雲端運算與資訊安全

漢昕科技：李仲捷

ISO27001、ITILV3.0、MCSE

Agenda

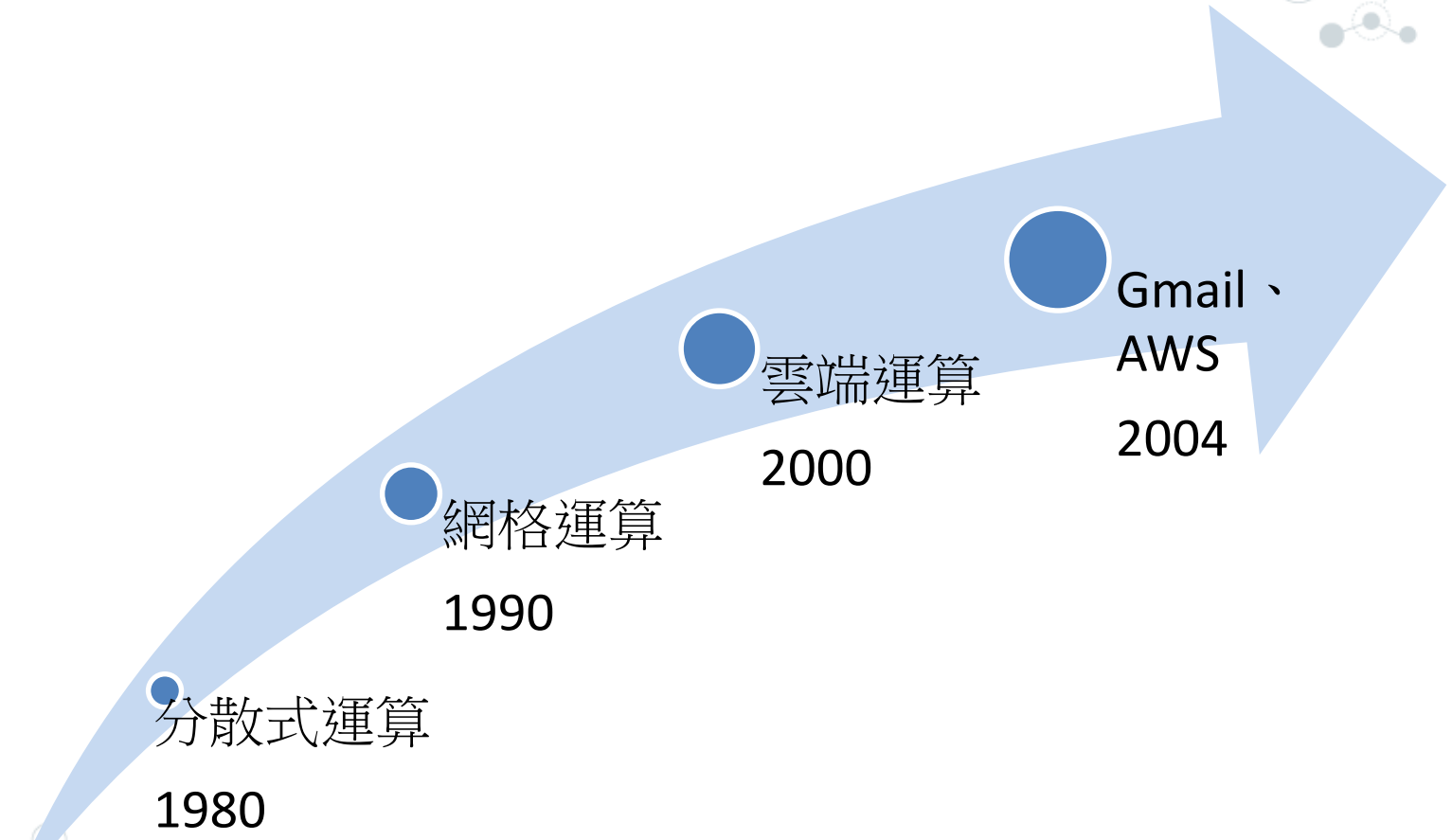
- 雲端基礎概念
- 雲端安全分析
- 雲端安全標準
- 雲端運算安全規劃
- 雲端應用安全

雲端基礎概念

雲端運算大事記

時間	事件
1960	大型主機開始用於商業運算
1969	網際網路的前身 ARPANET 誕生
1971	第一封 E-mail 由 ARPANET 寄出
1981	IBM 推出第一臺採用 Intel 8088 處理器的 IBM PC
1982	網際網路（Internet）誕生 Sun Microsystems 成立，提出「網路就是電腦」的概念
1984	蘋果電腦推出第一臺圖形介面的麥金塔
1991	Tim Berners-Lee 提出 World Wide Web（WWW）
1994	Amazon 成立
1997	雲端運算（Cloud Computing）一詞首度由 Ramnath Chellappa 教授提出
1998	Google 成立 x86 虛擬化廠商 VMware 成立
1999	Dot-com 興起，網路公司崛起 Salesforce 成立
2000	RSS 1.0 規格推出
2001	Dot-com 泡沫 IBM 提出自主運算（Autonomic Computing）
2002	部落格（Blog）開始出現
2004	Tim O'Reilly 提出 Web 2.0 概念 Google 提供 Gmail 服務 Amazon 提供 Amazon Web Services（AWS）雲端運算服務
2006	微軟提出「Software+Service」概念 Google 前執行長 Eric Schmidt 首度稱自家的服務是雲端運算
2008	相容於 AWS API 的開源雲端運算平臺 Eucalyptus 推出 微軟發表 Windows Azure 雲端平臺，由 VAX VMS 與 Windows NT 之父 Dave Cutler 坐陣開發 Salesforce 推出 Force.com 平臺 Google 推出 Google App Engine 平臺
2009	Oracle 執行長 Larry Ellison 公開指責雲端運算被炒作過頭了
2010	行政院通過「雲端運算產業發展方案」，5 年投入 240 億元
2011	美國聯邦雲端運算策略白皮書發布 工研院發表自製 Cloud OS Amazon 雲端運算服務大當機，歷時 3 天才恢復 蘋果推出 iCloud 雲端服務

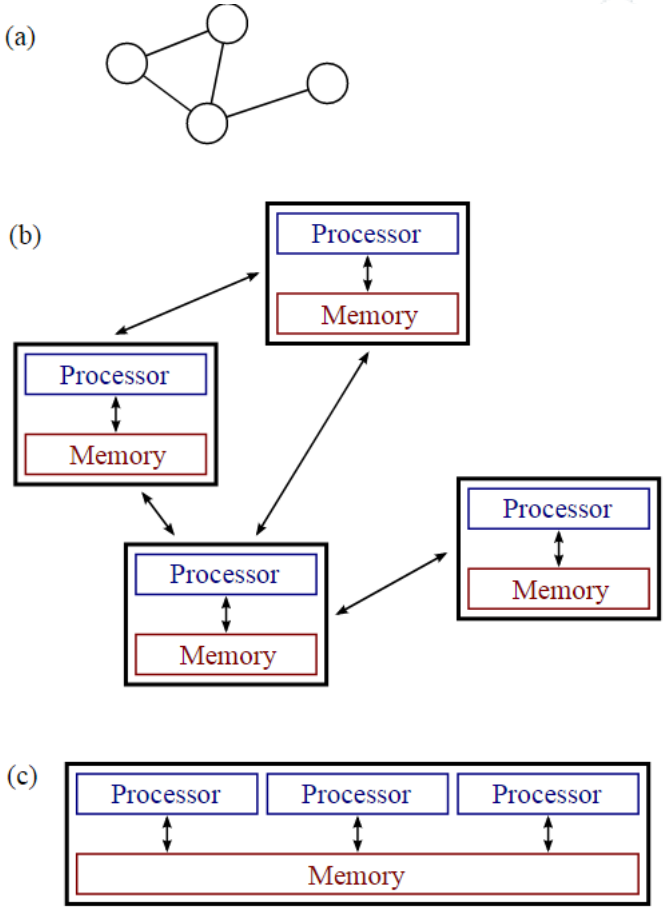
雲端運算技術演進



分散式運算

◎分散式運算（Distributed computing），這個研究領域，主要研究分散式系統（Distributed system）如何進行計算。分散式系統是一組電腦，透過網路相互連結傳遞訊息與通訊後並協調它們的行為而形成的系統。

◎元件之間彼此進行互動以實現一個共同的目標。把需要進行大量計算的工程資料分割成小塊，由多台電腦分別計算，再上傳運算結果後，將結果統一合併得出資料結論的科學。



分散式運算應用

- 對等是網路(P2P)
- 服務導向架構(SOA)：XML,HTTP(S)
- 大型多人線上遊戲
- 分散式運算專案

  - 通常使用世界各地上千萬志願者電腦的閒置計算能力，通過網際網路進行資料傳輸
    - Climateprediction.net：模擬百年以來全球氣象變化，並計算未來地球氣象
    - World Community Grid：幫助尋找人類疾病的治療方法，和改善人類生活的相關公益研究，包括愛滋病、癌症、流感病毒等疾病及水資源復育

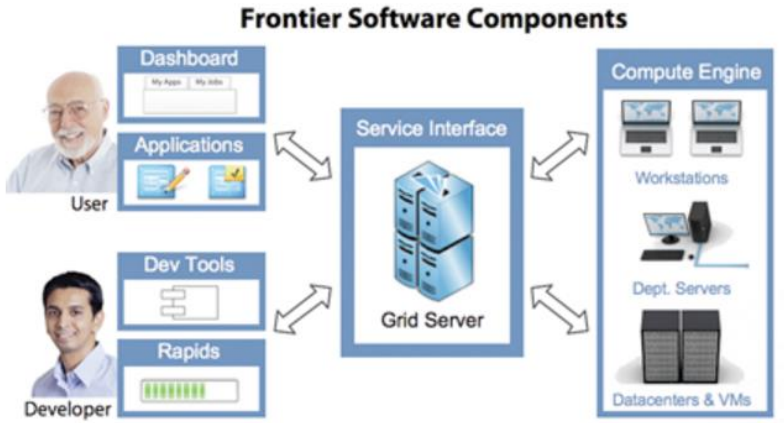
網格運算

- 網格計算（Grid computing）通過利用大量異構電腦（通常為桌上型電腦）的未用資源（CPU周期和磁碟儲存），將其作為嵌入在分散式電信基礎設施中的一個虛擬的電腦集群，為解決大規模的計算問題提供一個模型
- 網格計算的設計目標是：解決對於任何單一的超級電腦來說，仍然大得難以解決的問題，並同時保持解決多個較小的問題的靈活性。這樣，網格計算就提供了一個多用戶環境。它的第二個目標就是：更好的利用可用計算力，迎合大型的計算練習的斷斷續續的需求。

網格運算應用

- Parabon Computation
  http://www.parabon.com/
- Oracle Grid Engine

The **Frontier Grid Platform** is the collection of software used to manage our online Parabon Computation Grid utility HPC service. Packaged as Frontier Enterprise, it is the same solution we deploy for organizations wanting an in-house private grid. It's secure, OS-agnostic, unobtrusive and comes with a rich set of development tools to facilitate the rapid development of high-performance grid applications.



