

セキュリティ人材の確保に関する研究会  
中間報告

平成27年8月

セキュリティ人材の確保に関する研究会

## 目 次

### 1. はじめに

### 2. 情報処理技術者試験の現状と課題

- (1) 情報処理技術者試験
- (2) 情報セキュリティに関する試験

### 3. I T又は情報セキュリティに関する各種制度の概要

- (1) 公認システム監査人
- (2) 公認情報セキュリティ監査人
- (3) I Tコーディネータ
- (4) C I S S P

### 4. 情報セキュリティ人材像と制度設計の基本的方針

- (1) 必要となる情報セキュリティ人材像
- (2) 新たな制度の基本的方針

### 5. 情報セキュリティ人材の登録制度を構築するにあたっての論点

- (1) 登録制度導入の意義
- (2) 名称独占制度の必要性
- (3) 正式な資格名称
- (4) 更新条件に関する論点の検討
- (5) 既存の試験合格者などに関する経過措置
- (6) 資格登録者の責務
- (7) 登録制度の普及策

### 6. 終わりに

- (1) 登録制度の継続的見直し
- (2) 資格の国際性を目指して
- (3) 他の資格試験や情報処理技術者試験などの登録資格者としての取扱い
- (4) 登録制度は新たな始まり

# セキュリティ人材の確保に関する研究会報告書

## 1. はじめに

近年の情報技術の浸透に伴い、サイバー攻撃の件数は増加傾向にあり、その対象も個人から重要インフラ・行政までのあらゆる分野に広がり、その内容も巧妙化しているため、ひとたびインシデントが発生すると、被害が連鎖的に拡大したり、産業や生活など経済社会の基盤が著しく損なわれたりするおそれが高まっている。

このため、ネットワークにつながる全ての企業や個人が、それぞれの状況に応じて情報セキュリティを確保する必要が高まっており、情報システムを利用するユーザ企業等（以下「ユーザ企業」という。）の一部では、その必要性に関する意識が急速に高まりつつある。

ただし、残念ながら、未だにそうした意識が一部にとどまっている、又は、意識が高まっても具体的な取組につながっていない、という指摘がある。例えば、情報セキュリティの調達基準化やその検証方法について専門的な知識・技能をもって実行できる人材が少なく、的確な調達や検証ができていない、などである。

このため、ユーザ企業の意識を喚起し、取組を積極化させるべく、政府では、情報セキュリティの確保を含むガイドラインの作成に着手しており、今後ユーザ企業で取組が進むと見込まれる。

ユーザ企業でそうした取組が積極化すれば、体制を構築するために専門的な知識・技能を身に付けた人材の需要が高まり、これに呼応して、ベンダ企業でも、同様の人材を増やし社内の人材管理も必要となる。これらに質的・量的に応えられるよう、良質な情報セキュリティ人材を大量に育成し確保する必要がある。

また、平成27年6月に閣議決定された『「日本再興戦略」改訂2015』において、セキュリティリスクや高度化するサイバー攻撃への対策を確かなものとするべく、それを支える人材の育成が急務であるとした上で、2020年の東京オリンピック・パラリンピック競技大会の開催とそのための万全な情報セキュリティ体制の整備の必要性も念頭に置きつつ、「サイバーセキュリティに従事する者の実践的な能力を適時適切に評価できる試験制度の充実を図る」こととされている。

情報セキュリティ人材に関して、従来から、独立行政法人情報処理推進機構（以下「IPA」という。）が実施する情報処理技術者試験の中で、情報セキュリティの知識・技能を評価する情報セキュリティスペシャリスト試験（以下「SC試験」という。）が実施され、他の全ての試験区分で、平成26年度から関連する出題を強化・拡充している。

この情報処理技術者試験は、他の国家試験での優遇措置や官公庁の調達要件にされ、民間企業でも手当の対象や採用、登用時の考慮事項になるなど、官民で普及しているが、各試験の応募者数は減少傾向で、今後増大する情報セキュリティ人材の需要に対して、十分に供給できなくなる懸念がある。

以上を踏まえ、平成27年8月、経済産業省とIPAが事務局となって「セキュリティ人材の確保に関する研究会（以下「本研究会」という。）」が設置された。8月に5回の研究会を開催し、各種制度も参考にしつつ、産業構造審議会商務流通情報分科会情報経済小委員会IT人材ワーキンググループ（以下「人材WG」という。）で提示された、今後必要な3つの情報セキュリティ人材像をベースに制度の在り方を検討した。

その人材像とは、①ホワイトハッカーのような高度セキュリティ技術者、②ユーザ企業において、社内情報セキュリティ技術者と連携して企業の情報セキュリティ確保を管理する人材、③安全な情報システムを設計、開発、運用するために必要な情報セキュリティに関する知識・技能を身に付けた人材、である。

その結果は次のとおりであり、まず、3類型の人材全てについて育成・確保が必要であり、特に、②や③は大量の人材供給が期待される。

②については、平成28年春から情報セキュリティマネジメント試験の実施が予定されており、その応募者や合格者の状況を注視する。

③については、これまで試験合格後のフォローや試験合格者の情報がなかった点を改善し、定期的に実践的な能力を確認する更新制度や登録者の情報を公開する登録簿の整備等を柱とする制度を構築し、人材の質の担保と人定の可視化を提案する。

この成果を踏まえ、情報セキュリティ人材の育成・確保に向け、今後さらに取組を具体化するために、政府のみならず関係者がそれぞれの立場で制度の実現・普及に尽力していくことが求められる。

## 2. 情報処理技術者試験の現状と課題

### (1) 情報処理技術者試験

情報処理技術者試験は、情報処理技術者の不足と今後の需要の急増に対処するため、プログラマ認定制度創設への要望に応え、昭和44年に告示により「情報処理技術者認定試験制度」として創設された。その後、初回試験の大きな反響に鑑み、翌年に制定された「情報処理振興事業協会等に関する法律（昭和61年に「情報処理の促進に関する法律」に改正）」に制度の根拠を規定され国家試験として実施されている。

創設当初、第一種、第二種の2種類だった試験区分は、適宜見直され、平成6年に11区分、平成13年に13区分、平成21年に現在の12区分となった（ITパスポート試験、基本情報技術者試験、応用情報技術者試験、高度試験（9区分））。情報セキュリティに関しては、平成13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」（以下「SU試験」という。）が、平成18年に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」（以下「SV試験」という。）が創設され、平成21年に両試験を結合し「情報セキュリティスペシャリスト試験」が創設され、現在に至っている。

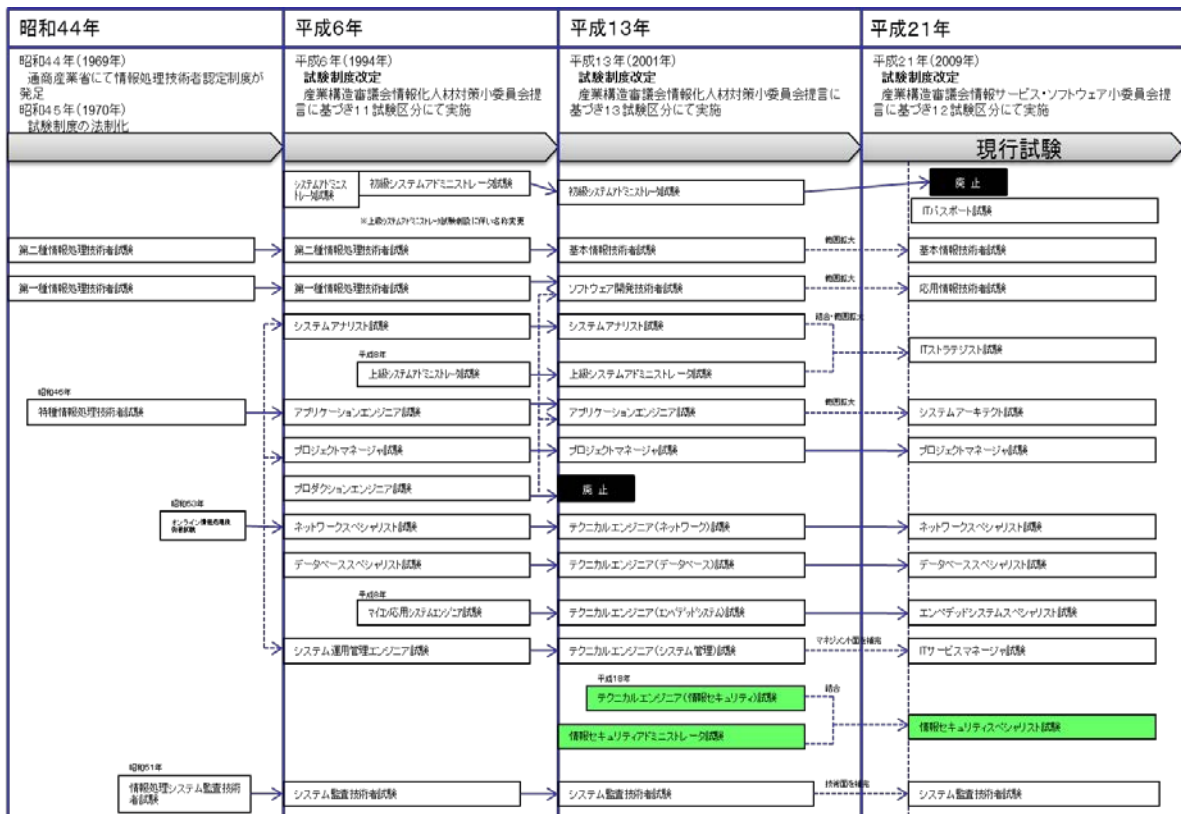


図1：試験区分の変遷

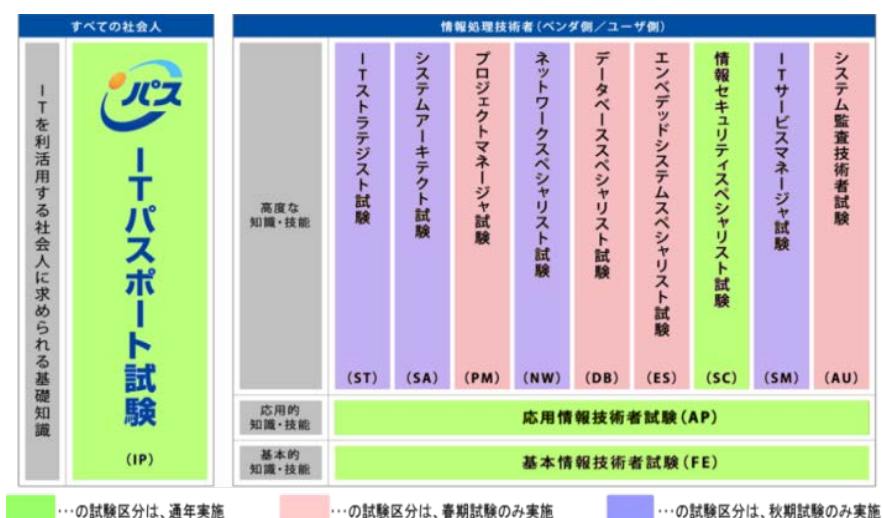


図2：情報処理技術者試験の全体像

試験のレベルは、入門から高度な技術分野まで広くカバーし、創設以来、累計で応募者数約1,820万人、合格者数約229万人に上る大規模な試験に発展した。

合格者は、中小企業診断士や弁理士の試験科目の一部免除、警察官採用試験（コンピュータ犯罪調査官）の応募条件など他の国家試験等で優遇措置を受けられ、官公庁では調達要件に、大学では奨学金給付や授業料減免の基準に活用され、企業等でもIT人材の育成や客観的な評価尺度として活用されるなど、官民の多数の機関で普及している。

