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）

令和６年12月25日

経済産業省

システム管理基準追補版改訂作業部会　名簿

【座長】

島田　裕次	東洋大学工業技術研究所 客員研究員、システム監査学会 会長

【委員】

安部　靖雄	公認会計士、日本公認会計士協会テクノロジー委員会 監査IT対応専門委員会 専門委員長
神崎　時男	公認会計士、公認情報システム監査人、日本公認会計士協会中小事務所IT対応支援専門委員会 委員
小池　聖一・パウロ	千葉商科大学会計大学院 教授、公認会計士、公認内部監査人、公認情報システム監査人
小林　尚明	公認会計士、日本公認会計士協会 常務理事
紫垣　昌利	公認会計士、日本公認会計士協会テクノロジー委員会委員長
中村　元彦	千葉商科大学会計大学院 教授、システム監査学会 常任理事
三木　孝則	公認会計士、公認情報システム監査人
宮城　潤	公認システム監査人、システム監査学会 会員
山口　達也	公認システム監査人、日本システム監査人協会 副会長
吉武　一	公認内部監査人、公認情報システム監査人、日本内部監査協会 理事

（五十音順・敬称略）

目次

コラム	・ ITガバナンス、ITマネジメントとIT全社的統制との関連に関する考え方の整理	Ⅱ章P10
	・ 非財務情報への言及・「財務報告」から「報告」への変更	Ⅱ章P15
	・ アジャイル/スパイラル開発手法について	Ⅱ章P19
	・ AI導入での留意点	Ⅱ章P20
	・ 全社員デジタル人材化に伴うリスク	Ⅳ章P10
	・ サイバーセキュリティ	Ⅳ章P34
	・ 外部委託	Ⅳ章P41
	・ IT業務処理統制について	Ⅳ章P50

まえがき

平成18年6月に成立した「金融商品取引法」によって、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、報告することが上場企業に義務付けられました（内部統制報告制度）。また、ITの急速な普及に伴って、調達・製造・販売・物流といった基幹業務から、財務・人事・給与等の管理業務に至るまで、様々な業務においてITへの依存度が増大していることから、財務報告に係る内部統制において、「ITへの対応」が求められるようになりました。

内部統制報告制度については、平成20年に適用されて以来、15年余りが経過し、内部統制報告制度を巡る状況の変化を踏まえて、内部統制の実効性向上を図る観点から審議・検討を行って、令和５年４月７日に「財務報告に係る内部統制の評価及び監査の基準並びに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の改訂について（意見書）」[1]（以下「意見書」という。）が公表されました。

ところで、「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）」（以下「追補版」という。）は、経済産業省が策定・公表しているシステム管理基準及びシステム監査基準（以下「システム管理基準等」という。）に基づいて構築されている情報システムを活用し、財務報告に係る内部統制で求められている「ITへの対応」を行っている、又は行うとしている企業において、「システム管理基準等」と「ITへの対応」との間の具体的な対応関係を明らかにするために策定し、平成19年３月30日に公表したものです。

「システム管理基準等」では、財務報告に係る内部統制における「ITへの対応」の整備・運用・評価について詳細まで言及していないこと等から、「システム管理基準等」を活用している企業が、財務報告に係る内部統制で求められている「ITへの対応」を行いやすくするために、「システム管理基準等」と「ITへの対応」との間の具体的な対応関係を明らかにするようにしました。また、「システム管理基準等」と意見書を念頭に、主要なケースを想定しつつ、「ITへの対応」に関する概念、経営者評価等を提供することを目指しました。追補版が参照している「システム管理基準等」は、情報通信技術の進展などを踏まえて、令和５年４月26日に改訂されたところです。また、同様に追補版が参照している意見書が公表されたことから、追補版の内容を見直すことが必要になりました。

経済産業省では、有識者で構成される検討会を開催して、「システム管理基準等」及び意見書の改訂部分と旧追補版との差異を点検し、整合がとれた追補版になるように改訂作業を行いました。

[1] 「財務報告に係る内部統制の評価及び監査の基準並びに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の改訂について（意見書）（令和５年４月７日企業会計審議会）」

具体的には、ITシステムの戦略的利活用が、組織体の価値の向上や企業の競争力の維持、向上を図る上で不可欠となっていることに加え、デジタル・トランスフォーメーション（DX）の普及やサイバー攻撃の高度化・複雑化等による新たなリスクの発生等により、システム・マネジメントの基となるガバナンスの重要性がより一層増加していることを考慮しました。また、海外市場の取込み、コア事業の競争力強化や新たな成長分野の獲得などのため、グローバル化や事業再編が進み、子会社管理を含めたグループ経営を行う企業においてグループ全体の企業価値向上を図るためのグループガバナンスの重要性も高まるとともに、ESG（環境・社会・ガバナンス）投資への注目への高まりに伴い、財務情報に加え、サステナビリティ情報も重要視され、その開示の要請についても高まりつつあることにも配慮しました。

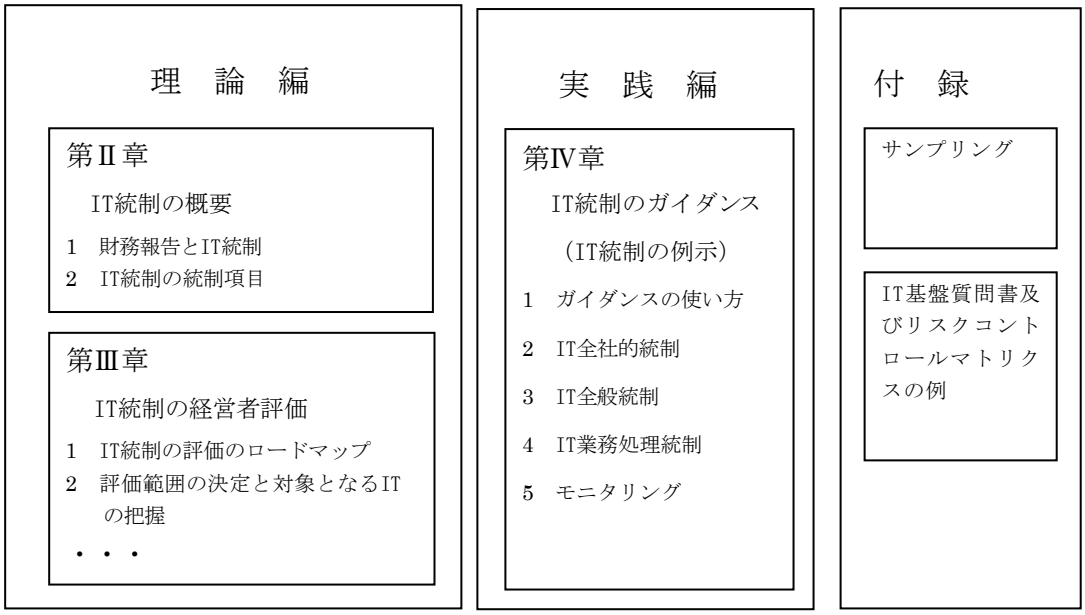
なお、追補版が提供するものは、あくまでも、主要なケースを想定した参考情報であり、それぞれの企業が「ITへの対応」をどのように実施し、経営者がその有効性をどのように評価するのかについては、個々の企業の事業内容や組織構造等によって、様々なケースが存在し得ることはいうまでもありません。

したがって、企業においては、第Ⅳ章の「IT統制のガイダンス」に挙げている項目をそのまま適用するのではなく、本追補版の第Ⅱ章及び第Ⅲ章で示している項目の整備・運用と評価に関する考え方を十分に理解し、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対応を行ってください。その際に、ガイダンスに挙げている項目をそのまま実施するのではなく、当該項目が想定しているリスクの大きさを踏まえて実施することが重要である点に留意してください。

第Ⅰ章 本追補版の構成と用語について

１．構成

本追補版は、「第Ⅱ章　IT統制の概要」「第Ⅲ章　IT統制の経営者評価」「第Ⅳ章　IT統制のガイダンス（IT統制の例示）」「付録」から構成されている。



第Ⅱ章は、財務報告とIT統制との関係、IT統制の意義・種類等、IT統制の基本的な概念について説明している。第Ⅲ章では、財務報告に係る内部統制の経営者による評価においてIT統制をいかに評価すべきか、そのポイントを説明している。この２つの章は、本追補版のいわば理論編に相当するもので、IT統制についての基本的な枠組みを提供するものである。

第Ⅳ章は、IT統制を構築し、評価するためのガイダンスであって、全社的な内部統制（以下「全社的統制」という。）、全般統制、業務処理統制ごとに、IT統制を例示している。また、それぞれのIT統制項目ごとに、「統制に関する指針」「統制目標の例」「統制の例と統制評価手続の例」を示すことによって、IT統制を導入、評価する場合のガイダンスとしている。

なお、この「第Ⅳ章　IT統制のガイダンス」は、専門家の経験に基づく例示であり、ベストプラクティスを示したものではない。各企業の状況や特性、更にはリスクの程度に応じて、当ガイダンスの内容を選択し、又は不足分を補って、企業ごとに適切なIT統制となるよう期待したい。

2. 用語

以下は、金融庁が公表している「財務報告に係る内部統制の評価及び監査の基準並びに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」（以下「実施基準」という。）と経済産業省が公表している「システム管理基準」の用語の定義が異なるため、その使用による混乱を避けるために簡単な解説を加えたものである。

●情報システムの範囲

「実施基準」では、情報システムとは、「手作業によるか、機械化された情報システムによるかにかかわらず、情報を処理及び伝達するための仕組みをいい、情報システムに取り入れられた情報は、分類、整理、選択、演算など、目的に応じて加工される（処理）」（⇒*（実施基準　Ⅰ．２（４）①）*）と説明され、ITを利用した情報システムと手作業によるものとを含めて捉えている。しかし、本追補版では、情報システムを「ITを利用し、情報を分類、整理、選択、演算等、目的に応じて加工するための機能のこと」とする。

●IT 統制の概念

「実施基準」では、「ITへの対応」について、①「IT環境への対応」、②「ITの利用」、③「ITの統制」と３つに分け、「ITの統制」を「情報技術を利用した情報システムに対する統制」と捉えている。本追補版では、③「ITの統制」を「IT統制」と呼ぶ。

①IT環境への対応	社内外のITの活用状況の考慮
②ITの利用[2]	財務情報の信頼性に係る内部統制の実現におけるITの利用 （例：アクセス制御機能による財務情報へのアクセス制限）
③ITの統制	ITを利用した情報システムに対する内部統制 （例：アクセス制御機能による財務情報へのアクセス制限を有効に機能させるためのID、パスワードの管理）

●「IT全社的統制」、「IT全般統制」及び「IT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。

[2] システム管理基準では「ITシステムの利活用」としているが、本追補版は過去との整合性を鑑みてITの利用としている。

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。
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、承認された業務が全て正確に処理、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)*

(ア) IT の統制目標としての財務情報の信頼性

「実施基準」では、財務情報の信頼性確保という内部統制の目標が列挙されていて、信頼性や完全性について述べられているが、下表に示すように、一般的な情報システム分野で広く使われている用語と定義が一致していない。本追補版では、「信頼性」及び「完全性」については、実施基準の定義に合わせる。

用語	実施基準	情報セキュリティ分野
信頼性	情報が組織の意思・意図に沿って承認され、漏れなく正確に記録・処理されること（正当性、正確性、完全性）。 ⇒ *(実施基準 Ⅰ．２（6）②〔ITの統制〕 イb)*	意図する行動と結果とが一貫している特性 ⇒ *(JIS Q27000)*
完全性	記録した取引に漏れ、重複がないこと。 ⇒ *(実施基準 Ⅰ．２（6）②〔ITの統制〕 イ)*	資産の正確さ及び完全さを保護する特性 ⇒ *(JIS Q27001、3.8)*

(イ) IT基盤の概念

「実施基準」では「IT基盤」という用語が登場するが、明確な定義がされていない。そこで、本追補版では、IT基盤を「ITに関与する組織の構成、ITに関する規程及び手順書等、ハードウェアの構成、ソフトウェアの構成、ネットワークの構成、関連する外部委託」と解釈する。

●情報システムの開発と保守

「システム管理基準」では、情報システムに対する「開発」と「保守」を分けている。開発とは情報システムの構成要素の開発のことをいい、保守とは情報システムの能力・機能の維持・更新のことをいう。一方、「実施基準」では、保守は開発に含まれて分類さ

れている。そのため、本追補版においても、「実施基準」との整合性の観点から、開発と保守を合わせて扱うこととする。また、「システム管理基準」では、情報システムの構成要素の変更などの変更管理も扱われているところ、本追補版ではそれを「変更管理」として扱っている。

●財務報告及び財務情報とIT統制

ITには、決算・財務報告（⇒*（実施基準 Ⅱ．１（１））*）に係る業務プロセス（⇒*（実施基準 Ⅱ．２（２））*）に直接係るITと、直接係らないITの２種類がある。前者は、例えば、会計システム等であり、後者は、受注システム等である。特に、財務報告に至る情報の流れを財務情報という。各種の業務プロセスで財務情報が仕訳され集計されて、最終的には財務報告につながる。したがって、IT統制は、財務報告に係るITに適用されて、改ざんや不正がないことを保証する。

（ウ）IT統制を実施する関係者

本追補版では、財務情報に係るIT基盤、アプリケーション・システム等を開発、運用管理するために、さまざまな関係者が登場する。これを以下に示す。

経営者	組織の全ての活動について最終的な責任を有しており、その一環として、取締役会が決定した基本方針に基づき内部統制を整備及び運用する役割と責任がある（代表取締役、代表執行役等）。⇒*（実施基準Ⅰ．４（１））* なお、システム管理基準においては、昨今のコーポレートガバナンスの考え方に基づき、「ガバナンス＝取締役会等」「マネジメント＝経営者/最高情報責任者（CIO）やシステム担当役員」を区別したモデルを想定している。そしてITガバナンスを有効に機能させるためにはITガバナンスとITマネジメントの橋渡し役が必要であり、ISO/IEC TS38501においてガバナンスとマネジメントの両方に責任を持つ組織として「ガバナンス運営グループ」を設定している。本追補版における「経営者」は、システム管理基準におけるこの「ガバナンス運営グループ」を想定することが概念としては最も近いものになると考えられる。
最高情報責任者(CIO)	企業内のITに関する最高責任者 システム管理基準においては、原則としてマネジメントに当たる役割であるが、「ガバナンス運営グループ」の構成メンバーでもあることから、ガバナンスにも責任を持つ立場として捉えることができる。
責任者	担当者への指示や統制を実施する責任を持つ。システム開発責任者、運用責任者、受入テスト責任者等
担当者	責任者により、財務情報を扱う権限を付与された者

運用担当者	IT基盤の運用担当者、実際のアプリケーション・システムの入力、出力等の実施者
開発者	情報システムのプログラム開発をする担当者、責任者（財務情報システムへのアクセスはできない。）

●管理項目と統制項目

「システム管理基準」や「情報セキュリティ管理基準」では、リスクを低減するための対策を「管理活動」や「管理策」と呼ぶが、本追補版では、「財務情報に係るIT統制」の視点から、「統制項目」と呼ぶことがある。

3. 参考となる他の基準等

（1）システム管理基準（経済産業省、令和５年４月26日改訂）
https://www.meti.go.jp/policy/netsecurity/sys-kansa/sys-kanri-2023.pdf

（2）情報セキュリティ管理基準（経済産業省、平成28年改正版）
https://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Management_Standard_H28.pdf

（3） 情報システム・モデル取引・契約書（受託開発（一部企画を含む）、保守運用）第二版（独立行政法人情報処理推進機構）

（4） 財務報告に係る内部統制の評価及び監査の基準並びに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の改訂について（意見書）（金融庁企業会計審議会、令和5年4月7日）
https://www.fsa.go.jp/news/r4/sonota/20230407/1.pdf

（5）システム管理基準ガイドライン（特定非営利活動法人日本システム監査人協会）[3]
https://gl.systemkansa.org/

（6）監査基準報告書315「重要な虚偽表示リスクの識別と評価」
https://jicpa.or.jp/specialized_field/publication/kansa/#anchor-01

（7） 監査基準報告書315実務ガイダンス第１号「ITの利用の理解並びにITの利用から生じるリスクの識別及び対応に関する監査人の手続に係るQ&A（実務ガイダンス）」
https://jicpa.or.jp/specialized_field/publication/kansa/#anchor-03

（8）財務報告内部統制監査基準報告書第１号研究文書第１号「内部統制報告制度の運用の実効性の確保に係る研究文書」
https://jicpa.or.jp/specialized_field/publication/kansa/#anchor-05

[3] システム管理基準ガイドラインは、迅速なアップデートを可能とするために、民間団体である特定非営利活動法人日本システム監査人協会が策定し公表することとされている。

第Ⅱ章　IT統制の概要

本章では、まず、財務報告とIT統制の関係を１節で述べ、IT統制の統制項目について２節で述べる。

１．財務報告とIT統制

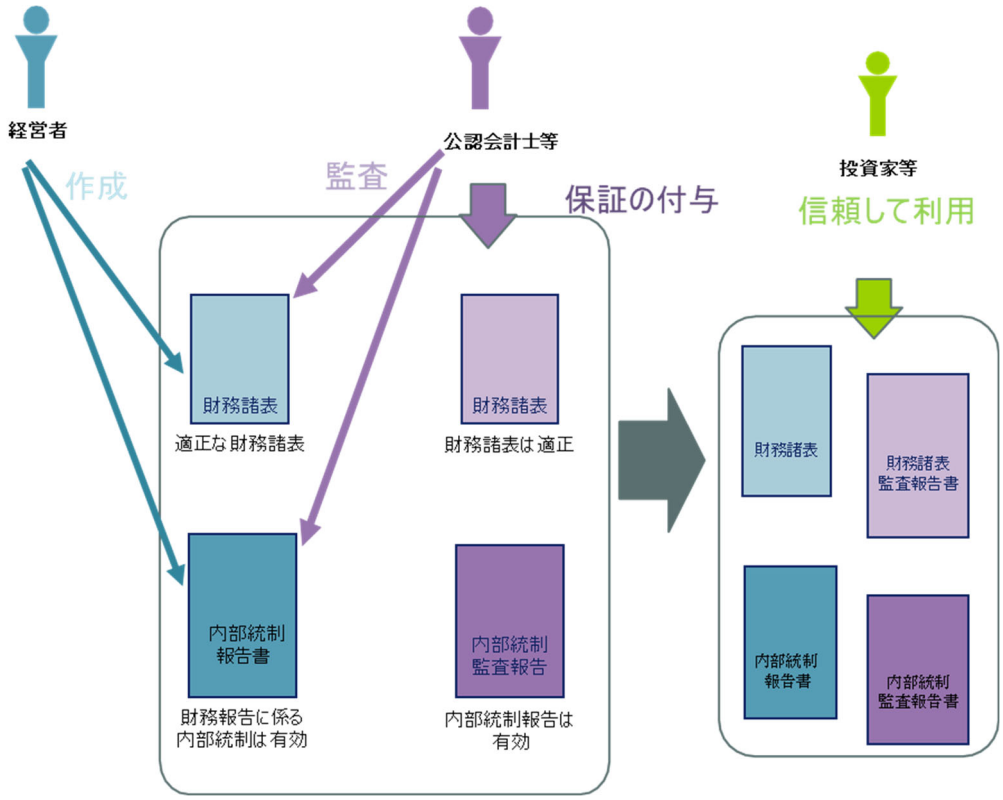
（１）　金融商品取引法で求められている内部統制とITの関係

①　財務報告と内部統制報告書

金融商品取引法第24条の４の４では、有価証券報告書提出会社のうち上場企業等に、事業年度ごとに、当該会社の属する企業集団及び当該会社に係る財務計算に関する書類その他の情報の適正性を確保するために必要なものとして内閣府令で定める体制（以下「財務報告に係る内部統制」という。）について、内閣府令で定めるところにより評価した報告書（以下「内部統制報告書」という。）を内閣総理大臣に提出することを要求している。また、内部統制報告書は、公認会計士又は監査法人（以下「公認会計士等」という。）による監査を受けなければならないと要求している。つまり、金融商品取引法では、有価証券報告書提出会社に対して財務報告の信頼性を確保するための内部統制の評価及びその報告が義務付けられ、更にその内容の信頼性を担保するために公認会計士等の監査を受けることが義務付けられている。

この制度を従来の、財務諸表の作成及びその監査の制度とあわせて図示すると図表Ⅱ.１－１のとおりとなる。

図表Ⅱ．１－１　連結財務諸表/財務諸表監査と内部統制監査について



財務報告を含む報告の信頼性を確保するためには、財務報告に関係する財務情報を識別、把握、処理及び伝達するための会計システムが存在し、あらかじめ適切な方針及び手続を定める等、それが適切に統制されていなければならない。このような会計システムには業務の効率性及び有効性の観点からITが利用されることが多い。一方、会計システムで利用するITにおいても、財務情報が適切に統制され、結果としての財務報告の信頼性が確保されるように統制機能が必須となる。

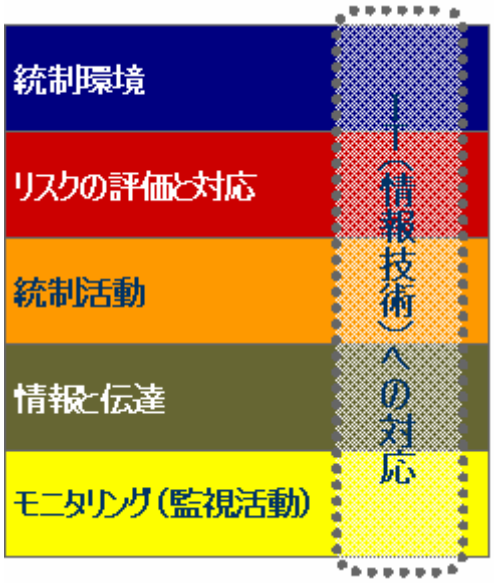
②　内部統制の基本的要素とIT

このような背景も踏まえて「実施基準」の内部統制の基本的枠組みでは、内部統制の基本的要素として、ITへの対応を加えている。

基本的要素は、内部統制の目的を達成するために必要とされる内部統制を構成する要素である。内部統制が有効であると主張するためには、全ての基本的要素が存在し、有効に機能している必要がある。ただし、ITへの対応は必須ではなく、他の５つの基本的要素についてITを利用している場合に基本的要素となる。ITを利用していなくても有効な内部統制は存在しうる。

なお、ITへの対応を評価する場合、ITへの対応は他の５つの基本的要素と独立して存在するものではないため、図表Ⅱ．１－２のように他の５つの基本的要素と一体となって評価することになる。

図表Ⅱ．１－２　実施基準の内部統制とITとの関係



ITへの対応は、IT環境への対応、ITの利用、IT統制から構成される。さらに、IT統制は、IT全社的統制、IT全般統制、IT業務処理統制に区分される。また、内部統制を構成する５つの基本的要素はそれぞれのIT統制と関係するが、本追補版においては、全社に共通する事項をIT全社的統制で説明している。なお、全体を統制するという観点から、モニタリングを独立して説明している。

（２）　財務報告とIT統制の関係

①　企業におけるIT統制の枠組み

システム管理基準を利用して自社の情報システムのIT統制を整備・運用している企業におけるIT統制の枠組みはITガバナンスとITマネジメントで構成されることになる。

ITガバナンスの定義

ITガバナンスとは、組織体のガバナンスの構成要素で、取締役会等がステークホルダーのニーズに基づき、組織体の価値及び組織体への信頼を向上させるために、組織体におけるITシステムの利活用のあるべき姿を示すIT戦略と方針の策定及びその実現のための活動である。⇒*（システム管理基準　前文）*

ITガバナンスとITマネジメントの関係

経営者は、取締役会等が設定したITガバナンスの方針と戦略に基づいて目標を達成する実行責任と取締役会等に対する説明責任を負っている。そこで、経営者は、経営方針及びITガバナンス方針に基づいて策定したIT戦略の各目標を達成するために、ITシステムの利活用に関するコントロールを実行し、その結果としてのパフォーマンス、コスト管理、リスク管理、コンプライアンス管理、社会的責任と持続性等の状況を経営者に報告するための体制を整備・運用することが必要となる。

IT戦略の策定及び取締役会等から経営者に対して指示する事項については、ITガバナンス編に記載しており、ITマネジメント編では、これらに基づいてITシステムの利活用に関する統制を実行するための達成目標と管理活動の例を記載している。⇒*（システム管理基準　前文）*

システム管理基準は、昨今のDX推進の流れ等を踏まえ、経営戦略策定等も含めたより包括的なIT利活用を想定した内容となっている。そのためその全ての要求事項を財務報告におけるIT統制で考慮する必要はなく、ITに係る内部統制の整備・運用に関連する部分を参考にすることが必要となる。

また、システム管理基準を参照する場合は、実施基準におけるIT統制の枠組み（IT全社的統制・IT全般統制・IT業務処理統制）とシステム管理基準における枠組み（ITガバナンス・ITマネジメント）の関係を次のように整理しておくとよい。

【IT全社的統制の定義（システム管理基準との関係）】

IT全社的統制とは、システム管理基準におけるITガバナンスの中で、特に内部統制整備・運用に関する方針・資源配分・モニタリングと、ITマネジメントの中で、全社レベルでの統制整備が必要となるプロセス（推進・管理体制等）を対象とした統制である。

