論　文

情報セキュリティに関する人材育成と professional のための国際規格の開発
Human Resource Development and International Standard Development of Professional for Information Security

杉　野　　隆
Takashi Sugino

要旨：組織における情報セキュリティの確保は経営における必須の要件となっている。情報セキュリティを確保するためには，情報セキュリティ技術の導入・構築だけでなく，それらを運用するための管理体制（management system）の整備，実施，そして人材の育成が不可欠である。本稿では，①情報セキュリティの現状，②情報セキュリティ関連資格の現状と最近の動き，③情報セキュリティ専門家人材の育成の重要性，③Information security management systems professional（ISMS–P）に関する ISO 規格策定の背景，開発状況などを紹介する。最後に，現状での課題について若干の考察を行う。

1. はじめに

筆者は1982年以来，情報処理技術者試験の作成委員を務めてきた。途中短い中断もあったが，現在も務めている。1969年からの48年間の社会人生活の 7 割の期間を試験委員としても過ごしたことになる。特に，2001年秋に開始された情報セキュリティアドミニストレータ（SU）試験からは，情報セキュリティ関連の三つの試験の制度設計，カリキュラム作成，試験問題作成に関わってきた。また，2012年からは，ISO/IEC JTC1/SC27 WG1 にエキスパートとして加わり，情報セキュリティ人材関連の国際規格の作成[1]に携わっている。本論文では，その間の仕事を省み，情報セキュリティ人材育成の今後の在り方について考察してみたい。

2. 情報セキュリティインシデントの深刻化

サイバー攻撃が巧妙化し，これによる情報漏えい事件が発生するたびに，組織における内部不正，組織運営のガバナンスの欠如，組織要員の不注意などが原因として指摘される。特に最近多発している標的型攻撃は，人間の行動心理の弱点に付け込んでウイルスを PC に送り込み，被害を拡大させるという特徴を持つ。図 1 に，社会に大きな影響を与えたサイバー攻撃の最近の事例を示す。

最近問題になっているランサムウェアは，メール添付ファイルまたは Web サイトを感染ルートとして被害者の PC にウイルスを送り込み，PC 内のファイルを勝手に暗号化するなどして PC を利用できなくし，金銭（身の代金）と引き換えにその暗号鍵を提供するいう攻撃である。重要ファイルを暗号化し，いわば，それを人質として金銭を要求するという手口である[2]。2013年から海外では発生していたが，2014年12月には，初めて日本語でメッセージが表示されるランサムウェアが確認された。Word や Excel など

国士舘大学21世紀アジア学部
School of Asia 21, Kokushikan University

[1] ISO 規格は著作権によって保護されている。本規格は現在まだ開発中であり，国際規格 IS として公表されていないが，現在審議中の規格案も同様に保護対象とされている。本稿では，Clause/Sub-clause（章，節に相当）までを紹介する。

- エストニア政府機関などへの DDoS 攻撃(2007 年 4-5 月）
- ジョージア政府機関と重要インフラへの DDoS 攻撃(2008 年 8 月）
- イランのプシュール原発の制御システムへの標的型攻撃（2010 年 6 月）
- 三菱重工業での情報収集型ウイルスへの感染（2011 年 8 月）
- 衆議院・参議院への標的型攻撃(2011 年 11 月）
- ロンドンオリンピック大会期間中にサイバー攻撃（2012 年 7-8 月）
- 韓国重要インフラへの標的型攻撃(2013 年 4 月）
- 米国 Sony Pictures Entertainment へのサイバー攻撃(2014 年 11 月）
- フランス TV5 モンド（2015 年 4 月）
- 日本年金機構への標的型メール攻撃（2015 年 5 月）
- 米国人事管理局（2015 年 6 月上旬）
- ウクライナ電力システムのマルウェア感染により大規模停電（2015 年 12 月）
- JTB 子会社への標的型攻撃(2016 年 6 月）

図 1　最近のサイバー攻撃の事例

の文書ファイル，画像や動画ファイルなどが対象とされる。トレンドマイクロの調査[3]によると，ランサムウェアの被害に遭い，攻撃者から金銭を払えば暗号化されたファイル（データ）を復旧すると言われた場合に，金銭を支払うと回答した241名（回答者総数534名の45.2％）を対象に，金銭を支払う理由を聞いた（複数回答）ところ，「業務が滞ってしまうから」を69.3％が選択し，続いて「自社では暗号されたファイル（データ）を復旧できないから」と回答した人が61.4％いた。ランサムウェアによる攻撃者から見れば，人間の心理に付け込んだこの成功率の高さが，さらに犯罪を繰り返させているわけである。

企業で使用される PC，いわゆる業務用 PC は，多くの場合に情報セキュリティ部門が十分な情報セキュリティ対策を講じた後に各部門に配布されて従業員の使用が許可される。しかし，このように情報セキュリティ対策を講じた PC は，その反面使いづらいものになってしまい，情報セキュリティ部門以外の一般利用者からは，より使いやすい（対策を一部緩和した）PC 環境を求められる。また，標的型攻撃などでは，利用者の業務シーンに合わせた巧妙なメールを送りつけるので，利用者は疑うことなくメールを開き添付ファイルを開封してしまう仕儀となる。そのため，業務用 PC のウイルス感染を完全には防げない。情報セキュリティ対策としては，感染をいかに早く検知し，組織内で感染情報を共有し，情報流出という損害を最小化するか，どのような再発防止策を講じるか，利用者の「これはどこかおかしい。誰かに相談しよう。」という情報セキュリティ意識をどのようにして向上させるかなどが課題になってくる。2015年 6 月に公表された日本年金機構における情報漏えい事件は典型的な事例である。

また，組織の従業員が顧客情報を不正に持ち出し，外部に売却することによって取引先の個人情報が大量に漏えいしたり，製品情報が従業員の退職時に不正に持ち出されたことによって，技術情報が競合企業に漏えいするといった事例が多発している。自宅で業務を行うために社内情報を無断で持ち出し，自宅 PC で仕事をしているときにウイルスに感染し，業務で使用中のファイルをアップロードされてしまうことによって持ち出されてしまうといった例もみられる。

