

# 情報のリスク管理・内部統制を支援する コンプライアンス推進ソリューション

藤村 隆\* (Takashi Fujimura) 郡 光則\*\* (Mitsunori Kori)  
 須藤 純吾\* (Jungo Sudo) 石井 篤\*\* (Atsushi Ishii)  
 中館 穂積\* (Hozumi Nakadate)

Solution to Promote Compliance with Information Risk Management and Internal Control

## 要 旨

三菱電機の IT システムビジョンでは、“安心”の中にセキュリティ、高信頼性、コンプライアンスなどを位置付けている。三菱電機インフォメーションテクノロジー(株) (MDIT) は、セキュリティとコンプライアンスを柱とし、更にこれらを統合するため三菱電機の独自技術である“統合ログ DB (DataBase)”を活用し、“コンプライアンス推進ソリューション”を提供している。このソリューションは、次の三つのシステムから構成される。

### (1) 内部統制管理

個人情報を含むデータや機密情報を含む電子文書を扱う業務フローの実行を、内部統制管理基準に従った職務権限で管理する。

### (2) 情報漏洩防止

機密情報の外部メディアへの書き出しや複製の防止・抑止を行い、内部犯行による情報漏洩を防止・抑止する。

### (3) 統合ログ管理

採取した監査証拠となるログを蓄積・管理し、監査結果をレポートとして出力する。

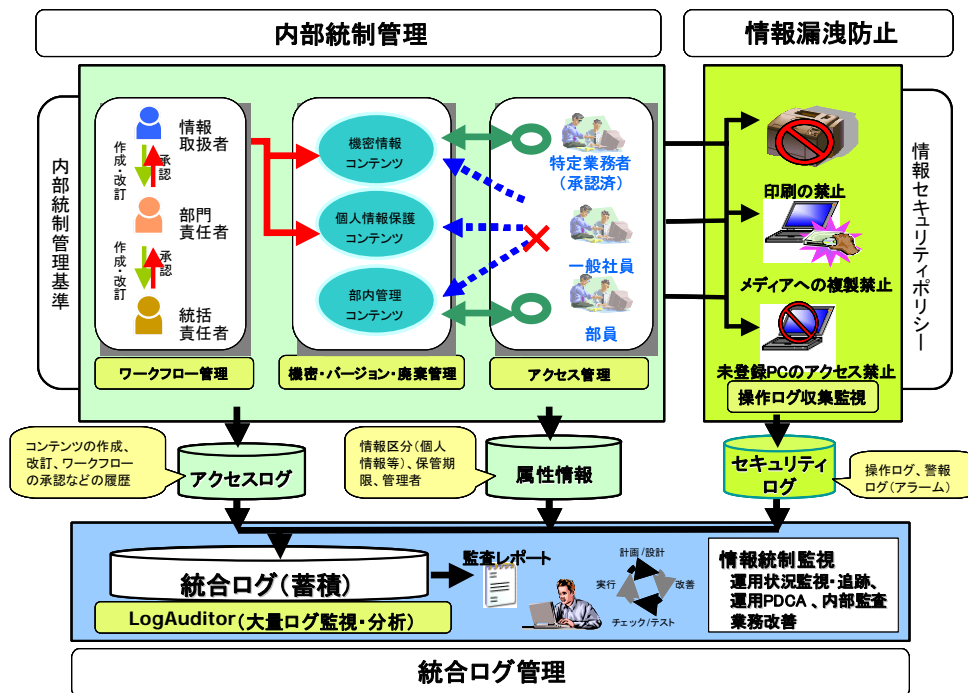
さらにこのソリューションでは、上記三つのシステムの導入を支援・コンサルティングするサービスメニューも提供している。

統合ログ管理では、多種多様な形式のログを一元管理でき、データ圧縮技術による大容量ログの蓄積及び蓄積したログからの高速検索、高速集計/レポート化機能を実現している。この統合ログ管理は、“LogAuditor Enterprise” (注1)としてすでに製品化しており、その一部機能を利用した製品“セキュリティリコメンデーションシステム LogAuditor for CWAT” (注2)は、金融・通信・流通などの各業種で実績がある。

