内部統制強化時代のアプリケーション開発を支援するデータベース ― 日立製作所／HiRDB編 ―

企業システムを構築する際の要となるデータベース．日本版SOX法をはじめとするコンプライアンスへの対応，および内部統制の強化を実現するためには，より高度で堅牢なセキュリティ機能を備えたデータベース製品が不可欠です．ミッションクリティカルな企業システムでの豊富な採用実績で培われた高い信頼性を備えた日立製作所の「HiRDB Version 8」は，内部統制とセキュリティ対策に適したデータベースです．

Part1 セキュアなデータベース構築を容易に実現するHiRDB

●データの改ざんを防止するWORM機能 ●簡単なSQLコマンドでWORM表を作成
●データへのアクセス履歴をチェック／追跡可能にする監査証跡機能 ●データへのアクセスを制御する各種機能
●ISO15408への取り組み

Part2 パッケージ開発をサポートする組み込み支援プログラム

●HiRDBパッケージ組み込み支援プログラムのメリット ●開発を容易にする組み込み支援機能
●開発を支援する手厚いサポート ●組み込みプログラムの事例が続々と登場

Part 1 セキュアなデータベース構築を容易に実現するHiRDB

内部統制の強化を目的とした日本版SOX法では，業務をITによって自動化することでリスクを低減するとともに，証跡や記録を保管することが求められています．保管しなければならないものは財務会計情報だけではありません．財務会計に至るあらゆる決済の記録，そのやりとりに利用した電子メールや社内文書などの活動の記録も保管する必要があることはもちろん，保管されている情報が正しいことの証明が求められる場合もあります．そうしたあらゆる情報の保管という重要な役目を担うのがデータベースです．

記録の保管を確実に行うためのデータベースには，不正目的の改ざんや破壊，操作ミスによる削除からデータを守るデータ改ざん防止機能が欠かせません．また，監査証跡を取得する機能，データの正当性の確保するためのアクセス制御機能，膨大な量と種類のデータを検索する機能などの要件も求められます．

データの改ざんを防止するWORM機能

先ごろバージョンアップをした日立のデータベース「HiRDB Version 8」は，これらの要件を満たすために，データの改ざんを防止し，データへのアクセス履歴のチェック／追跡を可能にし，データへのアクセスを制御するという３つの特徴的なセキュリティ機能を提供しています．

まず挙げられるのが，データの改ざんを防止する強固なWORM機能です．WORMとは，Write Once Read Manyを略したもので，CD-Rのように一度書き込んだら消すことができないという意味です．

データベースでは一般的に，ユーザのアクセス権を設定することによって，一度記録したデータの変更や削除を行えないようにしています．しかし，データベースそのものを管理しているDBA（Database Administrator＝データベース管理者）と呼ばれる人たちは，アクセス権のそのものの設定を変更したり，アクセス権が設定されていても更新や削除などのメンテナンスが行えたりします．DBAのIDやパスワードが万一盗まれたりすれば，この部分は内部統制を実現する上で一種のセキュリティホールと言えるでしょう．

HiRDBでは，DBAを含めたすべてのユーザに対し，一

度記録したデータは更新／削除が一切できないという機能をデータベース側で提供しています．この機能をアプリケーション側で実現しようとした場合，ユーザIDを確認して更新／削除の処理をすべて無視するというロジックを組まなければなりません．こうしたロジックの開発作業は容易でないばかりか，たとえアプリケーションにロジックを組み込んだとしても，アプリケーションを経由せず直接データベースを操作するツールなどを利用することで更新／削除ができてしまうなど，セキュリティホールを解消することはできません．データベース側でWORM機能を備えるHiRDBでは，どんなユーザ特権を持っていても，どんなデータベースアクセスツールを使っても，データを書き換えることができません．

