NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

JNSAワーキンググループ
2004年度成果報告会

教育部会
スキルマップ作成WGの活動について

佐久間 敦
株式会社 富士総合研究所
2005年6月13日

アジェンダ

1. スキルマップの背景
2. スキルマップの経緯と現状
3. 情報セキュリティ人材育成におけるミスマッチ再考
4. スキルモデルのアプローチ
5. 評価問題集
6. 今後の展開と課題

JNSA 教育部会について

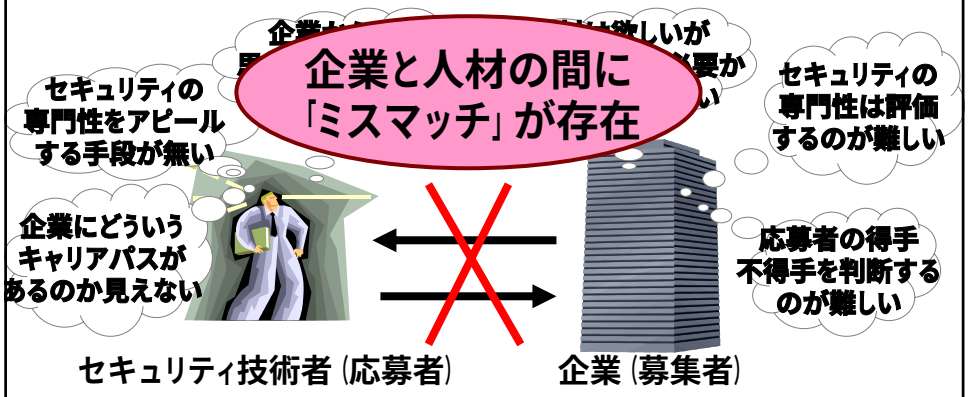
- 部会長：東京電機大学　佐々木先生
- セキュリティの教育に関する諸問題について検討
- 国や関連団体等からの支援を受けて調査・研究・実証実験を実施
- スキルマップ作成WGの活動と成果
  - セキュリティに携わる、開発者、コンサルタント、SE、教育機関など、幅広いバックグラウンドの人が参加
  - 過去3年間スキルマップの作成とその応用について検討
    - IPA「情報セキュリティプロフェッショナル育成に関する調査研究」(H14)
    - IPA「情報セキュリティスキルマップ構築の調査研究」(H15)
    - IPA「情報セキュリティスキルマップの普及促進に向けた調査研究」(H16)

2005年度教育部会の活動
- CISSPーWG
- 情報セキュリティ教育WG

1．スキルマップの背景

企業の現場での問題

- 情報漏洩、ウィルス、不正アクセス・・・
  ⇒ 企業において、情報セキュリティ対策が急務
- でも、「人」がいない！



問題意識

- 「情報セキュリティ技術者」って？
  ⇒ 人それぞれイメージが違う
- 人材が足りない？人材育成の問題は何？
  ⇒ 企業と教育機関の間にも「ミスマッチ」
- どうすれば人材育成が進む？
  ⇒ セキュリティプロに求められる「スキル」とは？

スキルマップWGの取り組み

- セキュリティに携わる、開発者、コンサルタント、システムエンジニア、ベンダ、教育機関など、幅広いバックグラウンドの人が参加
- 過去3年間スキルマップの作成とその応用について検討を継続
- 昨年度は、スキルマップの普及に向けて、企業の現場での適用例の検討や利用ガイドラインを策定

2．スキルマップの経緯と現状

「スキルマップ」とは？

技術知識の習得の度合い（レベル）を定量的に表現する「評価のものさし」を目指そう！

- 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**したもの（→ 16個の大分類）
- 学問的な分類体系よりも、**実用本位、実務本位**を重視。ＪＮＳＡスキルマップＷＧのメンバーが作成を担当
- 教育カリキュラムやテキスト、スキルスタンダードの作成する際の参照ベース