---

[2] 金銭の要求メッセージなどを日本語で表示する Crypto ランサムウェアは，2014年 3 月，12月に確認されている。
[3] トレンドマイクロ企業におけるランサムウェア実態調査2016，http://www.trendmicro.co.jp/jp/about-us/press-releases/articles/20160727064652.html

情報セキュリティ対策には，物理的対策，技術的対策，人的・組織的対策があるが，サイバー攻撃や内部不正に対しては，物理的対策や技術的対策のみでは限界があり，人的・組織的対策が不可欠である。

3. 情報セキュリティの重要性

現在では，情報セキュリティの重要性を云々する者はいないほど当然視されているが，社会的に認識されるようになったのは，『現代用語の基礎知識』1982年版の新語話題コーナーで用語「セキュリティー」が紹介されたころからではないか。もっとも，このコーナーでは,「安全。安全保障。戸締り。防犯設備。防犯。安心感。」と説明しており，コンピュータ，ネットワーク，情報化社会などとの関連にはまだ触れられていない。すでにこの頃には，銀行の CD や ATM が利用されはじめ，オンラインシステムによる不正送金[4]，コンピュータウイルスが In the wild で活動を始めていたのだが。ちなみに，『広辞苑』第四版（1991年出版）には「セキュリティ」という用語はなく，第五版（1998年出版）になっても，「①安全，保安，防犯，②担保，③証券」と説明されている。この説明は，『現代用語の基礎知識』1982年版と同じである。第六版（2008年出版）になって，ようやく「セキュリティー」の用例として,「セキュリティー－ホール」（コンピューターシステムやネットワークの安全機能上の欠陥のこと）が載った。

2000年 1–2 月には，中央省庁で Web サイトが不正アクセスされ，Web ページが軒並み改ざんされるという事件が発生した[5]。これが日本社会における情報セキュリティの重要性への目覚めであり，国を挙げての情報セキュリティ対策の出発点であった。情報処理技術者試験に SU 試験が開始されたのは翌年の2001年10月であった。

2014年11月に「サイバーセキュリティ基本法」が成立した。この法律は，サイバーセキュリティの確保は国の責務であると明記し，2005年に設置された「内閣官房情報セキュリティセンター」を「内閣サイバーセキュリティセンター」[6]（NISC）に改組し，省庁を横断する司令塔と位置づけ，サイバー攻撃に対抗するために機能，権限，要員を強化した[7]。この法律では，サイバーセキュリティは「情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置が講じられ，その状態が適切に維持管理されていること」（第二条を一部簡略化した。）と定義された。サイバーセキュリティが対象とする情報は,「電子的方式，磁気的方式その他人の知覚によっては認識することができない方式（以下この条において「電磁的方式」という。）により記録され，又は発信され，伝送され，若しくは受信される情報」に限定されている。米国では，2008年 1 月に公表された「The Comprehensive National Cybersecurity Initiative」以来，cybersecurity に統一され，日本でも2013年 6 月のサイバーセキュリティ戦略発表以

---

[4] 1981年 9 月に，三和銀行の行員がオンラインシステムを利用し，1 億3000万円を不正送金して逮捕された。

[5] 2001年 1 月23日に大阪で開催された南京大虐殺を否定する集会への反発が引き金になったのではないかといわれている。

[6] 2000年 1 月～2 月に中央官庁や政府機関を襲った一連の Web 改ざん事件をきっかけに，同年 2 月末に内閣安全保障・危機管理室に内閣官房情報セキュリティ対策推進室が設置され，2005 年 4 月に内閣官房情報セキュリティセンター（旧 NISC）に改組された。しかし，エストニア，グルジア，米韓各政府，日本では竹島問題に対する島根県庁などへの DDoS 攻撃への対処を巡って，サイバー攻撃への対策強化が要請されていた。

[7] 具体的な成果として，2015年 5 月に発生した日本年金機構における情報漏えいインシデントが挙げられる。日本年金機構の PC のウイルス感染が NISC によって確認された際に，PC からのデータ送信の異常に気付き，機構側に通報した。もっとも，通報を受けた機構側の対応がずさんだったため被害が拡大し，約125万件の情報が流出する結果となった。

来，「情報セキュリティ」は「サイバーセキュリティ」に切り替えられた。

情報セキュリティの対象は情報資産であり，アナログ情報（例えば，紙に書かれた情報），ディジタル情報（基本法に「電磁的方式」と表現された情報）の両方とされているが，この法律の対象はディジタル情報に限定されてしまった。狙いは，サイバー空間への脅威を排除し，サイバー空間の安全と秩序（＝持続性）を確保し，人命及び財産を保護することである。実際には，Internet を含む情報通信ネットワーク，ネットワーク設備，計算機室，ルータ，サーバなどのいわゆる ICT システムが物理的に存在するし，それらを運用管理する実空間なしではサイバー空間もあり得ず，両空間は連接・一体化[8] して運営，利用されている。両空間の安全性，強靭性も一体として確保する必要があるのだから，本法におけるサイバーセキュリティの定義は問題があると言わざるを得ない。以下では，サイバーセキュリティも包含して情報セキュリティとして論じる。

4.　情報セキュリティ人材の育成

情報セキュリティ分野で最も不足しているものは人材であるといわれる。情報セキュリティ人材には，様々な分野（職種）が含まれる。

4.1　情報セキュリティ関連の人材の分類

組織の情報セキュリティの劣化を防止し，向上させるためには情報セキュリティ関連の人材の充実が欠かせない。ユーザ企業の場合を考えても，次のように様々な人材が必要とされる。

