情報システム監査および保証業務基準 1401 報告

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 1401 報告

基準

1401.1 **情報システム監査および保証業務の専門家は、業務の完了時に結果を伝達するために、以下の内容を記載した報告書を提供すること。**

- **事業体名、想定される受領者、および内容と配布に関する制限事項**
- **実施した作業の範囲、目的、対象期間、および種類・時期・範囲**
- **発見事項、結論および勧告**
- **情報システム監査および保証業務の専門家の業務に関する範囲の限定あるいは制約**
- **監査規程または監査・保証業務契約書の条項に従った署名、日付および配布**

1401.2 **情報システム監査および保証業務の専門家は、監査報告書における発見事項の十分かつ適切な証拠による裏付けを確保すること。**

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。

- 監査業務の重要領域、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。証明業務においては、誤解が生じる可能性を軽減するために、被監査組織からの陳述を書面で入手する。
- 実施した業務の種類（下記参照）に対応させて様式および内容を変更する。
  - 監査（直接報告かアテスト）
  - レビュー（直接報告かアテスト）
  - 合意された手続
- 重大または重要な欠陥およびそれらが監査業務の目的の達成に与える影響を報告書に記述する。
- 最終版の報告書を作成し発行する前に、主題領域における報告書の草案の内容について経営者と討議し、必要に応じて最終版の報告書に発見事項、結論および勧告事項に対する経営者の回答を含める。
- 統治責任者および該当する場合は責任を有する権限者に、統制環境における重要な不備と重大な欠陥を伝達し、報告書でこれらが伝達されたことを開示する。
- 最終報告書で別個の報告書があれば、これを参照する。
- 重要な不備には至らないが軽微ではない内部統制の不備を被監査組織の管理者に伝達する。このような場合、かかる内部統制の不備が被監査組織の管理者に伝達されたことを、統治責任者あるいは責任を有する権限者に通知する。
- 業務の実施において適用された基準を特定し、基準への違反があれば伝達する。

用語

用語	定義
関連情報	統制に関して、基礎となる統制または統制の構成要素の運用状況について評価者に有意義なことを伝える。統制の運用状況を直接確認する情報が最も関連性が高い。統制の運用状況に間接的に関連する情報も関連性はあるが、直接的な情報よりは関連性が低い。COBIT 5 の情報品質の達成目標を参照。
信頼性の高い情報	正確で検証可能、かつ客観的な情報源からの情報。COBIT 5 の情報品質の達成目標を参照。
十分な情報	評価者が情報を収集した時に、合理的な結論を形成するために情報が十分であること。情報が十分であるためには、まず情報が適切なものでなければならない。 COBIT 5 の情報品質の達成目標を参照。
適切な情報	関連性（すなわち意図した目的に適合すること）、信頼性（すなわち正確で検証可能、かつ客観的な情報源によること）、適時性（すなわち適切な期間内に作成され、利用されること）を備えた情報。COBIT 5 の情報品質の達成目標を参照。
適時の情報	統制の不備が事業体にとって重大になる前にこれを防止もしくは発見できる期間内に作成され、利用される情報。COBIT 5 の情報品質の達成目標を参照

基準とガイドラインへのリンク

種類	表題
ガイドライン	2401 報告

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。