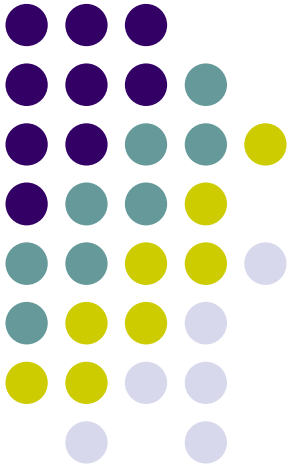
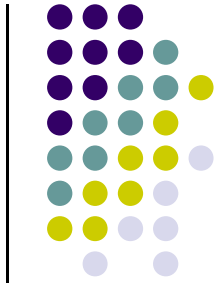
資訊安全教育訓練

力穎管理顧問有限公司

郭宏國



Agenda



- 淺談個人資料保護法
- 個資法之校園案例
- 資訊安全的迷思及觀念

個人資料保護法

個人資料保護法

- 電腦處理個人資料保護法：
  - 84年8月11日制定公布。
- 個人資料保護法：
  - 99年5月26日修正公布。
  - 101年10月1日施行。
    - 除第6、54條條文實施日期由行政院定之外
- 立法目的：
  - 規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用。（第一章第1條）

個人資料保護法
修法重點

- 新法修正重點：
  1. 擴大適用主體：
     - 打破行業別限制，包括各行各業及個人。
     - 受委託蒐集、處理或利用個人資料者，視同委託機關。
  2. 擴大保護客體：
     - 以任何方式（包括紙本）留存的資料。
     - 任何方式取得個人資料。
     - 生存之特定或得特定之自然人。
  3. 增訂告知義務：
     - 直接蒐集及間接蒐集之告知義務。
     - 當事人拒絕行銷之權利。
     - 資料違法外洩之通知義務

個人資料保護法
修法重點

- 新法修正重點：

4. 調整賠償義務及罰則：

  - 民事賠償：新台幣2千萬元 => 2億元
  - 刑事處罰：新台幣5萬元 => 100萬元

    有期徒刑：3年以下 => 5年以下

    意圖營利犯罪者，非告訴乃論
  - 行政處罰：新台幣10萬元 => 50萬元
  - 主管機關並得為下列處分：

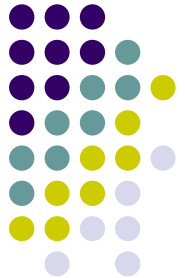
    禁止蒐集、處理或利用個人資料。

    命令刪除經處理之個人資料檔案。

    沒入或命銷燬違法蒐集之個人資料。

    公布違法情形及其姓名或名稱與負責人。

個人資料保護法 總覽



- 第一章 總則（1~14條）
- 第二章 公務機關對個人資料之蒐集、處理及利用(15~18條)
- 第三章 非公務機關對個人資料之蒐集、處理及利用(19~27條)
- 第四章 損害賠償及團體訴訟(28~40條)
- 第五章 罰則(41~50條)
- 第六章 附則(51~56條)

個人資料

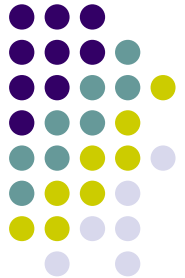
自然人的

一般資料
- 姓名
- 出生年月日
- 身分證號碼
- 護照號碼
- 特徵
- 指紋
- 婚姻
- 家庭
- 教育
- 職業
- 病歷
- 聯絡方式
- 財務情況
- 社會活動

特種資料
- 醫療
- 基因
- 性生活
- 健康檢查
- 犯罪前科

其他資料
- 得以直接或間接方式識別該個人之資料

校務行政相關的個人資料



- 家庭狀況
- 學生基本資料
- 健康檢查
- 病歷紀錄
- 家長聯絡方式
- 學生申請補助
- 教職員出缺勤紀錄
- 教職員人事資料
- 學生學業與操行成績資料
- 清寒家庭身分
- 學生輔導紀錄表之AB卡資料
- 獎懲及違規紀錄

