資料1

# セキュリティ人材の能力評価を巡る 現状と課題

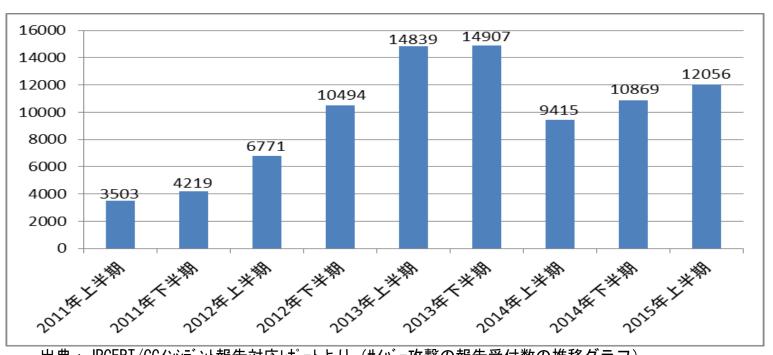
平成27年8月情報処理振興課

# 1. セキュリティ人材に係る緊急検討の背景

#### 第2回WG(平成27年3月25日)配付資料を一部修正

## 1. 情報セキュリティに係る現状(サイバー攻撃①)

- ◆ 我が国に対するサイバー攻撃は増加傾向。
- ◆ IT空間の拡大とともに、サイバー攻撃は巧妙化し、脅威も増大。
  - → 発電所や化学プラント等の重要インフラを狙うサイバー攻撃の脅威
  - → 政府機関や企業の機密情報を狙う標的型サイバー攻撃の増加
  - → スマートフォンやタブレットなどネットワークにつながる機器はどれも標的に
- ◆ 個人から重要インフラまで、あらゆる分野に対しての攻撃が増加。今後、早急に対処しないと、被害が連鎖的に拡大し、我が国の産業基盤や個人の生活基盤が著しく損なわれるおそれ。



出典: JPCERT/CCインシデント報告対応レポートより(サイバー攻撃の報告受付数の推移グラフ)

## 1. 情報セキュリティに係る現状(サイバー攻撃②)

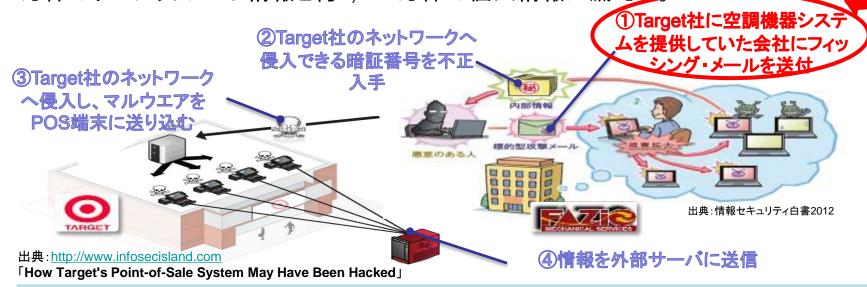
◆ 近年、標的型サイバー攻撃の手口は更に巧妙化しており、従来型ウイルス のような未然防止可能な攻撃ではなくなっている。

## ◎最新の標的型サイバー攻撃事例

対象を直接、攻撃するのではなく、<u>まず関連システム会社を攻撃し、</u>攻撃対象のネットワークに侵入。

≪米Target Corporation (2013年12月)の事例》

米売上高第5位の小売業者であるTarget社のPOS端末を狙った攻撃により、4,000万件のクレジットカード情報と約7,000万件の個人情報が漏えい。



注)Target社システムのセキュリティを常時監視していた、米FireEye社はネットワークに何者かが侵入していることをTarget社に警告。しかしながら、Target社は速やかな対応ができず、顧客データの流出が続いた。後日、経営層の経費削減という方針により、セキュリティ上の脆弱性を何年も放置していたことが判明。

出典:日経ビジネスオンライン「セキュリティ対策はコストではない~米国で起きた「ターゲットの悲劇」の教訓~」

http://business.nikkeibp.co.jp/article/opinion/20140604/266189/?rt=nocnt

## 1. 情報セキュリティに係る現状(サイバー攻撃③)

◆ 巧妙化したサイバー攻撃に対応するため、情報セキュリティ製品も進化している。一方で、情報セキュリティに関するリスクを認識し、情報セキュリティ製品を適切に活用しなければ速やかな対策が出来ない。

## ◎最新のセキュリティ対策事例

仮想環境上で、怪しいファイルを実行し、マルウェアかどうかを検知。

≪米FireEye社、サンドボックス技術≫

(概要)

