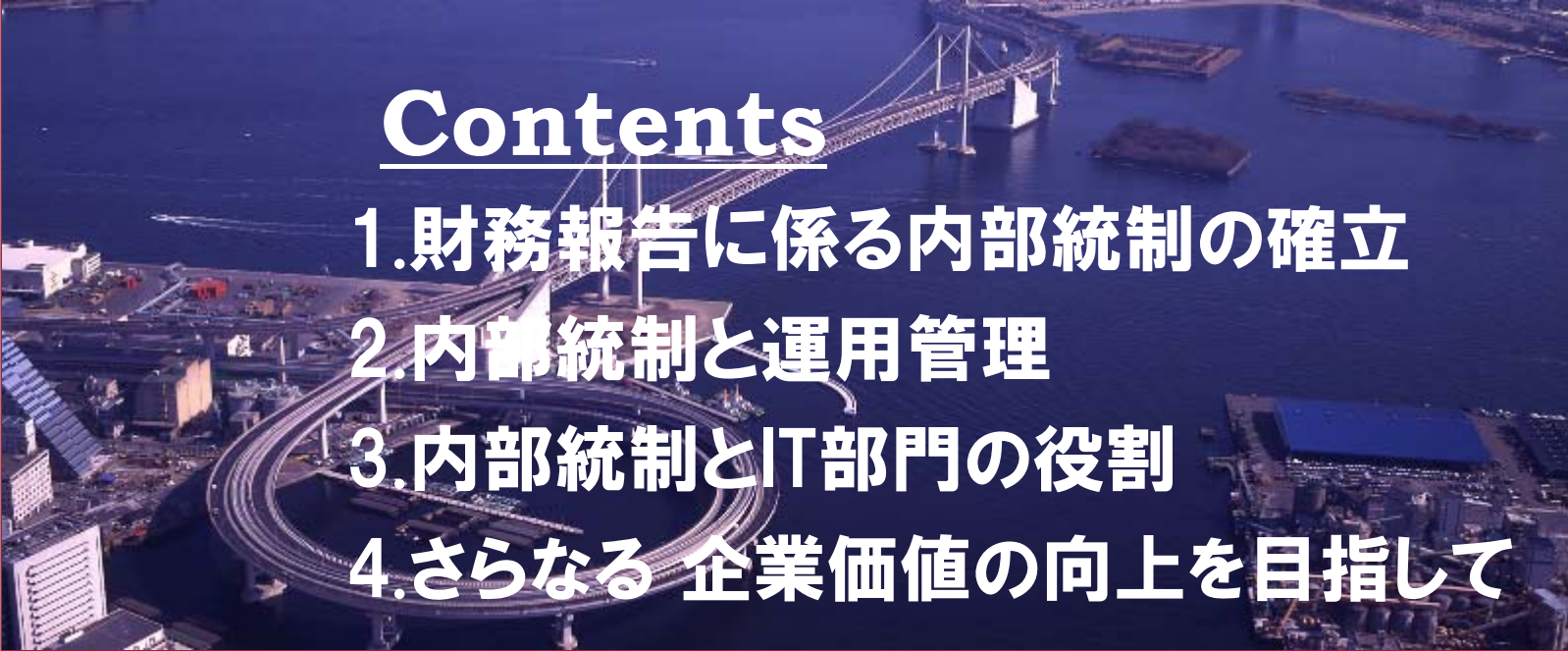


内部統制のために運用管理者は 何をすべきか？



(株) 日立コンサルティング
テクニカルディレクター
伊藤泰樹

2007年6月6日



Contents

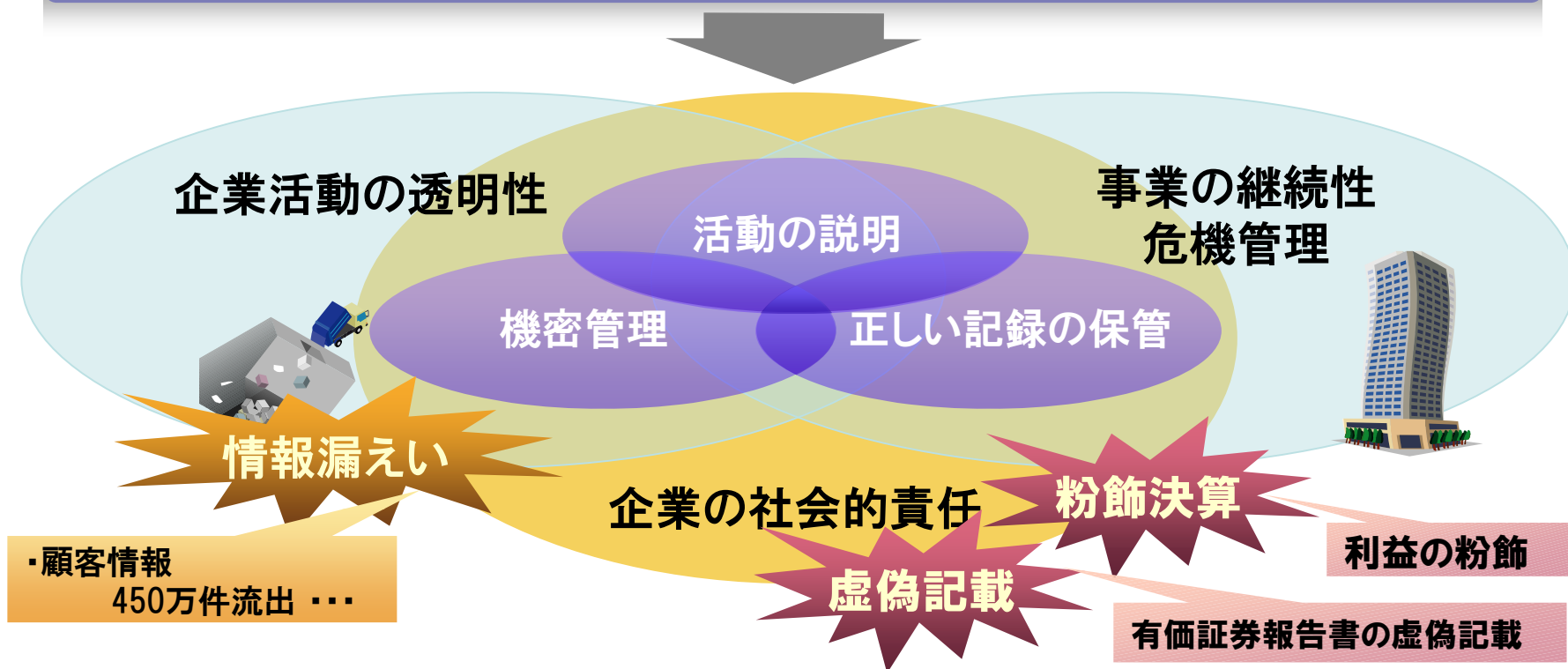
- 1.財務報告に係る内部統制の確立
- 2.内部統制と運用管理
- 3.内部統制とIT部門の役割
- 4.さらなる 企業価値の向上を目指して