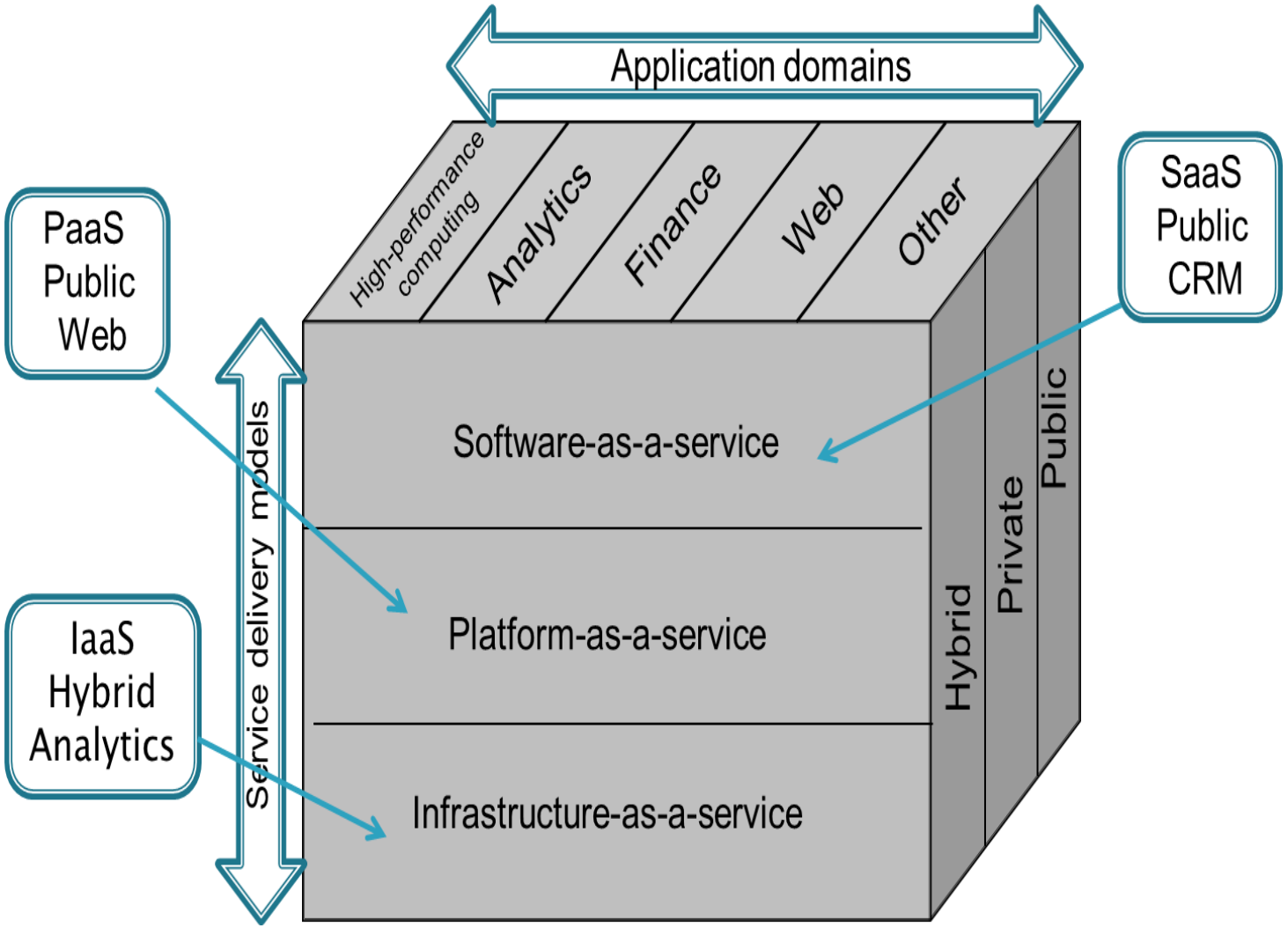
NIST雲端運算定義

iThome

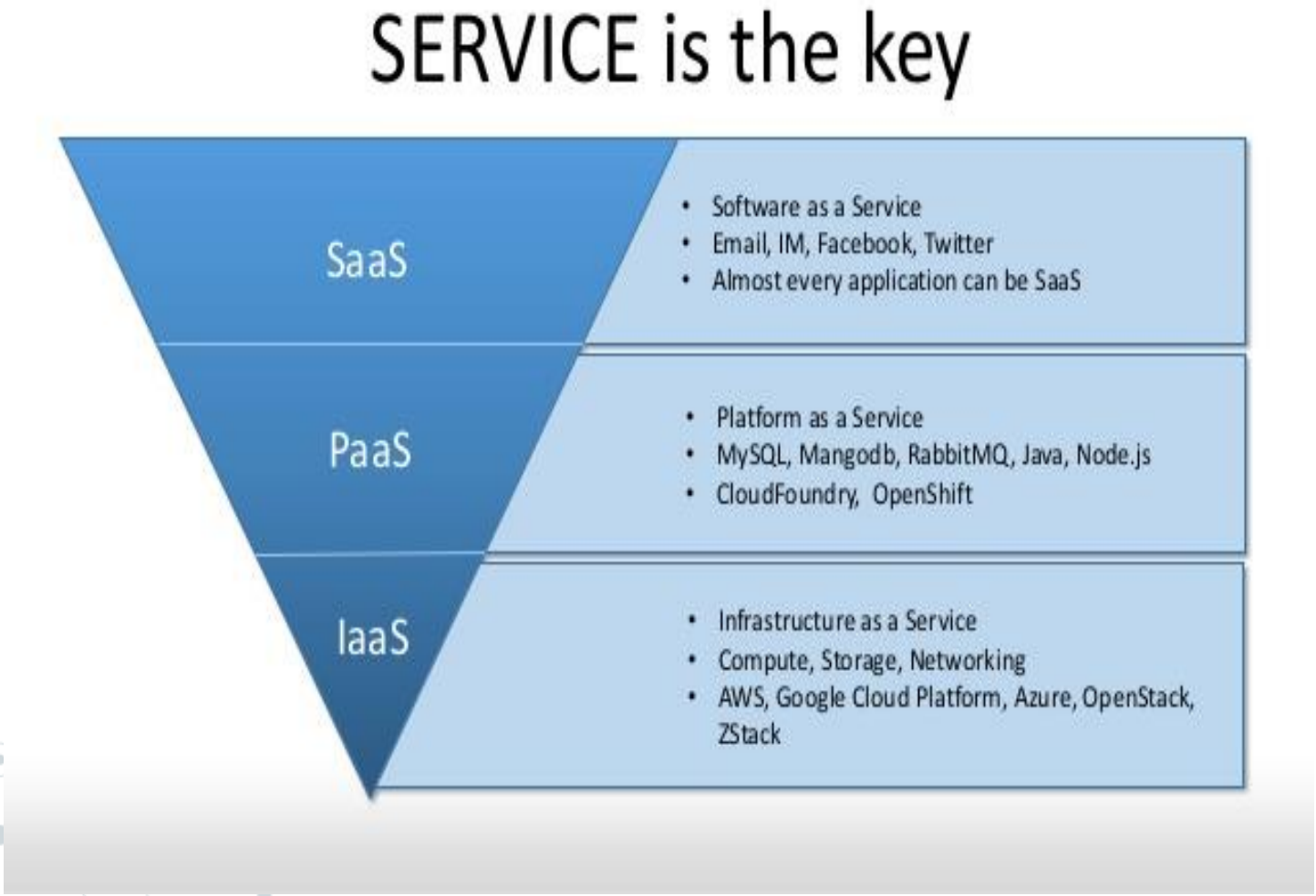
NIST定義雲端運算部署模式

- 公有雲（Public Cloud）：此種雲端運算架構是由銷售雲端服務的廠商所成立，對大眾或是大型的產業集團提供服務。
- 私有雲（Private Cloud）：此種雲端運算架構只為單一組織服務，可以是由該組織自己管理，或由第三方廠商管理，它可以部署在企業內，也可部署在企業外。
- 混合雲（Hybrid Cloud）：此種雲端運算架構，是結合2個或多個獨立的雲端運算架構（私有雲、社群雲或公有雲），藉由標準或是專屬的技術整合起來，讓資料與應用程式擁有可攜性。
- 社群雲（Community Cloud）：此種雲端運算架構是由多個組織共同成立，以服務擁有共同訴求與需求的群體。（例如有共同的任務、安全上的要求、政策與法規上的考量）它可以由這些組織或第三方廠商來管理，可以部署在組織內部或外部。

雲端服務SPI架構


Application domains
High-performance computing
Analytics
Finance
Web
Other
PaaS
Public
Web
SaaS
Public
CRM
Software-as-a-service
Platform-as-a-service
Infrastructure-as-a-service
Service delivery models
IaaS
Hybrid
Analytics
Hybrid
Private
Public

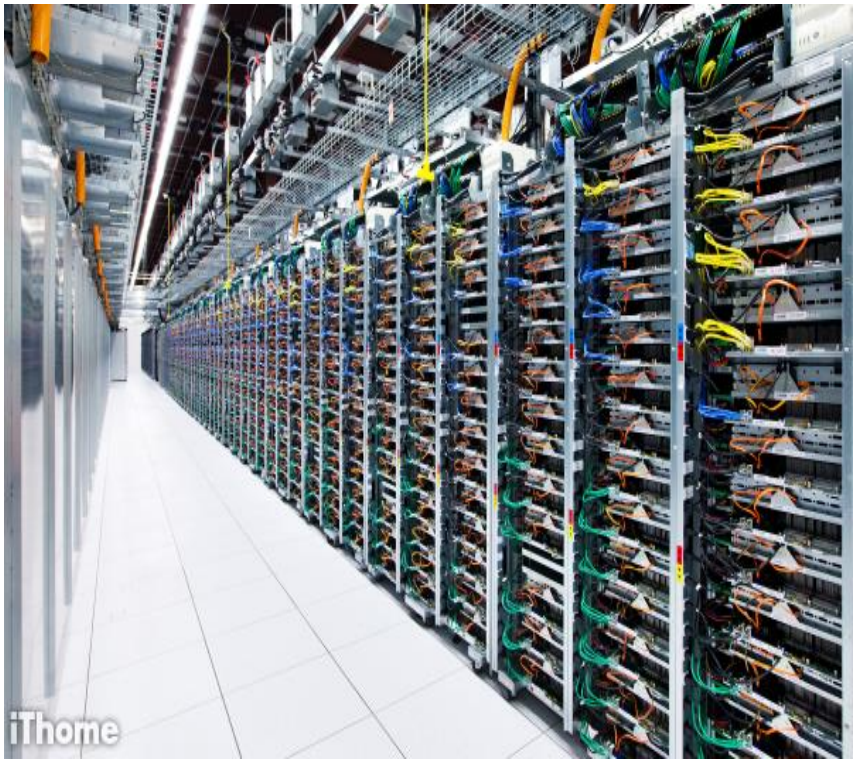
雲端運算服務架構


SERVICE is the key
SaaS
Software as a Service
Email, IM, Facebook, Twitter
Almost every application can be SaaS
PaaS
Platform as a Service
MySQL, Mangodb, RabbitMQ, Java, Node.js
CloudFoundry, OpenShift
IaaS
Infrastructure as a Service
Compute, Storage, Networking
AWS, Google Cloud Platform, Azure, OpenStack, ZStack

雲端服務類型

- 軟體即服務(SaaS)：位於三種服務最頂端，它可以讓使用者透過Web瀏覽器直接使用軟體服務，並以免費或按需求付費的方式向使用提供服務(e.g.Hotmail、Gmail)。
- 平台即服務(PaaS)：位於三種服務的中間層，是透過雲端業務提供商包裝的IT資源，可提供使用者程式開發的環境，把使用者建立或購入的應用程式部屬於此雲端平台服務上，無需管理網路，作業系統，儲存等設置(e.g.Google App Engine、Salesforce)。
- 基礎設施及服務(IaaS)：位於三種服務的最底端，最接近雲端運算基本定義的服務。雲端業務提供商把多台伺服器組成"雲"基礎設施作為服務提供給租用者，並以量計價(Amazon EC2、Microsoft Azure)。

Google Data Center



雲端運算的特性

多重租賃/共享資源 (multi tenancy)

Multiple users use the same resource in network level、host level and application level

極佳的擴充性 (Massive scalability)

Provides the ability to massively scale system、bandwidth and space.

