情報セキュリティにおける教育の重要性と人材の育成

Importance of Education and Human Resource Training in Information Security

田 中 信 也

要 約 近年では人，物，金，情報，に加えて「信用」が企業活動を支える五つ目の資産として注目を集めている．しかしながら，最近ではこの企業の「信用」を揺るがすような情報漏洩事件が相次いでおり，多くの企業が情報セキュリティ対策に取り組んでいる．情報セキュリティ事故は，原因の73%が人的要因と考えられる．従って，情報セキュリティ対策において情報セキュリティ教育は重要な要件といえる．本稿では，情報セキュリティ対策のPDCAサイクルのそれぞれのステップで求められる人材の育成と，その実現方法を紹介する．

Abstract In late years,“ Trust ”has shared the spotlight as the fifth asset with people, goods, capital and information, all of which carry the business activities. However recently, the disclosure of critical information has successively happened that shakes the trust of a company. In the result, many companies are working on the measure of information security. It is said that 73% of information security incidents are caused by human factors. Therefore, the education is one of important requirements for the security measures. This report describes the training for human resources for the information security based on each of PDCA cycle in the security measures, and how to fulfill that training.

1. はじめに

情報セキュリティ対策および個人情報保護対策の立案において，教育という視点は外すことができない重要な要件である．また，相次ぐ情報漏洩事件の発生や2005年4月の個人情報保護法完全施行を背景に，企業や消費者の情報セキュリティに対する関心が高まっている．情報セキュリティ関連ビジネスの2007年の市場規模は1兆1,647億円，年間平均成長率は24.0%と予測されている．このような市場の拡大に向けて日本ユニシスグループ内の情報セキュリティ人材の育成も急務である．

本稿では情報セキュリティ対策において教育が強く求められる背景を検証し，情報セキュリティに関連する各人材モデルに求められる主な役割，スキルを明らかにし，その育成に向けた教育の効果的な実現方法について述べる．

2. 情報セキュリティ教育が求められる背景

2.1 情報セキュリティに対する社会的要求の高まり

2.1.1 近年発生した情報セキュリティ事故の概要

近年，官民を問わず情報漏洩，サービス停止などの情報セキュリティ事故が後を絶たない．JNSA（NPO日本ネットワークセキュリティ協会）が2002年度および2003年度に行った調査によると，インターネット上に報道された情報漏洩事件の被害者数の合計は公開されているものだけでも2002年度の41万8,700人に対して2003年度は155万4,500人と大幅に増加している．

情報セキュリティとは，情報資産の機密性，完全性，可用性を維持することであると定義できる．情報セキュリティ事故とは，この状態が何らかの脅威により崩れることを言う．具体的な脅威としては，情報漏洩，情報改ざん，サービス停止，コンピュータウイルス感染などがある．

2.1.2　ネットワーク社会における情報漏洩のリスク

情報漏洩事件などの情報セキュリティ事故がここ数年で急増している背景には，ノートパソコンの普及およびメディアの大容量化により情報の持ち出しが容易になったことと，ブロードバンドの普及にともなうネットワークの高速化と大衆化がある．また，ネットワークの持つ匿名性も原因の一つと考えられる．

このような環境変化により情報資産に対するリスクは増大しており，「これまでと同じ感覚では事故を防ぐことはできない」という事実を，全社員に理解させることが重要である．

また，ネットワークの高速化と普及は，事故が発生した後の被害の拡大にも大きな影響を及ぼしている．ひとたびインターネットに流失した情報は，瞬く間に広まり，それを制御することはきわめて困難である．大手ブロードバンド接続事業者で発生した顧客情報流失事件で，未だに副次的な被害が発生していることを見れば，回収できない情報が残存リスクとして影響を及ぼすことは明らかである．

2.2　情報セキュリティ事故原因の分析と特性

2.2.1　情報セキュリティ事故の物理的要因

そもそも，情報セキュリティ事故はなぜ発生するのだろうか．情報漏洩事故が発生する要因を分析すると，大きくは物理的要因と人的要因の二つに分類することができる．

物理的要因とは管理体制の不備，外部からの不正アクセスや不法侵入などのことを言う．表1に情報漏洩事故の物理的要因の概要を示す．

表1　情報漏洩事故の物理的要因

管理体制の不備	管理・保管方法の不備による漏洩
外部からの不正アクセス	システム環境のセキュリティ不備による漏洩
不法侵入	外部からの侵入・盗難による漏洩

2.2.2　情報セキュリティ事故の人的要因

情報セキュリティ事故の人的要因とは，無知や過失，故意によるものなどが挙げられる．事故原因となっている人員が組織内部に存在するため，データに対する正規のアクセス権をもっていることが多く，システム的な防御が困難である．表2に情報漏洩事故の人的要因の概要を示す．

