第38回システム監査学会研究大会

「ITガバナンスと内部統制」研究プロジェクト

2024年6月14日

多和田肇

当研究プロジェクトについて

- 当研究PJではこれまで、様々な観点から「ITガバナンスと内部統制」について幅広く研究を行ってきました
- 2023年度からのテーマ（2024年度はメンバーの合議で変更の可能性はあります）
  - 「システム管理基準　追補版（財務報告に係るIT統制ガイダンス）」（2007年、経済産業省）（リンク先：https://www.meti.go.jp/policy/netsecurity/docs/secgov/2007_ZaimuHoukokuNiKakaruITTouseiGuidance.pdf）の見直し観点の検討
- 2024年度例会は月１回を予定（現状ではオンライン開催を予定）

システム管理基準追補版とは

- 掲出されている経済産業省WEBサイト https://www.meti.go.jp/policy/netsecurity/sys-kansa/の説明
- 財務報告に係る内部統制の整備運用に際して、「システム管理基準等」に基づいて構築されている情報システムを活用し、 財務報告に係る内部統制で求められている「IT への対応」を行っている、行うとしている企業において、「システム管理基準等」と「IT への対応」との間の具体的な対応関係を明らかにする必要があります。
- 本ガイダンスは、そのような企業に対して、主要なケースを想定しつつ、IT 統制に関する概念、 経営者評価、導入ガイダンス等を提供しようとするものです。

作成に携わった方々のご紹介（検討委員会）

- 企業の IT 統制に関する調査検討委員会 名簿（肩書は発表当時）
- 【委員長】鳥居 壮行 駿河台大学文化情報学部 教授
- 【委員】
  - 大木 栄二郎 特定非営利活動法人日本セキュリティ監査協会（JASA）
    保証型監査促進プロジェクトリーダー
  - 喜入 博 システム監査学会（JSSA）理事
  - 郡山 信 財団法人金融情報システムセンター（FISC）監査安全部長
  - 後藤 直樹 KDDI 株式会社 技術開発本部セキュリティ技術部
    企画推進グループリーダー

作成に携わった方々（続き）

- 島田 裕次 日本内部監査協会（IIA）
- 清水 恵子 日本公認会計士協会 IT 委員会 監査 IT 対応専門委員会専門委員
- 力 利則 日本電気株式会社 経営監査本部監査部長
- 西尾 秀一 社団法人情報サービス産業協会（JISA）セキュリティ部会副部会長（株式会社 NTT データ）
- 原田 要之助 大阪大学大学院工学研究科 特任教授
- 堀江 正之 日本大学商学部 教授
- 松尾 明 青山学院大学 教授
- 松原 榮一 社団法人日本情報システム・ユーザー協会（JUAS）調査研究部会委員
- 丸山 満彦 情報システムコントロール協会（ISACA）東京支部副会長
- 和貝 享介 特定非営利活動法人日本システム監査人協会（SAAJ）副会長

（五十音順・敬称略）

作成に携わった方々のご紹介（作業部会）

- 企業の IT 統制に関する調査検討委員会作業部会　名簿（肩書は発表当時）
- 【委員長】鳥居 壮行 駿河台大学文化情報学部 教授
- 【委員】
  - 石島 隆 大阪成蹊大学現代経営情報学部 助教授、法政大学大学院 客員教授
  - 加藤 俊也 公認会計士
  - 清水 恵子 公認会計士（日本公認会計士協会 IT 委員会 監査 IT 対応専門委員会専門委員）
  - 田中 太 財団法人金融情報システムセンター（FISC）監査安全部総括主任研究員
  - 千枝 和行 社団法人日本情報システム・ユーザー協会（JUAS）企業情報マネジメント研究会委員
  - 中村 元彦 公認会計士
  - 中山 清美 公認会計士

