



**システム導入・更改における統制構築・  
高度化に関するサービス**

# システム導入・更改に伴う内部統制の高度化

企業のIT環境高度化に対応できる内部統制の高度化が求められています

## ■規制当局からの要求水準の高まり

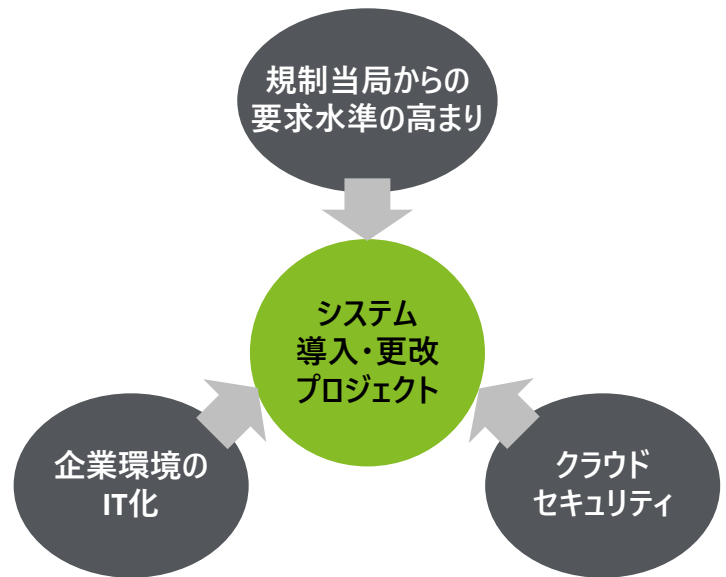
各国規制当局の連携実態及びJICPAの動向を踏まえると、ISA（国際監査基準）でもPCAOB基準で要求される高い水準での監査手続が求められるようになっており、遠からず日本基準でも高い水準での監査手続きに対応した内部統制の高度化が求められることが想定される

## ■企業環境のIT化

進化するビジネス環境において、企業によるITの利用環境および利用状況の進化により、システム導入・更改プロジェクトにおいては、ガバナンス強化を目的とした統制機能の構築が求められている

## ■クラウドセキュリティ

組織がクラウドサービス（SaaS、PaaS、IaaSなど）を利用する際に、情報漏えい・不正アクセス・サービス停止等のリスクを適切に管理・低減するために、内部統制の仕組みや運用を強化することが求められている



システム導入・更改プロジェクトにおいては、以下のような領域について、特に留意する必要があります

主な領域	主なPitfall
プロジェクト・ガバナンス	<ul style="list-style-type: none"> <li>経営者のプロジェクト関与が不十分で、経営者の意図に即さないシステムが構築される</li> <li>内部統制要件/セキュリティ要件の検討が不十分で、財務諸表監査に影響を及ぼす</li> <li>ベンダー主導による要件検討による業務処理パターンの検討が不十分で、要件の再検討のためにスケジュールが遅延する。</li> <li>標準機能、内部統制の知識が不十分で、稼働後に新規帳票作成などの追加開発が発生する</li> <li>ユーザトレーニングの検討が不十分で、稼働後に正しい処理（マスタ・伝票登録時の入力ミス・入力情報の不足等）が行われない</li> <li>データ移行の検討が不十分で、マスタ不備、データ不整合が発生する</li> <li>本番稼働判定基準作成されておらず、テスト結果が不十分にもかかわらず、バグが残存した状態でシステムを稼働させる</li> <li>ハイパーケア体制の検討が不十分で、稼働後にシステムが適切に運用されない</li> </ul>
テスト	
データ移行	
カットオーバー・ハイパーケア	
IT全般統制	<ul style="list-style-type: none"> <li>IT全般統制上の課題に対する検討が不十分で、稼働後に不備が識別される</li> <li>ログ出力機能、パスワード設定などのシステム設定機能の検討が不十分で、稼働後に不備が識別されたり、追加開発が必要になる</li> </ul>
業務プロセス統制	
職務分掌	<ul style="list-style-type: none"> <li>業務処理パターンの検討が不十分で、稼働後に手作業による修正が発生し、決算処理に影響を及ぼす</li> <li>権限ロール設計、ユーザー設定の検討が不正確で、アクセスセキュリティが不十分なままシステムを稼働させる</li> <li>業務記述書・業務フロー図、RCMなどの内部統制関連文書が更新されない</li> </ul>
クラウドセキュリティ	
	<ul style="list-style-type: none"> <li>クラウド内のセキュリティの設定が不完全であるか、過剰な特権アクセスが許可される</li> <li>リスク軽減のためのログが利用できない</li> </ul>