彈性(elasticity)

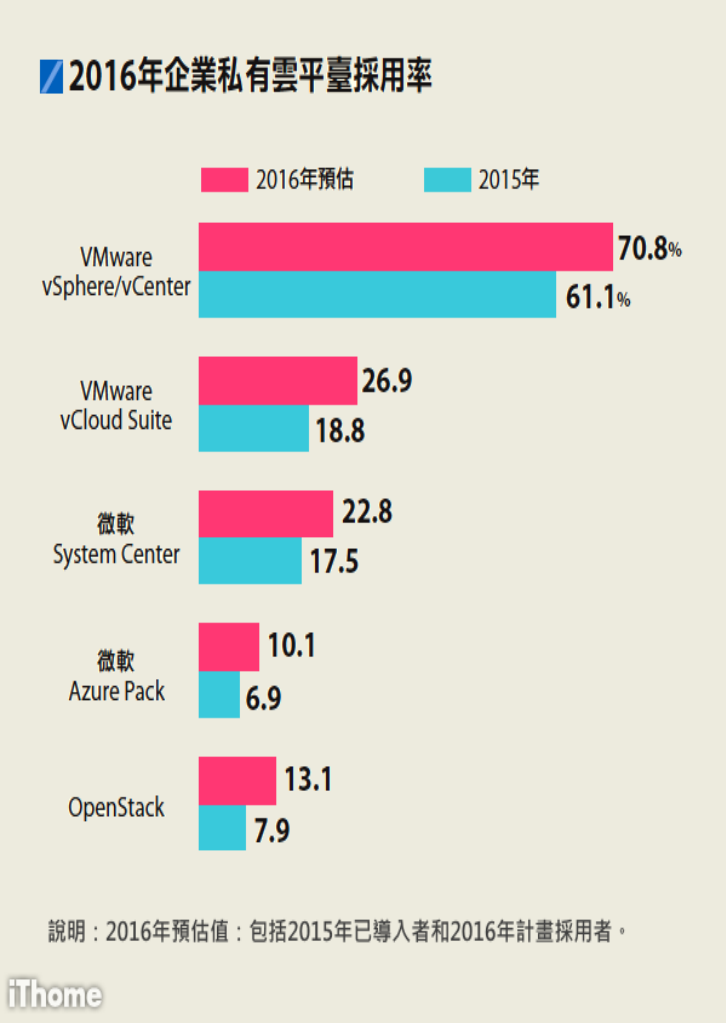
Users can rapidly increase and decrease their computing resources as they needed, as well as release resources to other users when they are no longer required.

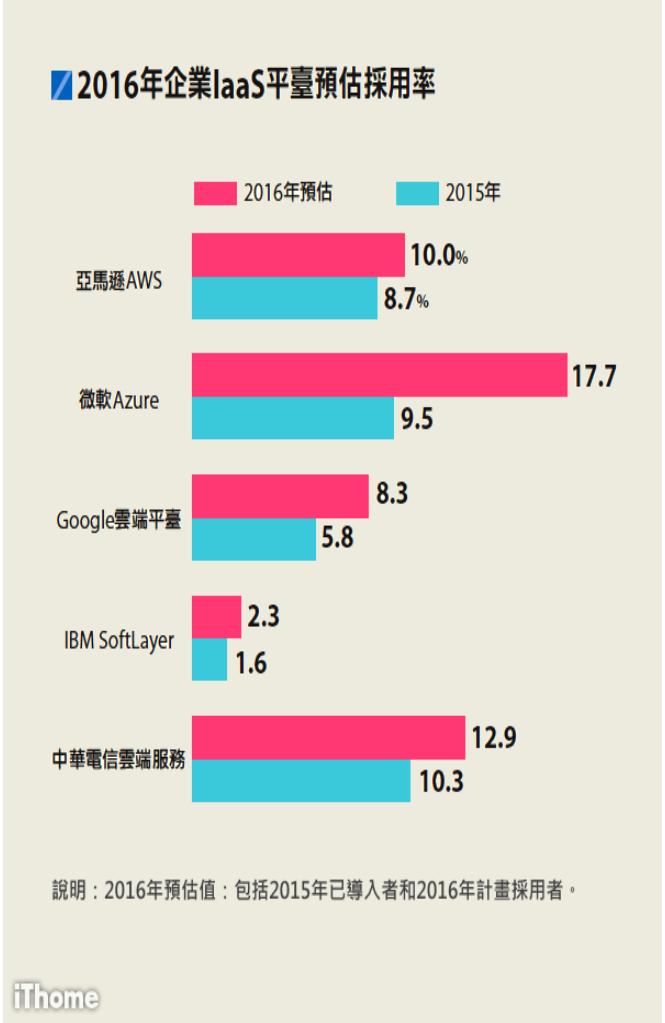
用多少付多少
(pay as you go)

Users pay for only the resource they actually use.

雲端運算應用情境示意圖

iThome 2016企業雲端部署調查





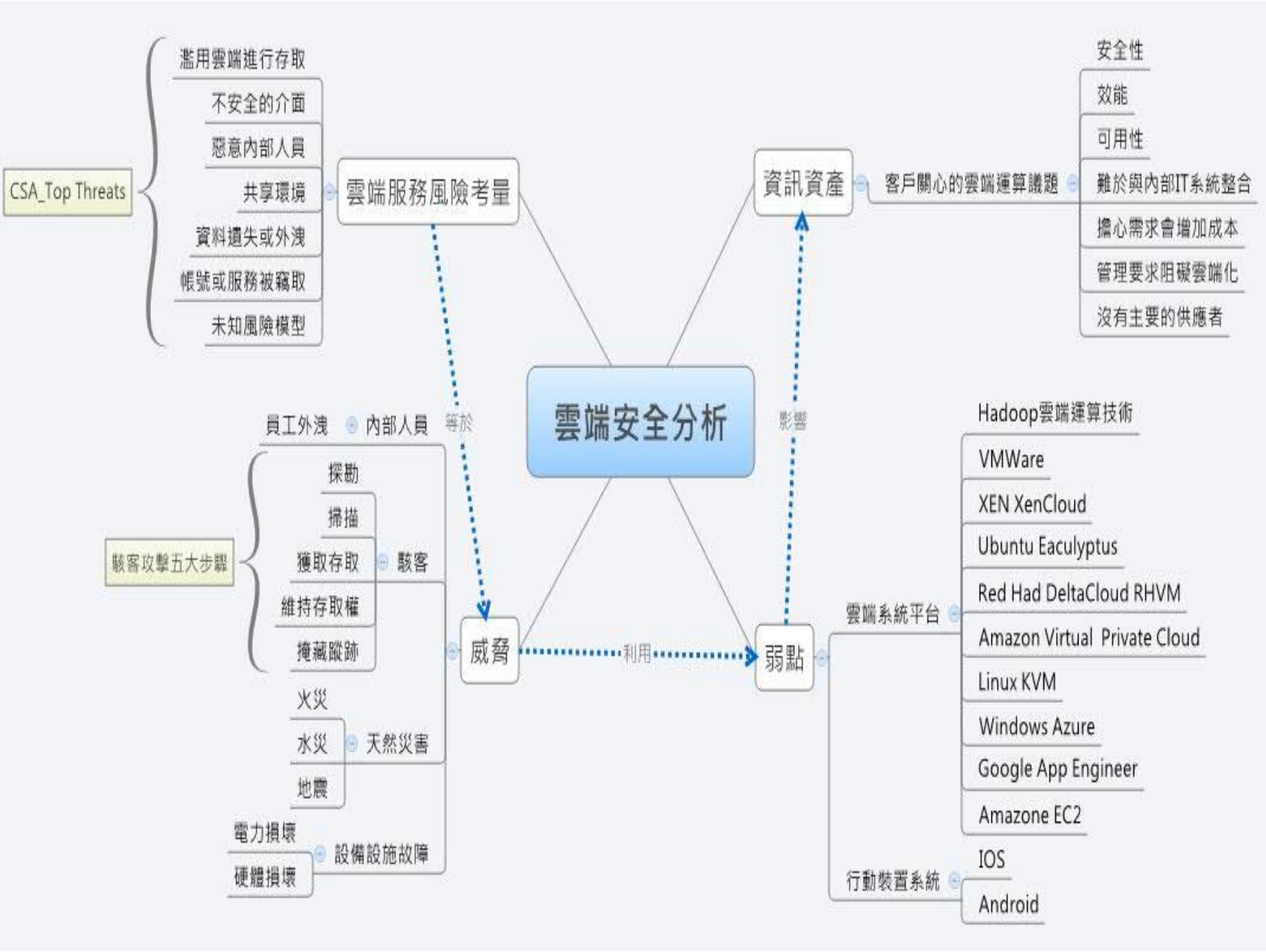
雲端的優點

- 低成本
- 免軟體、儲存空間、伺服器成本(免自購)
- 節能環保
- 節省設備維護人力
- 伺服器軟硬體升級容易
- 主機備份容易
- 使得安全稽核/測試更簡單
- 可運用雲端自動安全管理
- 簡化災難復原程序
- 將公開資料轉移到外部雲，減少暴露內部敏感資料的機會

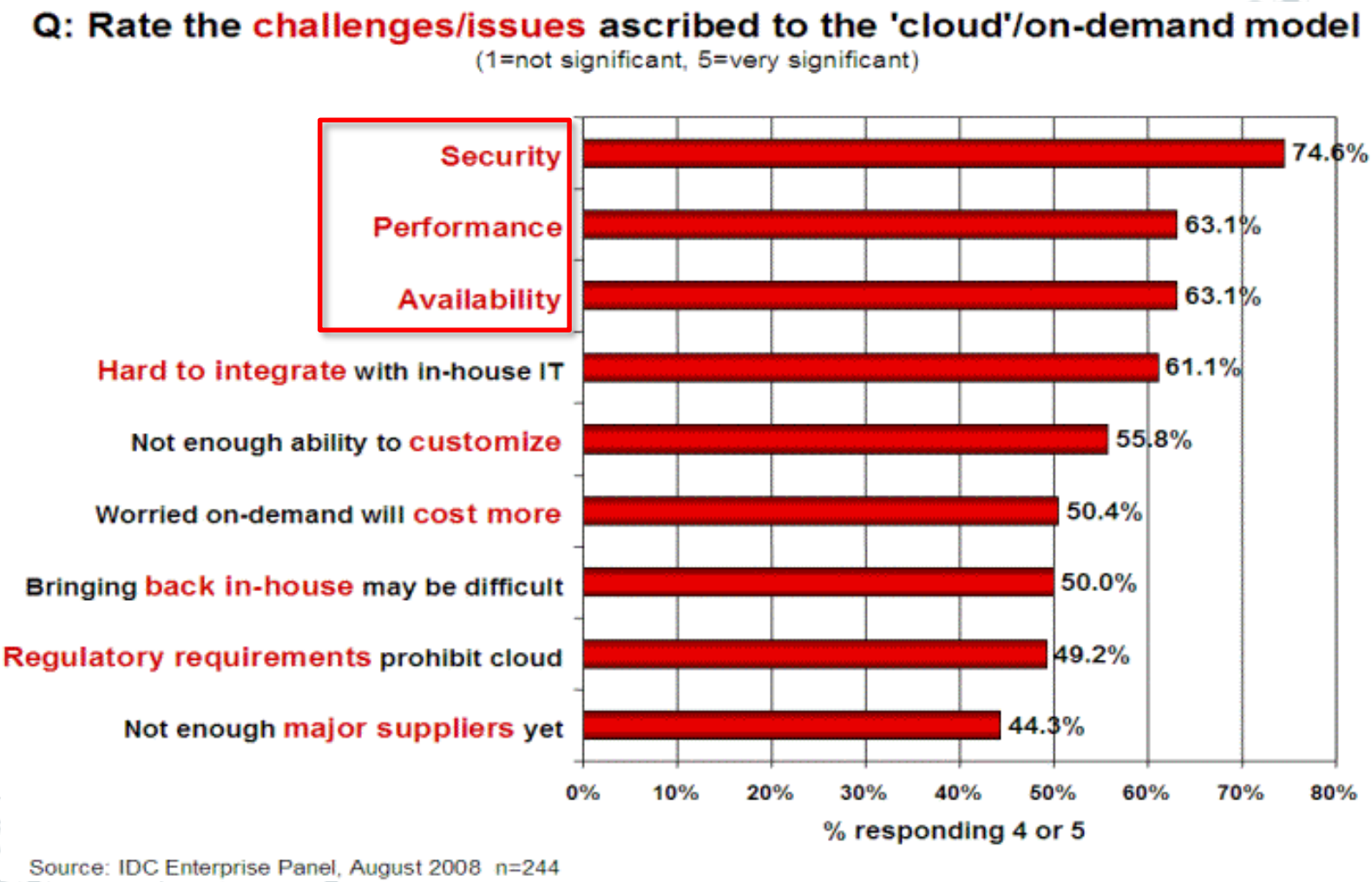
雲端的缺點

- 資料安全性
- 特殊使用者角色權限
- 法律規範，若有違法屬於誰！？
- 資料所屬位置（國家？）
- 資料隔離安全性
- 資料完整性（回復能力）
- 供應商永久性/供應商的安全模型
- 供應商隱私保護
- 喪失實體控制能力

