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）
（案）

平成１９年１月１９日

経済産業省

企業の IT 統制に関する調査検討委員会　名簿

【委員長】

鳥居　壮行	駿河台大学文化情報学部　教授

【委員】

大木　栄二郎	特定非営利活動法人日本セキュリティ監査協会（JASA） 保証型監査促進プロジェクトリーダー
喜入　博	システム監査学会（JSSA）理事
郡山　信	財団法人金融情報システムセンター（FISC）監査安全部長
後藤　直樹	KDDI 株式会社　技術開発本部セキュリティ技術部 企画推進グループリーダー
島田　裕次	日本内部監査協会（IIA）
清水　惠子	日本公認会計士協会 IT 委員会　監査 IT 対応専門委員
力　　利則	日本電気株式会社　経営監査本部監査部長
西尾　秀一	社団法人情報サービス産業協会（JISA）セキュリティ部会副部会長 （株式会社 NTT データ）
原田　要之助	大阪大学大学院工学研究科　特任教授
堀江　正之	日本大学商学部　教授
松尾　明	青山学院大学　教授
松原　榮一	社団法人日本情報システム・ユーザー協会（JUAS）調査研究部会委員
丸山　満彦	情報システムコントロール協会（ISACA）東京支部副会長
和貝　享介	特定非営利活動法人日本システム監査人協会（SAAJ）副会長

（五十音順・敬称略）

企業の IT 統制に関する調査検討委員会作業部会　名簿

【委員長】

鳥居　壮行	駿河台大学文化情報学部　教授

【委員】

石島　隆	法政大学ビジネススクール客員教授、大阪成蹊大学助教授
加藤　俊哉	公認会計士
清水　惠子	公認会計士（日本公認会計士協会 IT 委員会専門委員）
田中　太	財団法人金融情報システムセンター（FISC）監査安全部 総括主任研究員
千枝　和行	社団法人日本情報システム・ユーザー協会（JUAS） 企業情報マネジメント研究会委員
中村　元彦	公認会計士
中山　清美	公認会計士
原田　要之助	大阪大学大学院工学研究科　特任教授
丸山　満彦	情報システムコントロール協会（ISACA）東京支部副会長
堀江　正之	日本大学　商学部　教授
松原　榮一	社団法人日本情報システム・ユーザー協会（JUAS）調査研究部会委員

（五十音順・敬称略）

目次

まえがき		
Ⅰ章	本追補版の構成と用語について	P1
	１．　構成	P1
	２．　用語	P3
Ⅱ章	IT 統制の概要について	P1
	１．　財務報告と IT 統制	P1
	（１）　金融商品取引法に求められている内部統制と IT の関係	P1
	（２）　財務報告と IT 統制の関係	P3
	２．　IT 統制の統制項目	P7
	（１）　IT 全社的統制	P7
	（２）　IT 全般統制	P8
	（３）　IT 業務処理統制	P10
Ⅲ章	IT 統制の経営者評価	P1
	１．　IT 統制の評価のロードマップ	P1
	２．　評価の決定と対象となる IT の把握	P3
	３．　IT 全社的統制の評価	P6
	４．　業務プロセスに係る IT 統制の評価	P7
	５．　IT 統制の有効性の判断	P13
Ⅳ章	IT 統制の導入ガイダンス（IT 統制の例示）	P1
	目次	P1
	１．ガイダンスの使い方	P3
	２．IT 全社的統制	P7
	３．IT 全般統制	P14
	４．業務処理統制	P41
	５．モニタリング	P50
参考文献		
付録	付録１．システム管理基準追補版と他の基準との対応	
	付録２．システム管理基準の統制目標の使い方	
	システム管理基準の管理項目と統制目標の対応（例）	
	付録３．ＩＴコントロールとＩＴの具体的な技術の例示	
	付録４．評価手続等の記録及び保存	
	付録５．サンプリング	
	付録６．リスクコントロールマトリクスの例	
	IT 全般統制評価記述書	
	IT 全社的統制評価記述書	
	IT 業務処理統制評価記述書	

まえがき

情報技術(以下、IT という)の急速な普及に伴い、我が国企業においては、販売、物流、調達といった業務から、財務・人事・給与等の基幹業務に至るまで、数多くの業務において IT への依存度が増大している。

平成 18 年 6 月に成立した「金融商品取引法」により、経営者は、財務報告に係る内部統制の整備及び運用について適正に評価、報告することが義務付けられたが、上記のような IT への依存度増大を背景として、金融庁企業会計審議会内部統制部会が策定中の「財務報告に係る内部統制の評価及び監査の基準案」及び「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（公開草案)」においても、内部統制の枠組みの基本的要素の１つとして「IT への対応」が掲げられている。

我が国においては、昭和 60 年に、情報システムの適正な管理を目的とした「システム監査基準」が策定され、我が国企業で広く活用されてきた。

当該基準は、近年の技術進歩や情報セキュリティ対策の重要性の増大等を踏まえ、新たに「システム管理基準」及び「情報セキュリティ管理基準」（以下、システム管理基準等という)として改訂されており、現在、我が国企業においては、このシステム管理基準等が活用されているところである。

このような状況を踏まえれば、財務報告に係る内部統制の整備運用に際して、システム管理基準等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」を行う必要に迫られている企業は多数存在していると考えられる。

しかしながら、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 統制の構築や評価について詳細までは規定していないことから、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」を行っていくためには、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していくことが不可欠である。

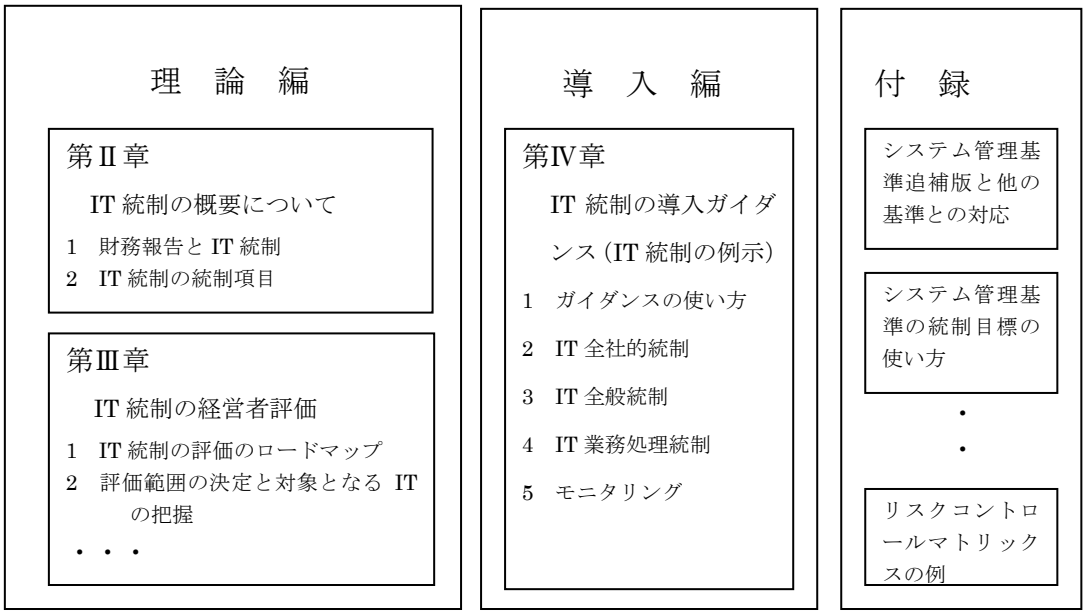
本追補版は、我が国企業が置かれているこのような現状を踏まえ、財務報告に係る内部統制を念頭に、主要なケースを想定しつつ、IT 統制に関する概念、経営者評価、導入ガイダンス等を示したものである。

なお、それぞれの企業が IT 統制をどのように構築し、経営者がその有効性をどのように評価するかについては、それぞれ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することは言うまでもなく、本追補版はこれらケースのすべてに対応しているわけではないことから、各企業は本追補版を参考にしつつも、それぞれのケースに応じた IT 統制を構築していくことが重要である。

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 統制の概要について」「第Ⅲ章　IT 統制の経営者評価」「第Ⅳ章　IT 統制の導入ガイダンス（IT 統制の例示）」「付　録」から構成されている。



第Ⅱ章は、IT 統制と財務報告との関係、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、全社的統制、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」「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 統制の導入ガイダンス」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、さら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、又は不足分を追加して、企業ごとの適切な 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「実施基準公開草案」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

「実施基準公開草案」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）」⇒*（実施基準公開草案　Ⅰ．２（４）②）*と説明され、IT を利用した情報システムと手作業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 を利用した）情報システムによる情報の分類、整理、選択、演算等、目的に応じて加工される（処理）のこと」とする。

●IT 統制の概念

「実施基準公開草案」では、「IT への対応」として以下に示す①～③のカテゴリーが示されているが、実際には②IT の利用と③IT の統制は密接な関係にある。

①IT 環境への対応	社内外の IT の活用状況
②IT の利用	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）

そこで本追補版では、「IT 統制」を②IT の利用及び③IT の統制を含んだ概念として用いる。

●「IT に係る全般統制」及び「IT に係る業務処理統制」の概念

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

IT 全社的統制	企業の統制が全体として有効に機能する環境を保証するための IT に関連する方針と手続等、情報システムを含む内部統制。 連結グループ全体としての統制を前提とするが、各社、事業拠点ごとの全体的な内部統制をさす場合もある⇒*（実施基準公開草案 Ⅱ．3（2）①）*
IT 全般統制	業務処理統制が有効に機能する環境を保証するための統制活動を意味しており、通常、複数の業務処理に関係する方針と手続のうち、IT 基盤を単位として構築する内部統制
IT 業務処理統制	業務を管理するシステムにおいて、承認された業務がすべて正確に処理、記録されることを担保するために業務プロセスに組み込まれた IT に係る内部統制

⇒*（実施基準公開草案　Ⅰ．2（6）② IT の統制 ロ）*

●IT の統制目標としての財務情報の信頼性

「実施基準公開草案」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、実施基準公開草案の定義に合わせる。

用語	実施基準公開草案	情報システム分野
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（完全性、正確性、正当性） ⇒*（実施基準公開草案　Ⅰ．2（6）② IT の統制 イｃ）*	与えられた状況下で定められた期間中に当該システムが提供する機能やサービスが期待どおりに動作し、正しい結果を出す性質をいう ⇒*（情報システムの信頼性向上に関するガイドライン、平成 18 年 4 月）*
完全性	記録した取引に漏れ、重複がないこと ⇒*（実施基準公開草案　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）*

●IT 基盤の概念

「実施基準公開草案」ではIT基盤という用語が登場する。しかし、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、外部委託の状況」と解釈する。

●エンドユーザコンピューティング（ＥＵＣ）

最近では、パーソナルコンピュータ（以下、PC という）を財務情報の計算や集計、連結決算等の目的で利用するケースが増加している。EUC の手段として、一般にはスプレッドシート（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）やデータベース管理ソフトが用いられることが多い。EUC の特徴は、入力される数式、処理を自動化するマクロ、小規模なプログラムの入力、作成や保守が情報システム部門ではなく、ユーザ部門により行われることである。EUC を利用する場合も、改ざんやエラーに対する適切な統制機能がなければ、その結果として得られる財務情報は信頼できるものとならない。しかし、「システム管理基準」では、EUC の管理項目について区別して扱っていない。それは、EUC であっても基本的な情報システム管理の考え方は同じであるからという理解に基づいているからである。しかしながら、経理部門等で利用されている EUC が財務報告に与える影響が大きいことを鑑みて、本追補版ではシステム管理基準とは異なり EUC についての統制項目を独立させて概論を述べる。

●情報システムの開発と保守について

「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機能（ソフトウェア）の開発のことをいい、保守は情報システムの機能（ソフトウェア）の維持・更新のことをいう。一方「実施基準公開草案」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、「実施基準公開草案」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、保守に伴うソフトウェアの更改等も扱われているが、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、財務情報と IT 統制について

決算・財務報告⇒*（実施基準公開草案　Ⅱ．１（１））*に係る業務プロセス⇒*（実施基準公開草案　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、IT による会計システム等であり、後者は、自動化された受注システム等である。とくに、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繋がる。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。

●IT 統制を実施する関係者について

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	組織すべての活動について最終的な責任を有しており、取締役会が決定した基本方針に基づき内部統を整備及び運用する役割と責任を持つ（代表取締役、代表執行役等）⇒*（実施基準公開草案、Ⅰ．４（1））*
情報統括責任者(CIO)	企業内の IT に関する最高責任者
担当者（権限を与えられた担当者）	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
開発者	IT 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について

「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項目と呼ぶが、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。

第Ⅱ章　IT 統制の概要について

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。なお、参考で、本追補版と他の基準との比較について述べている。

１．財務報告と IT 統制

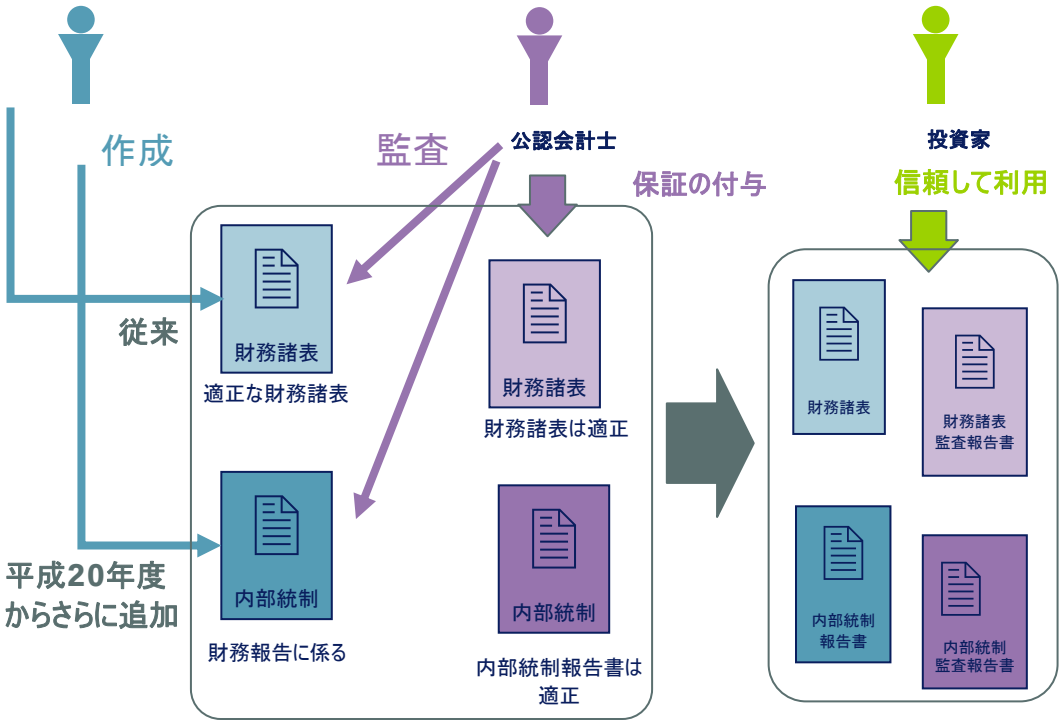
（１）　金融商品取引法に求められている内部統制と IT の関係

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、有価証券報告書を提出しなければならない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、さらにその内容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　財務諸表監査と内部統制監査について



財務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、それがあらかじめ適切な方針及び手続を定める等適切に統制されていなければならない。今日では、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

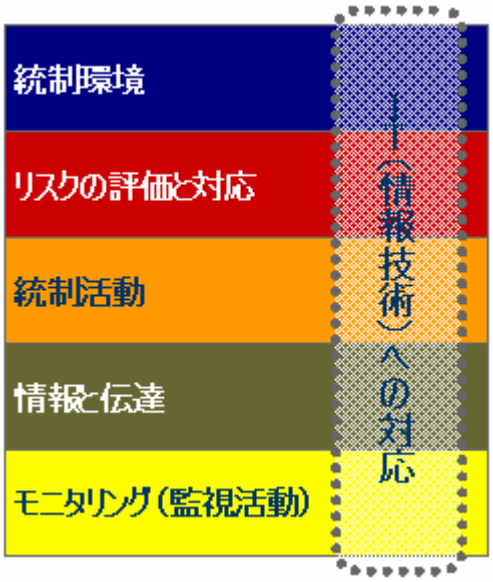
このような背景も踏まえて「実施基準公開草案」の内部統制の基本的枠組みでは、内部統制の基本的要素として、IT への対応を基本的要素として加えている。

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、すべ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つの基本的構成要素について IT を利用している場合に基本的構成要素となる。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　実施基準公開草案の内部統制と IT との関係



IT の対応は、IT 環境への対応と 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 の統制

企業は、経営戦略に沿って効果的な IT 戦略を立案し、その戦略に基づき IT の企画・開発・運用・保守というライフサイクルを確立している。企業では、この IT にまつわるリスクを低減するために、IT の統制をシステム管理基準に基づいて整備・運用している。
⇒（システム管理基準　前文）

したがって、システム管理基準を利用して IT の内部統制を整備・運用している企業は、財務情報に係る IT 統制について、システム管理基準との関係を明らかにして、IT 統制を評価すればよいことになる。

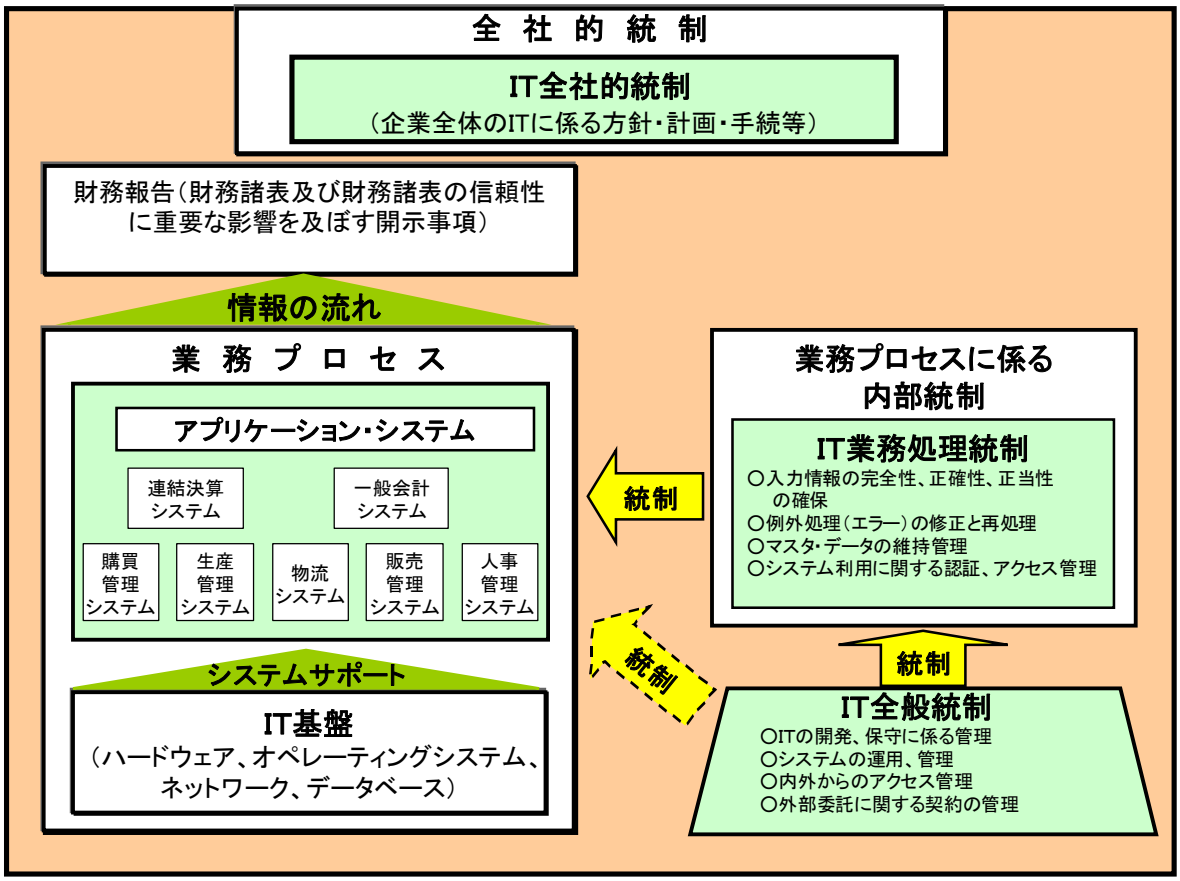
②財務報告と IT 統制の関係について

財務報告に必要な情報を作成するためには、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わっている。これらの業務プロセスは、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、財務報告を扱う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関わることになる。また、IT 基盤が、これらのアプリケーション・システムが稼動するために必要な情報システムのサポートを行う。この IT 基盤の財務情報に係る信頼性を保証する統制は IT 全般統制であり、IT 業務処理統制の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 全体に関わるものであり、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するという目的に限定しているためである。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。したがって、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



② 財務報告とアプーション・システムの関係

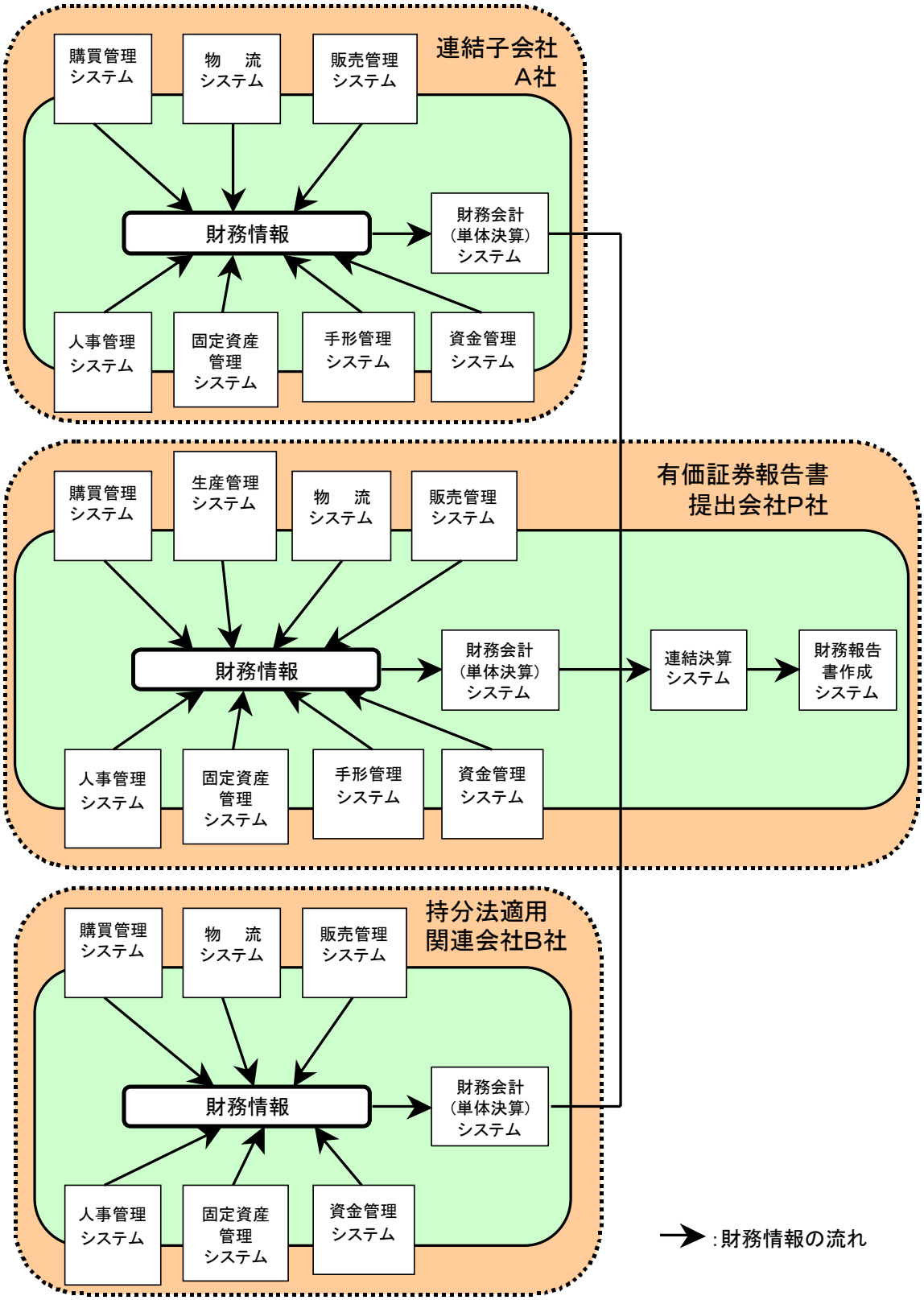
前述の財務報告に関係するアプリケーション・システムから財務報告に至る「情報の流れ」をグループ企業の場合を例に模式的に示したものが図表Ⅱ．１－４である。有価証券報告書提出会社、連結子会社及び持分法適用関連会社における各種のアプリケーション・システムで作成された情報は、財務会計システム（ここでは、単体決算のための総勘定元帳のシステムを意味し、一般会計システムと呼ばれる部分を指す）に集約される。

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、財務報告書作成システム）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。

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



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 に係わる内部統制のことであり、企業集団全体の IT を健全に維持、監督するために構築するものである⇒*（実施基準公開草案　Ⅱ．３（２））*。

②IT 全社的統制の概要

IT 全社的統制は、経営者が IT の利用について認知していること、それに伴う IT の利用業務や機能範囲が明確になっていること、導入した IT の脆弱性についてリスク評価が行われて対応されていること、財務情報の信頼性に大きな影響を与える IT の問題が発生したときに経営者に報告する仕組があること等を中心に整備を行い、運用されていることである。

IT 全社的統制は、IT の利用についての統制があることを確認する上で重要で、全社を対象として統制の存在することが確認されなくてはならない⇒*（実施基準公開草案　Ⅱ．３（２）①）*。

ａ．IT に関する基本方針の作成と明示（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。企業の CIO はこの方針にしたがって、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、その普及度合いにしたが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、従業員に対し教育が実施され、周知されているとよい。

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。また、IT 部門は、IT に係る全社的リスクに対して、分析と対応策の策定をすることになる。

ｃ．統制手続の整備と周知（統制活動）

IT は、業務の効率性や有効性を高めるだけではなく、内部統制機能に組込んで統制の質の向上を図る手段に利用することができ、業務推進側のみならず統制を行う側にも効果をもたらす。

ｄ．情報伝達の体制と仕組の整備（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、例えば、

電子メールやイントラネットなどのITを利用した伝達は全社に浸透させる上で効果的である。

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、その実施が適正に行われているか、実施部門及び内部の監査部門からの報告を通して、確認・評価作業を行うとよい。

例えば、IT を使ったモニタリング機能は適時に機能するため、内部統制を行う関係者に警告などを効率的に提供することができる。

（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、その具体例としては、①IT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等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⇒*（実施基準公開草案　Ⅰ．２（６）② ITの統制　ロａ）*。

①　IT を利用した内部統制の長所と短所

企業は、内部統制（業務処理統制）を手作業でも実施できるが、ITの利用によって、効率的かつ正確な処理が可能となる。すなわち、財務報告に係る内部統制（業務処理統制）はITで実現すると、意図的又は誤りによって変更を加えない限り、継続して機能する性質がある⇒*（実施基準公開草案　Ⅰ．２（６）② ITの統制　ロａ　①）*。

ITを利用した内部統制に短所もある。例えば、入力したデータに対する統制が組み込まれていない場合には、誤ったデータを正しいものとして後続の処理がなされる。誤った処理を検出できないため、誤ったまま実行されて、結果としての財務報告の有効性が保証されなくなる⇒*（実施基準公開草案　Ⅰ．２（６）② ITの統制　ロａ）*。

②　財務情報に係る 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⇒（システム管理基準　前文）。

一方、本追補版でいう 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、財務報告に関連す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。また、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。
- プログラムの運用では、未承認の処理や不正な処理が防止される。
- プログラムと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、プログラムとデータの復旧が適切に行われ、財務報告の信頼性が確保できればよい。そのため、事業継続計画は、企業としては推進することが望ましいが、財務情報の信頼性の評価の対象には含まれない。

③　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．IT の開発、保守に係る管理
- ソフトウェアの開発・調達
- IT基盤の構築
- 変更管理
- テスト
- 開発・保守に関する手続の策定と保守

ｂ．システムの運用・管理
- 運用管理
- 構成管理（ソフトウエアとIT基盤の保守）
- データ管理

ｃ．内外からのアクセス管理等のシステムの安全性の確保
- 情報セキュリティフレームワーク
- アクセス管理等のセキュリティ対策
- 情報セキュリティインシデント（事故）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

⇒*（実施基準公開草案　Ⅰ．３（２）ニａ）、（システム管理基準）*

（３）IT 業務処理統制

IT 業務処理統制とは、業務を管理する IT において、承認された業務がすべて正確に処理、記録されることを確保するために業務プロセスに組み込まれた内部統制のことである。

⇒（実施基準公開草案　Ⅰ．２（６）② IT の統制ロｂ）

① 情報処理と IT 業務統制の関係

情報処理そのものは、IT 業務統制ではない。例えば、リベート計算をする際、IT を利用した計算は情報処理そのものであり、リベート計算が承認された規則に沿って正確に実施されているか確かめることが統制である。すなわち、リベート計算の結果が一定の幅に収まっていることを IT で制御する仕組が IT 業務処理統制である。また、リベート計算の担当者が一部を手計算等で確認することも統制である。（なお、リベート計算を IT 業務処理統制として評価するときには、情報処理と統制を区分せずに、IT 業務処理統制とみなすことがある。この評価では、リベート計算の信頼性が最終的に確保されていることを確かめることになる。）

② 業務処理統制における IT と手作業の統制手続の関係

業務処理統制は、販売、購買等の業務プロセスの中のアプリケーション・システムに組み込まれた統制である。業務処理に IT を利用している場合に、業務処理統制は IT による自動化された統制（IT 業務処理統制）と手作業との組み合わせで実施される。

