検討の背景

◆ 「セキュア・ジャパン2006」（2006年6月15日　情報セキュリティ政策会議決定）

第2章 第4節

ウ）情報セキュリティ関連制度と内部統制制度等との整合性確保（内閣官房、金融庁及び経済産業省）

「政府が推進する情報セキュリティに関する取組みについて、政府全体としての整合性を確保するため、現在構築が検討されている内部統制制度のIT統制に係る部分において、情報セキュリティに関連する事項については、既存の対策基準等の情報セキュリティ関連制度との関連を考慮しつつ、2006年度に検討を進める。」

企業がIT統制を構築する際に参照する代表的なフレームワーク

- ◆ IT統制全般
  - COBIT（米国ITガバナンス協会）（→IT Control Objectives for SOX（同左））
  - **システム管理基準（経済産業省）**
- ◆ ITシステムの運用管理
  - ITIL（英国政府）
- ◆ その他
  - 自社で開発した基準　等

主にIT統制のために策定した基準であるが、情報セキュリティ関連部分についてはISO/IEC17799等との整合性を確保

SOX法対応のためにCOBITをベースにIT統制目標を整理し、統制を例示したもの

状況分析

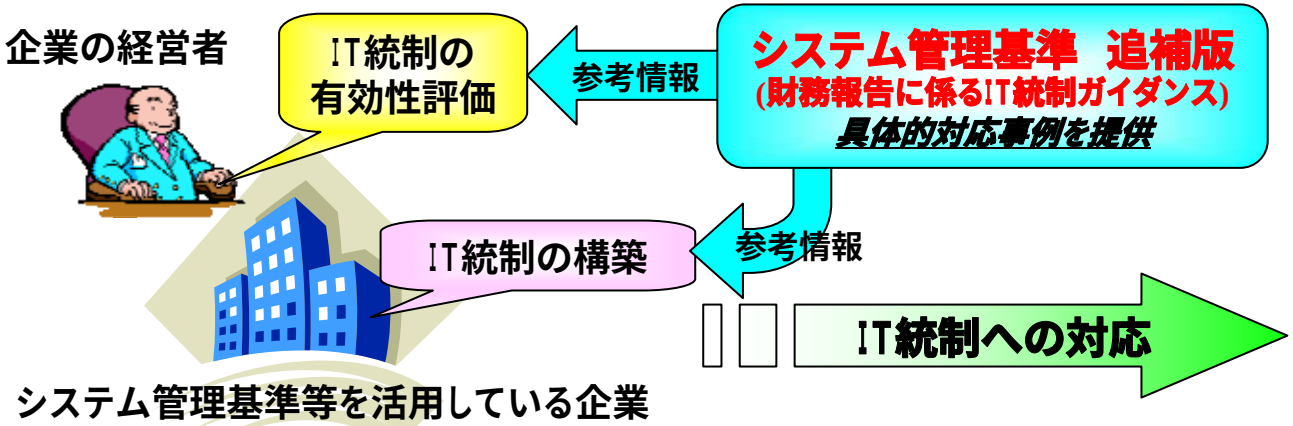
- ほとんどのフレームワークは全般統制にしか言及がないため、財務情報の適正性を確保する観点からIT統制を構築する際、企業は具体的に何をすべきかが明確ではない。
- また、海外のフレームワークは、欧米の商習慣を前提としているので、我が国の企業にそのまま適用しづらい面もある。（我が国企業がシステム監査の際に参照している基準等について調査した結果では、約75％の企業が「システム監査基準」（改訂前）を参照している。）

検討内容

- 企業がIT統制を構築する際に具体的に何をすべきかが判断できるよう、「システム管理基準（平成16年10月改定）」をベースに、金取法に則したIT統制の具体的な事例集（追補版）を検討。

「システム管理基準　追補版」の位置付け

- ２００６年６月に成立した**金融商品取引法により、上場企業等は、２００８年４月以降、財務報告に係る内部統制の整備及び運用状況の有効性について評価、報告することが義務化。**
- 我が国企業の数多くの業務において、ITへの依存度が増大していることを背景に、**金融商品取引法の枠組みにおいても、「ITへの対応(→IT統制)」は内部統制の基本的要素の一つ。**
- 我が国においては、経済産業省の策定した「システム管理基準」及び「情報セキュリティ管理基準」(以下、「システム管理基準等」)が、有効な情報システム管理のための指針として広く活用されているところであるが、システム管理基準等だけではIT統制に係る詳細が不明確。
- このため、経済産業省として、「企業のIT統制に関する調査検討委員会」等を設置し、2007年3月末、**システム管理基準等を活用している企業が「ITへの対応」を行っていくための「参考情報」として、主要なケースを想定しつつ、それぞれの企業がIT統制をどのように構築し、経営者がその有効性をどのように評価するかについての具体的対応事例集である「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)」を策定。**
- なお、金融商品取引法に基づき、経営者による有効性評価については、公認会計士又は監査法人がその適正性につき監査することとなっているが、本追補版はあくまでもIT統制の構築と経営者による有効性評価までを対象としていることに留意。



http://www.meti.go.jp/press/20070330002/20070330002.html

金融商品取引法における内部統制の６つの基本要素

1. 統制環境
2. リスクの評価と対応
3. 統制活動
4. 情報と伝達
5. モニタリング（監視活動）
6. **ITへの対応(→IT統制)**

(参考)財務報告に係る内部統制をめぐる日米比較

【法律】

財務報告に係る内部統制に関して、我が国の「金融商品取引法」に相当する米国の法律はＳＯＸ法(サーベンス・オクスリー法：２００２年７月成立)。

【内部統制の枠組み】

米国では、ＳＯＸ法に基づいて設置されたＰＣＡＯＢ(公開会社会計監視委員会)において、ＩＴ統制以外も含んだ内部統制の枠組みに係る基準として、「監査基準第２号」を作成。一方、日本では、企業会計審議会において、内部統制の枠組みに係る基準を作成。

