情報セキュリティ監査　用語集

Ver2.0

2015 年 1 月 22 日
日本セキュリティ監査協会

（本ページは、意図的に白紙としている）

はじめに

2003 年に情報セキュリティ監査制度が開始されて以降、多くの情報セキュリティ監査に関わる調査・研究がなされ、知識として蓄積をされてきた。これらの調査・研究は、その時々の情報セキュリティ監査を取り巻く環境を反映しており、用語に関しても、その時々に用いられているもので記述されている。

情報セキュリティ監査制度が 10 周年を迎えようという時点でこれらを通して見た結果、統一的な観点から、用語定義を見直す必要が生じた。

このため、技術部会に監査品質タスクフォースを設け検討を行ってきた。本用語集は、監査品質タスクフォースのメンバーによる 3 年間の議論を経て、用語集として取りまとめたものである。

メンバーは、多忙な日常業務の合間を縫って作業を行い、時には休日や深夜遅くまで議論をしながら、一語一語の定義や解釈を吟味してきた。本用語集は、これらメンバーの献身的な労苦により完成したものである。

ここに、下記に示すメンバーへの謝意を表するものである。

2014 年 4 月 17 日
日本セキュリティ監査協会　会長
土居範久

監査品質タスクフォース

リーダ	室谷　憲三	ビュルガーコンサルティング株式会社
	池田　秀司	i-3c 株式会社
	岩切　伸行	有限会社ケイ・アイ・エス
	小川　敏治	one 株式会社
	神吉　英行	スカパーJSAT 株式会社
	日浅　愼逸	
	平田　真悟	株式会社富士通マーケティング
	平野　秀幸	富士通株式会社

技術部会長　和貝 享介　（有限責任監査法人トーマツ）
事務局　　永宮 直史

2015 年の改訂について

2014 年 3 月に JIS Q 27000:2014、JIS Q 27001:2014、JIS Q 27002:2014 が大幅に改訂されて、発行された。特に、JIS Q 27000:2014 は情報セキュリティに関わる用語集として発行されたものであり、それにより、わが国の情報セキュリティに関わる業務における標準的な用語が明確になった。このことを踏まえて、今回、情報セキュリティ監査用語集を見直すこととした。

見直しにあたっては、当協会内の意見公募を行い、より監査の現場に即した内容にするように努めた。

2015 年 1 月 22 日

特定非営利活動法人　日本セキュリティ監査協会

【あ】

1 次利用者

【定義】 被監査主体の情報セキュリティ対策に直接の利害関係を持ち、その適否や有効性に特定の期待や要求水準を示している監査報告書の利用者。

【解説】 1次利用者は、被監査主体の監査テーマに直接の利害関係があり、何らかの形で監査費用を負担する立場にある（何らかの形とは、最終的に対価に反映されることを含む）。

【関連用語】 2 次利用者、社会的合意方式

インタビュー

【定義】 「質問」の項目参照。

【解説】 -

【関連用語】 -

ALE(えいえるいい)

【定義】 NIST（米国標準技術院）が推奨する定量的リスクアセスメント手法で用いられる年間の予想損失額。

【解説】 ALE は、Annualized Loss Exposure の頭文字。ある事象 1 回あたりの損失額にその事象の年間発生頻度を乗じて求める。
ALE で表現するリスクアセスメントの手法は ALE 手法（単に ALE と略すこともある）。

【関連用語】 -

閲覧

【定義】 マネジメント体制又はコントロールについての整備状況又は運用状況を評価するために、規程、手順書、記録（電磁的な記録も含む）等を調べ読むことによって問題点を明らかにする監査技法。

【解説】 「レビュー」ともいう。
閲覧の例；
・職務分掌規程や職務権限規程の閲覧・情報セキュリティポリシーや情報セキュリティ関連規程の閲覧・運用手順書の閲覧
・各種申請書類(ID の付与、アクセス権の付与など)や議事録、管理簿等の閲覧
・システム上の設定値の閲覧、システムログの閲覧

【関連用語】 監査技法、質問、観察、再実施

運用状況評価

【定義】 内部統制が実際に運用され有効に機能しているかを確かめること

【解説】 「整備状況評価」により有効にデザインされ実装されていると評価された内部統制が、実際に運用されて、デザイン通りの有効性を発揮しているかを確認する。

【関連用語】 整備状況評価

【か】

改善提言

【定義】 監査人が、指摘する検出事項の改善策を客観的かつ公正な立場で実践的規範として表明した事項。

【解説】 -

【関連用語】 助言型監査

外部監査

【定義】 監査対象組織の外部の利用者に対して監査結果を報告する目的で行われる監査。

【解説】 -

【関連用語】 内部監査

可用性（availability）

【定義】 認可されたエンティティが要求したときに、アクセス及び使用が可能である特性。（JISQ27000:2014）

【解説】 組織が認可した利用者が、必要とする時に情報資産にアクセスできるように、システムやデータを保護する

【関連用語】 機密性、完全性

監査(Audit)

【定義】 組織体の行為、行為の結果、組織の状態あるいはそれらを示す情報等について、独立の立場にある第三者が、一定の基準に基づき検証・評価することで、その真実性や妥当性などを確認し、その結果を関係者に報告すること。

【解説】 監査基準が満たされている程度を判定するために、監査証拠を収集し、それを客観的に評価するための体系的で、独立し、文書化されたプロセス。

(JISQ19011:2012)

【関連用語】 -

監査意見（Audit opinion）

【定義】 監査人が、監査報告書において、一般に公正妥当と認められる基準に準拠して監査を実施した結果の表明。

【解説】 監査意見は、情報セキュリティ監査人が情報セキュリティ監査基準に従って監査手続を行った範囲内での請け合いであって、かつ当該監査手続が慎重な注意のもとで実施されたことを前提に、述べられるものである。

【関連用語】 -

監査依頼者

【定義】 監査を監査主体に依頼する機関、組織又は人。

【解説】 監査対象に責任を持つ者が監査依頼者となる場合が多いが、監査対象の利害関係者が監査依頼者となる場合もある。
又、監査報告書の名宛人になることから、経営陣又は利用者。

【関連用語】 -

監査技法

【定義】 監査人が監査証拠を入手するための手段。

【解説】 情報セキュリティ監査制度では、閲覧・質問・観察・再実施の 4 つの技法がある。

【関連用語】 監査手続

監査基本計画書

【定義】 文書化された監査の基本的な方針とその方針に基づいた監査の企画。

【解説】 監査基本計画書に含まれる項目は、監査対象とする範囲、期間又は期日、段階（例えば、運用段階）、監査目標、監査業務の管理体制、他の専門職の利用の必要性と範囲等がある。

【関連用語】 監査実施計画

監査業務

【定義】 監査基本方針の策定、監査実施計画の立案、監査手続の実施、監査意見の形成、監査報告書の提出までの監査の全実行ステップの総称。

【解説】 監査人は、監査の目的が有効かつ効率的に達成されるように、適切な監査体制を整え、監査計画の立案から監査報告書の提出までの監査業務の全体を管理しなければならない。

なお、助言型監査においては、改善提言を監査業務に含むことがある。

【関連用語】 -

監査計画（Audit plan）

【定義】 監査リスクを合理的に低い水準に抑えるために、監査の基本的な方針を策定し、その方針に基づいた監査の企画。

【解説】 監査計画には、監査基本計画と監査実施計画がある。

【関連用語】 -

監査項目

【定義】 「監査範囲」の中から抽出された「監査手続」が適用される個々の対象。（システム監査学会、2005「システム監査用語の定義と解説」）

【解説】 -

【関連用語】 -

監査実施計画書

【定義】 監査基本計画書に基づいて、実施すべき監査の内容、手順、手続などについての事前に体系的に取りまとめた文書。

【解説】 監査実施計画書に含まれる項目は、監査手続の実施、場所、担当者、実施すべき監査手続の概要、時期、進捗管理手段又は体制等がある。

【関連用語】 監査基本計画

監査実施者

【定義】 監査チーム内において、実際に監査手続を実施する役割を担う者。他の専門職を含む場合もある。

【解説】 監査責任者が監査を実施するために必要な能力を備えた監査人と判断した監査人又は技術専門家等の他の専門職。

【関連用語】 監査人

監査責任者

監査主体

【定義】 監査の実施を請け負うことのできる組織体又は個人。

【解説】 監査に従事する個人の質の確保及び監査を行う主体としての質の確保がなされている組織体（企業）又は個人。

【関連用語】 被監査主体

監査証拠 (Audit evidence)

