No	用語	日本語読み	英文名	定義（又は説明）	解説	source	区分1	区分2
1	ITIL	アイチル	Information Technology Infrastructure Library	ITサービスマネジメントにおけるベストプラクティスをまとめたもの	ITILは、英国政府機関OGC（Office of Government Commerce：商務局）がITサービスマネジメントに関するベストプラクティスをまとめたガイドラインである。具体的には、ITシステムの運用領域に関してデファクトスタンダード（事実上の標準）として活用されている書籍群からなる。最新の書籍群はITIL V3である。 ITIL V3では、サービス・ライフサイクルに沿った書籍５冊の構成となっており、ITサービスを提供する組織は、このサービス・ライフサイクルに沿ってサービス提供を管理することが必要とされる。サービス・ライフサイクルでは、次の５つの各段階を実践することにより、より良いサービスの実現を目指すものである。 サービスストラテジ（戦略）→サービスデザイン（設計）→サービストランジション（移行）→サービスオペレーション（実施）→継続的サービス改善→（サービスストラテジ） 【ITIL V3の概要：itSMF JAPAN：ITIL V3ファンデーション・ハンドブック】 次の5冊。 ・「サービスストラテジ」：市場の定義、提供内容の開発、戦略的資産の開発、実行の準備、サービス・ポートフォリオ管理、需要管理、財務管理 ・「サービスデザイン」：サービスの設計、サービス・カタログの管理、サービスレベル管理、キャパシティ管理、可用性管理、ITサービス継続性管理、情報セキュリティ管理、サプライヤ管理 ・「サービストランジション」：移行の計画立案およびサポート、変更管理、サービス資産管理および構成管理、ナレッジ管理、リリース管理および展開管理、サービスの妥当性確認およびテスト ・「サービスオペレーション」：イベント管理、インシデント管理、要求実現、問題管理、アクセス管理、サービスデスク機能、技術管理機能、IT運用管理機能、アプリケーション管理機能 ・「継続的サービス改善」：７ステップの改善プロセス、サービス報告、サービス測定	新規		
2	ITF法	アイティエフホウ	Integrated Test Facility	監査対象ファイルの中にシステム監査人用の口座を作り、その口座に各種の操作をして処理の正確性を確認する方法のこと（システム監査技術者育成カリキュラム）	ITF法（Integrated Test Facility：統合テスト法）は、別称ミニカンパニー法とも呼ばれ、システムに架空の口座（ミニカンパニー）を設け、実稼動中にテストデータを流し、その結果をあらかじめ手作業にて得られた正しい結果と照合するという方法であり、オンラインシステムをテストする技法である。 実稼動中にテストデータを実データと共に入力して処理するため、いずれかの段階でテストデータを除去する必要がある。テストデータが業務処理および記録等に影響を与えないように留意する。	現行用語集		
3	ITガバナンス	アイティガバナンス	IT governance	企業が、ITに関する企画・導入・運営および活用を行うにあたって、すべての活動、成果および関係者を適正に統制し、目指すべき姿へと導くための仕組みを組織に組み込むこと、または、組み込まれた状態のこと（現経済産業省のIT経営ポータル）	ITガバナンスは、『コーポレートガバナンス』から派生した概念であり、、『コーポレートガバナンス』の一環として経営効率を増進させるために行うもので、IT効果の最大化、ITリスクの最小化、コンプライアンスを実現するための仕組みまたは体制のことである。 1999年頃は、通商産業省はITガバナンスを「企業が競争優位性構築を目的に、IT戦略の策定・実行をコントロールし、あるべき方向へ導く組織能力」と定義していた。ITガバナンス協会では、ITガバナンスは「取締役会および経営陣の責任である。それは企業ガバナンスの不可欠な部分で、リーダシップおよび組織的な構造、および組織のITがその組織の戦略および目的を保持し拡張することを保証するプロセスからなる」と定義している。日本監査役協会では、ITガバナンスを「『コーポレート・ガバナンス』の一側面であって、企業価値の向上を目指しつつ企業の社会的責任を果たし、かつ事業継続と業務の有効性及び効率性を達成するために、ITの戦略的利活用とそれに伴うリスクに対して、全社的に対処するための取締役の職能と責任の明確化、及びそれを独立した立場から監視・検証する監査役の職能と責任を通じて、企業グループ全体としてのIT利活用の適切な推進とIT利活用をめぐるリスク対処を効果的にするための仕組みないしは活動をいう」と定義している。	現行用語集	基準	シラバス
4	IT業務処理統制	アイティギョウムショリトウセイ	IT application control	業務を管理するシステムにおいて、承認された業務がすべて正確に処理、記録されることを担保するために業務プロセスに組み込まれたITに係る内部統制のこと（経済産業省「システム管理基準　追補版」（平成19年3月30日）第Ⅰ章２．用語）	個々のアプリケーション・システム（業務処理システム）において、開始された取引が承認され、漏れなく重複なく正確に入力され、処理・出力されることを確保するために行う統制活動である。『全般統制』と対比される考え方であり、アプリケーション・コントロールとも呼ばれる。情報システムのコントロールは、情報システムの『安全性』・『信頼性』・『効率性』に影響を与えるリスクを適切に処理する仕組みのことであり、一般には設備面・技術面・運用管理の面から設計されている。このコントロールは、エディットテスト、合計、照合調整、識別、過誤・不明・例外データの報告等から構成される。 日常の業務活動は、業務処理から生じる情報、業務を行う人の活動、及び情報の入出力、処理等をコンピュータ上で行うアプリケーション・システムが組み合わさって機能している。 システム監査人は、各『ビジネスプロセス』の内容を理解し、ITのコントロール目標が設定されているか、目標と実態を比較するチェック体制が整備されているかなどにより、業務処理統制を確認する。また、アプリケーション・システムは、各業務システムの『ビジネスプロセス』ごとに作成されていても他の業務と連携している場合が多いので、例えば原価計算について会計処理だけでなく在庫システム、 販売管理システム、売掛金管理システムおよび関係するシステムとのインタフェース処理を確認し分析する必要がある。	現行用語集	基準	

No	用語	日本語読み	英文名	定義（又は説明）	解説	source	区分1	区分2
5	IT全社的統制	アイティゼンシャテキトウセイ		企業の統制が全体として有効に機能する環境を保証するためのITに関連する方針と手続等、情報システムを含む『内部統制』のこと（経済産業省「システム管理基準　追補版」（平成19年3月30日）第Ⅰ章２．用語より）。	連結グループ全体としての統制を前提とするが、各社、事業拠点ごとの全体的な『内部統制』をさす場合もある（「システム管理基準　追補版」）。 金融庁企業会計審議会意見書「実施基準」では、企業集団全体に関わり連結ベースでの財務報告全体に重要な影響を及ぼす『内部統制』を「全社的な内部統制」としている。この「全社的な内部統制」を評価するに当たっての評価項目の例を「内部統制の基本的要素」である「統制環境」、「リスクの評価と対応」、「統制活動」、「情報と伝達」、「モニタリング」、「ＩＴへの対応」毎に示しているが、この評価項目うちの「ＩＴへの対応」の概念を「システム管理基準追補版」では、「ＩＴ全社的統制」としたものである。 具体的には、経営戦略に沿った情報戦略や情報システム計画が実施されるようにする為の統制であり、行われない事によるリスク、すなわち財務報告に与える影響を回避するための統制である。情報戦略や情報システム化計画を決定する委員会やそこでの手続きなどが該当する。		基準	
6	IT統制	アイティトウセイ	IT control	ITを利用した情報システムに対する『内部統制』のこと（「システム管理基準　追補版」（平成19年3月30日）第Ⅰ章２．用語より）	「財務報告に係る内部統制の評価及び監査の基準並びに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の設定について（意見書）」（平成19年2月15日企業会計審議会）の「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」では、「ITへの対応」の一つとしての「ITの統制」を「ITを取り入れた情報システムに関する統制であり、自動化された統制を中心とするが、しばしば、手作業による統制が含まれる」と説明している。 「システム管理基準　追補版（財務報告に係るIT統制ガイダンス）」（平成19年3月30日経済産業省）では、「ITの統制」を「IT統制」と呼び、ITを利用した情報システムの内部統制と説明し、具体的な統制内容を『IT全社的統制』、『IT全般統制』、『IT業務処理統制』の３つに分類している。			シラバス
7	アクセスコントロール	アクセスコントロール	access control	情報の使用を適切な資格を持つ人に制限するための方策のこと（独立行政法人　情報処理推進機構HPより引用）	物理的な制御としては、不正侵入を防止するための入退室管理、防犯設備、媒体機器への施錠等がある。論理的なアクセスコントロールとしては、ファイルやデータベース、ネットワークに対するユーザの不正なアクセスを防ぐための全ての対策が含まれる。 通常、アクセスコントロールでは、最初にユーザのリソース使用権限の認証を行い、使用権限の有無を確認する。これにより不正使用の確認ができる。次に、アクセス要求種別がアクセス権の許容範囲かどうかを確認し、許容範囲内ならアクセスを許可する。また、アクセスの許可／不許可にかかわらず、アクセスログを記録し、随時または定期的にアクセス状況を分析できるようにしておくことも必要である。	現行用語集		
8	アサーション	アサーション	acertion	経営者が自社の財務諸表は一定の要件を従属して、適正に作成されている旨の意思決定をすること	アサーションは、「経営者の主張」として日本公認会計士協会・監査基準委員会報告書第28号「監査リスク」（平成17年3月31日制定、平成18年3月30日改訂）で説明されている用語であるが、システム監査人はITに関わる監査の専門家として、内部統制に絡んで、財務諸表監査に参画することもあり、アサーション（「経営者の主張」）の意味を理解しておくことが望ましい。 アサーションに関する例示（監査基準委員会報告書第31号「監査証拠」（平成17年3月31日制定、平成18年3月30日改訂）第17項） （1）監査対象期間の取引や会計事象に係るアサーション ①発生、②網羅性、③正確性、④期間帰属、⑤分類の妥当性 （2）期末の勘定残高に係るアサーション ①実在性、②権利と義務、③網羅性、④評価と期間配分 （3）表示と開示に係るアサーション ①発生及び権利と義務、②網羅性、③分類と明瞭性、④正確性と評価			
9	暗号	アンゴウ	encryption	情報の機密性を保持するために、一定の規則に従って文章・数などを他の表現に変えて、その規則を知らない人には元が何かは判らなくすること	暗号技術は情報を第三者から読めなくする機密性のほか、本人が作製した文書であることを証明する認証や、文書が改ざんされていないことを証明する完全性を確保するための機能を併せ持っている。 また、元の状態に復元することを「復号」という。 現在広く使われている暗号の方法（暗号方式）を大別すると秘密鍵暗号方式と公開鍵暗号方式とがある。さらに秘密鍵暗号方式と公開鍵暗号方式を組み合わせたハイブリット暗号方式も利用されている。秘密鍵暗号方式は、送信側、受信側で予め同一の暗号／復号のための鍵を用意して利用する方式である。 公開鍵暗号方式は、受信側で秘密鍵と公開鍵を用意し、公開鍵を送信側が入手できるように公開する。送信側は、予め受信側から公開された公開鍵を使用して暗号化し、データを送信する。受信側では、暗号化されたデータを自分の手元においた秘密鍵で復号する方式である。公開鍵方式は、第三者認証機関が発行する電子証明書や電子署名に広く用いられている。 暗号化技術の主なものとして、秘密鍵暗号方式に用いられるDES（Data Encryption Standard）と公開鍵暗号方式に用いられるRSA(Rivest-Shamir-Adlemanの３人の頭文字)がある。	現行用語集		
10	安全性	アンゼンセイ	safety	情報システムの稼働を阻害するリスクに対して、情報システムが保護され、安定かつ正常に稼働すること	旧システム監査基準（平成8年1月30日改訂）では、用語の定義で安全性を、情報システムの自然災害、不正アクセス及び破壊行為からの保護の度合としている。JISでは、利用者が指定された利用の状況で、人、事業、ソフトウェア、財産又は環境への害に対して、容認できるリスクの水準を達成するためのソフトウェア製品の能力（JIS X 0129-1）と定義している。 最近ではネットワークの普及により、ウイルスやハッキングによる被害や外部からの不正侵入に対する安全対策の重要性が増しているため、ネットワークに対する安全性が話題となっている。ネットワーク以外のリスクとしては、コンピュータそのものによるハードウェアの不良、火災・水害、地震・停電、ハード・ソフトの設置環境、ソフトウェアのバグ、オペレーションミスなどの内部・外部の要因が掲げられる。	現行用語集		シラバス

No	用語	日本語読み	英文名	定義（又は説明）	解説	source	区分1	区分2
11	EA	イーエー	Enterprise Architecture	組織の全体最適化の観点より、業務及びシステム双方の改革を実践するために、業務及びシステムを統一的な手法でモデル化し、改善することを目的とした、設計・管理手法のこと	EAは、1987年にJohn A.Zachmanが提唱した「情報システムを設計するための枠組み」を基礎としており、1992年に情報システムだけでなく組織全体を対象とする概念に拡張された。米国では、1996年のIT投資管理改革法に基づいて、EA及びEAに基づくIT投資管理が導入されている。 日本政府では、2003年7月の「電子政府構築計画」の中で、EAの概念を取り込んだ「業務・システムの最適化計画策定指針」に基づいて、政府全体としての整合性を図りながら、2005年度末までに業務・システムの最適化を推進していくことを発表している。 日本政府のEA（業務・システム最適化計画の策定手順）は以下の通りである。 第１ステップ：組織横断的に政策・業務分析を行い、非効率的な業務手順、システムの重複・無駄を洗い出す、業務改革の方向性を確定する。 第２ステップ：確定した改革の方向性と問題意識を踏まえ、組織全体の現状を掘り起す。 第３ステップ：作成された現状（ASIS）モデルを元に、改革の方向性に基づいた最適化設計をしなおし、将来（TOBE）モデルを作成する。将来モデルの作成に当たっては、今ある組織や業務処理の方法とは関係なく、本来組織がすべき機能とそこに必要となる情報の２つを抽出し、そこから理想像を逆算設計する方法をとる。 第４ステップ：現状モデルから将来モデルに向かっていくための現実的なステップとして次期モデルを作成する。	現行用語集		
12	意見交換会	イケンコウカンカイ		システム監査報告書を監査依頼者に提出する前に、システム監査人と被監査部門との間で、システム監査報告書（案）の内容について意見を交換する場のこと	意見交換会は以下の目的のために実施する。 ・システム監査報告書（案）の内容について事実誤認がないことの確認 ・システム監査報告書（案）の『指摘事項』、『改善勧告』、『改善案』に対する被監査部門の意見の聴取 ・被監査部門としてシステム監査報告書（案）に記載して欲しい事項についての意見聴取 ただし、意見交換会はあくまでも被監査部門の意見を聞く場であり、システム監査報告書（案）のレビューを行う場ではないことに注意が必要である。被監査部門の意見を聞いた上で、システム監査人は自らの判断基準と責任において、システム監査報告書を完成させなければならない。	現行用語集		
13	一般基準	イッパンキジュン		システム監査人としての適格性及び監査業務上の遵守事項を規定した基準のこと	システム監査基準において、システム監査を実施する目的及び対象範囲、並びにシステム監査人の権限と責任を文書化した規定、または契約書等により明確に定められる遵守事項として、次の５つの項目を一般基準として定めている。 １．目的、権限と責任 ２．独立性、客観性と職業倫理 ３．専門能力 ４．業務上の義務 ５．品質管理		基準	
14	インタビュー法	インタビューホウ		特定の事項を立証するために、システム監査人が直接、特定者に問い合わせ回答を入手すること（システム監査技術者育成カリキュラム）	システム監査人が監査対象の実態を調査するためには、インタビューにより必要な情報が入手可能である。効率よく必要十分な監査証拠を入手するため、あらかじめインタビュー対象部門・対象者を十分に検討し、質問内容を吟味しておく必要がある。 インタビューでのチェックリストの利用、インタビューに代わるアンケート調査、現地調査でのインタビュー等、各技法の適切な組み合わせを検討する。	現行用語集		シラバス
15	外観上の独立性	ガイカンジョウノドクリツセイ		システム監査人が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という特性のこと	独立性の本質は精神上の独立であるが、外観上の独立性が損なわれると、精神上の独立性が損なわれているとの嫌疑がもたれるため、外観上の独立性を維持することが重要である。また、精神上の独立性が保たれているかについては、第三者がうかがい知ることができないため、外部の第三者にとって、外観上の独立性が維持されているかどうかは重要な問題となる。 外観上の独立性は、組織的に独立しているか、過去に自らが行った業務を自己レビューしていないか、システム監査人と被監査主体の責任者が親族関係にないか、等で検討する。		基準	
16	会計監査	カイケイカンサ	financial audit	組織体の財務諸表がその組織体の財産、損益の状況を適正に表示しているか否かを監査すること	法定監査としての会計監査の主体は、監査役と会計監査人(公認会計士または監査法人)に大別される。会社法では、会社の規模や株式譲渡制限の有無に応じて、株主総会や取締役、取締役会、監査役、監査役会、会計監査人、委員会、会計参与等の機関を設置するか否か、また設置の義務があるかどうかといった機関設計のパターンにより、会計監査の義務または任意が決められている。大枠は以下のとおりである。 ・大会社（資本金5億円以上または負債合計200億円以上 →会計監査人、監査役は会計監査を義務付ける ・全部株式譲渡制限会社である中小会社（資本金5億円未満かつ負債合計200億円未満 →会計監査人、監査役は会計監査を義務付ける ・公開会社である中小会社（資本金5億円未満かつ負債合計200億円未満） →会計監査人、監査役は会計監査を義務付ける	現行用語集		シラバス
17	会計監査人	カイケイカンサニン	financial auditor	組織体の作成する計算書類などの監査を行い、監査報告書を作成し、監査報告を行う監査人のこと	会社法（第337条）では、「会計監査人は、公認会計士又は監査法人でなければならない」としている。会計監査人は、株式会社の計算書類及びその附属明細書、臨時計算書類並びに連結計算書類を監査する（同法第396条）。	現行用語集		

No	用語	日本語読み	英文名	定義（又は説明）	解説	source	区分1	区分2
18	改善案	カイゼンアン		『改善勧告』を行うに際して、システム監査人が考えた『改善事項』に対する改善方法の案のこと	『改善事項』に対する改善方法を検討・策定し、『改善計画』にまとめることは、改善を実施する部門（通常は被監査部門）の責任である。システム監査人は、改善を実施する部門の改善活動に対する支援の一貫として、今までの経験に基づいて『改善事項』に対する改善方法の案を提示する。それが改善案である。 改善案の立案にあたって、システム監査人は、 ・改善案の有効性（問題解決の効果の大きさ） ・改善案の実現可能性（技術的困難さ、改善を実施する部門の成熟度などを考慮） ・改善案の投資対効果 を考慮することも必要である。	現行用語集		シラバス
19	改善勧告	カイゼンカンコク		システム監査人が、システム監査報告書に『改善事項』および『改善案』を記載し、『監査依頼者』に対して問題の改善を勧めること	システム監査人がシステム監査報告書に『改善事項』を記載するということは、その問題は現状のままで放置しておくことはできないと判断したということである。そして、改善勧告は、そのことを『監査依頼者』に伝え、『監査依頼者』から被監査部門に対する改善指示を勧めることである。 改善勧告によって、報告を受けた『監査依頼者』には改善実施の判断および改善指示の責任が、被監査部門には改善指示を受けて改善実施の責任が生じる。一方、システム監査報告を行ったシステム監査人は、被監査部門が行う改善活動に対する『フォローアップ』を行う必要がある。 システム監査人は、改善勧告および『改善案』の記載にあたっては、改善の実施を促進する明瞭、積極的かつ説得力のある記述に留意する必要がある。	現行用語集	基準	シラバス
20	改善計画	カイゼンケイカク		監査報告書に記載された改善勧告に対して、『監査報告』を受けた『監査依頼者』が改善指示を出し、その改善指示を受けた改善実施部門が改善の実施を計画すること	『改善勧告』に対する改善の実施には経営資源が必要であり、改善実施部門では、『改善勧告』の重要性・緊急性に加えて経営資源の状況も考慮した上で、『改善勧告』に対する改善実施の優先度を決定し、改善計画を策定する。 システム監査人は改善計画書を入手し、その妥当性を確認し、問題があれば改善実施部門に再検討を助言する。これも改善活動に対する支援・指導であり、『フォローアップ』の一環である。 最終的には、改善計画は改善実施部門の長、および組織体の長によって承認され、改善実施部門は改善計画に基づいて改善活動を実施する。	現行用語集		
21	改善事項	カイゼンジコウ		システム監査人が、『指摘事項』の中で改善が必要であると判断した事項のこと	『指摘事項』をすべて改善しなければならないかというと、それは『監査目的』やその背景にある経営目的（経営戦略の実現、経営目標の達成、経営課題の解決）に基づいて判断する必要がある。システム監査人が、そうした判断によって改善が必要と判断した『指摘事項』が改善事項である。 システム監査人は、改善事項の指摘にあたって、被監査部門と改善の必要性についての共通認識をもつよう努めなければならない。また、改善事項に対して『改善案』を提示することも、システム監査人の重要な責務である。	現行用語集		
22	改善措置	カイゼンソチ		『改善勧告』に対する改善策として、改善対象のシステムや業務プロセスなどに対して行われる変更のこと	改善措置は、改善実施部門で検討・策定され、『改善計画』に盛り込まれる。改善実施部門は改善措置の検討・策定にあたって、システム監査人がシステム監査報告書に記載した『改善案』を参考にする。システムに対する技術的変更、システムを活用する業務プロセスや活用ルールなどの運用面の変更、組織体制や役割分担の変更などの改善措置が考えられる。	現行用語集		
23	改善報告	カイゼンホウコク		改善実施部門が、『改善計画』に基づいて実施した改善活動の結果を報告書にまとめて報告すること	改善報告の方法としては、『内部監査』では、改善実施部門の責任者から直接、組織体の長に報告する方法と、一旦システム監査人が改善実施部門から報告を受ける方法がある。『外部監査』では、一般的には前者の方法だけである。 一旦システム監査人が改善報告を受ける場合には、システム監査人は改善報告の内容を確認し、改善報告書の内容に問題があれば、改善実施部門に再確認あるいは改善活動の追加実施を助言・指導する。さらに、システム監査人が改善結果について改善報告だけでなく、自ら確認する必要があると判断した場合には、『フォローアップ監査』を計画する。	現行用語集		
24	外部監査	ガイブカンサ	external audit	組織体の内部または外部の利害関係者のために、組織体から独立した外部の専門家が実施する監査のこと	もともと組織体外部の会計監査人など第三者が行う『会計監査』のことである。法律に基づく監査制度として、会社法・金融商品取引法による『会計監査人』(公認会計士または監査法人)の監査が代表的であるが、監督官庁の検査・監査など被監査組織体の意思に関係なく行われる監査もある。 なお、自治体の内部監査部門としての監査委員会に対し、外部監査の制度として「包括外部監査」と「個別外部監査」が制度化(地方自治法第252条の27)されている。 また、「品質及び/又は環境マネジメントシステム監査(JIS Q 19011)では、「外部監査には、一般的に第二者監査及び第三者監査と呼ばれるものが含まれる。前者は、顧客などその組織の利害関係者またはその代理人よって行われる。後者は、審査登録または認証する機関のような、外部の独立した監査機関によって行われる。」としている。	現行用語集		
25	外部統制	ガイブトウセイ	external control	法令・規則や業界団体など外部の利害関係者が定めた制度・組織・手続や規程等により、特定組織の経営管理の仕組みが影響を受けること	外部統制とは、法律や外部の利害関係者が定めた制度・組織、必要な手続および諸規程等からなる経営の仕組みの総称のことである。経営資源の適切かつ効率的な保全、正確な業務記録の作成と信頼ある業務報告、法令・規則への遵守を合理的に保証するために行う。	現行用語集		

