

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)
追加付録

平成 19 年 12 月 26 日
経済産業省

企業のIT統制に関する研究会 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 法政大学大学院 イノベーションマネジメント研究科 教授

加藤 俊也 公認会計士

河本 高文 東芝ソリューション株式会社

清水 恵子 公認会計士(日本公認会計士協会 IT委員会 監査 IT対応専門委員会専門委員)

田中 太 財団法人金融情報システムセンター 監査安全部 総括主任研究員

田吹 隆明 田吹技術士事務所

千枝 和行 社団法人日本情報システム・ユーザー協会 企業情報マネジメント研究会委員

中村 元彦 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

松原 榮一 社団法人日本情報システム・ユーザー協会 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 東京支部理事

(敬称略)

まえがき

経済産業省では、情報システムの適正な管理等を目的として策定している「システム管理基準」及び「情報セキュリティ管理基準」と、財務報告に係る内部統制で求められている「ITへの対応」との間の具体的な対応関係を明らかにするため、「企業のIT統制に関する調査検討委員会」における検討等を踏まえ、「システム管理基準 追補版（財務報告に係るIT統制ガイドランス）」を取りまとめ、平成19年3月30日に公表した。

今般、企業が内部統制を整備運用する上での更なる参考資料を提供するため、「企業のIT統制に関する研究会」において、平成19年8月以降計8回にわたって審議を行い、「システム管理基準 追補版（財務報告に係るIT統制ガイドランス）追加付録」をとりまとめた。

なお、本追加付録の提供するものは、あくまで主要なケースを想定した参考情報であり、それぞれの企業がIT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、個々の企業の事業内容や組織構造等によって、さまざまなケースが存在し得ることは言うまでもない。

したがって、本追加付録の利用にあたっては、各企業の実情に合わせた適用を行うこと。

検討の経緯

平成19年	8月	2日（木）	第1回研究会
平成19年	8月	9日（木）	第2回研究会
平成19年	8月24日（金）	第3回研究会	
平成19年	8月30日（木）	第4回研究会	
平成19年	9月	7日（金）	第5回研究会
平成19年	9月14日（金）	第6回研究会	
平成19年	9月28日（金）	第7回研究会	
平成19年	12月12日（金）	第8回研究会	

構成

- ・付録7．財務会計パッケージソフトウェアの機能等一覧表（例）の使い方
- ・付録8．IT統制のための財務会計パッケージソフトウェア向けプロテクション・プロファイル（シナリオ例）
- ・付録9．IT業務処理統制における業務プロセスごとの、リスク、統制活動、統制活動の評価手続の例示

付録 7. 財務会計パッケージソフトウェアの機能等一覧表（例）の使い方

はじめに

「財務会計パッケージソフトウェアの機能等一覧表（例）」（以下、一覧表という）は、財務会計パッケージソフトウェア（以下、会計パッケージという）をカスタマイズしないで使用している場合の IT 統制の評価に有用と思われる質問項目の例示であり、会計パッケージベンダーが、会計パッケージの機能等に関する情報をユーザに提供することにより、ユーザの内部統制の整備・構築、評価が効率的に実施されることを目的としたものである。質問項目は、「会計パッケージの機能についての質問」と「単に評価のために利用したい情報を収集するための質問」で構成されている。このため、質問項目の回答内容が全て「はい」であるからといって、会計パッケージの機能が優れているとか IT 統制が有効であると判断するものではない。例えば、質問項目「6-1-3DBMS 2. DBMS に関するデータインターフェイスの仕様の開示は可能か。」は、「単に評価のために利用したい情報を収集するための質問」であり、記載内容によって、統制目標を実現するために、会計パッケージ以外の DBMS に、どのような統制が実現されるべきかを検討することになる。

会計パッケージは、カスタマイズせず市販の状態のまま利用していることを前提としている。カスタマイズとはソースプログラムを変更して利用することであり、パラメータ設定の選択及び調整はカスタマイズに含まない。またアドオンとは特定の機能の追加に関して一連のソースプログラムを変更することなく、そのまま追加することを想定している。

なお、一覧表における「メニューによる設定状況」は、新規セットアップを実施した場合に、設定されている状態を「デフォルト（基本設定）」、会計パッケージのユーザが別途設定を変更しなければならない場合を「オプション（選択可能）」、電子帳簿保存法対応の選択を実施すると一括して設定される場合を「電子帳簿保存法対応のみ」に該当するものとして記載している。

本追補版の図表Ⅲ.4-2（⇒ 第Ⅲ章 4 節（3））でパッケージソフトウェアを利用する場合のリスク評価の例を示している。この中に、IT 全般統制に関する例として以下の記載がある。

- ・ 購入したパッケージソフトウェアにプログラム変更を行っていない場合、当該パッケージソフトウェアについては自社で不正なプログラム開発が行われているリスク等を回避していると評価できる。
- ・ バージョンアップ等のプログラムの変更は、パッケージソフトウェアを開発した外部の専門業者によって行われるため、不正にプログラム変更をするリスクは限定される。

このため、一覧表でも、プログラム変更についての情報収集と機能把握を行うために、「6-1-2 ソースプログラム」と、「6-2 バージョンアップ」の質問項目を設定している

また、IT業務処理統制の例として以下の記載がある。

- ・ IT 業務処理統制の機能を具備している場合には、業務の一貫性の確保、照合手続の自動化、例外事項報告書作成の自動化、職務分掌に従ったアクセス権限付与等が可能となるので、リスクが限定される。

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。

この一覧表は、会計パッケージに組み込まれた自動化された統制機能等を理解し、それがどのように利用され、もしくは利用されずに手作業などの統制と組み合わせることにより、IT 統制が整備されているかを評価するためのものである。各企業の業務の中で会計パッケージがどのように活用されているかを明らかにし、IT 業務処理統制を理解し、整備及び運用状況を評価する際の助けとなる。

企業は、パッケージの持つ以上のような機能等を一覧表により理解したうえで、その機能に対応した運用体制を、内部統制として整備、運用する必要がある。

一覧表を作成するにあたっての質問項目の意図及び記載内容を以下に示す。

1. データの入力

個々の取引ごとに入力するケースを前提として、手作業によるチェックという統制活動を評価するために必要な情報の収集を目的としている。

○ 1-1 入力の正確性と完全性の確保

個々の取引の入力時及び入力後の統制機能に関する質問である。

入力後の統制については、個別のチェックをするのか、複数回の入力をまとめて検証するのかについて記載する。帳票の出力がある場合は、帳票名を記載する。

○ 1-2 仕訳データ確定の承認機能

承認機能の有無に関する質問である。承認後に変更可能な場合には変更履歴がどのレベルにあるか（日付のみか変更内容も記録するか）について記載する。

○ 1-3 変更の可能性と履歴の保存及び追跡可能性

一定の期間について仕訳データの追加、訂正を禁止する設定にできるかどうか、また、その設定を解除することができるか。できる場合は、解除の履歴がどのレベルにあるか（日付のみか内容も記録するか）について記載する。

2. インターフェース

大量のデータを一括的に取り扱うケースを前提としている。最初に当該機能の有無について確認している。大量データの取り扱い機能は、単純作業の繰り返しにともなうエラーを回避すること等により作業の効率に資する。しかしながら、取り扱いを誤ると大量のエラーに結びつく場合があるので注意が必要である。

○ 2-1 アプリケーションとしてのインターフェース機能

同種類のパッケージソフトウェア間、例えば販売モジュールと会計モジュール間の同種パッケージ間のデータ連動等に関する質問である。販売モジュールで作成されたデータが、自動仕訳機能を使用して会計モジュールに入力される場合などは、自動仕訳機能の評価を実施すべき場合があるため、2-1-2において、こうした機能に関する情報の開示の有無を質問している。転送前の金額・件数と転送後の金額・件数等を出力もしくは比較することにより、データの網羅性を担保するなどの仕組みが存在するかについて記載する。

○ 2-2 汎用データによるインポート機能

ユーザが直接編集可能な状態のファイルを直接操作し取り込むことを前提としている。汎用データとは、例えば CSV 等のテキストファイルを想定している。仕訳データの手入力作業を効率化するために、ユーザが仕訳データを他のアプリケーション（スプレッドシート等を含む）で作成してインポートしている場合は、手入力の場合と異なるリスクが存在する可能性があるため、こうしたケースの有無や、関係する情報を把握するための質問である。2-1 と同様にインポート前の金額・件数と受入れ後の金額・件数等を出力もしくは比較することにより、データの網羅性や正確性を担保するなどの仕組みが存在するかどうかについて記載する。

また日付範囲やマスター等の整合性などデータの属性を検証する機能が存在することが想定されるため、これらに関する質問項目を追加している。

なお、2-3 エクスポートと 2-2 インポートの組合せによりデータ入れ替え等のリスクがあることに留意する。

○ 2-3 汎用データによるエクスポート機能

ユーザが直接編集可能な状態のファイルを直接作成し出力することを前提としている。会計パッケージで処理された仕訳データなどを、他のアプリケーション（スプレッドシート等を含む）で使用している場合には、汎用データによる受渡し業務に関するリスクを評価すべき場合があるため、こうしたケースの有無や、関係する情報を把握するための質問である。会計パッケージで処理されたデータを過不足なく正確に出力していることを確認する機能について記載する。

3 集計・検索・出力の機能

入力された個々のデータから、会計帳簿の作成、そして閲覧及び出力に至る領域に関する質問である。合計金額が正しいこと、勘定科目毎に集計されていることは会計パッケージの基本機能である。一覧表は会計パッケージベンダーが製品の総合テストを完了していることを前提としている。また、入力が不一致になる場合に最終的にその不一致を表示できるかどうかについて記載する。

○ 3-1 仕訳データの集計

仕訳データを複式簿記の原則にもとづいて一定の区分ごとに集計し、主要会計帳簿が正

確に作成されるかについて記載する。なお、主要会計帳簿は総勘定元帳、補助元帳、合計残高試算表、貸借対照表、損益計算表等を想定している。

また、3-1-4の質問では、例えば補助科目別集計表の合計金額と本勘定の残高とに不一致がある場合に、警告表示されたり、差額が印刷されたりする機能があるかどうかについて記載する。

○ 3-2 仕訳データの検索

検索機能は、メニューで可能かどうかについて記載する。また、ログからの仕訳データの検索については、メニューに検索機能がなくても、データが保存されており、別途のツールで検索可能な場合はその旨を記載すること。

○ 3-3 出力に関する機能

作業の進捗度に応じて、バージョンが異なるレポートを複数作成した場合、バージョンの相違が判別できない恐れがある。このため、入力確定時刻や出力時刻が判るなど、出力帳票のバージョン管理をする機能があるかどうかについて記載する。

4. 年次及び月次等の繰越処理

期首残高等について完全性、正確性、正当性を維持したまま残高を移行し更新できるかどうかについて記載する。

5. 各種法規対応

○ 5-1 消費税の処理

会計パッケージでは、仕訳データの入力のつど、自動的に、仮払消費税、仮受消費税を計算する機能を持っている場合がある。一方、そうした自動計算と合わせて、手入力や、自動計算した金額の手による訂正が可能になっている場合がある。こうしたいくつかの処理方法の使用が明確にならず、混在している場合などは、消費税計算の正確性に関するリスクが大きくなる場合がある。自動処理の後、手修正を可能とするかについて記載する。

○ 5-2 電子帳簿保存法への対応可能性

会計パッケージでは、「電子帳簿保存法対応」とするメニューを有している場合があり、「電子帳簿保存法対応」を選択した場合に、仕訳データの検索可能性や、変更記録の保存などの、電子帳簿保存法に定められる一定の要件を満たす機能が一括して設定される場合がある。こうした、機能の一括設定をユーザが使用しているかどうかを把握することが、リスクの評価に効率的な場合があるため、この質問を設定している。したがって、ユーザが実際に電子帳簿保存法の承認を受けているかどうか、とは別である。

6. パッケージ導入保守

会計パッケージ導入時、年度の繰越時の設定等についての質問である。会計パッケージ

の持つ重要で基本的な設定は、期中では変更できず、導入時や、年度の繰越時だけで変更可能となっているかについて記載する。

○ 6-1 新規セットアップ

・ 6-1-1 システム初期設定項目（パラメータ）

導入などに当たって、会計パッケージを自社の環境に適合させるために、メニューの初期設定項目（パラメータ）の変更を実施することを想定している。ここでは、パラメータのうちシステム管理上の重要な設定項目に焦点を当て、変更された際に証跡が残るかどうかを把握するために設定している質問である。

・ 6-1-2 ソースプログラム

ソースプログラムは開示されないなど、編集可能な状態にないことを確認することを目的としている。変更がないのであれば、当初意図されたとおりの内部統制の機能の発揮が期待されが、カスタマイズが実施されている場合にはリスクがまったく異なるため、カスタマイズがされている場合、判別することができるかどうかを把握するために設定している質問である。

・ 6-1-3 DBMS

DBMSに関する質問は、会計パッケージがなんらかのDBMSとの組合せで使用することを想定している。汎用的なDBMSを使用している場合は、使用しているDBMSに関するIT全般統制の評価を実施すべき場合があるため、評価に必要な情報を把握するために設定している質問である。

・ 6-1-4 OS

会計パッケージの機能がOSに依存している場合は、使用しているOSに関するIT全般統制の評価を実施すべき場合があるため、必要な情報を把握するために設定している質問である。例えば、シングルサインオン環境を構築している場合、評価者は会計パッケージとあわせて利用しているOSやネットワークレベルでの制御について検討する必要がある。会計パッケージにおいて、ユーザ権限の階層設定を適切に行っても、OSレベルの権限設定が適切に管理されていない場合、会計パッケージの内部統制機能を無効化するリスクが存在することに留意する。

また、セットアップ時にはデフォルトの管理者ID等のパスワードを変更できるかについて記載する。

○ 6-2 バージョンアップ

バージョンアップ時に会計パッケージベンダーの想定以外の変更ができないことについての確認の質問である。

7. システム運用管理

障害発生時の原因の究明及び復旧活動に関する質問である。

○ 7-1 稼働記録の保持

システムの稼働記録の適切性に関する質問である。障害対応は、人手による IT 統制の構築を含み、また抜本対策等はバージョンアップ等の対応であることから、6. パッケージ導入保守カテゴリとなるため、ここでは障害対応のトリガーとなる稼働記録の適切性に限定している。

○ 7-2 データファイルの保全

不測の事態に備えたバックアップの仕組みが存在するかに関する質問である。またデータのリカバリーをする際には、データの完全性、正確性の要件を充足しているかを記載する。

8. アクセス管理等

不正アクセス及び付与された権限の不正利用をどのように防止するかに焦点をあてた質問である。この目標の達成は下記のような複数統制の組合せにより実現される。

なお、8 アクセス管理等で質問している機能を DBMS や OS に依存している場合は、その旨の記載と、6 パッケージ導入保守への記載を行う必要があることに留意する。

○ 8-1 システムに対するアクセス制限

主にアプリケーション側のアクセス制御についての質問である。

ログインの制限は職務権限との一致が求められるが、ここでは、どのように設定するかではなく、権限の区分に対応する権限設定を可能とする機能があるかについて回答をする。システム管理者権限の行使は明確に区分されているか、もしくは会計パッケージベンダー側にしかシステム管理者権限がないかについて記載する。

なお、アカウントロックとは、誤ったパスワードが一定回数入力された場合、自動的に使用権限が取消される機能のことである。

○ 8-2 ユーザ ID の管理に資する機能

ユーザ ID は改廃の仕組みを構築することにより管理されるが、管理のための情報を出力できるか否かに焦点をあてている質問である。

ユーザ ID の棚卸などの管理手続を実施する際の効率性を高めるために、ユーザリストの一覧情報の出力機能があるかについて記載する。例えばユーザ ID の改廃履歴やユーザ ID 情報の最終更新日、ユーザ ID とそれに対応したシステム権限情報などをユーザが効率的に確認できる仕組みなどを想定している。

○ 8-3 ログ収集の可否

ログの収集はどのレベルでされているかについて理解できるように記載する。

○ 8-4 権限設定の制限など

本来兼務すべきことが好ましくない業務、例えば作成者と承認者が同一の場合、を制限することができる機能があるかについて記載する。

財務会計パッケージソフトウェアの機能等一覧表(例)

質問のカテゴリ	想定するリスク	統制目標	質問項目	*は、電子帳簿保存法の要求している要件	いいえ	はい	コメント	メニューによる設定状況			公表場所 (URLなど)
								デフォルト (基本設定)	オプション 選択可能	電子帳簿保存 法対応の場合 のみ	
1 データの入力	入力されるデータに漏れや重複がある。	入力データについて完全性、正確性、正当性を維持することができる。	1-1 入力の正確性と完全性の確保 1 入力の正確性を確保するため、入力時のマスタ・ファイルチェック、論理チェック等、プログラムによるチェック機能があるか。 ①伝票日付と会計期間の整合性のチェック機能 ②貸借金額のバランスのチェック機能 ③勘定科目(コード)のマスタへの実在性のチェック機能 ④勘定科目の貸借の位置に関するチェック機能 2 入力原票との正確性チェックに利用できる帳票出力機能があるか。(ある場合は、帳票名を記載) 3 データの入力後、入力総件数や合計金額に関するトータルチェックをおこなうための出力機能があるか。								
	正当で無いデータ(未承認)が入力される。		1-2 仕訳データ確定の承認機能 1 仕訳データの登録確定に関する権限者による承認機能があるか。 2 承認の履歴を保持し、表示、検索できる機能があるか。								
	入力されたデータに正当で無い変更が行われる。		1-3 変更の可能性と履歴の保存及び追跡可能性 1 確定登録済み仕訳データの変更を禁止し、赤伝票、黒伝票による訂正のみとすることができる機能があるか。 * 2 確定登録済み仕訳データを画面から直接に呼び出して変更可能としている場合に、変更証跡を残す機能があるか。 * 3 以下の一定の期間について、仕訳データの追加、訂正を禁止する機能があるか。 ①会計期間 ②半期 ③四半期 ④月次 4 一旦、一定の期間について、仕訳データの追加、訂正を禁止する設定とした後で、その設定を解除した場合に解除の記録は残す機能があるか。 5 変更した仕訳データの履歴が保存され、変更前後の仕訳データの対応を含めた検索、表示する機能があるか。								
2 インターフェイス	他のシステムから不正なデータを受け取る。	他のシステムから受け取るデータは正当、正確、完全である。	2-1 アプリケーションとしてのインターフェース機能 1 販売管理システムなどの他の業務管理システムから財務会計システムへの仕訳データの受け入れる機能があるか。 2 機能がある場合、可能な業務管理システムや、機能の内容が開示されているか。								
	他のシステムから受け取るデータが重複欠落する。 他のシステムから受け取るデータが正確で無い。 システムから正当でなデータが出力される。	システムから出力されるデータは正当、正確、完全である。	2-2 汎用データによるインポート機能 1 CSVなどの汎用データのインポート機能があるか。 2 インポートできる汎用データのレイアウトを開示しているか。 3 汎用データの受け入れの際に正当性、正確性、完全性確保のためのチェック機能があるか。 4 汎用データの受け入れの際に、期間帰属性確保のためのチェック機能があるか。								

