

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

松田 剛

教育部会 Skillmap作成WGリーダー

株式会社ヒューコム SMS事業本部

2003年 6月3日

WorkGroup紹介



教育部会Skillmap作成WGは、情報処理振興事業協会(IPA)の「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」事業の実行主体として平成14年度に発足

参加企業 (順不同)

ソニー株式会社、NTTコミュニケーションズ株式会社、横河電機株式会社、日本ネットワークアソシエーツ、TIS株式会社、セコム株式会社、株式会社インターネット総合研究所、NPOアイタック、クロスヘッド株式会社、株式会社インフォセック、工学院大学、株式会社アイセス、NECソフト株式会社、アライドテレシス株式会社、株式会社ディアイティ、株式会社富士総合研究所、株式会社ヒューコム

計17社

「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」事業は、経済産業省の補助事業として、情報処理振興事業協会 (IPA) により、NPO日本ネットワークセキュリティ協会及びNPOネットワークリスクマネジメント協会 (NRA) に下記を目的に委託された。

- 1) 政府、企業等において情報セキュリティに携わる人材、すなわち「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及び技術を明らかにするため、教育の現状、求められている技術等について調査し、現状を把握するとともにその原因を究明する。
- 2) 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及び技術を客観的に評価するためスキルマップを策定するとともに、地方企業等における人材育成策をとりまとめ、情報セキュリティプロフェッショナル育成を促進する。

1) 情報セキュリティに携わる人材の現状
アンケート調査

2) 情報セキュリティ教育の現状
大学・専門学校等へのヒアリング調査

3) 情報セキュリティに関するスキルマップ開発

(同時にNPOネットワークセキュリティ協会が地方自治体における人材育成策調査もあわせて実施した)

第一編

ベンダ企業/ユーザ企業における情報プロフェッショナル育成に関する調査結果

アンケート調査概要

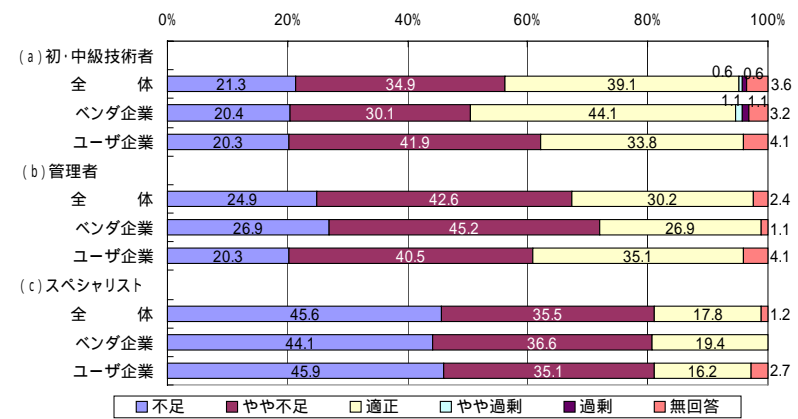
- 調査の目的：
 - 情報セキュリティ関連の製品、サービスの開発 / 提供 / 販売等を行っているベンダ企業における情報セキュリティにたずさわる人材の育成の状況を把握する。
 - 情報システムを運用 / 管理しているユーザ企業(一般企業)における情報セキュリティにたずさわる人材の育成の状況を把握する。
- 調査方法： 調査票の郵送による発送・回収
- 送付数及び抽出方法： 1.及び2.の合計 1,000社。
 1. JNSA会員企業(153社) + 電機計算機製造、ソフトウェア開発、情報処理サービス等を行なう株式会社(347社: 民間データベースより抽出)
 2. 東証1部・2部上場企業より任意抽出(500社: 1.との重複を除く)
- 実施時期：2002年11月22日～12月13日
- 回収率：169社 (回収率 17%)

- 1) 企業における情報セキュリティに携わる人材の現状
- 2) 情報セキュリティに携わる人材に要求されるスキル
- 3) 企業における情報セキュリティ教育の現状

1. 企業(ベンダ企業、ユーザ企業)における 情報セキュリティにたずさわる人材の現状

情報セキュリティに携わる人材の過不足感 **JNSA**

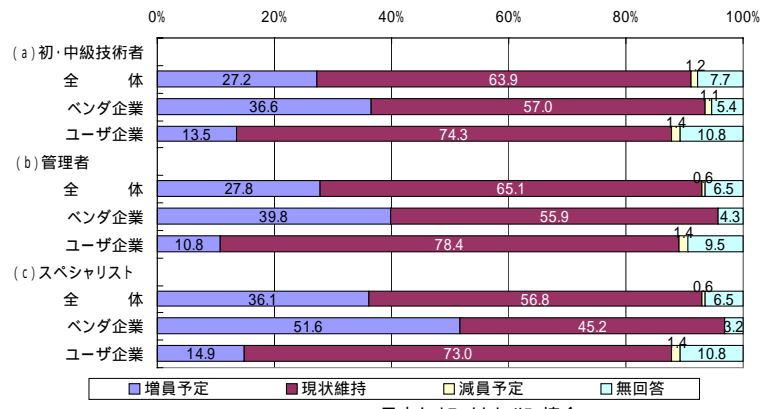
- ❖ ベンダ企業、ユーザ企業とも、全ての職種で、過半数が人材の不足感を感じている。
- ❖ 特に、情報セキュリティ専門の技術者として高度な知識とスキルを有する「スペシャリスト」へのニーズが高い。