## サービスの概要

システム開発プロジェクトにともない内部統制の見直し、高度化を図るための助言を実施します。

### ①システム導入・更改と並行した内部統制高度化に関する助言

システム導入・更改プロジェクトの計画に合わせて、内部統制の現状評価・分析を行い、課題を識別した上で対応計画を策定し本番リリースまでに内部統制が構築されていることを確認するための助言を実施します。

### 内部統制高度化の流れ

フェーズ	現状評価・分析			統制設計・文書化		ウォークスルー		
ステップ	①現状理解	②課題・ToDoとりまとめ	③統制整備・文書化計画	①統制設計	②内部統制文書の作成	①ウォークスルー	②プレ評価	③監査人レビュー課題・ToDo
目的・ゴール	<ul style="list-style-type: none"> <li>再構築する基幹システムの全体構想や業務フローをレビューし、業務実施上及び監査上のリスクや課題を洗い出す</li> </ul>			<ul style="list-style-type: none"> <li>評価・分析結果、SaaS固有リスク等を踏まえた効率的かつ実効性のある統制設計のための提案を実施</li> <li>統制の要点をまとめた3点セットの作成助言</li> </ul>		<ul style="list-style-type: none"> <li>ウォークスルーを通じ、整備状況のプレ評価が実施され、発見された課題・ToDoの対応方針が策定され、調査を監査人レビューに供されている</li> </ul>		
タスク	<ul style="list-style-type: none"> <li>①現状理解                             <ul style="list-style-type: none"> <li>資料の閲覧および関係者へのインタビューにより、現行の統制、新システムで計画されている統制を理解する</li> </ul> </li> <li>②課題・ToDoとりまとめ                             <ul style="list-style-type: none"> <li>既知の課題、現状理解で抽出した課題、チェックリスト等と突合して検出した課題等を取り纏め対応の方向性を決定する</li> </ul> </li> <li>③統制整備・文書化計画                             <ul style="list-style-type: none"> <li>後続フェーズへの影響を検討し、計画を詳細化する</li> <li>内部統制上の課題を整理し、監査部門等との認識合わせを行う</li> </ul> </li> </ul>			<ul style="list-style-type: none"> <li>①統制設計 (IT全般統制、業務処理統制を対象)                             <ul style="list-style-type: none"> <li>前フェーズで特定された課題に対して改善案を、業務部門・システム部門と討議する</li> <li>業務部門・システム部門と合意した統制活動を最終化する</li> </ul> </li> <li>②内部統制文書の更新                             <ul style="list-style-type: none"> <li>IT全般統制領域については、RCMを作成する</li> <li>業務処理統制の領域については3点セット(プロセスフロー、業務記述書、RCM)を作成する</li> </ul> </li> </ul>		<ul style="list-style-type: none"> <li>①ウォークスルーの実施                             <ul style="list-style-type: none"> <li>IT全般統制、IT業務処理統制のウォークスルーを実施</li> <li>母集団の網羅性を確認する</li> </ul> </li> <li>②プレ評価の実施                             <ul style="list-style-type: none"> <li>本番環境と同等の環境でIT全般統制、IT業務処理統制の評価を実施</li> </ul> </li> <li>③監査人レビュー、課題・ToDo                             <ul style="list-style-type: none"> <li>監査人のレビューに供する</li> <li>課題・ToDoを取りまとめる</li> </ul> </li> </ul>		

### ②IT統制監査に関するワークショップ

現在実施しているIT統制 (IT全般統制、IT業務処理統制) を対象に、トーマツのチェックリストや統制事例等の説明を受けるとともに、ワークショップとして自社で課題について検討し、IT統制への理解を深めることを目的としています。

