



教育機構資安通報平台

第一線人員使用者手冊

(3,4級資安事件)自行通報

(通報應變同時進行)說明

(2010.6.24)

報告：曾龍 副教授

簡報製作：陳柔伊

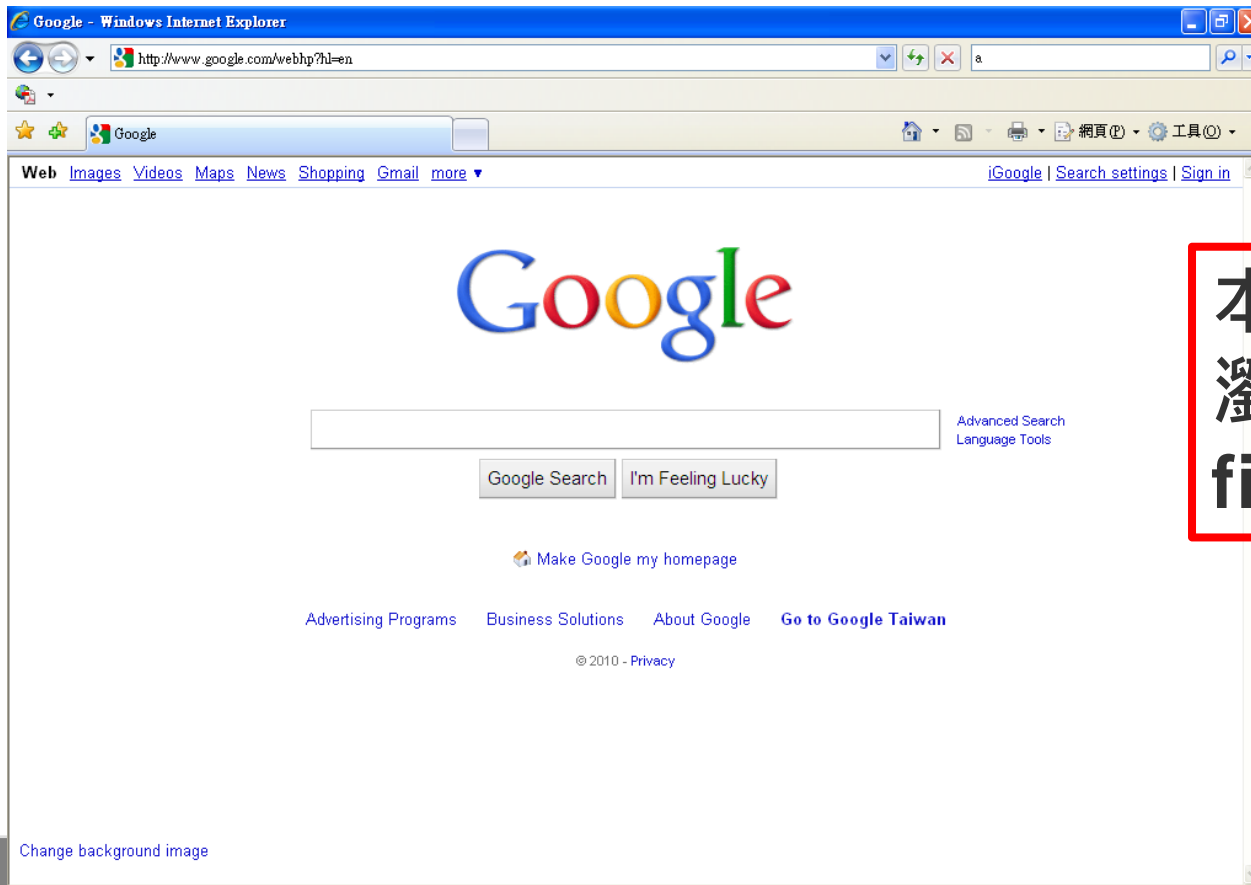
I.使用情況:

- 1.【**第一線人員**】發現資安事件時，須登入通報平台通報，填寫資安事件說明。
- 2.【**第一線人員**】**發現重要資安事件**(如個資法外洩，3級以上資安事件)時，須立即電話告知【**區縣市網人員**】及【**教育機構資安通報應變小組**】並於**1小時內登入**通報平台完成此資安事件之通報。

