

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偽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 年 月 日
日本公認会計士協会

- 目 次 -

	頁
本報告書の目的	1
リスク評価手続及び企業とその環境(内部統制を含む。)についての情報源	1
1. ITの概括的理解	1
企業とその環境(内部統制を含む。)の理解	2
1. 情報の信頼性	2
2. 経営者の主張(アサーション)とITのコントロール目標の関係	3
3. 各ビジネスプロセスとITとの関係の理解	5
4. 財務諸表の勘定科目、取引とアプリケーション・システムの関係の理解	5
5. 統制環境の理解	7
6. 財務報告目的の情報システム(関連する業務プロセスを含む)と伝達の理解	8
7. 統制活動の理解	8
8. 監視活動の理解	12
重要な虚偽表示リスクの評価	12
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	12
2. 全般統制に不備があった場合の留意点	12
3. 業務処理統制に不備があった場合の留意点	13
4. リスク評価の修正	13
経営者及び監査役等とのコミュニケーション	13
評価したリスクに対応する手続の実施	13
1. 記録や文書の査閲	14
2. 観察/システム運用現場視察	14
3. 質問/ヒアリング	14
4. 再計算/CAAT	15
5. 再実施/CAAT	15
6. 分析的手続	15
監査調書	15
ITの専門家の利用	15
アウトソーシングの位置づけ	16
発効及び適用	16
【表1】ITのコントロール目標と監査要点との関係の例示(販売取引サイクルの一部)	17

本報告書の目的

1. 企業が利用しているITは、監査人が実施するリスク評価に大きな影響を与えている。したがって、監査人には、企業が構築したビジネスプロセスとITに関する知識、及びそれに対応できる技術的な能力が求められる。また、監査人がITの専門家の業務を利用する場合においても、監査人は、ITの専門家としての能力と、その業務の客観性を評価し、その業務の結果が監査証拠として十分かつ適切であることを確かめる必要がある。このため、監査人には、ITの専門家が実施した業務の内容と指摘事項を理解するに足る能力が求められる。本報告書は、監査基準委員会報告書第27号「監査計画」、同第28号「監査リスク」、同第29号「企業とその環境の理解及び重要な虚偽表示リスクの評価」、同第30号「評価したリスクに対応する監査人の手続」及び同第31号「監査証拠」と一体で理解する必要がある。

リスク評価手続及び企業とその環境（内部統制を含む。）についての情報源

1. ITの概括的理解
2. 企業が利用している「ITを利用した情報システム（以下、本報告書では特に断りのない限り「情報システム」と言う）」の特質及びITの利用状況により、ITが内部統制に与える影響は異なる。したがって監査人は、監査計画を立案するに際して、下記の事項に留意し、まず企業のIT利用に関する環境を理解し、重要な虚偽表示リスクの評価の対象とするITを把握することとなる。IT利用に関する環境の理解は、実際にITに依存した重要な虚偽表示リスク評価を行うか否かに係わらず、内部統制の理解の一貫として実施しなければならない手続である。
 - (1) ITインフラの概要
監査人は、企業によるITの利用状況を理解するために、例えば次のITインフラの概要を理解する。（図1参照）
 - ・ハードウェア構成
 - ・基本ソフトウェア構成
 - ・ネットワーク構成
 - (2) アプリケーション・システムの構成
監査人は、取引の発生から財務諸表の作成に至るまでの会計処理過程のうち、ITが利用されている部分を識別するために、アプリケーション・システムの構成を理解する。これは、企業が利用するITを理解する際の基礎となるものであるため、監査人は、企業の業務活動の内容や流れ、ITが利用されている部分と利用されていない部分の範囲や相互の接点などに留意する。
 - (3) 電子商取引の利用
監査人は、企業がそのビジネスモデルに、どのようにITを利用しているか理解する。例えば、企業が電子商取引を行っている場合、従来の商習慣では判断しにくい法律問題や会計処理の問題が発生する可能性があることに留意する。
 - (4) 情報システムに対する投資
監査人は、企業が行っている情報システム投資を理解する。情報システムに対する投資には、ITインフラないしアプリケーション・システムへの直接的な投資のみならず、IT担当人員・組織構成といった人的投資も含まれており、この両者について把握することが、企業の内部統制を理解する上で有用である。また、企業が必要な情報システム投資を適時に行わない場合には、情報システムの陳腐化を招く恐れがある。

(5) 情報システムの変更

監査人は、企業が情報システムの変更を行っている場合には、内部統制（主に業務処理統制）のデザインが変更されている可能性があることに留意する必要がある。この場合、過去に行った内部統制のデザイン等の評価をそのまま利用することができないため、変更の有無及び変更の内容につき理解する。

(6) 情報システムの安定度

監査人は、企業の情報システムに重大な障害が発生している場合あるいは障害が多発している場合には、内部統制がデザイン通りに機能していない可能性があると考えられるため、過去における障害発生の有無及び障害の程度を理解する。

(7) アウトソーシングの利用状況

監査人は、企業がアウトソーシングを利用している場合には、その企業の統制環境が委託先に必ずしも及ばない可能性があるため、アウトソーシングの利用状況を理解する。

(8) アライアンスの状況

資本関係の無い企業間でアライアンスによりシステムを連携する場合には、その相手企業のシステムの信頼度が、企業の事業に影響を与える可能性があるため、企業間のシステムの連携の程度を理解する。

