ISMS professional の国際標準化について

Developing International standard on ISMS professionals

杉野　隆　Takashi Sugino

日本大学商学部
Faculty of Commerce, Nihon University

要旨　情報セキュリティ（IS）の重要性が強まる中，組織における ISMS の構築・運営を推進する IS 人材のトップレベルを提示することは，IS 専門家の確保，人材育成において重要な意味がある。ISO/SC27WG1[1]において筆者が参加するプロジェクトの 5 年間の活動の成果として国際規格 ISO/IEC 27021 が年内に成立する見通しである。本報告では，この国際規格の目的，開発経緯，内容の概略を紹介する。また，情報システム分野における他の専門家育成，国際標準化との関連にも触れる。

1.はじめに

ICT 分野の資格試験には，表 1 に示すように情報処理技術者試験[2]ITEE，技術士情報工学部門，PMP 試験が，情報セキュリティ分野に限ると，CISSP，CSX などがあり，2014 年には認定情報技術者 CITP 試験，2017 年 4 月には情報処理安全確保支援士 RISS の試験が開始された。このうち合格者に professional を呼称させている資格には*を付けた。なお，システム監査関連は除いた。

表 1　主な情報システム関連資格試験

地域	資格区分	資格認定試験名
日本のみ	ベンダ中立資格	情報処理学会：認定情報技術者(CITP)試験*
	国家能力認定	経済産業省：情報処理技術者試験(ITEE)（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，他）
	国家資格	経済産業省：情報処理安全確保支援士(RISS)試験
		日本技術士会：技術士情報工学部門*
		経済産業省：IT コーディネータ試験
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[3] Certified Information Systems Security Professional (CISSP)*
		ISACA[4] Cybersecurity Nexus (CSX) Specialist
		IEEE Professional Software Engineering Master(PSEM)*
		IEEE Professional Software Engineering Process Master(PSEPM)
		ITIL V3 Foundation
		PMI：PMP（Project Management Professional）試験*

2.情報セキュリティ人材[5]の育成

2.1 情報セキュリティ人材の現状・課題

2011 年に，ソニーの PlayStation Network 及び Qriocity への不正アクセス，Lockheed Martin 社，参議院・衆議院，三菱重工業，川崎重工業への標的型攻撃など，世界中の大企業などがサイバー攻撃の被害を受けた。これを契機に，サイバーセキュリティが日本社会の重要課題であり，とりわけサイバー人材不足が喫緊の課題であると認識された。2014 年にはサイバーセキュリティ基本法が成立し，国が本格的に取り組む姿勢を見せた。経済産業省は，2016 年 6 月に，情報セキュリティ人材の

[1] Subcommittee 27/Working group 1。ISO 内の組織であり，情報セキュリティマネジメントシステムに関する規格の開発を担当している。
[2] 経済産業省が所管する国家試験であるが，所定の能力を認定する認定試験であり，資格試験ではないとしている。
[3] International Information Systems Security Certification Consortium
[4] 当初 Information Systems Audit and Control Association として商号を登録していたが，後に ISACA に変更した。
[5] サイバーセキュリティはサイバー空間における安全確保と解釈できるが，本稿では情報セキュリティとサイバーセキュリティを動議として扱っている。

不足は，2016 年時点で約 13.2 万人，2020 年には約 19.3 万人に拡大するという推計結果を発表した。しかし，情報セキュリティ人材の需要が高まる一方で，人材不足はさらに深刻化する可能性がある[6]。

企業における ICT の利用は，業務の効率化による企業の収益性向上ばかりでなく，企業がグローバルな競争をする上での必須の条件となっている。それに呼応するかのように，サイバー攻撃は年々高度化，巧妙化してきており，企業経営に深刻な影響を引き起こす事件が多発している。サイバー攻撃が避けられないリスクとなっている現状では，経営戦略としての情報セキュリティ投資は必要不可欠かつ経営者としての責務である。

