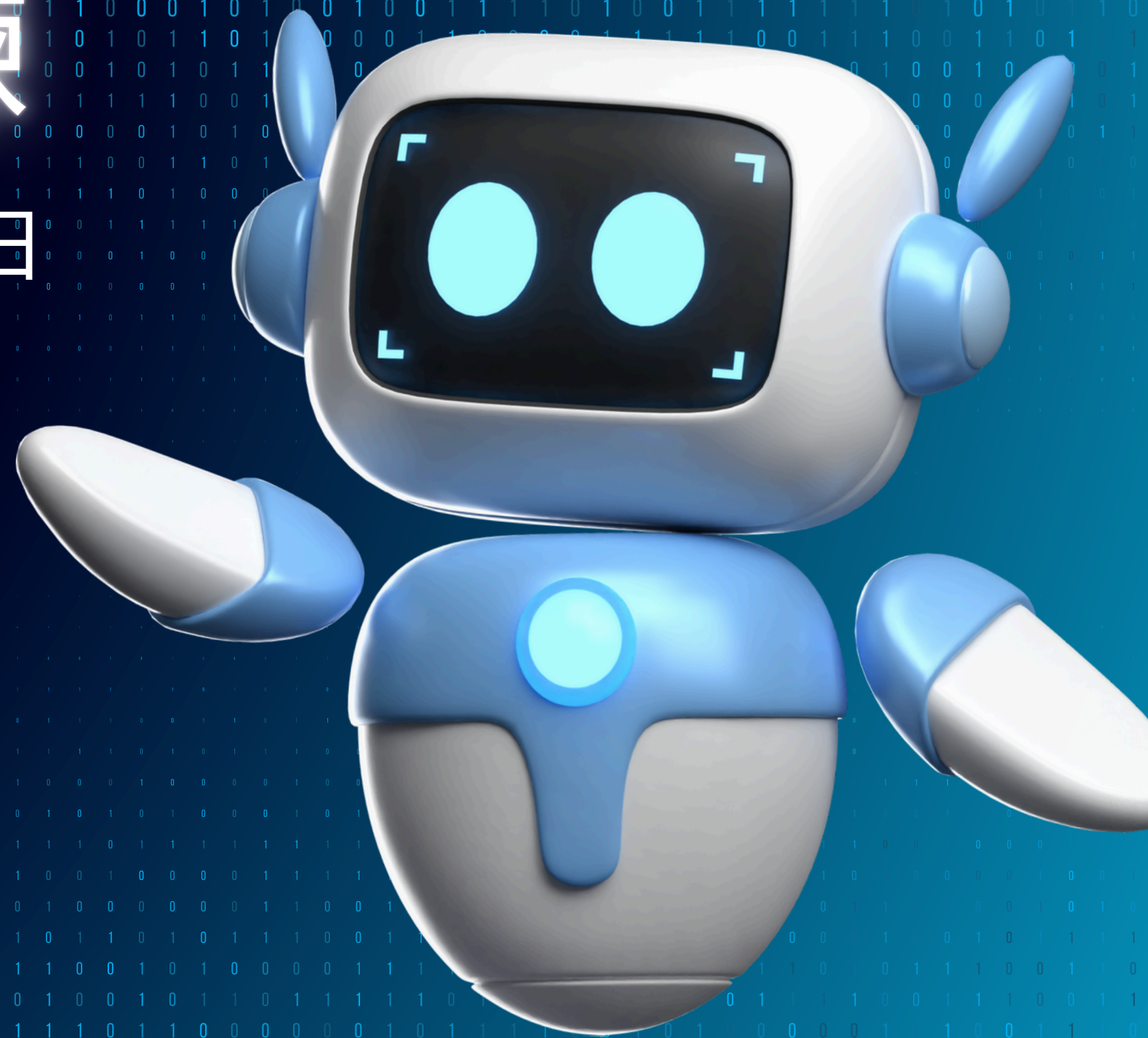


# 資安三小時訓練

基隆市中和國小113年09月18日



中華民國 113 年 07 月 18 日

## Certificate of Completion 通過認證時數證書

通過年度： 113 年      通過期間： 113/07/18-113/07/18

身分證字號： [REDACTED]      姓名： 吳信 [REDACTED]