校園情境案例


學生個人資料的保護
學生住家地址、聯絡方法、
家庭狀況和健康狀況


圖書館未還書籍名單
資保高中圖書館網站
姓名
學號
班級
借書人
在網站上公布借書逾期的名單，為利用個人資料的行為。


研討會簽到單
研討會簽到單
姓名：
服務學校：
聯絡電話：
個資法保護


電子郵件通聯紀錄
E-mail紀錄
不觸犯個資法！

個人資料保護守則

定期備份

1、個人資料檔案應定期備份，並防止個人資料被竊取、竄改、毀損、滅失或洩漏。

設定範圍

2、個人資料輸入、輸出、更新或註銷時，應該釐定使用範圍，以及調閱或存取的權限。

帳號密碼

3、個人資料檔案儲存於個人電腦者，應於該電腦設置可辨識身分之登入通行碼。個人資料檔案使用完畢後，應即退出應用程式，不得留置於電腦中。

個人資料保護守則

建立程序

4、含有個人資料的紙本，運用於申請、列印、存檔、轉交及銷毀等行為，應建立相關之授權、監督及行為記錄的機制。

彌封加密

5、內部傳遞或與其他機關交換個人資料時，應在實體文件封袋上，加上彌封；或對電子資料檔案壓縮加密，並加以記錄檔案的流向。

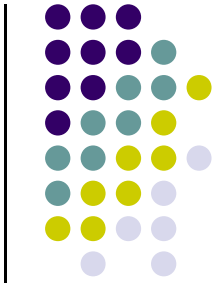
紀錄追蹤

6、對於調閱個人資料的人，加以記錄其調閱身分及行為。調閱紀錄可視機關實際需求存檔，以利後續人員查詢及追蹤。

審核公布

7、機關學校單位管理之網站或網頁內容，於確有必要公布個人資料時，需經所屬單位主管核准，且依相關法律及規範處理，才能公布。

設備管理須知



專人處理

1、應指定專人負責管理儲存個人資料的設備及設施，並檢查、處理設備的異常事件。

安全隔離

2、儲存個人資料之設備，應置放於安全區域，例如：門禁控管的辦公區域、機房等，避免有心人士或非授權人員存取。

委外監督

3、外部人員及個人，更新或維修電腦設備時，應指派專人在場，確保個人資料之安全，以及防止個人資料外洩。

徹底刪除

4、儲存個人資料之電腦或相關設備，如需報廢或移轉他用時，應確實刪除該設備所儲存的個人資料檔案。

人員管理須知

持續訓練

1、機關學校應對處理個人資料的人員，施予教育訓練，並定期於單位內宣導個資隱私保護之重要性。

帳密更換

2、處理個人資料之人員，其職務如有異動，應將所保管之資料移交。而接辦人員應重置通行碼，也應視需要更換使用者識別帳號。

權限取消

3、處理個人資料的人員，應簽訂保密切結書，並確認於離職或合約終止時，取消其使用者識別帳號，且收繳其通行證及相關證件。

個資法之校園案例

學校活動(社團)是否可透過信件寄發給所有學生? Who?

Yes

學校或社團辦活動可以透過信件寄發通知給學生，因為此舉符合學校教育及成立社團之特定目的。

Who

學校辦活動之單位、以及社團都可以寄發及使用學生的個人資料。

NG!

若學校活動是廠商的行銷活動，則有爭議空間；學校不可把學生資料給合辦活動的廠商來使用。

More

學校須評估學校使用學生個人資料之用途與目的，確認是否符合學校之「教育興學」目的，更謹慎的作法為與教育部討論，請教育部依學校教學需求，請法務部增修【特定目的】。

教授是否可要求助理、行政人員、電算中心提供學生資料?

Yes

老師因為教學所需（如與學生聯繫課業有關事項、了解學生家庭背景與能力等），可能會需要學生的個人資料。

No

學校負責保管資料的人員須判斷老師索取學生資料之目的，是否逾越教學必要範圍，以判斷是否提供。

More

建立個人資料調閱的申請與審核機制。

新生訓練是否是讓學生了解的恰當時機?