①最高情報セキュリティ責任者（Chief information security officer ; CISO）

組織の経営陣が提示する経営目標と組織のもつリスクを整合して，情報セキュリティ部門の目標を具体化し，部門の活動を指揮する。

②情報セキュリティ管理者（Information security manager）

組織目標と整合した情報セキュリティ対策を企画・立案・推進する。

③情報セキュリティ監査者（Information security auditor）

組織内において，情報セキュリティ対策の有効性を検査・保証する。

④情報セキュリティ技術者（Information security engineer）

組織の情報セキュリティシステムを企画，開発，運用する。

データベース，ネットワーク，Web システムなどに細分化されている。

⑤情報セキュリティ担当者

組織（企業，部門など）の情報セキュリティ対策を業務として実行する。

⑥一般従業員（管理者も含む）

情報セキュリティ部門に限らず，情報システムの利用者として，それぞれの業務を通して情報セキュリティ対策を実行する。

⑦情報セキュリティコンサルタント

組織内で充足できない力量を業務委託する。

---

[8] 情報セキュリティ政策会議サイバーセキュリティ2014，2014年 7 月

⑧情報セキュリティ運用管理

組織の情報セキュリティ管理システムを業務として実施する。また，通常のトラブル対応を行う。

⑨Computer Security Incident Response Team（CSIRT）

最近は，コンピュータセキュリティインシデントに関する報告を受け取り，調査し，対応することに責任を持つ組織体（ISO/IEC 27035:2011）が，定常組織あるいは臨時組織として設置されることが多い。ISIRT ともいわれる。ウイルス感染や不正アクセス，DoS 攻撃など情報セキュリティに対する脅威となる事象が発生した際に，組織内の対応窓口となって，あるいは外部の CSIRT と連携して，被害の拡大防止や関連情報の収集・告知，再発防止策の策定などの活動を行う。

本稿では，①～⑤，⑦，⑨を情報セキュリティ人材と呼ぶ。企業における情報セキュリティ人材（①～⑤）の不足が深刻化している。総務省系の「情報通信ソフト懇談会」が2003年に行った報告では，産業界において，情報セキュリティ分野の専門的な人材は約12万人不足している。中でも，特に高度な専門性を持った人材の不足は約 9 万人に上ると発表した[9]。2012年には IPA が，情報セキュリティ技術者は約26.5万人いるが，内16万人はスキル不足であり，実質 8 万人ほどの技術者が不足していると発表した[3][10]。情報セキュリティ状況がさらに厳しくなったこともあり，9 年経っても人手不足の実態は緩和されていないことが分かる。

情報セキュリティ技術者をどのようにして増加させるか。従来は高給与を提示することによって情報技術者を採用できると考えてきたが，情報セキュリティ技術者の場合には，そうもいかない。そもそもスキルを持った技術者そのものが不足しているからである。

5. 情報セキュリティ関連資格

5.1 資格の重要性，役割

ある人が特定の職業・任務・地位などに就くために必要な条件を資格という。この条件を客観的に評価可能な尺度によって表現するために，力量 competence という概念が用いられる。当該者の力量を第三者として評価する仕組みを認証（certification）という。また，組織における要員の新規採用，組織内での昇格，配置転換，教育機関からの卒業・修了の判定などに当たって，必要な力量を満たしているかを評価するための基準（qualification）としても資格は役立つ。

情報社会においては，様々な職業，業務の遂行に当たって情報通信技術（ICT）が必要とされる。しかも ICT の進歩が速いので，一般の利用者，ユーザ企業にはなかなか使いこなせない。その速度に対応するために新たな ICT（例えば，情報セキュリティ技術）に対応した資格として募集したい職種を特定し，（多くの技術者がその資格試験を受験して，自らの技術力を保証してくれていれば）その資格を取得した人材を採用することによって，人材育成もスピードアップでき，必要な ICT 要員を充足できる。また，充足している企業から不足している企業への転職という形で，技術者の流動性も確保される。これが，情報社会における資格の必要性の背景であろう。ICT 分野では官民を問わず，国内外を問わず，多種の資

[9] 情報通信ソフト懇談会　人材育成ワーキンググループ中間報告書，2003年
[10] IPA 情報セキュリティ人材の育成に関する基礎調査報告書，2012年

格が開発され，資格認定のための試験が実施されている。例えば，EU では，技術者を必要としている西欧と技術者が不足している東欧の間での技術者の流動性を確保するために，200以上の職種に関して 8 つのレベルに分類した欧州資格枠組み（European Qualifications Framework: EQF）開発し，運用している。その中でも ICT 関連では，さらに詳細化した e–QF と呼ぶ資格を2008年 4 月に発表している。

5.2　日本における情報セキュリティ関連資格

日本国内のみで実施されている ICT 関連資格試験には，ベンダ中立試験も各種あるが，IPA が国家能力認定試験[11] として実施している情報処理技術者試験が中心を占めている。情報セキュリティ関連の資格試験としては，2001年にマネジメントや運用に主眼を置いた「情報セキュリティアドミニストレータ試験」（SU 試験）が，2006年に情報セキュリティシステムの開発技術に主眼を置いた「テクニカルエンジニア（情報セキュリティ）試験」（SV 試験）が創設された。2009年には SU と SV 試験を統合し，「情報セキュリティスペシャリスト試験」（SC 試験）が創設された。これまでの 3 試験はベンダまたはユーザ企業の情報セキュリティ部門を対象にしてきたが，2016年には，組織における情報システムの利用部門にいる情報セキュリティリーダを対象とした「情報セキュリティマネジメント（SG）試験」が創設された。SC 試験のスキル熟達度（レベル 1～7）はレベル 4，SG 試験ではレベル 2 に設定されている[12]。

5.3　情報セキュリティ関連資格の実態

資格認定試験は，試験実施主体の背景によって，ベンダ資格試験，ベンダ中立資格試験，国家資格（能力認定）試験に分類される。また，実施地域によって，国内でのみの試験と，日本を含め世界中で実施する試験に分けられる。表 1 に主な情報セキュリティ関連の資格認定試験の名称を挙げた。

その他，例えば富士通（セキュリティマイスター認定制度）といった，ベンダ・ベンダ関連企業の技術者に対象を限定して資格を認定する試験もある。

世界中で実施されている資格認定試験の中では，米国の（ISC）2 が実施する Certified Information Systems Security Professional（CISSP）が最大の資格保有者数を誇るが，日本には1,600名ほどしかいない（表 2）。

世界的にみると，CISSP のシェアが非常に大きい。CISSP は登録制であるので，資格を更新しなかった者は資格保有者数にカウントされない。情報処理技術者と同様に CISSP も合格者数でカウントすれば，数字はもっと大きくなるはずである。情報処理技術者試験の SU 試験，SV 試験，SC 試験の合計合格者数73,901人（2016年秋試験合格発表まで）も引けを取らない数字である。しかし，情報処理技術試

