情報セキュリティ監査　用語集

Ver 3 .0

2023 年 10 月 1 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
特定非営利活動法人 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

特定非営利活動法人 日本セキュリティ監査協会

用語集の改訂作業について

情報セキュリティ監査用語集（「用語集」と略す）は、情報セキュリティ監査の基礎である。公認情報セキュリティ監査人資格協会認定研修コースの教科書（以下、「教科書」と略す）も用語集に基づき作成されている。

用語集は 2015 年に改訂されて以降、10 年近く見直しが行われないまま使用されていた。2021 年から開始した教科書の改訂作業を通じて、用語定義の追加等の必要性が認識された。この認識は資格認定委員会でも共有され、日本セキュリティ監査協会全体として用語集改訂に取り組む必要が叫ばれている。

しかし、本格的な用語集改訂作業には相応の時間が必要となる。一方で研修教科書の改訂は伸ばすことができない。このため、教科書の改訂を行っていた研修トレーニング小委員会が教科書と用語集の平仄をあわせ、必要最小限の改訂作業を進めることとした。

本改訂版は、教科書発行に向けて約半年の期間で行ったものである。今後、本格的な改訂が行われるまでの暫定版として、利用されることを想定している。

本改訂作業は、研修トレーニング小委員会メンバーの多大な貢献により行われた。また、内容のレビューは資格認定委員会及び試験小委員会の委員各位にご協力いただいた。これらの方々を含めて、改訂作業にあたっていただいた方々に深く感謝の意を表する次第である。

2023 年 10 月
特定非営利活動法人　日本セキュリティ監査協会
会長　手塚　悟

研修トレーニング小委員会委員名簿

委員長	間宮 正行	国立大学法人東京工業大学
	新井 雅	富士通株式会社
	池田 秀司	i-3c 株式会社
	板垣 一弘	NTT コミュニケーションズ株式会社
	太田 利次	ジーブレイン株式会社
	河野 省二	日本マイクロソフト株式会社
	菊地 宏紀	NEC セキュリティ株式会社
	幸田 一生	富士通株式会社
	小林 達司	株式会社バリューアップ ジャパン
	小室 武晴	リコージャパン株式会社
	桜井 秀紀	NTT コミュニケーションズ株式会社
	羽生田 和正	株式会社アスラボ

【あ】

1	ISMS （アイエスエムエス）	定義	情報セキュリティマネジメントシステム
		解説	ISMS は“Information Security Management System”の頭文字を組み合わせた略号である。一般用語としては情報セキュリティマネジメントシステムを意味する。 なお、商標登録された ISMS は「ISMS 適合性認証制度」に係るものである。例えば、ISMS 認証はこの制度の認証を意味する。商標登録された意味で使用する場合には注意が必要である。
		関連用語	-
2	1 次利用者	定義	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報告書利用者。
		解説	1 次利用者と監査主体の間で報告書の取扱いについて契約が必要である。
		関連用語	２次利用者
3	インタビュー	定義	質問
		解説	-
		関連用語	-
4	ALE （エー・エル・イー）	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、Annual Loss Expectation（年間損失予測）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回数を乗じて求める。 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	-
5	AUP （エー・ユー・ピー）	定義	合意された手続。
		解説	Agreed Upon Procedure
		関連用語	-

6	運用状況評価	定義	（情報セキュリティ）対策が（情報セキュリティ）目的を達成するために適正に行われていることの評価。
		解説	-
		関連用語	整備状況評価
7	閲覧	定義	ガバナンス、マネジメント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（媒体又は電子データ）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	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 など
		関連用語	レビュー