Copyright (c) 2002 NPO日本ネットワークセキュリティ協会

情報セキュリティに携わる人材の増員、減員の予定 **JNSA**

- ❖ 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。
- ❖ 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Slerでは74.2%が増員予定。

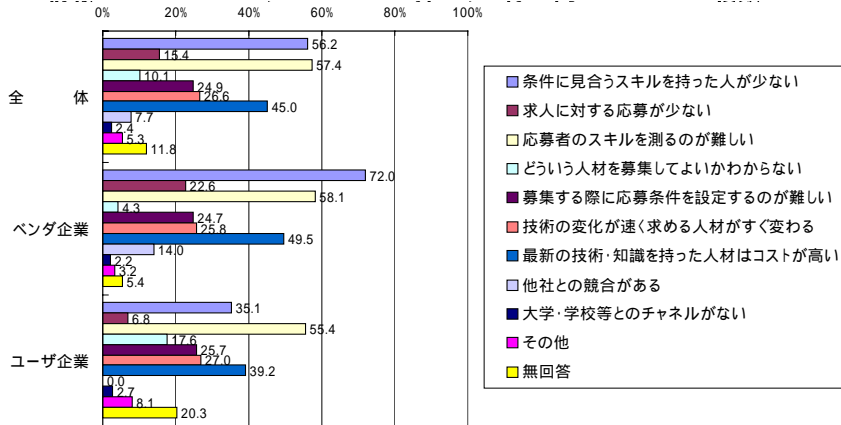


Copyright (c) 2002 NPO日本ネットワークセキュリティ協会

情報セキュリティに携わる人材を採用する際の問題点



- 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。



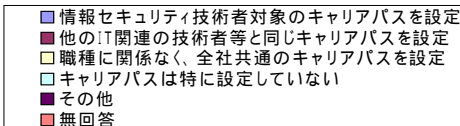
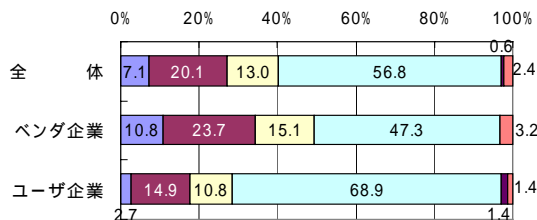
Copyright (c) 2002 NPO日本ネットワークセキュリティ協会

Page 11

情報セキュリティにたずさわる人材のキャリアパス



- キャリアパスを設定している企業は、ベンダ企業では49.6%、ユーザ企業では28.4%。
- しかし、情報セキュリティの専門技術者等を対象としたキャリアパスを設定しているのは少数(ベンダ企業 10.8% / ユーザ企業 2.7%)。
- キャリアパスを設定しない理由として、「そもそも対象となる従業員が少ない」、「スキルの測定や明示が困難」が多い



Page 12

矛盾したデータ

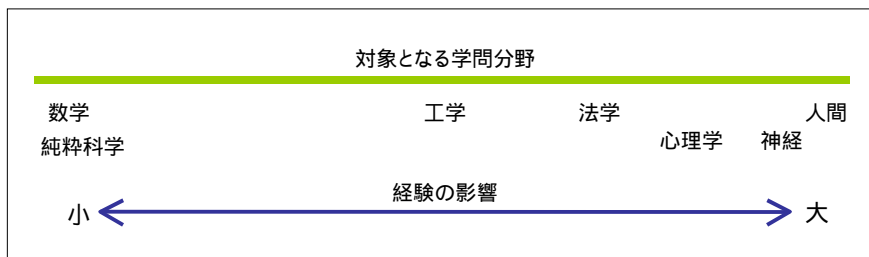
- ・ 情報セキュリティの専門技術者として高度な知識とスキルを有する「スペシャリスト」へのニーズが高い、(Page13 情報セキュリティに携わる人材の過不足感)
- ・ 一方で情報セキュリティ対策要員を積極的に増やそうとする企業は現時点ではそれほど多くはない (Page14 情報セキュリティに携わる人材の増員、減員の予定)
- ・ 情報セキュリティの専門家としての受け入れ態勢が整備されていない、(Page19 情報セキュリティに携わる人材のキャリアパス)

問題分析

- ・ 情報セキュリティは、その概念が捉えづらく且つその対象が非常に広範囲に及ぶため専門家(スペシャリスト)とは言っても何の専門家なのかよく分からない、
- ・ 従ってその人材像が明確にできず、採用時にどういう人材を採用して良いのか良く分からない、
- ・ 人材の採用、処遇を含めて極めて抽象的な概念である情報セキュリティを企業実務にどのように組み込んでいったらよいか良く分からない、