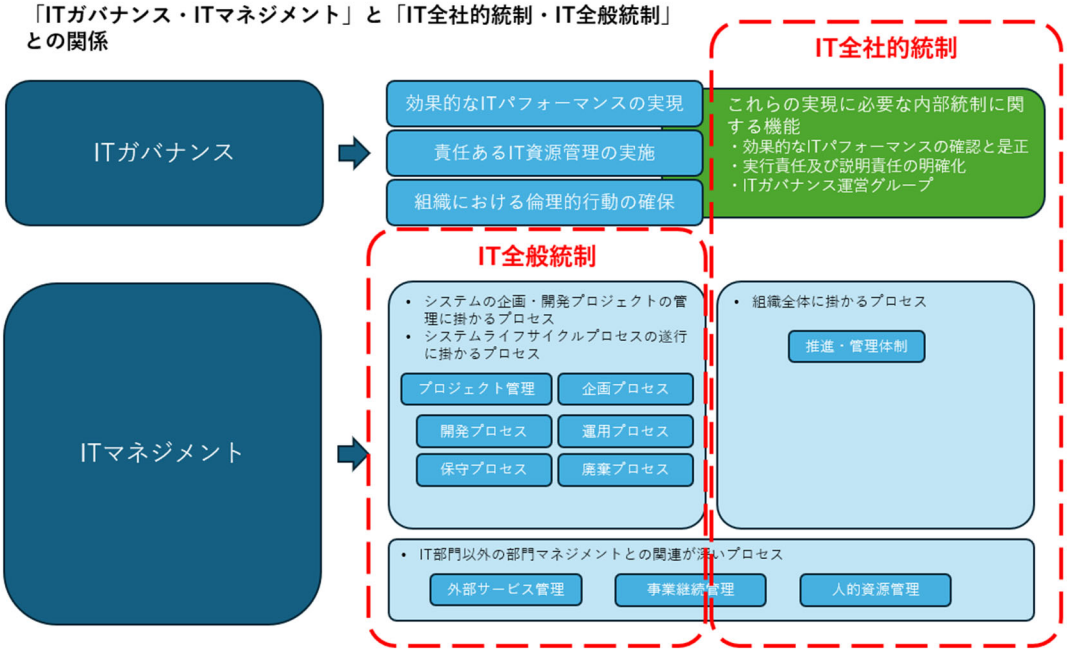
【IT全般統制の定義（システム管理基準との関係）】

ITマネジメントにおけるプロジェクト管理、企画プロセス、開発プロセス、運用プロセス、保守プロセス、廃棄プロセスは、原則システム環境ごとに設定されるものでありIT全般統制として区別される。また、外部サービス管理、事業継続管理、人的資源管理については、方針策定部分は全社的統制、対策実施部分は全般統制として区分する。

なお、プロジェクト管理等は、全社共通の統制によって管理する企業があるが、この場合は全社共通であることを以って全社的統制とするのではなく、IT基盤が１つである場合の全般統制として識別する。

<<コラム：ITガバナンス、ITマネジメントとIT全社的統制との関連に関する考え方の整理>>

- 令和５年改訂のシステム管理基準においては、IT ガバナンスと IT マネジメントの位置付け、目的、担うべき者（取締役、執行役員、部長等）がある程度整理されてきた。
- この中で、IT ガバナンスは DX 推進等の昨今のトレンドに合わせ、よりビジネス・経営の根幹に関わる分野として認識され、経営戦略を決定する際の重要な要素の１つとして認識された。そのため、戦略策定自体についても、ステークホルダーとの関連や、検討のための組織、リソース確保、倫理行動の確保等、いくつかの要素が定義されている。
- また、IT ガバナンスと IT マネジメントがより実態に即した区分（日本における現状＝代表取締役社長の存在を踏まえたガバナンス運営グループ[4]の設定）がされており、ガバナンスとマネジメントの有機的な連携の可視化も進展している。
- こういった状況と従来から内部統制監査の一環として定義されている IT 全社的統制を改めて比較した場合、例えば以下のような関係が考えられる。



- IT ガバナンス自体は企業の経営戦略の一部として、内部統制以外の領域も含め対応が必要とされている。一方、財務諸表監査においては、あくまでも内部統制が全社的に整備・運用されるための基盤部分を対象とすればよく、IT ガバナンス全体を対象とする必要はない。
  ガバナンス領域の内部統制に実際に必要になると思われるものとしては、基本原則にあるオーバーサイトとアカウンタビリティに関する仕組み（プロセス）と、ガバナンス・マネジメント間の情報連携に必要となるモニタリング辺りを想定する。
- IT マネジメントについても今回、４つのプロセスに分類がなされ、そのうち全社レベルのプロセスと定義されているのは、「推進・管理体制」、状況により全社レベル、各部門レベルがあり得るのが「外部サービス管理」「事業継続管理」「人的資源管理」となると考えられる。

[4] ISO/IEC TS38501（ITガバナンス：実装ガイド）に設置が定められているグループで、組織体のITガバナンスを効果的に推進する管理活動及び組織における変革プログラム活動の進捗の管理に責任を持ち、取締役会等による評価、指示及びモニタのために必要な関連情報を収集・調整し、適時に提供する機能を担う。

※「推進・管理体制」は従来、IT ガバナンス領域のものとして設定されていた。

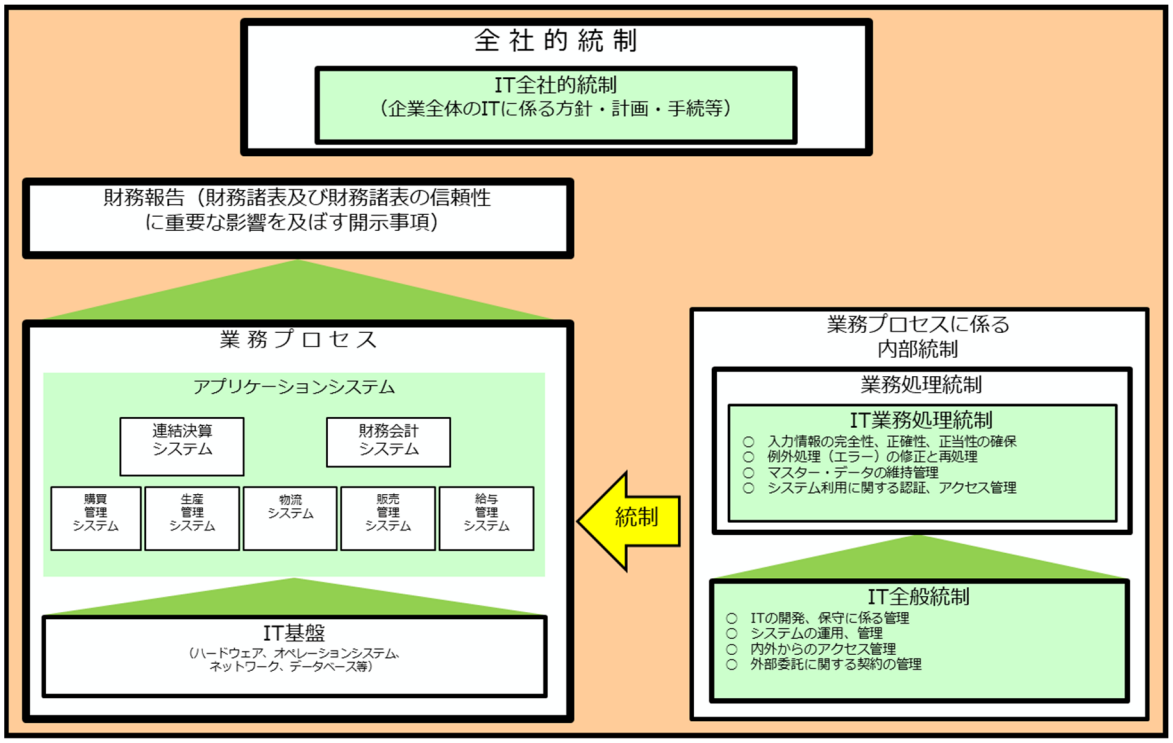
このような考え方に基づき、システム管理基準との関係を踏まえてIT全社的統制、IT全般統制を定義したものが、前述の定義となっている。

②　財務報告とIT統制の関係

財務報告に必要な情報の作成には、販売業務、購買業務、在庫管理業務等の各種の業務プロセスとその結果を集計する決算・財務報告の業務プロセスが関係している。これらの業務プロセスでは、各種のアプリケーション・システムによって、取引が処理され、会計システムへ財務情報が流れる。したがって、IT業務処理統制は、アプリケーション・システムにおいて処理される財務情報の信頼性に直接係ることになる。また、IT基盤は、これらのアプリケーション・システムが稼働するために必要な情報システムのサポートを行うので、IT業務処理統制が有効に機能するためには、IT基盤の統制活動が必要になる。これがIT全般統制であり、財務情報に係る信頼性の基礎となる。さらに、アプリケーション・システムとIT基盤全体を計画性と整合性を伴って統制する役割を持つのが、IT全社的統制である。IT全社的統制は、組織におけるIT全体に係るものであり、IT全般統制とIT業務処理統制の基盤となる。これらの関係を図表Ⅱ．１－３に示す。

なお、財務報告に係る内部統制において、IT業務処理統制及びIT全般統制は財務情報を処理するアプリケーション・システムとIT基盤における信頼性確保という絞り込まれた範囲を対象としているが、これは財務報告の信頼性に係る統制を整備したり評価したりするという目的に限定しているからである。例えば、サイバーセキュリティや個人情報保護に関する対象は、財務報告に係る内部統制において通常絞り込まれることになる。しかしながら、企業におけるIT 統制は、財務報告の信頼性のみのために構築・実施されるものではないことに留意する必要がある。特に、IT統制全体の信頼性を評価するためには、企業全体のITに係る方針・計画・手続等を総括的にIT全社的統制として捉えることになる。

図表Ⅱ．１－３　財務報告とIT統制との関係



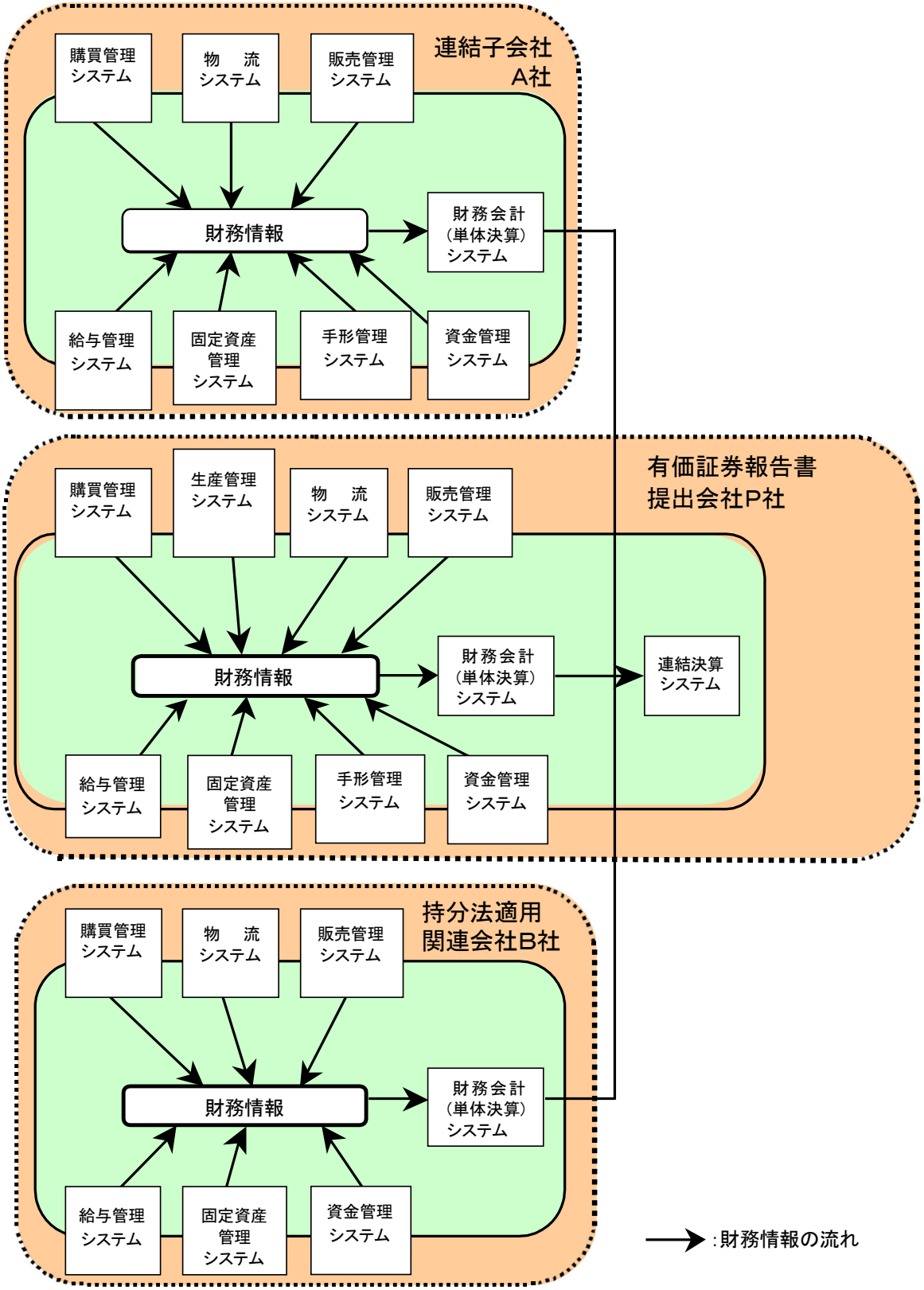
③　財務報告とアプリケーション・システムの関係

前述の財務報告に関係するアプリケーション・システムから財務報告に至る「情報の流れ」をグループ企業の場合を例に模式的に示したものが図表Ⅱ．１－４である。有価証券報告書提出会社、連結子会社及び持分法適用関連会社における各種のアプリケーション・システムで作成された情報は、財務会計システム（ここでは、単体決算のための総勘定元帳のシステムを意味する。）に集約される。

図表Ⅱ．１－４では、これらの会社のアプリケーション・システムの機能のうち、財務情報に関連する部分を緑色で示している（財務会計(単体決算)システム以外のアプリケーション・システムでは財務情報に関連する部分と関連しない部分がある。)。

これらの会社の財務会計システムから単体決算（個別財務諸表）の情報及び連結修正仕訳のための情報が、連結決算システムに送られる。有価証券報告書提出会社においては、連結決算、単体決算及びその他の開示情報を集約して、財務報告書作成システムにより有価証券報告書等が作成される。なお、連結決算及び財務報告書の作成はスプレッドシート等によって行われている場合もある。IT業務処理統制の評価において、評価対象となるアプリケーション・システムは、会計システム（財務会計システム、連結決算システム）及び評価範囲として選定された業務プロセスに係るアプリケーション・システムの機能のうち財務情報に関係する部分である。実施基準においては、内部統制の目的の一つである「財務報告の信頼性」を「報告の信頼性」としており、非財務情報も意識している。現在は財務情報が対象となっているが、サステナビリティ関連情報開示が進むことによって、バリュー・チェーンも含めた内部統制の構築・運用が検討課題となる。

図表Ⅱ．１－４　財務報告とアプリケーション・システムの関係



〈〈コラム：非財務情報への言及・「財務報告」から「報告」への変更〉〉

ステークホルダーからの会社に対する評価は「決算・財務報告」にとどまらず、非財務情報も含めた「報告」に対するものになってきている。例えば、「サステナビリティ(SDGs)に関する開示」「人的資本・多様性に関する開示」「サイバーセキュリティの状況に関する開示」などの分野が挙げられる。この点については、実施基準にも言及されている。

これらの非財務情報の開示に関しては、開示の範囲や定量的な数値を開示する場合、その妥当性などを外部監査人とも連携・協議して対応することが必要となる。

関係する省庁のウェブサイトなども参考にしていただきたい。

参考文献

「企業内容等の開示に関する内閣府令」等の改正案の公表について（金融庁）
https://www.fsa.go.jp/news/r4/sonota/20221107/20221107.html

④　ITを利用した内部統制の特徴と長所・短所

ITを利用した内部統制の特徴としては、一旦適切な内部統制（業務処理統制）を組み込めば、意図的に手を加えない限り継続して機能する性質を有する点が挙げられる。しかし、例えば、その後のシステムの変更の段階で必要な内部統制が組み込まれず、プログラムに不正な改ざんや不正なアクセスが行われるなど、全般統制が有効に機能しない場合には、適切な内部統制（業務処理統制）を組み込んだとしても、その有効性が保証されなくなる可能性がある。⇒*（実施基準　Ⅰ．２（６）②〔ITの統制〕　ロａ）*

その長所としては、手作業による統制活動に比べて迅速な情報処理が期待できるほか、人間の不注意による誤謬等の防止も可能となり、この結果として、内部統制の評価及び監査の段階における手続の実施も容易なものとなる。⇒*（実施基準　Ⅰ．２（６）②〔ITの利用〕　ハ）*

一方、その短所としては、その後のシステムの変更の段階で必要な内部統制が組み込まれず、また、プログラムに不正な改ざんや不正なアクセスが行われるなど、全般統制が有効に機能しない場合には、適切な内部統制（業務処理統制）を組み込んだとしても、その有効性が保証されなくなる可能性がある。⇒*（実施基準　Ⅰ．２（６）②〔ITの統制〕　ロａ）*

２．IT統制の統制項目

（１）　IT全社的統制

①　全社的な内部統制とIT

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。

経営者は、IT全社的統制を構築する責任があり、実施基準では、図表Ⅱ．２－１に示す項目の整備を推奨している。なお、本追補版の第Ⅳ章２節において、具体的な統制に関する指針、統制目標の例、統制の例と統制評価の例について述べている。

図表Ⅱ．２－１ITへの対応

ITへの対応

・経営者は、ITに関する適切な戦略、計画等を定めているか。

・経営者は、内部統制を整備する際に、IT環境を適切に理解し、これを踏まえた方針を明確に示しているか。

・経営者は、信頼性のある財務報告の作成という目的の達成に対するリスクを低減するため、手作業及びITを用いた統制の利用領域について、適切に判断しているか。

・ITを用いて統制活動を整備する際には、ITを利用することにより生じる新たなリスクが考慮されているか。

・経営者は、ITに係る全般統制及びITに係る業務処理統制についての方針及び手続を適切に定めているか。

⇒（実施基準（参考１）財務報告に係る全社的な内部統制に関する評価項目の例　ITへの対応）

②　IT全社的統制の概要

IT全社的統制の整備・運用は、例えば、前述の図表Ⅱ．１－２で示した内部統制の基本的要素を考慮して以下のようにまとめるとよい。

ａ．ITに関する基本方針の作成と周知（統制環境）

IT利用とIT統制のための基本方針の明示は、経営者の理念を伝えるものであり、経営者が行う。CIOはこの方針に従って、利用や統制活動を行う環境を整備する。基本方針による全社的IT環境の整備は、その普及度合いに従って業務活動や内部統制の品質向上に貢献する。

なお、経営者の方針は、従業員に対し教育を実施し、周知するとよい。

ｂ．ITに関するリスクの評価と対応（リスクの評価と対応）

ITは利用者に対し業務処理の効率化・有効化をもたらすが、管理しなければ企業価値に影響を与えるほどの潜在的な脆弱性を持つことになる。例えば、リスク管理部門は、事業推進に影響を与えないように、全社的統制の立場から適正なリスクの洗い出しと評価を行い、対応策を検討することになる。

一方、IT部門は、ITに係る全社的リスクに対して、リスク評価（識別、分類、分析、評価）を行って、リスク対応策（回避、低減、移転、受容）を選択することになる。

なお、リスクの評価の対象となるリスクには不正に関するリスクも含まれる。

ｃ．統制手続の整備と周知（統制活動）

経営者は、IT統制の整備を行い、その基本方針を策定して周知する。

ｄ．情報伝達の体制と仕組みの整備（情報と伝達）

経営者の方針や指示は、適正な手段で関係者に伝えられなければならないが、伝達手段は技術の進歩に合わせて見直しを図る必要がある。また、トップダウンだけで

なくボトムアップの情報提供も重要である。例えば、電子メールやイントラネットなどの「ITを利用した伝達」は、IT統制の概要について全社に浸透させる上で効果的である。

また、大量の情報を扱い、業務が高度に自動化されたシステムに依存している状況においては、情報の信頼性が重要である。⇒*（実施基準　Ⅰ．２（４）①）*

ｅ．全社的な実施状況の確認（モニタリング）

経営者は計画や統制の有効性に対して、実施部門及び内部監査部門からの報告を通して、確認・評価作業を行う。その場合に、統制等の実施状況のモニタリングにおいて効率性と有効性を高めるためには、ITの利用が望ましい。

〈〈コラム：アジャイル/スパイラル開発手法について〉〉

アジャイル開発手法が適用される情報システムの分野は拡大しており、内部統制報告制度の適用対象となる情報システムへの適用も広がってきている。一方、アジャイル開発手法に関して誤解されている部分もあることから、「アジャイルソフトウェア開発宣言」「アジャイルソフトウェアの12の原則」を参照してアジャイル開発手法の留意点を確認してほしい。

アジャイル開発は、「アジャイルソフトウェア開発宣言」で示されているように「ユーザニーズに適合する成果物を」「ユーザニーズの変化に素早く合わせて」提供することを目指した開発手法として受け入れられてきた。

IT全般統制について、ウォーターフォール方式開発の場合は、「ユーザ要求・仕様の受付」「開発」「レビュー」「テスト」「本番適用」などの各フェーズの区分を付けやすく、その都度確認・承認の手続を組み込みやすい。

しかし、アジャイル方式の場合は、「ユーザニーズ」との整合性確保、適切なレビューと承認、UAT（ユーザ受入テスト）及びサービスインの承認手続、開発委託をする場合の責任分界や契約形態など、ウォーターフォール方式とは異なる留意点も少なくない。したがって、これらのフェーズがスプリントの中に組み込まれて進められるため確認・承認の手続を意識的に設定し、バックログやスプリントレトロスペクティブでの記録などのエビデンスの保存も必要になる。

具体的には、以下のような監査証拠となりうる記録の保存が必要と考えられる。

[ガバナンスレベル]

・　アジャイル開発手法を採用することについての経営層での承認記録など

[マネジメントレベル]

・　ユーザの要求仕様をどの時点でどのように要件定義にしたかに関するバックログ等
・　スプリントにおける、UATに代わるユーザと開発者の合意に関する記録
・　本番適用についての責任・意思決定に関する明示的な記録
・　開発チームから運用・保守チームへの成果物の移行の明示的な記録
・　運用・保守のためのドキュメント

参考文献

※　システム管理基準「Ⅱ.1.2 システムライフサイクルモデル管理」
https://www.meti.go.jp/policy/netsecurity/sys-kansa/sys-kanri-2023.pdf
※　「アジャイルソフトウェア開発宣言」
https://agilemanifesto.org/iso/ja/manifesto.html
※　「アジャイルソフトウェアの12の原則」
https://agilemanifesto.org/iso/ja/principles.html
※　上記２点については情報処理推進機構の下記のサイトを参照していただきたい。
トップページ デジタル人材の育成 スキル標準 ITSS+、ITSS、UISS 関連情報 ITSS+（プラス）ITSS＋（プラス）アジャイル領域
https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/agile.html

<<コラム：AI導入での留意点>>

AI技術の進展に伴い、AI技術を利用したシステムの導入事例が増えてきている。

業務プロセスに利用する場合にはAIの特性として「ブラックボックスで出力が生成される」ことを踏まえて、プロセス中に適切な出力の正確性・妥当性などのチェック・承認を組み込むことが必要である。例えば、保険業で保険金申請に対するスクリーニングにAIが利用されているケースがある。このケースでは、契約に対して定型的に補償を適用できる申請と条件が複雑で人間系の判断が必要なものの仕分けをしている。

文章生成AI利用上の注意については、東京都「文章生成AI利活用ガイドライン」が参考になる。

参考文献

「文章生成AI利活用ガイドライン」の策定について（東京都）

https://www.metro.tokyo.lg.jp/tosei/hodohappyo/press/2023/08/23/14.html

（２）　IT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であり、例えば、①システムの開発、保守に係る管理、②システムの運用・管理、③内外からのアクセス管理などのシステムの安全性の確保、④外部委託に関する契約の管理がある。⇒*（実施基準　Ⅰ．２（６）②〔ITの統制〕　ロａ）*

①　財務報告に係るIT全般統制の範囲

企業は、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・運用することが望まれている。

一方、追補版でいうIT全般統制では、その対象が、財務報告に係る情報とその情報を処理するプログラムとデータに係る信頼性に絞り込まれる。すなわち、財務報告に係る業務プロセスにおける情報の信頼性を保証するための基盤としてのプログラムとデータの信頼性を確保するための統制であり、次のような過程でこれらの信頼性が確保される。

- 新規のプログラムは、信頼性がテストされ、承認されて本番環境に移行される。
- プログラムの保守においても、信頼性がテストされ、承認されて本番環境に移行される。
- 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、本番環境に移行される。
- システム運用では、未承認の処理や不正な処理が防止される。
- プログラム及びデータへのアクセスは、あらかじめ承認された者だけにアクセス権限が設定される（予防的統制）。さらに、アクセス違反をモニタリングすることで、プログラムとデータの改ざんが防止される（発見的統制）。
- さらに、開発・保守・運用を外部委託している場合、委託先（外部サービスの利用の場合も含む）で、以上のようなプログラムとデータの信頼性が確保されるようにする。

なお、IT全般統制では、財務報告の信頼性が確保できるようにプログラムとデータの復旧が適切に行われるようにしておけばよい。しかし、サイバー攻撃や重大なシステム障害によって、財務報告の作成が遅延するリスクが高まっているので、事業継続計画の策定を推進することが望ましい。

