【B4】InterBaseテクニカルセッション

「InterBaseセキュリティパワーアップ」

セキュリティ改善のコツとツール

キムラデービー
代表
木村明治(きむらめいじ)
http://kimuradb.com

CODE GEAR FROM Borland
Where Developers Matter
Integrated Development Environments for Windows, Java, and Web Developers
DEVELOPER CAMP

アジェンダ

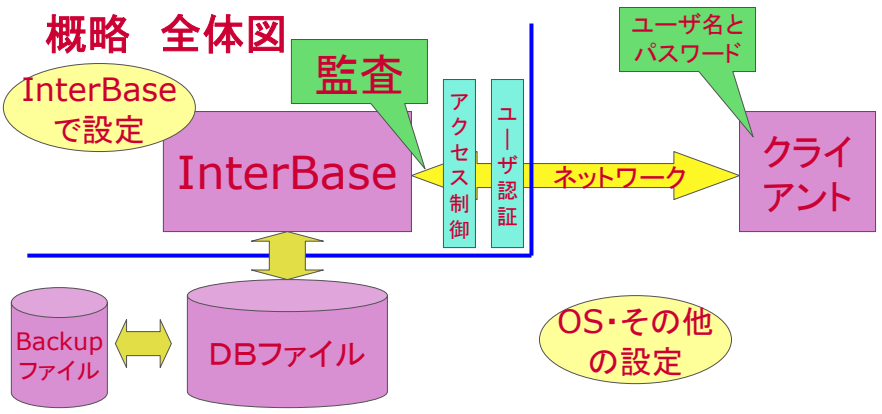
- DBセキュリティとは？
- InterBase本体が持つセキュリティ機能
- 通信経路の暗号化
- 格納データの暗号化

本文書の一部または全部の転載を禁止します。本文書の著作権は、著作者に帰属します。

DBセキュリティとは？

CODE GEAR FROM Borland
Where Developers Matter
Integrated Development Environments for Windows, Java, and Web Developers
DEVELOPER CAMP

概略　全体図



InterBase本体が持つセキュリティ機能

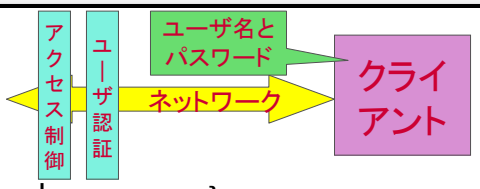
CODE GEAR FROM Borland
Where Developers Matter
Integrated Development Environments for Windows, Java, and Web Developers
DEVELOPER CAMP

基本機能のおさらい

- Grant/Revoke
- User/User Role
- DB alias
- ibconfig

本文書の一部または全部の転載を禁止します。本文書の著作権は、著作者に帰属します。

GRANT文



GRANT *privileges*
ON [TABLE] {*tablename* | *viewname*}
TO {*object*|*userlist* [WITH GRANT OPTION]|GROUP *UNIX_group*}

基本は、WITH GRANTするかどうか。

権限剥奪はREVOKE文で、おこなう。

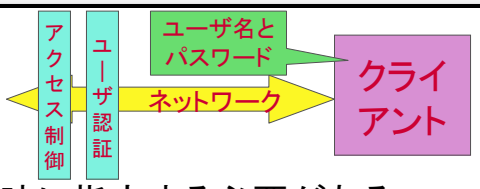
USER ROLE

InterBase 5.xから

USER ROLEの機能があり！

```
CREATE ROLE FULL_ACCESS;
GRANT ALL ON TEST_SCORES TO
  FULL_ACCESS;
GRANT FULL_ACCESS TO BJONES;
```

USER ROLE



ただ、GRANTしただけ

では使えない！→接続時に指定する必要がある。

SQL>connect tempemployee.gdb user bjones password bjones

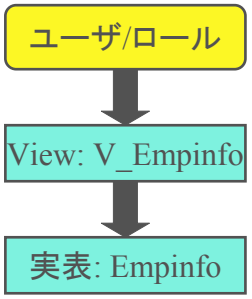
role full_access;

Database: tempemployee.gdb, User: bjones, Role: full_access

Viewを使ったアクセス制限

- 表に直接アクセスさせるのではなく、Viewに必要最小限の情報だけを与える。
  - SELECT文でのカラム
  - WHERE句での条件指定
  - WITH CHECKオプションによる、範囲外へのINSERT, UPDATEの抑止