1 財務報告に係る内部統制の確立



企業活動の社会責任

—企業倫理・営利追求—



「内部統制」について体系的・網羅的に評価して
外部に**説明**できるようにすることが新たに求められる

財務報告の信頼性から見た統制の全体像

統制(コントロール)事前対策によりリスクを防ぐ

規則/手順の指示

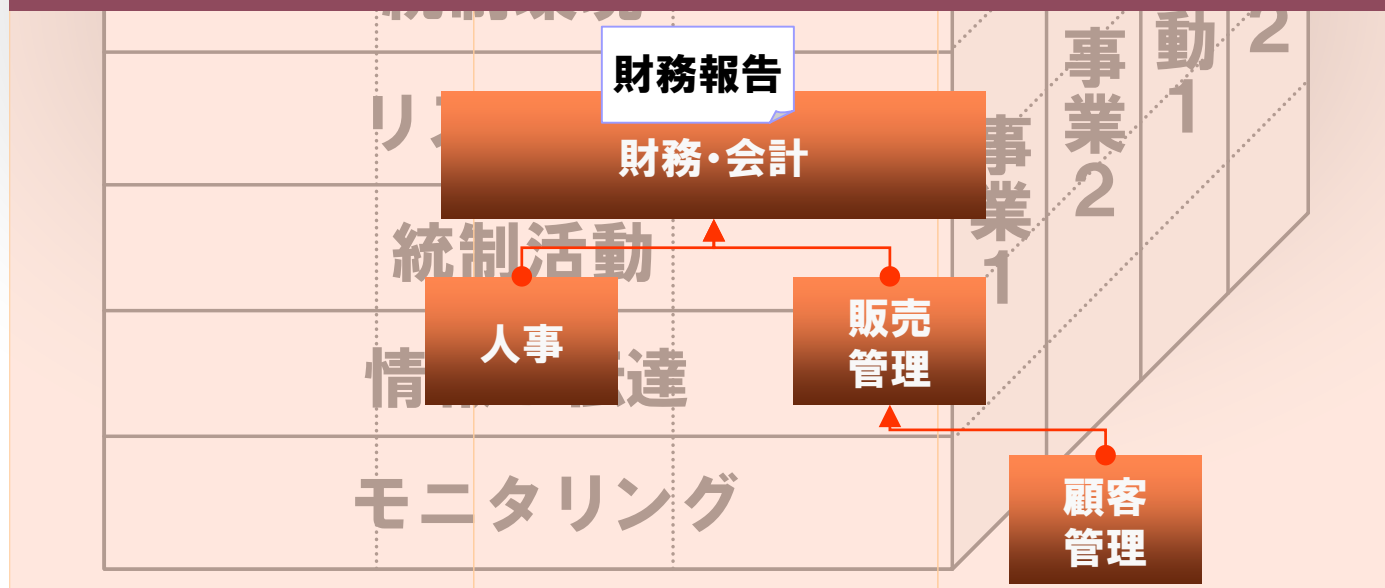
規則通り業務/活動が行われていることに関する組織的活動



業務の有効性と効率

財務報告の信頼

法令の遵



全社的な内部統制
連結ベースの財務報告全体に影響を及ぼす内部統制

全社的な内部統制

全社的な統制

統制環境

リスクの評価と対応

統制活動

情報と伝達

モニタリング

ITへの対応

適切な統制が全社的に機能しているかどうか心証を得る。

それに基づき、虚偽記載につながるリスクに着眼して業務プロセスに係る内部統制を評価。

業務プロセスに係る内部統制

業務プロセスに係る内部統制

業務プロセスに組み込まれ一体となって遂行される内部統制

財務報告における記載内容の適正性

・組織構造及び慣行・権限及び職責・人的資源に対する方針と管理

ITに係る統制

担保する

業務処理統制

入力情報の完全性、正確性、正当性等を確保する統制

例外処理(エラー)の修正と再処理

マスタ・データの維持管理

システムの利用に関する認証、操作範囲の限定などアクセスの管理

担保する

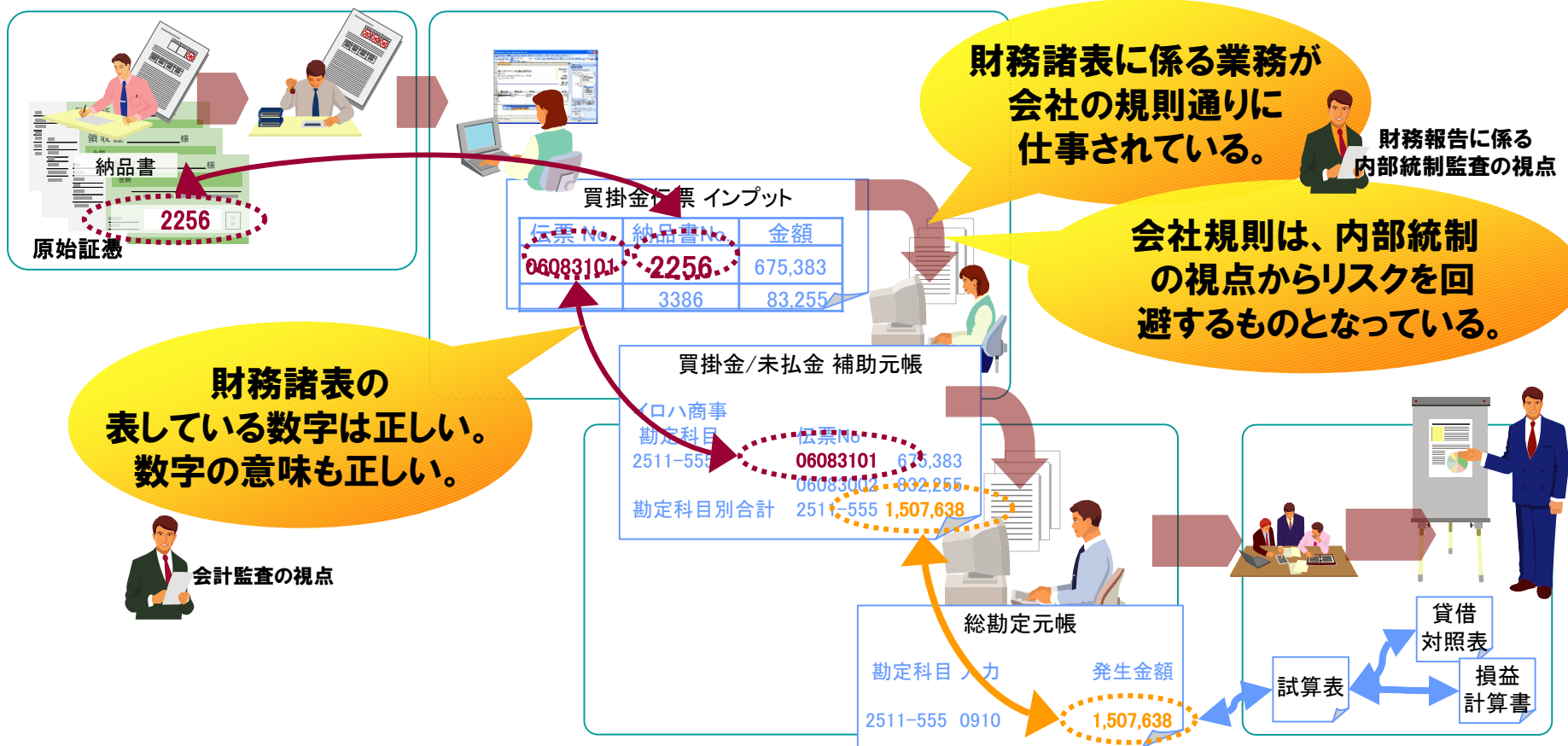
IT全般統制

ITの開発、保守に係る管理

システムの運用・管理

内外からのアクセス管理などシステムの安全性の確保

外部委託に関する契約の管理



内部統制監査(業務監査) 財務報告に係る業務の正当性を説明する

内部統制を説明するために。。。

業務を可視化(説明するための文書化)

