日本ユニシスグループにおける情報セキュリティ専門人材の育成

Developing Information Security Experts in Nihon Unisys Group

清　野　好　紀，吉　田　恵　美

要　約　企業において情報セキュリティを有効かつ継続的に機能させることは，企業価値を維持・向上させる意義がある．この目標を達成するためには判断力と専門知識を備えた情報セキュリティ専門人材が必要である．しかし企業における情報セキュリティという目標は，大規模であることと，技術要素が常に変化するという特徴を持っている．従って専門人材のスキルを定義し，計画的に育成しなければならない．日本ユニシスグループではシステムサービスを提供する企業として情報セキュリティ専門人材を計画的に育成している．このための施策として IT スキル標準に準拠した情報セキュリティスペシャリストの人材類型の定義，スキル調査，必要な研修の提供，技術認定制度といった仕組みを組み合わせ推進している．

Abstract　Making the information security function effective and continuous in the enterprise has the meaning to maintain and improve the corporate value. To achieve this target, information security specialists who have discretion and expertise are indispensable. However, the target of information security in the enterprise has the feature of large-scale and changing technological elements. It is, therefore, necessary to define their skills and to train them premeditatedly. Nihon Unisys Group systematically trains information security specialists as a systems service providing company. As a measure for this, combination of structures such as definition of security specialist types, skill investigation, offer of necessary training, and skill certification are promoted.

1. は　じ　め　に

各企業が日々の業務を行ううえで，各種情報システムを基盤としている今，これらの情報システムにおいてセキュリティ事故が発生することは，顧客への商品・サービスの継続的な提供を脅かすリスクとなっている．近年，事故が発生してから，対策が講じられ，顧客へのサービスの提供再開までの期間（場合によっては社会的責任の受容のプロセスを含む）が長期化する傾向があり，この間に被る損失は大変大きくなっている．従って，対症療法ではなく，事故を発生させない態勢をとることが重要である．ISMS（Information Security Management System）の構築やプライバシーマーク（P マーク）の取得といった態勢面を整えること，金融機関における生体認証の導入といった事例もその一つである．また逆に，情報セキュリティ体制を構築しマネジメントしていることを積極的にプレゼンテーションすることで情報セキュリティ上の安全性をアピールし，顧客からの支持や競争優位性の確立を狙うこともできる．ただし，近年は情報セキュリティ体制が整っていることが当然であり，体制が整っていないことによる競争劣後を甘んじないことしか価値のない場合もある．

企業において上記のような価値を持つ情報セキュリティを有効かつ継続的に機能させるためには，適切な判断力と専門知識を備えた情報セキュリティ専門人材の育成が必須である．しか

し一口に情報セキュリティ専門人材と言っても，その要員がカバーしなければいけない範囲は組織面からも縦に深く，技術面からも横に広い．かつ，顧客や社会から要求されるセキュリティ要件は年を追う毎に厳しくなり，技術上の要素も常に進化する．つまり情報セキュリティという目標は，規模も大きく，常に変化する特徴を持っている．

このような目標を追い続けるためには，「明確な戦略を描き，組織的に対応すること」，「情報セキュリティの管理プロセスのPDCAを定義し，そのレビューを続けていくこと」，「技術動向を追い，技術面をしっかり押さえていくこと」などを実現できる人材が必要となる．当然，これらの能力を単一類型の要員に求めることはできず，情報セキュリティ専門人材の類型，および，おのおのの類型に求められるスキルセットを定義し，計画的に育成・配置していかなければならない．

本稿では，情報セキュリティ専門人材の類型と，各々の類型に必要とされるスキルセットを，日本および国際的な資格制度と関連させながら整理することで，標準的なスキルセットの定義とその認定基準を明確にする．そして，日本ユニシスグループにおいてはどのような情報セキュリティ専門人材を定義しているのか，それらの育成プログラムをどのように考え・提供しているか，どのような認定制度を設け評価しているかを，それらに至った背景とともに解説する．

2. 情報セキュリティ専門人材とは

情報セキュリティがカバーする範囲は，組織マネジメントの観点，技術的な観点など非常に広い．また情報セキュリティに携わるのは情報セキュリティ専門人材にとどまらない．日々の業務を担う一般社員もその業務の範囲内において情報セキュリティに携わる．一般社員も含め，その担当する役割毎になすべき行動，または持つべきスキル・知識が異なる．役割については以下のように整理することができる．

1） 情報セキュリティ管理者
　自組織（企業，部門など）における情報セキュリティ対策を企画・立案・推進する
2） 情報セキュリティ監査者
　情報セキュリティ対策の有効性を検査・保証する
3） 情報セキュリティ技術者
　情報セキュリティシステムを提供する
4） 情報セキュリティ担当者（一般社員）
　自組織（企業，部門など）の業務において情報セキュリティ対策を実行する

なお，「情報セキュリティ技術そのものを研究・開発するもの」という人材類型もあり，暗号化技術の研究・開発，セキュリティプロトコルの研究・開発等の役割が期待されているが，本稿では対象外とする．

2.1 情報セキュリティ管理者

情報セキュリティ管理者とは，情報システムそのものをはじめ，機密情報や個人情報の管理など情報セキュリティ全般を統括管理する者をさす．セキュリティポリシーの設計，個人情報保護の方針策定，情報システムのセキュリティ対策の策定，リスク・マネジメント，企業情報の管理規定策定・漏洩防止などにつきそれらを統括管理することが求められている．

