

# IT内部統制 (実施基準案)

平成19年1月20日

ITコーディネーター

清水 恵子

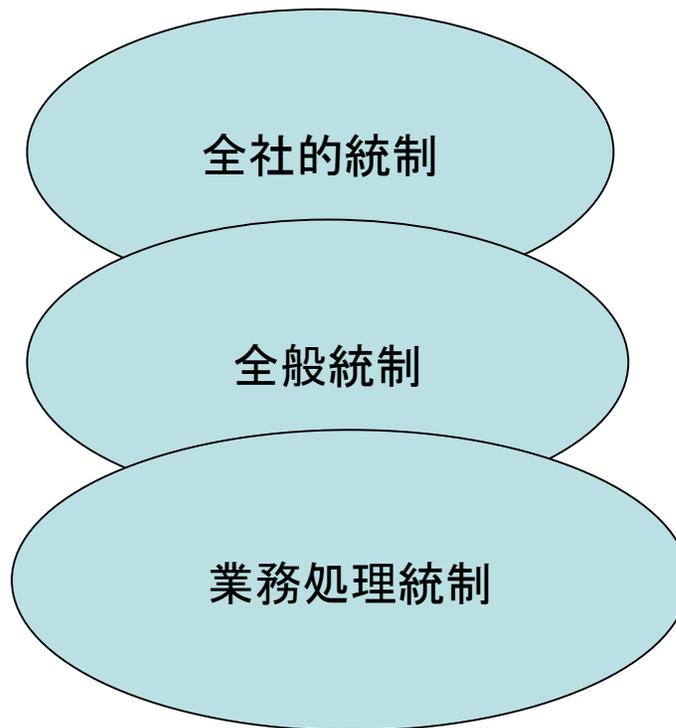
# 実施基準案の公表

- 2006年11月21日金融庁企業会計審議会内部統制部会より、「財務報告に係る内部統制の評価及び監査に関する実施基準（公開草案）」公表
- 実施基準案の構成
  - I.内部統制の基本的枠組み
  - II.財務報告に係る内部統制の評価及び報告
  - III.財務報告に係る内部統制の監査
- 2006年12月20日までコメント募集
- 2007年1月に企業会計審議会総会にて確定・公表予定
- 2008年4月1日以降に開始する事業年度から適用

# 1. 実施基準のIT統制

# ITの統制

- 全社的統制
- 全般統制
- 業務処理統制



# 実施基準 ITの統制

## ◆全社的統制

全社的な内部統制の整備状況を把握し、記録・保存する。

## ◆ITに係る全般統制

業務処理統制が有効に機能する環境を保証するための統制活動

## ◆ITに係る業務処理統制

ITに係る業務処理統制とは、業務を管理するシステムにおいて、承認された業務がすべて正確に処理、記録されることを確保するために業務プロセスに組み込まれたITに係る内部統制である。

# よくある質問

- ITの評価の範囲は？
  - 事業所等の区分とは必ずしも一致しない
- 全般統制は全部対象か？
  - 財務報告との関係を考慮
- 全般統制、業務処理統制の区分システム構成により異なる
- 最終的な評価もゴールは何かポイント

# 最終ゴールは？

- 財務報告の信頼性
- 情報そのものの信頼性
- システムの信頼性は財務情報の信頼性を支える統制が対象

# 情報の信頼性とは何か

- 情報の信頼性は、情報システムが有効に機能しているか否かに大きく依存している
- 情報システムが有効に機能しているということは、企業の経営資源（人、物、金）の状態が、その企業のビジネスプロセスにおいて、適時かつ正確に情報として反映されていることをいう

（日本公認会計士協会IT委員会報告第3号）

# 全社的統制を整備する意味

- 全体として内部統制の仕組が存在する
- 全社的統制が有効である場合は、業務プロセスの評価は簡易になる
  - 例えば、全グループ同じERPパッケージを利用する
  - 同一の統制についてはひとつの母集団
  - 統制が異なると種類毎に評価する

