

資通安全職能訓練

資通安全概論

Introduction
to Cyber Security

中華民國114年



數位發展部資通安全署
Administration for Cyber Security, moda

資通安全職能訓練

資通安全概論

Introduction
to Cyber Security

中華民國114年



數位發展部資通安全署
Administration for Cyber Security, moda

目錄 CONTENTS

前言

單元

1

資通安全基本觀念

- 1.1 資通系統之組成 16
- 1.2 建立資通安全之危機意識 19
- 1.3 資通安全之防護目標 21

單元

2

資通安全相關法規

- 2.1 我國資通安全管理體系 30
- 2.2 資通安全管理法與子法 34
- 2.3 其他相關法規 58

單元

3

資通安全風險管理

- 3.1 風險管理之流程 64
- 3.2 風險管理之全景建立 68
- 3.3 風險評鑑之作法 70
- 3.4 風險處理之作法 80
- 3.5 風險接受之作法 84
- 3.6 國際相關防護及管理標準 86

單元

4

資通安全管理面暨認知與訓練應辦事項

4.1	管理面－資通系統分級與防護基準	94
4.2	管理面－ISMS 之導入及 通過公正第三方之驗證	99
4.3	管理面－資通安全專責人員	105
4.4	管理面－內部資通安全稽核	106
4.5	管理面－業務持續運作演練	109
4.6	管理面－資通安全治理成熟度	123
4.7	認知與訓練－資通安全教育訓練	138
4.8	認知與訓練－資通安全專業證照及 職能訓練證書	140

單元

5

資通系統防護控制措施

5.1	「存取控制」之安全控制措施	146
5.2	「事件日誌與可歸責性」之安全控制措施	150
5.3	「營運持續計畫」之安全控制措施	155
5.4	「識別與鑑別」之安全控制措施	161
5.5	「系統與服務獲得」之安全控制措施	178
5.6	「系統與通訊保護」之安全控制措施	183
5.7	「系統與資訊完整性」之安全控制措施	194
5.8	「媒體控管及可攜式設備」之安全控制措施	19

單元

6

資通安全技術面應辦事項 — 資通安全之防護及偵測

6.1	「防毒軟體」之安全防護	204
6.2	「網路防火牆」之安全防護	209
6.3	「應用程式防火牆」之安全防護	214
6.4	「電子郵件過濾機制」之安全防護	218
6.5	「IDS 與 IPS」之安全防護	222
6.6	「APT」之攻擊防禦措施	228
6.7	「SOC」管理機制	231
6.8	「GCB」組態基準	235
6.9	「VANS」通報機制	239
6.10	「EDR」偵測及應變機制	242

單元

7

資通安全技術面應辦事項 — 安全性檢測及資通安全健診

7.1 安全性檢測	246
7.2 弱點掃描	247
7.3 滲透測試	258
7.4 應用程式安全	262
7.5 資通安全健診	271
7.6 網路安全	275
7.7 實體安全	296

單元

8

資訊委外安全管理

8.1 資訊委外之相關法規	312
8.2 資訊委外之類別及形態	317
8.3 資訊委外之風險	319
8.4 資訊委外之生命週期	321
8.5 資訊委外之資安要求	323

單元

9

資通安全事件通報及應變

9.1 資通安全事件通報及應變流程	328
9.2 資通安全事件通報及應變作業規範	340
9.3 資通安全事件等級評估	342
9.4 資通安全事件通報及應變作業流程	355
9.5 資通安全事件通報及應變演練作業	364
9.6 資通安全事件處理	366
9.7 數位證據及數位鑑識	379
9.8 社交工程	381

圖目次

圖 1	CNS 27002 之資產分類	18
圖 2	機密性威脅示意圖	22
圖 3	完整性威脅示意圖	22
圖 4	可用性威脅示意圖	23
圖 5	CIA 保護之不同防護技術與方法示意圖	26
圖 6	我國資通安全組織架構圖	31
圖 7	我國資通安全管理體系之層級架構圖	32
圖 8	第七期國家資通安全發展方案之推動策略與具體措施	33
圖 9	《資通安全管理法》適用對象之法規強度	39
圖 10	《資通安全管理法》適用對象之法規	40
圖 11	風險定義示意圖	65
圖 12	資通安全風險管理流程圖	66
圖 13	高階風險評鑑作法流程圖	72
圖 14	風險處理流程圖	80
圖 15	NIST 網路安全框架之核心功能圖	87
圖 16	營運持續計畫時程	112
圖 17	業務持續運作之管理程序圖	118
圖 18	資安治理與資安管理之關係圖	124
圖 19	資安治理架構與相關法規之關聯圖	125
圖 20	資安治理評估推動方式	136
圖 21	雜湊函式運作示意圖	154
圖 22	營運持續計畫之時間指標圖	157
圖 23	完整備份、差異備份及增量備份示意圖	158

圖 24	完整備份與差異備份範例	159
圖 25	完整備份與增量備份範例	159
圖 26	生物特徵登錄步驟流程圖	168
圖 27	生物特徵鑑別步驟流程圖	169
圖 28	同步式一次性通行碼技術流程圖	172
圖 29	非同步式一次性通行碼技術流程圖	174
圖 30	詰問與回應身分鑑別技術流程圖	175
圖 31	對稱式加解密運作流程圖	186
圖 32	對稱式加密之私密金鑰數量示意圖	187
圖 33	非對稱式加解密運作流程圖	188
圖 34	數位信封運作流程圖	189
圖 35	雜湊函式運作流程圖	191
圖 36	數位簽章運作流程圖	192
圖 37	防毒軟體部署方式示意圖	206
圖 38	網路防火牆部署範例	210
圖 39	網路防火牆 HA 部署示意圖	212
圖 40	網站 / 網頁應用程式防火牆示意圖	214
圖 41	硬體式 WAF 部署示意圖	216
圖 42	軟體式 WAF 部署示意圖	216
圖 43	匣道模式部署示意圖	219
圖 44	Bridge 部署示意圖	220
圖 45	IDS/IPS 設備部署位置示意圖	224
圖 46	資通安全威脅偵測聯防機制圖	233

圖 47	VANS 資訊資產涵蓋範圍	240
圖 48	弱點掃描流程圖	249
圖 49	內部掃描及外部掃描示意圖	251
圖 50	滲透測試流程圖	259
圖 51	程式庫維護流程圖	266
圖 52	應用程式輸入資料及輸出結果示意圖	268
圖 53	輸入惡意資料之風險示意圖	268
圖 54	網路區域規劃示意圖	276
圖 55	遠端使用者存取 VPN 示意圖	282
圖 56	Site-to-Site VPN 示意圖	282
圖 57	Extranet VPN 示意圖	283
圖 58	CMMC Model 2.0 之模型及評鑑	287
圖 59	雲端系統之一般架構	290
圖 60	雲端服務提供者及客戶之存取控制示意圖	291
圖 61	縱深防禦機制流程圖	297
圖 62	安全區域劃分示意圖	299
圖 63	安全偵測與滅火器位置規劃示意圖	300
圖 64	資通安全事件通報及應變作業時序流程圖	358
圖 65	公務機關資通安全事件通報及應變作業流程圖	359
圖 66	特定非公務機關資通安全事件通報及應變作業流程圖	362
圖 67	社交工程電子郵件案例	386

表目次

表 1	《資通安全管理法》條文摘要	35
表 2	《資通安全管理法施行細則》條文摘要	41
表 3	《資通安全責任等級分級辦法》條文摘要	45
表 4	《特定非公務機關資通安全維護計畫實施情形稽核辦法》條文摘要	48
表 5	《資通安全事件通報及應變辦法》條文摘要	50
表 6	《資通安全情資分享辦法》條文摘要	53
表 7	《公務機關所屬人員安全事項獎懲辦法》條文摘要	55
表 8	《資通安全管理法》與《個人資料保護法》比較	59
表 9	機密性之安全等級定義	74
表 10	完整性之安全等級定義	75
表 11	可用性之安全等級定義	76
表 12	法律遵循性之安全等級定義	77
表 13	管理面 - 資通系統分級與防護基準規定	94
表 14	資通系統防護需求分級原則	95
表 15	資通系統防護基準摘要	97
表 16	管理面 - ISMS 導入及驗證規定	99
表 17	ISO/IEC 27000 常見系列標準	100
表 18	CNS 27002 2023 之各章節名稱	102
表 19	管理面 - 資通安全專職人員規定	105
表 20	管理面 - 內部資通安全稽核規定	106

表 21	資通安全稽核類型	107
表 22	管理面 - 內部業務持續運作演練規定	109
表 23	管理面 - 資通安全成熟度評估規定	123
表 24	資安治理之流程構面與目標	125
表 25	能力度之等級及定義	127
表 26	成熟度之等級及定義	129
表 27	成熟度等級與流程構面之對應關係	133
表 28	資安治理成熟度等級之計算範例	134
表 29	資通安全認知與訓練應辦事項	138
表 30	資通系統防護基準之控制措施	144
表 31	存取控制構面之安全控制措施	146
表 32	事件日誌與可歸責性構面之安全控制措施	150
表 33	營運持續計畫構面之安全控制措施	155
表 34	識別與鑑別構面之安全控制措施	161
表 35	系統與服務獲得構面之安全控制措施	178
表 36	系統與通訊保護構面之安全控制措施	183
表 37	系統與資訊完整性構面之安全控制措施	194
表 38	資通系統防護基準參考資源	197

表 39	IDS 與 IPS 之差異比較	225
表 40	安全性檢測規定	246
表 41	弱點掃描服務範圍設備清單	256
表 42	弱點掃描工作項目	257
表 43	滲透測試之類型及類別	259
表 44	黑箱檢測法與白箱檢測法比較表	269
表 45	資通安全健診之辦理項目及頻率	272
表 46	雲端運算之服務模式	286
表 47	不同類型可燃物之滅火方式	308
表 48	政府資訊作業委外資安參考指引清單	315
表 49	資通安全事件等級評估表	342
表 50	資通安全事件機密性影響等級評估表	344
表 51	資通安全事件完整性影響等級評估表	346
表 52	資通安全事件可用性影響等級評估表	348
表 53	資通安全事件 CIA 影響等級評估總表	350
表 54	資通安全事件等級評估案例（一）	351
表 55	資通安全事件等級評估案例（二）	353
表 56	機關應配合辦理通報及應變之演練項目	365



前言

在數位化浪潮席捲全球的今日，資通安全已不再僅是技術人員的專屬領域，更超越了傳統資訊技術的範疇，更成為國家韌性的基石，企業營運的命脈，以及個人生活安寧的保障。

隨著物聯網、雲端運算、人工智慧等技術的飛速發展，我們的所有活動與資訊都前所未有地依賴資通網路與系統。從日常的線上購物、社交互動，到企業的核心業務運營、關鍵基礎設施（如電力、通訊、金融等）的穩定運作，無不置身於數位環境之中。這使得網路空間不僅是創新的搖籃，也成為各種風險與威脅的溫床。

資通安全所面臨的挑戰，已從單純的病毒感染演變為更為複雜、隱蔽且具有高度針對性的攻擊，例如國家級駭客攻擊、勒索軟體、惡意軟體、資料外洩、網路詐騙及社交工程攻擊等。這些威脅不僅可能導致個人隱私侵犯、財產損失，甚至影響個人日常生活的便利性；對企業而言，更可能造成營運中斷、鉅額財務損失、商譽受損，以及嚴峻的法律責任。事實上，資通安全事件的影響範圍與深度已遠超想像，輕則影響單一系統，重則癱瘓整個產業鏈，甚至危及國家安全與社會穩定。

資通安全防護不再是被動的應變控制措施，而是一種前瞻性的戰略部署，需要持續的警覺、專業的知識及跨領域的協作。無論您是資安領域的專業人士，或是任何組織中的一份子，乃至於每一位數位時代的公民，學習並掌握資通安全知識，已成為不可或缺的能力。

本概論之設計旨在全面性地探討資通安全領域，從宏觀的策略層面，深入探討組織落實資通安全政策與推動計畫上的考量；接著轉向管理層面，了解資通安全管理體系與日常運營中的應辦事項；最後則聚焦於技術層面，剖析各類資通安全防護技術與偵測應變措施。

本概論設定了明確的學習目標，旨在協助讀者充分掌握核心內容，從中獲得最大的學習效益，並將以此作為您未來資通安全職能訓練發展的起點，特別是銜接數位發展部資通安全署所推動的「資安職能訓練發展藍圖」，為後續進階學習課程奠定更穩固的基礎。

單元

1

資通安全基本概念

在數位化時代，資通安全已成為保障國家、社會與個人數位生活的重要基石。要有效地實踐資通安全，必須先從最根本的概念開始理解。本單元將引導深入探索資通系統的組成元素，剖析資通安全威脅的本質，並協助您建立必要的危機意識。同時，將明確闡述資通安全所追求的核心防護目標。

本單元學習重點如下：

- 1** 了解資通系統的組成元素，包括其定義與構成要素。
- 2** 建立對資通安全威脅的危機意識，認識潛在的危害與廣泛影響。
- 3** 了解資通安全的核心防護目標，掌握其在實務中的重要性。



1.1

資通系統之組成

在深入探討資通安全之前，我們必須清楚界定所要保護的對象。依據我國《資通安全管理法》第 3 條用詞定義的第 1 款及第 2 款，我們所要保護的核心正是「資通系統」與「資通服務」

1.1.1 資通系統

《資通安全管理法》第 3 條第 1 款定義：**資通系統**係指「用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統」。

- (1) 資通系統是指所有涉及資訊處理的軟硬體與網路環境的總稱。這涵蓋了從資訊的產生、處理、傳輸到最終的儲存與銷毀的整個生命週期中所使用的各種系統。
- (2) 例如：**考選部全球資訊網**是提供資訊流通的平台；**eCPA 人事服務網及公文系統**涉及資訊的蒐集、儲集與處理；**差勤系統**則管理人員的資訊與流程。這些都是我們日常運作中不可或缺的資通系統。

1.1.2 資通服務

《資通安全管理法》第 3 條第 2 款定義：**資通服務**係指「與資訊之蒐集、控制、傳輸、儲存、流通、刪除、其他處理、使用或分享相關之服務」。

- (1) 資通服務則是指圍繞在資通系統周邊，所有與資訊處理相關的支援性活動。
- (2) 例如：日常之個人電腦維護服務，旨在確保終端設備穩定運作，屬於資訊可用性的服務範疇；而伺服器維護服務，則著重於機房內核心系統之連續與穩定。此類維運服務雖非系統本體，卻是確保系統功能持續可用的關鍵環節。

1.1.3 關鍵要素

除了法律上的定義，從實務角度來看，資通系統的組成可以更細分為以下

五個關鍵要素，共同構成了我們需要保護的對象。了解這些要素，有助於我們全面性地評估資安風險，並採取適當的防護措施：

- ◆ **資訊 / 資料 (Information/Data)**：這是最核心且直接的保護對象。其涵蓋各種形式的數位數據，例如文件、檔案、資料庫、個人資料、業務流程數據等。保護資訊的機密性、完整性與可用性是資安的首要目標。
- ◆ **軟體 (Software)**：指應用程式、作業系統、資料庫管理系統等。保護軟體的完整性及可用性至關重要，以確保系統功能正常運作，不被惡意程式或不當修改影響。
- ◆ **硬體 (Hardware)**：包含電腦、伺服器、網路設備、儲存裝置等實體設備。這類資產需要實體與邏輯層面的保護，以防範被破壞、竊取或不當存取。
- ◆ **網路 (Network)**：指連接所有系統的基礎設施，如路由器、交換器、防火牆、傳輸線路等。網路是資訊傳輸的管道，必須確保其安全性，防止未經授權的存取、監聽或阻斷服務。
- ◆ **人員 (People)**：這是資通安全中最常被忽略但卻至關重要的環節。包括系統使用者、管理者、開發人員、維護人員等。人員的資安意識、行為規範及專業技能，直接影響資安防護的成效。許多資安事件往往源於人為疏失或社交工程攻擊，而非單純的技術漏洞，例如：機關同仁誤點擊釣魚郵件，可能導致憑證外洩。

1.1.4 CNS 27002：2023 之資產定義

為了更系統化地管理這些保護對象，我國標準 **CNS 27002：2023**（資訊安全、網宇安全及隱私保護 - 資訊安全控制措施，其內容與國際標準 **ISO/IEC 27002** 相對應）定義了「資產」的概念，將對組織具備價值的任何事物皆視為資產。

(1) 資產可以進一步細分為兩大類，如圖 1CNS 27002 之資產分類所示。

- ◆ **主要資產**：指對組織核心運作至關重要的資產，包括**資訊（包含資料）及營運過程與活動（組織的核心運作方式及相關活動）**。這些資產的受損將直接影響組織的使命與目標。
- ◆ **支援資產**：指支持主要資產運作所需的基礎設施與資源，包括**硬體、軟體、網路、人員、場域 (Site)**（例如機房、辦公地點）以及**組織結構（例如部門、職責劃分）**。這些支援資產的穩定性是主要資產安全運行的前提。

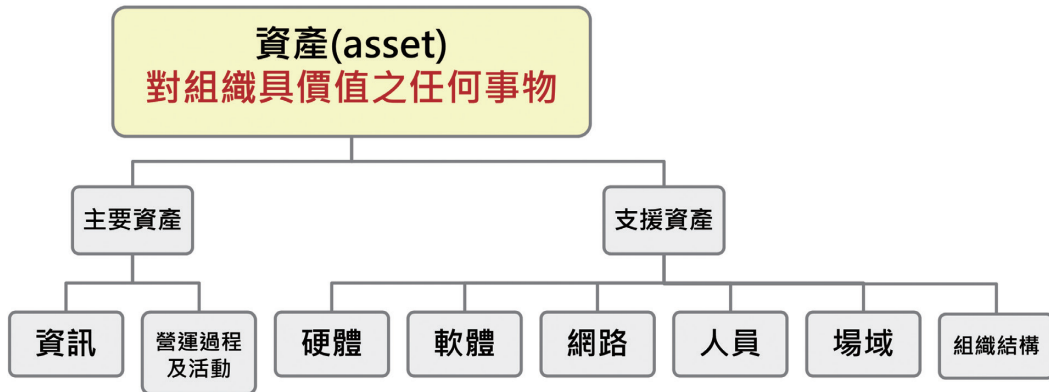


圖 1 CNS 27002 之資產分類

- (2) 資通系統的組成是多元且複雜的，涵蓋了資訊、技術、流程與人員等多個面向。有效的資通安全管理，必須從全面識別、評估並保護這些有價值的資產開始，確保無論是核心資訊或資料，還是支援其運作的基礎設施，都能得到適當的保護。

1.2

建立資通安全之危機意識

資通安全不單純是技術層面的問題，更是一種思維模式與普遍的認知。在快速變化的數位環境中，建立資通安全的危機意識是每個人、每個組織的首要任務。這種深植人心的意識，正是所有防護措施得以有效實施的基石。

1.2.1 資安威脅的潛在影響超乎想像

現今的資安威脅已非傳統的單純病毒感染，其規模與影響能力已達到前所未有的程度，往往超乎一般人的想像。當關鍵資通系統遭受攻擊並停擺時，可能導致嚴重的連鎖反應：

- (1) 對公共服務的衝擊：例如，醫院的資訊系統癱瘓可能導致病患照護中斷，危及生命；政府機關的系統停擺則可能導致公共服務無法提供，影響社會正常運轉。
- (2) 對企業營運的影響：企業可能面臨生產停滯、供應鏈中斷、客戶服務癱瘓等問題，進而導致鉅額的財務損失及市場競爭力下降。
- (3) 對國家安全的威脅：關鍵基礎設施（如電力、交通、通訊、金融等）若遭受網路攻擊，可能導致大規模的社會混亂，甚至危及國家安全。

1.2.2 資安攻擊無孔不入，影響層面廣大

隨著科技的進步，網路攻擊的途徑與手法也日益多元與隱蔽，使得資安威脅無所不在，影響範圍也日益擴大：

- (1) 物聯網 (IoT) 的雙面刃：物聯網裝置雖然帶來了極大的便利性與商機，但許多裝置在設計之初並未充分考慮資安問題，使其成為駭客入侵的新入口，增加了被攻擊的風險。一個被入侵的智慧家電可能成為跳板，進而攻擊整個家庭網路，甚至影響其他連結裝置。
- (2) 行動與無線通訊的便利與風險：手機、平板與無線網路的普及，使得我們隨時隨地都能存取資訊。然而，這些便利也伴隨著更大的資安風險。一旦



行動裝置或無線網路受到攻擊，個人資料可能外洩，通訊可能被監聽，甚至生活品質也會受到嚴重影響。

1.2.3 資安是每一個人應有的責任與警覺

資通安全絕非僅是資安專業人員的責任，其與我們每一個人息息相關：

- (1) 與國家安全息息相關：在網路戰與資訊戰日益頻繁的當代，資安問題有時已上升到國家安全的層次。保護數位環境，就是保護國家主權與人民福祉。
- (2) 現代公民的基本素養：在這個全面數位化的時代，具備一定的資安知識及警覺性，就像識字一樣重要。每個人都應了解基本的資安防護常識，例如：辨識釣魚郵件、使用強密碼、不隨意點擊不明連結、定期更新系統與應用程式、定期備份資料等。這些看似微小的個人行為，累積起來卻是國家整體資安防線的重要組成部分。

建立資通安全的危機意識，就是要認清資安威脅的普遍性與嚴重性，理解其對個人、組織乃至國家的潛在危害。唯有全民共同提升資安素養，從自身做起，保持警覺，才能有效地應對挑戰，共同築起堅不可摧的資安防線。

1.3

資通安全之防護目標

資通安全的核心目的在於保護資通系統與資訊資產免受各種威脅。要達到這個目標，資通安全領域確立了幾個關鍵的防護目標，其中最廣為人知且基礎的是「機密性、完整性、可用性」三原則，簡稱 **CIA (Confidentiality, Integrity, Availability)**。此外，對於政府機關或特定非公務機關而言，「法律遵循性 (Legal compliance)」也同樣重要。

1.3.1 資通安全的核心目標：CIA 三目標

依據《資通安全管理法》第 3 條第 3 款定義，**資通安全**是指「防止資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其「**機密性、完整性及可用性**」。這明確指出了資通安全的 3 個核心防護面向。

(1) 機密性 (Confidentiality)：

- ◆ **定義**：確保資訊不被未經授權的人員或系統存取。敏感資訊只能經由授權之人員或系統存取。
- ◆ **目標**：防止非授權人員存取資訊，確保資訊的秘密性與隱私。
- ◆ **重要性**：若機密性受損，可能導致個資外洩、商業機密被竊、國家機密洩露等嚴重後果。
- ◆ **解決方案**：常見的保護措施，包括資料加解密、存取控制、資料遮罩、去識別化等。
- ◆ **圖 2 機密性威脅示意圖**，顯示有一個人坐在電腦前，透過網路（地球圖示）傳輸資訊；中間有一隻眼睛被箭頭指向；另紅底白字標示 “loss of Confidentiality”，表示如果機密性沒有保護好，資訊就可能被洩漏。箭頭也指向電腦及網路，表示洩漏的途徑可能來自這兩端。

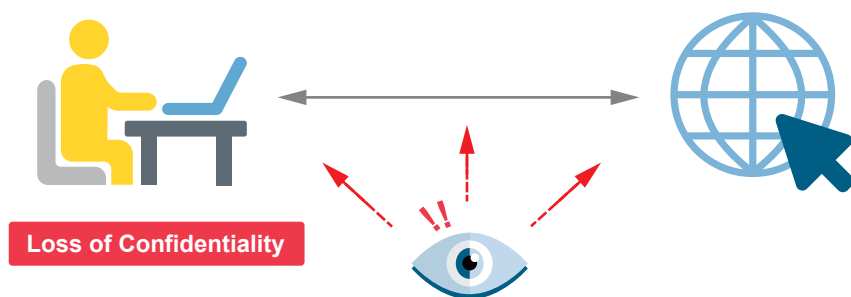


圖 2 機密性威脅示意圖

- ◆ **機密性案例：**某機關委外辦理推廣活動，廠商直播時不慎透漏抽獎網址，導致中獎人個人資料（姓名、手機）外洩。這直接影響了個資的機密性。
- ◆ **建議防範措施：**建議直播活動預先演練，確認內容無不當揭露；機關辦理對外活動或公告時，應確認內容妥適性及資安管理措施，避免資料外洩；敏感資訊應進行去識別化處理，降低外洩風險。

(2) 完整性 (Integrity)：

- ◆ **定義：**確保資訊在生命週期中持續正確、具一致性且可被信任。防止未經授權的修改或破壞。
- ◆ **目標：**防止非授權人員竄改資訊，確保資訊的正確性、可靠性與未被更動。
- ◆ **重要性：**若完整性受損，可能導致資訊失真、業務流程錯誤、甚至系統功能異常。
- ◆ **解決方案：**常見的保護措施，包括資料驗證、數位簽章、完整性驗證等。
- ◆ **圖 3 完整性威脅示意圖，**顯示一個人坐在電腦前，透過網路（地球圖示）傳輸資訊。中間有一個戴著帽子的可疑人物，表示資訊在傳輸過程中可能被竄改，導致「loss of integrity」。右下角有一個例子：「Buy 1 item => Buy 10,000 items」，說明了資料被竄改後可能造成的錯誤結果。

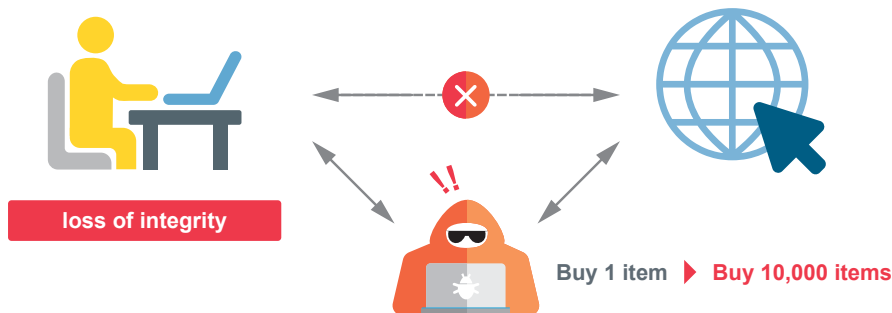


圖 3 完整性威脅示意圖

- ◆ **完整性案例：**某機關委請廠商進行個人電腦維護，駐點工程師因作業疏失輸入錯誤代碼，將機關內約 300 多台電腦的硬碟檔案刪除。這嚴重影響了資料的完整性。
- ◆ **建議防範措施：**定期備份重要資料以防範資料遺失；進行重大變更作業前，應先進行小範圍測試後再執行，減少錯誤操作的影響範圍；並應進行多重審核機制，以確保操作正確性。屬高等級之資通系統，其備份資料應進行異地保存。

(3) 可用性 (Availability)：

- ◆ **定義：**確保資訊與資源在需要時，可被授權使用者存取與使用，且系統功能正常運作。
- ◆ **目標：**防止系統故障或人為惡意阻斷服務，確保資訊與資訊處理的可獲得性。
- ◆ **重要性：**若可用性受損，可能導致服務中斷、業務停擺、用戶無法存取關鍵資源。
- ◆ **解決方案：**常見的保護措施，包括系統備援、系統監控、容量規劃、資料備份、容錯與負載平衡等。
- ◆ **圖 4 可用性威脅示意圖，**顯示一個人坐在電腦前，想要透過網路（地球圖示）存取資訊，但地球圖示上出現一個紅色的「X」及「404」錯誤訊息，下方標示 "loss of Availability"，表示網路或系統發生問題，導致資訊無法存取，喪失了可用性。

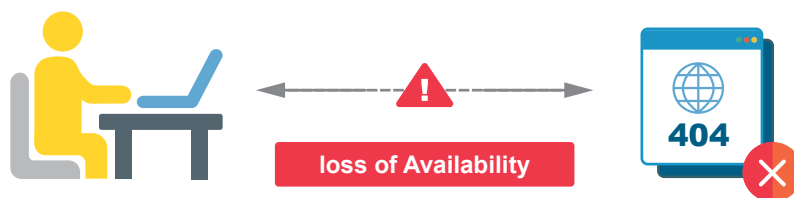


圖 4 可用性威脅示意圖

- ◆ **可用性案例：**113 年 10 月底康芮颱風過境，影響部分地區電力設施，部分機關因電壓供電不穩，致空調設備或主機設備異常，進而影響系統服務。這導致了服務的可用性受損。
- ◆ **建議防範措施：**機房電力、空調及資通系統服務等皆需建置備援機制，避免因斷電或供電不穩造成服務中斷；規劃與辦理核心業務或重要資通



系統之營運持續演練 (BCP)，並將電力異常納入演練情境，確保事件發生時可緊急切換。

(4) 法律遵循性 (Legal compliance)

除了 CIA 三目標外，對於政府機關（構）及特定非公務機關而言，「法律遵循性」同樣是資通安全的重要目標。

- ◆ **定義：**確保所欲保護的資訊內容與所有資安活動，皆遵循相關的法規要求。
- ◆ **目的：**確保組織的資安措施合法合規，避免因違法而面臨法律責任、罰款或聲譽受損。
- ◆ **重要性：**在數位政府及數位經濟的背景下，法律遵循性是組織合法運作及取得公眾信任的基礎。不符合法規要求，可能導致嚴重的行政、民事甚至刑事後果。
- ◆ **重要相關法規：**我國在資通安全領域已逐步建立完善的法規體系，列舉並簡要說明幾項重要的法規：
 - 《資通安全管理法》：作為我國資通安全安管理的基本大法，確立了資通安全防護的原則、架構與機關權責。（修正日期：114 年 9 月 24 日）
 - 《資通安全管理法施行細則》：進一步細化了資通安全管理法的具體實施細節。（修正日期：110 年 8 月 23 日）
 - 《資通安全責任等級分級辦法》：依據機關業務性質與風險，劃定資安責任等級，並規定相關應辦事項。（修正日期：110 年 8 月 23 日）
 - 《個人資料保護法》：規範個人資料的蒐集、處理與利用，旨在保護個人隱私權益。（修正日期：112 年 5 月 31 日）
 - 《國家機密保護法》：旨在保護攸關國家安全的重要機密資訊。（修正日期：112 年 12 月 27 日）
 - **其他業務相關法令法規：**各行各業依其特殊性，也會有特定的資安相關規定，例如《醫療法》涉及病患資訊安全、《兒童及少年福利與權益保障法》涉及兒少個資保護等。

1.3.2 CIA 保護之不同防護技術與方法

要實現上述的 CIA 與法律遵循性目標，需要綜合運用多種技術與管理方法，以應對不同層面的資安挑戰，以下說明如何保護 CIA 資訊的技術與方法：

(1) 機密性保護：

- ◆ **資料加解密**：將資料轉換為密文，只有擁有解密金鑰的授權者才能讀取。
- ◆ **存取控制**：透過身分驗證與授權機制，限制誰可以存取哪些資源。
- ◆ **資料遮罩**：隱藏部分敏感資訊，例如信用卡號碼只顯示後幾碼。
- ◆ **去識別化**：將資料中可以直接或間接識別個人的資訊移除、修改或替換掉，例如：將詳細地址改為縣市或地區。

(2) 完整性保護：

- ◆ **存取控制**：限制非授權者對資料的修改或刪除。
- ◆ **雜湊函數**：透過計算資料的「數位指紋」，驗證資料是否被竄改。
- ◆ **數位簽章**：透過密碼學技術驗證資料的來源與完整性，確保資料在傳輸或儲存過程中未被竄改，用於驗證資料來源的真實性與內容的完整性。
- ◆ **資料驗證**：檢查輸入或處理中的資料是否符合預設的規範與格式
- ◆ **補充說明**：版本控制、稽核追蹤也有助於確保資料的完整性。

(3) 可用性保護：

- ◆ **存取控制**：防止惡意行為阻斷合法使用者對系統的存取。
- ◆ **負載平衡**：設計系統以容忍單點故障，並將流量分散到多個伺服器，提高系統的穩定性與擴展性。
- ◆ **資料備份**：定期複製資料，確保在資料損壞或遺失時能夠復原。
- ◆ **容量規劃**：預先規劃足夠的系統資源，以應對高峰期或突發流量，避免因資源不足導致服務降級或中斷。
- ◆ **系統備援**：建立備用系統或冗餘組件，確保在主系統故障時能迅速切換，維持服務不中斷。
- ◆ **系統監控**：持續監測系統運作狀態、資源使用率，以及潛在的異常情況，以便及早發現及處理問題。
- ◆ **其他措施**：不斷電系統 (UPS)、災難復原計畫等，都是為了提高系統的可用性。



資通安全的防護目標是多面向的，必須從機密性、完整性、可用性及法律遵循性等角度全面考量。唯有綜合運用各種技術及管理策略，針對不同的安全目標及需求，選擇最適合的工具及策略，才能有效地保護資訊資產，確保數位環境的安全與穩定。

MEMO

Handwriting practice area with 20 horizontal dashed lines.

單元

2

資通安全相關法規

在資通安全日益受到重視的今日，完善的法規體系是推動資通安全發展、規範資通安全行為、確保國家安全與社會穩定的關鍵。目前，我國已建立一套以《資通安全管理法》及其子法為核心的法規框架，並輔以其他相關法規，共同構築了全面的資通安全防護法規基礎。

本單元將引導讀者全面了解我國資通安全管理體系的架構及主要參與單位。將深入剖析《資通安全管理法》及其重要的子法規定，並簡要介紹其他與資通安全議題密切相關的法規。透過本單元的學習，將能對我國的資通安全法規有更清晰的認識，為未來的實務運用提供更堅實的法規依據。

本單元學習重點如下：

- 1** 了解我國資通安全管理體系的組織架構與主要角色。
- 2** 深入理解《資通安全管理法》及其相關子法的核心內容。
- 3** 認識其他與資通安全議題相關的重要法規。



2.1

我國資通安全管理體系

我國的資通安全管理體系是一個由多個部會協同合作、層級分明的複雜結構，旨在統籌全國資通安全事務，提升整體防護能力。這個體系最上方是決策層級，向下延伸至規劃、監管及執行層面。

2.1.1 決策與協調層級：行政院國家資通安全會報

位於資安管理體系最頂層的是「行政院國家資通安全會報」。這是國家資安的最高指導與協調單位，負責制定國家資通安全政策的最終決策，確保國家資安戰略的有效推動，如圖 6 我國資通安全組織架構圖所示

- (1) 召集人：由行政院副院長擔任召集人。
- (2) 副召集人：行政院政務委員及指定相關部會首長 1 人。
- (3) 偕同副召集人：由國家安全會議諮詢委員兼任。
- (4) 委員：行政院部會首長、直轄市政府副市長、國安局副局長、學者及專家。

2.1.2 行政院國家資通安全會報組織架構

行政院國家資通安全會報下設有網際防護及網際犯罪偵防等兩大體系，分別負責不同性質的資安挑戰，以應對多元的資安威脅。

(1) 網際防護體系（數位發展部主責）：

- ◆ **說明：**這是負責提升各機關及特定非公務機關資安防護能力的體系，主要由數位發展部負責推動。
- ◆ **下轄組別：**包括關鍵資訊基礎設施安全管理組、產業發展組、資通安全防護組、法規及標準推動組、認知教育及人才培育組、外館網際防護組。
- ◆ **各部會分組：**各部會依其主管業務設有相關分組，包括通訊傳播、衛生福利、金融監督、交通事業、能源及水資源、科技園區、數位政府、資安法規及規範、國家標準、資訊服務、資安教育、競賽及產業交流。

(2) 網路犯罪偵防體系（內政部 / 法務部主責）：

- ◆ **說明：**負責處理網路犯罪的偵查及防制，由內政部及法務部共同主責。



(4) 納管機關：公務機關、特定非公務機關

- ◆ 最底層是被納管的對象，包括各級公務機關及特定的非公務機關，他們負責具體的執行工作。

圖 7 中以金字塔架構呈現了我國資通安全管理體系的架構與權責劃分，從上至下展示了決策、規劃、監管到執行的層層關係。

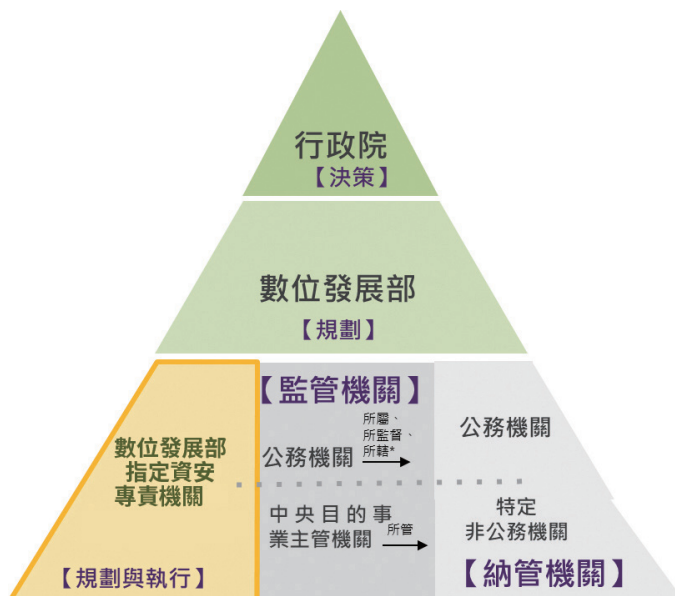


圖 7 我國資通安全管理體系之層級架構圖

- ◆ **【註】所轄公務機關：**在直轄市政府，指直轄市山地原住民區公所及直轄市山地原住民區民代表會；在縣（市）政府，指鄉（鎮、市）公所、鄉（鎮、市）民代表會。

2.1.4 國家資安業務規劃與執行：第七期國家資通安全發展方案

我國在資安業務的規劃與執行上，有明確的政策藍圖與法規基礎。以 114 年~117 年之「第七期國家資通安全發展方案」為例，其涵蓋了政策面、法規面及具體策略，指導著國家資安的整體發展方向。

(1) **願景：**建構韌性安全的數位社會。

(2) **目標：**為了實現上述願景，方案設定了三個主要努力方向：

- ◆ 強化全社會資安防禦韌性。
- ◆ 豐富資安產業生態系。

- ◆ 促進新興科技資安技術的發展與應用。

(3) **推動策略與具體措施**：方案將推動策略分為四個面向，每個面向都有具體的行動指南：

- ◆ **策略一：全社會資安防禦**：旨在提升整個社會的資安防護能力，包括完善國家資安應變機制、提升全民資安職能與意識、建構全民社會資安防護網等。
- ◆ **策略二：提升關鍵基礎設施資安韌性**：聚焦於保護對國家運作至關重要的基礎設施，包括建立關鍵基礎設施資安防護體系、提升關鍵基礎設施防禦能量、精進關鍵基礎設施治理能力等。
- ◆ **策略三：壯大我國資安產業**：強調發展及壯大國內的資安產業，包括推動資安產品檢測制度、強化政府採購供應鏈風險管理、擴大資安產業規模並邁向國際輸出等。
- ◆ **策略四：AI 新興資安科技應用與合作**：著眼於利用新興科技來提升資安能力並加強國際合作，包括拓展 AI 技術應用以提升資安防護能量、強化新興資安科技前瞻研究、促進國際資安交流合作等。

圖 8 呈現了第七期國家資通安全發展方案之規劃與執行的宏觀圖，包括政策、法規、願景、目標與推動策略。



圖 8 第七期國家資通安全發展方案之推動策略與具體措施

我國的資通安全管理體系是一個由上而下、多方協同、動態發展的整體架構。從最高層級的政策制定，到各級機關的具體執行，都依循著明確的法規與規劃，共同為提升國家整體資安防護水平而努力。

2.2

資通安全管理法與子法

《資通安全管理法》(以下簡稱「資安法」)是我國資通安全管理的核心法律，於 107 年 6 月 6 日公布，並於 108 年 1 月 1 日施行，114 年 9 月 24 日再修正。為使資安法能有效落實，相關子法亦將陸續制修定與公布，形成一套完整的資安法規體系。

2.2.1 《資通安全管理法》

資安法制定的主要目的在於「積極推動國家資通安全政策，加速建構國家資通安全環境，以保障國家安全，維護社會公共利益」。

(1) **新增修正內容**：資安法共分為五章，以下先針對新增修正內容進行說明。

◆ 第一章 總則 (§ 1- § 10)：

- 第 3 條：**新增**「受政府控制之事業、團體或機構」定義，以及「危害國家資通安全產品」定義，指經主管機關認定，對國家資通安全具危害風險，影響政府運作或社會安定之資通系統、服務或產品。」
- 第 4 條：**新增**「協助民間處理、因應及防範重大資通安全事件」。
- 第 5 條：**本條新增**，各政府機關、中央及地方應共同推動執行國家資通安全措施，由行政院應定期召開國家資通安全會報，由行政院院長或副院長擔任召集人。

◆ 第二章 公務機關資通安全管理 (§ 11- § 19)：

- 第 11 條：**本條新增**包括 1. 公務機關禁止使用危害國家資安產品。2. 例外情形得專案報核准後使用。
- 第 15 條：**新增**包括 1. 主管機關得定期稽核直轄市政府所轄原住民區公所及民代表會；縣政府所轄鄉鎮市公所及民代表會。
- 第 19 條：**本條新增**包括 1. 適任性進行查核。2. 查核未通過者，不得辦理涉國家機密之資安業務。3. 查核紀錄應保密處理。。

◆ 第三章 特定非公務機關資通安全管理 (§ 20- § 27)：

- 第 20 條：**新增**關鍵基礎設施提供者應設置資通安全專職人員，並訂定

資通安全維護計畫。

- 第 21 條：**新增**關鍵基礎設施以外之機構，應設置資通安全專職人員，並訂定資通安全維護計畫。
- 第 23 條：**本條新增**特定非公務機關應設置資通安全長，負責推動及監督資通安全事務。
- 第 25 條：**本條新增**中央目的事業主管機關調查特定非公務機關資通安全事件之權限、程序及保密義務。
- 第 26 條：**本條新增**特定非公務機關應對辦理資通安全業務績效優良人員予以獎勵。
- 第 27 條：**本條新增**中央目的事業主管機關得限制或禁止下載、安裝或使用危害國家資通安全產品。例外條件、管控機制。

◆ **第四章 罰則 (§ 28- § 31) :**

- 第 28 條：**新增**特定非公務機關所屬人員未依本法規定辦理，情節重大者，由該機關依規定予以懲處。

◆ **第五章 附則 (§ 32- § 35) :**

- 第 33 條：**新增**資通安全事件涉及個人資料外洩時，公務機關及特定非公務機關應另依個人資料保護法及其相關法令規定辦理。

(2) 條文摘要：如表 1。

表 1 《資通安全管理法》條文摘要

章名	條文摘要
第一章 總則	第 1 條 立法目的 1. 制定本法旨在推動國家資安政策。 2. 目標為保障國家安全及維護公共利益。 第 2 條 主管機關 1. 主管機關變更為數位發展部。 2. 數位發展部指定資安專責機關執行業務。 第 3 條 用詞定義 1. 修正資通安全及事件定義 (調整機密性 / 完整性 / 可用性影響文字) 。 2. 關鍵基礎設施及提供者之權責改由行政院管轄。 3. 新增「受政府控制之事業、團體或機構」定義。 4. 新增「危害國家資通安全產品」定義，指經主管機關認定，對國家資通安全具危害風險，影響政府運作或社會安定之資通系統、服務或產品。



章名	條文摘要
第一章 總則	第 4 條 國家資通安全發展 1. 政府應提供資源提升全民資安意識。 2. 新增「協助民間處理、因應及防範重大資安事件」。 3. 發展方案報請行政院核定後實施。 第 5 條 政策推動與協調 1. 行政院應定期召開國家資通安全會報。 2. 會報由行政院院長或副院長擔任召集人。 3. 中央及地方應共同推動資安措施。(本條新增) 第 6 條 情勢公告及備查 1. 主管機關應規劃整體防護等事宜。 2. 每年公布情勢報告、稽核概況報告及發展方案。 3. 報告與方案應送立法院備查。 第 7 條 責任等級分類 1. 機關應報請主管機關核定或備查資安責任等級。 2. 須符合等級要求並辦理管理、技術、認知及訓練等資安防護措施。 第 8 條 稽核管理 1. 主管機關得定期或不定期稽核公務 / 特定非公務機關。 2. 缺失應提改善報告。 3. 稽核年度計畫須報請行政院核定。 第 9 條 資安情資分享 1. 應建立資通安全情資分享機制。 2. 主管機關訂定情資分析、整合與分享等辦法。 第 10 條 委外契約規範 1. 委外應選任適當受託者並監督其資安管理。 2. 受託者須具備完善措施或通過公正第三方驗證。 3. 委外業務應簽訂書面契約。 4. 應配合資安演練，得導入第三方協力機制。
第二章 公務機關 資通安全 管理	第 11 條 禁用管制 1. 公務機關禁止使用危害國家資安產品。 2. 例外專案使用須經資安長核可並報主管機關核定。 3. 相關辦法由主管機關報請行政院核定。(本條新增) 第 12 條 資安長設置 1. 公務機關應置資通安全長 (副首長或適當人員兼任) 。 2. 負責推動及監督機關內資安事務。



章名	條文摘要
第二章 公務機關 資通安全 管理	第 13 條 維護計畫 1. 公務機關須符合責任等級要求。 2. 應訂定、修正及實施資通安全維護計畫。 第 14 條 實施情形提報 1. 公務機關每年向上級 / 監督機關提出資安計畫實施情形。 2. 無上級者，分層向主管機關或地方政府提出。 第 15 條 稽核辦法 1. 公務機關應稽核所屬或監督機關之資安計畫實施情形。 2. 新增：地方政府對轄下區 / 鄉鎮市公所之稽核責任。 第 16 條 改善措施 1. 缺失改善報告須向稽核機關提出，並連同稽核結果送交主管機關。 2. 稽核機關或主管機關得要求說明或調整。 第 17 條 事件通報 1. 應訂定資安事件通報及應變機制。 2. 知悉事件應向受實施情形機關及主管機關通報。 3. 應提出調查、處理及改善報告。 4. 重大事件時，受通報機關得提供協助並公告。 第 18 條 專職人員 1. 應符合等級要求，設置資通安全專職人員。 2. 績效優良者應予獎勵。 3. 遇重大事件，主管機關得調度資安人員支援。 第 19 條 適任性進行查 1. 適任性進行查核。 2. 查核未通過者，不得辦理涉國家機密之資安業務。 3. 查核紀錄應保密處理。(本條新增)
第三章 特定非公 務機關資 通安全管 理	第 20 條 關鍵基礎設施責任 1. 關鍵基礎設施提供者由中央目的事業主管機關指定，報請行政院核定。 2. 新增：資安專職人員。 3. 中央目的事業主管機關應定期稽核。 4. 稽核結果及改善報告送交主管機關。 第 21 條 專職人員及稽核 1. 關鍵基礎設施提供者以外之特定非公務機關，新增：資安專職人員。 2. 中央目的事業主管機關得要求提出實施情形及得稽核。 3. 稽核結果及改善報告送交主管機關。



章名	條文摘要
第三章 特定非公務機關資通安全管理	第 22 條 計畫內容 1. 本條由現行第十六條第六項及第十七條第四項合併修正移列。 2. 授權中央目的事業主管機關擬訂維護計畫、稽核等辦法，報主管機關核定。 第 23 條 資安長設置：特定非公務機關應設置資通安全長，負責推動及監督資通安全事務。(本條新增) 第 24 條 事件通報責任 1. 應訂定資安事件通報及應變機制。 2. 知悉應向中央目的事業主管機關通報。 3. 重大事件報告應送交主管機關。 4. 中央目的事業主管機關或主管機關得提供協助或公告。 第 25 條 事件調查 1. 重大資安事件，得行使調查權。 2. 調查程序包括通知陳述、要求第三方報告或派員檢查。 3. 當事人或關係人不得規避、妨礙或拒絕調查。(本條新增) 第 26 條 優良獎勵：特定非公務機關對於所屬人員辦理資通安全業務績效優良者，應予獎勵。(本條新增) 第 27 條 危害產品管控 1. 中央目的事業主管機關得限制或禁止特定非公務機關使用危害國家資安產品。 2. 例外須經資安長核可，報中央目的事業主管機關核定。(本條新增)
第四章 罰則	第 28 條 懲戒懲處 1. 公務機關人員未依規定辦理者應予懲戒或懲處。 2. 新增：特定非公務機關所屬人員未依本法規定辦理，情節重大者，由該機關依規定予以懲處。 第 29 條 處罰罰鍰：特定非公務機關未通報資安事件，處罰鍰新臺幣三十萬至一千萬元(上限提高)，並令限期改正。 第 30 條 維護及通報違規：特定非公務機關違反資安維護計畫、實施情形提出、改善報告、通報應變機制等規定，處罰鍰新臺幣十萬至五百萬元(上限提高)，並令限期改正。 第 31 條 拒絕調查罰鍰：新增：特定非公務機關違反第二十五條第三項規定，規避、妨礙或拒絕重大資安事件調查者，處罰鍰新臺幣十萬至一百萬元。



章名	條文摘要
第五章 附則	第 32 條 委辦與保密 1. 主管機關得委託機關或法人辦理資安整體防護、演練、稽核等事務。 2. 新增：特定非公務機關業務涉及數個中央目的事業主管機關時，主管機關得協調指定單獨或共同辦理本法所定事項。 第 33 條 個資外洩處理 1. 新增：資通安全事件涉及個人資料外洩時，公務機關及特定非公務機關應另依個人資料保護法及其相關法令規定辦理。 2. 應另依《個人資料保護法》規定辦理。 第 34 條 施行細則：本法之施行細則，由主管機關定之。 第 35 條 施行日期：本法之施行日期，由行政院定之。

(3) 適用對象：資安法明確劃分了兩大類適用對象：

- ◆ **公務機關**：指依法行使公權力之中央、地方機關（構）或公法人。需要注意的是，資安法「不包含軍事機關及情報機關」。
- ◆ **特定非公務機關**：指雖然不是政府部門，但因其重要性或對社會的影響，也被納入資安法規範圍的單位，例如：
 - **關鍵基礎設施提供者**：如台灣中油股份有限公司。
 - **公營事業**：如台灣糖業公司。
 - **特定財團法人**：指符合財團法人法第二條第二項、第三項或第六十三條第一項、第四項規定之財團法人，並屬該法第二條第八項所定全國性財團法人者，如工業技術研究院。
 - **受政府控制之事業、團體或機構**：指銓敘部依公務人員退休資遣撫卹法第七十七條第一項第二款第三目及第四目公告之事業、團體或機構，如臺灣集中保管結算所股份有限公司，具資通安全重要性，經中央目的事業主管機關指定，並經主管機關核定者；其受地方政府控制者，應經地方主管機關同意後，主管機關始得核定。
- ◆ 圖 9 呈現了《資通安全管理法》的適用對象及其法規義務強度，如同時具有關鍵基礎設施提供者及公營事業財團法人身分者，其適用之法規義務，則以關鍵基礎設施提供者適用之法規為先。

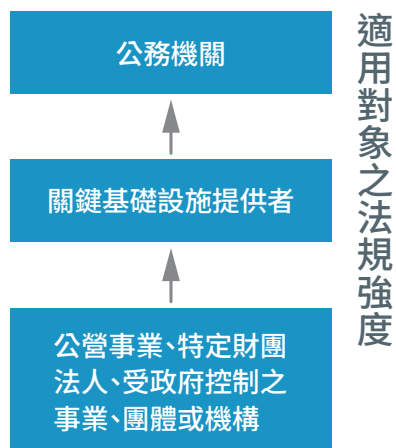


圖 9 《資通安全管理法》適用對象之法規強度

(4) 《資通安全管理法》主要義務：事前、事中、事後

《資通安全管理法》對公務機關及特定非公務機關在資安管理上設定了明確的義務，這些義務貫穿資通安全事件發生前的預防、事件發生時的應變，以及事件發生後的處理與改善。

◆ 事前：

- 均應訂定資通安全維護計畫。
- 均應訂定通報及應變機制。

◆ 事中：

- 均應接受資通安全稽核。
- 均應提出資通安全維護計畫實施情形。
- 當發生資通安全事件時，均應進行通報及應變。

◆ 事後：

- 均應於資通安全稽核後，提出改善報告。
- 於資通安全事件通報後，均應提出調查、處理及改善報告。

圖 10 清楚展示了公務機關及特定非公務機關在資安管理上，事前、事中、事後的主要義務流程。

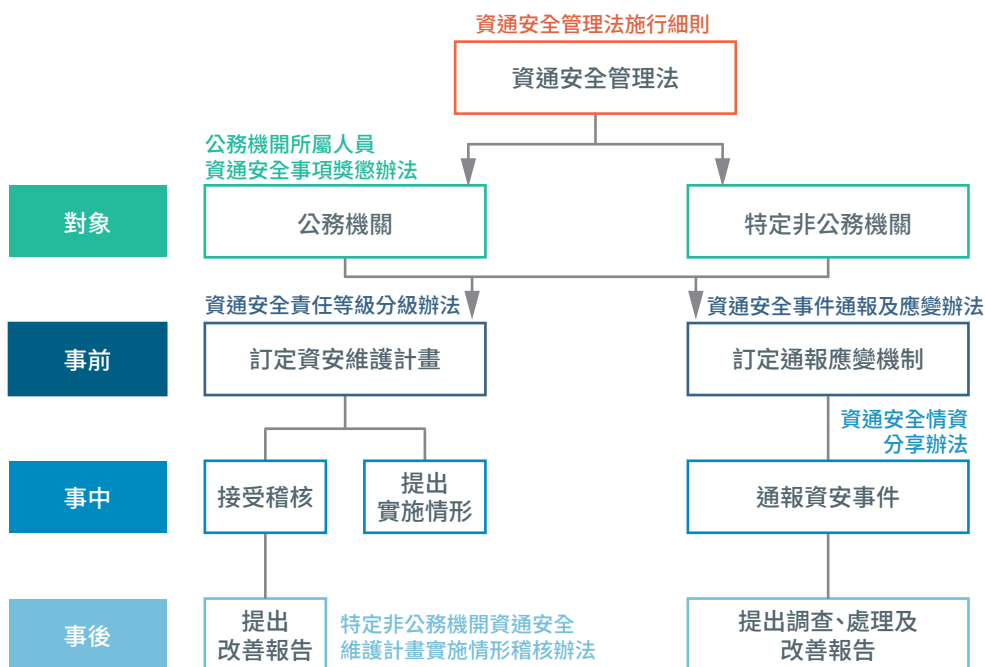


圖 10 《資通安全管理法》適用對象之法規

(5) 《資通安全管理法》子法：落實母法規範

為細化與落實資安法的規定，主管機關（數位發展部）已訂定 6 種子法。這些子法對母法中的原則性規定進行了具體化，提供了操作指南及標準。以下介紹 6 種子法。

2.2.2 《資通安全管理法施行細則》

本細則是依據《資通安全管理法》訂定，主要規範公務機關及特定非公務機關（各機關）如何具體執行資通安全管理事項。

(1) 主要內容：

- ◆ **定義明確：**界定了「軍事機關」與「情報機關」，以及「核心業務」與「核心資通系統」。
- ◆ **改善報告：**要求各機關需針對資通安全維護計畫的稽核結果，提交包括缺失、原因、改正措施及預定完成時程的改善報告。



- ◆ **委外管理**：明確規範委外資通業務時，受託者需具備完善資安措施、專業人員，對涉及國家機密者需進行適任性查核，且客製化系統應提供安全性檢測證明。
- ◆ **維護計畫內容**：規定資通安全維護計畫應包含核心業務、資安政策、組織、人力經費、資通系統盤點、風險評估、防護措施、事件通報應變演練及委外管理等十三項重點。
- ◆ **事件處理**：資通安全事件調查、處理及改善報告須包含影響範圍、損害評估、復原歷程、根因分析及防範措施。
- ◆ **重大事件**：明確「重大資通安全事件」為第三、四級事件，主管機關可公告相關內容，但須排除涉及營業秘密或依法應保密之資訊。

(2) 條文摘要：如表 2。

表 2 《資通安全管理法施行細則》條文摘要

條次	條文摘要
第 1 條	本細則依《資通安全管理法》第 22 條規定訂定。
第 2 條	– 軍事機關：國防部及所屬機關（構）、部隊、學校。 – 情報機關：依《國家情報工作法》第 3 條規定之機關。
第 3 條	各機關提出改善報告應包含： – 失或待改善項目及內容。 – 發生原因。 – 改善措施（管理、技術、人力、資源）。 – 成時程及進度追蹤方式。
第 4 條	委外辦理資通業務應注意事項： – 完善資通安全管理措施或通過第三方驗證。 – 配備資通安全專業人員。 – 是否可複委託及相關要求。 – 涉及國家機密者進行適任性查核。 – 核心系統或金額達一千萬元者需安全性檢測。 – 違法或事件發生需立即補救並通報。 – 契約終止時確保資料返還、刪除或銷毀。



條次	條文摘要
第 4 條	- 其他必要的資通安全措施。 - 委託機關定期稽核受託業務執行狀況。
第 5 條	書面文件 依《電子簽章法》規定，可用電子文件提交。
第 6 條	資通安全維護計畫 應包含： - 核心業務及其重要性。 - 資通安全政策及目標。 - 資通安全推動組織。 - 人力與經費配置。 - 公務機關配置資通安全長。 - 資通系統與資訊盤點，標示核心系統。 - 資通安全風險評估。 - 資通安全防護與控制措施。 - 資通安全事件通報、應變及演練機制。 - 資通安全情資評估與因應機制。 - 委外管理措施。 - 資通安全考核機制。 - 計畫精進及績效管理機制。
第 7 條	核心業務範圍： - 公務機關核心權責業務。 - 公營事業及政府捐助財團法人主要服務或功能。 - 運關鍵基礎設施所需業務。 - 及資通安全責任分級相關業務。 核心資通系統： 支援核心業務必要的系統或防護需求等級為高者。
第 8 條	資通安全事件 調查、處理及改善報告 應包含： - 事件發生或損害控制完成時間。 - 事件影響範圍及損害評估。 - 損害控制與復原歷程。 - 事件調查與處理歷程。 - 根因分析。 - 防範類似事件措施。 - 完成時程及追蹤機制。
第 9 條	指定 關鍵基礎設施提供者 前，應給予陳述意見的機會。



條次	條文摘要
第 10 條	重大資通安全事件 ：依《資通安全事件通報及應變辦法》第三級或第四級事件。
第 11 條	- 公佈重大資通安全事件時，應載明：發生時間、原因、影響程度、控制情形及改善措施。 - 涉及營業秘密或應保密內容時，可限制或部分公告。
第 12 條	特定非公務機關業務涉及多個中央主管機關時，可協調指定一個或多個主管機關共同辦理。
第 13 條	施行日期 ：由主管機關定之；修正條文自發布日起施行。

(3) 本細則進一步解釋及落實了母法的相關規定。例如，定義了細則第 7 條第 1 項「核心業務範圍」及第 7 條第 2 項「核心資通系統」，這對於後續的責任等級分級及維護計畫至關重要。

◆ **核心業務範圍定義**：涵蓋了不同類型機關的主要職責、功能，以及涉及較高資安責任等級的業務。其範圍如下：

- 公務機關依其組織法，足認該業務為機關核心職責所在。
- 公營事業及政府捐助之財團法人之主要服務或功能。
- 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 4 條第 1 款至第 5 款涉及之業務：
 - 一、業務涉及國家機密。
 - 二、業務涉及外交、國防或國土安全事項。
 - 三、業務涉及全國性民眾服務或跨公務機關共用之資通系統之維運。
 - 四、業務涉及全國性民眾或公務人員個人資料保護，且業務涉及全國性關鍵基礎設施
 - 五、屬中央級關鍵基礎設施。
 - 第 5 條第 1 款至第 5 款涉及之業務：
 - 一、業務涉及國家核心科技資訊之持有。
 - 二、業務涉及協助或研發前款之國家核心科技資訊之管理。

三、業務涉及區域性民眾服務或跨公務機關共用之資通系統之維運。

四、業務涉及區域性民眾或公務人員個人資料保護，且業務規模屬第三款所定等級

五、屬中央二級機關及其所屬各級機關（構）共用之資通系統之維運。

- ◆ **核心資通系統定義：**核心資通系統是指那些對於核心業務的持續運作至關重要的系統，或者是依據防護需求分級原則被判定為高風險的系統。

(4) 本細則亦說明了軍事機關、情報機關的排除適用，以及關鍵名詞的明確定義。同時規範了中央目的事業主管機關的指定、資通安全稽核、資通安全事件之通報及應變、資通系統服務委外辦理注意事項、資通安全維護計畫應備內容等。

(5) 本細則明訂通安全維護計畫應包含的內容：

- ◆ 依據《資通安全管理法施行細則》第 6 條，資通安全維護計畫應包含 13 個項目，涵蓋資安管理的各個面向，從核心業務的識別到持續的改進，確保資安維護計畫是全面且有效的。這些項目包括：
 - 核心業務及其重要性
 - 資通安全政策及目標
 - 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
 - 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

2.2.3 《資通安全責任等級分級辦法》

本辦法依據《資通安全管理法》訂定，旨在對公務機關及特定非公務機關的資通安全責任進行分級管理，以提升國家資通安全能力。資通安全責任等級

分為 A 級（最高）、B 級、C 級、D 級及 E 級（最低），並依據涉及的業務性質及影響程度進行判定。

(1) 主要內容：

- ◆ **等級劃分：**主要考量業務性質，如是否涉及國家機密、外交國防、全國性民眾服務、關鍵基礎設施維運、持有個人資料或屬於醫院等，以及資通系統失效對社會公共利益的影響程度。若機關符合多個等級，則歸列為其中之最高等級。
- ◆ **對應要求：**各機關必須依據其核定的責任等級，執行附表所規範的管理、技術、認知與訓練等資通安全維護事項。
- ◆ **系統分級：**資通系統本身亦依其機密性、完整性、可用性及法律遵循性等防護需求，分為高級、中級及普級，並須實施相應的防護基準控制措施。

本辦法確保不同風險程度的機關與資通系統，能有符合其重要性且具體的資安管理要求

(2) 條文摘要：如表 3。

表 3 《資通安全責任等級分級辦法》條文摘要

條次	條文摘要
第 1 條	本辦法依《資通安全管理法》第 7 條第 1 項規定訂定。
第 2 條	將各機關資通安全 責任等級 分為 A、B、C、D、E 五級。
第 3 條	機關責任等級 之核定、提交、備查、變更
第 4 條	屬 A 級 資通安全責任等級之情形，如備註。
第 5 條	屬 B 級 資通安全責任等級之情形，如備註。
第 6 條	屬 C 級 資通安全責任等級之情形，如備註。
第 7 條	屬 D 級 資通安全責任等級之情形，如備註。
第 8 條	屬 E 級 資通安全責任等級之情形，如備註。
第 9 條	若機關符合多個責任等級，應列為最高等級。



條次	條文摘要
第 10 條	資通安全 責任等級 可依國家安全或其他影響考量進行 調整 ，包含個資、公務機密等事項。
第 11 條	- 附表一至附表八：資通安全責任等級應辦理事項；附表九：資通系統防護需求分級原則 - 普、中、高；附表十：資通系統防護基準執行控制措施。 - 特定非公務機關主管機關得另訂防護基準。 - 有困難免執行某事項或控制措施，需報請核准。 - A/B 級機關應依主管機關指定方式，提報辦理情形。
第 12 條	施行日期 ：由主管機關定之，修正條文自發布日起施行。

備註：

- 各機關有下列情形之一者，其資通安全責任等級為 A 級：
 - 一、業務涉及國家機密。
 - 二、業務涉及外交、國防或國土安全事項。
 - 三、業務涉及全國性民眾服務或跨公務機關共用性資通系統之維運。
 - 四、業務涉及全國性民眾或公務員個人資料檔案之持有。
 - 五、屬公務機關，且業務涉及全國性之關鍵基礎設施事項。
 - 六、屬關鍵基礎設施提供者，且業務經中央目的事業主管機關考量其提供或維運關鍵基礎設施服務之用戶數、市場占有率、區域、可替代性，認其資通系統失效或受影響，對社會公共利益、民心士氣或民眾生命、身體、財產安全將產生災難性或非常嚴重之影響。
 - 七、屬公立醫學中心。
- 各機關有下列情形之一者，其資通安全責任等級為 B 級：
 - 一、業務涉及公務機關捐助、資助或研發之國家核心科技資訊之安全維護及管理。
 - 二、業務涉及區域性、地區性民眾服務或跨公務機關共用性資通系統之維運。
 - 三、業務涉及區域性或地區性民眾個人資料檔案之持有。
 - 四、業務涉及中央二級機關及所屬各級機關（構）共用性資通系統之維運。
 - 五、屬公務機關，且業務涉及區域性或地區性之關鍵基礎設施事項。
 - 六、屬關鍵基礎設施提供者，且業務經中央目的事業主管機關考量其提供或



維運關鍵基礎設施服務之用戶數、市場占有率、區域、可替代性，認其資通系統失效或受影響，對社會公共利益、民心士氣或民眾生命、身體、財產安全將產生嚴重影響。

七、屬公立區域醫院或地區醫院。

- 各機關維運自行或委外設置、開發之資通系統者，其資通安全責任等級為 C 級。前項所定自行或委外設置之資通系統，指具權限區分及管理功能之資通系統。
 - 各機關自行辦理資通業務，未維運自行或委外設置、開發之資通系統者，其資通安全責任等級為 D 級。
- (3) 各機關需每兩年核定或提交其資通安全責任等級，並報主管機關核定。
- (4) 本辦法可依機關業務的重要性及其對國家安全、社會公共利益的影響程度進行靈活調整，並要求各機關依其等級執行相關防護措施，確保運作安全及穩定。

2.2.4 《特定非公務機關資通安全維護計畫實施情形稽核辦法》

本辦法依《資通安全管理法》訂定，規範主管機關如何對特定非公務機關（受稽核機關）進行資通安全維護計畫的稽核作業。主管機關每年依據機關業務重要性、資通系統特性及過往稽核情況等因素，擇定稽核對象，並制定稽核計畫。稽核過程包括書面通知、現場稽核、訪談及文件查閱等，若受稽核機關無法配合，需書面說明理由並接受審核。

(1) 主要內容：

◆ 主管機關：

- 擬定稽核計畫
- 成立稽核小組
- 通知受稽機關（於稽核 1 個月前）
- 進行稽核（包含稽核前訪談、實地稽核）
- 交付稽核報告（完成後 1 個月內）

◆ 特定非公務機關：

- 接到通知：如有正當理由可以調整。
- 配合稽核作業。
- 提交改善報告（交付稽核報告後 1 個月內）。

- ◆ 中央目的事業主管機關：視主管機關要求，派員為必要之協助。

(2) 條文摘要：如表 4。

表 4 《特定非公務機關資通安全維護計畫實施情形稽核辦法》條文摘要

條次	條文摘要
第 1 條	本辦法依據《資通安全管理法》第 7 條第 2 項訂定。
第 2 條	所有書面文件可依《電子簽章法》規定，以電子文件形式處理。
第 3 條	- 主管機關每年擇定特定非公務機關（受稽核機關），以現場實地稽核方式執行稽核。 - 擇定受稽核機關時考量因素包括：業務重要性、系統規模、事件頻率、演練成果、歷史稽核結果等。 - 稽核計畫內容須包含：依據、目的、期間、重點領域、稽核方式等細節。
第 4 條	- 稽核計畫應於 1 個月前書面通知受稽核機關。 - 受稽核機關可在接到通知 5 日內申請調整稽核日期，但限 1 次。
第 5 條	- 稽核過程中，主管機關得要求說明、協力或提供文件並執行訪談及現場實地稽核。 - 正當理由無法配合稽核者，需提交書面申請並由主管機關審核。 - 若理由成立，停止稽核部分或全部；若不成立，繼續稽核並提前 10 日通知。
第 6 條	- 稽核小組由 3 人以上組成，應邀具政策、技術、管理或法律專業者參與，且公務機關代表不少於四分之一。 - 小組成員須遵守利益衝突迴避及保密義務，符合特定情形者需主動迴避。
第 7 條	- 每季稽核結果應於稽核作業完成後 1 個月內交付受稽核機關。 - 稽核報告內容包含範圍、缺失或改善事項、未配合原因及審核結果等要素。
第 8 條	- 發現缺失者，受稽核機關須於 1 個月內提出改善報告，並送交中央目的事業主管機關，可被要求補充說明或調整。 - 後續執行情形需依主管機關指定方式及時間提出。





條次	條文摘要
第 9 條	稽核過程中，主管機關可要求中央目的事業主管機關派員協助。
第 10 條	- 施行日期：由主管機關決定。 - 修正條文：自發布日施行。

- (3) 稽核小組由具專業知識的成員組成，且必須遵守利益衝突迴避及保密義務。稽核結束後，主管機關需於一個月內提交結果報告，若發現缺失，受稽核機關需於限期內提交改善報告並執行改善措施。
- (4) 稽核流程包括：主管機關擬定稽核計畫 -> 成立稽核小組 -> 通知受稽機關（於稽核 1 個月前） -> 進行稽核（包含稽核前訪談、實地稽核） -> 交付稽核報告（完成後 1 個月內） -> 提交改善報告（交付稽核報告後 1 個月內）。中央目的事業主管機關在過程中會提供必要協助。

2.2.5 《資通安全事件通報及應變辦法》

本辦法依《資通安全管理法》相關條文訂定，旨在規範公務機關及特定非公務機關對資通安全事件的通報與應變機制，以降低風險並保障資訊安全。規定了資安事件發生時，公務機關及特定非公務機關如何進行通報及應變，以及相關的時限、支援協助及演練要求。

(1) 主要內容：

- ◆ **資安事件劃分：**共有四個等級，並針對不同等級規定了不同的通報時限與處理要求。
 - 第一級：輕微影響，例如非核心業務資訊洩漏或受輕微竄改。
 - 第二級：較大影響，如非核心業務無法於容忍時間內回復或核心業務輕微洩漏。
 - 第三級：涉及核心業務的重大洩漏或竄改，如一般公務機密洩漏。
 - 第四級：最嚴重的情況，例如國家機密洩漏或關鍵基礎設施停擺。
- ◆ **事件通報規範：**公務機關與特定非公務機關在知悉資通安全事件後，需於 1 小時內通報，若等級變更需即時續行通報。若因故無法通報，需記錄原因並事後補行。

◆ 事件應變時限：

- 針對不同等級事件，規定完成損害控制與復原的時限：第一級、第二級：72 小時內完成。第三級、第四級：36 小時內完成。
- 事件處理完畢後，需於 1 個月內提交調查、處理及改善報告。

◆ 主管機關責任：

- 主管機關需於特定時間內審核事件等級，並可依實際情形進行覆核與變更等級：第一級、第二級：8 小時內審核。第三級、第四級：2 小時內審核。
- 需視情況為所屬機關或單位提供技術支援與協助。

◆ 安全演練

- 公務機關與特定非公務機關需定期進行資通安全演練，包括：
每半年 1 次的社交工程演練。
每年 1 次的通報與應變演練、網路攻防演練及情境演練。

◆ 內部作業規範

- 各機關需訂定資通安全事件的通報與應變規範，應包括事件等級判定流程、損害控制機制、內外部通報流程及相關演練機制。

◆ 協調與改善

- 主管機關可對第三級、第四級重大事件召開協商會議，邀請相關機關研商與協助損害控制及復原措施。
- 各機關如已有完善機制且運行一年以上，經核定後可沿用既有機制。

◆ 施行與修正

- 本辦法的施行與修正條文由主管機關公告與推動。

(2) 條文摘要：如表 5。

表 5 《資通安全事件通報及應變辦法》條文摘要

條次	條文摘要
第 1 條	本辦法依據《資通安全管理法》第 14 條第 4 項及第 18 條第 4 項訂定。
第 2 條	資通安全事件分為四級，依影響程度與範圍進行劃分，範例如非核心業務輕微洩漏（第一級）至國家機密洩漏（第四級）。





條次	條文摘要
第 3 條	資通安全事件 通報內容 應包括：發生機關、時間、狀況描述、等級評估、應對措施、外部支援需求及其他事項。
第 4 條	公務機關 知悉資通安全事件 後，應於 1 小時內通報，若等級變更應續行通報；若無法通報，需記錄原因並事後補行通報。
第 5 條	主管機關需於通報後特定時間內完成 事件等級審核 ：第一級、第二級 (8 小時內)，第三、四級 (2 小時內)。
第 6 條	公務機關應於特定時間內完成 損害控制或復原 ：第一級、第二級 (72 小時內)，第三級、第四級 (36 小時內)。並於 1 個月內 提交調查報告 。
第 7 條	- 相關中央及地方政府機關應視情形提供所屬公務機關支援。 第三級、第四級事件需召開會議研商並請求協助。
第 8 條	- 公務機關需每半年辦理社交工程演練。 - 每年辦理資通安全事件通報及應變演練。 - 完成後 1 個月內提交成果報告。
第 9 條	公務機關應訂定資通安全事件 通報規範 ，包括事件等級判定流程、內部通報流程及對外通知方式等內容。
第 10 條	公務機關應訂定 應變作業規範 ，包括應變小組組織、損害控制機制、事件發生後之復原及調查機制等內容。
第 11 條	特定非公務機關需於 知悉 資通安全事件 1 小時內通報，情況變更時應續行通報，若無法通報需事後補行並記錄原因。
第 12 條	中央目的事業主管機關需於通報後完成事件 等級審核 ：第一級、第二級 (8 小時內)，第三級、第四級 (2 小時內)，並依要求 提交結果 。
第 13 條	特定非公務機關需於特定時間內完成 損害控制或復原 ：第一級、第二級 (72 小時內)，第三級、第四級 (36 小時內)。並 提交調查報告 。
第 14 條	- 中央目的事業主管機關及主管機關應視情形提供特定非公務機關必要支援或協助。 - 第三級、第四級事件需召開會議研商。



條次	條文摘要
第 15 條	特定非公務機關應訂定資通安全事件 通報規範 ，內容包括等級判定流程、內部通報流程、對外通知方式及演練等。
第 16 條	特定非公務機關應訂定 應變作業規範 ，內容包括應變小組組織、損害控制機制、復原及調查機制、事件紀錄保全等。
第 17 條	主管機關可對第三級、第四級事件 召開會議 ，邀請相關機關共同研商損害控制及復原事宜。
第 18 條	公務機關需配合主管機關辦理資通安全演練，包括 社交工程演練 、 通報應變演練 、 網路攻防演練及情境演練 。
第 19 條	特定非公務機關需配合主管機關辦理 資通安全演練 ，如有影響其權利或利益的情況，需事先取得書面同意。
第 20 條	公務機關或特定非公務機關如已有資通安全應變機制，經主管機關核定後可繼續採用， 機制變更 時需重新核定。
第 21 條	– 施行日期：由主管機關定之。 – 修正條文：自發布日起施行。

2.2.6 《資通安全情資分享辦法》

本辦法旨在規範公務機關及特定非公務機關間的資通安全情資分享機制，規定了資安情資分享的內容、對象、方式、限制，以及如何透過情資的分析與應用，以提升整體的資安防護能力，並鼓勵各機關之間分享資安情資，以建立聯防機制，共同應對資安威脅。

(1) 主要內容：

- ◆ **情資內容**：明確定義情資範圍，包括惡意偵察、安全漏洞、攻擊方法、惡意程式、事件損害與防範措施等技術性資訊。
- ◆ **分享原則**：各機關應適時與主管機關或中央目的事業主管機關分享情資，並須辨識其來源可靠性與時效性，進行威脅與弱點分析，且採取對應的預防或應變措施。

- ◆ **分享限制與保護**：情資若涉及營業秘密或依法應秘密者不得分享；分享時需規劃適當的**安全維護措施**，避免個人資料或保密資訊外洩或竄改。
- ◆ **國際合作**：主管機關應就情資分享事宜進行國際合作。

(2) 條文摘要：如表 6。

表 6 《資通安全情資分享辦法》條文摘要

條次	條文摘要
第 1 條	本辦法之訂定依據為《資通安全管理法》第 8 條第 2 項。
第 2 條	定義「 資通安全情資 」（情資）的七項內容，包括惡意偵察、安全漏洞、安全控制措施失效方法、惡意程式、事件損害、偵測預防措施及相關技術性資訊。
第 3 條	規定情資分享的對象與原則 ：主管機關應進行國際合作，並與公務機關適時分享情資；中央目的事業主管機關與特定非公務機關間亦應適時分享。已公開或已分享者不在此限。
第 4 條	規定情資不得分享的兩種情形 ：涉及營業秘密或侵害公務機關、個人、法人或團體權益，除非有特例（公益、生命健康、當事人同意）；以及依法規應秘密或限制公開者。但允許部分分享。
第 5 條	各機關進行 情資分享 時，應 分析整合情資 ，並 規劃適當安全維護措施 ，避免情資內容、個人資料或不得分享資訊外洩，或遭未經授權存取或竄改。
第 6 條	各機關 收到情資後 ，應辨識來源可靠性及時效性，分析威脅與弱點，研判潛在風險，並採取對應的預防或應變措施。
第 7 條	各機關 整合情資時 ，得依來源、日期、期間、類別、威脅指標等項目進行關聯分析，並應分享整合後發現之新型威脅情資。
第 8 條	各機關 接收情資後 ，應採取適當的安全維護措施，以避免情資內容、個人資料或不得分享資訊外洩，或遭未經授權存取或竄改。
第 9 條	情資分享應依主管機關指定方式進行。若無法按 指定方式分享 ，經同意後可採書面、傳真、電子郵件、資訊系統或其他適當方式。



條次	條文摘要
第 10 條	未適用本法之個人、法人或團體，經主管機關同意後，得與其進行情資分享，但需以書面約定遵守本辦法第四條至第九條之規定。
第 11 條	施行日期：由主管機關決定。

2.2.7 《公務機關所屬人員安全事項獎懲辦法》

本辦法是依據《資通安全管理法》訂定，旨在規範公務機關所屬人員在資通安全方面的獎勵與懲處，以提升國家資通安全韌性。

(1) 主要內容：

- ◆ **機關自主訂定基準：**各公務機關可以依據本辦法的規定，自行訂定其所屬人員在資通安全事項上的獎懲基準。
- ◆ **獎勵情形：**明列了多種值得獎勵的資通安全相關行為，包含但不限於：
 - 有效實施資通安全維護計畫。
 - 績效優良的稽核與演練。
 - 成功預防資通安全事件或降低損害。
 - 及時發現並應變重大資通安全事件。
 - 提出具體建議或革新方案。
 - 對資通安全人才培育、科技研發、政策法制研析及國際合作等有貢獻。
- ◆ **懲處情形：**明確指出需懲處的重大違規行為，包括：
 - 未依規定辦理資通安全情資分享、資通安全維護計畫的訂定與實施、稽核、改善報告、通報應變機制以及事件通報與應變等重要事項，且情節重大者。
 - 資通安全業務績效不良且經疏導無效，情節重大者。
 - 其他違反相關法規或內部規範且情節重大者。
 - 對業務督導不力導致屬員或所屬機關發生上述情事者。
- ◆ **考核與申辯權利：**
 - 公務機關在進行平時考核時，應綜合考量獎懲情況、事件發生原因、過程、動機、目的、手段、表現及影響等因素。



- 對於聘用、約僱或其他有僱傭關係的人員，其獎懲情形應納入續聘參考。
- 在懲處前，應給予當事人申辯機會，並可視需要徵詢資通安全專家學者意見。

◆ **施行日期：**本辦法修正條文自發布日施行。

(2) **條文摘要：**如表 7。

表 7 《公務機關所屬人員安全事項獎懲辦法》條文摘要

條次	條文摘要
第 1 條	本辦法依據《資通安全管理法》第 15 條第 2 項及第 19 條第 2 項規定訂定。
第 2 條	公務機關可依本辦法， 自行訂定 其所屬人員辦理資通安全業務涉及獎懲的 具體基準 。
第 3 條	列出 12 項應予「獎勵」的情形，主要包括： – 符合本法或授權法規，訂定、修正及實施資通安全維護計畫，績效優良。 – 稽核所屬或監督機關之資通安全維護計畫實施情形，或進行資通安全演練，績效優良。 – 配合主管機關或上級機關辦理資通安全維護計畫的稽核或演練，經評定績效優良。 – 辦理資通安全業務切合機宜，防止資通安全事件發生，避免損害。 – 主動發現新型態資通安全弱點或威脅，並分享情資，防止事件發生或降低損害。 – 積極查察維護異狀，即時發現重大事件並通報及應變，防止損害擴大。 – 提出具體建議或革新方案並經採行，對資通安全業務有貢獻。 – 辦理資通安全人才培育事務，有具體貢獻。 – 辦理資通安全科技之研發、整合、應用或產業發展事務，有具體貢獻。 – 辦理資通安全軟硬體技術規範及相關服務發展，有具體貢獻。 – 辦理資通安全政策、法制研析或國際合作事務，有具體貢獻。 – 辦理其他資通安全業務有具體功績