2012 年の英ロンドン五輪大会の運営では，ネットワーク運用・管理者 800 人が関わり，うち 50～60 人はトップガン級の人材[7]をそろえたという。また，2020 年東京オリンピック・パラリンピック競技大会でも，競技周辺，関係組織，開催都市に対する大規模・連続的なサイバー攻撃が予想される。昼夜を問わない同時多発的な攻撃に競技期間中対処し続けるためには，ロンドン大会と同等以上の十分な体制の構築が必要であると言われている。

2017 年 4 月に，内閣官房サイバーセキュリティ戦略本部は，2020 年を見据えて，「サイバーセキュリティ人材育成プログラム」を発表した。このプログラムでは，サイバーセキュリティ技術者としてサイバー空間に関する AI や IoT など新しい ICT の応用分野にも立ち向かえる人材を育成するという方向性を示した。また，専門技術を一定程度理解したうえで，一般的な業務や組織マネジメントにも通じた「橋渡し人材」育成の重要性を示した。同様に，本稿では，高度な技術力とマネジメント力をもち，高い職業倫理に裏打ちされて業務遂行することが求められている ISMS professional（ISMS-P）を扱う。

2.2 サイバーセキュリティ人材の種類

情報セキュリティ人材には，さまざまな職種が必要となるが，一例を表 2 に示す。ISMS-P は，CISO 又は①に対応する職種である。

表 2　情報セキュリティ人材の職種分類[8]

名称	概　　要
①最高情報セキュリティ責任者	企業内で情報セキュリティを統括する担当役員
②セキュリティ戦略／統括	主に自社内の情報セキュリティ戦略立案，情報セキュリティ方針・規程などの策定及び子会社の情報セキュリティ対策の統括などを行う。
③企画／設計	主に企業の自社内及びグループ内における情報セキュリティシステム及びネットワークなどの企画，設計などを行う。
④開発／構築	主に企業の自社内及びグループ内における情報セキュリティシステム及びネットワークなどの開発，構築などを行う。また，自社が提供する製品などの開発や受託開発，これに関連する研究開発なども含む。
⑤運用／管理	主に企業の自社内及びグループ内における情報セキュリティシステム及びネットワークなどの運用や管理などを行い，情報システム部門や情報システム管理，品質管理部門の担当業務に相当する。このほか，サービスとして顧客から運用や管理を受託する場合も含む。
⑥監査／検査	主に顧客向けのサービスとして，情報セキュリティ監査，コンピュータフォレンジック対応，ペネトレーションテストなどを行う。また，監査部門などにおいて自社及びグループ内を対象とした情報セキュリティ監査や検査などを行う場合も含む。
⑦コンサルティング／教育	主に顧客向けのサービスとして，情報セキュリティに関する様々なコンサルティングを行う。情報セキュリティに関する研修・トレーニングなどのサービスや，教育機関で情報セキュリティに関する教育・研究活動を行う場合を含む。

3. なぜ professional が必要なのか

3.1 認定情報技術者 CITP の場合

CITP 試験を実施する情報処理学会は，次の 3 点から ICT 分野に professional は必要だとする[9]。す

[6] IPA 情報セキュリティ白書 2017
[7] 情報セキュリティについて専門的なスキル・知識を保有すべき人材
[8] IPA 情報セキュリティ人材の育成に関する基礎調査-調査報告書-，2012 年 4 月
[9] 次の資料を要約した。旭寛治　高度 IT 人材資格制度のビジョン，高度 IT 人材育成フォーラム，2012 年 2 月

なわち，①わが国の情報処理技術者の社会的地位が低い。情報処理技術が魅力ある分野として認識されていない，②産業としての魅力に欠け，学生から見ると，新たなフロンティアを開拓する発展性のある業務が少ない，③情報処理技術者のプロフェッションが確立していない 。プロフェッショナルコミュニティが形成されていない。

そして，CITP が情報処理技術者の professional 化を促すことによって，①情報処理技術者の自律的な質の向上 ，②社会に対する一層の貢献 ，③情報処理技術者の社会的地位の向上，が可能であるという。情報処理学会は，IT 分野における profession 確立の基盤として資格制度も必要であるとして，認定情報技術者の認証試験を開始したというビジョンを示した。

