情報システム監査および保証業務基準
1201 監査および保証業務計画

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 1201 監査および保証業務計画

基準

1201.1 **情報システム監査および保証業務の専門家は、各情報システム監査および保証業務を計画し、以下に対応すること。**

- **目的、範囲、スケジュールおよび成果物**
- **適用される法令および職業的専門家としての監査基準への準拠**
- **リスクベースのアプローチの利用（適切な場合）**
- **業務固有の課題**
- **文書化および報告に関する要求事項**

1201.2 **情報システム監査および保証業務の専門家は、以下について記述した情報システム監査または保証業務のプロジェクト計画を策定し、文書化すること。**

- **業務の内容、目的、スケジュール、および資源に関する要求事項**
- **業務を完了するための監査手続の実施時期および範囲**

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。

- 監査対象の活動を理解する。必要な知識の範囲は、事業体の特性、事業環境、リスクの領域および業務の目的により決定されるべきである。
- 政府または業界が公表した法令、規則、指令およびガイドラインにより提供される、主題に関するガイダンスまたは方向性を検討する。
- 業務においてすべての重要な事項が適切に対応されることに合理的な保証を提供するために、リスク評価を行う。そのうえで、監査の方針、重要性の基準値および資源に関する要求事項を策定することができる。
- 適切なプロジェクト管理手法を利用して、活動が順調かつ予算内で進行することを確実にするために、業務のプロジェクト計画を策定する。
- 計画には、以下のような業務固有の課題を含める。
  - 適切な知識、スキルおよび経験を備えた人的資源の利用可能性
  - 証拠の収集、テストの実施および報告用の情報の作成・要約のために必要なツールの特定
  - 使用すべき評価規準
  - 報告に関する要求事項および報告書の配布
- 以下の各項を明示した情報システム監査または保証業務のプロジェクト計画を文書化する。
  - 目的、範囲およびスケジュール
  - 資源
  - 役割と責任
  - 識別されたリスクの領域と監査・保証業務計画への影響
  - 採用するツールと手法
  - 実施すべき事実調査のインタビュー
  - 入手すべき関連情報
  - 入手した情報とその証拠としての利用を検討または検証するための手続
  - アプローチ、手法、手続、および予想される結果と結論に関する仮定
- 実施時期、資源の利用可能性、およびその他の経営者および被監査組織の責任と要求事項について、可能な範囲で業務の予定を決める。
- 新たなリスクや誤った仮定あるいは実施済みの手続からの発見事項といった、監査業務中に発生した事項に対応するために、情報システムの監査ま

重要事項続き

たは保証業務期間中にプロジェクト計画を変更する。

- 内部監査業務に関しては以下を行う。
  - 監査規程を被監査組織に伝達する。必要であれば契約書または同等の文書を使用して、特定の監査業務への関与についてより明確にする、あるいは確認する。
  - 計画を被監査組織に伝達することで、被監査組織に十分な情報を与えるとともに、必要な時に適切な個人、文書および他の資源にアクセスできるようにしてもらう。
- 外部監査・保証業務に関しては以下を行う。
  - 情報システム外部監査および保証業務ごとに、個別に契約書を作成する。
  - 情報システム外部監査および保証業務ごとに、プロジェクト計画書を作成する。この計画書には、最低限、業務の目的および範囲を記載すべきである。

ガイドラインへのリンク

種類	表題
ガイドライン	2201 監査および保証業務計画

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。