

# DB2 グローバル マスター 実践講座

DB2  
エンジニア

## 第2回

## DB2のセキュリティ

田中耕一郎 TANAKA, Koichiro



今回は、セキュリティについて解説します。セキュリティに関する問題は、全体的問題数から見ればそれほど多くは出題されませんが、しっかり理解しておくことが合格への近道となります。出題数が少ないからと言って偏った学習をするのではなく、万遍なく学習するように心がけてください。

### はじめに

エンジニア試験では、セキュリティカテゴリからの出題が全出題数の10%を占めています(表1)。エンジニア試験を攻略するためにセキュリティの項で学ばなければならないのは、セキュリティ機能によって何を達成しようとしているのか、また、どのようなメカニズムで行なわれているのかということです。

セキュリティの目的は各データベースによって似ていますが、それを実現する方法はデータベース独自の仕様に依存します。DB2でも特有の語句や方法を使ってこれらの機能が実装されていますので、これらを理解することがセキュリティカテゴリ攻略のカギとなります。

表1: エンジニア試験の出題項目と問題配分

カテゴリ	出題項目	配分
①	計画	15%
②	セキュリティ	10%
③	DB2 UDB データのアクセス	15%
④	DB2 UDB データの使用	30%
⑤	DB2 UDB オブジェクトの使用	20%
⑥	データの同時実行性	10%
	合計	100%

### データベースのセキュリティプラン

DB2が提供するセキュリティプランには、次のようなものが挙げられます。

1. 誰がDB2 インスタンス、あるいはデータベースにアクセスできるか
2. どのようにしてユーザーのパスワードが検証されるか
3. どのユーザーにどの権限レベルを与えるか
4. ユーザーがコマンドを実行する権限を与えるか
5. ユーザーにデータを参照させる権利、あるいは変更する権利を与えるか
6. ユーザーにデータベース・オブジェクトを作成／変更／削除させる権利を与えるか

### DB2のセキュリティメカニズム

DB2は、上の6つのセキュリティプランを達成するため、主に“認証”“権限”“特権”の3つのメカニズムを使用します。

認証は、ユーザーがDB2 インスタンス、あるいはデータベースにアクセスしようとしたときに、ユーザー ID とそれに結び付けられたパスワードで行なわれます。DB2は、この認証を OS や Kerberos のような認証システムによって行ないます。

権限と特権は、DB2のデータベース・オブジェクトにアクセスする権限を規定します。特権が各データベース・オブジェクトに対する権利(例えば、SELECT 特権:ある表に対して SELECT 文を発行する権利)を規定しているのに対し、権限はオブジェクトへのアクセスのほかにハイレベルのインスタンス、あるいはデータベースの管理機能を実行する権利を規定します。Oracleを知っている人なら、DB2の権限はOracleの“システム権限”、DB2の“特権”はOracleの“オブジェクト権限”と似ていると思うかもしれません。

### 認証

#### 認証タイプ

認証タイプ (Authentication Type) には、5つのタイプがあります(表2)。

#### 認証タイプのセット

表2の5つの認証タイプを、それぞれサーバー／クライアント双方にセットすることで、どちらで認証が行なわれるのかを決定できます。サーバーで認証タイプを設定するには次のコマンドを使用し、データベース・マ

ネージャ構成ファイルを更新します。

```
db2 update dbm cfg using authentication =>
SERVER_ENCRYPT
```

また、クライアントで認証タイプを指定するには、次のコマンドを使用します。

```
db2 catalog database [データベース名] at =>
node [ノード] authentication
SERVER_ENCRYPT
```

catalog コマンドは次回以降に説明します。ここでは、「クライアントからサーバーのデータベースに接続する際に必要なコマンド」と覚えておいてください。

## CLIENT 認証時の注意点

サーバーの認証タイプがCLIENT にセットされている場合でも、認証がサーバー側で行なわれる場合があります。DB2では、認証システムを持っていないようなクライアントOS (Windows 98やWindows Meなど) は信頼できないクライアントと定義します。逆にOS自体が認証システムを持っている場合には、信頼できるクライアントと定義します。