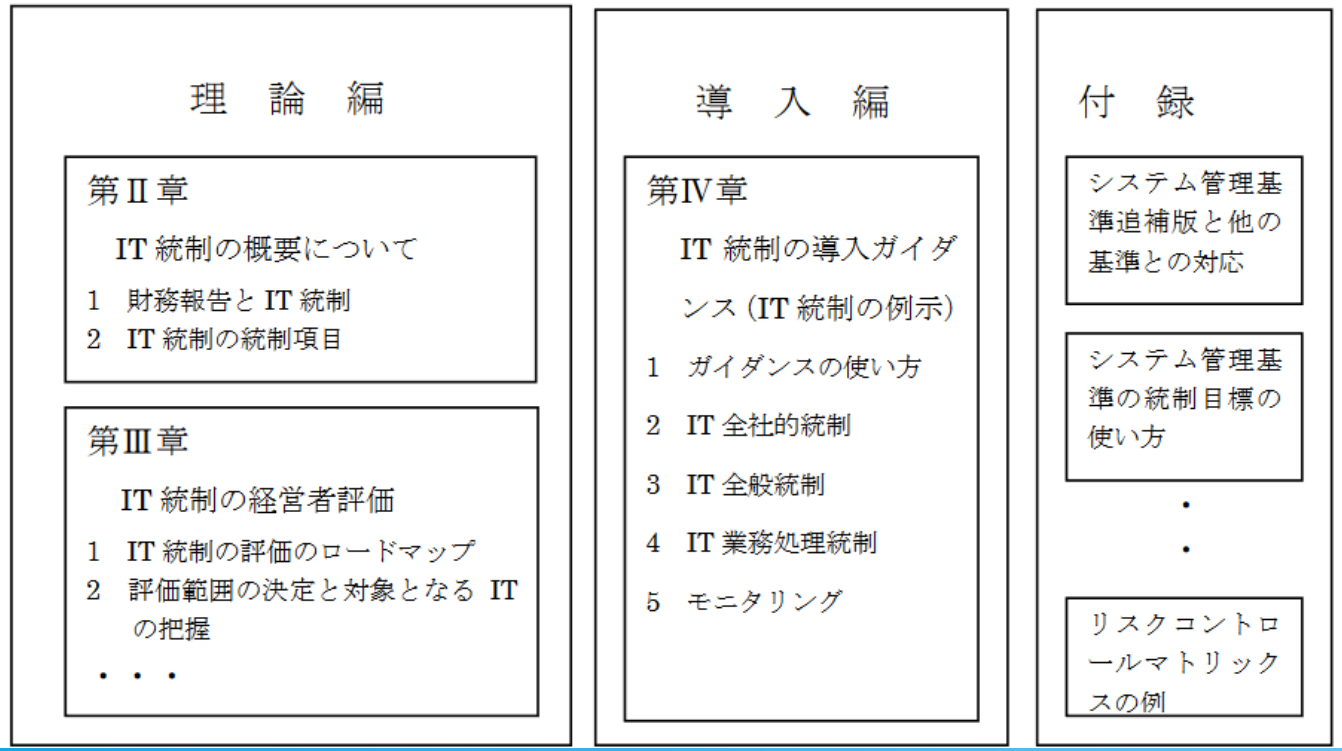
作成に携わった方々（続き）

- 原田 要之助 大阪大学大学院工学研究科 特任教授
- 堀江 正之 日本大学商学部 教授
- 松原 榮一 社団法人日本情報システム・ユーザー協会（JUAS）調査研究部会委員
- 丸山 満彦 情報システムコントロール協会（ISACA）東京支部副会長

（五十音順・敬称略）

構成（第1章から）

本追補版は、「第Ⅱ章　IT 統制の概要について」「第Ⅲ章　IT 統制の経営者評価」「第Ⅳ章　IT 統制の導入ガイダンス（IT 統制の例示）」「付録」から構成されている。



他の基準との関係（付録１から）

IT 統制の代表的な枠組みとしては、付録図表１－１のようなものがある。

付録図表１－１　IT 統制の代表的な枠組み

代表的な枠組み	策定者等	枠組みの範囲
システム管理基準	経済産業省	IT 統制全般
COBIT（第 4 版）	IT ガバナンス協会	
企業改革法遵守のための IT 統制目標（第 2 版）	IT ガバナンス協会	財務報告に係る IT 統制
IT 委員会報告第 3 号	日本公認会計士協会	
情報セキュリティ管理基準	経済産業省	IT のセキュリティ管理
JIS Q 27002	日本工業規格	
ISO/IEC 20000:2005 Information technology - Service management	ISO/IEC	IT の運用管理
ITIL （Information Technology Infrastructure Library）	英国商務局	

他の基準との関係（付録1続き）

なお、これらの枠組みのいずれも財務報告に係る内部統制の評価と監査の制度のための「一般に公正妥当と認められる IT 統制基準」として利用しうるかについての合意が得られているわけではない。例えば、これらの枠組みの中にはこの制度のためには必要のない項目が存在したり、項目が一部の領域に偏っていたりする場合がある。また、海外の枠組みは、欧米の商習慣を前提としており、我が国の内部統制制度では欧米にはない考え方も取り入れられているため、我が国の企業にそのまま適用しづらい面もある。