文書化されたとおりに業務が遂行できていることを説明するための記録

統制された業務展開している
ことを説明

正当な行動の説明

財務諸表に係る業務が
会社の規則通りに
仕事されている。

会社規則は、内部統
制の視点からリスク
を回避するものとなっ
ている。

規則・規定

規則・規定の正当性の
説明

行動原則の説明

業務記述書

業務フローの明示

リスクコントロールマ
トリックスの明示

行動の記録

帳簿

証憑

稟議の記録

突合せなどによる
監査記録

データのログの取得と
監査

アプリケーション
データの流れ

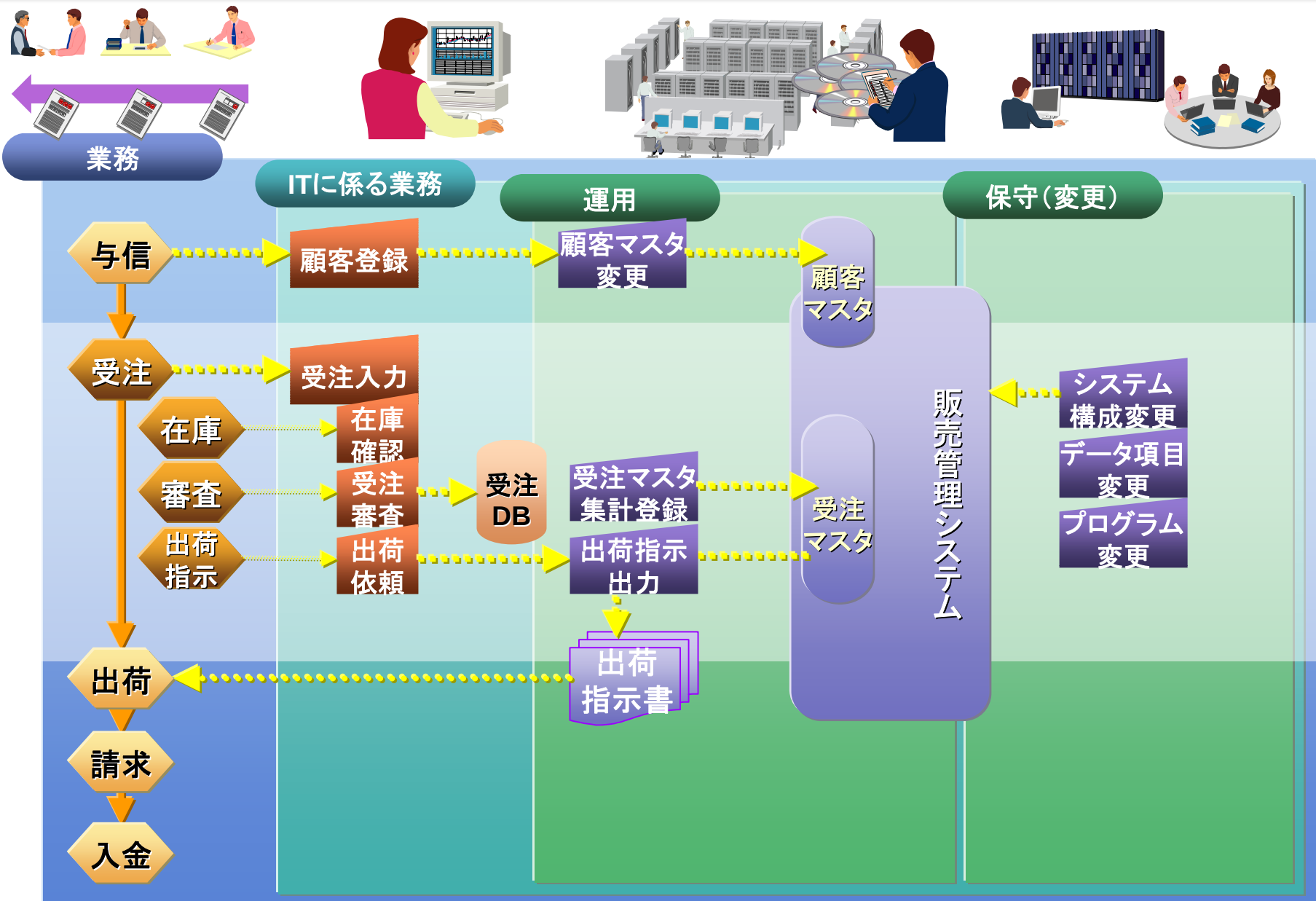
情報システム運用の正当性

日常業務の記録
規定された仕事の手順を踏んでいる説明

行動記録の説明

2 内部統制と運用管理 ーシステムの運用・保守・開発と統制の関係ー





業務プロセスに係る内部統制

✓業務を開始し、記帳していく流れ。その中で、システムの運用は業務の一貫として操作される。

開始

承認

記録

処理

報告

業務プロセスに係る内部統制

業務プロセスに組み込まれ一体となって遂行される内部統制

財務報告における記載内容の適正性

・組織構造及び慣行・権限及び職責・人的資源に対する方針と管理

ITに係る統制

担保する

業務処理統制

入力情報の完全性、正確性、正当性等を確保する統制

例外処理(エラー)の修正と再処理

