



雲端運算、資訊安全 與 日誌服務

李忠憲 教授

國立成功大學 電機工程學系

jsli@mail.ncku.edu.tw

中國3波數位導彈襲美



資料來源：

臉書掛點前中國3波數位「導彈」襲美 | 即時新聞 | 20140619 | 蘋果日報

<http://www.appledaily.com.tw/realtimenews/article/new/20140619/419474/>



中國樂視網為何租遠傳機房？



綠委爆中國「樂視網」租遠傳機房
恐有資安疑慮

資料來源：

中國樂視網為何租遠傳機房 (李忠憲) | 20141218 | 蘋果日報

<http://www.appledaily.com.tw/appledaily/article/headline/20141218/36273616/>



重點摘錄

2014年的IT安全管理報告

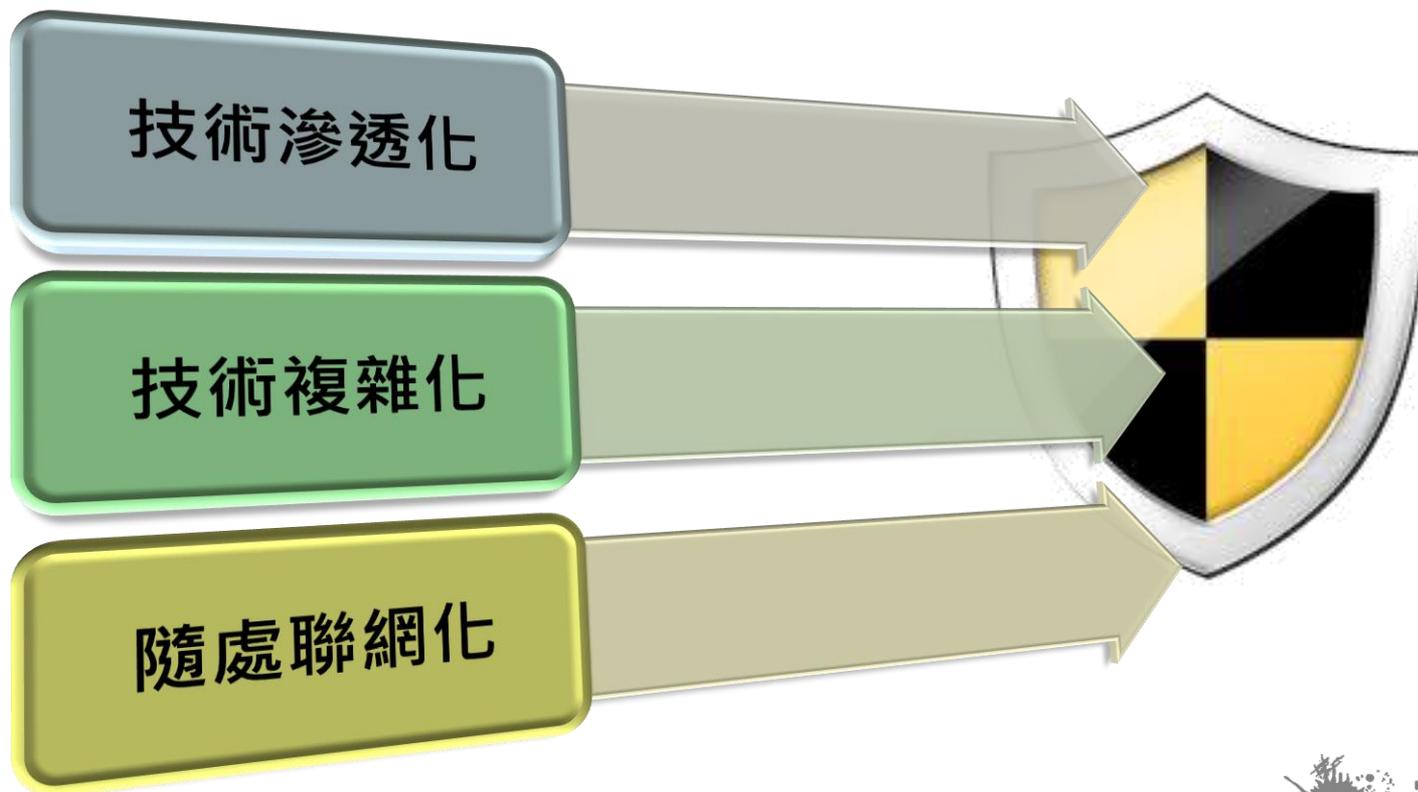
德國聯邦訊息安全辦公室 (BSI)

