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
２００３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

２００４年5月１８日

アジェンダ

- JNSA **教育部会 スキルマップ検討**WG**について**
- **「情報セキュリティプロフェッショナルの育成に関する調査研究」について**
- **「情報セキュリティのためのスキルマップ」の構築に関する研究**
- **まとめ**

JNSA 教育部会について

- **教育部会　(部会長：佐々木先生)**
  - **スキルマップ作成**WG
    - 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)
  - ITSS**実証実験評価** WG
    - **経済産業省** IT**スキルスタンダード教育実証実験に参加** (H15)
      「ケースメソッドによるセキュリティスキルアップ教育」を実施

スキルマップWGのモチベーション

- 「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ある「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

- 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）に現状に関する調査研究
- 「情報セキュリティのためのスキルマップ」の構築

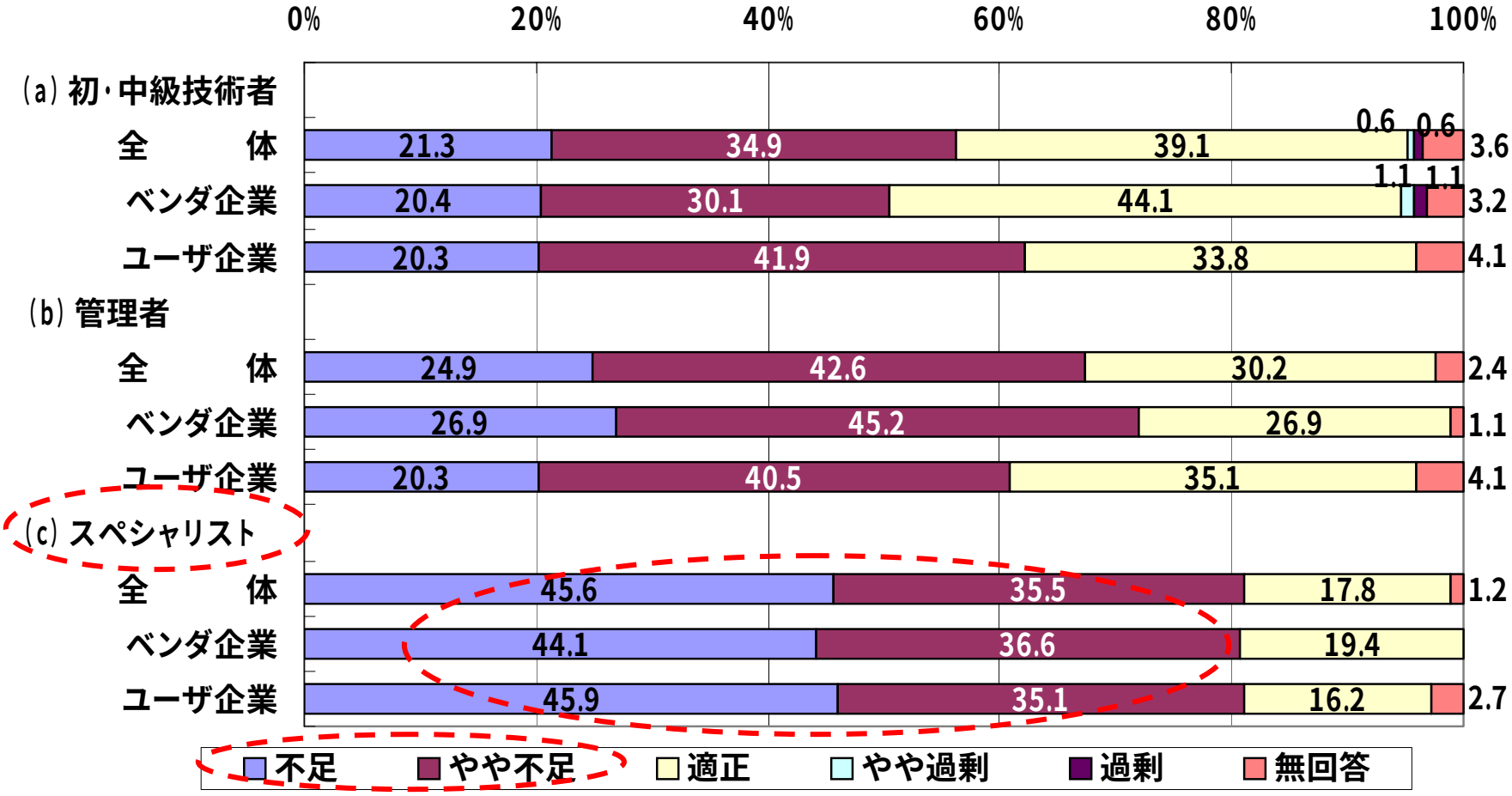
「情報セキュリティプロフェッショナルの育成に関する調査研究」（H14実施）の結果から

