連載企画

行政における情報セキュリティ対策と人材育成及び活用②

情報セキュリティ人材 ―必要な知識と育成・評価について―

(ISC)² Japan
代表　衣川　俊章（CISSP）

前回は、行政機関における情報セキュリティの必要性、その中に占める「人」の役割とその重要性について、米国での取り組みなども交えて説明しました。今回は、人材に必要とされる情報セキュリティに関する知識についてご紹介すると共に、人材の育成・評価の考え方、活用方法などについてお話をしたいと思います。

1. 情報セキュリティ人材の対象者

最初に明確にしておきたいのは、今回の連載における「情報セキュリティ人材」とは、行政機関の職員で、情報セキュリティを専門の業務としている方、又は他業務との兼務で担当している方々はもちろんですが、行政機関から業務委託を受けて、また指定の出入り業者として情報セキュリティ業務を担当している方々を含んでいるということです。

通常、行政機関の職員の方々は、2、3年毎のジョブローテーションが実施される中で、多くの場合は外部の人材に、自組織の情報セキュリティを任せる状況が多いと思われます。なので、情報セキュリティ人材には、行政機関の職員の方々だけではなく、こういった外部の方々にも当てはまるということになります。

実際に情報セキュリティ業務担当者の担当する業務は、非常に広範囲に渡っています。大きく分けると「マネジメント」と「技術」ということになるかと

図表1　情報セキュリティに係る人材に求められる知識

管理系分野	技術系分野	
マネジメント技術	セキュリティアーキテクチャ	侵入検知
リスク分析技術	NWインフラセキュリティ	ウイルス
情報セキュリティポリシー	セキュアプログラミング	不正アクセス手法
情報セキュリティ監査	セキュリティプロトコル	アプリケーションセキュリティ
法令・規格	認証	Webセキュリティ
事業継続経営（BCP・BCM）	アクセス制御	電子メールセキュリティ
教育訓練	PKI	DNSセキュリティ
物理セキュリティ	暗号	OSセキュリティ
プロジェクトマネジメント	電子署名	―
セキュリティ運用	ファイアウォール	―

「人材育成・資格制度体系化専門委員会報告書」より抜粋～内閣官房情報セキュリティセンター（NISC）　http://www.nisc.go.jp/

思います。「マネジメント」面においては、組織全体のセキュリティ対策デザイン・組織上層部の承認、組織のセキュリティポリシー・ガイドライン策定、BCP（事業継続計画）策定支援、策定された種々のポリシーなどの管理・運用、コンプライアンスやガバナンスへの対応、インシデント対応などが含まれます。「技術」面では、組織で導入するセキュリティ対策の技術側面からの評価、対策導入実施又は支援、その運用・管理、インシデント発生時のフォレンジックを始めとした技術対応などが挙げられます。

2. 人材に必要と思われる知識とは？

担当する業務や職責によって、必要とされる知識には差があるといいましたが、最低限全員が知っていないといけない知識群というのもあります。業務内容が「マネジメント」か「技術」を中心としたものであるかどうかで若干の差はありますが、ベースとなるものは共通ではないでしょうか。これらの知識群は、様々なところで過去にまとめられていますが、例として内閣官房セキュリティセンターの「人材育成資格制度化委員会報告書」（**図表1参照**）や、日本ネットワークセキュリティ協会で作成した「情報セキュリティ推奨教育の検討に関する調査報告書」内のスキル項目（**図表2参照**）などがあるかと思います。これらの項目全部をマネジメント、技術それぞれの職種に就いている人材が知っておく必要があるかについては、知っておく知識の浅深はあるにせよ、必要ではないかと考えます。各知識項目の詳細については、次回以降で説明したいと思います。

図表2　スキル項目リスト―大項目レベル

項番	分野	
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 NameSystem）
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	不正プログラム	
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	攻撃手法	
16	コンプライアンス？	
17	セキュリティプロトコル	
18	事業継続・災害復旧計画	
19	情報セキュリティ監査	
20	フォレンジック	
21	物理セキュリティ	

日本ネットワークセキュリティ協会（JNSA）：
情報セキュリティ推奨教育の検討に関する調査報告書

これらの知識に加えて、実際に行政機関で情報セキュリティ業務に従事しようと思うと、前述の基礎知識だけではなく、行政機関に特化した情報セキュリティ要件の知識も持ち合わせていないといけないと考えます。例えば、日本国の情報セキュリティ制度や政策について、GPKIや電子政府などの技術要素や、法律などについての知識を保有していることで、非常に幅広い視点から見据えた適切な情報セキュリティレベルを保つことができるようになります。私ども（ISC）[2]ではこれら行政機関に特化した情報

