情報セキュリティサービスに関する
審査登録機関基準

経済産業省

平成 30 年 2 月 28 日

目次

第１　目的

この基準は，情報セキュリティサービスに関する審査登録機関に対する要求事項について定めるものである。

なお，本基準の策定に当たっては，JIS Q 17065:2012 を参考としている。

第２　用語及び定義

この規格で用いる主な用語及び定義は，次による。

(1) 審査登録機関

申請者からの申請に基づき情報セキュリティサービス基準に関する適合性の審査及び登録（以下「審査・登録」という。）を行う機関をいう。

(2) 申請者

審査登録機関に対して，自らが行う情報セキュリティサービスに対する審査・登録を申請する者をいう。

(3) 情報セキュリティサービス基準

経済産業省が定めた情報セキュリティサービス基準をいう。

(4) 情報セキュリティサービス

情報セキュリティ監査サービス，脆弱性診断サービス，デジタルフォレンジックサービス及びセキュリティ監視・運用サービスのいずれか又は全てを行うサービス業をいう。

(5) 公平性

客観性の実在をいう。

(6) コンサルティング

審査，登録又は申請された情報セキュリティサービスについて，設計，実施，提供，又は維持に関与することをいう。

第３　総論

１　法的責任

審査登録機関は，その全ての審査・登録に係る活動（以下「審査登録活動」という。）

に法的責任を負うことができる法人又は法人の一部として明確に位置づけられていなければならない。

２　審査・登録の合意

審査登録機関は，申請者への審査活動の提供に関し，法的に拘束力のある合意を結ばなければならない。審査・登録の合意は，審査登録機関及び申請者が負うべき責任を考慮に入れなければならない。

３　公平性

⑴ 審査・登録活動は，公平に行われなければならない。

⑵ 審査登録機関は，その審査・登録の公平性に責任を負い，公平性を損なう商業的，財務的又はその他の圧力を容認してはならない。

⑶ 審査登録機関は，その公平性に対するリスクを継続的に特定しなければならない。

⑷ 審査登録機関は，公平性に対するリスクが特定された場合には，どのように当該リスクを排除又は最小化するかを実証できなければならない。また，第４の２に規定する仕組みにおいて，当該リスクに関する情報を利用できるようにしなければならない。

⑸ 審査登録機関には，公平性に対するトップマネジメントの宣言がなければならない。

⑹ 審査登録機関並びに審査登録機関が属する同じ法人及び審査登録機関の組織統制のもとにある法人のいかなる部門も，次に掲げる事項を行ってはならない。

ア　審査・登録された情報セキュリティサービスの設計，実施，提供又は維持

イ　申請者へのコンサルティングの申出又は提供

ウ　審査・登録の規則が申請者のマネジメントシステムの評価を要求している場合に，当該申請者に対するマネジメントシステムのコンサルティング又は内部監査の申出又は提供

⑺ 審査登録機関は，審査登録機関と関係のある別法人の活動，又は審査登録機関がその一部を構成する法人と関係のある別法人の活動が，審査・登録活動の公平性を損なわないことを確実にしなければならない。

⑻ ⑺ に示す別法人が，審査・登録されたサービス又は審査・登録に関するコンサ

ルティングを申し出る又は提供する場合，審査・登録機関の経営層の要員並びにレビュー及び審査・登録の決定のプロセスに関わる要員は，その別法人の活動に従事してはならない。また，その別法人の要員を，審査・登録機関のマネジメント，レビュー及び審査・登録の決定に関与させてはならない。

(9) 審査登録機関の活動は，コンサルティングを提供する組織の活動と結び付けてマーケティング又は営業をしてはならない。審査登録機関は，特定のコンサルティング組織を用いれば，認証が簡単，容易，迅速又は廉価になる旨の明示又は暗示をしてはならない。

(10) 審査登録機関は，要員がコンサルティングを提供した情報セキュリティサービスの審査に，審査登録機関が規則において規定する期間，当該要員を従事させてはならない。

