3D-05

情報セキュリティ人材育成におけるセキュリティ知識項目（SecBoK）の有効活用

平山敏弘†

日本アイ・ビー・エム株式会社†‡

1. はじめに

平成 26 年の独立行政法人情報処理推進機構（以下 IPA）の試算によれば，国内企業において，情報セキュリティ人材は約 8 万人と大幅に不足しており，さらに情報セキュリティに従事している技術者のうち，約 16 万人がスキル不足との調査結果が出るなど，情報セキュリティ人材の育成は急務である．現在不足している人材の多くは，ユーザー企業において，自社システムのセキュリティ確保を管理できる人材であり，このような人材はセキュリティ専門家とは限らない．本論文では，セキュリティスキルを持った IT 技術者を育成することが難しいユーザー企業側においても有効活用可能である，セキュリティの知識項目を整理した SecBoK を取り入れた人材育成方法を提言するものである．

2. セキュリティ知識項目（SecBoK）の作成経緯

知識体系（ Body of Knowledge：BoK）は，関連する職能団体によって定義される専門領域を構成する概念や知識体系があり，プロジェクト管理熟達のために使用されているプロジェクト管理知識体系（PMBoK）やビジネス分析専門家のための事業分析知識体系（BABoK)などが有名である．その中で情報セキュリティの知識項目として SecBoK も，以下の経緯を経ながら約 10 年前に作成されてセキュリティベンダーを中心に使用されている．

1)IPA からの依頼で，2004 年/2005 年（修正版）と情報セキュリティスキルマップを NPO 日本ネットワークセキュリティ協会(以下 JNSA)が作成
2)2007 年に経済産業省受託事業のアウトプットとして「情報セキュリティ教育の指導者向け手引書（2007 年版）」公開したが，その手引書内にある情報セキュリティ知識項目を SecBoK として名称変更し発表した。SecBoK は，図 1 にある通り 15 の情報セキュリティ知識項目の大分類があり，さらに中分類以下に約 600 の小分類スキル項目から構成されている．

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
		セキュアOS
5	ファイアーウォール	
6	侵入検知	
7	ウイルス	
8	セキュアプログラミング技法	
9	セキュリティ運用	
10	コンテンツセキュリティ	
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	

図 1　SecBoK スキルマップ大分類

3) 2009 年には，情報セキュリティ教育事業者連絡会(ISEPA) より，「情報セキュリティ人財アーキテクチャガイドブック」が公開．

ガイドブックの中では情報セキュリティの職種が 32 職種に分かれており，それぞれの職種で必要なスキルが定義されている．

3. 「iCD2015」へ SecBok の取り込み

国際的な競争が高まる中，近年では新たな IT サービスや IT インフラが台頭し，企業を取り巻くビジネス環境は刻一刻と変化してきている．そのような状況の中 IPA では，これらの環境変化に対応した IT 人材を育成可能とするため，「i コンピテンシ ディクショナリ」（以下，iCD）を発表している．企業において IT を利活用するビジネスに求められる業務（タスク）と，それを支える IT 人材の能力や素養（スキル）を「タスクディクショナリ」，「スキルディクショナリ」として体系化したもので，企業は経営戦略などの目的に応じた人材育成に利用することが可能である．最新版は iCD2015 が公開されており，前バージョンに加え，重点項目の１つである情報セキュリティに関しては，SecBoK 内の知識項目を新たに取り入れ対応している．

現バージョンの SecBoK は，2004 年に作成し，その後アップデートを重ねて 2009 年時点の内容が公開中であるが，その後のアップデートが行われていない．そこで現在本当に必要とされて

Effective practical use of the security knowledge item (Security Body of Knowledge) in information security personnel development.
†Toshihiro Hirayama , IBM Japan Ltd

いる情報セキュリティ人材育成に対応できるアップデートが必要と考え，JNSA において「情報セキュリティ知識項目（SecBoK）改訂委員会」を設置し，JNSA 外の有識者を含む検討委員によって改訂作業を平成 27 年 12 月現在実施中であり，平成 27 年度末までには改訂作業を終了し，公開する予定である．

4. ユーザー企業における人材育成の対応

冒頭に述べた通り，国内企業において，情報セキュリティ人材は約 8 万人不足していると報告されている通り，情報セキュリティ人材の不足は大変深厚な状況である．どの様な人材が不足しているかについては，様々な意見があるが，図２にある通りユーザー側社内においてのセキュリティ要員およびスキルの不足は明確である．

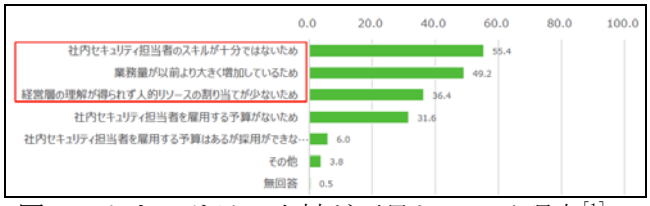

図２　セキュリティ人材が不足している理由[1]

そこで SecBoK 改訂委員会では，ユーザー企業も多く会員になっている日本シーサート協議会（以下 NCA）での平時と有事の必要タスクを参考に役割やロールを洗い出した．（図３）