Yes

除非學校使用個人資料有可能超過教育行政之特定目的，否則是不需要學生額外授權的。

但因為新法增加了「告知」的義務，因此在學生入學時應立刻履行告知義務，詳述學校使用個人資料之範圍用途等。

More

如果學校對於學生的個人資料有逾越特定目的之利用，應及早告知學生並取得其「書面同意」。

畢業紀念冊上面的資料是否屬個人資料?

Yes

畢業紀念冊上的學生資料是屬於個人資料。

More

過去畢業紀念冊的收集與公開並非違法行為，但因為現在有越來越多的販賣個人資料或詐騙個人資料之行為，所以學校應改變個人資料之保管方式，就能加以控管限制閱覽畢業紀念冊的人員。

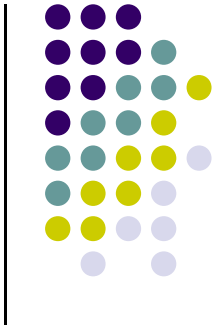
公司可否要求學校提供學生在學成績?

Yes

應由學生向學校提出申請，學生自行交付公司或由學校直接提供給公司。

No

學校無從判斷學生是否有到某公司謀職，所以不應主動提供學生在學成績。



資訊安全的迷思及觀念

台菲網路大戰
成功入侵菲國政府網站

大勝！台灣「匿名者」全軍出擊　成功斬首菲國政府網

ETtoday.net　ETtoday－2013年5月13日 上午8:09　-字 +字

政治中心／綜合報導

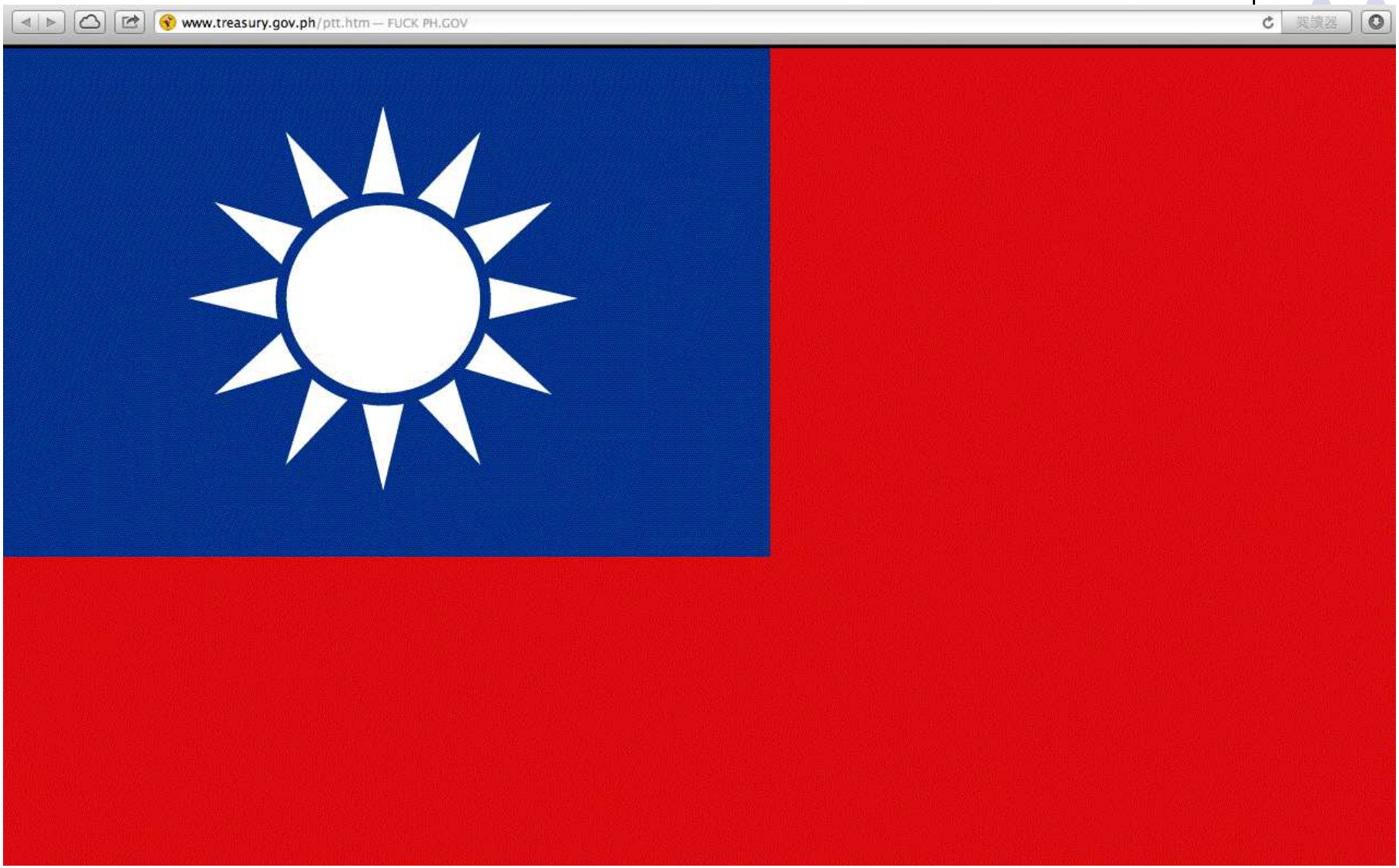
行家一出手，便知有沒有！台灣駭客13日凌晨成功攻破菲律賓網路防禦，全面控制菲國政府網站、電子郵件，換句話說，台灣在這場網路戰爭中搶先拿下一場漂亮的勝利。這個署名「匿名者－台灣分部」的駭客組織揚言，菲國政府若不道歉、逮捕濫殺台灣漁民的兇手，對菲國政府網站的攻擊將持續下去，「我們從不原諒，我們從不善忘」。

