People Assisting People

HITACHI Open Middleware World in KANSAI 2008

2008年2月12日（火）
【B-1】14:00～14:20

ＩＴ全般統制対応 内部統制評価支援ツール
【監査れポータル】 のご紹介

株式会社アシスト
西日本支社
2008年1月1版

情報活用のアシスト

Copyright © 2008 K.K. Ashisuto

内部統制に求められるもの　・・・おさらい

情報システムは業務プロセスと一体化
情報システムリスクはビジネスにおけるコアリスクとなっている

↓

リスクは連鎖する性質を持つ
些細な不具合や単純ミスが損害賠償責任に発展することも

↓　↓

経営者に求められる役割
戦略の実現
管理方針の明確化
改善の指示

各種リスクの適切な管理
業務プロセス改善

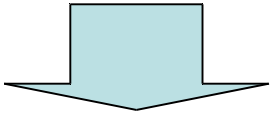
経営トップの関与　＝＞　重要性が増大

↓

リスクに見合ったコントロールが
継続的に機能していることの検証が必須

【監査れポータル】とは

内部統制の実施状況が一目で分かる
監査レポートのポータルサイト



- システム上のログを分析し、ＩＴ全般統制の運用状況の評価を支援するモニタリング・ツール
- ＩＴ全般統制の主要な統制項目（=標準的な監査項目）に対する評価ポリシーを雛形として提供
- 日本版SOX法に準拠したモニタリング・プロセスを実装
- 企業のＩＴインフラ環境に依存せずに評価レポートを提供
- 評価レポートは日常的に職務や権限に応じて提供

内部統制における【監査れポータル】の位置付け

初年度の作業（変更がない限り）２年目以降も継続的に行う作業

基本方針の決定

評価範囲の決定

整備状況の評価

運用状況の評価

全社的な内部統制

- 全社規定、組織の整備
- 整備状況の評価

▶

- 内部統制の実施記録
- 運用状況の評価

業務処理統制

- 業務規定、マニュアル類の整備
- ＥＲＰ導入
- 整備状況の評価
  （評価のための文書化）

▶

- 内部統制の実施記録
- 運用状況の評価
  （サンプリングテスト）

ＩＴ全般統制

- ＩＴ規程、マニュアル類の整備
- システム管理、セキュリティ製品の導入
- 整備状況の評価
  （評価のための文書化）

▶

- 内部統制の実施記録
- 運用状況の評価

監査れポータル

経営者による評価結果の報告

外部監査人による監査

ルールが正しいかを評価

ルール通り運用されているかを評価

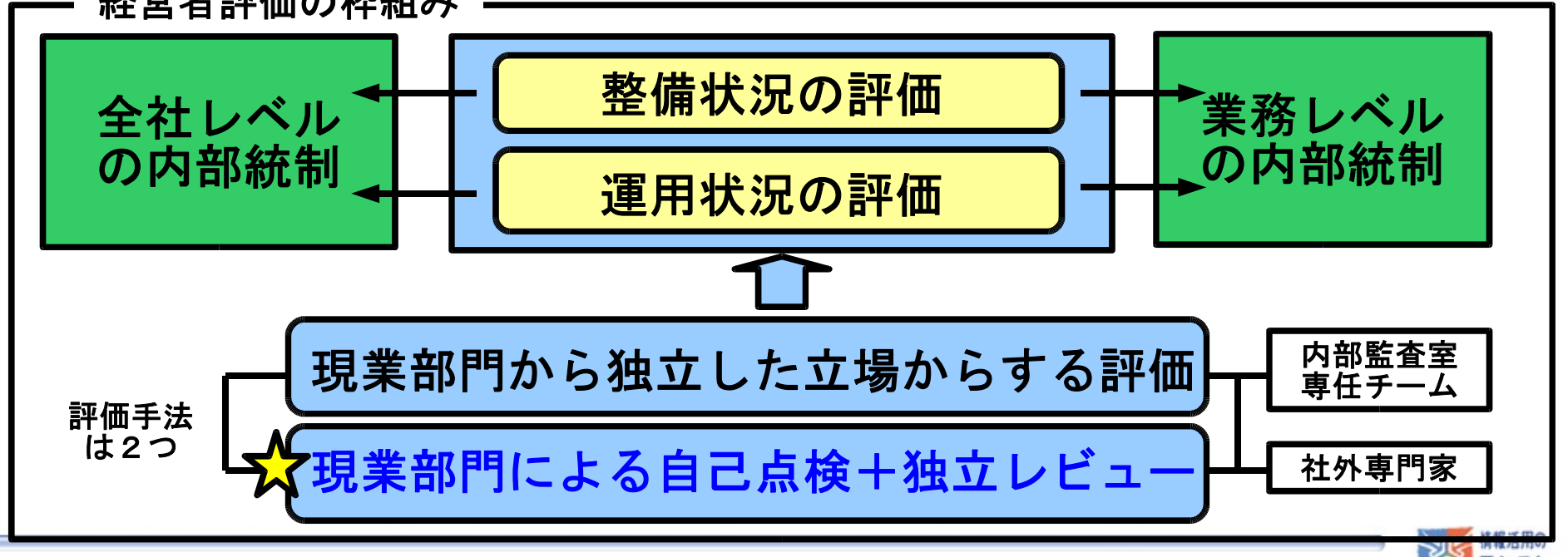
企業自らが毎年実施しなければならない
ＩＴ全般統制の運用状況の評価作業を支援するツール

