HITACHI
Inspire the Next

内部統制時代の企業情報システムの勘所

2008/2/12

株式会社 日立製作所
ソフトウェア事業部　新分野事業推進室

室長 工学博士　大場みち子

uVALUE

HITACHI
Inspire the Next

Contents

uVALUE

HITACHI
Inspire the Next

1

内部統制と企業ITシステム

uVALUE

1-1. 実施基準※における内部統制フレームワーク

HITACHI
Inspire the Next

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

- 統制環境
- リスクの評価と対応
- 経営理念や組織構造をはじめ、会社レベルで内部統制の基盤が整っている
- モニタリング
- ITへの対応

監査人の視点

①適切な統制が全社的に機能していることかどうか心証を得る

②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

各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

- 会社規則は内部統制の観点から見てリスクを回避するものとなっている
- 管理者によるレビュー
- 財務諸表に係る業務は会社規則通りに行われている
- 職務の分離

※金融庁「財務報告に係る内部統制の評価及び監査に関する実施基準」(2007年2月15日)

1-2. 全社的な内部統制の整備・評価

HITACHI
Inspire the Next

全社的統制チェックリスト

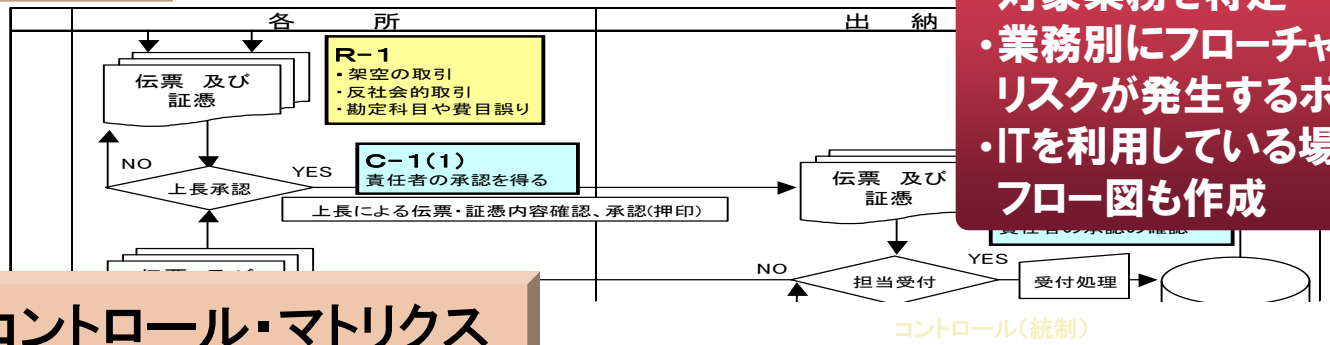
要　因	チェック項目（質問内容）	チェック項目に対する説明	テスト手続き				評価	
			テスト手法	YN	テスト結果	関連証憑	YN	理由
経営者の誠実性と倫理的価値観	経営者は企業経営にあたって誠実性と倫理的価値観を十分に尊重しているか。	・「企業行動基準」の制定・伝達 ・「取締役・執行役倫理綱領」 ・社長メッセージ等	・社内WEBでの確認、・質問等					
	経営者は従業員が不誠実で違法な、または倫理に反する行動をとるような動機や誘惑を除去・低減するための取組みを行っているか。	・「コンプライアンス通報制度」、 ・「ビジネス倫理ハンドブック」、 ・「就業規則」等	・社内WEBでの確認、担当部署での確認等					
	経営者は不正行為の誘因となるような非現実的な業績目標の達成を特に短期的業績について求めないようにしているか。	・経営ビジョン、 ・中期経営計画と予算制度、 ・経営者の報酬決定方法等						
	経営者は不正行為や反倫理的な行動に対し適切な措置をもって臨んでいるか。	・就業規則に基づく懲戒処分、 ・再発防止策等						
	株主、従業員、顧客、投資家、債権者、取引先、監査人等主要なステークホルダーとの間で、誠実性と倫理的価値観に基づいた関係を維持するための取組みを行っているか。	・「グループCSR報告書」、 ・「営業行動指針」、 ・「購買取引行動指針」等						
	経営者は内部統制手続きの構築・維持を自らの責任において行い、その運営にあたっては不当な干渉や重要な事項を放置することはないか。	・グループ内部統制再構築プロジェクト等						
能力に対する取組み	・経営者は各職務に要求される能力の水準を具体的に定める責任がある、・経営者の能力							
取締役会、監査委員会	・監督・執行・監視機能の分離、・監視機構の独立性、・職務・権限の明確化等							
経営者の経営理念と事業運営	・グループ運営への取組み、・経営判断にあたっての潜在リスク分析、・財務報告に対する姿勢・態度等							
組織構造	・適切な組織構造の構築、・適切な情報の流れ、・経営者の職務分掌と責任							

- 内部統制の5つの構成要素ごとに、質問に対して現状を整理・回答することにより、**会社レベルで内部統制の基盤が整っていることを確認**
- 不備があれば改善

1-3. 業務プロセスに係る内部統制の整備・評価

HITACHI
Inspire the Next

フローチャート



- 対象業務を特定
- 業務別にフローチャートを作成し、リスクが発生するポイントを特定
- ITを利用している場合、システムフロー図も作成

リスク・コントロール・マトリクス

ビジネスプロセス	影響する勘定科目	サブプロセス	プロセスの目的	リスク	内容	責任部署・責任者等	関連規定	テスト手続き 手法	テスト手続き YN	テスト手続き 結果	評価 YN	評価 理由
出納	現預金	支払	支払内容が適正かどうか確認されている	【R－1】架空取引、反社会的取引、有効でない記帳仕訳、支払遅延等	【C－1(1)】発行部門は、その内容及び金額を正当と認めた証憑書類に基づき、責任者の承認を得ること	伝票発行部門 山田太郎	財務管理規定 第1章2．1					
					【C－1(2)】伝票と証憑書類との照合を行	出納部門	財務管理規定					
			現金による出金は正しく処理されていること	【R－2】帳簿残高と現金の不一致(過払い等)	【C－							
			支払済の伝票及び証憑は適正に管理されていること	【R－3】証憑の二重使用、支払の事実・内容が不明となる	【C－							

- 特定したリスクポイントごとに、リスクの種類、コントロールの方法、基準などを記載
- テストの方法を検討し、サンプリングテストを実施
- 不備があれば改善

1-4. 業務プロセスの中で実行すべき統制の例

HITACHI
Inspire the Next

■ 業務プロセスの中に次のような統制を適切に配置することにより、リスクを排除

コントロールの種類	統制内容
照合/調整	二つの項目（数値）が一致あるいは整合しているかどうかを確認する
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
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
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

1-5. ITから見た内部統制フレームワーク

HITACHI
Inspire the Next

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

- 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

監査人の視点

①適切な統制が全社的に機能していることかどうか心証を得る

②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

各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

ITに係る統制 — 担保する — 業務リスク

ITに係る業務処理統制

- 入力情報の完全性、正確性、正当性等のチェック
- 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
- アクセス管理（ユーザ認証、操作範囲の限定など）

担保する — ITリスク

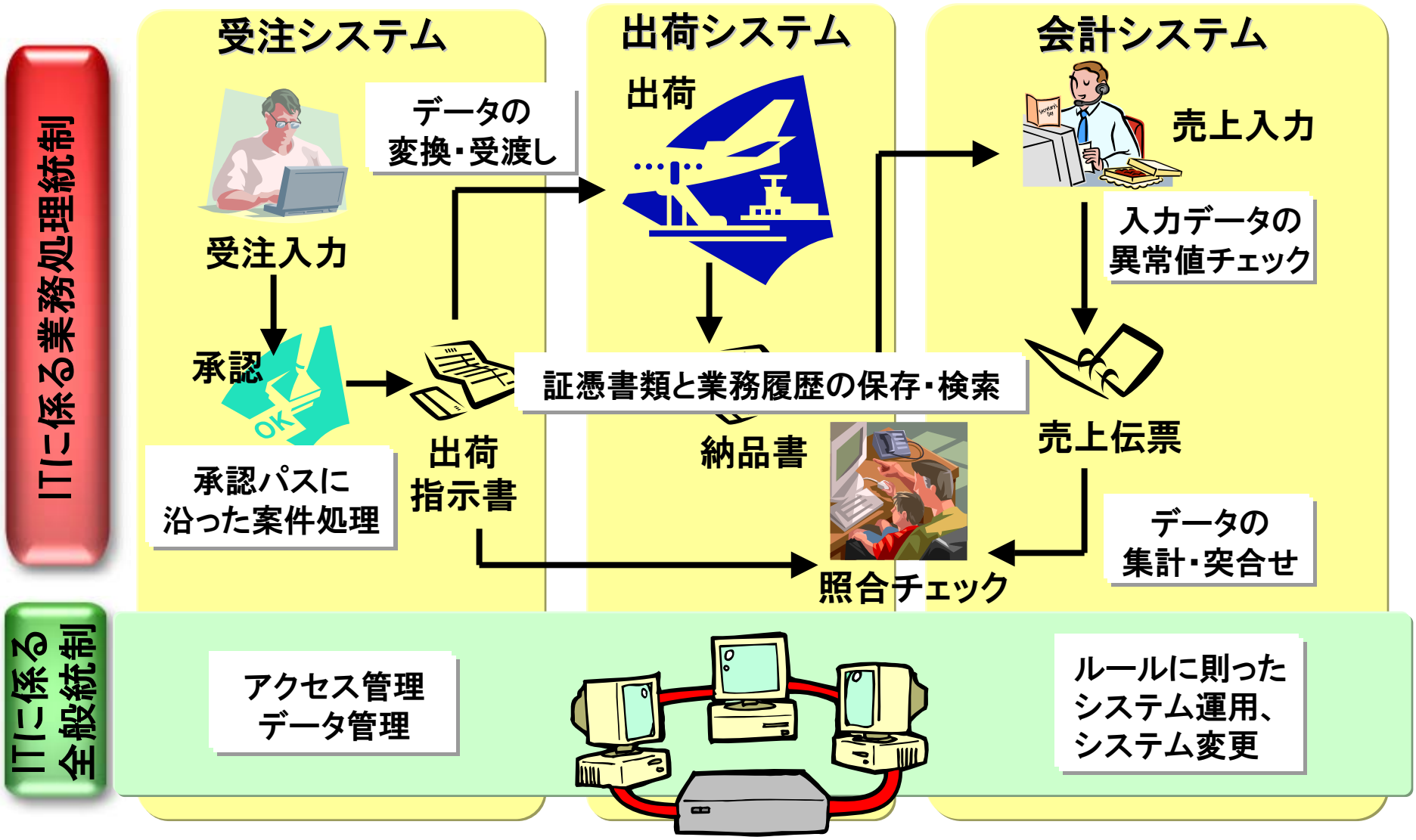
ITに係る全般統制

- システムの開発、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

uVALUE

1-6. 業務処理統制と全般統制の一例

HITACHI
Inspire the Next



1-7. IT活用による統制評価の効率化

HITACHI
Inspire the Next

ITを利用した内部統制は一貫した処理を反復継続するため、その整備状況が有効であると評価された場合には、ITに係る全般統制の有効性を前提に、人手による内部統制よりも、例えばサンプル件数を減らし、サンプルの対象期間を短くするなど、一般に運用状況の評価作業を減らすことができる。（実施基準）

【所要時間比較例※】

	手動統制による アプローチ	自動統制による アプローチ
コントロール数	500	500
コントロールあたりの文書化時間	1時間	3時間
トータルの文書化所要時間	500時間	1,500時間
コントロールあたりのサンプル数	10	1
サンプルテストの総数	5,000	500
サンプルあたりのテスト時間	30分	30分
トータルのテスト所要時間	2,500時間	250時間
総所要時間	3,000時間	1,750時間

※出典：「企業改革法遵守のためのITの統制目標（第二版）」 日本ITガバナンス協会（2006.9）

1-8. なぜ全般統制が必要か？

HITACHI
Inspire the Next

金融庁　実施基準

ITを利用した情報システムにおいては、一旦適切な内部統制（業務処理統制）を組み込めば、意図的に手を加えない限り継続して機能する性質を有しているが、例えば、その後のシステムの変更の段階で必要な内部統制が組み込まれなかったり、プログラムに不正な改ざんや不正なアクセスが行われるなど、全般統制が有効に機能しない場合には、適切な内部統制（業務処理統制）を組み込んだとしても、その有効性が保証されなくなる

