クラウド情報セキュリティ監査制度運営細則

第１章　総　則

第1条（目的）

この細則は、クラウド情報セキュリティ監査制度規程（以下「規程」という。）第 18 条の定めにより、クラウド情報セキュリティ監査制度の運営に係る細則を定めることを目的とする。

第2条（基本リスク、監査標準手続、外部評価手続の開示）

協議会は、規程第 15 条 1 項の委任に基づき、規程第 8 条、規程第 10 条及び規程第 11 条の定めにより、基本リスク、監査標準手続及び外部評価手続を定め、これらを協議会員及び規程第 12 条 2 項の申請をする者に開示する。

第3条（クラウド情報セキュリティ内部監査人の要件）

規程第 6 条１項に定めたクラウド情報セキュリティ内部監査人は、以下の要件を満たす情報セキュリティ監査人とする。

1. 公認情報セキュリティ監査人以上の資格を有すること
2. クラウドコンピューティングサービスに関する付表１に示す技術的知識を有すること
3. クラウド情報セキュリティ監査制度に関する知識を有すること

第4条（クラウド情報セキュリティ外部監査人の要件）

規程第 6 条２項に定めたクラウド情報セキュリティ外部監査人は、以下の要件を満たすこととする。

1. 公認情報セキュリティ監査人以上の資格を有すること
2. クラウドコンピューティングサービスに関する付表１に示す技術的知識を有すること。ただし保有資格をもって要件を満たすとする場合には、付表２に示す資格のいずれかを保有していること
3. クラウド情報セキュリティ監査制度に関する知識を有すること
4. 情報セキュリティ監査を業として行うために必要な内部管理体制を保有し、付表３に示す組織に所属していること

第２章　使用許諾

第5条（CS マークの使用許諾の要件）

１、協会が規程第 12 条第１項に定める CS シルバーマークの使用を許諾することができる者は、以下の要件を満たす CS 言明をした協議会員とする。

1. 基本リスクの全部又は一部に対する基本言明要件についての情報セキュリティ対策に関する所定の様式によること
2. 第 7 条に定める要件を満たす監査が行われた監査報告日から 3 年以内であること

2、協会が規程第 12 条第２項に定める CS ゴールドマークの使用を許諾することができる者のうち会員は、以下の要件を満たす CS 言明をしていなければならない。

1. 基本リスクの全部に対する基本言明要件についての情報セキュリティ対策に関する所定の様式によること
2. 前項第 2 号に定める要件を満たすこと
3. 第 8 条に定める要件を満たす監査が行われていること

3、協会が規程第 12 条第２項に定める CS ゴールドマークの使用を許諾することができる者のうち会員以外の者は、協会が定める事業者審査に適合し、かつ、以下の要件を満たす CS 言明をしていなければならない。

1. 基本リスクの全部に対する基本言明要件についての情報セキュリティ対策に関する所定の様式によること
2. 本条第１項第 2 号に定める要件を満たすこと
3. 第 8 条に定める要件を満たす監査が行われていること

第6条（標準と定める情報セキュリティ監査）

規程第 9 条の定めにより、標準と定める情報セキュリティ監査は、以下の要件を満たすものと定める。

1. 情報セキュリティ監査基準に準拠した監査であること
2. 基本リスクに対して、クラウド情報セキュリティ管理基準に準拠した管理策が実装され、運用されていることについての監査であること
3. 第 3 条に定めるクラウド情報セキュリティ内部監査人が行う監査であること。
4. クラウド情報セキュリティ内部監査人の独立性が確保されていること
5. 監査標準手続に準拠した監査手続により行われた監査であること
6. 所定の様式で監査のプロセスが記録されて、第三者がその妥当性を評価できること
7. 前 1～6 号の要件を満たすことについて、根拠資料に基づき説明が可能であること

第7条（自主監査の要件）

規程第 4 条２項に定める自主監査の要件は、以下のとおりとする。

1. 対象とするクラウドコンピューティングサービス及び情報セキュリティ対策を施した基本リスクを明確にした CS 言明が、所定の様式の言明書に記載されていること
2. 前号の CS 言明に対し、第 6 条の要件を満たす標準と定める情報セキュリティ監査が実施され、言明通りであることが確認されていること