以下では、「システム管理基準追補版（財務報告に係る IT 統制ガイダンス）」（以下、「追補版」という）と代表的な基準である「企業改革法遵守のための IT 統制目標（第 2 版）」（IT Control Objectives for Sarbanes-Oxley 2nd Edition、September 2006、以下、「IT 統制目標．Ｖ２」という）及び「IT 委員会報告第 3 号」（公認会計士協会 IT 委員会第 3 号「財務諸表監査における情報技術（IT）を利用した情報システムに関する重要な虚偽表示リスクの評価及び評価したリスクに対応する監査人の手続について」、平成 18 年 3 月 17 日改定、以下、IT 3 号という）を対比の表として、付録図表１－２に示す。

（参考）付録1-2イメージ

付録図表１－２　システム管理基準と他の基準との比較表

基準名 / 構成要素	IT３号	IT 統制目標．V2	システム管理基準追補版 （財務報告に係るIT統制ガイダンス）
序章	Ⅰ．本報告の目的	1．経営者向け要約	はじめに
財務報告に係る統制の基礎	Ⅲ．内部統制を含む企業及び企業環境の理解 1.情報の信頼性とIT 2.経営者の主張とITコントロール目標との関係 5.統制環境の理解	2．信頼できる財務報告の基礎 IT 統制に関する指針の必要性 3．企業改革法遵守のための変化に関する人的要素の管理 変化に対するコミットメント 現在の状況に対する評価	Ⅰ．IT 統制の概要について 1.財務報告と IT 統制の関係 (1)金融商品取引法に求められている内部統制と IT 統制の関係 (2)財務報告と IT 統制の関係
IT 統制の概要 （統制の分類）	Ⅱ．IT の概括的理解 Ⅲ．内部統制を含む企業及び企業環境の理解 3.各業務プロセスとITとの	2．信頼できる財務報告の基礎 IT 統制の把握 IT 統制 IT 統制に関する PCAOB の	Ⅰ.2.IT 統制の統制項目 (1)IT 全社的統制 (2)IT 全般統制 (3)IT 業務処理統制

付録２．システム管理基準の統制目標の使い方

１と３は省略

２ システム管理基準の管理項目の整理
企業が財務報告の信頼性に係る IT 統制の整備や評価を行う際に、システム管理基準をより活用しやすくするため、システム管理基準の全管理項目について以下のような整理を行った。表中の左から次のようになっている。
・システム管理基準の管理項目を項番順に示している。
・管理項目ごとの統制種別（IT 全社的統制、IT 全般統制、IT 業務処理統制）を、それぞれ、全社、全般、業務、－（該当なし）と例示している
・管理項目ごとに、目指している統制目標を例示している
・管理項目ごとに、財務情報に係るリスクがより大きいものをコントロール（C）、相対的に小さいものをサブコントロール（S）として分類し、例示している。また、財務報告に係る内部統制に直接かかわらないと考えられるものは、空白としている。
・管理項目の主旨（システム管理基準解説書の主旨より要約）を例示している

（参考）付録2-1イメージ

付録2－1　　システム管理基準の管理項目と統制目標の対応（例）

項番	システム管理基準の管理項目	統制種別	統制目標（例）	ガイダンス項番	C/S種別	システム管理基準の趣旨
I	情報戦略					
1	全体最適化					
1.1	全体最適化の方針・目標	全社				
(1)	ITガバナンスの方針を明確にすること。	全社	ITガバナンスの方針（計画）を策定する	2-(1)-①	C	ITガバナンスの確立に際し、その方針を明確にしておく必要がある。
(2)	情報化投資及び情報化構想の決定における原則を定めること。	全社	経営戦略にあわせた情報化計画を定める	2-(1)-①	C	首尾一貫した全体最適化計画を策定するため、情報化投資及び情報化構想の決定における原則を定めておく必要がある。
(3)	情報システム全体の最適化目標を経営戦略に基づいて設定すること。	全社	情報システムの最適化計画を経営戦略と整合させる		S	経営目的を実現する情報システムを企画するため、最適化計画の目標は、経営戦略との整合性を考慮して策定する必要がある。
(4)	組織体全体の情報システムのあるべき姿を明確にすること。	全社	全体最適化計画を策定する	2-(1)-①	C	組織体全体の情報システムは、個別の情報システムが有機的に関連し、整合性が相互に保たれて効率的かつ効果的に目的を達成するものであるため、全体最適化計画は、情報システムのあるべき姿を明確にする必
(5)	システム化によって生ずる組織及び業務の変更の方針を明確にすること。	全社	全体最適化計画は、システム化する組織や業務の変更について示す	2-(3)-①	C	全体最適化計画では、情報システムの（再）構築と同期して行われる組織及び業務の新設、改変及び廃止の方針を明確にする必要がある。
(6)	情報セキュリティ基本方針を明確にすること。	全社／全般	全体最適化計画を、情報セキュリティ基本方針と整合させる	2-(1)-⑤ 2-(3)-① 3-(3)-①-イ	C	不正防止、機密保護、プライバシー保護等は、健全な経営活動推進の基盤であるため、情報セキュリティ対策の方針を全体最適化計画で明確にする必要がある。

