特集論文

情報セキュリティを支えるデータ分析フレームワーク“AnalyticMart”

小出健太*
村松祐一郎*

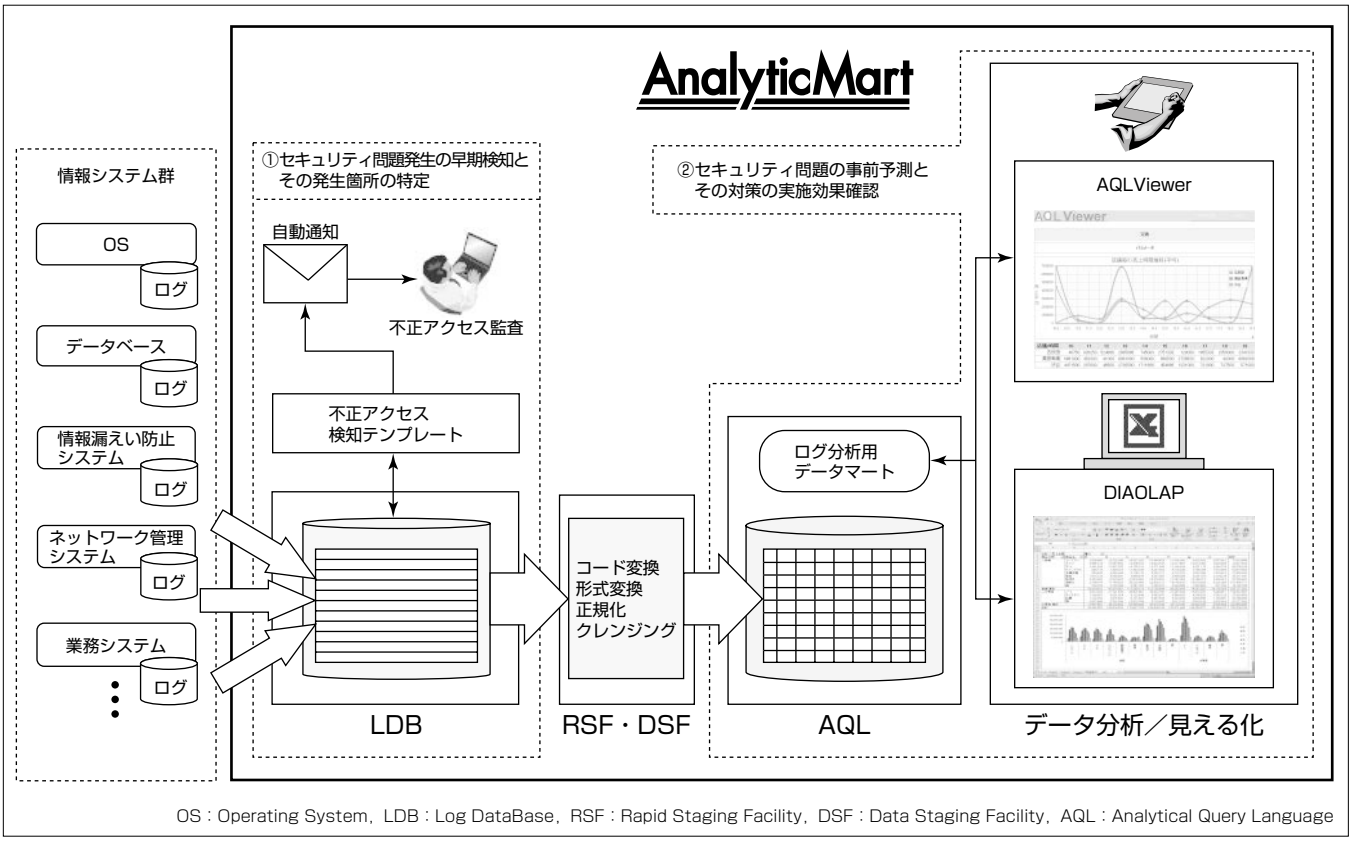
Data Analysis Framework "AnalyticMart" for Foundation of Information Security