仮想環境上でいったんファイルを実行し、実行後の振る舞いをチェックして マルウェアかどうかを検知する技術。\_\_\_\_



注)Target社は未契約だったため、除去は手動運用であったため、対策に時間を要した。

検知したマルウェアを自動除去するにはオプション契約が必要。

## 1. 標的型攻撃の脅威が深刻化

- ◆ 今年5月、日本年金機構において、職員の端末に対する外部からのウィルスメールによる不正アクセスにより、約125万件の個人情報が外部に流失。
- ◆ 日本年金機構と同様の「標的型メール」の攻撃は急増しており、手口も巧妙 化・複雑化している。

## 【政府機関への脅威件数等】



- ■センサー監視等による通報件数 [件] (左軸)※
- □不審メール等に関する注意喚起の件数 [件] (左軸)
- ◆センサー監視等による脅威件数 [万件] (右軸)
- ※ GSOC(政府機関情報セキュリティ横断監視・即応調整チーム)により 各府省庁等に置かれたセンサーが検知等したイベントを通知した件数。

## 【外部からの攻撃に係る2014年度の特徴】

以前にも増して政府機関に大量の不審メール、不正プログラムが送付されており、 標的型メールによる脅威が一層深刻化。

- センサー監視等による通報件数は前年度から倍増(264件)、そのうち約4割は標的型メール(標的型メールの通報件数は前年度比約3倍に増加)。
- ◆ 不審メール等の注意喚起件数は前年度から倍増(789件)。
- センサー監視等による
   育威件数は約399万件。
   (約8秒毎に1回脅威を認知。前年度より減少したのは、GSOCシステムの能力向上によって、軽微なものの判別対象からの除外を含め、脅威の識別精度が向上したことによるもの。脅威そのものは一層深刻化。)
- ◆ 文書作成ソフト等の未知の脆弱性を利用した攻撃や、不正通信の接続先にクラウド上のサーバが利用される等、認知・防御が困難に。

## 【2014年度の主なサイバー攻撃事案】

2014.9	[法務省] サーバに対する外部からの不正アクセスが発覚。
2014.10	[国土地理院] パソコンがウイルスに感染、情報流出の可能性を発表。
2015.2	[日本貿易振興機構] 標的型メールによるパソコンのウイルス感染が発覚。
(参考)	
2015.6	[日本年金機構] パソコンがウイルスに感染、約125万件の情報流出を公表。

## 1. 成長戦略における位置づけ

◆ 「日本再興戦略」改訂2015において、「セキュリティ従事者の実践的な能力 評価をするため試験制度の充実を図る」こととされた。

## <u> @「日本再興戦略」改訂2015(平成27年6月閣議決定)抜粋</u>

- 一. 日本産業再興プラン
- 4. 世界最高水準のIT社会の実現
- (3)新たに講ずべき具体的施策
- i )国民・社会を守るサイバーセキュリティ
- ④サイバーセキュリティの確保に向けた基盤強化(技術力の強化・産業育成、人材育成) イ)人材育成

顕在化・深刻化しているセキュリティリスクや、急速な技術革新とともに高度化するサイバー攻撃への対策を確かなものとするためには、それを支える人材の育成が急務である。(中略)

さらに、企業等の経営におけるセキュリティ対策の責任者を育成するためのセキュリティマネジメント試験を来年春に導入する。

あわせて、2020年東京オリンピック・パラリンピック競技大会の開催も見据え、高度な実践的人材の育成を強化する。このため、産学官の協力体制構築に向け、緊密な連携や情報共有の促進に加え、実践的なサイバー演習環境をクラウド環境で整備する。また、実践的な教材の産学官共同開発を支援する。さらに、<u>官民連携により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</u>試験制度の充実を図る。

## <参考> サイバーセキュリティ戦略本部におけるこれまでの議論

- ◆「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)において、以下の方針が示されている。
  - ※平成17年5月30日高度情報通信ネットワーク社会推進戦略本部長決定により設置。同会議での決定事項は平成27年2月10日以降、サイバーセキュリティ戦略本部に引き継がれている。

#### <u>◎「新・情報セキュリティ人材育成プログラム」該当部分抜粋</u>

- 3. 今後の取組方針
- (2)必須能力としての情報セキュリティ
  - ②情報セキュリティ能力の評価基準・資格等の整備 (中略)

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、<u>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。</u>

## <参考>海外の民間資格

## **OCISSP**(Certified Information Systems Security Professional)

(ISC)2SMが認定を行っている、国際的に認められたベンダーフリーの情報セキュリティ・プロフェッショナル認証資格。CIO、CISOを始めと する管理職、技術職、コンサルタント、営業など幅広い職種でIT業務に取組む人が取得している。(ISC)2認定資格「SSCP」の上位資格に あたる。

<受験条件>

CISSPに関する共通知識分野10分野のうち2もしくはそ れ以上の分野において5年以上(大卒者または(ISC)2が 認める資格の取得者は4年以上)のプロフェッショナルと しての業務経験があること