マスタ・データの維持管理

システムの利用に関する認証、操作範囲の限定などアクセスの管理

担保する

ITの開発、保守に係る管理

システムの運用・管理

内外からのアクセス管理などシステムの安全性の確保

外部委託に関する契約の管理

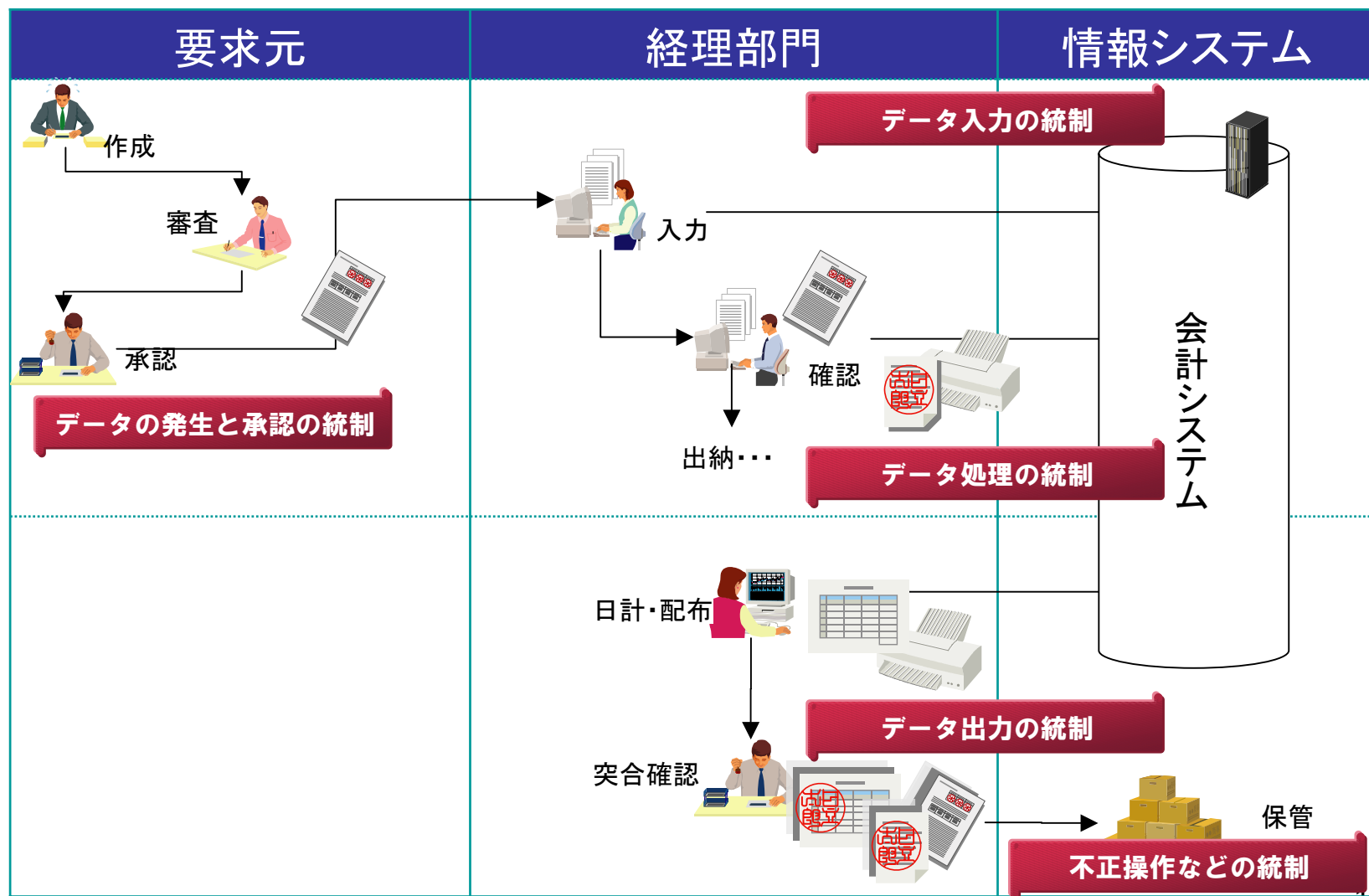


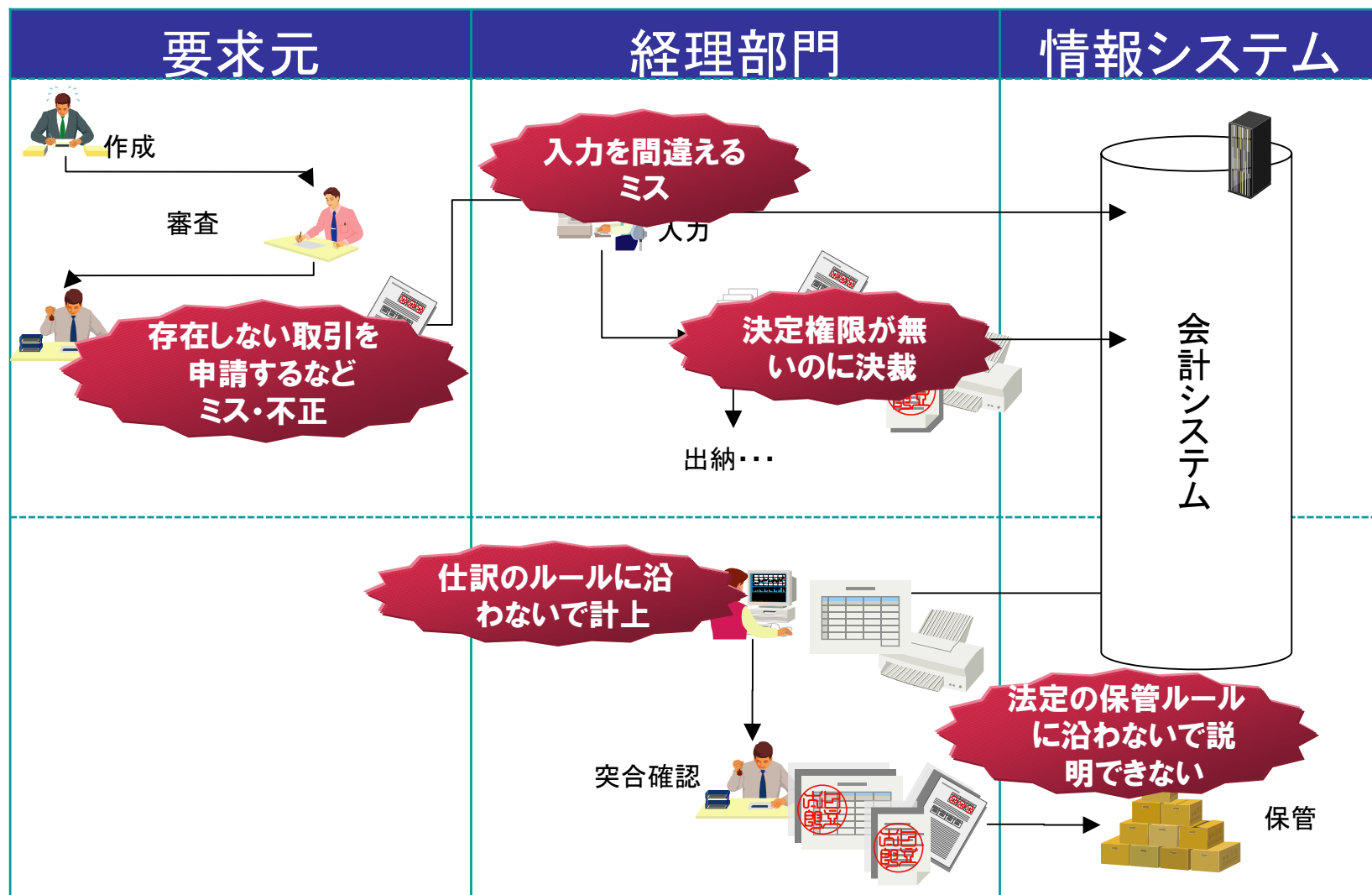
2 業務処理の中で実行すべき統制の例

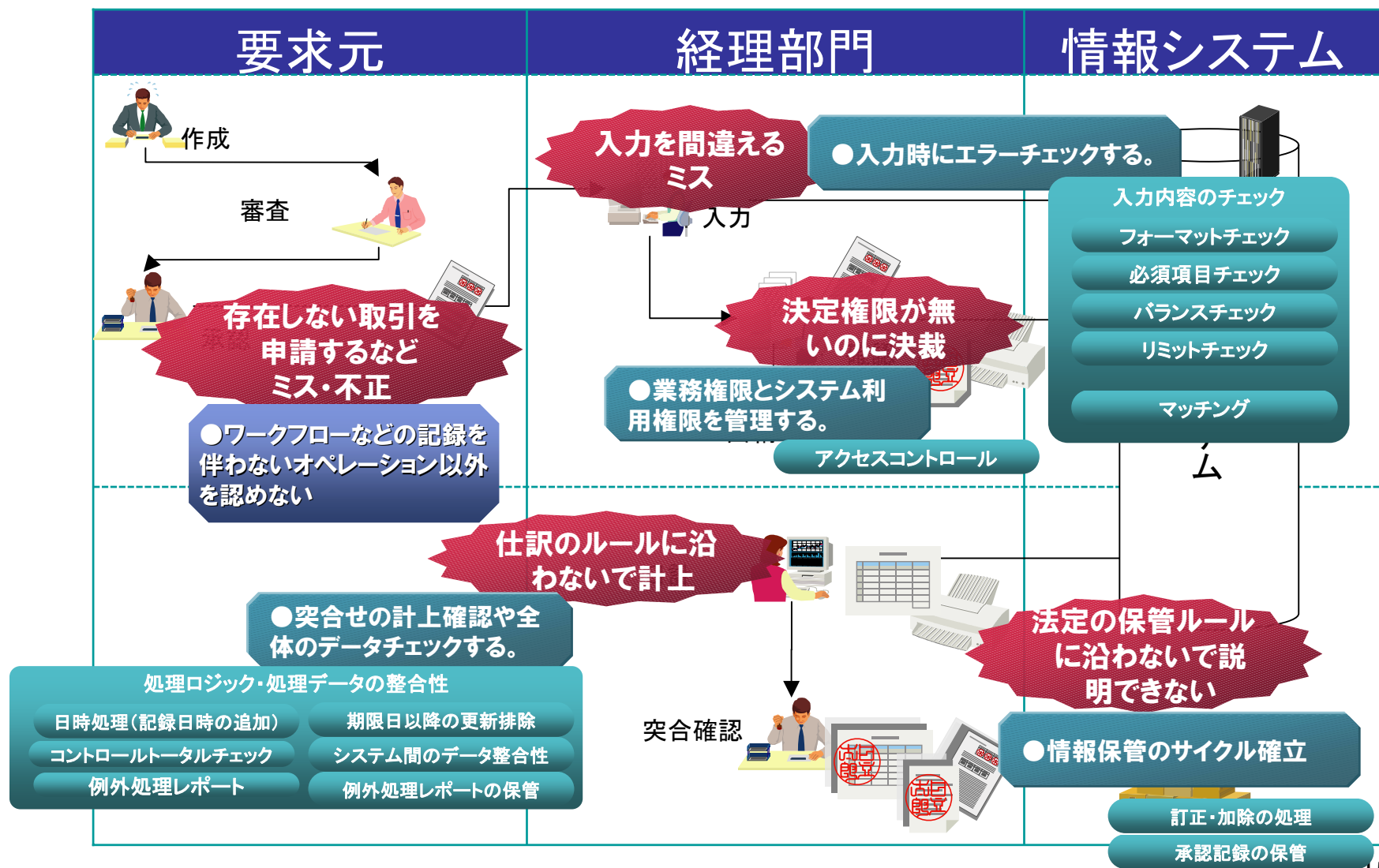
- 業務処理の中では次のような統制によりリスクを排除している。

コントロールの種類	内容
照合/調整	2つの項目(数値)が一致あるいは整合しているかどうかを確認する統制
承認/決裁	定められた方針や手続に従って、承認権限者が取引の実行や処理の開始等を許可・決裁する行為
管理者によるレビュー	作業を実施した者以外の者で、その作業を分析/監査する立場にある者が行う分析や監視。(相互レビューも含む)
予算/指標対比	管理者が、予算比または前年比等の指標を使用して、目的達成の進捗状況の評価、異常値等を抽出すること。
職務の分離	誤謬や不正行為の発生及び隠蔽を防ぐために、職務分掌及び職務権限を適切にする統制。

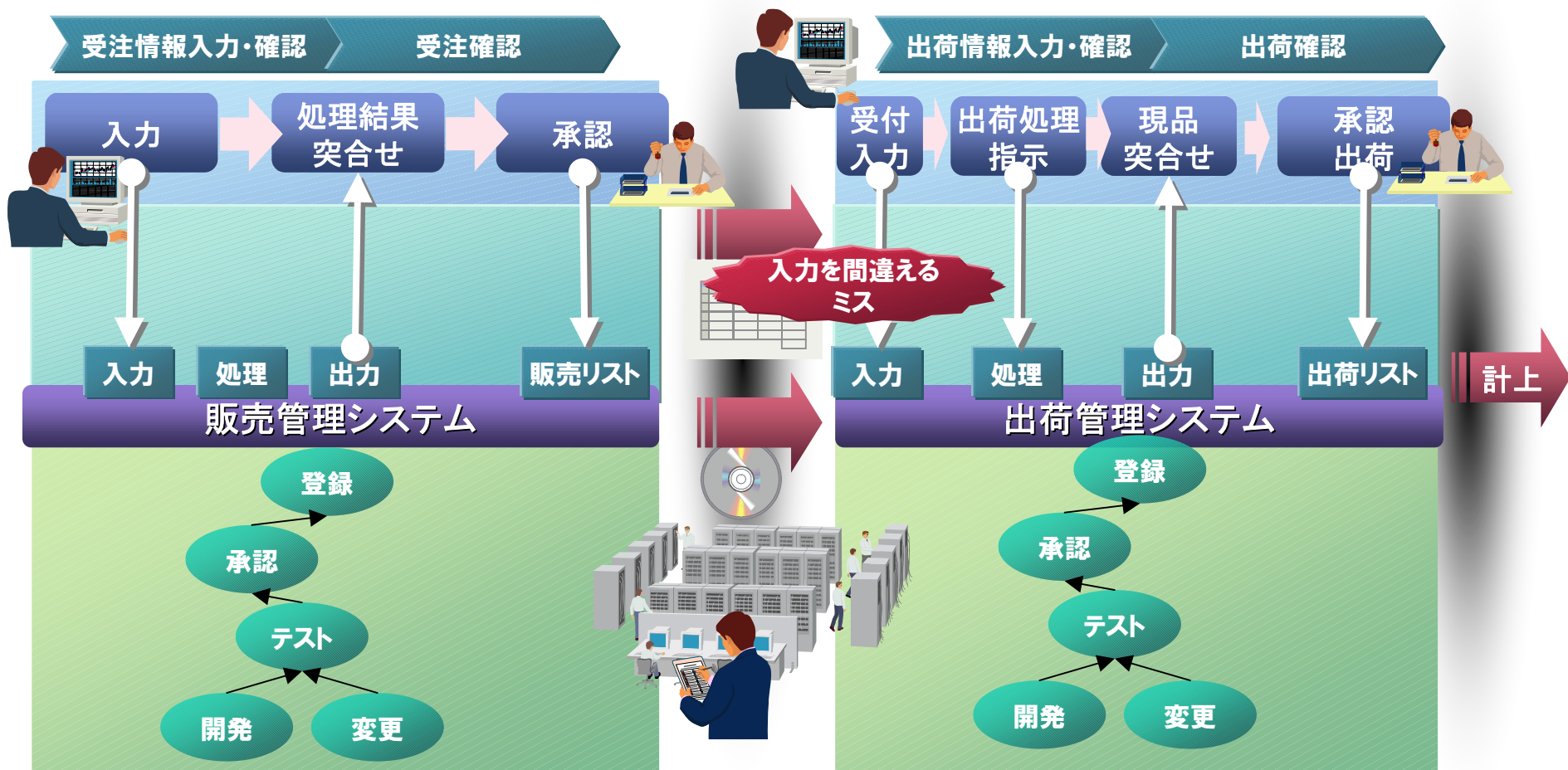
2 日常で必要になる業務とITの関係(例)