アンケート調査の概要

- **調査の目的**
  - **ベンダ企業（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）、ユーザ企業（一般企業）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を把握する。**
- **調査期間**
  - 2002年11月22日～12月13日
- **調査方法**
  - **国内民間企業1000社に対して調査票郵送**
  - **有効回答数 169通（回収率 17%）**

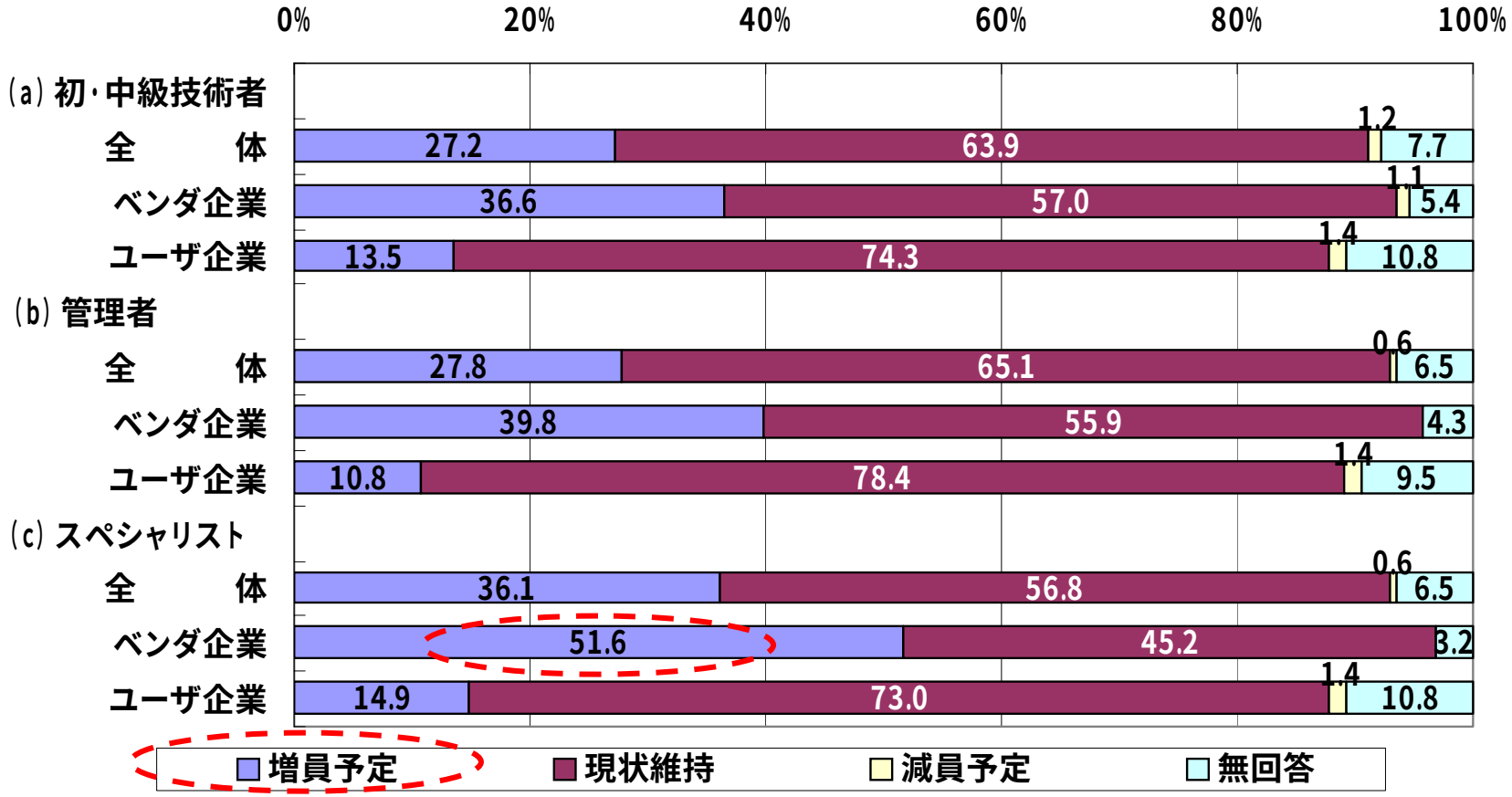
人材の過不足感

- ベンダ企業、ユーザ企業とも、全ての職種で、**過半数が人材の不足感**を感じている。
- 特に、情報セキュリティ専門の技術者として高度な知識とスキルを有する「**スペシャリスト**」へのニーズが高い。