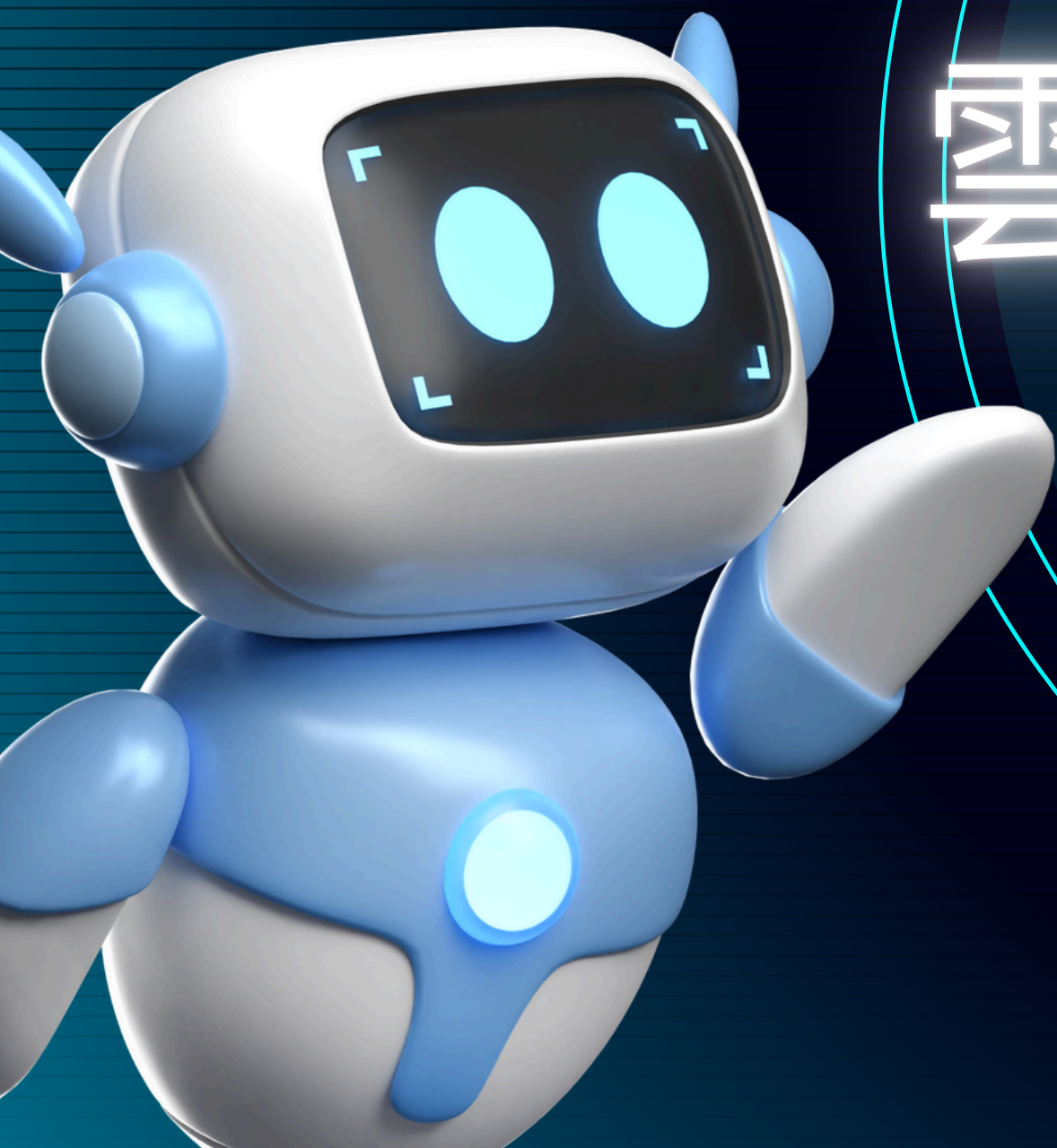
下列課程成績合於規定

| 序號 | 課程編號          | 課程類別 | 課程名稱     | 通過日期      | 通過認證時數 |
|----|---------------|------|----------|-----------|--------|
| 1  | PACSI13100007 | 開放式  | 雲端應用安全實務 | 113/07/18 | 1.0    |

頁數：1/1      總計時數：1.0

 等公務園學習平臺  
<https://elearn.hrd.gov.tw>

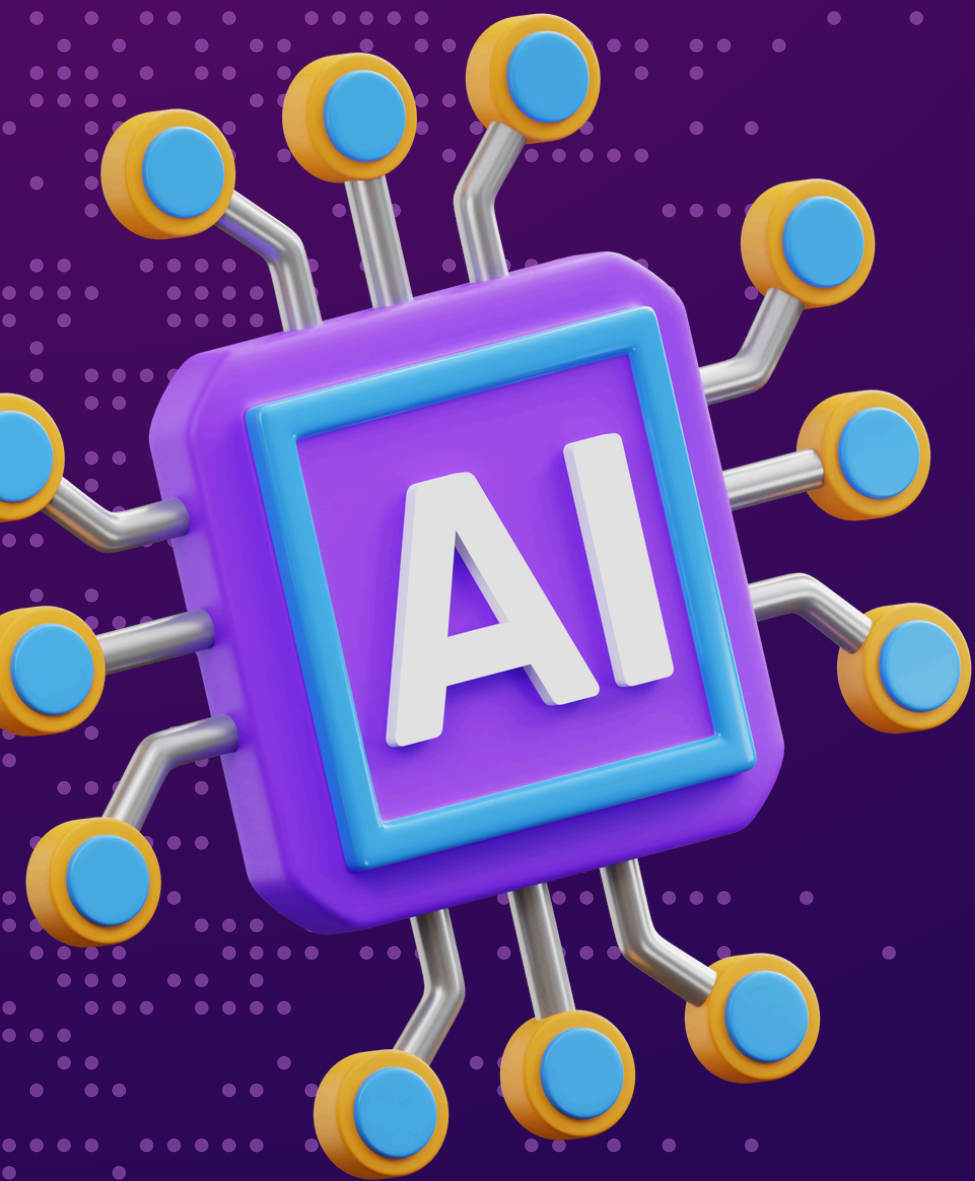




# 雲端安全 應用實務

[https://www.youtube.com/watch?  
v= EXHFQAqNps](https://www.youtube.com/watch?v=EXHFQAqNps)