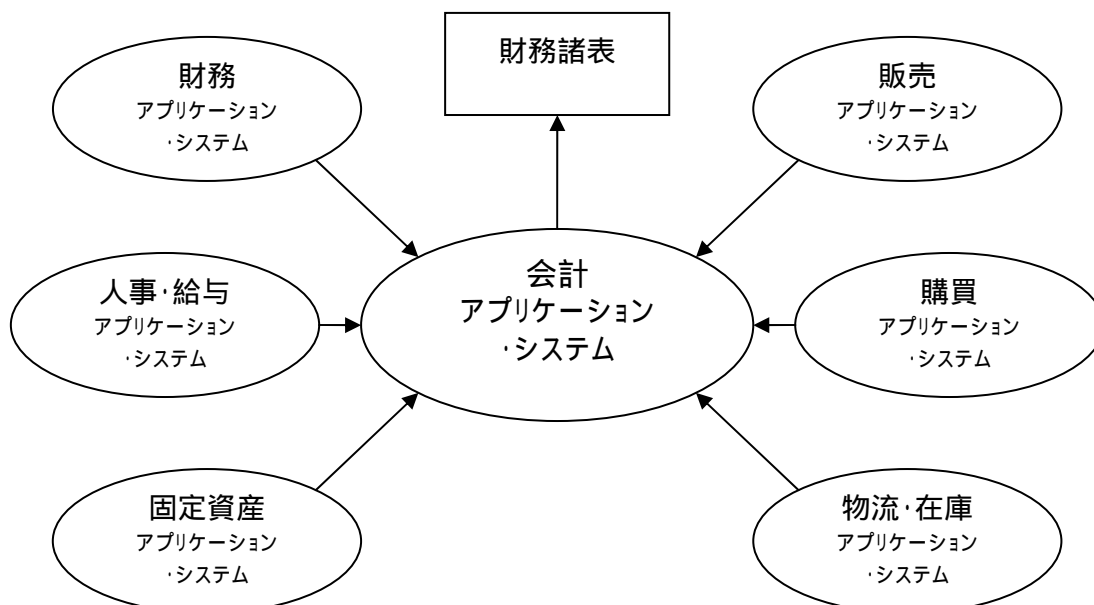
3. 企業における IT の利用度が低くかつ安定度が高く、情報システムに前年度との間で重要な変更がない場合には、監査人は、前項に掲げるような IT の利用状況の理解を行った後、下記の手続を実施する際にその一部を省略することが可能である。しかしながら、IT の利用度が低い場合であっても、情報システムにおいて、前年度監査で内部統制上重要な不備が発見されている、あるいは当年度において重要な変更が行われているような場合には、以下の手続の実施を省略する合理的理由はない。

企業とその環境（内部統制を含む。）の理解

1. 情報の信頼性

4. 企業の財務諸表は、アプリケーション・システムから出力される情報によって作成されるが、情報システムに IT が利用されている場合は、通常、情報は種々の業務アプリケーション・システムで作成され、その情報が会計アプリケーション・システムに反映される。このため、監査人は、これらのアプリケーション・システムによって作成される財務情報の信頼性を確保することに関連する内部統制を評価する必要がある。また、経営者が財務情報以外の情報を利用しており、それを監査上利用する場合には、監査人は財務情報以外の情報の信頼性の確保についても留意する必要がある。次の【図1】は、財務諸表、会計アプリケーション・システム及び業務アプリケーション・システムの関係を示したものである。情報の信頼性は、情報システムが有効に機能しているか否かに大きく依存している。情報システムが有効に機能しているということは、企業の経営資源（人、物、金）の状態が、その企業のビジネスプロセスにおいて、適時かつ正確に情報として反映されていることをいう。

【図1】財務諸表、会計アプリケーション・システム及び業務アプリケーション・システムの関係（例示）



2. 経営者の主張（アサーション）とITのコントロール目標の関係

5. 情報システムの内部統制は経営者が構築するものであるが、その情報システムを有効なものとするために経営者が設定する目標が、ITのコントロール目標である。監査人は、財務諸表監査において、このITのコントロール目標のうち企業の情報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となるものを、情報システムに関する重要な虚偽表示リスクの評価のために利用する。監査人は、財務報告目的に関する内部統制を特定の経営者の主張と関連付けて理解し、評価する。したがって、監査人は、ITのコントロール目標の達成度（ITを利用した統制活動の有効性）に係る評価結果を、直接的あるいは間接的に経営者の主張と関連付けて理解することになる（付録【表1】参照）。なお、経営者の主張とその経営者の主張に関連するITのコントロール目標は、企業の業種、組織、ITの状況などに対応して、監査人が自らの判断で選定する。

6. 監査人が情報システムに関する重要な虚偽表示リスクの評価のために利用できるITのコントロール目標として、例えば、次のものが挙げられる。なお、これらの目標には、経営者の主張と直接的に関係するものと、間接的に関係するものがあることに留意する。

- 準拠性: 会計原則、会計基準、関連する法律及び社内規則等に合致していること
- 網羅性: 情報が漏れなくかつ重複なく記録されていること
- 可用性: 情報が必要とされるときに利用可能であること
- 機密性: 情報が正当な権限者以外に利用されないように保護されていること
- 正確性: 情報が正確に記録され、提供されていること
- 維持継続性: 必要な情報の継続使用が可能なこと
- 正当性: 情報が正規の承認手続を経たものであること
- 整合性: ファイル間などで情報の内容に矛盾がないこと

7. 監査計画の策定において、監査人が情報システムに関する重要な虚偽表示リスクの評価を行うためには、ITのコントロール目標と経営者の主張との関係を理解することが重要となる。例えば、監査人が販売取引に関する経営者の主張について重要な虚偽表示リスクの評価を行う場合は、販売取引が適正に総勘定元帳に

記録されていることを確かめることになる。この場合、情報システムに関する重要な虚偽表示リスクの評価としては、業務処理統制、全般統制に分け、例えば次の事項を確かめる。