雲端安全分析


雲端安全分析
雲端服務風險考量
濫用雲端進行存取
不安全的介面
惡意內部人員
共享環境
資料遺失或外洩
帳號或服務被竊取
未知風險模型
CSA_Top Threats
資訊資產
客戶關心的雲端運算議題
安全性
效能
可用性
難於與內部IT系統整合
擔心需求會增加成本
管理要求阻礙雲端化
沒有主要的供應者
等於
影響
威脅
內部人員
員工外洩
駭客
探勘
掃描
獲取存取
維持存取權
掩藏蹤跡
駭客攻擊五大步驟
天然災害
火災
水災
地震
設備設施故障
電力損壞
硬體損壞
利用
弱點
雲端系統平台
Hadoop雲端運算技術
VMWare
XEN XenCloud
Ubuntu Eaculyptus
Red Had DeltaCloud RHVM
Amazon Virtual Private Cloud
Linux KVM
Windows Azure
Google App Engineer
Amazone EC2
行動裝置系統
IOS
Android

企業最關心雲端運算的議題



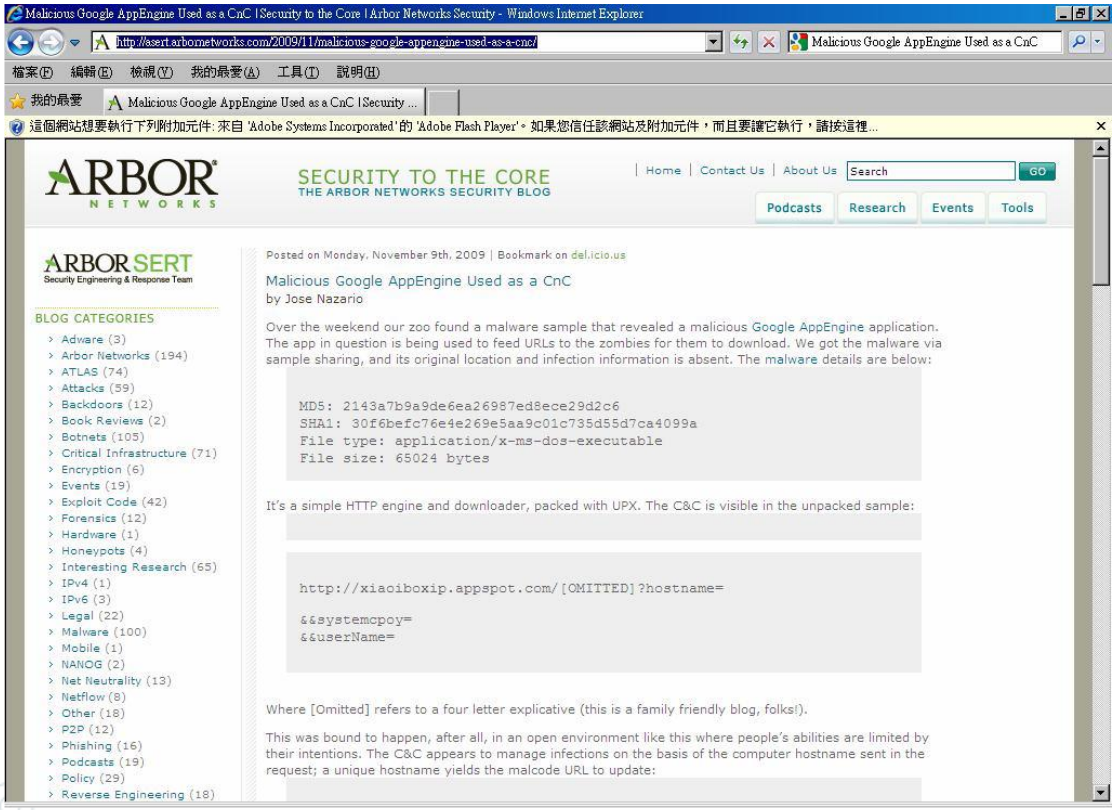
CSA Top Threats To Cloud Computing

- 透過雲端運算進行非法的行為
  (Abuse And Nefarious Use Of Cloud Computing)
- 不安全的應用程式開發介面
  (Insecure Interface And APIS)
- 惡意的內部人員
  (Malicious Insiders)
- 共享環境所造成的議題
  (Shared Technology Issues)
- 資料遺失或外洩
  (Data Loss Or Leakage)
- 帳號或服務被竊取
  (Account Or Service Hijacking)
- 未知的風險模型
  (Unknown Risk Profile)

透過雲端運算進行非法的行為

- 此威脅主要是針對雲端運算服務的供應者。惡意者透過雲端服務供應商提供的資源來進行惡意攻擊或是非法行為。
- 例如:殭屍電腦、散播木馬程式、分散式阻斷服務攻擊。

透過Google App Engine傳遞殭屍網路指令



駭客利用Amazon EC2傳遞殭屍網路指令

不安全的應用程式開發介面

- 使用者需透過雲端服務供應商提供的使用者介面或是應用程式與雲端業者進行互動，因此這些介面與應用程式安全與否會間接或直接的影響到雲端運算服務本身的安全性。
- 例如:使用者介面驗證與授權功能、應用程式相容性。

Web應用程式弱點範例說明

	弱點名稱	成因與攻擊方式	造成之影響
1	參數竄改	程式設計者藉由隱藏欄位傳遞數值，卻沒有進行檢查，導致駭客可修改欄位數值傳送僞造資料。	駭客得以傳送僞造資料，變更成網站交易行爲。
2	跨站指令碼	網站程式允許使用者將輸入的資料顯示在網站上，卻沒有過濾輸入資料。	讓惡意攻擊者可以將惡意的javascript程式碼塞入網站上，影響其他無辜的瀏覽者。
3	SQL 程式碼注入	網頁程式沒有過濾特殊字元，駭客得以控制後端資料庫。	可將資料庫資料竊出，嚴重者可取得資料庫主機的控制權。
4	跨目錄存取	網頁程式沒有過濾特殊字元，駭客得以輸入特殊跳脫字串，瀏覽檔案。	可瀏覽 Web 主機檔案，嚴重者可因此取得系統控制權。
5	指令插入	網頁程式沒有過濾特殊字元，駭客得以輸入特定字元加上命令，對伺服器下達指令。	可針對Web主機下達指令，嚴重者可因此取得系統控制權。
6	目錄瀏覽	伺服器設定不當，駭客可列出網站目錄下的所有檔案。	可能將目錄下的機密檔案列出。

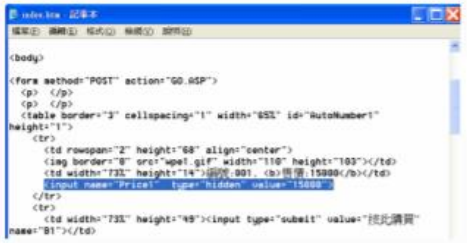
參數竄改問題


編號:001, 售價:15000
按此購買
編號:002, 售價:12300
按此購買
編號:003, 售價:9000
按此購買
編號:004, 售價:11000
按此購買
駭客的直覺反應：
按右鍵檢視原始檔
看是否有隱藏欄位
（hidden field）

修改隱藏欄位

檢視網頁原始檔， 駭客發現可能有隱藏欄位問題

將原始檔另存到本機端



修改隱藏欄位內容

```
<form method="POST" action="http://IP/XX/GO1.ASP">
…
<td width="73%" height="14">編號：001， <b>售價：15000</b></td>
<input name="Price"  type="hidden" value="100">
```

用瀏覽器開啓並且發送

修改成便宜的價錢，100元！

SQL Injection

SQL 程式碼注入弱點
（SQL injection）

- 程式開發人員未過濾輸入字串，駭客藉由跳脫字元可避開認證。

  - 程式碼：

    Select FIELDS from table where user='$user' and pass='$pass'
  - 駭客輸入：

    user：『' or ''='』，pass：『' or ''='』
  - 程式判斷則變成：

    Select FIELDS from DB where user='' or ''='' and pass='' or ''=''

    ⇨ 避開認證！！

惡意的內部人員

- 客戶使用雲端時並無法得知雲端服務供應商的內部人員安排，就資料的保密性而言除了要擔心雲端服務供應商遭受到外部的惡意威脅之外，也要擔心到資料儲存雲端時，雲端內部的員工因為其他因素竊取這些資料的風險。

- 根據Datapro Research Corporation的資安調查，約有5成的資安事件是由人為失誤所造成，加上離職員工或內部犯罪所佔1成，人為因素造成資安事件所佔的比例高達6成。

共享環境所造成的議題

- 雲端服務供應商在提供客戶使用時，使用者所使用的虛擬環境有可能是由許多不同類型客戶共享同一個實體環境，因此在虛擬化的環境下，雲端服務供應商是否能有效的隔離不同使用者，以避免彼此之間造成干擾，而造成其他客戶權利受損，也是十分重要的議題之一。

資料遺失或外洩

- 使用者使用雲端時，最擔心的安全之一就是資料外洩或是資料遺失。因此雲端服務供應商對於資料的處理方面，除了要能採用適當的加解密技術之外，對於認證、授權、使用上也必須額外的注意。
- 就資料遺失的部份除了受到攻擊之外，也有可能是雲端設備受到天災或是硬體故障等問題，因此資料的備份、異地救援也是十分重要的關鍵

帳號或服務被竊取

- 帳密管理對於傳統網路或是雲端服務來說都是十分重要的議題，然而對於雲端服務來說，假設有心人士取得使用者帳密之後，即可進行資料存取控制，或是進行惡意的攻擊。例如：故意放入病毒碼透過雲端內共享資機制導致其他用戶中毒或是利用竊取到使用者身分進行非法的行為等。

Yahoo 用戶帳號被竊

iThome

新聞 產品評測 技術 專題 Big Data Cloud DevOps 資安 Video 研討會 社群

搜尋

新聞

Yahoo坦承兩年前遭駭客入侵，至少5億用戶帳號被竊

Yahoo證實在2014年曾遭到駭客入侵，竊取至少5億筆用戶資料，包括帳戶、電子郵件、電話、生日，以及部份用戶的安全問題與回答已外流，Yahoo呼籲2014年以後未變更密碼的用戶更改密碼。

讚 4 萬 按讚加入iThome粉絲團 讚 535 分享 G+1 2

文/ 林妍溱 | 2016-09-23 發表

未知的風險模型

- 由於在使用雲端時，除了前面介紹的威脅之外，還有許多未知的資訊是使用者所不知道，例如雲端業者所使用的網路架構是否安全、軟體版本是否有即時更新等，許多層次的方面還是充滿許多未知，這些的未知相對於使用者來說就是無形的風險存在。

