

多種多様なログの統合管理を実現する LogAuditor Enterprise

LogAuditor Enterprise: Integrated Management System for Various Log Data

郡 光則*
(Mitsunori Kori)
森田 登**
(Noboru Morita)
藤村 隆**
(Takashi Fujimura)

要 旨

近年、企業内の内部統制やセキュリティ管理に対する関心の高まりを背景に、様々な情報システムが生成する大量のログを証拠保全のために蓄積保存するようになってきた。従来、これらのログは個々の情報システムごとに管理されることが多かったが、ログの種類増加に伴い、これらのログを統合的に管理し、管理コストの低減や原因分析の効率化を図る必要性が高まっている。一方、汎用の RDB (Relational DataBase) を利用する従来のログ管理では、形式の異なるログの一元的な取り扱い、蓄積・検索速度、ストレージコストなどの点に課題があった。

三菱電機インフォメーションテクノロジー(株) (MDIT) の内部統制推進ソリューション “LogAuditor Enterprise (注1)” は大量に発生する任意形式ログの収集・蓄積・分析を可能とするための、統合的なログ管理機能を提供するスイート製品である。

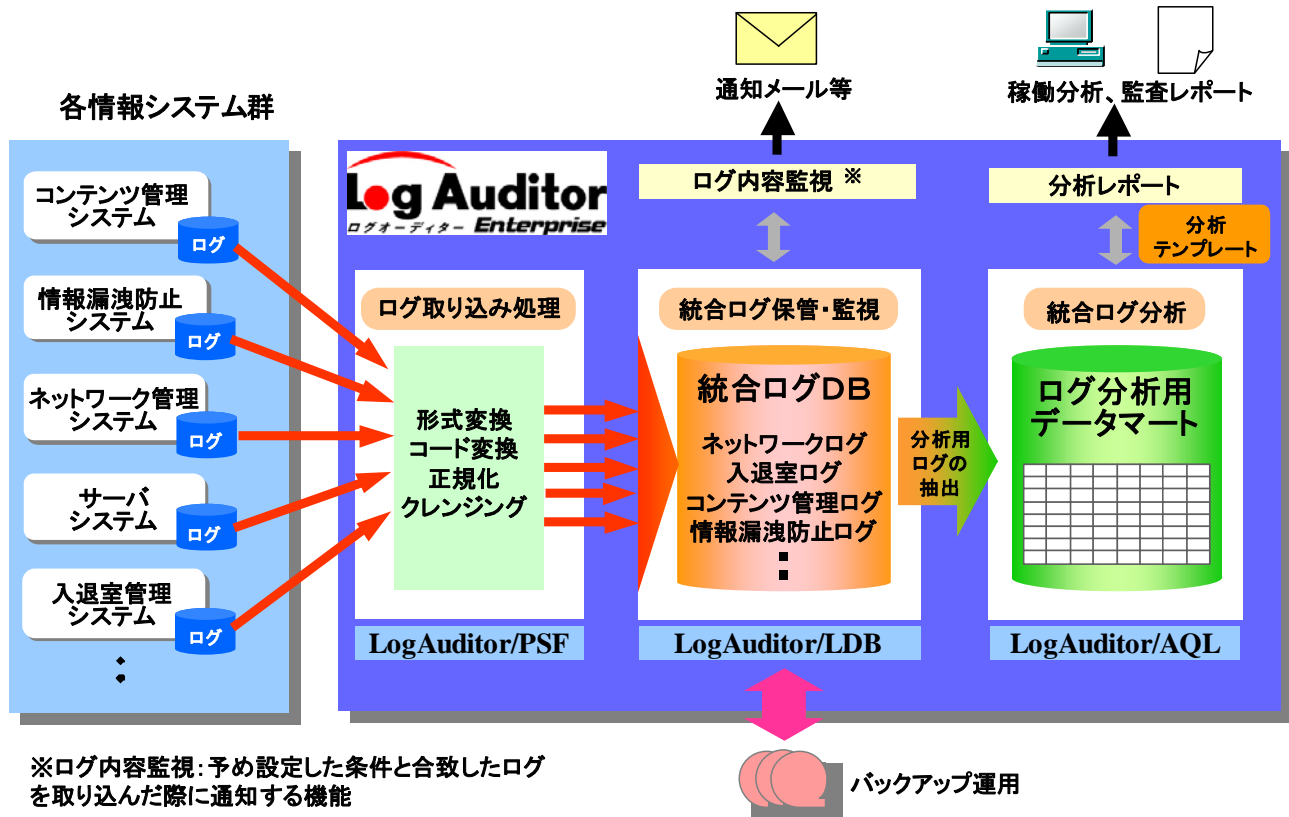
LogAuditor Enterprise は、以下の三菱電機独自の高速処理技術を活用して大規模なログの高速処理を実現した。