條次	條文摘要
第 4 條	列出 3 項應予「懲處」的情形，主要包括： - 情節重大未依規定辦理資安相關事項：包括情資分享、資安維護計畫的訂定與實施、稽核、改善報告、事件通報應變、調查處理等。 - 辦理資安業務績效不良，經疏導仍無效且情節重大。 - 其他違反《資通安全管理法》、相關法規或機關內部規範且情節重大的行為。
第 5 條	公務機關在對所屬人員進行平時考核時，應審酌獎懲情形，並綜合考量事件的原因、經過、行為動機、目的、手段、表現及影響等因素；對於聘用、約僱或其他僱傭關係人員，其獎懲結果應納入續聘考量。
第 6 條	公務機關在對所屬人員作出第四條所列的懲處前，應給予當事人申辯的機會；必要時，得就所涉及的資通安全專業事項，徵詢相關專家學者的意見。
第 7 條	施行日期：由主管機關另行決定。

2.3

其他相關法規

除了《資通安全管理法》及其子法外，我國還有其他與資通安全議題密切相關的法律。其中，《國家機密保護法》及《個人資料保護法》是兩個非常重要的法規，從不同角度強化了資訊的安全性。

2.3.1 《國家機密保護法》

《國家機密保護法》於 2003 年 2 月 6 日公布，並於 112 年 12 月 27 日修正。這部法律的核心目的在於「為確保國家安全或利益，對政府機關持有或保管之資訊，經依法核定機密等級者」提供嚴格的保密保護。

(1) 國家機密之定義與範圍：

- ◆ **定義：**指為確保國家安全或利益而有保密之必要，且經政府機關依本法核定機密等級的資訊。
- ◆ **範圍：**涵蓋多個重要領域，包括但不限於：
 - 軍事計畫、武器系統或軍事行動。
 - 外國政府之國防、政治或經濟資訊。
 - 情報組織與其活動。
 - 政府通信、資訊之保密技術、設備或設施。
 - 外交或大陸事務。
 - 科技或經濟事務。
 - 其他為確保國家安全或利益而有保密之必要者。
- ◆ 這些範圍內的資訊，一旦被核定為國家機密，就必須受到最嚴格的保護，以防範洩露對國家造成損害。

(2) 國家機密等級區分與保密期限：

- ◆ **國家機密**依照其敏感程度及洩漏後可能造成的損害程度，區分為三個等級：
 - **絕對機密：**最為敏感，保密期限不得逾 30 年。
 - **極機密：**高度敏感，保密期限不得逾 20 年。

- **機密**：一般敏感，保密期限不得逾 10 年。

- ◆ **核定原則**：應在必要之「最小範圍內」為之，且有核定權責人員應於接獲報請後 30 日內完成核定，並應併予核定其保密期限或解除機密之條件。

- ◆ **取消永久保密期限之檔案**：112 年本法修正後，原依本法核定永久保密之國家機密，應於第 12 條修正施行之日起 2 年內，依本法重新核定，其保密期限溯自原先核定之日起算；屆滿 2 年尚未重新核定者，自屆滿之日起，視為解除機密。

- ◆ **等級變更**：國家機密變更機密等級者，其保密期限仍自原核定日起算。

《國家機密保護法》對於保護攸關國家安全及利益的敏感資訊至關重要。所有公務人員都應該了解其相關規定，務必遵守相關規定，避免洩漏國家機密，以維護國家安全與利益。

2.3.2 《個人資料保護法》

《個人資料保護法》於 99 年 5 月 26 日公布，並於 101 年 10 月 1 日施行，112 年 5 月 31 日修正。這部法律的主要目的在於「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」。

(1) **立法目的**：旨在保障個人的隱私權益，同時兼顧個人資料在合理範圍內的流通與利用。

(2) **個人資料的定義**：《個人資料保護法》所稱的「個人資料」限定於「自然人」的資料，且能直接或間接識別該個人者，包括：

- ◆ **屬性資料**：例如姓名、生日、身分證字號等。

- ◆ **行為資料**：例如健康檢查報告、犯罪前科等。

- ◆ **其他可識別資料**：只要能直接或間接識別特定個人的資訊，例如聯絡方式、地址、病歷、消費紀錄等，都屬於個人資料的範疇。

- ◆ **規範行為**：《個人資料保護法》對個人資料的蒐集、處理與利用有嚴格的規範，確保個人資料的合法合規處理：

- **自主權利不可拋棄**：當事人（資料主體）的個人資料自主權利不得預先拋棄。

- **特定目的原則**：個人資料的蒐集、處理或利用必須有「特定目的」。

- **告知義務**：在蒐集個人資料時，必須明確告知當事人蒐集之目的、個

人資料類別、其使用範圍及資料來源。

- 刪除義務：應保持個人資料的正確性，並於蒐集目的消失後刪除。

《個人資料保護法》強調個人資料的保護，其為個人資料的生命週期（蒐集、處理、利用）設定了明確的法律界限，以防範個人權益受損。所有處理個人資料的單位及人員，都必須嚴格遵守《個人資料保護法》的規定。

2.3.3 《資通安全管理法》與《個人資料保護法》之比較

《資通安全管理法》與《個人資料保護法》雖然都與資訊安全相關，但兩者在主管機關、立法目的、適用對象及主要重點上存在顯著差異。了解這些差異，有助於我們更精確地掌握兩部法律的適用情境與側重點。如表 8《資通安全管理法》與《個人資料保護法》比較。

表 8 《資通安全管理法》與《個人資料保護法》比較

項目	資通安全管理法	個人資料保護法
主管機關	數位發展部	個人資料保護委員會
立法目的	為積極推動國家資通安全政策，加速建構國家資通安全環境，以保障國家安全，維護社會公共利益	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
適用對象	公務機關及特定非公務機關	於任何「公務機關」與「非公務機關」（公務機關以外之自然人、法人或其他團體）。因此，無論是公司、獨資、合夥、自然人、負責人等為個人資料保護法規範之對象
主要重點	著重納管機關之資安管理作業，並降低資安風險	著重個人資料的保護，限制個資外洩與不當使用

(3) **主管機關**：《資通安全管理法》的主管機關是數位發展部，而《個資法》的主管機關則是個人資料保護委員會。

(4) **立法目的**：《資通安全管理法》著重於國家層級的資通安全防護，強調組

織的整體資安韌性；個資法則側重於個人權益保護，規範個人資料的處理行為。

(5) **適用對象：**《資通安全管理法》主要規範公務機關及特定非公務機關（組織層面）；**個資法**則適用於所有蒐集、處理或利用個人資料的單位（無論公私部門，從公司到個人）。

(6) **主要重點：**《資通安全管理法》聚焦於納管機關的資安管理作業，降低資安風險；《個人資料保護法》主要關注個人資料的保護，限制個資外洩與不當使用。

- ◆ 總體而言，《資通安全管理法》是從組織層面出發，提升整體的資安防護能力；而《個人資料保護法》則是從個人權益出發，規範個人資料的處理行為。雖然目標不同，但在實務上兩者經常會相互影響。例如，良好的資通安全管理可以有效降低個資外洩的風險，自然也符合個資保護的要求。

本單元全面介紹了我國資通安全的法律框架，從體系架構到核心法規，再到其他相關法律。理解這些法律是資通安全專業人員及任何組織成員的基礎。在下一章中，將探討資通安全管理的核心環節 - 風險管理。

MEMO

單元

3

資通安全風險管理



在資通安全領域，僅有完善的防護措施仍不足以應對不斷變化的威脅。資通安全風險管理是一套系統化的流程，旨在協助組織識別、評估、處理及監控資通安全風險，以確保資訊資產在可接受的風險水平下運行，進而達成資通安全目標。

本單元將引導讀者了解風險管理的整體流程，從建立全景、進行風險評鑑，到選擇適當的風險處理策略（包括風險修改、留存、避免及分擔），並明確風險接受的考量因素。此外，我們也將介紹國際上廣泛採用的資通安全防護框架與風險管理標準，為讀者提供實務操作的參考依據。

本單元旨在幫助讀者建立資通安全領域的基礎背景，使其具備職務上所需要的資安知識與技能，同時為其他的資安相關教育訓練課程建立先備知識。課程內容以實用性為主軸，配合資通安全在策略面、管理面及技術面，全面性涵蓋資通安全之相關領域，並配合淺顯易懂的介紹或實例說明，避免太理論與深入複雜的學理研究。

本單元學習重點如下：

- 1** 了解資通安全風險管理的整體流程，包括其核心步驟與循環特性。
- 2** 掌握風險管理全景建立的重要性，包括內外部環境的識別與風險準則的設定。
- 3** 學習風險評鑑的作法，包括高階與詳細評鑑的選擇與執行。
- 4** 理解風險處理的各項策略，包括風險修改、留存、避免及分擔。
- 5** 明確風險接受的考量因素，以及殘餘風險的管理。
- 6** 認識國際上重要的資通安全防護與管理標準，如 NIST CSF 及 CNS 27005：2024。



3.1

風險管理之流程

資通安全風險管理是一個持續性的循環過程，其核心目標是在有限的防護成本投入下，獲得最佳化的安全性，而非追求絕對的零風險。這表示資安管理需要權衡成本與效益，找出最適合組織需求的防護水準。

3.1.1 「風險」的產生

在資安領域中，「風險」的產生源於三個關鍵要素之間的交互作用：

- (1) **威脅 (Threat)**：指可能對組織資產造成損害的潛在原因或事件。
- (2) **脆弱性 (Vulnerability)**：指資訊資產本身或其保護機制中存在的弱點，可能被威脅利用。
- (3) **衝擊 (Impact)**：指當威脅利用脆弱性成功造成資安事件時，對組織資產所造成的負面影響。

3.1.2 「風險」的定義

為「威脅利用其相對應的脆弱性，造成組織或政府機關的資訊資產受到衝擊的『可能性』」。風險的大小通常由「衝擊」與其發生的「可能性」這兩個因素結合來定義。例如：當「釣魚郵件」（威脅）被使用者點開，利用「未更新的防毒軟體」（脆弱性），可能導致「公文外洩」（衝擊）。

圖 11 透過圖示說明了威脅、脆弱性與衝擊如何交互作用，進而產生風險的概念。這提醒我們，資安防護不僅要防範威脅，也要修補脆弱性，才能有效降低衝擊。

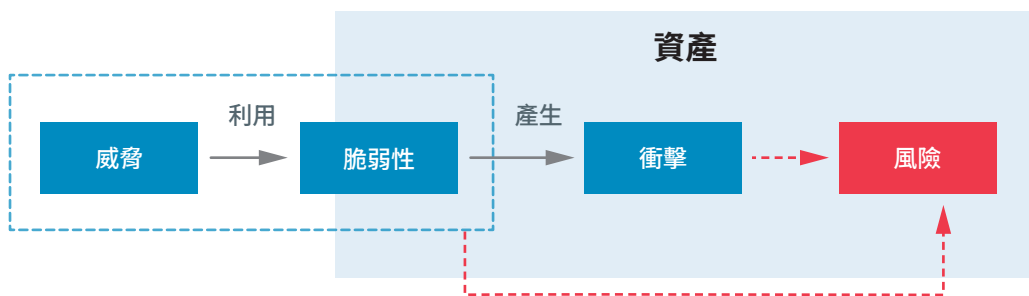


圖 11 風險定義示意圖

3.1.3 衝擊準則

為了客觀地評估資安事件可能造成的損害程度，我們需要訂定「衝擊準則」。這些準則定義了當威脅與弱點結合，破壞資訊或資通系統資產的機密性、完整性及可用性時，對組織可能造成的衝擊嚴重性。這些衝擊可能包含營運受損、信譽損害、資安危害、業務與財務價值損失，以及法律遵循性問題。

在實際評估中，衝擊嚴重性通常會依據資訊的機密性、完整性及可用性遭破壞的程度，分為「普（輕微）」、「中（嚴重）」、「高（非常嚴重或災難性）」三個等級。這將有助於更客觀地評估風險的嚴重性，並決定優先處理順序。圖 11 簡要說明了衝擊的概念，強調其對評估組織衝擊的重要性。

3.1.4 資通安全風險管理

資通安全風險管理是一個系統化的循環過程，旨在確保組織能夠持續識別、評估、處理及監控其資安風險，如圖 12 資通安全風險管理流程圖。這個流程通常包含以下主要階段，並強調各階段之間的持續溝通與協調：

- (1) **風險溝通及諮詢：**此環節貫穿整個風險管理流程，需要持續地與內外部利害關係人進行溝通及諮詢。這包括風險的定義、評估結果、處理決策及監控狀態等資訊的透明傳遞與意見交流。

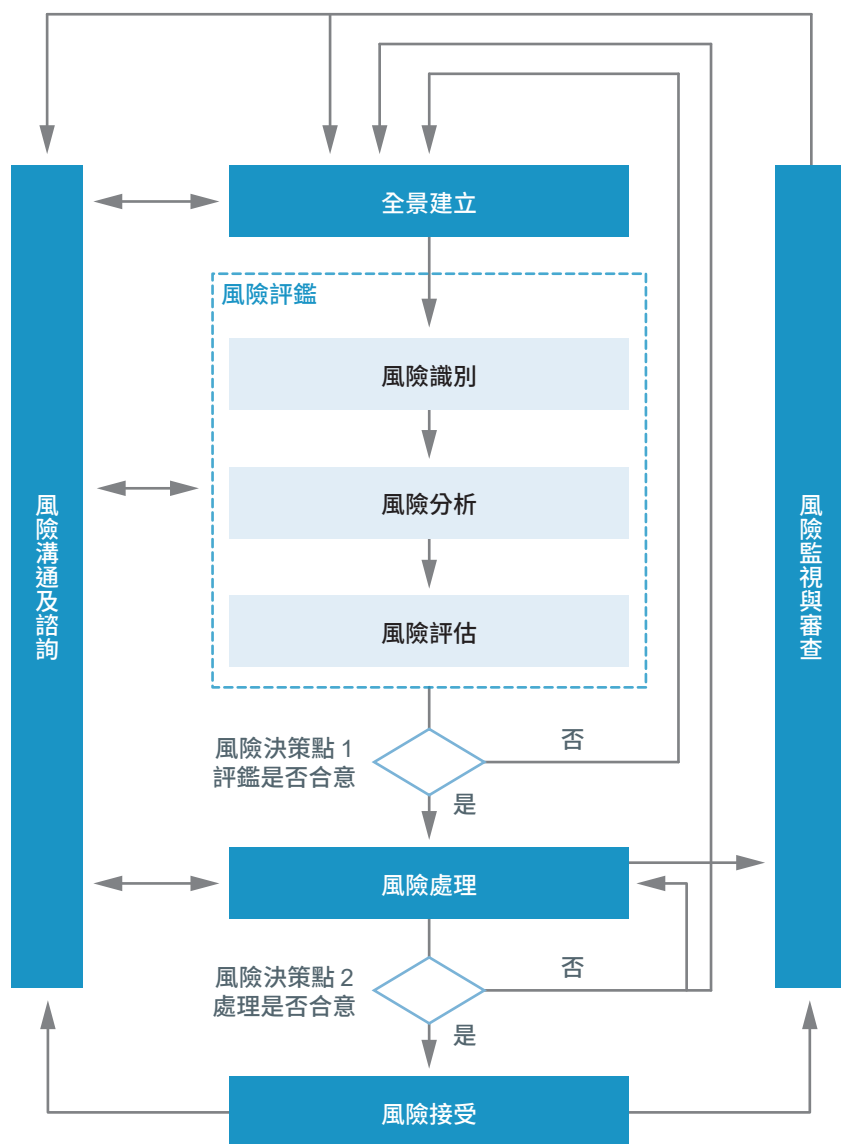


圖 12 資通安全風險管理流程圖

(2) **風險評鑑**：此是風險管理的核心步驟，旨在了解組織面臨的風險狀況，包含以下階段：

- ◆ **全景建立**：確定風險評鑑的範圍、限制與背景資訊，例如組織目標、內外部環境等。
- ◆ **風險辨識**：找出潛在的資通安全風險，包括識別資訊資產、威脅與脆弱性，以及現有控制措施。

- ◆ **風險分析**：評估威脅發生的可能性與事件發生後造成的衝擊，以決定風險等級。
 - ◆ **風險評估**：依據風險分析的結果，判斷風險的等級是否在可接受範圍內。
 - ◆ **風險決策點 1**：若評鑑結果允當，則進入風險處理；若不允當，則需返回風險評鑑階段重新評估。
- (3) **風險處理**：針對評估出的風險，選擇適當的處理方式。常見的策略包括風險修改、風險留存、風險避免或風險分擔。
- (4) **風險決策點 2**：若處理後的風險可接受，則進入風險接受；若仍不可接受，則需返回風險處理階段重新選擇策略。
- (5) **風險接受**：接受經過處理後的殘餘風險。這表示組織已決定承擔該風險可能帶來的後果。
- (6) **風險監視與審查**：持續監控風險及風險管理措施的有效性，並進行定期審查。這個階段的結果會回饋到「風險評鑑」階段，形成一個持續改進的循環，確保風險管理策略能夠隨時適應環境變化。

3.2

風險管理之全景建立

在啟動任何風險評鑑或資通安全防護措施之前，建立一個清晰的「全景」是成功的關鍵。這意味著要對組織內外部的環境有全面的了解，並明確資安管理的目標與準則。

依據我國相關法規，資通安全風險評鑑是法定要求。組織必須依據法規要求進行風險評鑑，以確定各項資訊作業的安全需求水準，並採行適當且充足的資安措施，確保資訊的蒐集、處理、傳送、儲存及流通安全。這不僅是為了符合法律遵循性，更是確保組織資產受到有效保護的基礎。

組織的資安政策應明確聲明，對於施政業務相關的資通系統，必須執行風險評鑑。同時，資安政策也需界定風險評鑑的範圍、參與角色及各自的責任。這確保風險管理工作有高層支持，並在組織內部形成共識，明確分工。

3.2.1 識別機關內、外各方面的安全需求

在進行風險評鑑與實作資安防護控制措施前，組織必須全面識別其內外部各方面的安全需求，這些需求源於組織所處的宏觀環境及自身的微觀運作。

(1) 外部環境：

- ◆ **衝擊組織目標的關鍵因素與趨勢：**例如市場變化、技術發展方向、產業競爭態勢等，這些因素可能引入新的風險或改變現有風險的衝擊程度。
- ◆ **社會與文化、政治、法律、法規命令、財務、科技、經濟及自然等因素：**包含國際、國家、區域性或本地的競爭環境。例如，新的法規（如GDPR、新的資安管理法規），可能會對組織的資安義務產生影響；經濟環境的變化可能影響資安預算；自然災害（如地震、颱風）則可能造成實體資產的損失。

(2) 內部環境：

- ◆ **機關治理、組織架構、角色及責任：**組織的治理模式、部門劃分、各角色的資安職責（如資安長、資安專責人員）以及權責劃分是否清晰，都會影響資安管理的效率與成效。

- ◆ **政策、目標及策略：**組織已制定的資安政策、長期目標及短期策略，是風險評鑑與處理的依據。評鑑應確保風險管理與這些政策保持一致。
- ◆ **能力、資源及知識：**組織在資安方面可用的資源（人力、財力、技術工具）及現有的知識水平（員工資安意識、專業技能），是決定風險管理策略可行性的重要因素。

全面了解組織內外部環境有助於更準確地識別及評估風險，確保風險評鑑的結果具有參考價值，並能夠制定出符合實際情況的資安防護策略。

3.2.2 規劃並定義風險管理基本準則

在啟動風險評鑑之前，組織需要規劃並定義一套共同遵循的風險管理基本準則。這套準則將作為整個評鑑過程的依據，確保評估的一致性與客觀性。主要準則包括：

- (1) **風險管理作法：**明確組織將採用何種風險管理模型或框架（例如基於 ISO/IEC 27005 或 NIST RMF），以及風險管理的整體策略。
- (2) **風險評估準則：**訂定評估風險的具體方法及標準，例如如何判斷威脅的可能性、如何評估脆弱性。
- (3) **衝擊準則：**明確資安事件對組織造成的可能衝擊等級（普、中、高）及其衡量標準。
- (4) **風險接受準則：**訂定組織在考慮成本、效益、法律遵循性等因素後，可以接受的風險水平。這將作為最終風險決策的依據。
- (5) **界定評鑑範圍，清查與盤點範圍內所有相關資通系統：**

如選用「詳細風險評鑑」作法，則需清查盤點資通系統的所有資訊及資通系統資產，同時整合這些資訊與資通系統資產，可能涉及的跨部門業務成員，共同組成資通系統風險評鑑組織，有助於執行與落實風險評鑑的成效。

3.3

風險評鑑之作法

風險評鑑是資通安全風險管理流程中至關重要的一環，旨在識別、分析及評估資通安全風險，以便組織能夠了解其風險暴露程度，並做出明智的決策。風險評鑑的作法可以依據評鑑的深度、所需資源及目標等因素，選擇不同的方法。組織可以依據風險管理的範圍與目標，採用下列不同的風險評鑑作法。

3.3.1 高階風險評鑑

- ◆ 這是一種相對快速、簡便的評鑑方法，依據《資通安全責任等級分級辦法》之資通系統防護需求分級原則，進行高階風險評鑑，以決定資通系統安全等級。旨在快速獲得組織資通系統的風險概觀，並找出最關鍵的風險點。

3.3.2 詳細風險評鑑

- ◆ 這是一種更深入、更精確的評鑑方法，會對資產進行深度識別與鑑別，詳細列出可能面臨的威脅與弱點，作為風險評估及處理的依據。此方法需要投入較多的時間及資源，且可能需要專家意見。
- ◆ 資訊資產一般作法係採詳細風險評鑑，並尋求適當風險處理方案。

在實際的風險管理循環中，組織可能會在不同階段選擇或發展不同的評鑑作法。例如，初期可能採用高階評鑑快速建立風險概觀，隨後針對高風險資產或在發生資安事件後，再執行詳細評鑑。

3.3.3 風險評鑑組織

為確保風險評鑑的客觀性、全面性與實用性，建議成立一個跨部門的風險評鑑組織。風險評鑑不應僅是資訊部門或資安人員的責任，而應納入熟悉各部門業務的人員，因為他們更清楚相關資訊及系統的重要性以及潛在的風險。

(1) **成員組成**：理想的風險評鑑小組成員，應包含但不限於：

- ◆ **資訊部門 / 資安人員**：提供技術專業知識。
- ◆ **總務部門**：協助評估實體安全、環境風險等。
- ◆ **人事部門**：協助評估人員相關風險，如人為失誤、內部威脅等。
- ◆ **會計部門**：協助評估財務衝擊。
- ◆ **業務承辦人員**：最熟悉各部門實際執行業務的承辦人員，能提供最精確的業務流程與資訊資產重要性資訊。

(2) **獨立性與客觀性**：應避免由單一成員執行所有資通系統的風險評鑑工作，以防產出結果過於主觀，不符合真實情況。透過跨部門協作，可確保評鑑結果的客觀性及全面性。

建立一個跨部門的風險評鑑組織，並納入熟悉業務的人員，才能更有效地識別及評估組織的資安風險，提升評鑑結果的可靠性與實用性。

3.3.4 高階風險評鑑的作法

高階風險評鑑是一種快速入門的評估方法，適用於初期建立風險管理機制，其主要優點是簡便易行，能快速獲得風險概觀。

(1) **作法與時機**：

- ◆ 適用於實作風險管理的第 1 年、第 2 年，或組織需要快速了解主要風險時。
- ◆ **直接依據資通系統分級方式進行風險評鑑**：
 - 依據「資通安全責任等級分級辦法」之資通系統防護需求分級原則，決定資通系統安全等級，以省時省力方式，進行高階風險分析。
 - **針對高等級資通系統，亦可再執行詳細風險評鑑**：資通系統經分級結果，屬高安全等級者，可在時間與資源允許情況下，或於資安事件發生後，進一步採行「詳細風險評鑑作法」，以尋求更適當風險處理方案。
- ◆ 可參考安全控制措施參考指引內容，選擇適用之安全控制措施，進行風險處理作業。

(2) **優點**：

- ◆ **簡便易行**：採用較簡單的作法，容易獲得風險評鑑參與人員的接受。
- ◆ **把握時效**：能夠快速找出最關鍵且需受保護的資通系統，優先提出與實作防護措施。



- ◆ **資源運用**：可將有限的資源與預算運用於最有利益之處。

(3) 缺點：

- ◆ **精確度較低**：評鑑結果可能較不精確，可能未識別某些營運過程或系統的潛在風險。
- ◆ **後續需求**：可視需要針對高安全等級的資產，進一步進行詳細風險評鑑作業。

3.3.5 資通系統安全等級處理流程

高階風險評鑑流程是一個系統化的步驟，依資通安全責任等級分級辦法資通系統分級原則，可快速評估資通系統之安全等級。如圖 13 高階風險評鑑作法流程圖。

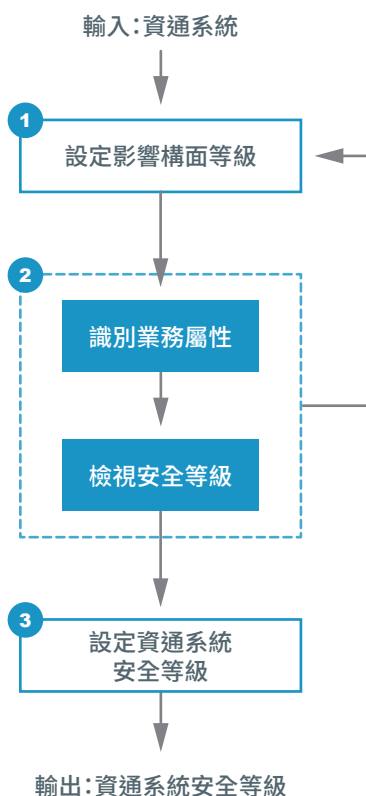


圖 13 高階風險評鑑作法流程圖

(1) 設定影響構面等級：

- ◆ 由業務承辦人依據機密性、完整性、可用性及法律遵循性等四個影響構面，分別考量資通系統於發生資安事件時可能造成的衝擊。
- ◆ **衝擊評估**：衡量資通系統資料外洩、資料遭竄改、系統故障等情事，可能造成的後果嚴重程度。
- ◆ **設定安全等級**：依據衝擊評估結果，初步設定安全等級（普級、中級、高級）。

(2) 識別業務屬性：

- ◆ 識別資通系統所支援的業務屬性，確認其與業務性質的關聯性。

(3) 檢視安全等級：

- ◆ 由承辦單位主管檢視業務承辦人所設定的安全等級是否合理。

(4) 設定資通系統安全等級：

- ◆ 經承辦單位主管與資訊主管確認後，最終由資通安全長核定資通系統安全等級。

3.3.6 資通系統安全等級之衝擊構面

在進行高階風險評鑑時，對資通系統安全等級的各個衝擊構面（機密性、完整性、可用性、法律遵循性）有明確的定義與說明，以便進行標準化評估。

(1) 影響構面「機密性」：

- ◆ **機密性構面**：當資通系統發生資安事件導致資料外洩或遭竄改，造成資料機密性受損時的衝擊程度，如表 9 機密性之安全等級定義。
 - **普級**：資料外洩僅造成**有限**負面影響（如輕微損害）。
 - **中級**：資料外洩將導致機關權益**嚴重**受損（如敏感性資料外洩，影響區域性或地區性個人資料）。
 - **高級**：資料外洩將造成**非常嚴重**或**災難性**負面影響（如機密資料外洩，危及國家安全或個人重大權益，包括特殊個人資料、醫療、財務、全國性個資等）。



表 9 機密性之安全等級定義

安全等級	定義	案例說明
普	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生 有限 之影響。	某政府機關的公開網站。若網站上的非敏感或已公開資訊被惡意揭露，雖然會造成一定的困擾及形象受損，但對機關的核心運作、重要資產或整體信譽造成的衝擊有限。
中	發生資通安全事件致資通系統受影響時，可能造成未經授權之 資訊揭露 ，對機關之營運、資產或信譽等方面將產生 嚴重 之影響。	某機關內部的客戶關係管理 (CRM) 系統。若其中包含客戶的聯絡方式、部分購買歷史等非高度敏感資料被未經授權揭露，可能導致客戶流失、商業競爭力受損，對機關的營運及信譽造成嚴重的負面影響。
高	發生資通安全事件致資通系統受影響時，可能造成未經授權之 資訊揭露 ，對機關之營運、資產或信譽等方面將產生 非常嚴重或災難性 之影響。	某醫院的電子病歷系統。若其中包含患者的詳細診斷、治療紀錄、藥物敏感資訊等高度敏感的個人健康資料被未經授權揭露，不僅會嚴重侵犯個人隱私，更可能導致醫療糾紛、鉅額罰款、患者信任度完全喪失，對醫院的營運、資產（聲譽）造成災難性的打擊，甚至影響其合法經營。

- **完整性構面**：當資通系統委外開發與營運時，若未有效執行資安防護，可能造成系統完整性遭受破壞時的衝擊程度，如表 10 完整性之安全等級定義。
- **普級**：未經授權之資訊修改或破壞，僅造成**有限**負面影響（如一般性資料遭竄改，不致影響機關權益或僅輕微受損）。
- **中級**：未經授權之資訊修改或破壞，造成**嚴重**負面影響（如敏感性資料遭竄改，嚴重損害機關權益，包含區域性重要資訊）。
- **高級**：未經授權之資訊修改或破壞，造成**非常嚴重或災難性**負面影響（如機密資料遭竄改，危及國家安全或導致機關權益重大損害，包含特殊個人資料、醫療、財務、全國性關鍵資訊等）。

表 10 完整性之安全等級定義

安全等級	定義	案例說明
普	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生有限之影響。	某大學的校園論壇系統。若有一般用戶的發帖內容被惡意竄改（如增加錯別字或修改語氣），雖然會影響發帖者表達的原意，但對大學的教學運作、學術資產或整體信譽造成的影響非常有限。
中	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生嚴重之影響。	某機關的庫存管理系統。若產品數量、型號、入庫時間等數據被惡意或意外竄改，將導致生產排程混亂、訂單延誤、財務報表不準確，對機關的生產營運及資產管理造成嚴重影響，可能導致經濟損失及客戶投訴。
高	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	某銀行的核心交易系統。若客戶的轉帳金額、帳戶餘額或交易記錄被惡意竄改，將直接導致客戶資金損失、銀行帳務混亂、金融秩序被破壞，對銀行的營運、資產和信譽造成災難性的衝擊，甚至可能引發系統性金融風險。

- **可用性構面：**當資通系統中斷服務，造成可用性受損時的衝擊程度，如表 11 可用性之安全等級定義。
- **普級：**資訊、資通系統存取或使用中斷，造成有限負面影響（如系統容許中斷時間較長，僅輕微影響社會、業務效能）。
- **中級：**資訊、資通系統存取或使用中斷，造成嚴重負面影響（如系統容許中斷時間較短，嚴重影響社會秩序、業務效能）。
- **高級：**系統中斷對機關造成非常嚴重或災難性影響（如系統容許中斷時間極短，影響社會、國安，業務可能停擺）。



表 11 可用性之安全等級定義

安全等級	定義	案例說明
普	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生有限之影響。	某圖書館的自助借還書機系統。若該系統因故障或攻擊而中斷服務數小時，讀者仍可透過人工櫃檯借還書，雖造成不便，但對圖書館的核心服務、資產運營和信譽影響有限。
中	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生嚴重之影響。	某機關的訂單處理系統。若該系統在業務高峰期（如促銷活動期間）因攻擊而中斷數小時，將導致大量訂單無法處理、客戶無法下單、商品積壓，對機關的營收、資產（庫存）及客戶信譽造成嚴重損失。
高	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	某機關的電力調度控制系統，若該系統因惡意攻擊或嚴重故障而中斷運行，將導致全國或大範圍停電，嚴重影響民生、工業生產、公共安全，對國家社會運作、經濟資產和政府信譽造成災難性後果，甚至可能引發社會動盪。

- **法律遵循性構面：**當資通系統運作違反相關法令或規範時，可能導致的法律責任程度，如表 12 法律遵循性之安全等級定義。
- **普級：**未遵循其他資通相關法令或規範（如其他資通系統設置或運作於法令有相關規範之情形，僅屬一般法規規範）。
- **中級：**違反資通相關法令，致人員受行政罰、懲戒或懲處（如可能導致資安事件或業務公正性受影響，並受行政處分）。
- **高級：**違反資通相關法令，致人員負刑事責任（如可能導致資安事件或業務公正性受影響，並需負刑事責任）。
- **違反情境案例：**特定非公務機關如違反第 18 條第 4 項所定辦法中有關通報及應變機制必要事項之規定，由中央目的事業主管機關令限期改正；屆期末改正者，按次處新臺幣十萬元以上一百萬元以下罰鍰。公

務機關所屬人員如未遵守本法規定者，應按其情節輕重，依相關規定予以懲戒或懲處。

表 12 法律遵循性之安全等級定義

安全等級	定義	案例說明
普	其他資通系統設置或運作於法令有相關規範之情形。	某機關的網站使用條款未完全符合最新的消費者保護法對隱私權聲明的細節要求，但並未造成實質損害或重大違規。可能需要修改，但通常不會引發嚴重法律後果。
中	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而 導致 資通安全事件，或 影響他人 合法權益或機關執行業務之公正性及正當性，並 使 機關或其所屬人員受 行政罰、懲戒或懲處 。	某機關未能有效落實《個人資料保護法》規定的資料安全措施，導致大量非敏感客戶資料（如電子郵件、電話號碼）外洩。這可能導致主管機關對機關處以行政罰鍰，並可能對相關負責人員進行內部懲戒。
高	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而 導致 資通安全事件，或 影響他人 合法權益或機關執行業務之公正性及正當性，並 使 機關所屬 人員負刑事責任 。	某金融機構的資通系統在反洗錢監管方面存在嚴重漏洞，且未能按規定申報可疑交易，導致大量犯罪資金透過其系統洗白。這可能不僅會導致鉅額罰款及業務限制，其相關負責人員（如高階主管、內控人員）可能因瀆職或協助洗錢而被追究刑事責任。

3.3.7 以「全球資訊網」為範例

以「全球資訊網」（官方網站，提供機關簡介與政策措施）為例，依據上述資通安全責任等級分級辦法，初步評估其在機密性、完整性、可用性及法律遵循性四個影響構面的安全等級：

(1) **機密性**：初估為「普」級。

原因說明：網站資訊皆為可公開的一般性資料，不涉及敏感資訊。



(2) **完整性**：初估為「普」級。

原因說明：主要提供資訊公告，資訊內容修改影響輕微。

(3) **可用性**：初估為「普」級。

原因說明：提供一般性資料瀏覽，系統中斷對機關日常作業影響有限。

(4) **法律遵循性**：初估為「普」級。

- ◆ **原因說明**：必須符合智慧財產權相關法令，並遵守兒童及少年福利與權益保障法及相關規定，惟不涉及從根本上違反法律之可能性，也不致因違反規範導致嚴重不良後果。

針對這個作為機關簡介及政策發布的「全球資訊網」，其初步的資安風險等級，在各個構面都被評估為普通。

3.3.8 詳細風險評鑑的作法

詳細風險評鑑是一種更為深入且結構化的過程，旨在對資產進行深度識別與鑑別，並詳細列出可能面臨的威脅與弱點，作為評鑑風險與風險處理方法的依據。相較於高階風險評鑑，詳細評鑑更精確，但也需要更多時間及資源，通常針對較重要的資產或在需要更精確評估結果時採用。

(1) **特點**：

- ◆ 對資產進行深度識別與鑑別，詳細列出可能面臨的威脅與弱點。
- ◆ 詳細步驟需考慮時間、耗費程度及專家意見。
- ◆ 可採用定量方法（計算具體損失金額）、定性方法（使用高、中、低等級描述風險），或兩者結合。
- ◆ 依據資產價值或需被保護的特性，評鑑威脅發生的可能性。

(2) **詳細風險評鑑三個階段**：

通常分為「風險識別」、「風險分析」及「風險評估」三個階段：

- ◆ **風險識別 (Risk Identification)**：

- **資產識別**：找出資通系統中應優先處理的資訊與資通系統資產。
- **威脅與脆弱性識別**：找出資通系統與資產存在的威脅及弱點。
- **現有控制措施識別**：評估目前已實施的防護措施。
- **後果識別**：預測若資安事件發生可能造成的後果。

- ◆ **風險分析 (Risk Analysis)**：

- **後果評估**：評估資通系統資產價值與事件可能造成的衝擊。

- **事件可能性評估：**評估資安事件發生的可能性。
- **決定風險等級：**綜合可能性與衝擊，決定風險的等級。

◆ **風險評估 (Risk Evaluation)：**

- **決定風險可接受等級：**依據風險分析結果，判斷風險是否在可接受範圍內。

風險評鑑是資安管理中不可或缺的環節。無論是採用高階或詳細評鑑，其目的都是為了更精確地識別及評估組織的風險，並為後續的風險處理提供明確的依據。

(3) 風險接受準則 (Risk Acceptance Criteria)：

- ◆ **先決定風險處理範圍：**機關會因所負責任務的類別與性質、服務對象、內部資源及經費預算等因素，影響風險處理範圍，在有限資源下，決定哪些風險影響層面較大，需優先進行處理，哪些風險影響層面較小，在資源不足情況下，暫時予以接受而保留風險。

◆ **可能影響風險接受準則項目：**

風險接受準則，因機關負責任務不同而考量重點不同，可能影響風險接受準則項目：

- 業務需求與目標
- 法律、法令、規章及契約方面要求
- 資源分配狀況
- 技術成熟度
- 經費預算
- 社會與人道主義因素

3.4

風險處理之作法

風險處理是繼風險評鑑之後的關鍵步驟，旨在針對已評估出的風險，選擇並實施適當的行動方案，以降低風險至可接受的水平。風險處理活動應依據風險評鑑結果、處理方案的預期成本及預期利益等因素，選擇最適合組織的行動方案。

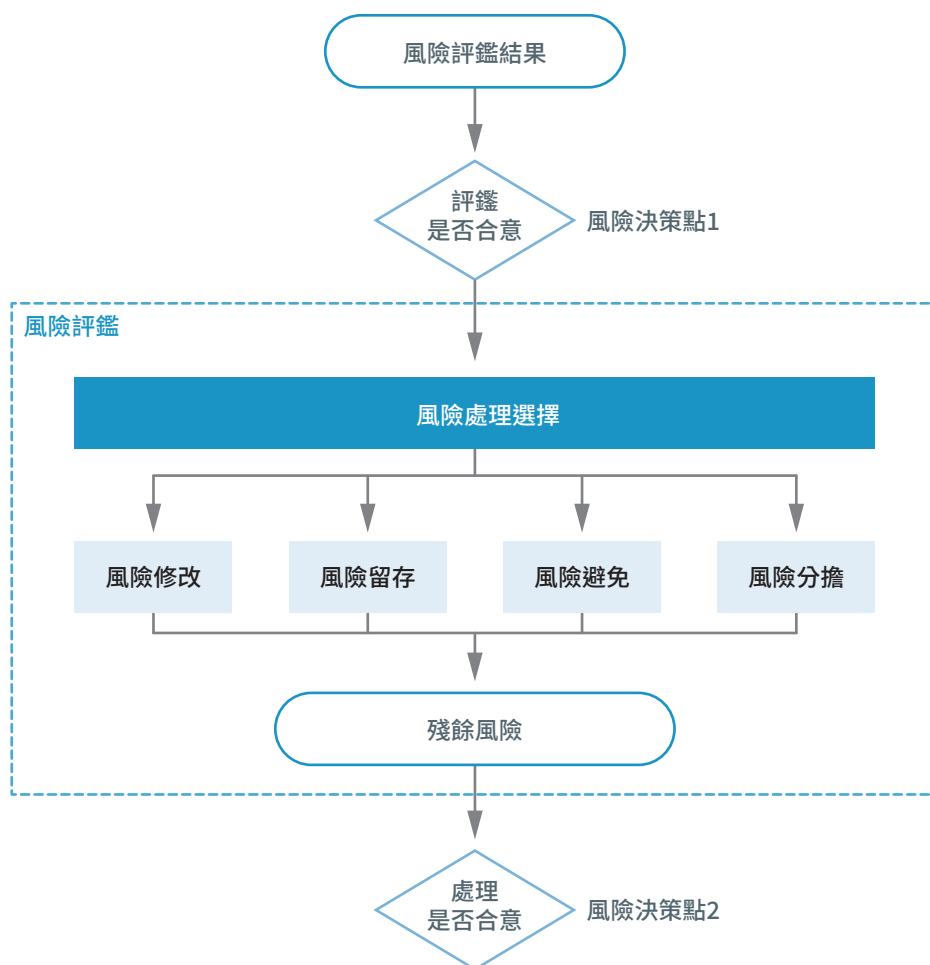


圖 14 風險處理流程圖

一般而言，風險處理的目標是使風險的不利後果能夠合理地降低。風險處理風險處理主要有四種策略，包括為風險修改、風險留存、風險避免、風險分擔，如圖 14 風險處理流程圖。

3.4.1 風險修改

是最常見的風險處理方式。其目的是藉由施行、移除或改變安全控制措施，修訂或降低風險等級，使殘餘風險被重新評定為可接受。

- (1) **主要方法**：透過調整安全控制措施，降低風險發生的可能性或其造成的衝擊。
- (2) **控制措施類型**：控制措施可提供多種形式的保護，包含：
 - ◆ **矯正 (Correction)**：修復已存在的漏洞或錯誤。
 - ◆ **消弭 (Elimination)**：完全移除風險來源。
 - ◆ **預防 (Prevention)**：阻止事件發生。
 - ◆ **衝擊最小化 (Impact Minimization)**：減輕事件發生後的損害。
 - ◆ **制止 (Deterrence)**：透過威懾手段阻止攻擊者。
 - ◆ **偵測 (Detection)**：及時發現資安事件。
 - ◆ **復原 (Recovery)**：恢復受損系統及資料。
 - ◆ **監視 (Monitoring)**：持續監測系統及環境。
 - ◆ **認知 (Awareness)**：提升人員資安意識。
- (3) **考量**：在選擇控制措施時，應權衡其實作及維護的成本，與被保護資產的價值進行比較，以確保成本效益。
- (4) **高階評鑑的控制措施選擇**：若組織採用「高階風險評鑑」作法，其控制措施的選擇可以參考「安全控制措施參考指引」，依據風險評鑑等級（普、中、高）選擇適用之安全控制措施。

風險修改是積極降低風險的手段，透過實施適當的安全控制措施，可以有效地減少潛在的損失。

3.4.2 風險留存

風險留存是指依據風險評估結果，確認無進一步行動，而保留風險的決策。這是一種被動的風險處理方式，通常在處理成本過高或沒有其他可行方案時採用，但需要持續監控及緊急準備。



- (1) **決策條件**：若風險等級符合風險接受準則，則不需要實作額外控制措施，風險將被保留。
- (2) **正式決策**：即使選擇保留風險，該決策也應基於正式的評估過程，並得到組織高層的批准。
- (3) **範例**：某自建機房容易斷電，但因空間限制無法建置發電機，也無法保險或搬遷至其他辦公場所，故只能選擇保留此風險。這說明在某些資源有限的情況下，組織可能不得不接受部分風險。
- (4) **後續管理**：即使選擇保留風險，該風險仍為「殘餘風險」，組織必須定期監控，並考量實施業務持續管理計畫，以便在風險真正發生時能夠快速因應處理。

風險留存是一種被動的風險處理方式，通常在處理成本過高或沒有其他可行方案時採用，但需要持續監控及應急準備，並應確保該決定是經過充分考量及批准的。

3.4.3 風險避免

風險避免是指組織直接放棄或避免可能造成特定風險增加的活動或情況，從根本上消除風險。

- (1) **主要方法**：透過終止或避免活動，徹底消除與特定風險相關的暴露。
- (2) **範例 1**：某機關為了避免遭受零日漏洞攻擊的風險，決定不在其核心系統中使用任何第三方未經嚴格安全審核的開源函式庫，並自行開發所有必要的程式碼。此例說明了如何透過某種管制行為來避免可能的風險。
- (3) **範例 2**：將發電機從容易淹水的地下室移置到樓上，以避免颱風淹水導致發電機損壞的風險。此例說明了透過改變環境或做法來避免可能的風險。

風險避免是最直接的風險處理方式，能夠從根本上消除風險。但有時可能會影響到組織的運作或目標的達成，因此需要仔細評估。

3.4.4 風險分擔

風險轉移是指依據風險評估結果，將部分或全部風險分攤至能有效管理特定風險的第三方。這是一種常見的風險處理方式，可以幫助組織減少自身承擔的風險及潛在損失。所採用的方式如下：

(1) **保險 (Insurance)**：適用於硬體資產，例如機房設備。透過購買保險，將因意外事件造成的損失風險轉移給保險公司。

(2) **契約中增訂懲罰性違約金條款**：在與供應商簽訂契約時，可以加入違約金條款。若供應商未能履行契約，則將因其未履行契約而造成的損失風險部分轉移給供應商。

風險分擔是一種將風險責任或財務負擔轉移給第三方的處理方式，通常用於處理成本較高或影響較大的風險，透過保險或契約條款，確保組織在發生資安事件時能夠獲得一定程度的補償或分擔。

MEMO

3.5

風險接受之作法

風險接受是風險處理計畫中的一個重要環節，涉及組織在全面了解殘餘風險後，決定是否承擔這些風險的過程。這個決策必須被明確記錄，並基於對組織利益、成本及潛在風險的權衡。

3.5.1 如何處理評定之風險，以滿足風險接受準則。

「風險接受準則」指的是決定哪些風險需要處理，哪些風險可以接受的標準。這個準則並非一成不變，此準則會因機關所負責任務的類別與性質不同而有所差異。影響風險接受準則制定的因素：

- (1) **業務需求與目標**：組織的核心業務對風險的承受度直接影響風險接受標準。
- (2) **法律、法令、規章及契約方面要求**：法規可能對某些風險有強制性的處理要求，組織必須遵循。
- (3) **資源分配狀況**：可用的預算、人力及技術資源會限制組織能夠處理的風險數量及深度。
- (4) **技術成熟度**：某些風險可能因缺乏成熟的技術解決方案而不得不接受。
- (5) **經費預算**：降低風險的成本若過於高昂，可能導致組織選擇接受該風險。
- (6) **社會與人道主義因素**：對於涉及公共安全或人道問題的風險，組織的接受度通常會非常低。

這些因素共同影響組織對風險的判斷，例如，如果某個風險會嚴重影響核心業務的達成，或者違反了法律規定，那麼組織可能就不太能接受這個風險。

3.5.2 殘餘風險的等級可能不符合風險接受準則

在某些情況下，即使組織已採取風險處理措施，殘餘風險的等級仍可能不符合常態的風險接受準則。這可能是因為最初制定準則時未考量當時的具體環境，或伴隨風險的利益非常吸引人，或風險修改成本過高。在這些特殊情況下，組織需要採取下列更為審慎及透明的策略，以管理這些不符合常態的風險。

- (1) **決策與記錄**：若決策者必須接受不完全符合常態風險接受準則的風險，應明確在該風險上註解，並包含無視常態風險接受準則的決策衡量理由。這確保了決策的透明性及可追溯性。
- (2) **持續監視**：即使風險被接受，組織仍應定期監視這些殘餘風險，因為風險狀況可能隨時間而變化。這包括追蹤潛在威脅的演變、檢測新的脆弱性，以及評估現有控制措施的有效性。
- (3) **應變計畫**：對於已接受的殘餘風險，應制定應變計畫，以在風險事件發生時能夠迅速應對，降低實際損害。這與業務持續運作計畫緊密相關。

風險接受是一個重要的決策環節，要求組織在利益、成本及風險之間進行權衡。主要強調了資安管理並非追求零風險，而是在充分理解並記錄的情況下，承擔部分風險，並持續監控與管理，以確保組織整體利益的最大化。

MEMO

3.6

國際相關防護及管理標準

除了國家法規與內部管理流程外，許多國際標準與框架也為資通安全風險管理提供了寶貴的指導。這些標準有助於組織建立與國際接軌的資通安全管理體系，提升防護能力，並促進全球資安社群的協同合作。

3.6.1 NIST CSF 2.0

美國國家標準與技術研究院 (National Institute of Standards and Technology, NIST) 所發布的資通安全框架 (Cybersecurity Framework, CSF) 是一套廣泛使用的自願性框架，旨在幫助組織更好地管理及降低網路安全風險。最新的 NIST CSF 2.0：2024 在原有基礎上進行了重要更新與擴展，此框架自 2014 年首次發布以來的最重大更新。

(1) 資通安全框架 - NIST CSF 2.0: 2024 文件之章節名稱如下：

- ◆ 資通安全框架 (Cybersecurity Framework, CSF) 概述
- ◆ CSF 核心 (Core) 介紹
- ◆ CSF 剖繪 (Profiles) 及層級介紹
 - 3.1. CSF 範疇
 - 3.2. CSF 層級 (Tiers)
- ◆ 補充 CSF 之線上資源介紹
- ◆ 加強網路安全風險溝通與整合
 - 改善風險管理溝通
 - 改善與其他風險管理計畫之整合
- ◆ 附錄 A：CSF 核心 附錄 B：CSF 層級 附錄 C：詞彙表

(2) 核心目的：

提供一套標準化的術語、流程及最佳實踐，幫助組織有效管理及降低網路安全風險。

(3) 主要內容：

這是 CSF 2.0 最引人注目的變革。在原有的「識別 (Identify)」, 「保護

(Protect)」、「偵測 (Detect)」、「回應 (Respond)」、「復原 (Recover)」五個功能之上，新增了第六個核心功能：「治理 (Govern)」。

◆ **六大核心功能**：如圖 15 NIST 網路安全框架之核心功能圖。



圖 15 NIST 網路安全框架之核心功能圖

- **治理 (Govern - GV)：**(CSF 2.0 新增的核心功能) 建立並溝通資通安全策略、角色、責任及監督。這強調了資安治理結構及決策在組織資安中的重要性。
- **識別 (Identify - ID)：**了解組織的資通安全風險，包括資產、業務環境、治理結構、風險評估及供應鏈。這是資安防護的第一步，確保組織了解所要保護的對象及其潛在風險。
- **保護 (Protect - PR)：**制定並實施保障措施，以支持限制或遏制資通安全事件的能力。這是關於如何建立防護機制來保護組織資產。
- **偵測 (Detect - DE)：**制定並實施活動，以識別資通安全事件的發生。及時發現資安事件對於後續的應對至關重要。
- **反應 (Respond - RS)：**制定並實施有關網路安全事件的行動。當資安事件發生時，組織需要有相應的處理流程。
- **回復 (Recover - RC)：**制定並實施應急計畫，以便在資通安全事件後恢



復能力及服務。在事件發生後，如何快速恢復正常運作也是非常重要的。

◆ **擴大適用範圍：**

- CSF 1.0 最初主要針對美國的關鍵基礎設施。CSF 2.0 則明確指出，其設計適用於所有行業、所有規模的組織，包括小型企業、非營利組織及政府機構。
- 這使得框架更具普適性，幫助更廣泛的組織提升網路安全韌性。

◆ **強調成果導向 (Outcomes-Oriented)：**

- CSF 2.0 更注重資通安全活動所帶來的實際「成果」及「成效」，而不僅僅是實施了哪些控制措施。
- 旨在幫助組織更好地衡量及溝通其網路安全投資的價值，並將資通安全活動與特定的業務成果聯繫起來。

◆ **強化供應鏈風險管理 (SCRM)：**

- 雖然在 1.1 版中已有涉及，但在 2.0 版中，供應鏈資通安全風險管理被提升到更重要的位置，並在「治理」功能中被明確突出。
- 這反映了當今供應鏈攻擊的日益頻繁及複雜，組織需要更好地識別、評估及管理其供應商及協力廠商帶來的資通安全風險。

◆ **改進實施指南及資源：**

- NIST 為 CSF 2.0 提供了更豐富、更具操作性的資源，包括：更清晰地解釋了 CSF Tiers（層級）及 Profiles（剖繪）的使用，幫助組織定制框架以適應其特定需求。
- 提供「快速入門指南」及可編輯的模板，降低組織開始使用框架的門檻。
- 強化了與其他框架（如 NIST SP 800-53、ISO 27001 等）的對應關係，便於組織整合現有安全措施。
- 推出 CSF 2.0 參考工具 (Reference Tool)，提供可搜索及可機讀的框架內容。

◆ **持續的靈活性與適應性：**

- 儘管更新了許多內容，CSF 2.0 仍保留了其固有的靈活性，不是一個合規性標準或清單，而是一個風險管理工具，允許組織依據自身的風險偏好、業務需求、資源及技術環境進行定制化實施。

3.6.2 CNS 27005：2024

CNS 27005 是我國的國家標準，其內容與國際標準 ISO/IEC 27005 相對應。主要提供組織如何管理資訊安全風險的指引，是建立及維持有效資訊安全風險管理體系的重要參考。

(1) 核心目的：

本標準旨在為組織提供關於資訊安全風險管理的指引，特別是針對 CNS 27001（資訊安全管理系統 - 要求事項）中關於處理資訊安全風險的要求，也補充了 CNS 27003（資訊安全管理系統實作指引）中的相關指引，並整合了 CNS 31000（風險管理 - 指導綱要）的一般風險管理原則。

(2) 主要內容與結構：

- ◆ **適用範圍：**說明本標準適用於所有類型、規模或行業的組織，協助其滿足 CNS 27001 中關於資訊安全風險評鑑與處理的要求。
- ◆ **術語與定義：**定義了資訊安全風險管理中的關鍵術語，如風險、威脅、脆弱性、後果、可能性、風險接受準則、風險胃納、剩餘風險等。
- ◆ **資訊安全風險管理過程：**
 - 描述了資訊安全風險管理的迭代過程，包括風險評鑑及風險處理。
 - 強調風險評鑑及處理是一個持續的循環，應依據組織內部及外部環境的變化定期更新，分為「策略循環」及「運作循環」。
- ◆ **全景建立：**指導組織識別其內部及外部環境，瞭解利害相關者的要求事項，並建立及維護資訊安全風險準則（包括風險接受準則及風險評鑑執行準則），這些準則應考量後果、可能性及風險等級的判定方法。
- ◆ **資訊安全風險評鑑過程：**
 - **風險識別：**發現、辨識及描述風險，包括風險來源（如人員、環境、技術）及事件。提供了「事件式作法」及「資產式作法」兩種常見方法。
 - **風險分析：**評估潛在後果（損害程度）及事件發生的可能性（機率或頻率），以判定風險等級。
 - **風險評估：**將風險分析結果與已建立的風險準則進行比較，判斷風險是否可接受，並排定風險處理的優先序。
- ◆ **資訊安全風險處理過程：**
 - **處理選項選擇：**提供多種風險處理選項，包括風險避免、風險修改（降低可能性或後果）、風險留存（知情選擇接受）、風險分擔（如透過



保險)。

- **控制措施判定：**依據選定的處理選項，判定所有必要的控制措施，這些措施可來自 CNS 27001 附錄 A 或客製化。
- **適用性聲明：**要求生成一份「適用性聲明 (Statement of Applicability, SOA)」，文件化所有必要的控制措施、納入理由、實作狀態以及排除 CNS 27001 附錄 A 中控制措施的理由。
- **風險處理計畫：**制定具體的風險處理計畫，包括責任、資源、時間表及績效指標，並由風險當責者核可，最終決定是否接受「剩餘風險」。
- ◆ **運作：**指導組織如何執行風險評鑑及處理過程，使其整合到日常營運中，並在規劃期間或事件觸發時進行。
- ◆ **善用相關之 ISMS 過程：**說明資訊安全風險管理如何與 ISMS 的其他過程（如組織全景、領導承諾、溝通、文件化資訊、監視與審查、矯正措施、持續改善）相結合，以確保其有效性及持續性。
- ◆ **附錄 A（技術示例）：**提供了詳細的技術示例及表格，說明如何建立風險準則（後果尺度、可能性尺度、風險矩陣），並列舉了典型威脅及脆弱性的分類，以實際支持風險評鑑過程。

CNS 27005:2024 是一份全面的指引文件，詳細說明了組織如何系統地識別、分析、評估、處理及監控資訊安全風險，以實現其資訊安全目標，並與 CNS 27001 等相關標準保持一致。

MEMO

Handwriting practice lines consisting of 20 horizontal dashed lines.

單元

4

資通安全管理面
暨認知與訓練應辦事項

資通安全不僅僅是技術層面的防禦，更是一個涵蓋策略、管理、人員與日常運營的全面性議題。為了確保組織的資通安全體系能夠有效運作並持續精進，除了技術防護措施外，完善的管理制度、明確的人員職責、持續的資安教育訓練與定期評估更是不可或缺。

本單元將深入探討這些「管理面」暨認知與訓練應辦事項，旨在為讀者建立清晰的資安管理認知，並了解如何透過組織層面的努力，共同提升資安防護能力。

本單元學習重點如下：

- 1** 了解資通系統分級與防護基準，掌握不同等級系統的資安要求。
- 2** 理解資訊安全管理系統 (ISMS) 的導入與驗證要求，以及相關國際標準。
- 3** 認識資通安全專責人員的配置規定與職責。
- 4** 掌握內部資通安全稽核的頻率與不同稽核類別的特點。
- 5** 了解業務持續運作演練的重要性，以及其核心指標與管理流程。
- 6** 學習資安治理成熟度的評估方式與等級定義，以衡量組織資安管理水準。
- 7** 認識資安認知與訓練的重要性，並了解不同角色應具備的資安素養與訓練要求。



4.1

管理面—資通系統分級與防護基準

為了確保資通安全資源的有效分配與風險的精準管理，我國《資通安全管理法》及其子法規定了資通系統的分級與防護基準。這項規定旨在讓各機關（構）能依據其所管資通系統的重要性、業務性質與潛在風險，實施相應的資安防護措施。

首先針對不同責任等級的公務機關及特定非公務機關設定了不同的應辦事項。如表 13 管理面 - 資通系統分級與防護基準規定。

表 13 管理面 - 資通系統分級與防護基準規定

資通安全責任等級		應辦事項
公務機關	特定非公務機關	
A 級、B 級		初次受核定或等級變更後之 1 年內，針對自行或委外開發之資通系統，依附表 9 完成 資通系統分級，並 完成 附表 10 之控制措施；其後應每年至少 檢視 1 次資通系統分級妥適性。
C 級		初次受核定或等級變更後之 1 年內，針對自行或委外開發之資通系統，依附表 9 完成 資通系統分級；其後應每年至少 檢視 1 次資通系統分級妥適性；並應於初次受核定或等級變更後之 2 年內， 完成 附表 10 之控制措施。
D 級、E 級		無要求

表 13 顯示，不同責任等級之機關，所需完成資通系統分級及實施控制措施方面，有不同的時程要求：

4.1.1 機關責任等級之應辦事項

- (1) **A 級及 B 級機關**：初次受核定或等級變更後的 1 年內，針對自行或委外開發之資通系統，必須依附表 9 完成資通系統分級，並完成附表 10 之控制措施；其後應每年至少檢視 1 次資通系統分級妥適性。這表示等級越高的系統，要求越快完成相關工作，且需定期檢視。
- (2) **C 級機關**：初次受核定或等級變更後的 1 年內，針對自行或委外開發之資通系統，依附表 9 完成資通系統分級；其後應每年至少檢視 1 次資通系統分級妥適性；並應於初次受核定或等級變更後之 2 年內，完成附表 10 之控制措施。相較於 A 級及 B 級之時間要求稍寬鬆。
- (3) **D 級及 E 級機關**：對於這兩個等級的機關，則沒有強制要求實施分級與控制措施。

需要注意的是，若資通系統的性質為共用性系統，則由該資通系統的主責設置、維護或開發機關判斷是否屬於核心資通系統。

4.1.2 資通系統防護需求分級原則

資通系統的防護需求會依據其所涉及的機密性 (C)、完整性 (I)、可用性 (A) 及法律遵循性 (L) 四個構面來評估，並將其影響程度劃分為「高」、「中」、「普」3 個等級。這些分級原則提供了評估系統風險的標準化依據，如表 14 資通系統防護需求分級原則。

表 14 資通系統防護需求分級原則

防護需求 等級 構面	高	中	普
機密性 (C)	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生 非常嚴重或災難性 之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生 嚴重 之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生 有限 之影響。





防護需求 等級 構面	高	中	普
完整性 (I)	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生 非常嚴重或災難性 之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生 嚴重 之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生 有限 之影響。
可用性 (A)	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生 非常嚴重或災難性 之影響。	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生 嚴重 之影響。	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生 有限 之影響。
法律遵循性 (L)	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統 受影響 而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關所屬人員 負刑事責任 。	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統 受影響 而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關或其所屬人員受 行政罰、懲戒或懲處 。	其他資通系統設置或運作於法令有相關規範之情形。

表 14 詳細定義了在機密性、完整性、可用性及法律遵循性這 4 個構面下，不同防護需求等級所對應的影響程度。例如：

- ◆ **機密性 (C) 高等級**：發生資通安全事件致資訊揭露，對機關營運、資產或信譽等方面將產生**非常嚴重**或**災難性**影響。
- ◆ **完整性 (I) 中等級**：發生資通安全事件致資訊錯誤或遭竄改，對機關營運、資產或信譽等方面將產生**嚴重**影響。
- ◆ **可用性 (A) 普等級**：發生資通安全事件致資訊、資通系統之存取或使用中斷，對機關營運、資產或信譽等方面將產生**有限**影響。
- ◆ **法律遵循性 (L) 高等級**：未遵循資通相關法令，使機關或其所屬人員負**刑事**責任。

4.1.3 資通系統防護基準

依據資通系統的防護需求分級，主管機關也訂定了一套具體的「資通系統防護基準」，列出了應實施的控制措施。這些措施涵蓋了 7 個主要構面，並依據高、中、普 3 個防護需求等級，對應了不同數量的控制措施。如表 15 資通系統防護基準摘要。

表 15 資通系統防護基準摘要

構面 (項次)	控制措施
1. 存取控制 (3 項)	帳號管理、最小權限、遠端存取
2. 事件日誌與可歸責性 (6 項)	記錄事件、日誌紀錄內容、日誌儲存容量、日誌處理失效之回應、時戳及校時、日誌資訊之保護
3. 營運持續計畫 (2 項)	系統備份、系統備援
4. 識別與鑑別 (5 項)	內部使用者之識別與鑑別、身分驗證管理、鑑別資訊回饋、加密模組鑑別、非內部使用者之識別與鑑別
5. 系統與服務獲得 (8 項)	系統發展生命週期之需求階段、設計階段、開發階段、測試階段、部署與維運階段、委外階段、獲得程序、系統文件
6. 系統與通訊保護 (2 項)	傳輸之機密性與完整性、資料儲存之安全
7. 系統與資訊完整性 (3 項)	漏洞修復、資通系統監控、軟體及資訊完整性



表 15 詳列了 7 個構面及其對應的控制措施，總計有 171 項控制措施，其中屬高等級防護需求的有 78 項，中等級防護需求的有 58 項，普等級防護需求的有 35 項。這些控制措施將在第六章「資通系統防護控制措施」中進一步詳細說明。透過資通系統的分級與防護基準，組織能夠有系統地實施資安防護，確保資源的有效利用。

MEMO

4.2

管理面—ISMS 之導入及通過公正第三方之驗證

資訊安全管理系統 (Information Security Management System, ISMS) 是一套系統化的方法，用於管理組織的敏感資訊，使其在適當的保護下始終安全。ISMS 的導入與通過驗證，是組織展現其資安管理能力的重要里程碑。

依據資通安全責任等級的不同，各級機關及特定非公務機關在 ISMS 的導入及驗證方面有不同的應辦事項要求，如表 16 ISMS 導入及驗證規定。

表 16 管理面 -ISMS 導入及驗證規定

資通安全責任等級		ISMS 導入要求	ISMS 驗證要求
公務機關	特定非公務機關		
A 級、B 級		初次受核定或等級變更後之二年內，全部核心資通系統導入 CNS 27001 或 ISO 27001 等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準	於三年內完成 公正第三方驗證 ，並持續維持其驗證有效性。
C 級			未要求
D 級、E 級		未要求	未要求

表 16 所謂「公正第三方驗證」指通過我國標準法主管機關委託機構認證之機構；第三方核發之驗證證書應有前開委託機構之認證標誌。這確保了驗證的公正性與權威性。

4.2.1 ISO/IEC 27000 系列標準

ISO/IEC 27000 系列標準是國際上廣泛使用的資訊安全管理標準族群，為組

織建立、實施、維護及持續改進 ISMS 提供了全面的框架與指引，如表 17 ISO/IEC 27000 常見系列標準，涵蓋了從概觀、要求、稽核驗證，到控制措施、風險管理，以及特定行業的應用指引。我們在前面提到的 ISO/IEC 27001 就是 ISMS 要求事項的標準，其附錄中所提及的相關控制措施清單，於 ISO/IEC 27002 標準中，有更詳細的說明；而 CNS 27005 則對應於 ISO/IEC 27005，是風險管理的指引。我國資通安全法規亦將 CNS 27001 或 ISO/IEC 27001 之 ISMS 導入及驗證納入機關應辦事項。

表 17 ISO/IEC 27000 常見系列標準

分類	ISO/IECV	年份	控制措施
詞彙標準	27000	2018	資訊安全管理系統 - 概觀及詞彙
要求事項標準	27001	2022	資訊安全管理系統 - 要求
	27006-1	2024	提供資訊安全管理系統審核與驗證機構的要求 - 第 1 部分：一般要求
	27006-2	2021	提供資訊安全管理系統審核與認證機構的要求 - 第 2 部分：隱私資訊管理系統
指導綱要標準	27002	2022	資訊安全控制措施
	27003	2017	資訊安全管理系統 - 指導綱要
	27004	2016	資訊安全管理 - 監控、測量、分析與評估
	27005	2022	資訊安全風險管理指引
	27007	2020	資訊安全管理系統稽核指導綱要
	27008	2019	資訊安全控制評鑑指導綱要
	27013	2021	ISO/IEC 27001 與 ISO/IEC 20000-1 整合實作指引
	27014	2020	資訊安全治理
行業待定指導綱要標準	27010	2015	跨行業與跨組織通訊的資訊安全管理
	27011	2024	基於 ISO/IEC 27002 的電信組織資訊安全控制措施





分類	ISO/IECV	年份	控制措施
行業待定 指導網要 標準	27017	2015	基於 ISO/IEC 27002 的雲端服務資訊安全控制措施指導網要
	27018	2019	作為個人可識別資訊 (PII) 處理者的公有雲保護個人可識別資訊指導網要
	27701	2025	隱私資訊管理系統要求事項及指導網要

4.2.2 CNS 27001：資訊安全管理系統

CNS 27001：2023 是我國的國家標準，等同於 ISO/IEC 27001：2022，是資訊安全管理系統的要求事項。此標準列出了組織建立、實施及維護 ISMS 所需遵循的框架。其附錄 A 則提供了資訊安全控制措施的參考，這些控制措施在 CNS 27002 中有更詳細的說明。以下為 CNS 27001：2023 各章名稱及其附錄 A 規定：

- ◆ 1. 適用範圍
- ◆ 2. 引用標準
- ◆ 3. 用語及定義
- ◆ 4. 組織全景
- ◆ 5. 領導作為
- ◆ 6. 規劃
- ◆ 7. 支援
- ◆ 8. 運作
- ◆ 9. 績效評估
- ◆ 10. 改善
- ◆ 附錄 A（規定）參考控制目標及控制措施
 - A.5 組織控制措施（共 37 項）
 - A.6 人員控制措施（共 8 項）
 - A.7 實體控制措施（共 14 項）
 - A.8 技術控制措施（共 34 項）



4.2.3 CNS 27002：2023

CNS 27002：2023 則是等同於 ISO/IEC 27002：2022 的國家標準，作為資訊安全控制措施的指導綱要。此標準詳細列出了組織控制措施、人員控制措施、實體控制措施及技術控制措施等四大類別下的具體項目，如表 18 CNS 27002：2023 之各章節名稱。

表 18 CNS 27002 2023 之各章節名稱

章次及章名	CNS 27002：2023 節次及節名	
1. 適用範圍		8
2. 引用標準		8
3. 用語、定義及續寫	3.1 用語及定義 3.2 續寫 18-13	8-13
4. 本標準之結構	4.1 節次 4.2 主題及屬性 4.3 控制措施布局	13-15
5. 組織控制措施	5.1 資訊安全政策 5.2 資訊安全之角色及責任 5.3 職務區隔 5.4 管理階層責任 5.5 與權責機關之聯繫 5.6 與特殊關注群組之聯擊 5.7 H 在脅情資 5.8 專案管理之資訊安全 5.9 資訊及其他相關聯資產之清冊 5.10 可接受使用資訊及其他相關聯資產 5.14 資訊傳送 5.15 存取控制 5.16 身分管理	5.17 鑑別資訊 5.18 存取權限 5.19 供應者關棒、中之資訊安全 5.20 於供應者協議中間明資訊安全 5.21 管理 ICT 供應鏈中之資訊安全 5.22 供應者服務之監視、審查及變更管理 5.23 使用雲端服務之資訊安全 5.24 資訊安全事故管理規劃及準備 5.25 資訊之評鑑及決策



章次及章名	CNS 27002：2023 節次及節名		
5. 組織控制措施	5.26 對資訊安全事故之回應 5.27 由資訊安全事故中學習 5.28 證據之蒐集 5.29 中斷期間之資訊安全 5.30 營運持續之 ICT 備妥性 5.31 法律、法令、法規及契約要求事項	5.32 智慧財產權 5.33 紀錄之保護 5.34 障私及 PII 保護 5.35 資訊安全之獨立審查 5.36 資訊安全政策、規則及標準之遵循性 5.37 書面記錄之運作程序	15-60
6. 人員控制措施	6.1 篩選 6.2 聘用條款及條件 6.3 資訊安全認知及教育訓練 6.4 獎懲過程	6.5 聘用終止或變更後之責任 6.6 機密性或保密協議 6.7 遠端工作 6.8 資訊安全事件通報	60-68
7. 實體控制措施	7.1 實體安全周界 7.2 實體進入 7.3 保全辦公室、房間及設施 7.4 實體安全監視 7.5 防範實體及環境威脅 7.6 於安全區域內工作 7.7 桌面淨空及螢幕淨空	7.8 設備安置及保護 7.9 場所外資產之安全 7.10 儲存媒體 7.11 支援之公用服務事業 7.12 佈纜安全 7.13 設備維護 7.14 設備汰除或重新使用之保全	68-81
8. 技術控制措施	8.1 使用者端點裝置 8.2 特殊存取權照 8.3 資訊存取限制 8.4 對原始碼之存取 8.5 安全鑑別 8.6 容量管理 8.7 防範惡意軟體 8.8 技術脆弱性管理 8.9 組態管理 8.10 資訊刪除 8.11 資料遮蔽 8.12 資料洩露預防 8.13 資訊備份	8.14 資訊處理設施之多備 8.15 存錄 8.16 監視活動 8.17 鐘訊同步 8.18 具特殊權限公用程式之使用 8.19 運作中系統之軟體安裝 8.20 網路安全 8.21 網路服務之安全 8.22 網路區隔 8.23 網頁過濾 8.24 密碼技術之使用 8.25 安全開發生命週期	81-129



章次及章名	CNS 27002：2023 節次及節名		
8. 技術控制措施	8.26 應用系統安全要求事項 8.27 安全系統架構及工程原則 8.28 安全程式設計 8.29 開發及驗收中之安全測試 8.30 委外開發	8.31 開發、測試與運作環境之區隔 8.32 變更管理 8.33 測試資訊 8.34 稽核測試期間資訊系統之保護	81-129
附錄 A (參考)	使用屬性		130-140
的錢 B (參考)	1CNS 27002：2023 （本標準）與 CNS 27002：20 15 之對應		140-147
參考資料			147-150
名詞對照			150-156

ISMS 是組織系統化管理資訊安全的核心。遵循 ISO/IEC 27000 系列標準，特別是 CNS 27001 及 CNS 27002，能夠協助組織建立一套符合國際最佳實踐的資安管理體系，從而有效地保護資訊資產，降低資安風險。

4.3

管理面一
資通安全專責人員

資通安全不僅是技術與制度的結合，更需要「人」的執行與管理。因此，資通安全專責人員的配置與職責，是確保資安政策與措施能夠有效落實的關鍵。我國資通安全管理相關法規對資通安全專責人員的配置有明確的規定。

資通安全專責人員，係指應全職執行資通安全業務者。不同資通安全責任等級的機關（構）所需配置的專責人員數量有所不同。如表 19 管理面 - 資通安全專責人員規定，A 級、B 級及 C 級機關之資通安全專責人員配置人數，分別為 4 人、2 人及 1 人，而公務機關之專職人員，指全職執行資通安全業務者。

表 19 管理面 - 資通安全專責人員規定

資通安全責任等級		資通安全責任等級	
公務機關	特定非公務機關	公務機關	特定非公務機關
A 級		初次受核定或等級變更後之 1 年內，配置 4 人；須以專職人員配置之。	初次受核定或等級變更後之 1 年內，配置 4 人。
B 級		初次受核定或等級變更後之 1 年內，配置 2 人；須以專職人員配置之。	初次受核定或等級變更後之 1 年內，配置 2 人。
C 級		初次受核定或等級變更後之 1 年內，配置 1 人；須以專職人員配置之。	初次受核定或等級變更後之 1 年內，配置 1 人。
D 級、E 級		無要求	

資通安全專責人員是資安管理體系中不可或缺的核心人力。明確的配置規定確保了各級機關能夠投入足夠的專業人力來執行資安業務，為組織的資安防護提供堅實的基礎。

4.4

管理面— 內部資通安全稽核

內部稽核是資通安全管理體系中自我檢查與持續改進的重要環節。透過定期進行內部稽核，組織能夠檢視自身資通安全維護計畫的實施狀況，發現潛在問題，並確保資安措施的有效性與法規遵循性。

不同資通安全責任等級的機關在辦理內部資通安全稽核的次數上有所不同，等級越高，稽核頻率越高。如表 20 管理面 - 內部資通安全稽核規定，A 級每年辦理 2 次、B 級每年辦理 1 次、C 級每 2 年辦理 1 次，D 級及 E 級則無要求。

表 20 管理面 - 內部資通安全稽核規定

資通安全責任等級		辦理內部稽核次數
公務機關	特定非公務機關	
A 級		每年辦理 2 次
B 級		每年辦理 1 次
C 級		每 2 年辦理 1 次
D 級、E 級		無要求

資通安全稽核可以依據其執行者、目的與範圍的不同，區分為三種類型：「第一方稽核」、「第二方稽核」及「第三方稽核」，如表 21 資通安全稽核類型。

表 21 資通安全稽核類型

第一方稽核	第二方稽核	第三方稽核
內部資通安全稽核	上級機關稽核下級機關， 或機關稽核委外廠商	導入及通過公正 第三方 ISMS 驗證
資通安全責任等級分級辦法第 11 條第 1 項應辦事項：內部資通安全稽核。	1. 資通安全管理法：第 5 條主管機關應定期公布對公務機關資通安全維護計畫實施情形稽核概況報告。第 13 條公務機關應稽核其所屬或監督機關之資通安全維護計畫實施情形。 2. 特定非公務機關資通安全維護計畫實施情形稽核辦法第 3 條主管機關除因不可抗力因素外，應每年擇定受稽核之特定非公務機關（以下簡稱受稽核機關），並以現場實地稽核之方式，稽核其資通安全維護計畫實施情形。 主管機關為辦理第 1 項稽核，應訂定稽核計畫。	CNS 27001：2023 9.2.2 內部稽核計畫：組織應規劃、建立、實作及維持稽核計畫。
1. 稽核範圍：全機關 2. 稽核項目： 稽核項目檢核表 資訊安全控制措施	1. 稽核範圍：全機關 2. 稽核項目： 稽核項目檢核表	1. 稽核範圍：驗證範圍 2. 稽核項目： 資訊安全控制措施

4.4.1 第一方稽核（內部資通安全稽核）

- (1) 目的：組織內部的自我檢查，用以確認自身資安維護計畫的實施狀況。
- (2) 稽核範圍：全機關。
- (3) 稽核項目：依稽核項目檢核表、資訊安全控制措施。
- (4) 說明：依據《資通安全責任等級分級辦法》第 11 條第 1 項應辦事項進行。

4.4.2 第二方稽核（上級機關稽核下級機關，或機關稽核委外廠商）

- (1) 目的：外部單位對供應商或下級單位的稽核，用以確認其是否符合契約或



法規要求。

(2) **稽核範圍**：全機關或委外廠商。

(3) **稽核項目**：依稽核項目檢核表。

(4) **說明**：

- ◆ 依《資通安全管理法》第 5 條及第 13 條，主管機關應定期公布對公務機關資安維護計畫實施情形的稽核概況報告，並稽核其所屬或監督機關。
- ◆ 依《特定非公務機關資通安全維護計畫實施情形稽核辦法》第 3 條，中央目的事業主管機關應每年擇定受稽核之特定非公務機關，進行現場實地稽核。
- ◆ 主管機關為辦理第一項稽核，應訂定稽核計畫。

4.4.3 第三方稽核（導入及通過公正第三方 ISMS 驗證）

(1) **目的**：由獨立的第三方認證機構進行，以取得國際認可的資安管理系統驗證（如 CNS 27001：2023）。

(2) **稽核範圍**：驗證範圍。

(3) **稽核項目**：資訊安全控制措施。

(4) **說明**：依 CNS 27001：2023 9.2.2 內部稽核計畫，組織應規劃、建立、實作及維持稽核計畫。

不同類型的稽核扮演著不同的角色，共同確保組織資通安全防護的有效性與合法性。內部稽核是組織自律的體現，第二方稽核是監督與管理，而第三方稽核則是取得外部認可的途徑。

4.5

管理面—
業務持續運作演練

業務持續運作演練是確保組織在面臨突發事件（如資安事件、天然災害等）時，仍能維持核心業務運作的關鍵，不僅測試應變計畫的可行性，也提升人員的應變能力與協作效率。

不同資通安全責任等級的資通系統，需要對其核心業務系統進行業務持續運作演練的頻率有所不同，如表 22 管理面 - 內部業務持續運作演練規定，A 級全部核心資通系統每年辦理 1 次、B 級全部核心資通系統每 2 年辦理 1 次、C 級、D 級及 E 級則無要求。

表 22 管理面 - 內部業務持續運作演練規定

資通安全責任等級		辦理演練次數
公務機關	特定非公務機關	
A 級		全部核心資通系統 每年辦理 1 次
B 級		全部核心資通系統 每 2 年辦理 1 次
C 級、D 級、E 級		無要求

4.5.1 營運持續計畫

營運持續計畫 (Business Continuity Plan, BCP) 是業務持續運作演練的基礎。其中，有兩個重要的時間指標，用以衡量組織對資料損失及服務中斷的容忍度：

(1) 復原點目標 (Recovery Point Objective, RPO)：

- ◆ **定義：**訂定系統可容忍資料損失的時間要求。指從災害發生回溯至最近



一次可用備份的時間長度，代表組織能容忍的最大資料丟失量。

- ◆ **重要性：**RPO 越短，表示組織需要越頻繁地備份資料，以減少資料損失。
- ◆ **應辦事項：**應將備份還原作為營運持續計畫測試的一部分；應定期測試備份資料，以驗證備份媒體的可靠性及資訊的完整性。

(2) 復原時間目標 (Recovery Time Objective, RTO)：

- ◆ **定義：**訂定資通系統從中斷後至重新恢復服務之可容忍時間要求。指從災害發生到系統服務恢復運作的時間長度，代表組織能容忍的服務中斷時間。
- ◆ **重要性：**RTO 越短，表示組織需要更快速的復原機制，如備援設備或替代方案。
- ◆ **應辦事項：**原服務中斷時，於可容忍時間內，由備援設備或其他方式取代並提供服務。

(3) 最大可容忍中斷時間 (Maximum Tolerable Period of Disruption, MTPD)

此外，最大可容忍中斷時間也是一個關鍵概念，指的是組織於發生業務運作中斷而無法提供產品或服務時，可承受最長的空窗期間。MTPD 通常包含 RTO 及工作恢復時間 (Work Recovery Time, WRT)，即 $MTPD = RTO + WRT$ 。例如「線上報稅系統的 MTPD 可能是 24 小時，超過即影響國家財稅作業。

(4) 系統備份

營運持續計畫有兩個關鍵面向，包括系統備份及系統備援。首先介紹系統備份，系統備份是指對資料進行複製及存儲的過程，以便在資料丟失、損壞或系統故障時能夠恢復。以下資通系統防護基準之系統備份規定。