補足資料

情報セキュリティの学問的位置づけ

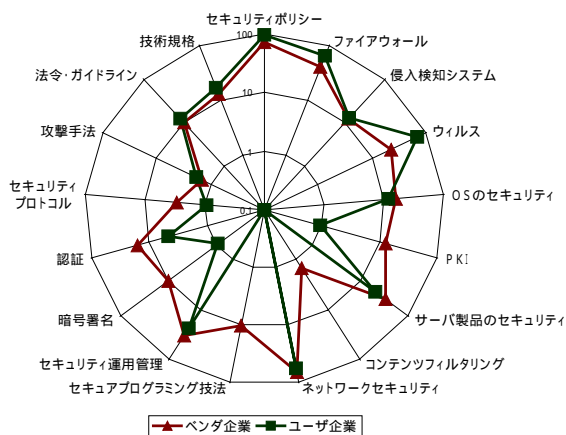


純粋科学としての数学に始まり、法学、経済学、経営学、心理学、神経から人間そのものの知識へと広がる (情報セキュリティ=総合科学)

2. 企業(ベンダ企業、ユーザ企業)において要求されるスキル

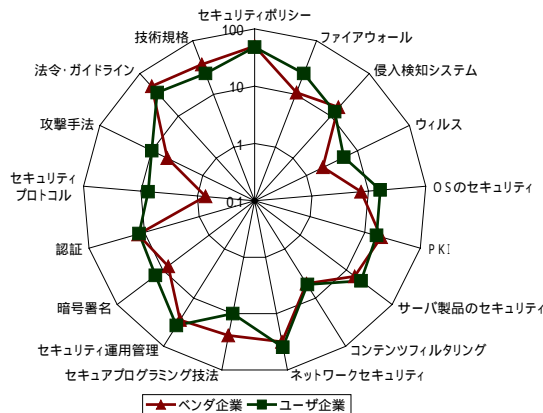
企業において重視されている知識項目

- ベンダ企業: 「1位:セキュリティポリシー」「2位:ネットワークセキュリティ」「3位:ファイアウォール」
- ユーザ企業: 「1位:セキュリティポリシー」「2位:ウイルス」「3位:ファイアウォール」



企業において不足していると認識されている JNSA 知識項目

- ベンダ企業：「1位:セキュリティポリシー」「2位:法令・ガイドライン」「3位:技術規格」
- ユーザ企業：「1位:セキュリティポリシー」「2位:ネットワークセキュリティ」「3位:セキュリティ運用管理」



Copyright (c) 2002 NPO日本ネットワークセキュリティ協会

Page 17

総括及び問題分析



| | 重視している知識 | 不足している知識 |
|-------|-------------------------------------------------|---------------------------------------------------|
| ベンダ企業 | 1位:セキュリティポリシー 2位:ネットワークセキュリティ 3位:ファイアウォール | 1位:セキュリティポリシー 2位:法令・ガイドライン 3位:技術規格 |
| ユーザ企業 | 1位:セキュリティポリシー 2位:ウィルス 3位:ファイアウォール | 1位:セキュリティポリシー 2位:ネットワークセキュリティ 3位:セキュリティ運用管理 |

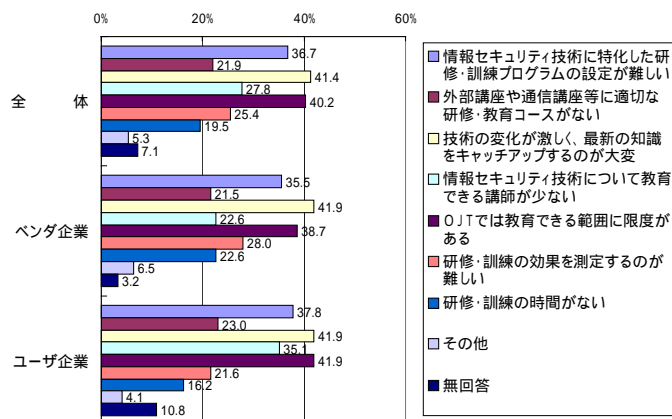
企業において要求されるスキル = セキュリティポリシー

総合科学としての情報セキュリティ分野を俯瞰・鳥瞰し、全体をコントロールする仕組み作り、マネジメントできる人材が要求されている。

3. 企業(ベンダ企業、ユーザ企業)における 情報セキュリティにたずさわる人材の教育

情報セキュリティにたずさわる人材の研修・訓練 における問題点

- ベンダ企業、ユーザ企業ともに、「技術の変化への対応の困難さ」、「OJTの限界」、「研修・訓練プログラムの設定の困難さ」が問題になっている。
- 特に、ユーザ企業では、「情報セキュリティ技術について教育できる講師が少ない」ことも問題として認識。



データ

- ・ 研修、訓練プログラム設定の困難さが指摘 (Page20 情報セキュリティに携わる人材の研修・訓練における問題点)

分析

- ・ 情報セキュリティ分野は、必要となる知識が広範囲に渡り且つ体系化されていない。
- ・ そもそも教えられる人材が少ない。
- ・ SE(技術者)と言っても構築系、開発系、コンサル系から始まり様々な職種が存在し各々の職種にあったプログラムを都度作成することは、教育サービス提供側にとって負担が大き過ぎる。教育事業者にとっては事業としての魅力にかける。
- ・ 従来型の知識植え込み型教育では、有能な人材を育成できない。教育手法の不備。