Kenta Koide, Yuichiro Muramatsu

要　旨

昨今，内部統制やセキュリティ問題に対応するため，情報セキュリティ対策がますます重要になってきている。情報セキュリティ対策のためにはセキュリティログを十分に監視し活用することが必須であるが，セキュリティ問題発生時の即応性(課題①)や，セキュリティ問題の事前予測と対策(課題②)という複合的なデータの運用が必要であり，セキュリティログを十分に活かしきれていないという問題があった。これに対して，三菱電機インフォメーションテクノロジー㈱(MDIT)ではデータ分析フレームワーク“AnalyticMart”を発表し，これらデータ活用の課題への対応を図っている。

“AnalyticMart”では，課題①の“セキュリティ問題発生の早期検知とその発生箇所の特定”のために，ログデータベース“LDB”への多様なセキュリティログの蓄積と不正アクセス検知テンプレートによる自動的なセキュリティログの監視機能を提供している。また，課題②の“セキュリティ問題の事前予測とその対策の実施効果確認”のためには，情報分析ツール“DIAOLAP”による高度な非定型分析と，分析・表示ツール“AQLViewer”による簡易な操作による定型分析と見える化の機能を提供している。特にAQLViewerはノートパソコンよりも携帯性の高いタブレット端末に対応することで，多種多様な情報セキュリティ対策の現場での活用を実現している。



“AnalyticMart”の機能構成

各情報システムから集められたログ情報はLDBに集積され，同時にRSF・DSFによってデータ化されてAQLに蓄積される。LDBへの蓄積情報は蓄積タイミングでの自動的に監視対象となり，AQLへの蓄積データは分析に使用される。

*三菱電機インフォメーションテクノロジー㈱

1. まえがき

セキュリティ分野におけるデータ活用は，セキュリティ事故による企業価値の毀損を防ぐためや，内部統制等の外的要因によって，欠かせないものとなっている。これら内部統制におけるITでの対応としては，各情報システムから出力されるアクセス・操作・メール等の履歴や，情報漏えいや誤送信といった事件が発生した場合の追跡，ヒヤリハットによって，事件発生のリスクが高い箇所を特定し，事前対策を取ることが必要となる。しかし，情報セキュリティ分野のデータ，特に中心となるセキュリティログは多種多様に存在する上，日常的に増え続ける性質があり，取りこぼしが許されないものであることから，管理コストが高く，多様な分析を行う必要があるといった問題が存在し，重要度に比して導入難度が高く，敬遠されがちであった。

MDITでは，データ活用を包括的に支援する，データ分析フレームワークAnalyticMartを提供している。このAnalyticMartを用いることで，セキュリティ分野におけるデータ活用の問題点を解決することができる。

本稿ではセキュリティデータ活用として，データ分析／見える化を容易に実現するDIAOLAP及びAQLViewerを中心にAnalyticMartの特長と機能について述べる。

2. AnalyticMart

2.1 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。

2.2 AnalyticMartの特長

⑴ 多様なデータの分析・蓄積に対応するデータベース

AnalyticMartは，高速処理技術[1]が組み込まれた2つのデータベース“LDB”“AQL”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。同時に，データベース間をつなぐETL(Extract，Transform，Load)ツールを組み合わせることによって，販売／経理データに代表される構造化データから，システムへのアクセスログのような非構造化データまで様々なデータの分析を実現している。

①LDB

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，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。

②AQL

AQLは，データ分析プラットホームとして10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の保存と，高速なデータ検索・集計が可能なコンポーネントである。

③ETLツール

AnalyticMartでは2つのETLツール“RSF”と“DSF”を提供している。RSFは，企業内に存在する様々なログデータを収集・加工する高機能ETLツールである。DSFは加工済みデータに対して，高速にソート，JOIN(列の結合)を行う簡易ツールとして用意されている。

⑵ 短期間の構築ですぐに使えるシステム

親しみやすく簡単に扱えるBI(Business Intelligence)ツール(DIAOLAP，AQLViewer)や，目的別の各種テンプレートによって，短期間の構築で運用できるシステムを提供している。

