特集論文

統合ログ管理ソリューション“AnalyticMart for LogAuditor”

和田貴成*
大塚哲史*
阿波基文*

Integrated Log Management System "AnalyticMart for LogAuditor"

Takashige Wada, Tetsufumi Otsuka, Motofumi Awa

要　旨

近年，内部統制やセキュリティ等，様々な側面からログ管理の必要性が高まっている。その中で，蓄積したログをうまく活用できない，活用に手間がかかる，統合ログ管理システムの必要性は理解できるが費用対効果が見えにくく，導入の敷居が高いといった問題が現れてきた。

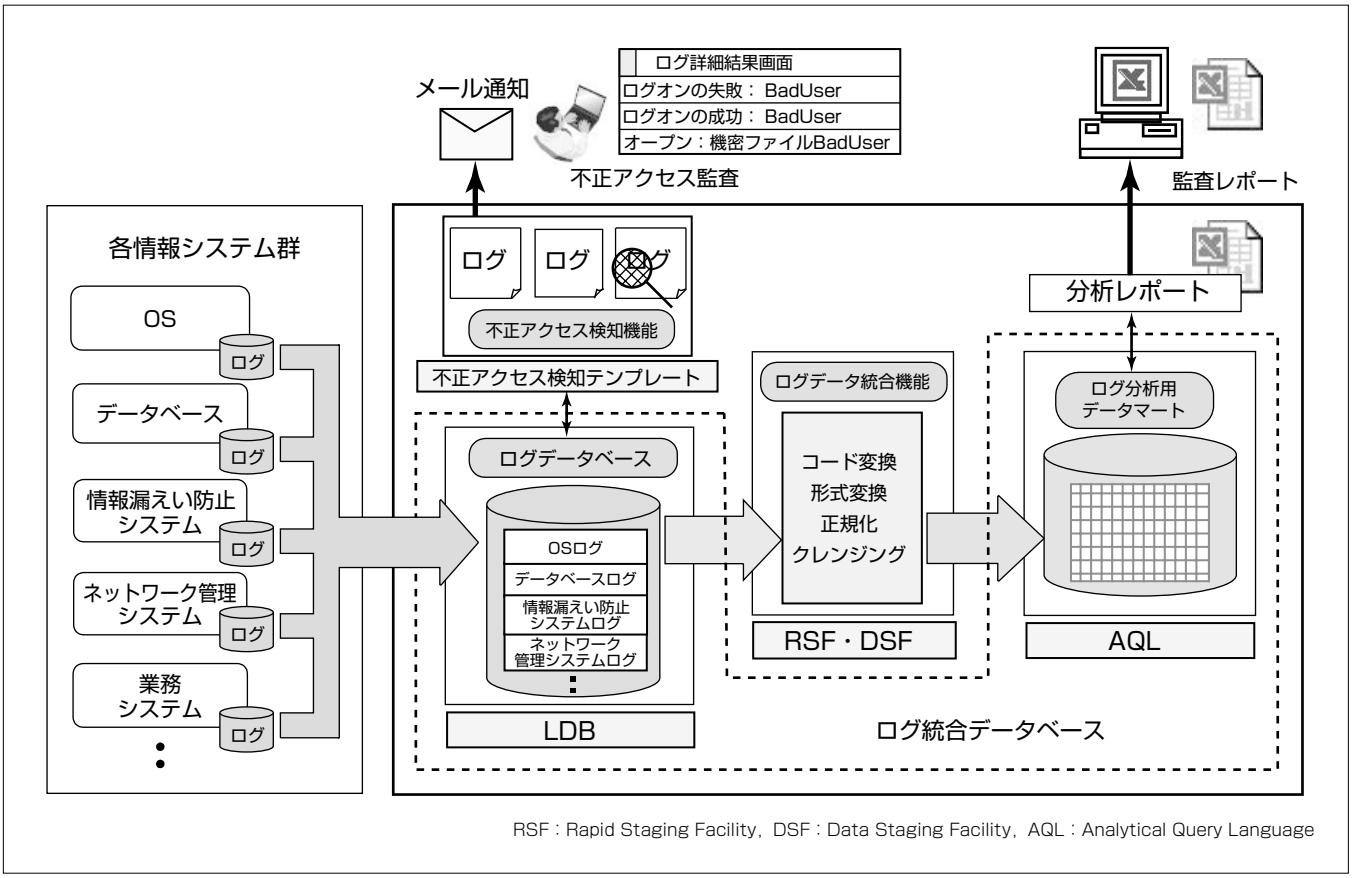
三菱電機インフォメーションテクノロジー㈱（MDIT）の統合ログ管理ソリューション“AnalyticMart for LogAuditor”は，これらの課題を解決する統合ログ管理製品である。

