システム監査用語	定義	例示 ［出典］	コメント
監査とは何か			
・監査; かんさ	audit 監査人が、あるものの行為やその行為の結果としての情報を批判的に検討し、その真実性や妥当性や準拠性等を確かめ、一定の保証を与えるため利害関係者に報告することをいう。	(基) 監査対象から独立かつ客観的立場のシステム監査人が情報システムを総合的に点検及び評価し、組織体の長に助言及び勧告するとともにフォローアップする一連の活動　［旧－Ⅱ(1)］	旧システム監査基準は、内部監査の視点でまとめられており、外部監査を視野に入れると、「組織体の長に」ではなく「利害関係者に」報告することが強調される。
		(基) **システム監査**とは、専門性と客観性を備えたシステム監査人が、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、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の一類型である。［監査－前文[1]］ (基) また、**システム監査**は、情報システムにまつわるリスク(以下「情報システムリスク」という。)に適切に対処しているかどうかを、独立かつ専門的な立場のシステム監査人が点検・評価・検証することを通じて、組織体の経営活動と業務活動の効果的かつ効率的な遂行、さらにはそれらの変革を支援し、組織体の目標達成に寄与すること、又は利害関係者に対する説明責任を果たすことを目的とする。［同上］	現システム監査基準は、監査を保証型監査と助言型監査の2種類に分類している。
		監査には以下の特徴がある。 ・保証行為である ・監査基準に従って実施し、ある規準に基づいて意見が述べられる ・意見は主観的である ・意見は合理的な基礎にささえられている。 (基) システム監査人は適切かつ慎重に監査手続を実施し、保証または助言についての監査結果を裏付けるのに十分かつ適切な監査証拠を入手し、評価しなければならない。［旧－ Ⅳ3.1］ 監査人は、自己の意見を形成するに足る基礎を得るために、経営者が提示する財務諸表項目に対して、実在性、網羅性、権利と義務の帰属、評価の妥当性、期間配分の適切性及び表示の妥当性等の監査要点を設定し、これらに適合した十分かつ適切な監査証拠を入手しなければならない。［監査基準第三一3］ ・組織的かつ計画的に実施される。	(保証と証明の違いについては別項を参照) (基準と規準の違いについては別項を参照) 会計監査では、「監査基準」に従って監査が実施され、企業会計原則や金融商品取引法などの規準に基づいて意見が述べられる。 意見というものはその特性上，主観的なものである。ただし、単なる感想や思い込みや偏見であってはならないのは言うまでもない。 そこで、具体的な証拠を入手して、意見の根拠をしっかりと固めるのである。だからこそ，意見が本質的に主観的(前項参照)でも，立場の客観性は確保される。 その結果、どの監査人が監査したとしても、当然に実施すべき監査手続きを実施したなら、監査意見は同様の内容となるはずである。 監査チームのことを"one or more auditors conducting an audit"と定義しているものがある。［ISO9000　3.9.10］ しかし、実際上ひとりで監査はできるものではない。内部審査制度や様々な分野の専門家が必要なことから、"more than one"でなければ、事実上それは監査とは言えなくなる。
・基準; きじゅん	standard 何らかの行為のもととなるきまり。標準も同意。	(基) 本**基準**は、情報システムの信頼性、安全性及び効率性の向上を図り、情報化社会の健全化に資するため、システム監査に当たって必要な事項を網羅的に示したものである。［旧－Ｉ主旨］ (基) システム監査**基準**は、システム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。［旧－Ｉ.前文］	旧システム監査基準は、基準といいながら、監査実施の方法についての規範性が貧弱である。たとえば、実践規範として、本調査では何をすべきであるのか、監査人自らの判断に対する根拠を明確にするためにどのような証拠を集めるべきか等について記述されていなかったが、平成16年の改訂で、システム監査基準とシステム管理基準とに分け、システム監査基準に規範性のある条項を集め、システム管理基準に判断規準を示すようにした。 現行は左記の通り。
		(基)「**システム監査基準**」とは、情報システムのガバナンス、マネジメント又はコントロールを点検・評価・検証する業務の品質を確保し、有効かつ効率的な監査を実現するためのシステム監査人の**行為規範**である。［監査－前文[2]］	
・規準; きじゅん	criteria 何らかの判定をするためのきまり、判断手段。 判断基準であることを一般的に説明する場面でのみ規準という。 [JICPA 環境報告書保証業務指針]	(基) **システム管理基準**は、平成16年のシステム監査基準の改訂において、(中略)システム監査基準の姉妹編として策定された。その主旨は、システム監査とシステム管理の実践規範を明確に切り分けることによって、システム監査実践の独立性・客観性を明確に位置づけるとともに、監査の効率的・効果的遂行を可能にする**判断の尺度**として有効活用されることを企図するものであった。［管理－前文］	システム管理基準と「基準」という字を使っているが、内容は規準となっている。