表2　情報漏洩事故の人的要因

無　知	問題行動を認識していないことによる安易な取り扱い
過　失	操作ミスや外部に持ち出した情報の紛失盗難
故　意	売却等を目的とする外部への持ち出し

2.2.3　人的対策の重要性

JNSA が公表する「2003 年度情報セキュリティインシデントに関する調査報告書」によると，情報漏洩事故原因のうち「設定ミス」,「誤操作」,「管理ミス」などの技術的要素による人為ミスが 46%,「置き忘れ」などの非技術的要素による人為ミスが 2%,「内部犯罪」や「情報の持ち出し」,「盗難」などの非技術的要素の犯罪・過失が 25% と報告されており，これらを合計すると 73% が人的要因による事故といえる．これらの事故は，物理的要因に対する対策だけ行っていても防ぐことができないということになる．

内部の人間は，本来の業務で個人情報を始めとする各種の機密情報にアクセスする権限を持っている．故意であれ，過失であれ，正規の手順に従って取り出されるデータをシステム側では拒否することはできない．一度取り出された情報は大容量のメディアや電子メールなどでセキュリティゾーンから持ち出され，漏洩の危険にさらされるのである．

システム的な制御が困難である以上，情報を扱う人員に対して適切な利用を求めるしか現段階では有効な方法はないと言えるだろう．

筆者はこれまで顧客企業の人事部門担当者や教育担当者から，情報セキュリティ教育に関する相談を受けてきたが，一般社員の情報セキュリティに対する意識は想像以上に低いという印象を受けた．人的要因による情報漏洩事故は，ネットワークにおけるファイア・ウォールのように一部の担当者が頑張れば防げるというものではない．社員・職員の全員が情報セキュリティのファイア・ウォールにならなければ情報漏洩は防ぐことができないのである．

このような背景もあり，情報セキュリティ教育では対象者が全社員におよぶケースも多い．情報セキュリティ教育を実施することで，無知による事故を防ぎ，過失を起こさないよう注意を喚起することができ，さらに故意による情報漏洩に対してもある程度の抑止効果が期待できる．

2.3　情報セキュリティ事故を防ぐための対策

2.3.1　情報セキュリティ事故を防ぐための企業の取り組み

情報セキュリティ対策を実現するプロセスを考える際の基本となるのが 「PDCA サイクル」である．情報セキュリティ対策における PDCA サイクルは図 1 に示すように計画・構築，実施・運用，点検・監視，見直し・改善の四つのプロセスになる．

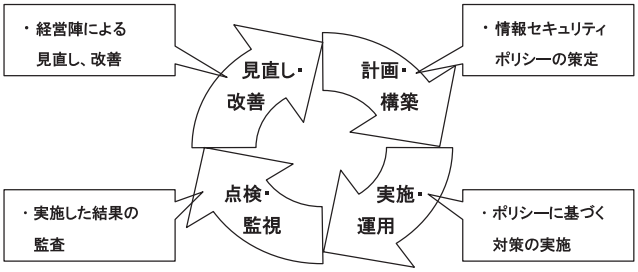

図 1　情報セキュリティ対策の PDCA サイクル

情報セキュリティ対策における PDCA サイクルの計画・構築プロセスで策定しなければならないものに,「情報セキュリティポリシー」がある．情報セキュリティポリシーは企業の情報セキュリティに関する基本方針であり，情報セキュリティを重視する経営方針を社内外に示

す重要な宣言でもある．広義には情報セキュリティ対策基準や個別の具体的な実施手順も情報セキュリティポリシーに含まれる．

情報セキュリティポリシーの一般的な構成を図 2 に示す．

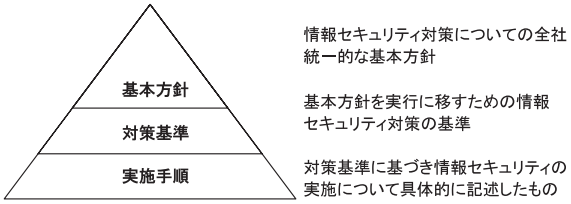

図 2　情報セキュリティポリシーの階層構造

情報セキュリティ人材は「情報セキュリティポリシー」の役割と位置付けをしっかりと理解し，その策定から組織内への浸透まで関与できるスキルが必要である．

情報セキュリティポリシーでは，ポリシーの目的を始めとし，用語の定義や情報資産の取扱原則，推進組織の役割や周知徹底のための教育研修，監査や危機管理などについて策定しなければならない．このため情報セキュリティポリシーの策定には，管理部門だけではなく経営層から業務部門まで，すべての関係部門が参画する必要がある．このメンバーが，情報セキュリティ委員会を構成し，情報セキュリティポリシーの推進組織となる．

情報セキュリティ教育の観点では，この推進組織のメンバーに対して，ポリシー策定を推進する動機となるような強い意識付けと，ポリシーを策定するために必要な知識を習得させることが必要となる．

また，情報セキュリティポリシーは策定しただけでは絵に描いた餅になってしまう．策定したポリシーの運用も考えなければならない．情報セキュリティポリシーの運用は，情報を取り扱う全ての社員・職員に関係するため，全社レベルの制度化された運営組織が必要である．具体的には情報セキュリティ委員会に加えて，部門毎に情報セキュリティ責任者等を任命する必要がある．