資料來源：

德國2014網路安全報告重點摘錄

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile

三個數位化特徵，對資安的新挑戰

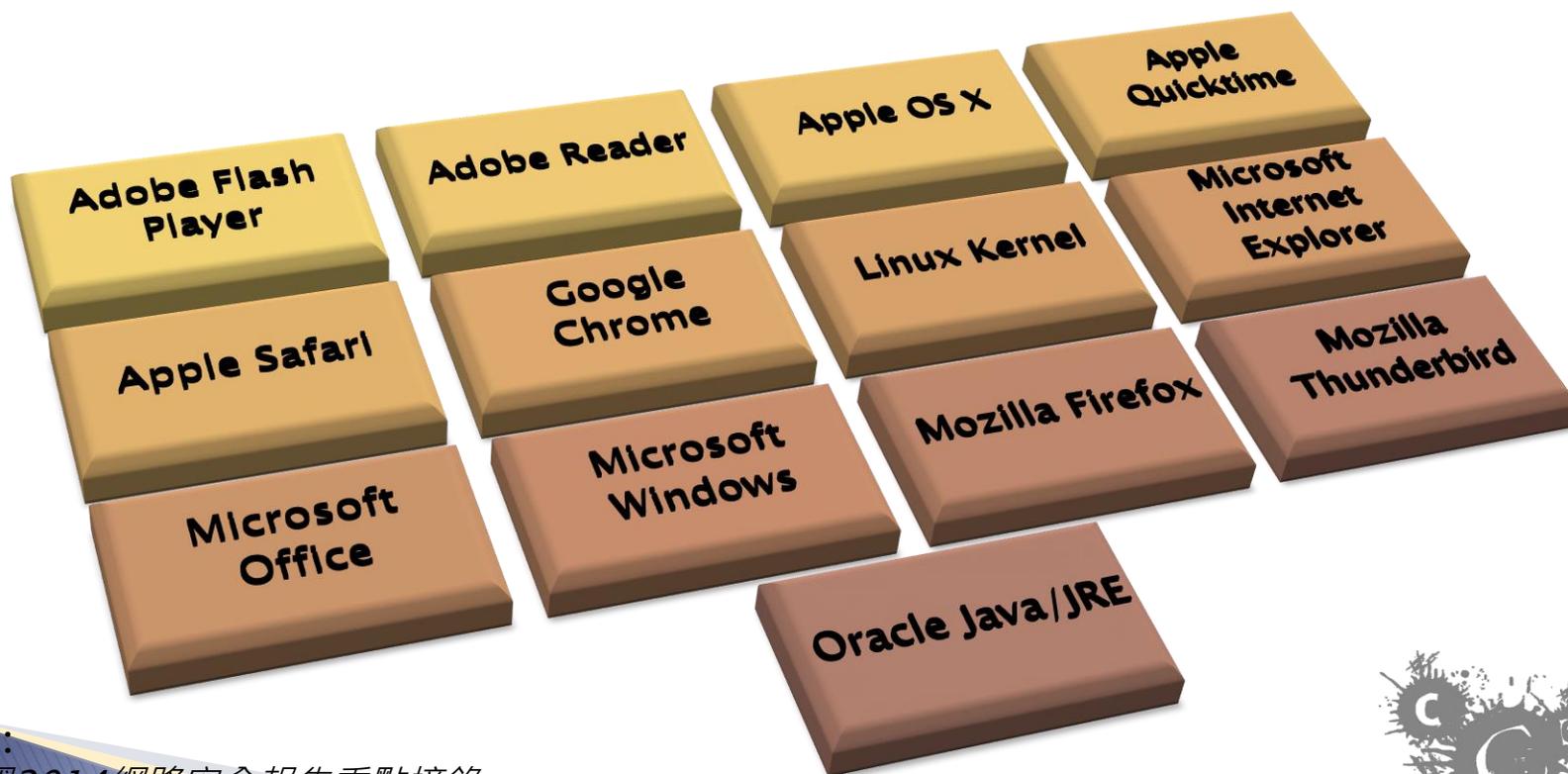


資料來源：

德國2014網路安全報告重點摘錄

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile

嚴重網路安全漏洞，與日俱增



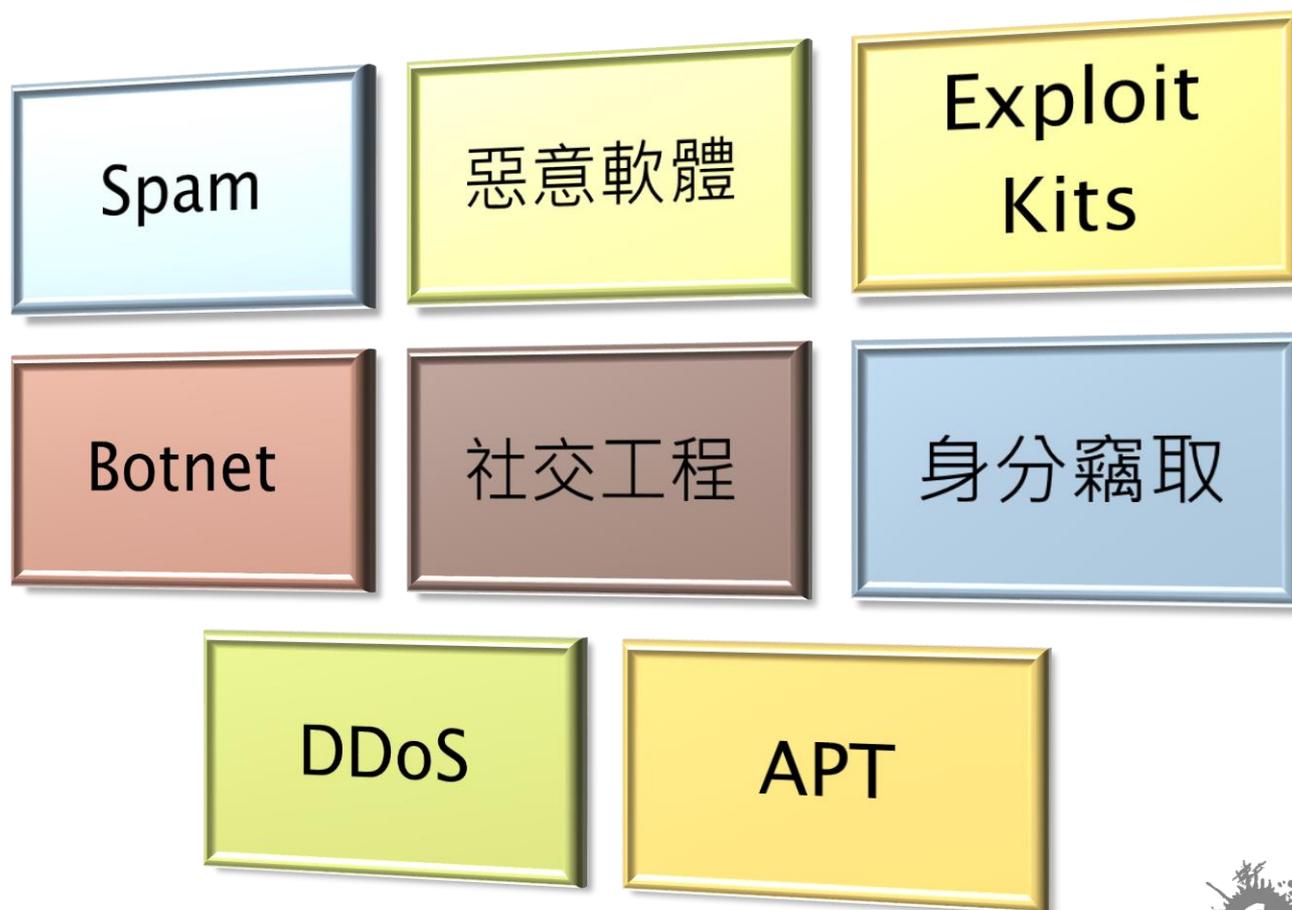
資料來源：

德國2014網路安全報告重點摘錄

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile



攻擊媒介和工具

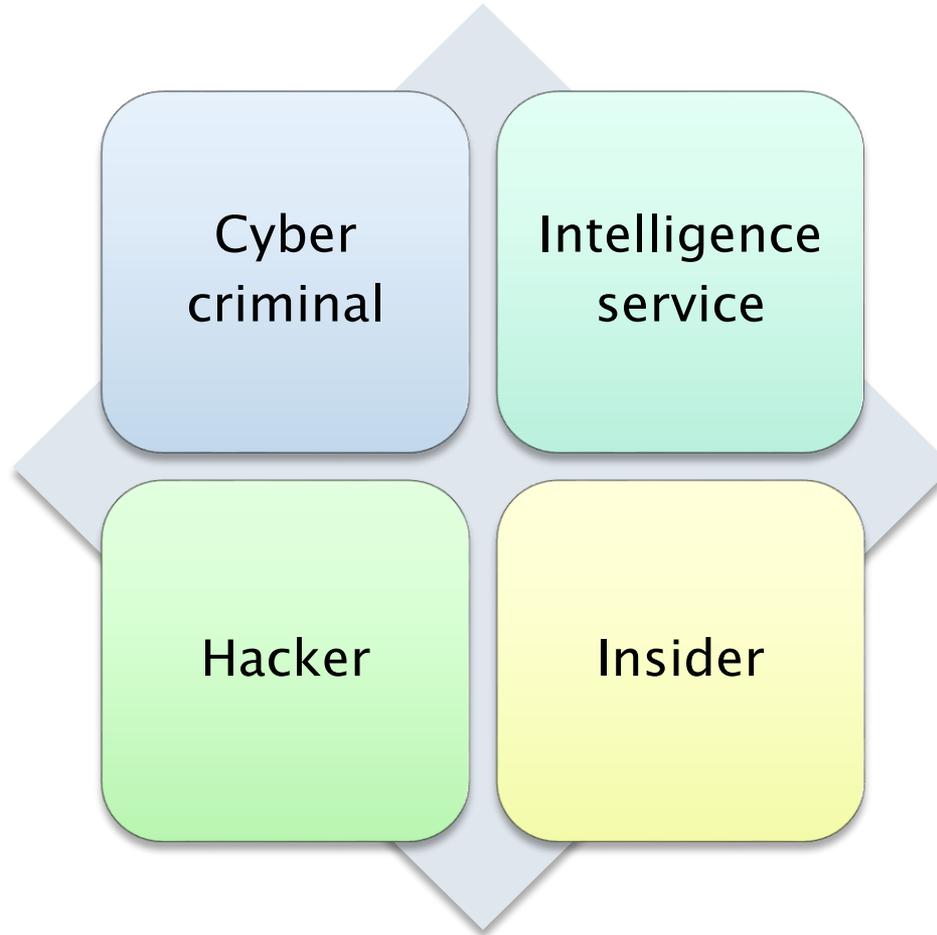


資料來源：

德國2014網路安全報告重點摘錄

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile

攻擊者的分類



資料來源：

德國2014網路安全報告重點摘錄

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile

資安威脅的影響

個人用戶

- 垃圾郵件及社交工程附加的惡意程式
- 釣魚網頁
- 個資外洩

數位天真

國家/ 企業組織

- 針對性的社交工程和間諜行動
- 利用已知和未知漏洞，竊取資料或攻擊
- DDoS

資料來源：

