動きは鈍い。

（2）情報セキュリティにたずさわる人材の育成の難しさ

情報セキュリティに関する技術や知識はそれ自体を独立して習得できるものではなく、基礎的な IT やネットワークに関する技術知識や業務経験等の土台として、相互に関連付けながら学んでいく必要がある。対応する学問分野も、情報科学、ネットワーク技術、OS 技術から経営、社会科学、法律まで非常に裾野が広い。また、単なる技術知識だけではなく、未知の現象に対する応用力や適応力が重要となる。加えて、情報セキュリティを含む IT 分野においては、技術の進化と方向性の変化のスピードが速く、

コースやカリキュラムの設定を難しくしている。

（3）情報セキュリティにたずさわる人材の多様性に起因する混乱

そもそも一口に「情報セキュリティエンジニア」あるいは「情報セキュリティ技術者」といっても、ベンダ企業／ユーザ企業といった業態や業種、また、エンジニア自身がたずさわる業務によって、求められる知識やスキル、業務経験等はまったく異なっている。にもかかわらず、情報セキュリティ分野の歴史の浅さも手伝って、どのような人にどのような内容・水準の知識やスキルが求められるかが、IT にかかわる他の分野以上に整理されていないのが現状である。それゆえ、情報セキュリティにたずさわる人材のキャリアパスをどう考えるかについて基準のない企業も多い。

表 2-1　2002 年度「情報セキュリティプロフェッショナル育成に関する調査研究」の概要

タイトル	調査方法	主な調査内容
A．企業（ベンダ企業／ユーザ企業）の情報セキュリティにたずさわる人材の現状と育成に関する調査	1. 情報セキュリティ関連の製品、サービスの開発／提供／販売等を行っているベンダ企業 2. 情報システムを運用／管理しているユーザ企業（一般企業） 上記 1. 及び 2. の国内企業合計 1,000 社に調査票を郵送／回収／分析（有効回答率 17%）	・ 情報セキュリティにたずさわる人材の現状 ・ 情報セキュリティにたずさわる人材に要求されるスキル ・ 情報セキュリティにたずさわる人材の育成の現状と課題
B．教育機関における情報セキュリティ教育の現状に関する調査	情報セキュリティ教育を提供する大学や専門学校に対して、ヒアリング調査を実施（合計 7 者）	・ 情報セキュリティにたずさわる人材を育成するために提供されているコースやカリキュラムの状況 ・ 情報セキュリティ教育の実績 ・ 情報セキュリティ教育における問題点・課題
C．地方自治体における情報セキュリティにたずさわる人材の現状と育成に関する調査	全国の地方自治体（都道府県／政令指定都市・東京 23 区／市／町／村）を対象として、合計 500 自治体に調査票を郵送／回収／分析（有効回答率 31%）	・ 地方自治体における情報セキュリティポリシー ・ 情報セキュリティに関する基本体制 ・ 情報セキュリティ運営に関わる職員の教育
D．地方企業における情報セキュリティにたずさわる人材の現状に関する調査	SI 登録をしている情報サービス企業を中心とした地方のベンダ企業を対象として、合計 500 社に調査票を郵送／回収／分析（有効回答率 16%）	・ 地方企業における情報セキュリティにたずさわる人材の現状 ・ 地方企業における情報セキュリティにたずさわる人材のスキル ・ 地方企業における情報セキュリティにたずさわる人材の教育

[2] http://www.ipa.go.jp/security/fy14/reports/professional/ikusei-seika-press.html参照

上記の（1）～（3）に見られる問題・課題を背景として、情報セキュリティ人材にかかわる「ミスマッチ」が様々な文脈で生じている。

特に、企業と教育機関の間では、企業側は基礎力と実践的能力を身に付ける教育を望んでいる一方で、教育機関でこれまで行なわれていた教育が企業での実務をあまり考慮したものでなかったなど、必ずしも教育機関における情報セキュリティ人材教育が企業側のニーズを満たすものにはなっていなかった。逆に、企業の側も、大学と共同研究開発などを行ってきたものの、積極的に大学教育に関与しようとするケースは少なく、学生の採用の確保を主目的とする限定的な関係にとどまっていたことが指摘されている。

このような人材の需要側（＝企業）と供給側（＝教育機関）の「ミスマッチ」の溝は深いものとなっている（図 2-1）。

背景	**高度な情報セキュリティに関する技術、知識、分析能力等を有する人材は、質・量ともに不足**	
ミスマッチ	**需要側 (企業、自治体等)**	**供給側 (教育機関等)**
	● **即戦力** ● **応用力** ● **専門分野の明示**	● **基礎研究(大学院)** ● **製品操作(企業教育)** ● **先生・講師の勘と経験**

図 2-1　ミスマッチの認識

（出典：2002 年度 IPA「情報セキュリティプロフェッショナル育成に関する調査研究」）

2．1．2 2002 年度版スキルマップの試作とそのコンセプト

上記のような情報セキュリティに関する問題・課題の原因の一つは、情報セキュリティにかかわる様々な職種や業務において、どのような技術知識が必要になるかが整理されていなかったことがあげられる。

そこで、上記 2002 年度「情報セキュリティプロフェッショナル育成に関する調査研究」の一環として、情報セキュリティのたずさわる人材に求められる技術知識を体系的に整理した「情報セキュリティのためのスキルマップ」の試作とその活用に向けた検討を行った。

以下に、スキルマップのコンセプトを示す。

（1）スキルマップの定義と構成

スキルマップとは、「情報セキュリティにたずさわる人材に求められる能力（スキル）のうち技術要素に関する知識項目に着目し、これを基本要素まで分解し体系的に整理することで、人材の有する知識の種類、範囲、レベルを測るための共通の基準を与えることを目的とするもの」として定義される。

2002 年度に試作したバージョンでは、情報セキュリティプロフェッショナルに必要

とされる知識を表 2-2 に示す 16 項目の大分類と 400 以上の小分類に体系的に整理した。表 2-3 にスキルマップの抜粋を示す。また、スキルマップを利用した人材のスキルのレベルの表現形式の一例として、レーダーチャート形式を作成した（図 2-2、図 2-3 参照）。

（2）スキルマップの目標

スキルマップは以下の 2 点を目標とする。

- 情報セキュリティに関する技術知識の体系を整理し、その知識体系を基盤とした評価の尺度（ものさし）を与えることにより、情報セキュリティにたずさわる人材に求められる各技術知識の水準（レベル）を定量的に表現できる表現形式を導入すること
- 将来的なゴールとして、情報セキュリティの技術に関する知識以外の、能力や業務経験（あるいは適性）といった要素も包含できるより広義なスキルを整理、構造化し、人間が理解できる表現形式で可視化すること

（3）スキルマップの特徴

スキルマップでは、精緻な学問的な分類体系の構築を目指すというより、企業や組織の現場で情報セキュリティにかかわる業務にたずさわっている人に使ってもらえることを念頭においている。それゆえ、実用本位、実務本位の観点から、情報セキュリティにたずさわる開発者、システムエンジニア、コンサルタントら自らが作成した点にもっとも大きな特徴がある。それゆえ、スキルマップの分類は、必ずしも既存の情報セキュリティ関連の学問体系や教育カリキュラムの構成と一致しているわけではない点に注意する必要がある。

（4）スキルマップの活用場面

スキルマップの活用場面として、以下のようなものを想定している。

- 情報セキュリティにたずさわる人材の採用する際の能力要件定義として
- 社内、組織内の人材育成における目標設定、効果測定の評価基準（criteria)として
- 教育機関、教育サービスベンダにおけるカリキュラムやテキスト、研修実施の参照ベースとして

表 2-2　2002 年度版スキルマップの大分類

フェーズ		知識項目	備考（補足説明）
ライフサイクル	a.要件定義・概要設計	1.情報セキュリティポリシー	人的/物理的対策
	b.詳細設計・構築	2.ネットワークインフラセキュリティ	
		3.サーバアプリケーションセキュリティ	Web/Mail/DNS/ディレクトリ
		4.OS セキュリティ	Unix/Windows/TrustedOS
		5.ファイアーウォール	
		6.侵入検知システム	
		7.ウィルス	
	c.開発・実装	8.セキュアプログラミング技法	
	d.運用・監査	9.セキュリティ運用	ログ管理/解析/パッチ管理
ライフサイクル外	e.基盤技術	10.セキュリティプロトコル	
		11.認証	
		12.PKI	
		13.暗号	
		14.署名	
	f.関連知識	15.攻撃手法	
		16.法令・規格	

（出典：2002 年度 IPA「情報セキュリティプロフェッショナル育成に関する調査研究」）

表 2-3　2002 年度版スキルマップの例（7.ウィルス）

大分類	知識区分	小分類
ウィルス	応用知識（Level.2）	ウィルス種類と感染位置
		発病時の行動パターン
		ウィルスの自己防御機能
		防御システムの構築（ウィルスからの防御システム構造）
		流行の傾向と予測
		ログの集中管理
		対応ポリシー（感染時）
		設定ポリシー
	基礎知識（Level.1）	構成要素
		スキャン方式と検出方法
		感染媒体の種類と感染方法
		分類および定義の理解
		定義ファイルの理解
		定義ファイルのアップデート

（出典：2002 年度 IPA「情報セキュリティプロフェッショナル育成に関する調査研究」）

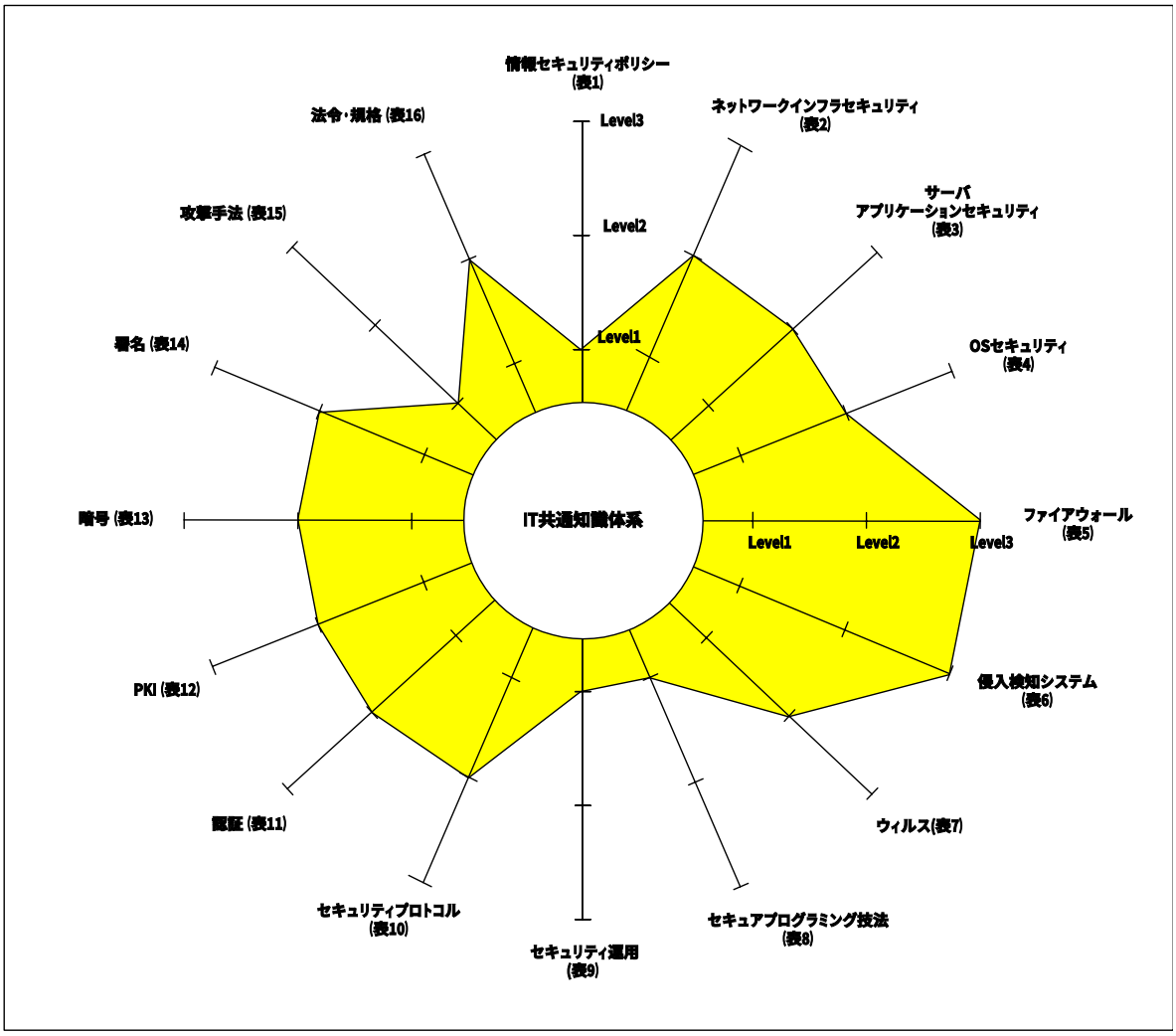


図 2-2　2002 年度版スキルマップを利用した人材のスキルレベルの表現例(構築系技術者)

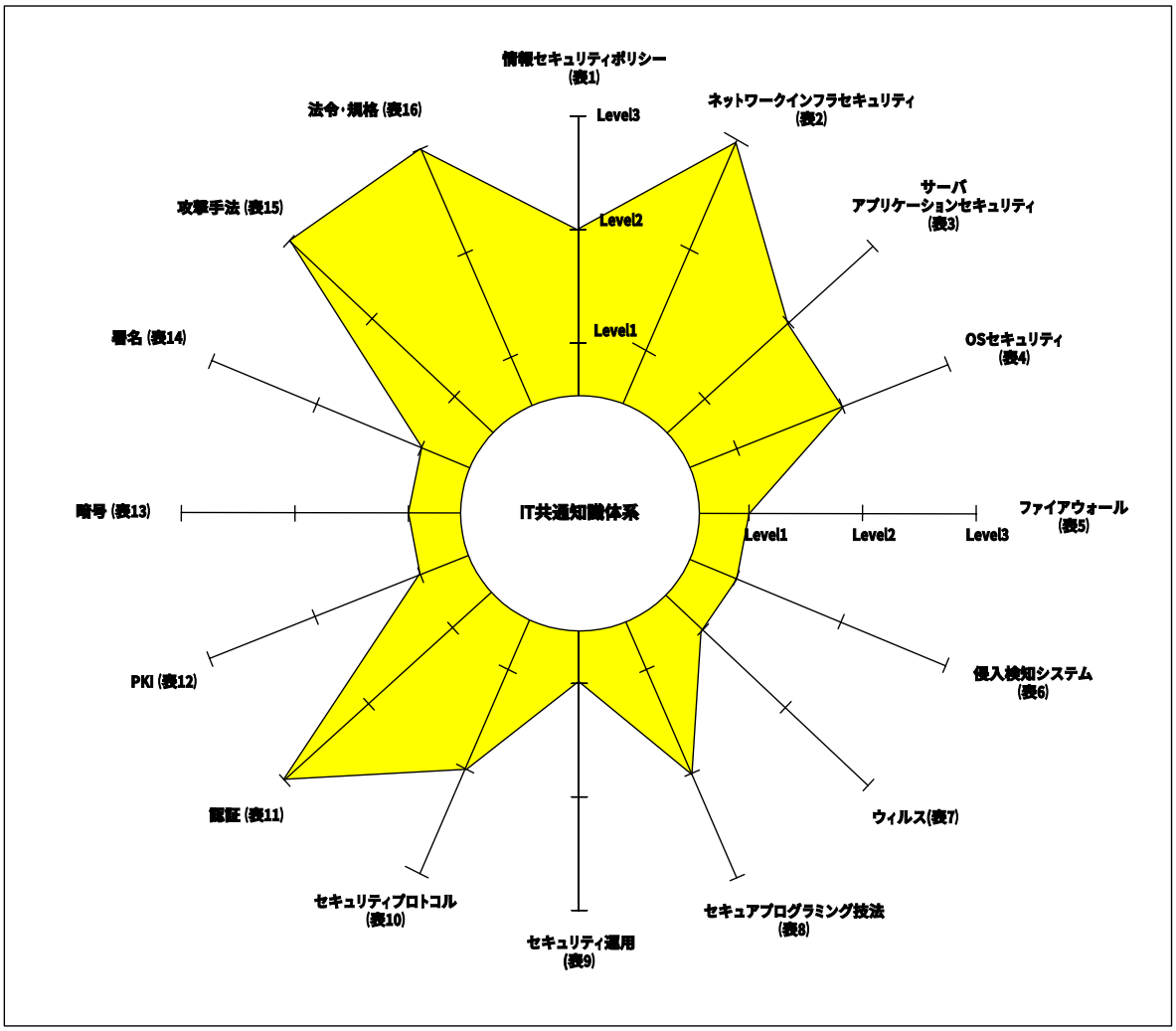


図 2-3　2002 年度版スキルマップを利用した人材のスキルレベルの表現例(開発系技術者)

２．２ スキルマップのアップデートについて

２．２．１ 2002 年度版スキルマップの課題

2002 年度に IPA に設置された「情報セキュリティプロフェッショナル育成に関するワーキンググループ」（主査： 佐々木良一東京電機大学教授）において、スキルマップのレビューを行った（第 1 回 2002 年 12 月 10 日／第 2 回 2003 年 2 月 3 日）。また、表 2-1 に示す「B. 教育機関における情報セキュリティ教育の現状に関する調査」の一環として、教育機関の立場からスキルマップへのコメントや要望をうかがった。

2002 年度版スキルマップに対しては、これらのレビュー、ヒアリング調査のなかで、下記のような課題が指摘されている。

（1）スキルマップの構成に関して
- 大分類によって、小分類の粒度にバラツキがある。
- レベルの定義と実際の使用場面の対応関係がわかりづらい（例えば、レベル 2 だとその技術者は何ができるのか？）
- 項目の間に一部構成上の齟齬が見られる。

（2）スキルマップの位置付けに関して
- スキルマップが「主として」想定している対象が良くわからない。誰にどのように使わせるかを議論すべき。
- 専門技術の項目を扱っていることから、ユーザよりも、開発者、設計者、システムエンジニア等の方がなじみ易いのではないか。

（3）スキルマップの利用に関して
- 人事部の採用担当者など、情報セキュリティ関連の技術に精通していない者が、レーダーチャートを定義するのは実際には難しいのではないか。
- スキルマップを使う人（情報セキュリティにたずさわる人材）のスキルをどのように測るかが難しい。

2003 年度の調査研究では、上記のような指摘を踏まえ、試作版として昨年度積み残した課題の解決と実際の現場での実用性の向上を目指して、スキルマップのアップデートを行った。さらに、スキルマップを実際の現場で活用し易くするためのツールとして、以下の 2 点について検討した。

1. スキルモデル：情報セキュリティに関する個別の業務やタスクについて求められる技術的な知識項目に関するレベル等を整理したモデル（「３．情報セキュリティに関する「スキルモデル」の策定」参照）
2. スキルレベルチェックテスト： スキルマップの利用者等が自己あるいは他者のスキルレベルをチェックするために使用できる、スキルマップをベースとしたテスト問題及びその解答のリスト（「４．情報セキュリティに関するスキルレベルチェックリストの策定」参照）

２．２．２ スキルマップの構築作業について

重点的な調査検討を要する「スキルマップのアップデート」「スキルモデルの策定」「スキルレベルチェックリストの策定」の 3 つの項目については、タスクフォースを設けて詳細な検討にあたった。

加えて、今年度の調査研究では、大学や民間企業の情報セキュリティ分野の有識者に対してヒアリング調査やグループインタビューを行い、スキルマップの精度のさらなる向上を図った（図 2-4 参照）。上記ヒアリング調査ならびにグループインタビューの詳細については「５．有識者ヒアリングとグループインタビューによる調査結果の整理」を参照されたい。

（下記「ドラフト作成」）

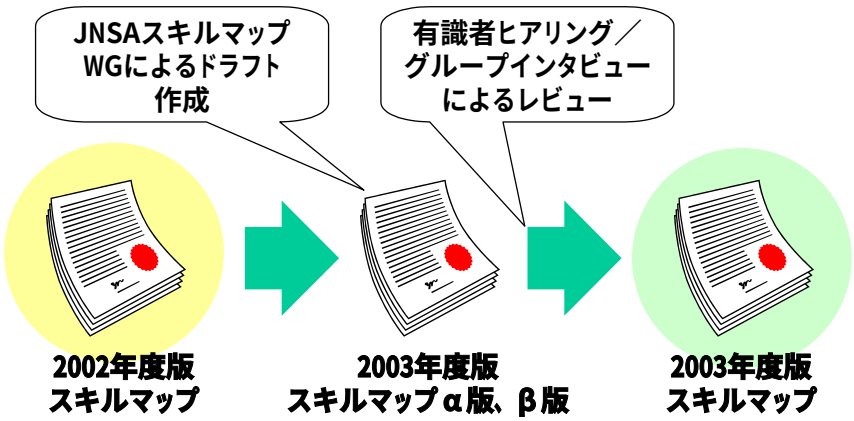


図 2-4　2003 年度版スキルマップの構築作業

２．３ 2003 年度版スキルマップの概要と見直しの論点

2003 年度版スキルマップでは、構成と内容の両面から見直しを行った。以下に、2003 年度版スキルマップの概要と見直しにあたっての論点やポイントを整理する。

２．３．１ 2003 年度版スキルマップの概要

2003 年度版スキルマップは、表 ２-４に示す 16 の「大分類」から構成されている。

この大分類は、情報セキュリティに関わる非常に広範に渡る技術知識体系やその中に含まれる知識の項目を、企業や組織における実務的な観点から捉えて整理した一つの「断面」と考えることができる。それぞれの大分類は「中分類」「小分類」（及び「備考」）を含む階層的な構成となっており、表形式で整理されている。このようなスキルマップにおける大分類の整理の考え方、およびその階層構造の概要については、「２．３．２ スキルマップのアップデートに係る論点（２）スキルマップの構成について」を参照されたい。

なお、表中の「別 A 不正コピー防止と電子透かし」については、スキルマップに附属する「別表」として位置付けられている（詳細については「２．３．２ スキルマップのアップデートに係る論点（４）別表の取り扱いについて」を参照）。

表 2-4　2003 年度版スキルマップの大分類と中分類

項番	大分類		中分類
1	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、情報セキュリティ監査、関連知識
2	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、ネットワークアクセスコントロール VPN、無線 LAN
3	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
		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
		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
4	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
		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
		Trusted OS	強制アクセス制御の概念（MAC）
5	ファイアーウォール		ファイアーウォールの導入・運用、NAT、ネットワークアクセスコントロール
6	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
7	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
8	セキュアプログラミング技法		Web アプリケーション、DB、アプリケーション全般、XML、PHP JAVA、Perl、VB/ASP、C/C++、UNIX、コンパイラ・仮想マシン、Windows
9	セキュリティ運用		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）
10	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
11	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
12	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、公開リポジトリ、認証局の構築と運用、法的枠組み、PKI の要素技術、PKI が提供するサービス
13	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
14	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
15	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
16	法令・規格		基準・指針・ガイドライン等、法令、国際標準規格、国際ガイドライン
別 A	不正コピー防止と電子透かし		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、電子透かしの基本概念、電子透かしの方式、電子透かしの応用形態

２．３．２ スキルマップのアップデートに係る論点

（１）スキルマップの想定する主要な対象者について

ユーザ企業やベンダ企業といった業種・業界や、システム設計やセキュリティポリシー構築といった個別の業務にかかわらず、情報セキュリティに関する高度なスキルを求められる人材（＝ 情報セキュリティプロフェッショナル）には、広範な分野にまたがる技術知識の正確な理解に裏打ちされた、高い業務遂行能力が求められる。2002年度に実施した企業向けアンケート調査研究では、人員の採用に際して重視することを質問しているが、即戦力として期待される中途採用者に対しては「情報セキュリティに関する専門知識」をあげた割合がもっとも大きくなっている（図 2-5参照）。このことは、情報セキュリティプロフェッショナルにおいて、技術知識の必要性の比重が大きいことを表わしていると考えられる。

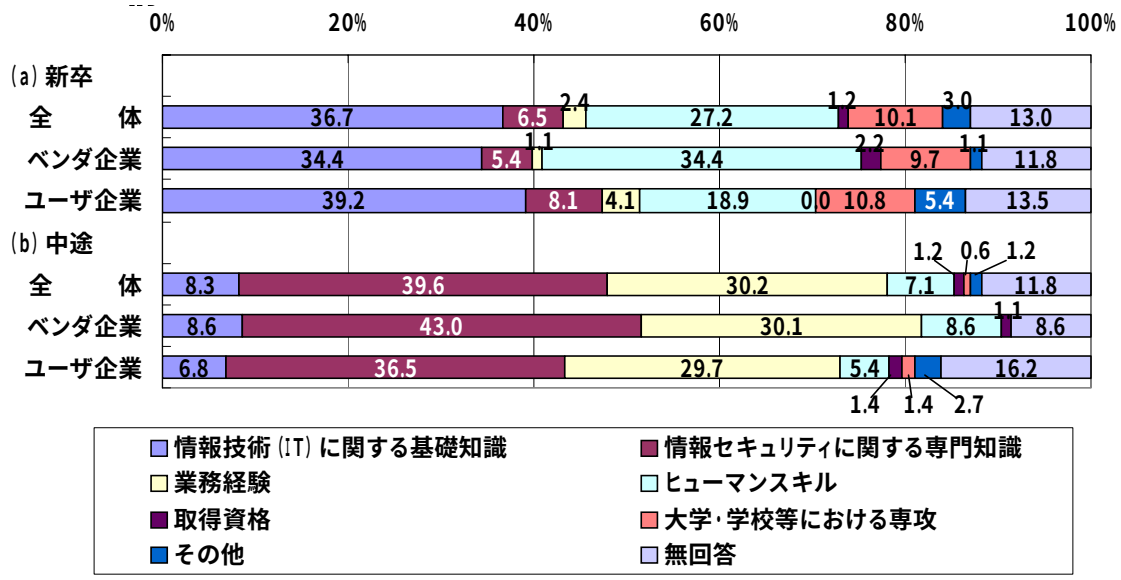


図 2-5　情報セキュリティにたずさわる人材の採用において重視すること（N=169）
（出典：2002 年度 IPA「情報セキュリティプロフェッショナル育成に関する調査研究」）

スキルマップでは、このような「情報セキュリティプロフェッショナル」を主要な対象者として想定し、詳細かつ専門的な技術知識に関わる項目を含んでいる。ここで、想定している情報セキュリティプロフェッショナルの例としては、以下のような人材があげられる。

- 顧客のセキュリティポリシーの策定やセキュリティマネジメントの実施を支援するコンサルタント
- 顧客の要望をまとめてシステムインテグレーションの提案を行うシステムエンジニア

- プロダクトを導入しコンフィギュレーションやカスタマイズを行うエンジニア
- 脆弱性調査やログ解析など、インシデント対応を行うエンジニア
- 企業や組織のセキュリティマネジメントに責任をもつ CISO（Chief Information Security Officer）
- 企業や組織の情報システムやネットワークのセキュリティマネジメントに実対応する担当者
- 企業や組織のセキュリティマネジメントの正当性・妥当性を評価する監査者

情報セキュリティの高度な専門的な知識を有するプロフェッショナル的な人材が求められる一方で、情報セキュリティ侵害が影響する範囲は以前と比較して格段に広まっており、情報セキュリティや IT の専門家以外の一般ユーザ（エンドユーザ）においても情報セキュリティの基本的な概念や必要な対策に関する知識が必要になってきている。そこで、スキルマップでは、プロフェッショナルだけでなく一般ユーザにも適用可能なものとなることを念頭においている。

（2）スキルマップの構成について

スキルマップの大分類は、情報セキュリティの学問的な体系と必ずしも一致していない。スキルマップは、企業や組織の現場で実務にたずさわるエンジニアやコンサルタントが自らの業務経験を踏まえて、人材育成や採用においてスキル（能力）のうち技術知識に関する「ものさし」として使用することを目的とする実用本位の観点から整理したことが特徴となっている。それゆえに、大分類の軸の数についても取り扱いがし易い程度に留めるため 16 個の大分類とした。16 分類は、スキルマップの活用イメージである「スキルモデル」（「3．情報セキュリティに関する「スキルモデル」の策定」参照）などにおいて、レーダーチャートによる知識の習得度合いや能力要件などのレベルを表現しようとする際にも有利である。

スキルマップの大分類は、図 2-6 に示すように、「中分類」「小分類」と階層的に構造化されている。2003 年度版スキルマップでは、合計 479 個の小分類を含んでいる[3]。加えて、小項目を補足する内容や例示を与えるために、フリーフォーマットで記述される「備考」の欄を設けてある。備考は空欄になっている場合もある。

また、表 2-4 を見ると、大分類「3．アプリケーションセキュリティ」「4．OS セキュリティ」にはそれぞれ「Web／電子メール／DNS」「Unix／Windows／Trusted OS」といった項目が含まれている。これらは対応する大分類の中分類ではなく、「サブ大分類」として定義されており、関連のある中分類をグループ化している。サブ大分類は、スキルマップを応用とする際にカスタマイズされることを想定している。

[3] 参考： 2002 年度版の小分類に相当する項目数は 437 個。

<table>
<tr><td colspan="3">大分類　AAAA</td></tr>
<tr><td></td><td colspan="2">中分類　BBBB</td></tr>
<tr><td></td><td>小分類　CCCC</td><td>備考　cccc（小分類 CCCC の補足）</td></tr>
<tr><td></td><td>小分類　DDDD</td><td>備考　dddd（小分類 DDDD の補足）</td></tr>
<tr><td></td><td>・・・</td><td>・・・</td></tr>
<tr><td></td><td colspan="2">中分類　EEEE</td></tr>
<tr><td></td><td>小分類　FFFF</td><td>備考　ffff（小分類 FFFF の補足）</td></tr>
<tr><td></td><td>・・・</td><td>・・・</td></tr>
<tr><td colspan="3">大分類　GGGG
・・・</td></tr>
</table>

図 2-6　スキルマップの階層構造（イメージ）

（3）「レベル」の考え方

スキルマップのもっとも主要な目的が、スキルマップの体系を基盤として、情報セキュリティにたずさわる人材に求められる各技術知識の水準を定量的に表現できる「評価の尺度（ものさし）」を与えることである。2002 年度の調査研究の段階から、スキルマップに含まれる各知識の項目を単に「知っている」「知らない」ということだけでなく、その知識に関する習熟度や知識の活用の度合い、あるいは業務の経験などによって客観的に判断される「レベル」の概念を導入することを目指してきた。今年度の調査研究においてもレベル定義をどのように考えるかが、主要な研究テーマの一つとなっている。

2002 年度スキルマップでは、小分類の項目を「基礎知識」と「応用知識」の 2 つに区分したうえで、レベルとの対応づけを行った。「基礎知識」は、大分類のあらわす分野において当然知っていることが期待される知識項目、「応用知識」はより高度な知識あるいは基礎知識を活用する知識の項目となっている。表 2-5 に 2002 年度スキルマップの知識区分の例を示す。このように各小分類を「基礎知識」「応用知識」に区分した上で、表 2-6 に示すようにレベルを対応づけた。このうち、Level3 については、「基礎知識」「応用知識」を習熟し、それらを高度な実務に応用できる人材（エキスパート）に期待されるレベルを想定している。図 2-2 及び図 2-3 のレーダーチャートのレベルは、このようなレベル定義の考え方に基づいて設定されている。

表 2-5　2002 年度スキルマップの知識区分の例（ウィルス）

大分類	知識区分	小分類
ウィルス	応用知識 (Level 2)	ウィルス種類と感染位置
		発病時の行動パターン
		ウィルスの自己防御機能
		防御システムの構築（ウィルスからの防御システム構造）
		流行の傾向と予測
		ログの集中管理
		対応ポリシー（感染時）
		設定ポリシー
	基礎知識 (Level 1)	構成要素
		スキャン方式と検出方法
		感染媒体の種類と感染方法
		分類および定義の理解
		定義ファイルの理解
		定義ファイルのアップデート

（出典：2002 年度 IPA「情報セキュリティプロフェッショナル育成に関する調査研究」）

表 2-6　2002 年度スキルマップのレベル設定

レベル	レベルの説明
Level 0	知識がない（知る必要がない）
Level 1	基礎知識を習得している
Level 2	応用知識を習得している
Level 3	応用知識を使いこなせる

（出典：2002 年度 IPA「情報セキュリティプロフェッショナル育成に関する調査研究」）

このような、2002 年度版スキルマップの知識区分（基礎知識／応用知識）とレベル（Level 0～Level 3）を対応づける方法は、スキルマップの構成と対応をしているため、理解しやすい点がメリットである。その一方で、スキルマップの実用性を考慮した場合、以下のような問題点が指摘されている。

（a）職種や業務によってレベルの意味や内容が異なる

情報セキュリティにかかわる業種や職種、あるいは個別の業務の内容によって、レベルの考え方やレベルの重みは異なる。例えば、同じ「ファイアーウォール」という大分類についても、ファイアーウォールのパッケージ製品を設計、開発する開発技術者と、その製品を企業のシステムに導入し、設定を行うシステムエンジニアやプロダクトサポートエンジニアとでは、要求される技術知識の内容やレベルのもつ重みは変ってくるはずである。

（b）基礎知識／応用知識を区分するのは難しい場合がある

何が基礎知識で、何が応用知識になるのかは、（a）と同様、職種や業務によって

も異なり、2002 年度版スキルマップのように統一的な知識区分を設定することは難しい場合がある。

また、基礎知識の方がより習得が易しく、応用知識の方が難しいとは一概にいえない。暗号技術は、セキュリティの各分野の「基礎」を成しているが、習得するためには高度な数学理論を理解している必要がある。「基礎」「応用」という区分は言葉の使い方としても誤解を招く恐れがある。

（c）レベルの内容は画一ではない

上述のように、2002 年度版スキルマップでは、基礎知識あるいは応用知識の有無をもってレベルの定義をしていたが、業務や技術知識の性質によっては、「知っている／知らない」という評価軸のほかに「業務としての経験がある／ない」「知識を活用することができる／できない」など、さまざまな方法論への要求があるかもしれない。スキルマップをより汎用的なものとするために、レベル定義の内容を画一的に決めてしまうのではなく、ある程度自由にカスタマイズできるようなものとなっている方が望ましい。

これらの問題は、スキルマップのレベル定義をどうするかということだけでなく、情報セキュリティにたずさわる人材に求められる技術知識の水準をどのように扱うか、というより本質的な議論を含んでいる。2003 年度版スキルマップでは、以上の論点を踏まえ、レベルの考え方について以下のように整理することとした（図 2-7 参照）。

- 2002 年度版スキルマップの知識区分（基礎知識／応用知識）とそれに紐づけられたレベル定義を廃し、スキルマップによる技術知識の体系的整理とレベル定義とを切り離して考える。
- 新たに「スキルモデル」のコンセプトを導入し、情報セキュリティに関する個別の業務やタスクにおいて求められるスキルとそのレベルを整理する。
- スキルモデルにおいて、新しいレベル定義の考え方を導入し、個別のレベルを表現するためにレーダーチャート表現を活用する

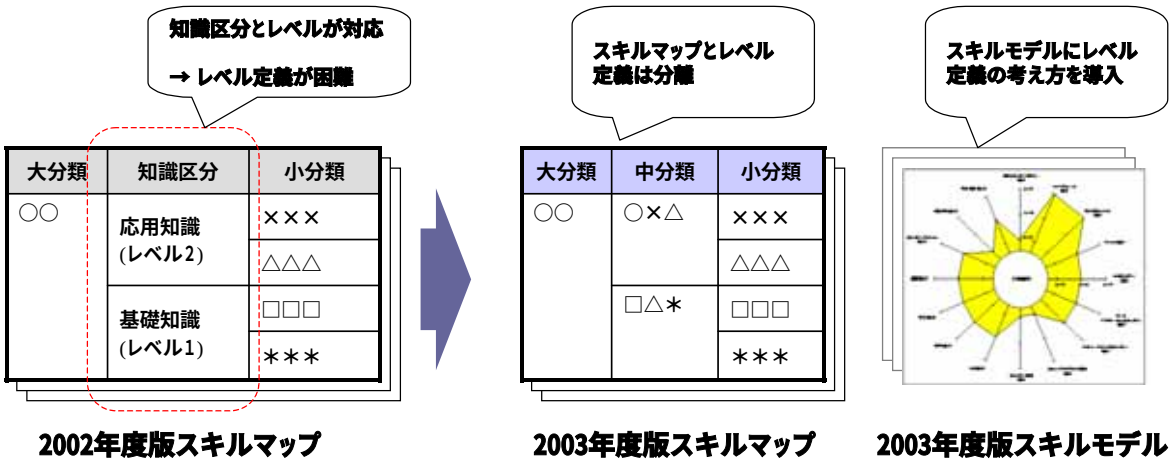


図 2-7　2003 年度版スキルマップ／スキルモデルにおけるレベル定義のコンセプト

今年度の調査研究において新たに導入されたスキルモデルのコンセプト及びその活用方法の詳細については、「３．情報セキュリティに関する「スキルモデル」の策定」にて説明する。また、職種・業務とレベルの考え方、レーダーチャートの活用に関しては同章にて再度考察する。

（４）別表の取り扱いについて

2003 年度版スキルマップでは、スキルマップに附属する「別 A 不正コピー防止と電子透かし」を整理している（表 2-4 参照)。スキルマップでは情報セキュリティに関する技術知識を扱っているが、情報セキュリティの分野は裾野が広く、かかわりのある応用分野、発展分野に関する知識をどのように整理するかについても検討が必要になる。

そこで 2003 年度版スキルマップは、基本的な 16 分類を維持しつつ、応用・発展分野への拡張に対応するために、「別表」を設けている。今年度は、「別 A 不正コピー防止と電子透かし」として当該分野の技術知識を試行的に整理をしているが、将来的にはプライバシー保護等、関連ある分野が追加されることを想定している（「２．５ スキルマップの活用方法に関する考察（３）スキルマップの大分類の構成とカスタマイズの可能性について」参照)。

２．４ 2003 年度版スキルマップの詳細

以下に、2003 年度版スキルマップの各大分類について示す。なお、以下本章では、スキルマップを説明する表の番号は「(表ｘｘｘ)」と表記し、他の表と区別する。

（表０）2003 年度版スキルマップの大分類

項番	大分類	
1	情報セキュリティマネジメント	
2	ネットワークインフラセキュリティ	
3	アプリケーションセキュリティ	Web
		電子メール
		DNS (Domain Name System)
4	OS セキュリティ	Unix
		Windows
		Trusted OS
5	ファイアーウォール	
6	侵入検知	
7	ウィルス	
8	セキュアプログラミング技法	
9	セキュリティ運用	
10	セキュリティプロトコル	
11	認証	
12	PKI (Public Key Infrastructure)	
13	暗号	
14	電子署名	
15	不正アクセス手法	
16	法令・規格	
別 A	不正コピー防止と電子透かし	

（表１）情報セキュリティマネジメント

大分類	中分類	小分類	備考
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	・セキュリティの3大要素 ・PDCA サイクル ・セキュリティポリシーの3階層
		マネジメントシステムの確立	・実施すべき項目（基本方針、リスクアセスメント等）
		マネジメントシステムの導入・運用	・実施すべき項目（対応計画、教育等）
		マネジメントシステムの監視・見直し	・実施すべき項目（有効性の見直し、内部監査等）
		マネジメントシステムの維持・改善	・実施すべき項目（改善策の実施等）
		情報セキュリティのドキュメント体系	・基本方針、対策基準、実施手順・規定類
	リスク分析技術	リスクアセスメント手法	・ベースラインアプローチ ・非形式的アプローチ ・詳細リスク分析 ・組み合わせアプローチ
		情報資産の調査・評価	・調査方法 ・評価基準
		脅威・脆弱性の調査	・脅威の分類・調査 ・脆弱性の把握・評価
		リスク評価	・定量的リスク評価 ・定性的リスク評価
		対策システムの検討・整理	・対策検討
	情報セキュリティポリシー	基本方針	・記述すべき項目（目的、適用範囲、組織と体制等）
		物理的対策	・物理的対策標準 ・サーバルームに関する標準 ・職場環境に関する標準 ・媒体の取り扱いに関する標準
		技術的対策	・ユーザ認証標準 ・アカウント管理標準 ・外部公開サーバに関する標準 ・サーバに関する標準 ・クライアント等に関する標準 ・ウィルス対策標準 ・ネットワーク構築標準 ・有線 LAN に関する標準 ・無線 LAN に関する標準 ・リモートアクセスサービス利用標準 ・専用線および VPN に関する標準
		人的対策	・電子メール対策標準 ・Web サービス対策標準 ・セキュリティ教育に関する標準 ・プライバシーに関する標準

大分類	中分類	小分類	備考
		運用･管理対策	・システム維持に関する標準 ・システム監視に関する標準 ・セキュリティ情報収集及び配信標準 ・セキュリティインシデント報告･対応標準 ・監査標準 ・委託時の契約に関する標準 ・事業継続管理 ・罰則に関する標準 ・スタンダード更新手順 ・プロシージャ配布の標準
	情報セキュリティ監査	情報セキュリティ監査の目的	・内部監査 ・外部監査
		情報セキュリティ監査手法	・監査の実施手順、評価方法 ・監査証跡の収集、分析手法 ・脆弱性検査手法、侵入テスト ・監査ツール
		監査報告書	・監査報告書の要件
	関連知識	情報セキュリティの関連制度	・ISMS 適合性評価制度 ・プライバシーマーク制度 ・情報セキュリティ監査制度
		情報セキュリティの標準化	・OECD セキュリティガイドライン ・JIS Q 15001 ・BS7799 ・ISO/IEC 17799 ・ISO/IEC TR 13355
		情報セキュリティの関連法規	大分類「法令･規格」参照
		セキュリティ監査（内部監査、外部監査）	・目的、実施手順、評価方法

