内部統制の中のIT統制

～内部監査の実務～

08年4月16日　二瓶　豊

コンテンツ

- 内部統制の目的
- 内部統制の構成要素
- IT統制の構成要素
- IT統制の内容
- ITコンプライアンスの為の手順
- 文書化例～ITGC（RCM)
- 文書化のポイント～ITAC（RCM)

内部統制の目的

～財務報告に係る内部統制の評価及び監査の基準（企業会計審議会）

①業務の有効性及び効率性

業務の達成度及び資源の合理的な利用度を測定・評価し、適切な対応を図る体制を設けることにより、組織が設定した業務の有効性及び効率性に係る目標の達成を支援する

②財務報告の信頼性

財務報告の重要な事項に虚偽記載が生じることのないよう、必要な体制を整備し、運用することにより、組織の財務報告に係る信頼性を支援する

③事業活動にかかわる法令等の遵守

法令等を遵守して事業活動を営むための体制を整備し、運用することであり、これらを通じ、組織の存続及び発展が図られる

④資産の保全

資産の取得、使用及び処分が正当な手続き及び承認の下に行われる

内部統制の構成要素

～財務報告に係る内部統制の評価及び監査の基準（企業会計審議会）

①統制環境

組織の気風を決定し、組織内のすべての者の統制に対する意識に影響を与えるとともに、他の構成要素の基礎をなし、他の構成要素に影響を及ぼす基盤となる

②リスクの評価と対応

組織目標の達成に影響を与える事象について、組織目標の達成を阻害する要因をリスクとして識別、分析及び評価するプロセス

③統制活動

経営者の命令及び指示が適切に実行されることを確保するために定める方針及び手続

④情報と伝達

必要な情報が識別、把握及び処理され、組織内外及び関係者相互に正しく伝えられることを確保すること

⑤モニタリング

内部統制が有効に機能していることを継続的に評価するプロセス

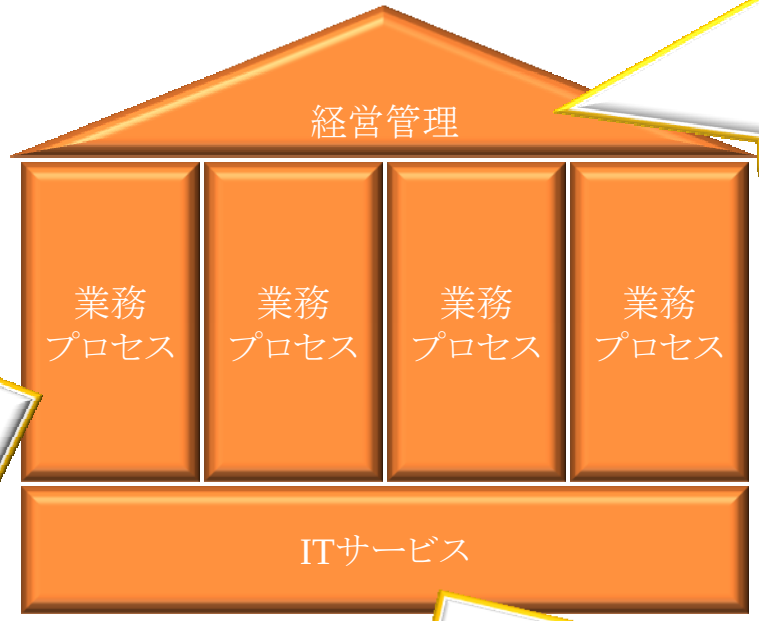
⑥ITへの対応

組織目標を達成するために予め適切な方針及び手続を定め、それを踏まえて、業務の実施において組織の内外のITに対し適切に対応すること

IT統制の構成要素

【経営管理】
経営者は、経営目標を設定し、方針を確立して、企業の資源配分と管理に関する決定を行う。