・認証; にんしょう	certification 調査人(審査員)が、あるものの行為の結果としての言明が規準にどの程度合致しているかを判定し、その結果を格付けとして公表することをいう。	認証には以下の特徴がある。 ・証明行為である ・証明は行為者の言明に対して述べられる ・ある規準あるいは規格に照らして判定される ・規準がない事項については判定しない ・格付けをする場合が多い (基) 委託先が第三者による保証又は**認証**を受けており、当該保証等報告書に依拠し、上記手続の一部を省略する場合、当該第三者の能力、客観性及び専門職としての正当な注意について検討を行った上で、委託業務の重要性とリスクを勘案する必要がある。［監査-基準8.5.(2)］	認証は審査と密接に関係している 審査するには言明は必須である。コンサルに言明が必ずしも必須でないことと対照的である。 特定個人情報保護評価指針で個人情報保護審議会または個人情報保護審査会による点検を受けるものとすると規定している。
・認証; にんしょう	authentication, certification ログイン時などに、正当な資格者であることを証明する手続をいう。	(基) 適切な**認証**がないと、データへの改ざんや不正な参照が起きる。［追　Ⅳ3(3)②］	認証の対象が人の場合(本人認証、相手認証)と、人以外の場合(ドメイン、メッセージ、時刻など)がある。 相手認証を authentication といい、第三者認証は certification という。

システム監査用語	定義	例示 ［出典］	コメント
・認可； にんか	authorization 一定の操作する権限を与えること。	(基) 情報処理設備及びシステムの正確かつセキュリティを保った運用を実施するために、**認可**された利用者が運用システムにアクセスし、認可されていないアクセスを防止するアクセス管理ルールを作成し、関係者に周知徹底し、変更管理、定期的な見直し、特権管理などの運用を適切に行う必要がある。 ［管理－ Ⅴ．運用・利用フェーズ3.3.2(1)〈主旨〉］	通常、認証と認可はほとんど同時に実施される。
・レビュー； れびゅー	review 批判的に検討すること。	(基) ドキュメントの作成にあたり、関係者が**レビュー**していること。［管理－ X. .ドキュメント管理 1(5)〈着眼点〉①］ (基) 監査手続の適用に際しては、チェックリスト法、**ドキュメントレビュー**法 インタビュー法、ウォークスルー法、突合・照合法、現地調査法、コンピュータ支援監査技法などが利用できる。［監査-基準8.3］	
	会計監査では、限られた監査技術を用いて中位の水準の保証を付与するものを言う。		保証の程度が会計監査よりは低いというあいまいさを有するので誤解を招きやすい。
・自己点検； じこてんけん	self assessment 評価される者が自らを評価すること。	(例) 特定個人情報保護評価書（全項目評価書）のⅣその他のリスク対策①**自己点検**で②監査の前に実施されることが想定されている対策。 (基) システム監査の実施に際しては、システム監査業務の品質を維持し、さらにはシステム監査業務の改善を通じてその品質を高めるために、内部監査部門内等での**自己点検**・評価（内部評価）、及び組織体外部の独立した主体による点検・評価（外部評価）を定期的に実施することが望ましい。［監査-基準3.3］	重点項目評価書では、8.監査の中で自己点検と内部監査と外部監査が実施されているかどうかを回答する様式になっているが、自らを監査することは有り得ないので、ここは、監査が実施できない場合にはせめて自己点検だけでも実施することが求められていると考えるべきであろう。
・自己評価(査定)； じこひょうか、さてい	self assessment 同上	(基) 情報システムリスクは常に一定のものではないため、システム監査人は、その特性の変化及び変化がもたらす影響に留意する必要がある。情報システムリスクの特性の変化及びその影響を理解したり、リスクに関する情報を更新したりする手法として、例えば監査対象部門による**統制自己評価**(Control Self-Assessment: CSA)や、システム監査人による監査対象部門に対する定期的なアンケート調査やインタビューなどがある。［監査-基準7.3］	
・コントロール・セルフ・アセスメント；	contol self assessment 定義は右の通り	(定) 内部統制の有効性について、組織や業務の運営を担う人々が自らの活動を主観的に評価する手法のこと。 ［朝日監査法人 同名冊子］	自らを主観的に評価するという点で、第三者が客観的に評価する監査とは異なる。内部監査も監査客体から独立した第三者が実施する点で監査に属することとなる。
・コンサル；	consulting business etc コンサルタント業 職業的専門家が、依頼者の依頼事項に対して助言、勧告し、あるいは改善策の策定に携わることをいう。 依頼者から相談された内容を分析・診断し、課題を明らかにして解決策を示す、または主体的にかかわる業務	コンサルには以下の特徴がある。 ・保証行為でない場合が多い ・意見が述べられるが、判断規準は一般に認められたものでなくともよい ・意見は説得的であれば客観的でなくともよい ・組織的かつ計画的に実施されなくともよい ・一般的に自己の言明について損害賠償責任を負うことはない	コンサルは、依頼者のニーズに応えることが第一であるので、依頼者を満足させるという結果が大切であって、助言勧告に至る過程で意見形成のための証拠を客観的に集めることは要請されない。 この用語集では、監査の意義を分かりやすくするため、監査、審査（認証）、コンサルを対比している。
