【B5】InterBaseテクニカルセッション

EMBARCADERO TECHNOLOGIES

DEVELOPER CAMP

パワーアップ InterBase！
2009新機能とサポートツールズのご紹介

キムラデービー代表
木村明治(きむらめいじ)

アジェンダ

EMBARCADERO TECHNOLOGIES
DEVELOPER CAMP

- InterBase SMP 2009
  - 暗号化機能
  - SMP
  - その他の新機能
- サポートツールズ
  - IBReplicator(IBPhoenix社製レプリケーションツール)
  - FBScanner(IBSurgeon社)
  - IBTransactionMonitor(IBSurgeon社)

EMBARCADERO TECHNOLOGIES

DEVELOPER CAMP

InterBase SMP 2009

InterBase SMP 2009の目玉と言えば....

EMBARCADERO TECHNOLOGIES

DEVELOPER CAMP

暗号化！

New features in InterBase 2009

EMBARCADERO TECHNOLOGIES
DEVELOPER CAMP

- データベースとカラムレベルの暗号化
- オーバーザワイヤー(OTW)ネットワークの暗号化
- バックアップファイルの暗号化
- To-Go Edition

暗号化とは

EMBARCADERO TECHNOLOGIES
DEVELOPER CAMP

- 暗号化とは第三者に内容を知られないように、内容を特別な知識なしでは読めないよう変換すること。使われる暗号技術は大きく三つに分類できる。
  - ハッシュ関数
  - 共通鍵暗号(秘密鍵暗号ともいう)
  - 公開鍵暗号＆デジタル署名
- InterBase2009で利用するのは「共通鍵暗号」

共通鍵暗号

EMBARCADERO TECHNOLOGIES
DEVELOPER CAMP

- 共通鍵暗号は、暗号と復号に同一の鍵を用いる暗号方式。代表的なものには、DES（Data Encryption Standard）やAES（Advanced Encryption Standard ）がある。
- 両者共暗号化の際、元のデータを一定のブロック長に分割した後、ビット列をかき混ぜ(攪拌:かくはん)してゆく。
- 攪拌には、鍵から複数の副鍵を生成して、その副鍵を使う。攪拌は十数回行われ、その結果として暗号文が生成される。
- 鍵のbit長が長いほど、暗号化の強度が増す。

利用のチェックポイント

EMBARCADERO TECHNOLOGIES
DEVELOPER CAMP

- 利用する側が認識する必要があるのは次の項目。
  - (1) アルゴリズムの新旧
  - (2) 鍵の長さ
  - (3) 鍵の強度とパフォーマンスのトレードオフ

- (1) アルゴリズムの新旧
  - DESは長らく使われてきたが、1990年代後半に総当たり攻撃を用いた完全解読が可能であることが実証された。
  - そのため、次世代の暗号化アルゴリズムとしてAESが採用された。採用は1997年にNIST(アメリカ国立標準技術研究所)が公募して、全世界から21種類のアルゴリズムが応募された。最終的には5つのアルゴリズムがファイナリストとして残り、その中からRijndael(ラインデール)が採用された。