AnalyticMart for LogAuditorは，ログを管理するため標準的なコンポーネントをあらかじめセットにし，導入しやすくした製品である。この製品の特長を，次に示す。

(1) 可変長，不定形型等，各種形式のログデータを1個のデータベース（Log DataBase：LDB）で一元管理

(2) LDBに対し，横断検索することによって，不正アクセスの一連動作を高速に追跡することが可能

(3) “不正アクセス検知テンプレート”の利用によって，複数OSのログ管理を容易に実現でき，不正アクセスの証跡に相当するログデータを効率的に見つけ出すことが可能



RSF：Rapid Staging Facility，DSF：Data Staging Facility，AQL：Analytical Query Language

“AnalyticMart for LogAuditor”のシステム構成

AnalyticMart for LogAuditorは，統合的にログを保管するLDB，主にログの加工を行うRSF・DSF，統合的なログの分析エンジンであるAQLから構成される。また，分析フロントエンドとなるMicrosoft Excel(注1) アドインツールDIAOLAP，さらに，監査条件に基づいて管理者に対しメール通知をする不正アクセス検知テンプレートが提供される。

（注1） Excelは，Microsoft Corp. の登録商標である。

*三菱電機インフォメーションテクノロジー㈱

1. まえがき

近年，内部統制(コンプライアンス遵守など)徹底の高まりや，数多く報告される個人情報漏えいなどのセキュリティ事故を背景に，様々な側面からログ管理の必要性が高まっている。企業の内部統制(IT全般統制)では，企業内の各情報システムから出力されるアクセス・操作・メール送受信等の履歴が，情報漏えい事件などが発生した場合の監査証跡として重要度が増している。そのため，ログを蓄積する作業自体は多くの企業で始まっている。しかし，ログ管理システムの導入・運用が進んでいく中で，蓄積したログを十分に活用できない，活用に手間がかかる，統合ログ管理システムの必要性は理解できるが費用対効果が見えにくく導入の敷居が高いといった問題が表面化してきた。

MDITでは，システムログ・アクセスログ・セキュリティログ等の様々なログを証跡として収集・蓄積し，一元管理するAnalyticMart for LogAuditorを開発し，これらの課題を解決した。

本稿では，統合ログ管理を低コストで容易に実現できることを特長とする不正アクセス検知テンプレートを中心に，AnalyticMart for LogAuditorの特長，機能について述べる。

2. ログ管理の課題

日本版SOX法(米国企業改革法)成立以降，内部統制を実現するために，多くの企業がログ管理システムを導入し，企業内で発生するログの蓄積を開始している。しかし，ログ管理を行う上で，次のような課題が顕著になってきた。

(1) 日本版SOX法の施行によって，ログの収集自体は開始したが，分析はほとんど行わずに蓄積するだけの運用になっている。

(2) システム単位でログを管理しているため，ログの集約や紐(ひも)付け等を手作業で実施する必要があり，手掛かりを掴(つか)むためのログ解析に膨大な時間がかかる。

(3) 統合ログ管理製品は導入・運用のためのまとまったコストが必要となるため，すぐには導入ができない。

AnalyticMart for LogAuditorは，これらの課題を解決し，多種で大量のログの効率的な統合管理を実現する。

3. AnalyticMart

3.1 AnalyticMartとは

AnalyticMartは，販売分析，顧客分析，ログ分析，環境データ分析といった多様で形式の異なるデータの分析を，統一したアーキテクチャで効率よく低コストで実現でき，かつ中小規模から大規模まで，規模に合わせたデータ分析システムの構築・運用を可能とするフレームワークである。

