

JP1による内部統制強化のススメ

～ JP1 V8.1で実現する内部統制支援とは ～

2007.6.6



株式会社 日立製作所 ソフトウェア事業部
ネットワーク管理ソフト設計部
加藤 恵理

Contents

1. 内部統制・・・何のためにやるのか？
2. 業務プロセスに潜むさまざまなリスクと
ITを活用した統制のポイント
3. JP1 V8.1による内部統制強化支援とそのポイント
4. JP1 による内部統制支援
5. JP1 による内部統制強化のススメ

1

内部統制・・・何のためにやるのか？

1-1. 内部統制とは？

1-2. 内部統制の整備は IT 抜きには成立しない

1-3. 「ITへの対応」を二つの側面から考える

内部統制とは、

経営者・従業員の不正・ミスによるリスクを無くすための
仕組み、および組織的活動



統制 (コントロール)

- 規則/手順の存在
- 規則通り業務/活動が行われていることに関する組織的なチェック等の活動

事前対策により、
リスクを防ぐ

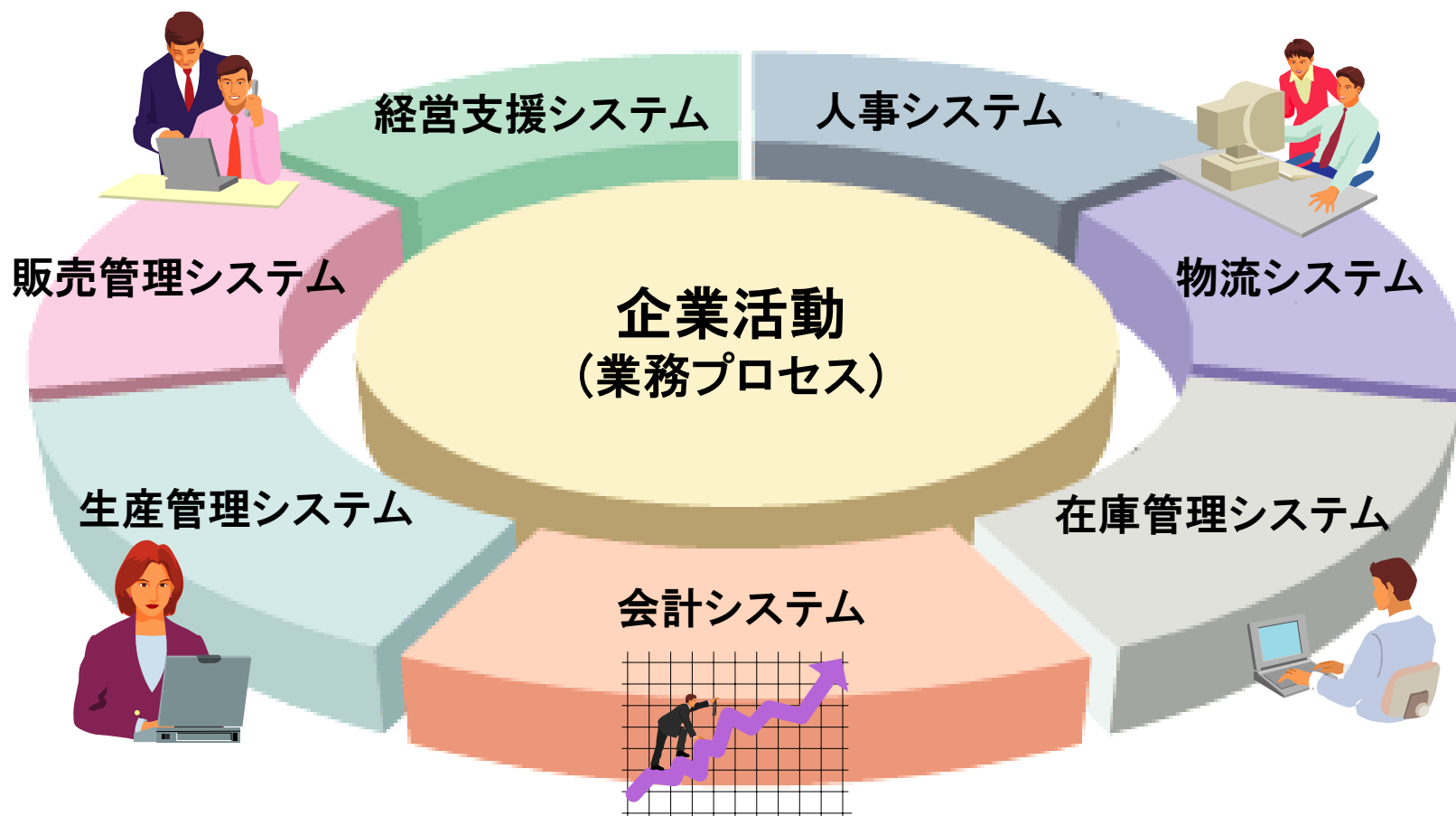
不正
・
ミス

- ◆ 財務諸表の改ざん/不当表示
→ 費目の付け替え、期末の押し込み
- ◆ オペレーションミス
- ◆ 犯罪(会社資産の個人使用)
- ◆ ミス/不正の隠匿

リスク

- ◆ 資本市場からの信頼喪失
→ 株価暴落、上場廃止
- ◆ 顧客からの信頼喪失
→ 不買運動による業績低下
- ◆ 行政処分

財務会計を始めとする企業の業務プロセスの多くは、
ITシステムによって処理されている。



ITによる統制

業務リスク削減のために
ITの機能↓を活用する

- ・判断/処理のルール化
- ・異常値の検知とアラーム
- ・例外処理の禁止
- ・証跡の取得
- ・業務関連者の限定 等

ITを活用して、間違いや不正な処理が
起きない強固な業務の統制を実現する

業務リスクの把握

ITの統制

IT構築・運用の不備に
起因するリスク↓を削減する

- ・システム変更による不正処理
- ・プログラムのバグ等による
異常処理
- ・不正目的のデータ改竄
- ・システムダウン、データ消失等

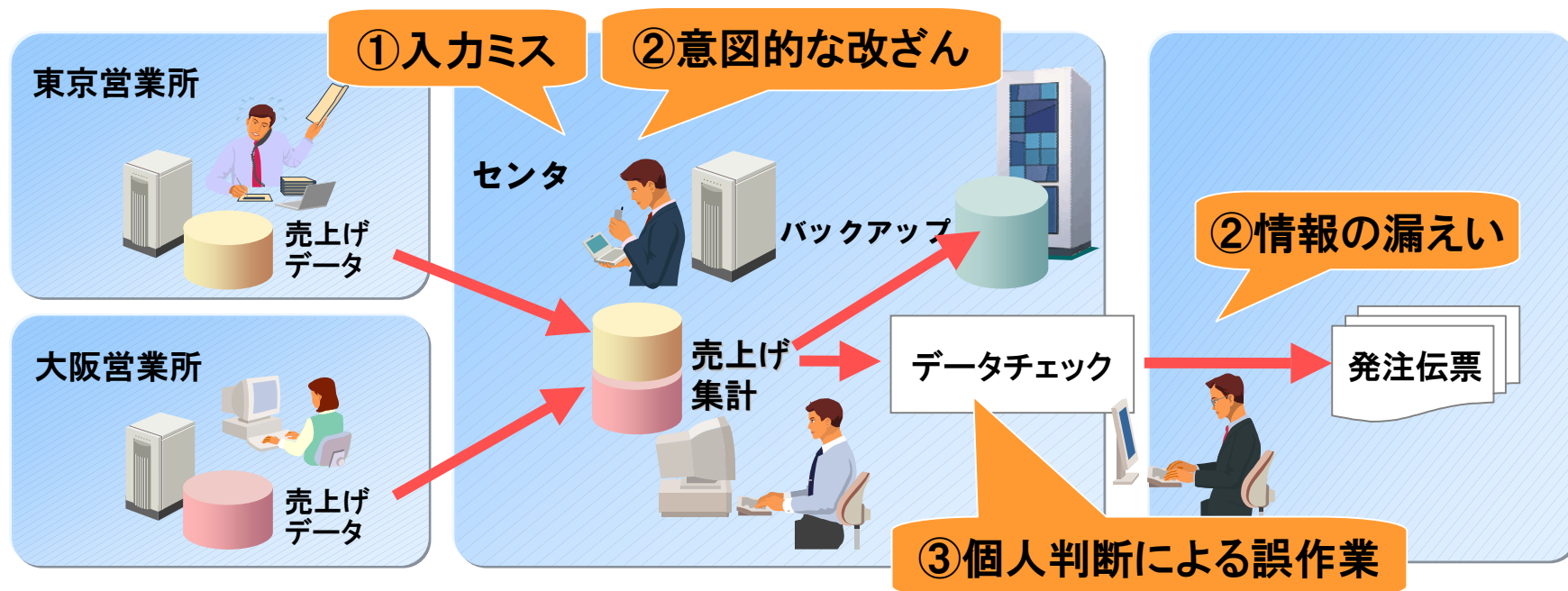
IT自身を信頼できるものにするために
セキュリティや運用の面から統制すること

ITリスクの把握

2

業務プロセスに潜むさまざまなリスクと ITを活用した統制のポイント

- 2-1. 業務に人が介在することのリスク
- 2-2. 作業手順の未整備によるリスク
- 2-3. システム監視の不備によるリスク
- 2-4. 業務運用実績の確実な記録とその証明
- 2-5. ITを活用した主な統制ポイント



■考えられるリスク

- ① データ入力ミスによる誤ったデータをチェックする手段が不十分
- ② 担当者に必要以上の権限を与えているため、データの改ざん・漏えいが発生しやすい環境になっている
- ③ 担当者の勝手な判断による誤作業 など