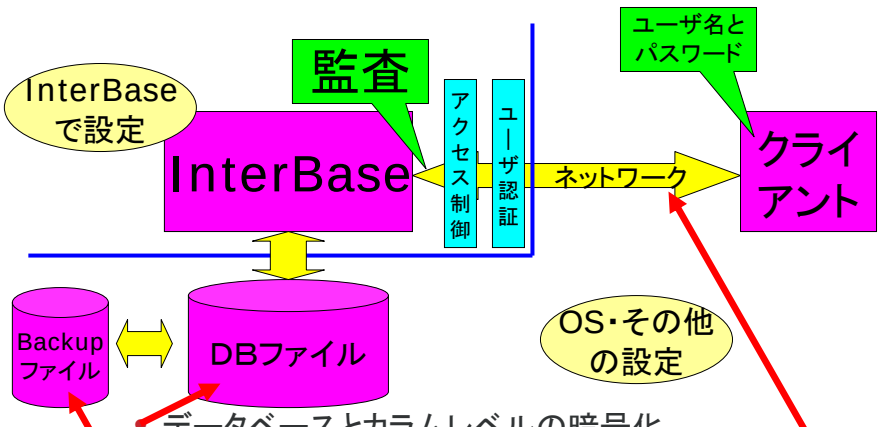
利用のチェックポイント

EMBARCADERO TECHNOLOGIES
DEVELOPER CAMP

- (2) 鍵の長さ
  - AESは規格として、鍵の長さは128ビット、192ビット、256ビットの3つが利用できる。鍵の長さが長いほどより暗号強度を高めることができる。
- (3) 鍵の強度とパフォーマンスのトレードオフ
  - 暗号・複合化は必ずパフォーマンスの劣化が伴う。
  - 全体として必要なパフォーマンスとのトレードオフを必ず確認する。

概略　全体図

EMBARCADERO TECHNOLOGIES
DEVELOPER CAMP



- データベースとカラムレベルの暗号化
- オーバーザワイヤー(OTW)ネットワークの暗号化
- バックアップファイルの暗号化

データベースとカラムレベルの暗号化

EMBARCADERO TECHNOLOGIES
DEVELOPER CAMP

- まずSYSDSOが必要。
  - SYSDSO: System Database Security Owner.
  - 暗号化の各種作業を行う。
  - SYSDBAのように予約されたユーザ名。
- そしてSEPが必要。
  - SEP: System Encryption Password
  - 暗号化に使ったキーをプロテクトするのに使う。
  - データベース毎に設定し、複数のデータベースを扱う場合は、それぞれ変更するのが望ましい。

暗号化のステップ

EMBARCADERO TECHNOLOGIES
DEVELOPER CAMP

- 1.EUA(Embedded User Authentication)が有効かどうか確認
- 2.SYSDSOの作成
- 3.SEPの作成
- 4.暗号化キーの作成
- 5.暗号化実行の権限の付与
- 6.データベース・カラムの暗号化
- 7.暗号化されたデータの復号化権限の付与・剥奪
- 3～5をSYSDSOが、それ以外はオーナーが行う。

1.EUAが有効かどうか確認

EMBARCADERO TECHNOLOGIES
DEVELOPER CAMP

- オーナーが行う
  - 操作ガイド(Operation Guide: 6-4)参照
- EUAとは
  - Embedded user authentication (EUA) はユーザ名やパスワード情報を直接データベースに埋め込みます。ユーザ認証がデータベースに埋め込まれることにより、データベースのメタデータIPは外部からの操作によりよいプロテクションを提供する。
  - 通常はadmin.ib(旧: isc4.gdb)に格納されている。
  - EUAはまた、トランスポータブルなDBをよりセキュアにする。
- Isqlで設定
  - CREATE DATABASE <database name> [WITH ADMIN OPTION]
  - ALTER DATABASE <database name> [ADD ADMIN OPTION]
  - ALTER DATABASE <database name> [DROP ADMIN OPTION]

2.SYSDSOの作成

EMBARCADERO TECHNOLOGIES
DEVELOPER CAMP

- オーナーが行う
- Isqlで設定
  - CREATE USER SYSDSO SET PASSWORD 'PASSWORD';
  - SET PASSWORD 句が指定されない場合は、SYSDSOを作成したユーザのパスワードが使われます。

```
Use CONNECT or CREATE DATABASE to specify a database
SQL> create database "localhost/3052:c:¥test2" with admin option;
SQL> create user sysdso set password 'mastkerkey';
```

3.SEPの作成

EMBARCADERO TECHNOLOGIES
DEVELOPER CAMP

- SYSDSOが行う

```
SQL> connect "localhost/3052:c:¥test2" user 'sysdso' password 'mastkerkey';
Database:  "localhost/3052:c:¥test2", User: sysdso
```

- SYSDSOがSEPを作成する場合は、以下のようにalter databaseを発行する。
- alter database set system encryption password <パスワード>
  - パスワードは255文字までの長さで、空白を含むことができる。
  - SEPは、マシン特有の情報から導出されたキーで暗号化され、データベース内に格納される。

```
SQL> alter database set system encryption password 'codegear';
SQL> _
```


