IS Auditing Standards

情報システム監査基準ハンドブック

2009 年 7 月 1 日発行

IS Auditing Standards

情報システム監査基準ハンドブック

Tokyo Chapter

ISACA

2008 ー 2009 東京支部　理事会

会　長・理事	太田　均
副会長・理事	堀越　繁明
副会長・理事	長尾　慎一郎
副会長・理事	中村　努
副会長・理事	日髙　祐子
副会長・理事	滝本　憲広
理事	榎木　千昭
理事	原田　要之助
理事	梶本　政利
理事	高須　昌也
理事	丸山　満彦

2008 ー 2009 東京支部　基準委員会

委員長	武田　隆一
常任委員	畠中　一浩
常任委員	三堀　眞美
常任委員	糠森　浩二
常任委員	富田　勲
委員	山内　哲也
委員	高木　和夫
委員	土屋　創
委員	芳賀　健治
委員	坂本　哲

本書の利用に際しては以下の点につき留意が必要である

1. 本書は IS Auditing Standards の普及のために、ISACA 東京支部が国際本部の許可を得て作成したものである。
2. 本書は 2009 年 1 月の情報にもとづき作成されている。IS Auditing Standards は定期的に改訂されるので、国際本部ホームページ等により、常に最新の情報を確認すること。
3. 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 は本書の使用が成功を保証するとは主張していない。本書に、適切な手順やテストがすべて含まれているわけでは無い。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。
4.

情報システム監査基準ハンドブック日本語版出版に寄せて

ISACA（情報システムコントロール協会）が公表している、「情報システム監査基準」（IS Standards for Auditing and Control Professionals）は、ISACA 会員及び公認情報システム監査人（CISA）の資格保持者が行う情報システム監査業務に適用される事となっています。

東京支部の基準委員会では、国際本部の基準改定時に日本語レビューを実施してきておりますが、２００９年は、国際本部 40 周年であると共に、東京支部 25 周年に当たり、これを機に、情報システム監査基準ハンドブック日本語版として出版し、皆様のお手元へお届けする事としました。又、ISACA 東京支部ホームページ上でも無償公開を予定しています。

今回のとりまとめ・出版に当たっては、武田委員長を始めとして基準委員会の皆様のご協力を頂き、日本語版として広く皆様に提供出来る事は大変喜ばしい限りです。ISACA 会員及び公認情報システム監査人（CISA）の皆様にはバイブルとして活用して頂ければと思います。

又、この基準については、基本となる考え方をまとめている事もあり、ISACA のみならず他の監査、コントロールの専門家の方にも有効に活用して頂けるものと考えます。これからも、多くの皆様に有用な情報を提供出来る様、ISACA としての活動を推進して参りたいと思います。

ISACA　東京支部 2008 － 2009　会長
太田　均

目次

ページ

職業倫理規定 [注)]

ISACA は当協会メンバーと当協会公認資格者の専門職として自ら行う行為を指導することを目的として本職業倫理規定を公表するものである。

メンバーと ISACA 公認資格者は：

1. 情報システムの適切なる基準、手続及び管理策の実施を支援すると共に準拠することを推進する。
2. 専門的基準とベストプラクティスに従い、客観性、忠実義務及び専門職的注意を以て職務に従事する。
3. 行為及び品位の高い基準を維持しつつ、適法かつ誠実に利害関係者のために務め、専門性を損なう行為はしない。
4. 法務当局から開示要求された場合を除き、職務を通じて得た情報のプライバシーと機密性を保持する。そのような情報を個人の利益や不適切な団体へ開示しない。
5. 各自の分野で力量を維持し、自ら専門職としての力量をもって完遂できると合理的に想定しうる活動範囲のみ請け負うことに同意する。
6. 業務遂行結果を適切な関係者に通知する。全ての知り得た重要な事実を開示する。
7. 情報システムのセキュリティとコントロールについて利害関係者の理解を高めるべく専門的教育を支援する。

本綱要遵守不履行は、メンバー及び公認資格者の行為を調査し、最悪、懲戒処分もありえる。

注）本職業倫理規定は、当ハンドブック作成に伴い、ISACA 東京支部基準委員会により翻訳されたものであり、ISACA 本部の正式なレビュー・承認を受けたものではない。正式版としては、ISACA 本部の原文（英文）を参照していただきたい。

Code of Professional Ethics

The Information Systems Audit and Control Association, Inc. (ISACA) sets forth this Code of Professional Ethics to guide the professional and personal conduct of members of the Association and/or its certification holders.

Members and ISACA certification holders shall:

1. Support the implementation of, and encourage compliance with, appropriate standards, procedures and controls for information systems.
2. Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards and best practices.
3. Serve in the interest of stakeholders in a lawful and honest manner, while maintaining high standards of conduct and character, and not engage in acts discreditable to the profession.
4. Maintain the privacy and confidentiality of information obtained in the course of their duties unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties.
5. Maintain competency in their respective fields and agree to undertake only those activities, which they can reasonably expect to complete with professional competence.
6. Inform appropriate parties of the results of work performed; revealing all significant facts known to them.
7. Support the professional education of stakeholders in enhancing their understanding of information systems security and control.

Failure to comply with this Code of Professional Ethics can result in an investigation into a member's or certification holder's conduct and, ultimately, in disciplinary measures.

