

情報を守る！IBM i 5250型内部統制対応セキュリティツール

Bitis[®] JS *Journal Supervisor*



情報セキュリティの定義。それは「情報を守ること。」

いかに外部からの攻撃に対するセキュリティシステムを用意しても、社内で発生する不正行為は防ぎづらいものです。

J-SOX法対応、内部統制の観点から管理業務が増えることが考えられ、運用管理の負担は今後ますます重くなることが予想されます。

Bitis JSは、現状分析から監査までスムーズにセキュリティ環境が構築できる為、お客様の情報セキュリティの確保と運用管理の負担軽減を実現します。

ジャーナルが
活用できていない

すぐに始めたい
運用に手間
を掛けたくない

不正アクセス
を知りたい

ジャーナルデータ
を参照したい



が解決します！

重要なデータは
しっかり守りたい

- 不正アクセスの監視・ログ取得
- 重要オブジェクトの保護や更新ログを取得し検索可能
- アクセスルール自動作成など、すぐに始められてずっと使える簡単運用
- 不正アクセス時に管理者へ、メッセージでの通知が可能
- ツール自身の改ざんや不正を防止するセキュリティ機能搭載

① アナライザー

監査・ユーザージャーナルを元に現在の使用状況を自動的に収集・分析します。

アクセス状況DB

参照

更新



② アジャスト

アナライザーで分析したアクセス状況DBに、アクセス時間や回数を調整して監視対象ルールDBを作成します。

監視対象ルールDB

ログ出力



③ モニター

日々発生する参照・更新情報と、監視対象のルールを比較してエラーを抽出します。抽出情報は画面より表示可能。



- ・サインオンエラー
- ・サインオン時間エラー
- ・オブジェクトアクセスエラー

④ サーベイ

参照・更新情報のジャーナルをデータベースに出力・蓄積し重要オブジェクトのフィールドレベルまでの更新情報が参照可能です。



検査項目

- ・ユーザー
- ・オブジェクト
- ・日時

⑤ ホールド

重要オブジェクトに登録されたDBに対してアクセスエラーが発生した場合、使用しているジョブを即座にホールドやメッセージで管理者に通知します。

⑥ ディフェンス



特権ユーザーの不正行為を防止する機能。ジャーナルの停止やBitis JS関連のDBへの直接更新などを監視して、ログを蓄積します。

⑦ウォール

重要オブジェクトとして登録されたDBに対して、外部からのアクセスを監視します。



⑧ スナイパー

ターゲットにしたユーザープロファイルのコマンドログを取得・参照します。



その他の社名、製品名などは、一般に各社の商標または登録商標です。