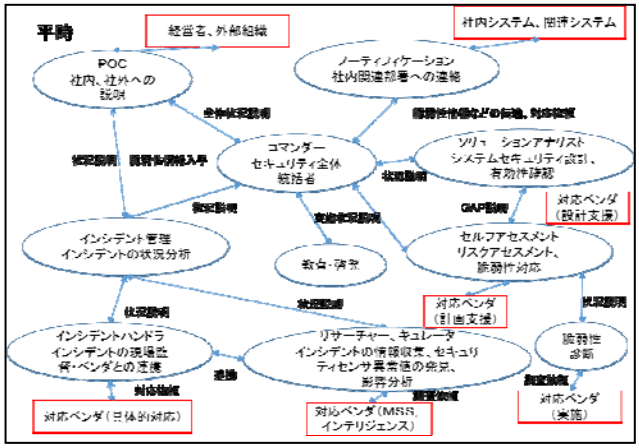

図３NCA におけるセキュリティ人材タスク整理図

考慮すべき事項としては，各ロールはインシデントの同時多発が想定される大企業向けであり，必要に応じて兼務可能なことを明示する点や，ユーザ企業とセキュリティベンダの役割分担も一律ではないため，双方の可能性を踏まえてまとめている．改訂された SecBoK は，グローバルスタンダードに対応できることも目標としているため，米国での National Initiative for Cybersecurity Education（以下 NICE）フレームワークも参照している．NICE は米国で NIST（National Institute of Standards and Technology）で策定されたフレームワークであり，各省庁での情報セキュリティ人材育成計画の策定に利用されている．

5. スキルマップの利用イメージ

図４は，インシデント管理・インシデントハンドラー・キュレーターに関するスキルマップ案である．このようなスキルマップを作成することにより，セキュリティ教育コンテンツ作成時のリファレンス利用や，情報処理技術者試験をはじめとする各種試験で必要とするスキル項目が明確になるものである．

分野	大項目	小項目
基礎	ICT基礎	ネットワーク通信を提供するために、ネットワークサービスとプロトコルがどのように作用するかに関する知識
		ネットワークプロトコル（例：TCP/IP、DHCP）およびディレクトリサービス（例：DNS）に関する知識
		データバックアップ、バックアップの種類（フル、インクリメンタル）及び復元コンセプトとツールに関する知識
	ビジネス基礎	損失評価の実施に関するスキル
セキュリティマネジメント	総論	計算機ネットワーク防御のポリシー、手続きおよび規制に関する知識
ネットワークセキュリティ	総論	ネットワーク通信のセキュア化に関するスキル
		何がネットワーク攻撃及び脅威と脆弱性の双方への関係を構成するかに関する知識
		トポロジー、プロトコル、構成要素及び原理を含むネットワークセキュリティアーキテクチャのコンセプト（例：真相防御のアプリケーション）に関する知識
	トラフィック解析	ネットワークトラフィック解析手法に関する知識
		パケットレベル解析に関する知識
	侵入検知	侵入検知技術を通じたホスト及びネットワークベースの侵入を検知するための侵入検知手法と技術に関する知識
システムセキュリティ	総論	システムとアプリケーションのセキュリティ上の脅威と脆弱性（例：バッファオーバフロー、モバイルコード、クロスサイトスクリプティング、PL/SQL及びインジェクション、競合状態、秘密の通信路、リプレイ、リターン指向攻撃、悪意のコード）に関する知識
セキュアシステム設計・構築	総論	基本的なシステム管理、ネットワーク及びOSのハードニングに関する知識
セキュリティ運用	インシデント対応	インシデントのカテゴリ、インシデントレスポンス及び応答のタイムラインに関する知識
		インシデントレスポンスとハンドリングの方法論に関する知識
	その他	セキュリティイベントの相関ツールに関する知識
サイバー攻撃手法	総論	一般的な攻撃ステージ（例：フットプリンティング及びスキャン、列挙、アクセス権取得、特権の昇格、アクセス権の保持、ネットワークのエクスプロイト、追跡回避）に関する知識
		脆弱性の種類と関連する攻撃の認知とカテゴライズに関するスキル
	マルウェア	マルウェアの取扱いに関するスキル
		マルウェアからのネットワークの保護に関するスキル
		マルウェア解析のコンセプトと手法に関する知識
	その他	攻撃クラスの相違（例：受動的、能動的、内部、近接、分散）に関する知識
		運用上の脅威環境の違い（例：第一世代（スクリプトキディ）、第二世代（非政府機関による支援）、第三世代（政府機関による支援）に関する知識
デジタルフォレンジック	総論	標準の運用手続きまたは国内標準に関する証拠の完全性の維持に関するスキル

図４　スキルマップ案

5. おわりに

2016 年の伊勢志摩サミット，2019 年ラグビーワールドカップに本大会，2020 年東京オリンピック・パラリンピック競技大会とイベントが目白押しである日本において，サイバーセキュリティの脅威も格段に増加することが予想される．そのような状況の中，セキュリティ対応できる技術者の育成は急にであるが困難な点も数多い．当論文が現在日本か抱えている情報セキュリティ技術者育成の一助になれば幸いである．

参考文献

[1] 情報セキュリティ・ 材の必要性と求められるスキル・養成方法　https://gartner-em.jp/srm2015/report/pdf/JSI15_NRI_Webreport_DL.pdf