情報システム監査に関する一般基準

序文

情報システムコントロール協会は、情報システム監査業務の特別な性質、監査を実施するのに必要な技能から、情報システム監査に適用される一般基準を制定し、公表する必要があると判断した。
情報システム監査は、関連する自動化されていない処理、及びそれらとのインターフェイスを含む、自動化された情報処理システムのすべての局面（またはその一部分）について調査し、評価する監査と定義する。
情報システムコントロール協会が公表した情報システム監査基準は、情報システムコントロール協会の会員及び公認情報システム監査人（CISA）の資格保持者が行う情報システム監査業務に適用される。

目的

本情報システム監査基準の目的は、監査人に対し職業倫理規程に定められた専門家としての責任を果たす上で最低限必要な能力の水準を理解させ、経営者及びその他の関係者に監査実施者の業務について専門家としての期待できる水準を認識させることである。

情報システム監査基準

概要

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 ー 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 ー 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。
ー パフォーマンス測定
ー IT コントロール・プロファイリング
ー 認識
ー ベンチマーキング
■COBIT コントロール手続 ー 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 ー 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無い。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 International Headquarters、"3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008 USA" まで郵送にて、ISACA 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。

インデックス

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 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。

独立性 S2

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、監査の過程における独立性に関する基準と指針を定めることである。

基準

03　専門家としての独立性
情報システム監査人は、監査に関するすべての点において、態度に於いても、外見的にも、被監査人に対し、独立を保つべきである。

04　組織としての独立性情報システム監査の機能は、監査業務の目的完遂を可能とするために、被監査分野や被監査活動に対し、独立を保つべきである。

コメント

05　監査ポリシーないし監査契約書は、監査機能の独立性及び説明責任を明確に記すべきである。

06　情報システム監査人は、常に、態度に於いても 外見的にも 独立を保ち、また、そう見えるようにすべきである。

07　独立性が、実際に、あるいは、外見的に損なわれる場合、その詳細が適切な関係先（party）に開示されるべきである。

08　情報システム監査人は、被監査分野から、組織的に独立しているべきである。

09　独立性は、情報システム監査人、経営者、監査委員会（存在する場合）により、定期的に評価されるべきである。

10　他の専門基準ないし監督当局によって禁止されている場合を除き、情報システム監査人が情報システムに係る非監査活動を行う場合、その情報システム監査人が独立性を保つ必要は無く、また、独立性を保っているように見える必要も無い。

11　「専門家としての独立性」ないし「組織面の独立性」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 G17、情報システム監査人の独立性に対する非監査業務の影響
  （IS Auditing Guideline G17, Effect of Nonaudit Role on the IS auditor’s Independence）
- ■情報システム監査指針 G12、組織間の関係と独立性
  （IS Auditing GuidelineG12, Organizational Relationship and Independence）
- ■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

12　本基準は、2005 年1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。

専門家としての倫理と基準 S3

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、情報システム監査人が、「 ISACA の職業倫理規定（ISACA Code of Professional Ethics）」を遵守し、専門家として当然の注意を払うための基準を定め、指針を提供することである。

基準

05 ISACA が定める「職業倫理規定」は、「最新の動向」と「監査分野からの要求」に適合させるため、適宜修正される。 ISACA 会員と情報システム監査人は、常に最新の「職業倫理規定」に精通し、情報システム監査人としての責務を果たすに当たり、当該基準を遵守すべきである。

06 ISACA が定める「情報システム監査基準」は、継続的な改善のために定期的なレビューが行われ、監査分野における新たな課題に対応するため、必要に応じ修正される。 ISACA 会員と情報システム監査人は、適用可能な最新の情報システム監査基準を認識し、監査を実施する際には、専門家としてのしかるべき注意を払うべきである。

コメント

07 ISACA 会員ないし CISA 資格保持者が、「 ISACA の職業倫理規定」及び / 又は「情報システム監査基準」を遵守できない場合、その会員ないし CISA 資格保持者の行為が調査されることがあり、最終的に懲戒処分となる場合がある。

08 ISACA 会員と情報システム監査人は、監査を行うに当たり、そのチームメンバーと良く意思疎通し、そのチームが「職業倫理規定」と適用可能な情報システム監査基準を遵守することを保証すべきである。

09 情報システム監査人は、監査を行うに当たり、「専門家としての倫理」あるいは「情報システム監査基準」の適用を懸念させる事柄に直面した場合、これに適切に対応すべきである。情報システム監査人は、「専門家としての倫理」あるいは「情報システム監査基準」の遵守が不徹底ないし不徹底と見なされる場合、その業務を辞退することを考慮すべきである。

10 情報システム監査人は、高潔と高い品行を保ち、監査業務の獲得または実施のため「違法な、非倫理的な、専門家としての規範に反すると見なされる手法」を採用しないようにすべきである。

11 専門家としての倫理とその基準に関し、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 G19、不正行為・例外処理及び不法行為
  （IS Auditing Guideline G19, Irregularities and Illegal Acts）
- ■情報システム監査指針 G7、専門家としてのしかるべき注意
  （IS Auditing Guideline G7, Due Professional Care）
- ■情報システム監査指針 G12、組織の関連と独立性
  （IS Auditing Guideline G12, Organizational Relationship and Independence）
- ■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

12 本基準は、2005 年1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。

専門家としての能力 S4

概要

01　ISACA 監査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、指針を定め提供することにより、情報システム監査人に対し、専門家としての能力を確保してそれを維持することを求めることである。

基準

03　情報システム監査人は、監査業務を遂行するための技能と知識を有し、専門家としての能力を備えているべきである。

04　情報システム監査人は、適切な専門的教育と訓練を継続することにより、専門家としての能力を維持すべきである。

コメント

05　情報システム監査人は、監査を開始する前に、専門家として充分な能力（予定された監査業務に係る技能、知識、経験）を備えていることについての合理的な保証を示すべきである。情報システム監査人がそのような能力を保持していない場合、その監査業務を（実施中であっても）辞退すべきである。

