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③

情報セキュリティ人材に必要な知識

(ISC)² Japan
代表　衣川　俊章（CISSP）

今回からは3回にわたって、情報セキュリティ業務に従事する人間にとって必要となる知識について説明します。最初の2回はベースとなる基礎知識群について、そして最後に行政機関に特化した情報セキュリティ要件の知識について（ISC)²の策定した4つのドメイン（知識分野）に基づいて説明していきます。

基礎知識をまとめた物としては、前回も紹介したように、内閣官房情報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**）を参照するのが良いかと思います。これらの知識群は、大きく分類すると、マネジメント系、技術系と分けられます。当然、両方にかかってくる分野もありますが、今回は、前述の2種類の報告書記載の知識項目を、この2分類に分けて、その中でもマネジメント系の知識分野について説明していきたいと思います。

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/

1. 情報セキュリティマネジメント

まず知っておかないといけないのは、情報セキュリティの3要素と呼ばれているものです。情報が常に利用できる状態になっていて（可用性）、その情報が改ざんなどされずにあるべき状態にあり（完全性）、かつ見れるべき人にしか見れないようになっている（機密性）状態を確立することが情報セキュリティには必要だという概念のことです。この理解を軸に、適切なセキュリティマネジメントを行うために必要なルール作り（ポリシー、スタンダード、プロシージャ、ガイドラインの策定）、文書化、実施方法について理解すると共に、そのマネジメントを有効に実施するため、情報の分類、リスクの特定、リスク評価、リスク分析（定性的・定量的）等の手段を用いてセキュリティの脅威を特定し、資産を分類し、システムの脆弱性を評価する方法について理解することが必要となります。

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 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	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

2. セキュリティアーキテクチャ

セキュリティ対策を実装するに当っては、企業や組織における青写真というのが必要となります。最適な青写真を作るための概念、原則、構造、規格・標準について理解することも非常に重要な知識です。これをベースにすることで、組織にとっての最適インフラを設計し、モニターし、セキュリティを確保することが可能になります。

ここで言っているインフラとは、ハードウェア、ソフトウェア、オペレーティングシステムとそれに関わる全ての機能、アプリケーションやネットワーク環境、そしてセキュリティ意識向上とトレーニングプログラムや、ポリシー・プロシージャ・ベースラインなどのルール、そしてアーキテクチャ策定に参照すべき規格・標準までを含む、基盤全体のことを指しています。

3. 運用

ハードウェアやPCのハードドライブやUSBメモリーなどの記録媒体、また、これらのリソースにアクセス権を持つオペレーターや管理者等を管理する方

法について理解することで、実装されている対策の実効性を高めることができます。様々なインフラの構成管理や変更管理策や手法を理解し、情報資産保護の観点からの運用上の違反行為の特定基準、検出方法、管理策の策定から、運用システムの種類と必要性、また情報資産保護環境（データセンター、サーバールーム、コンピュータルームなど）の必要性についての理解をしている事が求められます。

4. 事業継続

災害やインシデントなどにより、正常な事業運営機能が停止した場合、重要な事業プロセスを保護するため、業務の維持と復旧計画を策定し、その内容をテストし、維持更新していくことに関しての知識を保有していることは非常に重要な要素です。重要な事業プロセスを特定するためのリスク分析や、インシデントレスポンス計画の洗い出しと組織としての選択基準などの知識も得ておく必要があるでしょう。

5. 法令・規格

情報資産保護に関連する法令、規則、コンプライアンスを理解しておかないと、先に述べた情報セキュリティマネジメントは適切に施行されていきません。ここでは特定の法令の理解と同様に、情報資産に関連する法体系や法的概念についても理解をしておく必要があります。またインシデント発生時の原因特定や犯罪が行われたかどうかを判断するために使用する捜査手段と技術、証拠の収集方法、法執行機関への連絡方法などについても知っておく事は、インシデントの適切なハンドリングには不可欠となります。

6. 物理セキュリティ

全ての情報資産は、物理的な環境上で格納され、保護されています。そのため、その環境を保護するための適切な物理セキュリティについては、総務担当や資材管理部署に対してインプットが出来るだけの知識は持ち合わせておく必要があります。外部周辺エリアから内部のデータセンターやサーバールームを含むオフィスエリアにおけるすべての情報資産やその施設全体の物理的な保護技術については、階層化モデル、環境設計、施設の場所、施設建設の影響、インフラサポート設備などを知識として持ち合わせておく必要があります。

7. セキュリティ監査

導入、実装されている情報セキュリティ対策が、適正に機能しているかどうかについて担保することは非常に重要な要素です。システム仕様が必要な機能を網羅しているか、脆弱性が存在せず、日々の運用が適切に行われ、それがログや各種記録によって証明されているかを確認することが監査ですが、これに関する原則や現存する法令・制度の理解、また具体的な監査手法、内部・外部監査の違いなどについて知っておく必要があります。

以上が、組織の情報資産を保護するために必要な基礎知識の中で、マネジメント系と分類した項目の個々における説明となります。次回は、技術系と分類した項目について説明をしたいと思います。