PTT鄉民10日「鍵盤開戰」，利用DDoS攻擊癱瘓多個菲國政府網站，立即引來菲國駭客以同樣方式還擊，灌爆我國總統府、經濟部等政府機關網站，菲國駭客「PINOY VENDETTA」還將戰果放在臉書上挑釁，要台灣人別太囂張。

未料2天後，「匿名者－台灣分部」(AnonTaiwan)就攻破了菲國政府網站，把所有頁面都換成了要求菲國道歉、交出兇手的聲明，「匿名者－台灣分部」在文末還指名道姓嗆聲「PINOY VENDETTA」，指他的不義行為將導致自我毀滅。

有網友形容，PTT鄉民的「鍵盤開戰」和「PINOY VENDETTA」的攻擊，像是跑到人家家門口狂按門鈴，按到對方覺得煩死了、受不了，乾脆把門鈴拆掉；但「匿名者－台灣分部」是成功控制所有掛上菲國政府網址的DNS，等於直接把對方大門拆掉，攻入大本營燒殺擄掠，若駭客有心要對菲國造成影響，後果恐怕非常嚴重。

台菲網路大戰
網頁入侵



中國信託疑出包，大量個資外洩

中國信託疑似出包？大量個資外洩！

05/13/2013 0 Comments

今天由PTT八卦版爆出，中國信託網站疑似將客戶個資外洩，由網址內進去便可以從選單中找到自己的電話…

最新消息：該網頁已經撤下，現在已經看不到當初流出的個資了；Google暫存的資料也已經遭到刪除，後續動作算是坐的相當完善。希望這段時間內那些資料沒有被不肖商人拿去利用。