【全社統制（ITCLC）】
組織の気風と企業文化を決定する。全社レベルのIT統制は会社全体の統制環境の一部である。



【業務プロセス】
価値を創造し、実現する仕組み。入力、処理、出力といった機能がある。

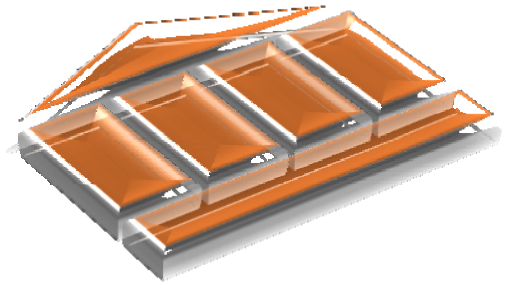
【業務処理統制（ITAC）】
財務の統制目標を直接サポートする業務プロセスのアプリケーション内に組み込まれる統制。

【ITサービス】
業務の基礎を成し、業務プロセスまたは事業拠点ごとに分離されるのではなく、全組織を通じて提供される。

【全般統制（ITGC）】
信頼できる運用環境を提供し、業務処理統制の有効な運用をサポートする。

ITCLC : IT Company Level Control
ITGC : IT General Control
ITAC : IT Application Control

IT統制の内容



IT統制環境

統制環境に含まれるものとして、ITの戦略計画、ITのリスク管理プロセス、遵守および規制に対する管理、ITの方針、手続き、及び基準がある（以上がIT統制プロセス）。また、ITを業務要件に準拠させるために必要なモニタリングと報告が含まれる。

コンピュータ・オペレーション

オペレーションとは、ITインフラの定義、調達、導入、構成、統合および保守管理に係る統制である。具体的には、サービス・レベルの管理、サードパーティサービス業者の管理、システムの利用可能性、顧客管理、構成およびシステム管理、問題とインシデント管理、オペレーション管理スケジュールの作成、施設管理など、毎日の情報サービスの提供に関係するものである。

プログラムとデータへのアクセス

安全なパスワードやインターネットのファイアウォール、データの暗号化、暗号キーなどの適切なアクセスコントロールである。また、ユーザアカウントやアクセス権の統制は、適切な職務分掌を促す役割もある。

プログラム開発とプログラム変更

新しいアプリケーションソフトウェアの調達・導入と既存のアプリケーションの保守管理である。このプロセスは、システムの拡張、広範なテスト、ユーザの再研修、手続きの変更といった手続きが必要となり、他のIT統制と統合して進めていく必要がある。