【ＩＴ統制の枠組み(参考情報)】

米国では、ＩＴ統制の枠組みとして、民間のＩＴガバナンス協会(ＩＴＧＩ)等が提唱するＣＯＢＩＴ（Control Objectives for Information and related Technology）等が一般的に使用されており、同協会は、米国ＳＯＸ法におけるＩＴ統制に対応するために、具体的対応事例を提供する”IT Control Objectives for SOX”を公表。日本において、前者に相当するものが「システム管理基準等」であり、**後者に相当するものが、今般策定した「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)。**

	日本	米国
法律	金融商品取引法	SOx法
内部統制の枠組み(政省令等に相当)	「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) 「実施基準」(企業会計審議会)	PCAOB監査基準第2号
ＩＴ統制の枠組み(参考情報)	システム管理基準等 ＋ 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)	COBIT等 ＋ IT Control Objectives for SOX

(参考)「企業のIT統制に関する調査検討委員会」名簿

【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
島田 裕次	日本内部監査協会（IIA）
清水 惠子	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

(参考)「企業のIT統制に関する調査検討委員会作業部会」名簿

【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 惠子	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
原田 要之	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

「システム管理基準　追補版」の構成

第Ⅰ章 構成と用語について	本追補版の全体構成、各章の概要、本追補版で使用する用語について解説したもの	
第Ⅱ章 IT統制の概要について	財務報告とIT統制の関係、IT統制の意義、種類等、IT統制の基本的な概念について解説したもの	主に経営者等を想定
第Ⅲ章 IT統制の経営者評価	財務報告に係る内部統制を経営者が評価するに際して、IT統制をいかに評価すべきかのポイントを解説したもの	
第Ⅳ章 IT統制の導入ガイダンス （IT統制の例示）	企業がIT統制を構築するため、財務情報に係るIT関連のリスクとIT統制の関係、具体的なIT統制の事例等を項目別に解説したもの	主に実務者等を想定
付録1～6	本追補版の利用にあたり参考となる情報を示したもの（本追補版と米国の関連指針等との比較表、システム管理基準と本追補版を合わせた活用方法の例、等）	

（注）本追補版の提供するものは、あくまでも、主要なケースを想定した参考情報であり、第Ⅱ・Ⅲ章を十分理解し、必要に応じて、第Ⅳ章に掲げる項目の修正・削除・追加等を行いつつ、自社の実情に合わせた運用を行っていくこと。