質問のカテゴリ	想定するリスク	統制目標	質問項目	*は、電子帳簿保存法の要求している要件	いいえ	はい	コメント	メニューによる設定状況			公表場所 (URLなど)
								デフォルト (基本設定)	オプション 選択可能	電子帳簿保存 法対応の場合 のみ	
	システムから出力されるデータが正確で無い。 システムから出力されるデータに重複漏れがある。		2-3 汎用データによるエクスポート機能 1 CSVなどの汎用データのエクスポート機能があるか。 2 エクスポートできる汎用データのレイアウトを開示しているか。 3 汎用データのエクスポートの正当性、正確性、完全性を確保する機能があるか。								
3 集計・検索・出力の機能	仕訳データが承認された勘定科目に正確に反映されない。 仕訳データの勘定科目合計に漏れや重複がある。 関連する帳票の整合性が取れない(不完全、不正確)。 仕訳データが検索できない(不完全、不正確)。 仕訳データやログが印字できない。	仕訳データが正当な勘定科目に正確完全に反映され集計される。 必要とされる仕訳データのログは正確で完全に保存され検索可能である。 必要とされる仕訳データやログは印字可能である。	3-1 仕訳データの集計 1 入力された仕訳データをもとに、主要会計帳簿の集計結果を正確に作成することができるか。 2 仕訳データの変更は、主要会計帳簿の集計結果に正しく反映されるか。 3 バッチ更新処理のタイミング等により、仕訳データの追加、訂正が集計結果に反映されないことが無いようにする制御機能があるか。 4 関連する帳票間の整合性を確認するために、合計金額・件数等の情報を表示する機能があるか、もしくは照合した結果を表示する機能があるか。 3-2 仕訳データの検索 1 仕訳データを特定する項目を有しているか。また、その項目は何か。 * 2 伝票番号の入力方法(自動採番、手入力など)は明示されているか。(番号を入力しないことが可能な場合も記載する)。 3 伝票番号の一括付け直し(月別の連番への付け直し等)が可能な場合に元の入力日付等のログは残るか。 4 伝票番号の欠番チェック及び重複チェックできる機能があるか。 5 仕訳データの処理日である入力日が、データ上保持され、必要に応じ表示できるか。 6 以下の項目により、仕訳データを検索する機能があるか。 * ①伝票番号 ②伝票日付 ③入力日付 ④入力者 ⑤承認者 3-3 出力に関する機能 1 出力帳票等に、出力者ID、出力日付(もしくは最終処理日の日付の印字)、出力累計回数等が印字できるか。								
4 繰越処理	正しい期首残高が維持されない。	期首残高について完全性、正確性、正当性を維持することができる。	4 年次及び月次等の繰越処理 1 期首残高を確定しないと、仕訳を入力することができないなど一定の制限する機能があるか。 2 期首残高を修正した場合には、修正の証跡を残すことができるか。 3 確定処理後の残高を修正した場合には、修正の証跡を残すことができるか。								

質問のカテゴリ	想定するリスク	統制目標	質問項目	*は、電子帳簿保存法の要求している要件	いいえ	はい	コメント	メニューによる設定状況			公表場所 (URLなど)
								デフォルト (基本設定)	オプション 選択可能	電子帳簿保存 法対応の場合 のみ	
5 各種法規対応	消費税の入力が不正確、不完全になる。 電子帳簿保存法対応機能が明確で無く設定が不十分でデータの正当性、正確性、完全性が確保されない。	消費税が正当、正確、完全である。 電子帳簿保存法対応の機能が有効に設定され、データの正当性、正確性、完全性が確保される。	5-1 消費税の処理								
			1 仮払消費税、仮受消費税の自動計算による仕訳と手入力による仕訳を区別して表示する機能があるか。 2 自動計算した消費税等の金額を手で訂正した場合、ログを残す機能があるか。								
			5-2 電子帳簿保存法への対応可能性								
			1 電子帳簿保存法への対応を可能とする機能があるか。その場合の対応機能が明示されているか。								
6 パッケージの導入保守	想定外のプログラム、パラメータ、データの追加及び変更がなされる。 アクセス可能なDBMS及びOS環境下にて運用している場合、DBMSに直接アクセスしてプログラム、パラメータ、データの改ざんをされる。	変更が必要な対象項目以外は保護されている。 変更された場合には変更の事実を把握できる。 変更履歴が記録される。 適切なアクセス権限の管理がなされている。	6-1 新規セットアップ								
			6-1-1システム初期設定項目(パラメータ)								
			1 システム管理上の重要な設定項目が変更された場合の変更証跡を残すことができるか。 2 ユーザの希望に応じて初期設定項目そのものを変更することができるか。 3 マスタ・データ(マスタ・ファイル、テーブル)の項目の追加変更の記録が保存され、常時、表示ができるか。 4 特定の項目について変更のタイミングを制御する機能があるか。(例えば導入時や年度の繰越時だけに制限されている等)								
			6-1-2ソースプログラム								
			1 パッケージ導入時のプログラム変更を防止する仕組みはあるか。(ソースコードは開示しないなど。なお開示とは顧客と合意のうえパッケージのコア部分を改変するような場合を想定している。) 2 カスタマイズが行われないよう保護されているか。 3 カスタマイズをしている場合にはカスタマイズしたことを判別できるか。								
			6-1-3DBMS								
			1 管理方法の確立している汎用的なDBMSを使用しているか。 2 DBMSに関するデータインターフェイスの仕様の開示ができるか。 3 パッケージが使用するDBMSのIDはインストール時にパスワードを変更することができるか。 4 パッケージが使用するDBMSのIDは運用時にパスワードを変更することができるか。								
6-1-4OS											
1 会計パッケージの一般ユーザに基盤OSの管理者権限を与えない設定ができるか。 2 パッケージに使用するOSのIDはインストール時にパスワードを変更することができるか。 3 パッケージに使用するOSのIDは運用時にパスワードを変更することができるか。											
6-2 バージョンアップ											
1 バージョンアップ時に、変更される機能は、明示されているか。 2 バージョンアップ時に既存のデータやプログラムに影響がある場合はその影響は明確であるか。 3 バージョンを表示する機能があるか。 3 正常にバージョンアップが終了したことを確認する機能(仕組み)があるか。 4 バージョンアップ失敗時にロールバックできる機能(仕組み)があるか。											

質問のカテゴリ	想定するリスク	統制目標	質問項目	*は、電子帳簿保存法の要求している要件	いいえ	はい	コメント	メニューによる設定状況			公表場所 (URLなど)	
								デフォルト (基本設定)	オプション 選択可能	電子帳簿保存 法対応の場合 のみ		
7 システム運用管理	障害が検知されない。障害に対して誤った対応がなされる。障害対応が放置される。 データ及びログを喪失した際、復元することができない。	障害発生が記録される仕組みがある。 バックアップ及びリカバリーに関するサポート機能がある。	7-1 稼働記録の保持									
			<ol style="list-style-type: none"> 1 障害が発生した場合に適切に記録される仕組みになっているか。 2 システムの稼働記録(ログ)を保持し、必要に応じて表示する機能があるか。 3 システムの稼働記録(ログ)の変更は、改ざんできないように保護されているか。 									
			7-2 データファイルの保全									
			<ol style="list-style-type: none"> 1 会計データの自動バックアップの機能があるか。 2 バックアップファイルを使用したデータのリカバリー機能があるか。 									
8 アクセス管理等	職務権限と大幅に乖離した権限の付与がなされる。 管理者権限の不正利用がなされる。	ユーザID及び権限付与状況の一覧情報が出力される。 システム管理者と一般ユーザを区分することができる。 システム利用者の職務権限とアクセス権限を一致させ特定することができる。 特定ユーザのログを収集することができる。	8-1 システムに対するアクセス制限									
			8-1-1ログイン方法									
			<ol style="list-style-type: none"> 1 ユーザIDとパスワードによりログインできる者を制限する機能があるか。 2 パスワードの桁数制限や、アカウントロック機能があるか。 									
			8-1-2制御方法									
			<ol style="list-style-type: none"> 1 システム管理上の重要な設定項目(ユーザIDの改廃、権限の付与、等)のアクセス権を特定の管理責任者に限定する機能があるか。 2 一般ユーザとシステム管理者の権限を区別して管理する機能があるか。 3 メニューによる機能単位や、勘定科目単位に制限する機能があるか。 4 一定の権限を束ねた権限グループを設定する機能があるか。 									
			8-2 ユーザIDの管理に資する機能									
			<ol style="list-style-type: none"> 1 ユーザIDの一覧を出力する機能があるか。 2 ユーザID一覧とあわせて最終更新日付を入手する機能があるか。 3 ユーザIDの追加、変更、削除の履歴を入手する機能があるか。 4 すべてのIDのパスワードの変更状況を管理する機能があるか。 5 異動や退職に応じて、期中でユーザの削除、新規登録、権限を変更する機能があるか。 									
			8-3 ログ収集の可否									
			<ol style="list-style-type: none"> 1 ユーザ(特権ユーザ、一般ユーザ)のログインログを把握する機能があるか。 2 ユーザ(特権ユーザ、一般ユーザ)の実行ログを把握する機能があるか。 									
			8-4 権限設定の制限など									
			<ol style="list-style-type: none"> 1 兼務すべきでない権限の組み合わせ等(承認者と申請者が同一の場合等)を制限する機能があるか。 2 代理承認等(承認者不在時の対応)の機能はあるか。 3 ある場合には代理承認等であることを確認することができるか。 									

付録 8. IT 統制のための財務会計パッケージソフトウェア向け プロテクション・プロファイル (シナリオ例)

はじめに

1. 本プロテクション・プロファイル(シナリオ例)の位置づけ

十分なセキュリティが要求される IT 製品・システムのセキュリティ機能を評価する基準として、国際規格である ISO/IEC 15408 が制定されており、これらの規格に基づく我が国のセキュリティ評価・認証制度が運用されている。IT 製品・システムを開発する上で、必要十分なセキュリティ機能が備えられることを保証する最初のステップとして、プロテクション・プロファイル(以下、PP という)の開発は効果的である。更に、適切な PP を使用すれば、調達者はセキュリティの基本ニーズを正確に開発者に提示することが可能になり、かつ、開発者は、調達者の要求を満たすセキュリティターゲットの作成が容易になることから、本追補版を利用して会計パッケージソフトウェアが具備すべき機能を例示するための PP を検討した結果をシナリオ例として示す。

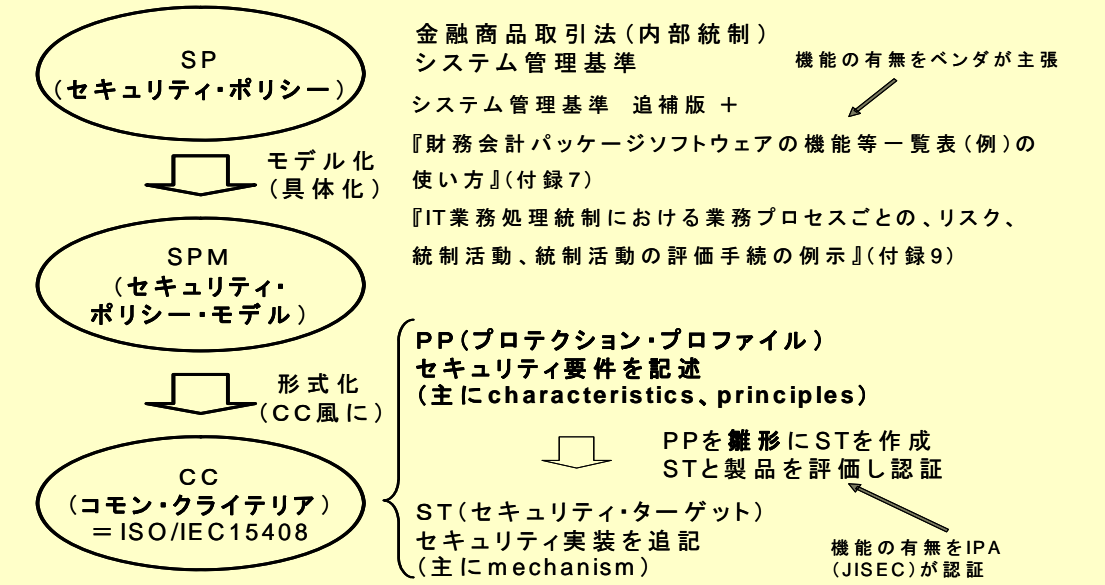
なお、本付録は会計パッケージベンダが PP を作成する際の考え方を例示したものであり、国際規格である ISO/IEC 15408 等に基づき PP として評価・認証されたものではないことに留意する。実際に PP を作成する際には、「IT セキュリティ認証及び認証制度」の評価基準「情報技術セキュリティ評価のためのコモンクライテリア バージョン 3.1」(CC V3.1)及び評価方法である「情報技術セキュリティ評価のための共通方法 バージョン 3.1」(CEM V3.1)を用いて、PP モデルの内容の妥当性について検討する必要がある。

また、会計パッケージが IT セキュリティ認証を取得していれば、各機能の有無を客観的に確認することが可能になり、IT 統制を評価する上での参考となると考えられるが、IT セキュリティ認証がそのまま IT 統制の有効性を証明するものではないことに留意する必要がある。

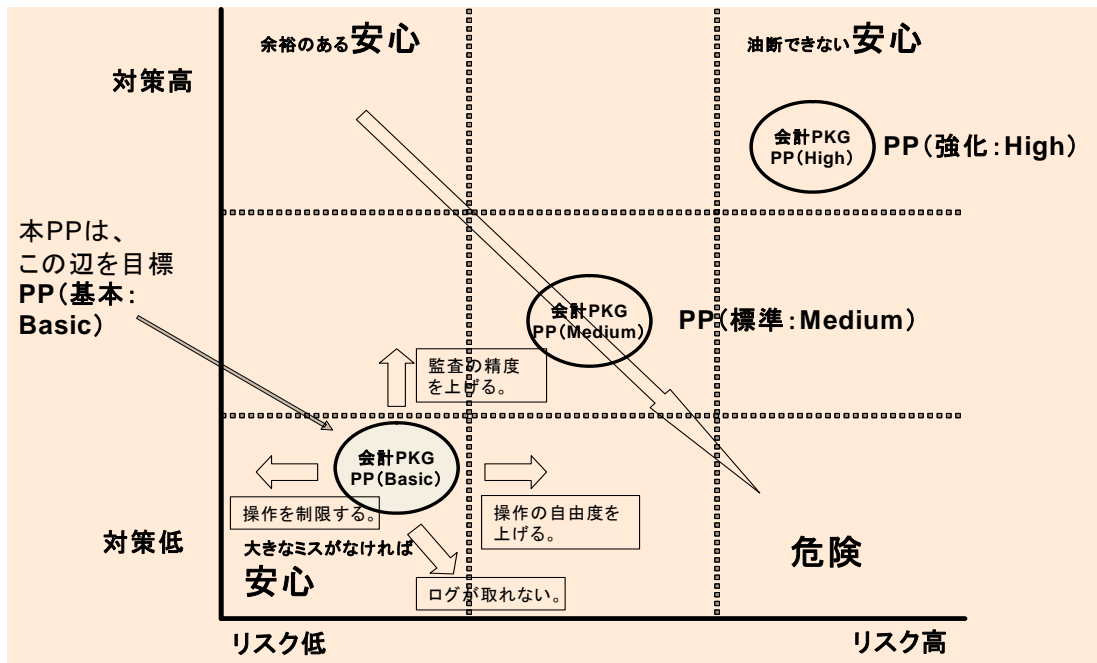
本PPの具体的な位置づけについて、付録図表8-1、及び付録図表8-2に示す。

付録図表 8-1 本PPの作成作業位置付け

PP作成作業の位置付け(セキュリティの言葉にすると)



付録図表 8-2 本PPの位置付け(リスクと対策の関係)



2. 本 PP の方針

本 PP は、システム管理基準追補版を利用する場合に、会計パッケージが具備すべき機能を例示したものである。主に会計パッケージベンダ向けの参考資料であり、システム管理基準追補版本編及び付録と整合を取るよう配慮している。

本 PP は、比較的リスクの低い、制限された環境で、市販会計パッケージが利用されることを想定している。(PP:基本(Basic))外部システム(販売パッケージなど)との連携に関する対策や、外部ネットワークからの攻撃、ウイルス対策などは、実施済みであることを前提とする。会計パッケージベンダが、より高いレベルの対策を、パッケージに組み込み CC 認証取得(ST:標準(Medium)、強化(High))を目指すことも考えられる。

3. 本 PP の概要

(1) 評価対象

a. 対象システム

市販の会計パッケージとする。前提として、他のパッケージソフトウェアとの連携や外部ネットワークの対策は実施済みとする。

b. 運用組織

様々な業種の上場会社(最低限の職務分離は必要。)

(2) 関係者

- ・経営者、会計責任者、会計担当者、他の従業員(外部の者は除外)
- ・攻撃者は、社内の会計担当者、他の従業員
- ・攻撃者のITスキルレベルは低い。(会計パッケージのモジュールを置き換えできない。会計パッケージ機能を使わずに、DB、ファイルを更新できない。など)
- ・経営者は信頼できる、トラスト・アンカー。
- ・会計責任者は、会計専門家。不正やミスの可能性が低い。

(3) 保護資産

財務報告に係る会計データ。マスタ(勘定科目マスタなど)、トランザクション(仕訳データなど)

(4) 想定脅威(リスク)

財務報告に係る社員の不正やミス(会計データの正当性、正確性、完全性が損なわれる事象)情報漏えいなどの対策は、実施済みとする。

(5) 対策(コントロール)

a.事前対策(予防的)

- ・識別と認証(会計担当以外の従業員の不正対策)

会計担当者以外の従業員による会計パッケージの使用を識別と認証機能によって拒否する。

b.事後対策(発見的)

- ・ログと監査(会計担当者の不正、ミス対策)

会計担当者の不正やミスに対して、会計データの入力や認証の試行など操作履歴(ログ)を採取し、会計責任者がログを検査し、不正やミスを検出して、適切な対策を講ずる。

c.対策補強

- ・確定後のデータロック(監査の負荷軽減、ミス防止)

確定後のデータを会計担当者は操作できないように、ロックし会計責任者の監査範囲を限定し、負荷を軽減する。

4. その他

(1)本 PP のバージョン

ISO/IEC 15408 の規格のバージョンについては、現在、V2.3、V3.1 がともに利用にされているが、2008 年 4 月から V3.1 のみとなる。本付録は、V2.3 ベースで作成している。

(2)米国政府 PP 作成ガイド(参考)

- Development Process For US Government Protection Profiles (PP)

http://www.niap-ccevs.org/pp/pp_dev_process.pdf

- Consistency Instruction Manual

For development of US Government Protection Profiles

http://www.niap-ccevs.org/pp/basic_rob_manual-3.0.pdf

**IT統制のための財務会計パッケージソフトウェア向け
プロテクション・プロファイル（シナリオ例）**

目 次

1. プロテクション・プロファイル（PP）概説	6
1.1. PP識別	6
1.2. PP概要	6
1.3. CC適合	7
1.4. 略語・用語	7
2. TOE記述	9
2.1. TOEの種別	9
2.2. TOEの利用	9
2.3. TOEの構成	10
2.4. 関係者と役割	12
2.5. 保護資産	13
2.6. TOEの機能	15
2.7. TOEのセキュリティ機能	16
2.8. TOEのセキュリティ機能以外の機能	16
3. TOEセキュリティ環境	17
3.1. 前提条件	17
3.2. 脅威	17
3.3. 組織のセキュリティ方針	19
4. セキュリティ対策方針	20
4.1. TOEのセキュリティ対策方針	20
4.2. 環境のセキュリティ対策方針	21
5. ITセキュリティ要件	23
5.1. TOEセキュリティ要件	23
6. 根拠	29
6.1. セキュリティ対策方針根拠	29
6.2. セキュリティ要件根拠	31

1. プロテクション・プロファイル (PP) 概説

1.1. PP 識別

PP 名称	:IT統制のための財務会計パッケージソフトウェア向けプロテクション・プロファイル
PP バージョン	:0.3
作成日	:2007/12/26
作成者	:財務報告に係るIT統制研究会
TOE 名称	:財務会計パッケージ
TOE バージョン	:1.0
評価保証レベル	:EAL1
キーワード	:財務会計パッケージ
CC バージョン	:Common Criteria for Information Technology Security Evaluation,Ver.2.3 CCIMB Interpretations-0512