從「常用繳費」選單中，可以看到約4000筆資料…大辣辣的公佈在網頁上！

〔圖片由板友提供〕

違反著作權

上傳音樂至部落格　女子違反著作權法遭判刑

2011/07/21 20:35 地方中心／新竹報導

字級 小 中 大 巨

隨便下載歌曲恐有觸法之虞，新竹一名女子日前被警方指控從youtube網站下載歌曲，上傳到自己的部落格播放，被網路警察發現後依照違反著作權法判刑四個月。

這名24歲的劉姓女子，因為從youtube網站下載了116首歌曲，被唱片公司以及網路警方巡邏查獲，並移送法辦。但劉姓女子卻宣稱，不知道自己從youtube上下載歌曲並上傳到部落格播放是違法行為，也強調許多網友都是從網路上下載免費的歌曲播放。

儘管劉姓女子辯稱歌曲只是作為自己欣賞用，但法官認為，被告將大量的歌曲放置網路上供網友觀看，已嚴重傷害了唱片公司的損失。另外，政府政策宣導中也常見關於「智慧財產權」的相關報導，法官表示劉姓女子不可能不清楚這是違法的行為。

為了省錢下載免費的音樂，劉姓女子相當後悔。法官依照違反著作權法，判處被告四個月的有期徒刑，如易科罰金，必須給予12萬元的罰金。新竹市刑大科技隊也呼籲民眾，千萬不要隨便亂下載音樂供網友點閱，以免觸法。

妨害電腦使用

大學姊妹淘不和 退課挨告

自由時報 自由時報 - 2013年5月15日 上午6:14

字 +字

〔自由時報記者王定傳／新北報導〕新北市某大學連姓女學生與張姓好友鬧翻，竟偷偷上網，把張女原本選好的「舞蹈」課程給退掉，張女發現後氣炸提告；新北地院法官念及連女犯後態度良好，未有前科，且張女僅表示要讓對方記取教訓，因而依妨害電腦使用罪，判連女罰金3萬元，緩刑2年，可上訴。

連、張本來是要好的同班同學，後因相處細節產生衝突，一方抱怨她生病時，對方沒來關心，導致鬧僵。去年8月間，連女偷偷上網輸入張女的選課帳號及密碼，將「女生體育- 舞蹈」課程退選，張女發現後提告。事發後，連女不斷道歉，表明後悔欲賠償，但張女仍然很氣憤，未達成和解，僅表示要讓對方記取教訓。

如何上網才安全？

如何上網才安全？Google 告訴你

Matt Kan

2012年5月16日 17:53

10 萬 讚 | 0 推薦 | 2 +1

記者甘偉中／台北報導

網路安全很重要，大家都知道，不過有多少人會主動去學習相關知識？某些用戶可能還以為裝了防毒軟體就百毒不侵。事實上，很多網路威脅的產生，是因為「使用者自己」對網路安全的觀念不清楚所導致。Google 過去幾個月分別在英國、德國及美國推出「不可不知（Good to Know）」網站教育網路用戶，分享簡易且可操作的資安常識，協助使用者保護自己在網路上的個人資訊，而這個網站目前也提供了中文版。

Google 推出「不可不知」網站教育網路用戶，分享簡易且可操作的資安常識，協助使用者保護自己在網路上的個人資訊（圖片取自／網路）

Google 今日（16）推出「不可不知（Good to Know）」網站包含中文在內的 30 種語言頁面，並將在未來幾週陸續支援其他 30 種語言。用戶可透過該網站學習如何在網路上保護自己的安全、了解網站如何解讀個人資料等，例如：設定高度安全的密碼、判別網路釣魚網站陷阱，以及強化個人帳號安全的兩步驟驗證等知識。

洩密
一張一億

「一張一億」　工程師洩4機密照遭償4億

TVBS – 2013年5月20日 下午12:15

字 +字

相關內容

「一張一億」　工程師洩4機密照遭償4億

「一張一億」　工程師洩4機密照遭償4億

台灣三星去年委託耕興公司新竹實驗室，測試當時還未上市的Galaxy S3原型機，一名洪姓工程師竟然將手機拍照上傳臉書，結果他不僅丟了工作，還被判刑半年，現在耕興公司，再以洩密造成商譽、營運受損，向這名工程師求償4億1300餘萬元的天價賠償，讓洪姓工程師根本不知道該怎麼辦。

