安全なPC環境維持と情報管理が「内部統制」につながる

《 基調講演 》

情報システム部門に求められる内部統制

～　IT統制の構築を目指して何をすべきか　～

2006年7月

新日本監査法人

システム監査部
AAA(Advanced Audit＆Advisory Service)グループ
シニアマネージャ　岡村和彦

目　次

Ⅰ．内部統制について

Ⅱ．IT統制

Ⅲ．IT統制の構築

Ⅰ．内部統制について

Ⅰ-(1) なぜ今、内部統制の強化が必要か（その1）

＜＜ SOX法の経緯 ＞＞

2001年12月　米国のエネルギ大手企業エンロンの破綻

2002年 6月　通信大手企業ワールドコムの不正経理が発覚

➡ ニューヨーク証券取引所の上場企業の発行株式時価総額が8兆円下落

2002年 7月　サーベンス・オクスリー法（SOX法）成立

➡ SOX法は、基本的に証券資本市場におけるディスクロージャー制度の信頼性を高め、投資家の利益を擁護することを目的として

- 「会計基準全般の見直し」
- 「監査人の独立性の強化と監視機関の設置」
- 「経営者の社会的責任意識の向上と企業のコーポレート・ガバナンスの向上」

の3本柱で構成されている。

SOX法の内部統制は、1992年に米国のトレッドウェイ委員会組織委員会（COSO：the Committee of Sponsoring Organization of the Treadway Commission）が公表した内部統制のフレームワークを示した「COSOの報告書」に準拠している。

Ⅰ-(1) なぜ今、内部統制の強化が必要か（その2）

＜＜　日本版SOX法誕生の経緯　＞＞

① 国内の相次ぐ企業の不祥事

2004年　2月　旧ソフトバンクBB（現BBテクノロジー）で450万件を超える個人情報を漏洩

2004年10月　西武鉄道の有価証券報告書の大株主の状況における虚偽記載の発覚

2005年 4月　カネボウの過去数年に及ぶ巨額粉飾が発覚、同年7,9月カネボウ経営者と担当の公認会計士が逮捕

2005年11月　顧客の預金約10億円を着服した疑いで東京三菱銀行の元派遣社員が逮捕

2005年12月　みずほ証券、ジェイコム株の誤発注で400億円を超える損失

2006年　1月　ライブドアの経営者が証券取引法違反容疑で逮捕

➡ 企業存続のために、多くのステークホルダーのため、不祥事の防止が必要となった。

② 会社法の成立

2005年　6月　会社法が成立し、大会社の内部統制システムの基本方針策定が義務化した。

Ⅰ-(1) なぜ今、内部統制の強化が必要か（その3）

＜＜　日本版SOX法の最新動向　＞＞

2005年12月　金融庁の企業会計審議会内部統制部会が「財務報告に係る内部統制の評価及び監査の基準案」を発表。

2006年6月7日　上場企業に対して内部統制の構築を義務付ける内容を含む「金融商品取引法」（いわゆる日本版SOX法）が参院本会議で可決、成立した。

2006年6月末現在　内部統制の構築、評価、監査のガイドラインとなる実施基準を策定中。

実施基準は、2006年6月公表の予定が延び、秋以降の見込み。

日本版SOX法が適用されるのは2008年4月1日からの事業年度。2006年末に対応を始めると準備期間は1年強しかない。

金融商品取引法には、上場企業に内部統制システムの整備や、内部統制報告書を提出することを義務付ける条文が盛り込まれている。

財務報告に係る内部統制についてその有効性を経営者自らが評価、内部統制報告書を作成、有価証券報告書と併せて開示する。その評価が適正であるかをどうかを、同企業の財務諸表監査を行っている公認会計士等が監査して担保する。

金融商品取引法では、企業が内部統制報告書を提出しなかったり、虚偽の報告書を提出した場合、5年以下の懲役もしくは500万円以下の罰金、または両方の罰則を科すといったことを定めている。

日本版SOX法は一般的に、金融商品取引法に、金融庁の企業会計審議会内部統制部会が2005年12月に公表した「財務報告に係る内部統制の評価及び監査の基準案」（以下、「基準案」という）と、同じく年内に公表する予定の「実施基準」の3つのことをいう。