目次

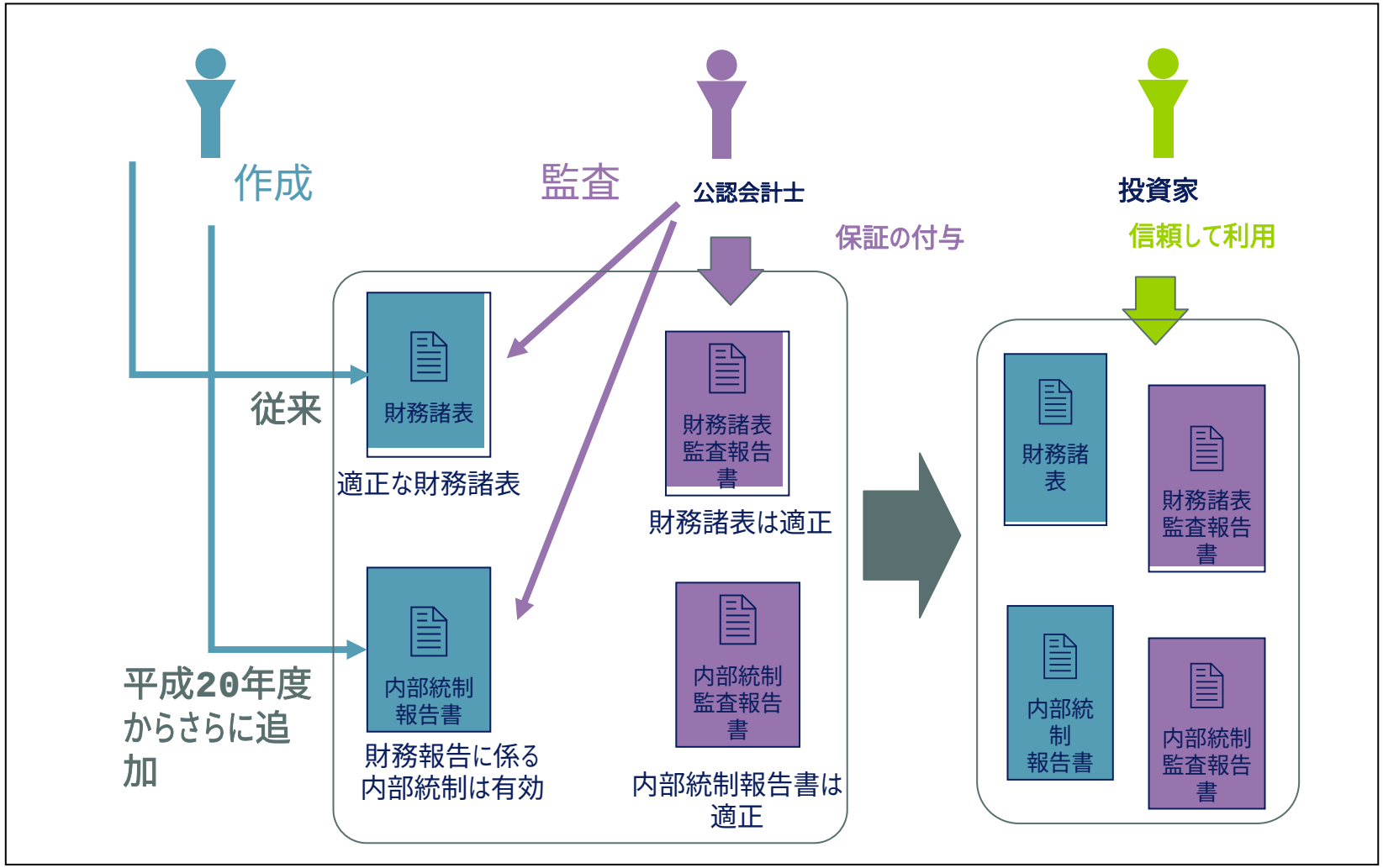
第Ⅰ章　IT統制（ITに係る内部統制）の概念

■ 「ITに係る全般統制」及び「ITに係る業務処理統制」の概念

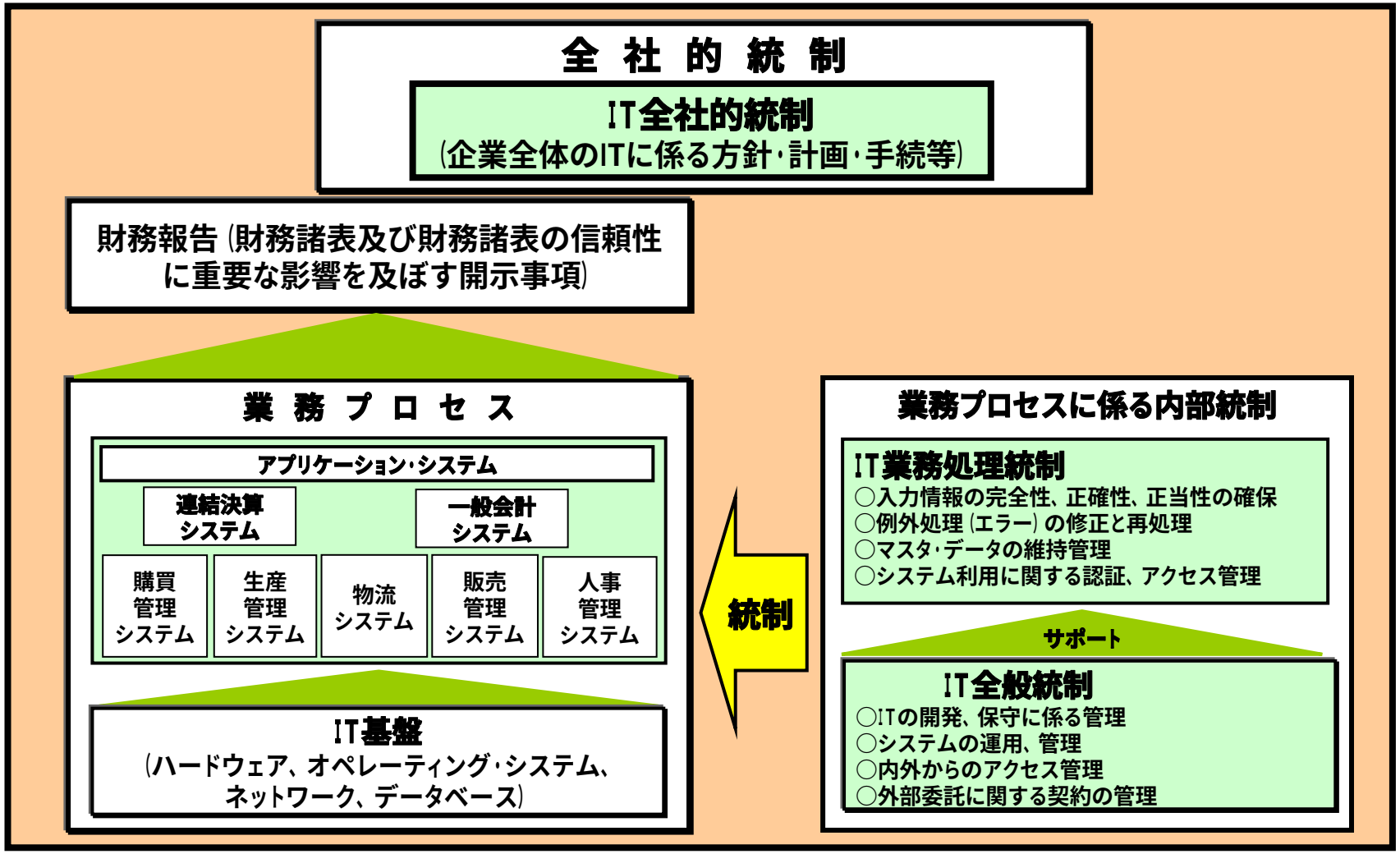
「実施基準」では、「ITに係る全般統制」（以下、「IT全般統制」という）と「ITに係る業務処理統制」（以下、「IT業務処理統制」という）の用語が登場する。
本追補版では、ITに直接係る部分とそれ以外とを区別するため、「IT統制」について以下のように分類する。