- (1) データ量を 1/10 以下に削減し、ストレージコスト低減と高速化を実現するデータ圧縮技術
- (2) データ規模に応じた処理速度とスケーラビリティの高いシステム構成を実現する並列処理技術
- (3) データ蓄積後のログ形式判別や、索引を使用しない検索を高速に行う高速文字列照合技術

また、LogAuditor Enterprise を活用したソリューションとして提供する “分析テンプレート” により、各種のログを統合した監査レポートを出力することができる。

今後は、ログの大規模化と多様化が進むと予想されるため、更なるスケーラビリティの拡大及び分析テンプレートの充実化を図っていく予定である。

(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。



※ログ内容監視: 予め設定した条件と合致したログを取り込んだ際に通知する機能

LogAuditor Enterprise のシステム構成

LogAuditor Enterprise はログの取り込みを行う LogAuditor/PSF、統合的にログを保管・監視する LogAuditor/LDB、統合的なログの分析エンジンである LogAuditor/AQL から構成される。また、分析フロントエンドとなる Microsoft Excel アドインを利用できる分析テンプレートが提供される。

*三菱電機 (株) 情報技術総合研究所

**三菱電機インフォメーションテクノロジー (株)

1. まえがき

近年の企業内の内部統制やセキュリティ管理に対する関心の高まりを背景に、コンテンツ管理システム、情報漏洩防止システム、ネットワーク管理システムなど様々な情報システムから生成される利用履歴（ログ）が証拠保全のために蓄積・保存されるようになってきた⁽¹⁾。蓄積されるログの量は年間数十テラバイトに及ぶ事例も見られる。従来、これらのログは個々の情報システムごとに管理されることが多かったが、ログの種類やデータ量の増加に伴い、これらのログの統合的な管理により、管理コストの低減や原因分析の効率化を図る必要性が高まっている。

MDITでは企業内の情報システムで採取されるログを証拠として収集・蓄積し、分析する内部統制推進ソリューション LogAuditor Enterprise を提供し、多種多様なログの統合管理を実現した。

本稿では、従来のログ管理の課題と、LogAuditor Enterprise による解決策及びそれを支える高速処理技術について述べ、併せて LogAuditor Enterprise を活用したテンプレートについても紹介する。

2. ログ管理の課題

従来のログ管理では、汎用の RDB を利用することが多かった。しかし、OLTP (On-Line Transaction Processing) などを主対象として発達してきた RDB は、様々な形式を持ち、長大なデータを含むことの多いログの効率的処理には必ずしも適していない⁽²⁾。このため、ログの種類や量の増大に伴い、以下の問題が見られるようになってきた。

- (1) 異なる形式のログを一元的に取り扱うために事前にデータ形式を統一する必要がある、予め想定していない形式のログに対応困難
- (2) 蓄積や検索に要する処理時間が長い
- (3) 長期保存に必要なストレージコストが高い

LogAuditor Enterprise はこれらの課題を解決し、多様で大量のログの効率的な統合管理を実現する。

3. LogAuditor Enterprise

3.1 LogAuditor Enterprise のねらい

LogAuditor Enterprise は、大量に発生する任意形式ログの収集・蓄積・分析を可能とするための、統合的なログ管理機能を提供するスイート製品である。従来、企業内で発生するログは各々の専用システムから出力され、単体で蓄積、管理が行われており、それらを統合して管理運用することは、前述のログ管理の課題で記した技術的な課題もあり難しかった。そのため複数のログを横断的に分析し企

業内で発生しているイベント、機器の操作などを総合的に把握及び分析することは困難で、蓄積されたログを必ずしも十分に活用できるとは言い難かった。LogAuditor Enterprise は、この課題を解決するソリューション製品である。