# 業務プロセスにおける内部統制

- リスクの評価は、財務報告の虚偽表示リスク
- 重要なリスクと統制上の要点を識別する
- ウォークスルー(取引の開始、承認、記録、処理、報告を含め、取引の流れを把握する)ことにより、重要な統制を識別する

# 全般統制

- IT全般統制が不備だとIT業務処理統制の有効性が保障されない
  - IT業務処理統制が有効でないとその統制は利用できない場合がある
  - 全般統制は直接には、財務報告の信頼性には影響しない
  - 但し、財務報告に関係の無い全般統制は評価対象ではない

# 全般統制はなぜ財務報告と関係するか：実施基準の例

## ① システム開発又は変更

- ・システムは当初の設計どおりに財務報告が適正に実施されるように実装されているか
- ・不正なプログラム変更が実施されていないか

## ② アクセスの管理対策

- ・職務権限とアクセス権は一致しているか
- ・不正な使用は制限されているか

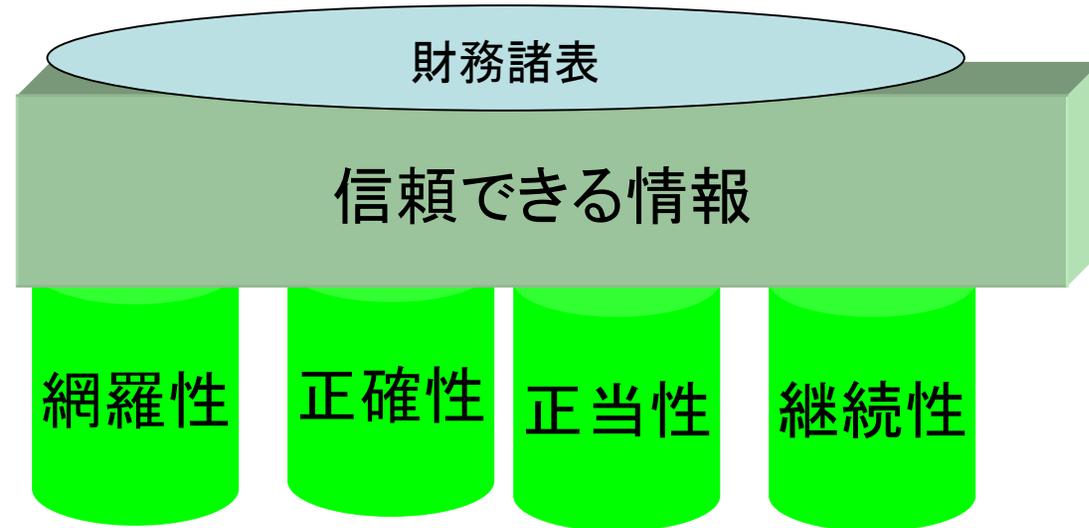
# 適切な財務報告作成のための 要点(アサーション)

- 実在性: 資産及び負債が実際に存在し、取引や会計事象が実際に発生していること
- 網羅性: 計上すべき、資産、負債、取引や会計事象を全て記録していること
- 権利と義務の帰属: 計上されている資産に対する権利及び負債に対する義務が企業に付属していること
- 評価の妥当性: 資産及び負債を適切な価額で評価していること
- 期間配分の適切性: 取引や会計事象を適切な金額で記録し、収益及び費用を適切な期間に配分していること
- 表示の妥当性: 取引や会計事象を適切に表示していること

# ITの統制目標

- 有効性及び効率性：情報が業務に対して効果的、効率的に提供されていること
- 準拠性：情報が関連する法令や会計基準、社内規則等に合致して処理されていること（正当性、完全性、正確性）
- 可用性：情報が必要とされるときに利用可能であること
- 機密性：情報が正当な権限を有するもの意外に利用されないように保護されていること

# コントロールの評価の視点



## ■ ITのコントロール目標 (IT3号)

- 網羅性とは「情報が漏れなくかつ重複することなく記録されていること」
- 正確性とは「情報が正確に記録され、提供されていること」
- 正当性とは「情報が正規の承認手続を経たものであること」
- 維持継続性とは「必要な情報の継続使用が可能なこと」
- この他に準拠性、可用性、機密性の目標が記載されている