これらを制御するために、TRUST\_ALLCLNTS パラメータと TRUST\_CLNTAUTH パラメータが認証を行なう場所を決定します。

### ● TRUST\_ALLCLNTS

このパラメータは、クライアント側で認証できるかどうかを規定します。次の値を取ります。

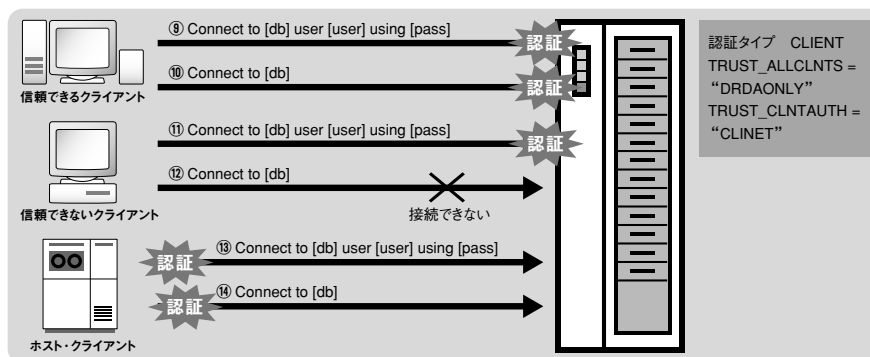
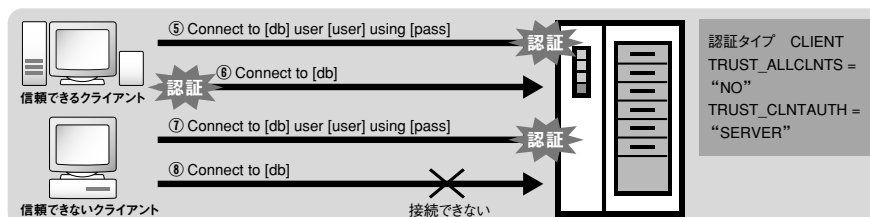
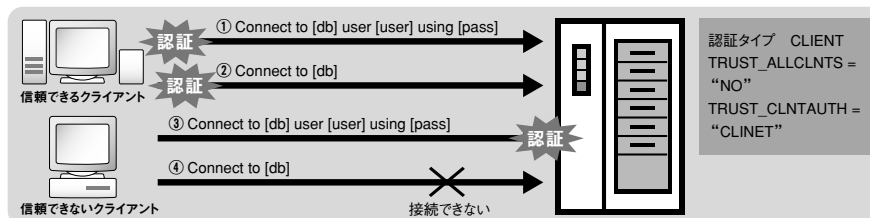


図1：組み合わせるタイプによって、認証される場所が異なる

**YES**：クライアントが信頼できる、できないにかかわらず、すべての認証はクライアント側で行なわれる

**NO**：信頼されないクライアントはすべて、サーバー側で認証される

**DRDAONLY**：クライアントOSが、MVS、OS/390、VM、VSE、OS/400などのホスト系クライアントの場合のみ、クライアント側で認証される

### ● TRUST\_CLNTAUTH

このパラメータは、ATTACH コマンドあるいはCONNECT コマンドを発行する際にユーザーIDとパスワードを指定した場合に、認証がどこで行なわれるかを規定します。次の値を取ります。

**CLIENT**：認証はクライアント側で行なわれる

**SERVER**：認証はサーバー側で行なわれる

それぞれの認証タイプで、認証がどこで行なわれるのかを理解するのは面倒だと思うかも知れません。特に認証タイプがCLIENT にセットされている場合は、クライアントのタイプ、TRUST\_ALLCLNTS、TRUST\_CLNTAUTH の設定にも影響されるので、より複雑になります。そこで、図1に、それぞれを組み

