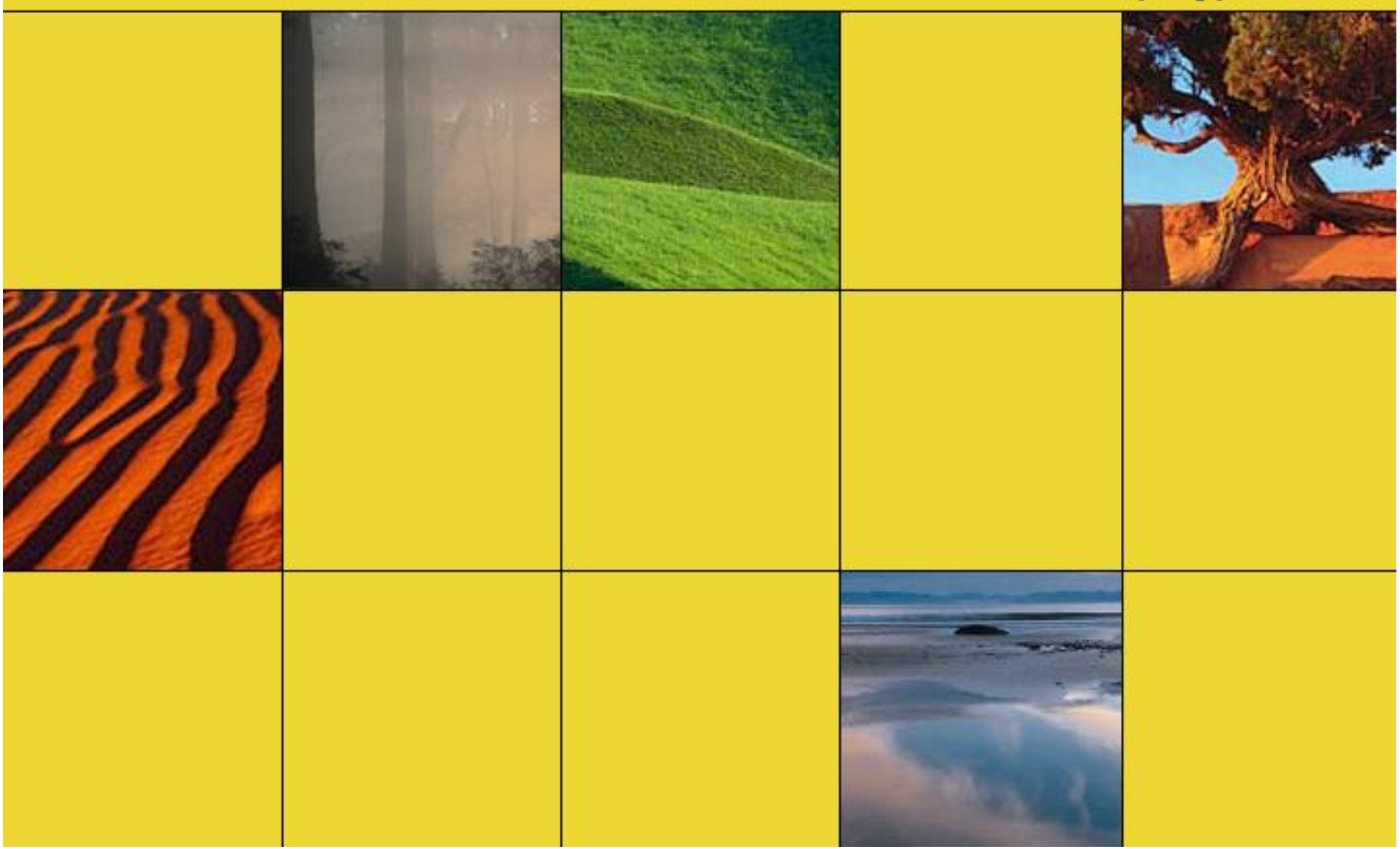
第四堂 預存程序

聯成電腦
張明泰 mtchang.tw@gmail.com



SQL的製作

- 在執行程式時產生的SQL稱為動態SQL，通常有SQL inject的問題。

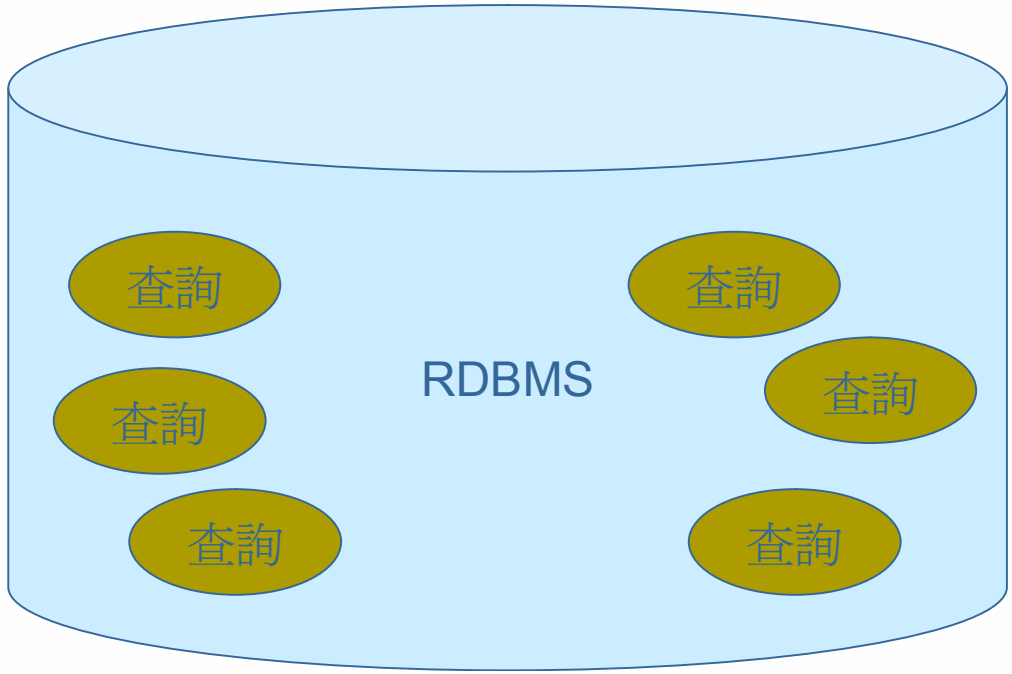
  Select * from students where 姓名="<?php …. ?>";

- 不會變化的SQL稱為靜態SQL。

  Select * from students where 姓名="張小明";

