クラウドセキュリティ監査制度における
内部監査人の独立性ガイドライン

Ver2.0

2016 年 7 月 14 日

特定非営利活動法人　日本セキュリティ監査協会
JASA－クラウドセキュリティ推進協議会

目　　次

1. はじめに

本ガイドラインは JASA-クラウドセキュリティ推進協議会が実施するクラウドセキュリティ監査制度にもとづき、クラウド事業者の内部監査により取得できる内部監査済言明書「CS マーク」付与にかかる内部監査の過程において、監査を実施する内部監査人が担保するべき独立性の考え方について記載するものです。

CS マーク（シルバー）
内部監査済言明書

クラウドセキュリティ監査制度は、クラウドサービスの普及の過程において、クラウドサービスを利用することを希望する企業が抱えるリスクや採用の障壁として、常に課題の上位に挙げられる情報漏えいや法規制・コンプライアンスなどのセキュリティに対する不安や懸念の解消とサービス選択時のセキュリティに関する選定基準を明確化することを目指して制定された制度です。

クラウドサービスの安全対策は利用者から直接見ることが難しいため、クラウドサービス事業者が適切な対策を講じ、それを利用者に説明することが求められます。事業者が適切な対策を講じていることを利用者に納得して頂くためには、クラウド事業者が公平かつ一定な基準に基づき、定められた手順を順守して、サービスの安全対策を行うことが、まず基本となります。更に、サービスの安全対策の実務について監査を行い、その結果を公開することが必要です。

クラウド情報セキュリティ監査制度では、この情報公開を「言明書」の形で行います。公開される言明書が定められた方法による一定水準以上の内容であり、かつ公平・公正に行われたことにより、信頼できる監査により、確認された結果であることを示す査証が「CS マーク」です。

「CS マーク」は、内部監査の結果に基づき付与されるマークです。クラウドサービス事業者自身による内部監査であっても、監査を実施する監査人は「公認情報セキュリティ監査

人[1]」以上の資格を保有し、かつ、クラウド特有のリスクに関する教育を受けた者に限定されています。

公平で公正な監査を実施するためには、資格保有者であっても、監査人にはクラウドサービス事業者の組織内での独立性が求められます。この独立性を定義したものが本ガイドラインです。

なお、本ガイドラインは特定非営利活動法人 日本セキュリティ監査協会 審査委員会「情報セキュリティ監査人の独立性のガイドライン」をベースとして「CS マーク」の内部監査人の独立性に特化して記載されたものとなっています。

また、情報セキュリティ監査全般に関する情報セキュリティ監査人の独立性の考え方や公認情報セキュリティ監査人としての独立性に関しては「情報セキュリティ監査人の独立性のガイドライン」を参照してください。[2]

2. 独立性の意義

クラウドセキュリティ監査制度の根拠となる情報セキュリティ監査基準では、情報セキュリティ監査を客観的に実施するために、監査人に対して監査対象から独立していることを求めています。

表 2-1 情報セキュリティ監査基準（抜粋）

一般基準 １．目的、権限と責任 情報セキュリティ監査を実施する目的及び対象範囲、並びに情報セキュリティ監査人の権限と責任は、文書化された規程又は契約書等により明確に定められていなければならない。 ２．独立性、客観性と職業倫理 ２．１ 外観上の独立性 情報セキュリティ監査人は、情報セキュリティ監査を客観的に実施するために、監査対象から独立していなければならない。監査の目的によっては、被監査主体と身分上、密接な利害関係を有することがあってはならない。 ２．２ 精神上の独立性 情報セキュリティ監査人は、情報セキュリティ監査の実施に当たり、偏向を排し、常に公正かつ客観的に監査判断を行わなければならない。 ２．３ 職業倫理と誠実性 情報セキュリティ監査人は、職業倫理に従い、誠実に業務を実施しなければならない。