4.暗号化キーの作成

EMBARCADERO TECHNOLOGIES
DEVELOPER CAMP

- SYSDSOが行う
- 書式
  - create encryption *key-name* [as default] [for {AES | DES}] [with length *number-of-bits* [bits]] [password {*'user-password'* | system encryption password}] [init_vector {NULL | random}] [pad {NULL | random}] [description 'some user description']
- 例)
  - CREATE ENCRYPTION revenue_key FOR AES WITH LENGTH 192 BITS INIT_VECTOR RANDOM;
  - CREATE ENCRYPTION expenses_key FOR DES INIT_VECTOR RANDOM;

Init_vecotor →ブロック化暗号モード を設定

EMBARCADERO TECHNOLOGIES
DEVELOPER CAMP

- ブロック化暗号モード(block cipher mode)
- DESやAESでは、データをブロック単位で暗号化する。
- しかし、単純にブロック単位で、元データを暗号化していくとすると、元データに繰り返しパターンがあると 暗号文にも同じパターンが現れてしまうという欠点がある。(後述するECB)
- そのため、前のブロックの暗号化の結果に基づいて次のブロックに対する 暗号化処理を変えていく暗号モードが導入された。
- その指定がInit_vector。
- 代表的な暗号モード
  - ECB（Electronic Code Book）電子コードブック
  - CBC（Cipher Block Chaining）暗号ブロック連鎖
  - CFB（Cipher Feedback）暗号フィードバック
  - OFB（Output Feedback）出力フィードバック

InterBase 2009で
指定できる暗号モード

5.暗号化実行の権限の付与

EMBARCADERO TECHNOLOGIES
DEVELOPER CAMP

- SYSDSOが行う
- 書式
  - GRANT ENCRYPT ON ENCRYPTION key-name to user-name;
- 例) revenue_keyをSYSDBAに許可する場合
  - GRANT ENCRYPT ON ENCRYPTION revenue_key to SYSDBA;

6.データベース・カラムの暗号化

EMBARCADERO TECHNOLOGIES
DEVELOPER CAMP

- オーナーが行う
- データベース単位の暗号化
  - 書式: alter database encrypt [[with] key-name]
  - 例) revnue_keyを使ってデータベース全体を暗号化する
  - alter database encrypt with revnue_key;
- カラム単位の暗号化
  - **書式:** alter table table-name (alter column column-name encrypt [[with] keyname]
  - 例) expenses_keyをつかってtotal_valueカラムを暗号化する
  - alter table SALES alter column total_value encrypt with expenses_key

7.暗号化されたデータの復号化権限操作

EMBARCADERO TECHNOLOGIES
DEVELOPER CAMP

- オーナーが行う
- データの復号化
  - データベース単位: alter database decrypt;
  - カラム単位: alter table table-name alter [column] column-name decrypt;
- 復号化権限の付与
  - grant decrypt[(column-name, …)] on table-name to user-name;

暗号化デモ＆メモ

EMBARCADERO TECHNOLOGIES
DEVELOPER CAMP

- 現状、デフォルトではAESの指定はできない。

```
SQL> alter database encrypt with revenue_key;
Statement failed, SQLCODE = -906

product STRONG DATABASE ENCRYPTION is not licensed
```

  - CodeGearに連絡して、追加のライセンス(無料)を有効化する必要がある。
- 一般的なInterBaseのコマンドと同じように、エラーが出たときのメッセージはわかりにくいので、あまり驚かないように….

```
SQL> GRANT ENCRYPT ON ENCRYPTION wrong_key to SYSDBA;
Statement failed, SQLCODE = -607

unsuccessful metadata update
-STORE RDB$USER_PRIVILEGES failed in grant
-no current record for fetch operation
-action cancelled by trigger (0) to preserve data integrity
```

間違ったキーを指定した場合

バックアップファイルの暗号化

EMBARCADERO TECHNOLOGIES
DEVELOPER CAMP

- gbakに新たなオプションが追加
  - -sep
  - -encrypt
  - -decrypt
- 使用例
  - 暗号化
    - Gbak –b employee.ib employee.ibak –sep “enc_test” –encrypt backup_key
  - 復号化
    - Gbak –r employee.ib employee.ibak –sep “enc_test” –decrypt backup_key