---

[11] IPA が実施している情報処理技術者試験は，資格試験ではなく，受験時点における受験者の能力を認定する能力認定試験である。資格試験であれば，その質を保証するために，資格を期限付きで登録し，資格更新のためには別途手続きが必要となる。2016年10月に後述する情報処理安全確保支援士が創設されたが，これは情報処理術者試験とは別体系を取る資格試験である。

[12] 2002年12月に発表された IT スキル標準（ITSS）V1 は，職種を13，専門分野を25に分け，スキル達成度を 7 段階に区分して，技術者の能力を評価している。ITSS は2006年 4 月に V2，2008年 3 月に V3 と改定され，この段階で情報処理技術者試験との対応を明確にした。V3 では，11職種，35専門分野にわたって IT スキルを定義している。2008年10月には，共通キャリア・スキル・フレームワーク（CCSF）を通して，UISS（ユーザ企業技術者対象），ETSS（組み込み系技術者対象）ともリンクされた。

表 1　主な情報セキュリティ資格認定試験

地　域	資格区分	資 格 認 定 試 験 名
日本のみ	ベンダ中立資格	情報セキュリティ管理士認定試験
		情報セキュリティ初級認定試験
	国家能力認定	情報セキュリティスペシャリスト
		情報セキュリティマネジメント試験
	国家資格	情報処理安全確保支援士
日本含む世界中	ベンダ資格	Symantec Certified Specialist（SCS）
		Symantec Certified Professional Program（SCP）
	ベンダ中立資格	（ISC）2[13] Certified Information Systems Security Professional（CISSP）
		ISACA[14] Certified Information Systems Auditor（CISA）
		ISACA Certified Information Security Manager（CISM）
		ISACA Cybersecurity Nexus（CSX）Specialist
		SANS GIAC Certified Incident Handler（GCIH）

表 2　世界の CISSP[15]

国　　名	資格保有者数
日本	1,595
米国	72,685
韓国	2,674
シンガポール	1,428
オーストラリア	1,470
世界	110,980

注　2016年11月16日現在

験は国家試験であり，日本では強い信頼感を持っているため，これらの試験の CISSP に対する比較優位は崩れていない。

5.4　日本における情報セキュリティ関連資格の問題点

5.3で述べたように，日本における情報セキュリティ関連資格において情報処理技術者試験の占める比重は非常に大きい。しかし，情報処理技術者試験は能力認定試験であり，資格試験ではなく，技術者の現在の能力を保証するものではない。SC 試験を含め高度試験において，試験合格後の質保証のためのフォロー（資格登録制，継続研鑽，更新制）が義務付けられていない。倫理規定も制定されていない（図 2）。最新の動向を踏まえて専門的な力量が維持されているかを確認できないなどの共通の課題を抱えている。

[13] International Information Systems Security Certification Consortium
[14] 元は，Information Systems Audit and Control Association として商号を登録していたが，現在は ISACA に変更している。
[15] https://www.isc2.org/japan/

登録制（Registration）
継続研鑽（Continuing Professional Development；CPD）
更新制（Renewal of certification）
倫理規定の遵守（Code of conduct）
プロフェッショナルコミュニティの形成（Professional community）

図2　資格試験の要件

5.5　ICT 関連資格試験の最近の動き

近年，ICT 関連のプロフェッショナル資格を巡って二つの大きな動きがあった

情報処理学会が運営している認定情報技術者（Certified Information Technology Professional；CITP）は，「IT 技術者の社会的地位の確立を図る」という理念のもとに2014年に発足した。経済産業省の IT スキル標準に則り，情報処理技術者試験の高度試験（レベル 4）の12試験区分（「システム監査技術者試験」を除く。）の合格者が，主要業務・研修・資格・professional 貢献の記録，業務経歴書，達成度指標チェックシート，業務経歴書，達成度指標チェックシート，スキル熟達度チェックシートを添えて申請する。審査委員会が，審査したうえで申請者の能力を認定する。資格は登録制であり，その有効期間は 3 年である。CITP からなる professional コミュニティを構築し，コミュニティ活動を通じて社会および産業界のニーズに応えることを目的としている。2016年 4 月現在，認定情報技術者の登録者数は307名である[16]。「学会・コミュニティ活動」を奨励しているように見えるが，認定情報技術者申請書を見る限り，各 CITP の判断に任されているようである。情報処理学会がコミュニティの核になるということではなさそうである。また，CITP 本人は情報処理学会員である必要はない。

また，2016年10月には IPA が「情報処理安全確保支援士」を創設し，2017年 4 月 1 日に初回の登録を行う予定であるが，既に4,000名を超える登録申請があり（2017年 2 月15日IPA 発表による），関心は高い。SC 試験を情報処理技術者試験から分離し，上述の 5 つの条件を備えた資格試験として開始される。「情報処理安全確保支援士」は，サイバーセキュリティに関する専門的な知識・技能を活用して企業や組織における安全な情報システムの企画・設計・開発・運用を支援し，サイバーセキュリティ対策の調査・分析・評価やその結果に基づく指導・助言を行う（IPA 解説より）。ただ，英文名称は，Registered information security specialist となっており，professional とは称しておらず，SC 試験の名残が見える。

このような動きが ICT 関連のさまざまな職種に生じることを期待している。

6.　ISMS 専門家に関する国際規格 ISO/IEC 27021（以下，27021）の開発

6.1　専門家 professional

6.1.1　Profession（専門職）と Professional（専門家）とは

Professional の定義は多数あるが，社会学者である Ernest Greenwood は，専門職（profession）の属

[16] http://www.ipsj.or.jp/CITPholders.html

性として帰納的に次の 5 つを挙げている[4][17]：

- 専門領域を構成する概念，用語，活動を体系化した知識体（BOK）をもっている，
- 社会から専門家としての権威と信頼を受けている，
- コミュニティにおける承認，
- 職業倫理，
- コミュニティのメンバは固有の価値，規範，象徴の文化を共有している。

日本において代表的な professional である弁護士，公認会計士，中小企業診断士，建築士，技術士などは士[18] 業と呼ばれ，高度な専門性を要求される職業が多く，資格自体が法律で国家資格として定義されるなど，専門性と共に公益性も担保されている。また，士業には営利目的ではなく職能であるという意味が込められているので，職業倫理を課せられている。士業は，無資格者がそれらの業務を行うと罰せられる業務独占資格と，各士業が所属する職能団体を持っていることが特徴である。医師や薬剤師のように，専門養成課程を卒業・修了することが要件に含まれる資格は，日本では狭義の士業から除外されている。