#### 他の国家試験等における優遇措置

情報処理技術者試験（指定試験区分）の合格者は、他の国家試験などにおいて一部免除制度等の優遇措置が受けられる。また、警視庁をはじめ、各地方警察本部において、サイバー関連の捜査官の応募条件としても活用されている。

<ul style="list-style-type: none"> <li>・中小企業診断士試験、弁理士試験 → 科目の一部免除</li> <li>・教員採用試験 → 学科の一部免除など</li> </ul>	<ul style="list-style-type: none"> <li>・警察官採用試験（コンピュータ犯罪捜査官＝サイバー犯罪捜査官） → 応募資格（警視庁、千葉、群馬、茨城 等）</li> </ul>
---	--

#### 大学における優遇措置

情報処理技術者試験の合格者に対して、奨学金の給付、入学料免除や授業料減免などの優遇措置をする学校が存在。また、合格者に対し、入試優遇、単位認定、受験対策支援講座を実施している学校が数多く存在。高等教育機関においても高い評価を得ている。

入試優遇	157校
単位認定	119校
受験対策支援講座の実施	167校

【IPA調査】全国の大学・短大

#### 官公庁における調達要件(企業の技術力の指標)

- 政府は、政府におけるITガバナンス強化のため、情報システム調達やプロジェクト管理に関する共通ルール等を定める「政府情報システムの整備及び管理に関する標準ガイドライン」と「実務手引書」を新たに策定。この「実務手引書」の中で、調達における情報システム構築側への人材要求要件として、当試験の合格者などの有資格者を含め、実質的な能力及び技術力を備えた人材の参画を要求としている。
- 地方公共団体（北海道、山梨県、大阪府、広島県、大分県など）の情報システム開発の競争入札参加資格において、情報処理技術者試験の合格者を求めている。

図3：官民での活用状況

応募者数は平成14年度の80万人をピークにその後は減少傾向にあり、平成21年度の新試験創設を含む制度改正により、平成22年度にいったん62万人まで回復したものの、平成23年度の東日本大震災以降、再び減少に転じ、平成26年度は46万人とピーク時の約57%まで減少している。

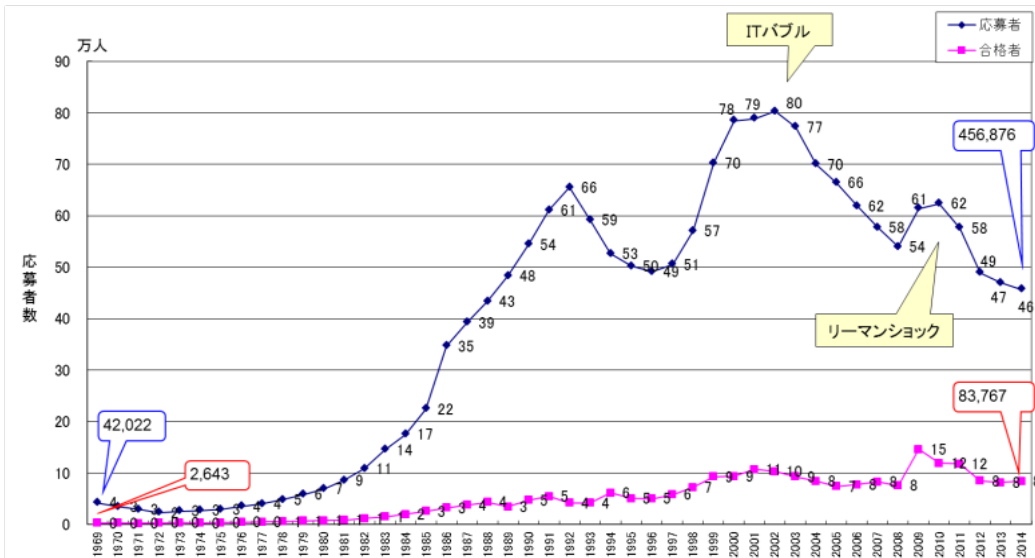


図4：応募者数、合格者数の推移

情報セキュリティ関係の試験区分の応募者数は、平成18年度に6.3万人とピークを迎え、その後は情報処理技術者試験全体と同様に減少傾向にあったものの、平成21年度に増加に転じ、平成22年度に5.9万人に達して以降は5万人台をキープし、平成13年の情報セキュリティ関係の試験区分創設時（2.3万人）に比べると大幅に増えている。また、合格者数は平成21年度以降5千人台で、受験者数に対する合格率は14%前後で推移している。

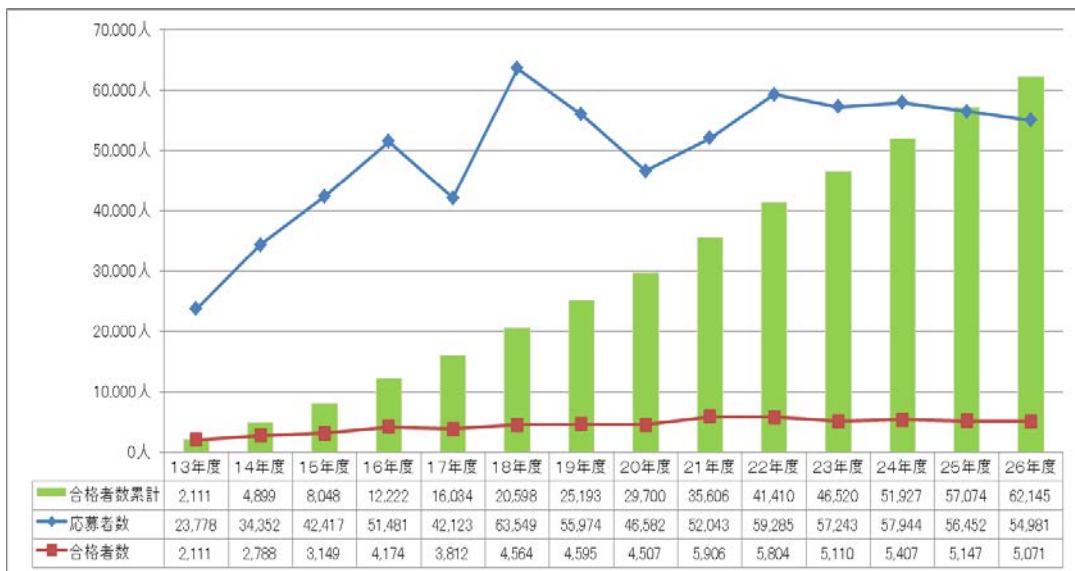


図5：情報セキュリティ関係の試験区分の応募者数、合格者数の推移

国際的にみても、我が国が提唱した「アジアITスキル標準化イニシアティブ」に基づき、インド、シンガポール、韓国、中国、フィリピン、タイ、ベトナム、ミャンマー、台湾、マレーシア、モンゴル、バングラデシュの12か国・地域との間で、相互認証が

行われており、IT人材の流動性の向上・有効活用に寄与している。また、フィリピン、タイ、ベトナム、ミャンマー、マレーシア、モンゴル、バングラデシュの7か国で、同じ日の同じ時間に同じ問題を使用した共通統一試験が実施されており、IPAが情報処理技術者試験の経験・ノウハウを活かして貢献している。

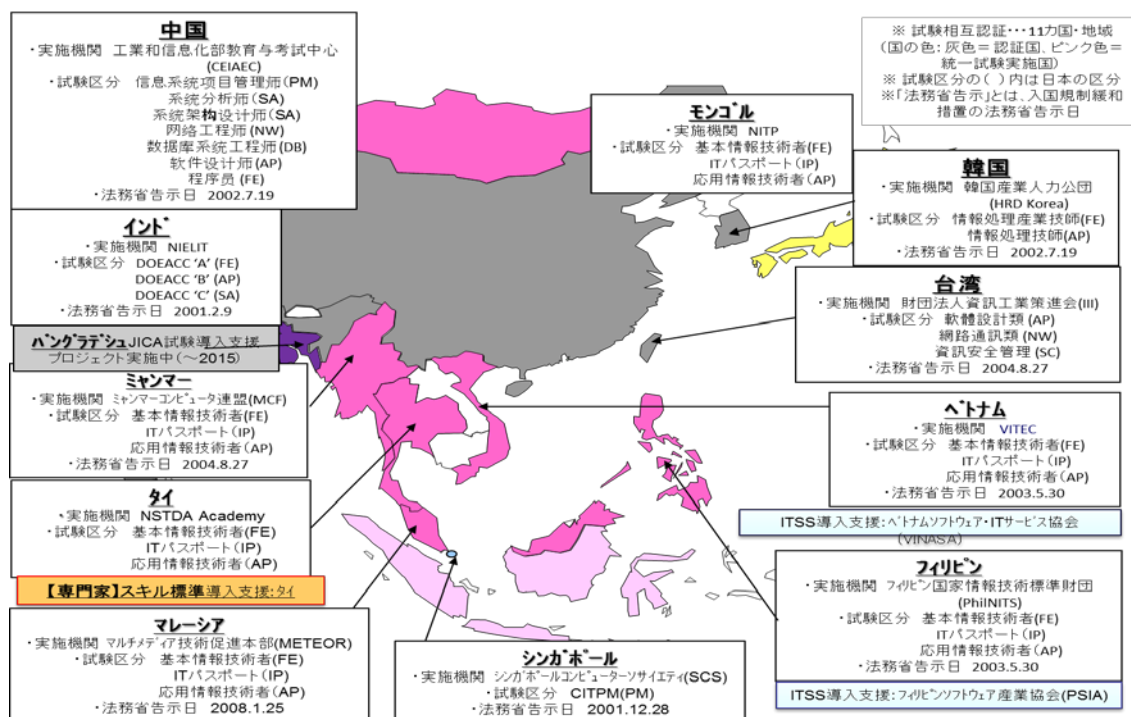


図6：相互認証の状況

## (2) 情報セキュリティに関する試験

前述した変遷を経て平成21年にSC試験が創設され、現在に至っている。また、平成26年度からITパスポート試験や基本情報処理技術者試験、応用情報技術者試験でも情報セキュリティ関係の出題比率を高くするなど、全ての試験区分で情報セキュリティに注力している。