①DIAOLAP

AQLのヘビーユース向け分析用フロントエンドである。詳細は**3. 2. 1項**で述べる。

②AQLViewer

AQLのライトユース向け分析用フロントエンドである。詳細は**3. 2. 2項**で述べる。

③各種テンプレート

近年求められるログへの即時対応をサポートする。主に以下の4種を用意している。

・不正アクセス検知テンプレート
・ISMS(Information Security Management System)テンプレート
・環境データ見える化テンプレート
・情報漏えい対策テンプレート

⑶ スモールスタート可能性と拡張性

AnalyticMartは柔軟なコンポーネント構成とすることができ，要旨の図に示すAnalyticMartの機能構成で，LDB周辺までを含めてデータの蓄積のみのスモールスタートから始め，ETLツールやAQLを駆使しての，様々なデータの統合分析へ徐々に構成を拡張させることも可能である。

3. AnalyticMartを使ったセキュリティ対策

この章では，AnalyticMartを使ってセキュリティ対策を行うにあたってのセキュリティの問題を改めて整理し，AnalyticMartでの解決策(対応機能)及び，セキュリティ対策の実際の運用について述べる。

セキュリティ分野について，データを使って捉えるべき課題は大きく分けて次の2つがある。

⑴ セキュリティ問題発生の早期検知とその発生箇所の特定
⑵ セキュリティ問題の事前予測とその対策の実施効果確認

3.1 セキュリティ問題発生時の早期検知とその発生箇所の特定

セキュリティ問題の発生は，できる限りの早期検知と発生箇所の確実な特定が必要となる。セキュリティログの日

常的な監視は問題の発生有無確認につながり，蓄積は問題が発覚した後の追跡のために必須である。AnalyticMartではこれらの対策のため，LDB及び不正アクセス検知テンプレートを提供している[2]。LDBにはセキュリティにかかわるログを全て蓄積することができる。LDBへ日常的に蓄積されるログに対して，不正アクセス検知テンプレートは，“ログイン失敗が短時間に何度も発生している”“深夜に機密ファイルへ定期的なアクセスが行われている”といった，不正アクセスが疑われるログを自動的に発見し，ユーザーへメール通知する機能を備えている。これによって，問題発生の迅速な検知が実現される。この通知メールには発生したログそのものの情報も記載されており，LDBにアクセスすることで実データやその周辺データに関して追跡調査を行うことができ，問題発生箇所を特定することが可能となる。

3.2 セキュリティ問題の事前予測とその対策の実施効果確認

セキュリティ問題は発生してしまうと社会的信用の失墜につながってしまうため，問題を未然に防ぐことが重要になる。セキュリティ問題を未然に防ぐためには，セキュリティログの分析による問題発生要因や危険な箇所の予測・特定とそれらへの対策実施・実施効果確認が必要になる。同時に，セキュリティの現場は多岐にわたるため，得られたセキュリティについての知見をどのような現場でも見える化できる工夫が必要になる。AnalyticMartでは，DIAOLAPとAQLViewerという2つのツールによってセキュリティログの分析と見える化を実現している。これら2つのツールはともに分析と見える化を行うAnalytic Martのフロントエンドである。両者にはAQLのヘビーユース向け(DIAOLAP)と，ライトユース向け(AQLViewer)という用途の違いがあり，セキュリティログに対して，知見を得るための非定型分析はDIAOLAPによって行い，得られた知見の展開や各種の現場での情報セキュリティデータ活用ではAQLViewerを活用するといった用途による使い分けを想定している。

3.2.1 DIAOLAP

DIAOLAPはAQLのヘビーユース向けとして，セキュリティログを情報システムセキュリティの部門が詳しく分析を行うような用途に向いている。その特長を次に述べる。

(1) インタフェースにExcel(注1)を採用

Excelのアドオンツールとして提供しており，使い慣れたExcelからシームレスに利用できる。セキュリティログを時間帯別，ユーザー別，操作種別，対象別に，アクセス回数や失敗回数で集計(ピボットテーブル)し，グラフで表示するといった手間のかかる処理の自動化をサポートしている。