- ◆ **訂定系統可容忍資料損失之時間要求 (RPO)**
 - RPO 代表在發生資通安全事件時，企業所能容忍的最大資料損失量。換句話說，指在災難發生前，最近一個有效備份的時間點。例如，如 RPO 為 4 小時，則表示企業可以接受最多損失 4 小時的資料。
 - 這決定了備份的頻率。為了達到較小的 RPO，需要更頻繁地進行備份。
- ◆ **應將備份還原，作為營運持續計畫測試之一部分。（適用高等級之資通系統）**
 - 強調了定期測試備份還原過程的重要性。光有備份是不夠的，必須確保備份能夠成功還原，並且資料是完整的。

- ◆ 應定期測試備份資料，以驗證備份媒體之可靠性及資訊之完整性。（適用高等級及中等級之資通系統）

- 這說明了不僅要測試還原過程，還要定期檢查備份本身，確保備份媒體沒有損壞，並且備份的資料是完整且可用的。

(5) 系統備援：

系統備援是指在主要系統中斷後，啟動備用系統或恢復服務的策略及過程，以確保業務的連續性。以下資通系統防護基準之系統備援規定。

- ◆ 訂定資通系統從中斷後至重新恢復服務之可容忍時間要求 (RTO)

- RTO 代表在發生資通安全事件後，企業所能容忍的最大服務中斷時間，即從中斷發生到服務完全恢復正常運行的時間。例如，如 RTO 為 2 小時，則表示企業必須在 2 小時內恢復服務。
- 這決定了恢復策略的選擇（例如熱備援、冷備援），以及所需的資源及技術。

- ◆ 原服務中斷時，於可容忍時間內，由備援設備或其他方式取代並提供服務。

- 這明確指出，當主要服務中斷時，必須在預先設定的 RTO 時間內，利用備援設備或其他方式的恢復策略，來接管並提供服務，以最小化業務停擺的影響。

營運持續計畫中兩個關鍵的目標指標 - RPO 及 RTO，以確保系統能在發生中斷時快速恢復運作。這有助於提高組織的業務連續性及抗災能力。

(6) 營運持續計畫時程：

以下說明營運持續計畫 (BCP) 時程，以甘特圖的形式展現了從災害發生到業務恢復正常運作的各個階段及子任務。並說明一個典型的 BCP 文件包含的目錄，如圖 16 營運持續計畫時程，將 BCP 的時程分為以下主要階段：

- ◆ 災害發生：是整個流程的起點，表示有突發事件或災難發生。

- ◆ 啟動階段：

- 緊急處理：在災害發生後立即進行的初步應對措施。
- 災害評估：評估災害的影響範圍、嚴重程度，以及對業務運作造成的衝擊。
- 是否啟動：依據災害評估結果，決定是否啟動 BCP。
- 通報作業：向相關人員、部門及利害關係人發布災害及 BCP 啟動的通知。

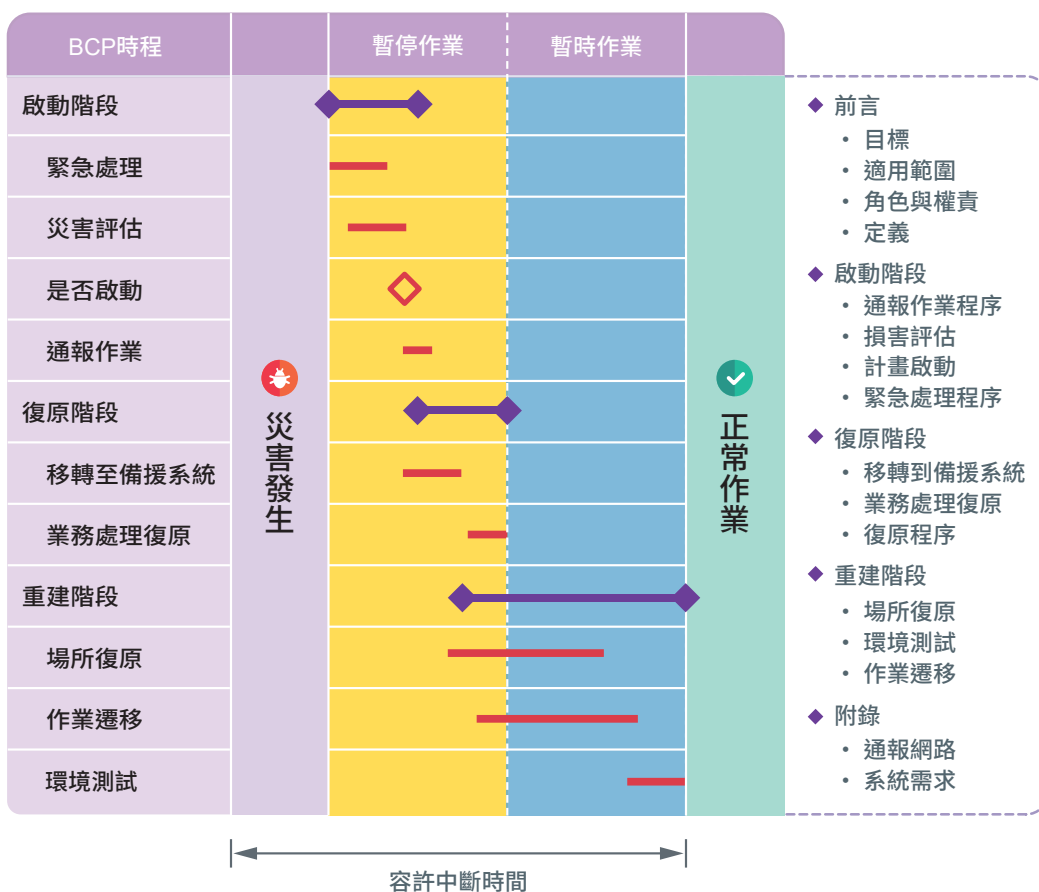


圖 16 營運持續計畫時程

◆ 復原階段（復原階段）

- 移轉至備援系統：將業務運作從受損的主系統轉移到預先準備好的備援系統。
- 業務處理復原：在備援系統上恢復關鍵業務流程的運作。

◆ 重建階段

- 場所復原：修復或重建受損的辦公場所、設施等。
- 作業遷移：將業務運作從備援系統逐步遷回修復好的主系統或新場所。
- 環境測試：測試新的或復原的環境，確保所有系統及流程正常運作。

圖中的橫條表示每個任務的持續時間，從圖中可以看出：

- ◆ 啟動階段通常在災害發生後立即開始，並且持續時間相對較短。
- ◆ 復原階段緊隨啟動階段之後，主要涉及系統及業務的快速恢復。
- ◆ 重建階段的時間跨度可能較長，因為涉及場所及基礎設施的恢復。

下方的「容許中斷時間」表示從災害發生到業務恢復到可接受水平之間所允許的最長時間。這是一個關鍵指標，用來衡量 BCP 的有效性。圖中的顏色區塊代表不同的運作狀態：

- ◆ **暫停作業（黃色）**：表示業務受到中斷，正在進行緊急處理及評估。
- ◆ **暫時作業（藍色）**：表示業務在備援系統上進行，或以暫時方式運作。
- ◆ **正常作業（綠色）**：表示業務已完全恢復正常運作。

右側的文字是一個典型的 BCP 文件的目錄，通常包含以下章節：

① **前言（前言）**：介紹 BCP 的目的及重要性。

- ◆ **目標**：說明 BCP 旨在達成的具體目標，例如降低災害影響、縮短復原時間等。
- ◆ **適用範圍**：界定 BCP 涵蓋的業務範圍、部門或系統。
- ◆ **角色與權責**：明確災害發生時各個角色及部門的職責。
- ◆ **定義**：解釋 BCP 中使用的專業術語。

② **啟動階段**：詳細描述災害發生後如何啟動 BCP。

- ◆ **通報作業程序**：具體的通知流程及通訊方式。
- ◆ **損害評估**：如何進行災害損失及影響的評估。
- ◆ **計畫啟動**：啟動 BCP 的條件及程序。
- ◆ **緊急處理程序**：緊急狀況下的應對措施。

③ **復原階段**：描述如何恢復業務運作。

- ◆ **移轉到備援系統**：將運作轉移到備援系統的步驟。
- ◆ **業務處理復原**：恢復關鍵業務流程的細節。
- ◆ **復原程序**：詳細的復原步驟。

④ **重建階段**：描述如何將業務恢復到常規運作狀態。

- ◆ **場所復原**：修復或重建實體場所的步驟。
- ◆ **環境測試**：測試恢復後環境的程序。
- ◆ **作業遷移**：將業務從備援系統遷回主系統的計畫。

附錄：額外支援資訊。

- ◆ **通報網路**：緊急聯絡人名單及通訊方式。
- ◆ **系統需求**：BCP 實施所需的 IT 系統及資源。

(7) **資通安全維護計畫範本**：

數位發展部資通安全署為協助各機關推動資安維護工作，特於官方網站提

供「資通安全維護計畫範本」供機關參考。各機關在訂定此計畫時，應明確將前述所討論的「最大可容忍中斷時間」納入其中，以確保服務持續性。以下將針對資通安全維護計畫範本中三個關鍵要素進行說明：「核心資通系統」、「重要性說明」以及「最大可容忍中斷時間」。

◆ **核心資通系統：**

- 依資通安全責任等級分級辦法規定，此為支持核心業務運作必要之系統。
- 依資通安全責任等級分級辦法附表 9 資通系統防護需求分級原則之規定，判定其防護需求等級為高，亦應列為核心資通系統。

◆ **重要性說明：**

- 依數位發展部資通安全署提供的維護計畫範本內容，重要性說明係指說明該業務對機關之重要性
- 例如對機關財務及信譽上影響，對民眾影響，對社會經濟影響，對其他機關業務運作影響，法律遵循性影響或其他重要性之說明

◆ **最大可容忍中斷時間 (MTPD)：**

- 指在無法提供核心服務或未執行核心服務需要的作業或系統時，可能產生的不利衝擊變得無法接受所需的時間
- 可能是法令法規的要求、契約的要求，或利害相關方（如主管機關）的要求。

(8) 業務持續運作之必要性

- ◆ 為使組織不會因突發事件造成業務運作中斷，需要有專責人員去識別來自組織外部，包含全球大環境的風險與威脅。
- ◆ 因應資通安全管理法實施，機關需要透過資通安全責任等級分級辦法核定的資安等級，識別出業務持續運作需求。
- ◆ 要成功將業務持續運作機制校準施政目標，並納入組織日常運作，需要機關高層人員支援與調用資源，並與業務持續運作專責人員共同協作。

4.5.2 業務持續運作管理系統 – ISO/IEC 22301：2019

ISO/IEC 22301：2019 是一個國際標準，為組織建立、實施、維護及持續改進業務持續運作管理系統，提供了一個要求事項。可參考 CNS 22301：2021 安全與復原力－事業持續管理系統－要求事項。

- (1) **標準名稱：**安全與韌性 - 營運持續運作管理系統 - 要求事項 (Security and Resilience-Business Continuity Management Systems-Requirements)
- ◆ 這明確了該標準的全名，並強調了「安全」與「韌性」是業務持續性的核心，並且這是一個「要求事項 (Requirements)」的標準，意味著組織可以依據這個標準來建立自己的管理系統，並尋求第三方驗證。
- (2) **目的：**規範實施與維護營運持續運作管理系統 (BCMS) 的結構與要求事項
- ◆ 這點出了標準的核心目標。ISO/IEC 22301 的目的就是提供一套明確的指引，告訴組織如何架構其 BCMS，包括所需的政策、程序、角色職責、資源分配等，並提出具體的要求，以確保 BCMS 的有效運作。
- (3) **適用範圍：**本文件規定了實施、維護及改善營運持續運作管理系統的要求事項，以防止、減少發生營運中斷的可能性、準備、應變及恢復
- ◆ 這說明了標準的應用範圍，並涵蓋了 BCMS 的整個生命週期：
 - **實施 (Implementation)：**如何建立 BCMS。
 - **維護 (Maintenance)：**如何讓 BCMS 持續有效運作。
 - **改善 (Improvement)：**如何依據變化和經驗不斷優化 BCMS。
 - ◆ 最終目標是多方面的：
 - **防止 (Prevent)：**降低中斷事件發生的可能性。
 - **減少 (Reduce)：**即使事件發生，也能減少其衝擊。
 - **準備 (Prepare)：**預先做好應對中斷的準備。
 - **應變 (Respond)：**在中斷發生時能有效採取行動。
 - **恢復 (Recover)：**在中斷後能迅速恢復業務運作。
- (4) **實作指引：**安全與韌性 - 業務持續管理系統 - ISO 22301 之使用指引 - ISO 22313:2020 (Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301)
- ◆ ISO 22301 是「要求事項」，其相關的標準 ISO 22313 就是提供「指引」。此標準提供了更詳細的建議及最佳實踐，幫助組織理解如何實踐 ISO 22301 中的要求。對於那些希望深入了解如何實施 BCMS 的組織來說，ISO 22313 是一個非常有用的補充文件。

4.5.3 業務持續運作 - 名詞解釋

在 ISO 22301:2019 標準中，與業務持續運作相關的一系列核心名詞及概



念。這些定義是理解業務持續性管理系統的基礎。以下是每個名詞的詳細解釋：

(1) 業務持續運作 (Business Continuity, BC)

- ◆ **定義：**「組織在業務運作中斷期間，以預定容量在可接受的時間範圍內，繼續交付產品與服務的能力」
- ◆ **說明：**這是最核心的概念，不是指「不讓業務中斷」，而是指當業務確實發生中斷時（例如，因為災害、系統故障、疫情等），組織有能力在預先設定的限制內（「預定容量」和「可接受的時間範圍」），繼續提供其關鍵產品和服務。這強調了**韌性 (Resilience)** 及**恢復能力 (Recovery Capability)**。

(2) 業務持續運作管理 (Business Continuity Management, BCM)

- ◆ **定義：**「實施與維護業務持續運作的過程」
- ◆ **說明：**BCM 是指組織為了達到「業務持續運作」的目標，所採取的一系列管理活動、流程及措施，是一個持續性的過程，包括規劃、實施、監控、審查及改進所有與業務持續性相關的活動。它是「業務持續運作」這個「能力」的「實現方法」。

(3) 業務持續運作管理系統 (Business Continuity Management System, BCMS)

- ◆ **定義：**「建立、實施、維運、監控、審查、維護及改善業務持續運作的整體管理系統的一部分 (ISO 22300：2021)」
- ◆ **說明：**BCMS 是一個更正式、系統化的框架。它將 BCM 的各項活動組織成一個結構化的管理系統。就像 ISO 9001 是品質管理系統，ISO 27001 是資訊安全管理系統一樣，BCMS 是專門針對業務持續性而設計的管理系統，包含政策、目標、流程、文件、角色及職責等，旨在確保 BCM 活動能夠有效、一致地執行並持續改進。括號中提到是 ISO 22300：2021 的一部分，這表示 ISO 22300 是一個更廣泛的詞彙及核心概念標準，而 BCMS 是其中的一個具體應用。

(4) 業務持續運作計畫 (Business Continuity Plan, BCP)

- ◆ **定義：**「指導組織因應業務運作中斷、反應重啟及恢復業務持續運作目標之文件化資訊」。
- ◆ **說明：**BCP 是 BCMS 的一個具體「產物」或「文件」，是實際指導應對及恢復行動的詳細指引。這份文件包含了在不同中斷情境下的應變步驟、恢復程序、聯絡資訊、團隊職責、所需資源等。當災害或中斷發生時，

團隊成員需要依循的「操作手冊」。BCP 是 BCMS 的核心組成部分，不只是文件，真正重要的是背後的管理系統及執行能力。另業務持續運作計畫之名稱，依資通系統防護基準稱為營運持續計畫。

(5) 營運衝擊分析 (Business Impact Analysis, BIA)

- ◆ **定義：**「分析業務運作中斷隨時間推移對組織的衝擊的過程」
- ◆ **說明：**BIA 是一個關鍵的分析工具，用於識別組織的關鍵業務功能、這些功能對 IT 系統或其他資源的依賴性，以及如果這些功能中斷，可能在不同時間點（例如，中斷 1 小時、4 小時、1 天、1 週）對組織造成的潛在影響。這些影響包括財務損失、聲譽損害、法律合規問題、安全風險等，例如若公文系統中斷 1 天，則會造成公務延誤與法規遵循風險。BIA 的結果是設定 RTO（復原時間目標）及 RPO（復原點目標）的基礎，並幫助組織優先保護最重要的業務活動。

(6) 最大可容忍中斷時間 (Maximum Tolerable Period of Disruption, MTPD)

- ◆ **定義：**「組織於發生業務運作中斷而無法提供產品或服務時，可承受最長的空窗期間」
- ◆ **說明：**MTPD 是指在業務中斷發生後，如果超過這個時間，組織的業務功能將無法恢復到最低可接受的運作水平，甚至可能導致組織面臨不可逆轉的嚴重後果，例如破產、法律制裁、聲譽毀滅或失去關鍵客戶等。代表了**業務功能可以停止運作的絕對最長時間極限**。MTPD 的設定通常是基於業務影響分析 (BIA) 的結果，是決定所有恢復策略及時間目標的**上限**。一旦超過 MTPD，後果可能非常嚴重。

(7) 復原點目標 (Recovery Point Objective, RPO)

- ◆ **定義：**「組織於發生業務運作中斷事件後，復原可以用來啟動業務持續運作達成最低業務持續運作目標的資料時間點（係 組織能容忍的最大資料損失量）」
- ◆ **說明：**RPO 關注的是資料的「新鮮度」或可接受的「資料損失量」，是一個時間點，表示在業務中斷發生時，組織能容忍的最大資料損失。例如，如果 RPO 設定為 4 小時，這意味著組織可以接受最多損失最近 4 小時的資料更新。這直接影響到備份及複製的頻率：要達到更小的 RPO，就需要更頻繁的資料備份或更即時的資料同步。

(8) 復原時間目標 (Recovery Time Objective, RTO)

- ◆ **定義：**「組織於發生業務運作中斷事件後，啟動業務持續運作達成最低

業務持續運作目標的時間點」

- ◆ **說明：**RTO 關注的是服務的「恢復速度」，是一個時間點（或時間長度），表示在業務中斷發生後，組織必須在多長時間內將其關鍵業務功能及相關系統恢復到最低可接受的運作水平。例如，如 RTO 設定為 2 小時，則意味著從中斷發生起，組織有 2 小時的時間將受影響的服務重新上線。RTO 的設定直接影響到恢復策略的選擇，例如是採用熱備援或是冷備援，以及所需的人力、技術及資源。

4.5.4 業務持續運作 - 管理程序

業務持續運作管理程序是一個系統性的方法，旨在確保組織在面臨中斷或災難時，仍能維持其核心業務功能的運作。如圖 17 業務持續運作之管理程序圖：

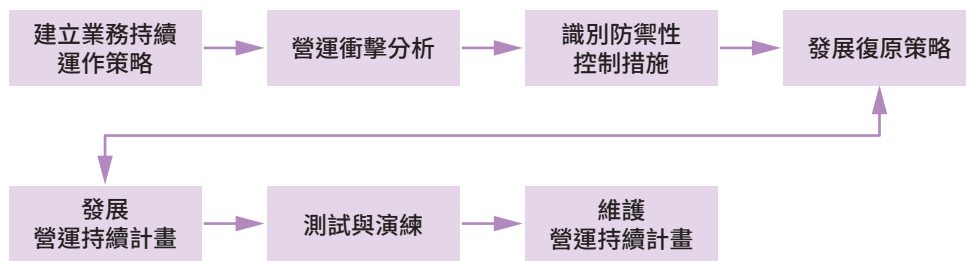


圖 17 業務持續運作之管理程序圖

圖 16 中的程序是循序漸進的，且環環相扣，以下說明每一個步驟的程序：

(1) 建立業務持續運作策略

- ◆ **目的：**這是整個業務持續計畫的起點。在此階段，組織會定義其業務持續的願景、目標、範圍及原則。這包括決定要保護哪些關鍵業務功能、可容忍的中斷時間及資料損失量，以及投入的資源預算等。這是高階管理層級的決策。

(2) 營運衝擊分析 (BIA)

- ◆ **目的：**識別並評估業務中斷可能對組織造成的潛在影響，用來了解當災害發生後的嚴重程度，以及需要多少時間來處理。BIA 的結果將幫助組織確定哪些業務功能需要最優先的保護。以下說明 BIA 的處理步驟：
- ◆ **BIA 的步驟**
 - 識別機關的核心業務功能

- 識別核心業務所仰賴的資源
- 計算核心業務可容許缺少資源的時間
- 識別核心業務面臨的威脅與弱點
- 計算不同業務功能的風險
- 確認業務功能與資源復原的先後順序

(3) 識別防禦性控制措施

- ◆ **目的：**在此階段，依據營運衝擊分析的結果，識別並實施一系列預防性措施，以降低中斷事件發生的可能性或減輕其潛在影響。這些措施可能包括：系統冗餘、資料備份、安全措施（如防火牆、入侵偵測系統）、供應商管理、人員培訓等。

(4) 發展復原策略

- ◆ **目的：**針對那些無法被預防的潛在中斷，制定詳細的恢復策略。這包括選擇合適的技術解決方案（如異地備援中心、雲端備份與恢復）、定義恢復團隊的職責、確定供應商的支援等。復原策略應與 RTO 及 RPO 目標一致。

(5) 發展營運持續計畫 (BCP)

- ◆ **目的：**將前面步驟中確立的策略、分析結果、控制措施及復原策略，具體化為一份正式、詳細的文件。這份計畫書應包含緊急聯絡資訊、應變流程、角色職責、恢復步驟、溝通計畫等，是實際執行業務持續運作的藍圖。

(6) 測試與演練

- ◆ **目的：**定期對營運持續計畫進行測試及演練是至關重要的。這能驗證計畫的可行性、有效性及效率，並發現潛在的弱點或不足之處。演練可以是桌面演練、模擬演練或全面演練，以確保團隊成員熟悉應變流程。

(7) 維護營運持續計畫 (BCP)

- ◆ **目的：**業務環境、技術及組織結構都會不斷變化。因此，營運持續計畫不是一次性的文件，而是一個需要持續維護及更新的「活文件」。定期審查、更新、並依據測試結果、業務變動或新風險進行調整，以確保其始終符合組織的需求。

營運持續計畫的實施需要投入大量的資源（時間、金錢、人力）。如果沒有高階管理層的充分理解、承諾及支持，計畫很難獲得必要的資源，也無法有效推動各部門的配合，最終可能流於形式，難以成功。



多人誤以為業務持續性是 IT 部門的責任，因通常涉及到技術系統的恢復。然而，業務持續運作的核心是保護業務功能的連續性，這涉及到人力資源、財務、法務、供應鏈管理等所有核心業務部門。資訊部門負責的是 IT 系統的恢復（這是災難恢復，是業務持續性的一部分），但業務部門必須主導識別其關鍵流程、評估其衝擊，並參與恢復策略的制定，因為他們最了解自己的業務運作。這是一個跨部門的協作努力。

4.5.5 業務持續運作演練

業務持續運作 (Business Continuity) 演練的目的、實務操作要求，以及情境設計的考量，這對於驗證及強化營運持續計畫 (BCP) 的有效性至關重要。

(1) 演練目的

演練的目的是為了改進，故組織應依據演練中發現的問題及學習到的經驗，將對應的程序文件及 BCP 進行「滾動式調整」（即持續、動態地更新及改進）。調整後的計畫也需提報資安長。這體現了「計畫 - 執行 - 檢查 - 行動 (PDCA)」的管理循環精神。

◆ 檢驗 BCP 的可行性並補強未考量之缺陷

- **說明：**這是演練最主要的目的。撰寫好的 BCP 只是理論上的藍圖，實際操作中可能存在許多未預料到的問題或流程上的缺陷。透過演練，可以實際模擬中斷情境，測試 BCP 的應變步驟、恢復程序及團隊協作是否可行，並找出文件上或實際操作中可能存在的不足之處，從而加以改進。

◆ 確保在可容許中斷時間內可完成復原作業

- **說明：**演練的另一個重要目的是驗證組織是否能在設定的「復原時間目標 (RTO)」內，成功恢復關鍵業務功能。這包括測試備援系統的啟動速度、資料的恢復效率，以及各部門之間的協調，是否能達到預期目標。

◆ 使相關人員熟悉相關災害復原的作業

- **說明：**人員的熟悉度及應變能力是成功的關鍵。透過定期演練，可以使參與者熟悉各自在災害應原中的角色及職責、了解復原流程、熟練操作相關設備或系統，從而提高在真正中斷發生時的應變效率及信心。

(2) 演練實務

◆ 對全部核心資通系統訂定營運持續計畫，定期辦理業務持續運作演練：

- **說明：**這強調了演練的範圍及頻率。所有被認定為「核心」的資訊與通訊系統，都必須有對應的營運持續計畫 (BCP)，並且必須定期進行演練。
- A 級機關每年至少演練過 1 次；B 級、C 機關每 2 年至少演練過 1 次。

◆ 演練情境要求：這部分提出了設計演練情境時需要考慮的要素，以確保演練的有效性與真實性：

- 演練情境是否納入業務單位角色，演練結果與持續營運目標之符合性，亦應經業務單位確認，以確保業務持續運作演練之有效性，並應提報資安長。
- 是否依演練結果滾動調整相關程序及業務持續運作計畫、並提報資安長。
- 建議評估是否需納入複合式演練情境。
- **說明：**鼓勵組織考慮設計更複雜、更貼近現實的演練情境。單一故障的情境可能不足以應對現實中的複雜挑戰。複合式情境可能包括：
 - 多種災害同時發生（例如，地震導致電力中斷，同時網路也受損）。
 - 供應商服務中斷。
 - 人員短缺或無法到達工作地點。
 - 網路攻擊與實體災害結合，採用複合式情境可以更全面地測試組織的應變能力及 BCP 的韌性。

◆ 演練時間要求：這部分提供了在進行演練及設定相關時間目標時的具體指導原則：

- 是否至少針對核心業務訂定最大可容忍中斷時間 (MTPD)，並至少針對防護要求為中等級以上之資通系統，訂定從中斷後至重新恢復服務之可容忍時間要求 (RTO)？
- 核心資通系統之 RTO 亦不宜大於非核心資通系統之 RTO：
核心系統的 RTO 應該更短，或至少不應該比非核心系統的 RTO 長。換句話說，優先級高的系統，其恢復速度要求應該更高。如果核心系統的 RTO 大於非核心系統，這在邏輯上是不合理的，因為資源分配和恢復順序通常會優先保障核心系統。



- MTPD (最大可容忍中斷時間) = RTO + WRT :
此提供了一個計算 MTPD 的公式，將其分解為兩個部分：
 - RTO (Recovery Time Objective)：這是從中斷發生到系統恢復到「最低運作狀態」的時間。
 - WRT (Work Recovery Time / Workaround Recovery Time / Workflow Recovery Time)：工作復原時間。這是指在系統恢復到最低運作狀態後，到「完全恢復正常運作」所需的時間，或者是在系統恢復的同時，業務人員進行資料修復、人工操作或其他工作，以處理中斷期間累積的業務量所需的時間，可能包括人工資料輸入、業務流程的重新啟動、積壓工作的處理等。
- 確認設定之合理性，RTO 不可大於 MTPD。
 - 這提醒組織在定義 RTO 時，要明確其範圍。有些組織的 RTO 可能僅指 IT 系統的恢復，而不包含業務資料的恢復或業務流程的重啟。這個要求是確保 RTO 與 MTPD 保持合理的邏輯關係。最重要的是，RTO **絕不能**超過 MTPD，否則業務在技術恢復前，就已經遭受了無法承受的損失。
- 確認備份週期不可大於 RPO。
 - 再次強調了 RPO 與備份頻率的直接關係。為了確保資料損失在可容忍範圍內，備份的頻率（週期）必須等於或小於所設定的 RPO。例如，如 RPO 是 1 小時，則備份至少每小時進行一次，才能保證最多損失 1 小時的數據。

4.6

管理面—
資通安全治理成熟度

資通安全治理成熟度評估是組織衡量自身資通安全管理水平的重要工具，旨在提供一個客觀的視角，幫助組織識別其資通安全治理的強項與弱項，並規劃提升路徑，從而達到更全面、更有效的資通安全防護。

資通安全治理成熟度評估通常僅適用於公務機關，且不同等級的機關有不同的評估頻率，如表 23 管理面 - 資通安全成熟度評估規定，A 級及 B 級每年應辦理一次，C 級、D 級及 E 級則無要求。

表 23 管理面 - 資通安全成熟度評估規定

資通安全責任等級		辦理 資安治理成熟度評估 次數
公務機關	特定非公務機關	
A 級、B 級		每年應辦理 1 次
C 級、D 級、E 級		無要求

4.6.1 資安治理與資安管理之關係

資安治理與資安管理是兩個相互關聯但層次不同的概念，如圖 18 資安治理與資安管理之關係圖，以下說明兩者之關係。

(1) 資安治理：

負責高層決策，確立資安方向及目標。其權責範圍包括機關首長、資通安全長、資通安全治理推動小組。從「組織需求」出發，透過「評估」後，對資通安全管理產生「指導」及「監視」作用。

(2) 資安管理

負責具體執行，將治理層的目標轉化為實際行動。其權責範圍包括資通安全長、資通安全治理推動小組、使用者，包含「規劃」（調整、規劃及組織）、

「建立」（建立、獲得及建置）、「執行」（交付、服務及支持）、「監督」（監督、評估及評估）4 個主要階段，並由「管理回饋」送回治理層進行「評估」。

圖 17 清晰地展示了資安治理與資安管理之間的層級關係，強調資安治理為資安管理確立方向及目標，而資安管理則負責具體落實這些目標。兩者相輔相成，共同推動組織的資安發展。

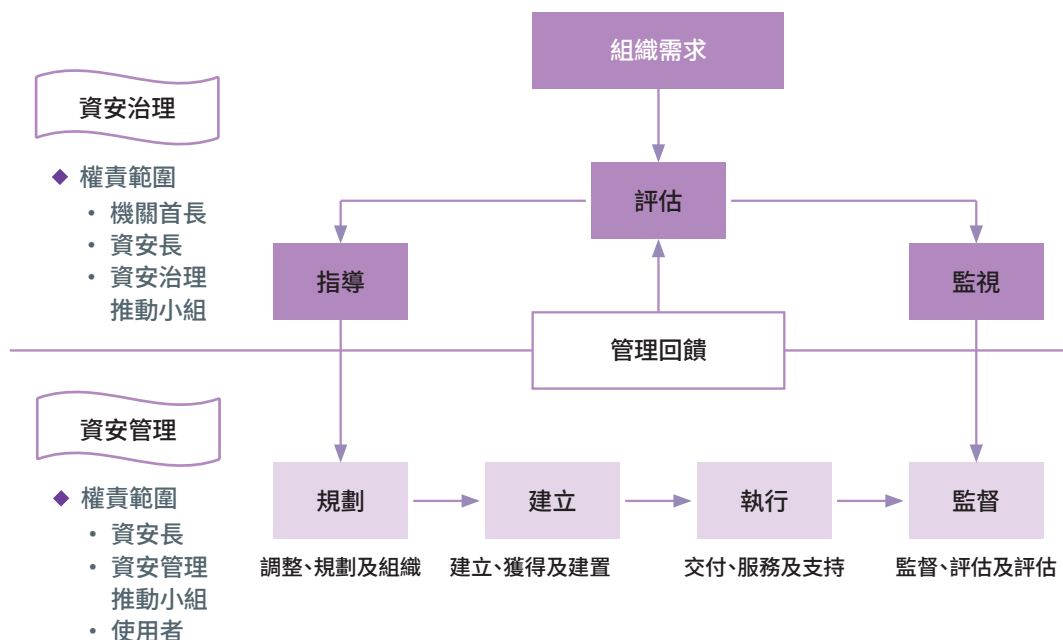


圖 18 資安治理與資安管理之關係圖

4.6.2 資安治理架構

資安治理架構可以分為策略面、管理面及技術面三個面向，這些面向與相關法規緊密關聯，共同構建了完善的資通安全治理體系，如圖 19 資安治理架構與相關法規之關聯圖。

圖 19 以金字塔圖示呈現了資安治理架構的策略面 (S)、管理面 (M) 及技術面 (T) 三個面向，並列出了其對應的流程構面及相關法規。

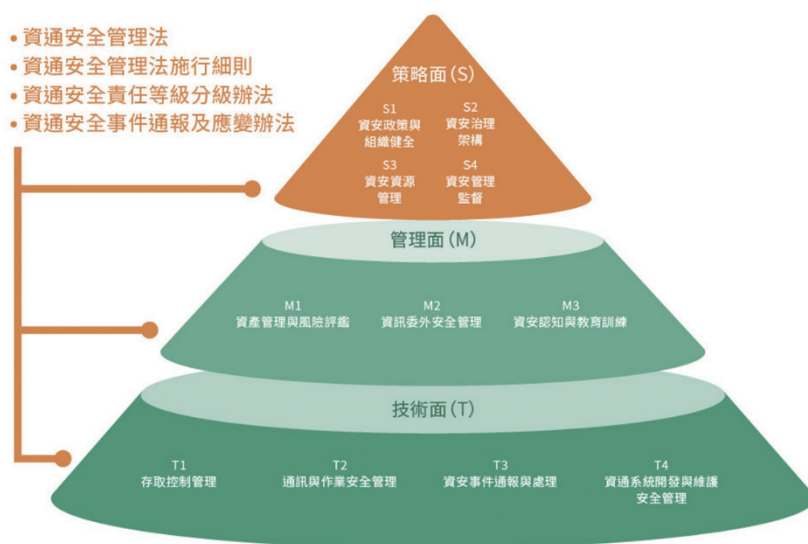


圖 19 資安治理架構與相關法規之關聯圖

4.6.3 資安治理之流程構面與目標

資安治理不僅有架構面向，更有其流程構面與具體目標。以下的說明將前面的資安治理架構面向（策略、管理、技術）與資安治理的流程構面及其目標範圍進行對應，以釐清各流程構面在不同層次下的具體目標，如表 24 資安治理之流程構面與目標。

表 24 資安治理之流程構面與目標

面向	流程構面	目標範圍	
策略	S1 資安政策與組織健全	- 資安政策建立 - 資安組織與管理審查	資安相關法規遵循
	S2 資安治理架構	資安新興議題評估	利害關係人溝通
	S3 資安資源管理	資安資源確保	資安專職人員配置
	S4 資安管理監督	績效與成果監督	業務持續運作管理



面向	流程構面	目標範圍	
管理	M1 資產管理與風險評鑑	- 資安風險管理	- 資通系統分級與防護
	M2 資訊委外安全管理	- 委外廠商資安專業能力 - 委外廠商資安管理	- 委外資安稽核
	M3 資安認知與教育訓練	- 資安認知與教育訓練	
技術	T1 存取控制管理	- 網路安全管理 - 權限管理	- 加密管理
	T2 通訊與作業安全管理	- 惡意軟體管理 - 遠距工作管理 - 電子郵件安全 - 實體環境控制措施 - 資料備份	- 儲存媒體處置 - 資通安全監控 - 資通安全防護 - 安全性檢測
	T3 資安事件通報與處理	- 資安事件通報應變 - 日誌紀錄保存 - 政府資安警訊	- 政府領域資安聯防情資 - 資安事件通報逾時
	T4 資通系統開發與維護安全管理	- 安全系統發展生命週期 (SSDLC) 落實	

(1) 策略面：

負責制定資安政策與組織架構，規劃治理方向，確保資源與監督機制。包括 S1 資安政策與組織健全、S2 資安治理架構、S3 資安資源管理、S4 資安管理監督等。

(2) 管理面：

負責落實資產與風險管理，強化委外安全，推動資安教育訓練。包括 M1 資產管理與風險評鑑、M2 資訊委外安全管理、M3 資安認知與教育訓練等。

(3) 技術面：

負責建立技術防護措施，完善通報與日誌管理，確保系統開發與維護安全。

包括 T1 存取控制管理、T2 通訊與作業安全管理、T3 資安事件通報與處理、T4 資通系統開發與維護安全管理等。

4.6.4 能力度之等級及定義

能力度之等級及定義，是依據 ISO/IEC 33020：2015 標準來衡量及評估組織在處理特定事項上的能力水平，將能力等級分為六個層次，從 Level 0 到 Level 5，每個等級都有其定義、要求，以及累進的條件，如表 25 能力度之等級及定義。以下說明每個能力度之等級及定義。

表 25 能力度之等級及定義

能力度等級	能力度定義	累進要求
Level 5 最佳化流程 (Optimizing Process)	基於過去執行成效分析或其他創新方式強化與優化該流程	需滿足 Level 1~4
Level 4 可預測流程 (Predictable Process)	- 該流程可透過衡量結果了解 - 執行成效 - 該流程已被量化管理	需滿足 Level 1~3
Level 3 標準化流程 (Established Process)	- 該流程已被標準化 - 該流程已被有效地部署	需滿足 Level 1~2 範圍擴大或深化應辦事項要求
Level 2 已管理流程 (Managed Process)	- 該流程執行過程已被管理 - 該流程產出已被管理	需滿足 Level 1 符合應辦事項要求
Level 1 已執行流程 (Performed Process)	該流程之執行結果已達預先設定	-
Level 0 未執行流程 (unperformed Process)	組織未建立該流程或無法達成該流程	-

(1) Level 0 未執行流程 (Unperformed Process)

- ◆ **能力度定義：**組織尚未建立該流程，或無法達成該流程。
- ◆ **說明：**這是最低的等級，表示組織完全沒有相關的流程，或者即使有流



程也無法有效執行。

(2) Level 1 已執行流程 (Performed Process)

- ◆ **能力度定義：**該流程之執行結果已達預先設定。
- ◆ **說明：**組織已經有該流程，並且能夠按照預期完成任務，達到設定的目標。

(3) Level 2 已管理流程 (Managed Process)

- ◆ **能力度定義：**
 - 該流程執行過程已被管理。
 - 該流程產出已被管理。
 - **累進要求：**需滿足 Level 1。
- ◆ **說明：**不僅能夠執行流程，而且執行的過程及產出的結果都被有效監控及管理，以確保流程的穩定性及可靠性。旁邊的方塊提到「符合應辦事項要求」，表示達到此等級需符合應辦事項要求。

(4) Level 3 標準化流程 (Established Process)

- ◆ **能力度定義：**
 - 該流程已被標準化。
 - 該流程已被有效部署。
 - **累進要求：**需滿足 Level 1~2。
- ◆ **說明：**流程已經標準化並形成正式文件，且這些標準化的流程已經在組織中被廣泛且有效地實施及應用。旁邊的方塊提到「範圍擴大或深化應辦事項要求」，表示達到此等級後，組織在相關應辦事項上的處理能力，可以應用到更廣泛或更深入的範圍。

(5) Level 4 可預測流程 (Predictable Process)

- ◆ **能力度定義：**
 - 該流程可透過衡量結果了解執行成效。
 - 該流程已被量化管理。
 - **累進要求：**需滿足 Level 1~3。
- ◆ **說明：**流程不僅標準化，而且透過量化數據及指標來衡量其執行成效。這表示組織能夠預測流程的結果，並基於數據進行管理及改進。

(6) Level 5 最佳化流程 (Optimizing Process)

- ◆ **能力度定義：**基於過去執行成效分析或其他創新方式強化與優化該流程。
 - **累進要求：**需滿足 Level 1~4。

- ◆ **說明：**這是最高的等級，表示組織能夠持續地分析流程的執行成效，並主動尋找創新方法來優化及改進流程，以達到最高的效率及效能。這是一個持續學習及改進的循環。

表 25 提供了一個評估組織流程能力度的框架，從最基礎的「沒有流程」到最高層次的「持續優化流程」，幫助組織識別其當前能力水平，並指引其如何逐步提升以符合更高標準的要求。

4.6.5 成熟度之等級及定義

成熟度 (Maturity) 之等級及定義，是依據 ISO/IEC 33004：2015 標準來評估組織資安治理的成熟度。這是一個用來衡量組織在特定領域（在這裡是資安治理）的流程及實踐達到何種程度的框架，將成熟度分為 6 個等級，從 Level 0 到 Level 5。如表 26 成熟度之等級及定義。以下說明每個成熟度之等級及定義。

表 26 成熟度之等級及定義

成熟度等級	成熟度定義	累進要求
Level 5 創新型 (Innovating)	透過 識別創新應用、技術、新機會 或潛在風險優化各流程構面	Level 1 至 Level 5 之流程構面皆達能力度等級 5
Level 4 可預測型 (Predictable)	依組織目標定義流程量化指標，建立 穩定、可預測之流程 ，蒐集與分析歷史數據，持續改善	Level 1 至 Level 4 之流程構面皆達能力度等級 4
Level 3 制度化型 (Established)	有效 定義與部署標準化流程 ，使其成為常規作業	Level 1 至 Level 3 之流程構面皆達能力度等級 3
Level 2 管理型 (Managed)	相關 流程構面已進行管理 ，包含規劃、執行及監督之過程	Level 1 至 Level 2 之流程構面皆達能力度等級 2
Level 1 基礎型 (Basic)	相關 流程構面執行結果已達成預先設定 ，且可支持組織之業務	Level 1 之流程構面皆達能力度等級 1
Level 0 未成熟型 (Immature)	係指組織尚未有效執行相關之基本流程	Level 1 之任一流程構面能力度為 0



(1) Level 0 未成熟型 (Immature)

- ◆ **成熟度定義：**係指組織尚未有效執行相關之基本流程。
 - **累積要求：**Level 1 之任一流程構面能力度為 0。
- ◆ **說明：**這是最低的成熟度等級，表示組織在資安治理方面缺乏基本流程或無法有效執行。

(2) Level 1 基礎型 (Basic)

- ◆ **成熟度定義：**相關流程構面執行結果已達成預先設定，且可支持組織之業務。
 - **累積要求：**Level 1 之流程構面皆達能力度等級 1。
- ◆ **說明：**組織已經有基本的資安治理流程，且這些流程的執行能夠達到預設的目標，並對組織的業務運作提供支持。這表示資安措施已經到位，並能發揮基本作用。

(3) Level 2 管理型 (Managed)

- ◆ **成熟度定義：**相關流程構面已進行管理，包含規劃、執行及監督之過程。
 - **累積要求：**Level 1 至 Level 2 之流程構面皆達能力度等級 2。
- ◆ **說明：**組織不僅有流程，而且這些資安治理流程已經被有效管理，包括詳細的規劃、實際的執行，以及對執行過程的監督。這表示資安活動不再是隨機的，而是有系統地進行。

(4) Level 3 制度化型 (Established)

- ◆ **成熟度定義：**有效定義與部署標準化流程，使其成為常規作業。
 - **累積要求：**Level 1 至 Level 3 之流程構面皆達能力度等級 3。
- ◆ **說明：**資安治理的流程已經被明確定義並標準化，形成組織的常規作業及規範。這些標準化的流程被廣泛部署及遵循，確保資安實踐的一致性及可靠性。

(5) Level 4 可預測型 (Predictable)

- ◆ **成熟度定義：**依組織目標定義流程量化指標，建立穩定、可預測之流程，蒐集與分析歷史數據，持續改善。
 - **累積要求：**Level 1 至 Level 4 之流程構面皆達能力度等級 4。
- ◆ **說明：**在此等級，資安治理流程已經可以被量化衡量。組織會定義具體的績效指標，並透過收集及分析歷史數據，來了解流程的執行情況，使其具有穩定性及可預測性，並在此基礎上進行持續改進。

(6) Level 5 創新型 (Innovating)

- ◆ **成熟度定義：**透過識別創新應用、技術、新機會或潛在風險優化各流程構面。
- **累積要求：**Level 1 至 Level 5 之流程構面皆達能力度等級 5。
- ◆ **說明：**這是最高的成熟度等級。組織不僅擁有高度可預測的資安治理流程，而且能夠主動識別並採用新的技術、創新的方法或利用新的機會，來進一步優化及提升資安治理能力，並主動應對潛在的風險。這是一個不斷創新及卓越的狀態。

表 26 提供了一個衡量組織在資安治理方面成熟度的路線圖。其可幫助組織評估當前的資安治理水平，並指引其如何逐步提升，從基本的資安實踐到能夠持續創新及優化的策略性資安治理。每個成熟度等級都建立在前一個等級的基礎之上，並且需要相應的流程構面達到特定的能力度等級。

4.6.6 成熟度等級與流程構面之對應關係

接著說明流程構面分級原則的成熟度等級與流程構面之對應關係，流程構面分級原則包括「基礎流程」及「擴展流程」兩大流程，將說明此兩大流程之各級成熟度所需流程構面的資安治理能力，如表 27 成熟度等級與流程構面之對應關係。

(1) 成熟度等級與流程構面之對應關係：

- ◆ **成熟度等級：**每個成熟度等級對應到特定的資安治理流程構面。以數字 (1~5) 表示資安治理的成熟度，數字越高表示成熟度越高。表 26 列出了從 Level 1 到 Level 5 的成熟度等級。
- ◆ **流程構面名稱：**各流程構面有專屬名稱，如 S1 資安政策與組織健全、M1 資產管理與風險評鑑等。每個成熟度等級下，都說明了相應的資安治理流程構面，這些流程構面以代碼（如 S1, M1, T1）及名稱（如資安政策與組織健全、資產管理與風險評估等）表示。這些代碼通常代表了特定的資安領域或功能模組（例如，S (Strategy) 代表策略面，M (Management) 代表管理面，T (Technical) 代表技術面。

(2) 成熟度等級說明：

- ◆ **成熟度等級 1：**
 - **S1 資安政策與組織健全：**這是資安治理的基石，建立明確的政策及健



全的組織結構是任何資安工作的起點。

- **M3 資安認知與教育訓練：**提升員工的資安意識及能力，這是最基本的防禦線。
- **T2 通訊與作業安全管理：**確保日常通訊及運營活動的安全。
- **說明：**這表示組織要達到基礎型 (Level 1) 的資安治理成熟度，必須先在這些核心流程構面上達到一定的能力。
- ◆ **成熟度等級 2：**
 - **M1 資產管理與風險評估：**識別並管理資訊資產，評估其面臨的風險，是制定有效防禦策略的基礎。
 - **M2 資訊委外安全管理：**管理與外部廠商合作時的資安風險，這在現代 y 組織中非常普遍。
 - **T1 存取控制管理：**確保只有授權人員才能存取敏感資訊和系統。
 - **說明：**在 Level 1 的基礎上，達到 Level 2 管理型的成熟度，需要更進一步在資產、風險、委外及存取控制等方面，實施有效的管理。
- ◆ **成熟度等級 3：**
 - **S3 資安資源管理：**有效規劃及分配資安相關的資源（人力、預算、技術等）。
 - **T3 資安事件通報與處理：**建立完善的事件應對機制，能及時應變及處理資安事件。
 - **T4 資通系統開發與維護安全管理：**將資安納入系統開發的整個生命週期，確保系統本身的安全性。
 - **說明：**從 Level 3 開始，進入「擴展流程」，意味著資安治理涵蓋的範圍更廣，更強調系統性的建設及應變能力。
- ◆ **成熟度等級 4：**
 - **S4 資安監督：**對資安實踐進行持續的監控及審查，確保其符合政策及法規要求。
 - **說明：**達到 Level 4 可預測型，組織需要對資安資源進行更精細的管理及持續的監督，以確保資安績效的可預測性。
- ◆ **成熟度等級 5：**
 - **S2 資安治理架構：**這是最高層次的流程構面，強調建立一個整合且持續優化的資安治理框架。
 - **說明：**達到 Level 5 創新型，組織需要將資安治理提升到戰略層面，實

現全面的整合與持續創新優化。

表 27 為組織呈現了一幅清晰的資安治理成熟度路線圖，將資安治理的複雜性拆解為一系列可管理的流程構面，並巧妙地將這些構面與不同的成熟度等級進行對應，進而有效指引組織，使其能從最基本的資安實踐開始，逐步提升並建構具備規劃性的資安能力。

表 27 成熟度等級與流程構面之對應關係

成熟度等級	流程構面名稱
5	S2 資安治理架構
4	S4 資安管理監督
3	S3 資安資源管理
	T3 資安事件通報與處理
	T4 資通系統開發與維護安全管理
2	M1 資產管理與風險評鑑
	M2 資訊委外安全管理
	T1 存取控制管理
1	S1 資安政策與組織健全
	M3 資安認知與教育訓練
	T2 通訊與作業安全管理

4.6.7 資安治理成熟度等級之計算範例

依據前面所提的流程構面分級原則、成熟度等級及流程構面之能力度等級，再利用資安治理成熟度評估系統之檢核項目，就可以計算出機關整體的成熟度，如表 26 資安治理成熟度等級之計算範例，這個範例是基於 ISO/IEC 33004：2015 標準的成熟度模型。表 28 展示了如何依據各流程構面的「能力度等級」來判斷組織的整體「成熟度等級」。



表 28 資安治理成熟度等級之計算範例

成熟度等級	流程構面名稱	檢核項目題號範圍	流程構面能力度等級	機關整體成熟度
5	S2 資安治理架構	第 4 ~ 6 題	1	Level 2 成熟度等級 1 至等級 3 對應之流程構面（S1、M3、T2、M1、M2、T1、S3、T3 及 T4），其能力度等級未全數達能力度 3（含）以上，故成熟度等級未達 Level 3。 ↑ 成熟度等級 1 至等級 2 對應之流程構面（S1、M3、T2、M1、M2 及 T1），其能力度等級皆達能力度 2（含）以上，故成熟度等級滿足 Level 2。 ↑ 成熟度等級 1 對應之流程構面（S1、M3 及 T2），其能力度等級皆達能力度 1（含）以上，故成熟度等級滿足 Level 1。
4	S4 資安管理監督	第 9 ~ 11 題	2	
3	S3 資安資源管理	第 7 ~ 8 題	3	
	T3 資安事件通報與處理	第 40 ~ 47 題	2	
	T4 資通系統開發與維護安全管理	第 48 ~ 52 題	4	
2	M1 資產管理與風險評鑑	第 12 ~ 14 題	4	
	M2 資訊委外安全管理	第 15 ~ 17 題	3	
	T1 存取控制管理	第 22 ~ 24 題	4	
1	S1 資安政策與組織健全	第 1 ~ 3 題	4	
	M3 資安認知與教育訓練	第 18 ~ 21 題	4	
	T2 通訊與作業安全管理	第 28 ~ 39 題	3	

(3) 左側表格說明：

- ◆ **成熟度等級**：標示了每個流程構面所屬的成熟度等級 (Level 1 到 Level 5)。
- ◆ **流程構面名稱**：列出了具體的資安治理流程構面，例如「S2 資安治理架構」、「M1 資產管理與風險評估」等。
- ◆ **檢核項目題號範圍**：這列指出每個流程構面可能對應的具體評估題目範圍，1 表示實際評估會通過一系列問題來進行。
- ◆ **流程構面能力度等級**：這是此範例最關鍵的輸入數據，表示該組織在每個特定流程構面上的「能力度等級」評分（例如，S2 資安治理架構的能力度等級是 3，M1 資產管理與風險評估的能力度等級是 5）。

(4) 右側「機關整體成熟度」說明：

這部分是依據左側表格中各流程構面的能力度等級，來推導出組織的整體成熟度等級的說明，並從最低的成熟度等級開始判斷，逐級向上。

◆ 滿足 Level 1：

- 條件：成熟度等級 1 之流程構面 (S1、M3、T2) 的能力度等級皆需達到或超過 1。
- 範例結果：圖中顯示 S1 (5)、M3 (4)、T2 (4) 都大於等於 1。
- 判斷：「故成熟度等級滿足 Level 1」

◆ 滿足 Level 2：

- 條件：成熟度等級 1 至等級 2 之流程構面 (S1、M3、T2、M1、M2、T1) 的能力度等級皆需達到或超過 2。
- 範例結果：
 - Level 1 的 S1 (5)、M3 (4)、T2 (4) 都大於等於 2。
 - Level 2 的 M1 (5)、M2 (4)、T1 (3) 都大於等於 2。
- 判斷：「故成熟度等級滿足 Level 2」

◆ 未達 Level 3：

- 條件：成熟度等級 1 至等級 3 之流程構面 (S1、M3、T2、M1、M2、T1、S3、T3、T4) 的能力度等級皆需達到或超過 3。
- 範例結果：
 - Level 1 及 Level 2 的所有流程構面能力度等級 (S1(5)、M3(4)、T2(4)、M1(5)、M2(4)、T1(3)) 都大於等於 3。
 - 但是，Level 3 的流程構面：
 - S3（資安資源管理）能力度等級是 4（滿足 ≥ 3 ）。
 - T3（資安事件通報與處理）能力度等級是 2（不滿足 ≥ 3 ）。
 - T4（資通系統開發與維護安全管理）能力度等級是 4（滿足 ≥ 3 ）。
 - 因 T3 的能力度等級為 2，未能達到 Level 3 所要求的「所有流程構面能力度等級皆需達到或超過 3」的條件。
- 判斷：「因其能力度等級未能全數達到能力度 3（含）以上，故成熟度等級未達 Level 3。」

表 28 是示範如何計算組織資安治理整體成熟度的一個具體範例。這對於組織進行資安治理評估及改進非常有用，其指出了提升整體成熟度需要關注的薄弱環節。



4.6.8 資安治理評估推動方式



圖 20 資安治理評估推動方式

資安治理評估推動方式係採用多方參與的循環式流程，其核心目的在於協助機關持續提升資安治理成熟度。此流程主要涉及數位部資安署（含其上級或監督機關）、機關推動人員與機關自評人員等多個關鍵角色，如圖 18 資安治理評估推動方式，以下將逐步說明圖中所示的詳細流程。

(1) 前期準備與啟動（由數位部資安署主導）：

- ◆ **數位部資安署制定公務機關之防護能力目標：**
 - 數位部資安署為所有公務機關設定一個宏觀的、理想的資安防護能力目標。
- ◆ **數位部資安署制定機關自評表：**
 - 為了評估各機關是否達成防護能力目標，數位部資安署會編制一份標準化的自評表，供各機關使用。
- ◆ **機關自評人員執行自我評估：**
 - 機關內部的自評人員依據資安署提供的自評表，對本機關的資安治理現狀進行初步的自我評估。

(2) 資安治理評估與分析（由機關自評人員與資安治理評估工具共同完成）：

◆ 資安治理評估工具 & 資安治理自評資料庫：

- 執行自我評估後，相關數據會輸入到資安治理評估工具中，並存儲在自評資料庫裡。這個工具可能是用來處理數據、計算分數、生成報告的自動化系統。

◆ 檢視與提出自評結果報告：

- 機關自評人員透過工具整理及檢視自評結果，生成正式的自評報告。

◆ 分析自評結果及檢討成熟度提升比率：

- 機關的自評人員或相關負責人會進一步分析報告，特別關注資安治理成熟度的現況，以及相較於過去是否有提升。

(3) 改進與規劃（由機關資安治理推動人員主導）：

◆ 發展改善行動方案呈資安長 / 資安管理審查委員會：

- 依據自評分析結果，機關的資安治理推動人員會制定具體的改善行動方案。這些方案會提交給資安長或資安管理審查委員會審核，以獲得批准及資源支持。

(4) 監督與調整（由數位部資安署 / 上級或監督機關與機關共同參與）：

◆ 檢視與分析各級機關自評結果：

- 數位部資安署或上級監督機關會收集並檢視、分析所有或各級機關提交的自評結果。這可以讓資安署了解整體公務機關的資安治理狀況。

◆ 決定各流程構面最低能力等級：

- 基於整體評估結果、政策要求及風險考量，數位部資安署或上級機關會決定或調整各資安治理流程構面應達到的最低能力等級要求。這是一個基於整體環境及目標的決策。

◆ 調整資安治理推動重點與規劃：

- 依據新的能力等級要求及各機關的評估結果，數位部資安署 / 上級機關會調整其資安治理的推動重點與整體規劃，例如發布新的指導方針、資源分配策略等。

(5) 執行機關自評：

- ◆ 整個流程進入下一個循環，機關再次執行自評，以評估調整後的效果和新的要求。

圖 18 說明了一個持續改進的資安治理評估循環流程，實現了 PDCA (Plan-Do-Check-Act) 循環管理的思想，是提升組織資安治理成熟度的有效途徑。

4.7

認知與訓練— 資通安全教育訓練

資通安全防護的最終環節是「人」。無論技術與制度多麼完善，若人員缺乏資安意識與應對能力，仍可能成為資安鏈上最脆弱的一環。因此，持續的資安認知與訓練是組織資安防線的基礎。

依據資通安全責任等級的不同，各級機關在資安認知與訓練方面有不同的應辦事項，如表 29 資通安全認知與訓練之應辦事項，其詳列了資通安全教育訓練蓋資通安全專職人員、資通安全專職人員以外之資訊人員，以及一般使用者及主管之應辦理項目。

表 29 資通安全認知與訓練應辦事項

辦理項目		辦理內容	A 級 機關	B 級 機關	C 級 機關	D 級、 E 級機關
資通 安全 教育 訓練	資通安全 專職人員	每人每年至少接受 12 小時以上之資通安全專業課程訓練或資通安全職能訓練		V		無要求
	資通安全 專職人員 以外之資 訊人員	每人每 2 年至少接受 3 小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受 3 小時以上之資通安全通識教育訓練		V		無要求
	一般使用 者及主管	每人每年接受 3 小時以上之資通安全通識教育訓練		V		V



辦理項目	辦理內容	A 級機關	B 級機關	C 級機關	D 級、E 級機關
資通安全專業證照及職能訓練證書	初次受核定或等級變更後的 1 年內，至少 X 名資通安全專職人員需持有相關證照及證書各 1 張以上，並持續維持有效性	至少 4 名	至少 2 名	至少 1 名	無要求
	二、本辦法中華民國 100 年 8 月 23 日修正施行前已受核定者，應於修正施行後 1 年內符合規定。	V			無要求

備註：資通安全專業證照：指由主管機關認可之國內外發證機關（構）所核發之資通安全證照。

4.7.1 資通安全專職人員 (A, B, C 級機關要求)

- ◆ 每年至少 12 小時專業訓練。
- ◆ 重點：確保核心資安人員專業能力與新知持續更新。

4.7.2 資通安全人員以外之資通訊人員 (A, B, C 級機關要求)

- ◆ 每 2 年至少 3 小時專業訓練 + 每年 3 小時通識教育。
- ◆ 重點：提升 IT 開發 / 維運人員的資安技能與意識，防範系統面資安問題。

4.7.3 一般使用者及主管 (A, B, C, D 級機關要求)

- ◆ 每年至少 3 小時通識教育。
- ◆ 重點：強化全員資安意識，特別是防範社交工程、釣魚等常見威脅；主管需具備資安治理概念。

4.8

認知與訓練—資通安全專業 證照及職能訓練證書

4.8.1 資通安全專業證照及職能訓練證書 (A, B, C 級機關要求)

- ◆ 核定後 1 年內，A 級至少 4 名，B 級至少 2 名，C 級至少 1 名人員需持有相關證照及證書各 1 張以上，並持續維持有效性。
- ◆ **重點：**量化資安專業能力，鼓勵考取相關證照及證書。

4.8.2 專業證照及職能訓練證書

- ◆ **資通安全專業證照：**指由主管機關認可之國內外發證機關（構）所核發之資通安全證照。可參考資通安全署資安法規專區之資通安全專業證照清單 (<https://moda.gov.tw/ACS/laws/certificates/676>)。

資安訓練是持續性工作，從通識到專業，全面提升人員資安素養，是建構韌性資安防護網的關鍵。透過定期且針對性的訓練，組織能夠提高整體資安防護能力，降低人為失誤造成的資安風險。

MEMO

Handwriting practice lines consisting of 20 horizontal dashed lines.

單元

5

資通系統防護控制措施

在資通安全領域，有效防禦惡意攻擊，並確保資訊資產安全，需要一系列嚴謹且全面的防護控制措施。這些措施不僅涵蓋技術層面，亦須融入管理流程與人員操作規範，共同構築多層次的防禦體系。本單元將深入剖析資通系統的各種防護控制措施，從最基本的存取管理，到複雜的系統安全維護，為讀者提供實用的知識與實作指引。

本單元學習重點如下：

- 1** 了解「存取控制」的各類存取機制與原則，以限制未經授權的存取。
- 2** 掌握「事件日誌與可歸責性」的重要性，學習如何記錄、保護與利用日誌資訊。
- 3** 理解「營運持續計畫」的核心概念與實施策略，確保業務在災害中持續運作。
- 4** 學習「識別與鑑別」的技術與管理措施，以確認使用者身分。
- 5** 認識「系統與服務獲得」過程中，將安全考量融入系統發展生命週期的重要性。
- 6** 探索「系統與通訊保護」的各項加密與簽章技術，以確保資料傳輸與儲存安全。
- 7** 了解「系統與資訊完整性」的維護措施，包括漏洞修復與系統監控。
- 8** 掌握「媒體控管及可攜式設備」的安全管理，以防範資料外洩。



依資通安全責任等級機關應辦事項的第 1 個辦理項目規定，各機關必須建立資通系統分級及防護基準，其辦理內容如下：包括：「初次受核定或等級變更後之 1 年內，針對自行或委外開發之資通系統，依附表 9 完成資通系統分級，並完成附表 10 之控制措施；其後應每年至少檢視 1 次資通系統分級妥適性。」

這些資通系統的防護基準控制措施，具體內容列於表 30 資通系統防護基準之控制措施。此表主要針對資通系統訂定了詳細的防護基準，共包含七大構面，並詳列了每個構面應採取的具體措施內容。

表 30 資通系統防護基準之控制措施

構面	1. 存取控制	2. 事件日誌與可歸實性	3. 營運持續計畫	4. 識別與鑑別	5. 系統與服務獲得	6. 系統與通訊保護	7. 系統與資訊完整性
控制措施	帳號管理	記錄事件	系統備份	內部使用者之識別與鑑別	SSDLC 需求階段	傳輸之機密性與完整性	漏洞修復
	最小權限	日誌紀錄內容	系統備援	身分驗證管理	SSDLC 設計階段	資料儲存之安全	資通系統監控
	遠端存取	日誌儲存容量		鑑別資訊回饋	SSDLC 開發階段		軟體及資訊完整性
		日誌處理失效之回應		加密模組鑑別	SSDLC 測試階段		
		時戳及校時		非內部使用者之識別與鑑別	SSDLC 部署與維運階段		
		日誌資訊之保護			SSDLC 委外階段		
					獲得程序		
					系統文件		

本單元將針對高、中、普等級之資通系統，進一步說明其防護基準在不同的構面，其所對應的控制措施內容。

5.1

「存取控制」之安全控制措施

存取控制是資通安全防護的核心基礎，其主要目的在於限制與管理對系統資源的存取權限，確保僅有經過授權的人員才能夠接觸資料及資源，進而大幅降低資安風險。有效的存取控制機制，能強力遏止未經授權的資訊洩露、竄改或破壞等資安事件。

表 31 詳細列出不同防護等級的資通系統，在存取控制構面下，關於帳號管理、最小權限及遠端存取等面向的安全控制措施。

表 31 存取控制構面之安全控制措施

措施內容	高	中	普
帳號管理	1. 機關應定義各系統之詞童時間或可使用期限與資還系統之使用情況及條件。 2. 逾越機關所許可之間置時間或可使用期限時，系統應自動將使用者登出。 3. 應依機關規定之情況及條件，使用資通系統。 4. 監控資通系統帳號，如發現帳號這常使用時回報管理者。 5. 等級「中」之所有控制措施。	1. 已逾期之臨時或緊急帳號應刪除或禁用。 2. 瓷還系統閉室帳號應禁用。 3. 定期審核資通系統帳號之申譜、建立、修改、啟用、停用及刪除。 4. 等級「普」之所有控制措施。	建立帳號管理機制，包含帳號之申譜、建立、修改、啟用、停用及刪除之程序。
最小權限	採最小權限原則，僅允許使用者（或代表使用者行為之程序）依機關任務及業務功能，完成指派任務所需之授權存取。		無要求





措施內容	高	中	普
遠端存取	1. 遠端存取之來源應為已預先定義及管理的存取控制點 2. 等級「普」之所有控制措施		1. 對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化。 2. 使用者之權限檢查作業應於伺服器區議完成。 3. 應監控遠端存取機關內部網段或資通系統後臺之連線。 4. 應採用加密機制。

5.1.1 帳號管理

帳號管理是存取控制的重要環節，旨在確保所有帳號從建立到失效的整個生命週期都受到嚴格管控。

(1) 高中普等級：

建立帳號管理機制：應建立帳號的申請、建立、修改、啟用、停用及刪除等程序，確保所有操作皆有紀錄並符合規定。

(2) 高中等級：

- ◆ **臨時與緊急帳號管理：**針對臨時或緊急用途建立的帳號，應在逾期後立即刪除或禁用，以防被濫用。
- ◆ **閒置帳號管理：**閒置過久的資通系統帳號應被禁用，避免成為潛在的入侵點。
- ◆ **帳號定期審核：**應定期審核資通系統帳號的申請、建立、修改、啟用、停用及刪除情況，確保帳號使用的合法性與合規性。

(3) 高等級：

- ◆ **系統操作限制：**應明確定義各資通系統的閒置時間或可使用期限與資通系統的使用情況及條件，以防止長時間的閒置會話或不當使用。



- ◆ **帳號自動登出**：若使用者逾越機關所許可的閒置時間或可使用期限，系統應自動將使用者登出，減少未經授權存取的風險。
- ◆ **系統使用規定**：應依機關規定之情況及條件，規範資通系統的使用行為，確保所有使用者都清楚其資安責任。
- ◆ **系統帳號監控**：應持續監控資通系統帳號的異常使用行為，如發現帳號違常使用，應即時回報管理者進行處理。

5.1.2 最小權限（高中）

採最小權限原則是資訊安全管理中的核心概念之一，其目的是僅允許使用者（或代表使用者行為之程序）依機關任務及業務功能，完成指派任務所需之授權存取。

這能有效減少因權限過大導致的安全風險，例如內部威脅或外部攻擊者一旦入侵後所造成的損害。透過權限分級管理與定期審查機制，確保權限分配與使用符合業務需求，避免不必要的權限累積。

5.1.3 遠端存取

遠端存取管理是資通安全中不可或缺的一部分，確保使用者在遠端存取系統時，能夠在安全且受控的環境下進行操作，避免因未經授權的存取或資料傳輸過程中的漏洞而導致安全風險。

(1) 高中普等級：

- ◆ **遠端存取授權**：對於每一種允許的遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化，以確保遠端存取的合法性。
- ◆ **權限檢查實作**：使用者之權限檢查作業應於伺服器端完成，確保存取權限的有效性與即時性。
- ◆ **連線監控**：應監控遠端存取機關內部網段或資通系統後台之連線，及時發現異常行為。
- ◆ **連線加密**：應採用加密遠端存取，其來源應為機關已預先定義及管理的存取控制點機制，防止資料在傳輸過程中被監聽或竊取。

(2) 高中等級：

- ◆ **來源管制**：遠端存取之來源應為機關已預先定義及管理的存取控制點，以限制可連線至內部網路的外部來源。

5.1.4 存取控制之授權原則

存取控制中的授權原則是規範使用者如何被授予權限、以及被授予什麼權限的基礎。

- (1) **業務僅知原則 (Need-to-Know)**：只提供執行業務上所需知道的資訊。這確保了資訊只暴露給需要使用的人員，最小化資訊洩露的風險。
- (2) **最小權限原則 (Least Privilege)**：權限開放時採用最小權限原則。這與業務僅知原則相輔相成，限制使用者僅能執行其職責所需的最低操作，減少因權限過大而造成的損害。
- (3) **職務區隔 (Separation of Duties)**：避免某些衝突或監督工作職務由同一個人來進行。這可以防止單一人員濫用職權或串通舞弊，提高內部控制的安全性。
- (4) **特殊權限管理 (Privileged Access Management)**：對於系統管理者帳號及相關安全組態設定權限，應採特別的控管方式，並詳細記錄特權人員的存取行為。這是因為特權帳號擁有高度權限，一旦被濫用，可能造成重大損害，因此需要更嚴格的監控。

5.1.5 存取控制之類型

存取控制可以藉由以下不同的類型來控制：

- (1) **實體類控制 (Physical Controls)**：透過實體手段限制存取。例如：門、窗及圍牆（防止未經授權的進入）、鎖（保護設備及區域）、警衛（監控及應對實體威脅）。
- (2) **技術類控制 (Technical Controls)**：透過軟硬體技術管理存取。例如：通行碼鑑別（驗證使用者身分）、加解密技術（保護資料機密性）、生物特徵識別技術（利用個人生理特徵進行驗證）、防火牆系統（限制網路流量）。
- (3) **管理類控制 (Administrative Controls)**：透過政策與程序來規範存取行為。例如：政策與程序（提供操作指引）、安全認知訓練（提升人員資安意識）、風險管理（識別及處理存取相關風險）。

存取控制是一個多層次、多面向的資安防護環節。透過帳號管理、最小權限原則、遠端存取規範、明確的授權原則，以及不同類型的控制措施，組織能夠有效地限制對資通系統的未經授權存取，從而保護資訊資產的安全。

5.2

「事件日誌與可歸責性」之安全控制措施

事件日誌與可歸責性是資通安全中不可或缺的一環，其目的在於記錄及保存資通系統及網路活動的日誌，以便追蹤系統及使用者的操作行為。這不僅是事後分析及調查的依據，更是建立可歸責性、主動監控與符合法規要求的重要基礎。

表 32 詳細列出針對不同防護等級的資通系統，在事件日誌與可歸責性構面下，關於記錄事件、日誌記錄內容、日誌儲存容量、日誌處理失效之回應、時戳及校時、日誌資訊之保護等面向的安全控制措施。

表 32 事件日誌與可歸責性構面之安全控制措施

措施內容	高	中	普
記錄事件	1. 應定期審畜機關所保留資通系統產生之日誌 2. 等級「普」之所有控制措施		1. 訂定日誌之記錄時間週期及留存政策，並保留日誌至少六個月。 2. 確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事件。 3. 應記錄資通系統管理者帳號所執行之各項功能。
日誌記錄內容	資通系統產生之日誌應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，採用單一日誌機制，確保輸出格式之一致性，並應依資通安全政策及法規要求納入其他相關資訊。		
日誌儲存容量	依據日誌儲存需求，自己置所需之儲存容量。		

5.2.1 記錄事件

事件日誌記錄是追蹤系統與使用者行為的基礎，對於及早發現可疑活動並

進行追溯至關重要。日誌記錄的內容詳盡程度與儲存容量，直接影響日誌的分析價值與可用性。

(1) 高中普等級：

- ◆ **日誌留存：**應訂定日誌的記錄時間週期及留存政策，並確保日誌至少保留 6 個月，以提供足夠的歷史資料供後續分析。
- ◆ **保存項目：**應包含作業系統日誌 (OS event log)、網站日誌 (web log)、應用程式日誌 (AP log) 及登入日誌 (logon log) 等關鍵日誌。
- ◆ **事件記錄：**應確保資通系統有記錄特定事件的功能，並明確決定應記錄之特定資通系統事件。
- ◆ **觸發行為：**於特定系統事件發生時（例如異常登入、系統錯誤、檔案存取等）應觸發日誌記錄行為。
- ◆ **管理者行為記錄：**應記錄資通系統管理者帳號所執行的各項功能，這有助於追查資安事件或發現濫權行為。

(2) 高中等級：

- ◆ **日誌審查：**應定期審查機關所保留資通系統產生的日誌，以主動發現潛在的安全威脅、異常活動或配置錯誤，並檢視日誌記錄的完整性和有效性。

5.2.2 日誌記錄內容（高中普）

資通系統產生的日誌應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊。應採用單一日誌機制，確保輸出格式的一致性，並應依資通安全政策及法規要求納入其他相關資訊。詳盡且格式一致的日誌內容，對於理解事件的脈絡、評估其影響程度至關重要。

5.2.3 日誌儲存容量（高中普）

依據日誌儲存需求、保留政策以及法規要求，配置所需之儲存容量。充足的儲存空間能確保日誌資料得以長期保存，支援歷史趨勢分析及應對未來的安全事件。



5.2.4 日誌處理失效之回應

確保日誌系統的穩定運作至關重要。當日誌處理發生失效時，及時的回應能夠避免日誌記錄中斷，影響後續的分析及追蹤。

(1) 高中普等級：

- ◆ **回應行動：**資通系統於日誌處理失效時，應採取適當之行動。例如，對於高防護等級的系統，日誌處理失效可能意味著安全監控的中斷，因此需要及時通報相關人員進行處理。

(2) 高等級：

- ◆ **即時通報：**機關規定需要即時通報之日誌處理失效事件發生時，資通系統應於機關規定之時效內，對特定人員提出警告。

5.2.5 時戳及校時

精確的時間戳對於關聯不同資通系統的資安事件、進行時間序列分析，以及符合法規要求至關重要。

(1) 高中普等級：

- ◆ **時戳：**資通系統應使用系統內部時鐘產生日誌所需時戳，並可以對應到世界協調時間 (UTC) 或格林威治標準時間 (GMT)，以確保時間資訊的標準化與準確性。

(2) 高中等級：

- ◆ **校時：**系統內部時鐘應定期與基準時間源進行同步，避免因時間偏差導致的日誌分析錯誤。

5.2.6 日誌資訊之保護

保護日誌資訊的機密性及完整性，防止未經授權的存取、竄改或刪除，確保日誌的可用性及可信度，對於確保日誌的證據價值至關重要。

(1) 高中普等級：

- ◆ **存取控制：**對日誌之存取管理，僅限於有權限之使用者，限制對日誌的存取，防止未經授權的查看、修改或刪除。

(2) 高中等級：

- ◆ **完整性：**應運用雜湊或其他適當方式之完整性確保機制。

(3) 高等級：

- ◆ **定期備份：**定期備份日誌至原系統外之其他實體系統。

5.2.7 雜湊函式 (Hash)

雜湊函式是一種重要的密碼學工具，用於從任何長度的資料中，建立固定長度的「數位指紋」（訊息摘要）。雜湊 (Hash) 的概念及其在資訊安全中的應用，特別是與日誌完整性息息相關。

(1) 特性：

- ◆ **固定長度：**將任何長度的資料轉換成固定長度的訊息摘要。
- ◆ **抗碰撞性：**在計算上難以找到兩個不同輸入資料產生相同雜湊值。
- ◆ **單向性：**無法從雜湊值回推原始資料（單向），不具有可逆性。

(2) 應用：

- ◆ 雜湊常用來驗證資料完整性（透過比對原始資料的雜湊值與現有資料的雜湊值，判斷資料是否被竄改），
- ◆ 也可用來儲存使用者密碼（即使資料庫洩漏，攻擊者也難以直接取得原始密碼）。

(3) 演算法：

常見的雜湊演算法包括 MD5、SHA-256、SHA-512、SHA3-512 等。

圖 21 展示了雜湊函式將任意輸入轉換為固定長度雜湊值的過程，並說明了雜湊值比對在驗證資料完整性中的應用，說明如下：

- (1) 原始檔案經過 SHA-256 運算後得到雜湊值。
- (2) 現有檔案經過 SHA-256 運算後得到新雜湊值。
- (3) 比對兩個雜湊值是否相同，若相同則表示檔案內容極可能未變更，若不同則表示檔案內容已變更。
- (4) 雖然雜湊函數的設計旨在保證唯一性，但理論上及在被攻擊的情況下，仍然有機會生成不同內容的檔案但具有相同的雜湊值。這種情況被稱為雜湊碰撞 (Hash Collision)。攻擊者若能成功實施「碰撞攻擊」，就能創建一個具有相同雜湊值但內容不同的偽造檔案。不過，現代的加密雜湊演算法（如 SHA-256）具有極高的抗碰撞性，使得這種攻擊在計算上極度困難。

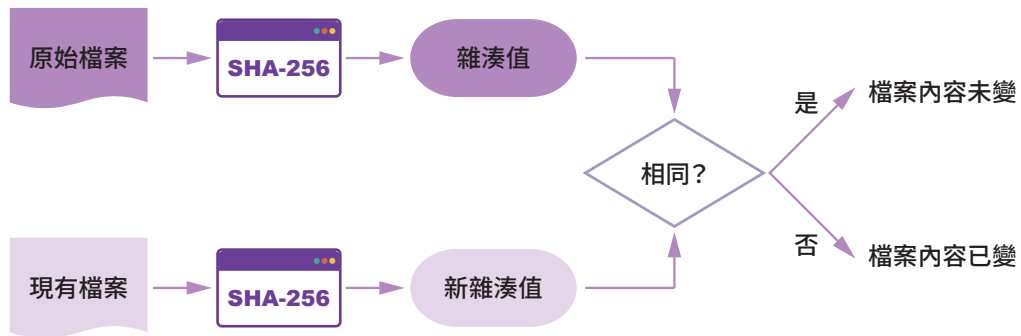


圖 21 雜湊函式運作示意圖

(5) 強化密碼安全：

- ◆ 雖然雜湊的單向性很強，但在儲存密碼的場景中，仍然需要一種稱為 Salt（鹽）的技術來進一步強化安全。
- ◆ Salt 是一個隨機、唯一的資料字串。在對密碼進行雜湊處理前，系統會將 Salt 與使用者的密碼結合 (concatenate)，然後再對結合後的字串進行雜湊，產生最終儲存的雜湊值。最終雜湊值 = Hash（密碼 + Salt）。
- ◆ Salt 主要用於抵禦兩種常見的攻擊方式：
 - 彩虹表攻擊 (Rainbow Table Attack)：彩虹表是一個預先計算好的雜湊值與密碼對應的表格：加入 Salt 後，即使兩個使用者的密碼都是“123456”，因為他們的 Salt 不同，所以計算出來的最終雜湊值也會完全不同。這使得彩虹表攻擊變得無效。
 - 碰撞攻擊 (Collision Attack)：即使有兩個使用者使用相同的密碼，因為 Salt 不同，它們儲存在資料庫中的雜湊值也會不同，這樣攻擊者就無法僅僅透過相同的雜湊值來識別出密碼相同的帳戶，進一步提高了安全性。

事件日誌與可歸責性是資安防禦的重要組成部分。透過完整的日誌記錄、嚴格的保護、精確的時戳，以及雜湊等技術的應用，組織能夠有效地追蹤、分析資安事件，確保可歸責性，並持續改進資安防護能力。

5.3

「營運持續計畫」之安全控制措施

營運持續計畫 (Business Continuity Plan, BCP) 之目的是在確保組織在突發事件或災難情況下，其關鍵業務能夠持續運作。這不僅涉及技術層面的備份與復原，更涵蓋了流程、人員與管理上的準備，以最大程度地降低服務中斷帶來的影響。

表 33 詳細列出針對不同防護等級的資通系統，在營運持續計畫構面下，關於系統備份及系統備援兩個面向的安全控制措施。

表 33 營運持續計畫構面之安全控制措施

措施內容	高	中	普
系統備份	- 應將備份還原，作為營運持續計畫測試之一部分。 - 應在與運作系統不同地點之獨立設施或防火櫃中，儲存重要資通系統軟體與其他安全相關資訊之備份。 - 等級「中」之所有控制措施	- 應定期測試備份資訊，以驗證備份媒體之可靠性及資訊之完整性。 - 等級「普」之所有控制措施	- 訂定系統可容忍資料損失之時間要求 - 執行系統源碼與資料備份
系統備援	- 訂定資通系統從中斷後至重新恢復服務之可容忍時間要求 - 原服務中斷時，於可容忍時間內，由備援設備或其他方式取代並提供服務		無要求

5.3.1 系統備份

系統備份是營運持續計畫的基石，旨在對抗資料毀損的威脅與抵抗勒索攻



擊，以保護資料的可用性。

(1) 高中普等級：

- ◆ **復原點目標**：訂定系統可容忍資料損失的時間要求。RPO 越短，表示組織需要越頻繁地備份。
- ◆ **定期測試**：應將備份還原作為營運持續計畫測試的一部分；應定期測試備份資料，以驗證備份媒體的可靠性及資訊的完整性。
- ◆ **系統源碼與資料備份**：應執行系統源碼與資料備份，這是系統恢復的基礎，涵蓋應用程式、資料庫、作業系統配置等關鍵組件。

(2) 高中等級：

- ◆ **測試備份媒體**：應定期測試備份資料，以驗證備份媒體的可靠性及資訊的完整性。僅有備份不足夠，還原能力同樣重要。

(3) 高等級：

- ◆ **還原測試**：應將備份還原，作為營運持續計畫測試的一部分。營運持續計畫 (BCP) 應定期演練，在災害復原過程中應使用備份資料驗證備份機制是否正確可靠。
- ◆ **異地備份**：應在與運作系統不同地點之獨立設施或防火櫃中，儲存重要資通系統軟體與其他安全相關資訊之備份，以應對本地災難。機關亦可參考「我國電腦機房異地備援機制參考指引」，異地備份 / 備援機制提及之主機房與異地備援機房距離應 30 公里以上。

5.3.2 系統備援

系統備援旨在確保在發生系統中斷時，業務能夠在可接受的時間內恢復正常運作。

(1) 高中等級：

- ◆ **復原時間目標 (RTO)**：訂定資通系統從中斷後至重新恢復服務之可容忍時間要求。
 - RTO 的設定直接影響組織恢復關鍵服務的速度。組織應依據業務連續性的需求，設定合理的 RTO。
 - 較低的 RTO 通常意味著需要投入更多的資源和更複雜的備援方案。