MDIT は、日本版 SOX (Sarbanes-Oxley) 法、個人情報保護法などでますます重要となるコンプライアンスに対応したソリューションを、データ統合の技術及びノウハウを活かして、今後も提供していく所存である。

(注1) LogAuditor は、三菱電機インフォメーションテクノロジー(株)の登録商標である。

(注2) CWAT は、株式会社インテリジェントウェイブの登録商標である。



PC: Personal Computer PDCA: Plan Do Check Action

## コンプライアンス推進ソリューションのシステム構成

内部統制管理にて、職務権限による内部文書へのアクセス制限・管理を行い、その履歴ログを採取。情報漏洩防止にて、機密情報の外部メディアへの書き出しや複製の防止・抑止を行い、操作ログを採取。各システム個別に採取したログを、監査証拠として一元的に統合することで初めて可能となる内部統制・情報セキュリティ管理を目的とした監査レポートを提供するソリューションである。

\* 三菱電機インフォメーションテクノロジー(株)

\*\*三菱電機(株) 情報技術総合研究所

## 1. まえがき

これまで企業などの情報管理では、漏洩防止対策が主に行われてきたが、近年ではそれに加えて、内部統制管理を徹底したいという要望が強まっている。MDITでは従来の情報漏洩防止対策だけでなく、内部での情報アクセスを制限・管理し、蓄積された各種アクセスログを統合・解析して、内部監査や業務改善の立案を推進する“コンプライアンス推進ソリューション”を提供している。

本稿では、コンプライアンス推進ソリューションを構成する“内部統制管理”、“情報漏洩防止”、“統合ログ管理”について述べる。

## 2. コンプライアンス推進ソリューション

情報システムにおける日本版SOX法、個人情報保護法などへの対応として、MDITが提供するコンプライアンス推進ソリューションは、表1に示す製品構成となっている。

表1. コンプライアンス推進ソリューション製品構成

製品区分	主な機能	サーバ構成
内部統制管理	<ul style="list-style-type: none"> <li>アクセス管理</li> <li>バージョン管理</li> <li>属性情報管理</li> <li>承認ワークフロー管理</li> <li>ライフサイクル/ログ管理</li> </ul>	コンテンツ管理サーバ
情報漏洩防止	<ul style="list-style-type: none"> <li>PC操作監視・抑止</li> <li>不正PCのネットワーク接続監視</li> <li>不審挙動検出</li> <li>操作ログ収集</li> </ul>	監視マネージャーサーバ
統合ログ管理	<ul style="list-style-type: none"> <li>多様ログの統合・蓄積</li> <li>監査レポート出力(定型)</li> <li>高速ログ検索・集計による非定型レポート出力</li> </ul>	ログ分析サーバ

内部統制管理、情報漏洩防止の各システムで個別に運用監視・管理している状態では、企業の全体システムを統制することは困難である。この問題を解決すべく、各システムで採取したログを統合し、そこから内部統制に必要な“監査レポート”を出力するソリューションを提供する。

このソリューションは、内部統制フレームワークCOSO(the Committee of Sponsoring Organization of the Treadway Commission)の五つの構成要素と図1のように対応している。

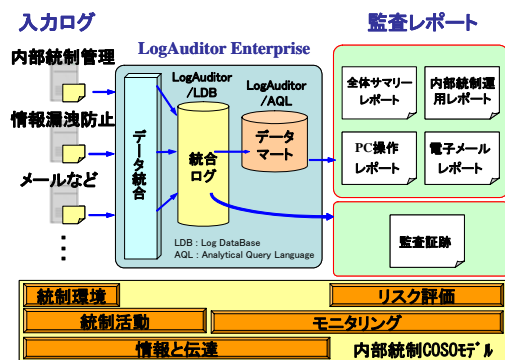


図1. ソリューションで提供する機能構成

## 3. 内部統制管理

### 3. 1 内部統制管理の要件と実現機能

内部統制管理では、情報利用におけるセキュリティの確保、業務フローの透明化と整合性が必要であり、特に文書などの非構造化データの扱いが重要となる。主な機能は図2の通りであり、コンテンツ管理システムにて実現する。