Copyright © 2008 K.K. Ashisuto

情報活用のアシスト

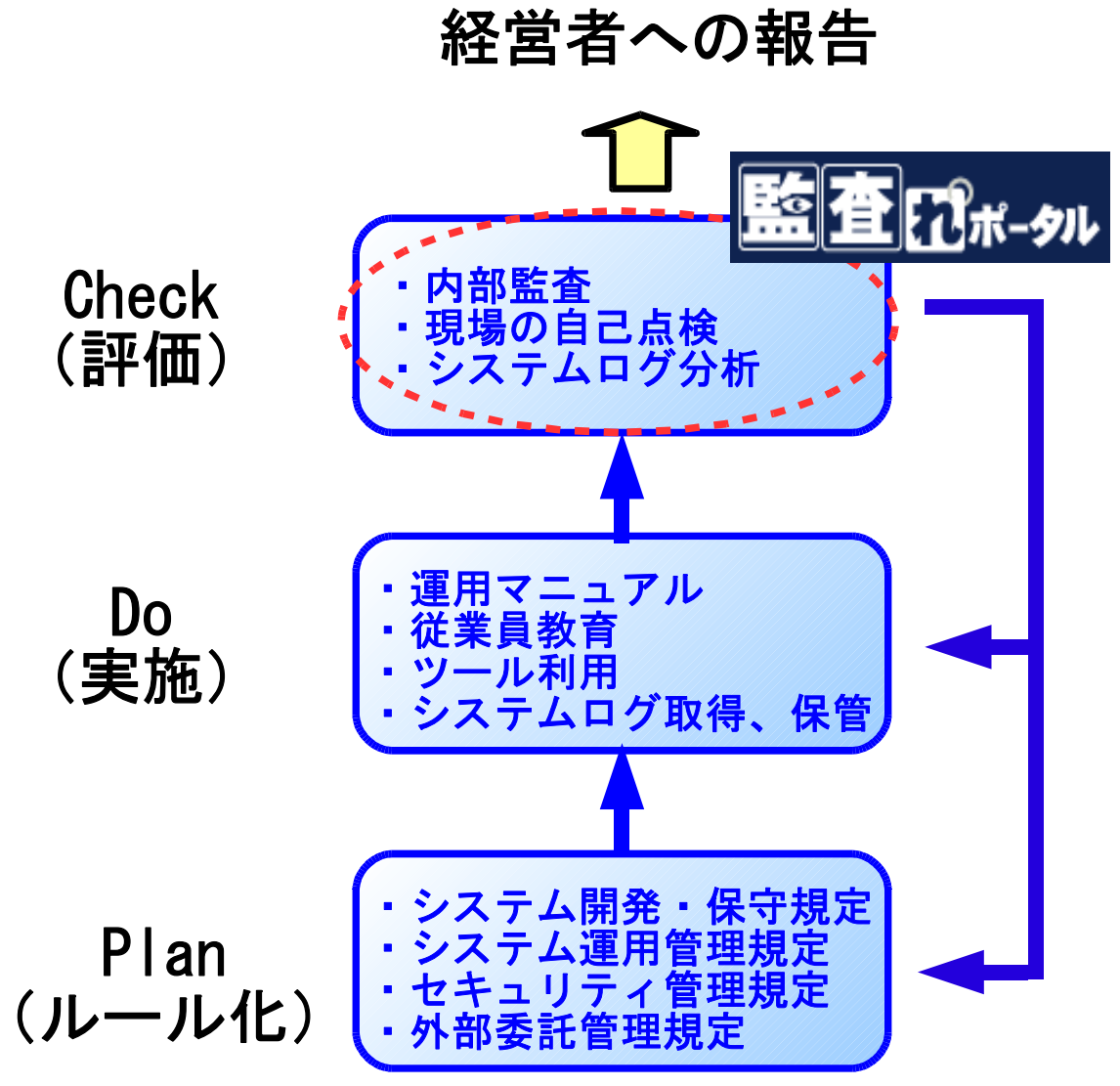
日本版SOX法の経営者評価の枠組み

- 整備状況の評価
  - 適切な統制（ルール）が導入されているか評価する
  - 評価のためには統制を明文化する必要がある → 文書化
- 運用状況の評価
  - 統制（ルール）が実際に運用されているか評価する
  - 評価のためには統制の実施履歴を取得し検査する必要がある → テスト
    - マニュアル統制の場合 ⇒ 伝票の押印や日付をチェック
    - ＩＴ統制の場合 ⇒ ★システムログをチェック