【定義】 監査人が監査手続を通じて入手した記録（監査証跡を含む）、文書、証言、その他の事実の内、監査人が監査意見を形成するために使用したすべてもの。

【解説】 証拠の採用にあたっては、監査の目的又は監査人が適用する基準（判断の尺度）に関連付けられたものでなければならない。また、監査証拠は監査意見の形成に必要かつ十分な量と、質（証明力）を備えていなければならない。

【関連用語】 監査証跡

監査証跡 (Audit trail)

【定義】 情報セキュリティ管理のプロセスや情報システムの処理の内容等を、監査人が追跡するために時系列に保存された記録。

【解説】 -

【関連用語】 監査証拠

監査所見

【定義】 収集した監査証拠を監査基準に対して評価した結果。
(JISQ19011:2012)

【解説】 -

【関連用語】 -

監査責任者

【定義】 監査チーム内において、監査業務に最終責任を負う者。監査業務全体を指揮し、管理する役割を担う。

【解説】 監査主体は監査業務を行う場合、初めに監査責任者を決定し、監査責任者が中心となって引受け可否、監査チーム編成、監査計画、監査手続きなどの検討を行う。

【関連用語】 監査人、監査実施者、品質管理者

監査組織

【定義】 監査を行うことを業とする事業主、監査法人、会社・団体等。

【解説】 -

【関連用語】 監査対象組織

監査対象組織

【定義】 監査人が監査の対象とする組織。

【解説】

【関連用語】 監査組織

監査対象

【定義】 「監査目的」達成のために、「監査手続」の適用範囲となり得る対象。（システム監査学会、2005「システム監査用語の定義と解説」）

【解説】 監査対象は、組織、サービス、施設・設備・機器、情報通信システム、媒体など、情報資産ならびにそれを取り扱う環境および人のうち、監査目的に関係するものである。
監査対象の範囲で、監査テーマと監査リスクにより監査範囲が決定される。

【関連用語】 監査範囲

監査チーム

【定義】 監査を実施するチームで、監査責任者と監査実施者からなる。

【解説】 監査責任者が、監査を実施するために必要な能力を備えた監査実施者を、監査に必要な工数に応じて配員した組織体。
監査責任者が必要と判断した場合、技術専門家等の他の専門職の配員を検討する。

【関連用語】 -

監査チェックリスト

【定義】 個別管理基準等を元に監査手続の一覧性を確保し、実施状況を確認するための作業文書。

【解説】 有効かつ効率的な情報セキュリティ監査を実施するために用いる。
監査人が複数にわたる場合には、監査人ごとにチェックリストを作成すると、各々の監査人の作業進捗状況が確認できる。
監査人が 1 名の場合には、監査チェックリストと監査手続書を併用することもある。

【関連用語】 監査手続書

監査調書 (Working papers)

【定義】 監査人が、情報セキュリティ監査にあたり、十分かつ適切な監査証拠に基づいて、客観的な立場から監査意見を形成したことを立証するために体系化された資料。

【解説】 監査調書は、監査手続から監査意見形成の一連の過程をトレースできるように、記載されていることが必要である。

【関連用語】 -

観察 (Observation)

【定義】 マネジメント体制又はコントロールについての整備状況又は運用状況を評価するために、監査人自らが現場に赴き、目視によって確かめる監査技法。
「サイトレビュー」あるいは「視察」ともいう。

【解説】 観察の例;
運用担当者が運用手順書に従った操作を実際に行っていることを監査人自ら直接に見て、その妥当性や適否を判断すること。
クリアデスクやクリアースクリーンの状況を目視で確認すること。
入退室の際のカードによる制御で、共連れがない状況を確認することなど。

【関連用語】 監査技法、質問、閲覧、再実施

監査テーマ

【定義】 監査目的実現のために、どこに焦点をおき、監査するかを表した、具体的な監査の主題。

【解説】 監査テーマとは、監査目的に基づき定められた、その監査で具体的に評価しようとすることがらである。
監査テーマは、監査実施に先立ち、監査実施依頼者の意向、及び監査人が行う事前調査などに基づいて、監査人がその内容を検討し、監査依頼者の了承を得て決定される。

【関連用語】 -

監査手続（Audit procedure）

【定義】 監査人が監査証拠を入手するために必要と判断した監査技法を組み合わせて実施するプロセス。

【解説】 -

【関連用語】 監査技法

監査手続書（Audit program）

【定義】 監査対象範囲に関する個別管理基準の各項目に対応し、必要な監査手続を記載した文書。

【解説】 監査実施計画の一部をなすもので、基準の項目別に、何を対象として、どのような方法で、そのような証拠を収集するかを記載したもの。

【関連用語】 監査チェックリスト

監査人（Auditor）

【定義】 監査主体として、監査を実際に行う監査の専門家。

【解説】 監査チームが編成される場合は、監査責任者及び監査実施者に分けられる。但し、監査業務の品質管理者は含まない。

【関連用語】 監査責任者
監査実施者

監査の品質管理

【定義】 監査業務の信頼性、有効性及び効率性の向上を目的とした管理活動。

【解説】 監査の品質管理は、監査責任者による品質管理と、監査チームから独立した品質管理者による品質管理がある。
監査責任者は、監査の各プロセスで適切な品質が確保できるように努める。
品質管理者は、監査チームが実施した監査が、情報セキュリティ監査基準に準拠して適切に行われているかどうかを、客観的な立場から確かめる。

【関連用語】 品質管理統括責任者、品質管理者

監査範囲

【定義】 「監査対象」のうち、「監査手続」を適用する範囲。（システム監査学会、2005「システム監査用語の定義と解説」）

【解説】 実際に監査手続に従って監査を受ける範囲であり、場所、組織単位、活動、プロセス、システム等を指す。
監査人は、監査対象の諸制限（費用や時間、通常業務への影響等）を考慮し、監査範囲を設定する。

【関連用語】 -

監査品質審査制度

【定義】 日本セキュリティ監査協会会員の申請、もしくは協会の独自の判断により選択された監査が、情報セキュリティ監査制度の基準に適合した品質を有するか否かを審査する制度。

【解説】 -

【関連用語】 -

監査報告書（Audit report）

【定義】 監査人が監査の結論を表明するために作成した文書。

【解説】 監査報告書は、監査人が監査報告書の想定利用者に対して監査の結果を伝達するものであり、かつ、監査人が自らの役割と責任を明確にする手段でもある。

監査報告書には、監査の目的に応じて監査人が必要と認めた事項を明確に記載しなければならない。利害関係者からの開示請求又は監査報告書受領者の判断によって監査報告書が外部に公表されるような場合には、監査の結果が誤解なく伝わるものでなければならず、監査報告書に記載した事項については監査人が全面的に責任を負うこととなることに留意する。

【関連用語】 -

監査報告（Reporting of the audit）

【定義】 監査人が行った監査の結果をとりまとめ、監査依頼者に伝達すること。

【解説】 -

【関連用語】 -

監査目的

【定義】 監査を実施することによって被監査主体または監査依頼者が達成しようとする事項または状態。

【解説】 -

【関連用語】 -

監査リスク（Audit risk）

【定義】 監査プロセスにおいて、監査人が誤った監査意見を表明してしまうリスク。

【解説】 監査リスクは、監査人が十分な監査証拠を収集できない、あるいは監査人が重要な問題を見逃すことにより生じる。

【関連用語】 リスクアプローチ、監査リスクモデル

監査リスクモデル

【定義】 監査リスクを合理的に低いレベルに抑えるために、固有リスク、統制リスク、発見リスクの 3 つの要素で管理するモデル。

【解説】 固有リスク、統制リスクは監査人がコントロールできないため、監査リスクを下げるには発見リスクを下げることが必要となる。

【関連用語】 監査リスク、リスクアプローチ、監査リスクモデル、固有リスク、統制リスク、発見リスク

完全性（Integrity）

【定義】 正確さ及び完全さの特性。（JISQ27000:2014）

【解説】 情報が破壊、改ざん又は消去されていない状態を確保すると共に情報及び資産の正確な処理方法を保護する。

【関連用語】 機密性、可用性

管理策 （Control）

【定義】 リスクを修正（modifying）する対策（JISQ27000:2014）

【解説】 リスクを管理する手段（方針、手順、指針、実践又は組織構造を含む。）であり、実務管理的、技術的、経営的又は法的な性質をもつことがあるもの。コントロール（Control）の訳語。