【か】

8	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	-

9	ガバナンス基準	定義	情報セキュリティガバナンスを評価するための判断の尺度。
		解説	情報セキュリティガバナンス基準は、情報セキュリティ監査において、ガバナンスの責任を負うトップマネジメントの判断の尺度として用いる。なお、トップマネジメントは組織を代表するものであり、一般に株式会社では取締役がその任にあたる。このため、ガバナンスの監査は取締役の業務執行監査の一環として監査役監査として行われることが想定されている。 なお、情報セキュリティガバナンス基準は、政府の告示した情報セキュリティ管理基準には含まれていないが、ISO/IEC27014 などを参照して作成することができる。
		関連用語	マネジメント基準 管理策基準
10	外部監査	定義	被監査主体の組織外の報告書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	外部監査の反意語としての「内部監査」は、内部監査人協会（IIA）において内部目的の監査として定義されている。これに対応し、外部目的の監査を外部監査という。 なお、一般には監査を外部に委託した場合に「外部監査」と呼ぶことがあるが、概念の混乱があるので注意する必要がある。
		関連用語	内部監査
11	可用性	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 。 （JISQ27000:2019）
		解説	組織が認可した利用者（人やシステムなど）が、必要とする時に情報資産にアクセスできることを目的として、システムやデータを保護することで可用性が保たれる。
		関連用語	

12	監査	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	監査は、「監査の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，文書化したプロセス」である。(JISQ27000:2019 に基づく)
		関連用語	
13	監査意見	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監査の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	監査所見
14	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	-
15	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

16	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
17	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、改善指導を監査業務に含むことがある。
		関連用語	-
18	監査計画	定義	監査のあるべき目標を設定し、その目標を達成するための可能な手段を体系化し、その手段の遂行手順、スケジュールを明示化したもの。
		解説	監査計画には、監査基本計画と監査実施計画等がある。文脈によりその内容を判断することが必要となる。
		関連用語	-
19	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	-

20	監査実施計画書	定義	監査基本計画に基づき、個々の監査テーマに従って評価すべき事項、評価の基準、評価のための監査手続及び監査を完遂するために必要な事項を体系化し、その遂行の手順とスケジュールを取りまとめた文書。
		解説	監査の基本的な方針に基づいて、個々の監査単位に実施すべき監査手続についての詳細な計画として作成したもの。
		関連用語	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。
21	監査実施者	定義	監査メンバー
		解説	-
		関連用語	-
22	監査主体	定義	監査を実施する組織体又は個人。
		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
23	監査証拠	定義	監査の目的又は監査人が適用する基準（判断の尺度）に関連し，かつ，検証できる，記録（監査証跡を含む），事実の記述又はその他の情報。
		解説	証拠として採用する資料は、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監査証拠の量と、証拠の質（証明力）を備えていなければならない。 定義文は JISQ19011：2019 の本文のうち「監査基準」を「監査の目的又は監査人が適用する基準（判断の尺度)」と変更したものである。
		関連用語	監査証跡

24	監査証跡	定義	情報システムの処理の内容やプロセス及び人の手による管理の手続等を、監査人が追跡するために時系列に保存された記録。
		解説	監査証跡は一般に以下の 2 つがある。 ・トランザクション証跡：処理内容と結果の関連性を追跡するための記録 ・アクセス証跡：重要ファイルやデータベースといった資源へのアクセスに対する関連性を追跡するための記録 よい監査証跡は「時系列的に事象を再現し、検証することが可能な記録」であり、監査人が意見形成をするための証拠として採用することができる。
		関連用語	監査証拠
25	監査所見	定義	監査意見
		解説	-
		関連用語	-
26	監査責任者	定義	組織の監査業務を統括する者。
		解説	監査組織における監査業務全体の責任を負う。 監査を業とする組織にあっては、監査業務を受託する組織単位の事業責任者が監査責任者となることが一般的である。 内部監査組織であって、部門等の部署が設置されている場合には、当該部署の管理責任者が監査責任者となることが一般的である。 部門等の部署が設置されていない内部監査の場合、監査チームリーダーが監査責任者を兼務することが多い。
		関連用語	監査チームリーダー 監査組織
27	監査組織	定義	監査業務の遂行を共通目標とし、成員間の役割や機能が分化・統合された秩序のある集団、又は監査を業とする個人あるいは団体。
		解説	-
		関連用語	-

28	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。 監査対象となるシステムを「監査対象システム」、施設を「監査対象施設」と呼ぶ。
		関連用語	監査範囲、 監査対象組織
29	監査対象期間	定義	期間監査において対象とする始点の期日から終点の期日までの間。
		解説	
		関連用語	基準日
30	監査対象組織	定義	監査人が監査の対象とする組織。
		解説	監査人が監査の対象とする組織とは、被監査主体の組織において監査範囲に含まれる部署等で、監査手続の対象となりえる組織。
		関連用語	
31	監査チーム	定義	監査を実施する者のグループをいい、監査チームリーダーと監査メンバーからなる。
		解説	監査チームリーダーが、監査を実施するために必要な能力を備えた監査メンバーを、監査に必要な工数に応じて配員した組織体。 監査チームリーダー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	