#### (1) 承認ワークフロー

規則に基づいた運用を行うため、作成した文書を責任者が承認するプロセスが必要となる。承認ワークフローでは、文書を投稿すると部門責任者にメールが届き、部門責任者は内容を確認の上、承認・否認操作を行う。必要ならば更に上の統括責任者へ依頼される。承認された文書はコンテンツとしてリリースされ閲覧可能となる。

#### (2) アクセス管理/属性

リリースされたコンテンツはコンテンツアクセス者の権限により、閲覧・修正可否が制御される。例えば、機密文書類は特定の業務者のみが閲覧でき、一般社員は閲覧不可など、用途に応じた管理が可能である。更にコンテンツに属性を設けることで、関連する属性を持つコンテンツを仕分けすることが可能となる。

#### (3) バージョン管理

コンテンツの修正が必要な場合は、それをシステムから取り出し、修正してから再投稿する。承認後、コンテンツは自動改版されリリースされる。

#### (4) ライフサイクル管理/ログ管理

文書の作成から承認、改訂、廃棄までのライフサイクルを把握し履歴を管理することで、生きた情報活用が可能になる。更に、コンテンツの作成、改訂、ワークフローの承認などに関するアクセス履歴と、セキュリティレベルなどのコンテンツ属性をログとして出力することが可能である。

### 3. 2 内部統制管理による効果

前節の結果、全ての情報の素性が明確になり、バージョンも統一されて、信用できるものとなる。権限があれば、誰でも情報にアクセスでき、情報の有効活用が図れる。

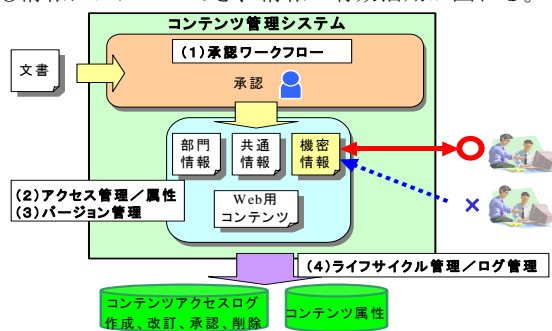


図2. 内部統制管理の主要な機能

## 4. 情報漏洩防止

### 4. 1 情報漏洩防止の概要

情報漏洩防止では PC 操作の制御（操作の禁止／抑止）及び監視（操作証跡のログ記録）が必要であり、これらの機能を備えた CWAT（シーワット：Cyber Warning Alert Termination）で実現している。

CWAT は、予め定義したルール（ポリシー）に沿って PC の制御／監視を行い、ルールに違反した行為を抑止するとともにログを出力する。CWAT 監視モジュール（エージェント）を PC 上に常駐させることにより、ネットワークへ接続された状態ではもちろんのこと、モバイル環境においても同様の制御／監視が行われる。

### 4. 2 CWAT 製品構成

CWAT は、次のコンポーネントで構成される（図 3）。

#### (1) オーガナイゼーションモニタ（OM）

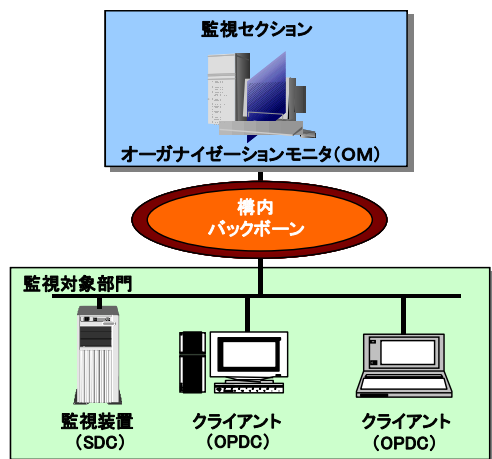
管理コンソールとして、ユーザ・ノードなど監視対象の管理、ポリシー設定による監視内容の定義、各種ログ管理などを行う。

#### (2) オペレーションディフェンスコントローラ（OPDC）

既存の PC 端末へ導入するエージェントであり、外部接続デバイスなどの接続監視・制御及びファイル書き出し、アプリケーションのインストール、ユーザファイル操作、印刷、電源オン／オフ、ログのオン／オフなどの操作の監視・制御を行う。違反操作の検知時は、動作を抑止すると共に OM へ違反行為を示す“警告ログ”として発報を行う。同時に、PC 端末内にも操作証跡としての“監査ログ”を保存する。