業務処理統制

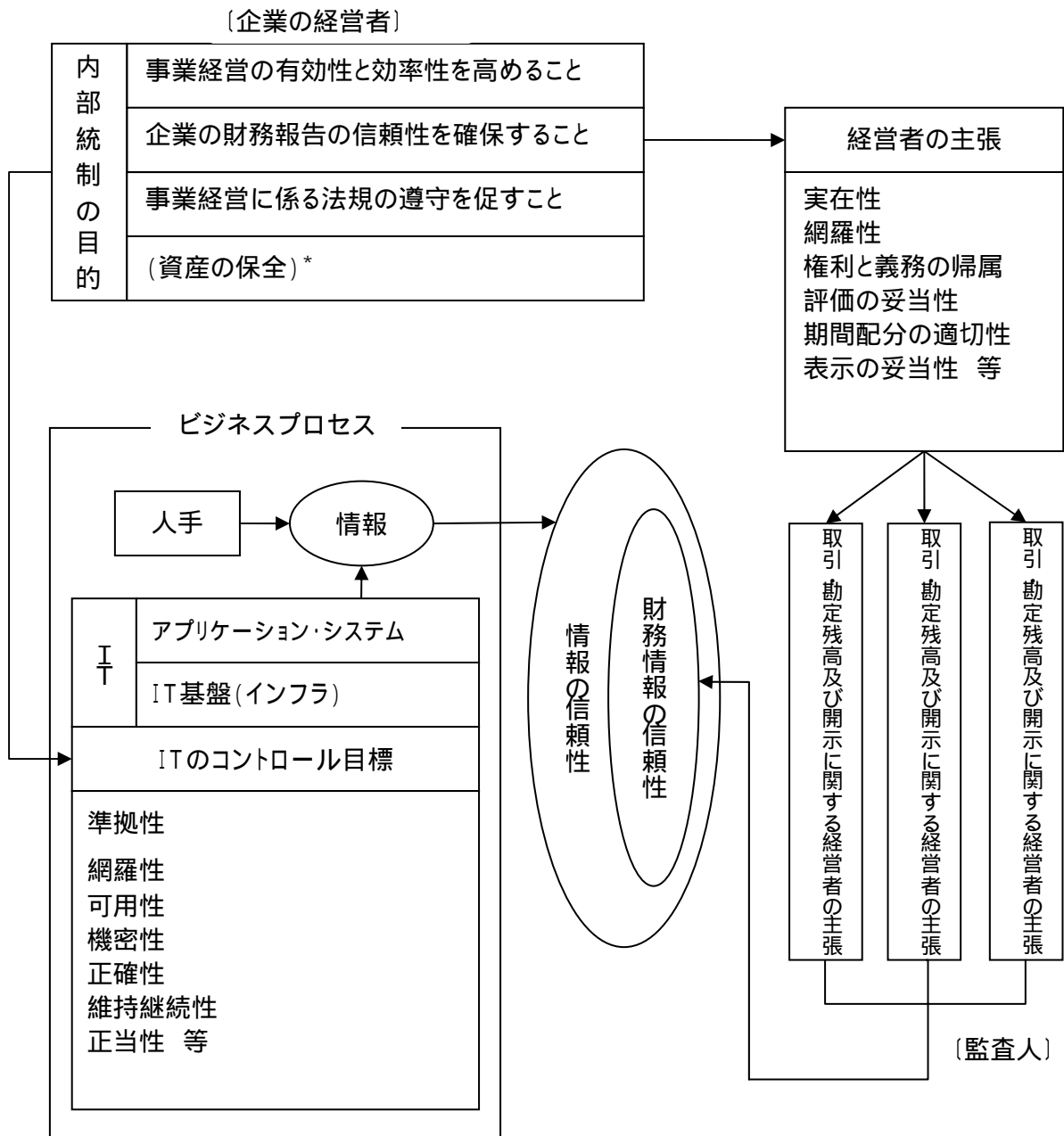
- ・販売管理システムから会計システムへの売上データの転送処理が、漏れなく重複なく処理されたことを確かめることができる統制活動があること（網羅性）
- ・売上取引を入力する際に、得意先や価格をマスタ・ファイルと照合する統制活動があらかじめプログラムされていること（正確性）（付録【表2】参照）

全般統制

- ・プログラム変更管理体制があること（正当性、正確性）
- ・アプリケーション・システムの運用監視体制があること（可用性・維持継続性）

監査人は、上記のような内部統制によって確保される、ITのコントロール目標の達成度を経営者の主張と関連付けることにより、情報システムに関する重要な虚偽表示リスクの評価を行う。情報システムが、企業のビジネスプロセスで要求される有効性及び効率性の水準を満たしているか否かは、監査人にとって直接的に確認する対象ではない。しかし、情報システムが要求水準を満たさない場合は、情報が適切に利用されず、不正や誤謬が発生する可能性がある。このため監査人は、企業のITの実際の利用状況についても理解する。上述したITのコントロール目標と経営者の主張との関係を図示すると、次の【図2】のとおりとなる。

【図2】 ITのコントロール目標と経営者の主張との関係



3. 各ビジネスプロセスとITとの関係の理解

8. 監査人は、重要な虚偽表示リスクの評価を、監査基準委員会報告書第29号に示された手順に従って実施する。情報システムに関して監査人は、まず企業の主要な取引を理解するとともに、取引と財務諸表、及び各ビジネスプロセスとITとの関係を理解する。企業がITを利用して財務情報を処理している場合には、監査人は、情報システムに関する重要な虚偽表示リスクの評価を行う。その際に監査人は、評価の対象として、どの情報システムを選択するかを適切に判断する必要がある。