例えば、入力データが承認されていることを検証する機能が IT に組込まれていない場合には、業務プロセスにおいて、取引の最初の入力データの申請、承認を手作業で実施することになる。この場合、IT では入力データが正式な承認を経たものかどうかの判断を行えないので、手作業による統制が行われないと、入力データが信頼できないことになる。最初の手作業による申請、承認の統制が適正であれば、それ以降の業務処理システムを流れる情報の信頼性が担保される。

例えば、販売プロセスの取引の開始から財務報告作成までのプロセスの情報の流れの中で、最初の受注データが誤っていた場合には、誤出荷や誤請求につながり、売上データも誤ったものになる。

③自動化された IT 業務処理統制

従来、ホストコンピュータを利用した情報システムでは、手作業による入力の確認作業、出力結果と伝票との照合による統制で、全体としての統制を構築していた。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た。

一方、インターネットの普及によって、Web での受注や EDI を利用する受発注システムでは、手作業を経ないで自動化された情報システムの内部で、IT 業務処理統制が実施されることがある。このような業務プロセスではプログラムに組込まれて信頼性（完全性、正

確性、正当性）の統制を実現している。この統制は、業務システムの開発段階で組込まれ、本番で利用する前にテストされている。

④IT 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 統制は、会計上の取引記録の信頼性（完全性、正確性、正当性）を確保するために、業務処理の入力プロセス、出力プロセス、内部プロセスにおいて、以下の統制が実施される。

・入力管理
・出力管理
・データ管理

IT 業務処理統制の具体例としては、以下のような例がある

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

⇒*実施基準公開草案　Ⅰ．２（６）② IT の統制 ロｂ*

- エンドユーザコンピューティング

なお、IT 業務処理統制については、トランザクションの統制と、ファイルやデータベースなどの統制がある。トランザクションの場合は、業務処理で扱われる取引データの信頼性（完全性、正確性、正当性）が統制目標となる。一方、ファイルやデータベースの場合は、記録されたマスタテーブルが最新であり、関連するマスタ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（維持継続性）及びマスタ・ファイルの信頼性（完全性、正確性、正当性）があることが統制目標となる。この場合、マスタ・ファイルに記録されているデータと本来あるべきデータとをファイルマッチングすることで、マスタ･ファイルの信頼性が確保できる。例えば、与信限度額のマスタ・ファイルの信頼性は、与信規程にしたがって修正された与信限度額のリストと照合することで担保される。

⑤EUC（エンドユーザコンピューティング）について

企業では、財務担当者等が PC を利用して財務報告に係る集計処理等に EUC を利用するケースがある。この EUC には、財務担当者によるスプレッドシート（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)、データベース管理ソフト等が含まれる。

財務報告に係る情報処理で EUC を利用するときの問題として、多くの企業においてユーザ部門により行われ、また、利用者の PC が利用されるため、全社的な管理から漏れていることが考えられる。そのため、スプレッドシートや作成されたデータのバックアップが十

分でないことがある。財務情報を処理するという観点からは、計算式等の誤りや決算データの恣意的な修正等、虚偽記載につながる可能性について考慮しなければならない。

また、会計処理の結果を表計算ソフトから出力し、別のアプリケーション・システムにこのデータを読み込み、財務報告を作成する企業もある。この場合にも、データ転送時にデータの欠落や改ざん等によって虚偽記載につながるリスクがある。

したがって、経営者は、これらのリスクを十分に認識し、データや処理の正確性を確保するための統制を考慮する。企業の置かれている状況や EUC の利用状況によって異なるが、管理体制（当事者以外による点検等）や手続の整備、利用者に対する意識付けなどを行うとよい。また、表計算ソフトなど EUC で処理している内容を、当事者以外が再計算することで統制機能を代替することできる。経営者は、虚偽表示のリスク、対策のコスト、統制の効果等を勘案して、自社に適した方法を選択する。

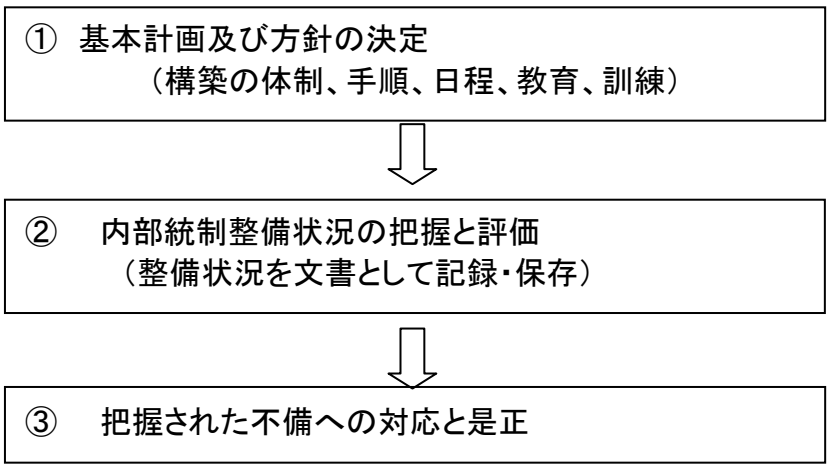
第Ⅲ章　IT 統制の経営者評価

１．IT 統制の評価のロードマップ

（１）　内部統制構築の流れ

経営者は、内部統制を整備･運用する役割を担っており、財務報告に係る内部統制の評価の信頼性を確保する中で IT 統制の整備・運用の評価を行う。評価の流れを、図表Ⅲ．１－１に示す。IT 統制については、内部統制整備の一部として評価することになる。

図表Ⅲ．１－１　財務報告に係る内部統制構築のプロセス



①　基本計画及び方針の決定

企業の内部統制構築については、経営者自らが内部統制にどのように IT を利用するかを決定することになる。IT の利用は必須の内部統制の基本的要素ではないが、IT を業務処理に利用する場合には、内部統制構築の基本方針に IT の利用、IT の導入方針、期間、体制、教育等を加えて決定する。また、評価方法についても方針を検討する。IT そのものや IT 統制については専門的な知識が必要であること及び評価の独立性と客観性の観点から、情報システム部門以外の監査部門設置や外部専門家の利用の方針を決定する⇒*（実施基準公開草案　Ⅱ．３（１））*。

②　内部統制整備状況の把握と評価

経営者は、自社の既存の内部統制に関する規程、慣行、遵守状況、IT 統制等を総合して内部統制の整備・運用状況を把握し、記録・保存する。その際、重要な勘定科目に係る業務プロセスについては、リスクの大きさによって評価の対象に追加する。この追加された業務プロセスに IT が係っている場合には、IT 統制も評価対象となる⇒*（実施基準公開草案　Ⅱ．２（２））*。

③　把握された不備への対応と是正

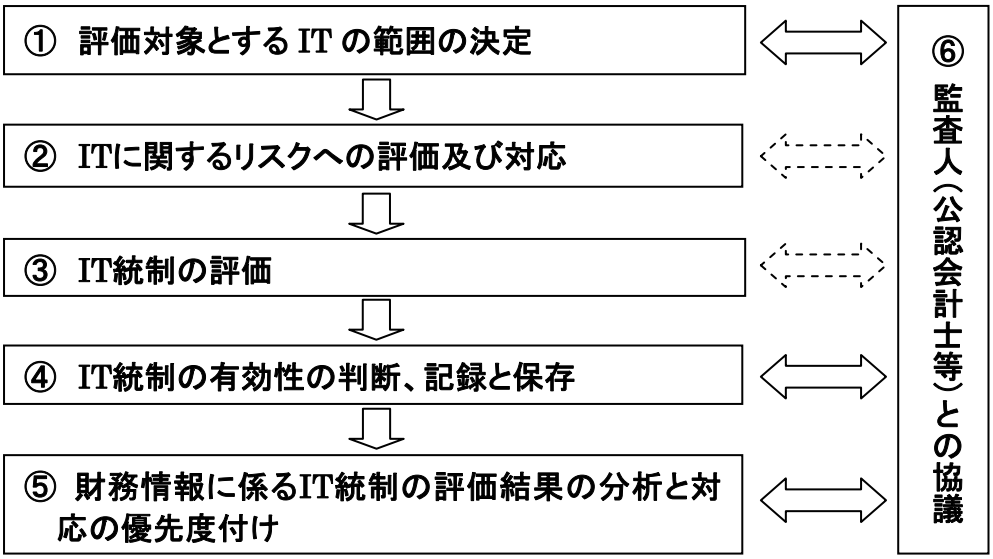
全社的な内部統制に不備がある場合には、業務プロセスに係る内部統制に与える影響と財務報告に虚偽記載をもたらす可能性について慎重に検討することになる⇒*（実施基準公開草案　Ⅱ．３（１））*。

また、全社的な内部統制に不備があっても、業務プロセスに係る内部統制が機能することもある。ただし、全社的な内部統制に不備がある場合には、全体としての内部統制が有効に機能する場合は限定される。これは、IT 統制についても同様である⇒*（実施基準公開草案　Ⅱ．３（４））*。

（２）　IT 内部統制評価の流れ

図表Ⅲ．１－１の②「内部統制整備状況の把握と評価」における IT 統制の評価のロードマップを図表Ⅱ．１－２に示す。

図表Ⅲ．１－２　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．２節「評価範囲の決定と対象となる IT の把握」に述べる。

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わ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（例えば、ソフトウェア処理を行うことで数字の改ざんをできなくすることやデ

ータベースを利用することで、権限のない変更ができなくする等）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。とくに、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

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

④ IT統制の有効性の判断、記録と保存

Ⅲ．５節「IT統制の有効性の評価」と、付録４「記録と保存」に述べる。

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、業務処理統制が依存する全般統制）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。内部統制の実現は、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。

⑥ 監査人（公認会計士等）との協議

IT 統制の評価においては、早期に監査人との協議が望ましい⇒*(実施基準公開草案　Ⅱ．２（２）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、監査人から不備を指摘される可能性がある。とくに、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、IT 統制を整備する初期段階で、監査人と IT の評価範囲について協議しておいて、認識を一致させておくことが望まれる。このような協議は、②～⑥の各段階でも適宜行うことが望まれる。

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あたって、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、グループ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おればよい。

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⇒*（実施基準公開草案　Ⅱ．２（１）①）*。グループの決算･財務報告プロセスに係る IT は、すべて 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

勘定科目を業務の流れとデータの流れとで把握して記入すると分かりやすい⇒*（実施基準公開草案　Ⅱ．参考２）*。

IT に関して把握すべき内容は、以下の項目である。

図表Ⅲ．１－３　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・ネットワーク等の概要、外部委託の状況等）
- IT に関与する組織、方針

⇒*（実施基準公開草案　Ⅱ．３（３）⑤ロ）*

（４）評価範囲の決定にあたっての留意事項

①　全社的統制に関係する IT の評価について

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 が利用されているときには、こうした IT も評価の範囲に含めることがある。

例えば、LAN 等の社内のネットワークが、統制環境、リスクの評価と対応、情報と伝達、モニタリング等において重要な役割を果たしているときには、社内ネットワークを評価す

ることがある。また、ある業務プロセスから重要な情報が自動的に経営者に発信され、端末でチェックされることによって、経営者のモニタリングが確保されるシステムとなっているときには、情報の自動発信を行っているアプリケーション・システムを評価することがある。このようなネットワークや、アプリケーション・システムは、評価すべき IT の範囲に含めて、業務プロセスの評価段階で、IT 業務処理統制、IT 全般統制の評価を実施することになる。

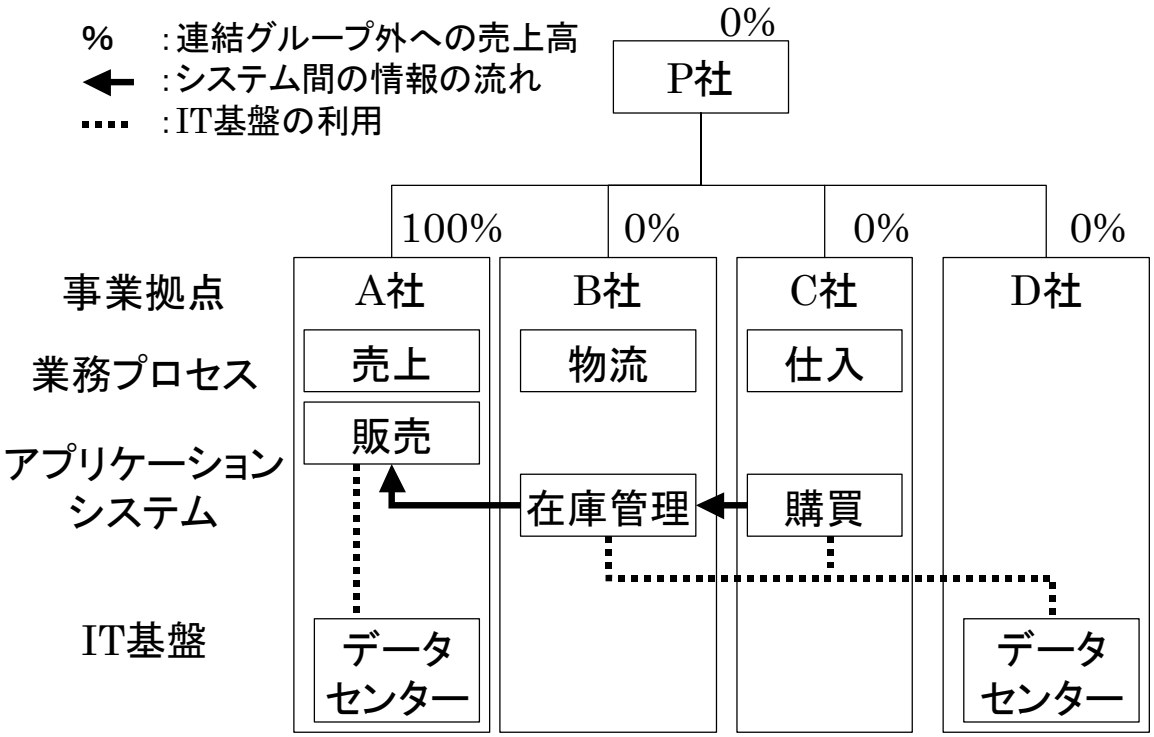
②　IT と組織区分の相違について

決算・財務報告以外の業務プロセスに係る内部統制の評価範囲は、売上高等によって、本社、子会社、支社、支店、事業部等の事業拠点が対象として一旦選定される⇒*（実施基準公開草案　Ⅱ．２（２）①）*。しかし、事業拠点の組織区分と業務プロセスは、必ずしも一致していない場合があり、業務プロセスに含まれるアプリケーション・システムも、対象として選ばれた組織区分と一致しない場合がある。例えば、図表Ⅲ．２－１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物流プロセス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係わらず、売上高に関係する業務プロセスとして、当該子会社の出荷業務を評価範囲に含めることになる。

一方、IT 統制の評価の観点からは、出荷情報の処理を行うアプリケーション・システムを評価するには、IT 全般統制も評価対象となることもある。例えば、IT 基盤が別の子会社に所属するデータセンタで運用されている場合には、子会社の売上高に関係なく、そのデータセンタをも評価範囲に含めることになる。そのため、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．２－１の例では、販売、在庫管理、購買の各アプリケーション・システムと、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は、すべて IT 統制評価の対象となると考えられる。

なお、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、監査人と協議を行っておくことが適切である⇒*（実施基準公開草案　Ⅱ．２（２）②ロ d）*。

図表Ⅲ．２－１　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

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基本である。例えば、ネットワークの整備・運用の方針や利用する基本ソフトウェア、プラットフォーム等の選択の方針が全社的に確立され実施されていれば、IT に関する企業の管理体制が一定のレベル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。一方、例えば、全社的な方針が徹底されていないなどの不備があり、IT 全社的統制が不十分な場合には、ネットワークや基本ソフトウェアがアプリケーション・システムごとに整合性なく構築されていることが考えられる。そのため、IT 基盤ごとに個別に評価することになる。各アプリケーション・システムを接続する IT 基盤のインタフェースについても同様である。

IT 全社的統制の評価では、図表Ⅲ．２－２に示す点に留意する。

図表Ⅲ．２－２　IT 全社的統制の評価における留意点の例

①．経営者が内部統制を支える IT の重要性について認識している：これが全社的統制のベースとなる。
②．経営者が財務情報に係る IT の信頼性について、リスクの評価と対応を検討している：リスクへの対応方針が、全社的な方針、規程となる。

③. 経営者が財務情報に係る IT の整備・運用に係る予算を承認している：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、この承認がないと整備・運用は不可能である。
④. 財務情報に係る IT の整備・運用の状況につき経営者が適宜報告を受け、改善が行われる仕組がある：情報と伝達及びモニタリングによって PDCA サイクルが確立される。
⑤. IT 統制に係る記録の採取と保存に関する規程や体制が存在する：これがないと後日、経営者による評価や監査人による監査に支障をきたすことがある。

（2） IT 全社的統制の評価

IT に係る規程類の内容が不十分である場合や、従業員への周知・徹底が不十分である場合は、各事業拠点のすべてが、均質で同じ水準の IT 統制が行われていない可能性がある。その場合は、全社的な方針がないので、すべての主要な業務拠点について、IT 全般統制及び IT 業務処理統制の評価を実施することになる。

また、企業の IT に関する戦略や計画が不明確なため、大規模システムの更改に失敗し、業務に混乱が生ずることで、財務報告に誤りが含まれたり、財務諸表そのものが作成できなくなったりする可能性が高まれば、経営者は重要な欠陥と評価することになる。

（3） IT 全社的統制が不十分な場合の事例と教訓

IT 全社的統制が不十分な場合の事例として、巨大銀行の合併の際に、システム統合に不具合が生じ ATM が長期間停止したり、振込等のサービスが不可能になり、企業の存続にも影響しかねない問題が発生した例を挙げることができる。この事例では、経営者が事業統合について IT の重要性（システム統合や負荷等によるリスク）を認識していなかったことが、問題の原因と考えられる。

このように、重要なシステムの新規開発や大規模なシステムの変更が予定されている場合、それらが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

（1） 業務プロセスに係る IT 統制の意味

① IT 全般統制

IT に係る全般統制とは、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。

⇒*（実施基準公開草案　Ⅰ．２（６）② IT の統制 ロ a）*

経営者は、IT に係る全般統制が、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。

・IT 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等のシステムの安全性の確保
・外部委託に関する契約の管理
⇒*（実施基準公開草案　Ⅱ．２（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.　IT の開発・保守
- IT に関する開発(含む調達)業務では、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、並びに 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 IT に関する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取引を防止する機能を組み込んでいない等、完成した IT の信頼性が期待できないことがあることに留意する。また、開発業務に関しては、ユーザ部門の参画による十分なテストが実施されているかを評価する。また、保守に関しては、プログラム等の移行や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.　情報セキュリティ
- 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、破壊等を防止するために、アクセス管理や自然災害等への対策のための統制を整備・運用しているかを評価する。

d.　外部委託
- 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。
- 外部に委託している業務が基幹業務の一部である場合には、委託先におけるシステム障害が、委託元の業務の運営に支障をきたす可能性がある。したがって、経営者は、委託先との間で合意されているサービスレベルが管理されているかを評価する。

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、承認された業務がすべて正確

に処理、記録されることを確保するために業務プロセスに組み込まれた IT に係る内部統制である⇒*（実施基準公開草案　Ⅰ．２　（６）②IT 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⇒*（実施基準公開草案　Ⅱ．２（３）⑤ニ b)*。

経営者が、企業の財務報告の信頼性を確保することに関連する IT 業務処理統制を理解するにあたっては、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）

経営者は、IT 業務処理統制を評価するにあたって、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要件（以下、アサーションという、また、経営者の主張ともいう）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。

経営者は、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活動が、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ウォークスルー(財務報告目的の IT における取引の開始から財務諸表の作成までを追跡すること）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

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

業務プロセスは、実施基準公開草案では、２つに分類されている。⇒*（実施基準公開草案　Ⅱ．２（２)*。

① 決算・財務報告プロセス

② 決算・財務報告上記以外のプロセス

①「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・財務報告に関わる業務プロセスであり、原則として、全社的な内部統制に準じてすべ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、会計システム、連結パッケージ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 EUC で利用する場合があり、このよ

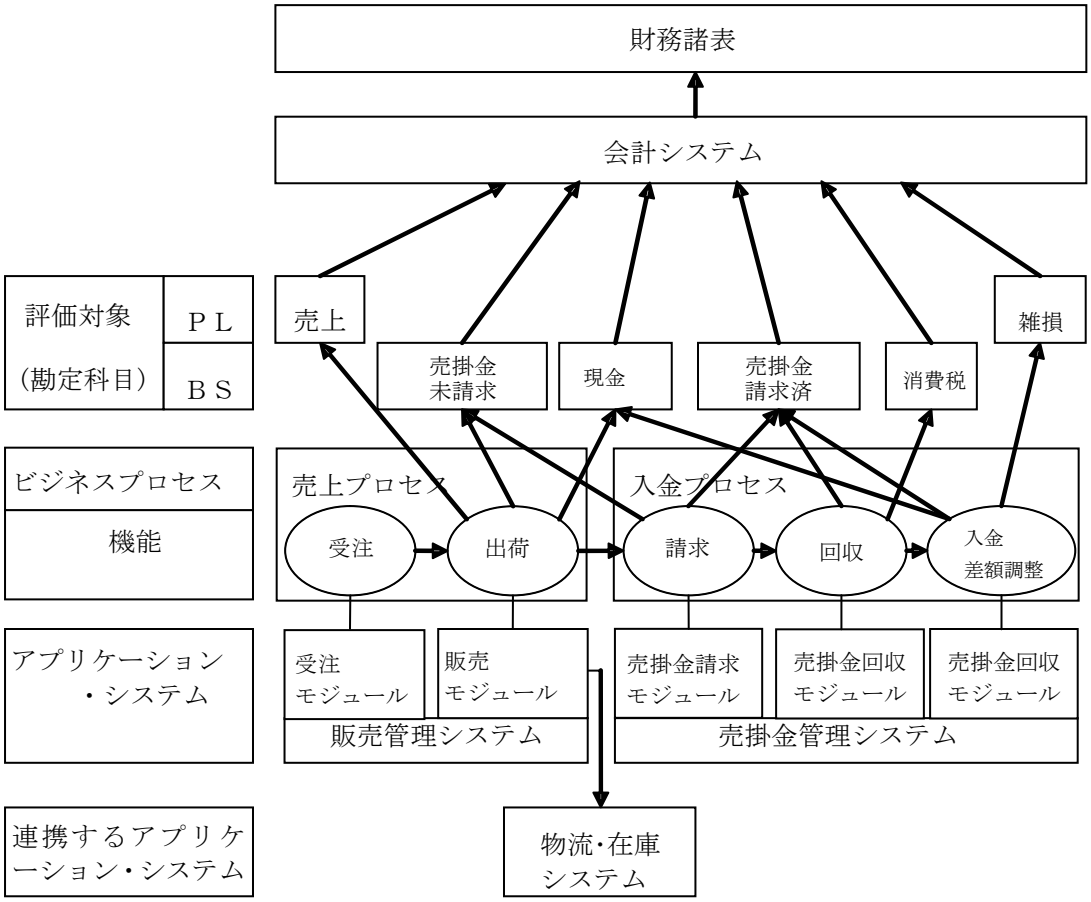
うな場合には、計算式のコピー忘れや計算式の誤りが財務報告の正確性や網羅性に直接影響する。したがって、EUC を利用している場合には、EUC の統制についても評価することになる。

一方、②「決算・財務報告以外のプロセス」については、業務プロセスの機能と関連する情報システム（業務アプリケーション・システム）の概要及び業務プロセスの働きと財務情報の流れを把握することになる。

図表Ⅲ．４－２では、販売サイクルの中で、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（財務報告）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、財務報告が作成される。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。このように、「どのアプリケーション･システムの取引データが財務情報となるか」の概要の把握が必須である⇒*（実施基準公開草案　Ⅱ．３（３）⑤ハ）*。

なお、図表Ⅲ．４－２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．４－２　勘定科目とアプリケーション・システムの関係



（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、IT に係る不正又は誤りにより、財務諸表が虚偽となるリスクを識別する。

このリスクを低減させる IT 統制を検討するにあたっては、アサーションと IT の統制目標の関係を考慮する。IT 統制は経営者が構築するものであるが、IT 統制を有効なものとするために経営者が設定する目標（IT の統制目標）は、必ずしも適切な財務情報を作成するためだけではない。

しかし、経営者は、内部統制の評価において、この IT の統制目標のうち企業のシステムが信頼できる情報を提供しているか否かの判断指針（正当性、正確性、完全性）となるものを、適切な財務情報を作成するための要件と関係付けることによって利用することができる。

例えば、IT の統制目標である「完全性」は、販売プロセスにおいて、すべての顧客の注文分の商品を漏れなく重複なく発送するという販売業務のために設定される。また、この

「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というアサーションとしての「網羅性」の確保と結びつく。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の発生を低減する統制にあたる。図表Ⅲ．４－３に IT の統制目標とアサーションの関係を整理した例を示す。

図表Ⅲ．４－３　IT の統制目標とアサーションの関係の例

IT の統制目標	アサーション
完全性	網羅性、期間配分の適切性、
正確性	実在性、評価の妥当性、期間配分の適切性、表示の妥当性
正当性	実在性、権利と義務の帰属、評価の妥当性

なお、IT 統制目標には、この他に、記録されたマスタテーブルが最新であり、関連するマスタ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（Ⅱ章（３）④）がある。

経営者は、内部統制の評価において、全社的な内部統制と業務プロセスに係る内部統制が相互に影響し合い、補完する関係にあることに留意する。これは IT 統制についても同様である。

内部統制は企業のリスクマネジメントとして費用対効果を勘案して構築すべきものであるため、企業の行う業務の性質等により、全社的な統制と業務プロセスに係る統制のどちらに重点を置くべきかが異なることがある。

リスク評価の例として、自社開発をせず、市販の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を例示する。この場合、リスクの評価にあたり、図表Ⅲ．４－４に示す点について留意する。

図表Ⅲ．４－４　パッケージソフトウェアのリスク評価の例

- あらかじめ一定の機能が設定されているため、プログラムに変更を加えていない場合は、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。
- 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、不正な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、業務の一貫性が確保され、照合手続が自動化され、例外事項報告書の作成や職務分掌の実施が容易となるので、リスクが限定される。

ただし、市販の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や独自のプログラム変更を加えた場合は、図表Ⅲ．４－４のようなリスク評価となら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アクセス制御等の運用上の統制は要請される⇒*（実施基準公開草案　Ⅰ．（６）②　IT の統制　ロ a）*。

５．　IT 統制の有効性の評価

（１）　IT 全社的統制の有効性の評価

①　IT 全社的統制の有効性の評価

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

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、それらが重要な欠陥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。ただし、IT 全社的統制に不備がある場合は、IT 全般統制と IT 業務処理統制の評価範囲を広げる。例えば、多くの店舗があり、IT 全社的統制として、「店舗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を拡大する。

（２）IT に係る業務プロセスの内部統制の有効性の判断

①　業務プロセスへの IT 統制の整備状況及び運用状況の有効性の評価

IT を利用した内部統制の評価では、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もある。

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）と、証憑書類（領収書等裏付けとなるもの）との照合 ・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 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につながるものではないため、直ちに重要な欠陥と評価されるものではない。

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、IT 全般統制としての運用体制が有効に機能していない場合には、当該 IT 業務処理統制の有効性が成り立たないこともある。例えば、プログラムの変更についての文書化が十分でない場合に、開発段階での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、不備とは見なさなくてもよい場合がある。

IT 全般統制の不備は IT 業務処理統制と密接に関連するため、不備の影響度合いと不備によって財務報告の虚偽記載が発生する可能性について評価を行うことが重要である。なお、IT 全般統制の不備が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につながるものではなくても、速やかに改善することが求められる。⇒（実施公開草案基準　Ⅲ．４（３）③）

③　IT 業務処理統制に不備がある場合

IT 業務処理統制のうち、自動化された統制活動に不備がある場合は、不備が繰り返されていないか留意する。例えば、受注処理において、顧客コードが誤っていて、それを検出する仕組がない場合、不備が繰り返され、虚偽記載のリスクがある。このように IT 統制に不備がある場合、他の統制で不備を補うことがある。なお、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に与える影響を十分に検討する。

第Ⅳ章　IT 統制の導入ガイダンス（IT 統制の例示）

本章では、システム管理基準追補版を実際に利用する場合のための例示を行う。最初に、リスクと統制をどのように関係付けるかについて述べ、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。なお、ここで示すものは、例示であり、全ての業種・企業に当てはまるものではない。

本章の目次

１．ガイダンスの使い方 3

（１）リスク要因について 3
（２）リスクの評価 3
（３）IT統制目標の選択プロセスとシステム管理基準 5
（４）本章の利用に際しての留意点 6

２．IT全社的統制 7

（１）　ITに関する基本方針の作成と明示（統制環境） 7
（２）　ITに関するリスクの評価と対応（リスクの評価と対応） 8
（３）　統制手続の整備と周知（統制活動） 10
（４）　情報伝達の体制と仕組の整備（情報と伝達） 11
（５）　全社的な実施状況の確認（モニタリング） 12

３．IT全般統制 14

（１）　情報システムのソフトウェアの開発・調達 14
①　ソフトウェアの開発・調達 14
②　IT基盤の構築 16
③　変更管理 17
④　テスト 21
⑤　開発・保守に関する手続の策定と保守 23
（２）システムの運用・管理 24
①　運用管理 24
②　構成管理 27

③ データ管理 28
（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 30
① 情報セキュリティフレームワーク 30
② アクセス管理等のセキュリティ対策 31
③ 情報セキュリティインシデント（事故）の管理 35
（４）外部委託先の管理 36
① 外部委託先との契約 36
② 外部委託先とのサービスレベルの定義と管理 38