（表２）ネットワークインフラセキュリティ

大分類	中分類	小分類	備考
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）	・装置 ・通信経路
		論理設計技術（論理設計時のセキュリティ対策）	・ネットワークの分割・配置 ・アドレス体系
		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）	・スタティックルーティング ・ダイナミックルーティング
		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	・ＩＤＳ、ＳＮＭＰ、ログ等によるセキュリティ対策 ・機器のセキュリティ対策
	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)	環境構築	・配置 ・暗号化方式 ・認証方式 ・アクセス制御
		IPSec による VPN 装置（ファイアーウォール含）	・利用形態 ・認証 ・暗号化 ・クライアント設定
		ルータによる VPN 装置	・利用形態 ・暗号化
		SSL による VPN 装置	・利用形態 ・認証 ・暗号化 ・利用サービス
	無線 LAN	認証・暗号化	・ESS-ID ・MAC アドレス ・IEEE802.1x ・WEP ・WPA ・IEEE802.11i
		その他	・ネットワーク分割 ・認証サーバとの連携

（表３）アプリケーションセキュリティ

大分類	中分類	小分類	備考
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	・バッファオーバーフロー ・クロスサイトスクリプティング ・パラメータ改ざん ・バックドアとデバッグオプション ・強制的ブラウズ ・セッション・ハイジャック／リプレイ ・パスの乗り越え ・SQL の挿入（SQL Injection） ・OS コマンドの挿入（OS Command Injection） ・クライアント側コメント ・エラーコード
		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	・デフォルトアカウントの無効化、パスワードの設定等
		ファイル／ディレクトリのアクセス権の設定	
		ユーザ認証	・Basic 認証 ・Digest 認証 ・証明書を利用したクライアント認証
		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	・通信のセキュア化 ・アクセス制御の強化 ・コンテンツアップロードツール（Secure FTP、rsync、WebDAV）
		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	・入力チェック ・特殊文字のサニタイジング（無害化）
		CGI(Common Gateway Interface)	・インタプリタの格納場所 ・入力チェック ・サンプル CGI プログラムの削除
		Web のセッション管理	・乱数とハッシュによるセッション ID 生成 ・Cookie の利用の注意
	Web ブラウザのセキュリティ	Web ブラウザに対する脅威	・ウィルス感染 ・悪意あるプログラム、スクリプトのダウンロードと実行（Java、JavaScript、ActiveX 等） ・Cookie や個人情報の漏洩 ・ブラウザクラッシャー
		Web ブラウザのセキュリティ対策	・OS、Web ブラウザに対するセキュリティパッチの適用 ・Web ブラウザのセキュリティ及びプライバシー設定（アクティブコンテンツ、Cookie、Java 等）

大分類	中分類	小分類	備考
	Web 関連プロトコルの基礎知識	HTTP(Hyper Text Transfer Protocol)	・リクエスト、レスポンスメッセージ（ヘッダ、ボディ） ・セッションレスプロトコル ・GET／POST メソッド
		SSL(Secure Socket Layer) / TLS(Transport Layer Security)	・鍵交換の仕組み ・証明書の取得 ・SSL アクセラレータの利用
		SOAP(Simple Object Access Protocol)	大分類「セキュアプログラミング技法」の中分類「XML」参照
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	・ブラックリスト（RBL）の利用 ・ブラックリスト（RBL）からの離脱 ・POP before SMTP ・SMTP Auth
		迷惑メール対策	・外部 Spam フィルタの利用
		Spam メール（UCE(Unsolicited Ccommercial E-mail)/ UBE(Unsolicited Bulk E-mail)）対策	
		ユーザ情報の漏洩	・コマンドの使用制限（VRFY/EXPN）
		代表的メールサーバアプリケーションの脆弱性対策	・セキュリティパッチの適用
	メールクライアントのセキュリティ	盗聴対策	・PGP ・S/MIME ・SSL
		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	・セキュリティパッチの適用
	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	・スプリット DNS（内部・外部 DNS の分割）
		ゾーン転送対策	・ファイアーウォールでの対策 ・DNSSEC（暗号化） ・ゾーン転送を許可するサーバの登録
		DNS キャッシュ攻撃（ポジションキャッシュ）攻撃対策	・Dynamic Update による認証 ・再帰的問い合わせの制限 ・問い合わせを受けるホストの制限
	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	

大分類	中分類	小分類	備考
		メールサーバの監視	
		インシデント対策と体制	

（表４）OS セキュリティ

大分類	中分類	小分類	備考
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	・ スーパーデーモン (inetd) と起動スクリプトによる起動の制限 ・ TCP Wrappers によるアクセス制御 ・ r コマンド使用上の注意
		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	・ umask と必要に応じた権限付与の変更
		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	・ PAM（Plaggable Authentication Modules） ・ NIS (Network Information Services) ・ ディレクトリ
		シャドウファイル	・ パスワードを保存する際に DES、MD5 等で暗号化する方法がある
		強いパスワード/弱いパスワード	・ 管理側でのパスワードポリシーの決定
		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	
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	・ Baseline Security Analyzer
		パッチの一括・一斉配布	・ Soiftware Update Services (SUS)
		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	・ 管理ツール(サービス)

大分類	中分類	小分類	備考
	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	・より細かいレベルでのログ監査
		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	・ラベル（パーミッション）の概念
		root 特権の委任	

（表５）ファイアーウォール

大分類	中分類	小分類	備考
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	・データマイニング ・侵入相関分析（対象となるイベントについて同一オブジェクトの関係、時間的関係、因果関係、社会的関係等の調査）
		侵入検知装置ログとの違い	・・採取したログの性質の違い
		DMZ 等構成の設計	・公開セグメント、非公開セグメントの区分け ・IP ルーティング
		フィルタリングルールの設計	・許可するサービス、拒否するサービス
	NAT(Network Address Translation)	StaticNAT	・1:1（グローバル IP:プライベート IP）の固定的アドレス変換
		DynamicNAT	・1:N（グローバル IP:プライベート IP）の動的アドレス変換
		IP マスカレード	・1:N（グローバル IP:プライベート IP）の動的アドレス変換
	ネットワークアクセスコントロール	Packet Filterling	・IP、TCP 層（IP、ポート番号等）でのアクセス制御
		Circuit Level Gateway	・トランスポート層でのアクセス制御
		Application Level Gateway	・アプリケーション層でのアクセス制御
		ステートフルインスペクション	・アプリケーション層でのアクセス制御

（表６）侵入検知

大分類	中分類	小分類	備考
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	・取りこぼし ・誤検知 ・未知の攻撃手法 (Misuse) ・検出の回避方法 ・Stick 攻撃 ・暗号環境の未検出 ・FalseNegative と FalsePositive
		ログ解析	・データマイニング ・侵入相関分析 (対象となるイベントについて同一オブジェクトの関係、時間的関係、因果関係、社会的関係等の調査)
		ファイアーウォールログとの違い	・採取したログの性質の違い
	侵入検知システムの機能	管理コンソールへの告知	
		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)	
		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	・定量分析 (しきい値モデル) ・統計的手法 (しきい値学習モデル) ・クラスタ分析 ・ルールベースアプローチ ・ニューラルネットワーク
		不正検出	・パターンマッチング
	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	
		ハニーポッド	
		改竄検知	

（表７）ウィルス

大分類	中分類	小分類	備考
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	・感染経路の複合化（メール、共有ファイル） ・発病内容の複合化
		バックドアの作成	
		改竄	・レジストリ、データ
		情報発信	・パスワード、データのメールへの添付送信
		外部攻撃	・DoS 攻撃 ・DDoS 攻撃
		メール発信	・大量のメール発信
		破壊活動	・ファイルの破損 ・ディスクのフォーマット
	検出方法と駆除	予知検出	・亜種、ウィルスらしきプログラムの検出
		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	・隔離 ・駆除 ・削除 ・アクセス拒否
		スキャン方式の種類	・オンアクセス、オンデマンド等
		定義ファイル	
		検出方法の種類	・パターンマッチング ・割り込み監視 ・ヒューリスティック ・整合性チェック ・メモリ検出 等
	感染	ウィルスの自己防衛機能	・ステレス機能 ・ポリモフィック（ミューテーション）機能
		脆弱点の利用	・Windows やその他のアプリケーションの脆弱点を利用してウィルスに感染させる。代表的なものとしては、バッファーオーバーフロー、フォーマット違反等
		兆候	・処理速度が落ちる ・関係ない情報が表示される ・ネットのトラフィックが高くなる 等

大分類	中分類	小分類	備考
		手段（媒体）	・メール ・共有フォルダ ・FD ・CD-ROM ・送り込み ・Web ・チャット ・ファイルのダウンロード
		経路	・FD ・CD-ROM ・インターネット ・イントラネット
	種類	ウィルスの機能構成	・自己伝播機能 ・潜伏機能 ・発病機能
		デマウィルス	
		ジョークウィルス	
		不必要なプログラム	・Spyware、キーロガー等、コンピュータのデータを無断で入手する為のソフト
		マクロウィルス	
		トロイの木馬	
		ワーム	
		スクリプト	・Java スクリプト型 ・ActiveX 型 ・VBS
		ウィルス	・ファイル感染型 ・ブートセクター感染型 ・ファイルおよびブートセクター等に感染 等

（表８）セキュアプログラミング技法

大分類	中分類	小分類	備考
セキュアプログラミング技法	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	
	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	

大分類	中分類	小分類	備考
	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	

（表９）セキュリティ運用

大分類	中分類	小分類	備考
セキュリティ運用	定常運用時のセキュリティ確保	事前設定	・ログファイルの記録／更新設定 ・制御･設定ツール(SNMP 他)
		モニタリング	・異常アカウントの有無 ・異常プロセスの有無 ・システムの負荷の状況 ・記録装置の空き容量の変化
		セキュリティホール対策	・セキュリティホールの影響評価 ・設定変更による被害回避 ・パッチの効果と副作用 ・パッチの適用可否の判断基準（目的、対象） ・対策の有効性の検証法
		定常作業	・バックアップ･リストアの設定／実施 ・アカウント管理 ・パスワード管理
		ユーザ対応等	・ユーザへのアナウンス ・ユーザ教育（セキュリティ啓発） ・ルール違反対策（発見、対応）
	異常時対応	異常検知	・IDS からのアラーム（大分類「IDS」参照） ・モニタリングによる異常検知 ・ユーザからの異常報告 ・誤検知かどうかの判断
		原因究明･トラブルシューティング	・異常要因の切り分け ・特徴の分析（再現性、影響範囲等） ・対策の実施
		緊急時対応	・緊急事態かどうかの判断（被害、影響の評価） ・運用継続の可否 ・被害の拡大防止（ネットワークの切り離し等） ・代替措置 ・関係組織への報告 ・緊急時対応の訓練
	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	・ソフトウェア、システムベンダからの情報 ・セキュリティベンダからの情報 ・公的機関からの情報
		脆弱性情報の意味と分析	・重要性、緊急性の分類 ・情報の信頼性の判断

（表１０）セキュリティプロトコル

大分類	中分類	小分類	備考
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)	

（表１１）認証

大分類	中分類	小分類	備考
認証	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	・CAPTCHA
	認証デバイス	IC カード	
		USB トークン	
		耐クローン	
		耐タンパ	・NIST FIPS140-1、FIPS140-2 ・耐タンパ性に対する解析法（破壊型解析法（プローブ解析）、非破壊型解析法（故障利用解析、タイミング解析、電力解析））
	認証プロトコル	AKE(Authenticated Key Exchange)	・PAKE(パスワード認証) ・証明書による認証
		Kerberos	
		RADIUS	
		SSH(Secure SHell)	・パスワード認証 ・秘密鍵認証
	Web 認証	Cookie	
		SSL(Secure Socket Layer)認証	・パスワード認証 ・秘密鍵認証
	システム認証	サーバ間認証	・IP アドレスによる認証 ・MAC アドレスによる認証
	シングルサインオン	アクセス制御	・ポリシーベース ・ロールベース
		セッション管理	
		ログ管理	
		構成	・エージェント型 ・リバースプロキシ型

（表１２）PKI(Public Key Infrastructure)

大分類	中分類	小分類	備考
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	・ Web サービス ・ SSL ・ 暗号メール ・ IPSec ・ コード署名 ・ XML 署名
		利用方法の規格化	・ 暗号通信（SSL、TLS、SET、SECE、Ipsec、WAP、SSH） ・ 暗号メールとデジタル署名（S/MIME） ・ データの暗号化とデジタル署名（Code Signing、XML、PKCS#7 と CMS） ・ 暗号インターフェース（PKCS#11、GSS、GSS-IDUP） ・ タイムスタンプ（Time Stamp Protocol）
	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	・ 属性証明書の意味 ・ 属性証明書の利用方法
	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)	・ OCSP の後継として SCVP 等の標準仕様が策定されつつある
	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)	

大分類	中分類	小分類	備考
		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）	
	PKI の要素技術	認証機関	
		証明書リポジトリ	
		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	

（表１３）暗号

大分類	中分類	小分類	備考
暗号	公開鍵暗号	公開鍵暗号の原理	・数学的原理と暗号になる理由と強度の保障（素因数分解、離散対数問題、組み合わせ複雑性、等） ・暗号化と復号化 ・鍵生成と登録
		公開鍵暗号で実現できる機能	・秘匿 ・鍵配送 ・署名 ・親展
		共通鍵暗号のアルゴリズム	・RSA ・RSA-OAEP(Optimal Asymmetric Encryption Padding) ・ELGamal
		Diffie-Hellman 鍵配送	
		楕円曲線上の演算を利用した暗号法	主な暗号法： ・楕円 ElGamal ・楕円 Diffie-Hellman 鍵配送 ・ペアリングを使った方式
	共通鍵暗号	共通鍵暗号の原理	・置換（転置）、換字、非線形撹乱 ・ブロック暗号とその原理 ・ストリーム暗号とその原理 ・強度と脆弱性 ・ブロック暗号の利用モード
		共通鍵暗号のアルゴリズム	・DES(Data Encryption Standard) ・AES(Advanced Encryption Standard) ・DSA(Digital Signature Algorithm) ・Misty
		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	・ハッシュ関数の定義 ・ハッシュ関数が情報セキュリティにもたらす機能
		ハッシュ関数の構成法	
		専用ハッシュ関数	主な関数例： ・MD4、MD5 ・RIPEMD128、RIPEMD160 ・SHA1 ・SHA256、SHA384、SHA512
	暗号用乱数	暗号用乱数の原理	・統計的乱数性 ・長周期性 ・線形複雑度
		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	

大分類	中分類	小分類	備考
	ゼロ知識証明	ゼロ知識証明の原理	・ゼロ知識と対話証明の定義と実現の原理 ・ゼロ知識証明のプロトコル
		ゼロ知識証明プロトコル	・プロトコルの例： ・平方剰余問題のゼロ知識対話証明 ・グラフ非同型問題のゼロ知識対話証明
		ゼロ知識証明の応用	・なりすましの脅威を排除した個人認証、等
	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	・鍵全数探索攻撃法 ・テーブル参照法 ・タイムメモリートレードオフ法
		ショートカット法	・差分攻撃法 ・線形攻撃法 ・高階差分攻撃法 ・SQUARE 攻撃法 ・補間攻撃法 ・中間一致攻撃法 ・関連鍵攻撃法
		サイドチャネル攻撃法	・タイミング攻撃法 ・故障利用攻撃法 ・電力攻撃法
		暗号技術評価プロジェクト(CRYPTREC)	CRYPTREC「電子政府推奨暗号リスト」参照

（表１４）電子署名

大分類	中分類	小分類	備考
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	・RSA ・DSA ・ESIGN ・ECDSA ・SFLASH ・ペアリング方式
		電子署名に利用されるハッシュ関数	・SHA 1 、SHA-256 、 、SHA-384 、SHA512 ・RIPEMD-160 ・MD2、MD5
	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	・秘密鍵を利用するため、本人性を保証
		ハッシュ関数の利用	・ハッシュ値をとるため、平文そのものより暗号時間を短縮 ・ハッシュ関数利用により、入力サイズに関わらず、出力サイズが一定
		署名検証の容易さ	・署名生成者の公開鍵は公開されているため、誰でも署名検証可能、等

（表１５）不正アクセス手法

大分類	中分類	小分類	備考
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	・リモートバッファーオーバーフロー ・ローカルバッファーオーバーフロー
		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	・古典的タイプ ・ファイル変更型 ・シェルポートバインド ・ＬＫＭタイプ
		なりすまし	・ユーザ ID、パスワードでのなりすまし ・IP アドレスによるなりすまし
		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	・SSID の危険性 ・WEB ・ステルス機能（ビーコンの停止）
		アナログ無線の傍受	
	偵察行為	TCP(Transmission Control Protocol)スキャン	・TCP 接続スキャン ・TCP SYN スキャン ・TCP FIN スキャン ・TCP クリスマスツリースキャン ・TCP NULL 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	

（表１６）法令・規格

大分類	中分類	小分類	備考
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	・経済産業省制定
		コンピュータウィルス対策基準	・経済産業省制定
		コンピュータ不正アクセス対策基準	・経済産業省制定
		システム監査基準	・経済産業省制定
		ソフトウェア管理ガイドライン	・経済産業省制定
		情報通信ネットワーク安全･信頼性基準	・総務省制定
		情報システム安全対策指針	・国家公安委員会制定
		行政情報システムの安全対策指針	・行政情報システム各省庁連絡会議幹事会了承
		情報セキュリティポリシーに関するガイドライン	・情報セキュリティ対策推進会議決定
		情報セキュリティ監査制度関連基準･ガイドライン	・経済産業省制定
		情報セキュリティマネジメントシステム(ISMS)認証基準	・Ver.2.0 を 2003 年 4 月に(財)日本情報処理開発協会制定
	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	重要な規格例： ・ISO/IEC 15408（JIS X5070） ・ISO/IEC 17799（JIS X5080） ・ISO/IEC TR13335）
		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	・情報システム及びネットワークのセキュリティのためのガイドライン ・プライバシー保護と個人データの国際流通についてのガイドライン ・暗号政策に関するガイドライン」
		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」	

（別表A）不正コピー防止と電子透かし

大分類	中分類	小分類	備考
不正コピー防止	不正コピー対策	不正コピーの脅威	
		不正コピー防止技術	
		権利管理技術の基本概念	
	権利管理技術(DRM)の要素技術	暗号技術	
		認証技術	
		鍵管理技術	
		電子透かし技術	
		リニューアル技術	
	権利記述言語の標準化	XrML（eXtensible rights Markup Language)	
		ODRL (Open Digital Rights Language)	
	法的要件	著作権法	
		不正競争防止法	
電子透かし	電子透かしの基本概念	電子透かしの埋め込みと検出	
		不可視性	
		ロバスト性	
		完全性	
	電子透かしの方式	知覚モデルの応用	
		周波数マスキング	
		周波数領域への埋め込み	
		位相への埋め込み	
		スペクトル拡散法	
		統計的方法	
	電子透かしの応用形態	著作者の識別	
		所有権の証明	
		改竄防止	
		コピー制御 (機器制御)	
		フィンガープリンティング	
		コンテンツの認証	
		放送の監視	

２．５ スキルマップの活用方法に関する考察

2003 年度は、スキルマップのアップデートに関する検討のなかで、その利用方法や普及のための課題等の論点から検討を行った。また、本調査研究の一環として実施した、学識者ならびに企業担当者へのヒアリング調査、情報セキュリティに関する業務にたずさわる方へのグループインタビューを通じて、スキルマップに関する意見を収集した（「５．有識者ヒアリングとグループインタビューによる調査結果の整理」参照)。

上記のような活動を通して得られた知見をもとに、スキルマップの活用方法及びその課題に関する考察として、以下の 3 つの観点から整理を行った。

（１）スキルマップの応用・展開について（スキルモデルとスキルレベルチェックテスト）

スキルマップの策定にあたっては、情報セキュリティにたずさわる人材の育成の指針策定や情報セキュリティに関するカリキュラム作成など、現場の実務での多様なニーズに対応できるように、可能な限りの網羅性を確保できることを重視した。そのために、実際に情報セキュリティに関する業務にたずさわるエンジニアやコンサルタントらが多岐に渡って詳細に検討を行い、現在必要と思われる項目を抽出した。

一方、実際にスキルマップが使用される場面を考慮すると、特に人材育成などにおいては、人事部門や研修教育部門など、一般に情報セキュリティに関する詳細な技術知識に必ずしも精通しているわけではない人が利用することも考えられる。スキルマップは、技術知識を表形式に整理しているが、このままでは上記のような人にとっては敷居の高い場合もあると考えられる。

また、前述の「スキルマップの目標」（「２．１．２ 2002 年度版スキルマップの試作とそのコンセプト」参照）に示したように、スキルマップを情報セキュリティに関する技術知識の評価の尺度（ものさし）として活用できるにするためにも、表形式に技術知識の項目を整理しただけでは不十分である。

そこで本調査研究では、スキルマップの具体的な活用イメージを与えるものとして、「スキルモデル」と「スキルレベルチェックテスト」の策定について検討を行った。

「スキルモデル」は、情報セキュリティに関する個別の業務やタスクについて求められる技術的な知識項目に関するレベル等を整理したモデルであり、レーダーチャート表現を利用して、ある業務にたずさわる人材に求められる技術知識の「レベル」を直感的に理解できるようにしている点に特徴がある。利用者が簡単にそれぞれのニーズに合わせたスキルモデルを設定できるようにツールの整備を行った。

「スキルレベルチェックテスト」は、スキルマップの利用者等が自己あるいは他者のスキルレベルをチェックするために使用できる、スキルマップをベースとしたテスト問題及びその解答のリストであり、本調査研究ではスキルマップの大分類に対応したサンプルテスト問題を試行的に作成した。

スキルモデルとスキルレベルチェックテストの詳細にてついては、それぞれ「３．情報セキュリティに関する「スキルモデル」の策定」「４．情報セキュリティに関するスキルレベルチェックリストの策定」を参照されたい。

（2）カリキュラム作成にスキルマップを活用する際の課題

スキルマップを情報セキュリティに関するカリキュラムの作成や教育・研修コースの設定に利用したいというニーズは多い。情報セキュリティに関する教育教材の開発や出版、資格認定等を推進する団体である SEA/J（Security Education Alliance／Japan）[4] では、「SEA/J 情報セキュリティ技術認定 基礎コース」において 2002 年度版スキルマップに対応したカリキュラムを設定している

カリキュラム作成にスキルマップを活用する際に課題として、情報セキュリティに関する基礎教育にどのように対応するか、という問題がある。現在のスキルマップは、専門的な技術知識にフォーカスしており、「セキュリティとは？」といったセキュリティの基本概念など、必要最小限知っておくべきカリキュラムを整理しているわけではない。

スキルマップにおいては、

- SIer、メーカ、サービスプロバイダ、ユーザ企業といった業種やアプリケーション開発者、システムインテグレータ、研究者などの職種によって、何が「基礎」になるかは異なる。
- 「情報セキュリティの基礎」と一口にいっても、ネットワーク技術など IT に関する基本的な知識や情報科学、数学など、どこまでをそれに含めるかについては、それぞれのカリキュラムや教育・研修コースの範囲や目的に応じて決められるべき。

といった観点から、何が基礎にあたるかについては、スコープの範囲外とすることとした。スキルマップをセキュリティ導入教育などに利用しようとする際には、このようないわば「入門編」にあたるカリキュラムについては、スキルマップの体系とは別に整理される必要がある。上記の「SEA/J 情報セキュリティ技術認定 基礎コース」では、「情報セキュリティ概論」において、秘匿性、完全性、可用性などの概念やセキュリティ侵害による金銭的損害のリスク、情報倫理などについて教えている。

（3）スキルマップの大分類の構成とカスタマイズの可能性について

前述のようにスキルマップは、情報セキュリティに関する業務に実際にたずさわる者の目から見て現時点において必要と思われる項目を整理したものである。そのため、ユーザ企業などにおいては、別の分類項目を設けるなどのカスタマイズの要求が出てくることも考えられる。スキルマップ作成の開始時点から、スキルマップは固定的なものではなく、あくまでも利用者がそれぞれのニーズに応じて、カスタマイズ可能であることを意識している。

2003 年度版スキルマップでは、情報セキュリティの応用・発展分野への拡張に対応するためのカスタマイズ方法の一例として、大分類「不正コピー防止と電子透かし」を別

[4] SEA/J ホームページ： http://www.sea-j.net/

表の形で整理している（「２．３．２ スキルマップのアップデートに係る論点（４）別表の取り扱いについて」を参照)。このような使い方は、現在の 16 大分類とは独立に整理した方が、利便性が高いと思われる項目の大分類を別表に追加していくことを想定している。

特に、今後整理されるべき項目としては、「セキュリティと個人情報保護」などがあげられる。2003 年 5 月に個人情報保護法が成立したこともあり、個人情報を取り扱う事業者が、情報セキュリティとのかかわりからも必要な知識を身に付けておくことが求められている。個人情報保護は、情報セキュリティと一面において両立するが、他面においては、無関係あるいは対立する概念となる場合もあるため（表 2-7 参照)、今後、関連する研究の成果等を踏まえた議論が必要になると思われる。

表 2-7　セキュリティ対策と個人情報保護対策の関係

No.	関係		例
	分類	小分類	
1	両立	セキュリティ対策が個人情報の手段	第三者対策： ファイアーウォールなどの不正侵入対策が個人情報の流出を保護
2	無関係	セキュリティ対策は無効か、直接的関係なし	匿名性維持対策など
3	対立	セキュリティ対策と個人情報の保護の一方を実現しようとすると他方の成立が困難	(a) 公開鍵証明書の情報から個人情報が知られる (b) 暗号化メールを許すことが個人の情報の流出を見逃す

（出典： 佐々木良一「セキュリティと個人情報保護の関係に関する考察」
電気情報通信学会技術研究報告 SITE2003 - 14）

３．情報セキュリティに関する「スキルモデル」の策定

「情報セキュリティのためのスキルマップ」をベースに、情報セキュリティにたずさわる人材に求められるスキルの汎用的なモデル化を目指す「スキルモデル」の策定について検討を行った。

本章では、スキルモデルの策定に関して、以下の項目について述べる。

1. スキルモデルの策定について
2. スキルモデルのコンセプト
3. スキルモデルサンプル
4. スキルモデルの活用方法に関する考察

３．１ スキルモデルの策定について

スキルモデルの策定の背景とスキルモデル策定に係る活動について整理する。

３．１．１ スキルモデルの策定の背景

2002 年度「情報セキュリティプロフェッショナル育成に関する調査研究」の成果を踏まえ、2003 年度版スキルマップのアップデートを行うにあたって、スキルマップの具体的な活用イメージとして、情報セキュリティプロフェッショナルに求められるスキルをモデル化することが指摘された。スキルモデル策定の背景として、以下のような状況が認識されている。

（1）情報セキュリティプロフェッショナルの現状

2002 年度「情報セキュリティプロフェッショナル育成に関する調査研究」では、企業や組織において情報セキュリティに関する業務にたずさわる「情報セキュリティプロフェッショナル」の現状について調査を行った。

企業や自治体などへのアンケート調査や有識者へのヒアリング調査において、異口同音に指摘された重要な論点に「情報セキュリティにたずさわるエンジニアあるいは技術者は、独立した職種として捉えることができるか」という問題がある。

情報セキュリティの専門要員を置いている企業は、セキュリティ専業ベンダやセキュリティ監査サービスの提供事業者など一部の業種に限られており、一人のエンジニアや担当者が情報セキュリティに関する業務を兼任する場合も多い。情報セキュリティ関連の製品やサービスを専門的に扱う専業ベンダや事業者以外は、多くの企業にとって情報セキュリティへの対応は重要ではあるものの、関連のある業務の中で個別に対応しているのが実情ではないか。

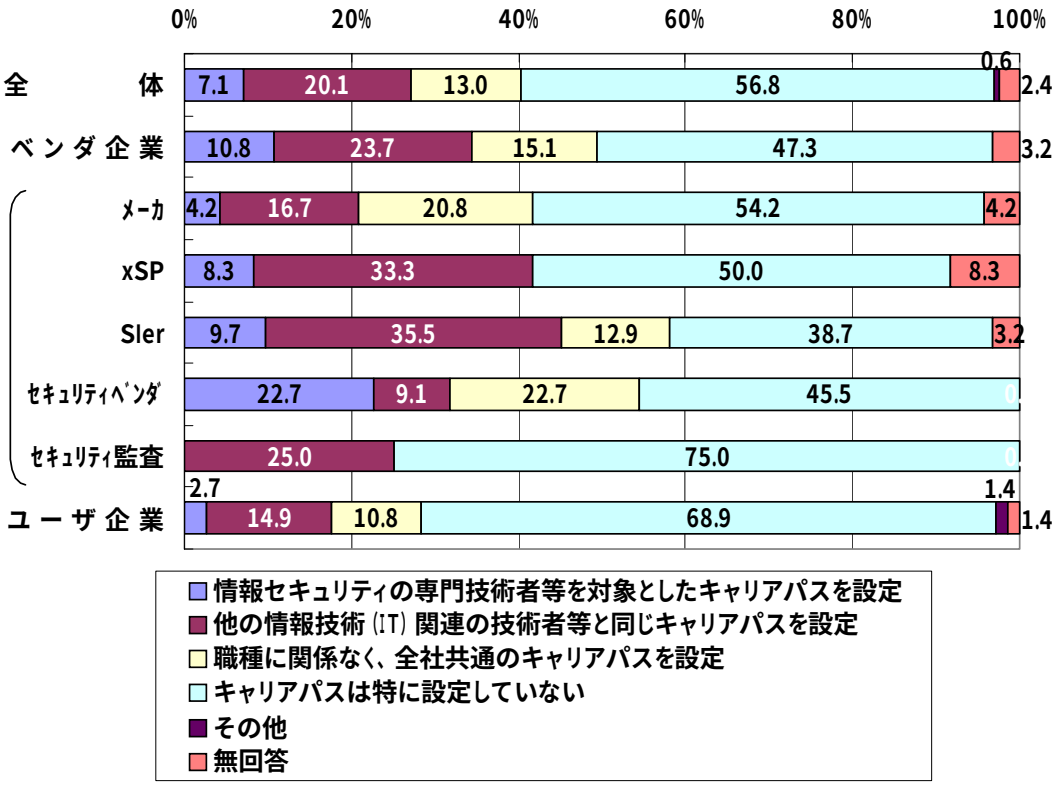


図 3-1　情報セキュリティにたずさわる人材に対するキャリアパスの状況（N=169）
（出典：2002 年度 IPA「情報セキュリティプロフェッショナル育成に関する調査研究」）

また、情報セキュリティプロフェッショナルに要求される専門性、対象となる要員の少なさゆえに、キャリアパスを明示的に設定している企業は少ない（図 3-1 参照）。情報セキュリティプロフェッショナルのスペシャリスト的な側面により、「プログラマ」→「システムエンジニア」→「コンサルタント」または「マネージャ」などといった IT エンジニアの一般的なキャリアパスが馴染み難いという指摘もある。キャリアパスを設定するためのスキルの明示や評価が難しいことがその一因となっている。

（2）情報セキュリティプロフェッショナルの育成に関する課題

現在、情報セキュリティにかかわる人材育成は、OJT を中心とした方法が採られることが一般的になっているが、技術の変化への対応の難しさ、研修・訓練プログラムの設定難しさなどが大きな問題となっている。情報セキュリティを習得するためには、OS、ネットワーク技術、プログラミング、情報科学、経営等、セキュ基礎となる分野の知識が必要になる。加えて、セキュリティに関する体系的な理論や知識の習得と、様々な製品固有の技術知識の双方が求められる。

情報セキュリティを含む IT の分野においては、情報処理技術者試験がわが国の IT 技術者の育成において重要な貢献を行ってきた。一方で、「試験の内容が実務の内容と

必ずしも一致していない」、「資格取得と仕事・給与が結びつけている企業が少ない」、「変化の速い最新技術への対応が遅れる傾向が見られる」「一度取得すると生涯認められるため、その資格によって認定される知識の陳腐化が懸念」などの指摘もあった。また、合格／不合格の二元的な判定基準しかなく、試験を受けた人が自分はどの分野が得意で、どこに弱点があるか、といったことを分析することはできない。

近年では、IT ベンダが自社の製品や技術などに関する知識の認定を行う、いわゆる「ベンダ資格」を重視する企業も増えてきている。しかし、ベンダ資格に対しても、「技術の陳腐化が速く、実際のビジネスにどれ位役立っているか正確に検証しにくい」、「個別の製品に特化するあまり、総合力や基礎力を判断するには不向き」といった意見もある。

情報セキュリティにたずさわる人材の育成やその評価において、個別の技術知識の習得レベルを客観的に判断できる指標が求められているといえる。

（3）情報セキュリティプロフェッショナルのスキルと業務の関係

「ユーザ企業」、「ベンダ企業」といった業種、あるいは、「Web アプリケーション開発」、「ネットワーク構築」、「セキュリティポリシー構築」といった、エンジニアや開発者がたずさわる個別の業種や業務の内容によって、求められる技術知識の内容、範囲、レベルが異なってくる。情報セキュリティプロフェッショナルに求められるスキルについて検討する場合、職種、業務とスキルの関係について整理をする必要がある。

また、通常、情報システムや製品の開発などは、プロジェクトチームを編成して対応する場合が一般的であるが、チームの要員計画の観点から、チーム全体として求められるスキルと個人単位のスキルの関係をどう捉えるかについても、検討課題のひとつとなっている。

3．1．2 スキルモデルの策定作業について

上記のような問題意識を背景に、情報セキュリティに関する「スキルモデル」の検討を行った（「2．2．2 スキルマップの構築作業について」参照）。本年度の調査研究活動では、スキルモデルのコンセプトを広く理解してもらうために、情報セキュリティにかかわる業務の例として 5 つを抽出し、それぞれの業務に対応するスキルモデルのサンプルを作成した（「3．3 スキルモデルサンプル」参照）。

また、スキルモデルの客観性を高め、より汎用性のあるものとするため、学識者や業界関係者へのヒアリングや現業で情報セキュリティ関連の業務にたずさわっている人を対象としたグループインタビューの場で、スキルモデルのコンセプトの妥当性や活用の可能性について、レビューを行った。

図 3-2に、スキルモデルの検討プロセスを示す。

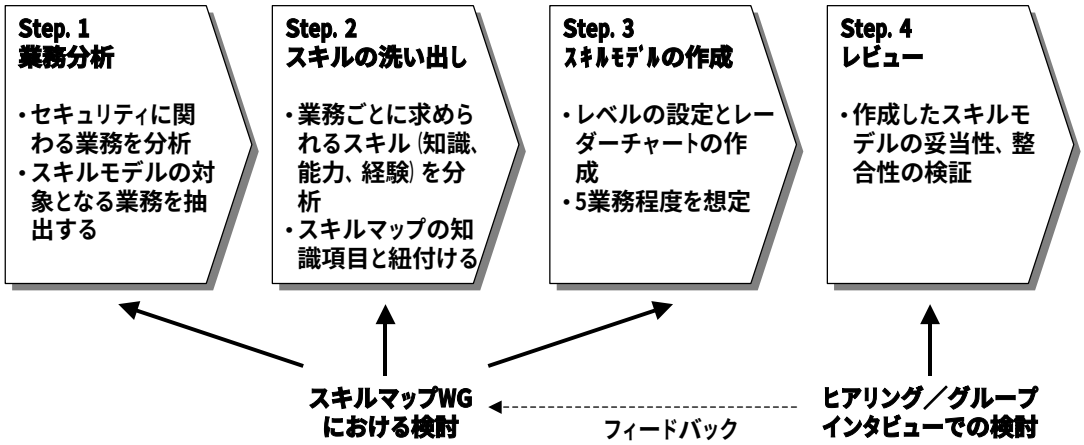


図 3-2　スキルモデルの検討プロセス

３．２ スキルモデルのコンセプト

以下に、本調査研究にて検討したスキルモデルのコンセプトについて示す。

（1）スキルモデルとは

スキルモデルとは「情報セキュリティに関する個別の業務やタスクにおいて求められるスキルとそのレベルを整理したもの」であり、以下のようなことが可能になることを目的とする。

- スキルマップのコンセプトを基礎として、情報セキュリティに関する業務ごとに求められる知識の内容とレベルを整理する。
- 人材育成や採用、能力評価、調達など、幅広い用途に活用できるものとする。
- スキルマップの使用者が、それぞれの目的や用途に応じてカスタマイズしようとする時の活用イメージを与える

（2）スキルモデルの特徴

「３．１．１ スキルモデルの策定の背景（1）情報セキュリティプロフェッショナルの現状」にて述べたように、情報セキュリティプロフェッショナルは、独立した職種として捉えきれない場合も多い。その一方、ネットワークの構築、IT 関連製品の開発、情報システムの開発と運用など、企業において情報セキュリティが関係する「業務」は確実に存在する。そこで、スキルモデルにおいては、情報セキュリティに関する「職種」よりもむしろ、情報セキュリティプロフェッショナルのたずさわる「業務」に着目し、個別の「業務」の遂行において求められる技術知識の「レベル定義」を導入している点が特徴的である。この「業務」の考え方、ならびに、「レベル定義」の考え方については、本節の「(3）スキルモデルにおける「業務」と「レベル定義」の考え方について」及び「(5)「スキルレベルテーブル」を用いたレベル定義について」にて説明する。

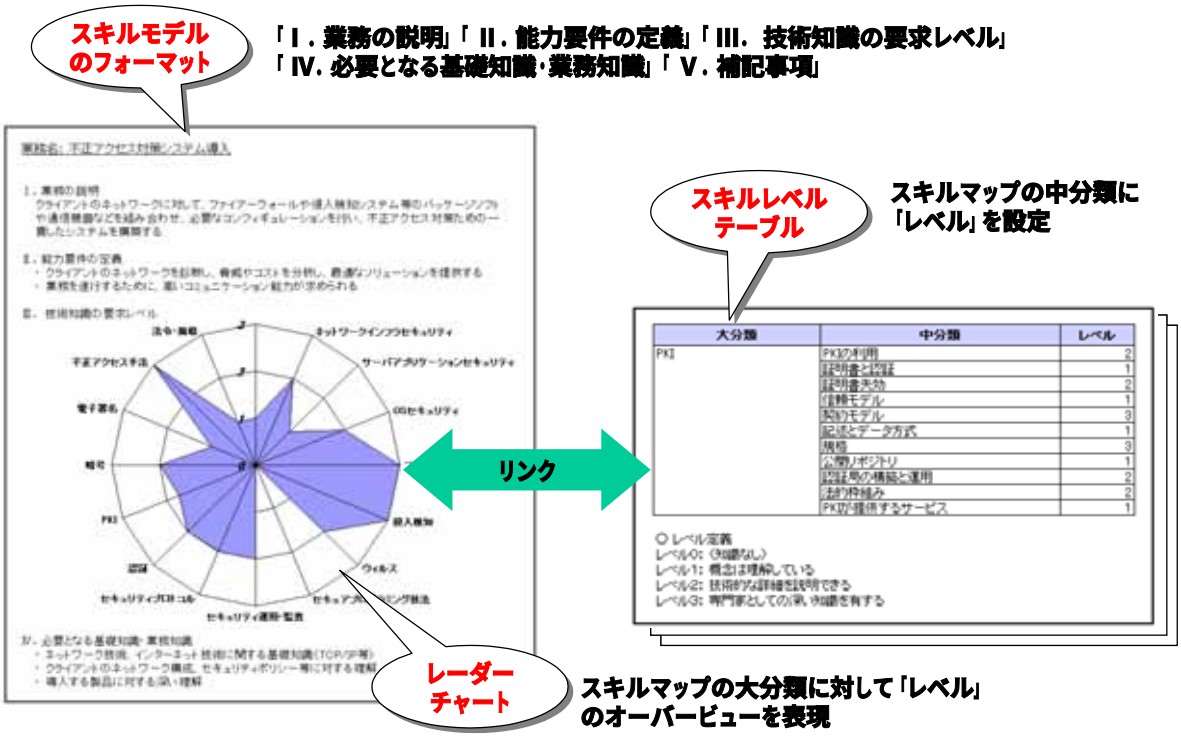


図 3-3　スキルモデルの概要

スキルモデルでは、業務に対する能力の要件（スキルや技術知識を含む）を定型的に表現するフォーマットを用意し、カスタマイズ可能なモデルとしている。レーダーチャート表現によってオーバービューを示すと同時に、スキルマップの中分類を対象にレベル設定を行う「スキルレベルテーブル」と大分類に対してレベルのオーバービューを表示する「レーダーチャート」を組み合わせることによって、レベル定義の厳密性と一覧性の両立を図っている（図 3-3 参照）。

（3）スキルモデルにおける「業務」と「レベル定義」の考え方について

2002 年度版スキルマップの検討の時点から、スキルマップに「レベル」の概念を導入することによって、情報セキュリティにたずさわる人材に求められる技術知識のモデル化を検討してきた。

しかしながら、「2．3．2 スキルマップのアップデートに係る論点（3）「レベル」の考え方」において述べたように、情報セキュリティに関係する職種や業務によってレベルの意味や内容が異なる場合があり、また、そのレベルの内容は画一ではないこともあり、一概に定義することが難しい場合がある。さらには、「3．1．1 スキルモデルの策定の背景（1）情報セキュリティプロフェッショナルの現状」において指摘したように、「『情報セキュリティプロフェッショナル』は、独立した職種として捉えることことができるか」という問題もある。それゆえ、このような職種・業務とレベル定義の関係を整理する必要がある。