Ⅰ-(2) 内部統制とは

内部統制（internal control）とは、一般に企業などの内部において、違法行為や不正、ミスやエラーなどが行われることなく、組織が健全かつ有効・効率的に運営されるよう各業務で所定の基準や手続きを定め、それに基づいて管理・監視・保証を行うこと。
そのための一連の仕組みを内部統制システムという。

「内部統制」という言葉は、昨今新たに誕生したものではない。従来から主に会計監査の分野でこの内部統制という概念が使われていた。財務諸表が適正に作成されたものかどうかを第三者が監査する際、**有効な内部統制が整備・運用されていることを前提に**、膨大な取引記録の中から“抜き取り検査”を行い、財務諸表に対する監査意見が形成されてきた長い歴史がある。

内部統制は、経営目的達成のために企業の経営者によって作られ、役職員（全員）によって行なわれるマネジメント・プロセスであり、企業を経営していく上で業務の有効性・効率性を目的とするなど、経営戦略とも言える前向きな仕組みでもある。

Ⅰ-(3) 内部統制の定義（金融庁が主宰する企業会計審議会内部統制部会による内部統制の定義）

内部統制の定義：

内部統制とは、基本的に4つの目的が達成されているとの合理的な保証を得るために、業務に組み込まれ、組織内の全ての者によって遂行されるプロセスをいい、6つの基本的要素から構成されている。

目的	業務の有効性及び効率性	事業活動の目的の達成のため、業務の有効性及び効率性を高めること （例）CS（顧客満足度）向上活動による業務の有効性向上、改善活動による効率性向上
	財務報告の信頼性	財務諸表及び財務諸表に重要な影響を及ぼす可能性のある情報の信頼性を確保すること （例）ステークホルダーに信頼できる財務報告を提供する
	事業活動に関わる法令等の遵守	事業活動に関わる法令その他の規範の遵守を促進すること （例）不正競争防止法、労働基準法、著作権法など関連法規・規範の遵守の促進
	資産の保全	資産の取得、使用及び処分が正当な手続及び承認の下に行われるよう、資産の保全を図ること (例）製造設備の修繕計画に基づく維持、不用な資産の適切な処分、特許権の取得・管理など
基本的要素	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、他の基本的要素の基礎をなし影響を及ぼす基盤 （例）経営方針・戦略、組織構造及び慣行、権限・職責等
	リスク評価と対応	組織の目標の達成に影響を与えるリスクを識別、分析及び評価することによって、当該リスクへの適切な対応を行う一連のプロセス (例）新規取引先の信用調査
	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 （例）明確な職務分掌・内部牽制、継続記録の維持、資産管理活動、組織内適切な分析・監視
	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 (例)イントラネット等による社内情報伝達、法令による財務情報の開示等
	モニタリング	内部統制の有効性を継続的に評価するプロセス （例）社員の業務日報を管理者がレビュー、顧客のクレームを定期的レビュー、従業員の規定遵守状況の定期的確認、内部監査等
	IT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 （例）IT全般統制、IT業務処理統制　等

黄色の部分はCOSOの内部統制のフレームワークに追加されたもの

Ⅱ. IT統制

Ⅱ-(1)「ITへの対応」

金融庁企業会計審議会内部統制部会「財務報告に係る内部統制の評価及び監査の基準のあり方について」(2005年12月8日公表)では、「ITへの対応」が次のように定義されている。

「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への対応」は、「IT環境への対応」および「ITの利用および統制」から構成される。

① IT環境への対応

組織目標を達成するために、組織の管理が及ぶ範囲において予め適切な方針と手続を定め、それを踏まえた適切な対応を行う。

IT環境とは、組織が活動する上で必然的に関わる内外のITの利用状況のことであり、社会及び市場におけるITの浸透度、組織が行う取引先等におけるITの利用状況、及び組織が選択的に依拠している一連の情報システムの状況等をいう。

② ITの利用および統制

組織内において内部統制の他の基本的要素の有効性を確保するためにITを有効かつ効率的に利用すること、並びに組織内において業務に体系的に組み込まれて様々な形で利用されるITに対して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、内部統制の他の基本的要素をより有効に機能させること。