筆者は，開発・運用技術者の professional 資格の取得は，情報システム（IS）の高い品質を確保することにも貢献すると考えている。Professional 資格の取得は，職業倫理の自覚を促し，自己の業務執行の姿勢を正すことに繋がるからである。情報セキュリティにおける ISMS-P も同様である。

3.2 Agency 理論による解釈

Principal（依頼人）と agent（代理人）の関係において，専門的な知識を有するとともにモラルや忠誠心にあふれた代理人が，依頼人の立場に立ってベストな行動を選択する場合には，両者の間には特に問題は生じないであろう。通常，代理人は依頼人の利益を第一に行動すべきであるが，実際はそのような行動を常にとるとは限らない。そのため，依頼人は代理人の行動を監視し，抑制しなければならない。この際にかかる費用を agency cost という。ここで，代理人を professional に，依頼人を発注者に置き換えてみよう。発注者が，ある情報システムの開発を professional に発注するとする。もし，professional がその資格通りに力量を十分に発揮してくれれば，たとえ高額の開発費用を支払ったとしても，発注者は受託者の行動を監視したり，厳しい検収を行ったりせずに，所定の情報システムを実現できるわけであり，開発コストの削減につながることになる。

3.3 professional とは何か

西洋社会では，17 世紀頃には聖職者，医師，弁護士の 3 つが古典的 profession として確立していた[10]。日本における ICT 分野の代表的な profession は，技術士（情報工学部門）であろう。日本技術士会は，profession の概念を次のように示している[11]。

1. 教育と経験により培われた高度の専門知識及びその応用能力を持つ。
2. 厳格な職業倫理を備える。
3. 広い視野で公益を確保する。
4. 職業資格を持ち，その職能を発揮できる専門職団体に所属する。

Profession という職業集団の構成員が professional である。Professional については様々な定義があるが[12]，技術士会は次のように定義している[13]。

1. 体系化された理論に基づく専門的能力を保有する（専門職の個人属性）
2. 倫理規範に基づく業務の遂行能力を保有する（専門職の個人属性）
3. 能力と規範の推進のための職業団体を組織する（社会的仕組み）
4. 社会から存在意義を認められている（社会的仕組み）

4. ISMS-P の紹介

4.1 ISO/IEC における要員認証[14]の仕組み

ある仕事に関して，人が適格な力量を有していることを第三者が証明することは，その仕事の結果を利用する者にとって，結果の信頼性を判断するために重要なことである。個人がある特定の基準に照らして力量を持っていることを，第三者である認証機関が評価・証明し登録することを，要

[10] 石村善助　現代のプロフェッション，至誠堂，1969 年
[11] 日本技術士会　プロフェッションの概念，https://www.engineer.or.jp/c_topics/000/attached/attach_29_1.pdf
[12] 米国ではすでに 1947 年労使関係法（いわゆる Taft-Hartley 法）において，また P. Drucker は“The Practice of Management”において professional employee（専門職従業員）の属性を同様に規定している。日本で現在話題となっている高度プロフェッショナルもこれに属するはずだが，概念は全く異なる。
[13] 日本技術士会 技術士への道：https://www.engineer.or.jp/c_topics/000/attached/attach_885_4.ppt
[14] 17024 は certification of persons と表記しており，個人認証が適切な表現だが，本人認証のための例えば生体認証などを個人認証と呼ぶことから，一般的に要員認証と呼ぶことが多い。本来，要員とは，組織に属する個人たちの集合的表現である。

員認証と呼ぶ。17024「適合性評価－要員の認証を実施する機関に対する一般的要求事項」（17024[15]）は，要員認証機関が，国際的に，認証機関としての信頼性を確保するために技術者の力量の評価・認証業務を審査し，当該認証機関を認定 accreditation する要求事項を規定した国際規格である[16]。ただし，要員に要求される知識・技能は分野によって異なるので，17024 は各分野共通の認証スキームを定め，各分野固有の力量の要求事項は当該専門の SC の制定する規格に依存している。図 1 に要員認証の一般的なスキーム[17]を示す。

