



IBM System i 対応の監査ソリューション

QJRN/400は実務環境でのすべてのクリティカルなイベントを管理したい企業に対して監査とセキュリティ管理の最適な組合せを提供します。

システム監査

システム監査モジュールはセキュリティ、接続攻撃、システム・コンフィグレーション、ライブラリ、オブジェクトに関する監査要求に対応します。

精度の高いモニター（リモート・メンテナンス、サービス・プロバイダ）

重要なスプール・ファイルなどで実施されたアクション監査

プロファイル、システム・バリュー、ネットワーク属性、重要なオブジェクトでの権限への介入

セッションへのオープン、許可されていないリソースへアクセス攻撃

オフィス時間外のアクティビティ・モニター

監査パラメータでの整合性チェック

実務への転送管理をモニター

データベース監査

データベース監査モジュールはシステム上のすべてのデータベース・ファイルへの修正に関する詳細なレポートを提供します。

フラッグとレポートで：

権限ファイルへの変更

与信制限に対する異常な変更

出し入れがない銀行口座の挙動

ユーザ・プロファイルへの不適切な変更

重要なフィールド（銀行口座、クレジット・カード等）への介入

外部アプリケーション（DFU、SQLなど）からのオペレーション

外部からのリモートでのアプリケーションへの修正

主な機能

ジャーナル管理

すべてのジャーナル(システム、データベース、またはユーザ定義)はQJRN/400

で表示・モニターすることができます。機能には新規ジャーナル作成、すでにあるジャーナルのレジスターが含まれます。

各環境は完全にジャーナル化されたデータベースでフィールドを定義したレポジトリーを保有しています。レポジトリーは自動で生成され、カスタマイズには制限はありません。

HAプラットフォームとの完全な互換性

QJRN/400はSystem iで開発された主なHAソリューションと互換性があります。

Quary Manager

Quary Systemsというユニークで新しいコンセプトを導入したQJRN/400はビジネス・インテリジェンスのレベルをジャーナル・プロセスへと高めました。各レシーバのコンテンツは不正動作や重要なデータへの不適切なアクセスの可能性を示す特別で、ユーザ定義されたイベントまたは、シンタックス用にクエリされます。この特定のデータベース、ファイル、フィールド用のこれらのクエリをカスタムができる能力により、ユーザに分かりやすく、完璧なフォーマットでレシーバ・コンテンツを提供します。

監査プロセスの自動化

Query Managerはユーザにほとんど範囲制限のないデータとイベントの取得機能を提供するだけでなく、高度なカスタマイズ可能レポート・エンジンを搭載しています。シンプルなOS/400メッセージやEメールが自動で作成され、個別のイベントやアラームで始動(トリガー)されます。日々、週ごと、時間ごとのプリント・レポート、PDFファイル、Eメールを適切な部署に配信することができます。

重要情報の選択

QJRN/400は不正行為の可能性のある「Concept Sensitive」イベントを識別することができます。

System i 管理者はスタンダード・オペレーション(=, >, <, Like, Range, List...)や、すべてのフィールドに特別なプログラムを適応させることで多くの選択が可能です。

選択または除外する値(バリュー)のリストはプログラムまたは以前のクエリで入力することができます。

「時間外で実行されたオペレーション」や「アプリケーション外で実行されたオペレーション」などの一般的な選択

関連ナンバー、プロファイル(クラス、グループ、特別権限)、プログラム、ジョブ、システム、期間での選択

プロセス・モード

組込まれた柔軟なリアルタイム・セキュリティ・ソリューション

クエリ・オンデマンド・モード:クエリはインタラクティブでもバッチ・モードでも稼働させることが可能です。このモードは管理者が即ちステータス・レポートを抽出し、悪意なイベントや不正行為のソースを分離するために利用されます。

コンティニユアス・モード:Query Managerは絶えずモニターし、不正行為を暗示するパターンや傾向を検知することができます。このコンティニユアス・モードはまた特別なイベントをトリガーする例外やソフトウェア・バグを検知することにも使用できます。アラートはモニターしていたイベントが発生するに従って適切な担当者に送ることができます。

オートマチック・モード:レシーバが検知された時に自動でオフ設定します。このモードはクオリティ・モニタリングの場合には、統計またはトレース・アビリティのどちら用であってもデータ収集を確実にします。

スケジュール・モード:ユーザが指定した期間(年、月、日、時間、分)でのユーザのアプリケーションまたはシステムの過去情報を抽出します。

マルチ・レポート・ツールとフォーマット

管理者がデータを抽出しようとするモードに関係なく、QJRN/400はFTPやSMTPプロトコルを使用して、幅広い出力フォーマット(PDF, EXCEL, WORD)を提供します。

単一イベントから月単位のアクティビティまで、担当者は内部および外部監査要求に適合できるレポートを簡単に作成することができます。

イベント&トレンド・レポート:ユーザの行動とトレンドを特定できるレシーバの単一エントリー、またはイベント数のサマリーの決められたイメージでキャプチャーすることができます。

トリガー・イベント・レポート:即時の注意が要求される疑わしいアクティビティ(例、クレジット制限の変更など)の結果からトリガーされたEメール警告

トレース・ファイル・レポート:これはクリティカル、または関連性するイベントのみを含むヒストリー・ログの圧縮サマリーです。ジャーナルからすべてを取得するよりも選択したイベントを取得するほうがオンラインでのストレージ容量を削減することができます。より有益なレポートが可能です。

プリパレーション・ファイル・アウトプット:大容量用で、ユーザは1つ以上のクエリで使用されることができる事前選択を実行することができます。

リモート・レプリケーション

QJRN/400はユーザがリモートでもまったく同じクエリとレポート・モデルを実行することができます。この機能により、中央のIT部門がリモート・オフィスに対して、最初からまたビジネス・ルールを構築することなく、一貫性のあるセキュリティ・プロセスを構築することができます。

株式会社クライム

〒103-0014

東京都中央区日本橋蛸殻町1-25-4

日本橋栄ビル4F

電話 03-3660-9336 FAX 03-3660-9337

Email: soft@climb.co.jp

http://www.climb.co.jp

Climb Inc.
Growing to Meet Your Needs