一般に，専門家の資格には，業務独占，必置（組織に必ず置かねばならない），名称独占，更新制度という特徴があるが，その様態は，国や資格の種類によって異なる[19]。

6.1.2　professional 確立までの歴史

語源をたどると，professional[20] は「神の前で信仰を告白した人」を意味するが，professional という概念が，宗教的にではなく世俗的に確立した時期は，17世紀中ごろとみられる。これは，professional を育成する制度的機関としての大学の世俗化現象にともなって現れた。

ちなみに，specialist は，文字通り special な人であり，「ある技術を極めた人」を意味する違った概念である。expert は「経験として得た高度な技能や知識を持った人」を意味する。例えば，医師は，内科，外科，など多くの科を持つが，一括して professional と呼ばれる。一方，その専門分化した，例えば心臓外科医は心臓専門医として specialist in cardiology という呼称を持つことになる。

6.2　今日における professional の役割

日本では，professional も specialist も同じく専門家を意味することが多く，専門家の概念把握が未成熟である。広辞苑でも同義と説明している。かつて日本では，企業の求める人材像として，ゼネラリストを典型とし，加えて補完的にスペシャリストやエキスパートを求める程度であった。多くの従業員は，ゼネラリストとして働くことを選択し，管理職を目指していた。しかし，1990年代のバブル崩壊後，上述

[17] 杉野情報システムの専門家集団，情報システム学会誌，Vol.7，No.1，2012年

[18]「士」は中国期限の言葉であり，官位・俸給を有し，人民の上位にあるもの」を意味した。論語泰伯編に，「士不レ可二以下一弘毅一」（道に志す者は心が大きく強くなければならない）とある。

[19] 医師法は，「石でなければ，偉業をなしてはならない」（第17条），「医師でなければ医師又はこれに紛らわしい名称を用いてはならない」（第18条）と規定している。

[20] 1450年ころに，ラテン語 professionem から，修道会に入るための誓約（信仰を告白する）“声明”という意味で使われ始めたが，1667年には，“熟達したと公言する職業”という用例が初出している。Oxford English Dictionary による。

した専門家の要請が高まってきた。専門家はある特定分野における高度な専門スキル・知識を成果に直接結びつける能力（力量）が期待される。そのような成果を出すためには，高い仕事意欲やビジョン，洞察力，職業倫理なども持ち合わせていなければならない。さらに，専門家は，確固たるビジョンを持ち，各メンバの能力を見極めつつ，目標を達成するためのチームワークを上手に形成していくことが期待される[1][21]。また，専門家であることを第三者に対して客観的に示すために，資格化が行われる。例えば，法律家には弁護士，技術コンサルタントには技術士といった資格がある。

professional を以上のように定義することは，組織から独立した専門家としての professional を前提にしたものであるが，日本では，組織に所属した professional が非常に多いと思われる。この場合には，組織においてマネジメントの配下に配属されるが，本人は管理者としてではなく，組織内の専門家として職務を行っていくケースが多いものと思われる。

6.3　情報セキュリティマネジメントシステム（ISMS）とは

ISMS は，組織が保有し取り扱う情報の情報セキュリティを確保するための計画，運用，評価，改善を行うためのマネジメントシステムをいう。組織が自らこれらの情報を直接に管理する場面を主に想定し，その要求事項を定めた一連の規格を27000ファミリ規格（附-1 参照）と呼ぶ。この規格群には二つの中核的な規格がある。マネジメントシステムの要求事項を定めた ISO/IEC 27001と，体系的な情報セキュリティ対策を「管理策 control」と「実施の手引 implementation guidance」として示した ISO/IEC 27002である。管理策は，ISO/IEC 27001の附属書としても掲載されており，これら二つの標準が密接に繋がっていることを示している。組織が自らの ISMS について第三者の認証を受ける場合，ISO/IEC 27001は，すべての組織に適用される ISMS 認証基準として位置づけられる。また，ISO/IEC 27002は，実際に組織が情報セキュリティマネジメントを計画，運用，評価，改善するに当たって参考とすべき標準的な対策（ベストプラクティス）を管理策として列挙し，またそれらを実施するうえでの手引書として役立てることを目指している。

6.4　ISMS-P はなぜ必要か

6.1では専門家の一般論を述べたが，上述の 5 つの情報セキュリティ人材の内①，②，⑦は ISMS-P としての成果が期待される人材[22]である。そればかりでなく，②～④が ISMS-P を目指す身近な自己啓発の目標となる。このことによって，情報セキュリティ部門における人材育成のキャリアパスを示すことができる。

又，人材育成部門にとっては，教育研修の目標を設定することができる。大学にとっては，専門教育のカリキュラムを作成，教育する補助となろう。

---

[21] 金　雅美 professional とスペシャリスト金のアカデミズムの現場から　第四回，2000年 http://sternjapan.com/modules/bulletin_2/index.php?page＝article&storyid＝15

[22] 筆者らが本規格開発の初期段階で日本での活用を検討していたときには，ISMS-P の理想像として CISO を措定していた。しかし，WG1 会合では，この規格の利用者は CISO ばかりでなく情報セキュリティ管理者（上述の②）までをも含むべきであるとの意見が強く，そのように定義された。

6.5 Competence[23] の定義

一般に組織において個人が成果を出すための能力としては，アウトプット，知識，スキル，マインドスタンスの四つの要素が必要だといわれる。情報セキュリティ人材についても然りである。しかし，第三者がその能力を認証するための評価基準としては，客観的に評価可能か否かがポイントになる。