(2) 高中等級：

- ◆ **備援設備**：原服務中斷時，於可容忍時間內，由備援設備或其他方式取

代並提供服務。

- 為了在 RTO 內恢復服務，組織需要準備備援硬體、軟體或雲端資源。
- 訂定資通系統從中斷後至重新恢復服務之可容忍時間要求。

5.3.3 營運持續計畫之時間指標

圖 22 呈現了營運持續計畫在時間軸上，各關鍵時間指標 (RPO、RTO、WRT、MTPD) 間之關係，茲說明如下：

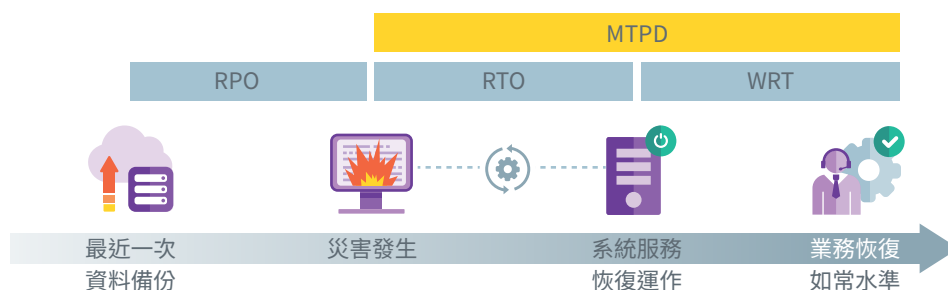


圖 22 營運持續計畫之時間指標圖

- (1) 最近一次資料備份：代表資料備份的時間點。
- (2) 災害發生：標示業務中斷的時刻。
- (3) 系統服務恢復運作：標示系統恢復並開始運作的時間點。
- (4) 業務恢復至正常水準：標示業務完全恢復正常運作的狀態。
- (5) 關鍵時間指標：

- ◆ **RPO**：指復原點目標，表示資通系統從中斷後至重新恢復服務之可容忍時間要求。從災害發生回溯至最近一次可用備份的時間長度，代表可容忍的資料損失量。
- ◆ **RTO**：指復原時間目標，表示資通系統從中斷後至重新恢復服務之可容忍時間要求。從災害發生到系統服務恢復運作的時間長度，代表可容忍的服務中斷時間。
- ◆ **WRT (Work Recovery Time)**：指工作復原時間，讓核心業務回到災害發生前的服務水準所需之時間，其中工作如復原資料、驗證系統及資料正確性等
- ◆ **MTPD (Maximum Tolerable Period of Disruption)**：指最大可容忍中

斷時間，為核心業務與其所需資源評估最大可容忍忍中斷之時間，應涵蓋 RTO 及 WRT。

5.3.4 資料備份

資料備份有多種方式及模式，可以依據組織的需求及資源進行選擇。

(1) **目的：**為對抗資料毀損的威脅與抵抗勒索攻擊，以保護資料的可用性。

- ◆ 個人使用者可為自己的重要資料進行備份。
- ◆ 機關應有系統人員對內部重要系統與檔案統一進行備份。
- ◆ 機關應建立備份資料復原程序。
- ◆ 備份媒介可為光碟、行動碟、其他電腦、磁帶與大型儲存系統。

(2) **備份方式：**

- ◆ **完整備份：**將要備份的檔案完整地複製一份保存在備份儲存媒體中。優點是恢復最完整，但耗時長且佔用空間大。
- ◆ **差異備份：**備份上次完整備份後，內容有變更或新增的檔案。速度比完整備份快，佔用空間較少，但還原時需要完整備份加上最近一次差異備份。
- ◆ **增量備份：**備份上次完整備份或增量備份後，內容有變更或新增的檔案。速度最快，佔用空間最少，但還原過程最複雜，需要依序套用所有相關增量備份。

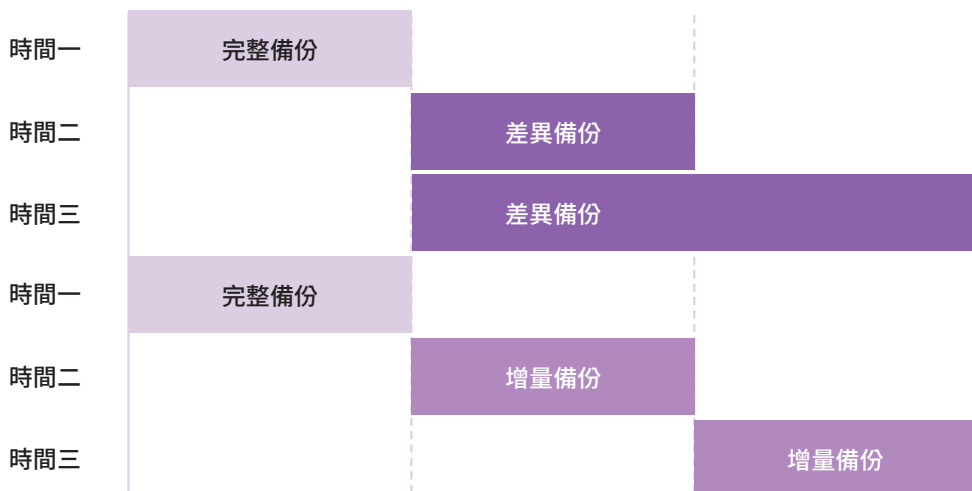


圖 23 完整備份、差異備份及增量備份示意圖

圖 23 以時間軸方式圖示了完整備份、差異備份及增量備份之執行時機及原理。

◆ 完整備份與差異備份範例

圖 24 假設星期一進行完整備份，星期二至星期五進行差異備份，若星期五時資料毀損，則需要復原星期一的完整備份與星期四的差異備份。

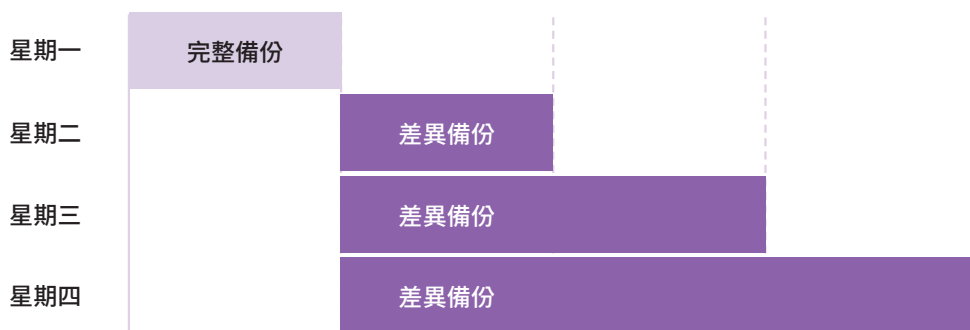


圖 24 完整備份與差異備份範例

◆ 完整備份與增量備份

圖 25 假設星期一進行完整備份，星期二至星期五進行增量備份，若星期五時資料毀損，則需要復原星期一的完整備份與從星期二至星期四的所有增量備份

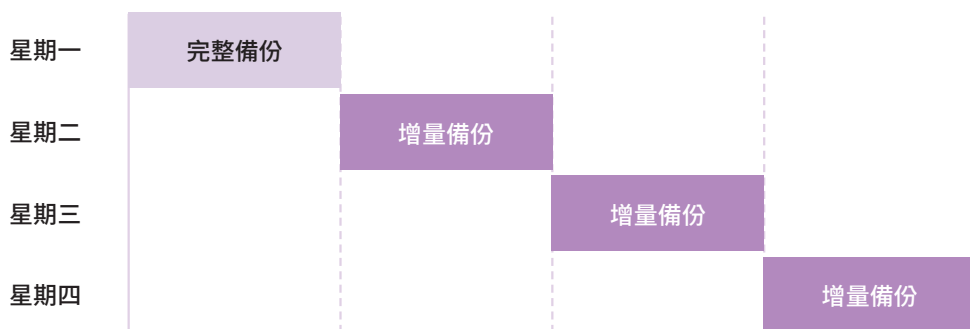


圖 25 完整備份與增量備份範例

(3) 備份模式：

- ◆ **本地備份：**將檔案儲存至備份媒體後，保存於原地點。
 - 如果使用的備份媒體存在於同一部電腦的硬碟中，雖然備份的程序最簡便，但是當電腦硬碟故障時，備份資料亦同時受損，則備份的效能

無法發揮。

- 如備份媒體使用光碟片，但保存於同一機房中，雖然可以避免前例硬碟故障的問題，但若機房發生火警時，則備份資料亦可能同時毀損。
- ◆ **異地備份**：將檔案儲存至備份媒體後，保存於不同地點。
 - 應考慮地震帶、颱風、土石流等因素，規避同時受災可能性。
 - 異地備份地點相距愈遠，其防護效果愈佳。
- ◆ **例如**：當地震發生時，相距 10 公里內的距離可能遭受同樣程度的毀損，但相隔 100 公里的距離則其毀損程度可能就大不相同。

(4) 備份週期

- ◆ 每日、每週、每月及每季。

(5) 回存測試

- ◆ 應確認備份的資料回復之後可正常運作。

(6) 資料備份 - 注意事項

在執行資料備份時，應注意下列事項，以確保備份策略的有效性。

- ◆ **備份範圍**：應事先評估備份的範圍，避免遺漏重要的資料。
- ◆ **備份媒體**：資訊設備變化快速，應定期檢驗備份媒體是否仍有合適的存取設備，確保其相容性。
- ◆ **檔案格式**：備份檔案的格式可能因年代久遠而找不到相容的工具。應定期檢查備份檔案，確認仍有合適的應用軟體或工具可開啟。
- ◆ **備份設施**：機關應提供足夠之備份設施，確保發生災害後可復原。
- ◆ **回復演練**：機關應進行備份資料的回復演練，以確保備份資料可以正確的回復。
- ◆ **回復測試**：測試備份資料回復時，應先於專屬媒體上執行，以防止復原過程失敗，造成資料毀損。相關計畫應列入營運持續計畫中辦理。

營運持續計畫及其核心的系統備份與備援，是組織韌性的關鍵。透過 RPO 與 RTO 的明確設定、多樣化的備份策略與定期的演練，組織能夠在面對突發事件時，最大程度地減少業務中斷，確保關鍵服務的連續性。

5.4

「識別與鑑別」之安全控制措施

識別與鑑別是資通安全防護的第一道關卡，其目的是在確保只有經過授權的使用者才能存取系統，從而保障資通系統的安全。這是一個多層次的概念，包括確認使用者身分（識別）及驗證其所聲稱的身分（鑑別）。

表 34 詳細列出針對不同防護等級的資通系統，在識別與鑑別構面下，關於內部使用者之識別與鑑別、身分驗證管理、鑑別資訊回饋、加密模組鑑別、非內部使用者之識別與鑑別等面向的安全制措施。

表 34 識別與鑑別構面之安全控制措施

措施內容	高	中	普
內部使用者之識別與鑑別	1. 對資通系統之存取採取多重認證技術。 2. 等級「中」及「普」之所有控制措施	資通系統應具備唯一識別及鑑別機關使用者（或代表機關使用者行為之程序）之功能，禁止使用共用帳號。	
身分驗證管理	1. 身分驗證機制應防範自動他程式之登入或密碼更換嘗試。 2. 密碼重設機制對使用者重新身分確認後，接送一次性及真有時效性符記。 3. 等級「普」之所有控制措施		1. 使用預設密碼登入系統時，應於登入後要求立即變更。 2. 身分驗證相關資訊不以明文傳輸。 3. 具備帳戶鎖定機制，帳號登入進行身分驗證失敗達五次後，至少十五分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。 4. 使用密碼進行驗證時，應強制最低密碼複雜度；強制密碼最短及最長之效期限制。



措施內容	高	中	普
身分驗證管理			5. 密碼變更時，至少不可以與前次使用過之密碼相同。 6. 第四點及第五點所定措施，對非內部使用者，可依機關自行規範辦理。
鑑別資訊回饋	資通系統應遮蔽鑑別過程中之資訊		
加密模組鑑別	資通系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存。		無要求
非內部使用者之識別與鑑別	資通系統應識別及鑑別非機關使用者（或代表機關使用者行為之程序）		

5.4.1 內部使用者之識別與鑑別

針對組織內部的使用者，識別與鑑別是確保安全存取的基礎。

(1) 高中普等級：

- ◆ **唯一識別及鑑別功能：**資通系統應具備唯一識別及鑑別機關使用者（或代表機關使用者行為之程序）的功能，禁止使用共用帳號。這有助於確保人員的可歸責性，追蹤其在系統中的操作行為。

(2) 高等級：

- ◆ **多因子鑑別技術：**對資通系統之存取採取多因子鑑別技術。MFA 結合兩種或以上的鑑別因素（例如：您知道什麼、您擁有什麼、您是什麼），顯著提高身分鑑別的強度，降低單一憑證洩漏或被破解導致的風險。

5.4.2 身分驗證管理

旨在確保使用者聲稱的身分真實可靠，防止冒用行為，並透過嚴格的密碼策略來提高安全性。

(1) 高中普等級：

- ◆ **變更預設密碼：**使用預設密碼登入系統時，應於登入後要求立即變更。預設密碼通常公開且容易猜測，強制變更為使用者自訂的強密碼是基本的安全措施。
- ◆ **禁止明文傳輸：**身分驗證相關資訊不以明文傳輸。敏感的身分驗證資訊，如密碼，在傳輸過程中必須經過加密保護，防止被攔截竊取。
- ◆ **帳戶鎖定：**具備帳戶鎖定機制，帳號登入進行身分驗證失敗達 5 次後，至少 15 分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。這能有效防禦暴力破解密碼的攻擊。
- ◆ **密碼複雜度與效期：**使用密碼進行驗證時，應強制最低密碼複雜度（包含文字、數字、符號、大小寫），並強制密碼最短及最長之效期限制，以提高密碼強度。
- ◆ **密碼歷程：**密碼變更時，至少不可以與前 3 次使用過之密碼相同。這可以防止使用者重複使用容易被猜測或已洩漏過的舊密碼，提升密碼變更的安全性。
- ◆ **對非內部使用者，可依機關自行規範辦理密碼複雜度與效期及密碼歷程。**

(2) 高中等級：

- ◆ **防範自動化程式：**身分驗證機制應防範自動化程式之登入或密碼更換嘗試。例如，實施全自動公開圖靈測試用於區分電腦與人類 (Completely Automated Public Turing test to tell Computers and Humans Apart, CAPTCHA) 之驗證碼或其他反自動化機制，以有效阻止惡意程式進行暴力破解密碼的嘗試。
- ◆ **密碼重設：**密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記，以防止未經授權的密碼重設。

5.4.3 鑑別資訊回饋（高中普）

資通系統應遮蔽鑑別過程中之資訊。在使用者輸入密碼時，應使用星號或其他符號遮蔽實際輸入，防止旁人窺視，降低密碼洩漏的風險。

5.4.4 加密模組鑑別（高中）

資通系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存。這確



保了密碼等敏感鑑別資訊在儲存時受到保護，降低洩漏風險。

5.4.5 非內部使用者之識別與鑑別（高中普）

針對非組織內部的使用者，識別與鑑別同樣重要，有助於控制外部存取，保護內部資源不被未經授權的外部人員存取，故資通系統應識別及鑑別非機關使用者（或代表機關使用者行為之程序）。

以下將進一步說明使用者的識別符及鑑別符。

5.4.6 使用者識別符 (Identifier)

本節將進一步探討使用者識別符的要求及管理，這對於建立可歸責性至關重要。

(1) 使用者識別符（名稱、代碼或帳號）的要求：

- ◆ 必須唯一，以確保人員的可歸責性，不能有多人共用帳號的情形。
 - 說明：每個使用者都應擁有唯一的識別符，以便追蹤其在系統中的操作行為，並確保責任歸屬清晰。
- ◆ 與使用者真實身分連結，在資通系統中代表使用者身分。
 - 說明：識別符應能對應到真實的使用者，方便管理和稽核。
- ◆ 發展命名格式並遵循（例如：Firstname_Lastname）。
 - 說明：一致的命名規則有助於管理及辨識使用者帳號。
- ◆ 不代表其在機關中的角色或職位。
 - 說明：識別符應基於使用者個體，而非其職責，以避免因職位變動而需要變更帳號。

(2) 使用者識別符的管理：

- ◆ 機關必須有識別符申請、異動及刪除的管理程序，可與人事異動之管理流程結合。
 - 說明：應建立完善的帳號生命週期管理流程，與人員的入職、離職或職務變更同步進行。
- ◆ 識別符的申請、異動及刪除必須獲得授權主管的核准。
 - 說明：帳號的創建、修改和停用應經過授權批准，以確保安全性。
- ◆ 應定期盤查使用者識別符，以發現已離職或非授權識別符。

- 說明：定期稽核帳號列表，移除不再需要或未經授權的帳號，降低安全風險。
- ◆ 識別符刪除後應暫停一段時間新增相同名稱的識別符。
 - 說明：避免短時間內重複使用相同的識別符，以防止混淆或繞過某些稽核記錄
- ◆ 一段時間沒使用的識別符應停用。
 - 說明：停用閒置帳號可以減少潛在的安全風險。

5.4.7 使用者鑑別符 (Authenticator)

除了了解使用者識別符，接下來我們將介紹使用者鑑別符 (Authenticator)。

(1) 使用者鑑別符：

使用者鑑別符是用來驗證使用者身分的佐證資訊或物品，例如：通行碼（密碼）、晶片卡、數位憑證、動態通行碼產生器，或是指紋等生物特徵。鑑別符是驗證使用者是否為其所聲稱身分的依據，而不同類型的鑑別符，則提供不同程度的安全性。

(2) 使用者鑑別符的管理：

- ◆ 確保鑑別符具備足夠的強度。
 - 說明：例如，通行碼應符合複雜度要求，數位憑證應由可信賴的憑證機構簽發，生物特徵辨識系統應具備足夠的準確性。
- ◆ 為初始鑑別符的配發、遺失鑑別符及註銷鑑別符建立與實作管理程序。
 - 說明：應有明確的流程來發放新的鑑別符給使用者、處理遺失或遭竊的鑑別符，以及在使用者離職或不再需要時撤銷鑑別符。
- ◆ 在資通系統安裝時變更預設的鑑別符。
 - 說明：避免使用系統預設的鑑別符，因為預設的鑑別符通常是公開或容易猜測的。
- ◆ 建立鑑別符最長壽命的限制，以及重新使用的情況。
 - 說明：定期強制更換通行碼或憑證，以及限制舊通行碼的重複使用，可以提高安全性。
- ◆ 定期變更鑑別符。
 - 說明：定期更換鑑別符，是降低長期使用的鑑別符被破解風險的有效方法。

- ◆ 保護鑑別符內容，以避免非授權洩漏與修改，並保護鑑別符安全。
 - 說明：鑑別符本身需要妥善保護，例如通行碼不應以明文儲存或傳輸，晶片卡應妥善保管。
- ◆ 需要使用者擔負與設備實作特定的防護措施，以保護鑑別符安全。
 - 說明：使用者也應對其鑑別符的安全負責，例如不輕易洩漏通行碼，妥善保管硬體憑證。

5.4.8 識別符及鑑別符之可歸責性

為確保所有存取行為皆能歸責於使用者真實身分，識別符與鑑別符在實現可歸責性方面至關重要。以下列出至少應滿足可歸責性的條件：

- (1) 首先必須要具備唯一識別符可代表使用者真實身分。
 - ◆ 說明：每個使用者必須擁有唯一的帳號，才能將其操作行為與個人身分關聯起來。
- (2) 足夠強固的使用者鑑別技術，能防止身分鑑別機制被破解。
 - ◆ 說明：採用強密碼策略、多重認證等技術，確保使用者是其所聲稱的身分，防止冒用。
- (3) 系統所有存取路徑經嚴謹被強制控管。
 - ◆ 說明：確保所有對系統資源的存取，都必須經過嚴格的驗證及授權。
- (4) 所有存取行為不論成功或失敗都被詳實記錄。
 - ◆ 說明：完整的日誌紀錄是追蹤使用者行為、分析安全事件的基礎。
- (5) 系統存取紀錄的時戳代表存取順序。
 - ◆ 說明：精確的時間戳有助於還原事件發生的順序，進行更精確的分析。
- (6) 系統存取紀錄應被妥善保護，任何人均無法修改或刪除。
 - ◆ 說明：保護日誌的完整性，防止被竄改或銷毀，確保其作為證據的有效性。

實現存取行為的可歸責性是資訊安全的重要目標之一。透過唯一識別、強固鑑別、嚴格的存取控制，以及完善且受保護的日誌紀錄，才能將使用者在系統中的行為與其真實身分關聯起來，提升整體的安全防護能力。

5.4.9 身分鑑別技術

在身分鑑別技術中，我們常用三種主要鑑別因子。這些因素通常會結

合使用，以提高鑑別的強度，也就是所謂的多因子鑑別 (Multi-Factor Authentication, MFA)。

(1) 鑑別因素

- ◆ **基於所知 (Something You Know)：**依賴使用者記憶的資訊。
 - **範例：**通行碼（密碼、PIN 碼等）。
 - **說明：**這是最常見的鑑別因素，依賴使用者記憶的資訊。其安全性取決於密碼的強度及使用者的保密意識。
- ◆ **基於所有 (Something You Have)：**依賴使用者擁有的實體物品。
 - **範例：**晶片卡、智慧卡、USB Key、手機等。
 - **說明：**這種鑑別因素依賴使用者擁有的實體物品。其安全性在於物品的唯一性及使用者的保管。
- ◆ **與生俱備 (Something You Are)：**依賴使用者的生理特徵。
 - **範例：**指紋、虹膜、臉部辨識等生物特徵。
 - **說明：**這種鑑別因素基於使用者的生理特徵，具有唯一性及不可否認性。其安全性取決於生物辨識技術的準確性及防偽能力。

(2) 強固鑑別技術

強固鑑別技術即多因子認證 (MFA)，指同時採用兩種或以上不同鑑別因素的鑑別方式，以提高身分驗證的安全性。

- ◆ **範例：**
 - **晶片卡 (Have) 配合 PIN 碼 (Know)：**
使用者需要同時擁有晶片卡，並知道 PIN 碼才能通過驗證。
 - **指紋 (Are) 配合通行碼 (Know)：**
使用者需要提供生物特徵（指紋），並輸入通行碼才能通過驗證。
 - **晶片卡 (Have) 配合指紋 (Are)：**
使用者需要同時擁有晶片卡，並提供生物特徵才能通過驗證。

(3) 生物特徵鑑別技術

生物特徵鑑別是一種利用人類獨有的生理或行為特徵，進行身分識別與鑑別的方式，提供了高準確性。

- ◆ **採用人類具備的屬性進行識別與鑑別：**
- ◆ **最昂貴、最複雜、也最能識別人員身分的鑑別技術**
生物特徵通常具有唯一性及穩定性，因此在身分驗證方面具有較高的準確性。然而，其部署及維護成本通常也較高。

- ◆ 但人類社會中對這種技術的接受性較低（隱私、侵入性及傳染病等）
生物特徵鑑別可能引發隱私疑慮，例如個人生物數據的儲存及使用。某些技術也可能被認為具有一定的侵入性或存在傳染疾病傳播的風險（雖然技術不斷進步已在很大程度上緩解了這些問題）。
- ◆ **生物特徵登錄步驟（以指紋為例），如圖 26 生物特徵登錄步驟流程圖。**
說明了生物特徵登錄的典型步驟，即將使用者的生物特徵資料註冊到系統中的過程。
 - ① **登錄請求：**使用者在客戶端發起登錄請求。
 - ② **輸入指紋：**使用者將手指放置在指紋掃描設備上。
 - ③ **擷取特徵值：**指紋掃描設備擷取使用者的指紋圖像，並提取獨特的生物特徵點。
 - ④ **轉換成數位內容：**擷取的指紋特徵被轉換成數位格式的特徵值。
 - ⑤ **加密：**數位化的指紋特徵值通常會被加密。
 - ⑥ **回傳加密後的指紋：**加密後的指紋特徵值被傳輸到伺服器。
 - ⑦ **解密：**伺服器接收到加密後的指紋特徵值後，可能會進行解密或其他處理。
 - ⑧ **保存：**處理後的指紋特徵值被安全地儲存在伺服器的資料庫中，用於後續的驗證比對。

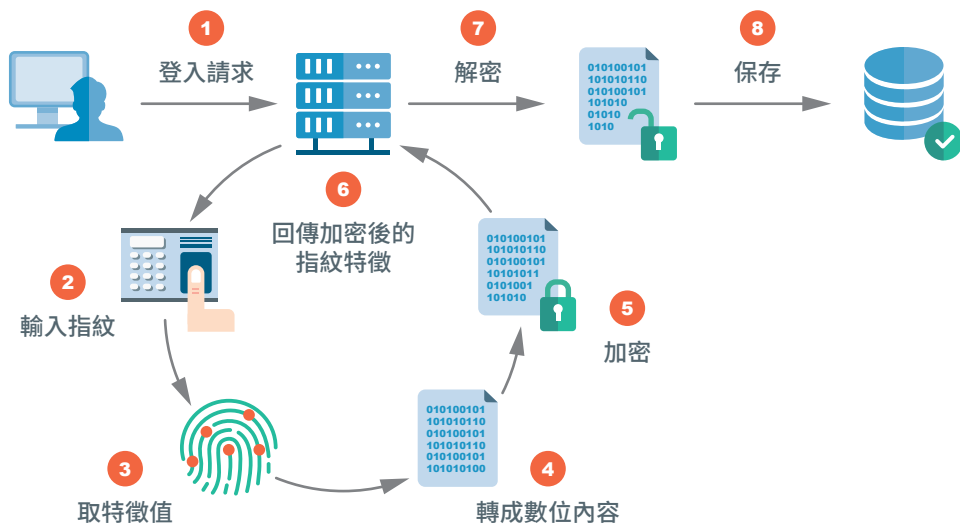


圖 26 生物特徵登錄步驟流程圖

- ◆ **生物特徵鑑別步驟（以指紋為例）**，如圖 27 生物特徵鑑別步驟流程圖，說明了生物特徵鑑別的典型步驟，即使用者嘗試登入系統時，系統如何比對驗證其提供的生物特徵與已註冊的範本。

- ① **擷取特徵值**：使用者將手指放置在指紋掃描設備上，設備擷取使用者的指紋圖像，並提取特徵值。
- ② **轉換成數位內容**：擷取的指紋特徵被轉換成數位格式的特徵值。
- ③ **加密**：數位化的指紋特徵值通常會被加密。
- ④ **傳送**：加密後的指紋特徵值被傳輸到伺服器。
- ⑤ **解密**：伺服器接收到加密後的指紋特徵值後，進行解密或其他必要處理。
- ⑥ **特徵值比對**：伺服器將接收到的使用者指紋特徵值與資料庫中儲存的該使用者的註冊範本進行比對。
- ⑦ **相似度判斷**：比對結果會產生一個相似度分數，系統將這個分數與預先設定的閾值進行比較，以判斷是否驗證成功。如果相似度超過閾值，則認為驗證成功。

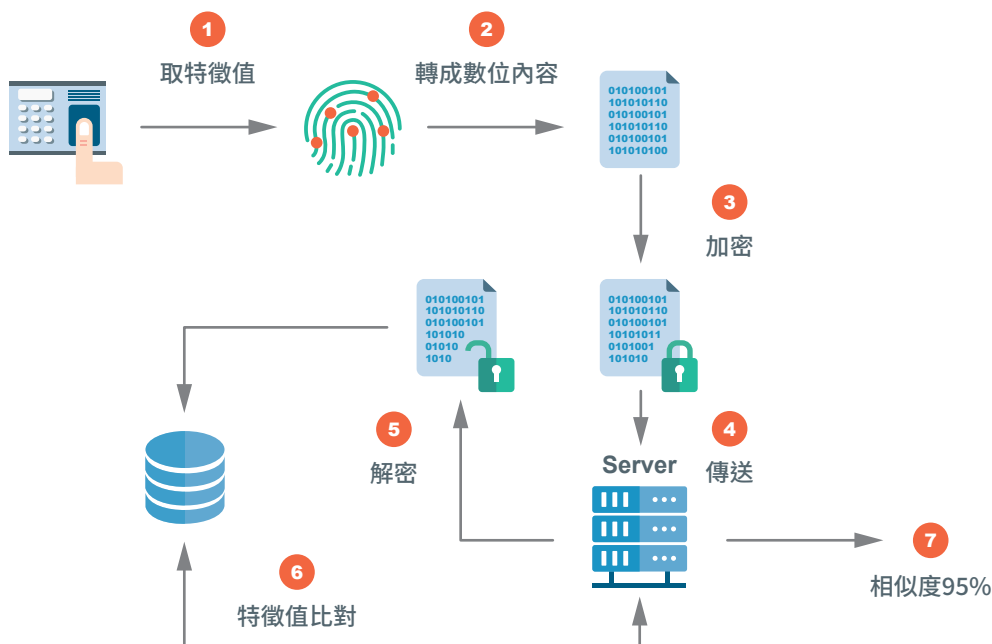


圖 27 生物特徵鑑別步驟流程圖



(4) 通行碼（密碼）鑑別技術

- ◆ 通行碼（密碼）鑑別技術是目前**最廣泛且最簡便**的身分鑑別技術，但其安全性也相對較低，因其容易遭受字典猜測、暴力破解及竊聽等攻擊。
- ◆ **相對較弱的身分鑑別技術**：使用者選用「懶人通行碼」、共用通行碼、將通行碼貼在螢幕上、從不更改通行碼、輸入通行碼時被別人看到按下的通行碼等。
- ◆ **針對通行碼的攻擊，包括：**
 - 字典猜測法。
 - 暴力式通行碼猜測。
 - 通行碼監聽。
- ◆ **避免通行碼被破解的防護措施：**
 - **系統強制要求長度至少 8 碼**：包含文字、數字與符號，包含大小寫，且在字典中查不到。
說明：強制使用足夠長度且包含多種字元組合的密碼，可以顯著提高其強度，抵抗暴力破解及字典檔攻擊。
 - **區分公務與私人服務密碼**：不得在公務服務與私人服務（個人郵件、社群等）使用同一組通行碼。
說明：一旦任一服務（尤其是常見的私人服務）發生資料外洩，攻擊者也無法利用此通行碼登入，並存取更敏感的公務系統，從而避免「一碼被盜，全面失守」的災難性後果。
 - **系統強制要求使用者定期更換通行碼**。
說明：定期更換密碼可以降低長期使用的密碼被洩漏或破解的風險。
 - **由系統判斷通行碼不重複使用**。
說明：限制使用者重複使用近期用過的密碼，防止他們為了方便而選擇弱密碼。
 - **可限制通行碼容許登入失敗的次數**。
說明：應限制來源 IP 登入失敗次數，並配合帳戶鎖定機制，可以有效防禦暴力破解嘗試。
 - **登入成功或失敗都應被記錄**。
說明：記錄登入日誌有助於監控潛在的未授權存取嘗試。
 - **使用通行碼檢測工具尋找脆弱性通行碼**。
說明：定期使用脆弱性密碼掃描工具，可以幫助識別並要求使用者更

換不安全的密碼。

- **通行碼不以明碼方式儲存（雜湊）。**

說明：使用雜湊演算法並加密處理後儲存密碼，即使資料庫洩漏，攻擊者也難以直接取得原始密碼。

- **通行碼不以明碼方式在網路上傳送。**

說明：在網路傳輸過程中，應使用加密協議（例如 HTTPS）保護通行碼的安全。

- **加強保護集中存放通行碼雜湊值的伺服器。**

說明：儲存密碼雜湊值的伺服器是高價值目標，必須採取嚴格的安全措施進行保護。

(5) 一次性通行碼鑑別技術

一次性通行碼 (One-Time Password, OTP) 或稱動態通行碼，是一種比靜態密碼更安全的驗證方式，每次產生的通行碼只能使用一次，有效防止通行碼被竊聽或猜測攻擊。

- ◆ **一次性通行碼 (One-Time Password) 或稱動態通行碼的特質：**

- **由隨身攜帶的符記 (Token) 或軟體自動產生登入用通行碼。**

說明：OTP 通常由硬體符記或安裝在智慧型手機上的應用程式產生。

- **登入時每次產生的通行碼只能使用一次。**

說明：這是 OTP 最主要的優點，即使通行碼被攔截，也因為只能使用一次而失效。

- **可防止通行碼被竊聽而偽冒登入的問題。**

說明：由於每次使用的密碼都不同，即使攻擊者竊聽到某一次的 OTP，也無法用於後續的登入。

- **可防止通行碼猜測攻擊。**

說明：因為每次使用的密碼都是隨機產生且一次性，所以猜測特定有效密碼的難度很高。

- ◆ **同步式一次性通行碼技術：**

- **同步式 OTP (Synchronous OTP)：**這種一次性通行碼技術的產生符記 (Token) 與鑑別伺服器間存在同步機制，通常是基於時間或事件計數。透過共享的金鑰及時間同步來產生一致的一次性通行碼 (OTP)，如圖 28 所示的「同步式一次性通行碼技術流程圖」。

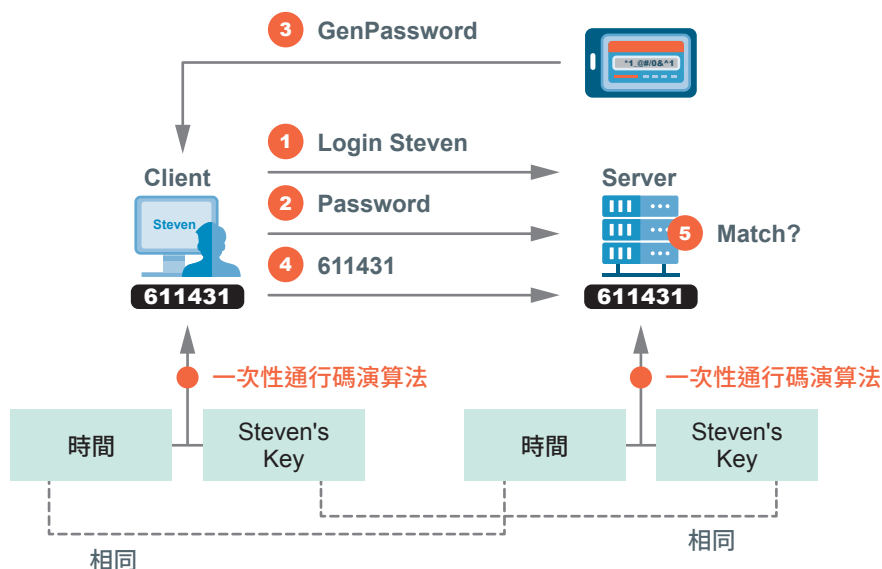


圖 28 同步式一次性通行碼技術流程圖

• 流程說明：

① LoginSteven (Client to Server)：

使用者 Steven 在客戶端輸入帳號，並嘗試登入伺服器。

② Password (Client to Server)：

Steven 可能還需要輸入一個靜態密碼作為第一層驗證。

③ GenPassword (User to Client)：

Steven 操作其 OTP 產生器（符記），產生當前的一次性通行碼 (611431)。這個 OTP 的產生是基於當前時間及儲存在符記中的 Steven 的金鑰，並透過特定的 OTP 演算法計算得出。

④ 611431 (Client to Server)：

Steven 將產生的一次性通行碼 (611431) 輸入到客戶端，並傳送給伺服器。

⑤ Match? (Server)：

伺服器端也使用相同的 OTP 演算法、Steven 的金鑰，以及伺服器當前的時間（或一個時間窗口）來計算預期的一次性通行碼。伺服器將接收到的 OTP 與其計算出的 OTP 進行比對。如果兩者匹配，則驗證成功。

- **同步式一次性通行碼的產生與驗證：**

圖 27 下半段詳細展示了使用者端 (Client) 及伺服器端 (Server) 如何獨立地產生相同的一次性通行碼，並以此來驗證使用者身分。以下說明時間同步產生 OTP 的過程：

- **時間 (Time)：**

這是產生一次性通行碼的一個關鍵輸入。通常，OTP 系統會依據一個同步的時間戳來確保兩端產生相同的數值。

- **Steven's Key：**

這是一個預先共享的秘密密鑰，只有使用者 (Steven) 的裝置（例如：OTP 產生器或軟體）及伺服器知道。通常在使用者註冊或首次設定 OTP 時安全地建立。

- **一次性通行碼演算法 (One-Time Password Algorithm)：**

這是一個數學函數，將「時間」及「Steven's Key」作為輸入，並生成一個獨特的、時效性的一次性通行碼。這種演算法是公開的，但因為「Steven's Key」是秘密的，所以其他人無法預測或複製這個通行碼。

- ◆ **非同步式一次性通行碼技術**

- **非同步式 OTP (Asynchronous OTP)：**

與同步式不同，非同步式一次性通行碼的產生符記與鑑別伺服器間不具備時間或事件同步機制。主要依賴於伺服器發出的挑戰值 (Challenge Value) 來生成通行碼。非同步式 OTP 的安全性同樣建立在客戶端（例如 OTP 產生器）與伺服器之間共享的秘密金鑰之上，但其一次性通行碼的產生，是基於伺服器所發送的隨機挑戰值。如圖 29 所示的「非同步式一次性通行碼技術流程圖」。

- **流程說明：**

- ① **LoginSteven (Client to Server)：**使用者 Steven 在客戶端輸入帳號，並嘗試登入伺服器。
- ② **GenRandomNum 232443 (Server)：**伺服器產生一個隨機的挑戰值 (232443)。
- ③ **Challenge 232443 (Server to Client)：**伺服器將這個挑戰值傳送給客戶端。

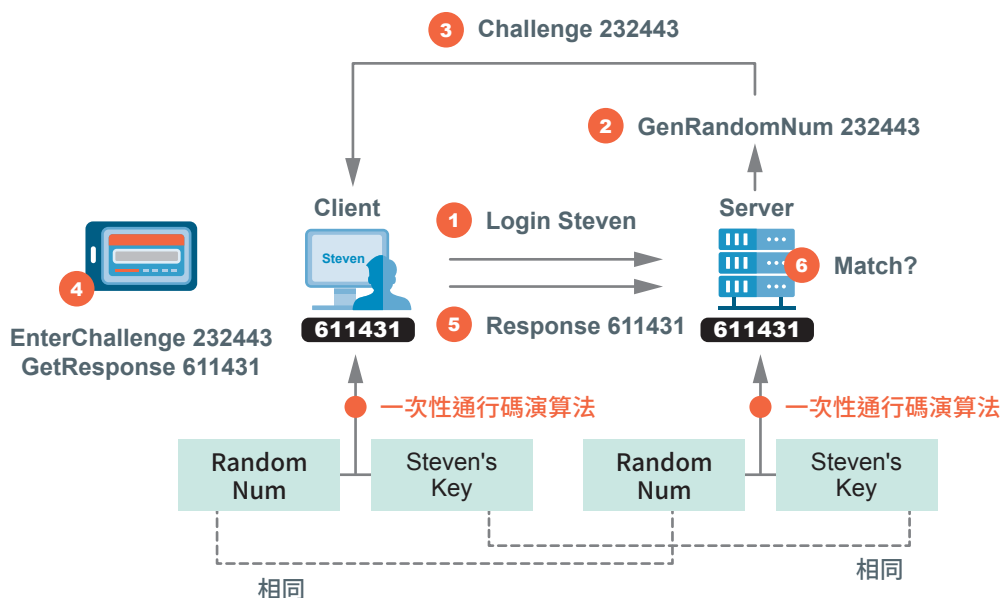


圖 29 非同步式一次性通行碼技術流程圖

④ EnterChallenge 232443 GetResponse 611431 (User to Client) :

Steven 在其 OTP 產生器（符記）上手動輸入這個挑戰值 (232443)。符記使用這個挑戰值、儲存在其中的 Steven 的金鑰，以及特定的 OTP 演算法，計算出一次性回應 (611431)。

⑤ Response 611431 (Client to Server) :

Steven 將產生的一次性回應 (611431) 輸入到客戶端，並傳送給伺服器。

⑥ Matched? (Server) :

伺服器端也使用相同的 OTP 演算法、Steven 的金鑰，以及先前產生的挑戰值 (232443) 來計算預期的回應。伺服器將接收到的回應與其計算出的回應進行比對。如果兩者匹配，則驗證成功。

• 非同步式一次性通行碼的產生與驗證：

圖 28 下半段詳細展示了在非同步式 OTP 機制下，客戶端 (Client) 及伺服器端 (Server) 如何透過一個隨機挑戰值及共享的金鑰，來獨立計算並比對通行碼。以下說明時間同步產生 OTP 的過程：

– 挑戰值 (Random Num / Challenge) :

這是一個由伺服器在每次認證嘗試時隨機生成的數字（例如圖中的 232443）。伺服器會將這個挑戰值發送給使用者端。不同於同步式

OTP 依賴時間，非同步式 OTP 的隨機數確保了每次認證的獨特性。

– **Steven's Key :**

這是一個**預先共享的秘密金鑰**，僅使用者 (Steven) 的裝置 (例如：硬體 Token) 及伺服器知道。此金鑰在使用者首次設定 OTP 時安全地建立並儲存。

– **一次性通行碼演算法 (One-Time Password Algorithm) :**

這是一個預設的數學函數，將**隨機挑戰值**及 **Steven's Key** 作為輸入。

- 透過這個演算法，無論是使用者端還是伺服器端，只要輸入相同的挑戰值及金鑰，就能產生相同的通行碼。

(6) 詰問與回應身分鑑別技術：

挑戰 - 回應 (Challenge-Response) 身分鑑別機制基於非對稱金鑰 (Asymmetric Cryptography)，通常被稱為數位簽章式身分驗證。如圖 30 詰問與回應身分鑑別技術流程圖，說明使用者 (Steven) 如何使用其私鑰 (PrivateKey) 對伺服器發出的挑戰進行「簽章」(或以私鑰進行簽章)，然後伺服器使用 Steven 的公鑰 (PublicKey) 來驗證這個簽章，從而確認 Steven 的身分。

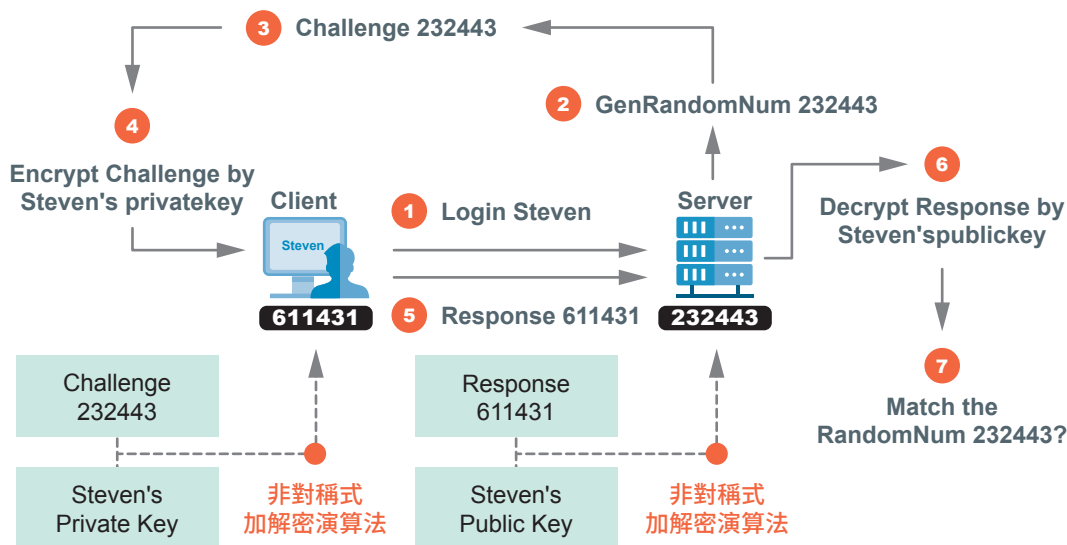


圖 30 詰問與回應身分鑑別技術流程圖



◆ 採用加密機制完成身分鑑別：

- 運用非對稱式加密演算法。
- 雙方不必分享共同的金鑰。
- 不必輸入任何通行碼或回應訊息即可完成鑑別。

◆ 流程說明：

- ① **LoginSteven (Client to Server)**：使用者 Steven 在客戶端輸入帳號，並嘗試登入伺服器。
- ② **GenRandomNum 232443 (Server)**：伺服器產生一個隨機的挑戰值 232443。
- ③ **Challenge 232443 (Server to Client)**：伺服器將這個挑戰值傳送給客戶端。
- ④ **EncryptChallengebySteven' sprivatekey -> 611431 (Client)**：客戶端使用 Steven 的私鑰對挑戰值 (232443) 進行加密，產生回應 (611431)。
- ⑤ **Response 611431 (Client to Server)**：客戶端將加密後的回應 (611431) 傳送給伺服器。
- ⑥ **DecryptResponseBySteven' spublickey -> 232443 (Server)**：伺服器使用 Steven 的公鑰解密接收到的回應 (611431)，得到解密後的數值 (232443)。
- ⑦ **MatchtheRandomNum 232443? (Server)**：伺服器將解密後的數值與其先前產生的隨機挑戰值 (232443) 進行比對。如果兩者匹配，則驗證成功。

◆ 驗證說明：

- 客戶端使用 Steven 的私鑰對挑戰值進行加密。
- 伺服器使用 Steven 的公鑰對回應進行解密。由於只有擁有 Steven 私鑰的人才能成功加密出能被其公鑰正確解密的結果，因此可以驗證 Steven 的身分。

5.4.10 符記 (Token)

符記是一種適合隨身攜帶的卡片或感應器，用來實作「基於所有 (Something you have)」身分鑑別技術。符記作為一種「持有物」的鑑別因素，

可以與「所知」或「與生俱備」的因素結合使用，實現更安全的強固鑑別。

(1) 通常可分為下列幾種類型：

- ◆ 記憶卡
- ◆ 智慧卡：智慧卡內含晶片，可以儲存憑證及執行加密運算。

(2) 依其感應或資料傳輸的方式又可區分：

- ◆ 接觸式
- ◆ 非接觸式

(3) 符記的外型：

- ◆ 卡片式（例如：信用卡、員工識別證等）。
- ◆ 隨身型計算機：通常用於產生一次性密碼，如計算機造型的 OTP 產生器。
- ◆ 鑰匙環裝飾品的 USB 符記：通常用於儲存數位憑證，如 USB 造型的符記。

(4) 記憶卡：

- ◆ 沒有微處理器，甚至沒有積體電路，只有磁條。
- ◆ 記憶空間中只存放身分鑑別時所需的資訊（如私密金鑰與帳號）。
- ◆ 使用者至少需要輸入 PIN 碼。
- ◆ 將帳號、PIN 碼及記憶卡中的鑑別資訊，傳送到後端鑑別伺服器，經解密或雜湊運算後，比對即可完成身分鑑別。

(5) 智慧卡：

- ◆ 智慧卡的特質：
 - 具備微處理器與積體電路。
 - 可記憶也可運算。
 - 具備防拆解與竄改的保護機制。
 - 必須輸入 PIN 或通行碼啟動智慧卡功能。
- ◆ 智慧卡可運用在：
 - 存放生物識別特徵碼。
 - 挑戰與回應的私密金鑰儲存與加密運算。
 - 存放持有人的購物紀錄與就醫紀錄。

識別與鑑別是構建資通系統安全的第一步。透過多種技術與管理措施的結合，從基礎的帳號管理到先進的生物特徵識別，組織能夠有效地確認使用者身分，防止未經授權的存取，從而保障資訊資產的安全。

5.5

「系統與服務獲得」之安全控制措施

系統與服務獲得是指在資通系統的整個生命週期中，從需求、設計、開發、測試到部署與維運各個階段，都充分考慮安全性需求，以打造具備安全體質的資通系統。這強調了「將安全深度融入設計」的理念，而非僅在系統建成後才考慮資安。

表 35 詳細列出針對不同防護等級的資通系統，在系統與服務獲得構面下，關於系統發展生命週期之需求階段、設計階段、開發階段、測試階段、部署與維運階段、委外階段，以及獲得程序及系統文件等面向的安全控制措施。

表 35 系統與服務獲得構面之安全控制措施

措施內容	高	中	普
系統發展生命週期需求階段	針對系統安全需求（含機密性、可用性、完整性）進行確認		
系統發展生命週期設計階段	1. 根據系統功能與要求，識別可能影響系統之威脅，進行風險分析及評估。 2. 將風險評估結果回饋需求階段之檢核項目，並提出安全需求修正。		無要求
系統發展生命週期開發階段	1. 執行「源碼掃描」安全接測。 2. 系統應具備發生嚴重錯誤時之通知機制。 3. 等級「中」及「普」之所有控制措施	1. 應針對安全需求實作必要控制措施。 2. 應注意避免軟體常見漏洞及實作必要控制措施。 3. 發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息。	
系統發展生命週期測試階段	1. 執行「滲透測試」安全檢測。 2. 等級「中」及「普」之所有控制措施	執行「弱點掃描」安全檢測。	

措施內容	高	中	普
系統發展生命週期 部署與維護階段	1. 於系統發展生命週期之維運階段，應執行版本控制與變更管理。 2. 等級「普」之所有控制措施		1. 針對威脅，更新與修補、關閉不必要服務及埠口 2. 資通系統不使用預設密碼
系統發展生命週期 委外階段	資通系統開發如委外辦理，應將系統發展生命週期各階段等級將安全需求（含機密性、可用性、完整性）納入委外契約。		
獲得程序	開發、測試及正式作業環境應為區隔		無要求
系統文件	應儲存與管理系統發展生命週期之相關文件		

安全系統發展生命週期 (Secure System Development Life Cycle, SSDLC) 強調在專案各階段及早加入安全思維，以打造具備安全體質的資通系統。以下分別說明各階段之重要性、實施方式及效益：

5.5.1 需求階段 - 確認安全需求（高中普）

- (1) **重要性：**在系統需求階段就考慮安全需求（如機密性、可用性、完整性），是構建安全系統的基礎。
- (2) **實施方式：**針對系統安全需求（含機密性、可用性、完整性）進行確認。系統安全需求可能來自於法規或業界標準要求、內部資安政策或業務需求等來源，應仔細確認後再開始進行系統設計與實作等活動。
- (3) **效益：**從源頭融入安全，避免後期因安全缺陷導致的重大變更。

5.5.2 設計階段 - 威脅識別與風險評估（高中）

- (1) **重要性：**在系統設計階段考慮潛在的安全風險，並設計相應的防護措施，能夠有效地降低系統的脆弱性。
- (2) **實施方式：**依據系統功能與需求，識別可能影響系統之威脅，進行風險分

析及評估；將風險評估結果回饋需求階段之檢核項目，並提出安全需求修正。普等級之資通系統，則無要求。

- ◆ 風險是指威脅利用其相對應脆弱性造成組織或政府機關資訊資產受到衝擊的可能性。
- ◆ 識別資通系統面臨之資安威脅，並進一步分析各種威脅之風險。

(3) **效益：**在早期階段識別及緩解安全風險，降低開發及部署階段的成本及複雜性。

(4) **安全需求修正：**

將風險評估結果回饋需求階段之檢核項目，並提出安全需求修正。當完成上述威脅識別與風險評估活動後，可能從中發現當初未考慮到之威脅，此時應思考對應之安全控制措施，並進行安全需求之修正。

5.5.3 開發階段 - 安全需求實作

(1) **重要性：**在系統開發過程中實施安全措施，例如安全編碼及漏洞掃描，有助於減少系統中存在的安全漏洞。

(2) **實施方式：**

◆ **高中普等級：**

- 應針對安全需求實作必要控制措施；資通系統應訂定安全需求項目，包含機密性、完整性及可用性等相關要求，並應確實實作。
- 應注意避免軟體常見漏洞及實作必要控制措施；稽核驗證宜確認機關相關管理規範及安全強化作為。
- 發生錯誤時，使用者介面應顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息；系統宜客製化錯誤頁面，隱藏錯誤程式碼位置與內容等機敏訊息。

◆ **高等級：**

- 執行「源碼掃描」安全檢測，並包含中等級及普等級之所有控制措施。
- 執行「源碼掃描」安全檢測時，機關宜選用具安全檢測能力之工具，以發現源碼安全弱點。
- 系統應具備發生嚴重錯誤時之通知機制，避免無人發覺與處理。

(3) **效益：**開發出更安全的軟體，減少部署後需要修補的安全漏洞，提升系統的整體安全性。

5.5.4 測試階段

- (1) **重要性：**在系統部署前進行安全測試，如滲透測試或弱點掃描，有助於發現並修復潛在的安全漏洞。
- (2) **實施方式：**
 - ◆ **高中普等級：**
 - 執行「弱點掃描」安全檢測。
 - 弱點掃描包含系統（主機）弱點掃描與網站弱點掃描
 - 機關宜選用具安全檢測能力之自動化檢測工具，對目標進行掃描，常見如連接埠掃描、作業系統識別、版本掃描、常見弱點檢測等。
 - ◆ **高等級：**
 - 執行「滲透測試」安全檢測，並包含中等級及普等級之所有控制措施。
 - 一般由資安專家手動進行，效果取決於人員經驗與技術。
- (3) **效益：**降低已部署系統的風險，避免因已知漏洞導致的安全事件。

5.5.5 部署與維護階段

- (1) **重要性：**系統部署後的安全維護至關重要，包括漏洞修補、安全更新及組態管理，以應對新的威脅。
- (2) **實施方式：**
 - ◆ **高中普等級：**
 - **系統更新與修補：**針對威脅，更新與修補、關閉不必要服務及埠口，如作業系統安全性更新。系統服務與埠口 (Port)：原則關閉，有需要才開放。
 - **禁用預設密碼：**資通系統不使用預設密碼，相關軟體（例如套裝軟體、資料庫、Web 伺服器）應避免使用預設密碼，建議於系統正式上線前停用或完成密碼變更。
 - ◆ **高中等級：**
 - 於系統發展**生命週期**之維護階段，應執行版本控制與變更管理，並包含普等級之所有控制措施。
 - **版本控制與變更管理：**版本控制目的在需要時可取回特定版本，機關應依 ISMS 或其他相關規定進行系統變更。



- (3) **效益**：維持系統的安全狀態，降低因未修補漏洞或不安全組態所帶來的風險。

5.5.6 委外階段 - 委外安全需求（高中普）

- (1) **重要性**：當系統開發或服務委外時，確保供應商也遵循組織的安全要求，保護敏感資訊及系統安全。
- (2) **實施方式**：資通系統開發如委外辦理，應將系統發展生命週期各階段依等級安全需求（含機密性、可用性、完整性）納入委外契約。
 - ◆ 將系統安全需求明確納入委外契約，並據以驗收。
- (3) **效益**：確保委外開發或服務符合組織的安全標準，降低供應商帶來的安全風險。

5.5.7 獲得程序 - 作業環境區隔（高中）

- (1) **重要性**：安全的獲得程序有助於確保開發、測試及正式作業環境的隔離，降低環境間互相影響的風險。
- (2) **實施方式**：開發、測試及正式作業環境應為區隔。普等級之資通系統，則無要求。
 - ◆ 開發環境、測試環境及正式作業環境應實作必要之存取控制，以保護正式作業環境之系統與資料。
- (3) **效益**：防止開發或測試環境的問題影響到正式運行的系統。

5.5.8 系統文件 - 文件儲存與管理（高中普）

- (1) **重要性**：完善的系統文件記錄系統發展生命週期的相關資訊，有助於理解系統設計、組態設定及安全措施。
- (2) **實施方式**：應儲存與管理系統發展生命週期之相關文件。
 - ◆ 系統發展生命週期之相關文件應以書面或電子化形式進行文件保存，並被納入管理程序。
- (3) **效益**：便於系統的管理、維護及安全稽核。

5.6

「系統與通訊保護」之安全控制措施

系統與通訊保護是資通安全防護的關鍵，旨在確保資通系統及資訊在傳輸、儲存及處理過程中的機密性、完整性與可用性。主要透過應用加密與簽章技術來實現，以防止未經授權的存取、監聽、竄改或偽造。

表 36 詳細列出針對不同防護等級的資通系統，在系統與通訊保護構面下，關於傳輸之機密性與完整性，以及資料儲存的安全控制措施。

表 36 系統與通訊保護構面之安全控制措施

措施內容	高	中	普
傳輸之機密性與完整性	1. 資通系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變更。但傳輸過程中有蓄代之實體保護措施者，不在此限。 2. 使用公開、國際機構驗證且未遭破解之演算法。 3. 支援演算法最大長度金鑰。 4. 加密金鑰或憑證應定期更換。 5. 伺服器端之金銷保管應訂定管理規範及實施應有之安全防護措施。	無要求	無要求
資料儲存之安全	資通系統重要組態設定檔案及其他真保護需求之資訊應加密或以其他適當方式儲存。	無要求	無要求

5.6.1 傳輸之機密性與完整性（高）

(1) **重要性：**保護資料在傳輸過程中的機密性，防止未經授權的存取；同時確保資料的完整性，防止傳輸過程中被竄改。

(2) **實施方式：**

◆ **傳輸加密：**

- 資通系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變更。但傳輸過程中若有替代之實體保護措施者，不在此限。
 - 資通系統應實作傳輸加密機制，如 HTTP 1.2/1.3、SSH、SFTP 及 VPN 等加密傳輸協定，或其他足以確保資料傳輸過程機密性與完整性之安全控制措施。
 - ◆ **演算法：**
 - 主機或網站弱點使用公開、國際機構驗證且未遭破解之演算法。
 - 掃描通常可檢測出是否已啟用不安全的傳輸協定。
 - ◆ **金鑰長度：**
 - 支援演算法最大長度金鑰。
 - 站台在選擇加密傳輸金鑰時，較長之金鑰長度強度較高。
 - ◆ **金鑰憑證更換：**
 - 加密金鑰或憑證應定期更換。
 - 避免使用萬年憑證而增加被破解的風險，已過期憑證應儘速更換。
 - 對外服務站台應使用合法憑證中心核發之伺服器憑證。
 - ◆ **金鑰保管：**
 - 伺服器端之金鑰保護應訂定管理規範及實施應有之安全防護措施。
 - 強化存取控制，加密金鑰與加密資料應分開存放，以確保金鑰的機密性、完整性及可用性。
 - ◆ 中普等級，則無要求。
- (3) **效益：**保障資料在傳輸過程中的安全性，防止敏感資訊洩漏和資料被惡意修改。

5.6.2 資料儲存之安全（高）

- (1) **重要性：**保護儲存的資料不被未經授權的存取，確保資料的機密性及完整性。
- (2) **實施方式：**
- ◆ **組態與資料保護：**資通系統重要組態設定檔案及其具保護需求之資訊應加密，或以其他適當方式儲存。中普等級，則無要求。
- (3) **效益：**防止儲存在系統中的敏感資訊被未經授權的人員存取，提高資料的安全性。

5.6.3 加密與簽章技術

加密與簽章技術是確保資訊機密性、完整性、鑑別性及不可否認性的主要手段，廣泛應用於資通系統的各種安全防護機制中。

- (1) **主要用途：**確保資訊的「機密性」、「完整性」、「鑑別性」及「不可否認性」。
- (2) **常見應用：**資料通訊的安全 (VPN、SSL 或 SSH 等)、資料儲存的安全 (硬碟加密、檔案加密或資料庫加密)、身分鑑別的安全 (數位憑證身分鑑別)、資料完整性與不可否認的安全 (電子簽章)。
- (3) **加密技術：**
 - ◆ **對稱式加解密演算法：**使用秘密金鑰，加密與解密用同一把金鑰。
 - ◆ **非對稱式加解密演算法：**使用公開金鑰與私密金鑰，公開金鑰加密只能用私密金鑰解密，私密金鑰加密只能用公開金鑰解密。
- (4) **簽章技術：**雜湊函數、數位簽章。

5.6.4 加密技術強度

- (1) 加密技術的強度衡量其密碼被破解所需花費的時間與資源，
- (2) 加密技術強度通常牽涉到下列等因素的影響：
 - ◆ 演算法強度、金鑰保護機制、金鑰長度及亂數產生器不可預測性。
- (3) 密碼系統的安全性不在於演算法的保密，而應經得起挑戰。
 - ◆ 專屬的演算法不見得安全，經得起挑戰的演算法才是被證明為安全的。
- (4) 目前加解密被成功攻擊的原因大部分屬人為因素：
 - ◆ 不正確的實作加密機制。
 - ◆ 不安全的金鑰保密機制。

5.6.5 加密技術強度的相關法令

- (1) **電子票證應用安全強度準則：**
 - ◆ 明確要求金融服務業，對於電子票證相關服務必須採用經認證的加密或簽章演算法強度。
 - ◆ **電子票證：**指以電子、磁力或光學形式儲存金錢價值，並含有資料儲存或計算功能之晶片、卡片、憑證或其他形式之債據，作為多用途支付使用之工具。



5.6.6 對稱式加密演算法

對稱式加密演算法的特點是加密與解密使用同一把「秘密金鑰」，因此金鑰的保護至關重要。

- (1) 對稱式密碼學 (Symmetric Cryptography) 又稱作「私密金鑰密碼學 (Secret Key Cryptography)」。
- (2) 也就是加密與解密用的是「同一把金鑰」。
- (3) 這把金鑰雙方都必須好好保護，才能確保密文的安全強度，因此叫「秘密金鑰」。
- (4) **運作說明：**如圖 31 對稱式加密運作流程圖，呈現了對稱式加密的基本流程。
 - ◆ **加密：**明文透過「對稱式加密演算法」及一把紅色的「秘密金鑰」轉換成密文。
 - ◆ **解密：**若要將密文還原成明文，則需要使用相同的「對稱式加密演算法」及相同的「秘密金鑰」。



圖 31 對稱式加解密運作流程圖

(5) 常見演算法：

- ◆ **DES (Data Encryption Standard)：**美國密碼演算法標準，有效金鑰長度 56 位元，但已不夠安全。
- ◆ **Triple-DES (3DES)：**DES 演算法重複使用，有效金鑰長度 112/168 位元，安全性更高但效率不如新演算法。
- ◆ **RC2, RC4, RC5, RC6：**美國 RSA 公司開發之演算法，金鑰長度可變，其中 RC4 曾廣泛使用，現已認為不安全。
- ◆ **AES (Advanced Encryption Standard)：**比利時 Joan Daemen 與 Vincent Rijmen 所開發，於 2000 年 AES 計畫中獲選為新一代密碼演算法標準，目前廣泛認為安全且高效。
- ◆ **優點：**
 - 加解密速度較非對稱式加解密演算法快。
 - 如果金鑰長度夠長，將難以被破解。

◆ 缺點：

- 當加密對象多時，金鑰的保護與交換變得麻煩，需要額外的安全機制。
- 只提供機密性保護功能，無法提供不可否認性功能。

(6) 對稱式加密之秘密金鑰數量：

當對稱式加密對象人數愈多時，就代表秘密金鑰的個數也愈多，此對稱式加密的缺點，特別是在需要與多個對象進行安全通訊時，將造成金鑰管理的挑戰。

其計算公式如下：

- ◆ N 個使用者需要 $N(N-1)/2$ 把金鑰。
- ◆ 若 3 個使用者，則需要 3 把金鑰。
- ◆ 若 10 個使用者，則需要 45 把金鑰。
- ◆ 若 1,000 個使用者，則需要 499,500 把金鑰。

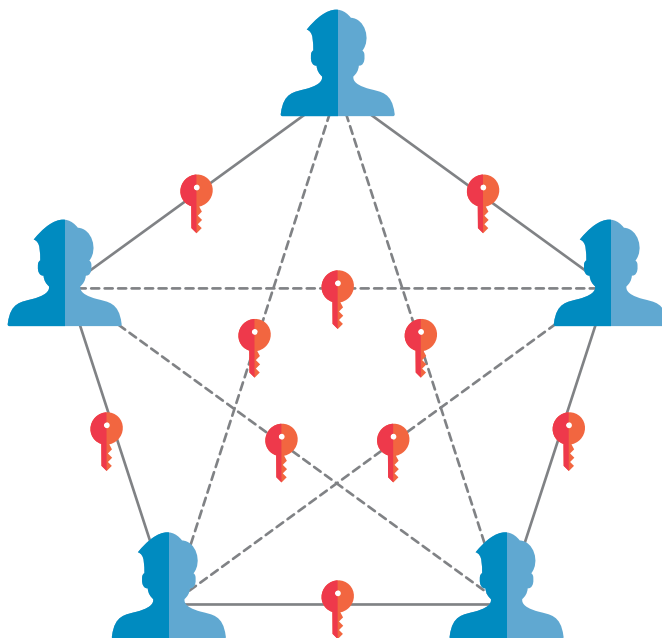


圖 32 對稱式加密之私密金鑰數量示意圖

- ◆ 圖 32 呈現了 5 個使用者之間使用對稱式加密進行通訊的情形。每 2 個使用者之間都有一把獨立的秘密金鑰（以紅色的鑰匙表示），總共有 $5 * (5-1) / 2 = 10$ 把金鑰。這清楚地展示了隨著使用者數量的增加，金鑰數量呈指數級增長，這凸顯了金鑰管理的複雜性。



5.6.7 非對稱式加解密演算法

非對稱式加解密演算法使用一對金鑰（公開金鑰與私密金鑰），公開金鑰加密的密文只能用私密金鑰解密，私密金鑰加密的密文只能用公開金鑰解密。這種特性使其能夠同時實現機密性與身分驗證（透過數位簽章）。如圖 33 非對稱式加解密運作流程圖。

流程一：



流程二：



圖 33 非對稱式加解密運作流程圖

(1) 運作說明：

- ◆ **流程 1（加密以確保機密性）：**明文使用綠色的「公開金鑰」透過「非對稱式加解密演算法」加密成密文。該密文只能使用對應的紅色「私密金鑰」還原成明文。
- ◆ **流程 2（加密以確保鑑別性 / 簽章）：**明文使用紅色的「私密金鑰」透過「非對稱式加解密演算法」加密成密文（此時更像是產生簽章）。該密文只能使用對應的綠色的「公開金鑰」驗證（或解密）其來源。

(2) 常見演算法：

- ◆ **RSA (Rivest-Shamir-Adleman)：**最廣泛使用的演算法，安全性導因於因數分解的困難度，具有資料加密與數位簽章功能。
- ◆ **ElGamal：**安全性導因於解離散對數的困難度，具有資料加密與數位簽章功能。
- ◆ **優點：**
 - 金鑰管理較容易，每個人兩把金鑰，+1,000 個人也只要 2,000 把金鑰。
 - 公開金鑰可以任意公開傳送，不需額外的保護機制。

- ◆ 缺點：加解密速度比對稱式加解密演算法慢。

5.6.8 數位信封

數位信封結合了對稱式與非對稱式加解密演算法的優點，如同將資料裝入信封，只有接收者才能拆開信封看到資料，如圖 34 數位信封運作流程圖。

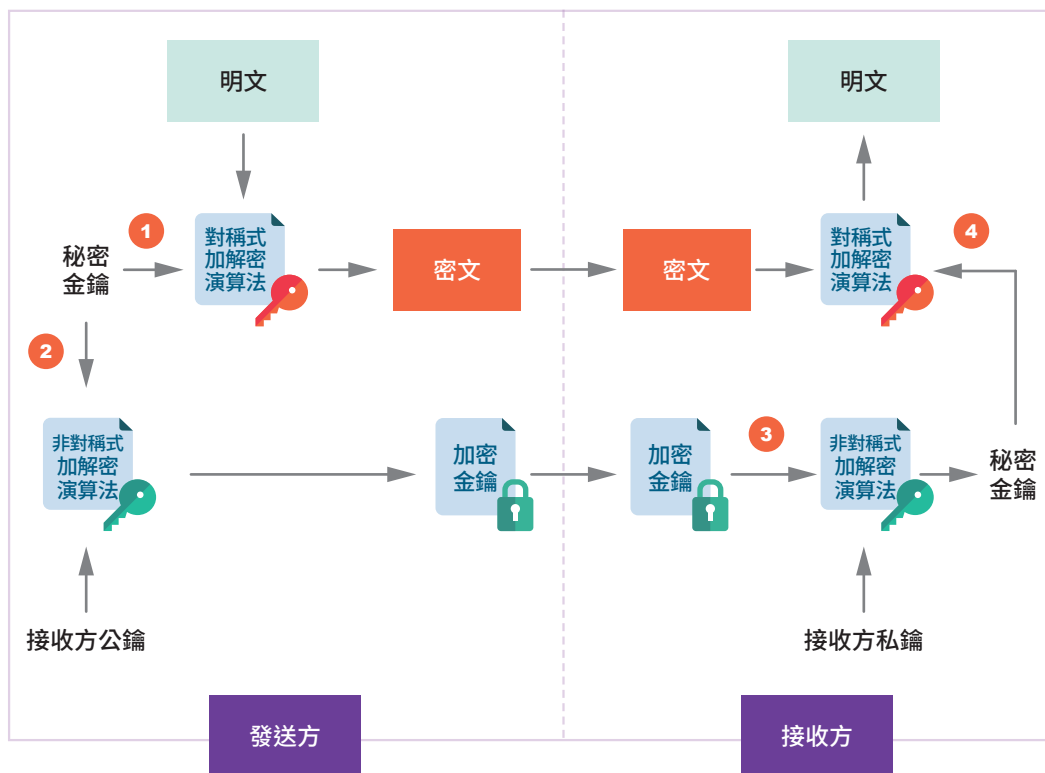


圖 34 數位信封運作流程圖

(1) 運作說明：

◆ 發送方：

- ① 發送方加密明文：發送方隨機生成一個一次性的對稱式加密金鑰（即秘密金鑰），發送方使用此「秘密金鑰」，對「明文」進行加密，生成「密文」。
- ② 發送方加密對稱金鑰：發送方使用「接收方公鑰」對該「秘密金鑰」進行非對稱式加密，生成「加密金鑰」。

說明：發送方將「密文」及「加密金鑰」一同傳送給接收方。

◆ 接收方：

③ **接收方解密對稱金鑰**：接收方收到「密文」及「加密金鑰」後，使用自己的「接收方私鑰」對「加密金鑰」進行非對稱式解密，得到原始的「秘密金鑰」。

④ **接收方解密密文**：接收方使用解密得到的「秘密金鑰」對「密文」進行解密，還原出原始的「明文」。

(2) 優點：

- ◆ 使用對稱式加密來加密大量的資料，速度快。
- ◆ 使用非對稱式加密來安全地傳輸對稱金鑰，簡化了金鑰管理，只有接收方的私鑰才能解開這個「信封」（即解密對稱金鑰）。

因此，數位信封結合了對稱式加密的速度及非對稱式加密的安全性，是一種高效且安全的資料傳輸方法。

5.6.9 雜湊函數之特性與安全性分析

雜湊函式是依據同一函式，將任何長度的資料轉換成固定長度「訊息摘要 (Message Digest)」，也稱為「數位指紋 (Digital Fingerprint)」。

(1) 特性：

- ◆ 原始訊息不變則雜湊值相同（且唯一）。
- ◆ 無法從雜湊值回推原始訊息（單向），不具有可逆性。
- ◆ 如果兩個雜湊值是不相同的，那麼這兩個雜湊值的原始輸入也是不相同的。

(2) 演算法：MD5、SHA-256、SHA-512、SHA3-512。

MD5 之演算法已被證實存在多種安全漏洞，特別是容易受到碰撞攻擊 (Collision Attack)，即攻擊者可以找到兩組不同資料能產生相同的 MD5 雜湊值。這使得 MD5 不再適用於需要安全性的應用場合，例如數位簽章、憑證驗證與檔案完整性檢查等用途。

(3) 運作說明：

- ◆ 圖 35 展示了雜湊函式的運作流程，強調其作為資料「數位指紋」的特性。
- ◆ 對不同輸入文本，應用雜湊函數後，得到的固定長度的雜湊值 (Hash sum)。即使輸入的內容略有不同，產生的雜湊值也會完全不同。
- ◆ 常用於驗證資料的完整性（透過比較資料的雜湊值）、儲存密碼（儲存

雜湊值而非明文)，以及數位簽章等應用。

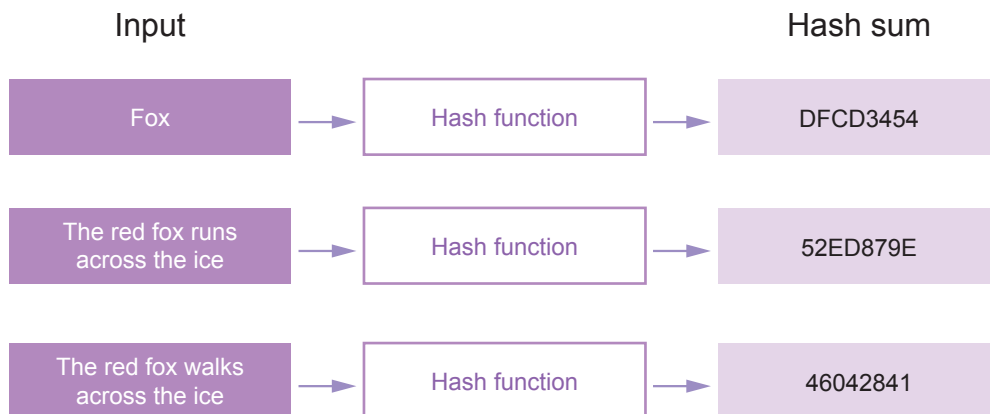


圖 35 雜湊函式運作流程圖

5.6.10 數位簽章

數位簽章的目的是證明電子檔案為簽章者所傳送，並能在資料被竄改時發現。數位簽章技術同時提供了訊息的「完整性」、「鑑別性」及「不可否認性」。

(1) 特性：

- ◆ 數位簽章的流程結合了雜湊函數及非對稱式加密。
- ◆ 發送方使用私鑰簽署訊息的雜湊值，接收方使用對應的公鑰驗證簽章。
- ◆ 由於只有發送方擁有私鑰，因此簽章提供了鑑別性及不可否認性。
- ◆ 而雜湊值的比對則保證了訊息的完整性。

(2) 運作說明：如圖 36 數位簽章運作流程圖。

- ◆ **發送方：**發送方的目的是為「明文」產生數位簽章，並可選擇性地加密明文，以確保機密性，然後將其與簽章一同傳送。
 - ① **發送方雜湊明文：**對原始「明文」進行雜湊 (hash) 運算，產生固定長度的「訊息摘要 (Message Digest)」。這是明文的「數位指紋」。
 - ② **發送方簽章：**使用發送方自己的「私鑰 1」（非對稱金鑰對的一部分），對上述的「訊息摘要」進行加密（即簽章），產生「數位簽章」。這個簽章證明了訊息的來源及完整性。

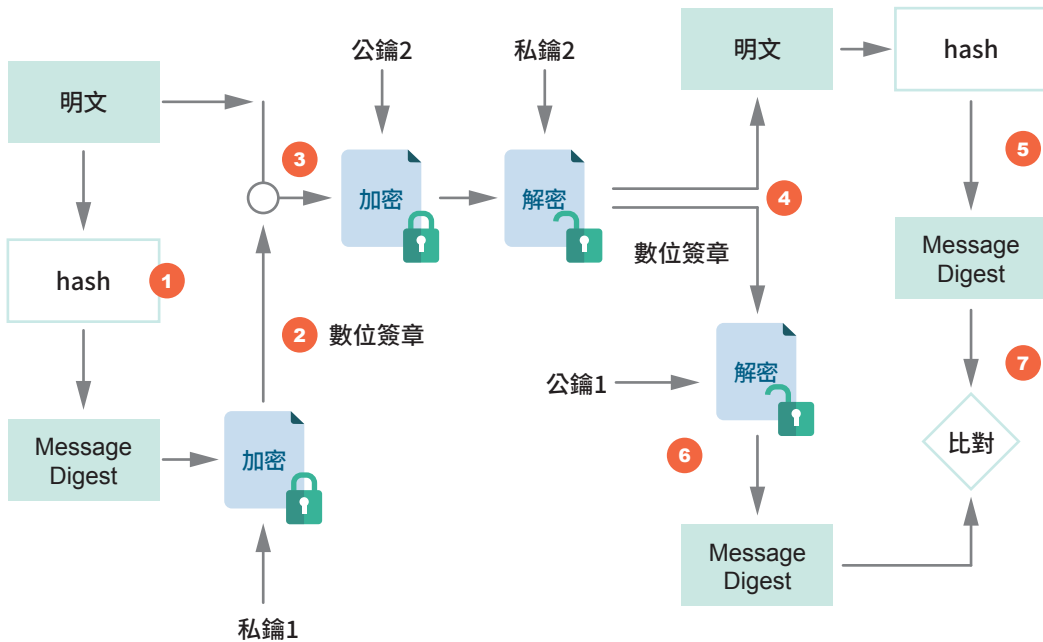


圖 36 數位簽章運作流程圖

③ 發送方選擇性加密與傳送：

- **加密明文（選用）：**若需確保訊息的機密性，發送方會使用接收方的「公鑰 2」（接收方的公開金鑰）對「明文」本身進行加密。這使得只有擁有對應私鑰（接收方私鑰 2）的人才能解讀明文。
- **傳送：**將加密後的「明文」（或未加密的明文），以及步驟 2 產生的「數位簽章」一同傳送給接收方。
- ◆ **接收方：**接收方的目標是驗證訊息的完整性和發送方身分，並在需要時解密明文。
- ④ **接收方解密明文（若已加密）：**若發送方在步驟 3 中加密了明文，接收方會使用自己的「私鑰 2」對收到的密文進行解密，以還原出原始的「明文」。
- ⑤ **接收方驗證訊息摘要：**對接收到的「明文」（無論是否經過解密）進行與發送方相同的雜湊運算，產生一個新的「訊息摘要」。
- ⑥ **接收方解密簽章：**使用發送方的「公鑰 1」（與發送方私鑰 1 配對的公開金鑰）對收到的「數位簽章」進行解密，從中還原出發送方簽章時所用的「訊息摘要」。

- 若兩者完全相同，則驗證成功，表示訊息內容在傳輸過程中未被篡改，且確實由發送方發出（完整性與不可否認性）。

系統與通訊保護是資安防護的核心環節。透過對稱式與非對稱式加密、數位信封、雜湊函式及數位簽章等技術的綜合運用，組織能夠有效地保護資訊在傳輸與儲存過程中的機密性、完整性與可用性，從而建立安全可靠的通訊環境。

MEMO

5.7

「系統與資訊完整性」之安全控制措施

系統與資訊完整性保護旨在確保資通系統及其儲存及處理的資訊不被非法篡改或破壞，從而維持資料的準確性、一致性與可靠性。這主要透過漏洞修復、系統監控與軟體及資訊完整性檢查來實現。

表 37 詳細列出針對不同防護等級的資通系統，在系統與資訊完整性構面下，關於漏洞修復、資通系統監控、軟體及資訊完整性的安全控制措施。

表 37 系統與資訊完整性構面之安全控制措施

措施內容	高	中	普
漏洞修復	1. 定期確認資通系統相關漏洞修復之狀態。 2. 等級「普」之所有控制措施		系統之漏洞修復應測試有有效性及潛在影響，並定期更新。
資通系統監控	1. 資通系統應採用自動化工具監控進出之通信流量，並於發現不尋常或未授權之活動時，針對該事件進行分析。 2. 等級「中」之所有控制措施	1. 監控資通系統，以偵測攻擊與未授權之連線，並識別資通系統之未授權使用。 2. 等級「普」之所有控制措施	發現資通系統有被入侵跡象時，應通報機關特定人員。
軟體及資訊完整性	1. 應定期執行軟體與資訊完整性檢查。 2. 等級「中」之所有控制措施	1. 使用完整性驗證工具，以偵測未授權變更特定軟體及資訊。 2. 使用者輸入資料合法性檢查應置放於應用系統伺服器端。 3. 發現違反完整性時，資通系統應實施機關指定之安全保護措施。	無要求

5.7.1 漏洞修復

漏洞修復是維護系統與資訊完整性的關鍵環節，旨在及時修補系統及應用程式中的安全漏洞，防止攻擊者利用這些缺陷進行入侵。

(1) **重要性：**及時修補系統及應用程式中的安全漏洞，可以防止攻擊者利用這些缺陷來破壞系統或竊取資訊。

(2) **實施方式：**

◆ **高中普等級：**

• **修復漏洞及定期更新：**

- 系統之漏洞修復應測試有效性及潛在影響，並定期更新。
- 定期進行軟體更新，先於測試用主機上完成更新可行性評估並通過測試後，始於正式環境進行更新。

◆ **高中等級：**

• **確認漏洞修復狀態：**

- 定期確認資通系統相關漏洞修復之狀態，並包含普等級之所有控制措施。
- 機關宜注意相關之安全漏洞訊息（如透過 CVE 相關訊息網站、廠商安全通告等）。
- 由弱點掃描與滲透測試等安全檢測活動所檢出之系統漏洞應設法修復，並定期追蹤修復進度，或配合定期之安全檢測作業確認複測。
- 稽核驗證宜檢視機關弱點修補追蹤管理機制