また、ワークショップを通じて、現状評価・分析工程で作成した課題や統制設計・文書化を進めるための知見を身に付けることを目的とします。

### ワークショップの流れ

STEP	1. 事前準備	2. ワークショップ開催	3. 振り返り
クライアント	<ul style="list-style-type: none"> <li>依頼書に基づく事前資料のご準備</li> <li>現状業務・課題の情報共有</li> <li>事前協議 (対象範囲の検討含)</li> <li>ご参加メンバーの決定</li> <li>事前勉強会・WS開催日程の決定</li> <li>事前勉強会への参加</li> <li>資料の事前読込・課題検討</li> </ul>	<ul style="list-style-type: none"> <li>WSへのご参加                             <ul style="list-style-type: none"> <li>WSの狙いの理解</li> <li>WS実施 (ハンズオン)</li> <li>ハンズオン結果についてのディスカッション</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>WS振り返りへのご参加                             <ul style="list-style-type: none"> <li>WSを通じて得た気づきや、今後に向けてのアクションプランに関するディスカッション</li> </ul> </li> </ul>
当法人	<ul style="list-style-type: none"> <li>事前に協議・決定したテーマに基づく事前資料準備依頼書の作成・ご提示</li> <li>現状業務・課題の情報確認</li> <li>事前協議</li> <li>WSのコンテンツ作成</li> <li>事前勉強会・WS開催日程の調整</li> <li>事前勉強会の実施</li> </ul>	<ul style="list-style-type: none"> <li>WSのファシリテート                             <ul style="list-style-type: none"> <li>IT監査基礎知識の説明</li> <li>WS実施 (ファシリテート)</li> <li>ハンズオン結果についてのディスカッション</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>WS振り返りのファシリテート                             <ul style="list-style-type: none"> <li>WSを通じて得た気づきや、今後に向けてのアクションプランに関するディスカッション</li> <li>WSを通じて検出した課題を現行分析・評価に反映</li> </ul> </li> </ul>

### ①J-SOX対応の専門知見

J-SOX対応に関し監査法人の知見を活用したアプローチを有しています

アプローチを活用した、効果的・効率的な構築・文書案作成を立案・実施いたします

「トーマツ内部統制報告制度対応アプローチ」「タスクリスト」

### ②テクノロジーフレームワークの活用

デロイトの知見を集約した、IT全般統制の標準化された評価の枠組みであるテクノロジーフレームワークを有しています

テクノロジー毎のリスク対応のリーディングプラクティスに基づいた評価手法であり、実質的なリスク領域を識別することで監査品質を向上し、標準化された手続きを実施することができます

典型的な発見事項

- 不要なユーザーが存在する
- 承認しなくては必要なアクセス権限が存在する
- 業務上不要となる、過大な権限が付与されている
- 適切な職務分離(SOD)が維持されていない
- M/Sワードが定期的に変更されないまたは、教習で容易に複製される
- アクセスが適時にモニタリングされていない

### ③内部統制高度化の知見

内部統制の高度化に多くの知見を有しています

内部統制文書の整備、評価の過程で発見した内部統制の課題「リスクのある統制処理」「非効率/効率化の余地のある統制」「電子化の可能性」「効果的な評価」等余地がある点について、課題提起が可能です

代表的な発見事項と会社に求められる対応

発見事項	会社に求められる対応
全ての処理が実行できる権限が一般ユーザを含めたユーザに付与されている	【暫定対応】 権限過剰なユーザが存在する場合、実施ログの抽出と監査人への説明 ・権限の引き上げの低い設定場になっている場合、アクセス権限を削減して適切な権限の抽出と監査人への説明
調査検証のためのデバッグ権限が本番環境で一般ユーザに付与されている	【暫定対応】 権限を適正化するための検討、影響調査・テスト ・デバッグ権限を適正化するための検討、影響調査・テスト
本番環境において、プログラムを直接作成・変更を可能な設定となっている	【暫定対応】 権限を適正化するための検討、影響調査・テスト ・デバッグ権限を適正化するための検討、影響調査・テスト
該権限のデフォルトユーザの初期パスワードが変更されておらず、不正にログインされる可能性のある状態である	【暫定対応】 権限を適正化するための検討、影響調査・テスト ・デバッグ権限を適正化するための検討、影響調査・テスト

**Point** 不備が発見された場合、実施ログの抽出・監査人への説明などの暫定対応に加え、権限・設定値の適正化の検討、影響調査などの恒久的対応もあり、会社には多くの自対応が求められます。

※貴社および貴社との関係会社とデロイト トーマツ グループの関係において監査人としての独立性が要求される場合、本サービス内容が提供できない可能性があります。詳細はお問合わせください。