預存程序

- 預存程序：將相關的查詢放在一起，只要命令一次即可使用
- 優：減少網路流量、處理速度較快
- 缺：撰寫麻煩、應用不方便

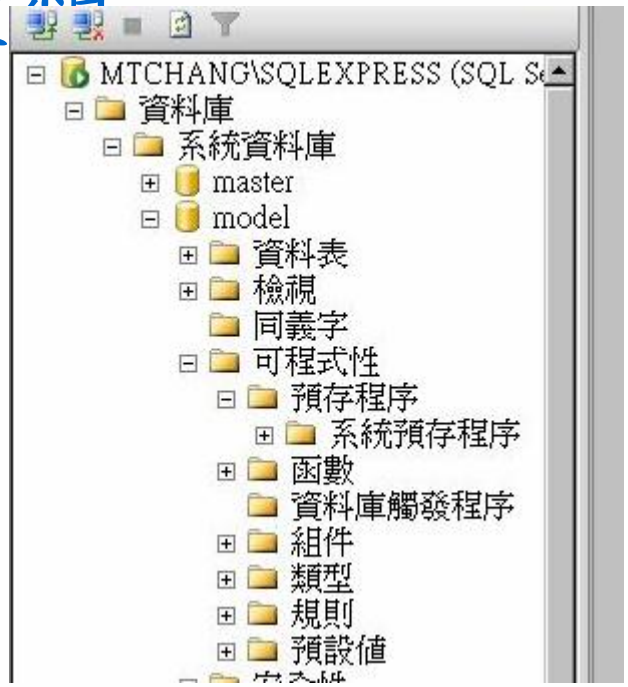


擴充SQL

- 擴充SQL是使用SQL來進行程式設計，擴充SQL是程式語言的一種，因此也可以進行引數的指定和流程控制。
- 擴充SQL也可以在預存程式中使用，只要把使用擴充SQL的製作出來的一連串程式當成預存程序儲存起來，就可以只用一個查詢指令完成很複雜的操作。
- 不同的RDBMS使用的擴充SQL就會不同。Oracle是PL/SQL。MS-SQL是使用Transact-SQL。

MSSQL2005預存程序的種類

- 系統預存程序
- 觸發程序
- 一般預存程序
- 擴充預存程序
  (系統資料庫才有，且分版本)



你的第一個StoreProcedure

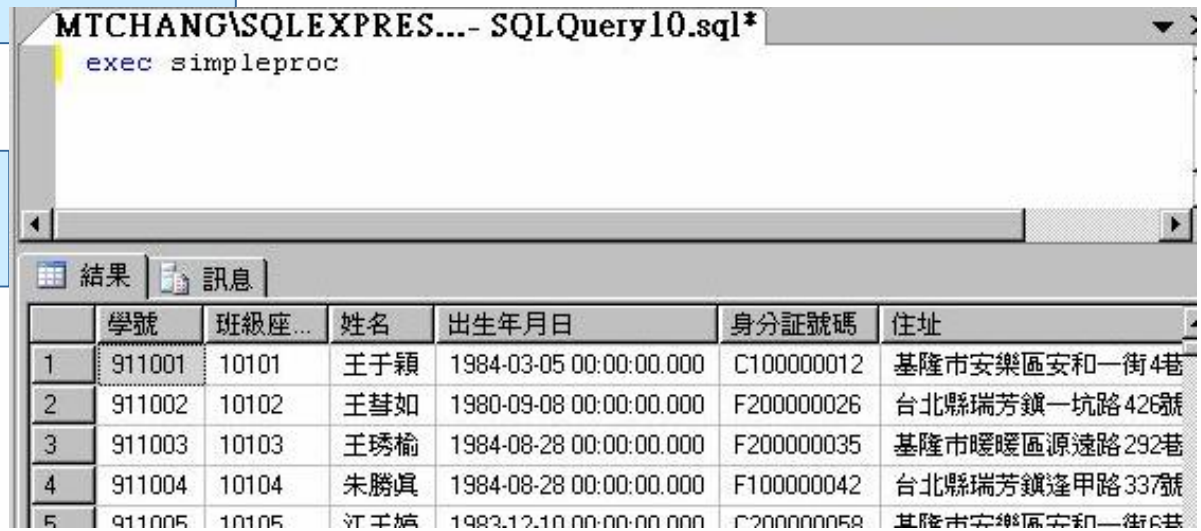
建立procedure

```
CREATE PROCEDURE simpleproc
AS
BEGIN
        SELECT * From students
END
```

Create procedure 爲建立預存程序
Simpleproc() 爲程序名稱
AS之後爲SQL敘述
Begin及end 爲程式的區段範圍
exec 爲呼叫預存程序執行

執行storeProcedure

```
exec simpleproc
```



	學號	班級座...	姓名	出生年月日	身分証號碼	住址
1	911001	10101	王于穎	1984-03-05 00:00:00.000	C100000012	基隆市安樂區安和一街4巷
2	911002	10102	王彗如	1980-09-08 00:00:00.000	F200000026	台北縣瑞芳鎮一坑路426號
3	911003	10103	王琇榆	1984-08-28 00:00:00.000	F200000035	基隆市暖暖區源遠路292巷
4	911004	10104	朱勝眞	1984-08-28 00:00:00.000	F100000042	台北縣瑞芳鎮逢甲路337號
5	911005	10105	江于婷	1983-12-10 00:00:00.000	C200000058	基隆市安樂區安和一街6巷

以內建樣本改出來的程式

```
-- ============================================
-- 這是SQL預存程序的樣本檔，你可以將他存成.SQL的檔案
-- Create Procedure (New Menu).SQL
--
-- Use the Specify Values for Template Parameters
-- command (Ctrl-Shift-M) to fill in the parameter
-- values below.
--
-- This block of comments will not be included in
-- the definition of the procedure.
-- ============================================
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
-- =============================================
-- Author:     <作者mtchang>
-- Create date: <2007.02.08>
-- Description: <測試SQL>
-- =============================================
CREATE PROCEDURE simpleproc
  -- 可設定變數或是引數
  -- <@Param1, sysname, @p1> <Datatype_For_Param1, , int> = <Default_Value_For_Param1, , 0>,
  -- <@Param2, sysname, @p2> <Datatype_For_Param2, , int> = <Default_Value_For_Param2, , 0>
AS
BEGIN
  -- SET NOCOUNT ON added to prevent extra result sets from
  -- interfering with SELECT statements.
  SET NOCOUNT ON;

    -- 這句才是真正的SQL敘述
  SELECT * From students
END
GO
```

帶有參數的StoreProcedure

格式：

```
CREATE PROCEDURE 程序名稱
<參數名稱 資料型態>
AS
BEGIN
   declare 宣告變數  資料型態
   set  變數運算
   SQL敘述
END
```