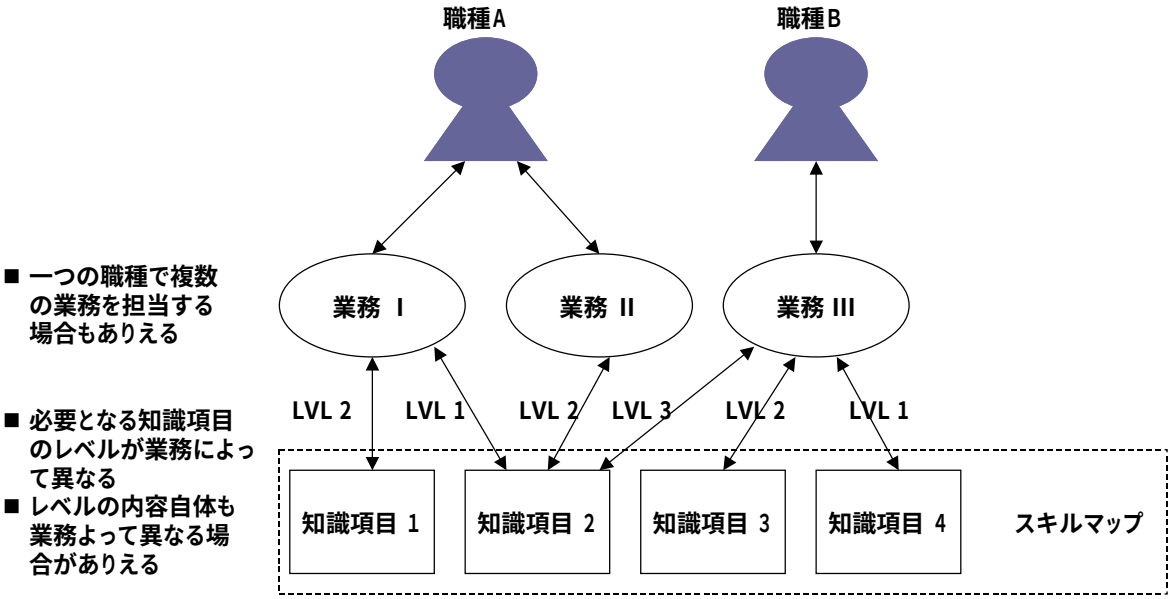


図 3-4　スキルモデルにおける「業務」と「レベル定義」の考え方

図 3-4に示すように、ある職種（職種 A）においては、複数の業務（業務Ⅰ、業務Ⅱ）を担当する場合（あるいは、「職種 A」は「業務Ⅰ」及び「業務Ⅱ」から構成される、といってもよいかもしれない）もあるし、他の業務（職種 B）においては単一の業務（業務Ⅲ）のみを担当する場合も考えられる。さらに、業務によって、それぞれ必要とされる技術知識の内容及び深さ（レベル）も異なってくる。逆に、同じ知識項目の種類でも、業務によって求められるレベルが異なる場合もあるだろう（例： 図 3-4中の「知識項目２」は、「業務Ⅰ」においてはレベル 1、「業務Ⅱ」においてはレベル 2、「業務Ⅲ」においてはレベル３が求められる）。

さらに、知識項目によっては、レベルそのもの内容が異なってくる場合もありえる。例えば、知識の有無（知っている／知らない）に基づくレベルのほか、業務経験（業務としての経験がある／ない）、知識の活用度合い（知識を活用することができる／できない）などが考えられる。

上記のような問題意識を踏まえ、スキルモデルでは情報セキュリティに関連する「業務」を対象として扱い、「業務」ごとに「レベル」を定義することとした。現在のスキルモデルでは、レベル設定のし易さを考慮して、表 3-1に示す 3 段階を基本タイプとしている。

また、表 3-1のレベル定義は、スキルモデルの利用者が自身のニーズに応じて、「業務」ごとにレベル定義の内容を変更しても良い。

表 3-1　スキルモデルのレベル定義（基本タイプ）

レベル	レベルの内容
レベル0	知識がない、または、経験がない
レベル1	知識項目の概要を理解している水準である。業務を通じて、より詳細な技術的な内容を習得することができる。
レベル2	習得した知識項目を、業務において他の指導･援助を得つつ実践できる水準である。知識項目の技術的な内容について具体的に事例を示し説明することができる。
レベル3	知識を活用して、業務を自力で実践できる水準にある。実務を通じた数多くの実践経験に基づくノウハウを持っている。

上表のレベル定義において、「レベル０」のベースラインをどこに置くかが議論となる。「３．１．１ スキルモデルの策定の背景（２）情報セキュリティプロフェッショナルの育成に関する課題」にて述べたとおり、情報セキュリティに関する業務を担当するためには、その前提として、IT 関連の基礎技術や関連する業務知識が必要不可欠である。

本調査研究においては、ある程度の IT 分野における業務を経験した（2～3 年程度)、初級技術者や担当者をベースラインとして想定することとした。企業や業務の内容によっては、情報処理技術者試験の「基本情報技術者」や経済産業省が策定している「IT スキル・スタンダード」における「エントリレベル」（レベル 1～2）の人材が対応するかもしれない。

ただし、上記の想定はあくまでも便宜的なものであり、スキルモデルを使用する際には、それぞれの企業、組織の実用に即したベースラインが設定されるべきである。

（4）スキルモデルのフォーマット

上記のような「業務」と「レベル定義」のコンセプトにもとづいて、スキルモデルを表現するためのフォーマットを作成した[5]。

フォーマットでは、スキルモデルの対象とする業務ごとに、表 3-2 に示す内容を定型的に記載する形をとっている。記載項目のうち「Ⅲ．技術知識の要求レベル」が、スキルマップに対応した「レーダーチャート」になり、このフォーマットに附属する「スキルレベルテーブル」にて、各大分類の中分類ごとにレベルを設定する。

このフォーマットは、完全に固定されたものでなく、スキルマップやスキルモデルの利用者が、それぞれのニーズに応じてカスタマイズして使用することを想定している。

[5] 現在のバージョンは Microsoft Excel 形式のファイルとして提供されている（「７．１ スキルモデルのフォーマット」参照）

表 3-2　スキルモデルのフォーマット

項目	記載内容
Ⅰ．業務の説明	対象となる業務の内容、求められる 成果、どういった職種が担当することが想定されるのか等について記述
Ⅱ．能力要件の定義	業務を遂行するにあたって必要となる能力を定義
Ⅲ．技術知識の要求レベル	スキルマップの各知識項目に対するレベルの定義。「スキルレベルテーブル」と「レーダーチャート」によって表現
Ⅳ．必要となる基礎知識・業務知識	スキルマップに規定される技術知識以外の知識項目について規定（例： 「TCP/IP」、「電子申請システムに対する知識」）
Ⅴ．補記事項	その他、特記事項を記載（例： 業務に必要な資格等）

（5）「スキルレベルテーブル」を用いたレベル定義について

スキルモデルのフォーマット（Microsoft Excel 形式）に附属する形の「スキルレベルテーブル」は、スキルマップの各大分類の中分類を抽出したものであり、スキルモデルの利用者はスキルレベルテーブルの各項目にレベルを定義する形となる（図 3-5）。スキルレベルテーブルは、図 3-3 中の「レーダーチャート」にリンクしており、スキルレベルテーブルの中分類の各項目にレベルを設定すると、レーダーチャートが自動的に更新されるようになっている。

スキルモデルでは、レーダーチャートによって、業務ごとに求められる技術知識のレベルのオーバービュー（大分類ごとの相対関係）を与えると同時に、各大分類個別の知識項目ごとの詳細レベルついて、必要に応じてスキルレベルテーブルを参照することができる。このようにスキルモデルでは、レベル定義の一覧性と詳細化の両立を図っている。

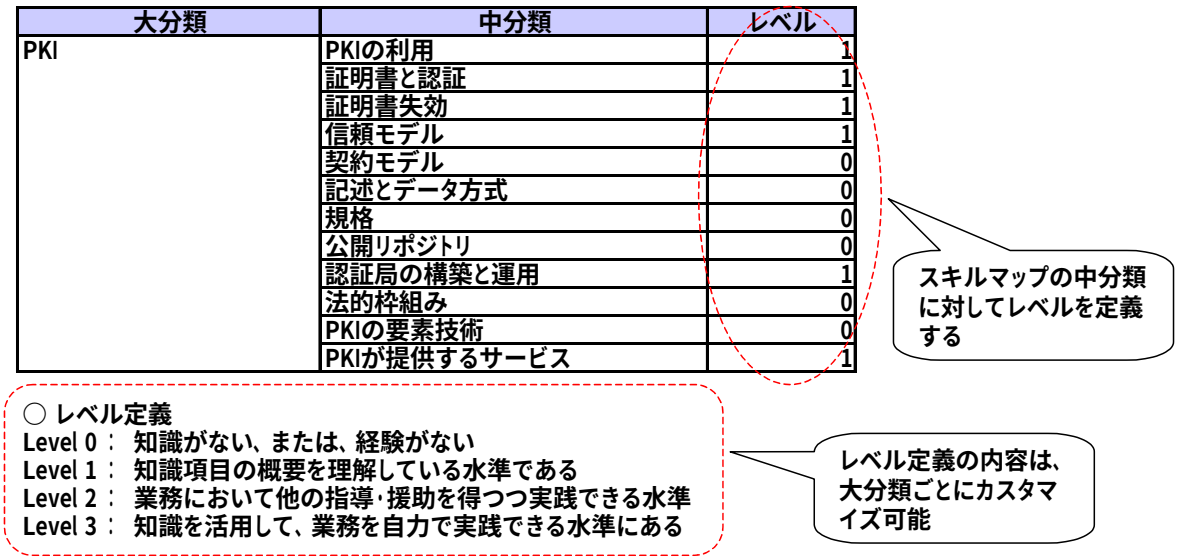


図 3-5　スキルレベルテーブルの内容

３．３ スキルモデルサンプル

本調査研究においては、情報セキュリティに関する下記の 5 つの業務を取り上げ、スキルモデルの具体的なサンプルを作成した。

1. セキュリティポリシー導入
2. システム全体に対するセキュリティ設計
3. 不正アクセス対策システム導入
4. ネットワーク系アプリケーション設計・開発
5. セキュリティ運用管理

以降に、上記 1.～5.のスキルモデルサンプルを示す。

（1）セキュリティポリシー導入

【スキルモデルサンプル】

業務名： セキュリティポリシー導入

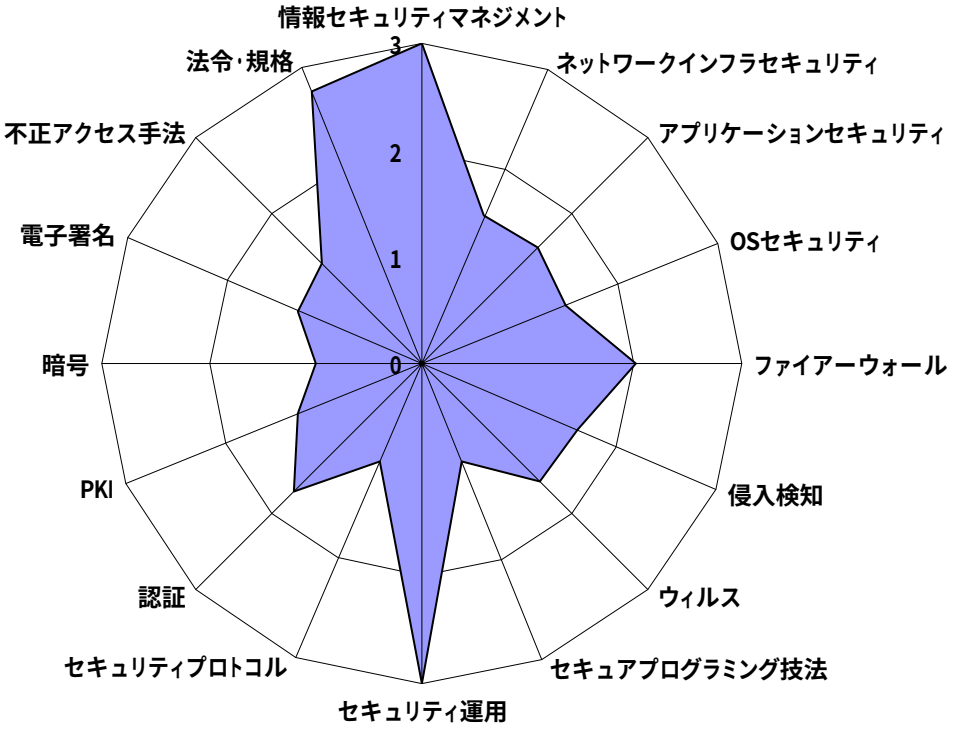
Ⅰ．業務の説明

ユーザ（企業）に対して、ISMS 認証取得を目指した情報セキュリティポリシーを、リスク分析を含めて策定する。

Ⅱ．能力要件の定義

- **情報セキュリティポリシーを策定する能力**
- **ユーザ（企業）が ISMS を構築し、サイクル運用できるようになるために必要な助言をできる能力（必要項目、課題解決）**
- **リスク分析・報告をする能力**
- **コンサルティング能力**

Ⅲ．技術知識の要求レベル



Ⅳ．必要となる基礎知識・業務知識

- **インターネット技術に関する基礎知識（TCP/IP 等）**
- **ネットワーク技術、サーバ技術**
- **セキュリティ製品の知識**
- **関連法規**

Ⅴ．補記事項

【スキルレベルテーブルサンプル】

レベル０：　知識がない、または、経験がない
レベル１：　知識項目の概要を理解している水準である。業務を通じて、より詳細な技術的な内容を習得することができる。
レベル２：　習得した知識項目を、業務において他の指導・援助を得つつ実践できる水準である。知識項目の技術的な内容について具体的に事例を示し説明することができる。
レベル３：　知識を活用して、業務を自力で実践できる水準にある。実務を通じた数多くの実践経験に基づくノウハウを持っている。

大分類	中分類	レベル
情報セキュリティマネジメント	マネジメント技術	3
	リスク分析技術	3
	情報セキュリティポリシー	3
	情報セキュリティ監査	3
	関連知識	3
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	2
	ネットワークアクセスコントロール	2
	VPN	1
	無線 LAN	1
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	2
	Web サーバのセキュリティ対策	2
	Web サーバの運用	1
	Web アプリケーション設計	1
	Web ブラウザのセキュリティ	1
	Web 関連プロトコルの基礎知識	1
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	2
	メールサーバのセキュリティ対策	2
	メールクライアントのセキュリティ	2
	メールサーバの運用	1
アプリケーションセキュリティ【DNS】	DNS サーバに対する脅威	2
	DNS サーバセキュリティ対策と構成	2
	DNS サーバの運用	1
OS セキュリティ【Unix】	ログ管理	2
	パッチ適用管理	2
	サービスの管理	1
	ファイルシステム管理	1
	アカウント管理	2
OS セキュリティ【Windows】	構成･設定管理	2
	パッチ適用管理	2
	監査	1
	ログ管理	2
	プロセス管理	1
	サービス管理	1
	ファイルシステム管理	1
	アカウント管理	2
	ネットワーク保護	2
OS セキュリティ【TrustedOS】	強制アクセス制御の概念（MAC	0
ファイアーウォール	ファイアーウォールの導入･運用	3
	NAT	1
	ネットワークアクセスコントロール	2
侵入検知	侵入検知システムの導入･運用	3

大分類	中分類	レベル
	侵入検知システムの機能	2
	検出アルゴリズム	1
	検出方法	1
	侵入検知システム	1
ウィルス	管理体制	3
	感染後のポリシー	2
	予防ポリシー	2
	発病	1
	検出方法と駆除	1
	感染	1
	種類	1
セキュアプログラミング技法	Web アプリケーション	1
	DB	1
	アプリケーション全般	1
	XML	1
	PHP	1
	JAVA	1
	Perl	1
	VB/ASP	1
	C/C++	1
	UNIX	1
	コンパイラ・仮想マシン	1
	Windows	1
セキュリティ運用	定常運用時のセキュリティ確保	3
	異常時対応	3
	運用関連情報（脆弱性情報・対策情報・攻撃情報・被害情報）	3
セキュリティプロトコル	アプリケーション層	1
	トランスポート層	1
	ネットワーク層	1
	データリンク層	1
認証	パスワード認証	2
	バイオメトリック認証	1
	認証デバイス	2
	認証プロトコル	2
	Web 認証	2
	システム認証	2
	シングルサインオン	1
PKI	PKI の利用	2
	証明書と認証	1
	証明書失効	1
	信頼モデル	1
	契約モデル	1
	記述とデータ方式	1
	規格	1
	公開リポジトリ	1
	認証局の構築と運用	2
	法的枠組み	1
	PKI の要素技術	1

大分類	中分類	レベル
	PKI が提供するサービス	2
暗号	公開鍵暗号	2
	共通鍵暗号	2
	ハッシュ関数	1
	暗号用乱数	1
	鍵管理	1
	ゼロ知識証明	0
	その他の暗号方式	0
	暗号解読･強度評価	1
電子署名	電子署名の利用	2
	電子署名の要素技術	1
	電子署名の仕組み	1
	電子署名の利点	1
不正アクセス手法	遠隔不正侵入･操作	2
	サービスの停止	2
	盗聴行為	1
	偵察行為	1
	情報収集	1
	古典的不正アクセス技法	1
法令･規格	基準･指針･ガイドライン等	3
	法令	3
	国際標準規格	2
	国際ガイドライン	3

（2）システム全体に対するセキュリティ設計

【スキルモデルサンプル】

業務名： システム全体に対するセキュリティ設計

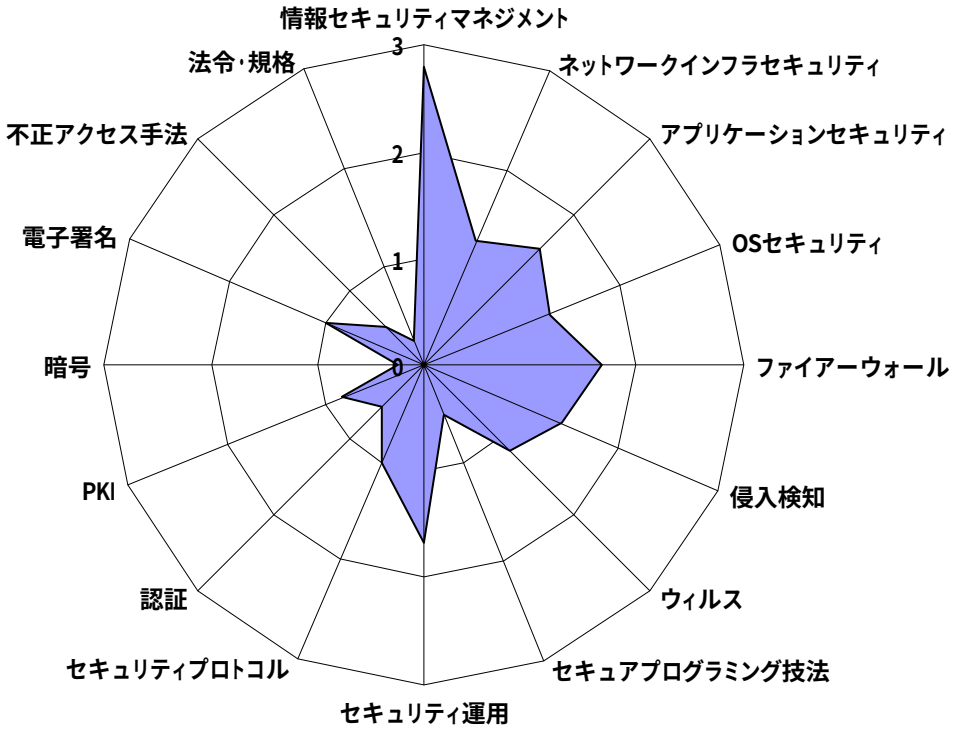
Ⅰ．業務の説明

新規のシステム開発時における、システム全般にまたがるセキュリティの要件分析を行い、最適なセキュアシステムを設計する。

Ⅱ．能力要件の定義

- **システム全体（開発・インフラ）に対する、広範囲な知識と理解能力が求められる**
- **システム要件のとりまとめ、分析を行い、総合的なセキュリティコンセプトを設計できる**
- **プロジェクト全体をコントロールするための高いマネジメント能力が求められる**
- **業務を遂行するために、高いコミュニケーション能力が求められる**
- **基本的に全分野に対するセキュリティの理解が必須となる**
- **トータルシステムとして、セキュリティ施策の必要充分条件の見極めが出来る能力が必要**

Ⅲ．技術知識の要求レベル



Ⅳ．必要となる基礎知識・業務知識

- **提案、設計、導入、運用など一連の業務手順に関する高度な理解。**
- **開発／構築するシステムへの総合的な理解が必要（業務やデータの流れを含む）**

Ⅴ．補記事項

【スキルレベルテーブルサンプル】

レベル０：　知識がない、または、経験がない
レベル１：　知識項目の概要を理解している水準である。業務を通じて、より詳細な技術的な内容を習得することができる。
レベル２：　習得した知識項目を、業務において他の指導・援助を得つつ実践できる水準である。知識項目の技術的な内容について具体的に事例を示し説明することができる。
レベル３：　知識を活用して、業務を自力で実践できる水準にある。実務を通じた数多くの実践経験に基づくノウハウを持っている。

大分類	中分類	レベル
情報セキュリティマネジメント	マネジメント技術	3
	リスク分析技術	3
	情報セキュリティポリシー	3
	情報セキュリティ監査	2
	関連知識	3
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	2
	ネットワークアクセスコントロール	1
	VPN	1
	無線 LAN	1
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	2
	Web サーバのセキュリティ対策	2
	Web サーバの運用	1
	Web アプリケーション設計	1
	Web ブラウザのセキュリティ	1
	Web 関連プロトコルの基礎知識	1
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	2
	メールサーバのセキュリティ対策	2
	メールクライアントのセキュリティ	2
	メールサーバの運用	1
アプリケーションセキュリティ【DNS】	DNS サーバに対する脅威	2
	DNS サーバセキュリティ対策と構成	2
	DNS サーバの運用	1
OS セキュリティ【Unix】	ログ管理	1
	パッチ適用管理	1
	サービスの管理	1
	ファイルシステム管理	1
	アカウント管理	2
OS セキュリティ【Windows】	構成･設定管理	2
	パッチ適用管理	1
	監査	1
	ログ管理	1
	プロセス管理	1
	サービス管理	1
	ファイルシステム管理	1
	アカウント管理	2
	ネットワーク保護	2
OS セキュリティ【TrustedOS】	強制アクセス制御の概念（MAC	1
ファイアーウォール	ファイアーウォールの導入･運用	2
	NAT	1
	ネットワークアクセスコントロール	2
侵入検知	侵入検知システムの導入･運用	2

大分類	中分類	レベル
	侵入検知システムの機能	2
	検出アルゴリズム	1
	検出方法	1
	侵入検知システム	1
ウィルス	管理体制	2
	感染後のポリシー	1
	予防ポリシー	1
	発病	1
	検出方法と駆除	1
	感染	1
	種類	1
セキュアプログラミング技法	Web アプリケーション	1
	DB	1
	アプリケーション全般	1
	XML	1
	PHP	0
	JAVA	0
	Perl	0
	VB/ASP	0
	C/C++	0
	UNIX	1
	コンパイラ・仮想マシン	0
	Windows	1
セキュリティ運用	定常運用時のセキュリティ確保	2
	異常時対応	2
	運用関連情報（脆弱性情報・対策情報・攻撃情報・被害情報）	1
セキュリティプロトコル	アプリケーション層	1
	トランスポート層	1
	ネットワーク層	1
	データリンク層	1
認証	パスワード認証	1
	バイオメトリック認証	0
	認証デバイス	0
	認証プロトコル	1
	Web 認証	1
	システム認証	1
	シングルサインオン	0
PKI	PKI の利用	1
	証明書と認証	1
	証明書失効	1
	信頼モデル	1
	契約モデル	1
	記述とデータ方式	0
	規格	1
	公開リポジトリ	1
	認証局の構築と運用	1
	法的枠組み	0
	PKI の要素技術	1

大分類	中分類	レベル
	PKI が提供するサービス	1
暗号	公開鍵暗号	1
	共通鍵暗号	1
	ハッシュ関数	0
	暗号用乱数	0
	鍵管理	0
	ゼロ知識証明	0
	その他の暗号方式	0
	暗号解読･強度評価	0
電子署名	電子署名の利用	1
	電子署名の要素技術	1
	電子署名の仕組み	1
	電子署名の利点	1
不正アクセス手法	遠隔不正侵入･操作	1
	サービスの停止	1
	盗聴行為	0
	偵察行為	0
	情報収集	1
	古典的不正アクセス技法	0
法令･規格	基準･指針･ガイドライン等	1
	法令	0
	国際標準規格	0
	国際ガイドライン	0

（3）不正アクセス対策システム導入

【スキルモデルサンプル】

業務名： 不正アクセス対策システム導入

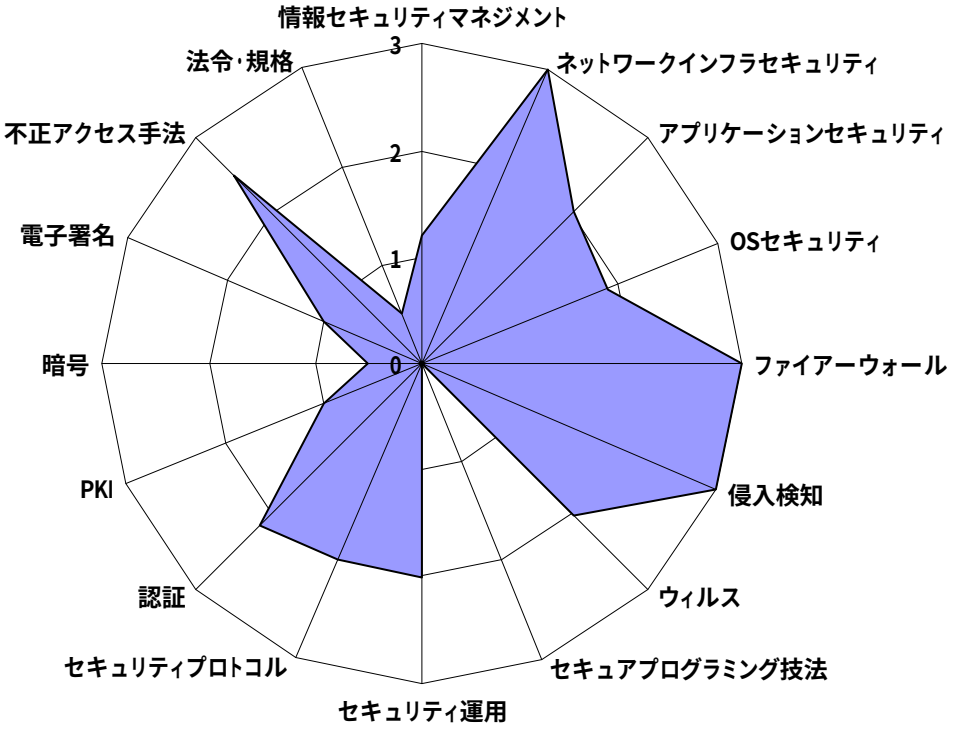
Ⅰ．業務の説明

ネットワークシステム全体の基本設計を元に、インフラ周りのセキュリティ詳細設計を実施する。不正アクセス防止のためファイアーウォールや侵入検知システム等の機器選定、各設定項目のしきい値決定などを含むドキュメント作成作業を行う。

Ⅱ．能力要件の定義

- **不正アクセス手法を熟知し、技術面、コスト面等総合的に踏まえた最適なソリューションを提案できる。**
- **クライアント、基本設計者、プロダクト技術者、開発系職種など関係者との適切なコミュニケーション、リーダーシップ、調整能力が求められる。**

Ⅲ．技術知識の要求レベル



Ⅳ．必要となる基礎知識・業務知識

- **提案、設計、導入、運用など一連の業務手順に関する高度な理解。**
- **セキュリティポリシー等、マネジメントに関する基礎知識。**
- **LAN、WAN、プロトコル（TCP/IP）等ネットワークに関する高度な知識。**
- **開発手法、プログラミングに関する基礎知識。**

Ⅴ．補記事項

【スキルレベルテーブルサンプル】

レベル０：　知識がない、または、経験がない
レベル１：　知識項目の概要を理解している水準である。業務を通じて、より詳細な技術的な内容を習得することができる。
レベル２：　習得した知識項目を、業務において他の指導・援助を得つつ実践できる水準である。知識項目の技術的な内容について具体的に事例を示し説明することができる。
レベル３：　知識を活用して、業務を自力で実践できる水準にある。実務を通じた数多くの実践経験に基づくノウハウを持っている。

大分類	中分類	レベル
情報セキュリティマネジメント	マネジメント技術	1
	リスク分析技術	1
	情報セキュリティポリシー	2
	情報セキュリティ監査	1
	関連知識	1
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	3
	ネットワークアクセスコントロール	3
	VPN	3
	無線 LAN	3
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	2
	Web サーバのセキュリティ対策	2
	Web サーバの運用	2
	Web アプリケーション設計	2
	Web ブラウザのセキュリティ	2
	Web 関連プロトコルの基礎知識	2
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	2
	メールサーバのセキュリティ対策	2
	メールクライアントのセキュリティ	2
	メールサーバの運用	2
アプリケーションセキュリティ【DNS】	DNS サーバに対する脅威	2
	DNS サーバセキュリティ対策と構成	2
	DNS サーバの運用	2
OS セキュリティ【Unix】	ログ管理	2
	パッチ適用管理	2
	サービスの管理	2
	ファイルシステム管理	2
	アカウント管理	2
OS セキュリティ【Windows】	構成･設定管理	2
	パッチ適用管理	2
	監査	1
	ログ管理	2
	プロセス管理	1
	サービス管理	2
	ファイルシステム管理	2
	アカウント管理	2
	ネットワーク保護	2
OS セキュリティ【TrustedOS】	強制アクセス制御の概念（MAC	2
ファイアーウォール	ファイアーウォールの導入･運用	3
	NAT	3
	ネットワークアクセスコントロール	3
侵入検知	侵入検知システムの導入･運用	3

大分類	中分類	レベル
	侵入検知システムの機能	3
	検出アルゴリズム	3
	検出方法	3
	侵入検知システム	3
ウィルス	管理体制	2
	感染後のポリシー	2
	予防ポリシー	2
	発病	2
	検出方法と駆除	2
	感染	2
	種類	2
セキュアプログラミング技法	Web アプリケーション	0
	DB	0
	アプリケーション全般	0
	XML	0
	PHP	0
	JAVA	0
	Perl	0
	VB/ASP	0
	C/C++	0
	UNIX	0
	コンパイラ・仮想マシン	0
	Windows	0
セキュリティ運用	定常運用時のセキュリティ確保	2
	異常時対応	2
	運用関連情報（脆弱性情報・対策情報・攻撃情報・被害情報）	2
セキュリティプロトコル	アプリケーション層	2
	トランスポート層	2
	ネットワーク層	2
	データリンク層	2
認証	パスワード認証	3
	バイオメトリック認証	0
	認証デバイス	1
	認証プロトコル	3
	Web 認証	3
	システム認証	3
	シングルサインオン	2
PKI	PKI の利用	1
	証明書と認証	1
	証明書失効	1
	信頼モデル	1
	契約モデル	1
	記述とデータ方式	1
	規格	1
	公開リポジトリ	1
	認証局の構築と運用	1
	法的枠組み	1
	PKI の要素技術	1

大分類	中分類	レベル
	PKI が提供するサービス	1
暗号	公開鍵暗号	1
	共通鍵暗号	1
	ハッシュ関数	1
	暗号用乱数	0
	鍵管理	1
	ゼロ知識証明	0
	その他の暗号方式	0
	暗号解読･強度評価	0
電子署名	電子署名の利用	1
	電子署名の要素技術	1
	電子署名の仕組み	1
	電子署名の利点	1
不正アクセス手法	遠隔不正侵入･操作	3
	サービスの停止	3
	盗聴行為	2
	偵察行為	3
	情報収集	3
	古典的不正アクセス技法	1
法令･規格	基準･指針･ガイドライン等	1
	法令	0
	国際標準規格	1
	国際ガイドライン	0

（4）ネットワーク系アプリケーション設計・開発

【スキルモデルサンプル】

業務名： ネットワーク系アプリケーション設計・開発

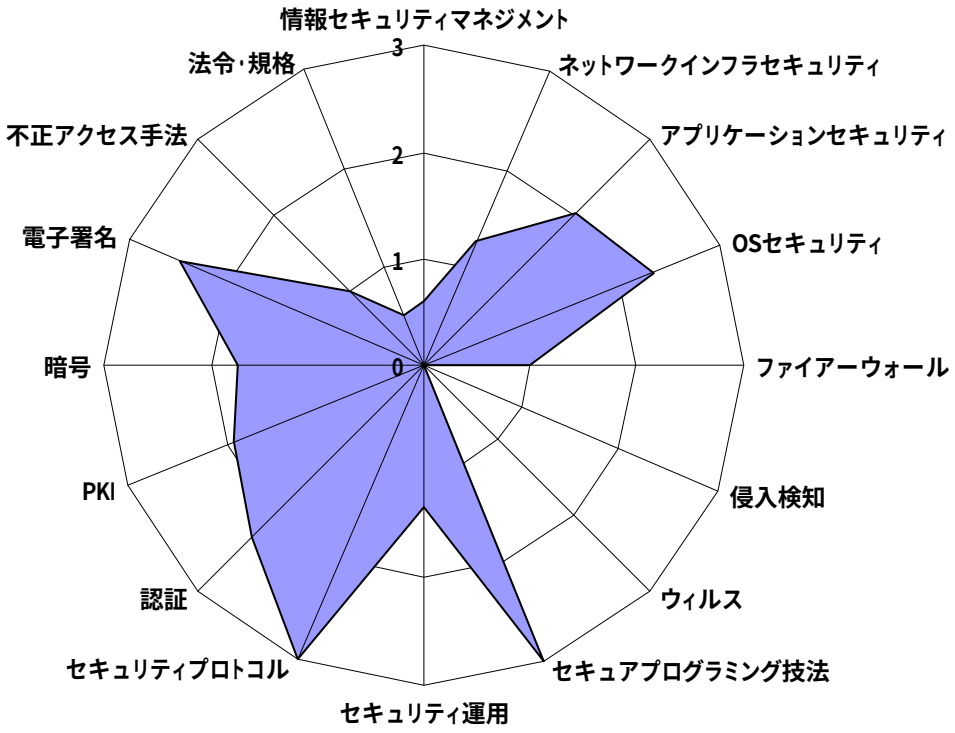
Ⅰ．業務の説明

要求仕様書、基本設計書をもとにセキュリティを考慮した詳細設計、機能設計を行いアプリケーション開発を行う。また開発アプリケーションのテスト仕様を作成する。

Ⅱ．能力要件の定義

- **要求仕様をもとに、適切なセキュリティ対策を行う**
- **既存の脆弱性を考慮し、設計に反映させる**
- **セキュアプログラミング**
- **コミュニケーション能力、現状および要求を分析する能力**

Ⅲ．技術知識の要求レベル



Ⅳ．必要となる基礎知識・業務知識

- **ネットワークに関する基礎知識**
- **セキュリティプロトコルに関する基礎知識、認証に関する知識**
- **PKI、暗号、電子署名に関する知識**
- **セキュリティプログラミング技法の詳細な知識**

Ⅴ．補記事項

【スキルレベルテーブルサンプル】

レベル０：　知識がない、または、経験がない
レベル１：　知識項目の概要を理解している水準である。業務を通じて、より詳細な技術的な内容を習得することができる。
レベル２：　習得した知識項目を、業務において他の指導・援助を得つつ実践できる水準である。知識項目の技術的な内容について具体的に事例を示し説明することができる。
レベル３：　知識を活用して、業務を自力で実践できる水準にある。実務を通じた数多くの実践経験に基づくノウハウを持っている。

大分類	中分類	レベル
情報セキュリティマネジメント	マネジメント技術	1
	リスク分析技術	1
	情報セキュリティポリシー	0
	情報セキュリティ監査	0
	関連知識	1
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	1
	ネットワークアクセスコントロール	2
	VPN	1
	無線 LAN	1
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	2
	Web サーバのセキュリティ対策	2
	Web サーバの運用	2
	Web アプリケーション設計	3
	Web ブラウザのセキュリティ	3
	Web 関連プロトコルの基礎知識	3
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	2
	メールサーバのセキュリティ対策	2
	メールクライアントのセキュリティ	2
	メールサーバの運用	2
アプリケーションセキュリティ【DNS】	DNS サーバに対する脅威	1
	DNS サーバセキュリティ対策と構成	1
	DNS サーバの運用	1
OS セキュリティ【Unix】	ログ管理	3
	パッチ適用管理	1
	サービスの管理	3
	ファイルシステム管理	3
	アカウント管理	3
OS セキュリティ【Windows】	構成･設定管理	3
	パッチ適用管理	1
	監査	2
	ログ管理	3
	プロセス管理	1
	サービス管理	3
	ファイルシステム管理	3
	アカウント管理	3
	ネットワーク保護	3
OS セキュリティ【TrustedOS】	強制アクセス制御の概念（MAC	0
ファイアーウォール	ファイアーウォールの導入･運用	1
	NAT	1
	ネットワークアクセスコントロール	1
侵入検知	侵入検知システムの導入･運用	0

大分類	中分類	レベル
	侵入検知システムの機能	0
	検出アルゴリズム	0
	検出方法	0
	侵入検知システム	0
ウィルス	管理体制	0
	感染後のポリシー	0
	予防ポリシー	0
	発病	0
	検出方法と駆除	0
	感染	0
	種類	0
セキュアプログラミング技法	Web アプリケーション	3
	DB	3
	アプリケーション全般	3
	XML	3
	PHP	3
	JAVA	3
	Perl	3
	VB/ASP	3
	C/C++	3
	UNIX	3
	コンパイラ・仮想マシン	3
	Windows	3
セキュリティ運用	定常運用時のセキュリティ確保	2
	異常時対応	0
	運用関連情報（脆弱性情報・対策情報・攻撃情報・被害情報）	2
セキュリティプロトコル	アプリケーション層	3
	トランスポート層	3
	ネットワーク層	3
	データリンク層	3
認証	パスワード認証	3
	バイオメトリック認証	0
	認証デバイス	2
	認証プロトコル	3
	Web 認証	3
	システム認証	3
	シングルサインオン	2
PKI	PKI の利用	2
	証明書と認証	2
	証明書失効	2
	信頼モデル	2
	契約モデル	2
	記述とデータ方式	2
	規格	2
	公開リポジトリ	2
	認証局の構築と運用	2
	法的枠組み	1
	PKI の要素技術	2

大分類	中分類	レベル
	PKI が提供するサービス	2
暗号	公開鍵暗号	2
	共通鍵暗号	2
	ハッシュ関数	2
	暗号用乱数	2
	鍵管理	2
	ゼロ知識証明	1
	その他の暗号方式	1
	暗号解読･強度評価	2
電子署名	電子署名の利用	2
	電子署名の要素技術	3
	電子署名の仕組み	3
	電子署名の利点	2
不正アクセス手法	遠隔不正侵入･操作	1
	サービスの停止	1
	盗聴行為	1
	偵察行為	1
	情報収集	1
	古典的不正アクセス技法	1
法令･規格	基準･指針･ガイドライン等	0
	法令	0
	国際標準規格	2
	国際ガイドライン	0

（5）セキュリティ運用管理

【スキルモデルサンプル】

業務名： セキュリティ運用管理

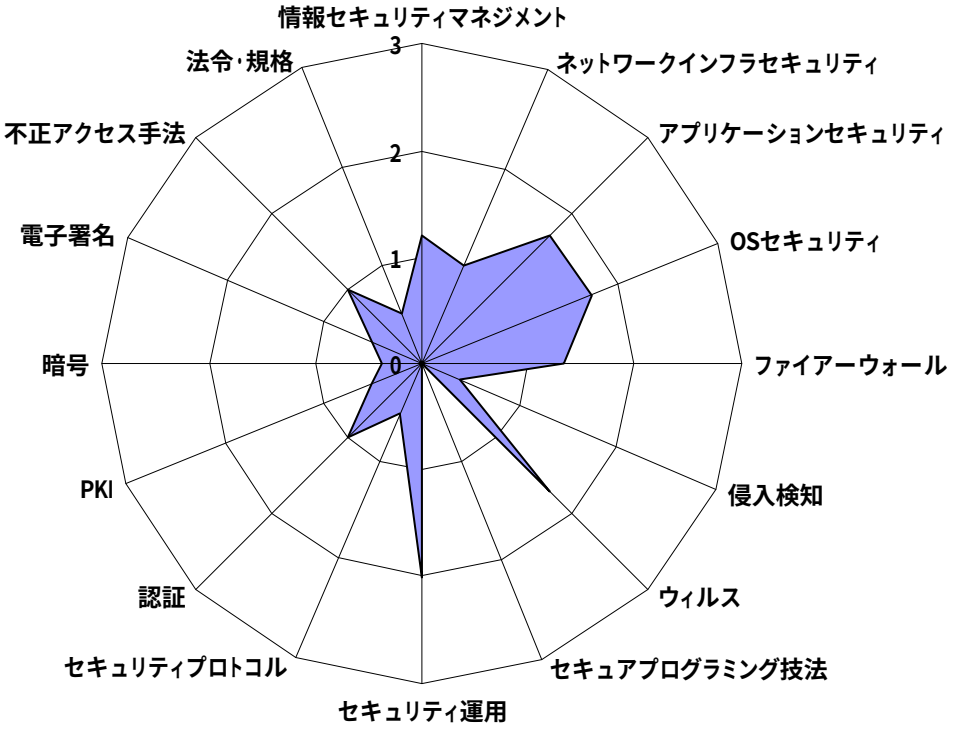
Ⅰ．業務の説明

ユーザ企業においてセキュリティを維持するために、全社的なセキュリティポリシーに従い、日常の運用としてアカウントの管理、セキュリティパッチ適用、バックアップ、監視、分析、情報収集等を行う。

Ⅱ．能力要件の定義

- **自社のネットワークインフラ全般に対する基本的な知識を有する**
- **日常の管理業務の中で PDCA のサイクルを用いてセキュリティレベルを安全に保つ**
- **全社的にセキュリティの認識を高め、協力を要請するコミュニケーション能力が求められる**

Ⅲ．技術知識の要求レベル



Ⅳ．必要となる基礎知識・業務知識

- **ネットワーク技術、インターネット技術に関する基礎レベルの知識（TCP/IP 等）**
- **自社のネットワーク構成、使用しているハード、ソフトの基本的な意味合いが分かるレベル**
- **SI に要求仕様の概要を伝えられるレベル**
- **自社の情報資産に関連する脅威に関する情報を識別できるレベル**