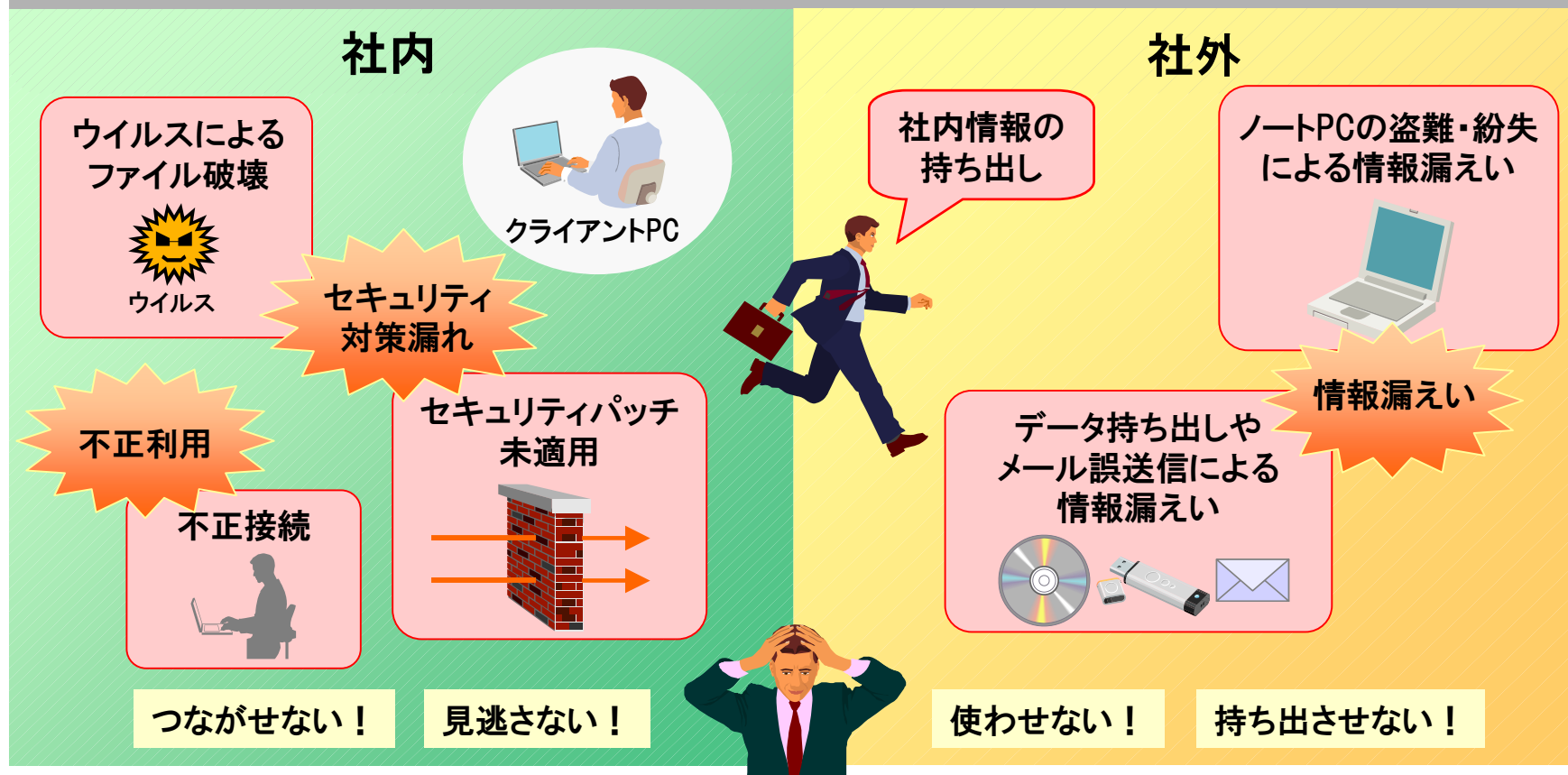
ITを使って整備すること

業務の自動化

業務を自動化することで
ミスや不正を排除する

安定したサービスの提供

ビジネス環境におけるセキュリティ脅威



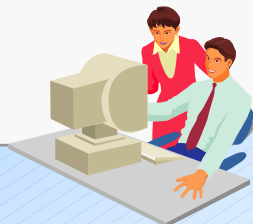
ITを使って整備すること

クライアントPCの統制

クライアントPCと媒体の統制

→ 安全なビジネス環境の維持

システム変更は口頭での
依頼で、現場が独自に実施



新計算方式の変更が反映されず、
誤った帳票を提出

データ入力、帳票チェックなど、
一人が複数の業務を兼務



データ改ざんや情報漏えい事件に発展

ITを使って整備すること

作業プロセスの統制とシステムの変更管理

システムの変更が正当な手続き・承認の下に
行われ、管理されていること

業務を分担し、互いにチェックしあうなど、
権限の分離がおこなわれていること

確実な変更の実施

→ 不正な処理の回避

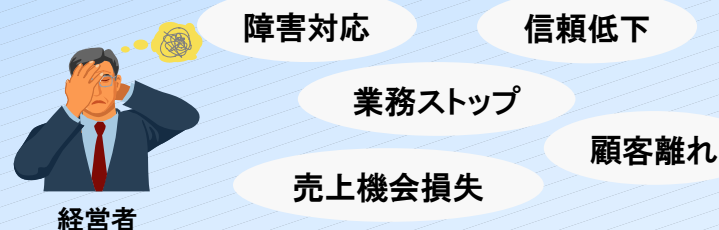
業務分担、権限の分離

→ ミスや不正行為が起こりにくい環境