Copyright © 2008 K.K. Ashisuto

IT全般統制における【監査れポータル】の位置付け

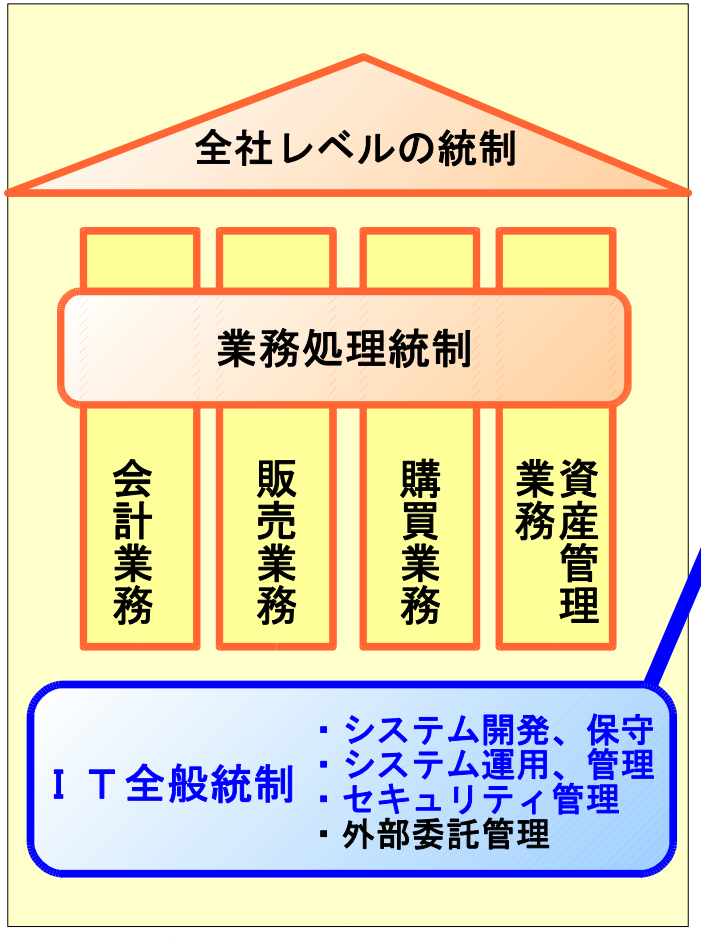


J-SOXでは特に
・職務分掌
・アクセス管理
・システム変更管理
が重要視される

Copyright © 2008 K.K. Ashisuto

【監査れポータル】が提供する評価カテゴリ

IT全般統制の中でも特に
重点的に統制すべき項目に
注力した監査レポートを提供



1．重要システムの利用状況
2．重要データへのアクセス状況
3．特権ユーザIDの利用状況
4．データの社外持出し状況
5．アカウント管理状況
6．重要システムの変更状況

Version1で
対応

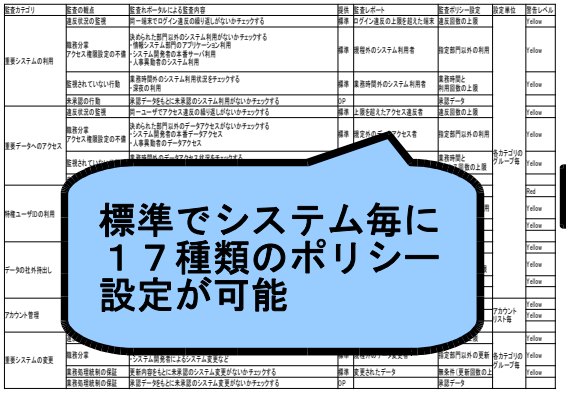
クライアントPCの
セキュリティ設定状況
サーバ、データベースの
セキュリティ設定状況
ジョブ（バックアップ）実行状況
問題の発生と対処状況
ＩＴサービスの提供状況

