情報システム監査および保証業務基準
1203 実施および監督

情報システム監査および保証業務の専門性およびそのような業務を実施するために必要なスキルには、情報システム監査および保証業務に専ら適用される基準が必要となる。情報システム監査および保証業務基準の策定と普及は、ISACA®の職業的専門家による監査業界に対する貢献の基礎となる。

情報システム監査および保証業務基準は、情報システム監査と監査報告の必須要件を規定し、以下の情報を提供する。

- 情報システム監査および保証業務の専門家に対し、ISACA 職業倫理規定（ISACA Code of Professional Ethics）に規定された職業的専門家の責任を果たすために必要な、最低限許容可能な実施水準
- 経営者およびその他の関係者からの、業務実施者の作業に関する職業的専門家のへの期待
- CISA®（Certified Information Systems Auditor®）資格保有者に対し、その要件。この基準に違反すると、ISACA 理事会または関係する委員会により CISA 保有者の行為が調査され、最終的に懲戒処分となる場合がある。

情報システム監査および保証業務の専門家は、業務が ISACA 情報システム監査および保証業務基準またはその他の適用される職業的専門家としての基準に従って実施されたという表明文を、必要に応じて各自の作業において含めるべきである。

情報システム監査および保証業務の専門家のための *ITAF™* フレームワークは、以下の複数レベルのガイダンスを提供している。

- **基準**は、次の 3 つに分類される。
  - 一般基準（1000 シリーズ） – 情報システム監査および保証業務の専門家が活動するガイダンスとなる原則。これはすべての業務の実施に適用され、情報システム監査および保証業務の専門家の倫理、独立性、客観性および正当な注意、ならびに知識、能力およびスキルに関するものである。「基準」の記述（太字表記）は必須事項である。
  - 実施基準（1200 シリーズ） – 計画と監督、範囲の決定、リスクと重要性、資源の動員、監督と業務割り当ての管理、監査および保証業務の証拠、職業的専門家としての判断と正当な注意等、業務の実施に関するものである。
  - 報告基準（1400 シリーズ） – 報告書の種類、伝達手段および伝達される情報に関するものである。
- **ガイドライン**は、基準を支援するものであり、同様に 3 つに分類される。
  - 一般ガイドライン（2000 シリーズ）
  - 実施ガイドライン（2200 シリーズ）
  - 報告ガイドライン（2400 シリーズ）
- **ツールと技法**は、情報システム監査および保証業務の専門家のための追加的ガイダンス、例えばホワイトペーパー、情報システム監査・保証業務手続書、COBIT® 5 製品シリーズ、を提供する。

ITAF で使用する用語のオンライン用語集が *www.isaca.org/glossary* で提供されている。

免責条項：ISACA は、ISACA の職業倫理規定（ISACA Code of Professional Ethics）に規定された職業的専門家の責任を果たすために必要な最低限許容可能な実施水準として、当ガイダンスを策定した。ISACA は当文書の利用が成功する結果を保証するとは主張していない。当出版物は、適切な手続やテストをすべて含むものではなく、また同じ結果を得るための他の手続やテストを排除するものではない。個別の手続やテストの妥当性を判断する際、統制の専門家は、特定のシステムや情報システム環境から生じる特定の統制の状況に対し、自らの職業的専門家としての判断を適用すべきである。

ISACA の Carrier Management Committee (PSCMC)は、基準およびガイダンスの策定に際して広範な意見聴取に取り組んでいる。ドキュメントの発行に先立ち、パブリックコメントを得るため国際的に公開草案を公表する。コメントは、E メール（*standards@isaca.org*）、ファクス（+1.847.253.1443）または郵送（ISACA International Headquarters, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, USA）で、Director of Professional Standards Development 宛に提出できる。

情報システム監査および保証業務基準 1203 実施および監督

基準

1203.1 情報システム監査および保証業務の専門家は、識別されたリスクを対象とした承認済みの情報システム監査計画に従い、合意済みのスケジュール内に作業を実施すること。

1203.2 情報システム監査および保証業務の専門家は、監査の目的を達成し、適用可能な職業的専門家としての監査基準を満たすために、監督責任をもつ情報システム監査スタッフに対して監督を行うこと。

1203.3 情報システム監査および保証業務の専門家は、その知識とスキルのレベル以内である職務か、または監査業務遂行中にスキルを習得するあるいは監督下で職務を達成することが合理的に期待できる職務のみを引き受けること。

1203.4 情報システム監査および保証業務の専門家は、監査の目的を達成するために十分かつ適切な証拠を入手すること。監査の発見事項と結論は、この証拠を適切に分析し、解釈することにより裏付けること。

1203.5 情報システム監査および保証業務の専門家は、監査作業および発見事項と結論を裏付ける監査証拠について記述し、監査プロセスを文書化すること。

1203.6 情報システム監査および保証業務の専門家は、発見事項を識別し、結論付けること。

重要事項

情報システム監査および保証業務の専門家は、以下を満たすべきである。

- 各自のスキルおよび経験が業務の必要性に一致するようチームメンバーを選任する。
- 必要に応じて情報システム監査チームに外部資源を追加し、外部資源の作業が適切に監督されることを確保する。
- 業務全般において、特定の情報システム監査チームメンバーの役割および責任を管理し、最低限、以下に対応する。
  - 実務およびレビューの役割分担
  - 手法およびアプローチを設計する責任
  - 監査または保証手続書の作成
  - 作業の実施
  - 発生した課題、懸念事項、問題への対処
  - 発見事項の文書化および明確化
  - 監査報告書の作成
- 別の適任のチームメンバーによって、チームメンバーが実施した業務のすべての職務がレビューされる。
- 入手可能な最良の監査証拠を使用する。監査証拠の使用は、監査目的の重要性および証拠の入手に要する時間と労力との関係と調和させるべきである。
- 入手した証拠が、意見形成や発見事項と結論を裏付けるのに十分かつ適切な規準を満たさない場合、職業的専門家の判断により追加的証拠を入手する。
- 業務期間中に実施した作業について、予め定められた文書化と承認手続に従い整理して文書化する。

情報システム監査および保証業務基準 1203 実施および監督

重要項目

続く

- 以下を文書に含める。
  - 監査の目的、作業範囲、監査手続書、実施した監査の手順、入手した証拠、発見事項、結論および勧告事項
  - 分別があり、知識のある人であれば、業務中に実施した職務を再実施し、同じ結論に達することが可能な程度に十分な詳細情報
  - 各職務の実施者と、文書作成やレビューにおける当該実施者の役割
  - 文書を作成およびレビューした日付
- 業務の重要領域、発生した問題とその解決策、ならびに被監査組織のアサーションについて明瞭かつ詳細に記載した確認書を被監査組織から入手する。
- 監査業務に関する被監査組織の責任の認識を示すために、被監査組織が確認書に署名し、日付を記載しているか、確かめる。
- 監査業務の実施過程で受領した書面または口頭による陳述を調書化して保存する。

基準とガイドラインへのリンク

種類	表題
基準	1005 職業的専門家としての正当な注意
基準	1205 証拠
基準	1401 報告
ガイドライン	2202 計画におけるリスク評価

適用開始日

本 ISACA 基準は、2013 年 11 月 1 日以降に開始されるすべての情報システム監査および保証業務に適用される。