問題は検知できていたが、
担当者不在でそのまま放置



後に、重大なシステム障害に
発展し、ビジネスに影響

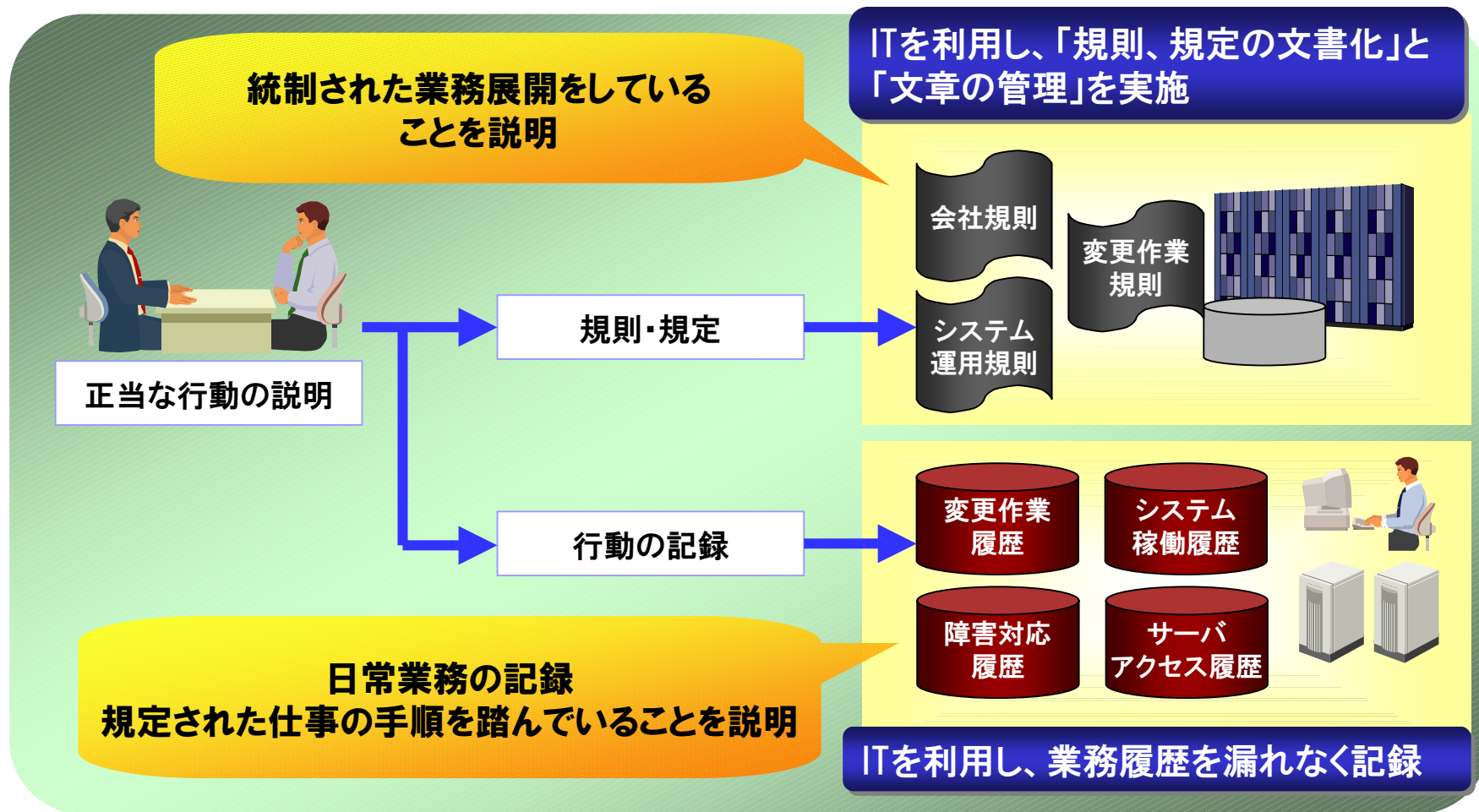


ITを使って整備すること

システムの稼働監視

問題の対策状況が把握でき、
システムが正常に稼働するように管理されていること

障害予兆の早期把握 → ビジネスへの影響を最小限にとどめる



ITを使って整備すること

活動履歴の採取

業務を見える化

→ 業務システムの正当性の証明

ミスや不正を起こりにくくするために...

業務の自動化

- ・安定したサービスの提供
- ・人の介在によるリスクの回避

安全なシステム環境を維持するために...

クライアントPCの統制

- ・情報漏えいリスクの回避
- ・安全なビジネスインフラの構築

業務要件の変更に追従するために...

作業プロセスの統制と システムの変更管理

- ・作業状況の監視
- ・不正な変更の回避

システムの信頼性を保障するために...

システムの稼働監視

- ・処理能力超過による異常動作の回避
- ・システム増強計画時のボトルネック把握

各プロセスの正当性を証明するために...