４．業務処理統制 41

（１）入力管理（入力統制） 41
（２）データ管理（処理統制） 42
（３）出力管理（出力統制） 44
（４）エンドユーザコンピューティング（ＥＵＣ） 45

５．モニタリング 50

（１）日常的モニタリング 50
（２）独立的モニタリング（内部監査部門等による監視体制） 51
① IT全社的統制のモニタリング 52
② IT全般統制のモニタリング 53
③ IT業務処理統制のモニタリング 54

１．ガイダンスの使い方

（１）リスク要因について

企業は、財務報告に係る IT 統制の有効性を評価する場合、まず、想定されるリスクを洗い出す。具体的には、財務報告に関わる情報システムとそれを支える IT 基盤に対するリスク要因や、業務プロセスにおけるリスク要因を洗い出すこととなる。リスク要因には、図表Ⅳ．１－１に示すようなものがある。

図表Ⅳ．１－１　リスク要因について

リスク要因	←　高い　　リスク　　低い→	
不正等への機会	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⇒*（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⇒*（実施基準　Ⅰ．２（２）②）*。ITのリスク対応では、システム管理基準や情報セキュリティ管理基準の管理項目を用いるとよい。

②　リスクの評価には、影響度と発生頻度の両方を考察する。

発生頻度に係るものには、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 リスク評価について経験の少ない企業では、短期間で内部統制を整備し評価するのは難しい。そのため、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、経験の少ない企業向けのものであり、自社のリスクを分析して対応できる企業は自社が確立した技法で進めればよい⇒*(実施基準　Ⅲ．４（２）④ロ)*。

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⇒*（実施基準公開草案　Ⅲ．４（２）④ロ）*。

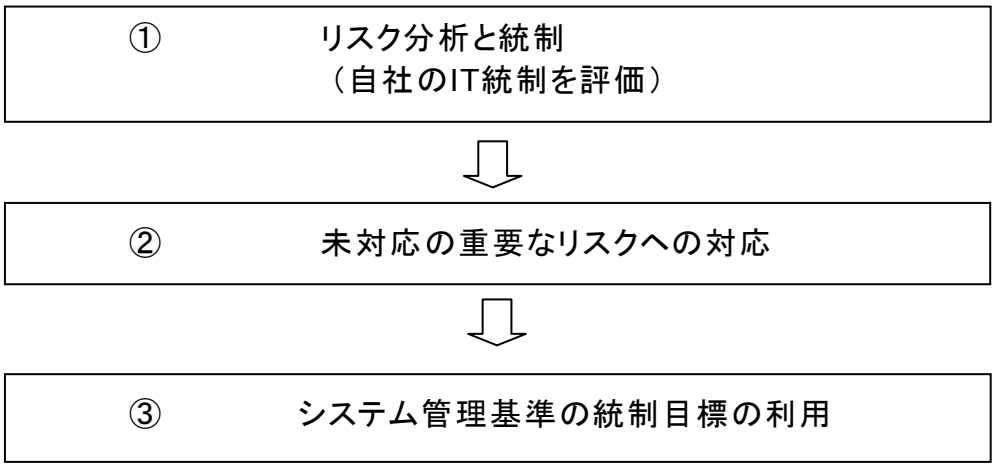
（３）IT 統制の整備と評価に必要な統制目標の選択

対応すべきリスクが特定されたあとは、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、組み合わせて用いられる。

⇒*（実施基準公開草案、Ⅰ．２（２）①）*

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統制について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．２－２に示す。

図表Ⅳ．２－２　IT 統制目標の選択プロセス



①　リスク分析と統制

企業は、まず、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、統制を実施することになる。この場合、まず、自社や属する業界で実施している管理項目を用いて、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、すべ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、財務報告の虚偽表示に係る重要な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」等の管理項目から、自社のリスクを低減する適切な項目を選択する。これらの統制項目により、財務報告の虚偽表示に係るリスクが低減され、受容できるリスクレベルになることを確認する。さらに、残余リスクが無視できないときには、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　システム管理基準統制目標の利用

企業が財務報告の虚偽表示に係るリスクが低減させるためにシステム管理基準と、本章の２節から５節に述べる統制区分ごと統制目標や統制例を用いる。システム管理基準を利用するにあたっては、「付録２　システム管理基準の統制目標の使い方」に具体的な統制項目の選び方を示す。（システム管理基準を参照するに当たっては、基準の章番号と大項目（最初の２文字で表記している。例えば、「開発業務」であれば「開発」としている）、項番で表記している）。

本章の２節から５節では、統制項目を選ぶ際の目安となるように、IT 全社的統制、IT 全般統制、IT 業務処理統制、モニタリングに分けて、統制項目を例示している。その際、**【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】**の順で整理している。

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、リスクコントロールマトリックスにまとめて、整備や評価を管理すると分かりやすい。このリスクコントロールマトリックスの例を「付録６　リスクコントロールマトリックスの例」に示す。

（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ている⇒*（「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」　実施基準公開草案　Ⅰ．２（６）② ITの統制 イ）*。したがって、本章で示すIT統制の例示は、あくまでも、財務報告に係る信頼性の整備や評価の目的に限ったものであることに留意する。

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 に関する戦略、計画、予算等の策定により基本方針を明示するとともに、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⇒*（実施基準公開草案　Ⅱ（参考１）IT への対応）*。

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

⇒*（実施基準公開草案　Ｉ．２（６）②ロ IT への対応 イ）*。

【統制目標の例】

2-(1)-①	経営者が財務報告に関連した IT への対応について戦略・計画を定めること。
2-(1)-②	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こと⇒*（システム管理基準　Ｉ情報１．１（１）、Ｉ情報１．１（５））*。
2-(1)-③	IT に関する業務の役割分担、責任及び権限が明確になっていること⇒*（システム管理基準　Ⅵ共通４．２（１）、Ｉ情報２．２（１）～（２））*。
2-(1)-④	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・育成及び教育訓練が適切に行われていること⇒*（システム管理基準　Ⅵ共通４．３（１）～（３））*。
2-(1)-⑤	情報セキュリティの基本方針を定めていること⇒*（システム管理基準　Ｉ情報１．１（６））*。

【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。以下同様。）、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たり、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、外部委託先（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会社に周知・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、外部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、外部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への方針がないと、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。

（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】

リスクの評価と対応と IT との関係には２つの側面がある。１つは、IT を利用することにより新たに生じるリスクをどのように評価し、対応するかという面であり⇒*（実施基準公開草案　Ⅱ（参考１）IT への対応）*、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を設定し、適切な対応を図ることを意味する⇒*（実施基準公開草案　Ⅱ（参考１）リスクの評価と対応）*。

もう１つは、IT に関連するリスクに限らず、財務報告に関連するリスクの評価と対応にどのように IT を利用するかという側面である。リスクの評価と対応には、必ずしも IT を利用する必要はないが、IT を利用してリスク情報の把握と共有を行うことによって、より有効かつ効率的にリスクの評価と対応を行うことが可能となる場合がある⇒*（実施基準公開草案　Ⅰ．２（６）② IT の利用 ロ）*。

【統制目標の例】

2-(2)-①	IT に関するリスク評価の方針が定められており、運用されていること⇒*（システム管理基準　Ⅰ情報４（２））*。
2-(2)-②	統制活動への IT の利用によって、新たに生じるリスクを考慮していること⇒*（システム管理基準　Ⅲ開発１．（４））*。
2-(2)-③	財務報告に関連するリスク情報の把握と共有に IT を利用している場合には、IT の利用が効果的に行われていること。

【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-(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いる。	全社レベル、業務プロセスレベルの IT リスク評価に関する規程が制定されており、重要な問題点が経営者に報告されている。
2-(2)-②	統制活動への IT の利用によって、新たなリスクが生じる。	統制活動への IT の利用によって、新たに生じるリスクを考慮してリスクへの対応を行うこと。	財務報告に重要な影響を及ぼす可能性のある IT の開発等の変化を把握し、IT リスク評価に関する規程に定める手順にしたがって、リスクの再評価とリスクへの対応を実施していることを確かめる。
2-(2)-③	財務報告に関連する情報が共有されず、重要なリスクを見落とす。	財務報告に関連する IT を利用している場合に、適切な IT 利用の方針、計画等を示すこと。	経営者が、財務報告に関連するリスク情報の把握と共有に係る IT の利用に関する方針を示し、又は承認していることを確かめる （→本項目については、本章４．IT 業務処理統制において、具体的な評価を行う）。

（３）　統制手続の整備と周知（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 業務処理統制に関する方針と手続をどのように定めて運用するかという側面（⇒*（実施基準公開草案　Ⅱ（参考１）IT への対応）*）と、統制活動に IT を利用する場合にどのように業務プロセスに組込んで適切に運用するかという側面からなる（⇒*（実施基準公開草案　Ⅰ．２（６）② ハ IT の利用）*）。

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、生産管理システムの中に、たな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したが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、帳簿在庫と実在庫の差を把握し、一致していない場合には、問題の発見に役立てることできる。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⇒*（実施基準公開草案　Ⅰ．２（６）② ハ IT の利用 ハ）*。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会社に周知・徹底し、実施することになる。

【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。⇒*（システム管理基準　Ⅰ情報１．１（５）～（６））*
2-(3)-②	統制活動へのITの利用に係る方針及び手続を適切に定めていること⇒*（システム管理基準　Ⅰ情報４（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
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に周知・徹底していること。	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、財務報告の信頼性が確保されない。	統制活動に IT を利用する場合には、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事項についての方針が定められていること。	統制活動に IT を利用する場合には、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事項についての方針が定められ、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。

（４）　情報伝達の体制と仕組の整備（情報と伝達）

【統制に関する指針】

IT に関連する情報と伝達には、IT に係る業務プロセスに関する情報伝達の体制と仕組の側面と、企業における情報と伝達に IT をどのように利用するかという側面がある。

情報の伝達及び共有を行うために体制を構築し、IT の利用により企業内部での情報伝達の手段を効果的に業務プロセスに組み込むことができる場合もある。また、企業内のみならず、ホームページを利用して、企業外に向けた伝達を適時に行うことや、自社製品へのクレーム情報等を外部から収集したりすることも可能である⇒*（実施基準公開草案　Ⅰ．２（６）② ハ IT の利用 ニ）*。

【統制目標の例】

2-(4)-①	IT に係る業務プロセスに関する情報を識別・把握・処理し、その情報を企業内及び企業外の関係者に伝達する仕組が整備され、適切に運用されていること。
2-(4)-②	情報と伝達において IT を利用して情報を識別・把握・処理している場合、その情報を企業内及び企業外の関係者に伝達する仕組が整備され、適切に運用されていること。

【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-(4)-①	IT に関する重要な問題点が、共有されないことにより、早期の対応ができない。	経営者が、IT 部門又は IT に関する業務の委託先における重要な問題点を、伝達する方針を示すこと。	IT 部門又は IT に関する業務の委託先における日常業務及び IT 関連プロジェクトの活動状況に関する重要な情報が、経営者に適宜、報告されているか確かめる。
2-(4)-②	情報の識別・把握・処理・伝達の仕組に IT を利用している場合、その仕組が適切でないことにより、重要な問題が経営者に伝わらない、もしくは経営者の方針が周知されない。	経営者が、情報と伝達における IT の利用についての方針を示すこと。	経営者が、情報と伝達に対して IT を利用する場合の方針を、IT に関する計画、年度予算等によって承認し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「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ックスについて

IT 全社的統制は、財務報告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、詳細な統制内容の検討は、IT 全般統制及び IT 業務処理統制の評価において実施し、IT 全社的統制の検討においては、経営者の責任において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ックスを作成すると分かり易い。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ックスの作成の例を、付録６「リスクコントロールマトリックスの作成の例」に示す。

会社名	
決算期	

作成者・作成日	
質問への回答者の役職及び氏名	

基本的要素	リスク	統制目標	No.	統制の状況	整備運用	統制評価手続 （文書化、教育・周知、体制、実施、監視・改善の観点から評価する）	評価並びに検出事項 （検出事項がある場合、その影響）	調書番号	リスク評価結果
統制環境	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・計画を定めること。		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	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。	なし	記載省略	低
	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こと。		ITに関する具体的な方針決定と運営のため、情報システム化委員会が設けられている。	整備	「情報システム化委員会規程」を閲覧し、そのメンバーと役割をするか、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。	なし	記載省略	低
				情報システム化委員会が有効に運営されている。	運用	情報システム化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確かめた。	なし	記載省略	低
	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									

３．IT 全般統制

本節では、財務情報の係る IT 基盤等の共通する統制項目について述べている。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 の運用についてである。後者については、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。

（１）　情報システムのソフトウェアの開発・調達

⇒（*実施基準公開草案　Ⅲ．４（２）ロａ*）

①　ソフトウェアの開発・調達

【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、経営目標の達成上重要なプロセスであるので、誤りや不正を防止ために、標準化された開発手法、テスト、本番への移行手続きを用いる。

企業が財務情報の処理に情報システムを利用するときには、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。経営者はまた、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、組織の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、仕様どお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。

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、担当者を限定するために認証機能が用いられるが、実際に担当者ごとに ID やパスワードを設定し、担当者がアクセスできる範囲を決めなければ、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、責任者が承認していること⇒（*システム管理基準　Ⅲ開発１（１）～（２）、Ⅲ開発２（１）、Ⅲ開発３（１）*）。
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⇒*（システム管理基準　Ⅲ開発２（４）～（５）、（１１）*）。
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⇒*（システム管理基準　Ⅲ開発２（９）*）。

ｂ．調達

3-(1)-①-ニ	財務情報に係る情報システムの調達は、全社的な IT 方針に沿って計画されていること⇒*（システム管理基準　Ⅱ企画３（１）*）。
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⇒*（システム管理基準　Ⅲ開発２（１２）、４（４）、５（１）～（１３）*）。

【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プログラムが埋め込まれたり、処理に誤りが顕在化する	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、更改されている。	・財務情報に係る過去のプロジェクトを調べ、開発、更改の際に、開発方針、手続がどのように利用されたかについて確かめる。 ・開発、更新の各プロセスが適切に進められたことを文書や成果物等で確かめる。

	リスクの例	統制の例	統制評価手続の例
3-(1)-①-ロ	IT の開発プロセスにおいて、意図的な不正や、処理に誤りの起きる可能性がある。	IT の開発プロセスにおいて、財務情報の信頼性に係る完全性、正確性、正当性の統制が確実に実現できるようになっている。	・アプリケーション・システムを開発する際の標準等入手して、誤りや不正を防止するための開発プロセスについての記載があるか確かめる。 ・IT の開発プロセスにおける整備状況を確かめる（例えば、開発における概念設計と詳細設計において、適切な IT 業務処理統制の機能が検討されて、盛り込ま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、テストが行われたか確かめる（例えば、関係者へのヒアリングや記録を確かめる）。 ・財務情報に係る情報システムの開発のテストのプロセスで、完全性、正確性、正当性に関するテストが実施されたかを確かめる（例えば、売上データの二重投入がテストされ、その結果が記録されているかを確かめる）。

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アプリケーション・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。とくに、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、財務報告のアプリケーション・システムの信頼性を保証する上で極めて重要である。

IT 基盤が適切でない場合には、財務報告のアプリケーション・システムに正しいデータを提供できないリスク、財務報告のアプリケーションが正しく動作しないリスク、財務報告に至るまでの段階での不正な処理や改ざんが検出できないリスクが高まる可能性がある。

【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）が、財務情報に係る情報機器の信頼性が達成されていること⇒*（システム管理基準　Ⅲ開発１（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
3-(1)-②-イ	IT 基盤のインタフェースが信用できないと、扱うデータを信頼できない。	転送されたデータが信頼できることを確かめるために、IT 基盤のインタフェースのテストが実施されている。	・財務報告にとって重要な IT 基盤を調べ、データの送受テストで正確性について検証され、その結果が記録されていることを確かめる。 ・IT 基盤に統一的なアーキテクチャ等が採用されている場合には、その事実を確かめる。
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、設定の記録や保守での記録によって確かめる。 （例えば、担当者が利用している PC について、企業が定めている標準にしたがって、OS、ソフトウェア類が利用され、利用制限が加えられている）。

③　変更管理

財務報告に係る IT は、情報処理の完全性、正確性、正当性を維持するための変更や改変を、変更管理により統制する。

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、財務報告の信頼性に影響を及ぼす可能性がある。

変更管理は、プログラムや重要なデータが無断で改変されないように、ソフトウェアの変更、システムの変更及びソフトウェアの保守における変更、あるいは、データの変更を適切に管理することが望まれる。

【統制に関する指針】

変更管理は、企業が財務情報に係る情報システムの機能を変更する場合に最終的な財務報告の信頼性を失わないようにする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、勘定項目を変更する際は、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．変更の管理

3-(1)-③-イ	変更管理ルールと手順を定め、担当者、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　Ⅵ共通６．１（１））*。
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⇒*（システム管理基準　Ⅵ共通６．２（２））*。
3-(1)-③-ハ	緊急の変更要求は文書化され、変更管理手続にしたがっていること。

ｂ．変更結果の管理

3-(1)-③-ニ	変更の結果は、担当者、開発、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　Ⅵ共通６．２（３））*。
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　Ⅵ共通６．１（３））*。

ｃ．一般ソフトウェア（プログラムを開発する場合）の変更管理

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、担当者及び保守の責任者が承認すること⇒*（システム管理基準　Ⅴ保守３（１））*。
3-(1)-③-ト	プログラムの変更は、変更管理手順に基づき、責任者の承認を得ること⇒*（システム管理基準　Ⅴ保守３（２））*。

3-(1)-③-チ	プログラム設計書に基づいてプログラミングしていることを検証すること⇒*（システム管理基準　Ⅴ保守３（３））*。
3-(1)-③-リ	プログラムのテストの実施は、テスト計画に基づいて行うこと⇒*（システム管理基準　Ⅴ保守４（１））*。
3-(1)-③-ヌ	プログラムのテストには担当者が参画すること⇒*（システム管理基準　Ⅴ保守４（３））*。
3-(1)-③-ル	プログラムのテスト結果は、担当者、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　Ⅴ保守４（４））*。
3-(1)-③-ヲ	プログラムの本番への移行は、権限を与えられた者のみが実施すること。
3-(1)-③-ワ	プログラムのテスト結果、本番への移行結果を記録及び保管すること（記録および保存については、テストを参照）⇒*（システム管理基準　Ⅴ保守４（５））*。

ｄ．パッケージソフトウェアの変更管理

3-(1)-③-カ	機能の追加等の変更は必須の項目に限ること。
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	本番への移行は権限を与えられた者のみが実施すること。

【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、変更管理手続にしたがっている（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、インフラの変更を含む、本番環境のすべての変更について、変更管理手続にしたが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、本番への移行するまで、追跡されていることが望まれる）。 ・プログラム変更は、変更管理手続にしたがって、統制された環境で、適切（職務の分離等）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。機能用件やセキュリティ、IT 基盤との接続等についても検討され、テストされたかについて確かめる）。 ・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したがっている。	・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。 （例えば、緊急に実施されたすべての活動に対して、変更ログが存在し、承認されているか確かめる。） ・緊急変更のための手続に、取消手続があるか確かめる。 ・すべ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したがっていることを確かめる。 （例えば、「緊急変更」の記載のある変更の例を調査し、承認がなされているか、また、特別にアクセス権を付与した場合、変更終了後にアクセス権が削除されているかを確かめる。さらに、変更が記録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)-③-ニ，3-(1)-③-ト	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、移行作業にあ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、牽制の仕組があることを確かめる。 （例えば、本番移行がシステム開発者任せになっていないことを、実施記録や、結果報告等の記録から確かめる）。

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、アプリケーション・システムが設計どお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、アプリケーション・システムや IT 基盤が設計で意図したどおりに機能せず、その結果、財務情報が信頼できなくなる。

【統制目標の例】

a．テスト方針と手続

3-(1)-④-イ	アプリケーション・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　Ⅲ開発２（２））*。
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　Ⅲ開発５（１））*。

b．テスト環境

3-(1)-④-ハ	テストは、本番環境と隔離された環境で行うこと⇒*（システム管理基準　Ⅲ開発５（５））*。

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　Ⅲ開発５（８））*。
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　Ⅲ開発５（９））*。

ｃ．テスト作業の権限の分離と結果の保管

3-(1)-④-ヘ	テストは、開発当事者以外の者が参画すること⇒*（システム管理基準　Ⅲ開発５（１０））*。
3-(1)-④-ト	テストで発生した問題点について、問題毎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　Ⅲ開発５（１２））*。

【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、財務情報が正確かどうか分からない。	・IT 基盤の機能をテストする手順が策定され、システムが意図した通りに動作するために、単体テスト、システムテスト、統合テスト、及び受入テストを実施する。 ・IT 基盤の更改では、マスタデータの配信、新旧システム間のデータ変換、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、これにしたがって進められたことを確かめる。 ・その中で、財務情報の信頼性に係る機能項目についてのテストが実施されたことを確かめる。（例えば、IT 基盤のシステム間接続でのデータ転送に、誤りや改ざんの可能性がある（完全性が不備）と、財務情報の信頼性が保証できないことになる）。
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・システムは、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したがって、ロードテスト（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たことを確かめる。（なお、負荷テストと限界性能テストでは、例えば、取引件数やトラフィック量について、妥当なレベルであること。また、テストに際しては、他のサービスの性能への影響が調べられているとよい）。
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け入れ側の承認について確かめる。 移行に際しては、以下の項目が実施されたかを確かめる。 ・データ変換について突合せテストが行われ、差異がなかった。 ・追加された新しい機能の確認 ・移行手順の検証 ・受入テストの実施
3-(1)-④-ヘ	受入テストを開発者が実施すると、誤りや不正の可能性が残る。	財務情報に係る情報システムの受入テストでは、中立の立場の者が参画する。	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について、テストには中立の立場の者が参画していることを確かめる。
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かの証拠がない。	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・保守管理ならびに必要な文書化の各プロセスが見直される。方針と手続きの変更は、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　Ⅵ共通１．１（１）～（５））*。

【統制の例と統制評価の例】

	リスクの例	統制の例	統制評価の例
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、運用にかかわる方針と手続が変更されないと、リスクが大きくなる。	企業は、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かかわ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。	・財務報告に係る IT に関連する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　⇒*（実施基準公開草案　Ⅲ．４（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。とくに、財務報告に係る IT の運用に不備がある場合、結果として財務報告の信頼性に重大な影響を及ぼすことがある。

例えば、売上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、売上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順守

3-(2)-①-イ	運用ルールを定め、順守すること⇒*（システム管理基準　Ⅳ運用１（１）～（２））*。
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　Ⅳ運用２（１）～（３））*。

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　Ⅳ運用２（６））*。

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したがって運用すること⇒*（システム管理基準　Ⅳ運用２（４）～（５））*。

ｃ．運用の実施記録、ログの採取と保管

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　Ⅳ運用２（９））*。
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　Ⅳ運用２（１１）～（１２））*。

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　Ⅳ運用２（１３）～（１４））*。

【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、財務情報に係るすべての処理が、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、これにしたがっている。	・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。ジョブスケジューリングどお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）。 ・自動化された 24 時間 365 日運用の情報システムの場合には、処理の連続性と、運用面での変更がないことを確かめる。（例えば、情報システムの運用を無人運転に変更した場合には、補完的な入退出管理等の補完的な統制を確かめる。補完的統制がないと不正な変更の可能性がある）。
3-(2)-①-ハ	運用時の不正な操作等を発見できない。	情報システムとデータ処理について、企業にログ採取・分析についての方針があり、それに基づいてログが採取されて、必要な項目がモニタリングされている。	企業に、ログ採取に関する方針があることを確かめる。次に、必要なログ（不正操作等のモニタリングに必要な項目）が記録され、保管されていること、また、保存されたログを利用できることを確かめる。
3-(2)-①-ヘ	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もとに、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、システムの誤りや不正の防止につながる。	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。

構成管理は変更管理の統制により発生した結果を管理しており、変更管理と一体となって管理することにより、その効果を発揮する。

構成管理はシステム構成、ネットワーク構成、ソフトウェア構成、マスタデータ等の情報システムの構成に関する基礎的な情報を管理し、提供する機能を持っている。構成管理が適切に行われない場合、財務情報の作成・処理に影響を及ぼす可能性があるので、適時・適切な管理を実施する。

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。管理者は、適切な措置を行うことにより、財務情報の信頼性を維持することができる。

【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、責任者が承認すること⇒*（システム管理基準　Ⅳ運用６（１）、７（１））*。
3-(2)-②-ロ	許可された以外のソフトウェア、ハードウェアは使用禁止にすること⇒*（システム管理基準　Ⅳ運用６（２））*。

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、サポート条件

3-(2)-②-ハ	導入や調達したソフトウェア、ハードウェア及びネットワークの記録が適切に管理簿に反映されていること。
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　Ⅳ運用９（２））*。
3-(2)-②-ホ	緊急時を含む障害対策があること⇒*（システム管理基準　Ⅳ運用７（４）、８（４））*。

3-(2)-②-ヘ	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．ハードウェア及びネットワーク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⇒*（システム管理基準　Ⅳ運用７（２）、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)-②-イ	ソフトウェア、ハードウェア、アプリケーション・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。	購買、設置、固定資産、廃棄等が適切に管理されている。	情報システムの購買、設置、廃棄等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。
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】

企業における財務情報の入力、登録、処理、集計、報告等データを完全性、正確性、正当性を保証するために適切なデータ管理が用いられる。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。

【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　Ⅳ運用４（１）、（６））*。
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　Ⅳ運用４（６）、（７））*。

ｂ．データのインテグリティの維持

3-(2)-③-ハ	不正アクセス又は改ざんから論理的、物理的に保護すること⇒*（システム管理基準　Ⅳ運用４（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　Ⅳ運用４（５）、Ⅵ共通７．３（２））（実施基準公開草案　Ⅲ．４（２）②ロｂ）*。
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　Ⅵ共通７．４（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-(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無いか調べる）。
3-(2)-③-ハ	データの保管や移送の際には、改ざん、不正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、無駄なデータが長期保管される。	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、この条件にしたが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

⇒（実施基準公開草案　Ⅲ．４（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、とくに、情報の改ざん、削除等のリスクがある。これらの IT では、情報セキュリティ基本方針が順守され、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　Ⅰ情報１．１（６））*、*（情報セキュリティ管理基準　１．１．１．２、１７）*。

【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】

財務情報に係るアプリケーション・システムでは、とくに、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、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、適切なアクセス制御がなく、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かぎり、不正確な財務報告につながる可能性がある。

【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⇒*（システム管理基準　Ⅳ運用４（２）、６（２）、７（２））、（情報セキュリティ管理基準　７．１．１）*。
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　７．２．１）*。
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　７．２．１）*。
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　７．２．１）*。
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に対応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　７．２．２）*。

ｂ．パスワードの管理

3-(3)-②-ヘ	パスワードの割当ては、アクセス手順にしたがって付与されること⇒*（情報セキュリティ管理基準　７．２．３）*。

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　７．４．１）*。
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　７．４．２）*。

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　7．5．2）*。
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　7．7．1）*。
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⇒*（情報セキュリティ管理基準　7．6．1）*。

【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)-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。	すべ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、手順にしたが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、これにしたがっている。	・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	インターネットを利用する場合は不正侵入対策が実施されている。	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等の適切な統制が存在して、不正アクセスを防いでいる。	（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、すべ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）。

③　情報セキュリティインシデント（事故）の管理

【統制に関する指針】

問題管理や事故管理は、企業が通常の運用の範囲を超えたアクセスや行為に対して、文書化して担当者に通知して、モニタリングすることで対応する。問題管理や事故対応に不備がある場合、結果としての財務報告の信頼性に重要な影響を及ぼす可能性がある。

【統制目標の例】

ａ．事故の報告、記録及び対応ルールと手順

3-(3)-③-イ	事故及び障害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　Ⅳ運用２（１０））*。
3-(3)-③-ロ	事故及び障害の内容を記録し、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　Ⅳ運用２（１１））*。

ｂ．事故の原因究明及び再発防止

3-(3)-③-ハ	事故及び障害の原因を究明し、再発防止の措置を講じること⇒*（システム管理基準　Ⅳ運用２（１１））*。

【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	事故の対応が適切に行われないと、被害が拡大する。	問題管理の仕組を導入して、データの信頼性に係る問題が発生したとき、適時に記録されて、分析され、解決する。	問題又は事故(障害)報告書のサンプルを検討し、問題が適時に対応（記録、分析又は解決）されたかを確かめる。
3-(3)-③-ハ	ログ取得されず、事件や事故の原因究明ができない。	適切なログ機能により事故の原因を究明する。 （ログを採らず、サーバ停止の場合に、再開処理した場合は、同じ事故の再発のリスクが高い。）	ログが証跡記録に、事故(障害)を追跡ができる情報を含んでいるかについて確かめる。 （例えば、過去のサーバの停止事故の例を選び、問題を解決するためにイベントログから事故の発生に至る過程を分析して問題解決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
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る。	不当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、セキュリティ事故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、事故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、過去の違反例を調べ、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があることを確かめる）。

（４）外部委託先の管理　　⇒（*実施基準公開草案　Ⅲ．４（２）ロｄ*）

①　外部委託先との契約

【統制に関する指針】

外部委託業務の管理は、財務報告に係る IT の運用や財務情報作成等を目的として、外部委託業者に業務委託する場合の管理のことをいう。外部委託業務で起こり得る不備は、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、外部委託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。

【統制目標の例】

ａ．委託計画

3-(4)-①-イ	（財務報告に直接係る）IT を外部委託するとき、その委託計画が承認されていること⇒*（システム管理基準　Ⅵ共通５．１（１））*。
3-(4)-①-ロ	委託業務の目的、範囲、予算、体制等が明確になっていること⇒*（システム管理基準　Ⅵ共通５．１（２））*。

ｂ．委託先の選定

3-(4)-①-ハ	IT を外部委託するとき、組織の委託業者選定方針にしたがって業者選定していること⇒*（システム管理基準　Ⅵ共通５．２（１））*。
3-(4)-①-ニ	候補業者の業務提供能力の評価と財務上の適格性を判断していること。