順次
リリース予定

Copyright © 2008 K.K. Ashisuto

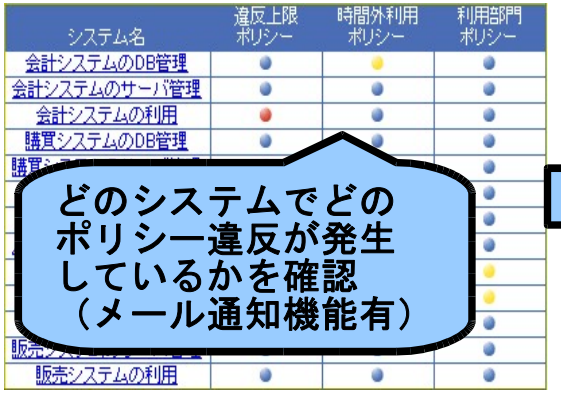
【監査れポータル】が提供する機能

①監査ポリシーの設定



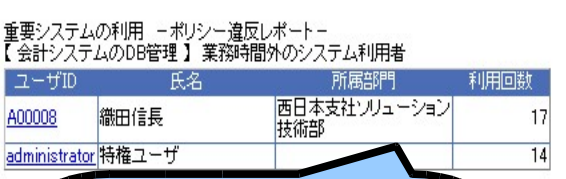
標準でシステム毎に１７種類のポリシー設定が可能

②ポリシー違反状況の確認



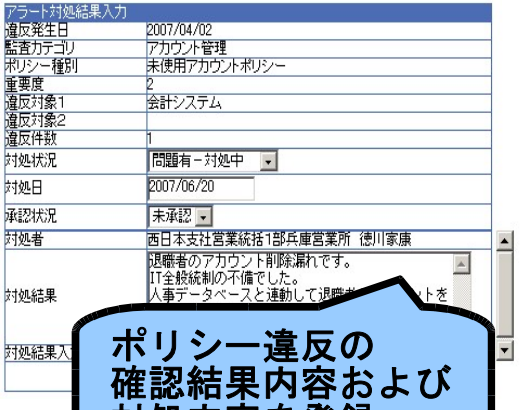
どのシステムでどのポリシー違反が発生しているかを確認（メール通知機能有）

③違反内容の確認



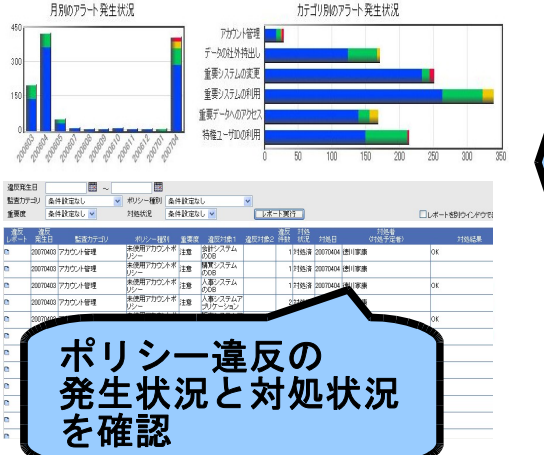
どの部署の誰がポリシ違反を起しているかを確認

④確認結果の入力



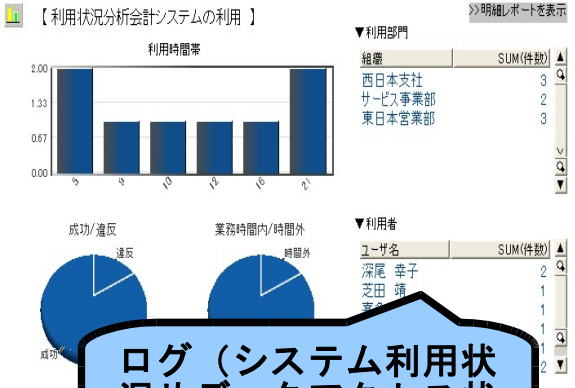
ポリシー違反の確認結果内容および対処内容を登録

⑤統制状況の確認



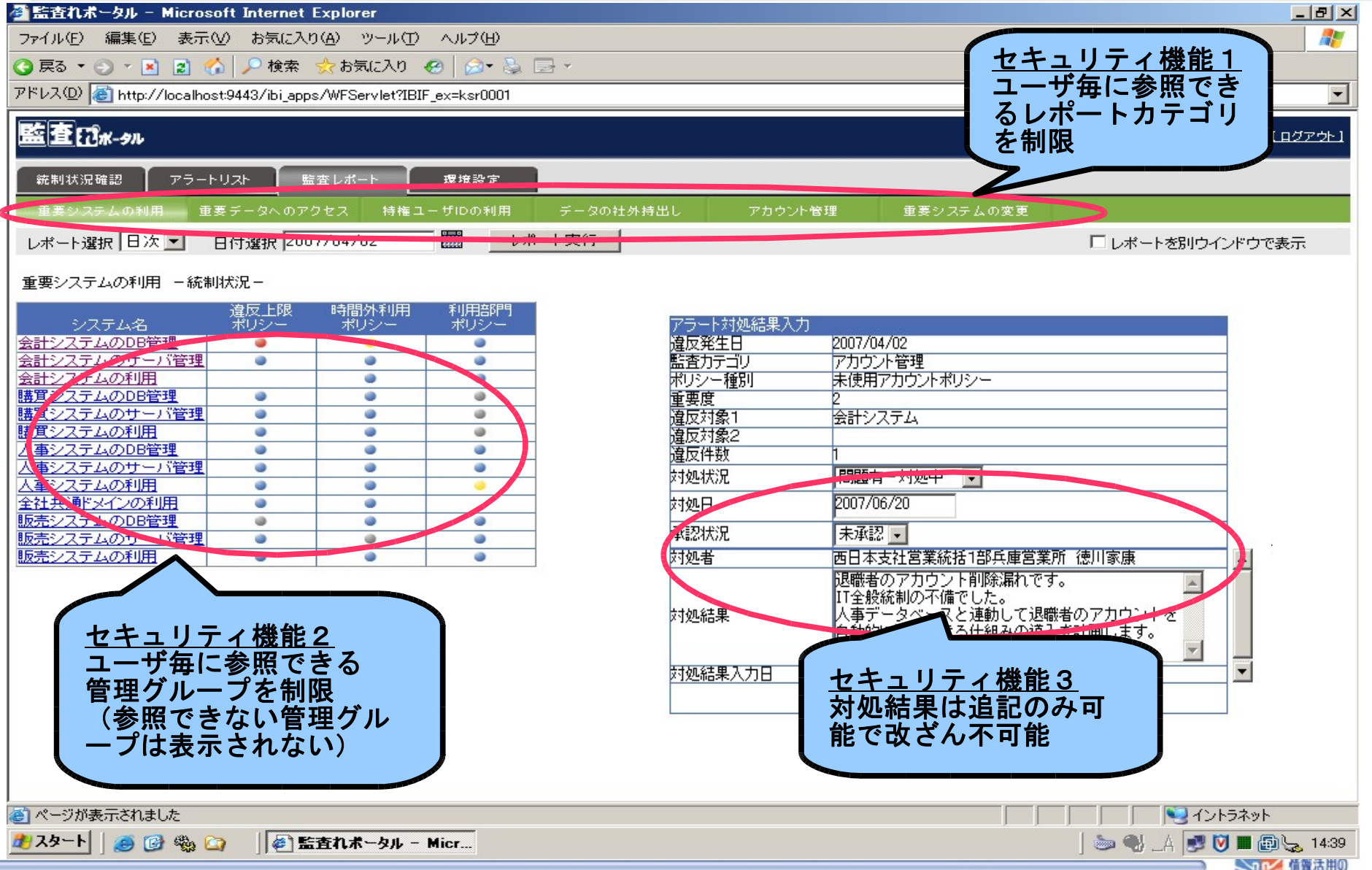
ポリシー違反の発生状況と対処状況を確認

⑥システム利用状況分析



ログ（システム利用状況やデータアクセス状況など）を自由に分析

【監査れポータル】 セキュリティ機能



【監査れポータル】 導入の効果

- ＩＴ全般統制評価のあるべき姿（ベスト・プラクティス）を導入できる
  - 主要な統制項目を網羅した評価ポリシーの提供
  - 日本版SOX法に対応したモニタリング・プロセスを実装
- 内部統制への取り組み状況を監査人や監督省庁に提示できる
  - 評価ポリシー、自己点検状況、問題の対処状況、経営者による確認記録 など
- 経営者評価の質の向上
  - 全ての統制活動記録(ログ)を自動的にチェック可能
＝＞ サンプリング・リスクがない
  - 現業部門・担当者による自己点検が可能
- 内部統制の評価コストの削減
  - 自己評価コストの削減 ← ログ点検作業の自動化
  - 外部監査対応コストの削減 ← 監査人の心証アップによる要求項目の削減
  - 評価システム構築コストの削減 ← 自社開発した場合に比べて
- 専門家でなくてもログ分析が可能
  - 氏名、部署名でログ情報を表示
  - ログフォーマットを意識しなくても良い
  - 簡単な操作でログ分析が可能