AnalyticMart for LogAuditorは，AnalyticMart製品ラインアップの中からログを管理するための標準的なコンポーネントをあらかじめセットにし，導入しやすくした製品である。また，多様なテンプレートが使える拡張性とログ数に依存しないライセンス体系を備えた製品となっている。

次に，AnalyticMart for LogAuditorの特長を挙げる。

(1) 可変長，不定形型等，各種形式のログデータを1個のデータベース(LDB)で一元管理

(2) LDBに蓄積した複数種類のログに対し，共有キーワードで横断検索することによって，情報漏えいに至るまでの一連動作を高速に追跡することが可能

(3) 不正アクセス検知テンプレートを利用することによって，複数OSのログ管理を低コストで容易に実現することが可能

3.2 製品の構成と機能

AnalyticMart for LogAuditorは，統合的にログを保管するLDB，統合的なログの分析エンジンであるAQL，主にデータの加工・変換機能を提供するRSF・DSFで構成している。さらに，分析フロントエンドとなるMicrosoft ExcelアドインツールDIAOLAP，不正アクセス検知テンプレート，ISMS(Information Security Management System)監査作業支援に利用できるISMSテンプレート(オプション製品)を提供する。それらのコンポーネント，動作環境について**表1**，**表2**に示す。

(1) LDB

LDBは，非構造化データを蓄積するのに最適なDBMS(DataBase Management System)であり[3]，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機能を持つコンポーネントである。

LDBは，中国語，韓国語等を含むログデータに対応し，文字コードとしてUTF-8をサポートした。

表1．AnalyticMart for LogAuditorの構成コンポーネント

コンポーネント	機能
LDB	統合ログデータの蓄積保管・監視 高速な検索
AQL	分析用ログデータの保存 高速な検索・集計
RSF，DSF	ログデータの収集と加工，取り込み
DIAOLAP	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
不正アクセス検知テンプレート	監査条件の設定 不正アクセスログ高速検索，メール通知
ISMSテンプレート	ネットワークセキュリティ管理テンプレート 監査ログ管理テンプレート

表2．AnalyticMart for LogAuditorの動作環境(注2)

サーバ	Microsoft Windows Server 2008 R2
クライアント	Microsoft Windows 7 Professional／Enterprise Microsoft Windows Vista Business Microsoft Windows XP Professional

(注2) Windows，Windows Server，Windows Vistaは Microsoft Corp.の登録商標である。

⑵ AQL

AQLは，データ分析プラットホームとして十年以上の実績を持つ高性能DBMSであり，集計・分析に適した構造化データとしてログを保存し，高速なデータ検索・集計が可能なコンポーネントである。

AQLは，近年更に増大するデータに対応し，ロード性能，データ圧縮性能の向上を実現した。

⑶ RSF，DSF

RSFは，企業内に存在する様々なログデータを収集・加工するツールであり，次の特長を持つ。

①きめ細かいデータの加工・編集機能

②高い生産性・保守性

③サポートするデータソースは，各種ログを格納した主要RDB(Relational DataBase)，又はCSV(Comma Separated Values)などのフラットファイル

DSFは，RSFによる加工済みデータに対して，高速にソート，JOIN(列の結合)を行うコンポーネントである。

⑷ DIAOLAP

DIAOLAPは，AQLの分析用フロントエンドであり，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，次の特長を持つ。

①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

②柔軟な非定型分析，ウイザード形式での容易な操作

③集計値から明細の分析データに遡るドリルスルー機能

⑸ 不正アクセス検知テンプレート

不正アクセス検知テンプレートは，内部統制における標準的な不正アクセスの検知を，低コストで容易に実現できる製品である。**5章**で詳細を述べる。

⑹ ISMSテンプレート

ISMSテンプレートは，ISMS監査レポートの作成を支援するテンプレート製品である。対象は，Webアクセスログ，ファイアウォール，RDBへのセッションログ，及びSQL(Structured Query Language)文実行ログ等，各分野の代表的な管理ソフトウェアから発生するログ計8種類である。