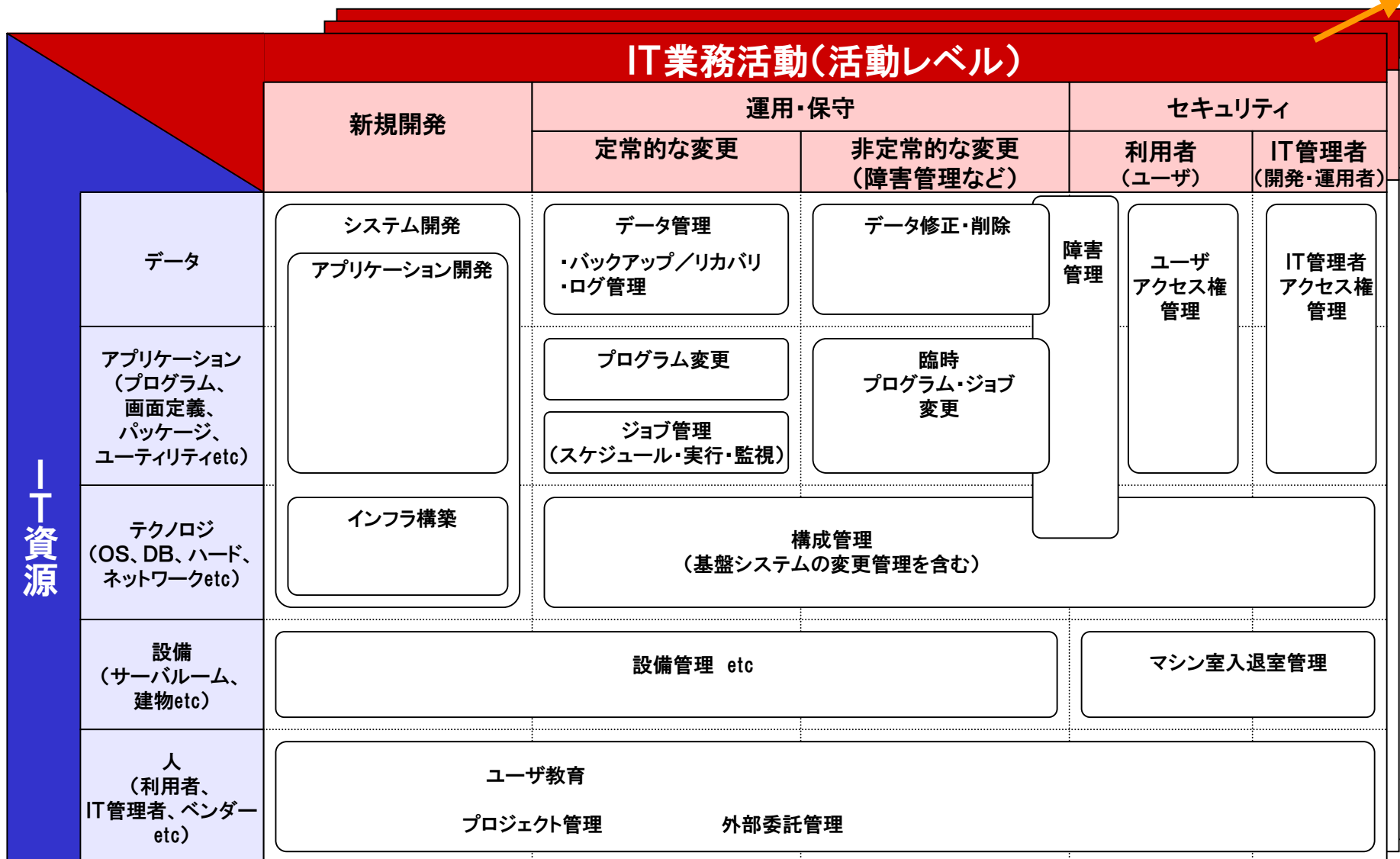


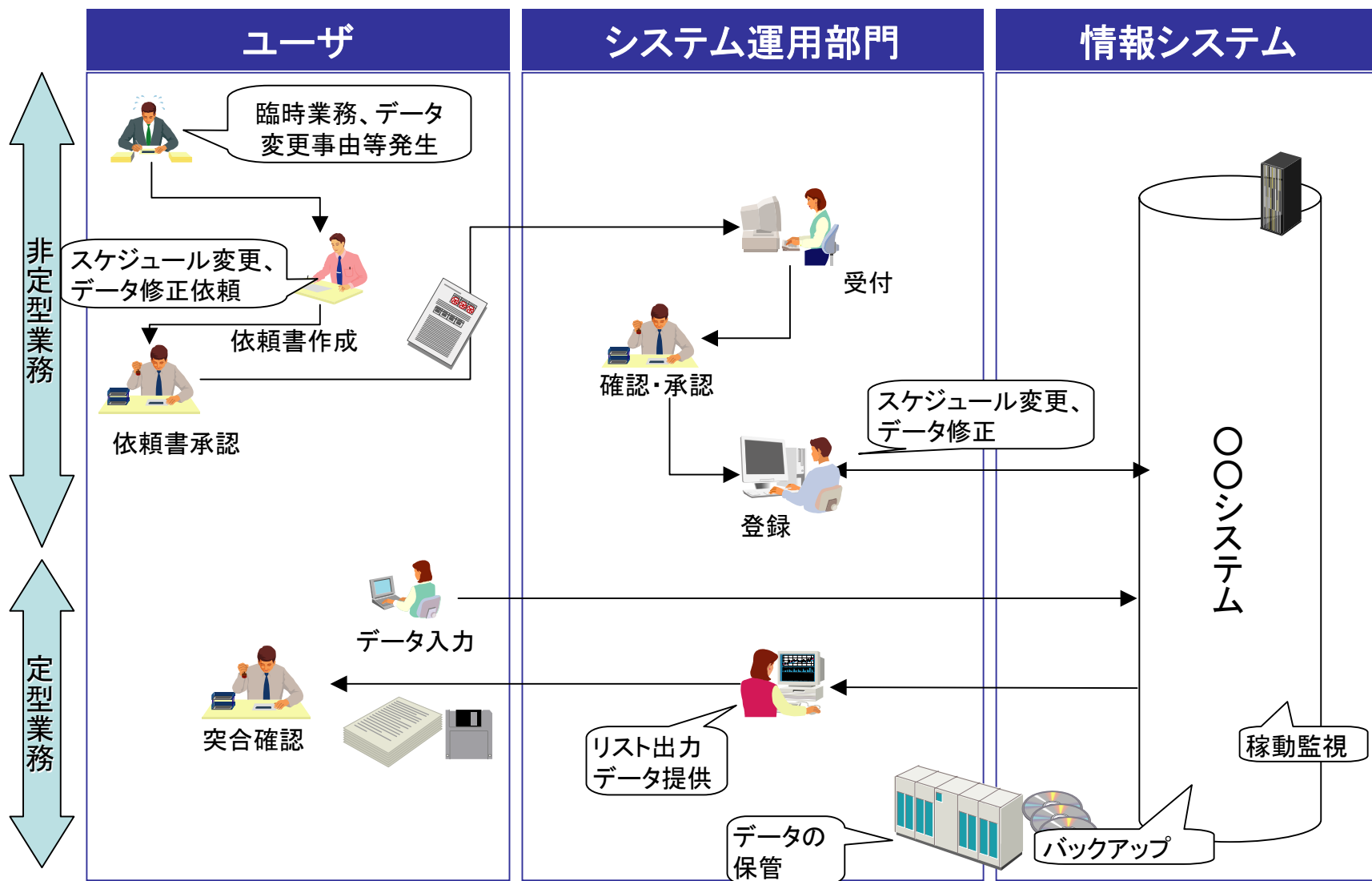


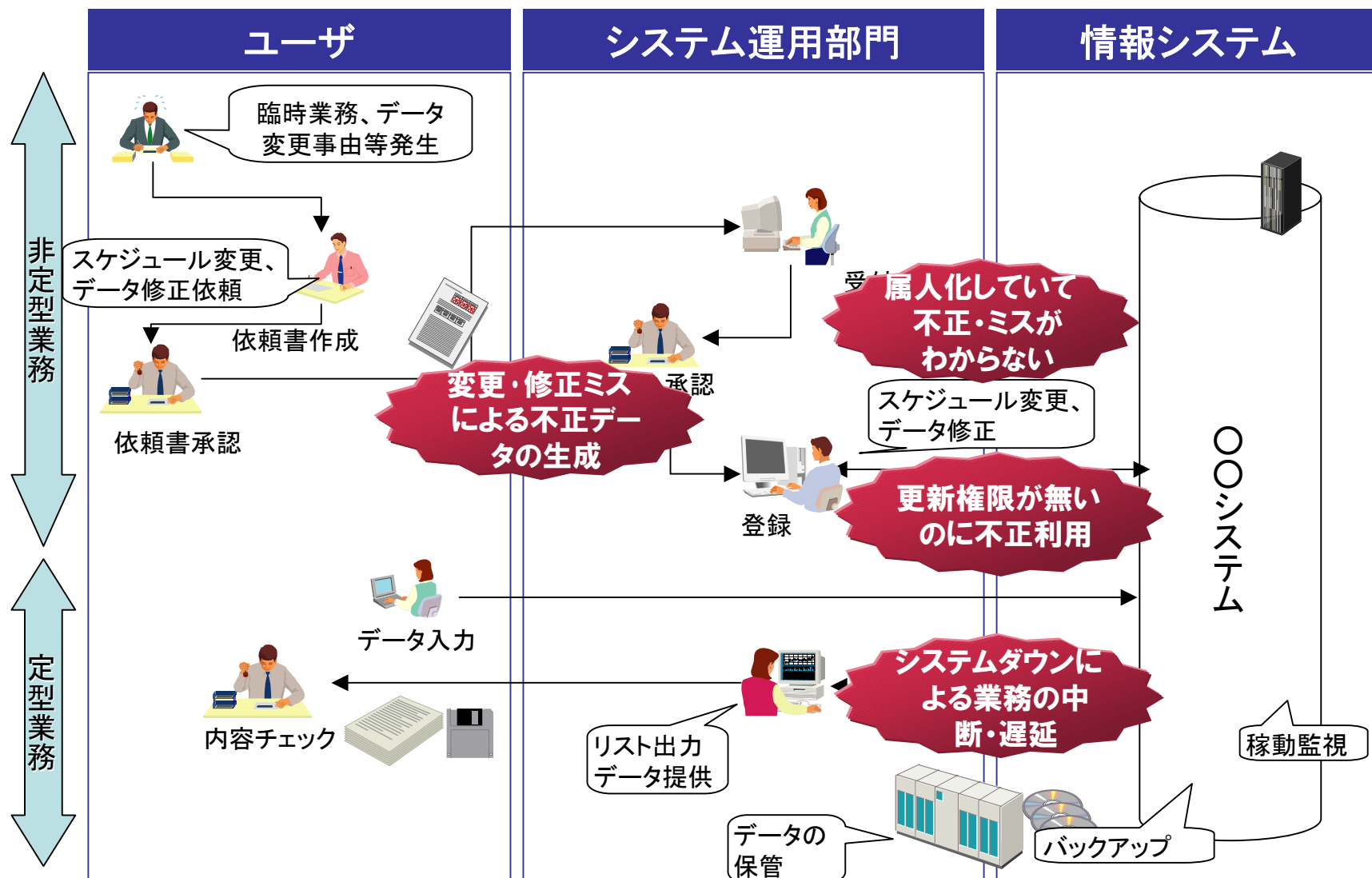
✓部門をまたがった処理に関しては、「データの再入力」など業務の分断される場所にリスクが入り込みやすいと言われる。

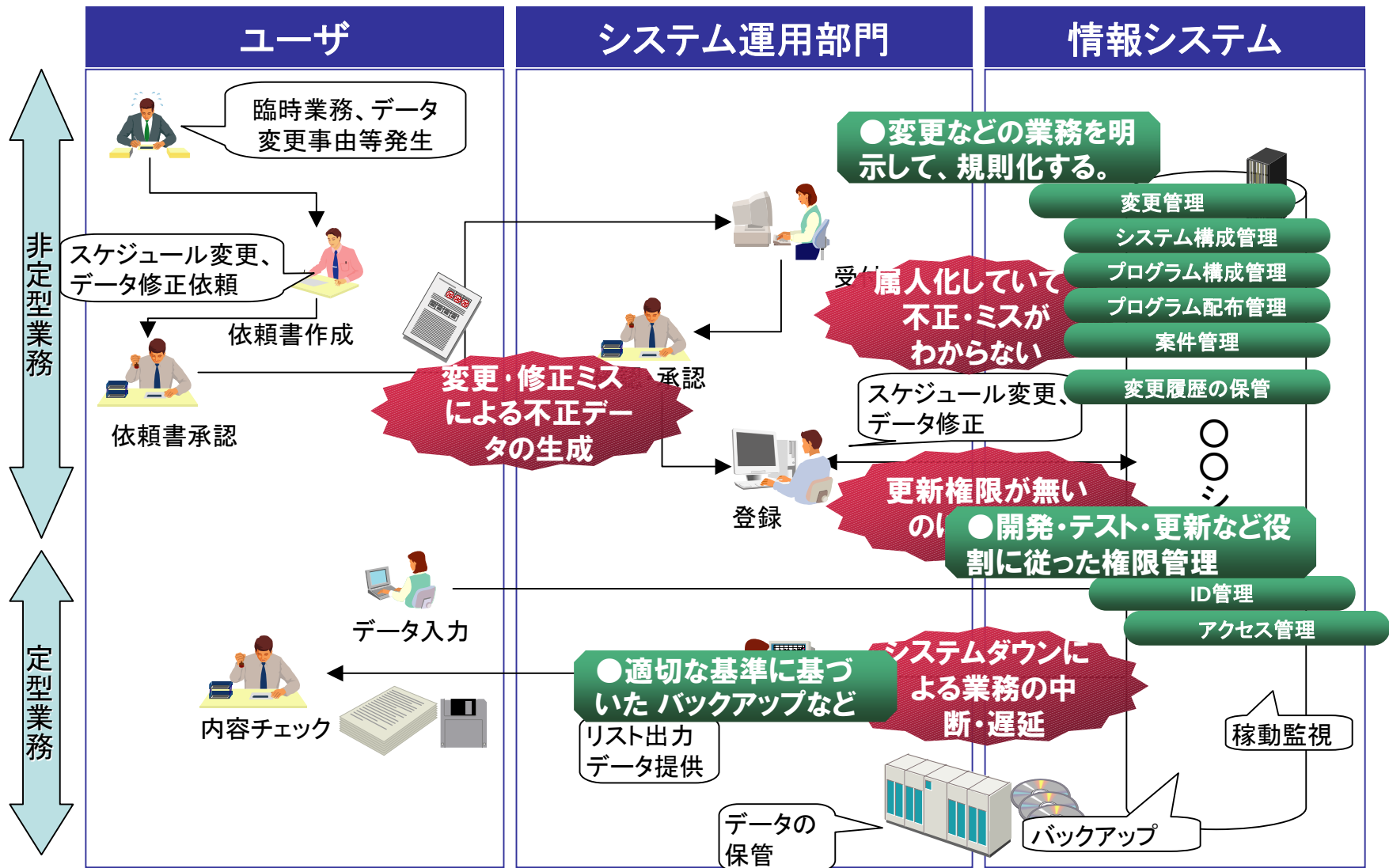


※システム稼働環境単位(ホスト・サーバなどに複数存在)