情報セキュリティ教育の観点では，各部門の情報セキュリティ責任者に対して，情報セキュリティポリシーの運用に必要な責任者・管理者教育を行う必要がある．

2.3.2　情報セキュリティ管理体制に関する第三者認証制度

情報セキュリティにおける管理･推進体制の構築には,基準として各種のガイドラインがある．そのような基準に「準拠している」ことを証明するものとして,第三者による認証制度がある．

情報セキュリティに関する第三者認証制度としては「ISMS 適合性評価制度」がある．ISMS 適合性評価制度とは企業の情報セキュリティマネジメントシステム（情報セキュリティ対策の PDCA）が国際標準規格である「ISO/IEC 17799」に準拠しているかどうかを，日本情報処理開発協会（JIPDEC）が認証する制度である．ISMS の認証取得を目指す企業の情報セキュリティ委員会メンバーや，情報セキュリティビジネスで ISMS の認証取得を支援するサービスを提供する人材は，詳細を把握しておきたい制度である．

情報セキュリティとは別に個人情報保護に関する第三者認証として,「プライバシーマーク制度」がある．プライバシーマーク制度は，日本情報処理開発協会（JIPDEC）またはその登

録機関が個人情報保護に関する国内企画である「JIS Q 15001」に基づいて審査，認証を行う制度であり，認証を取得した企業には「プライバシーマーク」と呼ばれるロゴの使用が許可される．プライバシーマークの認証取得は近年急速にニーズが広がっている領域であるため，情報セキュリティビジネスの拡大という観点では対応できるようになっておきたい制度である．

個人情報保護の国内認証制度としてはプライバシーマーク制度に人気があるが，インターネットのビジネスに国境は存在せず，企業のグローバル化が進んでいることを考えれば，国内の認証を取得するだけでは充分ではない場合もある．TRUSTe（トラストイー）プログラムは，個人情報を扱う Web サイトが利用者に対する信用度・信頼度を向上するという目的で作成されており，現在世界 26 か国で展開されている．情報セキュリティ人材として概要は把握しておきたい制度である．

3. 情報セキュリティ教育の対象領域

3.1 情報セキュリティマネジメントを実現する管理体制

3.1.1 情報セキュリティ管理体制の概要

企業が情報セキュリティ対策の PDCA サイクルを廻すためには，計画の策定から，構築，運用，監査，改善までを行う体制作りが欠かせない．具体的な体制は企業の規模や組織の構造などにより変わってくるが，ここでは一般的な体制を紹介し，情報セキュリティ人材の全体像を捉えることにする．

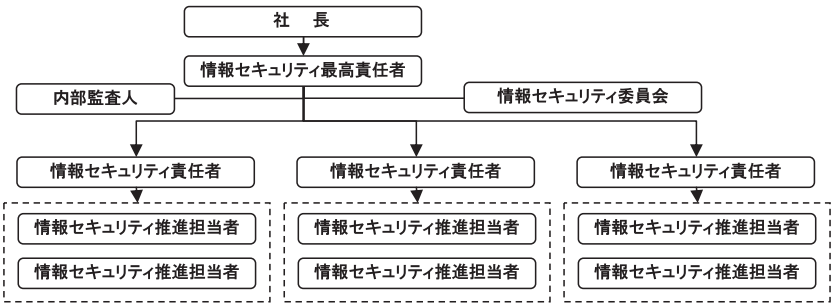

図 3　情報セキュリティ管理体制

情報セキュリティ対策の推進にあたっては，図 3 ような体制を組織し，全体をマネジメントしていくことになる．情報セキュリティ人材とはこれらのメンバー，およびこれらのメンバーをビジネスとして支援する人材のことを言う．

3.1.2 個人情報保護体制の概要

個人情報保護管理体制は企業の規模によっては，情報セキュリティ管理体制のメンバーが兼任することもあると考えられる．しかし，個人情報保護における責任と役割を明確化するためにも，体制としては情報セキュリティ管理体制とは別に定義しておくことが望ましい．