Competence の概念をビジネスの世界に導入するきっかけとなったのは心理学者である D.C. McClelland の論文 ‘‘Testing Competence Rather Than ‘Intelligence’ ’’（1973）である。McClelland は，数多くの卓越した業績を挙げている外交官とそうでない外交官の特性を分析し，優れた業績を挙げる人達には共通の行動特性があることを見出し，それを competency と名付けた。McClelland によれば，人々の業績や人生の成功は，知識の豊富さや学力とは必ずしも対応せず，動機に関連づけられたある種の能力，competence と高い相関があることがデータにより裏付けられたという。更に，competence を強化すれば成果につながる確率が高くなるので，人材開発や目標管理に応用できる可能性があるという。その後，competence は人材の採用，昇格，配置，育成の基準として使用されるようになった。

competence は図 3 に示す氷山モデルを用いて説明される。氷山モデルはヒトの「能力」に着目した断面で切断されている。人によっては解釈や定義は異なるが，competence は氷山の水面から見える部分である。人の能力は，氷山のうち水面上に目に見える特性だけでは判断することはできず，水面下に隠れている特性が結果に大きく影響を及ぼす。水面下に隠れているものとしては，価値観，性格，動機がある。Professional の能力として測定可能な特性は表に現れたものだけであり，力量は知識とスキルで構成されるということになる。ISO/IEC 17024:2012（以下，17024）は competence を次のように定義している：

ability to apply knowledge and skills to achieve intended results

意図する成果を達成するために知識とスキルを活用する能力

27021 でもこの定義を参照している。

7. 27021の開発

ISMS とは，情報セキュリティの計画，運用，評価，改善によって，その組織の目的を達成するプロセ

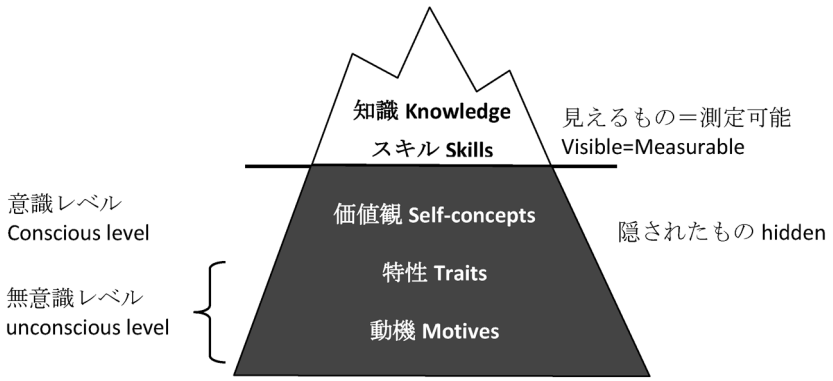

図 3 氷山モデル

[23] Competency と competence を同意語として使っている。

スを確立するための，相互に関連又は相互に作用する一連の要素（組織の構造，役割及び責任，計画，運用など）のことである。

27021は ISMS を計画，運用，評価，改善する責任者である ISMS–P の能力（力量）として要求される事項を定義する規格である。まず ISMS–P に期待される役割 Role を定義し，その役割を果たすために要求される力量を要求事項として設定し，この要求事項に準拠して第三者評価することによって，専門家を認証するという論理を適用している。また，各国がこの規格に準拠して人材を評価することによって，ある国で力量を認められた ISMS–P が他の国で技術者として容易に受け入れられ，専門家の国際的流動性を支援できることになる。ISO において17024は，個人の能力を第三者評価するための汎用規格として策定されている。

17024は他の個人の力量の認証基準の枠組みとしても使用されている。例えば，組織がその品質マネジメントシステム QMS の認証を受ける場合には，認証機関の審査員がその組織の QMS を審査して認証可否を判断する。この QMS 審査員の力量を認証するための要員認証機関に対する一般的な要求事項を規定した規格が17024である。

7.1　ISO 規格の策定手順と関連文書

国際規格 IS を速やかに作成するために，ISO の各小委員会（Subcommittee；SC）は，開始されるプロジェクトについて，各段階完了の目標期日を定める際の指針として，表 3 の目標期日が定められている。

プロジェクトは，SC の会合で提案され承認されると，分担する作業グループ（Working group；WG）は予備段階から開始し，年 2 回世界各地持ち回りで開催される会合における expert たちの議論を Co-Editors がまとめて規格案として文書化する。各段階の中ではコメントの要請（Call for Comments），次の段階に進むためには電子投票（Electronic Balloting）を実施していく。表 3 において，CD 作成までは SC 内での検討であり，各 national body（国代表団体；NB）から参加する expert によるコメント提出，投票が繰り返されるが，DIS 以降では SC レベルを離れ，各 NB が投票することになる。規格が承認され，IS が発行される。さらに，3 年ごとに定期的見直し Systematic review が行われ，規格の存続可否と改定

表 3　プロジェクトの各段階と関連文書，策定手順

段　階	名　　称	略語	目標期日	作 業 内 容
予備段階	予備業務項目 Preliminary work item	PWI		
提案段階	新業務項目提案 work item proposal	NP	開始	NP の採択によって開始
作成段階	作成原案 Working draft	WD	12か月以内	WD の作成
委員会段階	委員会原案 Committee draft	CD	6 か月以内	CD から FDIS の作成
照会段階	照会原案 Draft international standard	DIS	24か月以内	国代表団体からの意見取り上げ，DIS から FDIS の作成
承認段階	最終国際規格案 Final DIS	FDIS	33か月以内	国代表団体から FDIS の承認取付
発行段階	国際規格 International standard	IS	36か月以内	IS の印刷・配付
国際規格の定期的見直し				

の要否が議論される。また，様々な段階で expert に対して，Call for contribution が発行され，様々な意見要請がなされる。

7.2 27021開発の現状

ISO の中で SC27小委員会は，セキュリティ技術の国際規格を策定している。SC27には WG1～WG5 の五つの作業グループがあり，規格文書を開発している。筆者が属する WG1 は ISMS 関連の規格策定を行っている。WG にはコンビーナ WG-Convenor，各プロジェクトにはコエディタ Co-Editors（プロジェクト開始前はラポータ Rapporteur と呼ばれる。）が expert の中から複数名指名される。27021では，3 名が指名された。

27021プロジェクトの発端から CD 投票にいたる主な会合と検討の概要を次に記す。

⑴ 2012/05 Stockholm 会合：新規格開発の提案と Study period（SP）の開始

スウェーデンから情報セキュリティマネジメントスペシャリストの国際認証標準 International Certification of Information Security Management Specialists（ICISM-S）の開発に関する提案がなされ，6 か月間の Study period が承認された。ラポータにスウェーデン，韓国，日本から計 3 名が選任された。