世界資格取得者数:98,421人 国内資格取得者数: 1.380人

(H27.3/1現在)

<試験>

CISSP試験

試験スコア(1000点中700点取得) 業務経験、現役のCISSP認定資格保持者の推薦、など

<登録>

登録(有効期間:3年間)

<更新条件>

<更新登録要件> 3年間に120ポイント、かつ 毎年最低20ポイント取得

- ・『(ISC)2倫理規約』を遵守すること
- ・必要な継続教育単位(CPEクレジット)を取得し、申請す ること(1年あたりのCPE:40ポイント、認定期間3年間の 合計CPE: 120ポイント)
- ・毎年の請求書の受領時に年会費を支払うこと(年会 費:12.000円(消費税込み))

出典:(ISC)2ホームページ(https://www.isc2.org/japan/default.aspx)を基に作成

## <参考>民間資格の活用事例

## OCISSP(Certified Information Systems Security Professional)

#### <米国>

- 国家安全保障局(NSA) 取得義務付け
- 国防総省(DoD) 取得必須資格要件

#### <欧州>

- ・ 英国スコットランドヤード(ロンドン市警)のコンピュータ犯罪局 取得を推奨
- インターポール(国際警察機構) 取得を推奨

## OCompTIA Security+

セキュリティエンジニアの基本レベルのセキュリティスキルおよび知識を評価するために作成された、ワールドワイドで提供されているベンダーニュートラルの認定資格。

CompTIA Network+に相当するネットワーク環境の実務経験を持つ技術者に必須となるセキュリティスキルを評価するために設計され、セキュリティの一般概念、インフラストラクチャセキュリティ、暗号技術、業務・組織面でのセキュリティ策定など、セキュリティに関連する知識と改善能力、問題解決能力などが幅広く問われる。

#### <米国>

国防総省の情報保証に関連している全ての人材に対し、必須資格となっている。

## OGIAC (Global Information Assurance Certification)

GIACは、実社会で真に通用するコンピュータ、ネットワーク、およびソフトウェアセキュリティのスキルを認定。GIACは能力確認テストであり、理論や用語の知識だけに限らず、実際に情報セキュリティ・コンピュータ・サーバ操作、監査、タスク管理の実用的な知識・スキルを試験し、認定を行う。試験領域は、Security Essentials、セキュリティ監査、侵入検知、インシデント・ハンドリング、ファイアウォール、フォレンジック、Windows OS、Unix/Linux OSなど、入門レベルから高度な専門性を要求される分野までのすべてをカバーしている。2012年11月14日現在35のトレーニングコースと、それに対応する23の認定資格が存在する。

#### <米国>

政府関係者(軍、FBI、CIAなど含む)15,000名/年がコースを受講。

出典:平成24年度情報セキュリティ対策推進事業(情報セキュリティ人材の育成指標等の策定事業)報告書

## 2. 情報処理技術者試験を巡る状況

## 2. 情報処理技術者試験の概要

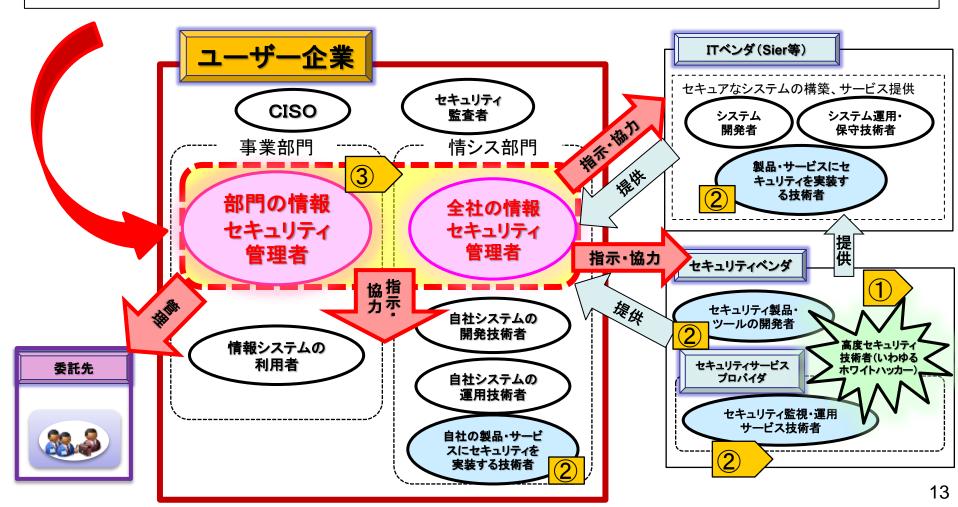
- <u>情報処理技術者試験は、「情報処理の促進に関する法律(第7条)」に定められている国家試験</u>であり、経済産業大臣が独立行政法人情報処理推進機構に試験事務を行わせている。
- 情報技術者の不足、プログラマ認定制度創設への要望を背景に、昭和44年よりスタートした情報処理技術者試験は、年間の応募者数が 45万人規模の大規模な国家試験へと発展し、数多くの企業 や教育機関などで活用されている。
- 平成26年度までの46年間に応募者数は<u>1,802万人</u>を数え、合格者総数も<u>226万人に達し、我が</u> 国のIT人材育成に大きな役割を果たしている。





