内部統制における「ＩＴ統制」の整備・運用支援の視点について

～　IT全社的統制、IT全般統制、IT業務処理統制　～

特定非営利活動法人東京ITコーディネータ

内部統制支援業務の取り組み方について

1.内部統制への取組のスタンスは、その目的により2通りあります。

A：本来の意味（「会社法」の要求事項に近い）での内部統制の仕組みの構築

⇒内部統制の4つの目的にバランスよく対応する

B：「金融商品取引法」（日本版SOX法）への対応のための内部統制の整備

⇒目的を財務報告の信頼性確保に絞り込んで対応する

2.企業の置かれた立場により、A，Bの何れを狙うかを決めることになる。

①長期的な視点から、Aに取り組むケース

⇒内部統制を「やらされる」のではなく、内部統制の整備で企業価値を高めるアプローチが理想的

⇒日本版SOX法対応の必要性が無い場合はこのアプローチが良い

②当面の課題として先ずBをクリアすることを目的とし、Bから着手するケース

⇒財務報告の信頼性確保の視点からリスク分析、対応策等を絞り込んで必要最小限のものを期限までに実施する

内部統制支援業務の範囲について

1.内部統制構築の支援方法

A：内部統制全般対応のケースへの支援

・自己診断を行い、課題マップを策定する

・経営としての目標を明確にして、経営視点の構築方針を決める

・構築方針が、リスクの考え方・対象範囲・対象業務・アプローチ方法・仕組みの精粗の度合いを決めることになる

・基準としては、COSOレポート、日本版SOX法の実施基準等を参考にする

B：日本版SOX法対応のケースへの支援

・日本版SOX法の「実施基準」に準拠して内部統制の仕組みを構築し、その整備・運用の有効性を評価する

・リスクの考え方・対象範囲・対象業務・アプローチ方法についてのおよそのガイドラインが出ているので、詳細部分について各企業で判断する

2.内部統制構築業務の範囲

・4頁を参照して構築の負荷を想定し、取組の優先順位を検討する

3.内部統制の検討に当たっては、リスクの識別が重要である（5頁参照）

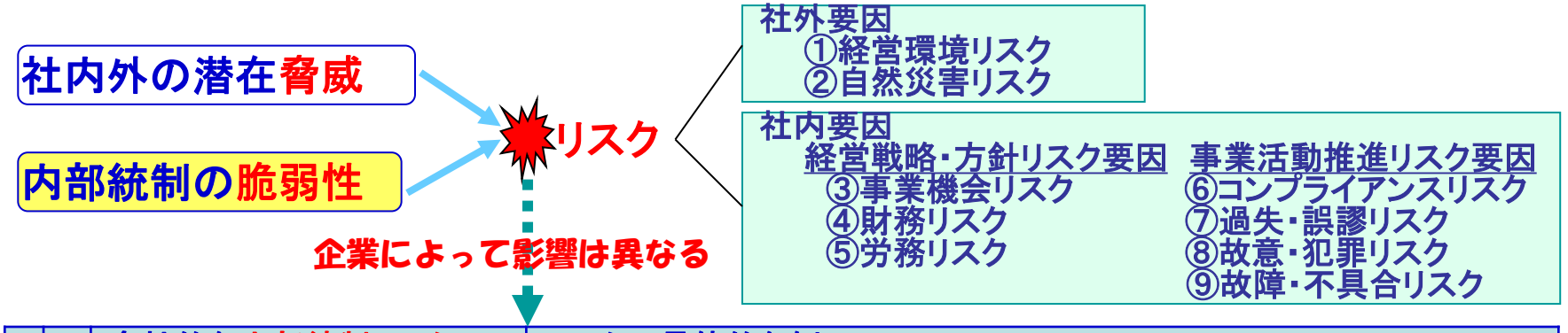
内部統制プロジェクト対象範囲

▼ 監査人確認

	1	2	3	4	5	6	7	8
	内部統制方針策定		内部統制の整備		内部統制の運用		モニタリング・監査・改善	有効性評価報告書作成
	現状分析と準備	方針決定		設計の評価		運用の評価		