Copyright © 2008 K.K. Ashisuto

【監査れポータル】の評価

●システム監査に強い、某監査法人様

この内容で日々統制状況の自己点検を実施している企業であれば、IT全般統制関連の監査は１日以内で終了させることが可能。企業に採用してもらえると監査人としても助かる。

●404条監査に対応された某日本企業様

404条監査で指摘された事項の日常点検がほぼ網羅されている。
404条監査対応前に導入していたかった。

●システム監査対応されている某地方銀行様

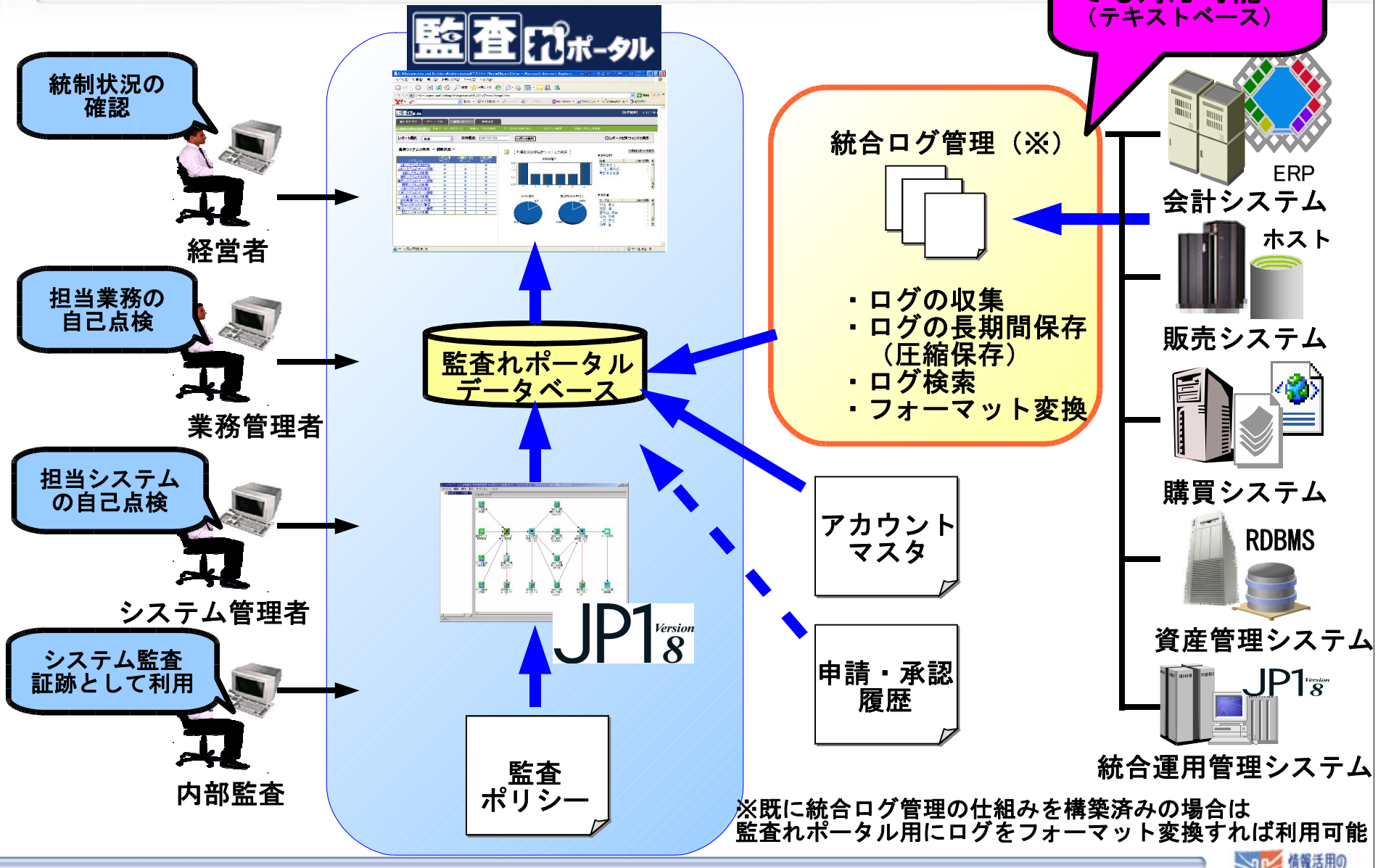
金融庁の検査事項の網羅性という意味で不足がない。地銀で展開を計れるよう、当行からも情報提供していきます。

●監査れポータル監修　J-SOX対応促進協議会顧問　公認不正検査士　戸村 智憲様

監査れポータルでは、IT統制のキーとなるあらゆるログを一括管理し、ITに詳しくない経営者でも簡便かつ迅速に監査法人が指摘してくる問題に着実に対処できる優位性があります。このようなツールがあれば、J-SOXコンサルタントとしても、自信を持ってIT統制の整備・運用・改善に着手でき、経営者の「内部統制のBI・見える化」や「内部統制の意思決定」をサポートする上で、非常に有益です。不正・不祥事の予防・フォレンジックにも強力に力を発揮するツールとしても魅力的です。