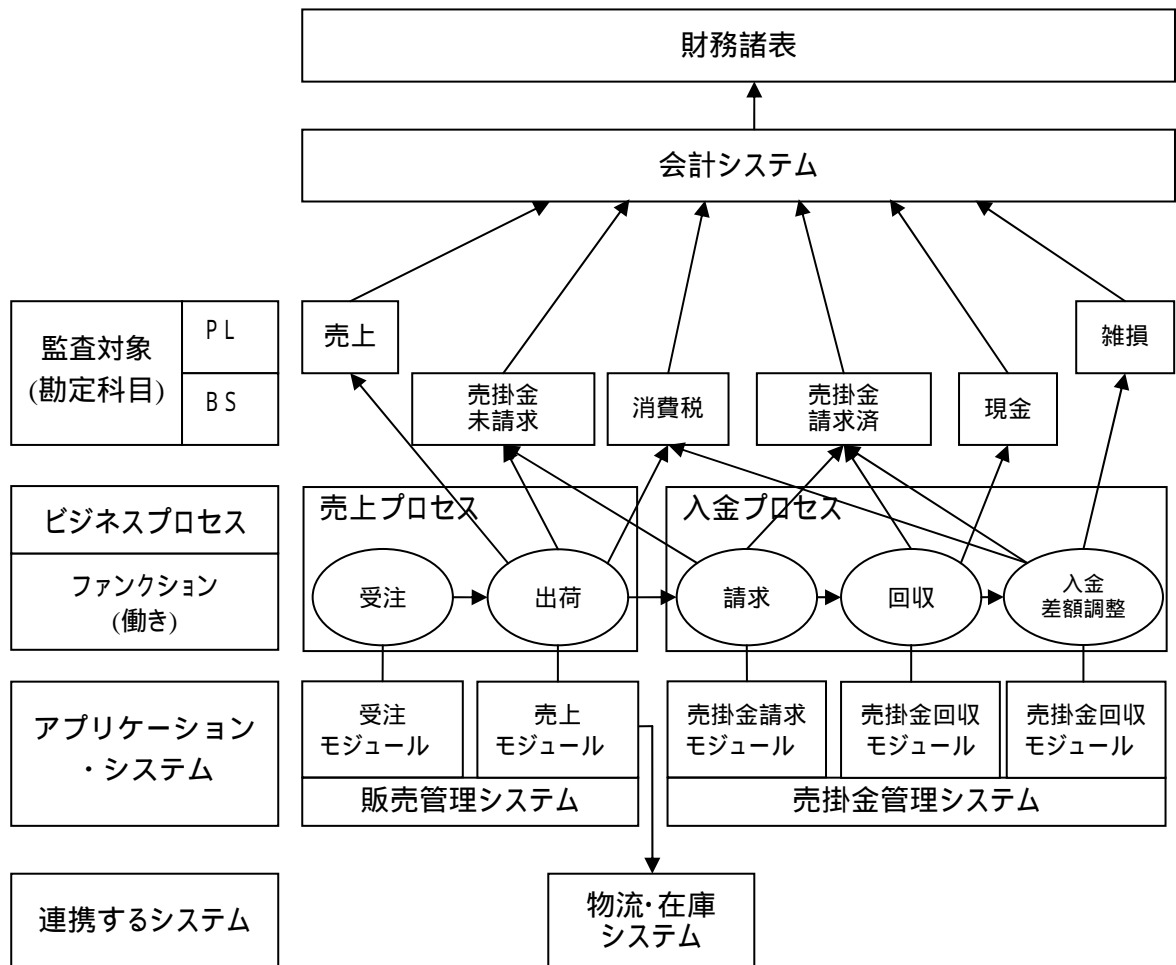
4. 財務諸表の勘定科目、取引とアプリケーション・システムの関係の理解

9. 監査人は、財務諸表の重要な勘定科目が、どのような取引、企業のビジネスプロセス及びアプリケーション・システムと関連しているかについて理解する。【図3】は、販売取引における売上と入金ビジネスプロセス、ファンクション(働

き)及び会計データとの関連を、一つの例として図式化したものである。企業の各ビジネスプロセスはファンクション(働き)ごとに細分化され、そのファンクション(働き)に基づいてシステム化される場合が多い。例えば、販売取引の売上プロセスは、受注や出荷等のファンクション(働き)に分類され、必要に応じてシステム化される。監査人は、財務諸表の勘定科目と取引、ビジネスプロセス及びアプリケーション・システムとの関係を理解するに当たって、必ずしもこのような図を作成する必要はないが、主要な取引等について、どの会計データがどのアプリケーション・システムに依存しているのかを理解する。また、監査人は、そのアプリケーション・システムが手作業によるものかITを利用しているのかを識別し、重要な勘定科目に関する財務情報の信頼性を確保することに関連する内部統制を理解する。

10. 監査人は、理解した関係が実際に存在することを確認するため、ウォークスルーを実施する。例えば、【図3】のケースで実施するウォークスルーとしては、販売管理システムの出荷データと売掛金管理システムの請求データとを照合することがあげられる。

【図3】販売取引におけるビジネスプロセス、ファンクション(働き)及び会計データとの関連(例示:売上と入金)



5. 統制環境の理解

11. 監査人は、情報システムに関するITの概括的理解に加えて、次の統制環境を十分に理解し、監査計画を策定する。

(1) 経営者の関心、考え方及び理念

経営者の関心、考え方及び理念は、企業の構成員の内部統制に対する意識に影響を与える。情報システムに対する投資、情報システムの信頼性及びセキュリティに関する経営者の意識や認識もこれに含まれる。経営者の意識は、後述する全般統制の基本的なものの一つである。

(2) 知的資産

情報システムは、手作業を単に機械に置き換える情報システムから、知的資産（無形資産）としての情報の信頼性を支える情報システムに変化しつつあり、経営者は自ら、知的資産の管理責任者として管理すべき情報を明確にし、その資産を保全するためのセキュリティを確保するとともにその方針をセキュリティポリシーとして社内に周知する必要がある。したがって、監査人は、経営者が情報を管理すべき知的資産として認識しているか及びその情報に対するセキュリティの認識とリスク評価の過程に留意する。

(3) 経営者の管理すべき範囲（スコープ）

E D I（電子データ交換）やインターネットを利用した企業間取引など、他社と連携するビジネス形態においては、他社の出力データが自社の入力データとなることや、逆に、自社の出力データが他社の入力データとなることがある。したがって、監査人は、他社の情報システムに関する重要な虚偽表示リスクの程度が、自社のビジネスに影響を及ぼす可能性があり、また、自社の情報システムが、他社に影響する場合もあることを経営者が認識しているかに留意する。また、監査人は、経営者が、その管理すべき範囲を認識しているか、またその範囲の設定が適切であるかに留意する。

(4) ネットワークの利用

インターネットによる電子商取引のようにネットワークを利用する環境においては、企業外部の顧客等が、企業内部の基幹システムで使用するデータを入力することがある。このように、企業の構成員とは異なる価値観や倫理観を持つ人間が、企業の情報システムに重要な影響を与える場合がある。したがって、監査人は、企業の情報システムが、企業外部の様々な人間によって影響を受ける可能性について、経営者が認識しているかに留意する。

(5) 法令等への準拠性

法令等への準拠性については、その全てが財務諸表監査に直接関係するものではない。しかし、法令等への準拠性は、電子商取引のビジネスモデルの特許問題や個人情報の保護、及びソフトウェアの不正使用などに関する訴訟の可能性、また、多国間のインターネット取引に関する課税問題など、企業の財務諸表に影響を与える可能性がある。したがって、監査人は、これらの法律問題に対して、経営者が注意を払っているかに留意する。

(6) ITの発達に伴う社会の基本的なインフラの変化

ITの発達に伴う社会の基本的なインフラの変化は、企業が保有する情報システムを陳腐化させる可能性がある。したがって、監査人は、経営者が必要な情報システム投資を行わないこと、又は必要以上に高いコストを情報システムに払うことなどにより、企業のビジネス自体の継続性に問題が生じたりすることのないように、経営者がITの動向に注意を払っているかに留意する。

