教育部102年度學術機構分組資通安全通報演練計畫

壹、依據

一、行政院國家資通安全會報函頒之「國家資通安全通報應變作業綱要」辦理。

二、依據101年5月行政院核定之「國家資通訊安全發展方案」(101年至105年)辦理。

貳、目的

一、檢驗「教育機構資安通報平台」所登錄單位資安聯絡人資料之正確性。

二、檢驗各區縣網通報反應及處理能力與審核機制是否完善。

三、測試學術機構分組資安聯絡人聯絡管道是否暢通。

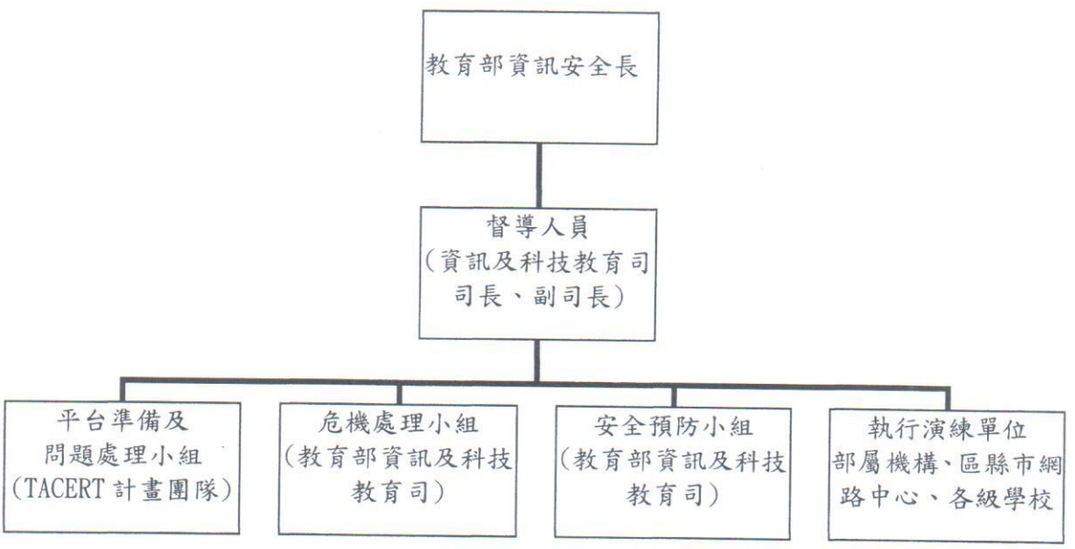
四、測試各單位於發現資安事件時，是否可正確、快速執行通報作業。

五、測試通報網站、電子郵件、電話等各種通訊聯絡管道暢通與存活率。

參、任務編組

本次學術機構分組資通安全通報演練之任務編組如下：

一、任務編組架構：



二、工作內容：

(一)平台準備及問題處理小組：

負責教育機構資安通報演練平台維護、規劃演練各項事宜及問題處理。

(二)危機處理小組：

負責規劃演練各種模擬狀況及處理突發狀況。

(三) 安全預防小組：

負責規劃參演單位及支援演練計畫執行處理作業。

(四) 執行演練單位：

負責執行報演練作業。

肆、演練期程

一、演練資料整備作業：自102年09月30日起至102年10月13日止

二、資安通報演練作業：

(一)第一梯次演練：102年10月14日至102年10月18日止。

(二)第二梯次演練：102年10月21日至102年10月25日止。

伍、演練資料整備作業

一、整備項目：

(一)教育機構資安通報平台帳號資料確認

教育機構資安通報平台係以行政院研考會所核發之物件識別碼(OID)作為各單位登入帳號，各執行演練單位資安聯絡人若忘記登入帳號時可至該網站查詢；如名稱有所異動時，請先行至行政院研究發展考核委員會申辦OID，並告知臺灣學術網路危機處理中心(TACERT)辦理帳號異動。

Edited by Foxit Reader
Copyright(C) by Foxit Software Company,2005-2008
For Evaluation Only.