一般的な個人情報保護管理体制の例を図 4 に示す．

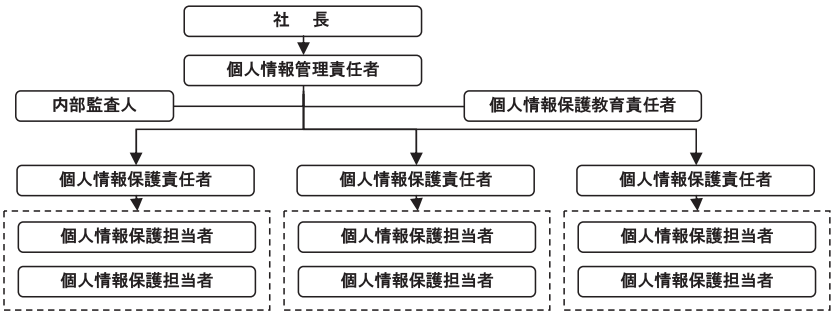

図 4　個人情報保護管理体制の例

3.2　情報セキュリティ管理体制を構成する人材モデル

1）　情報セキュリティ最高責任者の主な役割

情報セキュリティ最高責任者（CISO）は組織内の情報セキュリティに関する全ての問題を統括する責任者である．

情報セキュリティ最高責任者の主な役割は以下の通りである[1]．

・情報セキュリティ対策の実施を統括する
・情報セキュリティ委員会と経営層との間の連絡と報告を行う
・情報セキュリティポリシーと各種規程のメンテナンスを指示する
・インシデント対応の調整を行う
・企業全体の情報セキュリティ意識向上プログラムの管理を行う，等

情報セキュリティ最高責任者は情報セキュリティと情報技術に関するある程度の知識が求められるため，そのような素養を持つ人材を選出し，教育を行うことが必要である．

2）　情報セキュリティ委員会の主な役割

情報セキュリティ委員会を構成するメンバーは管理部門に限らず，広く業務部門を含めて構成する必要がある．このため情報セキュリティ委員会のメンバーは通常の業務との兼任者が多くなる．このような組織を適切に運営していくためには専任の事務局を設置することが望ましい．

情報セキュリティ委員会の主な役割としては，以下のようなものが挙げられる[1]．

・情報セキュリティポリシーを策定し，経営層の承認を得る
・情報セキュリティポリシーに基づき情報セキュリティ対策を策定する
・情報セキュリティ対策の実施を監視する
・情報セキュリティポリシーの効果をレビューする
・情報セキュリティ問題の意識向上を推進する，等

情報セキュリティ委員会のメンバーは，情報セキュリティポリシーの策定において大きな役割を果たすため，ポリシー策定に関わるスキルを身に付けてもらう必要がある．

3）　情報セキュリティ責任者の主な役割

各部門の情報セキュリティ責任者は組織の規模や形態によっては，情報セキュリティ委員会のメンバーが兼任するケースもある．その場合，部門の情報セキュリティ責任者としても，自部門の情報セキュリティ対策を推進しなければならない役割がある．

情報セキュリティ責任者の主な役割としては以下のようなものがある．

・部門内の情報セキュリティ対策実施を統括する
・情報セキュリティ委員会との間の連絡と報告を行う
・部門内の情報セキュリティ対策を実施する
・部門内のインシデント対応を調整する
・部門内の情報セキュリティ意識向上プログラムの管理を行う，等

情報セキュリティ責任者には，委員会や自部門で定めたポリシーを，組織のメンバーに遵守させるためのスキルも求められる．

4) 情報セキュリティ推進担当者の主な役割

情報セキュリティ責任者は部門長が兼任するケースが多いため，実作業を行う推進担当者を別に設置しなければならない場合もある．情報セキュリティ推進担当者は情報セキュリティ責任者の指示を受け，部門内の情報資産の洗い出しや，社員に対する情報セキュリティ教育などを実施する．

5) 個人情報管理責任者の主な役割

個人情報管理責任者（CPO）には個人情報保護体制の確立を担う中心的なリーダとしての役割が求められる．CPO を中心とした体制の下，コンプライアンスプログラムと呼ばれるマネジメントシステムが構築され，運用されていくことになる．

6) 個人情報保護責任者の主な役割

個人情報保護責任者は，各部門においてコンプライアンスプログラムの実施・運用を推進し，個人情報保護を実効あるものとする管理者である．個人情報保護責任者は主に企業内/組織内の部長，課長，係長等個人情報を取り扱う従業員を管理する立場にいる人材を任命する．

7) 内部監査人の主な役割

情報セキュリティ対策や個人情報保護対策は，策定した瞬間から陳腐化が始まる．情報セキュリティ対策の PDCA サイクルでも監査は継続的な改善を行うためのプロセスの一つとして求められている．自社内に内部監査の体制を作るためには監査人の育成教育が必要になる．

8) 情報システム部門セキュリティ担当の主な役割

人的対策が適切に取られていれば技術的対策が不要というわけではない．技術的対策としては，ネットワークや認証システムの管理，外部接続点や社内ネットワークの監視，各種情報収集とインシデント対応などが挙げられる．

3.3 情報セキュリティベンダーに求められる人材モデル

3.3.1 情報セキュリティスペシャリストの主な役割

1) 情報セキュリティコンサルティングの実施

情報セキュリティスペシャリストとは IT 企業において情報セキュリティビジネスを推進する人材である．企業にとって情報セキュリティポリシーの構築が不可欠となった現在，その策定から運用までをサポートするコンサルティング能力が情報セキュリティスペシャリストには求められる．ISMS やプライバシーマークなどの第三者認証取得の支援を行う場合もある．