06　情報システム監査人は、CISA ないし他の監査資格を保持している場合、その専門家としての継続教育（ないし能力開発）の要件を満たすべきである。 CISA 資格を保持しない ISACA 会員、あるいは、他の監査資格を保持しない ISACA 会員が、情報システム監査に携わる場合、その会員は、正式な教育、訓練、実務について、充分な経験を積んでいるべきである。

07　情報システム監査人がレビューを行うチームを主導する場合、この情報システム監査人は、対象となる業務に必要な専門家としての適切な能力を、そのチームのメンバー全員が保持していることについての合理的な保証を示さなければならない。

08　専門家としての能力に関し、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。

- ■CISA 資格取得のための教材（CISA certification and training material）
- ■CISA 継続教育の要件（CISA continuing certification and education requirements）
- ■COBIT「フレームワーク」、コントロール目標 M2、M3、M4
  （COBIT Framework, Control objectives M2, M3 and M4）

適用開始日

09　本基準は、2005 年 1 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。

計画策定 S5

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、監査計画策定に係る基準を定め、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、監査の目的を満たし、関係諸法規と当該分野の諸監査基準に準拠するよう、情報システム監査の範囲を定めた計画を策定すべきである。

04　情報システム監査人は、リスクベース監査の手法を導入・構築し、文書化すべきである。

05　情報システム監査人は、監査計画を作成・文書化し、その監査の性格・目的、時期、範囲、必要な諸リソースを詳述すべきである。

06　情報システム監査人は、監査プログラムと手順を作成すべきである。

コメント

07　内部監査について、少なくとも年に1回、実施中の監査活動を前提に、全体監査計画が策定・更新されるべきである。この計画が監査活動の枠組みとなり、監査ポリシーで定められた責任を果たすことを支えるべきである。「新規の」あるいは「更新された」計画は、監査委員会が存在する場合、その委員会によって承認されるべきである。

■（訳注：米国の場合、監査委員会は通常社外取締役により構成される）

08　情報システムに係る外部監査の場合、監査計画は、通常、「個別の監査」あるいは「個別の非監査案件」毎に作成されるべきである。この計画策定の過程で、監査の目的を文書化すべきである。

09　情報システム監査人は、「監査対象となる活動」を理解していなければならない。監査に必要な知識の程度は、監査対象組織の特性、その組織をめぐる環境、諸々のリスク、監査の目的により決定されるべきである。

10　情報システム監査人は、計画中の監査において、すべての重要な事項が充分確認されるであろうことについて、合理的な保証を提示するために、リスク評価を行うべきである。この手順を踏むことにより、監査の戦略、監査の重要度、監査に必要な諸々のリソースを定めることが出来る。

11　監査中に発生した課題（新たなリスク、誤った仮定、既に実施した監査の発見事項）に対処するため、監査中に、監査プログラムないし監査計画、またはその双方を修正する必要が生ずる場合がある。

12　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 G6 情報システムの監査に係る重要性の概念
（IS Auditing Guideline G6, Materiality Concepts for Auditing Information Systems）

■情報システム監査指針 G15 計画策定（IS Auditing Guideline G15, Planning）

■情報システム監査指針 G13 監査計画の作成におけるリスク評価の活用
（IS Auditing Guideline G13, Use of Risk Assessment in Audit Planning）

■情報システム監査指針 G16 組織の IT コントロールに対するサードパーティの影響
（IS Auditing Guideline G16, Effect of Third Parties on an Organisation’sIT Controls）

■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

13　本基準は、2005 年 1 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。

監査業務のパフォーマンス S6

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、監査業務のパフォーマンスに係る基準を定め、指針を提供することである。

基準

03 監督 ー 情報システム監査のメンバーは、監査の目的が達成され、当該分野の諸監査基準が満たされていることについての合理的な保証を確保するため、監督されるべきである。

04 証拠 ー 監査の過程において、情報システム監査人は、監査の目的を達成するために、確実で妥当な証拠を充分得るべきである。監査の発見事項と監査の結論は、この証拠を適切に分析し、解釈することにより裏付けられる。

05 文書化 ー 監査プロセスは、「監査内容」と、「監査発見事項と監査の結論を裏付ける監査証拠」を記述するために、文書化されるべきである。

コメント

06 監査を開始するに当たり、情報システム監査チームの役割と責任、少なくとも、判断実施者、作業実施者、レビュー実施者を定めるべきである。

07 監査(契約) 期間中に実施した業務は、定められた文書化手順に従い、整理・文書化されるべきである。文書化する事項は、監査の目的、監査範囲、監査プログラム、監査実施の行程、収集された監査証拠、監査発見事項、監査の結論、勧告事項等を含むべきである。

08 監査に係る文書は、独立した第三者が同じ結論を得るために監査中に行われたすべての作業を再実施出来るような、充分な内容にすべきである。

09 監査に係る文書には、監査の各業務を行った監査メンバーと、その役割の詳細を記すべきである。一般的に、監査メンバー（のグループ）により実施された、監査の業務、判断、行程、結果は、すべて、検討対象項目の重要性に従い任命された別のメンバーがレビューすべきである。

10 情報システム監査人は、「監査目的の重要性」と「監査証拠を得るために必要な時間と労力」を勘案し、それらに見合った収集可能な監査証拠を使用するよう、計画を立案すべきである。

11 監査証拠は、意見をまとめるために、あるいは、発見事項と監査の結論を裏付けるために、充分かつ確実で、（点検対象事項と）密接な関連性を持つべきである。監査証拠が上記の要件を満たしていないと判断した場合、情報システム監査人は、追加の監査証拠を収集すべきである。