ｃ．契約

3-(4)-①-ホ	契約書には、委託業務に関する主要なリスクに対する統制方法を明記していること⇒*（システム管理基準　Ⅵ共通５．４（４））*。

ｄ．財務情報に係る IT を外部委託するときの、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　Ⅵ共通５．３（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　Ⅵ共通５．４（３））*。
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　Ⅵ共通５．４（５））*。
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、委託業務の結果サンプリング等で検証して）、問題があれば、責任者に報告すること⇒*（実施基準公開草案　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-リ	サービスレベルをモニタしないと、処理される財務情報の完全性、正確性、正当性が保たれない。	責任者が委託業者のサービスレベルをモニタして、報告する。	外部委託の管理責任者が、提供されているサービスレベルや成果の管理体制を確かめる。 （例えば、外部委託の例を選び、契約や管理の状況を確かめる）。
3-(4)-①-ハ	業者選定や業者管理方針がいい加減であると、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。	企業の委託業者選定方針に沿って外部委託業者を選定する。	企業の業者管理方針を入手して、外部委託業者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	外部委託業者選定が不十分で、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。	外部委託業者の選定前に、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。	外部委託業者選定にあたっての基準を入手する。 これらの基準に、外部委託業者の財務上の安定性、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-イ	外部委託業者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。	業務の外部委託前に、外部委託業者との契約について、社内で承認され、契約書が交わされるための手続があり、これにしたがっている。この手続には、内部統制の要件定義と外部委託業者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。 ・ 外部委託業者が、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-ト	外部委託業者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。	外部委託業者の信頼性（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。	委託先企業について、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）⇒*（実施基準公開草案Ⅱ．２（２）②ｂ）*。

②　外部委託先とのサービスレベルの定義と管理

【統制に関する指針】

外部委託業務のサービスレベルの定義と管理のプロセスは、担当者の期待にいかに応えるか、そして最終的には事業目標をいかに達成するかに関わる。サービスが要求通りに実施されていることを確実にするため、委託事業者との役割と責任が規定される。

とくに、財務報告書の作成を外部委託しているような場合、委託先の情報システム不備がある場合、企業の財務報告と開示に重大な影響を及ぼす可能性がある。

【統制目標の例】

ａ．サービスレベル

3-(4)-②-イ	財務報告・財務情報に係る情報システムを外部に委託する場合、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、委託先企業とサービスレベル契約（SLA）を結ぶことが望ましい。

【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
3-(4)-②-イ	サービスレベルが定義されていないと、外部の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。	・外部委託の契約の中で、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外部に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)-②-イ	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　IT 全般統制のリスクコントロールマトリックスについて

全般統制によって、想定されたリスクから財務情報の信頼性（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。全般統制が整備され運用されていることを評価するためには、リスクコントロールマトリックスを作成すると分かり易い。この例を以下に示す。具体的なリスクコントロールマトリックスの作成の例を、付録６「リスクコントロールマトリックスの作成の例」に示す。

会社名	
決算期	
事業拠点	
対象システム	販売システム
関連する勘定科目	

作成者・作成日	◇◇◇◇　2007/1/23
質問への回答者（実施部署）	

リスク	統制目標 留意事項		No.	統制の状況	整備運用	予防発見	手作業自動化	整備状況 文書	整備状況 プロセス	整備状況 システム実装	頻度	統制評価手続	評価並びに検出事項 （検出事項がある場合、その影響）	調書番号	評価結果
財務情報の信頼性に係わるソフトウェアが適正に開発、調達されず、処理結果の財務情報に信頼を置くことができない。	開発	ITを開発する際に意図的な不正プログラムが埋め込まれたり、処理に誤りが顕在化する		ITを開発するための標準化された方針および手続があり、これに基づいて、ITが開発され、更改されている。	整備	予防	手作業	○	○	NA	四半期	対象とするITの開発は標準化された手順、文書で実施されていることを確かめた	なし	記載省略	低
		ITの開発プロセスにおいて、意図的な不正や、処理に誤謬の起きる可能性がある		ITの開発プロセスにおいて、財務情報の信頼性に係る正当性、完全性、正確性の統制が確実に実現できるようになっている。	運用	予防	手作業	○	○	NA	四半期	・開発の仕様書、基本設計書（概念設計書）等で財務情報の信頼性確保の統制機能が織り込まれていることを確かめた。	なし	記載省略	低
		以下省略													
保守が適切に実施されないと業務処理統制の信頼が失われる	保守	プログラムが改ざんされたり、承認なく変更される		システムソフトの変更を含むプログラム変更、システムの変更およ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）。	整備・運用	発見	手作業	○	○	NA	月週	変更管理手続の規定があることを確かめた。変更管理規定どうりに変更管理を実施していることを25件テストした。	25件のうち1件、承認漏れがあったが、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。25件の追加テストの結果、押印漏れはなく、単なる押印漏れのミスであると判断した。	記載省略	低
				以下省略											

４．業務処理統制

（１）入力管理（入力統制）

入力データの作成から保管等までの情報システムのデータの管理

【統制に関する指針】

業務プロセスに IT を利用する場合は、入力する元データの作成、入力の実施、確認、入力した元データの保管、廃棄の管理を実施する。入力は、手作業で実施される場合とフロッピー、CD 等の磁気媒体、EDI 等のデータ伝送、インターネットを経由してくる場合がある。ここでの入力管理は、主に手作業での入力を想定している。データの最初の入り口で誤りや不正があると、このデータから生成される財務情報に誤りや不正が発生する。

【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　Ⅳ運用３（１））*。
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　Ⅳ運用３（２））*。
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　Ⅳ運用３（４））*。
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　Ⅳ運用３（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
4-(1)-①	財務情報の元となるデータの入力に管理ルールが無く誤りが発生､もしくは不正な入力が行われる。	入力データの作成、授受、検証、入力の実施、入力後の確認、保管等、情報システムへのデータ入力に伴う一連の作業について手順、検証方法、承認方法を入力管理ルールとして明文化する。	・入力データの作成、授受、検証、入力の実施、入力後の確認、保管等、情報システムへのデータ入力に伴う一連の作業について手順、検証方法、承認方法を入力管理ルールとして明文化しているか確かめる。

	リスクの例	統制の例	統制評価手続の例
4-(1)-②	財務情報の元となる取引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、二重入力等の誤りが発生しないように制御、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、入力データに欠落、二重入力等の誤りが発生しないように制御、検証する機能があることを確かめる。
4-(1)-②	財務情報の元となる取引データの入力に誤りが発生､もしくは不正な入力が行われる	入力管理ルールに記載されている手順に従い、正確に入力が行われるように制御、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、正確に入力が行なわれるように制御、検証する機能があることを確かめる。
4-(1)-③	財務情報に係る情報システムを入力する際に不正な入力が行われる。	誤り防止、不正防止及び機密保護等のために、正当な承認に基づいて入力データの作成、取扱い等をする。	入力データの作成、取扱い等は正当な承認に基づいて実施されていることを確かめる。
4-(1)-④	財務情報の紛失、盗難、漏えいが発生する。	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。	入力データの保管及び廃棄は入力管理ルールに基づいていることを確かめる。

（２）データ管理（処理統制）

データの授受、交換、複製及び廃棄に伴う一連の作業の管理

【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、送信される場合がある。その場合には、データに係る統制があらかじめプログラミングとして組込まれていることが望まれる。例えば、送信元が正当な得意先であることを確かめる仕組が組込まれていないと､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　Ⅳ運用４（１））*。
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　Ⅳ運用４（２））*。
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　Ⅳ運*

	用４（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Ⅳ運用４（６）*。
4-(2)-⑤	データの交換は、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　Ⅳ運用４（７）*。
4-(2)-⑥	データの保管、複写及び廃棄は、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　Ⅳ運用４（８）*。

【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	財務情報に係るデータ管理ルールが無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、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ことを確かめる。
4-(2)-②	財務情報に係るデータに不正なアクセスが行われ､誤りや不正が発生する。	データへの不正アクセスの防止、不正利用の防止、機密保護及び個人情報保護のため、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おり、アクセスログがレビュー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を確かめるコントロールトータル等により検証されていることを確かめる
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よっている。	データの授受は、データ管理ルールに基づいていることを確かめる。
4-(2)-⑤	データ交換の際に誤り､機密漏えいが発生する。	データの交換では、エラー修正やデータの内容を確認する。	データの交換では、機密保護の対策を確かめる。
4-(2)-⑥	データの保管、複写、不要データの廃棄の際に不正利用､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、不正防止及び機密保護の対策を講ずる。	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（例えば、アクセス制御、データの消去、テープの裁断等）を確かめる。

IT 業務処理統制のデータ管理は、IT 全般統制のデータ管理と重なるところがある。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 業務処理統制のデータ管理は各業務アプリケーションに固有のデータ管理の IT 統制である。それぞれの IT の構成や企業の組織内の管理体制に合わせて構築・評価することになる。例えば、バックアップデータの管理は IT 全般統制で評価し、得意先からの受発注データ等は、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）

出力データの作成、授受、検証、出力の実施、出力後の確認、保管等、情報システムへのデータ出力に伴う一連の作業の管理

【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　Ⅳ運用５（１）*）。
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　Ⅳ運用５（２）*）。
4-(3)-③	出力情報の作成手順、取扱い等は、誤り防止、不正防止及び機密保護の対策を講じること⇒（*システム管理基準　Ⅳ運用５（３）*）。
4-(3)-④	出力情報の引渡しは、出力管理ルールに基づいて行うこと⇒（*システム管理基準　Ⅳ運用５（４）*）。
4-(3)-⑤	出力情報の保管及び廃棄は、出力管理ルールに基づいて行うこと⇒（*システム管理基準　Ⅳ運用５（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
4-(3)-①	財務情報の元となる取引データの出力にルールがなく、誤り、不正が発生する。	出力方法の誤り、不正利用、漏えい等を防止し、機密及び個人情報保護のため、情報の出力手続、承認等のルールを定める。	出力方法の誤り、不正利用、漏えい等を防止し、機密及び個人情報保護のため、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､もしく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していることを確かめる。
4-(3)-④	財務情報に係る情報システムから出力する際に改ざん等が不正に行われる。	出力情報の作成、取扱い等を正確に行い、改ざん、盗難、漏えい等を防止するため、誤り防止、不正防止及び機密保護の対策を講ずる。	出力情報に誤り防止、不正防止及び機密保護の対策が定められ、ルールどおりに実施されていることを確かめる。
4-(3)-⑤	出力された財務情報を引き渡す際に紛失や機密漏えいが行われる。	出力情報の、引渡し手続等のルールを定め、遵守する。	出力情報の引渡し手続等のルールを定め、遵守していることを確かめる。
4-(3)-⑥	出力された財務情報の保管､廃棄の際に紛失や機密漏えいが行われる。	保管及び廃棄は、出力管理ルールに基づいて行う。	保管及び廃棄は、出力管理ルールに基づいて行っていることを確かめる。

（４）　エンドユーザコンピューティング（ＥＵＣ）

【統制に関する指針】

EUC の利用は、財務実務担当者の業務の効率化をもたらし、財務報告作成に欠かせないものとなっている。しかし、EUC は手軽な反面、リスクを併せ持っている。例えば、EUC が全社的な情報システムとしての管理から漏れている可能性がある。また、財務報告を作成するという観点からは、計算式等の誤りや決算データの恣意

的な修正等、虚偽記載につながる可能性がある。そのため、以下のようなリスクに対する対策が考えられる。

① スプレッドシート（表計算ソフトで作成した表や数式）の作成者と担当者が同一である場合、作成された表計算ソフトやマクロを第三者が検証していないと、不正や計算式の誤り等が見逃されるリスクがある。これを防ぐための対策として、例えば、企業としての規則、仕組、チェック体制等の整備が挙げられる。
② スプレッドシート等では内容が文書として記録されず、不明になるリスクがある。これを防ぐための対策として、例えば、繰り返し利用するものについて、文書化することが挙げられる。
③ EUC では、アプリケーション・システムに比べると、バックアップが十分でなく、データが失われるリスクがある。これを防ぐための対策として、例えば、財務報告に係る IT については、EUC についてもバックアップすることが挙げられる。
④ EUC では、財務担当者の PC が利用されることが多く、アプリケーション・システムに比べると、アクセス制御が十分でないことがある。このような環境では、財務報告にデータの改ざん、消失が生じるリスクがある。これを防ぐための対策として、例えば、財務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仕組が挙げられる。
⑤ スプレッドシートの処理結果について、計算結果等の検証が適切になされないと処理結果としての財務報告に誤りや虚偽が発生するリスクがある。これを防ぐための対策として、例えば、電卓等を用いた手計算で確かめる等の代替的な手段がとられることが挙げられる。

【統制目標の例】

財務報告に影響を与える EUC 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)-イ	EUC 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)-ロ	EUC の利用について承認されていること。
4-(4)-ハ	EUC を財務情報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、順守されていること。
4-(4)-ニ	担当者が作成した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)-ホ	担当者が作成したスプレッドシート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)-ヘ	利用者が、スプレッドシートの数式やマクロ等を変更できないようにしていること。
4-(4)-ト	スプレッドシートの表等に完全性、正確性、正当性を検証できる仕組（検算できる等）が組み込まれているか、もしくは手計算で検算すること。

（なお、システム管理基準は EUC 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)-イ	財務担当者が利用する EUC 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。	EUC の完全性、正確性、正当性に関する方針と手続が存在し、これにしたがっている。	・EUC に関する方針や手続を入手し、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。 （例えば、EUC を利用している財務担当者を任意に選び、EUC の方針を理解し、これにしたがっているかを質問する）。
4-(4)-ロ	承認を受けない PC で、財務報告が行われると、虚偽記載の可能性がある。	承認を受けた EUC（PC 等の IT 基盤を含む）を利用する。	・財務担当者が利用している PC で財務情報が扱われているとして、管理され、承認されているかについて担当者へのヒアリング等で確かめる。

	リスクの例	統制の例	統制評価手続の例
4-(4)-ハ，4-(4)-ト	スプレッドシート等では誤処理や改ざんが起こりやすい。	EUC について文書化されており、処理の完全性、正確性、正当性がチェックされている。	・実際に用いられている EUC（PC 等の IT 基盤も含む）について調査する。 ・完全性、正確性、正当性について表計算ソフトの数式や表等を見直す頻度、利用範囲について確かめる。 ・EUC で実施されている表計算ソフトの一部を入手して、処理内容を確認して、有効性を確かめる。 ・スプレッドシート（表）の検算機能を確かめる。
4-(4)-ホ	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。	スプレッドシートやデータ等はバックアップをとり、安全に保管する。	・スプレッドシートやデータ等のバックアップの状況を確かめる。 （例えば、バックアップの方法、タイミング、保管場所等について質問する）
4-(4)-ヘ	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。	スプレッドシートやデータ等は、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 PC にアクセス制御が実施されていることを確かめる。 （例えば､財務担当者の PC への不正アクセスを試みる)。 ・スプレッドシートやデータ等への不正な改ざんを発見する仕組があるかを確かめる。

（５）IT 業務処理統制のリスクコントロールマトリックスについて

業務処理統制では、想定されたリスクから財務情報の信頼性（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。IT 業務処理統制が整備され運用されていることを評価するには、リスクコントロールマトリックスを作成すると分かり易い。この例を以下に示す。具体的なリスクコントロールマトリックスの作成の例を、付録６「リスクコントロールマトリックスの作成の例」に示す。

会社名	○○株式会社
決算期	平成○○年3月
場所	受注センター
取引サイクル	販売サイクル
ファンクション	受注
関連する勘定科目	売上、売掛金

作成者・作成日	◇◇◇◇　2006/12/23
確認者・確認日	□□□□　2007/1/24

リスク	統制目標 / 留意事項		No.	主要な統制活動	自動手動	頻度	経営者の主張 網羅性	実在性	期間配分	権利と義務	評価	表示	整備運用	統制評価手続	評価並びに検出事項（検出事項がある場合、その影響）	調書番号	評価結果
財務情報に漏れや重複が発生する	網羅性	全ての受注は漏れなく重複なく記録されているか	1	EDIによる受注はJCA手順によって制御され異常な伝送があればシステム担当者にメールが送信される	自動	四半期	○	NA	○	NA	NA	NA	整備・運用	特定の月を選び、システム運用報告をレビューしJCA手順による異常終了が担当者に報告され、フォローされていりことを確かめる	なし	記載省略	低
			2	FAX受注はコールセンターで受信後に連番を記入し、一人が入力した後で、プルーフリストを出力し、他の一人が内容をFAXと照合する	自動・手動	日	○	NA	NA	NA	NA	NA	運用	特定の月の25件を選び、プルーフリストが照合されていることを確かめる	なし	記載省略	低
			3	在庫引当された受注のみが出荷指図ファイルに登録される。未引当の受注残は、受注残ファイルに記録され営業担当者がフォローして消しこんでいる。	自動	日	○	○	NA	NA	×	NA	整備・運用	受注残ファイルが営業担当者により、消しこまれていることを確かめる	なし	記載省略	低
財務情報が正確に記録されない	正確性	受注の登録に誤りがないか	4	EDIで受信した受注データは得意先マスタ、商品マスタと存在性のチェックをし、エラーについてはエラーファイルが作成され、エラーデータについては、得意先に返送し、再送を依頼する。エラーファイルは訂正データが再送されるまで保存される。	自動	日	NA	○	NA	○	○	○	整備・運用	特定の月のエラーファイルの処理状況を25件確かめる。	なし	記載省略	低
			5	FAX受注はコールセンターで受信後に連番を記入し、一人が入力した後で、プルーフリストを出力し、他の一人が内容をFAXと照合する。	自動・手動	月日	NA	○	NA	○	○	○	整備・運用	特定の月の25件を選び、プルーフリストが照合されていることを確かめる	なし	記載省略	低
			6	受注日付は機械日付で登録される	自動	日	NA	○	○	NA	NA	○	整備・運用	売上日付の設定を確かめ、売上データの日付が機械日付であることを確かめる	なし	記載省略	低
			7	得意先コードにより、得意先マスタから得意先名がロードされる	自動	日	NA	○	NA	○	○	○	整備・運用	得意先コードにより得意先名が登録されることを画面で確認する	なし	記載省略	低
			8	単価は得意先ごとにマスタに登録された単価が自動的にロードされる	自動	日	NA	○	NA	NA	○	○	整備・運用	単価が自動的に登録されることを確かめる	なし	記載省略	低
正当でない財務情報が記録される	正当性	正当でない受注が登録される	9	得意先マスタに登録された得意先以外は登録できない	自動	日	NA	○	NA	○	NA	NA	整備・運用	マスタに登録された相手先しか登録できないことを確かめる（設定はマスタ登録で確かめる）	なし	記載省略	低
			10	単価は得意先ごとにマスタに登録された単価が自動的にロードされる	自動	日	×	○	NA	○	○	○	整備・運用	単価は登録単価が登録され、単価入力ができないことを確かめる（単価登録はマスタ登録で確かめる）	なし	記載省略	低
			11	受注入力は、担当者のIDとパスワードで制御されている	自動	日	NA	○	NA	NA	NA	NA	整備・運用	担当者のIDとパスワードでしか受注画面が開かないことを確かめる（注）シングルサインオンの場合はパスワード設定は、全般統制で確かめる。ただし、販売システムへのアクセス権限は、業務の権限と一致して設定されいることは、業務処理統制で確かめる	なし	記載省略	低
			12	得意先の与信限度を超える受注は入力できない	自動	日	NA	○	NA	NA	NA	NA	整備・運用	与信限度を超える入力ができないことを確かめる	なし	記載省略	低
			13	以下省略										以下省略			

５．モニタリング

企業は、自社における内部統制が有効に機能しているかを監視するためにモニタリングする。モニタリングには、企業が継続的に内部統制を改善していくための是正行為も含まれる。モニタリングは、①日常的モニタリングと②独立的モニタリングに区分できる。

モニタリングには、企業の経営層、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。企業の各階層に関係するため、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）にマスタファイル等のたな卸（マスタファイルの内容について誤りがないか点検）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、もしくは目標に対する乖離の度合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ファイルのたな卸をする等、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ファイル等に対して実施する。例えば、マスタファイルを定期的にたな卸することで、マスタデータ等の信頼性が確保され、マスタ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、現業、と各管理層で行う。異常値の設定については、経営層から管理層、現業に順次周知され、逆に、異常値の発生についての報告は、現業から管理層、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、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）独立的モニタリング（内部監査部門等による監視体制）

独立的モニタリングは、内部監査部門、監査役による監視等第三者による監視活動である。独立的モニタリングとして IT 統制に関する内部監査の実施は、IT 部門以外の部門によって実施される。独立的モニタリングの一つである内部監査において IT を利用するのは、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。これらのツールを利用する監査はデータの原本性の問題とともに、業務に支障を生じない形式で実施する。

独立的なモニタリング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、一定の金額まではシステム上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あげられる。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あげられる。

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、独立的モニタリング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、是正改善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	独立的モニタリングを担当する部署は、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 全社的統制、IT 全般統制、IT 業務処理統制のそれぞれに分かれる。

①　IT 全社的統制のモニタリング

【統制目標の例】

5-(2)-①	IT に関連する上位組織によるモニタリングの仕組（見直しと改善）が整備され、有効に運用されていること⇒*（システム管理基準　Ⅰ情報２．１（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
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。

	リスクの例	統制の例	統制評価手続の例
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と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定等で確かめる。
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。	内部監査が実施されていることを報告書等で確かめる。

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。よって、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 に関する監査機能が整備され、有効に運用されていること⇒*（システム管理基準　Ⅲ開発２（１４））*。
5-(2)-②-ロ	IT を利用したモニタリングの仕組が利用され、有効に機能していること⇒*（システム管理基準　Ⅳ運用２（１５））*。

【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、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収集されている。	・モニタリング対象として選んだログが、24 時間 365 日収集されていることを確かめる。 ・内部監査部門等がログ収集についてチェックしていることを確かめる。
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が組込まれている。	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が組込まれて、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。
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。
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。
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。

【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データの信頼性が損なわれる。	マスタデータを適宜にチェックする。	・マスタ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ていることを確かめる）。
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、もしく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）。

	リスクの例	統制の例	統制評価手続の例
5-(2)-③-ロ	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）。

x

参考文献

（１） システム管理基準、平成 16 年基準策定版（経済産業省、2005 年 10 月 8 日）
http://www.meti.go.jp/policy/netsecurity/downloadfiles/system_kanri.pdf

（２） 情報セキュリティ管理基準（経済産業省、2003 年 3 月 26 日）
http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Audit_Annex01.pdf

（３） 情報システムの信頼性向上に関するガイドライン（経済産業省、2006 年 6 月 15 日）
http://www.meti.go.jp/press/20060615002/guideline.pdf

（４） コーポレートガバナンス及びリスク管理・内部統制に関する開示・評価の枠組について-構築及び開示のための指針-(案)（経済産業省企業行動の開示・評価に関する研究会、2005 年 7 月 13 日）
http://www.meti.go.jp/press/20050713001/050713kigyokodo.pdf

（５） 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（公開草案）(金融庁企業会計審議会、2006 年 11 月 21 日）
http://www.fsa.go.jp/news/newsj/17/singi/f-20050713-2/01.pdf

付録１．システム管理基準追補版と他の基準との対応

IT 統制の代表的な枠組みとしては、付録図表１－１のようなものがある。

付録図表１－１　IT 統制の代表的な枠組み

代表的な枠組み	策定者等	枠組みの範囲
システム管理基準	経済産業省	IT 統制全般
COBIT（第 4 版）	IT ガバナンス協会	
企業改革法遵守のための IT 統制目標（第 2 版）	IT ガバナンス協会	財務報告に係る IT 統制
IT 委員会報告第 3 号	日本公認会計士協会	
情報セキュリティ管理基準	経済産業省	IT のセキュリティ管理
JIS Q 27002	日本工業規格	
ISO/IEC 20000:2005 Information technology - Service management	ISO/IEC	IT の運用管理
ITIL （ Information Technology Infrastructure Library）	英国商務局	

なお、これらの枠組みのいずれも財務報告に係る内部統制の評価と監査の制度のための「一般に公正妥当と認められる IT 統制基準」として利用しうるかについての合意が得られているわけではない。例えば、これらの枠組みの中にはこの制度のためには必要のない項目が存在したり、項目が一部の領域に偏っていたりする場合がある。また、海外の枠組みは、欧米の商習慣を前提としており、我が国の内部統制制度では欧米にはない考え方も取り入れられているため、我が国の企業にそのまま適用しづらい面もある。

以下では、「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）と代表的な基準である「企業改革法遵守のための IT 統制目標（第 2 版）」（IT Control Objectives for Sarbanes-Oxley 2nd Edition、September 2006、以下、「IT 統制目標．Ｖ２」という）及び「IT 委員会報告第 3 号」（公認会計士協会 IT 委員会第 3 号「財務諸表監査における情報技術（IT）を利用した情報システムに関する重要な虚位表示リスクの評価及び評価したリスクに対応する監査人の手続について」、平成 18 年 3 月 17 日改定、以下、IT３号という）を対比の表として、付録図表１－２に示す。

付録図表１－２　システム管理基準と他の基準との比較表

基準名 構成要素	IT３号	IT 統制目標．V2	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)
序章	Ⅰ．本報告の目的	1．経営者向け要約	はじめに
財務報告に係る統制の基礎	Ⅲ．内部統制を含む企業及び企業環境の理解 1.情報の信頼性と IT 2.経営者の主張と IT コントロール目標との関係 5.統制環境の理解	2．信頼できる財務報告の基礎 IT 統制に関する指針の必要性 3．企業改革法遵守のための変化に関する人的要素の管理 変化に対するコミットメント 現在の状況に対する評価	Ⅰ．IT 統制の概要について 1.財務報告と IT 統制の関係 (1)金融商品取引法に求められている内部統制と IT 統制の関係 (2)財務報告と IT 統制の関係
IT 統制の概要 （統制の分類）	Ⅱ．IT の概括的理解 Ⅲ．内部統制を含む企業及び企業環境の理解 3.各業務プロセスと IT との関係 4.財務諸表の勘定科目、業務プロセスとアプリケーション・システムの関係の理解 6.財務報告の目的の情報システムと伝達の理解 7.統制活動の理解 8.監視活動の理解	2．信頼できる財務報告の基礎 IT 統制の把握 IT 統制 IT 統制に関する PCAOB の指針 IT システムの統制 4．基本原則の制定 COSO の定義 COSO の IT への適用	Ⅰ.2.IT 統制の統制項目 (1)IT 全社的統制 (2)IT 全般統制 (3)IT 業務処理統制
統制フレームと統制目標	外部資料（監査委員会報告 29 号、30 号、31 号等）	参考資料 B．COSO と COBIT 参考資料 C．IT 全般統制 アクティビティレベルの IT 統制 参考資料 D．業務処理統制（アプリケーション統制） 業務処理統制の重要性 業務処理統制の実ケース 業務処理統制の投資対効果 アプリケーションのベンチマークの設定 自動化された業務処理統制の例	付録2．システム管理基準の統制目標の使い方 付録2-1．システム管理基準の管理項目と統制目標の対応（例）

統制活動の実際 （統制と評価の手続）	Ⅳ．重要な虚位表示リスクの評価 1.情報システムに関するリスク評価における重要性の判断 2.全般統制に不備があった場合の留意点 3.業務処理統制に不備があった場合の留意点 4.リスク評価の修正 Ⅴ．経営者及び監査役等とのコミュニケーション Ⅵ．評価したリスクに対応する手続の実施 Ⅷ．IT 専門家の利用 Ⅸ．アウトソーシングの位置付け	5．IT コンプライアンスのためのロードマップ 企業改革法の遵守	Ⅱ．IT 統制の経営者評価 1.IT 統制評価のロードマップ 2.評価の決定と対象となる IT の把握 3.IT 全社的統制の評価 4.業務プロセスに係る IT 統制の評価 5.IT 統制の有効性の判断
事例・その他	Ⅶ．IT に関する監査手続の具体例 1.記録や文書の閲覧 2.観察／システム運用現場視察 3.質問 4.再計算／CAAT 5.再実施／CAAT 6.分析的手続 Ⅹ．発行及び適用	参考資料 A．SOX 法入門 参考資料 E．アプリケーションとテクノロジーレイヤの一覧の例 参考資料 G．固有リスクの評価と統制の優先順位付け表 リスク評価に関して考慮すべき事項 情報技術のリスク評価 統制を考慮すべき箇所についての推奨事項 参考資料 H．統制の文書化とテストのテンプレートのサンプル 参考資料 I．不備の評価決定手順の例 参考資料 J．スプレッドシートのサンプルアプローチ 参考資料 K．学んだ教訓 参考資料 L．SAS70 調査報告書を用いる際の課題範囲 統制の記述 タイミング テストの性質と範囲 限定付適正意見（限定意見）と除外事項 外部サービス業者（サードパーティ）の監査人 参考資料 M．重要な会計アプリケーションにおける職務分離 参考資料 N．図表リスト	Ⅲ．IT 統制の導入ガイダンス（IT 統制の例示） 1.ガイダンスの使い方 2.IT 全社的統制 3.IT 全般統制 4.業務処理統制 5.モニタリング 付録 1．システム管理基準追補版と他の基準との対応 付録 2．システム管理基準の統制目標の使い方 付録 3．IT コントロールと IT の具体的な技術の例示 付録 4．評価手続等の記録及び保存 付録 5．サンプリング 付録 6． リスクコントロールマトリクスの例 ６－1．IT 全社的統制評価記述書 ６－2．IT 全般統制評価記述書 ６－3．IT 業務処理統制評価記述書

「IT３号」は、監査人の会計監査を中心としたITを利用した内部統制のリスク評価の考え方と手続を中心に整理されており、内部監査人や会計監査人が実施していくうえでの手引書として利用するのに適している。

「IT統制目標．V2」はCOSO（トレッドウェイ委員会組織委員会）フレームワークを念頭に置いてIT統制目標が整理され、米国を中心に普及が図られたが、２年間の適用を経て見直しが図られた。初版との違いは、エグゼクティブサマリーに１章を割いて、統制を管理する側へのガイダンスを設けて理解を促すとともに、参考資料に評価基準とテンプレートを多数用意して、広範囲に活用できるように整理された。内部統制の関係者に対し、各々の立場で手引書として利用できるよう構成されている。