No	用語	日本語読み	英文名	定義（又は説明）	解説	source	区分1	区分2
26	可用性	カヨウセイ	availabi l ity	情報が必要とされるときに利用可能であること（「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のⅠ.2(6)②」金融庁）	JISでは、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（JIS Q 13335-1:2006）と定義している。 可用性とは、利用を許可されているユーザ（利用者）が、利用が許可されている時間帯で必要な時に、許可されている情報へのアクセス要求をする場合に、アクセス可能とすることをいう。すなわち、ユーザが情報システムの機能や資源を必要とするときに、直ちにそれを使用できることである。情報システムが使用可能である状態を確保するための可用性対策として、一部に障害が発生しても代替設備で運用を継続できるように装置を多重化したり、短時間（数分）で予備用装置に切り替えたり修復できるよう準備しておくことなどが行われる。 このため、24時間365日の連続利用のニーズに対応する耐故障性を備えたコンピュータ（フォールトトレラントコンピュータ)も開発されており、ネットワークを利用したビジネスなどに利用されている。 可用性は、『機密性』、『完全性』とともに情報セキュリティの重要要素であるCIA（Confidentiality, Integrity, Availability）の一つである。	現行用語集		
27	監査計画	カンサケイカク		『監査目的』を有効かつ効率的に達成するために立てられた、監査実施の計画のこと	監査計画は、『監査目的』を達成するために監査を有効かつ効率的に行うための計画である。 監査計画は、一般に期間計画と『個別計画』に分けられ、期間計画は、『中長期計画』および『基本計画』（年度計画）に分けられる。監査計画は、監査人が立案し、監査計画書として文書化され、監査依頼者の了承を得て決定される。	現行用語集		シラバス
28	監査項目	カンサコウモク		『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のこと	監査項目は、『監査テーマ』への取組みのために、『監査範囲』の中から監査人によって抽出された、『監査手続』を適用する個々の対象である。 例えば、『監査テーマ』が「管理会計システムは、タイムリーかつ適切な情報を経営者に提供できているかを確かめる」で、『監査範囲』が「利用者としての経営者（経営企画部門）、情報システム部門が遂行する開発・運用業務、管理会計システム」の場合、利用者である経営企画部門の管理会計システムに対する評価・意見、管理会計システムのシステム運用実態、管理会計システムのシステム設計書などが監査項目の例である。 システム管理基準に規定された各項目見出しは、一般的な監査項目を示したものといえる。	現行用語集		
29	監査時期	カンサジキ		監査を実施する時期のこと	監査時期は、監査の実施・報告に関する時期を示すもので、年度の上半期/下半期、月、旬程度のスケジュールのことである。中長期計画書を受けて年度単位に策定される基本計画においては、監査対象別に、具体的な開始日、終了日を監査時期（予定）として記載できないこともあり、監査時期としての表示となることが多い。 個別計画では、監査時期ではなく、具体的な開始日、終了日を表示表示する監査日程を記述する必要がある。（ ⇒「監査日程」を参照のこと。）			シラバス
30	監査資源	カンサシゲン		監査を実施・報告するのに必要な要員、経費、場所、道具等の資源のこと	監査を実施・報告するにあたっては、被監査対象に独立な立場でシステム監査を実施及び報告できる専門能力を持ったシステム監査人が必要である。システム監査人は、適切な教育と実務経験を通じて、専門職としての知識及び技能を保持することにより、システム監査の信頼性を担保することが可能となる。組織体は人的な監査資源の確保に際して、システム監査技術者の人員計画・能力開発計画，経費予算計画等を考慮する必要がある。 また、監査を実施・報告するための経費や実施場所、道具等の資源の確保も資源計画で考慮する必要がある。			シラバス
31	監査証拠	カンサショウコ	audit evidence	システム監査報告書に記載する監査意見を立証するために必要な事実のこと	監査証拠は、物理的証拠、文書的証拠、文書化された口頭的証拠、分析的証拠に大別され、『監査調書』に記述される。 JIS Q 19011:2003では「監査基準に関連し、かつ、検証できる、記録、事実の記述又はその他の情報。監査証拠は定性的又は定量的なものがあり得る。」と定義している。 （補足）監査基準（audit criteria）：一連の方針、手順又は要求事項 システム監査人は、監査テーマを立証するために監査対象に監査技術を選択し適用し、監査証拠を入手する。監査証拠とは、システム監査人の観察結果、インタビュー結果の記録、収集した資料、監査テスト結果等のことである。監査テーマを立証するためには、十分な監査証拠が必要である。十分な監査証拠の要件としては、妥当性、正当性、適切性、有効性が要求される。 ・妥当性とは、監査対象に精通した監査人であれば、同一の結論に到達するほどに、事実に基づき、妥当で説得力のあること ・正当性とは、依存できる情報で、しかも適切な監査技法の実施を通して、最も達成可能なこと ・適切性とは、監査による発見事項や勧告を裏付け、かつ監査テーマと合致していること ・有効性とは、組織体がその経営目標を達成することに貢献すること 監査証拠は、物理的証拠、文書的証拠、文書化された口頭的証拠、分析的証拠に大別されるが、それぞれは以下のとおりである。 ａ．物理的証拠とは、監査人が直接観察した事実。 ｂ．文書的証拠とは、議事録、レビューシート、設計書、テスト結果、ログリスト等、書面で残っている書類。監査人によって収集される最も一般的なタイプの証拠。書類での証拠には内部あるいは外部のものがある。また、文書的証拠の形態としては、紙や電子媒体などが挙げられる。 ｃ．文書化された口頭的証拠とは、システム監査人の質問等に対する、被監査部門の書面または口頭での回答を文書化し確認したもの。 ｄ．分析的証拠とは、物理的証拠や文書的証拠などの関連性を分析したもの。	現行用語集	基準	シラバス

No	用語	日本語読み	英文名	定義（又は説明）	解説	source	区分1	区分2
32	監査証跡	カンサショウセキ	audit trail	各コントロール機能が情報システムの信頼性、安全性、効率性、有効性の確保に結びついていることを事後に実証するための手段のこと	監査証跡とは、情報システムおよび情報システムを運用する手続きが持っている各コントロール機能が、情報システムの健全性を確保することに有効であることを、事後に双方向で追跡し確認できる仕組みのことである。監査証跡から得られるものは時系列的な監査証拠になりうる。 具体的には、以下のものがある。 ・トランザクション証跡 『監査対象』の情報システムの取引を選び出し、データ処理内容と処理結果の相互関連を追跡できる一連の仕組み。 ・アクセス証跡 システム資源へのアクセスに関して因果関係を事後に追跡するための仕組み。 システム監査人は、監査証跡の十分性、正当性、適切性、有効性を確認した上で、監査証跡により各種コントロール機能の有効性を確認する。	現行用語集		シラバス
33	監査責任者	カンサセキニンシャ		個別の監査の実施・報告に際し、監査チームを指揮し、監査計画作成、監査実施、監査報告書の作成、報告、フォローアップを行う監査チームの責任者のこと	組織体における監査担当部署の責任者（例えば、システム監査部長・室長等）を指すのではなく、個別計画を受けて、個々のシステム監査ごとに監査目標（監査目的を詳細化したもの）の設定から監査実施、監査報告、フォローアップまでの全プロセスにおける監査作業の責任者を指している。監査報告書の評価・結論に関しては、監査担当者間、被監査部門との間の意見の整合性を図り、監査チームの責任者として、今年度の方針、重点監査テーマ、監査目的を考慮し、全社的な視点からの検討し、結論を導く。			シラバス
34	監査対象	カンサタイショウ		『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のこと	監査対象は、『監査目的』から必然的に導かれる、『監査手続』の適用範囲となり得る全対象を意味し、その切り口は、業務、システム、組織、人、物、場所など、『監査目的』によって様々である。 例えば、『監査目的』が「当社情報システムは経営に役立っているかを確かめる」の場合、経営者、経営戦略・情報戦略、計画中・稼動中の情報システム、情報システム部門、情報システムの利用者などが監査対象の例である。 監査対象は、『監査手続』の適用範囲となり得る全対象を意味し、監査人は、監査対象の中から、『監査テーマ』、及びスケジュール、投下可能資源（人、もの、金など）等の制約条件も考慮して『監査範囲』を決定する。	現行用語集		シラバス
35	監査調書	カンサチョウショ	audit working paper	システム監査において、監査人が作成し、または収集した資料のこと	監査調書は、監査報告書を作成する基礎資料、立証するための資料となる。 システム監査人は、システム監査の計画立案もしくは監査契約締結から、監査業務の遂行を経て、監査報告書の作成に至る全過程において、監査証拠となりうる資料を作成・入手し、必要に応じて記録・編集して、監査調書を作成する。 システム監査人が、監査調書を作成する目的は、次のとおりである。 ・監査業務の品質管理に役立てる。 ・監査責任者による監査担当者の業務を指導監督するのに役立てる。 ・次期以降の監査の合理的な実施を図るための資料として役立てる。 監査調書は原則として監査を実施した監査人が所有するが、被監査会社の許可なくして、その全部又は一部を他人に開示してはならない。	現行用語集	基準	シラバス
36	監査テーマ	カンサテーマ	audit theme	『監査目的』実現のために、何処に焦点をおき監査するかを表した、具体的な監査の主題のこと	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監査の主題である。そして、監査テーマが、監査人が監査報告書において意見表明する具体的ターゲットとなる。 例えば、『監査目的』が「当社情報システムは経営に役立っているかを確かめる」の場合、「管理会計システムの安全性／有効性を確かめる」「管理会計システムは、タイムリーかつ適切な情報を経営者に提供できているかを確かめる」などが監査テーマの一例である。 監査テーマは、監査実施に先立ち、監査実施意思決定者の意向、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、監査実施意思決定者の了承を得て決定される。 監査テーマは、『監査範囲』、『監査項目』、『監査要点』設定の主要な要件となる。 『監査計画』の内、『中長期計画』、『基本計画』においては、その期間に実施する監査において重点を置く『監査テーマ』を「重点監査テーマ」として明確化する場合もある。	現行用語集		シラバス
37	監査手続	カンサテツヅキ	audit procedures	監査人が、『監査要点』に対する合理的な評価、結論を得るために、その十分な証拠の収集を目的として『監査項目』に対して監査技術を選択し、適用する手続のこと	システム監査個別計画書に記載されるもので、予備調査及び本調査の際の調査手段として、資料（文書）の閲覧・収集、質問書・調査票の利用、現地調査、インタビュー、監査ツールの利用等各種の監査技法を選択適用する方法あるいは過程のことである。 例えば、『監査項目』が「管理会計システムのシステム設計」で、監査要点が「システム設計書はユーザの承認を受けているか」の場合、管理会計システムのシステム設計書の閲覧により、ユーザの承認の記録を確認する、あるいは、インタビューによりユーザ部門の責任者に管理会計システムのシステム設計書の承認を確認するなどが監査手続の例である。	現行用語集	基準	シラバス

No	用語	日本語読み	英文名	定義（又は説明）	解説	source	区分1	区分2
38	監査日程	カンサニッテイ		監査を実施する日程のこと	監査日程は、監査の実施・報告に関する日程を示すもので、開始年月日、終了年月日を表したものである。監査日程の方が、監査時期より具体化した予定（スケジュール）を指している。 個別計画では、監査時期ではなく監査日程として記述されることが望ましい。（ ⇒「監査時期」を参照のこと。）			シラバス
39	監査の手順	カンサノテジュン		監査を実施する手順のこと	システム監査基準では、実施基準において、システム監査の手順を、「監査計画に基づき、予備調査、本調査、評価・結論」としている。報告については、報告基準で記述されており、監査の手順の作業項目とはされていない。		基準	シラバス
40	監査範囲	カンサハンイ		『監査対象』のうち、『監査手続』を適用する範囲のこと	監査範囲は、『監査対象』の一部または全部であり、『監査テーマ』への取組みのために、監査人が必要と判断した、『監査手続』の適用範囲である。監査範囲は、監査人が、『監査テーマ』、及びスケジュール、投下可能資源（人、もの、金など）等の制約条件も考慮し、『監査対象』の中から抽出する。 例えば、『監査対象』が「経営者、経営戦略・情報戦略、全情報システム、情報システム部門、情報システムの利用者」で、『監査テーマ』が「管理会計システムは、タイムリーかつ適切な情報を経営者に提供できているかを確かめる」の場合、利用者としての経営者（経営企画部門）、情報システム部門が遂行する開発・運用業務、管理会計システムなどが監査範囲を構成する例である。	現行用語集		シラバス
41	監査報告	カンサホウコク		システム監査人がシステム監査の結果をシステム監査報告書にまとめ、『監査依頼者』に報告すること	監査報告の方法としては、『監査報告会』を開いて、システム監査人がシステム監査報告書に基づいて報告する方法が一般的である。場合によっては、『監査報告会』を開かず、システム監査報告書を『監査依頼者』に提出することで監査報告とすることもある。 また、『監査依頼者』に対する報告以外に、被監査部門の責任者に対する報告、被監査部門の関連部門の責任者に対する報告、監査役に対する監査報告など、組織体の状況や監査の目的に応じて、さまざまなケースがある。	現行用語集	基準	シラバス
42	監査報告会	カンサホウコクカイ		システム監査人が、システム監査報告書に基づいて、システム監査の結果を『監査依頼者』に報告する場のこと	監査報告会には、『監査依頼者』（民間企業であれば組織体の長、自治体であれば首長など）およびCIO（情報統括役員）、被監査部門の責任者が出席するのが一般的である。 監査報告会は短時間であること、出席し報告を受けるのが組織体の長や首長、上級管理者であることから、システム監査報告書を逐一報告するのではなく、重要なポイントに絞って報告することが有効である。そのために、システム監査報告書の重要な点をまとめた上級管理者向サマリ版を作成することは、よく採られる方法である。	現行用語集		シラバス
43	監査目的	カンサモクテキ		監査を実施することによって達成しようとする事項または状態のこと	監査目的とは、一つまたは複数の『監査テーマ』への取り組みを通し、その監査で達成しようとする事項または最終的な状態をいう。すなわち、監査目的は、監査実施を通し達成しようとする直接的事項の他、監査を実施し、指摘をして、その改善を通して最終的に到達しようとする状態を示す場合もある。 監査目的は、当該監査活動の意義を示し、全ての監査活動の拠り処となる。そして明確な監査目的は、監査活動を一貫したものとする。 例えば、企業経営において戦略的な情報システムの活用を志向する企業では、「当社情報システムは経営に役立っているかを確かめる」、又は「当社情報システムを経営に役立たせる」などが監査目的の一例である。 監査目的は、監査実施に先立ち、監査を行なう、または監査を受けようと決める人（監査実施の意思決定者）がその内容を決定する。監査目的から必然的に『監査対象』が導かれ、また、監査目的を基に『監査テーマ』が決定される。 監査目的は、その内容をより明確にするため、その内容をブレイクダウンし具体化した「監査目標」により補足される場合もある。例えば、監査目的が「当社情報システムは経営に役立っているかを確かめる」の場合、「現状の管理会計システムは経営に役立っているかを確かめる」などが監査目的を補足する監査目標の一例である。	現行用語集		シラバス
44	監査モジュール法	カンサモジュールホウ		監査対象ファイルよりシステム監査人が指定した抽出条件に合致したデータをシステム監査人用ファイルに記録し、レポートを出力するモジュールを、本番プログラムに組み込む方法のこと（システム監査技術者育成カリキュラム）	監査モジュールは、監査用のモジュールを組み込み、監査人がパラメータで指定した抽出条件に合致したデータが通過する際に、このデータを抽出して、システム監査人用ファイルに記録するプログラムである。	現行用語集		
45	監査役監査	カンサヤクカンサ		取締役の職務の執行について監査役が行う監査のこと（会社法第381条）	監査役は原則として、業務監査権限と会計監査権限を有する。但し、公開会社でない株式会社で監査役会や会計監査人を設置していない会社においては、定款で定めることにより監査役の権限が会計監査に限定されることもある。 『会計監査』、『業務監査』などの項目参照。	現行用語集		