簡単なSQLコマンドでWORM表を作成

HiRDBでWORM機能を利用するには，通常の表を定義するSQL文にオプション指定をするだけでWORM表を作成できます．（図1）はWORM表を作成するためのSQL文の一例です．ここでは，一度だけ更新可能な列，何度でも更新可能な列を設定するとともに，記録から10年間は更新／削除できない表を作成しています．この例のように，表全体をWORM化するのではなく，表の中に更新可能な列を設定したり，改ざん防止期間を指定するなど，柔軟なデータベース運用が可能になっています．

このWORM表は，あらかじめデータベース側で作成しておけばアプリケーション側では何も意識する必要はありません．万一，操作ミスによってデータベースを更新／削除しようとしても，データベースがエラーを返します．取引履歴，決裁済み文書，アプリケーションのログ，フォレンジックデータなどの保管に最適なソリューションを提供する機能と言えるでしょう．

データへのアクセス履歴をチェック／追跡可能にする監査証跡機能

特徴的なセキュリティ機能の2つ目は，データへのあらゆる操作を記録してデータの正当性を証明する監査証跡機能です．HiRDBは，データベースに対するあらゆるオペレーション，アクセスのログを記録し，監査証跡ファイルとして保存する機能を備えています．この監査証跡ファイルを調べることによって，例えば，通常の業務時間以外に行われたデータベースアクセス，あるいは特定の情報へのアクセス集中など，ユーザの特異な行動をチェック／分析することができます．また，前述したWORM機能と組み合わせることが可能になっており，監査証跡ファイル自体をきちんと保護することができます．

データへのアクセスを制御する各種機能

3つ目は，ユーザ権限により不正アクセスを防御する機能です．HiRDBは，パスワード文字制限により安易なパスワードを禁止したり，不正なパスワードを入力したユーザの接続を拒否する機能を備えています．これは，外部ネットワークから侵入してくるクラッカーやウイルスなどの不正アクセス，内部ユーザによる不正操作を防止するために欠かせない機能です．

また，Sun Java™ System Directory ServerなどのLDAPサーバと連携し，HiRDBに接続するユーザ認証とアクセス制御を企業システム全体で一元管理できる

■ CD-Rのように「一度書き込んだら消せない」，それをデータベースで実現

■ 柔軟な運用を可能にする，改ざん防止期間の指定，更新可能列も設定可能

WORM表を作成するためのSQL例

```
CREATE TABLE 受注履歴 ······························ 「受注履歴」テーブルを作成
  (顧客ID CHAR(3), 商品コード CHAR(5), 注文数量 INTEGER, 注文日 DATE, ······ ① 列を設定
   記録日時 DATE NOT NULL WITH DEFAULT SYSTEM GENERATED, ······ ② DBへの記録時間を記録する列を設定(自動取得)
   オプション指定 CHAR(30) UPDATE ONLY FROM NULL, ······ ③ 一度だけ更新可能な列「オプション指定」を設定
   備考 CHAR(30) UPDATE) ······························ ④ 更新可能な列「備考」を設定
INSERT ONLY WHILE 10 YEARS BY 記録日時 ······················ 記録から10年間は更新·削除できない表に設定
```

受注履歴

顧客ID…①	商品コード…①	注文数量…①	注文日…①	記録日時…②	オプション指定…③	備考…④
502	10235	2	2006/3/2	2006/3/2	NULL	
653	11597	15	2006/3/25	2006/3/25	Aタイプ	年度内納品要
417	20486	5	2006/4/5	2006/4/5	NULL	
109	10355	1	2006/4/12	2006/4/12	NULL	