「システム管理基準追補版」がIT側の立場を強く意識した視点で整備されているのに対し、「IT統制目標．V2」は統制を管理するという視点に基づいている。そのためIT統制の関係者がこれらを補完的に参照することで、より理解が深まることが期待できる。また、金融庁の「実施基準公開草案」を海外拠点の会社（とくに米国）にまで広げて適用させることが不透明である場合には、「IT統制目標．V2」を参照することは意味があると思われる。

付録２．システム管理基準の統制目標の使い方

１　システム管理基準の統制目標

システム管理基準は、情報システムをめぐるリスクへの対応のため、組織体が IT ガバナンスの確立を図り、情報システムの企画･開発･運用･保守にいたるサイクルの中で情報システムが健全に機能するように管理･統制するための基準である。システム管理基準は、第一義的には情報処理側が使用する基準であるが、システム監査の際にはシステム監査人が監査上の判断の尺度として使用しているものである。

⇒（システム管理基準、序文）

２　システム管理基準の管理項目の整理

企業が財務報告の信頼性に係る IT 統制の整備や評価を行う際に、システム管理基準をより活用しやすくするため、システム管理基準の全管理項目について以下のような整理を行った。表中の左から次のようになっている。

- システム管理基準の管理項目を項番順に示している。
- 管理項目ごとの統制種別（IT 全社的統制、IT 全般統制、IT 業務処理統制）を、それぞれ、全社、全般、業務、－（該当なし）と例示している
- 管理項目ごとに、目指している統制目標を例示している
- 管理項目ごとに、財務情報に係るリスクがより大きいものをコントロール（C）、相対的に小さいものをサブコントロール（S）として分類し、例示している
- 管理項目の主旨（システム管理基準解説書の主旨より要約）を例示している

３　システム管理基準の利用方法

システム管理基準の利用方法は次のようになる。

① 管理項目および管理項目の主旨を理解する
② 対応する統制項目を明確にして、ガイダンスの管理項目のリスクを理解する
③ 該当するリスクが低減したいと考えているものであれば、統制項目の候補となる
④ 統制項目をリストアップして、企業のリスクを低減できることを確認する（リスクコントロールマトリックスの利用など）

付録2－1　　システム管理基準の管理項目と統制目標の対応（例）

項番	システム管理基準の管理項目	統制種別	統制目標（例）	ガイダンス項番	C/S種別	システム管理基準の趣旨
Ⅰ	情報戦略					
1	全体最適化					
1.1	全体最適化の方針・目標	全社				
（1）	ITガバナンスの方針を明確にすること。	全社	ITガバナンスの方針（計画）を策定する	2-(1)-②	C	ITガバナンスの確立に際し、その方針を明確にしておく必要がある。
（2）	情報化投資及び情報化構想の決定における原則を定めること。	全社	経営戦略にあわせた情報化計画を定める		C	首尾一貫した全体最適化計画を策定するため、情報化投資及び情報化構想の決定における原則を定めておく必要がある。
（3）	情報システム全体の最適化目標を経営戦略に基づいて設定すること。	全社	情報システムの最適化計画を経営戦略と整合させる		S	経営目的を実現する情報システムを企画するため、最適化計画の目標は、経営戦略との整合性を考慮して策定する必要がある。
（4）	組織体全体の情報システムのあるべき姿を明確にすること。	全社	全体最適化計画を策定する		C	組織体全体の情報システムは、個別の情報システムが有機的に関連し、整合性が相互に保たれて効率的かつ効果的に目的を達成するものであるため、全体最適化計画は、情報システムのあるべき姿を明確にする必
（5）	システム化によって生ずる組織及び業務の変更の方針を明確にすること。	全社	全体最適化計画は、システム化する組織や業務の変更について示す	2-(1)-② 2-(3)-①	S	全体最適化計画では、情報システムの（再）構築と同期して行われる組織及び業務の新設、改変及び廃止の方針を明確にする必要がある。
（6）	情報セキュリティ基本方針を明確にすること。	全社／全般	全体最適化計画を、情報セキュリティ基本方針と整合させる	2-(1)-⑤ 2-(3)-① 3-(3)-①-イ	C	不正防止、機密保護、プライバシー保護等は、健全な経営活動推進の基盤であるため、情報セキュリティ対策の方針を全体最適化計画で明確にする必要がある。
1.2	全体最適化計画の承認	全社				
（1）	全体最適化計画の立案体制は、組織体の長の承認を得ること。	全社	全体最適化計画は、経営幹部の承認を得る		S	全体最適化計画は、経営戦略に基づき情報システムの中長期計画として策定する必要があるため、立案体制を組織的に確立し、組織体の長が承認する必要がある。
（2）	全体最適化計画は、組織体の長の承認を得ること。	全社	全体最適化計画は、経営幹部の承認を得る		S	経営戦略に基づいて組織体全体で整合性かつ一貫性を確保した情報化を推進するため、全体最適化計画は、組織体の長が承認する必要がある。

システム管理基準の管理項目と統制目標の対応（例）

項番	システム管理基準の管理項目	統制種別	統制目標（例）	ガイダンス項番	C/S種別	システム管理基準の趣旨
(3)	全体最適化計画は、利害関係者の合意を得ること。	全社	全体最適化計画を、組織内外の関係者に周知する		S	円滑に運用できる全体最適化計画とするために、利害関係者の合意を得る必要がある。
1.3	全体最適化計画の策定	全社				
(1)	全体最適化計画は、方針及び目標に基づいていること。	全社	全体最適化計画を策定する		C	経営戦略に基づいて組織体全体で整合性かつ一貫性を確保した情報化を推進するため、全体最適化計画は、方針及び目標に基づいて策定する必要がある。
(2)	全体最適化計画は、コンプライアンスを考慮すること。	全社	全体最適化計画は企業のコンプライアンス方針と整合する		S	関連法規、業界の自主基準等に違反しないよう、全体最適化計画は、コンプライアンスを考慮して作成する必要がある。
(3)	全体最適化計画は、情報化投資の方針及び確保すべき経営資源を明確にすること。	全社	全体最適化計画の経営資源を確保する		S	情報化の費用対効果を高め、実効性のあるものとするために、全体最適化計画は、情報化投資の方針及び確保すべき経営資源を明確にする必要
(4)	全体最適化計画は、投資効果及びリスク算定の方法を明確にすること。	全社	全体最適化計画の投資効果とリスク算定を行う		S	全体最適化計画は、計画採択の判断の基準及び修正を検討すべき判断の基準を明確にするため、投資効果及びリスク算定の方法を示す必要があ
(5)	全体最適化計画は、システム構築及び運用のための標準化及び品質方針を含めたルールを明確にすること。	全社	全体最適化計画は企業のシステム構築の標準化、品質方針を含めている		S	組織体における情報システム相互の整合性を保持し、システム構築及び運用を効率的かつ高品質・均質な品質で行うため、システム構築及び運用のための標準化の方針及び品質の方針を明確にする必要がある。
(6)	全体最適化計画は、個別の開発計画の優先順位及び順位付けのルールを明確にすること。	全社	全体最適化計画は経営課題の重要性や緊急性を考慮している		S	経営課題の重要性及び緊急性を反映し、開発資源を有効に活用するため、全体最適化計画は、個別計画の優先順位及び順位付けのルールを明確にする必要がある。
(7)	全体最適化計画は、外部資源の活用を考慮すること。	全社	全体最適化計画では資源活用の考慮がなされている		S	全体最適化計画において資源面の制約事項を排除するためには、組織体内部の資源だけでなく、外部資源の活用を考慮する必要がある。
1.4	全体最適化計画の運用	全社				

システム管理基準の管理項目と統制目標の対応（例）

項番	システム管理基準の管理項目	統制種別	統制目標（例）	ガイダンス項番	C/S種別	システム管理基準の趣旨
(1)	全体最適化計画は、関係者に周知徹底すること。	全社	全体最適化計画を周知し、理解を深める		C	全体最適化計画を実行性の高いものとするため、全ての利害関係者に周知徹底し、理解させる必要がある。
(2)	全体最適化計画は、定期的及び経営環境等の変化に対応して見直すこと。	全社	全体最適化計画を維持・管理する		S	全体最適化計画を硬直化・陳腐化させないために、定期的な見直し及び経営環境等の変化に対応した見直しを行う必要がある。
2.	組織体制					
2.1	情報システム化委員会	全社				
(1)	全体最適化計画に基づき、委員会の使命を明確にし、適切な権限及び責任を与えること。	全社	全体最適化を実現するために情報システム化委員会を編成する		C	経営戦略に基づいた情報システムの全体最適化を実現するため、経営トップ（執行機関）は、情報戦略の実現を推進する情報化システム委員会を設置し、委員会の使命と権限、責任を明確にする必要がある。
(2)	委員会は、組織体における情報システムに関する活動全般について、モニタリングを実施し、必要に応じて是正措置を講じること。	全社	情報システム委員会が適正な監督活動を行う	5-(2)-①	C	全体最適化計画に基づいた情報システムの企画、開発、運用、保守を実施するため、情報システム化委員会は、全社の情報化活動を総攬する権能と責任を有し、不適切な状況に対しては、是正のための適切な措置を講じる
(3)	委員会は、情報技術の動向に対応するため、技術採用指針を明確にすること。	全社	情報技術基盤の採用について、合理的な基準を制定する。		S	変化する情報技術動向に適切かつ迅速に対応し、組織全体としての整合性の取れた情報技術基盤を確立しリスクを低減させるため、情報システム化委員会は、技術採用指針を明確にする必要がある。
(4)	委員会は、活動内容を組織体の長に報告すること。	全社	情報システム化委員会は、経営活動の意思決定に資する		S	情報システム化委員会は、経営活動の意思決定に資するため、その活動内容を適時に組織体の長に報告する必要がある。
(5)	委員会は、意思決定を支援するための情報を組織体の長に提供すること。	全社	情報システム化委員会は、全体最適化計画と情報システムに関わる重要な事項を経営方針に反映させる		S	情報システム化委員会は、全体最適化計画にかかわる環境変化、技術動向、開発、運用、保守の実施状況を適切かつ迅速に経営方針に反映させるため、経営活動の意思決定を支援する情報を組織体の長に適時提供する必要がある。

システム管理基準の管理項目と統制目標の対応（例）

項番	システム管理基準の管理項目	統制種別	統制目標（例）	ガイダンス項番	C/S種別	システム管理基準の趣旨
2.2	情報システム部門	全社				
(1)	情報システム部門の使命を明確にし、適切な権限及び責任を与えること。	全社	情報システム部門の役割、機能を明確にするとともに、適切な権限と責任を与える	2-(1)-③	C	適時に適切な情報システム機能を遂行するために、組織体の長は情報システム部門の役割、機能を明確にするとともに、適切な権限と責任を与える必要がある。
(2)	情報システム部門は、組織体規模及び特性に応じて、職務の分離、専門化、権限付与、外部委託等を考慮した体制にすること。	全社	情報システム部門は全体最適化計画を実現させるための体制をとる。	2-(1)-③	S	全体最適化計画を効果的に、効率的に実現するため、情報システム部門は、自社内の資源とともに外部資源も適切に活用し、組織体の情報化ニーズや投資効果に見合った体制にする必要がある。
2.3	人的資源管理の方針	全社				
(1)	情報技術に関する人的資源の現状及び必要とされる人材を明確にすること。	全社	組織体は全体最適化の達成に必要な人材を確保する		S	組織体は全体最適化の目標を達成するために、自組織内における情報技術に関する人的資源の現状を適切に把握し、今後必要とされる人材、能力を明らかにする必要がある。
(2)	人的資源の調達及び育成の方針を明確にすること。	全社	組織体は全体最適化に必要な人材を確保する		S	組織体の情報化に必要な人材の現状および将来計画に従って、人的資源の採用、育成の方針を明文化し、これを周知する必要がある。
3.	情報化投資					
(1)	情報化投資計画は、経営戦略との整合性を考慮して策定すること。	－	情報化投資を経営課題の解決に役立たせる			情報化投資を経営課題の解決に役立たせるため、経営に与える利益効果、業務処理の改善等の全体最適化の観点から、経営戦略と整合性をもった情報化投資計画を策定する必
(2)	情報化投資計画の決定に際して、影響、効果、期間、実現性等の観点から複数の選択肢を検討すること。	－	情報化投資計画を利害関係者の合意の上で決定する			情報化投資計画を利害関係者の合意の上で決定するために、影響、効果、期間、実現性等の観点から複数の選択肢を挙げて検討し、最適なものを選択する必要がある。
(3)	情報化投資に関する予算を適切に執行すること。	－	情報化投資計画を確実に実行する			情報化投資計画を確実に実行するため、適切な時期、金額、契約形態等で予算を執行する必要がある。

システム管理基準の管理項目と統制目標の対応（例）

項番	システム管理基準の管理項目	統制種別	統制目標（例）	ガイダンス項番	C/S種別	システム管理基準の趣旨
(4)	情報化投資に関する投資効果の算出方法を明確にすること。	－	情報化投資の効果を客観的に評価し、今後の情報化投資計画にフィードバックする			情報化投資の効果を客観的に評価し、今後の情報化投資計画にフィードバックするため、投資効果の算出方法を事前に明確にしておく必要があ
(5)	情報システムの全体的な業績及び個別のプロジェクトの業績を財務的な観点から評価し、問題点に対して対策を講じること。	－	情報システムの全体的な業績及び個別のプロジェクトの業績を財務的な課題を早期に発見し適切な対策を講じる			情報システムの全体的な業績及び個別のプロジェクトの業績を財務的な課題を早期に発見し適切な対策を講じるために、財務的な観点からのモニタリングを行うとともに、想定される課題については事前に対応手順を準備しておく必要がある。
(6)	投資した費用が適正に使用されたことを確認すること。	－	情報化投資を計画通りに行い、また計画とのずれがあった場合にそれを適切に修正する			情報化投資を計画通りに行い、また計画とのずれがあった場合にそれを適切に修正するために、投資金額、用途等を確認する必要がある。
4.	情報資産管理の方針					
(1)	情報資産の管理方針及び体制を明確にすること。	－	組織体の経営上重要な資産である情報資産を適切に管理し、有効利用する	2-(3)-②	C	組織体の経営上重要な資産である情報資産を適切に管理し、有効利用するため、管理の方針を定め、その体制を明確にする必要がある。
(2)	情報資産のリスク分析を行い、その対応策を考慮すること。	－	情報資産の信頼性、安全性を確保する	2-(2)-①	C	情報資産の信頼性、安全性を確保するため、情報資産が持っている顕在的なリスクや潜在的なリスクについて洗い出し、それぞれの大きさを決定し、対応策を講じる必要がある。
(3)	情報資産の効率的で有効な活用を考慮すること。	－	経営戦略や情報戦略の目的を達成する		S	経営戦略や情報戦略の目的を達成するため、情報化投資の方針に基づき、情報資産を効率的かつ有効に活用する必要がある。
(4)	情報資産の共有化による生産性向上を考慮すること。	－	経営戦略や情報戦略の目的を達成する			経営戦略や情報戦略の目的を達成するため、情報資産の共有化による生産性向上を図る必要がある。
5.	事業継続計画					
(1)	情報システムに関連した事業継続の方針を策定すること。	－	組織体の事業継続性を確保する			組織体の事業継続性を確保するため、情報システムに関連した事業継続の方針を定める必要がある。

項番	システム管理基準の管理項目	統制種別	統制目標（例）	ガイダンス項番	C/S種別	システム管理基準の趣旨
(2)	事業継続計画は、利害関係者を含んだ組織的体制で立案し、組織体の長が承認すること。	－	事業継続に関わる事象が発生した場合に全ての利害関係者が円滑に対応できるようにする			事業継続に関わる事象が発生した場合に全ての利害関係者が円滑に対応できるようにするため、利害関係者を含んだ組織体制で実行性の高い事業継続計画を立案し、組織体の長が承認する必要がある。
(3)	事業継続計画は、従業員の教育訓練の方針を明確にすること。	－	事業継続に関わる脅威が発生しても、迅速かつ確実に事業継続計画に定められた手続を実行できるようにする			事業継続に関わる脅威が発生しても、迅速かつ確実に事業継続計画に定められた手続を実行できるようにするため、事業継続計画には従業員の教育訓練の方針を明確にする必要が
(4)	事業継続計画は、関係各部に周知徹底すること。	－	事業継続計画の実行性を高める			事業継続計画の実行性を高めるため、事業継続計画を関係者に周知徹底する必要がある。
(5)	事業継続計画は、必要に応じて見直すこと。	－	事業継続計画の有効性を維持する			事業継続計画の有効性を維持するため、必要に応じて見直し及び更新を行う必要がある。
6.	コンプライアンス					
(1)	法令及び規範の管理体制を確立するとともに、管理責任者を定めること。	－	法令及び規範を遵守し適切に管理する			法令及び規範を遵守し適切に管理していくためには、組織として、法令及び規範の所管部署を明らかにし、管理体制を確立するとともに、管理責任者を定めて管理を推進する必要があ
(2)	遵守すべき法令及び規範を識別し、関係者に教育及び周知徹底すること。	－	組織として遵守すべき法令及び規範を明確に識別し特定する			法令及び規範を遵守し適切に管理していくためには、組織として遵守すべき法令及び規範を明確に識別し特定することが必要である。その上で、特定した法令及び規範を関係者に知らせるための教育体制を確立し、関係者に周知徹底する必要がある。
(3)	情報倫理規程を定め、関係者に教育及び周知徹底すること。	－	組織体として、法令及び規範を遵守し適切に管理する			組織体として、法令及び規範を遵守し適切に管理していくためには、組織体内の遵守すべきルールとして、情報倫理規程を定めるとともに、組織体内外の関係者に教育し、周知徹底する必要が必要である。

項番	システム管理基準の管理項目	統制種別	統制目標（例）	ガイダンス項番	C/S種別	システム管理基準の趣旨
(4)	個人情報の取扱い、知的財産権の保護、外部へのデータ提供等に関する方針を定めること。	－	組織体としての考え方を明確にした方針を定める			法令及び規範を遵守していく上で、組織体内外の各種権利保護の観点から、個人情報の取扱い、知的財産権の保護、外部へのデータ提供等に関して、組織体としての考え方を明確にした方針を定める必要がある。
(5)	法令、規範及び情報倫理規程の遵守状況を評価し、改善のために必要な方策を講じること。	－	組織としての遵守状況を定期的に点検・評価し、指摘事項に対し改善する			法令及び規範を遵守し適切に管理していくために、特定した法令及び規範、また社内ルールとして策定した情報倫理規程等について、組織としての遵守状況を定期的に点検・評価し、指摘事項に対し改善のために必要な方策を講ずる必要がある。
Ⅱ	企画業務					
Ⅱ．1	開発計画	全般				
(1)	開発計画は、組織体の長が承認すること。	全般	組織体として開発計画を実行に移すための意思決定を行う。		C	開発計画が全体最適化計画に基づいていることを確認し、開発計画を実行に移すため、組織体の長が承認する必要がある。
(2)	開発計画は、全体最適化計画との整合性を考慮して策定すること。	全般	開発する情報システムは、組織体として最大の効果をあげる必要がある。		S	開発する情報システムは、関連する他の情報システムと役割を分担し、組織体として最大の効果をあげる機能を実現するため、開発計画は、全体最適化計画との整合性を考慮して策定する必要がある。
(3)	開発計画は、目的、対象業務、費用、スケジュール、開発体制、投資効果等を明確にすること。	全般	情報システムの目的、機能等について関係者が共通認識を持ち、情報システムの投資効果を確認する		S	情報システムの目的、機能等について関係者が共通認識を持ち、情報システムの投資効果を確認するため、開発計画は、目的、対象業務、費用、スケジュール、開発体制、投資効果等を明確にする必要がある。
(4)	開発計画は、関係者の教育及び訓練計画を明確にすること。	全般	情報システムの品質を保ちスケジュールどおりに実現する。		S	開発計画で策定した情報システムの品質を保ちスケジュールどおりに実現するため、開発関係者の計画に対する理解の統一と技術力を向上させる教育及び訓練計画を明確にする必

項番	システム管理基準の管理項目	統制種別	統制目標（例）	ガイダンス項番	C/S種別	システム管理基準の趣旨
(5)	開発計画は、ユーザ部門及び情報システム部門の役割分担を明確にすること。	全般	開発、運用及び保守業務を効果的に実施する。		S	開発、運用及び保守業務を効果的に実施するため、ユーザ部門と情報システム部門の役割分担を明確にし、相互に確認しておく必要がある。
(6)	開発計画は、開発、運用及び保守の費用の算出基礎を明確にすること。	全般	情報システムのライフサイクルを通した費用を合理的に算出する		S	情報システムのライフサイクルを通した費用を合理的に算出するために、開発計画は、開発、運用及び保守に関する費用の算出根拠を明確にする必要がある。
(7)	開発計画はシステムライフを設定する条件を明確にすること。	全般	情報システムのシステムライフを合理的に見積もる		S	情報システムのシステムライフを合理的に見積もるため、システムライフの条件を明確にする必要がある。
(8)	開発計画の策定に当たっては、システム特性及び開発の規模を考慮して形態及び開発方法を決定すること。	全般	全体最適化計画と整合性をとり、情報システムを最も効率よく開発する		S	全体最適化計画と整合性をとり、情報システムを最も効率よく開発するため、開発計画の策定にあたっては、システム特性及び開発の規模を考慮して情報システムの形態及び開発方法を決定する必要がある。
(9)	開発計画の策定に当たっては、情報システムの目的を達成する実現可能な代替案を作成し、検討すること。	全般	情報システムに要求される機能、能力、品質等を最も効率よく実現する		S	情報システムに要求される機能、能力、品質等を最も効率よく実現するために、複数のシステム実現案を作成し、比較及び評価する必要がある。
2.	分析	全般				
(1)	開発計画に基づいた要求定義は、ユーザ、開発、運用及び保守の責任者が承認すること。	全般	ユーザ、開発、運用及び保守の各部門の理解を一致させ、確定させる		C	要求定義の内容についてユーザ、開発、運用及び保守の各部門の理解を一致させ、確定したものとするため、要求定義は、ユーザ、開発、運用及び保守の責任者が承認する必要が
(2)	ユーザニーズの調査は、対象、範囲及び方法を明確にすること。	全般	ユーザニーズを的確に反映する		S	ユーザニーズを的確に反映するため、事前にユーザニーズの調査の対象、範囲及び方法を明確にする必要
(3)	実務に精通しているユーザ、開発、運用及び保守の担当者が参画して現状分析を行うこと。	全般	現行業務処理の流れ、手続、業務量等を把握する		S	現行業務を的確かつ効率的に分析し、現行業務処理の流れ、手続、業務量等を把握するため、現状分析は、実務に精通したユーザ、開発、運用及び保守の担当者が参画する必

システム管理基準の管理項目と統制目標の対応（例）

項番	システム管理基準の管理項目	統制種別	統制目標（例）	ガイダンス項番	C/S種別	システム管理基準の趣旨
(4)	ユーザニーズは文書化し、ユーザ部門が確認すること。	全般	ユーザニーズの調査結果を的確に開発計画の策定、開発業務に反映する		S	ユーザニーズの調査結果を的確に開発計画の策定、開発業務に反映するため、ユーザニーズは文書化し、ユーザ部門の責任者が確認することが必要である。
(5)	情報システムの導入に伴って発生する可能性のあるリスク分析を実施すること。	全般	情報システムの健全な運用のため		C	情報システムの健全な運用を図るため、情報システムの導入に伴って発生する可能性のあるリスクを分析する必要がある。
(6)	情報システムの導入によって影響を受ける業務、管理体制、諸規程等は、見直し等の検討を行うこと。	全般	報システムの導入によって生じる業務、管理体制、諸規定等への影響を的確に把握する		S	情報システムの導入によって生じる業務、管理体制、諸規定等への影響を的確に把握し、情報システムの運用を円滑に行うため、業務等の新設、改変及び廃止、管理体制の変更、及び諸規程の見直しを行う必要
(7)	情報システムの導入効果の定量的及び定性的評価を行うこと。	全般	開発計画のモニタリング（効果の定量、定性評価）		－	開発計画で算出した効果に基づいて、合理的に効果を算出するため、情報システムの効果の定量的及び定性的評価を行う必要がある。
(8)	パッケージソフトウェアの使用に当たっては、ユーザニーズとの適合性を検討すること。	全般	導入計画の見直しモニタリング（パッケージソフトの評価）		－	情報システムが、期待された機能、効果を得られることを確認するため、パッケージソフトウェアの導入に際しては、機能、効果の観点からユーザニーズとパッケージソフトウェアの適合性を確認する必要がある。
3.	調達	全般				
(1)	調達の要求事項は、開発計画及びユーザニーズに基づき作成し、ユーザ、開発、運用及び保守の責任者が承認すること。	全般	開発計画に従って構築する情報システムの機能、性能、品質等を満足させる要求事項をまとめる	3-(1)-①-ニ	C	構築する情報システムの機能、性能、品質等の要求を計画に従って達成するために、情報システムの構築に必要な各種の資源の調達要求事項は、開発計画及びユーザニーズに基づき作成し、ユーザ、開発、運用及び保守の責任者が承認する必要が
(2)	ソフトウェア、ハードウェア及びネットワークは、調達の要求事項を基に選択すること。	全般	要求される機能、能力等を備えたシステム構成とする		S	要求される機能、能力等を備えたシステム構成とするため、開発計画及びユーザニーズに基づき、ソフトウェア、ハードウェア、ネットワーク等を選択する必要がある。

項番	システム管理基準の管理項目	統制種別	統制目標（例）	ガイダンス項番	C/S種別	システム管理基準の趣旨
(3)	開発を遂行するために必要な要員、予算、設備、期間等を確保すること。	全般	情報システムの開発を計画通りに実施する		S	情報システムの開発を着実に行うため、必要な要員、予算、設備、期間等を確保する必要がある。
(4)	要員に必要なスキルを明確にすること。	全般	情報システムの開発を計画通りに実施する		S	開発計画で策定された機能、性能及び品質を実現するために、開発にかかる組織内要員、組織外要員に必要なスキルを明確にする必要がある。
(5)	ソフトウェア、ハードウェア及びネットワークの調達は、ルールに従って実施すること。	全般	情報システムの開発を計画通りに実施する		S	開発における必要な資源を適時に、要求事項に整合性をとり調達するために、ソフトウェア、ハードウェア及びネットワークの調達は、ルールに従って行う必要がある。
(6)	調達した資源は、ルールに従って管理すること。	全般	情報システムの開発を計画通りに実施する		S	資源を開発計画に準拠し効果的に利活用するため、調達した資源は、ルールに従って管理する必要があ
Ⅲ	開発業務					
1.	開発手順	全般				
(1)	開発手順は、開発の責任者が承認すること。	全般	開発手順がシステム分析及び要求定義で定めた要員、予算、期間等を満たしていることを確認する	3-(1)-①-イ	C	開発手順が、システム分析及び要求定義で定めた要員、予算、期間等を満たしていることを確認するため、文書化された開発手順を開発の責任者が承認する必要がある。
(2)	開発手順は、開発方法に基づいて作成すること。	全般	開発手順は、組織体として標準化されている	3-(1)-①-イ	S	組織体として一貫し、効率的な開発作業を確実に遂行するため、開発手順は、組織体として標準化された開発方法に基づいて作成する必要があ
(3)	開発手順は、開発の規模、システム特性等を考慮して決定すること。	全般	情報システムを効率よく開発し、かつ要求された品質を確保する		S	情報システムを効率よく開発し、かつ要求された品質を確保するため、開発手順は、情報システムの規模、期間、特性等を考慮して決定する必要
(4)	開発時のリスクを評価し、必要な対応策を講じること。	全般	情報システムを開発計画どおりに高品質で効率よく開発する	2-(2)-②	C	情報システムを開発計画どおりに高品質で効率よく開発するため、開発プロセス全般におけるリスクの洗い出しと評価を実施し、必要な対策を講ずる必要がある。
2.	システム設計	全般				

付録2－1　　システム管理基準の管理項目と統制目標の対応（例）

項番	システム管理基準の管理項目	統制種別	統制目標（例）	ガイダンス項番	C/S種別	システム管理基準の趣旨
(1)	システム設計書は、ユーザ、開発、運用及び保守の責任者が承認すること。	全般	システム設計書の品質を確保し、要求定義との整合性を図り、ユーザ、開発要員及び運用担当者の共有物とする	3-(1)-①-イ	C	システム設計書の品質を確保し、要求定義との整合性を図り、ユーザ、開発要員及び運用担当者の共有物とするため、システム設計書は、ユーザ、開発、運用及び保守の責任者が承認する必要がある。
(2)	運用及び保守の基本方針を定めて設計すること。	全般	運用及び保守作業を円滑かつ効果的に推進する	3-(1)-④-イ	C	運用及び保守作業を円滑かつ効果的に推進するため、システム設計段階で運用及び保守の基本方針を定め、設計に反映しておく必要がある。
(3)	入出力画面、入出力帳票等はユーザの利便性を考慮して設計すること。	全般	データ入力時のミスの防止、作業効率の向上及び出力情報の利用効率の向上を図る		S	データ入力時のミスの防止、作業効率の向上及び出力情報の利用効率の向上を図るため、入出力帳票、入出力画面及びコードは、ユーザが利用しやすいように設計する必要があ
(4)	データベースは、業務の内容及びシステム特性に応じて設計すること。	全般	大量及び多種のデータを効率よく格納し、検索し、更新できる	3-(1)-①-ロ	C	大量及び多種のデータを効率よく格納し、データ群の中から必要な情報を要求定義を満たす性能で検索し、更新できるようにするため、データベースは業務の内容に応じて設計する必
(5)	データのインテグリティを確保すること。	全般	データ処理の正確性を保証する	3-(1)-①-ロ 3-(1)-②-イ	C	データ処理の正確性を保証し、データ入力から出力に至るすべての過程におけるデータの誤びゅう、重複、脱落等を防止し、改ざんがないことを示すため、データのインテグリティを確保する必要がある。
(6)	ネットワークは、業務の内容及びシステム特性に応じて設計すること。	全般	ネットワークは、要求定義を満たす性能とする	3-(1)-②-イ	C	大量及び多種のデータの要求定義を満たす性能で伝送するため、ネットワークは、業務の内容及びシステム特性に応じて設計する必要がある。
(7)	情報システムの性能は、要求定義を満たすこと。	全般	システムに期待される効果を実現する	3-(1)-②-イ	C	情報システムに期待される効果を実現するため、情報システムの性能は、要求定義を満たす必要がある。

