資料3

公認情報セキュリティ監査人資格について

NPO日本セキュリティ監査協会　資格認定委員長
主席監査人　原田要之助

本資料の内容のうち，★については，日本セキュリティ監査協会のホームページで公開しています

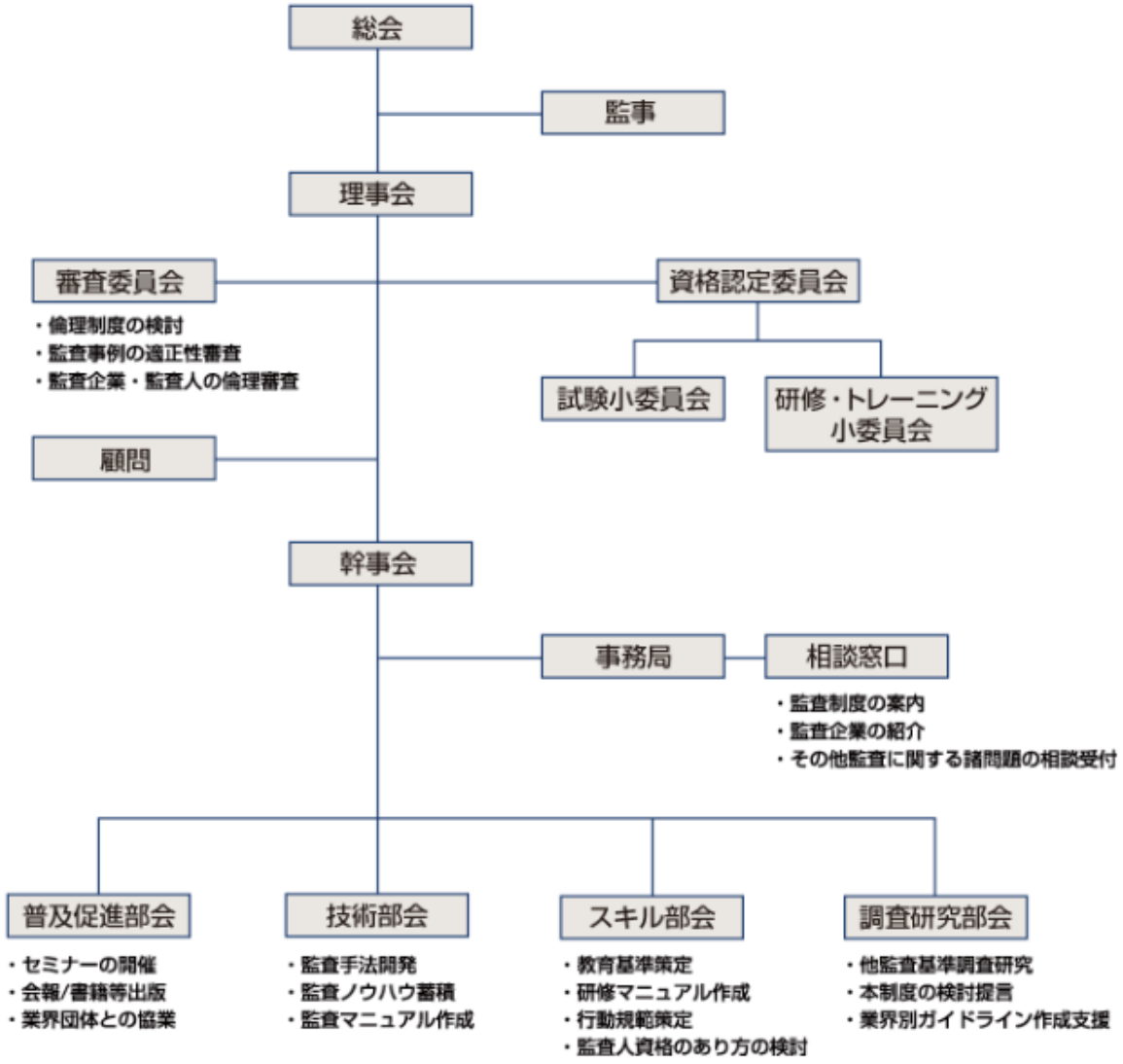
★

資格の体系について

- 目的
  - 経済産業省により施行された「情報セキュリティ監査制度」のもと、「公正かつ公平な情報セキュリティ監査」が実施され、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、以下の資格を認定する
- 資格体系
  - 公認情報セキュリティ主任監査人（英語名称：CAIS-Lead Auditor）
  - 公認情報セキュリティ監査人（英語名称：CAIS-Auditor）
  - 情報セキュリティ監査人補（英語名称：CAIS-Assistant）
  - 情報セキュリティ監査アソシエイト（英語名称：CAIS-Associate）
  - 公認情報セキュリティ主席監査人（英語名称：CAIS-Principal Auditor）