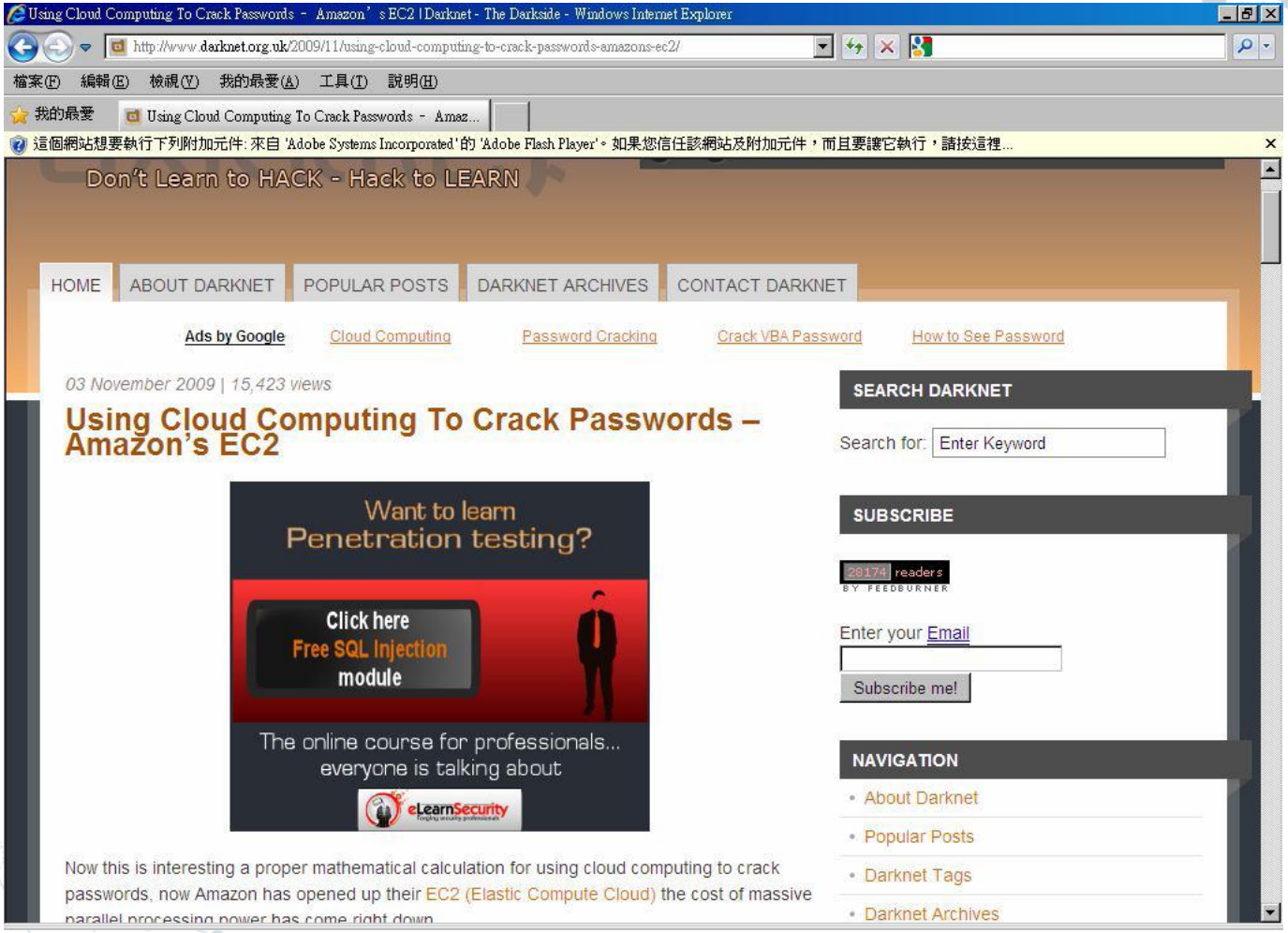
駭客如何看待雲端

- 犯罪服務平台CaaS (Cybercrime as a service)
  - – 殭屍網路(botnet)的溫床
  - – 超便宜密碼解破平台
  - – DDOS的發動源頭
  - – 無限的資料可以偷
- – ……

駭客攻擊流程


Hacking Phases
Reconnaissance
Scanning
Gaining Access
Maintaining Access
Clearing Track

比超級電腦成本低很多的EC2



人人都愛用的Google
當然包含駭客

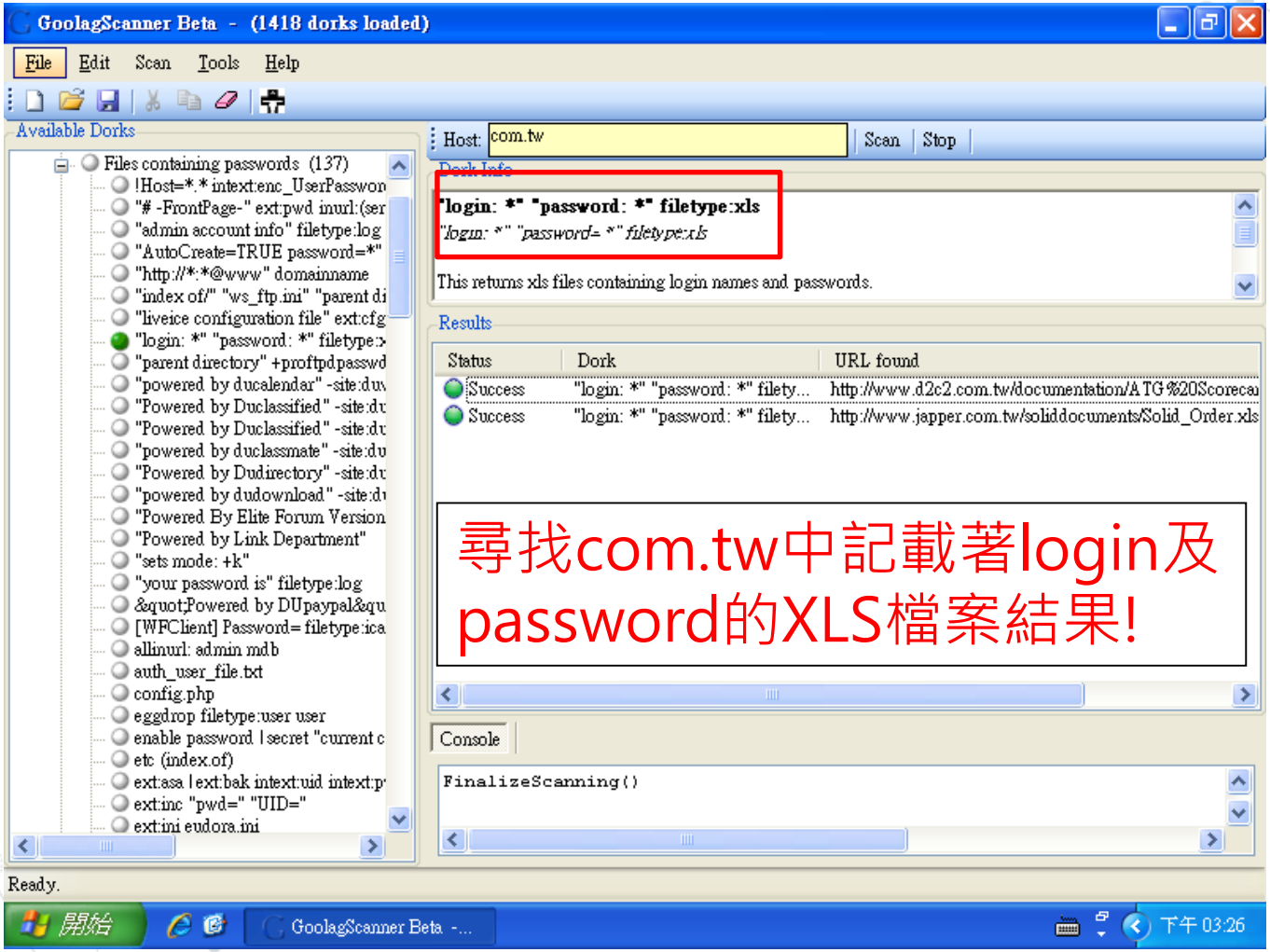
Goolag Scanner

- Advisories and vulnerabilities
- Error messages
- Files containing juicy info
- Files containing passwords
- Files containing usernames
- Footholds
- Pages containing login portals
- Pages containing network or vulnerability data
- Sensitve Directories
- Sensitive Online Shopping Info
- Various Online Devices

Goolag Scanner(cont.)

- Vulnerable Files
- Vulnerable Servers
- Web Server Detection
- By Arrakis

記載著登入密碼的網頁


GoolagScanner Beta - (1418 dorks loaded)
File Edit Scan Tools Help
Available Dorks
Files containing passwords (137)
!Host=*.* intext:enc_UserPasswon
"# -FrontPage-" ext:pwd inurl:(ser
"admin account info" filetype:log
"AutoCreate=TRUE password=*"
"http://*:*@www" domainname
"index of/" "ws_ftp.ini" "parent di
"liveice configuration file" ext:cfg
"login: *" "password: *" filetype:x
"parent directory" +proftpdpasswd
"powered by ducalendar" -site:du
"Powered by Duclassified" -site:du
"Powered by Duclassified" -site:du
"powered by duclassmate" -site:du
"Powered by Dudirectory" -site:du
"powered by dudownload" -site:du
"Powered By Elite Forum Version
"Powered by Link Department"
"sets mode: +k"
"your password is" filetype:log
"Powered by DUpaypal&qu
[WFClient] Password= filetype:ica
allinurl: admin mdb
auth_user_file.txt
config.php
eggdrop filetype:user user
enable password | secret "current c
etc (index.of)
ext:asa | ext:bak intext:uid intext:p
ext:inc "pwd=" "UID="
ext:ini eudora.ini
Host: com.tw
Scan
Stop
Dork Info
"login: *" "password: *" filetype:xls
"login: *" "password= *" filetype:xls
This returns xls files containing login names and passwords.
Results
Status
Dork
URL found
Success "login: *" "password: *" filety... http://www.d2c2.com.tw/documentation/ATG%20Scoreca
Success "login: *" "password: *" filety... http://www.japper.com.tw/soliddocuments/Solid_Order.xls
尋找com.tw中記載著login及password的XLS檔案結果!
Console
FinalizeScanning()
Ready.
開始
GoolagScanner Beta -...
下午 03:26

Android App潛藏開放埠漏洞

新　聞

研究：數百款Android程式潛藏開放埠漏洞，允駭客偷走手機內的資料、控制裝置

密西根大學研究團隊掃描Google Play上使用開放埠的行動程式，發現其中有410款沒有妥善保護開放埠安全，另以手動檢視確認有開放埠漏洞的則有57款，可能導致駭客遠端入侵裝置竊取資料。

惡意程式假冒遊戲攻略滲透 Google Play

iThome

新聞 產品評測 技術 專題 Big Data Cloud DevOps 資安 Video 研討會 社群

搜尋

新聞

惡意程式假冒遊戲攻略滲透Google Play，200萬Android裝置恐遭感染

FalseGuide多藏身於網路或手機遊戲指南App，利用玩家尋找遊戲秘笈的心理誘騙下載，一旦使用者下載後會要求玩家開放系統權限，藉此播放廣告或建立殭屍網路，進一步可能發動DDoS攻擊或入侵企業內網。

讚 4 萬 按讚加入iThome粉絲團 讚 321 分享 G+1 4

文/ 陳文義 | 2017-04-26 發表

惡意軟體透過雲端儲存竊取用戶銀行資訊

標題	[國際]惡意軟體 CloudFanta，透過雲端儲存 APP 竊取用戶銀行資訊
發佈日期	2016-10-28 16:05:48
參考位址	http://securityaffairs.co/wordpress/52750/malware/cloudfanta-malware.html https://resources.netskope.com/h/i/297473838-cloudfanta-malware-campaign-technical-analysis

消息內容

1. 資安專家分析，自今年七月起至今，惡意軟體 CloudFanta 疑似成功竊取 26000 組有效 Email 帳密。
2. CloudFanta 主要以釣魚郵件方式，透過附件或連結誘使用戶點選，藉由下載 SugarSync 雲端儲存 APP 以進行資料探勘。
3. 專家分析釣魚郵件目的為連結至“https[:]//www[.]sugarsync[.]com/pf/D3202366_07280196_66523?directDownload=true.”。
4. 該連結所自動下載的壓縮 ZIP 檔包含一個雙副檔名“.PDF.JAR”的下載器，若誤認為 PDF 開啟，便會暗地下載 DLL 檔至 "C:\users\public\[username]"。
5. 而 DLL 檔的副檔名偽冒成“.PNG”並使用SSL / HTTPS通訊協定，以躲避防火牆及其他入侵偵測系統，並隨後將檔名改為主機名加附檔名“.TWERK”。
6. 這些 DLL 檔案就是負責竊取受害者的電子郵件帳密，並代表受害者發送釣魚電子郵件，同時監看受害人的網路銀行活動。
7. 當受害者連結的電子郵件服務在監控範圍中，如 Gmail，便會重新導向至偽造的頁面以擷取帳密並傳送至 C&C 後才再導向回原來官方的登入頁面。
8. 而在使用網路銀行為避免鍵盤側錄，啟用虛擬鍵盤時，則會被偵測到，並開始在每次的滑鼠點擊時儲存畫面及以文字檔紀錄在“C:\Users\Public\[username]\alfa”，以便駭客查看。

遊戲APP社交工程手法

標題	[國際]看似 Google Play 要求上傳手持身分證的自拍照，切勿輕信!
發佈日期	2016-10-17 11:18:59
參考位址	http://news.softpedia.com/news/android-trojan-asks-victims-to-submit-a-selfie-holding-their-id-card-509303.shtml

消息內容

●重點摘要：
1. 資安專家發現網路銀行木馬 Acecard ，再度變種出現新的社交工程手法。
2. 在之前的版本，該木馬通常藏在某個21點遊戲 APP，並透過 Google Play 散播。
3. 而新版木馬會假扮成各種第三方的APP，諸如 Adobe Flash Player、pornographic apps 或影片解碼器等。
4. 當使用者安裝後，會不斷跳出權限許可要求畫面，直到使用者最後按下同意，而那其實就是管理員權限。
5. 隨後木馬會靜待直到使用者開啟 Google Play 的 APP 時才開始動作，藉以讓使用者誤信為 Google Play 所跳出的要求。
6. 首先會跳出要求輸入有關信用卡的各項細節，接著要求使用者拍下並上傳身分證正反面及手持身分證的自拍照。
7. 資安專家表示，駭客可藉此確認受害者身分，除了可有效存取銀行帳戶之外，更能透過社交軟體假冒或挾持受害者帳號以圖利。

