

「IT委員会研究報告第31号」「IT委員会報告第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」Q & A」の一部改正について

平成22年6月9日
日本公認会計士協会

「IT委員会研究報告第31号」「IT委員会報告第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」Q & A」（最終改正 平成22年2月23日）を次のように一部改正する。

新	旧
<p>IT委員会研究報告第31号</p> <p>IT委員会報告第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」Q & A</p> <p>平成18年3月17日 改正 平成20年3月25日 改正 平成20年11月5日 改正 平成22年2月23日 <u>最終改正 平成22年6月9日</u></p> <p>日本公認会計士協会</p> <p>(Q1からQ31まで略)</p> <p><u>(全般統制に不備が存在した場合に想定されるリスクに対する監査人の評価及び対応について理解を深める。なお、対応例については、全般統制に不備が存在したことを前提とする。)</u></p> <p><u>Q32：全般統制に不備が存在した場合に想定されるリスクの評価及び対応はどのようなものですか。</u></p> <p>1. 全般統制の不備 IT委員会報告第3号第25項において、「全般統制の不備は、直接的には重要な虚偽表示リスクに繋がるものではない。しかしながら、全般統制は、主要な取引、勘定残高、開示等並びにそれらに関連する経営者の主張のほとんどに関係しているため、全般統制に重要な不備があった場合には、たとえ業務処理統制が有効に機能するようにデザインされていたとしても、その継続的な運用を支える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。」とあります。しかし、監査人は、開発管理や運用管理といった特定の不備がある全般統制が支援しているアプリケーション・システムの範囲や不備自体の性質等を考慮し、重要な虚偽表示リスクに与える潜在的な影響の範囲を明確化することができます。</p> <p>2. 全般統制の不備に対する一般的な手続 監査人が特定の全般統制の不備を発見した場合は、(1)当該不備を補完する他の全般統制を評価する、(2)関連する業務処理統制の評価手続を拡大する、又は(3)実証手続を拡大する、といった対応があります。</p> <p>(1) 当該不備を補完する他の全般統制を評価する対応 全般統制のリスクの評価においては、ITのコントロール目標の達成度を考慮に入れるため、監査</p>	<p>IT委員会研究報告第31号</p> <p>IT委員会報告第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」Q & A</p> <p>平成18年3月17日 改正 平成20年3月25日 改正 平成20年11月5日 最終改正 平成22年2月23日</p> <p>日本公認会計士協会</p> <p>(Q1からQ31まで略)</p> <p>(新設)</p>