(7) 外部委託のサービスレベル

外部委託のサービスレベルは、相手先との契約上の合意によって決まる。した

がって、監査人は、外部委託に関する契約内容について、経営者が注意を払っているかに留意する。

(8) ITに関する教育

監査人は、IT担当者がその企業の情報システムに関して十分な知識や経験等を有しているか、また、新しい情報システムの導入時には、IT担当者のみならずITのユーザ(利用者)に対しても適切な教育を行う必要があることに経営者が注意を払っているか、情報システムの維持・継続に十分な人員を確保しているかに留意する。

6. 財務報告目的の情報システム(関連する業務プロセスを含む)と伝達の理解

12. 企業は、情報の信頼性を確保するために、ITのコントロール目標を具体的に設定する。監査人は、企業の経営者が適切な判断を行うために必要な信頼性の確保された情報を入手できるように情報システムを設計していることを確かめる。例えば、滞留在庫や不良品、滞留売掛金など企業にとって不利な情報が、内部統制責任者に適時に正しく報告されているか否かは、監査人にとって重要な検討事項である。また、ITの発達は、知的資産としての情報の共有を可能にしている。現在、企業は、ITの利用により文書情報の共有が可能であるため、顧客のクレーム情報や各部署の成功事例についても、企業のデータベースとして共有し、有効に活用することができる。このため、企業がこれらの情報を収集する情報システムを有しているか否かは、企業の情報システムと伝達に対する経営者の姿勢を監査人が判断する際の材料になり、また、その情報システムの有無が財務諸表監査に影響を与える場合があることに留意する。

7. 統制活動の理解

(1) 全般統制の理解

13. 全般統制は、主要な取引、勘定残高及び開示並びにそれらに関するほとんどの経営者の主張に関係している。この全般統制は、取引、勘定残高及び開示における情報の信頼性を確保すること、及び業務処理統制の継続的な運用を確実にすることを間接的に支援するものである。監査人が全般統制を理解するに当たっては、その統制活動の対象となっている範囲に留意する。

企業が大型汎用コンピュータを中心とするホスト系システムを利用している場合、全般統制は、主にソフトウェアの開発、変更、運用及び保守というプログラムに関する統制活動を対象としている。一方、業務処理統制は、主にアプリケーション・システムでのデータの処理に関する統制活動を対象としている。このような場合、アプリケーションの共通基盤としての全般統制は、例えば情報システム部といったITに関する専門部署が担当していることが多いため、全般統制を容易に識別することができる。

しかし、企業がクライアント・サーバシステムを利用している場合は、全般統制は情報システム部のみが担当するだけでなく、アプリケーションごとに担当が異なっている可能性がある。この場合、全般統制と業務処理統制との区別が明確にできない恐れがあるため、監査人は、企業の実態を十分検討の上、全般統制の適用範囲を識別することになる。

企業がWebアプリケーションを利用している場合などにおいては、プログラムとデータが一体となってネットワーク上で伝達されているため、監査人は、個々のアプリケーション・システムに対する、開発、変更、運用及び保守といった全般統制だけではなく、ネットワーク全体の運用・管理まで一体とした統制活動としての全般統制を理解する。

また、最近のネットワーク技術の進展に伴い、境界のない接続環境が実現されているため、その企業の支配力が直接及ばない範囲までをも管理の対象として考慮する必要が生じてきている。例えば、EDI（電子データ交換）やインターネットを通じて、企業外部からデータが入力され、出力される環境においては、従来、企業が管理できていたハードウェアやソフトウェアも、他の企業や個人の支配下にあることになるため、監査人は、企業外における全般統制の適用状況について、直接的ないし間接的に把握する必要がある可能性がある。

このように監査人は、企業を取り巻くITの変化を斟酌し、企業内外のネットワーク環境への対応なども加えた情報システムに関する統制活動を対象として全般統制を理解することとなる。

(2) 全般統制の例示と評価上の留意点

14. 全般統制は、情報システムの企画から実際の運用に至る様々な段階に関係しており、その主なものとしては以下の15項から18項のものがあげられる。

15. 情報システムに関する企画・開発・調達業務の統制活動

情報システムに関する企画・開発・調達業務では、監査人は、情報システムの新規開発やパッケージソフトの導入、並びに情報システムの運用・管理のための内部統制が整備されているかについて検討する。企業が、情報システムに適切な内部統制を組み込むためには、企画・開発・調達段階で組み込むべき内部統制の内容を検討する必要がある。企業が情報システムに関する企画・開発・調達の過程を適切に管理していない場合には、完成した情報システムの信頼性が期待できないことがある。このように、情報システムに関する企画・開発・調達は、他の内部統制の整備状況に影響を与える。特に、ユーザ部門の参画による十分なテストの実施・検収や、適切なプログラム等の移行・変更管理は、情報システムの信頼性に影響を与える。

16. 情報システムに関する運用業務の統制活動

監査人は、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内部統制を整備しているかを検討する。この内部統制には、例えば、次の事項が含まれる。

- ・オペレータによる手動又は自動実行ツールによるプログラム等の運用手順
- ・プログラムによる処理結果の確認手続
- ・実行スケジュール管理
- ・エラーが発生した場合の再処理の方法を含めた対応手順
- ・適切なプログラムの使用のためのライブラリ管理

17. セキュリティに関する統制活動

監査人は、企業がデータ、ソフトウェア、ハードウェア及び関連設備等の不正使用、改竄、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内部統制を整備していることを確かめる。この内部統制には、アクセス管理用のソフトウェアを導入し、IDとパスワードの組合せをプログラムでチェックするような論理的なものだけでなく、コンピュータールームへの入室を制限して、ハードウェアの物理的な破壊や盗難を防止するような対策も含まれる。企業は、このセキュリティに関する方針を、情報システムの企画・開発・調達段階においても検討し、文書化することが必要である。