システム管理基準の管理項目と統制目標の対応（例）

項番	システム管理基準の管理項目	統制種別	統制目標（例）	ガイダンス項番	C/S種別	システム管理基準の趣旨
(8)	情報システムの運用性及び保守性を考慮して設計すること。	全般	情報システムの円滑な運用を図り、トラブルの原因を速やかに発見し、有効な対策、改善等のための保守作業を効果的に行う		S	情報システムの円滑な運用を図り、トラブルの原因を速やかに発見し、有効な対策、改善等のための保守作業を効果的に行うため、運用業務及び保守業務で必要となる性能管理、構成管理、障害対策等の技術的な実現方法を考慮した上で設計する必要が
(9)	他の情報システムとの整合性を考慮して設計すること。	全般	ITインフラストラクチャや他の情報システムと整合する	3-(1)-①-ハ	S	システムの設計を行う場合、当該システムだけではなく、ITインフラストラクチャや他の情報システムとの整合性を考慮して設計を行う必要がある。
(10)	情報システムの障害対策を考慮して設計すること。	全般	情報システムの障害発生を未然に防止し、障害の影響を最小限にとどめ、速やかに回復させる		S	情報システムの障害発生を未然に防止し、障害の影響を最小限にとどめ、速やかに回復させるため、情報システムの障害対策を考慮して設計する必要がある。
(11)	誤謬防止、不正防止、機密保護等を考慮して設計すること。	全般	情報システムの安全性を確保し、健全な運用を確保する	3-(1)-①-ロ	C	情報システムの安全性を確保し、健全な運用を確保するため、誤びゅう防止、不正防止、機密保護及びプライバシー保護の機能を考慮して設計する必要がある。
(12)	テスト計画は、目的、範囲、方法、スケジュール等を明確にすること。	全般	情報システムが設計どおりに開発されたことを確実かつ効率的に確認する	3-(1)-①-ホ	C	情報システムが設計どおりに開発されたことを確実かつ効率的に確認するため、テスト計画の目的、範囲、方法、スケジュール等を明確にする必
(13)	情報システムの利用に係る教育の方針、スケジュール等を明確にすること。	全般	情報システムを円滑に導入し、期待される効果を実現する		S	情報システムを円滑に導入し、期待される効果を実現するため、情報システムの利用にかかわるユーザ教育方針、スケジュール等を設計時に明確にする必要がある。
(14)	モニタリング機能を考慮して設計すること。	全般	当該システムが設計どおりの性能を発揮しているかを確認できる	5-(2)-②-イ	C	システムの稼動後に、システム開発計画の主旨に基づき、当該システムが設計どおりの性能を発揮しているかを確認するため、システム内にモニタリングの機能を組み込み、定期的に測定・解析する必要がある。

項番	システム管理基準の管理項目	統制種別	統制目標（例）	ガイダンス項番	C/S種別	システム管理基準の趣旨
(15)	システム設計書をレビューすること。	全般	システム設計書は、情報システムに対するユーザ要求を適切に反映させている		S	システム設計書は、情報システムに対するユーザ要求を適切に反映させている必要があり、ユーザ、開発、運用及び保守の各部門の関係者も参加してレビューを行い、適切に評価する必要がある。
3.	プログラム設計	全般				
(1)	プログラム設計書は、開発の責任者が承認すること。	全般	プログラム設計書の品質を確保し、システム設計との整合性を図り、確実なプログラミング作業を可能にする	3-(1)-①-イ	C	プログラム設計書の品質を確保し、システム設計との整合性を図り、確実なプログラミング作業を可能にするため、プログラム設計書は、開発の責任者が承認する必要がある。
(2)	システム設計書に基づいて、プログラムを設計すること。	全般	システム設計で定義された機能及びシステムの構造を過不足なく正確にプログラムに反映する		S	システム設計で定義された機能及びシステムの構造を過不足なく正確にプログラムに反映するため、システム設計書に基づいて、プログラムを設計する必要がある。
(3)	テスト要求事項を定義し、文書化すること。	全般	プログラム設計及びプログラミングの結果の妥当性を確認する		S	プログラム設計及びプログラミングの結果の妥当性を確認するために、テスト要求事項を定義し文書化する必要がある。
(4)	プログラム設計書及びテスト要求事項をレビューすること。	全般	プログラム設計の品質を高める		S	プログラム設計の品質を高めるために、プログラム設計書及びテスト要求事項をレビューする必要がある。
(5)	プログラム設計時に発見したシステム設計の矛盾は、システム設計の再検討を行って解決すること。	全般	システム設計及びプログラム設計の整合性を確保する		S	システム設計及びプログラム設計の整合性を確保するため、プログラム設計時に発見したシステム設計の矛盾は、システム設計の再検討を行って解決する必要がある。
4.	プログラミング	全般				
(1)	プログラム設計書に基づいてプログラミングすること。	全般	プログラム設計書で定義された機能を過不足なく正確にプログラムに反映する		C	プログラム設計書で定義された機能を過不足なく正確にプログラムに反映するため、プログラム設計書に基づいてプログラミングする必要があ
(2)	プログラムコードはコーディング標準に適合していること。	全般	プログラムの品質を確保		S	プログラムの品質を確保するため、プログラムコードはコーディング標準に適合している必要がある。

項番	システム管理基準の管理項目	統制種別	統制目標（例）	ガイダンス項番	C/S種別	システム管理基準の趣旨
(3)	プログラムコード及びプログラムテスト結果を評価し、記録及び保管すること。	全般	プログラミングされた機能が、プログラム設計書に過不足なく正確に稼動することを検証し、プログラムテストの妥当性を確認する		C	プログラミングされた機能が、プログラム設計書に過不足なく正確に稼動することを検証し、プログラムテストの妥当性を確認するため、プログラムコートの評価及びプログラムテストの結果を記録及び保管する必要があ
(4)	重要プログラムは、プログラム作成者以外の者がテストすること。	全般	プログラミングにおける誤びゅう及び不正を防止する	3-(1)-①-ホ	C	プログラミングにおける誤びゅう及び不正を防止するため、重要なプログラムは、作成者以外の者がテストする必要がある。
5.	システムテスト・ユーザ受入れテスト	全般				
(1)	システムテスト計画は、開発及びテストの責任者が承認すること。	全般	システムテスト計画の妥当性を確保する	3-(1)-①-ホ 3-(1)-④-ロ	C	システムテスト計画の妥当性を確保するため、システム計画書は開発及びテストの責任者が承認する必要が
(2)	ユーザ受入れテスト計画は、ユーザ及び開発の責任者が承認すること。	全般	ユーザ受入れテスト計画の妥当性を確保する	3-(1)-①-ホ	C	ユーザ受入れテスト計画の妥当性を確保するため、ユーザ受入れテスト計画書はユーザ及び開発の責任者が承認する必要がある。
(3)	システムテストに当たっては、システム要求事項を網羅してテストケースを設定して行うこと。	全般	システム要求を満足していることを確認する	3-(1)-①-ホ	S	システム要求を満足していることを確認するため、システム要求事項を網羅してテストケースを設定し、システムテストを実施する必要がある。
(4)	テストデータの作成及びシステムテストは、テスト計画に基づいて行うこと。	全般	システムテストの目的を確実かつ効率的に達成する	3-(1)-①-ホ	S	システムテストの目的を確実かつ効率的に達成するため、テスト計画に基づいてテストデータの作成及びシステムテストを実施する必要がある。
(5)	システムテストは、本番環境と隔離された環境で行うこと。	全般	本番環境に影響を与えないシステムテストを実施する	3-(1)-①-ホ 3-(1)-④-ハ	S	システムテストを実施することで本番環境に悪影響を及ぼすことが考えられるため、システムテストは本番環境と隔離された環境で実施する必要が
(6)	システムテストは、開発当事者以外の者が参画すること。	全般	開発した情報システムが全体として機能することを公正かつ客観的に検証する	3-(1)-①-ホ	C	開発した情報システムが全体として機能することを公正かつ客観的に検証するため、開発当事者以外の者が参画する必要がある。
(7)	システムテストは、適切なテスト手法及び標準を使用すること。	全般	効率的でかつ効果的にシステムテストを実施する	3-(1)-①-ホ	S	効率的でかつ効果的にシステムテストを実施するため、適切なテスト手法及び標準を採用し、使用する必要が

項番	システム管理基準の管理項目	統制種別	統制目標（例）	ガイダンス項番	C/S種別	システム管理基準の趣旨
(8)	ユーザ受入れテストは、本番同様の環境を設定すること。	全般	ユーザ要求事項の妥当性を確認する	3-(1)-①-ホ 3-(1)-④-ニ	S	ユーザ要求事項の妥当性を確認するため、ユーザ受入れテストは本番同様の環境を設定する必要がある。
(9)	ユーザ受入れテストは、ユーザマニュアルに従い、本番運用を想定したテストケースを設定して実施すること。	全般	ユーザ受入れテストは、ユーザの視点でユーザが自ら本番運用を想定して実施する	3-(1)-①-ホ 3-(1)-④-ホ	S	ユーザ受入れテストは、ユーザの視点でユーザが自ら本番運用を想定して実施する最終確認のテストであるため、要件定義書やユーザマニュアルに従い、本番運用を想定したテストケースを設定して実施する必要があ
(10)	ユーザ受入れテストは、ユーザ及び運用の担当者もテストに参画して確認すること。	全般	ユーザ受入れテストは、本番運用を想定して実施する	3-(1)-①-ホ 3-(1)-④-ヘ	S	ユーザ受入れテストは、本番運用を想定して実施する最終確認のテストであり、本番開始後のトラブルを最少化させるため、業務に精通したユーザ及び運用の担当者もテストに参画して確認する必要がある。
(11)	システムテスト及びユーザ受入れテストの結果は、ユーザ、開発、運用及び保守の責任者が承認すること。	全般	システムテスト及びユーザ受入れテストの結果に対する理解を一致させる	3-(1)-①-ホ	C	システムテスト及びユーザ受入れテストの結果に対する理解を一致させるため、ユーザ、開発、運用及び保守の責任者が承認する必要がある。
(12)	システムテスト及びユーザ受入れテストの経過及び結果を記録及び保管すること。	全般	運用業務におけるトラブルの原因究明の基礎データとする	3-(1)-①-ホ 3-(1)-④-ト	C	運用業務におけるトラブルの原因究明の基礎データとするとともに、保守業務の作業に備えるため、システムテスト及びユーザ受入れテストの結果を記録及び保管する必要がある。
(13)	パッケージソフトウェアを調達する場合、開発元が品質テストを実施したことを確認すること。	全般	パッケージソフトウェアの開発元が品質テストを実施したことを確認する	3-(1)-①-ホ	S	パッケージソフトウェアを採用して情報システムを構築する場合、情報システムの品質はパッケージソフトウェアの品質に影響されるため、パッケージソフトウェアの開発元が品質テストを実施したことを確認する必要があ
6.	移行	全般				

付録2－1　　システム管理基準の管理項目と統制目標の対応（例）

項番	システム管理基準の管理項目	統制種別	統制目標（例）	ガイダンス項番	C/S種別	システム管理基準の趣旨
(1)	移行計画を策定し、ユーザ、開発、運用及び保守の責任者が承認すること。	全般	システムの開発・テスト段階から運用段階に円滑にかつ効率的に移行する		C	移行は、開発計画に基づき開発部門がシステムを利用するユーザ部門、運用する運用部門、保守作業を行う保守部門に引き渡す作業であり、システムの開発・テスト段階から運用段階に円滑にかつ効率的に移行するため、移行計画を策定し、各部門の責任者が承認する必要がある。
(2)	移行作業は文書に記録し、責任者が承認すること。	全般	運用段階における稼働を確実なものとする		S	運用段階における稼働を確実なものとするため、開発業務の作業成果を本番環境に移行した作業結果を文書として記録し、責任者が承認する必要
(3)	移行完了の検証方法を移行計画で明確にすること。	全般	情報システムの本番稼動環境が整ったことを確認する		S	情報システムの本番稼動環境が整ったことを確認するため、移行完了の検証方法を移行計画書で明確にする必要がある。
(4)	移行計画に基づいて、移行に必要な要員、予算、設備等を確保すること。	全般	移行計画どおりに作業を実施する		S	移行計画どおりに作業を実施するため、移行に必要な要員、予算、設備等を確保する必要がある。
(5)	移行は手順書を作成し、実施すること。	全般	移行作業をの実施にあたって、漏れ、重複、評価・確認不足などを防止する		S	移行計画どおりに移行作業を実施し、漏れ、重複、評価・確認不足などを防止するため、また移行作業を行う要員の教育を兼ね、移行の手順書を作成し事前確認を行う必要がある。
(6)	移行時のリスク対策を検討すること。	全般	移行時における有害事象を特定する		S	移行時における有害事象の影響を特定し、その影響を最小限に抑えるため、移行時にもリスク対策を検討しておく必要がある。
(7)	運用及び保守に必要なドキュメント、各種ツール等は開発の責任者から引き継いでいること。	全般	システムの運用及び保守が円滑に入れるようにする		S	移行作業終了後正式稼動前までに、システムの運用及び保守の関係者が円滑にそれぞれの作業に入れるよう設計書、テスト結果、移行結果、各種ツール類と操作マニュアル等が開発の責任者から引き継がれている必要
(8)	移行は関係者に周知徹底すること。	全般	当該システムに関連するシステムの運用に支障をきたさない		S	当該システム及び内外の関連するシステムのそれぞれの運用に支障をきたさないため、関係者に対し、移行の概要を周知徹底する必要がある。

システム管理基準の管理項目と統制目標の対応（例）

項番	システム管理基準の管理項目	統制種別	統制目標（例）	ガイダンス項番	C/S種別	システム管理基準の趣旨
Ⅳ	運用業務					
1.	運用管理ルール	全般				
(1)	運用管理ルール及び運用手順は、運用の責任者が承認すること。	全般	運用管理のルール及び運用手順を制定し、承認する	3-(2)-①-イ	C	運用管理ルール及び運用手順は、運用を円滑かつ効率的に行うために必要なものであり、運用の責任者があらかじめ内容を確認し、承認をする必
(2)	運用管理ルールは、運用設計に基づいて作成すること。	全般	運用業務を効率よく実施する	3-(2)-①-イ	S	運用管理ルールは、各アプリケーション及び基本となるインフラストラクチャの設計時の運用設計に基本原則が定められているので、運用設計に基づいて作成されている必要がある。大規模システムで全体最適化計画に基づく運用管理方式が定められていたり、サービスを利用する運用形態をとる場合は、それらの基本運用管理方式に基づき作成する必要がある。
(3)	運用手順は、運用設計及び運用管理ルールに基づいて、規模、期間、システム特性等を考慮して作成すること。	全般	運用業務を効率よく実施する		S	運用業務を効率よく実施するため、運用設計及び運用管理ルールに基づき、さらに規模、期間、システム特性から運用手順を決定する必要があ
(4)	運用設計及び運用管理ルールに基づいて、担当責任者を定めること。	全般	運用の担当責任者を明確にする		S	運用を円滑に行う上で担当責任者を明確にすることは、通常運用以外に例外処理、障害対応などで迅速な意思決定が発生する場面で特に重要であり、システム機能等の単位で担当責任者を決める必要がある。
2.	運用管理	全般				
(1)	年間運用計画を策定し、責任者が承認すること。	全社	年度単位で運用計画を策定する	3-(2)-①-ロ	C	情報システムの運用を円滑に行い、各情報システムのイベントをスケジュール通りに消化推進するため、年度単位で運用計画を策定し、関係者の合意の上、責任者が承認し、関係者に周知徹底する必要がある。
(2)	年間運用計画に基づいて、月次、日次等の運用計画を策定すること。	全社	情報システムの運用を円滑かつ効率的に進める	3-(2)-①-ロ	S	情報システムの運用を円滑かつ効率的に進めるため、年間運用計画に基づいて月次、日次等の運用計画を策定する必要がある。

システム管理基準の管理項目と統制目標の対応（例）

項番	システム管理基準の管理項目	統制種別	統制目標（例）	ガイダンス項番	C/S種別	システム管理基準の趣旨
(3)	運用管理ルールを遵守すること。	全般	情報システムにかかわる誤びゅう及び不正を防止する	3-(2)-①-ロ	C	運用の標準化を図り、情報システムにかかわる誤びゅう及び不正を防止するため、管理体制、手続等、ルールとして定められた基準に従って運用管理を行う必要がある。
(4)	ジョブスケジュールは、業務処理の優先度を考慮して設定すること。	全般	運用における資源を有効利用する	3-(2)-①-ニ	S	資源を有効利用し、ユーザニーズに対応した業務処理を行うため、ジョブスケジュールは、業務の優先度を考慮して設定する必要がある。
(5)	オペレーションは、ジョブスケジュール及び指示書に基づいて行うこと。	全般	操作上の誤り及び不正を防止する	3-(2)-①-ニ	S	資源を有効に活用し、操作上の誤り及び不正を防止するため、ジョブスケジュール及び指示書に基づいたオペレーションを実施する必要がある。
(6)	例外処理のオペレーションは、運用管理ルールに基づいて行うこと。	全般	操作上の誤り及び不正を防止する	3-(2)-①-ハ	C	操作上の誤り及び不正を防止し、業務処理を円滑に行うため、例外処理は、運用管理ルールに基づいて適格に行う必要がある。
(7)	オペレータの交替は、運用管理ルールに基づいて行うこと。	全般	業務処理を正確かつ円滑に遂行する		S	業務処理を正確かつ円滑に遂行するため、オペレータの交替は、運用管理ルールに基づいて行う必要があ
(8)	ジョブスケジュール及びオペレーション実施記録を採り、ジョブスケジュールとの差異分析を行うこと。	全般	操作上の誤り及び不正を防止		S	操作上の誤り及び不正を防止し、業務処理を円滑に遂行するため、ジョブスケジュールとオペレーション実施記録の差異分析を行う必要がある。
(9)	オペレーション実施記録は、運用管理ルールに基づいて一定期間保管すること。	全般	操作上の誤り、不正、事故及び障害の原因を究明する	3-(2)-①-ホ	C	操作上の誤り、不正、事故及び障害の原因を究明するため、オペレーション実施記録は、運用管理ルールに基づいて一定期間保管する必要があ
(10)	事故及び障害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。	全般	事故及び障害の規模や影響度に応じて対応する	3-(3)-③-イ	C	事故及び障害は、発生箇所や大きさに応じて影響度も大きくなるため、規模や影響度に応じて対応を柔軟に変えていくエスカレーションフローを明確にし、適切な処置と同時に影響の拡大を最小限に抑制する必要がある。
(11)	事故及び障害の内容を記録し、情報システムの運用の責任者に報告すること。	全般	事故及び障害の迅速な回復及び再発防止	3-(2)-①-ヘ 3-(3)-③-ロ 3-(3)-③-ハ	S	事故及び障害の迅速な回復及び再発防止のため、事故及び障害の内容を記録し、運用の責任者に報告する必要がある。

項番	システム管理基準の管理項目	統制種別	統制目標（例）	ガイダンス項番	C/S種別	システム管理基準の趣旨
(12)	事故及び障害の原因を究明し、再発防止の措置を講じること。	全般	事故及び障害の迅速な回復及び再発防止	3-(2)-①-ヘ	S	事故及び障害の発生を防止するため、発生時に原因を明らかにし、再発を防止する処置を講ずる必要があ
(13)	情報システムのユーザに対する支援体制を確立すること。	全般	EUC業務への貢献と円滑な処理を行う	3-(2)-①-ト	S	EUC等を中心にユーザの情報処理への利用機会が増加しており、業務への貢献と円滑な処理のため、情報システム部門が中心となってユーザに対する支援体制を確立する必要が
(14)	情報セキュリティに関する教育及び訓練をユーザに対して実施すること。	全般	ユーザの情報セキュリティに関する意識を向上させる	3-(2)-①-ト	S	ユーザの情報セキュリティに関する意識を向上させるため、教育及び訓練を実施する必要がある。
(15)	情報システムの稼動に関するモニタリング体制を確立すること。	全般	情報システムの信頼性、安全性、効率性、有効性、リソース等を確認・管理する	5-(2)-②-ロ	C	情報システムの信頼性、安全性、効率性、有効性、リソース等を確認・管理するため、情報システムの稼動に関するモニタリング体制を確立する必
(16)	情報システムの稼動実績を把握し、性能管理及び資源の有効利用を図ること。	全般	情報システムの費用対効果を高める		S	情報システムの費用対効果を高めるため、情報システムのモニタリング結果に基づき、稼動実績の把握と分析を行い、関係者で討議した後、性能管理及び資源の有効利用を図る必
3.	入力管理	業務				
(1)	入力管理ルールを定め、遵守すること。	業務	情報システムへのデータ入力に伴う一連の作業について手順、検証方法、承認方法を明文化する	4-(1)-①	C	入力データの作成、授受、検証、入力の実施、入力後の確認、保管等、情報システムへのデータ入力に伴う一連の作業について手順、検証方法、承認方法を入力管理ルールとして明文化し、遵守する必要がある。
(2)	データの入力は、入力管理ルールに基づいて漏れなく、重複なく、正確に行うこと。	業務	入力データに欠落、二重入力等の誤りが発生しない	4-(1)-②	S	情報システムにデータを入力する際は、入力データに欠落、二重入力等の誤りが発生しないように入力管理ルールに記載されている手順に従い、正確に行う必要がある。
(3)	入力データの作成手順、取扱い等は誤謬防止、不正防止、機密保護等の対策を講じること。	業務	入力データの作成、取扱い等での不正を防止する		S	入力データの作成、取扱い等を正確に行ない、不正を防止するため、データの作成手順、取扱い等は、誤びゅう防止、不正防止及び機密保護等の対策を講じる必要がある。

項番	システム管理基準の管理項目	統制種別	統制目標（例）	ガイダンス項番	C/S種別	システム管理基準の趣旨
(4)	データの入力の誤謬防止、不正防止、機密保護等の対策は有効に機能すること。	業務	データを正確に入力する	4-(1)-③	S	データを正確に入力するための誤びゅう防止、不正防止、機密保護、及び個人情報保護の対策は有効に機能する必要がある。
(5)	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。	業務	入力データの紛失、盗難、漏えい等を防止する	4-(1)-④	S	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必要が
4.	データ管理	業務				
(1)	データ管理ルールを定め、遵守すること。	全般／業務	データの誤処理防止、機密保護及び個人情報保護	3-(2)-③-イ 4-(2)-①	C	データの誤処理防止、機密保護及び個人情報保護のため、開発、運用及び保守業務に応じたデータの取扱い、管理の体制等をルールとして明文化し、遵守する必要がある。
(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。	全般／業務	データへの不正アクセスの防止、不正利用の防止、機密保護及び個人情報保護	3-(3)-②-イ 4-(2)-②	C	データへの不正アクセスの防止、不正利用の防止、機密保護及び個人情報保護のため、アクセスコントロール及びモニタリングが有効に機能していることを確認する必要がある。
(3)	データのインテグリティを維持すること。	全般／業務	データを正確かつ完全にする	3-(2)-③-ハ 4-(2)-③	C	データが正確かつ完全であり、正常である状態を保つためにデータが正しく更新される必要がある。
(4)	データの利用状況を記録し、定期的に分析すること。	業務	データの不正利用を防止する		S	データの利用を予想し、不正利用を防止するため、データの利用状況を記録し、定期的に分析する必要があ
(5)	データのバックアップの範囲、方法及びタイミングは、業務内容、処理形態及びリカバリの方法を考慮して決定すること。	業務	データの記録媒体の障害、誤操作、コンピュータウイルス等による影響を最小にする	3-(2)-③-ニ	C	データの記録媒体の障害、誤操作、コンピュータウイルス等による影響を最小にするため、データのバックアップの範囲及びタイミングは、業務内容、処理形態及びリカバリの方法を考慮して決定する必要がある。
(6)	データの授受は、データ管理ルールに基づいて行うこと。	全般／業務	データの誤使用、不正利用、改ざん等を防止する	3-(2)-③-イ 3-(2)-③-ロ 4-(2)-④	S	データの誤使用、不正利用、改ざん等を防止するため、データの授受は、データ管理ルールに基づいて行う必要がある。
(7)	データの交換は、不正防止及び機密保護の対策を講じること。	全般／業務	データの不正利用の防止、機密情報の漏えい及び個人情報保護	3-(2)-③-ロ 4-(2)-⑤	S	不正利用の防止、機密情報の漏えい及び個人情報保護のため、データの交換は、不正防止及び機密保護の対策を講ずる必要がある。

項番	システム管理基準の管理項目	統制種別	統制目標（例）	ガイダンス項番	C/S種別	システム管理基準の趣旨
(8)	データの保管、複写及び廃棄は、誤謬防止、不正防止及び機密保護の対策を講じること。	業務	データの不正利用、漏えいの防止及び個人情報の侵害等を防止する	4-(2)-⑥	C	データの不正利用、漏えいの防止及び個人情報の侵害等を防止するため、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講ずる必要がある。
(9)	データに対するコンピュータウイルス対策を講じること。	業務	コンピュータウイルスから保護する		S	データをコンピュータウイルスから保護するため、コンピュータウイルス対策を講ずる必要がある。
(10)	データの知的財産権を管理すること。	－	構築したデータの知的財産権の保護及び外部から導入したデータの知的財産権の侵害を防止			構築したデータの知的財産権の保護及び外部から導入したデータの知的財産権の侵害を防止するため、知的財産権を管理する必要がある。
5.	出力管理	業務				
(1)	出力管理ルールを定め、遵守すること。	業務	出力での誤びゅう、不正利用、漏えい等を防止し、機密保護及び個人情報保護する	4-(3)-①	C	出力方法の誤びゅう、不正利用、漏えい等を防止し、機密及び個人情報保護のため、情報の出力手続、承認等のルールを定め、遵守する必要が
(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。	業務	出力情報に結果の誤り、欠落、二重出力などの発生を防ぐ	4-(3)-②	C	情報システムからデータ出力を行う際は、出力情報に結果の誤り、欠落、二重出力などが発生しないように出力管理ルールに記載されている手順に従い、正確に行う必要がある。
(3)	出力情報の作成手順、取扱い等は、誤謬防止、不正防止及び機密保護の対策を講じること。	業務	改ざん、盗難、漏えい等を防止する	4-(3)-③	C	出力情報の作成、取扱い等を正確に行い、改ざん、盗難、漏えい等を防止するため、誤びゅう防止、不正防止及び機密保護の対策を講ずる必要があ
(4)	出力情報の引渡しは、出力管理ルールに基づいて行うこと。	業務	出力情報の引渡しの誤り、紛失、盗難等を防止する	4-(3)-④	S	出力情報の引渡しの誤り、紛失、盗難等を防止するため、引渡し手続き等のルールを定め、遵守する必要が
(5)	出力情報の保管及び廃棄は、出力管理ルールに基づいて行うこと。	業務	出力情報の紛失、盗難、漏えい等を防止する	4-(3)-⑤	S	出力情報の紛失、盗難、漏えい等を防止するため、保管及び廃棄は、出力管理ルールに基づいて行う必要が
(6)	出力情報のエラー状況を記録し、定期的に分析すること。	業務	出力情報を正確に維持する		S	出力情報を正確に維持するため、エラー状況を記録し、定期的に分析する必要がある。
(7)	出力情報の利用状況を記録し、定期的に分析すること。	業務	出力情報の有効活用を図る		S	出力情報の有効活用を図るため、利用状況を記録し、定期的に分析する必要がある。

システム管理基準の管理項目と統制目標の対応（例）

項番	システム管理基準の管理項目	統制種別	統制目標（例）	ガイダンス項番	C/S種別	システム管理基準の趣旨
6.	ソフトウェア管理	全般				
(1)	ソフトウェア管理ルールを定め、遵守すること。	全般	ソフトウェアの適切な利用と不正を防止する	3-(2)-②-イ	C	ソフトウェアの適切な利用及び不正防止のため、開発、運用及び保守業務に応じたソフトウェアの取扱い、管理の体制等をルールとして定め、遵守する必要がある。
(2)	ソフトウェア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。	全般	ソフトウェアの不正利用を防止する	3-(2)-②-ロ 3-(3)-②-イ	C	ソフトウェアの不正利用を防止するため、アクセスコントロール及びモニタリングが有効に機能していることを確認する必要がある。
(3)	ソフトウェアの利用状況を記録し、定期的に分析すること。	全般	ソフトウェアの不正利用を防止する		S	ソフトウェアの稼動効率の向上を図り、不正利用を防止するため、ソフトウェアの利用状況を記録し、定期的に分析する必要がある。
(4)	ソフトウェアのバックアップの範囲、方法及びタイミングは、業務内容及び処理形態を考慮して決定すること。	全般	ソフトウェアの記録媒体の障害、誤操作、コンピュータウイルス等によるリスクを最小にする		S	ソフトウェアの記録媒体の障害、誤操作、コンピュータウイルス等による影響を最小にするため、ソフトウェアのバックアップの範囲及び方法は、業務内容及び処理形態を考慮して定める必要がある。
(5)	ソフトウェアの授受は、ソフトウェア管理ルールに基づいて行うこと。	全般	ソフトウェアの誤使用、不正利用、改ざん等を防止する		S	ソフトウェアの誤使用、不正利用、改ざん等を防止するため、ソフトウェアの授受は、手順、方法等を定めたソフトウェア管理ルールに基づいて行う必要がある。
(6)	ソフトウェアの保管、複写及び廃棄は、不正防止及び機密保護の対策を講じること。	全般	ソフトウェアの誤使用、不正利用、改ざん等を防止		S	ソフトウェアの不正利用、漏えい等を防止するため、ソフトウェアの保管、複写及び不要ソフトウェアの廃棄は、不正防止及び機密保護の対策を講ずる必要がある。
(7)	ソフトウェアに対するコンピュータウイルス対策を講じること。	全般	ソフトウェアをコンピュータウイルスから保護する		S	ソフトウェアをコンピュータウイルスから保護するため、コンピュータウイルス対策を講ずる必要がある。
(8)	ソフトウェアの知的財産権を管理すること。	－	開発したソフトウェアの知的財産権の保護及び導入したソフトウェアの知的財産権の侵害を防止する			開発したソフトウェアの知的財産権の保護及び導入したソフトウェアの知的財産権の侵害を防止するため、知的財産権を管理する必要がある。