第8条（適合監査の要件）

規程第 4 条３項に定める適合監査の要件は、以下のとおりとする。

1. 第 7 条の要件を満たす自主監査であること
2. 第 4 条に定めるクラウド情報セキュリティ外部監査人により、外部評価手続に従

って自主監査の品質が評価されること

3. 前号の評価を行うクラウド情報セキュリティ外部監査人は、被監査主体から独立した外部の組織に所属していること
4. 第 2 号の評価の結果に基づき、協会により標準と定める情報セキュリティ監査に適合すると認められること

第9条（審査の届出及び CS マークの使用許諾）

下記に関わる手続きについては、別途定める補則による。

1、自主審査の届出及び CS シルバーマークの使用許諾

2、適合審査の届出及び CS ゴールドマークの使用許諾

3、CS シルバーマーク及び CS ゴールドマーク使用継続又は使用中止

第10条 （CS マークの使用許諾期間）

CS マークの使用許諾期間は原則 3 年とする。なお、使用許諾申請の期間を含む許諾期間の取扱いについては別途定める。

第11条 （CS シルバーマークの使用許諾の独立と CS ゴールドマークの使用許諾の従属）

1、同一の CS シルバーマークの使用対象とされる複数の CS 言明書がある場合、ある CS 言明書に対する CS シルバーマークの使用許諾は、他の CS 言明書に対する同一の CS シルバーマークの使用許諾から独立したものとする。

2、同一の CS ゴールドマークの使用対象とされる複数の CS 言明書がある場合、ある CS 言明書に対する CS ゴールドマークの使用許諾は、他の CS 言明書に対する同一の CS ゴールドマークの使用許諾に従属したものとする。

第12条 （CS マークの使用許諾の取消）

協議会は、CS マークの使用許諾に係る要件が以下の各号のいずれかに該当すると認める場合には、CS マークの使用許諾を取り消すことができる。

1. 第 5 条の要件を満たさない場合
2. 第 7 条又は第 8 条の要件を満たさない場合
3. 本細則の定めに基づいて行われた申請若しくは届出に重大な瑕疵がある場合又は必要な申請若しくは届出が行われなかったと認められる場合
4. その他、CS マークの使用許諾を受けた者に、本制度の主旨に反した行為があったと協議会が認めた場合

第13条 （CS マークの使用許諾の解除）

協議会は、CS マークの使用許諾に係る要件が次の各号のいずれかに該当すると認める場合には、CS マークの使用許諾を解除することができる。

1. CS マークの使用許諾を受けた者が、協議会が別途定める CS マーク使用規定に違反した場合
2. CS マークの使用許諾を受けた者が、協会により除名、資格停止の処分をうけた場合

3. CS マークの使用許諾を受けた者が、第 5 条に定める CS マークの要件を満たさないと認められる場合
4. CS マークの使用許諾を受けた者が、反社会的な行為を行った、又は、行うおそれがある場合
5. CS マークの使用許諾を受けた者が、第 17 条各号の責務を怠った場合

第 14 条　（CS マークの使用許諾の失効）

CS マークの使用許諾は、以下の各号のいずれかに該当する場合には、失効する。

1. 協議会会員であって、CS マークの使用許諾を受けた者が協議会を退会した場合
2. CS マークの使用対象とする CS 言明書に記載のクラウドコンピューティングサービスが提供されなくなった場合
3. CS マーク使用中止の届出がなされた場合

第 15 条　（使用許諾の消滅した CS マークの取扱）

1、CS マークの使用許諾を受けた者が以下のいずれかの事由によりその使用許諾が無効となったときには、使用許諾されていた CS マークを、別途定める CS マーク使用規定に従い、処分しなければならない。

1. CS マークの使用許諾期間が終了したとき
2. CS マークの使用許諾を取消されたとき
3. CS マークの使用許諾が解除されたとき
4. CS マークの使用許諾が失効したとき

2、協議会は前項の事由により使用許諾の消滅した CS マークを公表することができる。

第 3 章　責　務

第 16 条　（CS マークの表示の責務）

1、CS シルバーマークの使用許諾を受けた者は、別途定める CS マーク使用規定に従って、当該 CS シルバーマークをその使用対象となる CS 言明書に表示しなければならない。