32	監査チームリーダー	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	監査主体が監査業務を行う場合、監査責任者が監査チームリーダーを決定する。監査チームリーダー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	監査メンバー
33	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「チェックリスト」の用語に２つの意味がある。 ①IT の内部監査を背景とする人々は、チェックリストとは「評価を目的とした一覧表」を指す。 ②会計監査を背景とする人々は、チェックリストとは「監査チームの各メンバーに割り当てた作業が漏れなく行われているかを確認する表」を指す。 本用語の「監査チェックリスト」は①を指す。
		関連用語	監査手続書
34	監査調書	定義	監査人が、情報セキュリティ監査にあたり、情報セキュリティ監査基準等に基づいて監査を実施したこと、及び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	-

35	観察	定義	マネジメント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。
		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	「サイトレビュー」、「視察」
36	監査テーマ	定義	監査において明確にする中心的な内容。
		解説	監査テーマは、監査における根本的意図をもって監査の実施と結果に統一的効果を確保するために設定する。
		関連用語	-
37	監査手続	定義	監査人が監査証拠を入手するための体系化されたプロセス
		解説	監査手続は一つ又は監査技法を組み合わせて実施する。
		関連用語	監査技法
38	監査手続書	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、どの方法で、どの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
39	（監査における）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	-
		関連用語	監査リスクモデル

40	監査人	定義	監査を実施する専門家。
		解説	監査チームが編成される場合は、監査チームリーダー及び監査メンバーに分けられる。但し、監査業務の品質管理者は含まない。
		関連用語	監査チームリーダー 監査メンバー
41	（監査人の） 独立性	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。外観上の独立性と精神上の独立性がある。
		解説	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を参照し、独立性を保つようにする必要がある
		関連用語	独立性

42	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、監査チームリーダーによる品質管理と、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。 監査チームリーダーは、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	
43	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、監査依頼者と協議し、監査範囲を設定する。
		関連用語	-
44	監査品質審査制度	定義	監査品質審査は、日本セキュリティ監査協会の会員又は日本セキュリティ監査協会が資格或いは能力を認定した監査人が実施した監査の品質を、情報セキュリティ監査基準等に基づき評価し、必要に応じ品質向上の支援のあり方を示す制度。
		解説	-
		関連用語	紛争審査制度 倫理審査制度
45	監査報告	定義	監査人が行った監査の結論をとりまとめ、監査依頼者に表明すること。
		解説	-
		関連用語	監査報告書

46	監査報告書	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
47	監査目的	定義	監査依頼者が監査を実施することによって達成しようとする事項又は状態。
		解説	内部監査の場合は、経営陣が監査依頼者となり、監査目的を設定する。
		関連用語	-
18	監査リスク	定義	監査人が誤った監査意見を述べるリスク。
		解説	監査リスクには、重大なリスクの原因があるにもかかわらず見落とすことと、重大なリスクがないにもかかわらず実在するように誤認することの二つがある。
		関連用語	固有リスク 統制リスク 発見リスク
49	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	-
		関連用語	（監査における）リスクアプローチ

50	完全性	定義	正確さ及び完全さの特性。 （JIS Q27000:2019）
		解説	情報が生成された時と同じ状態で維持されていること。 完全性の確保のためには、情報を取り扱うあらゆる場面で、ノイズ、劣化、消失などによる情報の損傷から保護するための手段を講じると共に、完全性が損なわれていないことの確認が必要となる。
		関連用語	
51	管理策	定義	リスクを修正する対策。（JIS Q 27000:2019）
		解説	-
		関連用語	コントロール
52	管理策基準	定義	情報セキュリティ管理基準のうち、管理策を評価するための判断の尺度。
		解説	-
		関連用語	ガバナンス基準 マネジメント基準 詳細管理策
53	管理手続	定義	詳細管理策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	言明書
54	期間監査	定義	情報セキュリティ対策が有効に機能していることを一定期間で検証する監査。
		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 監査対象期間
55	聞き取り	定義	質問
		解説	-
		関連用語	-