Copyright © 2008 K.K. Ashisuto

【監査れポータル】のシステム概要



Copyright © 2008 K.K. Ashisuto

【監査れポータル】 エディションによる機能の違い

		監れポBE	監れポSE	監れポEE	
利用ユーザ数		25	25	無制限	
評価カテゴリ	重要システムの利用	○	○	○	
	重要データへのアクセス	－	○	○	
	特権ユーザIDの利用	○	○	○	
	データの社外持出し	－	○	○	
	アカウント管理	○	○	○	
	重要システムの変更	○	○	○	
	追加予定カテゴリ	－	○	○	
アクセス状況分析レポート（VD）		－	○	○	
カスタムレポート開発機能		－	OP	○	←開発予定機能
部署別ビュー機能		－	－	○	←開発予定機能
価格		480万	750万	2400万	

○　：提供可能
－　：提供不可能
OP　：オプション機能として提供可能

【監査れポータル】 稼働環境

- サーバ動作環境
  - ＯＳ　　：Windows 2000 Server SP2 以上
Windows Server 2003
  - 前提ソフト　　：Internet Information Server
  - ＤＢ　　：Oracle Database 10g Release2
  - ＣＰＵ　　：Dual Core Xeon 2GHz 以上（１ＣＰＵ２コアまで）
  - メモリ　　：2GB 以上
  - ディスク　　：10GB 以上
- サポートブラウザ
  - Internet Explorer 6.0

1．重要システムの利用状況 -カテゴリ詳細-

- 標準で提供される監査ポリシーと監査レポート
  - 利用違反に関するポリシー
    - 監査ポリシー設定　：　違反上限回数を設定
    - 監査レポート　：　ログイン違反上限を超えた端末
    - 監査例　：　システムへの不正アタックの兆候がないかチェックする
  - 利用時間に関するポリシー
    - 監査ポリシー設定　：　業務時間を設定
    - 監査レポート　：　業務時間外のシステム利用者
    - 監査例　：　深夜のシステム利用状況をチェックする
  - 利用者に関するポリシー
    - 監査ポリシー設定　：　利用可能（不可能）者の設定
    - 監査レポート　：　規定部門以外のシステム利用者
    - 監査例　：　職務分掌違反やアクセス権限設定の不備がないかチェックする
      - 情報システム部員の本番アプリケーション利用
      - システム開発者の本番サーバ利用
      - 部署異動者のシステム利用
- 標準で提供される分析レポート
  - システム毎に時間軸、成功/失敗、部署、個人の軸でログを分析できる
- 前提となるログ
  - システム（アプリケーション、サーバ、データベース）へのログインログ
    または それに相当するログ

Copyright © 2008 K.K. Ashisuto

２．重要データへのアクセス状況　–カテゴリ詳細–

- 標準で提供される監査ポリシーと監査レポート
  - アクセス違反に関するポリシー
    - 監査ポリシー設定　：　違反上限回数を設定
    - 監査レポート　：　違反上限を超えたデータアクセス違反者
    - 監査例　：　重要データへの不正アタックの兆候がないかチェックする
  - アクセス時間に関するポリシー
    - 監査ポリシー設定　：　業務時間を設定
    - 監査レポート　：　業務時間外のデータアクセス者
    - 監査例　：　深夜のデータアクセス状況をチェックする
  - アクセス者に関するポリシー
    - 監査ポリシー設定　：　利用可能（不可能）者の設定
    - 監査レポート　：　規定部門以外のデータアクセス者
    - 監査例　：　職務分掌違反やアクセス権限設定の不備がないかチェックする
      ・情報システム部員の本番トランザクション実行
      ・システム開発者の本番データアクセス
      ・部署異動者のデータアクセス
- 標準で提供される分析レポート
  - データ毎に時間軸、成功/失敗、参照/更新、部署、個人の軸でログを分析できる
- 前提となるログ
  - データ（ファイル、データベース）へのアクセスログ または
    アプリケーション機能やプログラムの実行ログ

Copyright © 2008 K.K. Ashisuto

３．特権ユーザIDの利用状況　-カテゴリ詳細-

- 標準で提供される監査ポリシーと監査レポート
  - 利用違反に関するポリシー
    - 監査ポリシー設定　：　違反上限回数を設定
    - 監査レポート　：　ログイン違反上限を超えた特権ユーザID
    - 監査例　：　特権ユーザIDの不正利用の兆候がないかチェックする
  - 操作端末に関するポリシー
    - 監査ポリシー設定　：　利用可能（不可能）端末の設定
    - 監査レポート　：　規定端末以外での特権ユーザＩＤ利用
    - 監査例　：　サーバ室以外の特権ユーザIDの利用がないかチェックする
  - 利用確認に関するポリシー
    - 監査ポリシー設定　：　利用があった場合
    - 監査レポート　：　特権ユーザIDの利用状況
    - 監査例　：　特権ユーザIDの利用状況をチェックする
・委託先、ベンダー利用時の操作内容の確認
- 標準で提供される分析レポート
  - システム毎に時間軸、成功/失敗、利用端末、特権ユーザＩＤの軸でログを分析できる
- 前提となるログ
  - 特権ユーザIDのログインログ
  - 特権ユーザIDの操作ログ

Copyright © 2008 K.K. Ashisuto

４．データの社外持出し状況　–カテゴリ詳細–

- 標準で提供される監査ポリシーと監査レポート
  - 持出し違反に関するポリシー
    - 監査ポリシー設定　：　違反上限回数を設定
    - 監査レポート　：　違反上限を超えたデータ持出し違反者
    - 監査例　：　データの不正持出しの兆候がないかチェックする
  - 持出し時間に関するポリシー
    - 監査ポリシー設定　：　業務時間を設定
    - 監査レポート　：　業務時間外のデータ持出し者
    - 監査例　：　深夜のデータ持出し状況をチェックする
  - 持出しファイルに関するポリシー
    - 監査ポリシー設定　：　持出し禁止ファイル名
    - 監査レポート　：　業務時間外のデータ持出し者
    - 監査例　：　指定キーワードに該当するファイルの持ち出しをチェックする
（全ての持出しファイルをチェックすることも可能）
- 標準で提供される分析レポート
  - 部署毎に時間軸、持出し手段、成功/失敗、個人、ファイル名の軸でログを分析できる
- 前提となるログ
  - 外部媒体へのファイルコピーログ
  - メール添付ファイルの送信ログ