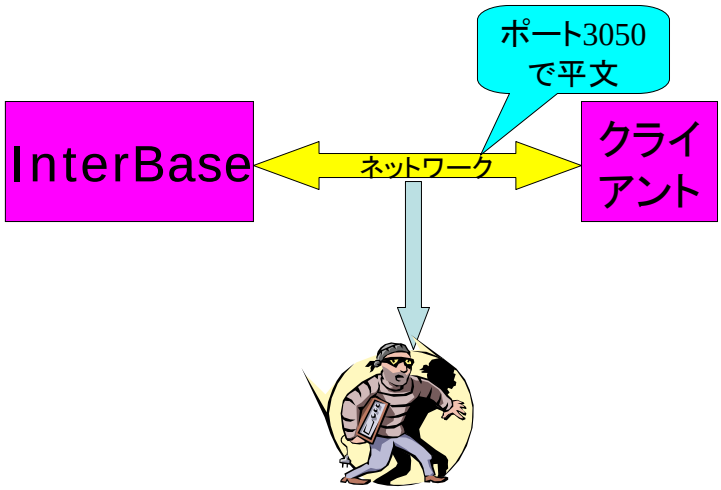
OTWネットワークの暗号化

EMBARCADERO TECHNOLOGIES
DEVELOPER CAMP

- ワイヤプロトコルの暗号化
- サーバサイドとクライアントサイドでX.509設定が必要
  - OTW暗号化はSSL v3 とTLS v1 セキュリティプロトコルを使って提供されている。
  - SSLはX.509標準を公開キーのインフラとして使っている。

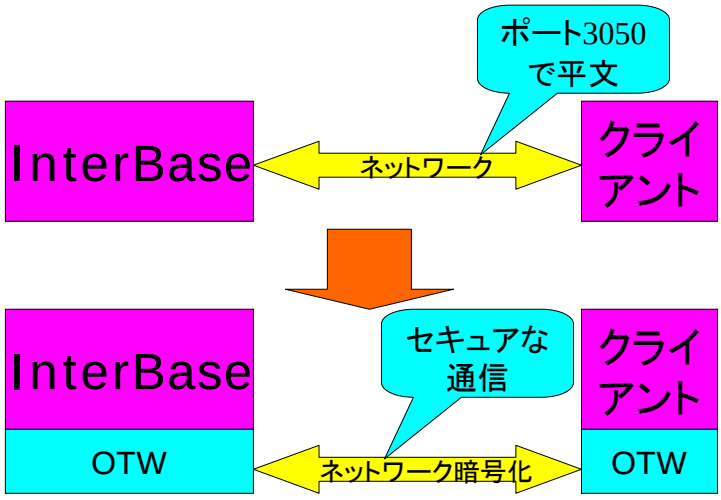
InterBaseの通信イメージ

EMBARCADERO TECHNOLOGIES
DEVELOPER CAMP



InterBaseの通信イメージ

EMBARCADERO TECHNOLOGIES
DEVELOPER CAMP



新機能: その他のトピック

EMBARCADERO TECHNOLOGIES
DEVELOPER CAMP

- To-Go Edition
  - インプロセスで使えるDBライブラリ
  - SQLiteや、Firebirdのembmedded Server、MySQLのlibmysqldと同じ形態。
- SMP対応強化
  - InterBase7からSMP対応