スキルマップの大分類

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

- 上記１６分類以下に中分類、小分類を階層的に整理
- 応用・発展分野への拡張にも対応

スキルマップのサンプル：「情報セキュリティマネジメント」

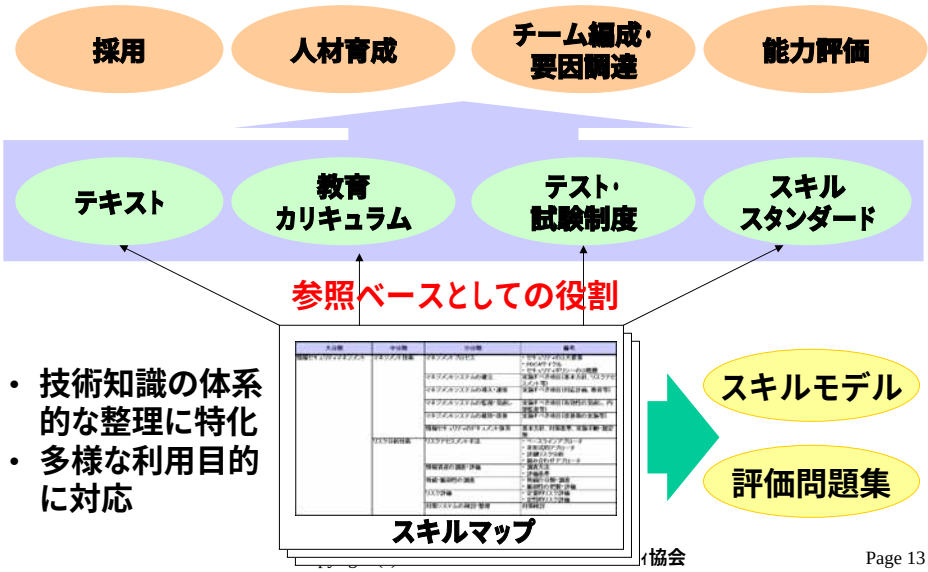
大分類	中分類	小分類	備考
情報セキュリティマネジメント	マネジメント技術	マネジメントプロセス	・セキュリティの3大要素 ・PDCAサイクル ・セキュリティポリシーの3階層
		マネジメントシステムの確立	実施すべき項目（基本方針、リスクアセスメント等）
		マネジメントシステムの導入・運用	実施すべき項目（対応計画、教育等）
		マネジメントシステムの監視・見直し	実施すべき項目（有効性の見直し、内部監査等）
		マネジメントシステムの維持・改善	実施すべき項目（改善策の実施等）
		情報セキュリティのドキュメント体系	基本方針、対策基準、実施手順・規定類
	リスク分析技術	リスクアセスメント手法	・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

（抜粋）

スキルマップの特徴

- スキルマップの分類は学問的な分類法というよりは、実際に使われている製品や技術に則して体系化
- 各項目は絶対的なものではなく、利用者がニーズや使途に応じてカスタマイズすることができる
- 「スキルモデル」、「レベルチェックテスト」などのバリエーション

スキルマップの役立ち



- 技術知識の体系的な整理に特化
- 多様な利用目的に対応

情報セキュリティプロフェッショナル総合教科書

- 監修: 佐々木良一(東京電機大教授)
- 著者：JNSA教育部会 スキルマップ作成ワーキンググループ
- ISBNコード：4-7980-0880-X
- 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、スキルマップの16項目の大分類に体系化して整理・解説

3．情報セキュリティ人材育成における ミスマッチ再考

これまでの検討の論点

- 「セキュリティ技術者」は、独立した職種としてとらえることはできるか？？
  ⇒ むしろ、様々な職種にセキュリティが絡んでくる
  例：「セキュリティが得意なネットワークエンジニア」

- 業種・業界・職種で異なる情報セキュリティのスキルをどう教育するか？？そして、能力をどう評価する？？
  ⇒ 画一的な試験や資格制度には限界がある
  その資格を持っていても、何ができるのかわからない

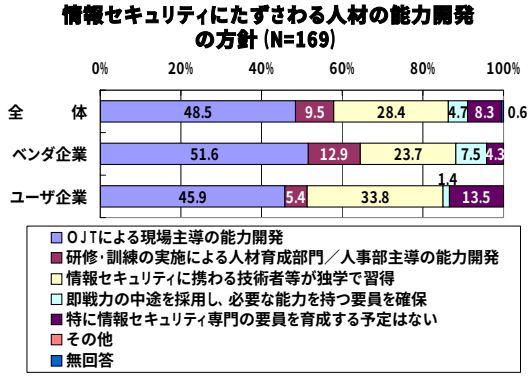
セキュリティに関わる職種

- そもそも、セキュリティエンジニアとは？
  - 顧客の要求希望をまとめてシステムインテグレーションの提案などを行うシステムエンジニア
  - 脆弱性調査やLOG解析などを行いインシデント対応行うネットワークエンジニア
  - セキュリティ機器販売に伴う設定や顧客対応を行うサポートエンジニア
  - 顧客のセキュリティ関連のポリシーなどを構築するコンサルタント
  - ハード／ソフトのセキュリティ機能を作りこむ開発系エンジニア
  - などなど