# ITに係わる業務処理統制 (実施基準の例示)

- 入力情報の完全性、正確性、正当性等を確保する統制
- 例外処理(エラー)の修正と再処理
- マスターデータの維持管理
- システムの利用に関する認証、操作範囲などのアクセスの管理

# アサーションとIT統制目標 ひとつの例示

ITのコントロール目標	アサーション
網羅性	網羅性、期間帰属
正確性	正確性、評価、分類 期間帰属
正当性	発生、実在性、権利と義務

## 2. 委託業務の管理

# 委託業務の管理

- 委託業務については、委託会社に責任がある
- 重要な業務プロセスについては、委託している場合は、その内部統制の有効性を評価する

# 委託先の内部統制の評価

- サンプルングによる検証
  - 業務結果の検証
  
- 委託会社の評価結果の利用
  - 18号
  - SAS70

監査基準委員会報告書第18号（中間報告）  
委託業務に係る統制リスクの評価  
日本公認会計士協会

- 監査人は会計士か監査法人
- 受託会社とは、委託会社の財務諸表の基礎となる取引の承認、実行、計算、集計、記録等の業務を受託している会社
- 内部統制整備状況報告書
- 内部統制整備及び運用状況報告書

# SAS70

- 米国公認会計士協会監査基準書第70号
- タイプ1：整備状況
- タイプ2：整備状況、一定期間の運用状況
- タイプ2が必要

# 在外子会社

- 在外子会社については
  - 在外子会社等で他国の内部統制制度が適用されている場合の内部統制報告書を利用する

# 米国の動向：SECの経営者による内部 統制評価に関する解釈指針案の概説

(参考資料)

# SECのアクション

・経営者の財務報告に関わる内部統制(ICFR)の年次計画・  
実施を支援する解釈指針案

以下のホームページの「提案された規則」の欄に記載

<http://sec.gov/news/whatsnew/wn122006.shtml>

**MANAGEMENT'S REPORT ON INTERNAL CONTROL  
OVER FINANCIAL REPORTING**

<http://sec.gov/rules/proposed/2006/33-8762.pdf>

# IT全般統制について

- 自動化されたコントロール又はITに依存するコントロールの適切かつ一環した運用はIT全般統制に依存
- IT全般統制の評価範囲は企業の実情により、内部統制評価により異なる
- 財務報告に必要な部分のみが対象
- IT全般統制が有効であれば自動化されたコントロールのほうが効率的である

# 経歴

清水 恵子

大手監査法人で会計監査と会計監査の一貫としてのシステム監査に従事し、繊維、通信、運輸、金融機関等のシステム監査を幅広く経験した。システム導入の評価、情報セキュリティ監査も実施している。平成15年度は電子政府構築計画のガイドライン作成業務に従事、CIO補佐官研修資料作成。現在、EA(業務・システム最適化計画)策定の支援業務を中心に活動し、情報セキュリティ監査、システム監査にも関与している。

公認会計士、システム監査技術者、ITコーディネータ、ISMS主任審査員。

著書「ITリスクと会計情報」(中央青山監査法人編、2003年 税務経理協会)

「新版システム管理基準解説書平成16年度基準確定版」(監修 経済産業省商務情報政策局)システム監査と内部統制の実務(中央青山監査法人編、2005年 税務経理協会)

公職:公認会計士協会 監査対応IT委員会専門委員、内部統制フレームワーク検討委員会委員

(財)日本情報処理開発協会 平成15年度 システム監査基準検討委員会の委員、16年度システム監査基準普及検討委員会およびシステム管理基準WG委員

内閣府 経済財政政策関係業務等に必要なシステムに係るレガシーシステム検討会委員  
経済産業省 情報セキュリティ対策ベンチマークWG委員

平成17年度企業のIT統制に関する調査検討委員会委員 経済産業省