2.2　情報セキュリティ監査者

情報セキュリティ監査とは，企業・組織が推進している情報セキュリティ対策（マネジメント）が適切であるという保証を与えること，情報セキュリティ対策の改善に寄与する助言を行うことを目的としている．監査は情報システムに加え情報資産も対象とする．すなわち情報セキュリティ全般がその対象となる．また，監査は，情報セキュリティの強度を検証するのではなく，情報セキュリティマネジメントが正しく効果的に実施されているかを検証する．経済産業省が公表した「情報セキュリティ監査研究会報告書」では，情報セキュリティ監査を「情報セキュリティに係わるリスクのマネジメントが効果的に実施されるように，リスクアセスメントに基づく適切なコントロールの整備，運用状況を，情報セキュリティ監査人（情報セキュリティ監査を行う主体）が独立かつ専門的な立場から，国際的にも整合性の取れた基準に従って検証または評価し，もって保証を与えあるいは助言を行う活動」[1]としている．

2.3　情報セキュリティ技術者

情報セキュリティ技術者はそのサービス範囲から表１のようにいくつかの類型に分類することができる．

表１　情報セキュリティ技術者の類型と役割[2]

類型	役割
構築系技術者 （システム構築）	システムインテグレータ等でユーザの要望に従い，市販のパッケージソフトや通信機器などを組み合わせ一つのシステムとして完成させる業務に従事する技術者
開発系技術者	Web を活用した電子商取引のアプリケーションを開発するなどの課程において，要求定義，システム設計，機能設計，詳細設計，テスト仕様決定等の工程を担当する技術者
運用系技術者	ユーザ企業の情報システム部門において，提供されているサービス・機器を日常的に管理・運用することを主たる業務とする技術者
ポリシー構築系技術者	ユーザ企業やコンサルティング企業等で自社または顧客の情報セキュリティポリシーの策定，情報システムの利用における監査などを主業務とする技術者
脆弱性検査系技術者	システムインテグレータやコンサルティング企業等で顧客情報システムの脆弱性の検査等を行う技術者

2.4　情報セキュリティ担当者

情報セキュリティ担当者とは，業務の現場において各組織階層における情報セキュリティをリードする役割を担った者（リーダー），または一般職員・社員，さらには，派遣社員，パート，アルバイト要員をさす．正社員であるなしに関わらず情報セキュリティ担当者の一翼を担っていると考える．担当者は日々の具体的な情報セキュリティ活動を担う．表２は担当者が取り組む作業の項目の一覧である．現場担当者が理解し実施しなければいけない項目も多岐にわたることがわかる．

表 2　情報セキュリテイ担当者の役割[3]

情報セキュリティに対する組織的な取り組み 情報セキュリティポリシーの実践，情報資産の取り扱い，情報ライフサイクルにおける適切な措置，各種契約におけるセキュリティの考慮，採用，部門要員の具体的な育成
物理的セキュリティ 建物・施設におけるセキュリティ対策の遵守，入退出者管理，機器の災害対策，モバイル機器の管理
情報システム及び通信ネットワークの運用管理 情報システムの運用の保護実践，コンピュータウィルス対策の実践，利用者ID の適切な使用
情報セキュリティ上の事故対応 システム障害が発生した場合に対する対処の準備

しかし，担当者にとって情報セキュリティの維持・向上はその業務において留意すべきものであるが，オーバーヘッドともなる．従って，そのプロセスはなるべく自動的に軽量で遂行できるものであることが望ましい．ただし，最新のプロセスに従い主体的に取り組めるよう，意義のリマインドを反復・継続していくことも必要である．

3.　情報セキュリティ専門人材育成の重要性

情報セキュリティ管理者と情報セキュリティ監査者，情報セキュリティ技術者をあわせた人材を情報セキュリティ専門人材と呼ぶ．本章以降ではその育成に焦点を当てて述べる．

情報セキュリティ専門人材は，情報セキュリティを継続的に機能させるため，適切な判断力（人間力）と専門知識を備えていることが必要である．企業活動を進めていくうえで，いわゆる人・物・金という 3 大資産が重要であることにかわりはないが，近年これに加え情報も重要な資産とみなされている．情報はその性質上前述の 3 大資産にくらべ，より大きな脆弱性を抱えており，その脆弱性が現実の危機とならないよう機密性，完全性，可用性といった視点から保護する必要がある．当然，情報セキュリティは対策を施すほどそのためにかかる費用は上昇する．情報セキュリティを効率よく維持するためにも効果的な手法が必要であり，その目的で整備されたフレームワークが情報セキュリティマネジメントシステム ISMS と呼ばれるものである．ISMS においては PDCA サイクルに基づき，継続的に改善しつつ情報セキュリティを維持していく．従って，PDCA サイクルを適切に回すためにも情報セキュリティ管理者が必要とされる．IPA では情報セキュリティ管理者のスキルを表3のような枠組みで定義している．

表 3　情報セキュリテイ管理者のスキル抜粋[4]

1 マネジメント技術
2 リスク分析技術
3 情報セキュリティポリシー策定
4 情報セキュリティ監査
5 ファイアーウォール
6 関連知識

一方，情報セキュリティの技術的な側面からも専門人材の育成が必要となる．情報セキュリティ技術者は前述の表 1 であげたように役割の幅が広い．また，その情報技術も，取り扱う製品やプロトコル，サービスを提供する顧客の事業特性などによって異なり，深さが増す．さら