全社的な内部統制	・基本的要素チェックリスト診断（実施基準） ・倫理規定・行動規範 ・経営戦略・方針・計画 ・**社内規定集** ・内部統制教育	・基本的計画・方針の策定 ・組織体制 ・評価範囲 ・取締役会・監査役会の機能化 ・PJ活動計画	・全事業拠点 ・**リスク分析** 財政・法的・依存 ・規程整備 ・組織慣行明文化 ・内部通報制度 ・内部統制マニュアル	・チェックリスト見直し ・不備の改善	・全事業拠点啓蒙 ・規程遵守教育 ・運用状況記録・保存	・業務観察 ・ヒアリング ・記録の検証 発令・議事録 ・不備の改善	・自己点検 ・内部監査 ・是正措置 ・継続的改善	・評価範囲 ・有効性判断 ・不備・重要な欠陥への対応
業務プロセスに係る 内部統制	・重要拠点 ・決算財務報告 ・主要勘定科目業務 ・財務報告影響	・対象と可視化 ・業務手続 ・権限・職責 ・作業見積 ・文書化ガイド	・主要業務プロセス ・**リスク分析** 誤謬・不正・不具合 ・文書化3点セット ・人間系とIT系	・ウォークスルーテストと改善 職務分離、内部・相互牽制	・教育と定着 ・運用状況記録・保存	・サンプリングテスト計画・実施 ・業務観察 ・記録の検証 ・不備の改善	・自己点検 ・内部監査 ・是正措置 ・継続的改善	・有効性判断 ・不備・重要な欠陥への対応
IT業務処理統制	・業務処理システム機能体系	IT処理 ①入力チェック ②エラー対応 ③マスタ照合 ④アクセス管理	・**リスク分析**‥データのITコントロール目標 ・EUC統制 ・RCM	・仕様書の検証 ・不備の改善	・運用状況記録・保存	・サンプリングテスト計画・実施 ・記録の検証 ・EUC統制評価 ・不備の改善	・自己点検 ・内部監査 ・是正措置 ・継続的改善	・有効性判断 ・不備・重要な欠陥への対応
IT全般統制 IT基盤別の内部統制	・チェックリスト診断 ・インフラ説明図	IT手続 ①開発・保守 ②運用・管理 ③安全性確保 ④委託契約管理	・**リスク分析**‥処理のITコントロール目標 ・文書化3点セット ・アウトソーシング	・ウォークスルーテストと改善 変更管理 安全管理 委託先管理	・教育と定着 ・委託先評価 ・運用状況記録・保存 アクセス権	・サンプリングテスト計画・実施 ・記録の検証 ・不備の改善	・自己点検 ・内部監査 ・是正措置 ・継続的改善	・有効性判断 ・不備・重要な欠陥への対応
IT基盤共通の統制環境	・チェックリスト診断 ・IT部門規程 ・IT環境理解 ・システム体系図 ・セキュリティルール	・IT化戦略・方針・計画の確認 ・IT関係組織体制 ・IT関係規程体系	・**リスク分析** ITガバナンス・法的 ・ IT部門規程 開発・保守・運用 ・IT利用規程 ・セキュリティ規程	・不備の改善	・IT部門教育 申請・承認制度 ・IT利用者教育	・運営ルール遵守状況 ・利用ルール遵守状況 ・不備の改善	・自己点検 ・内部監査 ・是正措置 ・継続的改善	・有効性判断 ・不備・重要な欠陥への対応