No	用語	日本語読み	英文名	定義（又は説明）	解説	source	区分1	区分2
46	監査要点	カンサヨウテン		『監査項目』について、評価する内容のこと	監査要点は、『監査テーマ』への取組みのために、『監査項目』について、監査人が評価、確認する内容であり、その監査における、『監査項目』の判断の尺度である。 例えば、『監査テーマ』が「管理会計システムは、タイムリーかつ適切な情報を経営者に提供できているかを確かめる」で、『監査項目』が「管理会計システムのシステム設計」の場合、「システム設計書はユーザの承認を受けているか」などが監査要点の一例である。 システム管理基準に規定された小項目は、一般的な監査要点を示したものといえる。 システム監査の実務では、『監査項目』とその判断の尺度（『監査要点』）とを合わせて『監査項目』と表現する場合もある。しかし、『監査項目』と『監査要点』はその内容に本質的差異があるので、両者を『監査項目』と『監査要点』に区分し定義することが、監査の構造、監査の理論体系を明確に整理する上で有効といえる。	現行用語集		
47	監査リスク	カンサリスク	audit risk	固有リスク、統制リスク、および発見リスクの三つの要素で構成され、監査人が財務諸表の重要な虚偽の表示を見過して誤った意見を形成する可能性のこと（日本公認会計士協会HPより引用）	監査リスは、監査人が財務諸表の重要な虚偽の表示を看過して誤った意見を形成する可能性を意味する。監査に内在するリスクを指している。一般に監査リスクは、固有リスク×統制リスク×発見リスクの積で表される。固有リスクは内部統制が存在しないと仮定した場合にその組織自体で監査証拠となるものに重要な虚偽表示が発生する可能性をいう。統制リスクはその組織の内部統制によって重要な虚偽表示を防止または発見されない可能性を指す。発見リスクは、監査人が内部統制において防止または発見されなかった重要な虚偽表示を発見できない可能性を指す。 現在の監査においては、監査対象のリスクの大きさにより監査の程度や実施方法を定め、重大な問題が発生する可能性のあるところを重点に十分な監査証拠を入手しようとするリスクアプローチを用いることが主流となってきている。監査は日常業務への影響を最小限におさえることが求められており、時間や要員などの資源に限りがあるため、適切かつ重要な分野に絞って実施するが、監査リスクが内在することも考慮にいれておくことが必要である。	現行用語集		
48	完全性	カンゼンセイ	integrity	情報および処理方法が正確であるようにすること、および、その正確である状況を保持すること	JISでは、資産の正確性及び完全さを保護する特性（JIS Q 13335-1:2006）と定義している。また、金融庁の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（Ⅰ.2(6)②）では、記録した取引に漏れ、重複がないことと定義している。 許可されていない利用者、または内部利用者によって情報が改ざん、または破壊されたりしないようにすることにより、情報の正確性と完全性を常に維持すること。 完全性は、『機密性』、『可用性』とともに情報セキュリティの重要要素であるCIA（Confidentiality, Integrity, Availability）の一つである。	現行用語集		シラバス
49	基本計画	キホンケイカク		『中長期計画』を基にした、当該年度の監査の期間計画のこと	基本計画は、『中長期計画』に基づき、具体化された当該年度の監査年間計画である。 主な記載項目は、本年度の監査の方針、『監査対象』、重点監査テーマ、対象情報システム又は業務、実施体制、監査スケジュール、『監査項目』、所管部門、監査責任者・担当者、予定時期、要員計画、品質管理計画、経費予算等が挙げられる。	現行用語集		シラバス
50	機密性	キミツセイ	confidentiality	情報が正当な権限を有する者以外に利用されないように保護されていること（「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のⅠ.2(6)②」金融庁）	JISでは、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、情報を使用不可又は非公開にする特性（JIS Q 13335-1:2006）と定義している。 機密性は、アクセスを許可された者だけがアクセスでき、アクセスを許可されていない者が利用できないようにすることである。情報の共有者 (個人、組織体)以外の第三者(特に競合者)に、その情報が故意または偶然の手段で知られた場合には、損失が生じる。また、アクセス権を持たない者がアクセスすると、情報改ざん、不正情報の混入や漏洩などの被害が生じてしまう。このような被害が起きないように、機密性を高める施策がとられる。 機密性は保護の対象とする情報、情報を処理する機器や仕組みなどを議論する場面で考慮する。 情報に対する機密性では、企業や組織では機密情報の管理方針を策定し、すべての情報資源を機密区分することが重要である。機密区分とは、情報資源の機密度に応じて、極秘、秘、社外秘、部外秘などに区分される。情報システムでは、情報資源の機密度に応じてアクセス権限や利用者を区別する。この機密区分に基づいて、情報の利用（閲覧、変更、加工）、配布、持出し・持込み、保管、消去、廃棄に関する手順を定める。 機密性は、『完全性』、『可用性』とともに情報セキュリティの重要要素であるCIA（Confidentiality, Integrity, Availability）の一つである。	現行用語集		シラバス
51	脅威	キョウイ	threats	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要因のこと（JIS Q 13335-1）	脅威は、脆弱性により誘引され、顕在化することにより、情報資産に損害を与える。脅威の大きさは、その要因や対象となる情報資産ごとにその発生の可能性を評価して決定される。 脅威は、人間的脅威と環境的脅威に大別される。前者は更に意図的脅威と偶発的脅威に分けられる。意図的脅威は盗聴、情報の改ざん、システムのハッキング、悪意のあるコード、盗難などが該当し、偶発的脅威は誤り及び手抜かり、ファイルの削除、不正な経路、物理的事故が該当する。また、後者は、地震、落雷、洪水、火災等が該当する。	現行用語集		
52	業務監査	ギョウムカンサ	business audit operating audit	組織体の人事、購買、製造、販売等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	組織体の経営目標の達成を目的とし、合法性、合理性の観点から経営諸活動を監査することで、内部監査部門の監査、監査役監査がそれぞれの立場でこれに関わっている。 また、この両監査と会計監査人監査をあわせて、「三様監査」と呼び、それぞれの立場を維持しつつお互いに協力して監査を行う。「ネットワーク監査」とも呼ばれている。これを監査主体別に区分すれば、次のようになる。 ・監査役監査(取締役の職務執行の適法性の監査) ・会計監査人監査(財務諸表の適正性の監査) ・内部監査部門の監査(組織体の内部統制の監査)	現行用語集		シラバス

No	用語	日本語読み	英文名	定義（又は説明）	解説	source	区分1	区分2
53	緊急改善	キンキュウカイゼン		『改善勧告』のうち、システム監査人が重大な問題であり、技術面・経済面から見た改善の実現可能性、改善にかかる投資対効果などを考慮した上で、速やかな改善実施が必要と判断した事項のこと	『改善事項』を改善するためには、経営資源の投下が必要であり、すべての『改善事項』に対して同じ緊急度、優先度で改善を実施することは効率的ではない。システム監査人は、『監査目的』を踏まえ、『改善事項』の問題の大きさ（緊急性、重要性）を基本に、改善の実現可能性などを考慮した上で、緊急改善と『通常改善』に分けて、メリハリのある『改善勧告』を行う必要がある。 問題としてはそれほど大きくはないが、すぐに改善でき効果が期待されるものを緊急改善にして、改善実績を作るという方策もときには効果的である。 また、『改善事項』によっては、根本的な改善（恒久対応）には時間がかかるので通常改善とするが、問題としては放置できないので最低限の改善（暫定対応）を緊急改善とするということもあり得る。	現行用語集		シラバス
54	緊急時対応計画	キンキュウジタイオウケイカク	contingency planning	緊急事態またはシステム中断があった場合にITサービスを復旧させるための暫定的な処置のこと（独立行政法人　情報処理推進機構HPより引用）	通常発生するような故障は、緊急時対応計画に含めない。情報システムについては、地震や水害などの災害や、停電、通信回線の不通、あるいはサイバーテロなどへの対応などがある。 ITシステムには、軽度（短時間の停電、ディスクドライブ障害など）から、重度（装置損壊、火災など）まで、自然災害からテロ行為に至る様々な脅威が存在する。そしてITシステムは、それらの脅威に対して脆弱である。多くの脆弱性は、技術的管理や組織のリスクマネジメント業務の一環としての運用ソリューションによって最小化できるが、すべてのリスクをなくすことは事実上不可能である。多くの場合、重要なリソースが組織の統制の及ばないところに存在する場合（電力や通信など）、組織はその可用性を保証することはできない。したがって、システム及びサービスの可用性低下リスクを低減するには、効果的な緊急時対応計画、実施、テストが不可欠である。 （独立行政法人　情報処理推進機構HPより引用）	現行用語集		
55	金融機関等のシステム監査指針	キンユウキカントウノシステムカンサシシン		公益財団法人金融情報システムセンターにより作成・改訂されているもので、金融機関等がシステム監査を実施する場合に参考となる手引き・参考書として活用されている指針のこと	公益財団法人金融情報システムセンター（FISC；The Center for Financial Industry Information Systems、別掲参考URL参照）が1987年に作成し、2000年７月、大幅に改訂したもので、金融機関等がシステム監査を実施する場合に参考となる手引き・参考書として活用されているシステム監査指針である。 この新しい指針の構成は、以下のとおりである。なお、第1部は７ページ、第２部は40ページである。第３部のチェックポイント集も大部で、要点項目ごとに、①リスクは何か、②誰が、何をコントロールするのか、③どのようにコントロールするのか を記述した上で、大項目、小項目に別れてチェックポイントと関係資料の例示がある。 第１部　エグゼクティブサマリー 第２部　フレームワーク 第Ⅰ章　システム監査の基本概念 第Ⅱ章　システム監査の実践 第３部　チェックポイント集 １　情報システムの計画と管理 ２　情報システムリスクの管理 ３　情報セキュリティ ４　システム開発 ５　システム運用 ６　システム利用 ７　入出力等の処理 ８　ＥＵＣ ９　ネットワーク １０　システム資産・資源管理 １１　外部委託 １２　コンティンジェンシープラン １３　ドキュメンテーション 用語の注釈　　付録	現行用語集		

No	用語	日本語読み	英文名	定義（又は説明）	解説	source	区分1	区分2
56	金融検査マニュアル	キンユウケンサマニュアル		金融機関等の法令等遵守を含むリスク管理態勢を検査官が検証していく際に必要となる検査の基本的考え方と具体的着眼点を整理した「金融検査官の手引書」のこと	金融庁では、信用、市場性、流動性、事務、システムなどの各種のリスクに対応した検査マニュアルを用意しており、システムリスクについては「システムリスク管理態勢の確認検査用チェックリスト」がある。 チェックリストは検査官用の手引書の位置付けであるが、金融機関等では自己責任原則の下、このチェックリストを踏まえて更に詳細なマニュアルを自主的に作成し、業務の健全性、適切性の確保に努めることが期待されている。 「システムリスク管理態勢の確認検査用チェックリスト」の確認検査項目を列挙すると、Ⅰ.リスク管理に対する認識等、Ⅱ.適切なリスク管理態勢の確立、Ⅲ.監査及び問題点の是正、Ⅳ.企画・開発体制のあり方、Ⅴ.体制の整備、Ⅵ. 防犯・防災・バックアップ・不正利用防止となる。このうち上記Ⅲの冒頭の記述を参考に例示する。 Ⅲ. 監査及び問題点の是正 １. 内部監査 (1)内部監査部門の体制整備 ①内部監査部門は、システム関係に精通した要員を確保しているか。 (注)「しているか」とあるのは、全ての金融機関に対しミニマム・スタンダードとして求められる項目である。	現行用語集		
57	経営計画	ケイエイケイカク	management plan	経営目標を達成するための計画のこと	経営理念とそれに基づいた経営戦略を実現するため、企業は経営計画を策定し、実行する。経営計画には、中長期（３～５年）の期間を対象とするものと、単年度を対象とするものとがあるが、前者を中長期経営計画、後者を（年次）経営計画という。システム監査計画においても、中長期監査計画は中長期経営計画と、また基本監査計画は（年次）経営計画と、各々整合していることが重要である。			シラバス
58	経営戦略	ケイエイモクヒョウ	management strategy	企業のあるべき姿を描き、そこに至る方策を示すこと	具体的には、自社や競合相手の内的要因・外的要因の分析・評価、経営目標の設定、目標達成への戦略の策定、戦略の実行、戦略の評価、戦略の変更・再設定等のプロセスを繰り返して、企業全体・企業グループの優位性を構築・維持することである。 経営戦略は、組織のレベル、機能のレベルに応じて、全社戦略、事業戦略、機能別戦略と分類される。他にも、特定の目標計画を達成するための成長戦略、知的財産戦略、IT戦略等がある。			シラバス
59	経営目標	ケイエイモクヒョウ	business objectives	経営活動によって達成するための到達点のこと	経営目標を達成するために、重点的に取り組むべきものを主要成功要因（ＣＳＦ Critical Success Factors ）という。また、目標達成の度合いを計るための指標を設定して評価を行う。代表的指標として、重要目標達成指標（ＫＧＩ Key Goal Indicator ）や重要業績評価指標（ＫＰＩ Key Performance Indicator ）等が挙げられる。			シラバス
60	現地調査法	ゲンチチョウサホウ		システム監査人が被監査部門へ赴き、そこでの作業状況を、自ら調査すること（システム監査技術者育成カリキュラム）	システム監査人が自ら監査対象の現状を確認し、理解することが重要である。 現地での調査は、システム環境（センター、事務所、工場等）における対象業務の始点および取引の発生源から開始し、業務処理フローをトレースすることが効果的である。現地の業務の妨げにならないような注意が必要であり、スケジュール調整をする。	現行用語集		シラバス
61	公認システム監査人	コウニンシステムカンサニン	Certified Systems Auditor(CSA)	特定非営利活動法人日本システム監査人協会が認定しているシステム監査人の資格取得者のこと	公認システム監査人（Certified Systems Auditor(CSA)）とは、特定非営利活動法人日本システム監査人協会（Systems Auditors Association of Japan=SAAJ；以下SAAJ）が創設・運営している公認システム監査人認定制度で認定されたシステム監査人のことである。 産業構造審議会の情報産業部会・情報人材対策小委員会は、その中間報告(1999.6.1)で次の２点の指摘を行った。一つは、「システム監査人がユーザの信頼を得るためには、単に知識等に習熟するのみならず、実践的監査経験を積むことが重要である。その観点から、従来より実施しているシステム監査技術者試験に合格した上で、一定の有効な実務経験を積んだことを確認することにより、システム監査人として認定する制度の創設を検討する。」またもう一つは「IT技術が急速に変化する中で、システム監査人が最新の技術動向に対応できるよう情報処理技術者試験の見直しと併せて定期的セミナーの受講を義務づけるなどの方策を検討する。」である。 この提言を受けて、SAAJが2002年4月に、経済産業省の指導のもとにこの制度を創設した。システム監査技術者試験の合格者について、実務経験を確認し継続教育を義務づけて「公認システム監査人」(CSA)として認定する制度であり、システム監査の実務経験を積む間は、「システム監査人補」（Associate Systems Auditor (ASA)）として認定され、両者ともに一定の継続教育を受けることを義務づけられる。 なお、その他の高度情報処理技術者や公認会計士等関連資格の保持者に対して特別認定制度の講習・試験の合格を条件にシステム監査人補に認定する特認制度が設けられている。	現行用語集		

No	用語	日本語読み	英文名	定義（又は説明）	解説	source	区分1	区分2
62	効率性	コウリツセイ	efficiency	情報システムの資源の活用及び費用対効果が適切であること	旧システム監査基準（平成8年1月30日改訂）では、用語の定義で効率性を、情報システムの資源の活用及び費用対効果の度合としている。JISでは、明示的な条件の下で、使用する資源の量に対して適切な性能を提供するソフトウェア製品の能力（JIS X 0129-1）と定義している。 効率性とは、情報システム、情報システムを開発・運用する設備、施設、要員などの資源を最適に活用することである。 投資をしてコンピュータを導入しても、開発した情報システムが現場に適応しておらず使えなかったり、全体の作業効率を低下させたり、という例は少なくない。高度で複雑な情報システムや通信システムの運用では、サービスの継続性や事業の継続性に影響を与える事態も発生している。このため情報システムの資源を有効活用し、投資対効果を高める工夫が求められている。 システム監査は、システム開発投資や運用に対して効率性・『有効性』の視点から診断し、システム部門の組織活動やシステム開発や運用状況を確認するので、極めて有効である。	現行用語集	基準	シラバス
63	COSO	コーソー	The Committee of Sponsoring Organizations of the Treadway Commission	トレッドウェイ委員会組織委員会のこと	1980年代前半、アメリカにおける金融機関を含む多くの企業の経営破綻により、多くの企業不祥事が問題となった。1985年にアメリカ公認会計士協会（AICPA）は、関連団体に働きかけ、「不正な財務報告全米委員会（The National Commission on Fraudulent Financial Reporting）」（委員長J.C.Treadway, Jr.の名前を付けトレッドウェイ委員会と呼ぶ。）を共同で設立した。トレッドウェイ委員会は、1987年に「不正な財務報告（通称「トレッドウェイ委員会報告書」）」と題する最終報告書を公表して、不正な財務報告を防止し発見するためのフレームワークとその方策を、上場企業（経営者）、外部監査人、米国証券取引委員会（SEC）およびそのほかの行政・立法機関、教育機関に向けて、さまざまな勧告を行った。 トレッドウェイ委員会の勧告を受けて、COSO（トレッドウェイ委員会組織委員会）は、内部統制に関する総合的な研究に着手し、1992年「インターナル・コントロールの統合的枠組み（通称COSOレポート）」を発表、1994年には「『外部関係者への報告』の追補」を発表した。この内部統制の枠組みが、「COSOの内部統制フレームワーク」「COSOフレームワーク」と呼ばれるものである。 また、2004年９月にCOSOより、公表された「Enterprise Risk Management－Integrated Framework」は、COSOフレームワークを踏まえて、そのリスクマネジメントへの適用を提示したものとして注目されている。	現行用語集		
64	コード比較法	コードヒカクホウ		あらかじめシステム監査人によって検証されたプログラムと監査対象プログラムとを、コーディングのレベルで1行づつ比較して、監査対象プログラム改竄の有無（ロジックの正確性）を確認する技法のこと（システム監査技術者育成カリキュラム）	コード比較（Program Code Comparison）法は、本番用プログラムを、監査用プログラムと比較して、その正当性を検討する技法である。 ソース・コードあるいはオブジェクト・コードについて行なわれるが、使用中のプログラムとドキュメンテーションの間に差異がないかどうかの調査が可能である。 コード比較には、ソース・コードの２世代間比較、本番用オブジェクト・コードの２世代間比較、本番用オブジェクト・コードと監査用オブジェクト・コードの同一世代間比較、本番用オブジェクト・コードと監査用オブジェクト・コードの２世代間比較の４形態がある。	現行用語集		
65	コーポレートガバナンス	コーポレートガバナンス	corporate governance	企業経営を規律するための仕組のこと	企業経営を担うのは経営者であるため、基本的には企業経営者、社長といったトップマネジメントだけでなく、経営を執行する経営陣も含まれる。経営陣をどのように規律していくかがコーポレートガバナンスである。	auシラバス		
66	個人情報	コジンジョウホウ		生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの	個人情報とは、「個人に関する情報、氏名、性別、生年月日等個人を識別する情報に限られず、個人の身体、財産、職種、肩書などの属性に関して、事実、判断、評価を表すすべての情報であり、評価情報、公刊物等によって公にされている情報や、映像、音声による情報も含まれ、暗号化されているかどうかを問わない。また、他の情報と容易に照合することができ、それにより個人を識別することができるものを含む（個人情報保護に関する法律（平成15年法律第五十七号　同年５月30日一部施行、平成17年４月１日全面施行）。 なお、死者に関する情報が、同時に、遺族等の生存する個人に関する情報でもある場合には、当該生存する個人に関する情報となる。また、「生存する個人」には日本国民に限られず、外国人も含まれるが、法人その他の団体は「個人」に該当しないため、法人等の団体その他のものに関する情報は含まれない。（ただし、役員、従業員等に関する情報は個人情報） （以上「個人情報保護に関する法律についての経済産業分野を対象とするガイドライン（平成２１年１０月９日厚生労働省経済産業省告示第２号）」参照）	現行用語集		

No	用語	日本語読み	英文名	定義（又は説明）	解説	source	区分1	区分2
67	個人情報保護関連法規	コジンジョウホウホゴカンレンホウキ		個人情報保護に関わる法規やガイドライン	個人情報を取り扱う事業者は、事業に関連する個人情報の取扱いの法令，同法が定める指針及びその他の規範の制定・改廃状況に注意し，必要に応じて速やかに個人情報保護マネジメントシステムに反映できる手順を確立する必要がある。法令やガイドラインとしては、 ・個人情報保護法， ・行政機関の保有する個人情報の保護に関する法律(平成15年法律第58号)， ・独立行政法人等の保有する個人情報の保護に関する法律(平成15年法律第59号)， ・各地方自治体が制定している個人情報保護条例， ・その他の法令， ・行政機関が制定している個人情報の保護に関する指針(ガイドライン)， ・認定個人情報保護団体が定めた個人情報保護指針， ・各業界が定めたガイドライン 等がある。			
68	個人情報保護方針	コジンジョウホウホゴホウシン		事業者が個人情報を保護するための全般的な方針を定め文書化したもの	プライバシーポリシーともいう。以下、個人情報保護に関するコンプライアンス・プログラムの要求事項（JIS Q 15001)(2006年に改訂)基づき解説する。事業者は、プライバシーポリシーを策定、文書化し、役員及び従業員に周知させるとともに、一般の人が入手可能な措置を講じなければならない。プライバシーポリシーに盛り込まなければならない項目は次のとおりである。 a) 事業の内容及び規模を考慮した適切な個人情報の取得，利用及び提供に関すること（特定された利用目的の達成に必要な範囲を超えた個人情報の取扱い（以下，“目的外利用”という。）を行わないこと及びそのための措置を講じることを含む。）。 b) 個人情報への不正アクセス，個人情報の漏えい，滅失又はき損の防止並びに是正に関すること。 c) 苦情対応に関すること。 d) 個人情報の取扱いに関する法令，国が定める指針及びその他の規範を遵守すること。 e) 個人情報保護マネジメントシステムの継続的改善に関すること。 f) 代表者の氏名 （経済産業省HPより引用） （http://www.meti.go.jp/policy/it_policy/privacy/jis_shian.pdf） なお、個人情報には、電子化されたデータのみならず、個人情報が記された書類等も全て含まれる。また、プライバシーポリシー（個人情報保護方針）を一般の人が入手可能な措置については、会社のホームページに掲載することなどが行われている。	現行用語集		
69	COBIT	コビット	Control Objectives for Information and related Technology	組織体に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にITガバナンス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資料やツールのこと	情報システムコントロール協会 (ISACA)とITガバナンス協会 (ITGI)が1992年に作成を開始した情報技術 (IT) 管理についてのベストプラクティス集（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ベストプラクティスを提供して情報技術を利用して得られる利益を最大化するための補助とし、企業内の適切なITガバナンスや内部統制の開発の補助となる。	現行用語集		
70	誤謬摘示機能	ゴビュウテキジキノウ	editing control	業務処理の過程で誤謬や不正が発生した場合にそのことを速やかに検知し、報告・警告する機能のこと	誤謬摘示機能は業務処理の過程で誤謬や不正が発生した場合に、そのことを速やかに検知し、報告・警告など被害を最小限に抑えるために適切な対処がとれるようにすることである。『予防牽制機能』、『修正回復機能』とあわせ、『内部統制』を構成する３つの主要機能の１つ。 誤謬摘示機能は、プログラムによる誤謬摘示、記録や実在する資産との照合、発見された誤謬に関する適切な措置の機能に分類される。例えば、入力されたデータが事前に定められた範囲の数値や基準と異なる場合に、警告して入力訂正を促し、潜在エラーを解消する。	現行用語集		
71	個別計画	コベツケイカク		『基本計画』を基に実施する、個々の監査の計画のこと	個別計画は、期間計画（『中長期計画』、『基本計画』）に基づき実施する個々の監査の計画である。個別計画は、その監査の規模、複雑さにより更に具体化した実施計画に展開される場合もある。 個別計画は、個々の監査活動の拠り所となる計画であり、主な記載項目は、『監査対象』、所管部門、重点『監査テーマ』、当該監査の『監査目的』、監査責任者・担当者、監査コスト、監査期間、報告時期、『監査手続』、監査着眼点、『監査範囲』、担当者名、実施日の記載、実施体制、品質管理手法等が挙げられる。	現行用語集		シラバス
72	コントロール	コントロール	control	望ましくない事象を防止する手段のこと、またはその手段が機能していること	例えば、「不正アクセス」という「望ましくない事象」を防止する対策として「資格者確認機能」が挙げられるが、その場合「資格者確認機能」をコントロールと呼ぶ、もしくは「資格者確認機能」が機能していることをコントロールと呼ぶ。 システム監査では、情報システムのライフサイクルに応じて、リスクを低減するためのコントロールを適切に整備・運用するための実践規範としてのシステム管理基準で287のコントロール項目を定めている。	システム管理基準	基準	シラバス