3.2 製品の構成

LogAuditor Enterprise は、主にログの取り込みを行う LogAuditor/PSF (Power Staging Facility)、統合的にログを保管・監視する LogAuditor/LDB (Log DataBase)、統合的なログの分析エンジンである LogAuditor/AQL (Analytical Query Language) から構成され、更に、分析フロントエンドとなる Microsoft ^(注2) Excel ^(注2) アドインツールを提供する。それらの機能、動作環境を表1、表2に示す。

表1. LogAuditor Enterprise を構成するコンポーネント

コンポーネント	機能
LogAuditor/PSF	ログデータの収集と加工、取り込み
LogAuditor/LDB	統合ログデータの蓄積保管・監視 高速な検索
LogAuditor/AQL	分析用ログデータの保存 高速な検索・集計
分析フロントエンド	分析テンプレートなどによる定型レポート 非定型分析レポート

表2. LogAuditor Enterprise の動作環境

サーバ	Microsoft Windows ^(注2) Server 2003 ^(注2)
クライアント	Microsoft Windows XP ^(注2) Professional Microsoft Windows 2000 ^(注2) Professional

(1) LogAuditor/PSF

LogAuditor/PSF は、企業内に存在する様々なログデータを収集し加工するシステムであり、以下の特長を持つ。

- ・ きめ細かいデータの加工、編集機能
- ・ 高い生産性・保守性
- ・ サポートされるデータソースは、各種ログが格納された主要 RDB、または CSV などのフラットファイル

(2) LogAuditor/LDB

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⁽³⁾、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。事前にログ形式の特定は不要
- ・ 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保持
- ・ データ圧縮により必要なストレージ容量を概ね 1/10 以下に削減。また、ログを日単位などの“範囲”に分割し、それぞれの範囲でバックアップ、削除するなど時系列的な管理が可能（特許出願中）

(注2) Microsoft、Excel、Windows、Windows 2000、Windows Server 2003、Windows XP は、米国 Microsoft 社の登録商標である。

(3) LogAuditor/AQL

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、以下の特長を持つ。

- ・ 集計・分析に適した構造化されたデータとしてログを保存
- ・ 高速なデータ検索・集計
- ・ データ圧縮による必要ストレージ容量の削減
- ・ 標準 SQL (Structured Query Language) に準拠した柔軟なアクセスインタフェース

(4) 分析フロントエンド

LogAuditor/AQL の分析用フロントエンドとして表計算ツールである Microsoft Excel から直接アクセスし、分析レポートの作成を可能とする Excel アドインツールを提供し、以下の特長を持つ。

- ・ 定型レポートの雛型となる分析用テンプレートの作成、利用が可能
- ・ 柔軟な非定型分析、ウィザード形式での容易な操作
- ・ 使い慣れた Excel からシームレスに利用可能、集計表（ピボットテーブル）を自動生成
- ・ 集計値から明細の分析データに遡るドリルスルー機能
- ・ 原始ログデータとも連携可能なアプリケーションやマクロの利用

4. LogAuditor Enterprise の高速処理技術

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) に基づき大規模ログの高速処理を実現した。以下に、その主要技術について示す。

4. 1 データ圧縮技術

LogAuditor/LDB、LogAuditor/AQL はログを自動的に圧縮して蓄積することにより、必要なストレージ容量を概ね 1/10 以下に削減する。また、データ圧縮によりストレージ入出力が削減されるため、蓄積・検索速度も向上する。

図 1 に LogAuditor/LDB にパソコン操作ログ（レコード長約 700 バイト）を格納した場合のデータ量削減効果の一例を示す。本例では RDB を使用した場合と比較して必要なストレージ容量が約 1/23 に削減されている。

4. 2 並列処理技術

LogAuditor/LDB、LogAuditor/AQL では圧縮、伸張、検索処理を複数のプロセッサにより並列処理し、プロセッサ数に応じた処理速度の向上を実現する。また、データを複数のストレージに自動的に分散配置し、並列に入出力を行う。これにより、ログのデータ量に応じたプロセッサやストレージを用意することによってスケーラビリティの高いシステムを提供できる。図 2 にパソコン操作ログを対象