・コンサルテーション；	consultation n 相談、協議、諮問、診察 [新英和大辞典]		consultingは、「諮問の、顧問資格の」といった形容詞であり日本語の「コンサル」に対応する用語ではない。
・監査人； かんさにん	auditor 監査をする者 誰でも監査人となれるわけではなく、監査の依頼者から信頼される資質と能力が備わってなければならない	(基) システム監査の実施に際しては、その目的及び対象範囲、並びに**システム監査人**の権限と責任が、文書化された規程等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。［監査-基準1］ システム監査の品質を高め、組織体の状況やIT環境の変化等に対応して、効果的なシステム監査を実施するために、**システム監査人**は、適切な研修と実務経験を通じて、システム監査の実施に必要な知識・技能の保持及び向上に努めなければならない。［監査-基準2］ ・第三者性を求められる ・意見を報告する（言明の伝達） ・総合的な意見を求められる ・総合的意見を表明するために 高度な知識と経験を求められる 計画的・組織的な取組みが求められる	
・コーディネーター；	coordinator 対等な立場で調整する者	例えば、ベンダーとユーザーの間に立ってプロジェクトの進行を調整する役	
・ファシリテーター；	facilitater 手助けをする者	例えば会議などで、議論が円滑に進むよう調整する進行役、盛り上げ役	ファシリテーターが、主体的に意見を述べたり議論を引っ張るのではなく、メンバーの意見出しを促進することが重要

システム監査用語	定義	例示 ［出典］	コメント
・言明;	statement あるものの行為やその行為の結果としての情報を明確に記述すること	(具) 会計監査での財務諸表 　　特定個人情報保護評価制度での全項目評価書 (基) 例えば、経営陣が、取引先等からの信頼を得るために、経営者による**言明書**の範囲内で、自組織の情報システムのマネジメントが有効に機能していることのお墨付きを得たいというニーズをもっている場合、「システム管理基準」に照らして情報システムのマネジメントの状況を評価・検証し、もって保証を目的としたシステム監査が行われる。 [監査-基準3.1.(1).①]	
・保証; ほしょう	assurance 他の者の行為やその結果としての事実について一定の責任を請け負うこと。	(基) システム監査人は適切かつ慎重に監査手続を実施し、**保証**又は助言についての監査結果を裏付けるのに十分かつ適切な監査証拠を入手し、評価しなければならない。［旧-Ⅳ3 3.1］ (基) システム監査とは、専門性と客観性を備えたシステム監査人が、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1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の一類型である。[監査-前文[1]]	監査におけるassuranceの保証とは、ある事について自信、確信をもって意見をいうこと。心配、疑念を取り除くための意見を言うこと。
・保証; ほしょう	guarantee 確かだ、間違い無い（万一の時は責任を取る）と請け合うこと。 [新明解国語辞典]		guaranteeの保証とは、ある事について将来の結果、責務、状態を約束すること。例えば製品の保証、老後の保証。
・保障 ; ほしょう	security それが守られるように手段を講じること。 [新明解国語辞典]	(使) 「権利（人権・生活）を保障する」 [新明解国語辞典] (使) 日米安全保障条約	保険業界では、保証（年金）、保障（生保）、補償（損保）と使い分けているそうだ。
・証明; しょうめい	attestation 他の者の行為やその結果としての事実の有無について証拠立てて明らかにすること。	(使) 巨大なソフトウェアにバグがないことを**証明**するのは，事実上不可能である。	システム監査でも，正しくないことを証明するのはたやすい（ひとつ例を見つければよい）が，正しいことを証明するのは難しい。
	certification 証明、認可 設定した規準や要求に合格したものとして文書などで公式に認め証明すること。 [研究社　新英和中辞典]	(使) "We certify that …"-1930年頃までの米国の会計監査の報告では、このように「・・・を証明する」と表現しており、「監査証明書」(audit certificate)と称されていたが、その後この文言は削除され「監査報告書」(auditor's report)と呼ばれるようになった。	金商法監査で監査報告のことを「監査証明」と言うことがあるが、これは立法時に誤訳したまま慣用的に使われている語であって、誤解を招くので、正しくは「監査意見」と言うべきである。
・検査; けんさ	inspection 品物を何らかの方法で試験した結果を品質判定基準と比較して個々の品物の良品・不良品の判定を下し、又はロット判定基準と比較してロットの合格・不合格の判定を下すこと。 [旧JIS Z 9001]	(使) SEが外部委託したプログラムを**検査し**、一部を不合格と判定した。 (使) 個人情報保護委員会の「立入検査」	監査人も検査を行う場合があるが、あくまでも監査証拠を得るための手段であり、それ自体が目的でないことに留意したい。つまり、監査人は検体の品質を保証するわけではない。 検査は、検査する側が起点になることがある。 監査は、監査を求める者が起点になり監査する者が起点になることはない。