に必要とされる情報セキュリティ技術者として，企業においてセキュリティに関する製品や企画を専任に行う者以外に，顧客のシステムを構築するシステムエンジニアもその範囲に入ってくる．IPA では情報セキュリティ技術者に求められるスキルをスキルマップとして表 4 のような枠組みで定義している．個々の項目の詳細は省略する．

表 4　情報セキュリティ技術者のスキル抜粋[4]

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
4 OS セキュリティ
5 ファイアーウォール
6 侵入検知
7 ウィルス
8 セキュアプログラミング技法
9 セキュリティ運用
10 セキュリティプロトコル
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

4.　情報セキュリティ専門人材育成の難しさ

4.1　情報セキュリティ専門人材育成の現状

情報セキュリティ専門人材の育成の状況は，IPA の調査した「情報セキュリティプロフェッショナル育成に関する調査研究」[2]を簡単にまとめると次のようになる．要員についてはユーザ企業，ベンダー企業とも増加させる傾向にあるものの，需要に追いつかず不足感を感じている企業が多い．ベンダー企業などでは，情報セキュリティ専門人材の採用を予定し，直接の手当を検討している企業が半数となる．またベンダー企業，ユーザ企業ともに，「技術の変化が速く，要員の知識のレベルを保つのが難しい」ことをもっとも大きな課題としてあげている．さらに情報セキュリティ専門人材を育成するためのキャリアパスはユーザ企業のみならずベンダー企業でも非常に少ない．

4.2　情報セキュリティ専門人材育成の難しさ

情報セキュリティ専門人材に求められる能力には，広範囲な技術分野だけではなく，交渉力や判断力，経営知識，コンプライアンスの意識も含まれる．さらに，情報セキュリティ専門人材を育成することの直接的な投資対効果を把握することが難しいことも，情報セキュリティ専門人材の育成の難しさを増長させている．専門人材類型のうちでも，情報セキュリティ技術者の育成は，セキュリティ技術を取り込んだサービス・商品の売上と利益という可視化可能な評価尺度を持ちうるが，自組織の情報セキュリティを向上させるための投資については表 5 にあげるような評価の難しさが存在する．この情報セキュリティ投資の評価の難しさが，情報セキ

ュリティ管理者，情報セキュリティ監査者，情報セキュリティ担当者といった人材類型の育成を難しくしている．

表5　情報セキュリティ投資の判断の難しさ[5]

困難性	要素
IT 事故発生のリスクが明確でなく，適正な情報セキュリティ投資の判断が困難	・ 事故発生に経済的損失の計測が難しい ・ ステークホルダーからの信頼感喪失を予見しづらい ・ 想定したリスクに対する対策投資の判断基準がない
情報セキュリティ対策への取り組みと企業価値向上が直接リンクしない	・ トラブル未然防止という以上にリスク低減の効果が見えづらい ・ 企業戦略としての情報セキュリティの取り組みが差別化優位性を確保する一要素としか認知されていない
事業継続性確保の必要性が十分に認識されていない	・ 個々の事業形態・特性などを考慮した上で事業継続を確保することの必要性が十分に認知されていない

5.　情報セキュリティ専門人材の認定

5.1　認定制度の効果

育成の難しい情報セキュリティ専門人材であるが，国内外には専門人材のスキルを認定する資格制度が存在する．これらの資格制度ではおのおのの専門人材が保有するスキルセット（スキルの集合）が定義され，スキルセットの修得度などで認定が行われる．これらの資格認定制度を活用することで，表6にあげるような効果を得ることができる．

表6　認定制度を活用することの効果

効果	説明
保有スキルの客観的評価	認定制度では評価対象となるスキルセットを定義し，試験などによって保有するスキルの評価を行う．認定試験が一定の評価基準のもと行われることで，スキルレベルの客観的な評価を行うことができる．
保有スキルの棚卸し	認定制度の定義するスキルセットを参照することで，専門人材を目指す者が保有するスキルの過不足を検証することができる．
育成パスの設計	スキルセットを習得するための育成施策（研修・OJT・ローテーション等）を企画することができる．採用から任命にいたるキャリアの中において，いつどのようなスキルを習得させるべきかを検討する基準となる．
育成コストの可視化	専門人材にしたい人材が保有するスキルの現状と，目指す人材像のギャップを埋めるための育成施策が育成コストとなり，計画を立案しやすくなる．
育成投資の判断基準	可視化された育成コストと，事前に情報セキュリティが維持できなかった際のリスクアセスメントの結果を比較検証することで，育成投資を判断することができる．

5.2　認定制度の例

情報セキュリティに関する認定制度にはさまざまなものがある．大別すると，特定のソフトウェアプロダクトやハードウェアプロダクトによらない認定制度と，プロダクトごとに用意されたセキュリティ機能に関する認定制度になる．また日本国内で設計・開発され主として日本国内で通用する認定制度と，国際的に通用する認定制度に分けることもできる．表7から表9は特定のプロダクトによらない認定制度を人材類型（管理者，監査者，技術者）別に整理し，おのおのの認定制度が認定しようとしているスキルを整理したものである．