活動履歴の採取

- ・業務システムの正当性を証明
- ・各種作業の正当性を証明

3

JP1 V8.1による内部統制強化支援とそのポイント

3-1. JP1が考える新たな時代の運用管理

3-2. JP1 V8.1 デビュー

3-3. JP1 V8.1 による内部統制強化のポイント

経営とITが融合したビジネスレベルのシステム運用実現

- SOAシステムの運用PDCAサイクルを最適化
- J-SOX法対応に必要なIT全般統制のPDCAサイクルを最適化

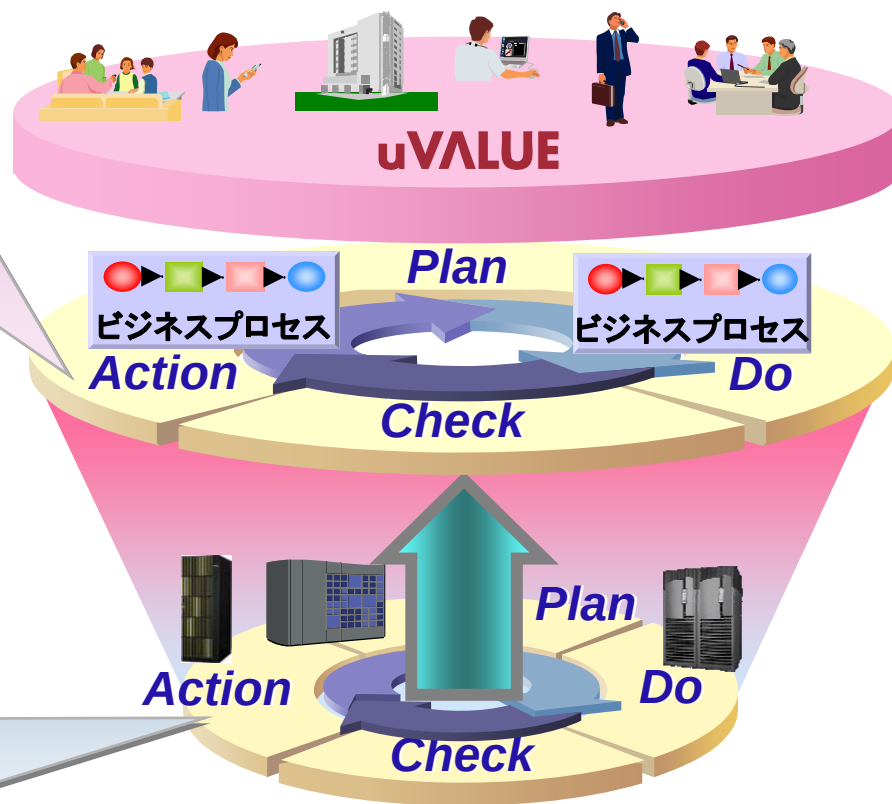
これから

ビジネスの観点を取り入れて
運用プロセスの
PDCAサイクルを最適化

ビジネスレベル運用

これまで

ITレベルで
運用プロセスの
PDCAサイクルを最適化



ビジネス

ビジネスレベル
〔ビジネスプロセス、
サービス〕ITレベル
IT資産
〔ハード/ソフト〕

ビジネスレベル運用を確立する
運用管理の羅針盤へ

JP1 V8.1
— 内部統制の強化 —

2007/3末出荷開始

JP1
Version 8

2006/6末出荷開始

ポリシーベースの
自律運用管理

JP1
Version 7i

2003/7末出荷開始

ITによる内部統制強化
の支援

変化の激しいビジネス環境において、
サービス品質の維持とビジネスの透明性確保を支援し、
最適なビジネスレベル運用を実現

IT運用プロセスの統制強化

● ITプロセス管理: JP1/IM-SS

審査・承認を漏れなく行うなど運用プロセスの統制により、
確実に正しい業務運用を遂行します。

新製品

正しく運用させる
ための統制

JP1/IM-SS : JP1/Integrated Management - Service Support



正しく運用されて
いるかの証明

運用実績の記録と管理の容易化

● 監査証跡管理: JP1/NETM/Audit

業務システムにおいて内部統制がきちんと機能していることを
証明するために必要とされる証跡記録を管理して監査を実現します。

新製品

4

JP1による内部統制支援

4-1. 業務の自動化

4-2. クライアントPCの統制

4-3. 作業プロセスの統制とシステムの変更管理

4-4. システムの稼働監視

4-5. 活動履歴の採取

ミスや不正を起しにくくするために...

業務の自動化

オートメーション

安全なシステム環境を維持するために...

クライアントPCの統制

ITコンプライアンス

業務要件の変更に追従するために...

作業プロセスの統制と
システムの変更管理

モニタリング

ITコンプライアンス

システムの信頼性を保障するために...

システムの稼働監視

モニタリング

各プロセスの正当性を証明するために...

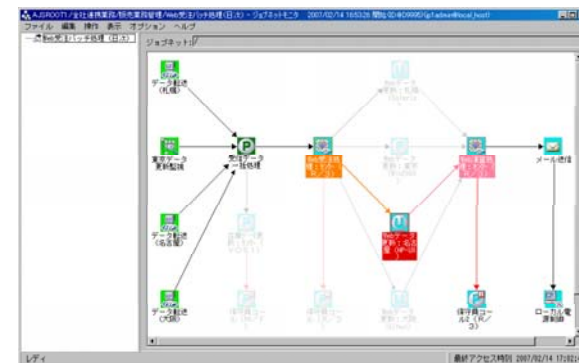
活動履歴の採取

ITコンプライアンス

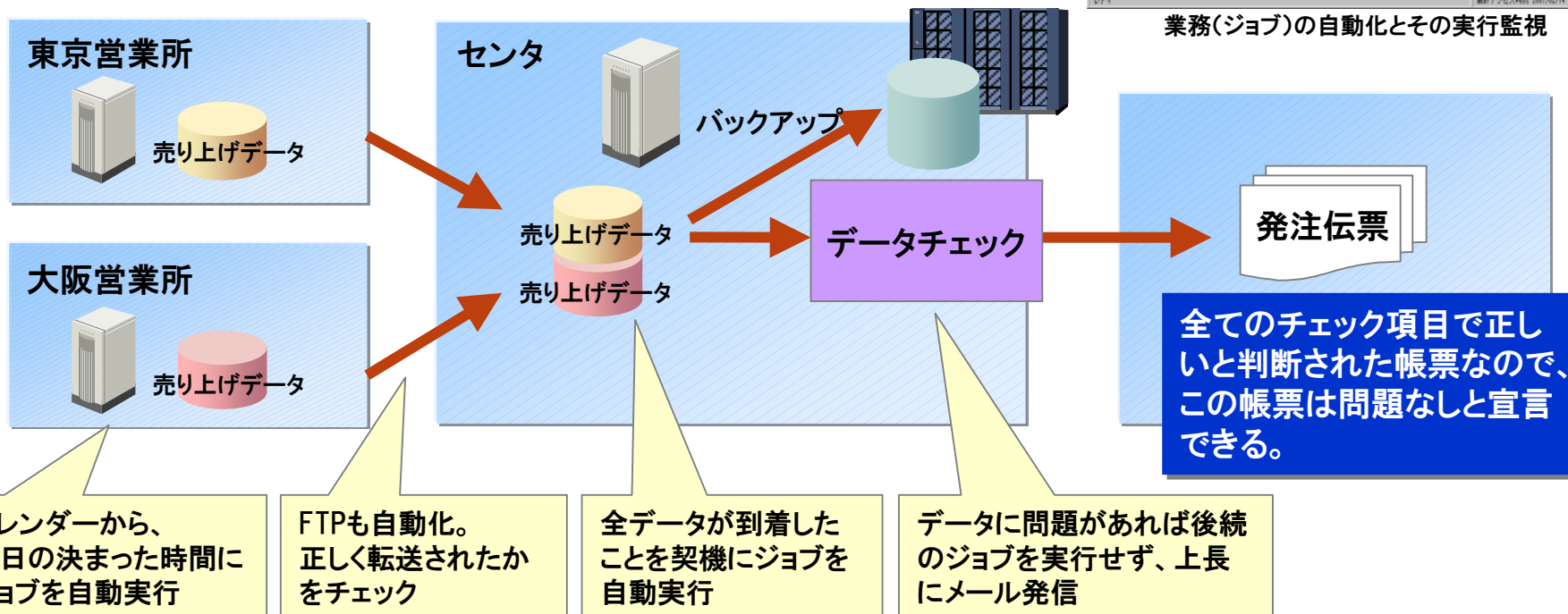
- 日々実行される業務を自動化することでシステムを正しく動かし、人手によるリスクを軽減します。