・試験; しけん	test サンプル又は試験片などの供試品についてその特性を調べること。 [旧JIS Z 9001]	(使) 営業所に導入したADSLの速度測定試験を行なう。	ADSLのようなベストエフォートを標榜するサービスでは，合否判定の基準値は存在しないので，「試験」となる。
・説明責任; せつめいせきにん	Accountability ある行為に責任を負う者が、その責任を果たしていることを説明すること。	(基) また、システム監査の実施は、組織体のITガバナンスの実現に寄与することができ、利害関係者に対する**説明責任**を果たすことにつながる。［旧-前文］ (基) また、システム監査は、情報システムにまつわるリスク（以下「情報システムリスク」という。）に適切に対処しているかどうかを、独立かつ専門的な立場のシステム監査人が点検・評価・検証することを通じて、組織体の経営活動と業務活動の効果的かつ効率的な遂行、さらにはそれらの変革を支援し、組織体の目標達成に寄与すること、又は利害関係者に対する**説明責任**を果たすことを目的とする。 [監査-前文[1]] (使) 監査は、発生史的には、第三者による当事者の会計責任を解除する手段として誕生したものである。 [監査の理論的考え方 鳥羽至英・秋月信二]	アカウンタビリティ、会計責任、報告責任などともいう。
・可監査性; かかんさせい	Auditability 監査を受ける体制が整い、いつでも監査人が必要とする証拠を提示できる状態。		IT成熟度のレベルにより監査が可能であるかどうかが監査人により検討される。 コントロールがどの程度整備されているか、ルールが無くて属人的な運用がされている状況なのか、規程は明文化されているが実際には使われていない状況なのか、運用はされているが見直しがされていない状態なのか、などのレベルにより可監査性は検討される。
・IT成熟度; アイティーせいじゅくど	IT maturity level (initial) (managed) (defined) (quantitatively managed) (optimizing)	代表的な定義は、CMMI(Capability Maturity Model Integration)が記述したものであり次の5段階に区分している。 ・レベル1:場当たり的な状態 ・レベル2:成功経験を反復する状態 ・レベル3:文書化標準化された状態 ・レベル4:定量的にも管理された状態 ・レベル5:最適化された状態	

システム監査用語	定義	例示 ［出典］	コメント
・指摘；	point out, indication 情報システムリスクの存在を明示すること（法規・公的基準・社内規準等に準拠していない事象及びシステム監査人の判断基準で情報システムリスクが存在する事象であると判断したものを明示すること）［佐竹博利］	(基) **指摘**事項；システム監査人が自らの判断基準に基づき指摘した問題点　［旧Ⅱ(10)］ (具) OSに最新のパッチが当てられていないので，セキュリティホールが攻撃される可能性があると**指摘**した。 (基) 例えば、経営陣が、自組織のシステム開発管理に重大な不備があるのではないかと不安に思っており、もし不備があればそれを**指摘**してもらい、改善の具体的な方策を知りたいというニーズをもっている場合、「システム管理基準」に照らして現状のシステム開発管理の状況を評価・検証し、指摘事項とともに改善提案を行う、助言を目的としたシステム監査が行われる。［監査-基準3.1.(1).②］	
・勧告；	recommendation 提言ともいう （proposal） 現状の被監査部門の置かれた情報システム環境から考えて社内の仕組みや基準・規定を変更する等、全社的な対応が必要であるとシステム監査人が判断した場合にその旨要請すること ［佐竹博利］	(基) 改善**勧告**；改善事項を緊急性を要する事項とその他の事項に分けて整理した勧告 ［旧-Ⅱ(12)］ ＊ **改善勧告**の記載に際しては、**重要改善事項**と**通常改善事項**等、あるいは緊急改善事項と中長期改善事項等、その重要度や緊急度に区別して記載すること。あわせて、改善に責任を有する担当部署を明確にする必要がある。 ＊ 改善勧告の記載に際しては、改善事項のみならず、改善によって期待される効果等を記載することが望ましい。 ［監査-基準11.4.(2).例2］	勧告は、定義にあるように監査を受けた側が必ずアクションを取らねばならない指摘をすることであるので厳しい表現である「勧告」という用語を使う。 内部監査として実施するシステム監査の場合は、指摘・指導・提言という表現がなじみやすいかもしれない。外部監査人が経営者に表明する場合は、「勧告」という表現で違和感はない。
・改善勧告；	同上	(基) 監査報告書には、実施した監査の対象、実施した監査の概要、保証意見又は助言意見、制約又は除外事項、指摘事項、**改善勧告**、その他特記すべき事項について、証拠との関係を示し、システム監査人が監査の目的に応じて必要と判断した事項を明瞭に記載しなければならない。 ［旧-Ⅴ3］	旧システム監査基準にあるように、緊急改善と通常改善とに分けて監査報告書に記載することが一般的である。