表2：5つの認証タイプ

認証タイプ ※1	説明
SERVER	認証はサーバー側で行なわれる
SERVER_ENCRYPT	認証はサーバー側で行なわれる。パスワードはクライアント側で暗号化され、サーバー側に送られる
CLIENT	認証はクライアント側で行なわれる
KERBEROS ※2	KERBEROS 認証システムによって行なわれる
KRB_SERVER_ENCRYPT	クライアントがKERBEROS を利用できるようにすればKERBEROS 認証を使用する。そうでない場合は、SERVER_ENCRYPT が使用される

※1 V7 でサポートされていた DCE と DCE\_SERVER\_ENCRYPT の認証タイプは V8 ではサポートしない。認証システムとしては将来的に有望な KERBEROS のみをサポートする

※2 KERBEROS とは、MIT (マサチューセッツ工科大学) で開発された認証システム。この認証タイプを利用できるのは、サーバーとクライアントが Windows 2000 のときのみ (将来的には、KERBEROS が使用できる UNIX ファミリーの OS でもサポート)

合わせて使用した時にどこで認証が行なわれるのかを図示しました。

すべてのケースを網羅しているわけではありませんが、それぞれのケースでなぜそこ(クライアント/サーバー)で認証が行なわれるのかを考えてみてください。もし、よく分からない場合は前述の説明をもう一度読み直してください。

さて、ここまで認証タイプについて説明してきましたが、実はグローバルマスター試験の観点からはあまり重要ではありません。というのも、セキュリティのカテゴリから出題される問題数は5問程度で、次に説明する権限と特権から多くが出題される傾向が強いからです。

#### 【例題】

ユーザーIDとパスワードが検査されないのはどこですか？

- [A] DB2
- [B] クライアントアプリケーションが実行されている Windows 2000
- [C] サーバー側の OS
- [D] KERBEROS 認証システム

解答：A

#### 【解説】

DB2では、OSの認証機能を利用してユーザー認証を行ないます。DB2自体では認証を行ないません。

#### 【例題】

認証タイプとして間違っているものは次のうちどれですか？

- [A] SERVER\_ENCRYPT
- [B] KERBEROS
- [C] CLIENT
- [D] DCE

解答：D

#### 【解説】

分散環境で使用される認証プロトコルである DCE (Distributed Computing Environment) は、DB2 V8からサポートされなくなりました。

#### 【例題】

Windows 2000 で稼動している DB2 サーバー側のパラメーターが以下のとき、Windows Me から CLP (コマンドラインプロセッサ) を起動し、次のコマンドを発行しました。

##### パラメーター

```
DB2 CONNECT TO MYDB USER MYUSER USING MYPASS
```

##### コマンド

```
AUTHENTICATION = CLIENT  
TRUST_ALLCLNTS = NO  
TRUST_CLNTAUTH = CLIENT
```

この場合、認証はどこで行なわれるでしょう？

- [A] サーバー側
- [B] KERBEROS 認証システム
- [C] クライアント側
- [D] 接続は拒否される

解答：A

#### 【解説】

コマンドでは、TRUST\_ALLCLNTS=NO に設定されているので、Windows 98や Windows Meのような「信頼されないクライアント」はすべてサーバー側で認証が行なわれます。

## 権限

DB2の権限とは、データベース特権、オブジェクト特権のセットと、データベース管理のためのハイレベルな操作をする権利をまとめたもので、全部で5つのタイプがあります。権限と特権は階層的な構造をしています(図2)。

#### 権限タイプ

##### ● SYSADM (システム管理権限)

DB2に対するすべての特権が与えられます。ユーティリティの実行、データベース・コマンド/データベース・マネージャー・コマンドを実行できます。また、全データへのアクセスが可能です。