56	規準	定義	基準
		解説	-
		関連用語	-
57	基準	定義	監査における判断の尺度及び監査人の行為規範
		解説	情報セキュリティ管理基準は監査における判断の尺度であり、情報セキュリティ監査基準は監査人の行為規範である。
		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
58	基準日	定義	時点監査において監査対象となる日。
		解説	時点監査では過去のある一断面の状況を評価する。この断面を基準日と呼ぶ。基準日に証跡が揃わない場合には基準日以前の証跡から、基準日の状況を推定し、評価を行う。
		関連用語	時点監査 監査対象期間
59	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
60	機密性	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。（JIS Q 27000:2019）
		解説	-
		関連用語	-
61	脅威	定義	システム又は組織に損害を与える可能性があるインシデントの潜在的な原因。(JISQ27000:2019)
		解説	-
		関連用語	-

62	業種業態別基準	定義	特定の業種・業態の情報セキュリティ対策を評価するための参照基準。
		解説	情報セキュリティ管理基準に基づき、業種業態の特性に合わせて項目の変更・追加・削除を行って作成する。ISMAP 情報セキュリティ管理基準等の例がある。
		関連用語	情報セキュリティ管理基準
63	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誤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	-
64	経営陣	定義	組織のパフォーマンス及び適合性について説明責任を負う個人又はグループ。（JISQ27000：2019）
		解説	-
		関連用語	トップマネジメント
65	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	-
66	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	-

67	言明	定義	被監査主体の経営陣による「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、経営陣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	-
68	言明書	定義	言明内容を関係者が共有するためにとりまとめた文書
		解説	-
		関連用語	-
69	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

70	合意	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	
71	合意された手続	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）と監査人との間で合意された手続が存在す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	AUP
72	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	-

73	COBIT(こうびっと)	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	
74	合理的保証	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	
75	個別管理基準	定義	個々の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。
		解説	個別管理基準は、監査主体が情報セキュリティ監査を行なう実際の判断の尺度である。
		関連用語	情報セキュリティ管理基準 業種業態別管理基準

76	個別品質管理担当者	定義	監査を業とする組織において監査チームが実施する個別の監査業務について品質管理を担当する者。
		解説	個別品管理担当者は監査チームと独立した者を品質管理統括責任者が指名する。
		関連用語	品質管理者 品質管理統括責任者
77	固有リスク	定義	状況から生じるか、環境に存在するリスク。
		解説	定義は「管理策がないこと、又は状況の修正が行われないこと」を前提としている。 会計監査における定義は下記のとおり「関連する内部統制が存在していないとの仮定の上で、財務諸表に重要な虚偽の表示 がなされる可能性」（リスク・アプローチに関する最近の状況:令和元年 12 月 6 日、金融庁資料） 固有リスクの例示：用いる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、経営理念等など。
		関連用語	
78	コンサルティング	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	業務又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	-

79	コントロール	定義	意図通りに人やモノなどを動かすこと又はそのための仕組み。
		解説	意図通りに人やモノなどを動かすための仕組みには、組織ルール等や技術的な制御などがある。 これらの仕組みを管理策というため、管理策を「コントロール」ということがある。このため、「人やモノなどを動かすこと」か「そのための仕組み」かは、文脈から判断する必要がある。
		関連用語	管理策 情報セキュリティコントロール

【さ】

80	再実施	定義	管理策の運用状況評価のために、監査人自らが組織体の管理策に基づく行為を実行し、コントロールの有効性を確かめる監査技法。
		解説	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	テスト
81	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
82	サイトレビュー	定義	観察
		解説	-
		関連用語	-

83	サンプリング	定義	試査
		解説	-
		関連用語	-
84	残留リスク	定義	リスク対応の後に残っているリスク。
		解説	-
		関連用語	-
85	視察	定義	観察
		解説	-
		関連用語	-
86	試査	定義	監査対象（母集団）の中からサンプルを抽出し、当該サンプルから母集団の特性又は傾向を推定し、証拠として収集する方法。
		解説	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。 いわゆる標本検査である。
		関連用語	・サンプリング ・精査
87	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	-