とする LogAuditor/LDB のプロセッサ数ごとの全件検索速度性能の一例を示す。

4. 3 高速文字列照合技術

LogAuditor/LDB は蓄積時にログの形式を指定する代わりに、蓄積後にログ形式を判別しながらログを抽出可能であるという特長を持つ。しかし、従来の文字列照合方式ではログの形式判別に必要な複雑な照合処理に十分な速度が得られなかった。LogAuditor/LDB では当社独自の sDFA (size-reduced Deterministic Finite Automaton) 方式⁽⁴⁾ (特許出願中) により条件式規模によらずほぼ 1 億文字/秒の高速処理を実現し、この問題を解決した (図 3)。

一般にデータベース検索の高速化には索引を利用することが多いが、ログ管理では蓄積速度の低下やストレージ容量の増大が問題になる。LogAuditor/LDB では高速文字列照合技術により、蓄積速度、ストレージ容量と検索速度の両立を図った。

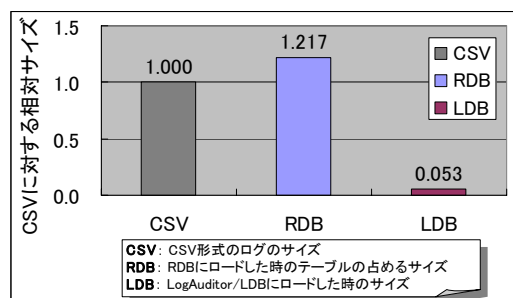


図 1. データ圧縮によるデータ量比較 (LogAuditor/LDB)

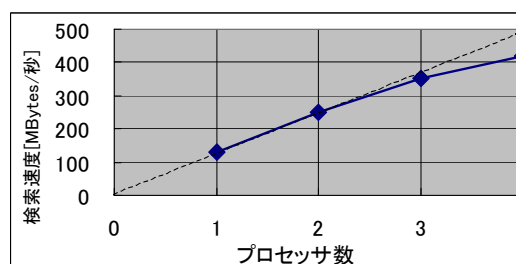


図 2. ログの全件検索速度性能 (LogAuditor/LDB)

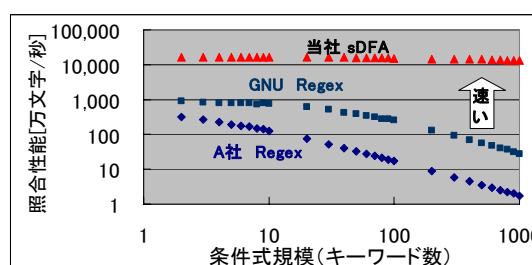


図 3. 文字列照合速度性能の比較

5. 統合ログ管理ソリューション活用例

MDITでは、LogAuditor Enterpriseを活用したソリューションとして、企業内の業務フロー実行ログ、パソコン操作ログ、ファイルサーバアクセスログなどを統合管理した結果から、内部統制を目的とした監査レポートを出力する“分析テンプレート”を提供している。分析テンプレートは、対象とする製品のログ仕様ごとに、統合ログDBの構造、ログ分析用データマートの構造、ログの取り込み形式を定義することで、これらを統合したログからMicrosoft Excel形式の監査レポートを出力する。