申請OID時請至網站 http://oid.nat.gov.tw/OIDWeb/chmain.html 點選「申請組織與團體OID說明」選項），相關申請流程請參考網頁說明。

(二)教育機構資安通報平台資安聯絡人資料確認

各執行演練單位請於演練資料整備期間內至「**教育機構資安通報平台**」登錄資料，各機構、學校至少應填列 2 名資安聯絡人，並檢查資安聯絡人資料是否正確並完成密碼更新。

二、配合注意事項：

（一）本年度因進行OID帳號分割，各聯絡人需以各自帳號登入進行聯絡人資料確認及密碼更新作業。

（二）密碼更新於單位收到演練公文開始至演練結束期間，至少前二位連絡人需進行密碼變更，方算完成作業。

(三)建議使用高強度密碼，以大、小寫英文、數字、符號至少擇其二種組合成6碼以上之密碼。

陸、資安通報演練作業

一、演練說明：

本次演練通報流程依據會報函頒之「國家資通安全應變中心作業手冊」及教育部頒之「教育機構資安通報應變手冊」標準以模擬事件來檢視各學術機構資安事件通報是否符合「國家資通安全事件通報應變機制」作業及通報流程。希望透過此次演練檢視所有機構、學校資料更新程度，並了解各區域、縣市網路中心及機構、學校反應能力。

二、執行演練單位：

(一)第一梯次執行演練單位

執行演練單位：臺北區域網路中心、桃園區域網路中心、竹苗區域網

Edited by Foxit Reader
Copyright(C) by Foxit Software Company,2005-2008
For Evaluation Only.

路中心、宜蘭區域網路中心、花蓮區域網路中心、臺東區域網路中心、基隆市教育網路中心、臺北市教育網路中心、新北市教育網路中心、桃園縣教育網路中心、金門縣教育網路中心、連江縣教育網路中心、新竹市教育網路中心、新竹縣教育網路中心、苗栗縣教育網路中心、宜蘭縣教育網路中心、花蓮縣教育網路中心、臺東縣教育網路中心等，及其所服務之連線學校、機構。

(二)第二梯次執行演練單位

執行演練單位：新竹區域網路中心、臺中區域網路中心、南投區域網路中心、雲嘉區域網路中心、臺南區域網路中心、高屏澎區域網路中心、臺中市教育網路中心、南投縣教育網路中心、雲林縣教育網路中心、嘉義市教育網路中心、嘉義縣教育網路中心、臺南市教育網路中心、高雄市教育網路中心、屏東縣教育網路中心、澎湖縣教育網路中心等，及其所服務之連線學校、機構。

三、演練方式：

(一)本次演練將以「**告知通報**」形式進行，教育部將於資安通報演練作業期間以郵件及簡訊傳送「資安事件通報單」。為避免與真實事件產生混淆，演練模擬事件通知簡訊及郵件上皆加註「**告知通報演練**」字樣，另事件單編號皆以「DRILL」開頭進行編碼。

(二)系統將以教育部模擬之10種情境樣本以亂數方式於演練期間分別發送至所有學術單位，執行演練單位於收到mail及簡訊通知後，應於1小時內至**教育機構資安通報演練平台**完成事件通報流程，並依事件等級於處理時限內完成事件應變處理並結案。

演練平台網址：https://drill.cert.tanet.edu.tw

四、演練模擬事件類型：

演練情境由教育部根據行政院研考會99年6月頒之「G-ISAC情報交換格式說明文件」中所規範之主要攻擊事件類型加以規劃，共計有10種

模擬資安事件來進行各學術機構的演練，藉此檢測各學術機構是否能於符合教育部規範的時限內正確地完成通報應變流程。

10種模擬資安事件系分別選自「G-ISAC情報交換格式說明文件」中所規範之兩大主要攻擊事件類型：入侵攻擊事件(INT)及網頁攻擊事件(DEF)。為考量到全面性，因此將此兩大主要攻擊事件類型發生頻率高的所有子類型全部涵蓋，10種模擬資安事件之說明如下表：