(3) **效益：**降低系統被利用的風險，維持系統的穩定性及安全性。

5.7.2 資通系統監控

(1) **重要性：**監控系統的運行狀況和資源使用情況，有助於及早發現異常行為或潛在的攻擊。

(2) **實施方式：**

◆ **高中普等級：**

• **監控通報**

- 發現資通系統有被入侵跡象時，應通報機關特定人員。

◆ **高中等級：**

- **監控資通系統連線：**
 - 監控資通系統，以偵測攻擊與未授權之連線，並識別資通系統之未授權使用，並包含普等級之所有控制措施。
- ◆ **高等級：**
 - **採用自動化監控工具：**
 - 資通系統應採用自動化工具監控進出之通信流量，並於發現不尋常或未授權之活動時，針對該事件進行分析，並包含中等級之所有控制措施。
 - 部署 IPS、IDS、WAF、防火牆等具備自動化監控能力之網路安全防護產品，以監控資通系統網路行為。
- (3) **效益：**提升對資安事件的感知能力，有助於快速反應及遏制潛在的威脅。

5.7.3 軟體及資訊完整性

- (1) **重要性：**確保軟體及資訊在儲存、傳輸及處理過程中，未被未經授權地修改，維持資料的準確性及可靠性。
- (2) **實施方式：**
 - ◆ **高中等級：**
 - **使用完整性驗證工具：**使用完整性驗證工具，以偵測未授權變更特定軟體及資訊。
 - **於伺服器端檢查：**使用者輸入資料合法性檢查應置放於應用系統伺服器端。
 - 輸入檢查 (Input Validation) 應實作於伺服器端，不可依賴客戶端檢查（如 JavaScript 等），以避免被惡意繞過。
 - **發現違反完整性時：**資通系統應實施機關指定之安全保護措施。
 - ◆ **高等級：**
 - **定期檢查完整性：**應定期執行軟體與資訊完整性檢查，並包含中等級之所有控制措施。
 - 定期比對上線正式版本與版本控制系統之版本之內容差異，以發現潛藏之資安事件。
- (3) **效益：**保證軟體及資訊的準確性及可靠性，防止資料被惡意竄改，維護業務運作的正常進行。

系統與資訊完整性保護是一個多層次的防護體系，涵蓋了漏洞修復、系統監控與軟體及資訊完整性檢查。透過這些措施的綜合運用，組織能夠有效地保護資訊資產的準確性與可靠性，確保資通系統的穩定運行。

5.7.4 資通系統防護基準 - 參考資源

為了協助組織提升資通安全防護能力，國家資通安全研究院網站 (www.nics.nat.gov.tw) 提供了一系列可自行下載的參考文件。表 38 資通系統防護基準參考資源列舉了多個參考文件，涵蓋資通系統防護基準驗證實務、Web 應用程式安全參考指引、安全軟體發展流程指引、安全軟體測試參考指引、安全軟體設計參考指引、安全控制措施參考指引，以及資通系統委外開發 RFP 範本等。這些資源是組織在實施資安防護時的寶貴指南。

表 38 資通系統防護基準參考資源

參考文件	用途說明
資通系統防護基準驗證實務	提供資通系統防護基準稽核驗證之參考
Web 應用程式安全參考指引	提供機關於 SSDLC 流程中於開發階段實作相關安全控制措施之參考
安全軟體發展流程指引	提供機關推動 SSDLC 流程之參考
安全軟體測試參考指引	提供機關於 SSDLC 流程中於測試階段進行安全檢測活動之參考
安全軟體設計參考指引	提供機關於 SSDLC 流程中設計階段進行威脅識別與風險評估活動之參考
安全控制措施參考指引	提供包含技術面與管理面等全面性安全控制措施之參考
資通系統委外開發 RFP 範本	提供機關委外開發資通系統之 RFP 參考範本

5.8

「媒體控管及可攜式設備」之安全控制措施

媒體控管與可攜式設備安全管理旨在防止儲存介質（如磁碟、磁帶、光碟、紙張）及可攜式設備（如 USB 硬碟、手機、筆記型電腦）中機敏資料的外洩，並防範其成為病毒感染的途徑。這是一個涵蓋資料生命週期各階段（使用、重用、丟棄）的安全管理範疇。

5.8.1 媒體控管的工作

- (1) **標示**：清楚標示媒體的資訊（名稱與版本、機密等級、建立者、建立日期、保存期限、應銷毀日期）。
- (2) **使用紀錄**：記錄媒體的使用情況。
- (3) **完整性檢查**：定期檢查媒體的資料完整性。
- (4) **實體存取保護**：限制未經授權人員對媒體的實體存取。
- (5) **存放環境保護**：確保媒體儲存環境的安全。
- (6) **運送保護**：確保媒體在運送過程中的安全。
- (7) **重用安全**：規範媒體重用前的資料清除。
- (8) **銷毀與丟棄**：規範媒體的最終銷毀。

5.8.2 媒體控管 - 標示

對儲存資訊的媒體進行清晰且完整的標示，是媒體控管的首要步驟。

- (1) **標示內容**：媒體上應清楚標示名稱與版本、機密等級、建立者、建立日期、保存期限、應銷毀日期。
- (2) **目的**：這些標示有助於使用者正確地處理媒體，例如依據機密等級採取相應的保護措施，並在達到保存期限後進行適當的處置。完善的標示是後續媒體管理工作（如使用紀錄、存取控制等）的基礎。

5.8.3 媒體控管 - 重用

在儲存媒體重複使用前，應注意下列安全事項，以避免資料殘留導致的資訊洩漏。

- (1) **儲存媒體被轉移**：當儲存媒體被轉移到不同安全等級之資通系統使用時，應將其原來的資料安全地刪除，以避免資料殘存的問題。
- (2) **刪除檔案或格式化是不夠安全的**：僅僅刪除檔案指標或格式化，不足以安全清除資料，磁區內的資料仍有機會被復原。
- (3) **安全的資料刪除方式**：常見的刪除作法包括：
 - ◆ **傳統硬碟 (HDD) 之單次覆寫 (Single Overwrite Pass)**：以單一字元（如所有 0）或隨機字元覆蓋所有使用者可定址的儲存空間。NIST 認為一次覆寫對於現代 HDD 已足夠。
 - ◆ **固態硬碟 (SSD) 之加密式清除 (Cryptographic Erase, CE)**：刪除加密金鑰。如 SSD 一直處於加密狀態，則刪除金鑰會使資料變得不可讀取，這是對 SSD 而言最快、最有效的方法。
 - ◆ **快閃記憶體 / 手機之原廠重設 (Factory Reset)**：透過裝置介面執行原廠重設 (Factory Reset)，但必須確認該操作包含對儲存空間進行覆寫或加密金鑰的刪除。

5.8.4 媒體控管 - 安全丟棄

在儲存媒體報廢或丟棄前，應採取下列安全措施，以防止資料洩漏。

- (1) **安全刪除或實體破壞**：媒體要丟棄或銷毀前，應先安全地刪除資料或進行實體的破壞。
- (2) **儲存媒體破壞方法**：
 - ◆ **磁碟機**：消磁設備或碎裂 (6mm)。
 - ◆ **磁帶**：消磁設備。
 - ◆ **光碟片**：碎裂 (6mm)。

5.8.5 可攜式設備 - 安全問題

可攜式設備，例如 USB 硬碟、手機及筆記型電腦，雖然提供了極大的便利性，但也伴隨著一系列潛在的資安風險。這些風險主要包括：

- (1) **資料外洩**：公務資料可能被員工不慎或故意攜出辦公場所而外洩。
- (2) **離職員工保留資料**：離職員工可能將工作相關資料複製到個人可攜式設備上，離職後仍持有這些資料，存在潛在的安全風險。
- (3) **病毒感染途徑**：普遍使用的 USB 硬碟成為病毒感染的主要途徑，容易在不同電腦之間傳播惡意軟體。

5.8.6 可攜式設備 - 存取控制與稽核

針對可攜式設備的存取控制及稽核要求，旨在降低其帶來的安全風險。

- (1) **政策**：應建立可攜式設備的使用限制與範圍，規範哪些設備可以使用、在哪些範圍內使用，以及禁止哪些行為。
- (2) **存取控制**：
 - ◆ 可攜式設備對機關資通系統的存取，應符合機關使用限制與範圍。
 - ◆ 應關閉或避免觸發自動執行可攜式媒體中的程式，以避免病毒的傳染。
- (3) **稽核**：應監視可攜式設備對資通系統的非授權存取，並記錄及監控可攜式設備的連接及使用情況，以及時發現及應對未經授權的存取行為。

5.8.7 可攜式設備 - 自動化安裝或啟用控管程式

可安裝或啟用可攜式媒體控管程式，可「管制」、「偵測」及「記錄」各種可攜式媒體與設備的存取行為。

5.8.8 可攜式設備 - 稽核記錄內容

稽核記錄應包含以下欄位：

- (1) 事件發生時間（例如：2017-11-12 11:34:12）
- (2) 電腦名稱或 IP 位址（例如：WIN-LAB-05 或 192.168.10.150）
- (3) 使用者名稱（例如：RUBICON-SECURE\steven）
- (4) 程式名稱與 ID（例如：Explorer.exe）
- (5) 設備名稱（例如：USB, CD/DVD, iPhone）
- (6) 動作（例如：Open, Write, Delete, CreateDir, etc...）
- (7) 檔名（例如：D:\autorun.inf）。

媒體控管與可攜式設備安全管理是防止資料外洩與惡意軟體傳播的重要防

MEMO

單元

6

資通安全技術面應辦事項
——資通安全之防護及偵測

在資通安全領域，除了完善的管理制度與人員意識外，具體的技術防護與偵測措施更是構築堅實資安防線的關鍵。面對日益複雜多變的網路威脅，組織必須部署各種安全技術工具，從源頭阻斷攻擊、即時偵測異常，並快速回應資安事件，以保護資訊資產免受侵害。

本單元將引導讀者深入了解資通安全技術面的各項應辦事項，從終端裝置的防毒軟體，到網路邊界的防火牆，再到進階的入侵偵測與回應系統。我們將探討這些技術的用途、運作原理、部署方式，以及管理重點，旨在為讀者提供實用的知識與實作指引，使其能夠在實際工作中有效運用這些防護與偵測工具。

本單元學習重點如下：

- 1 了解「防毒軟體」的用途、部署方式、管理重點與選購考量。
- 2 掌握「網路防火牆」的定義、用途、部署方式與管理關鍵。
- 3 理解「應用程式防火牆 (WAF)」的運作原理、偵測技術與管理考量。
- 4 認識「電子郵件過濾機制」的判斷技術、部署方式與選購重點。
- 5 學習「入侵偵測系統 (IDS) 與入侵防禦系統 (IPS)」的技術類型、反應方式與比較。
- 6 探討「進階持續性威脅 (APT)」攻擊的特色、防禦措施與管理策略。
- 7 了解「資通安全威脅偵測管理機制 (SOC)」的核心目標、服務與聯防機制。
- 8 認識「政府組態基準 (GCB)」的組態管理、導入方式與類別項目。
- 9 掌握「政府機關資安弱點通報機制 (VANS)」的目的、服務與資訊資產涵蓋範圍。
- 10 了解「端點偵測及回應系統 (EDR)」的用途、技術類型與選購考量。
- 11 了解「防毒軟體」安全防護。

6.1

「防毒軟體」之安全防護

防毒軟體是資通安全防護中最基礎且不可或缺的工具，其主要目的是防止惡意程式（如病毒、蠕蟲、間諜軟體、後門程式及木馬程式等）入侵電腦軟體或系統，不僅保護單一電腦，也維護整個網路環境的安全。

防毒軟體的核心功能是偵測，並清除各種惡意程式。

- ◆ **病毒 (Virus)**：惡意程式碼片段，透過感染其他合法程式或檔案進行傳播，並在執行時造成破壞。
- ◆ **蠕蟲 (Worm)**：獨立運行的惡意程式，能透過網路自我複製與傳播，通常不需要使用者互動，即可造成大規模感染。
- ◆ **間諜軟體 (Spyware)**：旨在監控使用者行為、竊取個人資訊並秘密傳送出去，通常在使用者不知情的情況下運行。
- ◆ **後門程式 (Backdoor)**：允許攻擊者繞過正常身分驗證機制，遠端控制受感染的系統。
- ◆ **木馬程式 (Trojan Horse)**：偽裝成合法軟體，誘騙使用者下載並執行，一旦運行則會執行惡意行為。

6.1.1 惡意程式的來源

惡意程式的來源多種多樣，常見的傳播途徑包括：

(1) 電子郵件：

- ◆ 惡意程式最**常見**的傳播途徑，透過釣魚郵件、惡意附件或惡意連結進行傳播。
- ◆ 使用者應警惕不明郵件，不隨意點擊連結或開啟附件。

(2) USB 硬碟：

- ◆ 作為可移動儲存裝置，容易成為惡意程式的傳播媒介。
- ◆ 應在插入不明 USB 硬碟前進行掃描。

(3) 網站瀏覽：

- ◆ 惡意網站、掛馬網站或惡意廣告可能在使用者不知情的情況下植入惡意

程式。

- ◆ 應避免瀏覽不明網站或點擊可疑連結。

(4) 即時通訊：

- ◆ 透過即時通訊軟體傳送的檔案或連結也可能是惡意程式來源。
- ◆ 使用者應警惕透過即時通訊軟體收到的內容。

(5) 檔案傳輸 / 分享：

- ◆ P2P 軟體、雲端分享或網路芳鄰分享檔案時，也可能不小心下載或傳播惡意檔案。
- ◆ 應在分享前進行掃描。

6.1.2 防毒軟體 - 部署方式

防毒軟體的部署方式應涵蓋組織的各個層面，以建立多層次防護。

(1) 個人電腦與伺服器防毒：

- ◆ 個人電腦上的防毒軟體主要保護單一使用者設備。
- ◆ 伺服器防毒則著重於保護企業核心服務與資料，通常會提供更強大的集中管理功能。
- ◆ 強調兩者相輔相成，構成基礎防禦。

(2) 電子郵件防毒閘道：

- ◆ 在組織網路邊界 (DMZ 網段) 部署電子郵件防毒閘道 (如 SMTP AntiVirus)。
- ◆ 在郵件進入內部網路前，對所有進出郵件進行掃描及過濾，有效阻擋郵件惡意程式。
- ◆ 這是第一道重要的防線，可大幅降低內部網路的風險。

(3) 上網防毒閘道：

- ◆ 在內部網路與網際網路間部署上網防毒閘道 (如 HTTPS/FTP/POP3 AntiVirus)。
- ◆ 監控並掃描所有透過 HTTPS、FTP、POP3 等協定進行的網路流量。
- ◆ 在使用者瀏覽網頁或下載檔案時，即時阻擋惡意內容。
- ◆ 與電子郵件防毒閘道類似，也是一道重要的網路邊界防線。



(4) 防毒軟體 - 部署說明：如圖 37 防毒軟體部署方式示意圖。

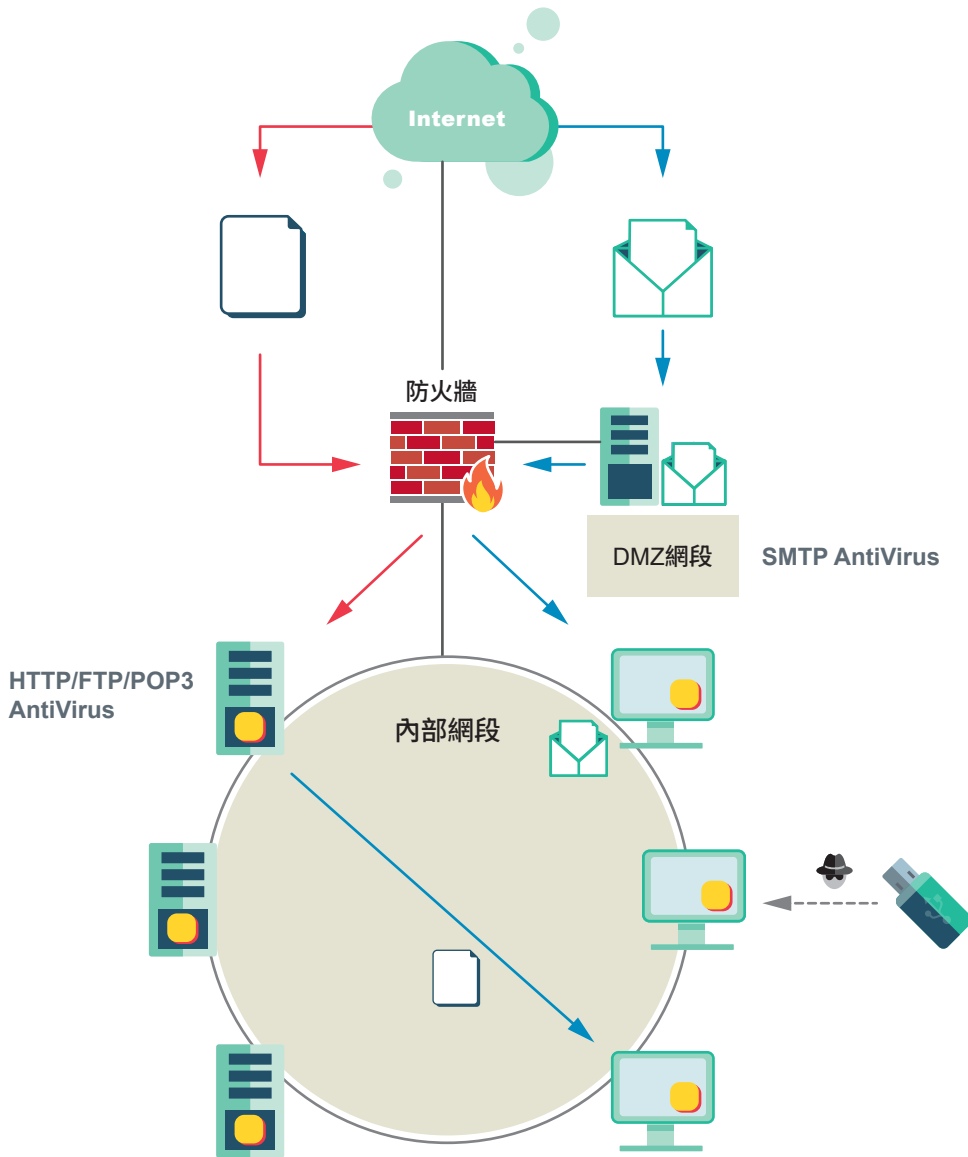


圖 37 防毒軟體部署方式示意圖

- ◆ **整體架構：**這張圖展示了一種多層次的安全防禦體系。透過防火牆作為第一道防線，DMZ 作為緩衝區隔離對外服務，以及在內部網路中部署額外的安全掃描（如防毒伺服器），共同保護組織的內部網路免受來自網際網路的威脅。以下是各部分的解釋：

- ◆ **網際網路：**

這是組織外部的公共網路，所有對外或對內的通訊都經由這裡。

◆ **防火牆：**

- 防火牆是網路安全的核心設備，像一道門衛，依據預設的安全規則，檢查並過濾所有進出網路的資料流量。
- 防火牆會阻擋惡意或未經授權的流量，同時允許正常的通訊通過。圖中的**紅線及藍線**顯示了資料流經防火牆。

◆ **非軍事區 (Demilitarized Zone, DMZ)：**是一個隔離區，專門放置需要對外部網路提供服務的伺服器。主要目的是增加安全性，即使 DMZ 內的伺服器被攻擊，攻擊者仍需再次突破防火牆才能進入更為敏感的內部網路。

- **SMTP AntiVirus 伺服器：**位於 DMZ 中，主要負責處理組織的電子郵件 (SMTP)，並對其進行病毒掃描。**藍色箭頭**表示郵件的流向。

◆ **內部網段：**這是組織的私有、安全的網路，承載著大部分內部使用者及敏感資料。

- **HTTPS/FTP/POP3 AntiVirus 伺服器：**這台伺服器位於內部網段，負責處理內部使用者的網頁瀏覽 (HTTPS)、檔案傳輸 (FTP) 及收到的電子郵件 (POP3)，並進行病毒及惡意軟體掃描。**紅色箭頭**可能表示 HTTPS/FTP/POP3 資料從網際網路進入內部網段後，需要經過這台伺服器掃描。
- **其他伺服器 / 電腦：**圖中有許多帶綠色方塊的電腦螢幕及伺服器，代表了內部網路中的使用者工作站及提供各種內部服務的伺服器。
- **USB 隨身碟：**這個圖示提醒我們，資料也可以透過實體媒介（如 USB 隨身碟）進出內部網路，這也是潛在的安全風險點，需要注意防範惡意軟體傳播。

圖 36 展示了防毒軟體在不同網路區域的部署位置，包括個人電腦、伺服器、電子郵件閘道及上網閘道，形成了多層次的防護。

6.1.3 防毒軟體 - 管理重點

有效的防毒軟體管理與謹慎的選購，是確保其防護效能的關鍵。

- (1) **定期自動更新病毒碼：**確保防毒軟體能夠有效偵測新興威脅，過舊的病毒碼會使防毒軟體形同虛設。
- (2) **病毒感染事件與趨勢定期分析：**定期檢視防毒軟體日誌，了解感染類型、來源與數量，有助於調整資安策略，預防未來攻擊。



- (3) **避免未安裝防毒軟體的電腦上線（配合 NAC 設備）：**未受保護的設備是網路破口，應導入網路存取控制 (NAC)，強制檢查設備是否符合安全規範。
- (4) **防火牆控管未經防毒閘道過濾的連線行為：**防火牆是網路邊界守衛，應確保所有關鍵流量（如郵件、網頁下載）必須先經防毒閘道掃描過濾，才能進入內部網路。
- (5) **採用不同廠牌：**「個人電腦與伺服器防毒系統」與「防毒閘道系統」可採用不同廠牌，以增加防護的多樣性，避免單一廠商的漏洞導致全面失效。這是資安「縱深防禦」的應用。

6.1.4 選購考量

- (1) **病毒偵測的精準度：**這是防毒軟體最基礎也是最重要的功能，應關注偵測率與誤報率，參考第三方獨立測試報告。
- (2) **對電腦效能的影響：**防毒軟體在執行時不應過度佔用系統資源，導致電腦變慢，影響使用者體驗。需找到防護能力與效能影響的最佳平衡點。
- (3) **是否提供中央控管機制：**對於組織而言，集中管理是效率與安全並行的關鍵。中央控管機制應能統一派送更新、設定策略、監控各端點狀態及處理事件，大幅降低管理成本與複雜度。

防毒軟體是資安防護體系中的第一道防線。透過全面的部署、嚴謹的管理與精明的選購，組織能夠有效地抵禦惡意程式的入侵，保護資訊資產安全。

6.2

「網路防火牆」之安全防護

網路防火牆是資通安全技術面防護的核心組件之一，作為網路邊界的守門員，其主要職責是依據特定的規則允許或限制資料的傳輸，是一台專屬的硬體設備，或是架設在一般硬體上的軟體。

6.2.1 主要用途

網路防火牆的主要用途包括網路區隔、資料封包過濾，以及提供稽核與控制功能：

- (1) **區隔不同安全等級網段：**防火牆最基本且最重要的用途，是將網路環境劃分為不同的安全區域，如：
 - ◆ **外部網路 (Internet)：**公眾區域，風險最高。
 - ◆ **內部網路 (LAN)：**企業內部辦公網，信任度高，需嚴格保護。
 - ◆ **DMZ 區 (Demilitarized Zone)：**非軍事區，用於放置對外服務的伺服器（如網站、郵件伺服器），即使遭到入侵也能有效阻止攻擊者直接進入內部網路，形成多層防護。
- (2) **過濾資料封包：**避免未經授權存取內部網路資源。防火牆能精準控制資料封包的來源 IP、目的 IP、通訊埠號 (Port) 及協定 (Protocol) 等資訊，阻擋非法連線嘗試。
- (3) **提供稽核與控制存取網路資源：**防火牆具備詳盡的日誌記錄功能，能記錄所有被允許或被拒絕的網路連線行為。這些日誌對於資安事件的追溯、分析異常流量模式，以及進行日常網路行為稽核非常重要，並能透過分析調整防火牆規則，強化安全策略。
- (4) **網路防火牆 - 部署說明：**如圖 38 網路防火牆部署範例。這張圖展示了一個典型且強固的多層次網路安全架構：
 - ◆ **外部流量過濾：**所有來自網際網路的流量首先會經過路由器，然後到達防火牆。
 - ◆ **防火牆的嚴格控制：**防火牆是關鍵的流量檢查點，只允許經過明確許可



的服務 (HTTPS 及 Mail) 進入 DMZ。所有試圖直接進入內部網路的流量都被阻擋。

- ◆ **DMZ 的隔離作用：**公開服務（郵件及網站）被放置在 DMZ 中，以保護內部網路免受直接攻擊。
- ◆ **內部網路的保護：**內部網路與 DMZ 及網際網路嚴格分離，最大限度地降低了外部威脅的風險。

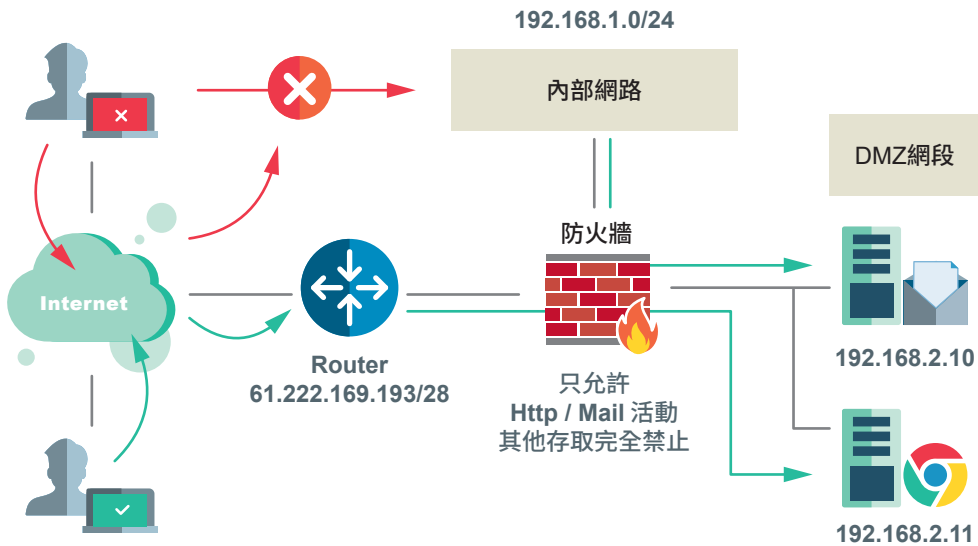


圖 38 網路防火牆部署範例

以下是各部分的解釋：

- **網際網路：**這是組織外部的公共網路，代表了來自全球的網路流量。圖中上方有筆記型電腦及伺服器的圖示，代表了外部使用者或服務。
- **路由器 (Router)：**路由器是連接內部網路與外部網際網路的設備。圖中顯示其公共 IP 位址為 61.222.169.193/28，這是一個 IP 位址範圍，用於對外連線，負責將資料包從一個網路轉發到另一個網路。
- **防火牆 (Firewall)：**防火牆是網路安全的核心設備，位於路由器與內部網路間，嚴格控制資料流量。圖中防火牆上的紅色「X」清楚地表示，所有從網際網路直接嘗試連線到內部網路的流量都被阻擋，這是一個關鍵的安全策略。
- **安全規則：**圖中明確標示「只允許 Web / Mail 活動，其他存取完全禁止」。這意味著防火牆被配置為：

- 只允許網頁瀏覽 (Web) 及電子郵件 (Mail) 相關的流量通過。
- 除了這兩類活動，所有其他來自外部的存取都被完全禁止，大大提升了內部網路的安全性。
- **DMZ 網段：DMZ (Demilitarized Zone)** 是一個隔離區，專門用於放置需要對外部網路提供服務的伺服器，同時又與內部網路分離。其目的是將這些對外開放的服務與組織的敏感內部資料隔離開來，形成一個緩衝地帶。即使 DMZ 內的伺服器被入侵，攻擊者仍需突破另一道防線才能進入內部網路。
- **Mail 伺服器：**IP 位址為 192.168.2.10，負責處理電子郵件服務。
- **Web 伺服器：**IP 位址為 192.168.2.11，負責提供網頁服務。
- 綠色箭頭顯示來自網際網路的 HTTPS 及 Mail 流量被引導至 DMZ 中的相應伺服器。
- **內部網路：**這是組織的私有、安全的網路，其 IP 位址範圍為 192.168.1.0/24。這是員工日常工作及儲存敏感資料的地方。
- **紅色「X」箭頭：**再次強調，外部網路無法直接存取內部網路，這是防火牆的主要作用之一。
- **綠色箭頭：**表示內部網路可以發起連線到 DMZ 或透過路由器存取網際網路，但其連出流量也可能受到防火牆規則的限制。

6.2.2 部署方式

網路防火牆的部署應考量資安需求，妥善劃分 IP 網段與虛擬區域網路，並確保其高可靠度運作。

(1) 考量資安需求，妥善劃分 IP 網段與虛擬區域網路：

在部署防火牆前，需深入評估組織資安需求，了解哪些資料最重要、哪些服務必須對外提供，以及潛在的威脅來源。依據資安需求，將網路環境進行邏輯上的分區，常見做法是劃分為不同的 IP 網段（如財務部門、研發部門、來賓網路等），並利用「虛擬區域網路 (VLAN)」技術進一步隔離不同部門或不同性質的流量。透過精細的網段劃分與 VLAN，可以限制橫向移動攻擊，即使一個區域被入侵，也難以迅速擴散到其他重要區域。

(2) 建置 2 台防火牆並設定成高可靠度 (High Availability) 運作模式：

當主要防火牆出現問題時，次要防火牆即能接手主要防火牆的工作，如圖

39 網路防火牆 HA 部署示意圖。

- ◆ **單點失效風險**：防火牆是網路的關鍵節點，一旦故障，可能導致網路癱瘓或門戶大開，造成業務中斷或資安風險大增。

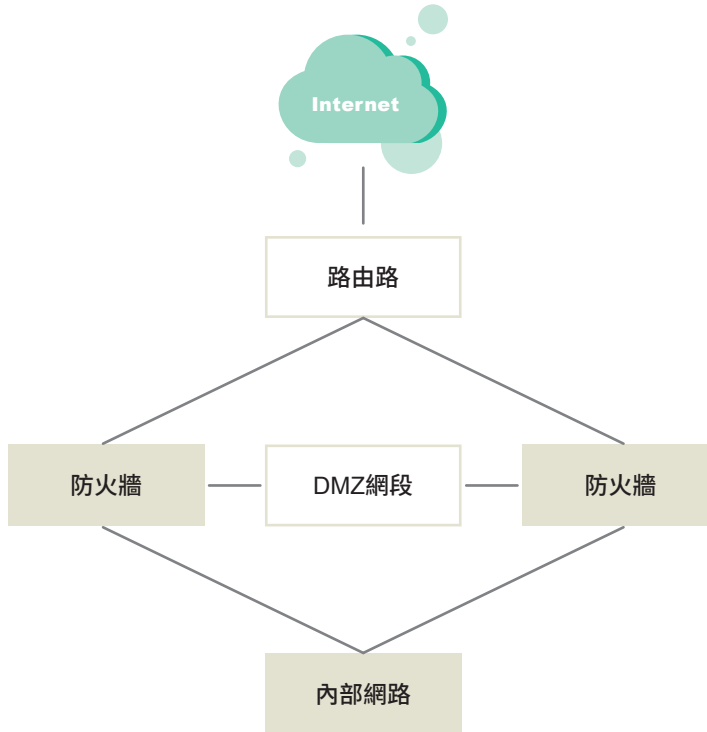


圖 39 網路防火牆 HA 部署示意圖

- ◆ **高可靠度 (HA)**：為了解決單點失效問題，建議部署兩台防火牆，並將它們配置成「高可靠度 (HA)」模式。
- ◆ **運作原理**：HA 模式下，通常一台防火牆作為「主要 (Active)」設備負責處理所有流量，另一台作為「備援 (Standby)」設備。當主要防火牆因故障時，備援防火牆會立即自動接手，無縫地繼續提供網路防護服務。
- ◆ **效益**：確保網路服務的連續性及資安防護的韌性，最大限度地減少因防火牆故障而造成的業務停擺或資安漏洞。

6.2.3 管理重點

有效的網路防火牆管理與謹慎的選購，是確保其防護效能與網路穩定性的關鍵。

- (1) **防火牆存取規則的變更管理程序：**變更（新增、修改、刪除）任何防火牆規則，都直接影響網路安全。務必建立標準的「變更申請、核准及記錄」流程，確保所有變更皆經授權且有跡可循。
- (2) **防火牆存取紀錄的即時匯出與保留：**日誌是資安事件調查與稽核的關鍵證據。應設定防火牆將存取日誌「即時匯出」到安全的集中式日誌伺服器，並保留足夠長度的時間。
- (3) **定期產出異常存取統計分析報表：**定期分析異常連線次數或被阻擋的惡意流量，及時發現潛在威脅，從被動防禦轉為主動應變。
- (4) **防火牆存取控管規則定期盤查：**規則會隨業務變化累積，需定期「全面審查所有規則」（例如 A 級機關每年 1 次，B 級機關兩年 2 次），檢查規則的有效性、是否冗餘或存在衝突，並移除不必要的規則。

6.2.4 選購考量

- (1) **防火牆本身的安全性：**防火牆本身若有漏洞，將成為攻擊目標。應選擇安全可靠且持續有維護的品牌，考量廠商信譽、產品安全更新頻率、是否經過第三方認證。
- (2) **可區隔的網路區段數：**評估防火牆是否支援「足夠的實體網路埠數量」，以靈活劃分內部網路、DMZ、來賓網路等多個安全區域，滿足當前與未來網路架構需求。
- (3) **可支援的傳輸頻寬大小：**防火牆是網路閘道，其「吞吐量」直接影響網路速度。需依據組織的總流量、尖峰流量，以及未來擴充需求，選擇具備足夠處理能力的防火牆，避免造成網路瓶頸。

網路防火牆是資通系統防護中不可或缺的邊界防禦。透過正確的部署、嚴謹的規則管理與持續的監控，組織能夠有效區隔網路、過濾流量，從而保護內部資源，建立堅固的資安邊界。

6.3

「應用程式防火牆」之安全防護

6.3.1 角色及運作原理

- (1) **定義與角色：**應用程式防火牆是一種專門針對「應用層封包」進行管控的防火牆機制。與傳統網路防火牆主要著重於網路層與傳輸層的 IP/Port 過濾不同，能更深入地檢查應用層的內容，主要專注於偵測與防禦針對網站應用程式的攻擊行為，如 SQL Injection 與 Cross-Site Scripting 等
- (2) **專注對象：**這種防火牆特別專注於「網站應用程式」的防護。因此，最常見的名稱是「網站應用程式防火牆 (Web Application Firewall, WAF)」。
- (3) **區別與互補：**強調 WAF 與傳統網路防火牆是互補而非取代關係。網路防火牆負責阻擋非法連線，而 WAF 則在合法連線中尋找惡意應用層攻擊。
- (4) **運作原理：**如圖 40 應用程式防火牆示意圖
 - ◆ 圖中顯示 HTTP 流量（來自多種來源）流向網站應用程式。
 - ◆ WAF 位於 HTTP 流量與網站應用程式之間，充當守門員。
 - ◆ 藍色箭頭表示合法流量可通過 WAF。
 - ◆ 紅色箭頭表示惡意流量會被 WAF 偵測並阻擋，無法到達網站應用程式。

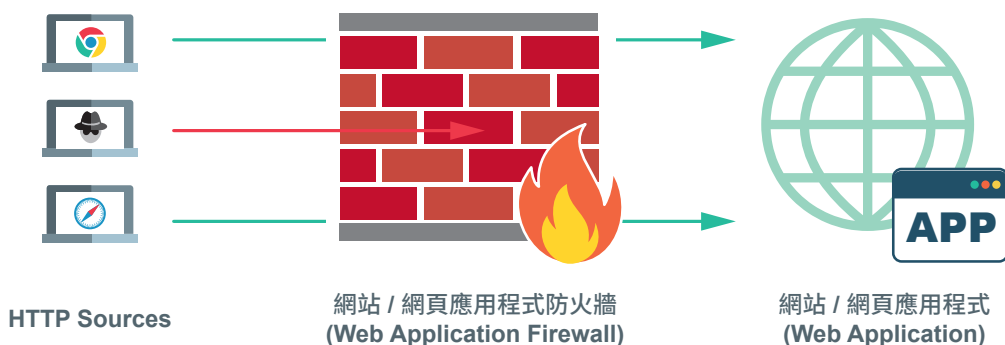


圖 40 網站 / 網頁應用程式防火牆示意圖

6.3.2 用途

- (1) **WAF 的核心用途**是「偵測並阻擋」針對網站應用程式層的惡意攻擊。
- (2) **常見攻擊類型**：舉例來說，WAF 能有效防禦如「SQL Injection(SQL 注入攻擊)」，這類攻擊試圖透過惡意 SQL 語句來操控或竊取資料庫內容；以及「Cross-Site Scripting (XSS，跨站腳本攻擊)」，利用在網頁中注入惡意腳本來竊取使用者資料或劫持會話。
- (3) **廣泛防禦**：除了上述兩種，WAF 還能防禦如路徑遍歷、遠端檔案包含、命令注入等 OWASP Top 10 中列出的其他應用層威脅。

6.3.3 偵測與過濾技術

WAF 採用多種技術來判斷流量是否為惡意攻擊。

- (1) **白名單 (Whitelist)**：只允許列在白名單的網頁與參數通過，其他一律拒絕。理論上最安全且可防範未知攻擊，但實務上難以學習到 100% 的白名單，容易造成誤擋。
- (2) **黑名單 (Blacklist)**：列在黑名單的網頁與參數一律拒絕。實施相對容易，對於已知攻擊模式防禦效果好，但無法防禦未知或變種的攻擊。
- (3) **攻擊特徵判斷 (Signature-based Detection)**：目前較常用的作法，基於龐大的已知攻擊特徵碼資料庫。偵測效率高且準確，但會有誤判與漏判的問題，且需要定期更新特徵碼資料庫。

6.3.4 類型與部署方式

WAF 可以分為硬體式及軟體式，兩者在部署、效能及成本上有所不同。

- (1) **硬體式 (Appliance-based) WAF**：如圖 41 硬體式 WAF 部署示意圖
 - ◆ **部署**：獨立的專用硬體設備，部署在網路關鍵位置，通常在網際網路流量進入實際的 Web 伺服器群組之前，扮演「反向代理」角色。
 - ◆ **優點**：高性能與高吞吐量，能處理大量網路流量並進行深度內容檢查，對後端 Web 伺服器效能影響小，部署相對簡單。
 - ◆ **適用情境**：大型企業、擁有大量 Web 應用程式或高流量網站的組織。

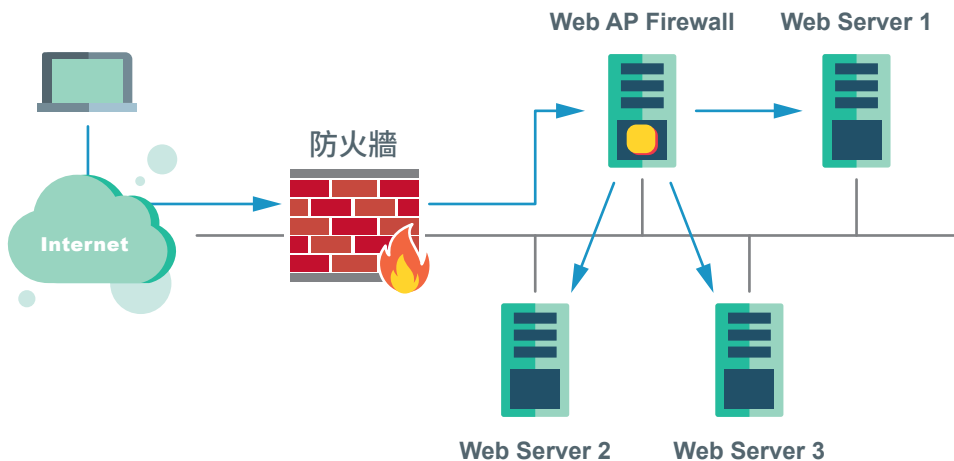


圖 41 硬體式 WAF 部署示意圖

(2) 軟體式 (Software-based) WAF：圖 42 軟體式 WAF 部署示意圖

- ◆ **部署**：安裝在 Web 伺服器上，作為應用程式或模組，直接在 Web 伺服器內部運行，過濾所有進出該伺服器的 HTTP/HTTPS 流量。
- ◆ **優點**：部署彈性高，成本相對較低，與應用程式整合度高。
- ◆ **考量**：與 Web 伺服器共享資源，可能對伺服器效能造成影響；管理上可能需要逐一配置及維護，複雜度會增加。

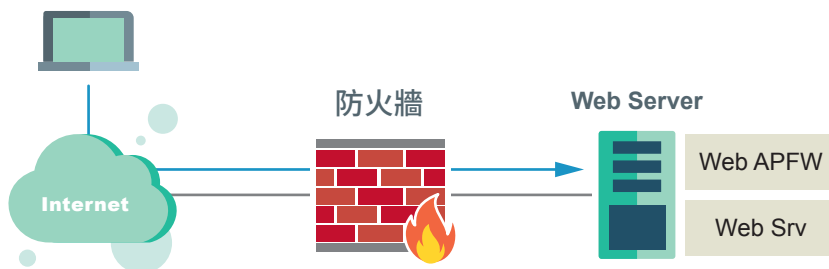


圖 42 軟體式 WAF 部署示意圖

6.3.5 管理重點

有效的 WAF 管理與謹慎的選購，是確保其防護效能的關鍵。

- (1) **存取規則的變更管理**：應建立管理程序（變更申請、核准及記錄），確保任何規則變更都經過審慎評估。

- (2) **異常網站應用程式攻擊事件的匯出與分析：**異常事件應立即匯出並保留足夠時間，定期分析以識別攻擊趨勢與手法。

6.3.6 選購考量

- (1) **處理效能：**應符合機關網站流量需求，避免成為性能瓶頸。
- (2) **中文 URL 及傳輸內容的判斷能力：**對於處理中文語系網站的 WAF 尤其重要，確保其對中文編碼的解析與判斷能力良好。
- (3) **HTTPS 加密連線的解密與過濾能力：**WAF 應能對 HTTPS 流量進行解密、檢查與過濾後再加密轉傳，確保加密流量中的威脅也能被有效防禦。

應用程式防火牆是 Web 應用程式安全的關鍵防線。透過對其技術原理、部署方式、偵測技術與管理重點的深入理解，組織能夠有效地保護其 Web 應用程式免受複雜的應用層攻擊，提升整體資安韌性。

MEMO

6.4

「電子郵件過濾機制」之安全防護

電子郵件過濾機制，一般指具垃圾郵件過濾之系統 (Anti-Spam System)，其主要目的在於識別並阻擋未經請求、批量發送的垃圾郵件，以及帶有惡意意圖（如釣魚郵件、病毒附件）的郵件，是郵件安全的第一道防線。

6.4.1 用途

電子郵件過濾機制的用途主要有兩方面：

- (1) **過濾垃圾與廣告郵件：**大幅減少使用者信箱中的垃圾郵件及不請自來的廣告郵件，提升郵件使用體驗，同時減少使用者處理無用郵件的時間，並降低信箱儲存空間的佔用，減少使用者不小心點擊惡意廣告的風險。
- (2) **避免電子郵件社交工程攻擊：**這是最重要的安全用途。過濾機制能夠識別釣魚郵件、詐騙郵件等利用心理弱點進行的社交工程攻擊。這些攻擊郵件通常偽裝成可信任的來源，誘騙收件人點擊惡意連結、下載惡意附件或洩露敏感資訊。

6.4.2 垃圾郵件判斷技術

電子郵件過濾機制採用多種技術來判斷郵件是否為垃圾郵件或惡意郵件：

- (1) **連線模式：**判斷寄件伺服器的 IP 位址、連線頻率、連線行為模式（例如，來自已知惡意 IP 位址的連線、或在短時間內發送大量郵件的伺服器）。
- (2) **關鍵字比對：**檢查郵件的主旨和內容是否包含常見的垃圾郵件關鍵字或詞組（如「中獎」、「免費」、「快速致富」等）。由於攻擊者不斷變化關鍵字，需要定期更新關鍵字庫。
- (3) **內容過濾條件：**更精細地分析郵件內容，例如郵件的格式、標頭資訊、附件類型等，偵測標頭是否偽造、郵件是否包含可疑的 HTML 語法、是否夾帶可執行檔案附件等。
- (4) **外部資料庫比對：**將寄件者的 IP 位址、網域名稱或郵件內容雜湊值與外部

的黑名單資料庫（如 RBL, Real-time Blackhole List）進行比對，快速且大規模地識別來自已知垃圾郵件發送者的郵件。

- (5) **貝氏演算法 (Bayesian Algorithm)**：透過分析大量垃圾郵件及正常郵件的詞彙頻率，建立判斷模型，計算特定詞彙出現在垃圾郵件或正常郵件中的機率，具備學習能力，可透過使用者標記訓練過濾器，使其判斷越來越精準。
- (6) **圖片辨識技術**：針對利用圖片傳播垃圾郵件或惡意資訊的行為。過濾器會分析圖片內容，例如圖片中是否包含文字、是否與已知惡意圖片相似等，有效對抗圖片垃圾郵件。

6.4.3 部署方式

電子郵件過濾機制的部署方式會影響其效能、安全性及故障時的行為，常見有匣道模式及 Bridge 模式。

- (1) **匣道模式 (Mail Relay)**：如圖 43 匣道模式部署示意圖。

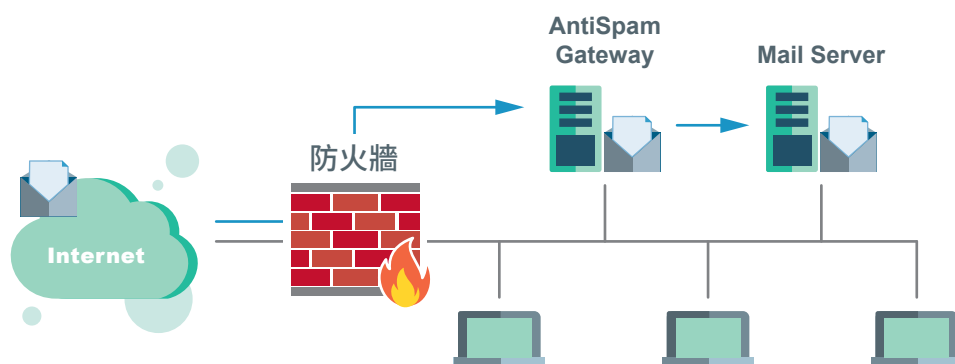


圖 43 匣道模式部署示意圖

- ◆ **部署**：部署在網際網路與內部郵件伺服器之間，作為郵件的「中繼站」。所有進出組織的郵件流量，都必須先通過這個閘道設備進行過濾與檢查。
- ◆ **優點**：不影響其他網路流量，因其只處理郵件流量；安全性高 (Fail Close)，設備故障時信件無法進出，確保安全，但可能造成服務暫時中斷。
- ◆ **適用情境**：對於郵件安全性要求極高，且能接受短暫服務中斷風險的企業。



(2) Bridge 模式（目前較少見）：如圖 44 Bridge 部署示意圖。

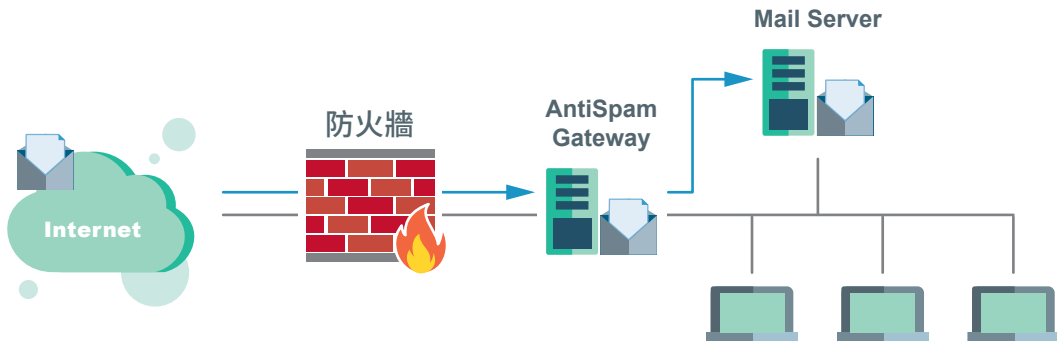


圖 44 Bridge 部署示意圖

- ◆ **部署**：直接部署在網路線路上，作為「橋接器」，不改變原有網路拓樸及 IP 設定，設備僅進行監聽及過濾。
- ◆ **缺點**：會影響其他網路流量，因其處於網路路徑上；安全性低 (Fail Open)，設備故障時會自動 Bypass 流量，優先確保網路連通性，但安全性暫時降低。
- ◆ **適用情境**：對於網路連通性要求極高，且能接受在設備故障時犧牲部分安全性的情境（但目前在企業環境中已較不常用）。

6.4.4 管理重點

- (1) **定期自動更新垃圾郵件辨識特徵碼**：確保郵件過濾系統能夠識別最新的垃圾郵件變種及釣魚手法。
- (2) **電子郵件過濾規則的變更管理程序**：應建立「變更申請、核准及記錄」的標準作業流程，確保所有規則調整都有嚴謹的管控與追溯機制。

6.4.5 選購考量

- (1) **垃圾郵件判斷的精準度**：核心功能，需考量「垃圾郵件偵測率」（成功阻擋比例）及「誤判率」（正常郵件誤標比例）。
- (2) **處理效能**：需符合機關郵件流量需求，避免導致郵件延遲或服務中斷。
- (3) **中文信件或多國語言的支援能力**：考量到台灣或跨國企業處理中文或多國語言郵件的需求，確保編碼解析、關鍵字判斷、內容分析能力良好。

- (4) **全文檢索支援能力：**支援中文全文檢索及郵件附件的檢索能力，滿足資安事件追溯及稽核需求。
- (5) **圖片廣告信件的支援能力：**具備圖片辨識技術，能夠分析圖片中的文字或特徵，有效偵測並阻擋這類郵件。

電子郵件過濾機制是資通安全防護中針對郵件威脅的重要技術。透過對其用途、判斷技術、部署方式、管理重點與選購考量的全面理解，組織能夠有效地阻擋垃圾郵件、防範社交工程攻擊，並維護郵件通訊的清潔與安全。

MEMO

6.5

「IDS 與 IPS」之安全防護

入侵偵測系統 (Intrusion Detection System, IDS) 入侵防禦系統 (Intrusion Prevention System, IPS) 是網路安全中重要的偵測與防禦工具，旨在識別網路中的異常行為與攻擊行為。兩者雖然目的相似，但在功能、反應方式及部署上有所不同。

6.5.1 用途

- (1) **識別異常與攻擊行為**：IDS 及 IPS 的主要功能是「識別網路中的異常行為與已知的攻擊行為」，會持續監控網路流量或系統活動，尋找潛在的威脅跡象。
- (2) **IPS 阻擋**：特別是 IPS，一旦識別到「特定的攻擊行為」，可以立即採取「阻擋」動作，例如中斷惡意連線或丟棄惡意封包，防止攻擊成功。
- (3) **SSL/TLS 加密連線限制**：注意一個重要的限制是，IDS/IPS 在未進行解密的情況下，無法識別 SSL 加密連線（如 HTTPS、SMTPS、FTPS 等）中的內容，因此攻擊者可以藉由加密流量來隱藏惡意行為。儘管如此，IDS/IPS 仍可針對未加密或可成功解密的流量，識別及即時阻擋已知的攻擊行為。若攻擊行為藏於未經解密的 SSL/TLS 隧道中（不僅用於 HTTPS，同樣適用於其他受保護協定如 SMTPS、FTPS 等），其內容將無法直接被 IDS/IPS 分析及阻擋。

6.5.2 技術類型

IDS 及 IPS 主要採用以下幾種技術，以偵測異常與攻擊：

- (1) **特徵碼比對 (Signature-based Detection)**：
 - ◆ **原理**：這是最常見的偵測方式，透過「比對攻擊特徵碼」來判斷是否存在攻擊。系統內建一個龐大的已知攻擊模式資料庫（如病毒碼、蠕蟲特徵、特定攻擊指令序列）。

- ◆ **優點：**針對「已知攻擊」，判斷精準度高，誤報率相對較低。
- ◆ **限制：**「只能偵測已知攻擊」。若新型的、變種的或尚未收錄到特徵碼庫中的「零日攻擊 (Zero-day attack)」，則無法有效偵測。

(2) 異常行為模式分析 (Anomaly-based Detection)：

- ◆ **原理：**這種方法不依賴已知特徵碼，而是透過「統計分析比對出異常行為」。系統會先建立正常網路流量或系統行為的「基準」，任何偏離此基準的活動都會被標記為異常。
- ◆ **優點：**能夠「偵測未知類型攻擊」，對於新型或變種的威脅具有較好的防禦能力。
- ◆ **挑戰：**相對「容易誤判」。若正常行為模式發生變化（例如新增服務、大量正常流量湧入），可能被誤認為異常而發出警報，需要較長時間的學習與調校。

(3) 狀態協定分析 (Protocol Anomaly Detection)：

- ◆ **原理：**事先定義「完整且正確的通訊協定行為規範」。IDS/IPS 會監控網路流量是否符合這些協定標準，任何「違反協定規範的行為」都會被視為異常或潛在攻擊。
- ◆ **優點：**這種方式「較為精準」，且能有效「偵測未知類型攻擊」，因為它不依賴特定的攻擊特徵，而是檢查行為是否合規。
- ◆ **挑戰：**通常「耗費較多運算資源」，因為需要深度解析及維護每個通訊協定的狀態，可能「影響系統效能」，對硬體要求較高。

6.5.3 反應方式

- (1) **被動方式 (IDS)：**只將異常事件記錄下來，並發出警報（如郵件、SNMP Trap），供管理員日後稽核分析使用。不主動介入阻斷流量，因此不會對網路服務造成干擾。
- (2) **主動方式 (IPS)：**偵測到攻擊事件後，會立即採取行動，如阻斷惡意連線、丟棄惡意封包或重置 TCP 連線，有效阻止攻擊蔓延。但也有可能誤擋正常流量。



6.5.4 部署方式

- (1) **監聽模式 (IDS)**：部署在網路交換機的 Port Mirroring 埠，被動地監聽網路流量副本。優點是不影響網路部署，且幾乎不影響網路效能；缺點是無法主動阻擋攻擊。
- (2) **Bridge 模式 (IPS)**：串接在網路路徑中，成為流量的必經之路。優點是具備強大的防禦能力，能即時阻擋惡意流量；缺點是如果 IPS 設備故障，則可能造成網路服務中斷。

6.5.5 部署位置

IDS/IPS 設備的部署位置非常關鍵，通常建議部署在 DMZ 區與內部網路的進出口，如圖 45 IDS/IPS 設備部署位置示意圖，防火牆後方即 DMZ 網路，然後再通過 IPS/IDS 進入內部網路，形成多層次防護。

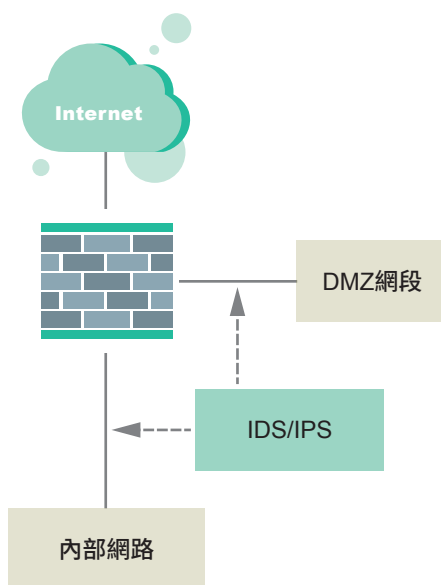


圖 45 IDS/IPS 設備部署位置示意圖

- (1) **DMZ 網段**：這是對外服務的區域，是攻擊者主要目標。部署 IDS/IPS 可監控進出 Web/Mail Server 等流量，防禦來自外部的攻擊。
- (2) **內部網路進出口**：監控內部網路之間的流量，以及內部網路對外的連線，有助於偵測內部威脅（如惡意程式擴散）、橫向移動攻擊，以及內部主機對外發起的惡意連線（如殭屍網路活動）。

6.5.6 IDS 與 IPS 之差異比較

表 39 呈現 IDS 與 IPS 在關鍵特性上的差異，有助於理解兩者在資安架構中的不同定位與功能。

表 39 IDS 與 IPS 之差異比較

特性	IDS（入侵偵測系統）	IPS（入侵防禦系統）
監控方式	被動	主動
反應能力	僅報告	自動防禦
部署位置	網路邊緣或主機	內聯於網路流量中
誤報風險	較低	較高
即時防護	無	有

(1) 監控方式：

- ◆ **IDS（被動）**：IDS 運作於「被動模式」，只負責監聽網路流量的副本，而不直接在流量路徑中，因此不會對網路傳輸造成任何實質性影響或延遲。
- ◆ **IPS（主動）**：IPS 運作於「主動模式」，會串接在網路流量的路徑中，成為流量的必經之處，以便在偵測到威脅時能立即介入。

(2) 反應能力：

- ◆ **IDS（僅報告）**：IDS 的主要反應是「僅發出警報或生成報告」，將偵測到的異常事件通知給管理員，但不具備自動阻斷攻擊的能力。
- ◆ **IPS（自動防禦）**：IPS 則具備「自動防禦」的能力。一旦偵測到符合攻擊特徵的流量，會立即採取行動，如阻斷連線、丟棄惡意封包，從源頭上阻止攻擊的擴散。

(3) 部署位置：

- ◆ **IDS（網路邊緣或主機）**：IDS 可以部署在「網路邊緣」監聽整體流量，也可以部署在「單一主機上」監控該主機的活動 (HIDS)。其監聽特性使其部署位置較靈活，不影響主流量。

- ◆ **IPS（內聯於網路流量中）**：IPS 由於需要主動介入，必須「內聯於網路流量中」，即串接在流量路徑上。這通常是在網路閘道、防火牆後方或不同安全區域之間。

(4) 誤報風險：

- ◆ **IDS（較低）**：由於 IDS 只負責告警不阻斷，即使發生「誤報」，也僅是發出錯誤的警報，不會直接影響正常網路服務的運作，因此其誤報風險導致的業務影響「較低」。
- ◆ **IPS（較高）**：IPS 一旦「誤判」，可能會「阻擋正常的網路流量」，導致合法的服務中斷。因此，IPS 的「誤報風險較高」，需要更精準的規則和持續調校。

(5) 即時防護：

- ◆ **IDS（無）**：IDS「不提供即時防護」，只能在攻擊發生後發出警報，無法在第一時間阻止攻擊。
- ◆ **IPS（有）**：IPS 則提供「即時防護」，能在偵測到攻擊的瞬間就採取阻斷措施，有效防止攻擊在網路中擴散或對系統造成損害。

6.5.7 選購考量

在選購 IDS 與 IPS 產品時，應考慮以下關鍵因素：

(1) 精準之特徵碼資料庫：

- ◆ **深度防護**：確保特徵碼資料庫不僅僅針對「特定攻擊」編寫，更要具備針對「軟體弱點」的防護能力。這意味著即使是未被識別的特定攻擊，只要它利用了已知的軟體漏洞，也能被偵測。
- ◆ **降低誤報漏判**：優秀的預設特徵碼應能「產生較少的誤判與漏判」，這直接影響系統的可用性與安全性。過多的誤報會造成管理負擔，而漏判則會讓威脅成功進入系統。

(2) 效能能經過實測：

- ◆ **避免瓶頸**：IDS/IPS 設備，特別是 IPS，是串接在網路流量中的關鍵點。其「處理效能（吞吐量、每秒連線數）」必須能夠承受機關的「實際網路流量與尖峰負載」。
- ◆ **評估**：在選購前，務必要求廠商提供「實際的效能測試數據」，或進行概念驗證 (PoC)，確保其性能符合需求，避免部署後反而成為網路的瓶頸。

(3) 針對 DoS/DDoS 攻擊能分辨合法封包與攻擊封包之差異：

- ◆ **複雜性**：分散式阻斷服務攻擊 (DDoS) 的挑戰在於，其攻擊流量可能由看似「合法的封包」組成，難以與正常流量區分。
- ◆ **關鍵能力**：好的 IDS/IPS 應具備進階的「行為分析和流量模式辨識能力」，能夠在大量流量中「分辨出看似正常卻是攻擊意圖的封包」，精準地識別並阻擋 DoS/DDoS 攻擊，而非僅僅基於源 IP 或連接埠。

(4) 報表系統、中央管理機制及 IM/P2P 管理能力：

- ◆ **報表與管理**：系統應提供「完整且彈性的報表系統」，方便管理員快速了解威脅態勢、偵測記錄及防護效果。同時，「中央管理機制」對於大規模部署至關重要，能統一管理、部署規則、監控多個設備。
- ◆ **應用層管理**：考量到即時通訊 (IM) 及 P2P 軟體可能被用作傳播惡意程式或資料外洩的途徑，IDS/IPS 應具備對這些「應用層協定的識別與管理能力」，例如阻擋惡意 P2P 流量或監控 IM 中的可疑行為，提供更全面的應用層防護。

總之，IDS 與 IPS 是網路防禦體系中不可或缺的組成部分。透過對其功能、技術、部署及管理重點的深入理解，組織能夠有效地偵測、阻擋網路攻擊，從而提升整體資通安全防護水平。

6.6

「APT」之攻擊防禦措施

進階持續性威脅 (Advanced Persistent Threat, APT) 是一種針對特定組織的複雜且多方位的網路攻擊。它與一般大規模散播的惡意程式不同，APT 攻擊高度客製化、目標明確，且通常由具備國家級或專業組織背景的攻擊者發起。

6.6.1 主要的攻擊特色

APT 攻擊的獨特之處在於其持續性、針對性、隱蔽性與複合性的特點。

- (1) **持續性**：攻擊者不求一擊得手，而是在滲透後長期潛伏在目標網路中，持續收集情報、擴大控制範圍。
- (2) **針對性**：攻擊目標明確，通常是針對特定行業、組織或個人，事先進行了詳細的情報偵察。
- (3) **隱蔽性**：攻擊過程極力隱藏行蹤，避免被偵測系統發現，常用各種規避技術。
- (4) **複合性**：攻擊手法多樣且複雜，結合了多種攻擊技術（如社交工程、零日漏洞、惡意程式）及不同階段的滲透策略。

6.6.2 APT 防禦措施

(1) 用途：

- ◆ **增強組織抵禦 APT 攻擊的整體能力：**
 - **核心目標**：APT 攻擊是高度複雜且持續性的威脅，其防禦無法僅依賴單一技術或產品。
 - **整合效益**：這裡強調的「用途」是透過一系列整合性的防禦措施（如多層次防護、情資分析、事件應變、持續監控），來「全面性地提升」組織在面對 APT 時的防禦、偵測、應變與復原能力。這是一個系統性工程。
- ◆ **降低 APT 攻擊造成的風險及損害：**
 - **預防與減輕**：APT 攻擊可能導致資料竊取、系統破壞、業務中斷等嚴重後果。

- **效益**：透過有效的防禦措施，即使無法完全杜絕攻擊，也能「降低攻擊成功的機率」，或在攻擊發生時「最小化其造成的風險與損害」，減少對組織的衝擊。

◆ **建立完善的 APT 防禦體系：**

- **體系化**：這表示不僅要部署單點防護，更要建立一個「涵蓋預防、偵測、應變、復原」的完整資安體系。
- **目標**：旨在構築一個能夠適應 APT 攻擊不斷演進的防線，確保資安防護的持續有效性。

(2) 部署方式：

◆ **多層次安全防護：結合網路、端點及應用層面的安全控制措施：**

- **縱深防禦**：APT 攻擊會利用各種管道滲透，因此必須部署「多層次」的防護。
- **涵蓋範圍**：這包括在「網路層面」（如防火牆、IPS、WAF）、在「端點層面」（如防毒軟體、EDR）以及在「應用層面」（如網站應用程式安全）都部署適當的安全控制措施，確保攻擊者在不同階段都面臨阻礙。

◆ **持續的威脅情報收集及分析：監控 APT 攻擊趨勢及手法。**

- **情資為王**：了解最新的 APT 攻擊趨勢、常用的攻擊手法、惡意程式特徵等「威脅情報」至關重要。
- **情報來源**：透過訂閱資安報告、參與情資分享平台、導入安全資訊及事件管理 (Security Information and Event Management, SIEM) 系統或安全協同、自動化與回應 (Security Orchestration, Automation and Response, SOAR) 系統來「持續收集與分析」這些情報，以便及時調整防禦策略。

◆ **完善的事件應變機制：建立快速檢測、遏制及修復的程序：**

- **應變計畫**：即使防禦再好，也難保不會被突破。因此，必須建立一套「完整且可操作的資安事件應變計畫 (IRP)」。
- **關鍵步驟**：強調快速的「檢測」（發現攻擊）、有效的「遏制」（限制攻擊範圍）、及時的「修復」（恢復受影響系統）等關鍵程序，以最小化攻擊影響。

◆ **持續監控及適應性調整：依據威脅變化不斷優化防禦策略：**

- **動態調整**：APT 攻擊是持續演進的，防禦策略也必須是動態的。

- **循環優化：**透過「持續監控」網路和系統行為，定期評估防禦措施的有效性，並依據不斷變化的「威脅情勢，不斷優化及調整」防禦策略，確保資安防線的韌性與適應性。

(3) 管理重點：

◆ 確保多層次安全防護的全面性及協同性：

- **整合而非堆疊：**管理的重點在於確保所有部署的安全措施（防毒、防火牆、WAF、IPS、EDR 等）不是各自為政，而是能「全面覆蓋」所有攻擊點，並能「協同運作」，形成聯動防禦。
- **效益：**系統之間的資訊共享與聯動反應，可有效提升整體防護效率。

◆ 持續更新及分析最新的威脅情報：

- **資訊來源：**管理層應確保組織有穩定的管道獲取「最新威脅情報」，並投入資源進行「有效分析」。
- **決策基礎：**這份情報是制定和調整防禦策略的基礎。

◆ 確保事件應變流程的高效性及可靠性：

- **演練重要：**管理層必須確保資安事件的「應變流程」不僅書面化，更要「定期演練」，以確保在實際攻擊發生時，能快速、高效、可靠地執行，將損失降到最低。

◆ 建立靈活的監控及調整機制：

- **彈性應變：**管理層需要建立一個能夠「靈活應變」的資安管理框架。這包括定期審查安全政策、調整監控閾值、更新偵測規則，以適應新的威脅挑戰。
- **持續改進：**資安防禦是一個持續改進的過程。

APT 防禦是一個複雜且持續的過程。組織必須從多層次防護、威脅情報分析、事件應變及持續優化等方面全面考量，才能有效地抵禦這些高階、隱蔽且具針對性的網路攻擊。

6.7

「SOC」管理機制

資通安全威脅偵測管理 (Security Operation Center, SOC) 指提供資通設備紀錄與資訊服務或應用程式紀錄等資安監控、事件處理、資安威脅預警等之服務。

6.7.1 核心目標

SOC 的核心目標是協助機關提升資安監控之有效性，即時掌握最新網路風險狀態及安全資訊。

6.7.2 SOC 監控範圍包括：以 A 級公務機關為例

SOC 可提供多種專業服務，涵蓋組織內外的資安設備監控，包括：

- (1) **端點偵測及應變機制 (EDR)**：專注於電腦、伺服器端點的活動，提供更深入的行為分析，以偵測並回應在端點上發生的進階威脅。
- (2) **防毒軟體 (Antivirus)**：監控防毒軟體的偵測紀錄、隔離事件、病毒碼更新狀態，確保端點免受已知惡意軟體的感染。
- (3) **網路防火牆 (Firewall)**：監控網路防火牆的連線日誌、拒絕連線紀錄、政策變更，以識別惡意連線嘗試及違反網路政策的行為。
- (4) **電子郵件過濾機制**：監控電子郵件系統的傳輸與過濾日誌，以阻擋垃圾郵件、釣魚郵件、惡意附件等。
- (5) **入侵防禦及偵測機制 (IDS/IPS)**：監控網路流量，識別攻擊特徵碼或異常模式，以偵測未經授權的存取或攻擊行為。
- (6) **應用程式防火牆 (WAF)**：專門保護 Web 應用程式，監控針對應用層的攻擊，如 SQL 注入、跨站腳本 (XSS) 等。
- (7) **進階持續性威脅攻擊防禦措施 (APT)**：結合多個數據源及威脅情資，分析及識別潛伏時間長、多階段的複雜攻擊。
- (8) **目錄服務系統**：監控如 Active Directory (AD) 的帳號登入、權限變更、群組異動等日誌，防止身分與存取層面的攻擊。

- (9) **核心資通系統之資通設備紀錄及資訊服務或應用程式紀錄：**監控組織最關鍵的 IT 基礎設施（如伺服器、資料庫）及核心業務應用程式的運行狀態與安全事件。

6.7.3 其他監控範圍

除了上述監控範圍外，建議機關據實際業務需求及風險評估，將其他必要的設備、系統或服務紀錄納入 SOC 的監控範圍，以達到最全面的防護。

6.7.4 協助機關提升資安監控的有效性

SOC 能夠透過多種方式協助機關提升資安監控的有效性：

- (1) **7x24 全天候監控服務：**確保任何時刻都能發現潛在的資安事件，大幅縮短威脅偵測時間。
- (2) **即時告警：**當系統偵測到符合預設規則或異常行為時，SOC 能即時發出告警給相關人員或自動化應變系統，為後續追蹤分析與應變處理爭取寶貴時間。
- (3) **追蹤分析與應變處理：**SOC 團隊不僅接收告警，更具備專業的追蹤分析能力，能對告警進行深入研判，判斷其真實性、影響範圍與攻擊意圖，並依據分析結果啟動應變處理流程。
- (4) **定期提供網路威脅分析統計報表：**定期彙整並分析所有資安事件日誌，產出報表，提供組織管理者宏觀的威脅趨勢洞察，有助於了解資安態勢、評估防護成效，並作為調整資安策略的依據。
- (5) **監控與網路同步運作：**納管多樣資安設備（如防火牆、IDS/IPS、WAF、防毒系統、伺服器日誌、AD 日誌等），並透過 SIEM 系統進行關聯分析，從而讓「整體分析更全面」。
- (6) **搭配全球預警、威脅情資等服務及專屬事件追蹤平台：**獲取最新的漏洞資訊、攻擊手法、惡意 IP 黑名單等情報，並自動化處理部分事件，加速複雜事件的安全協調與應變。

6.7.5 資通安全威脅偵測聯防機制

資通安全威脅偵測聯防機制是資安防禦進階化的重要環節，特別是在面對

高複雜度威脅時。它建立了多層次、多單位協同合作的模式，從國家層級到個別組織，共同提升資安防護與應變能力，如圖 46 SOC 聯防機制圖，係以 CI 提供者 SOC 為例，說明由下而上之聯防機制。

圖 46 右側清晰展現了三層聯防架構：最底層是「CI 提供者 SOC」進行「建置與監控」，向上傳遞「領域 SOC 情資」至「領域 SOC」，再到最上層的「N-SOC 情資」；同時，「N-SOC」會將分析後的情資「回傳」給「領域 SOC」及「CI 提供者 SOC」，形成一個完整的資通安全威脅偵測聯防機制。

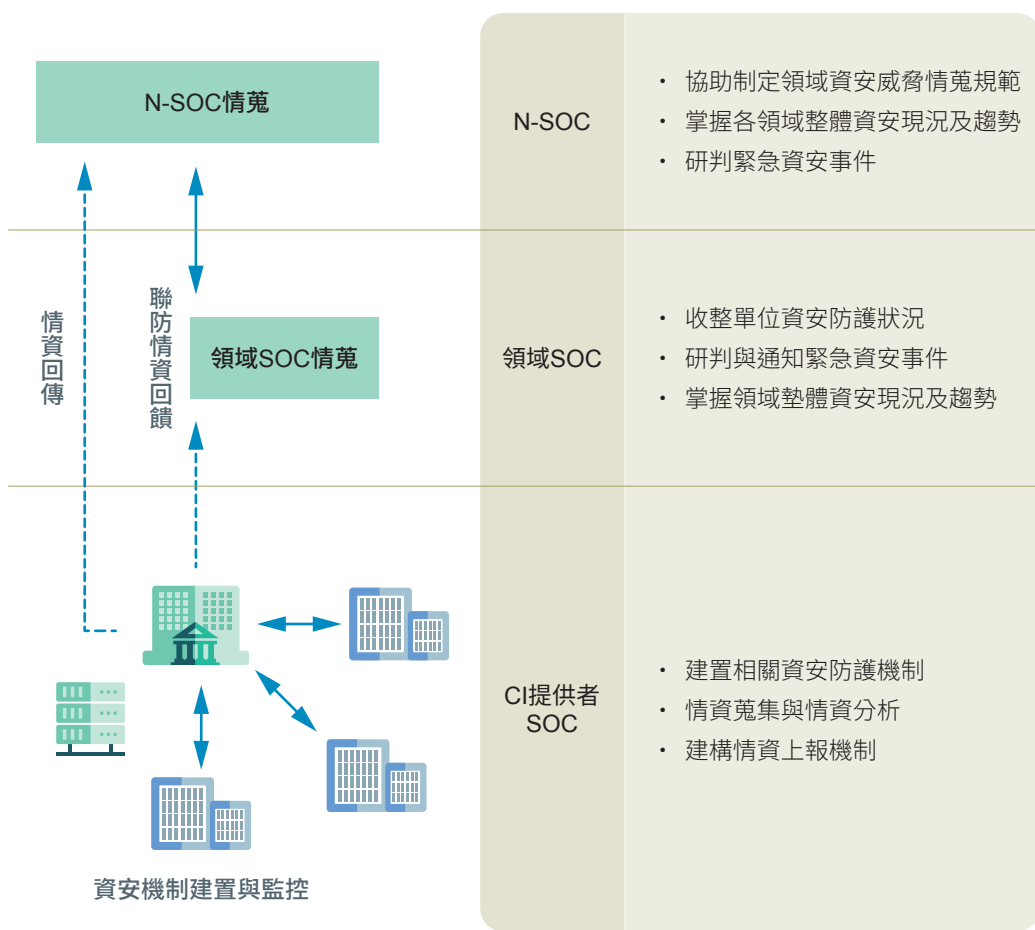


圖 46 資通安全威脅偵測聯防機制圖

(1) N-SOC（國家資通安全監控中心）：國家級 SOC 扮演統籌與協調的角色，負責協助制定領域資安威脅規範、掌握各領域整體資安現況及趨勢，並對全國性的緊急資安事件進行研判。同時，接收來自下層領域 SOC 的情資，並將分析後的國家級情資回傳，形成雙向溝通。



(2) **領域 SOC（產業或特定領域的資安監控中心）**：介於 N-SOC 與個別組織之間，負責收整單位資安防護狀況，對所屬領域內的緊急資安事件進行研判與通知，並掌握領域整體資安現況及趨勢。它將所屬機關的資安情資匯報至 N-SOC，同時接收 N-SOC 的指導與情資回饋，再傳達給下層單位。

(3) **CI 提供者 SOC（關鍵基礎設施提供者或個別企業的 SOC）**：最底層的資安聯防體系，由關鍵基礎設施 (CI) 提供者或個別企業內部建立的 SOC。負責建置相關資安防護機制、進行情資蒐集與情資分析，並建立情境資訊上報機制。

總結來說，SOC 是組織集中化管理與監控資安事件的核心樞紐。透過其提供的多樣化服務、監控機制與多層次的聯防體系，組織能夠有效地偵測、分析並應對各種資安威脅，從而提升整體資安防護水平。

MEMO

6.8

「GCB」組態基準

政府組態基準 (Government Configuration Baseline, GCB) 是一項重要的資通安全管理措施，旨在規範資通訊設備（如個人電腦、伺服器主機及網通設備等）的一致性安全設定（如密碼長度、更新期限等），以提升政府機關資通訊設備之資安防護。GCB 的導入有助於發展一致性的安全組態設定，並提升整體防護水準。

6.8.1 組態管理

(1) 組態 (Configuration)：

- ◆ 為 IT 系統的邏輯模型，包含服務、軟體、硬體、設定、文件及 IT 人員等組態項目 (Configuration Item, CI)。
- ◆ 組態項目間有互動與關聯性，例如一個應用程式（軟體 CI）需要特定的伺服器（硬體 CI）及網路設定（設定 CI）才能運行。

(2) 組態管理目標：識別、控制、維護及檢查現有 IT 系統中所有的組態元件及其之間的關聯性，確保 IT 環境的穩定性、一致性、安全性及合規性。

(3) 組態管理資料庫 (Configuration Management Database, CMDB)：

- ◆ 儲存最新 IT 系統所有組態項目及其關聯性的資料庫。CMDB 提供 IT 環境的單一真實來源，幫助 IT 人員全面了解 IT 服務與其底層組件之間的關係。
- ◆ 其儲存形式可以是文件、檔案或關聯式資料庫。

(4) 組態管理目的：

- ◆ IT 資產管理。
- ◆ 提供 IT 服務管理作業中所需的精確資訊。
- ◆ 降低因變更對系統造成的各類負面影響。

(5) 透過「變更管理」維護 IT 系統的組態現況：

- ◆ 在「變更管理」的流程中應加入「變更組態」的動作，以隨時更新組態資料庫



(6) 變更管理項目：

- ◆ **記錄變更內容與過程：**詳細記錄變更了什麼，以及如何變更，這對於後續的稽核、問題排除及追溯至關重要。
- ◆ **評估變更的衝擊、成本、效益、資源需求及風險：**在執行任何變更之前，應全面評估其可能帶來的衝擊、所涉及的成本、預期效益及潛在風險。
- ◆ **取得授權與核准：**所有變更都必須經過適當層級的授權與核准。
- ◆ **管理與協調變更的實作：**變更的實作過程需要有效管理與協調，特別是涉及多個團隊或系統的複雜變更。
- ◆ **變更實作監督與回報：**變更執行後，必須對其實作情況進行監督，並將結果回報給相關人員。

(7) 變更 CMDB 以反映變更後現況：在「變更管理」的流程中，應加入「變更組態」的動作，以隨時更新組態資料庫，確保 CMDB 中的資訊始終反映 IT 系統的真實現況。

(8) 當 IT 系統之組態變更時，應考量對系統營運的安全影響：

- ◆ **重要性：**任何對 IT 系統組態的調整，無論是硬體升級、軟體更新或參數修改，都可能對現有系統的「安全營運」產生潛在風險。
- ◆ **全面評估：**在進行變更前，必須仔細考量這些變更可能造成的「可用性影響」，例如服務中斷、性能下降、系統不穩定等，以確保變更不會對業務連續性造成負面衝擊。

(9) 變更前應釐清組態項目的關聯性：

- ◆ **核心步驟：**在執行任何組態變更之前，至關重要的是要「釐清受影響的組態項目及其相互之間的關聯性」。
- ◆ **安全組態影響：**變更可能牽一髮而動全身，影響到其他系統或應用程式的「安全組態設定」，例如防火牆規則、加密協定版本等，必須預先評估潛在的資安漏洞。
- ◆ **存取控制影響：**同樣，變更也可能意外地修改或破壞現有的「存取控制設定」，導致未經授權的存取，或阻擋合法使用者的權限。
- ◆ **降低風險：**充分理解這些關聯性有助於精確規劃變更、預防潛在問題，並在變更後能快速驗證其正確性。

6.8.2 政府組態基準 (GCB)

GCB 的導入是提升政府機關資通訊設備資安防護的重要策略。

- (1) **目的：**規範資通訊設備（如：個人電腦、伺服器主機及網通設備等）的一致性安全設定（如：密碼長度、更新期限等），以提升政府機關資通訊設備之資安防護。
- (2) **政策要求：**從中央部會推動至所屬機關及地方政府，確保各級政府單位都能遵循統一的資安標準。
- (3) **部署範圍：**從終端設備（如個人電腦）擴及至伺服器及所有資通安全設備，確保整個 IT 環境的安全一致性。
- (4) **強制性：**GCB 的導入是 A 級與 B 級公務機關必須辦理的事項。
- (5) **效益：**
 - ◆ **發展一致性安全組態設定：**透過 GCB，各級政府機關能夠「發展並實施一致的安全組態設定」，消除因設定不一致導致的資安漏洞，提高整體防護水準。
 - ◆ **提升資通訊設備之資安防護：**最終顯著「提升政府機關資通訊設備的資安防護能力」，形成更堅實的資安防線。