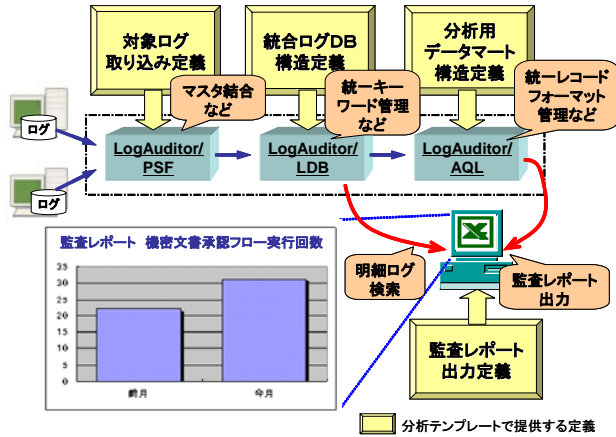


図4. 分析テンプレートの構成イメージ

通常、ログは文字列形式によりシステムで発生した事象を記録しており、その膨大な文字列情報から、如何なる行為や出来事が起こっているのかを、人間が直感的に把握するのは困難である。例えば、機密ファイルへのアクセス件数が、前月と比較して増えているのか、またその傾向は、業務フローの実行状況と関係があるのかなどは、ファイルサーバや業務アプリケーションのログ（文字列情報）参照だけでは解析が非常に困難である。この問題を解決すべく、無形のログを表やグラフ形式に可視化して報告する機能が監査レポートであり、その一例を図5に示す。機密ファイルのアクセスが、利用者の業務状況に合致しているか一目で分かる例を示しており、仮に異常なアクセス件数を示した場合には、適切な業務以外でのアクセスが多すぎると判断でき、セキュリティ管理策の検証や見直しなどに活用できる。

このように、異なるシステムのログであったものを同じ視点で集計・参照することで、複数システムの利用状況を統合的に管理することが可能になる。さらにLogAuditor Enterpriseでは、詳細な原因追求のために不可欠な“ログ明細に遡った検索”を、監査レポートの該当箇所から超高速に実行することが可能である（図5のログ明細表示）。

上記の内部統制での活用例の他、統合ログ管理ソリューションは、表3に示すような情報セキュリティ管理を始めとする様々な分野での活用が可能であり、今後分析テンプレートの充実化を推進している。

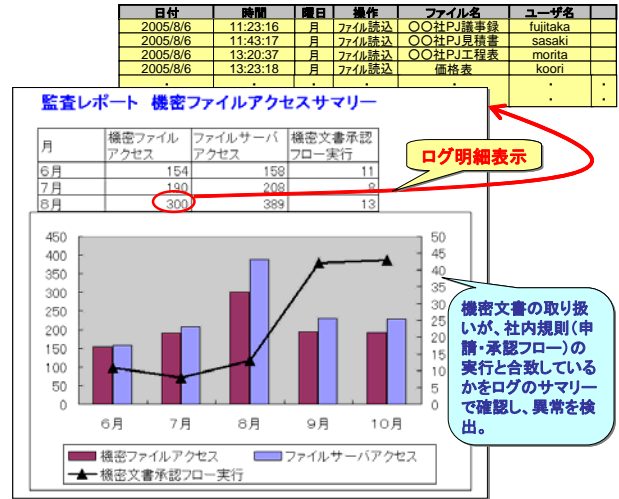


図5. 監査レポート例

表3. 統合ログ管理活用の対象業務例

対象業務	ログの種類	活用例
情報セキュリティ	・パソコン操作ログ ・サーバアクセスログ ・DBアクセスログ ・電子メールログ ・入室管理ログ ・ファイル暗号化ログ ・Webアクセスログ	利用者権限に合った社内情報使用の状況把握 → セキュリティポリシーの見直し(PDCAサイクル)
内部統制	・コンテンツ管理ログ ・パソコン操作ログ ・サーバアクセスログ	業務フローの実行と合わせた現場での情報利用の確認 → 監査資料の出力
情報インフラ管理	・ネットワークログ ・電子メールログ ・Webアクセスログ ・サーバアクセスログ ・複合機ログ	ネットワーク負荷状況、共有の情報システム機器の稼働状況の確認 → 情報インフラ整備の最適化
情報システム運用管理	・ネットワーク機器ログ ・パソコン操作ログ ・サーバアクセスログ	情報システム機器の運用状況の確認 → 機器、ジョブの運用スケジュールの最適化

6. むすび

多種多様なログの統合管理を実現する LogAuditor Enterprise について紹介した。今後は、ログの大規模化と多様化が進むと予想されるため、更なるスケーラビリティの拡大化及び分析テンプレートの充実化を図る予定である。

参考文献

- (1) 内部不正の目撃者, 日経コンピュータ 2006/5/1号, No.651, 40~55 (2006)
- (2) Sah, A.: A New Architecture for Managing Enterprise Log Data, Proc. of LISA 2002, 121~132 (2002)
- (3) 中村隆顕, 他: 大規模ログデータベースの実現、情報処理学会全国大会第68回、1D-2 (2006)
- (4) 中村隆顕, 他: 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) 藤村隆, 他: 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、三菱電機技報, 80, NO.4, 281~284 (2006)