例えば、次のようにリスクを回避できます

- ・スケジュールに従った自動運転のため、作業の遅れが発生しない
- ・ファイル転送ミスによるデータの欠落をチェック
- ・全データがそろってから計算を実施
- ・チェックも自動化し、問題があれば処理を中断



業務(ジョブ)の自動化とその実行監視



● クライアントPCからの情報漏えいの主な原因は、以下の2つです。

- ・従業員のセキュリティ対策に対する意識の低さ
- ・社内でのクライアントセキュリティ対策漏れ

ITによって情報漏えいを回避し、安全なビジネス環境の維持を支援します。

不正ソフトウェアを
使わせない

ウイルス対策
脆弱性対策

不正なPCの排除

社内情報を自宅に
持ち帰らせない

部署	最低点	平均点	台数
横浜支社/営業本部/第一営業部	3	51	32
横浜支社/営業本部/第二営業部	3	48	33
横浜支社/開発本部/第一開発部	6	55	31
横浜支社/開発本部/第三開発部	3	51	30
横浜支社/開発本部/第二開発部	3	51	45
川崎支社/人事本部/第一人事部	3	53	37
川崎支社/人事本部/第三人事部	6	49	28
川崎支社/人事本部/第四人事部	8	48	27
川崎支社/人事本部/第二人事部	6	58	44
川崎支社/品質保証本部/第一品質保証部			20
川崎支社/品質保証本部/第二品質保証部			34

クライアントPCの
セキュリティ対策評価

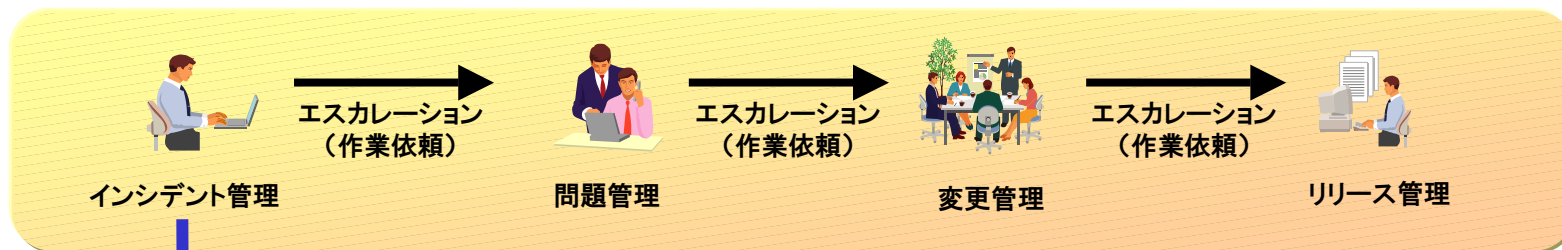
不正PC接続件数の集計

ネットワーク	サブグループ	グループ	IPアドレス	最終取得時刻	日	月	火	水	木	金	土	日
営業部	本社	本社	192.168.0.5	2007/01/16 18:58:55	13	18	30	16	0	0	0	0
総務部	本社	本社	192.168.1.5	2007/01/16 18:58:55	13	18	30	16	0	0	0	0
横浜支社	関東	支社	192.168.2.5	2007/01/16 18:58:55	13	18	30	16	0	0	0	0
千葉支社	関東	支社	192.168.3.5	2007/01/16 18:59:13	55	59	86	58	0	0	0	0
名古屋支社	中部	支社	192.168.4.5	2007/01/16 18:58:55	13	18	30	16	0	0	0	0
大阪支社	関西	支社	192.168.5.5	2007/01/16 18:58:55	13	18	30	16	0	0	0	0

漏れのないクライアントセキュリティ対策を実現するためには、
従業員のモラル向上 + ITの仕組みでガードすることが必要！

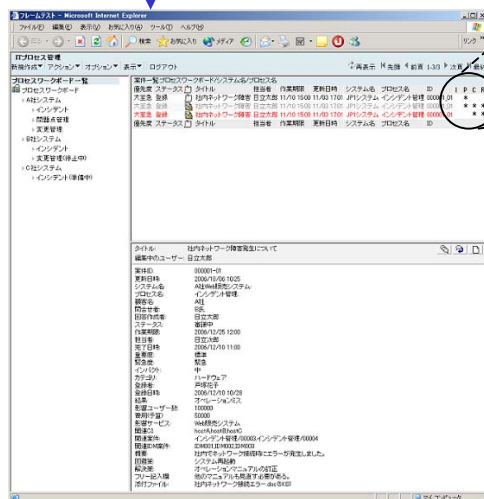
プラス

- ITIL®に沿った運用プロセスの統制を実現。エスカレーションや作業状況の監視など、作業統制に必要な運用を支援し、作業手順の未整備によるリスクを軽減します。



参照

依頼した作業の
状況はどうだろう？



メイン画面

時	IPCR
12/15 19:44:51	*
12/15 19:45:24	* * * *
12/15 19:45:41	* * *
時	IPCR

詳細表示

案件がどの段階までエスカレーション
されたかわかります(サマリ表示)

- ・I (Incident) : インシデント管理
- ・P (Problem) : 問題管理
- ・C (Change) : 変更管理
- ・R (Release) : リリース管理

システム	プロセス	案件ID	ステータス	エスカレーション元ID	エスカレーション先ID	プロセスID
システムA	インシデント管理	PWS1-000001	クローズ	-	PWS2-000003, PWS2-000005	000005-01
システムA	問題管理	PWS2-000003	調査中	PWS1-000001	PWS2-000006	000005-02
システムA	変更管理	PWS2-000005	審議中	PWS1-000001	PWS2-000008	000005-03
システムA	変更管理	PWS2-000005	計画中	PWS2-000003	PWS2-000010	000005-04
システムB	変更管理	PWS2-000008	計画中	PWS2-000005	-	000005-05
システムA	リリース管理	PWS2-000010	受付	PWS2-000006	-	000005-06
システム	プロセス	案件ID	ステータス	エスカレーション元ID	エスカレーション先ID	プロセスID

