



Information Systems  
Audit and Control  
Association

# 情報システム監査基準 監査ポリシー 文書番号 S1

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](http://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](mailto: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2004年10月15日に発効した。

## 監査ポリシー S1

### 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 本情報システム監査基準の目的は、監査の過程で適用される監査ポリシーに関する指針を定め、提供することである。

### 基準

- 03 **情報システム監査機能 ないし 情報システム監査業務の目的、責任、権限、説明責任は、監査ポリシー または 監査契約書により適切に文書化されている必要がある。**
- 04 **監査ポリシーないし監査契約書は、組織内の適切なレベルにおいて同意され、承認されている必要がある。**

### コメント

- 05 情報システムに係る内部監査機能において、監査ポリシーは実施中の監査活動のために準備されるべきである。監査ポリシーは少なくとも年 1 回、監査に係る責任が変更された場合は更に頻繁に、見直しが行われるべきである。情報システムに係る内部監査の場合、監査契約書は、「ある特定の監査ないし非監査業務」について、その内容を更に明確にする、あるいは、確認するために使用される。情報システムに係る外部監査の場合、監査契約書は、通常、「個々の監査」毎に、あるいは、「個々の非監査業務」毎に準備されるべきである。
- 06 監査ポリシーあるいは監査契約書は、監査機能あるいは監査業務に関する目的・責任・制約条件を十分に説明するよう詳細化されるべきである。
- 07 監査ポリシーあるいは監査契約書は、監査の目的および責任が文書化されていることを保証するために、定期的に見直されるべきである。
- 08 監査ポリシーあるいは監査契約書の作成に関し、追加情報を得るために、次に掲げる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 M4 (COBIT Framework, Control objective M4)

### 適用開始日

- 09 本基準は、2005 年 1 月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、プライスウォーターハウス・クーパーズ (PricewaterhouseCoopers)
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、バリュー・パートナー (Value Partners)
クリスティーナ・レデズマ (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、MACS、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、CISSP、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、ネクストリンクス・インド・プライベート (NextLinx India Private Ltd.)
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	米国、アテナ (Aetna Inc.)
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 2004

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](mailto:standards@isaca.org)

Web サイト: [www.isaca.org](http://www.isaca.org)