【関連用語】 コントロール

管理手続

【定義】 管理策基準に基づいて被監査主体が実装し、運用している管理策。

【解説】 管理手続は、保証型監査の対象として言明書に記載する。

【関連用語】 -

期間監査

【定義】 過去の一定期間の状況を対象とする監査

【解説】 期間監査は、運用状況の適切さを十分に確認するために有効な監査である。

調査期間の選択によっては、十分かつ適切な監査証拠を入手できない場合があるため、期間の選択が重要である。

【関連用語】 時点監査

聞き取り

【定義】「質問」の項目参照。

【解説】 -

【関連用語】 -

基準（Standard）

【定義】 監査における評価の尺度、行為の規範、または道しるべ。

【解説】 情報セキュリティ管理基準は、監査人の評価の尺度であり、被監査主体にとって行動規範となる。また、情報セキュリティ監査基準は、監査人の行動規範となる。

【関連用語】 情報セキュリティ管理基準
情報セキュリティ監査基準

技術的検証

【定義】 閲覧や再実施などの監査技法において、十分な監査証拠を得るための、IT 技術や知識を利用した検証。

【解説】 -

【関連用語】 ペネトレーションテスト、ぜい弱性検査

機密性（Confidentiality）

【定義】 認可されていない個人、エンティティ又はプロセスに対して、情報を使用させず、また、開示しない特性。（JISQ27000:2014）

【解説】 -

【関連用語】 可用性、完全性

脅威（Threat）

【定義】 システム又は組織に損害を与える可能性がある、望ましくないインシデントの潜在的な原因。（JISQ27000:2014）

【解説】 -

【関連用語】 -

業務監査

【定義】 組織体の会計以外の業務の監査をいい、組織体の人事、購買、製造、販売等の会計業務以外の業務活動全般にわたって、その遂行状況を監査することをいう。（システム監査学会、2005「システム監査用語の定義と解説」）

【解説】 IT を用いた業務に対する業務監査の手法として、システム監査が用いられる。

【関連用語】 -

検出事項

【定義】 監査人が、基準に照らして不十分と評価し、表明した事項。

【解説】 -

【関連用語】 -

限定付肯定意見

【定義】 監査人による「被監査主体が行った言明と実際の情報セキュリティ対策のうち、かい離がある一部を除き、言明が信頼できる」旨の意見を述べること。

【解説】 -

【関連用語】 -

言明 (Assertion)

【定義】 被監査主体の経営者による「被監査主体における情報セキュリティのマネジメントとコントロール」に関する主張。

【解説】 保証の本質的な意味を実現するためには、監査主体が責任を持って行うべきこと、つまり保証のための条件を明らかにする必要がある。
保証のための条件として、被監査主体が保証型情報セキュリティ監査を受けて保証を得るために実施すべき項目や手順、経営者の関わり方を表明することが言明である。この言明により被監査主体の責任が明確になる。
被監査主体の責任が明確になることで、監査主体が責任を持つべきことも再確認できる。これを踏まえて監査主体はその責任範囲を考慮して、監査プロセスを検証することができる。

【関連用語】 言明書、言明方式

言明書 (Statement of assertions)

【定義】 「情報セキュリティに関わるリスクマネジメントが効果的に実施されるよう、リスクアセスメントに基づいて適切なコントロールを整備し運用している」旨の経営陣(経営者又は情報システム管理責任者等)による確認書のことをいう。

【解説】 -

【関連用語】 言明、言明方式

言明方式

【定義】 監査対象組織の言明を保証の対象とする監査の方式。

【解説】 -

【関連用語】 実態方式、言明、言明書

合意 (Agree)

【定義】 情報セキュリティ監査の業務を行う際に、監査依頼者(報告書利用者を含む)と監査受嘱者が「監査主題とその評価方法に係る事項に関する意思が合致していること」を相互に了解すること。

【解説】 一般に合意とは、当事者双方の意思が一致していることを了解することを指す。合意があれば、互いに遂行する義務が発生する。
監査においては、利用者、被監査主体、監査主体、監査人の間で、情報セキュリティ基準の内容とそのコントロール、監査の種類、監査手続、監査報告書の用途などについて、意思が合致し了解していることを示す。

【関連用語】 -

合意された手続 (Agreed Upon Procedure:AUP)

【定義】 対象を評価又は測定するために、依頼者(手続実施結果の利用者を含む)と監査人との間であらかじめ実施する手続が合意されていることを前提として、実施した手続の結果について独立の第三者として結論を表明すること。

【解説】 -

【関連用語】 -

肯定意見

【定義】 監査人による、「被監査主体が行った言明と実際の情報セキュリティ対策に、かい離がみられず、言明が信頼できる」旨の表明。

【解説】 -

【関連用語】 -

COBIT(こびっと)

【定義】 組織の IT ガバナンスのための明確な方針とより良い実務を提供するための枠組みと詳細なコントロール目標のガイドを示す一連の考え方と、その実現を支援する資料ならびにツール。

【解説】 Control Objectives for Information and related Technology (COBIT)とは、米国 EDP 監査人財団（EDPAF）が定めたコントロール目標（control objectives）に起源を持ち、世界中の組織が基準として利用している情報技術(IT)管理についてのフレームワークである。
COBIT はマネージャ、監査人、IT ユーザーに一般に通じる尺度や判断基準、ビジネスプロセスやコントロール目標を示していてることから、情報技術を用いた組織内の IT ガバナンスや内部統制の開発の補助となる。

【関連用語】 -

合理的保証 (Reasonable assurance)

【定義】 保証型監査の監査人が情報セキュリティ監査基準に従って正当な注意を払い監査を実施した結果、監査の限界のもとで、言明と監査人が把握した事実との間に相違がないことについて、相当程度の心証を得たとの専門家としての判断を結論として述べること。

【解説】 -

【関連用語】 -

個別管理基準

【定義】 組織が効果的な情報セキュリティマネジメント体制を構築し、適切なコントロールを整備し、運用するための基準。また、監査主体が情報セキュリティ監査を行なう上での実際の監査項目。

【解説】 情報セキュリティ管理基準を参照し、当該組織にとって必要とされる項目を抽出後、項目中の文言を当該組織にとって適切な表現に修正する。
又、必要に応じて、項目の分割又は、統合を図る。
一度の策定に留まらず、組織の態様の変化及び外部要因によって、
徐々に評価・改善をしていくべきものである。

【関連用語】 -

固有リスク（Inherent risk）

【定義】 状況から生じるか、環境に存在するリスク。
（コントロールをとること、または状況を修正することが行われないことを前提として）

【解説】 組織内外の経営環境に起因して影響される様々なリスクであり、企業全般に影響を及ぼす。採用しているIT技術や情報システムに起因するリスク、業界の特殊な取引慣行の他、景気の動向、経営理念等、固有リスクの要因は多様である。
会計用語では、「関連する内部統制がないと仮定した上で、重大な虚偽の表示がなされる可能性」と定義されている。

【関連用語】 -

コンサルティング(Consulting)

【定義】 報酬を得て依頼者からの専門的な事柄の相談に応じ、指南、助言、支援すること。

【解説】 業務または業種に関する専門知識を持って、客観的に現状を観察して現象を認識、問題点を指摘し、原因を分析し、対策案を示して依頼者を支援する業務。
助言型監査は情報セキュリティ管理基準に準拠した個別管理基準に基づき、現象認識、問題点指摘、原因分析、対策案の提示をするが、コンサルティングは必ずしも基準を用いない。
また、助言型監査は独立性が問われるが、コンサルティングは独立性等の要件が必須ではない。