2、CS ゴールドマークの使用許諾を受けた者は、別途定める CS マーク使用規定に従って、当該 CS ゴールドマーク、前項の CS シルバーマークのいずれか一方又は両方をその使用対象となる CS 言明書に表示しなければならない。

第 17 条　（CS マークの使用許諾を受けた者の責務）

CS マークの使用許諾を受けた者は、以下の各号の責務を負う。

1. 別途定める CS マーク使用規定に従ったマークの使用
2. 第 6 条 7 号に規定する根拠資料の保全
3. クラウド情報セキュリティ監査で確認された管理策の確実な実施の継続
4. クラウド情報セキュリティ監査に関して協議会が行う調査活動への協力
5. 申請時に届け出たクラウド情報セキュリティ内部監査人が CS マークの使用許諾

を受けた者の指揮命令下にある場合、その能力の維持

6. CS マーク及びクラウド情報セキュリティ監査制度についての正しい広告・周知など、クラウドコンピューティングサービスの利用者の啓発活動
7. CS マークの使用対象となる CS 言明書に記載のクラウドコンピューティングサービスにおいて言明内容を棄損する懸念のあるインシデントが発生した場合の協議会への速やかな通知及び事後の報告（ただし、別途定める場合にはこの限りでない）
8. CS マークの使用対象となる CS 言明書に記載のクラウドコンピューティングサービスにおける情報セキュリティ事故に関して協議会が行う調査活動への協力
9. CS ゴールドマークの使用対象となっている CS 言明書に関わる対策の実施状況確認を目的とした自主監査の、少なくとも年 1 回の実施
10. 前号の自主監査の実施状況を確認するために協議会が別途定める様式の書面の協議会への少なくとも年 1 回の届出（ただし、協議会員を除く）

第 18 条 （クラウド情報セキュリティ監査人の責務）

1、監査人倫理規程は、当該規程のうち「特定非営利活動法人日本セキュリティ監査協会」を「協議会」と、「情報セキュリティ監査」を「クラウド情報セキュリティ監査」と、「情報セキュリティ監査人」を「クラウド情報セキュリティ監査人」と読み替えて、これを適用する。ただし、監査人倫理規程第 9 条は除く。

2、CS マークの使用許諾の届出に関わる自主監査を行ったクラウド情報セキュリティ監査人は、協議会が当該自主監査に関して行う調査活動に対し、その求めに応じて情報提供を行うなど、これに協力しなければならない。

3、CS マークの使用許諾の届出に関わる外部評価手続の結果を報告したクラウド情報セキュリティ外部監査人は、協議会が当該適合監査に関して行う調査活動に対し、その求めに応じて情報提供を行うなど、これに協力しなければならない。

第 4 章 制度維持の活動

第 19 条 （CS マークの信頼性に係る調査）

協議会は、CS マークの使用対象となる CS 言明書に記載のクラウドコンピューティングサービスの情報セキュリティに関わる事故（以下「情報セキュリティ事故」という。）の発生などにより CS マークの信頼性に疑義が生じた場合、規程第 14 条 1 号に定める措置として、以下の各号の調査をすることができる。

1. 当該 CS マークの使用許諾を受けた者に対する当該情報セキュリティ事故に関する調査
2. 当該 CS マーク使用許諾のための届出に関わる自主監査を行った、クラウド情報セキュリティ監査人に対する、当該自主監査に関する調査
3. 当該 CS マークに関して外部評価手続の結果を報告した、クラウド情報セキュリティ外部監査人に対する当該外部評価手続に関する調査