2） 情報セキュリティアーキテクチャの設計

情報セキュリティアーキテクチャの設計は，独立行政法人情報処理推進機構（IPA）が発表した「情報セキュリティスキルマップ構築の調査研究」[3] の中で示されているスキルモデルのうち，情報システム全体に対するセキュリティ設計と，ネットワーク系アプリケーションの設計・開発の二つの領域に相当する．

情報セキュリティ会社の分析によれば，近年攻撃の対象が Web サーバから Web アプリケーションに移ってきているという傾向が見られる．このような傾向に対応するため，高度な情報セキュリティアーキテクチャを設計できる人材の早期育成が望まれる．

3） 情報セキュリティプロダクトの導入

情報セキュリティプロダクトの導入は，「情報セキュリティスキルマップ構築の調査研究」[3] の中で示されているスキルモデルのうち，「不正アクセス対策システム導入」に対応する．この業務を担当するためには，各種情報セキュリティプロダクトに関する知識が求められる．

4. 対象領域毎の主な教授項目

4.1 管理体制を構築する人材に求められるスキル要件

4.1.1 情報セキュリティの基礎知識

1） エグゼクティブに必要な基礎知識

情報セキュリティ対策にはエグゼクティブのコミットとリーダシップが欠かせない．しかし，情報セキュリティ対策は直接利益を生み出すものではないため，エグゼクティブにとって積極的な投資の対象として考えることは難しいようである．このような問題を避けるため，エグゼクティブにもリスクアセスメントに参画してもらい，リスクを認識し，許容できるかどうかを見極めることで，どのリスクに対してどれだけの投資を行うべきかという判断をしてもらうのが良い．

2） 情報セキュリティ委員会のメンバーに必要な基礎知識

情報セキュリティ委員会のメンバーは情報セキュリティプロシージャの策定など，情報セキュリティ対策の計画段階から深く関与が求められる．情報システムの専門家でなくても，最低限必要な情報セキュリティの知識を身に付けておくべきである．

4.1.2 ISMS を構築するために必要なスキル

ISMS を構築するには，まず構築手順の概要を把握し，業務機能の関連把握，情報資産の洗い出しと脅威，脆弱性の明確化，リスク分析，管理目標・管理策の選択と残存リスクの認識などの手順について身に付ける必要がある．

4.1.3 コンプライアンスプログラムを構築するために必要なスキル

コンプライアンスプログラムを構築するためには，個人情報保護法とガイドラインとなる JIS Q 15001 規格の要求事項との関係，プライバシーマーク制度における CP 構築の概要について把握し，個人情報保護方針の策定，組織体制の編成，個人情報の特定，各種規程・手順書等の作成，教育と内部監査などを行うスキルを身に付ける必要がある．

4.1.4 内部監査を実施するために必要なスキル

内部監査は適切なスキルを持った人材が組織的に実施する必要がある．内部監査を行うには主に内部監査基本計画の策定，個別内部監査計画の策定，内部監査の実施，内部監査報告，是正・予防措置を実施するためのスキルを身に付ける必要がある．これらは内部監査員養成研修などで身に付けることができる．

4.2 情報セキュリティスペシャリストに求められるスキル要件

4.2.1 情報セキュリティスペシャリストに必要な基礎知識

情報セキュリティビジネスに関わる専門化として，どの領域の業務を担当するにしても，情報セキュリティの基礎技術に関する知識は欠かすことができない．情報セキュリティスペシャリストとして最低限理解しておきたい知識としては，以下に示すものが挙げられる．

・情報セキュリティの概要，セキュリティの分類，脅威の分類
・暗号化技術の要素と用語，暗号化方式の分類と比較，各暗号の特徴
・IP プロトコルの各層におけるセキュリティ
・攻撃者の種類と行動，攻撃の種類
・情報セキュリティポリシーの概要，各種認証方式
・デジタル署名と証明書
・ネットワークのアクセス制御，コンピュータのアクセス制御
・可用性と責任追及性の情報セキュリティ対策
・事業継続性の管理，等

情報セキュリティ関連プロジェクトのメンバーとして活動するためには，これらの知識を身に付けておくことは必須条件である．

4.2.2 情報セキュリティコンサルティングの実施に必要な主なスキル

情報セキュリティコンサルティングでは主に ISMS や CP の構築，認証取得，監査の支援を行なう．従って情報セキュリティコンサルティング業務に必要なスキルは，以下に示すようなものになる．

・ISMS 認証制度の概要，ISMS セキュリティポリシーと詳細管理策，
　ISMS 構築プロジェクトマネジメント手法，情報資産の洗い出し，
　ISMS 文書の作成，ISMS 適用宣言書作成
・個人情報保護法の概要，プライバシーマーク制度との関係，
　JIS Q 15001 の要求事項，コンプライアンスプログラム策定，
　個人情報の適正管理のためのセキュリティ構築，
　プライバシーマーク認定取得と継続的運用
・監査計画の策定，チェックリストの作成，監査サンプルの取得，
　監査の実施，不適合報告書の作成，マネジメントレビュー，等