No	用語	日本語読み	英文名	定義（又は説明）	解説	source	区分1	区分2
73	コンピュータウイルス	コンピュータウイルス	computer virus	第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムのこと	コンピュータウイルスの定義は、自己伝染機能、潜伏機能、発病機能のうち１つ以上を有しているものである。（「コンピュータウイルス対策基準」の用語の定義参照）） コンピュータウイルスは、ネットワークやフロッピーディスクなどを介して、コンピュータ内のファイルなどに密かに入り込み、そこからさらに別のコンピュータへと自分自身を複写して増殖していくことができ、特定の日時などの条件や、電子メールの開封といった特定の操作によって起動する様子が、人間や動物に感染して潜伏期間を経て発病する風邪（インフルエンザ）やエイズのウイルスに似ていることから、「コンピュータ・ウイルス」と呼ばれる。また、コンピュータウイルス対策プログラムをさして「ワクチン」ともいう。 コンピュータウイルス対策基準の３つの定義は、次のとおりである。 （１）自己伝染機能 自らの機能によって他のプログラムに自らをコピーしまたはシステムの機能を利用して自らを他のシステムにコピーすることにより、他のシステムに伝染する機能 （２）潜伏機能 発病するための特定時刻、一定時間、処理回数等の条件を記憶させて、発病するまで症状を出さない機能 （３）発病機能 プログラム、データ等のファイルを破壊したり、設計者の意図しない動作をする等の機能	現行用語集		
74	コンピュータウイルス対策	コンピュータウイルスタイサク		コンピュータウイルスに対しての予防、発見、駆除、復旧などの対策のこと	1990年２月、経済産業省（当時、通商産業省）は、コンピュータウイルスへの対策をとりまとめた「コンピュータウイルス対策基準」を制定し、その後2000年12月に改定された。新しい情報リスクとして出現したコンピュータウイルスに対し、それまでのセキュリティ対策基準を補完するため制定した。基準は、①システムユーザー、②システム管理者、③ソフトウェア供給者、④ネットワーク事業者、⑤システムサービス事業者の５つの対象ごとに、それぞれコンピュータウイルスに対する予防、発見、駆除、復旧などの対策を具体的に示している。	現行用語集		
75	コンピュータ支援監査技法	コンピュータシエンカンサギホウ		監査業務の過程において、コンピュータを使用する技法のこと	コンピュータを利用したシステム監査技法は、システム開発のテスト等に利用している技法であり、システム監査人側においても、コンピュータ内部処理の正確性をチェックするために利用する技法である。 なお、技法によっては、システム監査時に利用する技法と、システム開発の段階で、あらかじめツールをシステムに組み込むことが望ましい技法とがある。	現行用語集		シラバス
76	コンピュータ犯罪	コンピュータハンザイ		コンピュータが直接的あるいは間接的に介在した社会悪行為のこと（通産省（現経済産業省）のコンピュータセキュリティ研究会による報告書「健全なる情報社会の構築に向けて（1982年10月）」参照）	ここでのコンピュータの「直接的」介在とは、電磁的記録の破壊あるいは偽造などのようにコンピュータシステムそのものに対して行われる機能阻害あるいは不正使用であり、「間接的」介在とは、コンピュータ・システム自体の使用は適性であるがこれを媒介にして不正な行為が行われることをいう。例えば、インターネットを利用した海賊版ソフトの販売や詐欺行為のことをさしている。 コンピュータ犯罪は、情報技術やネットワークの進展につれて犯罪手法も従来は考えられなかったものも出現してきているが、一般的に以下のように分類されている。 （１）金銭及び物品の不法領得 （２）情報関連資産の窃取 （３）情報関連資産の破壊 （４）情報サービスの盗用 （５）妨害行為 また、広義には、コンピュータを不正に使用したネットワーク犯罪、不正アクセス禁止法違反を含め、ハイテク犯罪と呼称している。（警視庁広報資料参照） 近年、国内では、コンピュータ犯罪対策として、不正アクセス禁止法（平成12年２月発行）が法制化され、国際的には「サイバー犯罪防止条約」が検討されている。	現行用語集		シラバス
77	コンピュータ不正アクセス	コンピュータフセイアクセス		システムを利用する者が、その者に与えられた権限によって許された行為以外の行為を、ネットワークを介して意図的に行うこと。 （独立行政法人　情報処理推進機構HPより引用）	「不正アクセス行為の禁止等に関する法律（平成12年２月13日に施行）」（通称：不正アクセス禁止法）で禁止する行為は、①アクセス制御機能を有しているコンピュータ対して、②ネットワークを利用して、③本人のパスワード等（アクセス制限を免れることのできる情報、指令を含む）をコンピュータに入力する行為のことである。 以上の３つの要件が成立していれば、アクセスの結果として何もしていなくても法律違反となる。また、パスワード等のアクセス制御機能に係わる識別符号を正規の利用権者以外の者に対して提供した場合も不正アクセス行為を助長する行為として本法律違反となる。 《参考；コンピュータ不正アクセス対策基準》 コンピュータへの不正アクセスによる被害の予防、発見と復旧、拡大防止のために、企業や個人が取るべき対応策を定めたもの。経済産業省（旧通産省）が1996年８月に策定した。例えば、IDやパスワードを使ったユーザ認証を行ったり、データへのアクセスを制限したり、データ改ざんが起きた場合にはどのように対処するか、などのルールを決めておく。これらにより企業システムへの不正サクセスを防止するとともに、不正アクセスへの対処方法を明確にする。	現行用語集		

No	用語	日本語読み	英文名	定義（又は説明）	解説	source	区分1	区分2
78	コンプライアンス	コンプライアンス	compliance	法律、制度、業界規則、社内規定、倫理規程等組織体が守るべきものを守って行動すること	情報システムで処理される業務は、関連法規、業界規則、契約又は内部規程等に準拠して実施されなければならない。業務が正確に処理されていることを保証するためには、法令等のルールを遵守しているかを監査しなければならない。システム管理基準では、単に法令遵守だけでなく、社会的規範や組織体の倫理（モラル）規程の遵守も含めている。これは、コンプライアンス違反ではないが、モラル違反の行動により、社会的信用の失墜を招き、ITガバナンスの実現に支障を来すからである。なお、企業の社会的責任（履行）・CSR（Corporate Social Responsibility）も、法令遵守が前提であることに留意しなければならない。 IT関連の法的整備は、IT技術の進歩に追随できない局面があり、常に、IT関連法令の新設・整備状況をモニタリングする必要があるが、その際は社会的規範や組織体の倫理規程等を遵守する必要がある。			シラバス
79	採算性	サイサンセイ	profitability	組織体が行う事業、業務等で収支がとれること	企業経営では、事業で利益が出ることが求められ、採算性のよい事業であるか否かが問われる。 情報システムの採算性とは、一般に、情報システムを運用することにより見込まれる売上増加やコスト削減から、情報システムの構築費用及び運用・保守・廃棄までのシステムライフサイクルを通してのトータル費用を差し引いて、利益が出ていることである。			シラバス
80	サイバー犯罪	サイバーハンザイ	cyber crime	コンピュータ技術及び電気通信技術を悪用した犯罪のこと	わが国においてサイバー犯罪は、以下の３つの類型に区別される。 ①コンピュータ、電磁的記録対象犯罪 刑法に規定されているコンピュータや電磁的記録を対象とした犯罪 ②ネットワーク利用犯罪 上記の1.以外で、犯罪の実行にネットワークを利用した犯罪、又は、犯罪行為そのものではないものの、犯罪の敢行に必要不可欠な手段としてネットワークを利用した犯罪 ③不正アクセス行為の禁止等に関する法律違反 これらの３類型は具体的には、それぞれ次のような場合を指す。 ①コンピュータ、電磁的記録対象犯罪 ・金融機関などのオンライン端末を不正操作し、無断で他人の口座から自分の口座に預金を移した(電子計算機使用詐欺罪) ・サーバコンピュータに保存されているホームページのデータを無断で書き換えた(電子計算機損壊等業務妨害罪) ②ネットワーク利用犯罪 ・電子掲示板に販売広告を掲示し、覚せい剤等の違法な物品を販売した ・インターネットオークションで、自分が持っていない品物を出品し、落札者から代金をだまし取った ・インターネットに接続されたサーバコンピュータにわいせつな映像を置き、これを多くの人に対して閲覧させた など、犯罪の実行にあたりネットワークを利用した場合をいう。 ③不正アクセス行為の禁止等に関する法律違反 ○不正アクセス行為 ・他人のＩＤ、パスワードを無断で使用して、ネットワーク越しにコンピュータを不正使用した場合(なりすまし行為) ・不正なプログラムを使用する等して、コンピュータの安全対策上の不備(セキュリティ・ホール)を突き、ネットワーク越しにコンピュータを不正使用した場合(セキュリティ・ホール攻撃) ○不正アクセス助長行為 ・コンピュータを利用するためのID、パスワード等を、利用者に無断で第三者に教えた場合をいう。 （富山県警察HPより引用） （http://police.pref.toyama.jp/sections/6110/high-tech/cyber.html			
81	サブコントロール	サブコントロール	subcontro l	コントロールを細分化したもの	コントロールの下位に位置するもの（経済産業省「情報セキュリティ管理基準Ver1.0」（平成15年4月1日制定）より引用）。経済産業省「システム管理基準」（平成16年10月8日策定）では、287項目のコントロールを挙げている。そのうえで、「組織体が属する業界又は事業活動の特性等を考慮して、必要ある場合には、本管理基準の主旨及び体系に則って、該当する関係機関などにおいて、独自の管理基準を策定し活用することが望ましい。また、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。」と記述している。 「新版システム管理基準解説書」（2005年経済産業省監修）では、各項目がコントロールに当たり、着眼点がサブコントロールに当たる。		基準	
82	サンプリング	サンプリング	sampling	母集団全体の特徴を調べるために一部を抽出する行為のこと。	システム監査人は、監査手続において、十分かつ適切な監査証拠を入手するに当っては、母集団全体を対象として監査手続を行う精査という方法は通常困難であり、原則として母集団から対象を抽出して監査手続を行う試査という方法に基づき実施する必要があるが、その場合の監査手続の対象項目の抽出方法の１つとして、サンプリングという方法が取られる。 監査資源が限られている中で、監査対象全体（母集団）の特性を把握して、抽出したサンプル（標本）の検証で、全体の問題点を洗い出すため、場合によっては誤った判断（サンプリングリスク）を導くこともある。そのため、監査目的に応じて統計的サンプリングが求められる。			シラバス

No	用語	日本語読み	英文名	定義（又は説明）	解説	source	区分1	区分2
83	CIA	シーアイエー	Certified Internal Auditor	米国の内部監査人協会(The Institute of Internal Auditors)の実施するCIA（r=公認内部監査人）試験に合格し実務経験等を条件に認定される資格保持者のこと	CIA試験は、日本では日本内部監査協会(Institute of Internal Auditors Japan=IIA-J)が実施し、日本語で受験できる。試験科目は①監査理論および実務ガバナンス、リスク、コントロールにおける内部監査の役割、②内部監査の技術および手続内部監査の実施、③経営管理と情報技術ビジネス分析と情報技術、④監査環境ビジネス・マネジメント・スキルの四つで、各2時間半で２日間の試験である。科目単位の合格が認められる。 なお、日本内部監査協会では、システム監査関連では「情報システム監査専門内部監査士」の認定制度を、1988年から実施している。認定のための講習会が８９日間(4550時間)あり、所定の課程を修め、修終了論文を提出後資格審査委員会において審査され、合格者には「情報システム監査専門内部監査士」の称号を授与される。(別掲参考URL参照)	現行用語集		
84	CSA	シーエスエー	control self-assessment	『内部統制』の有効性が検証され評価される、業務に携わる者が自ら行う自己評価のプロセスのこと（米国内部監査人協会（IIA））	米国内部監査人協会（IIA）は、CSAとは「内部統制の有効性が検証され、評価されるプロセスである。この目的とは、すべてのビジネス目的が達成されるであろうという合理的な保証を与えるものである」と定義している。 内部統制は、業務遂行上でのリスクを識別しその上でリスクを軽減する為の統制を相対させる事により組み立てられているが、その有効性は、リスクとリスクに相対する統制とが正しく識別されている事が前提となっている。このリスクと統制とを評価する方法の一つがCSAである。 日本語で「統制自己評価」と訳せるように、CSAでは、業務に携わる者が自ら業務上のリスクの認識とそのリスクを是正あるいは発現阻止をする手段としての統制の有効性を評価する。			
85	CMMI	シーエムエムアイ	Capability Maturity Model Integration	ソフトウェア開発の組織成熟度を評価する手法のこと	CMMIは、1990年代から米カーネギーメロン大学ソフトウェア工学研究所が開発したソフトウェア開発プロセスの改善モデルとアセスメント手法であるCMMを改良したものである。CMMがソフトウェアの開発、運用、保守の生産性を向上させるため、チームや組織の連携により、発展的に問題点を克服し改善していく能力（成熟度）の向上を図る仕組みであるのに対し、CMMIはプロセス及び製品改善を支援し、独立したそれぞれのモデルを用いる際に起きる不一致をなくし、重複を減らすことを意図している。 このためCMMIは、システムエンジニリング、ソフトウェアエンジニアリング、ソフトウェア調達など、CMMより多くの分野をカバーしており、システム開発やソフトウェア開発及びそれらの調達におけるプロセス改善と供給者能力評価に使用できる。	現行用語集		
86	事業継続計画	ジギョウケイゾクケイカク	Business Continuity Plan	企業存続の生命線である「事業継続」を死守するための行動計画のこと。 （経済産業省商務情報政策局「企業における情報セキュリティガバナンスのあり方に関する研究会報告書　参考資料「事業継続計画策定ガイドライン」平成１７年６月」）	日本では、地震、火災・爆発、大規模なシステム障害などが相次ぎ、基幹となる事業の停止に追い込まれるケースが見られる中、BCP（Business Continuity Plan）及びBCM(Business Continuity Management)を構築することが望まれている。 BCPとBCMとは、事故や災害などが発生した際に、「如何に事業を継続させるか」若しくは「如何に事業を目標として設定した時間内に再開させるか」について様々な観点から対策を講じることであり、BCPはそのための計画自体のこと、BCMは、BCPの策定から運用、見直しまでのマネジメントシステム全体を指すものである。 （「事業継続計画策定ガイドライン」） 【経済産業省商務情報政策局「事業継続計画策定ガイドライン」】 主に突発的なIT事故の発生を対象した対策のガイドライン。 個々の企業等におけるBCPにて具体的に盛り込むべき項目について各フェーズ毎に具体的に記述されている。 （目次） 第Ⅰ章　基本的考え方 第Ⅱ章　総論（フレームワーク） 第Ⅲ章　BCP策定に当たっての検討項目 ３．１　検討項目の全体像とポイント ３．２　BCPの実施体制 ３．３　BCP発動フェーズにおける対応のポイント ３．４　業務再開フェーズにおける対応のポイント ３．５　業務回復フェーズい置ける対応のポイント ３．６　全面回復フェーズにおける対応のポイント ３．７　リスクコミュニケーションの重要性 第Ⅳ章　個別計画（ケーススタディ） 【経済産業省／中小企業庁「BCP策定のためのヒント」】 中小企業が緊急事態を生き抜くために。 （目次） 第Ⅰ部　BCP初版作成までの道のり 第Ⅱ部　もしも大規模地震等に見舞われたら 第Ⅲ部　緊急事態に強い会社を作る BCP策定のワンポイント解説			シラバス

No	用語	日本語読み	英文名	定義（又は説明）	解説	source	区分1	区分2
87	CISA	シサ	Certified Information Systems Auditor	米国のISACA（Information Systems Audit and Control Association）の実施するCISA試験の合格者に対し一定の実務経験を条件に認定される資格保持者のこと	CISA試験は、情報システム監査、コントロールおよびセキュリティの実務能力をテストするもので、200問の多肢選択式問題(４時間)からなる。世界各国で受験可能で日本では、日本語で受験できる。CISAは日本語で「公認情報システム監査人」と訳されている。なお、ISACA(情報システムコントロール協会)は、情報システムの安全性・有効性向上、システム監査の普及等を目的とした非営利団体で、米国イリノイ州に本部があり、日本には東京、名古屋、大阪に支部がある。 資格を維持するためには、毎年所定時間以上の継続教育活動を実践し報告する必要がある。 試験の運営は、米国本部と各支部が担当している。(別掲参考URL参照)	現行用語集		
88	試査	シサ		監査目標ごとに監査対象項目の一部に対してのみ監査手続を適用し、その結果に基づいて監査対象項目全件の状況を推定すること	試査とは、監査対象の一部を抽出して検討し、その適否をもって監査対象全体の適否を推定的に立証する方法である。試査の範囲を決定するためには、立証すべき監査テーマを設定し、入手すべき証拠資料の範囲を決定する必要がある。 試査の範囲を決定する方法としては、以下のものがある。 ・サンプリングによる試査 母集団の特性を代表するサンプルに対する監査手続の結果から、母集団全体の一定の特性を推定して母集団に関する結論を得る方法である。 ・特定項目抽出による試査 母集団に含まれる特定の性質を有する項目を識別して抽出し、これに対して監査手続を実施する方法である。 ・経験的試査 監査人が、内部統制の状況や監査対象の重要性、監査上の危険性、過去の実績等を考慮した経験的判断により、試査の範囲を決定し、監査手続の適用の結果を評価する方法である。 ・統計的試査 統計理論に基づいて決定されたサンプル数を無作為に抽出して検査し、サンプル結果を確率論に基づいて評価する方法である。	現行用語集		
89	システム監査	システムカンサ	ｓｙｓｔｅｍ audit	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ガバナンスの実現に寄与する活動のこと	この定義は、『システム監査基準（2004.10改訂）』にある「システム監査の目的」の記述から引用している。「情報セキュリティ監査基準(2003.4策定)」の情報セキュリティ監査の考え方と整合性をとっているので、別項の『情報セキュリティ監査制度』の項も参照のこと。以下若干の補足をして解説とする。 システム監査の対象は、電子計算機とネットワークを中核とした情報システム及びそのライフサイクルプロセスであり、情報及びデータの収集・作成から活用・管理・廃棄までの全てのプロセスを含むものである。これを「情報システム」と総称している。 また、情報システムは組織体の目標達成に役立つ情報及び業務処理を提供することを使命とするが、システム監査はその使命の達成に貢献することを目的とする。そしてその結果として組織体の『ITガバナンス』の実現に、また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の説明責任を果たすことに寄与することとなる。 適切であるか否かを問われる情報システムにまつわるリスクに対するコントロールの目的は、システム監査基準の前文に次の四つにわけて示されている。 ①情報システムが、組織体の経営方針及び戦略目標の実現に貢献するため ②情報システムが、組織体の目的を実現するように安全、有効かつ効率的に機能するため ③情報システムが、内部又は外部に報告する情報の信頼性を保つように機能するため ④情報システムが、関連法令、契約又は内部規程等に準拠するようにするため なお、『金融機関等のシステム監査指針（平成19年改訂第3版）』ではシステム監査を「情報システムの有効性、効率性、信頼性、安全性、及び遵守性を達成できるよう、情報システムリスクを把握し、情報システムに係るコントロール（ＩＴガバナンスを含む場合もある）が適切かつ効果的であることを、被監査部門から組織的に独立したシステム監査人が検証し、その結果を保証意見又は助言勧告としてとりまとめ、経営者に報告する監査」と定義している。	現行用語集		シラバス
90	システム監査企業台帳	システムカンサキギョウダイチョウ		システム監査を組織体の外部に委託する場合に参考にできるよう「システム監査企業に関する規則」（1991.3制定）により経済産業省に登録されたシステム監査を実施できる企業の台帳のこと	台帳を閲覧できるところは、従来は同省情報処理振興課、各地通産局機械情報産業課、都道府県立図書館、全国の商工会議所等であったが、現在はWebで公開されている。現在140社前後の企業が登録されているが、それぞれ「企業概要」、「システム監査実施の実績」、「システム監査従事者の概要」、「システム監査の得意分野、特色」等が記載されている。 なお2003年より情報セキュリティ監査を実施する企業の任意登録制度として「情報セキュリティ監査企業台帳」が創設されている。	現行用語集		