バイロット部門・プロセス ⇒ 全社展開

内部統制に影響を与えるリスク



		全社的な内部統制リスクの種類	リスクの具体的な例 特に、*財務報告の信頼性に影響を与えるリスクの例*
社外要因	①	**経済的・社会的異変の打撃**	オイルショック、大停電、***株価暴落***、***為替変動***、***金利変動***、***資源相場変動***などの影響
		国際的・政治的異変の打撃	戦争、政変、貿易摩擦、カントリーリスクなどの経営への影響
	②	自然災害・疾病の打撃	地震、風水害、火災、伝染病などの経営への影響
戦略・方針	③	商品開発失敗、リコール、PL訴訟	製品設計ミス（破損、健康障害）、製造ミス（破損、異物混入）など
	④	**資金的異変の打撃**	***資金不足***、***取引先倒産***などの影響
	⑤	**人事・労務上のトラブル・問題**	不明瞭な評価、不当異動、***従業員の犯罪・不祥事***、労働争議、職業病、過労死、
事業活動推進リスク要因	⑥	**法令違反・虚偽報告**	***違法行為***（独禁法、下請法、税法、商法、金商法など）、***不適正な適用***
	⑦	**経営上・業務上の不祥事**	***不正行為***、***情報漏洩***、反社会的行為、スキャンダル、内紛、M&Aなど
		経営上・業務上の判断ミス	***投資・融資・債権・取引リスク***、契約不備、***会計処理の誤謬***、***特定先依存***など
		事業の過失	環境汚染（土壌、排水、臭気など）、労働災害（安全衛生、事故）など
	⑧	企業脅迫・企業への悪意の犯行	異物混入など嫌がらせ、強盗、盗難、破壊活動な どによる被害
		経営不安説による株価暴落の打撃	マスコミの誤報、風説の流布、ネット上の風説等の経営への影響
	⑨	**情報システムのトラブル**	***情報システム故障・不具合、セキュリティ問題***