#### (3) その他

他にネットワークを監視するセグメントディフェンスコントローラ（SDC）により、不正端末の検知、不正アクセスの検知と共に“警告ログ”を発報する他、OPDC のオプションとして暗号化など豊富なオプションが用意されており、いずれもログの取得を行うことが可能となっている。



SDC: セグメントディフェンスコントローラ OPDC: オペレーションディフェンスコントローラ

図 3. CWAT システム構成例

## 5. 統合ログ管理

### 5. 1 統合ログ管理の概要

統合ログ管理は、図 4 に示すように各システムで個別に採取しているログを、一つのデータベースに統合し、管理・活用するためのプラットフォーム製品“LogAuditor Enterprise”を提供している。なお、本稿で挙げているコンプライアンス推進ソリューションは、対象ログを内部統制管理と情報漏洩防止としているが、統合ログ管理の機能としては、扱うログを限定するものではない。

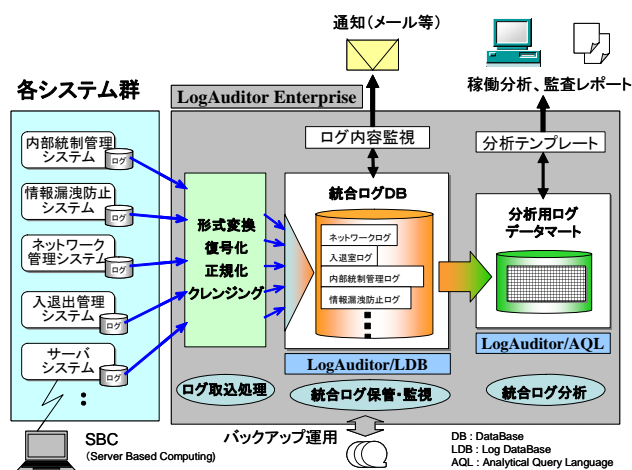


図 4. 統合ログ管理 (LogAuditor Enterprise)

### 5. 2 統合ログ DB

#### (1) 統合ログ DB

統合ログ管理にて統合ログ DB は次の機能を提供する。

- 様々な種類のログの一元的な管理
- 大量のログを対象とする迅速な監査、異常検知
- 長期間に渡るログの蓄積保存、管理

#### (2) LogAuditor/LDB

統合ログ DB はログ格納用データベース管理システムである LogAuditor/LDB によって管理される。

従来、ログの管理には汎用の RDBMS (Relational Database Management System) が利用されることが多かった。しかし、RDBMS で異なる形式のログを扱うには事前にデータ形式を統一する必要があり、予め想定していない形式のログに対応することは困難であった。また、大量のログを蓄積保存するとストレージコストの増大や処理速度の低下を招くという課題があった<sup>(1)</sup>。

LogAuditor/LDB は上記の課題を解決する新しい概念のデータベース管理システムであり、以下の特長を持つ。

- ログをその形式によらず完全に復元可能な形で蓄積保存する。事前にログ形式を特定する必要はない。
- テラバイト超の大規模ログにも対応可能な高速蓄積と正規表現指定による高速検索を実現する。
- データ圧縮により必要なストレージ容量を概ね 1/10 程度に削減する。また、ログを日単位などの“範囲”に

分割し、それぞれの範囲をバックアップ、削除するなど時系列的な管理を可能にする。

### (3) LogAuditor/AQL

ログの傾向分析には、LogAuditor/AQL の管理するログデータマートと呼ぶ分析用データベースを使用する。

LogAuditor/AQL はデータ集計・分析に適したデータベース管理システムであり、統合ログ DB から抽出したログをログデータマートに格納し、高速な集計・分析を行う。

### (4) 大規模データ高速処理アーキテクチャ SISA

LogAuditor/LDB と LogAuditor/AQL はいずれも当社独自の大規模データ高速処理アーキテクチャ SISA (Scalable Intelligent Storage Architecture) に基づいており、以下の技術によりログの高速処理を実現した<sup>(2)(3)(4)</sup>。