【関連用語】 -

コントロール（Control）

【定義】 情報セキュリティ確保に関わる特定の目的を達成するために、当該目的達成の責任者が何らかの影響力を行使すること。

【解説】 情報セキュリティを確保するための具体的な対策、マネジメントサイクルに組み込まれた個々の情報セキュリティ対策を指す。

【関連用語】 管理策

【さ】

再実施（Reperformance）

【定義】 コントロールの運用状況を評価するために、監査人自らが組織体のコントロールを運用し、コントロールの妥当性や適否を確かめる監査技法。

【解説】 「テスト」ともいう。

再実施の例；

・カードによる入室管理が行われている場合、アクセス権が付与されていないカードを利用し、監査人自らがエラーとなることを確認

・監査人が行うアクティブなペネトレーションテスト

・パスワードポリシーの順守状況を把握するために、監査人が疑似パスワードによるシステムへのアクセス試行

など。

【関連用語】 監査技法、閲覧、質問、観察

三者間の監査

【定義】 被監査主体、監査主体および利用者が、各々独立した関係にある場合の監査。

【解説】 会計監査における三者監査と同義である。

ISO19011 に記載される第三者監査も三者間の監査である。

【関連用語】 二者間の監査

サイトレビュー

【定義】 「観察」の項目参照。

【解説】 -

【関連用語】 -

サンプリング

【定義】 試査。

【解説】 -

【関連用語】 -

残留リスク

【定義】 リスク対応の後に残っているリスク。(JISQ27000：2014)

【解説】 -

【関連用語】 -

視察

【定義】「観察」の項目参照。

【解説】 -

【関連用語】 -

試査 (Audit sampling)

【定義】 監査対象(母集団)の中からサンプルを抽出し、当該サンプルに対して監査手続を実施し、その結果から母集団の特性又は傾向を推定する方法。

【解説】「サンプリング」ともいう。
監査対象となる項目のすべてを検証することができないか、又は効率的でない場合に利用される。サンプルの抽出と母集団の推定に統計的な手法を用いる統計的サンプリングと、サンプルの抽出を監査人の経験に基づく経験的(非統計的)サンプリングがある。また、試査を効果的に実施するためには、母集団の階層化や母集団の分割が有効な場合もある。

【関連用語】 精査

資産価値

【定義】 資産の有用性の程度

【解説】 資産の価値の表示には、定量的表現と定性的表現がある。
資産を総合的にとらえる場合と、機密性・完全性・可用性などの側面からとらえる場合がある。

【関連用語】 -

事実に関する見解の相違

【定義】 監査に基づいた事実の認定に関して、監査人と被監査主体で見方が相違していること、あるいは、ある事実が存在するかしないかについて、監査人と被監査主体で考えが異なること。

【解説】 事実に関する見解の相違が生じた場合には、監査人は別途証拠を集めて、見解の相違をなくするように努めることが望ましい。
見解の相違が解消できない場合、監査人は監査報告書に監査人の意見と監査対象組織の責任者の意見の両論を併記しなければならない。

【関連用語】 -

システム監査（Systems audit）

【定義】 組織体の情報システムにまつわるリスクに対するコントロールがリスクアセスメントに基づいて適切に整備・運用されているかを、独立かつ専門的な立場のシステム監査人が検証又は評価することによって、保証を与えあるいは助言を行い、もって IT ガバナンスに寄与すること。（経済産業省、2004「システム監査基準」）

【解説】 -

【関連用語】 -

実査

【定義】 監査対象の情報セキュリティに関わるマネジメントやコントロールの実施状況を、監査対象がマネジメントやコントロールを実施している場所において、その実施状況に関わる証拠を収集する手続。

【解説】 情報システムにおいては、ドキュメント、プログラム、データ、要員などの実際の存在、数量、使用状況等を確認する手続である。（システム監査学会、2005「システム監査用語の定義と解説」）

【関連用語】 -

実証性テスト

【定義】 管理手続によりもたらされた結果を実際に確かめることにより実装されたコントロールについて十分な心証を目的とするテスト。

【解説】 実証性テストの目的は、ある結果からその途中プロセスがルール通りであることを、十分な量の記録に基づきテストすることである。

【関連用語】 有効性監査
準拠性テスト

実装・運用監査

【定義】 組織が実装し、現在運用している情報セキュリティ対策が、組織が定めた情報セキュリティ対策とかい離がないことを、評価対象とする監査。
情報セキュリティ対策が有効に機能していることをある時点で検証する場合と、一定期間で検証する場合の 2 つのタイプがある。

【解説】 -

【関連用語】 設計監査

実態方式

【定義】 情報セキュリティについての実態を保証の対象とする監査の方式。
「非言明方式」ともいう。

【解説】 -

【関連用語】 言明方式

質問（Inquiry）

【定義】 マネジメント体制又はコントロールについての整備状況又は運用状況を評価するために、関係者に対して口頭または文書で問い合わせ、説明や回答を求める監査技法。「インタビュー」または「聞き取り」ともいう。

【解説】 組織内部の担当者又は管理者だけでなく、取引先、委託先等の外部への問い合わせも含まれる。

【関連用語】 監査技法、閲覧、観察、再実施

時点監査

【定義】 過去の一時点を基準日とし、その時点の状況を対象とする監査。

【解説】 運用状況を評価するため、時点監査においては基準日から一定期間さかのぼった状況について、証拠を収集する必要がある。
時点監査は、一定期間を対象とする期間監査と比べ、監査工数が少なく効率性が高いが、一方で信頼性が劣るため、監査ニーズに合わせて方式を選択する必要がある。

【関連用語】 期間監査

社会的合意方式

【定義】 社会的に合意された情報セキュリティ管理基準や監査基準に沿って、すべての利害関係者たり得る利用者にその結果を通知する方式。

【解説】 監査人は、主題の監査に必要かつ十分な監査手続を実施し、その結果を記載した監査報告書は利用者を限定せず、すべての利用者に伝える。

【関連用語】 被監査主体合意方式
利用者合意方式

準拠性監査

【定義】 定められた規格、基準、手順等に従って実際の運用が行われていることを評価する監査。

【解説】 準拠性監査では、コントロールに準拠しているとの心証を監査人が得ることを目的としている。したがって、違反がないとは言えないまでも、監査した範囲において、コントロールが機能していることが確認できることが求められる。

準拠性テストは監査の手法の一つであり、準拠性監査とは異なる概念である。

【関連用語】 有効性監査

準拠性テスト

準拠性テスト

【定義】 実装された管理手続が意図された通りに機能していることを確かめることを目的とするテスト。

【解説】 -

【関連用語】 準拠性監査、実証性テスト

情報資産

【定義】 情報そのもの、又は情報を扱う仕組みを指す。書類・電子データだけでなく、ハードウェア、ソフトウェア、インフラサービスといった情報システムをも指す。

【解説】 具体的には、情報に加えて、アプリケーション、プログラムといったソフトウェアや、ハードウェア、設備等の物理的資産、その他サービス、人、企業イメージ等が情報資産として定義される。

何を組織の情報資産として定義するかは、組織の業務特性などを考慮して決めることになる。

情報資産を識別し、情報資産の価値を決定することは、リスクアセスメントを実施する上で欠かせないステップである。

【関連用語】 -

情報セキュリティ（Information security）

【定義】 情報の機密性、完全性及び可用性を維持すること。
注記：さらに、真正性、責任追跡性、否認防止及び信頼性のような特性を維持することを含めても良い。（JISQ27000:2014）

【解説】 JISQ27000 によって次の 3 つの性質が定義されている。機密性(confidentiality)、完全性(integrity)、可用性(availability)、これら三つを、英語の頭文字を取って、情報の CIA ということもある。
上記の情報セキュリティの定義に、更に 1996 年に 3 つ、2006 年に 1 つが追加されている。
それら性質の定義は、次のとおりである。
真正性(authenticity)、責任追跡性(accountability)、否認防止(non-repudiation)、信頼性(reliability)、
上記に定義されている特性を維持し、被監査主体の情報資産を保護する仕組み。