EMBARCADERO TECHNOLOGIES

DEVELOPER CAMP

サポートツールズ

サポートツールズ

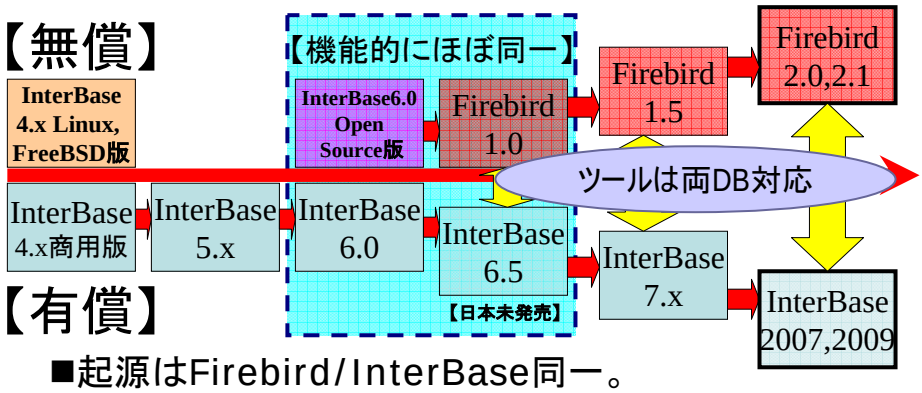
EMBARCADERO TECHNOLOGIES
DEVELOPER CAMP

1. IBReplicator(IBPhoenix社製レプリケーションツール)
2. FBScanner(IBSurgeon社)
3. IBTransactionMonitor(IBSurgeon社)

お問い合わせは、info@kimuradb.comまで。

EMBARCADERO TECHNOLOGIES
DEVELOPER CAMP

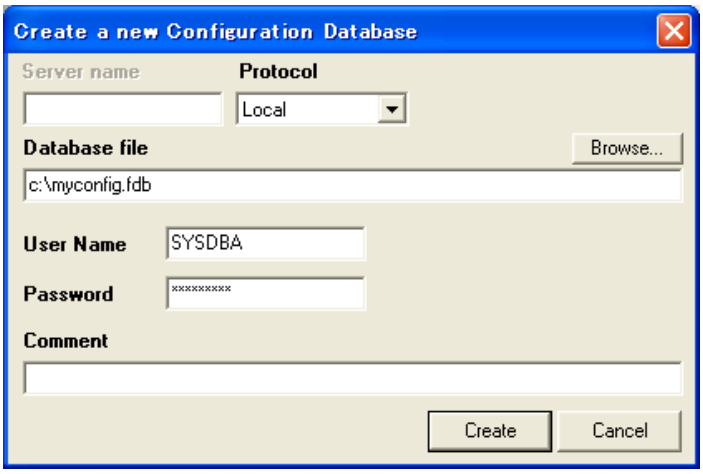
FirebirdとInterBaseの関係



- ■起源はFirebird/InterBase同一。
- ■一時オープン化されたソースから分岐
- ■現在はそれぞれ別の進化をとげる

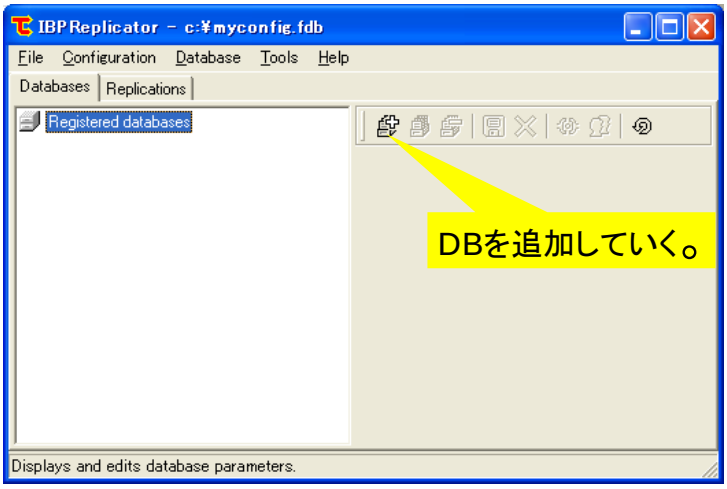
Replication Managerを使って新規のconfigを作成