(11) 審査登録機関は，他の個人，機関又は組織の活動から生じた公平性に対する何らかのリスクが認められた場合，それに対応する行動をしなければならない。

(12) 審査に影響を及ぼし得る全ての審査登録機関の要員（内部か外部かを問わない。）及び委員会は，公平に行動しなければならない。

４　債務及び財務

(1) 審査登録機関は，その運営から生じる債務を担保できる適切な備え（例えば，保険，別組織による債務負担行為又は準備金）をもたなければならない。

(2) 審査登録機関は，財務上の安定性及びその運営に必要な経営資源をもたなければならない。

５　非差別的条件

(1) 審査登録機関の事業を遂行するための方針及び手順，並びにその運用は，差別的であってはならない。

(2) 審査登録機関は，審査・登録の範囲内の活動を行う全ての申請者が，当該審査を利用できるようにしなければならない。

(3) 審査登録機関は，審査・登録に当たり，次に掲げるものを条件とした差別的取扱いをしてはならない。

ア　申請者の規模，又は協会若しくはグループの会員であること。

イ　既に適合性が審査・登録された情報セキュリティサービスの件数

ウ　不当な財務的又はその他の条件

(4) 審査登録機関は，審査・登録活動を，情報セキュリティサービス基準に基づく審査・登録範囲に関係する事項に限定しなければならない。

６　機密保持

(1) 審査登録機関は，審査・登録を実施するために得られた又は生じた全ての情報を，申請者が公開している情報及び公開に同意している情報を除き，機密情報とし，その管理について，責任を負わなければならない。

(2) 審査登録機関は，正当な理由又は申請者の同意なしに機密情報を開示してはならない。

(3) 申請者以外（例えば，苦情申立者又は規制当局）から得られた申請者に対する情報は，機密として取り扱わなければならない。

７　情報の公開

審査登録機関は，次の情報を（出版物，電子媒体又はその他の手段を用いて）維持し，要請に応じて利用できるようにしなければならない。

(1) 審査・登録手続についての情報

(2) 申請者に課せられる料金に関する一般的情報

(3) 申請者の権利及び義務の記述。これには，審査登録機関の名称，審査結果及び登録簿への記載についての言及方法に関する，要求事項又は制約事項を含む。

(4) 苦情及び異議申立ての処理手順に関する情報

第４　審査登録機関の組織

１　審査登録機関

審査・登録活動は，公平性が確保されるように組織され，管理されなければならない。

審査登録機関は，審査・登録に関わる要員及び全ての委員会の責任及び権限を示す組織構造を文書化しなければならない。

２　公平性確保のための仕組み

⑴ 審査登録機関は，その公平性を確保するための仕組みをもたなければならない。

⑵ 公平性を確保するための仕組みは，文書化されなければならない。

⑶ 審査登録機関は，公平性を確保するための仕組みに，主要な利害関係者の参加を求めなければならない。

第５　審査・登録の資源

１　審査・登録要員

⑴ 審査登録機関は，審査・登録の実施に必要な専門的な知見及び能力を有する者を確保しなければならない。

⑵ 審査・登録に関係する者は，正当な理由がある場合を除き，審査・登録を実施する過程で得られた又は生じた全ての情報について機密を守らなければならない。

２　外部委託

審査登録機関は，外部委託を行う場合にあっては，外部委託を受けた者の本基準該当事項の遵守も含め，外部委託を受けた者が行った委託に基づく行為の責任の全てを負わなければならない。

第６　審査手続

１　審査の基準

審査登録機関は，経済産業省が定める「情報セキュリティサービス基準」に基づいて審査・登録を行わなければならない。

２　申請

申請の受付に当たって，審査登録機関は，次に掲げる審査・登録を完了するために必要な全ての情報を申請書に記載させる等の方法により取得しなければならない。

⑴ 審査・登録を求める情報セキュリティサービスの種別

⑵ 申請者の名称，所在地その他申請者を識別することができる情報

⑶ 情報セキュリティサービスを実施する方法を確認することができる情報

⑷ 前各項に掲げるもののほか，情報セキュリティサービスの審査・登録に必要とな

る情報

3　申請のレビュー

(1) 審査登録機関は，次に掲げる事項を明らかにするために，申請内容のレビューを行わなければならない。

ア　申請者及び情報セキュリティサービスについての情報が，審査・登録を実施する上で十分であること。

イ　審査・登録を求めている情報セキュリティサービスの範囲が明確であること。

(2) 審査登録機関自身が申請者に既に行った審査の結果を理由として，審査の一部を省略する場合には，審査登録機関は，その記録の中で，当該審査の結果に言及しなければならない。また審査登録機関は，審査の省略を正当とする理由を示さなければならない。