付録６．リスクコントロールマトリックスの例

１ リスクコン トロールマ トリックス の項目
企 業 が リ ス ク コ ン ト ロ ー ル マ ト リ ッ ク ス を 利 用 す る 場 合 、 IT 業 務 処 理 統 制 、 IT
全社的統制、IT 全般統制の項目ごとに評価できるように表が掲載されている。ただし、この表は、リスク、統制目標、実際の統制の状況、整備･運用の種別、統制が予防・発見の種別、統制が自動・手動の種別、アサーション、統制の実施される頻度、統制の評価手続、評価及び検出事項、関連する監査調書、評価結果などを例示している。この例示は、あくまでもサンプルであり、企業は、これをベースに自社でカスタマイズして利用されたい。

１の後半と２は省略

（参考）付録6イメージ

付録6-2

IT全般統制評価記述書

会社名	
決算期	
事業拠点	
対象システム	販売システム

整備状況：文書 / プロセス / システム実装

作成者・作成日	◇◇◇◇ 2007/1/23
質問への回答者（実施部署）	

リスク	統制目標 / 留意事項	No.	統制の状況	整備・運用	予防・発見	手作業・自動化	文書	プロセス	システム実装	頻度	統制評価手続	評価並びに検出事項（検出事項がある場合、その影響）	調書番号	評価結果
財務情報に開発に係る誤謬を重大な虚偽表示に繋がることができない	開発		システムを開発する際に意図的な不正プログラムが埋め込まれていないか、また、処理に誤りがないか	整備	予防	手作業	○	○	NA	四半期	対象とするシステムの開発は標準化された手順、文書で実施されていることを確かめた	なし	記載省略	低
			システムの開発プロセスにおいて、意図的な不正や、処理に誤謬がないか	運用	予防	手作業	○	○	NA	四半期	開発の仕様書、基本設計書（概念設計書）等で財務情報の信頼性確保の統制機能が織り込まれていることを確かめた	なし	記載省略	低
			以下省略											
保守	保守		プログラムが改ざんされたり、承認なく変更されていないか	整備・運用	発見	手作業	○	○	NA	月週	変更管理手続の規定があることを確かめた。変更管理規定通りに変更管理を実施していることを25件テストした	25件のうち1件、承認漏れがあったが、責任者の押印漏れであり、実際には、承認されているとの説明を受けた。25件の追加テストの結果、押印漏れはな	記載省略	低