II. 操作步驟:

步驟1: 使用者登入通報平台

1.1 使用者打開瀏覽器，並輸入A-ISAC平台的網址



本平台最佳使用
瀏覽器為IE8.0、
firefox、chrome

II. 操作步驟:

1.2 使用者點選左上角之【**TANET教育機構資安通報平台**】按鈕，即可連線至通報平台。

點選之【**TANET教育機構資安通報平台**】按鈕



教育機構資安通報平台
member only

教育機構資安通報平台
member only

由此登入 >>>

A-ISAC緣由

自美國提出國家關鍵基礎設施保護計畫(National Plan for Critical Infrastructure Protection) 推動個別產業之ISAC，進行資訊安全相關資訊的蒐集、分析、判斷與傳遞給產業界與相關單位。美國民間企業部門亦遵照美第63號總統法令的建議，成立相關協會以從事資訊分享工作。美國學界也建置Research and Education Networking Information Sharing and Analysis Center (REN-ISAC)。其目的亦為進行資安訊息的蒐集、分析、發佈通知或作為資安預警防護之用，以提供並分享給高等教育和研究網路。行政院有鑒於上述計畫的重要性，在國家資通安全會中宣示並建立政府資通安全防護管理中心，以期連結重要核心政府機關(構)及關鍵民生基礎建設目的事業主管機關(構)之ISAC，同時累積資安技術分析能量。教育部配合行政院規劃建置「教育學術資安資訊分享與分析中心」平台，為所屬連網台灣學術網路(TANET)之各級學校提供安全保護與資安資訊分享機制，並依據行政院技術服務中心規劃分享架構中所提出之G-ISAC資料交換格式進行並透過web service的開發，藉由此資訊分享平台之建置可與行政院技服

相關連結

IT-ISAC

MS-ISAC

REN-ISAC

教育部校園資訊安全服務網

II. 操作步驟:

1.3 使用者填入**單位OID**與**密碼**後，需再填寫**圖形驗證碼**。填寫正確後即可進入通報平台進行通報應變作業。

教育機構資安通報平台
Ministry of Education Information & Communication Security Contingency Platform

會員登入

機關OID

登入密碼

5dlnx7

請填入驗證碼 登入

[忘記密碼](#)

弱點通告

2010-04-18 12:49:32.0 | [弱點通告：Microsoft Video ActiveX 控制項 msvidctl.dll 中存在遠端執行程式碼的弱點](#)
Microsoft Video ActiveX 控制項 msvidctl.dll 中存在遠端執行程式碼的弱點。攻擊者可惡意製作網頁，當使用者點選或檢視網頁時，此弱點可能會允許執行遠端程式碼。成功利用此弱點的攻擊者可以取得與登入使用者相同的使用者權限。

2010-04-18 13:42:55.0 | [弱點通告：Microsoft Active Template Library \(ATL\) 標頭 Memcopy 弱點](#)
Microsoft Active Template Library (ATL) 因為 IPersistStreamInit 介面的 Load 方法中含有一項錯誤，而存在遠端執行任意程式碼弱點。Load 方法可能允許以不受信任的資料呼叫 memcopy，如此可能允許遠端未驗證的使用者在受影響系統上遠端執行任意程式碼。攻擊者可能透過惡意製作的網頁，進行攻擊。當使用者檢視網頁時，可能會允許遠端執行任意程式碼。

2010-04-18 13:45:18.0 | [弱點通告：Apple Mac OS X Managed Client 系統 識別錯誤弱點](#)

II. 操作步驟:

1.4 當使用者登入平台時，於左方欄會顯示個人、主管機關與營運團隊資訊。

The screenshot displays a user interface with a left sidebar and a main content area. The sidebar, highlighted with a green border, contains the following information:

- 歡迎光臨**
- 機關名稱: 高雄市立資安國民小學
- 使用者: 王網安
- 主管機關**
- nsqc網路中心
- 聯絡人: 陳資安
- 聯絡電話: 07-123-4567
- E-Mail: samtn125@gmail.com
- 營運單位**
- nsqc營運單位
- 聯絡人: 審核人
- 聯絡電話: 07-012-3456
- E-Mail: samtn@ms94.url.com.tw

The main content area features a blue header with the text "新進告知通報" and a white table below it. The table indicates there is 1 record and lists the following data:

工單編號	發佈時間	距通報時間	逾時
155	10-05-21 18:00	51 小時	否

Below the table, there is a pagination control showing "到 1 頁,共1頁".

At the bottom of the page, there is a footer with the text "應變件處理" and the ISOC logo.

步驟2a: 使用者進行通報作業

2.1 使用者點選左點選左下方【自行通報】按鈕，即可進行資安作業(填寫資安工單)

歡迎光臨

機關名稱: 高雄市立資安國民小學
使用者: 王網安

主管機關
nsqc網路中心
聯絡人: 陳資安
聯絡電話: 07-123-6789
E-Mail: fixedstar125@yahoo.com.tw

營運單位
教育機構資安通報應變小組
聯絡人: 審核人
聯絡電話: 07-012-1234
E-Mail: ksu.nsqclab@gmail.com

回首頁
登出

通報
自行通報
工單處理狀態
歷史通報

分類統計
榮譽排行榜

修改個人資料
檢視聯絡人

填報時間: 2016-06-20 22:23:21

I. 通報流程

一、發生資通安全之機關(機構)聯絡資料:

◎機關(機構)名稱: 高雄市立資安國民小學
◎通報人: 王網安 ◎電話: 07-123-1234 ◎傳真: 07-123-1234
◎E-mail: samtn125@gmail.com

◎主管機關
機關名稱: nsqc網路中心
資安人員: 陳資安
電話: 07-123-6789
傳真: 07-123-6789
E-mail: fixedstar125@yahoo.com.tw

◎營運單位
機關名稱: 教育機構資安通報應變小組
資安人員: 審核人
電話: 07-012-1234
傳真:
E-mail: ksu.nsqclab@gmail.com

二、各機關因受外在因素所產生資通安全事件時通報事項:

◎為必填
欄位不得輸入特殊符號(如: 「!」、「"」、「|」、「\$」、「%」、「^」、「&」、「*」、「_」、「|」、「-」、「>」、「;」)

1) 通報型態:
■主動通報(各單位自行發現資安事件)

2) ◎事件發生時間:

3) 設備資料:
◎IP位置 (IP address): (範例: 120.114.22.33)

◎網際網路位置 (web-url): (範例: https://www.xxx.edu.tw/cba.index)

◎設備廠牌、機型: (範例1: 華碩TS100-E6/PI4, 範例2: Acer AT110 F1)

◎作業系統(名稱/版本): (範例1: Centos Linux 5.4, 範例2: Windows XP SP2)

7

步驟2a: 使用者進行通報作業

- ◆ 2.2資安工單的**填寫說明**，請參看編號A-ISAC-02:【資安工單填寫說明手冊】
- ◆ 說明1:本案例為【**通報應變同時進行**】，因此在通報流程之【**7) 是否同時進行通報 流程與應變流程?**】需選擇【**是**】。
- ◆ 說明2: 本案例為【**通報應變同時進行**】，因此使用者需立即進行應變流程作業。

步驟2a: 使用者進行通報作業

- ◆ 2.3 當使用者填寫(處理)完資安工單時，按【**發佈通報**】按鈕，即可完成通報流程。

7) ①是否同時進行通報流程與應變流程?

- 是(請繼續完成 II. 應變流程之作業)
- 否(會先完成 I. 通報流程 並結束，後續時間請儘快完成 II. 應變流程)

II. 應變流程

①II.1 緊急應變措施

- 已中斷網路連線，待處理完成後再上線
- 已停止伺服器之服務，待處理完成後再上線
- 直接處理完成，解決辦法詳見【解決辦法】
- 其它

①II.2 【解決辦法】(文字勿超過200中文字, 標點符號請用全形)

①解決時間:

步驟3: 使用者完成通報應變作業後 ，平台之後續作業

- ◆ 3.1 使用者完成通報應變作業之後，通報平台會自動寄發**四封Email**分別通知(1)【第一線人員】(2)【區縣市網人員】(3)【教育機構資安通報應變小組】(4)【教育部人員】
- ◆ 3.2 使用者完成通報應變作業之後，通報平台**不會**寄發**SMS簡訊通知**【第一線人員】。

。

步驟4: 使用者完成通報應變作業後 ，可檢視的工單後續處理狀況

說明1:教育部規範之【(3,4級資安事件)自行通報】，需完成下列作業:

- (1) 區縣市網人員需審核通報流程(3,4級資安事件，無需審核應變流程)
- (2) 教育機構資安通報應變小組需審核通報流程(3,4級資安事件，無需審核應變流程)

當(1)(2)都完成時，此資安事件才正式完成教育部規範之結案作業。

步驟4: 使用者完成通報應變作業後 ，可檢視的工單後續處理狀況

- ◆ 說明2: 當區縣市網審核完資安工單時，**不會**寄發**Email**與**SMS**簡訊通知。
- ◆ 說明3: 當教育機構資安通報應變小組審核完資安工單時，會寄發(審核結案)**Email**通知(1)【第一線人員】(2)【區縣市網人員】(3)【教育機構資安通報應變小組】(4)【教育部人員】，但**不會**寄發**SMS**簡訊通知。

步驟4: 使用者完成通報應變作業後

可檢視的工單後續處理狀況

- ◆ 說明4: 使用者可利用下列兩目錄所列之工單來檢視工單處理狀況:
- ◆ (1) 【**工單處理狀態**】是存放(教育部規範)尚未結案之資安工單。當【**第一線人員**】完成通報應變時，平台便會自動產生一筆工單顯示此筆工單之處理狀態。若已完成教育部規範之結案作業，則此工單會轉存放到【**歷史通報**】。
- ◆ (2) 【**歷史通報**】是存放(教育部規範)已結案之資安工單。