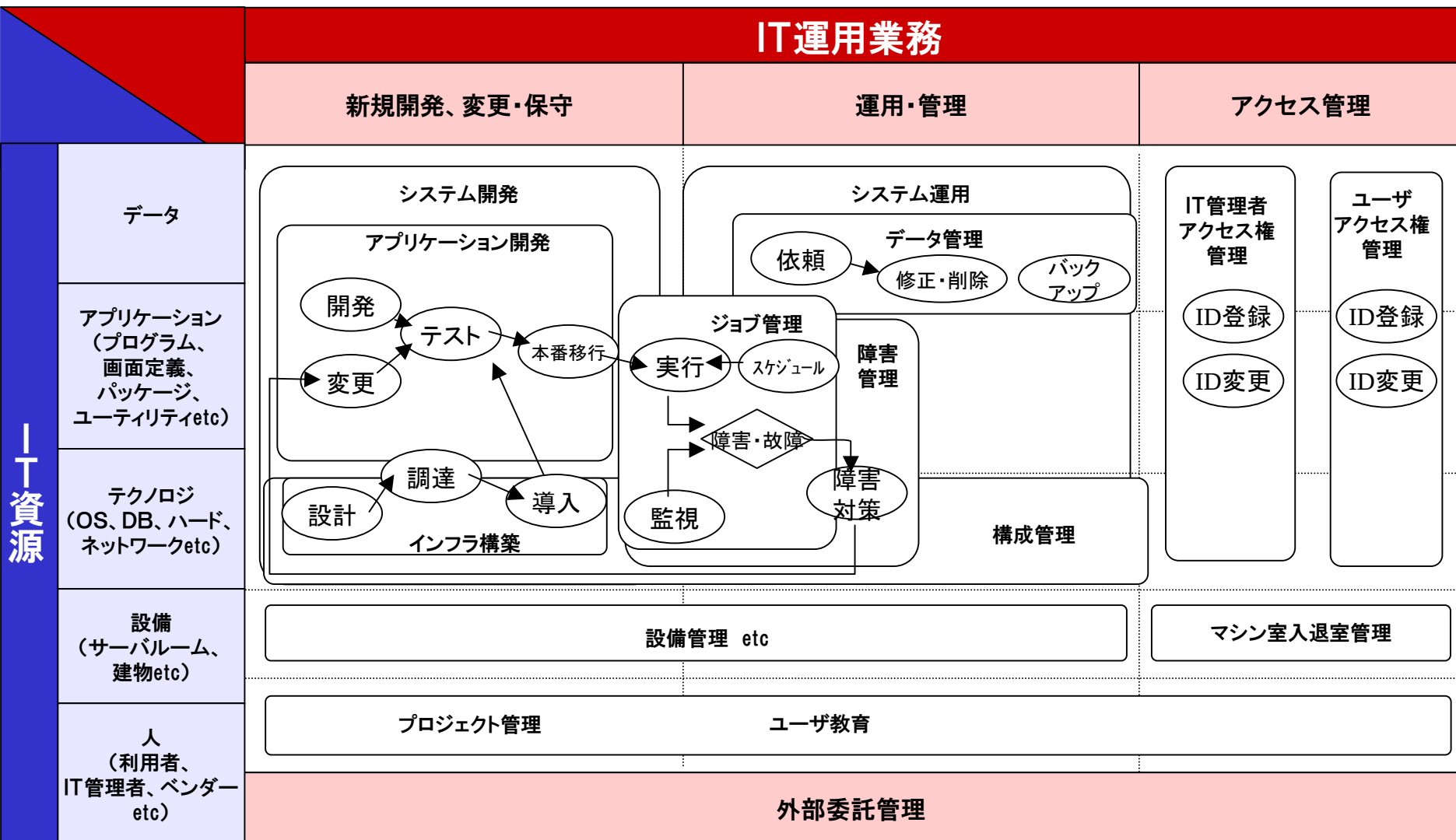




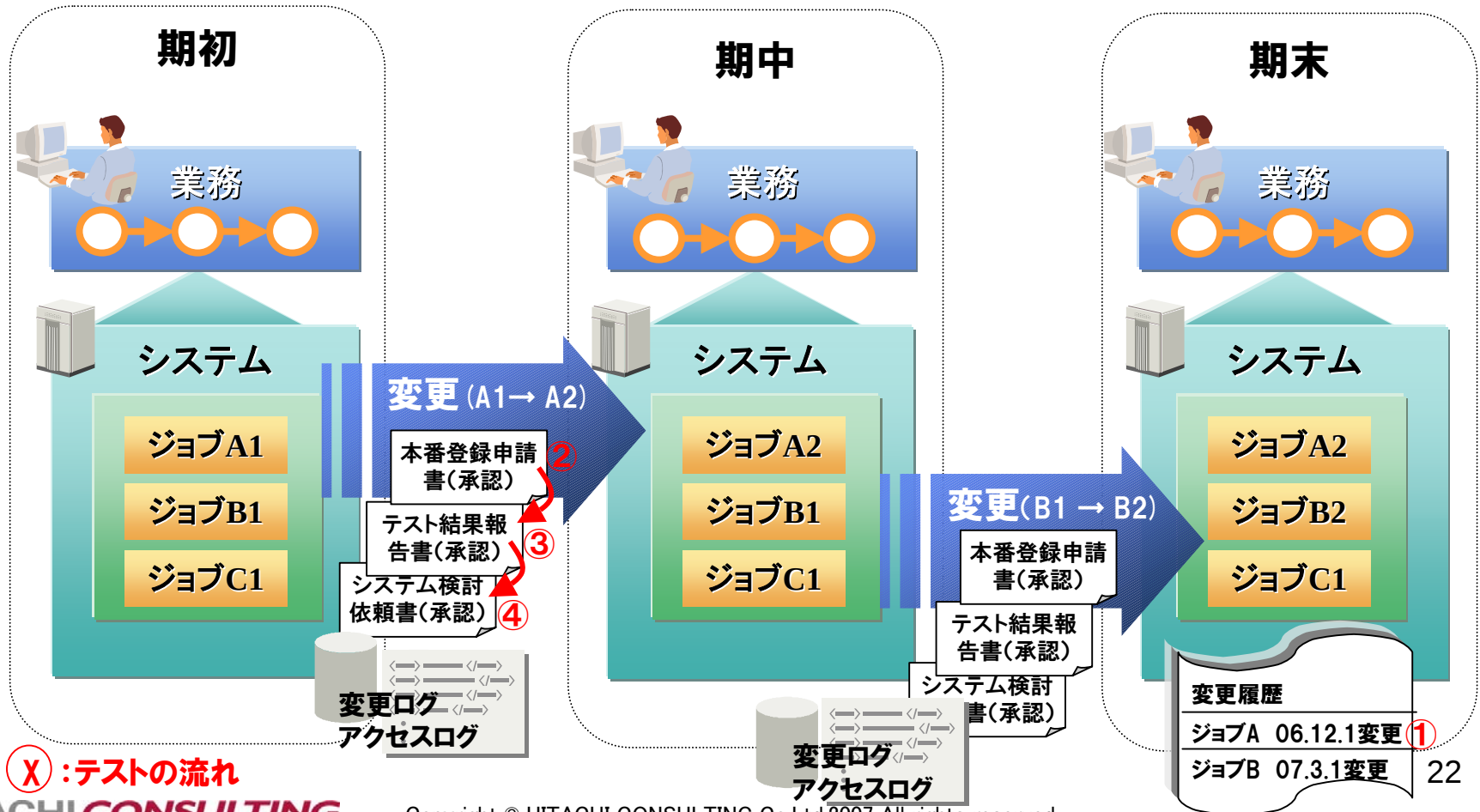




□ :IT運用業務 ○ :作業



- システムの動作や保守・運用が業務処理の統制に影響が無いことを示すことがIT全般統制である。
IT全般統制で必要になる証跡は、ITシステムの保守・変更に伴う行為が正当な理由に基づいて、正確に実行されたことを第三者(監査人など)に説明をする目的を持つ。
- ジョブの保守(変更)の例では、「ジョブの変更理由となる依頼書」、「依頼に基づいて、変更をした記録」に加えて、正しく変更したことを示すことができるように「システムから出力することができる システムの変更記録」が有用である。監査する視点では、該当の期間での変更の総量(回数)や変更の一覧から変更の記録をたどって正確・正当な変更作業されたことを突き合わせていく。



業務処理統制

データの発生と承認の統制

原始証憑の承認手続き

原始証憑のデータ収集

原始証憑のエラー取扱い

原始証憑の保管

ITに係る業務処理統制

データ入力
の統制

入力内容のチェック

フォーマットチェック

必須項目チェック

バランスチェック

リミットチェック

マッチング

プログラム

データ

マスターデータ

マスター変更管理

データ処理の
統制

処理ロジック・処理データの整合性

日時処理(記録日時の追加)

期限日以降の更新排除

コントロールトータルチェック

システム間のデータ整合性

例外処理レポート

例外処理レポートの保管

訂正・加除の処理

承認記録の保管

アクセスコントロール

IT全般統制

IT部門の統制

開発管理

変更管理

システム構成管理

プログラム構成管理

プログラム配布管理

案件管理

変更履歴の保管

運用(バッチ処理など)