× 更新·削除（DBAでも不可能）

○ 追加

当該レコードを記録した日時をシステムから自動挿入

一度だけ更新可能な列

更新可能な列

図1：データの改ざん防止を実現する WORM（Write Once Read Many）機能

機能も提供しています．この機能を利用することで，人事異動に伴うユーザ情報の変更にも柔軟に対応し，システム管理コストを大幅に削減することが可能です．

ISO15408への取り組み

このほかHiRDBは，情報システムや製品に組み込まれているセキュリティを客観的に評価するために必要な各種事項を定めた国際的な標準規格「ISO/IEC15408」の認証取得を推進しています．ISO15408対応製品は，政府調達要件になったり，平成18年度からの2年間の期限付きで情報基盤強化税制の対象になっています．HiRDBを導入することは，情報セキュリティの安全性を客観的に示すためにも非常に有効だと言えるでしょう．

Part 2 パッケージ開発をサポートする組み込み支援プログラム

セキュアなデータベース構築を容易に実現するHiRDBの導入を推進するために，日立ではアプリケーションパッケージを開発するISV向けに「HiRDBパッケージ組み込み支援プログラム」を実施しています．

これまでも，多くのアプリケーションパッケージにデータベースが組み込まれて発売されてきました．しかし，アプリケーションパッケージを開発する多くのISVは，データベースを採用するにあたってさまざまな問題を抱えています．その最大の課題と言えるのが，日本版SOX法やコンプライアンスに対応したセキュリティ対策です．また，企業間競争によるコストダウン，データベースに関連する充実したサポート体制の確立もISVにとって大きな負担になっています．HiRDBパッケージ組み込み支援プログラムは，そうした課題を解決するための最適な方法です．

HiRDBパッケージ組み込み支援プログラムのメリット

HiRDBは，前述したように日本版SOX法やコンプライアンスに対応した高度なセキュリティ機能を備えています．とりわけ，データの改ざんを確実に防止するWORM機能によって，アプリケーションに手を加えることなくセキュリティを高めることができるというメリットがあります．

また，HiRDBは上位互換性を維持しているため，データベースをバージョンアップしてもアプリケーションの変更は不要，または非常に少数の確認，保守工数だけで済みます．これにより，開発コストは大幅に低減され，特にランニングコストの面で企業間競争によるコストダウンが実現できます．機能的には，HiRDB Single Server Version 8が備えているすべてを組み込むことが可能です．HiRDBは，各種アプリケーション開発環境，他の企業システムとの連携を実現するトランザクション処理モニタやアプリケーションサーバなどに対応するとともに，Windows，Linux，HP-UX，AIX，Solarisなど主要プラットフォームをサポートしているため，マルチプラットフォームに対応したアプリケーションのデータベースとして利用できます．

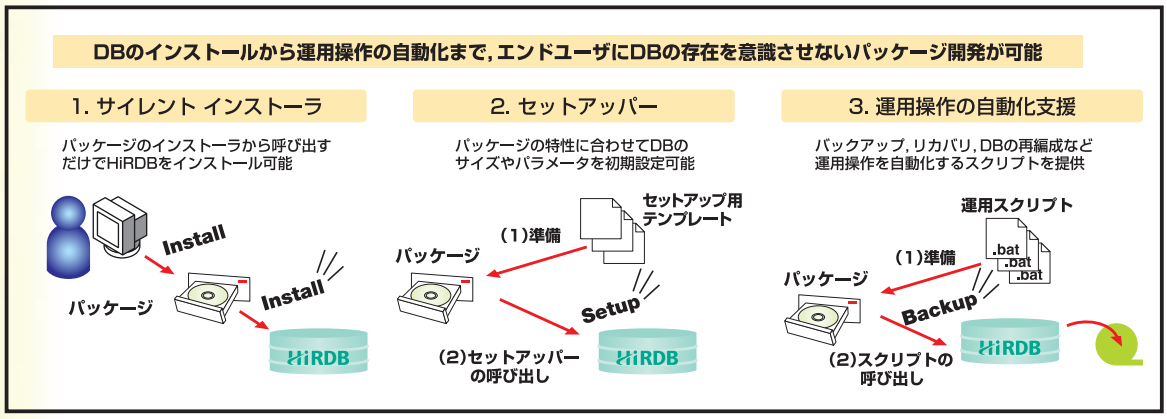
開発を容易にする組み込み支援機能

HiRDBパッケージ組み込み支援プログラムでは，パッケージ開発を容易にするための組み込み支援機能が用意されおり，エンドユーザにデータベースの存在を意識させないパッケージ開発が可能になっています（図2）．