EMBARCADERO TECHNOLOGIES
DEVELOPER CAMP



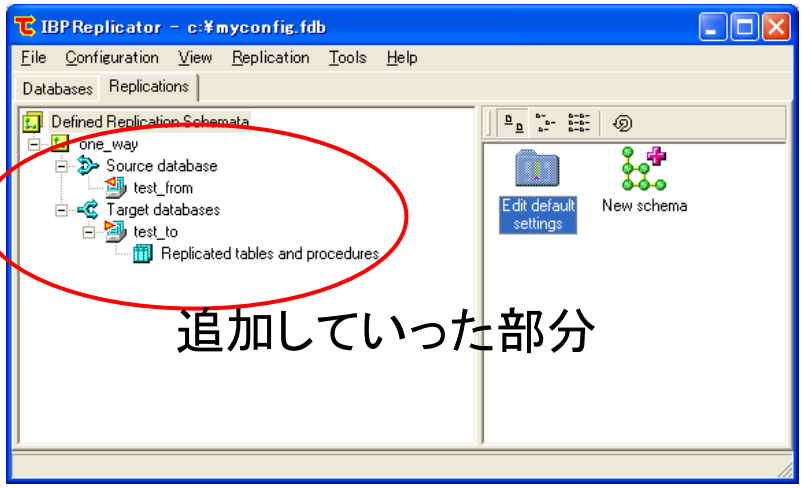
データベースの追加

EMBARCADERO TECHNOLOGIES
DEVELOPER CAMP



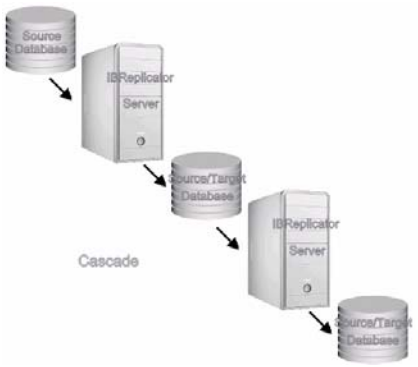
スキーマにDBを追加していく。

EMBARCADERO TECHNOLOGIES
DEVELOPER CAMP



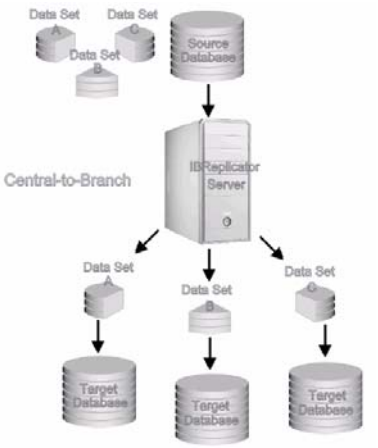
IBReplicatorの構成例

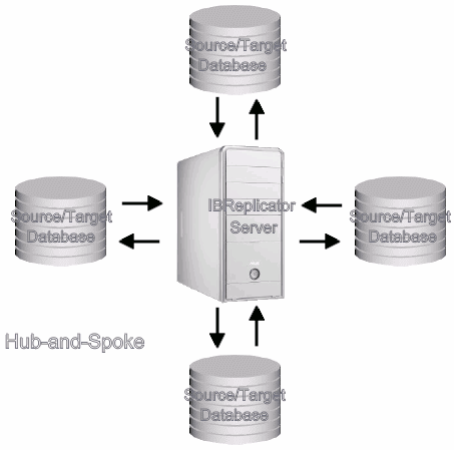
EMBARCADERO TECHNOLOGIES
DEVELOPER CAMP



IBReplicatorの構成例(続き)

EMBARCADERO TECHNOLOGIES
DEVELOPER CAMP





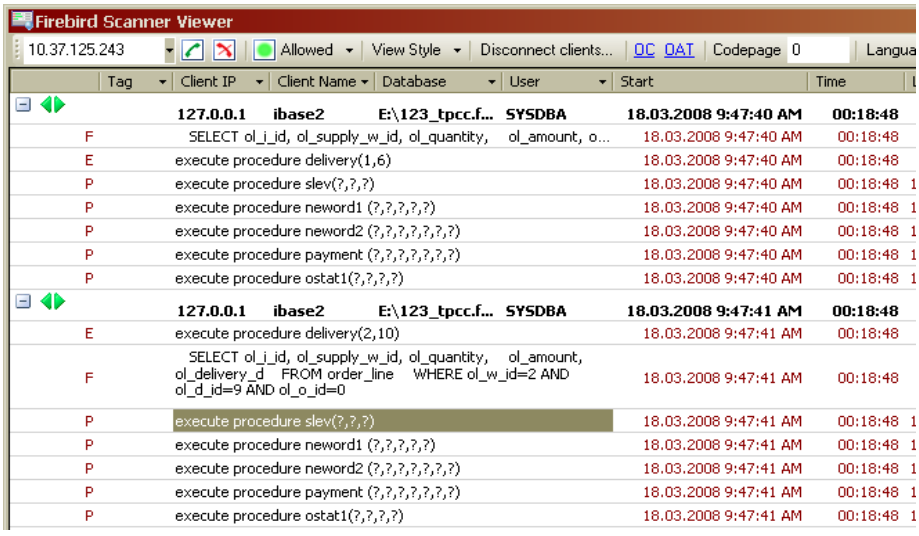
FBScanner(IBSurgeon社)