(6) GCB 之類別及項目

GCB 規範涵蓋了四類主要設備類別，每類都有具體項目，旨在為關鍵資通訊設備提供一致的安全配置標準。

- ◆ **網通設備 (Network Devices)：**
 - 涵蓋所有用於網路通訊的設備，如無線網路設備、Palo Alto Firewall 11、Fortinet Fortigate、Cisco Firewall 等防火牆。
 - 目的在於確保網路基礎設施的安全配置，防止未經授權的存取及網路攻擊。
- ◆ **作業系統 (Operating Systems)：**
 - 涵蓋廣泛使用的個人電腦及伺服器作業系統，如 Windows 和 Linux。
 - 目的在於規範作業系統的安全設定，如帳戶密碼策略、服務啟用、系統日誌配置等，以降低作業系統層面的安全風險。
- ◆ **應用程式 (Applications)：**
 - 涵蓋伺服器端或使用者端運行的關鍵應用程式，如 Exchange（郵件伺服器）、IIS（網頁伺服器）、SQL Server（資料庫伺服器）、Apache



- 目的在於確保這些應用程式本身及其相關配置符合安全規範，防範應用層漏洞被利用。

- 涵蓋主流的網頁瀏覽器，如 Chrome、Firefox 及 Edge。
- 目的在於規範瀏覽器的安全設定，如安全性區域設定、彈出視窗阻擋、插件管理等，以保護使用者免受惡意網站和網路釣魚的侵害。

MEMO

6.9

「VANS」通報機制

6.9.1 VANS 目的

政府機關資安弱點通報機制 (Vulnerability Analysis and Notification System, VANS) 旨在結合資訊資產管理與弱點管理，掌握整體風險情勢，並降低重大弱點爆發時可能造成之損害。VANS 不僅提供弱點通報，更協助機關進行資產盤點與風險評估，以提升整體資安防護，其目的說明如下：

- (1) **握整體風險情勢：**結合資訊資產管理與弱點管理，掌握整體風險情勢。
- (2) **降低重大弱點爆發損害：**透過及時發現和修補弱點，降低重大資安事件的發生機率和損害。
- (3) **資產清冊建立：**定期蒐集資通系統主機與電腦所使用的資訊資產項目及版本，建立資訊資產清冊，以達到降低風險與管控成本等目標。
- (4) **弱點比對：**將資訊資產清冊與弱點資料庫比對，以掌握所使用資訊資產是否存在已公開揭露之弱點資訊。

6.9.2 VANS 提供的服務

VANS 可協助機關落實資通安全管理法之資產盤點與風險評估應辦事項，並提供以下的服務：

- (1) **持續維護資訊資產盤點資料：**VANS 系統能協助機關「持續性地更新與維護」其資訊資產的盤點資料，確保資產清冊的即時性及準確性，是後續風險評估與弱點管理的重要基礎。
- (2) **系統化風險評估：**針對機關登錄的資訊資產項目進行弱點比對，協助進行系統化風險評估。VANS 會對機關已登錄的資訊資產項目，自動「進行弱點比對」作業，依據已知弱點資料庫識別資產中存在的潛在安全漏洞。
- (3) **即時提醒與修補作業：**依據機關所訂定之風險值門檻，即時提醒資訊資產風險情形，並進行弱點評估與修補作業。一旦偵測到資訊資產的風險等級超過門檻，便會「即時發出提醒」。

- (4) **微軟安全性更新檢測報告解析功能**：提供微軟安全性更新檢測報告解析功能，協助機關以自動化方式檢視安全性更新落實程度，確保所有補丁都已正確安裝，減少因更新不及時造成的安全漏洞。

6.9.3 VANS 資訊資產涵蓋範圍

VANS 在進行弱點管理與資產盤點時，涵蓋了不同層次的資訊資產，包括應用軟體資產、應用框架與程式語言、應用程式中介軟體及作業系統。這表示 VANS 需要深入到不同技術的細節來識別潛在弱點，其資訊資產涵蓋範圍，如圖 47 VANS 資訊資產涵蓋範圍，茲說明如下：



圖 47 VANS 資訊資產涵蓋範圍

- (1) **應用軟體資產**：最上層，代表終端使用者或業務部門直接使用的應用程式，通常是攻擊者嘗試利用的切入點，包括 Adobe 系列軟體、MySQL、Office 等。
- (2) **應用框架 / 程式語言**：中間層，代表應用程式開發所依賴的基礎框架和程式語言，其弱點可能影響多個應用程式，包括 Java 的 Struts2、PHP、.NET 等。
- (3) **應用程式中介軟體 (Middleware)**：支撐層，連接作業系統與應用程式，提供應用程式運行的基礎服務，包括 Microsoft IIS、Apache Tomcat 等。
- (4) **作業系統**：最底層，作為所有應用程式及服務運行的基礎平台，包括 Windows Server 及其他 Windows 系列作業系統。

VANS 是一個全面的資安弱點管理與通報機制。透過其資產盤點、弱點比

MEMO

6.10

「EDR」偵測及應變機制

端點偵測及回應系統 (Endpoint Detection and Response, EDR) 是一種用於偵測並回應發生在端點設備（如個人電腦、伺服器、筆記型電腦等）上的惡意活動的資安解決方案。它超越傳統防毒軟體，能識別更複雜的攻擊行為，並提供更詳細的攻擊事件資訊，幫助資安人員快速判讀與應變。

6.10.1 用途：EDR 系統的核心用途在於全面保護組織的端點設備

- (1) **偵測與阻擋威脅**：偵測並阻擋發生在端點設備上的惡意活動。它能識別更複雜的攻擊行為，包括無檔案攻擊、勒索軟體、零日漏洞利用和 APT 攻擊。
- (2) **確保端點設備安全**：透過持續監控端點活動、收集數據並進行分析，EDR 旨在全面確保端點設備的安全性。

6.10.2 技術類型：EDR 系統結合多種技術來實現高效的偵測與應變

- (1) **行為分析**：持續監控端點上的所有進程、檔案操作、網路連線、登錄檔變更等行為。透過分析這些行為模式，EDR 能夠識別異常或惡意的行為活動。
- (2) **規則比對**：將監控到的行為與已知的「惡意行為規則集」（例如，特定的 API 呼叫序列、惡意檔案雜湊值）進行比對，有助於快速識別已知攻擊模式。
- (3) **黑白名單**：黑名單阻止已知惡意檔案、進程或 IP；白名單允許已知安全、合法的程式運行。

6.10.3 選購考量：選購 EDR 系統時，應考慮以下關鍵因素

- (1) **偵測威脅的精準度**：評估 EDR 系統的偵測精準度，包括「誤報率」及「漏判率」。高誤報率會增加資安人員負擔，高漏判率則意味著大量威脅未能被發現。
- (2) **與防毒軟體整合**：理想的 EDR 應能與現有的防毒軟體或次世代防毒 (NGAV) 進行良好整合。NGAV 是一種採用機器學習及行為分析技術的進階防毒解決

(3) **系統呈現的攻擊事件資訊詳盡且易於判讀：**EDR 會產生大量的數據，因此一個優秀的 EDR 應具備「直觀的事件可視化界面」，能將複雜的攻擊事件以「詳盡且易於判讀」的方式呈現，包括攻擊鏈、受影響的設備、時間軸等，以便資安人員能快速理解、分析並進行應變。

MEMO

單元

7

資通安全技術面應辦事項——
安全性檢測及資通安全健診

在當前高度互聯的數位環境中，資通系統面臨的威脅日益複雜且難以預測。僅仰賴靜態的防護措施已不足以確保安全，持續性的安全檢測與定期的資通安全健診成為不可或缺的環節。這些評估工具能夠協助組織主動發掘潛在的弱點、辨識存在的風險，並提供具體的改善建議，從而強化整體資安防護能力，提升面對資安事件的韌性。

本單元將引導讀者深入了解資通安全技術面應辦事項中的安全性檢測與資通安全健診，從其法規規定、運作原理、執行流程，到不同類型的檢測方法與健診項目，並將探討如何透過弱點掃描、滲透測試等技術性評估，以及全面的資通安全健診，有效地辨識、分析並解決資安問題，為組織的資安管理提供客觀依據。

本單元學習重點如下：

- 1** 了解安全性檢測的法規規定，以及不同責任等級機關的檢測頻率。
- 2** 掌握弱點掃描的定義、目的、類型、流程與報告內容，並了解其執行考量。
- 3** 理解滲透測試的定義、目的、類型、流程與報告內容，以及其模擬攻擊的特性。
- 4** 認識應用程式安全的關鍵概念，包括 SSDLC、變更控制、輸入攻擊防護與檢測方法。
- 5** 了解資通安全健診的目的、頻率、健診項目與執行流程。
- 6** 學習網路區域規劃的原則與實踐，以及網路連線安全、虛擬私有網路與雲端運算安全。
- 7** 掌握實體安全的威脅類型與防護措施，包括進出控管、安全區域規劃、環境與消防安全。



7.1

安全性檢測

安全性檢測是資通安全防護體系中主動發現與修補弱點的關鍵步驟，其重要性已由法規明文規範。依《資通安全責任等級分級辦法》規定，已明確要求各級機關應依其資通安全責任等級，定期辦理全部核心資通系統之安全性檢測，包括弱點掃描及滲透測試。安全性檢測的頻率則依機關的資通安全責任等級而有所不同，具體規定如表 40 安全性檢測規定。

表 40 安全性檢測規定

機關級別	弱點掃描	滲透測試
A	每年 2 次	每年 1 次
B	每年 1 次	每 2 年 1 次
C	每 2 年 1 次	每 2 年 1 次
D	無要求	無要求
E	無要求	無要求

表 38 顯示資通安全責任等級越高的機關，其安全性檢測的頻率越高，以確保對資安風險的持續監控與管理。以下說明弱點掃描及滲透測試之目的及性質。

7.2

弱點掃描

7.2.1 何謂弱點掃描

弱點掃描作為一種重要的資安評估方法，它透過自動化工具與非侵入式檢查，對目標系統、網路及應用程式進行全面的安全評估。此技術旨在識別其中已知或潛在的安全漏洞，例如軟體版本過舊、不安全組態設定、預設密碼、開啟不必要的服務埠，以及已公開的軟體漏洞等。弱點掃描在資安防護體系中扮演著關鍵角色，是主動發現並啟動漏洞修補流程的首要步驟。

7.2.2 目的

- (1) **評估資安防護能力：**了解掃描目標目前的資安保護狀況，提供一份「檢測報告」。
- (2) **發現潛在弱點：**主動找出可能被利用的安全漏洞，這些漏洞如同資安防線上的「破口」。
- (3) **提供改善建議：**依據掃描結果，提供詳細的漏洞描述、風險評級及具體的修補或緩解建議。
- (4) **提升系統安全：**協助組織依據掃描結果進行修補，逐步消除已知安全隱患，強化整體系統的安全性。
- (5) **作為管理依據：**掃描結果可作為高階主管或資安管理單位進行資安決策的參考基準，幫助評估資安投資成效、監控資安風險趨勢。
- (6) **確認弱點已排除：**透過後續複掃，驗證已發現的弱點是否已成功修補，避免「假修復」的情況。

7.2.3 弱點掃描類型

依據掃描目標的性質，常見的弱點掃描通常分為以下主要類型：

- (1) **主機系統弱點掃描：**



- ◆ **範圍：**針對單一或多個主機（伺服器、工作站、電腦）進行，檢查其作業系統、網路服務、系統設定、帳號密碼管理等安全配置。
- ◆ **檢查項目：**至少應符合共同脆弱性及暴露 (Common Vulnerabilities and Exposures, CVE) 發布的弱點內容，包括作業系統未修正的弱點、常用應用程式的弱點、網路服務程式的弱點、木馬或後門程式的掃描、帳號密碼破解測試、系統的不安全或錯誤設定、網路通訊埠掃描等。

(2) Web 網頁弱點掃描：

- ◆ **範圍：**針對網站應用程式的安全弱點進行掃描。
- ◆ **檢查項目：**符合 **OWASP TOP 10**：2021 等最新版本。
 - ① A01 Broken Access Control（權限控制失效）
 - ② A02 Cryptographic Failures（加密失敗）
 - ③ A03 Injection（注入式攻擊）
 - ④ A04 Insecure Design（不安全設計）
 - ⑤ A05 Security Misconfiguration（安全設定錯誤）
 - ⑥ A06 Vulnerable and Outdated Components(脆弱及過時的組件)
 - ⑦ A07 Identification and Authentication Failures（身分識別及鑑別失效）
 - ⑧ A08 Software and Data Integrity Failures（軟體及資料完整性失效）
 - ⑨ A09 Security Logging and Monitoring Failures（安全日誌及監控失敗）
 - ⑩ A10 Server-Side Request Forgery)（伺服器端請求偽造）

7.2.4 弱點掃描流程

弱點掃描的推動與執行，應遵循典型的 PDCA (Plan-Do-Check-Act) 循環，以確保資安工作具備系統性與持續改善的有效性，如圖 48 弱點掃描流程圖，茲說明如下：



圖 48 弱點掃描流程圖

- (1) **確認掃描需求 (Plan)**：定義掃描目標、類型、範圍，確認合規性要求及排程。需合法授權並知會相關單位，避免影響業務。
- (2) **執行初掃 (Do)**：依據需求，使用選定工具（如 Nessus, Qualys）對目標進行首次全面掃描，並配置掃描參數，執行自動化掃描。
- (3) **分析初掃報告 (Check)**：分析原始掃描結果，排除誤報，並依據風險等級、影響程度對弱點進行優先級排序，提供專業判讀與分析。
- (4) **確認並修復弱點 (Act)**：針對高風險弱點進行驗證，將修復任務分配給相關團隊（IT、開發），並執行修補（安裝修補程式、修正組態、修正程式碼）。這是最重要的環節，強調修復的「執行力」。
- (5) **執行複測 (Do)**：修復後再次執行掃描，驗證之前弱點是否已成功修復，並確認未引入新問題，確保修復措施有效，避免「假修復」。
- (6) **生成複測報告 (Check)**：生成最終報告，總結修復成效，評估風險降低狀況，並提供後續建議。這是資安管理過程的證明，用於高層匯報及持續改進。

7.2.5 如何執行弱點掃描

弱點掃描服務通常包含以下具體執行步驟，從前期規劃到報告產出：

- (1) **事前準備與了解**：與目標組織溝通，了解其網路架構、系統環境（設備廠牌、系統版本等），確保掃描順利，避免影響業務。
- (2) **工具準備**：使用取得合法授權的商業掃描軟體，並在每次掃描前，將掃描工具的弱點資料庫更新至最新版本，確保掃描的完整與正確。



- (3) **執行初掃及產出報告：**安排適當的掃描時間（通常在非公務時段或與組織協調），減少對正常運作的影響；執行「初掃」並產出初掃報告。
- (4) **協助修補與追蹤：**依據初掃結果，協助組織理解發現的弱點並提供修補建議，並追蹤弱點修補進度，記錄未修補或排除的原因。
- (5) **執行複掃及產出報告：**在弱點修補後，就原先初掃報告找出之弱點，再次執行「複掃」及產出複掃報告，目的是確認先前的弱點是否已成功排除，確保掃描目標的安全。若複掃仍發現未修補的弱點，則服務提供者應協助組織解決問題。

7.2.6 弱點掃描報告

弱點掃描的主要產出是詳細的掃描報告，這是資安狀況的總結及未來行動的指引。通常包含以下內容：

- (1) **執行結果摘要：**簡要說明本次掃描的背景、範圍、發現的關鍵風險、整體安全態勢評估，以及最重要的發現和建議。
- (2) **專案執行計畫：**說明掃描期間、項目、範圍、執行人員、使用工具及方法。
- (3) **弱點統計分析：**依風險等級（高、中、低）及弱點類別進行分類統計，以數據化的方式呈現弱點分佈。
- (4) **詳細弱點清單：**列出每個發現的弱點名稱、描述、受影響的設備名稱、IP/URL、服務埠 (Port)，並標示弱點的風險等級，提供具體的修補建議。
- (5) **掃描誤判清單：**說明被掃描工具標示為弱點但經人工判斷為誤判的項目及理由。
- (6) **弱點排除清單：**說明因特定原因（如無法修補、已有其他配套措施）而暫不修補的弱點及其理由。
- (7) **複掃報告的差異化分析：**提供與初掃結果的比較，例如列出已修復的弱點數量、仍未修復的弱點或新發現的弱點。

7.2.7 弱點掃描考慮因素

在規劃及執行弱點掃描時，需考慮多個關鍵因素，這些因素會影響掃描的結果與適用情境：

- (1) 內部掃描 VS 外部掃描
- (2) 有登錄權限 (Authenticated) VS 無登錄權限 (Unauthenticated)

(3) 侵入式 VS 非侵入式

(4) 委外 VS 機關 IT 資安部門

7.2.8 內部掃描 VS 外部掃描

請參閱圖 49 內部掃描及外部掃描示意圖，該圖清楚展示了這兩種掃描模式在網路架構中的實際執行位置及其核心差異。外部掃描主要模擬來自網際網路的攻擊，著重於檢測組織對外開放服務的安全性，猶如檢查建築物的「大門」是否堅固；相對地，內部掃描則模擬內部人員或已突破周邊防線的攻擊，旨在評估內部網路與系統的「房間內部」是否存在弱點。這兩種掃描方式具備高度互補性，唯有同時執行，方能建構全面性的資安防護體系。

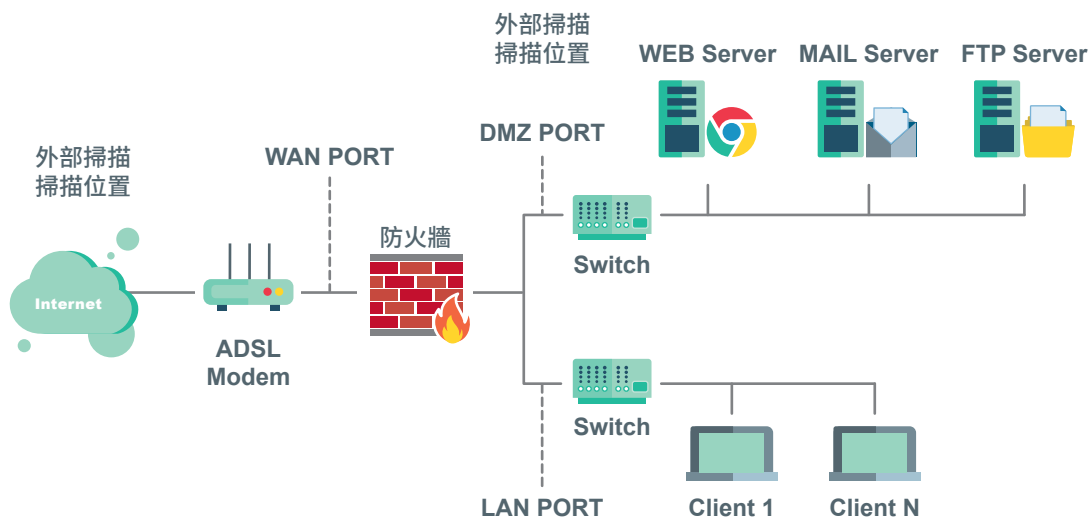


圖 49 內部掃描及外部掃描示意圖

(1) 外部掃描：

- ◆ **掃描位置：**如圖所示，外部掃描的發起位置在組織的防火牆「外部」，模擬來自網際網路的攻擊行為。掃描流量從外部通過 GSN 政府網際網路及 Firewall，嘗試探測組織暴露在公網上的服務。
- ◆ **目標：**主要檢測組織對外開放的服務，例如：
 - Web Server（網站伺服器）的公網 IP 位址及相關的 Web 應用程式漏洞。
 - Mail Server（郵件伺服器）的 SMTP/POP3/IMAP 服務漏洞。



- FTP Server（檔案傳輸伺服器）的漏洞（如果對外開放）。
- 防火牆的規則組態是否安全、是否有不必要的埠口開放。
- ◆ **情境：**模擬駭客從外部進行的資訊收集及初步攻擊嘗試。

(2) 內部掃描：

- ◆ **掃描位置：**如圖所示，內部掃描的發起位置在組織的防火牆「內部」，也就是內部區域網路 (LAN) 中。掃描主機可以位於 Client 1 或 Client N 旁邊，或部署在內部網段的伺服器上。
- ◆ **目標：**檢測組織內部網路中的所有資產，包括：
 - 內部使用的 Web Server、Mail Server、FTP Server（即使不對外開放）。
 - 各個 Client 端電腦（工作站）的作業系統、應用程式、組態漏洞。
 - 內網的 Switches（交換器）等網路設備的組態弱點。
 - 各種內部業務系統的漏洞，例如資料庫伺服器、ERP/CRM 系統等。
- ◆ **情境：**模擬內部人員的惡意行為、內部電腦被入侵後作為跳板的行為，或是內部組態錯誤導致的風險。

(3) DMZ：

- ◆ **說明：**圖中顯示的 DMZ 是一個特殊區域，位於防火牆內、但與內部 LAN 有所區隔。通常將對外提供服務的伺服器（如 Web Server，Mail Server，FTP Server）放置於此。
- ◆ **安全性考量：**DMZ 的掃描同時需要考慮內部及外部視角。外部掃描會直接觸及 DMZ 的外部介面，而內部掃描（從 LAN 內部發起）也可以檢測 DMZ 伺服器與內部網路之間的安全性隔離是否有效。

7.2.9 有登錄權限 VS 無登錄權限

有登錄權限與無登錄權限掃描的核心區別在於：使用「有登錄權限」進行弱點掃描，能比「無登錄權限」提供更為深入且徹底的檢測。無登錄權限掃描僅能針對登錄功能進行有限測試；而有登錄權限掃描則能進一步探測登錄後更多的系統功能。為獲得最全面的資安評估，建議優先採用具備登錄憑證的掃描模式。

(1) 無登錄權限掃描：

- ◆ **檢測範圍：**只能測試「無需登入」即可公開存取的服務及介面。

- ◆ **發現範例：**服務版本漏洞、首頁上可觸發的 XSS 漏洞、開放埠等。
- ◆ **局限性：**無法探測登入後的功能，容易遺漏深層次的應用程式邏輯漏洞。
- ◆ **情境：**模擬一個完全陌生的外部駭客進行初步探測。

(2) 有登錄權限掃描：

- ◆ **檢測範圍：**掃描器使用有效憑證登入，模擬合法用戶行為，能深入檢查系統內部配置及應用程式的登入後功能。
- ◆ **發現範例：**作業系統組態設定、內部服務漏洞、權限問題（水平 / 垂直）、登入後表單的注入攻擊、敏感資料存取等。
- ◆ **優勢：**觸及更多程式碼路徑，結果更全面、準確，誤報率較低。
- ◆ **情境：**模擬內部人員的惡意行為，或外部攻擊者成功入侵後進行的內部探測。

7.2.10 侵入式 VS 非侵入式

「侵入式 VS 非侵入式」，這是在資訊安全檢測（特別是弱點掃描及滲透測試）中，用來區分測試方法對目標系統影響程度的重要概念。

(1) 非侵入式：

- ◆ **不會對目標系統造成影響，主要透過分析響應判斷弱點：**

非侵入式測試在執行過程中，不會嘗試修改系統的組態、資料或運行狀態，也不會利用漏洞進行實際的攻擊。它通常是透過向目標系統發送特定的請求（如端口掃描、服務指紋識別、Banner Grabbing 等），然後分析系統的反應，從而推斷或判斷是否存在已知的弱點。

- ◆ **安全性高，適合運作環境：**

由於非侵入式檢測對系統沒有負面影響，因此在線上運行、對穩定性要求極高的生產環境中，是首選的測試方式。它能在不中斷業務的情況下，提供初步的弱點評估。

(2) 侵入式：

- ◆ **可能對系統造成不穩定或破壞，通常用於滲透測試，需謹慎授權：**

侵入式檢測（例如滲透測試）會模擬真實的攻擊行為，嘗試利用已發現的弱點，甚至執行某些操作（如注入惡意程式碼、提升權限、獲取敏感資料等）。這類測試因為涉及實際的攻擊模擬，確實有導致系統不穩定、功能異常甚至資料損壞的風險。因此，執行前必須獲得目標系統所有者



的明確且謹慎授權，通常在測試環境而非生產環境中進行。

◆ **弱點掃描主要採用非侵入式：**

雖然弱點掃描及滲透測試均旨在發掘漏洞，但一般而言，弱點掃描工具或服務為確保運作環境的安全性，多以非侵入式為主。相對地，滲透測試則傾向採用侵入式手段，以驗證弱點之可利用性及其潛在影響。

7.2.11 委外 VS 自行執行

關於弱點掃描的執行方式，主要有委外及機關資安部門自行執行兩種選擇，各有其主要考量。最終的選擇宜基於組織的資源現況、專業能力及風險承受度來決定。

(1) 委外：

- ◆ **簽訂契約，彈性較低：**服務範圍與時間表在契約中明確規定，不易變更，事前須充分考量。
- ◆ **費用與目標數量、掃描次數正相關：**費用依掃描範圍、深度及頻率計價，需依據預算精確規劃。
- ◆ **優勢：**專業性高、工具先進、結果客觀、節省內部人力。
- ◆ **劣勢：**成本較高、溝通成本、對內部系統理解有限、資料傳輸安全考量

(2) 機關資安部門自行執行：

- ◆ **弱點掃描軟體的購置與持續更新：**需要初期軟體投資，並持續投入維護與更新，確保資料庫最新。
- ◆ **弱點掃描之專業人才：**需具備專業資安知識 { 解讀報告、漏洞分析、修補建議、工具操作 } 及人員培訓。
- ◆ **優勢：**對系統熟悉、反應快速、資料保密、內部能力累積。
- ◆ **劣勢：**可能有些盲點、工具限制、人員流動風險。

7.2.12 弱點掃描服務委外

機關辦理委外弱點掃描服務時，其服務建議書宜涵蓋的重要內容，可參考文件：「政府機關弱點掃描服務委外服務建議書徵求文件」，該服務建議書之章節內容，說明如下：

(1) 弱點掃描服務委外服務建議書之章節：

壹、專案概述：

- ◆ **名稱與目標：**明確服務名稱、提升系統安全性或符合法規要求等專案目標。
- ◆ **範圍與期間：**詳細列出掃描的資產 (IP、URL、系統類型) 及服務起訖時間。

貳、專案工作項目：

- ◆ **掃描內容：**具體說明應執行的掃描類型 (主機、Web 應用程式，應符合 OWASP TOP 10 等)。

參、管理需求：

- ◆ **廠商資格：**規範廠商需具備的資質、認證及專業人員。
- ◆ **服務水準協定 (SLA) 與罰責：**定義服務標準與未達標的處罰機制。
- ◆ **品質與驗收：**明確報告品質、初測、複測標準及驗收流程。
- ◆ **業務機密安全：**強調機敏資訊的保密要求與簽署。
- ◆ **預算金額：**明確專案預算範圍。

肆、交付項目：

- ◆ **項目與時程：**規定應交付的成果報告及提交時間。
- ◆ **文件格式與說明：**規範報告的格式及內容要求。

伍、建議書製作規定：

- ◆ **格式與內容：**指導廠商如何撰寫建議書。

(2) 弱點掃描服務委外服務建議書之「壹、專案概述」：

以下深入說明 RFP 中「專案概述」的撰寫細節。這部分是整個委外專案的「地圖」，定義了服務的起始點及終點。使潛在的服務供應商（廠商）能快速理解專案的背景、目的及核心需求。

一、專案名稱：

- ◆ **說明：**專案名稱應簡潔明瞭，點出服務性質，便於後續溝通及文件管理。
- ◆ **範例：**「弱點掃描服務」委外服務案（以下簡稱本案）。

二、專案目標：

- ◆ **說明：**清楚闡明執行本次委外掃描所希望達成的具體效益。
- ◆ **範例：**「藉由本案之執行成果，以掃描目標之資安防護能力與發現潛在弱點，並依據掃描結果提出改善建議，協助掃描目標提升系統安全防護成效。」

三、專案範圍：

- ◆ **說明：**這是最重要的部分之一，明確界定哪些資產將被納入掃描範圍。



- ◆ **範例：**「本案的服務範圍如表 41 弱點掃描服務範圍設備清單」，茲說明如下：

表 41 弱點掃描服務範圍設備清單

項目	掃描類別	IP/URL	設備種類（如主機／伺服器種類、通訊設備種類、個人電腦等）	備註（如設備廠牌、系統版本）
1	系統弱點掃描			
2	網站弱點掃描			
	...			

- **掃描類別：**更細緻的分類，如「系統弱點掃描」、「網站弱點掃描」。
- **IP / URL：**具體列出要掃描的 IP 位址範圍或獨立 IP，以及每個 Web 網站的 URL。如果範圍很大，可以列出網段或提供附件說明。
- **設備種類：**通常包括主機 / 伺服器種類、通訊設備種類、個人電腦等。
- **備註：**用於補充說明，例如：設備廠牌、系統版本等。

四、專案期間：

- ◆ **說明：**定義整個服務專案的起始和結束日期。
- ◆ **範例：**「自簽約日起至 XXX 年 XX 月 XX 日止」。
- ◆ **提示：**應將掃描執行、報告提交、修復驗證等各階段的時間點考慮進去，而非僅僅是簽約日期

(3) 弱點掃描服務委外服務建議書之「貳、專案工作項目」：

機關專案工作項目應依表 42「弱點掃描工作項目」之主機系統與 Web 網頁，進行安全弱點掃描，以檢測潛在的安全弱點。掃描完成後，需提供相關結果報告，作為主機資訊安全管理的重要依據，並提供弱點修補方法的參考建議。完成弱點修復後，將進行複掃以確認所有弱點均已排除。

表 42 弱點掃描工作項目

主機系統弱點掃描	Web 網頁弱點掃描
1. 作業系統未修正的弱點掃描 2. 常用應用程式弱點掃描 3. 網路服務程式掃描 4. 木馬、後門程式掃描 5. 帳號密碼破解測試 6. 系統之不安全與錯誤設定掃描 7. 網路通訊埠掃描	1. A01 Broken Access Control (權限控制失效) 2. A02 Cryptographic Failures (加密機制失效) 3. A03 Injection (注入式攻擊) 4. A04 Insecure Design (不安全設計) 5. A05 Security Misconfiguration (安全組態錯誤) 6. A06 Vulnerable and Outdated Components (脆弱及過時的組件) 7. A07 Identification and Authentication Failures (識別及鑑別失效) 8. A08 Software and Data Integrity Failures (軟體及資料完整性失效) 9. A09 Security Logging and Monitoring Failures (安全日誌及監視失敗) 10. A10 Server-Side Request Forgery (伺服器端請求偽造)

(4) 弱點掃描服務委外服務建議書之「參、管理需求」：

應包括下列項目：

- 一、廠商資格
- 二、服務水準協定 (SLA) 與罰責
- 三、品質需求與驗收標準
- 四、業務保密安全責任

(5) 弱點掃描服務委外服務建議書之「肆、交付項目」：

應包括下列項目：

- 一、工作計畫書
- 二、弱點掃描服務中文報告
- 三、弱點複掃服務中文報告

弱點掃描是資通安全防護的基礎，也是持續改進的關鍵。透過對其定義、類型、流程、報告內容與各種考慮因素的深入理解，組織能夠有效地識別和修補資安弱點，從而提升整體資安韌性。

7.3

滲透測試

7.3.1 何謂滲透測試

滲透測試是一種深入的資安評估方法，係透過模擬有心人士之攻擊方式，對系統或物聯網設備進行安全強度測試。這項測試由專業的資安人員（通常稱為白帽駭客）執行，他們嘗試利用系統或網路中的漏洞來取得存取權限。

滲透測試的主要驗證現有安全防護措施的有效性，並找出弱點的實際可利用性。它不僅能發現已知的弱點，更能揭露複雜的邏輯漏洞及潛在的入侵路徑，藉此檢驗防護措施在實際攻擊下的成效。

由於滲透測試是一種更深入、更擬真的模擬攻擊，且通常具有侵入性，因此在執行前需要仔細的授權與規劃。

7.3.2 目的

- (1) **評估防護能力：**檢測受測目標在遭遇攻擊活動時之資安防護能力與執行成效。
- (2) **發現潛在弱點：**主動找出可能被利用的安全漏洞，包括複雜的邏輯漏洞。
- (3) **提供改善建議：**依據測試結果，提供修補弱點的方法與建議。
- (4) **確認弱點已排除：**透過複測，確認初測找出之資安漏洞已經完成修正。
- (5) **精進整體防護：**透過滲透測試報告及改善建議，檢討與精進受測目標之整體資安防護作為。

7.3.3 滲透測試之類型及類別

滲透測試的應用範圍相當廣泛，主要涵蓋作業系統、應用程式、網站服務、密碼破解，以及無線服務。

為了更精確地執行與管理，滲透測試還能進一步細分為不同的測試類型及測試類別。這些詳細的分類方式，通常會列於滲透測試的規劃文件或報告中，

如表 43 滲透測試之類型及類別。

表 43 滲透測試之類型及類別

測試類型	測試類別
作業系統	遠端服務、本機服務
網站服務	設定管理、使用者認證、連線管理、使用者授權、邏輯漏洞、輸入驗證、Web Service、Ajax
應用程式	電子郵件服務套件、檔案傳檔服務套件、遠端連線服務套件、網路服務套件、其它
密碼破解	密碼強度測試
無線服務	無線服務弱點測試

7.3.4 滲透測試之流程

滲透測試是一個高度客製化且需要精準規劃的過程，其進行流程如圖 50 滲透測試流程圖，茲說明如下。

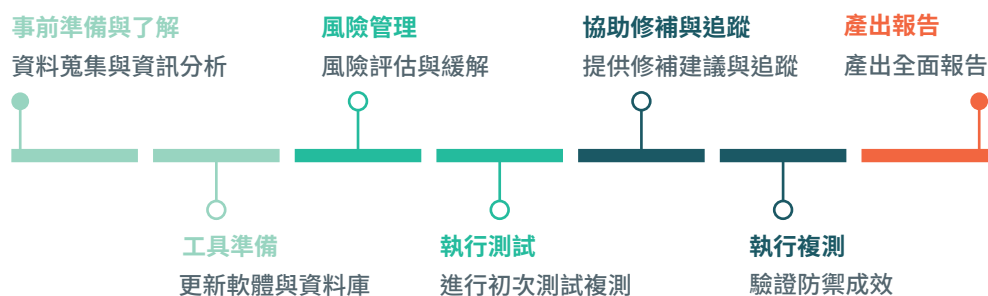


圖 50 滲透測試流程圖

(1) 事前準備與了解：

- ◆ 這是整個流程的起點，確保所有相關方對測試或稽核的範圍、目標及限制都有共同的理解。



◆ **資料蒐集與資訊分析：**

- 定義範圍：確認要評估的資通系統、網路區段或應用程式。
- 資產盤點：收集所有相關的硬體、軟體、使用者及資料清單。
- 文件審查：查閱現有的安全政策、流程文件、網路拓撲圖及先前稽核報告。
- 情資蒐集：分析潛在威脅情資，了解組織當前面臨的風險環境。

(2) 工具準備：

- ◆ 使用取得合法授權的商業滲透測試軟體。
- ◆ 在每次掃描前，將掃描工具的弱點資料庫更新至最新版本，確保掃描的完整與正確。

(3) 風險管理：

執行具侵入性質的檢測作業前，需與組織進行確認，並具備適當應變措施與風險評估後才進行。事前需提出對受測目標進行備份建議。

(4) 執行測試（模擬攻擊）：

- ◆ 可針對網際網路及 / 或內部網路進行測試。網際網路測試通常由遠端進行，內部網路測試則於現場進行。
- ◆ 安排適當的執行時間，通常於非公務時段或與組織協調適當時間進行。
- ◆ 通常包含初次測試（初測），包括探索、弱點發掘、漏洞利用。

(5) 協助修補與追蹤：

初測後，協助組織理解可利用弱點及其利用路徑，提供具體修補與防禦強化建議。

(6) 執行複檢（驗證防禦成效）：

- ◆ 在弱點修補後，再次執行複測。
- ◆ 目的是確認先前的弱點是否已成功排除，確保掃描目標的安全。
- ◆ 若複測仍發現未修補的弱點，服務提供者應協助組織解決問題。

(7) 產出報告：提交詳盡報告，包含攻擊路徑、利用證據、風險評估及具體修補建議。

7.3.5 滲透測試的報告

透測試的核心成果是詳細的測試報告（包括初測及複測報告），通常包含以下內容：

- (1) **執行結果摘要：**包括受測目標風險等級與數量列表 / 受測目標風險漏洞名稱列表 / 風險漏洞分布列表，以及簡要說明滲透測試結果。
- (2) **專案執行計畫：**包括測試期間、執行項目、執行範圍、執行人員及使用工具。
- (3) **滲透測試弱點發現：**
 - ◆ 列出詳細的測試結果，
 - ◆ 應說明詳細過程及內容（包括檢測目標、弱點名稱、問題 URL/IP、問題參數、測試語法、測試截圖等）。
 - ◆ 並說明可能造成的風險。
- (4) **分析報告：**對測試結果進行統計分析。
- (5) **改善與建議：**著重於提供弱點修補建議，以利組織快速掌握弱點並進行修復。
- (6) **結論。**

7.3.6 更深遠的意涵

除了法規遵循外，安全性檢測對於組織而言，亦有其他更深遠的意涵，茲說明如下：

- (1) **自主資安檢測：**即使法規沒有強制要求（如 D 等級及 E 等級之機關），組織仍應考量自身業務特性及潛在風險，自主規劃資安檢測，以提升整體防護能力。
- (2) **持續改進循環：**定期檢測不僅僅是為了找出問題，更重要的是依據檢測結果進行修補與改進，形成一個持續性的資安循環。
- (3) **多重目的：**這些檢測的目的不僅為了符合法規要求，更是為了確保資通系統的韌性、資料的機密性、完整性及可用性。

滲透測試是資安防護中不可或缺的實戰演練。透過對其定義、類型、流程與報告內容的深入理解，組織能夠有效地找出系統中的安全漏洞，並提出改善建議，最終提升整體資安防護能力。

7.4

應用程式安全

應用程式安全旨在確保應用程式從開發到維護的整個生命週期中，都具備足夠的安全性，以防止漏洞被利用，保護資訊資產。這要求將安全思維融入軟體工程的各個環節。

應用程式安全是軟體工程的核心議題，它涵蓋了應用程式層面的安全問題，需透過設計來解決；而架構安全則屬於系統管理問題，需透過設定來解決。

對於安全要求高的軟體，需要特別訂定安全性規格，並從實際應用角度評估風險，依需求設計軟體系統，以降低風險與損害。

安全系統發展生命週期 (Secure Systems Development Life Cycle, SSDLC) 是一種將安全思維融入軟體開發全過程的方法，旨在考量軟體功能性的同時，確保各項必要的安全控制措施被執行，從而降低軟體後續維運的成本與遭受入侵的損失。

7.4.1 傳統軟體開發與 SSDLC 之比較

(1) 傳統軟體開發之特性：

- ◆ 能性導向，在最短的時間，完成系統的開發與上線。
- ◆ 缺乏安全性考量的設計，面對日新月異的攻擊手法，難以建立有效的防護方法保護系統的安全，例如：資料隱碼攻擊 (SQL Injection) 等便是因此而崛起。

(2) SSDLC 之思維：

- ◆ 在考量軟體功能性的同時，導入安全性的思維，於系統開發過程中均進行各項必要的安全控制措施。
- ◆ 雖開發時程長，但降低了系統後續維運的成本及遭受入侵的損失。

7.4.2 SSDLC

SSDLC 指的是一套旨在確保系統安全的開發流程，主要包含以下幾個步驟。接下來，我們將深入探討 SSDLC 的具體流程。

- (1) **需求分析 (Requirements)**：進行風險分析並確認應用程式的資安需求，以符合使用者需求與法規遵循為目的。
- (2) **架構設計 (Design)**：依據需求分析結果，設計包含系統任務的目標、功能關聯、邊界範圍，以及各階層使用者的角色等內外部使用的規劃，並搭配適當的資安架構。
- (3) **程式實作 (Implementation)**：落實既有之規劃，將使用者介面、功能運作及安全性等完整的實現，並培養程式設計師注意正確安全的程式撰寫習慣。
- (4) **測試與驗收 (Testing)**：依據資安需求擬訂測試計畫，並依測試計畫進行測試與修正，確保各項功能與安全性皆可符合既定的需求。
- (5) **部署與維運 (Maintenance)**：進行軟體的部署，安排教育訓練，並落實軟體的穩定運作，定期修補漏洞 (Patch)、按步升級更新版本 (Upgrade) 及即時監控 (Monitor)。

7.4.3 安全控制 - 變更控制

前面討論了應用程式在開發階段的安全，接下來我們將聚焦於應用程式上線後，如何透過「變更控制」來維持其安全。

變更控制在應用程式安全中扮演著至關重要的管理角色，其主要目的是確保在進行任何修改後，安全狀態仍能符合既定的安全政策要求，同時盡可能降低變更對系統帶來的潛在負面影響。以下針對變更控制之原因、方法及步驟進行說明：

- (1) **原因**：應用程式上線後，因需求變更、新功能要求及發現瑕疵等因素，需要變更應用系統程式或組態。
 - ◆ **變更是常態**：應用程式上線後，會因「業務需求變更」、「新功能導入」、「發現與修補瑕疵/漏洞」等原因，需要不斷修改程式碼或系統組態設定。
 - ◆ **風險管理**：這些變更若無妥善管理，極易引入新的安全漏洞或導致系統不穩定。
- (2) **方法**：機關應實作應用程式變更控制流程，必須確保變更是獲得授權、經過測試且被記錄下來。
 - ◆ **實作標準變更控制流程**：
 - **流程化**：建立一套正式、文件化的變更管理流程，從變更「提出、評估、規劃、開發、測試、部署到驗證」的每一步都有明確規範。



- **協作**：涉及跨部門（業務、開發、測試、資安）的協同作業。
- **版本控制**：利用工具（如 Git）追蹤程式碼變更歷史。
- ◆ **確保變更的三個關鍵要素**：
 - **授權**：所有變更都需經過正式審批，依風險層級決定批准權限，避免未經批准的任意修改。
 - **測試**：變更後必須在受控環境進行「全面測試」，包括功能測試、回歸測試，以及特別重要的「安全測試」（如滲透測試），以確保變更沒有引入新的功能問題或安全漏洞。
 - **記錄**：每次變更的所有相關資訊，包括變更內容、原因、執行人員、時間、審批記錄、測試結果等，都必須詳細記錄，以便「追溯問題源頭」、「支援稽核」及「資安事件應變」。

(3) 步驟：

- ◆ **變更需求管理**：填寫變更需求申請、分析變更需求、發展實作策略與方法、計算變更所需成本。
- ◆ **變更評估**：評估變更與安全的關聯性、記錄變更請求。
- ◆ **變更審查**：提交變更申請進行核准、變更開發、進行應用程式變更的開發工作、記錄變更開發的產出（新增或刪除功能）。
- ◆ **變更測試與部署**：將變更的程式碼與變更申請連結（程式碼中的註解）、將變更後的程式碼交付測試與品質認可、變更程式碼版本（上線）。
- ◆ **變更結果報告**：向管理階層報告變更結果。

7.4.4 安全控制 - 職責區隔

職責區隔是確保應用程式安全的重要控制措施，其目的在於防止單一人員在軟體開發與部署過程中濫用權限，或無意中造成潛在的安全漏洞。以下是實施職責區隔的關鍵原則：

- (1) 作業人員不應有權限存取線上的程式碼或程式物件。
- (2) 程式設計人員不應存取線上運作中的軟體。
- (3) 品管部門應測試程式碼品質，且與開發部門採用不同的測試方法。
- (4) 一旦軟體被開發測試完成應被保存在程式庫中。
- (5) 線上運作的軟體應由程式庫中發行，不應直接由程式設計人員或測試人員進行更新。

這些職責區隔措施確保了開發、測試與營運環境的獨立性，透過分工合作及程式碼管理，提高應用程式的整體安全性。

7.4.5 安全控制 - 程式庫維護

程式庫維護是確保應用程式安全與可靠的關鍵環節，旨在集中管理程式碼，進行版本控制，並對存取進行嚴格控管。

- (1) **集中存放與存取控管：**應用程式應集中存放在程式庫中，並進行存取控管。
- (2) **版本控制：**程式庫應進行版本控制，並保留所有版本程式碼，包括主版本、次版本及緊急修正版本。
- (3) **開發與測試流程整合：**
 - ◆ 開發部門凍結版本後，應簽入 (Check In) 到程式庫，並應由程式庫中簽出 (Check Out) 取得最新版本進行修改。
 - ◆ 測試部門應由程式庫中簽出 (Check Out) 取得最新版本進行測試。
- (4) **上線發行：**上線人員應由程式庫中發行 (Release) 最新版本應用程式至線上系統。

接著，以圖 51 程式庫維護流程圖，進一步說明如何透過有系統的流程，以確保程式碼的版本控制與安全性。以下將重點闡述流程圖中「安全控制 - 程式庫維護」的核心環節：

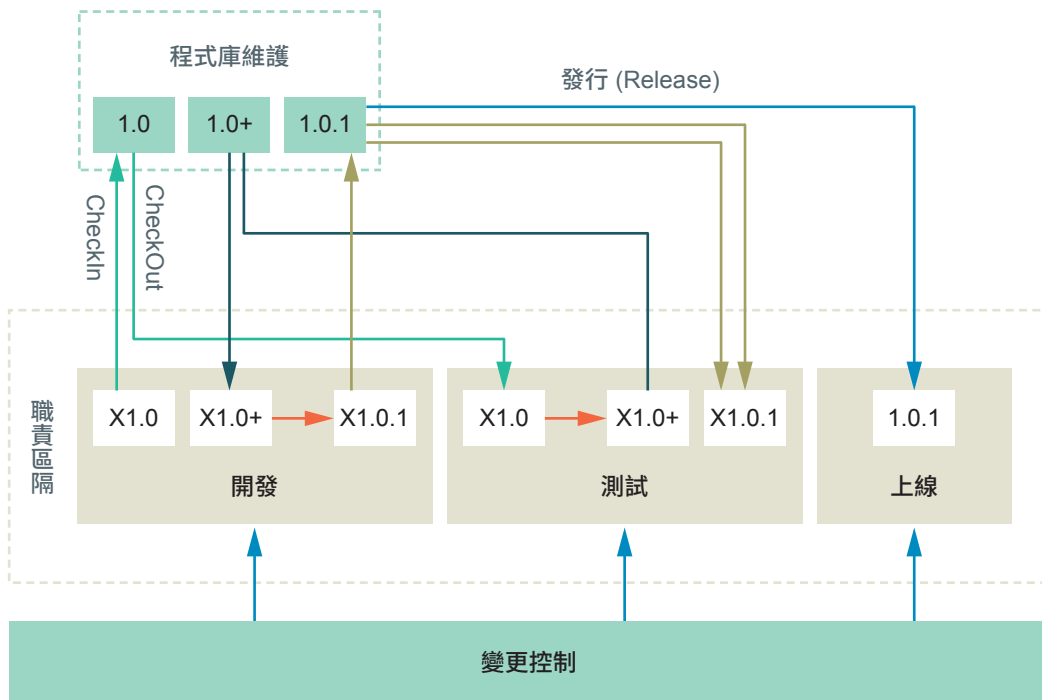


圖 51 程式庫維護流程圖

(1) 程式庫維護：

- ◆ 程式碼有不同版本，包括主版本 1.0、次版本 1.0+、緊急修正版本 1.0.1

(2) 開發、測試、上線流程。

- ◆ 開發人員將程式碼簽入 (CheckIn) 到程式庫
- ◆ 測試人員從程式庫簽出 (CheckOut) 取得最新版本進行測試
- ◆ 上線人員從程式庫發行 (Release) 最新版本至上線環境

(3) 職責區隔：

- ◆ 開發、測試、上線等角色分工明確，相互獨立
- ◆ 透過這種職責區隔，可以確保程式碼的安全性及可靠性

(4) 變更控制：

- ◆ 所有對程式碼的變更都需要經過嚴格的控制及審核

上述流程確保了程式碼的版本管理、開發測試的獨立性，以及變更的控制，從而提高應用程式的整體安全性。

7.4.6 行動應用程式安全

行動應用程式 (APP) 已成為我們數位生活不可或缺的一部分。然而，此類 APP 同樣面臨著嚴峻的資安威脅。駭客不僅可能運用傳統技術進行病毒感染，更會透過反向工程來變造應用程式，並將惡意版本上傳至應用程式商店，誘騙使用者下載。

為有效因應這些潛在的風險，無論是開發者或使用者，都應採取必要的安全措施。以下將分別說明在行動應用程式的開發與使用者應注意的事項，以共同築起更堅固的資安防線。

(1) 開發注意事項：

- ◆ **採用安全套件：**開發 APP 時，需注意採用安全的第三方套件。
- ◆ **避免索取過多敏感資訊：**開發 APP 時，應避免索取過多行動裝置上的敏感資訊（如通訊錄、行事曆、座標位置、郵件、簡訊內容等），以防侵犯隱私。

(2) 使用者注意事項：

- ◆ 不要在手機裡儲存重要資料。
- ◆ 不要下載不明 APP 以保護自己個資與財務安全。

7.4.7 安全威脅 - 輸入攻擊

輸入攻擊是 Web 應用程式最常見的攻擊類型之一，如 SQL 注入 (SQL Injection) 及跨站腳本 (Cross-Site Scripting, XSS)。這類攻擊主要利用應用程式未能對使用者輸入進行充分檢查與過濾的弱點，可能導致程式錯誤、執行邏輯被改變，甚至造成存取權限的跳脫。

為了解輸入攻擊的運作模式，並能有效防禦，我們將從以下幾個面向進行說明：

(1) 應用程式輸入資料及輸出結果：如圖 52 應用程式輸入資料及輸出結果示意圖。

- ◆ 使用者透過瀏覽器或其他介面提供輸入 (INPUT) 資料。
- ◆ 這些輸入資料會被傳送到應用程式 (Application) 進行運算與處理 (Process)。
- ◆ 最終，應用程式將處理結果輸出 (OUTPUT)，可能顯示給使用者，或儲存到資料庫。

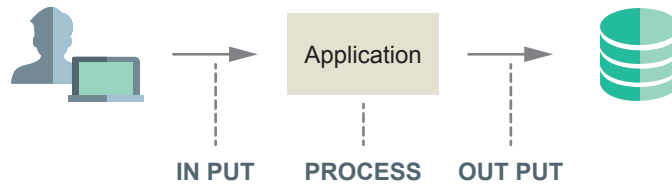


圖 52 應用程式輸入資料及輸出結果示意圖

(2) 輸入惡意資料之風險：

當應用程式缺乏適當的輸入驗證，惡意輸入會直接危害到應用程式本身及其背後的資料庫。如圖 52 輸入惡意資料之風險示意圖。

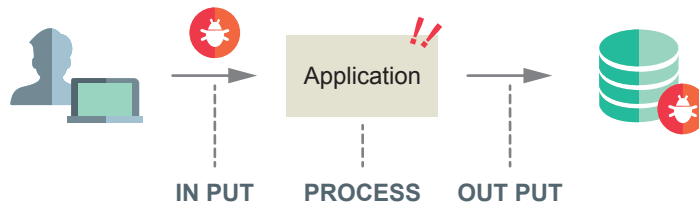


圖 53 輸入惡意資料之風險示意圖

- ◆ 當使用者輸入惡意資料 (INPUT)。
- ◆ 若應用程式 (Application) 沒有對這些惡意輸入進行適當的檢查與過濾 (Process)，則可能導致應用程式「發生錯誤」、「執行邏輯被改變」，甚至造成「存取權限跳脫」等嚴重問題。

妥善處理使用者輸入資料的重要性，開發者必須在設計階段就納入相關的安全防護機制，以確保應用程式的整體安全性。

7.4.8 WEB 應用程式 - 檢測

為確保 Web 應用程式的安全，定期執行安全檢測是至關重要的。這包括針對全部核心資通系統進行弱點掃描及滲透測試，茲說明如下：

- (1) **檢測頻率：**依機關級別而定，A 級機關每年 2 次弱點掃描及 1 次滲透測試；B 級機關每年 1 次弱點掃描及每 2 年 1 次滲透測試。

- (2) **常見檢測工具與方法：**

- ◆ **黑箱測試：**模擬攻擊者在不知道內部程式碼的情況下進行攻擊，如模擬 SQL Injection 或 XSS 等攻擊。

- ◆ **白箱測試**：靜態分析應用程式原始碼，從程式碼層面發現潛在的安全漏洞。
- ◆ **滲透測試**：針對權限跳脫與邏輯錯誤等深層問題進行模擬攻擊，驗證系統的實際防禦能力。
- ◆ **弱點修補策略**：
 - **有能力修改程式**：優先修補發現的應用程式弱點，從根本上解決問題。
 - **無能力修改程式**：建議建置 Web 應用程式防火牆 (WAF) 進行弱點防禦，作為一種外層防護措施，阻擋常見的 Web 攻擊。

(3) 黑箱檢測法與白箱檢測法比較：

前述 Web 應用程式之黑箱檢測法及白箱檢測法，其檢測方式在各個方面的差異，如表 44 黑箱檢測法與白箱檢測法比較表。

表 44 黑箱檢測法與白箱檢測法比較表

檢測方式	黑箱檢測法		白箱檢測法	
	人工滲透測試	AP 弱點掃描工具	人工源碼檢測	自動源碼檢測
弱點定位精準	普	差	佳	優
檢測詳細程度	差	普	優	優
執行時錯誤	優	佳	差	差
邏輯性錯誤	佳	普	差	差
存取控管機制	佳	普	差	差
檢測時效	差	佳	差	優
程式開發人員 修補溝通	普	差	佳	優
誤判情形	優	普	佳	普
綜合評比	佳	普	普	優

- ◆ 兩種檢測方法在弱點定位精準度、檢測詳細程度、執行時錯誤、邏輯性



- ◆ 若預算充足，可同時採用自動源碼掃描與人工滲透測試。
- ◆ 若預算有限，則優先採用自動源碼掃描。

MEMO

7.5

資通安全健診

資通安全健診是一種整合各資通安全項目的檢視服務作業，旨在提供機關資通安全改善建議，透過實施技術面與管理面的相關控制措施，提升整體資通安全防護能力，並針對已知弱點進行修補與持續追蹤。

7.5.1 健診目的

- (1) 整合各資通安全項目的檢視服務作業，透過系統性的檢查，全面了解組織在各個資安面向的表現。
- (2) 提供機關資通安全改善建議，依據健診結果，提供具體、可行的改善措施，協助組織提升資安防護能力。
- (3) 藉由實施技術面與管理面的相關控制措施，提升機關整體資通安全防護能力。
- (4) 針對已知弱點進行修補，並持續追蹤可能存在的風險。

7.5.2 健診辦理項目及頻率

資通安全健診項目分為網路架構、網路惡意活動、使用者端電腦惡意活動、伺服器主機惡意活動及安全設定檢視五大類。資通安全健診適用於 A 級、B 級及 C 級機關，且每年應辦理 1 次。D 級及 E 級機關則無強制要求。如表 45 資通安全健診之辦理項目及頻率。



表 45 資通安全健診之辦理項目及頻率

辦理項目	辦理項目細項	機關		
		A 級	B 級 / C 級	D 級 / E 級
資通安全健診	網路架構檢視	每年辦理 1 次	每 2 年辦理 1 次	無要求
	網路惡意活動檢視			
	使用者端電腦惡意活動檢視			
	伺服器主機惡意活動檢視			
	目錄伺服器設定及防水牆連線設定檢視			

7.5.3 健診項目

前述所提及的資通安全健診，其辦理項目廣泛涵蓋了資通環境的各個面向，旨在確保資通安全控制同時兼顧技術與管理層面。透過系統性的檢查，得以識別潛在弱點，並提供改善建議。

以下說明資通安全健診的各項重點檢視內容，包括：

(1) 網路架構檢視：

針對網路架構圖進行安全性弱點檢視，詳列發現事項之風險等級、風險說明與改善建議，以利機關後續修補與調整。

(2) 網路惡意活動檢視：

- ◆ 架設封包側錄設備，觀察內部電腦或設備是否有對外之異常連線，發現異常連線之電腦或設備應確認使用狀況與用途。
- ◆ 同時，檢視資安設備紀錄檔，分析過濾內部電腦或設備是否有對外之異常連線紀錄，發現異常連線之電腦或設備應確認使用狀況與用途。

(3) 使用者端電腦惡意活動檢視：

- ◆ 檢視使用者電腦之作業系統更新情形。
- ◆ 檢視使用者電腦之應用程式之安全性更新情形。
- ◆ 檢視使用者電腦是否使用已經停止支援之作業系統或軟體。

- ◆ 檢視使用者電腦防毒軟體安裝、更新及定期掃描結果之處理情形。

(4) 伺服器主機惡意活動檢視：

- ◆ 檢視伺服器主機之作業系統更新情形。
- ◆ 檢視伺服器主機應用程式之安全性更新情形。
- ◆ 檢視伺服器主機是否使用已經停止支援之作業系統或軟體。
- ◆ 檢視伺服器主機是否使用不合宜之作業系統。
- ◆ 檢視伺服器主機防毒軟體安裝、更新及定期掃描結果之處理情形。

(5) 目錄伺服器設定及防火牆連線設定檢視：

- ◆ **AD 伺服器組態設定：**以行政院國家資通安全會報技術服務中心所發展之「政府組態基準」內容為標準，確認目錄伺服器組態設定落實情形。
- ◆ 檢視防火牆連線設定規則是否有安全性弱點，確認來源與目的 IP 及通訊埠連通之適切性。

7.5.4 健診流程

資通安全健診是一個系統性的過程，旨在全面評估並提升組織的資安防護能力。其完整的執行流程涵蓋了從初期規劃到後續追蹤的各個階段，確保資安弱點能被有效識別、修補並持續改善。

以下將詳細闡述資通安全健診的 9 個主要執行步驟：

(1) 基本環境調查：

收集使用者電腦與伺服器主機資訊、政府組態基準部署現況與例外管理清單、服務主機與防護設備資訊、網段劃分資訊、網路交換器 (Switch) 是否支援 Port Mirror 功能、是否有網域環境等。

(2) 決定範圍與抽樣方式：

範圍與抽樣方式須具有代表性，並以範圍與抽樣方式決定檢測時程與預算金額。

(3) 檢測配合事項：由受測單位提供資料給檢測單位，包括檢測環境、網路架構檢視、網路惡意活動檢視、使用者端電腦惡意活動檢視、伺服器主機惡意活動檢視、目錄伺服器設定，以及防火牆連線設定檢視。

(4) 啟始會議：

- ◆ 執行檢測前，須辦理啟始會議，說明檢測項目與範圍，協調配合事項，並達成雙方共識。



- ◆ 參與人員應包含機關主管與相關業務承辦人。

(5) **執行檢測：**依據啟始會議決議項目執行，包括網路架構檢視、網路惡意活動檢視、使用者端電腦惡意活動檢視、伺服器主機惡意活動檢視、目錄伺服器設定及防火牆連線設定檢視。

(6) **撰寫檢測報告：**在完成所有檢測項目後，撰寫一份詳細的檢測報告，內容包括執行結果摘要、執行計畫、執行情形、結果建議、結論及附件。

(7) **提出改善建議：**針對各檢測項目發現事項，須詳查根因並提出相對應之改善建議。

(8) **結束會議：**

- ◆ 檢測完成後，須辦理結束會議，說明各項目發現事項、改善建議與結論。

- ◆ 參與人員應包含機關管領階層與相關業務承辦人。

(9) **修補規劃與追蹤：**

- ◆ 依據資安健診報告中之改善建議，規劃修補方式。

- 優先處理可即時修補與風險等級較高的弱點；

- 無法即時修補之弱點，需規劃改善計畫與改善時程，並持續追蹤修補進度。

- ◆ 針對已修補弱點，須留存弱點修補紀錄。

- ◆ 弱點修補完成後須執行複測，以確認修補方法之有效性。

在委外資通安全健診服務時，可參考「政府機關資安健診服務委外服務建議書徵求文件（範本）」，以確保服務內容與品質符合需求。

資通安全健診是組織資安管理中不可或缺的環節。透過其全面的檢測項目、系統化的流程與法規遵循，組織能夠有效地評估自身資安狀況，主動發現並解決弱點，從而持續提升整體資安防護能力。

7.6

網路安全

網路安全是資通安全領域中不可或缺的支柱，旨在保護網路基礎設施與其上傳輸的資料，防止未經授權的存取、使用、洩露、破壞或竄改。有效的網路安全措施，從網路區域規劃到雲端服務管理，都能夠確保網路通訊的機密性、完整性與可用性。

7.6.1 網路區域規劃

網路區域規劃旨在清楚界定不同屬性的網路區域，使其成為實施存取控制與制定安全策略的重要依據。這樣做的主要目的在於避免來自內部與外部的攻擊，並有效防範災害擴大，確保資通環境的穩固與安全。如圖 54 網路區域規劃示意圖所示，建議的區域劃分項目包括：

- ◆ 外部網路
- ◆ 內部網路 (LAN)
- ◆ 非軍事區 (DMZ)
- ◆ 網路管理區域
- ◆ 網路記錄區域
- ◆ 實體隔離區域

以下針對各個網路區域的特性及安全要求，進行詳細說明：

(1) 外部網路：

- ◆ 機關對外網路區域，連接外部廣域網路 (WAN)：

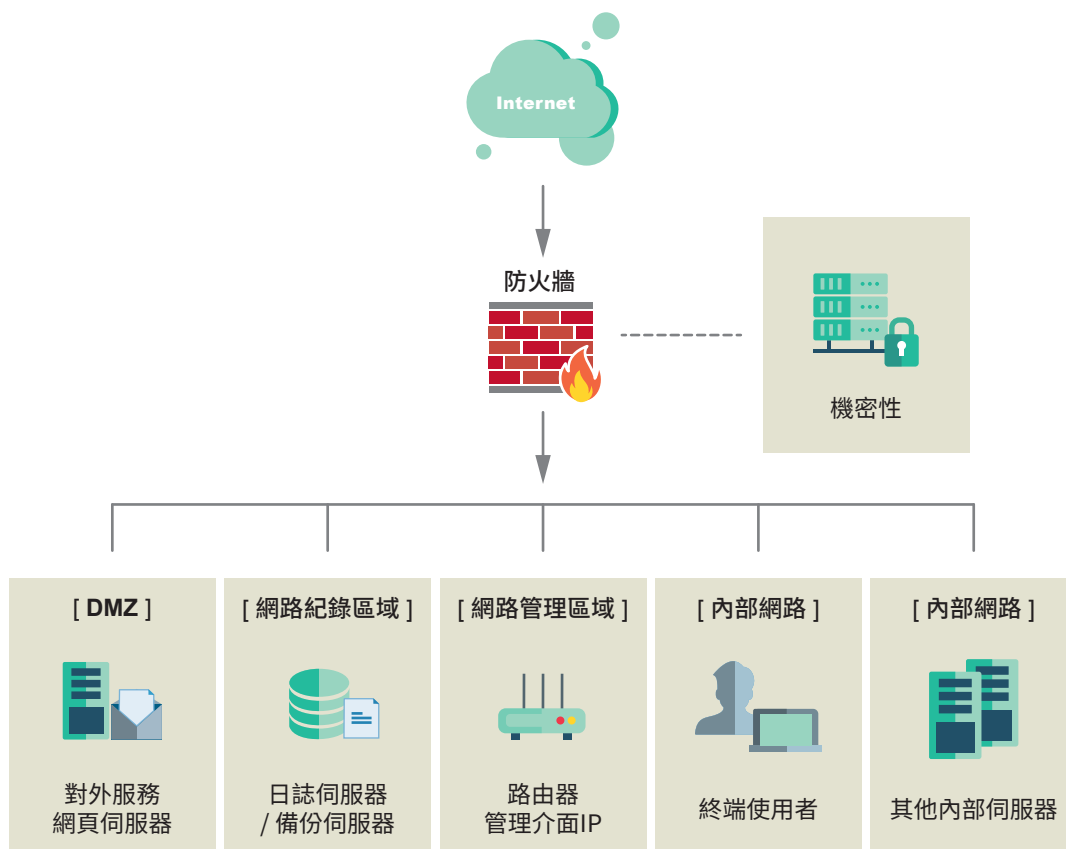
指的是組織與外部公眾網路（如網際網路）相連的區域。這是組織資訊對外發布及接收外部資訊的通道。

- ◆ 對內部需要經過防火牆的存取控制：

由於外部網路是潛在威脅的來源，任何來自外部、嘗試進入組織內部網路的流量，都必須經過防火牆的嚴格檢查及存取控制。防火牆在此扮演著第一道防線的角色。

- ◆ 非允許的服務與來源不能進入其他區域：

防火牆的規則會確保只有經過明確允許的服務（例如特定的通訊埠）及來自特定來源的連線才能通過，其他未經授權的連線一律阻擋，以防止未經授權的存取或攻擊。



*內部網路應視實際需求，評估是否再進行安全區域的細部隔離

圖 54 網路區域規劃示意圖

(2) 內部網路 (LAN)：

◆ 內部網路通常包含機關使用者終端、資通系統等設備：

指的是組織內部區域網路 (LAN)，其中包含了員工使用的電腦、印表機、伺服器、網路設備，以及各種資通系統等。

◆ 利用 VLAN 與不同路由等方式切開：

為了進一步提升內部網路的安全性與管理性，可以利用虛擬區域網路 (VLAN，Virtual Local Area Network) 技術，將內部網路劃分為多個邏輯子網。不同 VLAN 之間的通訊通常需要透過路由器或交換機來實現，並

可在此處設定安全策略。

◆ **外部網路無法直接連線內部網路：**

這是基於安全考量的重要原則。外部網路與內部網路之間必須有明確的隔離，通常透過防火牆進行嚴格的流量過濾，防止外部直接滲透。

◆ **並可考慮於內部網路架設代理伺服器控管與外部網段之連線：**

为了更好地控管內部網路對外部網路的存取，並提升安全性，可以考慮部署代理伺服器 (Proxy Server)。代理伺服器可扮演著內部網路與外部網路之間的中介角色，透過代理伺服器，所有內部使用者對外部的網路請求都會先經過代理伺服器，代理伺服器可以進行內容過濾、流量監控、身分驗證等，從而增強內部網路對外連線的安全性。

(3) 非軍事區 (DMZ)：

◆ **主要用於放置機關對外服務伺服器（如網頁伺服器、FTP 伺服器）：**

- DMZ 的主要功能是作為一個中介區域，用於放置那些需要從外部網路（例如網際網路）存取，但又不能直接放在內部網路的伺服器。
- 典型的例子包括：
 - ✓ 網頁伺服器：提供網站服務給外部使用者。
 - ✓ FTP 伺服器：提供檔案傳輸服務給外部使用者或合作夥伴。
 - ✓ 其他如郵件伺服器、DNS 伺服器、VPN 服务器等也常部署在 DMZ。

◆ **僅開放特定服務：**

- 部署在 DMZ 區域的伺服器，對外部網路只會開放其提供服務所需的特定通訊埠 (TCP Port)，如網頁伺服器通常只開放 TCP 80 (HTTP) 及 TCP 443 (HTTPS)。
- 這種「最小權限」原則可以限制攻擊面，即使伺服器被攻破，攻擊者也難以利用其他未開放的服務進行進一步的破壞。

◆ **需要嚴密控管此區域到內部區域的存取：**

- DMZ 的設計理念是將對外服務的伺服器與內部核心網路進行隔離。因此，從 DMZ 區域到內部網路的流量，必須受到比外部到 DMZ 更為嚴格的控制。
- 通常會有第二道防火牆或更嚴格的防火牆規則，僅允許內部網路發起的請求回應、或者極少數經過嚴格審核的、必要的服務從 DMZ 連向內部網路。這確保了即使 DMZ 內的伺服器被入侵，攻擊者也很難輕易地「跳轉」到更為敏感的內部網路。



(4) 網路管理區域：

◆ 放置機關網路管理設備（如網路管理系統、鑑別系統、監控系統）：

- 這個區域專門用於部署執行網路管理任務所需的各種系統及設備。
- 典型的例子包括：
 - ✓ 網路管理系統 (NMS)：用於監控、組態及管理網路設備（如路由器、交換機、防火牆等）。
 - ✓ 鑑別系統：例如 RADIUS(Remote Authentication Dial-In User Service) 或 TACACS+(Terminal Access Controller Access-Control System Plus) 伺服器，用於對管理員登入網路設備進行身分鑑別及授權。
 - ✓ 監控系統：用於收集網路效能數據、日誌，並提供告警功能。

◆ 應明確標示網路的路徑及維運方式：

對於網路管理區域，其網路連接路徑（如哪些管理設備連接到哪些被管理設備），以及維護操作的標準程序，都應該被清晰地定義及記錄。這有助於規範管理行為，減少錯誤，並在資安事件發生時進行追溯。

◆ 網路設備維運應該與服務的網段有所區隔：

- 這是一個非常重要的安全原則。管理網路設備的連線（例如 SSH、Telnet、SNMP 等）應該與提供業務服務的網路流量分開。理想情況下，應該使用獨立的管理網段 (Out-of-Band Management)，或者至少是邏輯上隔離的 VLAN。
- 這樣做的目的是為了避免當服務網段被攻擊，進而影響網路設備的管理。如攻擊者控制了服務網段，他們可能會嘗試進一步入侵網路設備本身，從而取得對整個網路的控制權。將管理流量隔離，可以為網路設備提供額外的保護層，即使業務網路受到影響，管理員仍然可以透過安全的管理網路進行緊急處理及修復。

(5) 網路記錄區域：

這個區域專門用於儲存重要的網路紀錄及備份資料，其主要特點及管理原則如下：

◆ 放置備份主機 (Backup Server) 及紀錄主機 (Log Server)：

- 備份主機 (Backup Server)：用於儲存各類系統、資料庫、應用程式等的備份。將備份主機放置在一個獨立且受保護的區域，可以確保資料在發生災害或攻擊時能夠被恢復。

- **紀錄主機 (Log Server)：**用於集中收集來自網路設備、伺服器、應用程式等各種系統的日誌 (log) 資訊。集中管理日誌對於安全事件的監控、分析、溯源及稽核至關重要。

- ◆ **存放的網段應特別規劃：**

網路紀錄區域所在的網段應該與其他業務網段、使用者網段等進行嚴格的邏輯或實體隔離。這有助於防止攻擊者在入侵其他區域後，輕易地存取、竄改或刪除重要的日誌和備份資料。

- ◆ **僅允許設備備份與記錄之發送及管理員管理連線行為：**

這個區域的存取控制應該極其嚴格，只允許兩個類型的流量：

- **設備備份與紀錄的發送：**只允許各設備將其備份資料或日誌資訊傳送到這個區域的備份主機及紀錄主機。
- **管理員管理連線行為：**只有經過授權的、用於管理這些備份及紀錄主機的**管理員**，才能進行必要的連線操作。

(6) 實體隔離區域：

這個區域的設計理念是提供最高等級的隔離，通常用於處理極度敏感或有特殊安全要求的系統。其主要特點和管理原則如下：

- ◆ **機關依據特定需求可將部分區域執行實體隔離：**

- 實體隔離意味著這些區域與其他網路間完全沒有實質的網路連線，通常專用於處理高度機密資訊、國家安全事務、需與外部網路完全斷開的重要系統。這是一種最徹底的隔離方式。
- 例如，某些處理國家機密的系統、研發核心技術的實驗室網路、關鍵基礎設施系統，或者需要進行安全審查的特殊環境，都可能採取實體隔離。

- ◆ **單向傳輸：**僅可將資料傳出，不可傳入。

- 在實體隔離的環境中，如果確實需要與外界交換資料，通常會採用「單向傳輸」的方式，即資料只能從高安全區域傳輸到低安全區域（或外部），而不能反向傳入。
- 這通常透過光閘 (data diode) 等單向資料傳輸設備實現，確保資料的流向是單一的，從而防止外部惡意病毒或攻擊進入實體隔離的系統。

- ◆ **可能危害途徑：**

- 儘管實體隔離提供了最高的安全防護，但仍存在一些可能被利用的途徑來繞過或破壞這種隔離。這顯示即使在實體隔離的環境下，仍須落



實嚴謹的管理與安全措施。可能的危害途徑包括：

- ✓ **破解門禁系統**：如攻擊者能夠進入實體隔離區域，那麼所有基於網路的防禦都將失效。這包括利用漏洞、假冒身分或透過其他方式突破實體門禁。
- ✓ **利用隨身碟竊取資料**：即使網路被隔離，如允許使用 USB 隨身碟等可攜式儲存設備，攻擊者仍可能利用這些設備將資料帶出或將惡意軟體帶入，這就是所謂的「空隙攻擊」(air-gap attack)。
- ✓ **私接網路對機密主機連線**：未經授權的人員私自將實體隔離區域內的電腦連接到外部網路，或者將一台外部設備連接到內部機密主機，從而繞過所有安全控制。

7.6.2 網路連線安全

網路連線安全旨在確保資料在傳輸過程中的機密性、完整性與不可否認性。這主要透過加密與數位簽章等技術來實現。以下將針對網路連線安全的核心概念與實現方式進行說明：

(1) 傳輸加密：保護資料機密性

- ◆ 傳輸加密的目的是保護資料在傳輸過程中的機密性，防止未經授權的第三方監聽或竊取通訊內容。應優先採用通道加密（如 VPN）與傳輸層加密（如 HTTPS、SSL/TLS 1.2/1.3），以確保資料在傳輸路徑上的隱私。
- ◆ **為避免已知的資安漏洞，應立即停用以下協定：**
 - SSLv3：存在 POODLE 等嚴重漏洞，應完全禁用。
 - TLS 1.0 / TLS 1.1：被視為過時且存在已知安全缺陷，應停止使用並升級。

(2) 資訊機密性的實現：加密演算法

- ◆ 資訊機密性可透過使用對稱式加密演算法（如 AES-GCM、ChaCha20-Poly1305 (AEAD)）與非對稱式加密演算法（如 RSA 至少使用 2048-bit 或更高長度、P-256(ECC)）來達成。對稱式加密使用相同的金鑰進行加密及解密，效率高；非對稱式加密則使用一對公開金鑰及私有金鑰，常用於金鑰交換及數位簽章。
- ◆ **為避免已知的資安漏洞，應立即停用以下演算法：**
 - RC4：存在偏向性漏洞，應禁用。

- 3DES 因 SWEET32 攻擊的潛在風險，應盡快淘汰

(3) 資訊完整性的實現：數位簽章技術

資訊完整性的確保，主要透過數位簽章技術來達成。數位簽章能驗證資料在傳輸過程中是否被竄改，並提供不可否認性，證明資料確實來自於簽署者。

(4) HTTP、FTP 與 TELNET 不安全的連線協定：明文傳輸的風險

HTTP（超文件傳輸協定）、FTP（檔案傳輸協定）及 TELNET（遠端登錄協定）等連線協定均採用明文傳輸。這意味著通訊內容在網路傳輸過程中是未加密的，極易被有心人士監聽、截取或分析，存在嚴重的資安風險。

(5) HTTPS、FTPS 與 SSH 安全的連線協定：加密傳輸的保障

相較之下，HTTPS（安全超文件傳輸協定）、FTPS（安全檔案傳輸協定）與 SSH（安全外殼協定）是一種加密的網路傳輸協定。它們能在不安全的網路環境中為網路服務提供安全的傳輸環境，有效防止資料遭到竊聽與篡改。特別是 HTTPS 連線時，還需進一步檢查伺服器憑證的有效性，以確認連線對象的身分合法性。

7.6.3 虛擬私有網路 (VPN)

VPN 的用途是在公開的網路上建立虛擬的私有通道，保護通訊資料的機密性與完整性。

(1) VPN 類型：

◆ 遠端使用者存取 VPN：隨時隨地安全連接公司資源

- 遠端使用者存取 VPN 使外勤人員及遠端工作者，即使身處網際網路的任何角落，也能安全地與公司內部網路建立連結。這就像在公眾網路上為您的資料建立了一條專屬且加密的秘密通道，確保資料傳輸的安全。
- 如圖 55 遠端使用者存取 VPN 示意圖所示，一位遠端使用者 (Remote User) 身處廣闊的網際網路 (INTERNET) 上，透過 VPN 設備建立起與公司內部站點 (Site) 的安全連線。這條經過加密的通道，能有效防範資料在公眾網路上被竊取或監聽的風險。
- 這項技術的優勢在於，無論員工是在外出差還是居家辦公，都能像在辦公室內部一樣，輕鬆且安全地存取公司內部的重要資源，例如：



- ✓ **檔案伺服器**：隨時隨地讀取、編輯與儲存公司文件。
- ✓ **內部應用程式**：順暢使用企業內部系統，提升工作效率。
- ✓ **其他內部資源**：享受如同身處辦公室般的網路體驗。

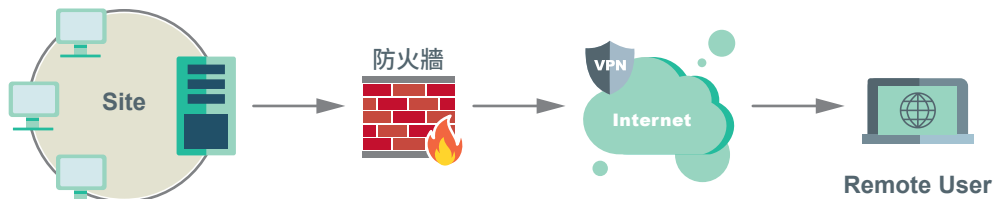


圖 55 遠端使用者存取 VPN 示意圖

◆ **Site-to-Site VPN**：總部與分點之內部網路透過網際網路建立安全通道

- 這種 VPN 類型用於連接兩個或多個地理位置分散的實體網路，例如公司的總部與其各個分公司或分點，如圖 56 Site-to-Site VPN 示意圖所示：

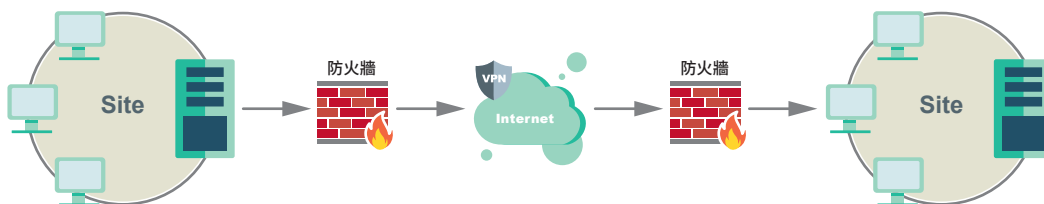


圖 56 Site-to-Site VPN 示意圖

- 「Site」代表一個內部網路（例如總部），另一個「Site」代表另一個內部網路（例如分公司）。兩者之間透過「INTERNET」（網際網路）連接。
 - 在每個站點的邊緣（通常是路由器或防火牆）部署 VPN 設備，建立起一條加密的「VPN」隧道，使得兩個站點的內部網路之間可以安全地通訊，彷彿它們處於同一個大型內部網路中。
 - 這種方式通常用於企業內部不同分支機構之間的資料交換及資源共享。
- ◆ **Extranet VPN**：與合作夥伴間透過網際網路建立安全通道
- Extranet VPN 用於連接組織的內部網路與外部合作夥伴（如供應商、客戶或協力廠商）的網路，如圖 57 Extranet VPN 示意圖所示：

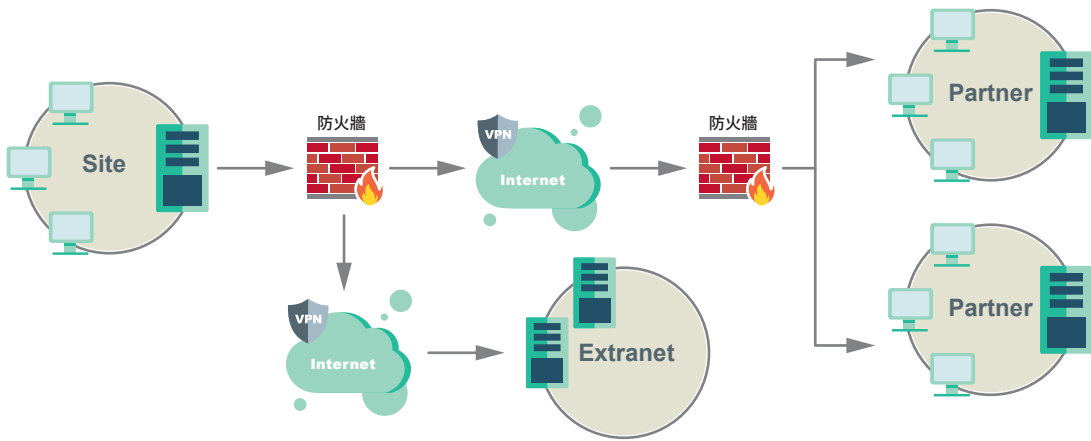


圖 57 Extranet VPN 示意圖

- 「Site」代表組織自身的內部網路，「Partner」代表合作夥伴的網路。
- 組織的內部網路與合作夥伴的網路之間，透過網際網路建立加密的「VPN」通道。
- 這種 VPN 允許組織與其信任的外部實體共享特定資源和資訊，同時保持其他內部數據的隔離和安全。
- **注意存取權限的控管：**由於是與外部夥伴連接，對於 Extranet VPN 來說，存取權限的管理尤為重要。必須精確地控制合作夥伴能夠存取組織內部哪些資源，以及哪些資源可以存取合作夥伴的網路，以避免不必要的資訊洩露或安全風險。