18. 外部委託の統制活動

企業が、情報システムの開発業務や運用業務等を外部に委託している場合には、監査人は、企業が委託業務を管理するための内部統制を整備していることを確かめる。すなわち、監査人は、企業による委託先の選定基準、成果物等の検収体制、委託先の内部統制を理解し、自社の内部統制に与える影響等を評価する。また、企業がその製品の物流・保管を外部の業者に委託している場合のように、企業の基幹業務の一部を委託先が担っている場合には、委託先のシステム障害が、企業の業務の運営に支障をきたす可能性がある。したがって、監査人は、企業と委託先との間で合意されているサービスレベルに留意する。

(3) 業務処理統制の理解

19. 監査人が、企業の財務報告の信頼性を確保することに関連する業務処理統制を理解するに当たっては、情報システム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）
- ・人とITが一体となって機能する統制活動

業務処理統制を理解するために、監査人は、企業の各ビジネスプロセスの内容を理解するとともに、ITのコントロール目標と経営者の主張を関連付けながら、統制活動と監視活動の整備状況を理解する。なお、アプリケーション・システムは、ビジネスプロセスごとに作成されることが多いため、監査人は、各企業の実態に応じてアプリケーション・システムを分析する。

業務処理統制に関するウォークスルーでは、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理解し、検証することに留意する。

(4) 業務処理統制の評価指針の例示

20. アプリケーション・システムは、企業のビジネスプロセスを支え、会計に関連する情報及びデータを提供するITである。その会計データとファンクション（働き）に関する業務処理統制を評価するための指針として、例えば、次のITのコントロール目標が挙げられる。〈付録表1参照〉

会計データの網羅性

- ・会計データが漏れなく、重複なく記録され、残高更新され、未決済及びエラーとなった会計データは、期間内に全て適切に処理されていること

会計データの正確性

- ・会計データは、正確に適時に適切な勘定に記録されていること
- ・エラーとなった会計データは、期間内に全て適切に処理されていること

会計データの正当性

- ・会計データは、当該企業に財務的影響を及ぼす取引その他の事象を表し、かつ当該企業に承認されたものだけが入力され、処理されていること
- ・適切な職務権限に応じて、アクセス権限が設定され、適切な担当者により処理されていること

ファイルの維持継続性

- ・マスタ・ファイルは、常に最新の状態に保たれ、正しく維持及び継続されていること
- ・異なるIT間で利用される分散マスタ・ファイル間の整合性が保たれていること

(5) 業務処理統制の検証手続の例示

21. 購買システムのうち、検収業務の監査上のリスクについて、業務処理統制及びその検証手続を例示すると以下のようになる。

監査上のリスク	ITのコントロール目標	業務処理統制	業務処理統制の検証手続
発注していない物品が検収される	会計データの正当性	検収入力ができるのは、システムに登録された発注取引に対してだけである	<ul style="list-style-type: none"> ・システムに登録されていない発注番号の入力ができないことを確認する ・分納や数量違いの場合の処理ロジックの妥当性を確認する ・完納済みの発注番号は検収入力できないことを確認する
		「検収違算報告書」が出力され、発注データと検収データのチェックができる	<ul style="list-style-type: none"> ・「検収違算報告書」の作成ロジックの妥当性を確認する
検収データが正確に入力されない	会計データの正確性	検収画面にエディット・バリデーション・チェックが組み込まれている	<ul style="list-style-type: none"> ・組み込まれているエディット・バリデーション・チェックの妥当性を確認する
		「入力プルーフ・リスト」が作成される	<ul style="list-style-type: none"> ・「入力プルーフ・リスト」のロジックの妥当性を確認する
購買取引が適切に記録、又は仕訳されない	会計データの正当性/正確性	発注入力、検収入力を行える者が限定されている	<ul style="list-style-type: none"> ・入力可能なデータ項目が、業務担当者の職務権限に対応した範囲に限定されていることを確認する ・パスワード等の登録、変更の手続をレビューする
		検収入力時に仕入計上され、システムにより自動仕訳される	<ul style="list-style-type: none"> ・システム上、検収入力時に仕入計上されることを確認する ・自動仕訳パターンの妥当性を確認する ・自動仕訳パターンの登録、変更の手続をレビューする

(注)エディット・バリデーション・チェック;入力内容が入力を予定している内容と一致しているかどうかをチェックする機能。

(6) リスク評価手続に係る実施計画の策定

22. 監査人は、業務処理統制と全般統制について、例えば以下のような情報システムに関するリスク評価手続の実施を検討する。

企業が重要な会計データを、会計システム以外の業務アプリケーション・システムによって作成している場合は、通常、監査人が利用する経営者の主張の

裏付けとなる統制活動は、その業務アプリケーション・システムに組み込まれているため、監査人は、会計システムに加え、そのアプリケーション・システムに関連する業務処理統制及び全般統制のデザイン及び業務への適用状況を評価し、重要な虚偽表示リスクを識別する必要がある。具体的な評価手続として、監査人は、システム担当者への質問やフローチャート等の作成により、統制活動の設定状況を理解する。また、監査人は、企業が実際に統制活動を実施している現場の観察や、文書による証拠などを検討する。さらに、監査人は、ITを利用しているユーザ部門における実施状況を検討することにより、企業が設定している統制活動が実際に業務に適用されていることを確かめる。

なお、ITを利用した統制活動が手作業による統制活動により補完されている場合には、監査人は、重要な虚偽表示リスクを識別するため、ITを利用した統制活動と手作業による統制活動の両方を総合的に評価する。内部統制の目的は、ひとつの統制活動で達成できるものではなく、いくつかの統制活動で補完されて達成される。したがって、監査人は、情報システムに関する統制活動の弱点を発見した際には、その弱点を補完する統制活動の有無を調査し検討する。

8. 監視活動の理解

23. 企業がITを利用して財務諸表を作成している場合には、経営者は、日常反復的な作業をITを利用した統制活動に依拠し、例外的事項に対してのみ日常的に監視活動を実施することにより、内部統制の有効性を効率的に確かめることができる。これら例外的事項の動向を定期的に又は随時に査閲し、適時な監視活動体制を確保するために、内部監査が必要となる。したがって、監査人は、企業の日常的な監視活動体制と、内部統制責任者や内部監査などによる定期的な又は随時の監視活動が、有効に機能しているか否かに留意する。また、監査人は、企業がITの設計段階で、あらかじめ監視すべき項目を設定していなければ、必要なデータを入手できないことや、情報システムが、単に各ビジネスプロセスに従って処理を実行しているだけでなく、経営者の監視活動に必要なデータが入手できるようにデザインされているか否かに留意する。