# CONTENTS



1

了解雲端服務的基礎知識、服務類型與部署模型

2

認識常見的雲端服務和新型態的雲端應用

3

掌握選擇雲端服務時的考量因素

4

深入理解雲端安全威脅和防禦策略，並能夠識別潛在的威脅

5

了解資料在雲端安全的角色、責任與保護方法

6

掌握身分識別和存取管理的策略和方法





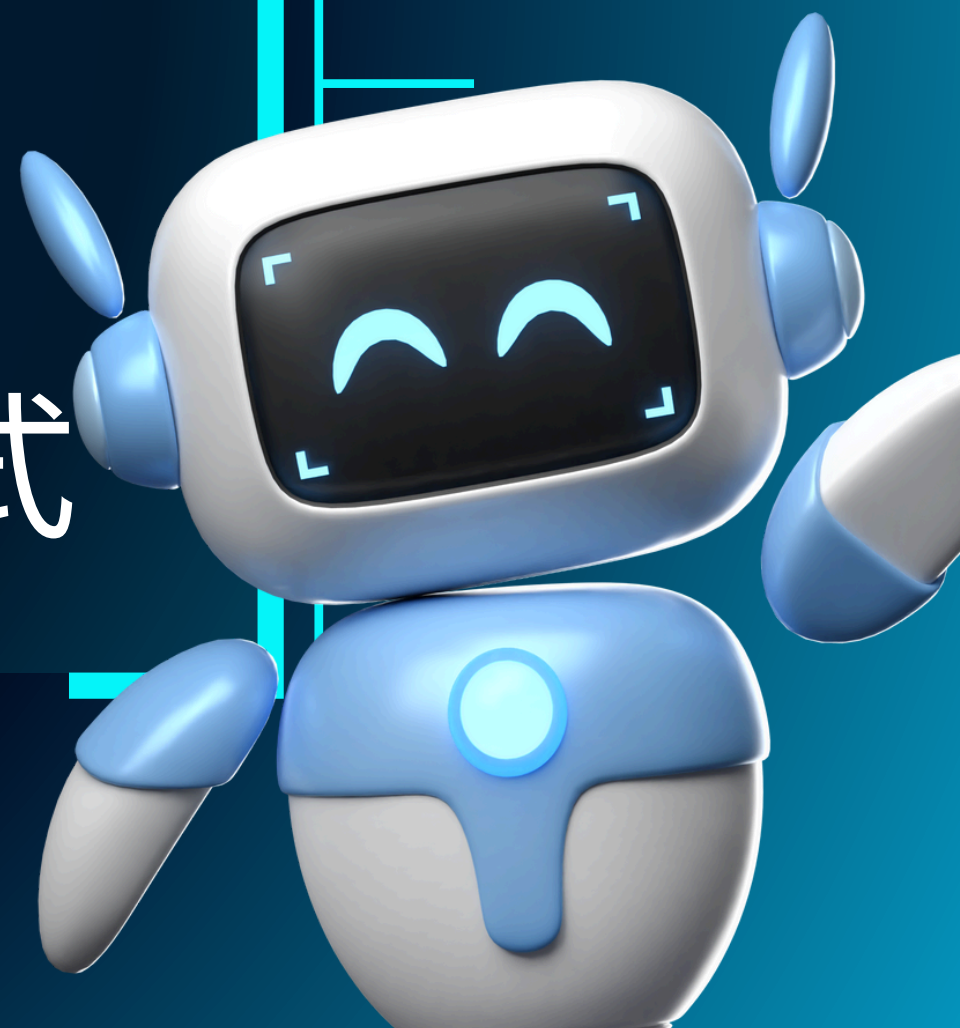
## 雲端服務簡介

### 1.服務類型與共同責任模型

IaaS:跟雲端服務供應商租用

PaaS:利用其平台做開發

SaaS:透過瀏覽器存取應用程式



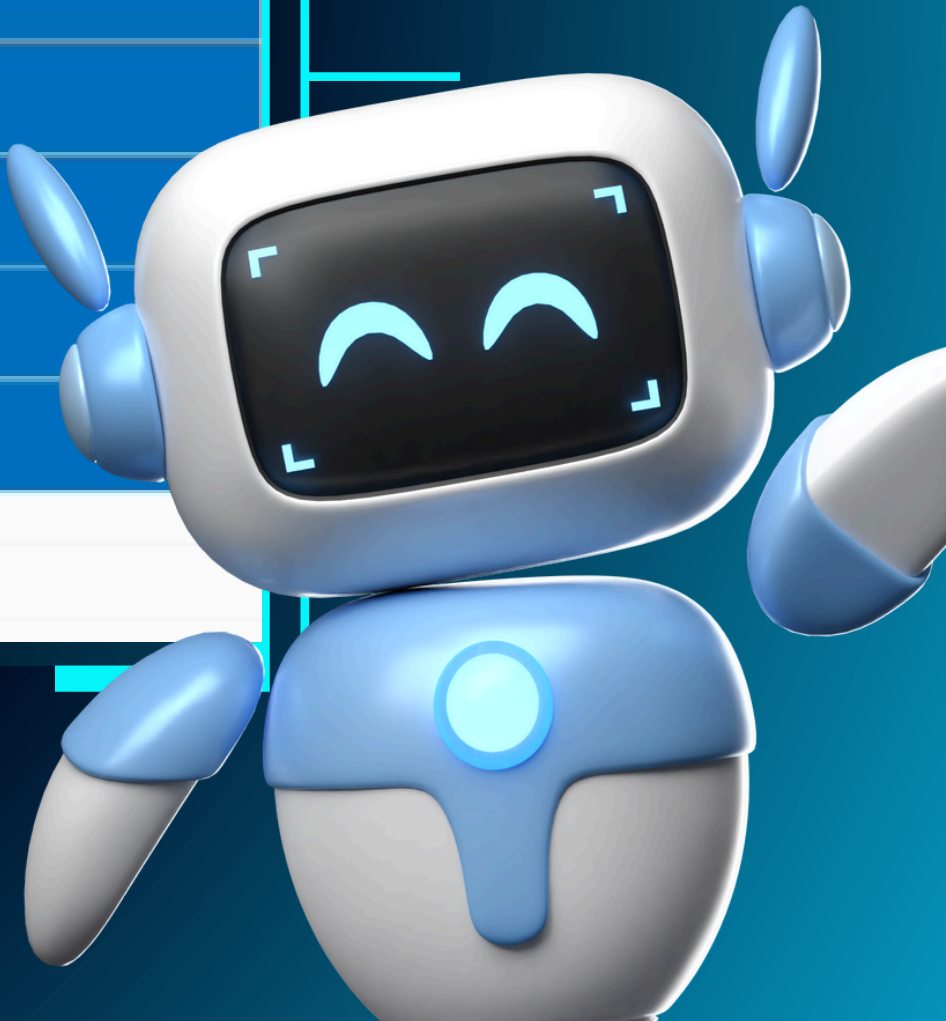


# 1 雲端服務簡介

| 地端(On-Premises) | 基礎設施即服務(IaaS) | 平台即服務(PaaS) | 軟體即服務(SaaS) |
|-----------------|---------------|-------------|-------------|
| 資料              | 資料            | 資料          | 資料          |
| 應用程式            | 應用程式          | 應用程式        | 應用程式        |
| 運行環境            | 運行環境          | 運行環境        | 運行環境        |
| 中介軟體            | 中介軟體          | 中介軟體        | 中介軟體        |