(2) 高度な非定型分析と表示ウイザードの提供

柔軟な呼び出し形態とExcelの分析機能による高度な非定型分析を実現している。データ呼出し条件の設定には，ウイザードで時間や場所といった変数を指定していく形式を採用し，容易な操作を提供している。これによって，多様な環境に潜在するセキュリティリスクを簡単な操作で洗い出していくことができる。

(3) ドリルスルー機能の提供

作成した集計表からセキュリティリスクやその予兆を発見したときに，ドリルスルー機能によって，その原因となる明細のデータにさかのぼって表示することができる。これによって，絞り込んだデータの実体であるセキュリティログを確認し，問題発生の前後に何が起こっているのかなどの確認が容易にできるようになる。

(注1) Excelは，Microsoft Corp. の登録商標である。

3.2.2 AQLViewer

AQLViewerはAQLのライトユース向けとして，セキュリティログの分析結果を，情報セキュリティにかかわる各現場で手軽に素早く提示することや，現場の情報システムやセキュリティに精通していないユーザーが分析結果を閲覧するような用途に向いている。AQLViewerは，DIAOLAPの提供する機能をライトユース向けにスリム化しつつ，同等レベルの分析能力を維持している(**図1**)。その特長を次に述べる。

(1) Webブラウザでの表示

クライアントの表示は標準のWebブラウザだけで実行可能としている。これによって，この機能はライセンスフリーで展開することができ，セキュリティ対策のコスト低減や，多数のライトユーザーへ定型の分析結果を展開したい場合，分析結果閲覧のためにインストールするソフトウェアの費用を低減できるといった効果がある。

(2) 容易なインタフェース

図2にあるように，DIAOLAPでは分析結果としてグラフを得るまでの操作に，ログインからグラフ表示操作まで含めて8ステップの作業が必須であった。AQLViewerでは，これらステップを整理して細かな設定を行う6ステップをサーバ側であらかじめ事前定義情報として作成して保存しておくことでクライアント側での作業量を低減し，4ステップでのグラフ表示を実現した。クライアントから閲覧する際は，定型となる事前定義情報の選択と，データ絞

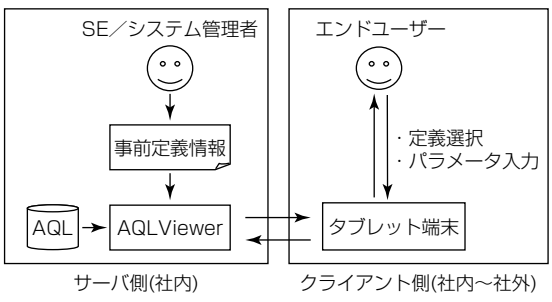


図1．AQLViewerの構成

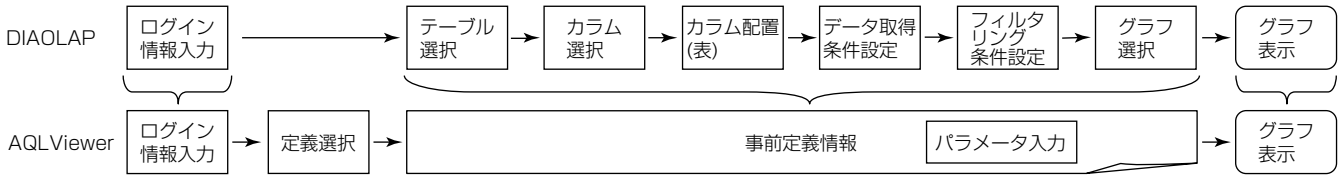


図2．DIAOLAPからAQLViewerへの操作削減

り込みパラメータの設定(年月日での範囲絞り込みや，特定サーバ／ファイルへのアクセス，特権ユーザーの指定等)を実施するだけでグラフが表示される。これらのパラメータ設定内容は事前定義情報内で全て決定されるため，パラメータ指定が必要なければ，定義の選択のみでグラフが表示されることになる。また，クライアント側では定型の表示のみとなって自由度が下がることになるが，サーバ側の事前定義情報にはクエリの自由記述や4種のグラフ表示の選択といった設定が可能であり，AQLViewer全体としてはDIAOLAPに近い表示の自由度を確保している。