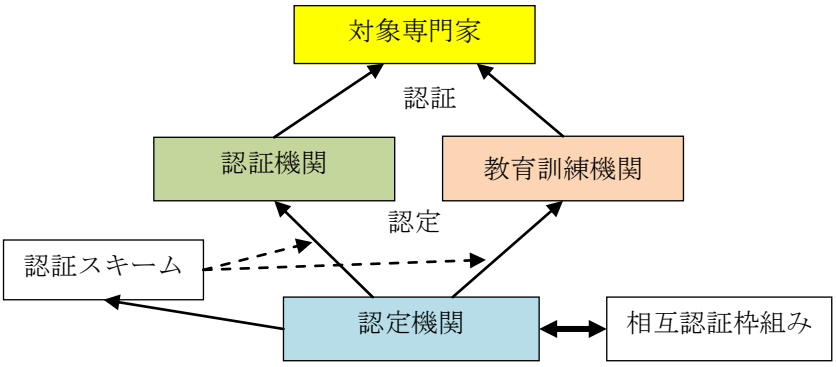

図 1　要員認証の一般的なスキーム

例えば，企業が自社の事業所で整えた情報セキュリティ管理体制を認証審査するチームを指揮する審査員は，日本適合性認定協会 JAB を認定機関とし，17024 に加えて，固有力量の要求事項は 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」（27021 に相当）に準拠して，要員認証機関を認定している。要員認証機関は，この認証スキーム[18]に基づいて試験を実施し，合格者に審査員資格を授与する。ISMS-P の場合，固有力量の要求事項を 27021 に期待している。要員認証に関するこのような枠組みは既に国際的に確立している[19]。

4.2 ISMS-P とは

ISMS とは，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に構築するマネジメントシステムである。ISMS-P とは，ISMS プロセスの計画，構築，運用，継続的改善を（包括的に）実施する者をいう[20]。ISMS-P は，情報セキュリティ管理部門の人々の具体的な自己啓発目標となり，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，人材育成部門にあっては，教育研修の目標を設定することができる。大学にあっては，情報セキュリティ専門カリキュラム作成の参考となろう。

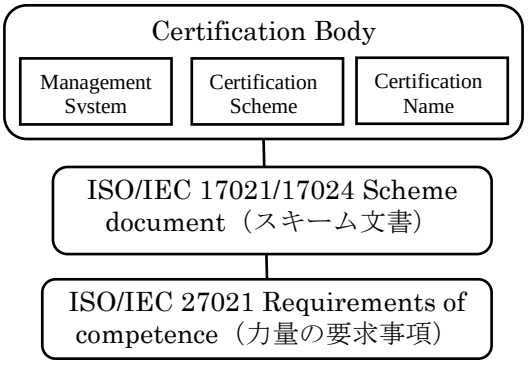

図 2　ISMS-P 認証の仕組み

4.3 27021 の開発

ISO/IEC SC27/WG1 内で ISMS-P の規格化を検討する提案が 2012 年 5 月に出され，検討期間 SP が設定され，予備作業項目（PWI）の検討を通じて，新たな国際規格としての市場性が議論された。2013 年 4 月に規格を開発するプロジェクトが承認され，Editors として，日，独，印から 3 名が選出された。しかし，国際規格（IS：International standard）制定に至るまでには，いくつかのステップを経ねばならない。

具体的には，2014 年 4 月に新業務項目提案（NWIP）が作成されて WG1 内の投票に付され，2014

---

[15] ISO/IEC 規格と JIS 規格は同一番号が対応しているので，以下，番号のみで参照する。例：ISO/IEC 27001，JIS Q 27001 →共に，27001

[16] 要員認証機関の認定(ISO/IEC 17024)，https://www.jab.or.jp/service/essential_member/

[17] 次の資料を参考にした。経済産業省　組込みソフトウェア開発力強化推進タスクフォース　認証・認定・登録制度調査調査報告書，2006 年。インストラクタ，CPD ポイント関連は省略した。

[18] 17024 の箇条 8.2 によれば，認証スキームが含むべき要素は，a) 認証の範囲，b) 職務及び業務の内容，c) 要求される力量，d) 能力（該当する場合）e) 前提条件（該当する場合），f) 行動規範（該当する場合）の 6 項目である。