EMBARCADERO TECHNOLOGIES
DEVELOPER CAMP

- FBScanner (Firebird Scanner) はサーバ(InterBase, Firebird)とクライアント間の全てのトラフィックを見たり、監視したりできるツール。接続されたクライアントのリアルタイムな以下の活動を表示することができる。
  - 接続(IP/Name, 接続時間, CPU 負荷)
  - クエリ(クエリテキスト, 状態, パラメタ)
  - トランザクション (パラメタ)

FBScanner(IBSurgeon社)

EMBARCADERO TECHNOLOGIES
DEVELOPER CAMP



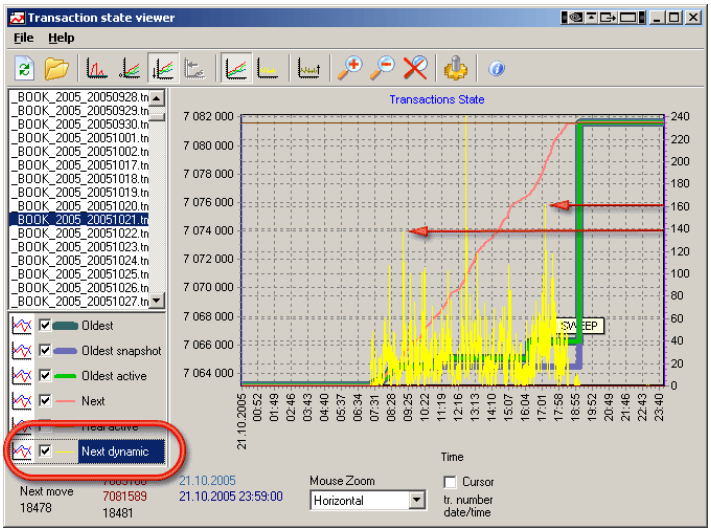
IBTransactionMonitor(IBSurgeon社)

EMBARCADERO TECHNOLOGIES
DEVELOPER CAMP

- IBTransactionMonitor (IBTM)はInterBaseとFirebirdデータベース内の動的なトランザクションを解析したり、閲覧したり、モニターしたりするソフトウエア。
- **IBTMの機能を使って、以下のような実際の問題や潜在的な問題を見つけることができる。**
  - パフォーマンスのボトルネック
  - 製品の実際の負荷
  - 異常終了やクライアントのクラッシュ
  - トランザクションの管理問題
  - データベースのアベイラビリティ.
  - 異なる色々な視点からトランザクションの振る舞いを視覚的に表示

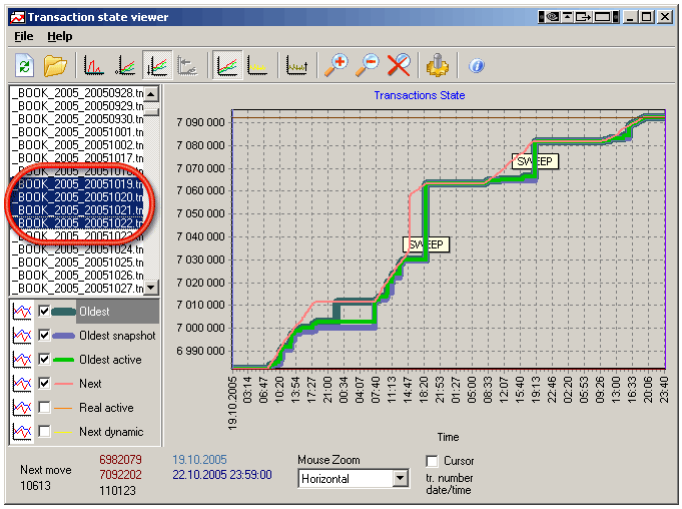
IBTransactionMonitor(IBSurgeon社)

EMBARCADERO TECHNOLOGIES
DEVELOPER CAMP



IBTransactionMonitor(IBSurgeon社)

EMBARCADERO TECHNOLOGIES
DEVELOPER CAMP



サポートツールズ、デモ＆メモ

EMBARCADERO TECHNOLOGIES
DEVELOPER CAMP