なお、監視活動のレベルの向上は、企業の内部統制の質を向上させ、情報システムに関する重要な虚偽表示リスクを軽減させるとともに、監査人による監査の効率性を高めることになる。

重要な虚偽表示リスクの評価

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

24. 監査人は、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においては、金額な面のみだけでなく、質的な面、及び当該リスクが企業に与えるその他の潜在的な影響の大きさなども勘案する。例えば、IDとパスワードの管理であっても、販売アプリケーション・システムの場合、アプリケーション・システム全体の管理者の管理は、売掛金等の特定のデータへのアクセス権を持つ担当者の管理よりも重要である。

2. 全般統制に不備があった場合の留意点

25. 全般統制に不備がある場合には、関連するすべての取引、勘定残高及び開示並びにそれらに関する経営者の主張に影響を及ぼすことに留意する必要がある。全般統制は、業務処理統制が有効に機能する環境を支えるものであることから、たとえ業務処理統制が有効に機能するように整備されていたとしても、その継続的

な運用を保証する全般統制に重要な不備があれば、情報システムの内部統制は有効に機能せず、重要な虚偽表示リスクが高まることとなる。例えば、アプリケーション・システムに適切な業務処理統制が組み込まれていても、全般統制としての運用状況が信頼できない場合には、当該業務処理統制の有効性が崩れてしまうため、そのままでは情報システムの内部統制に依拠できなくなる可能性がある。この場合に、監査人は、関連する取引、勘定残高及び開示並びにそれらに関する経営者の主張ごとの重要な虚偽表示リスクを評価する追加的リスク評価手続、運用テストの必要性及び実施する手続の内容、範囲等を検討し、何らかの追加的リスク評価手続、運用テストの実施が財務報告の信頼性の確保に寄与すると判断したときは、その手続を実施することになる。例えば、不備がある全般統制に関連する業務処理統制の運用テストの範囲を拡大し、また、評価の頻度を増やす等の対応が必要になる。

3. 業務処理統制に不備があった場合の留意点

26. 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に、監査人は、そのアプリケーション・システムにおいて同様の誤りが繰り返されている可能性があることに留意する。

一方、業務処理統制のうち、人とITが一体となって機能する統制活動に不備がある場合に、監査人は、その不備の内容が、人に関する部分から生じているものなのか、それともITに関する部分から生じているものなのかを識別する必要がある。ITに関する部分から生じている場合には、監査人は、自動化された統制活動の不備と同様、同じ種類の誤りが繰り返されている可能性に留意する。人に関する部分から生じている場合には、監査人は、一般的な手作業による内部統制に不備がある場合と同様の点に留意する。

4. リスク評価の修正

27. 監査人は、情報システムに関するリスク評価手続を実施し、内部統制に係るITのコントロール目標の達成度を確かめる。企業の情報システムに関するリスク評価において、内部統制が有効に運用されていると想定していたにもかかわらず、運用テストの実施により監査期間中に内部統制が適時に有効に運用されていないという監査証拠を入手することもある、このような場合、監査人はリスク評価を修正し、立案した監査手続を変更する。例えば、ある自動化された統制活動が有効に機能していなかった場合、監査人はこれに代わる他の自動化された統制活動の有無を確かめその有効性を評価する監査手続を立案するか、あるいはこの自動化された統制活動に依拠せず実証手続の範囲の拡大を立案することがある。

経営者及び監査役等とのコミュニケーション

28. 情報システムに関する内部統制に重大な欠陥がある場合には、監査人は企業の経営者及び監査役等に当該欠陥を報告し、改善を求める。

評価したリスクに対応する手続の実施

29. 監査人は、評価したリスクに対応する監査手続（リスク対応手続）、具体的には運用テストと実証手続を実施しなければならない。

監査人は、監査対象期間における業務処理統制の運用の有効性に関する十分な心証を得るために、原則として関連する全般統制の運用テストを実施するが、業務処理統制の運用テストの範囲を拡大する、あるいは評価の頻度を増やすことにより十分な心証を得る場合もある。

30. 監査人は、IT について以下の手続を実施して監査意見を形成するに足る合理的な基礎を得るための監査証拠を入手する。

(1) 監査人が必要と判断した場合に実施する経営者の主張ごとの重要な虚偽の表示を防止又は発見・是正する統制が有効に運用されているかについて評価する手続（運用テスト）

(2) 経営者の主張ごとの重要な虚偽の表示を発見するために実施する実証手続（取引、勘定残高及び開示に対する詳細テストと分析的実証手続）

監査人は、以下の第 31 項から第 36 項で示されている IT を利用した監査手続を実施する。単独または組み合わせて実施されるこれらの監査手続は、監査人が実施する目的により運用テスト又は実証手続となる。

(3) ロール・フォワード手続

自動化された業務処理統制に関しては、IT による処理に一貫性があるため、業務処理統制の業務への適用に関する監査証拠は、全般統制（特に、変更に関する内部統制）の運用の有効性に関する監査証拠と組み合わせることにより、監査対象期間における業務処理統制の運用の有効性に関する監査証拠を提供する（監査基準委員会報告書第 30 号 31 項）。

監査人は、前回、運用の有効性を確かめた時から変更された内部統制に依拠する場合、当年度の監査で内部統制の運用の有効性を確かめなければならない（監査基準委員会報告書第 30 号 39 項前段）。

全般統制の整備、運用状況を評価し、重要な変更がないことが確認出来る場合には、過年度に実施した自動化された統制活動に継続して依拠することができる。

1. 記録や文書の査閲

31. システムの運用記録、障害報告のレビューを行い、記録の網羅性についての統制のデザインを評価し、記録された障害報告の確認を行い、当期に発生した重大障害の把握、その対応の正確性を検討し、虚偽記載の発生の可能性を確認する。また、システム設計書等のレビューを行い、会計方針、法務要件、業務要件に合致したシステムが作成されていることを確認することも有効な手続である。