システム管理基準の管理項目と統制目標の対応（例）

項番	システム管理基準の管理項目	統制種別	統制目標（例）	ガイダンス項番	C/S種別	システム管理基準の趣旨
(9)	フリーソフトウェアの利用に関し、組織体としての方針を明確にすること。	全般	フリーソフトウェアによるリスクを最小にする		S	フリーソフトウェアは便利に低コストで使える反面、処理結果の無保証、コンピュータウイルス混入の危険性、知的財産権侵害等のリスクもあり、利用の際は、組織体として一定の方針を定める必要がある。
7.	ハードウェア管理	全般				
(1)	ハードウェア管理ルールを定め、遵守すること。	全般	ハードウェアの適切な利用を図り、障害を防止し、自然災害、不正行為等から保護する	3-(2)-②-イ	C	ハードウェアの適切な利用を図り、障害を防止し、自然災害、不正行為等から保護するため、ハードウェア管理ルールを定め、遵守する必要があ
(2)	ハードウェアは、想定されるリスクに対応できる環境に設置すること。	全般	障害、自然災害、不正行為等が情報システムに及ぼす影響を最少にする	3-(2)-②-ト 3-(3)-②-イ	C	障害、自然災害、不正行為等が情報システムに及ぼす影響を最少にするため、ハードウェアは想定されるリスクに対応できる環境に設置する必要がある。
(3)	ハードウェアは、定期的に保守を行うこと。	全般	ハードウェア障害による情報システムの停止及び機能低下を未然に防止する		S	ハードウェア障害による情報システムの停止及び機能低下を未然に防止するため、定期的に保守を実施する必要がある。
(4)	ハードウェアは、障害対策を講じること。	全般	情報システムの稼動停止及び機能低下を防止する	3-(2)-②-ホ	S	情報システムの稼動停止及び機能低下を防止し、障害発生時の早期普及のため、ハードウェアの障害対策を講ずる必要がある。
(5)	ハードウェアの利用状況を記録し、定期的に分析すること。	全般	ハードウェアの有効利用を図り、不正利用を防止する		S	ハードウェアの有効利用を図り、不正利用を防止するため、利用状況を記録し、定期的に分析する必要がある。
(6)	ハードウェアの保管、移設及び廃棄は、不正防止及び機密保護の対策を講じること。	全般	ハードウェアの盗難、紛失、廃棄等による機密情報の漏えい防止		S	ハードウェアの盗難、紛失等による権限者以外のハードウェア利用の防止、及びデータ等の情報資産保護のため、ハードウェアの保管、移設及び廃棄は、不正防止及び機密保護の対策を講ずる必要がある。
8.	ネットワーク管理	全般				
(1)	ネットワーク管理ルールを定め、遵守すること。	全般	ネットワークを正常かつ効率的に稼働させる		C	ネットワークの正常かつ効率的な稼働のため、ネットワーク管理ルールを定め、遵守する必要がある。

システム管理基準の管理項目と統制目標の対応（例）

項番	システム管理基準の管理項目	統制種別	統制目標（例）	ガイダンス項番	C/S種別	システム管理基準の趣旨
(2)	ネットワーク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。	全般	ネットワークへの侵入及び不正利用を防ぐ		S	ネットワークへの侵入及び不正利用を未然に防止し、早期に発見するため、ネットワークへのアクセスコントロール及びモニタリングが有効に機能していることを確認する必要があ
(3)	ネットワーク監視ログを定期的に分析すること。	全般	ネットワークへの侵入及び不正利用を防ぐ		S	ネットワークへの侵入及び不正利用を検出して必要な対策を講ずるために、ネットワーク監視ログを定期的に分析する必要がある。
(4)	ネットワークは、障害対策を講じること。	全般	情報システム及び電子メールやWebなどの各種サービスの可用性を確保する	3-(2)-②-ホ	C	情報システム及び電子メールやWebなどの各種サービスの可用性を確保するため、ネットワークの障害対策を講ずる必要がある。
(5)	ネットワークの利用状況を記録し、定期的に分析すること。	全般	ネットワークを効率的に安定稼働させる		S	ネットワークの効率的で安定した稼働を図るため、利用状況を記録し、定期的に分析する必要がある。
(6)	ネットワークを利用したサービスについて、組織体としての方針を明確にすること。	全般	ネットワークを組織体として効率的に利用する		S	ネットワークを利用した情報提供等のサービスについて、組織体としての方針を明確にして、効率的にサービスを利用する必要がある。
9.	構成管理	全般				
(1)	管理すべきソフトウェア、ハードウェア及びネットワークの対象範囲を明確にし、管理すること。	全般	ソフトウェア、ハードウェア及びネットワークを適切に管理する		C	ユーザ、ネットワーク管理の責任者、ベンダ間で、管理すべきソフトウェア、ハードウェア及びネットワークの二重管理の防止、及び管理の漏れが生じないように、管理の対象範囲を明確にして効率的に管理する必要があ
(2)	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、サポート条件等を明確にすること。	全般	情報システムの機能維持及び障害時の早期回復を図る	3-(2)-②-ニ	C	情報システムの機能維持及び障害時の早期回復を図るため、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、サポート条件等を明確にする必要がある。
(3)	ソフトウェア、ハードウェア及びネットワークの導入並びに変更は、影響を受ける範囲を検討して決定すること。	全般	情報システムの停止、機能低下等を防止し、安定稼働を図る	3-(2)-②-ト	S	情報システムの停止、機能低下等を防止し、安定稼働を図るため、ソフトウェア、ハードウェア及びネットワークの導入及び変更は、影響を受ける範囲を検討して決定する必要がある。

項番	システム管理基準の管理項目	統制種別	統制目標（例）	ガイダンス項番	C/S種別	システム管理基準の趣旨
(4)	ソフトウェア、ハードウェア及びネットワークの導入並びに変更は、計画的に実施すること。	全般	情報システムに与える影響を最少にする		S	情報システムに与える影響を最少にするため、ソフトウェア、ハードウェア及びネットワークの導入及び変更を計画的に実施する必要がある。
10.	建物・関連設備管理	全社				
(1)	建物及び関連設備は、想定されるリスクに対応できる環境に設置すること。	全社	情報システムの停止、破壊等による被害を最少にする建物、設備にする			情報システムの停止、破壊等による被害を最少にするため、建物及び関連設備は、想定されるリスクを回避できる環境に設置する必要がある。
(2)	建物及び室への入退の管理は、不正防止及び機密保護の対策を講じること。	全社	情報システムを隔離して不正行為から保護する			情報システムを不正行為から保護するため、建物及び室の入退管理に不正防止及び機密保護の対策を講ずる必要がある。
(3)	関連設備は、適切な運用を行うこと。（追加）	全社	情報システムを継続して同じ環境に保つ			関連設備は、管理・運用を行う上でのルールを定め、遵守することにより、継続的、安定的に運用する必要があ
(4)	関連設備は、定期的に保守を行うこと。	全社	関連設備の障害による情報システムの停止、機能低下等を防止する			関連設備の障害による情報システムの停止、機能低下等を未然に防止するため、定期的に保守する必要があ
(5)	関連設備は、障害対策を講じること。	全社	関連設備の障害を未然に防止し、早期に回復させる			関連設備の障害を未然に防止し、あるいは早期に回復させるため、障害対策を講ずる必要がある。
(6)	建物及び室への入退の管理を記録し、定期的に分析すること。	全社	入館及び入室者を特定し、追跡調査を可能とする（不正や犯罪の未然防止）			建物及び室に関する入退管理の要件として、事故発生時に入館及び入室者を特定し、追跡調査を可能とする必要がある。そのため、入館及び入室の状況を記録するとともに、入退管理の責任者が定期的に分析する
V	**保守業務**					
1.	保守手順	全般				
(1)	保守ルール及び保守手順は、保守の責任者が承認すること。	全般	保守業務を円滑に実施する		C	保守業務の標準化を図り、円滑かつ信頼性を確保して保守業務を実施するため、保守ルール及び保守手順を定め、保守業務の責任者が承認する必要がある。

システム管理基準の管理項目と統制目標の対応（例）

項番	システム管理基準の管理項目	統制種別	統制目標（例）	ガイダンス項番	C/S種別	システム管理基準の趣旨
(2)	保守手順は、保守の規模、期間、システム特性等を考慮して決定すること。	全般	保守業務を効率よく実施する		S	保守業務を効率よく実施するため、保守のルールに基づいて、保守の規模、期間、システム特性等から保守手順を決定する必要がある。
(3)	保守時のリスクを評価し、必要な対応策を講じること。	全般	システム障害等の各種トラブルを発生させないようにする		S	保守の実施によって、システム障害等の各種トラブルを発生させないため、想定されるリスクを洗い出し、評価した上で必要な対応策を講ずる必
2.	保守計画	全般				
(1)	保守計画はユーザ及び保守の責任者が承認すること。	全般	保守の範囲及び作業内容を明確にする		C	保守の範囲及び作業内容を明確にするため、調査及び分析結果に基づいて保守計画を策定し、ユーザ及び保守の責任者が承認する必要があ
(2)	変更依頼等に対し、保守の内容及び影響範囲の調査並びに分析を行うこと。	全般	保守作業を円滑に行う		S	変更依頼等の内容を正確に把握し、保守作業を円滑に行うため、保守の内容及び影響範囲を調査し、分析を行う必要がある。
(3)	保守のテスト計画は、目的、範囲、方法、スケジュール等を明確にすること。	全般	保守を円滑に実施する		S	保守のテストを円滑に実施するため、目的、範囲、方法、スケジュール等を設定したテスト計画を作成する必要
3.	保守の実施	全般				
(1)	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、ユーザ及び保守の責任者が承認すること。	全般	保守における誤びゅう、不正、機能の欠落等を防止・低減する	3-(1)-③-ヘ	C	誤びゅう、不正、機能の欠落等を防止・低減するため、保守計画に基づいてシステム設計書、プログラム設計書等を変更し、ユーザ及び保守の責任者が承認する必要がある。
(2)	プログラムの変更は、保守手順に基づき、保守の責任者の承認を得て実施すること。	全般	プログラムの変更等の誤びゅう及び不正を防止する	3-(1)-③-ト	C	プログラムの変更等の誤びゅう及び不正防止のため、保守手順に基づき、保守の責任者が承認する必要が
(3)	変更したプログラム設計書に基づいてプログラミングしていることを検証すること。	全般	プログラミング時の誤びゅうを防止する	3-(1)-③-チ	C	プログラミング時の誤びゅうを防止するため、変更したプログラム設計書に基づいてプログラミングしていることを検証する必要がある。
4.	保守の確認	全般				

システム管理基準の管理項目と統制目標の対応（例）

項番	システム管理基準の管理項目	統制種別	統制目標（例）	ガイダンス項番	C/S種別	システム管理基準の趣旨
(1)	変更したプログラムのテストの実施は、保守のテスト計画に基づいて行うこと。	全般	プログラムのテストを円滑かつ確実に実施する	3-(1)-③-リ	C	プログラムのテストを円滑かつ確実に実施するため、変更したプログラムは保守のテスト計画に基づいて行う必要がある。
(2)	変更したプログラムは、影響範囲を考慮してテストを行うこと。	全般	情報システムの機能及び性能に影響させない		S	情報システムの機能及び性能の低下をもたらさないため、変更したプログラムは、影響範囲を考慮してテストを行う必要がある。
(3)	変更したプログラムのテストは、ユーザが参画し、ユーザマニュアルに基づいて実施すること。	全般	情報システムが変更依頼等の要求を満たしていることを確認する	3-(1)-③-ヌ	S	情報システムが変更依頼等の要求を満たしていることを確認するため、プログラムのテストは、ユーザが参画し、ユーザマニュアルに基づいて実施する必要がある。
(4)	変更したプログラムのテストの結果は、ユーザ、運用及び保守の責任者が承認すること。	全般	情報システムの機能及び性能を確認する	3-(1)-③-ル	C	テストの妥当性を確認し、情報システムの機能及び性能を確認するため、テストの結果をユーザ、運用及び保守の責任者が承認する必要がある。
(5)	変更したプログラムのテストの結果を記録及び保管すること。	全般	テストの妥当性を確認する	3-(1)-③-ワ	C	テストの妥当性を確認し、障害等のトラブルの原因究明の基礎データとするため、テストデータ及びテスト結果を記録し、保管する必要がある。
5.	移行	全般				
(1)	移行手順は、移行の条件を考慮して作成すること。	全般	移行を正確にかつ円滑に行う		S	移行を正確にかつ円滑に行うため、期間、方法、体制等の条件を明確にし、移行手順を作成する必要がある。
(2)	変更前のプログラム及びデータのバックアップを行うこと。	全般	移行のトラブルに備える		S	移行のトラブルに備えるため、変更前のプログラム及びデータのバックアップを行う必要がある。
(3)	運用及び保守の責任者は、他の情報システムへ影響を与えないことを確認すること。	全般	移行による他の情報システムの機能及び性能低下等を防止する		S	他の情報システムの機能及び性能低下等を防止するため、運用及び保守の責任者は、情報システムの移行が及ぼす影響を確認する必要がある。
6.	情報システムの廃棄	全般				

項番	システム管理基準の管理項目	統制種別	統制目標（例）	ガイダンス項番	C/S種別	システム管理基準の趣旨
(1)	旧情報システムは、リスクを考慮して廃棄計画を策定し、ユーザ、運用及び保守の責任者の承認を得て廃棄すること。	全般	情報システムの廃棄によるリスクを最小にする		S	旧情報システムの廃棄を円滑かつ確実に実施するため、リスクを考慮した廃棄計画を策定し、ユーザ、運用及び保守の責任者の承認を得て廃棄する必要がある。
(2)	旧情報システムの廃棄方法及び廃棄時期は、不正防止及び機密保護の対策を考慮して決定すること。	全般	情報システムの廃棄に伴う不正防止、機密保護及びプライバシー保護		S	不正防止、機密保護及びプライバシー保護のため、廃棄方法及び廃棄時期は、不正防止及び機密保護の対策を考慮して決定する必要がある。
Ⅵ	共通業務					
1.	ドキュメント管理					
1.1	作成	全社				
(1)	ドキュメントは、ユーザ`部門及び情報システム部門の責任者が承認すること。	全社	ドキュメントの品質を確保し、組織体の共有物とする	3-(1)-⑤-イ	C	ドキュメントの品質を確認し、組織体の共有物とするため、ドキュメントは、ユーザ部門及び情報システム部門の責任者が承認する必要がある。
(2)	ドキュメント作成ルールを定め、遵守すること。	全社	組織体として一貫したドキュメントを作成する	3-(1)-⑤-イ	S	組織体として一貫したドキュメントを作成するため、体系、記述形式、記述内容等をルールとして定め、遵守する必要がある。
(3)	ドキュメントの作成計画を策定すること。	全社	必要なドキュメントを確実に作成する	3-(1)-⑤-イ	S	必要なドキュメントを確実に作成するため、ドキュメント作成計画を策定する必要がある。
(4)	ドキュメントの種類、目的、作成方法等を明確にすること。	全社	ドキュメントを使用目的に応じ効率よく作成する	3-(1)-⑤-イ	S	ドキュメントの種類の過不足を防ぎ、使用目的に応じ効率よく作成するため、ドキュメントの種類、目的、作成方法等をドキュメントの作成計画で明確にする必要がある。
(5)	ドキュメントは、作成計画に基づいて作成すること。	全社	ドキュメントには、必要な内容を網羅し、必要な時期までに用意する	3-(1)-⑤-イ	S	ドキュメントは、必要な内容を網羅し、必要な時期までに用意するために、作成計画に基づいて作成する必要がある。
1.2	管理	全社				

付録2－1　　システム管理基準の管理項目と統制目標の対応（例）

項番	システム管理基準の管理項目	統制種別	統制目標（例）	ガイダンス項番	C/S種別	システム管理基準の趣旨
(1)	ドキュメントの更新内容は、ユーザ部門及び情報システム部門の責任者が承認すること。	全社	変更したドキュメントの品質を確保する		C	変更したドキュメントの品質を確認し、組織体の共有物とするため、ドキュメントは、ユーザ部門及び情報システム部門の責任者が承認する必要
(2)	ドキュメント管理ルールを定め、遵守すること。	全社	情報システムの内容と整合したドキュメントを維持し、利用を円滑にする		S	情報システムの内容と整合したドキュメントを維持し、利用を円滑にするため、原本及び配布されたドキュメントの管理ルールを定め、遵守する必要
(3)	情報システムの変更に伴い、ドキュメントの内容を更新し、更新履歴を記録すること。	全社	情報システムの内容と整合したドキュメントを維持し、最新の状態を明確にする		S	情報システムの内容と整合したドキュメントを維持し、最新の状態を明確にするため、情報システムの変更時に関連ドキュメントの内容を更新し、更新履歴を記録する必要がある。
(4)	ドキュメントの保管、複写及び廃棄は、不正防止及び機密保護の対策を講じること。	全社	ドキュメントの不正利用、漏洩等を防止する		S	ドキュメントの不正利用、漏洩等を防止するため、ドキュメントの保管、複写及び不要ドキュメントの廃棄は、不正防止及び機密保護の対策を講ずる必要がある。
2.	進捗管理					
2.1	実施	全般				
(1)	進捗計画に基づいて方法、体制等を定め、ユーザ、企画、開発、運用及び保守の責任者が承認すること。	全般	企画、開発、運用及び保守業務を計画どおりに遂行する		C	企画、開発、運用及び保守業務を計画どおりに遂行するため、各々の特性に応じた進捗管理の方法、体制等を明確にし、責任者が承認する必
(2)	ユーザ、企画、開発、運用及び保守の責任者は、進捗状況を把握すること。	全般	問題点を早期に発見する		S	問題点を早期に発見するため、ユーザ、企画、開発、運用及び保守の責任者は、作業の進捗状況を的確に把握する必要がある。
(3)	進捗の遅延等の対策を講じること。	全般	企画、開発、運用及び保守業務を計画どおりに遂行する		S	企画、開発、運用及び保守業務を計画どおりに遂行するため、進捗の遅延等の対策を講ずる必要がある。
2.2	評価	全般				

システム管理基準の管理項目と統制目標の対応（例）

項番	システム管理基準の管理項目	統制種別	統制目標（例）	ガイダンス項番	C/S種別	システム管理基準の趣旨
(1)	業務の工程終了時に、計画に対する実績を分析及び評価し、責任者が承認すること。	全般	次工程の計画の見直し及び進捗管理の方法等の改善、並行実施または将来実施される同種の工程の計画へのフィードバックを図る		S	次工程の計画の見直し及び進捗管理の方法等の改善、並行実施または将来実施される同種の工程の計画へのフィードバックを図るため、企画、開発、運用及び保守業務の工程終了時に計画に対する作業実績を分析及び評価する必要がある。
(2)	評価結果は、次工程の計画に反映すること。	全般	次工程の計画の実現可能性を高める		S	次工程の計画の実現可能性を高めるため、評価結果を次工程の計画に反映する必要がある。
(3)	評価結果は、進捗管理の方法、体制等の改善に反映すること。	全般	進捗管理の作業を効率的かつ効果的に遂行する		S	進捗管理の作業を効率的かつ効果的に遂行するため、評価結果を進捗管理の方法、体制等の改善に反映する必要がある。
3.	品質管理					
3.1	計画(2)	全社				
(1)	品質目標に基づいて品質管理の計画を定め、ユーザ、企画、開発、運用及び保守の責任者が承認すること。	全社	組織体の目標を達成するに足る品質を維持する		C	情報システムのライフサイクルの全てにおいて組織体の目標を達成するに足る品質を維持するための品質管理計画は、品質管理を円滑かつ効果的に行うために必要なものであり、ユーザ、企画、開発、運用及び保守の責任者が承認を行う必要がある。
(2)	品質管理計画は、方法、体制等を明確にすること。	全社	組織体の品質管理マネジメントシステムを円滑に実施する		S	品質管理計画は、組織体の品質管理マネジメントシステムを円滑に実施するために、その実施方法、体制、実施時期等を明確にする必要がある。品質管理計画は、全体最適化計画の中で定められた品質管理方針を具体化
3.2	実施	全般				
(1)	業務の工程終了時に、計画に対する実績を分析及び評価し、責任者が承認すること。	全般	業務の品質管理目標を評価する		S	業務が計画どおりに実施され、品質管理目標を達成したか評価するために、その実績を品質管理ルールに基づき、計画に対する実績を分析及び評価して、責任者が承認する必要が

システム管理基準の管理項目と統制目標の対応（例）

項番	システム管理基準の管理項目	統制種別	統制目標（例）	ガイダンス項番	C/S種別	システム管理基準の趣旨
(2)	評価結果は、品質管理の基準、方法、体制等の改善に反映すること。	全般	組織体の品質管理目標を達成する		S	品質管理の評価結果は、組織体の品質管理目標を達成するための継続的な改善活動に役立てるため、品質管理の基準、方法、体制等の改善に反映する必要がある。
4.	人的資源管理					
4.1	責任・権限	全社				
(1)	要員の責任及び権限は、業務の特性及び業務遂行上の必要性に応じて定めること。	全社	誤びゅう及び不正を防止し、機密を保護する		C	企画、開発、運用及び保守業務を効率的に遂行し、誤びゅう及び不正を防止し、機密を保護するため、要員の責任及び権限を定める必要があ
(2)	要員の責任及び権限は、業務環境及び情報環境の変化に対応した見直しを行うこと。	全社	業務環境及び情報環境の変化に適応させる		S	業務環境及び情報環境の変化に適応させるため、要員の責任及び権限は定期的又は適切なタイミングで見直す必要がある。
(3)	要員の責任及び権限を周知徹底すること。	全社	業務を効率的かつ確実に遂行し、要員相互の連携を図る		S	企画、開発、運用及び保守業務を効率的かつ確実に遂行し、要員相互の連携を図るため、責任及び権限を個々の要員に周知徹底する必要が
4.2	業務遂行	全般				
(1)	要員は、権限を遵守すること。	全般	誤びゅう及び不正を防止する	2-(1)-③	C	誤びゅう及び不正を防止し、企画、開発、運用及び保守業務を効率的かつ確実に遂行するため、要員は権限を遵守する必要がある。
(2)	作業分担及び作業量は、要員の知識、能力等から検討すること。	全般	目的とした成果物の品質を確保する		S	企画、開発、運用及び保守業務を計画に基づき遂行し、目的とした成果物の品質を確保するため、作業分担及び作業量を要員の知識、能力等から検討する必要がある。
(3)	要員の交替は、誤謬防止、不正防止及び機密保護を考慮して行うこと。	全般	要員交代に伴う誤びゅう及び不正を防止する		S	要員交替に際しては、引継ぎミス等による誤びゅう発生の防止、担当を外れた要員による不正の防止、機密保護を考慮する必要がある。
(4)	不測の事態に備えた代替要員の確保を検討すること。	全般	業務の継続性を維持する		S	企画、開発、運用及び保守業務の継続性を維持するため、不測の事態に備えた代替要員の確保を検討しておく必要がある。

項番	システム管理基準の管理項目	統制種別	統制目標（例）	ガイダンス項番	C/S種別	システム管理基準の趣旨
4.3	教育・訓練	全社				
(1)	教育及び訓練に関する計画及びカリキュラムは、人的資源管理の方針に基づいて作成及び見直しを行うこと。	全社	組織体として一貫した教育及び訓練を行う	2-(1)-④	C	組織体として一貫した教育及び訓練を行うため、人的資源管理の方針に基づいたカリキュラムを作成し、情報技術の進歩等に応じて見直す必要
(2)	教育及び訓練に関する計画及びカリキュラムは、技術力の向上、業務知識の習得、情報システムの情報セキュリティ確保等から検討すること。	全社	要員の質的向上を図る	2-(1)-④	S	要員の質的向上を図るため、教育及び訓練のカリキュラムは、技術力の向上、業務知識の習得及び情報セキュリティの確保等から検討する必
(3)	教育及び訓練は、計画及びカリキュラムに基づいて定期的かつ効果的に行うこと。	全社	業務の遂行に必要な知識、能力等を習得させる	2-(1)-④	S	要員が、企画、開発、運用及び保守業務の遂行に必要な知識、能力等を習得するため、教育及び訓練は、カリキュラムに基づいて定期的かつ効果的に行う必要がある。
(4)	要員に対するキャリアパスを確立し、業務環境及び情報環境の変化に対応した見直しを行うこと。	全社	業務の遂行に必要な知識、能力等を習得させる		S	企画、開発、運用及び保守業務の遂行に必要な知識、能力等を習得させるため、キャリアパスを確立し、業務環境及び情報環境の変化に対応した見直しを行う必要がある。
4.4	健康管理					
(1)	健康管理を考慮した作業環境を整えること。	－	要員が身体的及び精神的に健康を保ち、業務を健全に遂行する			要員が身体的及び精神的に健康を保ち、企画、開発、運用及び保守業務を健全に遂行するため、健康管理を考慮した作業環境を整える必要が
(2)	健康診断及びメンタルヘルスケアを行うこと。	－	要員の身体面及び精神面について管理する			要員の健康を維持するため身体面及び精神面についての健康診断及びカウンセリングを行う必要がある。
5.	委託・受託					
5.1	計画	全般				
(1)	委託又は受託の計画は全体最適化計画に基づいて策定し、責任者が承認すること。	全般	委託又は受託業務の内容を具体化する	3-(4)-①-イ	S	委託又は受託の方針は、全体最適化計画の外部資源の活用（「Ⅰ．情報戦略　1．全体最適化　1．3　全体最適化計画の策定（7）」）の中で策定される。委託又は受託業務の内容を具体化するために委託又は受託の計画を策定し、責任者が承認する必要があ

項番	システム管理基準の管理項目	統制種別	統制目標（例）	ガイダンス項番	C/S種別	システム管理基準の趣旨
(2)	委託又は受託の目的、対象範囲、予算、体制等を明確にすること。	全般	委託又は受託業務の内容を明らかし、業務を円滑に遂行する	3-(4)-①-ロ	C	委託又は受託業務の内容を明らかし、業務を円滑に遂行するため、目的、対象範囲、体制、予算等を明確にする必要がある。
(3)	委託又は受託は、具体的な効果、問題点等を評価して決定すること。	全般	委託又は受託業務を確実に達成する		S	委託又は受託の目的を確実に達成するため、委託又は受託は具体的な効果、問題点、リスク等を評価した上で決定する必要がある。
5.2	委託先選定	全般				
(1)	委託先の選定基準を明確にすること。	全般	委託計画に基づいて委託先を選定する	3-(4)-①-ハ	C	委託計画に基づいて委託先を選定するために、選定基準を明確にする必要がある。
(2)	委託候補先に必要な要求仕様を提示すること。	全般	提案書を作成する際の受託条件を明確にする		S	提案書を作成する際の受託条件を明確にするため、委託候補先に必要な要求仕様を提示する必要がある。
(3)	委託候補先が提示した提案書の比較検討を行うこと。	全般	最適な委託先を公正に選定する		S	最適な委託先を公正に選定するため、選定基準に基づいて、委託先が提案した提案書を比較検討する必要
5.3	契約	全般				
(1)	契約は、委託契約ルール又は受託契約ルールに基づいて締結すること。	全般	委託契約を確実に行う		C	委託契約を確実に行うため、委託契約ルール又は受託契約ルールに基づいて締結する必要がある。
(2)	コンプライアンスに関する条項を明確にすること。	全般	情報の不正利用、漏えい、プライバシーの侵害等を防止する		S	情報の不正利用、漏えい、プライバシーの侵害等を防止するため、契約時に不正防止、機密保護等の対策を明確にする必要がある。
(3)	再委託の可否について明確にすること。	全般	再委託に係わるトラブルを防止する		S	再委託に係わるトラブルを防止するため、契約時に再委託の可否を明確にする必要がある。
(4)	知的財産権の帰属を明確にすること。	全般	知的財産権にかかわるトラブルを防止する		S	知的財産権にかかわるトラブルを防止するため、契約時に知的財産権の帰属を明確にする必要がある。
(5)	特約条項及び免責条項を明確にすること。	全般	問題発生を想定する		S	問題の発生が想定される事項に対応するため、契約時の特約条項及び免責条項を明確にする必要がある。