ID管理

アクセス管理

業務プロセス統制: 個々の業務において網羅性・正確性・正当性・維持持続性を確保する。

アプリケーション統制: 個々の業務アプリケーションにおいて使用されるデータの網羅性・正確性・正当性・維持持続性を確保する。

IT全体統制: 業務プロセス統制の健全性が維持できるように、ITインフラを統制する。IT戦略、企画、開発、取得、運用、保守およびそれらを維持する制度など。

ITに係る業務処理統制

- 業務に関する「規則・基準」のシステムへの織り込み（確認）
- 部門間のデータ移転（転送）に関する運用の明示

IT全般統制

- システムの変更や更新に伴うリスクを排除する。
- 定常の仕事の中で必要な情報の認識を持つ

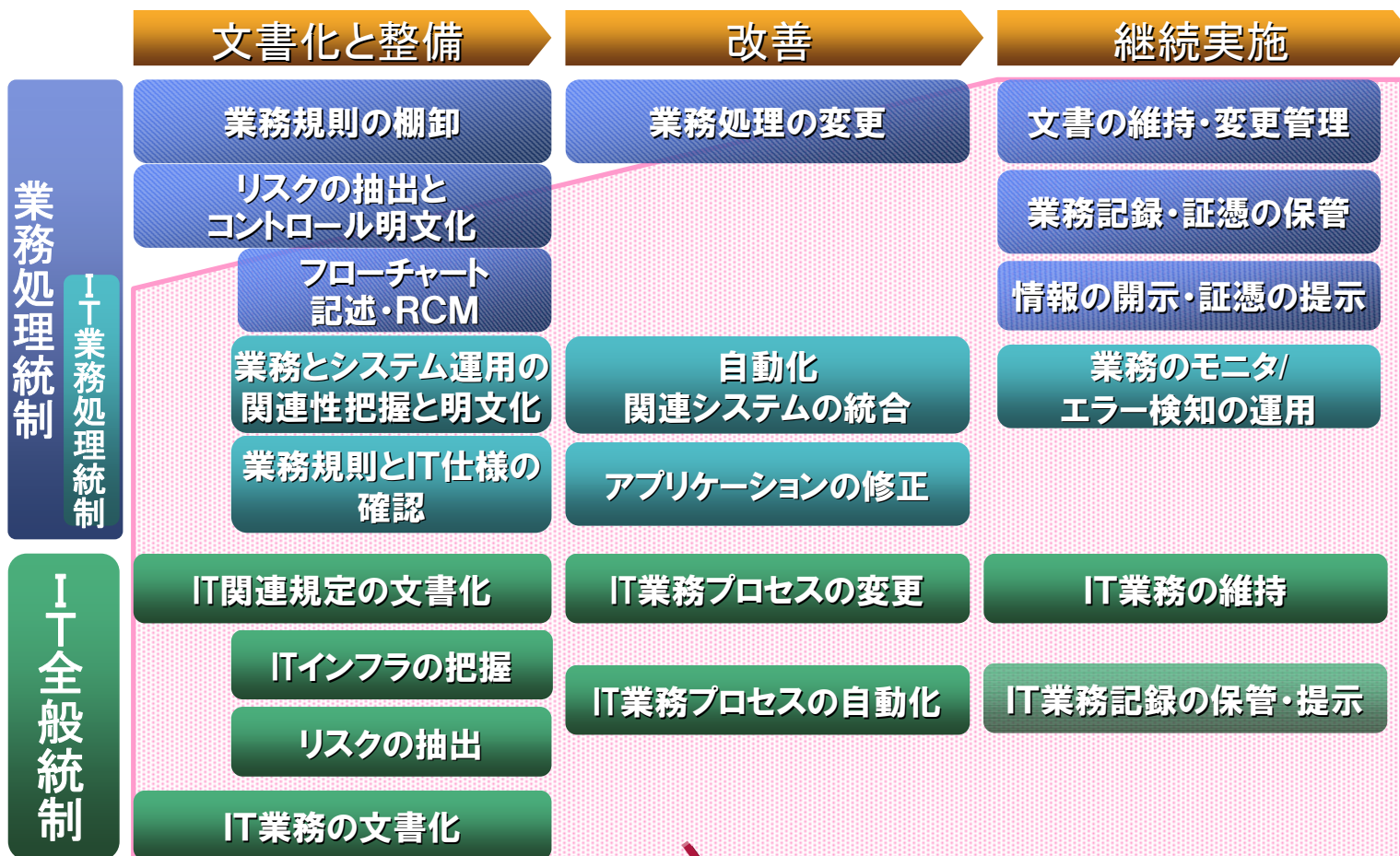
証跡（エビデンス）の維持

- バックアップの取得と証跡（エビデンス）の維持（IT部門に期待）

3 内部統制とIT部門の役割 －JSOXへの対応の本質－



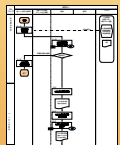
✓文書化の整備し、不備や根本の改善を実施していく場合や継続的に統制を実施する場合には、IT部門の関与する範囲が大きくなる。



IT部門の関与が必要な範囲

＜業務の見える化＞

- ・規定類の整備
- ・業務を明文化



→ リスクを把握

＜モニタリング＞

- ・証跡による、業務運用の証明
- ・不備の洗い出し



→運用上の不備を把握

不備の改善

文書化と整備で生まれる課題…

- ★ 部門を横断したカイゼンが必要だが
個別でやってしまう・・・

部門間で矛盾を備えたまま

全体最適 化が困難

- ★ 多量の証跡(管理文書)が各部門で発生、
各部門で保管

監査対応工数の増大

說明困難

- ## ★ 過剰な対応による運用上無理のある業務

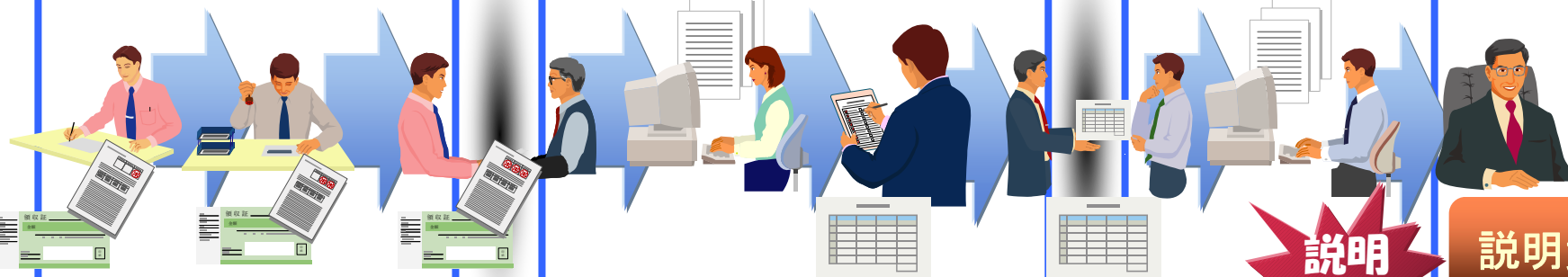
業務が形骸化、ルールが守られない

**リスクが
増大**

販売

会計

財務

説明
困難

説明責任

証跡や証拠の関連性が説明できない。見つからない。

全体最
適化が
困難リスクの多い場所での情報のやりとりが
「定型化」「標準化」「自動化」されていない。リスク
が増大

統制(予防的・発見的)の無理・無駄な適用による業務の破綻

内部統制が有効

財務報告に関わる業務に
ミスや不正がない

J-Sox対応前

熟練者が業務フローなしで対応
 ・業務フロー、承認処理が無くとも
 担当者が独自に最適な判断



“
統
制”