12 監査業務のパフォーマンスに関し、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。
■ COBIT「フレームワーク」、コントロール目標（COBIT Framework, Control objective M4）

適用開始日

13 本基準は、2005 年 1 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。

報告 S7

概要

01 ISACA の情報システム監査基準には、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、「監査の報告」に係る指針を定め・提供することにより、情報システム監査人がその責を果たすことが出来るようにすることである。

基準

03 情報システム監査人は、監査終了後直ちに、適切な様式の報告書を提出すべきである。この報告書には、報告書提出先の組織、具体的な宛先（受領者）、回覧上の制限を明記しておくべきである。

04 監査報告書には、監査範囲、監査目的、監査対象期間、実際に行われた監査作業の種類・時期・程度を記載すべきである。

05 報告書には、監査発見事項、監査の結論、勧告事項、情報システム監査人が当該監査に関し述べておくべき留保事項・制限事項・監査対象範囲の制約を記載すべきである。

06 情報システム監査人は、報告書に記載した個々の監査結果を裏付けるために必要な、充分かつ適切な監査証拠を保有しているべきである。

07 情報システム監査の報告書は、その発行に当たり、署名と日付の記載が為され、また、監査ポリシーないし監査契約書の定めるところに従い配布されるべきである。

コメント

08 報告書の形式と内容は、通常、下記の如き、サービスの種類あるいは契約の種類に応じて変化する。
■監査（直接監査、証明業務）
■レビュー（直接監査、証明業務）
■関係者間で合意された手順

09 情報システム監査人が契約に従い内部統制環境に係る意見表明をする必要があり、重大あるいは重要な弱点を示す監査証拠がある場合、情報システム監査人は、内部統制が有効であるという結論を除外すべきである。監査報告書には、「重大あるいは重要な弱点」と、「統制の要件が達成されることが及ぼす効果」について記述すべきである。

10 情報システム監査人は、報告書を確定し発行する前に、監査対象分野を担当する経営者（執行側）と報告書案の内容について討議を行い、記載すべき経営者（執行側）のコメントがある場合は、それを最終報告書に記載すべきである。

11 情報システム監査人が統制環境（経営執行の枠組み）に重要な不備を発見した場合、その情報システム監査人は、その不備を「監査委員会」ないし「類似の機能（非執行）」に伝え、重要な不備が（必要な連絡先に）連絡済みであることを監査報告書により開示すべきである。
■（訳注：米国の場合、監査委員会は、通常 社外取締役により構成される）

12 情報システム監査人が、個別の監査に関し複数の報告書を発行する場合、最終報告書において、他の報告書をすべて引用しておくべきである。

13 情報システム監査人は、「重要な不備に」比しより影響度が低い内部統制の不備については、経営者（執行側）に伝えて良いか否かを（検討する余地があるため（11 を参照））検討・評価すべきである。上記の場合、情報システム監査人は、「監査委員会」ないし「類似の機能（非執行）」に、その内部統制の不備が経営者（執行側）に伝達されたことを連絡すべきである。

14 情報システム監査人は、適切な対応措置が適切な時期に実施されたか否かを判断するため、以前の監査報告書に記載されている発見事項、監査の結論、勧告事項の情報を入手して、評価すべきである。

15　報告に関し、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。
■情報システム監査ガイドライン G20、報告（IS Auditing Guideline G20, Reporting）
■COBIT「フレームワーク」、コントロール目標 M4.7、M4.8
（COBIT Framework, Control objectives M4.7 and M4.8）

適用開始日

16　本基準は、2005 年 1 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。

フォローアップ S8

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、情報システム監査の過程で実施されるフォローアップ活動に関する基準を定め、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、発見事項と勧告事項に係る報告を行った後、経営者により、適切な時期に適切な対応措置が実施されたか否かを判断するため、適切な関連情報を収集して評価すべきである。

コメント

04　監査の結果示された勧告事項を実現するために経営者が提案した対応措置について 情報システム監査人との間で討議が為された場合、あるいは、かかる対応措置が情報システム監査人に対し提示された場合、これらの対応措置は、経営者の回答（マネジメントレスポンス）として、監査の最終報告書に記載されるべきである。

05　フォローアップの方法、時期、程度は、対象となる発見事項の重要性や、是正措置が取られなかった場合の影響の程度を考慮して決定されるべきである。フォローアップの対象となる事項を記した報告書との関係において、どのような時期にフォローアップを行うべきかということは、当該事項に係るリスクの特性や影響度、あるいは、このことに関して組織が負担すべきコスト等、多面的な要因を勘案した専門家としての判断に委ねられるべきである。

06　経営者の講じた是正措置が効果的に実施されていること、あるいは、是正措置を取らないことに伴うリスクの存在を経営上層部が受容する という手順が為されていることを定期的に監視し、確実にするために、フォローアップのプロセスが情報システムに係る内部監査機能により確立されるべきである。これらのフォローアップに係る責任は、内部監査機能に係る監査ポリシーで定義されることとなる。

07　監査契約の対象範囲と契約条件により、情報システムに係る外部監査人が、合意確定した勧告事項のフォローアップを、情報システムに係る内部監査機能に依存することがある。

08　経営者が勧告事項を導入実施するために為す行為に係る情報を提供し、情報システム監査人がその内容に疑問を感じた場合、フォローアップに係る結論を下す前に、実態を解明把握するため、適切なテストないし他の手段が実施されるべきである。