セキュリティ要件を4ドメインという形でまとめています。(**図表3参照**)

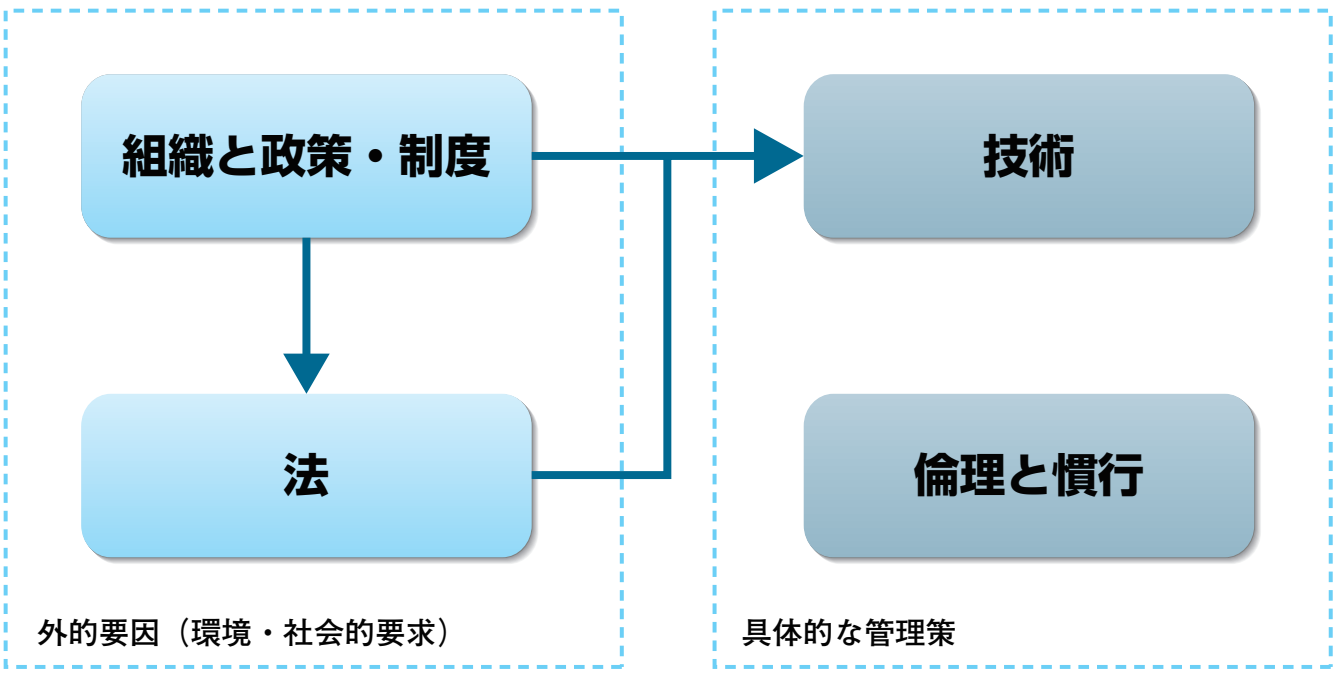
知識の習得という観点で大切なのは、ベースになる知識を持つことで、業務遂行をしていく上での基本スタンスを持てることです。何が適切なセキュリティ対策なのかを様々な観点から判断することができるようになることが、引いては組織の情報資産保護を最適なものに出来ると言えます。また、行政機関の職員の立場からすると、この知識を保有することで業務委託先の選択時の基準が出来るということにもなります。業務委託を受ける側にとっても、行政機関の必要としている状況の背景などまでも含めての提案や議論が出来ることで、結果的に提供できる内容の向上を図ることが出来るようになると言えます。

3. 人材育成及び活用・評価のポイント

ここからは、必要とされる人材の育成、またはそれら人材の活用・評価方法についてのポイントを説明したいと思います。

まず、人材育成という観点です。育成を考えるに当たり、最初にしないといけないのは組織において必要とされる人材像を明確にすることです。人材像を明確にするには、組織モデルと呼ばれているものを作成する必要があります。この組織モデルというのは、自組織において必要な情報セキュリティ業務というものを特定し、それらの業務を実施する人材を、基本的には職種という形で当てはめていくこと