②　IT全般統制の統制項目の例

以上のような観点から、評価対象となる統制の項目を挙げると、次のとおりとなる。

ａ．　システムの開発・保守

- 開発・保守に関する手続の策定
- ソフトウェアの開発・調達

- IT基盤の構築
- 検証（テスト）

ｂ．システムの運用・管理

- 運用管理に関する手続の策定
- 構成管理、変更管理（ソフトウェアとIT基盤の保守）
- データ管理

ｃ．内外からのアクセス管理などのシステムの安全性の確保

- アクセス管理等のセキュリティ対策
- サイバーセキュリティフレームワークの構築
- 情報セキュリティインシデントの管理

ｄ．外部委託に関する契約の管理

- 外部委託先との契約
- 外部委託先とのサービスレベルの定義と管理
- 契約に基づく外部委託先の管理

⇒*（実施基準 Ⅱ．３（３）⑤ニａ）、（システム管理基準各プロセス参照）*

（３）　IT業務処理統制

IT業務処理統制とは、業務を管理するシステムにおいて、承認された業務が全て正確に処理、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ITに係る内部統制のことである。

⇒*（実施基準 Ⅰ．２（６）②〔ITの統制〕ロｂ）*

①　情報処理とIT 業務処理統制の関係

情報処理そのものは、IT業務処理統制ではない。ITは処理の自動化等に使われることが多い。そして手作業に比べて誤処理のリスクは大幅に低減されることになる。そのためITを利用した情報処理がIT業務処理統制として統制の機能が組み込まれている場合もあり、両者の違いが分かり難いこともある。

②　業務システムに組み込まれたIT業務処理統制

業務処理統制は、販売、購買等の業務プロセスに組み込まれた統制であり、この中で、ITを利用した統制（例えば、データチェック機能）がIT業務処理統制である。また、ITによる自動化された統制（IT業務処理統制）と手作業との組合せで実施される。

ａ．自動化されていないIT業務処理統制

コンピュータを利用した情報システムでは、業務処理に組み込まれた自動化された統制と人手による入力の確認作業で、全体としての統制を構築している。すなわち、手作業での統制によって、財務情報の信頼性が有効となっている。

ｂ．自動化されたIT業務処理統制

Webでの受発注やEDIを利用する受発注システムでは、手作業を経ないで情報シス

テムの内部にIT業務処理統制が組み込まれることがある。このような業務プロセスでは、IT業務処理統制によって処理されたデータの信頼性を確保している。IT業務処理統制は、業務システムの開発段階で組み込まれ、本番で利用する前にテストされ、統制の有効性を確認している。

③　IT業務処理統制の目標と適正な財務情報を作成するための要件

財務情報の信頼性を確保するためのIT業務処理統制は、会計上の取引記録の信頼性を確保するために以下の統制を実施する。

・入力管理
・出力管理
・データ管理

IT業務処理統制としては、図表Ⅱ．２－２のような例がある

図表Ⅱ．２－２　IT業務処理統制の具体例

・ 入力情報の完全性、正確性、正当性等を確保する統制
・ 例外処理（エラー）の修正と再処理
・ マスター・データの維持管理
・ システムの利用に関する認証、操作範囲の限定などアクセスの管理

a．取引に係るIT業務処理統制

業務プロセスで扱われるトランザクションデータ（取引データ）の場合は、売上データが正確に、適時に適切に記録されていること、すなわち、信頼性の確保が統制目標となる。例えば、数量又は単価が、あらかじめ設定していた範囲を超えるとエラーになる等の統制機能が業務システムに組み込まれていることが挙げられる。

b．マスターに係るIT業務処理統制

マスター・データは、複数のトランザクションで参照されるマスター・テーブル等で管理されている。これにより例えば商品単価等が変更になった場合には、マスター・テーブルの更新により、基準日以降の取引に一律に改訂後の単価が適用されることになる。そのため、ファイルやデータベースの場合は、記録されたマスター・テーブルが最新であり、継続して使用が可能であること（維持継続性）及びマスター・データの信頼性を確保することが統制目標となる。

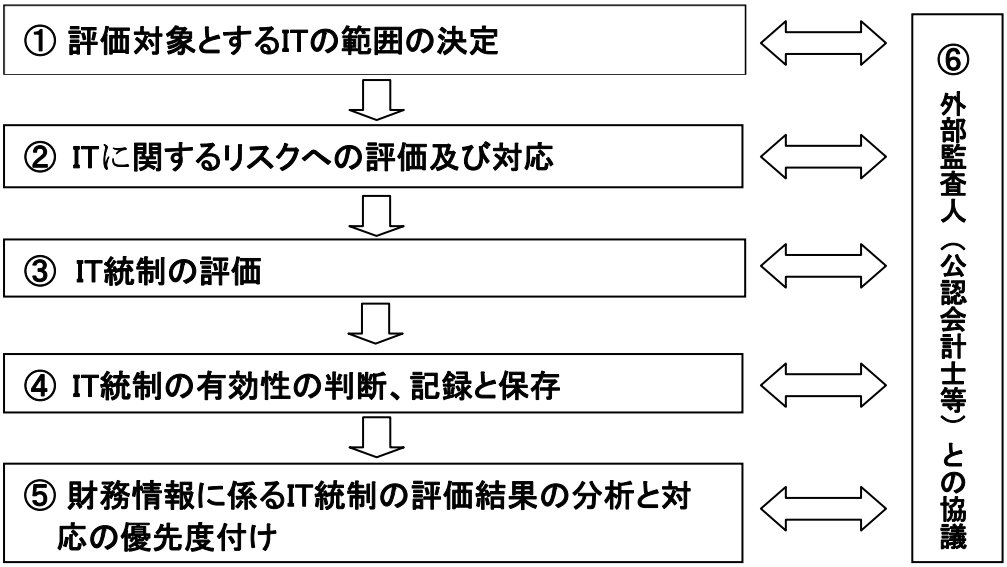
第Ⅲ章　IT統制の経営者評価

１．IT統制の評価のロードマップ

（１）　内部統制評価の流れ

経営者は、内部統制を整備･運用する役割と責任を有している。特に、財務報告の信頼性を確保するため、「内部統制の基本的枠組み」において示された内部統制のうち、財務報告に係る内部統制については、一般に公正妥当と認められる内部統制の評価の基準に準拠して、その有効性を自ら評価しその結果を外部に向けて報告することが求められる（⇒*（実施基準　Ⅱ．１）*）。IT統制については、内部統制の一部として整備・運用することになる。IT統制の評価のロードマップを図表 Ⅲ．１－１に示す。

図表Ⅲ．１－１　IT統制の評価のロードマップ



①　評価対象とするITの範囲の決定

第Ⅲ章２節「評価範囲の決定と対象となるITの把握」で述べる。

②　リスクへの適切な評価及び対応

・財務情報の重要な虚偽記載につながる可能性のある業務を明確にする。そこで、利用されている情報と情報システムに係るリスク評価と対応について検証する。

・業務プロセスに係る内部統制を明確にする。この際、ITを利用することで統制を強化する場合と、ITを利用した結果として新たに不正や改ざん等のリスクが増える場合の両面に留意する。特に、高いリスクが想定される分野では、より広範囲なテストの実施や、統制項目の追加を行う。

③　IT統制の評価

第Ⅲ章３節「IT全社的統制の評価」と、第Ⅲ章４節「業務プロセスに係るIT統制の評価」で述べる。

④　IT統制の有効性の判断、記録と保存

第Ⅲ章５節「IT統制の有効性の判断」で述べる。

⑤　　財務情報に係るIT統制の評価結果の分析と対応の優先度付け

a. IT統制の評価では、ITの利用者を含めた統制の継続的な実施について検証する。

b. 重要なIT統制が関係する統制（例えば、IT業務処理統制が依拠するIT全般統制）については、重点的に検証する。この際、重要度は、そのIT統制が財務情報や財務報告の虚偽記載に与える影響を考慮して決めることができる。

c.　IT業務を外部に委託することもある。内部統制の整備・運用は、企業の責任であるので、外部委託についてもIT統制の評価の一部として検証する。

d. 経営者は、IT統制の評価結果を分析して、リスクの高いものから優先順位を付けて対応策を実施する。

⑥　外部監査人（公認会計士等）との協議

IT統制の評価においては、必要に応じて外部監査人との協議を行うことが望ましい（⇒*（実施基準Ⅱ．２（３）外部監査人との協議）*）。例えば、①「評価対象とするITの範囲の決定」では、ITの評価範囲について外部監査人と見解が違うと、評価範囲に入れなかった子会社等のIT統制が不備の場合には、外部監査人から不備を指摘される可能性がある。特に、それが期末に判明した場合には、不備の是正のための時間的余裕がなくなることがある。したがって、事業年度のできる限り早い時期に、評価すべきIT基盤を決定するまでに、外部監査人とIT基盤について協議し、認識を一致させておくことが望まれる。

２．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

内部統制の有効性の評価を始めるに当たって、最初に、連結グループ全体（以下「グループ」という。）を対象に財務報告の観点から、ITの全体像を把握する。

まず、業界によってITの活用状況が異なることから、子会社等を含め企業の属している業界のIT環境やITの利用状況等を理解する。次に、グループのITの概要を把握する。ここでは、グループのITの接続概要図、重要なシステム間の連携等の全体像が把握されていればよい。

次に、グループの財務情報に係るアプリケーション・システムと、それに関係するIT基盤の概要について把握する。アプリケーション・システムについては、例えば、「○○販売システム」や「△△在庫管理システム」といった単位でシステム間の関係を理解できる程度に把握すれば十分であるが、対象とならない事業拠点においても業務プロセスの重要性にあわせて対象範囲に含める場合もある。さらに、グループのIT全社的統制としての組織、規程、標準等を把握する。

（２）　評価範囲の決定

IT統制の評価範囲の決定は、内部統制の評価範囲が基本となる（⇒*（実施基準　Ⅱ．２（１）①）*）。グループの決算･財務報告プロセスに係るITは、全てIT統制の評価範囲に含まれるが、それ以外の業務プロセスに関係するITについてもIT統制の評価範囲に含まれることがあることに留意する。例えば、評価範囲に含まれる事業拠点の重要な勘定科目に係る業務プロセスは評価に含まれるが、この場合、その勘定科目に係るアプリケーション・システムと支援するIT基盤もIT統制の評価範囲に含まれる。

（３）　把握すべき内容

業務の流れ図を作成し、データの流れを把握すると分かりやすい。⇒*（実施基準　Ⅱ．参考２）*

ITに関して把握すべき内容は、図表Ⅲ．２－１に示す項目である。なお、詳細については付録２－２を参照いただきたい。

図表Ⅲ．２－１　ITに関して把握すべき内容の例

- 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、外部委託等）
- ITに関与する組織、方針

（４）　評価範囲の決定に当たっての留意事項

①　全社的統制に関係するITの評価

統制活動だけではなく、統制環境、リスクの評価と対応、情報と伝達、モニタリングの基本的要素において、ITも評価の範囲に含めることがある。

昨今では、経営者のモニタリングやリスク評価、各種統制活動におけるコミュニケーション、各種統制活動の記録・保管等において、情報システムが活用されることが一般的であるが、これらの基本的要素で利用する情報自体の信頼性確保の観点から、それらの情報を生成・伝達・保管・出力をしているシステム自体も、評価すべきITの範囲に含めて、IT業務処理統制、IT全般統制の評価を実施することが必要になる場合がある。

②　IT基盤と組織区分の相違

企業が複数の事業拠点を有する場合には、評価対象とする事業拠点を売上高等の重要性により決定する（⇒*（実施基準　Ⅱ．２（２）①）*）。IT統制の評価範囲は、評価対象となる事業拠点のアプリケーション・システムとの関係から整理して把握することが基本になる。しかし、事業拠点の組織区分とアプリケーション・システム及びIT基盤は、一致していない場合があることに留意する。以下に、この例を示す。

・組織区分とアプリケーション・システム（IT業務処理統制）が一致しない場合

例えば、図表Ⅲ．２－２のように、売上の計上の重要なポイントである出荷情報の発生が特定の子会社の在庫管理アプリケーション・システムにおいて実施されている場合がある。この場合には、当該子会社の売上高にかかわらず、販売システムに関係するアプリケーション・システムとして、当該子会社の出荷業務を評価範囲に含めることになる。

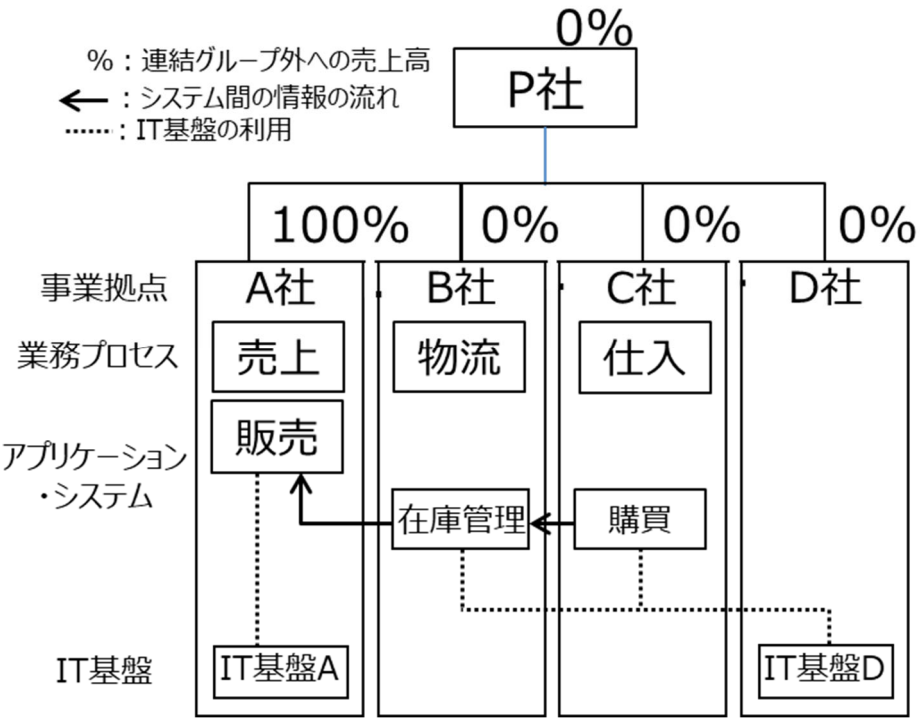
・組織区分とIT基盤（IT全般統制）が一致しない場合

例えば、IT基盤が別の子会社に所属するデータセンターやクラウドサービスで運用されている場合には、子会社の売上高に関係なく、そのデータセンターやクラウドサービスも評価範囲に含めることになる。このように、IT基盤は、「連結ベースの売上高等に基づく重要な事業拠点」の組織区分とは必ずしも一致せず、事業拠点の中に複数存在したり、複数の事業拠点に共通したりする。したがって、この場合のIT統制の評価では、評価対象となるアプリケーション・システムとの関係から整理して把握することになる。図表Ⅲ．２－２において、例えば、販売、在庫管理、購買の３つのアプリケーション・システムが、全て同一のIT基盤の上で稼働している場合、このアプリケーション・システムが設置されているデータセンターは、IT統制評価の対象となると考えられる。

したがって、経営者が、評価の範囲を決める場合には、当該範囲を決定した方法及びその根拠等について、必要に応じて、外部監査人と協議を行っておくことが適切である。

⇒ *（実施基準Ⅱ．２（３）外部監査人との協議）*

図表Ⅲ．２－２　ITの評価範囲の例



３．IT全社的統制の評価

（１） IT全社的統制の意味

経営者は、全社的な内部統制の評価結果を踏まえて、業務プロセスに係る内部統制の評価の範囲、方法等を決定する。⇒*（実施基準 Ⅱ．３（２）③）*

ITに関する全社的な方針、手続等を明確にすることは、IT統制が効果的に機能するための基礎になる。例えば、企業として重要なデータの定義・区分が実施され、この区分に従ったアクセス管理の方針が統一的に定められていれば、システム利活用の形態の差異に関係なく、一定の情報保護の効果が期待でき、ITに関する企業の管理体制が一定の水準に確保されていると考えられる。この場合、IT全社的統制に支えられているIT全般統制とIT業務処理統制の評価が容易になる。IT全社的統制が適切で、複数の事業拠点が同一の方針に基づいてITの運用・整備を行っていることが確認できれば、一部の事業拠点の業務プロセスに関するIT統制を評価することで、評価の範囲を絞り込める可能性がある。

一般的にIT全社的統制が有効であった場合、これに支えられるIT全般統制とIT業務処理統制に関する実効性確保と、評価作業の効率化が期待できる。

IT全般統制等の内部統制は、「組織的な枠組みの設定＝規程等のルール策定」「ルールの遵守」「遵守状況のモニタリング」「モニタリング結果に基づく改善」といったPDCAサイクルによって運用されている。このPDCAサイクルの確実な実施にIT全社的統制が必要となる。すなわちIT全社的統制が有効であることは、内部統制のPDCAサイクルが有効に機能していることを保証し、設定されたIT全般統制等の実効性確保（一時的に不足があったとしても、PDCAサイクルの中で自己改善される点を含む）に寄与することが期待できる。

また、IT全社的統制については、企業内の組織間、拠点間等の内部統制の差異を低減する方向で働く場合も少なくない。そこで、それぞれの組織・拠点等で同一のルールに基づいた内部統制が実効性のある形で実装されている場合には、例えば、IT全般統制を共通する１つの基盤に対する統制とみなし評価することによって、評価作業の効率化も期待できることになる。

IT全社的統制の評価では、図表Ⅲ．３－１に示す点に留意する。

図表Ⅲ．３－１　IT全社的統制の評価における留意点の例

① 経営者は、内部統制を支える重要な要素の１つとして、ITの利活用があることを認識しているか：ITの利活用なしに内部統制の整備・運用は実現しない。
② 経営者は、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か：リスク評価結果とその対応方針を基に全社的な方針、規程を含む内部統制の枠組みが構築される。
③ 経営者は、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か：適切な整備・運用のためには、ヒト、モノ、カネの経営資源が必要であり、経営者の承認がなければ整備・運用は難しい。
④ 財務情報に係るITの整備・運用の状況について、経営者に適宜報告され、経営者が改善を指示する仕組みがあるか：情報と伝達及びモニタリングによってPDCAサイクルが確立される。
⑤ IT統制に係る記録の取得と保存に関する規程が作成され、体制が整備されているか：内部統制は実態として機能しているだけでは不十分であり、その有効性を対外的に説明できる状態にしておくこと（アカウンタビリティの確保）が必要である。

（２）　IT全社的統制が有効でない場合

IT全社的統制が有効でない場合、基幹システムの更改に失敗し、業務に混乱が生じ、財務報告に誤りが含まれたり、適時に作成できなくなったりするリスクがあることに留意する。このような場合には、財務報告に係る内部統制に不備が生じて、財務報告の信頼性に重大な影響を及ぼすことのないように、経営者は経営戦略に合致したIT戦略に基づき、業務とシステムの全体最適化を考慮して計画的に実施されているかどうか、他のシステムへの影響を考慮した全体最適化が勘案されているか等について、リスクを認識して対応することが望まれる。

４．　業務プロセスに係るIT統制の評価

業務プロセスに係るIT統制を評価するには、業務アプリケーションをサポートしているIT基盤の統制であるIT全般統制と業務処理プロセスに対する統制であるIT業務処理統制を評価することになる。

（１）　業務プロセスに係るIT統制の意味

①　IT全般統制

IT全般統制は、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、複数の業務処理統制に関係する方針と手続をいう。

⇒*（実施基準　Ⅰ．２（６）②〔ITの統制〕ロa）*

経営者は、IT全般統制が、例えば、次のような点において有効に整備及び運用されているか評価する。

・システムの開発、保守
・システムの運用・管理
・内外からのアクセス管理など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

⇒（*実施基準 Ⅱ．３（３）⑤ニa）*

ITに係る全般統制の例示と評価における留意点の例を図表Ⅲ．４－１に示す。

図表Ⅲ．４－１　IT全般統制の評価における留意点の例

a. システムの開発、保守

- 経営者は、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、及びITの運用・管理のための統制が整備・運用されているかを評価する。企業が開発業務を適切に管理していない場合には、例えば、未承認の発注を防止する機能を組み込んでいない等、完成したシステムの正当性が確保されないため、統制が整備されていないという評価結果となることに留意する。
- また、開発業務に関しては、ユーザ部門等が参画したテストが実施されているかを評価する。保守業務に関しては、変更管理が適切に実施されているかを評価する。

b.システムの運用・管理

- 経営者は、企業が適切なデータを適切なプログラムで処理し、信頼できる処理結果を得るための統制が整備・運用されているかを評価する。

c.内外からのアクセス管理などのシステムの安全性の確保

- 経営者は、データ、ソフトウェア、ハードウェア及び関連設備等の不正使用、改ざん、破壊等を防止するアクセス管理などによる統制や自然災害等で財務情報が滅失しないような対策（統制）が整備・運用されているかを評価する。

d.外部委託に関する契約の管理

- 情報システムの開発業務や運用業務等を外部委託している場合には、経営者は、委託業務を管理するための統制が整備・運用されているかを評価する。経営者は、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等を評価する。
- 受託会社の管理のためには、契約段階で受託会社の内部統制を評価するための方法を盛り込むことが重要となる。内部統制の評価方法には、受託会社に質問書や確認書を送付する方式、直接往査する方式、受託会社の内部統制に関する保証報告書を入手して確認する方式が存在する。
- クラウドサービス等、受託会社のシステム障害等が委託業務の運営に大きな支障を与えるリスクに備え、受託会社のセキュリティ対応や障害対応に関してサービスレベル合意（SLA）を締結し、その状況を評価する。

パッケージソフトウェアの機能を変更せずに利用している場合のリスク評価を例示する。この場合、リスクの評価に当たり、図表Ⅲ．４－２に示す点について留意する。

図表Ⅲ．４－２ パッケージソフトウェアを利用する場合のリスク評価の例

・　パッケージソフトウェアにプログラム変更を行っていない場合、当該パッケージソフトウェアについては自社で不正なプログラム開発が行われているリスク等を回避していると評価できる。 ・　バージョンアップ等のプログラムの変更は、パッケージソフトウェアを開発した外部の専門業者によって行われるため、不正にプログラム変更をするリスクは限定される。 ・　IT業務処理統制の機能を具備している場合には、業務の一貫性の確保、照合手続の自動化、例外事項報告書作成の自動化、職務分掌に従ったアクセス権限付与等が可能となるので、リスクが限定される。

ただし、パッケージソフトウェアに、独自の機能を追加している場合は、図表Ⅲ．４－２のようなリスクの限定等ができないことに留意すべきである。

なお、パッケージソフトウェアを変更せずに利用する場合でも、プログラムの不正な使用、改ざん等を防止するために、システムへのアクセス管理に関して適切な対策を講じることが重要となる。⇒*（実施基準　Ⅰ．２（６）②〔ITの統制〕ロa）*

②　IT業務処理統制

IT業務処理統制とは、業務を管理するシステムにおいて、承認された業務が全て正確に処理、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ITに係る内部統制である。⇒*（実施基準　Ⅰ．２　（６）②〔ITの統制〕ロb）*

経営者は、識別したIT業務処理統制が、適切に業務プロセスに組み込まれ、運用されているかを評価する。⇒*（実施基準　Ⅱ．３（３）⑤ニb）*

ITに関連する統制活動を次のように分類する。

・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業務処理統制を評価するに当たって、ITが導入された各業務プロセスの内容を理解するとともに、ITの統制目標と適切な財務情報を作成するための評価要件を関連付けながら、統制活動と監視活動の整備・運用状況を理解し、評価する。

業務処理統制に関しては、業務プロセスにおいて適用されている統制が、手作業によるものであれ、ITを利用したものであれ、一体として実施されていることを、経営者がウォークスルー（財務報告に係る取引の開始から財務諸表の作成までを追跡すること）により理解することが有用である。

（２）　評価対象となる業務プロセスの把握と整理

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係を踏まえて評価する。IT全般統制とIT業務処理統制の評価の対象範囲は、財務報告と財務情報に係る業務プロセスに

関連する範囲に限定される。ITの利用状況を把握して、業務プロセスとの関係を明らかにする。

実施基準では、業務プロセスを２つに分類している。⇒*（実施基準　Ⅱ．２（２））*

① 決算・財務報告プロセス（連結財務諸表作成プロセスを含む）

② 決算・財務報告以外のプロセス

「決算・財務報告プロセス」は、主として経理部門が担当する決算・財務報告に係る業務プロセスであるが、総勘定元帳から財務諸表を作成し、財務諸表の開示事項を記載するための手続を管理するシステムが中心となることから、全社的な内部統制に準じて全ての事業拠点を対象として評価する。

「連結財務諸表作成プロセス」は、親会社の連結財務諸表の作成用の報告様式に、親会社・子会社・関連会社が財務情報を入力し、集計して連結財務諸表作成につなげていく業務プロセスである。