建立**procedure**

```
CREATE PROCEDURE simpleproc2
  @address varchar(20)
as
begin
  declare @tname varchar(20)
  set @tname= @address+'%'
  select * from students where 住址like @tname
end
```

執行結果

```
exec simpleproc2 '基'
```

結果 | 訊息

	學號	班級座...	姓名	出生年月日	身分証號碼	住址
1	911001	10101	王于穎	1984-03-05 00:00:00.000	C100000012	基隆市安樂
2	911003	10103	王琇榆	1984-08-28 00:00:00.000	F200000035	基隆市暖暖
3	911005	10105	江玉婷	1983-12-10 00:00:00.000	C200000058	基隆市安樂
4	911006	10106	余家男	1983-12-16 00:00:00.000	C100000067	基隆市七堵

執行storeProcedure

```
exec simpleproc2 '基'
```

修改程序

```
ALTER PROCEDURE [dbo].[simpleproc2]
  @address varchar(20)
as
begin
  declare @tname varchar(20)
  set @tname= @address+'%'
  select * from students where 住址like @tname
end
```

最快的方式：

刪除及修改預存程序

可以使用alter修改，drop刪除
ALTER PROCEDURE
DROP PROCEDURE

範例：**DROP PROCEDURE** simpleproc
說明：刪除simpleproc此程序

程式執行過程中看變數(debug)

```
ALTER PROCEDURE [dbo].[simpleproc2]
  @address varchar(20)
as
begin
  declare @tname varchar(20)
  set @tname= @address+'%'
  select @tname as 查詢字串 -- 加入這行看過程的變數
  select * from students where 住址like @tname
end
```

也可以使用PRINT指令：
Print @tname
但print的內容會出現在訊息

撰寫程式注意

- 不可以使用Creat default/trigger/procedure/view/rule在程式中的任何位置
- 程式如果很複雜時，需注意變數的有效範圍。
- 其餘關係到程式的效能及安全性問題，屬於SQL設計後期需調整的問題。

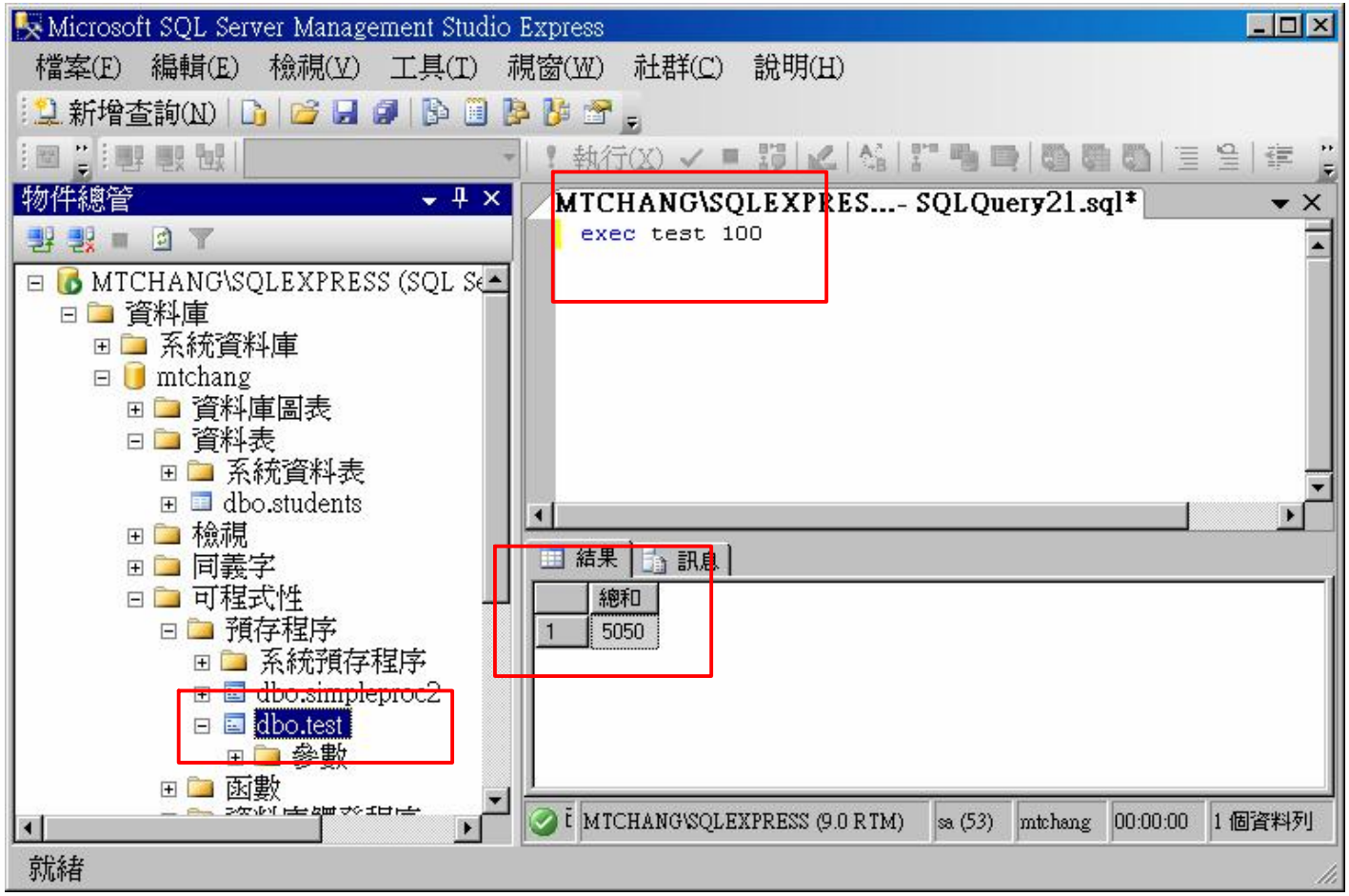
預存程序的編譯

- 這是create procedure選用功能
- With Recompile：每次執行時重新編譯
  這裡指的是cache要不要清除重編
- With Encryption：預存程序內容加密

練習：

- 題目：請建立一個名為test的預存程序，此程序用途為輸入一個數值n就可以算出1,2,3….+n的總和。例如：使用者只需下call test(100)；此指令，即會傳回5050的數值。
- Ps.請直接使用公式計算
  sum=(前+後)*總數/2