4. AnalyticMartの高速処理技術

AnalyticMartでは，LDBとAQLを支える次の主要な高速処理技術[(1)]によって，プロセッサ数に応じたスケーラビリティの高いシステムを提供している。

⑴ 必要なストレージ容量を10分の1程度に削減するデータ圧縮技術

⑵ 複数のプロセッサによる圧縮・伸張・検索処理や，複数のストレージに自動的に分散配置されたデータの入出力処理を効率的に処理することができる並列処理技術

⑶ sDFA(size-reduced Deterministic Finite Automaton)方式[(4)]によって，条件式規模によらずほぼ1億文字/秒の高速処理を実現する高速文字列照合技術

5. 不正アクセス検知テンプレート

⑴ 目的

不正アクセス検知テンプレートは，主に，次の2項目を実現することを目的に開発した製品である。

①内部統制上の標準的な不正アクセスの検知

内部統制(IT全般統制)上の標準的な不正アクセスには，**表3**に示す項目などが挙げられる。

不正アクセス検知テンプレートは，ファイルサーバへのログイン成功，ログイン失敗，機密ファイルのアクセス等のアクセスログ管理を容易に実現できるフレームワークを持っているため，**表3**の“ファイルの不正アクセス”“不正侵入”“パスワード搾取”を検知することができる。

②テンプレート化による容易な導入

不正アクセス検知テンプレートは，複数OS(Windows Server，HP-UX[(注3)]，Solaris[(注4)])のログを統合して管理できる製品であり，テンプレート化したことによって，導入コストの削減を実現している。また，ログ監査条件などの初期設定は，ブラウザベースのログ管理アプリケーションを通して行うことができ，統合ログ管理システムを容易に導入することが可能である。

(注3) HP-UXは，Hewlett Packard Co.の登録商標又は商標である。
(注4) Solarisは，Oracle Corp.及びその子会社，関連会社の登録商標である。

⑵ 機能

不正アクセス検知テンプレートが保有する機能を次に示す。

①設定管理機能

監査条件及びメール通知先の設定，ログの詳細情報検索を，ブラウザベースのログ管理アプリケーションから利用することができる。

②運用機能

監査条件に基づいた検索，及び条件に一致した場合のメール通知を行うことができる。

⑶ 運用例

不正アクセス検知テンプレートのシステム運用例について，次に述べる。

表3．内部統制上の標準的な不正アクセス例

分類	例
ファイルの不正アクセス	セキュリティホールを悪用して，ファイルを盗み見・削除・改変する行為
不正侵入	バックドア(不正侵入を行うための裏口)などを仕掛け，そのパソコンを踏み台に他のパソコンへ侵入する行為
パスワード搾取	盗聴や総当り攻撃によるパスワードの搾取
妨害攻撃	正常なアクセスを妨害するDDoS(Distributed Denial of Service)攻撃

まず，運用を開始するまでに，社内のポリシーや監査対象とするログの種類を考慮した上で，ログ監査条件をブラウザベースのログアプリケーションから設定する(**図1**)。入力項目は，ログの種類(Windowsセキュリティログ，HP-UXログイン／SUログ，Solarisログイン／SUログ計5種)，事象(ログオン成功，ログオン失敗，機密ファイルへのアクセス等計26種)，時間帯(00:00:00～23:59:59)，検出判定指標とその回数(検出判定指標は，連続で一定回数以上の検知，一定期間に一定回数以上等計4種)，監査ログ検知時のメール通知先である。なお，メール通知先に関しても，**図2**に示す“メール通知先設定画面”から容易に設定することができる。

この運用例では，監査対象サーバがWindows，HP-UX，Solaris各1台計3台であった場合に，次の3個の監査条件を設定して運用を開始したとする。

①Windowsサーバへの深夜時間帯ログイン失敗(5回連続)

②HP-UXサーバへの深夜時間帯ログイン失敗(5回連続)

③Solarisサーバへの深夜時間帯ログイン失敗(5回連続)