[19] IFIP（International Federation for Information Processing）は，資格認証のスキームとして ISO/IEC 17024 及び 24773「ソフトウェア技術者認証」に準拠した IP3（International Professional Practice Partnership）を 2006 年に制定している。IP3 によって各国の資格制度は相互認定されることになる。CITP が IP3 の認定を受けているかどうかは不明である。

[20] ISO/IEC 27021 の定義であるが，この定義の一部のみを分担する者ではない。筆者らは本規格開発の当初，ISMS-P の目標として CISO を措定していた。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が，包括的に実施できるものであることには変わりはない。

年 9 月に NWIP が承認され，プロジェクトが正式に発足し，作業原案（WD）の作成に着手した。2 回の WD 作成を経て，2016 年 4 月に委員会原案（CD）の作成に至り，SC27 内投票の結果承認された。さらに，2016 年 10 月に照会原案（DIS）が作成され，投票によって承認され，2017 年 4 月に最終国際規格案（FDIS）に至った，FDIS は ISO の全 National body[21]の投票に付され，2017 年 9 月に 2/3 以上の賛成の結果，承認された。2017 年内に正式に IS が発行される予定である。

4.4 27021 の構造

27021 は，組織において，27001 が要求する ISMS を確立，実施，見直し，改善するために従事する個人に要求される力量 competence[22]を規定している。27021 は，力量として必要とされる知識 knowledge と技能 skills の範囲と項目を定義し，また知識については，Body of Knowledge（BOK）を定義している。ただし，この規格は BOK のひな形を提示するまでであり，具体的な BOK は教育機関，認証機関[23]などが自らの目的に応じて作成する。Professional としての一般的な要件は 17024 に規定されており，ISMS-P 固有の力量についてのみ 27021 で規定している。認定機関は，要員認証を実施する認証機関の定める資格認証スキームが 17024 及び 27021 に準拠していることを認定するという構造である（図 2）。末尾の付属資料に 27021 の目次を示す。

4.5 ISO における Software engineer professional の認証

情報セキュリティ以外の ICT 関連の要員認証についてみてみよう。表 3 に ICT 関連資格を比較した。情報システム関連技術者は，今後国際的に流動することが予想される。そこで，ソフトウェア技術者（SE）の professional 資格認証を国際的に相互互換する[24]ための比較枠組みが，ISO/IEC JTC1/SC7 の WG20（ソフトウェア及びシステム知識体系とプロフェッショナル形成）において検討され，24773:2008[25]が発行された。BOK には，IEEE Computer Society が開発してきた SWEBOK が採用された。ただし，資格認証のための要求事項を直接的に定めた規格ではない。ISO/IEC が，要員認証はすべて 17024 の枠組み内で行うと規定しているからである。情報システム関連の professional の資格認証もすべてこの枠組みに従わねばならない。CITP の場合には，17024 と 24773 を認証スキームとし，IFIP が主導する IP3 が認定機関となり，情報処理学会を認証機関として認定するという枠組みを想定しているようである。

表 3　各種 IT 資格の相互比較[26]

	ISO/IEC 24773 の評価項目					備考
	知識・スキルの明示	実務経験の評価	技術者倫理	CPD（継続研鑽）	資格更新	
情報処理技術者 ITEE	○	△（試験）	×	×	×	情報処理の促進に関する法律
情報処理安全確保支援士 RISS	○	△（試験）	△	○	○	
技術士（情報工学）PE	○（策定中）	○	○	○	×	技術士法
IT 企業・社内資格	○	○	△（企業ごとに異なる）			社内規程
認定情報技術者 CITP	○	○	○	○	○	情報処理学会
ACS，CIPS，CISSP など	○	○	○	○	○	法律には依拠せず

注　参考資料 15 から，CITP の企業認証関連記述を除き，RISS 関連記述と備考を追加した。

表 3 において，技術士法は，信用失墜行為の禁止，秘密保持義務，公益確保の責務，名称表示の場合の義務，資質向上の責務という professional として必要な義務を明記している。しかし，RISS では，信用失墜行為の禁止，秘密保持義務，受講義務（資質向上の責務と同等），名称の使用制限（名称表示の場合の義務と同等）を定めているが，公益確保の義務の定めはない。Professional に必須の