09　フォローアップの状況に関する報告書（合意確定した勧告事項の導入実施が為されていないことの報告を含む）は、監査委員会が存在する場合は監査委員会に、あるいは、その代わりに、監査対象組織の適切なレベルの執行側経営者に提出されることとなる。

■（訳注：米国の場合、監査委員会は、通常 社外取締役により構成される）

10　フォローアップの一環として、情報システム監査人は、発見事項に係る対策実施が為されていない場合、その発見事項が、フォローアップを実施しているその時点でもなお、問題のある事柄との関連性がある事項となっているか否かを評価すべきである。

適用開始日

11　本基準は、2005 年 1 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。

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跡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跡は、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跡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。

IT ガバナンス S10

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 IT ガバナンス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、情報システムの機能が、監査対象組織のミッション、ビジョン、企業価値、目的、戦略に一致しているか否かをレビューし評価すべきである。

04 情報システム監査人は、情報システムの機能に関し、監査対象企業の業務部門が期待するパフォーマンス（実効性と効率性）についての明確なステートメントが存在するか否かをレビューすべきである。また、その達成度合いを評価すべきである。

05 情報システム監査人は、情報システムの「資源とパフォーマンス」の管理プロセスの実効性をレビューし評価すべきである。

06 情報システム監査人は、法的要件、環境と情報の質に係る要件、受託者責任とセキュリティに係る要件への準拠状況をレビューし評価すべきである。

07 情報システム監査人は、情報システムの機能を評価するために、リスクベース・アプローチを使用すべきである。

08 情報システム監査人は、監査対象組織の統制環境をレビューし評価すべきである。

09 情報システム監査人は、情報システムの環境に悪影響を与える可能性のあるリスクをレビューし評価すべきである。

その他の指針

10 情報システム監査人は、情報システム監査指針 G18「IT ガバナンス」（IS Auditing Guideline G18, IT Governance）を参照すべきである。

11 情報システム監査人は、監査対象組織のビジネス活動を支える情報システムの稼動環境に係るリスクをレビューし評価すべきである。情報システム監査活動は、大きなリスクに曝されている状況を識別・評価し、リスク管理と統制システムの改善に貢献することにより、その組織を支援すべきである。

12 IT ガバナンスは、それ自体をレビューすることも、情報システムの機能として実行されるあらゆるレビュー中で考慮して行くことも、共に可能である。

13 情報システム監査人は、IT ガバナンス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（IS Auditing Guidelines）：

- G5 監査ポリシー
- G6 情報システムの監査に係る重要性の概念（Materiality Concepts for Auditing Information Systems）
- G12 組織の関連と独立性（Organisational Relationship and Independence）
- G13 監査計画におけるリスク評価の実施（Use of Risk Assessment in Audit Planning）
- G15 計画（Planning）
- G16 組織の IT 統制に対するサードパーティの影響（Effect of Third Parties on an Organisation’s IT Controls）

－G17 情報システム監査人の独立性に対する「監査以外の役割」の影響
（Effect of a Nonaudit Role on the IS Auditor’s Independence）
■COBIT マネジメントガイドライン（COBIT Management Guidelines）
■COBIT「フレームワーク」、コントロール目標（COBIT Framework, Control Objectives）。本基準は COBIT のすべてのドメインのすべてのコントロール目標が関係する。
■取締役に対する IT ガバナンスの概要説明、第 2 版、IT ガバナンス協会
（Board Briefing on IT Governance, 2nd Edition, IT Governance Institute）
■米国企業改革法に関する IT コントロール目標、IT ガバナンス協会
（ IT Control Objectives for Sarbanes-Oxley, IT Governance Institute）
■米国企業改革法（2002 年）や他の規則が適用される可能性もある。

適用開始日

14　本基準は、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。

監査計画立案時のリスク評価の使用 S11

概要

01　ISACA の情報システム監査基準には、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　本基準の目的は、監査計画立案時のリスク評価の使用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、情報システムに係る包括的な監査計画を策定し、監査のための諸資源の効果的な配分のための優先順位を決めるに当たり、適切なリスク評価手法を使用すべきである。

04　情報システム監査人は、個別分野のレビューを計画するに当たり、レビュー対象の分野に関連するリスクを識別し、評価すべきである。

コメント

05　リスク評価とは、情報システム監査の対象領域全体の中で監査可能な対象部署・分野等を調査し、「最も大きなリスクにさらされている領域群」をレビュー対象に選択して情報システムの年間計画に含めるために使用する手法である。

06　監査可能な対象部署・分野等は、「組織すべてとそれが使用しているすべてのシステム」の一部分として定義される。

07　「何が情報システム監査の対象領域全体となるか」ということを決定するに当たっては、その組織の IT 戦略計画に関する知識、その運用、責任を担う経営陣との討議に基づいた判断をすべきである。

08　情報システム監査計画策定の基となるリスク評価作業は、少なくとも年 1 回実行され、文書化されるべきである。組織の戦略計画と目的、及び、その組織全体のリスク管理の枠組みは、リスク評価作業の一環とみなされるべきである。

09　個別の監査プロジェクトを選択するためにリスク評価結果を使用することは、情報システム監査人が、情報システム監査計画全体、あるいは、特定分野のレビューを完了させるために必要な情報システム監査のための諸資源の量を数値化し、正当化することを可能にする。また、情報システム監査人は、計画された諸々のレビューをリスクの状況を理解することに基づき優先順位を付け、リスク管理の枠組みの文書化に貢献することができる。

10　情報システム監査人は、レビューを行っている分野に関し、予備的なリスク評価を行うべきである。各々の個別レビューに係る情報システム監査チームの監査目的は、上記のリスク評価の結果を反映すべきである。