関連案件状態画面(エスカレーション先の詳細)

さらに詳細がわかります。
エスカレーション先の案件は
調査中？担当者？ など

- 過去の変更履歴を確認できます。問題が発生した機器のハードウェアやソフトウェアの変更状況を確認でき、不正なシステム変更の防止を支援します。

部署	
変更日付	(YYYYMMDD) 以前 ▼
資産番号	
変更項目	☒ CPU ☒ メモリ ☒ ディスク

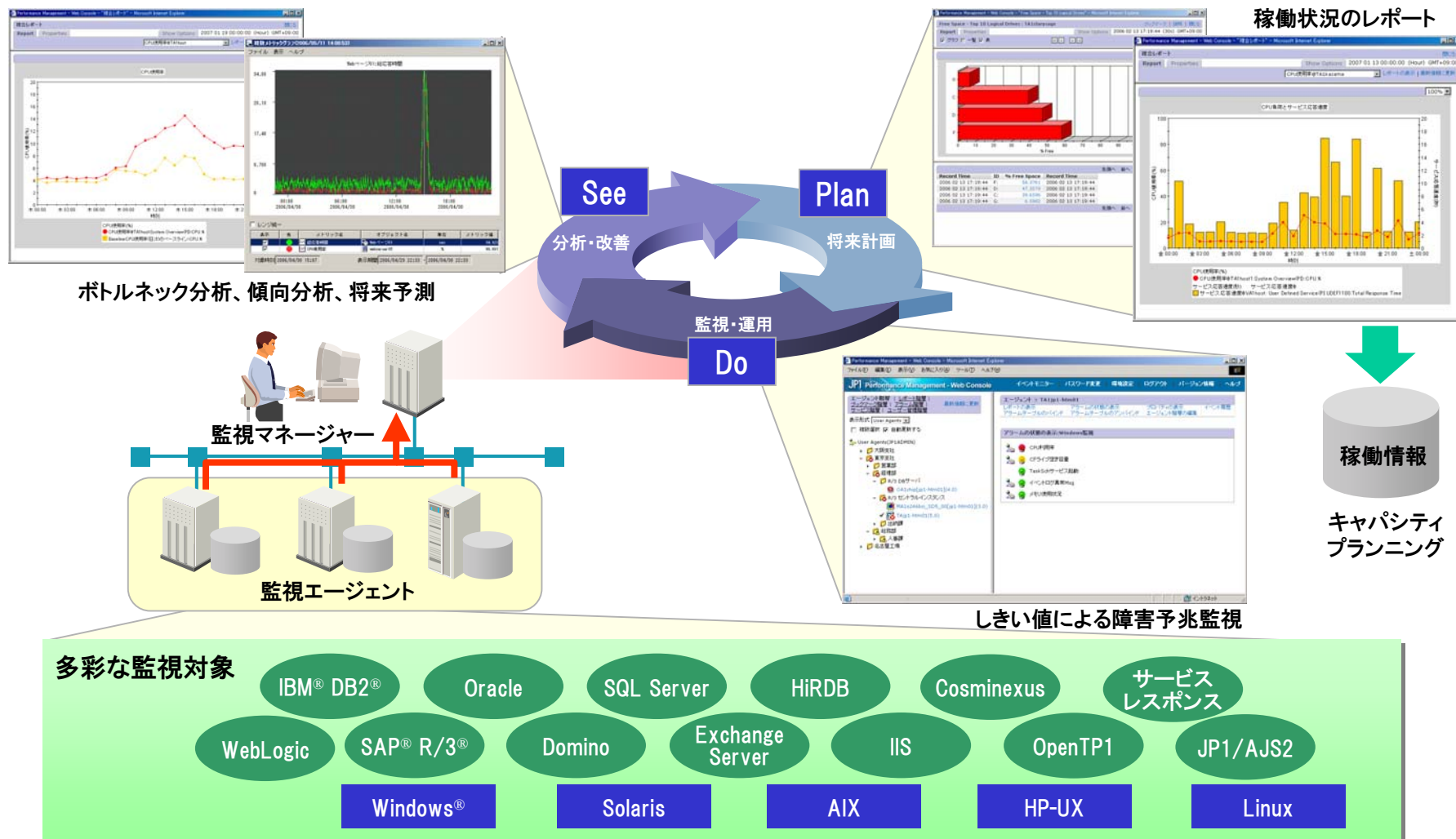
検索

変更日時、変更項目等の検索条件を指定して検索

検索条件に合った機器の一覧を表示

変更日付△	変更前	変更後	資産番号	部署	ユーザ名
2004/01/18 02:57:41	CPUクロック数: CPU数: CPU: メモリサイズ: ディスク容量:	CPUクロック数:1000MHz CPU数:2 CPU: Intel Pentium III メモリサイズ:128MB ディスク容量:20GB	1000000001	本社/営業部/営業1課	営業太郎
2004/01/20 02:00:00	メモリサイズ:128MB ディスク容量:20GB	メモリサイズ:256MB ディスク容量:40GB	1000000001	本社/営業部/営業1課	営業太郎
2004/01/25 02:00:00	メモリサイズ:256MB ディスク容量:40GB	メモリサイズ:512MB ディスク容量:60GB	1000000001	本社/営業部/営業1課	営業太郎
2004/02/01 02:00:00	メモリサイズ:512MB ディスク容量:60GB	メモリサイズ:1024MB ディスク容量:80GB	1000000001	本社/営業部/営業1課	営業太郎
2004/02/10 02:00:00	ディスク容量:80GB	ディスク容量:100GB	1000000001	本社/営業部/営業1課	営業太郎
2004/02/18 02:57:42	CPUクロック数: CPU数: CPU: メモリサイズ: ディスク容量:	CPUクロック数:500MHz CPU数:1 CPU: Intel Pentium III メモリサイズ:512MB ディスク容量:40GB	1000000005	本社/資産管理部	資産太郎