Ⅱ-(2) IT統制の2つの基本概念

IT統制には、次の2つの概念がある。

① ITそのものを内部統制の対象とする概念

ITそのものを内部統制の対象とする概念。システム構築やITの新規導入などが、コンプライアンスの確保、利益の増大などの企業目標の達成につながるようにITを統制する。

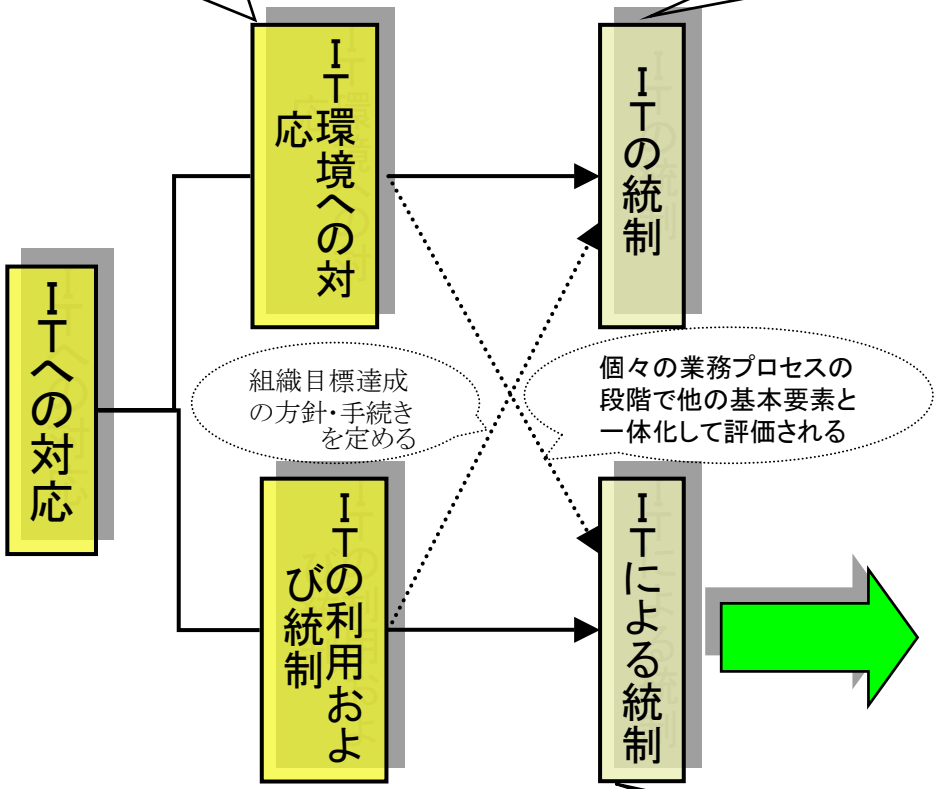
② ITへの対応以外の内部統制の基本的要素を有効に機能させるためにITをさまざまな形で利用する。

「ITへの対応」以外の内部統制の基本的要素(「統制環境」「リスクの評価と対応」「統制活動」「情報と伝達」「モニタリング」)を有効に機能させるためにITをさまざまな形で利用する。

Ⅱ-(2)　IT統制の2つの基本概念（その2）

組織目標を達成するために、組織の管理が及ぶ範囲において予め適切な方針と手続を定め、それを踏まえた適切な対応を行う

ITそのものを内部統制の対象とする概念。システム構築やITの新規導入などが、コンプライアンスの確保、利益の増大などの企業目標の達成につながるようにITを統制する。



基本的要素	ITによる統制の内容（例）
統制環境	イントラネットを利用した経営理念、倫理・行動規範などの周知。電子メールによる行動規範などの周知、経理上の留意事項の周知など。
リスクの評価と対応	情報システムを利用した取引相手の財務状況などの分析。与信管理システムや売掛債権管理システムの、財務リスクや事業リスクなどを評価するツールなど。
統制活動	アプリケーションシステムのプログラムによる入力データのチェック、財務会計システムへ連結するデータの正確性・適切性のチェックなど。
情報と伝達	財務会計システムや管理会計システムなどによる財務情報の把握、経営情報システムを利用した経営者や管理者による状況の把握、電子メールなどを利用した関係者への情報伝達など。
モニタリング	管理会計システムによる異常データのチェック、監査プログラムを利用したデータ分析など。

