

# クラウド情報セキュリティ監査における内部監査人の独立性について

説明資料

JASAークラウドセキュリティ推進協議会



# クラウド情報セキュリティ監査における内部監査人の独立性のあり方(方針)

- クラウド情報セキュリティ監査における内部監査は、情報セキュリティに関する声明の根拠となる重要な監査であるため、協議会会員は、内部監査人の精神的独立性、外観的独立性を確保する措置を講ずることとする



## (参考)クラウドの内部監査人の独立性について

原則として、三者間の監査のスキームが望ましい。

ただし、クラウドと情報セキュリティ監査の両方の知識を持つ人材が限られており、三者間の監査ができる場合には、独立性が損なわれるリスクに対する管理策を行うことを条件に、二者間の監査を行うことができる。

◆三者間の監査の場合は、独立性ガイドライン通りの運用とする

◆二者間の監査である場合には、下記の条件を踏まえることとする

- 職務分掌上、内部監査人は自分が担当している業務は監査しない
- 内部監査人が公平な監査ができる組織体制（外観）をもつ
- 内部監査人が必要な情報を得ることができる権限を持つ

### 独立性を確保するための方法

クラウド情報セキュリティ監査に関する内部監査ルールの明文化

- ① 内部監査の独立性を確保するための措置を明文化した内部監査ルールを設ける
- ② 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、その管理策を整理する
- ③ 内部監査ルールに基づき、監査を実施する

### 独立性を確認するための外部監査人の評価

- 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子の確認
- 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



# 三者間の監査における独立性の阻害要因

阻害要因	三者間の監査
1 ) 禁止すべき利害関係（経済的利害関係）	<ul style="list-style-type: none"> <li>① 内部監査部門または内部監査人は、被監査主体と協力したビジネス活動に関与している</li> <li>② 内部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</li> <li>③ 内部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</li> <li>④ 内部監査人は、自分自身に利害関係があり、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</li> <li>⑤ その他、内部監査部門に内部監査活動の目的および計画の達成を妨げるような制約がある</li> </ul>
2 ) 避けるべき外観（不適正な外観）	<ul style="list-style-type: none"> <li>⑥ 内部監査部門または内部監査人は、被監査主体の配下の部署に所属しており、組織上独立していない</li> <li>⑦ 必要な情報及び資料の入手が困難である</li> <li>⑧ 内部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</li> <li>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</li> </ul>



# 二者間の監査における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、評価及び助言勧告等がしにくい環境がある	経営者が、内部監査の結果について公正さを確保することを明言し、公正さの確保と内部監査人の保護が公式の文書に記載されている
②	内部監査部門または内部監査人は、被監査主体の配下の部署に所属しており、組織上独立していない	事業部門の指揮命令系統と内部監査業務の指揮命令系統は異なり、内部監査業務が事業部門の影響を受けない仕組みがある
③	内部監査人の個人評価と事業部門の業績が関係する	内部監査人は内部監査業務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
④	内部監査人は、被監査主体のビジネス活動に関与している	監査の期間中はビジネス活動を行わない
⑤	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	自分の行った業務は別の部署の人が監査を行う
⑥	内部監査活動の目的および計画の達成を妨げるような制約があり、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、内部監査所管の長より内部監査の通知が被監査部門に行われる



## 内部監査の区分と要件（JASA 独立性ガイドラインより加筆）

	内部監査	具体的な要件
三者間の監査	内部監査の結果を被監査主体以外のラインに報告する監査	外観上の独立性 精神上の独立性 職業倫理と誠実性
二者間の監査（被監査主体と報告書の利用者が同一となる監査）	内部監査の結果を被監査主体に報告する監査	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