【関連用語】 機密性、完全性、可用性、真正性、責任追跡性、否認防止、信頼性

情報セキュリティインシデント（Information security incident）

【定義】 望ましくない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連のセキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの。（JISQ27000:2014）

【解説】 インシデントとは情報セキュリティ事象に含まれ、その中で業務の遂行や情報資産の保護を特に脅かす確率の高いものをいう。情報セキュリティにかかわる事件・事故である。具体的な内容は被監査主体で決めるのが基本であり、事件・事故の経験を踏まえて業務に支障を与える事象（情報漏えい、破損、改ざん、不正アクセス、システム停止など）をインシデントと定義する。

【関連用語】 情報セキュリティ事象

情報セキュリティ監査（Information security audit）

【定義】 情報セキュリティに係るリスクのマネジメントが効果的に実施されるように、情報セキュリティマネジメントの体制及びコントロールの整備、運用状況を、独立かつ専門的な立場から、一定の基準に従って検証又は評価し、もって保証を与えあるいは助言を行う活動。

【解説】 コントロールの整備等は、リスクアセスメントに基づく必要がある。

【関連用語】 -

情報セキュリティ監査基準

【定義】 情報セキュリティ監査業務の品質を確保し、有効かつ効率的に監査を実施することを目的とした監査人の行為規範である。一般基準、実施基準、報告基準からなる。

【解説】 情報セキュリティ監査基準は、組織体の内部監査部門等が実施する情報セキュリティ監査だけでなく、組織体の外部者に監査を依頼する情報セキュリティ監査においても利用できる。さらに、本監査基準は、情報セキュリティに保証を付与することを目的とした監査であっても、情報セキュリティの欠陥に対して助言を行うことを目的とした監査であっても利用できる。

【関連用語】 情報セキュリティ管理基準

情報セキュリティ管理基準

【定義】 組織体が効果的な情報セキュリティマネジメント体制を構築し、適切なコントロールを整備、運用するための実施規範であり、情報セキュリティ監査を実施する際の判断の尺度の参照基準ともなる。

【解説】 経済産業省では、平成 15 年に策定された「情報セキュリティ管理基準」（平成 15 年経済産業省告示第 112 号）を改定し、「情報セキュリティ管理基準（平成 20 年改正版）」（平成 20 年経済産業省告示第 246 号、平成 21 年 2 月 1 日適用）を発行した。

改訂版は、国際規格である ISO/IEC27001:2005（JISQ27001:2006）及び ISO/IEC27002:2005（JISQ27002:2006）に基づいており、ISMS 認証取得、及び情報セキュリティマネジメントの確立を目指す組織、並びに情報セキュリティ監査の実施、及び監査を受ける組織など幅広い利用者を想定した情報セキュリティのための管理基準である。

【関連用語】 情報セキュリティ監査基準

情報セキュリティ事象（Information security event）

【定義】 情報セキュリティ方針への違反若しくは管理策の不具合の可能性、又はセキュリティに関係し得る未知の状況を示す、システム、サービス又はネットワークの状態に関連する事象（JISQ27000:2014）

【解説】 情報セキュリティ事象は、異状を示すできごとを意味する。情報システムにおいては、認可されないポートスキャン、SPAM メール、ウイルス感染、DoS 攻撃、など。組織マネジメントにおける、入館カードの紛失や退職者のアカウントの消し忘れなども含まれる。

情報セキュリティ事象は、情報セキュリティインシデントが生じる兆候、あるいは実際にインシデントが生じていることの表れである可能性がある。また、情報セキュリティマネジメントが有効に機能していないことを示すシグナルであることもあり得る。

【関連用語】 情報セキュリティインシデント

情報セキュリティにおけるコンサルティング

【定義】 依頼者からの情報セキュリティのマネジメント又はコントロールの改善に関する課題の相談に応じ、課題の解決を支援する業務。

【解説】 コンピュータウィルス、不正アクセス行為、システムダウンによる業務中断、故意や不注意による情報漏えいなどの脅威に対する対策に関する問題点を指摘し、原因を分析し、対策案を示して依頼者を支援する業務。

助言型監査は情報セキュリティ管理基準を踏まえた個別管理基準に照らして評価を行うが、コンサルティングは個別管理基準を必ずしも使う必要はない。

【関連用語】 -

情報セキュリティマネジメント（Information security management）

【定義】 組織、サービスあるいはシステムに関わる資産（情報、データなど）の機密性、可用性、完全性を確実にするプロセス

【解説】 -

【関連用語】 -

情報セキュリティマネジメントシステム（Information security management system）

【定義】 情報セキュリティに関わる、方針、目的及びその目的を達成するためのプロセスを確立するための、相互に関連する又は相互に作用する、組織の一連の要素
注記：マネジメントシステム；方針、目的及びその目的を達成するためのプロセスを確立するための、相互に関連する又は相互に作用する、組織の一連の要素
（JISQ27000:2014）

【解説】 被監査主体における、情報セキュリティの確立、導入、運用、監視、レビュー、改善に関わる体系的な実施プロセスである。情報を管理し機密を守るために、コンピュータシステムのセキュリティ対策だけでなく、情報を適切に扱うための基本方針の確立、実施計画の策定、計画の実施・運用、一定期間ごとの方針・実施計画の見直しまでを含む、リスクマネジメント体系である。
ISMS と略される。

【関連用語】 -

情報伝達

【定義】 目的を達成するために、構成員が、必要な情報を識別、収集、処理し、伝達すること。（経済産業省、2003「リスク管理・内部統制に関する研究会」報告書）

【解説】 情報伝達とは、監査を実施するため、必要な情報の識別・把握・処理が関係する組織や責任者に、適宜、適切に伝えられること。

【関連用語】 -

助言意見

【定義】 助言型監査における監査意見。

【解説】 助言意見は、検出事項と改善提言により構成される。

【関連用語】 -

助言型監査

【定義】 情報セキュリティのマネジメント又はコントロールの改善を目的として、監査対象事象に関わる客観的な基準とのギャップを測ることで、情報セキュリティ対策上の欠陥及び懸念事項等の問題点を検出し、必要に応じて当該検出事項に対応した改善提言を監査意見として表明する形態の監査。

【解説】 言明方式の助言型監査の場合には、言明を評価する基準に基づき、言明が適切であると言いきれない状況が存在するか否かを検証する。
実態方式の場合には、客観的基準と実態とのかい離を検証する。

【関連用語】 保証型監査

真正性（Authenticity）

【定義】 エンティティは、それが主張するとおりのものであるという特性。
（JISQ27000：2014）

【解説】 組織又はシステムの主張どおりに情報及び資産が確実に保護されていることが確認できる手段がある状態。

【関連用語】 -

信頼性（Reliability）

【定義】 意図する行動と結果とが一貫しているという特性。
（JISQ27000：2014）

【解説】 一定の条件下で安定して期待された役割（システムなどの障害や不具合の発生しにくさ）を果たすことができる能力。

【関連用語】 -

精査

【定義】 監査対象のすべてを検証の対象範囲として監査手続を実施する方法。

【解説】 -

【関連用語】 試査

ぜい弱性（脆弱性）（Vulnerability）

【定義】 一つ以上の脅威によって付け込まれる可能性のある、資産又は管理策の弱点。（JISQ27000：2014）

【解説】 ぜい弱性とは、意図された手順とは異なった方法、又は目的で使用される情報資産の性質又は属性であり、脅威の発生原因によって利用されることにより、リスクがあらわになること。

ぜい弱性は、単独でその利用されやすさのレベルを評価する場合（①）と、脅威の発生頻度評価の際の一要因として考慮される場合（②）とがある。

この関係をリスク計測における数式で表現すると:

①リスク＝脅威×ぜい弱性×資産価値

②リスク＝脅威×脅威の発生頻度×資産価値

ただし、脅威の発生頻度はぜい弱性の関数となる。

【関連用語】 ぜい弱性検査

ぜい弱性検査

【定義】 システムやソフトウェアにぜい弱性がないかを調べること

【解説】 ファームウェアを含むシステムを構成するソフトウェアのバージョンやパッチの適用状況の調査や、設定状況の調査を通じて、既知のぜい弱性が残されているか、簡易な方法で侵入が可能であるか等を確認する検査である。