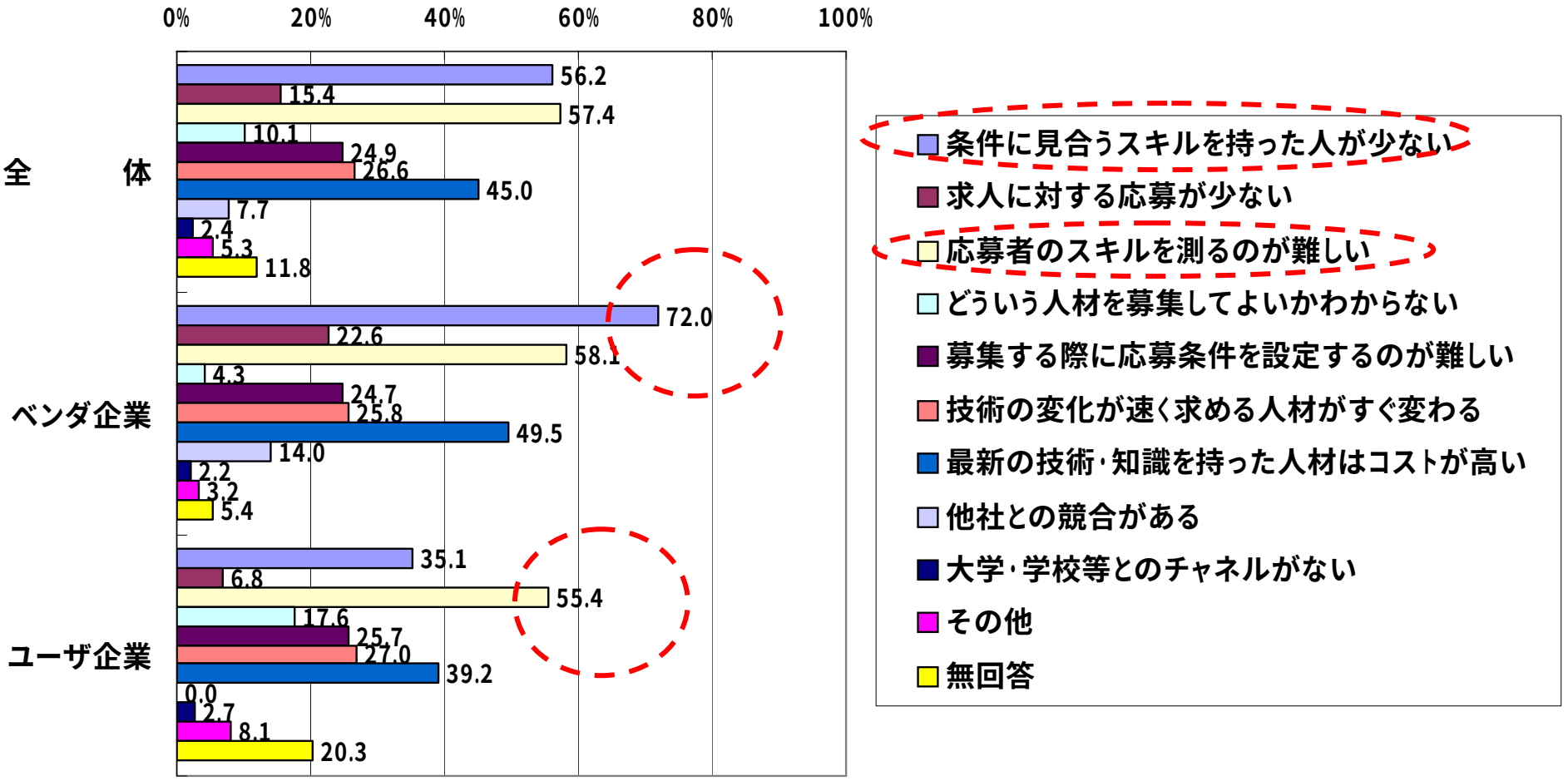
増員、減員の予定

- ベンダ企業、ユーザ企業ともに積極的な増員を予定している企業は、現時点ではそれほど多くはないが、**総じて増加傾向**にあるといえる。
- ベンダ企業では**スペシャリストを増員**すると回答した企業が過半数を超え、特にSIerでは74.2%が増員予定。