・指導；	guidance 助言ともいう 指摘事項が発生しないまたは発生しにくくする方法のうち被監査部門で対応可能なものを示すこと　［佐竹博利］	(基) 5. 監査報告に基づく改善指導（フォローアップ） システム監査人は、監査の結果に基づいて所要の措置が講じられるよう、適切な**指導**性を発揮しなければならない。 ［旧-Ⅴ5］ (基) 監査報告書の発行前に、監査の**指導**機能により、監査対象部門の自発的な取り組みによって発見された不備への改善が実施される場合もあるが、それはフォローアップとは区別されなければならない。［監査-基準12.1.(1)］ (具) 水滴の落下対策として，IT機器をエアコンの真下から移動させるように**指導**した。	
・改善指導；	follow up 改善勧告したことが、その後勧告通りに実施されたかどうかを監査人が確かめること	(基) システム監査人は、システム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及び**改善指導（フォローアップ）**までの監査業務の全体を管理しなければならない。 ［旧-Ⅳ4］	

システム監査用語	定義	例示 ［出典］	コメント
監査実施に関する用語			
・監査目的; かんさもくてき	**監査の目的とは、監査を実施することにより目指そうとしているものである。**監査目標などと対比して特に監査目的という場合には、監査がその存在理由として有している究極の到達点を指すものとする。 ただし、「目的」という語そのものは、目指すところとか目当という意味の普通名詞であるので、監査報告書の中でも、一般用語として「目的」という言葉を使うことは問題ないとすべきであろう。	(基) システム監査は、…情報化社会の健全化に資することを**目的**とする。［旧-前文］ (基) 監査手続は、それぞれ単独で実施される場合もあるが、通常は、一つの**監査目的**に対して複数の監査手続の組み合わせによって構成される。[監査－基準8.5] (使) (A社の)情報システムは有効に機能しているか。	監査目的、監査目標、監査テーマという用語には、明確な定義上の違いがないように思われる。三つの用語の間の関係についても曖昧だ。このような定義が必要なのは、システム監査が様々な目標を持っているためであると考えられる。 監査目的という語は、旧システム監査基準の冒頭で使用されている。システム監査基準を尊重して、最も抽象的な上位概念と位置付けることとする。
・監査目標; かんさもくひょう	**監査を実施する際に、監査目的の中から選ばれて、より具体的に規定された当面の達成すべき目当をいう。**	目標とは、「評価を行おうとする事項」といった監査対象ではなく、例えば、「安全性が確保されている」といった監査対象について達成されるべき命題である。 (使) 最近更新したA社の販売管理システムは有効に機能しているか。	以上のように、監査目的を上位概念と定義したので、監査目標は、監査目的と監査テーマの間に位置付けることとする。監査実施の局面で達成しようとする目当てのことを監査目標と考える。 システム監査は固定した目的をもつ監査ではない。 監査が求められる事情や監査対象などにより、その目的は変るものである。監査を実施するにあたり、いくつかの監査目的の中から選ばれて具体的に記述されたものを監査目標という。
・監査要点; かんさようてん	audit objective システム監査を実施するに際して、監査目標を具体的に記述したものをいう。 **監査目標を達成するために、各監査項目について立証すべき命題を監査要点という。**	(使) (最近更新したA社の販売管理システムで)要求定義を満たす仕様が実現できているか。 (基) (情報戦略は)情報システムの企画、開発、運用及び保守業務に係る標準化の方針を明確にしているか。 [旧-Ⅵ1(2)]	監査要点が、監査での専門用語であり、監査テーマや監査ポイントは、意義を厳密に定義することなく使われている一般的な用語である。特段の意味がないなら、会計監査で定着している「監査要点」を使い、システム監査人の認識を統一することが望まれる。 旧システム監査基準では、その大半を占める実施基準が監査要点の記述に終始しているため、監査要点を羅列したものが監査基準だという誤解を生みやすくなっている。
・監査テーマ;	監査要点(前項)に該当する。 (監査に馴染んでいない人に対しては、監査要点というよりは、監査テーマといった方が理解しやすいので用いる。)	(使) 1.監査目的　信頼性の高いシステム開発に向けた整備・改善を行う 2.**監査テーマ**　システム開発業務、設計段階のレビュー方法の妥当性　他 3.監査項目　　・・・ 「システム監査個別計画書(作成例6)」	監査目標が、一連の監査の統一テーマであるとするなら、監査テーマは、個別テーマと位置付けることができる。 ただし、監査目標の意味で使われる場合もあり、あいまいになりがちなので、監査目標あるいは監査要点という用語を使い分けることが望まれる。 作成例をみると、監査目的は監査目標の、監査テーマは監査要点の意味で用いられていることがわかる。
・監査ポイント;	監査要点と同義語である。		
・監査対象; かんさたいしょう	subject matter 監査対象とは、監査目的によりすでに限定されたをいう。	(基) システム監査人は、**監査対象**の領域又は活動から、独立かつ客観的な立場で監査が実施されているという外観に十分に配慮しなければならない。[監査-基準4]	監査対象と監査範囲は、監査人により混乱して使われることが多く、監査報告書などを作成する段階で意味を峻別して使うことが望まれる。