(3) 審査登録機関は，申請のレビューの結果，申請内容から(1)に掲げる事項が明らかにされていることが確認できなかった場合には，その旨を申請者に通知しなければならない。

(4) 審査登録機関は，(3)の通知を行ったにも関わらず，申請者により(1)に掲げる事項が明らかにされていることが確認できる申請内容の是正がされない場合には，その旨及びその理由を申請者に通知し，申請のレビューを終了させなければならない。

4　審査

(1) 審査登録機関は，規則において，情報セキュリティサービス基準に基づき申請者が必要となる資格要件等について，判断の指針となる内容を定めなければならない。

(2) 審査登録機関は，審査・登録の実施を可能とする体制の整備をしなければならない。

(3) 審査登録機関は，規則に従って，審査・登録を実施しなければならない。

(4) 審査登録機関は，審査の結果，申請に係る情報セキュリティサービスが基準に不適合となる事由が認められる場合には，全ての不適合を申請者に通知し，是正を要求しなければならない。

(5) 審査登録機関は，(4)の場合に申請者から審査の継続を求められた場合には，申請者において不適合が是正されたことについて，審査登録機関が検証するために必要となる情報の提供を求め，審査手続を繰り返さなければならない。

(6) 全ての審査の結果は，文書化されなければならない。

５　審査の結果

(1) 審査登録機関は，審査の結果に責任を負い，かつ，権限を持たなければならない。

(2) 審査登録機関は，申請に係る情報セキュリティサービスが情報セキュリティサービス基準及び審査・登録の規則に適合する場合には，その旨を申請者に通知しなければならない。

(3) 審査登録機関は，４(4)の通知を行ったにも関わらず，期限までに申請者により不適合となる事由が是正されない場合には登録できない旨及びその理由を申請者に通知し，審査手続を終了させなければならない。

６　審査結果文書

(1) 審査登録機関は，５(2)の通知を行う場合には，次に掲げる内容を記載した文書（以下「審査結果文書」という。）を申請者に提供しなければならない。

ア　審査登録機関の名称及び住所

イ　登録簿への登録を行った日付

ウ　申請者の名称，所在地その他申請者を識別することができる情報

エ　情報セキュリティサービスの種別

オ　登録の期間又は有効期限

カ　前各号に掲げるものの他審査の規則により記載することとされている情報

(2) 審査登録機関は，審査結果文書に審査登録機関の責任者の署名その他の審査・登録の規則に定められた，申請に係る情報セキュリティサービスが情報セキュリティサービス基準及び審査・登録の規則に適合していることを認める旨を記載しなければならない。

７　登録

審査登録機関は，情報セキュリティサービス基準及び審査・登録の規則に適合している情報セキュリティサービスに関して，次に掲げる項目を含む情報を記載した登録

簿を作成し，インターネットの利用により公示する方法その他の規則の定める方法により公表しなければならない。

(1) 情報セキュリティサービスの種別

(2) 申請者の名称，所在地その他申請者を識別することができる情報

(3) 前各項に掲げるものの他規則により記載することとされている情報

８　サーベイランス

(1) 登録簿に登録された者（以下「登録者」という。）が，その登録簿の有効期間内に，情報セキュリティサービス基準又は審査・登録の規則に適合しないことが明らかとなった場合その他サーベイランスが要求される場合には，審査登録機関は，審査・登録の規則に定めるところにより，情報セキュリティサービスのサーベイランスを実施しなければならない。

(2) 審査登録機関がサーベイランスを行う場合には，４から６までに定める規定を準用する。

９　審査・登録に影響を与える変更

(1) 審査登録機関は，審査・登録の規則の内容の変更をし，当該変更が申請者が既に行っている申請に影響することが認められる場合には，当該変更を全ての申請者に連絡しなければならない。