データベースのインストール用に，アプリケーションパッケージのインストーラから呼び出すだけでHiRDBを導入できる「サイレントインストーラ」を提供しています．またインストール時には，アプリケーションの特性に合わせてデータベースのサイズやパラメータを初期設定できる「セットアッパー」も用意しています．これは，セットアップ用テンプレートを用意してパッケージのインストーラに組み込み，そこからセットアッパーを呼び出すという方法で利用できます．

さらに，データベースを運用管理する上で欠かすことのできないバックアップ，リカバリ，データベース再編成などの操作を自動化するスクリプトも提供しています．これをパッケージの運用に合わせ，アプリケーションのメニューやジョ

図2：パッケージ開発を容易にするための組み込み支援機能



ブに組み込むなどカスタマイズして活用できます．

また，SQLの機能としてトリガ，参照制約などのデータメンテナンスを自動化したり，豊富な文字列操作，日付操作用の関数を装備しています．ほかにも，ODBCやJDBCなどの各種標準データベースアクセスインターフェイスに対応するなど，アプリケーションの開発を強力に支援しています．

開発を支援する手厚いサポート

日立の手厚いサポートもHiRDBパッケージ組み込み支援プログラムを採用する大きなメリットです．HiRDBパッケージ組み込み支援プログラムでは，前述のようにHiRDBのフル機能，および組み込み支援機能を搭載しているのに加え，実際に製品テストが行える体験版を無償で提供，それを使った評価が行えます．

HiRDBパッケージ組み込み支援プログラムを採用したISVの開発者向けには，HiRDBの導入教育や自習教材を無償で提供．オンサイト支援を含む技術的なQ&Aサービスも無償で受けることができます（具体的な内容は個別相談となります）．

組み込みプログラムの事例が続々と登場

HiRDBの高度なセキュリティ機能によって，パッケージ組み込み支援プログラムを採用した事例も続々と登場しています．

例えば，日立ソフトウェアエンジニアリングのセキュアメールアーカイブシステム「TERAFILE Mail Archive」には，HiRDBがデータベースとして採用されています．このシステムは，フィルタリングによる情報漏えい対策と悪質なメールの受信防止，アーカイブ化したメールのオンライン検索／参照を目的としたものですが，ファイルシステムでのデータの更新と消去防止，検索キーを格納した管理データベースの改ざん防止，全保存メールを対象とする高速な検索処理などでHiRDBの機能が利用されています．アーカイブ化したメール自体は，光ディスクライブラリのWORMメディアに格納し，メールのヘッダ情報は，HiRDBのWORM機能を利用して高速なハードディスクに改ざんできない形で格納されています．

このほか，医療の現場で利用されるISV製の電子カルテシステムのパッケージにHiRDBが組み込まれている例があります．このパッケージで利用された理由も，データの改ざんを防止するHiRDBのWORM機能，データベースを構成するファイルへの攻撃を防ぐHiRDB File Access Control機能など，HiRDBの高度なセキュリティ機能を搭載しているためです．電子カルテのようなアプリケーションは，患者に正しい情報を伝えるインフォームドコンセントを実現しつつ，個人情報を確実に管理し，データ改ざんを決して許さないという要件が強く求められます．こうしたパッケージにとって，HiRDBは最適なデータベースと言えます．

製品に関する問い合わせ先 HiRDB 8

株式会社日立製作所 ソフトウェア事業部 販売企画センタ
TEL.03-5471-2592
http://www.hitachi.co.jp/hirdb/

取材協力／日立製作所