新	旧
<p>人が特定の全般統制の不備を発見した場合において、同じ目的を達成する他の全般統制によりリスクを低減できることがあります。</p> <p>一般に、監査人は、リスク評価手続の実施の際に防止と発見の組合せによって、同じ目的を達成する他の全般統制によりリスクを低減できるかを考えます。例えば、監査人が防止的な全般統制の不備を発見した場合において、事後の承認やログのレビュー等の発見的な全般統制が有効に機能しているときは、リスクが低減されていると判断できることがあります。</p> <p>なお、監査人が全般統制の不備に基づくリスクが発現していないことを確かめることで、リスクを評価できる場合があります。</p> <p>(2) 関連する業務処理統制の評価手続を拡大する対応</p> <p>全般統制に重要な不備が存在した場合には、当該全般統制により継続的な運用を支えられている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ります。ただし、全般統制の不備の影響を受ける業務処理統制の範囲を特定し、業務処理統制の運用評価手続の範囲（件数、期間等）を拡大するなどにより業務処理統制の継続的な運用についての十分な心証が得られる場合もあります（IT委員会報告第3号第29項を参照）。</p> <p>また、監査人は、インプットデータとアウトプットデータの突合や、データ間の整合性の検討、計算結果の再計算などにより、結果が正しく処理されているかを検証することもできます。その際には、情報システムに対して実施されるテストをすべて再現するわけではなく、財務報告に影響する部分について必要な手続を実施することに留意します。</p> <p>(3) 実証手続を拡大する対応</p> <p>監査人は、(1)又は(2)の対応により、十分な心証を得られない場合には、財務諸表項目レベル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、開示等に対する詳細テストと分析的実証手続）（監査基準委員会報告書第30号第47項から第54項参照）を実施します。</p> <p>分析的実証手続を実施する場合には、監査人は、システム外で作成される情報や、他のシステムで生成された情報の利用を検討します。</p> <p>また、システムにおける誤謬や改ざんは、システムの性質上、同様の誤謬や改ざんを含む伝票等を大量に作成することが多くなる傾向があるため、仕訳テスト等の手続も有効な手段となります。</p>	
<p>Q33：システムに組み込まれた業務処理統制の整備状況が、仕様書等により評価できない場合に想定されるリスクの評価及び対応例について教えてください。</p> <p>1. 仕様書等の整備に関する全般統制に不備が存在したことにより想定されるリスク</p> <p>システムの仕様書等は、システムの企画開発の段階から、システムの設計に変更を加える保守の段階まで、設計の内容を明らかにするために作成されます。現状のシステムについての仕様等を記録するプロセスの全般統制の不備としては、(1)仕様書等が作成されておらず、もともと存在しない場合、(2)仕様書等が作成されているが、記録が不完全又はシステムの改修の記録がないなど不十分である場合、とがあります。</p> <p>上記(1)又は(2)である場合、監査上必要とされる業務処理統制がどのように設計されているかが判明しないため、監査人は、業務処理統制の整備状況の評価できないこととなります。</p> <p>2. 想定されるリスクに対するコントロール</p> <p>システムの仕様書等は、一般的に次のような点に留意して、確立したプロセスにおいて設計の内容を記録として残したものです。</p> <p>(1) 企画開発段階において記述の標準化を図り、記述を一定のルールの下で作成して判読を容易にする。また、設計途中での変更の管理をし、記述の不整合や漏れを防止する。</p> <p>(2) 保守段階においてシステムの変更管理の手順を定め、変更の履歴を残し、変更内容の記述を標準化する。</p>	<p>(新 設)</p>

新	旧
<p>監査人はこれらの点に留意して、業務処理統制の整備状況を評価するために必要な範囲の仕様書等が適切に作成されていることを確かめます。</p> <p>3. 全般統制に不備が存在した場合の対応例</p> <p>監査人は、システム開発者やユーザに対してシステムに組み込まれている業務処理統制について質問し、仕様書等により確かめます。しかし、仕様書等が不十分で確かめられない場合には、次のような対応が考えられます。</p> <p>(1) 仕様書等以外の書類等による検討</p> <p>監査人は、ユーザマニュアル等のユーザ向け操作手順書により業務処理統制を読み取る。この場合、ユーザマニュアル等は、システム開発者が作成したものやパッケージソフトのベンダから提供されたものであることが望ましい。</p> <p>監査人は、業務処理統制となるプログラムのソースコードを利用し、その内容を確認する。プログラム上に記述されているコメント(コンピュータ言語で記述されているソースコードではなく、人がプログラムの修正などのメモとして記述した注釈)が十分でない場合は、他の手続と組み合わせることで実施することにより、業務処理統制を確認する。この方法は、ソースコードが入手可能で、かつ、理解できることが前提となる。また、実施に当たっては、ITの専門家の利用が必要になる場合がある。</p> <p>(2) 上記の対応がとれない場合の検討</p> <p>(1)の対応がとれない場合には、監査人は、例外的に次のような対応をとることが考えられます。ただし、この場合はシステムの設計内容が明確に把握できないため、特定の機能しか確かめられないことに留意する必要があります。</p> <p>業務の実際の操作や制御画面を観察し、組み込まれている業務処理統制を確認する。</p> <p>アクセス権限の制御、承認入力や与信設定等の実際のシステムの設定情報を確認する。</p> <p>原始証憑や入力データ等を用いた処理の結果について、手作業やCAATによる再計算等により、組み込まれている業務処理統制を確認する。</p>	
<p>Q34：データベースの会計データを直接修正する手続に不備が存在した場合に想定されるリスクの評価及び対応例について教えてください。</p> <p>「データベースの会計データを直接修正する手続」とは、会計システムなどのアプリケーション・システムを通さず、データベースの更新権限をもつIDを使って、データベース上の会計データに直接アクセスし、データの追加、変更又は削除を行うことをいいます。</p> <p>1. データベースの直接修正に関する全般統制に不備が存在したことにより想定されるリスク</p> <p>アプリケーション・システム上に保持されている会計データは、各業務プロセスにおいて各種の承認手続を経て登録や計上されたものであり、その修正方法についても業務プロセス上で定められ、アプリケーション・システム上で実行されているのが通常です。しかしながら、業務上修正が必要であるにも関わらず、アプリケーション・システムの機能ではユーザにより会計データの修正を行えない場合や、バグなどの影響により、会計データがユーザの意図しない状態に変わってしまった場合には、例外的にデータベースを直接修正しなければならないことがあります。データベースの直接修正に対する全般統制に不備が存在した場合には、業務上は意図しない内容の会計データの修正が行われるリスクが存在します。</p> <p>なお、データベースの直接修正が頻繁に発生しているような場合には、監査人は、それ自身が重要な虚偽表示リスクとなる可能性があることに留意する必要があります。</p> <p>2. 想定されるリスクに対するコントロール</p> <p>データベースが直接修正されるリスクに対するコントロールとしては、一般に次のようなものが考え</p>	<p>(新 設)</p>