##### ● SYSCTRL (システム制御権限)

インスタンスレベルあるいはデータベース・レベルでのすべての管理コマンドを実行できます。データベース内のデータにはアクセスできません。

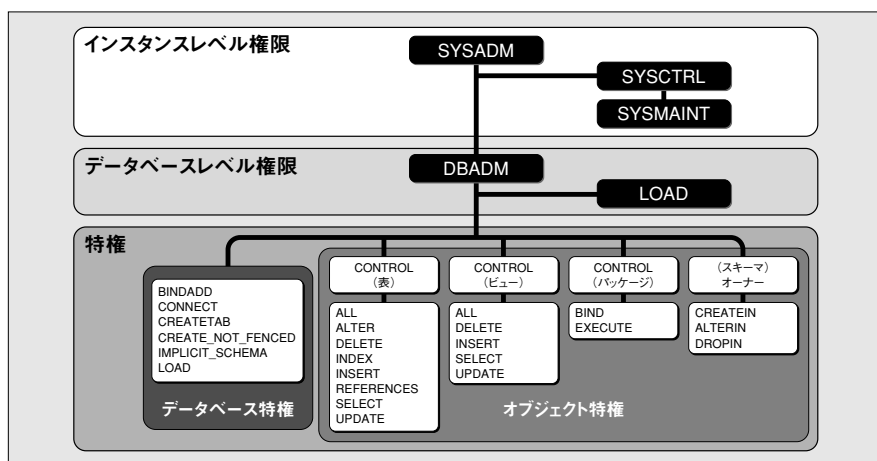


図2：DB2の5つの権限タイプ

### ● SYSMANT (システム保守権限)

システムをメンテナンスするために SYSCRTL のサブセット機能が提供されます。

### ● DBADM (データベース管理権限)

データベースを制御するための特権が与えられます。データベース・レベルでのほとんどのタスクが許されますが、データベースの削除、バックアップ／リストア、データベース構成ファイルの更新などは例外です。また、SYSCRTL や SYSMANT と違い、データベース内のすべてのデータにアクセスできます。

### ● LOAD

データを表にロードできます。それ以外にも、RUNSTATS コマンド (統計情報を更新するコマンド)、QUIESCE コマンド (表スペースを一時停止するコマンド)、LIST TABLESPACE コマンドを実行できます。LOAD INSERT コマンドを実行するときは、LOAD 権限のほか INSERT 特権を持っている必要があります。LOAD REPLACE コマンドを実行するときは、LOAD 権限のほか INSERT、DELETE 特権を持っている必要があります。

表 3 は、SYSADM、SYSCRTL、SYSMAINT、DBADM のそれぞれの権限で実行できるタスクの一覧です。

#### 【例題】

次の権限のうち、データベース内の表を参照できる特権を持つのはどれですか (2つ選択)?

- [A] SYSMANT
- [B] SYSCRTL
- [C] SYSADM
- [D] DBADM

解答: C、D

#### 【解説】

データベース内のデータにアクセスできるのは、SYSADM と DBADM です。SYSCRTL と SYSMANT は、システム管理に必要な特権セットが与えられます。

#### 【例題】

次の権限のうち、インスタンスを起動／停止できない権限はどれでしょう?

- [A] SYSMANT
- [B] SYSCRTL

表 3: 権限タイプ別実行可能タスクの一覧

	SYSADM	SYSCRTL	SYSMAINT	DBADM
データベース構成ファイルの更新	○			
DBADM 権限の授与／取消	○			
ユーザーの強制ログオフ	○	○		
データベースの作成／削除	○	○		
新しいデータベースへの復元	○	○		
データベース構成ファイルの更新	○	○	○	
データベース／表スペースのバックアップ	○	○	○	
既存のデータベースへの復元	○	○	○	
ロールフォワード回復の実行	○	○	○	
インスタンスの開始／停止	○	○	○	
表スペースの復元	○	○	○	
トレースの実行	○	○	○	
モニタースナップショットの取得	○	○	○	
表スペースの状態の問い合わせ	○	○	○	○
ログ履歴ファイルの更新	○	○	○	○
表スペースの静止	○	○	○	○
表へのロード	○			○
イベントモニターの作成／削除	○			○
CHECK PENDING 状態のセット／アンセット	○			○

- [C] SYSADM
- [D] DBADM

解答: D

#### 【解説】

DBADM は、個別のデータベースにアクセスし、制御するための特権セットが与えられます。インスタンスレベルの操作は許されていません。

#### 【例題】

LOAD 権限を持つユーザーが実行できないコマンドは次のうちどれですか?