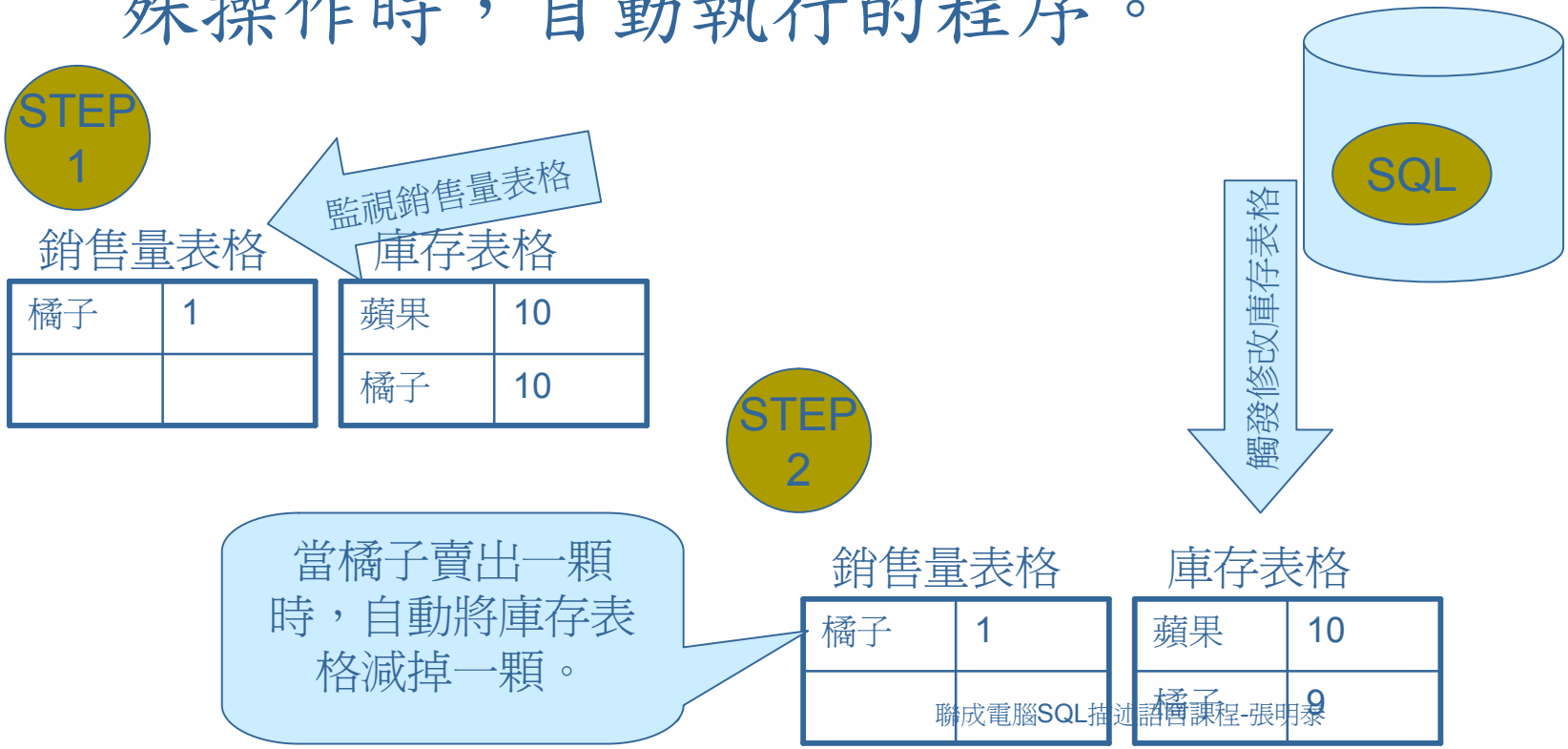
練習執行結果


Microsoft SQL Server Management Studio Express
檔案(F) 編輯(E) 檢視(V) 工具(T) 視窗(W) 社群(C) 說明(H)
新增查詢(N)
執行(X)
物件總管
MTCHANG\SQLEXPRESS (SQL Se
資料庫
系統資料庫
mtchang
資料庫圖表
資料表
系統資料表
dbo.students
檢視
同義字
可程式性
預存程序
系統預存程序
dbo.simpleproc2
dbo.test
參數
函數
MTCHANG\SQLEXPRES...- SQLQuery21.sql*
exec test 100
結果
訊息
總和
1
5050
MTCHANG\SQLEXPRESS (9.0 RTM)
sa (53)
mtchang
00:00:00
1 個資料列
就緒

休息一下

觸發

- 指的是在表格被insert,update,delete等等作特殊操作時，自動執行的程序。



Triggers觸發

語法：

```
CREATE TRIGGER trigger_name
ON { table | view }
{ FOR | AFTER | INSTEAD OF }
{ [ INSERT ] [ , ] [ UPDATE ] [ , ] [ DELETE ] }

AS { sql_statement  [ ; ] [ ,...n ] | EXTERNAL NAME <method
specifier [ ; ] > }
```

詳細請參考MSDN網站

http://msdn2.microsoft.com/zh-tw/library/ms189799.aspx

建立觸發

建立觸發：

```
CREATE TRIGGER test_tri
ON students   FOR INSERT    AS
  BEGIN
    insert into students2 (學號) values ('111111')
  END
```