新	旧
<p>られます。</p> <p>(1) データベースの直接修正に関する承認 プログラムの変更手続と同様に、データベースの直接修正について変更の申請及び承認に関するコントロールを整備し、運用する必要があります。例えば、データベースの直接修正について事前に申請を行い、適切な権限者の承認を得ていることが必要となります。また、修正後の会計データに対する承認の手続も必要です。</p> <p>(2) 職務の分離 職務の分離を適切に実施することにより、データベースの直接修正に関するリスクを低減することができます。例えば、ユーザ部門が自ら会計データを修正するのではなく、依頼によりシステム部門が修正を実施します。</p> <p>(3) 更新権限の限定 データベースの更新権限を付与する人員は、システム部門内でも一部の担当者に限定し、それ以外の担当者への更新権限の付与を制限します。</p> <p>(4) 更新ログの分析によるモニタリング データベースの直接修正が行われた場合には、その内容を後で確かめることができるよう、修正に関するログを残し、モニタリングします。</p> <p>3. 全般統制に不備が存在した場合の対応例</p> <p>(1) データベースの修正に関する承認手続に不備が発見された場合 データベースの修正に関する承認手続に不備が発見された場合、監査人は、修正された内容の妥当性を個々に確かめることで、会計数値への影響の有無を評価することが可能と考えられます。また、検出された不備以外には承認のない変更が存在しないことを確かめ、被監査会社が行ったすべての変更の問題がないことを根拠に当該不備に関連するリスクが少ないという心証を得ることも可能と考えられます。</p> <p>(2) 職務の分離及び更新権限の限定に不備が発見された場合 職務の分離及び更新権限の限定に関して、例えば、次のような状況があった場合には不備と考えられる可能性があります。</p> <ul style="list-style-type: none"> ・ データベースの更新権限者がプログラム開発や保守業務にも従事している。 ・ データベースの更新権限者がユーザ部門の業務にも従事している。 ・ データベースの更新権限者を特定できない（IDやパスワードの共有、データベース管理業務に関係していないユーザへの更新権限の付与など）。 <p>上記のような場合には、更新ログの分析によるモニタリングにより、全般統制の不備を補完することが可能と考えられます。監査人は、モニタリングの実施方法やその結果について評価又は検討が必要となります。</p> <p>(3) 更新ログの分析によるモニタリングに関する不備が発見された場合 更新ログの分析結果により十分な心証が得られない場合には、監査人は、被監査会社に追加的に分析を依頼し、再度その結果を入手することを検討します。例外的に、分析の結果の検討ではなく、監査人自らがログを分析することで心証を得ることができる場合があります。</p> <p>更新ログが適切に保管されていない場合には、監査人は、ログを利用したモニタリングの評価を有効に行うことができないため、「2.(4) 更新ログの分析によるモニタリング」に対するコントロールに依拠することができません。このような場合、監査人は、まず、「2.(1) データベースの直接修正に関する承認」、「2.(2) 職務の分離」又は「2.(3) 更新権限の限定」に対するコントロールの評価で十分に心証を得られるかどうかを確かめる必要があります。その際に、アクセスログを利用できる場合があります。</p> <p>十分な心証が得られない場合には、監査人は、補完統制となる業務処理統制に依拠するか、又は実証手続による対応を検討する必要があります。</p>	

