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

郡　光則*
森田　登**
藤村　隆**

“LogAuditor Enterprise”: Integrated Management System for Various Log Data

Mitsunori Kori, Noboru Morita, 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，ログの種類の増加に伴い，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㈱（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

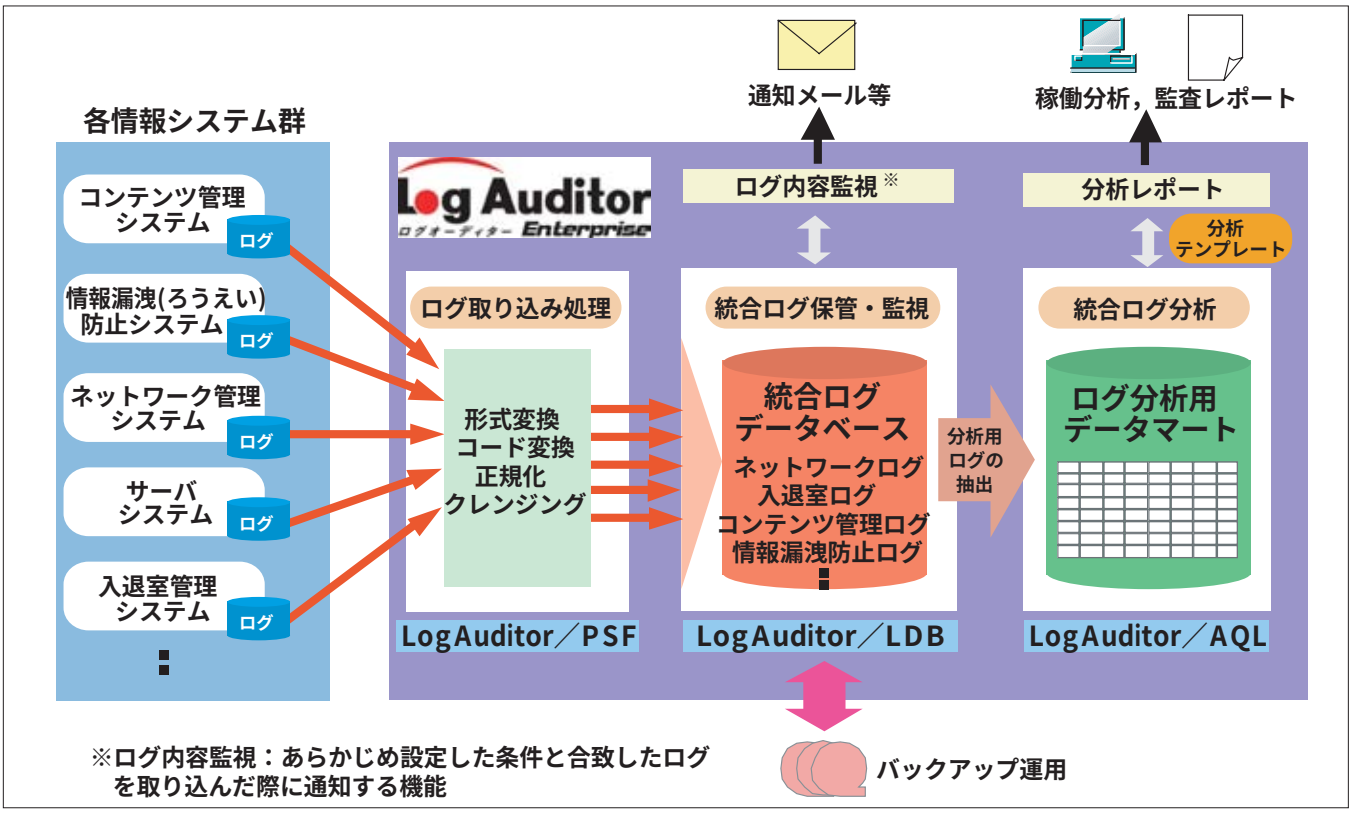
(2)　データ規模に応じた処理速度とスケーラビリティの高いシステム構成を実現する並列処理技術

(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化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㈱の登録商標である。



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㈱ 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㈱