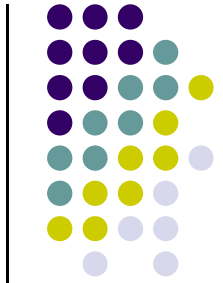
就是這幾張照片，讓洪姓工程師丟了工作，還吃上官司，但是更讓她痛苦的是，公司因為他洩密，造成商譽營運受損，求償4億1300多萬。洪姓工程師：「當初只是一時的好奇，沒想到鬧這麼大，自己也很後悔。」

4億1300多萬，對32歲的他來說，根本就是天價，一輩子也還不起，他懊悔的說，當初基於好奇，將手機外觀等4張照片上傳網路，沒想到事情鬧那麼大，PO上網的4張照片，現在一張等於就要一億元，一時的好奇衝動，讓他損失慘重。

資訊安全的迷思
修補所有系統弱點

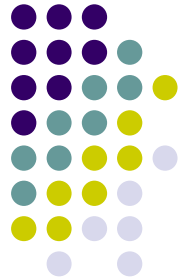
- 安全性弱點是一種產品瑕疵，它使產品無法防止(即使在正確使用產品的情況下) 攻擊者奪取使用者系統上的專用權、控制它的作業、洩露系統上的資料、或獲得未經授與的信任。
- 任何會導致應用程式、系統、設備或服務出現隱含或外顯的問題，都可被定義為弱點

資訊安全的迷思
防毒軟體無用論



- 防毒軟體功用
  - 即時掃描防護
  - 攔截病毒感染
  - 解除中毒的檔案
  - 個人防火牆
- 定時更新病毒碼

資訊安全的迷思
資安政策必需是全面性



- 資安政策越多越好?
- 資安政策越嚴密越能保護系統的安全?
- 資安政策涵蓋範圍越廣越好?

資訊安全的迷思
防火牆不防火?

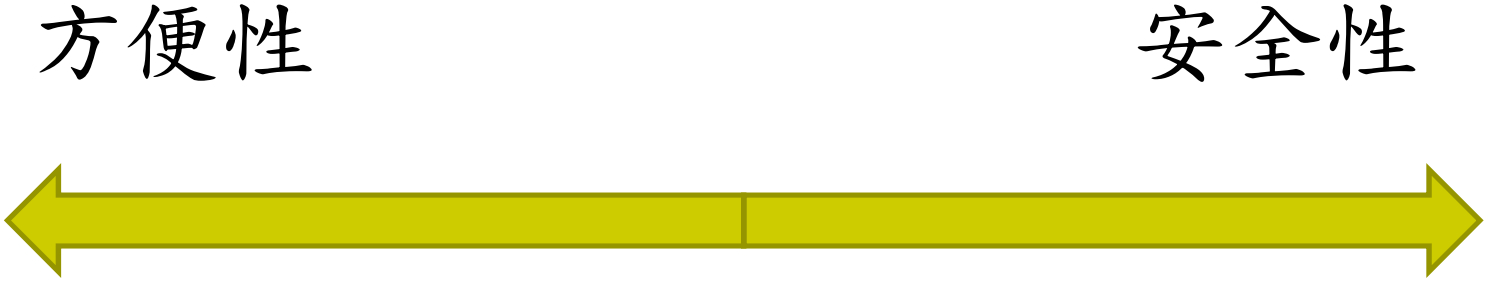
- 防火牆系統是一個網路安全設備，主要的功效為：
  - 安全政策執行
  - 網路路由轉換
  - 網路狀況管理
- 來源、目的、服務、動作

資訊安全的迷思
資訊安全是資訊人員的責任?