No	用語	日本語読み	英文名	定義（又は説明）	解説	source	区分1	区分2
91	システム監査技術者	システムカンサギジュツシャ		情報処理技術者試験（経済産業省が認定している国家試験）におけるシステム監査技術者試験の合格者のこと	システム監査技術者とは、「情報処理の促進に関する法律」に基づき経済産業省が、情報処理技術者としての「知識・技能」の水準が或る程度以上であることを認定している国家試験の中で、高度試験に位置づけられているシステム監査技術者試験の合格者のことである。 システム監査を普及するためには、システム監査人の養成が必要であり、そのための通産省・経済産業省の施策として能力認定試験（1986年以降）が行われてきた。当初「情報処理システム監査技術者試験」の名称であったが、1994年から現在の「システム監査技術者試験」となっている。その間、高度情報化人材育成標準カリキュラムに基づく育成カリキュラムに準拠した試験へ、更に現在の出題範囲、スキル標準の策定・公表による試験の実施に変わるなど制度改善が行われてきた。 試験(2009年春より)は、午前問題は午前Ⅰと午前Ⅱから構成される。前者は30問(50分)で高度試験に共通であり、技術レベル3の問題をテクノロジ系、マネジメント系、ストラテジ系から幅広く出題している。後者は25問(40分)でシステム監査に特化した技術レベル3または4の問題を出題している。何れも多肢選択式(四肢択一)で全問解答である。午後問題は午後Ⅰと午後Ⅱから構成される。前者は4問中2問選択記述式(90分)、後者は3問中１問選択論述式(小論文、120分)である。「合格率は新旧制度累計で平均7.6%」となり、情報処理技術者試験の中で最も難しい試験の一つとされる。2011年春までの累計合格者は8,417人に達している。 なお、本試験制度の運営は独立行政法人情報処理推進機構:情報処理技術者試験センター（別掲参考URL参照）が行っている。(Information-technology Promotion Agency, Japan=IPA)	現行用語集		シラバス
92	システム監査基準	システムカンサキジュン		経済産業省により策定公表されているもので、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システム監査人の「行為規範」を示した基準のこと	1985年通産省（当時）によって策定され公表されたもので、システム監査に必要な事項を網羅的に示すガイドラインとしての役割を果たしてきた。1996年１月に第１回の改訂、そして今回2004年10月８日に第２回の改訂が公表された。改訂の内容はIT投資の目的が現場の合理化から経営革新へと大きく変化するなか、国際的動向も踏まえたものとなり、旧システム監査基準の実施基準の主要部分を抜き出して、『システム管理基準』に独立させた。それは組織体のシステムリスク低減のための実践規範、システム監査人の「判断の尺度」に位置付けられている。 スリムになった新システム監査基準は、監査人の行為規範として位置付けられ、組織体の内部監査部門等が実施するシステム監査だけでなく、外部に監査を依頼するシステム監査においても利用できる。また保証型監査であっても、助言型監査でも利用できる内容である。 その構成は、次のようになっている。 ①前文 システム監査の位置づけ、性格、システム管理基準の関係等の記述 ②システム監査の目的 システム監査の目的の記述 ③一般基準（８項目） システム監査人としての適格性及び監査業務上の遵守事項を規定 ④実施基準（７項目） 監査計画の立案及び監査手続の適用方法を中心に監査実施上の枠組みを規定 ⑤報告基準（５項目） 監査報告に係る留意事項と監査報告書の記載方式を規定	現行用語集	基準	

No	用語	日本語読み	英文名	定義（又は説明）	解説	source	区分1	区分2
93	システム監査規程・マニュアル	システムカンサキテイ・マニュアル		システム監査人がシステム監査を実施するに当たって、必要とするすべての規定や手順書類のこと	システム監査マニュアルは、システム監査の品質向上や効率性向上、システム監査人の育成のために、有効である。 監査マニュアルとしては、以下のものが挙げられる。 ・システム監査規程 ・システム監査実施要領 ・システム監査報告要領 ・システム管理実施基準 ・チェックリスト ・各種ドキュメントフォーム ・システム監査ツール使用マニュアル 等 監査マニュアルの記述内容としては、以下の項目が挙げられる。 ・システム監査の目的 ・システム監査の対象（組織、業務、情報資産等） ・システム監査人の役割、責任、権限 ・システム監査人の資格要件、教育、訓練 ・システム監査人の倫理規定 ・システム監査計画書の作成基準 ・システム監査実施基準 ・システム監査調書の作成基準 ・システム監査報告書の作成基準 ・システム監査結果のフォローアップ ・システム監査人の判断の尺度としてのシステム管理基準 ・他監査との調整指針 ・関連法制度、基準　等	現行用語集		
94	システム監査技法	システムカンサギホウ		システム監査を実施する際に適用する監査技法のこと	システム監査技法には、例えば、チェックリスト法、ドキュメントレビュー法、突合・照合法、現地調査法、インタビュー法などがある。一般的に監査技法は、システム監査にも適用されるが、ベネトレーションテストやグラフィックボックスチェックはシステム監査独自の技法である。システム監査技法にはそれぞれ長所・短所があるので、監査目標やシステム環境などの状況に応じて適切なシステム監査技法を適用すること。			シラバス
95	システム監査計画	システムカンサケイカク	syatem audit plan	システム監査を実施する計画のこと	システム監査の実施に当たっては、組織体の経営目的との適合性を明確にして監査の効果をあげ、かつ監査業務の効率化を図るための監査計画を立案する。監査計画は、基本計画と個別計画に分けて策定する。			
96	システム監査人の独立性	システムカンサニンノドクリツセイ		システム監査を客観的に実施するために、システム監査人は監査対象から外観上または精神上の独立性を有していること	システム監査が常に公正かつ客観的に実施されるためには、システム監査人の独立性が要求される。そのためには、システム監査人が被監査主体である情報システム部門はもちろんユーザ部門などから、外観上も精神上でも独立性を保持していることが必要である。 『システム監査基準』ではその一般基準の中で、「外観上の独立性」と「精神上の独立性」について、項を分けて定めている。	現行用語集		

No	用語	日本語読み	英文名	定義（又は説明）	解説	source	区分1	区分2
97	システム管理基準	システムカンリキジュン	system management standards	経済産業省により新たに策定公表されたもので、組織体が主体的に経営戦略に沿って効果的な情報戦略を立案し、その戦略に基づき情報システムの企画・開発・運用・保守というライフサイクルの中で、効果的な情報システム投資のための、またリスクを低減するためのコントロールを適切に整備・運用するための実践規範であり、同時にシステム監査人の監査上の「判断の尺度」として位置付けられている基準のこと	経済産業省は2004年10月に『システム監査基準』の２回目の改訂を公表した。改訂の内容はIT投資の目的が現場の合理化から経営革新へと大きく変化するなか、国際的動向も踏まえ、システム監査基準の中の実施基準の主要部分を抜き出して、「システム管理基準」として独立させ、「システム監査基準」とともに姉妹編を構成することとなった。 この「システム管理基準」は、上述のように組織体の実践規範と位置づけられると同時に、システム管理基準に従ってシステム監査を実施する場合のシステム監査人の「判断の尺度」となる基準でもある。なお、情報セキュリティの確保の観点からの監査に際しては、情報セキュリティ管理基準の活用が望ましいとされている。 システム管理基準を分離した「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システム監査人の「行為規範」として位置付けられる。 システム管理基準の構成は、前文に続いて次のようになっている。 ①情報戦略(47項目) ②企画業務(23項目) ③開発業務(49項目) ④運用業務(73項目) ⑤保守業務(19項目) ⑥共通業務(76項目) また、金融庁企業会計審議会内部統制部会が策定した「財務報告に係る内部統制の評価及び監査の基準」及び「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」における内部統制の基本的要素の１つとしての「ITへの対応」に対応するために、経済産業省より平成19年3月に「システム管理基準追補版（財務報告に係るIT統制ガイダンス）が公表されている。	現行用語集	基準	
98	実査	ジッサ		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きのこと	実査は、会計分野の専門用語であり、その意味は、企業の現物のある資産について、実際の存在、数量、使用状況等を確認する手続きのことである。一般には、現金や受取手形等がその適用範囲であるが、棚卸資産や有形固定資産等にも必要に応じて適用される。 システム監査の観点で見ると、情報資産についての実際の存在、数量、使用状況等を確認する手続きということになる。	現行用語集		
99	実施基準	ジッシキジュン		システム監査計画の立案及びシステム監査手続きの適用方法を中心にシステム監査実施上の枠組みを規定した基準のこと	システム監査基準において、システム監査が適切に実施されるように監査計画の立案、監査手順、監査対象等のシステム監査の実施に必要な手続きの遵守事項として、次の６項目を実施基準として定めている。 １．監査計画の立案 ２．監査の手順 ３．監査の実施 ４．監査業務の体制 ５．他の専門職の利用 ６．情報セキュリティ監査		基準	

No	用語	日本語読み	英文名	定義（又は説明）	解説	source	区分1	区分2
100	実証性調査	ジッショウセイチョウサ		情報システムの生成するデータ、意思決定者の利用度、情報システムが使用している資源等の直接的に検証すること	システム監査における実証性調査では、監査の効率性、経済性、正確性の観点より調査する。 また、実証性調査の技法としては、以下のものがある。 ・コンピュータを利用しない場合 ①再実行 ある種の判断が行為の基礎となっている場合に、結果が同じになるかどうかを確認すること。 ②実査 記録された最終結果と現状の物理的な比較をすること。 ③証憑突合 記録された最終結果より、その起因となった取引、トランザクションを示す伝票類にさかのぼり突き合せること。 ④構成分析 最終結果を分類、集計することによって、その内容の理解を深めること。 ⑤照合調整 本来一致すべき２つの数字の間の違いを明確にし、説明すること。 ⑥カットオフテスト 取引、トランザクションが適切な期間に記録されているか判断するために書類等を検査すること。 ・CAATを適用する場合 ①汎用監査ソフトウェア法 ②ユーティリティ・ソフトウェア法 ③専用監査プログラム法 実証性テストの実施にCAATを適用する場合の留意点は、以下のとおりである。 －監査目的にあった明細の記録されているファイルを確保する。 －ファイルとして入手したデータの合計値を確定する。 －原始データのサンプリング自体の正確性と妥当性を、その証拠能力に応じて適時にテストする。 －上記のステップで信頼性が確認されたファイルのデータを監査人の汎用監査プログラム等を用いて、並行シミュレーションなどにより実行する。 －例外データ、危険項目等の以上項目のみを論理的に抽出し、効果的な監査を実施することができる。－計算、突合せ等の再実行は、全データに対して容易に実施することができる。	現行用語集		
101	指摘事項	シテキジコウ		システム監査人が、『予備調査』および『本調査』の結果を踏まえ、自ら設定した合理的な判断基準に基づいて問題であると判断した事項のこと	システム監査人は、『予備調査』および『本調査』を通じて入手した『監査証拠』を『監査目的』に照らして分析・評価し、その結果をシステム監査報告書にまとめて『監査依頼者』に報告する。システム監査人は、『監査証拠』を分析・評価した結果として、『監査対象』において問題であると判断した事項を、システム監査報告書に記載する。これが指摘事項である。 システム監査人は、『予備調査』および『本調査』の結果、『監査対象』において問題であると判断した事項は、小さな問題であっても指摘すべきである。小さな問題であっても、将来大きな問題に発展する可能性もあるからである。 ここでいう「問題」とは、監査計画で設定した監査基準と調査した結果とのギャップである。そして、定義にある「判断基準」には、次のようなものが含まれる。 ・調査によって分かった事実がギャップに該当するかどかの判断基準 ・ギャップを指摘事項にするかどうかの判断基準 ・指摘事項を改善事項にするかどうかの判断基準 ・改善事項を緊急改善と通常改善に切り分けるときの判断基準 定義で「自ら設定した判断基準」といっているが、監査実施組織が所属するシステム監査人の経験を集めて、監査実施組織としての判断基準を設けることは、判断の均質化が図れて有効である。 システム監査人は、システム監査報告書に指摘事項を記載するにあたって、以下の点に留意が必要である。 ・問題であることの『監査証拠』による明確な裏付け ・被監査部門との意見交換による問題点についての事実誤認の排除と共通認識の確立 なお、監査テーマとは直接関係ない事項について、『予備調査』、『本調査』を通じてシステム監査人が知り得た事実のうち、システム監査人が『監査依頼者』に報告した方がよいと判断したことがあれば、補足意見という形でシステム監査報告書に記述して報告することがある。	現行用語集	基準	シラバス

No	用語	日本語読み	英文名	定義（又は説明）	解説	source	区分1	区分2
102	修正回復機能	シュウセイカイフクキノウ	recovery control	業務処理の過程で誤謬や不正を発見した場合に、速やかな修正・回復を図り、組織体の業務活動に与える影響を最小限にとどめる機能のこと	修正回復機能は業務処理の過程で誤謬や不正を発見した場合に、速やかな修正・回復を図り、組織体の業務活動に与える影響を最小限にとどめる機能である。 例えば、障害などの異常が発生した場合に、正常な元の状態に修復するための平均修復時間などの指標を使って、システムの保守の指針としても活用される。修正回復機能は、誤謬や不正が検出されることを前提として、検出機能と組み合わせて利用する。 また、修正回復機能は、日常的な回復機能と緊急回復機能に分けて考えるとよい。日常回復機能は、発生頻度の高いデータの不整合や誤謬を修正する機能で、緊急回復機能は災害発生時など、発生するとダメージが大きく、回復にも多くの時間や費用を要する場合の対応である。 いずれの場合も、事前に対応可能な回復手続を定めておくことが重要である。	現行用語集		
103	守秘義務	シュヒギム	obligation to keep secrets	『機密性』のある情報を職務上知り得る立場にある者が、その情報を故意や過失により第三者に開示しないよう努める義務のこと	守秘義務はシステム監査人のように『機密性』の高い情報を職務上知り得る立場にある者が、その情報を故意や過失により第三者に開示しないようつとめる義務である。システム監査上で知りえた秘密は漏らさない、監査の目的以外に利用しない、また第三者に利用されるような状況に置かないことが大切である。システム監査人は職業的専門家としての正当な注意を払い、入手する情報を扱い、保管することが期待されており義務がある。守秘義務を確認するため、一般にはNDA（秘密保持契約書）を相互に交わして会話や情報交換を始める。 なお、守秘義務に関し、システム監査基準では、次のように定めている。 「システム監査人は、監査の業務上知り得た秘密を正当な理由なく他に開示し、又は、自らの利益のために利用してはならない。」	現行用語集	基準	
104	準拠性	ジュンキョセイ	compliance	情報システムの開発や運用、情報システムの利用が、法規制や外部のルール、組織内部の方針やルールに沿って実施されていること	準拠性とは、情報システムの開発や運用、情報システムの利用が、法律・規則や外部のルール、組織内部の方針やルールに適合し、運用されていることである。 情報システムの開発や運用、情報システムの利用は、法規制や所属する業界や地域社会などの外部のルールに従うことで適法性を維持し違法性から逃れ、利用者の信頼を得る。	現行用語集		シラバス
105	準拠性調査	ジュンキョセイチョウサ		経営管理者によって設定されたコントロール（規定およびマニュアル類に規定されている事項）の整備および運用状況を検証すること	システム監査における準拠性調査では、情報システムの運用手続きやプログラムの処理の妥当性を内部統制の観点より調査する。 また、準拠性調査の技法としては、以下のものがある。 ・コンピュータを利用しない場合 ①証拠の調査 記録、書類、報告書等のように、特定のコントロールが正しく適用されたことを示す証拠を調査すること。 ②再実行 ある種の判断が行為の基礎となっている場合に、結果が同じになるかどうかを確認すること。 ③視察 実際の業務の実施されている現場に行き、内部統制が守られていることを確かめること。 ・CAATを適用する場合 ①テストデータ法 ②ITF法 ③並行シミュレーション法 ④汎用監査ソフトウェア法 ⑤コード比較法 ⑥監査モジュール法 準拠性テストの実施にCAATを適用する場合の留意点は、以下のとおりである。 －情報システムの処理フローを十分分析し、監査目的、コントロール、実証性テストによる監査手続との関連、監査リスク等を考慮して、対象とする運用手続き、プログラム処理手続きを決定する。 －対象とする運用手続き、プログラム処理手続きに対しては、さらに運用フロー、システムフロー等を参照のうえ分析し、対象とすべき運用手続き名、プログラム名、マスターファイル名、取引ファイル名、入出力帳票、画面等を明確にする。 －単純なプログラム処理の場合は、監査人自らプログラムを作成し、並行シミュレーションにより監査するのが効率的である。 －複雑なプログラムの場合は、種々の技法を複合的に利用する。	現行用語集		

No	用語	日本語読み	英文名	定義（又は説明）	解説	source	区分1	区分2
106	情報システム計画	ジョウホウシステムケイカク		『情報戦略』に基づき中長期あるいは年度単位に立てられた情報システム化に関する計画のこと（情報処理推進機構「システム監査技術者試験シラバス」[2009年]より）	シラバスでは、「システム監査の計画」の「中長期計画書の作成」、「基本計画書の作成」の各々の概要の項で、「中長期の経営計画、情報戦略、情報システム計画」、「年度の経営計画書及び情報システム計画書」に対応した各監査計画書を作成することとしている。 　中長期の情報システム計画は、経営戦略に基づいて策定された情報戦略に沿った中長期レンジでの情報システム化の計画であり、年度の情報システム計画はそのうちの年度単位のものとなる。 情報戦略で立てられた方針に基づき、個々の開発計画を計画期間内でどのように進めて行くのかを示したものであり、策定に当たっては、情報戦略で示されている全体最適化の方針・目標に沿って投資効果分析、リスク算定、優先付けを行う事が必要である。			シラバス
107	情報セキュリティマネジメントシステム	ジョウホウセキュイｒティマネジメントシステム	information security management system	個別の問題毎の技術対策の他に、組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源配分して、システムを運用すること	一般財団法人日本情報経済社会推進協会（以下JIPDEC）で運用している「ISMS適合性評価制度（Version2.0 H15.4.1）」では、企業・組織が自らの事業の活動全般およびリスク全般を考慮して文書化したISMSを構築、導入、維持し、かつこれを継続的に改善していくプロセスとしている。ISMSの基準で使われるプロセスは、次の図に示すPDCAモデルに基づいている。（以下JIPDECのISMSパンフレットから抜粋） １）「１．ISMSとは」の文言を以下のものと差替え （JIPDEC「ISMS適合性評価制度の概要」を適切な参照資料と判断し、差替えた） ISMS適合性評価制度（Version2.0 H15.4.1）」→「ISMS適合性評価制度（JIS Q 27001:2006（ISO/IEC 27001:2005）対応版）」 「●機密性：認可されていない個人、エンティティ（団体等）又はプロセスに対して、情報を使用不可又は非公開にする特性」 「●完全性：資産の正確さ及び完全さを保護する特性」 「●可用性：認可されたエンティティ（団体等）が要求したときに、アクセス及び使用が可能である特性」 （JIPDEC ISMS適合性評価制度の概要より引用）	現行用語集		
108	情報セキュリティ	ジョウホウセキュリティ	information security	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よい（JIS Q 27002:2006より引用）	組織経営に不可欠である情報は、適切に保護されなければならない。情報が適切に保護されていないと、漏洩したり、内容が不正確であったり、必要なときに使えない等、業務の遂行に支障をきたすリスクが発生する。情報セキュリティとは重要な情報をこのようなリスクから守ることをいう。また、機密性、完全性、可用性を指して情報セキュリティの３要素ともいう。関連用語：機密性、完全性、可用性の定義を参照。	現行用語集		シラバス
109	情報セキュリティ監査	ジョウホウセキュリティカンサ	information security audit	情報セキュリティ監査人が、独立かつ専門的な立場から、組織体の情報セキュリティの状況を検証又は評価して、情報セキュリティの適切性を保証し、情報セキュリティの改善に役立つ的確な助言を行うこと	情報セキュリティ監査の実施に当たっては、組織体における情報セキュリティの適否を判断するための尺度が必要である。情報セキュリティ監査の代表的な基準としては、情報セキュリティ監査基準と情報セキュリティ管理基準がある。 監査上の判断の尺度として情報セキュリティ管理基準を用い、監査対象が情報セキュリティ管理基準に準拠しているかどうかという視点で行われることを原則とする。また、情報セキュリティ監査人の行為規範を定めている情報セキュリティ監査基準には、情報セキュリティ監査の目的も定めている。監査基準では、監査の目的を、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人が独立かつ専門的な立場から検証又は評価して、もって保証を与えあるいは助言を行うことにあるとしている。 情報セキュリティのマネジメントは第一義的には組織体の責任において行われるべきものであり、情報セキュリティ監査は組織体のマネジメントが有効に行われることを保証又は助言を通じて支援するものである。 情報セキュリティ監査は、情報セキュリティに係るリスクのマネジメント又はコントロールを対象として行われるものであるが、具体的に設定される監査の目的と監査の対象は監査依頼者の要請に応じたものでなければならない。 情報セキュリティ監査人の行為規範を定めている基準としては情報セキュリティ監査基準が定められているが、本監査基準の姉妹編である	現行用語集		シラバス