[1] 2020 年までは情報セキュリティ監査人補でもよい

[2] 「情報セキュリティ監査人の独立性のガイドライン」
http://www.jasa.jp/about/examine/downf/judger11.pdf

表 2-1 に示すように、同基準では、情報セキュリティ監査を客観的に実施することの要件として、精神上の独立性だけでなく、外観上の独立性も監査人に求めています。

2.1. 外観上の独立性

外観上の独立性とは、第三者から見た際に、誠実性、客観性が阻害されていると推測される次のような事実や環境を避けることを言います。

１）禁止すべき利害関係（経済的利害関係）

２）避けるべき外観（不適正な外観）

監査人と被監査主体の間に監査の判断を歪める恐れのある身分上または利害上の関係があると、監査結果に疑義が生じる恐れがあります。したがって、監査人の独立性の保持に疑いをもたれるような関係や外観を避けるための措置を講じる必要があります。

2.2. 精神上の独立性

「情報セキュリティ監査人は、情報セキュリティ監査の実施に当たり、偏向を排し、常に公正かつ客観的に監査判断を行わなければならない。」と一般基準には記載されています。これはクラウドセキュリティ監査についても同様です。

ここで「偏向を排し」とは、情報セキュリティ監査の専門家としての判断をゆがめるおそれのある諸要因から影響を受けない精神状態を保持していることをいいます。

「常に公正かつ客観的に監査判断を行わなければならない」とは、客観性を確保し、専門家としての公正不偏な態度を堅持できる状態を保持していることをいいます。

2.3. 職業倫理と誠実性

「情報セキュリティ監査人は、職業倫理に従い、誠実に業務を実施しなければならない。」と一般基準に記載されています。CS マークに関わる内部監査人の職業倫理も日本セキュリティ監査協会が定めている監査人倫理規定[3] に記載の内容を参照してください。

3. 監査人倫理規定における独立性

日本セキュリティ監査協会が定めたこの監査人倫理規定では、監査人の基本的責務の一つとして、監査人が情報セキュリティ監査業務を行うに際して外観上の独立性、精神上の独立性及び誠実性を求めています。また監査人が独立性を損なっている場合には、協会は、監査人が本倫理規程に違反したとして、監査人資格の剥奪または監査人に対する戒告を行うことができる（日本セキュリティ監査協会監査人倫理規定第 10 条）と規定されています。なお、この処分を行う際には、協会の審査委員会の裁定を経ることになっています。

---

[3] 日本セキュリティ監査協会「監査人倫理規定」
http://www.jasa.jp/qualification/regulationf/regul11.pdf

表 3-1　日本セキュリティ監査協会監査人倫理規定（抜粋）

監査人倫理規程　（2004 年 11 月 4 日制定） 第３条（監査人の基本的責務） １．　監査人は、情報セキュリティ監査制度の普及促進、監査技術の向上、監査主体の質の向上、ならびに監査制度の国際標準の調査研究や改善提言への協力を通じて、情報セキュリティ監査制度の健全な発展に寄与しなければならない。 ２．　前項の目的を達するため、監査人が情報セキュリティ監査業務を行うに際しては、外観上の独立性、精神上の独立性、誠実性、秘密保持に努めなければならない。

4. CS マーク取得における内部監査人の独立性

「CS マーク」発行を目指すクラウドサービスの監査は内部監査として実施されます。この場合、監査の対象となるクラウドサービスの企画・設計・構築・運用を行う部門やサービス担当者が「被監査主体」として定義されます。同様に「報告書の利用者」とは経営者またはクラウドサービスの事業責任者、情報システム管理責任者（CIO／CISO）など、言明を行う責任者（言明書冒頭に氏名を記載する責任者）を指します。

クラウドサービスに対する情報セキュリティ内部監査では、技術的な知識等の制約から事業部門[4]に所属する者が監査業務に携わらざるを得ない状況があり得ます。監査部門など事業部門から独立した部門による監査であれば、監査人の独立性が確保しやすいのですが、事業部門に所属した内部監査人が監査チームに含まれる場合には外観上の独立性が曖昧となるおそれがあります。このような場合でも、適切な管理を行い監査人の独立性を確保することで、情報セキュリティ内部監査の品質を保つ必要があります。