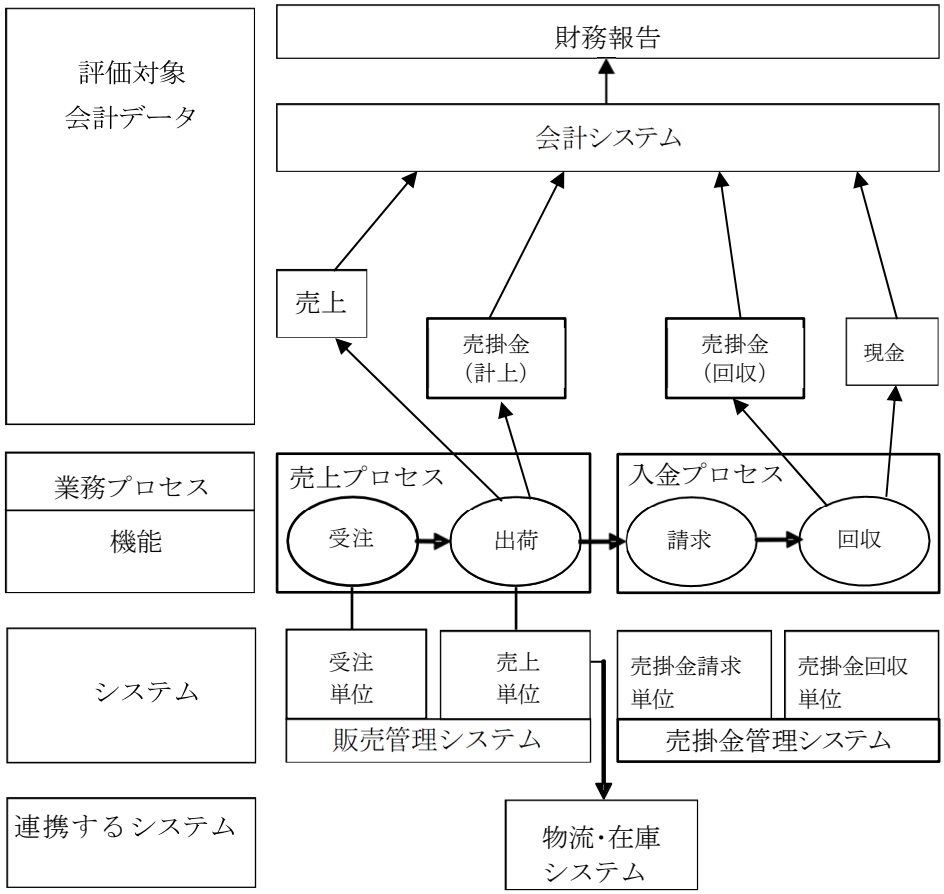
なお、「決算・財務報告プロセス」では、財務会計システム、連結決算システム等の専用ソフトウェアの利用の他に、スプレッドシート等を利用する場合があり、このような場合には、計算式のコピー忘れや計算式の誤りが財務報告の正確性や網羅性に直接影響する。したがって、スプレッドシート等の統制についても評価することになる。

一方、「決算・財務報告以外のプロセス」については、業務プロセスに関連する業務アプリケーション・システムの概要と業務アプリケーション・システムにおける財務情報の流れを把握することになる。

図表Ⅲ．４－３では、売上プロセス（受注機能と出荷機能により構成）と入金プロセス（請求機能と回収機能等により構成）から、売上・売掛金などの勘定科目に関する財務情報が作成され、それが集計されて財務諸表が作成されることが示されている。この場合、「販売管理システム」と「売掛金管理システム」から、「会計システム」に取引データを受け渡すことで、財務諸表が作成される。したがって、「販売管理システム」と「売掛金管理システム」は、財務情報に係るアプリケーション･システムに該当し、評価対象となる。経営者は、財務諸表の勘定科目と取引、業務プロセス及びシステムとの関係を理解し、主要な取引等について、どの会計データがどのシステムに依存しているのかを把握する必要がある（⇒*（実施基準　Ⅱ．３（３）⑤ハ）*）。

なお、図表Ⅲ．４－３では、出荷機能に、「物流・在庫システム」が関係しているので、「物流・在庫システム」の出荷に係る部分も評価対象となる。また、売上という勘定科目には、対象企業の取引の形態により、出荷基準、着荷基準、検収基準等、種々の処理のための会計基準が存在するため、売上という勘定科目に関するIT業務処理統制を評価する場合には、「対象企業が採用している正しい会計基準にしたがった処理が行われる」という準拠性が重要となることに留意する。

図表Ⅲ．４－３ 勘定科目とアプリケーション・システムの関係



出所：金融庁　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

（３）　業務プロセスへのIT利用において、虚偽記載の発生するリスクの識別とこれを低減する統制

経営者は、評価対象となる業務プロセスにおいて、実在性、網羅性、権利と義務の帰属、評価の妥当性、期間配分の適切性、表示の妥当性といった適切な財務情報を作成するための要件のうち、どの要件に影響を及ぼすかについて理解しておくことが重要となる（⇒*（実施基準　Ⅱ．３（３）②イ）*）。そこで、実在性、網羅性、権利と義務の帰属、評価の妥当性、期間配分の適切性、表示の妥当性（以下「評価要件」という。）が満足されているかを評価する。これらの評価要件が満足されていない場合には、結果として報告に虚偽記載の可能性がある。

業務アプリケーション・システムでは、不正又は誤りのリスクを低減させるIT統制が整備されている。したがって、経営者が、業務プロセスを評価する場合には、この不正又は誤りのリスクが、どのIT統制目標を達成することによって低減されているのかを明らかにし、IT統制が評価要件を満足していることを確かめることになる。例えば、ITの統制目標である「完全性」は、販売管理システムにおいて、顧客が注文した商品が、全て、漏れなく、重複なく処理されるという目的のための統制である。一方、この販売プロセスの「完全性」は、財務諸表に売上高が漏れなく重複なく計上されることに

つながり、結果として、評価要件の「網羅性」が満足されていることになる。したがって、IT統制目標の「完全性」の確保は、売上高の計上漏れによる虚偽記載が発生するリスクを低減する統制にあたる。

なお、IT統制目標には、この他に、記録されたマスター・テーブルが最新であり、関連するマスター・テーブル間で齟齬がなく継続して使用が可能であることを保証する維持継続性（第Ⅱ章２（３）③）がある。

５．　IT統制の有効性の判断

（１）　IT全社的統制の有効性の判断

①　IT全社的統制の有効性の評価方法

IT全社的統制については、まず、グループ全体の内部統制を管理している部署やITを管理している部署に対するヒアリング、資料の収集と分析等を行う。例えば、グループ全体を管理する部署が存在していない場合や、存在していても機能していない場合は、グループ全体の内部統制の実施状況を網羅的に把握できないことから不備と判断されることもある。

②　IT全社的統制に不備がある場合の対応

IT全社的統制を評価して、不備が存在している場合には、不備の一覧表を作成し、不備とされた統制を代替する統制の有無等を勘案して、それらが開示すべき重要な不備に該当するかどうかを判断する。この場合、IT全社的統制の不備は、各業務プロセスの内部統制によって、補完される場合がある。また、IT全社的統制に不備がある場合は、当初計画した評価対象の範囲を広げて、IT全般統制とIT業務処理統制を評価することもある。例えば、多くの店舗があり、IT全社的統制として、「アプリケーション・システムに共通して使用されるべきITに関する手続、規程が存在しない」という不備が存在している場合は、評価するIT全般統制とIT業務処理統制の評価を行う店舗の対象数を増やす。

（２）　財務報告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

ITを利用した内部統制の評価は、整備状況と運用状況に分けて実施する。ただし、内部統制が自動化されている場合は、整備状況の有効性の評価が運用状況の評価につながることがある。

手作業による内部統制が一定時点において実際に業務に適用されていることを把握したとしても、対象期間を通じて内部統制が有効に機能していたという評価にはならない。業務の自動化された処理及び統制に、IT全般統制が有効に機能している場合には、一貫性があると考えられることから、整備状況の有効性の評価の結果が運用状況の有効性の評価としても利用できることがある。

IT統制の評価技法の例には、図表Ⅲ．５－１に示すようなものがある。

図表Ⅲ．５－１　IT統制の評価技法の例

・　担当者（開発責任者、システム管理者、業務プロセスの責任者）へのヒアリング
・　IT統制の整備・運用状況の観察（システム操作を通じて業務処理している状況の観察等）
・　IT統制の整備･運用を行うために作成された書類の収集と分析
・　ITの処理結果（会計記録など）と、証憑書類（領収書等裏付けとなるもの）との突合
・　システム上のデータの流れの検証

②　IT全般統制に不備がある場合

ITを利用した内部統制に係るITの全般統制は、IT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であり、仮に、全般統制に不備があった場合には、たとえ業務処理統制が有効に機能するように整備されていたとしても、その有効な運用を継続的に維持することができない可能性がある。したがって、全般統制に不備が発見された場合には、それを速やかに改善することが求められる。⇒*（実施基準 Ⅲ．４（２）④ニ）*

・IT全般統制の不備が財務報告に係る内部統制の開示すべき重要な不備につながらない場合

IT全般統制の不備は、財務報告の重要な事項に虚偽記載が発生するリスクに直接つながるとは限らないので、直ちに開示すべき重要な不備と評価されるものではない。

例えば、システム変更に関する文書化が十分でなくても、プログラム受入テストと同等な機能テストを実施してIT業務処理統制が有効に機能していることが確認されていれば、不備とはみなさなくてもよい場合がある。

・IT全般統制の不備が財務報告に係る内部統制の開示すべき重要な不備につながる場合

アプリケーション・システムに適切なIT業務処理統制が組み込まれていても、運用体制が有効に機能していないなどIT全般統制に不備がある場合には、当該IT業務処理統制が有効に機能しないこともある。

例えば、各アプリケーション・システムでのIT業務処理統制が機能していても、ファイルへのアクセス管理が不十分な場合には、データが改ざんされる可能性がある。このような場合には、容易にデータが改ざんされないような対策を追加する等、IT全般統制を有効に機能させる必要がある。

③　IT業務処理統制に不備がある場合

IT業務処理統制に不備がある場合は、財務諸表の虚偽表示のリスクを十分に検討する。

自動化された統制活動に不備がある場合は、不備が改善されていることを確認する。具体的には、例えば、受注処理において、顧客コードの誤りを検出できない場合、その誤りが繰り返されて財務報告の信頼性が確保できないリスクがある。この場合において、誤りを検出するためのプログラムの修正が実施できないときは、補完的な統制として手作業などによるIT以外の統制などでIT業務統制の不備を補う必要がある。

第Ⅳ章　IT統制のガイダンス（IT統制の例示）

本章では、本追補版を実際に利用する場合の例示を行う。最初に、財務情報に係るIT関連のリスクとIT統制の関係について述べ、IT全社的統制、IT全般統制、IT業務処理統制、モニタリングについて述べる。また、ここで示す項目は、あくまでも、主要なケースを想定した参考情報であって、全ての企業に当てはまるものではないため、必要に応じて修正・削除・追加等して利用されることを想定している。なお、ここに例示する全ての統制を実施することを勧めているのではなく、企業は、自社にとって重要なリスクについて、必要な統制に絞り込んで対応することが基本である。

本章の目次

１．ガイダンスの使い方

（１）　リスクについて

企業は、財務報告に係るIT統制の有効性の評価に当たって、まず、財務報告に係るIT全社的統制の状況を把握する。全社的なITの管理水準が分かれば、情報システムについてのリスクへの対応水準が分かるからである。次に、財務報告に係る業務プロセスにおけるアプリケーション・システムのリスクを把握する。アプリケーション・システムのリスクがIT基盤に係る場合は、業務プロセスに与えるリスクを洗い出すことになる。リスク要因（リスクとなる主要な原因）と結果であるリスクの関係（リスクシナリオ）には、図表Ⅳ．１－１に示すようなものがある。

リスクについては、例えば、以下のような状況において、発生又は変化する可能性がある。⇒*（実施基準 Ⅱ．２（２）②ロ）*

- 規制環境や経営環境の変化による競争力の変化
- 新規雇用者
- 情報システムの重要な変更
- 事業の大幅で急速な拡大
- 生産プロセス及び情報システムへの新技術の導入
- 新たなビジネスモデルや新規事業の採用又は新製品の販売開始
- リストラクチャリング
- 海外事業の拡大又は買収
- 新しい会計基準の適用や会計基準の改訂

図表Ⅳ．１－１　リスク要因とリスクについての例

リスク要因	←　高い　　リスク　　低い→	
不正等の機会	統制が存在しないか、弱い	統制が有効である
外部環境	外部環境の大きな変動 外部（株主、金融機関等）からの圧力が大きい	外部環境の変化がない 外部（株主、金融機関等）からの圧力が小さい

技術的要因	複雑なシステム 独自システム	単純なシステム 標準的なシステム
人的要因、誘因、圧力	要員（経験者）不足 トレーニング不足 IT知識の欠如 職場への不満（金銭的な欲求等） 過度の成果主義（売上達成への圧力等）	経験者や専門家が存在 十分なトレーニング IT知識の共有と活用 モラルの高い職場 適度な成果主義
場所的な要因	業務アプリケーション・システムが複数に分散	集中化されたシステム

（２）　リスクの評価

①リスクの評価においては、財務報告へのリスクや財務情報に係るITのリスクについて考慮する。リスクの評価の対象となるリスクには、不正に関するリスクも含まれる（⇒*（実施基準　Ⅰ．２（２）①）*）。対応すべきリスクが特定されれば、リスク対応を行って企業が受容できるレベルまでリスクを低減させる。ITのリスク対応では、システム管理基準の達成目標や情報セキュリティ管理基準の管理項目等を用いるとよい。

②リスクの評価では、影響度と発生頻度の両方を考慮する。

発生頻度に係るものとしては、次のような項目が想定される。

- ITに関連する過去の事故や事件の件数
- アプリケーション・システムで実行されるトランザクションの件数
- IT基盤やアプリケーション・システムの種類や複雑さ
- プログラムの変更の頻度と複雑さ
- パッケージプログラムの比率

財務報告に係るITのリスクへの対応については、一義的には企業の責任である。しかし、ITリスクの評価について、要員が不足していたり、要員の知識や経験が不十分であったりする企業では、短期間で内部統制を整備し評価するのは難しい。ITリスクの評価を理解するために、財務情報に与える影響と発生頻度によるリスク評価の考え方の一例を図表Ⅳ．１－２に示す。この例では、(a)財務情報への影響度（大、中、小）

と(b)発生頻度（大、中、小）に合わせて、リスクを評価（高、中、低）している。

なお、この考え方は、あくまで例示であり、自社のリスクを分析して対応できる企業の場合には、自社が確立した技法で進めればよい。

図表Ⅳ．１－２　リスク評価の考え方の例

		(a) 財務情報への影響度		
		大	中	小
(b) 発生頻度	大	高	中	中
	中	中	中	低
	小	中	低	低

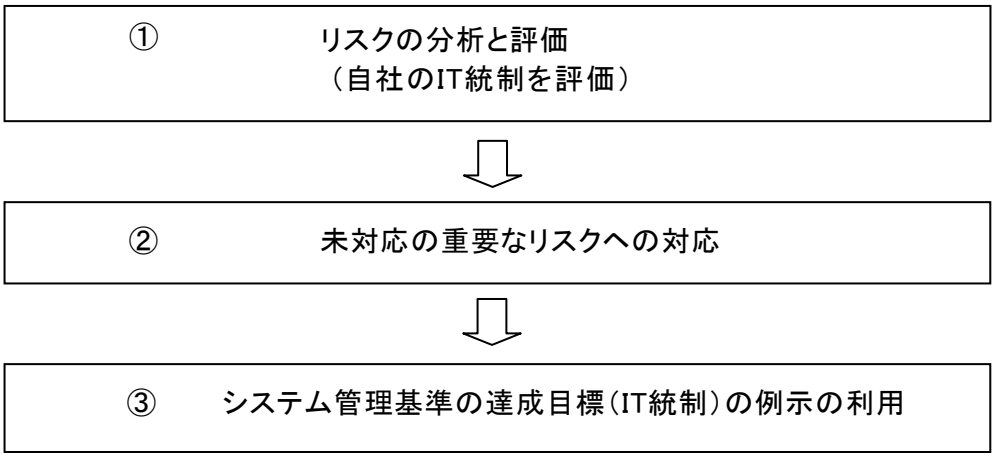
経営者は、リスクが「高」と評価されたものから、対応することになる。なお、リスクが「低」のもので、経営者がこのリスクレベルを受け入れるのであれば、リスク対応は不要となる。⇒*（実施基準　Ⅰ．２（２）②）*

（３）　IT統制の整備と評価に必要な統制目標の設定

対応すべきリスクを特定した後に、リスクへの対応を決める。リスクへの対応には、回避、低減、移転、受容があり、単独で、又は組み合わせて用いられる。⇒*（実施基準　Ⅰ．２（２）②）*

企業は、IT統制を整備、運用、評価することが求められている。IT統制の整備と評価に必要な統制目標の選択プロセスを図表Ⅳ．１－３に示す。

図表Ⅳ．１－３　IT統制目標の選択プロセス



①　リスクの分析と評価

企業は、自社における財務報告に不正又は誤り等の行為が発生するリスクを低減するためにリスク分析を行って、統制を実施している。この中でITに係るリスクについては、統制が機能しているか評価する。評価に当たっては、次のように進めていくことが考えられる。まず、自社（子会社等も含む）におけるITについて実施しているIT統制項目により、財務報告に係るITのリスクを低減しているかについて、評価する。

②　未対応の重要なリスクへの対応

リスク分析の結果、全ての重要なリスクが対応されているときは、IT統制が有効に機能していることになる。一方、財務報告の信頼性に関する重要なITに係るリスクが存在する場合については、そのリスクが内部統制の不備になるか評価する。評価の結果、リスクへの対応が必要な場合には、IT統制を整備することになる。この際の、IT統制項目には、経済産業省が策定した「システム管理基準」や、「情報セキュリティ管理基準」等の達成目標・管理項目等から、自社のリスクを低減する適切な項目を選択する。これらの統制項目により、財務報告の信頼性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する。

なお、「システム管理基準」から実施方法等の「実践部分」について切り離して別冊化された「システム管理基準ガイドライン」（特定非営利活動法人日本システム監査人協会）において、リスク、着眼点等が示されているので、これを参考にしてもよい。必要なIT統制を実施した後のリスクが無視できないときには、ITによらない追加の統制項目を用いる。例えば、財務情報の信頼性に係るリスクについては、システムが作成した出力結果を手作業で確認するという統制も候補となる。

③　システム管理基準の統制目標（IT統制）の例示の利用

財務報告の信頼性に係るリスクを低減させるために、企業はシステム管理基準や情報セキュリティ管理基準等を用いることができる。システム管理基準や情報セキュリティ管理基準等を用いる際、重要なことは、全ての管理策を実施することではなく、自社のITに係るリスクを低減する統制を実施することである。

統制項目の選択に当たっては、IT統制の例示として本章の２節から５節で述べる統制目標や統制例を用いることもできる。これは、図表Ⅳ．１－　３のプロセスから作成できるものであり、統制項目について、【統制に関する指針】、【統制目標の例】、【統制の例と統制評価手続の例】の順で整理して、「リスクの例」とその「統制の例」、「統制評価手続の例」を例示している。企業は自社のリスクの高い分野について、関係する統制項目と例示を調べ、統制や統制の評価を参考にすることができる。

なお、財務報告に係る虚偽記載のリスクを低減するための統制項目を整備・評価する場合、必要な統制項目をリストアップして、付録２「IT基盤質問書及びリスクコントロールマトリクスの例」に示すようなリスクコントロールマトリクスにまとめて、整備や評価を管理すると分かりやすい。

（４）　本章の利用に際しての留意点

本章では、財務報告に係る信頼性の確保という観点からIT統制に係る整備と評価について、具体的な統制目標について述べる（*「財務報告の信頼性以外の他の目的を達成するためのITの統制の整備及び運用を直接的に求めるものではない」（⇒（実施基準　Ⅰ．２（６）②〔ITの統制〕イ）*）。本章で示すIT統制の例示は、あくまでも、財務報告に係るIT統制の整備や評価の目的に限ったものである。どのIT統制項目を採用するかについては、企業が自主的に決めることに留意されたい。

また、業種業態によっては、システム管理基準等の内容が当てはまらないこともあるが、その場合は、独自の管理策を用いることが要請されることもある。

２．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）

【統制に関する指針】

企業には、IT環境を適切に理解し、組織のITに関する適切な戦略、計画、予算等の策定により基本方針を明示することが求められている（⇒*（実施基準　Ⅱ（参考１）ITへの対応）*）。また、人材の採用、育成により、ITを活用する体制を整備することが望まれており、その整備に責任を持つのは経営者である。

統制環境の中でITに関連する事項と例としては、次のものが挙げられる。

（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

⇒*（実施基準　Ⅰ．２（６）②「ITの利用」イ）*

【統制目標の例】

2-(1)-①	組織体におけるITシステムの利活用のあるべき姿を示すIT戦略を策定し、それに基づいてITマネジメントの責任者に指示する。
2-(1)-②	経営戦略及びIT戦略で定められた目標を達成するために、ITシステムの利活用に関するコントロールを実行し、その結果としてのパフォーマンス、コスト、リスク管理、コンプライアンス管理、社会的責任と持続性等の状況を経営者に報告するための体制を整備・運用する。
2-(1)-③	ITに関する業務を適正かつ効率的に行うために、要員の責任及び権限を定める。
2-(1)-④	必要なITに関する人材を確保するために、ITに関する人的資源管理計画及び教育カリキュラムに基づいて、要員の教育・訓練を管理する。
2-(1)-⑤	情報セキュリティ等のITに係る基本方針を定めていること。

【統制の例と統制評価手続の例】

	リスクの例	統制の例	統制評価手続の例
2-(1)-①	ITへの対応が組織として計画的に実施されないことにより、財務報告の信頼性を阻害する。	経営者が財務報告に関連するITへの対応の方針を提示し、取締役会等で承認されている。	ITへの対応についての経営者の方針が、ITに関する計画（中期、年度等の別を問わない。以下同じ。）、年度予算等に盛り込まれ、取締役会、経営会議等において承認されていることを確かめる。
2-(1)-②	ITに関連する組織の不備により、財務報告に関連するITへの対応が適切に実施されない。	財務報告に関連するITへの対応を含むITに関する具体的な方針決定と運営のための全社的な組織が設けられ、有効に運営されている。	ITへの対応について、全社的な調整を図るため、企業グループの実情に合わせて、情報システム化委員会等を設置するか、取締役会、経営会議等において調整が図られる仕組みとなっていることを確かめる。
2-(1)-③	ITに関する業務の管理・実施責任が不明確なことにより、不正やミスが見逃され、情報の信頼性が確保されない。	ITに関する業務の役割分担と責任が明確になっている。	IT部門、ユーザ部門、委託先（情報システム子会社を含む）の役割と責任が職務分掌規程等により適切に定められ、その内容が関連する部門及びグループ企業に周知・徹底されていることを確かめる。
2-(1)-④	ITに関連する業務に携わる適切な人材が確保されないことにより、業務が適切に実施されない。	ITに関連する業務に携わるIT部門及びユーザ部門の人材の採用・育成及び教育訓練を適切に行う（また、社内における人材の確保に代えて、委託を行うことも考えられる）。	ITに関連する業務に携わるIT部門及びユーザ部門の人材の採用と育成についての方針が、ITに関する計画、年度予算等に盛り込まれ、取締役会、経営会議等において承認されていることを確かめる。 なお、委託を行っている場合には、その方針についても確かめる。
2-(1)-⑤	明確な情報セキュリティに関する方針がなければ、適切な情報セキュリティが保証されない。	情報セキュリティ基本方針（情報セキュリティポリシ）が作成され、経営者により承認されている。	情報セキュリティ基本方針が作成され、経営者により承認され、関連する部門及びグループに周知・徹底されていることを確かめる。

<<コラム：全社員デジタル人材化に伴うリスク>>

近年、プログラミングの代わりにアイコン等の組合せでアプリケーションを開発するノーコード開発サービス等の進化により、ITスキルが高くないスタッフでも簡単にロボティック・プロセス・オートメーション（RPA）などの自動処理ツールを使ってシステム化を推進できるようになった。しかし、このような情報システム部門の管理外でのシステム化が広まると、スプレッドシート（表計算ソフトで作成した数式、マクロ、プログラム等を含む表やデータベースソフト等）やエンドユーザコンピューティング（EUC）と同様に、ツールの引き継ぎやセキュリティ対策が困難になるリスクがある。そのため、情報システム部門が全てのツールを把握し、適宜テストやモニタリングに関与したり、ツール使用のドキュメント化を推進させたりする必要がある。また、現場や経理部門のスタッフと情報システム部門との連携を強化し、ツール開発に関するガイドラインを策定することが求められる。ノーコード開発ツールの利便性を活かしつつ、リスクを抑えるためには、システム部門と現場や経理部門のスタッフの一体化が不可欠である。

（２）　ITに関するリスクの評価と対応（リスクの評価と対応）

【統制に関する指針】

ITに関するリスクの評価と対応とは、自社を取り巻くIT環境に関連するリスク評価を適切に行い、それに基づいて必要な対応を行うことであり、更には統制活動にITを利用することにより新たに生じるリスクを考慮することが求められている。

また、信頼性のある財務報告の作成に重要な影響を及ぼす可能性のある変化が発生する都度、リスクを再評価する仕組みを設定し、適切な対応を図ることを意味する。
⇒*（実施基準　Ⅱ（参考１）リスクの評価と対応）*

【統制目標の例】

2-(2)-①	組織体の目的及びIT戦略の目標を達成するために、達成に及ぼす影響についてリスクを評価し、対応を行う。⇒*（システム管理基準　Ⅰ．２．４）*

【統制の例と統制評価手続の例】

	リスクの例	統制の例	統制評価手続の例
2-(2)-①	ITリスク評価が実施されないことにより、重要なリスクを見落とす（対策が講じられない）。	ITリスク評価に関する規程が定められており、規程に基づいてリスクの評価と対応が実施されている。	全社的及び業務プロセスに係るITリスク評価に関する規程が定められており、重要な問題点が経営者に報告されていることを確かめる。

（３）　IT利用と統制（統制活動）

【統制に関する指針】

統制活動とITとの関係は、IT全般統制及びIT業務処理統制についての方針及び手続を適切に定めているかという側面（⇒*（実施基準 Ⅱ（参考１）ITへの対応）*）と、ITを利用した統制活動を、適切に設計して業務プロセスに組み込むことにより、統制活動の自動化が可能となるという側面からなる（⇒*（実施基準 Ⅰ．２（６）② ITの利用ハ）*）。