模擬狀況編號	攻擊類型(事件類型)	攻擊子類型(事件子類型)	攻擊事件說明
1	DEF	網頁置換	單位網站首頁遭竄改
2	DEF	釣魚網站	單位內某網站被植入偽造認證網站(釣魚網站)
3	DEF	惡意網頁	單位內網站被植入惡意網頁
4	DEF	惡意留言	單位內網站討論區被灌入大量不當留言
5	DEF	個資外洩	單位內透過不同方式散播個人資料
6	INT	對外攻擊	單位內某電腦重複嘗試入侵他人系統
7	INT	散播惡意程式	單位內部電腦中毒並迅速感染其他電腦
8	INT	BOT	單位內電腦中毒成為BOTNET成員
9	INT	SPAM	單位內某電腦大量散佈電子郵件
10	INT	中繼站	單位內部電腦被植入惡意程式後形成BOT中繼站

五、演練模擬事件通報方式：

各執行演練單位將於受測期限內某時間收到演練平台所寄發之簡訊及電子郵件兩種告知訊息，各學術機構需根據教育部頒之「教育機構資安通報應變手冊」標準進行通報應變流程，本文件可於臺灣學術網路危機處理中心網站（http://cert.tanet.edu.tw）中之「資安文件」處下載。

六、發送之簡訊格式與範例：

格式:(告知通報演練)[受測單位],[事件類型]警訊,[事件編號],請盡速至

平台完成事件處理。

範例1：(告知通報演練)[國立XX大學],[入侵攻擊]事件警訊,[15],請盡速至平台完成事件處理。

範例2：(告知通報演練)[國立YY大學],[網頁攻擊]事件警訊,[16],請盡速至平台完成事件處理。

七、發送之電子郵件主旨欄格式與範例：

主旨欄格式:(事件單編號:DRILL-AISAC-XX)(告知通報演練)[事件類型]事件警報

範例1：(事件單編號：DRILL- AISAC-15)(告知通報演練)入侵攻擊事件警報)

範例2：(事件單編號：DRILL- AISAC-16)(告知通報演練)網頁攻擊事件警報)

八、發送之演練事件通知單內容範例：

教育機構資安通報【演練平台】

教育部暨學術機構分組資通安全演練事件通知單

演練事件類型:入侵事件警訊

演練事件單編號:DRILL-AISAC-xx

原發布編號	DRILL-INT-201310-xxxx	原發布時間	2013-10-xx xx:xx:xx
演練事件類型	中繼站	原發現時間	2013-10-xx xx:xx:xx
演練事件主旨	貴單位[**受測單位**][IP:xxx.xxx.xxx.xxx]主機進行大量BOT嘗試連線警訊通知		
演練事件描述	1.若來源IP該連線行為已得到授權，則請忽略此訊息。2.若來源IP該連線為異常行為，可先利用掃毒軟體進行全系統掃描，並利用ACL暫時阻擋該可疑IP。同時建議管理者進行以下檢查： a.請查看來源IP有無異常動作（如：新增帳號、開啟不明Port、執行不明程式)。 b.確認防毒軟體的病毒碼已更新為最新版本、系統已安裝相關修正檔，或關閉不使用的應用軟體與相關通訊埠。3.請查看事證報告，確認該流量是否合法。		
手法研判	無		
建議措施	來源IP可能遭受駭客入侵或遭植入木馬程式，並造成資訊外洩或成為殭屍網路一員而對外發動攻擊。此警示表示有人企圖利用 Pushdo 殭屍病毒（Bot）進行		

Edited by Foxit Reader
Copyright(C) by Foxit Software Company,2005-2008
For Evaluation Only.