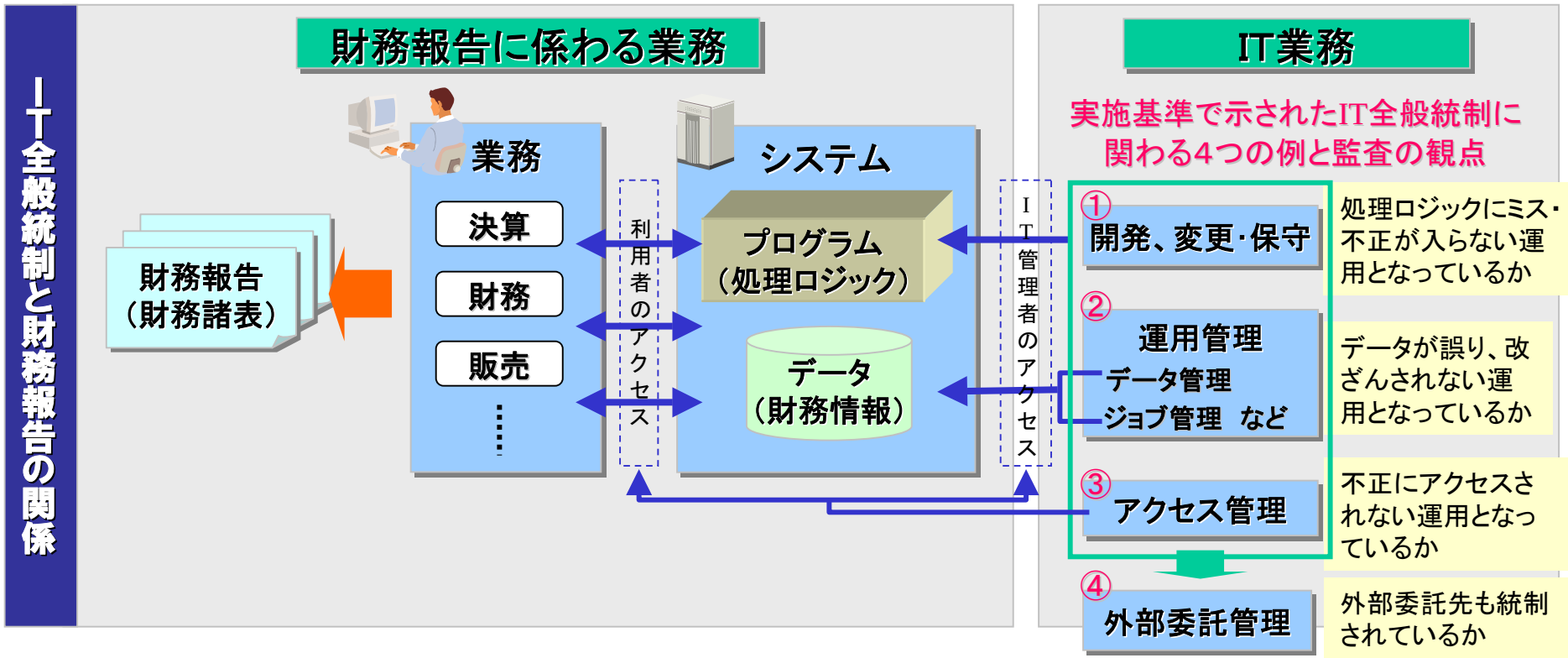
全般統制は業務処理統制の大前提

公認会計

アプ…般統制としての運用状況が信用できない場合には、当該業務処理統制の有効性が崩れてしまう…監査人は…何らかの追加的リスク評価手続、運用評価手続の実施が財務報告の信頼性の確保に寄与すると判断したときは、その手続を実施することになる。例えば、不備がある全般統制に関連する業務処理統制の運用評価手続の範囲（件数、期間等）を拡大するなどの対応が必要になる。

1-9. IT全般統制に関する監査の視点

◆財務報告に直接的に影響を与えるのは、プログラム（処理ロジック）とデータ。
◆課題：プログラムとデータが継続的に信頼できる環境となっているか？



監査の視点

財務報告は正しいか？	財務報告の信頼性が確保されるよう業務が統制されているか？	業務において、ITによる自動化統制はどう機能しているか？	ITによる自動化統制が**継続的に有効に機能する環境**が確保されているか？

1-10. 統制すべきIT業務例

HITACHI
Inspire the Next

- 財務報告の信頼性を担保するには、多くのIT関連業務の統制が必要
  情報システム部門の業務をリスクの観点から再チェックすべき

✔プログラム変更管理
- ①開発者と運用者の職務分掌
- ②変更手続きの明確化
- ③変更ログの保管

✔ジョブ実行管理
- ①臨時・例外処理は記録を残す
- ②認可されていない処理を行わない

✔データ修正管理
- ①許可なくデータを変更しない
- ②修正記録を残す
- ③修正できる人は最小限に

✔障害管理
- ①障害対策手続きの明確化
- ②対策内容の記録を残す

✔アクセス管理
- ①ID発行・削除手続きの整備、ログ保管
- ②発行済IDの有効性管理
- ③職務分離(発注と検収など)への対応
- ④高権限(ｽｰﾊﾟｰﾕｰｻﾞ)IDの適正化

✔バックアップ/リカバリ

✔OS管理/ネットワーク管理

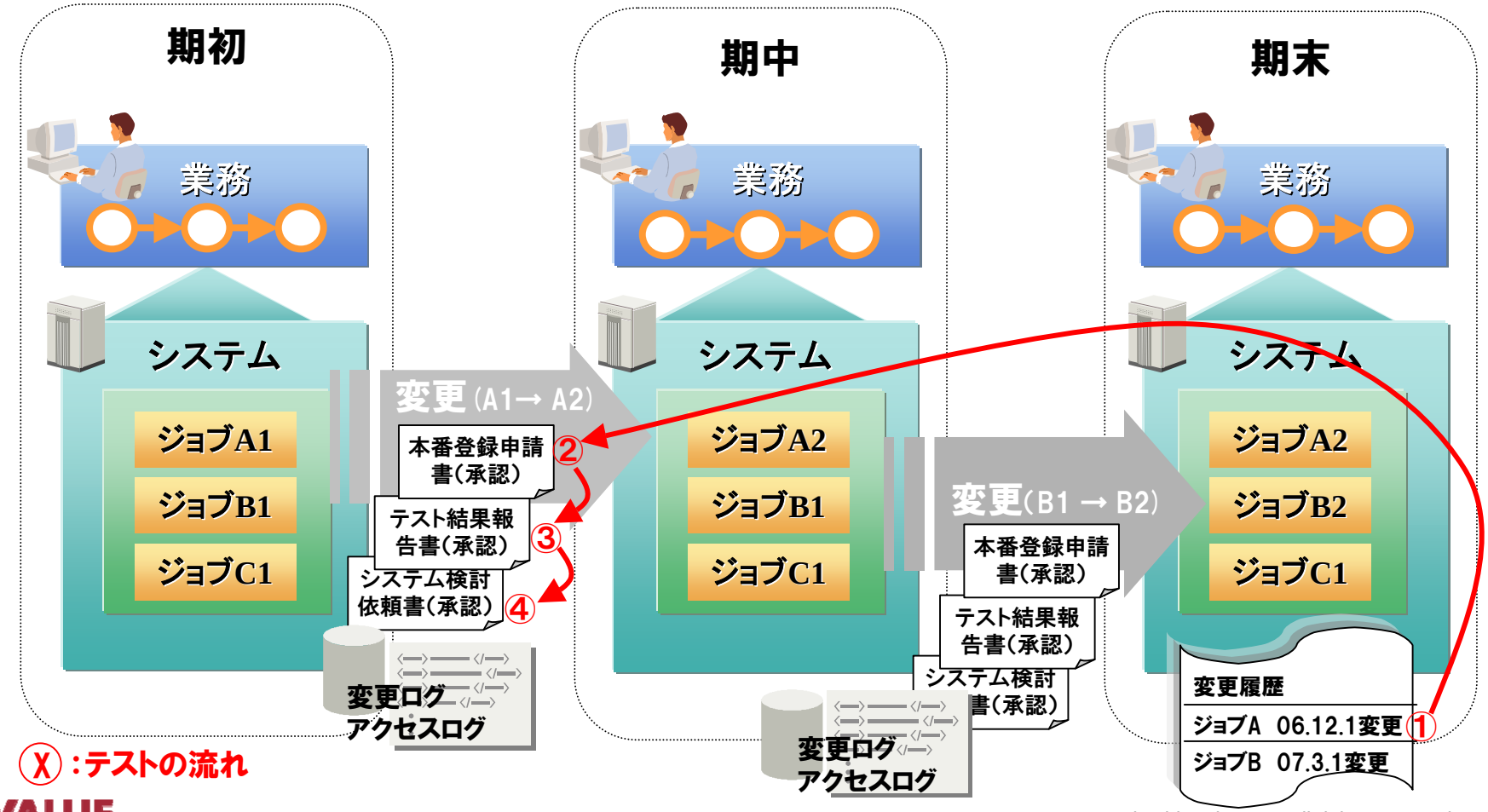
✔EUC※統制　・・・

※ End User Computing

1-11. IT全般統制における証跡

HITACHI
Inspire the Next

- 目的：システムの変更が、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
- 必要なもの：「変更の理由となる依頼書」、「依頼に基づいて変更をした記録」、
  「システムが自動出力する変更一覧（履歴）」
- 検証方法：該当期間での変更一覧からサンプルを選び、その変更が正当な理由に応じて正確に行われたことを、証跡を逆順にたどって確認する。（逆進テスト）



uVALUE

HITACHI
Inspire the Next

2

業務処理統制を支援する
日立オープンミドルウェア

uVALUE

2-1. 業務処理統制を支援する日立オープンミドルウェア

HITACHI
Inspire the Next

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

- 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

監査人の視点

①適切な統制が全社的に機能していることかどうか心証を得る

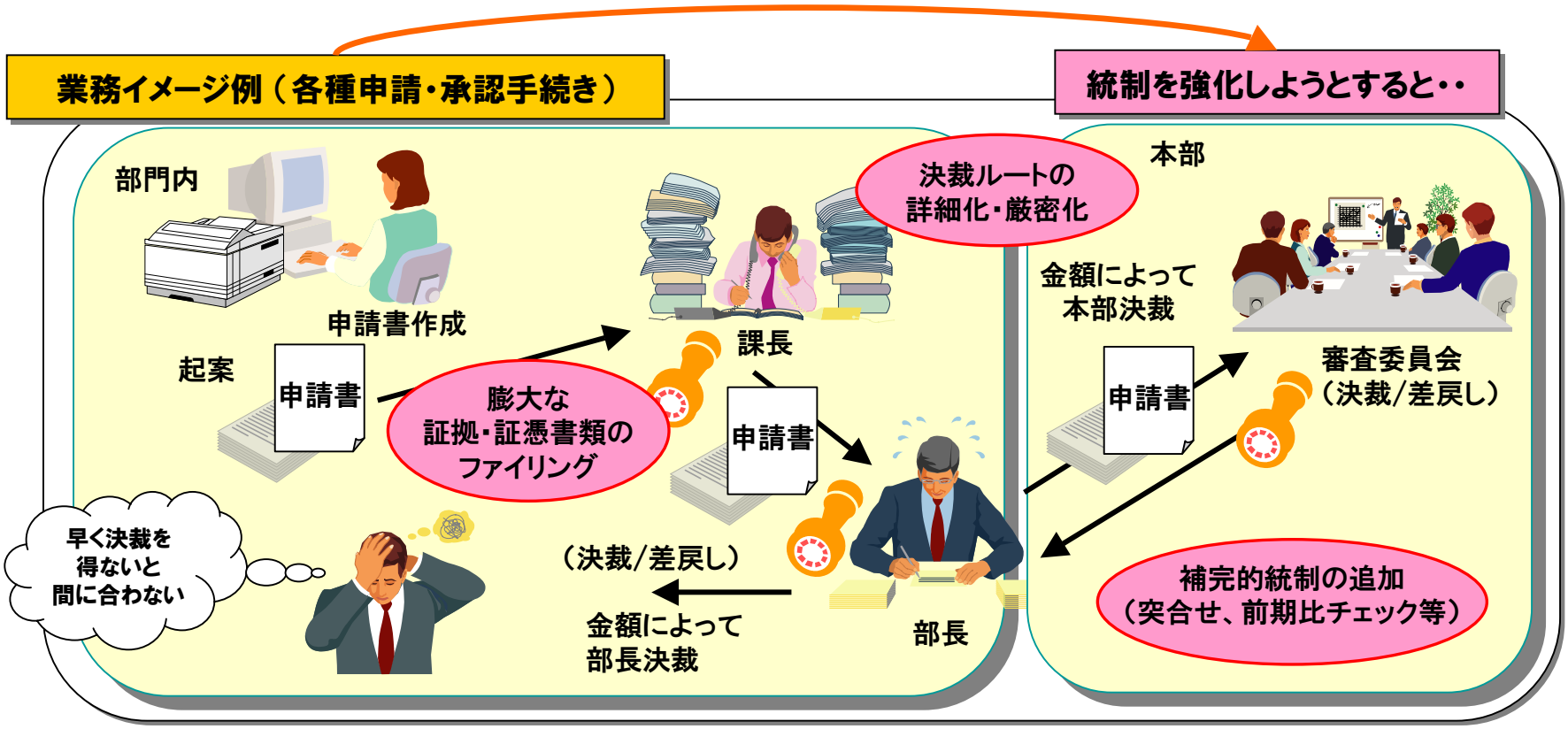
②それに基づき、虚偽記載につながるリスクに着眼して業務プロセスに係る内部統制を評価