組織内において内部統制の他の基本的要素の有効性を確保するためにITを有効かつ効率的に利用すること、並びに組織内において業務に体系的に組み込まれて様々な形で利用されるITに対して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、内部統制の他の基本的要素をより有効に機能させること

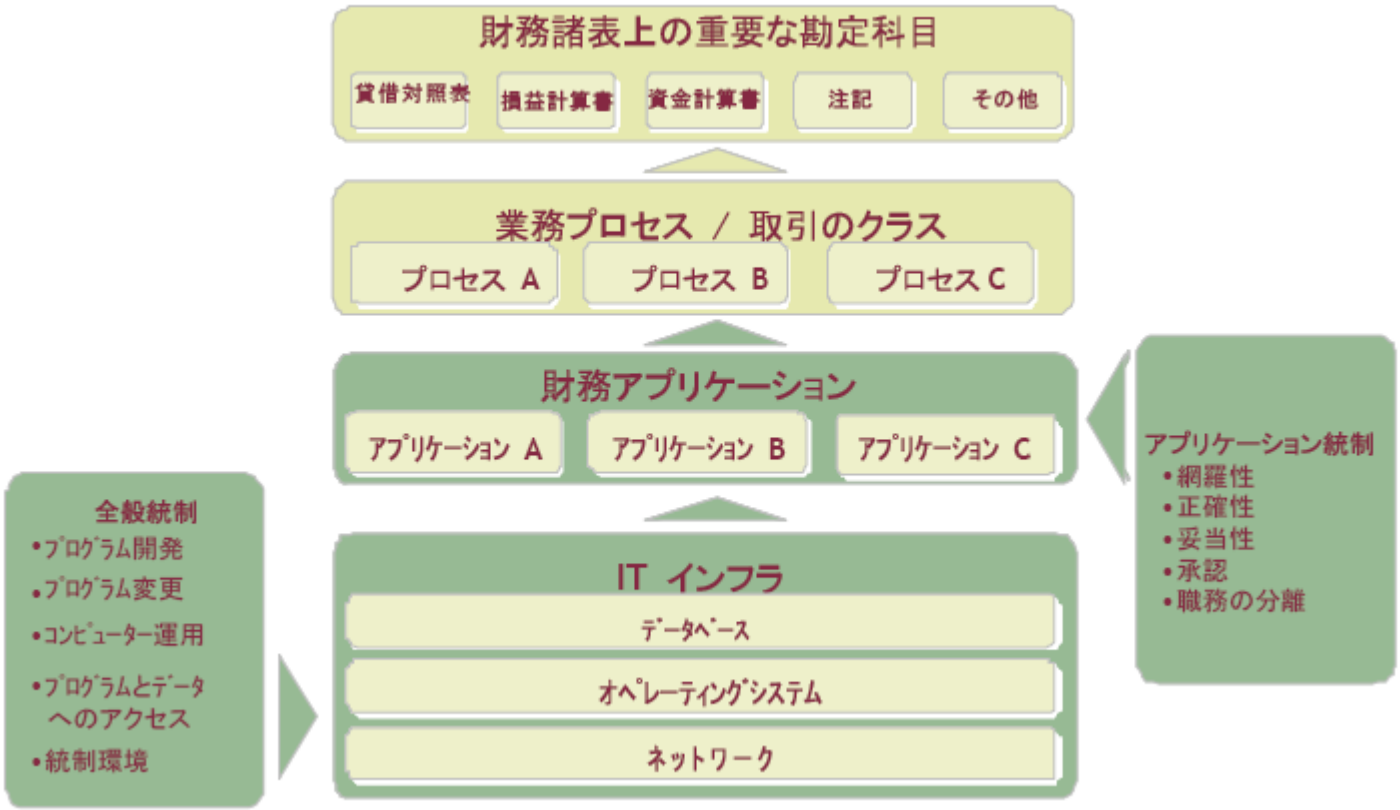
ITへの対応以外の内部統制の基本的要素を有効に機能させるためにITをさまざまな形で利用

IT環境とは、組織が活動する上で必然的に関わる内外のITの利用状況のことであり、社会及び市場におけるITの浸透度、組織が行う取引先等におけるITの利用状況、及び組織が選択的に依拠している一連の情報システムの状況等をいう。