IT全社的統制	企業の統制が全体として有効に機能する環境を保証するためのITに関連する方針と手続等、情報システムを含む内部統制。 連結グループ全体としての統制を前提とするが、各社、事業拠点ごとの全体的な内部統制をさす場合もある⇒（実施基準　Ⅱ．３（２）①）。
IT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を意味しており、通常、複数の業務処理に関係する方針と手続のうち、IT基盤を単位として構築する内部統制⇒（実施基準　Ⅰ．２（６）②〔ITの統制〕ロa）。
IT業務処理統制	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、記録されることを担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⇒（実施基準　Ⅰ．２（６）②〔ITの統制〕ロb）。

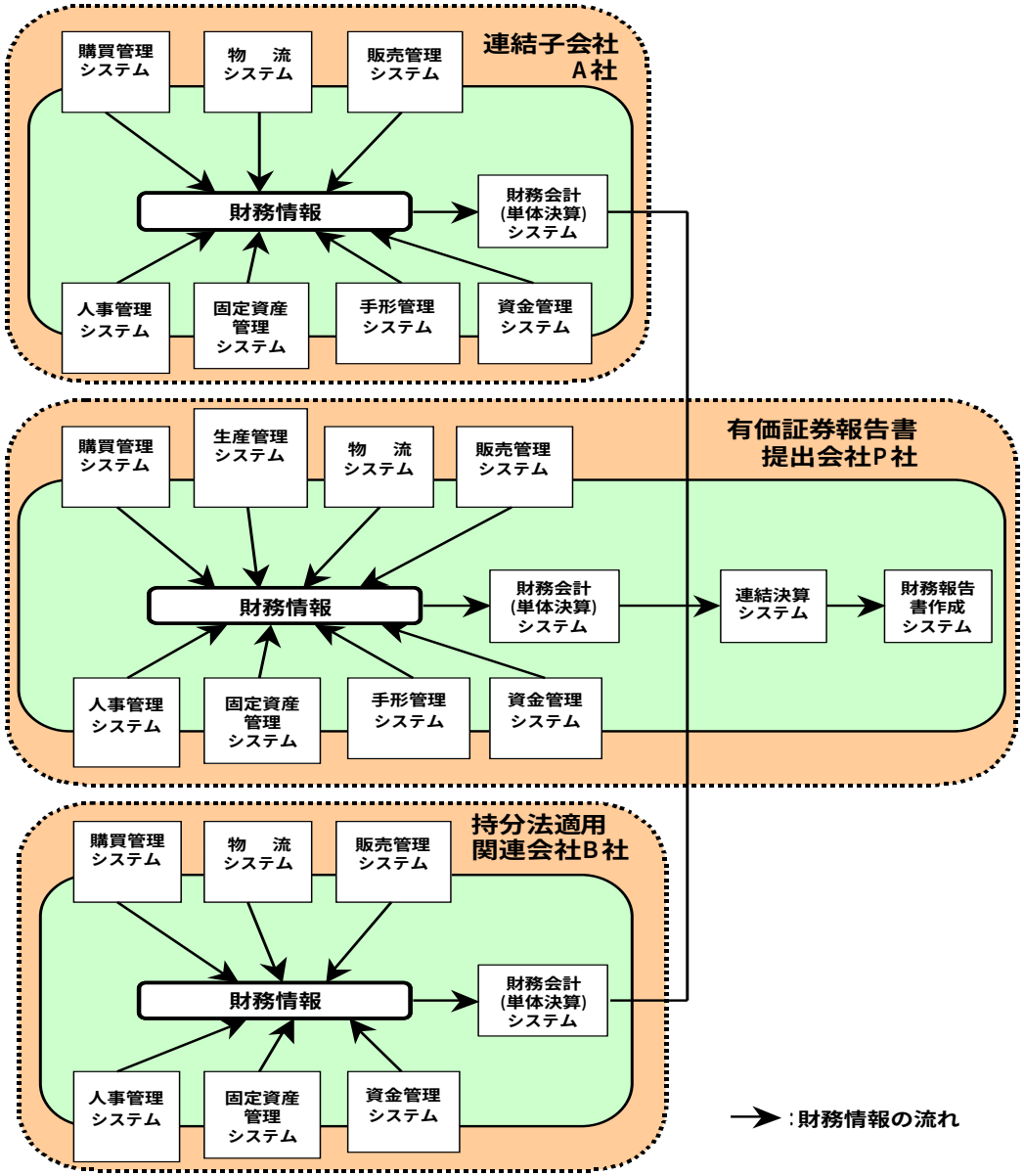
第Ⅱ章　財務諸表監査と内部統制監査



第Ⅱ章　財務報告とIT統制との関係



第Ⅱ章　財務報告とアプリケーション･システムの関係



第2章　IT統制の統制項目　①IT全社的統制

■ IT全社的統制とは、企業集団全体（連結対象企業を含む）を対象としたITに係わる内部統制のことであり、企業集団全体のITを健全に維持、監督するために構築するものである

a．ITに関する基本方針の作成と明示（統制環境）
b．ITに関するリスクの評価と対応（リスクの評価と対応）
c．統制手続の整備と周知（統制活動）
d．情報伝達の体制と仕組の整備（情報と伝達）
e．全社的な実施状況の確認（モニタリング）