第二編

大学、専門学校等における教育の現状に関する調査 － 学識者ヒアリングのまとめ －

1. ヒアリングの実施経過
2. セキュリティ教育の現状
3. 今後のセキュリティ教育のあり方
4. 論点のまとめ

ヒアリングの実施経過



実施目的: 情報セキュリティ教育を提供する大学や専門学校等における情報セキュリティ教育の現状に関する知見を得る。

訪問先: 7件(大学6校+専門学校1校)。詳細は下表の通り。

訪問者: JNSA 教育部会SkillmapWGメンバー + 富士総合研究所

| | | |
|--------|------------|--------------------------|
| 11月25日 | 内田勝也 専任研究員 | 中央大学研究開発機構情報セキュリティ研究ユニット |
| 11月26日 | 佐々木 良一 教授 | 東京電機大学 工学部 情報メディア学科 |
| 11月27日 | 塚本 克治 教授 | 工学院大学 情報工学科 |
| 11月29日 | 植田 威 部長 | 学校法人岩崎学園 経営企画部 |
| 12月 2日 | 村岡 洋一 教授 | 早稲田大学 理工学部情報学科 |
| 12月 6日 | 森井 昌克 教授 | 徳島大学 工学部知能情報工学科 |
| 12月18日 | 山口 英 教授 | 奈良先端科学技術大学 図書館長 |

セキュリティ教育の現状



- 情報セキュリティにたずさわる人材を育成するための教育として、提供されているコースやカリキュラム等
 - 情報セキュリティの専門家(研究者、技術者)を育成するコースは、調査範囲内では存在しない。
 - 情報システム、ネットワーク、メディア等のコースの中で実施されている「情報セキュリティ教育」について分析。
- 情報セキュリティ教育の実績
 - 注目すべき実践例
 - 情報セキュリティ教育と就職の関連性
学生の専門が決まる前に内定が出るためほとんど無関係
- 情報セキュリティ教育の問題点

東京電機大学大学院:「ネットワークセキュリティ特論」

将来の企業の情報セキュリティ技術者または大学の情報セキュリティの研究者として必要な項目を提供。

早稲田大学:「ネットワークセキュリティ基礎」他

国内民間企業から専門技術者を招いて、トピックス的な内容を講義(NRAが協力)。アタックや防御の実習も実施。

工学院大学:通常講座内でセキュリティ教育を実施。

情報セキュリティの比率は15~20%程度。独自テキスト使用。

岩崎学園

国家資格やベンダの認定試験等の取得に対応した教育課程を提供。受講希望者は増加傾向。

徳島大学:社会人向け短期集中講義の実施

企業からの依頼をもとに、情報セキュリティに関する短期集中講義を実施。(2~3日、30時間程度)

自治体向けに、情報セキュリティに関するサーベイ、必要性について講演。(1日4時間×2日程度)

奈良先端科学技術大学院大学:遠隔講義

「インターネットのセキュリティ対策」:WIDEプロジェクトにおけるsoi (school of internet)講座。3キャンパスから受講可。

中央大学大学院:COEプログラムによる講座

「電子社会の信頼性向上と情報セキュリティ」の拠点。03年度開講。講義内容は、「技術者・管理者向け情報セキュリティ教育試案」がベース。

教育できる人材の不足

- 現在の情報セキュリティ研究者は、暗号技術、インターネット技術、ネットワークシステムの専門家がいずれかではなく、トータルな安全性評価ができない。
- 地方では人材確保難より、教育できない問題がより深刻。

歴史の浅さ・重要性の認識不足

- IT技術者教育のための学科の創設に時間がかかる。
- ソフト・ハードの開発者がセキュリティホールやバグのない製品を開発できるようになることが先決。
- 大企業は自前でセキュリティの専門技術者を育成すべき。
- セキュリティマインドを身に付ける教育が必要。

技術革新の速さ・陳腐化

- 日本の情報分野の教育や資格に更新教育がないのが問題。
- 察早い技術革新に対応するためには、大学で普遍的な内容を養い、最新技術は企業内教育に委ねるべき。
- 攻撃側に対抗すべくSEA/Jのような活動をもっと行うべき。

27

関連分野の広さ

- セキュリティを教えるには情報システムやネットワークの基礎知識が不可欠だが、時間が限られ教えられない。
- 日本の教材はボリュームが足りない。
- 情報セキュリティ分野を横断的に考えられる人が少ない。
- 今の教育はオペレータ教育がほとんど。

その他

- 企業側ニーズとしての情報セキュリティ技術者像が見えてこない。
- 基礎知識が身に付いていない学生など、企業が必要とする人材と大学が供給する人材にミスマッチがある。
- 運用管理や対策などの実地体験が重要だが、大学の講義では限界。
- セキュリティ対策より、開発者がバグのない頑強な製品を作れるようになることが先決。
- 地方では、情報セキュリティ技術者の前にネットワーク技術者自体が不足している。

情報セキュリティ教育の要件

- 研究者・技術者向け教育
 - ・ セキュリティ教育のみを取り出して何かやる、ということは専門家向けとしてはありえない。情報セキュリティ単独でなく、IT技術者としてのセキュリティ分野の知識が問われる。
 - ・ 各分野の専門技術者を民間から呼んで講義してもらうべき。
 - ・ セキュアなシステムを開発できる技術者の育成が先決。
- ユーザ側管理者教育
 - ・ 外部の専門家集団によってサポートされる仕組みが必要。
- 一般利用者向け教育
 - ・ 初中等教育における、倫理を含む教育の早急な充実。
 - ・ セキュリティを意識しないで済む方向への制度等の設計。