	拒絕服務（DoS）攻擊。入侵偵測防禦系統偵測到來源 IP(xxx.xxx.xxx.xxx)，啟用包含 BotNet 特徵之封包，對目標 IP（多個目標 IP）進行連線。此事件來源 PORT （多個來源 PORT），目標 PORT （多個目標 PORT）。攻擊若是得逞，可能會造成目標伺服器發生 DoS 狀況。
此演練事件需要進行通報，請 貴單位資安聯絡人登入資安通報演練平台進行通報應變作業	
如果您對此通告的內容有疑問或有關於此演練事件的建議，歡迎與我們連絡。	

教育機構資安通報應變小組
演練平台網址：https://drill.cert.tanet.edu.tw
電話：07-5250211
電話二：07-5251535
VOIP 網路電話：98400000
E-Mail：service@cert.tanet.edu.tw

請特別注意：
1. 資安聯絡人資料更新請上「教育機構資安通報平台」(https://info.cert.tanet.edu.tw/)
2. 通報演練請上「教育機構資安通報演練平台」(https://drill.cert.tanet.edu.tw/)

九、評分對象：分為區縣(市)網路中心及各可連線服務機構、學校

(一)區縣(市)網路中心以管轄單位密碼更新比率、通報完成率及是否依通報應變流程時限內完成審核作為評比標準。

(二)機構、學校以是否依通報應變流程時限內完成通報、應變及單位聯絡人資料準確度及完整性作為評比標準。

對象	評分標準	說明
區縣(市)網路中心	密碼更新率	密碼更新比率
	通報完成率	管轄單位通報完成比率
	審核及時率	是否依通報應變流程時限內完成審核
機構、學校	通報及時率	是否依通報應變流程時限內完成通報
	應變及時率	是否依通報應變流程時限內完成處理
	資料正確率	單位聯絡人資料準確度及完整性

Edited by Foxit Reader
Copyright(C) by Foxit Software Company,2005-2008
For Evaluation Only.

十、評分標準說明：

(一)密碼更新率：以各區縣(市)網路中心所屬機構、學校登入帳號之密碼更新比率給分。

(二)通報完成率：以各區縣(市)網路中心所屬機構、學校是否在時限內完成通報給分。

(三)審核及時率：以各區縣(市)網路中心是否能於時限內完成案件審核給分。1、2 級資安事件需於 16 小時內審核完畢，3、4 級資安事件需於 4 小時內審核完畢。

(四)通報及時率：以各級(A、B、C、D)機構、學校依事件等級時限內完成通報。

(五)應變及時率：以各級(A、B、C、D)機構、學校依安全等級時限內完成處理。1、2 級資安事件需於 72 小時內完成應變作業，3、4 級資安事件需於 36 小時內完成應變作業。

(六)資料正確率：各校需於教育機構資安通報平台登錄至少 2 名資安連絡人，並隨時保持資料最新且正確。

各區（縣）網路中心評分標準說明

給分標準 / 評分項目	1	0
密碼更新率	達 80%	未達 80%
通報完成率	所轄連線單位於 24 小時內完成通報的比率達 80%	所轄連線單位於 24 小時內完成通報的比率未達 80%
審核及時率	所轄連線單位事件單審核作業於時限內完成率達 70%以上但未達 80%	所轄連線單位事件單審核作業於時限內完成率未達 70%

Edited by Foxit Reader
Copyright(C) by Foxit Software Company,2005-2008
For Evaluation Only.

各機構及學校評分標準說明

給分標準 / 評分項目	2	1	0
通報及時率	4 小時內完成	24 小時內完成	24 小時內未完成
應變及時率	時限內完成	(時限+4 小時)內完成	未於(時限+4 小時)內完成
資料正確率	2 位以上資安聯絡人所有欄位資料填寫完整	填寫 2 位以上資安聯絡人，但僅一位資安聯絡人所有欄位資料填寫完整	1. 未填寫資安聯絡人 2. 資安聯絡人資料資料均不完整

十一、獎懲標準說明：

(一)為鼓勵積極推動資通安全防護及即時完成通報作業，教育部將依據本次演練結果挑選績優單位及改善單位，並辦理所屬機構獎懲作業。

(二)績優單位：區縣(市)網路中心部分連線單位 200 個(含)以上挑選前 2 名、50~199 個挑選前 2 名、50 個以下挑選前 2 名；連線單位部分 AB 級機構、學校挑選前 5 名、CD 級機構、學校挑選前 5 名、部屬館所挑選前 2 名，由教育部發文該單位建議予以獎勵(請依權責自行敘獎)。

