情報システム監査および保証業務基準
1207 非遵守行為および違法行為

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。

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 1207 非遵守行為および違法行為

基準

1207.1 **情報システムの監査および保証の専門家は、業務中、非遵守行為および違法行為のリスクを検討すること。**

1207.2 **情報システムの監査および保証の専門家は、業務中、職業的専門家としての懐疑心を維持すること。**

1207.3 **情報システムの監査および保証の専門家は、重要な非遵守行為および違法行為があれば、該当当事者に適時に文書化して伝達すること。**

重要事項

情報システム監査および保証の専門家は、以下を満たすべきである。

- 業務の計画および実施において、以下により、監査リスクを許容可能な水準まで軽減する。
  - 非遵守行為および違法行為のリスクの評価に関係なく、非遵守行為および違法行為による重大な誤謬、統制の不備、虚偽表示が存在する可能性を認識している。
  - 業務の主題、範囲および目的に関連する非遵守行為および違法行為を防止または発見する目的の内部統制を含む、事業体とその環境の理解を得る。
  - 事業体内において、実際に発生したか、発生の疑いまたは申立てがある非遵守行為および違法行為を、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、十分かつ適切な証拠を入手する。
- 監査手続の実施時、非遵守行為および違法行為が原因で重大な誤謬、統制の不備または虚偽表示のリスクを示すような、異常もしくは予期しない関係性を考慮する。
- 内部統制の適切性および経営者が非遵守行為および違法行為を防止または発見することを意図した統制を無効にするリスクをテストするための手続を立案し、実施する。
- 識別された誤謬、統制の不備または虚偽表示が非遵守行為および違法行為の兆候を示しているか評価する。そのような可能性がある場合、その業務における他の状況、特に経営者の陳述に関係して、暗示された事柄を考慮する。
- 以下の目的のため、業務に応じ最低年 1 回またはそれ以上の頻度で、経営者確認書を入手する。
  - 非遵守行為および違法行為を防止し発見するために内部統制を整備する責任が経営者にあることを認める。
  - 非遵守行為および違法行為の結果である誤謬、統制の不備または虚偽表示の存在を示すリスク評価に関する結果を開示する。
  - 内部統制において重要な役割を持つ経営者と従業員に関して、事業体に影響する非遵守行為および違法行為における経営者の認識を開示する。
  - 従業員、元従業員、監督当局その他関係者から伝えられた事業体に影響を及ぼす、申し立てられたか疑われた非遵守行為および違法行為に関する経営者の認識を開示する。
- 以下に対して適時に伝達を行う。
  - 適切なレベルの経営者に、重大な非遵守行為および違法行為が存在す

©2013 ISACA All Rights Reserved.

重要事項続き

るかもしれないという識別または入手した情報を伝達する。
- ガバナンス責任者に、内部統制において重要な役割にある経営者または従業員が関わる重大な非遵守行為および違法行為を伝達する。

- ガバナンス責任者に、たとえそれが対象範囲外であっても、監査業務中に識別された、非遵守行為および違法行為の防止および発見を意図した内部統制の整備における重大な欠陥について伝達する。
- 状況に応じて、法令等に基づき、また職業的専門家として報告書に関して要求される事項を検討する。
- 重大な誤謬、統制の不備、虚偽表示、または違法行為が、監査業務の継続的実施に影響を及ぼす場合は、監査業務からの撤退を検討する。
- 経営者、ガバナンス責任者、監督当局などに報告された重要な非遵守行為および違法行為について、すべてのコミュニケーション、計画、結果、評価および結論を文書化する。

用語

用語	定義
非遵守行為	確立している管理ポリシーや規制上の要求事項に違反すること。重大な過失あるいは意図的ではない違法行為による、監査対象領域または事業体に関する意図的な虚偽表示や情報の非開示からなる。
重要な虚偽表示	監査結果への影響が無視できない程度大きい、偶発的または意図的な事実に反した記載
職業的専門家としての懐疑心	疑問を持つ精神および監査証拠の批判的な評価を含む態度。出典：米国公認会計士協会（AICPA）AU 230.07

基準とガイドラインへのリンク

種類	表題
基準	1008 規準
基準	1202 計画におけるリスク評価
基準	1205 証拠
ガイドライン	2206 他の専門家の作業の利用
ガイドライン	2207 非遵守行為および違法行為

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。

©2013 ISACA All Rights Reserved.