【関連用語】 ペネトレーションテスト、技術的検証

成熟度モデル

【定義】 組織の能力を評価し、「判断の尺度」として段階に区切り、どの程度のレベルまで達成しているか示す指標。

【解説】 -

【関連用語】 -

責任追跡性（Accountability）

【定義】 あるエンティティの動作が、その動作から動作主のエンティティまで一意に追跡できることを確実にする特性。（JISQ13335-1:2006）

【解説】 情報の履歴などがたどれる状態を、責任追跡性が保たれているという。いつ誰がその情報を更新したのか、削除したのか、通信したのかを追跡できることを確実にすること。

【関連用語】 -

設計監査

【定義】 組織が定めた(設計した)情報セキュリティ対策が、第三者から求められているレベルに達していることを評価対象とする監査。

【解説】 設計されたコントロールのある時点の整備状況について検証するものである。

【関連用語】 実装・運用監査

整備状況評価

【定義】 識別したリスクを低減するための内部統制が組織の中に存在するかを確かめること

【解説】 内部統制の監査においては、整備状況評価と運用状況評価を行う。整備状況評価では、内部統制が有効にデザインされ実装されていることを確認する。

【関連用語】 運用状況評価

【た】

他の専門職

【定義】 特殊な監査判断を行うにあたって、専門的な立場から監査人を支援する者。

【解説】 ネットワークスペシャリスト、システムアナリスト、ビジネスコンサルタント、技術士、弁護士、公認会計士等の専門職が考えられる。
また、セキュリティアーキテクト、セキュリティエンジニア、セキュリティテスター、セキュリティシステムアドミニストレーター、セキュリティアナリスト、フォレンジックアナリスト、インシデントハンドラー（いずれも、情報セキュリティ人財アーキテクチャガイドブック；ISEPA；2009 による）などの技術者が有用である。

【関連用語】 監査人

定性的リスクアセスメント手法

【定義】 リスクをその大きさに応じて分類して表現し、評価する方法。

【解説】 リスクの大きさの表現としては、「影響の度合いを大・中・小で分類する」、「頻度を頻繁、希少、時々で分類する」という方法などが用いられる。分類の結果を数値でランクとして表現する方法も定性的リスクアセスメント手法の一部である。

【関連用語】 定量的リスクアセスメント手法

定量的リスクアセスメント手法

【定義】 リスクを数量として表現し、評価する手法。

【解説】 分かりやすい表現としては、金銭的な表現がある。

【関連用語】 定性的リスクアセスメント手法

デジタル・フォレンジックス（Digital forensics）

【定義】 情報セキュリティインシデントの原因究明や被害状況を把握するために、電子機器に残留している電磁的な記録（正式な記録および残留している記録の痕跡など）を証拠保全・調査・分析し、その法的な証拠性を明らかにする一連の科学的調査方法や技術

【解説】 単に、フォレンジックスと略されることがある。
デジタル・フォレンジックスはコンピュータ・フォレンジックス(Computer forensics)やネットワーク・フォレンジックス(Network forensics)などがある。デジタルデータを扱う機器全般を対象とし、不正アクセスの疑いのあるハードディスクから証拠となるファイルを探し出したり、サーバのログファイルから不正アクセスの記録を割り出したり、破壊・消去されたディスクを復元して証拠となるデータを押収したりといった技術が該当する。
電磁的な記録等は書き換えが可能であるなど可変であるため、証拠の保全や収集した記録が証拠として使えるか（証拠力の検証）などについて、一定の手続きが必要となる。

【関連用語】 -

統制活動（Control activities）

【定義】 リスク対応策が適切に実行され、経営者の適正な業務指示が実行されるための方針と手続き。

【解説】 組織の業務を適正に実行するための、適正な権限及び職責を付与、職務の分掌等の広範な方針及び手続きを定め、実行する事を指す。

【関連用語】 -

統制環境（Control environment）

【定義】 組織が保有する価値基準、及び組織の基本的な人事、職務の制度等を総称する概念。

【解説】 統制環境とは、組織の気風を決定し、組織内のすべての者の統制に対する意識に影響を与えるとともに、他の基本的要素の基礎をなし、リスクの評価と対応・統制活動・情報と伝達・モニタリング及び IT への対応に影響を及ぼす基盤をいう。
（「財務報告に係る内部統制の評価及び監査に関する実施基準」より）

【関連用語】 -

統制リスク（Control risk）

【定義】 組織の内部統制によって防止または発見されないリスク。

【解説】 情報セキュリティのマネジメントまたはコントロールが有効でない場合、情報セキュリティのリスクが高まる。

【関連用語】 監査リスク、リスクアプローチ、監査リスクモデル、固有リスク、発見リスク

独立性（Independence）

【定義】 監査を客観的、不偏的に実施するために、監査人が監査対象から独立すべきとする要件。

【解説】 外観上の独立性と精神上の独立性がある。

情報セキュリティ監査人として外観上の独立性を損ねることは、本来的独立性としての精神上の独立性に著しい悪影響を及ぼす可能性があることから、情報セキュリティ監査人に対して監査対象組織との間の経済上・身分上の利害関係を禁止していることに外観上の独立性の本旨がある。

情報セキュリティ監査人としての独立性は、本来的には、精神上の独立性を保持することによってはじめて確保されるものである。

独立性の要件については、仕様書等にその要件についての記載がなくても検討しなければならない。検討の結果、独立性に抵触する可能性があると判断される場合、監査責任者は監査依頼者に独立性に抵触する可能性のある旨及びその理由を説明し、独立性に抵触しないように監査対象を変更するか、監査報告書に独立性についての注記を記載する旨の説明をし、同意を得なければならない。

情報セキュリティ監査人は協会が定める独立性ガイドラインを参照し、独立性を保つようにする必要がある

【関連用語】 -

【な】

内部監査 （Internal audit）

【定義】 組織体の目標達成のために行われる助言型監査。

【解説】 内部監査は、以下の特徴を有する
・リスクマネジメント、コントロール及びガバナンスの各プロセスの有効性の評価と改善を行う
・体系的で規範的アプローチ
内部監査の実施は、被監査組織の一員が内部監査人として行う場合と、外部監査人に委託して行う場合がある。

【関連用語】 外部監査

内部統制 （Internal control）

【定義】 企業がその業務を適正かつ効率的に遂行するために社内に構築され、運用される体制及びプロセス。（経済産業省、2003「リスク管理・内部統制に関する研究会」報告書）

【解説】 内部統制はマネジメント体制を整備し、コントロールを整備・運用することによって行うことができる。
内部統制が不十分な状況で情報セキュリティ管理基準に照らして監査を行うと、多くの検出事項が発見されるため、限られた時間内では検出事項の網羅的発見は困難となる可能性が高い。
このような場合、監査依頼者に事前に了解を得ておくことが望ましい。

【関連用語】 -

内部統制環境

【定義】 企業がその目的を達成するために、企業活動を適正かつ効率的に運営するための価値観、組織、規則等であり、企業構成員の様々な行為の基礎となるもの。（経済産業省、2003「リスク管理・内部統制に関する研究会」報告書）

【解説】 内部統制環境とは、組織内のすべての者の統制に対する意識に影響を与えるとともに、他の基本的要素の基礎・基盤となるもの。
具体的には、誠実性・倫理観、経営者の意向・姿勢、経営方針・経営戦略、組織構造と慣行などが挙げられる。

【関連用語】 -

二者間の監査

【定義】 被監査主体と独立した監査主体の二者の間で行われる監査

【解説】 会計用語の二者監査は二者間の監査の一形態である。
ISO19011 に記載されている第一者監査は、被監査主体と報告書利用者が同一であり、第二者監査は監査主体が報告書利用者となる。
監査の独立性を考えると、報告書利用者は利害関係者であるので、第二者監査は二者間の監査とは言えない。第二者監査は報告書利用者が行う内部監査の一部である。

