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④

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）

今回は前回に引き続き、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ていきたいと思います。今回は、ベースとなる基礎知識群の中で技術系の知識分野について紹介していきたいと思います。

今回説明をする技術系の知識分野については、前回もご紹介しました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**）の中から抽出しています。各図の青色で囲った部分が技術系の知識分野ですが、これを見れば分かるように、情報セキュリティの知識分野における技術系の占める割合は大きいものになっています。ということで、これらの原則を理解する事は情報セキュリティに関わる人であれば必須かと思います。

情報セキュリティに関わる技術要素の理解をするに当たっては、前提知識としてのネットワーク技術の理解が必要となります。多くの情報セキュリティ

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/

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 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

技術は、ネットワーク技術要素や機能を利用した形で成り立っていることも多く、これらの理解無しでは、情報セキュリティ技術理解は難しいと言えます。行政機関の情報セキュリティにおいては、GPKIや住基ネットワークなど特有の技術要素を利用したシステムが存在していますので、前回説明したマネジメント系の知識はもとより、前提知識としてのネットワーク技術も含めた技術系分野の知識もきちんと理解をすることで、適切な情報セキュリティ対策導入、運用が出来るようになると思います。

1. 暗号

昔から、通信を見せたい相手にだけ確実に完全な状態で見せることを目的として、さまざまな形で暗号化というのが行われてきました。現在でも、完全性・機密性・信頼性を確保するために暗号は様々な形で使用されています。ここでは、暗号化の原則、手段及び方式、また暗号への脆弱性や脅威・攻撃方法についての理解が重要です。原則を知るための基礎知識としての暗号技術の歴史や、さまざまな暗号方式・アルゴリズムの原則・種類・特徴、暗号の理解には欠かせない公開鍵・共通鍵のアルゴリズム、鍵に関する様々なコンセプト、また暗号の実装形態としてのPKI、電子署名などについても理解をしておく必要があります。

2. アクセス制御

情報資産を保護するに当たって、とても重要な要素となるのが、アクセス制御です。誰がどの情報に、どのように、いつアクセスすることが出来るかを具現化する技術としてのアクセス制御技術について知っている事は、ある意味では情報セキュリティの根幹部分とも言えると思います。識別、認証、認可の違いの理解、説明責任をどのように実現するのか、アクセス制御の原則・基本概念や、アクセス制御の種類及び分類、アクセス制御技術とモデル、監視システム、監査方法等について十分な知識が必要となります。また、これらの制御をやぶろうとするリスク、脆弱性の種類、そして様々な不正なアクセス手法（代表的なものとして、バッファーオーバー

フロー、なりすまし、トロイの木馬、パスワードクラックなどがあります）を理解することで、自組織の状況と照らし合わせた最適なアクセス制御を実装することができるようになります。

3. ネットワークインフラセキュリティ

ここでは、複数のデバイスが情報交換できるよう相互接続された環境におけるセキュリティ技術について理解をする必要があります。セキュリティ技術を理解する前提としてのネットワーク構造（LAN、WAN、インターネットやリモートアクセスなど）や伝送（トランスミッション）方式、伝送（トランスポート）形式などについて知った上で、可用性・完全性・機密性を提供するために使用されるセキュリティ手段、専用通信網・公衆通信網・メディア上の通信認証技術、ネットワーク上の脅威およびその防護策について理解をしないといけません。特にセキュリティ手段の中では、ファイアウォール（FW）ついては、様々な種類のFW についてメリット、デメリットについて認識し、その他侵入検知技術についてもネットワーク構造や伝送方式・形式によって異なる要素を適用しないといけないということを理解することはネットワーク上の情報保護においては非常に重要です。またネットワーク上の脅威については、攻撃者の進歩やネットワークの複雑化に伴い、脅威の質も向上してきていますので、常にアンテナを張り情報収集をし、理解をすることで、それらへの的確な対策が取れるようになります。

4. アプリケーションセキュリティ

多くの情報がコンピューター上に格納されている状況の中で、そのコンピューターを動かし、様々な機能を提供しているソフトウェアに関してのセキュリティ概念を理解することは必須だと考えます。特に、ライフサイクル管理と呼ばれるプロセスにおいてのシステム及びアプリケーションを保護する為の知識、手法、原則や、システム開発プロセスにおいて可用性、完全性、機密性を実現する為の概念についても知っておく必要があります。当然、日常的に発生しているウィルスを始めとしたアプリケーションレベルの脅威とその対策についても理解しておかないといけません。ただプログラマーではないので、ソフトウェアの開発工程や方法などについて詳細まで理解をする必要はなく、開発段階でセキュリティがきちんと組み込まれる為に必要な知識や概念を、プログラマーなどに的確に適宜、伝達できることが求められています。

5. オペレーティングセキュリティ

ソフトウェアには、前述のアプリケーションともう一つオペレーティングシステム（OS）が存在しています。ここではOSの種類を理解し、それぞれにどういった脅威が存在しているのか、またその対策についてなどを理解しておかないといけません。当然アプリケーションセキュリティ同様、開発段階でセキュリティ確保がなされる為、開発工程や方法などについてきちんと理解をしておく必要もあります。

次回は、最終回となりますが、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たいと思います。