SC試験の規模は、応募者数が毎年5～6万人で推移しており、現在までの約6年間で、応募者数のべ36.5万人、合格者数35,068人にのぼっている。なお、前身のSU試験及びSV試験の合格者は、それぞれ、24,796名、4,904名である。

情報セキュリティ分野でのSC試験の浸透度を合格者の属性からみると、ベンダ企業の情報セキュリティ部門の従事者のうち、情報処理技術者試験のいわゆる高度試験（SC試験など、応用技術者試験よりも一つ高いレベル4の試験9区分）の合格者を100とすると、約2/3に相当する64.4%がSC試験の合格者である。また、SC試験の合格者を100とすると、情報セキュリティ部門の従事者は4.8である。全ての試験区分の合格者を100として情報セキュリティ部門の従事者が1.4であることと比



べると、約3.4倍特化している。情報セキュリティの分野ではSC試験が十分に浸透し、しっかりと根付いているものと思われる。

試験区分	ST	PM	SA	NW	DB	ES	SC	SM	AU	合格者合計
合格者割合	2.1%	2.6%	1.3%	19.0%	4.2%	1.3%	64.4%	2.4%	2.6%	100%

表1. 情報セキュリティ部門従事者が合格している高度試験区分の比率  
(平成26年度、IPA作成データを加工)

試験区分	ST	PM	SA	NW	DB	ES	SC	SM	AU	FE	AP	全試験平均
従事者割合	1.2%	0.7%	0.6%	3.9%	1.0%	0.8%	4.8%	1.8%	2.8%	0.8%	1.0%	1.4%
全試験平均比	0.9	0.5	0.4	2.8	0.7	0.6	3.4	1.3	2.0	0.6	0.7	1.0

表2. 各試験区分及び全試験の合格者のうち情報セキュリティ部門従事者の割合  
(平成26年度、IPA作成データを加工。下段は全試験平均を1.0としたときの比)

(凡例) ST: ITストラテジスト試験、PM: プロジェクトマネージャ試験、SA: システムアーキテクト試験、NW: ネットワークスペシャリスト試験、DB: データベーススペシャリスト試験、ES: エンベデッドシステムスペシャリスト試験、SC: 情報セキュリティスペシャリスト試験、SM: ITサービスマネージャ試験、AU: システム監査技術者試験、FE: 基本情報技術者試験、AP: 応用情報技術者試験

しかし、試験合格後のフォローがなく、最新の動向を踏まえて専門的な知識・技能が維持されているか確認できないなどと指摘する声もあり、前述のような応募者数の推移を考えると、今後とも、最新の情勢、社会的に求められる人材を的確に把握し、不断に見直しすることにより、情報セキュリティ人材を育成していくことが求められている。

### 3. IT又は情報セキュリティに関する各種制度の概要

IT又は情報セキュリティに関する制度については、これまでも様々な制度が実施されており、運営している団体から制度の概要や運営に関する状況を聴取及び調査した。ここでは、各種制度の概要について簡記する。詳細については第2回研究会の配布資料<sup>i</sup>を参照されたい。

#### (1) 公認システム監査人

創設の経緯は、平成11年に、産業構造審議会情報化人材対策小委員会の中間報告を受けて、特定非営利活動法人日本システム監査人協会において平成14年7月に「公認システム監査人制度」を創設したものであり、システム監査人に相応しい「実務経験」と「継続的な能力の維持・向上」に努めているかを評価する。資格は、「公認システム監査人（以下「CSA」という。）及び「システム監査人補」（以下「ASA」という。）の2種類を認定し、平成27年現在、CSA330名、ASA92名が認定されている。

登録までの仕組みは、情報処理技術者試験のうち、システム監査技術者試験（以下「AU試験」という。）の合格者を対象に、一定の継続教育を受けることを条件としてASAを認定し、さらにASAを対象に、2年以上のシステム監査の実務経験を審査しCSAとして認定し、同協会に登録する。また、併せて提出した監査実務経歴書に基づきテーマ選定し小論文を執筆させるとともに、概ね30分程度の面接試験を実施している。

なお、AU試験と関連のある資格所有者（例：他区分の情報処理技術者試験合格者、中小企業診断士、公認会計士、技術士、ITコーディネータ等）については、特別認定制度により一定の教育を受けることなどを条件として同様に認定している。資格認定の期間は2年間であり、更新の際の条件には、CSAは、2年間で80時間（ASAは40時間）の継続教育を受講することとされ、10年連続更新者については特例として56時間とされている（同28時間）。手数料に関しては、認定及び更新のいずれについても、CSA：21,000円（会員）、31,500円（非会員）、ASA：10,500円（会員）、15,750円（非会員）となっている。

#### (2) 公認情報セキュリティ監査人

平成15年に経済産業省により告示された「情報セキュリティ監査制度」のもとで、特定非営利活動法人日本セキュリティ監査協会において、公正かつ公平な情報セキュリティ監査を目指して実施された。情報社会にとって有益なものとして機能することをめざし、情報セキュリティ監査人に求められる知識・経験・技術に応じて、「公認情報セキュリティ主任監査人」「公認情報セキュリティ監査人」「情報セキュリティ監査人補」「情報セキュリティ監査アソシエイト」「公認情報セキュリティ主席監査人」の4種類を認定している。

<sup>i</sup> [http://www.meti.go.jp/committee/kenkyukai/shoujo/security\\_jinzai/002\\_haifu.html](http://www.meti.go.jp/committee/kenkyukai/shoujo/security_jinzai/002_haifu.html)

資格認定の手続きとしては、同協会認定の研修コースを受講し修了試験に合格した者に対して、資格登録を認めるが、公認情報セキュリティ監査人及び同主任監査人の2つについては、監査経験を確認するための小論文を受験し合格することが求められ、主任監査人については、更に面接審査が実施されている。現在の登録者は全ての資格を合計して約1,000名となっており、資格保有者の名簿は本人の同意を前提に公開している。

制度創設当初は、以前から監査業務に従事していた者について、小論文の執筆と経験を認定して資格者とした。資格認定の期間は3年間で、年度ごとの一定ポイント取得と3年間での合計取得ポイントの2段階で資格及び専門性の更新を行っている。

具体的には、資格の社会的な要請に合わせて、監査実績時間数に加えて、研修・セミナーの受講や自己学習、関連する他の資格の取得などをポイントに換算して蓄積。同時に、資格維持に関しては、一定割合を抽出して真正な資格維持の活動に関してエビデンスの提出を求めるなどを実施するとともに、海外勤務や異動等によって監査業務に従事することが困難だった者に対して資格保留制度を実施している。資格登録時に20,736円、資格の有効期限（3年間）までに毎年15,552円、更新時には20,736円が手数料として設定されている。

### (3) ITコーディネータ

最新の経営とITの知識を日々学習し、学習で得た知識を実務を通して磨き、最適なIT経営をコーディネートするための実務能力を維持・向上する仕組みを提供することを目的として、特定非営利活動法人ITコーディネータ協会が、平成13年から実施している資格更新制度である。

ITコーディネータ試験の合格と6日間の集合研修やeラーニングの受講を経て資格登録される。平成27年3月末現在、累計の資格取得者は11,181名、資格を維持している資格登録者は6,241名となっている。資格登録者からの業務経歴等の情報が提供されれば公開することとなっている。

資格の有効期間は、4月1日から翌年3月31日までの1年間で、毎年度更新が必要である。資格更新に関しては、ITコーディネータの活動実績をポイントで表し、その成果を可視化し、更新可否を判定している。

具体的には、継続学習と実務活動のスキルとキャリアの両面での活動を義務付け、これらのポイント換算により更新を判定する仕組みである。ポイント制度は実務活動と学習活動の区分からなり、両方をバランスよく取得することを奨励する。年間合計で10ポイント以上を更新条件とする。更新手数料は21,600円/年となっている。

#### (4) C I S S P

国外では、情報セキュリティへのニーズの高まりに応じ、(ISC)<sup>2</sup>がC I S S P (Certified Information Systems Security Professional)を実施するなど、民間で登録制度が実施されている。C I S S Pは1995年に開始され、国際的、普遍的に必要な知識を理解する情報セキュリティプロフェッショナルを認定するもの。米国を中心に世界で6万人超の資格者がおり、我が国では千数百名ほどの資格保持者がいるとされる。

試験に合格し、業務経験を簡記した書類や他の資格者からの推薦状などを提出して登録される。3年に一度の更新が必須であり、更新条件は、関連セミナーや関係団体の会合への参加、ボランティア、執筆活動、関係雑誌の購読等を通じて得られる合計ポイントが一定以上であること。ただし、職務経験はポイントにカウントしない。手数料は、試験時に試験費用として599ドル、更新時に会費として255ドルが必要である。