第2章　IT統制の統制項目　②IT全般統制

■ **IT全般統制とは、財務情報の信頼性に直接関連する業務処理統制を有効に機能させる環境を実現するための統制活動**

■ **ITの企画・開発・運用・保守というライフサイクルの中で、リスクを低減するための統制を適切に整備・運用**

【IT全般統制の具体例】
- **システムの開発、保守に係る管理**
- **システムの運用・管理**
- **内外からのアクセス管理等のシステムの安全性の確保**
- **外部委託に関する契約の管理**

■ 新規のプログラム
  – 信頼性がテストされ、承認されて本番環境に移行

■ プログラムの保守
  – 信頼性がテストされ、承認されて本番環境に移行
  – 旧システムから変換されて、新システムに移行されるデータも同様の過程を経て、本番環境に移行

■ プログラムの運用
  – 未承認の処理や不正な処理が防止

■ プログラムとデータへのアクセス
  – あらかじめ承認された者だけにアクセス権限を設定（予防的統制）
  – アクセス違反をモニタリング：プログラムとデータの改ざんが防止（発見的統制）。

■ 開発・保守・運用を外部委託
  – 委託先で、プログラムとデータの信頼性が確保

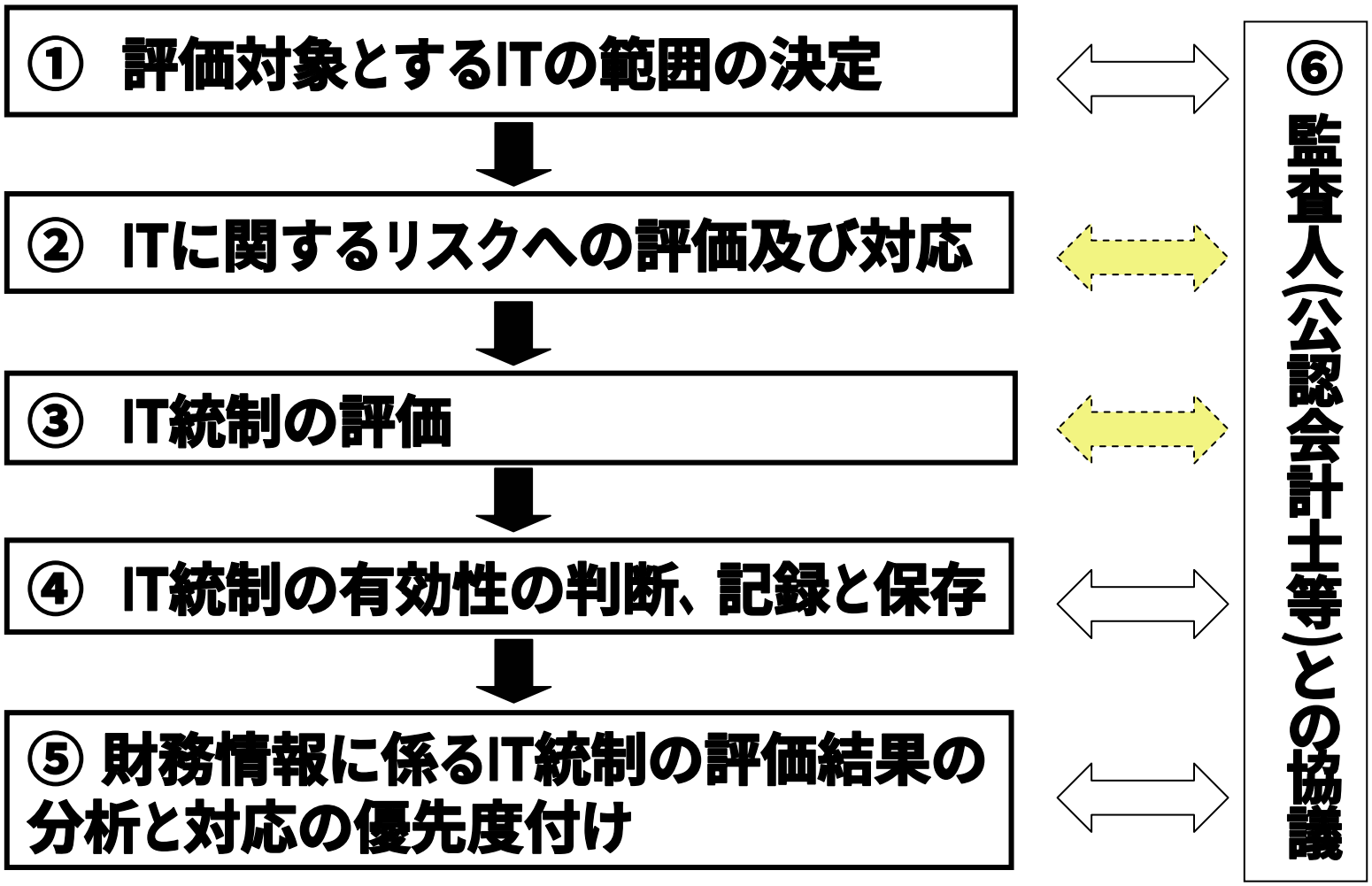
第2章　IT統制の統制項目　③IT業務処理統制

■ **IT業務処理統制とは、業務を管理するIT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内部統制**