(當students資料庫有insert異動時，插入一筆資料111111到students2資料庫的

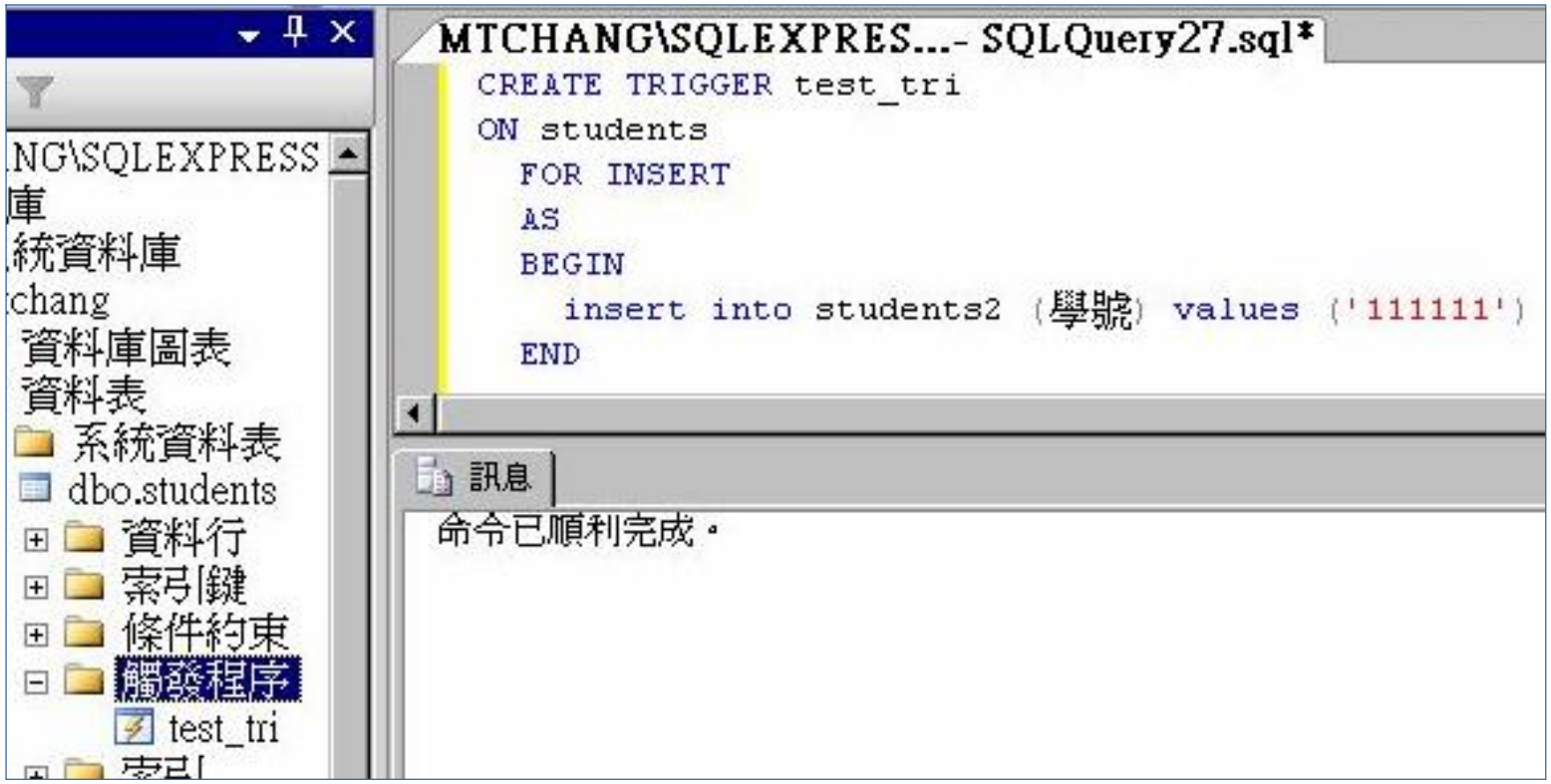
引起觸發：

```
INSERT INTO students(學號,姓名,住址) VALUES ('222222','張小明','高雄縣');
```

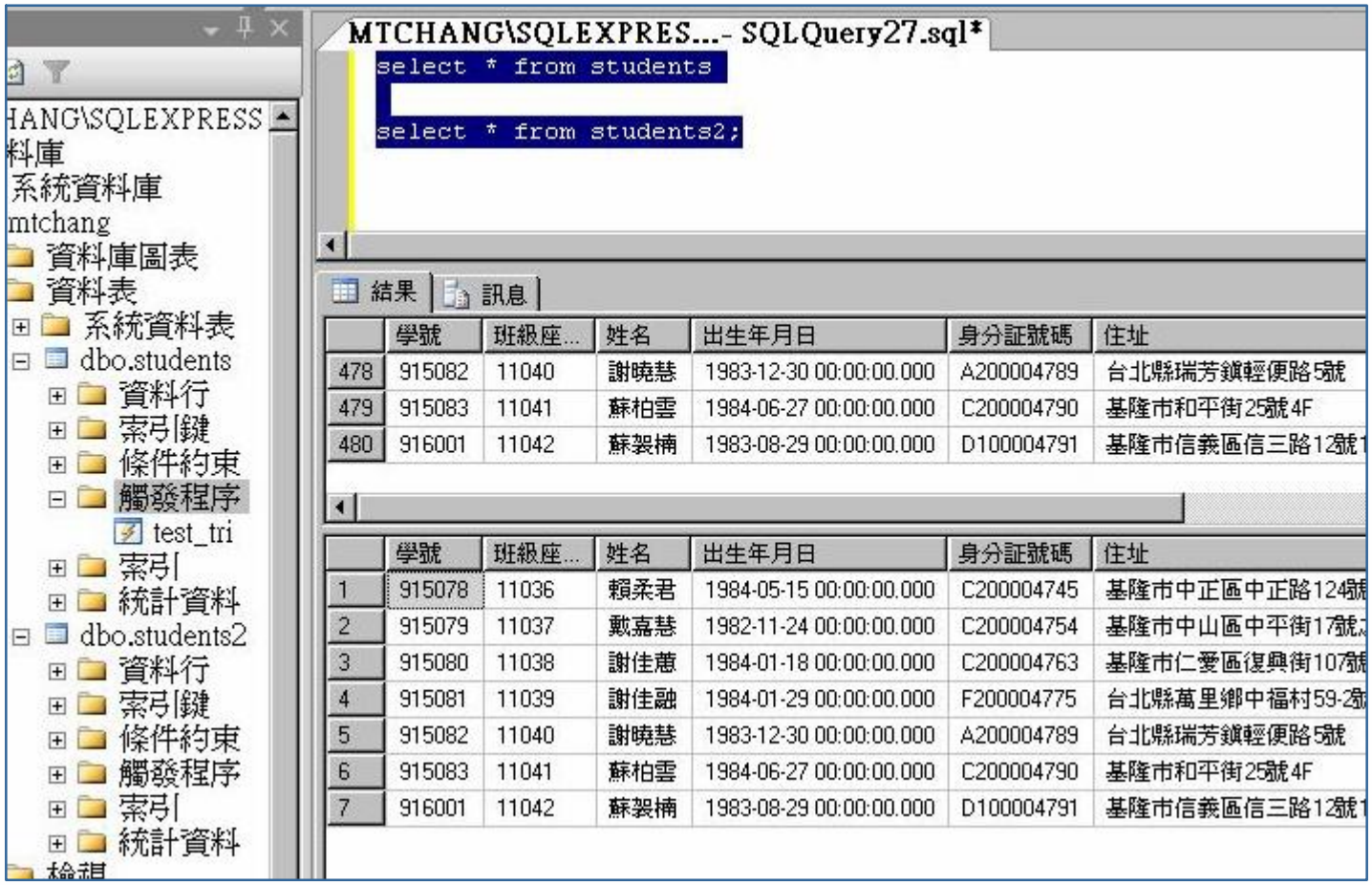
若要擷取 被刪除deleted 資料表中的所有值請使用：

```
SELECT * FROM deleted
```