表7　国内/国外におけるプロダクトに依存しない情報セキュリティ認定制度の例（管理者）

人材類型	国内認定のスキル基準	国外認定のスキル基準
管理者	**情報処理技術者認定試験 情報セキュリティアドミニストレーター** 情報システムの企画，計画，構築，運用というシステムライフサイクルに対応して，情報セキュリティに関する企画，実施，運用，分析，見直しに関する業務に従事することになる．当技術者は，この基本的な業務において，物理的観点，人的観点および技術的観点から情報セキュリティを保つための施策を計画・実施し，その結果を評価する能力が求められる． （IPA 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より転記）[6]	CISM(Certified Information Security Manager) 企業等の情報セキュリティプログラムに係る，プロフェッショナル（セキュリティマネージャー，セキュリティ担当役員，セキュリティ担当役職者，セキュリティコンサルタント）を対象とし，五つの領域をカバーする． ・ 情報セキュリティガバナンス: 情報セキュリティ戦略がビジネス目標に合致し，適用される法規に適合していることを保証するためのフレームワークを確立し維持する． ・ リスクマネージメント: ビジネス目標を達成するために，情報セキュリティリスクを明確化し管理する． ・ 情報セキュリティプログラムマネージメント: 情報セキュリティガバナンスのフレームワークを実践する情報セキュリティプログラムを設計，開発及び管理する． ・ 情報セキュリティマネージメント: 情報セキュリティプログラムを遂行するための情報セキュリティ活動を監視及び監督する． ・ レスポンスマネージメント: 破壊的な情報セキュリティイベントへの対処と復旧の能力を開発及び管理する （情報システムコントロール協会東京支部 CISMより転記/編集）[7]

表８　国内/国外におけるプロダクトに依存しない情報セキュリティ認定制度の例（監査者）

人材類型	国内認定のスキル基準	国外認定のスキル基準
監査者	**情報処理技術者認定試験 システム監査技術者** システム監査技術者は，情報システムを総合的に点検・評価し，監査結果をトップマネジメントおよび関係者に説明し，改善点を勧告する，いわゆるシステム監査業務に従事することになる．当技術者には，監査計画を立案し，監査を実施し，監査結果をトップマネジメントおよび関係者に報告する能力が求められる．さらに，情報システムに関するコントロール機能の改善を促進し，その実効性を担保することによって，企業経営はもとより，情報社会・ネットワーク社会の健全化に貢献できる能力が求められる． （IPA 情報処理技術者試験 システム監査技術者 より転記）[8] **公認情報セキュリティ監査人** 情報セキュリティ監査制度に対する知識と経験を有するとともに，実証された能力として，監査計画を立案し，監査計画に基づいて監査を実施し，報告書を作成し，監査結果を被監査主体に報告する役割を行う．また，上位の監査人の指導のもとで，ＯＪＴとして監査チームリーダを務め，経験を積んで，公認情報セキュリティ主任監査人をめざすことができる．加えて，情報セキュリティ監査人補がＯＪＴとして監査に参加している場合は，これを指導し評価する． （日本セキュリティ監査協会 公認情報セキュリティ監査人より転記）[9]	CISA(Certified Information Systems Auditor) CISAは情報システムの監査および，セキュリティ，コントロールに関する高度な知識，技能と経験を有するプロフェッショナルとして認定する国際資格．六つの領域をカバーする． ・組織の情報技術および業務システムが適切にコントロール，モニター，評価されていることを確認するため，一般に受け入れられた情報システムの標準やガイドラインに従って情報システム監査を行うプロセスの評価． ・情報システムの管理，計画，組織に関わる戦略，方針，基準，手続，および関連する実践内容の評価． ・組織の業務目的を満たすことを確認するため，業務アプリケーション・システム開発，購入，導入，保守の方法論とそのプロセスについての評価．またリスクが組織の業務目的に従って管理されることを確認するため，業務システムとプロセスについての評価． ・組織の技術上，運営上のインフラが適切に組織の業務目的をサポートすることを確認するため，その導入および継続的管理の効果と効率の評価． ・情報資産が許可無しに使用，開示，変更されたり，損傷，損失を受けないように保護するための組織上の業務要件を満たすことを確認するため，論理的，環境上，およびITインフラ関連のセキュリティの評価． ・災害時の業務オペレーションと情報処理の継続に関する，文書化され，伝達され，テストされた計画を策定し維持するためのプロセスの評価． （情報システムコントロール協会東京支部 CISAより転記/編集）[10]

表 9　国内/国外におけるプロダクトに依存しない情報セキュリティ認定制度の例（技術者）

人材類型	国内認定のスキル基準	国外認定のスキル基準
技術者	**情報処理技術者認定試験 テクニカルエンジニア（情報セキュリティ）** テクニカルエンジニア（情報セキュリティ）は，情報システム基盤（業務システム共有のシステム資源）の構築・運用，個別の情報システムまたはセキュリティ機能の開発プロジェクトにおいて，情報セキュリティに関する脆弱性や脅威を分析・評価し，それらのリスクを回避・防止するため対象（情報システム基盤，情報システム，セキュリティ機能等）に求めるべきセキュリティ要件の定義，実装の計画から，設計，構築，移行，運用，維持管理までを推進または支援し，もしくはセキュアな開発プロジェクト環境の整備を含むプロジェクト管理を技術的側面から支援する能力が求められる． （IPA 情報処理技術者試験 テクニカルエンジニア 情報セキュリティより転記）[11]	CISSP（Certified Information Systems Security Professional） (ISC)2が認定を行っている国際的に認められた情報セキュリティ・プロフェッショナル認証資格．10個の領域をカバーする． ・ 情報セキュリティとリスクマネジメント ・ セキュリティアーキテクチャと設計 ・ アクセス制御 ・ アプリケーションセキュリティ ・ 運用セキュリティ ・ 暗号学 ・ 通信とネットワークのセキュリティ ・ 物理セキュリティ ・ 事業継続と災害復旧の計画 ・ 法・規則・コンプライアンス・捜査 （（ISC)2 より転記 ）[12]