| 作業系統            | 作業系統          | 作業系統        | 作業系統        |
| 虛擬化             | 虛擬化           | 虛擬化         | 虛擬化         |
| 伺服器             | 伺服器           | 伺服器         | 伺服器         |
| 儲存              | 儲存            | 儲存          | 儲存          |
| 網路              | 網路            | 網路          | 網路          |

您管理

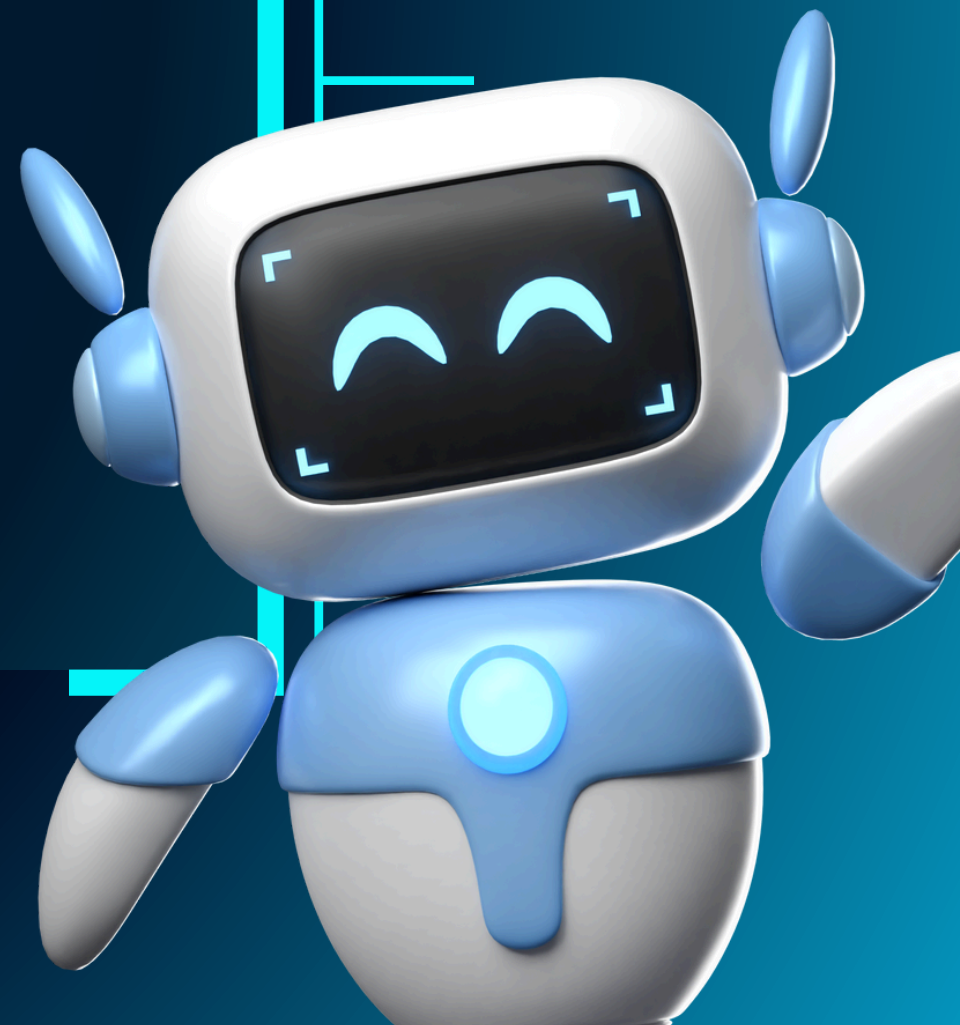
雲端服務供應商管理





## 雲端服務簡介

- 1.公有雲:供應商提，客戶支付費用或免費
- 2.私有雲:專為單一組織設定，提供專屬雲端環境。
- 3.混合雲:結合上述兩者
- 4.社區雲:多個組織共享一個雲端資源環境





1

# 雲端服務簡介

## 1-3 常見的雲端服務

- **Microsoft Office 365** : Word、Excel、PowerPoint、Outlook
- **Google Workspace** : Google文件、Google試算表、Google簡報、Gmail
- **影音平台** : Netflix、Disney+、YouTube
- **網路硬碟** : Dropbox、Google Drive、Microsoft OneDrive
- **線上會議平台或遠端通訊平台**
- **開發相關** : Amazon EC2、Github、Gitlab