この点を踏まえて、情報セキュリティ内部監査における監査人の独立性の条件は、表 4-1 に示すものとします。

[4] 事業部門とは、全体または一部が被監査部署となる部門

表 4-1 監査チーム編成と内部監査人の独立性の条件

監査チーム編成	例	独立性の条件
事業部門に所属しない監査人で、監査業務が行われる	監査チームメンバー全員が監査部門に所属し、うち一人がクラウドサービスに知識のある技術系職務経験者である	外観上の独立性 精神上の独立性 職業倫理と誠実性
事業部門に所属する検査部署等の監査人が監査チームに加わり、監査業務に携わる	事業部門の検査部署に所属する内部監査人が、専門家として参加し、技術的な監査を行う	精神上の独立性 職業倫理と誠実性 外観上の独立性については、独立性を阻害するリスクを把握し、その管理策を実装・運用する

4.1. 事業部門に所属しない監査人の独立性の条件

事業部門に所属しない監査人が情報セキュリティ内部監査を行う場合には、被監査主体・監査人・監査報告書の利用者が独立して存在しているため、監査人は独立性を確保しやすいといえますが、被監査主体と監査人の関係においては経済的利害関係や不適切な外観等、独立性を阻害する要因も存在します。監査を行う場合、監査人は表 4-2 の阻害要因を取り除き、独立性の条件を満たさなければなりません。

表 4-2　事業部門に所属しない監査人の独立性を阻害する要因

避けるべき状態	阻害要因
1）経済的利害関係	① 監査部門または内部監査人は、被監査主体と協力した情報セキュリティに関する業務に携わっている ② 監査部門または内部監査人は、被監査主体の監査対象となる情報セキュリティの設計、構築、検査の業務に関わっている ③ 監査部門または内部監査人は、被監査主体から便益や贈与を受けている ④ 内部監査人は、被監査主体と自分自身との間に利害関係がある、または公正な判断に影響を及ぼすと合理的に推測される ⑤ その他、監査部門に情報セキュリティ監査活動の目的及び計画の達成を妨げるような制約がある
2）不適正な外観	⑥ 監査部門または内部監査人は、被監査主体の事業と密接に関係している ⑦ 必要な情報及び資料の入手が困難である ⑧ 監査部門または内部監査人は、助言勧告等がしにくい環境がある ⑨ 監査人が前事業年度に在籍していた組織（部門や子会社等）が被監査主体である

4.2. 事業部門に所属する監査人の独立性の条件

事業部門に所属する監査人は、独立性を阻害するリスクを把握し、その管理策を実装・運用して、表 4-3 の条件を満たすようにしなければなりません。

表 4-3　事業部門に所属する監査人の独立性の条件

①　内部監査人自らが担当した、または担当している業務の監査ではない
②　内部監査人が公平な監査を実施できる体制（外観）がある
③　内部監査人に、必要な情報を得ることができる権限がある

なお、監査チームのリーダは、リーダとして行う監査全体についての責任を有するため、監査対象の業務に従事している（あるいは従事した）場合には、監査人としての独立性を認めることができません。

5　内部監査人の独立性を確保するための方法

5.1. 事業部門に所属しない監査人の場合

事業部門に所属しない内部監査人の独立性を確保するために、明文化した情報セキュリティ内部監査ルールに、独立性を阻害する要因を排除する規定を記載し、そのルールに従った運用を行うことが必要です。

なお、表 4-2　⑨にある「監査人が前事業年度に在籍していた組織（部門や子会社等）が被監査主体である」場合など、職務上の経歴による阻害要因がある場合には、該当する監査人は、監査人が事業部門に所属すると想定しての運用を行うこととします。

5.2. 事業部門に所属する監査人の場合

5.2.1. 監査実施時の監査人の独立性確保の方法

前述の通り、事業部門に所属する監査人については、特段の独立性の確保が、公正な監査のために必要な条件となります。表 4-3「事業部門に所属する監査人の独立性の条件」に挙げた条件を満たすためには、明文化された情報セキュリティ内部監査ルールが必要となります。更に、この情報セキュリティ内部監査ルールが正しく実行されていることをもって、事業部門に所属する監査人が独立性を確保しているとすることができます。