なお、日本語訳は独立行政法人情報処理推進機構 (IPA) セキュリティセンター発行の以下のものを使用している。

平成 17 年 12 月翻訳第 1.0 版、補足-0512 適用

1.2. PP 概要

本 PP は、一般企業で利用される市販の財務会計パッケージソフトウェア (以下、会計パッケージという) のプロテクション・プロファイルを記述している。

企業の業種・業態は多様であり、「内部統制」と言っても紙情報を原本とするマニュアル統制や電子情報を原本とするシステム統制、またそれらを折衷した統制など、多様な統制を想定しなくてはならない。

更に、企業の規模によっては、一人の従業員がいくつもの仕事を掛け持ちせねばならず、職務の分離など人を中心とした「内部統制」による会計データの信頼性よりは、専ら従業員の間の信頼性を基礎とした暗黙の統制により成り立っていると考えられる。

しかし、その様な状況でも、今日的にはコンピュータシステムを利用しない会計処理は考えられず、多くは市販の会計パッケージに依存している。そのことは、会計パッケージが受け持つ業務範囲で、効果的な統制を行っていることを説明できれば、利用する企業にとってはメ

リットが大きい。そこで、市販会計パッケージなどに、誤謬や不正、または誤入力や改ざん防止または発見できる仕組みをできるだけ取り込むことで、会計データの信頼性を確保し、「内部統制」の一部を説明出来ることが有効である。

本PPは、会計パッケージが、具備していることを期待される「内部統制」に関する上記のようなセキュリティ要件を整理したものである。

なお、ここでは、会計パッケージの標準機能のみを使った運用を想定しており、追加機能の開発やアドオン機能の付加などは考慮されていない。また、販売管理パッケージなど他システムとの連携によるリスクや、外部ネットワークを利用する際の脅威については、すでに対策済みであることを前提として記述している。

1.3. CC 適合

本 TOE は、以下の情報セキュリティ基準に適合する。

機能要件は、Part2 適合である。

保証要件は、Part3 適合である。

評価保証レベルは、EAL1 適合である。

1.4. 略語・用語

<本PPにおける用語>

会計システム: サーバやクライアント PC などのハードウェア、OS や DBMS、市販会計パッケージなどのソフトウェアから構成されるシステム。

市販会計パッケージ: TOE であり、財務会計処理を電子的に行うソフトウェア。

<CC 関連略語>

CC(Common Criteria): コモンクライテリア

EAL(Evaluation Assurance Level): 評価保証レベル

IT(Information Technology): 情報技術

PP(Protection Profile): プロテクション・プロファイル

SF(Security Function): セキュリティ機能

SFP(Security Function Policy): セキュリティ機能ポリシー

SOF(Strength Of Function): 機能強度

ST (Security Target) : セキュリティターゲット

TOE (Target Of Evaluation) : 評価対象

TSF (TOE Security Functions) : TOE セキュリティ機能

TSC (TSF Scope of Control) : TSF 制御範囲

SFR (Security Functional Requirements) : セキュリティ機能要件

TSP (TOE Security Policy) : TOE セキュリティポリシー

2. TOE 記述

本章では、TOE の種別、TOE の利用、TOE の構成、関係者、保護資産、TOE の機能を記述する。

2.1. TOE の種別

TOE である市販会計パッケージは、一般企業において財務会計処理を電子的に行なうソフトウェア製品である。

2.2. TOE の利用

本節では、TOE の利用目的、利用環境、利用方法を記述する。

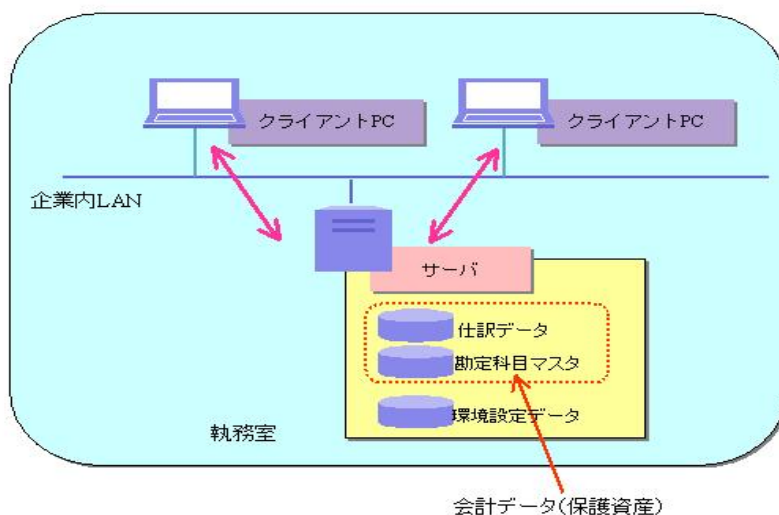
2.2.1. 利用目的

本 TOE(市販会計パッケージ、以下同様)を利用することにより、企業の会計担当者が、仕訳伝票の作成や勘定科目マスタの更新、財務報告書の作成を、仕訳データと勘定科目マスタの正確性、正当性、完全性を確保しつつ、効率的に処理することを目的とする。

2.2.2. 利用環境

会計システムの利用環境、利用方法は、それぞれの企業により様々であり、TOE である市販会計パッケージが想定する利用環境、利用方法もひとつに固定することはできない。

ここでは、TOE を含む会計システムの利用環境の一例を付録図表 2-2-2 に示す。



付録図表 2-2-2 会計システムの利用環境の一例

この例では、会計システムは、サーバ、クライアント PC、企業内 LAN から構成され、サーバとクライアント PC は、企業内 LAN で接続される。サーバ、クライアント PC は、会計担当者が作業を行う執務室に設置される。執務室では、会計担当者と入室を許可された従業員が作業を行う。

2.2.3. 利用方法

ここでは、会計システムの利用方法の一例を示す。

- ①会計担当者は、クライアント PC を使用してサーバにアクセスし、TOE を利用して識別と認証に成功すると、仕訳データの作成や勘定科目マスタの更新、財務報告書の作成を行なうことができる。
- ②TOE は、作成された会計データをサーバに格納する。
- ③会計責任者は、会計担当者の入力したデータの正確性、正当性、完全性を確認する。誤りがある場合には、会計担当者に修正を指示し、問題がなければ承認する。
会計責任者は、会計担当者による一定時期(日次、月次、年度)以前の会計データの更新を禁止するために、TOE を利用して、その期間の会計データをロックすることができる。
- ④TOE は、会計責任者により承認された会計データを、サーバに保持する。
- ⑤会計責任者は、クライアント PC を使用してサーバにアクセスし、TOE を利用して識別と認証に成功すると、会計担当者の識別認証情報を登録、変更、削除することができる。

なお、会計責任者は、会計担当者の識別認証情報を登録の際に、利用者 ID、パスワード、グループ ID(会計担当者としての役割)を決定して、利用者 ID とパスワードを会計担当者に提供する。パスワードは推測が困難なものを設定する。

2.3. TOE の構成

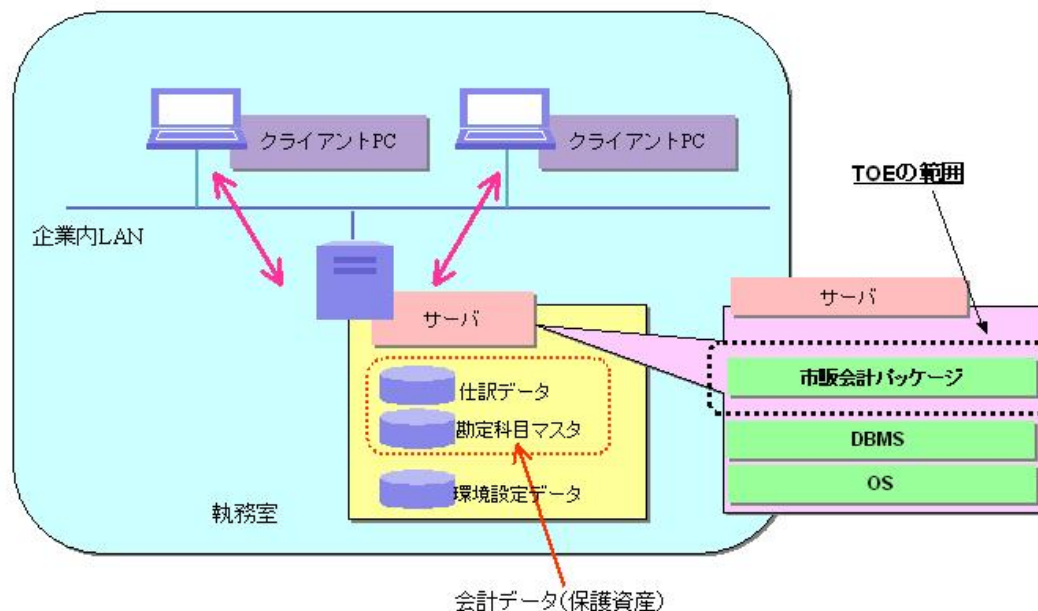
本節では、TOE を含む会計システムのシステム構成を記述する。

2.3.1. システム構成

以下に、TOE を含む会計システムのシステム構成の一例を付録図表 2-3-1 に示す。

この例では、TOE である市販会計パッケージや、保護資産である会計データ、環境設定データなどがサーバに設定されている構成としているが、これらがクライアント PC に設定される例もあ

る。



付録図表 2-3-1 会計システムのシステム構成の一例

(1) ハードウェア構成と概要

①クライアント PC :

会計責任者および会計担当者が TOE にアクセスするのに用いるパソコン。

②サーバ:

会計データ、環境設定データが格納されているサーバ。この例では、TOE が搭載され、会計業務ロジックが動作する。

③企業内 LAN:

企業内に敷設されたローカル・エリア・ネットワーク。クライアント PC、サーバが接続される。

(2) ソフトウェア構成と概要

①市販会計パッケージ:

この例では、サーバ上で稼動し、クライアント PC からの要求に対して、仕訳データの登録や勘定科目マスタの更新、財務報告書の作成などのサービスを提供するソフトウェアであり、本システムの TOE である。

②DBMS :

サーバ上で稼動し、会計データを格納するデータベース管理ソフトウェア。

③OS :

サーバ上で稼動するオペレーティングシステム。

2.4. 関係者と役割

本 PP における関係者は、経営者、会計責任者、会計担当者、非許可従業員である。

企業の規模によっては、一人の従業員がいくつもの仕事を掛け持ちせねばならず、職務の分離など人を中心とした「内部統制」が難しいことがあるため、必要最低限の職務の分離として、会計処理上の職務を、操作を行なう会計担当者と、それを管理監督する会計責任者の二分割するに止めた。

会計処理上の不正、誤謬を抑止、防止、検出するために、人的な信頼の拠り所(信頼点: trust anchor)を必要とするが、本 PP においては、経営者を人的な信頼点とする。

不正に加担する経営者などを想定するならば、人的な信頼点を組織外部の会計監査者などに求めることも考えられるが、本 PP の範囲を超える。

(1) 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制を整備及び運用する役割と責任がある。

会計処理について、信頼できる会計責任者を任命し、権限を委任することができる。

会計処理を含め、経営上の意図的な不正は行わないものとする。

(2) 会計責任者

会計担当者への指示や統制を実施する責任を持つ。

会計担当者が、市販会計パッケージを操作、処理した内容を確認して承認を行う。承認の操作を行うことがない場合でも、会計処理上の責任を負う。

財務会計の専門家で、会計処理上の誤りを犯す可能性は低い。

経営者の方針に従って会計処理を行い、意図的な不正処理は行わないものとする。

(3) 会計担当者

会計責任者より、財務情報を扱う権限を付与された者。

会計責任者の方針、指示に従って、市販会計パッケージを操作することを許可されている従

業員。

会計処理上の意図的な不正操作を行うことがあるかもしれない。

不正操作は、市販会計パッケージの標準機能で実行できる範囲で、高度な IT スキルは持ち合わせていないものとする。

(4) 非許可従業員

市販会計パッケージの操作を許可されていない従業員。

会計処理上の意図的な不正操作を行うことがあるかもしれない。

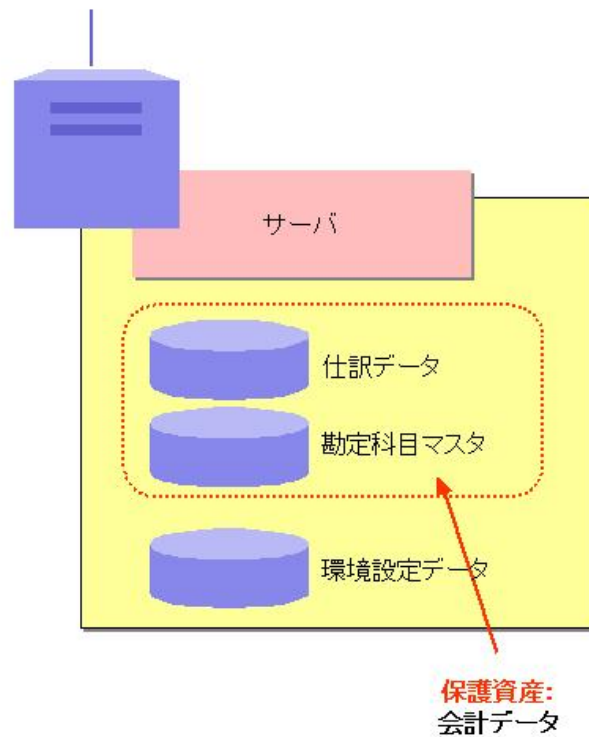
不正操作は、会計パッケージの標準機能で実行できる範囲で、高度な IT スキルは持ち合わせていないものとする。

なお、本 PP における会計システムは、外部システム(販売パッケージなど)との連携に関する対策や、外部ネットワークからの攻撃に対する対策、ウイルス対策などは、実施済みであることを前提としているので、脅威エージェントは、会計担当者と非許可従業員である。両者は、IT 技術について高度な専門知識を保持しておらず、低レベルの攻撃しか行わないものとする。

2.5. 保護資産

以下に、TOE の保護資産の一例を図 2-5 に示す。

この例では、保護資産である会計データや環境設定データなどがサーバに設定されている構成としているが、これらがクライアント PC に格納される例もある。



付録図表 2-5 TOE の保護資産の一例

この例では、サーバ上の財務報告に係る会計データを保護資産(一次資産)として管理する。会計データは、トランザクションデータである仕訳データと、マスタ・ファイルである勘定科目マスタから成る。

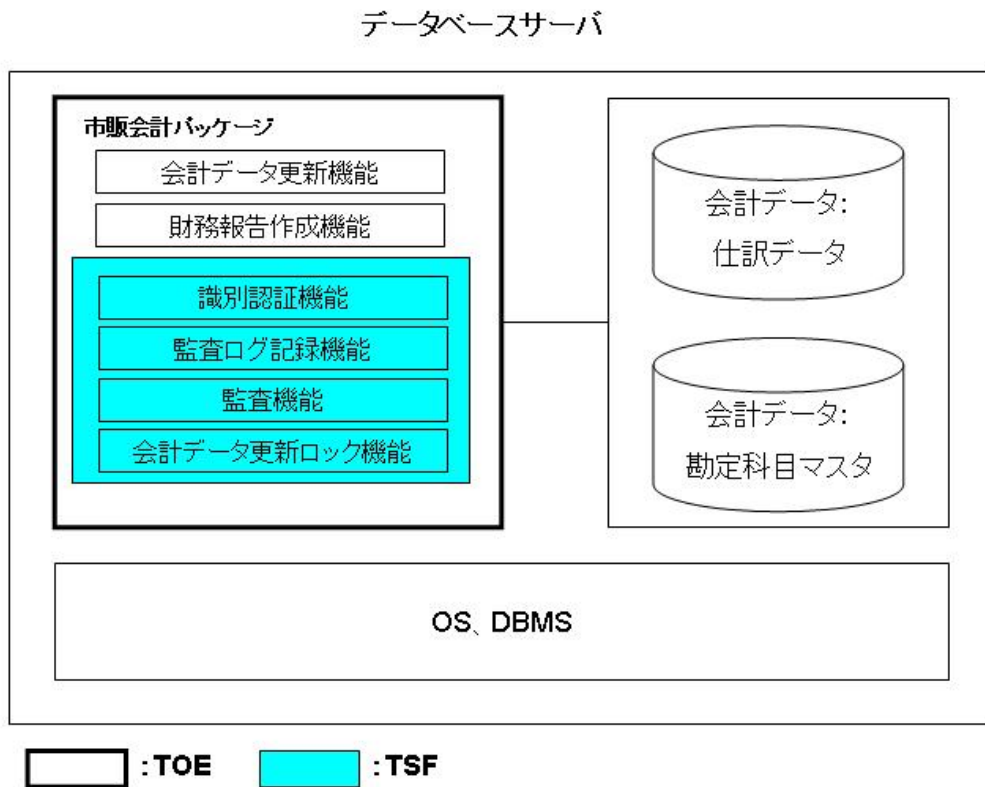
なお、環境設定データには、保護資産を守るために必要な識別と認証情報や、会計データの更新を禁止するロック情報などが格納される。このため、環境設定データも、二次資産として保護される必要がある。

2.6. TOE の機能

TOE は、「市販会計パッケージ」であり、「標準的な会計処理機能」と「識別と認証機能」「監査ログ記録機能」「監査機能」「会計データ更新ロック機能」などの内部統制に必要な機能を提供することが想定される。この例では、TSF は「識別と認証機能」「監査ログ記録機能」「監査機能」「会計データ更新ロック機能」としている。

TOE の機能構成イメージの一例を付録図表 2-6 に示す。

この例では、TOE である市販会計パッケージが、サーバに設定されている構成としているが、これらがクライアント PC に設定される例もある。



付録図表 2-6 TOE の機能構成の一例

2.7. TOE のセキュリティ機能

TOE が提供する内部統制のためのセキュリティ機能の一例を示す。

(1) 識別と認証機能

利用者 ID、パスワードを使用して、TOE へのアクセスの許可／非許可を判断する機能。パスワード入力時には、パスワードの漏えいのリスクを低減させるために利用者が入力した文字数分の「*」のみを表示する。

(2) 監査ログ記録機能

会計担当者による勘定科目マスタ、仕訳データの入力、修正、削除された履歴や、識別と認証試行の失敗、識別と認証情報の登録、修正、削除などの履歴を、日付・時刻、操作プログラム、操作者などと伴に記録する。

(3) 監査機能

会計責任者が、採取された監査ログをレビューする際に、特定の監査ログを検索したり、解釈しやすい形式で表示する機能。

(4) 会計データ更新ロック機能

会計責任者が、会計担当者による一定時期(日次、月次、年度)以前の会計データの更新を禁止するために、その期間の会計データをロックする機能。

2.8. TOE のセキュリティ機能以外の機能

(1) 市販会計パッケージが提供する標準的な会計処理機能である。

3. TOE セキュリティ環境

本章では、前提条件、脅威、組織のセキュリティ方針について述べる。

3.1. 前提条件

本 PP は、内部統制のために、市販会計パッケージに必要なセキュリティ要件を整理したものであるため、明示しないが、他システムとの連携によるリスクや、外部ネットワークを利用する際の脅威については、すでに対策済みであることを前提とする。