- [A] RUNSTATS の実行
- [B] INSERT 特権を持っている表への LOAD INSERT の実行
- [C] INSERT 特権を持っている表への LOAD REPLACE の実行
- [D] QUIESCE TABLESPACE FOR TABLE の実行

解答: C

#### 【解説】

LOAD REPLACE を実行するには、LOAD 権限のほか該当の表に対する INSERT 特権と DELETE 特権が必要です。

RUNSTATS も QUIESCE TABLESPACE FOR TABLE も、LOAD 権限の付与に際して暗黙的に与えられる特権です。

### 特権

特権とは、あるデータベースオブジェクトを作成したり、オブジェクトにアクセスするための権利です。特権は大きく2つのカテゴリに分けられます。1つはデータベース特権で、もう1つはオブジェクト特権です。

#### データベース特権

データベース特権は、例えばテーブルを作成したり、データベースに接続したりとい

ったデータベース・レベルの特権を規定します。表4に、データベース特権の名称と内容を示します。

### オブジェクト特権

オブジェクト特権は、個々のオブジェクトを操作するのに必要な権利を規定します。それぞれの特権の名称と、対象となるオブジェクト、説明を表5に示します。

### 明示的な特権の付与

データベース特権およびオブジェクト特権は、明示的にも暗黙的にも与えることができます。明示的に特権を与えるには(または剥奪するには)、次のようにGRANT/REVOKEコマンドを使用します。

#### ・特権を与える場合

```
GRANT [特権名] ON [オブジェクトの種類] ⇒  
[オブジェクト名] TO [USER or GROUP or ⇒  
PUBLIC] [ユーザー名 or グループID]
```

#### ・特権を剥奪する場合

```
REVOKE [特権名] ON [オブジェクトの種類] ⇒  
[オブジェクト名] FROM [USER or GROUP or ⇒  
PUBLIC] [ユーザー名 or グループID]
```

例えば、SYSADM権限を持つDBAがユーザー“TARO”の“ABC”表をユーザー“JIRO”にも参照可能にさせたい場合は、次のGRANTコマンドを発行することで実現できます。

```
GRANT SELECT ON TABLE TARO.ABC TO USER JIRO
```

WITH GRANT OPTIONを付加することによって、JIROは他人にABC表を参照させるためのGRANTコマンドを発行できます。

```
GRANT SELECT ON TABLE TARO.ABC TO USER ⇒  
JIRO WITH GRANT OPTION
```

JIROからABC表を参照する権利を剥奪するには、次のREVOKEコマンドを発行します。

```
REVOKE SELECT ON TABLE TARO.ABC FROM ⇒  
USER JIRO
```

表4：データベース特権の一覧

データベース特権	説明
CREATETAB	データベース内に表を作成できる
BINDADD	BIND コマンドを使用して、データベース内にパッケージを作成できる。パッケージとは、静的 SQL を事前にコンパイルすることによってデータベース内に作成される、SQL を実行するのに必要なアクセスプランなどの情報のこと
CREATE_NOT_FENCED	非分離 (NOT FENCED) ユーザー定義関数 (UDF) またはプロシージャを作成できる。非分離 (NOT FENCED) ユーザー定義関数 (UDF) とは、データベース・プロセス内で実行される UDF のこと
IMPLICIT_SCHEMA	存在していないスキーマ名を指定した CREATE ステートメントを使用してオブジェクトを作成することによって、暗黙にスキーマを作成できる。SYSIBM が暗黙に作成されたスキーマの所有者になる
LOAD	表にデータをロードできる
QUIESCE_CONNECT	データベースが静止状態にあるときに、データベースにアクセスできる
CREATE_EXTERNAL_ROUTINE	アプリケーションや他のユーザーによって使用できるプロシージャや UDF を作成できる