Ⅱ -(3) IT統制の分類

ITに関連する統制を分類すると次の3つになる。
（米国上場会社会計監視審議会（PCAOB）から公表されている監査基準書第2号の概要から）

- ◆ 全社レベルの統制（全社的な内部統制）
- ◆ IT業務処理統制（別名：ITアプリケーション統制） ⇒ アプリケーションシステムの開発・保守・利用部門
- ◆ IT全般統制 ⇒ 情報システム部、データセンターの企画、運用管理部門



図表 IT統制 出典：「サーベインズ・オクスリー法（企業改革法）遵守のためのIT統制目標」（IT Governance Institute 2004年翻訳版）

Ⅱ-(4) IT全般統制

各アプリケーションシステムが機能する環境やシステムの管理・運用面におけるコントロールのことで、IT業務処理統制が有効であることを間接的に保証するコントロールのこと。IT業務処理統制が有効に機能する間接的なIT統制のこと。

一般的には、ネットワークの運用管理、システム・ソフトウェアの取得及び保守、アクセスコントロールやアプリケーションシステムの取得・開発及び保守に関する統制活動

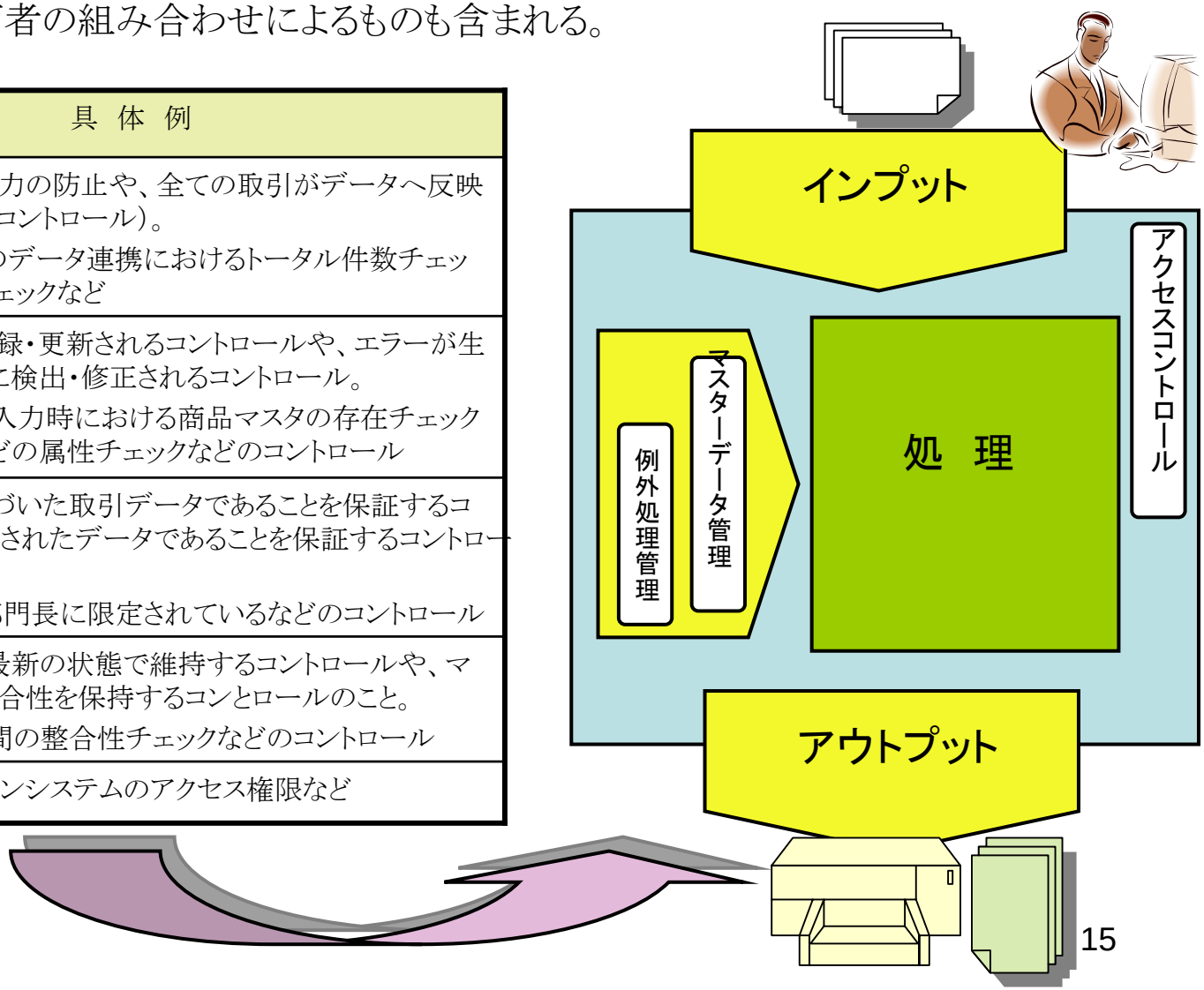
工場の生産管理システムなどを情報システム部門でなく他部門が管理している場合、IT全般統制の有効性は、システム管理部門別などの統制単位に評価する。