11　情報システム監査人は、レビューの完了後、その組織全体のリスク管理の枠組み、あるいは、リスク登録制によるリスクの登録（共に存在する場合）が、レビューの発見事項と勧告事項、及び、それらの事項に関するその後の活動を反映して更新されいることを保証すべきである。

12　情報システム監査人は、情報システム監査指針 G13「監査計画立案時のリスク評価の使用」（IS auditing guideline G13 Use of Risk Assessment in Audit Planning）、及び、情報システム監査手順 P1「情報システムのリスク評価における測定」（IS auditing procedure P1 IS Risk Assessment Measurement）を参照すべきである。

適用開始日

13　本基準は、2005 年 11 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。

監査の重要性 S12

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、監査の重要性、および監査のリスクとの関連性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、監査手順の種類、時期、範囲を決定する際に、監査の重要性および監査リスクとの関連性を考慮すべきである。

04 監査計画の策定において、情報システム監査人は、潜在的なコントロールの欠陥または欠如を考慮し、さらに、コントロールの欠陥または欠如が情報システムに重大な不備または重要な欠陥をもたらすかどうかを考慮すべきである。

05 情報システム監査人は、コントロールの軽微な不備または欠陥と欠如が累積することにより、情報システムにとって重大な不備または重要な欠陥となることを考慮すべきである。

06 情報システム監査人の報告では、無効なコントロールまたはコントロールの欠如、及びコントロールの不備の重要性、重大な不備または主要な欠陥により欠陥が顕在化する可能性を明らかにすべきである。

その他の指針

07 監査リスクとは、情報システム監査人が監査の発見事項に基づいて不正確な結論に達することである。情報システム監査人は、固有リスク、統制リスク、発見リスクといった監査リスクの 3 つの要素に注意すべきである。リスクに関する詳細は、「G13 監査計画の作成におけるリスク評価の活用（G13, Use of Risk Assessment in Audit Planning）」を参照すること。

08 監査の計画及び実施において、情報システム監査人は、監査リスクを容認可能な低レベルに抑えて監査目的を達成しようとすべきである。これは、情報システム及び関連するコントロールを適切に評価することで達成される。

09 コントロールの欠如が、コントロール目標の達成を合理的に保証できない結果をもたらすならば、コントロールの欠陥は「重要」と見なされる。

10 重要と分類される欠陥は、以下の内容を伴う。

- コントロールがあるべき場所にない、コントロールが機能していない、コントロールが不十分であるのいずれか及び全て。
- 深刻化が確実であること。

11 重要な欠陥とは、望ましくない出来事が防止されず発見されないというわずかな可能性を高める結果となる、重大な不備であるか、または重大な不備の複合体である。

12　監査の重要性と情報システム監査人が受容できる監査リスクのレベルは反比例する。すなわち、重要性レベルが高くなればなるほど、監査リスクの受容レベルが低くなり、重要性レベルが低くなれば監査リスクの受容レベルが高くなる。これにより、情報システム監査人は監査手順の種類、時期、範囲を決定することができる。たとえば、情報システム監査人が特定の監査手順を計画する際に、重要性を低くすることに決めると、それにより監査リスクは高まる。そのため、情報システム監査人は、コントロールのテスト範囲を広げるか（統制リスクの評価を低減する）、実質的なテスト手順を拡大する（発見リスクの評価を低減する）ことで、補完することを期待する。

13　情報システム監査人は、コントロールの不備または不備の複合体が重大な不備または重要な欠陥であるかどうかを判断する際に、補完コントロールの影響を評価し、さらに、そのような補完コントロールが有効であるかどうかを評価すべきである。

14　情報システム監査人による重要性と監査リスクの評価は、状況と環境の変化により、時によって異なる。

15　情報システム監査人は、「情報システム監査指針 G6、情報システムの監査に係る重要性の概念（IS Auditing Guideline G6 Materiality Concepts for Auditing Information Systems）」を参照すべきである。

16　監査の重要性に関する詳細は、以下の指針を参照すること。

■情報システム監査指針（IS Auditing Guidelines）：
－G2 監査証拠の必要条件（G2 Audit Evidence Requirement）
－G5 監査ポリシー（G5 Audit Charter）
－G8 監査書類（G8 Audit Documentation）
－G9 不正行為に対する監査の勘案（G9 Audit Considerations for Irregularities）
－G13 監査計画の作成におけるリスク評価の活用
（G13 Use of Risk Assessment in Audit Planning）
■COBIT 4.0、IT ガバナンス協会、2005 年
■米国企業改革法に関する IT コントロール目標、IT ガバナンス協会、2004 年
（IT Control Objectives for Sarbanes-Oxley, IT Governance Institute）

適用開始日

17　本基準は、2006 年 7 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。

他の専門家の作業を使用 S13

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、情報システム監査人が監査において他の専門家の作業を利用する際の指針を定め、提供することである。

基準

03 情報システム監査人は、必要に応じて、他の専門家の作業を監査に利用することを考慮すべきである。

04 情報システム監査人は、他の専門家に依頼する前に、その人物の専門家としての資格、能力、関連のある経験、リソース、独立性、品質管理プロセスを評価し、それらが満足のいくものでなければならない。

05 情報システム監査人は、他の専門家の作業を監査の一環として評価、レビューおよび査定し、その作業の利用および依拠の範囲を判断すべきである。

06 情報システム監査人は、実施中の監査の目的を達成するために、他の専門家の作業が十分かつ完全であるかどうかを判断すべきである。そのような結論は明確に文書化しておくべきである。