表 5-1　事業部門に所属する監査人の独立性確保の方法

①　監査人の独立性を確保するための措置を明文化した監査ルールを設ける ②　監査ルール作成にあたっては、独立性を阻害するリスクを体系的に洗い出し、そのリスクに対する管理策を整理する ③　監査ルールに基づき、監査を実施する

この場合、新たに作成した監査ルールと既存の内部監査規定との整合性を確認してください。情報セキュリティ内部監査として特例を設ける場合には経営層の承認を得ておくことが必要です。

5.2.2. 監査ルールの作成方法（独立性を阻害するリスクの例）

前項（表 5-1）で述べた監査人の独立性を確保するための措置を明文化した監査ルールの作成において、「独立性を阻害するリスクを体系的に洗い出し、その管理策を整理する」と定義されています。ここではリスクと管理策の例を提示します。

表 5-2　事業部門に所属する監査人の独立性を阻害するリスクと管理策の例

No	リスク	管理策
①	内部監査人は、被監査主体の情報セキュリティに関する業務に携わっている	情報セキュリティ監査の期間中は被監査主体の情報セキュリティに関する業務に携わらない
②	内部監査人は、監査対象となる情報セキュリティの企画、設計、構築、検査、運用の業務に関わっている	自らの行った業務は別の監査人が監査を行い、各々の監査人が担当した部分について記録を残す
③	情報セキュリティ内部監査人は、被監査主体と同一または配下の部署に所属しており、組織上独立していない	情報セキュリティ内部監査の業務は、所属長（例えば、グループ長）より上位の部門の長（例えば、情報システム部長）が所管し、情報セキュリティ監査人から情報セキュリティ内部監査を所管する長に直接レポートされる
④	内部監査人は、自分自身に被監査主体との利害関係があり、または公正な判断に影響を及ぼすと合理的に推測される	内部監査人は情報セキュリティ内部監査を所管する長により保護され、監査報告の内容により、人事評価等を左右されることがない（事業部門に不利な報告内容であっても、評価にそれを反映してはならない）
⑤	その他、内部監査人に情報セキュリティ監査活動の目的及び計画の達成を妨げるような制約がある	内部監査人は情報セキュリティ内部監査を所管する長により保護される
⑥	内部監査人は、必要な情報及び資料の入手が困難である	内部監査人への協力義務が明文化され、情報セキュリティ内部監査を所管する長より情報セキュリティ内部監査の通知が被監査主体に行われる
⑦	内部監査人が助言勧告等をしにくい環境がある	情報セキュリティ内部監査の公正さを確保することが、明文化された情報セキュリティ内部監査ルールに記載されており、関係者に周知されている

これら表 5-2 で挙げたリスクの整理は、一般的に考えられる項目とその管理策を例示したものであり、クラウドサービス事業の運営体制や組織規模や構造によってはその他の独立性を阻害するリスク要因が生じる場合もあります。このため各事業者の実情に応じてリスクの整理と管理策の整備を行ってください。

以下では、表 5-2 について解説します。

① 監査人が情報セキュリティに関する業務に携わっている問題への管理策

情報セキュリティ担当者は、顧客や現場からの情報セキュリティに関わる問い合わせへの対応、対外的な自社システムの安全性の説明、社内のセキュリティに関する専門的な助言、あるいは、情報セキュリティの企画、設計、構築、検査、運用に関わる実務などの業務を行っていることが少なくありません。

このような立場の人が情報セキュリティ内部監査を行う場合には、監査業務の実施期間はこれらの業務には携わらないルールを定めて、社内各部門の了解を取っておくことなどの、対策が必要です。

② 監査人が情報セキュリティの企画、設計、構築、検査、運用の業務に関わっている問題への管理策

内部監査人自身がクラウドサービス事業に係わるシステムの企画、設計、構築、検査、運用の業務に携わった場合、その業務範囲の監査を行わないことが必要です。

内部監査人がこれらの業務を行っている場合には、他部署の人が監査人の資格を取得し、技術者でかつ内部監査人でもある人の業務に対する監査を実施することが必要です。

仮に、社内に有資格者が不足している場合には、有資格者を保有する外部の組織に、当該部分を対象とする監査を委託することも考慮する必要があります。

③ 監査人が被監査主体と監査組織の 2 つの指揮系統下にある問題への管理策

内部監査人が被監査主体と同一事業部門または配下の部署に所属する場合には、事業運営の指揮命令系統と、情報セキュリティ内部監査業務の指揮命令系統を分離し、情報セキュリティ監査業務が事業運営の影響を受けない仕組みを構築する必要があります。例えば、グループ長の指揮命令を受けている技術者が内部監査人として監査業務を行う場合には、情報システム部長の直接的な指揮命令を受けるというようなことが挙げられます。