ITコンプライアンスの為の手順

IT統制の評価計画と対象範囲の決定

〇プロジェクト全体の文書化をレビューし、アプリケーション統制を把握する
〇対象範囲のアプリケーションを把握する
〇対象範囲のインフラとデータベースを把握する

ITリスクの評価

〇財務諸表の誤りまたは不正をもたらすITシステムの可能性と影響を評価する

統制の文書化

〇アプリケーション統制の文書化
〇IT全般統制の文書化

統制の設計上・運用上の有効性評価

〇すべての関連統制が文書化されているかを判断する
〇運用上の有効性を確認するための統制をテストする

不備の優先順位付けと改善

〇財務諸表の誤りまたは不正をもたらす不備の影響と可能性を評価することにより、不備を優先順位付けする
〇補完統制が存在し、依拠することが可能かを検討する

持続可能性の構築

〇信頼性を改善し、テスト作業を軽減するため自動化されたコントロールを検討する
〇重複する統制を除外するため、合理化を図る

文書化例～ITGC（RCM）

ID	コントロール目標		想定されるリスク	コントロール						テスト方法
				コントロール例	コントロールタイプ		コントロールシステム対応		コントロール頻度	コントロール確認文書	
					防止的	発見的	手作業	自動化			
AC1－1	セキュリティポリシーの承認と周知	企業情報の機密性、完全性、可用性を確保するための網羅的な情報セキュリティポリシーが文書化され、責任者によって周知されていること。情報セキュリティポリシーは必要に応じて更新され、更新内容は責任者によって承認されていること。	情報セキュリティポリシーが定められていない場合、日常業務におけるセキュリティ遵守が不明瞭になり、情報資産が適切に保護されない、あるいはセキュリティ対策が実施されない恐れがある。	情報セキュリティポリシーが明確に定義され、従業員に周知されている。 情報セキュリティポリシーは必要に応じて更新され、更新内容は責任者によって承認されている。 定期的に情報セキュリティ講座を開催し、従業員の情報セキュリティ遵守を強化している。	●		●		年次	情報セキュリティポリシー	セキュリティポリシーを確認する従業員への周知回数を確認する。セキュリティポリシーの変更の際の承認履歴を確認する。Eラーニングの受講実績を確認する。
AC1－2	ユーザIDの申請と管理	ユーザIDの申請と管理に関する手続きなどが明確に定義されていること。 退職者や異動者を考慮し、定期的なユーザIDの棚卸とレビューによって使用されていないユーザIDが適時削除されていること。	ユーザIDの管理が曖昧な場合、不正なユーザIDが作成される、あるいはユーザIDが不正に使用され、重要なデータが改竄あるいは破壊される恐れがある。	ユーザIDの申請と管理手順が明確に定義され、手順にそって全てのユーザID管理が実施されている。ユーザIDを一元管理するユーザID管理ツールが導入されており、人事システムと連携したユーザID管理が実施されている。	●		●	●	随時	ICカード認証システム運用について 業務連絡表	ユーザ登録手順が定義されている文書を確認する。 申請書が適切な承認者により承認されていることを確認する。 承認された申請書の数と、登録・更新された数を比較する。 連携（インターフェース）のログを確認する。 退職者のIDが削除されていることを確認する。
AC1－3	パスワード設定方針の定義と周知	パスワードの有効文字・桁数、有効期限、再発行手順、自己管理方針等が明確に定められ、従業員へ周知されていること。	パスワードの管理が曖昧な場合、パスワードが奪取・盗用される可能性があり、不正アクセスによって重要なデータが改竄あるいは破壊される恐れがある。	パスワードの有効文字・桁数・有効期限、再発行手順、自己管理方針等をユーザID管理手順書に定義し、従業員に周知している。 パスワードを一元管理するユーザID管理ツールが導入され、そのツールを活用したパスワード管理が実施されている。	●		●	●	随時	ICカード使用操作手順書 ICカード認証システム運用について	パスワード設定ルールを確認する。パスワード再発行手順書を確認する。パスワードルール周知履歴を確認する。 パスワードが定期的に変更されているかどうかを確認する。パスワードがデフォルトのままになっていないかどうかを確認する。

文書化のポイント～ITAC（RCM）

	レビューポイント	内容
1	5W1Hの記述	コントロールの内容について、5W1H（誰が、いつ、何処で、何を、どのように、なんのために）を意識した説明が記述されているか。
2	アサーションとの関連	ITACにおいてはアサーションを意識した記述がなされているか。 例）●●の網羅性、正確性を担保する目的で・・・
3	トリガーの記述	処理の発生するトリガーが記述に含まれているか。 例）●●を受領することにより、■■をする
4	コントロール対象の記述	「照合」、「査閲」、「承認」などのサブステップでは、照合（査閲、承認）対象が記述に含まれているか。 例）●●と■■を照合する
5	コントロール結果の記述	「照合」、「査閲」、「承認」などのサブステップでは、照合（査閲、承認）結果の証跡が記述に含まれているか。 例）●●を照合し、■■に押印する
6	確認文書の記述	方針、規程、マニュアル等のルール、判断基準を参照する場合は、それらの正式名称を記述しているか。業務上証憑類、システム帳票を使用する場合は、それらの正式名称を記述しているか。
7	システム名称の記述	ITACにおいてシステムにより業務が処理される場合、システムの正式名称が記述に含まれているか。入力画面などは特定された記述になっているか。
8	名称の統一	書類名、部署名、システム名の記述は業務記述書、フローチャート、RCMにおいて統一されているか。
9	記述の整合性	業務記述書の記述欄とRCMのコントロール欄との記述の整合性が確保されているか。