Ⅴ．補記事項

セキュリティ管理者として、外部の知識の支援を受けることが前提

【スキルレベルテーブルサンプル】

レベル０：　知識がない、または、経験がない
レベル１：　知識項目の概要を理解している水準である。業務を通じて、より詳細な技術的な内容を習得することができる。
レベル２：　習得した知識項目を、業務において他の指導・援助を得つつ実践できる水準である。知識項目の技術的な内容について具体的に事例を示し説明することができる。
レベル３：　知識を活用して、業務を自力で実践できる水準にある。実務を通じた数多くの実践経験に基づくノウハウを持っている。

大分類	中分類	レベル
情報セキュリティマネジメント	マネジメント技術	1
	リスク分析技術	1
	情報セキュリティポリシー	2
	情報セキュリティ監査	1
	関連知識	1
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	1
	ネットワークアクセスコントロール	1
	VPN	1
	無線 LAN	1
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	2
	Web サーバのセキュリティ対策	2
	Web サーバの運用	2
	Web アプリケーション設計	1
	Web ブラウザのセキュリティ	2
	Web 関連プロトコルの基礎知識	1
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	2
	メールサーバのセキュリティ対策	2
	メールクライアントのセキュリティ	2
	メールサーバの運用	2
アプリケーションセキュリティ【DNS】	DNS サーバに対する脅威	1
	DNS サーバセキュリティ対策と構成	1
	DNS サーバの運用	2
OS セキュリティ【Unix】	ログ管理	2
	パッチ適用管理	2
	サービスの管理	1
	ファイルシステム管理	2
	アカウント管理	3
OS セキュリティ【Windows】	構成･設定管理	2
	パッチ適用管理	2
	監査	1
	ログ管理	2
	プロセス管理	1
	サービス管理	1
	ファイルシステム管理	2
	アカウント管理	3
	ネットワーク保護	2
OS セキュリティ【TrustedOS】	強制アクセス制御の概念（MAC	0
ファイアーウォール	ファイアーウォールの導入･運用	2
	NAT	1
	ネットワークアクセスコントロール	1
侵入検知	侵入検知システムの導入･運用	1

大分類	中分類	レベル
	侵入検知システムの機能	0
	検出アルゴリズム	0
	検出方法	0
	侵入検知システム	1
ウィルス	管理体制	2
	感染後のポリシー	2
	予防ポリシー	2
	発病	2
	検出方法と駆除	1
	感染	2
	種類	1
セキュアプログラミング技法	Web アプリケーション	0
	DB	0
	アプリケーション全般	0
	XML	0
	PHP	0
	JAVA	0
	Perl	0
	VB/ASP	0
	C/C++	0
	UNIX	0
	コンパイラ・仮想マシン	0
	Windows	0
セキュリティ運用	定常運用時のセキュリティ確保	2
	異常時対応	2
	運用関連情報（脆弱性情報・対策情報・攻撃情報・被害情報）	2
セキュリティプロトコル	アプリケーション層	1
	トランスポート層	1
	ネットワーク層	0
	データリンク層	0
認証	パスワード認証	2
	バイオメトリック認証	1
	認証デバイス	1
	認証プロトコル	0
	Web 認証	1
	システム認証	1
	シングルサインオン	1
PKI	PKI の利用	1
	証明書と認証	1
	証明書失効	1
	信頼モデル	1
	契約モデル	0
	記述とデータ方式	0
	規格	0
	公開リポジトリ	0
	認証局の構築と運用	1
	法的枠組み	0
	PKI の要素技術	0

大分類	中分類	レベル
	PKI が提供するサービス	1
暗号	公開鍵暗号	1
	共通鍵暗号	1
	ハッシュ関数	1
	暗号用乱数	0
	鍵管理	0
	ゼロ知識証明	0
	その他の暗号方式	0
	暗号解読･強度評価	0
電子署名	電子署名の利用	1
	電子署名の要素技術	0
	電子署名の仕組み	0
	電子署名の利点	1
不正アクセス手法	遠隔不正侵入･操作	1
	サービスの停止	1
	盗聴行為	1
	偵察行為	1
	情報収集	1
	古典的不正アクセス技法	1
法令･規格	基準･指針･ガイドライン等	1
	法令	1
	国際標準規格	0
	国際ガイドライン	0

３．４ スキルモデルの活用方法に関する考察

本調査研究の一環として実施した、学識者ならびに企業担当者へのヒアリング調査、情報セキュリティに関する業務にたずさわる方へのグループインタビューを通じて、スキルモデルに関する意見を収集した（「５．有識者ヒアリングとグループインタビューによる調査結果の整理」参照）。

上記のような活動を通して得られた知見をもとに、スキルモデルの活用方法及びその課題に関する考察として、以下の 2 つの観点から整理を行った。

（１）スキルモデルの利用場面

スキルモデルを実際の企業の現場での利用方法として、以下のようなものが考えられる。

（ａ）採用

特に、中途の経験者を採用しようとする際に、仕事内容や権限、責任範囲などを記述する職務要件書（Job Description）の能力要件の定義に活用することが考えられる。情報セキュリティの分野では、職務経験のみならず技術知識の習得度合いが重要となる。また、担当する業務によっても必要なる技術知識の分野や内容、そのレベルは異なる。応募者側からも自身のレベルを提出してもらうことで、採用側と応募側のコミュニケーションツールとして機能することが期待される。

（ｂ）人材育成

スキルモデルを利用して、人材育成におけるスキル獲得のゴールを設定することが考えられる。スキルモデルは個別の業務に対応して設定されるため、業務ごと、あるいは、関連する複数の業務を単位に人材育成計画を策定することが可能になる。

また、レベル診断テストなどと組み合わせることで、その人が現在どの分野（スキルマップの大分類）の技術知識に強いか弱いかが分かり、業務に必要とされる知識のレベルとの差分をみることで、どこを重点的に学習すれば良いかの方向付けを与えることができる。

（ｃ）チーム編成／要員計画

一般にそれぞれの業務は複数の人からなるチームを単位として遂行される場合が多い。プロジェクトチームを編成する際の要員計画において、スキルモデルを活用することが考えられる。個々人のスキルのレベルを重ね合わせたものがチームとしてのレベルと考えれば、どのような人材がどれくらい必要になるかを見積もることができるようになる。

（ｄ）能力評価

人事考課のうち、その人が業務を通じて、現在どの程度のスキルを身に付けているかを評価する能力効果の指標の一つとして、スキルモデルを活用するケースもありえ

る。「（ａ）採用」と同様に、評価者と従業員のコミュニケーションを支援することが期待される。

ただし、実際の人事考課は、能力の評価だけではなく、所定の期間でどの程度の成果を達成したかを評価する業績の評価と組み合わせて行われることが一般的であり、それぞれにどの程度のウェイトを置くかが検討課題になる。

（ｅ）調達

地方自治体や民間企業などが、コンサルタント、エンジニア等を調達する際の調達要件書における対応要員に求められる技術レベルの定義に活用することが考えられる。

（2）スキルモデルのカスタマイズについて

「3．3 スキルモデルサンプル」では、情報セキュリティに関する業務として 5 つをサンプルとして取り上げ、スキルモデルの例を示した。実際の企業の現場で使用しようとする際には、より多様な業務が存在しており、それぞれの要求に応じてスキルモデルが設定されるものと考えられる。その際、スキルモデルでは、その記載事項やレベル定義を自由にカスタマイズして使用することを想定している。

主なカスタマイズのポイントして、以下のようなものがあるだろう。

（ａ）大分類／中分類

スキルモデルの利用者は、必要な大分類あるいは中分類のみを用いればよい。例えば、情報システムのユーザ企業のセキュリティ運用管理担当者は、大分類「セキュアプログラミング技法」のレベル定義は必要ではないかもしれない。

また、「2．3．1 2003 年度版スキルマップの概要（2）スキルマップの構成について」に示したように、一部の大分類は「サブ大分類」で中分類をグループ化している。カスタマイズの際は、必要となるサブ大分類のみにレベルを設定することも考えられる。例えば、大分類「OS セキュリティ」には、サブ大分類「Unix」「Windows」「Trusted OS」が含まれているが、Unix 系の技術者であれば、サブ大分類「Unix」のみのレベルを定義し、その他の項目についてはスキルレベルテーブルから削除しても良い。

（ｂ）レベル定義

本調査研究では、レベル定義の基本タイプとして表 3-1 に示すものを設定した。利用者のニーズに応じて、レベル定義の内容やレベル数（3 段階、5 段階、あるいは、20 点満点など）をカスタマイズして使用することが考えられる。

本調査研究のサンプルでは、すべての大分類で表 3-1 の同じレベル定義を用いているが、大分類に応じて別々のレベル定義を設定する方が、より実際の運用のイメージに近いかもしれない。

４．情報セキュリティに関するスキルレベルチェックリストの策定

「情報セキュリティのためのスキルマップ」をベースに、技術者やエンジニアが、情報セキュリティに関する基本的な知識について、自己のレベルをセルフチェックできる問題と解答のリストである「スキルレベルチェックテスト」の策定について検討を行った。

本章では、スキルレベルチェックテストの策定に関して、以下の項目について述べる。

1. スキルレベルチェックテストの作成について
2. スキルレベルチェックテストのコンセプト
3. スキルレベルチェックテストサンプル
4. スキルレベルチェックテストの利用法に関する考察

４．１ スキルレベルチェックテストの作成について

スキルレベルチェックテストを作成するに当たっての前提条件について、以下に整理する。

４．１．１ スキルレベルチェックテスト作成の目的

スキルレベルチェックテストとは、技術者やエンジニアが情報セキュリティに関する基本的な知識について、以下の各種の用途についての評価を行うための問題と解答の組合せのことを指す。

（1）自己のレベルについてのセルフチェック

自分の現在の知識の習得状況を、自己評価することに相当する。

（2）他者評価

上司や人事担当者などが、評価対象スキルについての被評価者における知識習得の達成度を評価する場合に相当する。

（3）第三者評価

公的資格の認定試験などにおいて、特定の対象範囲についての知識の習得状況を判定することに相当する。

４．１．２ 本調査研究における到達目標

スキルレベルチェックテストの妥当性を評価するためには、実際に多様な被験者を対象としてテスト問題を用いた試行を実施するのが理想的である。ただし、本調査研究においてはスキルマップの改良とスキルモデルの構築の各作業を同様に重視している。本調査研究においては本格的なテストプールの構築に向けて、テストサンプル（問題文、選択肢、正答、解説、等）の作成を行うものとする。

４．２ スキルレベルチェックテストのコンセプト

スキルレベルチェックテストの検討にあたり、その問題形式、レベル、難易度、問題の性質などの視点からそのあり方の考察を行う。

４．２．１ スキルレベルチェックテストの問題形式

テストの問題形式としては、一般に以下の方法が利用されている。

（１）多岐選択式

2 つ以上の選択肢の中から、適切な解を表現しているものを選択する方法である。問題文が正しいかどうかの正誤（○×）を選択する方法もこの一種とみなすことができる。一般に、選択肢が多いほどいわゆる「まぐれ当たり」を防ぐことが可能となり、難易度も高まる傾向にある。また、正答以外の選択肢を明らかな誤答とするのではなく、問題文で与えられた条件を満たす複数の選択肢の中から、問題文の状況に応じて最も適切なものを選択させることにより、問題の難易度を高めることもできる。

多岐選択式の最大の長所は、採点が容易であることといえる。マークシート化により、大量の回答を高速に処理することができる。

（２）記述式

単語レベルの語句や数値を記入させるものから、50～100 字程度の文章で回答させるものまでを含む。あいまいな理解では完全な正解を記述することができないため、知識として実際に身についているかどうかを確かめる能力の点で多岐選択式より優れているが、採点に人手を要する点が問題になる。

（３）論述式

200～4000 字程度で、問題として与えられた課題についての自身の論考を記述する方法である。この方式の場合、模範解答との比較で採点することはできず、採点者にも問題の対象となる分野についての相応のスキルや知識が要求される。一般に高度なスキルを評価するために利用されるが、採点に膨大なコストを要するため、（１）の方式と併用して採点対象数を予め絞るなどの工夫が用いられることも多い。

こうした 3 種類の方法の特徴を比較すると、スキルレベルチェックの方法としては、セキュリティを対象としていることが選定の条件にはならないとみなすことができる。そこで、基本的な知識を問う問題から高度なものまでを幅広くカバーすることへのニーズと、テストの実施運用上の容易性とを考慮し、今回のテスト方法は多岐選択式をベースに検討するものとする。

４．２．２ スキルレベルチェックテストにおける『レベル』の種類

スキルレベルチェックテストのレベルについては、以下の３種類の『レベル』が想定される。

（1）テスト問題のレベル（難易度）：

テスト問題そのものに定義された問題の難しさを表象する。

（2）スキルモデルのレベル：

業務に紐づけられたレベル定義を表象する。

（3）人のレベル（成績）：

テストを行った結果の成績を表象する。

こうした３種類の観点の相互関係を整理すると、次図のようになる。

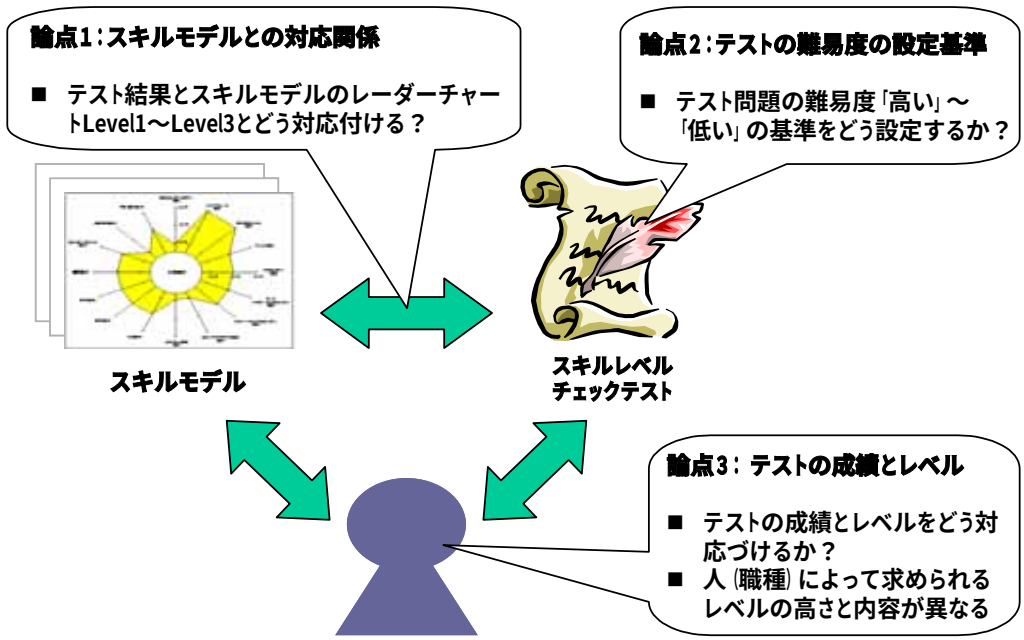


図 4-1　スキルレベルチェックリストのレベルに関する３つの論点

４．２．３ スキルレベルチェックテストにおける難易度の設定基準

スキルレベルチェックテストを構成する問題について、その難易度の設定基準の考え方を整理すると、次表のようになる。

表 4-1　スキルレベルチェックテストの難易度の設定基準例

レベルの種類	備考	難易度の基準例
考え方１： 基本問題／応用問題	■ 分類基準の設定を比較的簡単に行える。昨年度調査研究の知識区分の考え方に近い。 ■ スキルマップ／スキルモデルのレベル（3 段階）との整合について検討する必要がある。	■ 基本：知識を問う問題 ■ 応用：考え方を問う問題
考え方２： 難易度Ａランク～Ｃランク	■ スキルマップ／スキルモデルとの紐づけが容易。 ■ 客観的な設定基準が必要となるが、現実的には主観で決めざるを得ないケースもある。	■ ランク A：基礎 ■ ランク B：応用 ■ ランク C：発展
考え方３： ベータテストによる方法	■ 最も客観性の高いレベル定義を与えることができる。 ■ 今回の調査研究の範囲内では実施が困難。	―

今回の調査研究においては実際のテストを実施することが困難であるため、「考え方３」を選択することは不可能である。そこでレーダーチャートのレベル定義、ならびに問題文の作成の指針設定の容易さを考慮すると、今回検討するスキルレベルチェックテストは、「考え方２」に基づいて作成するのが最も適切と考えられる。

４．２．４ スキルレベルチェックテストにおける問題文のタイプの分類

難易度とは別に、スキルレベルチェックテストを構成する問題文はその構成から 3 種類に分類される。これをスキルレベルチェックテストのタイプ 1～3 と呼び、それぞれ以下のように定義する。

（1）タイプ１：言葉を問う（穴を埋める）問題

解答の選択肢が、「SPAM」、「DES」などの単語の形で表現されるものがこのタイプに該当する。一般的に、その単語についての知識があるかどうかの評価のための問題となることが多いが、非常に専門的な用語を問う問題や、例外を選ぶ問題などは高度ないし全体的な知識が必要となるため、難易度の低さと相関するとは限らない。

（2）タイプ２：意味を問う問題

解答の選択肢が、文章の形で表現されるものがこのタイプに該当する。後述するタイプ３との相違点として、「公開鍵暗号の特徴について、文章の選択肢から適切なものを選べ」のように、問題文が比較的短く、1～2 文で表現される。一般論としての知識を問う問題が中心となる。

（3）タイプ３：プロセスを問う問題

問題文が比較的長く、その文中に解答を選択する際の条件としての状況設定や、問題内容に至るまでのプロセスが記述され、こうした条件の下での正解を求めるものがこのタイプに該当する。タイプ２の問題が一般論を問うのに対して、タイプ３の問題は状況判断を求める問題が中心となる。

さらにタイプ３の問題の特徴として、明らかな誤答ばかりの中から唯一の正解を選ぶのではなく、50%や 80%の正解が並ぶ中から「最も適切なもの」として 100%の正解を選ぶ問題を作成可能であることが挙げられる。こうした問題は、単に細かい専門的知識を問うことで問題の難易度を高めるのではなく、問題文に設定された状況やプロセスを正確に理解し、判断できるかを難易度の根拠にできるため、タイプ１や２とは異なる形での難度の高い問題を作成するために有用である。

４．２．５ スキルマップ／スキルモデルとの対応関係

スキルマップ、スキルモデルとこのスキルレベルチェックテストとの対応の考え方について、それぞれ以下に整理する。

４．２．５．１ スキルマップとの対応関係

スキルレベルチェックテストとスキルマップとの対応関係は、スキルマップに記載された項目を対象にテスト問題が作成されることにある。スキルマップに基づくテスト問題の種類としては、以下の 2 種類が想定される。

（1）主に中分類を対象として問題文を作成

小分類または備考に関する内容が選択肢や解答になる。不適切な選択肢を選ぶような問題の場合、中分類全体の幅広い知識を問うものとなる。

（2）主に小分類を対象として問題文を作成

備考に関する内容や備考の記述から派生する内容が選択肢や解答になる。（1）と比較して、個別的な項目についての問題が中心となる。

４．２．５．２ スキルモデルとの対応関係

スキルレベルチェックテストとスキルモデルとの関係では、スキルレベルにおいて設定されるレベルとテストの難易度をどう対応づけるべきかが課題となる。この対応付けの方法として、以下の３種類の考え方が想定される。

（考え方１）業務ごとに質問文と難易度を設定し、スキルモデルのレベルと紐づける

（考え方２）業務に共通的な知識項目として質問文と難易度を設定し、スキルモデルのレベルと紐づける

（考え方３）業務に共通的な知識項目として質問文と難易度を設定し、スキルモデルのレベルとは独立にする

このうち、「考え方１」はスキルモデルにおけるレベルの測定方法としてスキルレベルチェックテストを利用できて理想的であるが、全てのモデルに問題を用意することは現実的ではない。実際上は、「考え方２」を基本とせざるを得ないが、当面は紐づけるための方法論が確立されていないこともあり、「考え方３」の適用を検討するのが妥当と考えられる。この場合、スキルモデルのレベルとの関係は別途検討議論が必要となる。

４．３ スキルレベルチェックテストサンプル

スキルレベルチェックテストの実現に向けたアプローチとして、テストのサンプル（問題文と解答）を作成する。

４．３．１ サンプルの作成要領

スキルレベルチェックテストに用いる問題のサンプルは、以下の要領で作成するものとする。

（１）サンプルテストの問題数

問題の多様性を確保する観点から、16 種類の大分類毎に各 10 問ずつ作成し、合計 160 問とする。

（２）サンプルテストの形式

サンプルテストの形式は、４つの選択肢からひとつだけを選ぶ「４問択一式」とし、タイプの構成は下記のように各レベルの問題を揃えるものとする。ただし、タイプ 3 の問題については、要素技術に関する大分類を中心に対象とする知識の特徴上、状況設定などが行いにくいものもあるため、こうした大分類においては該当数がゼロでも差し支えないものとしている。

- タイプ１（言葉を問う問題例）：3～5 問
- タイプ２（意味を問う問題例）：3～5 問
- タイプ３（プロセスを問う問題例）：0～2 問

（３）サンプルテストの内容

サンプルテストの問題とすべき内容の選択基準として、以下を示している。

- 第 2 章で作成した「2003 年度版スキルマップβ版」の知識項目（大分類、中分類、小分類、備考）をベースにする。
- テスト問題を作成する単位（ターゲット）は、スキルマップの中分類または小分類とする。中分類／小分類のいずれをターゲットにすれば良いかについては、特に問わないものとする。
- 選択肢／解答として、小分類、備考の記載事項、スキルマップの記載にある以外のもの、いずれを用いても構わないものとする。

（4）サンプルテストの作成の担当者

サンプルテストの作成は、スキルマップ WG メンバーが担当した。このとき、各担当者には問題の作成にあたって第三者等の権利を侵害しないことの周知を行っている。

４．３．２ スキルレベルチェックテストのサンプル問題

以下、サンプル問題の例を、各タイプにつき 2 種類ずつ示す。なお、本調査研究においてスキルレベルチェックテストの問題として大分類毎に作成した成果は、「７．２ スキルレベルチェックテストサンプル」において示すものとする。

（1）タイプ1（言葉を問う問題）の例

表 4-2　サンプル問題の例（タイプ１・その１）

大分類	セキュリティプロトコル
中分類／小分類 (ターゲット)	［中分類］アプリケーション層
タイプ	1
問題文	次のプロトコルのうち、VPN (Virtual Private Network)で使用されないものはどれか。
選択肢（４問択一）	ア．SSL イ．S/MIME ウ．L2TP エ．SOCKS
解答	イ
備考	

表 4-3　サンプル問題の例（タイプ１・その２）

大分類	暗号
中分類／小分類 (ターゲット)	［中分類］鍵管理
タイプ	1
問題文	鍵管理方式として安全性の証明されている方式はどれか。
選択肢（４問択一）	ア．鍵生成方式 イ．鍵共有方式 ウ．Shamir 閾値方式 エ．鍵管理サーバ方式
解答	ウ
備考	

（2）タイプ2（意味を問う問題）の例

表 4-4　サンプル問題の例（タイプ2・その1）

大分類	OS セキュリティ【Unix】
中分類／小分類 (ターゲット)	［中分類］サービスの管理 ［小分類］一般ユーザでのデーモンの起動
タイプ	2
問題文	サーバで起動するサービスの実行権限について適切なものを選択せよ。
選択肢（4問択一）	ア．インターネットから公開WWWサーバへの不正なアクセスを防止するために設置する。 イ．一般社員による不正アクセスや誤用を防ぐため、社内で機密性の高い情報を処理するサーバやセグメントを分離する目的で設置する。 ウ．組織のセキュリティポリシーに従って、社内から利用できるインターネット上のサービスを制限するために設置する。 エ．インターネット経由でのコンピュータウィルスの感染を防ぐために設置する。
解答	ウ
備考	

表 4-5　サンプル問題の例（タイプ2・その2）

大分類	ファイアーウォール
中分類／小分類 (ターゲット)	［中分類］ファイアーウォールの導入・運用
タイプ	2
問題文	ファイアーウォールの設置目的として最も適切でないものはどれか。
選択肢（4問択一）	ア．インターネットから公開WWWサーバへの不正なアクセスを防止するために設置する。 イ．一般社員による不正アクセスや誤用を防ぐため、社内で機密性の高い情報を処理するサーバやセグメントを分離する目的で設置する。 ウ．組織のセキュリティポリシーに従って、社内から利用できるインターネット上のサービスを制限するために設置する。 エ．インターネット経由でのコンピュータウィルスの感染を防ぐために設置する。
解答	エ
備考	

（3）タイプ3（プロセスを問う問題）の例

表 4-6　サンプル問題の例（タイプ3・その1）

大分類	情報セキュリティマネジメント
中分類／小分類(ターゲット)	［中分類］情報セキュリティポリシー ［小分類］基本方針
タイプ	3
問題文	ある企業において、情報セキュリティの基本文書を2年前に作成した。その後、企業のおかれている環境、ビジネスの内容も変化したため、見直しを進めている。このような場合、次の項で最も適切なものを選択せよ。
選択肢（4問択一）	ア．新社長が就任し、経営戦略等も新しくなり、変更されたので、「情報セキュリティの基本文書」をもう一度新しい視点で見直してみる。 イ．最近、「情報セキュリティの基本文書」に関して、他社の良い例の発表会があり参加した。大変良いので、自社のものを、全面変更することを考えている。 ウ．会社の新しい施策は出されているものの、まだ「情報セキュリティの基本文書」の作成から2年しか経っておらず、当面はこのままにすることにした。 エ．「情報セキュリティの基本文書」を見直した結果、社長に承認を頂いた。実際は、当初の予定より、少ない変更であるので、各部署に正式に変更連絡を行うと、そのための作業が多く、効率が悪いことから、今回は各部署への連絡は省こうと考えている。
解答	ア．
備考	経営戦略が変更になったら、「情報セキュリティの基本文書」をもう一度見直すことは、必須である。かつ、変更した場合は、各部署に伝達することも必要である。

表 4-7　サンプル問題の例（タイプ３・その２）

大分類	セキュリティ運用
中分類／小分類(ターゲット)	［中分類］セキュリティホール対策 ［小分類］パッチの適用可否の判断基準（目的、対象）
タイプ	3
問題文	A社は一般消費者向けオンラインショップを自前のサーバで運用している。あるとき、オンラインショップ用サーバで用いているOSのベンダから、OSのセキュリティホール対策のパッチの提供のアナウンスと、そのセキュリティホールを悪用したワームの発生のアナウンスが、ほぼ同時に伝えられた。A社の運用ルールでは、パッチを提供する際には、いきなり実運用環境に適用するのではなく、全く同じ構成からなるテスト環境に適用して悪影響のないことを確認した上で実運用環境に適用することになっているが、テスト環境での確認には通常2～3日かかる。なお、今回のセキュリティホールの対象は、このオンラインショップ用サーバで現在使用していないサービスを対象としたものであり、OSベンダの提供する情報には、サービスが不要な場合は停止することでワーム感染を予防できる旨が書かれている。こうした状況において、A社がとるべき最も適切な対策は次のうちのどれか。
選択肢（４問択一）	ア．直ちにオンラインショップ用サーバを停止させる。テスト環境での悪影響なしの確認が終わった後に実運用環境にもパッチを適用した上で、サーバを再起動し、オンラインショップを再開する。 イ．今回のワームは現在使用していないサービスを対象にしているので、ワームが用いるサービスの停止を確認した上でパッチは適用せず、そのまま運用を続ける。 ウ．ワームが用いるサービスの停止を確認し、情報収集と異常監視の警戒体制を強化した上でオンラインショップの運用を継続する。テスト環境での悪影響なしの確認が終わった後にパッチを適用するが、当分の間は警戒態勢を維持する。 エ．ワームが発生したのは緊急事態であるので、テスト環境での確認なしに直ちに実運用環境にパッチを適用し、適用後のサーバでオンラインショップを運用する。
解答	ウ
備考	ワームについては、亜種の発生を考慮する必要があることを前提とした問題。

４．４ スキルレベルチェックテストの利用法に関する考察

スキルレベルチェックテストに関する今後の利用法のあり方について、実際のレベル評価に向けた応用の可能性と課題についての分析を行う。

４．４．１ テスト問題を用いたスキルレベルのチェック方法

「４．３ スキルレベルチェックテストサンプル」で作成したサンプルテスト問題をもとに、自己評価と第三者評価のそれぞれの立場でスキルレベルをチェックするための要件について検討する。

（１）スキルレベルチェックテストを自己評価に使用する場合

分野別の理解度の把握を中心とする用途であれば、各テスト問題とスキルマップとの対応関係に関する情報を整理することにより、スキルレベルチェックテストにおける正答率を用いた分野別の理解度の評価が可能になる。この場合はテスト問題の難易度を厳密に評価する必要性は低い。

（２）スキルレベルチェックテストを第三者による評価に使用する場合

（１）と対照的に、資格認定試験のように正解を得点に換算し、一定の設定値を超えた得点を得た場合を合格とするようなケースでは、難易度や出題のバランスにおける厳密性へのニーズは高くなる。既存の資格認定制度では、モニタによる試行を行うことなどにより検証されているが、スキルマップの対象としている知識の一部には関係する専門家ないし技術者の数が少ないものもあり、統計的な信頼性を確保することが難しいケースが生じる可能性もある。

なお、同一の試験の受験者間で得点の序列を作るような場合は、厳密性へのニーズは（１）と（２）の中間的な位置付けになる。

４．４．２ スキルレベルチェックテストの利用における課題

スキルレベルチェックテストを実際に利用していくにあたって考慮すべき課題について、以下に整理する。

（１）ベータテストの実施

現在のサンプル問題はその妥当性や効果についての検証を行っていないため、正解として設定されているものが誤っている可能性まで考慮すると、テストで得られた結果に客観的な意味を見出すことはまだできない。そこで、サンプル問題を発展させたベータテストを実施することにより、テストとしての機能の検証を行う必要がある。このときの、ベータテストの要件については、自己評価用、第三者評価用などのテストの用途により相当に異なることになるため、こうした用途を明確化した上で仕様を詰めていく必要がある。

（2）スキルレベルの定義のあり方

「4．2．5．2 スキルモデルとの対応関係」で議論したように、スキルレベルチェックテストとスキルモデルとのレベルの対応付けに関しては、テスト問題から直接的にスキルモデルにおけるレベルの評価が行えるものと、困難なものに分かれる。今後の利用に際しては、こうした困難なものについて、どのようにスキルモデルにおけるレベルの測定を行うかの方法論を明らかにしていく必要がある。

（3）テスト問題の品質の確保

スキルレベルチェックテストで用いるテスト問題の品質を今後も確保していくための方法について、そのアップデートの方法を中心に議論する。

（a）テストプールのアップデートの方法

テスト問題を更新、追加していく際にその品質を確保するために、以下の項目について検討する必要がある。

- テスト問題作成のガイドラインの作成
  スキルマップとの対応、スキルモデルとの関係における共通部分の定義、解釈によって正解が異なることのないようにするための条件設定など、問題作成者が留意すべき事項をガイドラインとしてまとめることが望ましい。
- テスト問題に対する評価手法の作成
  テスト問題の難易度、対象とする知識の種類（基本的なもの、専門的なもの、状況判断を求めるもの、等）を評価するための手段を提供すると、今後のテスト問題の選択、作成時に有用である。手段としては、評価すべき項目をチェックリスト化したものなどが想定される。

（b）社会環境の変化や情報セキュリティ技術の進展への対応の方法

スキルレベルチェックテストを社会環境の変化や情報セキュリティ技術の進展に適ったものとして維持するため、（a）とは別に継続的なアップデートは必要不可欠といえる。こうした観点からアップデートを行う際に留意すべき事項としては、以下が挙げられる。

- 新たな技術、サービスの普及度
  テストの対象とできるほど、対象とする技術、サービスが普及、普遍的になっているかどうかを評価する。
- セキュリティ確保の視点からの項目の網羅性
  アップデートの時点でセキュリティを確保するために知っておくべき項目が、テスト問題内に網羅されているかどうかを評価する。

アップデートの頻度としては、スキルマップのアップデートと同じタイミング（2～3 年）で全体の見直しを図ることが適切と考えられるが、上記第 2 項にあるように情報セキュリティのそれまでの常識を覆すような新たな脅威や技術が登場したような場合は、こうした更新頻度に関わらず見直しを図る必要もあるといえる。

４．４．３ スキルレベルチェックテストの活用場面

スキルレベルチェックテストの活用場面として、今後想定されるものを有識者ヒアリング等での指摘を踏まえ、以下に整理する。

（1）人材採用における利用

採用時の職務能力判定の際、情報セキュリティに関する技術知識の習得状況の評価手段として、スキルレベルチェックテストを利用することが考えられる。情報セキュリティに関するスキルとしては技術知識以外の要素の寄与度が多いことが有識者ヒアリングで指摘されており、実際に評価に利用する場合は、本テスト以外の方法と併用することを検討すべきといえる。

（2）能力評価手段としての利用

能力評価の観点の違いから、次の 2 種類に分けて整理する。

（a）自己評価

有識者ヒアリングにおいて、簡便なセルフチェックテストへのニーズは存在することが指摘されている。このセルフチェックテストの手段として、スキルレベルチェックテストは有用と考えられる。自己評価のあり方としては、「４．４．１ テスト問題を用いたスキルレベルのチェック方法（１）スキルレベルチェックテストを自己評価に使用する場合」における検討を踏まえ、スキルマップ上の知識項目や分類毎の正答率などをもとに、評価のための指標を整備していくことが考えられる。

（b）他者評価

上司やプロジェクトリーダーによる構成員のスキル評価の手段や、人事評価上のランクを設定する際の要件としての活用が期待される。「４．４．１ テスト問題を用いたスキルレベルのチェック方法（２）スキルレベルチェックテストを第三者による評価に使用する場合」に示すように、対象者全員で同じ試験を受験するような場合は、スキルレベルチェックテストの成績をそのまま利用しても問題はないが、得点や正答率などの絶対値で評価を行う場合は、テストの難易度について客観性を高めるための配慮が必要となる。

（3）資格制度、能力認定制度としての利用

前述の通り、第三者的な評価認定制度への利用に際しては、テストの難易度の評価方法等を別途確立する必要があり、現行のスキルレベルチェックテストの枠組みだけでは十分ではない。個々の制度との対応では、以下の点が考慮される。

- 資格制度

  スキルモデルとの組み合わせが考えられる。
- 能力認定

スキルマップにおける 16 分類の特性を活かすことが期待される。

（4）教育カリキュラムにおける利用

教育機関による教育ならびに事業者内教育において、カリキュラムにスキルマップに対応する教育内容を含む場合、該当項目についての理解度のテストにこのスキルレベルチェックテストを用いることで、別途テスト問題を用意する手間を省くことができる。

（5）外部発注時の利用

業務を外部発注する際に、発注先企業に対して担当する技術者の要件を指定する必要がある場合など、目安として提供することができると考えられる。この場合も、上記（3）と同様スキルモデルとの組み合わせが想定される。

５．有識者ヒアリングとグループインタビューによる調査結果の整理

前述の「２.「情報セキュリティのためのスキルマップ」の構築」ならびに「３．情報セキュリティに関する「スキルモデル」の策定」における分析の手法として本調査研究において実施した、有識者ヒアリング調査とグループインタビュー調査について、ここにその概要と得られた成果を整理する。

1. 有識者ヒアリング調査
2. グループインタビュー調査

５．１ 有識者ヒアリング調査

ヒアリング調査については 2002 年度調査研究においても実施しているが、本調査研究ではスキルマップのより実践的な活用に視点を置き、スキルマップの活用を担う立場の関係者へのヒアリングを中心として実施している。

５．１．１ 有識者ヒアリング調査の概要

今回の調査研究における有識者ヒアリング調査の位置付けと、位置付けに基づくヒアリング先の選択の結果について、以下に概要を示す。

（１）目的

以下の２点を主たる目的とする。

（ａ）スキルマップのアップデート

項目や構成のへのアドバイスやレビューを得る。

（ｂ）スキルモデルの策定

現状の情報セキュリティに関する業務やタスクの遂行に求められるスキルを明らかにする。

（２）対象

以下の２種類の有識者を主たる対象とする。

（ａ）情報セキュリティ分野の学識者

（ｂ）情報セキュリティに関連する製品またはサービス等を提供する企業もしくは情報セキュリティに関連する活動を行っている団体

（３）ヒアリング先

上記（２）の各項目について、（ａ）（ｂ）を各 4 件選定した。ヒアリング先一覧を次

表に示す。なお、なお事業者ヒアリングについては、後述するグループインタビューの参加者の所属する企業と異なる業種を中心に選定を行っている。

表 5-1　有識者ヒアリングの概要（順序は実施順）

分類	ヒアリング先
学識者	東京電機大学工学部情報メディア学科・佐々木良一教授
	中央大学研究開発機構・内田勝也助教授
	東京大学生産技術研究所・今井秀樹教授、古原和邦助手
	国士舘大学情報科学センター・杉野隆教授
事業者	システムインテグレータ、教育サービス事業者
	ソフトウェアベンダ日本法人
	システムベンダ、システムインテグレータ
	電気通信事業者

（4）ヒアリング調査に用いたスキルマップ

有識者ヒアリングにおいてレビューの対象としたのは、2003 年度版スキルマップのベータ版である。これは、2002 年度調査研究の成果をもとに「2．2．1 2002 年度版スキルマップの課題」にて示したワーキンググループで指摘された事項を中心に反映を行ったものに相当する。

5．1．2 ヒアリング項目

ヒアリング項目として想定した事項を以下に示す。なお、実際の質問項目は、ヒアリング先の特徴に応じ、適宜取捨選択の上実施している。

（1）スキルマップについてのレビュー

（a）スキルマップの妥当性、改良すべき点

- スキルマップ全体（バランス、漏れ）
- ヒアリング対応者の専門分野、担当分野におけるスキルマップ内容の妥当性
- その他スキルマップ全体で気づいた事項

（b）スキルマップを用いたプロフェッショナルのスキル評価のありかたについて

- 高いスキル、最低限必要なスキルに求められる要件は何か
- スキルレベル（3 段階程度）の判断は何を基準にすべきか
  （知識の幅広さ/理解度、専門的知識の多少、知識の活用/応用/実践能力、他）
- スキルのチェックの視点でみた項目のバランス

（c）スキルマップと他の評価制度との対応・比較

- ベンダ資格、情報処理試験、米国資格（CISSP 他）

・ ISMS 審査員制度、システム監査人制度、ITSS
・ その他

（2）スキルモデルの考え方

（a）スキルモデルの設定について

・ スキルモデルとして想定すべき、セキュリティに関わる職種・業務にはどのようなものがあるか（ご対応者の組織を例にした場合）
・ スキルモデルの構成要素とすべき事項についてのご意見（スキルマップにおける大分類とレベル、セキュリティ以外の分野の知識、対象分野での経験、他）

（b）スキルモデルについての論点

・ グループ全体でみたスキルと個人単位のスキルの関係（個人毎で評価する意味、グループ単位での評価の考え方）
・ スキルと経験年数、キャリアパス、資格保有等との関係
・ コンピテンシーの観点からみたスキルの要件（優秀とされる技術者は、セキュリティスキルとしてどのような知識、資質を備えているのか）

（c）スキルモデルの利用場面

・ 自部署においてどのような活用方法が考えられるか（人材採用・公募時の利用、人材育成方策・カリキュラムへの応用、能力評価手段としての可能性、等）
・ その他自組織内、ないしセキュリティ業界全体でどのような活用が想定されるか

（3）その他

（a）本調査研究の実施内容、進め方への意見、要望
（b）今後の情報セキュリティ教育における本調査の成果物の活用方法

5．1．3 ヒアリング内容の要旨

ヒアリングにて指摘された内容をテーマ別に整理の上、以下に示す。

5．1．3．1 スキルマップについて

（1）スキルマップの内容に関する指摘事項

各大分類毎の指摘事項を次表に整理する。

表 5-2　スキルマップについての有識者ヒアリングにおける指摘事項の要旨

大分類（名称は調査開始時点のもの）	指摘事項
1. **情報セキュリティポリシー**	・「情報セキュリティポリシー」の関連知識として「情報セキュリティマネジメント」があるが、両者の関係は逆のほうがよい。 ・実際の現場では頻繁に例外が発生するため、その対策技術や未知の事態における緊急対策のような項目も重要。 ・リスク分析技術をどう系統立てるかも検討すべき。
2. **ネットワークインフラセキュリティ**	・WPA は認証にも使うので、「無線 LAN」の小分類は「認証・暗号化」に一本化するとよい。 ・無線 LAN のほか、ADSL の安全な設定なども重要。
3. **サーバアプリケーションセキュリティ**	・個別のクライアント／サーバシステムにおけるクライアントシステムのセキュリティについても検討すると望ましい。 ・粒度が揃っていない印象を受ける部分がある。 ・攻撃の証跡確保を行う場合の手がかりとして、NTP に関する項目がほしい。
4. OS**セキュリティ**	・「Active Directory」の機能はアカウント管理だけではないので、「統合管理」などの項目を設けてそこに入れる方が適切。 ・「セキュリティポリシー」「ソフトウェア制限ポリシー」「プロセス管理」「起動制限」などの項目の追加を検討してもよい。 ・個別の製品名を入れると数が多くなってしまうので、項目ごとに丸めてしまうのも一案。例えば、中分類「パッチ適用管理」を「修正プログラムの一斉配布」など。
5. **ファイアーウォール**	・「ファイアーウォール」を「認証」などとまとめて「アクセス制御管理」にすることも考えられるが、実用を考えると現在の構成の方が良い。 ・教育で使うことを考えると、分類が重複しているものも多い。例としては、ファイアーウォールと IDS など。
6. **侵入検知**	・「データマイニング」に関する項目を追加すべき。
7. **ウィルス**	（コメントなし）
8. **セキュアプログラミング技法**	・セキュアプログラミングを理解している人が不足しており、その育成は大きな課題。その意味で大分類「セキュアプログラミング」は重要。 ・バッファオーバーフローは、C/C++言語だけに関係するものではない。 ・中分類「アプリケーション全般」に、コンパイラセキュリティなどの項目も追加すべき。 ・「スクリプト言語」「コンパイラ言語」「バーチャルマシン言語（ないしは中間言語）」位のレベルに丸めてしまうのも一案。
9. **セキュリティ運用･監査**	・運用・監査の項目としてセキュリティの定義に相当するものが含まれている。他の大分類の要素との整合をとる必要がある。
10. **セキュリティプロトコル**	（コメントなし）
11. **認証**	・「認証」「PKI」「暗号」「電子署名」は２つ程度にまとめられる。特に、「電子認証・電子署名」など。現状は少し多い印象。 ・現在の項目はいずれも個人認証に関わるもの。サーバ間の相互認証など、システムの認証も含まれるべき。 ・「耐クローン性」（注：紙やカードが偽造できないようにすること）を追加すべき。 ・中分類「認証プロトコル」に「PAKE(Password-Authenticated Key-Exchange)」が含まれるべき。