④ 監査人と被監査主体の利害が関係する問題への管理策

売上評価や納期など被監査主体の成果が内部監査人個人の評価などに関連付けされることにより、監査業務が適正に実施されない可能性があります。これを回避するため、情報セキュリティ内部監査業務は、被監査主体の業績の評価と監査業務の成果評価を切り分けることを予め情報セキュリティ内部監査ルールに記載し、その記載に従った運用を行う必要があります。

⑤ 監査活動の目的及び計画の達成を妨げるような制約への管理策

組織として①から④の管理策が行われていても、上司や同僚などの理解が得られず内部監査人が孤立してしまうリスクがあります。情報セキュリティ内部監査を所管する長は、こうしたことが生じないように内部監査人を取り巻く環境などを監視し、内部監査人を保護する必要があります。

⑥ 監査人が必要とする情報及び資料の入手が困難な場合の管理策

適正な監査を実施するために、経営層または監査人が所属する事業部門の責任者は内部監査人への協力義務を明文化し、監査業務の期間において、被監査主体から適正な監査に必要な情報及び資料の入手が行われるような体制を敷く必要があります。

⑦ 監査人が助言勧告等をしにくい環境への管理策

被監査主体の発言力が高い場合や社内における情報セキュリティ監査への理解の不足などのために、情報セキュリティ監査における助言やそれに基づく勧告が行いにくい雰囲気があると、監査の公正さが損なわれる可能性があります。経営層または監査人が所属する事業部門の責任者は、情報セキュリティ内部監査の意義を文書化し、監査結果の公正さを確保するために情報セキュリティ内部監査ルール等の文書で社内にそれを周知することが必要です。

6. 独立性を確認するための外部監査人の評価

日本セキュリティ監査協会およびJASA-クラウドセキュリティ推進協議会はCSマークの発行に際し、内部監査の体制や評価内容に対して独立性を外部監査人による評価を行う場合があります。また監査結果に関して疑義が生じた場合にも同様です。

このような場合、外部監査人は以下の項目について評価を実施することができるものとします。

表 6-1　外部監査人による内部監査人の独立性の評価

①　内部監査ルールの内容規定で独立性の確保について記述されていることの確認
②　リスクが体系的に洗い出され、管理策が整理されていることの確認
③　経営者、内部監査の責任者及び内部監査人に対するインタビューで、 ルールに基づいた監査が行われていることの確認など

外部監査人の確認により、二者間の監査の実施において、これらの項目が満たされておらず、独立性を損なっていると認められた場合、協会の審査委員会の裁定を経て、監査人、監査人資格の剥奪または監査人に対する戒告等の処罰や、CSマークの認定取り消し等の社会的制裁を受ける場合もあります。これらの条件を予め理解し、内部監査を実施する前に必ず内部監査ルールの明文化を行うようにしてください。

7　おわりに

特定非営利活動法人 日本セキュリティ監査協会（以下、「協会」という）では、協会が認定している公認情報セキュリティ監査人の独立性を確保するために、監査人倫理規程

（2004 年 11 月 4 日制定） を策定し、その第 3 条において、公認情報セキュリティ監査人の独立性について規定しています。公認情報セキュリティ監査人は協会の監査倫理規定に準拠して業務を行うという意味から、一般の監査人よりもその業務の信頼性が高いと評価することができます。クラウドセキュリティ監査の内部監査においても、公認情報セキュリティ監査人は、本ガイドラインに沿って、より的確な独立性を確保・運用することが望まれます。

改訂履歴

日付	版名	改訂事由
2016 年 7 月 14 日	第 2 版	監査人の所属属性の明確化
2015 年 11 月 15 日	第 1 版	初版公開