Viewを使ったアクセス制限

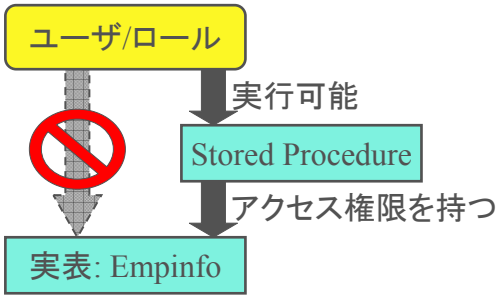


CODE GEAR FROM Borland
Where Developers Matter
Integrated Development Environments for Windows, Java, and Web Developers
DEVELOPER CAMP

SPを使ったアクセス制限

- SP(Stored Procedure)を使う。
- データへのアクセスをSP経由だけにして、アクセス制限を行う。
- Viewに似ているが、さらにフレキシブルなものにできる。
- トリガによる監査はUPDATE/INSERT/DELETEのみになるが、SELECTによる監査も可能になる。

SPを使ったアクセス制限



DB alias

- InterBase 7.5以降で追加。
- Gsecコマンドで、データベースに別名を付けることが出来る。
- 以下のような利点あり
  - 接続文字列にデータベースフルパス指定なしでよい。
  - Unix, Windowsのパス区切りをクライアント側で意識する必要がない。
- http://dn.codegear.com/jp/article/37600

ibconfig

- #EXTERNAL_FILE_DIRECTORY
  - ## If your external files are not in <interbase_home>/ext,
  - ## specify their location here. For security reasons, do not
  - ## put other files in this directory.
- #EXTERNAL_FUNCTION_DIRECTORY
  - ## If your UDF library is not in <interbase_home>/UDF, then specify
  - ## the location of the library here. For security reasons, do not
  - ## put other files in this directory.

CODE GEAR FROM Borland
Where Developers Matter
Integrated Development Environments for Windows, Java, and Web Developers
DEVELOPER CAMP

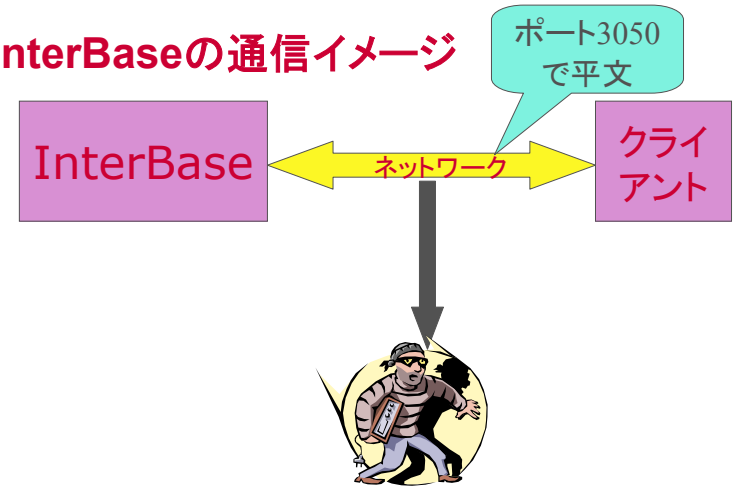
その他のTips

- SYSDBAを使わないようにしよう！
  - データベースをSYSDBA以外のユーザーで作る。
    - 一部ツールなどでは問題が起こる可能性あり。
- パスワードを変更しよう！
  - ‘masterkey’を使わないように。
- クライアントにパスワードを平文で格納しないようにしよう！
  - 付箋でモニターにパスワード張っているのとおなじ。