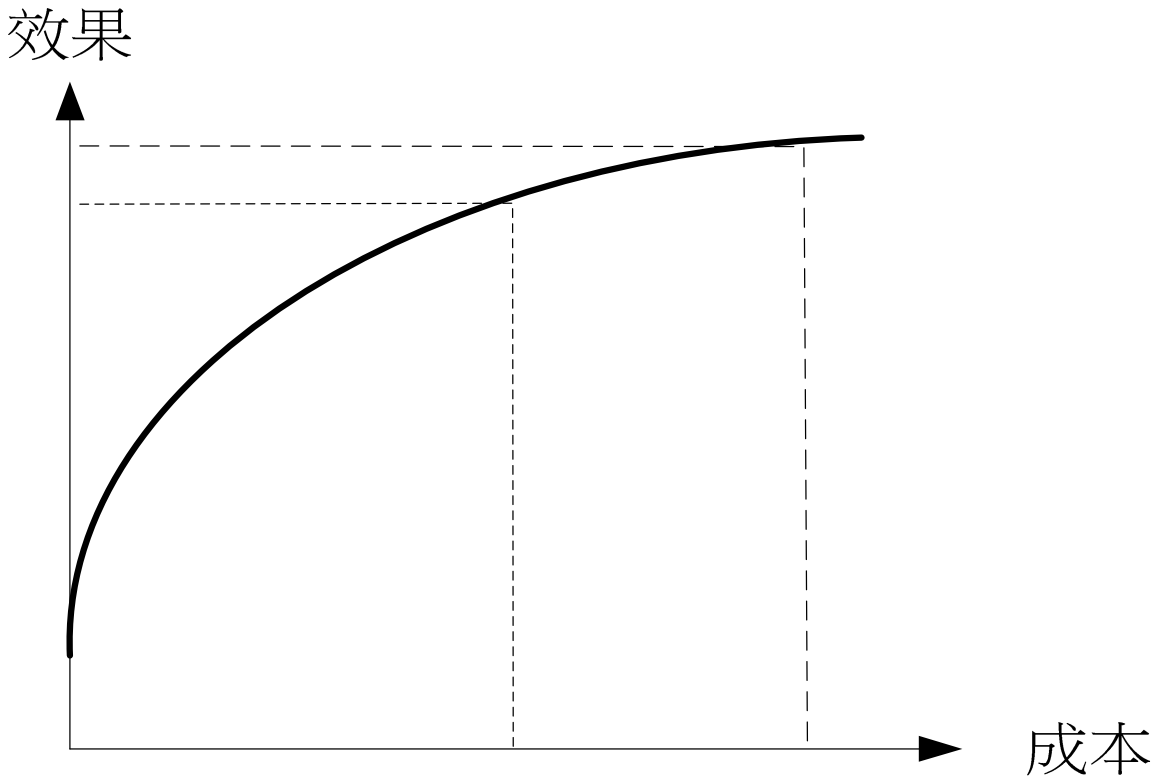
理想狀態

實際上

資訊安全的觀念
方便性與安全性

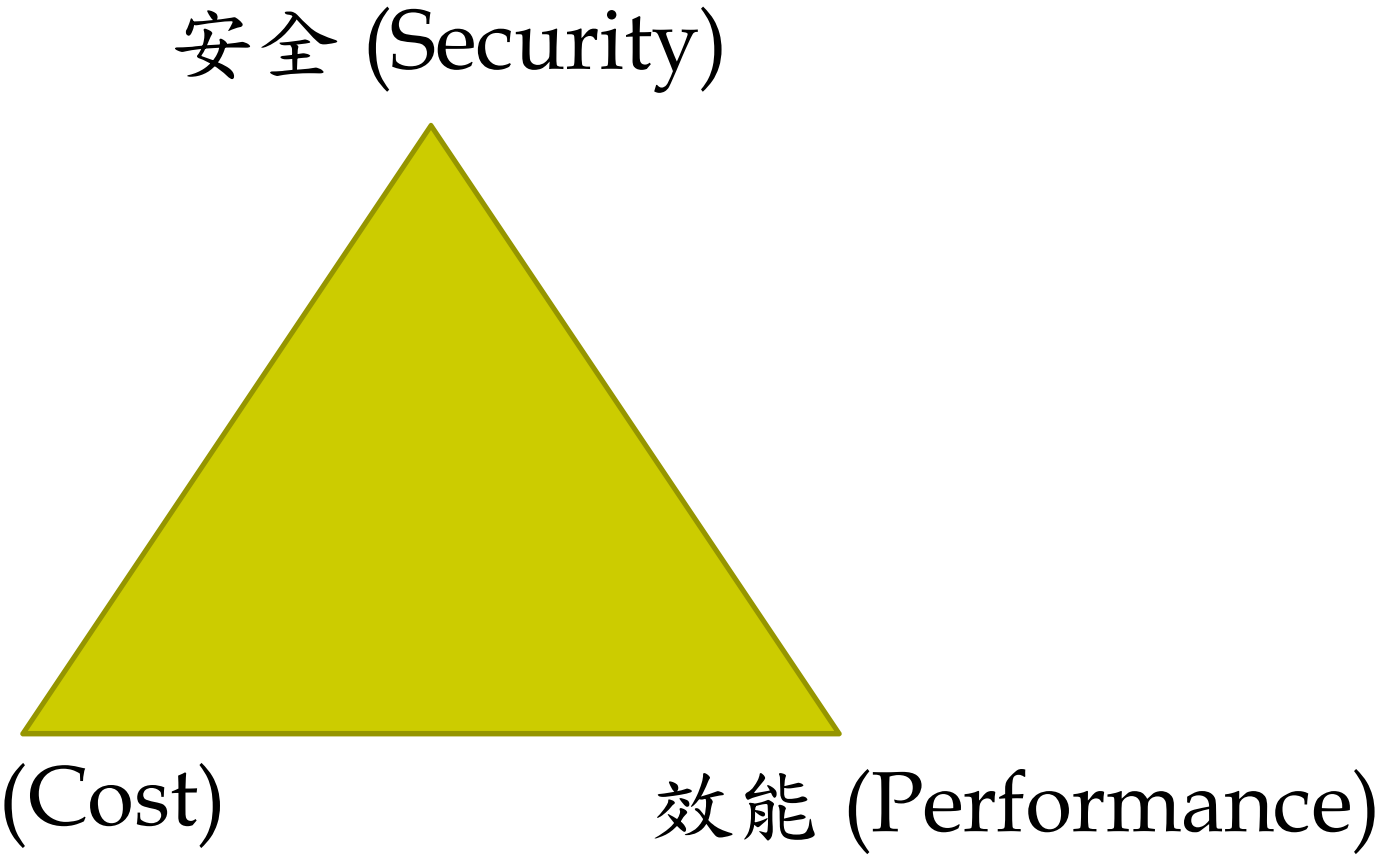


資訊安全的觀念
投資成本與效益

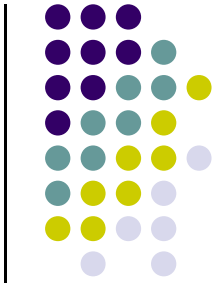


資訊安全的觀念

SCP

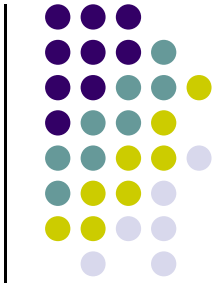


資訊安全的弱點



- 系統漏洞
- 人為疏失
- 過度於注重便利性
- 無危機意識
- 無所謂
- 實體環境防護不良

資訊安全的觀念

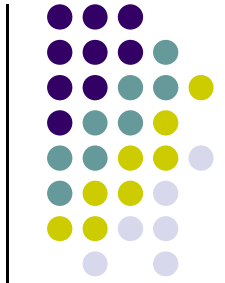


- 資訊安全是個持續性的工作。
- 看不見並不表示沒問題。
- 沒有100%的安全防護。
  - 增加攻擊的困難度
  - 增加攻擊的時間
- 資訊安全領域不只是網路安全而已，還包含機密性、完整性、可用性跟適法性。

資訊安全觀念

- 資訊安全，人人有責
- 沒有任何一項產品，可以提供100%的安全防護
- “怕”有兩種，“不怕”也有兩種

資訊安全需要長官們的全力支持



Q&A