A. 会計データのバックアップ

ハードウェア故障やソフトウェア障害により会計データが破壊された時に備えて、会計データのバックアップを実施する。

A. バックアップ媒体の保護

会計データのバックアップ媒体上の情報が改ざんされることがないものとする。

A. 正確な日付設定

会計システムを構成するサーバには、正確な日付が設定されるものとする。

A. パスワードの設定

会計責任者および会計担当者を TOE 利用者として認証するためのパスワードは、推測が困難なものを設定する。また、同一のパスワードを長期間継続して使用しない。

A. 会計責任者の信頼

会計責任者は、会計システムを不正に使用することはないものとする。

3.2. 脅威

想定する脅威は、付録9. IT 統制目標とアサーションの関係の考え方(1)②個別決算プロセスにおけるリスクから抽出する。

< マスタ登録 >

T.勘定科目マスタの不正登録

会計担当者および非許可従業員が、会計責任者により承認されていない勘定科目マスタを、不正に登録するかもしれない。また、既存の勘定科目マスタを、不正に修正、削除するかもしれない。

－承認されていない、会計方針と異なるマスタ登録が行われる。

T.勘定科目マスタの登録誤り

会計担当者が、勘定科目マスタを、誤って登録、修正、削除するかもしれない。

－マスタの二重登録や不足がある。

－マスタ登録に誤りがある。

－マスタが最新でなく、継続使用できない。

<集計>

T.財務情報の未集計

会計担当者が、財務情報の集計操作を誤って、不正確に財務情報を集計するかもしれない。

－一部の手で計算している処理を飛ばしてしまう。

<修正仕訳>

T.仕訳データの不正入力

会計担当者および非許可従業員が、会計責任者に承認されていない不正な仕訳データを入力するかもしれない。また、既存の仕訳データを、不正に修正、削除するかもしれない。

－不正な仕訳入力がある。

T.仕訳データの入力誤り

会計担当者が、仕訳データを、誤って入力、修正、削除するかもしれない。

－修正仕訳の二重入力、入力漏れが発生する。

－誤った修正仕訳が入力される。

－修正仕訳ファイルに権限者以外が不正な入力をする。

<報告>

T.財務報告書の不正作成

会計担当者および非許可従業員が、会計責任者に承認されていない財務報告書を不正に作成するかもしれない。

T.財務報告書の作成誤り

会計担当者が、財務報告書の作成操作を誤って、不正確な財務報告書を作成するかもしれない。

3.3. 組織のセキュリティ方針

組織のセキュリティ方針は想定しない。

4. セキュリティ対策方針

本章では、TOE のセキュリティ対策方針、及び環境のセキュリティ対策方針について述べる。

4.1. TOE のセキュリティ対策方針

TOE のセキュリティ対策方針は以下の通りである。

○.利用者の識別と認証

TOE は、識別と認証に成功した利用者だけに、TOE の操作を許可しなければならない。

○.プルーフリスト

TOE は、入力、修正、削除された勘定科目マスタ、仕訳データのプルーフリストを出力しなければならない。

なお、プルーフリストは、TOE の標準機能で修正、削除できないこと。

プルーフリストは、会計責任者が、会計処理上の不正や誤謬を判別しやすい形式で出力すること。

- － 貸借のバランスのチェック機能
- － 日付・時刻、操作プログラム、操作者、勘定科目などによる検索機能

○.監査証跡

TOE は、不正や誤謬に関連する可能性がある特定の事象が発生した場合、これを監査証跡として保管しなければならない。

なお、監査証跡には、事象の日付・時刻、事象の操作プログラム、操作者、事象の内容を含めて生成すること。

監査証跡は、TOE の標準機能で修正、削除できないこと。

監査証跡は、会計責任者が、会計処理上の不正や誤謬を判別しやすい形式に検索、編集できること。

特定の事象とは、識別と認証情報の登録、修正、削除や、償却方法の変更など環境設定データの修正を含む。

○.会計データ更新ロック

TOEは、会計責任者により承認された会計データを、それ以降、入力、更新、削除を禁止する機能を提供しなければならない。

－更新ロック処理後の伝票訂正は、赤黒伝票での処理になる。

4.2. 環境のセキュリティ対策方針

4.2.1. 非IT的環境のセキュリティ対策方針

非IT環境のセキュリティ対策方針は以下の通りである。

OE. プルーフリスト確認

会計責任者は、会計担当者が入力、修正、削除した勘定科目マスタ、仕訳データのプルーフリストを出力し、内容の正確性、正当性、完全性を確認しなければならない。また、確認の結果を記録し保管しなければならない。

OE. 監査証拠確認

会計責任者は、会計上の不正や誤謬が発生していないか、定期的に監査証拠を確認しなければならない。

OE. 定期的なバックアップ

会計責任者は、定期的に会計データのバックアップを取らなければならない。

OE. バックアップ媒体の管理

会計責任者は、バックアップ媒体を施錠できる場所に保管し管理しなければならない。

OE. 正確な日付設定

会計責任者は、会計システムを構成するサーバに正確な日付が設定されるように管理しなければならない。

OE. パスワードの設定

会計責任者および会計担当者は、TOE利用者として認証するためのパスワードを、利用者ID

や生年月日、氏名など容易に推測できるものを避けて設定しなければならない。また、パスワードは定期的に変更しなければならない。

OE.会計責任者の信頼

経営者は、会計責任者に信頼できる者を選任し、管理、指導しなければならない。

5. IT セキュリティ要件

本章では、TOE セキュリティ要件、及び IT 環境に対するセキュリティ要件について述べる。

5.1. TOE セキュリティ要件

本節では、TOE セキュリティ要件として、TOE セキュリティ機能要件、及び TOE セキュリティ保証要件について述べる。

5.1.1. TOE セキュリティ機能要件

TOE セキュリティ機能要件は以下の通りである。

◆セキュリティ監査 (FAU)

FAU_GEN.1 監査データ生成

下位階層: なし

FAU_GEN.1.1 TSF は、以下の監査対象事象の監査記録を生成できなければならない:

- a) 監査機能の起動と終了;
- b) 監査の[選択:最小、基本、詳細、指定なし:から一つのみ選択]レベルのすべての監査対象事象;及び
- c) [割付:上記以外の個別に定義した監査対象事象]。

FAU_GEN.1.2 TSF は、各監査記録において少なくとも以下の情報を記録しなければならない:

- a) 事象の日付・時刻、事象の種別、サブジェクト識別情報、事象の結果(成功または失敗);及び
- b) 各監査事象の種別に対して、PP/ST の機能コンポーネントの監査対象事象の定義に基づいた、[割付:その他の監査関連情報]

依存性: FPT_STM.1 高信頼タイムスタンプ

FAU_SAR.1 監査レビュー

下位階層: なし

FAU_SAR.1.1 TSF は、[割付:許可利用者]が、[割付:監査情報のリスト]を監査記録から読み出せるようにしなければならない。

[割付:許可利用者]:会計責任者

[割付:監査情報のリスト]:

{事象の日付・時刻、事象の操作プログラム、操作者、事象の内容、事象の結果(成功または失敗)、}

FAU_SAR.1.2 TSF は、利用者に対し、その情報を解釈するのに適した形式で監査記録を提供しなければならない。

依存性: FAU_GEN.1 監査データ生成

FAU_STG.1 保護された監査証跡格納

下位階層: なし

FAU_STG.1.1 TSF は、格納された監査記録を不正な削除から保護しなければならない。

FAU_STG.1.2 TSF は、監査証跡内の監査記録への不正な改変を[選択:防止、検出:から一つのみ選択]できねばならない。

[選択:防止、検出:から一つのみ選択]:防止

依存性: FAU_GEN.1 監査データ生成

◆識別と認証(FAU)

FIA_AFL.1 認証失敗時の取り扱い

下位階層: なし

FIA_AFL.1.1 TSF は、[割付:認証事象のリスト]に関して、[選択:[割付:正の整数値], [割付:許容可能な値の範囲]内における管理者設定可能な正の整数値]]回の不成功認証試行が生じたときを検出しなければならない。

FIA_AFL.1.2 不成功の認証試行が定義した回数に達するか上回ったとき、TSF は、[割付:アクションのリスト]をしなければならない。

依存性: FIA_UAU.1 認証のタイミング

FIA_ATD.1 利用者属性定義

下位階層: なし

FIA_ATD.1.1 TSF は、個々の利用者に属する以下のセキュリティ属性のリスト[割付:セキュリティ属性のリスト]を維持しなければならない。

[割付: セキュリティ属性のリスト]

・グループ ID(会計責任者 GID、会計担当者 GID)

依存性: なし

FIA_SOS.1 秘密の検証

下位階層: なし

FIA_SOS.1.1 TSF は、秘密が[割付: 定義された品質尺度]に合致することを検証するメカニズムを提供しなければならない。

依存性: なし

FIA_UAU.2 アクション前の利用者認証

下位階層: FIA_UAU.1

FIA_UAU.2.1 TSF は、その利用者を代行する他の TSF 調停アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。

依存性: FIA_UID.1 識別のタイミング

FIA_UAU.7 保護された認証フィードバック

下位階層: なし

FIA_UAU.7.1 TSF は、認証を行っている間、[割付: フィードバックのリスト]だけを利用者に提供しなければならない。

[割付: フィードバックのリスト]

・入力されたパスワードの文字数分の「*」

依存性: FIA_UAU.1 認証のタイミング

FIA_UID.2 アクション前の利用者識別

下位階層: FIA_UID.1

FIA_UID.2.1 TSF は、その利用者を代行する他の TSF 調停アクションを許可する前に、各利用者に自分自身を識別することを要求しなければならない。

依存性: なし

◆セキュリティ管理(FMT)

FMT_MTD.1(1) TSF データの管理

下位階層: なし

FMT_MTD.1.1 TSF は、[割付: TSF データのリスト]を[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]する能力を[割付: 許可された識別された役割]に制限しなければならない。

[割付: TSF データのリスト]

- ・識別認証情報(利用者 ID、パスワード、グループ ID)
- ・会計データ更新ロックフラグ

[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]

- ・問い合わせ、改変、削除、[割付: その他の操作]

[割付: その他の操作]

- ・登録

[割付: 許可された識別された役割]

- ・会計責任者

依存性: FMT_SMF.1 管理機能の特定

FMT_SMR.1 セキュリティ役割

FMT_MTD.1(2) TSF データの管理

下位階層: なし

FMT_MTD.1.1 TSF は、[割付: TSF データのリスト]を[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]する能力を[割付: 許可された識別された役割]に制限しなければならない。

[割付: TSF データのリスト]

- ・利用者本人のパスワード

[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]

- ・改変

[割付: 許可された識別された役割]

- ・会計担当者

依存性: FMT_SMF.1 管理機能の特定

FMT_SMR.1 セキュリティ役割

FMT_SMF.1(1) 管理機能の特定

下位階層: なし

FMT_SMF.1.1 TSF は、以下のセキュリティ管理機能を行う能力を持たねばならない:[割付: TSF によって提供されるセキュリティ管理機能のリスト]。

[割付:TSF によって提供されるセキュリティ管理機能のリスト]

- ・識別認証情報管理機能
- ・会計データ更新ロック機能

依存性: なし

FMT_SMF.1(2) 管理機能の特定

下位階層: なし

FMT_SMF.1.1 TSF は、以下のセキュリティ管理機能を行う能力を持たねばならない:[割付: TSF によって提供されるセキュリティ管理機能のリスト]。

[割付:TSF によって提供されるセキュリティ管理機能のリスト]

- ・本人パスワード変更機能

依存性: なし

FMT_SMR.1 セキュリティ役割

下位階層: なし

FMT_SMR.1.1 TSF は、役割[割付: 許可された識別された役割]を維持しなければならない。

[割付: 許可された識別された役割]

- ・会計責任者
- ・会計担当者

FMT_SMR.1.2 TSF は、利用者を役割に関連づけなければならない。

依存性: FIA_UID.1 識別のタイミング

◆TSF の保護(FPT)

FPT_RVM.1 TSP の非バイパス性

下位階層: なし

FPT_RVM.1.1 TSF は、TSC 内の各機能の動作進行が許可される前に、TSP 実施機能が呼び出され成功することを保証しなければならない。

依存性: なし

FPT_STM.1 高信頼タイムスタンプ

下位階層: なし

FPT_STM.1.1 TSF は、それ自身の使用のために、高信頼タイムスタンプを提供できなければならない。

依存性: なし

5.1.2. TOE セキュリティ保証要件

本 TOE の評価保証レベルは、EAL1であり、TOE セキュリティ保証要件は以下の通りである。

- ACM_CAP.1 バージョン番号
- ADO_IGS.1 設置、生成、及び立上げ手順
- ADV_FSP.1 非形式的機能仕様
- ADV_RCR.1 非形式的対応の実証
- AGD_ADM.1 管理者ガイダンス
- AGD_USR.1 利用者ガイダンス
- ATE_IND.1 独立テスト準拠

6. 根拠

本章では、セキュリティ対策方針根拠、セキュリティ要件根拠について述べる。

6.1. セキュリティ対策方針根拠

本節では、セキュリティ対策方針の必要性、及びセキュリティ対策方針の十分性について述べる。

6.1.1. セキュリティ対策方針の必要性

セキュリティ対策方針と TOE セキュリティ環境との対応を以下の「付録図表 8-1-1」に示す。

付録図表 8-1-1 TOE セキュリティ環境とセキュリティ対策方針

	△会計データのバックアップ	△バックアップ媒体の保護	△正確な日付設定	△パスワードの設定	△会計責任者の信頼	□勘定科目マスタの不正登録	□勘定科目マスタの登録誤り	□財務情報の未集計	□仕訳データの不正入力	□仕訳データの入力誤り	□財務報告書の不正作成	□財務報告書の作成誤り
○.利用者の識別と認証						○			○		○	
○.プルーフリスト						○	○	○	○	○	○	○
○.監査証跡						○			○		○	
○.会計データ更新ロック						○			○		○	
OE.プルーフリスト確認						○	○	○	○	○	○	○
OE.監査証跡確認						○			○		○	
OE.会計データのバックアップ	○											
OE.バックアップ媒体の管理		○										
OE.正確な日付設定			○									
OE.パスワードの設定				○								
OE.会計責任者の信頼					○							

表の通り、全てのセキュリティ対策方針は少なくとも一つの TOE セキュリティ環境と対応している。

従って、全てのセキュリティ対策方針の必要性は満たされている。

6.1.2. セキュリティ対策方針の十分性

A.会計データのバックアップ

会計責任者が、定期に会計データのバックアップを行うので、十分である。

A.バックアップ媒体の保護

会計責任者が、バックアップ媒体を施錠できる場所に保管することで、バックアップ媒体上の情報を改ざんされることはない。以上により十分である。

A.正確な日付設定

会計責任者が、サーバに設定されている日付を管理するので、正確な日付を実現できる。以上により十分である。

A.パスワードの設定

会計責任者および会計担当者は、パスワードに利用者 ID や生年月日、氏名など容易に推測されるものを避けて設定する。また、パスワードを定期的に変更するので、長期間継続して同じパスワードを使用することはない。以上により十分である。

A.会計責任者の信頼

経営者が、会計責任者に信頼できる者を選任し、管理、指導することで、会計責任者が会計システムの不正な使用を行わないことを実現できる。以上により十分である。

T.勘定科目マスタの不正登録

脅威エージェントである会計担当者とは非許可従業員ごとに、分けて十分性の根拠を示す。

会計担当者が、不正に勘定科目マスタを操作しても、「O.プルーリスト」により、勘定科目マスタの操作記録は、プルーリストに出力される。これを、「OE.プルーリスト確認」により、会計責任者が、操作内容の正当性を確認するため、不正を検知して対策できる。以上により十分である。

なお、「O.プルーリスト」により、会計責任者は不正を判別しやすい形式で確認することができる。また、「O.会計データ更新ロック」により、会計責任者の確認が必要な会計データの期間

の範囲を狭めることができるため、確認の負荷を軽減することができる。

一方、非許可従業員は、「O.利用者の識別と認証」により識別と認証されなければ、会計システムを使用することができない。以上により十分である。

なお、非許可従業員が、TOE の識別と認証に対して、不正な試行を行った結果は、「O.監査証跡」により監査証跡として保管される。これを「OE.監査証跡確認」により、会計責任者が、不正な試みを確認して対策できる。

以下同様のため、省略。

T.勘定科目マスタの登録誤り

T.財務情報の未集計

T.仕訳データの不正入力

T.仕訳データの入力誤り

T.財務報告書の不正作成

T.財務報告書の作成誤り

6.2. セキュリティ要件根拠

本節では、TOE セキュリティ機能要件根拠、セキュリティ機能要件の依存性の妥当性、セキュリティ機能要件の相互サポート構造、評価保証レベルの妥当性、及びセキュリティ保証要件の必要性について述べる。

6.2.1. TOE セキュリティ機能要件根拠

(1) TOE セキュリティ要件の必要性

TOE セキュリティ機能要件と TOE セキュリティ対策方針との対応を以下の「付録図表 8-2-1-1」に示す。

付録図表 8-2-1-1 TOE セキュリティ機能要件と TOE セキュリティ対策方針

	○ 利用者の識別と認証	○ プルーフラスト	○ 監査証跡	○ 会計データ更新ロック
FAU_GEN.1		○	○	
FAU_SAR.1		○	○	
FAU_STG.1		○	○	
FIA_AFL.1	○			
FIA_ATD.1	○			
FIA_SOS.1	○			
FIA_UAU.2	○			
FIA_UAU.7	○			
FIA_UID.2	○			
FMT_MTD.1(1)	○	○	○	○
FMT_MTD.1(2)	○			
FMT_SMF.1(1)	○	○	○	○
FMT_SMF.1(2)	○			
FMT_SMR.1	○	○	○	○
FPT_RVM.1	○			
FPT_STM.1		○	○	

表の通り、全ての TOE セキュリティ機能要件は少なくとも一つの TOE セキュリティ対策方針と対応している。従って、全ての TOE セキュリティ機能要件の必要性は満たされている。

(2) TOE セキュリティ機能要件の十分性

○.利用者の識別と認証機能

「○.利用者の識別と認証機能」を実現するためには、会計責任者や会計担当者が市販会計

パッケージを使う前に、会計責任者や会計担当者であることの識別と認証が成功することを要求すればよい。

FIA_UID.2 及び FIA_UAU.2 は、市販会計パッケージの使用を許可する前に、会計責任者や会計担当者の識別及び認証が成功することを要求している。

従って、「O.利用者の識別と認証」を実現するのに十分である。

なお、FMT_SMF.1(1)は、識別と認証を行うための情報、つまり識別認証情報を管理する機能を要求し、FMT_MTD.1(1)は、識別認証情報を管理する機能(登録、問い合わせ、改変、削除)の使用を、会計責任者に制限することを要求している。

また、FIA_ATD.1 は、識別認証情報に含まれる会計責任者と会計担当者を識別するための属性、つまりグループIDの維持を要求し、FMT_SMR.1 は、TOEが会計責任者の役割を維持し、利用者を会計責任者に関連付けることを要求しており、会計責任者 GID を持ち会計責任者として識別と認証された利用者、つまり会計責任者は、識別認証情報管理機能を用いて、市販会計パッケージを使用することが出来る会計担当者及び、識別情報管理機能を用いることが出来る会計責任者を識別認証情報に登録する。

また、FMT_SMF.1(2)は、会計担当者のパスワードを変更する機能を要求し、FMT_MTD.1(2)は、本人パスワード変更機能の使用を、会計担当者に制限することを要求し、FMT_SMR.1 で利用者である会計担当者を維持することを要求している。

また、FIA_SOS.1 は、パスワードの定義された品質尺度を要求し、FIA_AFL.1 は、パスワードを試行入力する非許可従業員による連続した攻撃に対してアカウントを15分間ロックし、攻撃が成功する可能性を減少させている。

また、FIA_UAU.7 は、認証を行っている間利用者に入力されたパスワードの文字数分の「*」のみをフィードバックし、パスワードの暴露の機会を減少させている。

また、FPT_RVM.1 は、市販パッケージの使用が許可される前に識別と認証機能が必ず実行されることを要求し、迂回されることを防止している。

以下、同様に十分性の根拠を記述する。(省略)