		(具) 全社、本社、製造部門、営業部門など 企画、開発、運用、保守の各業務 ソフトウェア、ハードウェア、施設、ネットワークなど 分散システム、EUC、エンベデッドシステム、自治体など	組織で区分する場合、 業務で区分する場合、 情報資産で区分する場合 システム手法やシステム環境で区分する場合 など様々な取上げ方があり、それらを組み合わせる場合が多い。
・監査範囲; かんさはんい	scope of auditing, (extent of tests) 監査対象のうち選択した監査手続を適用する部分を監査範囲という。	(具) たとえば、監査対象がソフトウェアである場合に、監査範囲は本社第一営業部の顧客管理ソフトに絞られるといったことである。 (基) システム監査の実施に際しては、その目的及び**対象範囲**、並びにシステム監査人の権限と責任が、文書化された規程等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。[監査-基準1]	監査を受ける客体を監査対象といい、監査の実施段階で実際に監査手続が適用される部分を指して監査範囲というと解釈すると、分かりよいのではないか。 左は、「監査範囲」の用例ではないが、「対象」と「範囲」が明確に区分されていない例として掲げる。
・監査項目; かんさこうもく	実際の監査の場面で、選択された監査手続が実施される単位である。	(具) 情報システムを構成するハードウェア、ソフトウェアといった情報資産単位、企画・開発・運用・保守といった業務単位、あるいは、経営者・システム管理者・利用者といった単位など様々な単位で選ぶことができる。 (具) 会計監査では、現金勘定、棚卸資産勘定、売上高勘定などである。	会計監査では勘定科目として一義的に定義できるが、システム監査では監査目標が様々であるので監査項目は一義的には定義できない。
		(基) (2)実施基準(191項目)　実施基準は、システム監査の対象である情報システムの企画、開発、運用及び保守業務並びに共通業務に対する**監査項目**を定めている。 [旧-Ⅲ基準の構成]	旧システム監査基準では、基準の構成を説明するところで監査項目という表現を使っているが、これは、「情報戦略は、経営戦略との整合性を考慮して策定しているか」に始まる監査で立証すべき命題であるので、監査要点と記述する方が誤解を招かないと思われる。
		(基) 時々の関連技術動向、関連法令、及び社会規範などを考慮し、それらを反映した詳細な**サブコントロール項目**を策定することが望ましい。 ・・・システム管理基準においても情報セキュリティの確保に関連する項目が挙げられているが、それぞれの**項目**について、情報セキュリティ管理基準を活用して監査を実施することが望ましい。[旧-前文]	現行のシステム管理基準では、監査項目という用語は避けられている。

システム監査用語	定義	例示 ［出典］	コメント
監査手続に関する用語			
・監査手続; かんさてつづき	auditing procedures 監査証拠を求めるために適切な監査技術を、実施する時期、範囲、担当者などを考慮して選択し、一定の手順で実行に移すこと。	(基) システム監査人は適切かつ慎重に**監査手続**を実施し、保証又は助言についての監査結果を裏付けるのに十分かつ適切な監査証拠を入手し、評価しなければならない。［旧-Ⅳ3 3.1］ (基) システム監査人は、実施した**監査手続**の結果とその関連資料を、監査調書として作成しなければならない。［Ⅳ3 3.2］ (使) 知的財産権に関する法規が遵守されているかが監査目標の場合:監査範囲をパソコンにインストールされているパッケージソフトに限定し→ソフトの購入契約書を閲覧し、パソコン画面でソフトのシリアルナンバーを確かめ、担当者に違法コピーをしていないことをヒアリングする。	会計監査の定義が、システム監査でも、そのままに使える。
・監査技術; かんさぎじゅつ	auditing technique 監査証拠を求める手段である。	(具) 質問、視察、閲覧、突合、比較、分析、コンピュータ利用監査技法等がある。	システム監査でも、会計監査と同様の定義が当てはまる。ただ、監査技術の例示の中から、帳簿突合、勘定分析、財務分析的手続は除かれ、コンピュータ利用監査技法(テストデータ法、ITF…)などが追加されるだろう。
		(定) 記録や文書の閲覧、観察／システム運用現場視察、質問、再計算／CAAT、再実施／CAAT、分析的手続 ［JICPA　IT委員会報告第3号］	突合や照合は、記録や文書の閲覧に含まれる。 [JICPA　監査基準委員会報告書第31号 26項]
・CAAT;(CAATs) ・コンピュータ利用監査技法;	Computer-assisted audit techniques コンピュータを監査の用具として利用する監査手続用のアプリケーションである。 [国際会計士連盟(IFAC)　専門用語集]		
・監査証拠; かんさしょうこ	audit evidence 監査要点を客観的に立証する資料であって、監査人の意見形成の基礎となるもの。	(基) システム監査人が作成した監査報告書は、**監査証拠**に裏付けられた合理的な根拠に基づくものでなければならない。［旧-Ⅴ2］ (基)システム監査人は適切かつ慎重に監査手続を実施し、保証又は助言についての監査結果を裏付けるのに十分かつ適切な**監査証拠**を入手し、評価しなければならない。［旧-Ⅳ3 3.1］ (使) 某市販パッケージをインストールした複数台のパソコンで，シリアルナンバーが同一であった。	意見の裏付けの根拠となるもの