「ＩＴ統制」への取り組み方について

1.IT統制の位置づけについては次頁参照

2.IT統制構築の支援方法

Ａ：一般的な内部統制対応のケースにおける支援方法

・経営としての「ITガバナンス目標」を明確にして、取り組み方針を決める

・取り組み方針によって、ITに係るリスクの考え方・対象範囲・対象業務・アプローチ方法・精粗の度合いを決めることになる

・基準としては、COBITforSOX、システム管理基準追補版等を参考にする

Ｂ：日本版SOX法対応のケースにおける支援方法

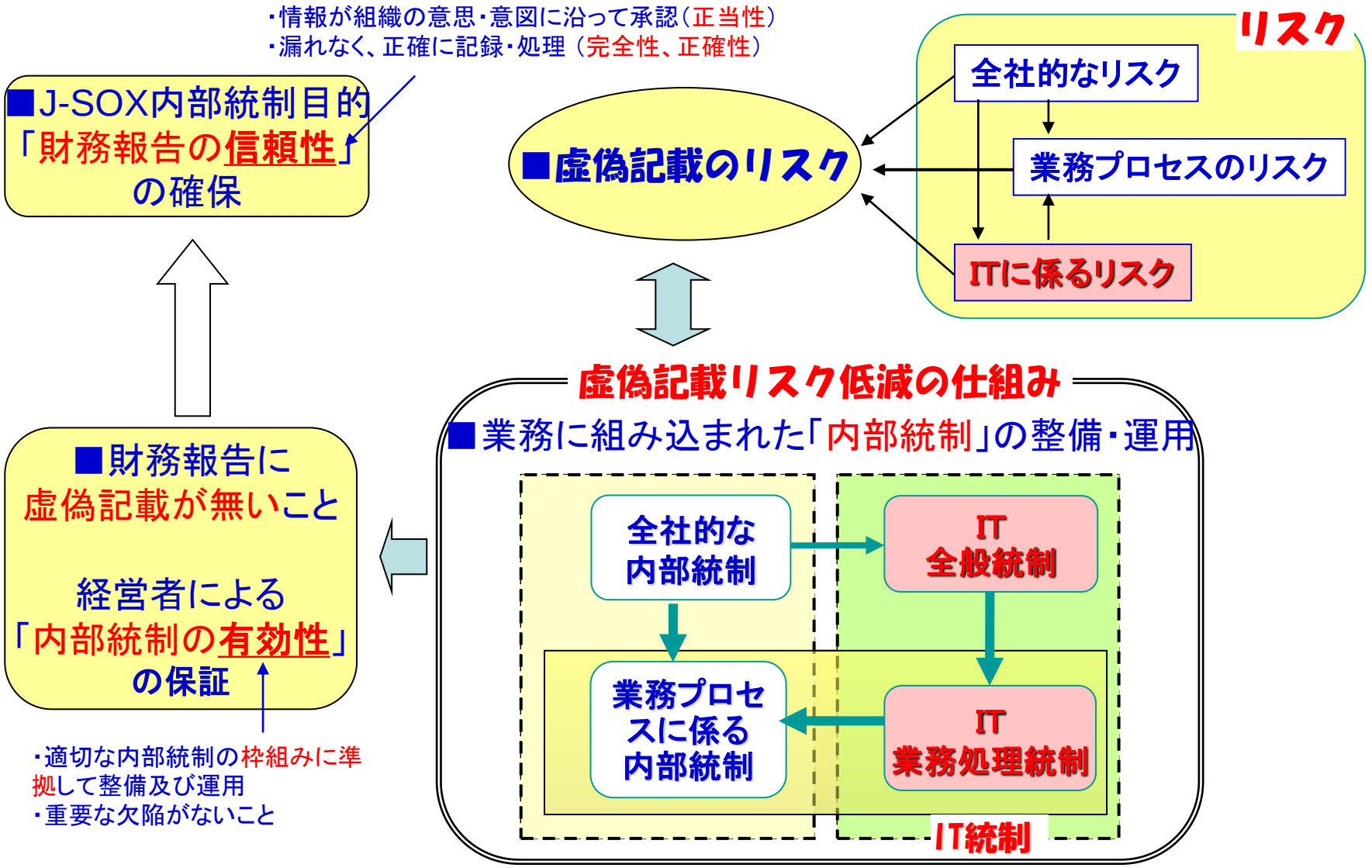
・日本版SOX法の「実施基準」におけるIT統制の要求事項を勘案して仕組みを構築し、その整備・運用を支援する

・IT統制についてのリスクの考え方・対象範囲・アプローチ方法についての詳細は実施基準では明確で無いので、COBITforSOX、システム管理基準追補版等を参考にする

3.IT統制業務の範囲例

・日本版SOX法の「実施基準」におけるIT統制の概要を以下に示す

内部統制における「ＩＴ統制」の位置づけ



「ＩＴへの対応」と「ＩＴ統制」

ITへの対応

・内部統制の6番目の「**基本的要素**」
・予め適切な方針及び手続を定め、業務実施において**組織内外のITに対し適切に対応すること。**
・業務内容や情報システムがITに高度に依存している場合には、内部統制の目的を達成するために不可欠の要素として「**内部統制の有効性に係る判断の規準**」となる。

IT環境への対応（経営者による理解）

a.社会及び市場における**ITの浸透度**
b.組織が行う取引等における**ITの利用状況**
c.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**
d.ITを利用した**情報システムの安定度**
e.**外部委託の状況**

ITの利用及び統制

ITの利用（ITによる統制）

a.統制環境の*有効性を確保するためのITの利用*
(ア) 経営者のITに対する関心、考え方
(イ) ITに関する戦略、計画、予算等の策定及び体制の整備
(ウ) 組織の構成員のITに関する基本的な知識や活用する能力
(エ) ITに係る教育、研修に関する方針
b.リスクの評価と対応の*有効性を確保するためのITの利用*
c.統制活動の　〃
d.情報の伝達の　〃
e.モニタリングの　〃