IT については、システム要件、設計の確認を行うことによって実証テストをかねることができるケースが存在することに留意する。また、障害対応については、監査の目的から障害を未然に防ぐ統制より、会計記録の正確性により重点がおかれることになる。対象としては、システム全般統制に関するドキュメントの査閲、電子データを利用した総勘定元帳、補助元帳、各種証憑書類等との突合の実施が考えられる。

2. 観察 / システム運用現場視察

32. IT システムの運用、管理現場の視察を行い、システム運用、変更に関する統制についての把握、テストを行う。観察は主に、リスク評価手続で利用されるが、IT については、リスク評価手続を通して、運用のテストをかねることができるケースが存在する。

3. 質問 / ヒアリング

33. 過年度の監査において、自動化された内部統制が意図したように運用されていたことを確かめている場合、監査人は、その自動化された内部統制について、運用の継続的な有効性に影響する変更の有無に関する監査証拠を経営者への質問

及びどの内部統制が変更されたかを示す記録の閲覧により入手する。(監査基準委員会報告書第31号30項~34項例示)

質問は、すべての対象に対して有効であるが、証明力の弱い手続であるため、自動化された統制につき、過年度の監査結果に依拠する場合は、質問による確認のみならず、変更記録の保管状況を検討する必要がある。

4. 再計算 / CAAT

34. IT を利用する場合、監査人は、企業から電子ファイルを手に入るとともに、計算方法(ロジック)を手にし、まず計算方法(ロジック)自体の検証を行う。その後監査人は、企業のシステムとは別のシステムにより計算を行い、計算結果の比較を行う。検証対象としては、減価償却、外貨換算等の計算、売上高の合計転記などの集計計算が該当する。

5. 再実施 / CAAT

35. IT を利用する場合としては、自動化された統制に対して、入力時の統制についての再実施、記録された電子情報間の整合性を確認する IT を利用した照合手続の再実施が考えられる。入力統制の検証にあたっては、本番環境へのテストデータの投入は、会社の情報システムに多大に影響を与えることが考えられるため、慎重に行う必要がある。なお、本番環境へのテストデータの投入に代え、DDL(データ・ダウン・ロード)技法を行うことがある。検証対象としては、システムアクセス統制、自動化される統制で行われる入力時のマスターチェック、限界値のチェックなどの各種入力統制及びシステム間のデータ連携についての照合、財務諸表の組替、名寄処理の再実施等が該当する。

6. 分析的手続

36. IT を利用することにより、分析的手続として、手作業で実施するより大量データを利用した詳細な分析・検討を行うことが可能となる。対象としては、たな卸資産の回転期間分析、売掛金の年齢調べ、製品別原価率の算定等が該当する。

監査調書

37. 監査人は実施した手続及びその結果、結果に至る過程につき明瞭に監査調書に記載しなければならない。

ITの専門家の利用

38. 監査人は、監査計画の策定及び監査の実施に際して、ITの利用状況及びITが内部統制に及ぼす影響の評価について、専門家の業務を利用するか否かの判断を行う必要がある。監査人は、専門家の業務を利用する場合には、その専門家が、単にITの知識のみではなく、情報システムに関する重要な虚偽表示リスクの評価について必要な知識を有しているかなど、専門家としての能力、客観性を検討する。

監査人は、監査の目的を達成するために、対象となる情報システムの範囲及び監査人が想定するリスクをITの専門家と具体的かつ十分に協議する必要がある。監査人は、その業務の結果が監査証拠として十分かつ適切であることを確かめ、その内容を自らが行うリスク評価に適切に結びつけなければならない。

専門家としての能力、客観性の評価、専門家との協議内容及び業務の結果につ

いての監査人の判断は、監査調書に適切に記載しなければならない。

アウトソーシングの位置づけ

39. ITに関わる様々な業務については、これを自社で行わず、外部業者へ委託(アウトソーシング)しているケースが非常に多い。情報システムの開発局面だけでなく、日々の運用に際して例えばデータセンター、ASP(Application service provider)と言われる外部の業者に多くの部分を委託することも一般的なこととなりつつある。このような状況の下では、情報システムに関する重要な虚偽表示リスクの評価を行うにあたって、被監査会社だけでなく委託先もその対象に加える必要がある。この場合に監査人は、委託先に対する監査手続の実施可能性につき留意する。

発効及び適用

40. 本報告書は、平成 年 月 日に発効し、平成 18 年 4 月 1 日以後開始する事業年度に係る監査から適用する。ただし同日前に開始する事業年度に係る監査から本報告書を適用することを妨げない。なお、早期適用するに当たっては、監査基準委員会報告書第 27 号「監査計画」、同第 28 号「監査リスク」、同第 29 号「企業とその環境の理解及び重要な虚偽表示リスクの評価」、同第 30 号「評価したリスクに対応する監査人の手続」及び同第 31 号「監査証拠」を同時に適用することとする。

以 上

〔付録〕

【表1】ITのコントロール目標と監査要点との関係の例示（販売取引サイクルの一部）

ITの コントロール目標	会計データの 網羅性	会計データの 正確性	会計データの 正当性	ファイルの 維持継続性
具体的なITの コントロール目標	売上取引が漏れなく、重複なく記録され、残高更新され、未決済及びエラーとなった売上取引は期間内に全て適切に処理されていること。	売上取引は、正確に適時に適切な勘定に記録されていること。エラーとなった売上取引は期間内に全て適切に処理されていること。	売上取引は、実際に生じた経済事象を表し、かつ、当該企業に関連するものであり、承認されたものだけが入力され、処理されていること。	コンピュータに入力され、処理されたすべての売上取引が、販売管理システム及び会計システムに正確に更新されていること。
統制活動の例	コンピュータに入力された出荷指図書の連番管理。 売上データが出荷された出荷指図書ごとに作成され、販売管理システムから会計システムにバッチで転送される際に、数量と金額の件数と合計の突合が行われる。	コンピュータに入力された出荷指図書の数量又は単価が、一定の範囲を超えるとエラーになる。 コンピュータ入力時に、得意先及び価格についてマスタ・ファイルとの存在チェックが行われる。	コンピュータへの入力時に、得意先、価格及び与信限度について、マスタ・ファイルとの存在チェックが行われる。 与信限度を超えた取引は上司の承認入力が必要となる。	販売管理システムの売上取引の合計額と会計システムの売上高は、システム上で照合されている。
監 査 要 点	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			