建立觸發


MTCHANG\SQLEXPRES...- SQLQuery27.sql*
CREATE TRIGGER test_tri
ON students
FOR INSERT
AS
BEGIN
insert into students2 (學號) values ('111111')
END
訊息
命令已順利完成。
NG\SQLEXPRESS
庫
統資料庫
chang
資料庫圖表
資料表
系統資料表
dbo.students
資料行
索引鍵
條件約束
觸發程序
test_tri

引起觸發前


MTCHANG\SQLEXPRES...- SQLQuery27.sql*
select * from students
select * from students2;
結果
訊息
HANG\SQLEXPRESS
料庫
系統資料庫
mtchang
資料庫圖表
資料表
系統資料表
dbo.students
資料行
索引鍵
條件約束
觸發程序
test_tri
索引
統計資料
dbo.students2
資料行
索引鍵
條件約束
觸發程序
索引
統計資料
檢視
學號 班級座... 姓名 出生年月日 身分証號碼 住址
478 915082 11040 謝曉慧 1983-12-30 00:00:00.000 A200004789 台北縣瑞芳鎮輕便路5號
479 915083 11041 蘇柏雲 1984-06-27 00:00:00.000 C200004790 基隆市和平街25號4F
480 916001 11042 蘇裘楠 1983-08-29 00:00:00.000 D100004791 基隆市信義區信三路12號
學號 班級座... 姓名 出生年月日 身分証號碼 住址
1 915078 11036 賴柔君 1984-05-15 00:00:00.000 C200004745 基隆市中正區中正路124號
2 915079 11037 戴嘉慧 1982-11-24 00:00:00.000 C200004754 基隆市中山區中平街17號
3 915080 11038 謝佳蕙 1984-01-18 00:00:00.000 C200004763 基隆市仁愛區復興街107號
4 915081 11039 謝佳融 1984-01-29 00:00:00.000 F200004775 台北縣萬里鄉中福村59-2號
5 915082 11040 謝曉慧 1983-12-30 00:00:00.000 A200004789 台北縣瑞芳鎮輕便路5號
6 915083 11041 蘇柏雲 1984-06-27 00:00:00.000 C200004790 基隆市和平街25號4F
7 916001 11042 蘇裘楠 1983-08-29 00:00:00.000 D100004791 基隆市信義區信三路12號

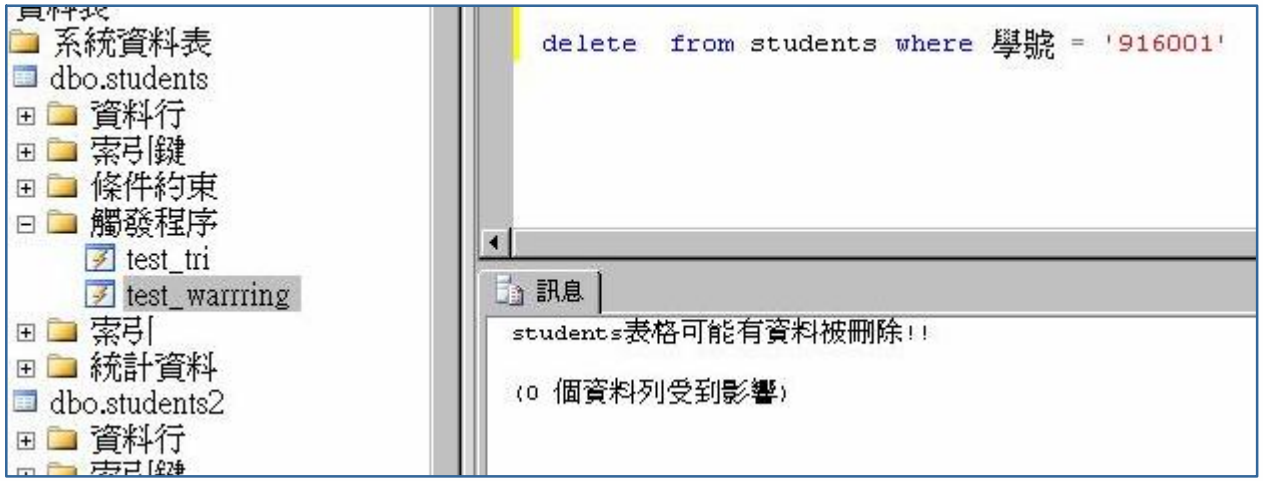
觸發後

	學號	班級座...	姓名	出生年月日	身分証號碼	住址	家
478	915082	11040	謝曉慧	1983-12-30 00:00:00.000	A200004789	台北縣瑞芳鎮輕便路5號	謝
479	915083	11041	蘇柏雲	1984-06-27 00:00:00.000	C200004790	基隆市和平街25號4F	蘇
480	916001	11042	蘇裘楠	1983-08-29 00:00:00.000	D100004791	基隆市信義區信三路12號15樓	蘇
481	222222	NULL	張小明	NULL	NULL	高雄縣	NU

	學號	班級座...	姓名	出生年月日	身分証號碼	住址	家長
1	915078	11036	賴柔君	1984-05-15 00:00:00.000	C200004745	基隆市中正區中正路124號4樓	賴啓彰
2	915079	11037	戴嘉慧	1982-11-24 00:00:00.000	C200004754	基隆市中山區中平街17號之3 4F	戴朝宗
3	915080	11038	謝佳蕙	1984-01-18 00:00:00.000	C200004763	基隆市仁愛區復興街107號	謝朝陽
4	915081	11039	謝佳融	1984-01-29 00:00:00.000	F200004775	台北縣萬里鄉中福村59-2號	謝阿屘
5	915082	11040	謝曉慧	1983-12-30 00:00:00.000	A200004789	台北縣瑞芳鎮輕便路5號	謝崇義
6	915083	11041	蘇柏雲	1984-06-27 00:00:00.000	C200004790	基隆市和平街25號4F	蘇禾成
7	916001	11042	蘇裘楠	1983-08-29 00:00:00.000	D100004791	基隆市信義區信三路12號15樓	蘇大成
8	111111	NULL	NULL	NULL	NULL	NULL	NULL