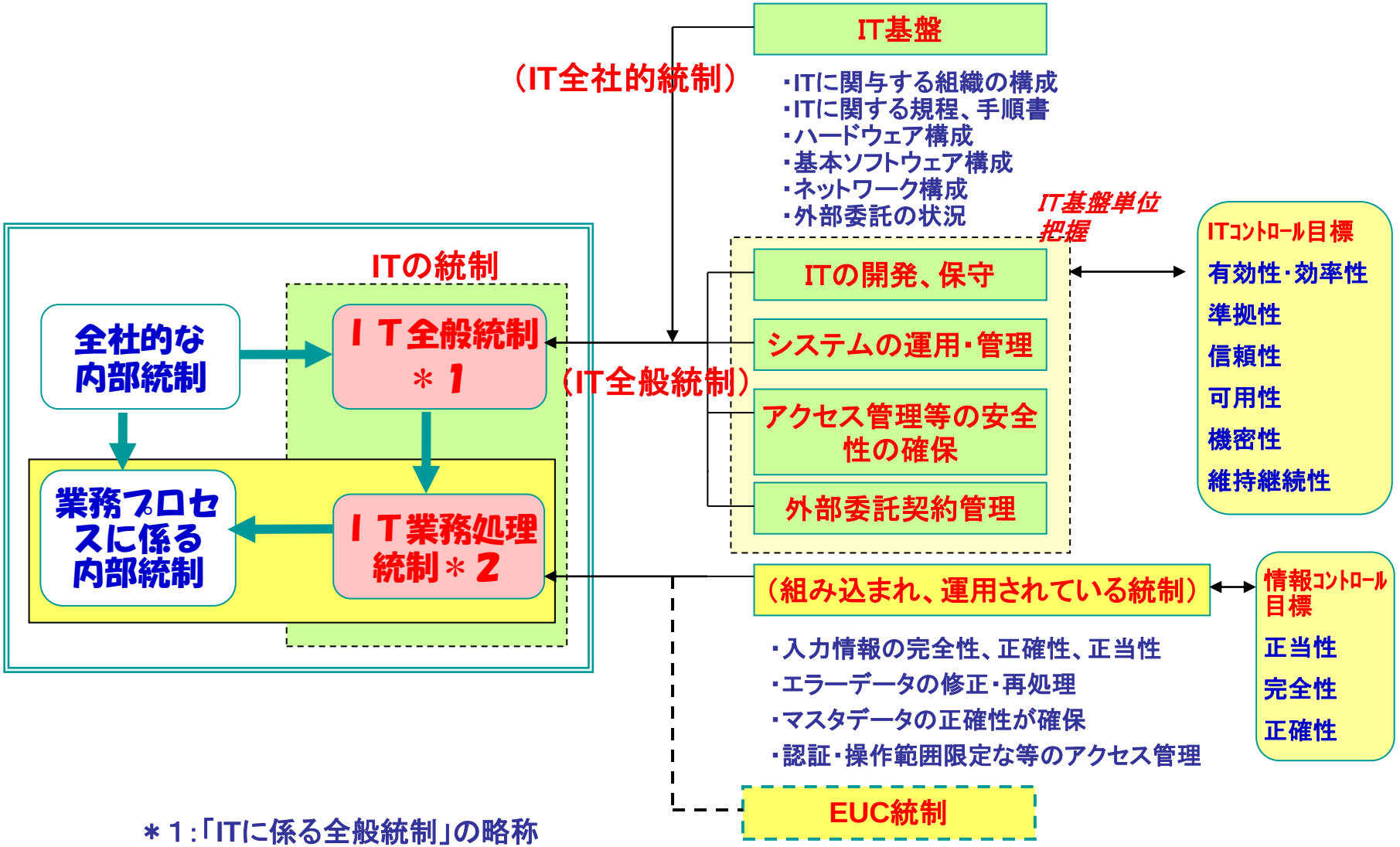
ITの統制（ITに対する統制）

a.「自動化された統制」と「手作業による統制」
b.組織目標を達成するための「ITの統制目標」
(ア) 有効性及び効率性
(イ) 準拠性
(ウ) 信頼性（正当性、完全性、正確性）
(エ) 可用性
(オ) 機密性