•情報処理とIT業務統制は異なるもの
•業務処理統制ポイント
•入力管理
•出力管理
•データ管理

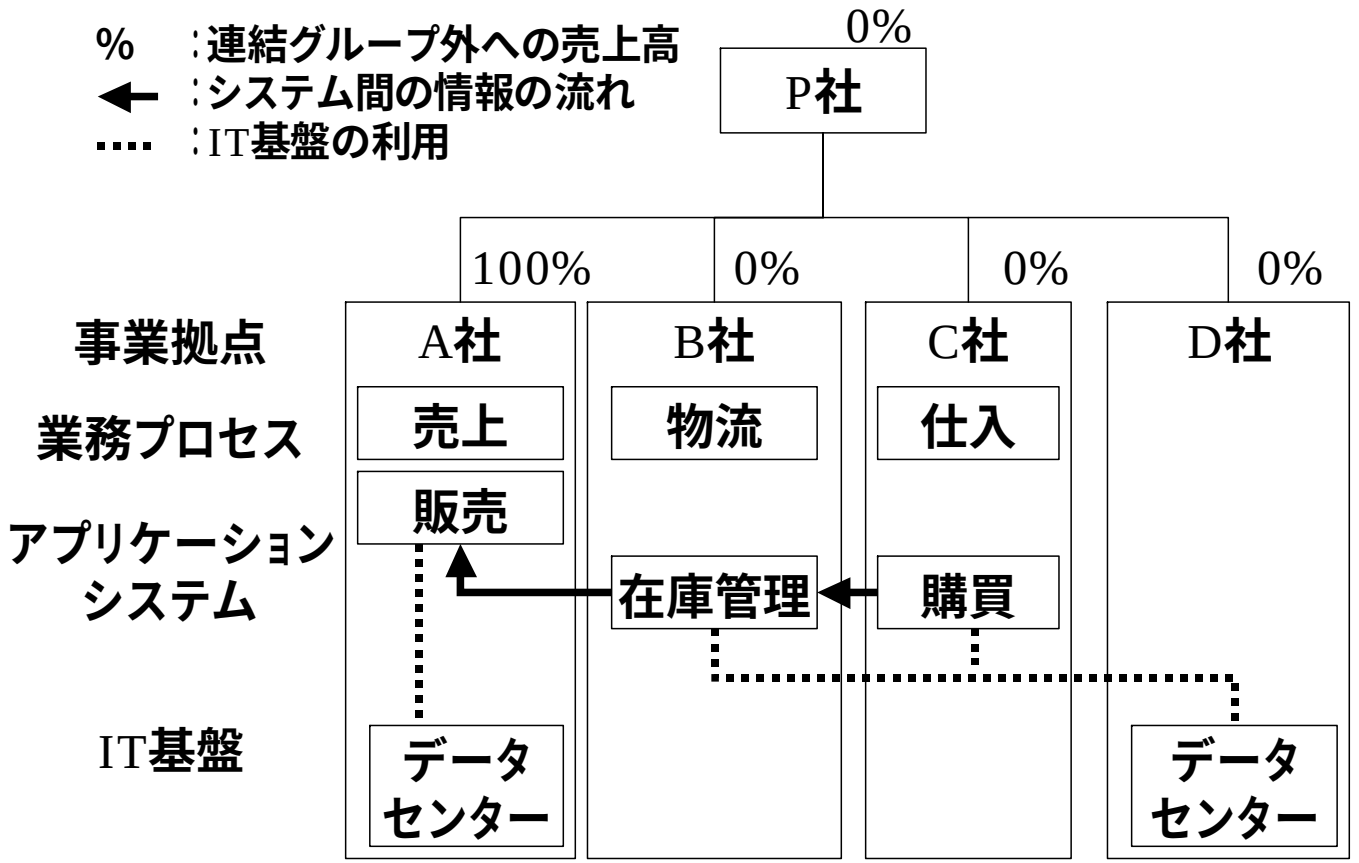
【スプレッドシート等】
- 利用者のPCが全社的な管理から漏れている
- 計算式等の誤りや決算データの恣意的な修正等、虚偽記載のリスク
- 対策
  - 管理体制（当事者以外による点検等）
  - 虚偽表示のリスク、対策のコスト、統制の効果等を勘案して、自社に適した方法を選択する

IT統制の評価のロードマップ



評価範囲の決定と対象となるITの把握

(1) ITの全体像の把握
(2) 評価範囲の決定
(3) 把握すべき内容
- 業務プロセス
- 業務プロセスに関係するアプリケーション・システム
- IT基盤（ハードウェア・基本ソフトウェア・ネットワーク等の概要、外部委託の状況等）
- ITに関与する組織、方針　⇒（実施基準　Ⅱ．3 (3) ⑤ロb）