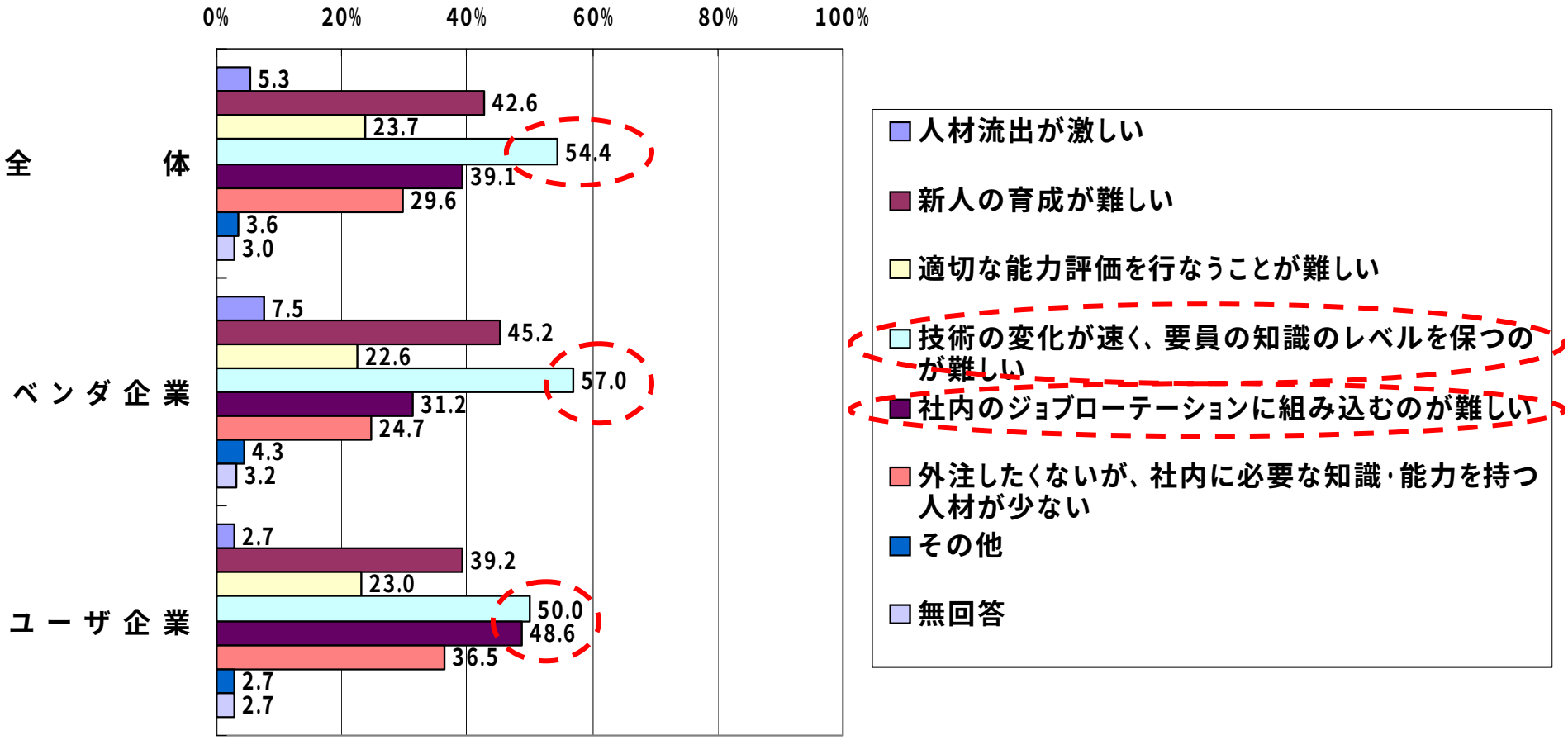
人材の採用における問題点

- ベンダ企業では「条件に見合うスキルを持った人が少ない」、ユーザ企業では「応募者のスキルを測るのが難しい」と回答する割合が高い
- ユーザ企業では「どういう人材を募集してよいかわからない」ことも大きな問題の一つ。