- システム内のさまざまな稼働状況を一元監視。障害予兆検知や、ボトルネック、将来予測などの分析を実現し、システム監視の不備によるリスクを軽減します。



- システム内のさまざまな事象を一元管理。障害発生場所の特定から影響範囲の把握まで迅速に対応できるため、対処遅れによるリスクを軽減します。

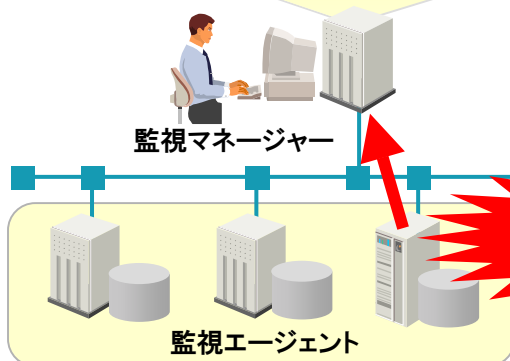


障害、予兆検知

場所の特定、影響範囲の把握

インシデントの自動登録

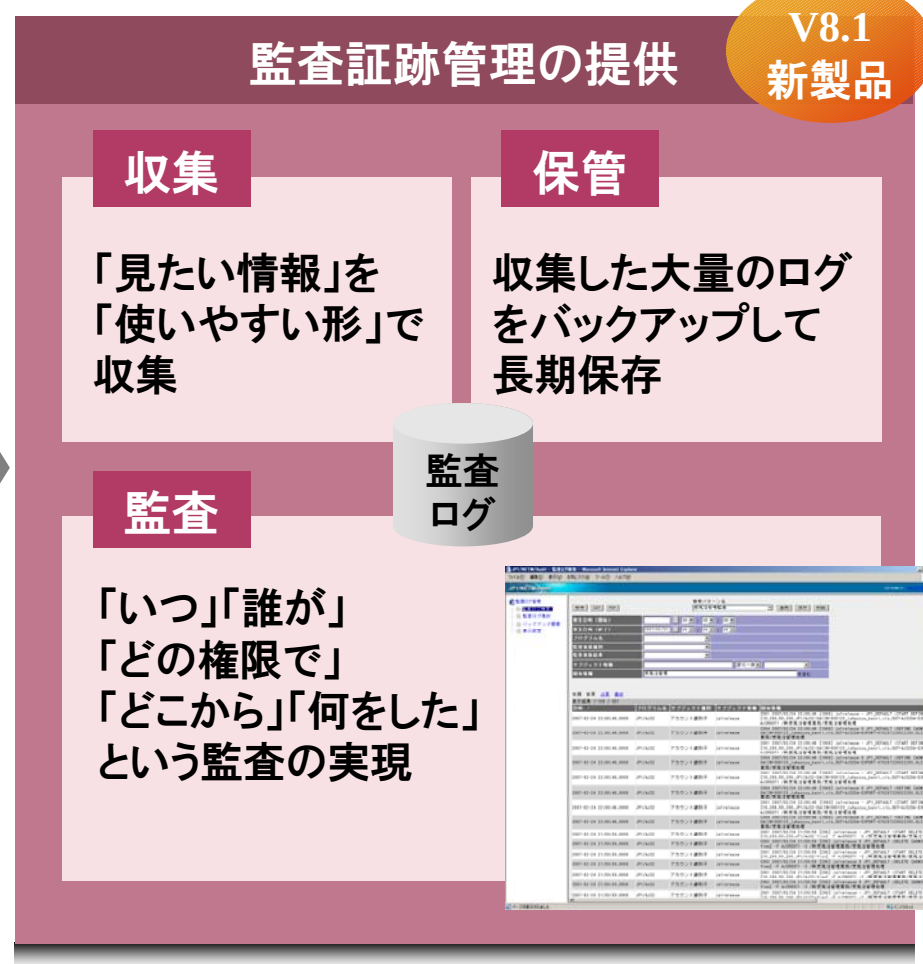
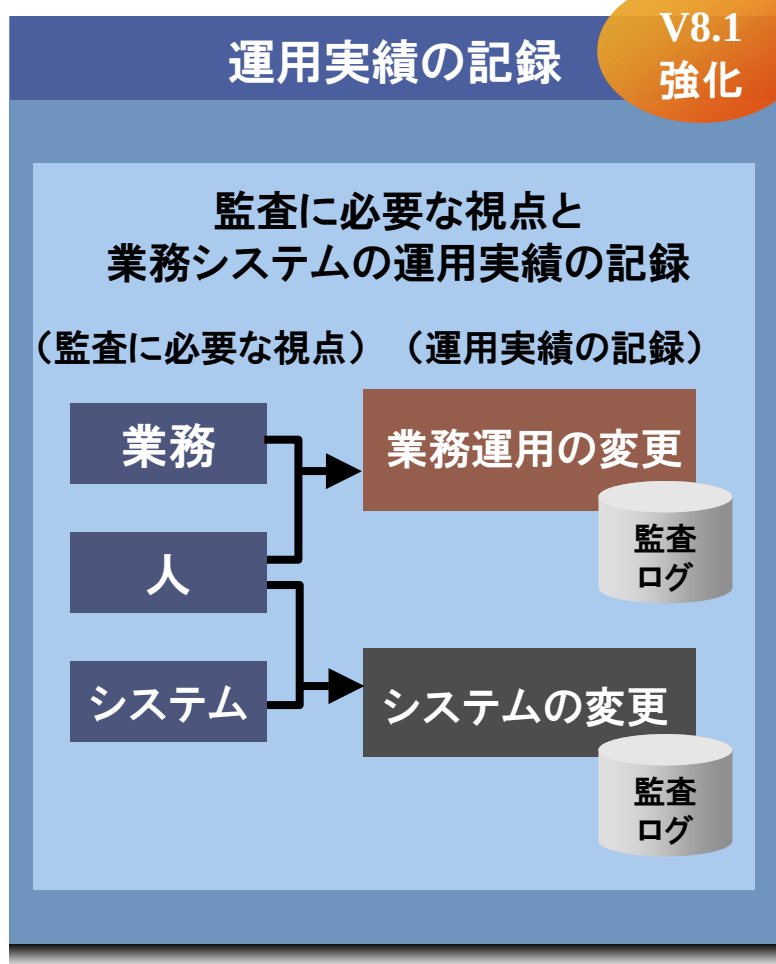
遠隔への自動通知



業務(ジョブ)の遅延
リソース不足の兆候
など



- 業務運用の変更、サーバ上で動作するアプリケーションの更新、ユーザー情報の追加・変更といった、サーバ運用に関するログ情報を自動収集し一元管理します。また、検索機能などにより、監査時の運用を容易化します。