表5：オブジェクト特権の一覧

オブジェクト特権の名称	対象となるオブジェクト	説明
CONTROL	表、ビュー、索引、パッケージ、エイリアス、UDF、シーケンスなど	所有者特権。対象となるオブジェクトを作成したユーザーに自動的に与えられる特権。オブジェクトに対して、すべての操作が可能。また、GRANT あるいは REVOKE ステートメントによって他のユーザーにオブジェクトの特権を与えたり、取り消したりできる
DELETE	表、ビュー	DELETE ステートメントを発行できる
INSERT	表、ビュー	INSERT ステートメントを発行できる
SELECT	表、ビュー	SELECT ステートメントを発行できる
UPDATE	表、ビュー	UPDATE ステートメントを発行できる
ALTER	表	ALTER TABLE ステートメントを使用して、表の定義を変更できる
INDEX	表	CREATE INDEX ステートメントを使用して、表内に索引を作成できる
REFERENCES	表	従属表を作成する際に、親表のある列をキーとして定義できる。B 表を作成する際に、A 表のあるキーを親キーとして定義するには、ユーザーは A 表の REFERENCES 特権を持つ必要がある
BIND	パッケージ	REBIND コマンドにより、既存のパッケージを再作成するときに必要。データベース特権の BINDADD 特権と混同しないように
ALTERIN	スキーマ	スキーマ内のオブジェクトに対して、ALTER ステートメントを発行して、オブジェクトの定義を変更できる。注意点として、ALTER ステートメントを実行するには、スキーマに対する ALTERIN 特権と該当オブジェクトに対する ALTER 特権が必要
CREATEIN	スキーマ	スキーマ内にオブジェクトを作成できる。表を作成するためにはこの特権のほかに CREATETAB データベース特権が必要となる
DROPIN	スキーマ	スキーマ内のオブジェクトをドロップできる

### 暗黙的な特権の付与

オブジェクトを作成したときや、権限あるいは表のCONTROL特権など高度な権限／特権を与えられたときは、それに伴って関連する特権が自動的に付与される場合があります。これらの特権は「暗黙的な特権」と呼ばれます。例えば、次のような場合があります。

・CREATE TABLE を実行したときに、その表に対するCONTROL特権が作成したユーザーに与えられる

・CREATE DATABASE を実行したときに、すべてのユーザー(PUBLIC)にBINDADD、CONNECT、CREATETAB、IMPLICIT\_SCHEMAなどの特権が与えられる

・あるユーザーにDBADM権限を付与すると、自動的にBINDADD、CONNECT、CREATETAB、CREATE\_NOT\_FENCED、IMPLICIT\_SCHEMA、LOADの特権が自動的に与えられる。もしDBADM権限を剥奪されたとしても、これらの特権は残る



### 【例題】

表 EMPLOYEE には次のような列があります。

```
NAME VARCHAR(32)
DEPARTMENT VARCHAR(64)
PHONE_NUMBER VARCHAR(16)
```

ユーザー“TARO”に DEPARTMENT 列だけ参照を許可するには、どうしたらよいでしょうか？

- [A] DEPARTMENT 列だけのビューを作成し、TARO に作成したビューの SELECT 特権を与える
- [B] GRANT SELECT (DEPARTMENT) ON TABLE employee TO user1
- [C] GRANT UPDATE (DEPARTMENT) ON TABLE employee TO user1
- [D] GRANT REFERENCES (DEPARTMENT) ON TABLE employee TO user1

解答: A

### 【解説】

B の SELECT 特権は、列単位では付与できません。D の REFERENCES 特権は、従属表が親表の列をキーとして参照する際に必要です。

### 【例題】

USER1 が、自分の所有する表“TAB1”の UPDATE 特権を USER2 に次の GRANT 文で与えました。

```
GRANT UPDATE ON TABLE USER1.TAB1 TO
USER USER2 WITH GRANT OPTION
```