人材の確保における問題点

- ベンダ企業、ユーザ企業ともに、**「技術の変化が速く、要員の知識のレベルを保つのが難しい」**ことがもっとも大きな課題
- ユーザ企業では**「社内のジョブローテーションに組み込むのが難しい」**ことも問題になっている



問題意識
(H14年度調査研究のまとめ)

- 情報セキュリティに関する高度な知識や能力、経験を有した人材が不足
- 教育機関においては、実務能力の教育が十分になされていない
- 情報セキュリティにかかわる知識、技術は、非常に幅広い分野に渡る。職種や業種によって、求められる知識の内容やレベルも大きく異なる。
- 情報セキュリティに関する人材育成を難しくしている原因
  - 求める人材像を定義することが難しい
  - 能力を測る共通の評価基準がないこと
  - 技術の変化が速く、要求する知識や技術の内容や水準もそれに対応して変わっていく

人材育成における「ミスマッチ」

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

「情報セキュリティのためのスキルマップ」の構築に関する研究

「スキルマップ」とは？

- 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）
- 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」を目指す
- 学問的な分類体系よりも、実用本位、実務本位な観点から、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、コンサルタントらが自らが作成
- 「スキルモデル」、「レベルチェックテスト」などの応用

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）

「スキルモデル」について

- 情報セキュリティプロフェッショナルのスキルに関する論点
  - 情報セキュリティ技術者は、独立した職種として捉えることができるか？
  - 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の必要性

- スキルマップに関する論点
  - 業種、職種、業務で求められるスキルとそのレベルは異なる
  - カスタマイズ可能なレベル定義に対するニーズ

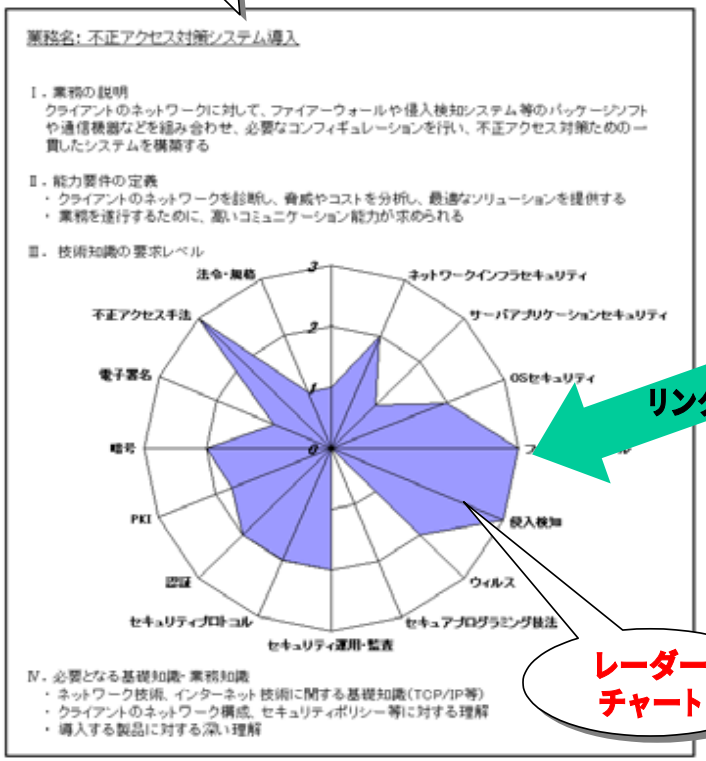
情報セキュリティに関する「スキルモデル」の策定

- 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
- 人材育成や採用、能力評価、調達など、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

スキルモデルの概要

スキルモデル
のフォーマット

「Ⅰ．業務の説明」「Ⅱ．能力要件の定義」「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」「Ⅴ．補記事項」



スキルレベル
テーブル

スキルマップの中分類に
「レベル」を設定

大分類	中分類	レベル
PKI	PKIの利用	2
	証明書と認証	1
	証明書失効	2
	信頼モデル	1
	契約モデル	3
	記述とデータ方式	1
	規格	3
	公開リポジトリ	1
	認証局の構築と運用	2
	法的枠組み	2
	PKIが提供するサービス	1