統制活動	具 体 例
情報システムに関する計画と組織の統制活動	**情報システム計画が文書化されて経営者の承認を得ている。 業務分担は明確で担当者間の相互牽制が考慮されている。**
情報システムに関する企画・開発・調達業務の統制活動	システム開発の各工程で管理者によるレビュー・承認を受けている。 システム変更は承認済みの依頼書に基づいて行われている。
システムに関する運用業務の統制活動	臨時のオペレーションは承認された申請書によって行われる。
セキュリティに関する統制活動	ID・パスワードなどによりアクセス管理を行う。
外部委託とそのサービスレベルの統制活動	業務委託先のサービス内容を評価する手続が定められている
監視活動	コンピュータ資源の使用状況の監視 ネットワークの監視 情報システムに関する内部監査

Ⅱ-(5) IT業務処理統制 （その1）

IT業務処理統制とは、販売システムや在庫管理システムなどの個々のアプリケーションシステムにおいて、開始された取引が承認され、洩れなく重複なく正確に記録され、処理されることを確保する統制活動をいう。入力データのフォーマットチェックなどのシステムによるものと入力原票の承認などの人によるもの、両者の組み合わせによるものも含まれる。

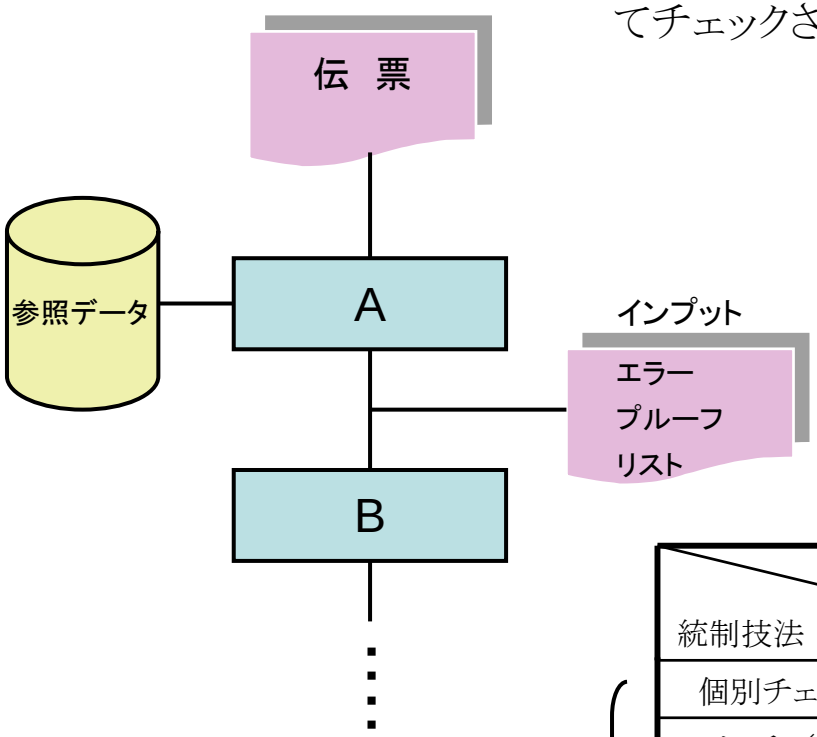
統制目標	具　体　例
データの網羅性	入力もれ・重複入力の防止や、全ての取引がデータへ反映されるための統制（コントロール）。 例：　システム間のデータ連携におけるトータル件数チェック、ファイル通番チェックなど
データの正確性	データが正しく記録・更新されるコントロールや、エラーが生じたデータが適切に検出・修正されるコントロール。 例：　注文データ入力時における商品マスタの存在チェックや、数値や文字などの属性チェックなどのコントロール
データの正当性	実際の取引に基づいた取引データであることを保証するコンとロールや、承認されたデータであることを保証するコントロールのこと。 例：承認機能が部門長に限定されているなどのコントロール
ファイルの維持・継続性	マスタファイルを最新の状態で維持するコントロールや、マスタファイル間の整合性を保持するコンとロールのこと。 例：マスタデータ間の整合性チェックなどのコントロール
その他	例：アプリケーションシステムのアクセス権限など