全社的統制のイメージは省略

付録6-3

IT業務処理統制評価記述書

会社名	○○株式会社
決算期	平成○○年3月
場所	受注センター
取引サイクル	販売サイクル
ファンクション	受注
関連する勘定科目	売上、売掛金

要件：網羅性 / 実在性 / 期間配分 / 権利と義務 / 評価 / 表示

作成者・作成日	◇◇◇◇ 2006/12/23
確認者・確認日	□□□□ 2007/1/24

リスク	統制目標 / 留意事項	No.	主要な統制活動	自動化手作業	頻度	網羅性	実在性	期間配分	権利と義務	評価	表示	整備・運用	統制評価手続	評価並びに検出事項（検出事項がある場合、その影響）	調書番号	評価結果
財務情報に漏れや重複が発生する	網羅性		全ての受注は漏れなく重複なく記録されているか													
		1	ＥＤＩによる受注はＪＣＡ手順によって制御され異常な伝送があればシステム担当者にメールが送信される	自動化	四半期	○	NA	○	NA	NA	NA	整備・運用	特定の月を選び、システム運用報告をレビューしＪＣＡ手順による異常終了が担当者に報告され、フォローされていることを確かめる	なし	記載省略	低
		2	ＦＡＸ受注はコールセンタで受信後に連番を記入し、一人が入力した後で、ブルーフリストを出力し、他の一人が内容をＦＡＸと照合する	自動化・手作業	日	○	NA	NA	NA	NA	NA	運用	特定の月の２５件を選び、ブルーフリストが照合されていることを確かめる	なし	記載省略	低
		3	在庫引当された受注のみが出荷指図ファイルに登録される。未引当の受注残は、受注残ファイルに記録され営業担当者がフォローして消し込んでいる	自動化・手作業	日	○	○	NA	NA	×	NA	整備・運用	受注残ファイルが営業担当者により、消し込まれていることを確かめる	なし	記載省略	低
財務情報が正確に記録されな	正確性		受注の登録に誤りがないか													
		4	ＥＤＩで受信した受注データは得意先マスタ、商品マスタと存在性のチェックをし、エラーについてはエラーファイルが作成され、エラーデータについては、得意先に返送し、再送を依頼する。エラーファイルは訂正データが再送されるまで保存される	自動化	日	NA	○	NA	○	○	NA	整備・運用	特定の月のエラーファイルの処理状況を２５件確かめる	なし	記載省略	低
		5	2と同じ。ＦＡＸ受注はコールセンターで受信後に連番を記入し、一人が入力した後で、ブルーフリストを出力し、他の一人が内容をＦＡＸと照合する	自動化・手作業	日	NA	○	NA	○	○	NA	整備・運用	2と同じ。特定の月の２５件を選び、ブルーフリストが照合されていることを確かめる	なし	記載省略	低
		6	受注日付は機械日付で登録される	自動化	日	NA	○	○	NA	NA	NA	整備・運用	売上日付の設定を確かめ、売上データの日付が機械日付であることを確かめる	なし	記載省略	低
		7	得意先コードにより、得意先マスタから得意先名がロードされる	自動化	日	NA	○	NA	○	○	NA	整備・運用	得意先コードにより得意先名が登録されることを画面で確かめる	なし	記載省略	低

検討課題として考えられる項目

- 内部統制実施基準の改訂に合わせた修正等
- システム管理基準の改訂に合わせた記載内容の修正
- その他の基準類（COBIT for SOXなど）の改訂に合わせた修正
- その他

検討課題として考えられる項目（続き）

- 内部統制実施基準の改訂に合わせた修正等
  - サイバー攻撃への対応
  - 業務委託に係る統制の見直し
  - インターバル評価等IT統制評価の見直し

検討課題として考えられる項目（続き）

以下の3つの基準も内部統制基準の2023年度改訂の観点から、記載を見直し、追補版への反映を行う

- システム管理基準の改訂に合わせた記載内容の修正
→ガイドラインも含めて検討
- 「内部統制報告制度に関する事例集～中堅・中小上場企業等における効率的な内部統制報告実務に向けて～」（金融庁規格市場局,2011年（初版）、2023年8月改訂）リンク先https://www.fsa.go.jp/news/r5/sonota/20230831-2/04.pdf
- その他の基準類（COBIT for SOXなど）の改訂による影響
→例えばISACAではIT Control Objectives for Sarbanes-Oxley, 4th Edition(2022)(COBIT 2019をベースにしている）が最新版

（参考）内部統制報告制度に関する事例集IT関係イメージ

（IT に係る全般統制に関するチェック・リスト例）

質問項目			はい：○ いいえ：× 該当なし：N/A 変更なし：ー	補足事項
分類	No	内容		
情報セキュリティの方針/ユーザの認識	G1	プログラム及びデータへのアクセスに対する方針を定め、関係者（外部委託先を含む）に周知しているか		
物理的アクセス	G2	情報処理施設への物理的アクセスを必要な要員のみに制限するための対策を講じているか		
アクセス権限の設定	G3	業務分掌と合致するアクセス権限のみをユーザに付与するための対策を講じているか		
アクセス管理	G4	ユーザ ID 及びアクセス権限の付与申請、承認、発行、一時停止、削除を適切に行うための対策を講じているか		

（IT に係る全般統制に関するチェック・リスト例）

質問項目			はい：○ いいえ：× 該当なし：N/A 変更なし：ー	補足事項
分類	No	内容		
情報セキュリティの方針/ユーザの認識	G1	プログラム及びデータへのアクセスに対する方針を定め、関係者（外部委託先を含む）に周知しているか		
物理的アクセス	G2	情報処理施設への物理的アクセスを必要な要員のみに制限するための対策を講じているか		
アクセス権限の設定	G3	業務分掌と合致するアクセス権限のみをユーザに付与するための対策を講じているか		
アクセス管理	G4	ユーザ ID 及びアクセス権限の付与申請、承認、発行、一時停止、削除を適切に行うための対策を講じているか		

検討課題として考えられる項目（続き）

2023年度は前項のような項目出しの段階ですので、今後実際に追補版の付録２－１（システム管理基準の管理項目と統制目標の対応（例）の内容の検討をすすめて行きたいと考えています。

現在もこのようなガイダンスの必要性はあることを想定して、この追補版を今後も使い続けられるよう、次回の研究大会で報告したいと考えています！

参加を希望される方は是非応募してください！！