No	用語	日本語読み	英文名	定義（又は説明）	解説	source	区分1	区分2
110	情報セキュリティ監査基準	ジョウホウセキュリティカンサキジュン		経済産業省により告示されているもので、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を定めた基準のこと	2003年経済産業省によって告示され公表されたもので、情報セキュリティ監査に必要な事項を網羅的に示すガイドラインである。 その構成は、次のようになっている。 ①前文 情報セキュリティ監査の位置づけ、性格、情報セキュリティ管理基準等のの関係の記述 ②情報セキュリティ監査の目的 情報セキュリティ監査の目的の記述 ③一般基準（５項目） 情報セキュリティ監査人としての適格性及び監査業務上の遵守事項を規定 ④実施基準（４項目） 監査計画の立案、監査の実施、監査業務の体制等を規定 ⑤報告基準（５項目） 監査報告書の提出、監査報告の根拠、監査報告書の記載事項、監査報告についての責任等を規定		基準	
111	情報セキュリティ監査制度	ジョウホウセキュリティカンサセイド		情報セキュリティ監査を行うために制度化された情報セキュリティ監査基準、同管理基準、同監査企業台帳など一連の経済産業省の施策のこと	情報セキュリティ監査は「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人が独立かつ専門的な立場から検証又は評価して、もって保証を与えあるいは助言を行うこと」と定義できる。これは、2003年4月に策定された情報セキュリティ監査基準に定められている。経済産業省は2002年9月より諮問研究会として「情報セキュリティ監査研究会」を設置して検討を行い、その成果としてこの監査制度が出来あがった(2003.3.26)。 その主な点は、①情報セキュリティ監査のあり方、②情報セキュリティ監査の標準的な基準と監査主体のあり方、③電子政府に対する情報セキュリティ監査のあり方、それぞれへの提示であった。 情報セキュリティ監査制度の構成としては、以下のとおりである。 1.情報セキュリティ監査企業台帳 ①情報セキュリティ監査企業台帳（2009年8月更新） ②情報セキュリティ監査企業台帳に関する規則（平成15年経済産業省告示第113号） 2.基準等（PDF形式またはWord／Excel形式でダウンロード可能） ①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） ②情報セキュリティ管理基準（平成20年改正版）管理策基準 ③個別管理基準（監査項目）策定ガイドライン ③電子政府情報セキュリティ管理基準モデル ④情報セキュリティ監査基準（平成15年経済産業省告示第114号） ⑤情報セキュリティ監査基準実施基準ガイドライン ⑥情報セキュリティ監査基準報告基準ガイドライン【 ⑦電子政府情報セキュリティ監査基準モデル ⑧情報セキュリティ監査手続ガイドライン ⑨情報セキュリティ監査手続ガイドラインを利用した監査手続策定の手引 なお、本制度の運用開始を受け、監査企業や監査人、一般企業や団体が一同に会して特定非営利活動法人日本セキュリティ監査協会(Japan information Security Audit association=JASA)を設立している(2002年２月、別掲参考URL参照)。 また、同協会は「公認情報セキュリティ監査人」資格制度（英語名称：Certified Auditor for Information Security 略称： CAISケイズ）を創設した。同協会内に資格認定委員会を組織し、資格制度の運用ならびに資格認定を行うとともに、2004年12月から資格認定の前提となる知識・経験を修得するための研修・トレーニングコースの開催、2005年2月より認定を始めている。	現行用語集		

No	用語	日本語読み	英文名	定義（又は説明）	解説	source	区分1	区分2
112	情報セキュリティポリシー	ジョウホウセキュリティポリシー	information security policy	企業・組織が自己の保有する情報資産に対して、情報セキュリティを確保するための全般的な方向性および行動指針を規定したもの	情報セキュリティ基本方針ともいう。ここで定義する情報セキュリティポリシーの体系は、最上位に情報セキュリティ基本方針、次に情報セキュリティ基準、最後に情報セキュリティ実施基準の３階層からなる。情報処理技術者試験においては、情報セキュリティ基本方針と情報セキュリティ基準の２階層を合わせて情報セキュリティポリシー（広義のセキュリティポリシー）と位置付けている。 以下、JIPDEC（一般財団法人日本情報経済社会推進協会）で運用する情報セキュリティマネジメントシステム（以下ISMSという）適合性評価制度に基づき解説する。 （１）情報資産については、電子化されたデータのほか、紙ベースの情報、音声・画像等のデータも含まれる。対象とする情報資産はISMSの適用範囲で定義する。 （２）情報セキュリティの確保とは、情報資産に対する機密性、完全性、可用性を確保することをいう。 （３）情報セキュリティポリシーは、次の項目を満たす必要がある。 ①ISMSの目標を設定するための枠組みを含み、情報セキュリティに関する全般的な方向性および行動指針を確立すること。 ②事業上の要求事項および法的または規制要求事項、並びに契約上のセキュリティ義務を考慮すること。 ③ISMSを確立し、維持するために必要な戦略上の視点からみた組織環境、並びにリスクマネジメントのための環境を整備すること。 ④リスクを評価するための基準を確立し、定義されたリスクアセスメントの構造を確立すること。 ⑤経営陣（社長、情報セキュリティ担当役員などの上位経営管理者）による承認を得ること。	現行用語集		シラバス
113	情報戦略	ジョウホウセンリャク		情報システム全体の最適化目標を経営戦略に基づいて設定した戦略のこと（「システム管理基準」経済産業省商務情報政策局セキュリティ政策室・平成16年10月6日編より）	組織体の情報化に関する基本方針を定めたものが情報戦略であるが、今日では情報化の対象領域が社内事務中心からインターネットの普及などで直接、顧客や組織体外の関連者に広がって来ていることから、組織体の経営目標とそれを支える情報戦略とはより密接な関係となって来ている。 『システム管理基準』では、情報戦略における「全体最適化の方針・目標」として次の６点をあげ、情報戦略は経営戦略に基づいて全体最適化を図るべきこととしている。 （１）ITガバナンスの方針を明確にすること。 （２）情報化投資及び情報化構想の決定における原則を定めること。 （３）情報システム全体の最適化目標を経営戦略に基づいて設定すること。 （４）組織体全体の情報システムのあるべき姿を明確にすること。 （５）システム化によって生ずる組織及び業務の変更の方針を明確にすること。 （６）情報セキュリティ基本方針を明確にすること。			シラバス
114	除外事項	ジョガイジコウ		監査意見の表明に当たって、重要な影響を与える可能性のある事項のこと	システム監査基準においては、「除外事項」の具体的な内容は記載されておらず、上記の定義は、財務諸表監査に関するものである。しかしながら、システム監査においても、保証型意見の表明に際し「除外事項」という用語を財務諸表監査の場合と同様の意味で用いられている。因みに、「システム監査基準」（昭和60年１月策定、平成8年1月30日・平成16年10月8日改訂）の「V．報告基準」では、「３．監査報告書の記載事項」として、「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。」と定められている。		基準	
115	職業倫理	ショクギョウリンリ	professional ethics	監査人が専門家として備えるべき特定の使命、社会的責任あるいは行動規範のこと	職業倫理はシステム監査人などの特定職業に携わる専門家が備える特定の使命、社会的責任あるいは行動規範、また倫理的な活動規範のことである。システム監査人には倫理基準の遵守、守秘、公正不偏の態度、独立性等が要求される。 倫理は組織の倫理と個人の倫理とに区分され、組織の倫理は会社の構成員がある特定の行為を行うような組織の定義や規則のこと。また、個人の倫理とは、個人がある特定の行為を行う上での氏名、責務、社会的責任や倫理観をいう。ここでは、職業倫理は、特定の職業に従事する者が備えるべき倫理事項であり、個人の倫理を問う。 例えば、倫理は次のような場合に問題になる。 ・倫理上の問題についての一般的なビジネス上の理解 ・法規の遵守 ・利害衝突 ・接待費および贈与にかかる費用 ・顧客とサプライヤーとの関係（贈与やキックバックを与えたり、受け入れたりすること） ・社会的責任 なお、職業倫理についてシステム監査基準では、次のように定めている。 「システム監査人は、職業倫理に従い、誠実に業務を実施しなければならない」 システム監査学会では「倫理綱領」を、日本システム監査人協会では「システム監査人倫理規定」を定めている。	現行用語集	基準	シラバス

No	用語	日本語読み	英文名	定義（又は説明）	解説	source	区分1	区分2
116	職務権限	ショクムケンゲン	job functions	組織および職位ごとに定めた、職務上の指示・実行の及ぶ範囲と責任のこと	職務権限は、組織および職位ごとに定めた、職務上の指揮命令・指示・実行の及ぶ範囲のことで、通常、職務権限規程で明文化されている。 権限には責任が付随し、その責任は、職務遂行責任（Obligation）・結果責任（Responsibility）・報告責任（Accountability）に分類される。このうち結果責任・報告責任の追及されない権限は、濫用に繋がる。職務権限を明確にしないことによって、指揮命令系統が混乱したり、権限が特定個人に偏重したりすることによる影響は大きい。業務が円滑に進まないだけでなく、不正や誤謬が発生するリスクが高まる。小規模組織では、これらを兼務することがあるが、組織の規模がある程度大きくなってきた段階で『職務分掌』・職務権限を明らかにすることが重要である。	現行用語集		
117	職務の分離	ショクムノブンリ	segregation of duties	『相互牽制』の観点から、職務をある組織または然るべき職位の要員に割当て、１つの職務を２つの組織が交互に行ったり、１人の担当者が２つ以上の職務を兼ねることのないようにすること	職務の分離は、『相互牽制』の観点から、職務をある組織または然るべき職位の要員に割当てコントロールすること。 例えば、次のようなコントロールが該当する。 ・１人の担当者が２つ以上の職務を兼ねることのないようにする（申請と承認、実行と監視） ・２人以上担当者が検査して処理する（入力と処理） ・１つの職務を２つの組織が交互に行なう（検査） このように仕事上の責任を分散させることで、処理の誤りや違反行為を予防し、誤りや違反の事実を発見することができる。	現行用語集		
118	職務分掌	ショクムブンショウ	job duty	組織および組織を構成する役割や要員ごとの、業務処理過程における職務分担および責任・権限に関する定めのこと	職務分掌は業務処理過程の職務分担と責任・権限について、組織および組織を構成する役割の単位や要員ごとに定めたもの。企業がある程度の規模になると、社長一人あるいは特定少数の者だけでは経営が立ち行かなくなる。そこで、分業（職務分掌）の必要が発生し、さらに分業が進んでくると、権限とその裏返しとしての責任の問題が生じる。会社が小規模のうちは、社長が自分の思っていた通りに物事を判断し、進めることが出来る。しかし規模が拡大していくと、個人の能力の限界を超えた部分について機能しない事態が発生する。個人の管理能力の限界は、仕事の量、人の数だけでなく、扱う金額等によっても、発生してくる。そこで自然と分業が進むか、分業を進めざるを得なくなり職務分掌と責任権限をどう定めるかの課題が起きる。 急成長会社の場合は、会社の成長のスピードに組織がついていけないことがあり、規模の拡大が、権限の明確化や体制整備より速い場合は、必要にせまられて権限が分散してしまうこともある。歴史のある企業の場合、公式的に権限を委譲するための組織改革が事業環境の変化に遅れている場合も多い。	現行用語集		
119	助言	ジョゲン		システム監査の実施を通して、『監査対象』の改善のための指摘を行うこと	システム監査の目的は、『監査対象』の『監査テーマ』についての状況を、『監査手続』を使用して調査し、改善すべき事項があれば指摘し改善につなげることである。これは「助言」に該当する。	現行用語集		
120	信頼性	シンライセイ	reliability	与えられた状況下で定められた期間中に当該システムが提供する機能やサービスが期待どおりに動作し、正しい結果を出す性質のこと（「情報システムの信頼性に関するガイドライン」）	旧システム監査基準（平成8年1月30日改訂）では、用語の定義で信頼性を、情報システムの品質並びに障害の発生、影響範囲及び回復の度合としている。JISでは、指定された条件下で利用するとき、指定された達成水準を維持するソフトウェア製品の能力（JIS X 0129-1）と定義している。 情報システムに関する信頼性とは、一般的には、システムの不具合（例えば、プログラムミス、設計エラーなど）やハードウェアの障害により情報システムの正常なサービスが停止したり、異常な出力結果になることを防ぐことをいう。実際にトラブルが発生したときには、損害に直結しないよう、また被害が拡大しないようにすること、速やかに復旧することを含む。 IT活用が進み、情報システムの重要性が増すほど、落雷・洪水・地震等の自然災害や回線の故障、人的な操作の誤り等によってシステムがダウンした場合の損失は重大となる。このような環境下では、情報システムの『安全性』や信頼性がどのレベルにあるのかを把握し、事前にこれらのリスクを推定し、事業への影響を最小限にとどめるため想定される事故や災害に備えておくことが重要となる。しかし、現在では情報システムが複雑化し、機能停止に陥った場合、手作業による回復処理は不可能な場合が多い。 そこで、障害発生防止や信頼性を高める対策として、厳重なシステムテスト、機器構成や通信回線の多重化、バックアップセンターの設置などを行う。また訓練や定期点検などの事前対策や障害発生後の回復手続き等の点検・評価を行う。	現行用語集		シラバス
121	精査	セイサ		監査目標ごとに監査対象項目の全件に対して監査手続を適用する監査方法のこと	精査とは、特定の監査手続の実施に際して、監査対象の母集団からそのすべての項目を抽出して、それに対して監査手続を実施することである。 監査対象項目を全件監査することは、かなりの手間がかかるため、期間と労力を必要とする。個別計画を立案する際、精査で監査を実施するのか、試査で監査を実施するのか決めておく必要がある。	現行用語集		
122	脆弱性	ゼイジャクセイ	vulnerability	一つ以上の脅威がつけ込むことのできる、資産または資産グループが持つ弱点のこと（JIS Q 13335-1）	脆弱性は、それだけでは何ら障害とはならないが、脅威を顕在化させ損害や障害を発生させる原因となる。逆をいえば脅威が存在しない脆弱性は、あまり気を配らなくてもよいことになる。 なお、脆弱性は、環境・施設、ハードウェア、ソフトウェア、組織などに大別し、さらに情報資産の特性や属性とそれらに対応する脅威との関連において個々に整理し対策を講じる必要がある。	現行用語集		
123	精神上の独立性	セイシンジョウノドクリツセイ		システム監査人がシステム監査の実施にあたり、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いう特性のこと	精神上の独立性はシステム監査人の心の問題であり、本当のところは外からうかがい知ることができない。しかしながら、少なくとも外観上の独立性が担保されていない場合は、精神上の独立性が侵されている可能性が高いと想定できる。したがって、本質的な問題として精神上の独立性は重要であるが、第三者からの懸念を抱かれないようにするために外観上の独立も重要となる。 精神上の独立性と外観上の独立性は、それぞれが相まって信頼されるシステム監査業務の遂行に寄与する。		基準	

No	用語	日本語読み	英文名	定義（又は説明）	解説	source	区分1	区分2
124	制約	セイヤク		監査の状況により、重要な監査手続を実施できないこと	財務諸表監査においては、監査基準「第四　報告基準　五　監査範囲の制約」によれば、監査範囲の制約を受けた場合は、その重要性を勘案し、監査範囲の制約の影響につき除外事項を付した限定付適正意見を表明するか、あるいは、意見を表明しないことになる。 システム監査基準においては、「制約」の具体的な内容は記載されていないが、上記の務諸表監査に関するものと同様の意味で用いられている（「除外事項」の解説を参照）		基準	
125	セキュリティホール	セキュリティホール	security hole	コンピュータのOSやソフトウェアにおいて、プログラムの不具合や設計上のミスが原因となって発生した情報セキュリティ上の欠陥のこと（総務省HPより引用）	通常は、プログラムのバグに起因する不具合をさすが、関係者からパスワードを聞き出し、担当者に成りすましてシステム侵入することなど人的管理上の弱点などを含め広い意味で定義している。ハッカーやクラッカーは、このセキュリティホールを狙って攻撃をしてくるので、セキュリティホールを発見し、それを塞ぎ、また、セキュリティホールを攻撃された場合に迅速に対応する体制を整えておくことは、セキュリティ対策の最重要事項である。 セキュリティホールを攻撃された場合の具体的な被害例としては、以下の通り。 ①知らない間にWWWサーバ上のHTMLファイルが改ざんされてしまう ②あるWEBページにアクセスした人のハードディスクの内容が消去されてしまう ③アクセスしてきた人の個人情報が盗まれる	現行用語集		
126	IT全般統制	ゼンパンントウセイ	IT general control	業務処理統制が有効に機能する環境を保証するための統制活動を意味しており、通常、複数の業務処理に関係する方針と手続のうち、IT基盤を単位として構築する『内部統制』のこと（経済産業省「システム管理基準　追補版」（平成19年3月30日）第Ｉ章　２．用語）	業務活動全体を対象とするコントロールで、ジェネラルコントロールとも呼ばれ『業務処理統制』と対比する考え方である。従来、ITに関連する統制活動は、業務処理統制と全般統制に分けて考えられてきた。全般統制は、ITを利用した情報システムが適切に運用管理されることにより、複数の『業務処理統制』が有効に機能することを間接的に確保する統制活動である（COSOの定義）。 全般統制には、ネットワークの運用管理、アクセス・コントロールなどのセキュリティ管理、アプリケーションの取得・開発・運用、外部委託管理などが含まれる。	現行用語集	基準	
127	専門監査人	センモンカンサニン	Certified Master Auditor(CMA)	システム監査学会の学会員の中で一定の要件を満たしたシステム監査人を専門監査人として認定し、精度の高い監査の実施による情報社会の安全化・安定化に資することを目的とした制度のこと	システム監査学会（JSSA；Japan Society for Systems Audits）が2004年度から運営を開始した制度である。現在、専門監査人の区分として、情報セキュリティ専門監査人、個人情報保護専門監査人、会計システム専門監査人の３つが設定されており、今後、新しい専門監査人区分の設定も検討されている。 それぞれの専門監査人の要件、認定を受けるための手順、認定を受けた後の更新手順などについては、システム監査学会のホームページに掲載されているので、参照のこと （別掲参考URL参照）。	現行用語集		
128	総合評価	ソウゴウヒョウカ		監査テーマに対する監査対象の状況についての、システム監査人の評価・結論の内容	『予備調査』、『本調査』で得た『監査証拠』を分析した結果として、『監査テーマ』に対する『監査対象』の状況についてシステム監査人が『評価・結論』としてまとめた内容であり、システム監査報告書の中に記載される。 評価には合理性、納得性、客観性、専門性が要求される。合理性は、適切な『監査手続』に基づいて十分な調査が行われていることによって得られる。納得性は、評価が明確な事実（監査証拠）に基づいて下されていることによって得られる。客観性は、明確な基準に照らして評価を行っていることによって得られる。さらに、専門性は、システム監査についての高い専門技術をもったシステム監査人が評価を行っていることによって得られる。 なお、評価・結論の内容を『監査依頼者』に報告するにあたっては、定性的な評価だけではなく、３段階あるいは５段階などの定量的評価も含めた方が、評価・結論の内容が明確に伝わり改善に結びつきやすい。	現行用語集		シラバス
129	相互牽制	ソウゴケンセイ	check and balance	業務の遂行過程において、２名以上の組織構成員又は2つ以上の組織に分担させ、職務を分離することにより、不正や誤謬の発生を発見・予防し、あるいは自動的に検証できるようにした仕組みの総称のこと	相互牽制とは業務の遂行過程において、２名以上の従業員に分担させ、職務を分離することにより、不正や誤謬の発生を発見・予防し、あるいは自動的に検証できるようにした仕組みの総称。内部牽制ともいう。 相互牽制は、取引を特定の人物のみで完結させずに、複数の者により分担して行わせることにより相互に牽制させ不正や誤謬を防ぐことをいい、一般に、①物の管理と②お金の管理と③帳簿の管理を分離して、三つのうち二つ以上の管理を兼任させないようにする。	現行用語集		