●TWCERT/CC 建議不要輕易下載使用第三方 APP，且當跳出不合理要求的視窗如上傳機敏資料等照片，請小心警慎，以免遭駭客利用。

Google網址參數潛藏危機

標題	[國際] Google網址參數潛藏危機，登入網址可被利用轉傳惡意網站或檔案
發佈日期	2016-09-02 14:04:16
參考位址	http://www.businessinsider.com/google-login-page-phishing-2016-8 http://unwire.pro/2016/09/01/google-parameter-phishing/news/ https://www.aidanwoods.com/blog/faulty-login-pages

消息內容

●重點摘要：
1. Google 登入網址的 continue 參數值用於決定用戶登入後自動前往的網址。
2. 對於登入後轉址，Google 已設定白名單，僅 Google 域名的網址才可轉址。
3. 然而資安專家表示，只要在continue 參數值改為https://www.google.com/amp/[any_domain_here]
4. 在使用者輸入正確之帳號密碼按下登入後，即會被轉址至參數所指定之網址。
5. 因此當駭客在參數後面指定一個模仿登入畫面的釣魚網站，要求使用者再次輸入帳密，即可能藉此取得登入憑證。
6. 另外 continue 參數亦可插入 Google Doc 檔案連結，便可能利用使用者登入時自動下載特製的惡意檔案。
7. 然而資安專家表示已經將此情況通知 Google，但 Google 選擇不做任何事情。。

●TWCERT/CC建議，用戶在登入後出現要求重新輸入帳密或其他個人資訊時，請務必重複確認網址是否仍來自google.com，並在登入前確認網址尾端是否有不正常連結。

漏洞公告平台

Common Vulnerabilities and Exposures

The Standard for Information Security Vulnerability Names

CVE in Use

As the international industry standard for cybersecurity vulnerability and exposure names, CVE Identifiers are included in numerous products and services and are the foundation of others.

CVE Compatibility

U.S. National Database (NVD)

Community

Government

CVE COMPATIBILITY

Products and services can be made "CVE Compatible" by following the Requirements and Recommendations for CVE Compatibility. Numerous organizations from around the world already include CVE IDs in their capabilities, processes, products, services, etc.

Examples of enterprise security areas enhanced by CVE Compatibility include the following:

- Vulnerability Management
- Vulnerability Alerting

U.S. National Vulnerability Database (NVD)

Launched by the National Institute of Standards and Technology (NIST) in 2005, NVD provides a vulnerability database of enhanced CVE content that is fully synchronized with the CVE List, so any updates to CVE appear immediately in NVD.

NVD provides the following enhanced CVE content:

- CVSS Calculator for CVE IDs
- Fix Information for CVE IDs
- Advanced Searching

雲端安全標準

雲端安全標準

標準組織	專案或議題	研究角度
ITU	雲端安全框架，雲端安全營運及指引	通訊產業雲端安全
CSA	雲端安全指南、雲端安全威脅等	ICT產業雲端安全實踐
GSMA	雲端服務安全框架	行動營運商的雲端業務系統安全需求及實踐
OASIS	雲端環境之身份管理制定	雲端安全技術
NIST	雲端安全定義、雲端運算隱私等	雲端架構、安全和部署業務
CCSA	雲端運算應用與安全技術要求等	雲端安全技術、管理、營運各層面

雲端安全聯盟(CSA)

- 為推動雲端運算應用安全的研究交流與協作發展，業界多家公司於2008年12月聯合成立了CSA(雲端安全聯盟)，該聯盟是一個非營利組織，旨在提供在雲端運算環境下的最佳安全方案，推廣雲端運算應用安全的最佳實踐。
- 目前其企業成員包括思科、Dell、Novell、VMware、RSA、Google、HP、Intel、Microsoft、Oracle、AT&T、CA、McAfee、Trend、Symantec、MSFOCUS、3PAR。
- CSA確定的15個雲端運算安全焦點領域：資訊生命週期管理、政府和企業風險管理、法規和審核、立法、eDiscovery、加密和金鑰管理、認證和連線管理、虛擬化、應用安全、便攜性和共用性、資料中心、操作管理和事故回應、通知與修復、傳統安全影響、體系結構。
- 雲端安全認證：CSA Star 認證是作為解決關於雲端安全特定問題，增強ISO / IEC 27001而發展的新獨特認證。

雲端矩陣11項控制區域

控制區域	控制措施
法規遵循	稽核計畫與實施 資訊系統法規對照
資料治理	資料分級分類 資料保留政策 資料安全處置
設備及場所安全	實體安全政策 存取控制措施 設備與資產管理
人力資源安全	人員背景審查 人員聘雇協議 人員職務終止
資訊安全	資訊安全管理計畫 基本要求與政策審查 使用者存取與授權 安全責任與教育訓練 加密管理與弱點修補 資安事故處理與回應

雲端矩陣11項控制區域(Cont.)

控制區域	控制措施
法律議題	保密協議 第三方協議
營運管理	營運政策與文件化要求 資源規畫與設備維護
風險管理	風險管理與評估 風險處理計畫
服務發行管理	服務開發與取得 服務變更與品質管控 委外服務與軟體控管
服務彈性	管理計畫與衝擊分析 營運持續計畫與測試 環境管控與設備失效因應
安全架構	客戶存取要求 使用者識別管理 資料與應用程式安全 網路安全與入侵偵測

雲端控制矩陣表

CCMv3.0.1 CLOUD CONTROLS MATRIX VERSION 3.0.1

Control Domain	CCM V3.0 Control ID	Updated Control Specification	Architectural Relevance					
			Phys	Network	Compute	Storage	App	Data
Business Continuity Management & Operational Resilience Equipment Location	BCR-06	To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable distance.	X					
Business Continuity Management & Operational Resilience Equipment Maintenance	BCR-07	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel.	X	X	X	X	X	X

美國國家技術標準局(NIST)

- 美國國家標準技術研究所，National Institute of Standards and Technology（NIST），前身為國家標準局（NBS，1901年~1988年），是一家測量標準實驗室，屬於美國商務部的非監管機構。
- NIST在雲端運算領域相關出版品如下
  - SP800-125 安全虛擬化技術安全指南
  - SP800-144 公有雲中的安全和隱私指南
  - SP800-145 雲端運算定義
  - SP800-146 雲端運算概觀和建議
  - SP500-291 雲端運算標準路線圖
  - SP500-292 雲端運算參考體系架構
  - SP500-293 美國政府雲端運算技術路線圖

雲端運算安全規劃

雲端運算之資訊安全規劃

- 架構與服務模式多樣化，選擇太多
  - 三種服務模式SPI 要選哪一種？
  - 四種建構模式、放在內部或外部？
- 沒有通用的安全控制準則
  - 各種情境的安全管控需求不完全相同
- 建議方式
  - 列出採行雲端運算前後的優劣與風險
  - 評估風險承受能力是否大過雲端帶來的好處
- 五個步驟

Step1 辨識要移入雲端環境的資產

- 移入雲端的資產大略可分為兩種
  - 資料
  - 軟體/ 功能/ 程序
- 資產移入雲端後，不一定放在同一個地方
- 僅將部分資產移入雲端
  - 軟體與資料仍放在本身的資訊中心
  - 部份功能移到PaaS 模式的雲端環境
- 重點：找出哪些資料與功能要移入雲端

Step2 對資產進行詳盡評估

- 評定資產的特性：機敏等級、重要程度
- 從CIA 三個角度觀察受損程度
  - C：資產被廣泛公諸於世且到處散佈
  - C：供應商員工越權取得這些資產
  - I：程序或功能被外界入侵操控
  - I：資料遭到竄改
  - A：程序或功能失常，無法提供應有結果
  - A：資料無法取用

Step3 將資產對應至適當的模式

- 了解各種建構模式的安全特性
- 能否接受各種建構模式帶來的風險
  - 公用雲
  - 私有雲：放置於組織內部
  - 族群雲：考量放置地點、供應商、族群內其他成員
  - 混合雲：大略設計各個組件、功能與資料的放置位置

Step4 挑選合適的服務模式與供應商

- 針對SPI 三種服務模式
  - 評估各需要採行何種程度的安全控管措施
  - 目標：將風險降至可承受範圍內
- 納入原本環境的安全需求
  - 例如：資料處理規範

Step5 描繪資料流程

- 針對所挑選的建構模式，描繪資料流程
  - 本身組織
  - 雲端服務
  - 其他相關客戶/ 工具
- 確認
  - 流程是否正確、合理、安全
  - 整個流程的安全控管措施是否一致有效

虛擬化架構

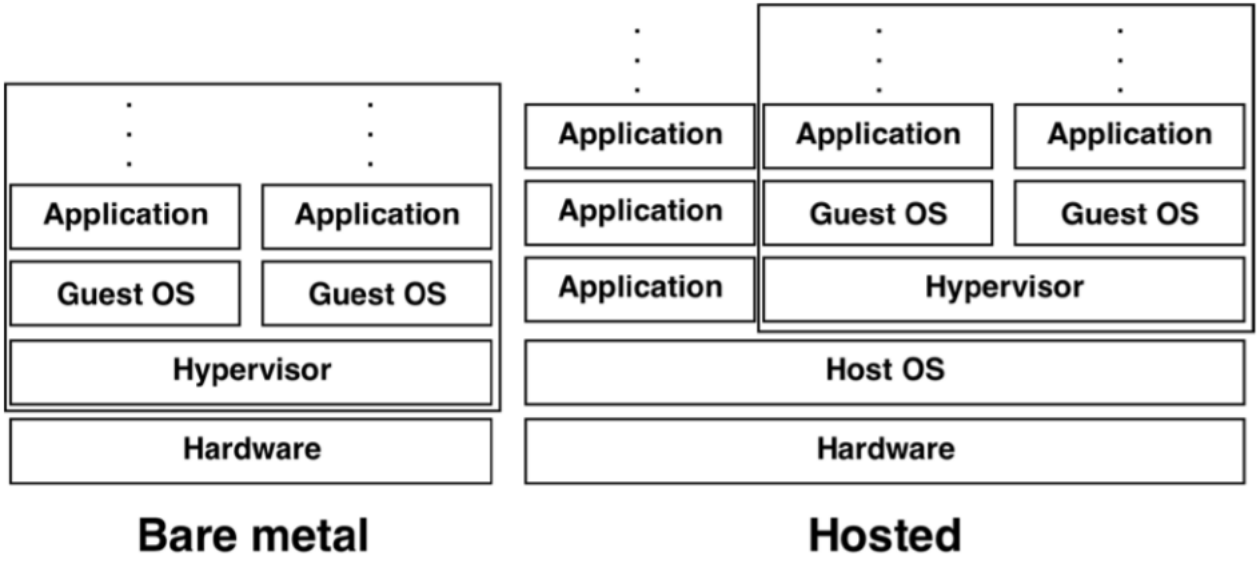
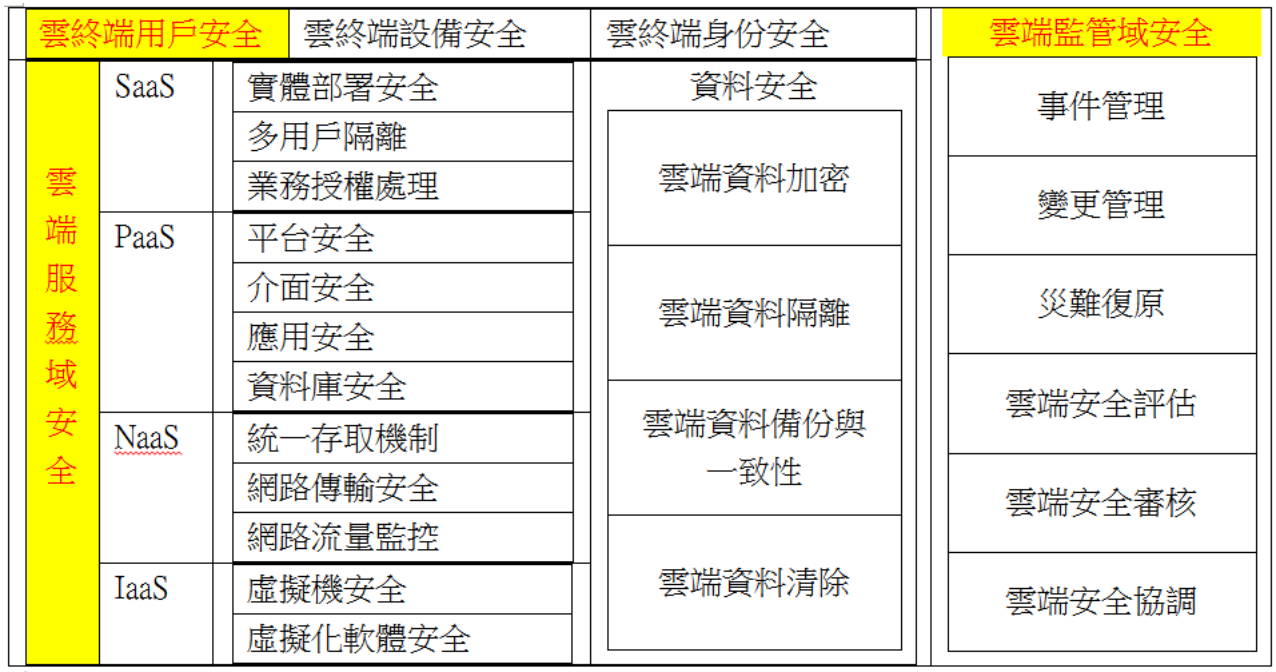