これらの資格制度を活用するうえで重要なことは，資格取得と業務のアサインメントを連動させることである．後述するように日本ユニシスグループでは資格取得と社内の技術者認定をリンクさせている．資格を取得することが社内の技術者認定の認定基準となり，社内技術者認定で認定されることが，特定の業務へのアサインメントとつながっている．このことではじめて資格取得が活きてくる．また資格取得のコストの効果が計測できるようになる．

また，資格取得には資格取得時のコストだけではなく継続維持のコストもあることを認識しなければならない．特に国際的な資格制度は数年おきの資格更新申請が必要であり，この際，情報セキュリティの専門家としての業務経験や情報セキュリティに関する継続的な学習（研修受講や学会への出席など），情報セキュリティに関する貢献（論文執筆や学会活動など）を証明する必要があるものが多い．これらの更新活動をすることで実務的なスキルを維持できると考えるべきである．

6.　情報セキュリティ専門人材に求められるヒューマンスキル

情報セキュリティ専門人材に求められるのは，管理的・技術的な知識・スキルにとどまらない．多くの部門を動かし，企業としての情報セキュリティを維持していくためにはヒューマンスキルも重要となってくる．表 10 にあげたものは「情報セキュリティに携わる人材に求められるようになるスキル」として IPA の「情報セキュリティプロフェッショナル育成に関する調査研究」[2]に寄せられた回答の一部である．興味深いのは自己学習能力があげられていることである．情報セキュリティの技術革新は日進月歩であり，情報セキュリティ専門人材は常にアンテナを張り，技術動向に興味関心を持たなければならない．

表 10　情報セキュリティに携わる人材に求められるようになるスキル

コンサルティング能力	・ 情報システムの可用性とのバランスを図りながら，中期的なセキュリティレベルを維持するための方策を提案・実行できる能力 ・ 提案ができ，キーマンを説得することができる総合力 ・ ネットワーク全体を見て脆弱な箇所を指摘し，解決策を提案できる能力
インテグレーション能力	・ セキュリティ関連製品やサービスを組み合せ，最適なシステム構築することができる能力
自己学習能力	・ 技術革新の方向性への洞察力と先見性 ・ 常に発生する新しい脅威の把握と迅速な対応ができるスキルとその更新 ・ 最新の技術動向を幅広くつかみ，技術の変化を調査し，速やかに対応する能力
一般知識/ヒューマンスキル	・ 経営者を説得できる経営感覚ならびにコミュニケーションスキル ・ 人脈形成能力やビジネス知識を含むヒューマンスキル ・ コンプライアンスマインドの理解と実践

7.　日本ユニシスグループにおける情報セキュリティ人材の育成

日本ユニシスグループでは従来から会社の成長は人の成長により実現すると考えており，人材育成に積極的に投資してきた．人的資産の可視化を実現し，成長サイクルを促す仕組みつくりもその一つである．人的資産の可視化のフレームワークとして人材モデル（図 1）を定義し，プロフェッショナル人材のあるべき姿をその役割，求められるスキルと知識によって表現している．

人材モデルをベースとした日本ユニシスグループの人材育成のための仕組みは

- キャリアパスを実装する育成プログラム（研修ロードマップ）
- スキル調査
- 技術認定制度
- 目標設定制度

などの制度によって実現している．

人材モデルを軸に育成計画や個々人のキャリアデザインのベースとなるベーシックキャリアパスを示している．そのキャリアパスに合わせて育成プログラムを策定し，実施，運営をすることで技術者の育成を図っている．

スキル調査はシステム職の社員に対して毎年行っている．現在のスキル状況を自己評価して，保有するスキルの棚卸しを行い，スキルの保有状況，現在対応している人材モデルとそのレベル，職務履歴（業務実績），保有している各種資格などの現状を把握した上で，中長期の個々人の成長目標・組織としての育成目標を立てている．また，会社全体の人的資産を人材モ

図1　日本ユニシスグループ人材モデル

デルベースで可視化することでビジネス戦略，組織戦略へのインプットとして活用したり，優秀な専門人材の保有するスキルや経験などを分析して育成計画に活用している．

技術認定制度は人材モデルをベースとして専門技術者のレベルを認定し，実践を通じてさらに高いレベルの人材モデルに育成することを目的とした制度である．認定されることでプロフェッショナルとしての自覚を促し，後進の育成や技術の継承を行うと同時に，その高い技術力を証明された認定技術者が，高品質と高付加価値のサービスを提供することにより，グループ全体の競争力強化を狙っている．

これらの人材育成のための仕組み（成長サイクル）をベースとして社員の自立的な成長を支援している．個人は自身のキャリアをデザインする上で人材モデル毎レベル毎に定義されている必要な経験や知識，スキル，資格を具体的な中長期の目標とし，その目標レベルに到達するために必要となる知識，スキルを補完するために研修プログラムを受講することができる．