・監査証跡; かんさしょうせき	audit trail 監査要点を立証する監査証拠のうち、ログで監査人のみが読出しできるものをいう。	(基) ログ等の**監査証跡**を確保できるよう考慮すること。 [管理-Ⅲ. 開発フェーズ2(1)<着眼点>⑬] (具) 監査人だけが読出し参照可能なアクセスログやウイルス対策ソフトのバージョンアップ履歴ファイル (使) システム監査ではログを利用した運用監査証跡やそれに類する追跡能力のある証跡も含めて**監査証跡**とし、これを活用することが現実的であると考えられる。 [情報システム監査　吉田洋]	一般的な監査証拠の意味で監査証跡と言うのは間違っている。監査証跡は極めて情報システム独自の専門用語であるので、その違いを強調する場合にのみ使うべきである。 ログは証跡(証拠)であるが、監査証拠として使える場合に監査証跡となる。どのログでも監査証跡となるわけではない。
・事前協議; じぜんきょうぎ	(pilot test) preliminary arrangements 監査契約を締結する前に、監査依頼者と監査人が、監査の依頼事項を確認し監査目標を定める手続である。	(基) システム監査を効果的に実施し、監査の実施に係るトラブルを避け、監査実施へ協力を得るため、監査の実施に先立って、システム監査人に関する権限と責任を組織体の内部監査規程等によって明確にし、周知しておくこと、あるいは外部の専門家に依頼する場合は、契約に先立ち十分な**事前協議**を行うことが重要である。[監査-基準1.主旨]	監査の依頼事項を確認し監査目標を定める手続は、システム監査では不可欠かつ重要であるので、予備調査や本調査とは別に用語の解釈のレベル合わせをしておくことも必要と考えられる。 特に、予備調査との違いを明確にしておく意義は大きい。
・予備調査; よびちょうさ	preliminary review 本調査を始める前に、問題点の背景や概要を知り、監査計画を立案するための調査をいう。	(基) **予備調査**によって把握するべき事項には、例えば、監査対象(情報シス テムや業務等)の詳細、事務手続やマニュアル等を通じた業務内容、業務分掌の体制などがある。[監査-基準8.2.(1)] (具) 監査対象のシステムに関係する組織図，経営計画書やネットワーク構成図の入手、情報システム部門長へのインタビュー　等	システム監査の場合も、監査計画との関係で予備調査は定義すべきであろう。
・本調査; ほんちょうさ	audit 実地に証拠を入手して既知の問題点を確認し、監査人独自の立場から新たな問題点を発見する過程。	(基) **本調査**は、監査の結論を裏付けるために、十分かつ適切な監査証拠を入手するプロセスをいう。十分かつ適切な監査証拠とは、証拠としての量的十分性と、確かめるべき事項に適合しかつ証明力を備えた証拠をいう。 [監査-基準8.2.(3)] (具) システム運用者に対するインタビュー、外部委託する範囲の明確化状況の確認のための契約書閲覧　等	
・監査計画; かんさけいかく	audit plan 右の通り	(基) システム監査人は、実施するシステム監査の目的を効果的かつ効率的に達成するために、監査手続の種類、実施時期、及び適用範囲等について、適切な**監査計画**を立案しなければならない。監査計画は、状況に応じて適時に変更できるように弾力的なものでなければならない。 [監査-基準6]	

システム監査用語	定義	例示 ［出典］	コメント
リスクに関する基礎用語			
・脆弱性; ぜいじゃくせい	vulnerability 情報システムから得られる効用に伴って不可避的に発生し内在化する欠陥 ［松田貴典『情報システムの脆弱性』］	(基) IT は利用者に対し業務処理の効率化・有効化をもたらすが、管理しなければ企業価値に影響を与えるほどの潜在的な**脆弱性**を持つことになる。[追　Ⅱ2(1)②b] (具) メールとコンピュータ・ウィルス、 インターネットの利用と内部データの不正流出 等々	メールには電話やFAXにない効用があるが、コンピュータ・ウィルスに犯されるという欠陥がある。
・リスク分析; りすくぶんせき	risk anarysis 情報システムを利用することに伴って発生する可能性のあるリスクを洗い出し、その影響度合を分析すること　［Ⅱ(9)］	(基) ハードウェアに関する**リスク分析**を計画的に行っていること。 [管理−Ⅴ．運用・利用フェーズ6.6.2(3)<着眼点>①] (基) **リスク分析**の結果に基づき、リスクに対応できる環境条件を明確にしていること。 [管理−Ⅴ．運用・利用フェーズ6.6.2(3)<着眼点>②]	
・リスクマネジメント; りすくまねじめんと	risk management リスク分析やリスク評価を行い、情報システムに内在するリスクの予防、軽減、分散等のためにセキュリティシステムを構築し、その効果的運営を通じて組織体の安全を図る一連のプロセス。	(使) データセンターの**リスクマネジメント**を行ない，火災によるリスク対策として損害保険に加入することにした。 (基) **リスクマネジメント**の対応力を高めるため、経営陣は関係者に周知徹底する必要がある。 [管理−Ⅰ．ITガバナンス9(4)<主旨>]	