図表3　(ISC)²日本行政情報セキュリティプロフェッショナル資格CBK(共通知識分野)4ドメイン

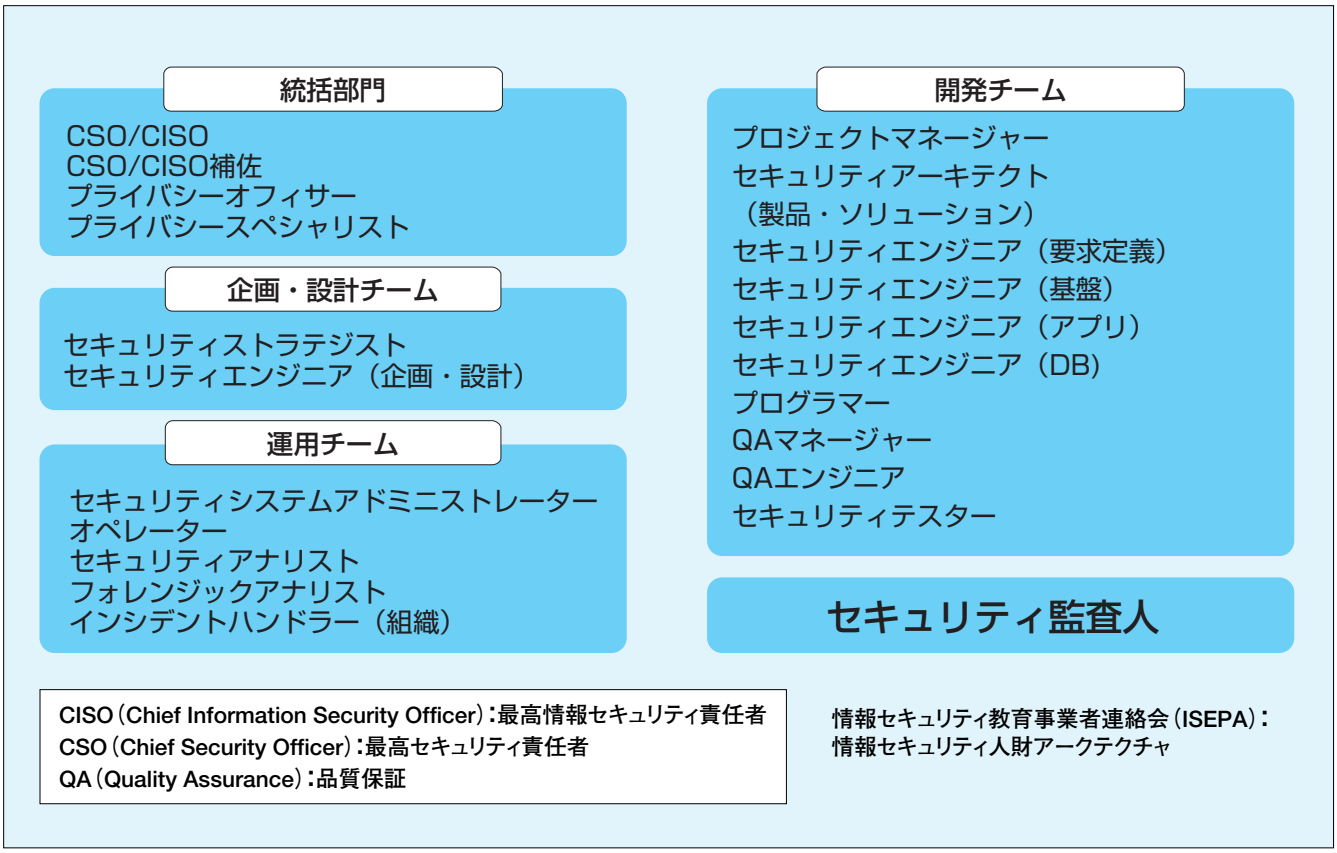


で作成できます。組織モデル自体、各組織、またプロジェクト毎で固有のものになりますが、情報セキュリティ教育事業者連絡会（ISEPA）において、この組織モデルの事例を作っていますので、**図表4**にて参考までに掲載します。

前述しました「職種」ですが、個々の名称は、人や組織によって違ってきますし、定義もそれぞれ異なることになるかと思いますが、要は自組織において必要とされる業務遂行をする人材を何と呼ぶかということですので、組織固有のものでも構いません。一旦、組織において必要とされる業務と職種の特定が終わると、次にそれぞれの職種における業務遂行に必要な知識・スキルをリストアップする必要があります。職種と知識・スキルの結び付けも、個々の組織の業務内容と職種の定義によって変わってくるわけですが、こちらも参考として、ISEPAにおける成果物の一部を**図表5**にて掲載しておきます。