業務プロセスに係る内部統制

各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

2-2. 業務の統制に伴う悩み



内部統制をもっと強化したいのだが・・・

- 統制活動に要する時間によって、業務効率が低下する
- 紙で書類を保管しているため、過去の案件の監査・検証が困難
- 案件の承認進捗状況が把握できず、滞留や決裁漏れを防ぎきれない

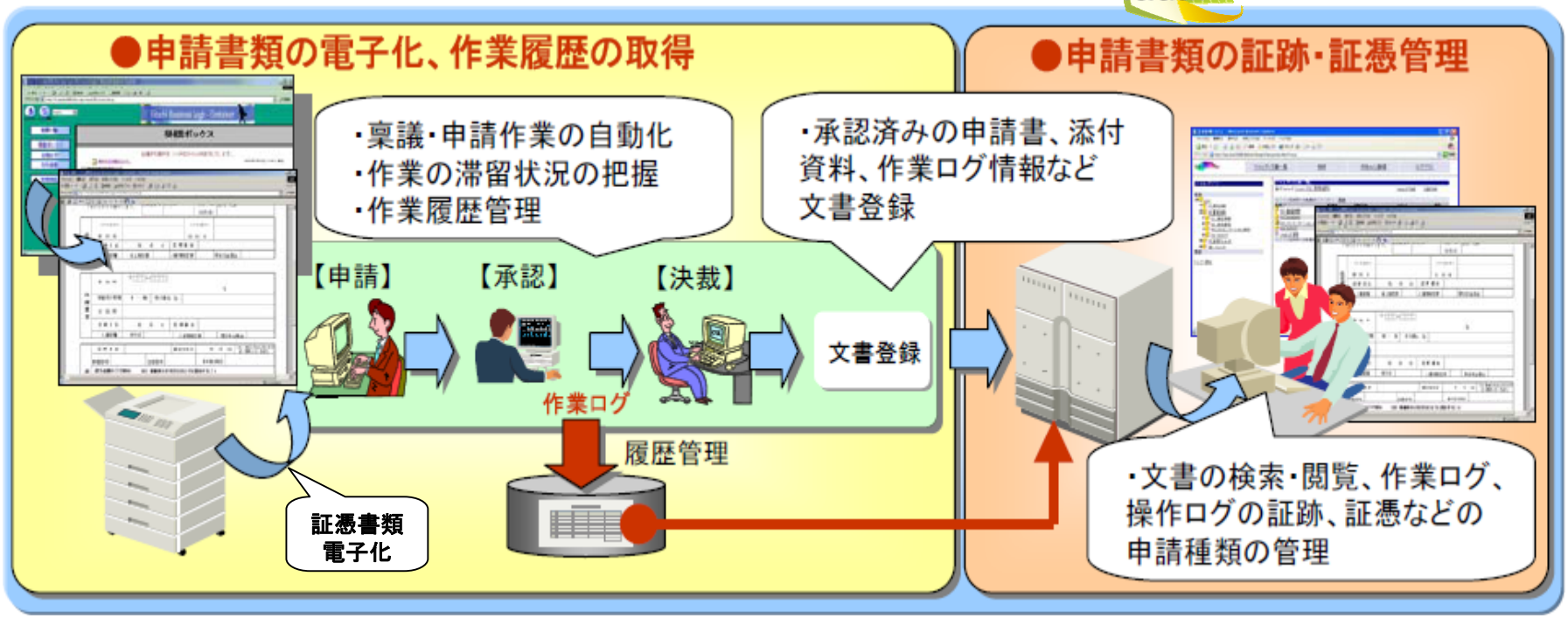
2-3. プロセスの自動化(ワークフロー)と証跡・証憑書類の電子化(記録管理)

HITACHI
Inspire the Next

Cosminexus Version 7 電子フォームワークフローセット

DocumentBroker Version 3

HiRDB Version 8



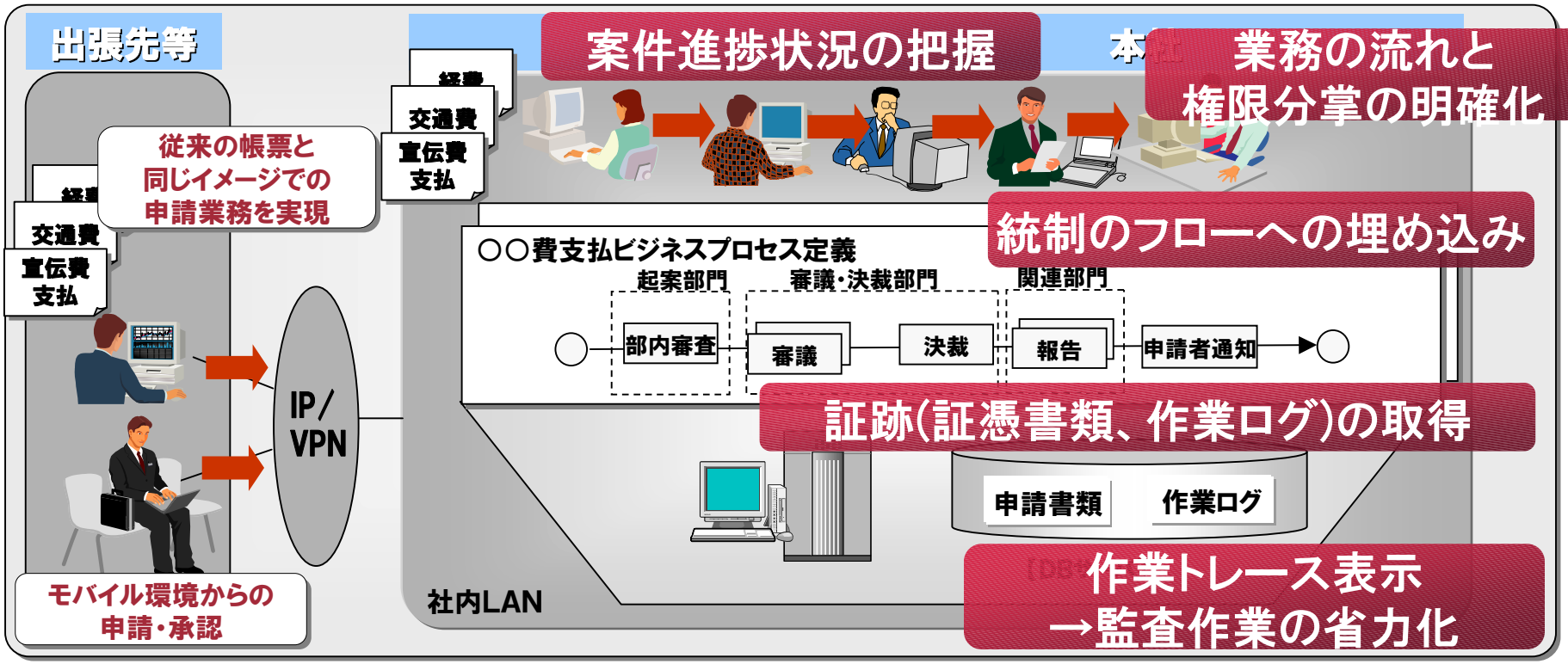
電子フォームワークフローによる業務プロセスの自動化

- 配送の自動化・柔軟なルート定義により、業務効率向上と確実な統制を両立できます。
- 作業の滞留状況がリアルタイムに把握でき、早期に対策が打てます。
- 業務のボトルネックが可視化され、業務改革に向けた検討が可能になります。