[21] ISO は各国の NB（民間組織）から構成される。また，各国際規格は Subcommittee(SC)/Working group(WG) が担当して制定，改正する。
[22] Competent は，having the necessary ability, knowledge, or skills to do something successfully という意味を持つ。Oxford Dictionary of English (2010)による。
[23] 表 1 に示した professional 試験を実施している ISC2 及び ISACA はオブザーバとして出席している。
[24] A 認証機関と B 認証機関で相互認証可能になれば，A 認証機関で認証され他資格保持者は B 認証機関でも同等の資格保持者とみなされ，資格保持者の国内・国際での流動性が確保される。
[25] Software Engineering – Certification of Software Engineering Professionals – Comparison Framework
[26] 次の資料を参考にした。旭寛治　認定情報技術者制度(1)～制度の概要～，情報処理，Vol.55，No.8，Aug.2014

倫理規範を欠いている。もっとも，RISS は Registered Information Security Specialist の頭字語であることから分かるように，professional とはいっていない。

５．今後の課題

筆者が 27021 の開発に携わった経験をもとに，情報セキュリティにおける professional の必要性と要員認証の一般的な枠組み，ISMS-P の役割と 27021 の考え方，27021 の開発経緯，SE を含め，IS 関連要員認証の現状及び問題点について述べてきた。

27021 の今後の課題であるが次の 3 点を考えている。

①27021 の見直しの必要性

発行間近ではあるが，既にいくつかの技術的誤りが指摘されている。ISO の規定では 3 年ごとの systematic review による改定，又は，緊急時の対処として Technical corrigenda and amendments（技術的正誤表と修正版）の発行がある。今後，対応を検討していきたい。また，BOK はこれまでの審議では十分に議論されていなかったので，改めて内容を吟味する必要がある。

②CISSP などの既存の要員認証機関が 27021 準拠を表明するか。

CISSP など国際的に実施されている認証機関は 17024 準拠を言明しているが，情報セキュリティ固有の要求仕様については各機関が独自に関発している。27021 との対応を言明すれば，複数の認証機関間の力量の範囲と内容が比較可能になる。相互認証の可否は各機関の経営判断であるが。

③情報システム学会が提唱する情報システムプロデューサの資格認証への展開

本稿のテーマとは対象が少しずれるが，情報システムプロデューサは ISSJ が提唱する新しい職種であり，“情報システムの企画・実現・活用を通じて，事業目標の達成と，事業の成長を推進していく”人材と定義されている（社会への提言 2017 年 5 月）。今後，資格化を検討することになれば，professional 資格を目指すべきであり，27021 で行ったような力量の定義，BOK の作成といった検討が必要になるであろう。研究発表大会の場で議論できれば幸いである。

６．謝辞

本研究は，2012 年度国士舘大学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 としての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。

附属資料　ISO/IEC 27021 の目次

Information technology -- Security techniques -- Competence requirements for information security management systems professionals

Foreword
Introduction
1 Scope
2 Normative references
3 Terms and definitions
4 Concept and structure
4.1 General
4.2 Concept of ISMS competence
4.3 Structure of ISMS competence
4.4 Demonstration of competence
4.5 Structure of this document
5 Business management competence for ISMS Professionals
5.1 General
5.2 Competence: Leadership
5.3 Competence: Communication
5.4 Competence: Business Strategy and ISMS
5.5 Competence: Organization design, culture, behavior and stakeholder management
5.6 Competence: Process design and organizational change management
5.7 Competence: Human Resource, team and individual management
5.8 Competence: Risk management
5.9 Competence: Resource management
5.10 Competence: Information systems architecture
5.11 Competence: Project and portfolio management
5.12 Competence: Supplier management
5.13 Competence: Problem management
6 Information security competence for ISMS professionals
6.1 ISMS Competence: Information Security
6.2 ISMS Competence: Information Security Planning
6.3 ISMS Competence: Information Security Operation
6.4 ISMS Competence: Information Security Support
6.5 ISMS Competence: Information Security Performance evaluation
6.6 ISMS Competence: Information Security Improvement
Annex A (informative) Including knowledge for ISMS professionals as part of a body of knowledg