新	旧
<p data-bbox="210 254 1460 359">Q35：システム部門が存在せず、担当者一名のみでシステムの管理を行っている場合に、プログラム開発担当者や変更担当者や運用担当者の職務の分離がされていないときに想定されるリスクの評価及び対応例について教えてください。</p> <p data-bbox="231 401 1469 464">1．プログラム開発担当者や変更担当者や運用担当者の職務の分離に関する全般統制に不備が存在したことにより想定されるリスク</p> <p data-bbox="252 470 1469 646">システム部門が存在せず、担当者一名のみでシステムの管理を行っている場合には、実際の業務で使用されているソフトウェアが稼働している本番環境に新規又は変更したプログラムを適用するに当たって、予め導入手順が明確に定められていたとしても、誤って又は故意に当該手順に従わずに行うことが可能です。これにより、データが不適切に修正されたり、機能の検証等が不十分なプログラムやバージョン違いのプログラムがリリースされる可能性があります。</p> <p data-bbox="231 684 753 716">2．想定されるリスクに対するコントロール</p> <p data-bbox="252 720 1469 783">システムの担当者が一名である場合には、プログラム開発担当者や変更担当者や運用担当者の職務の分離を行ってコントロールを機能させることができません。</p> <p data-bbox="252 789 1469 966">ただし、担当者が一名であっても、上位の権限者の事前承認や利用部門の動作確認を得ることによって、一定の牽制機能が期待できる場合があり、定められた手順に従って業務を実施したことについて作業記録を残す方法が考えられます。作業記録には、自動的に取得されるログだけではなく、紙に記録しているものも含まれます。作業記録には、業務の実施前に権限者が承認した結果、実際の作業内容、利用部門の動作の確認結果や作業の結果報告などが考えられます。</p> <p data-bbox="231 1003 753 1035">3．全般統制に不備が存在した場合の対応例</p> <p data-bbox="252 1039 1469 1144">作業記録が残されている場合において、監査人は、プログラム等の重要な変更について適切に内容が記載されており、その作業記録に対して権限者による承認等が行われているかを評価し、当該変更について全般統制の不備の影響が小さいと判断できることがあります。</p> <p data-bbox="252 1150 1469 1213">作業記録が残されていない場合には、関連する業務処理統制の評価手続又は実証手続を拡大するといった対応をとることになります。</p>	<p data-bbox="2131 254 2237 285">(新設)</p>
<p data-bbox="210 1318 1460 1381">Q36：システム部門において、プログラムの開発担当者や保守担当者や運用担当者の職務の分離がされず、業務が運用されている場合に想定されるリスクの評価及び対応例について教えてください。</p> <p data-bbox="231 1430 1469 1493">1．システム部門において、プログラムの開発担当者や保守担当者や運用担当者の職務の分離に関する全般統制に不備が存在したことにより想定されるリスク</p> <p data-bbox="252 1499 1469 1604">プログラム開発担当者や保守担当者や運用担当者の職務の分離とは、一般的には、プログラム開発担当者や保守担当者や運用担当者の職務を区分し、前者の本番環境へのアクセスを認めない、又は一定の手続を定めてアクセスを制限することを指します。</p> <p data-bbox="252 1610 1469 1715">しかし、障害が発生したときの対応が効率化されることや、ユーザ部門からの変更要求に迅速に応えられる等の業務的な利点を考慮し、プログラムの開発担当者や保守担当者が運用を担当している場合があります。</p> <p data-bbox="252 1722 1469 1919">本番環境で稼働するプログラムは、新規に開発される場合又は変更される場合であっても、当初意図したとおりの動作をすることが十分にテストされ、品質が保証された上で業務に利用されることが必要です。職務の分離が十分でない場合には、開発担当者や保守担当者自身が本番環境に容易にアクセスできるため、自身で開発や変更したプログラムを、ユーザによる受入れテスト、移行承認等の他者のチェックを入れずに、本番環境で稼働させることができる状態にあります。このような管理体制では、不適切な内容、バージョン違いのプログラムやデータが本番で使用されるリスクが存在します。</p>	<p data-bbox="2080 1331 2187 1362">(新設)</p>