(三)改善單位：區縣(市)網路中心及各級機構、學校總分在 3 分以下，請該單位檢具檢討改善報告(附件)報部備查，並列入教育部資訊安全稽核優先名單。

(四)各縣市政府參演成績將列入「102 年度統合視導地方教育事務」評分項目之一，如有待加強事項，教育部將於視導單位時驗證單位改善成效。

類別	對象	說明
績優單位	區縣(市)	連線單位 200 個(含)以上，取演練成績較佳 2 名

	網路中心	連線單位50(含)至200個，取演練成績較佳2名
		連線單位50個以下，取演練成績較佳2名
	機構、學校	AB級機構、學校，取演練成績較佳5名
		CD級機構、學校，取演練成績較佳5名
	部屬館所	取演練成績較佳2名
改善單位	全體	區縣(市)網路中心及各級機構、學校演練成績總分在2分以下

十二、協調聯絡資訊

(一)教育機構資安通報平台網址：https://info.cert.tanet.edu.tw

(二)通報平台操作相關事宜可洽TANet CERT服務人員協助

連絡電話：(07)525-0211

VOIP網路電話：98400000

E-mail： service@cert.tanet.edu.tw

附件：

教育部102年度學術機構分組資通安全通報演檢討改善情形報告

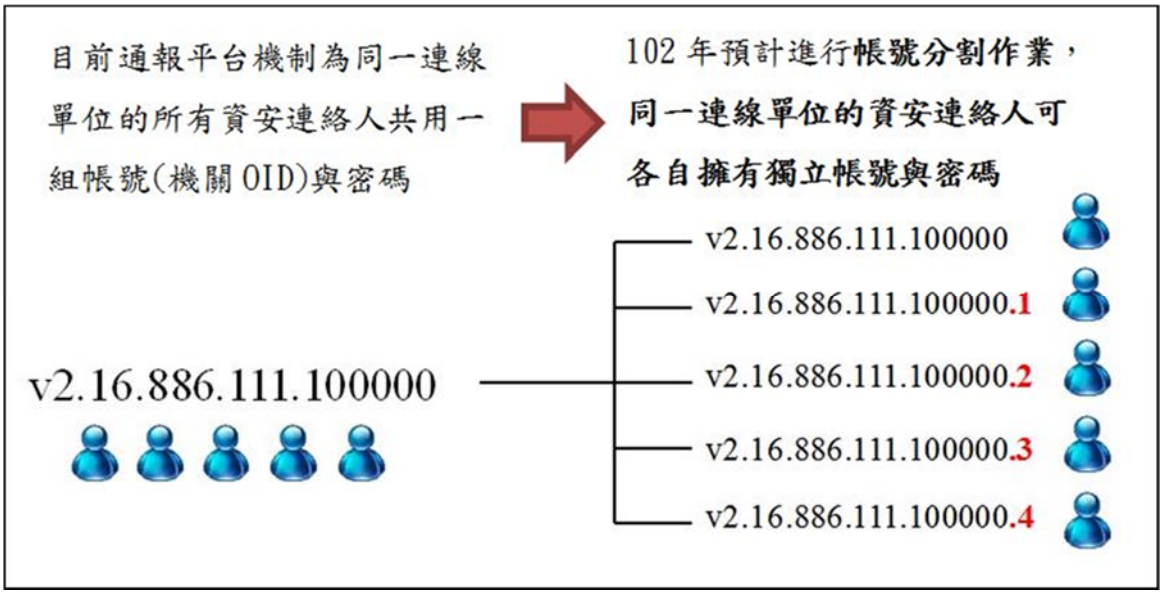
＿＿＿年 機構、學校名稱 **檢討改善情形報告**
一、 演練整備情形說明： （說明機構、學校於本次資安通報演練之**整備**概況與尚待精進之處。以 500 字為限。） **二、 通報作業檢討：** （檢討本次資安**通報及演練作業**概況與尚待精進之處。以 500 字為限。） **三、 改善計畫與改善情形說明：** （了解現行作業是否符合「教育體系資安事件應變處理機制」作業及通報流程[登載於 https://tacert.tanet.edu.tw]要求，提出改善計畫與改善情形說明。以 500 字為限。） **四、 通報應變作業建議：** （針對「國家資通安全事件通報應變機制」及「101 年度行政院國家資通安全會報學術機構分組資通安全通報演練計畫」，提出改善或相關建議。以 500 字為限。）