大学・専門学校の役割

- 基礎を知っていて応用が利く人材、自分で学ぶことができる人材が求められている。
- 考え方を身に付けさせる教育の提供。
- 大学は教育で得られるキャリアパスを提示すべき。
- 大学と専門企業がジョイント講座を設置し、社会人と大学院生が一緒に受講。
- 社会人教育は大きなターゲット。
- 研究室と個別の企業レベルが連携する仕組み。
- OJT、eラーニング、集合講座の組合せ。

他の機関の役割

- JNSAのような専門家集団の企業を超えた連携。
- 個人利用者を対象としたボランティア組織とその活動の支援。
- コンピュータ第一世代の定年退職者活用。
- 産学連携で相互にメリットがある仕組み。
- 地方においては行政の主導が重要。

情報セキュリティスキルの考え方

- 何を学ぶべきか自分で考える能力。
- 実際に手を動かして初めて習得できる部分も大きい。
- 法務、人事、総務に働きかけていける能力。
- リスクをアセスメントする能力。

資格制度・更新制度

- 国家資格は基本的な知識を、ベンダ資格は頻繁な更新が必要なもの、などの使い分けを。
- 国際水準を保ち、東アジアでの統一フレームになるような相互認証された制度を。
- 情報セキュリティ事業を行う際は有資格者を必須とするなどの制度化が必要(電気主任技術者などのように)。
- 技術者の評価、資格制度と教育は一体で。
- 更新は必須。2～3年程度。

その他

- 情報セキュリティは総合科学として、技術以外の分野も取り込むべき。
- 教育で対応できる部分はロングタームにならざるを得ない。
- セキュリティ全般を教えたらジェネラリスト。そのような人材は多くは必要ない。
- eラーニングの効果は大きく、実習と併用することも可能であるが、学習者に意欲がある場合のみ効果がある。
- 大学がeラーニングをやると民業圧迫の指弾の恐れ。
- 法制度化の際は、ネットワーク上の自由を過度に縛ることがないように留意。

対立した議論

- ・ 情報セキュリティ分野は総合科学。よって暗号やアクセスコントロール技術等個別分野に特化した教育では不十分。総合的教育によって専門家を育成すべき。
- ・ 職種として「セキュリティエンジニア」は存在し得ない。スペシャリストとしては「セキュリティが分かる 専門家」というキャリアパスが自然。

問題分析

- ・ 情報セキュリティ専門家に対する企業側のニーズは強い。
- ・ 教育機関側で専門家を育成したとしても、企業側がそれら人材を受け入れない、適切に処遇できない状況。
- ・ 現在の教育はオペレータ教育にかたより過ぎ、開発者教育をより重視すべき。
- ・ 育成の議論よりも、組織の情報セキュリティ管理はどうあるべきか、社会全体として情報セキュリティに対する品質管理をどのように行っていくのか、大学×企業×NPO等で議論を優先すべき。

第三編

「情報セキュリティに関するスキルマップ」 開発の経緯及びその概要

- ・Security Engineerの技術レベルを適切に評価する
基準・尺度が存在しない
- ・情報Security分野の知識が体系化されていない

企業側が人材を採用する際にミスマッチが多発

専門家層が結局何の専門家なのかよく分からない

Project等で構成員の技術レベルが適切に評価できないため役割分担が難しい、国際的Projectは更に深刻

学生や若年層SEがキャリアプランや学習目標を立てづらい

教育サービス提供側がニーズにあったカリキュラムを提供しにくい

Skillmapの実装機能

技術者のスキルレベルを適切に評価できる

- ・ 人材採用時のミスマッチ防止に
- ・ 専門家の定義、その専門性の具体化を
- ・ 案件毎の役割分担を容易にまた企業をまたがるアライアンスや国際的協業の推進を
- ・ 大学や企業の人材育成政策や人材評価の共通基盤として

知識体系 (Security分野) の整理・分類

- ・ 学生や若手技術者のキャリアプランや学習目標設定時の参考資料として
- ・ 他分野を専攻する技術者がSecurity分野の基礎知識を習得しやすいように (全体的なスキルレベルの底上げ)

既存のSkillmap研究 1



英国 : Skills Framework for the Information Age (SFIA)

米国 : National Workforce Center for Emerging Technology (NWCET)

日本 : ITスキルスタンダード(ITSS)

経済産業省 現在策定中

情報処理技術者スキル標準

JITEC (情報処理技術者試験センター)