Figure 2-1. Full Virtualization Architectures

Hypervisor

- Hypervisor 有哪些型態?
  - 虛擬化的 Hypervisor 有兩種型態，Type 1 (Bare-Metal hypervisor) 與 Type 2 (Hosted hypervisor)。Type1 又稱為 Native VM，Type2 也稱為 Hosted VM。
- 兩者有何不同?
  - Bare-Metal 中文譯為裸機或裸金屬，hypervisor 直接安裝於空機或新機上，直接掌控硬體資源，硬碟無須先有OS。Type 2 hypervisor 則需先有 Windows 或 Linux 才能安裝。
- Type 1與Type 2 各有哪些產品?
  - Bare-Metal 型態：VMware ESX / ESXi、Microsoft Hyper-V、Citrix Xen Server、RedHat KVM、Oracle Virtual Iron 等。
  - Hosted 型態：VMware Wrokstation / Fusion、Microsoft Virtual PC / Server、Sun VirtualBox、Parallels Desktop 等。

雲端安全架構


雲終端用戶安全
雲終端設備安全
雲終端身份安全
雲端監管域安全
雲端服務域安全
SaaS
實體部署安全
多用戶隔離
業務授權處理
PaaS
平台安全
介面安全
應用安全
資料庫安全
NaaS
統一存取機制
網路傳輸安全
網路流量監控
IaaS
虛擬機安全
虛擬化軟體安全
資料安全
雲端資料加密
雲端資料隔離
雲端資料備份與一致性
雲端資料清除
事件管理
變更管理
災難復原
雲端安全評估
雲端安全審核
雲端安全協調

雲端服務域安全

- 虛擬機安全(虛擬機自身安全、隔離技術，遷移擴充技術，更新管理技術，部署管理)，
- 虛擬軟體(防火牆、存取控制、弱點掃描
- Naas(身份管理，密碼與認證，連線授權，稽核、網路傳輸安全(VPN，Ipsec，金鑰交換技術，存取控制技術)，網路流量監控(DPI技術，DFI技術)
- PaaS(平台安全，介面安全，應用安全，資料庫安全)
- SaaS(實體部署，多用戶隔離)
- 資料安全(雲端資料加密(DES，AES，IDEA，RC4)，金鑰管理(PKI)，安全基礎設施(CA(憑證，安全閘道，加密檔案資料，雲端數據隔離(共用表架構，分離資料庫架構，分離表架構)，雲端資料備份，雲端資料清除

雲端監管域安全

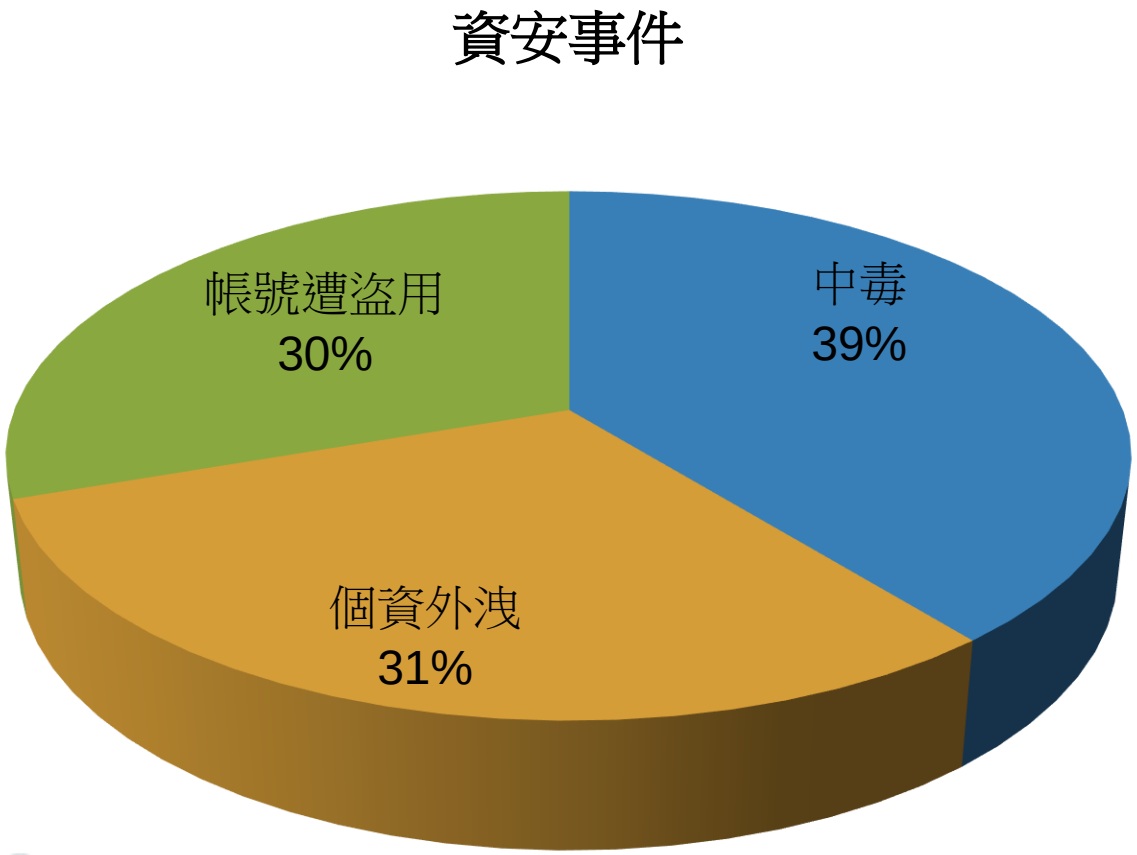
- 運行監控管理、惡意行為監控
- 事件管理(監控，預警，回應)
- 安全更新管理
- 災難復原(營運持續計畫)
- 雲端安全評估(風險評估CSA CCM V3.0)
- 雲端安全稽核

雲終端域安全

- 終端設備安全：
  - 伺服器、桌上型電腦、筆記型電腦、平板、智慧手機)
- 終端身份管理：
  - Single Sing-on(SSO)：e.g. Microsoft Live ID
  - 多因子認證：e.g. 密碼+手機簡訊
  - 生物辨識：指紋、臉部、虹膜

雲端應用安全與用戶

國內消費者資安事件調查



資料來源iThome

網路安全四大迷思

- 電子郵件一定有加密
- 無痕視窗絕對不留痕跡
- 關掉GPS一定安全
- 高強度的密碼一定足夠

電子郵件一定加密?

根據調查，只有 46% 的人了解並不是每封電子信件加密保護，加密保護是指只有寄件人和收件人能夠取得信件內容。儘管許多電子信箱服務，像是 Gmail、奇摩信箱這些都會自動將每封信件加密，但這並不代表所有信箱服務網站都會。像大家一定有被 Gmail 詢問過「該信箱不安全，確定要寄出嗎？」的問題。

無痕視窗不留痕跡?

◎使用無痕視窗雖然可以讓 Chrome、Firefox 這類的瀏覽器部記錄任何你去過的網站、做過的事，瀏覽器本身不會留下歷史紀錄。但這並不代表你去的網站不會記錄，問卷調查中，只有 39% 的人知道這個事實。

關掉GPS一定安全?

◎手機 GPS 定位只是收集資料的其中一種管道而已。調查顯示，有將近一半的受訪者不知道或是不確定關掉 GPS 是否就搞定了。答案是：錯！手機只要有連到訊號基地台或是 Wifi 無線網路，這些都可以是被用來追蹤定位的來源。

高強度的密碼一定安全?

- 這麼說其實並沒有錯，但網路安全專家們還是建議額外使用「雙重驗證功能」(Two-Factor authentication)進一步保護帳號安全。這類驗證會需要登入者額外輸入一組寄到自己其他信箱或是電話的驗證碼，才能登入。這樣子就算駭客知道了你的帳號密碼，他也還是無法登入。

J;6m/3fu/4 

20170416 

駭客魔爪伸入LINE別再亂轉長輩文

- 調查資料顯示，民眾收到任何有關健康、災難或政府政策等實用性訊息，69.7%會傳給親朋好友(只要收到就傳1.9%、通常會傳16.0%及看狀況51.8%)，由於轉發者多有一定社會歷練，因而被時下年輕人戲稱為「長輩文」，但轉發「長輩文」這類消息的民眾，卻僅有不到5成會進一步確認資訊真偽，而朋友、家人如果就這麼隨手點進惡意網站，可能就順了駭客之意！手機內的重要資料馬上被「一覽無遺」！

該如何保護 Facebook 帳號

- 加強密碼強度，使用密碼管理員
- 不再其他地方使用相同密碼
- 定期更換密碼：養成固定四個月到半年就換一次密碼的習慣
- 永遠不要讓不信任的網站記得密碼
- 只有信任的電腦才記住密碼，只有自己的個人電腦才讓它自動記住密碼