ここまで出来た段階で、今度は、完成した組織モデルと知識･スキルをベースに、個々人に対してのキャリアパスを明確化し、そこに行き着くまでの

図表4　組織モデル―企業内情報セキュリティ機能―



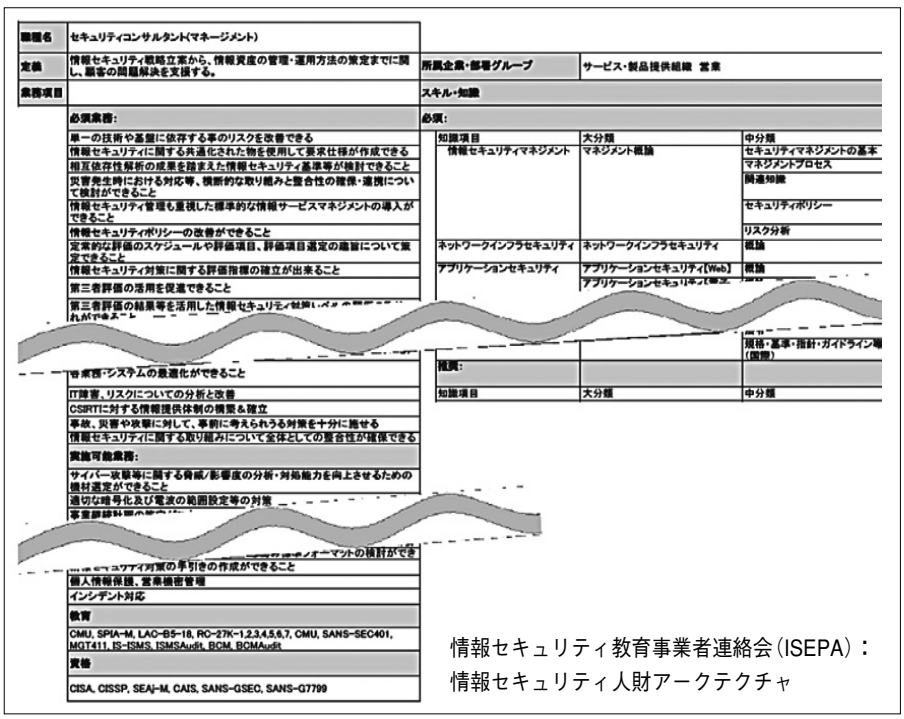
PDCAサイクルといったものを作成します。このPDCAは、「現状認識」－「目指す方向性の確認」－「必要知識の習得」－「現状認識」といったサイクルになります。当然知識の習得には、自社内外の研修、OJTなどを最大限有効に活用することが必要となります。重要なのは、これらを個々人の努力に任せるのではなく、組織としてきちんと対応することです。

次に、育成した人材の評価のポイントについてお話ししたいと思います。評価については、大きく分けると2点あります。知識習得レベルの確認、そして実務レベルにおいての評価です。重要なのは、知識習得という観点からだけの評価では、組織に貢献できる人材は育たないし、有効活用できないということです。知識習得レベルの評価においては、資格取得などのベースにして行うことは有効性が高いと言われています。客観的な第3者の認定を受けていることで、一定レベルの知識を身につけていることを証明することができるからです。実務レベルでの評価に関しては、実習的な研修や、当然業務上での上司や同僚などからの評価・観察によって行うことになります。これらの評価は、前述しました人材育成のPDCAサイクルに当てはまった形で行う必要があり、人材育成同様、組織としての制度として策定し、昇進なども含めた総括的な人事制度の中に取り入れていくことが重要になります。

これらの人材育成や評価の制度ですが、自組織の人材にだけ当てはまる訳ではありません。多くの行政機関の情報セキュリティ業務がアウトソースされている現状では、人材像やPDCAサイクルを含めた仕組み、人材評価制度などを、業務委託決定要件の一部として取り入れることで、一定レベル以上の業務遂行を保証することが可能になります。

次回以降、2回にわたり、情報セキュリティ人材に必要な知識について、詳細に渡りご説明したいと思います。

図表5　ISEPAにおける成果物の一部



情報セキュリティ教育事業者連絡会(ISEPA)：
情報セキュリティ人財アークテクチャ