(3) タブレット端末への対応

近頃利用され始めた，ノートパソコンより携帯性に優れたタブレット端末に対応している。これによって，ノートパソコンでも手狭な場所での操作や，移動先での突然の閲覧，早急に分析結果を出さなければならない場合など，多くの場面で蓄積・分析した情報セキュリティのデータを活用することができる。また，指先での操作や視認性の悪い場所での操作に対応して，大型ボタンの配置や押すべきボタンの配色を目立たせるといった工夫を行い，タブレットの特性を活用するユーザーインタフェースとしている。

3.3 AnalyticMartを用いたセキュリティ対策の運用

ここまで，AnalyticMartによるセキュリティ分野のデータに対するアプローチを述べてきた。最後に，実際にAnalyticMartを用いたセキュリティ対策を運用する際のデータの流れとその効果を，**図3**に沿って述べる。

最初に，各情報システムからセキュリティのデータを取り出すため，ISMSテンプレートを用いて自動的にセキュリティログをLDBへ蓄積するシステムを構築する。蓄積されるセキュリティログは不正アクセス検知テンプレートによって常に監視され，問題があればユーザーへ即座にメール通知される。問題発生後に，問題となったログそのものを確認したい場合も，通知メールの内容からLDBの該当ログをスムーズに表示し，詳細を確認することができる。問題が発生しない日常では，LDBに蓄積されたデータはRSF・DSFによって分析用に整理され，AQLに保存される。これによってログの高速な分析システムが整う。ユーザーは非定型のログ分析をDIAOLAPによって行い，セキュリティの脆弱(ぜいじゃく)性が存在していないかを確認する。確認したログについて問題があれば，ドリルスルーによってより生のデータに近いものを確認し，不正アクセス検知テンプレートへの監視事項追加や，その他の対策へつなげることができる。既知となっているセキュリティ状況の指標についてはAQLViewerで定型化しておき，タイムリーに見える化したデータを入手できる。特に，セキュリティがかかわる場面は幅広いため，監査のサイトツアーでの実データ提示や，サーバラック裏などの手狭な場所での閲覧，データの説明時にデータを手元から示すといった様々な状況が想定される。そのため，セキュリティ分野のデータ活用でタブレット端末に対応したAQLViewerは有用なツールである。

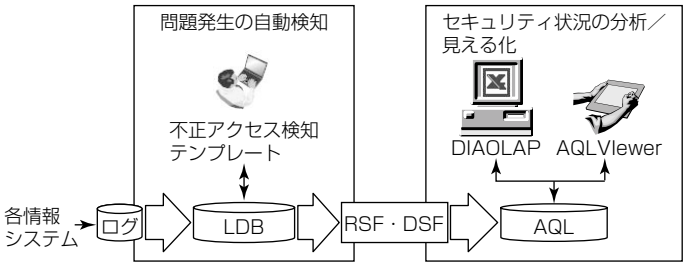


図3．AnalyticMartでのセキュリティ対策の流れ

4. むすび

多種多様なデータの分析基盤となるAnalyticMartのセキュリティ分野への適用と，その効果について述べた。本稿では主に，分析と見える化を行うフロントエンドツールについて述べ，用途に沿って使い分けるツールを提供していること，またそれぞれのツールの特長について述べた。

AnalyticMartを用いることで，セキュリティ問題発生の早期検知とその発生箇所の特定，及びセキュリティ問題の事前予測とその対策の実施効果確認が可能となる。今後は使い勝手の向上や使用環境の拡充を進め，より多くの場面で活躍できるプラットホームにしていく予定である。

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) 和田貴成，ほか：統合ログ管理ソリューション“AnalyticMart for LogAuditor”，三菱電機技報，**86**，No.7，391～394（2012）