## 2-1. 今後必要となるセキュリティ人材像

◆ 今後必要となるセキュリティ人材は、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安全な情報システムを作るために必要なセキュリティ技術を身につけた人材、③ ユーザー企業において、社内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。



## 2-2. 必要な人材像(セキュリティ技術者)

◆ 安全な情報システムの構築やサービスを実現するために専門的なIT技術者については、従来から情報処理技術者試験において情報セキュリティ分野を専門とする情報セキュリティスペシャリスト試験を実施。



(情報セキュリティを利用者側の現場で管理する者)





情報セキュリティ対策を実施

## 情報セキュリティスペシャリスト人材

(安全な情報システムを作る者)

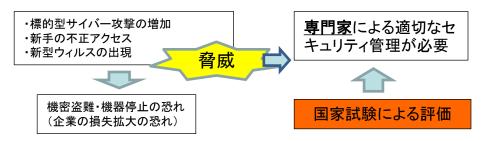


(典型的な人材像:セキュリティ技術者)

情報セキュリティ分野を専門とするIT技術者であり、<u>情報システムのセキュリティ機能を実装し、</u>また、<u>情報セキュリティ</u>技術の専門家として情報セキュリティ管理を支援する。

## <参考>情報セキュリティスペシャリスト試験の概要

#### 情報セキュリティスペシャリスト試験とは・・・



#### セキュリティの専門家を評価する国家試験

#### 【情報処理技術者試験における位置づけ】



#### 【対象者像】

高度IT人材として確立した専門分野をもち、情報システムの企画・要件定義・開発・運用・保守において、情報セキュリティポリシに準拠してセキュリティ機能の実現を支援し、又は情報システム基盤を整備し、情報セキュリティ技術の専門家として情報セキュリティ管理を支援する者

#### 【情報セキュリティスペシャリスト試験の応募者数等(直近3年分)】

	平成26年度	平成25年度	平成24年度
応募者数	54,981	56,452	57,944
(全体に占める 応募者割合)	(12.0%)	(12.0%)	(11.9%)
合格率	14.0%	13.9%	13.8%

#### 【出題範囲(午後)】

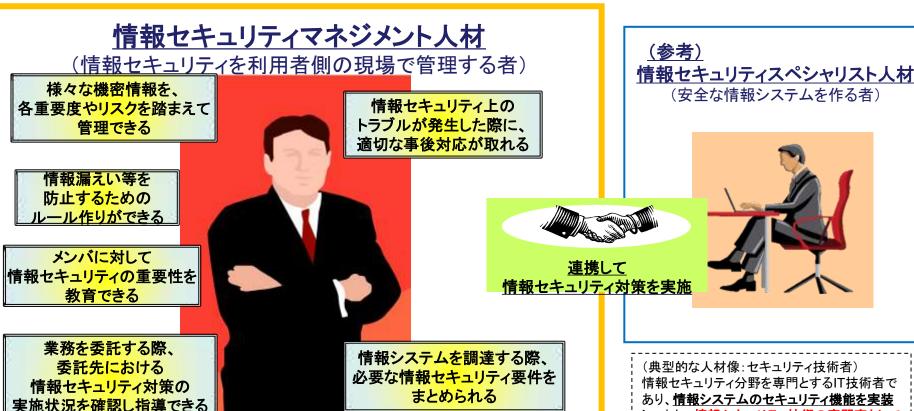
- ○情報セキュリティシステムの企画・要件定義・開発・運用・保守に 関すること(セキュアプログラミングなど)
- ○情報セキュリティの運用に関すること(不正アクセス対策など)
- ○情報セキュリティ技術に関すること(ウイルス対策技術など)
- ○開発の管理に関すること(開発環境の情報セキュリティ管理など)
- ○情報セキュリティ関連の法的要求事項などに関すること(著作権 法、個人情報保護など)

15

#### 第2回WG(平成27年3月25日)配付資料を一部修正

## 2-3. 必要な人材像(ユーザ企業のセキュリティ管理者)

◆ 今後必要となるセキュリティ人材のうち、ユーザー企業において、一定の技術知識を持 ちつつ、自社内で情報セキュリティ対策の実務をリードできるマネジメント人材を対象と する新試験を創設。(平成28年4月から実施予定。)



(典型的な人材像:業務部門セキュリティ管理者)