大分類（名称は調査開始時点のもの）	指摘事項
11. **認証（続き）**	・通信相手が人間かそれとも不正を働くための自動スクリプトやプログラムかどうかを判断する技術が含まれるべき。この技術はCAPTCHA (http://www.captcha.net/ 参照)と呼ばれ、今後重要になってくる。
12. PKI	・「属性証明書」に関する項目が必要。現在は、「規格」の中に小分類「属性証明書の規格」があるのみ。 ・「Base64エンコーディング」はPKIだけで用いられるものではない。「エンコーディング」とし備考に「Base64」で良い。
13. **暗号**	・「楕円曲線上の演算を利用した暗号法」の備考「楕円RSA」は、現実の使用状況から削除が妥当。また「ペアリングを使った方式」を追加。 ・「DES」及び「AES」については、小分類「共通鍵暗号のアルゴリズム」を新たに設定し、その備考とするのが良い。公開鍵の「RSA」「ElGamal」等も同様。 ・「鍵管理」に「KPS(Key Predistribution System)」を含める。 ・「暗号技術評価プロジェクト（CRYPTREC）」の備考に「CRYPTREC『電子政府推奨暗号リスト』」が含まれているが、各暗号方式のリストがある方が良い。 ・「ゼロ知識証明」は最近の使用状況から小分類が妥当。新たに中分類「暗号プロトコル」などを設け、その中に整理すると良い。 ・「MAC(Message Authentication Code)」、「量子暗号」、「秘密分散(Secret Sharing)」に関する項目が必要。 ・複数のプロトコル等を組み合わせた時の安全性の証明である「コンポーザビリティ」の概念が広まりつつある。ただし、まだPracticalな段階に至っていない。
14. **電子署名**	・署名やPKIは暗号技術をベースに実現されるものであるが、スキルマップの実用性を考慮すると独立させるのも妥当。署名は技術的にPKIと類似部分もあるが、法的要件や使用目的が明確な点は異質。 ・項目の詳細度が不十分であり、「暗号」と同程度の整理が必要。「暗号」との整合性も考慮すべき。製品化例も多く、電子署名法や電子政府の観点からも検討すべき。 ・メッセージダイジェストは署名以外にも用いる。この分類にあるのは適切か。
15. **不正アクセス手法**	（コメントなし）
16. **法令･規格**	・「基準・指針・ガイドライン等」にある関連省庁の各ガイドラインは、どの機関が出したものかわかるようにすべき。 ・法令には、著作権法やe-Japan関連の法律を含めた方が良い。
A. **不正コピー防止と電子透かし**	・不正コピーや電子透かしで使われる技術はセキュリティ技術そのものであり、整理しておく必要はある。 ・「不正コピー・電子透かし」を大分類に入れる手もあるが、軸が多すぎると一覧性が損なわれるため現在の形で良い。 ・別表としては、情報漏洩や匿名性に踏み込んだプライバシーなども考えられる。

（2）スキルマップで不足、ないし扱い方に問題のある概念について

現在のスキルマップで扱われていない、あるいは扱われていても扱いの不十分、ないし不適切と指摘される概念を以下に列挙する。

（ａ）マネジメント

プロジェクトマネジメントができる人材の育成の視点が欠けているとの指摘がある。これは、スキルマップに限定されたことではなく、セキュリティ業界における問題点とされている。今後必要となるマネジメント関連の知識の例として、forensics など裁判対応の知識が挙げられている。

（ｂ）上流工程・構築

要件定義からテストまでのプロジェクト管理を通じてどのようにセキュリティを確保していくかの視点が抜けているとの指摘である。すなわち、セキュリティは上流工程でしっかり設計しておくべきであり、開発の時点で検討しても遅いにもかかわらず、スキルマップでは大分類「セキュアプログラミング技法」などにこうした考え方が十分反映されていないことが示されている。

また、サービスを提供する立場では単に技術知識を知っているだけではなく、サービスを最終的にどう実現するかが重要であり、個々の技術を活用してどのように設計、開発、構築を行っていくかというスキルが求められるにも関わらず、スキルマップにこうした考慮がなされていないとの指摘がなされている。

（ｃ）運用・情報管理

運用についてはすでに独立した大分類があるが、内容が限定的との指摘がある。特に、情報資源の管理についての視点が不十分とされる。

（ｄ）物理的セキュリティ

物理的なハードウェアにおける対策などの項目が不十分との指摘がなされている。

（ｅ）基礎知識

セキュリティの基礎となるべき知識は、技術者としての土台となるものであることから幅広い分野にわたって身につける必要があるが、スキルマップにおける知識が基礎から応用まで大分類別に縦割りに整理されていると、基礎を身につけるために 16 分類すべてを対象にせざるを得ない恐れが出てくる。そこで、こうした基礎知識については、コアスキルとして 16 分類から独立させるべきとの提案がなされている。教育的な視点からも、基礎を独立させて教えることの重要性が指摘されている。

基礎知識の具体的な内容としては、以下が挙げられている。

- セキュリティに携わる上での基本的な知恵に相当するものとして、セキュリティは一番弱いところから破られるといった感覚を持つこと
- 複数の技術を組み合わせると、新たな脆弱性を生み出してしまう危険があることを理解し、どのような組合せならば良いかを判断できること
- ネットワーク上で通信相手とやり取りを行う以上、必要最低限のツールを使いこなせること
- 経営や法律などの背景知識

（ｆ）倫理・モラル

倫理(Ethics)やその教育の必要性が指摘されている。法律やマネジメントと同様、別途独立させる方法と、現行の大分類「セキュリティマネジメント」に含める方法が提案されている。

（ｇ）プライバシー

セキュリティとプライバシーの関係において、セキュリティはプライバシーを保護する手段である一方、個人の匿名性を保障することがセキュリティ上の脅威を増すことに繋がる場合もあることから、プライバシーとセキュリティのうち一方を強化することでもう一方が制約される状況が今後増えていく可能性があり、重要な論点になるとの指摘がなされている。

（ｈ）知識項目間の相互関係

スキルマップに記載されている知識の間には、ある知識を習得するために別の知識が前提となるなど、依存関係にあるものが存在する。また、同様の概念が複数の項目に記載されているものもある。こうした相互関係を、マップ形式だけではなく、ツリー構造やネットワーク、関連図のような形で補完することにより、カリキュラム作成の際などで非常に有用になるとの意見が出されている。

（３）スキルマップに関するその他の指摘事項

スキルマップに関して、項目別の内容と不足している概念以外の指摘事項を以下に示す。

（ａ）スキルマップで扱うべき関連知識の範囲について

情報セキュリティ分野に属さない知識でも、セキュリティを習得するために必要となる関連知識は多い。ネットワーク技術に関するものが典型である。こうした関連知識については、必要だからといってスキルマップに加えていくと際限が無くなる恐れがあるため、境界を決めてセキュリティに限定することが提案されている。

スキルマップに盛り込むべき内容の参考として、JIPDEC が過去に作成した「高度情報処理技術者育成指針」が有用であるとの指摘がなされている。

（ｂ）その他の事項

スキルマップ全体に関わる課題として、小分類のレベル感が統一されておらず分かりづらい、ツールなどの個別の名称が分類名として適切かどうか、などの指摘がなされている。

（３）スキルモデルについて

（ａ）想定される人材像

情報セキュリティプロフェッショナルとは何か、という全体像が明確でないとの指摘がなされている。具体的には、以下のような項目が挙げられている。

- ベンダ企業とユーザ企業の両方を対象とされているにもかかわらず、ベンダ系やコンサルティング系の企業で独立して仕事ができる人材像を目指している印象があり、ユーザ系企業における業務が十分に意識されていない。このとき、ユーザ部門はレベルが低くても良いということにならず、むしろ業務も含め、より幅広い知識が必要。
- 実際の現場においては、情報セキュリティプロフェッショナルは、プロジェクトマネージャというよりもむしろセキュリティの部分を担当するスタッフであることが一般的のはず。この情報セキュリティプロフェッショナルは、情報セキュリティのシステムに対して、上流から下流までを理解し、関与しているのが望ましい。
- 例えば、暗号の研究家や専門家は、あらゆる場合の攻撃を想定して、安全性の評価を行うが、こういった能力は知識に加え経験が必要になる。暗号分野だけでなく情報セキュリティの分野全般において、同様のことが言える。

（b）職種、業務などの分類数

スキルモデルで扱う職種については、その総数は多くて 10 種類程度とし、一般的な職種に対するスタンダードをまず決めて、使う側が例外的な項目を追加すればよいとの考え方が示されている。業種の参考例として、セキュリティ分野の研究者については出身別に「暗号」「インターネット」「システム」など、企業では「構築」「運用」「セキュリティポリシー構築」「監視」などが想定されている。

一方業務については実用性を高めるためには細かく分類する必要があり、ユーザやベンダごとに必要なスキルの基準を星取表のような形で整理することで、全体で 200 分類程度にしなければ、実際の業務のモデルにはならないとの指摘がある。

また、スキルモデルにおける業務は、セキュリティに特化した業務だけでなく、ユーザ企業等における一般的な業務のなかでセキュリティが必要なものを想定すべきとの意見も出されている。

（c）レベルの考え方について

レベルの考え方については多くの意見が得られているが、内容別に整理すると以下のようになる。

- 設定方法としては、抽象的な度合いを設定する方法と、知識（知っている）と実践（することができる）でレベルを捉える方法とが考えられる。例えば、初級、中級を「知識のある／なし」、上級を「実践できる」などで組み合わせることも考えられる。また、「知っている」「使える」「語れる」のそれぞれの段階でレベルを分けることもできる。
- レベルの数については、多すぎても使いにくくなるため、3 段階程度でよい。レベルの内容については、レベル１とレベル３の内容をフィックスし、レベル

2 は相対的にレベル１とレベル３の中央になるようにすることが考えられる。

- レベル１（最低レベル）を考える際は、どこまでが基礎かが議論になるが、テキストの入門編を理解していることなどを基準にすることができる。このとき、テキストの中身が問題になるが、厳密に決めることは不可能であり、何人かのレフリー役を設定して評価すればよい。
- レベル３（最高レベル）については、分野別の個別の中身にならざるを得ないが、「１人で判断や問題解決ができること」などでおおよその合意は得られるのではないか。
- スキルモデルを活用できるようにするには、レベルに客観性を持たせることが出来るかどうかがカギになる。
- 「セキュリティポリシー」と言っても、ユーザとコンサルタントでは求められる水準が違うため、レベルの設定については、使い方を踏まえて考える必要がある。また、実務経験と知識のレベルは分けて評価することが必要ではないか。
- スキルマップの内容を備考まで説明できるのを、より高いレベルとするのがよいかどうかは答が出せない。レベルと知識項目は一体で考える必要がある。

（ｄ）グループによるスキルについて

セキュリティ業務はグループで担当することも多く、この場合個々のメンバのスキルでなく、グループとしてのスキルを評価すればよいとの考え方に関しては、一定の理解が得られているが、Business Continuity Planning などを例とした場合、その時に発生するインシデントにより必要な人材は異なるので評価は難しいのではないかとの指摘もある。

（ｅ）キャリアパスについて

IT 分野で旧来想定されてきたような、プラグラマ→SE→コンサルタントあるいは管理者といった、職階や年功によるキャリア形成に関する非合理性の指摘がなされているほか、こうした弊害を改め､エキスパートやプロフェッショナルとマネージャのキャリアパスを分離したコースが、情報セキュリティ技術者についても提供されている事例が示されている。ただし、企業におけるセキュリティ研修は必要に迫られて実施されているケースが多く、長期的な情報セキュリティプロフェッショナルの育成を考えているゆとりがないのが現状との指摘もある。

（ｆ）スキルモデルの実装方法について

業務に応じたスキルモデルの作成に際しては、業務アプリケーションごとにセキュリティの観点と対応付け、情報セキュリティプロフェッショナルとしてどの程度の知識を身に付けていれば良いか、といった観点から整理すべきとの指摘がなされている。また、スキルモデルを利用者がカスタマイズして使うことが前提であれば、スキルマップのレーダーチャートもカスタマイズ可能にすべきとの意見がある。

（4）スキルマップ・スキルモデルの活用について

スキルマップ及びスキルモデルの活用方法について、得られた意見を分野別に整理する。

（a）大学教育での活用

教育カリキュラムの設定等には使えるとの指摘がある。特に、今後増える可能性のある情報セキュリティ学科などでコアカリキュラムを検討する際に有用とされる。

スキルマップに記載された項目をベースに教育を行うことに関しては、大学教育では細かい業務内容を教えることは難しく、基礎・基盤の技術や汎用的な理論を教えることが中心にならざるを得ないとの意見が得られている。

（b）教育サービスへの活用

教育サービスを提供する立場からは、基礎／応用の知識区分があったほうがアジェンダの設定がし易いとの意見がある。これは、受講者がエンドユーザなど「サービス・システムの提供を受ける側」とベンダなど「サービス・システムを提供する側」の 2 つの立場に大別され、それぞれの目的に応じて基礎的な内容で良い場合と応用に踏み込む必要がある場合を考慮する必要があることによる。

スキルマップはセキュリティに必要となる分野が洗い出されているため、コースやカリキュラムを設定する際に相互の関連を検討しやすい点がメリットである旨の指摘が得られている。また受講者側においても、その教育を受けて習得した知識のレベルを雇用者など他者に伝える際に、視覚的に訴えることができることでメリットになることが期待されている。

（c）自己申告への活用

技術者がスキルを自己申告する手段として使えるようにすべきとの提案があるが、逆に自己申告に用いると評価認定としての価値が落ちてしまうため、やはりオフィシャルな認証が必要ではないかとの意見もある。この場合、認証には有効期限を設定し、継続教育を前提とした場合は有効期限を 3 年程度とするのが妥当としている。

（d）採用への活用

採用を目的にスキルモデルを利用する場合は、分類の基準を業務を中心にすべきことが指摘されている。ただし、採用の際の評価基準としては技術知識以外の要素の比重が大きく、スキルマップやスキルモデルの影響は大きくないとの意見が多い。

（e）人材育成への活用

人材育成を主眼に置く場合、スキルモデルの設定方法は職種ごとに整理されている方が使いやすいとの意見が得られている。これまでの企業教育は足りない部分を補うことを優先に実施されていたが、現在では人材育成を行ったことにより、いか

に市場価値を高めるかが重要になっているとの指摘がある。

（ｆ）人事考課、能力評価への活用

人事考課については、スキルそのものよりも成果が重視されるため、スキルマップの効果は限定されるとの意見が得られている。ただし、半年に１回など定期的な能力評価のレビューを行うような場合に、どういったスキルを持っているかを体系的に評価するための拠りどころとして有用との指摘がある。これは、スキルマップにリストアップされている項目を、能力考課のチェックシートとして使うことが想定されている。

（ｇ）調達・要員計画への活用

社内で情報セキュリティプロフェッショナルの募集する際の要件として、「PKI について語れること」といった形でスキルマップを使うことが提案されている。またプロジェクトを編成する際に、大工の棟梁が職人を集めるときと同じ要領で、スキルマップを要員計画策定のためのスキル評価ツールとして使えるようにしてはどうかとの指摘がある。

（５）スキルレベルチェックテストについて

テスト問題の難易度は個別に設定するというよりも、対象となる内容の難しさに依存するケースが多く、ベースとなるテキストもないことから、問題のレベルを客観的に設定するのは難しいのではないかとの意見のもと、「知識を問う問題」「考え方を問う問題」といった問題の内容に応じてレベルを設定するなど、ある程度の割り切りが必要性ではないかとの指摘がなされている。

また、スキルマップの能力認定はレーダーチャートとの整合を考慮すると、合否ではなく成績のスコアを測定する TOEIC などのようなスコア型の検定方式を参考にすべきとの意見が得られている。

（６）スキルマップ・スキルモデルの更新・維持管理について

変化の激しい情報セキュリティ分野において、新しい概念が今後も出てくることは避けられないが、これをどこまで含めるべきかが課題となる。ともすると分類学的議論に陥り、収束しなくなる危険もあるため、見直しのたびに軸が大きくぶれることがないようにするとともに、意見や注文に備えるため、スキルマップの作成の考え方をまとめ、Q&A のような形で明示することが重要との指摘がなされている。

スキルマップの内容のメンテナンスについては、各項目の中にはあまり変化しないもの、変化の激しいものが様々に含まれており、かつ新たに出てくるものを適宜取り込んでいく必要がある。このことを留意し、2〜3 年の間で見直しを行っていくのが妥当との意見がある。また、スキルマップやスキルモデルの内容の変化に伴う、継続教育との関係も整理すべきとの指摘がなされている。

（7）今後の調査研究の進め方について

スキルマップ関連の今後の調査研究の進め方について、得られた意見を以下に整理する。

（a）実証実験の実施

スキルマップやスキルモデルの活用方法について、大企業等をフィールドに実証実験的なことを実施する必要性が指摘されている。当初の理念等は時間の経過とともにブラックボックス化する恐れがあるため、調査研究を良いものにするには最初に方向を固めておくべきとされる。

（b）スキルマップ上の要素技術の活用についての事例研究の実施

スキルマップに整理された要素技術を、実際のセキュリティ対策やインシデント対応などの場面でどのように活用するかを結びつけるための事例研究が提案されている。業務に対して技術知識をどのように適用していくべきかを整理したマッピング作りを行うことにより、インシデントその他のリアリティのある事例を蓄積し、ノウハウとして共有化していくことが可能になるため、スキルマップを通じた社会全体のセキュリティレベルの向上も期待される。こうした構想を実現するため、各種の研究会等を通じて、業務的な部分の比重を高めた取り組みを推進することが求められている。

（c）機運の醸成への寄与

企業ではセキュリティ人材の必要性は認識しつつも、それをどのように育成していけばよいか良くわかっていないケースが多く、また個別の案件への対応を優先して、トータルの人材育成戦略やキャリアパスの中でセキュリティに関わる人材の育成をどう位置付けていくかという発想がないところも多いことから、スキルマップの普及など、情報セキュリティ向上に向けた機運を高めていくことが必要との指摘がなされている。

（d）カスタマイズへの対応

スキルマップを各種のニーズに応えられるようにするための要件として、自由度の高いものであることが必要であり、軸をカスタマイズできるユーザインターフェースやツールなどがあると便利との提案がなされている。

（8）情報セキュリティ教育のあり方についての関連事項

上記以外で情報セキュリティ教育に関して得られた意見を、以下に整理する。

（a）情報セキュリティに関するスキルについて

情報セキュリティに関するスキルをどのようにとらえるべきかについて、指摘された意見を以下に示す。

- セキュリティのスキルには、ナレッジとテクニカルの要素がある。
- セキュリティ技術によって何が守られるのかを感覚的に身につけていない人が多い。これは全ての根本になるが、一番難しいところかもしれない。
- 企業では経験年数もスキル評価の一つの目安であるが、プロジェクトの規模の大小で決めることはできない。
- インシデントレスポンス等は経験させることができないため教育が難しいという人がいるが、やり方次第と考えている。国内の多くの情報セキュリティはウィルスやワーム対策が中心だが、物理的なセキュリティや心理的な影響などもセキュリティの範疇だと考えている。
- セキュリティの分野でも理論と製品知識のどちらも重要になるが、ウェイトは職種によって変ってくるだろう。問題は、技術者がその両方をバランスよく学ぶ機会が少ないことではないか。

（b）OJT について

OJT の利用方法としては、基礎を養った上で、その後で何を学ぶべきかをわかる形で取り入れるべきとの意見が挙げられている。日本の OJT の仕方には批判もあるが、鍵はプロジェクトマネージャをどれだけ OJT によって経験を積ませ、育成できるかではないかとの見解である。

（c）大学の役割

教育における大学の役割としては、基礎的な学力の教育、大学でしかできない教育についての期待が大きい。具体的には、プログラミングがすぐにできるようになったり、ツールが使えたりということではなく、ベーシックな数学やネットワーク技術の基本などが想定されている。情報セキュリティ分野では、暗号技術に偏りすぎたカリキュラムは問題があるにしても、署名や電子透かしの原理を教えることには意義があるとの指摘がなされている。

（d）資格について

一般に資格制度はマーケットが大きくないと成立しないものであり、情報処理技術者試験のようにかつて職種ごとに狭めることを検討したものの、トレードオフを考慮して広い技術群を対象とする結果となった例もあり、職種などを絞った制度は難しいのではとの指摘がある。

（e）日本の情報セキュリティ分野の特徴

日本の情報セキュリティ分野の特徴として、暗号に強く、暗号を中心に展開が可能な点があることから、今後の日本のセキュリティ教育でもこうした特徴を活かしていくべきことが提案されている。また、日本の文化等を考慮した体系をもっておくことは意義があるとの指摘もある。

（ｆ）リテラシー教育

企業や組織セキュリティを守るためには、セキュリティアウェアネスを社員に対していかに持たせるかといったリテラシー教育が重要との意見が得られている。また交通安全教育のようなものを実施すべきことが指摘されている。

５．１．４ ヒアリング結果に基づく考察

以上のヒアリング調査で得た発言内容をもとに、本調査研究の各テーマについて考察を加えた結果を以下に整理する。

５．１．４．１ ヒアリング指摘事項に基づいたスキルマップの見直し

ヒアリング調査をもとに実施したスキルマップの見直し事項は、「２．３ 2003 年度版スキルマップの概要と見直しの論点」に示した通りである。大分類「情報セキュリティポリシー」を「情報セキュリティマネジメント」に変更して構成の見直しを行ったほか、認証、PKI、暗号、電子署名の各項目の拡充、特定の製品に依存する項目についての内容の精緻化などを実施している。

５．１．４．２ ヒアリングで指摘された論点

上述のスキルマップに関する見直し事項以外の範囲で、今回のヒアリング調査で得られた論点を整理すると、それぞれ以下のようになる。

（１）スキルマップについて

スキルマップに求められる事項として、以下が挙げられる。

（ａ）不足を指摘されている概念

情報セキュリティに必要な知識や考え方のうち、現在のスキルマップで十分に盛り込まれていない概念として、以下の項目が指摘されている。

- マネジメント
- 上流工程・構築
- 運用・情報管理
- 物理的セキュリティ
- 基礎知識
- 倫理、モラル
- プライバシー

このうち、マネジメントや運用、情報管理、倫理・モラルについてはそのスキルが知識以外の要素に依存する部分が大きく、スキルマップでは表現しにくいものと言える。一方、上流工程・構築に関してはセキュリティ対策に関する知識はプロセスの中に埋め込まれる形になるため、スキルマップ化した場合にセキュリティ以外の要素が大半となり、認識しにくくなる恐れがある。基礎知識と物理的セキュリティについては対象範囲が広くなるため、どこまでを範囲とすべきかが議論になる。

また、プライバシーについては、狭義の情報セキュリティの範囲から外れる概念といえる。このように、指摘された概念はいずれもそのままスキルマップに追加することが容易ではないものであるが、セキュリティ向上の見地からは重要性の高いものであり、今後の調査研究の過程で対応方針を定めていくことが求められる。

（b）スキルマップ記載項目の相互関連性の追加

スキルマップに記載されている項目間に依存関係がある場合、個別の項目毎にそれがわかるような仕組みを付加してはどうかとの提案がなされている。特に教育カリキュラムを検討する際に有用との意見が多い。本調査研究ではこれまでスキルマップ項目の整備を優先したためこうした検討はなされていないが、今後は用途を考慮した上で実現方法を検討することも必要と考えられる。特に、スキルマップを電子媒体上に実装する場合は平面的な整理にとらわれないこともあり、利便性に優れた実装の可能性も期待される。

（2）スキルモデルについて

スキルモデルとして業務別のモデルを作成し、項目別のスキルをランク付けするという考え方への異論は特に出ていない。ただし、そのモデルを用いて評価しようとする人材像についての意見は多様である。また、レベルの根拠についても様々な意見が出されている。これは、業務の種類によってレベル設定の考え方に違いが生じざるを得ないことによるところが大きいと考えられる。

現時点ではスキルモデルは実験的な事例を作成した段階にとどまっており、今後モデルが整備、具体化されるに応じてその妥当性についての議論が必要といえる。

（3）活用用途と今後の展開について

スキルマップやスキルモデルの活用用途としては、教育現場で有用との意見が多い反面、業務現場での利用については限定的なものになるとの意見が主流である。これは、業務現場で求められるスキルにおける技術知識の占める比率が限定的なものであることによるところが大きく、スキルマップそのものの課題とはいえない面もあるが、企業における人材育成などの用途での活用を発端として、今後もニーズに応じた改良を加えていく必要がある。

調査研究の今後の展開に関しては、実証実験の実施と事例研究の 2 つの提案がなされている。実証実験としては、現在の調査研究の方向のもとでスキルモデルとスキルレベルチェックテストの有効性を検証することが想定される。一方の事例研究は、スキルマップに整理された要素技術を実際のセキュリティ対策やインシデント対応の場面でどのように活用するかを整理するものであり、実際の現場で有用な知識を体系化する手段としてスキルマップを活かすためにも重要なテーマといえる。

５．２ グループインタビュー調査

今年度調査において新たに実施した、業種の異なる事業者によるグループインタビュー調査について、その経過と成果を示す。

５．２．１ グループインタビューの概要

情報セキュリティに関わる業務にたずさわっておられる方にご参加いただき、情報セキュリティプロフェッショナルの人材育成やキャリア等の現状や課題について意見を交換するグループインタビューを実施した。

（１）開催要領

- 日　時： 2003 年 10 月 30 日（木）16:00～18:00
- 場　所： 株式会社 富士総合研究所 本社（東京都千代田区）
- 出席者： 参加者７名、司会・進行 4 名、オブザーバ 1 名

（２）参加者属性

今回の参加者 7 名の所属企業の業種と、企業内での参加者の職種と職位を下表に整理する。なお、オブザーバ 1 名はスキルマップ WG メンバーである。

表 5-3　グループインタビュー参加者の属性

参加者識別名	参加者所属企業業種	参加者職種・職位(*)
A 社・a 氏	セキュリティサービスベンダ、システムインテグレータ	技術統括執行役員 CISO（情報セキュリティ統括役員）
B 社・b 氏	セキュリティサービスベンダ	システムインフラ担当チーフ
C 社・c 氏	情報システムベンダ、システムインテグレータ	セキュリティプロダクト技術グループ長
D 社・d 氏	損害保険	IT リスクプロジェクトリーダ
E 社・e 氏	ソフトウェアベンダ、システムインテグレータ	コンサルティング事業部マネージャ
F 社・f 氏	セキュリティサービスベンダ、システムインテグレータ	コンサルタント
G 社・g 氏	監査法人	シニアマネージャ

(*) 特定企業に固有と思われる職種名については、匿名化のため一部同義語で表現。

（３）討議内容

- 私と情報セキュリティのかかわり方（自己紹介を兼ねて、職種と業務について）
- 自組織における情報セキュリティ人材の現状と課題（採用、育成、評価、キャリアパス、等）
- 「スキルマップ」と「スキルモデル」について
- その他、ご意見（スキルマップの活用案、セキュリティ教育の問題、等）

（4）討議方法

グループインタビューにおける討議の進行は、以下に留意の上実施した。

- 参加者の率直な発言を促すため、インタビュー結果の整理・公開時に参加者の所属と氏名は公開しない旨を、開始に先立って司会者が説明し、参加者の了承を得ている。
- 司会者は各参加者の発言の機会が偏らないように配慮するとともに、ある参加者の発言に対し他の参加者が直接コメントするような議論の流れを尊重し、誘導的、統制的な発言を促すような進行の調整は避けるように努めている。

5．2．2 グループインタビューにおける発言内容の要旨

グループインタビューにおける発言を、前項（3）で示したテーマのそれぞれについて以下の各表に分けて整理する。

表 5-4　グループインタビューにおける発言内容の整理（その１）
現在の職務とセキュリティとの関わり

参加者･業種	現在の職務、セキュリティとの関わり
A 社･a 氏 セキュリティサービスベンダ，システムインテグレータ	■ 自社の技術担当執行役員兼CISOとして自社の情報セキュリティを執り行うほか、セキュリティ動向調査、リセールス、セミナー、時には執筆など。
B 社･b 氏 セキュリティサービスベンダ	■ PKI関係の社外サービスの構築や、運用サポートのほか、関連製品の設計･構築･サポートにも参加。 ■ かつてファイアーウォールという言葉が出始めた時に、そのサポートを担当した以降、なし崩しにウェブのセキュリティ、認証ウェブサーバ、PKIを担当。
C 社･c 氏 情報システムベンダ，システムインテグレータ	■ 自社のネットワークセキュリティ製品担当部署の管理者。エンドユーザの技術サポート、IDSやファイアーウォールの導入サービス、ポリシー作成、監査などを提供。セキュリティ業務に係わるきっかけは、ネットワークの導入支援に携わったこと。
D 社･d 氏 損害保険	■ 主に通信系、若しくは情報サービス業者向けの保険の構築と提供を担当。こうした業界では、情報セキュリティの重要性が高まるとともに、情報セキュリティ分野の保険のニーズも高まりつつある。 ■ 電子商取引･電子決済に伴うリスクの保険によるヘッジなどの企画開発も担当。
E 社･e 氏 ソフトウェアベンダ，システムインテグレータ	■ コンサルティング担当部署に所属し、ISMSの取得コンサルティングがメイン。 ■ セキュリティ業務へ携わったきっかけは7-8年程前、親会社の製品を売り込む話が出た時に言葉を偶然知っていた人間が駆り出されたこと。その後はSETの認証システム、指紋など本人認証技術など。
F 社･f 氏 セキュリティサービスベンダ，システムインテグレータ	■ 現在スキルマップに記載されている項目は全部行っている。 ■ 私の初めてのセキュリティ業務は、社内の内部監査、リスク管理体制の構築。
G 社･g 氏 監査法人	■ セキュリティマネジメントの仕事と支援業務、ISMSの取得、セキュリティの監査を担当。UNIXやWindowsだけでなく汎用機も扱い、Webや電子メール以外の業務パッケージのセキュリティもこなす。 ■ 最初に担当した仕事がセキュリティであったことが、私のセキュリティとの係わり。

表 5-5　グループインタビューにおける発言内容の整理（その２）人材教育の現状

参加者･業種	人材教育の現状
A 社･a 氏 **セキュリティサービスベンダ，システムインテグレータ**	■ 自社内で体系立った教育は無い。脆弱性コンサルティングなどを担当する技術者は、自社のCEなどの中からセキュリティに興味を持ち、技術的にも出来る人間を異動させているのが現状。 ■ コンサルタントは高度の技術者である必要は無く、顧客との折衝能力がある人物を選ぶ。
B 社･b 氏 **セキュリティサービスベンダ**	■ 体系的な教育プランはない。新人教育は縦割りで部署毎に講座を開くため、全体としての教育は難しい。これを打破する為にスキルを持つ人への特別手当制度を設けたものの、結果的にスキルよりもアピール能力が高い者が得をすることになってしまっている。
C 社･c 氏 **情報システムベンダ，システムインテグレータ**	■ 私の部署では、IDSやファイアーウォール等のプロダクトの教育が中心。 ■ 外部のセキュリティに関するカリキュラムで本当に有益なものは無い。 ■ 顧客対応のスキルが求められるが、その教育は難しいと感じている。 ■ 社員の年齢が高いのでOJTが適している。
D 社･d 氏 **損害保険**	■ 自組織には個別技術の専門家がいるわけではない。ユーザの立場でセキュリティ人材を考えたとき、ある程度全体的に解っている人が必要と思われる。
E 社･e 氏 **ソフトウェアベンダ，システムインテグレータ**	■ セキュリティに特化したSIと呼ばれながらも、セキュリティだけでビジネスをするのは難しいのが現状。よって人材教育で固有のセキュリティ技術に特化した人を育ててしまうと、その人の活躍の場が限られてしまうため、固有のセキュリティ技術に特化した人物を育てることはしていない。 ■ 当部では固有の技術を教えるための教育スケジュールは持たず、OJTがメイン。
F 社･f 氏 **セキュリティサービスベンダ，システムインテグレータ**	■ セキュリティは信頼が肝心であり、中途採用した新入社員を直ちにセキュリティ業務に配属することはない。 ■ 人材教育としてはOJTというより、実際に製品評価をやらせて習得させるようなことをしている。
G 社･g 氏 **監査法人**	■ セキュリティ技術者に関する体系的な教育制度は備わっておらず、必要に応じてOJT、外部セミナーへの出席などにより行っている。またセキュリティ技術専門家向けに特化した評価制度は無い。 ■ セキュリティの技術系を中途採用するのは困難な状況。実際には銀行や証券でシステムを扱っていた30歳代から40歳代の人、総合研究所、コンサルティング会社から転職した人がセキュリティ関連業務へ配属される場合が多い。

表 5-6　グループインタビューにおける発言内容の整理（その３）スキルモデルについて

参加者･業種	スキルモデルについて
A 社･a 氏 セキュリティサービスベンダ，システムインテグレータ	■ レーダーチャートの面積を毎年見直す必要があるのではないか。 ■ 採用する際は職務経歴と資格をみる。セキュリティに特化した技術者はめったにいないので、職務経歴におけるUNIXの経験、サーバの経験、ネットワークの経験を見て、その中でセキュリティでは何をしていたかを見るのが実情。
B 社･b 氏 セキュリティサービスベンダ	■ 評価を受ける側が自分の知識の充実度を見る為には、詳細に分類してあると良い。今後の自己啓発への資料として使える。 ■ 評価する側での利用はまだ難しい印象。
C 社･c 氏 情報システムベンダ，システムインテグレータ	■ 採用をする為の資料やキャリアプランをする為の資料、能力を示す為の資料といった全てを満たすことを考えるとまとまらないと思う。現時点では、どのような人材を欲しているかという意思表示手段としては使えると思う。採用の場合を充実させて、その後の育成プランに使えるかどうかは改めて議論をした方が良い。
D 社･d 氏 損害保険	■ セキュリティ担当者も、まずは基本的な法律知識は必要。特殊な法律（個人情報保護法、不正アクセス禁止法、電子商取引の準則など）を理解する前に、民法などで定められた法律上の賠償責任というものが何かということだけでも、理解してほしい。しかし、あまり理解していない人が多い。
E 社･e 氏 ソフトウェアベンダ，システムインテグレータ	■ スキルモデルは、こちらが望む人材の要件を示すのには使えるが、相手から示される内容は信用できないので使えない。社内で個人の能力を育成するとき、スキルモデルに挙げている項目を全て必要とする業務はなく、多くとも二つ程度ではないか。 ■ 自分の部署の人材を俯瞰する管理者にとっては、組織の得意分野や欠けている部分を素早く分かるという意味で有用。 ■ セキュリティ技術者と呼ぶ時には、ほぼ全ての分野において、レベル0から1の間の知識を理解する必要はあるはず。また普段の情報の入手先や、どれだけのものを調べているかで分けることも可能ではないか。 ■ セキュアプログラミングだけ出来る人をセキュリティ技術者と呼ぶのは疑問。
F 社･f 氏 セキュリティサービスベンダ，システムインテグレータ	■ スキルモデルにはコスト感覚、市場感覚が含まれていない。実際にはレーダーチャートの軸ごとの面積が異なるのではないか。例えば、セキュアプログラミング技法とセキュリティ運用は同じレベルでも面積が違うはず。 ■ このようなグラフは、丸に近い方が偉いというイメージがある。 ■ セキュリティ技術者を求める会社があるかどうかはわからない。セキュリティ技術者になりたい人、それをキャリアパスに望む人は世の中にあまりいないのではないか。スキルモデルが使えるかどうかは、欲している人がいるかによる。
G 社･g 氏 監査法人	■ 「不正アクセス対策システム導入」のスキルモデルのレーダーチャートで示される形になるための順番はあるか。すぐにこの形になれる人はいないはず。徐々に大きくしていくか、いずれかの部分を強くしていくのかになる。 ■ スキルモデルは採用に用いるには絞りすぎの印象。 ■ このスキルモデルだけで100%というのは無理である。

表 5-7　グループインタビューにおける発言内容の整理（その４）スキルマップについて

参加者･業種	スキルマップについて
B 社･b 氏 セキュリティサービスベンダ	■ 暗号はともかく、なぜ署名･PKI･認証は分かれているのか。 ■ モデルの項目に依存関係があるのではないか。依存関係が視覚的に見えると、とても良いものになると思う。
G 社･g 氏 監査法人	■ 電子署名･暗号･PKIは3つに分けてあるが、システム運用という業務面からみると暗号を1つくくりだす必要があるか疑問である。

表 5-8　グループインタビューにおける発言内容の整理（その５）
人材像、スキルマップの応用、その他について

参加者･業種	人材像、スキルマップの応用、その他について
B 社･b 氏 セキュリティサービスベンダ	■ 段々とセキュリティ業務がなくなる可能性もある。
D 社･d 氏 損害保険	■ 情報セキュリティ対策は予防の観点が重視されがちだが、保険は、事故が起った後の具体的な損害をいかに処理するのかというアプローチ。よって、リスク分析･リスクシナリオ作成では最終的に誰にどのような損害が発生するのかを重視する。誰の損害なのかを判断する上で、法律上の知識が必要。よって、顧客であるセキュリティ担当者に対して、法律の解釈を教えることは多い。こうした法律知識があれば、一味違ったセキュリティプロフェッショナルになる。
E 社･e 氏 ソフトウェアベンダ，システムインテグレータ	■ 採用をするための資料やキャリアプランをするための資料、能力を示すための資料、といった全てを満たすことを考えるとまとまらない。現時点では、どのような人材を欲しているかという意思表示手段としては使えるのではないか。 ■ 採用の場合を充実させて、その後の育成プランに使えるかどうかは改めて議論をした方が良い。 ■ セキュリティだけで稼げる時代は終わりつつある。
F 社･f 氏 セキュリティサービスベンダ，システムインテグレータ	■ セキュリティ以外のSIにおいて、発注側と受注側の課題があり、発注内容など、発注者の能力は確かではない。これには困っていた。 ■ システムインテグレーションの過程でセキュリティは当たり前になるはずで、最終的にセキュリティ技術者は危機管理責任者になるのではないか。

５．２．３ 発言内容に基づく考察

以上の発言内容をもとに、今回の調査研究項目についての分析を行う。

５．２．３．１ 発言における論点

グループインタビューの議論の流れにおいて示された論点として、顕著なものを以下に整理する。

（１）情報セキュリティ技術者と人材教育の現状

十分なスキルを有する技術者が充足している状況にないことがわかる。ただし、その対策としては拙速な教育カリキュラム等ではなく、OJT を通じて段階的にスキルアップを図っている傾向が見受けられる。こうした傾向から、グループインタビュー参加企業では不十分なスキルしか持たない技術者がセキュリティ業務に従事することによるリスクは回避できていると想定される。しかしながら、逆に高いスキルを有する一部の技術者に業務が集中している可能性は否定できない。

（２）情報セキュリティ技術者に求められるスキル

知識以外の部分を重視すべきとの意見が多く出されている。これは、有識者ヒアリングと共通の傾向と見なせる。

（３）スキルマップとスキルモデルについて

スキルマップについての意見は少なく、大分類の区分方法に関して暗号、認証関連の項目が多いことへの疑問が出ている程度である。依存関係に関しては、「５．１．４．２ ヒアリングで指摘された論点」と同様の意見が出ている。

一方スキルモデルに関しては、不足している項目として、コスト感覚、市場感覚などが指摘されている。また、レーダーチャート形式での表現がスキルを表現するために適切かどうかとの意見がある。具体的には、一般的なレーダーチャートでグラフの形状が大きな円形になるのが理想となるような使われ方が多いのに対し、スキルモデルでは理想的なスキルの構成であってもグラフに凹凸があることが前提となっているため誤解を招きやすい点や、スキルモデルを構成する各大分類の軸ごとの面積はその影響の大きさによって異なってしかるべきではないか、といった指摘がなされている。

（４）スキルマップとスキルモデルの今後の活用について

有用とされているのが、個人における自己啓発のための資料や、組織の得意分野や欠けている部分の把握などへの活用である。この場合、スキルの妥当な評価を行うための方法の整備が前提となる。また、採用や発注時にどのような人材を欲しているかの意思表示手段にも使えるという意見もあり、これは現在のスキルモデルの延長での活用が可能な用途と考えられる。

反面、活用の可能性に関する否定的な意見も少なくない。採用時については、応募者の自己申告は信用できないとされ、スキルモデルをベースに採用の可否を判断する

のは絞りすぎの印象があると指摘されている。人材の評価用に関しては、前述の通り知識に依存する比重が限られることもあり、難しいとの印象が示されている。

（5）今後の情報セキュリティ技術者の人材像について

情報セキュリティのみを専門とする技術者のニーズについては、悲観的な見解が支配的である。さまざまな専門性をもった技術者が、セキュリティに関する知識も身に付けていることを示す手段としてスキルモデルを利用することが現実的と考えられる。

また、現行でセキュリティ業務が分野別に分かれ、それぞれの担当者がセキュリティの特定分野の知識しかもたないことが指摘されているが、スキルマップを活用することでこれを改善できる可能性がある。具体的な例として、法律的知識を有する情報セキュリティプロフェッショナルが提案されていることが注目される。