○ レベル定義
レベル0：（知識なし）
レベル1：概念は理解している
レベル2：技術的な詳細を説明できる
レベル3：専門家としての深い知識を有する

リンク

レーダー
チャート

スキルマップの大分類に対して「レベル」
のオーバービューを表現

Level 0 ： 知識がない、または、経験がない
Level 1 ： 知識項目の概要を理解している水準
Level 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
Level 3 ： 知識を活用して、業務を自力で実践できる水準

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
  - 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を方向付け
- 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
  - 現在のスキルレベルを評価する指標の一つとして活用
- 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

「スキルレベルチェックリスト」

- スキルレベルチェックリストについて
  - 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できるものを目指す
- スキルレベルチェックテストの問題形式
  - 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

スキルレベルチェックリストの例 (ファイアーウォールの導入)

JNSA

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

まとめ

ー 情報セキュリティにたずさわるの人材の育成に向けて ー

再び、ミスマッチ

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

スキルマップの今後の展開

- スキルマップの活用に向けた課題
  - 技術知識以外の能力･スキルへの展開
  - 事例研究等を通じたノウハウやナレッジの共有化
  - 知識項目間の関連性、相関性の整理
- スキルマップに基づく能力検定の可能性と課題
  - スキルレベルチェックのベータテスト
  - スキルレベルチェックのWeb能力検定の提供
- 情報セキュリティ人材育成に向けた課題
  - 民間と教育間の連携強化
  - 情報セキュリティ教育に関する検討を行なうための「場」の活性化

ご静聴、ありがとうございました

本件のお問い合わせ先：
佐久間（富士総合研究所）sakuma@cyg.fuji-ric.co.jp

参考資料

(参考) 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

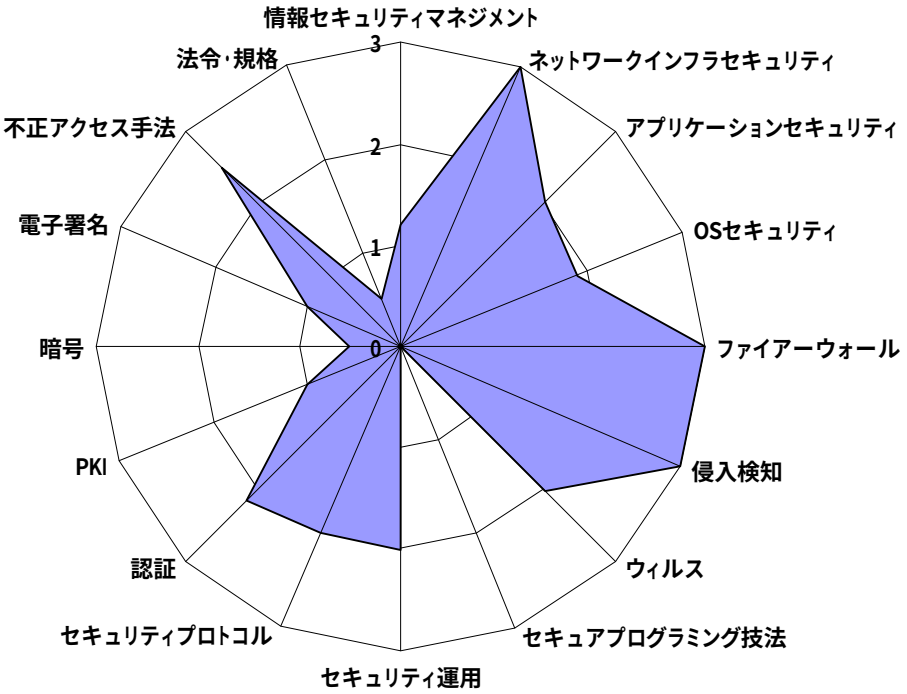
Ⅰ. 業務の説明

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

(参考) スキルレベルチェックリストのサンプル

JNSA

Q1　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。(「侵入検知」からの出題)

A)　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。
B)　通信を暗号化し機密性を確保する。
C)　不正アクセスを検出し、管理コンソールに通知する。
D)　アクセス制御 (コントロール) する。

Q2　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。
(「ネットワークインフラセキュリティ」からの出題)

A)　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。
B)　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。
C)　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。
D)　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。

Q3　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。

A)　証明書の内容が改竄されていないこと。
B)　証明書が有効期限内であること。
C)　証明書が確かに認証局によって発行されたこと。
D)　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。

答え: Q1－C ／ Q2－C ／ Q3－B

(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