既存のSkillmap研究 2



モデル: 経済産業省 ITスキルスタンダード

レベル

縦割型職種業務区分
理想的モデルの一つ

| 職種 (キャリア) | 業務 (ジョブカテゴリ) | レベル | | | | | | |
|-----------------|-------------------------------------|-----|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| コンサルタント | IT(Business Transformation) | | | | | | | |
| ITアーキテクト | IT | | | | | | | |
| | ITパッケージ適用 | | | | | | | |
| | ITアプリケーション | | | | | | | |
| プロジェクトマネジメント | データベースネットワーク | | | | | | | |
| | ネットワーク | | | | | | | |
| | セキュリティ | | | | | | | |
| | システムマネジメント | | | | | | | |
| ITスペシャリスト | システム開発 / アプリケーション開発 / システムインテグレーション | | | | | | | |
| | クラウドソリューション | | | | | | | |
| | ネットワークサービス | | | | | | | |
| | ビジネスソリューション | | | | | | | |
| アプリケーションスペシャリスト | クラウドネイティブ開発 | | | | | | | |
| | クラウドフォーム | | | | | | | |
| | クラウドプラットフォーム | | | | | | | |
| | システム管理 | | | | | | | |
| ソフトウェア開発 | データベース | | | | | | | |
| | ネットワーク | | | | | | | |
| | 分散コンピューティング | | | | | | | |
| | セキュリティ | | | | | | | |
| マーケティング | 業務システム | | | | | | | |
| | 業務パッケージ | | | | | | | |
| 販売 | クラウドプラットフォームマーケティング | | | | | | | |
| | 訪問販売コンサルティングセールス | | | | | | | |
| カスタマーサービス | 訪問販売高付セールス | | | | | | | |
| | メディア制作高付セールス | | | | | | | |
| 運用 | システムインテグレーション | | | | | | | |
| | ネットワークオペレーション | | | | | | | |
| 教育 | カスタマーサポート | | | | | | | |
| | 研修企画 | | | | | | | |
| | インストラクション | | | | | | | |

既存のSkillmap研究 3

| レベル | 年収の目安 | 経験年数の目安 |
|------|-------------|---------|
| レベル1 | 300～400万円程度 | 2～3年程度 |
| レベル2 | 400～500万円程度 | 4～5年程度 |
| レベル3 | 500～600万円程度 | 7～8年程度 |
| レベル4 | 700～800万円程度 | 10年程度 |
| レベル5 | 1,000万円程度 | 15年程度 |
| レベル6 | 1,200万円程度 | 20年程度 |
| レベル7 | 1,500万円程度 | 25年程度 |

レベル=キャリアパス

| タスク | Ability | Knowledge |
|-----------------|---------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| ジョブカテゴリ: セキュリティ | レベル7 | ・セキュリティ要件の把握 ・セキュリティ機能、プロトコル、運用の定義 ・セキュリティデザイン ・耐監査性設計 ・機密性設計 ・完全性設計 ・識別と認証設計 ・PKI ・暗号化技術の適用 ・ネットワークセキュリティ技術の適用 ・その他 |
| セキュリティデザイン | レベル6 | |
| | レベル5 | |
| | レベル4 | |

モデル: 経済産業省 ITスキルスタンダード

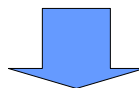
詳細は資料参照

Copyright (c) 2002 NPO日本ネットワークセキュリティ協会

Page 39

研究結果

- ・ Skillmapというよりスキルスタンダード(技能標準)・標準キャリアパス的要素が強い
- ・ 職種(業務)区分やLevelの設定は組織運営及び技術者能力の理想系モデル(こうあるべき)の一つ



- ・ JNSAでは既存Skillmap(主にITSS)の補完的位置付けとして実務性・利便性を重視したMap作成を行う(技術的知識・スキルの参照項として。理想系の追求は行わない)

Copyright (c) 2002 NPO日本ネットワークセキュリティ協会

Page 40

Skillmap(JNSA案)の基本コンセプト



ユニークな組織・ユニークな業務オーダーにも対応可能なようユーザ参加型のSkillmap作成を目標とする

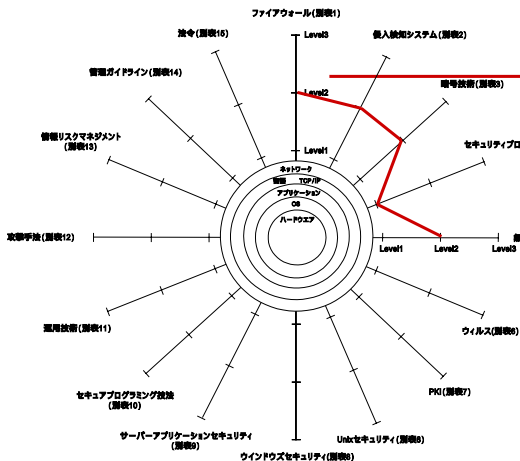
- ・Targetの設定について
 エンドユーザ及びベンダー(開発企業・インテグレータ)のセキュリティ関連技術者層 (これ以上Skillmapの中で職種/業務区分は設定せず利用者に委ねる・縦割職種区分は行わない)
- ・職種や業務区分、スキルレベル等は利用者が各自で設定できるように、より柔軟で汎用性を重視する

Skillmap(JNSA案)イメージ



レーダーチャート案

利用者が目的に応じ自由にこのフォーマットを活用する
ユーザ参加型Skillmap



利用者側で記載
人材採用時の職種・Skill Level
人事評価時のLevelや目標設定の定義等

- ・Level 1
 知識がある(質問に答えられる)
- ・Level 2
 知識を使える(設計や仕様に従ってドキュメント化できる)
- ・Level 3
 抽象化できる(職務設計や実施職務のドキュメント化ができる)