5．2．3．2 グループインタビュー全体の傾向

前項で示した個別の発言内容以外に、グループインタビュー全体を俯瞰して得られた傾向について、以下に考察する。

（1）業種間の相違

セキュリティサービスの提供側と利用側、システムの構築側と監査、利用側等で見解の相違が発生することはなかった。ただしこうした傾向となった最大の原因は、今回のグループインタビュー参加者が日常的に社外の情報セキュリティに関する NPO 活動に参加しているか、参加はしていなくても活動状況を理解していることによるところが大きい。よって、今回のグループインタビューで見解の相違や対立が見られなかったことを根拠に、現在の我が国における情報セキュリティ分野における関係者間での問題意識の一致等を論じるのは無理といわざるを得ないものの、十分な情報の共有を得た条件の下では、業種の相違を超えた合意形成等も可能であることを示唆する傾向であるとみることができる。

（2）有識者ヒアリングにおける意見との対比

有識者ヒアリングにおける事業者を対象にした調査と、グループインタビューとでは、強調されたポイントを含め、ほぼ同様の傾向に基づく意見が得られている。全体的な傾向としては、有識者ヒアリングではスキルマップとスキルモデルの資料の説明を中心とした調査であったため、調査研究成果へのコメントが主流であるのに対し、グループインタビューでは参加者間で人材教育の現状などの情報を共有した上でスキルモデル等の在り方について議論を行ったため、情報セキュリティ教育に関する問題点を中心とする議論になったことが違いとして挙げられるが、有識者ヒアリング対象者とグループインタビューの参加者との間での問題意識の相違はほとんどなかったものと判断される。

６．スキルマップの活用支援策の検討

本調査研究の実施にあたって、各種検討やヒアリング、グループインタビューなどの活動を行ってきたが、情報セキュリティ人材育成が情報化社会の安全性確保において非常に重要な課題であり、それを難しくしている要因が多々存在している現状を再確認する形となった。

本調査研究では、問題の解決に貢献することを目指し、本年度策定したスキルマップやスキルモデル、スキルレベルチェックテストなどのツールを広く普及させ、活用していくことの可能性について検討を重ねてきた。また、ヒアリングやグループインタビューからは、スキルマップの有用性について前向きなコメントが多数得られたのと同時に、実際の企業の現場で活用にするためには、クリアしなければならないハードルも少なくないことも指摘されている。

本章では、本調査研究の総括として、スキルマップ活用に向けた施策の検討とわが国における情報セキュリティ人材の充実に向けた論点として以下の項目について整理する。

1. スキルマップの活用に向けた課題
2. スキルマップに基づく能力検定の可能性と課題
3. 情報セキュリティ人材育成に向けた課題

６．１ スキルマップの活用に向けた課題

（１）技術知識以外の能力・スキルへの展開

スキルマップは、情報セキュリティにかかわる技術に関する項目を中心に整理体系化を行ってきたが、企業の現場においては、技術知識を習得するだけではなく、それを如何に活用していくがより重要となる。また、人材育成や能力評価、採用などにおいては、技術知識の有無と同様（あるいはそれ以上に）、技術知識以外のスキルや能力に対するウェイトが高い場合が多い。

情報セキュリティにおいて求められるスキルとして、以下のようなものが重要になると考えられる。

- 未知の現象や問題に対して適切に対応する洞察力、問題解決能力
- 自社（あるいは他者）の情報資産に対するリスクを分析する能力
- インシデントの発生による被害とセキュリティ対策のコストのバランスについて計量的に判断できるスキル
- 顧客や自組織の他の部門とのコミュニケーション能力
- 新しい技術や知識に対して積極的に取り組もうとする学習能力

真の意味での情報セキュリティ人材育成においては、技術知識に加えて上記のような能力やスキルをいかに強化していくが重要となるが、「３．１．１ スキルモデルの策定の背景（１）情報セキュリティプロフェッショナルの現状」などにおいて指摘したように、情報セキュリティにたずさわるエンジニアや技術者が独立した職種としてとらえることが難しい、キャリアパスや求められる能力要件が明らかになっていないなど、課題

は少なくない。スキルマップに関する調査研究の延長として、情報セキュリティにかかわる業務あるいは職種について、どのような能力・スキルが求められるかについて整理する必要があるだろう。本年度のスキルモデルの作成においても、5 つの業務をサンプルとして取り上げ、業務遂行のための能力要件について検討したが、より詳細かつ一般化することが求められている。

同様に、技術知識の習得を上記の業務遂行能力の発揮にどのようにしてつなげていくかが重要となる。スキルマップに整理された要素技術を、実際のセキュリティ対策やインシデント対応などの場面でどのように活用するかについて、両者を結びつけるための事例研究などが有用ではないだろうか。さらには、これらの活動を得られた知見をナレッジやノウハウとして、広く共有化し、社会全体のセキュリティレベルの向上へとつなげていくことが期待される。

（2）教育カリキュラムへの応用

スキルマップの応用分野の一つとして、教育カリキュラム策定が考えられる。カリキュラムを策定する場合、項目間の関連や習得すべき項目の順序を整理する必要がある。現在のスキルマップは、知識項目を表形式に整理しているため、このような関連性を表現することはできない。

スキルマップの小分類を見ると 470 以上の項目があることからわかるように、情報セキュリティに関する技術知識だけでも非常に多くの内容を含んでいる。さらに、情報セキュリティについて学ぶためには、ネットワーク技術や IT に関する基礎技術や数学、法律、経営など、多くの分野がかかわってくる。特に、大学など高等教育機関でのカリキュラムを想定すると、教養課程、専門課程の他の分野などさらに多くの科目・項目が複雑にかかわってくるだろう。

スキルマップに関する議論の延長として、このような項目間の複雑な関係を 3 次元 CG などの技術によって表現する視覚化技術の導入なども検討の視野に入ってくるかもしれない。類似の活動としては、東京大学工学教育プロジェクト「工学知の構造化と可視化」において、工学分野の教育カリキュラムの構造化と視覚化技術の導入に関する検討を行っている[6]。

（3）スキルマップの継続的なアップデート

情報セキュリティ分野の技術の進化と方向性の変化のスピードは速く、スキルマップの継続的な見直しとアップデートが必要である。ただし、情報セキュリティ関連の製品や技術は、高機能化、複合化が進んでいるため、スキルマップではある程度技術的に確立された基礎的な事項を中心に整理されるのが望ましいと考えられる。

整理にあたっては、現在の 16 大分類を維持しつつ、中分類以下を適宜見直していく方法が一貫性を保てるが、場合によっては大分類の統廃合や再整理なども必要に応じて行うべきである。また、「2．3．2 スキルマップのアップデートに係る論点（4）別表

[6] http://www.t.u-tokyo.ac.jp/esp/ESPHP1.htm 参照

の取り扱いについて」に示したように、情報セキュリティに関連する分野などを別表形で追加していく方法も考えられる。

6．2 スキルマップに基づく能力検定の可能性と課題

（1）スキルレベルチェックのベータテスト（試行実施）

本調査研究の一環として、スキルレベルチェックテストのサンプルとして 160 問を作成した（「4．情報セキュリティに関するスキルレベルチェックリストの策定」）。「タイプ 1： 言葉を問う問題」「タイプ 2： 意味を問う問題」「タイプ 3： プロセスを問う問題」の 3 種類の問題文を用意したが、作成にたずさわったメンバから以下のような意見が指摘されている。

- 問題のタイプと問題の難しさが必ずしも一致しない。例えば、「タイプ１： 言葉を問う問題」でも、分野によっては正解を答えられる人は少ない（知らなければ答えられない）。
- 分野ごとの難易度のばらつきがわからない。
- 実際に試験を受けた人の「生」の意見を問題に反映させていくことが必要。

スキルレベルチェックテストの質的向上を図るため、モニタを対象にベータテストを試行的に実施し、そこで得られた正答率やコメントなど、問題文の作成や難易度の設定のための基礎データを得ることが有用である。各大分類ごとの正答率を分析することで、分野ごと、問題ごとの難易度をどの程度にすればよいか、定量的に判断することが可能になる。

ベータテストの実施にあたっては、テストプールの充実や難易度設定、問題作成の方法論の検討に加えて、受験者に対して試験結果をどのようにフィードバックすればよいかも検討課題となる。

（2）スキルレベルチェックの Web 能力検定の提供

利用者が簡単に自分の技術知識のレベルを測ることができるようにするために、スキルレベルチェックする能力検定サービスを Web 上で提供することも考えられる。Web 上で検定サービスを提供することにより、いつでも自由にテストを受けられるようになる、採点結果を即座にフィードバックできるなどのメリットがある。この際、採点結果をスキルマップの 16 大分類を軸とするレーダーチャートで表示するインターフェースを提供することで、受験者は、分野ごとに自分がどの分野に強く、どこが弱いかを判断できるようになる。

職種や業務などに対応して、求められる技術知識のレベルを提示することで、目標を与えることができる。特に、セキュリティに対する初学者などが自身の学習の目標設定とその成果を測定するのにも効果的だろう。

スキルマップをベースとした能力検定の場合、テスト結果で合否を判定するのではなく、点数（スコア）を受験者にフィードバックする「スコア型」の検定の方がなじみや

すいと考えている。基準点をクリアすると合格となる合否判定型は、受験者が一定水準に達していることを判断するに適しているが、幅広いニーズに対応して対象範囲が広がると、その試験の合格者がどういった技術に優れているかがわかりづらくなる、という意見もある。特に、情報セキュリティの分野は、関連する技術知識の裾野が広いうえ、さまざまな業務ごとに要求される知識の内容や水準も異なっている。スキルマップをベースとした能力検定では、分類ごとにスコアを対応させることによってどの分野の技術知識に優れているか、個人の特徴を提示しやすくなる。

（3）スキルモデルとスキルレベルチェックテストの連携

スキルモデルのレベル定義とスキルレベルチェックテストの結果をどのように対応付けるかについては今後の検討課題の一つである。スキルモデルの各項目のレベルを判断する基準として、スキルレベルチェックテストの試験結果を用いることが考えられる。

この場合、問題の難易度や何点取ればスキルモデルの各レベルに対応すると判断できるか、などについて検討する必要がある。そのためにも、前述したスキルレベルチェックテストの試行実施は役に立つものと考えられる。

6．3 情報セキュリティ人材育成に向けた課題

（1）既存制度との連携

2002 年 12 月に「IT スキル・スタンダード（Ver1.0）」（ITSS）が経済産業省より発表されている[7]。ITSS は、各種 IT サービスの提供に必要とされる能力を明確化・体系化した指標であり、以下のような要素より構成されている。

- IT サービスを「職種／専門分野」として区分
- 経験・実績を記述した「達成度指標」を設定
- スキル項目毎に修熟の度合いを示す「スキル熟達度」と必要な「知識項目」を展開

ITSS では、以下の 2 つの職種において、セキュリティに関する専門分野が規定されている。

- IT アーキテクト
  ビジネス上の課題解決のためのアーキテクチャ設計を実施する
- IT スペシャリスト
  システム上の課題解決に係るシステム設計、構築、導入及びテストを実施する

ITSS では、専門分野ごとに必要な知識項目とスキル熟達度にレベルを定義しており、スキルを客観的に観察する指標である経達成度指標とあわせて、主として「人」の観点

[7] http://www.meti.go.jp/policy/it_policy/jinzai/g030701aj.html 参照

からスキルついての整理を試みている。一方、スキルマップでは「技術」の観点から知識項目の体系化を図るとともに、技術を軸とした評価のものさしと機能するためにスキルモデルやスキルレベルチェックリストの検討を行った。ITSS とスキルマップは、情報セキュリティ分野において、いわば相補的な関係にあるといえる。ITSS の体系中に情報セキュリティに関する項目が出てくるのは上記の 2 つの職種だが、情報セキュリティはすべての部門、職種にかかわるものである。職種共通の情報セキュリティ関連の知識項目に関する部分については、スキルマップを参照するなどの連関も考えられる。

IPA は 2003 年 7 月に「IT スキル標準センター」を設立し、ITSS の改版や、企業等での活用事例の収集・分析、及びプロフェッショナルの後進育成に有益な情報発信などを行うこととしている[8]。今後、スキルマップの普及に向けて、このような取り組みと協調が図られることが望まれる。

（2）情報セキュリティ人材育成の推進に向けて

経済産業省の諮問機関である産業構造審議会セキュリティ部会は今年 10 月、「情報セキュリティ総合戦略」を答申した。わが国ではじめて策定された総合的な情報セキュリティに関する戦略として位置付けられており、「世界最高水準の高信頼性社会の構築」を目標にかかげて 3 つの戦略と 42 の施策項目を提言している。総合戦略では専門的な実務家・専門家の育成と、一般ユーザを対象としたセキュリティリテラシの向上の両面から施策を推進することとしている。コンピュータのみならず、家電や自動車、携帯通信機器などあらゆるものがネットワークでつながれていくなかで、すべての人が安心かつ安全に新しい情報社会に参加できるようになるために、情報セキュリティの確保はより一層重要となる。社会全体の情報セキュリティレベルの向上に努め、個人ユーザを含めた各層に対して情報セキュリティに対する認識を普及させていくことが求められている。

本調査研究では、スキルマップの整備やスキルモデル、スキルレベルチェックリストなどのツールの策定を通じて、情報セキュリティに関する高度な専門知識を持つ人材の育成に主として焦点を当ててきた。しかし、上記のように情報セキュリティは社会全般にかかわる課題となっており、産業界、教育界、公的部門がオープンな「場」において、課題の解決に向けて現状と課題の問題意識について共有することが重要である。今後、情報セキュリティ人材の育成を足がかりとして、このような「場」の活性化に取り組んでいくことを予定している。

（了）

8 http://www.ipa.go.jp/itss/参照

7．付録

7．1 スキルモデルのフォーマットと作成ツール

「3．情報セキュリティに関する「スキルモデル」の策定」にて述べたように、本調査研究では、スキルマップをベースに「スキルモデル」の策定について検討を行い、5 つの業務を対象としてサンプルを作成した。

スキルモデルは、企業や組織がそれぞれのニーズや状況に応じて作成することを想定しており、利用者がスキルモデルを簡単に作成できるようにするための作成ツールを用意した。現在のバージョンのフォーマットは Microsoft Excel 形式のファイルとして提供されている（別添：スキルモデル作成機能.xls 参照）。

以下に作成ツールの使用方法示す。

【スキルモデル作成ツール（スキルモデル作成機能.xls）使用方法】

① シート[スキルモデルサンプル]に「業務名」「Ⅰ．業務の説明」「Ⅱ．能力要件の定義」「Ⅳ．必要となる基礎知識・業務知識」「Ⅴ．補記事項」を記入。それぞれの記載内容については「表 3-2　スキルモデルのフォーマット」を参照。
② スキルマップの大分類に対応するシート[1]～[16]の中分類にレベルを定義する。
③ 自動的にシート[スキルモデルサンプル]の「Ⅲ．　技術知識の要求レベル」が描画される。
④ レベル定義の内容や大分類、中分類は、ニーズに応じてカスタマイズして使用する。

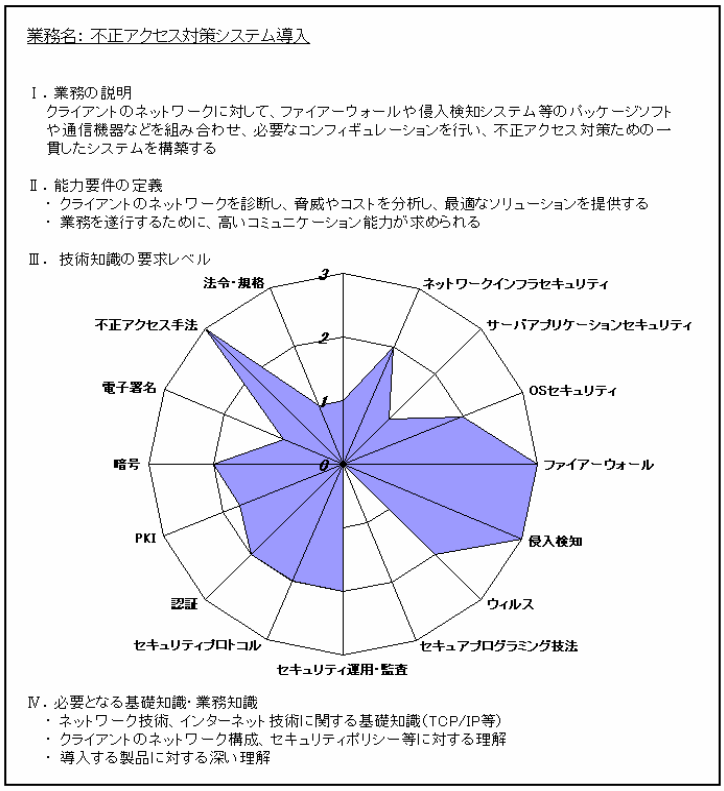


図 7-1　スキルモデルの完成イメージ

７．２ スキルレベルチェックテストサンプル

(1) 情報セキュリティマネジメント
(2) ネットワークインフラセキュリティ
(3) アプリケーションセキュリティ
(4) OS セキュリティ
(5) ファイアーウォール
(6) 侵入検知
(7) ウィルス
(8) セキュアプログラミング技法
(9) セキュリティ運用
(10) セキュリティプロトコル
(11) 認証
(12) PKI
(13) 暗号
(14) 電子署名
(15) 不正アクセス手法
(16) 法令・規格

【注】
・タイプ欄の数字は以下の３種類のいずれかに属することを示す。
　タイプ１： 言葉を問う問題
　タイプ２： 意味を問う問題
　タイプ３： プロセスを問う問題
・ターゲット欄：テスト問題を作成した単位。原則としてスキルマップの中分類または小分類を対象とする（表中の記号は[中]＝中分類項目、[小]＝小分類項目を表す）。
・知識項目（大分類、中分類、小分類、備考）は「2003年度版スキルマップβ版」に記載のものをベースとしている。

(1)　情報セキュリティマネジメント

No.	タイプ	問題	選択肢	正解	ターゲット 備考（※印）
1-01	1	セキュリティの3大要素は、略してCIAと言われている。日本語で該当するものを選択せよ。	ア．人的、管理的、システム的 イ．人的、論理的、物理的 ウ．機密性、完全性、可用性 エ．人、物、金	ウ	[中]マネジメント技術 [小]マネジメントプロセス **※機密性**（Confidentiality）、**完全性**（Integrity）、**可用性**（Availability）
1-02	1	情報システムのセキュリティを考える際の「9原則」が提示されているのはどれか、適切なものを選択せよ。	ア．経済産業省「コンピュータウイルス対策基準」 イ．経済産業省「情報システム安全対策基準」 ウ．経済産業省「システム監査基準」 エ．OECD「情報システム及びネットワークのセキュリティのためのガイドライン」	エ	[中]関連知識 [小]情報セキュリティの標準化 **※OECDの「情報システム及びネットワークのセキュリティのためのガイドライン」は基本的な知識として、一読が必要である。**
1-03	1	ISMS認証基準（Ver.2.0）では、組織においてISMSを確立、導入、運用、監視、維持し、かつそのISMSの有効性を改善する際に、奨励していることで、最も適切なものを選択せよ。	ア．プロセスアプローチ イ．リスクマネジメント ウ．評価基準 エ．教育	ア	[中]関連知識 [小]情報セキュリティの関連制度 **プロセスアプローチとは、インプットをアウトプットに変換するために、経営資源を使用して運営管理されるあらゆる活動をプロセスとみなし、組織内のプロセスを明確にし、その相互関係を把握し、これら一連のプロセスをシステムとして適用して、運営管理することである。**
1-04	2	組織の情報資産の適切な保護を維持するためには、どのようなことを実施すべきか。最も適切なものを選択せよ。	ア．重要な情報資産には保存箱の施錠を徹底する。 イ．重要な情報資産は耐火金庫に入れる。 ウ．資産の情報目録の作成とレベルに応じた保護。 エ．全員の啓蒙教育による徹底。	ウ	[中]リスク分析技術 [小]情報資産の調査･評価 **※情報資産の目録を作成し、分類の指針を示し、情報の共有又は制限する、業務上の必要性、影響を考慮して、適切なレベルでの保護を確実にすることが重要である。**

No.	タイプ	問題	選択肢	正解	ターゲット 備考 (※印)
1-05	1	人による誤り、盗難、不正行為、又は設備の悪用のリスクを軽減するために行う管理策として具体的なものとして、どれが該当するか、最も適切なものを選択せよ。	ア．セキュリティポリシーの策定 イ．アクセス制御 ウ．秘密保持契約書への署名 エ．セキュリティが保たれた領域での作業	ウ	[中]情報セキュリティポリシー [小]人的対策 **※人的セキュリティに関しては、大きく分けて、職務定義及び雇用におけるセキュリティ、利用者の訓練、セキュリティ事件・事故及び誤動作への対処等がある。**
1-06	2	情報処理設備の正確、かつ、セキュリティを保った運用を確実にするための管理対策の具体例の組み合わせとして、最も適切なものを選択せよ。	ア．操作手順書 ／ 秘密保持契約 イ．事件・事故管理手順 ／管理責任者の設置 ウ．外部委託による施設管理 ／ 秘密保持契約 エ．雇用条件の設定 ／ 開発施設及び運用施設との分離	イ	[中]情報セキュリティポリシー [小]運用・管理対策 **※秘密保持契約、雇用契約は、人的対策になる。**
1-07	2	システムの計画において、システム故障の発生する可能性を最小限に抑えるための管理対策を実施する場合、具体的なものとしてどれが該当するか。最も適切なものを選択せよ。	ア．容量・能力の計画作成 イ．情報のバックアップ ウ．運用の記録 エ．障害記録	ア	[中]情報セキュリティポリシー [小]運用・管理対策 **※ア.以外に、新しい情報システム、改訂版および更新版の受け入れ基準を確立し、受け入れ前に適切な試験を実施すること、等もある。**
1-08	2	刑法、及び民法、その他の法令、規制又は契約上の義務、並びにセキュリティ上の要求事項に対する違反を避けるために、具体的な管理対策が講じられることが大切である。次の具体策のなかで、これに該当しないものを選択せよ。	ア．各情報システムについて、全ての関連する法令、規制及び契約上の要求事項を明確に定め,文書化すること。 イ．地震・災害等の被害のリスクヘッジとして、信用のおける保険会社と保険契約を結ぶ。 ウ．関連法令に従って個人情報を保護するために、管理策を適用する。 エ．組織の重要な記録は、焼失、破壊改ざんから保護されること。	イ	[中]情報セキュリティポリシー [小]運用・管理対策 **※イは、リスクマネジメントに関することである。**
1-09	2	重大な障害または災害による事業活動の中断に対して、重要な業務手続きを保護するための方策として、もっとも適切なものはどれか。	ア．組織は、情報処理設備を含む領域を保護するために幾つかのセキュリティ境界を利用すること。 イ．特別なセキュリティ要求事項のあるオフィス、部屋及び施設を保護するために、セキュリティの保たれた領域を設定すること。 ウ．装置についての継続的な可用性及び完全性の維持を可能とするために、装置を正しく保守すること。 エ．事業運営を重要な業務手続の中断又は障害の後、適切な時間内で維持又は復旧させるための計画を立てること。	エ	[中]情報セキュリティポリシー [小]運用・管理対策 **※特に重要な「事業継続管理」に関した問題である。**

No.	タイプ	問題	選択肢	正解	ターゲット 備考（※印）
1-10	3	ある企業において、情報セキュリティの基本文書を2年前に作成した。その後、企業のおかれている環境、ビジネスの内容も変化したため、見直しを進めている。このような場合、次の項で最も適切なものを選択せよ。	ア．新社長が就任し、経営戦略等も新しくなり、変更されたので、「情報セキュリティの基本文書」をもう一度新しい視点で見直してみる。 イ．最近、「情報セキュリティの基本文書」に関して、他社の良い例の発表会があり参加した。大変良いので、自社のものを、全面変更することを考えている。 ウ．会社の新しい施策は出されているものの、まだ「情報セキュリティの基本文書」の作成から2年しか経っておらず、当面はこのままにすることにした。 エ．「情報セキュリティの基本文書」を見直した結果、社長に承認を頂いた。実際は、当初の予定より、少ない変更であるので、各部署に正式に変更連絡を行うと、そのための作業が多く、効率が悪いことから、今回は各部署への連絡は省こうと考えている。	ア	[中]情報セキュリティポリシー [小]基本方針 **※経営戦略が変更になったら、「情報セキュリティの基本文書」をもう一度見直すことは、必須である。かつ、変更した場合は、各部署に伝達することも必要である。**

(2)　ネットワークインフラセキュリティ

No.	タイプ	問題	選択肢	正解	ターゲット 備考（※印）
2-01	1	あるインターネットショッピングサイトにおいて、顧客がショッピングをする際、クレジットカードで決済する運用を行う。その際、利用者がクレジットカード番号を入力して、サーバ側に送信するシステムである場合に、一般的に利用される暗号通信システムとして適切なものを選択せよ。	ア．SSH イ．SSL ウ．VPN エ．S/MIME	イ	[中]VPN
2-02	1	WEPによる暗号化に使われる秘密鍵方式はどれか。	ア．RC4 イ．AES ウ．DES エ．RSA	ア	[中]無線LAN
2-03	1	無線LANにおける認証用プロトコルとして、最近普及が進みつつある規格は次のうちのどれか。	ア．IEEE 1394 イ．IEEE 802.3 ウ．IEEE 802.1x エ．IEEE 802.11b	ウ	[中]無線LAN [小]認証
2-04	2	ネットワーク上でアドレス変換を行うことによるセキュリティ面からの利点として、正しくないものはどれか。	ア．実際のクライアントで用いているIPアドレスを外部から隠蔽することにより、外部からの攻撃を受けにくくする。 イ．複数のクライアントからのアクセスを1つのグローバルIPアドレスからのアクセスの形で利用することにより、利用時の匿名性を高める。 ウ．アドレス変換を行うルータを起動する毎に異なるグローバルIPアドレスが割り当てられるため、特定のIPアドレスを狙った攻撃が行いにくい。 エ．アドレス変換の前後で異なるポート番号を利用することができるため、外部からの特定ポートを狙った攻撃が行いにくい。	ウ	[中]ネットワーク設計技術 [小]アドレス変換
2-05	2	パケットフィルタリングの機能としてもっとも適切なものを選択せよ。	ア．IPアドレスやポート番号などの識別子を解析し、パケットの通過／遮断を制御する。 イ．ブラウザとWWWサーバの間で代理要求/代理応答の役割をしている。 ウ．パケットフィルタリングの導入により、ウイルス感染を防ぐことが可能である。 エ．パケットフィルタリングでは、外部からの不正アクセスを制限することはできるが、内部から外部へのアクセスの制限はできない。	ア	[中]ネットワークアクセスコントロール
2-06	2	ポートベースVLANの説明のとして適切なものは、次のうちのどれか。	ア．さらにプロトコルベースVLANとサブネットベースVLANの2つに区分される。 イ．IPアドレスを基準にVLANを構成する方法である。 ウ．MACアドレスを基準にVLANを構成する方法である。 エ．スイッチングハブの接続口を基準にVLANを構成する方法である。	エ	[中]ネットワークアクセスコントロール [小]ポートベースVLAN

No.	タイプ	問題	選択肢	正解	ターゲット 備考（※印）
2-07	2	IPsecの機能に関する記述として、最も適切なものを選択せよ。	ア．暗号化には公開鍵暗号化方式だけを利用する。 イ．IPsecでは、アプリケーションに無関係に暗号通信が可能である。 ウ．IPsecを利用するためには、アプリケーションの修正が必要である。 エ．IPsecでは、認証アルゴリズムも備えており、第三者のなりすまし行為を防ぐことができる。	イ	[中]VPN
2-08	2	SSLを用いたVPN（SSL-VPN）の一般的な特徴についての説明として、正しくないものは次のうちのどれか。	ア．途中経路にNATなどのアドレス変換が行なわれても通信可能である。 イ．アプリケーションで使えるプロトコルはHTTPのみである。 ウ．途中のファイアーウォールでは、SSLポート(443番)が開いていればよい。 エ．クライアントにSSLに対応しているブラウザを使う場合は、特に新たなソフトウエアは必要ない。	イ	[中]VPN [小]SSLによるVPN装置
2-09	2	無線LANを利用する際のセキュリティを高める方法として、以下のうちで正しくないものはどれか。	ア．128bit長の鍵を用いたWEPを設定することにより、通信内容を暗号化する。 イ．無線LAN装置に予め登録したMACアドレス以外からの接続は拒絶するように設定する。 ウ．通信路上で使用するパスワードには十分な長さと記号を含めたものを用いることにより、パスワードの解読を困難にする。 エ．ESS-IDを指定しないアクセスは拒絶するとともに、ESS-IDには利用者や組織名を連想させない文字列を使用する。	ウ	[中]無線LAN
2-10	3	ネットワークの構築･運用における留意点として不適切なものを選択せよ。	ア．DMZには、グローバルIPアドレスを設定され、外部クライアントからの要求がファイアーウォール経由で到達するために、不正アクセスのリスクは小さくなるが、、公開サーバのアクセス監視は必要である。 イ．スイッチのＶＬＡＮ機能によって分割されたＬＡＮのグループは、別々のネットワークグループとして運用管理できる。 ウ．グローバルIPアドレスとプライベートIPアドレスの使い分けによって、内部サーバのログ監視業務を省略することができるため、効率が良い。 エ．IPマスカレードは、内部ネットワークで利用するIPアドレスやポート番号が隠蔽できる為、内部の端末のIPアドレスを不正利用されるリスクを軽減できる。	ウ	[中]ネットワーク設計技術

(3)　アプリケーションセキュリティ

No.	タイプ	問題	選択肢	正解	ターゲット 備考（※印）
3-01	1	クロスサイトスクリプティングについて正しくないものを選択せよ。	ア．サイトをまたがってスクリプトを転送してクライアントの情報を漏洩するものである。 イ．REFERERヘッダー、フォームフィールドやCookieの内容を信用するのは、Webアプリケーションのセキュリティとして正しい。 ウ．　Javaスクリプトの機能を使い、クライアント側のクッキー情報などを搾取するものである。 エ．HTMLのCGIへの入力の確認表示で、タグ情報(<>で囲まれた文字列)を表示してはならない。	イ	[中]Webサーバに対する脅威 [小]Webアプリケーションに対する攻撃
3-02	2	SQLインジェクションを利用した攻撃について適切な解説文を選択せよ。	ア．リクエストに SQL コマンドを入力し任意のSQLコマンドを実行させることができる。 イ．SQLサーバの脆弱性をついて管理者権限を奪うことを目的としている。 ウ．SQLコマンドを利用してサイトを踏み台にし他のサイトを攻撃できる。 エ．SQLインジェクションではデータの取得を目的としている。	ア	[中]Webアプリケーションに対する脅威 [小]Webアプリケーションに対する攻撃
3-03	2	Webサーバとブラウザ間を暗号化するSSLに関しての記述で明らかに間違っていると思われるものを選択せよ。	ア．SSLには暗号強度の違いがいくつかあり、セキュアに利用するためには強度の高いものを利用する。 イ．SSLではサーバ認証、クライアント認証も行っている。 ウ．SSLでは公の認証機関の発行した証明書がないと利用できない。 エ．最近はブラウザ間での通信のみにとどまらずVPNでの利用などにも使われている。	ウ	[中]Web関連プロトコルの基礎知識 [小]SSL/TLS **※自製の証明書を使ってSSLのサイトを構築することも可能である。**
3-04	3	Webサーバのアクセス権の不備によって発生する可能性のある問題を選択せよ。	ア．適切に利用されないためディスク容量の浪費が発生する。 イ．パフォーマンスの低下を招く。 ウ．意図しないファイルの公開により情報漏洩の危険性がある。 エ．同時アクセス数が制限されサービスレベルの低下が起こる。	ウ	[中]Webサーバのセキュリティ対策 [小]ファイル/ディレクトリのアクセス権の設定
3-05	2	Webサーバから発行され、クライアント側に保存されるCookieに関する記述として正しいものを選択せよ。	ア．Cookieに保存される情報は容易に解読できないため特別な配慮はいらない。 イ．Cookieは設置したサーバからのみコントロール可能であるので、不正に取得されることは考慮しなくてもよくできている。 ウ．クロスサイトスクリプティングなどにより不正にCookieを取得されるおそれがある。 エ．Cookieは個々人のものであるので他人は利用できない。	ウ	[中]Webブラウザのセキュリティ
3-06	2	クライアントユーザーが考慮すべきWebブラウザ(ブラウジング時)の対策として間違っているものを選択せよ。	ア．最新のパッチを適用する。 イ．通常の通信(HTTP)ではデータの暗号化がされていないことを意識する。 ウ．ActiveXで「実行しても安全」とされているものは安全性が保証されている。 エ．不用意にリンクをクリックしない。	ウ	[中]Webブラウザのセキュリティ

No.	タイプ	問題	選択肢	正解	ターゲット 備考（※印）
3-07	1	インターネットに接続されるメールサーバにおいて、発信者アドレスを偽ってスパムなどの用途に不正に使われないようにするには、どのような対策が有効であるか。	ア．第三者中継を許可しないように設定する。 イ．ユーザのメールボックス容量を大きくする。 ウ．メールサーバと違うドメインへのメール発信を制限する。 エ．登録アカウントを最低限にする。	ア	[中]メールサーバに対する脅威
3-08	1	通信経路においてメール盗聴防止のために、有効な手段を選択せよ。	ア．メール本文を添付ファイルにし圧縮して送る。 イ．HTMLメールにて送る。 ウ．メッセージを暗号化する エ．署名をほどこす。	ウ	[中]メールサーバのセキュリティ対策 [小]盗聴対策
3-09	1	DNSサーバにおいてマスタサーバとスレーブサーバ間で更新された情報をやりとりすることを何というか？	ア．ゾーン転送 イ．データエクスチェンジ ウ．キャッシュ同期 エ．データダウンロード	ア	[中]DNSサーバに対する脅威
3-10	2	DNSサーバの持つ脅威、脆弱性について誤ったものを選択せよ。	ア．DNSサーバとして広く使われているBind自体の脆弱性が多く報告され攻撃の対象となることが多い。 イ．ゾーン転送に対する制限を設定しておらずネットワーク、ホスト情報などを漏洩させることがある。 ウ．DNSのキャッシュ情報を不正に操作することで異なったサイトへ誘導が可能になる。 エ．セカンダリDNSサーバに格納されている名前情報が漏洩してしまう。	エ	[中]DNSサーバに対する脅威 **※セカンダリDNSサーバは、もともと公開されている。**

(4)　OS セキュリティ

No.	タイプ	問題	選択肢	正解	ターゲット 備考（※印）
4-01	2	【Unix】【Windows】 不正アクセスの証拠保全のために行う「ログオンイベントの監査」はどのように行ったらよいか、最も適切なものを選択せよ。	ア．辞書攻撃やブルートフォース攻撃を検知するため、「失敗」を記録し、1つのIDに多量の失敗ログが記録されていないか監査を行う。 イ．パスワードの漏洩や認証が回避された場合に備え、「失敗」だけでなく「成功」も記録する。 ウ．「失敗」を記録すると大量のログが発生し、監査しきれないばかりか最大ログサイズに達したために古いログが上書きされる恐れがあることから「成功」のみ記録する。 エ．不正アクセスはどこから行われるか分からないため、オブジェクトへのアクセスはすべてログに記録しなければならない。	イ	[中]ログ管理
4-02	2	【Unix】 サーバで起動するサービスの実行権限について適切なものを選択せよ。	ア．重要なサービスは、サービスの停止を極力避けるため、管理者権限で実行する。 イ．重要なサービスは管理者のみが設定を変更できるようにするため、管理者権限で実行しなければならない。 ウ．不正アクセスにより権限を奪われた場合に備え、できるだけ低い実行権限で起動し、権限を奪われた場合の被害を少なくする。 エ．サービスの脆弱性を突いた攻撃コードを含むアクセスを受けた場合に、踏み台にされたサイトへ被害が拡大しないよう、できるだけ低い実行権限で起動する。	ウ	[中]サービスの管理 [小]一般ユーザでのデーモンの起動
4-03	1	【Windows】 現在システムに適用済みのパッチと、マイクロソフトのWebサイトで公開されている公開状況データベースを照合し、適用されていないものをリストアップするツール名を選択せよ。	ア．HFNetchk イ．Hotfix ウ．MSTK エ．Qchain.exe	ア	[中]パッチ適用管理 [小]HFNetchk ※MSTK**の中に**HFNetchk **がある、**Qchain.exe**は、**Hotfix**間の整合性をチェックし、レベルダウンが起きないように監視するツール**
4-04	2	【Windows】 社内での利用者が多い、重要な業務アプリが稼動するサーバにおける安全なパッチ適用策として、もっとも適切なものを選択せよ。	ア．WindowsUpdateの自動更新機能によって、常に最新の修正モジュールを常に適用するように設定する。 イ．LAN上にあるSUS（SoftWare Update Service）サーバなどから、必ず検証済みの修正モジュールを適用するよう設定する。 ウ．更新によるインターネット接続の帯域が集中することなく修正モジュールを適用するよう設定する。 エ．更新によるインターネット接続の帯域が集中することなく修正モジュールを適用するよう設定する。	イ	[中]パッチ適用管理 [小]Windows-Update

No.	タイプ	問題	選択肢	正解	ターゲット 備考（※印）
4-05	2	【Unix】ftp，rcp，telnet SSHの4種類のサービスについて、 外部ネットワークを経由して利用した場合に情報漏洩やなりすましが生じる可能性が大きい順に並べたものは、次のうちのどれか。	ア．ftp ＞ rcp ＞ SSH ＞ telnet イ．rcp ＞ telnet ＝ ftp ＞ SSH ウ．rcp ＞ ftp ＞ telnet ＝ SSH エ．telnet ＞ ftp ＞ SSH ＞ rcp	イ	[中]サービスの管理 [小]サービスの制限とアクセス制御
4-06	1	【Windows】 ディスク自体の暗号化、HDDの盗難対策（復号鍵は共有）NTFSディレクトリがユーザIDによるアクセス制御の他に備える、権限を持たない利用者によるアクセスに対する機密性対策は何か。	ア．EFS イ．ESS-ID ウ．CIPHER エ．AES	ア	[中]ファイルシステム管理 [小]暗号化ファイル（EFS） **※ CIPHER はEFSで暗号化に使用するコマンド**
4-07	1	【Unix】 暗号化されたパスワードハッシュを全て読み取り可能な/etc/passwdからrootにしか読み取れない/etc/shadowに移動することでシステムセキュリティを向上させる機能は何か。	ア．シャドウパスワード イ．ワンタイムパスワード ウ．CHAP (Challenge Handshake Authentication Protocol) エ．Kerberos認証	ア	[中]アカウント管理 [小]シャドウパスワード
4-08	3	【Unix】【Windows】 パスワードによる認証の管理は不正アクセスの防止に必須であるが、サーバ側の仕組みと設定する側の利用者の利便性を考慮して、強固なパスワード設定を徹底するのに最も適切なものを選択せよ。	ア．意味の無い文字、数字と記号を組み合わせたパスワードの設定を全社員に教育した上で、定期的変更も含めてサーバ側で強制し徹底する。 イ．十分な強度を有し、覚えやすいパスワードの作成方法や、他人に利用されないためのパスワードの管理方法などについて、利用者への教育を行う。 ウ．インターネット側からの不正アクセスに晒されるサーバのユーザIDに関しては厳密な管理を行う必要があるが、社内の一般利用者のパスワードは各自の自由に任せてよい。 エ．パスワードは十分な強度を持つパスワードを最初に配布した方が自分で設定させるより効果が高い。	イ	[中]アカウント管理 [小]強いパスワード/弱いパスワード **※エは紛らわしいが、配布した管理側が把握していることに機密性上の問題がある**
4-09	2	【Windows】 パーソナルファイアーウォールをクライアントPCに導入することで期待できる効果は何か。	ア．バックドアへのアクセスやスパイウェア等による個人情報の漏洩を検知できる。 イ．PCのなりすまし利用を未然に防ぐことができる。 ウ．主にパケットフィルタリング型とアプリケーションゲートウェイ型に分類できる。 エ．ウイルス、ワームの検知、駆除を主に行う。	ア	[中]クライアントセキュリティ管理 [小]パーソナルファイアーウォール
4-10	1	【TrustedOS】 管理者によって定められた方針に基づいたアクセスを強制し、ユーザによる任意の権限の受渡しが許されないアクセス制御手法は何か。	ア．ACL イ．DAC ウ．MAC エ．RBAC	ウ	[中]強制アクセス制御の概念（MAC）

(5)　ファイアーウォール

No.	タイプ	問題	選択肢	正解	ターゲット 備考（※印）
5-01	1	Webサーバやメールサーバなど、インターネットに公開する必要のあるサーバは、ファイアーウォールを介し、社内LANセグメントやインターネットセグメントとは別のセグメントの上に置かれることが多い。このセグメントの名前として最も適切なものはどれか。	ア．NAT イ．VPN ウ．DMZ エ．SSL	ウ	[中]ファイアーウォールの導入･運用
5-02	2	ファイアーウォールの設置目的として最も適切でないものはどれか。	ア．インターネットから公開WWWサーバへの不正なアクセスを防止するために設置する。 イ．一般社員による不正アクセスや誤用を防ぐため、社内で機密性の高い情報を処理するサーバやセグメントを分離する目的で設置する。 ウ．組織のセキュリティポリシーに従って、社内から利用できるインターネット上のサービスを制限するために設置する。 エ．インターネット経由でのコンピュータウイルスの感染を防ぐために設置する。	エ	[中]ファイアーウォールの導入･運用
5-03	1	社内からインターネットへのWWWのアクセスを行うとき、ファイアーウォールで通信を許可する必要性が最も薄いサービス(プロトコル)は以下のうちどれか。	ア．Domain (DNS) イ．HTTP ウ．SMTP エ．HTTPS	ウ	[中]ファイアーウォールの導入･運用 **※アはURIの名前解決に必要。**
5-04	2	ダイナミックNAT(実装の違いにより、NAPT, IP マスカレードなどと称する場合もある)の特徴として、最も適切なものはどれか。	ア．内部ネットワークからインターネットにアクセスする際に、多数のPCのプライベートアドレスを予め指定したグローバルアドレスに変換してアクセスさせることができる。 イ．内部ネットワークやDMZ上に設置したサーバをインターネットに公開する際に使用されることが多い。 ウ．変換された後のアドレスは常にグローバルアドレスでなければならないので、組織の内部に設置されたファイアーウォールで使うことは難しい。 エ．内部ネットワークのPCから外部ネットワーク上へアクセスする際に、発信元ポートを変換せずに発信元アドレスを変換することができる。	ア	[中]NAT
5-05	2	パケットフィルタリングにおいて使用される技法の一つにIngress Filtering がある。この説明として正しいものを以下の選択肢から選べ。	ア．インターネットから内部へのパケットが着信した場合、アクセスを全て拒否する。 イ．内部で使用しているプライベートアドレスをソースアドレスとして持つパケットがインターネットから着信した場合、アクセスを拒否する。 ウ．インターネットで使用されるグローバルアドレスをソースアドレスとして持つパケットが内部から着信した場合、アクセスを拒否する。 エ．内部からインターネットへのパケットが着信した場合、アクセスを全て拒否する。	イ	[中]ネットワークアクセスコントロール **※ウは**Egress (Exgress) Filtering **の説明。**