⑵ 2012年10月 Rome 会合：SP 結果の報告と SP の再度実施

（以後，筆者が参加）

ラポータ（韓国，日本）から各国の情報セキュリティ管理者（ISM）資格の実態に関する調査結果が報告された。しかし，新規格の市場性に関する疑問が出されたため，expert に更なる調査（Contribution）をもとめる依頼（2013年 2 月を期限とする）がなされ，再度 SP を実施することになった。

⑶ 2013年 4 月 Sophia Antipolis 会合：NWIP を作成

議論の中で，ISMS-P の市場性と，したがって ISMS-P を認証する仕組みの必要性は了解された。また，要員の力量を認証する17024は汎用規格であり，情報セキュリティ管理（ISM）という Domain specific な標準が必要であるという意見が大勢を占めた。

この規格のまず第一の利用者は（ISC）2，ISACA といった認証機関である。認証機関は ISM 分野の既存あるいは将来の27000シリーズに準拠して活動する専門家の力量を保証するための認証スキームとして利用するであろう。

また，同時に他の WG から提出されていたプロジェクトと名称をそろえるという理由で，規格名称は，ICISM-S から Requirements for the certification of information security management professionals（R-CISM-P）に変更された。また，specialist は筆者の提案で professional に変更された。

---

[24] CASCO（Committee on Conformity Assessment；適合性評価委員会）は ISO における資格認証の規格策定委員会，CAB（Conformity Assessment Bodies；適合性評価委員会）は IEC における資格策定委員会，JTC1（Joint Technical Committee 1）は ISO と IEC の合同委員会のことである。

⑷ 2013年 6 月：NWIP 電子投票開始，ただちに中止

NWIP の投票開始時に，ISO/CASCO，IEC/CAB，JTC1[24] の間で適合性評価に関連する ISO/IEC Directives 6.0（専門業務用指針）に示す業務手続きに適合していないとの指摘がなされた。SC27は，投票開始日に直ちに投票を中止し，7 月には NWIP 投票そのものを取り下げた。

⑸ 2013年10月　Incheon 会合：CASCO/CAB との意見調整後に再度 NWIP の作成へ

NWIP 投票中止の経緯についての説明，とりわけ，個人認証の規格策定に関しては，ISO における規格作成に関する原則と規則を定めた専門業務用指針に示されるように ISO/CASCO と IEC/CAB の協力が不可欠であることの説明があった。ISO/CASCO と IEC/CAB は，個人認証のための規格を作成する用意があるが，情報セキュリティは専門外なので，SC27 WG1 にはそのための competence specification を作成してほしいということになったと思われる。また，その後のラポータと CASCO，CAB 間のネット会議の結果，文書の名称を RCISM−P から Certification of Information Security Management Professionals（CISM−P）に変更することになった。

⑹ 2014年 4 月　Hong Kong 会合：ISMS−P の概念の明確化

ISMS の PDCA サイクルに責任を持つ専門家であることを明確にするために，規格名称でも Information Security Management Systems と明記することにした。文書名称については会合終了後ももめたが，本規格は professional を評価するための認証基準とはしない（これは CASCO, CAB のいわば専権事項である）ので，Certification を Competence requirements に変更し，結局 CISM−P から Competence requirements for information security management systems professionals（CRISMS−P）へと修正され，現在に至っている。

⑺ 2014年 5 月28日から　NWIP 電子投票と可決

電子投票で NWIP が可決され，新プロジェクトとして開始されることが決定した。

⑻ 2014年 9 月 9 日　ISO のプロジェクトとして登録

プロジェクト期間を2014年 9 月 9 日から2017年 9 月 9 日までの 3 年間とし，3 年以内に IS 文書を作成し，ISO 規格として登録することを要請された。

⑼ 2014年10月　Mexico City：WD1 作成へ

Co-Editors がドイツ，日本，インドから選出された。

ISMS−P のもつべき competence について Free Discussion を行った結果をもとに，会議後に Co-Editors が WD1 を作成した。この文書は WG1 内の exerts に回付され，コメントを求めた。

⑽ 2015年 4 月　Kuching 会合：WD2 作成

文書構造は27001に合わせることとした。本規格の利用者 audience は ISMS professionals，人材開発部門，認証機関，学生，教育機関であるとした。WD2 に関するコメントを experts に求めた。日本が

BOK の案を提示した。会議後に WD2 版が作成された。この文書は WG1 内の experts に回付され，コメントを求めた。

⑾ 2015年/10月　Jaipur 会合：WD2 改訂版作成

コメントを集約して WD2 改訂版を作成し，さらにコメントを求めた。

⑿ 2016年 4 月　Tampa 会合：CD 投票へ

Co-Editors の一人がインドから英国に交代した。議論の結果 CD 投票に付すことについて合意され，電子投票を行った。

⒀ 2016年10月　Abu Dhabi 会議：DIS 投票へ

CD 投票で賛成多数となり，DIS 投票に進むことになった。

⒁ 2017年 1 月　DIS 投票

2017年 3 月30日が DIS 投票期限であり，承認されれば 4 月に開催される Hamilton 会議で各 NB のコメントの集約結果が確認される。2017年 9 月までに IS を成立させることを目指している。

7.3　現在の文書構成

現在，DIS 投票のために各 NB に提示されている DIS 案の文書構造を図 4 に示す。

Clause 3 までと最後の Bibliography はすべての ISO 文書に共通の章立てであり，Clause 4 から Annex までは，各規格ごとに独自の構造を作っている。Clause 4 は文書全体の構成に関する解説である。

先ず ISMS-P を，「一つまたはそれ以上の ISMS プロセスに責任を持つ人」と定義した。ISMS-P に要求される具体的な力量 competence を，General management competence area（Clause 5）と Information security specific competence areas for an ISMS professional（Clause 6）の二つに分ける。Clause 5