業務部門において、普段は総務や企画等を担当しつつ、情報セキュリティト ラブルの発生時には部門長やセキュリティ技術者と連携して被害の最小化 を図る

あり、情報システムのセキュリティ機能を実装 し、また、情報セキュリティ技術の専門家として 情報セキュリティ管理を支援する。

## 2-4. 情報セキュリティマネジメント試験(仮称)に求められる内容

- ◆ 情報セキュリティマネジメント試験(仮称)を通じて確認する、情報セキュリティマネジメントを行う上で最低限必要な「知識」内容は以下のとおり。
  - 1. 情報セキュリティマネジメントの計画、情報セキュリティ要求事項に関すること



ガイドラインなどを参考にして、ITシステムなど情報セキュリティ対策をすべき対象を特定し、業務継続等に配慮しつつリスク評価を行い、戦略の立案に参画。

2. 情報セキュリティマネジメントの運用・継続的改善に関すること

機密保持の 教育訓練等



監視



報告•相談

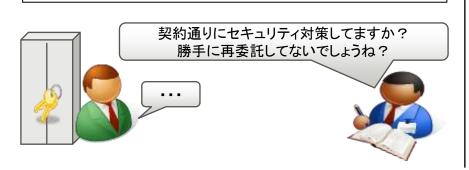






必要に応じて 規程の見直し

3. 外部委託、コンプライアンス(遵守指導等) に関すること



4. (上記1~3の前提となる)情報セキュリティマネジメントの基礎知識に関すること

関連法規 ガイドライン

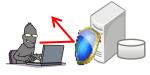




セキュリティ 管理・監査手法









## 2. 試験の官民における活用状況

◆ 情報処理技術者試験は、他の国家試験等における優遇措置や官公庁における調達要 件等に活用されている。

#### 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。

- •中小企業診断士試験、弁理士試験
- ·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)

→ 科目の一部免除

→ 応募資格 (警視庁、千葉、群馬、茨城 等)

- •教員採用試験
  - → 学科の一部免除など

#### 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、入学金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)

- (イ) 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するとしている。
- (ロ) 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。

## <参考> 中央省庁・地方公共団体における活用事例

◆ 情報処理技術者試験は、中央省庁・地方公共団体の情報システム開発の競争入札参 加資格やサイバー犯罪捜査官採用試験の受験資格等に採用されている。

#### 1. 中央省庁の事例

府省庁	件 名	情報処理技術者試験 の位置付け
内閣府	国民経済計算システムに関する設計・開発作業	入札参加資格
総務省	次期政府統計共同利用システムの仕様書策定等支 援業務の請負	入札参加資格
法務省	矯正総合情報通信ネットワークシステムにおける サーバ集約化に伴う工程管理支援業務の調達	入札参加資格
外務省	任期付外務省職員の臨時募集(文書管理・情報公開システム分野) 任期付外務省職員の臨時募集(領事関連情報システムの企画開発、運用保守分野)	入札参加資格
財務省	財務省行政情報化LANシステム等再構築に係る 調達仕様書作成等に関するコンサルティング業務	入札参加資格
文部科学省	高等学校卒業程度認定試験システムに係る運用支 援及びアプリケーション保守作業	入札参加資格
厚生労働省	厚生労働省ネットワークシステムの更改に係る調 達支援業務及び工程管理支援業務	入札参加資格
農林水産省	農林水産省行政情報システム機器賃貸借及び保守 業務	入札参加資格
経済産業省	鉱業権出願処理システムの運用保守業務	入札参加資格
国土交通省	港湾空港関係情報システム運用保守(関東地方整 備局)	入札参加資格
環境省	平成27年度環境省次期ネットワークシステム調達 支援等業務	入札参加資格
防衛省	防衛省中央OAネットワーク・システム更改に伴う システム分析検討に関する支援役務	入札参加資格
人事院	人事・給与関係業務情報システムのプロジェクト 管理支援業務	入札参加資格

