「IT内部統制のための統制項目表」の活用方法

～「IT内部統制のための統制項目表」の概要と活用について ～

2007年4月20日

ソリューションサービス事業委員会
IT内部統制専門委員会

(株)日立製作所
米井　達哉

JEITA

目　次

1．作成に至る背景
2．「IT内部統制の為の統制項目表」の作成目的
3．作成のための要件
4．項目の説明
5．想定される活用方法例
6．IT内部統制項目表（サンプル）

＜ご参考＞
・利用ITツール（サンプル）
・規程類等（サンプル）

1 作成に至る背景

- 日本版SOX法の一つの特色とし、内部統制の基本的要素の一つに、「IT（情報技術）への対応」が切り出されている。

- ITを預かるIT部門や、ITに関わる業務部門にとって、自らが提供、または利用するITサービスの改善、品質向上は、ますます重要な課題となる。

- しかし、一方で、これら企業のITに関わる部門が参考にできるような、ITサービスの統制項目のリファレンスとなる情報は、現時点では十分に整備されているとは言いがたい。

2 「IT内部統制の為の統制項目表」(*)の作成目的

(*) 以下、IT内部統制項目表と略す

目的

- 企業に向けたIT内部統制におけるリファレンスの提示。
  (「アプリケーションソフトウェアの調達と保守」、「変更管理」、
  「システムセキュリティの保証」、「データ管理」の4プロセスを対象)

対象

- ITサービスの改善、品質向上を目指すIT部門
- ITに関わる業務部門

3 作成のための要件

(1) ITプロセスに応じた統制項目が、グローバルスタンダードと整合性を保ち体系化されていること

- 整理軸として、SLA／SLM専門委員会の「ITサービスリスク／SLAマトリクス」の軸（ITプロセスの分類方法や管理項目・発生リスク）を活用。
- 「ITサービスリスク／SLAマトリクス」は、情報システムコントロール財団（ISACA）が策定したCOBIT®Ver. 3.0（グローバルスタンダード）と、経済産業省が策定したシステム管理基準（日本スタンダード）を組み合わせた軸でITサービスリスクを整理。
- これにより、「IT内部統制項目表」を各スタンダードと対応付け、参照する方の理解し易さに配慮。

3 作成のための要件

(2) 統制方法などが、ITサービスの改善、品質向上活動の参考にできるレベルで提示されていること

- 統制方法の記述粒度は、企業のIT部門や、関連する業務部門における、日頃のITサービスの改善、品質向上活動に適用し易い表現に。
- 統制活動を効率化するために利用可能なITツールを例示。
- 統制に際して作成・参照すべき規定やマニュアルを列挙。
- さらに、利用ITツールの用語表と、規程類の一覧表も作成。

3 作成のための要件

(3)「実施基準(*)」に即した内容であること

- IT内部統制項目表を活用度の高いものとするため、実施基準にて示された評価視点との整合性を確保。
- 「開発・保守」、「運用・管理」、「システムの安全性の確保」、「外部委託の契約管理」との対応付けを明確化。

(*) 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
(金融庁企業会計審議会内部統制部会)

3 作成のための要件

(4) 企業の関心の高いIT内部統制活動に重点がおかれていること

- ITガバナンス協会 (ITGI) では、COBIT®のSOX法に関連する部分をCOBIT for SOXとして体系化
  (全社レベルの15プロセスと、業務レベルの12プロセス)
- 業務レベルの12プロセスの中から、実施基準、及び今回のアンケート調査結果などを鑑み、より重要度が高いと思われる以下の4プロセスを対象。
  - 「アプリケーションソフトウェアの調達と保守」
  - 「変更管理」
  - 「システムセキュリティの保証」
  - 「データ管理」

JEITA

4 項目の説明

#	項目名		説　明
1	システム管理基準 項目番号		「システム管理基準」に記載されている項目番号。 わかりやすくするため、項目番号の下に内容を追記
2	管理項目		「システム管理基準」の管理項目の内容
3	発生リスク		管理項目に記述された活動がなされない場合に発生が予想されるリスクの例
4	統制活動	統制項目	IT内部統制における統制項目の例
5		統制のタイプ	統制活動にITツールが適用可能な場合は「自動」に○。人手を介する場合は「手動」に○
6		利用ITツール	統制活動に利用することが出来るITツールの名称
7		規定類等	統制のための基準、ルールなどを記述するドキュメント例
8		実施基準対応	実施基準との対応付け