IT全般統制

IT業務統制

「ＩＴ統制」の仕組みの概要



＊１:「ITに係る全般統制」の略称
＊２:「ITに係る業務処理統制」の略称

「ＩＴ全社的～ＩＴ全般統制」の整備

・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
　「有効性･効率性、準拠性、可用性、機密性、維持継続性」の確保
・システムを支援するIT基盤（ハード、ソフト、ネットワーク等）を単位として構築

ＩＴ統制への協業方法について

1.IT統制の2つの視点からの専門的支援が可能

（1）マネジメントシステムとしてのアプローチ⇒弊NPO担当

・ITガバナンスの視点から、当該企業の方針・業務レベル・ITレベルに適合したマネジメントシステムを設計・構築・運用を支援する

（2）技術インフラ面からのアプローチ⇒貴社担当

・ITインフラ整備方針に基づき、その方針を実現するための最適のツールを選定して導入し、その効果的な使用をコンサルティングする

2.IT統制業務の協業分野

（1）マネジメントシステムの診断機能、監査機能の支援

（2）マネジメントシステムの整備・運用・評価機能の支援

（3）技術インフラ面からの診断機能、監査機能の支援

（4）技術インフラ面からの整備・運用・評価機能の支援

「ＩＴ統制」に関わる協業の内容

業務 サービス	IT全般統制		IT業務処理統制
	IT全社的統制 （IT基盤共通）	IT全般統制 （IT基盤単位）	
① IT統制診断 現状診断	チェックリストによる診断と提案	チェックリストによる診断と提案	チェックリストによる診断と提案
②IT統制整備支援 整備状況の評価と改善支援	リスク評価 IT方針・IT部門規程・ツール等の整備 IT資産管理	リスク評価 手順書等の整備 RCM等作成と検証	リスク評価 仕様書整備 業務プロセスRCM等作成・検証
③IT統制運用支援 運用状況の評価と改善支援	運用ルール設計・ツール導入 （教育と運用指導） 自己点検チェックリストによる運用状況確認		サンプリングテスト 自己点検チェックリスト運用状況確認
④IT統制監査支援 内部監査と有効性評価の支援	内部監査と有効性評価		業務プロセスに係る内部統制については別途

「ＩＴ統制」の整備の進め方

		IT統制		
		IT全社的統制	IT全般統制	IT業務処理統制
財務報告の信頼性確保に係る統制	ITによる統制		□稼働状況・運用管理モニタリング □システム利用状況ログ管理 □アクセスログ管理 □電磁媒体管理	□下記システムの入力チェック、エラーデータ処理 ・会計情報システム ・会計情報システムに繋がる業務システム □マスターの正確性確保 □アクセス権管理
	ITによらない人間系統制	□IT戦略、IT方針、IT計画書 □情報セキュリティポリシ、規程 □IT部門組織、役割責任分担 □会計関連・システム化計画書 □IT利用規程	□IT開発規程 □IT変更管理規程 □IT運用規程 □委託先管理規程 □安全管理規程	□上記システム各種仕様書 □上記システム運用・操作マニュアル □アクセス権申請承認制度 □EUC管理規程
財務報告の信頼性確保に直接的には関わらない統制	ITによる統制	□グループウェア、メール管理	□サーバログ管理 □端末アクセス管理	□端末操作モニタリング
	ITによらない人間系統制	□IT部門規程 □IT投資・調達規程 □IT化計画書、予算 □IT資産管理台帳	□IT基盤保守計画	□伝票照合作業等