Ⅱ-(5) IT業務処理統制（その2）　インプットコントロールの例

入力された取引データは、最初のアプリケーションプログラムAによってチェックされる。この時点において管理要点は次のものがある。

1. インプットの完全性（網羅性）
   全ての取引データがインプットされたか
2. インプットの正確性
   取引データは、正しくインプットされたか



2005年12月に起きたみずほ証券のジェイコム株の誤発注にはどのコントロールが有効か？

統制タスク ＼ 統制技法	インプット	
	網羅性	正確性
個別チェック法	○	○
バッチ／トータルチェック法	○	○
シーケンスチェック法	○	
コンピュータ突合法	○	○
エディトチェック法		○
事前記録のインプット		○
2回インプット		○
キーベリファイ		○

Ⅱ-(6) IT業務処理統制とIT全般統制との関係

IT全般統制とIT業務処理統制の有効性に関する関係の例

	IT全般統制	IT業務処理統制	事　例
ケース1	有効	有効でない	例：コンピュータ室への入室管理が十分行われているが、アプリケーションシステムにはユーザ認証のアクセスコントロールが組み込まれていない。 ⇒　入室可能な者であれば、システムを使用することができ、内部の者によってシステムが不正に利用される可能性がある。
ケース2	有効でない	有効	例：アプリケーションプログラムが勝手に変更される。 ⇒　アプリケーション統制が有効であってもプログラムが不正変更される可能性があり、継続して有効であることが保証できない。

Ⅲ．IT統制の構築

情報システム部門が、日本版SOX法に対応するために、これからすべきこと。

Ⅲ-(1) 整備範囲を明確化

整備範囲を明確化する。

全社的な対応指針のもとで、あらかじめ整備範囲を明確に定義する。
日本版SOX法で要求される財務報告に関わる内部統制を*優先して中心に*整備を行う。

Ⅲ-(2) 文書化

内部統制の整備及び運用の方針及び手続の状況、内部統制の整備及び運用状況、財務諸表に係る内部統制の有効性の評価手続及びその評価結果並びに発見した不備及びその是正措置に関して記録し保存しなければならない(「基準案」より)。

IT部門に求められる文書化は次のようなものになる。

① **手作業から自動化された統制**(アプリケーション統制)**部分の文書化**(手作業の統制に関しては各部門で担当)

② **アプリケーション統制を担うコンピュータシステムの管理プロセス**(IT全般統制)**とIT部門全体としての取組み姿勢**(IT企業レベル統制)**等のIT部門自身の業務に関する文書化**

③ **内部統制の有効性評価により、統制に改善が求められ、それが修正要求につながる場合への対応**

① **フローチャート**
各業務プロセスの業務処理手順を文書にした説明書

② **業務手続説明書**
業務プロセスごとに詳細作業と情報の流れを図示した一覧表

③ **リスク・コントロールマトリックス**
プロセスごとに洗い出したリスクを記載し、リスクを低減するための統制活動を記載した一覧表。

④ **内部統制の整備範囲の決定事由**
全社的な対応指針を示した上で、ITまで含めた包括的な整備範囲を明確に定義し、この整備範囲の決定理由を明確にする。

⑤ **改善活動の記録**
特にIT業務処理統制の場合、正式な変更手続きに基づいた修正を実施することが、IT全般統制が整備されていることを証明するためにも重要である。