【関連用語】 -

2 次利用者

【定義】 被監査主体と直接の利害関係のある 1 次利用者と利害関係があるために、間接的に被監査主体の監査テーマに関係を持つ利用者。

【解説】 1 次利用者と2次利用者との関係は、サービス提供業者と顧客との関係などで見ることができる。サービス提供業者がデータセンタ（DC）を使っている場合、そのセキュリティが問われる。DC の監査の結果はサービス提供業者が直接的に利用する。顧客等からサービス提供業者が DC のセキュリティについて問われた時に、当該 DC が監査済みであることを説明に用いることがある。

【関連用語】 -

任意監査

【定義】 法律によって監査が義務付けられていないが、特定の目的（業務の効率化、適正化等）を達成するために監査人に依頼して行う監査。

【解説】 -

【関連用語】 法定監査

【は】

発見リスク（Detection risk）

【定義】　組織の内部統制により防止又は発見できなかった情報セキュリティ上のリスクが、監査人の監査手続によっても発見できないリスク。

【解説】　監査の時間的・技術的制約により、監査手続が及ばないことが生じる。この場合に発見リスクが大きくなる恐れがある。監査人は、発見リスクを小さくするように、あらかじめ監査リスクを把握し、リスクに応じた監査手続を計画することが必要である。

【関連用語】　監査リスク、リスクアプローチ、監査リスクモデル、固有リスク、統制リスク

判断に関する見解の相違

【定義】 判断に関する見解の相違とは、検出事項の重要性等について、監査人と監査対象組織の責任者との間で判断の重要性が異なる場合等をいう。

【解説】 判断に関する見解に相違が生じた場合、監査責任者は監査対象組織の責任者と協議し、見解の相違が解消するように努める。見解の相違が解消できない場合、監査人は監査報告書に監査人の意見と監査対象組織の意見の両論を併記しなければならない。

【関連用語】 事実に関する見解の相違

被監査主体

【定義】 監査を受ける対象(機関、組織又は人)。

【解説】 被監査主体は、対象範囲における情報セキュリティマネジメントについて責任を有する。このため、情報セキュリティに関わるリスクを評価し、その結果に基づくリスク受容水準にあわせて、適切な管理策を選択・実装・運用する。

【関連用語】 監査主体

被監査主体合意方式

【定義】 被監査主体が、利害関係者に向けて説明するために、特定の監査テーマを定め、その監査手続を監査人と相談し合意の上で定める場合で、かつ、監査テーマと監査手続について監査報告書の利用者の同意あるいは確認が取れている場合の保証型監査のやり方。

【解説】 監査人は、被監査主体の依頼を受けて、監査テーマに関して被監査主体と合意した監査手続に従って、被監査主体が定めた情報セキュリティマネジメントの実態が存在するかどうかを主眼に監査を実施し、監査結果を報告する。

【関連用語】 利用者合意方式
社会的合意方式

非言明方式

【定義】 「実態方式」参照。

【解説】 -

【関連用語】 -

否定意見

【定義】 監査人による「被監査主体が行った言明と実際の情報セキュリティ対策に重大なかい離があり、言明が信ずるに足ると言いえない」旨の表明。

【解説】 -

【関連用語】 -

否認防止 (Non-repudiation)

【定義】 主張された事象又は処置の発生、及びそれを引き起こしたエンティティを証明する能力。(JISQ27000:2014)

【解説】 デジタル証明を利用した行為、又それによって起きた事象を事後になってその利用事実を否定することができないように証拠を残すこと。

【関連用語】 -

品質管理者

【定義】 監査チームとは独立して、監査チームが実施した監査業務の品質を管理する者。

【解説】 監査主体は、監査品質を維持し、向上させることを目的として、監査人の能力の保証、実施した監査手続のレビュー、監査達成状況の評価等を行う品質管理者を置く。品質管理者は、監査業務が情報セキュリティ監査基準、実施基準ガイドライン、報告基準ガイドライン、その他監査主体が所属している組織の基準等に準拠していることが求められる。
品質管理者は、監査チームの業務を公正な立場から評価できるように、監査チームから独立していること、及び、品質管理を行う権限が付与されている必要がある。このため、品質管理を行う権限を裏付ける規程等を整備しておくことが望まれる。
なお、必ずしも専任の品質管理者を置く必要はない。

【関連用語】 監査責任者

品質管理統括責任者

【定義】 監査組織において情報セキュリティ監査業務の品質管理を統括する責任者

【解説】 監査主体は、監査品質を維持し、向上させることを目的として、監査人の能力の保証、実施した監査手続のレビュー、監査達成状況の評価等を行う品質の管理者を置く。このうち、組織全体の品質管理について、責任を有するものを品質管理統括責任者という。
個別業務ごとの品質管理は、品質管理統括責任者が品質管理者を指名し、実施する。
なお、陣容の十分でない監査組織にあっては、自己が監査責任者である業務以外の業務について、品質管理統括責任者が品質管理者を兼務することができる。

【関連用語】 監査責任者、品質管理者

フォレンジックス

【定義】 デジタル・フォレンジックスの略語（情報セキュリティに関係する場合）

【解説】 -

【関連用語】 -

フォローアップ

【定義】 フォローアップ監査

【解説】 -

【関連用語】 -

フォローアップ監査

【定義】 助言型監査の結果に基づき被監査主体が行っている情報セキュリティ管理の改善が、助言の主旨に沿って実施されているかを監査人が評価すること
フォローアップと略されることがある

【解説】 -

【関連用語】 -

紛争審査制度

【定義】 監査の内容又は品質に関し、被監査主体あるいは利害関係者と監査主体の間に生じた紛争を契機として、当該監査が情報セキュリティ監査制度の基準に適合するか否かを審査し、紛争の裁定を行う制度。

【解説】 -

【関連用語】 -

ペネトレーションテスト（Penetration test）

【定義】 コンピュータやネットワークのセキュリティ上の弱点を発見するテスト手法の一つで、システムへの侵入が可能かを、実際に試みて分析する手法。

【解説】 ペネトレーションテストには、実際に攻撃を試みるアクティブテストと、通信の応答からシステム設定を分析し侵入できることを確認するパッシブテストがある。
システム侵入検査ともいう。

【関連用語】 ぜい弱性検査、技術的検証

法定監査

【定義】 法律によって実施することが義務付けられている監査。

【解説】 法定監査の代表的な例は、公開企業の財務諸表監査（会計監査）である。

【関連用語】 任意監査

保証

【定義】 情報セキュリティ管理に責任を負うものが表明した言明に対して、想定利用者の信頼の程度を高めるために、監査人が自ら入手した証拠に基づき基準に照らして判断した結果の表明

【解説】 -

【関連用語】 -

保証意見

【定義】 保証型監査における監査意見。

【解説】 保証意見には、肯定意見、限定付き肯定意見、否定意見の 3 つの種類がある。

【関連用語】 -

保証型監査

【定義】 監査対象たる情報セキュリティのマネジメント又はコントロール若しくはこれらに関する監査対象に責任を持つ者の言明が、監査手続を実施した限りにおいて適正である旨（又は不適正である旨）を監査意見として表明する形態の監査。

【解説】 情報セキュリティ監査では言明方式を採用している。監査人は、監査した範囲において、言明が適切であるとの心証を得られた場合に、適正意見を述べる。

【関連用語】 助言型監査

保証業務

【定義】 監査対象の経営者が発した言明に対し、監査人が合理的な方法と証拠に基づき、監査の対象となる組織体の情報セキュリティに関するマネジメントとコントロールが監査手続きを実施した限りにおいて適正である旨（または不適正である旨）の意見を述べること。

【解説】 -

【関連用語】 -

保証水準

【定義】 監査人が保証業務において意見を述べる際の適正（あるいは不適正）の程度

【解説】 保証水準には、監査対象が基準に適合していることを積極的に保証する合理的保証水準（「適正である」といえる水準）と、消極的に保証する限定的保証水準（「適正でないとはいえない」といえる水準）の 2 種類がある。