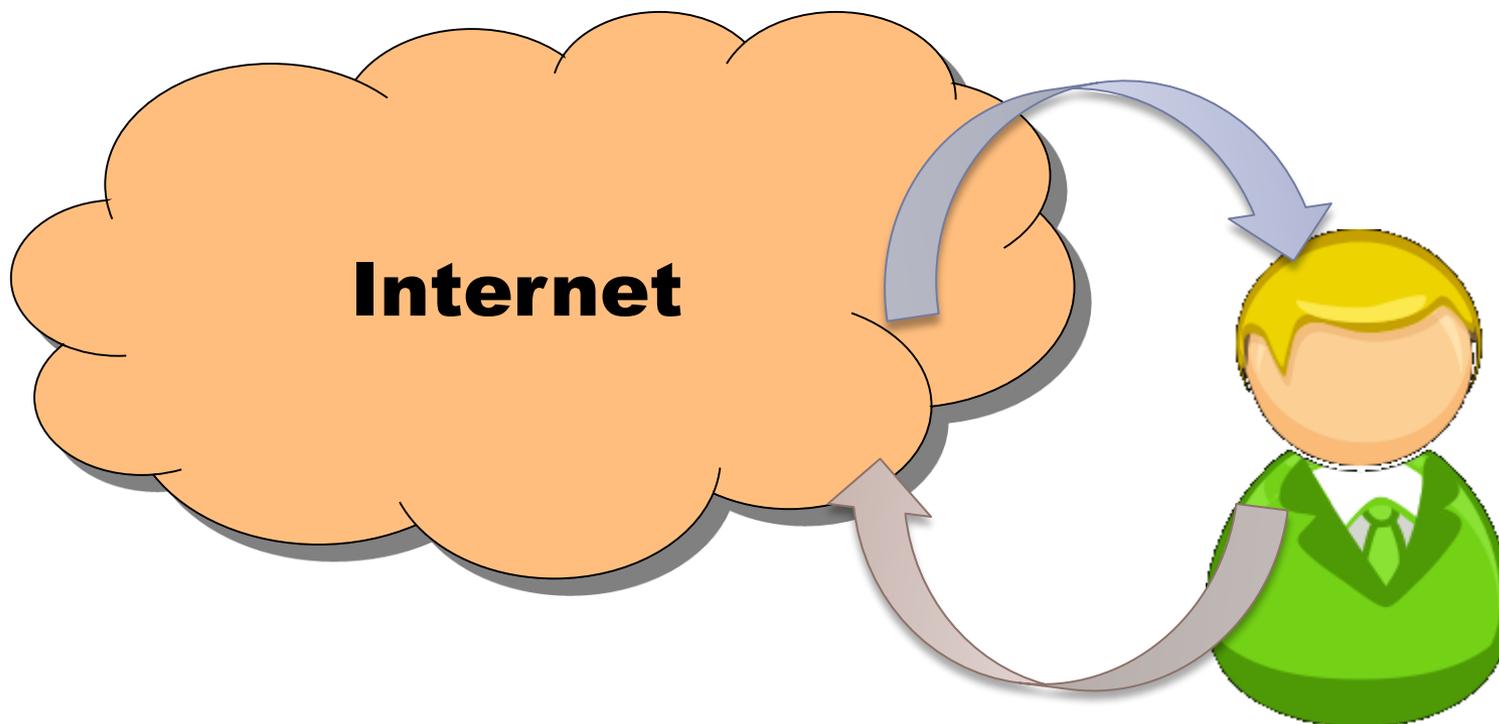
德國2014網路安全報告重點摘錄

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile

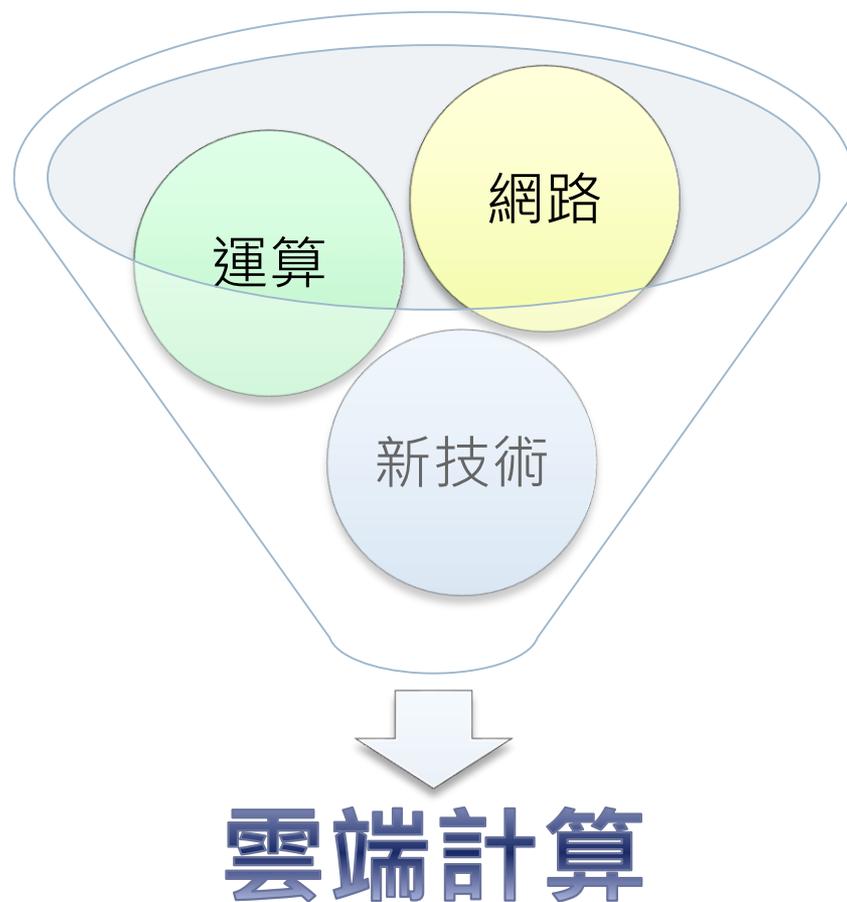


何謂「雲端計算」？

什麼是雲

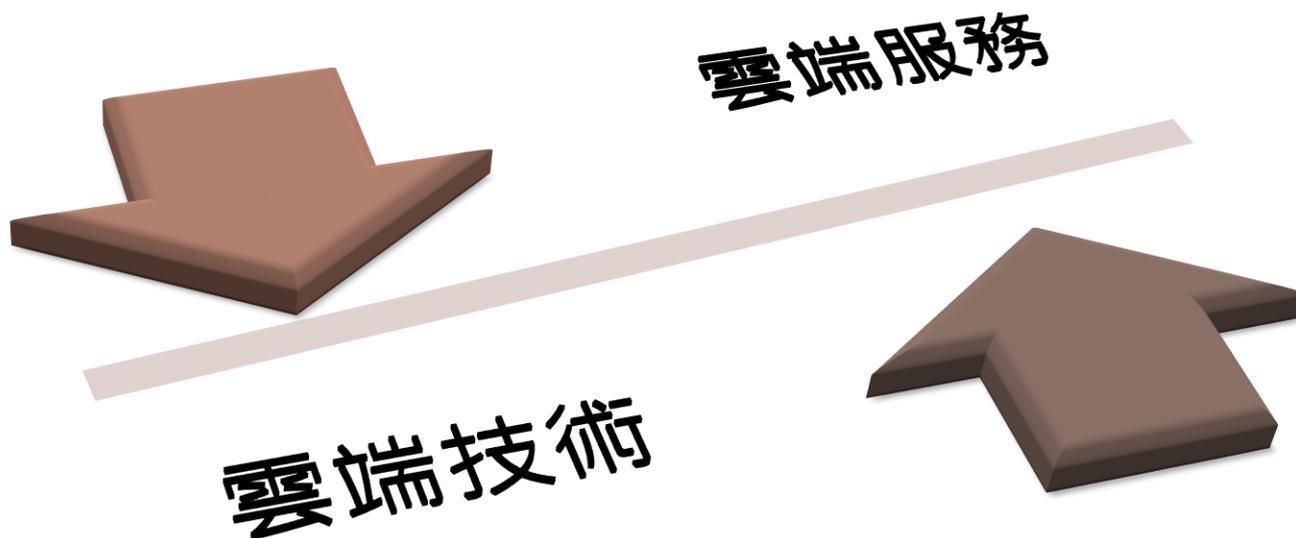


「雲端計算」是一種概念



細分雲端計算

GARTNER say...

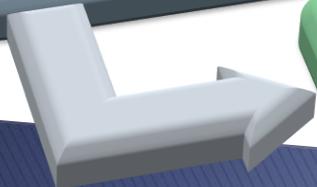


from COMPUTER WORLD

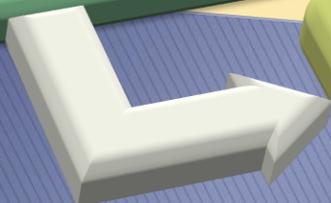


資訊安全需求

Confidentiality



Integrity



Availability

Non-repudiation

Authenticity

Authority

Accountability



雲端資安的特點

CSA
安全指導原則

Gartner
雲端資安風險

CSA安全指導原則

雲端安全聯盟
(Cloud Security Alliance)

Security Guidance for Critical Areas of Focus in Cloud Computing V2.1

治理

治理與企業風險管理

法律與電子資料搜尋

法規遵守與稽核

資訊生命週期管理

可攜性與互通性

維運

傳統上的安全、業務持續與災難復原

資料中心維運

事件處理、通知與回復

應用程式安全

加密與金鑰管理

身份與存取管理

虛擬化

Ref: <http://www.cloudsecurityalliance.org/csaguide.pdf>

Gartner 七大雲端資安風險



Ref: <http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853?page=0,1>



日誌服務

後**個資法**時代之稽核記錄管理

日誌管理實務

清查來源
確認內容
完整實用

關鍵記錄
儲存管理

可否因應
未來挑戰

日誌管理規劃建議

適當的管理政策

適合的收集方式

適當的分析工具

適當的儲存方式

時間同步是關鍵



NCKU

CANS

END !!

Thank You For Attention

THANK YOU FOR ATTENTION