

情報システム監査の専門性、および、そのような専門性を持つ監査を実施するために必要な技能には、情報システム監査に専ら適用される特別な基準が必要となる。ISACA® (Information Systems Audit and Control Association®) の目標の1つは、そのビジョンを実現するために、世界的に通用する基準を普及させることである。情報システム監査基準 (IS Auditing Standards) の開発と普及は、ISACA が専門家として監査分野に貢献する上で、その基礎となる。情報システム監査基準の枠組みには、次のようないくつかのレベルの指針がある。

- **基準**は情報システム監査とその結果報告の必須要件を規定する。内容は次のとおり。
 - (基準は、) 情報システム監査人に、ISACA の「職業倫理規程 (Code of Professional Ethics) 」で定められた専門家としての責任を果たすために最低限必要な業務遂行レベルに関する情報を提供する。
 - (基準は、) 経営者や他の関係者に、監査専門家の業務について期待し得る水準に関する情報を提供する。
 - (基準は、) CISA® (Certified Information Systems Auditor®) 資格保持者に、その必要要件に関する情報を提供する。この基準を遵守できない場合、ISACA 理事会 (ISACA Board of Directors) または該当する ISACA 委員会により、CISA 保持者の行為が調査されることがある。最終的に懲罰が課される場合がある。
- **ガイドライン**は情報システム監査基準を適用する際の指針である。情報システム監査人は、システム監査基準をどのように適用するかを判断する際、このガイドラインを勘案すべきである。また、システム監査基準の適用に当たり専門家としての判断をすべきであり、システム監査基準からの逸脱について正当な理由を示すことができるようにすべきである。情報システム監査ガイドラインの目的は、情報システム監査基準の遵守方法について、追加情報を提供することである。
- **手順**は、実際の監査において、情報システム監査人が従うであろう手順の例を示す。手順に関するドキュメントは、情報システム監査を実施する際システム監査基準を遵守する方法を示しているが、必要要件は規定していない。情報システム監査手順の目的は、情報システム監査基準の遵守方法に関わるより詳細な情報を提供することである。

CobIT® は、ベスト・プラクティスを実施する上での指針として使用されるべきである。CobIT のフレームワーク (当該名の分冊) は、「企業の資産を守るのは経営者の責任である。この責任を果たすと共に、期待される役割を果たすために、経営者は適切な内部統制システムを確立する必要がある。」と示している。CobIT は、情報システムを管理する際の詳細なコントロールおよびコントロール技法を提供する。CobIT において、「ある特定の監査の対象範囲」に対し適用できる最も適切な部分の選択は、特定の CobIT IT プロセスを選定すること、及び、CobIT の「情報管理基準」を勘案することに基づいて為される。

CobIT フレームワークで述べられているように、下記の各分冊は、各々 IT マネジメントプロセスにより構成されている。CobIT は、ビジネスに係る経営管理者、IT に係る経営管理者、そして情報システム監査人が使用することを想定している。従って、CobIT を使用することにより、ビジネス目標の理解、ベスト・プラクティスの伝達、および、広く理解され十分尊重されている基準を参照して勧告を実施する事が可能になる。CobIT には次の内容が含まれる。