O.プルーフリスト

O.監査証跡

O.会計データ更新ロック

6.2.2. セキュリティ機能要件の依存性の妥当性

セキュリティ機能要件とその依存先との対応を以下の「付録図表 8-2-3」に示す。

表には、セキュリティ機能要件で要求された依存先(依存性欄)と実際に選択した依存先を示している。依存先が FIA_UID.1、FIA_UAU.1 に対しては、上位互換である FIA_UID.2、FIA_UAU.2 を選択する。

付録図表 8-2-3 セキュリティ機能要件と依存先

	依存性	FAU_GEN.1	FIA_UAU.2	FIA_UID.2	FMT_SMF.1(1)	FMT_SMF.1(2)	FMT_SMR.1	FPT_STM.1
FAU_GEN.1	FPT_STM.1							○
FAU_SAR.1	FAU_GEN.1	○						
FAU_STG.1	FAU_GEN.1	○						
FIA_AFL.1	FIA_UAU.1		○					
FIA_ATD.1	なし							
FIA_SOS.1	なし							
FIA_UAU.2	FIA_UID.1			○				
FIA_UAU.7	FIA_UAU.1		○					
FIA_UID.2	なし							
FMT_MTD.1(1)	FMT_SMF.1(1) FMT_SMR.1				○		○	
FMT_MTD.1(2)	FMT_SMF.1(2) FMT_SMR.1					○	○	
FMT_SAE.1	FMT_SMR.1 FPT_STM.1						○	○
FMT_SMF.1(1)	なし							
FMT_SMF.1(2)	なし							
FMT_SMR.1	FIA_UID.1			○				

FPT_RVM.1	なし							
FPT_STM.1	なし							

表の通り、セキュリティ機能要件の依存性は満たされている。従って、セキュリティ機能要件の依存性は妥当である。

6.2.3. セキュリティ機能要件の相互サポート構造

この相互サポート構造は、非活性化防止、迂回防止の観点から構成されている。

非活性化防止

FMT_MTD.1(1)により、FIA_ATD.1、FIA_UAU.2、FIA_UID.2、FMT_SMR.1 の管理対象項目である識別認証情報を変更できるのは会計責任者に限られることが保証されている。

FMT_MTD.1(2)により、FIA_UAU.2 の管理対象項目であるパスワードを変更できるのは会計担当者本人に限られることが保証されている。

迂回防止

FPT_RVM.1 により、TOE を利用する前に、必ず利用者を識別と認証する FIA_UAU.2、FIA_UAU.7、及び FIA_UID.2 が呼び出され成功することが保証されている。

以上により、全ての TOE セキュリティ機能要件の相互サポート構造は妥当である。

6.2.4. 評価保証レベルの妥当性

TOE を含む会計システムは、他システムとの連携によるリスクや、外部ネットワークを利用する際の脅威については、すでに対策済みであることを前提としているので、脅威エージェントは、組織内部の会計担当者とは非許可従業員である。

両者は、IT 技術について高度な専門知識を保持しておらず、低レベルの攻撃しか行わない。従って、TOE の脅威は重大とはみなされないため、EAL1 を評価保証レベルとするのが妥当である。

6.2.5. セキュリティ保証要件の必要性

以下のセキュリティ保証要件は、評価保証レベル 1 を満たす為に必要である。また、これらの全てのセキュリティ保証要件は依存性を満たしている。

- ACM_CAP.1 バージョン番号
- ADO_JGS.1 設置、生成、及び立上げ手順
- ADV_FSP.1 非形式的機能仕様
- ADV_RCR.1 非形式的対応の実証
- AGD_ADM.1 管理者ガイダンス
- AGD_USR.1 利用者ガイダンス
- ATE_IND.1 独立テスト準拠

付録 9. IT 業務処理統制における業務プロセスごとの、リスク、統制活動、統制活動の評価手続の例示

1. はじめに

本追補版の第IV章4. では、IT 業務処理統制について、【統制に関する指針】、【統制目標の例】、【統制の例と統制評価手続の例】を記載しているが、IT 統制の構築・評価の実務においては、販売、購買などの具体的な業務プロセスごとに、リスク、統制活動、統制活動の評価手続、を設定していく必要がある。

そのため、業務プロセスに係る IT 統制評価手続の参考として役立てるため、IT 業務処理統制における業務プロセスごとの、リスク、統制活動、統制活動の評価手続の例示をここに示す。なお、各業務プロセスのファンクション(働き)毎に統制活動を例示しているが、このファンクションは、どのような局面でどのようなリスク、統制活動、統制評価手続があるかを理解するための単なる例示であり、ベストプラクティスもしくはベタープラクティスとして例示しているものではない。

企業は、自社に応じた業務処理統制のリスクコントロールマトリックスを作成する際にこの例示を参考として利用することができるが、その際には、本追補版の第IV章1. (3)、(4)の記載に留意されたい。

2. 使い方と留意点

各業務プロセスについてマスタ登録を記載しているのは、IT を業務に利用する際には、その業務の前提として、マスタ登録の適正な管理なしには、IT の信頼性を確保することが困難であるためである。

例えば、マスタ登録の正当性は、承認されないマスタが登録されるリスクを避けるための統制目標であり、マスタは責任者の承認後に登録される。ここでは、紙で承認したマスタ登録の申請用紙に承認印を押印する手作業の統制後に入力するか、もしくは、画面上で承認するかは定義していない。また、正当性の統制手続として、アクセス権の制御を例示しているが、これは取引の正当性を確保するためのひとつの手段として、業務上の適切な職務と権限の分離とアクセス権限が一致することを想定している。また、完全性、正確性のコントロールについてもプルーフリストの出力をせずに、画面上で確認することを否定しているわけではなく、IT によって自動的に検証することを否定しているものでもない。具体的な統制活動が手作業であるか IT であるかはその企業の実態に則して実施されることを前提としている。

なお、ファイルへのアクセス制御は、各 IT 業務処理統制での制御もあるが、IT 部門のシステム管理者や利用部門のシステムオーナー等の特権のアクセス管理が必要である。特権のアクセス権の管理は、IT 全般統制での制御として評価する場合は想定される。

(1) 財務報告プロセス

財務報告プロセスは、IT 全社的統制と同様に評価する部分と個別の業務プロセスとして確認する部分がある。財務報告プロセスのどの部分を IT 全社的統制とし、どの部分を個別の業務プロセスの統制とするかは、具体的には、会社の実態に合わせて検討を要するが概ね、以下のような項目は全社的統制として区分されると考えられる。

連結グループ全体に適用する会計方針、連結決算の方針、手続等は全社的統制として区分される。ここで対象としているのは、主に個別のプロセスとして区分されると想定される部分である。よって、財務報告プロセスの例示においては、会計方針、連結決算の方針、連結の記載様式等は、既に適正に決定されていることを前提としている。財務報告プロセスは連結財務諸表作成システムや財務会計システムだけでなくスプレッドシート等を利用して行われる場合も多い。よってスプレッドシート等の統制にも留意する。

①連結決算プロセス

連結決算プロセスは、連結財務諸表作成システムを利用することを想定しているが、手作業での処理にも読み替えられるように配慮している。連結決算プロセスは連結財務諸表を作成する際の基本的と考えられる手順を想定したが、必ずしもこの区分が必須ではない。連結の規模によっては取引消去と科目組替等を無理に区分せずに単に修正仕訳として管理することが現実的な場合もある。また、連結の範囲の決定、連結財務諸表作成用の統一フォームへの記載等のプロセスは適切に実施されていることを想定している。

②個別決算プロセス

個別決算プロセスについては、集計は手入力を想定している。財務会計システムに他システムからデータを取り込む場合は、他システムとのインターフェースについての統制が要請される。このため、集計の完全性、正確性については、コントロールトータルチェック、マスタとのチェックなどの IT の技術的なコントロールに置き換えて評価することになる。

修正仕訳のプロセスは手作業による部分が極めて大きいと考えられ、最終の注記等は、スプレッドシート等で実施される場合がある。

(2) その他のプロセス

その他のプロセスは、ある程度のそのプロセスが企業にとって内部統制評価に該当する規模であることを前提としている。これらのプロセスはある前提を置いて作成しているが、これは単なる例示であって標準ではない。参考として利用することを想定している。

①販売プロセス

販売については受注から回収までのプロセスを想定しているが、受注残の管理と返品に

については、企業の業態により手順が異なるため、ここでは記載していない。また、与信管理は適切であることを前提としている。なお、貸倒引当金の検討プロセスは省略している。

②購買プロセス

購買については、発注から支払いまでのプロセスを想定しているが、発注残の管理と返品については、企業の業態により手順が異なるため、ここでは記載していない。また、検収についても、業態によって求められる検収の度合が異なるため、ここでは記載していない。なお、購買の支払は、すべて未払費用勘定を経由して支払うことを想定している。

③たな卸資産プロセス

たな卸資産については、期末に評価替えを実施するが、その評価替えは適正に実施されることを前提としている。また、製造プロセスとの関係が複雑になる場合があるため、製品、商品、半製品のみを対象とし、原材料、貯蔵品は対象外としている。

④固定資産プロセス

固定資産については、工場等のある程度の設備投資をすることを想定している。よって、年間の設備投資計画を立て、年間計画による稟議番号により管理され、基本的に事前の予算枠が無い購入はできない。小規模の備品購入等は別としてすべての支払は、一旦建設仮勘定に登録後に資産と費用に配分される。ここまでの管理を要求しない場合には、単に購入申請に対する承認の手続を経て購入する。固定資産の検収は適切に実施されているものとする。

⑤人事給与プロセス

勤怠管理は適切に実施されていることを前提としている。従って、勤怠管理のプロセスそのものは対象としていない。勤怠の入力はその従業員自らが入力する場合とタイムカード等により人事担当者が入力する場合がある。その両方に対応できるように入力者としているため、企業の実態によって読み替えることができる。

⑥仕訳計上プロセス

仕訳計上のプロセスは、各企業の保有する情報システムの構成や取引形態によって異なるため、各業務プロセスに組み込まずに別に参考とした。

特に業務処理においては仕訳の計上のタイミングは事業の形態、利用するシステム構成により異なる。例えば、出荷時点で売上を計上するにしても出荷毎に売上と売掛金を即時に仕訳計上する場合もあれば、1日単位で計上することもある。また、月に1回の月次単位で計上することもある。この全てを例として各業務処理に記載することは困難なことから、仕訳計上として別の例示とした。この例示においても仕訳計上のタイミングは、利用

者が設定することを想定している。

(3) 利用する際の統制手続と統制評価手続

例示には具体的な統制手続及び統制評価手続については記載していない。統制評価手続は、「統制手続があることを確かめる」との記載としている。利用者は、企業の統制の実態に則して、その整備と運用について具体的な評価手続を実施する。IT 統制は、IT のみではなく、手作業との組合せで実施される場合を想定する必要がある。また、IT 統制の整備と運用を同時に評価できる場合もある。

3. IT 統制目標とアサーションの関係について

企業の業態や取引の形態によりアサーションの区分の仕方は様々であるが、ひとつの考え方の例示として「IT 統制目標とアサーションの関係の考え方 (例)」を作成した。これはひとつの例示であり、考え方が首尾一貫していれば企業はどのようなアサーションの区分を採用しても良い。

(1) アサーション

「適切な財務情報を作成するための要件」は、経営者が、公表している財務諸表が適切であることを主張する根拠に該当するため、「経営者の主張 (アサーション)」という用語で述べられる場合がある。本追補版では「アサーション」としている⇒ (第Ⅲ章4節(1))。

(2) IT 統制目標

本追補版の図表Ⅲ. 4-4 (⇒ 第Ⅲ章4節(3)) に、IT 統制目標とアサーションの関係を記載している。IT 統制目標の正確性については、基本的にアサーションの実在性と対応させている。正確性をアサーションの項目として独立させている場合は、正確性はアサーションの正確性と対応させることになる。

IT 統制目標は、到達すべき目標を記載している。このため、アクセス管理は正当性を確保するための手段として位置づけている。職務権限の分離も正当性の確保の手段として位置づけている。なお、この位置づけは実務の便宜上アクセスコントロールや職務分離を統制すべき項目として区分することを否定するものではない。

正当性、完全性、正確性はトランザクションデータを対象としている。維持継続性は、ファイルやデータベースの正当性、完全性、正確性が保持されることを要請している。このため、ファイルの正当性、完全性、正確性の確保のモニタリングとファイル自体へのアクセス制御が統制の評価対象になる。

ひとつの統制手続は、正当性、完全性、正確性のうちのひとつの統制目標のみを達成する場合と複数の統制目標を同時に達成する場合がある。例えば、入力原票と入力のプルーフリストを一対一でチェックする際に、入力が漏れなく重複無く、また、入力項目ひとつひとつが正確に入力されていることを確かめる場合には、完全性と正確性の二つの統制目標が同時に達成されている。

(3) IT 統制目標とアサーションの関係の考え方 (例)

経営者の主張 (アサーション) については、取引の形態等により異なるアサーションの区分をすることがある。

たとえば、財務諸表監査において、監査人は、監査の実施に当たって、「経営者の主張 (アサーション)」に監査要点を設定することを求められることに対応して、日本公認会計士協会監査基準委員会報告第31号「監査証拠」では、「経営者の主張 (アサーション)」を13項目に区分している。

これは区分の考え方であり監査基準委員会報告第31号においても企業の取引の実態により種々の区分のまとめ方を選択できるとしている。今回、例示を作成するにあたり、例示の作成において複数の解釈をさけるため付録図表9-1のような整理を行って対応付けを実施してみた。これは、あくまで考え方の一例に過ぎず取引の形態等により相違する場合があり、実務において下記の分類を強制するものではないことに留意する。

付録図表9-1 アサーションの整理

		適切な財務情報を作成するための要件(財務報告に関する内部統制の評価及び監査の実施基準)				
		資産及び負債が実際に存在し、取引や会計事象が発生していること	計上すべき資産、負債、取引や会計事象をすべて記録していること	取引や会計事象を適切な金額で記録し、収益及び費用を適切な期間に配分していること	計上されている資産に対する権利及び負債に帰属していること	資産及び負債を適切な価額で計上していること
経営者の主張(監査基準委員会報告書第31号「監査証拠」)		実在性 *1	網羅性	期間配分	権利と義務 *2	評価 *3
(1) 監査対象期間の取引や会計事象に係る経営者の主張						
① 発生	記録された取引や会計事象が発生し企業に関係していること	○			*2	
② 網羅性	記録すべき取引や会計事象がすべて記録されていること		○		*2	
③ 正確性	記録された取引や会計事象に関して金額や他のデータが正確に記録されていること	○ *1			*2	*3
④ 期間帰属	取引や会計事象が正しい会計期間に記録されていること			○		*3
⑤ 分類の妥当性	取引や会計事象が適切な勘定科目に記録されていること	○				*3
(2) 期末の勘定残高に係る経営者の主張						
① 実在性	資産、負債及び資本が実際に存在すること	○				
② 権利と義務	企業は資産の権利を所有しており、負債は企業の債務であること				○ *2	
③ 網羅性	記録すべき資産、負債及び資本がすべて記録されていること		○			
④ 評価と期間配分	財務諸表に含まれる資産、負債及び資本が適切な金額で記録され、評価又は期間配分に係る修正が適切に記録されていること			○		○ *3
(3) 表示と開示に係る経営者の主張						
① 発生及び権利と義務	開示されている取引、会計事象及びその他の事項が発生し企業に関係していること	○			○	
② 網羅性	財務諸表に開示すべき事項がすべて開示されていること		○			
③ 分類と明瞭性	財務情報が適切に表示され開示が明瞭であること			○		
④ 正確性と評価	財務その他の情報が適正かつ適切な額で開示されていること	○				○
ITの統制目標(システム管理基準追補版)						
① 完全性	情報が漏れなく重複無く記録されていること		○	○		
② 正確性	情報が正確に記録され提供されていること	○		○		○
③ 正当性	情報が正規の承認手続を経たものであること	○			○	○
④ 維持継続性	必要な情報が正確に更新されかつ継続使用が可能なこと	○	○	○	○	○

*1 (1)③正確性については実在性の前提条件として、これに含むものとして考えている。

*2 権利と義務については、期末等の時点における権利・義務という整理を行った。そのためデリバティブ等特殊な場合を除き、個々の取引レベルにおいては対応付けを行っていない。

*3 評価については、対象物の帳簿価額とその現在価値の比較における要件として整理を行った。そのため単純な価格の入力エラー等については他の要件にて含まれることになる。

- * 1 連結方針や連結資料の様式等は、決定されていることを想定している
 * 2 個別財務諸表は適正に作成されていることを前提とし、連結用の様式への記載のプロセスはここでは省いている
 * 3 連結の範囲やセグメント等の決定のプロセスはここでは省いている
 * 4 修正仕訳等の仕訳自体の適正性の判断のプロセスは省いている経理部長は適正な承認をしていることを想定している

項番	IT統制目標	リスク	統制活動の例	統制活動の評価	適切な財務諸表作成の要件						
					網羅性	実在性	期間配分	権利と義務	評価	表示	
1	マスタ登録	正当性	承認されないマスタ登録が行われる(連結方針と異なる登録)	マスタ登録の内容は連結方針にそって承認されたものだけが登録される	承認された内容のみがマスタ登録されていることを確かめる		○				○
2			入力者は、アクセス権で制御されている	入力者は、アクセス権で制御されていることを確かめる		○				○	
3		完全性	マスタの二重登録や不足がある	マスタ登録後にブルーリストを出し、登録内容を確認する	ブルーリストによる確認が実施されていることを確かめる	○		○			○
4		正確性	マスタ登録に誤りがある	マスタ登録後にブルーリストを出し、登録内容を確認する	ブルーリストによる確認が実施されていることを確かめる		○	○			○
5		維持継続性	マスタが最新でなく、継続使用できない	マスタの登録内容が最新の状態で更新されていることをリストを出して確認する	マスタの登録内容が最新の状態で更新されていることをリストを出して確認する	○	○	○			○
6	集計	正当性	承認されない財務情報の入力が行われる	入力者は、アクセス権で制御されている	入力者は、アクセス権で制御されていることを確かめる		○				○
7				管理者により承認された財務情報のみが入力される	管理者により承認された財務情報のみが入力されていることを確かめる		○				○
8		完全性	財務情報の二重入力、入力漏れが発生する	入力後にブルーリストを出し連結対象会社の財務情報が全て、登録されたことを確認する	ブルーリストによる確認が実施されていることを確かめる	○			○		○
9				全ての財務情報が集計されない	一部を手で再計算している	再計算により確認していることを確かめる	○			○	
10		正確性	入力に誤りがある	入力後にブルーリストを出し連結対象会社の財務情報が全て、登録されたことを確認する	ブルーリストによる確認が実施されていることを確かめる		○				○
11				関連する数値のチェック機能(関連数値、貸借一致)によるチェック結果を確認する	チェック結果を確認し、異常が無いことを確かめる		○				○
12				集計に誤りがある	一部を手で再計算している	再計算により確認していることを確かめる		○			
13		維持継続性	財務情報の集計ファイルに権限者以外が不正な入力をする	入力者は、アクセス権で制御されている	入力者は、アクセス権で制御されていることを確かめる	○	○	○			○
14				一次入力後の修正入力は、リストに出力され、検証される	一次入力後の修正入力は、リストに出力され、検証されていることを確かめる	○	○	○			○
15	開始仕訳	正当性	不正な開始仕訳が入力される	開始仕訳の前年との連続性を経理部長が確かめる	開始仕訳の前年との連続性を経理部長が確かめていることを確認する		○				○
16				期首剰余金の分析は、経理部長が承認している	期首剰余金の分析は、経理部長が承認していることを確かめる		○				○
17				期中の資本移動の会計処理は経理部長が承認している	期中の資本移動の会計処理は経理部長が承認していることを確かめる		○				○
18				アクセス権で制御されている	アクセス権で制御されていることを確かめる		○				○
19		完全性	開始仕訳の二重入力、入力漏れが発生する	開始仕訳の前年との連続性を経理部長が確かめる	開始仕訳の前年との連続性を経理部長が確かめていることを確認する	○		○			○