上記の知識の習得に加えて，コンサルタントに本来求められる各種のヒューマンスキルや業務知識も合わせて身に付け，OJT で実践経験を積むことが必要である．

4.2.3　情報セキュリティアーキテクチャの設計に必要な主なスキル

情報セキュリティアーキテクチャの設計では，セキュアなシステムを設計・構築することが求められる．そのためにはシステムを構成する様々なプラットフォームやソフトウェアの堅牢化を図り，開発するアプリケーションの情報セキュリティ対策，事故が発生した場合に備える危機管理など，以下に示すようなスキルが求められる．

・Windows セキュリティにおける攻撃手法の理解
・Windows の堅牢化テクニック
・インシデントハンドリング
・ネットワークセキュリティにおける攻撃手法の理解
・UNIX におけるセキュリティ
・Web アプリケーションのセキュリティ対策，等

情報セキュリティ侵害のテクニックは日々進化しているため，情報セキュリティスペシャリストのスキルも常に最新の技術に対応していることが求められる．このため，情報セキュリティスペシャリストに対する継続教育は欠かせない．

4.2.4　情報セキュリティプロダクトの導入に必要な主なスキル

情報セキュリティプロダクトの導入に必要なスキルは，取り扱う情報セキュリティ製品に依存する．個々のプロダクトに関する詳しい知識に加えて，目的に合わせてプロダクトを選定できる判断力や，複数のプロダクトを組み合わせる場合の構成を検討するスキルも要求される．

プロダクトのスキルは，利用するプロダクトに合わせて育成を図る方法が現実的である．ただし，各プロダクトの概要や特徴は全ての情報セキュリティスペシャリストが把握しておきたい情報であり，プロダクトの説明会などは全ての情報セキュリティスペシャリストを対象に実施すべきと考える．

5.　情報セキュリティ教育の実現手段

5.1　管理体制を構築するために有効な教育手段

5.1.1　集合研修のメリットとデメリット

情報セキュリティ管理体制を構築するための教育は，情報セキュリティ最高責任者から情報セキュリティ委員会メンバーなど，比較的限られた対象者に対して実施される．このような場合の教育手段としては一般的に集合研修が用いられる．

集合研修では講師，受講者同士の相互作用で研修効果を高めることが可能である．また受講者のレベルに合わせて，教授内容をアレンジしたり，受講者の要望に合わせて情報提供を行うこともできるため，効果的な教育を実施することができる．

そのようなメリットがある反面，集合研修にはデメリットも存在する．まず，集合研修は同じ時間に同じ場所に集まって実施する必要がある．このため参加者のスケジュールを調整することが困難な場合が多く，受講者が各地に散在する場合，研修会場に集まるための旅費が大きな費用負担となる．

5.1.2　集合教育の成果を高める各種の学習形態

講師が教育内容を説明することだけが集合教育ではない．集合教育のメリットを引き出すた

めには，目的に応じた教授形態を採用することが重要である．

1)　ケーススタディ

ケーススタディは実際に起こった，あるいは想定した事例を基に受講者が議論を行ないながら解決策や提案などを導き出す学習形態である．通常の講義では一方的な知識の伝達に陥りやすいが，その知識を活用した事例として，演習にケーススタディを取り入れると知識と実践の間の橋渡しを行うことができる．

2)　グループワーク

講師が与えた課題に対して，受講者がグループで結果を導き出す学習形態．単に結果を導き出す方法を学ぶだけでなく，メンバー同士の議論を通して，様々な考え方や事象の捉え方などを学ぶことができる．具体的な作業を行うことで，講義で学んだことを疑似体験することができ，実践に備えた予行演習ができる．

【管理者向け研修の事例】

当社では個人情報保護法完全施行を控えた平成 16 年末に，管理者向けにケーススタディとグループワークを組み合わせた個人情報保護対策セミナーを実施した．ケーススタディでは個人情報漏洩の兆候を身の回りの様々な事象から見つけ出すという演習，グループワークでは個人情報が漏洩した場合の被害総額の算出を行った．

受講者からの所感を分析すると，様々な気付きや動機付けが行なわれたことが確認でき，高い教育効果が実証できた．

5.2　全社員向け情報セキュリティ教育の効率的な実現方法

5.2.1　全社員向け教育における e-Learning の有効性

管理者向けの教育と比較して，全社員向け教育では対象者数が飛躍的に増加する．このような教育を集合研修で実施しようとすると実施費用が嵩むケースが多い．まず 1 回の研修で受講できる人数はファシリティによる制限を受ける．仮に大きな講習室が確保できるとしても，全社員のスケジュールを短期間の日程に調整することは困難なため，通常は何回にも分けて実施しなければならない．しかし，このようにして数多くの集合研修を実施したとしても，社員全員が 100% 受講できるというケースは極めて少ないと思われる．このような問題を解決するための有効な教育手段として，e-Learning が注目を集めている．

e-Learning には「PC とネットワークさえあれば，いつでも，どこでも学習できる」という独自のメリットがある．これは集合研修で見られた，「スケジュールの調整が困難」というデメリットを解消することに役立つ．また，全国の拠点に対する教育を実施する際に，地域間の格差を取り除き，講師の移動などに伴うコストを削減することができる．さらには，中途採用やアルバイトなど，不定期に発生する教育ニーズにも大きな費用を掛けずに対応することができる e-Learning のメリットは大きい．