制度	実施主体	登録のための試験費用 <>内は受験要件	登録要件	更新要否	更新期間	更新要件 <>内はポイントとなる活動
公認システム監査人	日本システム監査人協会	21,000円(会員)、31,500円(非会員)	<ul style="list-style-type: none"> <li>システム監査技術者試験合格</li> <li>実務経験2年以上</li> <li>小論文</li> <li>面接試験</li> </ul>	必須	2年	<ul style="list-style-type: none"> <li>2年間で80時間の継続教育</li> <li>＜協会主催の教育、講演会・研究会、実務、論文、出版、普及啓発活動＞</li> <li>更新料(21,000円(7,000円/年)(会員)、31,500円(10,500円/年)(非会員))</li> </ul>
公認情報セキュリティ監査人	日本セキュリティ監査協会	研修終了試験5,184円、トレーニング修了試験10,368円、監査経験確認試験10,368円 登録手数料20,736円	<ul style="list-style-type: none"> <li>認定研修、トレーニング受講・修了試験合格</li> <li>監査経験確認試験合格</li> <li>情報技術で4年以上、情報セキュリティで2年以上の実務経験</li> </ul>	必須	3年	<ul style="list-style-type: none"> <li>ポイント(3年間120P)</li> <li>＜研修セミナーの受講、社内研修等の受講、情報セキュリティ監査に関連する資料の閲覧、他資格の取得、監査実績＞</li> <li>更新料(有効期限まで毎年15,552円、更新時に20,736円(約6,900円/年))</li> </ul>
ITコーディネータ	ITコーディネータ協会(NPO)	19,440円 一部免除：9,720円	<ul style="list-style-type: none"> <li>試験合格</li> <li>ケース研修の受講修了(6日間、21.6万円)</li> </ul>	必須	毎年	<ul style="list-style-type: none"> <li>ポイント(3年間30P)</li> <li>＜実践活動、協会活動、セミナー受講、機関誌購読、関連他資格取得等＞</li> <li>実務活動報告の提出</li> <li>更新料(21,600円/年)</li> <li>研修(2回目まで：4~9万円)</li> </ul>
CISSP (Certified Information Systems Security Professional)	(ISC) <sup>2</sup> (International Information Systems Security Certification Consortium)	599ドル(74,276円) <small>＜CISSPに関する再試験期間が約10分の一のうちに2回もしくは3回以上以上の分野において卒業し、(卒業後またはISC)2が定める資格の取得後(4年以上)のCPDプログラムとして履修が義務づけられていること＞</small>	<ul style="list-style-type: none"> <li>4-5年間の業務経験</li> <li>試験合格(1,000点中700点以上)</li> <li>推薦状(他の資格者からの)</li> <li>無作為監査合格</li> </ul>	必須	3年	<ul style="list-style-type: none"> <li>ポイント(3年間120P)</li> <li>＜セミナー受講、セキュリティ団体年会、ベンダとの打合せ、大学院コース参加、執筆、自己学習、ボランティア、セキュリティ雑誌定期購読等＞</li> <li>倫理規約遵守</li> <li>会費(3年255ドル(31,620円)(85ドル/年))</li> </ul>
CISM (Certified Information Security Manager)	ISACA (Information Systems Audit and Control Association 情報システムコントロール協会)	会員：445~495ドル(55,180円~61,380円) 一般：595~645ドル(73,780円~79,980円)	<ul style="list-style-type: none"> <li>試験合格(800点満点で450点以上)</li> <li>過去10年以内の経験(最低5年間)</li> </ul>	必須	3年	<ul style="list-style-type: none"> <li>職業倫理規定遵守</li> <li>毎年最低20時間(3年間で120時間)の継続専門教育(CPE)</li> <li>毎年継続専門教育の維持費用(会員：45ドル(5,580円)、非会員：85ドル(10,540円))</li> </ul>
PMP (Project Management Professional)	PMI (Project Management Institute)	会員405ドル(50,220円) 一般555ドル(68,820円) ＜4500(7500)時間以上の実務、36(60)ヶ月のPM経験、35時間のPM研修＞	<ul style="list-style-type: none"> <li>PMP試験合格</li> </ul>	必須	3年	<ul style="list-style-type: none"> <li>ポイント(3年間60P)</li> <li>＜研修受講、書籍読解等の自習、記事・書籍の執筆、講演、ボランティア、実務活動等＞</li> <li>更新料(会員60ドル(7,440円)(20ドル/年)一般150ドル(18,600円)(50ドル/年))</li> </ul>
認定情報技術者	情報処理学会	5,100円 ※情報処理技術者試験の受験料	<ul style="list-style-type: none"> <li>情報処理技術者試験の合格(ES、AU以外の高度試験)</li> <li>業務経歴書</li> <li>推薦書</li> <li>申請料(2万円)</li> <li>登録料(1万円)</li> </ul>	任意	3年	<ul style="list-style-type: none"> <li>ポイント(3年間150P)</li> <li>＜研修等受講・講師、研究会発表、論文掲載、著作、公的団体貢献、特許等の技術的成果、資格取得等の自己学習等＞</li> <li>業務実績(レベル4以上の役割で1,800時間以上の実績)</li> <li>更新料(1万円(約3,300円/年)(予定))</li> </ul>
技術士(CPD)	日本技術士会	一次試験：11,000円 二次試験：14,000円 ※一次試験合格後実務経験(4~7年)が必要	<ul style="list-style-type: none"> <li>技術士登録</li> <li>ポイント(3年150P)</li> <li>CPD会員申請料(3千円)</li> </ul>	任意	3年	<ul style="list-style-type: none"> <li>ポイント(3年間150P)</li> <li>＜研修等受講、論文発表、業務経験、公的資格取得、公的委員、自己学習等＞</li> <li>更新料(会員)(3千円(1,000円/年))</li> </ul>

図7：各種制度の概要と比較

#### 4. 情報セキュリティ人材像と制度設計の基本的方針

ここでは、必要となる情報セキュリティ人材像と制度設計の方向性を整理した。具体的には、人材WGで提示された情報セキュリティに関する人材像を確認し、制度設計の概要や考慮すべきステークホルダの関心など基本的方針を整理した。

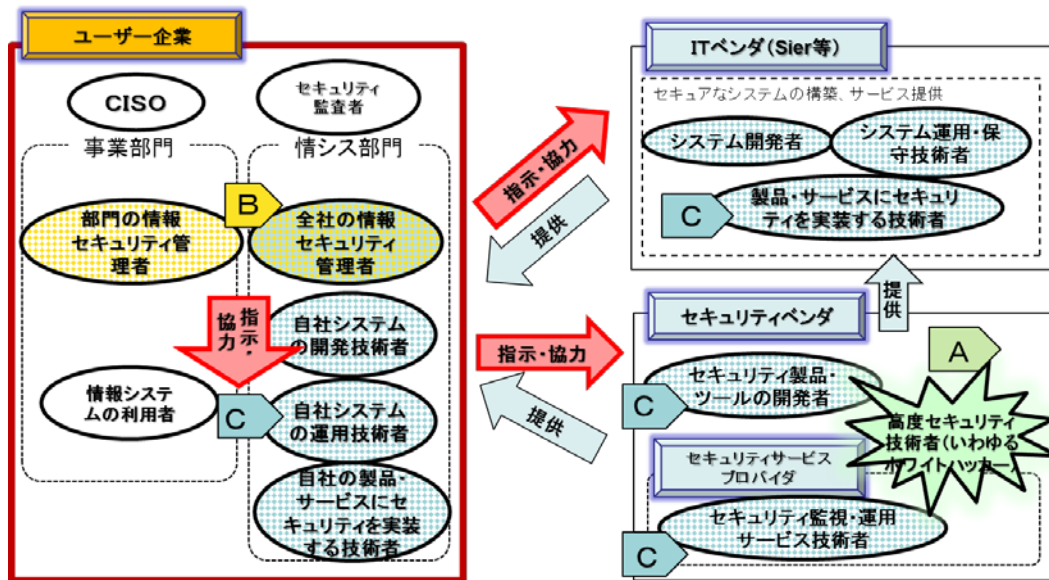
##### (1) 必要となる情報セキュリティ人材像

今後増大していくと見込まれる人材像は、ユーザ企業やベンダ企業に在籍し、専門的な知識・技能に基づいて互いにコミュニケーションをとりつつ、企業の情報セキュリティを確保していく人材である。

これに対して、人材WGでは今後必要となる情報セキュリティ人材像として、

- A. ホワイトハッカーのような高度セキュリティ技術者、
- B. ユーザ企業において、社内情報セキュリティ技術者と連携して企業の情報セキュリティ確保を管理する人材、
- C. 安全な情報システムを設計、開発、運用するために必要な情報セキュリティに関する知識・技能を身に付けた人材、

の3類型が提示されている。



参考1：第2回人材WG（平成27年3月25日開催）配付資料を一部加工

このうち、A. については、IPAが、民間企業とも連携しつつ、最新の知識・技能を伝授する場として、若年層情報セキュリティ人材の育成合宿（セキュリティ・キャンプ）を平成16年度から実施しており、国際的に活躍する人材も輩出するなど一定の成果を挙げている。こうした人材は、我が国の情報セキュリティ技術の頂点にあり、我が

国の総合的な情報セキュリティ水準の向上につながる人材として今後も育成に注力しなければならない。

しかし、必要となる人材像は、冒頭に述べたとおりユーザ企業やベンダ企業に広く普及することが見込まれており、A. のように情報セキュリティ技術の頂点に立つほどの知識・技能を持つ希少な人材だけでは量的に対応することは困難である。

B. については、一定の知識・技能を持ち、社内の情報セキュリティ技術者と連携して情報セキュリティ対策の実務をリードする人材であり、情報セキュリティの確保に向けた取組を進めようとするユーザ企業にとって重要な人材である。

こうした人材を評価するために、IPAが新試験（情報セキュリティマネジメント試験）を平成28年春から実施する予定である。各企業に複数名必要となる人材であるため、ユーザ企業を中心に、人材確保が進むように、政府、IPAには大いに期待したい。

ただし、現段階では試験の応募者やレベルが不明確であるため、新試験の合格者を後述の対象とすべきとまでは判断できなかった。当面は社会全体の情報セキュリティの向上に資する重要な試験として、充実・普及を期待したい。

C. は、安全な情報システムを設計、開発、運用するために情報セキュリティに関する知識・技能を網羅しつつも部分的には詳細に指摘できるだけの知識・技能を有する人材であり、従来からベンダ企業には存在していたものの、ユーザ企業には一部の業種にしか存在していなかった。

このため、ユーザ企業が情報セキュリティの専門的な知識・技能に基づいて調達基準の作成やその検証が十分にできなかった。ガイドライン等で提示しようとしている人材は、これに対応できベンダ企業と相互にコミュニケーションのとれる人材である。

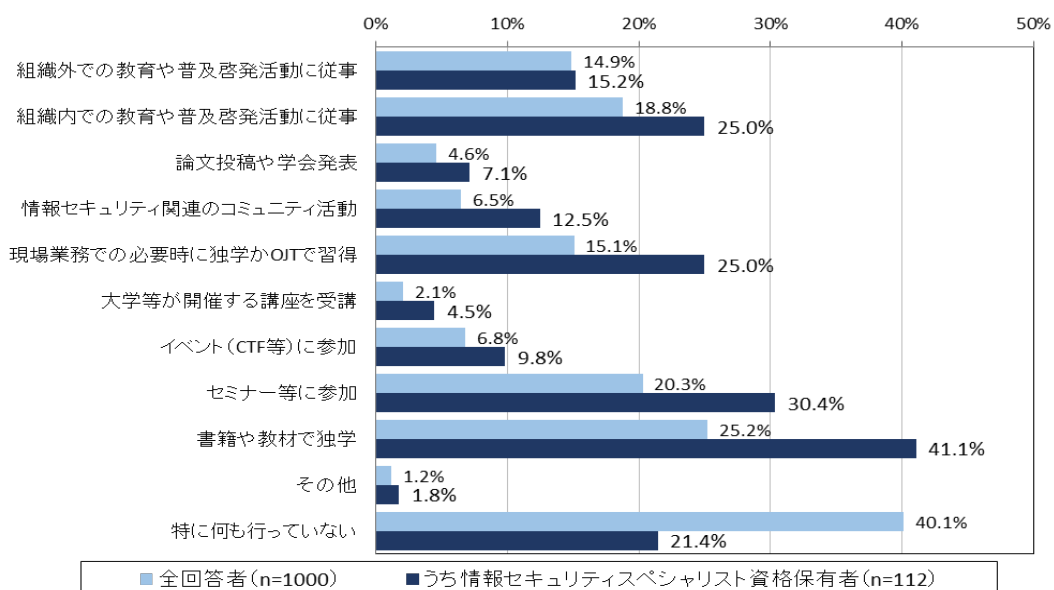
IPAは、従来からSC試験を実施し受験時点での知識・技能を測定しているが、ソフトウェア等の脆弱性の発見件数は増加し、攻撃手法の巧妙化も進んでいるにもかかわらず、合格後に最新の知識・技能を継続的に習得するなどの資質向上の取組を行っているかどうか確認する仕組みがない、との指摘が本研究会でも出された。