★

日本セキュリティ監査協会



★

- 公認情報セキュリティ主任監査人
  - 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。
- 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。
- 情報セキュリティ監査人補
  - 情報セキュリティ監査制度に対する知識と経験を有し、OJTとして監査に参加する。監査経験を積んで、公認情報セキュリティ監査人をめざすことができる。
- 情報セキュリティ監査アソシエイト
  - 監査チームリーダの要請によりチームの一員として専門知識にもとづく助言を行う。

★　資格認定要件

資格区分		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
知識	専門分野知識	情報技術分野で少なくとも4年以上の業務経験があること。その内、情報セキュリティ関連分野で少なくとも2年以上の業務経験があること。 なお、下記資格の保有で情報セキュリティ関連分野の業務経験を代替することも可能とする。		情報技術分野で少なくとも3ヶ月以上の業務経験があること、あるいは情報技術分野について、専門的な教育を受けていること。	専門分野（分野は問わない）での3年以上の業務経験を有すること、又は業務経験を代替する資格を保有すること。
	協会認定研修 受講・修了試験 （監査制度の知識）	協会認定の2日間研修コースを受講、履修し協会所定の研修終了試験に合格すること。			
経験	協会認定 トレーニング 受講・修了試験 （監査制度の知識）	協会認定の3日間トレーニングコースを履修し協会所定のトレーニング終了試験に合格すること。			－
	監査経験確認試験	協会認定の監査経験確認試験に合格すること。※		－	－
	実務経験	「公認情報セキュリティ監査人」の実務経験に加えて、過去2年以内に最低3回延べ15日間は、主任情報セキュリティ監査人の指導のもとでの監査チームリーダとしての監査実施経験（うち2回以上は情報セキュリティ監査制度に基づく助言型監査又は保証型監査）があること。	過去3年以内に最低4回延べ20日間の監査メンバーとしての監査実施経験（うち2回以上は情報セキュリティ監査制度に基づく助言型監査又は保証型監査）があること。※	－	－
実証された能力		「公認情報セキュリティ監査人」の実証能力に加えて、資格認定委員会委員による面接審査に合格すること。	監査人、主任監査人、主席監査人又は協会会員からの推薦があること。 （会員企業の社員は推薦は不要）	－	－

※2007年4月末日までに小論文試験を受験し、トレーニングを修了したと認定された者はこの限りではない。

資格取得の手順

・研修については，認定された事業者が実施できる
・また，認定された大学の講座の受講で置換が可能
ただし，修了試験の合格が必要
・修了試験問題，テキストは協会が作成

・研修については，トレーニングコースを認定された事業者が実施できる
・トレーニングについては，認定された大学の講座の受講（演習）で置換が可能　ただし，修了試験の合格は必要
・修了試験問題及びテキストは協会が作成

★

資格制度設計

- 資格認定
  - 資格認定には、監査人としての能力（知識・経験・実証された能力）、監査人としての適切な行動（倫理基準への遵守）が求められており、協会は、これら資格認定の前提となる知識・経験を修得するための研修・トレーニングコースを開催する
- 基本としたしくみ
  - 資格制度を運営するために、ISO/IEC17024（適合性評価ー要員の認証を実施する機関に対する一般要求事項）に則り、協会内の独立した機関として資格認定委員会を設けて、資格制度の運用と資格に係るレベル認定を行う。
  - 有効期間：資格認定月を基準にして3年後の当該半期の末日まで
  - 資格維持活動：資格維持のためには別に定める通り活動実績をポイント換算し、一定水準以上を満たす

資格認定について補足

- 情報セキュリティ監査の立ち上げ
  - 2004年度の「情報セキュリティ監査制度」（公示）に基づいて，資格者を育成するために，10月に特定非営活動法人日本セキュリティ監査協会を設立して，情報セキュリティ監査を実施することになった
  - 2005年から監査人教育を実施し，監査資格者の認定を開始
- 初期の資格者確保
  - 発足から試験制度が出来るまで（2007年4月末）は，グランドファーザ（法改正などで資格が必要になっても、以前からその仕事についていた人は、資格試験を受けなくても今まで通り業務をできる ＝ 既得権益条項）として，資格候補者に，小論文の受験と経験（他資格・経験）を認定して，資格者とした
  - 公認情報セキュリティ監査人資格を最初に，関連資格を追加