DocumentBrokerによる証跡・履歴情報の確実な保管

- 電子化した証憑書類や作業ログを保存し、業務の正当性を証明する証跡を残せます。
- 監査時に必要となる情報は、文書検索機能により迅速的確に取り出せます。

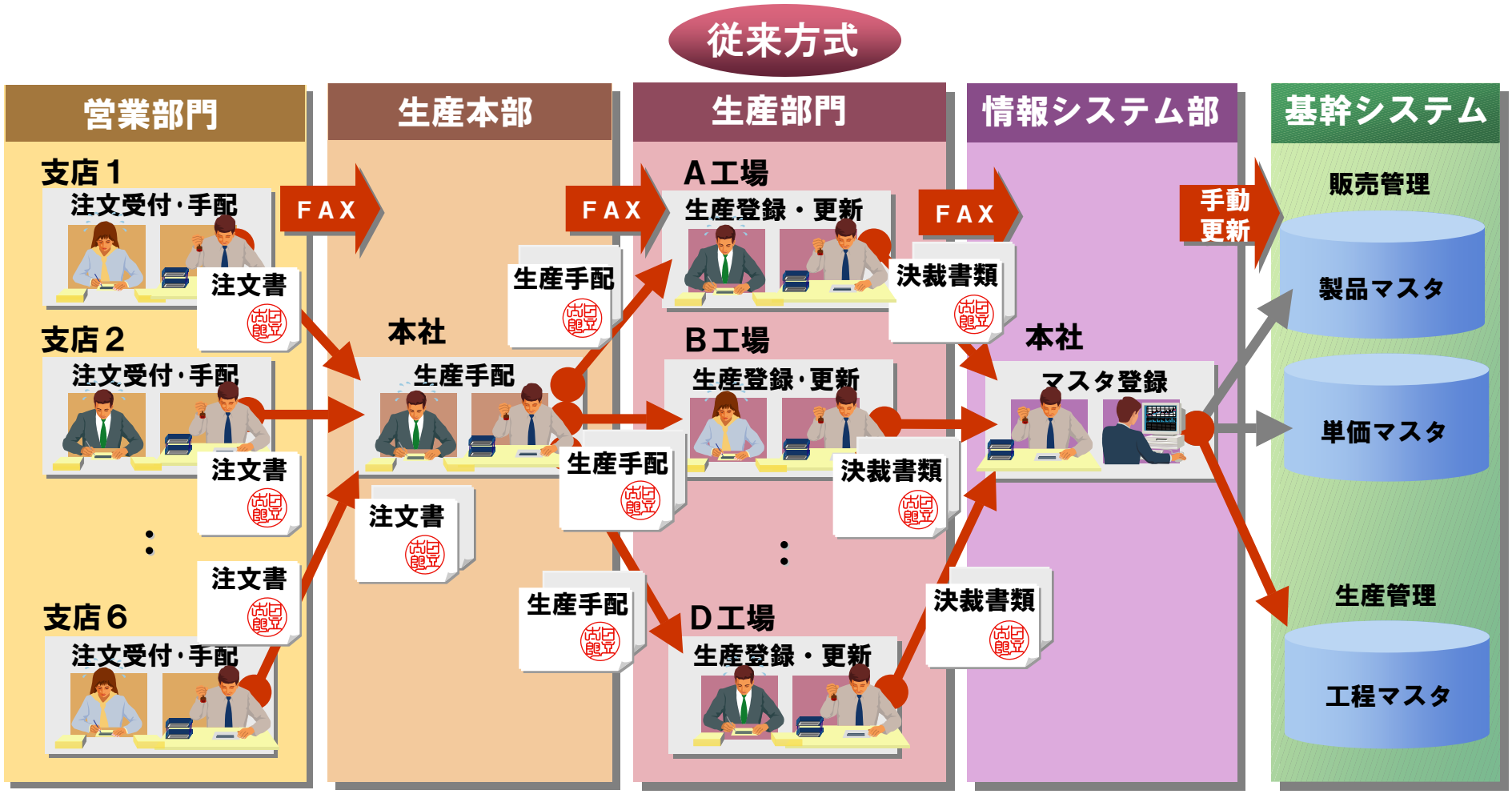
2-4. 導入事例1：申請・決裁業務のスリム化と統制強化



導入効果

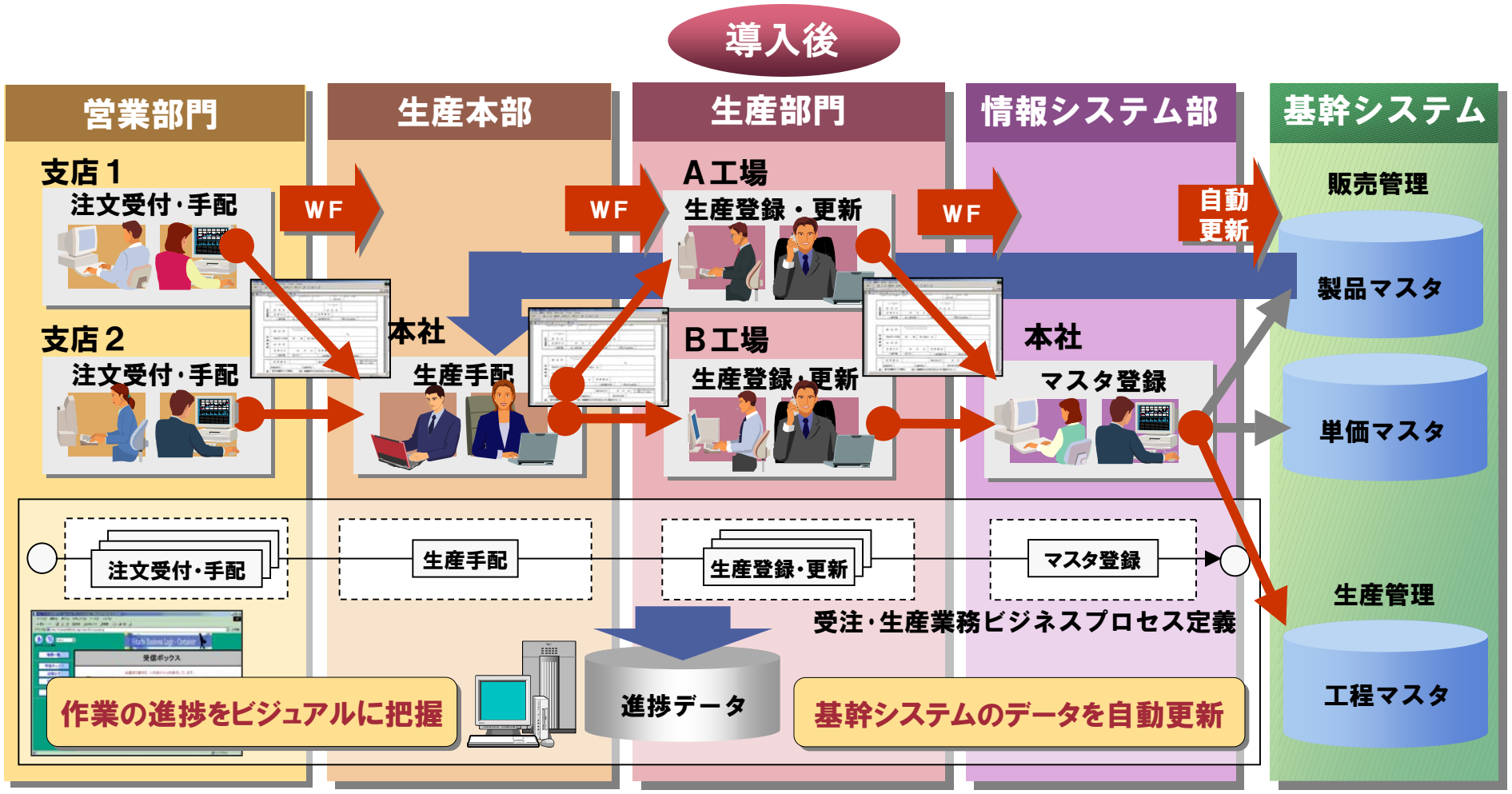
- ビジネスプロセス定義の過程で業務の流れの明確化とスリム化を実現。
- 内部統制監査対応時の作業の省力化が期待できる。
- 業務のボトルネックが可視化されることにより、業務改革に向けた検討が可能に。
- 使い慣れた帳票イメージのまま電子化。入力値のエラーチェックも。

2-5. 導入事例2：複数部門間をまたがる業務の自動化と統制



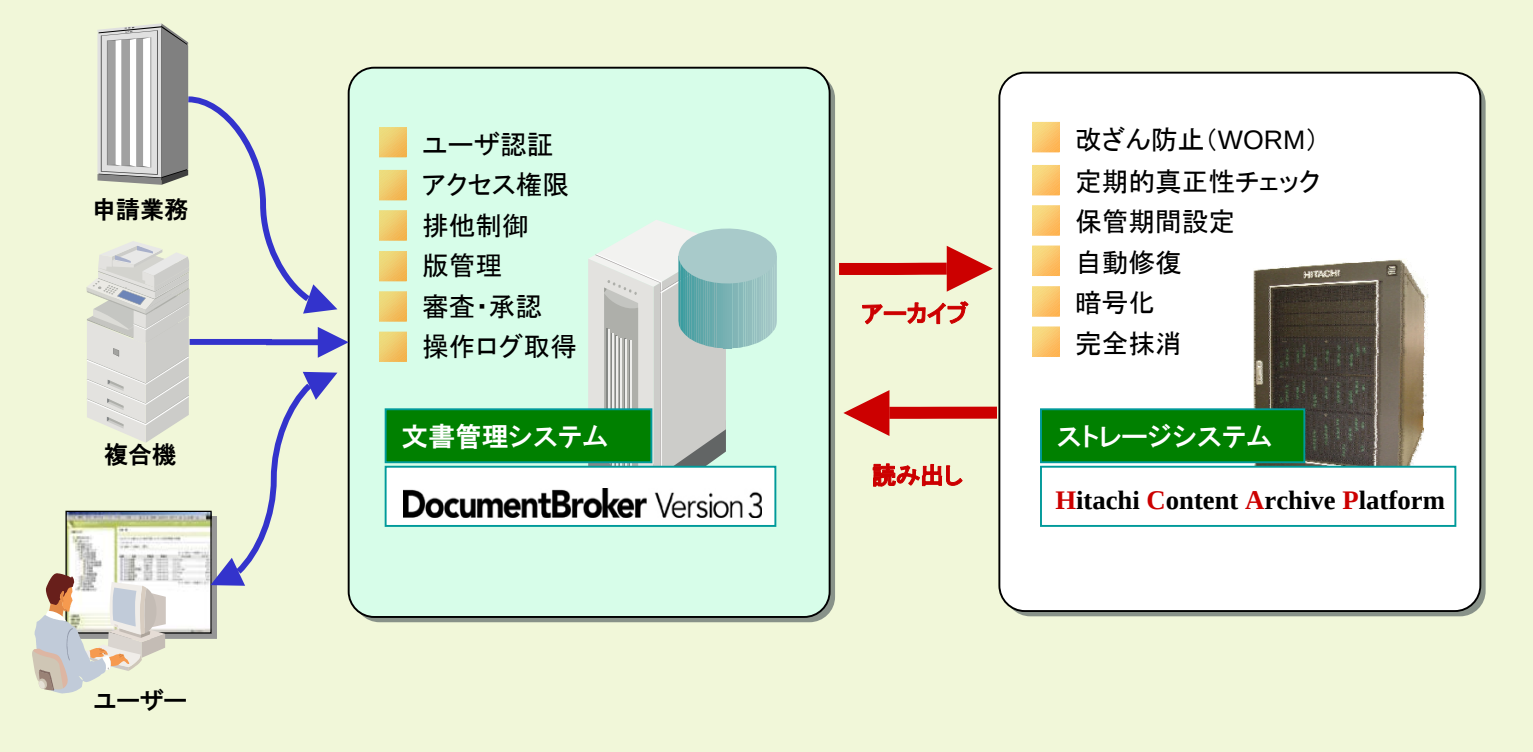
- 部門をまたがる際には書類をFAX送信し、次工程で再入力
- 入力ミス、送信先誤り、案件の滞留や決裁漏れ等のリスクが潜在

2-6. 導入事例2：複数部門間をまたがる業務の自動化と統制



- 注文受付から手配、生産、基幹システムへのデータ登録までを一貫して自動化
- 部門間でのデータ受渡し（送信、再入力）に伴うリスクを排除
- 案件の滞留や決裁漏れも防止

2-7. 証跡データの安全な長期保管



真正性を維持した状態で証跡データを長期保管

- 改ざん防止機能と定期的チェックにより、格納データの真正性を維持
- 悪意やミスによる重要データの削除を防止（指定期間中は管理者でも削除不可）
- 不要となったデータは痕跡を残さず完全削除

文書管理システムとアーカイブ用ストレージシステムをシームレスに連携

- 使いやすいインターフェースでアーカイブ機能を利用可能

HITACHI
Inspire the Next

3

IT全般統制を支援する
日立オープンミドルウェア

uVALUE

3-1. IT全般統制を支援する日立オープンミドルウェア

HITACHI
Inspire the Next

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

- 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

監査人の視点

①適切な統制が全社的に機能していることかどうか心証を得る

②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

各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

ITに係る統制 — 担保する — 業務リスク

ITに係る業務処理統制

- 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リスク

ITに係る全般統制

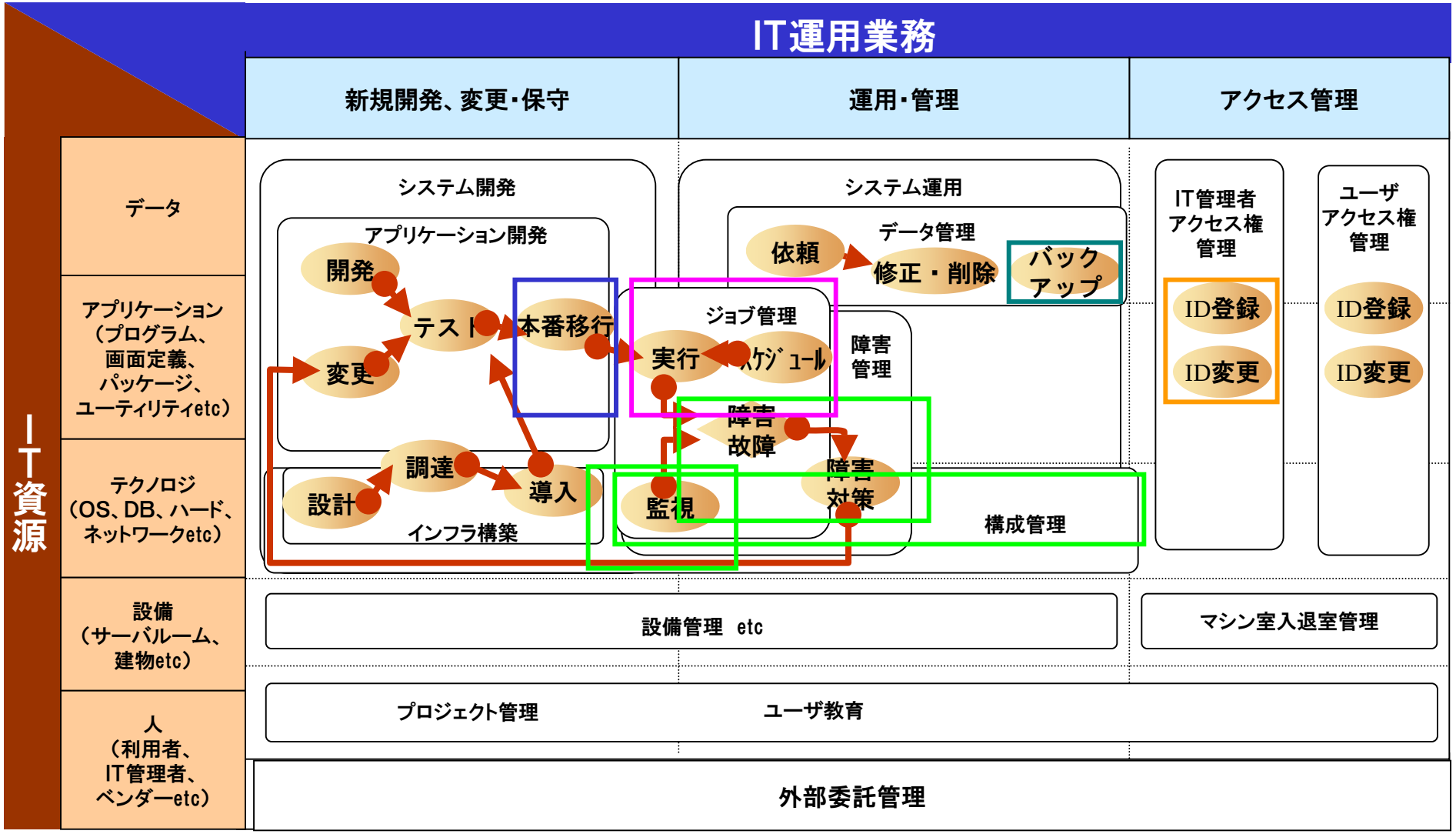
- 発、保守に係る管理
- の運用・管理
- などシステムの安全性の確保
- 関する契約の管理