・リスクへの対応;	risk treatment リスクの許容 リスクの軽減 リスクの転嫁 リスクの除去	(具)　まれにフリーズするが安価なOSの採用 セキュリティ対策(リスク対策) 保険、資源の移動(アウトソーシングなど) 接続の遮断、処理の停止	セキュリティ対策を必要としない状況である。 　セキュリティ対策がうまくいかないときに、リスクの転嫁を考えるのか、リスクの転嫁はセキュリティ対策の前にあるのか、リスクの除去は軽減、転嫁ができない場合に採るものか・・・はたして順番は？
・リスク; りすく	risk ･脅威が実現する蓋然性 。 ･災害、障害、不正や犯罪が起る可能性	(基) システム監査は、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適切に整備・運用されていることを担保するための有効な手段となる。[旧−前文] (基) 情報システムの導入に伴って発生する可能性のある**リスク**を分析すること。[旧−Ⅱ2(5)] (基) システム監査人は、システム監査を行う場合、**情報システムリスク**、及びシステム監査業務の実施に係る**リスク**を考慮するリスクアプローチに基づいて、監査計画を策定し、監査を実施しなければならない。[監査−基準7]	リスクは、脅威が発生する確率と発生した場合の損失又は被害の大きさの関数として評価される。
・脅威; きょうい	threat ･情報システムに被害や損失を及ぼすおそれがあるもの ･災害、障害、不正や犯罪など	(基)事業継続に関わる**脅威**が発生しても、迅速かつ確実に事業継続計画に定められた手続を実行できるようにする。 [追　付2−1 5(3)] (具) 地震，HDDの故障，コンピュータウイルス	
・損失; そんしつ	loss 利益を失うこと。金銭面や用役面で使われる。	(使) システムダウンにより顧客獲得の機会を失うことは損失にあたる。 (基) 情報システム部門長は、情報システムに係る被災の程度に応じた業務の復旧の重要性及び緊急性を明確にするため、情報システムの停止等によって組織体が被る**損失**について利害関係者を入れ、分析する必要がある。 [管理−Ⅷ.事業継続管理1(2)<主旨>]	「損失」と「被害」は，システム監査上は，厳格に区別しなくても差し支えない場合が多いと考える。
・被害; ひがい	damage 害されること。物質面や精神面で使われ	(使) 火災により通信ケーブルが**被害**にあった。 (基) 情報システムの停止、破壊等による**被害**を最小にするために、建物及び関連設備は、想定されるリスクを回避できる環境に設置する必要がある。 [管理−Ⅴ．運用・利用フェーズ7(1)<主旨>]	
・災害; さいがい	disaster 自然災害：地震、風水害、落雷など	(具) 静電気、ノイズ、振動、錆、粉塵、噴火、塩害、動植物によるもの (基) 情報システム部門長は、**自然災害**等のリスク及び情報システムに与える影響範囲を明確にすること。 [管理−Ⅷ.事業継続管理1(1)<主旨>]	人災や事故は災害ではなく障害に含める。
・障害; しょうがい	fault、failures **意図的でないもの**をいい 人災事故：火災、停電など ハードウェアでは老朽化、故障 ソフトウェアではバグ ネットワークでは大規模通信障害 データでは消失・漏洩 人にはエラーがある。	(基)情報システムの**障害**対策を考慮して設計すること。 [旧−Ⅲ2(10)] (具) 電波障害、交通事故、爆発 損傷、紛失、誤動作、停止 プログラムミス、想定誤りによる設計ミス チェーンメール、切断 文字化け 勘違い、無知、無能、モラルハザード	システム監査上は，軽微なもの（顕在的かつ潜在的に）は除外して差し支えない。
・不正、犯罪; ふせい、はんざい	irregularities,crime **意図的なもの**をいい、 ハードウェアでは損壊、盗難 ソフトウェアでは不正使用 データでは改竄・消去・盗用 ネットワークでは踏み台、なりすまし 人では破壊活動などがある。	(基) データの入力の誤謬防止、**不正**防止、機密保護等の対策は有効に機能すること。[旧−Ⅳ3(4)] (具) 持ち出し、侵入、改造、無権限使用、動作阻害 ウィルス、違法コピー、プログラム書換 窃盗、横流し 否認、サイバーテロ、DOS攻撃、不正アクセス 妨害、風説流布、非難中傷、暴露	情報システムに関する法律や判例が成熟するまでは、システム監査においては、違法である場合に限定せず，公序良俗に反するものも含めるべきであろう。 　内部統制や会計監査ではfraudが不正として使われることが多いが、fraudは人を欺して財産や権利を奪うこと（詐欺、欺瞞）という意味合いが強いので、愉快犯や自己顕示目的のクラッキングやサイバーテロを含む情報システムでの不正にはfraudは適切ではない。

凡例

例示のコラムには、出典を[ ]で示している。アラビア数字ではじまるものは、システム監査基準の章節を表している。

略号は、それぞれ、(具);具体的な事例,(使);文章の中での使用例,(基);システム監査基準またはシステム管理基準での記載例、(定);他の文献での定義を意味する。
なお、(基)には、平成30年4月改訂版のシステム監査基準とシステム管理基準の両者を引用している。出典に[監査]とあるのはシステム監査基準、[管理]とあるのはシステム管理基準である。。旧システム監査基準の場合は[旧]と表示した。

JICPAは日本公認会計士協会のことである。