# Deloitte. トーマツ.

## デロイト トーマツ

デロイト トーマツグループは、日本におけるデロイト アジア パシフィック リミテッドおよびデロイト ネットワークのメンバーであるデロイト トーマツ 合同会社ならびにそのグループ法人（有限責任監査法人 トーマツ、デロイト トーマツ リスク アドバイザリー 合同会社、デロイト トーマツ コンサルティング 合同会社、デロイト トーマツ ファイナンシャル アドバイザリー 合同会社、デロイト トーマツ 税理士 法人、DT 弁護士 法人およびデロイト トーマツ グループ 合同会社を含む）の総称です。デロイト トーマツ グループは、日本で最大級のプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従いプロフェッショナルサービスを提供しています。また、国内約30都市に2万人超の専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループ Web サイト、[www.deloitte.com/jp](http://www.deloitte.com/jp) をご覧ください。

Deloitte（デロイト）とは、デロイト トウシュ トーマツ リミテッド（“DTTL”）、そのグローバルネットワーク組織を構成するメンバーファームおよびそれらの関係法人（総称して“デロイト ネットワーク”）のひとつまたは複数数を指します。DTTL（または“Deloitte Global”）ならびに各メンバーファームおよび関係法人はそれぞれ法的に独立した別個の組織体であり、第三者に関して相互に義務を課しまたは拘束させることはありません。DTTL および DTTL の各メンバーファームならびに関係法人は、自らの作為および不作為についてのみ責任を負い、互いに他のファームまたは関係法人の作為および不作為について責任を負うものではありません。DTTL はクライアントへのサービス提供を行いません。詳細は [www.deloitte.com/jp/about](http://www.deloitte.com/jp/about) をご覧ください。

デロイト アジア パシフィック リミテッドはDTTLのメンバーファームであり、保証有限責任会社です。デロイト アジア パシフィック リミテッドのメンバーおよびそれらの関係法人は、それぞれ法的に独立した別個の組織体であり、アジア パシフィック における100を超える都市（オークランド、バンコク、北京、ベンガルール、ハノイ、香港、ジャカルタ、クアラルンプール、マニラ、メルボルン、ムンバイ、ニューデリー、大阪、ソウル、上海、シンガポール、シドニー、台北、東京を含む）にてサービスを提供しています。

Deloitte（デロイト）は、最先端のプロフェッショナルサービスを、Fortune Global 500®の約9割の企業や多数のプライベート（非公開）企業を含むクライアントに提供しています。デロイトは、資本市場に対する社会的な信頼を高め、クライアントの変革と繁栄を促進することで、計測可能で継続性のある成果をもたらすプロフェッショナルの集団です。デロイトは、創設以来180年の歴史を有し、150を超える国・地域にわたって活動を展開しています。“Making an impact that matters”をバース（存在理由）として標榜するデロイトの約46万人の人材の活動の詳細については、[www.deloitte.com](http://www.deloitte.com) をご覧ください。

本資料は皆様への情報提供として一般的な情報を掲載するのみであり、デロイト トウシュ トーマツ リミテッド（DTTL）、そのグローバルネットワーク組織を構成するメンバーファームおよびそれらの関係法人（総称して“デロイト ネットワーク”）が本資料をもって専門的な助言やサービスを提供するものではありません。皆様の財務または事業に影響を与えるような意思決定または行動をされる前に、適切な専門家にご相談ください。本資料における情報の正確性や完全性に関して、いかなる表明、保証または確約（明示・黙示を問いません）をするものではありません。またDTTL、そのメンバーファーム、関係法人、社員・職員または代理人のいずれも、本資料に依拠した人に関係して直接または間接に発生し得る損失および損害に対して責任を負いません。DTTLならびに各メンバーファームおよび関係法人はそれぞれ法的に独立した別個の組織体です。

Member of  
**Deloitte Touche Tohmatsu Limited**

© 2025. For information, contact Deloitte Tohmatsu Group.



IS 669126 / ISO 27001



BCMS 764479 / ISO 22301

IS/BCMSそれぞれの認証範囲はこちらをご覧ください  
<http://www.bsigroup.com/clientDirectory>