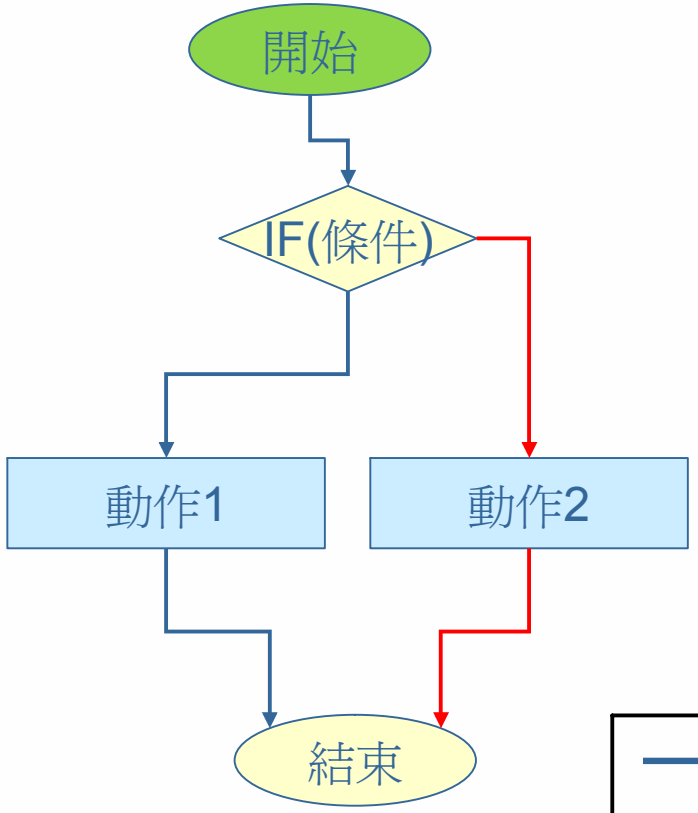
練習

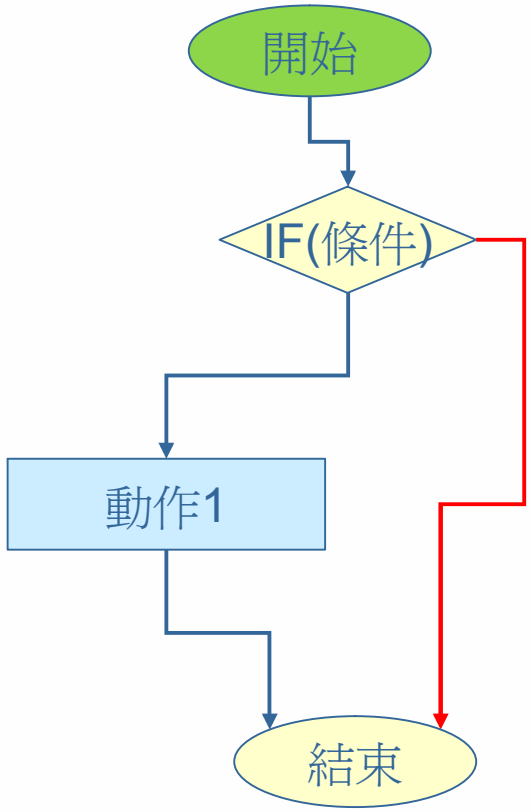
建立一個觸發程序test_warring，功能爲當students有delete動作發生時，在訊息畫面顯示「students表格可能有資料被刪除!!」，在結果畫面列出被刪除的資料。

