

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・保証業務手順書、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。

ISACA 2012-2013 Professional Standards and Career Management Committee	
Steven E. Sizemore, CISA, CIA, CGAP, Chairperson	Texas Health and Human Services Commission, USA
Christopher Nigel Cooper, CISM, CITP, FBCS, M.Inst.ISP	HP Enterprises Security Services, UK
Ronald E. Franke, CISA, CRISC, CFE, CIA, CICA	Myers and Stauffer LC, USA
Murari Kalyanaramani, CISA, CISM, CRISC, CISSP, CBCP	British American Tobacco IT Services, Malaysia
Alisdair McKenzie, CISA, CISSP, ITCP	IS Assurance Services, New Zealand
坂川 克己, CISA, CRISC, PMP	株式会社 JIEC, Japan
Ian Sanderson, CISA, CRISC, FCA	NATO, Belgium
Timothy Smith, CISA, CISSP, CPA	LPL Financial, USA
Rodolfo Szuster, CISA, CA, CBA, CIA	Tarshop S.A., Argentina

情報システム監査および保証業務基準 1205 証拠

基準

- 1205.1** 情報システムの監査および保証業務の専門家は、業務の結果の基となる合理的な結論を導き出すために、十分かつ適切な証拠を入手すること。
- 1205.2** 情報システムの監査および保証業務の専門家は、結論を裏付けし、業務の目的を達成するため、入手した証拠が十分であることを評価すること。
-

重要事項

業務の実施において、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。

- 以下を含む十分かつ適切な証拠を入手する。
 - 実施した手続
 - 実施した手続の結果
 - 原始文書（電子形式または書面による）、記録、業務の裏付けに利用された補強情報
 - 業務の発見事項および結果
 - 作業が実施されたこと、および適用される法令やポリシーに準拠していることの文書化
- 文書作成において以下の条件を満たすべきである。
 - 一定期間保存して利用可能とし、監査または保証業務を実施する組織のポリシーならびに関連する職業的専門家としての基準、法令を満たした形式とする
 - 作成および保存期間を通じて、無許可での開示または修正から保護する
 - 保存期間終了時に適切に廃棄する
- 統制のテストによる証拠の入手時に、統制リスクの評価レベルを裏付けるための証拠の十分性を考慮する。
- 証拠を適切に識別し、相互参照し、分類する。
- 証拠の信頼性を評価する際は、証拠の情報源、種類（書面、口頭、目視、電子形式など）、真正性（デジタル署名、手書き署名、印鑑など）などの特性を考慮する。
- 業務の目的とリスクを満たすために必要な証拠を収集する際には、最も費用対効果が高く時宜にかなった方法を考慮する。ただし、入手の難しさや費用は必要な手続を省略するための正当な理由にはならない。
- 監査対象の主題によって（すなわち、主題の性質、監査の実施時期、職業的専門家としての判断によって）、証拠を収集するための最適な手続を選択する。証拠を入手するために利用する手続には、以下が含まれる。
 - 質問と確認
 - 再実施
 - 再計算
 - 計算
 - 分析的手続
 - 閲覧
 - 観察
 - 一般的に認められたその他の方法

情報システム監査および保証業務基準 1205 証拠

重要事項 続き

- 情報の信頼性と追加的な検証の要件を評価するために、得られた情報の情報源と種類を考慮に入れる。通常、次の場合に、証拠の信頼性はより高い。
 - 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、専門家が入手した場合
 - 独立した第三者によって証明された場合
 - 独立した第三者に保持されていた場合
 - 査閲の結果
 - 観察の結果
- 適格な第三者がテストを再実施しても同様の結果および結論が得られるように、客観的な証拠を入手する。
- 関連する事項とリスクの重要性に見合う証拠を入手する。
- 企業から入手した情報が情報システム監査または保証業務の専門家によって監査手続を実施するために使用される場合、情報の正確性および網羅性に相応の重点を置く。
- 情報システム監査または保証業務の結果の伝達と整合する方法で十分な証拠を入手できないような状況があればそれを開示する。
- 証拠を未承認のアクセスおよび変更から保護する。
- 情報システム監査または保証作業の完了後、すべての関係法令とポリシーを遵守するために必要な期間、証拠を保存する。

用語

用語	定義
適切な証拠	証拠の質的尺度
十分な証拠	監査の目的および範囲に対するすべての重要な質問に答えうる証拠の量的尺度。証拠を参照。

ガイドラインへのリンク

種類	表題
ガイドライン	2205 証拠

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。