No	用語	日本語読み	英文名	定義（又は説明）	解説	source	区分1	区分2
130	チェックリスト法	チェックリストホウ		システム監査人が作成したチェックリスト（質問書）に対して、特定者より回答を求めること（システム監査技術者育成カリキュラム）	チェックリストは、チェック項目に対する有無のみを確認する場合に使用し、質問書については、チェック項目の有無も含めて質問項目に対する回答を要求する場合に使用する。 個別の監査対象に対して、そのまま合致するチェックリストはないため、当該監査対象に精通したシステム監査人がカスタマイズする必要がある。 システム監査の各関係諸団体から公表されている基準・ガイドライン（システム監査基準、FISCのシステム監査指針等）を利用して、チェックリストを作成する場合が多い。 システム監査人には、適用対象組織体の業種、企業規模およびシステム規模等により、監査の目的を考慮する必要があり、監査対象の実態に適合するような質問内容・範囲に調整する能力が要求される。	現行用語集		シラバス
131	知的財産権関連法規	チテキザイサンケンカンレンホウキ		知的財産権に関わる法規	システム監査関連分野の知的財産権として、コンピュータプログラムが著作権で保護されたり、ビジネスモデル特許として特許権で保護される場合がある。 「知的財産権」とは、特許権、実用新案権、育成者権、意匠権、著作権、商標権その他の知的財産に関して法令により定められた権利又は法律上保護される利益に係る権利を指し、関連法規として、特許法、実用新案法、意匠法、商標法、著作権法、種苗法（ＵＰＯＶ91年条約）、半導体集積回路の回路配置に関する法律、不正競争防止法、独占禁止法等が挙げられる。	auシラバス		
132	中長期計画	チュウチョウキケイカク		中長期の経営計画および情報化計画と対応した、数年間を見通した監査の期間計画のこと	中長期計画は、『監査計画』の内の期間計画の一つに位置付けられる。 中長期計画は、３～５年を展望した『システム監査』の実施方針、及び実施計画であり、監査対象組織体の中長期『経営計画』および中長期『情報システム計画』と連動し、中長期的視点から情報システムのリスクに対するコントロールが、適切に整備・運用されているかを監査する計画である。 『中長期計画』への主な記載事項は、当該期間における『監査目的』、重点監査テーマ、『監査対象』（必要により『監査範囲』）、監査スケジュール（優先順位）、概算予算、育成計画を含めた監査要員計画、品質管理方針等が挙げられる。	現行用語集		シラバス
133	通常改善	ツウジョウカイゼン		『改善勧告』のうち、システム監査人が『緊急改善』と判断した以外の事項のこと	速やかに改善を実施する必要はないが、問題が存在していることは事実であり、計画を立てて改善を実施していく必要のある『改善事項』である。 重要性からいうと『緊急改善』に相当する問題であっても、改善に長期間あるいは多大な投資が伴うものは、通常改善として段階的改善を検討させることが現実的な場合もある。	現行用語集		シラバス
134	ディジタルフォレンジックス	ディジタルフォレンジックス	digital forensics	情報の完全性を保護し、データの厳密な保管と引渡し管理を維持しながら、データの識別、収集、検査、および分析に科学的手法を適用すること	フォレンジック（forensic）は、「法廷の」を意味し、ディジタルフォレンジックスは、コンピュータ/ネットワークフォレンジックスとも呼ばれ、ディジタルデータを訴訟等における証拠性確保の技術・手法を指す。 参考 特定非営利活動法人　デジタル・フォレンジック研究会 http://www.digitalforensic.jp/wdfitm/wdf.html 「デジタル・フォレンジックとは？」 インシデントレスポンス（コンピュータやネットワーク等の資源及び環境の不正使用、サービス妨害行為、データの破壊、意図しない情報の開示等、並びにそれらへ至るための行為（事象）等への対応等を言う。）や法的紛争・訴訟に対し、電磁的記録の証拠保全及び調査・分析を行うとともに、電磁的記録の改ざん・毀損等についての分析・情報収集等を行う一連の科学的調査手法・技術を言う。 デジタル証拠の確保が図られることによって、コンピュータセキュリティを積極的に維持することができる。 具体的には、以下のような分野に展開される。 1．ハイテク犯罪や情報漏えい事件などの不正行為発生後にデジタル機器等を調査し、いつどこで誰が何をなぜ行ったか等の情報を適切に取得し、問題を解決するインシデントレスポンスとして。 2．定期的にフォレンジックを用いた監査を行う事により、不正行為の発生を抑止するとともに発生後の対応を迅速に行えるようにする、広義の意味でのインシデントレスポンスとして。 3．デジタル・データの保全、解析、保管等の取り扱い手法に関して適切に行われているかを議論する事により、相互の法的権利を正しく守る活動として。 不正アクセスや機密情報漏洩などコンピュータに関する犯罪や法的紛争が生じた際に、原因究明や捜査に必要な機器やデータ、電子的記録を収集・分析し、その法的な証拠性を明らかにする手段や技術の総称。"forensics" には「法医学」「科学捜査」「鑑識」といった意味があり、分かりやすく意訳すれば「デジタル鑑識」。	auシラバス		シラバス
135	テストデータ法	テストデータホウ		準備されたテストデータを監査対象プログラムに投入し、期待した結果が出力されるか否かを確認する方法のこと（システム監査技術者育成カリキュラム）	システム監査人が事前準備したテストデータを監査対象のプログラムに投入し、期待した結果が出力されるか否かを検証して、プログラム処理過程の正確性を確認する。特定機能に限定したテストおよび総合的な計算機能・コントロール機能のテスト等、システム監査人の判断により範囲を限定することができる。 また、テストしたシステムが実際に稼動しているものと同一であることを確認する必要がある。	現行用語集		

No	用語	日本語読み	英文名	定義（又は説明）	解説	source	区分1	区分2
136	ドキュメントレビュー法	ドキュメントレビューホウ		特定の情報を収集するために、関連する資料および文書類をシステム監査人が自ら通査すること（システム監査技術者育成カリキュラム）	システム監査人は、事前準備の際、被監査部門におけるドキュメントの整備状況を確認して、どのドキュメントが利用可能かを明確に把握しておく必要がある。 ドキュメントレビューの目的は、監査テーマについての状況を調査する監査証拠を入手することである。また、ドキュメント管理の監査として、ドキュメント（仕様書・変更依頼書等）の内容は、常に最新の状態を反映しているかを調査し、文書管理状況（原本の保管）を確認する。	現行用語集		シラバス
137	突合・照合法	トツゴウ・ショウゴウホウ		関連する記録間を突き合わせること、記録された最終結果をその起因となった事象を示す原始データまで遡り突き合わせること（システム監査技術者育成カリキュラム）	関連する複数の証拠資料を突合せる技法、記録された最終結果をその起因となる事象を示す原始データまで遡って突き合わせる技法等である。 なお、突合せ対象の関連する記録が、相互に同期していることを確認しなければならない。（ブルーフリストによる照合、入力データと出力結果の照合等）	現行用語集		シラバス
138	内部監査	ナイブカンサ	internal audit	組織体の経営目的の達成のために、被監査主体及びその諸活動を、被監査主体から独立した専門家が実施する監査のこと	内部監査とは、組織体の長が、経営管理機能の一つである監視機能を内部監査組織に権限を委譲し、被監査主体を監査することである。近年、組織体の長による不正が多発しており、内部監査の役割は変化してきている。 日本公認会計士協会では、「内部監査の利用」（監査基準委員会報告書610；平成23年12月22日）で、内部監査機能の目的は「経営者、該当する場合には取締役会及び監査役若しくは監査役会又は監査委員会（以下、監査役若しくは監査役会又は監査委員会を「監査役等」という。）によって決定されるとしている。 社団法人日本内部監査協会では、内部監査基準（平成16年改訂）において、「内部監査の本質」として「内部監査とは、組織体の経営目標の効果的な達成に役立つことを目的として、合法性と合理性の観点から公正かつ独立の立場で、経営諸活動の遂行状況を検討・評価し、これに基づいて意見を述べ、助言・勧告を行う監査業務、および特定の経営諸活動の支援を行う診断業務である」としている。 また「品質及び/又は環境マネジメントシステム監査(JIS Q 19011)では、内部監査を「第一者監査 (独立性は監査の対象となる活動に関する責任を負っていないことで実証)と呼ぶこともあり、マネジメントレビュー及びその他の内部目的のために、その組織自体またはその代理人によって行われ、その組織の適合を自己宣言するための基礎としてもよい。多くの場合、特に中小規模の組織の場合は、独立性は、監査の対象となる活動に関する責任を負っていないことで実証することができる。」としている。	現行用語集		シラバス
139	内部監査人監査	ナイブカンサニンカンサ		組織体内に設置された内部監査部門等によって実施される内部監査のこと	内部監査人は、企業の業務内容全般について、合理性、効率性、適法性等の観点より、経営者の要請に基づいて監査を行う。 『内部監査』の項目参照。	現行用語集		

No	用語	日本語読み	英文名	定義（又は説明）	解説	source	区分1	区分2
140	内部統制	ナイブトウセイ	internal control	企業経営者の経営戦略や事業目的等を組織として達成していくための仕組のこと（「コーポレートガバナンスと内部統制」第1章1.1（１）、経済産業省）	内部統制とは、以下の範疇に分けられる目的の達成に関して合理的な保証を提供することを意図した、事業体の取締役会、経営者、その他の構成員によって遂行されるプロセスのことである。 ① 業務の有効性と効率性 ② 財務報告の信頼性 ③ 関連法規の遵守 この定義は『内部統制の統合的枠組み[COSO レポート]』（1992年）の記述を参考にしている。COSOのフレームワークでは、以下の５つを構成要素としている。 ① 統制環境 ② リスク評価 ③ 統制活動 ④ 情報と伝達 ⑤ 監視活動（モニタリング） 更に COSO-ERM では、戦略を加味して、「戦略」、「業務」、「報告」、「遵守」に拡張している。 【ご参考】企業会計審議会『財務報告に係る内部統制の評価及び監査の基準』（2007年） ・内部統制の目的： ① 業務の有効性と効率性 ② 財務報告の信頼性 ③ 関連法規の遵守 ④ 資産の保全 ・内部統制の要素 ① 統制環境 ② リスクの評価と対応 ③ 統制活動 ④ 情報と伝達 ⑤ 監視活動（モニタリング） ⑥ ＩＴへの対応 内部統制の他の要素と必ずしも独立に存在するものではないが、組織の業務内容がＩＴに大きく依存している場合や組織の情報システムがＩＴを高度に取り入れている場合等には、内部統制の目的を達成するために不可欠な要素。	現行用語集		シラバス
141	任意監査	ニンイカンサ	voluntary audit	法律には実施の規定がない、組織体の自由意思によって行う内部監査のこと	任意監査は、『法定監査』・強制監査の監査役監査、会計監査人監査や監督官庁の検査・監査と区別される。 システム監査は任意監査である。ただし監査の目的や監査主体によって法定監査・強制監査に該当することもある。『システム監査基準』に規定されるシステム監査は『内部監査』の位置づけであったが、現在は『内部監査』、『外部監査』に共通する基準になっている。『金融機関等のシステム監査指針』もシステム監査を「内部監査の一環として経営者からの委任を受けて実施するもの」としているが、外部機関の利用も有効としている。	現行用語集		
142	汎用監査ソフトウェア法	ハンヨウカンサソフトウェアホウ		監査対象ファイルの検索、抽出、計算等、システム監査上使用頻度の高い機能に特化した、しかも非常に簡単な操作で利用できるソフトウェアを利用する方法のこと（システム監査技術者育成カリキュラム）	汎用監査ソフトウェア（監査プログラム）は、システム監査人の指定した機能に従って、ファイルからデータを抽出して演算・比較を行い、レポート作成の機能を有し、汎用監査プログラム・パッケージとして開発されている。 提供される機能には、ファイルのアクセス・再編成、データの選択、統計的サンプリング、演算・比較（定量的分析）、層別分類と詳細分析、ファイル処理（整理）、レポート作成等がある。	現行用語集		シラバス

No	用語	日本語読み	英文名	定義（又は説明）	解説	source	区分1	区分2
143	ビジネスプロセス	ビジネスプロセス	business process	組織体が特定の目的を達成するために行う一連の活動、および組織の内外で連続する活動や手続の連鎖のこと	ビジネスプロセスは、組織が戦略を実行するための具体的な手法であり活動そのものである。ビジネスプロセスを業務プロセスとして細分化して捕らえると技術開発、調達、製造、販売、アフターサービス、請求回収、物流などの基幹業務プロセスと、財務経理、人材育成、IT活用や総務人事などの支援業務プロセスに分けることができる。 組織が活動する環境や競争条件が変化すると、組織は存続するために新しい環境に適応する『ビジネスモデル』を作る。これがビジネスプロセスの再構築(BPR)であるが、従来手法の改善や不採算事業からの撤退、新規事業への参入といった程度ではなく、企業の存続をかけた大規模な改革を指している。特に、インターネットをはじめとする情報通信技術の急速な発展に伴い、時間や距離の概念が大きく変わった1990年代の後半以降、企業では製造拠点や販売物流の手法が大きく変わってきた。 これは、事業を継続する組織体が、ビジネスプロセスとして情報通信技術の導入と活用方法を工夫して大きく変化させながら、コストの発生と付加価値を創造するプロセスを冷静に見極めるようになってきたことを意味する。	現行用語集		シラバス
144	ビジネスモデル	ビジネスモデル	business model	企業が特定の目的を達成するため、何をどこでどのように実行して利益を得るかの仕組み、手法、形態のこと	ビジネスモデルは、特定の顧客や市場に対して、即時処理や従来の手続を簡略化するなどの時間的サービスや新たな付加価値を提供することにより顧客の支持を得て、圧倒的な集客やコスト削減に結びつけるような仕組みのことである。伝統的な企業では、長期間にわたり顧客や取引先からの信頼を得ている特徴や、事業として利益や技術力を維持確保している企業独自の工夫もビジネス上のノウハウや手法といえる。 デルモデル：ビジネスモデルの代表例である「デル・ダイレクト・モデル（デルモデル）」は、顧客からの注文を受けてから生産を開始するため、必要なときに必要な量だけ部品を調達する徹底したSCMによる完全注文生産であり、見込み生産はゼロである。コンピュータシステムを駆使することにより、独自のBTO（Build To Order=注文生産）とサプライチェーン・マネジメント（SCM）を実現しているところに特徴がある。このデルモデルは、基本を確立して以降、付加価値サービスを拡大した第2段階、インターネットによるビジネスとサービスの積極的な展開を開始した第3段階を経て、総合的なサービスやコンサルテーションを提供する第4段階にまで進展しているといわれる。	現行用語集		
145	ビジネスリスク	ビジネスリスク	business risk	企業がその目的を達成できないようなリスクのこと	企業にとって不利な影響を与える可能性のある事象のこと。ビジネスリスクが存在すると、自社の事業継続を脅かすことになり、事業活動に影響を与える可能性のある事象を把握しておく必要がある。	auシラバス		シラバス
146	評価・結論	ヒョウカ・ケツロン		調査結果を踏まえて、監査対象の実態が監査目的に則して妥当であるか判断すること	本調査終了後、調査結果を踏まえて評価する。評価をより正確に行うため、システム監査人は、監査結果を被監査部門との意見交換を通じて確認した後、自らの判断基準に基づいて最終結論を下す。	現行用語集	基準	シラバス
147	品質管理	ヒンシツカンリ	quality control	システム監査の有効性を担保し、監査結果の適正性を確保するために、システム監査業務を適切にマネジメントし、その成果物の品質についてコントロールすること	システム監査は、監査のシステム監査人の品質管理と監査業務の品質管理から構成される。システム監査人の品質管理は、一定の能力を認める技能認定等の実施、監査業務中におけるOJT（On-the-Job-Training）、監査業務後の人事評価とその結果のフィードバック等がある。一方、監査業務の品質管理は、システム監査引き受け前のシステム監査主体による審査、監査業務実施中の上席者や監査チーム外の品質管理担当者による監査調書のレビュー、監査実施後の品質管理専門チームによる業務レビュー（審理）等がある。 「システム監査基準」（昭和60年１月策定、平成8年1月30日・平成16年10月8日改訂）の「Ⅲ．一般基準」では、「５．品質管理」として、「システム監査人は、監査結果の適正性を確保するために、適切な品質管理を行わなければならない。」と定めている。 システム監査における品質管理の目的は、システム監査の有効性を評価するとともに、システム監査が当該基準及びシステム監査人が所属する組織の倫理綱領等、社内規程や契約を遵守していることを保証し、システム監査人が業務の改善を促進することにある。システム監査業務の品質管理は、システム監査業務実施前、業務実施中、業務実施後の３段階で実施することが望ましい。	auシラバス		シラバス
148	フォローアップ	フォローアップ		『改善勧告』に対する改善活動が『改善計画』の通りに行われるよう、システム監査人がシステム監査人の立場で支援・指導すること	システム監査は『監査報告』によって終了となるのではない。システム監査人が監査報告書に記載した『改善勧告』に対する改善が実施されてはじめて、システム監査を実施した意義が生まれる。 『改善勧告』に対する改善活動を計画・実施することは、改善実施部門の役割である。システム監査人は自らが行った『改善勧告』に対する改善活動が計画通りに実施されるよう、改善実施部門の改善活動の状況を定期的に確認し、改善実現のためにシステム監査人の立場で支援・指導する必要がある。システム監査人は、立場上、改善実施部門が行う改善活動に直接参加することはできないが、改善活動が計画通りに進んでいない場合、改善活動を円滑に進める方法を提案する、改善実施部門や関連部門の責任者に改善活動の円滑な実施について要請を行うといった行動はとることができる。これが、システム監査人の立場での支援・指導である。 ここでは、被監査部門と区別して改善実施部門という表現を採った。多くの場合、被監査部門が改善実施部門となるが、まれに、被監査部門以外が改善実施部門になることもある。 『内部監査』の場合には、監査部門がフォローアップ活動を行う。『外部監査』の場合には、一般的には『監査報告』までを外部監査企業と契約するが、フォローアップ活動を含めて契約し、外部監査企業が定期的なフォローアップ活動を行う方法もあり得る。しかし、多くは、組織体の中の然るべき部門（監査部門や経営管理部門など）が改善活動の状況を把握し、外部監査企業には次の監査の機会に前回の『改善勧告』に対する改善実施状況を含めて監査してもらうという方法が採られる。	現行用語集	基準	シラバス

No	用語	日本語読み	英文名	定義（又は説明）	解説	source	区分1	区分2
149	フォローアップ監査	フォローアップカンサ		改善実施部門が行った改善活動の結果（改善状況）を、システム監査人が改めてシステム監査手続を用いて確認すること	フォローアップ監査の手順は、システム監査の手順と同じである。ただし、『監査対象』および『監査項目』は『改善事項』に対する改善状況に限定する。それも、すべての改事項を対象にするのではなく、『監査手続』を用いて監査することが必要と判断したものだけを対象に実施する。 システム監査のプロセスとして、『監査報告』から６カ月後、あるいは１年後にフォローアップ監査を実施することを決めておくケースもある。この場合、改善実施部門はフォローアップ監査の実施時期を考慮して、『改善計画』を策定しなければならない。	現行用語集		
150	プライバシーマーク制度	プライバシーマークセイド		日本工業規格「JIS Q 15001個人情報保護マネジメントシステム―要求事項」に適合して、個人情報について適切な保護措置を講ずる体制を整備している事業者等を認定して、その旨を示すプライバシーマークを付与し、事業活動に関してプライバシーマークの使用を認める制度のこと	本制度は、アメリカ、OECD加盟国などの個人情報保護法制化の動きを受け、経済産業省の外郭団体である日本情報処理開発協会（JIPDEC）（当時）が、1998年４月１日から制定・運用を開始している。認証取得のための個人情報保護に関するコンプライアンス・プログラムの要求事項は、1999年３月20日にJIS化（JIS Q 15001）された。事業者は、プライバシーマークを取得し、そのマークを事業活動の際に使用できるので、個人情報の保護に関する信頼獲得のインセンチブ（企業イメージアップ）が与えられ、一方消費者は、事業者の個人情報取扱いの適切性を容易に判断できる材料（プライバシーマーク）を得ることができる。 なお、プライバシーシール制度は、上記JIPDECのプライバシーマーク制度のほか、他にも幾つか著名な制度がある。 ①BBBOnline 米国 BBBOnLineは、米国やカナダの消費者を対象としてオンラインで業務を行う事業者が、ある一定の個人情報保護の規則を満たしているか審査認証して、プライバシーシールを付与する制度。JIPDECのプライバシーマーク制度のモデルとなった制度で、プライバシーマークとの相互認証が可能である。 ②TRUSTe インターネット上で公開、選択、アクセス、安全対策の４つのプライバシー原則への合意を示すサイトに、トラストマークと呼ぶシール表示が許可される制度。米国基点で、シールを表示するサイトはTRUSTeによる監視および紛争調停にも合意する。 ③WebTrust制度 インターネット取引で、取引内容の開示、取引の正確な実施及び個人情報保護のための内部統制について、公認会計士がWebTrust原則及び規準に照らして監査し、「問題がない」場合にWebTrustシールを付与する制度。米国公認会計士協会及びカナダ勅許会計士協会が米国ベリサイン社の協力で共同開発し、1998年からサービスが開始された。 これらのプライバシーシール制度は、認可を受けた事業者のホームページや広告にシールが貼付されることにより、消費者が安心して取引できることの判断を容易にすることを目的としている。	現行用語集		
151	プロジェクトマネジメント	プロジェクトマネジメント	project management	プロジェクト目標を達成するために必要な知識、スキル、ツール、技法などをプロジェクト活動に適用すること	プロジェクトマネジメントでは、組織やチームに課せられた課題を目標期日までに達成するために全体と個々の目標成果を明らかにし、特定スキルをもつ人材、設備などを有効活用して日程、品質、予算やコストを最適化を図る。 プロジェクトマネジメントとは、使命を達成するための有機的なチームを編成して、プロジェクトを公正な専門的手段で効率的、効果的に遂行して、確実な成果を獲得する実践的能力の総称。通常業務との違いは、目標とする成果は定型的でなく独創的なもので特定使命を受けて実施されること。また始まりと終わりのある特定期間に、資源、状況など、特定の制約条件のもとで達成を目指すもので、価値創造的なマネジメントである。 スキル標準では、プロジェクトマネジメントの職種を「プロジェクトの立ち上げ、計画策定、遂行及び進捗管理を 実施し契約上の納入物にも責任を持つ」と定めている。IT投資プロセスでは、戦略的情報化企画（課題整理/分析(ビジネス/IT)、ソリューション設計(構造/パターン)）、開発（コンポネント設計(システム/業務)、ソリューション構築(開発/実装)）及び運用・保守（ソリューション運用(システム/業務)、ソリューション保守(システム/業務)）を主な活動局面として以下を実施する。 －戦略的情報化企画　・基本計画の策定 ・管理／統制 －開発　・管理／統制 －運用・保守　・管理／統制	現行用語集		
152	並行シミュレーション法	ヘイコウシミュレーションホウ		特定の監査目的を検証する機能を持ったプログラムを、システム監査人側で独自に準備し、それと監査対象プログラムに対して同一のデータを入力して、両者の実行結果を比較する方法のこと（システム監査技術者育成カリキュラム）	並行シミュレーション法（Parallel Simulation）は、アプリケーション・プログラムのすべての機能をテストするのではなく、システム監査人が監査目的のために、必要と認める機能のみを対象としている。 この技法はプログラム機能（入力確認手続、処理論理、コントロール等）をシミュレートするため、テスト用プログラムを用いて本番データを処理する。本番の適用業務システムをシミュレートしたテスト用プログラムの作成が必要となる。例として、在庫量が基準値以下になると、自動発注するような取引の自動生成ロジックのテストに効果的である。	現行用語集		