Copyright © 2008 K.K. Ashisuto

５．アカウント管理状況 －カテゴリ詳細－

- 標準で提供される監査ポリシーと監査レポート
  - 新規アカウントに関するポリシー
    - 監査ポリシー設定　：　アカウントマスターを設定
    - 監査レポート　：　未確認アカウント一覧
    - 監査例　：　無許可でアカウントが登録・利用されていないかチェックする
  - 未使用アカウントに関するポリシー
    - 監査ポリシー設定　：　未使用期間を設定
    - 監査レポート　：　長期間システム未使用者一覧
    - 監査例　：　長期間利用されていないユーザＩＤがないかチェックする
- 前提となるログ
  - システムへのログインログ（またはそれに相当するログ）

Copyright © 2008 K.K. Ashisuto

６．　重要システムの変更状況　　-カテゴリ詳細-

- 標準で提供される監査ポリシーと監査レポート
  - 変更違反に関するポリシー
    - 監査ポリシー設定　：　違反上限回数を設定
    - 監査レポート　：　違反上限を超えたシステム変更違反者
    - 監査例　：　重要システムの不正更新の兆候がないかチェックする
  - 変更者に関するポリシー
    - 監査ポリシー設定　：　変更可能（不可能）者の設定
    - 監査レポート　：　規定部門以外のシステム変更
    - 監査例　：　職務分掌違反やアクセス権限設定の不備がないかチェックする
・システム開発者の本番プログラムの変更
・担当者以外のマスターデータの変更
  - 変更確認に関するポリシー
    - 監査ポリシー設定　：　変更があった場合
    - 監査レポート　：　変更されたデータ
    - 監査例　：　変更されたデータを確認し、申請通りの変更かチェックする
- 標準で提供される分析レポート
  - システム、データ毎に時間軸、成功/失敗、部署、個人の軸でログを分析できる
- 前提となるログ
  - プログラムやマスターデータの更新ログ（またはそれに相当するログ）
  - システム設定（アクセス権限など）の変更ログ

Copyright © 2008 K.K. Ashisuto

ＩＴ全般統制の重要性

- 日本版SOXは全社的な統制（全般統制）重視

- アプリケーション統制の有効性はＩＴ全般統制が保証している
  - アプリケーションに組み込まれた統制（データ検証やユーザ認証など）はIT全般統制のシステム変更管理やアクセス管理の上で成り立っている
  - ＩＴ全般統制が脆弱であるとアプリケーション統制の監査工数が増大する

  例）　テストサンプリング件数の違い
  変更されていないことが保証できるアプリケーション＝１件
  vs
  変更されていないことが保証できないアプリケーション＝２５件以上

- 内部統制に関係なく情報システム部門が取り組むべき課題
  - ＩＴ全般統制は情報システム部門の業務そのもの
  - 軽視していいのか？

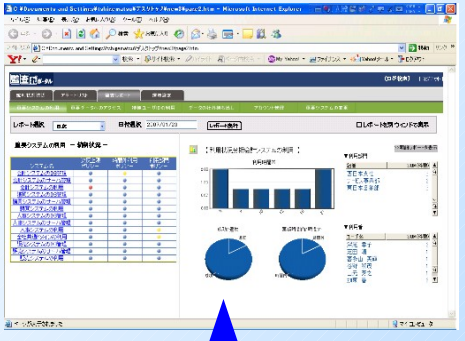
【監査れポータル】で必要となるログとアシスト対応ツール

評価カテゴリ	必要となるログ	評価対象システム			
		Webアプリケーション	サーバOS	データベース	クライアント
		RSA Access Manager	CA Access Control	PISO	秘文AE IF
重要システムの利用	ログインログ	○	○	○	―
重要データへのアクセス	リソースアクセス（操作）ログ	△（URL）	○（ファイル）	○（テーブル）	―
特権ユーザIDの利用	ログインログ	―	○	○	―
	リソースアクセス（操作）ログ	―	○（ファイル）	○（テーブル）	―
データの社外持出し	ファイルの持出しログ	―	―	―	○（外部媒体、印刷、メール）
アカウント管理	ログインログ	○	○	○	―
重要システムの変更	リソースアクセス（システム変更）ログ	△（URL）	○（ファイル）	○（テーブル）	―

―:該当せず

【監査れポータル】の周辺ソリューション

監査れポータル



監査れポータル
データベース

監査
ポリシー

統合ログ管理

- ログの収集
- ログの長期間保存
  （圧縮保存）
- ログ検索
- フォーマット変換

統合アカウント管理

アカウント
マスタ

- 申請・承認
  ワークフロー
- 人事ＤＢとの連動
- 各システムとの連携
- 管理履歴の取得

システム変更管理

申請・承認
履歴

- 申請・承認
  ワークフロー
- 管理履歴の取得

システム運用管理

- インシデント管理
- バックアック管理
- ＩＴ資産管理
- サービスレベル管理

セキュリティ対策（ログ取得）

ERP
会計システム

ホスト
販売システム

購買システム

RDBMS
資産管理システム

Copyright © 2008 K.K. Ashisuto

アシストのＩＴ全般統制構築ツール

- ログ取得＆アクセス制御
  - サーバ　：CA Access Control
  - データベース　：PISO、Oracle Database Vault
  - クライアント　：秘文AEシリーズ、JP1/NETMシリーズ
  - Webアプリケーション　：RSA ClearTrust
- 統合ログ管理
  - 大規模向け　：SenSage Enterprise Security Analytics
  - 中・小規模向け　：LogStorage3
- 統合アカウント管理
  - 大規模向け　：Oracle Identity Manager
  - 中・小規模向け　：LDAP Manager
- システム運用管理（システム変更管理含む）
  - サービスサポート　：JP1、UIS Ticket One
  - サービスデリバリ　：JP1