新	旧
<p>2. 想定されるリスクに対するコントロール システム部門の存在する被監査会社では、アプリケーション・システムやデータベース等を開発又は変更するときには、ユーザ部門からの依頼として受け付けます。プログラム開発担当者や保守担当者が、開発環境において開発又は変更の作業を行い、運用担当者がプログラムを本番環境へ導入します。導入作業をプログラム開発担当者や保守担当者が行う場合でも、通常は本番環境への無制限のアクセスを認めず、一定の手続を定めてアクセスを許可します。プログラム開発担当者や保守担当者と運用担当者が同一の場合には、必要なチェックを受けることなく、本番環境にプログラムを導入することができるため、両者を分離して一定の牽制を働かせます。プログラム開発担当者や保守担当者の誤り又は故意による不適切な変更を避けるために、書面による承認プロセスの確立や、ワークフロー・システムが導入されます。また、プログラムの管理を行うライブラリ管理システムが導入される場合があります。</p> <p>3. 全般統制に不備が存在した場合の対応例 システム部門において、プログラムの開発担当者や保守担当者と運用担当者の職務の分離がされていない場合には、新規又は変更されたプログラムの品質等が十分に担保されないリスクがあります。ただし、監査人は、次のように不備が存在した全般統制を補完する他の全般統制によりリスクが低減されていると判断できる場合があります。</p> <p>システム部門の存在する被監査会社では、アプリケーション・システムやデータベース等を変更するときには、ユーザ部門からの依頼に基づき作業を実施します。ユーザ部門からの依頼事項は、ワークフロー・システムや書面で起票され、ユーザ部門内での承認を受けた上でシステム部門に連絡され、システム部門内で台帳管理されます。さらに、システム部門では、プログラムの本番環境への移行や、プログラムの修正等の実施した作業内容の記録を残す手続が決められており、これらの記録には、実施したテスト結果、システム部門内の上位者による承認、ユーザ部門などの検証及び本番環境を変更した作業日時などが含まれます。これらの記録を監査人が確かめることにより、リスクが低減されていると判断できる場合があります。</p> <p>システム部門が、システムのプログラム変更履歴、本番環境へのアクセス記録や本番環境での操作履歴等の各種ログを記録し、これらのログと作業記録とを検証している場合があります。また、システム部門において、品質管理の一環でプログラムの事後レビュー等を実施している場合もあります。これらにより、監査人は、さらにリスクが低減されていると判断できる場合があります。</p>	
<p>Q37：システムの開発過程においてユーザ受入れテストが実施されていない場合に想定されるリスクの評価及び対応例について教えてください。</p> <p>1. ユーザ受入れテストに関する全般統制に不備が存在したことにより想定されるリスク ユーザ受入れテストは、システムを本番移行する前のユーザによる最終確認フェーズであり、本番と同等の環境で、実際にシステムを利用するユーザが参加して、関連する業務処理統制を含む機能が正常に機能するかについて確かめるものです。システムの開発過程においてユーザ受入れテストが行われないうち、業務に必要な機能の確認が適切に行われずにユーザ部門が要求する業務要件を満たしていないシステムが本番環境にリリースされるリスクがあります。</p> <p>2. 想定されるリスクに対するコントロール システムの開発過程において、ユーザの業務要件に基づきシステムの仕様が決定され、プログラムが作成されます。システムにユーザの業務の要件が適切に反映されているかどうかを確かめるには、システム部門のテストだけでは十分ではない場合があります。そのため、業務要件を理解した適切な能力を有するユーザが、テスト項目や内容を十分に検討し、テストを行います。</p>	(新 設)

