マイナンバー制度 (社会保障・税番号制度) は 2017 年 1 月から本格的に運用がはじまり、社会保障の分野などとの情報連携が開始されるようです。各自治体からは、個人あるいは法人に対してマイナンバーが通知されております。

各種媒体でニュースなどを見る機会は増えていますが、実際には「マイナンバーって何だろう?」と思っている人の方が多いのではないでしょうか?

さまざまな企業システムが乱立している中、これらのシステム運用に欠かせないのが「データ管理(情報管理)」という視点です。

- アクセス権の管理はきちんとされているのか
- アクセス ログはきちんと取得/管理されているのか
- ファイルの暗号化きちんとされているのか

誰が、いつ、どのような用途で情報にアクセスし、不必要なダウンロード、あるいは持ち出しがされていないのかを管理していく必要があり、適切なセキュリティ施策を実施することになります。

Actian PSQL v12 はマイナンバー制度への対応においても、しっかりとサポートしております。

PSQL の持つ基本的なセキュリティ

PSQL では、既に、堅牢なセキュリティを擁しています。簡単にご紹介します。

Btrieve データベース URI 機能

データベース URI 機能を使用すると、ファイルへの直接の OS レベルのクライアント側にアクセスすることなく、Btrieve データファイルにアクセスするアプリケーションを可能にします。データベース URI の使用によって、サーバ上の Btrieve データへのクライアント側の共有またはマップが必要ないため、クライアント側からの不正アクセス防止が可能となります。

Btrieve レベルのセキュリティ

Btrieve セキュリティのため、複数の使用可能な認証および許可モデルがあります。データベース セキュリティ モデルでは、データベース エンジンが Btrieve データファイルのユーザーの認証と許可を行います。ユーザーがデータに接続しアクセスする能力は、そのユーザーがアプリケーションを実行するコンピューターに正常にログインできる限りは、オペレーティング システムのアカウント識別情報やファイル システム権限とは関係ありません。このモデルの主な利点の 1 つは、オペレーティング システム ユーザーのデータ ファイルへのアクセスを制限する一方で、データベース エンジンを介したデータ アクセスにはフルアクセスを許可できることです。

SQL レベルのセキュリティ

PSQL の SQL レベルセキュリティをオンにすると、全ての SQL 経由のアクセスは、個々のテーブルのフィールドまでに制御し、ログイン認証されたユーザーとグループで管理することができます。

PSQL データファイルの強力な 128 ビットオンディスク暗号化

長いオーナーネームの暗号化を使用すると、ディスク上の Btrieve ファイルは強力な 128 ビット暗号化で保護されます。この 128 ビット暗号化は、Btrieve ファイル/テーブルに対して、長いオーナーネームと暗号化を設定することで簡単に得られます。下記の2設定方法があります:
(1) Btrieve の Set Owner オペレーション(29)の使用を設定する
(2) Maintenance ユーティリティを使用し、長いオーナーネームと暗号化を設定する

強力な 128 ビットのワイヤ暗号化

PSQL v12 には、PSQL 使用時に発生するデータベース関連のネットワーク トラフィックを暗号化する機能があります。特に外部からのネットワークアクセスが可能な場合、このようなネットワーク上で送信されるデータへの不正アクセスに対する追加の抑止力が推奨されます。

PSQL v12 / Vx 製品に関しては
http://www.agtech.co.jp/products/actian/psql/v12/

また、データベース選定のヒントになる PSQL 製品に関連した様々な情報を公開しております。
http://techtarget.itmedia.co.jp/tt/special/tt140401/

PSQL vs マイナンバー制度

PSQL のセキュリティについては、先に説明した通り、Oracle や SQL Server と同等のセキュリティを擁し、安心してご利用いただけます。また、マイナンバーガイドラインの技術的安全管理措置で挙げられている項目に対しても、以下の通り、PSQL 製品が対応可能であることを示しています。

		PSQL 既に対応済	Audit for PSQL で対応	備考
アクセス制御	テーブル毎のアクセス権設定	○		
	ファイルアクセス時のパスワード	○		
	アクセスログ		○	
アクセス者の識別と認証	ログインの強制	○		
	ユーザーの認証	○		
外部からの不正アクセス等の防止	外部からのファイル参照保護	○		OS のファイル共有機能を使用しない
情報漏えい等の防止	ファイル暗号化	○		
	通信回線上のデータ暗号化	○		

Audit for PSQL 製品に関しては
http://www.agtech.co.jp/products/actian/audit-PSQL/

- テーブル毎のアクセス権設定
  PSQL の機能で、テーブル毎(列毎)に読み込み、更新、削除の可否を設定することができます。
- ファイルアクセス時のパスワード
  オーナーネームを設定することで、読み込みのみ許可するか、読み書きを許可するかの設定ができます。
- アクセスログ
  オプション製品の「**Audit for PSQL**」を使用することで、だれがどのテーブル(ファイル)に対してどのような操作(読み込み、変更、削除等)を行ったか記録することができます。クエリ機能で特定のテーブルに対する操作を検索することも可能です。
- ログインの強制
  セキュリティを有効にすることで、アクセスに際しログインを強制できます。
- ユーザーの認証
  登録ユーザー以外がアクセスすることを防止できます。
- 外部からのファイル参照保護
  URI 形式でファイルパスを指定することで、Btrieve API でアクセスする際に OS のファイル共有機能を使わずに運用が可能です。これにより、サーバーの外部からファイルの存在を隠蔽できます。
- ファイル暗号化
  オーナーネーム設定時に、暗号化を有効にすることで、バイナリエディターで参照しても情報を読み取れなくできます。
  万が一、ファイルが持ち出された場合の対策ができます。
- 通信回線上のデータ暗号化
  クライアント/サーバーで運用時に通信回線上のデータを暗号化する設定を行えます。これにより、データの盗み見による漏えいを防止できます。

株式会社エージーテック
本　社:〒101-0054 東京都千代田区神田錦町 1-21-1 ヒューリック神田橋ビル 3F
TEL:03-3293-5300（代表）FAX:03-3293-5270
カスタマーセンター　TEL:03-3293-5283　Mail:info@agtech.co.jp

© 2016 Actian Corporation. All rights reserved. Actian は米国およびその他の国における Actian Corporation の商標です。
本資料で記載される、その他すべての商標、名称、サービス マークおよびロゴは、所有各社に属します。