また、「情報セキュリティ分野の資格に関するウェブアンケート」（調査委託先：みずほ情報総研株式会社、平成27年8月22日）（以下「ウェブアンケート」という。）の実施結果によれば、試験合格時に所属企業からの助成制度が一部についてあるのみで、昇進や昇格の要件としても5%程度であることから、必ずしも業務のインセンティブになっているか不明であるなど、最新の専門的な知識・技能の習得など、資質の維持・向上に向けたインセンティブが働かない状況にある。

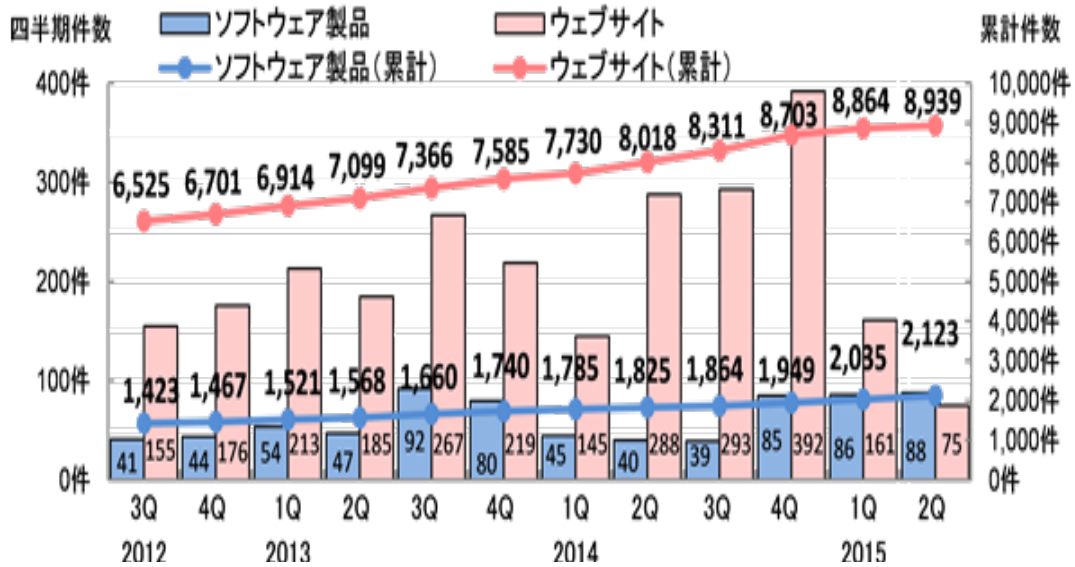


N=1000		受験料の助成制度（補助金支給など）	社内で試験対策講座を実施している	社外の試験対策講座の受講に対する助成（補助金支給など）	試験合格者（報奨金等）が支給される	試験合格者に対して、継続的な合格者手当等が支給される	社年次や職種などによって、最低限の合格すべき試験が決められている	試験合格が人事上の昇進・昇格の要件の一つになる	試験合格が、スキル標準に基づいて認定の要件の一つになる	左記には特にあてはまらないが、試験合格を推奨している	左記のいずれにもあてはまらないう（受）	試験合格者の有無や数などを外部発注時の要件に含めている	自社の合格者数を公表している	あてはまるものはない
1	情報セキュリティスペシャリスト試験	20.9%	4.7%	5.7%	20.4%	4.4%	2.2%	4.8%	4.2%	4.8%	6.3%	0.6%	6.9%	27.4%
2	システム監査技術者試験	17.7%	3.5%	5.3%	18.2%	4.5%	1.8%	4.4%	3.9%	4.4%	6.3%	0.8%	6.3%	31.7%
3	CISSP認定資格	8.6%	1.4%	2.1%	7.0%	1.8%	0.9%	1.7%	1.7%	3.5%	8.3%	0.2%	1.6%	48.9%
4	公認情報システム監査人	8.6%	1.5%	2.6%	7.1%	1.7%	1.3%	1.7%	2.2%	3.2%	8.4%	0.5%	1.7%	48.8%
5	公認情報セキュリティ監査人	8.0%	1.6%	2.3%	6.9%	1.8%	1.1%	1.6%	1.9%	3.1%	8.6%	0.3%	1.6%	49.4%
6	公認情報セキュリティマネージャー	8.2%	1.5%	2.2%	7.1%	1.7%	1.1%	1.9%	1.7%	2.8%	8.6%	0.5%	1.6%	49.6%
7	情報セキュリティ専門監査人	8.1%	1.4%	2.5%	6.7%	1.7%	1.0%	1.8%	1.9%	2.9%	8.8%	0.6%	1.8%	49.2%
8	GIAC認定試験各種	7.4%	1.0%	1.9%	5.5%	1.0%	1.0%	1.3%	1.7%	2.5%	8.5%	0.4%	1.1%	52.7%
9	Comp TIA Security+	7.4%	1.4%	2.0%	6.2%	1.1%	0.6%	1.3%	1.5%	2.4%	9.0%	0.1%	1.3%	51.7%
10	ネットワーク情報セキュリティマネージャー資格制度	7.8%	1.4%	2.2%	6.6%	1.4%	1.3%	1.5%	2.1%	2.8%	8.4%	0.2%	1.6%	50.8%
11	ISMS審査員	7.2%	1.3%	2.2%	5.9%	1.2%	0.9%	1.8%	1.8%	3.1%	8.5%	0.2%	1.7%	50.6%
12	ITコーディネータ	9.4%	1.5%	2.9%	7.5%	1.5%	1.0%	1.8%	2.3%	2.9%	8.5%	0.2%	2.1%	47.6%
13	Project Management Professional	12.4%	3.5%	4.0%	9.0%	1.8%	1.2%	2.8%	3.1%	3.3%	8.2%	0.4%	3.6%	43.1%

参考2：勤務先における資格・認定制度に関する制度や取組の有無（ウェブアンケート）



参考3：情報セキュリティに関する知識・スキルの習得方法について（ウェブアンケート）



参考4：ソフトウェア等の脆弱性届出の四半期ごとの推移

(出典：IPA「ソフトウェア等の脆弱性関連情報の取扱いに関する活動報告レポート」)

## (2) 新たな制度の基本的方針

前述を踏まえ、社会からの期待と信頼にこたえられるような新たな制度を以下のとおり提案する。

### ① 新たな制度の対象と骨格

A. の人材の発掘・育成に関する取組は継続・改善を期待するとともに、B. については、情報セキュリティマネジメント試験の開始後の状況を注視していく。C. について、上記の課題 ii を解決し、実践的な能力を適時適切に評価できるよう制度を改善すべく、SC試験をベースとした登録制度を構築していく方向で意見がまとまった。

ii 『新・情報セキュリティ人材育成プログラム』（平成26年5月情報セキュリティ政策会議決定）では、継続学習の重要性が指摘されている。以下、該当部分抜粋。

「情報通信技術を取り巻く環境が急激に変化している中で、情報処理技術者試験では引き続き最新の技術動向等を踏まえた出題が求められる。また、情報セキュリティに対する実践的な能力を常に評価・担保できる試験、資格・認証制度として位置付けられるよう、例えば海外の民間資格のように合格後に継続教育を設けるとともに、情報セキュリティ人材の能力を認証する等、試験制度に関する在り方についての検討を進める。また、それに先駆け、政府や企業においては情報処理技術者試験の合格年次で判断することや、同試験では合否のみでなく結果を点数でも表示されることから、繰り返し受験することを促すなどの取組が重要である。

また、情報セキュリティの分野は進歩が著しい分野であり、情報セキュリティ技術者として求められる能力・知識も進歩していくことから、資格等の整備においては常に最新の情報を身につけられるような教材や習得の場などの環境整備を行っていくことも重要である。」



なお、本研究会では、ここで検討したA. B. C. の3類型の人材供給で情報セキュリティが確保されるとの認識ではなく、IoTの進展等に伴い、ネットワークに接続する全ての者に、情報セキュリティの意識喚起や維持・向上が必要である。

## ② 登録者数

登録者は、各企業で情報セキュリティの確保に取り組むため、数万人規模になると想定される。また、平成26年7月に公表されたIPAの推計でもユーザ企業での情報セキュリティ人材の不足数が8万人超であるとされている。社会全体の情報セキュリティ水準を向上すべく、これらの人材不足数に対しインパクトのある規模で供給する必要がある。

この点、情報セキュリティマネジメント試験によってB. に関して相当数の人材供給が期待される。登録制度の登録者数も、万人単位で確保すべきであり、必要に応じて見直していくこととなろうが、当面は2020年に3万人を超える人数とすることを目標とすべき、という概ねの意見の一致をみた。