## 雲端服務簡介

### 8個上雲的主要理由

成本效益

異地備援

敏捷彈性

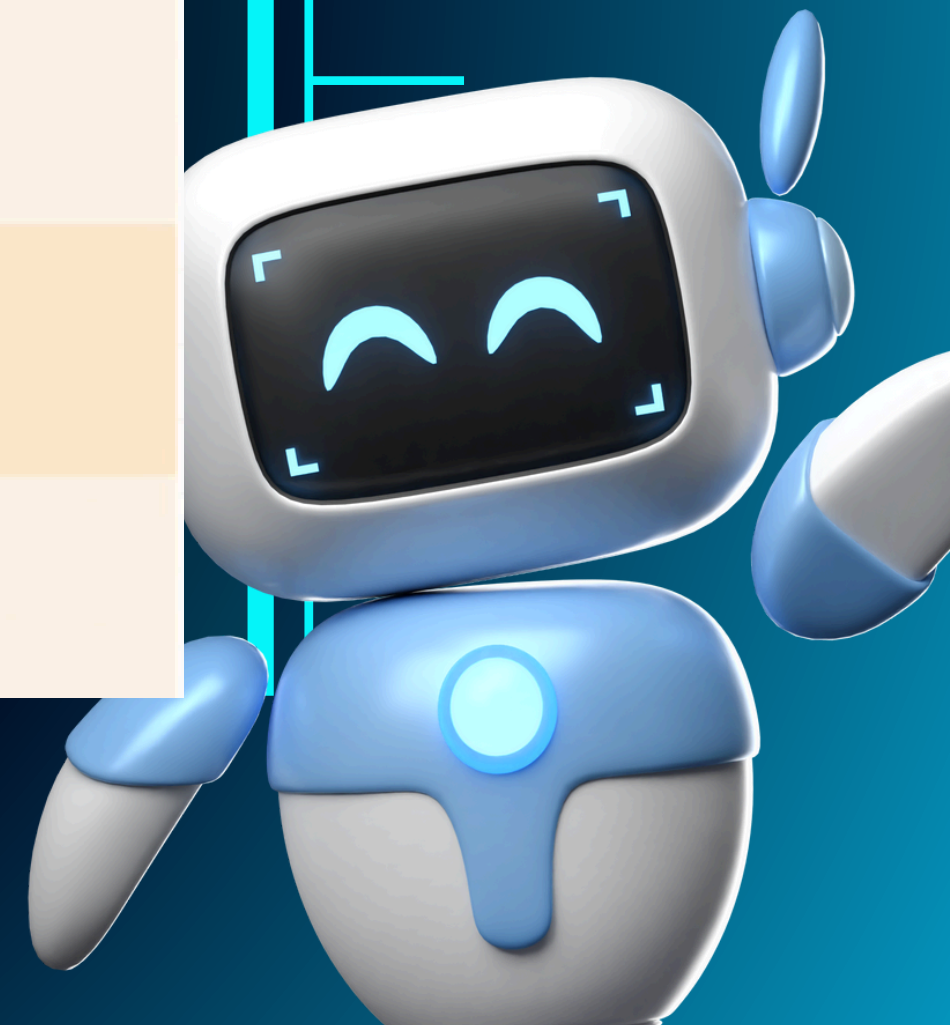
安全性

自動更新

\*符合性

遠端工作

碳足跡





1

## 雲端服務簡介

- ChatGPT、Microsoft Bing、Google Bard
- 物聯網的智慧家電
- 共享機車、美食外送

### • 車聯網

- **資料分析和收集**：持續收集和發送大量資料到雲端，包括車輛的運行資料、位置、故障診斷等，有助於改善產品和服務
- **行動應用**：允許車主遠程控制車輛、查看車輛狀態等
- **定期更新**：定期接收軟體更新用於修復錯誤，添加新功能或提高車輛性能、且不斷更新其地圖和自動駕駛演算法



- 根據雲端安全聯盟(CSA)2022/6/6的報告指出，Top 11雲端威脅如下

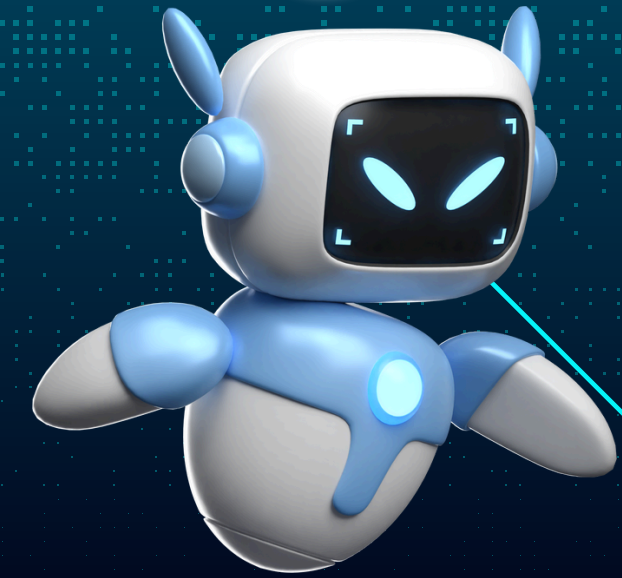
| 排名 | 雲端威脅名稱                  | 調查平均得分   |
|----|-------------------------|----------|
| 1  | 身分、憑證、存取和金鑰管理、特權帳號管理的不足 | 7.729927 |
| 2  | 不安全的介面和API              | 7.592701 |
| 3  | 配置不當和變更控制的不足            | 7.424818 |
| 4  | 缺乏雲端安全架構與策略             | 7.408759 |
| 5  | 不安全的軟體開發                | 7.275912 |
| 6  | 不安全的第三方資源               | 7.214493 |
| 7  | 系統漏洞                    | 7.143066 |
| 8  | 雲端運算資料的意外洩露             | 7.114659 |
| 9  | 無伺服器化和容器化工作負載的配置不當和利用   | 7.097810 |
| 10 | 有組織的犯罪、駭客和APT攻擊         | 7.088534 |
| 11 | 雲端儲存資料外洩                | 7.085631 |



Source: <https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-pandemic-eleven/>