88	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。
		関連用語	-
89	システム監査	定義	一定の基準に基づいて情報システムを総合的に点検・評価・検証をして、監査報告の利用者に情報システムのガバナンス、マネジメント、コントロールの適切性等に対する保証を与える、又は改善のための助言を行う監査。（システム監査基準平成 30 年版）
		解説	-
		関連用語	-
90	実査	定義	監査対象である情報システムのドキュメント、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。（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	-
91	実証性テスト	定義	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検証すること。
		解説	想定されるリスクの程度の大小を確認するためのものであり、管理手続の有効性の検証とは異なる。
		関連用語	有効性監査 準拠性テスト

92	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。
		解説	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。
		関連用語	
93	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。
		解説	「非言明方式」ともいう。
		関連用語	言明方式
94	質問	定義	ガバナンス、マネジメント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又は文書で問い合わせ、説明や回答を求める監査技法。
		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	インタビュー 聞き取り
95	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

96	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	社会的合意方式において、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
97	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
98	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検証。
		解説	-
		関連用語	準拠性監査 実証性テスト
99	詳細管理策	定義	情報セキュリティ管理基準における管理策の具体的な評価項目
		解説	詳細管理策は管理策の実装・運用手段を、情報セキュリティ対策のベストプラクティスである ISO/IEC27002 の手引等に記載された内容に基づき、項目ごとに整理したものである。各項目では管理策の実装や運用の具体例に基づき、具体的対策が一般化されている。 四桁管理策とも呼ばれる。
		関連用語	管理策基準

100	情報資産	定義	情報そのもの、又は情報を扱う仕組み
		解説	情報資産は、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用語である。 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、リスクを評価する上で欠かせないステップである。
		関連用語	-
101	情報セキュリティ	定義	情報の機密性、完全性及び可用性を維持すること。 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。（JISQ27000：2019）
		解説	機密性(confidentiality)、完全性(integrity)、可用性(availability)をあわせて、各々の英語の頭文字に基づき、情報の CIA ということもある。
		関連用語	

102	情報セキュリティインシデント	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。（JISQ27000：2019）
		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
103	情報セキュリティ監査	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、リスクアセスメントに基づく適切なコントロールの整備、運用状況を、情報セキュリティ監査を行う主体が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	-
		関連用語	-
104	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。
		解説	一般基準、実施基準、報告基準からなる。 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

105	情報セキュリティ管理基準	定義	情報セキュリティマネジメントの整備、実装、運用の評価に関わる判断の尺度の根拠となる参照規格。（情報セキュリティ監査制度研究会報告書 2003 年）
		解説	JISQ27001 及び JISQ27002 に基づいて作成されている。 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ている。
		関連用語	情報セキュリティ監査基準
106	情報セキュリティガバナンス	定義	情報セキュリティ目標を維持・拡大するための組織統制の仕組み
		解説	情報セキュリティガバナンスはトップマネジメントが整備し、運用する。 情報セキュリティガバナンスの要点は、以下のとおり。 ①組織内外の環境に配慮 ②組織が情報セキュリティ目標を維持・拡大するために行う ③透明・公正かつ迅速・果断な意思決定を可能にする ④リーダーシップ、構造、プロセス
		関連用語	トップマネジメント 情報セキュリティマネジメント 情報セキュリティコントロール

107	情報セキュリティコントロール	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影響力を行使すること。
		解説	コントロールは「ルール通りに人々や機器・装置が動くよう制御する」ために用いる。 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
108	情報セキュリティ事象	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，サービス若しくはネットワークの状態に関連する事象。 （JISQ27000：2019）
		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
109	情報セキュリティにおけるコンサルティング	定義	削除
		解説	
		関連用語	