5 想定される活用方法例

(1) IT部門における活用

- 社内のITサービスの改善、品質向上活動に向け、改善したいITプロセス毎の統制項目洗い出しの参考に。
- 統制を実現するための業務プロセスや基準、ルール作りの参考に。
- ITツール利用による効率化のヒントに

(2) 業務部門における活用

- 業務部門の役割、実施項目の明確化に。
  (システム要件の明確化、設計内容や使い勝手のレビューや承認など)

IT内部統制項目表（サンプル）

(1) アプリケーションソフトウェアの調達と保守

統制項目の洗い出しの参考

利用できるITツールは何か？

統制のために作成が有効なドキュメントは何か？

業務（ユーザ）部門の役割を例示

			統制活動									
				統制のタイプ								
		生リスク		自動	手動	IT		保守	用	安全性	契約管理	外部委託
II-03-0-(01)（企画）調達	調達の要求事項は、開発計画及び、ユーザニーズに基づき作成し、ユー	構築する情報システムの機能、性能、品質等の要求が、計画とおりに達成	調達要求事項は開発計画やユーザーニーズを基に作成する。		○		・システム開発規定 ・システム計画書 ・要求定義書 ・保守/運用規定	○	○			
			調達要求事項は、ユーザー部門責任者及び、システム部門責任者（企画/開発／保守運用）のレビュ・承認を受ける。	○	○	・文書管理 ・ワークフロー ・ID管理		○	○			
			調達要求事項レビュ実施記録を作成し、保存する。	○	○	・文書管理 ・ワークフロー ・ID管理 ・ログ管理		○	○			

6 IT内部統制項目表（サンプル）

(2) 変更管理

システム管理基準項目番号	管理項目	発生リスク	統制活動							
			統制項目	統制のタイプ		利用ITツール	規定類等	実施基準 IT全般統制との対応			
				自動	手動			開発保守	運用	安全性確保	外部委託契約管理
V-04-0-(03) V保守ー04 保守の確認	変更したプログラムのテストはユーザが参画し、ユーザマニュアルに基いて実施すること。	情報システムが変更依頼等の要求を満たせない。	業務に精通したユーザが参加してテストを行う テストはユーザマニュアルに基づいて実施する		○		・ユーザテスト計画書	○			
VI-06-6.2-(2) 共通変更管理（実施）	変更管理案件を実施した場合に、関連する情報システムの環境も同時に変更すること。	変更が効率的に実施できないだけでなく、対象外のシステムでトラブルが発生する。	変更管理案件実施による他システムへの影響も考慮して変更計画書を作成する。 変更計画書に基づいて変更管理案件を実施する	○	○	構成管理	・変更管理規定 ・プログラム変更計画書	○	○		

6 IT内部統制項目表（サンプル）

(3) システムセキュリティの保証

システム管理基準項目番号	管理項目	発生リスク	統制活動							
			統制項目	統制のタイプ		利用ITツール	規定類等	実施基準 IT全般統制との対応			
				自動	手動			開発保守	運用	安全性確保	外部委託契約管理
IV-06-0-(02) 運用（ソフトウェア管理）	ソフトウェアへのアクセスコントロール及びモニタリングは、有効に機能すること。	ソフトウエアの不正利用防止が図れない。	ソフトウェアへのアクセスに関するリスク分析（不正利用に関するリスク評価）を実施する。		○		・システム設計要綱		○	○	
			下記のような手段によりソフトウェアを保護する。 ・暗号化、パスワード等のデータ保護 ・データ格納容器の施錠、封印等 ・受渡し場所の特定　等	○	○	・暗号化 ・ID管理	・セキュリティ管理規定（セキュリティ管理ツールログ記録）		○	○	
			重要なソフトウェアの利用を制限されている。	○	○	・ID管理			○	○	
			ソフトウェアに関するセキュリティイベントをモニタする仕組みを設ける。	○	○	・ウィルス対策 ・ログ管理			○	○	
			運用に関する役割と責任が明確に定義されている。		○		・職務分掌規定 ・セキュリティ管理規程		○	○	