No.	タイプ	問題	選択肢	正解	ターゲット 備考(※印)
5-06	3	ファイアーウォールのログ解析に関する以下の記述のうち、最も適切と思われるものはどれか。	ア. インターネット上の同一のアドレスから、DMZ上WWWサーバに対し、宛先ポート番号の異なるTCPの通信が数秒間に1000件以上発生していたため、ポートスキャンが発生していたと判断した。 イ. 内部セグメントにおいて、使用していないはずの169.254.81.92 というアドレスからARPパケットが送出されていたので、外部からのIPスプーフィング攻撃(IP詐称攻撃)が発生していたと判断した。 ウ. インターネット上の異なったIPアドレスから、1~2分の間に内部の特定のホストに対して ICMP Time exceeded と ICMP Port Unreachable のパケットが送出されていたため、ICMPを用いたDoS攻撃を受けた可能性が高いと判断した。 エ. DMZ上の公開メールサーバから外部へのSMTPの通信が通常の20倍以上発生していることが判明したが、もともと許可している通信であるためメールサーバには問題がないと判断した。	ア	[中]ファイアーウォールの導入･運用 **※イはDHCPでIPアドレスを取得できなかった場合に発生する現象。DHCPクライアントを起動しているPCがないかどうか確認する。ウは内部からtracerouteを行った典型的な例。エは不正中継を疑い、メールサーバのログを確認するべきである。**
5-07	1	一部のVPNの通信やインスタントメッセージなどのアプリケーションでは、ファイアーウォールでNATを使用すると通信が正常にできなくなる場合がある。この問題点を解決する機能を総称して何というか。	ア. NATトラバーサル イ. ステートフル･インスペクション ウ. ダイナミックNAT エ. IPマスカレード	ア	[中]NAT
5-08	2	ファイアーウォールでのアクセス制御に関する記述のうち、最も適切なものはどれか。	ア. 公開FTPサーバに対してPUTコマンドを使用できないようにするため、サーキットレベルゲートウェイの機能を使用した。 イ. ステートフル･インスペクションの機能を持つファイアーウォールでは、クライアントからサーバへのアクセス要求に関するルールだけでなく、サーバからクライアントへの応答に関するルールも管理者が予め記述しておかなければならない。 ウ. パケットフィルタリングを使用すると、特定のIPアドレスからのアクセスを全て拒否することが可能になる。 エ. アプリケーションゲートウェイ(Proxy)を使用する際には、必ずNAT(ネットワークアドレス変換)を併用しなければならない。	ウ	[中]ネットワークアクセスコントロール
5-09	1	通常、外部に対して公開することはなく、アプリケーションゲートウェイではサポートされないサービス(プロトコル)を以下の選択肢から選べ。	ア. SMTP イ. HTTP ウ. FTP エ. SNMP	エ	[中]ネットワークアクセスコントロール

No.	タイプ	問題	選択肢	正解	ターゲット 備考（※印）
5-10	2	アプリケーションゲートウェイ(プロキシ)の特徴を述べた以下の文章の中で、最も適切でないものはどれか。	ア．アプリケーションゲートウェイを用いて中継したメールの発信元(From)アドレスと送信先(To)アドレス、題名(Subject)をログに記録することは原理上可能である。 イ．パケットフィルタリングと比較してアクセス制御に要するオーバヘッドが小さく、相対的に高速な処理が可能である。 ウ．製品によっては、使用したいアプリケーション(プロトコル、サービス)がサポートされていないことがあるため、導入前には入念な確認が必要である。 エ．一般的にはクライアントがプロキシのアドレスを指定し、クライアントからプロキシ、プロキシからサーバへといった形でアクセスが中継されるが、クライアントはプロキシのアドレスを指定せずにサーバに直接アクセスできる形を取れる製品もある。	イ	[中]ネットワークアクセスコントロール

(6)　侵入検知

No.	タイプ	問題	選択肢	正解	ターゲット 備考（※印）
6-01	1	侵入検知システムの基本的役割は何か、最も適切なものを選択せよ。	ア．区分けされたセグメントごとにパケットをルーティングする。 イ．通信を暗号化し機密性を確保する。 ウ．不正アクセスを検出し、管理コンソールに通知する。 エ．アクセス制御（コントロール）する。	イ	[中]侵入検知システムの導入・運用 [小]ファイアーウォール（ログ）との違い
6-02	2	通常外部（インターネット）と内部にはファイアーウォールが設置されアクセス制御を行っている。そこに侵入検知システムを設置する際、ファイアーウォールの設定について考慮すべき点を答えよ。	ア．侵入検知システムはファイアーウォールのアクセス制御機能を補完するため、侵入検知装置を導入すればファイアーウォール側のフィルタリングを厳密に設定する必要はなくなる。 イ．侵入検知システムはファイアーウォールと同等のアクセス制御機能を持つため、侵入検知システムを導入すればファイアーウォールは外して問題ない。 ウ．侵入検知システム側でログを採取しているため、ファイアーウォール側でログを取る必要はなくなる。 エ．侵入検知システムはアクセス制御機能をもたないため、ファイアーウォール側でのフィルタリング設定は導入前と変わらずにしておく必要がある。	エ	[中]侵入検知システムの導入・運用 [小]ファイアーウォール（ログ）との違い **※不正アクセスに対する侵入検知装置とファイアーウォールとの機能の違いを明確化する。**
6-03	1	侵入検知システムには検知方式、形態の違いにより種類がわかれるが、システム上に保存されるログを監視(ログファイルモニター)して不正アクセスの検出を行う種類の侵入検知システムの名称を答えよ。	ア．ホストベース型 イ．ネットワーク型 ウ．ハニーポット エ．改竄検知	ア	[中]検出方法 [小]ログファイルモニター
6-04	2	ネットワーク型侵入検知システムは、同じセグメント内の通信を監視するために検知エンジンのNIC（ネットワークインターフェースカード）をプロミスキャスモードへ変更するようになっている。プロミスキャスモードの説明として適切なものを答えよ。	ア．マルチキャスト通信のみを取り込むNICのモードを意味する。 イ．全ての通信を取り込むNICのモードを意味する。 ウ．ユニキャスト通信のみ取り込むNICのモードを意味する。 エ．何の通信も取り込まないNICのモードを意味する。	イ	[中]侵入検知システムの機能 [小]プロミスキャスモード
6-05	2	侵入検知システムには、不正アクセス受信時の動作としていくつかの防御機能を有する。防御機能の説明として適切なものを答えよ。	ア．防御機能は、どのような状況下でも有効に機能するため、検出した攻撃は必ず防御できる。 イ．TCPリセット機能は必ず有効に機能する。 ウ．いかなるルータデバイス（ルータもしくはファイアーウォール）との連携も必ず有効に機能する。 エ．侵入検知装置の防御機能により攻撃を100%防げるものではない。	エ	[小]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） **※侵入検知システムの目的は「不正アクセス検出」であり防御でないことを理解させる。**
6-06	1	侵入検知システムでは不正アクセスを検出するアルゴリズムとして異常検出方式と不正検出方式がある。異常検出の検出アルゴリズムでないものを答えよ。	ア．パターンマッチ イ．定量分析（しきい値モデル） ウ．統計的手法（しきい値学習モデル） エ．ニューラルネットワーク	ア	[中]検出アルゴリズム [小]異常検出及び不正検出

No.	タイプ	問題	選択肢	正解	ターゲット 備考(※印)
6-07	2	不正侵入によるホームページ書き換えなど、第三者によるデータの改ざんを検出すべく改竄検知(System Integrity Verifiers)システムが利用される。改竄検知システムの説明として最適なものを答えよ。	ア. データの完全性をチェックするために、データ全体のサイズを記録しておく。 イ. データの完全性をチェックするために、データ全体のハッシュ値を計算し、記録しておく。 ウ. データの完全性をチェックするためデータの変更日時を監視する。 エ. データの完全性をチェックするためにデータの所有者(Owner)を記録しておく。	イ	[中]侵入検知システム [小]改竄検知
6-08	3	侵入検知システムは、「正常な通信を不正アクセスとして検出してしまうFalse-Positive」と「不正な通信を不正アクセスとして検出できないFalseNegative」といった誤検出という現象がある。侵入検知システムを運用するにあたっては検出されたものが誤検出でないかを切り分ける作業を効率良く行うことがポイントとなる。False-Positiveについて、切り分けのポイントの説明として適切でないものを答えよ。	ア. シグネチャ名からFalseNegativeを判別する。 イ. 検出された不正アクセスの詳細(なぜ検出されたのか)を十分に把握しておく。 ウ. 宛て先ホストがどういったサービスを提供しているものか十分に把握しておく。 エ. 送り元ホストが内部であった場合、内部から送信されるサービス(通信)の概要を十分に把握しておく。	ア	[中]侵入検知システムの導入・運用 [小] FalseNegative と FalsePositive **※侵入検知システム運用において作業稼動を減らすために誤検出の切り分けは重要なポイントとされる。特に** FalsePositive **は必ず発生する誤検出であり、数量も多いため切り分けが即座にできるよう不正アクセスの詳細と監視している環境において** FalsePositive **を初期運用時に確認しておく必要がある。**
6-09	3	侵入検知システムでは検出された不正アクセスの履歴をログファイルに保存する機能がある。管理者が日々ログ解析を実施することが必要とされている理由として適切でないものを答えよ。	ア. シグネチャポリシーのチューニングを実施する際、ログ解析の結果から、ポリシー変更の根拠となる情報(例えば、誤検出洗出し、監視レベルを下げても良いシグネチャの検出、防御・告知方法等の適切な対応設定)を洗い出すことができるため。 イ. ログを解析するプロセスの中で相関分析を行い、検出された複数(数多く)の不正アクセスの中から、対応優先順位の高いものを探し出すことができるため。 ウ. 監視している環境の傾向を把握しておくため。 エ. ログを解析するプロセスの中でファイアーウォールのアクセス制御が適切に機能しているか確認できるため。	エ	[中]侵入検知システムの導入・運用 [小]ログ解析

No.	タイプ	問題	選択肢	正解	ターゲット 備考（※印）
6-10	3	侵入検知システムは、高度な運用スキルが必要とされる。管理者が最優先で日々行わなければならない項目としてあてはまらないものを選択せよ。	ア．情報セキュリティ（脅威、脆弱性、最近発生したインシデント、リリースされた修正パッチ情報）に関する情報の収集。 イ．監視している環境の脆弱性有無の確認及び対策指針の立案 ウ．侵入検知システムの防御機能により、脆弱性を有するシステムをどこまで守ることができるのか、その検証と確認作業を行う。 エ．シグネチャポリシーに関するカスタマイズ・チューニングの検討	ウ	[中]侵入検知システムの導入・運用 [小]運用体制とインシデント対応 **※侵入検知システムの役割はあくまでも「不正侵入の検出」であり、管理者としてはどのようにすれば侵入検知システムによる不正アクセス検出の稼動を下げられるか、効率的に活用できるかを日々検討すべきである。侵入検知システムの防御機能を活用するまえに監視対象（ネットワーク、サーバ）自身への対策を行うことが優先順位としては高いことを認識しておく。**

(7)　ウィルス

No.	タイプ	問題	選択肢	正解	ターゲット 備考（※印）
7-01	2	最近のウイルス感染の傾向について適切なものを選択せよ。	ア．OS自体の脆弱点を攻撃するウイルスが発生したためLANやインターネットの接続にも注意が必要である。 イ．ウイルスはメールに添付されてくるモノが多いので添付ファイルを不用意に実行しなければ安全である。 ウ．ウイルスは毎月定期的にリリースされる。 エ．ウイルス対策ソフトをインストールしていればとりあえず被害は防げる。	ア	[中]予防ポリシ [小]流行の傾向と予測 **※ 2003 年夏のBlaster 以降、WindowsのOS自体の脆弱性を狙ったウイルス、ワームが多く確認されている。ウイルス対策ソフトも定義ファイルを更新しないと安全とは言えない。**
7-02	2	ウイルス対策ソフトの利用にあたっての注意点として適切なものを選択せよ。	ア．ウイルス定義ファイルを最新にする。 イ．必要時以外は起動しないようにする。 ウ．常に監視を行うためにPCを常時起動しておく。 エ．圧縮されたファイルはチェックできないのでできるだけファイルの圧縮は避ける。	ア	[中]予防ポリシ [小]定義ファイル管理
7-03	1	Webブラウザ、メーラー、エクスプローラーなどでページ、メッセージ、ファイルの表示だけでウイルスのコードが実行される機能は何と呼ばれているか？	ア．ダイレクトファンクション イ．シングルアクション ウ．マルチファンクション エ．ダイレクトアクション	エ	[中]発病 [小]ウイルスの複合化 **※ Nimda 以降 IE, OEの脆弱性を利用してダイレクトアクション機能を利用したウイルスが増えている。**
7-04	2	ウイルス感染と思われる兆候が見られたときの対応としてもっとも適切なものを選択せよ。	ア．ネットワークから切り離し、ウイルス対策ソフトを利用してチェックする。 イ．不審な動きを止めるために一度再起動を行ったあとでウイルス駆除を実施する。 ウ．ウイルス感染の現象が確認できるまでは特別に対策をしなくてもよい。 エ．WindowsUpdateをすぐに実行する。	ア	[中]感染後のポリシ [小]駆除方法と手順
7-05	2	事前のウイルス対策のために、企業のとる対策として適切なものを選択せよ。	ア．外部からの侵入対策としてゲートウエイ型ウイルス対策装置を導入、内外からの全通信をスキャンする。同時にLANに繋がる全てのPCにもウイルス対策ソフトを導入する。 イ．個人所有のPCや外部からの持込PCは会社資産ではないため、管理対象外とする。持込PC等からウイルスが社内LAN全体に伝播した場合、持込んだ個人の責任とする。 ウ．組織的対応力を高めるため、ウイルス情報などの噂は入手できた時点で全社員に告知する。 エ．最近はクライアントPCでの被害が多いため、社内LANに接続するPC全てにウイルス対策ソフトを導入すれば対策は十分である。	ア	[中]予防ポリシ [小]システム管理 **※個人所有のPCは社内LANに接続させない施策や、ユーザ教育実施などを行うことは対策として有効である。**

No.	タイプ	問題	選択肢	正解	ターゲット 備考（※印）
7-06	1	ファイルに感染するたびに、ウイルス自体をランダムな暗号化コードを使用して、暗号化するコンピュータウイルスは何型ウイルスと呼ばれているか。	ア．ステレス型ウイルス イ．ワーム型ウイルス ウ．ポリモーフィック型ウイルス エ．ファイル感染型ウイルス	ウ	[中]感染 [小]ウイルスの自己防衛機能 **※ウイルスを発見しにくくするために、ウイルス感染を隠す技術をステレスと呼ぶ。**
7-07	3	企業等の組織体でウイルスに感染した場合、駆除作業の手順として最善と思われるのものはどれか。（他の感染していない媒体からOSを起動し、アンチウイルスソフトを実行することが理想であるが、それが出来ないと仮定する。）	ア．感染したクライアントのインターネットケーブルを外し、Windowsをセーフティモードで起動。アンチウイルスソフトを用いてウイルスを駆除する。破損ファイルはバックアップより戻す。 イ．感染したクライアントのインターネットケーブルを外し、アンチウイルスソフトを用いてウイルスを駆除する。破損ファイルはバックアップより戻す。 ウ．感染したクライアントに対して、通常のOSモードでアンチウイルスソフトを実行させ、ウイルス駆除を行う。 エ．感染レポートの上がったファイルに対してのみ駆除を試みるかまたは、そのファイルを削除する。	ア	[中]感染後のポリシ [小]駆除方法と手順 **※ウイルスが発見された場合、該当ファイル以外にもウイルス感染している可能性があり、全体をチェックする必要がある。またネット接続されていると駆除しても再度感染する可能性がある。また起動しているソフトの種類は最小限とする。**
7-08	1	一般的なウイルスの定義項目に含まれない機能はどれか。	ア．自己伝播機能 イ．潜伏機能 ウ．攻撃機能 エ．発病機能	ウ	[中]種類 [小]ウイルスの機能構成 **※IPAのWebに記載されている内容より抜粋**
7-09	3	ログ集中管理の必要性に対するもっとも適切と思われる説明はどれか。	ア．各クライアントの情報を集中管理する事により、定義ファイル、スキャンエンジンおよびプロダクトのバージョン状況の把握が確かなものとなり、ウイルスに対する防御状況を適切に把握できる事となる。 イ．各クライアントの情報を集中管理することで、どのクライアントがアンチウイルスソフトを停止しているかなどの状況把握が可能となり、注意を与えやすい。 ウ．各クライアントの情報を集中管理することにより、PCにインストールされている他のアプリケーションとの衝突等の障害情報が把握し易くなる。よってアンチウイルスソフト開発メーカに対しそれらデータを提供しやすくなる。 エ．各クライアントの情報を集中管理することにより、ソフトのバージョンアップや定義ファイルのダウンロード等に対する管理の手間暇や経費を最小限に押さえる事ができる。	ア	[中]予防ポリシ [小]システム管理 **※集中管理により定義ファイルの配布等も一括でできるようになる。経費の削減とはなるが、真の目的は感染の防御および感染を最小限に押さえる事である。**

No.	タイプ	問題	選択肢	正解	ターゲット 備考（※印）
7-10	2	ウイルスの侵入を防ぐため、システム構築に関して述べている中で、最良と思われる説明はどれか。	ア．クライアントやサーバにアンチウイルスソフトをインストールするのみでよい。 イ．ゲートウェイ、メールサーバ、サーバや各クライアントにアンチウイルスソフトをインストールし階層的に防御する必要がある。 ウ．ゲートウェイとメールサーバにアンチウイルスソフトをインストールしておけば、インターネット経由で外部からウイルスが入り込まないので十分である。 エ．外部とはインターネット経由で接続されていないので、各クライアントにアンチウイルスソフトをインストールしておけばよい。	イ	[中]予防ポリシ [小]イントラネットの構築 **※内部での感染拡大を考慮し、内部での各クライアントサーバにアンチウイルスソフトをインストールしておく事は重要である。**

(8)　セキュアプログラミング技法

No.	タイプ	問題	選択肢	正解	ターゲット 備考（※印）
8-01	2	アプリケーション開発の際に、後からセキュリティを追加するのは適切な方法ではないが、その理由として誤っているものはどれか。	ア．新たなバグを作りこむ可能性が高くなるから。 イ．既存の機能の外部機能としてセキュリティを組込むことになる可能性が高いから。 ウ．既に実装したアプリケーションインターフェースを変更する可能性があり、インターフェースに依存したプログラムを壊す可能性があるから。 エ．セキュリティを追加することにより発生する仕様変更により、コストが高くなる可能性が大きいから。	ア	（すべて）
8-02	2	バッファオーバーフローが発生するには、様々な理由があるが、その説明として正しいものはどれか。	ア．スタック上に宣言されたバッファサイズより大きなデータをコピーすると、そのバッファが上書きされるために発生する。 イ．動的なヒープメモリのオーバーフローに関しては、静的なメモリのオーバーフローより発生しにくいため、それほど注意を払う必要はない。 ウ．UnicodeとANSIのバッファサイズの不一致により発生するバッファオーバーフローは、様々なプラットフォームに共通した問題である。 エ．バッファオーバーフローは、文字列処理で最も多く発生するが、strcpy関数等の安全な関数を使用することで防げる。	ア	[小]バッファオーバーフロー
8-03	2	Webアプリケーションを設計する際に注意すべき危険性に関して、正しい説明はどれか。	ア．クロスサイトスクリプティングは、主にサーバ側で特殊文字列を適切に変換していないことが原因でおこるため、Webブラウザから送られてきた特殊文字を適切にサニタイジングする必要がある。 イ．セキュリティ上の決定を下す場合には、REFERERヘッダー、フォームフィールドやCookieの内容を信用する。 ウ．ASPプログラムでは、データベース接続文字列等の機密情報を格納せずに、COMオブジェクトを使用してレジストリなどの機密性を有するリソースデータにアクセスするべきであるが、プログラムファイルのコメントに関しては特に注意をする必要はない。 エ．データベース駆動のアプリケーションでは、ユーザ自身が自分のデータを追加、更新できる権限を持たないため、管理者アカウントを利用すべきである。	ア	[中]Webアプリケーション
8-04	2	Perlで記述されたスクリプトを実行する際に、Taintモードが果たす役割は次のうちのどれか。	ア．実行時のセグメンテーション違反が発生するのを未然に検出し、警告する。 イ．リスト変数で保持し得る範囲を超えた場合を検出し、エラーを生じさせる。 ウ．スカラー変数とハッシュとの間で危険な参照や代入が行なわれている場合を検出し、エラーを生じさせる。 エ．外部から与えられたデータを保持する変数で、スクリプトが予期しない動作をする可能性を検出し、エラーを生じさせる。	エ	[小]Taintモード

No.	タイプ	問題	選択肢	正解	ターゲット 備考(※印)
8-05	1	クロスサイトスクリプティングの防止のためのサニタイジング処理の際に、次の文字のうちで考慮しなくてよいものはどれか。	ア. 文字「<」 イ. 文字「=」 ウ. 文字「&」 エ. 文字「"」	イ	[小]クロスサイトスクリプティング
8-06	2	Javaで安全なプログラミングをするためのルールとして適切でないものはどれか。	ア. オーバーライドしないメソッドは, finalメソッドにする。 イ. 外部クラスからアクセスされないメソッドは, privateメソッドにする。 ウ. 継承クラスからしかアクセスされないメソッドは, abstractにする。 エ. 永続化する必要のない変数は, transient変数にする。	ウ	[中]Java
8-07	2	入力に際してバッファオーバーフローを避けるために心がけるべき手法は次のどれか	ア. 入力バッファを動的に確保し、オーバーランが起っても、プログラムコード領域が破壊されないようにする。 イ. 入力バッファは出来るだけ大きく取って、常識的な入力バイト数程度ではオーバーランしないようにする。 ウ. 入力値の取得するためには、入力バッファサイズを指定できる関数を使用し、さらに入力値に関して常にサイズチェックを行うべきである。 エ. 入力ループの折り返しのステートメントでデータのデリミッターを識別できるようにする。	ウ	[小]バッファオーバーフロー
8-08	1	次に示すC言語の文字列処理関数のうち、バッファオーバーフローの原因に最もなりにくいものはどれか。	ア. gets イ. strcat ウ. fscanf エ. fgets	エ	[中]C/C++ [小]危険な関数
8-09	2	サブシェルの呼び出しについて正しい記述はどれか。	ア. 外部から与えられた文字列をsystem()の引数としてコマンドを実行させるプログラミングは、どのように危険なコマンドが文字列として与えられるかどうかわからないので、決して行ってはならない。 イ. 外部から与えられた文字列をsystem()の引数として使う前に十分に内容をチェックして危険なコマンドが含まれていないことが確認できたならば、自由に使ってよい。 ウ. 文字列で与えられるコマンドが絶対パスで指定されていればsystem()の引数として使っても良い。 エ. system()の引数として働くコマンドを使用する場合、コマンドの所在ならびに正当性および安全性を確認する。	エ	[中]C/C++ [小]サブシェルの呼び出し

No.	タイプ	問題	選択肢	正解	ターゲット 備考（※印）
8-10	2	メモリリークについて正しいものはどれか。	ア．メモリリークとは、プログラムが利用したデータ領域がそのプログラムが終了したあとで別のプログラムから参照されることをいう。 イ．メモリリークとは、本来ローカル変数として定義されるべき変数がグローバル変数として定義されたために設計時の想定外の関数からもアクセスできてしまうことをいう。 ウ．メモリリークとは、動的に確保したメモリを解放しないことで、コンピュータ資源を消費し尽くして異常が起こる等の問題を引き起こすことをいう。 エ．メモリリークはシステムの動作を不安定にするという意味では避けるべきであるが、情報セキュリティ上の脅威とはならないので、セキュリティ対策上の問題とは切り離して考えるのが正しい扱いである。	ウ	[中]C/C++ [小]メモリリーク

(9)　セキュリティ運用

No.	タイプ	問題	選択肢	正解	ターゲット 備考（※印）
9-01	2	管理対象のコンピュータに生じている異常を確認する手段として、次の中で優先度が低いものはどれか。	ア．起動されているプロセスやアプリケーションを確認する。 イ．CPUの負荷状況を確認する。 ウ．稼働中のOSのバージョンを確認する。 エ．登録されているユーザ一覧を確認する。	ウ	[中]定常運用時のセキュリティ確保 [小]モニタリング
9-02	2	パッチの適用に際して考慮すべき項目として、不適切なものはどれか。	ア．パッチのサイズの大きさにより、影響する範囲の大きさがが変わることがある。 イ．パッチの適用の順番を間違えると、先に適用したパッチの効果が失われることがある。 ウ．パッチを適用することにより、これまで動作していたアプリケーションが正しく動作しなくなることがある。 エ．パッチの中には、セキュリティホール対策としての効果が不十分であるとして、後日中身が更新されることがある。	ア	[中]セキュリティホール対策 [小]パッチの効果と副作用
9-03	2	データバックアップ作業に関して留意すべき事項のうち、不適切なものはどれか。	ア．データのバックアップ先として用いた媒体は、データの保存されている媒体と、同時に被災する可能性が少なくなるように離して保管するのがよい。 イ．暗号化されたデータをバックアップした媒体は、そのままでは中身のデータを第三者が読み取ることができないので、保管時のセキュリティは考慮しなくても良い。 ウ．データバックアップ中に何らかのトラブルが発生して媒体が利用できなくなる可能性を考慮すると、バックアップ用の媒体は複数組用意する必要がある。 エ．バックアップしたデータが正しく復元できるかどうかの確認を、適切なタイミングで定期的に行うことは重要である。	イ	[中]定常作業 [小]バックアップ・リストアの設定・実施
9-04	2	アカウント作成時に用いる仮パスワードの取り扱いに関して、セキュリティ確保の面から最も妥当なものは次のうちのどれか。	ア．仮パスワードは、ユーザが最初に利用する際にのみ必要となる暫定的なものなので、管理の手間を考えて全ユーザ共通のものでも差し支えない。 イ．ユーザに与えられた仮パスワードがパスワードとしてのセキュリティ強度を満たし、ユーザにとって覚えやすいものであれば、正式なパスワードとして使い続けても差し支えない。 ウ．仮パスワードは、ユーザに配布後すぐに変更することが前提なので、パスワードの強度は低くても問題はない。 エ．仮パスワードは、ユーザに配布後すぐに変更することが前提なので、パスワードとしてのセキュリティ強度を満たすものであれば、機械的に生成した覚えにくいパスワードでも差し支えない。	エ	[中]定常作業 [小]パスワード管理 **※一般論としての正解なので、組織によっては異なる可能性がある。**

No.	タイプ	問題	選択肢	正解	ターゲット 備考（※印）
9-05	2	セキュリティ向上のために組織のセキュリティ管理担当者が組織内ユーザに向けて行う以下のアナウンスのうち、不適切なものはどれか。なおユーザは自分が使用するPCの管理者権限を行使できるものとする。	ア．各ユーザが使用しているPCにセキュリティホールがあり、対策用パッチが公表されたことをアナウンスし、各ユーザに早急の対策を促す。 イ．適切なパスワードの設定と変更のあり方、パスワードを忘れた場合の対応方法について、ユーザを啓発するためのアナウンスを行う。 ウ．自組織で用いているIDSで検知できない不正アクセスの種類について示し、その危険性をアナウンスすることを通じてユーザに警戒を促す。 エ．電子メールを介して感染する新型のウイルスが発生し、自組織のメールサーバ上に設置されている対策ソフトウェアがそのウイルスに対応する前にウイルスと思しきメールが到着した可能性がある場合、ユーザにその旨をアナウンスして警戒を促す。	ウ	[中]ユーザ対応等 [小]ユーザへのアナウンス
9-06	2	セキュリティホールやパッチについての情報源として、次のうち参考にすべきではないものはどれか。	ア．行政や公的機関がその職務として情報提供を行っているサイト イ．セキュリティサービス事業者が、SSLなどサーバ認証が可能な形で情報提供しているサイト ウ．ソフトウェアベンダからの、緊急事態なので異例の形で対応する旨とともにパッチが添付された電子メール エ．ソフトウェアベンダがパッチのアップデート用にASP事業者と契約して提供しているサイト	ウ	[小]情報源の種類と特徴
9-07	2	ネットワーク運用を担当する者が、日常においてセキュリティ関連情報の情報源について把握しておくべきことのうち、不適切なものはどれか。	ア．情報の詳細度、精緻さ イ．情報の速さ ウ．情報提供者の多さ エ．情報の信頼性、正確さ	ウ	[小]情報源の種類と特徴
9-08	2	自組織内にコンピュータウイルス（以下ウイルスと表記）に感染した可能性があるPCがある。このときそのPC（対象PC）の管理担当者が講じるべき対策として、最も適切なものはどれか。	ア．二次感染源となるのを防止し、ウイルスによる破壊活動を防ぐため、直ちに対象PCの稼働を停止させ、電源を切る。 イ．直ちにウイルスを駆除するためのソフトウェアのインストールもしくはウイルス定義ファイルの更新を行い、ウイルスの早期駆除に努める。 ウ．二次感染源となるのを予防するため、対象PCを組織内ネットワークから切り離し、対策はネットワークを経由しない方法で実施する。 エ．対象PCに生じた異常はウイルスによるものとは限らないため、状況が明確になるまでそのまま様子を見る。	ウ	[中]異常時対応 [小]原因究明・トラブルシューティング

No.	タイプ	問題	選択肢	正解	ターゲット 備考（※印）
9-09	3	A社でサーバ管理についての運用権限を任されているP氏のもとへ、B社で同様の業務に従事しているQ氏から「新手の不正アクセスが流行している」との連絡があった。P氏の管理しているサーバ周辺では特に異常は認められない。このときP氏が直ちに講じるべき対策は次のうちのどれが最も適切か。	ア．信用できる情報かどうかわからないので、無視して何も対策しない。 イ．直属の上司にQ氏からの情報を伝え、判断を仰ぐ。 ウ．信頼できる情報源に、該当する不正アクセスに関する情報がないか確認する。 エ．直ちに担当のサーバを停止させて、万全を期す。	ウ	[中]異常時対応 [小]緊急時対応
9-10	3	A社は一般消費者向けオンラインショップを自前のサーバで運用している。あるとき、オンラインショップ用サーバで用いているOSのベンダから、OSのセキュリティホール対策のためのパッチ提供のアナウンスと、そのセキュリティホールを悪用したワームの発生のアナウンスが、ほぼ同時に伝えられた。A社の運用ルールでは、パッチを提供する際には、いきなり実運用環境に適用するのではなく、全く同じ構成からなるテスト環境に適用して悪影響のないことを確認した上で実運用環境に適用することになっているが、テスト環境での確認には通常2～3日かかる。なお、今回のセキュリティホールの対象は、このオンラインショップ用サーバで現在使用していないサービスを対象としたものであり、OSベンダの提供する情報には、サービスが不要な場合は停止することでワーム感染を予防できる旨が書かれている。こうした状況において、A社がとるべき最も適切な対策は次のうちのどれか。	ア．直ちにオンラインショップ用サーバを停止させる。テスト環境で悪影響がないことの確認が終わった後（2～3日後）に実運用環境にもパッチを適用し、オンラインショップを再開する。 イ．今回のワームは現在使用していないサービスを対象にしているので、ワームが用いるサービスの停止を確認した上でパッチは適用せず、そのまま運用を続ける。 ウ．ワームが用いるサービスの停止を確認し、情報収集と異常監視の警戒体制を強化した上でオンラインショップの運用を継続する。テスト環境での悪影響なしの確認が終わった後にパッチを適用するが、当分の間は警戒態勢を維持する。 エ．ワームが発生したのは緊急事態であるので、テスト環境での確認なしに直ちに実運用環境にパッチを適用し、適用後のサーバでオンラインショップを運用する。	ウ	[中]セキュリティホール対策 [小]パッチの適用可否の判断基準（目的、対象） **※ワームについては、亜種の発生を考慮する必要があることを前提とした問題。セキュリティ重視のポリシーであれば、アが正解と考えてもおかしくないが、今回のケースでは過剰防衛。**

(10) セキュリティプロトコル

No.	タイプ	問題	選択肢	正解	ターゲット 備考（※印）
10-01	1	PPTP（Point-to-Point Tunnelling Protocol）はOSIによる7階層のうちのどの層で機能するプロトコルか。	ア．データリンク層 イ．ネットワーク層 ウ．トランスポート層 エ．アプリケーション層	ア	[中]データリンク層
10-02	1	次のプロトコルのうち、VPN (Virtual Private Network) で使用されないものはどれか。	ア．SSL イ．S/MIME ウ．L2TP エ．SOCKS	イ	[中]アプリケーション層
10-03	1	次のプロトコルのうち、データリンク層で機能するプロトコルではないものはどれか。	ア．MPLS（Multi-Protocol Label Switch） イ．MPOA（Multi-Protocol Over ATM） ウ．PPTP（Point-to-Point Tunnelling Protocol） エ．SSL（Secure Socket Layer）	エ	[中]データリンク層
10-04	1	次のプロトコルのうち、アプリケーション層で機能するプロトコルではないものはどれか。	ア．MPOA イ．PGP ウ．S/MIME エ．SSH	ア	[中]アプリケーション層
10-05	1	次のプロトコルのうち、暗号化や認証などに直接関係しないものはどれか。	ア．BGP イ．L2TP ウ．WEP エ．SSL	ア	（すべて）
10-06	2	IPsecに関する以下の説明のうち、正しくないものはどれか。	ア．IPv6においては、IPsecと同等のセキュリティ機能がプロトコルに含まれている。 イ．電子メールをIPsecで暗号化して相手に送付できるようにするためには、エンドユーザはあらかじめ相手との間で共通鍵を手動で設定しておく必要がある。 ウ．インターネットを介して2つのLANの間でVPN接続を行うときの暗号化や認証の手段としてIPsecを用いることができる。 エ．通信しようとする機器間のネットワークの経路上でアドレス変換などを行っている場合は、IPsecを用いた通信が不可能なこともある。	イ	[中]ネットワーク層
10-07	2	次に示す通信の用途とそれに用いるプロトコルとの組合せのうち、正しくないものはどれか。	ア．Webサイトへの送信情報の暗号化－ SSH イ．電子メールの暗号化 － PGP ウ．VPNの構築 － L2TP エ．ファイアーウォール機能の提供 － SOCKS	ア	（すべて） ※SSH→SSL
10-08	2	次のプロトコルについての説明のうち、誤っているものはどれか。	ア．TLSはSSLのバージョン3をベースに制定されたプロトコルであり、トランスポート層で機能する。 イ．SSHは別のコンピュータを操作するためのサービスであるtelnetやrlogin，rshの安全な代替手段として利用される。 ウ．L2TPはPPTPとL2Pを統合したダイアルアップ接続向けのプロトコルである。 エ．MPOAはADSL上におけるマルチプロトコルに対応した転送プロトコルである。	エ	（すべて） ※ ADSL → ATM

No.	タイプ	問題	選択肢	正解	ターゲット 備考（※印）
10-09	2	SSHが提供する機能として、正しくないものはどれか。	ア．SSHにより構築されるセッションをVPNとして用いることができる。 イ．認証局(CA)を用いた公開鍵暗号方式による経路の暗号化を行うことができる。 ウ．認証にワンタイムパスワード方式を用いることができる。 エ．公開鍵暗号を用いることにより、相手先コンピュータのパスワードを用いることなく、相手先コンピュータにログインすることができる。	イ	[中]アプリケーション層 [小]SSH
10-10	2	以下に示すSSLの特徴のうち、正しくないものはどれか。	ア．クライアントとサーバの双方を認証することができる。 イ．WWWサービスにおける通信内容を保護する手段として最も一般的に用いられている。 ウ．保護の対象となるデータ方式は、HTTPを用いたもの以外も可能である。 エ．証明書を予め取得していないサイトとの通信を暗号化することはできない。	エ	[中]トランスポート層 [小]SSL/TLS

(11) 認証

No.	タイプ	問題	選択肢	正解	ターゲット 備考（※印）
11-01	2	ワンタイムパスワードの特徴を説明するものとして適切なものはどれか。	ア. リプレーアタックを防ぐことはできない イ. ユーザはパスワードを入力する必要はない ウ. 匿名のユーザを認証するための手段である エ. パスワードを盗聴されても安全である	エ	[小]ワンタイムパスワード
11-02	2	バイオメトリクス認証の説明として誤っているものはどれか。	ア. 個人の生体的特徴を使用するためなりすましが不可能である イ. 正しく本人が認証されない認証エラーの可能性がある ウ. 運用する際にはプライバシーの問題を検討する必要がある エ. 指紋や虹彩などの身体的特徴のほか、筆跡などの行動的特徴を用いる方式がある	ア	[中]バイオメトリクス認証
11-03	1	プラグインなどの特別なソフトをサーバにインストールする必要がないシングルサインの方式はどれか。	ア. エージェント型 イ. デュアルホームホスト型 ウ. ネットワーク型 エ. リバースプロキシ型	エ	[中]シングルサインオン
11-04	1	ICカードに物理的改ざん加えようとしても、保管されているデータが消滅･無効化するなどして、情報の漏洩･盗難から保護されるしくみを何というか。	ア. 電子透かし イ. アクセス制御 ウ. 耐タンパ エ. 否認防止	ウ	[小]ICカード
11-05	1	Kerberosによる認証の構成要素ではないものはどれか。	ア. メッセージ認証コード イ. 発券サーバ ウ. 認証サーバ エ. チケット	ア	[中] Kerberos
11-06	2	固定パスワードの運用として誤っているものはどれか。	ア. パスワードの最低文字数を決め、指定文字数以下のパスワードはシステムが受け付けないようにする。 イ. アルファベット以外の文字列を必ず1文字以上パスワードに設定するようにし、アルファベットのみのパスワードはシステムが受け付けないようにする。 ウ. 頻繁にパスワードを変更するとユーザが忘れてしまうため、あまり頻繁にパスワードを変更できないようにする。 エ. ユーザ名と同じパスワードは受け付けないようにする。	ウ	[小]固定パスワード
11-07	2	SSHに関する説明として誤っているものはどれか。	ア. BSD UNIX起源の遠隔計算機利用のプログラムであるrlogin、rsh等と同等の機能を持ちセキュリティ面に関して強化されたアプリケーション及び、そのアプリケーションが用いるプロトコルのこと。 イ. SSHが備えるポートフォワーディング機能を利用すれば、POPやIMAPでもSSHが確立した安全な通信路を利用できる。 ウ. SSHは、公開鍵暗号技術に基づく強力な認証と共通鍵暗号による暗号化機能を備えている。 エ. SSHにはSSH1とSSH2があり、SSH2はSSH1の脆弱性を克服している。SSH1とSSH2には互換性がある。	エ	[小]SSH

No.	タイプ	問題	選択肢	正解	ターゲット 備考（※印）
11-08	2	RADIUSに関する正しい説明はどれか。	ア．RADIUSサーバとアクセス先のサーバ間では、パスワードは平文で流れる。 イ．RADIUSサーバは、アクセス先サーバから送信されたユーザIDをチェックした後、MD5を使ったチャレンジ･アンド･レスポンス形式でアクセスサーバと通信、パスワード認証を行う。 ウ．ユーザの認証を行うのみで、アクセスの許可･拒否は行わない。 エ．PPPにてよく利用されているが、UNIXログインでは利用されない。	イ	[小]RADIUS
11-09	2	セキュリティモジュールの耐性としてよく「耐タンパ性」という言葉が言われるが、耐タンパ性の説明として誤っているものはどれか。	ア．物理的、あるいは論理的に内部の情報を読み取られることに対する耐性のこと。 イ．FIPS 140は、ICカード等のハードウェア暗号モジュールの強度レベルを判定するための重要な指標であるが、ソフトウェアモジュールには適用されない。 ウ．FIPS 140では、耐タンパ性をタンパ明示性とタンパ検知性の2種対にわけて定義している。 エ．暗号モジュールなどに関して用いられることが多い概念である。	イ	[小]耐タンパ性
11-10	2	Cookieを利用する際の危険性の説明として誤っているものはどれか。	ア．Cookieは、重要な個人情報が含まれているため、同一のPCを不特定多数の人たちが共有する場所では、ブラウザのCookieの機能をオフにした方がよい。 イ．Cookie情報の管理方法はブラウザによって違うが、テキスト形式のファイルとして保存されているので、第3者に個人情報が漏洩する可能性が高い。 ウ．Cookieに書かれる可能性のある情報は、ユーザがサイトの画面から打ち込んだ情報、サイトがユーザに対して発行したパスワードなどの情報の2つである。 エ．SSLで暗号化された通信を経由して受け取った場合でも、Cookieに書き込まれている情報が暗号化されているとは限らない。	ウ	[小]Cookie