IT全般統制及びIT業務処理統制に関する方針と手続については、経営者の責任において、ITに関連する業務プロセス及び財務報告と財務情報に関する業務プロセスに関して規程を定め、関連する部門及びグループ企業に周知・徹底し、実施する。一方、統制活動は必ずしもITを利用しなくても実施できるが、ITを利用することにより、正確かつ効率的に実施できる場合もある。例えば、適切な生産管理システムを開発

し、その中に、棚卸の検証プログラムを組み込んでおき、製造部門が製造指図書のデータに従って在庫原材料の出庫数量を入力する手続や倉庫係が日々の原材料の実在庫データを入力する手続等を業務プロセスに組み込むことにより、瞬時に帳簿在庫と実在庫の差を把握し、問題の発見に役立てることができる（⇒*（実施基準　Ⅰ．２（６）②〔ITの利用〕ハ）*）。これにより、手作業による統制活動に比べて迅速な情報処理が期待できるほか、人間の不注意による誤り等の防止も可能となり、結果として、内部統制の評価及び監査の段階における手続の実施も容易なものとなる。したがって、経営者は統制活動へのITの利用についても、その方針及び手続を定め、関連する部門及びグループ企業に周知・徹底し、実施することが望ましい。

【統制目標の例】

2-(3)-①	IT全般統制及びIT業務処理統制に関する方針及び手続を適切に定めていること
2-(3)-②	統制活動にITを利用する場合に備えた方針及び手続があること

【統制の例と統制評価手続の例】

	リスクの例	統制の例	統制評価手続の例
2-(3)-①	ITに関する統制活動が適切に行われないことにより、財務報告の信頼性が確保されない。	IT全般統制及びIT業務処理統制の整備の方針を定め、関連する部門及びグループ企業に周知・徹底されている。	IT全般統制及びIT業務処理統制の整備の方針が取締役会、経営会議等において承認され、関連する部門及びグループ企業に周知・徹底されていることを確かめる。
2-(3)-②	統制活動にITを利用する場合には、その方針及び手続を適切に定めていないことによりITの適切な利用がなされない。	統制活動にITを利用するときのために、財務報告に関連するアプリケーション・システムにITを利用して適切に統制活動を行うための方針が定められ、関連する部門及びグループ企業に周知・徹底されている。	統制活動にITを利用するときに備えて、財務報告に関連するアプリケーション・システムに統制活動として組み込むための方針があり、関連する部門及びグループ企業に周知・徹底されていることを確かめる。

（４）　情報伝達の体制と仕組みの整備（情報と伝達）

【統制に関する指針】

ITに関連する情報と伝達とは、ITに関する経営者の方針が組織の各層に伝達され、また、ITに関する業務の状況についての情報伝達の体制と仕組みを意味する。なお、ITに関する経営者の方針の伝達については、第Ⅳ章２節（１）で示した事項と共通で

ある。

ITに関する業務の状況についての情報伝達の体制と仕組みにおいては、企業内（経営者、IT部門、ユーザ部門及び関係部門）及び業務委託先（企業グループ外に業務委託を行っている場合）における情報の双方向の伝達及び共有の体制と仕組みを適切に整備し、運用することが望まれる。

【統制目標の例】

2-(4)-①	組織体のITパフォーマンスが、取締役会等の意図や期待、倫理的行動、コンプライアンス上の義務を満足していることを確認するために、ITパフォーマンスの状況を適時確認して、必要な是正措置を指示する。

【統制の例と統制評価手続の例】

	リスクの例	統制の例	統制評価手続の例
2-(4)-①	ITに関する重要な問題点（システム障害、変更点、対応状況等）が、企業内（経営者、IT部門、ユーザ部門及び関係部門）、業務委託先、提携先、取引先等の関係者に適切に伝えられないため、ITに関するリスクの対応に支障が生じる。	経営者が、ITに関する業務及びIT関連プロジェクトにおける重要な問題点（システム障害、変更点、対応状況等）を企業内（経営者、IT部門、ユーザ部門及び関係部門）、業務委託先、提携先、取引先等の関係者に、伝達する方針と手続が定められ、運用されている。	ITに関する業務及びIT関連プロジェクトにおける重要な問題点（システム障害、変更点、対応状況等）に関する情報が、企業内（経営者、IT部門、ユーザ部門及び関係部門）、業務委託先、提携先、取引先等の関係者に必要に応じて伝達され、情報が共有されていることを確かめる。

（５）　全社的な実施状況の確認（モニタリング）

モニタリングについては、第Ⅳ章５節「モニタリング」において詳述する。

IT全社的統制のリスクコントロールマトリクスについて

IT全社的統制は、財務情報の信頼性を直接保証する統制ではないが、IT全般統制及びIT業務処理統制の有効性を確保するための基盤となるものである。したがって、IT全般統制及びIT業務処理統制の評価においては、詳細な統制内容を検討し、IT全社的統制の検討においては、全社的な方針と手続が設定されているかどうかを評価すればよい。

IT全社的統制の実施状況を評価するためには、リスクコントロールマトリクスを作成すると分かりやすい。この例を以下に示す。また、具体的なリスクコントロールマトリクスの例を、付録２「IT基盤質問書及びリスクコントロールマトリクスの

例」に示す。

３．IT全般統制

IT全般統制の重要な点は、財務情報を扱う情報システムの新たな開発と開発したITの運用について、的確な管理により財務情報の虚偽表示リスクを低減させることにある。運用については、運用時の情報システムに対するアクセス管理とソフトウェアやデータの変更管理が重要となる。以下では、開発から運用に至るITに共通な統制項目について例示する。

なお、IT基盤に係るIT全般統制は、IT業務処理プロセスに係る財務情報の信頼性の確保のために実施するものであり、IT基盤単独を対象にするものではない。

（１）　システムの開発、変更・保守

⇒（*実施基準 Ⅲ．４（２）②ロａ*）

①　システムの開発

【統制に関する指針】

財務情報に係る情報システムのソフトウェアの開発と調達は、財務報告の信頼性を確保する上で重要なプロセスであるので、誤りや不正を防止するために、標準化された開発手法、テスト、本番への移行手続を用いる。

財務情報に係る情報システム（販売管理システム、売掛金管理システム、財務諸表作成システム等）のソフトウェアを自社開発する場合とパッケージソフトウェアを利用する場合がある。また、利用形態としてもオンプレミスの場合と、自社で機器を持たずにSaaS等のクラウドサービスを利用する場合がある。どちらの場合にも、入出力や内部の情報処理に際して誤りや不正を防ぐ統制機能の整備と運用が重要であり、この統制に不備があると、結果として、財務情報の信頼性に重大な影響を与える可能性がある。

ソフトウェアを自社で開発する場合は、システムの要件を決める設計プロセス、ソフトウェアの作成プロセスにおいて、プログラムのエラーの発生を未然に防止し、開発者が不正なプログラムを埋め込めないような統制が望まれる。また、このプロセスにおいて意図的に改ざんや不正ができないようにするために、標準的な開発手法を定め、これに従うようにする。さらに、開発が終了した段階で、開発されたソフトウェアを十分にテストして、仕様通りに実装されていることを確かめる。なお、ソフトウェアのテストは、ソフトウェアの作成と独立して実施する

ことが望まれる。

オンプレミスにせよクラウドサービスを利用するにせよ、パッケージソフトウェアを調達する場合には購入したままの状態では十分な統制が実現できないことに注意する。例えば、不正なデータ改ざんを防止するためのアカウント管理や権限の設定、自動で起票される自動仕訳の設定、仕訳の承認者の設定、セグメント別開示に関わる組織の設定、他システムからのデータ連携の設定など、ソフトウェアに正しい設定を行わなければ十分な統制が存在することにならない。

【統制目標の例】

ａ．開発

3-(1)-①-イ	情報システムの開発方針・手続、開発手法（開発標準）が存在し、責任者がその方針や手法にあった体制やコミュニケーション方法を構築していること。
3-(1)-①-ロ	開発手法は、財務情報の完全性、正確性、正当性を考慮していること。
3-(1)-①-ハ	情報システムは、誤り防止、不正防止、可用性、他のシステムとの整合性を考慮して設計されていること。

ｂ．調達

3-(1)-①-ニ	プロジェクトの要求内容を満足する製品・サービスを取得するための調達手続を明確にし、それに基づいて調達を実施すること。
3-(1)-①-ホ	統制が有効に整備・運用されていることを検証するために十分で適切なテストが実施されること。

【統制の例と統制評価手続の例】

	リスクの例	統制の例	統制評価手続の例
3-(1)-①-イ	ITの開発の際に意図的な不正なプログラムが埋め込まれたり、処理に誤りが顕在化したりする。	ITを開発するための標準化された方針及び手続があり、これに基づいて、ITが開発されている。	ITの開発に係る方針、手続が作成されており、また、適時に更新されていることを確かめる。
3-(1)-①-ロ	ITの開発プロセスにおいて、意図的な不正や、処理に誤りが起きる可能性がある。	ITの開発において、財務情報の信頼性に係る統制機能の業務要件やプログラム仕様が明示されている。	財務情報に係る過去の開発プロジェクトで、業務要件やプログラム仕様の文書化が行われたか確かめる。（例えば、開発における要件定義書、プログラム仕様書が作成されていることを確かめる。）
3-(1)-①-ホ	誤りや不正防止機能が確実に動作しないと、誤りが起きる可能性がある。	ITの開発では、財務情報の信頼性に係る統制機能がテストされている（テスト内容については、下記の④テストを参照のこと）。	財務情報に係る過去の開発プロジェクトで、テストが行われ、結果が文書化されたかを確かめる。

②　IT基盤の構築

【統制に関する指針】

財務情報に係るさまざまな業務システムは、IT基盤が提供する情報処理・伝達機能（サーバ、ネットワーク、データベース、IT基盤に関わるクラウドサービス等）を利用している。したがって、IT基盤上の情報処理・伝達機能が、適切に動作するためには、IT基盤の設計、調達、導入のプロセスを適切に統制することが望まれる。特に、サーバ、ネットワーク、データベース等のIT基盤の構成要素に対する統制は、財務報告の業務システムの信頼性を保証する上で重要である。

【統制目標の例】

a．IT基盤の構築

3-(1)-②-イ	IT基盤（ネットワーク機器やソフトウェアを含むサーバ、コンピュータ等のインフラシステムで、IaaSを含む）が、財務情報に係る情報機器の信頼性を達成するものであること。⇒*（システム管理基準　Ⅱ．１．３）*

【統制の例と統制評価手続の例】

	リスクの例	統制の例	統制評価手続の例
3-(1)-②-イ	IT基盤の設定が不適切な場合、システムが正しく動作しない。	IT基盤の設定が適切に維持されている（不明な変更が加えられていないこと）。	IT基盤が適切に設定され、維持されていることを、事前の稟議承認記録、設定の計画、その実施結果報告設定の記録や保守での記録によって確かめる。

③　変更管理

財務報告に係るシステム処理の完全性、正確性、正当性が、システム変更によって阻害されないように変更管理を行う。

変更管理は変更や改変及びそのことにより発生する影響を管理する。そのため、変更管理が不十分な場合には、システムの異常動作やシステム停止、管理されていないデータの改変等が起きて、その結果、財務報告を含む報告の信頼性に影響を及ぼす可能性がある。

変更管理では、プログラムが無断で改変されないように、ソフトウェアのバージョンアップ、プログラムの変更及び適切な管理をする。

【統制に関する指針】

変更管理は、財務情報の誤りにつながるようなシステムの機能変更を防ぐために必須の統制である。変更管理に不備がある場合、財務報告に重要な影響を与える可能性がある。例えば、自動仕訳の対象データや使用する勘定科目を変更する際は、分類と報告の完全性を確実にするため、変更前の適切な承認と変更後のテストを実施する。

また、システムの変更に際しては、当該システムの変更が既存のシステムと整合性を保っていることを十分に検討し、その変更の過程について記録を保存する。

【統制目標の例】

a．変更管理全般

3-(1)-③-イ	変更管理ルールと手順を定め、業務責任者並びに開発及び保守の責任者が承認すること。⇒*（システム管理基準　Ⅱ．2．7）*
3-(1)-③-ロ	変更管理要求が生じた場合、他システムの影響を考慮すること。
3-(1)-③-ハ	緊急の変更要求は文書化され、変更管理手続に従っていること。
3-(1)-③-ニ	変更の結果は、業務担当者及び開発責任者が承認すること。変更によるIT基盤の運用や保守への影響は運用責任者や保守責任者に伝えられ、理解されていること。⇒*（システム管理基準Ⅱ．2．7）*
3-(1)-③-ホ	起案から完了までの状況を文書管理し、進捗を把握すること。⇒*（システム管理基準　Ⅱ．2．7）*

b.　独自開発のソフトウェアで重要となる変更管理

3-(1)-③-ヘ	システム設計書、プログラム設計書等は、保守計画に基づいて変更し、業務責任者並びに担当者、保守の責任者が承認すること。⇒*（システム管理基準　Ⅱ．6．3）*
3-(1)-③-ト	変更は、変更管理手順に基づき、保守の責任者の承認を得ること。⇒*（システム管理基準　Ⅱ．6．2）*
3-(1)-③-チ	設計書に基づいて開発していることを検証すること。
3-(1)-③-リ	テストの実施は、テスト計画に基づいて行うこと。⇒*（システム管理基準　Ⅱ．6．4）*
3-(1)-③-ヌ	テストには業務担当者等が参画すること。⇒*（システム管理基準　Ⅱ．6．4）*
3-(1)-③-ル	テスト結果は、担当者並びに運用及び保守の責任者が承認すること。⇒*（システム管理基準　Ⅱ．6．4）*
3-(1)-③-ヲ	本番への移行は、運用担当者が実施すること。⇒*（システム管理基準　Ⅱ．6．5）*
3-(1)-③-ワ	テスト結果、本番への移行結果を記録及び保管すること（記録及び保存については、テストを参照）。⇒*（システム管理基準　Ⅱ．6．6）*

c．パッケージソフトウェアで重要となる変更管理

3-(1)-③-カ	機能の追加等の変更は、その要否を検討の上で業務責任者等が承認すること。
3-(1)-③-ヨ	最新の承認されたパッチが導入されていることを確認すること。
3-(1)-③-タ	テストを実施して、結果を保管すること。
3-(1)-③-レ	本番への移行は、自社で行うにせよ外部に委託するにせよ、適切なモニタリングのもとで実施すること。

【統制の例と統制評価手続の例】

	リスクの例	統制の例	統制評価手続の例
3-(1)-③-イ	プログラムが改ざんされたり、承認なく変更されたりする。	システムソフトの変更を含むプログラム変更、システムの変更及び保守管理については、変更管理手続に従っている（標準化され、記録され、承認され、文書化されている）。	・変更管理手続が文書化され、ITの現状が把握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、財務報告に重要な営業を及ぼすパラメータの変更を含む、本番環境の全ての変更について、変更管理手続に従って管理されていることが望まれる。変更要請が、承認され、プログラムが作成され、テストされ、本番環境に移行されるまで、追跡されていることが望まれる）。 ・プログラム変更は、変更管理手続に従って、統制された環境で、適切（職務の分離や複数名で相互確認しながらの本番移行等）に実施されているかを確かめる。 （例えば、過去のアプリケーション等の変更を選び、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。） ・承認されていない不明な変更がないか確かめる。 （例えば、本番システムの変更記録を入手し、変更要請、承認、移行等を追跡して不明なものがないか確かめる）。
3-(1)-③-ハ	緊急時にプログラムが改ざんされたり、承認なく変更されたりする。	緊急の変更依頼は文書化された正式な変更管理手続に従っている。	・緊急な変更を管理するための手続が存在するか確かめる。 ・緊急変更のための手続に、取消手続があるか確かめる。 ・全ての緊急な変更がテストされ、変更後に標準的な承認手続に従っていることを確かめる。

	リスクの例	統制の例	統制評価手続の例
3-(1)-③-ニ、3-(1)-③-ワ、3-(1)-③-レ	本番環境に変更結果を移行する際にプログラムが改ざんされる。	変更されたプログラムの本番移行に際して、移行を責任者が承認し、移行作業に当たっては権限の分離が行われていること。	・プログラムの本番移行前に、承認がなされているか確かめる。 （例えば、責任者、システム開発者、担当者等による承認がなされていることを確かめる。） ・プログラムの本番移行に際して、移行の責任者とシステム開発者に、適切な職務権限の分離又は牽制の仕組みがあることを確かめる。

④　テスト

【統制に関する指針】

新しい情報システムやIT基盤を本番環境に導入する場合や変更を行う場合、業務システムが設計通りに動作していることを確かめるために、適切なテストを行う。テストが適切に実施されないと、業務システムやIT基盤が設計で意図した通りに機能せず、その結果、財務情報の信頼性に影響を及ぼす可能性がある。

【統制目標の例】

ａ．テスト方針と手続

3-(1)-④-イ	業務システムのソフトウェア及びIT基盤のテストのために、テストの方針と手続が定められていること。⇒*（システム管理基準　Ⅱ．４．３）*
3-(1)-④-ロ	テスト計画は、開発及びテストの責任者が承認すること。⇒*（システム管理基準　Ⅱ．４．３）*

ｂ．テスト環境

3-(1)-④-ハ	テストは、本番環境と隔離され、本番環境と同期を取ったテスト環境で行うこと。

3-(1)-④-ニ	テストに当たっては、要求事項を網羅し、実際の運用を想定したテストケースを設定し、テストデータを作成すること。⇒*（システム管理基準 Ⅱ．4．4）*
3-(1)-④-ホ	テストに当たっては、想定される環境での負荷を考慮して実施すること。また、ピーク負荷が情報システムの耐性に大きな影響がある場合には、ピーク負荷のテストを実施すること。⇒*（システム管理基準　Ⅱ．4．4）*

ｃ．テスト作業の権限の分離と結果の保管

3-(1)-④-ヘ	テストには、開発当事者以外の者（運用担当者や保守担当者等）が参画すること。⇒*（システム管理基準　Ⅱ．4．4）*
3-(1)-④-ト	テストで発生した問題点について、問題ごとの対応策とリスクが明確になっていること。その記録が保存されていること。⇒*（システム管理基準 Ⅱ．4．4）*

【統制の例と統制評価手続の例】

	リスクの例	統制の例	統制評価手続の例
3－(1)－④－イ	IT基盤の情報転送機能がテストされないと、財務情報が正確にシステム間で受け渡されているか確認できない。	・IT基盤の機能をテストする手順が策定され、業務システムが意図したとおりにデータが受け渡されているか、また正しく動作するかを検証するために、業務システムの出力データの検証等のテストを実施する。 ・IT基盤の更改では、業務システム等のマスター・データの配信、新旧システム間でのデータ変換、データ転送、財務情報の配信等のテストが実施されている。	過去の財務情報に係る重要な開発プロジェクトやIT基盤の機能更改プロジェクトを調べる。プロジェクトでは、テスト計画があり、これに従って進められたことを確かめる。
3－(1)－④－ロ	IT基盤のテストが事前に計画されていないとテスト項目に漏れが起きる。	IT基盤のテスト計画を事前に関係者でチェックして、テスト内容やテスト項目に漏れがないようにする。	過去の財務情報に係るIT基盤でのテストについて調べる。このテストにおいて、テストの内容や計画が事前に関係者に照会されてチェックされていることを確かめる。

	リスクの例	統制の例	統制評価手続の例
3-(1)-④-ホ	IT基盤やアプリケーション・システムが、負荷が大きいときに正しく動作しない。	テスト計画と確立されたテスト標準に従って、ストレステスト（負荷テスト)や限界性能テストを実施する。	・過去の財務情報に係る重要な開発プロジェクトやIT基盤の機能更改プロジェクトを調べる。 ・プロジェクトでは、ピーク負荷による性能低下が懸念される場合、負荷テストや限界性能テストが実施され、必要な対応が行われたことを確かめる。
3-(1)-④-ニ	財務情報データを旧システムから新システムに移行する際に、テストが行われないと、移行したデータが正確かどうか分からない。	新システムに移行されたデータが信頼できることを確認するため、旧システムのデータと突合せテストを実施する。	・財務情報のデータ移行が実施された際の記録を調べる。 ・データの移行の責任者及び受入側の承認について確かめる。 移行に際しては、旧システムのデータとの突合などによって正確に移行されたかを確かめる。
3-(1)-④-ヘ	受入テストをシステム開発した担当者が実施すると、誤りや不正が見逃される可能性が残る。	財務情報に係る情報システムの受入テストでは、開発担当者以外の者が参画する。	財務情報システムの過去のプロジェクトを選ぶ。その際の受入テスト記録から、テストが開発者のみで実施されていないことを確かめる。
3-(1)-④-ト	テスト結果の記録が残されていないと、機能が正しく開発されていることの確認ができない。	財務情報に係る情報システムの重要なテスト（受入テスト等）では、テスト項目や結果を記録して、保管する。	財務情報システムの過去のプロジェクトを選ぶ。その際の重要なテストについて、実施され、記録が残され、保管されていることを確かめる（問題管理表とその結果が保管されているとなおよい)。

⑤　開発・保守に関する手続の策定と保守

【統制に関する指針】

外部環境の変化に合わせて、ITに関する方針と手続が策定・変更されたときには、ソフトウェア開発方法論、調達、アプリケーションの開発・保守管理並びに必要な文書化の各プロセスが見直される。方針と手続の変更は、財務報告の信頼性の維持に役立つ。

【統制目標の例】

3-(1)-⑤-イ	企業の開発及び保守に係る手続は、環境変化に合わせて、適宜見直し、変更されること。⇒*（システム管理基準　Ⅱ．１．２）*

【統制の例と統制評価手続の例】

	リスクの例	統制の例	統制評価手続の例
3-（1）-⑤-イ	外部環境が変化したときに、開発やプログラムの変更管理、アクセス管理、運用に関わる方針と手続が変更されないと、リスクが大きくなる。	プログラム開発、プログラムの変更管理、プログラムやデータへのアクセス管理、コンピュータの運用に係る方針と手続が存在しており、経営者は適宜見直し、更新、承認する。	左記の方針と手続が変更された際に、経営者や責任者がその変更を承認しているかを確かめる。

（２）　システムの運用・管理

⇒*（実施基準 Ⅲ．４（２）②ロｂ）*

①　運用管理

【統制に関する指針】

財務報告に係るITの運用において、企業における財務情報の入力、登録、処理、集計、報告等、日常の業務処理の信頼性を確保できるように運用することが望まれる。特に、財務報告に係るITの運用に不備がある場合、結果として報告の信頼性に重大な影響を及ぼすことがある。

例えば、販売管理システムが故障した場合、売上データが消失する等のリスクがあり、財務情報の完全性、正確性、正当性が損なわれ、販売管理システムの結果を利用する財務報告の信頼性も損なわれる。

【統制目標の例】

ａ．運用管理ルールの策定と遵守

3-(2)-①-イ	運用ルールを定め、遵守すること。⇒*（システム管理基準　Ⅱ．５．１）*
3-(2)-①-ロ	運用ルールに基づいた運用計画を策定し、承認すること。⇒*（システム管理基準　Ⅱ．５．２）*

3-(2)-①-ハ	運用ルールには、例外処理のオペレーションが含まれること。⇒*（システム管理基準　Ⅱ．５．３）*

ｂ．運用計画の承認

3-(2)-①-ニ	規模、処理日時、システム特性、業務処理の優先度を考慮したジョブスケジュールに従って運用すること。⇒*（システム管理基準　Ⅱ．５．３）*

ｃ．運用の実施記録、ログの取得と保管

3-(2)-①-ホ	情報システムはアクセス記録を含む運用状況を監視することが望ましく、また、情報セキュリティインシデントを記録し、一定期間保管すること。⇒*（システム管理基準　Ⅱ．５．３）*
3-(2)-①-ヘ	情報システムで発生した問題を識別するために、システム運用の作業ログ・障害の内容ログ及び原因ログを記録し、保管すること。取得されたログは、内容が改ざんされないように保管することが望ましい。⇒*（システム管理基準　Ⅱ．５．7）*

ｄ．教育

3-(2)-①-ト	情報システムの利用に先立ち、担当者向けの支援プログラムや教育プログラムが準備され、教育研修が実施されていること。⇒*（システム管理基準　Ⅱ．５．１）*。

【統制の例と統制評価手続の例】

	リスクの例	統制の例	統制評価手続の例
3-(2)-①-イ	運用時の誤操作によって誤った処理が行われる。	本番環境での運用で、財務情報に係る全ての処理が、完全性、正確性、正当性を満足するように、運用について標準的な手続として文書化されており、これに従っている。	運用の手続を文書化しているかどうか、また、運用の状況を管理者が確認しているかを確かめる。 （例えば、運用状況について、日誌等で手続通り対応されているかを確かめる。ジョブスケジュール通りに運用されているか、もし、例外処理がある場合には、例外処理が承認されており、財務情報に係る処理の完全性と正確性が確保されているかについて確かめる。）
3-(2)-①-ハ	運用時の不正な操作等を発見できない。	不正な操作が懸念される部分について、企業にそうした操作を防止するための方針があり、それに基づいてログの保存や分析、及び不正が懸念される操作に対するアラート発報が行われている。	企業に、一定の操作を禁止する方針があり、この方針に沿ってログが保存されていることを確かめる。 また、大規模、高リスクなシステムの場合には、不正操作に対するアラート設定が適切に行われ、機能していることを確かめる。
3-(2)-①-ハ	情報システムが処理するデータの信頼性が保証されない。	情報システムとデータ処理のログが取得されて、ログファイルの完全性、正確性、正当性を保証される（ログが改ざんされずに記録され、保管されている）。	ログの記録や保管に際して、改ざんや削除ができないかについて確かめる。 （例えば、情報システムとデータ処理に関する操作状況を調査する。調査した時間帯のログのサンプルを取得する。入手したサンプルを基に、取得されたログの完全性と正確性を確かめる。）
3-(2)-①-ト	財務情報に係る情報システムの担当者が、リスクと適切な操作方法等について教育を受けていないと、誤操作によるシステムの誤りの防止につながる。	財務情報に係る情報システムが新しく導入されるときには、担当者に適切な教育が計画され、実施されている。	財務情報に係る担当者向け教育のカリキュラムとスケジュール、受講者を確かめる。