項番		IT統制目標	リスク	統制活動の例	統制活動の評価	適切な財務諸表作成の要件					
						網羅性	実在性	期間配分	権利と義務	評価	表示
20				開始仕訳ブルーリストで入力漏れが無いことを確認する	開始仕訳ブルーリストで入力漏れが無いことを確認する	○		○			○
21		正確性	誤った開始仕訳が実施される	開始仕訳の前年との連続性を経理部長が確かめる	開始仕訳の前年との連続性を経理部長が確かめていることを確認する		○	○			○
22				期首剰余金の分析は、経理部長が承認している	期首剰余金の分析は、経理部長が承認していることを確かめる		○	○			○
23				期中の資本移動の仕訳ブルーリストと経理部長の承認したリストと照合している	期中の資本移動の仕訳ブルーリストと経理部長の承認したリストと照合していることを確かめる		○	○			○
24		維持継続性	仕訳ファイルに権限者以外が不正な入力をする	開始仕訳はブルーリストに出力され経理部長が確認する	開始仕訳はブルーリストに出力され経理部長が確認していることを確かめる	○	○	○			○
25				入力者は、アクセス権で制御されている	入力者は、アクセス権で制御されていることを確かめる	○	○	○			○
26	取引消去	正当性	不正な消去仕訳が入力される	消去仕訳の実行者は、アクセス権で制御されている	アクセス権で制御されていることを確かめる		○				○
27				連結方針にそった消去仕訳が計上されていることを消去仕訳リストで確認する	消去仕訳リストでの確認が実施されていることを確かめる		○				○
28		完全性	消去仕訳の二重入力、入力漏れが発生する	期首剰余金の分析は、経理部長が承認している	期首剰余金の分析は、経理部長が承認していることを確かめる	○					○
29		正確性	誤った消去仕訳が実施される	期首剰余金の分析は、経理部長が承認している	期首剰余金の分析は、経理部長が承認していることを確かめる		○				○
30				関連する数値のチェック機能(関連数値、貸借一致等)によるチェック結果を確認する	チェック結果を確認し、異常が無いことを確かめる		○				○
31		維持継続性	仕訳ファイルに権限者以外が不正な入力をする	二次修正、三次修正等の入力は、出力され検証される	二次修正、三次修正等の入力は、出力され検証されていることを確かめる	○	○	○			○
32				入力者は、アクセス権で制御されている	入力者は、アクセス権で制御されていることを確かめる	○	○	○			○
33		修正仕訳	正当性	不正な仕訳が入力される	承認された仕訳のみが入力されていることをブルーリストで確かめる	ブルーリストが確認されていることを確かめる		○		○	○
34	入力者は、アクセス権で制御されている				入力者は、アクセス権で制御されていることを確かめる		○		○	○	
35	完全性		修正仕訳の二重入力、入力漏れが発生する	仕訳リストで消去仕訳を確認する	仕訳リストで消去仕訳を確認していることを確かめる	○		○	○	○	
36	正確性		誤った修正仕訳が入力される	関連する数値のチェック機能(関連数値、貸借一致)によるチェック結果を確認する	チェック結果を確認し、異常が無いことを確かめる		○		○	○	
37				開始仕訳はブルーリストに出力され経理部長が確認する	開始仕訳はブルーリストに出力され経理部長が確認していることを確かめる		○		○	○	
38	維持継続性		仕訳ファイルに権限者以外が不正な入力をする	二次修正、三次修正等の入力は、出力され検証される	二次修正、三次修正等の入力は、出力され検証されていることを確かめる	○	○	○	○	○	
39		仕訳ファイルへの入力が誤っている		入力者は、アクセス権で制御されている	入力者は、アクセス権で制御されていることを確かめる	○	○	○	○	○	
40				経理部長が前期比較等の仕訳の分析により、異常な数値が無いことを確認している	経理部長が前期比較等の仕訳の分析により、異常な数値が無いことを確認していることを確かめる	○	○	○	○	○	

項番		IT統制目標	リスク	統制活動の例	統制活動の評価	適切な財務諸表作成の要件					
						網羅性	実在性	期間配分	権利と義務	評価	表示
41	科目組替	正当性	不正な科目の組替が行われる	承認された連結方針にそった科目の組替のみが入力される	承認された科目の組替のみが入力されていることを確かめる		○				○
42				入力者は、アクセス権で制御されている	入力者は、アクセス権で制御されていることを確かめる		○				○
43		完全性	科目の組替が二重に実施されたり、入力漏れがある	連結方針にそった科目組替が実施されていることを仕訳リストで確認する	仕訳リストで確認していることを確かめる	○		○			○
44				科目組替伝票番号は連版管理される	科目組替伝票番号は連番管理されていることを確かめる	○		○			○
45		正確性	科目の組替が正確に入力されない	関連する数値のチェック機能(関連数値、貸借一致)によるチェック結果を確認する	チェック結果を確認し、異常が無いことを確かめる		○				○
46		維持継続性	科目組替のファイルに権限者以外が不正な入力をする	二次修正、三次修正等の入力は、出力され検証される	二次修正、三次修正等の入力は、出力され検証されていることを確かめる	○	○	○		○	○
47				経理部長が前期比較等の仕訳の分析により、異常な数値が無いことを確認している	経理部長が前期比較等の仕訳の分析により、異常な数値が無いことを確認していることを確かめる	○	○	○		○	○
48				入力者は、アクセス権で制御されている	入力者は、アクセス権で制御されていることを確かめる	○	○	○		○	○
49		報告	正当性	承認されない財務報告が作成される	承認された財務報告が出力される	出力される財務報告は承認されていることを確かめる		○			
50	完全性		財務報告に重複や漏れがある	関連する数値のチェック機能(関連数値、貸借一致)によるチェック結果を確認する	チェック結果を確認し、異常が無いことを確かめる	○					○
51				修正入力は、リストに出力され、検証される	修正入力は、リストに出力され、検証されていることを確かめる	○					○
52	正確性		財務報告が正確ではない	関連する数値のチェック機能(関連数値、貸借一致)によるチェック結果を確認する	チェック結果を確認し、異常が無いことを確かめる		○				○
53				修正入力は、リストに出力され、検証される	修正入力は、リストに出力され、検証されていることを確かめる		○				○
54	維持継続性		財務報告が不正に変更される	経理部長は前期比較等の分析により、異常点が無いことを確認している	経理部長は前期比較等の分析により、異常点が無いことを確認していることを確かめる	○	○	○		○	○
55				財務報告が誤って変更される	財務報告は確定後に変更ができないようにロックされる	財務報告は確定後にロックされていることを確かめる	○	○	○		○

- * 1 会計方針については適切な選択が実施されていると想定している
 * 2 評価や見積りのプロセスはここでは対象からはずしている
 * 3 分析等の監視的業務を誰が実施するかはその組織の実態できめるべきであり、ここでは特定していない

項番	IT統制目標	リスク	統制活動の例	統制活動の評価	適切な財務諸表作成の要件						
					網羅性	実在性	期間配分	権利と義務	評価	表示	
1	マスタ登録	正当性	承認されないマスタ登録が行われる(会計方針と異なる登録)	マスタ登録後の内容(勘定科目、償却の方法等)は会計方針にそって承認されたものだけが登録される	承認された内容のみがマスタ登録されていることを確かめる		○				○
2				入力者は、アクセス権で制御されている	入力者は、アクセス権で制御されていることを確かめる		○				○
3		完全性	マスタの二重登録や不足がある	マスタ登録後にブルーリストを出し、登録内容を確認する	ブルーリストによる確認が実施されていることを確かめる	○		○			○
4		正確性	マスタ登録に誤りがある	マスタ登録後にブルーリストを出し、登録内容を確認する	ブルーリストによる確認が実施されていることを確かめる		○	○			○
5		維持継続性	マスタが最新でなく、継続使用できない	マスタの登録内容が最新の状態で更新されていることをリストを出して確認する	マスタの登録内容が最新の状態で更新されていることをリストを出して確認する	○	○	○			○
6	集計	正当性	承認されない財務情報の入力が行われる	入力者は、アクセス権で制御されている	入力者は、アクセス権で制御されていることを確かめる		○				○
7				管理者により承認された財務情報のみが入力される	管理者により承認された財務情報のみが入力されていることを確かめる		○				○
8				伝票の訂正は赤黒伝票のみで実施する	赤黒以外に伝票訂正ができないことを確かめる		○				○
9				月次締後は、月次決算は修正できない	月次締後の変更ができないことを確かめる		○				○
10		完全性	財務情報の二重入力、入力漏れが発生する	入力後にブルーリストを出し、登録内容を確認する	ブルーリストによる確認が実施されていることを確かめる	○			○		○
11				全ての財務情報が集計されない	一部を手で再計算している	再計算により確認していることを確かめる	○			○	
12		正確性	入力に誤りがある	入力後にブルーリストを出し、登録内容を確認する	ブルーリストによる確認が実施されていることを確かめる		○				○
13				関連する数値のチェック機能(関連数値、貸借一致)によるチェック結果を確認する	チェック結果を確認し、異常が無いことを確かめる		○				○
14				集計に誤りがある	一部を手で再計算している	再計算により確認していることを確かめる		○			
15		維持継続性	財務情報の集計ファイルに権限者以外が不正な入力をする	入力者は、アクセス権で制御されている	入力者は、アクセス権で制御されていることを確かめる	○	○	○			○
16	前期比較表等の差異分析表を作成し、異常点を分析する			差異分析表をレビューし異常点を確認する	○	○	○			○	
17	修正仕訳	正当性	不正な仕訳が入力される	承認された仕訳のみが入力されていることをブルーリストで確かめる	承認された仕訳のみが入力されていることをブルーリストで確かめる		○		○	○	○
18					入力者は、アクセス権で制御されている	入力者は、アクセス権で制御されていることを確かめる		○		○	○
19		完全性	修正仕訳の二重入力、入力漏れが発生する	仕訳のブルーリストで確認する	仕訳のブルーリストで確認していることを確かめる	○		○		○	○
20		正確性	誤った修正仕訳が入力される	入力後にブルーリストを出し、登録内容を確認する	ブルーリストによる確認が実施されていることを確かめる		○		○	○	○
21					前期比較表等の差異分析表を作成し、異常点を分析する	差異分析表をレビューし異常点を確認する		○		○	○

項番		IT統制目標	リスク	統制活動の例	統制活動の評価	適切な財務諸表作成の要件					
						網羅性	実在性	期間配分	権利と義務	評価	表示
22		維持継続性	修正仕訳ファイルに権限者以外が不正な入力をする	入力者は、アクセス権で制御されている	入力者は、アクセス権で制御されていることを確かめる	○	○	○	○	○	○
23				前期比較表等の差異分析表を作成し、異常点を分析する	差異分析表をレビューし異常点を確認する	○	○	○	○	○	○
24	報告	正当性	承認されない財務報告が作成される	承認された財務報告が出力される	出力される財務報告は承認されていることを確かめる		○				○
25		完全性	財務報告に重複や漏れがある	関連する数値のチェック機能(関連数値、貸借一致)によるチェック結果を確認する	チェック結果を確認し、異常が無いことを確かめる	○					○
26				前期比較表等の差異分析表を作成し、異常点を分析する	差異分析表をレビューし異常点を確認する	○					○
27		正確性	財務報告が正確ではない	関連する数値のチェック機能(関連数値、貸借一致)によるチェック結果を確認する	チェック結果を確認し、異常が無いことを確かめる		○				○
28				前期比較表等の差異分析表を作成し、異常点を分析する	差異分析表をレビューし異常点を確認する		○				○
29		維持継続性	財務報告が不正に変更される	財務報告は確定後に変更ができないようにロックされる	確定後にロックされていることを確かめる	○	○	○	○	○	○

*1 仕訳作成のタイミングは、会社の業務フローによりいくつかの計上パターンが想定される。そのため下記表中では省略している。一般的には、出荷後 検収後 請求時 入金時などが想定される。
 *2 サービス契約のように期間按分された売上計上する場合には、期間配分の要件を考慮する場合がある。ここでは、按分計算のない単純な販売を想定しているため期間配分との対応付けを行っていない。
 *3 表示については、主として財務諸表作成にて検討すべき要件と整理し、取引分類の基礎となるマスターのみ対応付けを行っている。
 *4 返品は業種により複雑さが異なるため、今回は対象から外している。

関連する勘定科目：売上、売掛金、未収入金

項番	IT統制目標	リスク	統制活動の例	統制活動の評価	適切な財務諸表作成の要件						
					実在性	網羅性	期間配分	権利と義務	評価	表示	
1	マスタ登録	正当性	正当でない得意先が登録される	取引先の登録ルールに基づいて承認された取引先のみが登録される	承認された取引先のみがマスタ登録されていることを確かめる	○					
2			マスタの入力者は、アクセス権で制御されている	マスタ入力者は、アクセス権で制御されていることを確かめる	○						
3			正当でない与信限度や取引条件が登録される	与信会議で承認された与信限度、取引条件のみが登録される	与信会議で承認された与信限度、取引条件のみが登録されていることを確かめる	○					
4		完全性	マスタの二重登録や不足がある	マスタ登録後にブルーリストを出し、登録内容を確認する	ブルーリストによる確認が実施されていることを確かめる		○	○			
5		正確性	マスタ登録に誤りがある	マスタ登録後にブルーリストを出し、登録内容を確認する	ブルーリストによる確認が実施されていることを確かめる	○	○	○			○
6		維持継続性	取引先、取引条件、与信限度が見直されず正当でない取引先が登録される	マスタの登録内容を見直し、更新する	マスタの登録内容の見直しを実施されていることを確認する	○	○	○			
7	受注	正当性	正当でない受注が計上される	受注入力者は、アクセス権で制御されている	受注入力者は、アクセス権で制御されていることを確かめる	○			*2		
8			マスタに登録されていない取引先の受注は登録できない	マスタ登録されていない取引先の受注は登録されないことを確かめる	○				*2		
9			与信限度を超える受注は登録できない	与信限度を超える受注は登録できないことを確かめる	○					*2	
10			在庫引当ができない受注は登録できない	在庫引当ができない受注は登録できないことを確かめる	○					*2	
11		完全性	受注の二重入力、入力漏れが発生する	入力後にブルーリストを出し、登録内容を確認する	ブルーリストによる確認が実施されていることを確かめる		○				
12				受注番号は自動採番される	受注番号は自動採番されることを確かめる		○				
13				受注残リストが出力され検証される	受注残リストが出力され検証されていることを確かめる		○				
14		正確性	入力に誤りがある	入力後にブルーリストを出し、登録内容を確認する	ブルーリストによる確認が実施されていることを確かめる	○					
15				販売単価は得意先ごとにマスタ登録された掛率のみ登録される	マスタ登録された販売掛率のみで登録されていることを確かめる	○					
16				受注番号は自動採番される	受注番号は自動採番されることを確かめる	○					
17	維持継続性	受注ファイルに権限者以外が不正な入力をする	入力者は、アクセス権で制御されている	入力者は、アクセス権で制御されていることを確かめる	○	○					
18			受注状況与信残は毎日集計され、営業担当者に報告され確認される	営業担当者が報告を確認していることを確かめる	○	○					

(2)その他のプロセス ①販売プロセス

(2/3)

項番		IT統制目標	リスク	統制活動の例	統制活動の評価	適切な財務諸表作成の要件					
						実在性	網羅性	期間配分	権利と義務	評価	表示
19	出荷	正当性	正当な受注以外の出荷が行われる	受注データからのみ出荷指図が作成される	受注データからのみ出荷指図が作成されることを確かめる	○					
20				在庫引当された受注のみが出荷指図される	在庫引当された受注のみが出荷指図されることを確かめる	○					
21		完全性	出荷指図の二重入力、入力漏れが発生する	同一の受注番号は2回引当されない	同一の受注番号は2回引当されていないことを確かめる		○				
22				出荷後に出荷確認入力をする	出荷後に出荷確認入力が行われていることを確かめる		○				
23				出荷残リストが出力され検証される	出荷残リストが出力され検証されていることを確かめる		○				
24				出荷確認データから売上データに転送時のコントロールトータルを設定し一致を確認している	出荷確認データから売上データへのデータ転送のコントロールトータルを確認していることを確かめる		○				
25		正確性	誤った出荷が行われる	受注データからのみ出荷指図が作成される	受注データからのみ出荷指図が作成されることを確かめる	○		○			
26		維持継続性	出荷ファイルに権限者以外が不正な入力をする	入力者は、アクセス権で制御されている	入力者は、アクセス権で制御されていることを確かめる	○	○				
27				出荷残リストが出力され検証される	出荷残リストが出力され検証される	○	○				
28		請求	正当性	正当でない請求が行われる	請求書は取引条件により締め日毎に売上データから作成される	請求書が取引条件通りに作成されていることを確かめる	○			○	
29	請求書は営業部長の承認なしには発送されない				営業部長の承認なしには発送されないことを確かめる	○			○		
30	完全性		請求の二重計上、計上漏れが発生する	請求済みの売上はフラグで消しまれ2回請求されない	請求済みの売上はフラグで消しまれていることを確かめる		○				
31				請求番号は自動採番される	請求番号は自動採番されていることを確かめる		○				
32				請求残リストが出力され、営業部長がレビューする	請求残リストが出力され、営業部長がレビューしていることを確かめる		○				
33	正確性		誤った請求が行われる	請求書は取引条件により締め日毎に売上データから作成される	請求書は取引条件により締め日毎に売上データから作成されていることを確かめる	○				○	
34				請求書は営業部長の承認なしには発送されない	請求書は営業部長の承認なしには発送されないことを確かめる	○					○
35				請求済みの売上はフラグで消しまれ2回請求されない	請求済みの売上はフラグで消しまれていることを確かめる	○					○
36	維持継続性		請求ファイルが不正に改ざんされる	アクセス権は制御されている	アクセス権は制御されていることを確かめる	○	○				
37				請求残リストが出力され検証される	請求残リストが出力され、営業部長がレビューしていることを確かめる	○	○				
38	回収	正当性	正当でない入金データがある	入金データは経理で請求番号と消しまれる	入金データは経理で請求番号と消しまれていることを確認する	○			○		

項番	IT統制目標	リスク	統制活動の例	統制活動の評価	適切な財務諸表作成の要件					
					実在性	網羅性	期間配分	権利と義務	評価	表示
39			貸方科目は、担当部の管理者の承認なしには計上されない	貸方科目の承認を確かめる	○			○		
40	完全性	回収の二重計上、計上漏れが発生する	入金データは経理で請求番号と消込まれる	入金データは経理で請求番号と消込まれていることを確かめる		○				
41			消し込み残リストは営業に確認し、処理される	消し込み残リストは営業に確認し、処理されていることを確かめる		○				
42			回収残リストが出力され経理と営業でレビューされる	回収残リストが出力され経理と営業でレビューされていることを確かめる		○				
43			正確性	誤った消し込みが行われる	入金データは経理で請求番号と消込まれる	入金データは経理で請求番号と消込まれていることを確かめる	○			
44	消し込み残リストは営業に確認し、処理される	消し込み残リストは営業に確認し、処理されていることを確かめる			○				○	
45	回収残リストが出力され経理と営業でレビューされる	回収残リストが出力され経理と営業でレビューされていることを確かめる			○				○	
46	維持継続性	回収ファイルが不正に改ざんされる	アクセス権は制御されている	アクセス権は制御されていることを確かめる	○	○				
47			売掛金の滞留等の分析が実施される	売掛金の滞留等の分析が実施されていることを確かめる	○	○				