(2) **VPN 管理重點：**為了確保 VPN 的安全和有效運行，需要關注以下幾個管理方面：

◆ **虛擬私有網路的建立與使用者帳號的申請，應建立管理程序（變更申請、核准及記錄）：**

VPN 的建立及使用者帳號的申請（例如遠端使用者存取 VPN），必須有一套標準化的管理流程。這包括變更請求的提交、主管的核准、以及所有相關操作的詳細記錄。這有助於追溯操作、確保合規性，並防止未經授權的存取。

◆ **定期分析異常事件，例如 VPN 使用者簽入失敗：**

需要定期檢查 VPN 設備的日誌，並分析任何異常事件，例如多次登入失敗、來自異常地理位置的連線嘗試、或非預期的連線活動。這些異常可能預示著潛在的攻擊或帳號被盜用。



- ◆ **VPN 存取紀錄應即時匯出存檔，並保留足夠的時間：**

VPN 的所有存取紀錄（例如誰在何時從何地連線、連線時間多長等）都應該即時匯出並安全地存檔。這些紀錄對於安全事件發生後的調查、分析及溯源至關重要，並且應依據法規或內部政策保留足夠長的時間。

(3) VPN 選購考量：

- ◆ **可支援的 VPN 數量或使用者連線數量應滿足機關需求：**

所選購的 VPN 設備或服務，其性能及容量必須能夠支撐組織的實際需求，包括同時在線的 VPN 連線數量、最大吞吐量等。確保不會因為負載過大而影響業務運作。

- ◆ **本身應具備防火牆功能，以控管 VPN 連線的存取：**

理想的 VPN 設備應該內建或與防火牆功能緊密整合。這表示 VPN 設備不僅能建立加密隧道，還能針對隧道內的流量進行細緻的過濾及存取控制，例如限制 VPN 使用者只能存取特定內部資源，而不是整個內部網路。

- ◆ **與其他不同廠牌產品建立 VPN 連線的相容性：**

相容性是關鍵，以確保所選的 VPN 產品能夠與其他廠商的 VPN 設備（例如分支機構或合作夥伴使用的設備）建立穩定的、互通的 VPN 連線，避免因技術不兼容導致無法協同工作。

- ◆ **Extranet VPN 具支援多因子鑑別 (Multi-Factor Authentication, MFA) 功能。**

7.6.4 雲端運算

(1) 特性：

雲端運算是一種透過網路提供服務的模式，其特性包括隨選自助、廣泛網路存取、資源匯聚、快速靈活性、受量測服務及多租用。以下說明雲端運算的六個核心特性：

- ◆ **隨選自助 (On-demand Self-service)：**

使用者可以依據自己的需求，隨時隨地透過自助服務介面（例如網頁入口網站），自行配置及部署所需的運算資源（如伺服器、儲存、網路），無需等待供應商的人工介入。此提供了高度的靈活性及自主性。

- ◆ **廣泛網路存取 (Broad Network Access)：**

雲端服務可以透過標準的網路機制（如網際網路）廣泛地被存取，不受

設備或地點的限制。只要有網路連接，使用者就可以存取雲端資源，實現異地協作和遠端工作。

◆ **資源匯聚 (Resource Pooling)：**

雲端服務供應商將大量的運算資源（如處理器、記憶體、儲存、網路頻寬）匯聚起來，形成一個大型的共享池。

這些資源會動態地分配給多個不同的客戶。當某個客戶不需要這些資源時，它們可以被釋放回池中，並分配給其他需要的使用者。這種模式提高了資源利用率。

◆ **快速靈活性 (Rapid Elasticity)：**

雲端資源可以被快速且彈性地擴展或縮減。當使用者需求增加時，可以迅速擴展資源以應對高峰；當需求減少時，也可以快速縮減資源以節省成本。這種能力使得雲端服務能夠非常靈活地適應變化的業務需求。

◆ **受量測服務 (Measured Service)：**

雲端服務供應商會對資源的使用情況進行監控、測量及報告，通常是按照資源的實際消耗量來計費（例如按小時、按流量、按儲存空間等）。這使得使用者可以清晰地了解自己的資源使用情況，並支付實際使用的費用。

◆ **多租用 (Multi-tenancy)：**

多租用是指多個客戶（租戶）共享同一套基礎設施及應用程式，但每個客戶的資料及配置都是邏輯隔離的，互不影響。這是雲端服務供應商實現資源匯聚及成本效益的關鍵技術。雖然資源是共享的，但透過嚴格的隔離機制，確保了每個租戶的資料安全及隱私。

(2) 服務模式：

雲端運算共有 3 種主要的雲端服務模型，如表 46 雲端運算之服務模式。以下說明各雲端服務模型之使用者與雲端服務供應商各自的管理責任界線。

◆ **基礎設施即服務 (IaaS)：**

- **使用者管理層面：**負責作業系統、中介軟體、應用程式。

在 IaaS 模式下，使用者可以租用雲端供應商提供的基礎運算資源，例如虛擬機（伺服器）、儲存空間、網路設備。使用者需要自行負責這些虛擬資源之上的所有管理，包括作業系統的安裝和配置、中介軟體（如資料庫、Web 伺服器）的部署及管理，以及最終的應用程式的開發及運行。



表 46 雲端運算之服務模式

雲端服務模型	使用者管理層面	雲端服務供應商管理層面
基礎設施即服務 (IaaS)	伺服器、儲存、網路、作業系統、中介軟體（例如資料庫、Web 伺服器）、應用程式	硬體（伺服器、儲存、網路）的管理和維護
平台即服務 (PaaS)	應用程式、資料	硬體、作業系統、中介軟體（例如資料庫、Web 伺服器）的管理和維護
軟體即服務 (SaaS)	應用程式內的使用者設定及資料	硬體、作業系統、中介軟體、應用程式的管理及維護。使用者基本上只需要使用應用程式。

- **雲端服務供應商管理層面：**負責硬體、儲存、網路。

供應商負責底層的硬體基礎設施的管理及維護，包括實體伺服器、儲存設備及網路設備的運行、維護及升級。

◆ **平台即服務 (PaaS)：**

- **使用者管理層面：**負責應用程式、資料。

在 PaaS 模式下，供應商會提供一個已經配置好的應用程式開發及運行平台。使用者不需要管理底層的作業系統或中介軟體。他們只需要專注於部署及管理自己的「應用程式」及「資料」。這大大簡化了開發及部署的複雜性。

- **雲端服務供應商管理層面：**負責硬體、作業系統、中介軟體。

供應商負責底層的硬體、作業系統、以及各種中介軟體（例如資料庫伺服器、Web 伺服器）的管理及維護，確保平台環境的穩定及可用性。

◆ **軟體即服務 (SaaS)：**

- **使用者管理層面：**負責應用程式內的使用者設定及資料。

SaaS 模式下，雲端供應商直接提供可供終端使用者使用的應用程式。使用者不需要管理任何底層的基礎設施或平台。他們主要負責應用程式內的使用者設定（例如個人偏好設定），以及輸入及管理的「資料」。

- **雲端服務供應商管理層面：**負責硬體、作業系統、中介軟體、應用程式。供應商負責所有層面的管理及維護，包括底層硬體、作業系統、中介

軟體，以及應用程式本身的開發、部署、運行及維護。對於使用者而言，這是一種最簡單的服務模式，基本上只需要透過網路存取並使用應用程式。

7.6.5 資通安全防護框架：CMMC 2.0 (2021)

CMMC (Cybersecurity Maturity Model Certification)，即「網路安全成熟度模型驗證」。CMMC 2.0 是美國國防部 (Department of Defense, DoD) 於 2024 年發布的最新修訂版本 (version 2.13)，旨在確保與國防部合作的供應商（包括所有國防工業基地，DIB) 具備足夠的網路安全能力，以保護敏感的非機密資訊（尤其是受控非機密資訊，CUI）。

圖 58 展示了 CMMC Model 2.0（網路安全成熟度模型 2.0) 的架構與評鑑方式，透過一個立體視圖清楚呈現了其三個層級。此圖不僅概括了每個層級的核心「模型 (Model)」要求，同時也詳述了對應的「評鑑 (Assessment)」方法。

聯邦契約資訊 (Federal Contract Information, FCI)：透過實施 Level 1 的基礎要求來保護。受控非機密資訊 (Controlled Unclassified Information, CUI)：透過實施 Level 2 及 Level 3 的進階要求來保護。CMMC 透過分層級的方法，為國防部提供驗證承包商是否符合安全要求的一致性機制，從而加強整個國防供應鏈的資通安全態勢。

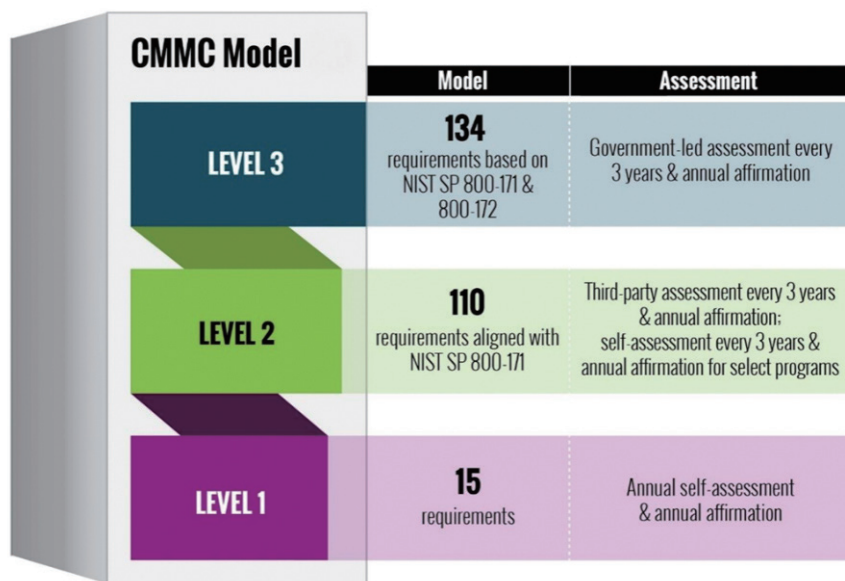


圖 58 CMMC Model 2.0 之模型及評鑑



(1) LEVEL 1 Foundational (基礎級) :

- ◆ 保護對象 :

- 保護聯邦契約資訊 (Federal Contract Information, FCI)。

- ◆ 安全要求 :

- ✓ 總計 15 項要求 (15 requirements)。
 - ✓ 這些要求是基於 48 CFR 52.204-21 (聯邦採購法規，即 FAR) 中規定的基本保障要求。

- ◆ 符合性評鑑 (Assessment) :

- ✓ 必須進行每年自我評鑑 (Annual self-assessment)。
 - ✓ 需進行年度確認 (annual affirmation)。

(2) LEVEL 2 Advanced (進階級)

- ◆ 保護對象 :

- 保護受控非機密資訊 (Controlled Unclassified Information, CUI)。

- ◆ 安全要求 :

- ✓ 總計 110 項要求 (110 requirements)。
 - ✓ 這些要求與 NIST SP 800-171 Rev 2 中的要求完全相同。

- ◆ 符合性評鑑 (Assessment) :

- ✓ 兩種評鑑路徑：
 - 每 3 年第三方評鑑 (Third-party assessment every 3 years) 及年度確認 (annual affirmation)。
 - 針對特定計畫 (select programs)，可以選擇每 3 年自我評鑑 (self-assessment every 3 years) 及年度確認 (annual affirmation)。
 - 需進行年度確認 (annual affirmation)。

(3) LEVEL 3 Expert (專家級)

- ◆ 保護對象：保護 CUI。

- ◆ 安全要求 :

- ✓ 總計 134 項要求 (134 requirements)。
 - ✓ 這些要求是基於 NIST SP 800-171 與 800-172；它包含 NIST SP 800-172 中的一個子集，並具備 DoD 批准的參數。

- ◆ 符合性評鑑 (Assessment) :

- ✓ 必須進行每 3 年政府主導的評鑑 (Government-led assessment every 3 years)。

✓ 需進行年度確認 (annual affirmation)。

7.6.6 雲端安全管理

接著，將深入探討雲端安全管理，特別引用 NIST SP 800-210：雲端系統的一般存取控制指引 (General Access Control Guidance for Cloud Systems)，並藉由圖 59 雲端系統一般架構圖，詳細說明雲端服務堆疊架構，以及客戶與服務之間的互動模式。

NIST SP 800-210：雲端系統的一般存取控制指引是美國國家標準與技術研究院 (NIST) 所發布的一份特別出版物。這份指引旨在為聯邦機構提供雲端服務安全採購、部署及管理的指引，同時也適用於其他組織。它透過提供系統性的指導，協助組織有效地識別、分析、評估及處理資訊安全風險，以保護其資訊資產，確保在雲端環境中的安全與合規。

(1) 雲端系統之一般架構

圖 59 將清晰地展示雲端系統之一般架構，由底層的硬體基礎設施逐步延伸至頂層的應用程式。以下是對各層次的詳細說明：

◆ 第 1 層：硬體 (Hardware)

這是雲端基礎設施的實體層，包括伺服器、儲存設備、網路設備等。這些是雲端運算服務的實體基礎，支撐所有上層服務的運作。

◆ 第 2 層：網路 (Networking)

這層包括雲端環境的網路連接、隔離、路由、負載平衡、防火牆等，確保資料在各層次之間安全高效地傳輸。

◆ 第 3 層：儲存 (Storage)

這層提供資料的儲存服務，包括區塊儲存、檔案儲存、物件儲存等，為應用程式提供持久化資料的空間。

◆ 第 4 層：虛擬機管理程式 (Hypervisor)

這層實現虛擬化的關鍵軟體層，位於硬體之上。它負責管理、排程及監控虛擬機器。在 IaaS（基礎設施即服務）中，這層的控制權通常歸雲端服務提供者所有。

◆ 第 5 層：作業系統 (Operating System)

這層運行在虛擬機器上的作業系統（例如 Windows Server、Linux 等）。在 IaaS 中，這通常是雲端服務提供者提供給客戶選擇並管理的部分；而在 PaaS（平台即服務）中，這層則由雲端服務提供者管理。

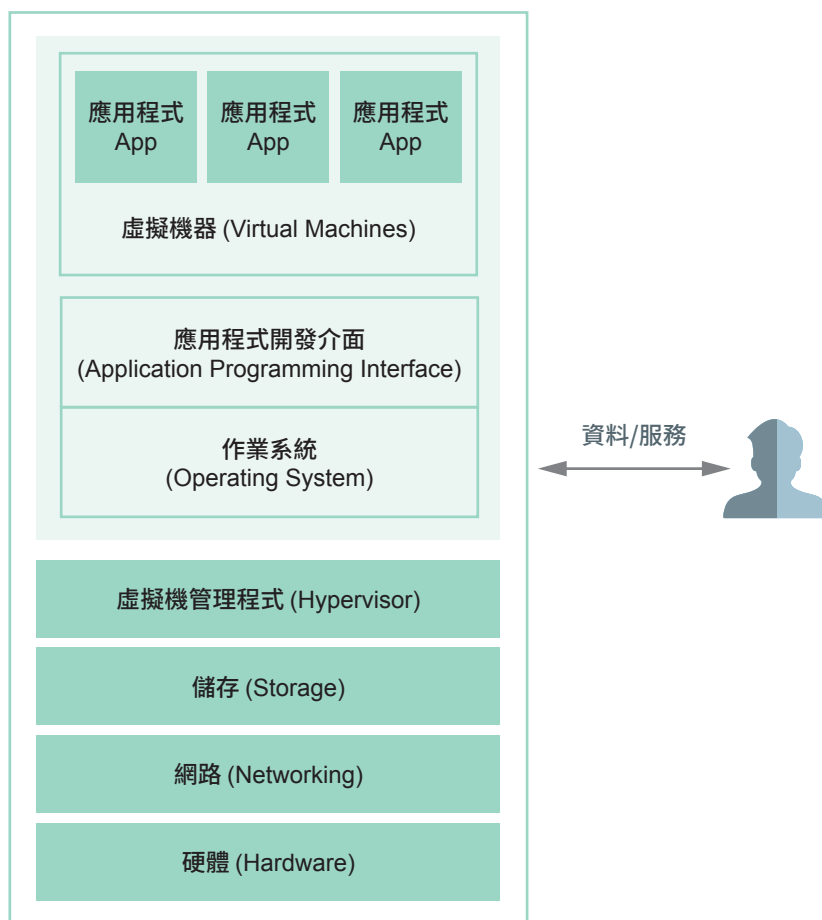


圖 59 雲端系統之一般架構

- ◆ **第 6 層：應用程式開發介面 (Application Programming Interface, API)**
這層 API 定義了應用程式與其他服務或系統互動的標準方法。在 PaaS 或 SaaS（軟體即服務）中，這通常是雲端服務提供者提供的部分，方便雲端服務客戶進行整合或開發。
- ◆ **第 7 層：虛擬機器 (Virtual Machines)**
這是指透過虛擬化技術創建的獨立虛擬計算環境。這些機器運行作業系統及應用程式，是 PaaS 及 IaaS 的主要交付形式。在 IaaS 中，使用者可直接配置及管理虛擬機器。
- ◆ **第 8 層：應用程式 (Applications)**
這是位於雲端堆疊最上層的最終雲端服務客戶應用程式（例如 Web APP、SaaS 服務）。這些是最終用戶直接使用的服務。

◆ 資料 / 服務與使用者互動模式

圖示還會明確展示「資料 / 服務」與「客戶」如何進行互動：

- **資料 / 服務**：這包括用戶在雲端環境中存取及使用的各種類型的資料及服務。
- **客戶**：最終雲端服務客戶是透過各種設備及介面，與雲端服務進行互動，他們透過特定的介面來存取及使用儲存在雲端的資料及服務。

(2) 雲端服務提供者及客戶之存取控制

以下另引用 **NIST SP 800-210** 一個更詳細的圖示，說明 IaaS、PaaS 及 SaaS 這 3 種雲端服務模式下，雲端服務提供者及客戶各自負責其管理層面的存取控制，如圖 60 雲端服務提供者及客戶之存取控制示意圖。

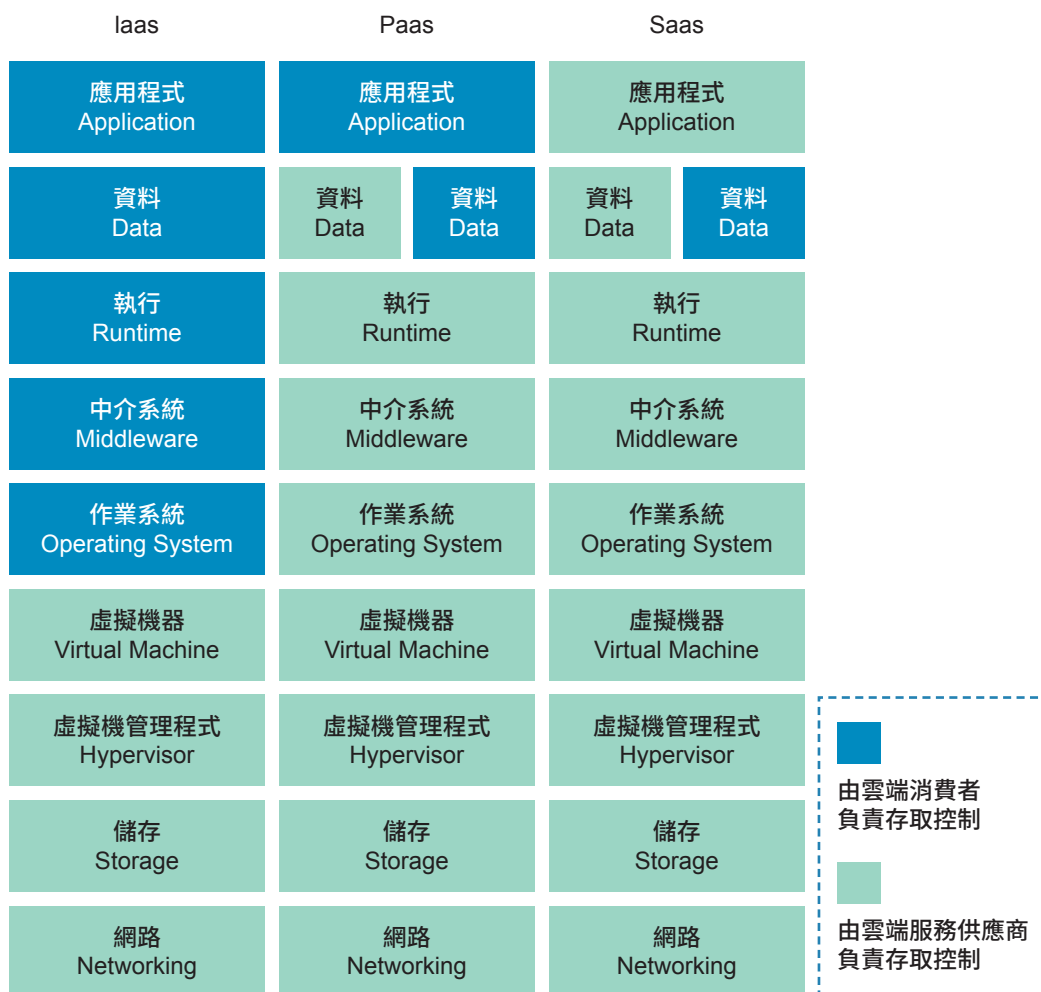


圖 60 雲端服務提供者及客戶之存取控制示意圖

圖 59 以 3 個垂直的堆疊圖來表示 IaaS、PaaS 及 SaaS 共 3 種雲端服務模式，每個堆疊都由底層的硬體往上到最上層的應用程式及資料。綠色區塊表示由雲端服務提供者負責存取控制，藍色區塊表示由客戶負責存取控制。

◆ **IaaS（基礎設施即服務）之存取控制責任歸屬**

- **雲端服務提供者（綠色）**：虛擬機器、虛擬機管理程式、儲存、網路。
- **雲端服務客戶（藍色）**：作業系統、中介系統、執行、資料、應用程式。
- **備註**：這表示在 IaaS 中，雲端提供者提供了基礎的虛擬化硬體資源，而雲端服務客戶則對這些資源之上的所有軟體層面負責，包括操作系統、中介系統、應用程式及其資料。

◆ **PaaS（平台即服務）之存取控制責任歸屬**

- **雲端服務提供者（綠色）**：虛擬機器、虛擬機管理程式、儲存、網路、作業系統、中介系統、執行、資料。
- **雲端服務客戶（藍色）**：客戶資料、應用程式。
- **備註**：在 PaaS 中，雲端服務提供者提供了包括作業系統、中介系統及運行時環境在內的平台，雲端服務客戶則專注於應用程式的開發及資料管理，大大減輕了底層系統管理的負擔。

◆ **SaaS（軟體即服務）之存取控制責任歸屬**

- **雲端服務提供者（綠色）**：虛擬機器、虛擬機管理程式、儲存、網路、作業系統、中介系統、執行、資料、應用程式。
- **雲端服務客戶（藍色）**：客戶資料。
- **備註**：在 SaaS 中，雲端服務提供者負責所有層面的管理，從硬體到應用程式及資料。雲端服務客戶只需透過網路使用應用程式，通常只需要管理應用程式內的使用者設定及輸入自己的資料，其他所有的底層維護都由雲端服務提供者處理。

7.6.7 雲端安全管理 ISO/IEC 27017：2015

本節將聚焦於 ISO/IEC 27017：2015 資訊科技－安全技術－基於 ISO/IEC 27002 之雲端服務資訊安全控制實務準則 (Information technology-Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services)，這份國際標準是一份針對雲端服務資訊安全控制實務的權威準則。這份標準以 ISO/IEC 27002 為基礎，並特別針對雲端服務提

供者及雲端服務客戶的資訊安全需求，增補了多項雲端環境獨有的控制措施與指導原則。我們將探討在雲端環境中進行安全管理時，ISO/IEC 27017：2015 所強調的 7 個專屬控制措施：

(1) 雲端環境下的角色共享與權責：

這是雲端安全管理的核心。由於雲端服務採用「責任共擔模型」，提供者及客戶在不同服務模式下 (IaaS, PaaS, SaaS) 有不同的安全責任。因此，明確界定各方在不同安全控制領域的角色、責任及權限至關重要，以避免責任真空或重複。

(2) 雲端服務客戶資產的移除：

指的是當客戶終止雲端服務時，確保其所有資料及應用程式（即客戶資產）都能被安全、徹底地從雲端服務提供者的基礎設施中刪除，防止資料殘留或洩露。這涉及資料銷毀及清理的流程。

(3) 虛擬運算環境的區隔：

在雲端環境中，多個客戶的虛擬機器及應用程式可能運行在同一實體的硬體上。因此，確保不同虛擬環境之間的嚴格隔離，防止「租戶間隔離失效」或資料洩露，是雲端安全的重要挑戰。這通常透過虛擬化技術及網路隔離來實現。

(4) 虛擬機器強化：

指的是對虛擬機器本身進行安全配置及加固，例如禁用不必要的服務、修補漏洞、實施最小權限原則等。這確保了虛擬機器作為計算單元本身的安全性。

(5) 管理者的操作安全：

雲端環境的管理通常透過 API 或專用管理介面進行。確保雲端管理人員（包括提供者及客戶的管理員）的操作過程安全，例如強身分驗證、嚴格的存取控制、操作日誌審核等，以防止特權濫用或管理帳戶被劫持。

(6) 監控雲端服務：

對雲端環境中的各種活動進行持續監控，包括資源使用、網路流量、安全事件日誌、組態變更等。這有助於及時發現異常行為、安全威脅及潛在的漏洞，並採取應對措施。

(7) 虛擬和實體網路安全管理的一致性：

確保在雲端環境中（虛擬網路）實施的安全策略及控制措施，與傳統實體網路環境中的安全管理策略保持一致性。這包括網路分區、防火牆規則、



入侵偵測及防禦機制等，確保無論是在虛擬還是實體層面，網路安全都得到同等重視及統一管理。

7.6.8 雲端運算 - 資安問題

本節將從客戶端及雲端服務提供者兩個視角，列舉並探討在雲端運算環境中可能面臨的資安挑戰及需要重點關注的面向。

(1) **客戶端：**以下這些問題主要與雲端服務的客戶在雲端環境中可能面臨的安全挑戰有關。

- ◆ **資料竊取：**客戶的敏感資料可能因為配置不當、存取控制缺陷或提供者的漏洞而遭到未經授權的存取或竊取。
- ◆ **資料可用性：**由於提供者的故障、中斷或遭受攻擊，可能導致客戶資料或服務無法正常存取，影響業務連續性。
- ◆ **網路封包竊聽：**儘管雲端環境通常會進行加密，但如果傳輸層未正確實施加密或存在漏洞，資料在雲端內部或傳輸過程中仍可能被竊聽。
- ◆ **資料內容加密保護：**客戶有責任確保其上傳到雲端的敏感資料在靜態（儲存中）及動態（傳輸中）狀態下，都得到適當的加密保護。即使提供者提供加密服務，客戶也應了解其機制，並確保符合自身需求。
- ◆ **共用環境的系統安全防護：**在多租戶雲端環境中，客戶的虛擬機器及應用程式可能與其他客戶共享底層實體基礎設施。客戶需要關注如何確保其環境在這種共享模式下的安全隔離及防護，避免受到來自其他租戶的攻擊或影響。
- ◆ **退租後資料完整刪除：**當客戶終止雲端服務或刪除資料時，需要確保提供者能夠承諾並實際執行對其資料的徹底、不可恢復的刪除，防止資料殘留導致洩露。

(2) **雲端服務提供者：**以下這些問題主要與雲端服務提供者需要負責及解決的安全挑戰有關：

- ◆ **虛擬化環境的系統與網路安全：**提供者必須確保其底層虛擬化基礎設施（包括虛擬機管理程式、虛擬網路及儲存）的系統及網路安全。這包括漏洞管理、安全組態設定、隔離技術的有效性等。
- ◆ **分散式阻斷服務攻擊：**雲端服務提供者需要具備強大的能力來防禦及緩解 DDoS (Distributed Denial of Service) 攻擊，因為這類攻擊可能影響多

個客戶的服務可用性。

- ◆ **即時阻絕資安威脅**：提供者需要建立有效的安全監控、事件偵測及即時反應機制，以便快速識別及阻斷各種資安威脅，保護客戶的資料及服務。

7.6.9 雲端運算 - 服務協定

(1) 雲端服務提供者與客戶之間會訂定契約 (Contract) 與服務水準協議 (Service Level Agreement, SLA)，來規範業者在約定的服務提供期間能達到客戶要求。

- ◆ 這指出在雲端服務的關係中，正式的法律文件是不可或缺的。
- ◆ **契約 (Contract)**：是雙方關係的總體法律約束，涵蓋了服務範圍、費用、終止條款、責任等。
- ◆ **服務水準協議 (SLA)**：則是契約的補充，更具體地定義了服務品質的各項指標及提供者應達到的效能標準。這兩者共同確保了服務提供方按照預期滿足客戶的需求。

(2) 契約明訂業者應提供的服務及罰則，而服務協定提供的是數值的度量，用來客觀的衡量業者提供的特定服務項目是否滿足客戶要求。

- ◆ **契約 (Contract)**：主要側重於定義服務提供者的義務、責任範圍，以及未履行義務時的懲罰條款（罰則），它提供了一個法律框架。
- ◆ **服務水準協議 (SLA)**：則更加具體及量化，包含了可測量的指標，例如服務的可用性（例如 99.9% 的正常運行時間）、性能（例如延遲、吞吐量）、反應時間、資料備份頻率、恢復時間目標 (RTO) 及恢復點目標 (RPO) 等。這些數值化的度量可以客觀地判斷雲端服務提供者是否達到了客戶期望的服務水平。如果未達到 SLA 中約定的標準，通常會觸發契約中的罰則。

網路安全是一個涵蓋廣泛且層次複雜的領域。從網路區域規劃的基礎，到網路連線的加密保護，再到 VPN 及雲端運算等先進技術的應用，組織必須全面考量並實施相應的措施，才能有效地保護網路環境與資訊資產。

7.7

實體安全

實體安全是資通安全防護體系中不可或缺的一環，旨在保護資訊資產所處的實體環境免受各種威脅，確保其機密性、完整性與可用性。這包括防範天然災害、供應鏈中斷、人為破壞及政治事件等外部與內部風險。

7.7.1 威脅類型

實體安全面臨的威脅主要可分為四大類：

- (1) **天然環境災害**：包括水災、颱風、地震、土石流、山崩及極端溫度等。這些災害可能導致建築物損壞、電力中斷、設備毀損等。
- (2) **供應系統中斷**：包括電力、通訊、瓦斯及水等。這些基礎設施服務的中斷會直接影響機房、辦公室等場所的正常運作。
- (3) **人為的破壞**：包括火災（電線短路、惡意縱火）、非授權入侵、破壞、偷竊、爆裂物及員工疏失（意外斷電、誤操作）等。
- (4) **政治事件**：包括抗議團體與恐怖組織。可能導致實體設施被破壞、運營中斷，甚至人員安全受到威脅。

7.7.2 防護措施規劃

實體安全防護措施的規劃應採多層次「縱深防禦」策略，旨在「嚇阻」犯罪發生、「延遲」入侵時間、「偵測」實體威脅，並在事件發生後「評估」事件狀態，並「處理」回復正常。

- (1) **「嚇阻」犯罪發生**：透過圍牆、警衛、警告標語及狗、夠大聲的警報器、加強警衛巡守頻率、布建全時攝影系統、公布違反實體控管要求人員姓名、簽署認同相關實體控管規範及訂定相關罰則等，以威懾潛在犯罪者。
- (2) **「延遲」入侵時間**：透過門鎖、隔間、人員及標示牌、階層式的防護設計（從門口到重要資產需要經過層層關卡），以延緩入侵者到達目標資產的時間。
- (3) **「偵測」實體威脅**：透過門窗開啟偵測、紅外線進出感應、動作感應器、煙霧偵測器、溫濕度偵測等，以及時發現並發出警報。

- (4) **「評估」事件狀態**：警衛應具備緊急處理標準程序，對事件性質、範圍及潛在影響進行判斷。
- (5) **「處理」回復正常作業**：明確處理人員或組織，制定相關緊急處理程序，並與警察、消防及醫療人員聯絡與通報。
- (6) **縱深防禦的脆弱環節**：攻擊（威脅）可能在「嚇阻」、「偵測」、「處理」及「逮捕」任一環節失敗或執行太慢，最終導致「攻擊成功」。因此，每個環節都必須有效運作並相互配合，如圖 61 縱深防禦機制流程圖。

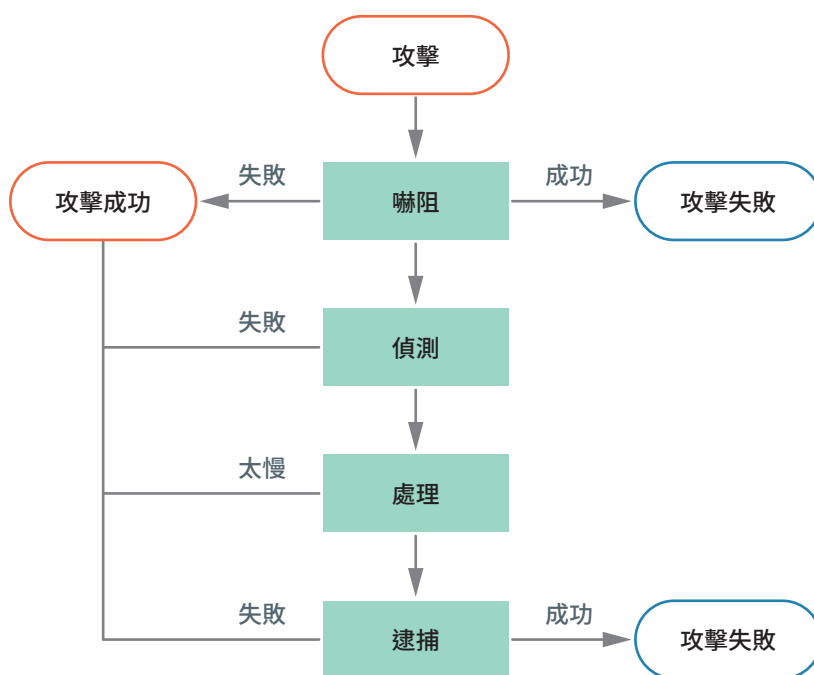


圖 61 縱深防禦機制流程圖

◆ 縱深防禦的脆弱環節在哪裡？

圖 60 之流程圖，描繪攻擊從開始到成功的各種路徑，同時也指出縱深防禦中的各個環節可能出現的問題。從流程圖中，我們可以識別出縱深防禦的脆弱環節：

- **「攻擊」**：流程的起點，代表潛在的威脅或惡意行為。
 - ✓ 攻擊發生後，首先面對的是防禦的第一道關卡：「嚇阻」。
- **「嚇阻」**：
 - ✓ 若嚇阻成功，則「攻擊失敗」。



- ✓ 若未被嚇阻且未被偵測到，則導致「攻擊成功」。
- ✓ 若未被嚇阻但被後續偵測到，則攻擊將進入下一個階段：「偵測」。
- 「偵測」：
 - ✓ 在偵測階段，若偵測系統**失敗**（未能發現入侵），則攻擊者可能直接導致「攻擊成功」。
 - ✓ 若偵測**成功**，則事件會進入「處理」階段。
- 「處理」：
 - ✓ 若在處理階段**太慢**，未能及時應對，攻擊也可能導致「攻擊成功」。
 - ✓ 若處理得當，事件會進入「逮捕」階段（這應理解為採取進一步的行動來制止攻擊者或其活動）。
- 「逮捕」：
 - ✓ 若逮捕**成功**，則「攻擊失敗」。
 - ✓ 若逮捕**失敗**，則最終導致「攻擊成功」。

7.7.3 進出控管

進出控管旨在管理人員及物品進出受控區域，以防止未經授權的進入，並確保可歸責性。以下說明需要進行實體進出控管的場所及實現進出識別的各種方式：

- (1) **進出口管理**：需要控管的進出口，包括主要與次要進出口（大門 / 側門）、緊急疏散出口、車輛與貨物進出口、屋頂、維護孔及窗等。
- (2) **進出識別**：
 - ◆ **識別證**：有相片的識別證，由警衛檢查。
 - ◆ **生物特徵辨識**：指紋、虹膜、臉部辨識等。
 - ◆ **卡片識別**：持有卡片識別。
 - ◆ **多重鑑別**：門禁卡及 PIN 碼雙重鑑別。
- (3) **尾隨進出**：
 - ◆ 非授權人員跟隨授權人員一起進入管制區域。
 - ◆ 防範措施包括警衛與人員的訓練與認知、旋轉門、驗票閘門、以及 Mantrap（人行閘）結合警衛或內外門的鑑別機制。

7.7.4 安全區域規劃

安全區域規劃旨在清楚界定規劃不同屬性的區域，作為存取控制與安全規劃的基準群組，避免來自內部與外部的攻擊，並防範災害擴大。以下說明如何進行安全區域的規劃：

(1) 需要加強保護的區域：

電腦資訊設備機房、儲存媒體存放室、電力與空調設備機房、電話與資料線路配接室、監控與錄影機房、管道間。

(2) 安全區域劃分：

安全區域的空間規劃應依據不同的安全等級進行劃分，以確保資訊資產獲得適當的保護。在規劃圖面上，必須清晰標示每個區域所屬的安全等級，例如「作業區」、「限制區」、「公開區」或「機敏區」。圖 62「安全區域劃分示意圖」即展示了這種分級管理的原則，其詳細說明如下。

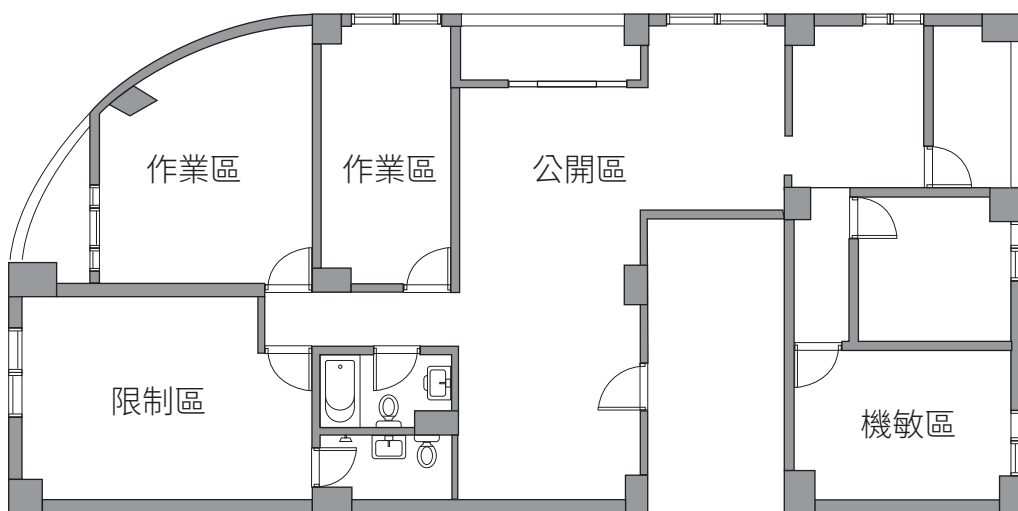


圖 62 安全區域劃分示意圖

- ◆ 「作業區」：通常指需要特定身分驗證才能進入的區域，例如部門辦公室。
- ◆ 「限制區」：指對進入人員有更嚴格限制的區域，可能需要額外的授權或陪同，如同伺服器機房前廳。
- ◆ 「公開區」：指訪客可以自由活動的區域，如大廳、接待區。
- ◆ 「機敏區」：指存放最敏感資料或關鍵設備的核心區域，通常需要最高等級的存取控制及監控，例如主機房內部。



(3) 安全偵測與滅火器位置規劃：

本節延續先前的安全區域劃分概念，將進一步探討如何在這些不同安全等級的區域中，規劃安全偵測設備與滅火器的配置位置。此外，對於具備較高安全等級的隔間，也將說明其所需的實體強化要求。規劃內容請參考圖 63「安全偵測與滅火器位置規劃示意圖」，其詳細說明如下。



圖 63 安全偵測與滅火器位置規劃示意圖

◆ 煙霧偵測器應置於天花板下風處：

這是為了確保在火災發生初期，煙霧能夠最快地被偵測到，通常煙霧會向上升並隨氣流飄散。在下風處佈置有助於及時發現。煙霧偵測器的位置分散佈置於各區域，包括「作業區」、「公開區」、「限制區」及「機敏區」。

◆ 滅火器應置於容易取得的位置：

為了在火災發生時能夠快速反應並使用，滅火器必須放置在易於接近、顯眼且不妨礙通行的位置。滅火器的位置同樣分散在各區域。

◆ 門窗開啟感應器：

這些感應器用於偵測門窗是否被非法開啟，觸發警報。主要分佈在進出口以及「機敏區」的窗戶附近，以加強對敏感區域的監控。

◆ 動作感應器：

用於偵測區域內的物體移動，是另一種入侵偵測手段。

- ◆ **溫濕度偵測器：**

用於監測環境的溫濕度，尤其在機房等對環境要求嚴格的區域，防止設備因環境異常而受損。

- ◆ **安全區域等級較高的隔間：**

應採用足夠強度的牆面，確定牆面由實際建物樓地板連接到天花板，通風口應加裝鐵網。

7.7.5 監視錄影

監視錄影系統是實體安全不可或缺的工具，其能有效監控場所、記錄事件，並在異常情況發生時提供關鍵證據。以下將介紹現代監視錄影系統的類型，以及選擇時應考量的關鍵因素。

(1) 監視錄影系統的類型：

現代監控系統的功能日益多元，從基礎的影像錄影到進階的智慧分析，都能滿足不同的安全需求：

- ◆ **單純錄影：**

這是最基礎的功能，系統僅負責捕捉與記錄影像畫面，不進行任何分析判斷。

- ◆ **動作偵測功能：**

系統能智慧偵測畫面中的物體移動。一旦偵測到動作，便會自動觸發錄影或發出警報，有效節省儲存空間並提升監控效率。

- ◆ **行為分辨：**

比動作偵測更為進階，此功能可識別特定的行為模式，例如人員徘徊、異常聚集、物品遺留或移除等，並在發現異常時即時發出警示。

- ◆ **身分識別：**

這是最複雜也最先進的功能，通常結合了臉部辨識技術，能從影像中辨識出特定人員的身分。

(2) 選擇合適的錄影系統考慮：

選擇及部署監視錄影系統時，需要綜合考慮以下多個因素，以確保其達到預期的安全效果：

- ◆ **CCTV 的目的（偵測 / 行為 / 識別）：**首先要明確安裝監控的目的，是為了單純的偵測入侵、分析特定行為，還是需要進行身分識別。不同的目



的會決定所需系統的功能及複雜程度。

- ◆ **CCTV 攝影機的放置環境（室內 / 室外）：**

攝影機的放置地點（室內或室外）會影響其所需的防護等級（如防水、防塵、防破壞）、光照適應性（如是否需要紅外線功能）及視野範圍。

- ◆ **需要監視錄影的區域（數量？）：**

明確需要監控的具體區域及其大小，以確定所需攝影機的數量、類型及部署角度。

- ◆ **監視錄影區域的照明（需要紅外線？）：**

評估監控區域的光線條件。若光線不足或需要在夜間監控，則需要選擇具備紅外線 (IR) 功能的攝影機來提供夜視能力。

- ◆ **儲存空間與保存期限需求：**

依據錄影的頻率、畫質、攝影機數量，以及法律法規或內部政策對錄影資料保存時間的要求，規劃足夠的儲存空間。

(3) 與其他安全系統的整合需求：

考慮監視錄影系統是否需要與其他安全系統（如門禁系統、警報系統、入侵偵測系統、消防系統）進行整合，以實現連動反應，例如當入侵警報觸發時，自動調出相關攝影機畫面，並開始錄影。

7.7.6 空調規劃

空調系統不僅是提供舒適環境的工具，更是保障設備運行、人員安全，以及應對突發事件的重要環節，需要進行嚴謹的功能設計及系統規劃。本節主要說明空調系統在實體安全中所扮演的角色及其相關規劃要點：

(1) 空調系統的功能：

- ◆ **溫度調節：**指出機房區域與人員作業對溫度的需求不同，需要進行區分調節。
- ◆ **濕度調節：**強調濕度對設備及靜電的影響。濕度過高容易導致設備生鏽，濕度過低則容易產生靜電。理想的相對濕度應控制在 40% ～ 60% 之間。
- ◆ **換氣功能：**說明換氣功能的重要性，即保持空氣新鮮及流通。

(2) 空調系統規劃：

- ◆ **安全區域應維持正風壓：**這是一個關鍵的安全設計原則，意指開門時風會往外吹。其目的是讓煙霧及不好的氣體向外流動，防止外部有害物質

進入安全區域。

- ◆ **保護進氣口：**旨在避免惡意污染，確保進入空調系統的空氣是新鮮的。
 - ◆ **自動偵煙與自動關閉機制：**說明系統應具備在偵測到煙霧時自動關閉的功能，以防止火勢蔓延或有害氣體擴散。
 - ◆ **緊急手動開關關閉：**提供手動控制的選項，以便在火災或發現不良氣體在室內散播時能緊急關閉系統。
- (3) **獨立的電力供應線路：**強調空調系統應有獨立的電源供應，確保其在其他電力系統故障時仍能正常運作，提高可靠性。
- (4) **文件描述維護程序：**意味著需要有詳細的文件來記錄及指導空調系統的維護程序，確保系統的長期穩定運行。

7.7.7 電力來源

在實體安全規劃中，電力來源的設計需要考慮到冗餘性和可靠性，不僅要有日常使用的主要電力，更要有能在突發情況下接手的次要電力來源，以應對各種電力中斷或不穩定的情況，確保關鍵系統的持續運行。以下介紹電力供應的分類及其作用：

(1) 主要電力來源：

- ◆ **供應日常電力：**指的是企業或設施日常運作所依賴的主要電力供應，通常來自於市電網（公共電網）。
- ◆ **必要時由變電所提供專屬電力供應：**這表示對於一些對電力穩定性要求極高的設施（例如大型資料中心、關鍵基礎設施），可能會直接從變電所引入專屬的電力供應線路，以確保更穩定、高品質的電力，減少因公共電網波動造成的影響。

(2) 次要電力來源：

- ◆ **當主要電力來源中斷時使用之電力（例如：發電機）：**這是備用電力系統的核心，當主要電力來源（市電）發生故障或中斷時，次要電力來源會立即啟動，接手供電，確保重要設備的持續運作，避免服務中斷和資料損失。
- ◆ **必要時由額外的變電所提供電力：**這是一種更高級別的電力冗餘策略。除了主要變電所的專屬供應外，還可能從另一個獨立的變電所引入電力，形成雙重或多重電力備援，進一步提升供電的可靠性及安全性。



7.7.8 電力備援

不斷電系統 (UPS) 在電力備援中扮演著關鍵角色，其核心功能是在市電異常（例如停電或電壓不穩）時，立即為所連接的設備提供穩定電力，確保設備能夠持續運作或安全關機。UPS 主要分為以下兩種主要類型：

(1) 在線式 (Online) UPS：

- ◆ 不論市電是否正常，電力的供應會通過 UPS 系統：

這是在線式 UPS 最重要的特點。它會持續將輸入的交流電轉換為直流電（充電並給電池供電），再將直流電逆變為純淨的交流電輸出給設備。這意味著設備永遠是從 UPS 的逆變器取電，而不是直接從市電取電。

- ◆ 當電力中斷時無需切換：

因為設備始終由 UPS 的逆變器供電，所以當市電中斷時，UPS 只是停止從市電取電，繼續使用電池供電，過程中沒有任何切換時間（零轉換時間），對敏感設備的影響最小。

- ◆ 電力的供應較為穩定：

由於電力經過「交流轉直流再轉交流」的雙重轉換，UPS 能有效濾除市電中的各種雜訊、突波、電壓不穩等問題，提供最純淨、最穩定的電力輸出。

- ◆ 適合對電力供應品質要求較嚴格的使用者：

由於其穩定性高、零轉換時間，以及對電力的優異處理能力，在線式 UPS 通常應用於伺服器、網路設備、精密儀器、醫療設備等對電力品質要求極高的關鍵應用場所。

(2) 非在線式 (Offline) UPS：

- ◆ 平時電力的供應並不會通過 UPS 系統：

與在線式不同，非在線式 UPS 在市電正常時，會讓市電直接 bypass（旁路）UPS，直接供應電力給設備。UPS 的逆變器此時處於待機或充電狀態。

- ◆ 只有當市電供應中斷時，設備的電力供應來源才會切換至 UPS 系統，持續供應電力：

當非在線式 UPS 偵測到市電異常時，它才會啟動逆變器並切換到電池供電模式。這個切換過程會有一個短暫的延遲（通常為幾毫秒到十幾毫秒），對於大多數非敏感的家用或辦公設備而言，這個延遲是可以接受的。

7.7.9 電力干擾

在實體安全領域中，電力品質的重要性不容忽視。電力供應的不穩定不僅會對資訊系統造成損害，更可能導致服務中斷及資料遺失。以下將說明電力不穩定可能引發的問題，強調電力狀態監測與記錄的必要性，並列舉常見的電力干擾來源，以提醒組織警惕並採取必要的防範措施。

(1) 電力供應常受到外部環境的干擾而導致電力供應不穩定：

這點是整個議題的起因，強調電力供應的穩定性容易受到外部因素影響。

(2) 電力供應不穩定將導致：不穩定的電力會對設備及資料造成多種負面影響。

- ◆ **設備故障（突然的高電壓）**：過高的電壓（如電壓尖峰或突波）可能瞬間損壞電子元件，導致設備故障甚至燒毀。
- ◆ **設備運作不正常（突然的低電壓）**：電壓突然降低（如電力驟降）可能導致設備無法正常啟動、運行不穩，甚至關機。
- ◆ **系統效能降低（持續低電壓）**：長時間的低電壓運行會影響設備的效能，使其無法達到最佳工作狀態。
- ◆ **瞬間資料遺失（電力不穩定）**：電力不穩定，無論是電壓波動、瞬間中斷或雜訊，都可能導致設備運行異常，進而造成資料來不及儲存或傳輸中斷，導致資料遺失。

(3) 電力供應的狀態應被偵測與記錄：為了有效管理電力問題，監測及記錄電力品質至關重要：

- ◆ **以掌握供電來源的品質**：透過持續監測電壓、電流、頻率等電力參數，可以了解供電來源的穩定性。
- ◆ **作為改善供電的依據**：監測數據能提供電力品質問題的證據，有助於分析原因並制定相應的改善措施，例如安裝穩壓器、突波抑制器或升級供電設施。

(4) 電力干擾來源：導致電力供應不穩定的主要外部來源包括：

- ◆ **閃電**：雷擊會產生巨大的電壓和電流，直接擊中或在附近感應產生突波，對電力系統及連接設備造成毀滅性打擊。
- ◆ **高壓電塔**：雖然高壓電塔主要用於輸電，但其周圍電磁場或可能發生的故障也可能間接影響附近電力品質。
- ◆ **電纜線**：老化、損壞或維護不當的電纜線可能導致電力洩漏、短路或不穩定。



- ◆ **電器用品：**同一電路中的大功率電器（如馬達、空調）啟動或關閉時，可能產生瞬間的電壓波動或雜訊，影響其他設備。

7.7.10 靜電防範

靜電累積是電子設備的隱形殺手，尤其在低濕度環境中，其潛在的破壞力更是不容小覷。靜電放電能對電腦設備造成嚴重且不可逆的損壞。因此，採取完善的防靜電措施至關重要。以下將說明如何有效防止靜電對電腦設備造成危害。

- (1) **在機房使用抗靜電高架地板：**高架地板通常由導電材料製成，並與接地系統連接，可以有效地將人員或設備產生的靜電電荷導走，防止靜電積聚及放電。
- (2) **使用抗靜電桌面：**在工作台面上使用抗靜電墊或桌面，這些材料同樣具有導電性，可以提供一個安全的工作表面，避免靜電損壞放置其上的電子元件。
- (3) **建築物、機房、電力設備及電腦設備要正常接地：**正確的接地是防靜電及電氣安全的基本要求。所有金屬結構、設備外殼及電力系統都應正確接地，以便將靜電電荷安全地導回大地，避免電荷積累。
- (4) **空調維持在合適的濕度：**適當的濕度有助於防止靜電累積。通常建議將濕度控制在相對濕度 40%~60% 之間，這能使空氣中的水分子幫助電荷消散。濕度過低是靜電產生及積聚的主要原因之一。
- (5) **在機房中不使用地毯，若有必要請使用抗靜電的地毯：**普通地毯容易因摩擦而產生靜電。在機房等敏感環境中，應避免使用地毯；若必須使用，則應選用具有抗靜電功能的地毯，以減少靜電產生。
- (6) **在組裝或拆解電腦硬體時戴上抗靜電手環：**當直接接觸電腦內部組件時，人體可能帶有的靜電電荷會對敏感元件造成損壞。佩戴與接地系統連接的抗靜電手環，可以將人體靜電安全導走，保護設備。

7.7.11 滅火方式

滅火的核心在於有效控制火災賴以存在的四大要素：熱能、可燃物、氧氣及化學鏈反應。了解並針對這些因素採取措施，是達成有效滅火的關鍵，這些基本原理廣泛適用於各類火災事故的預防與處理。以下將明火災的構成因素及

相應的滅火方式。

(1) 火由四種因素組成：

- ◆ **可燃物**：指任何能夠燃燒的物質，如木材、紙張、油料等，它們是火勢蔓延的燃料。
- ◆ **溫度超出燃點**：達到並維持可燃物燃點所需的熱量，是引發及維持燃燒的必要條件。
- ◆ **氧氣**：空氣中的氧氣是助燃劑，燃燒過程離不開它的支持。
- ◆ **化學反應**：燃燒是一個自我維持的連鎖反應過程，由燃料與氧氣在高溫下產生自由基，進而持續釋放熱能及光。

(2) 滅火的方式：針對上述火的構成要素，滅火策略可歸納為以下 4 種：

- ◆ **降低溫度（冷卻法）**：透過吸熱作用將燃燒物的溫度降至燃點以下。最常見的手段是噴水，水能大量吸收熱量並汽化，有效降低火場溫度。
- ◆ **去除可燃物（隔離法）**：移除或隔離燃燒中的物質或其附近的潛在燃料，切斷火勢的供給源。例如關閉瓦斯閥門、移開易燃物品或建立防火帶。
- ◆ **去除氧氣（窒息法）**：降低火場周圍空氣中的氧氣濃度至無法支持燃燒的水平。常見方法包括使用滅火毯覆蓋、噴灑二氧化碳或泡沫，形成隔絕層。
- ◆ **瓦解燃燒的化學反應（中斷法）**：使用特殊的滅火劑干擾或中斷燃燒的化學連鎖反應，阻止其持續進行。乾粉滅火劑及潔淨滅火劑即是透過此原理來撲滅火焰。

(3) 不同的可燃物必須採用適合的滅火方式：

這是因為不同物質燃燒的特性不同，若使用不當的滅火劑，可能無法有效滅火，甚至造成更大的危害

表 47 不同類型可燃物之滅火方式，係依據內政部消防署的防火宣導及教學指引，以表格方式說明各類可燃物所屬的火災類別，並列出應採用的合適滅火方法。



表 47 不同類型可燃物之滅火方式

火災分類	別名	可燃物	滅火方式
A	普通火災	木材、紙張、衣服及塑膠	水、ABC 類乾粉、泡沫之滅火器
B	油類火災	石油、焦油、油、溶劑、酒精及液態瓦斯	BC 類或 ABC 類乾粉、泡沫、CO ₂ 、FM-200 之滅火器
C	電氣火災	電器設備、電路及電纜	BC 類或 ABC 類乾粉、CO ₂ 、FM-200 之滅火器
D	金屬火災	鎂、鈉及鉀	乾粉（特殊滅火藥劑）

◆ A 類火災

- 別名：普通火災。
- 可燃物：木材、紙張、衣服及塑膠。
- 滅火方式：水、ABC 類乾粉、泡沫之滅火器。

◆ B 類火災：

- 別名：油類火災。
- 可燃物：石油、焦油、油、溶劑、酒精及液態瓦斯。
- 滅火方式：BC 類或 ABC 類乾粉、泡沫、CO₂、FM-200 之滅火器。

◆ C 類火災：

- 別名：電氣火災。
- 可燃物：電器設備、電路及電纜。
- 滅火方式：BC 類或 ABC 類乾粉、CO₂、FM-200 之滅火器。

◆ D 類火災：

- 可燃物型態：金屬火災。
- 可燃物：鎂、鈉及鉀。
- 滅火方式：乾粉（特殊滅火藥劑）。

7.7.12 漏水偵測

在資訊機房這類對環境極度敏感的場所，漏水偵測與預防的重要性不言而喻。即使是旨在保護資產的消防系統，其本身也可能帶來意想不到的水損風險，這使得機房需要採用特殊的滅火裝置。因此，在關鍵位置部署漏水偵測器，是保護昂貴設備及建築物基礎設施不可或缺的措施。以下將詳細說明資訊機房中漏水偵測的重要性，以及偵測位置的規劃。

- (1) **消防灑水系統可能會有漏水的問題：**儘管消防灑水系統是滅火的重要設施，但其本身也存在潛在的漏水風險，尤其在機房等對水敏感的環境中，一旦發生漏水，後果可能非常嚴重。
- (2) **機房無法灑水時，需裝設特殊滅火裝置：**這與前面提及的滅火系統選擇相呼應，強調機房不適合使用會對電子設備造成水損的灑水系統，應選用如氣體滅火系統等特殊裝置。
- (3) **水的偵測可避免損害：**及早偵測到漏水可以防止對以下關鍵資產造成損害。
 - ◆ **設備：**指機房內的伺服器、網路設備、儲存設備等。
 - ◆ **鋪設地板：**高架地板下通常佈設有線纜及管線，漏水會腐蝕地板，並損壞下方的基礎設施。
 - ◆ **牆：**水分可能滲透牆壁，導致結構損壞、霉菌滋生或電路短路。
 - ◆ **電腦：**水對電腦硬體有直接的腐蝕及短路風險。
 - ◆ **建築物基礎：**長期的水分滲透會影響建築物的結構穩定性。
- (4) **偵測水的位置：**為了有效地偵測漏水，感測器應放置在關鍵位置。
 - ◆ **高架地板下：**機房通常使用高架地板，下方空間是線纜、管線及冷卻系統的通道，也是漏水最可能首先積聚並造成損害的地方。
 - ◆ **天花板：**天花板上方可能有水管或空調系統，一旦漏水，可能會直接滴落到設備上。

實體安全是資通安全防護中不容忽視的環節。透過對威脅類型的全面認識、多層次的防護措施規劃、嚴格的進出控管、合理的安全區域劃分、持續的監視錄影、精準的環境與電力管理，以及完善的消防與漏水偵測系統，組織能夠有效地保護其資訊資產所處的實體環境，為資訊系統的穩定運作提供堅實保障。

單元

8

資訊委外安全管理

隨著數位轉型的加速，許多組織為提升效率、降低成本或獲得專業能力，會將部分資訊委託給外部廠商。然而，資訊委外在帶來便利的同時，也伴隨著顯著的資通安全風險，如資料外洩、系統遭駭或服務中斷等。若缺乏妥善的管理與監督，這些風險可能對組織造成嚴重的財務損失、聲譽損害甚至法律責任。

本單元將引導讀者全面了解資訊委外安全管理的各個面向，從相關法規規範、委外類別及形態的識別，到潛在風險的分析與防範。將深入探討資訊委外的生命週期中，各階段應如何融入資安要求，以及如何透過嚴謹的計畫、招標、決標、履約管理、驗收與保固等環節，確保委外的資通安全。

本單元學習重點如下：

- 1** 了解資訊委外相關法規，掌握其核心規範與要求。
- 2** 認識資訊委外的類別及形態，辨識不同委外模式的特點。
- 3** 理解資訊委外潛在的風險，特別是遠端維運的安全挑戰。
- 4** 掌握資訊委外的生命週期，了解各階段的資安重點。
- 5** 學習資訊委外各階段的資安要求，從計畫到保固，確保委外所有流程的安全。



8.1

資訊委外之相關法規

資訊委外雖然帶來便利，但也潛藏著資通安全風險。因此，我國已建立一系列法規，旨在規範委外行為，以有效管理資安風險。因此，了解下列與資訊委外安全管理的相關法規，至關重要。

8.1.1 《資通安全管理法》第 9 條

依《資通安全管理法》第 9 條規定：「公務機關或特定非公務機關，於本法適用範圍內，委外辦理資通系統之建置、維運或資通服務之提供，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。」，這條文確立了資訊委外應遵循的核心原則：

- (1) **適用對象**：強調了法律適用的對象，包括公務機關及特定的非公務機關。
- (2) **委外範圍**：包括資通系統的建置、維運及資通服務的提供。
- (3) **選任考量**：應綜合考量受託廠商的專業能力、經驗、委外項目性質及資安需求。
 - ◆ **專業能力與經驗**：在選擇受託者時，務必評估其專業能力與經驗，以確保其具備足夠的技術與知識來處理資訊安全問題。
 - ◆ **委外項目性質與資安需求**：不同的委外項目，其資訊安全需求會有差異。例如，涉及機敏資料的系統，其資安要求會遠高於一般網頁服務。
- (4) **監督責任**：選定適當的受託者後，不是就放任不管。機關必須持續監督受託者的資通安全維護情形，以確保其符合契約與法規要求。

8.1.2 《資通安全管理法施行細則》第 4 條第 1 項

為更進一步具體化《資通安全管理法》第 9 條的規定，於《資通安全管理法施行細則》第 4 條第 1 項詳細列出了委託機關在選任及監督受託者時應注意的事項。以下這 9 款規定詳述了資通服務委外時，從選擇、簽約、執行到終止整個生命週期的資安管理要求，並強調委託機關對風險的持續管理責任。了解並落實這些要求，是降低委外資安風險的關鍵。包括：

- (1) **資安管理能力：**受託者辦理受託業務之相關程序及環境，應具備完善資通安全管理措施或通過第三方驗證。
- (2) **專業人員配置：**受託者應配置充足且經適當資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員。
- (3) **業務複委託規範：**受託者辦理受託業務得否複委託、得複委託之範圍與對象，及複委託之受託者應具備之資通安全維護措施。
- (4) **業務涉及國家機密：**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，管制出境。
- (5) **安全性檢測：**受託業務包括客製化資通系統開發者，受託者應提供該資通系統之安全性檢測證明；該資通系統屬委託機關之核心資通系統，或委託金額達新臺幣一千萬元以上者，委託機關應自行或另行委託第三方進行安全性檢測；涉及利用非受託者自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。
- (6) **資安事件通報及補救：**受託者執行受託業務，違反資通安全相關法令或知悉資通安全事件時，應立即通知委託機關及採行補救措施。
- (7) **委託終止之資料處理：**委託關係終止或解除時，應確認受託者返還、移交、刪除或銷毀履行契約而持有之資料。
- (8) **其他維護措施：**受託者應採取之其他資通安全相關維護措施。
- (9) **定期稽核：**委託機關應定期或於知悉受託者發生可能影響受託業務之資通安全事件時，以稽核或其他適當方式確認受託業務之執行情形。
- (10) **其他說明：**限制使用有資安疑慮之大陸廠牌設備，以確保供應鏈安全。

在資訊務委外中，法規除了規範委外前的評估與契約簽訂，更重要的是「委外後的監督與管理」。以下說明委託機關如何透過「第二方稽核」來確保委外資安的有效性。

- (1) 委託機關對於委外廠商之管理措施，應確保委託業務如期如質執行。
包括核對服務水準協議 (SLA)、審查廠商定期提交的資安報告、檢視資安事件處理紀錄等。
- (2) 委託機關應檢視所有委外廠商，若囿於人力或經費不足無法每年確認所有委外廠商受託業務辦理情形，建議參照委外金額、涉及核心系統及業務性質等項面擬定相關計畫，並以書面稽核或其他適當方式，確認受託業務執行狀況。



◆ **稽核優先及判斷標準：**

- **委外金額：**金額越大的專案，通常其複雜度及潛在風險也越高。
- **涉及核心系統：**影響機關核心業務運作的系統，其資安風險最高，應優先稽核。
- **業務性質敏感性：**處理大量個人資料、涉及國家機密或關鍵基礎設施的業務，資安要求會更嚴格。

◆ **稽核方式彈性：**

- **書面稽核：**要求廠商提供資安政策、程序文件、訓練紀錄、弱點掃描報告等，透過文件審查進行。
- **現場稽核：**對於高風險或有疑慮的案件，進行實地訪查，確認實體安全、系統操作等。
- **其他適當方式：**如要求廠商進行資安演練，或透過資安監控平台確認其服務狀態。

◆ **委託機關應留存監督（稽核）結果紀錄、委外廠商之改善報告、以及後續追蹤紀錄**

- **後續追蹤的重要性：**稽核並非終點，問題的發現與解決才是關鍵。
- **文件化與證據：**這些紀錄是機關履行監督責任的證明，也是未來審查、法規遵循、甚至法律程序的重要依據。它也體現了資安管理 PDCA (Plan-Do-Check-Act) 循環中的「Check」與「Act」環節。

◆ **委託機關可參考行政院 111 年 5 月 26 日院臺護字第 1110174630 號函訂定「資通系統防護各階段資安強化措施」。**

- **實務指引：**此份行政院의 函文是機關在執行資安管理時非常重要的參考。
- **應用建議：**建議機關將函文中的具體要求，納入委外契約的附件、技術規範，或作為內部稽核的檢查表，以確保委外廠商在資通系統的規劃、設計、開發、測試、部署與營運等各階段都能符合資安要求。

8.1.3 《資通安全管理法施行細則》第 6 條第 1 項

依據《資通安全管理法施行細則》第 6 條第 1 項第 11 款規定，資通安全維護計畫應包括：「資通安全維護計畫應包含資通系統或服務委外辦理之管理措施」。依此規定，機關每年於其所訂的資通安全維護計畫中，應納入此項委外

辦理之管理措施，且應與同法第 4 條第 1 項所規範之委外應注意事項相結合，以確保所有委外活動皆能有效融入組織的整體資安策略，並符合其資通安全防護要求。

8.1.4 《資通安全責任等級分級辦法》第 11 條第 2 項

依據《資通安全責任等級分級辦法》第 11 條第 2 項規定，「各機關自行或委外開發之資通系統應依附表九 所定資通系統防護需求分級原則完成資通系統分級，並依附表十所定資通系統防護基準執行控制措施。」，此規定旨在將資安要求融入資通系統的整個生命週期，從源頭確保委外服務的安全性。

為協助各機關妥善辦理資訊委外作業，政府也提供了一系列參考指引，涵蓋了招標、契約簽訂到具體的資安要求等不同面向，詳細內容可參考表 48 所列的「政府資訊作業委外資安參考指引清單」。

表 48 政府資訊作業委外資安參考指引清單

編號	IDS (入侵偵測系統)	編號	IDS (入侵偵測系統)
1	政府資訊委外資安注意事項或常見缺失	10	行政院公共工程委員會「投標廠商聲明書範本 (1130112)」
2	政府資訊委外資安稽核表	11	行政院公共工程委員會「投標須知範本 (1120630)」
3	「Web 網站建置與個人資料管理維護」RFP 資安需求範例	12	行政院公共工程委員會「資訊服務採購契約範本 (1121123)」
4	「Infrastructure 基礎設施建置與維護管理」RFP 資安需求範例	13	行政院公共工程委員會「資訊雲端服務採購契約範本 (1130517)」
5	「雲端服務供應商提供資訊系統部署、託管及維護服務」RFP 資安需求範例	14	各類資訊 (服務) 採購之共通性資通安全基本要求參考一覽表 (1120925)
6	「政府機關資訊安全管理系統 (ISMS) 顧問輔導」RFP 資安需求範例	15	電腦軟體共同供應契約採購 - 雲端服務產品公開徵求 - 雲端服務檢測規範



編號	IDS (入侵偵測系統)	編號	IDS (入侵偵測系統)
7	「政府機關資訊安全管理系統 (ISMS) 公正第 三方驗證」 RFP 資安需求範例	16	委外廠商查核項目表
8	行政院公共工程委員會「政府資訊服務採購作業指引 (1120925)」	17	專有名詞英中對照表
9	數位發展部、行政院公共工程委員會「政府資訊服務採購經費估算編列手冊 (1130501)」		

表 48 列出 17 項重要的參考文件，包括：

- (1) **行政院公共工程委員會相關範本**：如投標廠商聲明書、投標須知、資訊服務採購契約、資訊雲端服務採購契約範本等，提供委外契約的標準模板。
- (2) **資訊作業委外資安檢核表**：協助機關在委外前評估廠商資安能力，並在委外後進行稽核。
- (3) **資安需求範例**：針對 Web 網站建置、基礎設施建置與維運、雲端服務等不同服務類型，提供資安需求範例。
- (4) **通用性資安要求**：各類資訊（服務）採購之共通性資通安全基本要求參考一覽表，提供了不同類型委外服務的通用資安要求。
- (5) **其他指引**：如政府資訊服務採購作業指引、經費估算編列手冊、委外廠商查核項目表、專有名詞英中對照表等。

總結來說，我國在資訊委外方面已建立起一套完善的法規與指引體系。了解並遵循這些規範，是確保委外活動合法合規、有效控制資安風險的關鍵，能從源頭將資安要求融入委外服務的各個環節。

8.2

資訊委外之類別及形態

資訊委外是一個廣泛的概念，涵蓋多種服務類別及具體形態。了解這些分類有助於委託機關更精準地定義需求、評估風險，並選擇最適合的委外模式。

資訊務委外的定義，是指將機關之資通服務所有相關活動，部分或全部委託由機關外之資通服務提供者完成。這意味著委外不一定將整個 IT 部門或所有 IT 服務外包，也可以僅是特定專案或功能。即使是部分委外，機關仍需對整體資安負責，委外改變的僅是風險管理的模式，而非責任的轉移。

資訊委外主要可分為四大類別，每個類別有不同的服務形態，總共有 22 種常見的服務形態，涵蓋了從開發到維運，從顧問到雲端應用的廣泛範疇。

8.2.1 系統發展類 (3 種形態)：聚焦於開發、維護或整合資訊系統。

- (1) **系統開發**：從零開始設計與建構新系統，例如開發新的客戶關係管理 (CRM) 系統。
- (2) **系統維護**：對現有系統進行功能更新、bug 修復、效能優化等。
- (3) **系統整合**：將多個異質系統連接起來，實現資料共享及業務流程協同。

8.2.2 維運管理類 (10 種形態)：確保資訊系統及基礎設施的穩定運行與日常管理。這是最常見也最廣泛的委外類別。

- (1) **設備操作**：負責伺服器、網路設備、儲存系統等硬體的日常監控、狀態管理與效能調校，確保基礎設施的穩定運行。
- (2) **硬體維護**：提供對資訊設備（如伺服器、網路設備、儲存設備）的定期保養、故障診斷以及實體維修服務。
- (3) **機房設施管理**：如電力、空調、消防、門禁等機房環境的管理。
- (4) **備份與復原服務**：定期備份資料，並確保在災害發生時能迅速復原。
- (5) **網路與資安服務**：如網路設備設定、防火牆管理、入侵偵測 / 防禦系統 (IDS/IPS) 管理、資安監控中心 (SOC) 服務等。



- (6) 網路管理：如網路架構規劃、IP 管理、頻寬監控等。
- (7) 資料處理：如大量資料的輸入、整理、分析、輸出等。
- (8) 資料登錄：如將紙本資料或非結構化資料轉換為數位格式。
- (9) 整體委外：如將整個 IT 運營部門或大部分 IT 功能外包給單一廠商。
- (10) 人力支援：如廠商提供 IT 技術人員派駐機關，進行日常運維或專案支援。

8.2.3 顧問訓練類 (6 種形態)：提供專業知識、建議及培訓，提升組織能力。

- (1) 顧問輔導：針對特定議題提供專業建議，如資安政策制定、風險評估等。
- (2) 稽核審查：對機關的資安管理制度、規範與政策進行獨立評估與符合性審查，確保其設計符合法規及最佳實務。
- (3) 系統稽核：針對資訊系統的實際運作、配置與安全控制進行深度檢視與評估，以找出潛在的安全弱點與操作上的不當之處。
- (4) 軟體驗證：針對軟體品質或安全性進行驗證測試。
- (5) 教育訓練：提供資安意識、專業技能等培訓課程。
- (6) 整體規劃：協助機關進行 IT 戰略規劃或資安架構設計。

8.2.4 雲端服務類 (3 種形態)：利用雲端技術提供彈性、可擴展的服務。

- (1) 軟體即服務 (SaaS)：直接使用雲端應用軟體，如雲端郵件、辦公軟體等。
- (2) 平台即服務 (PaaS)：租用雲端開發與部署平台，用於開發應用程式。
- (3) 基礎設施即服務 (IaaS)：租用雲端運算資源，如虛擬主機、儲存、網路。

資訊委外的類別及形態是多元且複雜的。委託機關應依據自身需求，了解不同委外模式的資安特性，選擇合適的廠商並擬定適當的契約條款，以實施有效的資安管理。

8.3

資訊委外之風險

本節旨在探討資訊委外所伴隨的資安風險，並闡述機關應採取的具體防範措施與管理作為，以確保資訊資產的安全。

8.3.1 遠端維運之常見資安風險

資訊委外在帶來效率與便利的同時，也潛藏著不容忽視的資通安全風險。近年來的多起資安事件顯示，駭客常利用委外廠商遠端維運的弱點作為攻擊途徑，透過遠端存取機制的漏洞，間接入侵委託機關的資通系統。常見的風險類型包含：

- (1) **帳密被竊取**：委外廠商的虛擬私人網路 (VPN) 或其他遠端連取帳號密碼一旦被盜用，將為攻擊者開啟入侵通道。
- (2) **惡意程式植入**：若廠商用於維運的主機本身缺乏足夠的資安防護，可能被植入惡意程式，進而成為攻擊機關係統的跳板。
- (3) **弱密碼或未限制來源 IP**：若遠端桌面服務（如 RDP）使用弱密碼或未限制來源 IP，極易成為駭客暴力破解或掃描攻擊的目標。

因此，如何強化遠端存取控制，已成為機關降低資安風險的重要課題。

8.3.2 遠端維運應採「原則禁止、例外允許」方式

為降低遠端維運帶來的資安風險，各機關在開放內部同仁及委外廠商進行遠端維護資通系統時，應採「原則禁止、例外允許」方式辦理。若因地理限制、處理時效及專案特性等因素確需開放，則應至少辦理下列防護措施：

(1) 依循法規並落實管理機制：

- ◆ 應依《資通安全管理法施行細則》第 4 條及《資通安全責任等級分級辦法》附表十中有關遠端存取相關規定辦理，並建立及落實管理機制。這包括制定詳細的遠端存取政策、申請流程、審批機制、監控機制、定期審查機制等，以確保所有遠端存取行為皆有據可查。



(2) 開放遠端存取期間原則以短天期為限，並建立異常行為管理機制：

- ◆ 「短天期」原則：遠端存取權限應該是臨時性的，用完即關閉。避免長期開啟的通道成為潛在漏洞。例如，如果廠商申請維護一天，就只開放一天。
- ◆ 異常行為管理：
 - 監控與告警：透過資安監控中心 (SOC) 或資安資訊與事件管理系統 (SIEM)，監控所有遠端存取行為，例如非工作時間登入、來自異常 IP 的連線、大量資料下載、未經授權的指令執行等。
 - 即時回應：偵測到異常時，應即時觸發告警並啟動調查和應變程序。
- ◆ 於結束遠端存取期間後，應確實關閉網路連線，並更換遠端存取通道（如 VPN) 登入密碼：
 - 即時關閉：於結束遠端存取期間後，應確實關閉網路連線，並更換遠端存取通道（如 VPN) 登入密碼。這是最容易被忽略但卻非常關鍵的一步，確保維護結束後立即斷開連線，並禁用或撤銷相關權限。
 - 更換登入密碼：即使是臨時開放的通道，其密碼也應在每次使用後立即更換。這能有效防止密碼外洩或被重複利用的風險，提高安全性。
 - 多因子鑑別 (MFA)：為遠端存取通道導入多因子鑑別（如 OTP、實體金鑰）是最佳實踐，能大幅提升帳號安全。

8.4

資訊委外之生命週期

在討論資訊委外的相關法規、風險及類型之後，本節將從更宏觀的角度，探討資訊委外完整的「生命週期」。如同任何重要專案，資訊委外應遵循結構化的生命週期管理，以系統性地管理風險，特別是資安風險。

本節將說明資訊委外從「決定需求」、「識別可行解決方案」、「選定解決方案」、「完成建置」到「確認營運服務」等面向，與其在計畫、招標、決標、履約管理、驗收等各階段的關係。下一節則會進一步詳述各階段的資安考量與具體管控建議。

8.4.1 決定需求

機關對資通系統明確定義需求，並識別出資通安全的『需求』。決定需求是資安委外最為關鍵的起始點，若未能在此階段清楚定義與規畫資安考量，後續工作可能埋下風險隱患。

- (1) **採購階段：**此階段應對資訊委外資安要求之計畫階段。
- (2) **需求定義的完整性：**在委外專案啟動之初，機關不能只關注功能性需求。資安需求（例如資料的機密性、完整性、可用性要求，存取控制等級，稽核紀錄要求，隱私保護措施等）必須在這個階段就明確、完整地識別出來。
- (3) **資安要求的重要性：**如果資安需求在這個階段沒有被明確定義，那麼後續的設計、開發、測試及驗收都可能缺乏資安依據，導致系統存在潛在風險

8.4.2 識別可行解決方案

在建置或選商前，審慎分析資訊作業環境現況與期望達成目標之差異，再識別出可行解決方案選項，並訂定適當的評估指標。

- (1) **採購階段：**此階段仍是對應資訊委外資安要求之計畫階段。
- (2) **現況分析與期望目標落差分析：**了解機關目前的資通環境、資安現狀，以及與期望目標之間的差距。這有助於判斷哪些部分適合委外，哪些不適合。
- (3) **多面向評估指標：**識別解決方案時，不能只考慮技術可行性或成本。資安



風險、廠商的資安能力、合規性、可維護性、可擴展性等都是重要的評估指標。

8.4.3 選定解決方案

由決策者選出適當的解決方案。

- (1) **採購階段**：此階段應對資訊委外資安要求之**決標階段**。
- (2) **機關**會依據之前設定的評估指標（包括資安指標），對所有合格的投標廠商進行綜合評估，選出適當的解決方案，並由決策者選出適當的解決方案。選定解決方案對應的是決標階段。

8.4.4 完成建置

於完成決標後，成立專案組織，督導服務廠商遵循 RFP 與契約，如期如質完成系統建置與測試工作。

- (1) **採購階段**：此階段對應資訊委外資安要求之**履約管理階段**。
- (2) **專案組織與監督**：委外專案啟動後，機關必須建立有效的專案管理機制，包含資安團隊的參與，持續監督廠商的進度與品質，特別是資安方面。
- (3) **RFP 與契約遵循**：這是最重要的依據。所有資安需求都應在 RFP 及最終契約中明確條列，並據此監督廠商的執行，並完成系統建置與測試工作。

8.4.5 確認營運服務

服務進入營運狀態，需持續量測服務水準是否滿足原規劃需求。

- (1) **採購階段**：此階段對應資訊委外資安要求之**驗收階段**。
- (2) **驗收完整性**：服務上線前，驗收環節除了功能性測試外，更要確認所有資安要求都已達成。這包括資安測試結果的複驗、資安文件交付完整性、資安管理流程的建立等。
- (3) **持續監測與評估**：服務進入營運階段後，並非資安責任的終點。機關需持續監測服務的資安表現（例如透過資安監控平台，並定期評估服務水準協議 (SLA) 中資安相關指標的達成狀況。
- (4) **應變計畫**：確保廠商有健全的資安事件應變計畫，並能配合機關執行資安演練。