- コントロール目標—最小限の良好なコントロールに関する高レベルかつ詳細な包括的記述
- コントロール手続—コントロール目標を具体的に実施する際の理論的裏付けと「実施方法」の指針
- 監査ガイドライン—各々のコントロール領域を理解する方法、個別のコントロールを評価する方法、準拠状況を評価する方法、コントロールが適切でないために発生するリスクを把握する方法に関する指針
- マネジメントガイドライン—成熟度モデル、様々な測定値、様々な主要成功要因 (CSF) を使って、IT プロセスのパフォーマンスを評価し、向上させる方法に関する指針。その内容は、経営主導の、継続的かつ先を見据えたコントロールの自己評価のための枠組みを提供する。このコントロールの自己評価は特に以下の点に焦点を当てている。
 - パフォーマンス測定—IT 機能はビジネス要件を十分サポートしているか？ マネジメントガイドラインは、自己評価のワークショップに使用できる。また、IT ガバナンスの枠組みの一部として、経営者が、継続的なモニタリングと改善の手順を導入することを支援するために使用できる。
 - IT コントロール・プロファイリング—どの IT プロセスが重要か？ 何が、コントロールに関する主要成功要因 (CSF) か？
 - 認識—目標を達成できない場合のリスクにはどのようなものがあるか？
 - ベンチマーキング—他の人々は何をしているか？ 結果をどのように測定し、比較することができるか？ マネジメントガイドラインは、ビジネスの視点から見た IT のパフォーマンスの評価を可能にする指標の例を提供する。重要目標の達成指標 (KGI) は、IT プロセスの成果を特定し、測定する。キー・パフォーマンス・インディケータ (KPI) は IT プロセスのイネーブラー (実行を可能にするために必要なもの) を測定することにより、IT プロセスがいかに適切に機能しているかを評価する。成熟度モデルと成熟度の属性は、能力評価とベンチマーキングの手段を提供し、経営者がコントロール能力を測定して、改善をするために、コントロールが不足している程度とそれを補うための戦略を特定するのに役立つ。

用語集は、ISACA の Web サイト (www.isaca.org/glossary) に掲載されている。監査とレビューという言葉は同義語として使用されている。

免責条項: ISACA は、ISACA の職業倫理規程 (ISACA Code of Professional Ethics) で定められた、専門家としての責任を果たすために必要な最低限のパフォーマンスを示す基準として本指針を策定した。ISACA は本品の使用が成功を保証するとは主張していない。本品に、適切な手順やテストがすべて含まれているわけではない。また、同じ結果を得ることを目指した他の手順やテストを排除することはしない。個別の手順やテストの優先度を判断する際、コントロールの専門家は、特定のシステムや情報技術環境に基づく特定のコントロール環境に対し、各自の専門家としての判断を適用すべきである。

ISACA 基準委員会 (ISACA Standards Board) は、情報システム監査基準、ガイドライン、手順の準備について広範な審議を委託されている。ドキュメントの発行に先立ち、基準委員会は、一般の意見を得るため原案を発表する。また、基準委員会は、必要に応じ、審議が予定されているトピックスに関する専門家、あるいは関心を持つ人材を募集する。基準委員会は、現在も基準策定を進めており、新しい基準が必要となる新たな課題を特定するための ISACA メンバーや他関係者の意見を歓迎する。意見・提案は、E メール (standards@isaca.org)、ファックス (+1.847.253.1443)、または、郵送 (本文書の最後にある住所宛) で、ISACA 国際本部の調査・基準・学術研究担当の理事宛てに送付願いたい。本文書は 2005 年 7 月 1 日に発効した。

不正行為・例外処理及び不法行為 S9

概要

- 01 ISACA の基準には基本的な原則および重要な手順が太字で示されており、これらは必須である。また同時に、これらに関連する指針も示されている。
- 02 本 ISACA 基準の目的は、情報システム監査人が監査の過程で考慮すべき不正行為・例外処理及び不法行為に関する指針を定め、提供することである。