110	情報セキュリティマネジメント	定義	情報セキュリティのリスクマネジメント
		解説	リスクマネジメントは「リスクに関して組織を指揮統制するための調整された活動」のこと。 情報セキュリティマネジメントは経営陣がその責任を有する。
		関連用語	情報セキュリティガバナンス 情報セキュリティコントロール リスクマネジメント
111	情報セキュリティマネジメントシステム	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。
		解説	被監査主体が情報セキュリティのリスクマネジメントのために、情報の取扱いに関する基本方針及び実施計画の策定、計画の実施・運用、一定期間ごとの方針・実施計画の見直しを体系的に実施する活動のことをいう。 なお、「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。」は JIS Q 27000:2019 のマネジメントシステムの定義である。
		関連用語	ISMS
112	情報伝達	定義	削除
		解説	
		関連用語	
113	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	-

114	助言型監査	定義	監査対象の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	削除
		関連用語	保証型監査
115	真正性	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。（JISQ27000:2019）
		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	
116	信頼性	定義	意図する行動と結果とが一貫しているという特性。 （JIS Q 27000:2019）
		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	-
117	精査	定義	監査対象の全てを検証の対象とする証拠の収集方法。
		解説	全数検査である。
		関連用語	試査

118	脆弱性	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。（JISQ27000:2019）
		解説	脆弱性とは、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。 脆弱性は、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×脆弱性×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＝ｆ（脆弱性）
		関連用語	-
119	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	-
120	整備状況評価	定義	情報セキュリティ目的を達成するのに必要な対策が適正に計画され実装されているかの評価。
		解説	
		関連用語	運用状況評価
121	責任追跡性	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。
		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	-

122	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。 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。
		解説	-
		関連用語	実装・運用監査

【た】

123	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
124	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
125	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

126	デジタル・フォレンジックス	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	デジタル・フォレンジックスはコンピュータ・フォレンジックスやネットワーク・フォレンジックスなどがある。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	フォレンジックス
127	テスト	定義	再実施
		解説	-
		関連用語	-
128	統制活動	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	-

129	統制環境	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	-
130	統制リスク	定義	内部統制の欠陥に起因するリスク。
		解説	情報セキュリティのマネジメント又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	-
131	独立性	定義	（監査人の）独立性
		解説	情報セキュリティ監査制度においては、前後の文脈から「監査人の独立性」を単なる「独立性」ということがある。
		関連用語	
132	トップマネジメント	定義	最高位で組織を指揮し，管理する個人又は人々の集まり。（JISQ27000：2019）
		解説	
		関連用語	経営陣 情報セキュリティガバナンス

【な】

133	内部監査	定義	組織体の運営に関し価値を付加し、また改善するために行われる、独立にして、客観的なアシュアランスおよびコンサルティング活動 （内部監査人協会による）
		解説	内部監査人協会では、「内部監査は、組織体の目標の達成に役立つことにある。」としている。このことから、内部監査が「組織体の目標達成のために行われる監査」であることが分かる。 この内部監査は、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
134	内部統制	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	-

135	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	-
136	二者間の監査	定義	被監査主体の組織と、経営上も独立した監査主体の組織の二者の間で行われる監査。
		解説	監査を業とする者の立場から、二者（被監査主体、監査主体）、三者（被監査主体、監査主体、監査報告書利用者）を規定する用語である。 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、第二者監査、第三者監査は組織体の数に着目した用語概念であり、視点が異なる。第一者監査である内部監査を外部委託する場合は二者間の監査となる。取引先監査を外部委託した場合には三者間の監査となる。
		関連用語	-
137	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	-
		関連用語	-
138	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】

139	発見リスク	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	
		関連用語	固有リスク 統制リスク 監査リスク 監査リスクモデル
140	被監査主体	定義	監査を受ける対象(機関、組織又は人）。
		解説	監査における予備調査、監査業務契約の締結、監査手続きの合意を行い、監査が実施されるよう監査対象組織に対し、監査を実施する旨を告知し日程に留意する。 上記の役割から、被監査主体は経営陣又は利用者。
		関連用語	監査主体
141	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	被監査主体合意方式においては、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
142	非言明方式	定義	「実態方式」参照。
		解説	-
		関連用語	-

143	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	-
144	否認防止	定義	主張された事象又は処置の発生，及びそれらを引き起こしたエンティティを証明する能力。 （JISQ27000：2019） （注記）エンティティ：参考に記載
		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	
145	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。 監査を業とする組織においては、組織の品質管理を統括する品質管理統括責任者を設置し、個々の監査の品質管理のために個別品質管理者の氏名を行うことが求められる。
		関連用語	品質管理統括責任者 個別品質管理担当者