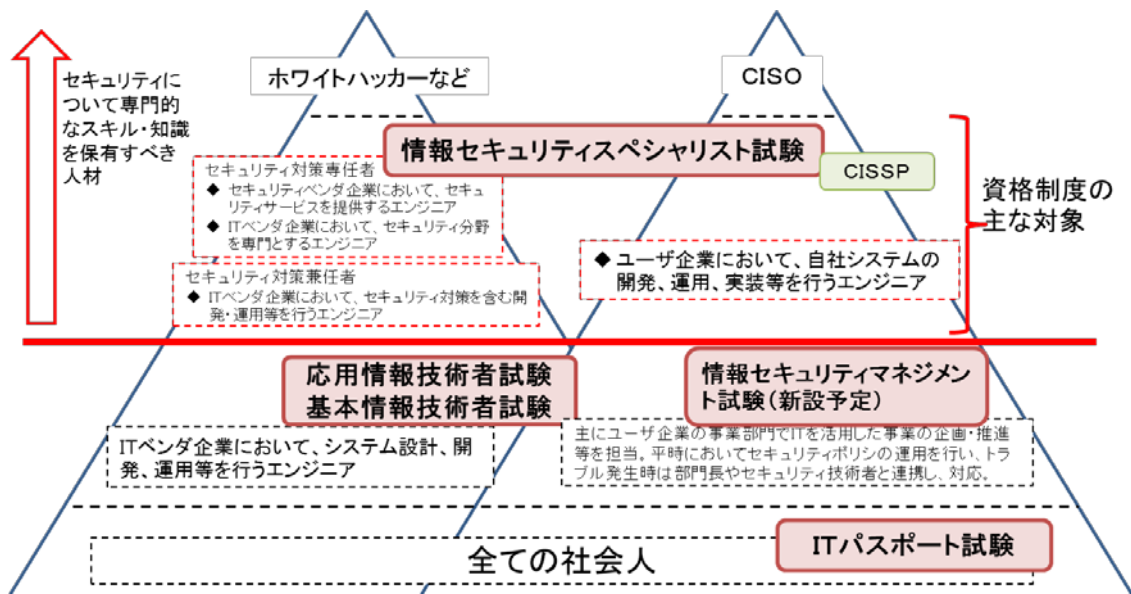


図8：情報セキュリティ人材のスキル・知識の全体像と試験や登録制度のマッピング

## ③ 制度のステークホルダの関心

制度の設計には、普及浸透のために、制度を取り巻くステークホルダの関心を踏まえて設計すべきである。具体的には、ア. 資格登録者、イ. ベンダ企業、ウ. ユーザ企業、エ. 登録制度運営者、の4者であり、その関心事項は、1) 制度の浸透や社会的評価、2) 有益性、3) 情報セキュリティ人材の質、4) 自立的運営の4つである。

### 1) 制度の浸透や社会的評価（権威性）

ユーザ側がコストをかけて登録制度を活用することに経済合理性を見出せるよう社

会的評価を高める必要がある。

具体的には、情報セキュリティ関係者が一目置くような著名な情報セキュリティの専門家が資格登録するよう促す、資格登録者のメディア登場を支援するなど考えられる。

## 2) 有益性

この登録制度の最終的な目的は情報システムのセキュリティ確保であり、そのメリットを最も享受するのはユーザ企業である。ユーザ企業がこのメリットを認識し、効率性とともな戦略性の観点から積極的に投資を進めることで、資格登録者は各企業で重用され、ベンダ企業も情報セキュリティ人材の単価増大によるメリットが得られる。登録制度はこうした Win-Win の関係にあることを広く認識してもらいたい。

具体策等については、制度の活用を推奨するガイドラインの提示や企業の情報セキュリティ対策評価などといった企業間取引への働きかけや企業間比較などが考えられる。

## 3) 情報セキュリティ人材の質

人材の質の向上・維持は、制度の根本にかかわる。これまでない更新制度を導入し、最新の専門的な知識・技能の習得を確認すべきである。詳細は後述する。

もちろん、質の維持・向上ばかりでなく、制度を通じて供給される人材の量など、社会的な意義やインパクトも勘案していく必要があることも指摘したい。

## 4) 自立的運営

制度運営の持続可能性を確保するため、ア) 制度運用コストと登録更新手数料の収支、イ) 登録者数・更新者数の規模の維持、ウ) 登録更新時に要する様々な負荷への対応、といった点について配慮が必要である。

したがって、登録制度運営にあたっては、2) 及び3) の両方の観点から量及び質を両立できるように、常に多様なユーザの声を広く聴取しバランス感覚を持って対応することを期待する。

## 5. 情報セキュリティ人材の登録制度を構築するにあたっての論点

具体的な登録制度の検討にあたっては、登録制度導入の意義をはじめ次の5つの論点で議論を進めた。以下では、本研究会で検討した登録制度の概要を提言していく。

- 論点1) 登録制度導入の意義について
- 論点2) 登録制度の対象となる試験や資格の範囲・名称
- 論点3) 登録制度の導入方法について
- 論点4) 試験・資格の普及・活用方策について
- 論点5) 登録制度導入に対しての経過措置

登録制度の全体像と上記の論点2)～5)との関係について、必ずしも最終的に運用される制度の姿とは完全には一致しないが、イメージは以下のとおり。

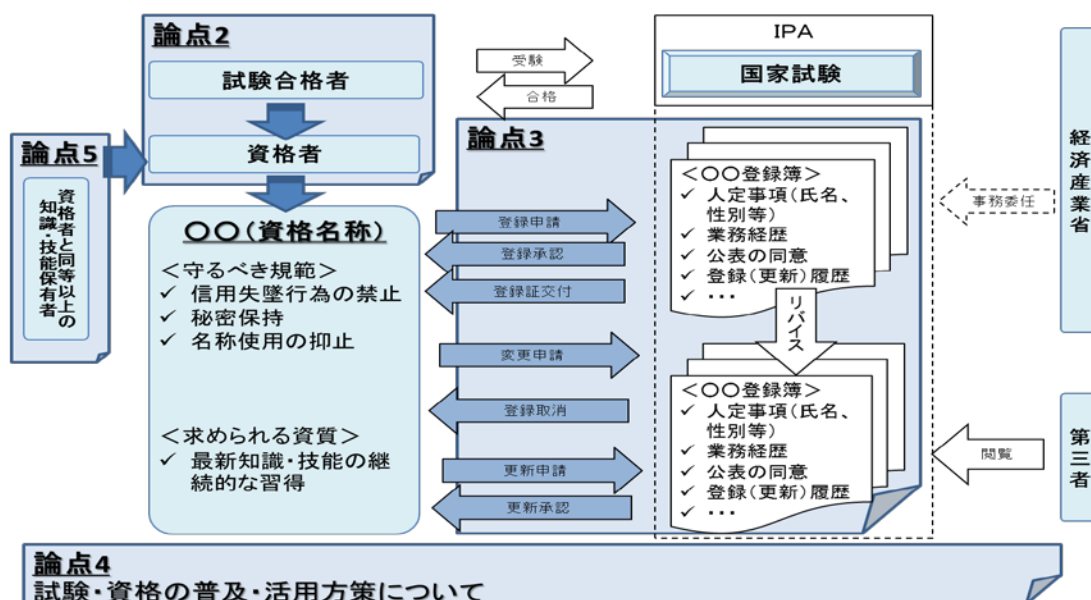


図9：登録制度の全体像と各論点の対応関係

### (1) 登録制度導入の意義

現在の試験制度で指摘される課題を解決するため、新たに、質と人定という2つの識別機能と実務経験の申告・公開機能を有する制度を提言する。

#### ① 更新制の必要性（最新知識保有など「質の識別機能」）

技術革新が著しいにもかかわらず、試験合格後も最新の知識・技能を継続的に保有していることを確認する手段がない。最新の知識・技能に追いついていない試験合格者の存在を指摘する声もある。

このため、例えば、一定の更新年限を定めて試験の一部を再受験させる、一定の実務経験を継続的に積む、最新の専門的知識を習得していることを確認するといった、更新時に一定の条件を課して知識・技能の陳腐化を防止する制度を創設し、資格登録者であ

れば最新の専門的知識・技能を有していることを識別できるようにする。

## ② 登録制の必要性（試験合否情報など「人の識別機能」）

情報セキュリティ人材の需要が増加しても、人材を識別する手段が存在しない。IPAでは、試験合格者の合格時点での人定情報を保有するだけで、個人情報であるため、外部に公開していない。

このため、資格登録者の人定情報を登録する制度を創設し、資格登録者か否かを客観的に識別できる手段を提供する。なお、これだけでは既存の試験について合格者名簿の公開と同じだが、上述の更新制度の受け皿機能に加えて、登録制度に実務経験の申告・公開の機能の付加など、制度の効果的な活用を期待する。

## （2）名称独占制度の必要性

登録制度に関しては、①弁護士のように独占的に業務を行い他の者には当該業務の取扱いを禁止する業務独占型の資格、②エネルギー管理士のように定型的類型的行為に関して一律に規制をかけて資格者を設置して業務を実施させる必置規制型の資格、③技術士のように規制をかけずに名称の独占の使用や秘密保持義務などで資格の信頼性を向上させる名称独占型の資格、の3類型がある。

情報セキュリティに関しては、近年、経済社会の基盤として生活や仕事の隅々まで様々な形で情報システムが浸透しており、全ての企業や個人が情報セキュリティを確保するよう求められている。また、企業でも、経営戦略での位置づけ、組織内での体制や求める品質が異なっており、それぞれの状況に応じて対応がなされている。

このため、上記3類型のうち、特定の者のみに業務を認め他の者が取り扱うことを禁じる業務独占や定型化・類型化した行為を対象に責任者を一律に設置させる必置規制は、現状ではそのまま導入するのは適当ではなく、したがって、名称独占型の資格になろう。

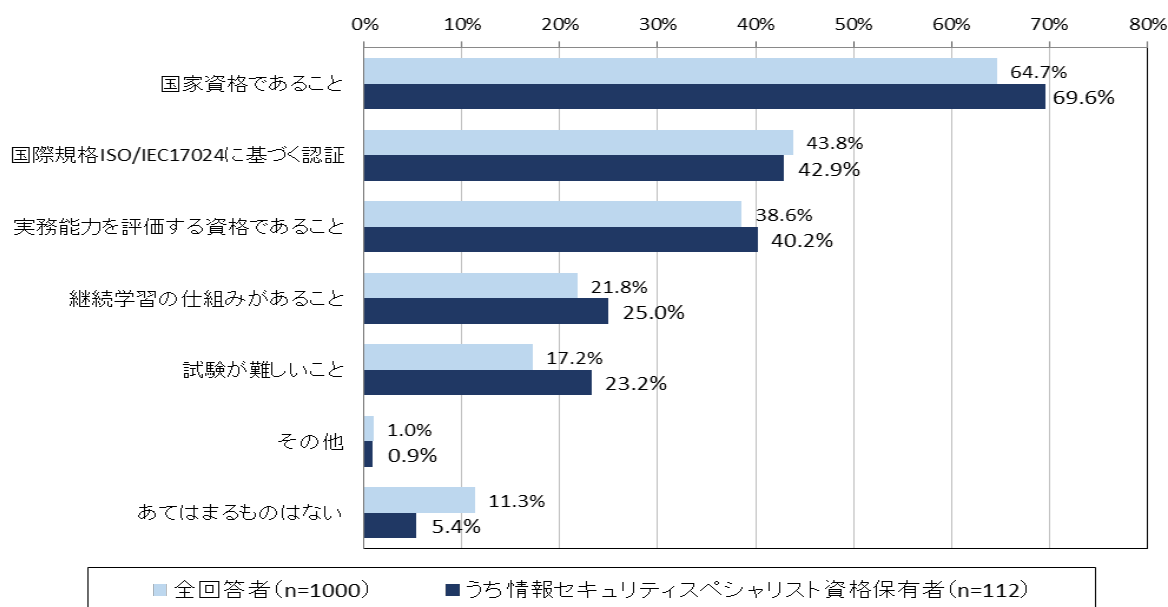
なお、登録制度により良質な人材供給を意図しながら、必置規制などにより人材の需要面での対策を講じないことは一貫していないように見えるが、ここでは法令による強制的な規制の要否を検討したものであり、ガイドラインによる推奨などの非強制的な手法については積極的に検討すべきであろう。