項番	システム管理基準の管理項目	統制種別	統制目標（例）	ガイダンス項番	C/S種別	システム管理基準の趣旨
(6)	業務内容及び責任分担を明確にすること。	全般	委託業務を円滑に遂行する	3-(4)-①-ヘ	S	委託業務を円滑に遂行するために、契約書、仕様書に委託業務の内容、責任分担を明確にする必要があ
(7)	契約締結後の業務内容に追加及び変更が生じた場合、契約内容の再検討を行うこと。	全般	委託先の委託業務内容を明確にし、円滑な業務を実施する		S	委託先の委託業務内容を明確にし、円滑な業務を実施するために、契約締結後の業務の内容に追加及び変更が生じた場合、契約内容の再検討を行う必要がある。
(8)	システム監査に関する方針を明確にすること。	全般	委託先の委託業務内容の信頼性、安全性、効率性の確保を担保する		S	委託先の委託業務内容の信頼性、安全性、効率性の確保を担保するために、委託契約にシステム監査に関する方針を明確にする必要がある。
5.4	委託業務	全般				
(1)	委託業務の実施内容は、契約内容と一致すること。	全般	委託業務の内容を過不足なく実施する		C	委託業務の内容を過不足なく実施するため、委託業務の実施内容は、契約書に記載された内容と一致させる必要がある。
(2)	契約に基づき、必要な要求仕様、データ、資料等を提供すること。	全般	委託業務を委託計画どおりに遂行する		S	委託業務を委託計画どおりに遂行するため、契約に基づき、必要な要求仕様、データ、資料等を委託先に提供する必要がある。
(3)	委託業務の進捗状況を把握し、遅延対策を講じること。	全般	受託業務を受託計画どおりに遂行する	3-(4)-①-ト	S	受託業務を受託計画どおりに遂行するため、受託業務における進捗状況を把握し、リスク対策を講ずる必要
(4)	委託先における誤謬防止、不正防止、機密保護等の対策の実施状況を把握し、必要な措置を講じること。	全般	委託契約どおりに誤謬防止、不正利用、漏えい、プライバシーの侵害等を防止する	3-(4)-①-ホ	C	委託契約どおりに誤謬防止、不正利用、漏えい、プライバシーの侵害等を防止する対策を実現するため、誤びゅう防止、不正防止、機密保護等の対策の実施状況を把握し、適切な対策を講ずる必要がある。
(5)	成果物の検収は、委託契約に基づいて行うこと。	全般	委託の目的の達成を確認する	3-(4)-①-チ	S	委託の目的の達成を確認するため、委託契約に基づいて成果物の検収を行う必要がある。
(6)	業務終了後、委託業務で提供したデータ、資料等の回収及び廃棄の確認を行うこと。	全般	業務終了後、不正競争防止、機密保持する		S	業務終了後、不正競争防止、機密保持の観点から委託業務で提供したデータ、資料等の回収及び廃棄の確認を行う必要がある。

項番	システム管理基準の管理項目	統制種別	統制目標（例）	ガイダンス項番	C/S種別	システム管理基準の趣旨
(7)	委託した業務の結果を分析及び評価すること。	全般	今後の委託計画及び委託先選定に反映する		S	今後の委託計画及び委託先選定に反映するため、委託した業務の結果を分析及び評価する必要がある。
5.5	受託業務	全社				
(1)	受託業務の実施内容は、契約内容を遵守すること。	全社	受託業務の内容を過不足なく実施する		C	受託業務の内容を過不足なく実施するため、受託業務の実施内容は、契約書に記載された内容と一致させる必要がある。
(2)	受託内容の進捗状況を把握し、リスク対策を講じること。	全社	受託業務を受託計画どおりに遂行する		S	受託業務を受託計画どおりに遂行するため、受託業務における進捗状況を把握し、リスク対策を講ずる必要
(3)	成果物の品質管理を行うこと。	全社	受託契約に基づく成果物の品質管理をする		S	受託契約に基づく成果物の検収基準に成果物が到達するように、受託側で品質管理を行う必要がある。
(4)	契約に基づき、受託業務終了後、提供されたデータ、資料、機材等を返却又は廃棄すること。	全社	業務終了後、不正競争防止、機密保持する		S	業務終了後、不正防止、機密保持の観点から受託業務で提供されたデータ、資料等の回収及び廃棄の確認を行う必要がある。
6.	変更管理					
6.1	管理	全般				
(1)	変更管理ルールを定め、ユーザ、開発及び保守の責任者が承認すること。	全般	変更を円滑かつ効果的に行う	3-(1)-③-イ	C	変更管理ルール及び変更手順書は、変更を円滑かつ効果的に行うために必要なものであり、ユーザ、開発、保守の責任者が、承認を行う必要がある。大規模な変更は管理基準での開発業務の管理となる。
(2)	仕様変更、問題点、ペンディング事項等の変更管理案件が生じた場合、他システムの影響を考慮して決定すること。	全般	稼働中の情報システムの円滑な運用を妨げない		S	仕様変更、問題点、ペンディング事項等の変更管理案件は、情報システムの円滑な運用を妨げないように、変更の対象となるシステムだけではなく、他のシステムへの影響も考慮して対処方法を決定する必要がある。
(3)	変更管理案件は、提案から完了までの状況を管理し、未完了案件は定期的に分析すること。	全般	組織体の業務上、必要な変更を適時に実施する	3-(1)-③-ホ	S	変更管理案件は、組織体の業務上、必要な変更が適時に実施されるように、提案から完了までの進捗状況を管理し、未完了案件は定期的に分析する必要がある。

項番	システム管理基準の管理項目	統制種別	統制目標（例）	ガイダンス項番	C/S種別	システム管理基準の趣旨
6.2	実施	全般				
(1)	変更管理案件は、変更管理ルールに従って実施すること。	全般	変更管理を円滑にかつ安全に実施する		S	変更管理案件は、変更管理を円滑にかつ安全に実施するために変更管理ルールに従って実行する必要があ
(2)	変更管理案件を実施した場合に、関連する情報システムの環境も同時に変更すること。	全般	変更によるシステムトラブル等を避け、変更を効率よく実施する	3-(1)-③-ロ	S	変更管理案件を実施する際には、変更によるシステムトラブル等を避け、変更を効率よく実施するため、関連する情報システムの環境も同時に変更する必要がある。
(3)	変更の結果は、ユーザ、開発、運用及び保守の責任者が承認すること。	全般	変更依頼どおりに実施されたことを確認する	3-(1)-③-ニ	S	変更の結果が、変更依頼どおりに実施されたことを確認し、ユーザ、開発、運用及び保守の責任者が承認する必要がある。
7.	災害対策					
7.1	リスク分析					
(1)	地震等のリスク及び情報システムに与える影響範囲を明確にすること。	－	災害時及びテロによる破壊行為発生時の情報システムの対応策を具体化する			災害時及びテロによる破壊行為発生時の情報システムの対応策を具体化するため、地震、洪水、テロ等のリスク及び情報システムに与える影響範囲を明確にする必要がある。
(2)	情報システムの停止等により組織体が被る損失を分析すること。	－	被災の程度に応じた業務の復旧の重要性及び緊急性を明確にする			被災の程度に応じた業務の復旧の重要性及び緊急性を明確にするため、情報システムの停止等によって組織体が被る損失を分析する必要があ
(3)	業務の回復許容時間及び回復優先順位を定めること。	－	被災による業務の停止及び影響を最小限にとどめ、効率的に復旧する			被災による業務の停止及び影響を最小限にとどめ、効率的に復旧するため、業務の回復許容時間及び回復優先順位を定める必要がある。
7.2	災害時対応計画	全社				
(1)	リスク分析の結果に基づき、事業継続計画と整合をとった災害時対応計画を策定すること。	全般	災害時に混乱することなく、適切な措置を迅速に確実に実行する			災害時に混乱することなく、適切な措置を迅速に確実に実行するため、事業継続計画と整合した災害時対応計画を策定する必要がある。

項番	システム管理基準の管理項目	統制種別	統制目標（例）	ガイダンス項番	C/S種別	システム管理基準の趣旨
(2)	災害時対応計画は、組織体の長が承認すること。	全般	災害発生時に混乱することなく、適切な措置を迅速に確実に実行する			災害発生時に混乱することなく、適切な措置が迅速に確実に実行されるため、災害時対応計画は、組織体の長が承認し、関係者に周知徹底する必
(3)	災害時対応計画の実現可能性を確認すること。	全般	被災の程度に応じて業務の継続性を確保し、確実に復旧する			被災の程度に応じて業務の継続性を確保し、確実に復旧するため、災害時対応計画の実現可能性を確認する必要がある。
(4)	災害時対応計画は、従業員の教育訓練の方針を明確にすること。	全般	災害時対応計画に定めた具体策に習熟し、確実に実行する			災害時対応計画に定めた具体策に習熟し、確実に実行するため、従業員の教育訓練の方針を明確にし、災害時対応計画に基づいた教育訓練を定期的に行う必要がある。
(5)	災害時対応計画は、関係各部に周知徹底すること。	全般	災害時対応計画に定めた具体策に習熟し、確実に実行する			災害時対応計画に定めた具体策に習熟し、確実に実行するため、災害時対応計画に基づいて、教育訓練を実施し、関係各部に周知徹底する必
(6)	災害時対応計画は、必要に応じて見直すこと。	全般	災害時対応計画は、経営環境及び業務の変化等に対応して、実現可能性を保持する			災害時対応計画は、経営環境及び業務の変化等に対応して、実現可能性を保持するため、適時に見直しを行う必要がある。
7.3	バックアップ	全般				
(1)	情報システム、データ及び関連設備のバックアップ方法並びに手順は、業務の回復目標に対応して定めること。	全般	情報システムを復旧作業の効率及び経済性を考慮して、確実に回復させる		C	復旧作業の効率及び経済性を考慮して、確実に回復させるため、業務の回復目標に対応して、バックアップ方法及び手順を定める必要がある。
(2)	運用の責任者は、バックアップ方法及び手順を検証すること。	全般	情報システムを確実に回復させる	3-(2)-③-ニ	S	定められたバックアップ方法及び手順の実現可能性を確認するため、運用の責任者は、バックアップ方法及び手順を検証する必要がある。
7.4	代替処理・復旧	全般				
(1)	ユーザ及び運用の責任者は、復旧までの代替処理手続き及び体制を定め、検証すること。	全般	停止した情報システムを復旧するまでの間、他の方法で業務を継続する			停止した情報システムを復旧するまでの間、業務を継続するため、代替処理手続き及び体制を定める必要がある。また、その実現可能性を確認するため、ユーザ及び運用の責任者が検証する必要がある。

項番	システム管理基準の管理項目	統制種別	統制目標（例）	ガイダンス項番	C/S種別	システム管理基準の趣旨
(2)	ユーザ及び運用の責任者は、復旧手続き及び体制を定め、検証すること。	全般	停止した情報システムを円滑かつ確実に復旧する	3-(2)-③-ホ	C	停止した情報システムを円滑かつ確実に復旧するため、復旧までの手続き及び体制を定める必要がある。また、その実現可能性を確認するため、ユーザ及び運用の責任者が検証する必要がある。

付録３．ＩＴコントロールとＩＴの具体的な技術の例示

１　入力段階における誤り防止・摘示機能

（１）入力誤り防止のための入力画面の機能

よく使われる機能の例を挙げると、次のとおりである。

① コード入力に代えて、プルダウンによる選択形式とする。

② 入力された得意先・取引先に関連する品番をプルダウン表示する等、入力時の選択範囲を狭める。

③ その入力担当者が、前回入力した項目や入力頻度の高い項目を表示する。

④ 入力担当者ごとに、担当範囲にしたがい入力できるコードの範囲を制限する。

⑤ エラーデータではないが、その入力担当者がこれまでに入力したことのないコードや異常な数値については、警告（ワーニング）の画面表示を行う。

（２）入力段階におけるプログラムによる誤り防止・摘示機能

入力段階において、入力画面又は入力データ（外部の取引先等から受信するデータを含む）の受入処理に際して、プログラムによってデータの検証を行うが、その際によく使われる機能の例を挙げると、付録図表３－１のとおりである。

付録図表３－１　入力段階におけるプログラムによる誤り防止・摘示機能

項　目	説　明
データ処理の網羅性のチェック	処理件数、コントロールトータル、ハッシュトータル、連番チェック等により、データの喪失、処理洩れの発見を行う。 (注)コントロールトータル:処理のステップの前後で計算した金額合計、ハッシュトータル、レコード件数等を比較することで、その処理のステップにおける漏れや重複がないかどうかをチェックすること。 ハッシュトータル:通常合計することに意味がない数値の合計によるデータの網羅性チェックのこと。例えば、入力原票上の品番（数値項目の場合）の合計を手作業で算出しておき、入力時に表示される品番の合計と比較する。
算術計算によるチェックの利用	限界値チェック、クロスフッティング、バランスチェック等により誤ったデータの混入を防止する。 (注)限界値チェック:あらかじめ定めたデータの値の範囲を外れていないかどうかを確かめること。 クロスフッティング：縦横合計の整合性チェックのことであり、例えば、給与計算において、支給総額、各控除項目、手取額についてそれぞれの合計を算出し、支給総額合計－各控除項目合計＝手取額合計となるかを確かめることがこれにあたる。 バランスチェック：会計処理における仕訳の借方合計と貸方合計が一致するかどうかを確かめること。
チェック・ディジットの利用	コードの記入誤りを発見・防止するために、コード中にチェック用の数値を組み込み、プログラムによってチェックする。 (注)チェック・ディジット：コード入力時の誤りを防止するため、例えば６

	桁のコードのうち先頭から５桁までの値を決め、この５桁の値から計算した値を６桁目に設定して６桁のコードとすること。
データ形式のチェック	ブランクテスト、数値項目か文字項目かのチェック、符号テスト等により、入力データの作成ミス、異なる種類のデータの混入を防止する。 (注)ブランクテスト:空白であるべき項目にデータが入っていないかのテスト。 符号テスト：数値データについて、正負があらかじめ特定されている場合に、正負が誤っていないかのテスト。
論理的合理性のチェック	入力データの項目間の関連チェック等により、論理的合理性のあるデータのみを受け入れる。
あらかじめ定めた管理値とのチェック	入力データとあらかじめ登録した信用限度額、支払限度額、数量限度、単価限度等とのチェックを行い、限度を上回る（又は下回る）データは受け入れない。
関連ファイルとのチェック	仕入データと発注ファイルとの照合、出荷指示データと受注ファイルとの照合等、相互に関連するデータ間のチェックを行う。

２　データ処理プロセスにおける誤り防止・摘示機能

データ処理プロセスでは、大量のデータを取り扱って集計・加工するため、処理結果の誤りに長期間気づかないこともある。

そこで、このプロセスにおいて、情報処理の正確性、網羅性、維持継続性を維持するための工夫が必要であり、誤りを防止するための機能又は誤りを摘示する機能の例を挙げると付録図表３－２のとおりである。

付録図表３－２　データ処理プロセスにおける誤り防止・摘示機能

項　目	説　明
更新時のエラー表示とフォローアップ	トランザクションデータ等でファイルを更新する際に、システム設計で指定された条件により更新ができなかったり、矛盾が生じた場合にエラーメッセージの表示により警告する機能であり、プログラム設計上の基本である。エラーメッセージの表示を見て、データ及び関連するプログラムの内容を調査して、原因を探すことになる。
更新結果の整合性の自動照合	以下のようなファイル間のデータ件数、数量、金額等の合計の整合性を自動的に照合してエラーの有無を検出することにより、更新結果の正確性・網羅性を確保する方法である。 ①　更新の元データの明細ファイル ②　元データにより更新されるファイルの更新内容 ③　更新の元データの集計ファイル
データベースの統合による情報源泉の一元化	基本となるトランザクションデータや集約データのデータベース（仕訳、勘定残高、生産実績、在庫、入出庫実績等）を一元化し、各種の出力情報をこの一元化したデータベースから出力することで、ファイル間の不整合による誤りを防止する方法である。
出力帳票と集計ファイルとの合計値、残高合計等の一致	出力帳票に出力された合計値、残高合計等を集計ファイルと照合することで、出力帳票作成時の誤りを防止する方法である。
ユーザ部門の管理者等による出力帳票のレビュー	データの内容に精通したユーザ部門の管理者や業務管理担当者・責任者が出力帳票をレビューすることで、誤りや矛盾点を発見する方法である。

３　アプリケーション・システム間のデータの関連性確保機能

財務報告及び財務情報に関連するデータの関連性（相互追跡可能性）を確保するための

機能である。データ間の関連性の確保は、アプリケーション・システム間のデータの自動転送（自動仕訳、自動連携等）に伴って必要性が生じる。相互参照の記録方法の例を挙げると付録図表３－３のとおりである。

付録図表３－３　アプリケーション・システム間のデータの関連性確保機能

項　目	説　明
個別参照方式	個別参照方式とは、アプリケーション・システム間で個別に参照の相手が認識できるようにする方式である。 この場合、一連番号、伝票番号等（同一の番号又は同一の番号に枝番を付加した番号等）の情報を双方のアプリケーション・システムのデータ上に記録することにより関連性を確保する。
合計参照方式	合計参照方式とは、あるアプリケーション・システムの集計結果を他のアプリケーション・システムに転送する場合に、転送元のアプリケーション・システムや集計範囲等の情報を記録することで参照相手を認識できるようにする方式である。 この場合、転送されたアプリケーション・システムのデータ上に集計対象項目（勘定科目、部門等）及び集計期間等を摘要として文字情報として記録したり、転送元のアプリケーション・システムの ID、自動仕訳パターン番号等を記録することにより関連性を確保する。

付録４．評価手続等の記録及び保存

１　IT 統制の記録

IT 統制が適切に整備・運用されていること示すために、また、IT 統制の整備状況及び運用状況を適切に評価したことを示すために、以下の事項を記録することが重要である。以下では、IT について述べているが、経営者評価にあたっては、IT だけではなく内部統制全体について述べることに留意されたい。

①　財務報告に係る IT 統制の整備及び運用の方針及び手続。 ②　IT 全社的統制の評価にあたって、経営者が採用する評価項目ごとの整備及び運用の状況。 ③　重要な勘定科目や開示項目に関連する業務プロセスの概要（各業務プロセスにおけるシステムに関する流れや IT 業務処理統制の概要、使用されているシステムの一覧などを含む)。 ④　各業務プロセスにおいて重要な虚偽表示が発生するリスクとそれを低減する IT 統制の内容（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、表示の妥当性との関係を含む。なお、IT 統制の具体的な技術内容を含む)。 ⑤　上記④に係る IT 統制の整備及び運用の状況。 ⑥　財務報告に係る IT 統制の有効性の評価手続及びその評価結果並びに発見した不備及びその是正措置。 ⑦　評価計画に関する記録。 ⑧　評価範囲の決定に関する記録（評価の範囲に関する決定方法及び根拠等を含む)。 ⑨　実施した IT 統制の評価の手順及び評価結果、是正措置等に係る記録。

⇒（*実施基準公開草案　Ⅱ．３（７)*)。

２　記録の保存

財務報告に係る内部統制について作成した記録の保存の範囲・方法・期間は、証憑例との関係を考慮して、企業において適切に判断されることとなる。これらの記録の保存は、有価証券報告書及びその添付書類の縦覧期間（５年）を勘案して、それと同程度の期間、適切な範囲及び方法（時期媒体、紙又はフィルム等）により保存することが考えられる⇒（実施基準公開草案　Ⅱ．３（６）②)。

電子的な記録は、評価後にシステム上の設定の誤りにより上書き又は削除されてしまう可能性もある。また、意図的な改ざん等を配慮して適切な記録の保存が望まれる。評価結果や関連する証拠書類等の記録を適切に存する。例えば、関連する証拠書類の紙への印刷や、上書きできない媒体への保存などが考えられる。また、改ざん防止のために、電子署名等を利用する方法も考えられる。

経営者評価の結果は、後日監査人による監査が可能となるように適切に記録しておくこと。なお、どのように評価結果を残しておくべきか、評価時に利用した関連する証拠書類はどの範囲まで残しておくべきか、それらをどのように保管しておくか（例えば、電子的記録の場合、印刷して保存するか、CD-ROM 等に保存するか、改ざん防止のための対策をするか）等について、事前に監査人と協議を行っておくこと。

付録５　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 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された場合には、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⇒*（実施基準公開草案　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

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）

がある。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思われる。しかし、四半期の処理、月次処理、週次処理などでは、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５－１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５－１　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５－１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５－１のサンプル件数と許容逸脱件数の組合せについては、統計的方法によるものではない。

IT 全般統制は、財務報告の虚偽記載に直接影響を及ぼすものではないが、IT 業務処理統制が有効に機能していることを保証するので、IT 業務処理統制ごとにアプリケーション・システムを検証することを軽減できる。この場合のサンプル件数は、例えば、付録図表５－１を参考にして選ぶことができる。

（２）　自動化された内部統制の場合

IT 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。したがって、次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⇒*（実施基準Ⅱ．３（３）ｃ）*。

付録図表５－２　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 に係る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	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

• 障害・エラー等の不具合が発生していない	継続して利用する。

付録６．　リスクコントロールマトリックスの例

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ックスの例を示す。

１　リスクコントロールマトリックスの項目

企業がリスクコントロールマトリッ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、システム管理基準の統制目標を用いて、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、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にカスタマイズして利用することに留意する。

- リスク：財務報告の虚偽リスクの具体的な内容で、自社がとくに注目するものなどをあげる
- 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する
- 統制の状況（統制活動）：企業の該当する統制の実施状況を概観する
- 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・手動の種別：統制目標が IT で実施されるか、人手との組合せかの種別
- 評価項目：IT 業務処理統制では、アサーションとなり、網羅性、実在性、期間配分、権利と義務の帰属、評価、表示などとなる。IT 全般統制と IT 全社的統制ではアサーションにあたるものはない
- 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示す
- 評価ならびに検出事項：評価の結果を記入し、とくに、問題があった場合は、その内容を記す
- 調書番号：統制評価の記録などの文書や帳票類（電子媒体もある）
- 評価結果：対象としたリスクが低減されているかを示す。リスクが「高」の場合は、統制項目の見直が必要となる

２　リスクコントロールマトリックスの利用方法

リスクコントロールマトリックスの利用方法は次のようになる。

①　リスクを記入する

②　実施している（構築を予定している）統制項目を記入して、関連する項目について、リスクコントロールマトリックスに記入していく

③　統制の状況を把握し、どのようなアサーションと関係するのかを概観する。統制評価の場合には、統制評価手続きを記入して統制の評価を実施する

④　想定したリスクに対して、選択した統制項目がリスクを低減しているかを評価する。構築の場合には、候補となる統制項目をリストアップして、リスクの低減が図れる最適な統制項目を選択する

⑤　統制評価のときには、該当するリスクが低減しているかを評価する

⑥　その結果を評価ならびに検出事項に記入し、低減されたリスクを右端の評価結果に記入する

付録6-1

ＩＴ全社的統制評価記述書

会社名	
決算期	

作成者・作成日	
質問への回答者の役職及び氏名	

基本的要素	リスク	統制目標	No.	統制の状況	整備運用	統制評価手続 （文書化、教育・周知、体制、実施、監視・改善の観点から評価する）	評価並びに検出事項 （検出事項がある場合、その影響）	調書番号	リスク評価結果
統制環境	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・計画を定めること。		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	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。	なし	記載省略	低
	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こと。		ITに関する具体的な方針決定と運営のため、情報システム化委員会が設けられている。	整備	「情報システム化委員会規程」を閲覧し、そのメンバーと役割をするか、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。	なし	記載省略	低
				情報システム化委員会が有効に運営されている。	運用	情報システム化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確かめた。	なし	記載省略	低
	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6-2

IT全般統制評価記述書

会社名	
決算期	
事業拠点	
対象システム	販売システム
関連する勘定科目	

作成者・作成日	◇◇◇◇　2007/1/23
質問への回答者（実施部署）	

リスク	統制目標 留意事項	No.	統制の状況	整備運用	予防発見	手作業自動化	整備状況 文書	整備状況 プロセス	整備状況 システム実装	頻度	統制評価手続	評価並びに検出事項 （検出事項がある場合、その影響）	調書番号	評価結果
財務情報の信頼性に係わるソフトウェアが適正に開発、調達されず、処理結果の財務情報に信頼を置くことができない。	開発 ITを開発する際に意図的な不正プログラムが埋め込まれたり、処理に誤りが顕在化する		ITを開発するための標準化された方針および手続があり、これに基づいて、ITが開発され、更改されている。	整備	予防	手作業	○	○	NA	四半期	対象とするITの開発は標準化された手順、文書で実施されていることを確かめた	なし	記載省略	低
	ITの開発プロセスにおいて、意図的な不正や、処理に誤謬の起きる可能性がある		ITの開発プロセスにおいて、財務情報の信頼性に係る正当性、完全性、正確性の統制が確実に実現できるようになっている。	運用	予防	手作業	○	○	NA	四半期	・開発の仕様書、基本設計書（概念設計書）等で財務情報の信頼性確保の統制機能が織り込まれていることを確かめた。	なし	記載省略	低
	以下省略													
保守が適切に実施されないと業務処理統制の信頼が失われる	保守 プログラムが改ざんされたり、承認なく変更される		システムソフトの変更を含むプログラム変更、システムの変更およ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）。	整備・運用	発見	手作業	○	○	NA	月週	変更管理手続の規定があることを確かめた。 変更管理規定どうりに変更管理を実施していることを25件テストした。	25件のうち1件、承認漏れがあったが、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。25件の追加テストの結果、押印漏れはなく、単なる押印漏れのミスであると判断した。	記載省略	低
			以下省略											

付録6-3

IT業務処理統制評価記述書

会社名	○○株式会社
決算期	平成○○年3月
場所	受注センター
取引サイクル	販売サイクル
ファンクション	受注
関連する勘定科目	売上、売掛金

作成者・作成日	◇◇◇◇　2006/12/23
確認者・確認日	□□□□　2007/1/24

リスク	統制目標 / 留意事項		No.	主要な統制活動	自動手動	頻度	経営者の主張 網羅性	実在性	期間配分	権利と義務	評価	表示	整備運用	統制評価手続	評価並びに検出事項（検出事項がある場合、その影響）	調書番号	評価結果
財務情報に漏れや重複が発生する	網羅性	全ての受注は漏れなく重複なく記録されているか	1	EDIによる受注はJCA手順によって制御され異常な伝送があればシステム担当者にメールが送信される	自動	四半期	○	NA	○	NA	NA	NA	整備・運用	特定の月を選び、システム運用報告をレビューしJCA手順による異常終了が担当者に報告され、フォローされていりことを確かめる	なし	記載省略	低
			2	FAX受注はコールセンターで受信後に連番を記入し、一人が入力した後で、プルーフリストを出力し、他の一人が内容をFAXと照合する	自動・手動	日	○	NA	NA	NA	NA	NA	運用	特定の月の25件を選び、プルーフリストが照合されていることを確かめる	なし	記載省略	低
			3	在庫引当された受注のみが出荷指図ファイルに登録される。未引当の受注残は、受注残ファイルに記録され営業担当者がフォローして消しこんでいる。	自動	日	○	○	NA	NA	×	NA	整備・運用	受注残ファイルが営業担当者により、消しこまれていることを確かめる	なし	記載省略	低
財務情報が正確に記録されない	正確性	受注の登録に誤りがないか	4	EDIで受信した受注データは得意先マスタ、商品マスタと存在性のチェックをし、エラーについてはエラーファイルが作成され、エラーデータについては、得意先に返送し、再送を依頼する。エラーファイルは訂正データが再送されるまで保存される。	自動	日	NA	○	NA	○	○	○	整備・運用	特定の月のエラーファイルの処理状況を25件確かめる。	なし	記載省略	低
			5	FAX受注はコールセンターで受信後に連番を記入し、一人が入力した後で、プルーフリストを出力し、他の一人が内容をFAXと照合する。	自動・手動	月日	NA	○	NA	○	○	○	整備・運用	特定の月の25件を選び、プルーフリストが照合されていることを確かめる	なし	記載省略	低
			6	受注日付は機械日付で登録される	自動	日	NA	○	○	NA	NA	○	整備・運用	売上日付の設定を確かめ、売上データの日付が機械日付であることを確かめる	なし	記載省略	低
			7	得意先コードにより、得意先マスタから得意先名がロードされる	自動	日	NA	○	NA	○	○	○	整備・運用	得意先コードにより得意先名が登録されることを画面で確認する	なし	記載省略	低
			8	単価は得意先ごとにマスタに登録された単価が自動的にロードされる	自動	日	NA	○	NA	NA	○	○	整備・運用	単価が自動的に登録されることを確かめる	なし	記載省略	低
正当でない財務情報が記録される	正当性	正当でない受注が登録される	9	得意先マスタに登録された得意先以外は登録できない	自動	日	NA	○	NA	○	NA	NA	整備・運用	マスタに登録された相手先しか登録できないことを確かめる（設定はマスタ登録で確かめる）	なし	記載省略	低
			10	単価は得意先ごとにマスタに登録された単価が自動的にロードされる	自動	日	×	○	NA	○	○	○	整備・運用	単価は登録単価が登録され、単価入力ができないことを確かめる（単価登録はマスタ登録で確かめる）	なし	記載省略	低
			11	受注入力は、担当者のIDとパスワードで制御されている	自動	日	NA	○	NA	NA	NA	NA	整備・運用	担当者のIDとパスワードでしか受注画面が開かないことを確かめる（注）シングルサインオンの場合はパスワード設定は、全般統制で確かめる。ただし、販売システムへのアクセス権限は、業務の権限と一致して設定されいることは、業務処理統制で確かめる	なし	記載省略	低
			12	得意先の与信限度を超える受注は入力できない	自動	日	NA	○	NA	NA	NA	NA	整備・運用	与信限度を超える入力ができないことを確かめる	なし	記載省略	低
			13	以下省略										以下省略			
財務情報が最新ではなく、継続的に使用できない	継続性	受注ファイルが不当に変更される	14	受注ファイルへの変更は、担当者のIDとパスワードで制御されている	自動	四半期	○	○	○	○	○	○	整備・運用	受注ファイルは担当者しかアクセスできないことを確かめる（DBが統合されている場合は全般統制でアクセス権限を確かめる場合がある）	なし	記載省略	低
			15	受注ファイルへのアクセスログはモニターされている。	自動・手動		NA	○	NA	NA	NA	NA	整備・運用	マスタへのアクセスログが一定の条件でモニタされていることを確かめる（アクセスログのモニターは全般統制で実施することもあるが、業務処理統制で実施する方が監視する範囲が絞り込まれる場合がある）	なし	記載省略	低
			16	在庫マスターは、流通センターのマザーマスターと毎晩、夜間バッチで置き換えられ、不一致が無いように管理されている	自動	日	○	○	NA	NA	NA	NA	整備・運用	在庫マスタが置き換えられていることを確かめる（バッチ処理が正常に実施されていることは全般統制で確かめる場合もある）	なし	記載省略	低