- これまでは、十羽一絡げで人材育成や能力評価の問題を議論
  ⇒ これが、**「ミスマッチ」を産んでいる原因**のひとつにも

セキュリティ教育の難しさ

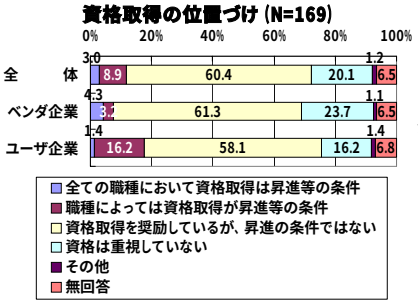
- 約半数の企業がOJTをセキュリティ技術者の教育の柱にしている
- 実際は、時間的制約や教える側の能力の問題が大きく、表面的なことに終始してしまうことも

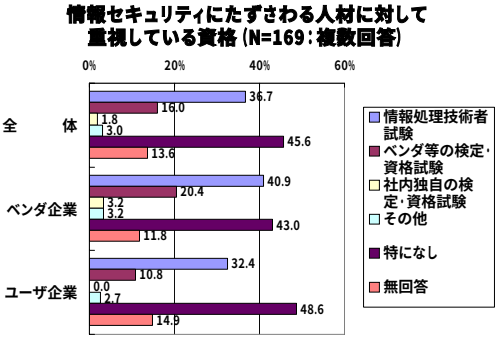


IPA「情報セキュリティプロフェッショナル育成に関する調査研究」より

情報セキュリティと資格

- 企業では資格の取得を奨励するも、昇進･昇給の条件としている会社は多くない
- 日進月歩の技術の変化に制度がどう対応するかが一番の課題
- 消防関係の国家資格「危険物取扱者」では資格と能力の対応がわかりやすく、セキュリティの分野でも参考になるかも？？





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」より

セキュリティ人材の中途･経験者求人の現状

- 既存の就職･転職サイト、人材関連情報誌等において、情報セキュリティ関連人材の募集が急増している。
- 募集職種は下記のとおり多岐にわたっており、同じ職種名でも業務の内容には大きな差異が認められる。
- 情報セキュリティの能力要件定義の難しさもあって、企業と人材との間で「ミスマッチ」を産む懸念。

4. スキルモデルのアプローチ

「スキルモデル」について

- セキュリティに関するスキルについての論点
  - 情報セキュリティ技術者のスキルとは何か？
    ⇒ 職種によって違う！
  - 個別の知識の習得度合いを客観的に判断したい
  - スキルに「レベル」はある？？
    ⇒ セキュリティの場合、「年功序列」でレベルが決まるものではないはず？？

情報セキュリティに関する「スキルモデル」を策定

- 個別の**業務やタスク**において求められる**スキルとレベル**を整理
- 幅広い用途に活用するため、**カスタマイズ可能なモデル**を目指す

スキルモデルのサンプル

業務名：不正アクセス対策システム導入

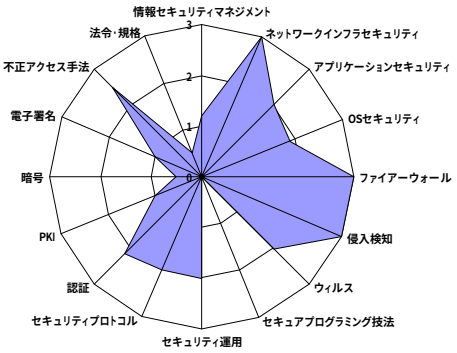
Ⅰ．業務の説明

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

- 特になし

スキルモデルの利用場面

- **採用**
  - **中途採用しようとする際に職務要件書（Job Description）として**
- **人材育成**
  - キャリアパスの目標設定
  - どこを重点的に学習すれば良いか、方向付け
- **チーム編成／要員計画**
  - プロジェクトチームの結成にあたって必要な人員の計画策定
- **能力評価**
  - エンジニアが自分のスキルのレベルを評価する「ものさし」として活用
- **調達**
  - コンサルタント、エンジニアを調達する際の調達要件書において活用