## （3）正式な資格名称

資格名称は、登録制度の信頼性に直結する重要な課題である。資格登録者にとって保有したくなるような魅力的な名称で、他の資格と混同されず、技術の進歩にも陳腐化せず、質が高く信頼のおける専門家と分かる名称が必要である。ただし、技術的な専門家というよりマネジメントも含めた広く情報セキュリティの知識・技能をもつ専門家ということが理解できる名称が望ましい。

なお、ウェブアンケートによれば、資格の取得意欲に関して、その資格が国家資格で

あることが最も重要視されている。登録制度の法制化を視野に入れて正式名称を検討するとともに、正式名称とは別に、資格取得のインセンティブになるような通称名称も検討すべきである。その際、商標等の所要の措置を講じるなど、名称が早期に定着し発展していくように、関係者が尽力すべきである。



参考5：資格取得に関するインセンティブの在り方（ウェブアンケート）

#### （4）更新条件に関する論点の検討

本研究会で最も議論が交わされた論点が更新条件であった。ステークホルダの関心を全て満たす更新条件がなかったためである。各種制度を参考に表3.の選択肢を整理し、このうち3つの選択肢を検討した。

具体的には、①再度SC試験のうち、実務経験を確認する部分である午後Ⅱの合格を求めるなど、試験による更新、②一定の職務経歴を経験し最新の専門的な知識・技能を有していることが確認できる職務経歴書の確認による更新、③一定の講習の受講歴等をポイント換算し一定以上であることの確認による更新、の3種類である。それぞれの検討結果は以下のとおり。

##### ① 一部免除付再試験

試験合格水準を維持していることを適正かつ客観的に判断できる方法であり、問題指摘に適切に対応できる方法。今回の登録制度を運営するIPAにとっては、従来まで運営してきた情報処理技術者試験と接合できるような更新制度として運営でき、人的物的な既存資産を活用できコストの最適化が図られる。ただし、試験だけでは、実務で直面する様々な課題解決の経験など、全てを判断できないという実務経験を重視する指摘もあった。

## ② 職務経歴書確認

ユーザ企業が資格登録者を活用する際に、実務をどの程度こなしてきたかを重視する声が多く、職務経歴を更新の条件としたらよいのではないかと指摘もあった。

ただし、①先端の技術であればあるほど特許や著作権などの知的財産権に抵触する可能性があり外部に公開できないことが多いこと、②利用している情報セキュリティサービスの内容は顧客企業にとって重大な情報であり守秘義務が課されるのが通常であること、から、職務経歴書に記載できる内容は抽象的にならざるを得ず、更新の条件として厳密に審査するのは困難であるとともに、適切な審査を実施することは事務負担も大きく、コスト的に高いものとなるのではないかと、それだけの有益性を確保できるのか、という指摘があった。

## ③ 講習受講などポイント制

公認システム監査人、情報セキュリティ監査人、ITコーディネータ、CISSPなど、現在の民間登録制度では、講習の受講数などを点数に換算して更新条件とする、いわゆるポイント制を採用しているケースが多い。ポイント制には2種類あり、雑誌購読や座学受講などの自己研鑽と資格試験の監督など制度普及活動がある。

こうしたポイント制について、ポイントを稼ぐことが主眼となりがちであり、ポイント制を原則として、全ての登録者の更新条件にするのは質の維持の観点から難しいのではないかと、との意見が多かった。

ただし、性悪説で見ればポイント制は質を劣化させるように見えるが、そもそもポイント制は、最新の知識の収集に熱心で実務経験が豊富な者にとって、日常的な資質向上の活動でもって評価される方法のはずである。IPAの認定などを受けた最新事例の講習を受講した場合などであれば、更新制度の本来の趣旨に沿ったものであるため、こうした者に限っては認めたいとの意見もあった。

	再試験の実施 (一部免除)			実務経験の確認 (職務経歴書)	知識技能の継続向上(ポイント制)		その他 (個別面接)
					自己研鑽で資質向上	資格普及など対外活動	
留意点	<ul style="list-style-type: none"> <li>既存の試験問題を活用可能</li> <li>ステータス確立が必要</li> <li>低合格率は規模縮小の懸念</li> <li>実務経験との密接な関連性への理解が必要</li> </ul>			<ul style="list-style-type: none"> <li>取引先との契約上の守秘義務</li> <li>チェック時の調査の限界</li> <li>登録簿公表に馴染むか</li> </ul>	<ul style="list-style-type: none"> <li>玉石混交のおそれ</li> <li>登録者同士の交流コミュニティに絡めやすい</li> </ul>	<ul style="list-style-type: none"> <li>登録者同士の交流コミュニティに絡めやすい</li> <li>結果的な資質向上</li> <li>第三者の目にさらされて質を維持できる</li> </ul>	<ul style="list-style-type: none"> <li>コストが膨大</li> <li>登録者も面接時間確保が必要</li> </ul>
具体例	<ul style="list-style-type: none"> <li>セキュリティスペシャリスト試験(午前I、II)</li> </ul>	<ul style="list-style-type: none"> <li>セキュリティスペシャリスト試験(午後IIのみ)</li> </ul>	<ul style="list-style-type: none"> <li>講習+チェックテスト</li> </ul>	<ul style="list-style-type: none"> <li>期間・規模・顧客・担当業務等の経歴</li> <li>雇用主、顧客の推薦状の添付</li> </ul>	<ul style="list-style-type: none"> <li>他の資格の取得</li> <li>民間の講習受講</li> <li>書籍購読</li> <li>論文や研究会発表</li> </ul>	<ul style="list-style-type: none"> <li>公的な役職(公的委員)</li> <li>査読のある論文発表</li> <li>講演、パネリスト経験</li> <li>メディア掲載歴(資格者としてのみ)</li> </ul>	<ul style="list-style-type: none"> <li>相手先に向いて面接</li> <li>年何回か大都市で面接</li> </ul>

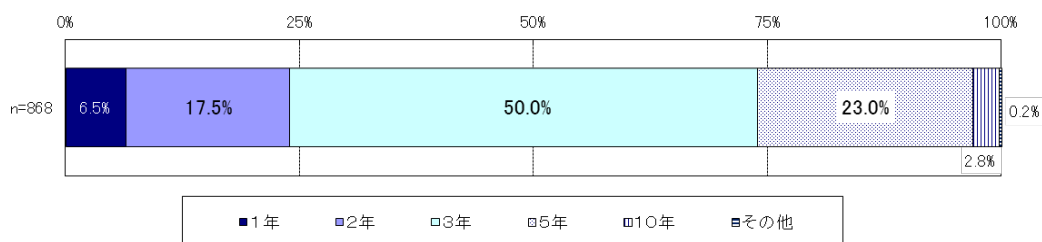
表3：更新条件に関する留意点等の比較表

以上を踏まえ、本研究会では、制度を円滑に継続的に運営していく持続可能性と経済合理性を勘案しつつ、更新の条件に関して複数の選択肢を認めることとした。具体的には、持続可能性と経済合理性については、4.(2)③4)で述べたとおり、ア)制度運用コストと登録更新手数料の収支、イ)登録者数・更新者数の規模の維持、ウ)登録更新時に要する様々な負荷への対応、といった点について配慮し、更新の条件について

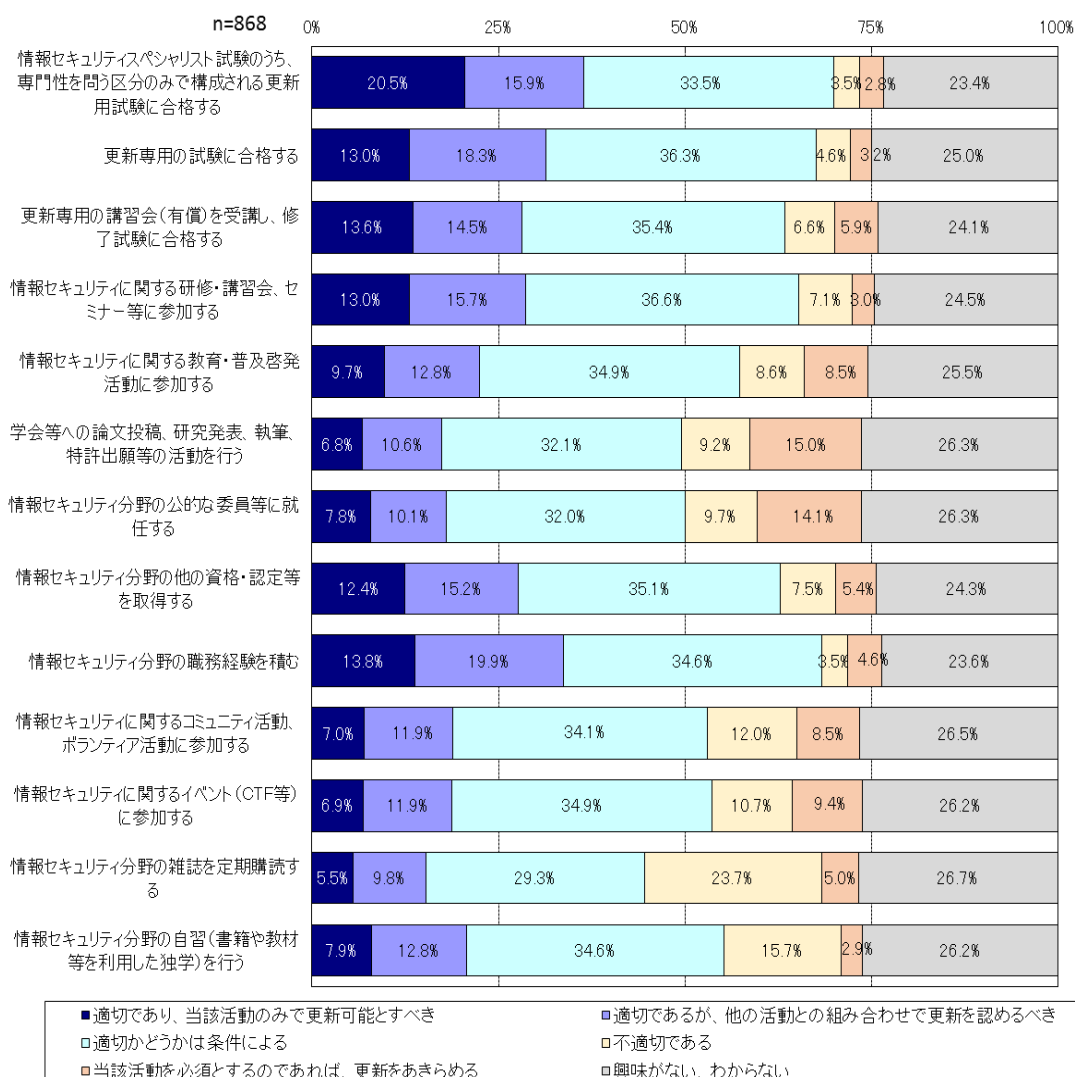


は、再試験の受験・合格を基本としつつ、実務に従事した経験や最新の専門的知識・技能を習得するためにIPA主催又は指定の講習等の受講による更新も、しっかりとした審査をして認める方向で結論を整理した。