7.1　情報セキュリティ専門人材定義

社内の情報セキュリティ専門人材には，情報セキュリティ管理者，情報セキュリティ監査者，情報セキュリティ技術者がある．その中で情報セキュリティ技術者については，人材モデルのひとつとしてITスキル標準に準拠した「セキュリティスペシャリスト」を定義している．セキュリティスペシャリストは主に顧客向けのサービスデリバリーを行う役割をモデル化したものであり，前述の情報セキュリティ技術者の類型（表1）では，運用系技術者を除く，構築系技術者，開発系技術者，ポリシー構築系技術者，脆弱性検査系技術者にあたる．そのセキュリティスペシャリストを育成するための育成プログラム群とセキュリティスペシャリストの技術認定資格を設け，積極的にセキュリティ専門人材の育成を図っている．セキュリティスペシャリストのモデル定義を表11に示す．スペシャリストのレベル基準についてもITスキル標準に準拠した形で定義している．

表 11　日本ユニシスグループのセキュリティスペシャリストの定義

<table>
<tr><th></th><th>役割</th><th>スキル</th><th>知識</th></tr>
<tr><td>全般</td><td>専門技術を活用し，システム基盤に関する以下の作業を実施する．構築したシステム基盤の性能，回復性，可用性などに責任を持つ．</td><td>－</td><td rowspan="3">・ハードウェア，ソフトウェア，ネットワーク，データベースなど情報技術に関する全般的な知識
・ＯＳ，ネットワーク，インターネットに関する技術，製品（ハードウェア，ソフトウェア，サービス）セキュリティに関する国際動向（含むセキュリティ標準）
・情報セキュリティマネジメント
・アプリケーションセキュリティ
・ファイアーウォール
・ウイルス
・セキュリティ運用
・認証，PKI，電子署名，暗号
・不正アクセス手法
・ネットワークインフラセキュリティ
・OSセキュリティ
・侵入検知
・セキュアプログラミング技法
・セキュリティプロトコル
・セキュリティ関連法令・規格
・技術問題解決手法の活用・実践
・品質計画，品質保証，品質コントロール</td></tr>
<tr><td>マネジメント</td><td>情報セキュリティに関する体系的な基礎知識を持ち，セキュリティポリシー及びリスク対応に関する構築/実装/評価/見直しの支援業務を行う．</td><td>・顧客情報や情報システムなどの情報資産について体系的なリスクアセスメントを行い，課題の定義と対策の提案ができる．
・リスクアセスメント結果に基づいたセキュリティポリシーの策定ができる．</td></tr>
<tr><td>テクニカル</td><td>システムにおけるセキュリティ評価/設計を行う．</td><td>【インフラセキュリティ】
・ネットワークシステム全体の基本設計を基に，不正アクセス防止，情報漏洩防止などのためのインフラのセキュリティ設計を実施する．
【アプリケーションセキュリティ】
・アプリケーションの要求仕様書を基にセキュリティを考慮した詳細設計，機能設計を行い，アプリケーション開発を行うことができる．</td></tr>
</table>

日本ユニシスグループの人材モデル定義についてはITスキル標準に準拠しており，前述のIPAの情報セキュリティ技術者に求められるスキルマップを包含するように定義している．このセキュリティスペシャリストは主にシステム開発におけるサービスに従事する役割での定義である．社内の他の情報セキュリティ専門人材である情報セキュリティ管理者と情報セキュリティ監査者については人材定義していないが，社内専門組織にて情報セキュリティ管理者や情報セキュリティ監査者の役割を担い，その部署内で個別に育成をしている．

7.2　人材育成プログラム

日本ユニシスグループでは前述の人材モデルを軸にベーシックキャリアパスとして図2のようなパスを想定しており，そのパスにあわせた育成プログラムを用意している．

システム職は全員がシステム開発に必要となる広く体系的な知識を取得し，ソフトウェアエンジニアリングスペシャリストとして活躍することが期待されている．その段階で基本的なセキュリティの基礎知識・スキルを習得する．ソフトウェアエンジニアリングスペシャリストとしてプロジェクトの経験を積みスキルを定着させたうえで，数あるキャリアオプションの中から自身に合う人材モデルを選び高度専門人材としてキャリアアップしていく．ソフトウェアエンジニアリングスペシャリストとしての経験はどの高度専門人材を選んだ場合にもキャリアアップしていく際の糧として必要であると考えているためである．セキュリティのプロフェッショナルとしてのキャリアを積んでいく際にも段階的にセキュリティ関連スキルを取得できるように研修のロードマップを設計している．セキュリティ関連の育成プログラムとして表12に