このような基本的なメリットに加えて，社員一人一人の学習履歴が保存される e-Learning では学習完了者や未受講者を簡単に検索することができ，未受講者に対して電子メールで催促の通知を送ることも可能である．情報セキュリティ教育の重要性は全員に漏れなく学習させることである．e-Learning の学習履歴管理機能はこの課題の解決に大きく貢献する．

5.2.2 標準コンテンツと独自開発コンテンツの使い分け

e-Learning の教材には大きく分けると教育ベンダーが開発・提供する標準コンテンツと，ユーザ企業が独自に開発する独自開発コンテンツがある．

標準コンテンツはベンダーが複数の企業に販売することを目的に開発しているため，情報セキュリティや個人情報保護に関する一般的な知識を学ぶためには最適な構成となっている．標準製品であるため費用も安く，低価格で高品質な教材を入手することができるが，ユーザ企業の独自色を出すためにはカスタマイズが必要になってしまう．

一方の独自開発コンテンツは，ユーザ企業が自社向けにコンテンツを開発するため，目的に合わせて自由にカリキュラムを構成することができる．情報セキュリティ管理体制が構築したマネジメントシステムには企業独自のルールが盛り込まれているため，その教育コンテンツとしては独自開発コンテンツが最適である．ただし，独自開発コンテンツは標準コンテンツと比較して開発費用が必要になるため，割高になることも多い．

5.2.3 独自コンテンツの開発方法

独自コンテンツは教育ベンダーに委託して開発する場合と，社内に開発チームを作り自社開発する場合がある．

教育ベンダーに委託して開発を行う場合には，ベンダーの豊富な経験を生かして教育効果の高いコンテンツを開発することができる．イラストや動画，音声などを活用したコンテンツは学習者の興味を引き，学習意欲を引き出すことにも貢献する．しかし，そのようなコンテンツの開発には相応の費用が掛かることも事実である．対象人数が多ければ 1 名あたりの費用はわずかになることも多いので，学習効果を考慮に入れて検討するようにしたい．

また，今日ではオーサリングツールと呼ばれるコンテンツを開発するソフトウェアが何種類も販売されており，ユーザが自分達でコンテンツを開発することも可能である．しかし，適切な開発を行わないと教育効果はあがらない．教材開発は適切な設計と実装が必要であり，コストの削減を目的とした安易な自社開発は避けるべきである．

その一方で自社開発は社員によるメンテナンスが容易であるというメリットもある．コンテンツの開発に関するスキルを身につけた上で取り組むのであれば，有効な手段と言える．

5.3 情報セキュリティスペシャリストを育成するための技術教育

5.3.1 情報セキュリティスペシャリストの基礎教育

先に述べた情報セキュリティスペシャリストに必要な基礎知識を学習するプログラムとしては，情報セキュリティの基礎技術を中心とした集合教育が適切であると思われる．ネットワークや OS に関する基礎技術を持つ IT 技術者を対象に，情報セキュリティ技術の基本的な要素を学んでもらう．

日本ユニシスグループでは 2005 年度のグループ向け情報セキュリティスペシャリスト育成研修の基礎編として CompTIA の Security＋に対応した情報セキュリティ技術基礎教育を 3 日間の日程で実施する．

5.3.2 情報セキュリティコンサルティング能力の育成

先に述べた情報セキュリティコンサルティングの実施に必要なスキルを身に付けてもらうた

めには，ISMS やプライバシーマークの認証取得に向けた各種の作業を演習などで体験できる実践的なプログラムが求められる．

日本ユニシスグループでは 2005 年度のグループ向け情報セキュリティスペシャリスト育成研修のマネジメント編として ISMS 認証取得，プライバシーマーク認証取得，内部監査の実施に向けた集合研修を 5 日間で実施する．

5.3.3　情報セキュリティアーキテクチャ設計能力の育成

先に述べた情報セキュリティアーキテクチャ設計に必要なスキルを身につけてもらうためには，実機を使ったシステム設定や攻撃対策などの実習が要となる．

日本ユニシスグループでは 2005 年度のグループ向け情報セキュリティスペシャリスト育成研修のテクニカル編として Windows と UNIX のプラットフォーム別セキュリティ対策と Web アプリケーションセキュリティ対策，インシデント・ハンドリングなどを中心とした応用技術コースを 5 日間の日程で実施する．