米国では、フローチャート、業務手続説明書、リスク・コントロールマトリックス等を作成するのが一般的である。

作業量を見積もり、準備スケジュールを立てる。

Ⅲ-(3) セルフチェックテストの実施 （その1）

ISACA（情報システムコントロール協会）から、企業改革法への対応を容易にできるように「企業改革法遵守のためのIT統制目標」（2004年翻訳版）が公表されている（http://www.isaca.gr.jp/research/）。米国のサーベンス・オクスリー法（企業改革法）の適用に対応するために作成された、IT Control Objectives for Sabanes Oxley Actの翻訳版。ここのIT統制目標は、企業が財務報告に係る内部統制の評価を行い、監査人がその監査を行う際の指針となるように策定されている。

⇒ 情報システム部門は、自らこの「企業改革法遵守のためのIT統制目標」を利用して、予めセルフチェックテストをして、テストの結果、不備や欠陥のある個所は改善する。

【ITの統制目標】

- 全社レベルの統制（全社的な内部統制）
  - 統制環境
  - 情報と伝達
  - リスク評価
  - モニタリング
- アプリケーション統制 － ビジネスサイクル
  - 販売におけるアプリケーション統制の目的
  - 購買におけるアプリケーション統制の目的
  - 棚卸資産に関するアプリケーション統制の目的
  - 資産管理におけるアプリケーション統制の目的
  - 人事部におけるアプリケーション統制の目的

- IT全般統制 － プログラム開発とプログラム変更
  - アプリケーションソフトウェアの調達または開発
  - 技術インフラの調達
  - 方針と手続きの策定と保守
  - アプリケーションソフトウェアと技術インフラの導入およびテスト
  - 変更管理
- IT全般統制 － コンピュータオペレーションおよびプログラムとデータベースへのアクセス
  - サービスレベルの定義と管理
  - サードパーティサービスの管理
  - システムセキュリティの保証
  - 構成管理
  - 問題と事故の管理
  - データ管理
  - オペレーション管理

Ⅲ-(3) セルフチェックテストの実施 （その2）

変更管理	
統制に関する指針	
統制目標－財務報告上重要なシステム変更は、本番環境に移行する前に承認され、適切にテストが実施されている合理的な保証を提供する。	
根拠－変更管理は、事業の財務報告の目的達成をサポートするため、組織がどのようにシステムの機能を変更するかに取り組むものである。この領域に不備がある場合、財務報告に重要な影響を与える可能性がある。例えば、財務データを勘定に振り分けるプログラムを変更する際は、分類と報告の万全性(インテグリティ)を確実にするため、変更前の適切な承認とテストが必要になる	
統制の例	統制テストの例
システムソフトへの変更を含む、プログラム変更、システム変更および保守管理の要求は、標準化され、文書化された正式な変更管理手続きに従っている。	文書化された変更管理手続きが存在し、現在のプロセスを反映するように内容が維持されているかを確かめる。 プログラム変更、システムの保守管理、インフラの変更を含む、本番環境の全ての変更について、変更管理手続きが存在するかを考慮する。 変更要求を統制し、モニターするための手続きを評価する。 変更要求は適切に開始され、承認され、最後まで追跡されているかを検討する。 プログラム変更は、職務の分離が行われた、統制された環境で実施されているかを確かめる。 アプリケーションまたはシステムに行われた変更のサンプルを選び、本番環境移行前に、これらが適切にテストされ、承認されたかを確かめる。オペレーション、セキュリティ、IT インフラの管理、IT の管理が承認手続きに含まれているかどうかを確かめる。 権限を与えられた/承認された変更のみが本番に移行していることを保証する手続きを評価する。 変更のサンプルを選び、変更依頼ログおよび根拠資料を追跡する。 これらの手続がシステムソフトの修正に適時に対応していることを確認する。サンプルを選び、文書化された手続きに従っているかを確かめる。

例 「企業改革法遵守のためのIT統制目標」(2004年翻訳版)「IT全般統制－プログラム開発とプログラム変更 変更管理」

講演内容に関するお問合せ、ご質問等

本講演内容に関するご質問、ご意見などございましたら下記宛にお願い致します。

新日本監査法人　システム監査部

AAAグループ　岡村和彦

E-Mail: okamura-kzhk@shinnihon.or.jp

Tel　：　03－3503－1138
Fax　：　03－3503－1966