②　構成管理

【統制に関する指針】

構成管理は情報資産の購買、設置、固定資産管理、廃棄等の統制結果を資産情報として管理し、間接的に財務情報に係る情報システムの統制を支援する。

構成管理では、変更管理により把握されたシステム構成、ネットワーク構成、ソフトウェア構成、マスター・データ等の変更情報を利用して情報システムの構成に関わる基礎情報を一元管理することで、情報システムを正しい構成に保ち、情報システムに関わる正確な構成情報を提供する。

また、構成管理に情報資産の有効期限に対するアラート（警報）機能を持たせることで、情報資産の劣化対策時期について、管理者に注意を促すことができる。

【統制目標の例】

a．ソフトウェア、ハードウェア及びネットワークの構成管理

3-(2)-②-イ	管理ルールと手順を定め、運用責任者が承認すること。⇒*（システム管理基準　Ⅱ．２．７）*
3-(2)-②-ロ	許可された以外のソフトウェア、ハードウェア、クラウドサービスは使用禁止にすること。⇒*（システム管理基準　Ⅱ．２．７）*

b．ソフトウェア、ハードウェア及びネットワークの構成、調達先、サポート

3-(2)-②-ハ	導入や調達したソフトウェア、ハードウェア、クラウドサービス及びネットワークの記録が適切に管理台帳に反映されていること。⇒*（システム管理基準　Ⅱ．５．４）*
3-(2)-②-ニ	調達先とのサポート体制を維持すること。⇒*（システム管理基準Ⅱ．５．４）*
3-(2)-②-ホ	緊急時を含む障害対応があること。
3-(2)-②-ヘ	ソフトウェア、ハードウェア及びネットワークの設定について適切であることを確かめるためのテストと評価を実施すること。

ｃ．ハードウェア、ネットワーク及びクラウドサービスの導入並びに変更は、影響を受ける範囲を検討して対応すること

3-(2)-②-ト	想定されるリスクを明らかにして、対応すること。

【統制の例と統制評価手続の例】

	リスクの例	統制の例	統制評価手続の例
3-(2)-②-イ	ソフトウェア、ハードウェア、業務システム等が無断で設置・廃棄されることにより、誤処理やシステム停止が起こる。	情報システムの管理（購買、設置、固定資産、廃棄等）が適切に行われ、誤処理につながる情報システムが使われないようにする。	財務情報を扱う情報システムが構成管理台帳と固定資産管理に正しく反映されているかどうかを確かめる（不正な持ち込みなどの情報システムがないことを確かめる)。
3-(2)-②-ハ	変更が正しくシステム管理情報に反映されないために、システムの不整合が起きるリスクがある。	変更管理の結果が、適時、構成管理に反映されている。	・変更管理の結果と構成管理台帳を突合せ、適切な情報管理が行われているかを確かめる。 ・システム構成情報、マスター情報の変更が適切に反映されているかどうか確かめる。
3-(2)-②-ハ	管理期限の経過したハードウェア等の継続使用により、処理に誤りが起こるリスクがある。	情報資産の有効期限が適切に管理され、更新される。	・情報資産の有効期限が正しく記録され、期限に合わせて使用停止等が管理されていることを構成管理台帳で確かめる。 ・構成管理台帳の期限管理機能により、情報資産の更新がIT計画に反映されているかどうかを確かめる。
3-(2)-②-ロ	許可されないソフトウェアの使用によってデータの改変やシステムの停止が起こる。	IT資産を使用する従業員には、許可されたソフトウェア以外の使用を禁止する（従業員のPCの特権IDやアドミニストレータ権限が禁止されている)。	情報セキュリティ基本方針を入手して、許可されたソフトウェア以外の使用を禁止する方針があるか確かめる。 （例えば、財務情報に係る情報システムのサーバやPCのサンプルを調査する。このサーバやPCに無許可のソフトウェアの使用がないか調査する。）

③　データ管理

【統制に関する指針】

データ管理では、データの完全性、正確性、正当性を保証するために、財務情報の入力、登録、処理、集計、報告等の各段階に必要なデータの改ざん防止やバックアップ等の対策を行う。このデータ管理に不備があると、財務情報の信頼性が損なわれる。例えば、取引の開始の承認についての統制がないと、出力された財務情報は信頼できない。この統制は、業務システムのデータベースなどがシステムと個別に設置されて、業務処理とは独立して管理されている場合などに相当する。

【統制目標の例】

記録・処理・報告されたデータの更新及び保管のプロセスにおいて、適切に管理することで、信頼性（完全性、正確性、正当性）を保証する。

ａ．データ管理

3-(2)-③-イ	データ管理ルールと手順を定め、責任者が承認すること。⇒*（システム管理基準　Ⅱ．５．３）*
3-(2)-③-ロ	データの送受、交換、複製及び廃棄は、データ管理ルールに基づいて、誤り防止、不正防止、機密保護の対策を行うこと。⇒*（システム管理基準　Ⅱ．５．３、Ⅱ．７．２）*

ｂ．データのインテグリティの維持

3-(2)-③-ハ	情報システムの内部のデータが不正アクセス又は改ざんから論理的、物理的に保護されること。⇒*（システム管理基準　Ⅱ．５．３）*

ｃ．データのバックアップ

3-(2)-③-ニ	障害や故障等によるデータ消失等に備え、財務情報や販売管理に関するデータは、バックアップすること。⇒*（システム管理基準　Ⅱ．９．３）*
3-(2)-③-ホ	バックアップ媒体からの復旧をテストすること。⇒*（システム管理基準　Ⅱ．９．３）*

【統制の例と統制評価手続の例】

	リスクの例	統制の例	統制評価手続の例
3-(2)-③-ロ	処理結果の配布や保存について手続が定められていないと財務情報を紛失したり、伝達できなくなる。	財務情報に係る情報が適切に処理され、適切な者に適時に伝達される手続が存在する。	処理データ及び報告用出力の取扱い、配布、保存に関する手続があり、実施されているか確かめる。 （例えば、出力したデータが正しい受取人に配送されているか、権限のない人に配送された事件がないか調べる）。
3-(2)-③-ハ	データの保管や移送の際には、改ざん、複写等の可能性がある。	財務情報の保管及び移送に際して、不正アクセス、改ざんから保護する。	・財務情報の保管及び移送の際には、情報セキュリティ対策（施錠等）が実施されているか確かめる。 ・入退室管理等の物理的セキュリティ対策が施されているか確かめる。
3-(2)-③-ホ	文書やデータについては、保管が正しくなされず、重要な情報を紛失したり、無駄なデータを長期保管したりする。	文書類、データの保管期間と条件が定められている。	データの保管に関する手続を入手する。その手続に、書類やデータ報告書等の保管期間と条件が明記され、この条件に従って保管されていることを確かめる。
3-(2)-③-ホ	バックアップされていないと、データを消失した場合に、復元ができない。	データやプログラムのバックアップに関する手順があり、バックアップが採取され、保管される。	・データとプログラムをバックアップするための方針と手順を調査する。 ・データやプログラムのバックアップのサンプルを入手して、保管場所、保管状況を確かめる。

（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

⇒（*実施基準 Ⅲ．４（２）②ロｃ*）

①　情報セキュリティフレームワーク

【統制に関する指針】

財務情報や財務報告に係るITでは、特に、情報の改ざん、削除等のリスクがある。また、個人情報や機密情報の漏えいは、損害賠償等の直接的な影響だけではなく、風評リスクによる間接的な影響を財務情報にもたらされる。これらのITでは、情報セキュリティ基本方針が策定され、これに基づいて情報セキュリティのフレームワークが構築されて、遵守される。

【統制目標の例】

3-(3)-①-イ	情報セキュリティ基本方針に基づいて組織の情報セキュリティのフレームワークを構築していること。⇒*（システム管理基準　Ⅱ．５．３）、（情報セキュリティ管理基準　５．１．１）*

【統制の例と統制評価手続の例】

	リスクの例	統制の例	統制評価手続の例
3-(3)-①-イ	情報セキュリティの基本指針とフレームワークがなければ、情報システムにおけるアクセス管理が適切に実施されない。	情報セキュリティのフレームワークが構築されている。	・情報セキュリティ基本方針や情報セキュリティ対策基準、マニュアルを入手し、セキュリティのフレームワークが現場で機能しているかを確かめる。 ・情報セキュリティを維持する体制があることを確かめる。

②　アクセス管理等のセキュリティ対策

【統制に関する指針】

財務報告に係るアプリケーション・システムでは、特に、売上情報や在庫情報等の改ざん、削除等のリスクがある。これらのITでは、正当な権限を持った担当者だけにアクセスを制限する。

財務報告に係るITへの不正アクセスを防ぐためには、アクセス管理が必須となる。アクセス管理には、例えば、担当者にアクセス権限を付与する承認行為や担当者がシステムにアクセスする際の認証、入力したデータを後に否定できない否認防止、セキュリティのレベルの付与、システムの動作やアクセスを記録するモニタリング等がある。

アクセス管理を中心とした情報セキュリティに関する不備は財務情報の完全性、正確性、正当性に重大な影響を与えるおそれがある。例えば、適切なアクセス管理がなく、誰が、いつ、どこからアクセスしたか把握できない会計システムが運用されている場合には、手作業による補完的な統制が実施されていないと、不正確な財務報告につながる可能性がある。

また、サイバー攻撃によるシステム停止、情報漏えいのリスクにも留意する。これらのリスクに対しては、外部ネットワークとの接続点において、通信を必要最低限のものに制限する、通信の異常をモニタリングするツールを利用する、利用するITの脆弱性情報を適時に把握し、セキュリティパッチを適用する等の対応がある。

【統制目標の例】

ａ．アクセス制御

3-(3)-②-イ	業務上及びセキュリティの要求事項に基づいて、職務権限に対応したアクセス範囲、アクセス権限のレベルを決めていること。
3-(3)-②-ロ	担当者の登録及び登録削除のための手順が定められ、承認されていること。⇒*（情報セキュリティ管理基準　９．２．１）*
3-(3)-②-ハ	担当者の役割又は職務に変更があったり、担当者が離職したりした場合には、直ちにアクセス権が解除されていること。⇒*（情報セキュリティ管理基準　９．２．１）*
3-(3)-②-ニ	担当者IDは、適宜点検されて、長期間利用されていない担当者ID等が削除され、この記録が保管されること。⇒*（情報セキュリティ管理基準　９．２．１）*
3-(3)-②-ホ	特権IDの付与にあたっては、担当者や利用期間を限定し、そのIDに対する業務にのみ利用していること。⇒*（情報セキュリティ管理基準　９．２．３）*

ｂ．パスワードの管理

3-(3)-②-ヘ	パスワードの方針を決定し、パスワードの割当ては、全てのITに適用するアクセス手順に従って付与すること。

ｃ．ネットワークアクセスの制御

3-(3)-②-ト	担当者のネットワークへの接続は、事前に定められたルールによって制限すること。⇒*（情報セキュリティ管理基準　９．１．２）*
3-(3)-②-チ	担当者のネットワークへのアクセス権は、アクセス制御方針にしたがって、維持し更新すること。⇒*（ 情報セキュリティ管理基準　９．　１．２）*

ｄ．オペレーティングシステムのアクセス制御

3-(3)-②-リ	認可されている担当者本人の認証を行う機能があること。⇒*（情報セキュリティ管理基準　９．４．２）*
3-(3)-②-ヌ	システムへの認証の成功及び失敗が記録され、保管されること。⇒*（情報セキュリティ管理基準 12.　４．１）*
3-(3)-②-ル	特定の業務用ソフトウェアの禁止及び接続に関するアクセス制御が実施されること。

【統制の例と統制評価手続の例】

	リスクの例	統制の例	統制評価手続の例
3-(3)-②-リ、3-(3)-②-ヌ	適切な認証がないと、データへの改ざんや不正な参照が起きる。	全ての担当者の認証及びアクセス制御機能が存在し、アクセスが記録されている。	・担当者に対する認証及びアクセス制御が導入されていることを確かめる。 （例えば、担当者のアクセス範囲を文書で検証し、実際にアクセスが制限されていることを確かめる）。 ・担当者の認証やアクセス制御がログに記録されていることを確かめる。 （例えば、担当者のPCには、タイムアウトする機能等が設けられていて、タイムアウトがログに記録されることを確かめる。）
3-(3)-②-ロ	担当者のアカウントの発行、停止等の管理がなされていないと不正使用されて、データへの改ざんや漏えいが起きる。	担当者のアカウントの申請、設定、発行、一時停止、廃止に関する手続が存在しており、手順に従って適時に処理されている。	・担当者の登録、変更及び削除の手続があり、変更の都度、処理されていることを確かめる。 （例えば、新規の登録のサンプルを抽出し、責任者がアクセス権を承認したか、承認されたアクセス権が設定されたアクセス権と合致しているか、確かめる。） （例えば、退職者のサンプルを抽出し、退職後、即座にアクセス権が削除されていることを確かめる。） ・不正アクセス等違反の場合は適時に検出できて、追跡調査できることを確かめる。

	リスクの例	統制の例	統制評価手続の例
3-(3)-②-イ、3-(3)-②-ハ	適切なアクセス制御機能がなく、データへの改ざんや不正な参照が起きる。	アクセス権に関して適宜見直して、確かめるための統制プロセスが存在し、これに従っている。	・担当者のアクセス権が職務権限と一致しているかを適宜見直していることを確かめる。 （例えば、担当者が異動して、アクセス権が変更になったサンプルを調べ、アクセス権の変更が適時に実施されていることを確かめる。） ・特別にアクセス権を付与されてアクセスした等の例外事項が発生したときは、後日、適切に対処されていることを確かめる。
3-(3)-②-ト	インターネット等外部ネットワークを利用する場合は不正侵入対策が実施され、データの破壊、暗号化、漏えいが発生する。	電子商取引等にインターネット等外部のネットワークを利用する場合には、ファイアウォール、侵入検知システム等が用いられている。さらに、脆弱性評価の結果によるパッチ適用等の適切な統制が存在して、不正アクセスを防いでいる。バックアップデータを安全な環境に保管する。	・（電子商取引等でインターネットを利用している場合）ファイアウォールや侵入検知システムを含む外部からのアクセス制御が実施され、適切であることを確かめる。 （例えば、過去に、企業が情報セキュリティに関して第三者評価を実施したかを確かめる。） ・ウイルス防止システムが、財務情報に係るシステムのセキュリティを保護するために用いられているかを確かめる。
3-(3)-②-イ	職務権限が決められていないと、不正なアクセスが起きて、データが改ざんされる危険性がある。	システムとデータへのアクセス権の申請と承認に関して、職務分離がなされている。	システムとデータへのアクセス権の申請及び承認のプロセスを調べる。その際、同一人物が両方の行為を実施していないことを確かめる。
3-(3)-②-ホ	特権ユーザは情報システムの変更や担当者の追加・削除等ができるため、統制されないと改ざん等の不正が発生する。	特権については、運用基準があり、特権の付与に際して、最小限にとどめていること。利用が終わって、不要になれば、すぐに特権を停止する。	・特権IDを調査して、正しい職務に適切に付与されていることを確かめる。 ・特権IDが、全ての機能を利用できる場合には、スプリットパスワードや相互監視等（デュアルコントロールとも呼ばれる）の別の統制が併用されていることを確かめる。
3-(3)-②-イ	施設へのアクセスに制限がなければ、関係者でない人物によって重要な財務情報にアクセスされたり、改ざんされたりする。	施設へのアクセスは、権限のある者に制限されていて、適切なIDと認証が実施される。	入退室に関する方針や手続を入手し、適切な本人確認を実現できているかを確かめる。 （例えば、担当者を抽出し、入館に際して、職務に基づいたアクセス権限と一致しているか確かめる。）

〈〈コラム：サイバーセキュリティ〉〉

デジタル化の進展に伴って、企業はサイバー攻撃の脅威に直面している。フィッシングメール、不正アクセス、ランサムウェアなどのインシデントは、データ漏えいやシステム停止、金銭的損害など、企業の財務報告に深刻な影響を与えかねない。財務報告においても、サイバーインシデント（サイバーセキュリティに係るインシデントをいう。以下同じ。）に起因した決算開示の遅延等が発生し、開示すべき重要な不備につながるといった問題も生じており、サイバーセキュリティリスクへの対応の重要性が増している。

これを受けて実施基準においても「サイバーリスクの高まり等を踏まえた情報システムに係るセキュリティの確保が重要である」旨が明記され、必要に応じて企業の内部統制がサイバー攻撃に対してどの程度効果的に機能しているかを評価し、必要な対策を講じることが求められるようになってきている。つまり、財務報告の信頼性の確保だけではなく、可用性の確保も重要になっているということである。

財務報告に影響を与える代表的なサイバーセキュリティリスクとしては、情報漏えい、データ改ざん、システム停止などがあり、それに対する内部統制としては、適時のセキュリティパッチの適用や不正侵入の防御と早期検知、インシデント発生時の適切なバックアップからの復旧手順の確立といったものが挙げられる。

一方で、サイバーインシデントが発生した場合には、「サイバー攻撃を受けた領域」から「財務報告に関連する領域」を整理・特定の上、財務報告に関連する領域のデータの信頼性影響や流出可能性の程度を確認することが求められる。この確認においては顕在化している費用だけでなく、将来の費用・損失の見積もりが必要となる可能性がある点にも留意が必要である。

参考文献

日本公認会計士協会テクノロジー委員会研究文書第10号「サイバーセキュリティリスクへの監査人の対応（研究文書）」

③　情報セキュリティインシデントの管理

【統制に関する指針】

財務情報などの情報セキュリティインシデントの管理は、通常の運用の範囲を超えたアクセスや違反行為に関して文書化して担当者に周知し、実施状況をモニタリングする。

【統制目標の例】

ａ．インシデントの報告、記録及び対応ルールと手順

3-(3)-③-イ	情報セキュリティインシデントの影響度に応じた報告体制及び対応手順を明確にすること。⇒*（システム管理基準　Ⅱ．５．５）、（情報セキュリティ管理基準 16.　１．１）*
3-(3)-③-ロ	情報セキュリティインシデントの内容を記録し、情報システムの運用の責任者に報告すること。⇒*（システム管理基準　Ⅱ．５．５）、（情報セキュリティ管理基準 16.　１．２、16.　１．３）*

ｂ．事故の原因究明及び再発防止

3-(3)-③-ハ	情報セキュリティインシデントの原因を究明し、再発防止の措置を講じること。⇒*（システム管理基準　Ⅱ．５．５）、（情報セキュリティ管理基準 16.　１．５）*

【統制の例と統制評価手続の例】

	リスクの例	統制の例	統制評価手続の例
3-(3)-③-イ	情報セキュリティインシデントへの対応が適切に行われないと、被害が拡大する。	情報セキュリティインシデントが発生したとき、適時に記録されて、分析され、解決される。	情報セキュリティインシデントの報告書のサンプルを検討し、インシデントが適時に対応（記録、分析又は解決）されたかを確かめる。
3-(3)-③-ロ	承認されていない行為をモニタできず不正な行為が行われて、インシデントが発生する。	不正行為等が起きた場合に、適時に管理者に通知し、警告する機能（ユーザアカウントをロックする等）等、情報セキュリティインシデント対応の機能が整備されている。	承認されていない行為（与えられた権限を超える違反行為も含めて）が発生したときは、直ちに検知して、適時に対処できることを確かめる。また、インシデント発生後の処理プロセスが存在することを確かめる。 （例えば、過去のインシデントから違反例を調べて、該当するものがある場合、違反者について、しかるべき処分がなされ、金銭的な被害について訴追できるような仕組みがあることを確かめる。）

3-(3)-③-ハ	ログ取得されず、インシデントの原因究明ができない。	ログを安全な環境（改ざん、滅失、意図しない暗号化などが行われない環境）に、あらかじめ定められた期間保存されるようにする。	インシデント発生時に、ログを用いて原因究明できる状態になっていることを確かめる。 （例えば、過去のサーバのインシデントの例を選び、ログからインシデントの発生に至る過程を分析して解決していることを確かめる。）

（４）　委託先の管理

⇒（*実施基準　Ⅲ．４（２）②ロｄ*）

①　外部委託先との契約とそれに基づく管理

【統制に関する指針】

委託業務の管理は、財務報告に係る情報システムの開発や運用、財務情報作成等を目的として、委託先に業務を委託する場合の管理のことをいう。委託業務の情報システムの開発、運用、保守に係るリスクが、委託元企業の正確な財務報告や開示に重要な影響を与える可能性がある。例えば、委託先業者による処理の正確性に関して統制が不十分な場合、不正確な財務報告になるリスクがある。特に特定の業務を数多くの企業から請け負うクラウドサービスの利用においては、委託先業者の内部統制がブラックボックスになりやすく、当該内部統制の品質を確認するための監査権の獲得、又は当該委託業務に係る内部統制の保証報告書を入手して内部統制の状況を確認することが重要となる。

（委託に係るリスクについては、企業や委託業務内容及び形態により異なっているため、一律に示すことはできない。委託する業務の内容や形態等自社の置かれているケースを分析し、適用リスクを識別することが望まれる。さらに、再委託についても、委託元企業と委託先との契約形態や業務形態によって異なるため、再委託先のリスクが委託元に与える影響等から識別することが望まれる。）

また、財務情報の適時な入手等のために、委託業務のサービスレベルを定義し、サービスが要求通りに実施されているかをモニタリングする。

【統制目標の例】

ａ．委託計画

3-(4)-①-イ	IT戦略に基づいて外部委託利用計画を策定し、それに基づいて外部管理委託手続を定め外部委託先を選定すること。⇒（*システム管理基準　Ⅱ．２．６*）

3-(4)-①-ロ	委託業務の目的、範囲、予算、体制、責任分界点等が明確になっていること。⇒*（システム管理基準 Ⅱ．２．６）*

ｂ．委託先の選定

3-(4)-①-ハ	情報システムの開発・運用等を委託するとき、組織の委託先選定方針に従って業者選定していること。⇒*（システム管理基準 Ⅱ．２．６）*
3-(4)-①-ニ	外部委託先候補の業務提供能力の評価と財務上の適格性、契約後の業務品質の確認方法を判断していること。
3-(4)-①-ニ	外部委託先候補の拠点が国外にある場合には、その国や地域の法令、当局の規制に起因するリスクを勘案して判断していること。

ｃ．契約

3-(4)-①-ホ	契約書には、必要に応じて委託業務に関する主要なリスクに対する統制方法やその確認のための監査権（再委託先へのものを含む）を明記していること。⇒*（システム管理基準 Ⅱ．２．６）*

d.サービスレベル

3-(4)-①-ヘ	財務報告・財務情報に係る情報システムの運用を委託する場合、サービスレベルを定義し、そのレベルに維持する。そのために、委託先とサービスレベル契約（SLA）を結ぶことが望ましい。⇒*（ システム管理基準 Ⅱ．８．５）*

e．財務情報に係る情報システムの開発・運用等を委託するときの、委託業務の実施

3-(4)-①-ヘ	業務内容及び責任分担を明確にすること。⇒*（システム管理基準 Ⅱ．２．６）*
3-(4)-①-ト	委託業務の実施状況を把握し、適宜、確認すること。⇒*（システム管理基準 Ⅱ．２．６）*
3-(4)-①-チ	成果物の検収は、委託契約に基づいて行うこと。⇒*（システム管理基準 Ⅱ．２．６）*
3-(4)-①-リ	財務情報に係る信頼性について、サービスレベルをモニタリングして（例えば、委託業務の結果をサンプリング等で検証する、又は内部統制の保証報告書を閲覧するなどして）、問題があれば、業務責任者に報告すること。⇒*（実施基準 Ⅱ．２．（１）②ロａ）*

【統制の例と統制評価手続の例】

	リスクの例	統制の例	統制評価手続の例
3-(4)-①-イ	委託先とのサービスレベルの契約がセキュリティ統制について触れていないと、サービスレベルが維持できなくなり、適切に財務情報が作成されなくなる。	業務の委託前に、委託先との契約について、社内で承認され、契約書が交わされるための手続があり、これに従っている。この手続には、内部統制の要件定義と委託先の受諾条件が含まれる。	契約書のサンプルを検討し、以下の点を確かめる。 ・実施するサービスが明示されている。 ・財務報告システムに関する統制の責任が適切に明示されている。 ・委託先が、セキュリティに関する方針と手続等、委託企業の方針及び手続に準拠することを承諾している。 ・契約に際して、適切な当事者が契約内容をチェックし、承認して、署名をしている。 ・契約に述べられた委託業務の統制項目は、企業が求めているものと一致している。
3-(4)-①-ハ	委託先選定や委託先の管理方針が不明確であると、サービスレベルが維持できなくなり、委託した財務情報が適切に得られなくなる。	委託先選定方針に沿って委託先を選定する。	企業の委託先管理方針及び選定時の資料を入手して、委託先の選定や管理が方針に沿って行われているかを確かめる。
3-(4)-①-ニ	委託先選定基準が不明確で、不適格な業者を選定すると、サービス品質が低かったり、納期が守れなかったりして、財務情報の信頼性を保証できなくなる。	委託先の選定前に、責任者が候補業者のサービス提供能力の評価と財務上の存続性に関して、適格性を判断する。	委託先選定に当たっての基準を入手する。 これらの基準に、委託先の財務上の安定性、財務情報に係るIT統制に関する経験や知識（例えば、過去の類似案件の件数、資格者の数等）が含まれているかを確かめる。
3-(4)-①-ヘ	サービスレベルが定義されていないと、安定したサービスを継続して利用できず、財務情報の信頼性が損なわれる。	財務報告システムの信頼性に係るサービスレベルを定義し、管理する。	・委託契約の中で、SLAを結んでいるものを選ぶ。この契約に、サービスレベルが記述されていて、このサービスレベルに維持されていることを確認しているかを確かめる。 ・財務報告そのものを委託しているときには、結果としての財務報告の提供がタイムリーか、記載されている情報に誤りがないか検証する部署とプロセスを確かめる。
3-(4)-①-ヘ	サービスレベルが維持されていることを管理しないと、サービスレベルが低下しても気づかない。	SLAを管理するための性能指標を確立する。	サービスレベルを実際に評価したときの報告書を入手し、主要な性能指標が含まれていて、実際に測定されていることを確かめる。