- *1 仕訳作成のタイミングは、会社の業務フローによりいくつかの計上パターンが想定される。そのため上記表中では省略している。一般的には、検収時 請求書到着時 支払時などが想定される。
- *2 分割納入のような場合には、期間配分の要件を考慮する場合がある。ここでは単純は購買を想定しているため期間配分との対応付けを行っていない。
- *3 表示については、主として財務諸表作成にて検討すべき要件と整理し、取引分類の基礎となるマスターのみ対応付けを行っている。
- *4 返品については、業種により複雑さが異なるため省略している

関連する勘定科目：仕入、買掛金、未払金

項番	IT統制目標	リスク	統制活動の例	統制活動の評価	適切な財務諸表作成の要件						
					実在性	網羅性	期間配分	権利と義務	評価	表示	
1	マスタ登録	正当性	正当でない得意先が登録される	取引先の登録ルールに基づいて承認された取引先のみが登録される	承認された取引先のみがマスタ登録されていることを確かめる	○					
2			マスタの入力者は、アクセス権で制御されている	マスタ入力者は、アクセス権で制御されていることを確かめる	○						
3		正当でない与信限度や取引条件が登録される	与信会議で承認された与信限度、取引条件のみが登録される	与信会議で承認された与信限度、取引条件のみが登録されていることを確かめる	○						
4		完全性	マスタの二重登録や不足がある	マスタ登録後にブルーリストを出し、登録内容を確認する	ブルーリストによる確認が実施されていることを確かめる		○	○			
5		正確性	マスタ登録に誤りがある	マスタ登録後にブルーリストを出し、登録内容を確認する	ブルーリストによる確認が実施されていることを確かめる	○	○	○			○
6		維持継続性	取引先、取引条件、与信限度が見直されず正当でない取引先が登録される	マスタの登録内容を一定時期に見直し、更新する	マスタの登録内容の見直しを実施されていることを確認する	○	○	○			
7	発注	正当性	正当でない発注が計上される	発注入力者は、アクセス権で制御されている	発注入力者は、アクセス権で制御されていることを確かめる	○					
8			マスタに登録されていない取引先への発注は登録できない	マスタ登録されていない取引先への発注は登録できないことを確かめる	○						
9			与信限度を超える発注は登録できない	与信限度を超える発注は登録できないことを確かめる	○						
10			発注権限者が承認しない発注は登録できない	発注権限者が承認しない発注は登録できないことを確かめる	○						
11		完全性	発注の二重入力、入力漏れが発生する	入力後にブルーリストを出し、登録内容を確認する	ブルーリストによる確認が実施されていることを確かめる		○				
12				発注番号は自動採番される	発注番号は自動採番されることを確かめる		○				
13				発注残リストが出力され検証される	発注残リストが出力され検証されていることを確かめる		○				
14		正確性	入力に誤りがある	入力後にブルーリストを出し、登録内容を確認する	ブルーリストによる確認が実施されていることを確かめる	○					
15				発注単価は取引先ごとにマスタ登録された単価のみ発注される	マスタ登録された購買単価のみで発注されることを確かめる	○					
16				発注番号は自動採番される	発注番号は自動採番されることを確かめる	○					
17	維持継続性	発注ファイルに権限者以外が不正な入力をする	入力者は、アクセス権で制御されている	入力者は、アクセス権で制御されていることを確かめる	○	○					
18			発注状況と信残は毎日集計され、発注担当者や管理者に報告され確認される	発注担当者、管理者が報告を確認していることを確かめる	○	○					
17	入荷	正当性	正当な発注以外の出荷が行われる	発注データからのみ入庫予定が作成される	発注データからのみ入庫予定が作成されることを確かめる	○					
18			入庫予定と入庫データは消し込まれ発注番号のある納品のみが入庫される	発注番号のある納品のみが入庫されることを確かめる	○						
19		完全性	入庫の二重入力、入力漏れが発生する	同一の発注番号は2回消し込まれない	同一の発注番号は2回消し込まれていないことを確かめる		○				
20				納品漏れが発生する	入庫予定と入庫データは消し込まれる	入庫予定と入庫データは消し込まれていることを確かめる		○			

項番		IT統制目標	リスク	統制活動の例	統制活動の評価	適切な財務諸表作成の要件							
						実在性	網羅性	期間配分	権利と義務	評価	表示		
21				入庫残リストが出力され検証してから入庫確定データが作成される	入庫残リストが出力され検証してから確定データが作成されていることを確かめる		○						
22				仕入の二重計上、計上漏れが発生する	入庫確認データから仕入データに転送時のコントロールトータルを設定している	入庫確認データから仕入データに転送時のコントロールトータルを確認する		○					
23				正確性	誤った入庫が行われる	発注番号は自動採番されている	発注番号は自動採番されることを確かめる	○		○			
24						入庫時に検品が実施され、入庫予定と不一致の納品は受け取らない	入庫時に検品が実施され、入庫予定と不一致の納品は受け取らないことを確かめる	○					
25				維持継続性	出荷ファイルに権限者以外が不正な入力をする	入力者は、アクセス権で制御されている	入力者は、アクセス権で制御されていることを確かめる	○	○				
26						入庫残リストが出力され検証される	入庫残リストが出力され検証されていることを確かめる	○	○				
27	請求請け処理	正当性	正当でない請求が行われる	請求書は発注番号で管理され、入庫ファイルと照合され、一致しないと支払リストに計上処理されない	入庫ファイルと一致しないと支払リストに計上されないことを確かめる	○			○				
28				請求書は発注担当者、管理者の承認なしには経理で支払いをしない	請求書は発注担当者、管理者の承認なしには経理で支払いをしないことを確かめる	○			○				
29				完全性	請求の二重計上、計上漏れが発生する	請求書は発注番号で管理され、入庫ファイルと照合され、一致しないと処理されない	請求書が入庫ファイルで消し込まれていることを確かめる		○	○			
30						未払ファイルの請求請け番号は自動採番される	請求請け番号は自動採番されていることを確かめる		○	○			
31		請求書は全て未払ファイルに登録後、支払をする	請求書は全て未払ファイルに登録後、支払をしていることを確かめる				○	○					
32		正確性	誤った請求請け処理が行われる	請求書は発注番号で管理され、入庫ファイルと照合され、一致しないと処理されない	請求書が入庫ファイルで消し込まれていることを確かめる	○				○			
33				請求書は発注担当者、管理者の承認なしには経理で支払いをしない	請求書は発注担当者、管理者の承認なしには経理で支払いをしないことを確かめる	○				○			
34		維持継続性	請求ファイルが不正に改ざんされる	請求ファイルへのアクセス権は制御されている	請求ファイルへのアクセス権は制御されていることを確かめる	○	○	○					
35				請求書一覧が支払い毎に作成され、発注担当者のレビューを受ける	請求書一覧が支払い毎に作成され、発注担当者のレビューを受けていることを確認する	○	○	○					
36		支払	正当性	正当でない支払データがある	請求支払一覧と請求書は経理部長が照合し未払ファイルから銀行支払依頼を作成する	請求支払一覧と請求書は経理部長が照合していることを確かめる	○			○			
37	借方科目は、担当課の管理者と経理部長の承認なしには計上されない				借方科目の担当課管理者経理部長承認を確かめる	○			○				
38	銀行への支払依頼未払ファイルからのみ作成される				銀行への支払依頼未払ファイルからのみ作成されていることを確かめる	○			○				
39	完全性		支払の二重計上、計上漏れが発生する	未払ファイルからのみ銀行の支払依頼は作成される	未払ファイルからのみ銀行の支払依頼は作成されることを確かめる		○						
40		入庫データと未払データは照合され、入庫済みで未請求分のリストが出力され、未払計上漏れが無いかを経理で検証する		未払計上漏れリストを経理が検証していることを確かめる		○							

項番	IT統制目標	リスク	統制活動の例	統制活動の評価	適切な財務諸表作成の要件					
					実在性	網羅性	期間配分	権利と義務	評価	表示
41			支払リストと支払残リストが出力され経理と購買でレビューされる	支払リストと支払残リストが出力され経理と購買でレビューされていることを確かめる		○				
42	正確性	誤った消し込みが行われる	経理部署は支払リストにエラー項目が無いことを確認し支払承認をする	経理部署は支払リストにエラー項目が無いことを確認し支払承認をしたことを確かめる	○				○	
43	維持継続性	支払ファイルが不正に改ざんされる	アクセス権は制御されている	アクセス権は制御されていることを確かめる	○	○	○			
44			一定の条件で支払状況を抽出し、異常点がないかを経理が確かめる	異常点の検証が経理により、レビューされていることを確かめる	○	○	○			
45			支払リストと支払残リストが出力され経理と購買でレビューされる	支払リストと支払残リストが出力され経理と購買でレビューされていることを確かめる	○	○	○			

* 1 仕訳作成については、下記表では省略している。ここでは在庫ファイルへの書き込みを想定している。在庫ファイルからどのタイミングで仕訳が作成されるかは企業の実態で異なる。
 * 2 入庫、出庫は、購買、販売、製造と連携していることを想定している。このため検収の過程は終了していることを前提としている。ブルーリストによる入力の照合は、システムが連動する場合は、システム間のデータ転送の結果を確認することに読み替えることになる。
 * 3 たな卸資産 評価のプロセスは、企業の事業形態や製品等の性質により異なるため、ここでは評価結果を受け入れるのみであり、評価プロセスは対象としていない

関連する勘定科目：製品商品、半製品

項番		IT統制目標	リスク	統制活動の例	統制活動の評価	適切な財務諸表作成の要件						
						実在性	網羅性	期間配分	権利と義務	評価	表示	
1	マスタ登録	正当性	承認されていない製品商品が登録される	生産管理本部長が承認した製品、商品、半製品のみがマスタ登録される	承認された製品、商品、半製品のみがマスタ登録されていることを確かめる	○						
2				マスタへの入力者は、アクセス権で制御されている	マスタ入力者は、アクセス権で制御されていることを確かめる	○						
3			正当でない予定単価等が登録される	承認された予定単価等のみが登録される	承認された予定単価等のみが登録されていることを確かめる	○						
4			たな卸資産の評価の方法、計算方法が会計の規則や、企業の会計方針に沿っていない	たな卸資産の評価の方法、計算方法は、企業の方針に沿って承認されたものが登録されている	たな卸資産の評価の方法、計算方法は、企業の方針に沿って承認されたものが登録されていることを確かめる	○		○		○		
5		完全性	マスタの二重登録や不足がある	マスタ登録後にブルーリストを出し、登録内容を確認する	ブルーリストによる確認が実施されていることを確かめる	○	○	○		○		
6		正確性	マスタ登録に誤りがある	マスタ登録後にブルーリストを出し、登録内容を確認する	ブルーリストによる確認が実施されていることを確かめる	○		○		○	○	
7		維持継続性	正当でないたな卸資産が登録される	マスタの登録内容を一定時期に見直し、更新する	マスタの登録内容の見直しを実施されていることを確認する	○	○	○	○	○	○	
8	入庫	正当性	正当でないたな卸資産が計上される	入庫入力者は、アクセス権で制御されている	入庫入力者は、アクセス権で制御されていることを確かめる	○						
9				マスタに登録されていない製品、商品の入庫は登録できない	マスタ登録されていない製品、商品の入庫が登録されないことを確かめる	○						
10				入庫予定と異なる入庫は登録できない	入庫予定と異なる入庫は登録できないことを確かめる	○						
11		完全性	たな卸資産の二重入力、入力漏れが発生する	入力後にブルーリストを出し、登録内容を確認する	ブルーリストによる確認が実施されていることを確かめる		○					
12				入庫番号は自動採番されるが製造時の製造ロット番号は引き継がれる	入庫番号は自動採番され、製造ロット番号は引き継がれていることを確かめる		○					
13				入庫予定がある場合は予定との差額リストが出力され検証される	入庫予定がある場合は予定との差額リストが出力され検証されていることを確かめる		○					
14		正確性	入力に誤りがある	入力後にブルーリストを出し、登録内容を確認する	ブルーリストによる確認が実施されていることを確かめる	○						
15				製品単価は取引先ごとにマスタ登録された単価のみで登録される。入庫ごとに単価が異なる場合は、発注者が承認した単価で入力される	製品単価は取引先ごとにマスタ登録された単価のみで登録されていることを確かめる	○						
16				ブルーリストによる確認が実施されていることを確かめる	ブルーリストによる確認が実施されていることを確かめる	○						
17		維持継続性	在庫ファイルに権限者以外が不正な入力をする	入力者は、アクセス権で制御されている	入力者は、アクセス権で制御されていることを確かめる	○						
18	入庫は毎日集計され、発注担当者と管理者に報告され確認される			発注担当者、管理者が報告を確認していることを確かめる	○	○						
19	内部移動	正当性	認められない資産の移動が計上される	資産の移動は、正式に承認された移動の依頼によって指示され、登録される	資産の移動は、正式に承認された移動の依頼によって指示され、登録されていることを確かめる	○						
20				移動の入力は、入力権限にある担当者のIDとパスワードで制御されている	移動の入力は、入力権限にある担当者のIDとパスワードで制御されていることを確かめる	○						

項番		IT統制目標	リスク	統制活動の例	統制活動の評価	適切な財務諸表作成の要件					
						実在性	網羅性	期間配分	権利と義務	評価	表示
21		完全性	すべての移動は記録される	移動元の出庫データは、入庫先で入庫がないと未受入残として表示される	移動元の出庫データは、入庫先で入庫がないと未受入残として表示されることを確かめる		○				
22				入力後にブルーリストを出し、登録内容を確認する	ブルーリストによる確認が実施されていることを確かめる		○				
23		正確性	移動すべきたな卸資産が正確でない	入力後にブルーリストを出し、登録内容を確認する	ブルーリストによる確認が実施されていることを確かめる	○					
24	出庫	正当性	正当な出庫指示以外の出荷が行われる	出庫指示データからのみ入庫予定が作成される	出庫指示データからのみ入庫予定が作成されることを確かめる	○					
25				出庫指示と出庫データは消し込まれる出庫指示番号のある製品等のみが出庫される	出庫指示と出庫データは消し込まれる出庫指示番号のある製品等のみが出庫されていることを確かめる	○					
26		完全性	出庫の二重入力、入力漏れが発生する	同一の出庫指示番号は2回消し込まれない	同一の出庫指示番号は2回消し込まれないことを確かめる		○				
27				出庫指示と出庫データは消し込まれる	出庫指示と出庫データは消し込まれていることを確かめる		○				
28				出庫残リストが出力され検証される	出庫残リストが出力され検証されていることを確かめる		○				
29				売上等の二重計上、計上漏れが発生する	出庫確認データから売上等データ等に転送時のコントロールトータルを設定している	出庫確認データから売上等データ等に転送時のコントロールトータルが設定されていることを確かめる		○			
30		正確性	誤った出庫が行われる	入力後にブルーリストを出し、登録内容を確認する	ブルーリストによる確認が実施されていることを確かめる	○					
31				出庫時に検品が実施され、出庫指示と不一致の出庫は出庫されない	出庫時に検品が実施され、出庫指示と不一致の出庫は出庫されないことを確かめる	○					
32		維持継続性	出荷ファイルに権限者以外が不正な入力をする	入力者は、アクセス権で制御されている	入力者は、アクセス権で制御されていることを確かめる	○					
33	評価	正当性	会社の会計方針に従わない評価がされる	会社のルール通りであることを一部計算して確かめる	会社のルール通りであることを一部計算して確かめていることを確かめる	○				○	
34		完全性	対象となる全ての資産が評価されない	月次等での評価結果の処理件数は確認されている	月次での評価結果の処理件数は確認し、処理漏れの無いことを確認していることを確かめる		○				○
35		正確性	対象となる資産の評価が正確ではない	一部の計算結果を手作業で確認している	計算結果を検証していることを確かめる	○					○
36		維持継続性	在庫ファイルに権限者以外が不正な入力をする	ファイルへの不正なアクセスは制限されている	正当な権限者のみがファイルにアクセスしていることを確かめる	○					○
37	たな卸	正当性	実在しない在庫が計上される	たな卸により、実在を確認した在庫が登録される	たな卸により、実在を確認した在庫が登録される	○				○	
38				たな卸の結果は、内部監査部恩と生産管理部門によって承認される	たな卸の結果は、内部監査部恩と生産管理部門によって承認されていることを確かめる	○				○	
39		完全性	たな卸資産の二重計上、計上漏れが発生する	たな卸結果は、継続帳簿と突合され差異が検証される	たな卸結果は、継続帳簿と突合され差異が検証されていることを確かめる		○				○
40				入力後にブルーリストを出し、登録内容を確認する	ブルーリストによる確認が実施されていることを確かめる					○	
41		正確性	たな卸の結果が正確に反映されない	入力後にブルーリストを出し、登録内容を確認する	ブルーリストによる確認が実施されていることを確かめる	○					○
42		維持継続性	在庫ファイルが不正に改ざんされる	アクセス権は制御されている	アクセス権は制御されていることを確かめる	○					
43				在庫ファイルの分析を経理が実施して異常点が無いかを確認する	在庫ファイルの分析を経理が実施して異常点が無いかを確認していることを確かめる	○	○	○		○	○
44		廃棄	正当でない廃棄データがある	廃棄は所定の承認手続により廃棄指示をし、廃棄される	廃棄は所定の承認手続によっていることを確かめる	○					○

項番	IT統制目標	リスク	統制活動の例	統制活動の評価	適切な財務諸表作成の要件					
					実在性	網羅性	期間配分	権利と義務	評価	表示
45			廃棄の実際の記録を確認して廃棄の登録をする	廃棄の実際の記録を確認して廃棄の登録をしていることを確かめる	○			○	○	
46	完全性	廃棄の二重計上、計上漏れが発生する	入力後にブルーリストを出し、登録内容を確認する	ブルーリストによる確認が実施されていることを確かめる		○	○	○	○	
47			廃棄指示の未処理残が経理で確認される	廃棄指示の未処理残が表示され経理で確認されていることを確かめる		○	○	○	○	
48	正確性	誤った廃棄が行われる	ブルーリストによる確認が実施されていることを確かめる	ブルーリストによる確認が実施されていることを確かめる	○				○	
49	維持継続性	支払ファイルが不正に改ざんされる	アクセス権は制御されている	アクセス権は制御されていることを確かめる	○					
50			一定の条件で在庫状況を抽出し、廃棄対象となるべき在庫が未処理となっていないなど異常点がないかを経理が確かめる	異常点の検証が経理により、実施されていることを確かめる	○	○	○	○	○	○

- * 1 仕訳作成については、下記表では省略している。仕訳作成のタイミングは、企業の実態に合わせる
 * 2 固定資産の評価については、評価プロセスは、省略している
 * 3 ここではある程度大規模な固定資産の購入を想定している。このため、固定資産購入計画に基づく事前稟議を想定している
 * 4 全ての固定資産の購入は一旦、建設仮勘定を経由してから各勘定科目の振り替えることを想定している。