07 情報システム監査人は、他の専門家の作業が十分で適切な監査証拠を提供しないような状況において、十分かつ適切な監査証拠を得るために、追加のテスト手続きを適用すべきである。

08 情報システム監査人は、追加のテスト手順から必要とされる証拠が得られない場合には、適切な監査意見を提供し、監査範囲の限定を考慮すべきである。

その他の指針

09 情報システム監査人は、監査作業の効果を損なう制約がある時、または監査の質が高まる可能性がある時には、監査において他の専門家の作業を利用するよう考慮すべきである。これには、たとえば、技術的な作業を実施する際に知識が必要な場合、監査リソースが不足しているような場合、時間の制約がある場合などがある。

10 「専門家」とは、外部の会計事務所の情報システム監査人、管理コンサルタント、IT 専門家、または経営陣や情報システム監査チームに任命された監査領域における専門家などを指す。

11 専門家は、組織の内部または外部の人物のいずれでも可能である。専門家が組織の別部門に従事している場合、専門家の報告に信頼がおかれる場合がある。場合によっては、情報システム監査人が裏付けを示す文書および作業書類を入手できなくても、それにより、情報システム監査の保障の必要性が減少することもある。情報システム監査人は、そのような場合の意見の表明については、慎重にすべきである。

12 情報システム監査人は、すべての作業書類、裏付けを示す書類、他の専門家の報告を入手しなければならない。ただし、入手により法的な問題が発生しない場合に限る。専門家が記録を入手することで法的な問題が起こり、入手が不可能になる場合、情報システム監査人は、専門家の作業の利用および依拠の範囲を適切に判断すべきである。

13 専門家の報告の採用に関する情報システム監査人の視点、妥当性、コメントは、情報システム監査人の報告書の一部を構成すべきである。

14 情報システム監査人は、監査目的を達成するために、十分な、信頼性ある、妥当かつ有用な証拠を取得する必要性について記載した「情報システム監査基準 S6 監査業務のパフォーマンス（IS Auditing Standard S6 Performance of Audit Work）」を参照すべきである。

15　情報システム監査人が、監査を実施するために必要とされる技能や他の能力を持たない場合、情報システム監査人は、他の専門家の支援を求める必要がある。ただし、情報システム監査人は、実施される作業に対する十分な知識を保持すべきであるが、専門家と同等の知識水準を期待されるべきではない。

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 G1 他の監査人及び専門家の作業の利用（IS Auditing Guideline G1 Using the Work of Other Auditors and Experts）」を参照すべきである。

17　他の監査人及び専門家の作業の利用に関する詳細は、以下の指針を参照すること。

■情報システム監査指針（IS Auditing Guidelines）：
－G5 監査ポリシー（G5 Audit Charter）
－G8 監査書類（G8 Audit Documentation）
－G2 監査証拠の必要条件（G2 Audit Evidence Requirement）
－G10 監査サンプリング（G10 Audit Sampling）
－G13 監査計画におけるリスク評価の使用（G13 Use of Risk Assessment in Audit Planning）
■COBIT 4.0、IT ガバナンス協会、2005 年
■米国企業改革法に関する IT コントロール目標、IT ガバナンス協会、2004 年
（IT Control Objectives for Sarbanes-Oxley, IT Governance Institute）

適用開始日

18　本基準は、2006 年 7 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。

監査証拠 S14

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、これらに関する指針も示されている。

02 本基準の目的は、監査証拠の構成要素、および情報システム監査人により収集される監査証拠の質と量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、監査結果の基となる合理的な結論を導き出すために、十分かつ適切な監査証拠を入手すべきである。

04 情報システム監査人は、監査の過程で得られる十分な量の監査証拠を評価する必要がある。

コメント

適切な証拠

05 監査証拠：

- ■監査人が実施する手続きを含む
- ■情報システム監査人が実施する手続きの結果を含む
- ■電子形式または書面による原資料、記録、監査の裏付けに使用された補完的情報を含む
- ■ 監査作業の発見事項と結果を含む
- ■ 関係諸法規と方針に基づいて作業が実施されたことを証明する

06 コントロールのテストから監査証拠を得る際は、情報システム監査人は、統制リスクの評価レベルを立証する監査証拠の完全性を考慮すべきである。

07 監査証拠は適切に識別し、相互参照して、一覧表にまとめる必要がある。

08 監査証拠の信頼性を評価する際は、監査証拠の情報源、種類（書面、口頭、目視、電子など）、真正性（デジタル署名、手書きの署名、スタンプなど）などを考慮すべきである。

信頼性の高い証拠

09 通常、監査証拠は次の場合に信頼性がより高まる。

- ■口頭表現ではなく、書面の形式をとる場合
- ■独立性を保つ情報源から取得した場合
- ■被監査組織から提出されたのではなく、情報システム監査人が自ら取得した場合
- ■独立した第三者によって証明された場合
- ■独立した第三者が保持している場合

10 情報システム監査人は、監査の目的とリスクを満たす必要のある証拠を取得する、最もコスト効果の高い方法を考慮すべきである。ただし、収集の難しさおよびコストは、必要なプロセスを省略するための正当な理由にはならない。

11 監査証拠を収集する手順は、監査対象によって異なる（監査の種類、監査のタイミング、専門的判断など）。情報システム監査人は、監査目的のために最も適切な手順を選択すべきである。

12　情報システム監査人は、次の方法によって監査証拠を取得することができる。
- ■検査
- ■観察
- ■質問と確認
- ■再実施
- ■再計算
- ■演算
- ■分析的手順
- ■一般的に受け入れられているその他の方法