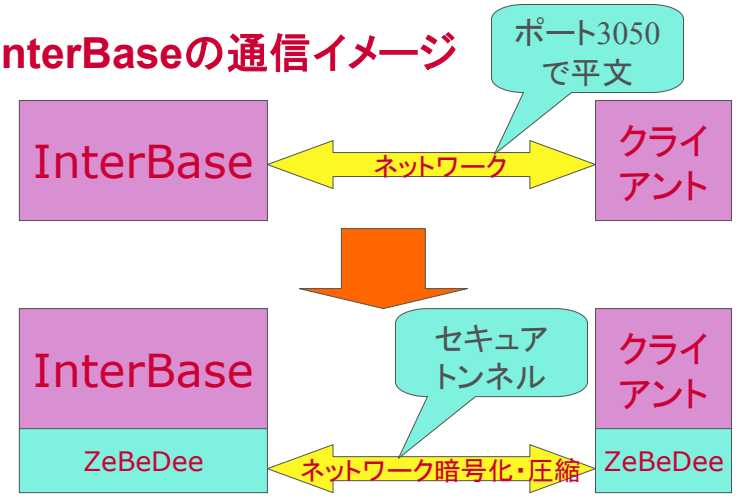
Memo & Demo

通信経路の暗号化

InterBaseの通信イメージ



InterBaseの通信イメージ



通信経路の暗号化

- ZeDeBee
  - http://www.winton.org.uk/zebedee/
  - http://www.linux.or.jp/JM/html/zebedee/zebedee.pod.html
- 暗号化とTCP/IPの圧縮
  - **Z**lib による圧縮
  - **B**lowfish による暗号化
  - **D**iffie-Hellman による認証

CODE GEAR FROM Borland
Where Developers Matter
Integrated Development Environments for Windows, Java, and Web Developers
DEVELOPER CAMP

シンプルな設定

- ZeBeDeeサーバー側
  - Zebedee –s localhost:3050
- クライアント側(kimuradb.comをサーバ名とする)
  - Zebedee 3051:kimuradb.com:3050
- 接続文字列
  - Localhost/3051:データベースパス名(or DB Alias)

複雑な設定 & more…

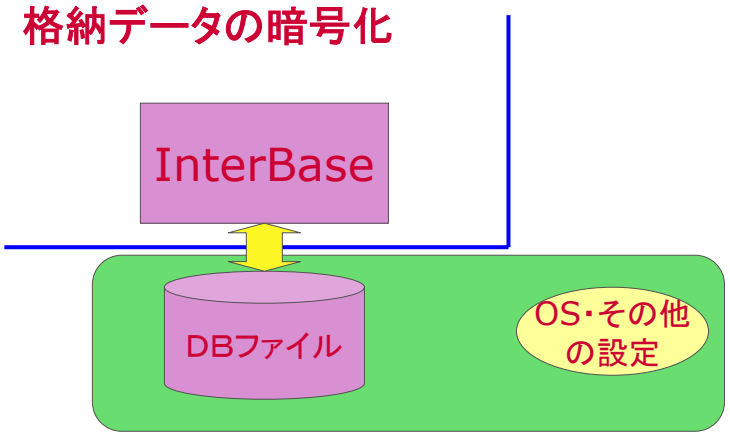
- サーバサイド、クライアントサイドで、設定ファイルを作成。
  - さらに詳細な設定が可能。

CODE GEAR FROM Borland
Where Developers Matter
Integrated Development Environments for Windows, Java, and Web Developers
DEVELOPER CAMP

格納データの暗号化

本文書の一部または全部の転載を禁止します。本文書の著作権は、著作者に帰属します。

格納データの暗号化

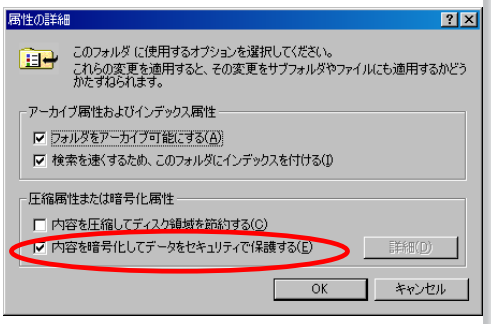


データファイルの暗号化

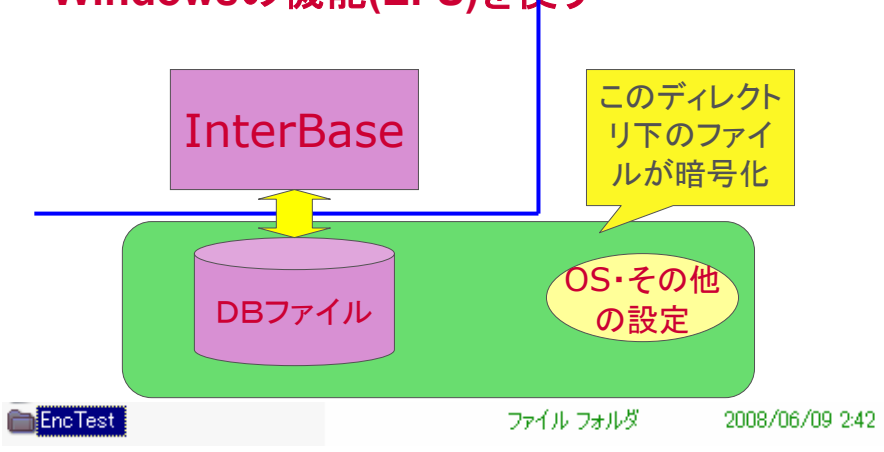
- OS自体の機能
  - Windows:「暗号化によるデータの保護」
  - http://www.microsoft.com/japan/windowsxp/pro/using/howto/security/encryptdata.mspx
- TrueCrypt
  - Windows/Linux/Mac OS X
  - http://www.truecrypt.org/