- クライアントPCにおける各種操作ログを統合的に監査。
クライアント監査の支援や従業員のモラル向上が図れます。

操作ログの検索画面で、外部に持ち出したり、
印刷を実行したファイルの追跡に必要な情報を取得。

取得可能なログ

- ・外部への持ち出し
- ・ファイルのコピー
- ・ファイルの移動、削除、印刷
- ・アプリケーションの起動 等

ファイル名や、外部媒体
へのコピーなどの操作で
ログ情報を絞り込み

マネージャー

JP1/NETM/DM Manager

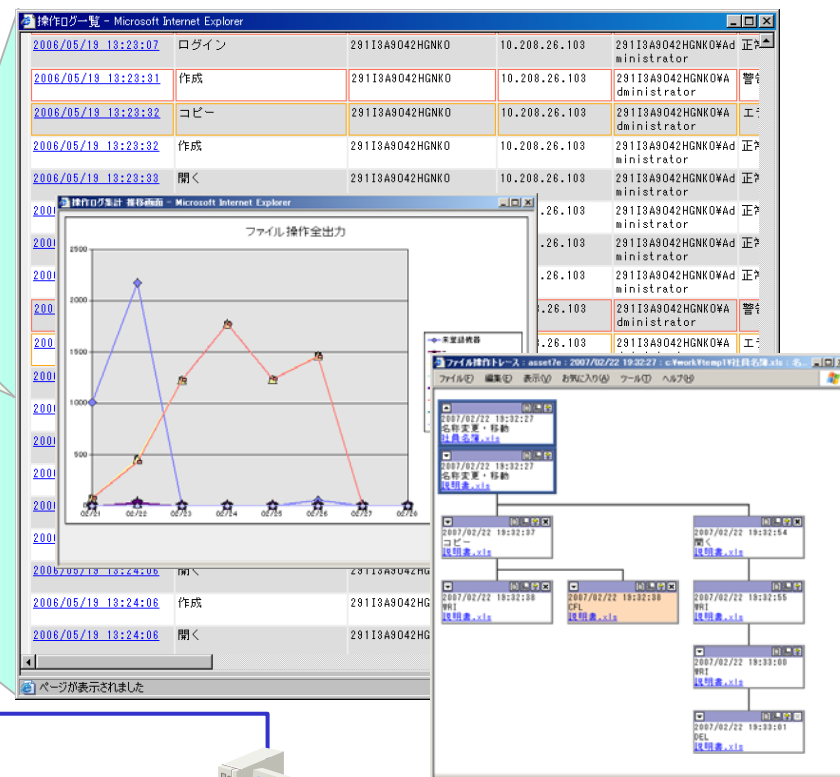
ファイル操作の
ログ情報を取得

ファイルのコピー、
移動、削除など
を実行

クライアントA

クライアントB

クライアントZ



5

JP1による内部統制強化のススメ

5-1. 内部統制を行うとこうなる！

5-2. 内部統制を支える運用管理ツール選択のポイント

内部統制は
J-SOX法に対応するため？

ー(マイナス)のイメージ



本来の業務とは別の
新たな課題が増える

コストが
かかる

発想の転換

内部統制は

●業務を見直し、効率化を図る良いきっかけ

- 新たな課題が増えるのではなく、本来あるべき姿にする
- コスト削減につながる

●強い企業に変わるチャンス！

+(プラス)のイメージ



せっかくやるなら
前向きに！

内部統制を行うと・・・

- 不正やミスが減る
= 余計な仕事が発生しない
→ リスクが小さくなる
- 業務の見直し、効率化が図れる
→ コストが下がる
→ 本来あるべき正しい業務プロセスになる
→ 業績アップにつながる

- 企業競争力、企業価値が高まる
(経営者や株主にとってもメリット)
- もちろん、J-SOX法に対応できる



①必要な部分から小規模に導入可能

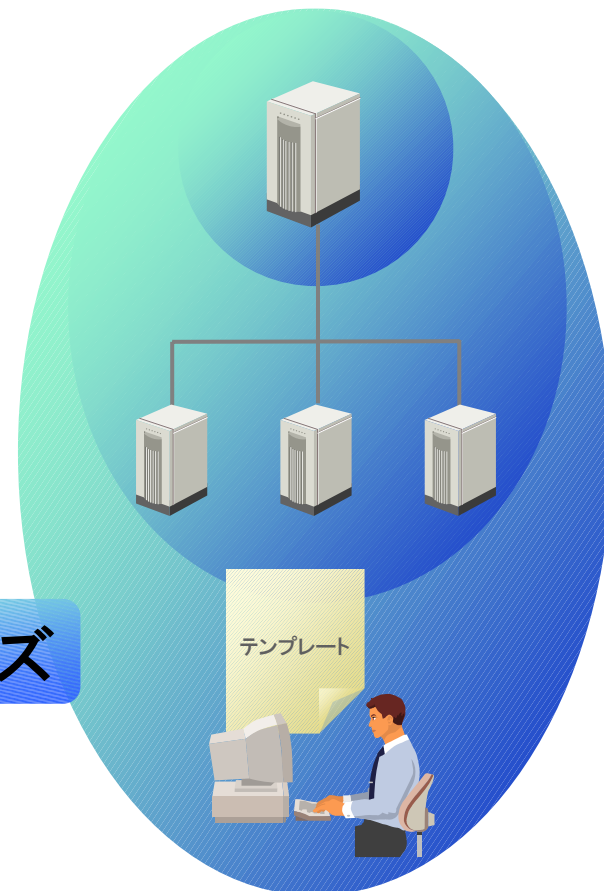
- ・内部統制の準備には時間をかけられない

②将来、システム全体への拡張が容易

- ・別システムを管理するときに別のツールが必要では、
かえって運用管理の負荷が高くなる

③テンプレート装備で運用開始がスムーズ

- ・高機能でも、使いこなせなければ運用負荷が高くなるだけ
- ・ツールの習熟に時間や費用をかけられない



JP1はすべての条件を満たしている上、さらに安心をプラス！

長期の存続性

+

豊富な導入実績

+

サポート力

内部統制の強化と同時に、企業価値を向上させる ITインフラの実現を支援します。

他社商品名、商標等の引用に関する表示

他社商品名、商標等の引用に関する表示

- AIXは、米国における米国International Business Machines Corp.の登録商標です。
- BEA WebLogic Serverは、BEA Systems, Inc.の登録商標です。
- DB2は、米国における米国International Business Machines Corp.の登録商標です。
- HPIは、米国Hewlett-Packard Companyの会社名です。
- HP-UXは、米国Hewlett-Packard Companyのオペレーティングシステムの名称です。
- IBMは、米国における米国International Business Machines Corp.の登録商標です。
- ITIL (IT Infrastructure Library) は、英国および欧州連合各国における英国政府OGC (Office of Government Commerce) の商標または登録商標です。
- Java、およびJavaに関連するすべての商標およびロゴマークは、米国 Sun Microsystems, Inc. の米国およびその他の国における商標または登録商標です。
- Linuxは、Linus Torvaldsの米国およびその他の国における登録商標あるいは商標です。
- Microsoftは、米国およびその他の国における米国Microsoft Corp.の登録商標です。
- ORACLEは、米国Oracle Corporation の登録商標です。
- R/3は、SAP AGのドイツおよびその他の国における登録商標または商標です。
- SAPは、SAP AGのドイツおよびその他の国における登録商標または商標です。
- Solarisは、米国Sun Microsystems, Inc. の米国およびその他の国における商標または登録商標です。
- Sunは、米国Sun Microsystems, Inc. の米国およびその他の国における商標または登録商標です。
- Windowsは、米国およびその他の国における米国Microsoft Corp.の登録商標です。
- 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。

◇ 本製品を輸出される場合には、外国為替 及び外国貿易法並びに米国の輸出管理関連法規などの規制をご確認の上、必要な手続きをお取りください。
なお、ご不明な場合は、弊社担当営業に お問い合わせください。

● 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。