関連する勘定科目：固定資産、未払金、建設仮勘定、修繕費、

項番	IT統制目標	リスク	統制活動の例	統制活動の評価	適切な財務諸表作成の要件						
					実在性	網羅性	期間配分	権利と義務	評価	表示	
1	マスタ登録	正当性	承認されていない固定資産が購入される	固定資産購入計画で承認された固定資産購入し予算稟議が承認される	承認された予算のみがマスタ登録されていることを確かめる	○					
2			承認された固定資産項目のみが登録される	承認された固定資産項目のみが登録されていることを確かめる	○						
3			マスタの入力者は、アクセス権で制御されている	マスタ入力者は、アクセス権で制御されていることを確かめる	○						
4		正当でない償却方法や計算式等が登録される	承認された償却方法のみが登録される	承認された償却方法のみが登録されていることを確かめる	○		○		○		
5		完全性	マスタの二重登録や不足がある	マスタ登録後にブルーリストを出し、登録内容を確認する	ブルーリストによる確認が実施されていることを確かめる	○	○	○		○	
6		正確性	マスタ登録に誤りがある	マスタ登録後にブルーリストを出し、登録内容を確認する	ブルーリストによる確認が実施されていることを確かめる	○		○		○	○
7		維持継続性	正当でない固定資産マスタが登録される	マスタの登録内容を一定時期にたな卸をし、更新する	マスタの登録内容のたな卸が実施されていることを確認する	○	○	○	○	○	○
8	計上	正当性	正当でない固定資産が計上される	入力者は、アクセス権で制御されている	入力者は、アクセス権で制御されていることを確かめる	○			○	○	
9			マスタに登録されていない科目への登録はできない	マスタに登録されていない科目への登録はできないことを確かめる	○				○	○	
10			予算稟議番号の該当の無い固定資産は登録できない	予算稟議番号の該当の無い固定資産は登録できないことを確かめる	○					○	○
11			予算限度を超える金額は登録できない	予算限度を超える金額は登録できないことを確かめる	○					○	○
12		完全性	固定資産の二重入力、入力漏れが発生する	入力後にブルーリストを出し、登録内容を確認する	ブルーリストによる確認が実施されていることを確かめる	○	○	○			
13		伝票番号は自動採番される	伝票番号は自動採番されることを確かめる	○							
14		全ての固定資産関連の支払は、全て建設仮勘定に入力し、そこから振替えられ、直接入力はできない	全ての固定資産関連の支払は、全て建設仮勘定から振替えられ、直接入力はできないことを確かめる	○							
15	正確性	入力に誤りがある	入力後にブルーリストを出し、登録内容を確認する	ブルーリストによる確認が実施されていることを確かめる	○		○		○		
16	建設仮勘定への登録は経理が証拠書類を確認後に入力する	建設仮勘定への登録は経理が証拠書類を確認後に入力していることを確認する	○				○		○		
17	維持継続性	発注ファイルに権限者以外が不正な入力をする	入力者は、アクセス権で制御されている	入力者は、アクセス権で制御されていることを確かめる	○						
18			建設仮勘定の残の内容を経理が4半期ごとに検証している	建設仮勘定の残の内容を経理が4半期ごとに検証していることを確かめる	○	○	○				
19	科目振替	正当性	発注ファイルに権限者以外が不正な入力をする	資産と費用の分類は基準通りに分類して振替えられていることを経理が確認している	資産と費用の分類は基準通りに分類して振替えられていることを経理が確認していることを確かめる	○					
20		完全性	計上すべき資産や費用に漏れがある	建設仮勘定の残の内容を経理が4半期ごとに検証し、振替漏れが無いことを確認する	建設仮勘定の残の内容を経理が4半期ごとに検証し、振替漏れが無いことを確かめる	○	○	○			

(2)その他のプロセス ④固定資産プロセス

(2/3)

項番	IT統制目標	リスク	統制活動の例	統制活動の評価	適切な財務諸表作成の要件						
					実在性	網羅性	期間配分	権利と義務	評価	表示	
21			資産の計上時に固定資産番号で区分される	資産の計上時に固定資産番号で区分されていることを確かめる		○	○				
22	正確性	計上すべき資産や費用が正確でない	費用と資産の振替は経理で内容を確認している	費用と資産の振替は経理で内容を確認していることを確かめる	○					○	
23	償却計算	正当性	会社の会計方針に沿って償却計算を実施できない	マスタに登録した償却計算しか実行できない	マスタに登録した償却計算しか実行できないことを確かめる	○		○		○	
24		償却計算の開始は、会社の規則(検収基準等)によっていない	償却計算の開始は、会社の規則(検収基準等)により、経理が設定する	償却計算の開始は、会社の規則によって経理が設定していることを確かめる	○		○			○	
25	完全性	償却計算の二重入力、入力漏れが発生する	同一の資産番号は2回計算されない	同一の資産番号は2回計算されていないことを確かめる			○	○			
26			償却計算を実施していない資産はリストされ経理が償却漏れが無いかを確認している	償却計算を実施していない資産はリストされ経理が償却漏れが無いかを確認していることを確かめる			○	○			
27	正確性	会社の会計方針に沿って償却計算を実施できない	費用と資産の振替は経理で内容を確認している	費用と資産の振替は経理で内容を確認していることを確かめる	○		○			○	
28			一部、経理が償却計算を検証している	一部、経理が償却計算を検証していることを確かめる	○		○			○	
29	維持継続性	償却計算ファイルに権限者以外が不正な入力をする	入力者は、アクセス権で制御されている	入力者は、アクセス権で制御されていることを確かめる	○	○	○			○	
30			経理は償却の合計額を分析し異常点が無いかを検証している	経理が償却の合計額を分析し異常点が無いかを検証していることを確かめる	○	○	○			○	
31	評価	資産価値の無い資産が計上される	経理は資産の期末時点での価値を評価し、経理部長の承認によりその結果を反映している	経理は資産の期末時点での価値を評価し、経理部長の承認によりその結果を反映していることを確かめる	○			○		○	
32			資産のたな卸により、資産の実在を確かめ、経理部長の承認により、結果を帳簿に反映する	資産のたな卸により、資産の実在を確かめ、経理部長の承認により、結果を帳簿に反映していることを確かめる	○				○		○
33	完全性	固定資産評価に漏れがある	固定資産台帳上で評価減された資産は明示され、経理が漏れが無いかを確認している	固定資産台帳上で評価減された資産は明示され、経理が漏れが無いかを確認していることを確かめる		○	○			○	
34	正確性	誤った評価が実施される	固定資産台帳上で評価減された資産は明示され経理が誤りが無いかを確認している	固定資産台帳上で評価減された資産は明示され経理が誤りが無いかを確認していることを確かめる	○		○			○	
35	維持継続性	固定資産ファイルが不当に書き換えられる	アクセス権は制御されている	アクセス権は制御されていることを確かめる	○	○	○			○	
36	廃棄	承認されない廃棄が行われる	固定資産の廃棄は廃棄申請により管理者が承認する	固定資産の廃棄は廃棄申請により承認し廃棄していることを確かめている	○			○		○	
37			廃棄終了の報告により、廃棄登録を固定資産台帳に入力する	廃棄終了の報告により、廃棄の登録をしていることを確かめる	○				○		○
38			廃棄入力は経理の担当のみが可能である	廃棄入力は経理担当のみが可能であることを確かめる	○				○		○
39	完全性	廃棄資産の二重計上、計上漏れが発生する	廃棄申請は番号で管理される	廃棄申請は番号で管理されていることを確かめる		○	○			○	
40			廃棄申請の未廃棄分はリストされ、廃棄実施の漏れが無いかを経理が確認する	廃棄申請の未廃棄分はリストされ、廃棄実施の漏れが無いかを経理が確認していることを確かめる			○	○			○
41	正確性	誤った廃棄の計上を実施される	廃棄リストは固定資産台帳から作成される	廃棄リストは固定資産台帳から作成される	○					○	
42	維持継続性	廃棄資産のファイルは不当に変更されない	アクセス権は制御されている	アクセス権は制御されていることを確かめる	○						

項番	IT統制目標	リスク	統制活動の例	統制活動の評価	適切な財務諸表作成の要件					
					実在性	網羅性	期間配分	権利と義務	評価	表示
43			固定資産台帳の増減分析を経理で実施し、異常点が無いことを確認する	固定資産台帳の増減分析を経理で実施し、異常点が無いことを確認していることを確かめる	○	○	○	○	○	○

- *1 給与計算は人事部の閉じられた中で詳細が計算され、合計のみが経理に紙の伝票で渡されることを想定している。人事課職員が、伝票を作成し、人事部長が給与リストと照合して押印し、経理に渡している。
- *2 給与支払の銀行への指図も人事部から行われ、経理は支払合計のみを伝票で知るのみである
- *3 勤怠管理は、給与計算システムとは別にあり、その結果を給与システムは受け取ることを想定している
- *4 人事考課は全く別の仕組であり、このシステムは給与計算のみである
- *5 給与から控除される税金、健康保険料、財形、家賃等は別途のサブプロセスで管理されていると想定している

関連する勘定科目：給与手当、通勤手当、預かり金、社会保険料、預金

項番	IT統制目標	リスク	統制活動の例	統制活動の評価	適切な財務諸表作成の要件						
					実在性	網羅性	期間配分	権利と義務	評価	表示	
1	マスタ登録	正当性	承認されていない給与マスタが登録される	人事部長が承認したマスタのみが登録される	承認された給与マスタ登録されていることを確かめる	○					
2			マスタの入力者は、アクセス権で制御されている	マスタ入力者は、アクセス権で制御されていることを確かめる	○						
3		正当でない職階や手当が登録される	担当部長と人事部長が承認した職階や手当のみが登録される	担当部長と人事部長が承認した職階や手当のみが登録されていることを確かめる	○						
4		完全性	マスタの二重登録や不足がある	マスタ登録後にブルーリストを出し、登録内容を確認する	ブルーリストによる確認が実施されていることを確かめる		○				
5		正確性	マスタ登録に誤りがある	マスタ登録後にブルーリストを出し、登録内容を確認する	ブルーリストによる確認が実施されていることを確かめる	○		○			○
6		維持継続性	給与マスタが見直されず正当でないマスタが登録される	マスタの登録内容を一定時期に見直し、更新する	マスタの登録内容の見直しを実施されていることを確認する	○	○	○			
7	入力・集計	正当性	正当でない勤怠や評価が計上される	勤怠の報告入力者は、アクセス権で制御されている	入力者は、アクセス権で制御されていることを確かめる	○					
8			マスタに登録されていない勤怠項目の登録はできない	マスタに登録されていない勤怠の登録はできないことを確かめる	○						
9			特別手当や賞与加算、減算は担当部署と人事部長承認で登録される	特別手当や賞与加算、減算は担当部署と人事部長承認で登録されていることを確かめる	○						
10		完全性	勤怠の二重入力、入力漏れが発生する	入力後にブルーリストを出し、登録内容を確認する	ブルーリストによる確認が実施されていることを確かめる		○				
11			人事コードはユニークである	人事コードはユニークであることを確かめる		○					
12			給与リストが出力され人事で異常点が無いか検証される	給与リストが出力され人事で検証されていることを確かめる		○					
13	正確性	入力に誤りがある	入力後にブルーリストを出し、登録内容を確認する	ブルーリストによる確認が実施されていることを確かめる	○						
14			勤怠システムに入力されたデータとマスタテーブルからのみ給与計算され、これ以外のルートでの変更はできない	勤怠システムに入力されたデータとマスタテーブルからのみ給与計算されることを確かめる	○						
15			一部、計算チェックを人事で実施する	一部、計算チェックを人事で実施していることを確かめる	○						
16	維持継続性	勤怠ファイルに権限者以外が不正な入力をする	入力者は、アクセス権で制御されている	入力者は、アクセス権で制御されていることを確かめる	○	○	○				
17			異常な残業等は人事でリストされ分析される。	異常な残業等は人事でリストされ分析されていることを確かめる	○	○	○				
18	給与支払額計算	正当性	人事部長が承認した支払が実施されない	人事部長が承認した給与のみが支払われる	支払は人事部長が承認していることを確かめる	○					
19		完全性	給与の二重入力、入力漏れが発生する	人事番号はユニークで2回消しこまれない	人事番号はユニークで2回消しこまれないことを確かめる		○				
20				給与支払について休職者や海外勤務者等は別途リストされ人事で個別に確認している。	給与支払について休職者や海外勤務者等は別途リストされ人事で個別に確認していることを確かめる		○				

(2)その他のプロセス ⑤人事給与プロセス

(2/2)

項番		IT統制目標	リスク	統制活動の例	統制活動の評価	適切な財務諸表作成の要件						
						実在性	網羅性	期間配分	権利と義務	評価	表示	
21		正確性	誤った給与計算が行われる	給与テーブルはマスタ登録され、変更はできない	給与テーブルはマスタ登録され、変更はできないことを確かめる	○						
22				人事がサンプル数件で計算を確認している	人事がサンプル数件で計算を確認していることを確かめる	○						
23		維持継続性	給与ファイルに権限者以外が不正な入力をする	アクセス権は制御されている	アクセス権は制御されていることを確かめる	○	○					
24				支払の総人数、支払総金額は給与計算のリストと確認される	支払の総人数、支払総金額は給与計算のリストと確認されていることを確かめる	○	○					
25	源泉納付等	正当性	正当でない納付が行われる	納付額等はマスタに登録されたテーブルや控除額に基づいて計上される。	納付額はマスタに登録されたテーブルや控除額に基づいて計上されていることを確かめる	○						
26				退職等の特例は必ず人事で計算調べをする	退職等の特例は必ず人事で計算調べをしていることを確かめる	○						
27		完全性	納付の二重計上、計上漏れが発生する	納付額はマスタに登録されたテーブルや控除額に基づいて計上され個人は1項目につき一度しか控除されない	納付額はマスタに登録されたテーブルや控除額に基づいて計上され個人は1項目につき一度しか控除されないことを確認する		○					
28				納付額は全て未払ファイルに登録後、支払をする	未払ファイルの残を検証する		○					
29		正確性	誤った控除が行われる	退職等の特例は必ず人事で計算調べをする	退職等の特例は必ず人事で計算調べをしていることを確かめる	○						
30				納付額等はマスタに登録されたテーブルや控除額に基づいて計上され個人は1項目につき一度しか控除されない	納付額等はマスタに登録されたテーブルや控除額に基づいて計上され個人は1項目につき一度しか控除されないことを確認する	○						
31		維持継続性	納付ファイルが不正に改ざんされる	アクセス権は制御されている	アクセス権は制御されていることを確かめる	○	○					
32		支払	正当性	正当でない給与支払が実施される	給与計算は勤怠の入力とマスタテーブル、人事部長に承認された特別手当で計算される	給与計算は勤怠の入力とマスタテーブル、人事部長に承認された特別手当で計算されることを確かめる	○					
33					納付額はマスタに登録されたテーブルや控除額に基づいて計上される。	納付額はマスタに登録されたテーブルや控除額に基づいて形状されていることを確かめる	○					
34			完全性	支払の二重計上、計上漏れが発生する	人事コードはユニークであり、二重計算が無いように制御されている	人事コードはユニークであり、二重計算が無いように制御されていることを確かめる		○				
35	給与支払について休職者や海外勤務者等は別途リストされ人事で個別に確認している。				給与支払について休職者や海外勤務者等は別途リストされ人事で個別に確認していることを確かめる		○					
36	正確性		誤った支払が行われる	納付額はマスタに登録されたテーブルや控除額に基づいて計上され個人は1項目につき一度しか控除されない	納付額はマスタに登録されたテーブルや控除額に基づいて計上され個人は1項目につき一度しか控除されないことを確かめる	○						
37				人事がサンプル数件の計算を確認している	人事でサンプルで数件の計算を確認していることを確かめる	○						
38	維持継続性		支払ファイルが不正に改ざんされる	アクセス権は制御されている	アクセス権は制御されていることを確かめる	○	○					
39				異常な残業等は人事でリストされ分析され、過大、過小な支払いはチェックされる	異常な残業等は人事でリストされ分析され、過大、過小な支払いはチェックされていることを確かめる	○	○					

- * 1 仕訳作成については、仕訳作成のタイミングは、企業の実態に合わせる
- * 2 会計システムにデータを送信する際に仕訳を自動的に業務側で作成することを想定している
- * 3 仕訳の受け入れ時に貸借の一致の確認をしていることを想定している
- * 4 会計システム側では、期間帰属を確認して受け入れることを想定している
- * 5 仕訳の訂正は、赤伝票、黒伝票のみで行うことを想定している
- * 6 伝票の承認が手作業か電子承認か承認を何段階にするかは会社の事情により異なる

関連する勘定科目:全勘定科目

項番	IT統制目標	リスク	統制活動の例	統制活動の評価	適切な財務諸表作成の要件						
					実在性	網羅性	期間配分	権利と義務	評価	表示	
1	マスタ登録	正当性	承認されていない勘定科目が登録される	経理部長が承認した勘定科目のみが登録される	経理部長が承認した勘定科目のみが登録されていることを確かめる	○					○
2			自動仕訳の設定は経理部長が承認した仕訳で設定されている	自動仕訳の設定は経理部長が承認した仕訳で設定されていることを確かめる	○					○	
3			マスタの入力者は、アクセス権で制御されている	マスタ入力者は、アクセス権で制御されていることを確かめる	○					○	
4		完全性	マスタの二重登録や不足がある	マスタ登録後にブルーリストを出し、登録内容を確認する	ブルーリストによる確認が実施されていることを確かめる	○	○				
5		正確性	マスタ登録に誤りがある	マスタ登録後にブルーリストを出し、登録内容を確認する	ブルーリストによる確認が実施されていることを確かめる	○		○			○
6		維持継続性	正当でない勘定マスタが登録される	マスタの登録内容を一定時期にたな卸をし、更新する	マスタの登録内容のたな卸が実施されていることを確認する	○	○	○			○
7	計上	正当性	正当でない仕訳が計上される	入力者は、アクセス権で制御されている	入力者は、アクセス権で制御されていることを確かめる	○					
8			マスタに登録されていない科目への登録はできない	マスタに登録されていない科目への登録はできないことを確かめる	○						
9			各業務システムからの伝送されるデータはあらかじめ設定された自動仕訳で送信される	各業務システムからの伝送されるデータはあらかじめ設定された自動仕訳で送信されることを確かめる	○						
10			個別の仕訳伝票は経理部長が承認する	個別の仕訳伝票は経理部長が承認していることを確かめる	○						
11		完全性	仕訳の二重入力、入力漏れが発生する	入力後にブルーリストを出し、登録内容を確認する	ブルーリストによる確認が実施されていることを確かめる	○	○	○			
12				伝票番号は自動採番される	伝票番号は自動採番されることを確かめる		○	○			
13				伝送されるデータはコントロールトータルチェックを行う	伝送されるデータはコントロールトータルチェックが行われていることを確かめる		○	○			
14		正確性	入力に誤りがある	入力後にブルーリストを出し、登録内容を確認する	ブルーリストによる確認が実施されていることを確かめる	○		○	○		○
15				マスタに登録されていない科目への登録はできない	マスタに登録されていない科目への登録はできないことを確かめる	○		○	○		○
16				日付は入力日か伝送時の日付で登録される	日付は入力日か伝送時の日付で登録されることを確かめる	○		○	○		○
17	伝送されるデータは期間帰属の日付チェックを実施する			伝送されるデータは期間帰属の日付チェックを実施していることを確かめる	○		○	○		○	
18	一旦登録された伝票の訂正は赤伝票、黒伝票でしかできない			一旦登録された伝票の訂正は赤伝票、黒伝票でしかできないことを確かめる	○		○	○		○	

(2)その他のプロセス ⑥仕訳計上プロセス

(2/2)

項番	IT統制目標	リスク	統制活動の例	統制活動の評価	適切な財務諸表作成の要件					
					実在性	網羅性	期間配分	権利と義務	評価	表示
19			各業務システムからの伝送されるデータはあらかじめ設定された自動仕訳で送信される	各業務システムからの伝送されるデータはあらかじめ設定された自動仕訳で送信されることを確かめる	○		○	○	○	
20	維持継続性	仕訳ファイルに権限者以外が不正な入力をする	入力者は、アクセス権で制御されている	入力者は、アクセス権で制御されていることを確かめる	○	○	○	○	○	○
21			各業務システムの月次の合計と各勘定の月次の合計を経理で照合する	各業務システムの月次の合計と各勘定の月次の合計を経理で照合している	○	○	○	○	○	○