JP1 Version 8

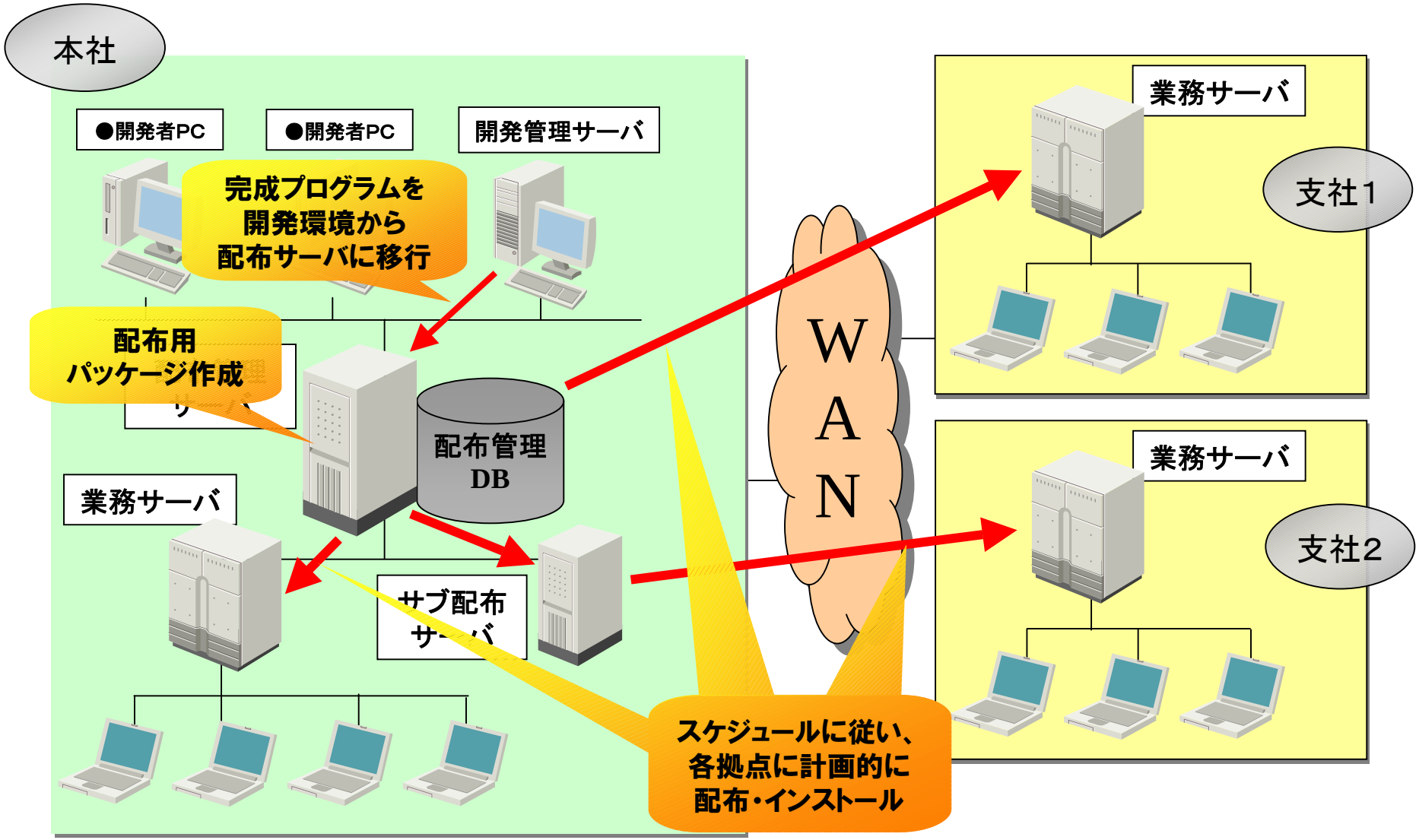
3-2. JP1が支援しうる主な全般統制関連業務

HITACHI
Inspire the Next

：業務種別　：作業



3-3. 分散拠点への業務プログラム配布管理



3-4. 配布ログの管理と配布後の操作監視

HITACHI
Inspire the Next

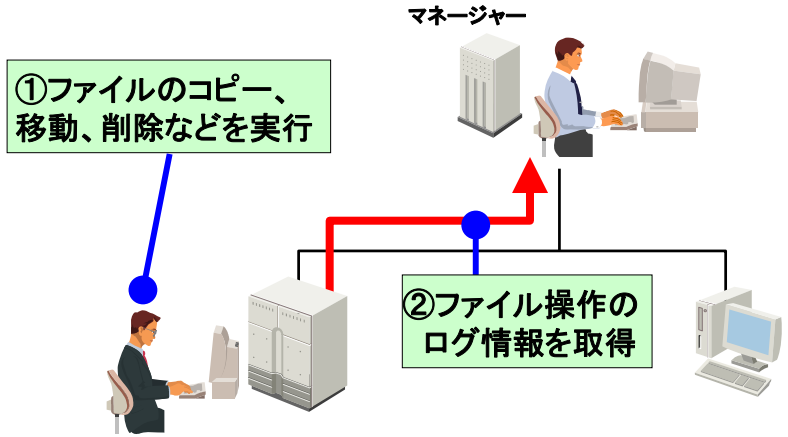
●完成後の業務プログラムをJP1で配布することにより、下記の事象をログに記録でき、内部統制監査の際、正しい手順に従ってプログラムの本番移行を行ったことを示せます。

- 業務プログラムパッケージの作成
- リモートインストールマネージャへのログイン
- 配布ジョブの作成・実行

配布ログ例（抜粋）

ctgry=StartStop, result=Success, subj:pid=908, msg="**起動しました。**"
ctgry=ContentAccess, result=Success, subj:uid= JP1USER, op=DMPK_REG, auth=JP1_DM_Admin, msg="**ソフトウェアをパッケージングしました。パッケージ識別**ID：20070227_175924 **パッケージ名：受注管理プログラム バージョン：**0200 **世代番号：**0"
ctgry=Authentication, result=Success, subj:uid=JP1USER, auth=JP1_DM_Admin, msg="**認証に成功しました。**"
ctgry=ContentAccess, result=Success, subj:uid= JP1USER, op=DMPKJOB_ACT, auth=JP1_DM_Admin, msg="**ジョブを実行しました。ジョブ名：リモートインストール**2007_02_27_18_0632"
ctgry=ContentAccess, result=Success, subj:pid=3984, op=DMPKJOB_ACT, msg="**ジョブが正常終了しました。ジョブ名：リモートインストール**2007_02_27_18_0632 **あて先情報：**SERVER001 **インストール完了日時：**2007-02-27 18:07:21 **パッケージ識別**ID：20070227_175924 **パッケージ名：受注管理プログラム バージョン：**0200 **世代番号：**0"

●配布先の業務サーバ上におけるユーザ操作のログを収集し、配布した業務プログラムに対して改竄等の不正な操作が行われていないか監視できます。

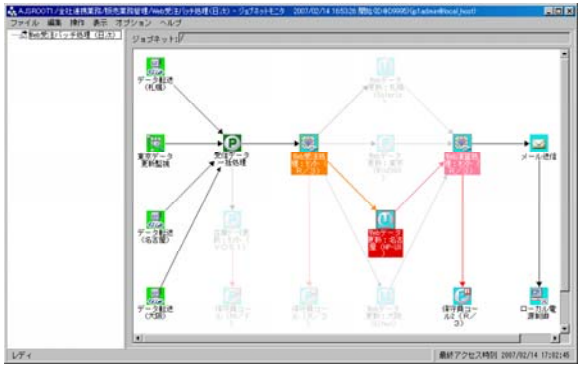


uVALUE

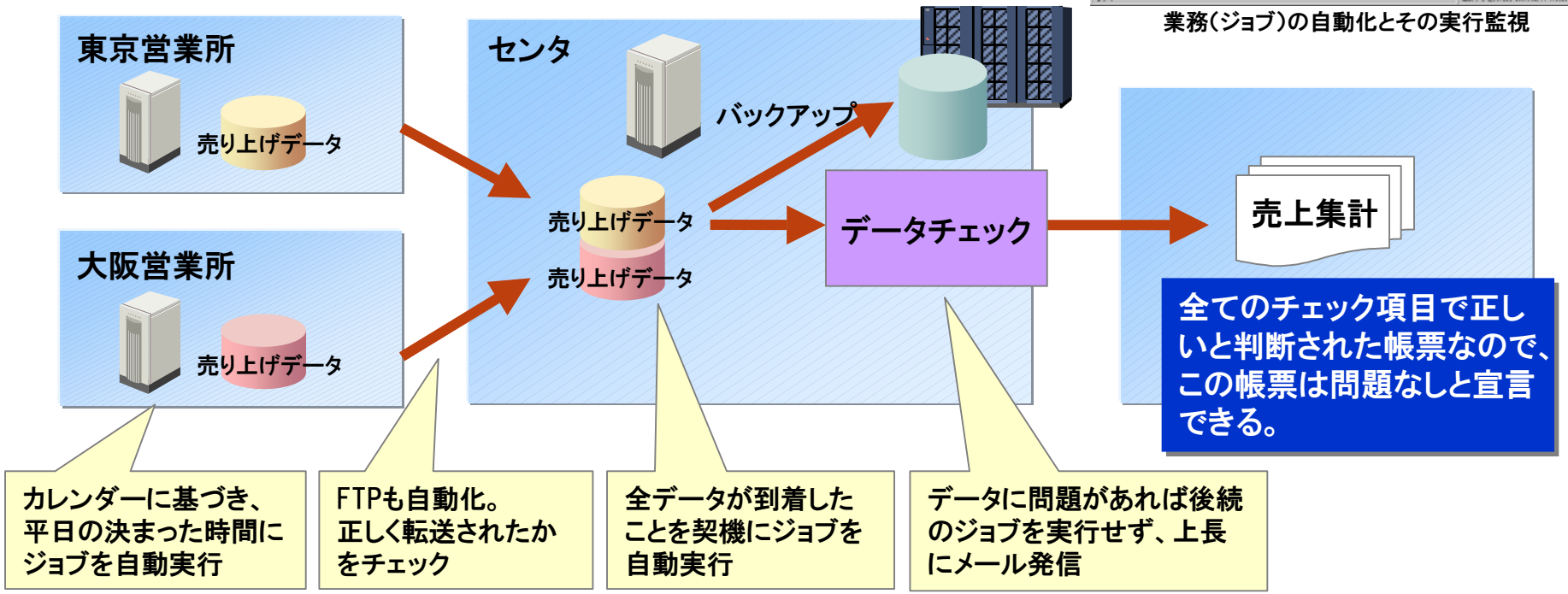
3-5. 業務運用のルール化と自動実行

複雑な運用スケジュールをルール化してジョブを自動実行することにより

- 人手を介することによるリスクを軽減
  - •データの欠落、誤り、改ざん
  - •ジョブの遅延、異常終了
- 臨時・例外ジョブの定型化により統制負荷を軽減
  - •臨時ジョブの申請に伴う統制手続き
  - •証跡の保存と監査対応