なお、更新期間については、他の登録制度やウェブアンケートも参考にして検討し、3年程度が妥当との結論であった。



参考6：望ましい更新間隔について（ウェブアンケート）



参考7：登録更新の方法について（ウェブアンケート）

#### (5) 既存の試験合格者などに関する経過措置

今後のSC試験の合格者が登録資格者となる一方で、これまでのSC試験の合格者は登録できないのは合理的ではない。適切な猶予期間を設け、登録資格者とすべきである。

また、過去に情報処理技術者試験で実施した情報セキュリティ関連の試験（2. で述べたSU試験やSV試験）の合格者も、専門的な知識・技能を有することが確認された者であることから、同様に取り扱うべきであろう。

加えて、実践的な能力を適時適切に評価するために試験制度を充実させるためには、知識・技能の向上・維持に前向きな姿勢と実践的な能力を有する者についても、この登録制度の資格者として相応しく、積極的に認めるべきである。

他の情報セキュリティに関する試験や資格が国内外で実施されているが、上記のSC試験等の合格者又は実践的な能力のある実務経験者のいずれかに該当するはずである。現時点で、そのいずれでもない者を登録資格者とする必要性は乏しい。なお、今後、実務経験など様々な要素を加味して個別に判断せねばならない事例が想定されるため、必要に応じて登録資格者を追加できるよう柔軟な制度設計にしておくべきである。

#### (6) 資格登録者の責務

資格登録者はユーザ企業の秘密を知り得るため、相手方との信頼関係を構築しなければならない。しかし、万一登録者が業務上知り得た秘密を漏えいした場合、利用者と当該登録者との信頼関係が毀損するだけでなく、登録者全体への信頼を失うことになる。また、社会的な信用を失墜する行為全般も、他の資格登録者の業務に多大な悪影響を及ぼし、ひいては登録制度そのものを瓦解させかねない。

資格登録者はこうした責任を自覚して登録者として恥ずかしくない行動を心掛けなければならないし、秘密保持違反や信用失墜行為に対しては、厳正かつ公正に処断し、登録の取消など処分を行っていくべきである。

本制度が確立していけば、登録者以外の者が、資格者と装って業務を実施する可能性が出てくる。こうした事態が発生すれば、資格者か否かを確認せねばならず、簡単な人材の質の識別機能という本制度の本来の趣旨が根底から覆されかねない。こうした事態が発生しないように用意する必要がある。

#### (7) 登録制度の普及策

登録制度を普及させ制度を確実に社会に定着させることが不可欠であり、以下に掲げる施策の的確な実施が必要である。登録制度の確立・普及に向け、率先してこの制度を活用し育成していくべきである。



① ユーザ企業での調達条件や人材採用での活用

登録制度により業務経歴等を識別できるため、ユーザ企業では、資格登録者の活用を調達条件にする、人材の採用、登用時の基準にするよう期待する。

そもそも登録制度がユーザ企業内で評価されている必要があり、情報セキュリティへの社会的な意識喚起、資格登録者による目立った活躍、ベンダ企業の納得のいく説明、同業他社等での導入動向の調査などの取組も必要である。

② ベンダ企業での従業員に対する資格登録・資質向上支援

ウェブアンケートによれば、資格登録への社内の助成金など経済的支援策が十分ではない。更新費用や継続学習などの資質向上に対する更なる支援を期待する。

また、登録制度の副次的な効果として、情報セキュリティ部門の拡充など、専門人材の確保が必要となる際に、業務経歴のある登録簿を活用することも考えられる。なお、ユーザ企業からの指摘、同業他社の動向の調査などの取組も必要である。

③ 資格登録者による登録者コミュニティなどの立ち上げ

取引先や雇用主に影響を受けるが、登録者コミュニティなどを自発的な立ち上げ、同じような状況にある仲間とのつながりから情報を得て資質向上に取り組むことはできる。主体的な関与が①や②の実現につながる。

登録制度の設定者である経済産業省と運営者であるIPAの積極的な関与が必要である。例えば、管理運営が整った資格登録者コミュニティに対して、IPAが公式にサポートを表明するなど、コミュニティの求心力を付与したり、重大なセキュリティインシデントの公式情報を配信したりすることも考えられる。

④ 登録制度運営者である経済産業省とIPA

経済産業省とIPAは登録制度に不可欠である。経済産業省は、基本的な運営及び普及への継続的主体的な関与が必要で、IPAは、資格登録者等へのサポートが必要である。

⑤ 経済産業省による制度的な支援や企業への働きかけ

登録制度の実施主体である経済産業省は、社会全体での情報セキュリティ水準の向上など、公共的な目的が実現することで、間接的に裨益する。

予算や法律といった制度的・資金的な面で関与するとともに、ユーザ企業による登録制度の活用を促すために、例えばガイドラインで各種業界団体に働きかけるなど、ユーザ企業とベンダ企業との連携促進が必要である。また、6.(1)に述べる意見聴取の場を、例えば、産業構造審議会の情報経済小委員会の中で位置づけることも考えられる。これらサポートに継続的に取り組むべきである。

⑥ 大学等教育関係者からの協力

大学や関係学会などの教育関係者からは、最新の専門的知識の提供や講習実施などへの積極的な協力がなされることを期待したい。

## 6. 終わりに

### (1) 登録制度の継続的見直し

本研究会は、短期間に議論したため、制度の骨格や鍵となるポイントを集中的に検討できたものの、今後、登録システムの運用に関する詳細な設計になるほど、様々な制約条件を踏まえて決めることが多くなる。

その際、登録制度のそもそもの意義や趣旨、ステークホルダの視点などの事項を踏まえて決めるべきであり、より良い制度運営にするための意見聴取の場を設置するよう提案する。5. (7) ⑤で述べたように、産業構造審議会の情報経済小委員会の下にWG等を設置するなど、政府による取組が必要である。

### (2) 資格の国際性を目指して

情報処理技術者試験は、2. (1) で述べたように、既に12か国・地域との間で相互認証が行われIT人材の流動性の向上・有効活用に寄与し、7か国で共通統一試験を実施する際に試験の経験・ノウハウが活用されるなど国際的に貢献している。

また、ウェブアンケートでも、ISO認証など資格の国際性を重視して取得資格を検討していることがうかがえる。本研究会でも、登録制度の国際性に関する指摘があった。登録制度を普及させる上でも意義がある。

この登録制度が国際的に通用し貢献する制度となるように、制度開始後に、ISO認証の取組状況や相互認証の状況などを(1)の意見聴取の場で報告されるよう期待する。

### (3) 他の資格試験や情報処理技術者試験などの登録資格者としての取扱い

今回の登録制度では、SC試験の合格者のみを登録資格者とし、経過措置として過去のSC試験の合格者や実務能力を有する者についても暫定的な登録資格者とした。

今後、SC試験以外の高度試験やSC試験に相当する民間試験の合格者に関する取扱い、実務能力の内容、等について個別に検討が必要な場合が出てくる。その場合も、(1)の意見聴取の場で検討すべきである。

併せて、資格登録者を選別するSC試験は、国際的なサイバーセキュリティ技術動向を踏まえた実践的な能力を評価でき、かつ、ステークホルダが納得し信頼を寄せられる、他の追随を許さない試験を目指すべきである。同様に、SC試験以外の情報処理技術者試験についても、引き続き、関係者から信頼される試験となるよう取組を期待したい。

### (4) 登録制度は新たな始まり

最後に、情報セキュリティ人材は、資格登録者だけでなく、ホワイトハッカーのような高度セキュリティ技術者やユーザ企業において社内情報セキュリティ技術者と連携

して企業の情報セキュリティ確保を管理する人材も必要である。また、そうした3つの類型の人材供給だけでなく、I o Tの進展等に伴って、ネットワークに接続する全ての者に、情報セキュリティに関する意識の喚起、情報セキュリティの向上・確保が求められるとの認識で一致している。

社会の変化に伴って、求められる情報セキュリティ人材像の変化を認識し、適時適切な、多面的な人材の育成・確保が必要であるとともに、関係者は、今回の登録制度の開始がゴールではなく、新たな始まりであることを胸に刻んで進んでいただきたい。

## セキュリティ人材の確保に関する研究会

### 委員名簿

(座長)	有賀 貞一	AIT コンサルティング株式会社代表取締役
	岩丸 良明	東京工業大学 特任教授 (情報処理技術者試験委員長)
	鵜飼 裕司	株式会社F F R I 代表取締役社長
	富永 由加里	株式会社日立ソリューションズ常務執行役員
	浜田 達夫	一般社団法人日本情報システム・ユーザー協会 常務理事
	原田 要之助	情報セキュリティ大学院大学 教授
	三谷 慶一郎	株式会社N T Tデータ経営研究所 情報戦略コンサルティングユニット長
	三輪 信雄	S & J 株式会社代表取締役

(五十音順、敬称略)

#### ○オブザーバ

内閣サイバーセキュリティセンター  
文部科学省高等教育局専門教育課

#### ○事務局

経済産業省商務情報政策局情報処理振興課  
独立行政法人情報処理推進機構

# セキュリティ人材の確保に関する研究会

## 開催経緯

### 第1回

日時：8月10日（月）15：00～17：00

場所：（独）情報処理推進機構会議室

議題：情報処理技術者試験などの概要

登録制度に関する論点

登録制度に関するウェブアンケート項目案

今後の進め方

### 第2回

日時：8月19日（水）10：00～12：00

場所：経済産業省会議室

議題：各種登録更新制度

登録制度構築に向けた検討

### 第3回

日時：8月22日（土）10：00～12：00

場所：（独）情報処理推進機構会議室

議題：登録制度構築に向けた検討

### 第4回

日時：8月22日（土）13：00～14：30

場所：（独）情報処理推進機構会議室

議題：登録制度構築に向けた検討

### 第5回

日時：8月30日（日）10：00～12：00

場所：（独）情報処理推進機構会議室

議題：研究会報告書（案）について