進入臉書設定帳號安全

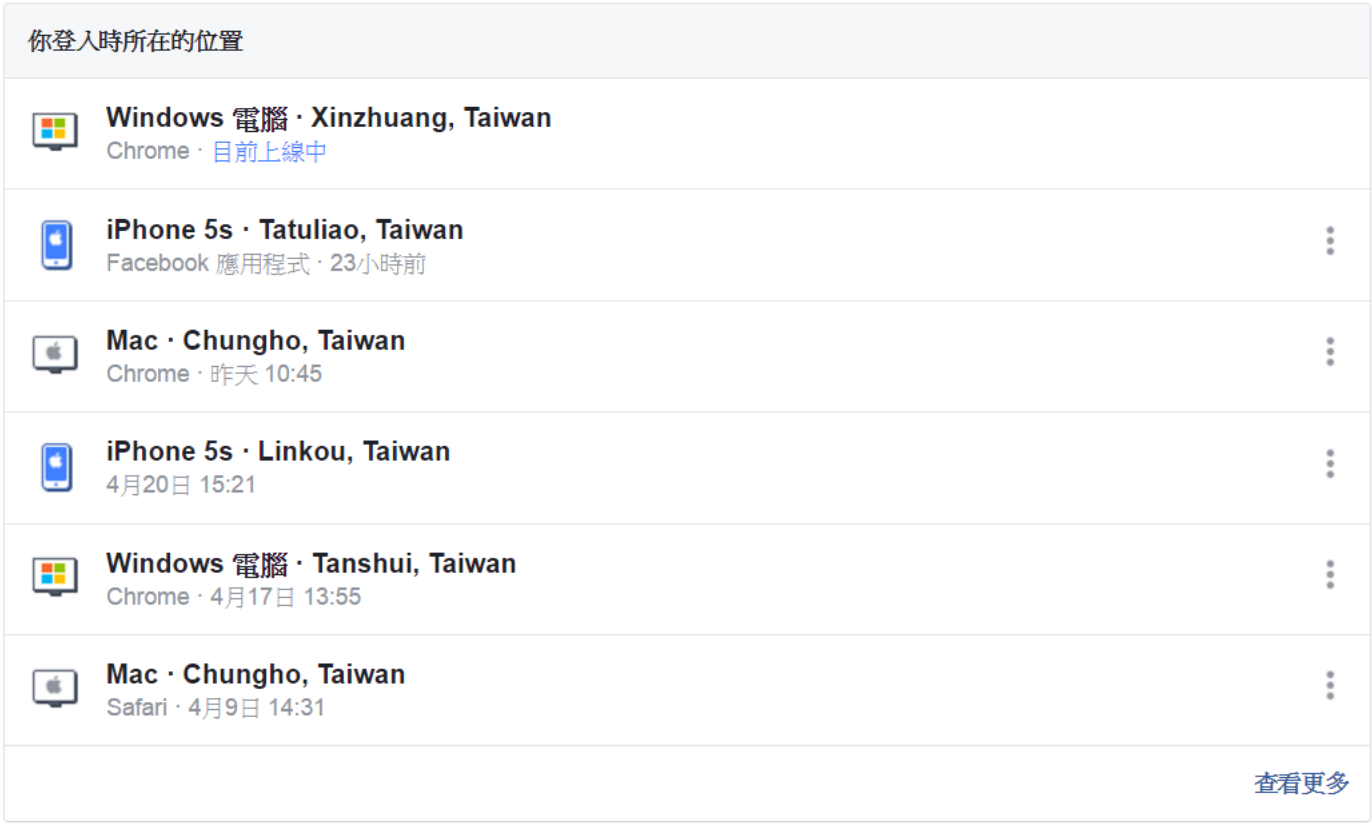

首頁
你的粉絲專頁：
T客邦的臉書基...
1 則訊息
PC home雜誌
3 則留言
T客邦 3C 科技
1 則訊息
查看更多.....
建立粉絲專頁
管理粉絲專頁
建立社團
管理社團
建立廣告
在 Facebook 上登廣告
活動紀錄
動態消息偏好設定
設定


一般
帳號安全和登入
隱私
動態時報與標籤
封鎖
語言
通知
行動版
公開的貼文
應用程式
廣告
交易付款
支援收件匣
影片

帳號安全設定


帳號安全和登入
我們重新整理了一些設定。紀念帳號代理人和帳號停用功能現在移到一般下方了。
建議
選擇可以在你不小心遭到鎖定時聯絡並尋求協助的朋友
請指定你帳號被鎖住時能夠提供協助的朋友（3 到 5 位）。建議所有人都設定此功能。
編輯
你登入時所在的位置
Windows 電腦 · Xinzhuang, Taiwan
Chrome · 目前上線中
iPhone 5s · Tatuliao, Taiwan
Facebook 應用程式 · 22小時前
查看更多

登入設備與位置確認


你登入時所在的位置
Windows 電腦 · Xinzhuang, Taiwan
Chrome · 目前上線中
iPhone 5s · Tatuliao, Taiwan
Facebook 應用程式 · 23小時前
Mac · Chungho, Taiwan
Chrome · 昨天 10:45
iPhone 5s · Linkou, Taiwan
4月20日 15:21
Windows 電腦 · Tanshui, Taiwan
Chrome · 4月17日 13:55
Mac · Chungho, Taiwan
Safari · 4月9日 14:31
查看更多

帳號安全設定

登入

更改密碼
建議使用與其他服務不同的強式密碼
編輯

使用大頭貼照登入
開啟 • 點按或點擊大頭貼照即可登入，不需使用密碼
編輯

設定額外的帳號安全

接收不明登入的警告
開啟 • 如果任何人從與平常不同的裝置或瀏覽器登入你的帳號，我們就會通知你
編輯

使用雙重驗證
使用手機收到的代碼，並搭配密碼登入
編輯

選擇你帳號被鎖住時能夠聯絡的朋友（3 到 5 位）
你信賴的聯絡人可以傳送 Facebook 代碼和網址，協助你重新登入帳號
編輯

進階

加密的通知電子郵件
為 Facebook 的通知電子郵件加上額外的安全措施（只有你可以將這些電子郵件解密）
編輯

使用大頭貼照登入


使用大頭貼照登入
開啟 • 點按或點擊大頭貼照即可登入，不需使用密碼
關閉
此瀏覽器
使用密碼
點擊大頭貼照，然後輸入密碼即可登入
關閉大頭貼照登入
使用電子郵件或電話號碼登入
其他裝置與瀏覽器
從 iOS 10 的 Facebook for iOS 瀏覽器移除大頭貼照登入
最後使用時間：2月6日 13:16
沒有通關密碼

不明登入警告


設定額外的帳號安全
接收不明登入的警告
開啟 • 如果任何人從與平常不同的裝置或瀏覽器登入你的帳號，我們就會通知你
關閉
在任何人從未經認可的裝置或瀏覽器登入你的帳號時收到警告訊息。
通知
接收通知
不要接收通知
電子郵件
傳送登入警告電子郵件至 sambalee@hotmail.com
不要接收電子郵件警告
新增其他電子郵件地址或手機號碼
儲存變更

使用雙重驗證


使用雙重驗證
使用手機收到的代碼，並搭配密碼登入
關閉
雙重驗證已關閉
設定
Add an extra layer of security to prevent other people from logging into your account. 瞭解詳情
簡訊（SMS）· 新增手機號碼
Use your phone as an extra layer of security to keep other people from logging into your account.
安全性金鑰 · 新增金鑰
使用通用第二要素（U2F）安全性金鑰，透過 USB 或 NFC 登入。
代碼產生器 · 停用
You can use Code Generator in your Facebook mobile app to reset your password or to generate login codes. Set up a 第三方應用程式 to generate codes.
復原代碼 · 取得驗證碼
你的手機不在身邊時（例如旅行時），請使用這些驗證碼。
應用程式密碼 · 產生
為不支援雙重驗證的應用程式（例如 Xbox、Spotify）取得唯一的單次使用密碼 瞭解更多

電子郵件加密


進階
加密的通知電子郵件
為 Facebook 的通知電子郵件加上額外的安全措施（只有你可以將這些電子郵件解密）
關閉
你的 OpenPGP 公開金鑰
在此輸入你的 OpenPGP 公開金鑰：
輸入 1 個 PGP 公開金鑰
用這個公開金鑰來加密 Facebook 寄給你的通知郵件？ [?]

手機遺失安全設定

iPhone手機遺失自保

對於 iPhone 的使用者來說，為了預防手機遺失時資料被竊取，建議平時就要養成習慣設定「螢幕鎖」以及 SIM 卡「PIN 碼」。當 iPhone 不慎遺失時，還能在第一時間內成為兩道基本防線，預防個資立即被盜取。

此外，iOS 協尋手機的機制有更佳的防護，使用者必須在手機端將「尋找我的 iPhone」開啟，並綁定 iCloud 帳號，未來才能在遠端進行定位功能與後續啟用遺失模式與清除iPhone資料等保護措施。

開啟設定進入隱私權

進入設定頁面，找到「隱私權」的選項。

點選定位服務

預設「定位服務」是開啟狀態，若為關閉則直接點選進入設定頁面。

開啟定位服務

在找到「定位服務」後，立即將此功能「開啟」。

於設定中點選iCloud

於設定選單裡，找到「iCloud」選項。

點選尋找我的iPhone

在 iCloud 頁面，找到「尋找我的 iPhone」，預設也是開啟，若為關閉則須點選進入變更。

開啟尋找我的iPhone

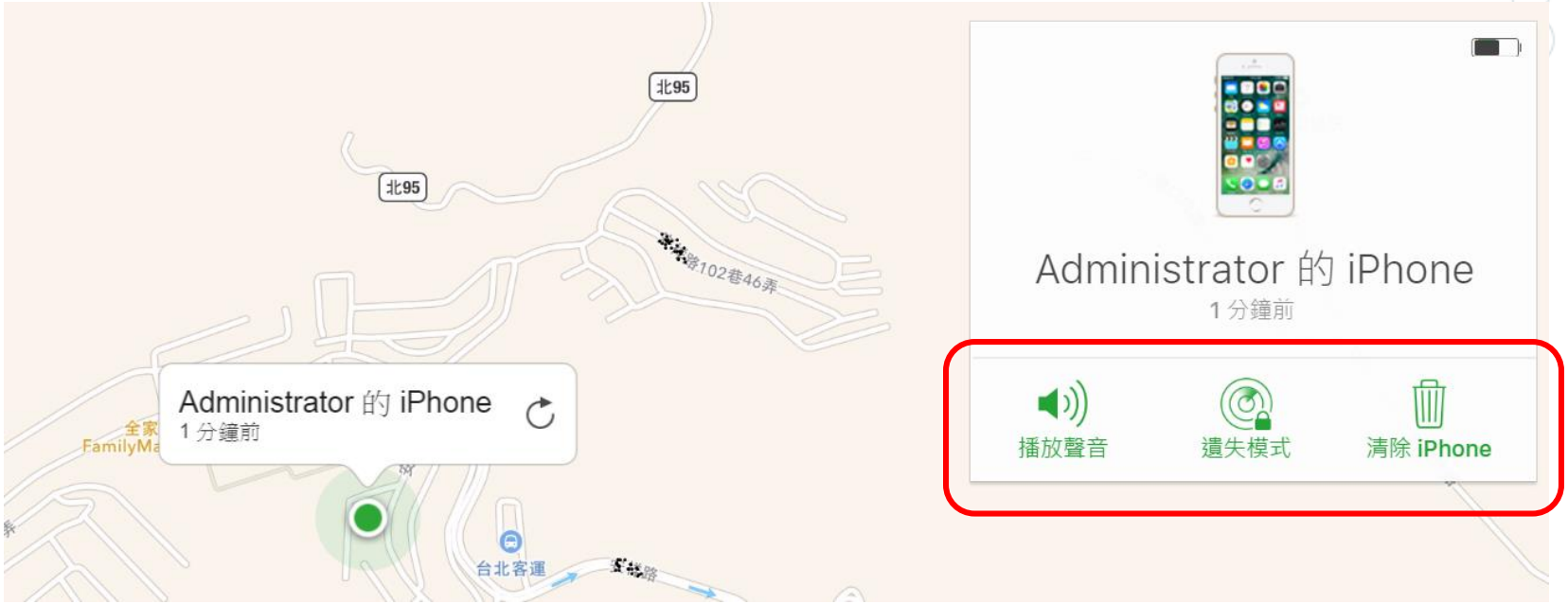
在「尋找我的 iPhone」頁面裡，將此功能開啟即可，下方也有文字說明，此功能可用來定位、鎖定及清除 iPhone。

若手機遺失時，先登入iCloud網站

進入尋找我的iPhone

點選iPhone裝置

遺失的處置選項


北95
北95
Administrator 的 iPhone
1 分鐘前
台北客運
Administrator 的 iPhone
1 分鐘前
播放聲音
遺失模式
清除 iPhone

手機防護軟體

防護軟體名稱	版本	下載人數	評價人數	評價	介面語言
NetQin Mobile Anti-Virus	4.8	>250,000	3,113	4.5	英文
Trend Micro Mobile Security	1.2	50,000-250,000	822	4	繁中
Norton Mobile Security	2.1.0.270	>250,000	6,905	4	英文
Kapsersky Mobile Security	9.10.75	5,000-10,000	486	4	英文
Lookout Mobile Security	6.0.1	>250,000	196,605	4.5	英文
360Safe Mobile Safe	1.9.5	50,000-250,000	2,054	4.5	簡中
Dr. Web Anti-virus Light	6.00.8	>250,000	22,435	4.5	繁中
AegisLab Anti-virus Free	0.4.24	10,000-50,000	356	4.5	繁中
HAURI ViRobot Mobile	1.6.0.1103	>250,000	1,793	4	英文
AVG Anti-Virus Free for Android	2.8	>250,000	116,827	4.5	簡中

Mobile Protection Rates		
	Protection Rate	False Positives
Bitdefender, Trend Micro	100,0%	0
Kaspersky Lab, Tencent	100,0%	1
G Data, ESET, McAfee	99,9%	3
Avira	99,8%	6
Antiy	99,8%	12
AVG	99,8%	14
Alibaba	99,7%	0
Baidu	99,5%	0
Avast[4]	99,0%	6

Thanks!