★

資格維持（更新）について

- 資格維持プログラム
  - 情報セキュリティの技術変化や、社会的変化による監査ニーズの変化に対応するため、有効期間3年毎に、資格及び専門性の更新を行う
    - 維持活動
    - 監査実績
    - 監査人の学習
    - 社会貢献
- 資格維持ポイント制の導入
  - 資格の社会的な要請に合わせて，資格毎にポイントを設けて，差をつける
  - 年度ごとのポイント取得と3年間での合計取得の二段階
- 公平な維持活動
  - チャレンジ制度
  - 資格保留制度
- 救済措置制度

★

監査実績

項目	摘要	ポイント数
情報セキュリティに関する外部監査・内部監査への従事※1	リーダ（品質管理者の経験含む）	3／1時間
	メンバー	2／1時間

※1： 活動時間には、監査の全体プロセスとそれに付随する作業（資料確認、資料作成など）を含む

監査人の学習

項目	摘要	ポイント数
情報セキュリティ監査に関連する研修・セミナーなどの受講	研修、セミナーなどの受講	1／1時間
	社内研修・社内教育等の受講	1／1時間
自己学習	情報セキュリティ監査に関連する資料等の閲覧※2	1／1時間※3
	CAIS登録者による情報セキュリティ監査に関連する勉強会等の参加	1／1時間
情報セキュリティ関連資格取得	情報セキュリティに関連する資格試験への合格　（CISSP,CISMなど）	5ポイント

※2： 協会ホームページに掲載される月例セミナー資料、協会成果物等

※3： 1年間の上限を5ポイントとする。ただし、学習した内容について、小論文（A4サイズ1枚程度）をまとめた場合、上限を40ポイントとする。

★ 社会貢献

項目	摘要	ポイント数
協会WG活動等※4	リーダ・サブリーダ	2／1時間
	メンバー	1／1時間
講師活動	情報セキュリティ監査に関連する研修、セミナー等の講師	2／1時間
	情報セキュリティ監査に関連する社内研修・社内教育等の講師	1／1時間
執筆活動	協会活動の成果物を含む、他団体などの情報セキュリティ監査に関連する論文、原稿・資料作成およびレビュー	1／1枚
その他、協会が社会貢献に意義があると認める情報セキュリティ監査に関連する活動	協会が主催するイベントのサポート等	1／1時間
	パブリックコメントへの投稿、アンケートへの回答等	1／1枚
	その他	※5

※4： 活動時間に資料作成、資料確認などに要した活動時間を含む場合には、WGリーダ等による活動時間の確認を必要とする。

※5： 申請書の提出が必要、資格認定委員会の審議により活動を承認する。

★

資格区分毎の資格維持ポイント

	年間	3年間合計
主任監査人 監査人	20ポイント以上	120ポイント以上
監査人補	5ポイント以上	20ポイント以上

資格維持のための活動

- 維持申請
  - 毎年，前1年の資格維持活動入力フォームを提出
  - 3年間の維持活動
- チャレンジ制度について
  - 毎年，資格登録者の一定割合（5%）を抽出し，前1年間の維持活動報告の証跡を求め，提示さいれた証拠が不備な場合，活動を実績と見なさない
- 救済措置制度について
  - 合理的な理由により本基準第8条に定められる資格維持ポイントに達しなかった場合，申請があれば資格認定委員会の審査にて救済.
- 資格保留制度について
  - 海外出張、異動、傷病等で長期間の活動が困難な場合の救済制度（適用期間中は資格維持ポイントが免除）

資格維持プログラムの運営が大変

- 資格認定委員会は，毎月実施して，制度の見直しや監査人の新規認定，維持の認定，維持プログラムの見直しを実施している.
- 多いのは，資格取得した後，仕事が変わり維持が難しくなるケースで，個々に判断する必要がある.

資格維持プログラム運営基準

2005 年 08 月 11 日制定
2005 年 12 月 16 日改定
2006 年 04 月 25 日改定
2008 年 04 月 28 日改定
2008 年 08 月 19 日改定
2008 年 11 月 25 日改定
2009 年 09 月 24 日改定
2010 年 10 月 13 日改定
2010 年 12 月 01 日改定
2011 年 12 月 16 日改定
2012 年 1 月 19 日改定
2012 年 7 月 13 日改定
2013 年 12 月 26 日改定