Skillmap別表のイメージ(案) 1



各分野の詳細項目

別表1 Firewall

| タスク | 知識(Knowledge) |
|-----------|-------------------------------------------------------------------------------------|
| ファイアーウォール | ポリシー設計 |
| | 構成の設計 (DMZ) |
| | サービスの設計 |
| | ファイアーウォール自体の脆弱性の理解 |
| | ログ解析と危険な箇所の理解 |
| | ユーザ認証技術 (パスワード・認証トークン) |
| | ロギング |
| | 暗号化通信 (VPN) |
| | NAT (Static NAT / Dynamic NAT / IPマスカレード) |
| | コンテンツフィルタリング |
| | ロードバランシング |
| | HA多重化機能 |
| | 侵入検知システムとの連携 |
| | リモート制御 |
| | ファイアーウォールのルーティング |
| 基礎知識 | アクセスコントロール技術 (Packet Filtering / Circuit Level Gateway / Application Level Gateway) |
| | ファイアーウォールの基礎的役割の理解 |

職種毎で異なる知識

あらゆる職種の共通知識

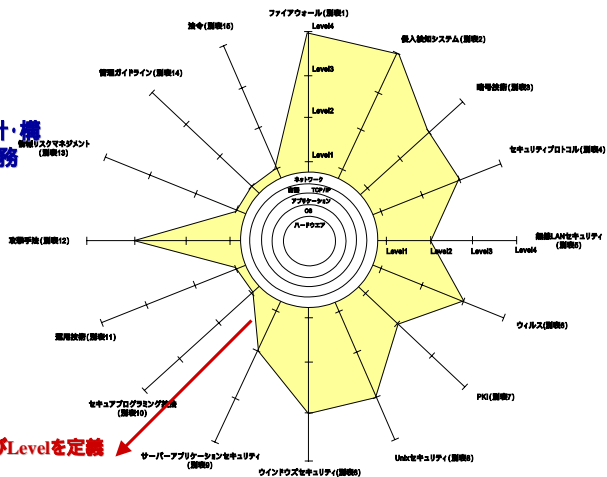
Skillmap(JNSA案)の運用例 1



東京在住のシステムインテグレータH社がファイアーウォールやIDSなどセキュリティ機器の構築・運用ができる技術者を募集した場合

求人広告

- 1) 職種: セキュリティエンジニア
- 2) 業務: セキュリティプロダクトの設計・構築・運用等のインテグレーション業務
- 3) 応募資格:
 - 技術レベル - Skillmap参照
 - 学歴: 大学卒以上
 - 希望年齢: 25歳 ~ 35歳程度望む
 - 性別: 不同
 - 勤務地: 東京杉並区
 - 勤務時間帯: 平日9:00 ~ 17:00
- 4)

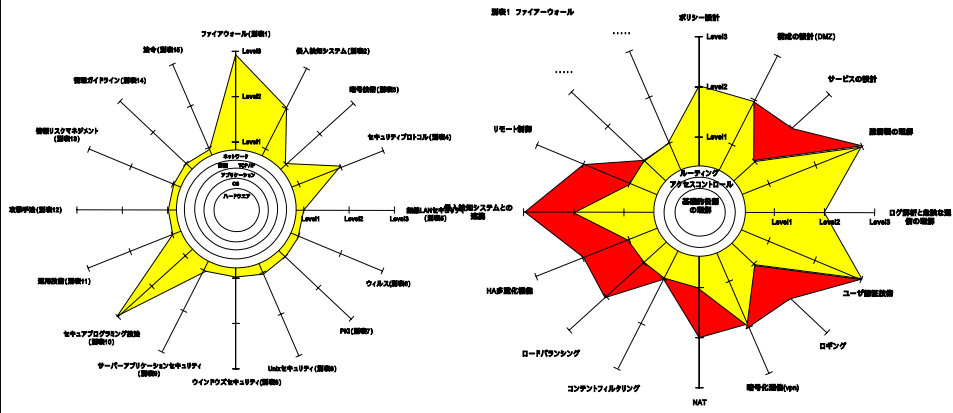


H社が採用したい技術者の職種とSkill及びLevelを定義
応募者側もH社の業務が理解しやすい

Skillmap(JNSA案)の運用例 2



自社でFirewall製品を開発している国内大手電機メーカーF社。課長のSさんは部下のM君に次のプロジェクトでIDSとの連携機能の組み込みを行って欲しいと考えている。評価をかねてM君の現在のスキルを細かく定義し、来年度以降の仕事に必要なスキルを表現した。夏までには不足している部分の知識を身につけて欲しいと考えている。



Skillmap(JNSA案)の運用例 3



LGWAN・住基ネットの本格運用が開始された。県庁。危機管理の徹底が叫ばれるなか確固としたセキュリティポリシを構築することを決めたが庁内にノウハウがないため地場SIerに一部アウトソースすることにした。コンサル契約を想定しているが入札仕様書にコンサルタントの能力を定義する際 Skillmapを活用した。将来的には同様の能力を自らが持つべく学習目標にもしようと思っている。