新	旧
<p>3. 全般統制に不備が存在した場合の対応例</p> <p>ユーザ受入れテストが実施されていない場合には、業務処理統制を含む機能が、システムに実装されているかの検証が十分に行われていないというリスクが想定されます。このような場合には、次のような対応が考えられます。</p> <p>(1) 通常システムの開発過程においては、ユーザ受入れテストの前にシステム部門が様々なテストを実施します。システム部門が実施する一連のテストにおいても、システムに必要な機能が充足されているかどうかの検証を行うこととなります。システム部門によるテストにおいても、十分に業務を熟知している担当者がユーザ視点も踏まえてテストを実施している場合や、極めて簡易なシステムのためユーザ自身が確認を行う必要性が低い場合などにおいて、システム部門のテストでユーザ受入れテストと同等とみなせることもあります。</p> <p>(2) ユーザが、予めシステムの本番移行後の試用期間を設定し、適切な数値の集計や業務処理統制が機能しているかを確認し、要求する業務処理統制を含む機能が実現されていない場合においては、修正を依頼していることがあります。監査人は、これらの修正依頼の記録を確認することで、リスクが低減されていると判断できる場合があります。</p>	
<p>Q38：会計システムの特権IDの管理が不十分で、必要最小限のユーザ以外にも権限が付与されている場合に想定されるリスクの評価及び対応例について教えてください。</p> <p>1. 会計システムの特権IDの管理に関する全般統制に不備が存在したことにより想定されるリスク</p> <p>会計システムの特権IDとは、例えばすべての勘定マスタ情報、パラメータ設定値の変更や会計データの作成、変更、削除及びそれらの権限の設定等が可能なシステム管理者が使用する特別なIDをいいます。</p> <p>特権IDの管理が不十分で、必要最小限のユーザ以外にも権限が付与されている場合は、例えば、次のような会計データに対する不正や誤謬についてのリスクが高まることとなります。</p> <ul style="list-style-type: none"> ・ 特権IDを用いて本来会計伝票の修正を赤黒処理すべきところを直接修正したり、締め後のデータを直接修正するなど、必要な統制を回避して修正するリスク ・ 特権IDの使い方や効力を理解していないユーザが、データやマスタを変更、破壊してしまうリスク ・ 経理部門の上級管理職になりすまし、自ら経費の水増し伝票を起票し、かつ承認することも可能になってしまうなど、自ら起票した伝票を自身で承認するリスク ・ 特権IDが共有されており、誰が使用して会計データを修正したかを特定することが困難なリスク <p>2. 想定されるリスクに対するコントロール</p> <p>特権IDは強力な権限を有しているため、必要最小限の者のみに付与されるべきであり、通常の操作に使用するIDの管理に加えて、例えば、次のようなコントロールが考えられます。</p> <ul style="list-style-type: none"> ・ 特権IDと通常の操作に使用するIDとを区別し、特権IDの使用を必要とする者でも会計システムの通常利用においては、通常の操作に使用するIDを使用する。 ・ 特権IDの管理をシステム部門に移管し、ユーザ部門で特権IDの使用を必要とする場合には、その都度に使用できる特権IDの貸出し及び返却を管理する。 ・ 個々の会計担当者の職責及び職務権限に応じてシステム上の権限が付与されるように、機能を限定した管理用のIDを個人ごとに設定し、発行する。 ・ 特権IDの操作に関しては、操作内容を文書化し、ユーザ部門管理者の承認を受ける。 ・ 会計システムのログの取得機能を活用し、事後的にモニタリングする等の発見的な統制を組み込む。 	<p>(新 設)</p>

新	旧
<p>3. 全般統制に不備が存在した場合の対応例</p> <p>特権IDの管理の不備の内容や程度によって、会計データが歪められているリスクの程度や可能性は変わるため、監査人は、次のような対応を検討することが考えられます。</p> <p>(1) 代替的又は補完的統制によりリスクを低減される程度を評価</p> <p>例えば、会計伝票がシステム出力を含む紙媒体で運用され、起票者及び承認権限者の印が押印されていることや、月次締めで他の帳票との照合を行うことなどの手作業による統制が有効であれば、監査人は、会計データが歪められているリスクは低減されていると判断できる場合もあります。</p> <p>また、特権IDの使用状況についてログの適時かつ適切なモニタリングが整備及び運用されていれば、特権IDの管理の不備による不正や誤謬が実際に発生したとしても、適時にそれが発見される可能性が高まります。したがって、監査人は、会計データが歪められているリスクは低減されていると判断できる場合もあります。</p> <p>(2) 特権IDの利用について不正や誤謬がないことを直接的に検証</p> <p>監査人自らが会計帳簿や伝票を閲覧し、アクセスログを検証する等の手続を実施することにより、本来通常の操作に使用するIDを用いてアクセスや操作がされるべきところに特権IDによってアクセスや操作が行われていないこと、又は特権IDによって会計データが不正に操作されているリスクが高くないことを確かめることができる場合があります。</p> <p style="text-align: right;">以 上</p>	<p style="text-align: center;">以 上</p>

以 上