#### 2. 都道府県の事例

都道		情報処理技術者試験
か 府 県	件名	情報処理技術有試練 の位置付け
	情報システムの開発 競争入札参加資格申請の手引き	様式に合格者人数記載
北海道 岩手		
	情報システム開発に関する競争入札参加資格申請	様式に合格者人数記載
宮城	宮城県電子県庁共通基盤システムに係るアプリケーション保守作業	入札参加資格
福島 茨城	福島県警採用試験 茨城県警察官サイバー犯罪捜査官採用試験	合格者レベル程度
		受験資格
栃木	栃木県警察官サイバー犯罪捜査官採用試験	受験資格
群馬	群馬県警察官サイバー犯罪捜査官採用試験	受験資格
埼玉	埼玉県警察官採用試験	加点対象
千葉	千葉県警サイバー犯罪捜査官採用試験	受験資格
東京	警視庁コンピュータ犯罪特別捜査官採用試験	受験資格
神奈川	神奈川県警察職員(情報工学職)採用試験	受験資格
富山	富山県警察職員採用試験	受験資格
石川	石川県警察官サイバー犯罪捜査官採用試験	受験資格
山梨	山梨県地理情報システム(統合型GIS)再構築業務委託	入札参加資格
長野	長野県警察官採用試験	受験資格
静岡	静岡県警採用試験	加点対象
愛知	サイバー犯罪捜査技術支援職員	受験資格
三重	三重県予算編成支援・財務会計システムSI支援業務	入札参加資格
京都	京都府警採用試験	加点対象
大阪	大阪府電子調達システム開発委託(第二期)	入札参加資格
兵庫	兵庫県警採用試験(特別区分-情報処理)	受験資格
和歌山	和歌山県教育ネットワーク整備事業	入札参加資格
鳥取	県内学校校内LAN運営支援業務	入札参加資格
岡山	岡山県警採用試験	加点対象(10点加点)
広島	国立原爆死没者追悼平和祈念館情報システム運用保守業務調達	入札参加資格
山口	山口県警察官サイバー犯罪捜査官採用試験	受験資格
徳島	徳島県警察官サイバー犯罪捜査官採用試験	受験資格
愛媛	愛媛県警採用試験	合格者レベル程度
高知	電子納品保管管理システム運用保守委託業務	入札参加資格
福岡	福岡県警察職員(情報処理)	受験資格
佐賀	佐賀県立学校校内LAN運用保守業務	入札参加資格
長崎	長崎県警察官 (サイバー犯罪捜査)採用試験	受験資格
大分	情報システムの開発業務の請負契約に係る競争入札参加資格審査申請	様式に合格者人数記載

## 2. 試験の官民における活用状況

- ◆ 合格者には一時金・資格手当などといった報奨金制度を設ける企業や、就職の際に試験合格を考慮する企業など、多くの企業から高い評価を受けている。
- ◆「日経ソリューションビジネス」で行ったアンケートでは、技術職においては、1位~10位 すべて情報処理技術者試験が独占している。営業職においても基本情報技術者試験と ITパスポート試験が1位、2位という結果。

#### 主要ソリューションプロバイダ101社が回答。上位10資格を掲載



※1.旧試験制度の「テクニカルエンジニア:情報セキュリティ」と「情報セキュリティアドミニストレータ」を統合 ※2.旧試験制度の「テクニカルエンジニア:ネットワーク」 ※3.旧試験制度の「アクニカルエンジニア:データベース」 ※4.旧試験制度の「アプリケーションエンジニア」 ※5.旧試験制度の「ソフトウェア開発技術者」 ※6.旧試験制度の「テクニカルエンジニア:ジステム管理 ※7.旧試験制度の「システムアナリスト」と「上級システムアドミニストレータ」を統合

# 3. 他の国家試験・資格の事例

## 3. 国家試験・資格の事例

- ◆ 総務省が実施した調査を基に国家試験・資格を分類すると、以下のとおり。
- ◆ 法律上有期限である資格については、3~5年程度での更新を求めている資格がある。

#### 主な登録制の資格

## 業務独占/124資格



運転免許、消防設備士、消防設備点検資格者、防火対象物点検資格者、防災管理点検資格者、介護支援専門員、ボイラー溶接士、液化石油ガス設備士、溶接工・・・等

## 必置資格/155資格



貸金業務取扱主任者、防火管理者、自衛消防組織統括管理者、防災管理者、清掃作業監督者・従事者、貯水槽清掃作業監督者・従事者、防除作業監督者・従事者、排水管清掃作業監督者・従事者・・・等

## <u>業務独占でも必置資格でもないもの</u> /18資格



出典:総務省「検査検定、資格認定等に係る利用者の負担軽減に関する調査」22 (平成23年10月)を基に経済産業省にて作成

# 4. 研究会の設置について

## 4. 研究会の設置について

◆ セキュリティ関連人材の実践的な能力を客観的かつ継続的に保証できるような制度について専門的な検討を行うため、研究会を設置する。

#### <メンバー構成>

- 学識経験者
- セキュリティ対策専門家
- 試験制度等関係者
- 情報システム開発業界関係者
- 情報システム利用企業関係者等を想定。

関係府省にもオブザーバで参加頂く想定。

## <u> <スケジュール></u>

短期間で集中的に検討を行い、9月上旬までにとりまとめることを目指す。

とりまとめた内容はIT人材WGに報告する。

## <庶務>

研究会の庶務は、経済産業省商務情報政 策局情報処理振興課と(独)情報処理推進機 構の共同で行う。

## <現時点で想定される論点>

(論点1)

登録制の対象となる試験や資格の名称

(論点2)

登録制の導入方法

✓ 登録条件(取消条件) 等

(論点3)