Windowsの機能(EFS)を使う。

- 暗号化するフォルダを右クリックし、**[プロパティ]** をクリックします。
- **[全般]** タブの **[詳細設定]** をクリックします。
- **[内容を暗号化してデータをセキュリティで保護する]** チェック ボックスをオンにします。

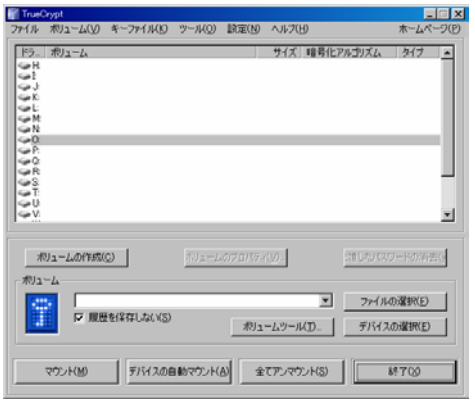


Windowsの機能(EFS)を使う



TrueCryptを使う

•通常のOSファイルをボリュームとして割り当て、マウントするイメージ。

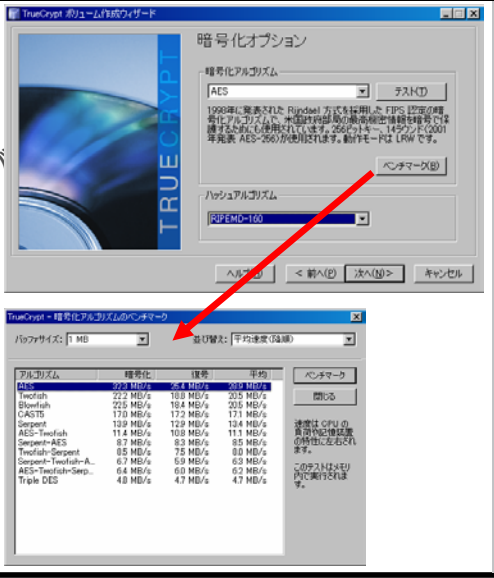


CODE GEAR FROM Borland
Where Developers Matter
Integrated Development Environments for Windows, Java, and Web Developers
DEVELOPER CAMP

TrueCryptを使う

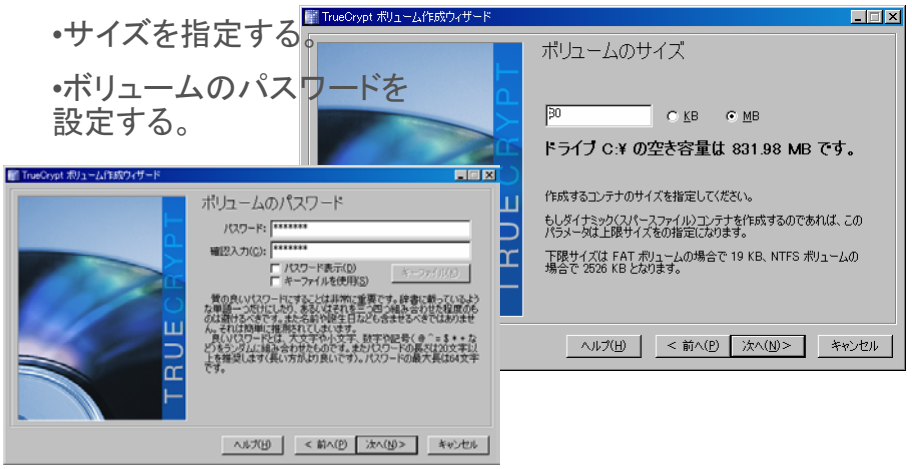
•暗号化やハッシュのアルゴリズムやサイズを選ぶことができる。

•暗号の強度とスピードはトレードオフ。ベンチマークで確認することができる。



TrueCryptを使う

- サイズを指定する。
- ボリュームのパスワードを設定する。



TrueCryptを使う & more...