USER2 は、“USER1.TAB1”の UPDATE 特権を USER3 に次の GRANT 文で与えました。

```
GRANT UPDATE ON TABLE USER1.TAB1 TO
USER USER3
```

USER1 が、USER2 から“TAB1”の UPDATE 特権を次の REVOKE 文を使って取り上げました。

```
REVOKE UPDATE ON TABLE USER1.TAB1
FROM USER USER2
```

この結果として、次の説明のうち正しいものを選んでください。

- [A] USER2 の UPDATE 特権が取り消されたので、USER3 の特権も取り消された
- [B] USER2 の UPDATE 特権が取り消されても、USER3 の特権は取り消されない
- [C] 問題文の REVOKE 文は失敗する
- [D] WITH GRANT OPTION はサポートされていない

解答: B

### 【解説】

WITH GRANT OPTION によってユーザーが与えられた特権は、たとえ特権を与えてくれたユーザーが取り消しても波及して取り消されることはありません。

### おわりに

さて、今回はセキュリティのカテゴリについて解説しましたが、いかがでしたでしょうか？ 覚えることがたくさんありすぎて大変だと感じたかもしれません。もしそう感じたなら、認証はしばし置いておき、とりあえず権限の種類(5つの権限タイプ)と特権の種類をしっかり覚えてください。

それでも、権限タイプによって実行できるタスク、できないタスクに関してすべてを暗記するのは大変な労力がかかりますので、まずはそれぞれのタイプの特徴を理解しましょう。そうすれば、特権についても自然と分かってくるはずです。頑張って学習していきましょう。

今回は「DB2 UDB データのアクセス」について解説します。

DBM

田中耕一郎 (たなかこういちろう)

たがわ製作所 技術主任。DB2、Oracle などの商用 RDBMS に精通したデータベースプログラマー。週末のバスフィッシングのために、平日身を粉にして働く。

## 日本アイ・ビー・エム より おトクなお知らせ

# DB2 グローバルマスター 1万人達成記念 スキルアップ・キャンペーン 実施中!

【期間】 2003年5月1日～12月20日まで

【対象】 DB2 アドバイザー資格保有者  
および DB2 エンジニア資格保有者

DB2 技術者の需要拡大に伴い、おかげさまで、昨年1年間で1万人以上の方が DB2 グローバルマスターの資格を取得され、その数は約1万2000名となりました。今年度は1万人達成記念として、上位資格の取得を目指す「DB2 アドバイザー」「DB2 エンジニア」の有資格者を対象に、スキルアップ・キャンペーンを実施しています。ぜひこの機会に上位資格を取得して、DB2 の知識をより深めていただくと同時に、データベースの世界において活躍の場を広げてください!

スキルアップ・キャンペーン

内容  
A

【対象】 DB2 アドバイザー資格保有者

### DB2 エンジニア取得支援

(2003年5月1日～9月30日まで)

- 試験対策セミナーと試験割引バウチャーをキャンペーン価格でご提供
- セミナー参加者、先着100名に  
翔泳社「iStudy (DB2 エンジニア模擬試験 CD-ROM)」(定価15,000円)をご提供
- エンジニア合格者には  
特製 DB2 グローバルマスターグッズ  
プレゼント(後日郵送いたします)

書籍『IBM 教科書 DB2 エンジニア』(翔泳社)を Web からご購入の方に、DB2 エンジニア認定試験割引バウチャーをご提供

14,000円 ⇒ 10,000円 (税別)

スキルアップ・キャンペーン

内容  
B

【対象】 DB2 エンジニア資格保有者

### DB2 エキスパート取得支援

(2003年5月1日～12月20日まで)

- 試験対策セミナーと試験割引バウチャーをキャンペーン価格でご提供
- セミナー参加者、先着100名に  
翔泳社「iStudy (DB2 エキスパート模擬試験 CD-ROM)」(定価15,000円)をご提供

キャンペーンの詳細はこちらをご覧ください。

[ibm.com/jp/software/data/db2gm](http://ibm.com/jp/software/data/db2gm)

DB2 グローバルマスターに関するお問い合わせ

E-mail: [db2gm@jp.ibm.com](mailto:db2gm@jp.ibm.com)