運用開始後，Windowsサーバに関する監査条件①が検知される事態が発生した場合，監査担当者(“メール通知先設定画面”の送信先アドレス項目指定者)に対してメールが通知される。メールを受信した監査担当者は，ログの詳細情報を取得するために，**図3**に示す“ログ詳細結果画面”を参照する。なお，**図3**は，複数OSのログに対して横断検索(条件：深夜時間帯)を行った検索結果である。この画面によって，ユーザーBadUserが，深夜時間帯にWindowsサーバへのログイン操作を5回連続で失敗していることを確認できる。また，その直後に，これとは異なるアカウント名によるHP-UXサーバに対する3回連続のログイン失敗が記録されており，これは，監査条件に合致した操作(この例の場合，監査条件①②③に該当する操作)以外にも不正な操作を試みた可能性があると推察することができる。

このように，複数OSのログを対象にした横断検索が実行できるため，事前に設定した監査条件以外にも，今後大きな問題につながる可能性のある兆候を見つけ出すことができる。

なお，調査の過程で取得した情報は，情報漏えいが発覚した際の監査証跡や，今後のセキュリティ管理策の検証や見直し等に活用することができる。

6. むすび

多種多様なログの統合管理を実現するAnalyticMart for LogAuditorについて述べた。また，複数OSのログ管理を低コストで容易に実現する“不正アクセス検知テンプレート”を開発した目的・備える機能・運用例についても述べた。今後は，統合ログ管理の多様なニーズにこたえるため，対応するログの種類の充実化を図る予定である。

ログ監査条件設定画面

検知条件	◉有効　○無効
検知条件名	Windowsセキュリティログ_ログオン失敗
ログの種類	Windows2000,2003_security
事象	ログオン失敗（ID=529）
時間帯指定	00:00:00～05:00:00
検出判定指標	一定回数以上の検知 5回
メール通知先	◉有効　○無効 default設定

図1．ログ監査条件設定画面

メール通知先設定画面

送信元アドレス	WinError@mdit.co.jp
送信先アドレス	AuditUser@mdit.co.jp
件名	不正アクセス発生通知
本文	Windowsサーバで不正アクセスが発生しました。
SMTPサーバ	SmtpServer
SMTPポート番号	25
最大添付ファイルサイズ	10,240KB以内

SMTP：Simple Mail Transfer Protocol

図2．メール通知先設定画面

ログ詳細結果画面

Bad2User:/dev/pts/4: Wed Nov 16 02:24:30 2011,2011/11/16 02:24:30,LoginError,SOLARIS
Bad2User:/dev/pts/4: Wed Nov 16 02:24:44 2011,2011/11/16 02:24:44,LoginError,SOLARIS
失敗の監査 529 2011/11/16 02:28:01 ログオンの失敗：パスワードが無効。ユーザー名：BadUser
失敗の監査 529 2011/11/16 02:28:10 ログオンの失敗：パスワードが無効。ユーザー名：BadUser
失敗の監査 529 2011/11/16 02:29:21 ログオンの失敗：パスワードが無効。ユーザー名：BadUser
失敗の監査 529 2011/11/16 02:29:33 ログオンの失敗：パスワードが無効。ユーザー名：BadUser
失敗の監査 529 2011/11/16 02:30:17 ログオンの失敗：パスワードが無効。ユーザー名：BadUser
Bad3User pts/ta 10.100.211.213 Wed Nov 16 02:34,2011/11/16 02:34:32,LoginError,HP-UX
Bad3User pts/ta 10.100.211.213 Wed Nov 16 02:34,2011/11/16 02:34:54,LoginError,HP-UX
Bad3User pts/ta 10.100.211.213 Wed Nov 16 02:35,2011/11/16 02:35:22,LoginError,HP-UX

図3．ログ詳細結果画面

参考文献

(1) 郡　光則，ほか：多種多様なログの統合管理を実現するLogAuditor Enterprise，三菱電機技報，**80**，No.10，615～618（2006）

(2) Sah，A.：A New Architecture for Managing Enterprise Log Data，Proc. of LISA 2002，121～132（2002）

(3) 中村隆顕，ほか：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，ほか：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，ほか：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）