J-Sox対応後

明文化された業務フロー
 ・確実な承認処理、決められた業務
 フロー以外のやり方の禁止



財務リスクの低減は達成するが。…一方で 管理工数の増大（管理コストの増加）

・以前と比べて煩雑な
運用を強いられる



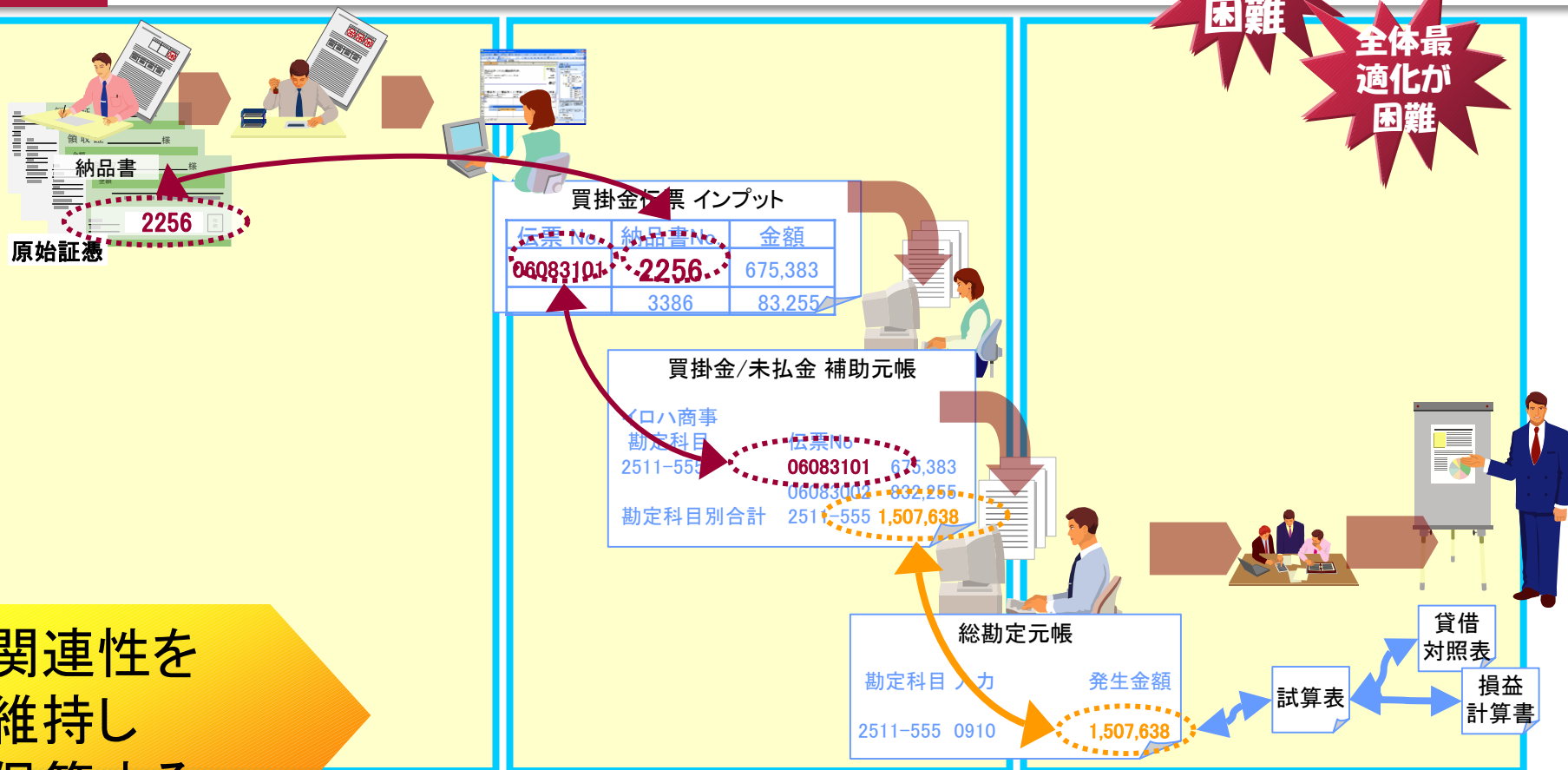
・増大する証跡等の保管



証跡を必ず残すための
膨大なドキュメント量

リスクが
増大

説明困難

説明
困難全体最
適化が
困難関連性を
維持し
保管する

帳簿

証憑

稟議の記録

突合せ記録

関連性を
維持し
保管する

縦割りの業務に横串を指す。

部門間の共通情報を管理する
ITが主体となつて

- ・システム・業務標準化
- ・データ・業務・権限
- ・共通化・統合
- ・関連業務の電子化推進

- ・必要証跡の確実な取得
- ・情報保管に対するポリシー
- ・ID,コードなど統一した管理

J-SOX対応で新たに生まれた課題

★ 部門を横断したカイゼンが必要だが
個別でやってしまう...



部門間で矛盾を備えたまま

全体最適
化が困難

★ 多量の証跡(管理文書)が各部門で
発生、各部門で保管



監査対応工数の増大

説明困難

★ 過剰な対応による運用上無理のある
業務



業務が形骸化

リスクが
増大

IT部門に課せられた課題

統治

- ・ガバナンスでの誘導(ITガバナンスを活用)
- ・IT部門主導で、業務データの統合やシステムの最適化

統合

- ・各部門依存となっている情報管理の方法をIT部門主導に誘導
- ・保管管理規定などから仕組みを提案

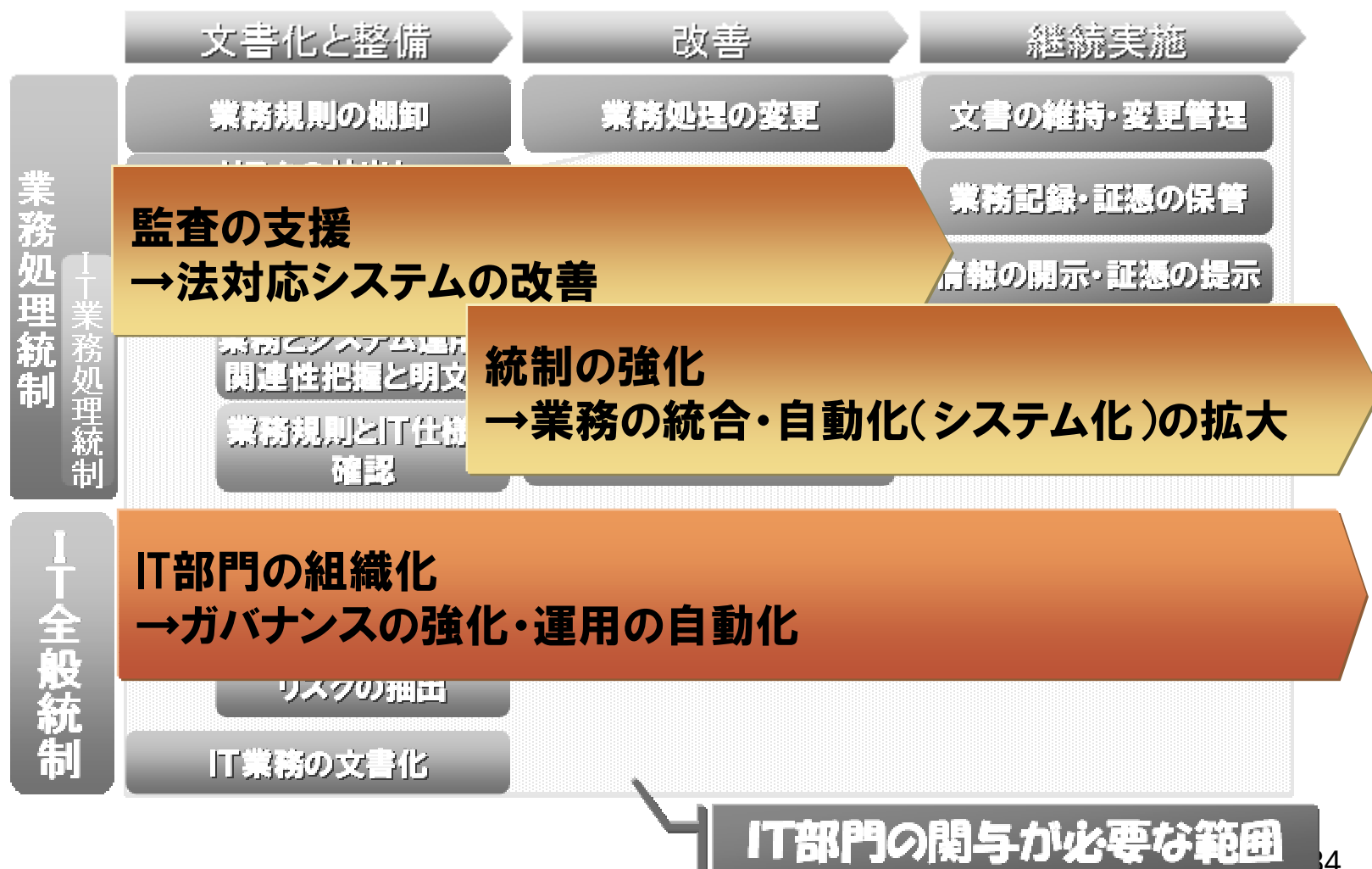
抗形骸化

- ・リスクの程度に合致した統制の見直し
- ・ワークフローの導入
- ・IT部門でのサービスデスクの導入

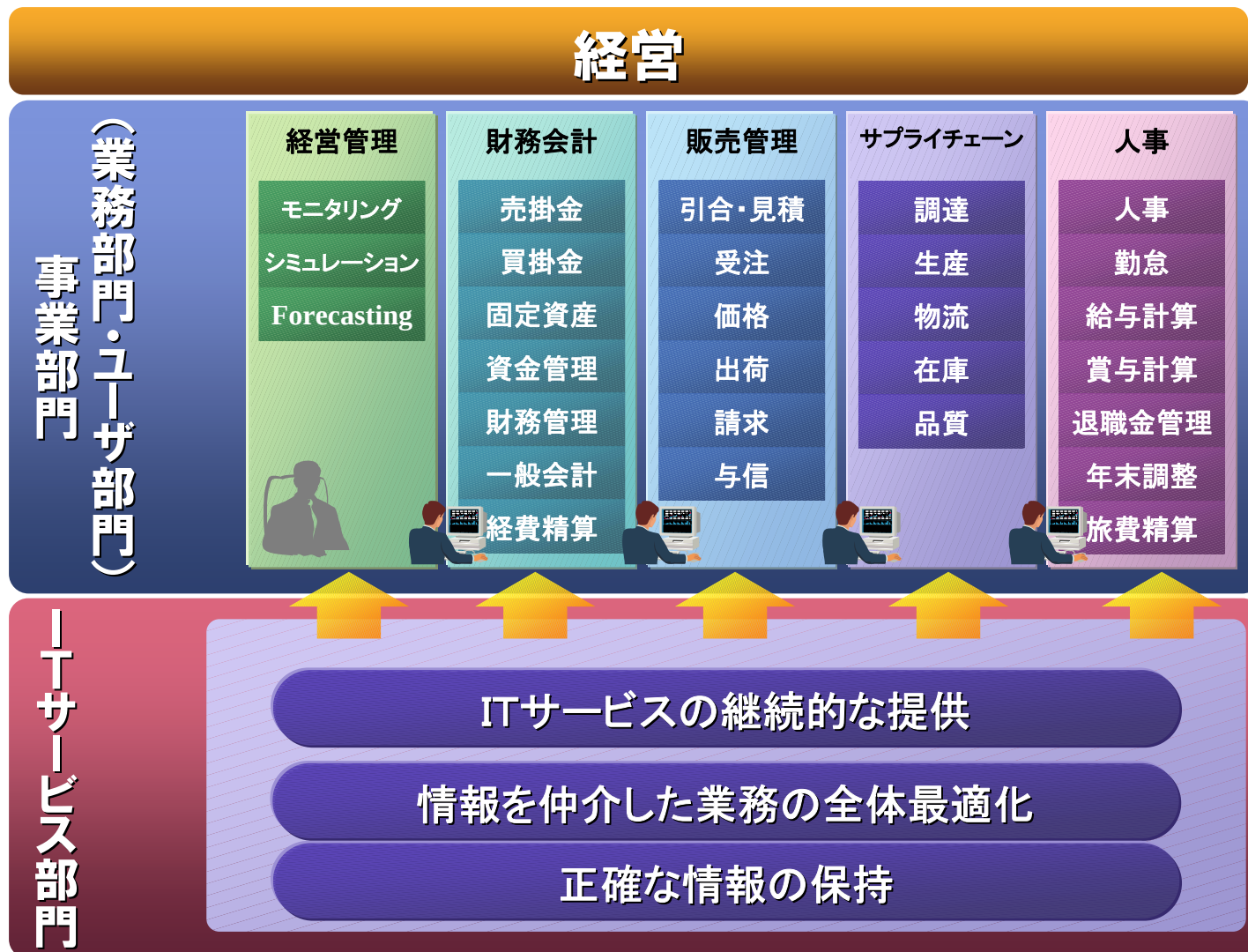
4 さらに 企業価値の向上を目指して —システムの運用・持続が企業を支える—



✓文書化の整備し、不備や根本の改善を実施していく場合や継続的に統制を実施する場合には、IT部門の関与する範囲が大きくなる。



・ITの運用・維持はこれからの企業経営の核となる。



内部統制のために運用管理者は 何をすべきか？



2007年6月6日

株式会社日立コンサルティング