【関連用語】 -

【ま】

モニタリング

【定義】 業務の遂行状況を継続的に監視する活動。（経済産業省、2003「リスク管理・内部統制に関する研究会」報告書）

【解説】 -

【関連用語】 -

【や】

有効性監査

【定義】 判断の基準（クライテリア）となる規格、基準（スタンダード）の意図する目的や目標が達成されるようにコントロールが整備され、そのコントロールがリスクを期待水準以下にしているかを評価する監査。

【解説】 有効性監査では、コントロールが目的又は目標を達成するために、有効に機能しているとの心証を監査人が得ることを目的としている。
コントロールが有効とされるには、以下の条件が必要である。
・適切な管理権限を持った者が定めたコントロールが存在する
・そのコントロールの目的を実現するための手段が実装されている
・コントロールの対象となる活動の記録は組織が定める水準以上の信頼度で取得され、保存されている
・コントロールに違反する活動は組織が許容する水準以下である

【関連用語】 準拠性監査

予備調査

【定義】 監査の依頼があった後に、監査対象と監査対象の実態を明確にし、円滑かつ効率的な本調査の実施を可能とするために行われる事前調査。

【解説】 本調査の前に、監査対象を明確にするために、監査対象の実態、問題点の背景や概要を調査する。
予備調査は本監査の計画立案に必要な情報収集を目的としている。
保証型監査の場合には、それに加えて、保証可能性の検証と監査の重点の絞り込みを行うための、情報収集を目的とする。

【関連用語】 -

【ら】

リスク（Risk）

【定義】 目的に対する不確さの影響
（JISQ27000:2014）

【解説】 影響とは、期待されていることから、好ましい方向又は好ましくない方向にかい（乖）離することをいう。
不確かさとは、事象、その結果又はその起こりやすさに関する、情 報、理解又は知識が、たとえ部分的にでも欠落している状態をいう。
リスクは、起こり得る事象、結果又はこれらの組合せについて述べることに よって、その特徴を記述することが多い。
リスクは、ある事象（周辺状況の変化を含む。）の結果とその発生の起こりやすさとの組合せとして表現されることが多い。
ISMS の文脈においては、情報セキュリティリスクは、情報セキュリティ目的に対する不確 かさの影響として表現することがある。
情報セキュリティリスクは、脅威が情報資産のぜい弱性又は情報資産グルー プのぜい弱性に付け込み、その結果、組織に損害を与える可能性に伴って生じる。
(JIS Q 27000:2014)

【関連用語】 -

リスクアセスメント（Risk assessment）

【定義】 リスク特定、リスク分析及びリスク評価のプロセス全体（JISQ27000：2014）

【解説】 リスクアセスメントの手法には、さまざまな手法があるが大きな流れとしては、1)対象領域の決定、2)リスク因子の特定、3)発生頻度および損失規模の推定、4)リスク全体の見積もりという手順を踏む。

【関連用語】 リスク特定、リスク分析、リスク評価

リスクアプローチ

【定義】 監査におけるリスクを軽減し、効率的かつ効果的に監査の目的を達成しようとする戦略を具体化したアプローチ。

【解説】 監査対象全体を俯瞰し、監査リスクが高い項目について重点的に監査の人員や時間を充てることにより、監査対象のリスクプロファイルに応じた効果的かつ効率的・経済的に監査を実施できる。

【関連用語】 監査リスク、監査リスクモデル

リスク基準（Risk criteria）

【定義】 リスクの重大性を評価するための目安とする条件。(JISQ27000:2014)

【解説】

【関連用語】 リスク評価

リスク対応

【定義】 リスクを修正するプロセス。(JISQ27000:2014)

【解説】 リスク対応の選択肢として、JIS Q 31000:2010 (ISO 31000:2009)では、以下の7つが例示されている。

a)リスクを生じさせる活動を開始又は継続しないと決定することによって、リスクを回避する。

b)ある機会を追求するために、そのリスクを取る又は増加させる。

c)リスク源を除去する。

d)起こりやすさを変える。

e)結果を変える。

f)一つ以上の他者とそのリスクを共有する(契約及びリスクファイナンシングを含む。)。

g)情報に基づいた意思決定によって、そのリスクを保有する。

【関連用語】 -

リスク特定 (Risk identification)

【定義】 リスクを発見、認識及び記述するプロセス。(JISQ27000:2014)

【解説】 リスク特定には、リスク源、事象、それらの原因及び起こり得る結果の特定が含まれる。リスク特定には、過去のデータ、理論的分析、情報に基づいた意見、専門家の意見及びステークホルダのニーズを含むことがある。

【関連用語】 リスクアセスメント、リスク分析、リスク評価

リスク評価 (Risk evaluation)

【定義】 リスク及び/又はその大きさが、受容可能か又は許容可能かを決定するために、リスク分析の結果をリスク基準と比較するプロセス (JISQ27000:2014)

【解説】 -

【関連用語】 リスクアセスメント、リスク特定、リスク分析

リスク分析 (Risk analysis)

【定義】 リスクの特質を理解し、リスクレベルを決定するプロセス
（JISQ2700:2014）

【解説】 -

【関連用語】 リスク特定、リスク評価、リスクアセスメント

リスクマネジメント（Risk management）

【定義】 リスクについて、組織を指揮統制するための調整された活動
（JISQ27000:2014）

【解説】 リスクマネジメントには、リスク分析・リスクアセスメント・リスク対応のプロセスがある。リスクコミュニケーションを通じて、経営者は適切なリスクマネジメントを行うことが必要である。
監査人は、リスクアセスメントに基づくリスク対応策が選択されているか、リスク対応策の選択に基づきコントロールの導入が行われているかどうかを把握することが重要である。
監査対象にリスクマネジメント体制自体の評価が含まれている場合、リスクに応じたコントロールが整備されているかどうかを確かめることになる。

【関連用語】 -

利用者

【定義】 直接又は間接的に監査報告書の全て又は一部を利用する機関、組織又は人。

【解説】 被監査主体の監査テーマに直接の利害関係のある１次利用者と、間接的に被監査主体の監査テーマに関係を持つ2次利用者とからなる。

【関連用語】 -

利用者合意方式

【定義】 被監査主体の情報セキュリティ対策に直接の利害関係を持ち、その適否や有効性に特定の期待や要求水準を示している監査報告書の利用者（１次利用者）が、監査人が採用する監査手続の十分性について暗黙又は明示的に合意している場合の保証型監査。

【解説】 監査人は、１次利用者の期待する情報セキュリティ確保の要求水準を満しているかどうかを確認するに十分な監査手続を実施し、その結果を１次利用者に報告する。

【関連用語】 社会的合意方式
被監査主体合意方式

倫理審査制度

【定義】 紛争審査や品質審査によらず、日本セキュリティ監査協会会員及び公認情報セキュリティ監査人資格制度（CAIS）資格登録者について倫理基準に違反する事実が判明したとき、その事実について懲戒処分を行うべきか否かを審査する制度。

【解説】 -

【関連用語】 -

レビュー

【定義】 「閲覧」の項目参照。

【解説】 -

【関連用語】 -

【参考】

第三者監査

【定義】 業務委託契約などにおける発注者と受注者の関係において、発注者、または、受注者が、独立した第三者に受注者の監査を依頼する場合。独立した第三者が監査主体となり、受注者が被監査対象となる。一般に、監査結果は、被監査対象（受注者）の利害関係者（発注者、他）が、被監査対象（受注者）の情報セキュリティ管理状況の確認、受注者の選定に利用する。

【解説】 会計監査における二者監査、三者監査とは異なる概念であることに留意すること。

会計監査においては、監査人が必ず介在するため、すべて第三者監査になる。

会計監査における二者監査は、監査報告書の利用者と被監査主体が同一で、監査人が評価した結果を報告する評価業務を指す。

三者監査は被監査主体、報告書利用者、監査人の三者関係がある場合の監査である。

【関連用語】 第二者監査

第二者監査

【定義】 業務委託契約などにおける発注者と受注者の関係において、発注者が監査主体となり、受注者が被監査対象となる場合。一般に、監査結果は、発注者が受注者の情報セキュリティ管理状況の確認、受注者への改善指導、受注者の選定に利用する。

【解説】 会計監査における二者監査、三者監査とは異なる概念であることに留意すること。（詳細は第三者監査の項参照）

【関連用語】 第三者監査