5.3.4　情報セキュリティプロダクト導入能力の育成

情報セキュリティプロダクトに関するスキルは前述したように，プロジェクトの内容や時代の推移とともに大きく変化するため，計画的な育成は難しい．

現状では必要に応じて各種プロダクトのベンダーが提供する教育コースに参加するなどして，必要な知識を身に付けていくのが良いと思われる．

5.3.5　情報セキュリティ技術者認定の概要

情報セキュリティ技術者のスキルを認定する資格制度としては国内外に多くの認定資格が存在する．

図 5 および表 3 に 2005 年 6 月現在で日本語試験が実施されている主な非ベンダー系資格の位置付けと概要をまとめる．

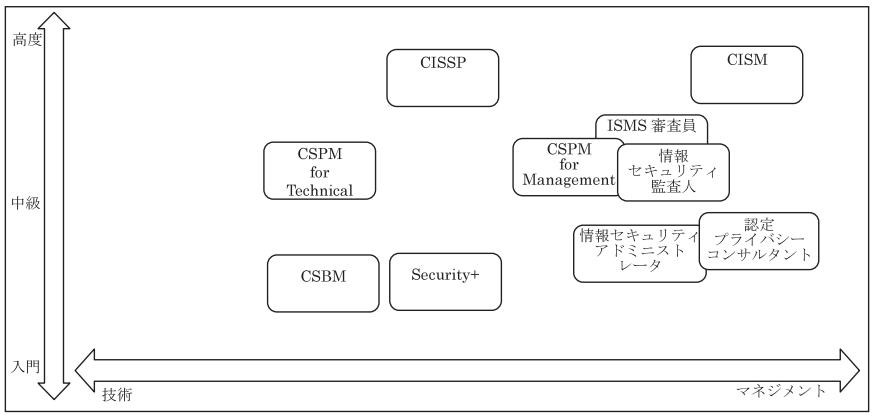

図 5　2005 年 6 月に日本語試験が実施されている主な非ベンダー系資格位置付け

今後ユニシスグループが情報セキュリティビジネスで確固たる地位を築くためには，より上位の資格を目指して情報セキュリティ技術者が精進する必要がある．

表 3　2005 年 6 月に日本語試験が実施されている主な非ベンダー系資格一覧

	資格名称	所轄機関
情報処理技術者試験	情報セキュリティアドミニストレータ	IPA（独立行政法人情報処理推進機構）
	テクニカルエンジニア（情報セキュリティ）	
情報システムセキュリティ・プロフェッショナル	CISSP	非特定営利活動団体（ICS）2
公認情報セキュリティマネージャ	CISM	ISACA（情報システムコントロール協会）
CompTIA	Security+	CompTIA
SEA/J	CSBM	SEA/J（セキュリティ・エデュケーション・アライアンス・ジャパン）
	CSPM for Management	
	CSPM for Technical	
ISMS 審査員	ISMS 審査員補	JIPDEC（財団法人 日本情報処理開発協会）
	ISMS 審査員	
	ISMS 主任審査員	
認定プライバシーコンサルタント	APC（Associate Privacy Consultant）	JPCA（特定非営利活動法人 日本プライバシーコンサルタント協会）
	CPC（Certified Privacy Consultant）	
公認情報セキュリティ監査人（CAIS）	情報セキュリティ監査アソシエイト	JASA（非特定営利活動団体 日本セキュリティ監査協会）
	情報セキュリティ監査人補	
	情報セキュリティ監査人	
	情報セキュリティ主任監査人	

6. お わ り に

本稿では情報セキュリティ対策における教育の重要性，情報セキュリティ対策の PDCA サイクルにおいて必要とされる人材とそのスキル要件，情報セキュリティ人材を育成するための教授項目と，情報セキュリティ教育の実現手段について紹介した．しかし，実際の情報セキュリティ教育は企業の規模や業務内容，従業員のおかれている環境などにより異る．そのような個別の教育ニーズに対して，最適な実現手段を提供するために，日本ユニシス・ラーニング（株）では情報セキュリティ教育のコンサルティングサービスを提供している．

情報セキュリティ教育は「実施すること」が最終目標ではない．「組織の情報セキュリティレベルを向上すること」，そして「情報セキュリティに関するより高度なテクニカルスキルやマネジメントスキルを持ったスペシャリストを育成すること」が本質的な目標である．我々は，お客様の情報セキュリティ対策の実現に欠かすことのできない情報セキュリティ人材の育成を，実践的な情報セキュリティの知識と各種教育技法のノウハウを活用し，効果的に実現していきたい．

参考文献　［1］ 岸田明，経営課題としての情報セキュリティ入門，ソフトバンクパブリッシング，2003
［2］ 山崎文明，情報セキュリティと個人情報保護完全対策改訂版，日経 BP，2004
［3］ IPA，情報セキュリティスキルマップ構築の調査研究，独立行政法人情報処理推進機構，2004

執筆者紹介　田　中　信　也（Shinya Tanaka）

1961年生．1984年日本大学商学部商業学科卒業．同年日本ユニシス(株)入社．主に人材育成コンサルティングと情報セキュリティ教育プログラムの企画に従事．現在日本ユニシス・ラーニング(株)HRDコンサルティング営業本部に所属．