IT全社的統制の評価

(1) 評価の意味

■ ITに係る規程類の内容が不十分、従業員への周知・徹底が不十分

→各事業拠点のすべてが、均質で同じ水準のIT統制が行われていない可能性

■ 企業のITに関する戦略や計画が不明確

→大規模システムの更改に失敗し、業務に混乱（財務諸表そのものが作成できなくなったりする可能性）

(2) 評価における留意点の例

① 経営者が内部統制を支えるITの重要性について認識している

② 経営者が財務情報に係るIT の信頼性について、リスクの評価と対応を検討している

③ 経営者が財務情報に係るITの整備・運用に係る予算を承認している

④ 財務情報に係るITの整備・運用の状況につき経営者が適宜報告を受け、改善が行われる仕組がある（情報と伝達及びモニタリングの確立）

⑤ IT統制に係る記録の採取と保存に関する規程や体制が存在する：経営者による評価や監査人による監査に支障

IT全般統制の評価

評価における留意点の例

a. **ITの開発・保守ITに関する開発(含む調達)業務**
   - 情報システムの新規開発やパッケージソフトウェアの導入、並びにITの運用・管理のための統制
   - ITに関する開発業務の管理
   - ユーザ部門の参画による十分なテストの実施
   - プログラム等の移行や変更管理

b. **システムの運用・管理**
   - 企業が適切なデータを適切なプログラムで処理

c. **情報セキュリティ**
   - 不正使用、改ざん、破壊等を防止するために、アクセス管理や自然災害等への対策

d. **外部委託**
   - 委託業務を管理
   - 受託会社の選定基準、成果物等の検収体制、受託会社の統制を理解し、自社の統制に与える影響

IT業務処理統制

- アプリケーション・システムに組み込まれた統制活動（自動化された統制活動）
- 手作業とITが一体となって機能する統制活動（ITによる情報を使用した統制活動）
- ITや手作業による統制を一体として実施されていることを、ウォークスルー（財務報告目的のITにおける取引の開始から財務諸表の作成までを追跡）により理解することが有用

業務プロセスの把握と整理

経営者は、財務報告に係るIT統制（IT全般統制とIT業務処理統制）について、業務プロセスとの関連で評価する

①「決算・財務報告プロセス」
・経理部門が担当する決算・財務報告に関わる業務プロセス
→原則として、すべての事業拠点を対象として評価
・連結財務諸表作成プロセス
→スプレッドシート等を利用する場合、スプレッドシートの統制についても評価

②「決算・財務報告以外のプロセス」
・業務プロセスと関連する業務アプリケーション・システムの概要及び業務プロセスの働きと財務情報の流れを把握

ITの統制目標とアサーション

ITの統制目標	アサーション（適切な財務情報を作成するための要件）
完全性	網羅性、期間配分の適切性、
正確性	実在性、評価の妥当性、期間配分の適切性、表示の妥当性
正当性	実在性、権利と義務の帰属、評価の妥当性

- IT全社的統制の有効性の判断
- IT全社的統制に不備がある場合
- ITに係る業務プロセスの内部統制の有効性の判断
  - ① 業務プロセスへのIT統制の整備状況及び運用状況の有効性の評価
  - ② IT全般統制に不備がある場合
  - ③ IT業務処理統制に不備がある場合

第IV章　ガイダンスの使い方

①リスク分析と統制（自社のIT統制を評価）

リスク分析の結果　→　すべての重要なリスクが対応　→　IT統制が有効に機能

②未対応の重要なリスクへの対応

（財務報告の虚偽表示に係る重要なリスクが存在する場合）

- ●リスクが内部統制の不備になるか評価 →リスクコントロールマトリックスの利用
- ●リスクへの対応が必要な場合には、IT統制を整備する
  →「システム管理基準等」の管理項目から、自社のリスクを低減する適切な項目を選択
  →統制項目により、財務報告の虚偽表示に係るリスクが低減され、受容できるリスクレベルになることを確認

③システム管理基準統制目標の利用

- ●管理項目および管理項目の主旨を理解する
- ●対応する統制項目を明確にし、ガイダンスの管理項目のリスクを理解する
- ●該当するリスクが低減したいと考えているものであれば、統制項目の候補となる
- ●統制項目をリストアップし、企業のリスクを低減できることを確認（ＲＣＭの利用など）

第Ⅳ章　IT統制の例の利用について

- IT統制の例は、整理、例示されている
- 【統制に関する指針】・・・IT統制についての概略
- 【統制目標の例】・・・統制目標についての例示
- 【統制の例と統制評価手続の例】・・・①リスクの例示、②統制の例示、③統制評価手続の例示