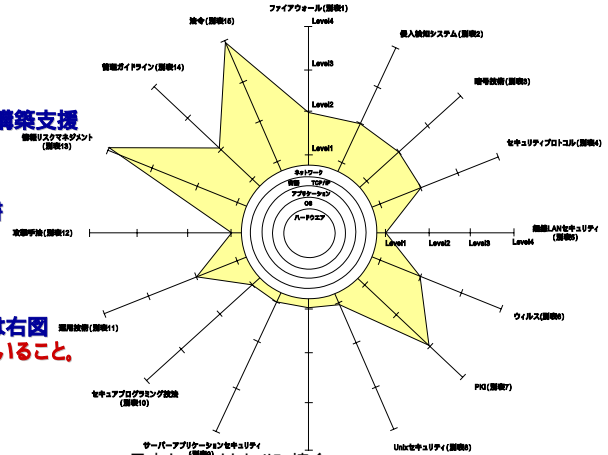
入札説明書

1. 契約担当官・・・
2. 契約件名等:セキュリティポリシ構築支援
3. 競争の方法:指名競争入札
4. 参加資格:・・・役務の提供A・・・

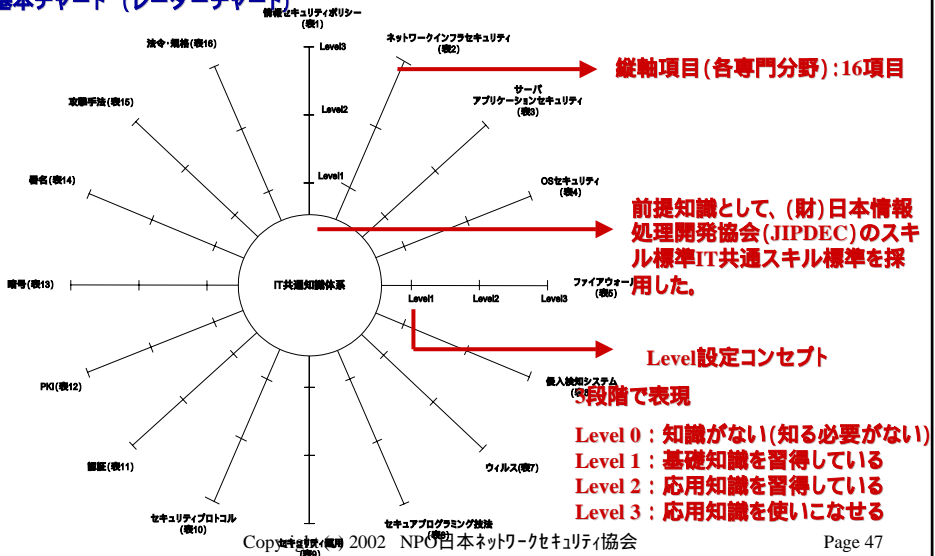
セキュリティポリシ構築支援仕様書

1. 適用範囲・・・
2. 支援依頼内容・・・
3. その他

上記業務を実施する技術担当者は右図 Skillmapの知識レベルを満足していること。



基本チャート (レーダーチャート)



基本チャート項目(別表1)

| フェーズ | 知識項目 | 備考(補足説明) | | |
|---------|-------------|-----------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------|--|
| ライフサイクル | 1.要件定義・概要設計 | 1.情報セキュリティポリシー 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 4.OSセキュリティ 5.ファイアウォール 6.侵入検知システム 7.ウイルス | 人的/物理的対策 Web/Mail/DNS/ディレクトリ Unix/Windows/TrustedOS | |
| | 2.詳細設計・構築 | 8.セキュアプログラミング技法 | | |
| | 3.開発・実装 | 9.セキュリティ運用 | ログ管理/解析/パッチ管理 | |
| | 4.運用・監査 | 10.セキュリティプロトコル | | |
| | ライフサイクル外 | 5.基礎技術 | 11.認証 12.PKI 13.暗号 14.署名 | |
| | | 6.関連知識 | 15.攻撃手法 | |
| | | | 16.法令・規格 | |

各専門領域(別表5)

| 大分類 | 知識区分 | 小分類 |
|----------|-------------------|------------------------------------------------------------------------------------------|
| ファイアウォール | 応用知識 (Level.2) | ネットワークポリシー設計 |
| | | DMZ等構成の設計 |
| | | ファイアウォール自体の脆弱性 |
| | | ロギング、ログ解析と危険な通信 |
| | | NAT (StaticNAT / DynamicNAT / IPマスカレード) |
| | | ロードバランシング |
| | | HA多重化機能 |
| | | 侵入検知システムとの連携 |
| | 基礎知識 (Level.1) | ファイアウォールのルーティング |
| | | アクセスコントロール技術 (PacketFiltering / Circuit Level Gateway / Application Level Gateway) |
| | | ファイアウォールの基礎的役割 |
| | | |
| | | |

Skillmap最新版のダウンロード

平成15年4月15日、当協会により作成された調査報告書及びSkillmapの最新版が経済産業省及び情報処理振興事業協会(IPA)のホームページにて掲載された。

経済産業省

<http://www.meti.go.jp/kohosys/press/0003929>

情報処理振興事業協会(IPA)

http://www.ipa.go.jp/security/fy14/reports/professional/ikusei_seika_press.html