填報人：＿＿＿＿＿＿　主管：＿＿＿＿＿＿　資訊安全長(副首長)：＿＿＿＿＿

OID 帳號分割作業

為加強教育機構資安通報應變平台的資料安全性，本年度計畫將進行連線單位帳號分割作業。

目前的通報平台機制為同一連線單位的所有資安聯絡人(上限為五人)共用一組機關 OID 與密碼。為加強安全性控管，本年度規劃將原有帳號分割為五份，提供同一連線單位的所有資安聯絡人五組不同的帳號與密碼設定(如圖所示)。



有關帳號、密碼及聯絡人對應關係表：

分割前：

OID 帳號(2.16.886.XXX.XXXXX・・・)				
密碼(共用)				
第一聯絡人	第二聯絡人	第三聯絡人	第四聯絡人	第五聯絡人

分割後：

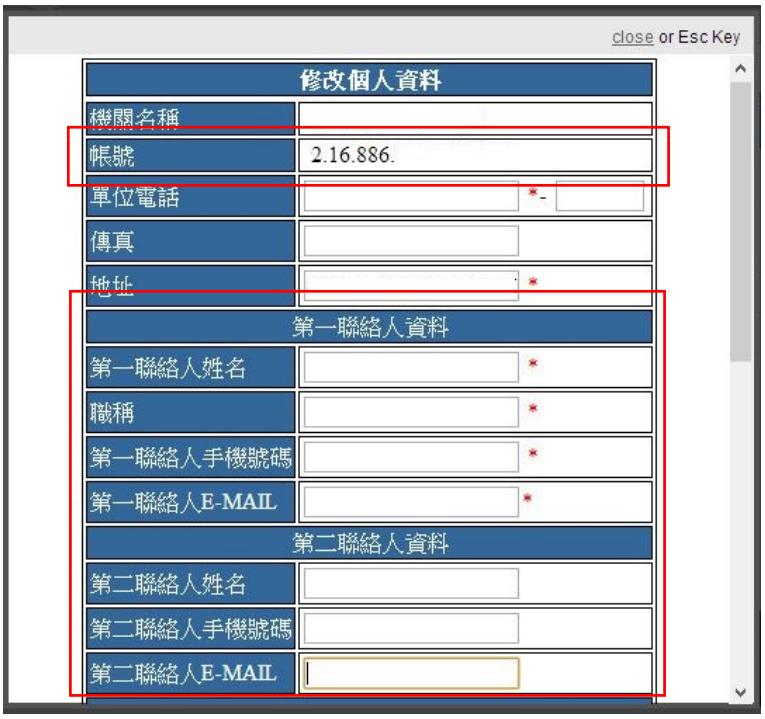
OID 帳號	OID 帳號.1	OID 帳號.2	OID 帳號.3	OID 帳號.4
密碼	密碼	密碼	密碼	密碼
第一聯絡人	第二聯絡人	第三聯絡人	第四聯絡人	第五聯絡人

