

S16 電子商取引

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® 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® (Control Objectives for Information and related Technology) は、コントロール要件、技術的問題、およびビジネスリスクの間に存在する隔たりを埋める、管理者のための情報技術 (IT) ガバナンスフレームワークであり、サポートツールセットである。CoBIT により組織全体において IT コントロールに関する明確なポリシー策定および良好な慣行が可能になる。さらに、規制に対するコンプライアンスを重要視し、IT により実現される価値の向上において組織を支援し、調整を可能にして、CoBIT フレームワーク概念の実施を簡素化できる。

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、良好な慣行の伝達、および、広く理解され十分尊重されているフレームワークを参照して勧告を実施する事が可能になる。CoBIT は ISACA の Web サイト (www.isaca.org/cobit) からダウンロードできる。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。

- **コントロール目標**—IT プロセスにおいて最小限の良好なコントロールに関する包括的記述
- **マネージメントガイドライン**—成熟度モデル、RACI チャート、様々な目標や測定値を使って、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 コントロール・プロファイリング
 - － 認識
 - － ベンチマーキング
- **CoBIT 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リスクと価値記述および「実施方法」の指針
- **IT 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

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、情報システム監査基準、ガイドライン、手順において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。ご意見・ご提案は、E メール (standards@isaca.org)、ファックス (+1.847.253.1443)、または本ドキュメントの最後にある住所まで郵送にて、ISACA International Headquarters、基準および学術関連研究のディレクターあてにお送りください。本文書は 2007 年 12 月 1 日に発効した。

S16 電子商取引

概要

- 01 ISACA の基準には基本的かつ必須の原則および重要な手順が黒色の太字で示されている。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、電子商取引環境のレビューに係る基準を定め、指針を提供することである。

基準

- 03 **情報システム監査人は、電子商取引業務が適切に管理されていることを保証するために電子商取引環境をレビューする際に、適用されるコントロールおよびリスクを評価すべきである。**

コメント

- 04 電子商取引とは、実現技術としてインターネットを使用し、顧客、サプライヤー、およびその他の外部のビジネスパートナーに対し、電子的にビジネスを行う組織のプロセスと定義される。そのため、これには企業間(B2B)電子商取引モデルおよび企業対消費者(B2C)電子商取引モデルが含まれる。
- 05 情報システム監査人は、適切なリスク評価手法を使用すべきであるか、情報システムに係る包括的な監査計画の策定に取り組むべきである。これには電子商取引環境も含むべきである。
- 06 情報システム監査人は電子商取引活動のレビューの際に、継続的保証の使用を含む、データ分析手法の使用を検討すべきで、これにより、継続的なシステムの信頼性を監視し、コンピュータから選択的な監査証拠を収集することができる。
- 07 電子商取引に関するコントロールとリスク管理の含意を理解するために必要な技能と知識の水準は、組織の電子商取引活動の複雑さによって異なる。
- 08 情報システム監査人は、監査を始める前に、電子商取引アプリケーションによりサポートされているビジネスプロセスの性質と致命度を把握し、適切な状況で結果が評価されるようにすべきである。
- 09 電子商取引に関し、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 G21 ERP(Enterprise Resource Planning)システムのレビュー(Enterprise Resource Planning (ERP) Systems Review)
 - 情報システム監査指針 G22 企業対消費者(B2C)電子商取引のレビュー(Business-to-consumer (B2C) E-commerce Review)
 - 情報システム監査指針 G24 インターネットバンキング(Internet Banking)
 - 情報システム監査指針 G25 仮想専用ネットワーク(VPN)のレビュー(Review of Virtual Private Networks (VPN))
 - 情報システム監査指針 G33 インターネットの使用に関する概論(General Considerations on the Use of the Internet)
 - 情報システム監査手順 P6 ファイヤーウォール(Procedure P6 Firewalls)
 - COBIT フレームワークおよびコントロール目標(COBI T framework and control objectives)

適用開始日

- 10 本基準は、2008年2月1日以降に開始された情報システム監査に適用される。

2007～2008 年度 ISACA 基準委員会

議長、ラビ・ムサクリシュナン (Ravi Muthukrishnan)、CISA、CISM、FCA、ISCA	インド、キャプコ IT サービスズ・インド・プライベート (Capco IT Services India Private Limited) 米国、グーグル(Google Inc.)
ブラッド・デビッド・チ(Brad David Chin)、CISA、CPA	ウルグアイ、ICI ペイント(ICI Paints)
セルジオ・フレジンスキー(Sergio Fleginsky)、CISA	スペイン、ホームランドオフィス(HomeLand Office)
マリア・ゴンザレス(Maria Gonzalez)、CISA	シンガポール、アーンスト&ヤング(Ernst & Young)
ジョン・ホー・チ(John Ho Chi)、CISA、CISM、CBCP、CFE	
アンドリュー J. マクリオード (Andrew J. 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)
ジョン G. オット(John G. Ott)、CISA、CPA	アメリカ、アメリソースバージェン(AmerisourceBergen)
ジェイソン・トンプソン(Jason Thompson)、CISA、	米国、KPMG LLP
CIA、ミーラ・ベンカッテッシュ (Meera Venkatesh)、CISA、CISM、ACS、CISSP、CWA	米国、マイクロソフト

© 2007 ISACA. All rights reserved.

ISACA
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