Forward
Introduction
1 Scope
2 Normative and references
3 Terms and definitions
4 Concept and structure
5 General management competence area
　5.1 Leadership
　5.2 Communication
　5.3 Business strategy and ISMS
　5.4 Organization design, culture and behaviour
　5.5 Process design and organizational change management
　5.6 HR, team and individual management
　5.7 Risk management
　5.8 Budgeting and financial management
　5.9 Information systems architecture
　5.10 Project and portfolio management
　5.11 Supplier management
　5.12 Problem management
6 Information security specific competence areas for an ISMS professional
　6.1 Competence area: General information security
　6.2 Competence area: Planning
　6.3 Competence area: Operation
　6.4 Competence area: Support
　6.5 Competence area: Performance evaluation
　6.6 Competence area: Improvement Competence
Annex (informative) A Including competences for ISMS professionals in ISO/IEC27021 as part of a Body of Knowledge
Bibliography

図 4　27021の Clause/Subclause 構成

表 4　competence の記述例

Competence	5.1 Leadership
ISO/IEC 27001 clause/sub-clause（if applicable）	5 Leadership
Intended outcome	Directing, motivating and encouraging staff across the organization to deliver information security
Knowledge required	• Theories of leadership • Negotiation techniques
Skills required	• Set and give direction for information security across the organization • Provide guidance, set objectives and drive progress within the information security function, team and the business *The rest is omitted.*

は ISMS 固有ではないやや一般的なマネジメント関連力量を扱っており，さらに12の competence に分類して記述している。27001に対応する competence は四つ（Risk management, Information systems architecture など）にとどまっている。Clause 6 は，ISMS に強く関連する competence area を扱っており，さらに六つの Sub-clause に分け，それぞれに一つ～三つの competence，合計12の competence を収めた。12の competence のうち27001に対応していないものは一つ（Technological trends and developments）のみである。

今後 ISO/IEC 27001が修正されれば当然に，また ISMS–P に要求される competence が環境の変化とともに増加してくれば，さらに知識やスキルも増加することがあると思われる。これらの competence に対して知識とスキルを個条書きにしているが，特に知識については，Annex A の Body of knowledge においてやや詳しく例示している。

7.4　27021の構造

それぞれの competence area には複数の competence が含まれる。そして，各 competence は表 4 に示す構造の表形式で内容を記述している。

1 行目は competence 番号と名称，2 行目は27001の対応する Clause / sub-clause を示す。General management competence area には，ISMS と直接は関係ない項目も含まれるので if applicable としている。3 行目は当該 Competence において ISMS–P に期待される成果を示す。4 行目，5 行目では必要な知識，スキル項目を列挙している。

8.　課　　題

1）　27021に準拠した認証機関の出現

27021は要求事項を定めるのみである。実際に，ISMS–P の個人認証を実施するには，17024に準拠する認証機関が27021に準拠した認証スキーム[25]を作成しないと，認証業務を行えない。各認証機関が

[25] 17024の clause 8.2には，認証の範囲，業務の記述，要求される力量，前提条件（あれば），行動規範が示されている。

27021にどのように対応するかは今のところ不明である。表 3 に示した認証機関の内，（ISC）2 及び ISACA は27021プロジェクトのリエゾンメンバであり，議論には加わっているが，彼らの認証業務における今後の対応については不明である。

2） Annex A に示す BOK の準拠性の確保

この BOK は一般的なものにすぎない。各認証機関は，自らの認証スキームの中で具体的な BOK を提示し，そのような条件下の ISMS-P をあるべき姿として認証評価を行うことになる。問題は，Annex A に示す BOK と各認証機関の BOK が内容的にどのような位置づけになるかが不明なことである。勝手に27021準拠であることと宣言されることは，27021の信頼性にもかかわることであり，何らかの歯止めを今後検討する必要があるのではないかと考えている。

3） ISMS-P の国際流動性の確保

各国の認証機関同士の連携あるいはグローバルな認証機関（例えば（ISC）2 の CISSP）によって認証スキームの互換性が確保されないと，ISMS-P の国際流動性は実現しない。

9. おわりに

27021規格の背景と考え方を紹介した。WG1 で作成した国際規格原案 Draft international standard は仏語へ翻訳を経て各国の投票に回された。なお，Software Engineer の専門家認証に関する規格 ISO/IEC 24773は既に2008年に成立している。情報通信技術の他の分野についても同様の検討が進むことを期待している。

本研究は，2012年度国外給費研究員としての派遣期間中の研究，2012年からの SC27/WG1 Expert 活動における調査研究の成果である。関係者に謝意を表する。

引用・参考文献

すべて脚注に示した。URL は2017年 1 月 5 日に確認した。

附１　27000ファミリ規格の全体

規格番号	規　格　名　称
JIS Q 27000 ISO/IEC 27000	情報セキュリティマネジメントシステム―用語 Information security management systems―Overview and vocabulary
JIS Q 27001 ISO/IEC 27001	情報セキュリティマネジメントシステム―要求事項 Information security management systems―Requirements
JIS Q 27002 ISO/IEC 27002	情報セキュリティ管理策の実践のための規範 Code of practice for information security controls
ISO/IEC 27003	Information security management system implementation Guidance
ISO/IEC 27004	Information security management―Measurement
ISO/IEC 27005	Information security risk management
JIS Q 27006 ISO/IEC 27006	情報セキュリティマネジメントシステムの審査及び認証を行う機関に対する要求事項 Requirements for bodies providing audit and certification of information security management systems
ISO/IEC 27007	Guidelines for information security management systems auditing
ISO/IEC TR 27008	Guidelines for auditors on information security controls
ISO/IEC 27009	Sector-specific application of ISO/IEC 27001―Requirements
ISO/IEC 27010	Information security management for inter-sector and inter-organizational communications
ISO/IEC 27011	Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
ISO/IEC 27013	Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000–1
JIS Q 27014 ISO/IEC 27014	情報セキュリティガバナンス Information security governance
ISO/IEC TR 27015	Information security management guidelines for financial services
ISO/IEC TR 27016	Information security management―Organizational economics
ISO/IEC 27017	Code of practice for information security controls based on ISO/IEC 27002 for cloud services
ISO/IEC 27018	Code of practice for protection of personally identifiable information（PII）in public clouds acting as PII processors
ISO/IEC TR 27019	Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry
ISO/IEC 27021	Requirements for Information security management systems professionals
ISO/IEC 27023	Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002

注１ 各規格文書名称の冒頭に付く「情報技術―セキュリティ技術―（Information technology―Security techniques―）」は共通であり，省略した。
注２ 作成中，発行済，改訂中すべての規格を含む。