# HW03作業三:名詞解釋

* (資訊安全的基本需求共七項，CIA+鑑別性+不可否認性+存取控制+稽核)，使用老師要求格式~定義, 功能, 種類, 應用, 舉例…. etc. by Google Table, Youtube,News…
* 機密性(Confidentiality)、完整性(Integrity)、可用(Availability)、鑑別性(Authentication)、不可否認性(Non-repudiation)、存取控制(Access Control)與稽核(Audit)

I3B54 410706228 賴秉豐

## 機密性(Confidentiality)

### 定義:

確保資料傳遞與儲存的隱密性，避免未經授權的使用者有意或無意的揭露資料內容。

參考網站:

<https://zh.wikipedia.org/wiki/%E4%BF%A1%E6%81%AF%E5%AE%89%E5%85%A8#%E6%9C%BA%E5%AF%86%E6%80%A7>

### 功能:

不讓非授權使用者有意或無意地接露資料內容。

參考網站:

<https://zh.wikipedia.org/wiki/%E4%BF%A1%E6%81%AF%E5%AE%89%E5%85%A8#%E6%9C%BA%E5%AF%86%E6%80%A7>

### 種類:

**絕對機密**

具有最高機密性之資料，洩漏後，足以使國家安全受到最嚴重損害者。

**極機密**

機密資料，洩漏後，足以影響國家安全、或嚴重損害國家利益與尊嚴及對外國政府有重大利益者。

**機密**

機密資料，洩漏後，足以損害國家利益或尊嚴、或有利於外國者。

**密**

其他應保守機密者。

參考網站:

<https://www.lawbank.com.tw/treatise/lawrela.aspx?lsid=FL010639&ldate=20031001&lno=7,8,13,22,23,27,28,29,31>

### 應用:

**進階加密標準（AES）**

是美國聯邦政府採用的一種區塊加密標準。這個標準用來替代原先的DES，已經被多方分析且廣為全世界所使用。

參考網站:

<https://zh.wikipedia.org/wiki/%E9%AB%98%E7%BA%A7%E5%8A%A0%E5%AF%86%E6%A0%87%E5%87%86>

**資料加密標準（DES）**

是一種對稱密鑰加密塊密碼演算法，1976年被美國聯邦政府的國家標準局確定為聯邦資料處理標準（FIPS），隨後在國際上廣泛流傳開來。它基於使用56位金鑰的對稱演算法。

參考網站:

<https://zh.wikipedia.org/wiki/%E8%B3%87%E6%96%99%E5%8A%A0%E5%AF%86%E6%A8%99%E6%BA%96>

**RSA加密演算法**

是一種非對稱加密演算法，在公開金鑰加密和電子商業中被廣泛使用。

參考網站:

<https://zh.wikipedia.org/wiki/RSA%E5%8A%A0%E5%AF%86%E6%BC%94%E7%AE%97%E6%B3%95>

### 舉例:

**Youtube:**

影片標題:**Confidentiality**



影片網站:

<https://www.youtube.com/watch?v=celrmrAdBdc>

**新聞:**

標題: **矽格伺服器受病毒感染 機密資料無影響**

內容為最近IC封測廠矽格的公司伺服器遭受病毒感染，所幸機密資訊都沒有受到影響。



新聞網站

<https://tw.stock.yahoo.com/news/%E7%9F%BD%E6%A0%BC%E4%BC%BA%E6%9C%8D%E5%99%A8%E5%8F%97%E7%97%85%E6%AF%92%E6%84%9F%E6%9F%93-%E6%A9%9F%E5%AF%86%E8%B3%87%E6%96%99%E7%84%A1%E5%BD%B1%E9%9F%BF-080456092.html>

## 完整性(Integrity)

### 定義:

代表確保資料無論是在傳輸或儲存的生命週期中，保有其正確性與一致性。

參考網站:

<https://zh.wikipedia.org/wiki/%E4%BF%A1%E6%81%AF%E5%AE%89%E5%85%A8#%E6%9C%BA%E5%AF%86%E6%80%A7>

### 功能:

使資料能保有正正確性和一致性。

參考網站:

<https://zh.wikipedia.org/wiki/%E4%BF%A1%E6%81%AF%E5%AE%89%E5%85%A8#%E6%9C%BA%E5%AF%86%E6%80%A7>

### 種類:

**資料完整性(Data Integrity):**

資料或軟體的改變是符合規範並授權，而非破壞性的改變

**系統完整性(System Integrity):**

系統功能正確無誤，不會遭到非授權的串改產生問題

參考網站:

<https://r888800009.github.io/network-security/net-sec1/>

### 應用:

**HashTab完整性驗證軟體:**

是一種將指定的資料建立獨一無二「驗證指紋」的驗證方式，因此只要檔案內容被「更改過」其所運算出來的雜湊值一定會不同，如此便可以驗證檔案的完整性。

### 舉例:

**Youtube:**

影片標題: **What is Integrity?**

影片網站:

<https://www.youtube.com/watch?v=P4z-2wGkQdo>

**新聞:**

標題: **資安一周第170期：國內多家上市櫃公司遭到網路攻擊。半導體資安標準即將於12月發布**



新聞網站:

<https://www.ithome.com.tw/news/147644>

## 可用性(Availability)

### 定義:

在資訊安全領域，可用性（Availability）是成功的資訊安全計畫應具備的需求，意及當使用者需透過資訊系統進行操作時，資料與服務須保持可用狀況(能用)，並能滿足使用需求(夠用)。

參考網站:

<https://zh.wikipedia.org/wiki/%E4%BF%A1%E6%81%AF%E5%AE%89%E5%85%A8#%E6%9C%BA%E5%AF%86%E6%80%A7>

### 功能:

使資料和服務保持在可用且能滿足使用者需求的狀況。

參考網站:

<https://zh.wikipedia.org/wiki/%E4%BF%A1%E6%81%AF%E5%AE%89%E5%85%A8#%E6%9C%BA%E5%AF%86%E6%80%A7>

### 種類:

**高可用性:**

高可用性是指企業可以對抗停電的能力，包括排定的關機時間及網站災禍。學習判定高可用性目標及目的。

**容量上限:**

如果超出系統限制，您可能會遭受到應用程式中斷或系統中斷的狀況。只要事先注意容量上限及系統限制，即可避免這些中斷狀況。

參考網站:

<https://www.ibm.com/docs/zh-tw/i/7.3?topic=availability>

### 應用:

**使用 HADB 備援單元改善可用性:**

若要改善可用性，一律請如建立效能目標中所述，在資料備援單元 (DRU) 中使用 HADB 節點。

**使用 HADB 備用節點改善容錯**

使用備用節點改善容錯。雖然備用節點不是必要項目，但可提供最佳的可用性。

**規劃容錯移轉容量**

容錯移轉容量規劃是指決定需要額外增加至 Application Server 部署的伺服器與程序數目，如此一來，當伺服器或程序故障時，系統可緊密地回復資料並繼續處理。若系統超載，可能會產生程序或伺服器故障，造成回應時間變慢或甚至失去整個服務。為這類事件做足準備對於成功部署非常重要。

若要維持容量，特別是在尖峰負載時，要將執行應用程式伺服器實例的備用機器增加至現有的部署中。

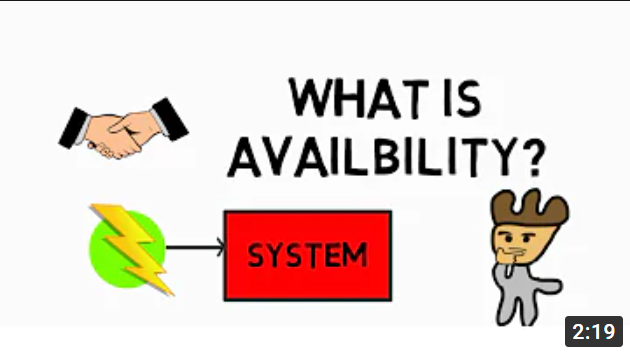
參考網站:

<https://docs.oracle.com/cd/E19159-01/820-4904/abfcy/index.html>

### 舉例:

Youtube:

影片名稱: **Thermodynamic Availability, What is?**



影片網址:

<https://www.youtube.com/watch?v=-04oxjgS99w>

**新聞:**

標題: **Windows 11 11月大規模推送 微軟稱已沒問題**

內容主要是Windows11官方已經改善處理了很多Bug。



新聞網址:

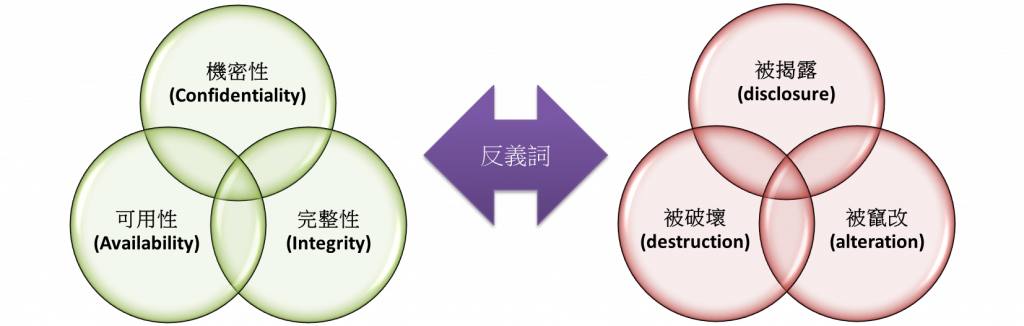
<https://news.xfastest.com/microsoft/102525/microsoft-windows-11-upgrade-4/>

### 補充:

機密性(Confidentiality)-----反義詞---->被揭露(Disclosure)

完整性(Integrity ) ------------反義詞---->被竄改(Alteration)

可用性(Availability)----------反義詞---->被破壞(Destruction)



圖片網站:

<https://ithelp.ithome.com.tw/articles/10238953>

## 鑑別性(Authentication)

### 定義:

識別資訊使用者的身分，可記錄資訊被誰所存取使用，例如：透過密碼或憑證方式驗證使用者身分。

實務做法：

參考網站:

<https://zh.wikipedia.org/wiki/%E4%BF%A1%E6%81%AF%E5%AE%89%E5%85%A8#%E6%9C%BA%E5%AF%86%E6%80%A7>

### 功能:

識別資訊使用者的身分，紀錄資訊被誰所存取使用。

參考網站:

<https://zh.wikipedia.org/wiki/%E4%BF%A1%E6%81%AF%E5%AE%89%E5%85%A8#%E6%9C%BA%E5%AF%86%E6%80%A7>

### 種類:

你所知道的（Something you know）：帳號／密碼

你所擁有的（Something you have）：IC卡、數位裝置、數位簽章、一次性密碼(OTP)

你所具備的（Something you are）：指紋、虹膜、聲紋、臉部特徵、靜脈脈紋、DNA

參考網站:

<https://zh.wikipedia.org/wiki/%E4%BF%A1%E6%81%AF%E5%AE%89%E5%85%A8#%E6%9C%BA%E5%AF%86%E6%80%A7>

### 應用:

**深偽技術（Deepfake）:**

又稱深度偽造，專指基於人工智慧的人體圖像合成技術的應用。此技術可將已有的圖像或影片疊加至目標圖像或影片上。

參考網站:

<https://zh.wikipedia.org/wiki/%E6%B7%B1%E4%BC%AA%E6%8A%80%E6%9C%AF>

### 舉例:

**Youtube:**

影片名稱: **What is Authentication**



影片網站:

<https://www.youtube.com/watch?v=927KdwZZoU0>

新聞:

標題: **Deepfake等於造假、違法？名聲敗壞的黑科技還能洗白？**

主要內容在介紹Deepfake和介紹各國的應用。



新聞網站:

<https://www.gvm.com.tw/article/83409>

## 不可否認性(Non-repudiation)

### 定義:

對一已發生之行動或事件的證明，使該行動或事件往後不能被否認的能力。

參考網站:

<https://isp.nuu.edu.tw/p/405-1074-1269,c82.php>

### 功能:

確保無法否認於系統上完成的操作。

參考網站:

<https://ithelp.ithome.com.tw/articles/10238953>

### 種類:

不可否認性服務對於訊息傳輸，可根據其幫助解決糾紛的類型進行分類，傳輸訊息至少涉及兩個實體，分別稱為原發者和接收者。涉及這類事件的潛在糾紛主要有兩類:

類型(一):事件的原發者受到懷疑，如被指控的原發者聲稱訊息被接收者偽造，或者被偽裝的攻擊者偽造。

類型(二)是捲入該事件的接收者受到懷疑，例如，被指控的接收者聲稱訊息沒有傳送，或者在傳輸中丟失，或者僅被偽裝的攻擊者接收。

### 應用:

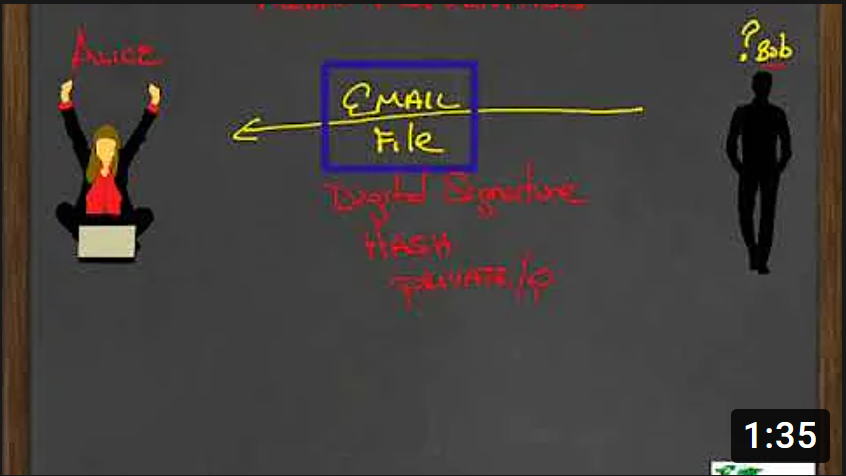
**數位簽章（英語：Digital Signature，又稱公鑰數位簽章）:**

是一種功能類似寫在紙上的普通簽名、但是使用了公鑰加密領域的技術，以用於鑑別數位訊息的方法。

### 舉例:

**Youtube:**

影片名稱: **Nonrepudiation**



影片網址:

<https://www.youtube.com/watch?v=CPZVYgSVnlA>

新聞:

標題:**證交所新聞**

主要內容為提供查詢開戶及交易資料服務



新聞網站:

<https://www.twse.com.tw/zh/news/newsDetail/5B0067CC8AE94628BC0EE6A36300964F>

## 存取控制(Access Control)

### 定義:

指對存取者向受保護資源進行存取操作的控制管理。該控制管理保證被授權者可存取受保護資源，未被授權者不能存取受保護資源。

參考網站:

<https://zh.wikipedia.org/wiki/%E5%AD%98%E5%8F%96%E6%8E%A7%E5%88%B6>

### 功能:

確保任何操作或人員均有適當的權限界定且受到合規的授權。

參考網站:

<https://ithelp.ithome.com.tw/articles/10238953>

### 種類:

存取控制有很多模型，比如：

**自主存取控制(英語：Discretionary access control):**

完全控制它們建立的物件或對它們的存取權限。

**強制存取控制(英語：Mandatory access control):**

基於物件的許可和物件的標籤而強制執行的系統。

**角色存取控制(英語：Role-based access control):**

定義組織中的角色，並為他們提供預設權限。

參考網站:

<https://ithelp.ithome.com.tw/articles/10218897>

**屬性存取控制(英語：Attribute-based access control):**

網路系統管理員應給檔案、目錄等指定訪問屬性。

參考網站:

<https://ithelp.ithome.com.tw/articles/10218897>

<https://www.easyatm.com.tw/wiki/%E8%A8%AA%E5%95%8F%E6%8E%A7%E5%88%B6>

### 應用:

**門禁系統:**

管制非特定人員進出某通道所使用的軟硬體系統。

參考網站:

<https://zh.wikipedia.org/wiki/%E5%AD%98%E5%8F%96%E6%8E%A7%E5%88%B6>

**多因素身份驗證：**

至少提供三種不同形式的身份認證中的兩種。

**會話管理：**

為用戶提供某種類型的憑證(Token)，他們使用憑證來獲取資源。

**註冊和身份證明：**

在註冊服務時：可能會要求您提供PII，其他人難以理解的個人問題。

**聯合身份管理（FIM）：**

在兩家公司之間共享身份驗證資料。

**憑證管理系統：**

密碼加密，防止未經授權的訪問

參考網站:

<https://ithelp.ithome.com.tw/articles/10218897>

### 舉例:

**Youtube:**

影片標題: **What is Access Control?**



影片網站:

<https://www.youtube.com/watch?v=GgquXOl4_t0>

**新聞:**

標題: **Access Control and Authentication Market Business Overview, Risks And Opportunities with COVID-19 Scenario to 2030**

主要內容為到2030 年 COVID-19疫情影響下，全球雙因素認證市場業務的概述、風險和機遇

新聞網站:

<https://www.taiwannews.com.tw/en/news/4330317>

## 稽核(Audit)

### 定義:

以有系統的過程，所有針對某項特定活動所進行之獨立調查均可稱為稽核。資安稽核的定義則為就所有資通訊實務作業，由稽核人員定期對機關之資訊安全管理。

參考網站:

<https://www.mjib.gov.tw/FileUploads/eBooks/60a5106846e1465785e637d70bd21f30/Section_file/2984620680ee4ae7a780721f21da7aeb.pdf>

### 功能:

針對某項特定活動進行獨立調查。

參考網站:

<https://www.mjib.gov.tw/FileUploads/eBooks/60a5106846e1465785e637d70bd21f30/Section_file/2984620680ee4ae7a780721f21da7aeb.pdf>

### 種類:

稽核種類分為三方，

**第一者稽核(First Party Audit):**

又稱「內部稽核」稽核人員通常為內部人員，是指公司內部自行實施作業流程與品質系統的自我診斷、檢討與評估。有稽核員不應該稽核本身工作的準則。

**第二者稽核(Second Party Audit):**

指公司對供應商的稽核。

**第三者稽核(Third Party Audit):**

所謂「第三者稽核」是指具有公信力的獨立認證機構，依一特定的標準對公司辦理評鑑，並發給證書以資證明。

參考網站:

<https://www.mjib.gov.tw/FileUploads/eBooks/60a5106846e1465785e637d70bd21f30/Section_file/2984620680ee4ae7a780721f21da7aeb.pdf>

<https://www.isoleader.com.tw/home/iso_news_detail/1317>

### 應用:

**電腦輔助稽核技術（Computer-assisted audit techniques，縮寫 CAATs）:**

是應用電腦進行稽核程序的自動化。最大特色為可以在個人電腦上操作，稽核人員可以至受查單位系統下載檔案至個人電腦再使用電腦輔助稽核軟體進行測試，其主要是讓稽核人員能更獨立地分析應用系統的資料檔。

**專業的稽核軟體:**

ACL、IDEA、Arbutus。

### 舉例:

**Table:**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **稽核者** | **被稽核者** | **舉例** |
| **第一者稽核** | 自家公司 | 自家公司 | 可口可樂公司進行內部作業流程之檢討與改進 |
| **第二者稽核** | 自家公司 | 外部公司 | 可口可樂公司對於各項原物料供應商之檢討評估 |
| **第三者稽核** | 第三方獨立機構 | 自家公司 | SGS對可口可樂進行評鑑與稽核 |

參考網站:

<https://www.isoleader.com.tw/home/iso_news_detail/1317>

**Youtube:**

影片標題: **匡騰安全檢查與稽核軟體介紹 (完整版) | 匡騰Quantum Compliance**



影片網站:

<https://www.youtube.com/watch?v=wWyMmmpUJwk>

**新聞:**

標題: **高雄警勾結不法業者洩漏個資案情擴大 警署：加強稽核、從嚴究辦**

主要內容為高雄市警察局近期發生員警涉嫌洩漏個資，案情逐漸擴大，因此要加強稽核機制，並要求各警察機關主動清查所屬員警有無違常使用情事。

****

新聞網站:

<https://news.ltn.com.tw/news/society/breakingnews/3718686>