平台畫面對照表：

登入平台後點選左側功能項「**修改個人資料**」呈現之畫面

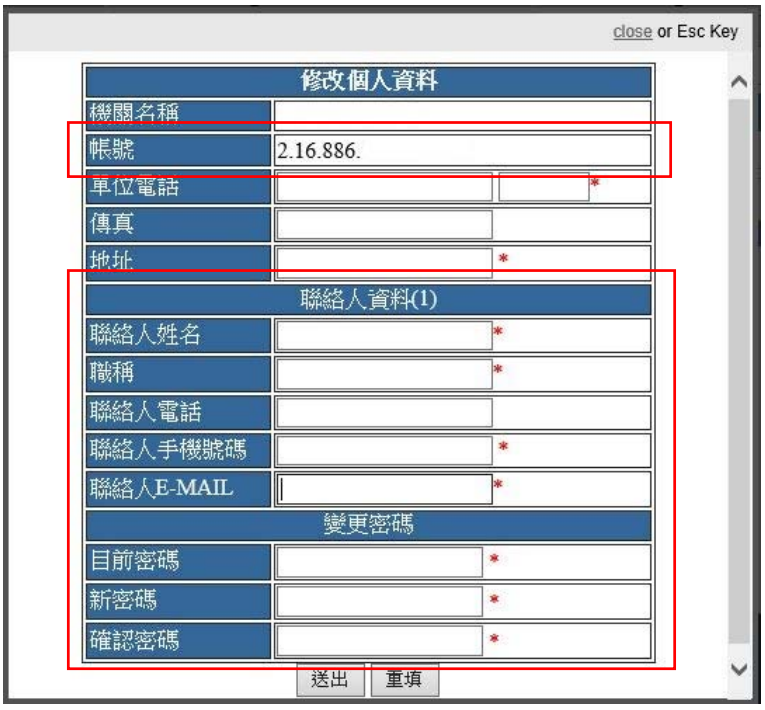
分割前：

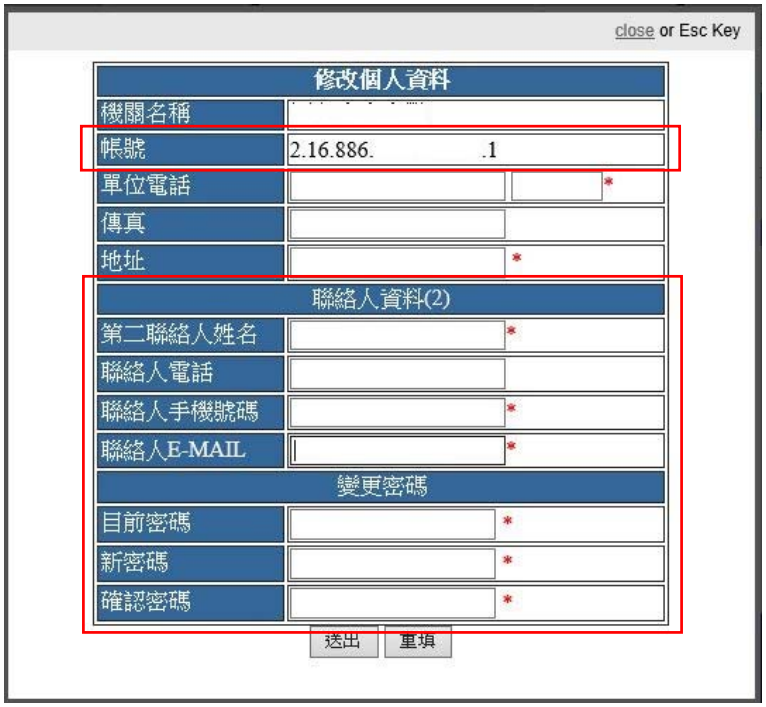
可看到於同一個畫面中，出現多個聯絡人資料。



分割後：

登入後，各別帳號只能看到單一聯絡人資料。





影響範圍：

平台內部所有 OID 帳號，包括一線單位、區縣市網路中心。

注意事項：

1. 帳號分割後，**原 OID 帳號為第一聯絡人所有使用**，故分割作業不影響平台使用。
2. 帳號分割後，各分割帳號**預設登入密碼為原先 OID 帳號之密碼**，煩請分配使用後，盡速登入平台進行資料確認及密碼變更。
3. 各單位建議至少需填寫二個帳號之資料，並落實代理人制度，以利通報平台資訊傳遞。