セキュリティ人材採用における問題点

- 企業側
  - 「欲しい人材を見つけるの難しい」
  - 「セキュリティの経験あり、といっても様々なレベルがある」
  - 「資格を持っていても、どのようなことができる人なのか良くわからない」
- 応募者側
  - 「募集要項を見ても、入社後にどのような業務や仕事に携わるのかイメージしづらい」
  - 「専門性をアピールしても伝わらない」

企業側／応募者側のコミュニケーションのギャップを解消するための
コミュニケーションツールとして、**「人材採用向けスキルモデル」**を策定

人材採用向けスキルモデルの考え方

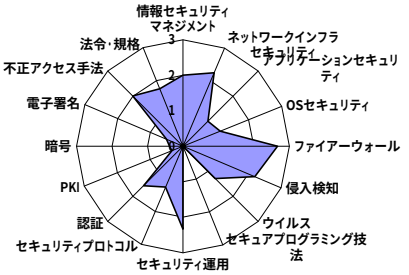
＜人材の採用における評価の考え方＞

専門的な知識・スキルの価値 × 業務の経験・実績 × ベーシックなビジネススキル

人材採用向けスキルモデルのスコープ

- 人材採用向けスキルモデルの構成
  - （Ⅰ）**スキルレベルシート**：どのような業務経験ないし実績を有しているか？（業務の内容、規模・期間、顧客の業種、業務での役割等）
  - （Ⅱ）**実績シート**：　どのような能力を持っているか？（保有しているスキルの種類とレベル、スキルの発揮、製品等の経験、資格・特技等）

（Ⅰ）スキルレベルシート

カテゴリ	項　目	保有スキル
Ⅰ．業務関連スキル	個別の業務知識	担当官公庁の業務関連システム及び法律に関する知識
	業界に関する知識	官公庁のIT予算に関する動向に関する知識
	その他	官公庁に対する営業ノウハウ
Ⅱ．ITスキル	ネットワーク関連	LANの基礎、インターネット／WAN基礎、ＴＣＰ／IP基礎
	OS関連	Windowsサーバインストール、Windowsサーバ運用設定
	開発関連（言語、DB、ﾐﾄﾞﾙｳｪｱ等）	
	その他	
Ⅲ．セキュリティスキル	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(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 その他	
Ⅳ．資格・特技	公的資格	情報処理技術者試験（情報セキュリティアドミニストレータ）
	ベンダ資格	
	その他	

* 「セキュリティスキル」のレベルについて

Level 0：　知識項目について聞いたことがある程度の水準である。関連する知識を活用する業務の経験はない。

Level 1：　知識項目の基本的な内容について理解している水準である。メンバーとして業務の担当する部分で、習得した知識項目を他の指導・援助を得つつ実践することができる。

Level 2：　知識項目の技術的な詳細について理解している水準である。メンバーあるいはサブリーダとして、業務の担当する部分について知識を活用して自力で実践でき、責任を負うことができる。

Level 3：　知識項目に関して、実務経験を通じた豊富なノウハウを持っており、他者に対して指導できる水準である。リーダーとして当該業務の全体の責任を負うことができる。

（Ⅱ）実績シート

No.	期間	顧客業種	担当業務内容（役割）	共通Tスキル	セキュリティ関連タスク										セキュリティスキルの詳細							
					A.調査分析	B.提案コンサル	C.基本設計	D.詳細設計	E.PG作成	F.導入設定	G.保守運用管理	H.教育	I.事故対応	J.監査・検査	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
1	1999.6 ～ 2000.1	民間企業 公的機関	ファイアーウォール、IDS製品のサポート （　サポート担当　）							○				○	異常時対応 パッチ適用				ファイアーウォール製品Aサポート		IDS製品Bサポート 不正アクセス手法の調査	
2	2000.1 ～ 2001.9	公的機関	ファイアーウォールの導入提案、基本設計、販売及び事後フォロー。 （　営業担当　）	Windows TCP/IP		○	○			○				○	緊急時対応				ファイアーウォール製品C導入設定			
3	2001.10 ～ 2002.3	公的機関	公的機関向けセキュリティ研修の企画、立案、教材作成及び講師スケジュール管理（講師5名）。 （　サブリーダー　）			○						○			セキュリティポリシー解説 ユーザのセキュリティ運用解説							関連法規の解説
4	2002.3 ～ 2002.12	公的機関	顧客の全国50箇所の拠点にVPN機器を導入、全体進捗管理、契約・官庁対応、導入教育の講師を担当（要員規模100人程度 （　プロジェクトリーダー　）	Windows TCP/IP		○	○			○		○				NW設計＋VPN製品D導入設定 IPSec	認証ポリシーの策定		NW設計＋VPN製品E導入設定		不正アクセス手法の調査	関連法規の解説
5			（　　）																			