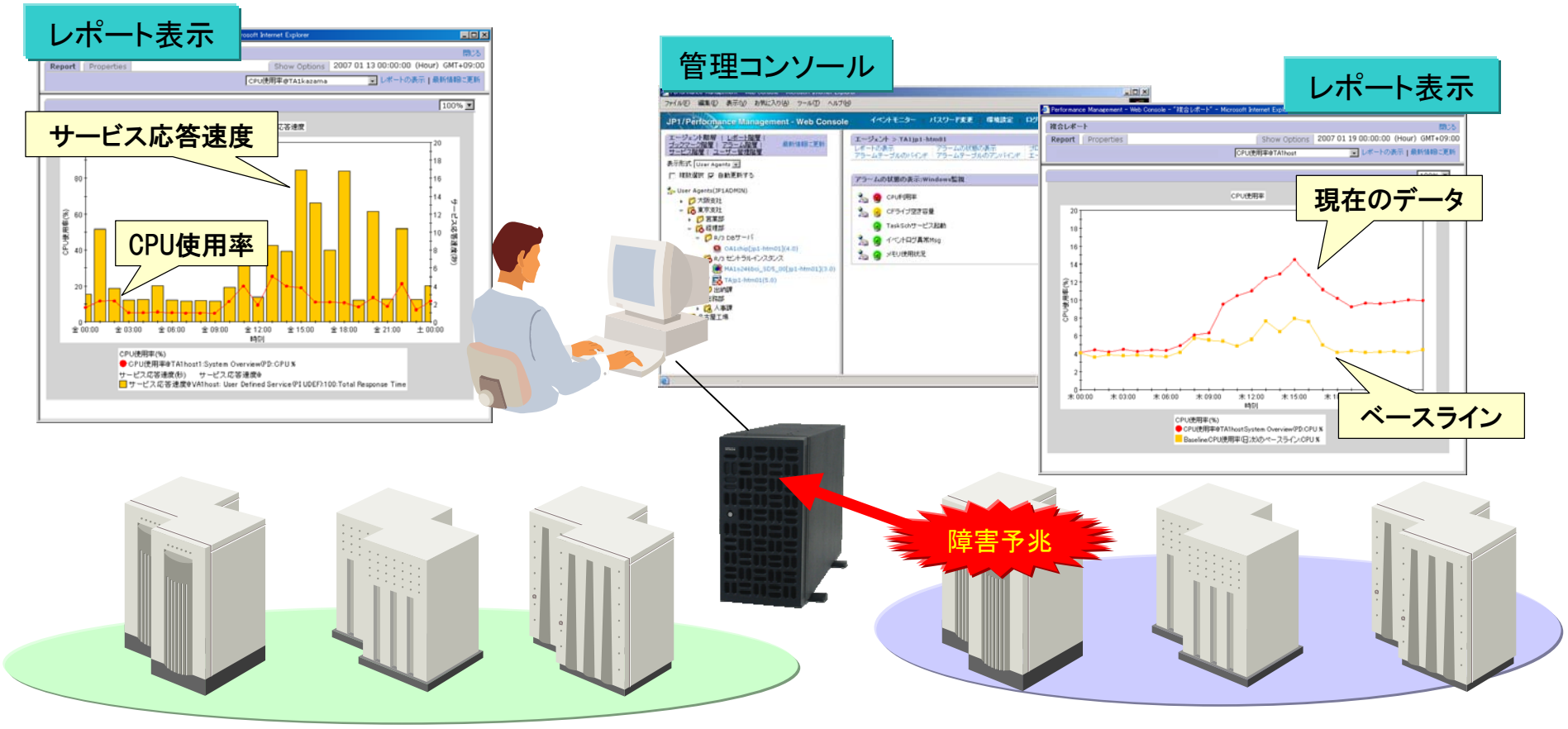


業務(ジョブ)の自動化とその実行監視



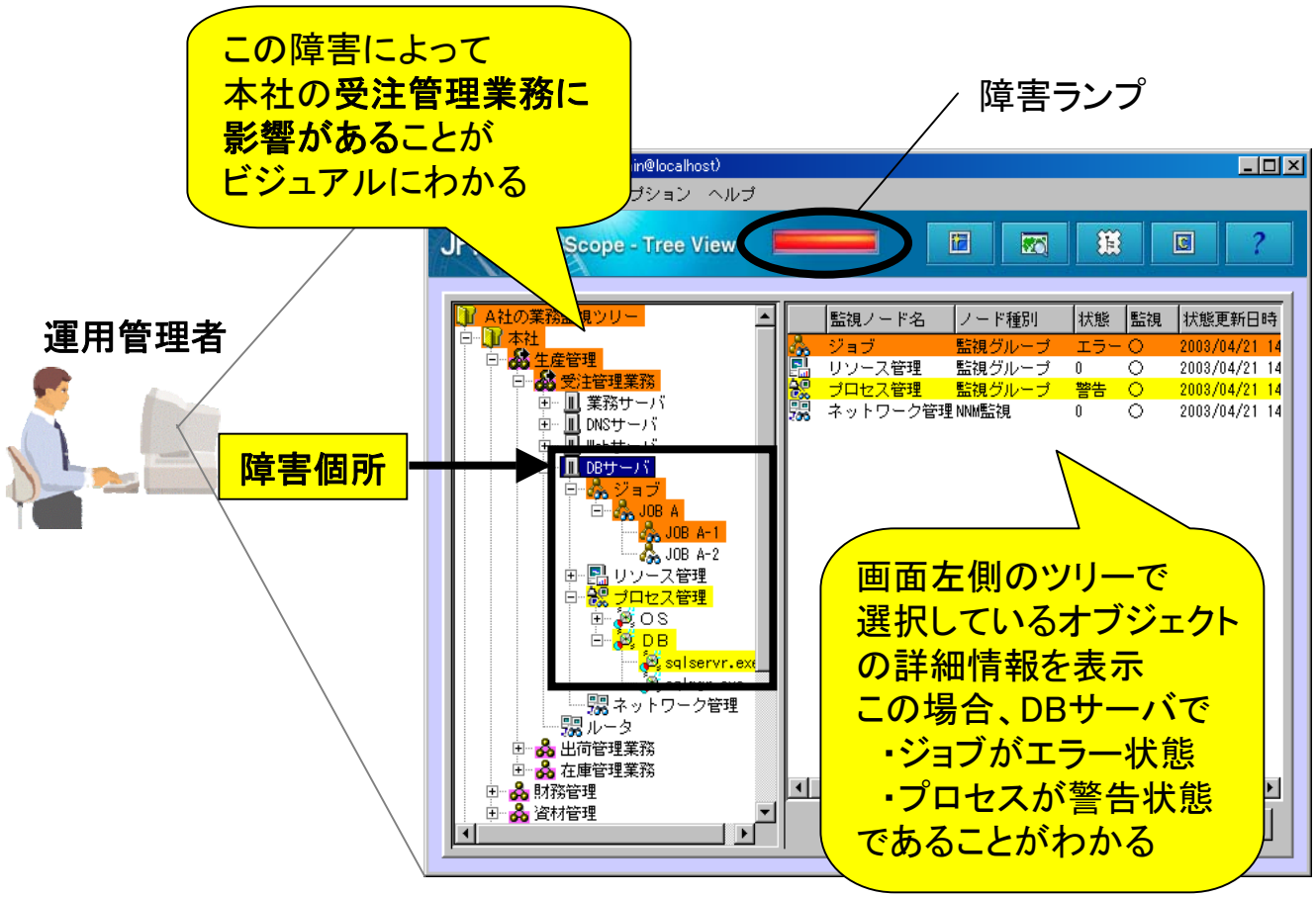
3-6. リソース監視による障害の未然防止

- ジョブの滞留時間や実行数など、業務サーバの稼働状況を継続的に監視
- レスポンス悪化やシステム障害の予兆を捉えて障害を未然に防止
  → 障害対応に要する統制活動、証跡管理、監査対応の負荷を軽減



3-7. 障害の影響を受ける業務の判別

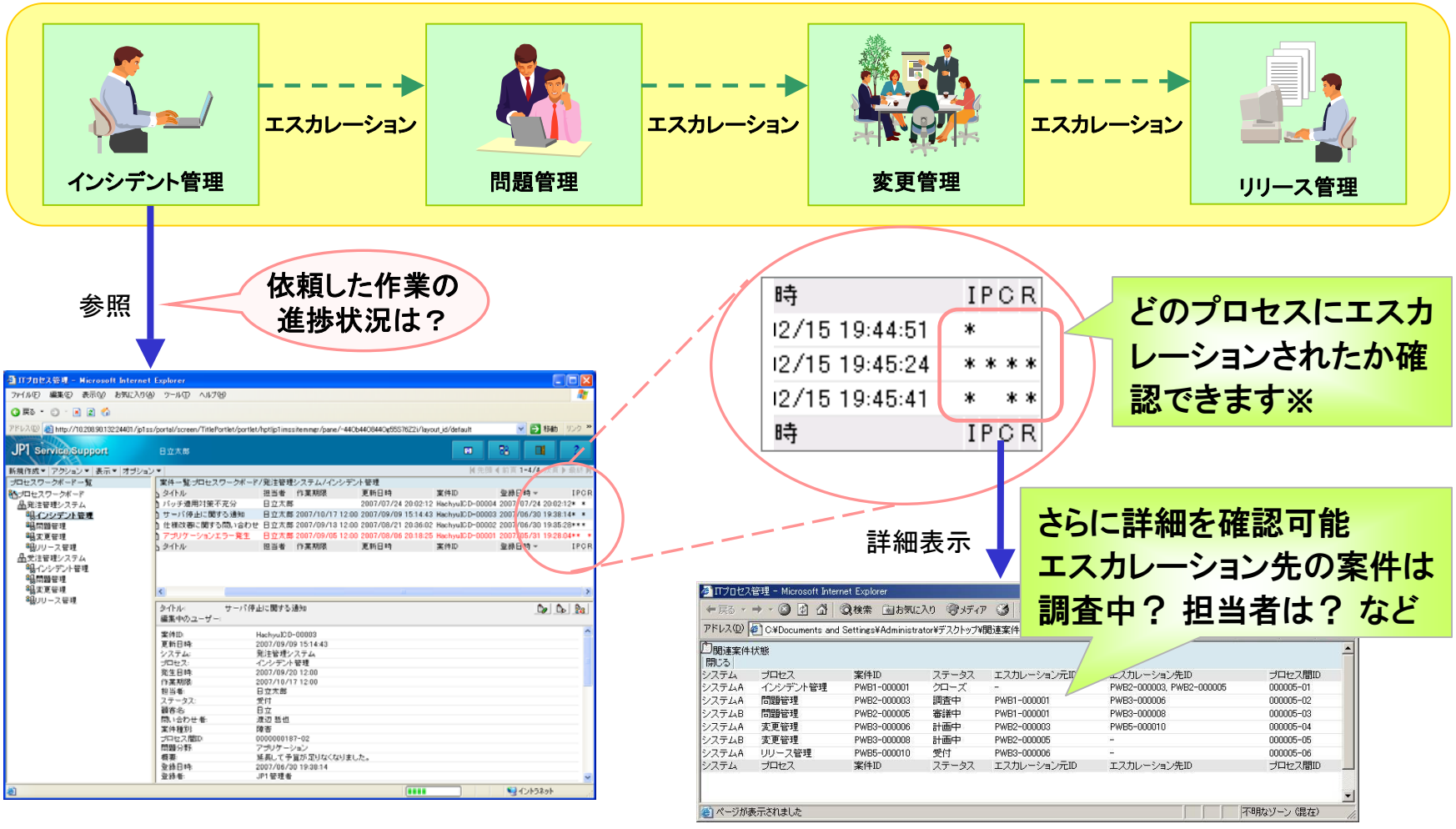
- 障害発生箇所と、影響を受ける業務の関係をビジュアルに表示
- 統制対象業務に関係する障害かどうかが一目で判別できます



3-8. 障害対応プロセス全体の監視と統制

JP1/IM-SS

ITIL®に沿った運用プロセスの統制を実現。作業の進捗状況の監視など統制に必要な運用を支援し、作業の停滞や手順誤りによるリスクを軽減します。



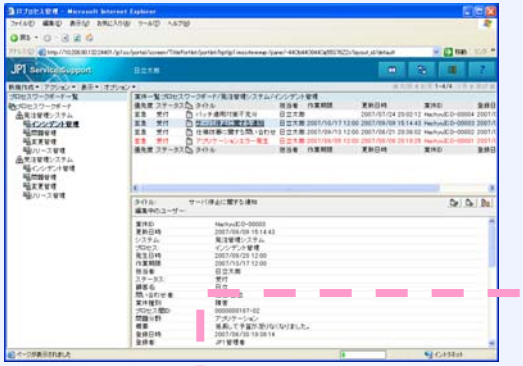
※I、P、C、R は、インシデント管理（Incident）、問題管理（Problem）、変更管理（Change）、リリース管理（Release）を表しています。

3-9. 権限の割り当てによるチェック体制の整備

HITACHI
Inspire the Next

役割に応じた適切な操作権限を割り当てることで不正な処理・操作を防止します。

権限の設定例



メイン画面

各人にそれぞれ下記のような権限を設定することで、
●担当者が作成した案件は**管理者A、管理者Bを経由しないとクローズできず、**
●**クローズした案件はすべて承認済みであることを保証**できる。