Copyright © 2008 K.K. Ashisuto

アシスト内部統制対応製品一覧

製品カテゴリ		製品名	製品概要
内部統制支援	整備・運用評価支援	Tosei Vision	内部統制の評価・承認のプロセスを可視化し、内部統制担当者、評価者、承認者の各レベルで、なすべき評価や承認の状況を一覧で確認するメニューを提供する。
	教育支援	Internet Navigware	Web上で従業員教育を実施できる、eラーニング・エンジン。ルールの定着、追加・変更の周知徹底のための教育環境を実現する。
		SoftSimulator	各種手順書の作成を簡易化するとともに、業務プロセスの文書化や可視化。情報システムの操作マニュアルを簡単に作成できる。
	内部監査支援	監査れポータル	IT全般統制が有効に機能しているかどうかを自己点検するために、ログを分析し、内部統制監査レポートを出力する。
		SenSage Enterprise Security Analytics	アプリケーション・ログやシステム・ログなどあらゆるログを一元管理する。
業務処理統制	自動連携	DataSpider Servista	データ、アプリケーションを自動的に連携し、マニュアル・ミスをなくし、データの整合性を保障する。
		iWay SOA Middleware	
IT全般統制	ID／アクセス管理	Oracle Identity Manager	アプリケーションやOS、DBなどが持つアカウント情報（ユーザID、パスワード）やその属性情報（部署、役職、権限など）を統合的に管理し、一括して登録、変更（削除）、監査などを行う。人事データベースと連携し変更情報を各システムへ自動的に反映したり、アカウント・メンテナンスのための申請・承認ワークフローを構築できる。
		RSA Access Manager	Webアプリケーションのユーザ認証およびアクセス制御を一元管理できるシングル・サインオン製品。
		CA Access Control	プラットフォームに依存することなくサーバOSのユーザ認証、アクセス制御、アクセス履歴を強化、管理できるサーバ・セキュリティ対策製品。
		Oracle Database Vault	データベース（Oracle）の特権ユーザ管理製品。
		NX NetMonitor	ネットワークに接続される機器類の正当性を保障する検疫ネットワーク製品。
		Citrix Presentation Server	クライアント・アプリケーションをサーバへ集中化することにより統制対象アプリケーションの母数軽減とアクセス制御、セキュリティの強化を行う。
	操作制限・監視	JP1資産・配布管理、 秘文 Advanced Edition	クライアントPCの操作履歴を取得したり、ポリシーに違反する不正操作を禁止する。（操作対象：データ外部持ち出し、印刷、ファイル操作、アプリケーション起動など）
		CA Access Control	サーバOSの操作履歴を取得したり、ポリシーに違反する不正操作を禁止する。（操作対象：ログイン、ファイル操作、コマンド実行、プログラム起動など）
		PISO	データベース（Oracle）の操作履歴を低負荷で取得し、ポリシー違反があった場合には管理者へ通知する。
	IT資産管理	JP1資産・配布管理	クライアントPCやサーバのソフトウェア／ハードウェア情報を一元管理し、資産の可視化、保全を支援する。
	開発・変更管理	JP1資産・配布管理	システム・メンテナンスの際の申請・承認のワークフローを提供する。また、承認後のソフトウェアの自動メンテナンス（配信）および配信結果の確認により、IT基盤が有効にリリースされたことを確認する。
	システムテスト支援	HP Quality Center, HP QuickTest Professional	システム開発、メンテナンス時に定型的に行うべきアプリケーション・テストを自動化できる。また、システム・テストの工程管理を行う。
	運用管理	JP1統合管理、JP1アベイラビリティ管理、JP1ジョブ管理、JP1ネットワーク管理	システム運用の日常業務の自動化および効率化を支援することで、脱属人化、運用品質の均一化を図り、IT基盤の安定稼働を支援する。　（運用オペレーションの自動化、インシデント管理、システム障害監視、システム・リソース管理など）
		HP Business Availability Center	ユーザ視点でのサービスレベル（レスポンスおよび可用性）を監視することにより、システムの信頼性を支援する。
		Performance Insight	Oracleデータベースのパフォーマンスを診断、監視することにより、システムの信頼性を支援する。
	データ保護	JP1ストレージ管理	マルチプラットフォーム環境のバックアップ運用を一元管理する。
	ITIL全般	HP Service Desk software	インシデント管理、問題管理、構成管理、変更管理などITサービス・マネジメント（ITIL）の各プロセスを支援する。

Copyright © 2008 K.K. Ashisuto

アシスト会社概要

設立	1972年3月
代表取締役	ビル・トッテン
売上高	182億円　（2006年度）
社員数	710名　（2007年4月現在）
事業内容	コンピュータ用パッケージソフトウェアの販売、技術サポート、教育およびコンサルティング
本社所在地	東京都千代田区九段北4-2-1 市ヶ谷東急ビル
オフィス所在地	札幌、仙台、長野、名古屋、金沢、大阪、神戸、広島、福岡、沖縄
取引会社数	4,900社（2006年度）
主要取扱製品数	50製品（2007年4月現在）

テクニカル・サポートおよび教育サービスを中心に提供する東京本社サービス事業部は、ISO27001の認証を取得しています。