5．評価問題集

スキルレベルチェックテスト

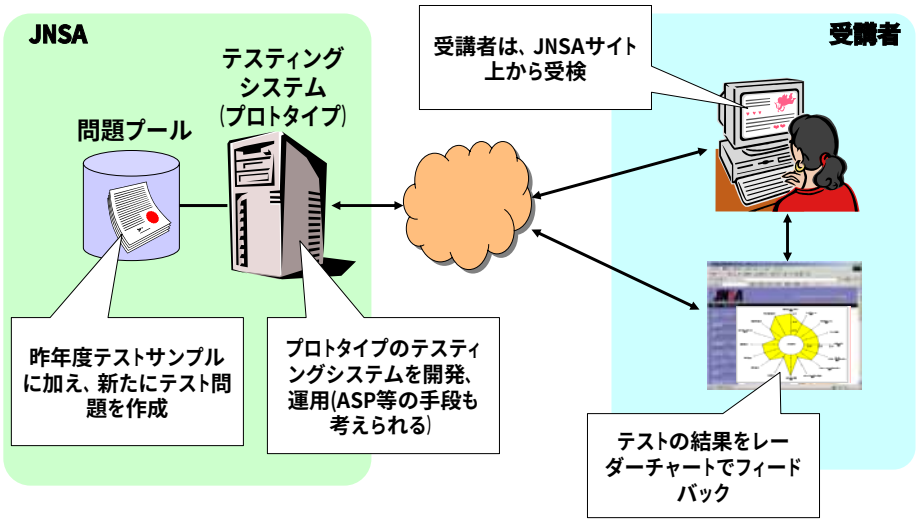
- スキルレベルチェックテストについて
  - 情報セキュリティに関する基本的な知識について自己評価を行なうための問題と解答のリスト
  - 他者評価／第三者評価にも活用
- 問題形式は4問択一方式
  - タイプ1：言葉を問う（穴を埋める）問題
  - タイプ2：意味を問う問題
  - タイプ3：プロセスを問う問題

今年度は、本格的なテストプールの構築に向けて、大分類ごとに各10問（合計160問）のサンプルテストを作成
(IPAのホームページで公開中)

スキルレベルチェックテストの例
(ファイアーウォールの導入)

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	タイプ2 (意味を問う問題)
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

Webトライアル検定 (案)



6．今後の展開と課題

スキルマップの今後の展開

- 根源的な問題
  - セキュリティ技術者にとって、技術知識以外の「能力」や「スキル」とはなにか？？
  - 次々と変化する技術や変化にどう対応するか？
- セキュリティ能力検定の可能性と課題
  - 評価問題集をベースとしてWeb上で能力検定を実施
- 情報セキュリティ人材育成に向けた課題
  - 教育機関と民間企業の連携強化
  - 情報セキュリティ教育に関する検討を行なうための「場」づくり

ご静聴、ありがとうございました

参考資料

(参考) 関連URL

- 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」(H14)
  - http://www.ipa.go.jp/security/fy14/reports/professional/ikusei-seika-press.html
  - http://www.meti.go.jp/kohosys/press/0003929/
- IPA「情報セキュリティスキルマップ構築の調査研究」(H15)
  - http://www.ipa.go.jp/security/fy15/reports/skillmap/index.html
- IPA「情報セキュリティスキルマップの普及促進に向けた調査研究」(H16)
  - http://www.ipa.go.jp/security/fy16/reports/skillmap/index.html

(参考) スキルマップの大分類・中分類 (1)

No.	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	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、予防ポリシ、発病、検出方法と駆除、感染、種類

(参考) スキルマップの大分類・中分類 (2)

No.	大分類	中分類
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、PHPJAVA、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