## ④ POTENTIAL PROBLEMS



### 2-2 使用者應注意之雲端安全威脅

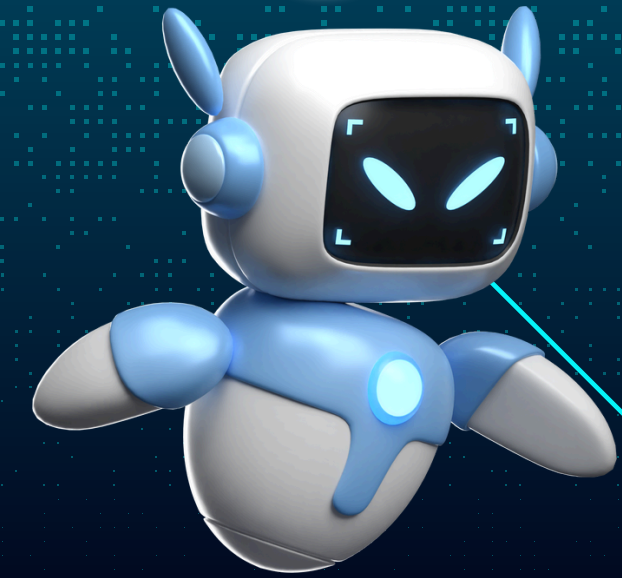
- 資料的安全性和隱密性

- 資料加密，資料壓縮加密，資料存取權限

- 帳號管理最佳實踐

- 特權帳號應嚴格控管
- 密碼要足夠複雜
- 應實施雙因子驗證

## ④ POTENTIAL PROBLEMS



### • 使用者資安意識、訓練與教育

- 資安意識(Awareness)：所有人。政策宣導、提高資安意識
- 訓練(Training)：特定一群人。達到對工作的要求或學會特定技能
- 教育(Education)：特定一群人。有證書或學位認證





## 雲端資料安全與保護



- 隱私權：個人資料保有被運用的權利
- 隱私處理原則：
  - 告知目的
  - 取得同意
  - 最小收集
  - 開放修改
  - 開放刪除
  - 做好資安
  - 出事通知
  - 出事負責



## 雲端資料安全與保護



- 去識別化：不算個資
- 匿名化：完全匿名且不可還原。例如
  - 把信用卡號的中間8位替換為XXXX-XXXX > 1234-XXXX-XXXX-5678
  - 1999/12/13 > 19XX/XX/31
  - 將姓名的順序打亂，「Ray Lin」變成「Ruru Cheng」
- 假名化：有條件回溯。例如
  - 加密患者的醫療記錄 12-34-5678 > u8~gA%D\*D+KaPdSg
  - 將信用卡號碼加密，但保持為16位數字 1234-5678-1234-5678 > jS1K-Kfj9-sjfL-!3fJ





### 3-5 資料的生命週期

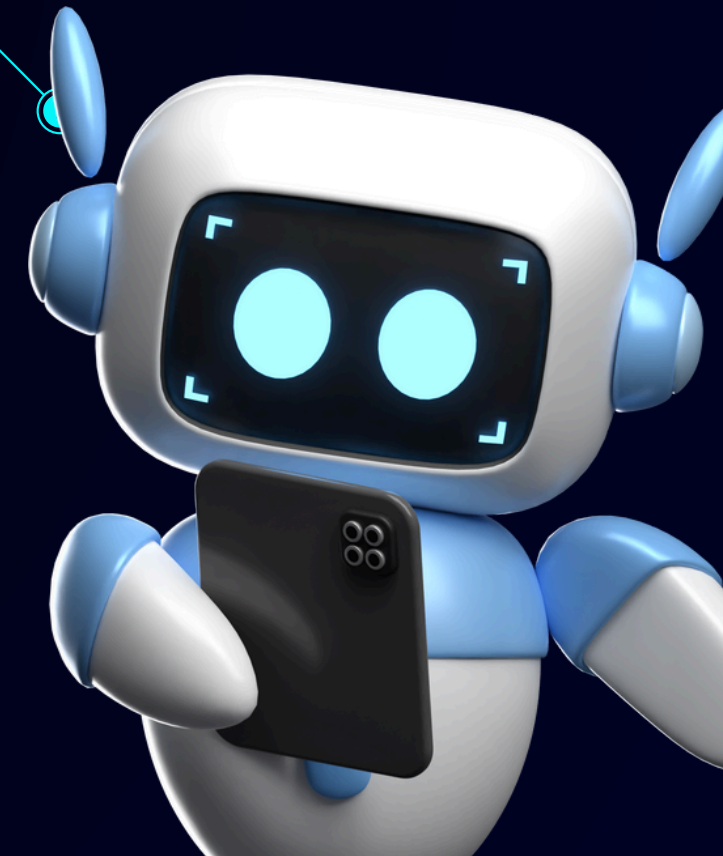
- **建立(Create)階段**：建立或生成新資料的階段。例如顧客在線上購物時填寫資料，或員工建立一份報告
- **儲存(Store)階段**：資料保存在某個位置的階段。例如資料庫、檔案，確保資料安全和完整性在此階段非常重要
- **使用(Use)階段**：資料被檢索和應用於某些特定目的或活動的階段。例如使用顧客資料進行銷售分析
- **分享(Share)階段**：資料被傳遞或分享給其他人或組織的階段。分享時要確保遵循適當的資料保護和隱私法規
- **封存(Archive)階段**：當資料不再經常使用，但仍需保存出於法律或業務原因時的階段，會進入此階段。封存的資料通常被存放在低成本的儲存解決方案中，且不常被存取
- **銷毀(Destroy)階段**：當資料不再需要，且沒有法律或規定要求繼續保存時，資料將被永久刪除或銷毀的階段。這通常涉及將物理媒體(如硬碟或紙張)進行碎片化或完全刪除以確保資料不可恢復



## ④ 身分驗證與存取管理

- 身分識別與存取管理(IAM, Identity and Access Management) : I+3A

1. 身分(Identity) : 可簡單當成帳號
2. 驗證(Authentication) : 常用密碼、簡訊或指紋
3. 授權(Authorization) : 誰授權、誰設定、誰控制，需注意職責分離
4. 記錄(Accounting) : 也可稱為會計、記帳或稽核 (Auditing)，並用於後續的可歸責性與追蹤，需注意特權帳號