13　情報システム監査人は、情報の信頼性と更なる立証の要件を評価するために、得られた情報の発生源と性質を考慮に入れるべきである。

十分な証拠

14　証拠が十分であると考えられるのは、監査の目的と範囲に関するすべての重要な論点に対する裏付けが得られる場合である。

15　資格のある第三者がテストを再実施しても同じ結果が得られるように、監査証拠は客観的で十分なものでなければならない。証拠はその事項の重要性と関連するリスクに見合うものでなければならない。

16　適切性が監査証拠の質の目安となる一方、十分性が監査証拠の量の目安となる。このような状況において、情報システム監査人が監査手順を実行するために組織から得た情報を使用する際、情報システム監査人は、その情報の正確さと完全性を重視すべきである。

17　情報システム監査人が十分な監査証拠を得られないと確信するような状況では、情報システム監査人は監査結果の報告と同じように、その事実を報告する必要がある。

保護及び維持

18　監査証拠は、未許可のアクセスおよび変更から保護されなければならない。

19　監査作業の終了後、監査証拠は、すべての関係諸法規と方針を遵守するために必要な期間保管されなければならない。

参照

20　監査証拠に関する詳細は、以下の指針を参照すること。
- ■情報システム監査基準 S6、監査作業の実施
  （IS Auditing Standard S6 Performance of Audit Work）
- ■情報システム監査指針 G2、監査証拠の必要条件
  （IS Auditing Guideline G2 Audit Evidence Requirement）
- ■情報システム監査指針 G8、監査書類（IS Auditing Guideline G8 Audit Documentation）
- ■COBIT コントロール目標、ME2 内部統制のモニタリングと評価、および ME3 規制に対するコンプライアンスの保証
  （COBIT control objectives ME2 Monitor and evaluate internal control and ME3 Ensure regulatory compliance）

適用開始日

21　本基準は、2006 年 7 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。

IT コントロール S15

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 本基準の目的は、IT コントロールに係る基準を定め、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、監査対象組織の内部統制環境に不可欠な要素である IT コントロールを評価し監視すべきである。

04 情報システム監査人は、IT コントロールの設計、導入、運用、改善に関する助言を与えて、経営者を支援すべきである。

コメント

05 経営者は、IT コントロールを含む、組織の内部統制環境に対する説明責任がある。内部統制環境は、内部統制システムの主要な目的を達成するための規律、フレームワーク、構造を提供する。

06 CobiT ではコントロールを「事業目標を達成し、望ましくないイベントの阻止または発見と是正を合理的に保証することを主眼として策定されたポリシー、手続、実践方法、および組織構造」と定義している。さらに、コントロール目標を「ある特定のプロセスでコントロール手順を導入することにより達成される、望ましい結果または目的を示す記述」と定義している。

07 IT コントロールは汎用的 IT コントロールを含む全般的 IT コントロール、詳細 IT コントロール、およびアプリケーションコントロールで構成されており、IT システムとサービスの調達、導入、提供、およびサポートにおけるコントロールを対象とする。

08 全般的 IT コントロールとは、組織の IT システムとインフラストラクチャの機能全般に対するリスク、および広範な自動化ソリューション（アプリケーション）セットに対するリスクを最小限に抑えるコントロールである。

09 アプリケーションコントロールとは、アプリケーション内に組み込まれたコントロールセットである。

10 汎用的 IT コントロールとは、IT 環境を管理し監視するための全般的 IT コントロールであり、そのためあらゆる IT 関連の活動に影響がある。これらは全般統制のサブセットである。なぜならこれらは IT の管理と監視に焦点を置く全般的 IT コントロールであるためである。

11 詳細 IT コントロールはアプリケーションコントロールに加えて、汎用的 IT コントロールを含まない全般的 IT コントロールから成り立っている。

12　情報システム監査人は、IT コントロールプロセスの状態に関して保証を与えるために、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と監査資源を効果的に配分するための優先順位の決定に取り組むべきである。コントロールプロセスは統制環境の一部を成す方針、手順、活動であり、リスク管理プロセスにより確立されたリスク許容範囲内にリスクが収まるように策定される。

13　情報システム監査人は、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、IT コントロールのレビューの際に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。

14　組織がサードパーティを使用すると、組織のコントロールおよび関連するコントロール目標の達成において、サードパーティは主要な要素となり得る。情報システム監査人は、IT 環境、関連するコントロール、および IT コントロール目標に関して、サードパーティが担う役割を評価すべきである。

15　IT コントロールに関し追加情報を得るために、次に掲げる ISACA および ITGI ™（IT Governance Institute®）指針を参照すべきである。

- ■情報システム監査指針 G3 コンピュータ支援監査技法（CAAT）の使用（Use of Computer-assisted Audit Techniques（CAATs））
- ■情報システム監査指針 G11 汎用的 IS コントロールの影響（Effect of Pervasive IS Controls）
- ■情報システム監査指針 G13 監査計画におけるリスク評価の使用（Using Risk Assessment in Audit Planning）
- ■情報システム監査指針 G15 計画（Planning）
- ■情報システム監査指針 G16 組織の IT コントロールに対するサードパーティの影響（Effect of Third Parties on an Organisation’s IT Controls）
- ■情報システム監査指針 G20 報告（Reporting）
- ■情報システム監査指針 G36 バイオメトリクス（生体特性識別）コントロール（Biometric Controls）
- ■情報システム監査指針 G38 アクセスコントロール（Access Controls）
- ■COBIT フレームワークおよびコントロール目標（COBIT framework and control objectives）

適用開始日

16　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。

電子商取引 S16

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 (COBIT 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。


ISACA®
Serving IT Governance Professionals