省略不可

●インシデント担当者
変更、参照：○
承認、エスカレーション：×
クローズ：×

●インシデント管理者A
変更、参照：○
承認、エスカレーション：○
クローズ：×

●インシデント管理者B
変更、参照：○
承認、エスカレーション：×
承認済み案件のクローズ：○

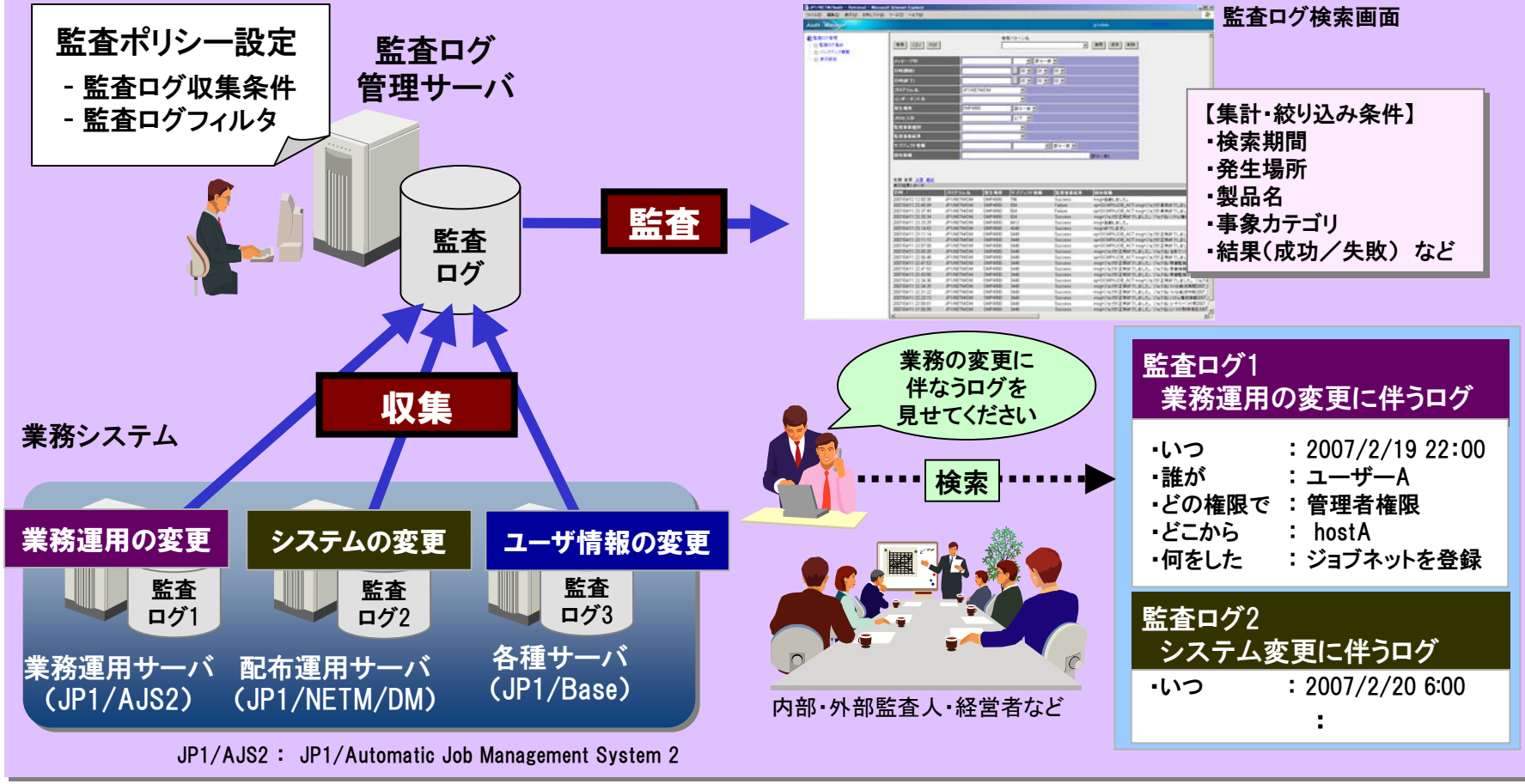
職務分掌を明確化し、作業手順を標準化して業務の信頼性を向上

3-10. 記録を収集し監査を支援

JP1/NETM/Audit

●サーバ運用に関するログ情報を自動収集し一元管理
●収集したログの調査は、さまざまな観点からきめ細かく容易に行えます

監査証跡管理の提供



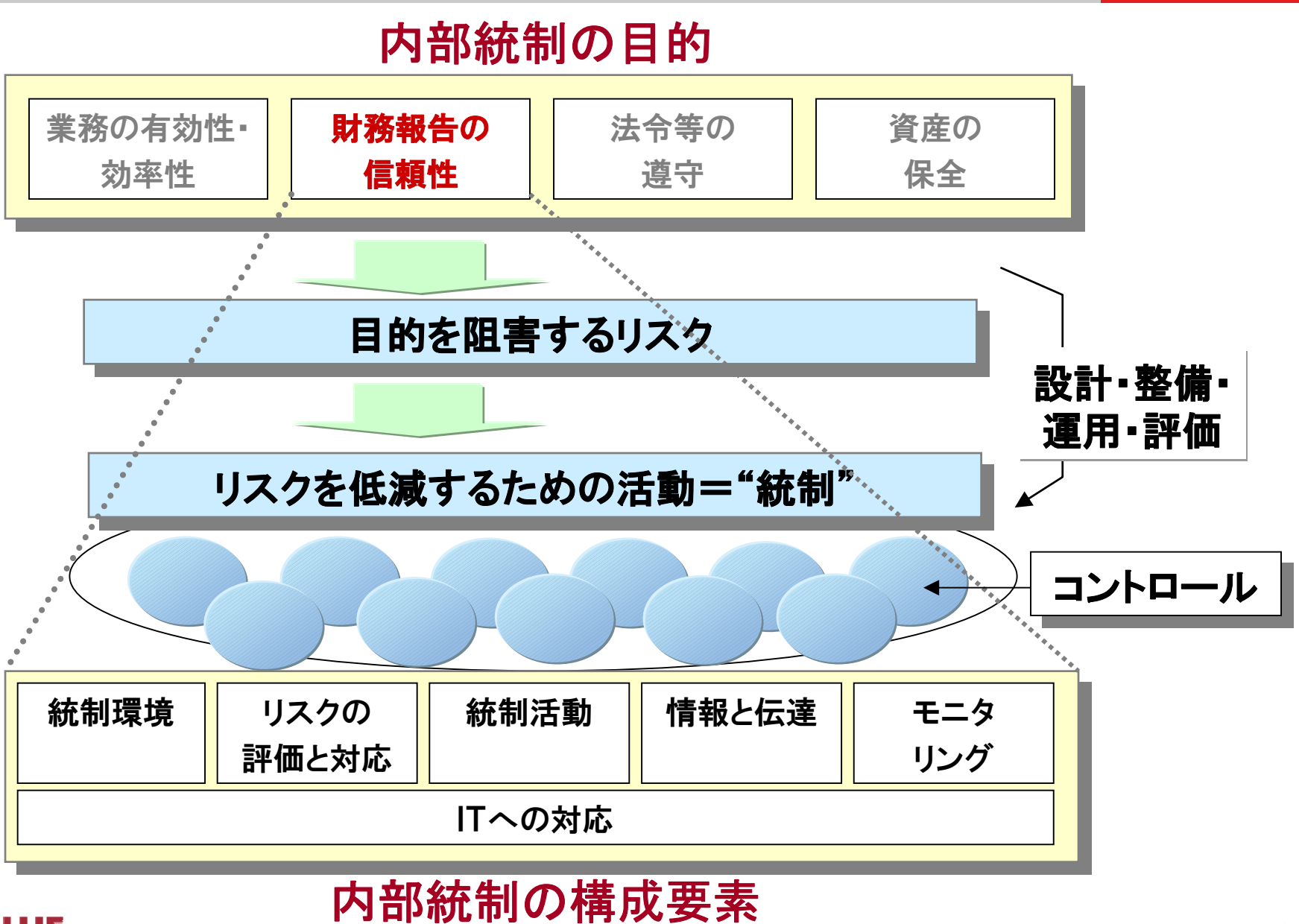
HITACHI
Inspire the Next

4

J-SOX法対応の落とし穴とその対策

uVALUE

4-1. 何が「リスク」となるかは目的によって異なる



4-2. J-SOX法対応の落とし穴

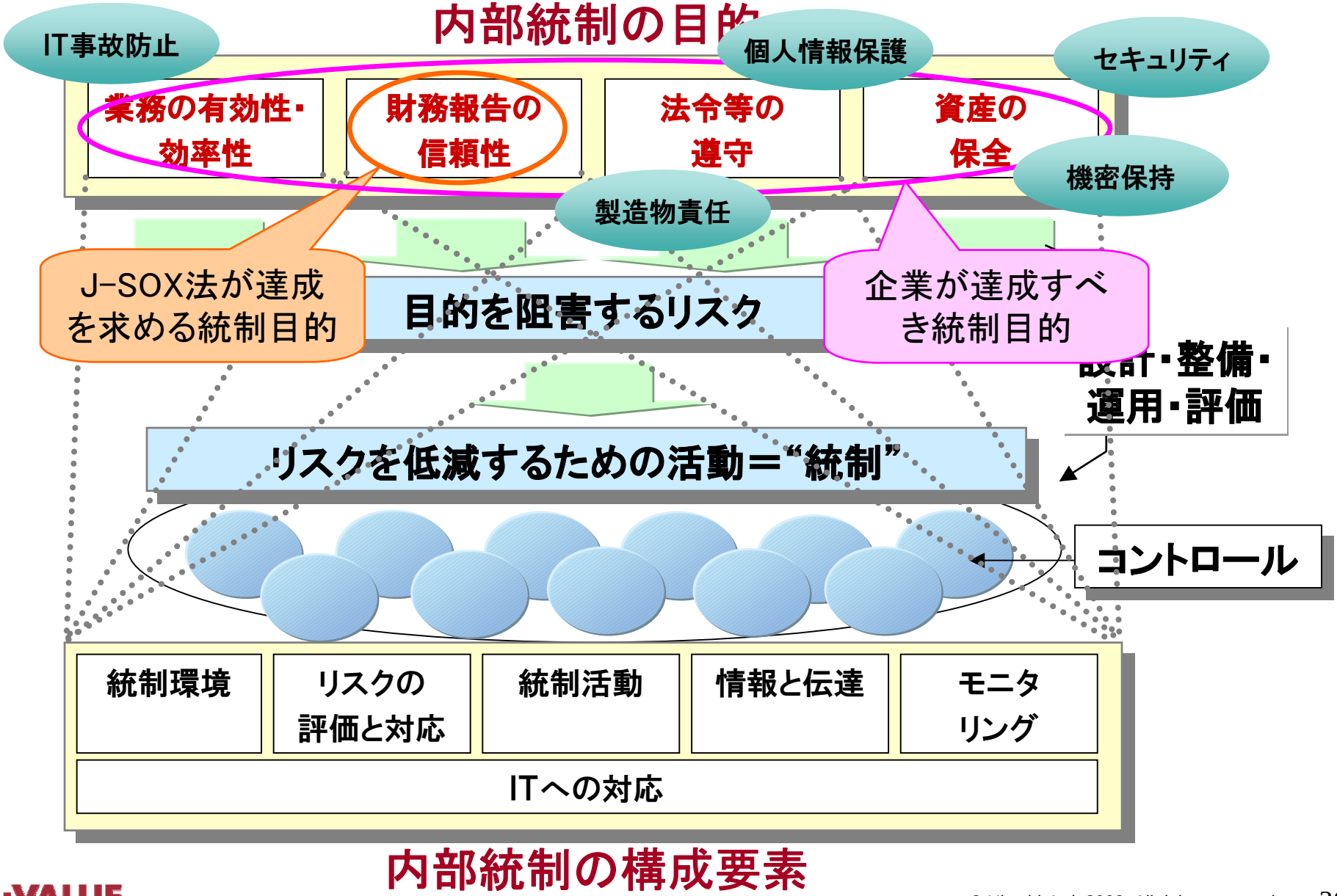
HITACHI
Inspire the Next

■金融商品取引法(J-SOX法)の目的は投資家保護
- 財務報告の信頼性(数字の正確さ)が問題
- その数字の良し悪しは問題ではない

■いわゆるセキュリティ管理は報告・監査の対象外
- 機密情報の漏えいやウィルス感染による業務停止で莫大な損失を出しても、その損失が正確に計上されていればJ-SOX法的にはOK
- では、セキュリティ確保のためのIT整備は不要？