- ・データ量に応じた処理能力の拡大を実現する“並列処理技術”
- ・メモリ上へのデータのキャッシュに依存せず、データ量が増加しても安定した処理性能を実現する“ストレージアクセス技術”
- ・大規模で複雑な検索条件に対しても1億文字/秒の高速照合を実現する“文字列照合技術”
- ・高速処理/高圧縮率を両立する“データ圧縮技術”

## 5. 3 監査レポート

監査レポート機能は、業務フローログ、PC 操作ログ、サーバアクセスログなど様々なログデータを統合した分析テンプレートを提供する。

### (1) リスク評価用テンプレート

リスク評価では、洗い出されたリスクについて、その影響度、発生可能性の大小、発生頻度などについて評価する必要がある。リスク評価用テンプレートでは、リスクに関連する業務フローや操作の実行回数、ユーザ数などを分析することができる。

### (2) モニタリング用テンプレート

内部統制では、統制活動が有効に機能しているかを継続的に監視、評価する必要がある。モニタリング用テンプレートでは、あらかじめ設定した業務フローやイベントの発生状況を時系列に集計、分析する。また、前月からの変化量など全体の傾向も把握できる。

監査レポートの信頼性を確保するためには、処理プロセスのログと処理結果のログを合わせて照合することが重要となる。例えば、機密情報の社外持ち出し処理が適正に運用されているかを評価する場合を考える。この場合、図5に示すように機密情報持ち出し申請の業務フローログとファイルの暗号化操作ログ、ファイルの外部メディアへのコピーの操作ログとを合わせて照合することで処理が正しく実行されているかどうかを評価することができる。このように複数のシステムのログを合わせて照合する場合、一般には、それぞれのログを蓄積したデータベースに

問い合わせ処理を行う必要がある。しかし、これには処理時間がかかったり、問い合わせ結果をマージするためのアプリケーション負荷が高くなるなどの課題がある。監査レポート機能では、異なるログを統合し、データ項目を共通化することによりこの課題を解決している。

月別操作件数レポート

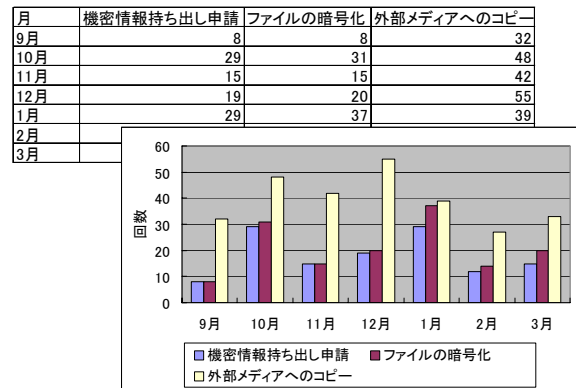


図5. 監査レポート例

## 6. むすび

企業における既存の情報システムは、通常その稼働状況やアクセス履歴などをログとして固有の形式で記録している。これらログは、内部統制で活用できる証拠として重要な内容を持ちながら、システムごとに閲覧・検索方法が異なるため、統一された管理ができなかった。

今回、この問題を内部統制管理と情報漏洩防止の二つのシステムのログを統合することで解決した。この仕組みはMDIT 社内システムで既に稼働している。今後は、電子メール、Web アクセス、DB アクセスなどのログも統合し、さらに監査対象範囲を拡張していく所存である。

## 参考文献

- (1) Sah, A. : “A New Architecture for Managing Enterprise Log Data.” Proc. of LISA 2002, 121~132 (2002)
- (2) 郡光則, 山岸義徳, 清水英弘, 金子洋介 : 検索機能を備えたストレージシステムによる大規模並列全文検索, 電子情報通信学会技術報告, CPSY-2002-47 (2002)
- (3) 上田尚純, 郡光則, 他 : ブロック化転置ファイルを利用したデータウェアハウス向けデータベース管理システムの評価, 情報処理学会論文誌, 42, No. SIG10 (2001)
- (4) 中村隆顕, 郡光則 : 大規模正規表現の高速照合方式, 情報処理学会全国大会第 67 回, 4F-5 (2005)
- (5) COSO : “Internal Control-Integrated framework” (1996)