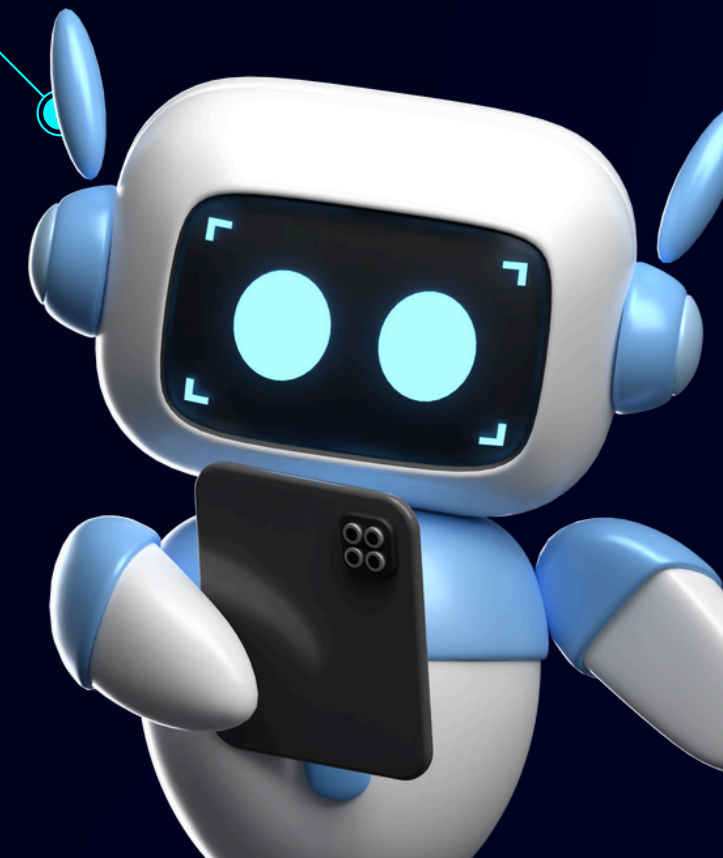
## ④ 身分驗證與存取管理

### • 身分驗證的因子

- 你知道的(Something you know)：只有你自己知道的資訊
- 你擁有的(Something you have)：目前你手上擁有的東西
- 長在身上(Something you are)：長在你身上的生物特徵

### • 多因子驗證(MFA)：三種身分驗證因子至少要包含兩種不同的因子

- 使用提款機領錢要插入金融卡+輸入密碼雙重驗證



## 4. 身分驗證與存取管理

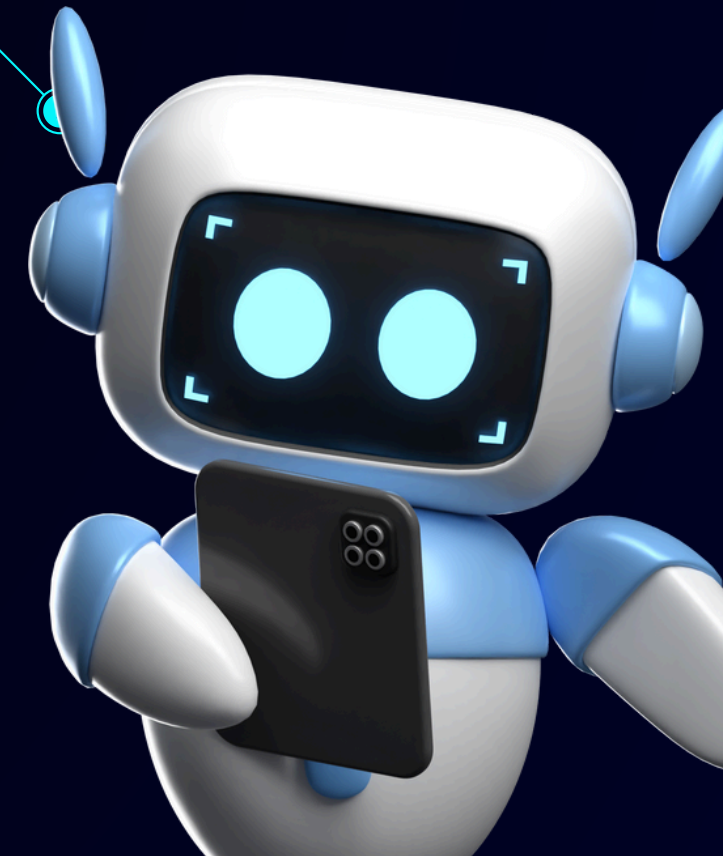
### • 你知道的(Something you know)