6 IT内部統制項目表（サンプル）

(4) データ管理

システム管理基準項目番号	管理項目	発生リスク	統制活動							
			統制項目	統制のタイプ		利用ITツール	規定類等	実施基準 IT全般統制との対応			
				自動	手動			開発保守	運用	安全性確保	外部委託契約管理
IV-03-0-(01)運用（入力管理）	入力管理ルールを定め、遵守すること。	入力データの作成、授受、検証、入力実施、入力後の確認、保管等が正しく行われない。	入力データの作成、授受、検証、入力実施、入力後の確認、保管等の入力管理ルールを明文化する。		○		・情報管理規定		○		
			入力管理ルールは情報システム部門の責任者（開発・保守・運用）が承認する。		○				○		
			必要に応じて入力の記録を残し、入力管理ルールが遵守されていることを検証する。	○	○	・文書管理 ・ワークフロー ・ID管理 ・ログ管理			○		

ご参考

利用ITツール（サンプル）

名称	ヨミ	意味
文書管理	ブンショカンリ	文書（情報、データ、ドキュメント、ファイル等）に対する更新履歴、承認、最新版の管理、公開（配布）を管理し、体系的に保管するツール。
ワークフロー	ワークフロー	文書作成、承認、回付、文書保管等の業務の流れをサポートするツール。
ID管理	アイディーカンリ	利用者を特定する為の番号、パスワードおよび権限等の発行・変更・削除等の管理を実行するためのツール。
ログ管理	ログカンリ	情報（データ）、ソフトウェア、ネットワーク等に対するアクセス及び、システムの運用の履歴を収集・集計・参照・分析するためのツール。
コーディングチェック	コーディングチェック	ソースコードの静的な正しさをチェックするツール。
開発テスト	カイハツテスト	開発したプログラムのテストを支援するツール
プロジェクト管理	プロジェクトカンリ	プロジェクトの管理運用（進捗、リソース、時間等）支援を行うツール
バックアップ	バックアップ	ソフトウェア、データを自動的にバックアップを保存し、業務継続性をサポートするツール。
暗号化	アンゴウカ	情報の盗難・悪用を防止するために、データの暗号化（並べ替え）を行うツール。

ご参考

規程類等（サンプル）

名称	ヨミ	意味
システム開発規程	システムカイハツキテイ	システムを開発するにあたり、その開発プロセス（要件定義、システム設計、プログラム設計、単体テスト、結合テスト、総合テスト、保守/運用、システム移行など）や手順について組織として守るべき方針やステップを規定した文書 。
要求定義書	ヨウキュウテイギショ	システム化要件を記述したドキュメント。主にシステム化目標、システム化対象範囲、費用対効果、適用業務要件、処理要件、品質要件や他システム要件、ハードウェア／ソフトウェア要件、システム設計の全体条件などが記述した文書
システム計画書	システムケイカクショ	要件定義書に基づいてシステム全体の概要を記述した文書。システム設計書に記載される内容を大枠で記述している。実際には、システム設計書で代用される事もある
プロジェクト計画書	プロジェクトケイカクショ	プロジェクトにおけるシステム化の目標／対象業務とその機能、システム構成の方針、開発範囲と開発スケジュールの大枠、開発の推進体制や開発方法／管理方法など、当該プロジェクトの基本方針や全体構想および開発方針といった基本的な計画を記述した文書
システム設計要綱	システムセッケイヨウコウ	要求定義書に基づいて、システムの構造を決定し、各サブシステムとの人間業務処理とのインタフェースを記述する手法を定義した文書。システム設計を行う上で、考慮すべき事項（フェールセーフ設計、二重化など）の定義を含む。
システム設計書	システムセッケイショ	要求定義書に基づいて、システムの構造を決定し、各サブシステムとの人間業務処理とのインタフェースを詳細を記述した文書。システム移行･運用方針を示し、結合テスト、総合テスト、システム移行の計画を記述した文書を含む
プログラム設計書	プログラムセッケイショ	システム設計書に基づき、各サブシステムのコンピュータの処理のソフトウェア仕様（プログラム構成、プログラムの基本仕様、実行形態など）を記述した文書

ご清聴ありがとうございました。

今回ご紹介したIT内部統制専門委員会の報告書（有償）は、
下記問合せ先にてお申し込み頂けます。

社団法人 電子情報技術産業協会（ＪＥＩＴＡ）
インダストリ・システム部
〒101-0062　東京都千代田区神田駿河台３丁目１１番地
三井海上別館ビル
電話：03-3518-6426　　FAX：03-3295-8724
Ｅメール：m-ichijo@jeita.or.jp
ＪＥＩＴＡホームページ：http://www.jeita.or.jp/japanese/index.htm