(2) 審査登録機関は，申請者による変更も含め，審査又は登録に影響を与えるその他の変更も考慮し，適切な処置を決定しなければならない。

10　サーベイランスに基づく対応

(1) 審査登録機関は，サーベイランスを実施した結果，登録者が行う情報セキュリティサービスについて，情報セキュリティサービス基準又は審査・登録の規則への不適合が立証された場合には，次に掲げる場合の区分に応じ，規則に定める取扱いを行うことを決定しなければならない。

ア　登録者が行う複数の登録情報セキュリティサービスの一部だけが不適合となった場合であって，登録者が不適合の是正を行う旨の意思表示を行わない場合　不適合となった情報セキュリティサービスを除く旨を内容とする登録簿の修正

イ　登録者が行う複数の登録情報セキュリティサービスの一部又は全部が不適合と

なった場合であって，登録者が不適合の是正を行う旨の意思表示を行う場合　登録者が不適合を是正するまでの間の不適合となった情報セキュリティサービスの登録簿への登録の一時停止

ウ　登録者が行う登録情報セキュリティサービスの全部が不適合となった場合であって，登録者が不適合の是正を行う旨の意思表示を行わない場合　登録簿からの抹消

(2) (1)の決定を行った場合には，登録者に対して，その旨を通知しなければならない。

(3) 審査登録機関は，(1)イの取扱いを決定した場合，登録者に対して，不適合が是正されたことについて，審査登録機関が検証するために必要となる情報の提供を求めなければならない。

(4) 審査登録機関が追加のサーベイランスを行う場合には，４から６までに定める規定を準用する。

(5) 審査登録機関は，追加の再審査の結果，不適合の是正がされたと判断でき，登録簿への登録を復帰させる場合には，審査の規則の定めるところにより必要とされる登録簿の修正を行わなければならない。

(6) 審査登録機関は，追加のサーベイランスの結果，不適合の是正がされたと判断できなかった場合には，その旨及びその理由を登録者に通知しなければならない。

11　登録の終了，一時停止又は取り消し

申請者の要請によって登録が終了する場合，又はサーベイランスその他の結果として登録が一時停止若しくは取消しになった場合，審査登録機関は審査・登録の規則の定めるところにより，必要な処置を取らなければならない。

12　記録

(1) 審査登録機関は，審査・登録手続が適切に実施されたこと（サーベイランスを実施した場合を含む。）を実証する記録を保管しなければならない。

(2) 審査登録機関は，記録の機密を保たなければならない。記録を，移送，伝送及び転送する場合には，機密保持が確実にされる方法で行わなければならない。

(3) 審査登録機関は，審査・登録の規則により定められた期間，記録を保管しなければならない。

13　苦情及び異議申立て

(1) 審査登録機関は，苦情及び異議申立てを受領し，評価し，苦情及び異議申立てに関して決定するための手続を定めなければならない。審査登録機関は，苦情及び異議申立て並びにそれを解決するためにとった処置を記録し，処理経過を追跡できるようにしなければならない。

(2) 審査登録機関は，苦情又は異議申立てを受領したときには，それが当該審査登録機関が行った審査・登録に関連するものかどうかを確認し，関連があることが認められた場合には，その苦情又は異議申立てを処理しなければならない。

(3) 審査登録機関は，正式な苦情又は異議申立てとしての受領を，申立者に対し通知しなければならない。

(4) 審査登録機関は，苦情又は異議申立てについて決定に達するために必要な（できる限り）全ての情報の収集及び検証に責任をもたなければならない。

(5) 審査登録機関は，利害抵触がないことを確実にするために，２年以内に申請者にコンサルティングを提供した要員又は申請者に雇用された要員を，この申請者に対する苦情又は異議申立ての解決のレビュー又は承認に従事させてはならない。

(6) 審査登録機関は，可能な場合には必ず，苦情処理プロセスの結果及び終了を申立者に対し正式に通知しなければならない。

(7) 審査登録機関は，異議申立て処理プロセスの結果及び終了を申立者に対し正式に通知しなければならない。