図 2　ベーシックキャリアパス

表 12　研修コース一覧

	コース名	コース内容
新人研修	セキュアプログラミング入門	セキュアなプログラミング開発の学習
	コンピュータアーキテクチャ	コンピュータの仕組みの理解
若年層	システム基盤基礎（ネットワーク・セキュリティ）	・システム構築設計を担当する若手エンジニアが基盤関連技術を体系立てて習得 ・セキュリティ・運用・性能・可用性などの基盤要件の目的と解決策について学習し，ITアーキテクチャ構築の勘所を押さえる
	Webアプリケーションセキュリティ基礎	Webアプリケーション開発時に適用する具体的なセキュリティ対策の学習
	情報セキュリティ技術者育成　セキュリティ基礎技術	セキュリティに関する基礎知識全般を習得
	情報セキュリティ技術者育成　セキュリティテクノロジー編	セキュリティスペシャリストに必要なテクニカルスキルをPCを使った実習で学ぶ
中堅～専門人材	情報セキュリティ　監査	情報セキュリティの監査と検証，ITセキュリティ評価についてワークショップを通して習得
	セキュリティ　レビュア	セキュリティレビューで使用するチェックシート（基盤，ＡＰ）の解説を行い，システム開発におけるセキュリティ実装のポイントを習得
	セキュリティ　要件定義ワークショップ	セキュリティ要件定義に関する実践的スキルの修得
ビジネススキル	コミュニケーション	サービスマインドの醸成とそのマインドに基づくコミュニケーションスキルの習得
	交渉力基礎	SEがシステム開発業務で日常に直面する顧客との交渉ケースを題材に，理論とロール・プレイングにより交渉スキルを体得する
	クリエイティブシンキング	柔軟に新たなコンセプトを創出する方法論習得と実践を目指す 習得する能力：創造的思考力
	ロジカルシンキング	ビジネスパーソンが成果をあげるために不可欠な，論理的に考える力，伝える力の習得を図る
	ファシリテーション基礎	企業変革におけるファシリテータの役割と重要性についての認識を深め，チームを生産的にするための具体的スキルを習得

あげる研修コースを用意している．新人～若年層，中堅～専門人材にキャリアアップしていく過程で，その段階での役割に必要なスキル，その後のキャリアアップで必要となるスキルを習得できるようにコースカリキュラムを組んでいる．

これらの研修を受講することで段階的にセキュリティ関連スキルを習得することができる．また，技術系の研修を受講するのと平行してビジネススキル研修もあわせて受講していくことにより総合的なスキルアップを図っている．さらにセキュリティ専門研修を受講することでセキュリティスペシャリストへのキャリアアップの支援をしている．監査者については研修ロードマップ上に専門の体系を持っていないが，ISMS のトレーニングを使って育成を図っている．

7.3　技術認定制度

日本ユニシスグループの技術認定制度の目的はプロジェクトの品質を保証することであり，定められた基準に照らして技術者を認定している．技術者は認定を取得することで自らの成長の目標を設定し，実感することで自立的にさらに高いレベルの技術者を目指せるような成長サイクルを廻すための重要な位置づけでもある．

セキュリティスペシャリストの認定資格については，担当したプロジェクトの実績について図 3 の難易度分類判定によりレベル判定を行っている．

認定についてはスキル調査結果でのスキルの保有状況，実績の証跡に加えて複数の有識者による面談で判定される．また，認定にあたっては CISSP など前述の外部資格を保持している必要がある．情報セキュリティ専門人材として必須となっているセキュリティ関連専門知識については前述のスキル調査結果でのスキル熟達度に加えて社外資格を保持していることで保証している．

プロジェクト難易度 ＼ 要因		易			新しくアサインされるプロジェクトのプロファイル					難
	10	9	8	7	6	5	4	3	2	1
役割として貢献したプロジェクト範囲のピーク時総人数	該当しない場合は10点で評価	nn 人	nn 人	nn 人	nn 人	nn 人	nn 人	nn人以上	nn 人以上	nn 人以上
・ネットワークSPの場合の規模		mm 拠点	mm 拠点	mm 拠点	mm 拠点	mm 拠点	mm 拠点	mm 拠点	mm 拠点	mm 拠点以上
・セキュリティSPでセキュリティビジネス単体の場合の規模（一人当たりの売上）		yy 万円	yy 万円	yy 万円	yy 万円	yy 万円	yy 万円	yy 万円	yy 万円	yy 万円以上
役割（職務責任）		要求定義、論理設計、物理設計、評価の工程において部分工程の技術的責任を担う			要求定義、論理設計、物理設計、開発の工程において全体的な技術的責任を担う			システム開発全工程に対し顧客と協同し開発チームを技術的側面で指導、指揮する役割を担う		
当社としてのソリューション難度		・手慣れたソリューション 当社で5回以上の同種のAP開発経験（同一プラットフォーム、プロダクトで5回以上の基盤システム開発）			・手慣れていないソリューション 当社で5回未満の同種のAP開発経験（新しいプラットフォーム、プロダクトでの基盤システム開発）			・未経験でミッションクリティカル又は複雑なソリューション 当社が過去に経験したことのない、又は前例からは極めて実現性の低い開発		
利害関係をもつステークホルダ数		担当作業を実施する際に利害関連を持ち、交渉・調整を要するステークホルダ数 <zz		zz≦	担当作業を実施する際に利害関連を持ち、交渉・調整を要するステークホルダ数 zz≦	zz≦	zz≦	担当作業を実施する際に利害関連を持ち、交渉・調整を要するステークホルダ数 zz≦		
対象分野リスク		・明瞭な要求定義 ・定まった技術／プロダクト			・部分的に不明瞭な要求定義 ・経験の少ない技術／プロダクト			・不明瞭な要求定義 ・未経験の最先端技術／プロダクト		
タイムスケール		全期0.5～1年程度で、且つコンテンジェンシ修復期間を含めた担当工程計画が認められている			全期1～1.5年程度の中で、タイトな工程 計画があり、且つコンテンジェンシ 修復期間が工程の15%以下			全期1.5年程度以上の中で、工程別の厳しい納期が決められており、且つコンテンジェンシ修復期間が工程の15%以上		
・セキュリティSPで セキュリティビジネス 単体の場合		十分な時間内での作業			緊急性が高く、タイトな期間での作業			緊急性が非常に高く、非常にタイトな期間での作業		