■企業が達成すべき内部統制は、J-SOX法が要求する統制だけではない
- 企業は、内部統制における他の目的をも満たせるようにITシステムを整備しなければならない

4-3. より広範なリスクへの対処が必要

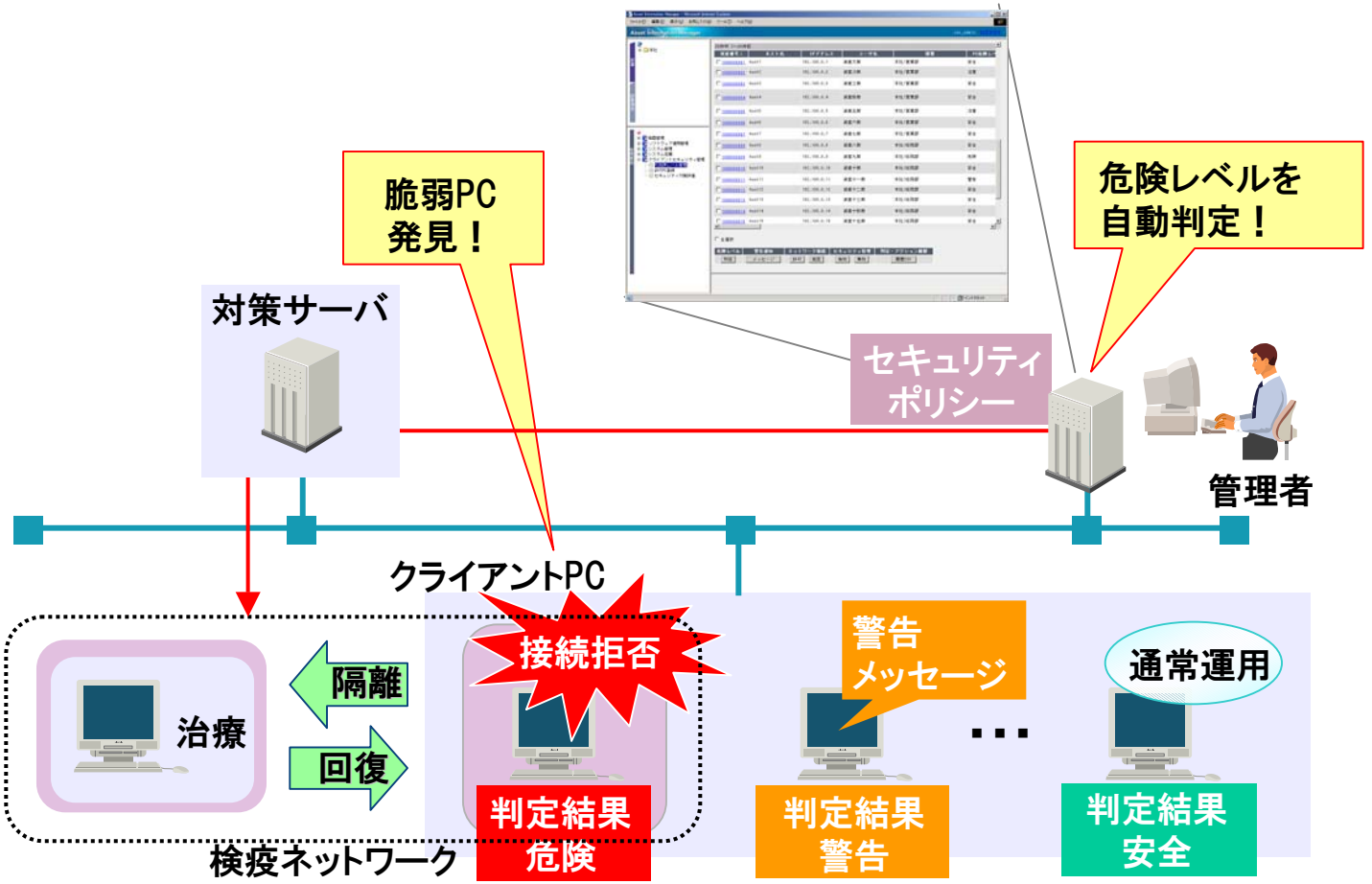


4-4. 脆弱なクライアントPCの隔離と治療

HITACHI
Inspire the Next

●セキュリティポリシーに基づくクライアントPCの検疫システムを実現

ウィルス感染や情報漏えいにつながる脆弱なクライアントPCを検出
業務ネットワークに接続する前に検査、隔離、治療を行い、エンドポイントで脆弱性を除去

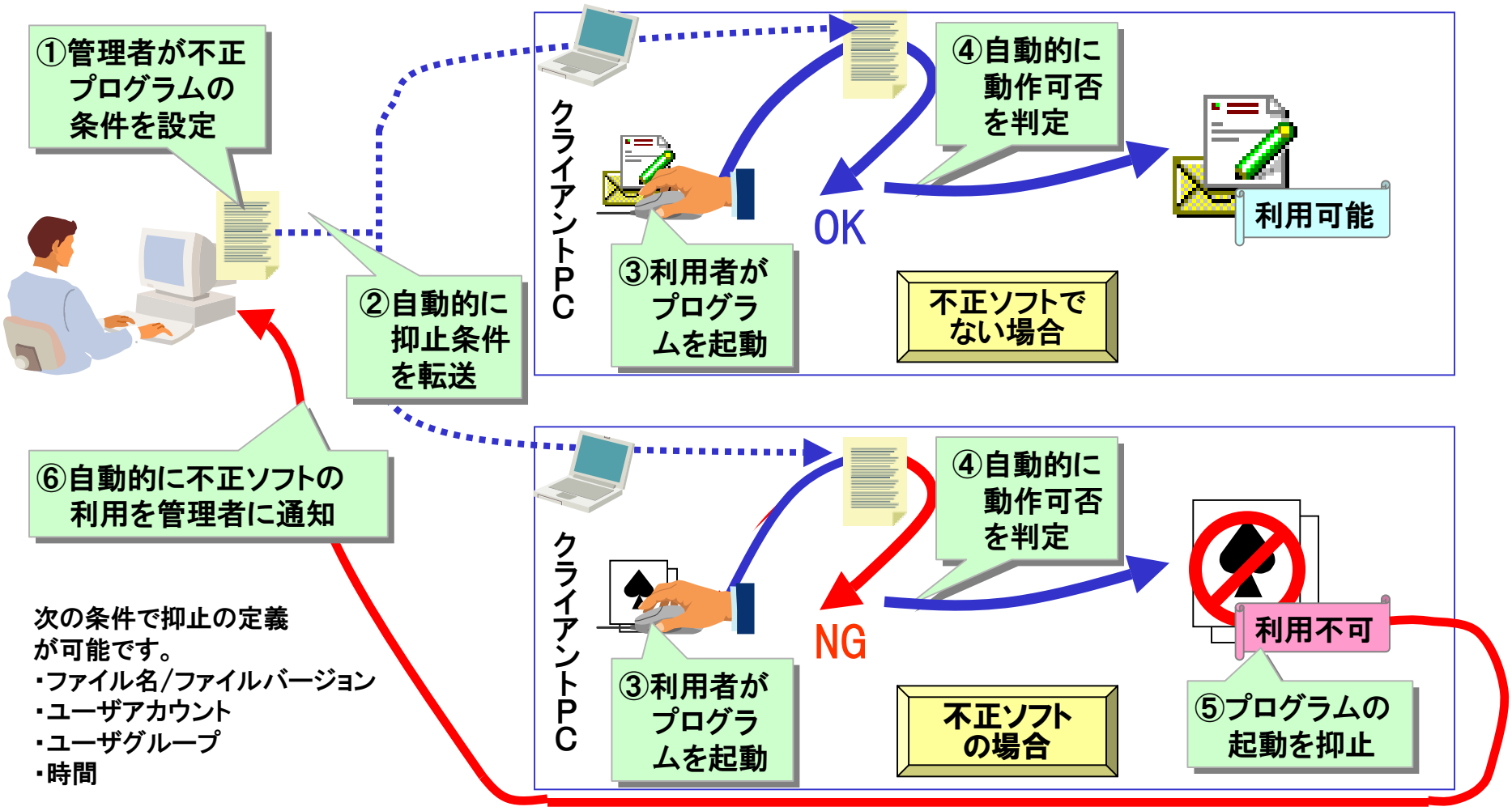


uVALUE

4-5. 不正ソフトウェアの起動抑止

HITACHI
Inspire the Next

●事前に登録された不正ソフトウェアのクライアント上での実行を抑止し、管理者に通報します。



次の条件で抑止の定義が可能です。
・ファイル名/ファイルバージョン
・ユーザアカウント
・ユーザグループ
・時間

4-6. 情報漏えいの防止

HITACHI
Inspire the Next

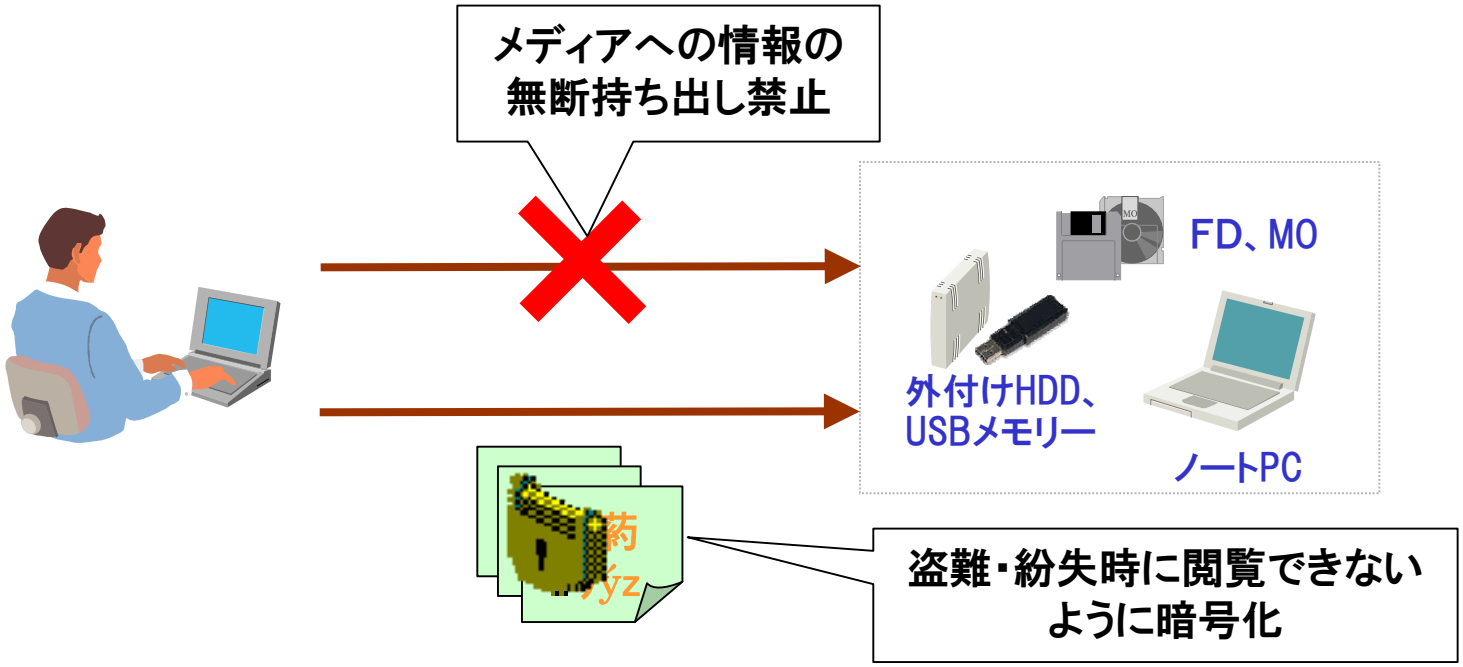
情報を持ち出させない　　**持ち出しても漏えいさせない**

●持ち出し制御

リムーバブルメディア(USBメモリー、MD、FDなど)へのファイル無断書き出しを禁止し、
社外へのファイルの持ち出しに関するモラルを向上できます。

●リムーバブルメディアやノートPCの暗号化

リムーバブルメディアにファイルを書き出す際に、自動的に暗号化できます。
また、ノートPCのドライブも暗号化できます。これにより盗難・紛失による漏えいを防止します。



HITACHI
Inspire the Next

5
まとめ

uVALUE

5-1. 内部統制時代の企業情報システムの勘所

HITACHI
Inspire the Next

- ITを活用することにより、業務の統制を強化・効率化するとともに統制活動とその評価に要する時間を短縮できる(ITに係る業務処理統制)
- 業務処理統制は、ITに係る全般統制が有効に機能していることを前提として成り立っている
- 全般統制の整備では、IT資源に対する変更が正しい手順に従って認可・実行され、その証跡が残されていることが重要
- **日立オープンミドルウェアは、ITに係る業務処理統制および全般統制の改善・強化を強力に支援します**
- 企業が達成すべき内部統制は、J-SOX法が要求する統制だけではない
  - 企業は、内部統制における他の目的をも満たせるようにITシステムを整備しなければならない

HITACHI
Inspire the Next

各製品の詳細についてはデモコーナーをご覧ください。
ご高覧、ご検討の上、弊社にご下命賜ります様
宜しくお願い申し上げます。

内部統制時代の企業情報システムの勘所

2008/2/12

株式会社日立製作所 ソフトウェア事業部 新分野事業推進室

uVALUE

HITACHI
Inspire the Next

他社商品名、商標等の引用に関する表示

•ITILは，英国政府OGC（Office of Government Commerce）のCommunity Trade Markおよび U.S. Patent and Trademark Officeにおける登録商標です。

その他記載されている会社名、製品名は各社の商標または登録商標です。

●画面表示をはじめ、製品仕様は、改良のため変更することがあります。

uVALUE