基準

- 03 情報システム監査人は、監査リスクが少なくなるよう監査を計画し実行するに当たり、不正行為・例外処理及び不法行為のリスクを考慮する必要がある。
- 04 情報システム監査人は、「自らが行った不正行為・例外処理及び不法行為に係るリスク評価の結果に拘らず その不正行為・例外処理及び不法行為に係る重要なステートメントの誤りが生ずる可能性」を認識し、監査中、専門家としての注意力を維持すべきである。
- 05 情報システム監査人は、監査対象となる組織と内部統制を含むその環境を理解すべきである。
- 06 情報システム監査人は、監査対象となる組織内に於いて、「実際に生じた不正行為・例外処理及び不法行為」、「不正行為・例外処理及び不法行為と疑われる行為」、「不正行為・例外処理及び不法行為と申し立てられた行為」を、経営者ないし他の関係者が認識しているか否かを判断するために、十分かつ適切な監査証拠を入手すべきである。
- 07 情報システム監査人は、監査対象となる組織とその環境を理解するために監査を実施するに当たり、不正行為・例外処理及び不法行為に起因する重要なステートメントの誤りが生ずるリスクを示すことがある。異例あるいは予期し難い(人的等の)相互関係に注意を払うべきである。
- 08 情報システム監査人は、「内部統制の適切性」及び「経営者により内部統制が無効にされるリスク」をテストする手順を策定し実行すべきである。
- 09 情報システム監査人は、ステートメントが誤りであることを識別した場合、それが不正行為・例外処理ないし不法行為の可能性を示しているか否かを評価すべきである。そのような可能性がある場合、情報システム監査人は、その監査における他の状況、特に経営者の意見表明が暗示する事柄に十分な注意を払うべきである。
- 10 情報システム監査人は、少なくとも 1 年に 1 回、あるいは、監査の実施状況に応じ更に頻繁に、経営者から書面による意見表明を入手すべきである。この意見表明には下記内容が含まれるべきである。
 - 不正行為・例外処理ないし不法行為を防止し発見するために内部統制を策定し導入実施する責任が経営者にあることを認めること
 - 不正行為・例外処理ないし不法行為の結果重要なステートメントの誤りが存在するリスクを評価した結果を情報システム監査人に開示すること
 - 下記に関連して、監査対象組織に影響する不正行為・例外処理ないし不法行為に関する経営者の認識を情報システム監査人に開示すること
 - 経営者
 - 内部統制に関し重要な役割を果たしている従業員
 - 監査対象の組織に影響を及ぼす「不正行為・例外処理ないし不法行為と申し立てられた行為」、「不正行為・例外処理ないし不法行為と疑われる行為」に関する経営者の認識を、従業員・元従業員・監督当局・その他関係者から伝えられた状況のまま、情報システム監査人に開示すること
- 11 情報システム監査人は、重要な不正行為・例外処理ないし不法行為を識別した場合、あるいは重要な不正行為・例外処理ないし不法行為が存在する可能性があるとの情報を得た場合、これらの事項を、適切なレベルの経営者に、適切な時期に通知すべきである。
- 12 情報システム監査人は、重要な不正行為・例外処理ないし不法行為に、「経営者」や「内部統制に関し重要な役割を果たしている従業員」が関わっていると識別した場合、これらの事項を、その組織のガバナンスの責任者に対し、適切な時期に通知すべきである。
- 13 情報システム監査人は、適切なレベルの経営者とガバナンスの責任者に対し、監査実施中に気付いた、不正行為・例外処理及び不法行為を防止し発見するための内部統制の策定と導入実施に係る重要な弱点と考えられる可能性がある事項を通知すべきである。
- 14 情報システム監査人は、不法行為または重要なステートメントの誤りにより、異常な状況に陥り、これが監査を継続遂行するための当該情報システム監査人の能力に影響を与えた場合、かかる状況の中で適用可能な法的責任および専門家としての責任 — これには、監査チームのメンバーへの報告、あるいは、場合によりガバナンスの責任者や監督当局への報告が必要か否かが含まれる — を考慮すべきである。また、場合によっては、監査を辞退することも考慮すべきである。
- 15 情報システム監査人は、経営者、ガバナンスの責任者、監督当局などに報告された重要な不正行為・例外処理及び不法行為について、すべての連絡内容、計画、結果、評価、結論を文書化すべきである。

コメント

- 16 情報システム監査人は、情報システム監査ガイドライン G19「不正行為・例外処理及び不法行為」で、不正行為・例外処理及び不法行為を構成する行為の定義を参照すべきである。
- 17 情報システム監査人は、不正行為・例外処理及び不法行為に起因する重要なステートメントの誤りが無いという合理的な保証を得るべきである。情報システム監査人は、判断の介在、テストの程度、内部統制本来の制約といった要因に伴い、絶対的な保証を得ることは出来ない。監査の過程で情報システム監査人が利用できる監査証拠は、本来の性質上、決定的なものではなく、むしろ説明のためのものと位置づけられるべきである。
- 18 不法行為は、情報システム監査人に対し事実や虚偽報告を隠蔽するために複雑な策がめぐらされている可能性があるため、不法行為に起因する重要なステートメントの誤りを発見できないリスクは、例外処理等ないし過誤に起因する重要なステートメントの誤りを発見できないリスクより大きい。
- 19 監査対象の組織に関する情報システム監査人の経験と知識は、監査に役立つ。情報システム監査人は、問合せや実際の監査を行うに当たり、過去の経験を完全に無視することをせず、また、専門家としての注意力を維持することを期待されるべきである。情報システム監査人は、経営者やガバナンスの責任者が正直で誠実であると信じてしまうことに基づく説得性の無い監査証拠に満足してはならない。情報システム監査人と監査チームは、監査を計画するその一環として、また監査を実施する間を通じ、監査対象の組織における不正行為・例外処理及び不法行為の発生し易さについて討議すべきである。