4.1 【工單處理狀態】的檢視

◆ 使用者點選左下方【工單處理狀態】按鈕，即可進行(教育部規範)尚未結案之資安工單處理狀態的檢視。

回首頁
登出

通報

自行通報
工單處理狀態
歷史通報

分類統計
榮譽排行榜

修改個人資料
檢視聯絡人

應變待處理

25筆

工單編號	事件等級	通報時間		距通報時間	逾時	流程
		發生時間	解決時間			
37	1級	10-05-27 09:38	10-05-26 09:38	276 小時	逾時(204小時)	應變 尚未解決
40	2級	10-05-27 10:22	10-05-05 10:20	275 小時	逾時(265小時)	應變 尚未解決
56	2級	10-06-06 23:37	10-06-06 23:40	22 小時	否	應變 尚未解決

到 1 頁,共1頁

共有25筆

工單編號	事件等級	第一線人員		區縣市劃人員		營運人員		第一線人員逾時	區縣市劃逾時
		通報	應變	通報	應變	通報	應變		
2	未通報	未通報	未通報	未	未	未	未	逾時(222小時)	否
3	未通報	未通報	未通報	未	未	未	未	逾時(222小時)	否
5	未通報	未通報	未通報	未	未	未	未	逾時(222小時)	否
8	未通報	未通報	未通報	未	未	未	未	逾時(222小時)	否
9	未通報	未通報	未通報	未	未	未	未	逾時(222小時)	否
11	未通報	未通報	未通報	未	未	未	未	逾時(222小時)	否
31	1級	已通報	已通報	未	×	未	×	否	逾時(188小時)
32	2級	已通報	已通報	未	×	未	×	否	逾時(188小時)
35	1級	已通報	已通報	未	×	未	×	否	逾時(188小時)
37	1級	已通報	未通報	未	×	未	×	逾時(131小時)	否

到 1 頁,共3頁

4.2 【歷史通報】的檢視

◆ 使用者點選左側左下方【**歷史通報**】按鈕，即可進行(教育部規範)已結案之資安工單的檢視。

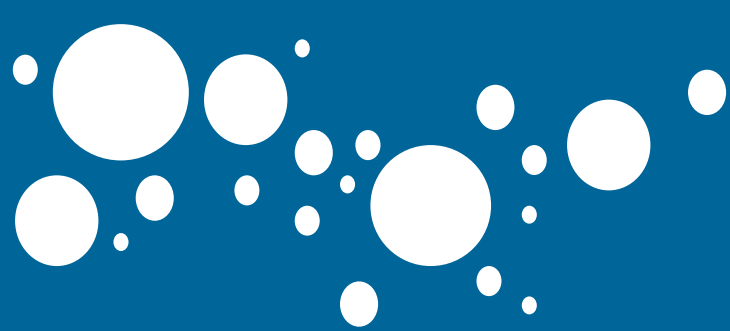
教育機構資安通報平台
TANet CERT
Ministry of Education Information & Communication Security Contingency Platform

歡迎光臨
機關名稱: 高雄市立資安國民小學
使用者: 王網安
主管機關
nsqc網路中心
聯絡人: 陳資安
聯絡電話: 07-123-6789
E-Mail: samtn@ms94.url.com
營運單位
nsqc營運單位
聯絡人: 審核人
聯絡電話: 07-012-1234
E-Mail: pan0438@gmail.com

回首頁
登出
通報
自行通報
歷史通報
分類統計
榮譽排行榜
修改個人資料
檢視聯絡人

歷史通報
時間範圍 自 至 查詢
總歷史通報共有18筆

工單編號	事件等級	通報時間 發生時間 解決時間	區縣市網通 報審核結果	營運通報審 核結果	區縣市網通 變審核結果	營運應變審 核結果
1	1級	10-05-26 14:16 10-05-26 13:00 10-05-26 14:16	通過	通過	無須審核	無須審核
4	2級	10-05-26 14:21 10-05-26 13:00 10-05-26 14:22	通過	通過	無須審核	無須審核
6	3級	10-05-26 16:00 10-05-26 13:00 10-05-26 16:01	通過	通過	通過	通過
7	1級	10-05-26 14:36 10-05-26 13:00 10-05-26 14:35	通過	通過	無須審核	無須審核
10	2級	10-05-26 14:27 10-05-26 13:00 10-05-26 14:27	通過	通過	無須審核	無須審核
12	2級	10-05-26 15:55 10-05-26 13:00 10-05-26 15:55	通過	通過	無須審核	無須審核
13	2級	10-05-26 15:13 10-05-26 13:00 10-05-27 15:12	通過	通過	無須審核	無須審核
14	3級	10-05-26 15:31 10-05-26 13:00 10-05-28 15:27	通過	通過	通過	通過
15	2級	10-05-26 14:13 10-05-26 14:05 10-05-26 14:13	通過	通過	無須審核	無須審核
16	1級	10-05-26 14:28 10-05-25 14:26 10-05-26 14:29	通過	通過	無須審核	無須審核



Thank you for listening.