3-(4)-①-ト	委託先とのサービスレベルの内容を見直さないと、サービス品質が低下していても分からない。	委託先の信頼性（完全性、正確性、正当性）のサービスレベルについて調査する。	委託先について、委託元の管理項目と水準で信頼性の実現レベルを評価していることを確かめる。 （委託業務に関連する内部統制の評価結果を記載した報告書等を委託会社から入手して、自らの判断により委託業務の評価の代替手段とすることができる。）⇒*（実施基準　Ⅱ．２（２）②ロｂ）*
3-(4)-①-リ	サービスレベルをモニタしないと、処理される財務報告の信頼性が保たれない。	委託先責任者が委託先のサービスレベルをモニタリングさせ、報告を求める。	委託先の管理責任者からの、提供されているサービスのレベルや成果の管理体制の報告を確かめる。 （例えば、委託の例を選び、契約や管理の状況を確かめる。）
3-(4)-①-リ	サービスレベルをモニタしないと、処理される財務報告の信頼性が保たれない。	委託業務の内部統制報告書を入手し、統制の内容や不備の状況を確認し、経営者に報告する。	委託業務の内部統制報告書を閲覧し、報告書の対象となるサービス範囲、統制の内容、不備の発生状況等を確かめる。

<<コラム：外部委託>>

クラウドサービスの普及により、企業のシステム外部委託が更に増加している。特に、財務報告に関わるシステムの外部委託を行う場合には内部統制が委託先に大きく依存することとなり、実施基準においても「ITの委託業務に係る統制の重要性が増している」と述べている。

適切な外部委託を行うためには、経営層が経営戦略に基づいて外部委託に関する方針を決定し、その方針に基づいて具体的な外部委託計画を策定することが求められる。

契約期間中の外部委託先のモニタリング方法としては、質問書形式や往査形式などがあるが、特に有力な手段として委託先の内部統制に関する保証報告書、いわゆるSOCレポートを活用する方法がある。SOCレポートとは、米国公認会計士協会の基準に基づく保証サービスであり、SOC1、SOC2、SOC3の3タイプがある。SOC1は財務報告に限定した内部統制を対象とし、日本公認会計士協会から公表されている保証業務実務指針3402「受託業務に係る内部統制の保証報告書に関する実務指針」に該当する。SOC2はセキュリティ、可用性、処理の完全性、機密性、プライバシーに関する保証を提供し、SOC3はSOC2の内容を一般に公開するものである。

SOCレポートを利用する際には、当該保証報告がカバーしているシステムの種類と範囲、保証の主題、保証期間、提示時期、保証業務実施者の独立性や能力を確認する必要がある。財務報告に係る内部統制の評価については基本的にSOC1レポートを利用することになるが、サイバーセキュリティリスクの増大も踏まえ、必要に応じてSOC2レポートを入手して委託先のセキュリティ等についての内部統制の状況を理解・評価することも重要である。

参考文献

※保証業務実務指針3000実務ガイダンス第４号「受託業務に係る内部統制の保証報告書に関するＱ＆Ａ（実務ガイダンス）」

※保証業務実務指針3702「情報セキュリティ等に関する受託業務のTrustに係る内部統制の保証報告書に関する実務指針」

４．IT業務処理統制

（１）　入力管理（入力統制）

【統制に関する指針】

情報システムに入力する根拠となる元データの作成、入力の実施、確認、入力に用いた元データの保管、廃棄等の管理を実施する。入力には、情報システムに対して手作業で実施する場合と電磁的記録媒体、EDI等のデータ伝送、インターネットを経由して実施する場合がある。データの入力に誤りや不正があると、このデータを処理し生成される財務情報に誤りや不正が含まれることになる。そのため、入力データに漏れや重複がなく、正しいデータが入力されるような対策が必要である。

【統制目標の例】

4-(1)-①	入力管理ルールを定め、遵守すること。⇒*（システム管理基準　Ⅱ．５．３）*
4-(1)-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。⇒*（システム管理基準　Ⅱ．５．３）*
4-(1)-③	データの入力の誤り防止、不正防止、機密保護等の対策は有効に機能すること。⇒*（システム管理基準　Ⅱ．５．３）*
4-(1)-④	入力データの保管及び廃棄は、入力管理ルールに基づいて行うこと。⇒*（システム管理基準 Ⅱ．５．３）*

【統制の例と統制評価手続の例】

	リスクの例	統制の例	統制評価手続の例
4-(1)-①	データの管理に適切なルールがなく誤りが発生、不正な入力が行われる。	入力の根拠となるデータの授受、検証、入力、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、承認等を入力管理ルールとして明文化する。	情報システムへのデータ入力に伴う一連の作業に関する入力管理ルールを閲覧し、その内容がリスクに対応する統制として十分な内容かを確認する。
4-(1)-②	データの入力に過不足が発生する。	入力管理ルールに記載されている手順に従い、入力データに欠落、重複入力等の誤りが発生しないように処理、検証をする。	入力管理ルールに記載されている手順が、入力データの欠落、重複入力等の誤りが発生しないような機能があるかを検討し、その運用を確かめる。
4-(1)-②	データの入力に誤りや不正入力が行われる。	入力管理ルールに記載されている手順に従い、誤りや不正を防止・検出し、正確に入力が行われるように正当な承認に基づいて処理、検証をする。	入力管理ルールに記載されている手順に従い、誤入力・不正入力を防止するように処理、検証する機能があるか検証しその運用を確かめる。
4-(1)-④	データの紛失、盗難、漏えいが発生する。	機密保護等のために、入力データの紛失、盗難、漏えい等を防止するため、保管及び廃棄は入力管理ルールに基づいて行う。	入力管理ルールに記載されている手順に従い、入力データの保管及び廃棄は機密保護が実施される機能があることを検証し、その運用を確かめる。

（２）　データ管理（IT業務処理統制）

【統制に関する指針】

インターネットの発達により、受注データ、購買データが企業外部で入力され、送受信される場合がある。その場合には、当該データの利用に際して信頼性が保証される必要がある。例えば、受注データを受信したときに送信元の信頼性や受信内容の正確性について、根拠となる情報との照合（事後を含む）などがプログラムや人手による検証として実施される仕組みが組み込まれていないと、受注が正当であることを検証できない。

【統制目標の例】

4-(2)-①	データ管理ルールを定め、遵守すること。⇒*（システム管理基準Ⅱ．５．３）*
4-(2)-②	データ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。⇒*（システム管理基準　Ⅱ．５．３）*
4-(2)-③	データのインテグリティを維持すること。⇒*（システム管理基準Ⅱ．５．３）*
4-(2)-④	データの授受は、データ管理ルールに基づいて行うこと。⇒*（システム管理基準　Ⅱ．５．３）*
4-(2)-⑤	データの交換は、誤り防止、不正防止及び機密保護の対策を講じること。⇒*（システム管理基準　Ⅱ．５．３）*
4-(2)-⑥	データの保管、複写及び廃棄は、機密保護の対策を講じること。⇒*（システム管理基準　Ⅱ．５．３）*

【統制の例と統制評価手続の例】

	リスクの例	統制の例	統制評価手続の例
4-(2)-①	データ管理ルールがなく財務情報の信頼性が失われる。	データの信頼性を確保するため、運用に応じたデータの取扱い、データ管理の体制等をルールとして明文化する。	データの取扱い、管理の体制等のルールが明文化されているかを検討しその運用を確かめる。
4-(2)-②	データに権限外のアクセスが行われ、誤りや不正が発生する。	データへの権限外のアクセスの防止、不正利用の防止、アクセスコントロール及びモニタリングを行う。	データへのアクセスは、正当な権限者にのみ許可されており、アクセスログが記録されモニタリングされていることを確かめる。
4-(2)-③	マスター・データが正しくないと財務情報の信頼性が失われる。	重要なマスター・データについては原本データとの一致を確認する。	重要なマスター・データについては原本データとの一致が確保されていることを確かめる。
4-(2)-③	データ更新時に財務情報に係るデータの信頼性が失われる。	データ更新の手続が定められ、データが正しく更新されたかを検証する。	データが正しく更新されているかが検証されていること及びその内容を確かめる。

4-(2)-③	データ処理の際に誤動作や不正な処理が発生する。	データの処理結果が正しい（所定の金額の範囲にあるか、関係する数値と一致するかなど）ことを検証する。	データの処理結果が正しいか検証されていること及びその内容を確かめる。
4-(2)-④	データ授受の際にデータの誤使用、不正利用、改ざん等が発生する。	データの授受はデータ管理ルールに基づき信頼性が検証されている。	データの授受は、データ管理ルールに基づいていること及びその内容を確かめる。
4-(2)-⑤	データ交換の際に誤り・不正が発生する。	データ交換の際に、誤りや不正についての検証、修正やデータの内容を確認する。	データ交換では、エラーの修正が完全に実施されるなど、誤りや不正に対する対応を確かめる。
4-(2)-⑥	データの保管、複写、不要データの廃棄の際に機密漏えいが発生する。	データの保管、複写、不要データの廃棄は適切な承認を得る等の不正防止及び機密保護の管理ルールに従って実施する。	データの保管、複写、不要データの廃棄は、不正防止及び機密保護の対策を実施していることを確かめる。

データ管理は、IT全般統制でもIT業務処理統制でも論じられている。IT全般統制のデータ管理は、IT基盤に共通するIT統制でありIT基盤全体を包括する方針である。これに対して、IT業務処理統制のデータ管理は業務アプリケーションごとの個別具体的な特質に合わせたIT統制であり、業務プロセスやアプリケーションによって異なることがある。例えば、バックアップデータの管理は、アプリケーションによる違いはなく共通であればIT全般統制で評価し、得意先からの受発注データ等の業務プロセスにより異なるものは、IT業務処理統制で評価することがある。

（３）　出力管理（出力統制）

【統制に関する指針】

出力管理は、誤りや不正等があると、財務情報の信頼性に重大な影響を与える可能性がある。例えば、倉庫の製品の出庫データの出力結果に誤りや不正があると、売上高も製品棚卸資産残高にも誤りと不正があることになる。したがって、出力管理が実施されていないと売上データの改ざんの可能性が存在して、その結果、財務情報の信頼性（完全性、正確性、正当性）を確保できない。

【統制目標の例】

4-(3)-①	出力管理ルールを定め、遵守すること。⇒（*システム管理基準　Ⅱ．５．３）*
4-(3)-②	出力情報は、漏れなく、重複なく、正確であることを確認すること。⇒*（システム管理基準　Ⅱ．５．３）*
4-(3)-③	出力情報の作成手順、取扱い等は、誤り防止、不正防止の対策を講じること。⇒*（システム管理基準　Ⅱ．５．３）*

【統制の例と統制評価手続の例】

	リスクの例	統制の例	統制評価手続の例
4-(3)-①	財務情報の元となる取引データの管理にルールがなく、誤り、不正が発生する。	出力方法の誤り、不正利用、漏えい等を防止するため、情報の出力手続、承認等のルールを定める。	出力管理に関するルールの明文化を確かめその内容（出力方法の誤り、不正利用、漏えい等）を防止するため、情報の出力手続、承認等のルールを確かめる。
4-(3)-②	財務情報の元となる取引データの出力に過不足が発生する。	出力情報に結果の誤り、欠落、二重出力等が発生しないように出力管理ルールの手順に従い制御、検証する。	出力管理ルールに記載されている手順に従い制御、検証されていることを確かめる。
4-(3)-③	財務情報の元となる取引データの出力に誤りが発生、又は不正な出力が行われる。	出力管理ルールの手順に従い、正確に出力されるように制御、検証する。	出力管理ルールに記載されている手順に従い、正確に出力されているか検証されていることを確かめる。

（４）　スプレッドシート等

【統制に関する指針】

スプレッドシート等の利用は、実務担当者の業務効率を向上させ、市販又は専門家により開発されたソフトウェア等と遜色のない利用が行われることもあり、財務報告に関する情報の信頼性に重要な影響を及ぼすこともある。一般にソフトウェアの開発や維持については情報システムの開発・運用・保守の統制に準じて行われるとよい。

しかしながら、スプレッドシート等については、実務担当者等が自ら利用することが可能であり、IT全般統制等で定められている開発の手順や記録を残さずに利用することが可能である。そのため、スプレッドシート等の利用が財務報告の作成に関わる場合は、その信頼性に関するリスクについて検討する必要がある。具体的には、以下のような対策が考えられる。

① スプレッドシート等による表や数式の作成者と利用者を区分するか、第三者が検証するような体制を整備する。
② スプレッドシート等によるプログラムの内容を文書化する。
③ スプレッドシート等と関連するデータを定期的にバックアップする。
④ スプレッドシート等が財務報告に関連する場合には、担当者以外が財務報告のデータにアクセスして内容を変更できないような体制を整備する。
⑤ スプレッドシート等の処理結果について、誤りや虚偽が発生するリスクを防ぐための対策として、再計算等の検証を検討する。

【統制目標の例】

財務報告に影響を与えるスプレッドシート等については、以下のような適切な統制を導入することにより、財務情報の信頼性を保証する。

ａ．方針と手続

4-(4)-①	財務報告に係るスプレッドシート等を利用する場合の職務権限、利用権限が定められていること。
4-(4)-②	財務報告に係る情報の作成・管理について、スプレッドシート等の利用が承認されていること。
4-(4)-③	スプレッドシート等を財務情報の作成・管理に利用する場合には、財務情報の完全性、正確性、正当性に関する方針と手続があり、遵守されていること。
4-(4)-④	財務報告に係るスプレッドシート等について文書化されており、処理の完全性、正確性、正当性が確保されていること。

ｂ．バックアップ

4-(4)-⑤	財務報告に係るスプレッドシート等とデータのバックアップを行い、安全に保管すること。

ｃ．改ざんを防止する機能や仕組み

4-(4)-⑥	利用者が、財務報告に係るスプレッドシート等の数式やマクロ等を改ざんできないようにしていること。
4-(4)-⑦	財務報告に係るスプレッドシート等に完全性、正確性、正当性を検証できる仕組み（検算できる等）が組み込まれているか、又はスプレッドシート以外の方法で検証すること。

（注：システム管理基準では、スプレッドシート等を独立した項目として扱っていない。）

【統制の例と統制評価手続の例】

	リスクの例	統制の例	統制評価手続の例
4-(4)-①	財務報告に係るスプレッドシート等で、財務情報の処理が適正に実施されていないため、結果が信用できない。	スプレッドシート等による財務情報の完全性、正確性、正当性に関する方針と手続に関するルールが存在し、これに従っている。	スプレッドシート等に関する方針や手続に関するルールを入手し、これらが正当性、完全性、正確性に関する統制に対応していることを確かめる。

	リスクの例	統制の例	統制評価手続の例
4-(4)-②	承認を受けないスプレッドシート等（PC等のIT基盤を含む）で、財務報告に係る処理が行われ処理の正当性が損なわれる可能性がある。	財務報告に係るスプレッドシート等の利用には適切な承認を受ける。	財務報告に係るスプレッドシート等の利用方針についてのルールと承認の有無を確かめる。
4-(4)-③、4-(4)-⑦	財務報告に係るスプレッドシート等では専門ソフトウェアに比べて誤処理や改ざんが起こりやすい。	財務報告に係るスプレッドシート等についてプログラムの内容が文書化されており、処理の完全性、正確性、正当性が検討されている。	実際に用いられている財務報告に係るスプレッドシート等についてプログラムの内容の文書化や処理に対する調査の状況を確かめる。
4-(4)-⑤	財務報告に係るスプレッドシートとデータ等がPCの故障等で損壊し、財務報告を適切に行えない。	財務報告に係るスプレッドシートとデータ等は、バックアップをとり、安全に保管する。	財務報告に係るスプレッドシートとデータ等のバックアップのルールとその実施状況を確かめる。
4-(4)-⑥	財務報告に係るスプレッドシートとデータ等が無断で変更され、誤った財務報告が行われる。	財務報告に係るスプレッドシートとデータ等は、アクセス制御により、不正アクセスによる改ざんや許可のない利用から保護されている。	財務担当者のハードウェア及びソフトウェアに権限のないものが触れたり、プログラムやデータの入力・修正をしたりできないことを確かめる。

（５）　IT業務処理統制のリスクコントロールマトリクス

業務処理統制では、想定されたリスクに対応するIT業務処理統制が整備・運用され財務情報の信頼性（完全性、正確性、正当性）が確保されていることが重要である。これを評価するには、リスクとコントロールの対応関係を示したリスクコントロールマトリクスを作成すると分かりやすい。この例を以下に示す。

なお、具体的なリスクコントロールマトリクスの例を、付録２「IT基盤質問書及びリスクコントロールマトリクスの例」に示す。

〈〈コラムIT業務処理統制について〉〉

業務処理における内部統制とは、個々の情報の信頼性を確保するための活動である。イメージとしては、取引等に伴う情報の入力や記録、承認、集計や分類等の各段階で行われる活動である。例えば、販売取引に関する申請の伝票が回付された場合、企業としての正当な取引と認めるために権限者による内容確認と承認が行われる。そして、承認未了の伝票は除外され、承認済の伝票が漏れなくかつ重複なく取引対象とすることで取引情報の信頼性を確保する。

このように業務処理統制は複数の統制から構成されることもあり、このような業務処理をITのプログラムにより実行するのがIT業務処理統制である。さらに、IT業務処理統制の全てがITのプログラムのみで完結するケース以外に、手作業との組合せで実施されるものもある。例えば、金額がしきい値を超えた取引をプログラムでリスト化し、当該リストに基づき適切な処理を人手で判断するという方法もある。

昨今、国内外の諸団体が内部統制に言及することがあるが、IT業務処理統制や情報処理統制のように使われている用語が異なることがある。そのことを意識して記述内容を理解することが肝要である。

５．モニタリング

モニタリングとは、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である。モニタリングにより、内部統制は常に監視、評価され、問題点に対して適切な対応、すなわち是正されることになる。モニタリングは、①日常的モニタリングと②独立的評価に区分できる（⇒*（実施基準　Ⅰ．２（5））*）。

モニタリングには、経営層、管理層、現業の各階層において問題点や例外事項を把握し対応する行為が含まれる。すなわち、現場における手順の変更等の小規模な改善、例外的事項の発生に対する管理者の緊急的な対応、経営全体の方針の変更等各階層における改善活動が含まれる。ITに関するモニタリングは、IT全社的統制、IT全般統制、IT業務処理統制のそれぞれにおいて実施される。

（１）　日常的モニタリング

日常的モニタリングは、以下の３つに分かれる。

① 経常的なモニタリング：経常的に実施され、一定の目標値と実績との差をチェックする。

② 定期的なモニタリング：定期的（週次、月次、年次等）にマスター・データ等の棚卸（マスター・データの内容について誤りがないか点検）をする、アクセスログ等をチェック（アクセス権の違反や許可されていないアクセスが起きていないかを確認）する。

③ 異常値モニタリング：異常値や、非定形的な事象の有無をチェックする。

経常的なモニタリングが、単なる報告と異なるのは、目標値が設定されていることである。経常的なモニタリングでは、目標値に対する達成度合い、又は目標に対する乖離の度合いを測ることでモニタリングを実施する。ITを利用した経常的なモニタリングは、目標と実績との差の測定が即時に、正確に測定され、報告される。

定期的なモニタリングは、例えば、決められた時期に商品マスター・データの棚卸をする等、データの信頼性（完全性、正確性、正当性）を確認することである。定期的なモニタリングは、業務取引そのものに対してではなく、データが累積されたマスター・データ等に対して実施する。例えば、マスター・データを定期的に棚卸することで、マスター・データ等の信頼性が確保され、マスター・データが最新

でかつ利用可能であることを確認できる。すなわち、定期的なモニタリングを実施することによって、情報の信頼性を維持継続することができる。

異常値モニタリングは、経営層、管理層、担当者、と各階層で行う。異常値のしきい値の設定については、経営層から管理層、担当者に順次周知され、逆に、異常値の発生についての報告は、担当者から管理層、経営層へと報告される。異常値モニタリングで検出された異常については、即時に現場に反映して改善する場合と管理層や経営層からの指示により改善する場合とがある。

なお、現在では、データアナリティクスも含め、ITの活用により、異常値モニタリングがより迅速にかつ正確に実施されるようになっている。

（２）　独立的評価（内部監査部門等による独立的評価等）

独立的評価としては、経営者、取締役会、監査役等、内部監査部門等による独立的評価があり、日常的モニタリングでは発見できないような経営上の問題がないかを、別の視点から評価するために定期的又は随時に行われるものである。また、監査役等、内部監査部門等、外部監査人等との連携が図られるとともに、内部監査部門（内部監査人）については取締役会及び監査役等への報告経路の確保が求められており、組織全般のモニタリングが有効に機能しているかに留意する必要がある。

独立的評価として行われるIT統制に関する内部監査は、IT部門以外の部門によって実施される。独立的評価の一つである内部監査においてITを利用する技法として、CAAT（Computer-Assisted Audit Techniques）と呼ばれるコンピュータ支援監査技法の利用も考えられる。なお、ITを利用する内部監査は、情報の信頼性を確認するとともに、業務に支障を生じない形式で実施する。

独立的な評価は、日常的なモニタリングと独立して実施される場合と補完的に実施される場合とがある。補完的に実施される場合の例としては、交通費等の申請で、一定金額まではシステムで自動承認処理をするが、一定金額を超えたものについては、申請内容を内部監査担当者が詳細に監査することが挙げられる。また、一定金額以下のものについても、ランダムに選択して内容を監査する等により、従業員の不正を牽制することが挙げられる（これらの検証を部門の経理担当者が定期的に日常的モニタリングとして実施する場合もある）。

一般的に、日常的モニタリングが適切に実施されている場合には、独立的評価の実施頻度を減らすことができる。

モニタリング実施の際の留意点は以下のとおりである。

5-(2)-イ	モニタリングの手続を定め、遵守すること。
5-(2)-ロ	モニタリングの指標(目標値や異常値)はモニタリングを実施する側に受け入れられ、周知されていること。
5-(2)-ハ	モニタリングの結果は、管理者に速やかに報告されること。
5-(2)-ニ	経営者は、モニタリングで問題点が検出されたときには、是正措置の優先度と緊急度を評価し、改善を実施すること。
5-(2)-ホ	モニタリングは継続的に実施されること。
5-(2)-ヘ	独立的評価を担当する部署は、財務情報に係る情報システムの開発や運用部門及び財務報告に責任のある部署と独立していること。
5-(2)-ト	モニタリングの結果は、不正調査の観点から証拠を保全すること。

【統制に関する指針】

内部統制の有効性の評価により、問題点を把握し、その是正を行い継続的な改善を実施し、内部統制の有効性を確保する。

【統制目標の例】

ITを利用した内部統制が継続的に有効に機能することにより、財務情報の信頼性を確保する。ITを利用した内部統制は、IT全社的統制、IT全般統制、IT業務処理統制に分けられる。

①　IT全社的統制のモニタリング

【統制目標の例】

5-(2)-①	組織体のITパフォーマンスが、取締役会等の意図や期待、倫理的行動、コンプライアンス上の義務を満足していることを確認するために、ITパフォーマンスの状況を適時確認して、必要な是正措置を指示する。⇒*（システム管理基準　Ⅰ．1．3）*

【統制の例と統制評価手続の例】

	リスクの例	統制の例	統制評価手続の例
5-(2)-①-イ	ITに関する問題点が報告されず、改善が実施されない。	ITに関する問題点が経営会議、情報システム委員会等、適切な管理者に報告され、その管理者が改善する仕組みがある。	経営会議や情報システム委員会等適切な管理者に対してITに関する問題点が報告され、改善措置が検討されていることを議事録等により確かめる。
5-(2)-①-ヘ	財務報告に責任ある部署がモニタリングに係る不正や誤りを発見できない。	財務報告に責任がある部署とモニタリングを行う部署は独立している。	情報システムに関するモニタリング（オンラインモニタリングと事後分析を含む）は独立した部署により実施されているか組織図や職務分掌規程等で確かめる。
5-(2)-①-ホ、5-(2)-①-ヘ	内部監査が実施されず、モニタリングが有効に機能しない。	内部監査が実施されている。	内部監査の結果が経営会議等で報告されていることを確かめる。

②　IT全般統制のモニタリング

IT全般統制のモニタリングは、IT基盤への統制が有効に機能しているかを監視し、問題点を是正するために行うものである。IT業務処理統制として実施されることが効率的である場合がある。したがって、以下に記載の項目についてIT業務処理統制として実施する場合もある。