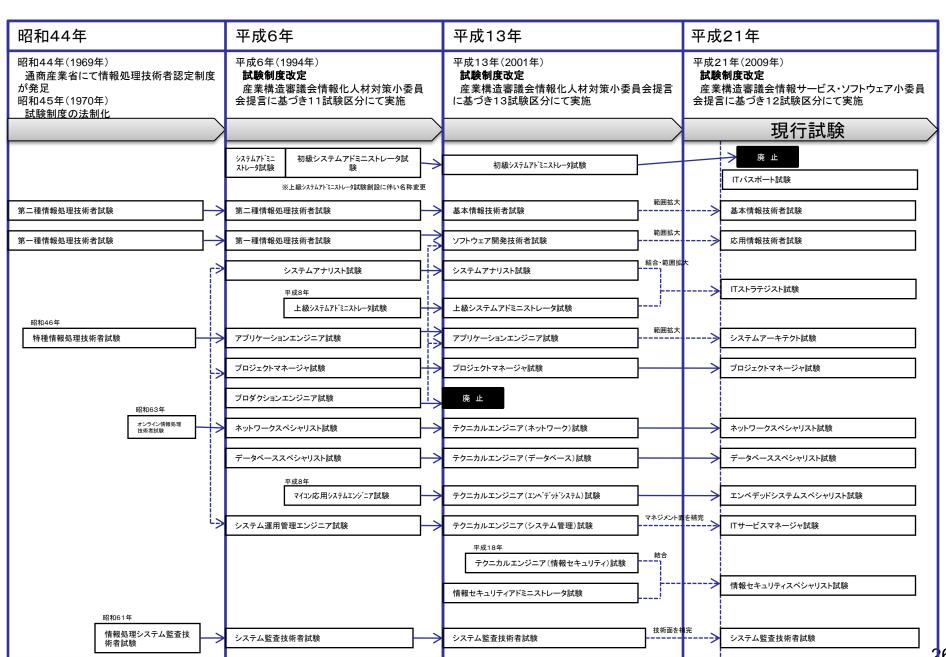
試験・資格の普及方策

(論点4)

登録制導入に対しての経過措置

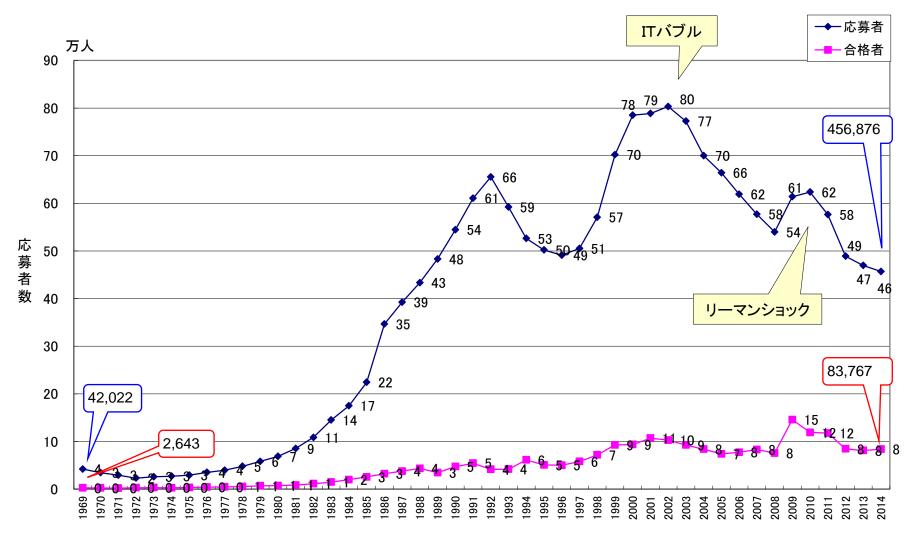
参考資料

## <参考>情報処理技術者試験の区分の推移



## <参考>情報処理技術者試験の応募者数推移(全区分)

■試験制度開始時からの応募者数・合格者の推移



## <参考>情報処理技術者試験における情報セキュリティ出題強化

- <背景> 〇 情報セキュリティの重要性の一層の高まり
  - 情報セキュリティ人材の量的・質的な不足



- ✓ 情報セキュリティに関する知識を含め、国民全体のITリテラシーの向上を図ることが必要 (世界最先端IT国家創造宣言 ※ 2013年6月14日閣議決定)
- ✓ 情報セキュリティ人材の発掘、育成、活用を進めることが必要 (サイバーセキュリティ戦略 ※ 2013年6月10日政府公表)

## 「iパス」をはじめとする情報処理技術者試験の全試験区分において、 「情報セキュリティ」に関する出題の強化・拡充を実施



#### iパス

基本情報技術者試験 (FE) 応用情報技術者試験 (AP)