(1)	入力管理ルールを定め、遵守すること。	業務	情報システムへのデータ入力に伴う一連の作業について手順、検証方法、承認方法を明文化する	4-(1)-①	C	入力データの作成、授受、検証、入力の実施、入力後の確認、保管等、情報システムへのデータ入力に伴う一連の作業について手順、検証方法、承認方法を入力管理ルールとして明文化し、遵守する必要がある。
(2)	データの入力は、入力管理ルールに基づいて漏れなく、重複なく、正確に行うこと。	業務	入力データに欠落、二重入力等の誤りが発生しない	4-(1)-②	S	情報システムにデータを入力する際は、入力データに欠落、二重入力等の誤りが発生しないように入力管理ルールに記載されている手順に従い、正確に行う必要がある。
(3)	入力データの作成手順、取扱い等は誤謬防止、不正防止、機密保護等の対策を講じること。	業務	入力データの作成、取扱い等での不正を防止する		S	入力データの作成、取扱い等を正確に行ない、不正を防止するため、データの作成手順、取扱い等は、誤びゅう防止、不正防止及び機密保護等の対策を講じる必要がある。

これらの例示を参考にして、自社のリスクと統制の指針にあう統制目標を決める。
その（経営者）評価は、統制評価手続きを参考に決める

第Ⅳ章

IT全社的統制

(1) ITに関する基本方針の作成と明示（統制環境）
(2) ITに関するリスクの評価と対応（リスクの評価と対応）
(3) IT利用と統制（統制活動）
(4) 情報伝達の体制と仕組の整備（情報と伝達）
(5) 全社的な実施状況の確認（モニタリング）

IT全般統制

(1) 情報システムのソフトウェアの開発・調達
① ソフトウェアの開発・調達　② IT基盤の構築
③ 変更管理　④ テスト
⑤ 開発・保守に関する手続の策定と保守
(2) システムの運用・管理
① 運用管理　② 構成管理
③ データ管理
(3) 内外からのアクセス管理等のシステムの安全性の確保
① 情報セキュリティフレームワーク　② アクセス管理等のセキュリティ対策
③ 情報セキュリティインシデントの管理
(4) 外部委託先の管理
① 外部委託先との契約　② 外部委託先とのサービスレベルの定義と管理

IT業務処理統制

(1) 入力管理（入力統制）
(2) データ管理（処理統制）
(3) 出力管理（出力統制）
(4) スプレッドシート等（EUC）

第IV章　2～4．リスクコントロールマトリックスの利用

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

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	自動手動	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	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、フォローされていりことを確かめる	なし	記載省略	低
			2	FAX受注はコールセンターで受信後に連番を記入し、一人が入力した後で、プ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・手動	日	○	NA	NA	NA	NA	NA	運用	特定の月の25件を選び、プ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こんでいる。	自動	日	○	○	NA	NA	×	NA	整備・運用	受注残ファイルが営業担当者により、消しこ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い	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	日	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	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、プ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・手動	月日	NA	○	NA	○	○	○	整備・運用	特定の月の25件を選び、プ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	日	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	日	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認する	なし	記載省略	低
			8	単価は得意先ごとにマスタに登録された単価が自動的にロードされる	自動	日	NA	○	NA	NA	○	○	整備・運用	単価が自動的に登録されることを確かめる	なし	記載省略	低
正当でない財務情報が記録される	正当性	正当でない受注が登録される	9	得意先マスタに登録された得意先以外は登録できない	自動	日	NA	○	NA	○	NA	NA	整備・運用	マスタに登録された相手先しか登録できないことを確かめる（設定はマスタ登録で確かめる）	なし	記載省略	低
			10	単価は得意先ごとにマスタに登録された単価が自動的にロードされる	自動	日	×	○	NA	○	○	○	整備・運用	単価は登録単価が登録され、単価入力ができないことを確かめる（単価登録はマスタ登録で確かめる）	なし	記載省略	低
			11	受注入力は、担当者のIDとパスワードで制御されている	自動	日	NA	○	NA	NA	NA	NA	整備・運用	担当者のIDとパスワードでしか受注画面が開かないことを確かめる（注）シングルサインオンの場合はパスワード設定は、全般統制で確かめる。ただし、販売システムへのアクセス権限は、業務の権限と一致して設定されいることは、業務処理統制で確かめる	なし	記載省略	低
			12	得意先の与信限度を超える受注は入力できない	自動	日	NA	○	NA	NA	NA	NA	整備・運用	与信限度を超える入力ができないことを確かめる	なし	記載省略	低
			13	以下省略										以下省略			

第IV章　5．モニタリング

(1) 日常的モニタリング
(2) 独立的モニタリング (内部監査部門等による監視体制)
　① IT全社的統制のモニタリング
　② IT全般統制のモニタリング
　③ IT業務処理統制のモニタリング

まとめ

- システム管理基準等を活用している企業が、財務報告の虚偽記載に係るリスクを低減するために、「ITへの対応」を行っていくための具体的対応事例集が「システム管理基準　追補版」である。

- 重要なことは、既存のIT統制をうまく活用しつつ、リスク分析を行った上で、リスク低減が十分でない項目について、対応する管理策を検討・実施することであり、「追補版」のすべての管理策を実施することではない。

- なお、今までシステム管理基準等を利用していない企業においても、例えば、「追補版」の管理策が対応するリスクと同様のリスクが存在する場合には、当該企業におけるIT統制項目を検討する際の参考として「追補版」の管理策を利用することが可能と考えられる。

ご静聴ありがとうございました

ご質問、ご意見等は・・・

経済産業省　商務情報政策局　情報セキュリティ政策室

TEL:03-3501-0397

FAX:03-3501-6639

E-mail:kanai-hideki@meti.go.jp

URL:http://www.meti.go.jp/policy/netsecurity/index.html