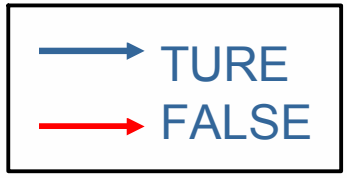


休息一下

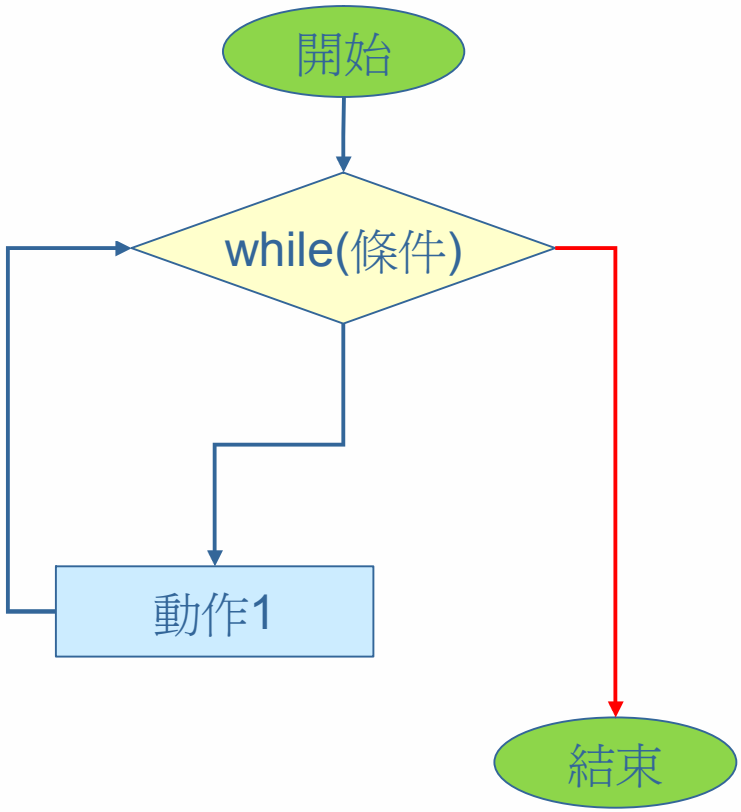
流程控制-IF

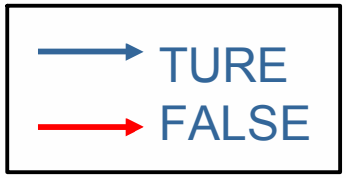






流程控制-WHILE

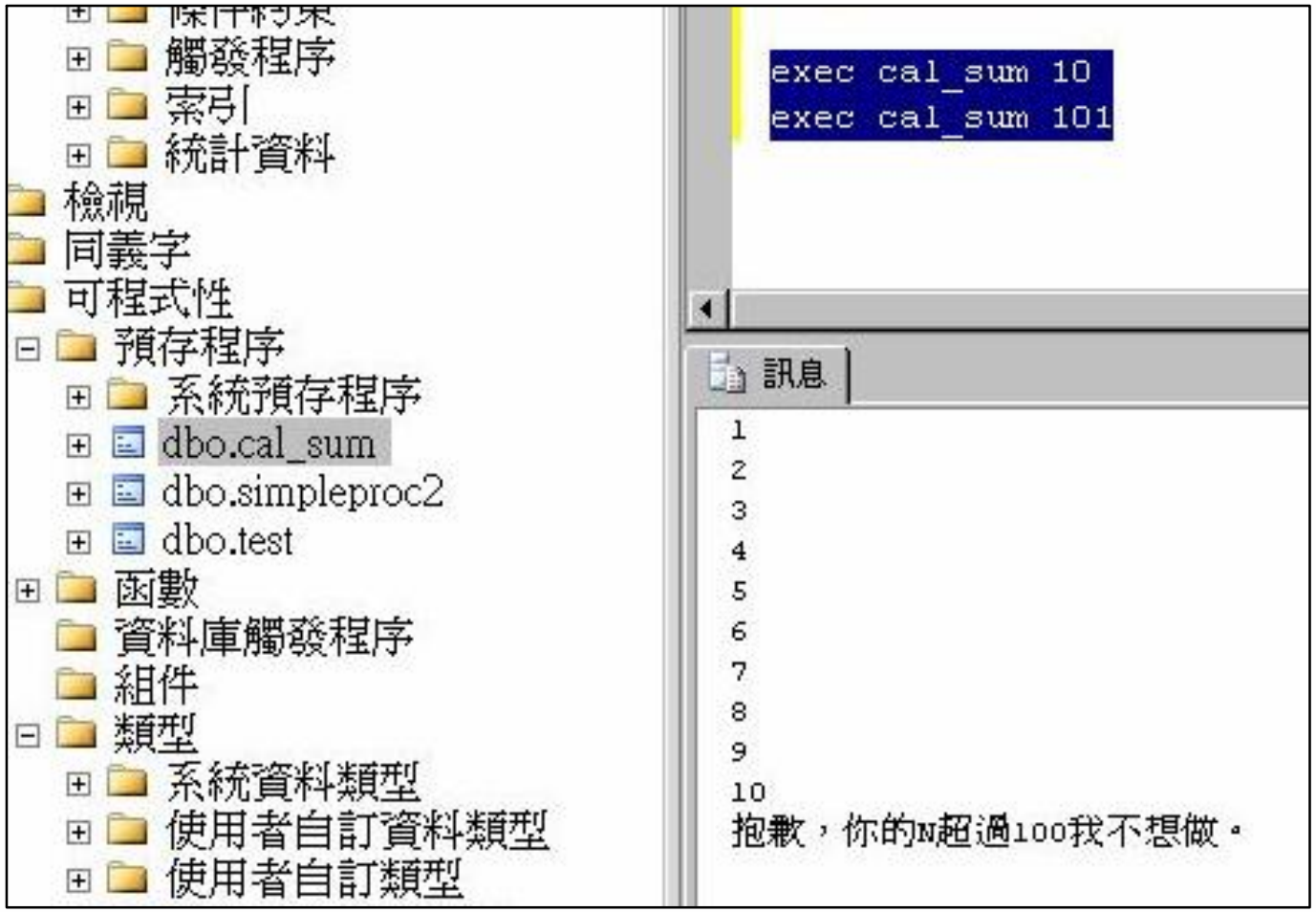




綜合程式範例寫成預存程式

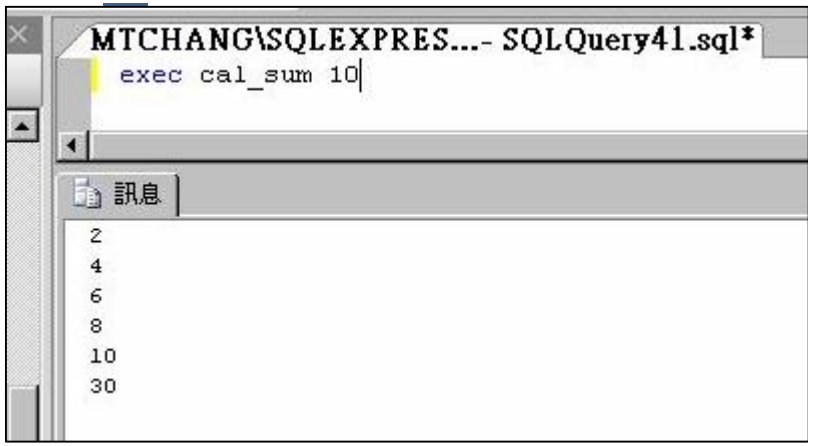
```
CREATE  PROCEDURE cal_sum  --宣告預存程式
  @n int  -- 宣告帶入的變數
as
begin
                declare @i int                  --宣告變數
                set @i=1                        --設定@i變數值
                if (@n<=100)                    --IF敘述
                                begin           --IF敘述begin-end區段ture區段
                                                while (@i<=@n)  --WHILE敘述
                                                begin
                                                                print @i        --顯示目前@i值
                                                                set @i=@i+1  --將目前的@i值加1
                                                end
                                end
                else
                                begin           --IF敘述begin-end區段FALSE區段
                                                print '抱歉，你的N超過我不想做迴圈。'  --顯示訊息
                                end
End  --程式結束
```

綜合程式範例寫成預存程式—執行結果



範例練習：

- 題目：請使用累積和的算法，寫一預存程序，可以直接帶入n值，以迴圈方式計算2+4+6+..+n的偶數和的值結果。
- 也就是說，只要執行exec cal_sum10
- 就會回應 總和為30
- 請勿使用公式方法計算。



%爲取餘數運算
範例：
5%2=1
6%2=0

休息一下

SQL Injection

- 影片範例
- http://tw.youtube.com/watch?v=MJNJjh4jORY
- http://tw.youtube.com/watch?v=AqsALBQcv9U

SQL Injection

```
`通常用來認證的SQL敘述寫法，利用使用者輸入的資料來組合 SQL 語法
strSQL="SELECT * FROM tblUser WHERE UserName='" & _Request("UserName") & "'
AND Password='" & Request("Pass") & "'"
'直接交給 SQL Server 執行
Set rec=.Execute(strSQL)
If NOT rec.EOF Then `如果有找到資料，就算認證成功
                Session("UserName")=Request("UserName")
                Response.Write "歡迎光臨 " & Request("UserName")
Else            `如果失敗就顯示登入失敗
                Response.Write "您的帳號/密碼輸入錯誤"
End If
```

SQL Injection

被**SQL Injection**的語法：
但在上面的例子中，如果使用者填入：

則程式的**SQL**的敘述：
SELECT * FROM tblUser WHERE UserName='admin'--' AND Password='asdf'
看不懂嗎？對於**SQL server**而就變成這樣
SELECT * FROM tblUser WHERE UserName='admin'

SQL Injection

如果不知道帳號是什麼？
‘ or 1=1--

SQL Server 所接收的整個語法變成：
SELECT * FROM tblUser WHERE UserName='' or 1=1--' AND Password='asdf'

看不懂嗎？對於**SQL server**而就變成這樣
SELECT * FROM tblUser WHERE UserName='‘ or 1=1

敵人從哪來？

- GOOGLE的搜尋
  關鍵字：login.asp site:gov.tw
- Google的用法
- http://www.google.com/support/?hl=zh_TW

報告完畢，謝謝收看。