- 20 情報システム監査人は、重要な不正行為・例外処理及び不法行為が存在するリスクを評価するため、以下の事項の使用を考慮すべきである。
- 監査対象の組織に関する知識と経験(経営者やガバナンスの責任者が正直で誠実であることについての経験を含む)
 - 経営者に対する質問で得られた情報
 - 経営者の意見表明と内部統制に関する承認
 - 監査中に得た、その他の信頼し得る情報
 - 経営者による不正行為・例外処理及び不法行為のリスクに関する評価と、かかるリスクを識別し対策を講じてきた過程
- 21 不正行為・例外処理及び不法行為に関する更なる情報を得るため、以下の指針を参照すべきである。
- 情報システム監査指針 G5、監査ポリシー (IS Auditing Guideline G5, Audit Charter)
 - COBIT「フレームワーク」、コントロール目標 DS3、DS5、DS9、DS11、PO6 (CobIT Framework, control objective DS3, DS5, DS9, DS11, PO6)
 - サーベンス・オクスレー法(米国企業改革法)(2002年)
 - 海外汚職行為防止法(1977年)

適用開始日

- 22 本 ISACA 基準は、2005 年 9 月 1 日以降に開始されたすべての情報システム監査に適用される。

ISACA 2004-2005 基準評議会 (Information Systems Audit and Control Association 2004-2005 Standards Board)	
議長、セルジオ・フレジンスキー (Sergio Fleginsky)、CISA	ウルグアイ、ICI ペイント (ICI Paints)
スペイン・アルダル (Svein Aldal)	ノルウェイ、アルダル・コンサルティング (Aldal Consulting)
ジョン・ベバリッジ (John Beveridge)、CISA、CISM、CFE、CGFM、CQA	米国、マサチューセッツ州監査人事務局 (Office of the Massachusetts State Auditor)
クラウディオ・チリ (Claudio Cilli)、Ph.D、CISA、CISM、CIA、CISSP	イタリア、タンジェリン・コンサルティング (Tangerine Consulting)
クリスティーナ・レデスマ (Christina Ledesma)、CISA、CISM	ウルグアイ、シティバンク NA スクルサル (Citibank NA Sucursal)
アンドリュー・マクリオード (Andrew MacLeod)、CISA、CIA、FCPA、PCP	オーストラリア、ブリスベン市評議会 (Brisbane City Council)
V. ミーラ (V. Meera)、CISA、CISM、ACS、CWA	米国、マイクロソフト
ラビ・ムサクリシュナン (Ravi Muthukrishnan)、CISA、CISM、FCA、ISCA	インド、イカノス・コミュニケーションズ (Ikanos Communications)
ピーター・ニブレット (Peter Niblett)、CISA、CISM、CA、CIA、FCPA	オーストラリア、WHK デイ・ニールソン (WHK Day Neilson)
ジョン G. オット (John G. Ott)、CISA、CPA	アメリカ、アメリソースバーゲン (AmerisourceBergen)
トーマス・トンプソン (Thomas Thompson)、CISA	アラブ首長国連邦、アーンスト&ヤング (Ernst & Young)

© Copyright 2005
 Information Systems Audit and Control Association
 3701 Algonquin Road, Suite 1010
 Rolling Meadows, IL 60008 USA
 電話: +1.847.253.1545
 Fax 番号: +1.847.253.1443
 電子メール: standards@isaca.org
 Web サイト: www.isaca.org