【統制目標の例】

5-(2)-②-イ	ITシステムの利活用に関するコントロールを実行し、その結果としてのパフォーマンス、コスト、リスク管理、コンプライアンス管理、社会的責任と持続性等の状況を経営者に報告するための体制が整備・運用されていること。⇒ *（システム管理基準　Ⅱ．１．１）*
5-(2)-②-ロ	ITを利用したモニタリングの仕組みが利用され、有効に機能していること。⇒ *（システム管理基準　Ⅱ．１．１）*

【統制の例と統制評価手続の例】

	リスクの例	統制の例	統制評価手続の例
5-(2)-②-イ	IT全般統制についてモニタリング機能がないため、誤りや不正等を検出できない。	ITの日常的なモニタリングに関するポリシや手続、ルールが定められ、これに基づいてモニタリング活動が実施され、記録が保存されている。	・日常的なモニタリングについて適切なポリシや手続があるか確かめる。 ・ポリシや手続に基づいて、モニタリングが行われていることを内部監査部門等が確かめる。 （例えば、ログ等の収集と分析が行われていることを確かめる。）
5-(2)-②-ロ	連続したモニタリングでないと、不正等を検出できない。	モニタリングのログ等の情報収集は連続して行われている。	・モニタリング対象として選んだログが、全ての期間で収集されていることを確かめる。 ・内部監査部門等が実施したログ収集の分析を行っているか確かめる。
5-(2)-②-ロ	モニタリングの証拠が正しく保全され、保管されていない。	ログ等の情報は正しく保全され、保管されている。	・ログは、一定期間保管されている。 ・ログは、証拠として利用できるか確かめる。
5-(2)-②-ロ	モニタリング情報が適切な管理者に適時に報告されない。	モニタリング情報が、適切な管理者に適時に報告される仕組みが組み込まれている。	処理の異常終了等が、適切な管理者に適時に報告される仕組みが組み込まれて、機能していることを確かめる。

③ IT業務処理統制のモニタリング

IT業務処理統制のモニタリングは、業務アプリケーション・システムの統制が有効に機能しているかを監視し、問題点を是正するために行う。アクセスログの監視は、全般統制で実施する場合もあるが、特定の業務アプリケーションのアクセスログを監視すれば適正な財務報告目的を達成可能な場合は、業務アプリケーションでアクセスログをモニタリングする。

【統制目標の例】

5-(2)-③-イ	日常的なモニタリングの手順やルールが定められ、実施されること。⇒*（システム管理基準　Ⅱ．５．７）*
5-(2)-③-ロ	財務情報の信頼性（完全性、正確性、正当性）を確保する統制が有効に機能していることを内部監査で確かめていること。
5-(2)-③-ハ	アクセス記録が取得され、保存され、適宜分析されていること。⇒*（システム管理基準　Ⅱ．５．７）*
5-(2)-③-ニ	異常な事項や例外事項は、責任者に報告されること。⇒*（システム管理基準　Ⅱ．５．７、Ⅱ．５．８）*
5-(2)-③-ホ	エラーリストは分析され、問題点は修正されていること。⇒*（システム管理基準　Ⅱ．５．７）*

【統制の例と統制評価手続の例】

	リスクの例	統制の例	統制評価手続の例
5-(2)-③-イ	アプリケーション・システムについてモニタリング機能がないため、不正や誤り等を検出できない。	ITの日常的なモニタリングの手続、ルールが定められ、これに基づいてモニタリング活動が実施され、記録が保存されている。	日常的なモニタリングについて適切な手続やルールがあるか、確かめる。 （例えば、与信を超える売上計上等の例外処理の事後的レビューが管理者により実施されていることを確かめる。）
5-(2)-③-ロ	財務情報の元となるマスター・データの信頼性が損なわれる。	マスター・データを適宜にチェックする。	マスター・データのチェックが実施され、結果の分析とフォローがなされていることを確かめる。 （例えば、得意先マスターと与信限度は定期的に伝票等の元データと照合されていることを確かめる。）
5-(2)-③-ハ	財務情報に係る情報システムを入力する際に誤りや不正、機密漏えいが行われる。	一定の条件でアクセスログを検索し異常なアクセスがないかを監視する。	アクセスログによる監視が実施されていることを確かめる。 （例えば、通常時間以外のアクセスログ等による監視の実施を確かめる。）

5-(2)-③-ホ	財務情報の元となる取引データの入力に誤りが発生、又は不正な入力が行われる。	一定の項目についてエラーチェックをし、エラーリストを出す。	エラーリストを確認し、エラーが分析され修正されていることを確かめる。
5-(2)-③-ハ	財務情報に係る情報システムの内部で処理結果の照合機能がないと不正や誤りが見逃される。	財務情報に係る情報システムの内部処理において照合機能が有効に機能しているかを内部監査で確かめる。	帳簿データと販売数量や入力データを照合する機能が実現されているかの確認を実施していることを内部監査で確かめる。
5-(2)-③-ニ	モニタリング情報が適切な管理者に適時に報告されない。	モニタリング情報が適切な管理者に適時に報告される仕組みが組み込まれている。	モニタリング情報が適切な管理者に適時に報告される仕組みが組み込まれ、機能していることを確かめる。 （例えば、一定率以上の値引きは、管理者に報告されているかを確かめる。）

付録１　サンプリング

１　サンプリング実施上の留意点

業務プロセスに係る内部統制の運用状況の評価の実施方法（サンプル件数、サンプルの対象期間等）を決定する際に考慮すべき事項として、以下の２つがある。

①　内部統制の形態・特徴等

②　決算・財務報告プロセス

内部統制の形態・特徴等では、

a.　内部統制の重要性

b.　内部統制の複雑さ

c.　担当者が行う判断の性質

d.　内部統制の実施者の能力

等を考慮して、運用状況の評価の実施方法を決める。また、ITを利用して自動化された内部統制は一貫した処理を反復して継続するので、その整備状況が有効であると判断した場合には、IT全般統制の有効性を前提に、人手による内部統制よりも、例えばサンプル数を減らし、サンプルの対象期間を短くする等、一般に運用状況の評価作業を減らすことができる。⇒*（実施基準 Ⅲ．４（２）②ハ）*

２　サンプリングの種類

一般にサンプリングには、サンプリングの抽出と推定の方法の違いにより、以下の２つがある。

①　統計的サンプリング

②　非統計的サンプリング（評価者の経験等に基づくサンプリング等）

母集団全体の状況を推定する際には、一般に統計的サンプリングによる評価が向いている。

したがって、運用状況の評価においても統計的サンプリングを利用することが多くなるものと考えられる。しかし、四半期の処理、月次処理、週次処理等では、母集団が小さいため、統計的サンプリングによらなくてもよい。

３　サンプル件数

（１）　手作業による場合

サンプル件数がどの程度が適切であるかを一概にいうことはできないが、全社的な内部統制が適切である場合には、業務プロセスに係る内部統制の運用状況の評価を行うためのサンプル件数及びそのときの許容逸脱件数として、例えば、付録図表１－１の表をあらかじめ定めておいて判定することが考えられる。実施の頻度は、内部統制の評価を行う対象の数であり、例えば、「取引件数」等が挙げられる。

付録図表１－１　サンプル件数の例

実施の頻度	サンプル件数	許容逸脱件数
１日につき多数	25	0
日次	25	0
週次	5	0
月次	2	0
四半期次	2	0
年次	1	0

付録図表１－１では、「１日につき多数の内部統制の運用が行われている母集団の内部統制の有効性を評価する場合、25件のサンプルを無作為抽出し、そのサンプルの中に１件の逸脱もない場合に内部統制は有効と判断する」ということを示している。なお、１日につき多数及び日次の場合のサンプル件数は、統計的方法により求められたものである。この場合、無限大の母集団から25件のサンプルをランダムに抽出した結果、１件の逸脱も発見されなかった場合、全体としては、９%以上の逸脱がないことを信頼水準90%で説明することができる（⇒*（実施基準　Ⅲ．４（２）①ロａ）*）。なお、付録図表１－１のサンプル件数と許容逸脱件数の組合せについては、１日につき多数及び日次の場合以外は、統計的方法によるものではない。

（２）　自動化された内部統制の場合

ITを利用して自動化された内部統制は、一度内部統制が設定されると、変更やエラーが発生しない限り一貫して機能するという性質がある（⇒*（実施基準Ⅱ．３（３）⑤ニｃ）*）。したがって、付録図表１－２のような方針に基づき運用テストを実施することができる。

付録図表１－２　自動化された内部統制の運用テスト

条件	運用テスト
• 関連する全般統制の整備及び運用状況を確認及び評価した結果、全般統制が有効に機能していると判断できる場合	IT業務処理統制ごとに 1つのアプリケーションを検証する。
上記に加え、以下の３つの条件に適合する場合 • 前年度に内部統制の不備が発見されていない • 評価された時点から内部統制が変更されていない • 障害・エラー等の不具合が発生していない	４つの条件に適合していることを記録し、前年度に実施した内部統制の評価結果を継続して利用する。

付録２　IT基盤質問書及びリスクコントロールマトリクスの例

IT基盤の概要を理解するための質問書及びIT全社的統制、IT全般統制とIT業務処理統制のリスクコントロールマトリクスの例を付録２－１及び付録２－２に示す。

付録２－１：IT基盤質問書

１　IT基盤質問書の項目

内部統制の評価を始めるに当たって、財務報告の観点からITの全体像を把握する必要がある。この理解は子会社等を含めたグループ全体の財務情報に係るアプリケーション・システムと、それに関係するIT基盤の概要について把握する。その理解に当たり、この質問書はITアプリケーション・システムの状況、情報システム管理組織、ITに関する主な規程、手順書等、IT投資計画、周辺ツールの管理状況、ネットワークとセキュリティの概要、重要な開発・障害の状況、IT全般統制の評価単位などを例示している。

・ITアプリケーション・システムの状況：パッケージソフトウェア名及びバージョン情報、開発形態、稼働時期、管理主管部署、プログラム変更や障害の状況、HWやOS/DB/IFの状況、バックアップの状況や外部委託の状況など

・情報システム管理組織：情報システム部門の名称、人数、担当役員及び部門長

・ITに関する主な規程、手順書等：システム管理、開発、情報セキュリティ等の規程及びマニュアルの名称及び最終改定日

・IT投資計画：中長期を含めたシステム投資計画の状況

・財務会計に関連する周辺ツールの管理状況：アクセス管理等のシステム管理ツール、BIツール、EUCやRPA、AI等の利用状況など

・ネットワークとセキュリティの概要：ファイアウォールやアンチウイルスソフトの導入状況、サイバーセキュリティの状況など

・監査計画へ重要な影響を及ぼす可能性のある事項の検討：ITアプリケーション・システムの状況等で理解した項目のうち、重要なシステム開発等、特に重要な事項をまとめて記載する

・評価対象とするITに係る全般統制とその評価単位の識別：ITアプリケーション・システムの状況等で理解した項目を基に、全般統制の評価単位を識別する

２　IT基盤質問書の利用方法

① グループ各社情報システム担当者に質問書を送付し、回答を求める。過年度の情報があればアップデートを中心とすればよく、また、各社で有しているシステム一覧等を活用してもよい。

② 回答の内容を基に「監査計画へ重要な影響を及ぼす可能性のある事項の検討」や「評価対象とするITに係る全般統制とその評価単位の識別」を整理し、IT基盤の評価範囲及び評価計画を策定する。

付録２−２：リスクコントロールマトリクス

１　リスクコントロールマトリクスの項目

企業がリスクコントロールマトリクスを利用する場合、IT業務処理統制、IT全社的統制、IT全般統制の項目ごとに評価できるように表が掲載されている。ただし、この表は、リスク、統制目標、実際の統制の状況、整備・運用の種別、統制が予防・発見の種別、統制が自動・手動の種別、評価要件（アサーション）、統制の実施される頻度、統制の評価手続、評価及び検出事項、関連する監査調書、評価結果などを例示している。この例示は、あくまでもサンプルであり、企業は、これをベースに自社でカスタマイズして利用されたい。

・リスク：財務報告の虚偽リスクの具体的な内容で、自社が特に注目するリスクなど
・統制目標：リスクに対応する（システム管理基準）の統制目標を記入
・統制の状況（統制活動）：該当する統制の実施状況を概説
・整備・運用の種別：統制目標の整備と運用の種別
・頻度：統制の実施される頻度（四半期、毎年、毎月、毎週、毎日などがある）
・自動化・手作業の種別：統制目標がITのみで実施されるか、手作業との組合せかの種別
・評価要件（アサーション）：IT業務処理統制では、適切な財務情報を作成するための要件（評価要件）である網羅性、実在性、期間配分、権利と義務の帰属、評価、表示を記入。なお、財務諸表監査では、適切な財務情報を作成するための要件について、アサーションという用語を使用しており、実務でもアサーションが多く使用されていることから、アサーションと表記している。
・統制評価手続：どのような統制評価を実施したかの手続を記入
・評価並びに検出事項：評価の結果を記入し、特に、問題があった場合は、その

内容を記入

・調書番号：統制評価の記録などの文書や帳票類（電子媒体を含む）

・評価結果：対象としたリスクが低減されているかを記入する。リスクが「高」の場合は、統制項目の見直しが必要

２　リスクコントロールマトリクスの利用方法

リスクコントロールマトリクスの利用方法は次のようになる。

① まず、リスクを記入する。

② リスクに対する統制目標及び実施している（構築を予定している）統制の状況を記入して、関連する項目について、リスクコントロールマトリクスに記入していく。

③ 統制の状況を把握する。IT業務処理統制の場合には、どのような評価要件（アサーション）と関係するのかを概観する。統制を評価する場合には、統制評価手続を記入して統制の評価を実施する。

④ 統制を整備する場合には、候補となる統制項目をリストアップして、リスクの低減・統制目標の達成が図れる最適な統制項目を選択する。

⑤ 統制を評価する場合には、想定したリスク及び統制目標に対して、統制の状況がリスクを低減しているかを評価する。

⑥ その結果を評価及び検出事項に記入し、低減されたリスクを右端の評価結果に記入する。

付録2-1

IT基盤質問書（例）

1. ITアプリケーション・システムの状況

システムNo	財務報告に関連するITアプリケーション・システム（注2）	重要な取引種類	勘定残高又は注記事項	開発形態	稼働時期	開発・変更管理主幹部署	年間プログラム変更案件概数	直近1年間の重要なシステム開発、変更	プログラム本番移送手段（ID）	プログラム本番移送用ID概数	ユーザID管理主幹部署	ユーザID管理者権限概数	主なユーザ部門	一般ユーザID概数	運用管理主幹部署	データベース（製品名/バージョン）	左記のDB修正権限概数	直近1年間の重要な障害（注1）	左記の障害によるDB直接修正の有無（注1）	オペレーティングシステム（製品名/バージョン）	本番機ハードウェア	本番機ハードウェア設置場所	バックアップ管理ツール	媒体	バックアップ媒体保管場所	タイミング	世代管理	外部委託先（開発、運用など）	左記の外部委託内容	利用クラウドサービス名	他のシステムとの連携データ	左記の他のシステムとの連携データと連携形式	備考
1	販売管理システム（〇〇社〇〇システム）	販売管理プロセス	売掛金、売上高	パッケージ（カスタマイズ無）	2022年4月	情報システム部開発管理課	約10件/年	〇〇年4月に新規システムへ移行された。	OS特権にて本番移送	1	情報システム部運用課	5	営業部門	100	情報システム部運用管理課	XXXX	3	会計システムへの連携エラー	無	XXXX	〇〇社〇〇〇〇	本社3Fサーバルーム	〇〇社〇〇	クラウドサーバ	不明（クラウドデータセンター）	プログラム：週次 データ：日次	プログラム：3世代 データ：7世代	①〇〇社 ②〇〇社	①プログラム開発 ②データセンター利用	②〇〇社〇〇サービス	①取引先Webシステムからの受注データ ②会計システムへの売上仕訳計上用データ	①CSVにダウンロードし、アップロード（手動処理） ②パッケージ機能による夜間自動処理	
2	※以下省略																																
3																																	
4																																	
5																																	

注1：ITに重大な障害が発生している場合には、内部統制がデザインどおりに機能していない可能性があると考えられるため、過去における障害発生の有無及び障害の程度を理解する。
注2：パッケージソフトウェアの場合にはパッケージソフトウェア名及びバージョン情報も記載する。

付録2-1

IT基盤質問書（例）

2. 全社的なIT環境

(1) 情報システム管理組織		
①	情報システム管理部門名	情報システム部
②	情報システム管理部門人数	○名
③	情報システム管理担当役員	○○　○○
④	情報システム管理部門長	○○　○○
(2) ITに関する主な規程、手順書等		
①	システム管理規程	システム管理全般について規定している　○○年○月最終改訂
②	システム開発規程	システム開発全般について規定している　○○年○月最終改訂
③	情報セキュリティ管理規程	情報セキュリティ全般について規定している　○○年○月最終改訂
(3) IT投資計画について		
①	年間のシステム導入、大規模変更計画の有無と、承認組織	次年度のIT導入、大規模な変更に関する計画を策定し、3月に取締役での承認を得ている。
②	中長期のシステム導入、大規模変更計画の有無と、承認組織	3年ごとに中長期のIT導入、大規模な変更に関する計画を策定し、該当年度の3月に取締役での承認を得ている。
③	回答日以降の主な財務会計関連のシステムの導入、大規模変更の予定	○○年○月・・・○○システムの導入 ○○年○月・・・○○システムの○○機能の追加
(4) 財務会計に関連する周辺ツールの管理状況、その他		
①	システム管理ツールの利用状況	アクセス管理ツール（○○社○○）・・・プログラム本番移送管理、ID統合管理 ログモニタリング（○○社○○）・・・不正アクセス監視 ライブラリ管理ツール（○○社○○）・・・○○システムのライブラリ管理 ジョブ管理ツール （○○社○○）・・・○○システムのジョブ管理
②	帳票出力ツール、BIツールの利用と主な用途	BIツール（○○社○○）・・・債権データを取り込み、債権管理に利用
③	ワークフローシステムの利用と主な用途	ワークフローシステム（○○社○○）・・・営業管理ツールにて受注データを承認 クラウド契約システム（○○社○○）・・・営業関連の契約に利用
④	EUC（エンドユーザコンピューティング）の利用状況	原価計算をエクセルマクロで作成したプログラムで実施している。
⑤	RPA（ロボティックプロセスオートメーション）の利用状況	経費精算エクセルフォーマットから基幹システムにデータ転記を行わせている。
⑥	フィンテックやブロックチェーンの利用状況	従業員に貸与している経費精算用クレジットカードの発行会社からの支払データの自動取り込みと伝票起票を行っている。
⑦	AI（人工知能）の利用状況	天候予想から売上予測を行い、在庫発注データを生成する。
⑧	電子帳簿保存法に基づき保存される帳簿、書類と対応システム	経費精算のための領収書や請求書について、経費管理システムにより管理している。
(5) ネットワークとセキュリティの概要		
①	ファイアウォールの設置状況	○○社○○を導入している。
②	アンチウイルスソフトの導入状況とバージョンアップの状況	○○社○○を導入している。最新のウイルス定義はサーバで自動更新の上、各クライアント端末に自動配信している。
③	サイバーセキュリティ対策方針と運用の状況	サイバーセキュリティ対応計画を策定している。 社内システム・インフラ等に対するデータ漏洩や不正侵入は、外部委託し、監視している。 不定期に標的型攻撃のテストメールを配信している。
④	事業継続計画の策定状況	事業継続計画を策定している。
⑤	直近の重大なサイバーセキュリティインシデント	情報システム部社員のPCがウイルスに感染後、サーバへID、PWが解読され、その後、ネットワーク内の各種サーバが暗号化された。 いずれもバックアップ媒体より、復旧した。
⑥	ユーザ教育の状況	疑いのあるメール等を受信した場合に対応について、セキュリティ管理規程・社内システム利用ルールに定めている。 また、詐欺メール、なりすまし、フィッシング等のリスクについては、ユーザに対するセキュリティ教育を実施している。

付録2-1

IT基盤質問書（例）

3. 監査計画へ重要な影響を及ぼす可能性のある事項の検討

重要なシステム開発・変更	期中に基幹システムの入れ替えがあり、新旧両システムを対象とする。
重要なシステム障害、サイバーインシデント	○○システムの障害が発生していたが、○○のため財務報告に影響を及ぼす事項ではないことを確認した。
過年度の不備事項	システム開発プロセスに不備があり、その後の対応状況を確認する。
新技術、その他	RPAを利用しているが、財務報告に影響を及ぼす統制行為に関連していないことを確認した。

4. 評価対象とするITに係る全般統制とその評価単位の識別

関連する業務プロセス	評価対象とするITアプリケーション・システム（注3）	本番機ハードウェア（注4）	本番機ハードウェア設置場所	開発形態	開発・変更管理主幹部署	ユーザID管理主幹部署	運用管理主幹部署	評価単位（注4）
販売管理プロセス	販売管理システム（○○社○○システム）	○○社○○○○	本社3Fサーバルーム	パッケージ(カスタマイズ無)	情報システム部開発管理課	情報システム部運用課	情報システム部運用管理課	情報システム部
※以下省略								

注3：関連する業務プロセスで利用され、業務処理統制が識別されており、その結果、ITの利用から生じるリスクの影響を受ける場合にはIT全般統制の評価が必要となるため、評価対象として記載する。
注4：IT基盤の概要を基に評価単位を識別する。評価単位は、部署名、ITアプリケーション名が利用されることが多い。

付録2-2

IT全社的統制
リスクコントロールマトリクス（例）

会社名	
決算期	

作成者	
作成日	
回答者	

基本的要素	No.	リスク	統制目標	統制状況	整備運用	予防発見	文書名	頻度	サンプル数	統制評価手続	評価結果	検出事項	調書番号
ITへの対応	1	ITへの対応が組織として計画的に実施されないことにより、財務報告の信頼性が阻害される。	経営者が財務報告及び財務情報に関連したITへの対応について戦略・計画を定める。	年度経営計画の中に財務報告に関連する ITへの対応の方針を記載し、経営会議及び取締役会で承認されている。	整備運用	予防	年度経営計画 取締役会議事録	年次	1	年度経営計画の中にITへの対応についての経営者の方針が記載され、経営会議及び取締役会において承認されていることを確かめた。	有効	なし	○○
	2	ITに関連する組織の不備により、財務報告に関連するITへの対応が適切に実施されない。	ITに関する方針や計画決定のための全社的な組織が設けられ、有効に運営されている。	ITに関する具体的な方針決定と運営のため、情報システム委員会が設けられ、運営されている。	整備運用	予防	情報システム委員会規程 情報システム委員会議事録	四半期	2	「情報システム委員会規程」及び「委員会名簿」を閲覧し、その位置付けと役割を確認し、全社的な調整のために必要なメンバーが参加していることを確かめた。 情報システム委員会の議事録を閲覧し、ITへの対応に関する具体的な方針が審議され、審議結果に基づいて必要な対応が図られていることを確かめる。	有効	なし	○○
		※以下省略											
リスクの評価と対応													
統制活動													
情報と伝達													
モニタリング													

付録2-2

IT全般統制
リスクコントロールマトリクス（例）

会社名	
決算期	
事業拠点	
対象システム	

作成者	
作成日	
回答者	

分類	No.	リスク	統制目標	統制状況	整備運用	予防発見	文書名	頻度	サンプル数	統制評価手続	評価結果	検出事項	調書番号
開発・調達管理	1	システムを開発する際に不正なプログラムが埋め込まれる、また、誤ったプログラムがリリースされる。	システムを開発するための標準化された方針及び手続があり、これに基づいて、システムが開発されていること。	システム開発方針及びシステム開発規程が存在し、これに基づいて、システムが開発されている。	整備	予防	システム開発方針 システム開発規程	-	-	システム開発方針及びシステム開発規程を閲覧し、適時に更新されていることを確認した。	有効	なし	○○
	2	システムを開発する際にユーザの要件を満たさず、機能的に不十分なプログラムがリリースされる。	統制が有効に整備・運用されていることを検証するために十分で適切なテストが実施されること。	ユーザによる受入テストが実施され、テスト実施結果報告書が作成され、承認されている。	運用	予防	テスト実施結果報告書	随時	25	テスト実施結果報告書を閲覧し、実施者及び承認者の記録が残されていることを確認した。	有効	サンプル1件について、承認の記録が残されていなかった。 ※責任者の押印漏れであり、実際には、承認されているとの説明を受けた。追加テストの結果、押印漏れは検出されず、例外的なエラーであると判断した。	○○
		※以下省略											
変更・保守管理													
運用管理													
アクセス管理													
委託先管理													

付録2-2

IT業務処理統制
リスクコントロールマトリクス（例）

会社名	
決算期	
事業拠点	
対象プロセス	販売管理

作成者	
作成日	
回答者	

							アサーション														
サブプロセス	リスク	統制目標	No.	統制活動	自動化手作業	頻度	網羅性	実在性	期間帰属	権利と義務	評価	表示	整備評価手続	評価結果	検出事項	調書番号	統制上の要点	運用評価手続	評価結果	検出事項	調書番号
受注	財務情報に漏れや重複が発生する	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。 異常終了については、月次で報告が行われる。	自動化・手作業	自動 月	○		○				システム運用報告をレビューし、異常終了が担当者に報告され、フォローされていることを確かめる	有効	なし	○○	－	－	有効	なし	○○
			2	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込んでいる。	自動化・手作業	日	○	○					受注残ファイルが営業担当者により、消し込まれていることを確かめる	有効	なし	○○	✓	テスト環境にテストデータを投入し、受注残ファイルが、仕様書のロジックに従って正確かつ網羅的に出力されていることを確かめる。	有効	なし	○○
	※以下省略																				