146	品質管理統括責任者	定義	監査を業とする組織において、組織として監査の品質管理を統括する者。
		解説	-
		関連用語	個別品質管理担当者 監査の品質管理
147	フォレンジックス	定義	デジタル・フォレンジックス。
		解説	-
		関連用語	-
148	フォローアップ	定義	フォローアップ監査。
		解説	-
		関連用語	-
149	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。
		解説	
		関連用語	フォローアップ
150	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	監査品質審査制度 倫理審査制度
151	ペネトレーションテスト	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。
		関連用語	-

152	報告書利用者	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
153	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
154	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	-
155	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	-
156	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

157	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（又は不適正である旨）の意見を述べること。
		解説	-
		関連用語	-
158	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】

159	マネジメント基準	定義	情報セキュリティ管理基準のうち、組織の情報マネジメントを評価するための判断の尺度。
		解説	ISO/IEC27001 に準拠している。
		関連用語	ガバナンス基準 管理策基準
160	モニタリング	定義	監視活動。
		解説	対象により内容が異なる。 組織マネジメントに関連して：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） IT に関連して：IT の状況を継続的に監視すること
		関連用語	

【や】

161	有効性監査	定義	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た監査。
		解説	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が、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が、組織が許容する水準以下である
		関連用語	準拠性監査
162	予備調査	定義	監査を業とする者が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、円滑かつ効率的な監査の実施を可能とするために行われる事前調査。
		解説	予備調査は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	予備的調査
163	予備的調査	定義	内部監査において企業等の内部組織が監査を行う場合、円滑な監査の実施のために、監査対象部署等の情報セキュリティ対策状況の実態を把握する調査。
		解説	内部監査を外部委託し、その委託先の監査主体が行う調査は予備調査である。 予備的調査の結果は、監査基本計画や監査実施計画に生かされる。
		関連用語	予備調査

【ら】

164	リスク	定義	目的に対して不確さの影響。 （JISQ31000:2019）
		解説	情報セキュリティのリスクは、ある脅威が，資産又は資産のグループの脆弱性につけ込み，そのことによって組織に損害を与える可能性。これは，事象の発生確率と事象の結果との組合せによって測定できる。
		関連用語	-
165	リスクアセスメント	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。（JISQ27000:2019）
		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。 （注）ISO/IEC31000：2009 では下記の用語定義がなされていた。 リスク特定：リスクを発見、認識及び記述するプロセス リスク分析：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 リスク評価：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（リスクの重大性を評価するための目安とする条件）と比較するプロセス
		関連用語	-
166	リスク対応	定義	リスクを修正するプロセス。（JISQ27000：2019）
		解説	リスク対応の選択肢として、リスクの回避、最適化、移転又は保有などがある。
		関連用語	-

167	リスク分析	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。（JISQ27000:2019）
		解説	-
		関連用語	-
168	リスクマネジメント	定義	リスクに関して組織を指揮統制するための調整された活動のこと。（JISQ27000：2019）
		解説	
		関連用語	情報セキュリティマネジメント
169	利用者	定義	報告書利用者
		解説	文脈において、単に「利用者」ということがある。
		関連用語	
170	利用者合意方式	定義	監査報告書の利用者が、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満たしている場合に、監査人が利用者の期待している水準を満たしているかどうかを監査する方式。
		解説	利用者合意方式においては、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たす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
171	倫理審査制度	定義	会員及び CAIS 資格登録/能力認定者に倫理規程違反の疑いがあるとき、その事実について審査する制度。
		解説	-
		関連用語	紛争審査制度 品質審査制度

172	レビュー	定義	閲覧
		解説	監査技法の用語として「閲覧」の代わりに用いられることがある。
		関連用語	

【参考】

173	エンティティ	定義	実体又は主体
		解説	情報セキュリティの文脈においては，情報を使用する組織及び人，他のシステム等に情報を要求する設備，ソフトウェア及び物理的媒体などを意味する。
		関連用語	可用性 機密性 真正性 責任追跡性 否認防止
174	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、又は、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。
		関連用語	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。
175	第二者監査	定義	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。
		解説	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