No	用語	日本語読み	英文名	定義（又は説明）	解説	source	区分1	区分2
153	ベストプラクティス	ベストプラクティス	best practice	最も優れた業績や評価を得ている企業や業務の実践方法のこと	優れていると考えられる業務プロセス、業務推進の方法、ビジネスノウハウのことで、最も効果的、効率的な実践の方法のこと、または最優良の事例である。「『ベンチマーキング』」手法では、自社を最高の状態に近づけるため、比較・分析の対象となる最高水準のモデルのことをベストプラクティスとする。 現実の業務改革プロジェクトでは、求められている改革の水準に到達できないケースが多い。これは、業務改革プロジェクトが、現在の組織、業務を前提とするか延長上で検討されているためであり、前提条件を変えない限り大改革は困難である。そこで、最高水準としてベストプラクティスの条件把握が求められる。 しかしながら、最適なベストプラクティスを調査し比較することは、現実的には困難である。『ビジネスモデル』、改革の理論、表面的な仕組みについて情報を得ても、その仕組みや成果を可能にしている条件や、関連する業務や取引先などの関係は社外や他業務との関係までは把握できないからである。 他社や他の業界の事例から、自社に必要な手法を学び取り応用する能力が問われる。	現行用語集		
154	ペネトレーションテスト	ペネトレーションテスト		無権限アクセス（不正アクセスを含む）からシステム資源が守られていることを確認するため、一般ユーザのアクセス権限あるいは無権限で、テスト対象システムへの侵入を試みる技法のこと	模擬（疑似）侵入テストともいう。 システムの脆弱性を発見するには、非常に有効な技法である。専門会社に委託してペネトレーションアタックを行う際、外部システムへの不正アクセス、情報の漏洩等が発生しないよう事前に契約書を交わす必要がある。	現行用語集		
155	ベンチマーキング	ベンチマーキング	benchmarking	組織が改善活動を行うときに、業界を超えて世界で最も優れた方法あるいはプロセスを実行している組織から、その実践方法を学び、自社に適した形で導入して大きな改善に結びつけるための一連の活動のこと(日本経営品質賞アセスメント基準書)	ベンチマーキングは、対象とする業務の『ベストプラクティス』（最も優れた実践方法）を探して、自社と比較分析して差異を把握し、そのギャップを埋めるように、自社の業務プロセスを改善する手法である。優れた業績や評価を得ている企業や業務の実践方法を学び、自社や自分のやりかたと比較して、その違いを解消していくことで、競合相手に対する優位性を確保していく手法である。 ベンチマーキングを進めるためには、自社の現状を正確に把握する必要がある。自社の強みと弱みを分析し、現状の競争能力と市場の評価を正確に評価します。そして、弱みを改善するのか、強みをより強くするのかの方針に基づき、競争力を向上させるために最も効果的な業務プロセスを選定する。次に、対象とする業務プロセスの観点から業種や業界にこだわることなく『ベストプラクティス』をもつ企業を探す。対象企業が決まれば、その企業の業務プロセスの詳細な情報を収集し、分析し、指標とした『ベストプラクティス』と自社との差異を評価する。自社が目標とする改善テーマや水準をもとに実行計画書を作成して実践する。 ベンチマーキング手法では、優れた個々のプロセスを学び実践するとしても、全体のパフォーマンス向上が目的であり、細部にとらわれないことが重要である。 なお、システム開発や運用の現場で実践されているハードウェアの性能評価モデルを作ることをベンチマークテストというので、区別する。	現行用語集		シラバス
156	報告基準	ホウコクキジュン		監査報告に係わる留意事項と監査報告書の記載方式を規定した基準のこと	システム監査基準において、監査目的に応じた監査を実施した結果、システム監査人の保証又は助言に関する評価を監査報告書等にまとめ、依頼者に報告する事項として、次の５項目を報告基準として定めている。 １．監査報告書の提出と開示 ２．監査報告の根拠 ３．監査報告書の記載事項 ４．監査報告についての責任 ５．監査報告に基づく改善指導（フォローアップ）		基準	
157	法定監査	ホウテイカンサ	statutory audit	法令によって実施が定められている監査のこと	会社法に定められている会社法監査、金融商品取引法に定められている金融商品取引法監査、国立大学法人法に定められている国立大学法人監査などが法定監査に該当する。 『監査役監査』、『会計士監査』などの項目参照。	現行用語集		
158	法定監査関連法規	ホウテイカンサカンレンホウキ		法令で義務づけられている監査に関わる法規	企業の財務諸表の適正を確保するために、金融商品取引法や会社法などの法令で義務づけられた監査や、個別の法令に基づく学校法人、労働組合、信用金庫等を対象とする監査がある。 法定監査のように法令で義務づけられていないが、任意監査として、特定の目的を果たすため、会計監査や業務監査を依頼する場合もある。 システム監査自体を法令で義務付けたものは、現時点ではない。			シラバス
159	保証	ホショウ		システム監査を実施した結果として、『監査対象』の状況について一定の保証を与えること	最近の考え方として、システム監査人が監査結果として述べる意見・評価や『指摘事項』は、『監査対象』の状況について、第三者への開示を目的に一定の「保証」を与えるという考え方がいわれている。しかし、この場合の「保証」は、システム管理基準などに基づいて組織体として設定した監査基準、採用した『監査手続』、サンプリングで調査した中での「保証」であることに注意が必要である。	現行用語集		

No	用語	日本語読み	英文名	定義（又は説明）	解説	source	区分1	区分2
160	保証意見	ホショウイケン		入手した監査証拠を評価した結果得られた合理的な根拠に基づく保証を表明した意見のこと	保証意見とは、監査報告書の記載事項のひとつであり、採用した『監査手続』の実施結果、サンプリング調査の実施結果が、システム管理基準などに基づいて組織体として策定した管理基準に照らして適切であることを保証するものである。 保証意見は絶対的な保証ではないが、保証意見が与える影響が大きいため、記入上には次のような留意が必要である。 ・保証意見は、一定の保証を付与するものであるため、システム監査人が負うかもしれない責任に十分に留意し、あいまいな表現を避け、助言意見と混同されることがないようにする。 ・システム監査の結果、無視し得ない指摘事項があることを監査意見として表明しなければならない場合、システム監査人は、監査報告書の外部開示又は非開示を考慮し、必要に応じて法律専門家に助言を求める等して、監査報告書の記載方法、表記方法、並びに取扱い方法を慎重に検討した上で、監査報告書を作成し、提出する。		基準	シラバス
161	本調査	ホンチョウサ		監査目的に則して対象業務の実態を調査・分析・検討すること	本調査では、個別監査計画の監査項目を順次監査し、監査の項目、監査手続き、問題点、監査実施などを監査調書に記録する。 本調査の実施手順は、以下のとおりである。 ①現状の確認 予備調査で得た心証について現状はどうかをシステム監査人自ら現場に行き確認する。その際、新たな問題点の存在の可能性について配慮する必要がある。 ②監査証拠の入手 個別計画書に従って、予備調査で得た心証を裏付ける資料を収集する。監査目標を達成するために必要な資料のみを入手し、不要な資料は入手しないようにする。また、資料の入手に際しては、可能な限り被監査部門の協力を得る。 ③証拠能力の評価 入手した監査証拠は、当該監査目標を立証するために必要な証拠能力を備えているか否かを評価する。証拠能力が不十分な場合、代替的な監査証拠の転用あるいは追加的な 監査証拠の入手を検討する必要がある。 本調査を実施する上での留意点は、以下のとおりである。 ①積極的な現地調査 ②被監査部門との十分な調整 ③個別監査部門の適時見直し ④監査調書の作成	現行用語集	基準	シラバス
162	有効性	ユウコウセイ	effectiveness	情報システムの目的達成に役立つこと	JISでは、利用者が指定された利用の状況で、正確かつ完全に、指定された目標を達成できるソフトウェア製品の能力（JIS X 0129-1）と定義している。 有効性とは、情報システムが、機能面、経済面だけでなく、当初の目的通りに『安全性』、『効率性』、『信頼性』、『可用性』、『機密性』、『完全性』、有用性、『戦略性』の観点から経営に役立っていることである。情報システムの有効性を評価する指標として、投資効果が測定される。しかし、情報システムは多くの側面で利用され、その効果は複合的に表れるため、投資効果の測定方法を確立している企業は少ない。情報システムの有効性は、省力化という定量的な成果から時間短縮、機能向上、機密保全、経営戦略の部分などの定性的な貢献が求められるようになり、また投資の時期から遅れて効果が生じるため、効果測定の評価尺度が複雑であるからである。 有効性の判断基準は事業環境や適用する情報技術により変化するので、従来システムと同様な視点からのやり方を繰り返すことは、 企業の競争優位を損なう危険性を増す場合がある。 投資をしてコンピュータを導入しても、開発した情報システムが現場に適応しておらず使えなかったり、 全体の作業効率を低下させたり、という例は少なくない。システム部門の組織活動やシステム開発や運用のアウトソース状況を確認するには、システム開発投資に対して『効率性』・有効性の視点を重視して診断する。	現行用語集	基準	シラバス
163	ユーティリティ・ソフトウェア法	ユーティリティ・ソフトウェアホウ		システム開発・運用・保守業務の支援のため、主としてメーカーから提供されるソフトウェア等を活用する技法のこと	監査目的によっては、ユーティリティ・ソフトウェア（テストデータ生成、テキストエディタ、ライブラリ・コピー、レポート生成プログラム等）およびアクセス管理ソフトウェア等を活用する技法がある。 しかし、ユーティリティ・ソフトウェアを使用するためには、システム監査人に技術的に高いスキルが要求される。	現行用語集		シラバス

No	用語	日本語読み	英文名	定義（又は説明）	解説	source	区分1	区分2
164	予備調査	ヨビチョウサ		監査対象の実態を明確に把握する調査のことで、本調査の円滑かつ効率的な実施を可能にするために行う事前調査のこと	予備調査の実施手順は、以下のとおりである。 ①監査対象の現状分析 監査対象業務やシステムの実態を次の点に留意し、現状分析する。 ・監査対象組織、各種規定類等 ・監査対象業務やシステムの範囲 ・関連業務やシステムとのインタフェース ・処理の流れ、データの流れ ・運用手続きとコンピュータ処理のインタフェース ②問題点の洗い出し 監査テーマに対する被監査部門や組織体が目標とするレベルと現実のレベルとのギャップを識別して、想定される問題点を洗い出す。この際、考えられる原因や改善策の実現可能性、費用対効果は考慮しない。問題点の分類・整理にとどめる。 ③本調査の見直し 個別計画書で計画した本調査の範囲及び手続きを見直す。 予備調査を実施する上での留意点は、以下のとおりである。 ①目標レベルの明確化 ②潜在的問題点に対する注意 ③本調査での監査手続きの詳細化及び具体化	現行用語集	基準	シラバス
165	予防牽制機能	ヨボウケンセイキノウ	preventive control	業務の過程で誤謬や不正を生じさせる可能性のある行動や機会を牽制することで、事前に誤謬や不正の発生を防止する機能のこと	予防牽制機能は、予め誤謬や不正の発生する機会を予防することで不正発生に至らないような組織上の仕組みを機能させて、業務処理の過程で誤謬や不正を生じさせる可能性のある行動や機会を牽制すること。 例えば、特定者に権限が集中することをさけ、複数名により相互チェックすることで処理の誤りや不正がおきにくいようにする。誤謬摘示機能と『修正回復機能』と同様に、『内部統制』を構成する３つの主要機能の１つ。 ログをとること、教育、規定の整備、なども予防牽制の役割を果たす。	現行用語集		
166	リスク	リスク	risk	事象の発生確率とその結果の組合わせ	当初は、リスクは損失が発生する可能性と言われていたが、リスクを損失だけでなく、発生していない危害やき危険が発生する可能性を指すようになってきた。このリスクは、まだ発生していない時点での不確実性を表すものなので、そのままでは管理の対象とすることができない。管理するためには、具体的に把握できる実体としての対象が必要であり、リスクをもたらす事象の発生確率とその結果の２つの要素の組み合わせに把握できるように定義されている。 「リスクマネジメント－原則及び指針」（JIS Q 31000:2010）では、リスクを「目的に対する不確かさの影響」と定義している。ここで、目的とは財務、安全衛生、環境に関する到達目標など、異なった側面があり、戦略、組織全体、プロジェクト、製品、プロセスなど、異なったレベルで設定されることがある。不確かさとは、事象、その結果またはその起こりやすさに関する情報、理解、知識がたとえ部分的にでも欠落している状態のことである。影響とは、期待されていることから、好ましい方向または好ましくない方向に乖離していることである。	現行用語集	基準	シラバス
167	リスクアセスメント	リスクアセスメント	risk assessment	リスク分析からリスク評価、までのすべてのプロセスのこと	（１）リスクアセスメント リスクアセスメントは、識別された資産に対するリスクを識別し、それらの大きさを手順に従い決定することである。 リスクアセスメントでは組織が保有する資産を対象に以下の事項を把握する。 ① どのような脅威が存在するのか ② その脅威はどの程度発生する可能性があるのか ③ 脅威が顕在化したときにどの程度の影響を受けるのか リスクアセスメントでは、「リスク分析を実施し、算定されたリスクについて「リスク評価」を行う。（JIPDEC ISMSユーザーズガイドより引用） （２）リスクアセスメントについての体系的な取組み方法の確立 1）ISMS、特定された事業上の情報セキュリティ要求事項、並びに特定された法令及び規制の要求事項に適したリスクアセスメントの方法を特定する。 2）リスク受容基準を設定し、またリスクの受容レベルを特定する。選択するリスクアセスメントの方法は、それを用いてリスクアセスメントが、比較可能で、かつ、再現可能な結果を生み出すことを確実にしなければならない。 （JIS Q 27001:2006 4.2.1 ISMSの確立、より引用） 「リスクマネジメント－原則及び指針」（JIS Q 31000:2010）では、リスクアセスメントを「リスク特定、リスク分析及びリスク評価のプロセス全体」としている。	現行用語集	基準	
168	リスクアプローチ	リスクアプローチ	risk approach	限られた資源をリスクの高い分野に優先的に配分して、効果的かつ効率的に対応して成果を得ようとする手法のこと	予算・要因・時間等の監査資源が限られる中、効果的かつ効率的監査を実施するためには、監査計画段階でリスク分析（リスクの大きさ、リスクの可能性、リスクコントロールの状況等の把握）を行い、リスクが大きくかつ発生確率の高いものに重点を置いて監査することが重要である。 例えば、監査の実施に際し、想定されるリスク要因に対し、網羅的に監査を行うのでなく、監査計画段階でリスク分析を行い、リスクが大きくかつ発生確率の高いものに対し、重点的に監査することにより、効果的かつ効率的な監査につながる。			シラバス

No	用語	日本語読み	英文名	定義（又は説明）	解説	source	区分1	区分2
169	リスクアプローチ監査	リスクアプローチカンサ	risk approach audit	リスクアプローチに基づく監査のこと	限られた監査資源の中、効果的かつ効率的な監査を目指すアプローチである。もともとは会計監査において、重要な虚偽の表示が生じる可能性が高い事項について、重点的に監査の人員や時間を充てることにより、監査を効果的かつ効率的なものとする監査アプローチである。 財務諸表監査においては、虚偽の表示が行われる可能性の要因に着目し、その評価を通じて実施する監査手続やその実施の時期及び範囲を決定することで、より効果的かつ効率的な監査を実現しようとしたものである。			シラバス
170	リスクコントロール	リスクコントロール	risk control	リスクマネジメントのプロセスにおいて、意思決定をする行動のこと	リスクコントロールは、具体的には、リスクの顕在化の防止およびリスク顕在化の場合の影響度を局限化するための諸施策について意思決定をすることである。リスク対策ともいう。広義においては事業体の経営理念の実現を阻害するすべての要素を排除するためのすべての活動、内部統制などに近い概念で表現されることもある。 リスク対策は通常、リスク回避、リスク低減、リスク移転、リスク保有の４つを組み合わせて選択して行う。リスク対策の４つの概念は、次のとおり。 ①リスク回避 リスクのある状況に巻き込まれないようにすること、又はリスクのある状況から撤退する行為。 ②リスク低減 リスクに伴う発生確率若しくは好ましくない結果、又はそれらの両方を小さくするために取られる行為。一般のリスク対策を行うこと。 ③リスク移転 リスクに関して、損失の負担、又は利益の恩恵を他社と共有すること。保険に加入することなどが含ま れる。 ④リスク保有 あるリスクからの損失の負担又は利益の恩恵を受容すること。何も対策を講じないで、損失が発生した場合は、自らその損失を負担すること。また、リスク低減対策を実施してもなおリスクが残ることが想定される。これを「残留リスク」といい、最終的には、「リスク保有」に含めて取り扱うこととなる。 なお、リスクそのものに利益を含むことが一般的になってきたため、TR Q 0008:2003(ISO/IEC Guide 73:2002)では「リスク低減」を「リスク最適化」と呼ぶこととなった。	現行用語集		
171	リスク評価	リスクヒョウカ	risk evaluation	リスクの重要性を明らかにするために、算定されたリスクを、与えられたリスク基準と比較する過程のこと	リスクのもつ２つの要素であるリスクが顕在化する「事象の発生確率（事態の確からしさ）」とリスクが顕在化した場合の「その結果（影響の大きさ）」を定量的または定性的に把握することがリスク算定であり、算定されたリスクの大きさ（リスク＝発生確率×影響の大きさ）を与えられたリスク基準と比較・評価して最終的な重要度を決定するプロセスがリスク評価である。 リスク評価において、それぞれ異質なリスクの重要性を比較する場合は、第1段階としてリスク算定における絶対的な数値を用い、第２段階としてそれぞれの算定値を評価基準と照らし合わせて相対的な評価値を出し、その結果を相互に比較することで評価をすることができる。	現行用語集		
172	リスク分析	リスクブンセキ	risk analysis	リスクの重大さを算定するためのプロセスのこと	リスク分析は、リスクアセスメントにおける前段のプロセスであり、リスクの発見、リスクの特定、リスクの算定の各ステップにより、すべてのリスクを明かにし、そのリスクが発生する確からしさと影響度を明らかにする手順のことである。 リスク分析の最初の出発点はリスクの発見から始まる。組織（システム）に影響を与える可能性のあるものすべてのリスクを把握することが出発点である。実際には新たなリスクがつぎつぎと顕れるため日々注意が必要である。組織として一度発見したリスクは必ず記録し財産とする必要がある。発見したリスクの中から組織に重大な結果をもたらす可能性のあるものを特定し、その特定したすべてのリスクについて、リスクのもつ二つの要素であるリスクが顕在化する発生確率（確からしさ）とリスクが顕在化した場合の結果（影響の大きさ）を明らかにする。次にそれらのリスクの二つの要素を定量的または定性的に把握してリスクの算定を行う。 また、リスク分析については、リスクの発見、特定、算定のための様々な手法があり、これらを称して「リスク分析手法」という。分析には、定性的、定量的、また経営に資することを目的とした分析、設計などに反映させるための技術的分析など目的に応じて様々な手法がある。 リスク分析の最初のステップで行うリスクの発見は、具体的な計画策定の最初に行うリスクの発見はこの手法で行えば完璧というものはなく、組織の能力に依存するところが多い。関係者の経験、ブレーンストーミング、学会や同業他社の事故事例など出来る限り多くの情報を集約することが一般的に行われる。 リスク発見の段階では個々のリスクの発生の蓋然性についての評価は行わず、特定のステップにおいて組織との関連性において検討すべきリスクを定める。 最後のステップは、リスク算定である。リスク算定により、個々のリスクに対する評価のための試料を提供することができる。 なお、ISMS適合性評価制度において紹介されている「リスク分析手法」には、ベースラインアプローチ、非形式的アプローチ、詳細リスク分析、組合せアプローチ（複合アプローチ）がある。（ISMS適合性評価制度ガイドライン参照：原出典は「ITセキュリティマネジメントガイドライン―第２部：ITセキュリティのマネジメント及び計画　TR X 0036-2:2001」）	現行用語集		シラバス
173	リスクマネジメント	リスクマネジメント	risk management	リスクに関して、組織を指導し管理する、調整された活動のこと	リスクマネジメントには、一般にリスク算定、リスク評価、リスク対応、リスク受容、およびリスクコミュニケーションを含む。古典的なリスクマネジメントでは、リスクの算定評価を行い、リスク対応（リスクコントロール）を通じて最小の費用で、リスクによる不利益の影響を最小化すること、などの定義がされ、最小のコストでリスクを最小化することを中心に定義されることが多い。 一方、このTR Q 0008:2003による定義は、リスクそのものに利益を含むため、リスクマネジメントの定義も適切な利益のためにはコストが必ずしも最小でなく合理的であればよいため、このような幅広い定義となっている。 なお、リスクコミュニケーションは最近重要視されている概念で、株主、取引先、住民、自治体、従業員などなどステークホルダー（利害関係者）と事業者のリスクに関する情報を共有することである。	現行用語集		