第20条　（事故対策委員会）

協議会は、前条に規定する情報セキュリティ事故が発生した場合、事故対策委員会を設置し、これに前条に規定する調査又は広報等の対処をさせることができる。

第21条　（審査委員会への報告）

協議会は、第 19 条の調査の結果、調査対象となった同条第 2 号のクラウド情報セキュリティ監査又は同条第 3 号の外部評価に瑕疵があり、情報セキュリティ事故の発生又は被害に影響を及ぼしたと認められる場合には、速やかに特定非営利活動法人日本セキュリティ監査協会の審査委員会（以下、「審査委員会」という）に報告し、その裁定を仰がなければならない。

第22条　（処分）

協議会は、前条のクラウド情報セキュリティ監査の瑕疵が JASA-クラウドセキュリティ推進協議会運営規則（以下「協議会運営規則」という。）第 9 条 3 号に該当すると認められる場合には、審査委員会の裁定を経て、以下の各号の処分を行うことができる。

1. 協議会運営規則第 9 条 1 号の定めによる除名、資格停止、又は戒告
2. クラウド情報セキュリティ外部監査人の登録名簿の記載抹消

第23条　（監査の品質の維持活動）

協議会は、規程第 14 条 2 号に定める措置として、以下の各号の措置を講じることができる。

1. 基本リスク、クラウド情報セキュリティ管理基準及び監査標準手続について、国際標準の動向等に応じ、適宜見直しを行う。
   ① 協議会は、改訂前後の経緯が分かるように、基本リスク、クラウド情報セキュリティ管理基準及び監査標準手続の版の管理を行う。
   ② 協議会は、基本リスク、クラウド情報セキュリティ管理基準及び監査標準手続の改訂の公表にあたり、適切と定めた経過期間を公表する。
2. 協議会員が適正な内部監査を行っているかについて調査等を行い、必要に応じて、制度の見直しや協議会員に対する是正等の勧告を行う。
3. 品質維持活動が適正に行われているかを監視する。
4. その他、必要な措置。

第24条　（監査人の品位と力量の維持活動）

協議会は、規程第 14 条 3 号に定める措置として、協議会員に対し監査の力量を保つための教育・研修の機会を提供する。

第25条　（細則の変更）

この細則の改定は協議会の総会の議決による。

付表 1　クラウドコンピューティングサービスに関する技術知識

項番	内　　容
1.	クラウド固有の技術知識 ・クラウドコンピューティングのコンセプト ・クラウドコンピューティングのアーキテクチャ
2.	クラウド固有のリスクの知識
3.	クラウド固有のセキュリティ管理策の知識

付表２　申請可能な外部資格

項番	内　　容	資格の運営組織
1.	CCSK (Certificate of Cloud Security Knowledge)	Cloud Security Alliance (CSA)
2.	CCSP (Certified Cloud Security Professional)	International Information Systems Security Certification Consortium (ISC)²
3.	ISMS クラウドセキュリティ審査員	マネジメントシステム審査員評価登録センター(JRCA)

付表３　外部監査人の所属組織

項番	内　　容
1.	当協議会に所属する監査法人
2.	情報セキュリティサービス基準適合サービスリストに監査サービスの実施主体として登録済の組織

附　則

第1条（施行期日）

この細則は、平成 27 年 1 月 29 日より適用する。

この細則は、平成 27 年 4 月 24 日より適用する。

この細則は、平成 28 年 3 月 9 日より適用する。

この細則は、平成 28 年 6 月 16 日より適用する。

この細則は、平成 29 年 7 月 20 日より適用する。

この細則は、平成 30 年 10 月 19 日より適用する。

この細則は、令和1年6月24日より適用する。

この細則は、令和3年6月24日より適用する。

第2条（経過措置）

細則第7条第2号において引用する同第6条第3号においてさらに引用する同第3条第1号の「公認情報セキュリティ監査人」及び同第4条第1号の「公認情報セキュリティ監査人」は、令和4年3月末日までの間に限り、「情報セキュリティ監査人補」に読み替えて適用する。

本経過措置を見直す場合には、別途定める補則において行う。

第3条（有効期日見直しに関する経過措置）

平成30年9月末日までに初回の自主監査を行って使用許諾を認められたCSマークについては、平成30年10月19日の本細則の改訂に伴い、使用許諾の期間を6ヵ月間延長する。

本経過措置を見直す場合には、別途定める補則において行う。