図 3　セキュリティスペシャリスト　技術認定のクライテリア

この技術認定は，システム開発のプロジェクト内でセキュリティ分野を担当してプロジェクトを成功裡に遂行した場合か，セキュリティ関連のコンサルティングやアセスメント，セキュリ

ティ対策などのセキュリティ単体ビジネスを担当した場合のどちらでも受けることができる．

システム開発プロジェクトでセキュリティ分野を担当した場合には，他のモデルと同様にプロジェクトのサイズや難易度などのプロジェクトプロファイルによりプロジェクトの難易度を判定する．セキュリティ単体ビジネスを担当した場合にはその売り上げ金額に応じて難易度を判定し，タイムスケールにおいても独自の視点での判定を用いている．セキュリティ対策や問題対応などのセキュリティ単体ビジネスにおいては緊急な案件が多く，非常に短時間での解決が求められ，その制約が難易度を上げているためである．また，監査者など実績の証跡が難易度分類判定の基準で判断することが難しい場合にも面談によって認定を受けることができる．

8. おわりに

情報セキュリティ専門人材について必要とされるスキルセットを整理し，その育成への日本ユニシスグループの取り組みについて紹介してきたが，現実は非常に難しい．情報セキュリティ専門人材に求められる知識・スキルは広範囲にわたるだけでなく，その技術革新のスピードは非常に速いため，あっという間に新しい技術に塗り替えられていく．技術者は常に新しい技術を追いかけ，自身の知識・スキルに磨きをかけていく必要がある．

今日，企業は経営目標実現のためにITの利用はもはや必須である．社会的責任を全うしていくために企業をとりまくIT環境に対して適切に対応していかなければならない．とりわけセキュリティの確保は必要不可欠である．そのためには情報セキュリティ専門人材の確保が重要な要因ともなっている．

情報セキュリティ専門人材の確保のためには人材育成の枠組みとしてセキュリティ人材モデル定義，資格，育成プログラムなど，トータルな育成の仕組み，育成プランが必要となる．企業として情報セキュリティ専門人材育成については個人の努力に頼り任せるのではなく，個人が成長できる環境，仕組み（評価/認定を含む）を提供していくことが重要である．

参考文献
［1］ 情報セキュリティ監査研究会 報告書，経済産業省，2003年3月，14ページ
［2］ 情報セキュリティプロフェッショナル育成に関する調査研究書，独立行政法人情報処理推進機構，2003年3月，20-37ページ，199-204ページ
［3］ 情報セキュリティ対策ベンチマークの質問一覧，独立行政法人情報処理推進機構，http://www.ipa.go.jp/security/benchmark/documents/BMVer.3_Questions.doc
［4］ 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年3月，20-22ページ
［5］ 企業における情報セキュリティガバナンスのあり方に関する研究会報告書，経済産業省，2007年3月，10-11ページ
［6］ 情報セキュリティアドミニストレーター試験HP，独立行政法人情報処理推進機構，http://www.jitec.ipa.go.jp/1_11seido/h13/su.html
［7］ CISM HP，情報システムコントロール協会東京支部，http://www.isaca.gr.jp/cism/
［8］ システム監査技術者試験HP，独立行政法人情報処理推進機構，http://www.jitec.ipa.go.jp/1_11seido/h13/au.html
［9］ 公認情報セキュリティ監査人HP，日本セキュリティ監査協会，http://www.jasa.jp/qualification/seido.html
［10］ CISA HP，情報システムコントロール協会東京支部，http://www.isaca.gr.jp/cisa/
［11］ テクニカルエンジニア試験HP，独立行政法人情報処理推進機構，http://www.jitec.ipa.go.jp/1_11seido/h13/sv.html

［12］ CISSP HP，（ISC）2 Japan，
https://www.isc2.org/japan/what_domain.html
［13］ 村上　拓史，「日本ユニシスのプロフェッショナル認定制度」，ユニシス技報，日本ユニシス，Vol.26 No.3 通巻 91 号，2007 年 2 月
［14］ 吉田　恵美，「人材モデルによる人的資産可視化と人材育成指針の提供」，ユニシス技報，日本ユニシス，Vol.26 No.3 通巻 91 号，2007 年 2 月

執筆者紹介　清　野　好　紀（Yoshinori Kiyono）
1987 年日本ユニシス（株）入社．総合教育部において主に顧客向け情報処理教育を担当．ホストシステム教育，Web 系教育を担当．その後，日本ユニシスグループ向け人材育成，顧客向け人材育成の企画・開発・推進に取り組む．現在，日本ユニシス・ラーニング（株）HRD 価値提供事業部長．エデュケーションプランナー．

吉　田　恵　美（Emi Yoshida）
1989 年日本ユニシス（株）入社．メインフレームで稼働するオンラインミドルウェアシステムの開発に従事．2003 年より日本ユニシスグループの人材モデル主管，システム職群向け社内教育サービスの企画・推進を担当．現在，日本ユニシス・ラーニング（株）HRD 価値提供事業部 システム研修グループ マネージャ．エデュケーションプランナー．