#### 高度試験

- ◆ 情報セキュリティに関する出題比率の大幅な引き上げ(2倍)
- ◆ 午前試験において「中分類11 セキュリティ」の出題比率を引き上げ
- ◆ 午後試験において「<u>情報セキュリティ分野」を 選</u> 択問題から必須問題に変更
- ◆ 午前 I 試験(共通知識)、午前 II 試験において「中分 類11 セキュリティ」の出題比率を引き上げ
- ◆ ITストラテジスト試験(ST)、プロジェクトマネージャ試験(PM)においては、<u>午前II試験の出題範囲に新たに「中分類11 セキュリティ」を追加</u>(高度全区分で出題)

〈参考〉 情報処理技術者試験のレベル感 (教育機関別受験状況) ▼ I T エンジニアを対象 出題における想定レベル		教育終了レベル感	合格者 平均 年齢	合格率[%](合格 <b>全受験者</b> 大学院 大学	各数/受験数) 高專 專門学校 高校
【レベル4】 <b>情報セキュリティ</b> スペシャリスト 試験	高度 I Tエンジニア システムの企画・開発・運用等 において、セキュリティの専門 家として活躍し、下位者を指導	社会人 (実務 経験要)	33 .4歳	14.0% (5,071/36,104) 30.0% (61/203) 27.1% (98/362)	21.1% (4/19) 18.9% (164/867) 17.5% (7/40)
【レベル3】 <b>応用情報</b> 技術者試験	ワンランク上の I Tエンジニア <u>独力で</u> 、I Tを活用したシステ ム設計、開発等を行える	大学院 卒業程度	<b>29</b> .0歳	20.2% (12,655/62,746) 38.8% (461/1,187) 32.8% (773/2,360)	34.3% (69/201) 18.1% (770/4,247) 23.9% (90/377)
【レベル <b>2</b> 】 <b>基本情報</b> 技術者試験	I Tエンジニアの登竜門 <u>上位者の指導の下</u> 、I Tを活用 したシステム設計、開発等を行 える	大学 卒業程度 (情報系)	25 .1歳	23.7% (23,953/100,879) 48.1% (1,341/2,790) (28.4% (3,963/13,969)	29.9% (371/1,242) 18.2% (2854/15,706) 15.6% (693/4,442)
▼ 全ての社会人、学生を対象					
【レベル1】 <b>i パス</b> (ITパスポート試験)	社会人・学生に必須のIT力 <u>情報セキュリティ</u> を含むIT知識 の他、経営、IT管理の基礎を 理解し、ITを適切に利活用	大学 卒業程度 (情報系 以外)	28 .7歳	47.9% (34,215/71,464) 65.7% (504/767) 45.9% (5,148/11,208) (	38.7% (287/741) 31.9% (2,192/6,869) 25.2% 2,794/11,078)

## <参考>ホワイトハッカーの育成(セキュリティ・キャンプ)

- ○若年層のセキュリティ人材を発掘し、世界に通用する善意のトップクラス人材(ホワイトハッカー)を創出するため、 IPAが民間企業と連携して、若年層セキュリティ人材(22歳以下)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。倫理面も含めたセキュリティ技術と、最新のノウハウを、第一線の技術者から若手に伝授する場を創 出。これまで約4百名が受講(平成26年度時点)。
- 〇最近ではキャンプ修了者から女性だけのセキュリティコミュニティ発足の動きも出ている。

石森 大貴 (いしもり だいき) さん (2007年修了生 24歳 (1990年生)) 高校時代にセキュリティ・キャンプに参加、その後、擬似ハッキ ングによる脆弱性診断や官公庁や企業へのセキュリティコンサル を行ない、そこからセキュリティ専門会社のゲヒルンを起業し、 現在、代表取締役を務める。このゲヒルンは、社員数わずか十数 名ながら高いセキュリティ診断技術ゆえに金融機関などの大手企 業からの依頼を多く手掛けている。

**丑丸 逸人** (うしまる はやと) **さん** (2010年修了生 25歳(1989年生)) 2013年8月、米国で開催された世界最高峰のハッカーコンテスト である「DEFCON21 CTF(Capture The Flag)」本戦に参加。ソフト ウエアを解析して脆弱性を見つけ出すハッカーとして、日本の チーム「sutegoma2」が全20チーム中6位にランクイン する快挙を成し遂げることに貢献した。セキュリティ対策企業 でも活躍。

「日本を守る「七人の侍」 - ホワイトハッカー、インスペクター、ゲートキーパー (2013/10/03 日経コンピュータ)」で紹介される。



#### セキュリティ・キャンプが輩出したホワイトハッカー

キャンプ修了生同志の交流を促進

最先端で活躍する技術者を 講師として招へい

講師

ヤキュリティ・キャンプ

若いサイバーセキュリティ人材の発掘と育成



官民連携による推進

セキュリティ・キャンプ 実施協議会