- 使用者帳號與密碼
- 個人識別碼(PIN)：插入銀行金融卡後要輸入的6-12位數字
- 安全問題：例如畢業的國小名稱、帳戶號碼、某一段特定的記憶或文字

### • 模式：圖形密碼

### • 知識型驗證

- CAPTCHA：用來確認使用者是人類的選擇正確圖片或輸入正確文字的挑戰
- 數學問題：例如  $3+4$  等於多少？

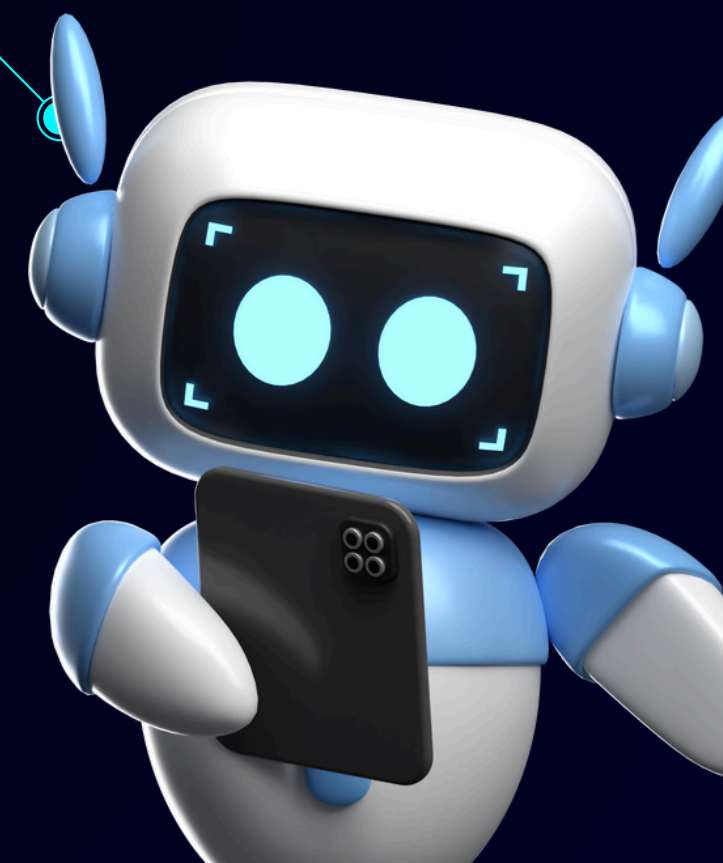




## 4. 身分驗證與存取管理

### • 你擁有的(Something you have)

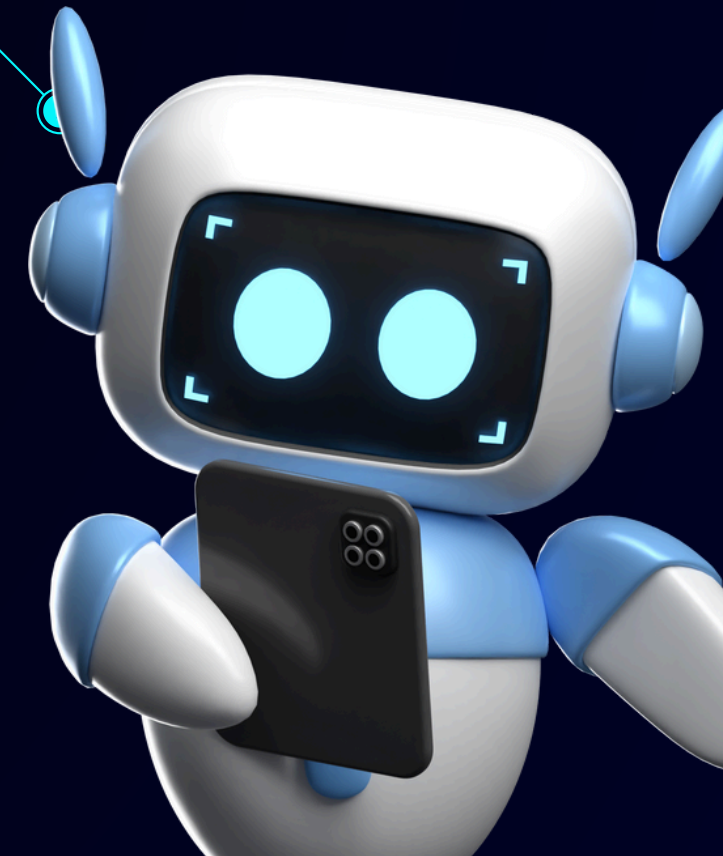
- 智慧卡(Smart Card)、RFID卡、磁條卡：將使用者唯一識別ID存在晶片IC或磁條以驗證身分，需要電力
- 智慧型手機、一次性密碼(OTP)、身分驗證應用程式
- 硬體Token：在LCD螢幕上每60秒自動變更密碼
- USB安全鑰匙：保存加密的密鑰資訊
- QR Code、NFC、藍牙裝置



## 4. 身分驗證與存取管理

### • 長在身上(Something you are)

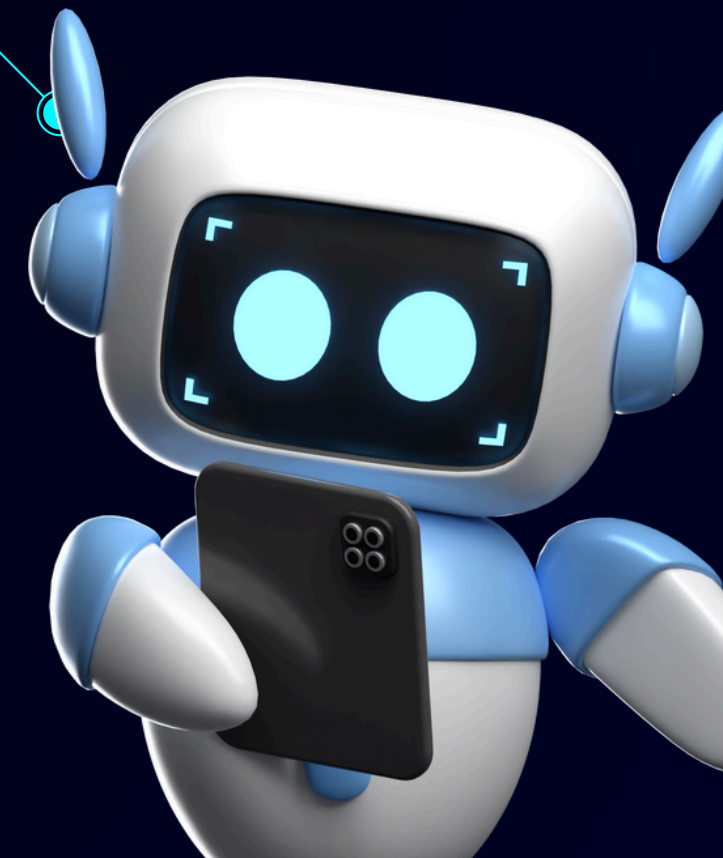
- **臉**：五官組合與位置、臉部輪廓、皮膚紋理、痣和疤痕位置、臉部的對稱性
- **手**：指紋、掌紋、指靜脈、手掌大小和形狀、指骨結構
- **眼**：虹膜、視網膜、瞳孔大小、眼白特點、眼瞼和睫毛特點
- **行為**：簽名的書寫方式、鍵盤打字方式和速度、行走的步態和節奏
- **聲音**：聲調和頻率、唇語和發音模式、聲音的響度和節奏
- **基因序列、染色體組成、遺傳標記和突變、血糖**





## 4. 身分驗證與存取管理

- 常見的網路硬碟：Dropbox、Google Drive、Microsoft OneDrive
- 重要資料備份：資料在雲端與本機都可以備份，以防勒索軟體
- 資料靜態加密：對資料加密後再上傳雲端
- 資料傳輸加密：使用SSL/TLS
- 加強帳號管理：使用多因子驗證進行保護



## 結語

- 資料是雲端中最有價值的資產，因此在「雲端資料安全與保護」的章節中，我們學習了如何分類、保護和管理這些資料，以確保其在雲端環境中的安全性。最後，在「身分識別與存取管理」章節，我們學習到存取雲端資源時應具備的安全觀念，以防止未經驗證與授權的存取。