(12) PKI

No.	タイプ	問題	選択肢	正解	ターゲット 備考（※印）
12-01	2	属性証明書の説明として、正しくないものは次のうちのどれか。	ア. 属性証明書は、属性証明局から発行され、所有者の公開鍵が含まれている。 イ. 属性証明書は、権限や役割を証明するものである。 ウ. 属性証明書は、人に対してだけでなく、アプリケーションなどに対しても発行されることがある。 エ. 属性証明書の所有者を認証する方法として、属性証明書所有者の公開鍵のメッセージダイジェスト値で確認する方法がある。	ア	[小]属性証明書
12-02	2	PKIに関する様々な規格が現状存在しているが、それぞれの規格に関して正しい説明をしているものはどれか。	ア. X.509 v.3では、公開鍵証明書フォーマット、CRLフォーマットを規定しているが、RFC3280で規定されているフォーマットとは同じものである。 イ. PKCSは＃1から＃15まで規定されており、よく利用されるのは、PKCS#1、PKCS#7、PKCS#12で、PKCS#7は秘密鍵、証明書交換フォーマットに関して規定している。 ウ. PKCS#10では、証明書申請形式が定義されているが、これは、RFC2511で定義されている証明書申請形式の定義と同じである。 エ. PKCS#11は、スマートカード関数インターフェースの規格であるが、Microsoft社のCrypto APIは、これと同じ規格である。	イ	[中]規格
12-03	2	2000年5月に成立した電子署名法(電子署名及び認証業務に関する法律)に関連する記述として正しい組み合わせはどれか。 ① 電子署名法では、電磁的記録（電子文書等）は、本人による一定の電子署名が行われているときは、真正に成立したものと推定することについて規定されている。 ② 電子署名法では、認証業務（電子署名が本人のものであることを証明する業務）のうち、法律で定める一定の基準を満たす業務を主務大臣が認定できることを規定している。 ③ 特定認証業務の認定には有効期限がないため、認定を受けた企業は、半永久的に認定企業となる。 ④ 電子署名法以外にも、商業登記に基づく電子認証制度にて、法人については法務局が登記情報に基づく電子認証制度を担うシステムが成立している。	ア. 全て イ. ②と③ ウ. ①と②と④ エ. ①と②	ウ	[中]法的枠組み

No.	タイプ	問題	選択肢	正解	ターゲット 備考（※印）
12-04	2	ディレクトリサーバは、デジタル証明書の検索手段としてよく用いられるが、そのディレクトリサーバに関する正しい説明はどれか。	ア. ディレクトリの標準化された通信プロトコルは、LDAPのみである。 イ. ディレクトリはツリー構造のデータベースで、検索中心の利用を想定しており、検索に特化したデータベースである。 ウ. 多言語対応しており、日本語は、SJIS、JIS、EUC、UTF-8で入力することが可能である。 エ. 画像などのバイナリデータは登録することができない。	イ	[小]ディレクトリサーバの利用
12-05	2	PKIを利用したセキュリティプロトコルとしてSSLが有名であるが、次のうちSSLの通信でクライアントがサーバ認証を行う際にチェックしないものはどれか。	ア. サーバ証明書は有効期限内か。 イ. サーバ証明書を発行した認証局は、自分が信頼するルート証明書のリストに入っているか。 ウ. サーバ証明書の署名は正しく検証されるか。 エ. サーバ証明書内の鍵アルゴリズムは、自分が使用できる鍵アルゴリズムと一致しているか。	エ	[中]PKIの利用
12-06	2	X.509証明書内に記述される各項目に関して、正しい記述はどれか。	ア. バージョンとは証明書のフォーマットバージョンで、現状はv3が使用されているため、3と記述される。 イ. シリアル番号は利用者が証明書を区別するための番号であるため、世界的にユニークである必要がある。 ウ. サブジェクトはこの証明書の所有者の名前である。利用者はこのサブジェクトを用いて証明書の所有者を識別する。 エ. 署名アルゴリズムは、証明書所有者が利用可能なアルゴリズムを指定する。	ウ	[小]証明書のフォーマット
12-07	2	CRLの説明として正しいものはどれか。	ア. 証明書取消しリストには全部で4種類あり、そのうちエンドエンティティに関する証明書取消しリストをデルタCRLと呼ぶ。 イ. CRL Scopeエクステンションは、CRLがカバーする証明書と破棄情報の範囲を指定する。 ウ. CRLはLDAPでのみ配布される。 エ. CRLは、証明書を発行した認証局によって発行され、不定期に更新される。	イ	[小]CRL
12-08	2	認証局が策定すべき運用規程に含めるべき内容として、適切でないものはどれか。	ア. 証明書が適用されるアプリケーションリストおよび適用が禁止されるアプリケーションのリスト。 イ. 認証局運用規程の解釈、保守、登録等に責任がある部署および連絡先。 ウ. CA･RA･利用者が負う義務。 エ. 利用者が運用規程に違反した場合の罰則。	エ	[小]認証局運用規程
12-09	1	GPKIのように、多数の省庁間の階層関係のないCAを相互認証するのに適している信頼モデルはどれか。	ア. 単独CAモデル イ. 階層型モデル ウ. メッシュモデル エ. ブリッジCAモデル	エ	[中]信頼モデル

No.	タイプ	問題	選択肢	正解	ターゲット 備考（※印）
12-10	2	デジタル証明書についている認証局の署名が正しく検証されたときに保証されないのはどれか。	ア．証明書の内容が改竄されていないこと。 イ．証明書が有効期限内であること。 ウ．証明書が確かに認証局によって発行されたこと。 エ．公開鍵が確かに持ち主のものであることを、認証局が保証していること。	イ	[小]証明書の有効性検証

(13) 暗号

No.	タイプ	問題	選択肢	正解	ターゲット 備考 (印)
13-01	1	次の暗号名の内、公開鍵暗号ではないものはどれか。	ア. ELGamal イ. RSA ウ. AES エ. ECIES-OAEP	ウ	[小]公開鍵暗号のアルゴリズム
13-02	1	現在実用に供されていない暗号方式はどれか。	ア. ストリーム暗号 イ. ブロック暗号 ウ. 量子暗号 エ. バーナム暗号	ウ	[中]その他の暗号方式
13-03	1	鍵管理方式として安全性の証明されている方式はどれか。	ア. 鍵生成方式 イ. 鍵共有方式 ウ. Shamir閾値方式 エ. 鍵管理サーバ方式	ウ	[中]鍵管理
13-04	1	暗号学的な見地から、ハッシュ関数について正しい記述はどれか。	ア. 常にある定まった長さの入力データに対し一定長の短いデータになるように圧縮する関数。 イ. 任意の長さの入力データに対し一定長の短いデータになるようにパターン抽出する関数。 ウ. 異なる2つの入力に対して、異なるハッシュ値を出力し、生成したハッシュ値から元のデータとの関係を同定できないことである。 エ. ハッシュ関数を改ざん検知に用いるためには鍵付きハッシュ関数を用いなければならない。	ウ	[小]ハッシュ関数の原理
13-05	1	次の暗号方式のうち、離散対数問題の困難性に安全の根拠をおいている暗号方式はどれか。	ア. RC5 イ. AES ウ. MULTI2 エ. DH鍵配送	エ	[小]Diffie-Helman 鍵配送
13-06	1	次の暗号方式のうち、整数の因数分解の困難性に安全の根拠をおいている方式はどれか。	ア. RSA イ. SHS ウ. E2 エ. CAMERIA	ア	[小]公開鍵暗号のアルゴリズム
13-07	1	ブロック暗号攻撃法として発明された差分攻撃法、線形攻撃法に対し、安全性証明付きで初めて開発された暗号はどれか。	ア. IDEA イ. RC4 ウ. MISTY エ. DES	ウ	[小]共通鍵暗号のアルゴリズム
13-08	2	現在の暗号利用における秘匿機能の実現に関する考え方の大きな流れは次のどれか。	ア. 暗号化鍵のような可変なデータは使わず暗号アルゴリズムを秘匿することで達成する方向にある。 イ. 暗号化鍵は使うが、鍵と併せて暗号アルゴリズムも秘匿し、秘匿機能を高める方向にある。 ウ. 暗号アルゴリズムは公開し、秘匿機能は専ら暗号化鍵の秘匿に依存する方向にある。 エ. 暗号機能をファームウェアに閉じ込めることで秘匿機能を達成する方向にある。	ウ	[小]共通鍵暗号の原理

No.	タイプ	問題	選択肢	正解	ターゲット 備考(印)
13-09	2	アルゴリズム公開型の暗号方式について誤っているものはどれか。	ア. 本方式の暗号では鍵の安全な維持･管理が重要である。 イ. 公開によってアルゴリズムの幅広い検討を期待できることが利点である。 ウ. アルゴリズムが公開されているので暗号化の都度鍵を変更しなければ強度を維持できないのが欠点である。 エ. アルゴリズムを公開することで不特定多数の相手と秘密通信を行う暗号化基盤として使えることが利点である。	ウ	[小]公開鍵暗号の原理
13-10	2	公開鍵暗号について正しいものはどれか。	ア. 現在実用化されている公開鍵暗号は、暗号化･復号化に際して、共通鍵暗号に比べて時間が掛るのが欠点である。 イ. 現在実用化されている公開鍵暗号はすべて、量子計算機が完成すると無効になることが証明されている。 ウ. 公開鍵暗号方式は全て数学的に安全性が証明されているので、秘密鍵の保管にさえ気をつければ、鍵の大きさにはそれほど注意を払わなくてもよいことが利点である。 エ. 共通鍵暗号を使って出来ることは全て公開鍵暗号を使って出来るので、共通鍵暗号は使われなくなりつつある。	ア	[小]公開鍵暗号の原理
13-11	2	暗号方式について正しいものはどれか。	ア. 現在実用に使われている暗号方式は、全て安全性が証明されていると仮定してよい。 イ. 全ての暗号方式は、解読者に無限の計算力があることを仮定するといずれも解読される、という意味で、安全ではないことが証明されている。 ウ. 共通鍵を預託できる信頼できる第3者を仮定するなら、公開鍵暗号でできることは、全て共通鍵暗号で出来るようなプロトコルが存在する。 エ. 現在使われている暗号方式の多くには、万一秘密鍵を紛失しても再生可能な機能が備わっている。	ウ	[中]暗号解読･強度評価 ※ vernam **暗号はこの仮定では解読できないため、イは誤り**
13-12	2	暗号方式の標準化動向について誤っているものはどれか。	ア. 米国においては、安全性の低下したDESの後継アルゴリズムとして鍵長をDESの2倍もしくは3倍としたTriple-DESが次世代の標準暗号AESとして定められた。 イ. 欧州においては、NESSIEプロジェクトが標準暗号アルゴリズムを制定した。 ウ. 日本においては、CRYPTRECが電子政府における調達のための推奨すべき暗号(電子政府推奨暗号)リストを作成した。 エ. ISOはISO/IEC JTC SC27WG2において、公開鍵暗号及び共通鍵暗号の標準を定めることを目標としたプロジェクトを開始した。	ア	[中]暗号解読･強度評価

(14) 電子署名

No.	タイプ	問題	選択肢	正解	ターゲット 備考（※印）
14-01	1	2002年度CRYPTRECにおいて電子署名アルゴリズムとして採用されなかったものは次のうちのどれか。	ア．DSA イ．ECDSA ウ．SFLASH エ．RSASSA-PKCS-v.1_5	ウ	[小]電子署名 署名に利用される暗号アルゴリズム
14-02	1	次に掲げる電子署名方式のうち離散対数問題に基づかない方式はどれか。	ア．ElGamal イ．DSA ウ．ESIGN エ．Schnorr	ウ	[小]電子署名 署名に利用される暗号アルゴリズム
14-03	2	電子署名に関して次に掲げる4つの説明のなかで、電子署名に必ずしも適合しないものはどれか。	ア．署名対象全文暗号化による秘匿性 イ．秘密情報を用いた本人性の保証 ウ．ハッシュ関数の利用による改ざん検知機能 エ．誰でも行える検証の容易性	ア	[中]電子署名 の利点
14-04	2	公開鍵暗号法を用いて作成する電子署名について正しいものはどれか。	ア．当該文書のハッシュ値に対し、受取者の公開鍵で暗号化したものを電子署名とする。 イ．当該文書のハッシュ値に対し、署名者の公開鍵で暗号化したものを電子署名とする。 ウ．当該文書のハッシュ値に対し、受取者の秘密鍵で暗号化したものを電子署名とする。 エ．当該文書のハッシュ値に対し、署名者の秘密鍵で暗号化したものを電子署名とする。	エ	[小]署名作成 方法
14-05	2	公開鍵暗号法を用いて作成された電子署名の検証法として正しいものはどれか。	ア．電子署名を受取者の公開鍵で復号したものを、当該文書のハッシュ値と比較する。 イ．電子署名を署名者の公開鍵で復号したものを、当該文書のハッシュ値と比較する。 ウ．電子署名を受取者の秘密鍵で復号したものを、当該文書のハッシュ値と比較する。 エ．電子署名を署名者の秘密鍵で復号したものを、当該文書のハッシュ値と比較する。	イ	[小]署名検証 方法
14-06	3	公開鍵暗号法を用いて作成する、不特定の受取人を対象とした電子署名の作成に用いるメッセージダイジェストについて正しいものはどれか。	ア．電子署名の作成においては、その署名が署名者でなければ実行出来ない暗号化であることが重要なので、メッセージダイジェストとしては署名対象データの一部分だけでもよい。 イ．電子署名の作成においては、メッセージダイジェストの作成においても鍵付きハッシュ関数を用いることで耐偽造性を高めることが必要である。 ウ．公開鍵暗号法は処理に時間が掛るので、メッセージダイジェストは短ければ短いほどよい。 エ．署名に用いるメッセージダイジェストは誰でも作成できるものでなければならない。	エ	[小]メッセージ ダイジェスト

No.	タイプ	問題	選択肢	正解	ターゲット 備考（※印）
14-07	2	PKI基盤による電子署名について述べた以下の4つの文のうち、正しいのものはどれか。	ア．署名者は自分が用いる署名アルゴリズム名と、自ら生成した鍵ペアのうちの公開鍵とを、出来るだけ多くの電子掲示板等に公表することで公開の事実を作る。 イ．署名者は自分が用いる署名アルゴリズム名と、自ら生成した鍵ペアのうちの公開鍵とを、多くの利害関係者と電子メール等で送り合って相互に相手の公開鍵証明書を発行し合うことで公開の事実を作る。 ウ．署名者は認証局と呼ばれる適当な機関が発行した公開鍵証明書を必要ならば通信相手に送ることで自己の鍵を公開する。 エ．署名者は出来るだけ多くの人と自分が知っている他人の署名アルゴリズムと公開鍵を相互に交換し合い、社会全体でその成員の署名に関する情報を共有することで電子署名流通の基盤を構築する。	ウ	[中]電子署名の仕組み
14-08	2	XML署名について以下の4つの文の中で、誤っているものはどれか。	ア．XMLの文法に基づく記述により、署名の対象、署名生成アルゴリズム、署名および公開鍵証明書などを統一して表現できる。 イ．XML署名全体は一つのXMLタグ付き文書として作成され、ASN.1構文に比べて分かりやすい。 ウ．データファイルやXML文書のみならず、文書の中の一部分に対しても署名を付けることができるので、部分署名や多重署名など、実際的かつ複雑な構造の署名処理にも対応できる。 エ．XML署名で参照する暗号アルゴリズムなどのオブジェクトの識別子は、ASN.1がOID（Object Identifier）を指定するのに対して、W3Cなどで定めているIDL（Interface Definition Language）を参照する。	エ	[小]XML署名(規格、利用)
14-09	2	コードサイニングについて誤っている記述はどれか。	ア．ベンダが開発したプログラムコード、ActiveXコントロール、あるいはプラグインモジュールなどに、作成者や発行者を示すためのデジタル署名データなどを埋め込むことをコードサイニングという。 イ．ベンダがコードサイニングを施すにあたっては、普通厳格なウイルスチェック行い、またトロイの木馬等の有害な機能が埋め込まれていないことを検証するので、コードサイニングのついたプログラムやプラグインをユーザは安心して利用することができる。 ウ．ユーザは、署名を調べることで、作成者、発行者、バージョンおよび有効期限などの情報のほか、コードが不当に改ざんされているかどうかを調べることができる。 エ．ユーザは署名を調べることで、プログラムが改ざんされている場合や信用できない発行元からのモジュールの受け入れを拒否することができる。	イ	[小]コードサイニング

No.	タイプ	問題	選択肢	正解	ターゲット 備考（※印）
14-10	2	PGP流儀の署名について誤っているものはどれか。	ア．PGPではRSA方式とDH/DSS方式の2つの暗号化･署名方式をサポートしている。 イ．PGPでは署名暗号化に際して、まず署名を作成し、それと平文とあわせて暗号化するので、署名部分を切り出すことはできない。 ウ．まだPGPを利用する環境を構築していなくても、自分宛ての暗号化文書を受け取ることだけはできる。 エ．PGPでは利用する環境を構築したあとで、自ら自分の公開鍵を公開鍵DBに登録するか、もしくは自分を信頼して秘密通信をおこなってくれる相手を探してからでなければ、有効な秘密通信は行えない。	ウ	[中]電子署名の要素技術

(15) 不正アクセス手法

No.	タイプ	問題	選択肢	正解	ターゲット 備考(※印)
15-01	2	攻撃者は、インターネット上から入手できる情報を入手し、事後の攻撃に役立てることが多い。以下はその技法についての説明であるが、誤っているものがある。それはどれか。	ア. Whois データベースからは、管理者のメールアドレスやサイトが使用しているプライベートアドレスの一覧を知ることができる。 イ. サイトの公開DNSサーバからは、ホストのIPアドレスを取得することができる。 ウ. サーバの出力するバナーからは、サーバの種類、バージョンなどを知ることができる。 エ. サイトが公開を意図していない情報が入手できる場合があり、その中に個人情報などが含まれることもある。	ア	[中]情報収集
15-02	1	攻撃に先立って行う偵察行為の一環として、ツールを用いて標的となるサーバに特殊なパケットを送信し、その反応からOSを推測することがある。そうした目的に用いられる技法を一般に何というか。	ア. タッピング イ. フィンガープリンティング ウ. スニッフィング エ. トラッシング	イ	[中]偵察行為
15-03	1	通常とは異なる手順でTCP接続を行うことで、標的となるマシン上にログが残らないようにするポートスキャンの手法を総称して何と呼ぶか。	ア. スロースキャン イ. CGIスキャン ウ. ステルススキャン エ. TCPコネクトスキャン	ウ	[中]偵察行為
15-04	1	外部からの不正侵入につながる脆弱性のうち、サーバプログラムが入力データのサイズをチェックしていないことが原因となって発生するものはどれか。	ア. バッファオーバーフロー イ. 競合状態(race condition) ウ. フォーマットストリングバグ エ. クロスサイトスクリプティング	ア	[中]遠隔不正侵入･操作
15-05	2	盗聴や情報漏洩についての説明のうち、誤っているものはどれか。	ア. スイッチやスイッチングルータで社内LANを構築していても、通信が盗聴される場合がある。 イ. CRT(ディスプレイ)から漏れる電磁波により、情報が漏洩することがあるので、リスクに応じて対策を講じる必要がある。 ウ. 無線LANは強力な暗号化が施されているので、積極的に使用することが望ましい。 エ. シェアドネットワークによって社内LANが構築されている場合、ネットワークの盗聴を行っているマシンを特定することは容易ではない。	ウ	[中]盗聴行為
15-06	2	DoS攻撃(サービス拒否攻撃)に関する以下の説明のうち、誤っているものはどれか。	ア. バッファオーバーフローの脆弱性を悪用することで DoS 攻撃が成立することはない。 イ. 政治的意図によって多数のWWWアクセスが発生し、DoS攻撃が成立することがある。 ウ. DoS攻撃が成立するためには必ずしも大量のアクセスを必要としない。 エ. 標的のマシンを直接攻撃するのではなく、経路上のルータやスイッチを攻撃することでもDoS攻撃は成立し得る。	ア	[中]遠隔不正侵入･操作

<table>
<tr><th>No.</th><th>タイプ</th><th>問題</th><th>選択肢</th><th>正解</th><th>ターゲット
備考（※印）</th></tr>
<tr><td>15-07</td><td>1</td><td>以下の文章のうち、空欄 a〜c に当てはまる字句として正しい組合せを選択肢の中から選べ。
侵入されたマシンには、様々なツールやソフトウェアがインストールされることがある。その一例として、アクセスログを消去するためのログクリーナや、攻撃者のプロセスやファイルを表示しないよう(a)化されたコマンド、正規の認証手段を回避して侵入するための(b)などがある。こうしたツールを一つのパッケージにまとめたものがインターネット上で流通しており、一般的に(c)と呼ばれることが多い。</td><td><table><tr><th></th><th>a</th><th>b</th><th>c</th></tr><tr><td>ア.</td><td>バックドア</td><td>トロイの木馬</td><td>スパイウェア</td></tr><tr><td>イ.</td><td>スパイウェア</td><td>バックドア</td><td>rootkit</td></tr><tr><td>ウ.</td><td>トロイの木馬</td><td>rootkit</td><td>スパイウェア</td></tr><tr><td>エ.</td><td>トロイの木馬</td><td>バックドア</td><td>rootkit</td></tr></table></td><td>エ</td><td>[中]遠隔不正侵入･操作</td></tr>
<tr><td>15-08</td><td>2</td><td>以下の行為のうち、ソーシャルエンジニアリングに当てはまるものはどれか、選択肢の中から選べ。
a) 清掃業者を装ってオフィスに入り、個人情報を盗み出す。
b) 官公庁のWWWサーバに侵入し、ホームページを改竄する。
c) 管理者の背後からキー入力を覗き込み、システムのパスワードを入手する。
d) 無線LAN機能つきのパソコンを使って、自由にアクセスできるところがないかを探す。</td><td>ア. a) と c)
イ. a) と d)
ウ. b) と c)
エ. b) と d)</td><td>ア</td><td>[中]古典的不正アクセス技法
[小]ソーシャルエンジニアリング</td></tr>
<tr><td>15-09</td><td>1</td><td>パスワード解読のため、想定される文字や数字、記号の組合せを全て試す手法を何というか。</td><td>ア. タンパリング
イ. ブルートフォース
ウ. 辞書攻撃
エ. ペネトレーション</td><td>イ</td><td>[中]情報収集</td></tr>
<tr><td>15-10</td><td>1</td><td>以下の説明の中から正しいものを選べ。</td><td>ア. DDoS攻撃では、単一のホストからのみ攻撃が行われるので、発信元の追跡が比較的容易である。
イ. 0-day exploit とは、脆弱性が公表された後で公開された攻撃用コード(プログラム)のことである。
ウ. シェルポートバインディングを用いてシステムに侵入するには、最初に侵入した時に使用したのと同じパスワードを用いる必要がある。
エ. LKM rootkit では、OSのカーネルが持つシステムコールを改竄するため、コマンドバイナリを変更せずに侵入の痕跡を隠蔽することができる。</td><td>エ</td><td>[中]遠隔不正侵入･操作</td></tr>
</table>

(16) 法令・規格

No.	タイプ	問題	選択肢	正解	ターゲット 備考(※印)
16-01	1	「コンピュータウイルス対策基準」が定めるウイルスのもつ機能として適切でないものはどれか	ア. 発病機能 イ. 自己伝染機能 ウ. 潜伏機能 エ. 破壊機能	エ	[小]コンピュータウイルス対策基準
16-02	1	次の内容は、どの法律またはガイドラインの説明か。 「ソフトウェアの違法複製等を防止するため、法人、団体等を対象として, ソフトウェアを使用するに当たって実行されるべき事項をとりまとめたもの」	ア. 著作権等管理事業法 イ. 著作権法 ウ. ソフトウェア管理ガイドライン エ. 情報システム安全対策指針	ウ	[小]ソフトウェア管理ガイドライン
16-03	2	国家公安委員会が平成11年に改正した「情報システム安全対策指針」(告示第19号)における「開放的なネットワークに接続する情報システムについて追加的に講ずべき安全対策」としてかかげられている項目として正しくないものはどれか。	ア. 開放的なネットワークとの接続は、必要最小限の機能、回線及びホスト等に限定すること イ. 回線の負荷状況等を監視する機能を設けること ウ. ネットワークの構成等に関する重要な情報は公開すること エ. 異状が発見された場合等必要がある場合は、接続されたネットワークを切り離すことができるようにすること	ウ	[小]情報システム安全対策指針
16-04	1	情報セキュリティマネジメントシステム(ISMS)の特徴をあらわすものとして適切でないものはどれか。	ア. 機密性、完全性、可用性 イ. PDCAモデル ウ. セキュリティポリシー エ. EAL	エ	[小]ISMS認証基準
16-05	2	2001年4月1日に施行された「電子署名及び認証業務に関する法律(電子署名・認証法)」の概要をあらわすものとして不適切なものはどれか。	ア. 指定調査機関制度の導入 イ. 認証業務に関する任意的認定制度の導入 ウ. 電磁的記録の真正な成立の推定 エ. 審査登録機関の認定	エ	[小]電子署名及び認証業務に関する法律(電子署名・認証法)
16-06	2	「個人情報の保護に関する法律(個人情報保護法)」における個人情報取扱事業者の義務をあらわすものとして正しいものはどれか。	ア. 個人データの正確性、最新性を確保するように務めなければならない イ. 個人情報の利用目的を特定してはならない ウ. 個人データを第三者に対して一切提供してはならない エ. 個人データの本人からの開示、訂正、利用停止の求めに応じてはならない	ア	[小]個人情報の保護に関する法律(個人情報保護法)
16-07	2	2000年2月13日に施行された「不正アクセス行為の禁止等に関する法律(不正アクセス禁止法)」の処罰の対称になる行為はどれか。	ア. サーバ上のサービスのポートスキャンを行う イ. 無断で他人のID、パスワードを第三者に提供する ウ. ネット上の掲示板に個人を中傷する内容を書き込む エ. 個人データを本人の了承を得ずに第三者に提供する	イ	[小]不正アクセス行為の禁止等に関する法律

No.	タイプ	問題	選択肢	正解	ターゲット 備考（※印）
16-08	2	ISO/IEC TR 13335の説明として正しいものはどれか。	ア. ITセキュリティ管理に関する英国規格として策定され、Part1とPart2からなる。Part1は2000年9月にISO標準として認定。 イ. セキュリティに関わるマネジメントプロセスをリスクマネジメントの観点からフレームワークとして提供する。5部構成からなる。 ウ. 情報処理関連製品および情報処理システムのセキュリティレベルを評価するための国際規格。 エ. 金融業務におけるセキュリティガイドライン。	イ	[小]ISO/IECセキュリティ関連規格
16-09	1	ISO/IEC 15408に基づく「ITセキュリティ評価･認証制度」において、個別製品の設計仕様書を表わす用語として正しいものはどれか。	ア. TOE イ. PP ウ. ST エ. CC	ウ	[小]ISO/IECセキュリティ関連規格
16-10	1	2002年に改訂されたOECDセキュリティガイドラインに掲げられた「情報セキュリティに関する9原則」に含まれないものはどれか。	ア. 認識(Awareness)の原則 イ. 対応(Response)の原則 ウ. リスクアセスメント(Risk assessment)の原則 エ. 正当性(Authenticity)の原則	エ	[小]OECDセキュリティ関連ガイドライン

７．３ 参考資料

[1] NPO 日本ネットワークセキュリティ協会(JNSA), NPO ネットワークリスクマネジメント協会(NRA), “情報セキュリティプロフェッショナル育成に関する調査研究”, http://www.ipa.go.jp/security/fy14/reports/professional/ikusei-seika-press.html, http://www.meti.go.jp/kohosys/press/0003929/

[2] 三輪信雄 (編集), 白橋明弘 (編集), その他, “インターネットセキュリティ教科書〈上／下〉”, DG ジャパン, 2002.

[3] インターネットプロトコルハンドブック編集委員会 (編集), “最新インターネットプロトコル・ハンドブック”, 朝日新聞社, 2001.

[4] シムソン ガーフィンケル, “UNIX & インターネットセキュリティ 第 2 版”, 山口英 (翻訳), オライリー・ジャパン, 1998.

[5] エリザベス・D. ツビッキー, “ファイアウォール構築 第 2 版 Volume1 理論と実践”, オライリー・ジャパン, 2003.

[6] エリザベス・D. ツビッキー, “ファイアウォール構築 第 2 版 Volume2 インターネットサービス”, オライリー・ジャパン, 2003.

[7] 佐々木良一他編集, “情報セキュリティ事典”, 共立出版, 2003.

[8] 山口英, 鈴木裕信編, “bit 別冊 情報セキュリティ”, 共立出版, 1999.

[9] 岡本龍明, 山本博資, “現代暗号”, 産業図書, 1997.

[10] Stuart McClure, “クラッキング防衛大全 ネットワーク攻撃の手口とセキュリティ対策 第 3 版”, 翔泳社, 2002.

[11] 上原 孝之, “情報セキュリティアドミニストレータ 平成 15 年度 情報処理教科書”, 翔泳社, 2003.

[12] 塚田孝則, “企業システムのための PKI”, 日経 BP, 2001.

[13] カーライル アダムズ他, “PKI 公開鍵インフラストラクチャの概念、標準、展開”, ピアソン・エデュケーション, 2000.

[14] Warwick Ford 他, “デジタル署名と暗号技術”, プレンティスホール, 2003.

[15] 経済産業省, “情報セキュリティ監査研究会報告書”, http://www.meti.go.jp/kohosys/press/0003614/, 2003.

[16] 熊谷誠治, “続・誰も教えてくれなかったインターネット・セキュリティのしくみ”, 日経インターネットテクノロジー, 日経 BP 社, 2001.

[17] 三輪信雄他, “インターネットセキュリティ 不正アクセスの手法と防御”, ソフトバンクパブリッシング, 2001.

[18] 馬場達也, “マスタリング IPsec”, オライリー・ジャパン, 2001.

[19] 青木隆一, 稲田龍他, “PKI と電子社会のセキュリティ”, 共立出版, 2001.

[20] 小松文子, “PKI ハンドブック”, ソフト・リサーチ・センター, 2000.

[21] William Stallings, “暗号とネットワークセキュリティ―理論と実際”, ピアソン・エデュケーション, 2001.

[22] サイモン・シン, “暗号解読―ロゼッタストーンから量子暗号まで”, 2001.

[23] Thomas R. Peltier, “セキュリティポリシーの作成と運用”, ソフトバンクパブリッシング, 2001.

[24] 田渕治樹, “国際セキュリティ標準 ISO15408 がみるみるわかる本”, PHP 研究所, 2002.

[25] 夏井高人, “電子署名法―電子文書の認証と運用のしくみ”, リックテレコム, 2001.

[26] Charlie Scott, “VPN 第 2 版”, オライリー・ジャパン, 2000.

[27] Ruixi Yuan, “実践 VPN―技術とソリューション”, ピアソン・エデュケーション, 2001.

[28] Tom Austin, “PKI 公開鍵基盤―電子署名法時代のセキュリティ入門”, 日経 BP 企画, 2001.

[29] Naganand Doraswamy, “IPSec テクニカルガイド―インターネット・イントラネット・VPN のセキュリティ標準”, ピアソン・エデュケーション, 2000.

[30] 三輪信雄他, “ネットワーク攻撃詳解―攻撃のメカニズムから理解するセキュリティ対策”, ソフト・リサーチ・センター, 2002.

[31] 織田博靖他, “セキュリティ IC カードの基礎と応用”, シーメディア, 2000

[32] 三和総合研究所, “IC カードビジネス最前線”, 工業調査会, 2000

[33] アイテック情報技術教育研究所, “2003 予想問題集情報セキュリティ”, アイテック,2003

[34] UNYUN, “ハッカー・プログラミング大全”, データハウス, 2001.

[35] Scott Oaks, “Java セキュリティ”, オライリー・ジャパン, 2001.

[36] Merike Kaeo, “ネットワークセキュリティ設計ガイド―安全なネットワークインフラストラクチャを構築するための手引き”, ソフトバンクパブリッシング, 2000.
[37] Warwick Ford 他, “ディジタル署名と暗号技術 第 2 版”, ピアソン・エデュケーション, 2001.
[38] Stephen Northcutt 他, “ネットワーク侵入解析ガイド―侵入検知のためのトラフィック解析法”, ピアソン・エデュケーション, 2001.
[39] Stephen Northcutt 他, “ネットワーク不正侵入検知”, 翔泳社, 2001.
[40] 古川久敬, “コンピテンシーラーニング”, 日本能率協会マネジメントセンター, 2002
[41] 太田隆次, “コンピテンシー人事 活用の仕方”, 経営書院, 2002
[42] 吉川弘之他, “技術知の本質”, 東京大学出版会, 1997
[43] Eric Maiwald, “Network Security A Begginner’s Guide Second Edition”, Osborne, 2003
[44] Shon Harris, “Cissp All-In-One Exam Guide (All-In-One)”, Osborne, 2003
[45] 内閣府, “ソフトウェア懇話会の報告書について”
http://www8.cao.go.jp/cstp/torikumi/torikumi.html
[46] 総務省, “情報セキュリティ対策の状況調査結果”,
http://www.soumu.go.jp/s-news/2002/020509_2.html
[47] 総務省, “地方公共団体における情報セキュリティポリシー（情報セキュリティ対策に関する基本方針）等の策定状況”
http://www.soumu.go.jp/s-news/2003/031107_3.html
[48] 総務省, “「情報通信ソフト懇談会」中間報告書の公表”,
http://www.soumu.go.jp/s-news/2003/030725_5.html
[49] 経済産業省, “情報セキュリティ総合戦略”
http://www.meti.go.jp/policy/netsecurity/strategy.htm
[50] 警察庁, “不正アクセス行為対策の実態調査”
http://www.npa.go.jp/hightech/cyberterror/nsresearch07/
[51] “コンピュータ不正アクセス対策基準”,
http://www.meti.go.jp/policy/netsecurity/UAaccessCMG.htm
[52] “コンピュータウイルス対策基準”
http://www.meti.go.jp/policy/netsecurity/CvirusCMG.htm
[53] “システム監査基準”
http://www.meti.go.jp/policy/netsecurity/systemauditG.htm
[54] “ソフトウェア管理ガイドライン”
http://www.meti.go.jp/policy/netsecurity/downloadfiles/softkanri-guide.htm
[55] “情報セキュリティ監査制度”
http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Audit_Annex01_1.doc
http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Audit_Annex02.doc
http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Audit_Annex03_1.doc
http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Audit_Annex03_3.doc
http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Audit_Annex04.doc
http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Audit_Annex05.doc
http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Audit_Annex06.doc
http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Audit_Annex06.doc
http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Audit_Annex07.doc
[56] 情報処理技術者試験センター, http://www.jitec.jp/
[57] 情報処理技術者スキル標準, http://www.jitec.jp/1_17skill/skill_00.html
[58] 経済産業省, “IT スキル標準”, http://www.meti.go.jp/policy/it_policy/jinzai/g030701aj.html
[59] IPA, “IT スキル標準センター”, http://www.ipa.go.jp/itss/
[60] ネットワーク情報セキュリティマネージャー（ＮＩＳＭ）資格
http://www.learningsite21.com/nism/top.html
[61] NTT コミュニケーションズ, “インターネット検定”, http://biz.ocn.ne.jp/master/index.html
[62] インターネット協会, “インターネットにおけるルール＆マナー検定”
http://www.iajapan.org/
[63] SEA/J, “Security Education Alliance/Japan”, http://www.sea-j.net/
[64] ISC^2, “CISSP Certification Common Body of Knowledge Study Guide”,
http://www.isc2.org/cgi-bin/request_studyguide.cgi.
[65] SANS, “GIAC (Global Information Assurance Certification)”, http://sans-japan.jp/
[66] ISACA, “CISM (Certified Information Security Manager)”, http://www.isaca.org/
[67] CSI, “CSI (Computer Security Institute)”, http://www.gocsi.com/
[68] CompTIA, “Security+”, http://www.comptia.jp/

[69] ISSEA, “SSE-CMM”, http://www.issea.org/
[70] Cisco, “Cisco Firewall Specialist／VPN Specialist／IDS Specialist”, http://www.cisco.com/jp/
[71] Check Point, “CCSA（Check Point Certified Security Administrator）／CCSE（Check Point Certified Security Expert）”, http://www.checkpoint.com/
[72] Baltimore , “E|security Master”, http://www.baltimore.co.jp/
[73] Purdue University, “Department of Computer Sciences, Course Information”, http://www.cs.purdue.edu/courses/
[74] CMU, “MUISTM (Master of Science in Information Security Technology and Management”, http://www.ini.cmu.edu/academics/MSISTM/msistm_overview.htm
[75] NIST CSRC, “SP 800-16 Information Technology Security Training Requirements”, http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf
[76] 東京大学大学院教育プロジェクト室, “東大工学教育プロジェクト「工学知の構造化と可視化」”, カレッジマネジメント, 2003 http://www.t.u-tokyo.ac.jp/esp/college_management119.pdf
[77] 日経 BP BizTech, “2003 年の米国技術者と管理者の平均給与は年間 8 万 8900 ドルで前年から減少”, http://biztech.nikkeibp.co.jp/wcs/leaf/CID/onair/biztech/biz/265985
[78] 日経 BP IT Pro, “腕試し！　あなたのセキュリティ知識をチェック” http://itpro.nikkeibp.co.jp/free/NBY/ITBASIC/20030620/1/
[79] 日経 BP IT Pro, “記者の眼： お受験体質が技術者を弱くする” http://itpro.nikkeibp.co.jp/free/ITPro/OPINION/20020514/1/
[80] 日経 BP IT Pro, “記者の眼： IT エンジニアのコアスキル，年収・職種で有意な差” http://itpro.nikkeibp.co.jp/free/ITPro/OPINION/20021120/1/
[81] 日経 BP IT Pro, “記者の眼： IT エンジニア教育の改革が日本を救う” http://itpro.nikkeibp.co.jp/free/ITPro/OPINION/20030714/1/
[82] 日経 BP IT Pro, “記者の眼： あなたは自分をプロの IT エンジニアと言えるか？” http://itpro.nikkeibp.co.jp/free/ITPro/OPINION/20020204/1/
[83] 日経 BP IT Pro, “記者の眼： 結果発表！「IT 資格意識調査」” http://itpro.nikkeibp.co.jp/free/ITPro/OPINION/20030401/1/
[84] 日経 BP IT Pro, “記者の眼： 情報処理技術者試験の今日的意義を考える” http://itpro.nikkeibp.co.jp/free/ITPro/OPINION/20020506/1/
[85] 日経 BP IT Pro, “記者の眼：日本で初めての職業別スキル・スタンダード，ITSS を活かせ” http://itpro.nikkeibp.co.jp/free/ITPro/OPINION/20030130/1/
[86] NIKKEI Net IT Business & News, ”ネット時評： 情報セキュリティー教育を考える”, http://it.nikkei.co.jp/it/njh/njh.cfm?i=20030924s2001s2
[87] NIKKEI Net IT Business & News, “ネット時評：有害プログラム対策を考える～ブラスター・ワームの被害から学ぶ～”, http://it.nikkei.co.jp/it/njh/njh.cfm?i=20030813s2000s2
[88] ZDNet エンタープライズ, ”Linux Column：「どうする？セキュリティ教育」”, http://www.zdnet.co.jp/enterprise/0204/02/02040288.html
[89] @IT, “セキュリティ技術者を「憧れの職業」にするには？” http://www.atmarkit.co.jp/fsecurity/column/sudoh/09.html
[90] @IT 自分戦略研究所, “新 DATA で見る「IT 系エンジニア」求人動向”, http://jibun.atmarkit.co.jp/lcareer01/rensai/kyujin/kyujin08.html
[91] @IT 自分戦略研究所, “こんなセキュリティエンジニアが欲しい（第 1 回～第 3 回）”, http://www.atmarkit.co.jp/fengineer/special/jinzaisec1/jinzaisec01.html http://www.atmarkit.co.jp/fengineer/special/jinzaisec2/jinzaisec01.html http://www.atmarkit.co.jp/fengineer/special/jinzaisec3/jinzaisec01.html
@IT 自分戦略研究所, “特別企画：セキュリティ技術の学び方” http://www.atmarkit.co.jp/fengineer/special/security_edu01/sec_edu01.html
[92] @IT 自分戦略研究所, “ファイアウォール・スペシャリストになるには”, http://jibun.atmarkit.co.jp/fengineer/special/tofwall/fwall01.html
[93] @IT 自分戦略研究所情報, “セキュリティ・コンサルタントになるには”, http://www.atmarkit.co.jp/fengineer/special/tosepolicy/sepolicy.html
[94] @IT 自分戦略研究所情報, “不正侵入検知のスペシャリストになるには”, http://www.atmarkit.co.jp/fengineer/special/tosecids/secids.html
[95] @IT 自分戦略研究所情報, “セキュリティエンジニアになるための条件（前編／後編）”, http://jibun.atmarkit.co.jp/fengineer/special/tosecurity01/tosecurity01.html http://jibun.atmarkit.co.jp/fengineer/special/tosecurity02/tosecurity02.html
[96] @IT 自分戦略研究所情報, “いまネットワークで求められる技術とは” http://jibun.atmarkit.co.jp/lskill01/special/tonet01/nettrend01/nettrend01.html

[97] @IT Engineer Life, “リレーエッセイ：エンジニアに資格は必要か？”
http://jibun.atmarkit.co.jp/fengineer/index/index_all.html#qualify
[98] japan.internet.com, 企業の情報セキュリティ、「ルール明文化」と「従業員教育」が重要”,
http://japan.internet.com/wmnews/20030728/5.html
[99] Mainichi Interactive, “進まぬ企業の情報セキュリティー　定期的な社員教育は 1 割”,
http://www.mainichi.co.jp/digital/network/archive/200307/28/1.html
[100] Asahi.com, “成果主義の「崩壊」　給料と直結やめた 1 部上場企業も”,
http://www.asahi.com/job/special/TKY200309030144.html
[101] Asahi.com, “元部長が告白、「大企業人事部は外資系に丸投げだった」”,
http://www.asahi.com/job/special/TKY200309100217.html
[102] About, “Security Certification Essentials”
http://certification.about.com/library/weekly/aa040102a.htm
http://certification.about.com/
[103] Information Security Magazine, “Translating Security For Managers”
http://infosecuritymag.techtarget.com/articles/august01/securitymarket.shtml
[104] Information Security Magazine, “Security Still Pays”
http://infosecuritymag.techtarget.com/2002/aug/securitymarket.shtml
[105] SearchSecurity.com, “Security Career Center – Salay Survey”,
http://searchsecurity.techtarget.com/salarySurveyResults/0,289723,sid14_idx1,00.html