8.5

資訊委外之資安要求

在探討完資訊委外的相關法規、風險、類別與生命週期後，本節將進一步聚焦於「如何在各個委外階段落實資安要求」。

我們將資訊委外視為一個專案，並將其分為 6 個主要階段：計畫、招標、決標、履約管理、驗收及保固。每個階段都有其獨特的資安考量與管控建議。將資安要求融入採購流程的每個環節，是確保委外服務安全的根本之道。

8.5.1 一般採購流程可區分以下階段，並提出各階段應有之資安管控建議，以確保資訊委外之資通安全

- (1) **計畫階段**：在專案初期就將資安需求明確化，並進行資安風險評估。
- (2) **招標階段**：將明確的資安要求納入招標文件，並評估投標廠商的資安能力。
- (3) **決標階段**：最終選定最符合資安要求的廠商，並將所有資安共識納入正式契約。
- (4) **履約管理階段**：確保廠商在服務交付過程中，持續遵循資安要求，並有效管理資安風險。
- (5) **驗收階段**：在服務正式上線或交付前，確認所有資安要求皆已達成，且系統是安全的。
- (6) **保固階段**：在服務或系統的保固期間內，持續確保其資安穩定性，並處理可能出現的資安問題。

這個完整的生命週期管理，強調將資安考量提前至專案初期，從源頭開始嚴格把關，並透過持續的監督與驗收，以建立堅實的資安防線。

8.5.2 計畫階段

資訊委外並非解決所有問題的萬靈丹，也並非所有業務都適合委外。在正式決定委外前，機關必須進行嚴謹的資安「可行性評估」與「風險評估」。

因此，在計畫階段應仔細評估個案的資安可行性與委外風險，以判斷是否適合進行委外。這包括評估委外是否能實際帶來資安效益，或是否會引入過高



的資安風險。對於某些高度敏感的業務，可能不適合完全委外，或需要制定更為嚴格的控管措施。這個階段的評估結果，將直接影響機關的最終決策，並指導後續如何安全地執行委外作業。

以下將計畫階段細分為 3 個步驟進行說明：「委外可行性分析」、「委外專案編成」及「委外資安需求識別」。

(1) 資訊委外可行性分析：

- ◆ **目的：**「篩選適合委託辦理之業務項目」、「進行成本效益分析」、「評估資訊委外資安風險與對策」。
- ◆ **篩選適合委託辦理之業務項目：**並非所有業務都適合委外。機敏性極高、涉及國家核心利益、或有嚴格法規限制的業務，需審慎評估是否完全委外，或應保留部分核心功能於內部。
- ◆ **進行成本效益分析：**這裡的「效益」不僅是經濟效益，還應包括資安效益。例如，委外是否能引入更專業的資安技術及人才，提升整體防護能力？潛在的資安事件損失也應納入成本考量。
- ◆ **評估資訊委外資安風險與對策：**
 - 本步驟關鍵於初期風險評估，在有限資訊與資源下，可採高階風險評估，以得出風險值，並制定降低風險之對策：
 - 當所識別之資安風險，若無法降低至可接受風險等級時，則不宜取得此項產品或服務。
 - 如風險值較高時，機關宜在簽訂委外契約前，進行詳細風險評估，以確保更精確之風險得以辨識。

(2) 資訊委外專案編成：

- ◆ **目的：**確立專案組織架構及資源配置，確保資安專業力量能有效參與。
- ◆ 指派對資訊委外專案性質或內容有充分了解能力之專案負責人。
- ◆ 視委外性質與規模邀請採購（總務）、法務、會（主）計、業務、資訊及政風等單位人員參與。必要時，須進行跨部門協作。

(3) 資訊委外資安需求識別：

- ◆ **建立資訊委外資安策略：**
 - **目的：**為委外服務設定明確的資安方向及原則。
 - **視專案時程定期審查資安策略：**資安策略並非一成不變。隨著時間推移、重大營運變革、新法規（如資通安全管理法及其子法、個人資料保護法等相關規定）發布、架構調整、政策或契約變更等，資安策略

都需要定期審查及調整。

- **確保資安策略議題相關人員知悉（包含委外廠商相關人員）：**資安策略的制定不是資安部門的單一任務，所有相關利害關係人，特別是未來將參與履約的委外廠商，都必須清楚了解這些資安原則與期望。這有助於後續的溝通與執行。

◆ **識別委外廠商之限制：**

- **目的：**依據委外業務的敏感性及法規要求，對潛在廠商設定資格限制。
- 視資訊委外產品或服務之本質，考量委外產品與服務是否涉及國家機密、影響國家安全或受 WTO 政府採購協定之規範，以限制投標廠商或其人員之資格：

◆ **邀請廠商提出對應措施方案：**

- **目的：**使潛在廠商針對機關的資安需求提出具體且可行的解決方案。
- 針對各項資通安全需求，經由 RFI 或 RFC 等方式徵詢委外廠商提供相對應建議措施。

◆ **建立資訊委外資安管理計畫：**

- **目的：**將資安要求具體化為可執行的計畫，作為後續履約的依據。
- 對委外個案應具備之資安需求項目進行詳細分析，並將之具體化為資訊委外資安管理計畫，以提供爾後以下文件之依據：
 - ✓ 徵求建議書文件（詳細陳述對欲採購產品或服務本身資安要求）。
 - ✓ 資訊委外契約書（明訂採購流程中廠商之資安義務與責任）。
 - ✓ 資訊服務水準協定（明訂可量測之服務水準）。

8.5.3 招標階段

在完成「計畫階段」的資安需求識別後，接下來就是進入實質的「招標階段」。這個階段的重點，是如何將規劃好的資安要求，有效地傳達給潛在廠商，並據此選出最適合且符合資安標準的委外廠商。

- (1) **招標階段之重點在選擇適宜之委外廠商：**透過公開、透明的招標程序，從眾多潛在廠商中，選出不僅能滿足業務需求，更重要的是能夠滿足機關嚴格資安要求的委外夥伴。
- (2) **招標階段作業包含定義委外廠商評估準則、備妥保密協議書、招標文件、蒐集廠商投標文件及評選服務建議書等作業。**



(3) 資安管理重點著重在 RFP 撰寫之完整度與評選準則中之資安要求符合度：

- ◆ **強調 RFP 的重要性：**一份完整且明確的 RFP 是避免未來爭議的基石。如果 RFP 中資安要求模糊不清，廠商可能無法提供符合期待的方案，履約後也難以監督。
- ◆ **符合度審查：**仔細審查廠商服務建議書中對資安要求的「符合度」。不僅要看廠商是否「會做」，更要看他們「如何做」，以及是否有具體的執行計畫和承諾。

(4) 招標文件之 RFP 及契約書，應依委外服務之資通系統等級，納入資通系統防護基準之系統發展生命週期相關規定，包括需求階段、設計階段、開發階段、測試階段、部署與維運階段、委外階段：

- ◆ **資通系統等級：**委外服務的資安要求應與所負擔資通系統的「資安責任等級」掛鉤。等級越高，要求越嚴格。
- ◆ **資通系統防護基準：**這是一個重要的法規依據，機關應將其中的要求融入 RFP 及契約。
- ◆ **安全系統發展生命週期：**這是一個「貫穿性」的要求。資安不再只是系統上線後的額外工作，而是從系統的「需求階段」（剛開始的規劃），到「設計階段」（架構）、到「開發階段」（程式碼撰寫）、到「測試階段」（漏洞檢測）、到「部署與維運階段」（安全配置、監控），甚至到「委外階段」（委外廠商的資安管理），都必須將資安融入其中。

以上招標階段是將「資安需求」轉化為「契約義務」的關鍵橋樑。透過完整明確的 RFP 及嚴謹的廠商評選，並將 SSDLC 概念融入其中，才能確保選到對的廠商，並為後續的資安履約管理打下堅實基礎。

8.5.4 決標階段

在完成「計畫階段」的資安規劃與「招標階段」的廠商評選後，我們現在進入到委外流程的關鍵時刻：「決標階段」。這個階段的重點在於選定最終的委外廠商，並將所有資安共識，透過「簽約」作業，轉化為具法律效力的義務與責任。

(1) **決標階段之重點為與廠商之簽約作業：**確保最終選定的委外廠商，不僅在技術及業務上符合需求，更重要的是，在「資安方面」能達成一致的協議，並將其明確載入契約，作為未來履約與監督之依據。

- ◆ **機關與委外廠商雙方應依據招標文件與廠商回應之服務建議書進行最終協議，於雙方協議並確定契約內容後，即進行簽約作業。**
- ◆ 這是簽約前的最後協商機會。雙方會依據招標文件（機關的要求）及廠商的服務建議書（廠商承諾的解決方案）進行條款的確認，特別是資安相關條款。

(2) 簽約行為重點：

- ◆ **查核廠商是否完成保密切結：**在正式簽約前，或甚至在招標階段廠商接觸機敏資訊時，就應要求廠商及其相關人員簽署保密協議，以確保廠商對機關的敏感資訊負有法律上的保密義務。

- ◆ **完成專案編成：**

這是決標後，廠商在正式履約前，需要配合機關完成的「專案啟動準備」工作。

- 例如：得標廠商於簽約前須依據招標文件規定，提出各項保密切結，並就機關需求規劃資通安全管理措施，廠商專案組織人員之遴選與質量需考量重新調整，並賦予適當職掌，以利承辦單位依據契約執行各項查核，並做成紀錄。
- **保密與資安措施規劃：**廠商需要依據契約要求，再次確認其保密承諾，並提出具體的資通安全管理措施計畫，說明如何符合機關的資安要求。
- **廠商專案組織與人員：**廠商應指派具備資安專業能力的人員擔任專案關鍵職位，並確保其人員素質符合機關要求。機關有權力要求廠商對專案團隊成員進行調整。
- **賦予適當職掌：**確保廠商內部資安職責明確，便於機關在履約期間進行查核與監督。
- **查核與紀錄：**這些準備工作都需要有明確的紀錄，作為未來機關進行履約管理、資安稽核的依據。這強調了過程中的文件化與證據留存的重要性。

決標階段不僅是選定廠商，更是透過「簽約」將資安要求法制化，並確保廠商在履約前做好充分的資安準備。這是資安管理從「規劃」走向「執行」的關鍵轉折點。



8.5.5 履約管理階段

在完成委外專案的計畫、招標與決標階段後，我們便進入了最核心且持續時間最長的「履約管理階段」。此階段的資安管理，是確保委外服務能持續安全運作的關鍵。如果說前幾個階段是為了做好「預防」，那麼履約階段的重點，便在於落實「監控」與「應變」。

以下將針對履約管理階段應注意的 7 個面向進行說明，包括：資通安全組織、持續性風險識別、人力資源安全、實體與環境安全、日常管理，以及資通安全事件管理。

(1) 資通安全組織：

- ◆ 機關與委外廠商皆應指定專案管理人員，負責推動、協調及督導資通安全管理事項。

- 說明：建立清晰的資安溝通與管理鏈。資安管理是雙方的共同責任，而非單向要求。機關應指定專門負責資安聯絡與管理的窗口，同樣地，委外廠商也應有明確的資安管理負責人，且定期召開資安協調會議，檢視資安管理進度，並將會議紀錄歸檔。

(2) 資訊委外風險持續識別：

- ◆ 機關資訊委外過程之資通安全風險，宜在核准廠商存取內部設施前加以識別，並作適當之控制措施。

- 說明：在授予廠商權限之前，機關必須充分了解潛在風險並採取預防措施。在履約階段，廠商將實際操作機關系統或接觸相關資料，這會產生新的資安接觸點。因此，在此階段必須再次識別這些潛在風險（例如：遠端存取、資料傳輸、特權帳號管理等），並規劃對應的控制措施。這也與前面所提的「遠端維運」風險管理相互呼應，強調任何存取行為都必須先經過嚴格的風險評估。

- ◆ 若需要允許委外廠商存取機關之資訊處理設施或資訊，宜執行風險評估以識別特定控制措施之要求。

- 說明：對於廠商的任何存取行為，都應有明確的風險評估流程。

(3) 資通委外人力資源安全（雇用前、期間、終止或變更）：確保委外廠商的執行人員具備資安意識，並在整個服務生命週期中遵循資安規範。包括：

- ◆ 委外前宜依工作職掌進行人員的篩選：
- ◆ 委外廠商之作業員工，由個人同意並簽署雇用同意書，該同意書陳述其

與機關對資通安全之責任。

- ◆ 宜提供資訊委外人員資安程序與資訊處理設施之正確使用認知教育及訓練，以將可能之資安風險降至最低。

(4) 資訊委外實體與環境安全：

- ◆ 防止機關內資通因資訊委外而遭未經授權之實體存取、損害及干擾，關鍵或敏感的資訊處理設施應置放於安全區域，並由適當之安全屏障與進出控制措施加以保護，確保這些設施免受未經授權之存取、損害及干擾。
 - 說明：確保委外廠商接觸或使用的機關實體資產與環境安全。
 - ✓ 當委外廠商人員需要進入機關內部機房、辦公區域或使用機關設備時，機關必須實施嚴格的實體安全控制。
 - ✓ 「關鍵或敏感的資訊處理設施」：如伺服器、網路設備、資料庫等，應放置在具備多層安全防護的「安全區域」內。
 - ✓ 「安全屏障與進出控制措施」：包括門禁系統、監視器、警衛、訪客登記、權限卡片管理等。

(5) 資訊委外管理：

- ◆ 資訊委外相關作業應符合機關資通安全政策與程序、資通系統防護基準之要求。
 - 說明：確保委外廠商的日常運作與機關的資安要求保持一致。這是資安合規性的體現。機關的資安政策、程序，以及資通系統防護基準，是所有資安活動的最高指導原則。委外廠商在執行任何作業時，都必須遵循這些規範。

(6) 資訊委外使用者存取管理：

- ◆ 為確保未經授權資安人員對資通系統存取，機關宜有正式程序，以控制資通系統與服務的存取權限配置作業。
 - 說明：嚴格管理委外人員的存取權限，最小化權限，防止越權存取。「正式程序」意味著存取權限的申請、審批、發放、變更、收回都必須有文件紀錄，並經過授權；最小權限僅授予完成任務所需的最小權限；時間權限應有時效性，到期自動收回。
- ◆ 程序應從開始登記使用註冊，到最終不再需要存取資通系統與服務註銷。
 - 說明：強調對委外人員存取權限的「完整生命週期管理」。從人員進入專案需要權限，到專案結束或人員離職，所有權限都必須「註銷」或「收回」。



(7) 資訊委外資通安全事件管理：

- ◆ 機關資訊委外應備妥正式的事件通報與提報程序，提供委外廠商配合並施予教育訓練。
 - 說明：建立快速、有效的資通安全事件通報與應變機制，確保委外廠商能與機關協同處理。這是「履約管理」最關鍵的資安要求之一。當資安事件發生時，時間就是金錢，快速通報與協同處理至關重要。機關需預先制定通報程序，並使委外廠商充分理解並能配合。
- ◆ 委外廠商宜認知可能對機關資產造成衝擊事件與弱點之通報程序，並要求所有人儘快向指定聯絡點通報任何資通安全事件與弱點。

8.5.6 驗收階段

在經歷了計畫、招標、決標及履約管理等階段後，我們終於來到「驗收階段」。這個階段的資安重點是確保委外服務或系統在正式上線前，已經確實符合所有資安要求，並準備好安全運作。如果說前面是「施工」，那驗收就是「交屋檢查」。

以下將針對驗收階段中應注意的 2 個面向進行說明，包括：一般驗收程序、資安驗收內容及專案結束後之處置。

(1) 一般驗收程序：

- ◆ 機關依據契約文件與「履約管理」階段執行成果辦理。
 - 說明：驗收的依據就是之前簽訂的「契約文件」，以及在「履約管理」階段所產出的各項成果與紀錄。這強調了文件的完整性及前面各階段管理的嚴謹性。
- ◆ 勞務驗收，得以書面或召開審查會方式辦理，其書面驗收文件或審查會紀錄，得視為驗收紀錄。
 - 說明：驗收形式可以多樣，不一定需要現場驗收，但無論是書面審查還是召開會議審查，都必須留下明確的「書面紀錄」。
- ◆ 機關可要求委外廠商於簽約後一定時間內提交「專案工作計畫書」，內容確認委外專案之進行方式、專案組織、相關時程及資通安全要求事項是否符合。
 - 提交時間：此計畫書應於簽約後提交，但其內容應與「計畫階段」所擬定的資安規劃緊密相關。這份計畫書是廠商承諾如何具體執行並符

合資安要求的藍圖。

- **資安審閱：**機關應仔細審閱計畫書中所有「資通安全要求事項」的內容，確認其與機關的資安策略及契約要求完全一致。若發現不符之處，則應立即要求廠商進行修正。
- ◆ **委外廠商也須將定期召開工作進度報告會議之內容，如應完成重要工作項目、已完成工作的項目、預計工作項目、問題與建議等，提供驗收單位佐證。**
 - **過程證據：**這強調了履約期間「工作進度報告會議」的重要性。會議紀錄不僅是專案管理的一部分，更是驗收時的重要「佐證資料」。
 - **資安監控：**這些會議中應包含資安工作項目報告，例如資安測試發現的問題、修補狀況、資安演練結果等。透過這些紀錄，驗收單位可以追溯廠商在履約期間是否持續關注並解決資安問題。

(2) 資安驗收內容

延續前文對驗收階段一般程序的探討，本節將進一步針對不同類型的委外服務，深入闡述其資安驗收的具體內容。由於委外服務性質各異，其資安驗收的側重點也將有所不同。

- ◆ **顧問訓練類：**
 - **主要提供管理與技術服務，在完成顧問服務時即可得知是否符合機關要求。**
 - ✓ 說明：顧問訓練類委外，其成果通常是報告、建議方案、培訓課程或資安管理制度的輔導。驗收的重點在於這些交付物是否符合機關最初的需求，且顧問提供的專業知識是否有效提升了機關的能力。
 - **對於需使用軟體輔助才可完成專案之情況，應確認委外廠商是否使用最適之檢測工具與版本。**
 - ✓ 說明：若顧問服務（例如弱點掃描、滲透測試、原碼檢測等）需要藉助資安工具完成，機關應要求廠商說明所使用的工具名稱、版本，並確認這些工具是業界公認的、具備最新漏洞庫的「最適」工具。避免廠商使用過時或功能不足的工具，導致資安盲點。
- ◆ **系統發展類：**確保新開發或維護的系統，從程式碼到部署，都具備高度的安全性。
 - **除功能與效能測試外，應要求委外廠商提供該資通系統之安全性檢測證明。**



- ✓ **重要性：**這是系統發展類委外資安驗收的核心。功能正常、效能優異是基本要求，但「安全性」更是關鍵。
- ✓ **檢測證明：**廠商應提供具體的資安測試報告，例如：
 - **弱點掃描報告：**涵蓋主機、應用程式層面。
 - **滲透測試報告：**模擬駭客攻擊，找出系統深層漏洞。
 - **原碼檢測報告：**檢查程式碼是否存在安全缺陷。
- **資通系統使用非委外廠商自行開發之元件時，宜要求委外廠商揭露第三方程式元件之來源與授權證明，以確保其元件非來自大陸地區或其他限制地區。**
- ✓ **供應鏈安全：**這點非常重要，直接關係到資訊系統的「供應鏈安全」。現代系統通常會使用大量的開源軟體、函式庫或第三方元件。
- ✓ **來源與授權：**機關必須要求廠商詳細揭露這些第三方元件的清單、來源（例如哪個開源專案、哪個供應商）、授權模式。
- ✓ **地域限制：**尤其強調「非來自大陸地區或其他限制地區」。這是政府機關資安採購的明確政策要求，旨在防範潛在的惡意後門、間諜軟體或受特定政治實體控制的資安風險。
- ◆ **維運管理類：**
 - **維運管理類與顧問訓練類之服務類似：**
 - ✓ **說明：**確保維運服務持續滿足資安要求，並對新發現的漏洞進行及時處理。維運管理類服務（例如機房管理、網路管理、資安監控等）與顧問訓練類服務類似，其資安驗收並非一次性的，而是持續性的。驗收的重點在於其日常營運是否符合資安規範，以及面對資安事件的應變能力。
 - **若維運過程有新發現程式漏洞，則需進程式修補或者定期進程式弱點掃描。**
 - ✓ **說明：**系統及應用程式會持續被發現新的漏洞。對於維運管理類委外，機關應在契約中要求廠商具備漏洞管理機制，並在發現新漏洞時，能夠及時進程式修補或定期安排弱點掃描。這是一種持續性的資安驗收。
- ◆ **雲端服務類：**
 - **雲端服務類與系統發展類類似：**

- ✓ **說明：**雲端服務本身可以視為一種「軟體即服務 (SaaS)」、「平台即服務 (PaaS)」或「基礎設施即服務 (IaaS)」。因此，其資安驗收也包含對功能及效能的確認。
- **除確認功能與效能外，對於產品或服務之資安保證大多來自於委外廠商所提供之證明**
 - ✓ **說明：**雲端服務的特殊性在於其「責任共擔模型」。雲端供應商負責底層基礎設施的安全，而客戶負責雲端上資料及應用程式的安全。因此，機關在驗收時，很大程度上需要依賴供應商提供的資安證明。
- **機關應確認與評估雲端服務供應商宣稱之認證範圍，包含控制與評估涵蓋功能及服務**
 - ✓ **說明：**供應商的資安驗證並非涵蓋所有服務。機關必須仔細審閱驗證報告，確認其驗證範圍是否涵蓋機關所使用的特定雲端服務及功能。例如，某個雲端供應商可能其 IaaS 通過 ISO 27001，但不代表其 SaaS 服務也通過相同驗證。

(3) 專案結束後之處置：

當專案結束後，機關應立即停止委外廠商之實體與邏輯存取權限，並回收或請委外廠商銷毀屬於機關之資訊資產，必要時可要求委外廠商出具銷毀證明。

- ◆ **說明：**確保委外專案結束後，所有資安風險點被徹底清除。無論是實體存取權限（如門禁卡、機房鑰匙）還是邏輯存取權限（如系統帳號、VPN 權限、特權帳號），都必須在專案結束或廠商人員離職後立即停用或移除，亦包括資產回收與銷毀。

8.5.7 保固階段

在歷經資訊委外生命週期的計畫、招標、決標、履約管理及驗收等階段後，我們來到最後一個關鍵環節 - 「保固階段」。許多人可能認為系統上線並完成驗收後便萬事大吉，但從資安角度而言，保固期內的維護服務與異常管理同樣至關重要，不容忽視。

(4) 保固服務：

- ◆ **保固期間不論軟硬體資產，應以維持驗收完成時之狀態為主要目的。**
 - **說明：**在保固期內，確保委外交付的軟硬體資產，其資安狀態能夠維

持在驗收時的安全水準。這意味著廠商有責任在保固期內修補缺陷、處理漏洞，並維持系統的穩定與安全。「維持驗收完成時之狀態」是指廠商應確保系統不會因其自身的錯誤、漏洞或其他非機關因素，導致資安狀況惡化。這包括對軟體缺陷的修補、硬體故障的排除，以及因廠商維護不當導致的資安風險。

(5) 異常管理：

◆ **保固期間運作中之資訊處理設施與應用軟體系統，均應受到嚴格之變更管理控制。**

- **說明：**即使在保固期內，任何對資訊系統及軟體的變更，都必須經過嚴格的資安審核及控制。變更管理是資安管理的核心環節。每一次變更都可能引入新的漏洞或風險。因此，即使是保固期內的維護或更新，也必須遵循機關既定的變更管理程序，包括變更申請、資安評估、核准、測試、實施及記錄。
- 若系統有重大資安顧慮或瑕疵，如屬委外廠商責任，需由委外廠商另提變更計畫。

◆ **保固期間系統如有委外廠商派駐人員協助者，發生異常事件時，應由派駐人員負責將問題反映至資訊業務承辦人員，再循正常程序陳報。**

保固階段係資通安全管理持續運作之核心環節。透過嚴謹的變更管理程序、明確之責任歸屬界定，以及完善之異常事件通報機制，機關得以確保委外服務於其完整系統發生命週期中，持續維繫所期望之資通安全防護水準，進而鞏固並強化整體資通安全防禦韌性。

MEMO

Handwriting practice lines consisting of 20 horizontal dashed lines.

單元

9

資通安全事件通報及應變

在資通安全領域，儘管組織投入大量資源於預防與防護措施，資通安全事件的發生仍是無可避免的現實。因此，除了事前防範外，資通安全事件的即時通報與有效應變，更是確保組織營運持續、最小化損害、並維護資訊資產安全的關鍵要素。資通安全事件的處理不僅是技術上的挑戰，更是一場與時間賽跑的競賽，嚴峻考驗著組織的應變能力與資安韌性。

本單元旨在引導讀者全面理解資通安全事件通報及應變之各面向。內容涵蓋事件處理之整體管理流程、相關法規規範、事件等級評估、詳盡之作業流程，乃至於關鍵之應變演練與處理步驟。此外，亦將探討數位證據之採集與鑑識，以及針對利用人性弱點之社交工程攻擊及其防範策略。期能為讀者提供實用之知識與實作指引，使其具備於實際工作中有效應對資通安全事件之能力。本單元學習重點如下：

- 1** 了解資通安全事件通報及應變的整體管理流程，及其法規依據。
- 2** 掌握資通安全事件通報及應變的作業規範，包括公務機關與特定非公務機關的要求。
- 3** 學習資通安全事件等級評估的方法，以資訊或資通系統性質與 CIA 衝擊性為判斷依據。
- 4** 深入理解資通安全事件通報及應變的詳細作業流程，包括不同層級機關的權責與時限。
- 5** 認識資通安全事件通報及應變演練作業的重要性與內容。
- 6** 掌握資通安全事件處理的各個階段，從準備到經驗學習。
- 7** 了解數位證據的取得與數位鑑識的原則及應用。
- 8** 認識社交工程攻擊的本質、常見手法及正確防範觀念。

9.1

資通安全事件通報及應變流程

在資通安全管理中，「預防」雖然至關重要，但「通報及應變」更是不可或缺的關鍵環節。沒有任何系統能做到絕對安全，資通安全事件的發生只是時間問題。因此，建立一套完善的資通安全事件通報與應變機制，是每個機關都必須具備的能力。

9.1.1 依據：《資通安全管理法》

- (1) 第 17 條第 1 項：公務機關為因應資通安全事件，應訂定通報及應變機制。
- (2) 第 24 條第 1 項：特定非公務機關為因應資通安全事件，應訂定通報及應變機制。

9.1.2 目的

此機制的設立旨在強化各機關應對資通安全事件的能力。透過完善的通報與應變機制，目標是全面提升所有機關處理資通安全事件的效能，其範圍不僅涵蓋技術層面，更包含管理層面的協調與人員的應變能力。

9.1.3 管理流程

通報及應變機制之管理流程，旨在強化各機關應對資通安全事件的能力，其範圍不僅涵蓋技術層面，更包含管理層面的協調與人員的應變能力。此機制涵蓋了事件處理的完整生命週期，從事前準備到事後檢討，形成一個不斷學習與改進的閉環。具體流程包括：建立標準化的作業規範；依事件影響程度進行分級；透過事前演練提升應變能力；在事件發生時進行通報及應變；以及在事後進行改善，以持續強化資安防護。

(1) 作業規範：

- ◆ **流程定義：**應明確界定資通安全事件處理的每一個步驟、每個環節的具體要求及執行方式。例如，誰負責接收事件通報、誰負責初步判斷、誰

負責協調應變等。

- ◆ **責任分配：**資通安全事件的處理涉及多個部門及人員，必須明確劃分每個角色在事件應變中的職責與權限。避免權責不清導致的延誤或推諉。

(2) 事件分級：

- ◆ **評估及分級：**針對不同的資通安全事件，需要依據其對機關造成的潛在影響（如資料洩露的敏感程度、服務中斷的時間長短、影響範圍大小）進行嚴重性評估及分級。
- ◆ **影響分析：**評估事件可能造成的業務影響、財務損失、聲譽損害等。分級的目的是為了決定應變資源的投入及通報的層級與時效。

(3) 事前演練：

- ◆ **模擬演練：**這是提升應變能力的最佳方式。定期進行資通安全事件的演練，模擬不同情境的攻擊情境。
- ◆ **應變計畫：**透過演練，可以驗證應變計畫的可行性，發現其中的不足並加以改進。同時也能提高團隊的協作能力及人員的應變速度。

(4) 事中通報及應變：

- ◆ **通報流程：**事件發生時，應立即啟動通報機制，明確向誰通報、通報什麼內容、以及通報的時限。內部通報、對外通報（如 N-ISAC、主管機關、司法單位）都需規劃。
- ◆ **應變措施：**這是實際執行層面，包括事件的偵測、抑制、根除、復原等一系列行動。例如，隔離受感染系統、清除惡意程式、修補漏洞、恢復服務等。

(5) 事後改善：

- ◆ **事件分析：**事件結束後，必須進行深入的事後分析，了解事件發生的根本原因、攻擊手法、應變過程中的優點與不足。
- ◆ **改善計畫：**依據分析結果，制定具體的改善計畫，包括技術防護的加強、管理制度的完善、人員培訓的補充等。這確保機關從每次事件中學習，提升整體資安防護能力。

9.2

資通安全事件通報及應變作業規範

在資通安全事件通報及應變管理流程的基礎上，本節將進一步探討支持其順暢運作之「通報」及「應變」的作業規範，其目的在於提供執行這些流程所需的實務指引及具體要求。

9.2.1 資通安全事件「通報」作業規範

- (1) 依據：資通安全事件通報及應變辦法
 - ◆ 第 9 條規定：公務機關應就資通安全事件之通報訂定作業規範。
 - ◆ 第 15 條規定：特定非公務機關應就資通安全事件之通報訂定作業規範。
- (2) 目的：確保資通安全事件的判斷、層級界定、內部傳達及外部知會都能迅速、準確且有效。
- (3) 「通報」作業規範之內容，應包括下列事項：
 - ◆ 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。

9.2.2 資通安全事件「應變」作業規範

- (1) 依據：資通安全事件通報及應變辦法
 - ◆ 第 10 條：公務機關應就資通安全事件之應變訂定作業規範。
 - ◆ 第 16 條：特定非公務機關應就資通安全事件之應變訂定作業規範。
- (2) 目的：確保資通安全事件發生時，能有組織、有計畫進行損害控制、復原並從中學習。

- ◆ 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機制。
- ◆ 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。

MEMO

9.3

資通安全事件等級評估

前面我們討論了資通安全事件的通報及應變之管理流程，其中提到「判定事件等級」是應變管理流程中的核心環節。本節將深入探討如何對資通安全事件進行「等級評估」。

為什麼要分級？因為不同等級的事件需要投入不同層級的資源，啟動不同範圍的應變計畫，並向不同層級的單位進行通報。因此，正確的事件分級，是確保應變措施得以有效執行的關鍵。

9.3.1 資通安全事件等級評估

資通安全事件依其嚴重程度，由輕至重分為「第 1 級」、「第 2 級」、「第 3 級」、「第 4 級」四個等級。在評定事件級別時，我們會綜合考量資訊與資通系統的性質，以及事件對機密性、完整性及可用性的衝擊程度。最終，將以 CIA 三者中最高的影響等級，作為該事件的綜合分級結果。詳細的評估標準，如表 49 資通安全事件等級評估表。

表 49 資通安全事件等級評估表

資訊或資通系統性質	CIA 衝擊性	綜評事件級別
1. (涉及 / 未涉及 CI) 核心業務資訊或資通系統 2. 非核心業務資訊或資通系統 3. 一般公務機密 4. 敏感資訊 5. 國家機密	機密性 完整性 可用性	以最高級別評為該資通安全事件通報等級

(1) 「資訊或資通系統性質」：指的是受影響的資訊或資通系統本身的敏感度、重要性。

- ◆ **涉及 / 未涉及 CI 核心業務資訊或資通系統：**受影響的系統若屬於核心業務或關鍵基礎設施，則事件嚴重性將顯著提升。
 - ◆ **非核心業務資訊或資通系統：**相較於核心業務，對非核心業務系統的衝擊，其事件等級會相對較低。
 - ◆ **一般公務資訊：**指機關持有或保管，依法有保密義務，但不涉及國家機密或敏感個資的資訊，例如對外公開資訊或非敏感行政資料。
 - ◆ **敏感資訊：**
 - **個人資料：**依個人資料保護法第 2 條規定，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。
 - **政府業務：**在政府機關業務中，許多系統都處理大量個人資料，如戶政、健保、稅務等。一旦發生資料外洩或不當使用，皆屬於高影響性的資通安全事件。
 - ◆ **國家機密：**
 - **定義：**依《國家機密保護法》第 2 條及第 4 條規定，國家機密指為確保國家安全或利益而有保密之必要，對政府機關持有或保管之資訊，經依本法核定機密等級者（絕對機密、極機密、機密）。
 - **影響：**這類資訊直接攸關國家安全，如國防情報或外交密件。任何涉及國家機密的事件，無論其衝擊程度，都將被視為最高級別的資通安全事件。
- (2) **「CIA 衝擊性」：**指的是資通安全事件對機密性、完整性、可用性所造成的影響程度。
- ◆ **機密性：**指資訊未經授權而揭露或外洩的風險。例如資料外洩、機密文件被非法存取。
 - ◆ **完整性：**指資訊未經授權而被修改或破壞的風險。例如資料被篡改、系統程式碼被植入惡意代碼。
 - ◆ **可用性：**指資訊或系統無法被合法使用者即時存取的風險。例如服務中斷、網站癱瘓、阻斷服務攻擊 (DDoS)。



9.3.2 機密性之影響等級評估

機密性是指資訊未經授權而揭露、竊取或外洩，所保持其內容的隱匿性與安全性。當資通安全事件影響到資訊的機密性時，我們將依據外洩資訊的性質及嚴重程度來評定事件等級。

機密性影響等級分為輕微、嚴重兩大類，並細分為 4 個級別，如表 50 資通安全事件機密性影響等級評估表，其影響等級詳細說明如下：

表 50 資通安全事件機密性影響等級評估表

影響等級		說明
輕微	第 1 級	非核心業務資訊遭 輕微洩漏
	第 2 級	非核心業務資訊遭 嚴重洩漏 ，或未涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏
嚴重	第 3 級	未涉及關鍵基礎設施維運之核心業務資訊遭 嚴重洩漏 ，或一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭 輕微洩漏
	第 4 級	一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭 嚴重洩漏 ，或國家機密遭 洩漏

(1) 輕微（第 1 級）：非核心業務資訊遭輕微洩漏。

- ◆ 案例：某機關內部研討會的非公開報告被少量洩漏，該報告屬機關非核心業務資訊的優化建議，但與實際系統運作無關。

(2) 第 2 級：非核心業務資訊遭嚴重洩漏。

- ◆ 案例：某機關的內部辦公網頁遭受攻擊，導致其內部刊物歷年來的草稿版本（非機密，但未公開，且非核心業務）被下載了數千份，並被上傳至公共論壇。

(3) 第 2 級：或未涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。

- ◆ 案例：某機關的專案管理系統，包含某核心業務專案的內部討論文件（涉及專案預算分配初稿，非最終定案，且與關鍵基礎設施無關），因設定錯誤，被外部合作廠商人員下載有外傳跡象。

- (4) **第 3 級：未涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏。**
- ◆ **案例：**某機關的研發部門因內部伺服器組態漏洞，導致其研究專案的數百份技術規格文件（非機密，未涉及關鍵基礎設，但具商業價值且為**核心業務**成果）被競爭對手惡意取得，並在地下市場販售。
- (5) **第 3 級：或一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。**
- ◆ **案例：**某機關的員工薪資系統，有部分員工的薪資資訊，被外部合作廠商人員下載有外傳跡象。
- (6) **嚴重（第 4 級）：一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏。**
- ◆ **案例：**某政府服務網站遭受駭客攻擊，導致數百萬筆民眾的個人資料（姓名、身分證字號、聯絡方式、病歷或金融資訊等）被竊取，並被公開販賣或勒索。
- (7) **嚴重（第 4 級）：或國家機密遭洩漏。**
- ◆ **案例：**國防單位的某作戰情報分析系統，其內部儲存的國家級防禦部署圖資或軍事通訊加密演算法，被敵對境外勢力滲透竊取。
- (8) **輕微洩漏 / 嚴重洩漏：由政府機關依洩漏所造成之影響自行認定其嚴重性。**
- ◆ **裁量權：**這是一個重要的原則。對於「輕微」及「嚴重」的判斷，雖然有普遍性的概念，但最終仍由「政府機關」依據洩漏事件對自身造成的具體「影響」來「自行認定」。

9.3.3 完整性之影響等級評估

完整性是指資訊或資通系統在儲存、傳輸及處理過程中，保持其準確性與一致性。當資通安全事件影響到資訊的**完整性**時，我們將依據資訊及資通系統的性質及嚴重程度來評定事件等級。

完整性影響等級分為輕微、嚴重兩大類，並細分為 4 個級別，如表 51 資通安全事件完整性影響等級評估表，其影響等級詳細說明如下：



表 51 資通安全事件完整性影響等級評估表

影響等級		說明
輕微	第 1 級	非核心業務資訊或非核心資通系統遭 輕微竄改
	第 2 級	非核心業務資訊或非核心資通系統遭 嚴重竄改 ，或未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改
嚴重	第 3 級	未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭 嚴重竄改 ，或一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭 輕微竄改
	第 4 級	一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭 嚴重竄改 ，或國家機密遭 竄改

(1) 輕微（第 1 級）：非核心業務資訊或非核心資通系統遭**輕微竄改**。

- ◆ 案例：某機關的內部公告欄網站，其中一則過期且不重要的內部活動公告，被惡作劇者修改了幾個錯別字，但內容主旨未變，且很快被發現並修正。

(2) 第 2 級：非核心業務資訊或非核心資通系統遭**嚴重竄改**。

- ◆ 案例：某機關的對外形象網站，首頁內容被駭客惡意替換為不雅圖片，導致網站無法正常運作約 1 小時。該網站僅提供機關介紹及新聞發布，不涉及核心業務。

(3) 第 2 級：或**未涉及**關鍵基礎設施維運之核心業務資訊或核心資通系統遭**輕微竄改**。

- ◆ 案例：某機關官方網站系統（非關鍵基礎設施）遭外部攻擊，導致發布中的核心業務公告內文被輕微竄改（例如：將某項補助金申請截止日期從「10 月 31 日」改為「10 月 30 日」）。該機關在數小時內即復原，因影響時間短且資訊差異輕微，未造成大量民眾申請權益受損。

(4) 第 3 級：未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭**嚴重竄改**。

- ◆ 案例：某機關的會計系統，其內部帳務資料（非關鍵基礎設施維運相關）遭到惡意竄改，導致數百筆的帳務紀錄與實際不符，需要耗費大量人力進行人工核對與資料恢復，造成業務流程嚴重延誤。

(5) **第 3 級：或一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改。**

- ◆ **案例：**某水利單位用於監測水庫水位數據的感測器，其傳輸的某個非關鍵性輔助資料（例如天氣預報中的相對濕度）被外部竄改，導致監測數據輕微異常，但對水庫實際運作判斷無實質影響，且很快被異常偵測系統發現。

(6) **嚴重（第 4 級）：一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重竄改。**

- ◆ **案例：**某健保單位的醫療給付系統遭駭客入侵，導致數十萬筆的民眾健保給付紀錄被惡意竄改，造成部分民眾無法獲得應有給付，或不當獲得給付，導致巨大的社會問題及財政損失。

(7) **嚴重（第 4 級）：或國家機密遭竄改。**

- ◆ **案例：**某國防單位級別的戰略指揮系統，其內部作戰地圖的關鍵目標數據或部隊調度指令，被敵對勢力透過網路攻擊成功竄改，嚴重影響了國防戰備能力。

(8) **輕微竄改 / 嚴重竄改：**由政府機關依竄改所造成之影響自行認定其嚴重性。

9.3.4 可用性之影響等級評估

可用性是指資訊或資通系統能被合法使用者，在需要時即時且持續地存取與使用。當資通安全事件影響到資訊的可用性時，我們將依據資訊及資通系統的性質及嚴重程度來評定事件等級。

可用性影響等級分為輕微、嚴重兩大類，並細分為 4 個級別，如表 52 資通安全事件可用性影響等級評估表，其影響等級詳細說明如下：

(1) **輕微（第 1 級）：非核心業務資通系統運作中斷，於可容忍中斷時間內回復正常運作。**

- ◆ **案例：**某機關的內部會議室預約系統（為非核心業務系統），因網路臨時故障導致無法存取約 3 小時，但在 IT 人員場修網路並重啟服務後，該系統可於最大可容忍中斷時間（4 小時）內回復正常運作。

(2) **第 2 級：非核心業務資通系統運作中斷，無法於可容忍中斷時間內回復正常運作。**

- ◆ **案例：**某機關的外部意見信箱系統（為非核心業務系統，不涉及關鍵基

礎設施運作），因伺服器硬碟故障，導致服務中斷 6 小時，期間民眾無法提交意見，該系統無法於最大可容忍中斷時間（4 小時）內回復正常運作。但該系統不涉及即時性或核心業務。

表 52 資通安全事件可用性影響等級評估表

影響等級		說明
輕微	第 1 級	非核心業務之運作受影響或停頓，於 可容忍中斷時間 內回復正常運作， 造成機關日常作業影響
	第 2 級	非核心業務之運作 受影響或停頓 ，無法於 可容忍中斷時間 內回復正常運作，或未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作 受影響或停頓 ，於 可容忍中斷時間 內回復正常運作
嚴重	第 3 級	未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作 受影響或停頓 ，無法於 可容忍中斷時間 內回復正常運作，或涉及關鍵基礎設施維運之核心業務或核心資通系統之運作 受影響或停頓 ，於 可容忍中斷時間 內回復正常運作
	第 4 級	涉及關鍵基礎設施維運之核心業務或核心資通系統之運作 受影響或停頓 ，無法於 可容忍中斷時間 內回復正常運作

(1) 第 2 級：或未涉及關鍵基礎設施維運之核心業務資通系統運作中斷，於可容忍中斷時間內回復正常運作。

- ◆ 案例：某機關的內部公文收發系統（如為核心業務系統，不涉及關鍵基礎設施運作），因電力系統故障導致服務中斷 1 小時，該系統可於最大可容忍中斷時間（4 小時）內回復正常運作。

(2) 第 3 級：未涉及關鍵基礎設施維運之核心業務資通系統運作中斷，無法於可容忍中斷時間內回復正常運作。

- ◆ 案例：某機關的線上申辦服務系統（如為核心業務系統，但不涉及關鍵基礎設施運作），因惡意程式感染導致資料庫損毀，服務中斷超過 12 小時，該系統無法於最大可容忍中斷時間（4 小時）內回復正常運作。期間民眾無法辦理業務，引起大量抱怨。

- (3) **第 3 級：或涉及關鍵基礎設施維運之核心業務資通系統運作中斷，於可容忍中斷時間內回復正常運作。**
- ◆ **案例：**某交通控制中心的交通號誌監控系統（涉及關鍵基礎設施維運的核心系統），因網路設備故障，導致監控畫面短暫中斷 1 小時，期間須人工調度警力指揮交通。該系統可於最大可容忍中斷時間（4 小時）內回復正常運作，但中斷期間可能影響交通流量及潛在安全。
- (4) **嚴重（第 4 級）：涉及關鍵基礎設施維運之核心業務資通系統運作中斷，無法於可容忍中斷時間內回復正常運作。**
- ◆ **案例：**某國家級電網的電力調度系統遭到惡意攻擊，導致部分地區電網服務中斷超過 8 小時，造成大規模停電，該系統無法於最大可容忍中斷時間（4 小時）內回復正常運作，影響民眾生活及重要產業運作。
- (5) **中斷時間 / 復原時間：**由政府機關依實際影響自行認定其嚴重性。
- ◆ **裁量權：**這是一個重要的原則。對於「中斷時間」或「復原時間」的判斷，雖然有普遍性的概念，但最終仍由「政府機關」依據事件對自身造成的具體「影響」來「自行認定」。

9.3.5 資通安全事件 CIA 影響等級評估

為提供一個快速且標準化的影響等級評估方法，以確保各級人員在面臨資通安全事件時，能迅速且一致地判斷其嚴重性，可參考表 53 資通安全事件 CIA 影響等級評估總表。



表 53 資通安全事件 CIA 影響等級評估總表

影響等級	機密性 (資訊洩漏)		完整性 (資訊 / 資通系統遭竄改)		可用性 (業務 / 資通系統運作中斷)	
	資訊性質	影響程度	業務資訊 / 資通系統	影響程度	業務	可否於容忍中斷時間回復
1 級	非核心業務	輕微	非核心	輕微	非核心業務	可
2 級	非核心業務	嚴重	非核心	嚴重	非核心業務	不可
	核心業務 (未涉及 CI 維運)	輕微	核心 (未涉及 CI 維運)	輕微	核心 / 資通系統 (未涉及 CI 維運)	可
3 級	核心業務 (未涉及 CI 維運)	嚴重	核心 (未涉及 CI 維運)	嚴重	核心 / 資通系統 (未涉及 CI 維運)	不可
	核心業務 (涉及 CI 維運)	輕微	核心 (涉及 CI 維運)	輕微	核心 / 資通系統 (涉及 CI 維運)	可
	一般公務機密、敏感資訊	輕微	一般公務機密、敏感資訊	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 / 資通系統 (涉及 CI 維運)	不可
	一般公務機密、敏感資訊	嚴重	一般公務機密、敏感資訊	嚴重		
	國家機密	-	國家機密	-		

組織可利用此評估總表綜評資通安全事件等級，進而更有效地進行後續管理、降低資安風險，並提高整體的資安防護能力。此總表能協助組織快速判斷事件的影響程度，並採取相應的應急措施：

- (1) **第 1 級及第 2 級事件**：通常可由內部團隊自行處理，以快速恢復正常運作。
- (2) **第 3 級及第 4 級事件**：需啟動更嚴格的事件處理流程，包括通報上級主管機關、啟動跨部門應變機制等，以應對更嚴重的衝擊。

總體而言，這套標準化的評估方法不僅有助於組織在事中進行快速有效的應變，更有利於事後進行分析及改進，透過具體數據持續優化資安管理措施。

9.3.6 資通安全事件等級評估案例（一）

在前幾節中，我們探討了資通安全事件分級的理論基礎，包括資訊系統的性質，以及對機密性、完整性、可用性 (CIA) 的衝擊評估。本節將透過一個具體案例，將這些知識應用於實務，進行綜合判斷，最終得出資通安全事件的通報等級，如表 54 資通安全事件等級評估案例（一）。

表 54 資通安全事件等級評估案例（一）

情境	A 機關自行發現內部一名員工電腦中的檔案被加密，此該員工負責處理機關內 核心資通系統 相關行政作業，該系統 未涉及關鍵基礎設施相關運作 ，但可以用其他電腦代替使用，並未造成資料外洩情形。A 機關資訊人員針對受駭電腦進行還原程序處理，並清查其電腦，沒有被加密之情形。A 機關資訊人員依通報應變作業規定登入通報應變網進行通報作業																										
解析	- 機密性：因此次事件未造成資料外洩情形，選擇「無須通報」 - 完整性：此電腦為核心業務使用，其系統已遭變更或竄改，故選擇「2 級」 - 可用性：因此次於事件無系統或設備運作受影響，故選擇「無須通報」	<table><tr><td></td><td>機</td><td>完</td><td>可</td></tr><tr><td>4</td><td></td><td></td><td></td></tr><tr><td>3</td><td></td><td></td><td></td></tr><tr><td>2</td><td></td><td></td><td></td></tr><tr><td>1</td><td></td><td></td><td></td></tr><tr><td>無</td><td></td><td></td><td></td></tr></table>			機	完	可	4				3				2				1				無			
	機	完	可																								
4																											
3																											
2																											
1																											
無																											
綜合評估	因第二項目為「2 級事件」，第一、三項目為「無須通報」，故綜合評估此資安事件為「2 級事件」。																										

(1) 案例（一）情境說明：

- ◆ **事件概述**：A 機關自行發現內部一名員工電腦中的檔案被加密。



- ◆ **受影響範圍 / 性質：**該員工只負責處理機關內核心資通系統相關行政作業，該系統未涉及關鍵基礎設施相關運作。
- ◆ **影響程度：**受害電腦檔案被加密，但可以用其他電腦代替使用。
- ◆ **應變措施：**A 機關資訊人員針對受駭電腦進行還原程序處理，並清查其餘電腦，沒有被加密之情形。
- ◆ **通報行為：**A 機關資訊人員依通報應變作業規定登入通報應變網站進行通報作業。

(2) 資通安全事件等級評估：

- ◆ **第一步：評估「機密性」衝擊**
 - 情境資訊：此次事件未造成資料外洩情形。
 - 評估等級：可視為 0 級。
- ◆ **第二步：評估「完整性」衝擊**
 - 情境資訊：員工電腦中的檔案被加密。
 - 評估等級：此電腦為核心業務使用，其系統已遭變更竄改，故選擇『第 2 級』。
- ◆ **第三步：評估「可用性」衝擊**
 - 情境資訊：受害者可以用其他電腦代替使用，此事件無系統或設備運作受影響。
 - 評估等級：可視為 0 級。
- ◆ **綜合評估：**
 - 依據準則：「以最高級別評為該資通安全事件通報等級」。
 - 評估結果：
 - ✓ 機密性：0 級
 - ✓ 完整性：第 2 級
 - ✓ 可用性：0 級

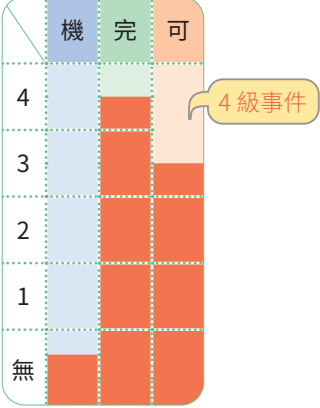
- (3) 綜評結果：依據「以最高級別為準」的原則，本次資安事件的最終通報等級為第 2 級。

9.3.7 資通安全事件等級評估案例（二）

為進一步加強實務判斷能力，我們將透過另一個具體案例，將資安事件分級原則應用於綜合判斷，最終得出通報等級，如表 55 資通安全事件等級評估案

例（二）。

表 55 資通安全事件等級評估案例（二）

情境	B 機關製程資料收集系統為負責 關鍵基礎設施運作 團隊存放執行紀錄系統，每日進行備份，資料處理人員發現系統無法正常開啟，經查發現製程資料收集系統遭植入 KillDisk 程式刪除主機的主要啟動磁區 (MBR) 與系統資料，事件發生後，處理人員透過備份還原機制，將前日資料還原，並由各執行團隊重新匯入當日執行紀錄	
解析	- 機密性：因此次資料收集系統未造成資料外洩情形，選擇「無須通報」 - 完整性：資料收集系統被植入一惡意程式，系統主要存放關鍵基礎設施執行團隊相關紀錄，故判定為涉及關鍵基礎設施維運之核心資通系統遭嚴重竄改，故選擇「4 級」 - 可用性：資料收集系統透過備份機制復原，判定為涉及關鍵基礎設施維運之核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作，故選擇「3 級」	 4 級事件
綜合評估	因第一項目為「無須通報」，第二項目為是「4 級」，第三項目為「3 級」，故綜合評估此資安事件為「4 級事件」。	

(1) 案例（二）情境說明：

- ◆ **事件概述：**B 機關的「製程資料收集系統」遭植入 KillDisk 程式，刪除主機的主要啟動磁區 (MBR) 與系統資料。
- ◆ **受影響範圍 / 性質：**「製程資料收集系統」為「負責**關鍵基礎設施運作**團隊存放執行紀錄系統」。
- ◆ **影響程度：**主機的主要啟動磁區 (MBR) 與系統資料被刪除。
- ◆ **應變措施：**處理人員透過備份還原機制，將前日資料還原。
- ◆ **通報行為：**B 機關資訊人員依通報應變作業規定登入通報應變網站進行通報作業。

(2) 資安事件等級評估：

- ◆ **第一步：**評估「機密性」衝擊



- **情境資訊：**案例中並未提及資料有被竊取或外洩。KillDisk 程式主要目的是破壞資料，而非竊取。
 - **評估等級：**可視為 0 級。
 - ◆ **第二步：評估「完整性」衝擊**
 - **情境資訊：**「製程資料收集系統」為「負責關鍵基礎設施運作團隊存放執行紀錄系統」，其「主機的主要啟動磁區 (MBR) 與系統資料」被「刪除」。
 - **竄改程度：**主機的主要啟動磁區及系統資料被刪除，這無疑是對系統「嚴重竄改」或「破壞」。即使資料能還原，在被刪除的當下，完整性已遭到嚴重破壞。故屬涉及關鍵基礎設施維運之核心資通系統遭嚴重竄改。
 - **評估等級：**故選擇『第 4 級』。
 - ◆ **第三步：評估「可用性」衝擊**
 - **情境資訊：**「製程資料收集系統」的主機被刪除 MBR 及系統資料，這意味著系統在被攻擊後，立即「運作中斷」。隨後「處理人員透過備份還原機制，將前日資料還原」。
 - **中斷時間：**被 KillDisk 刪除 MBR 意味著系統無法啟動，必須經過還原過程才能恢復。這個過程，即使有備份，也必然會造成一定時間的「運作中斷」。屬涉及關鍵基礎設施維運之核心業務資通系統運作中斷，但系統於可容忍中斷時間內回復正常運作。
 - **評估等級：**可視為第 3 級。
 - ◆ **綜合評估：**
 - **依據準則：**「以最高級別評為該資通安全事件通報等級」。
 - **評估結果：**
 - ✓ 機密性：0 級
 - ✓ 完整性：第 4 級
 - ✓ 可用性：第 3 級
- (3) **綜評結果：**依據「以最高級別為準」的原則，本次資安事件的最終通報等級為第 4 級。

9.4

資通安全事件通報及應變作業流程

資安事件等級評估完成後，組織需依據綜評結果，啟動相應的通報及應變作業程序。本節將詳細說明資安事件處理的相關訊息，主要包括以下三個部分：資安事件通報基本項目、損害控制內容，以及調查、處理及改善報告：

9.4.1 資安事件處理之相關訊息

(1) 資安事件通報基本項目：

目的：是記錄事件發生的基本訊息，包括發生機關、時間、事件描述等，為後續調查及處理提供依據。

- ◆ 發生機關
- ◆ 發生或知悉時間
- ◆ 狀況描述
- ◆ 其他相關事項
- ◆ 事件等級評估
- ◆ 外部支援需求評估
- ◆ 因應事件所採取的措施

(2) 損害控制內容：

目的：是記錄事件發生後，機關內部如何進行損害控制和系統復原的具體過程，為事後分析提供詳細記錄。

- ◆ 記錄損害控制或復原的過程

(3) 調查、處理及改善報告：

目的：是深入分析事件的根本原因，評估事件影響範圍及損害程度，並制定相應的改善措施，以防止類似事件再次發生。這部分涵蓋了時間線、影響分析、根因分析和改善計劃等關鍵內容。

- ◆ 事件發生或知悉、完成損害控制或復原的時間
- ◆ 事件影響範圍及損害評估
- ◆ 損害控制及復原過程



- ◆ 事件調查及處理過程
- ◆ 事件根因分析
- ◆ 為防範類似事件再次發生所採取的管理、技術、人力或資源等措施
- ◆ 預定完成時程及成效追蹤機制

9.4.2 通報及應變作業流程

為何「通報及應變」至關重要？資安事件處理的「黃金時間」概念，強調了及時通報與應變是降低損害、加速復原的關鍵。

(1) 公務機關 / 特定非公務機關的通報及應變責任：

- ◆ 事件知悉後「黃金 1 小時內」的通報責任：
 - 當其單位或人員知悉資安事件發生時，必須在 1 小時內 向上級呈報相關資訊。
 - 「知悉」的定義：強調不需待事件完全釐清或損害評估完成才通報，只要有合理懷疑或初步證據即應啟動。這是避免延誤通報的關鍵。
- ◆ 應變責任：在限定時間內儘速完成損害控制或復原。
 - 損害控制：隔離受影響系統、阻斷惡意連線、備份鑑識資料等。
 - 復原：恢復系統運作、清除惡意程式、修補漏洞等。強調這是一個持續的過程，初期的復原目標是恢復基本運作。

(2) 上級 / 監督機關及中央目的事業主管機關的審核與支援角色：

- ◆ 接獲通報後的職責：這些機關的角色是「審核」事件報告的正確性與完整性，並「視情況提供必要支援服務」。
- ◆ 支援服務範疇：技術支援（如派遣資安專家）、協調跨單位資源、提供情資、甚至協調執法單位介入等。
- ◆ 不同事件等級的審核時限：
 - 第 1 級及第 2 級事件（較輕微）：應於 8 小時內完成審核。
 - 第 3 級及第 4 級事件（較嚴重）：應於 2 小時內完成審核。
- ◆ 中央目的事業主管機關的彙報機制：須「定期彙送第 1 級及第 2 級資安事件」。即使是輕微事件，透過定期彙報也能幫助中央主管機關掌握資安趨勢、分析潛在風險、評估整體資安防護成效，並作為未來政策制定的參考依據。

(3) 主管機關的「覆核」與「會議」機制：

- ◆ **覆核作業的啟動：**當主管機關接獲審核機關呈報的所屬資安事件後，需進行「覆核作業」
- ◆ **召開資安防護會議的時機：**並視情況召開資安防護會議。
- ◆ **覆核範圍的差異：**
 - 公務機關：主管機關應覆核所有第 1 級至第 4 級之資安事件。
 - 特定非公務機關：主管機關得覆核所有第 1 級至第 4 級之資安事件。

(4) 通報及應變作業之時序流程

本節將以資通安全事件通報及應變的時序，整理整個作業流程，從事件發生、通報、處理到最終的改善報告。詳細內容請參考圖 64 資通安全事件通報及應變作業時序流程圖，以下詳細說明其時序流程：

- ◆ **通報機關的職責與時限**
 - **流程起始點：**此階段為資安事件處理的起點，通報機關的首要職責是進行初步的事件處理與損害控制。
 - **事件通報：**通報機關需將事件通報至其上級機關或監督機關，以及中央目的事業主管機關。
 - **審核時效：**上級機關或中央目的事業主管機關對通報事件的審核有明確的時間要求：
 - ✓ 第 3 級及第 4 級事件（較嚴重）：需在 2 小時內完成審核。
 - ✓ 第 1 級及第 2 級事件（較輕微）：需在 8 小時內完成審核。
- ◆ **事件處理與損害控制**
 - **核心環節：**這是整個流程的核心工作，貫穿於通報及報告提交期間。主要工作包括隔離受影響系統、阻斷惡意連線、進行鑑識，並執行系統復原等措施。
 - **支援協助：**在審核與處理過程中，上級或中央主管機關將提供必要的支援協助，確保事件能被有效應對。
- ◆ **改善報告與監督機制**
 - **流程終點：**事件處理完成後，通報機關需提交資通安全事件調查、處理及改善報告，其目的不僅是解決當前問題，更重要的是從中吸取教訓，防止類似事件再次發生。
 - **報告審查：**上級機關及中央目的事業主管機關在收到改善報告後，會進行檢視，以確保內容的完整性與改善措施的有效性，並視需要要求調整或說明。

- **最終監督**：無論是通報事件或改善報告，最終均需呈報至**主管機關**，以落實整體資安防護的監督責任。

◆ **重要注意事項**

- **報告提交時限**：「資通安全事件調查、處理及改善報告」應在 1 個月內提交。如有特殊情況，可提出延長提交申請。
- **等級變更申請**：若在調查過程中，事件的影響範圍或嚴重性擴大，通報機關必須適時提出等級變更申請，並詳細說明變更原因與事件調查情況。

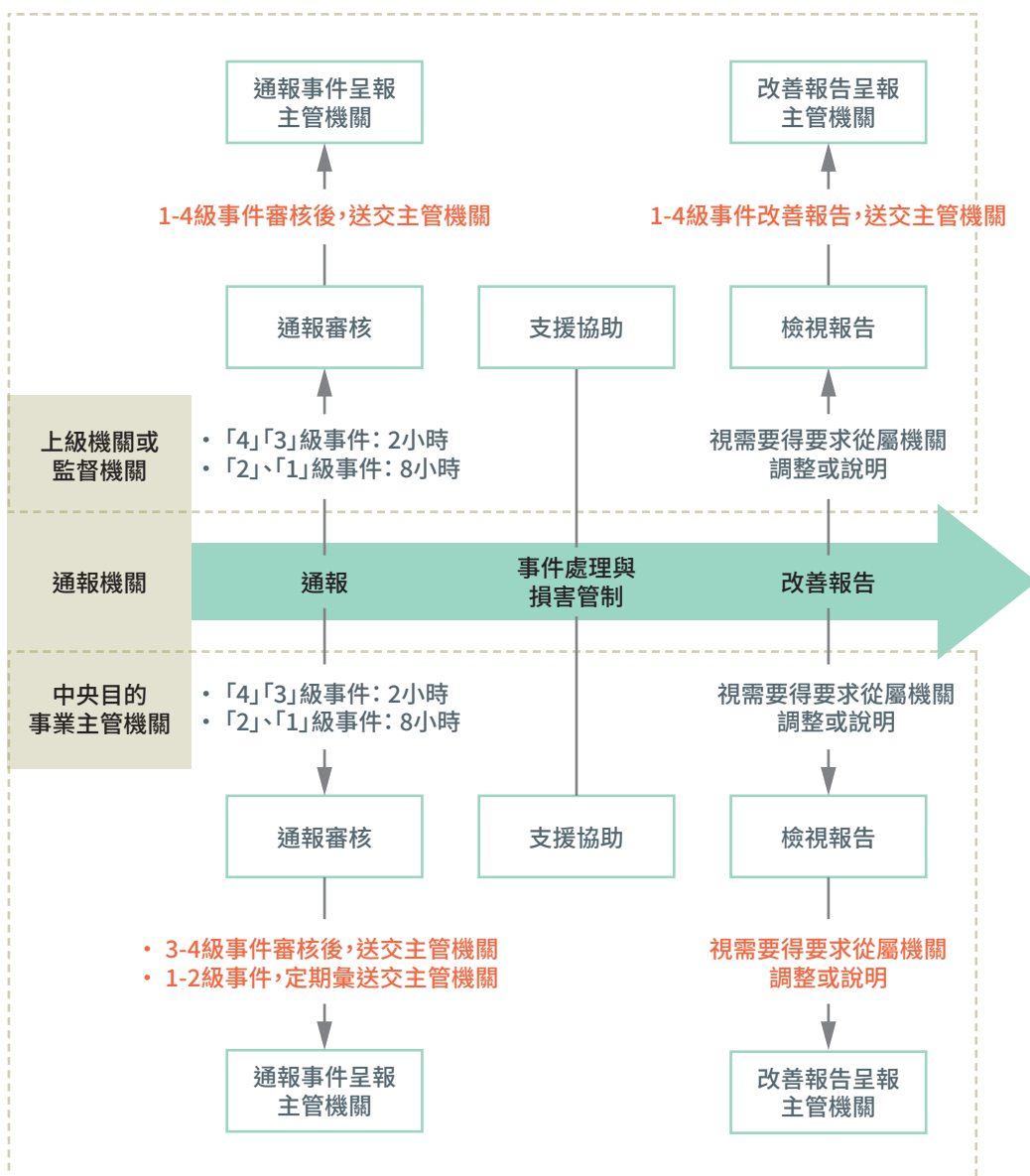


圖 64 資通安全事件通報及應變作業時序流程圖

(5) 公務機關資通安全事件通報及應變作業流程

本節說明公務機關在面對資安事件時的標準化作業流程，請特別留意各角色之間的權責劃分、通報路徑及關鍵時間點，詳如圖 65 公務機關資通安全事件通報及應變作業流程圖，以下詳細說明其作業流程：

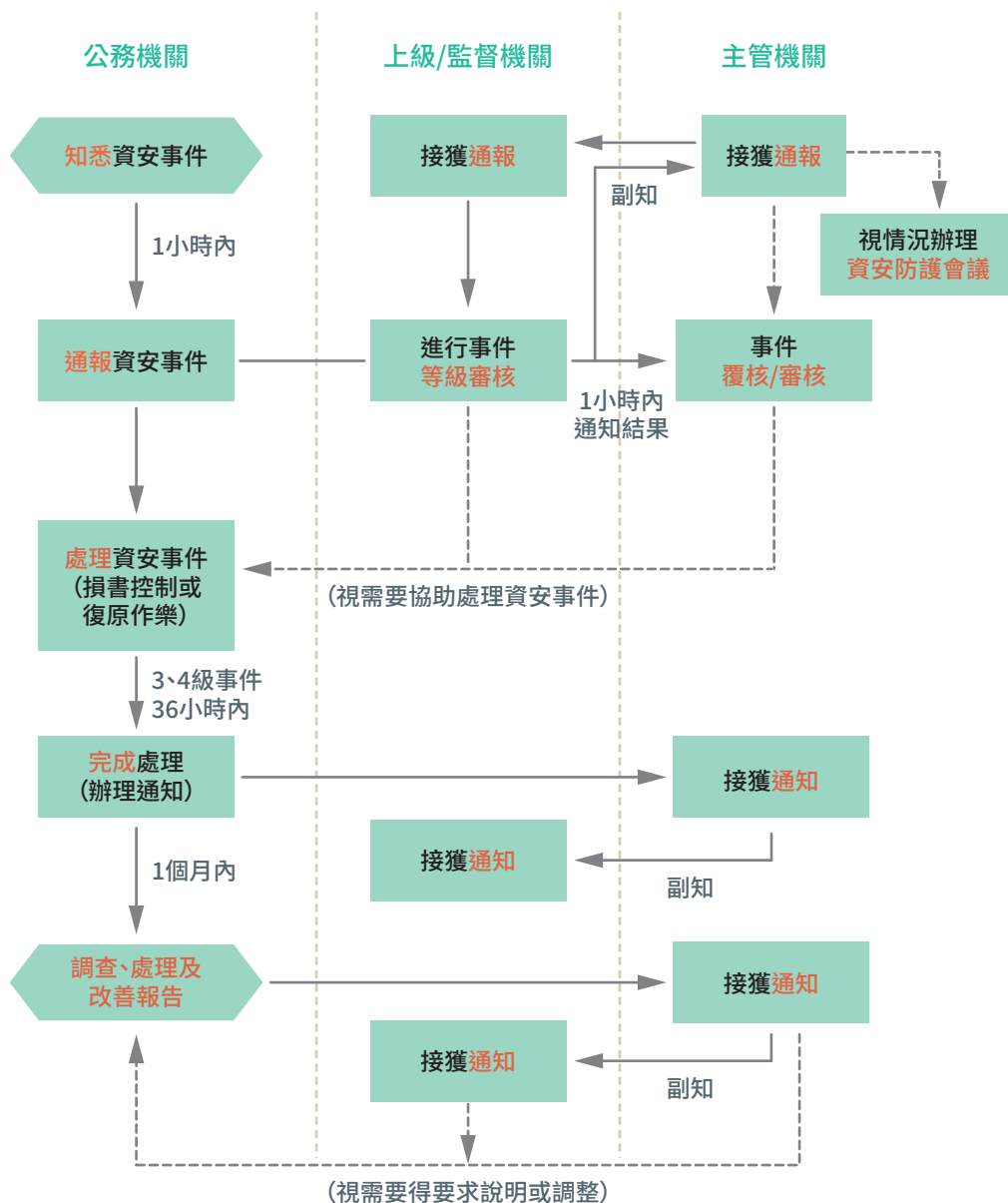


圖 65 公務機關資通安全事件通報及應變作業流程圖



◆ **【第一階段】事件知悉與初步通報（公務機關）**

- **知悉資安事件：**指公務機關的資安負責人或相關人員發現或被告知有資安事件發生。
- **1 小時內通報：**公務機關必須在知悉事件後 1 小時內，向其上級 / 監督機關及中央目的事業主管機關進行通報。

◆ **【第二階段】上級審核與支援（上級 / 監督機關）**

- **接獲通報及審核：**上級 / 監督機關收到通報後，會立即對事件進行等級判定（例如是否為 3、4 級事件等），確認通報內容的初步準確性。
- **1 小時內通知結果：**上級機關必須在收到通報的 1 小時內，將審核結果通知主管機關。
 - ✓ **【支援協助】：**如果需要，上級機關將提供必要的協助來處理資安事件。**常見支援：**包含技術諮詢、工具提供、人力支援、甚至是協調跨機關資源等。
- **副知主管機關：**上級機關在接獲通報時，會同步副知其所屬的主管機關，確保主管機關對重大事件有即時的初步認知。主管機關並視情況召開資安防護會議，這代表了最高層級的決策與協調。

◆ **【第三階段】事件處理及結案（公務機關）**

- **立即處理資安事件：**這是最關鍵的執行環節，公務機關需立即採取措施，如隔離受影響系統、備份鑑識資料、修補漏洞、恢復服務等。
- **第 3 級及第 4 級事件時限：**對於較為嚴重的第 3 級及第 4 級資安事件，公務機關必須在事件發生後 36 小時內，完成關鍵的損害控制和初步復原工作。
- **完成處理及結案：**當事件的立即性危機解除，主要損害已控制，服務已初步復原時，公務機關需向上級 / 監督機關提交結案通知。

◆ **【第四階段】調查、改善與最終報告**

- **1 個月內提交報告：**事件處理完成後，公務機關需於 **1 個月內提交資通安全事件調查、處理及改善報告**。此報告為最終書面成果，應包含事件的根因分析、處理過程、已採取的改善措施及未來預防建議。
- **上級 / 監督機關及主管機關的檢視：**此報告將同步送交上級 / 監督機關及主管機關進行檢視，以確保內容的完整性與改善措施的有效性。
- **主管機關的覆核及召開會議：**主管機關在此階段會對事件的處理進行最終的「覆核」。

- 無上級機關或監督機關者，知悉資通安全事件時，應依資通安全管理法第 14 條及第 17 條規定通報：
 - ✓ 總統府、國家安全會議及五院，向主管機關提出。
 - ✓ 直轄市政府、直轄市議會、縣（市）政府及縣（市）議會，向主管機關提出。
 - ✓ 直轄市山地原住民區公所、直轄市山地原住民區民代表會，向直轄市政府提出；鄉（鎮、市）公所、鄉（鎮、市）民代表會，向縣政府提出。

(6) 特定非公務機關資通安全事件通報及應變作業流程

本節說明特定非公務機關在資安事件通報與應變上的標準作業流程。此流程與公務機關有許多共通點，但其通報對象與權責劃分存在關鍵差異，詳如圖 65 特定非公務機關資通安全事件通報及應變作業流程圖，以下詳細說明其作業流程：

◆ 【第一階段】事件知悉與初步通報（特定非公務機關）

- **知悉資安事件：**指特定非公務機關的資安負責人或相關人員發現或被告知資安事件。
- **1 小時內通報：**無論是公務機關還是特定非公務機關，都必須在知悉事件後的 1 小時內啟動初步通報，體現資安應變的即時性。
- **通報對象：**特定非公務機關的直接通報對象為其直屬的中央目的事業主管機關，而非多層級的機關。

◆ 【第二階段】審核與支援（央目的事業主管機關）：

- **接獲通報及審核：**中央目的事業主管機關是特定非公務機關資安事件的第一線審核者。他們會對事件進行初步判斷和等級確認，並據此進行分級通報主管機關。對於特別嚴重的事件，主管機關會召開資安防護會議，進行更高層級的決策與資源協調。
 - ✓ **第 1 級及第 2 級事件：**對於影響較小的事件，中央目的事業主管機關自行管理，僅需定期彙整後呈報給主管機關。
 - ✓ **第 3 級及第 4 級事件：**對於影響較大、可能涉及關鍵基礎設施或大量個資外洩的嚴重事件，中央目的事業主管機關必須在接獲通報的 1 小時內，立即轉送給主管機關。
- **支援協助：**中央目的事業主管機關也會視需要，提供技術、資源等協助給特定的非公務機關，協助其處理資安事件。

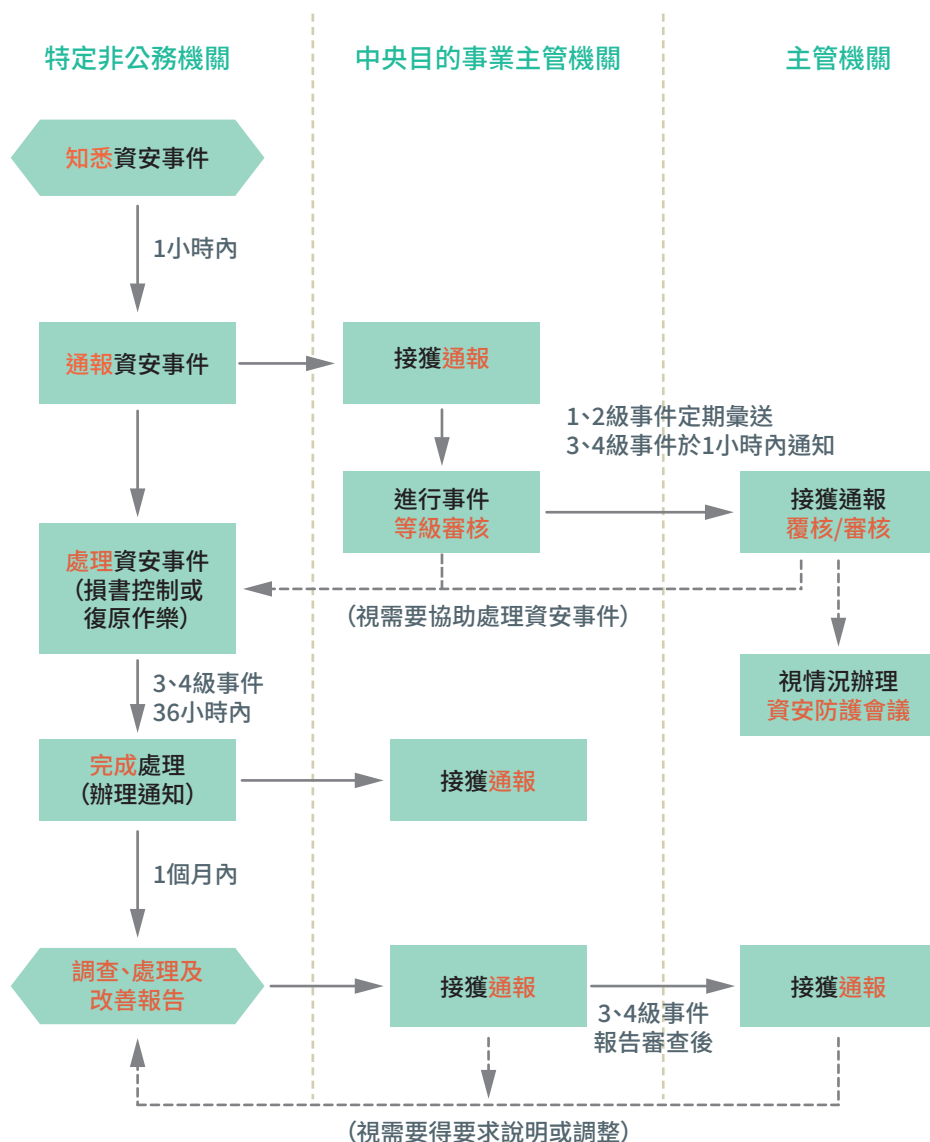


圖 66 特定非公務機關資通安全事件通報及應變作業流程圖

◆ 【第三階段】事件處理與結案：

- 立即處理資安事件：特定非公務機關在通報的同時，必須立即展開損害控制與復原作業。
- 完成處理及結案：完成初步處理後，特定非公務機關需向上層的中央目的事業主管機關提交結案通知。

◆ 【第四階段】調查、改善與最終報告：

- 1 個月內提交報告：事件處理完成後，特定非公務機關應於 1 個月內

- **中央目的事業主管機關的審查與轉送：**對於第 3 級及第 4 級事件的最終報告，中央目的事業主管機關需先進行審查，確認報告完整性與改善措施適切性後，再轉送給主管機關。
- **主管機關的覆核與召開會議：**主管機關主要接收並覆核來自中央目的事業主管機關轉呈的第 3 級及第 4 級資安事件報告。

9.5

資通安全事件通報及應變演練作業

在前幾節中，我們討論了資安事件處理的規範與流程。然而，一個完善的藍圖若缺乏實際演練，便難以發揮效用。演練是資安防護體系中不可或缺的一環，它能有效驗證應變計畫的可行性、提升人員的熟練度、發現潛在盲點，並在真實事件發生前提供寶貴的實戰經驗。

9.5.1 政府機關強制性演練要求

(1) 適用對象：

總統府、中央一級機關之直屬機關，以及直轄市及縣（市）政府。這些單位通常掌握國家關鍵資訊或承擔重要民生服務，其資安事件影響層面廣大，因此被列為強制演練對象。

(2) 演練作業：

上述單位應規劃並辦理資通安全演練作業，這意味著演練必須有正式的計畫與實際執行。

(3) 成果報告：

演練完成後，必須在一個月內將執行情形及成果報告送交主管機關。

(4) 演練內容：

演練作業之內容，應至少包括：

- ◆ 半年辦理 1 次社交工程演練：
- ◆ 每年辦理 1 次資通安全事件通報及應變演練：

9.5.2 公務機關與特定非公務機關的演練配合與內容

(1) 配合主管機關規劃：

公務機關與特定非公務機關皆應配合主管機關的規劃，辦理資通安全演練。這體現了主管機關在資安治理中的指導與協調角色。

(2) 演練項目：如表 56 機關應配合辦理通報及應變之演練項目所示，各演練項目內容說明如下：

表 56 機關應配合辦理通報及應變之演練項目

演練項目	公務機關	特定非公務機關
社交工程演練	V	
資通安全事件通報及應變演練	V	
網路攻防演練	V	V
情境演練	V	V
其他必要之演練	V	V

- ◆ **社交工程演練**：公務機關為強制要求。特定非公務機關則可由其中央目的事業主管機關另行規定。
- ◆ **資通安全事件通報及應變演練**：公務機關為強制要求。特定非公務機關則可由其中央目的事業主管機關另行規定。
- ◆ **情境演練**：公務機關及特定非公務機關均須辦理。
- ◆ **其他必要之演練**：公務機關及特定非公務機關均須辦理。

演練的最終目標並非追求完美，而是發現計畫中的弱點及人員的不足，以便持續改進。這體現了 PDCA（計畫 - 執行 - 查核 - 行動）管理循環中查核與行動的關鍵環節。唯有透過持續且多樣化的演練，才能真正提升組織面對資安事件的應變速度、效率及復原韌性。

9.6

資通安全事件處理

資通安全事件處理是一個系統化且多階段的程序，旨在確保組織能有效應對資安威脅，並在事件發生後迅速復原。本節將循序漸進探討處理資安事件的七大核心目的，並深入解析如何透過完善的處理計畫來建立持續有效的應變體系。接著，我們將介紹通用的事件處理程序，包括從準備、識別、封鎖、根除、復原到經驗學習的六個關鍵階段。最後，將特別針對具高法律風險與社會影響的個人資料外洩事件，闡述其特殊的處理要求與應變考量。

9.6.1 資安事件 - 處理目的

在討論過資安事件的通報、應變流程及演練後，我們回歸一個根本問題：處理資安事件的**目的**究竟是什麼？以下列出資安事件處理的七大核心目的：

(1) 確認資安事件是否發生：

這是處理流程的第一步。在啟動任何應變措施前，必須先**驗證警報或報告的真實性**，以避免「狼來了」效應，並確保資源的有效利用。

(2) 降低對業務與網路服務的中斷時間：

資安事件對組織最大的威脅是導致業務停擺或服務中斷。因此，將中斷時間降至最低是核心目標，這直接關乎組織的營運效率與客戶滿意度。

(3) 提供精準與及時的資訊：

在資安事件發生時，向內部（管理階層、員工）及外部（客戶、合作夥伴、監管機構、媒體）提供準確且及時的資訊至關重要，以維持信任及透明度。

(4) 於規定時間內完成損害控制或復原作業：

此目的直接呼應了通報與應變流程中的時限要求，確保事件處理不僅要迅速，更要符合既定標準，以快速恢復正常運作。

(5) 保障由政策與法律要求的權利：

資安事件處理必須符合內部政策與外部法律（如個資法、資通安全管理法）。此目的旨在確保組織在應變過程中，能維護自身的合法權益，並履行法定義務。

(6) 實作控制措施以維護監管鏈：

監管鏈指的是數位證據從收集、分析到最終呈現的完整性及可信度。此目的要求在處理事件時，必須按照嚴格程序收集、保存所有數位證據，以確保其可信度。

(7) 讓法務單位可對惡意者提起訴訟：

這是處理流程的延伸目標。透過嚴格的證據保全及鑑識分析，為法務單位提供足夠的證據，以便在必要時對惡意攻擊者提起訴訟，維護組織權益並產生嚇阻作用。

9.6.2 資安事件 - 處理計畫

在深入探討資安事件的通報、應變流程及具體措施，並確立了七大核心處理目的後，我們將焦點轉向一個更宏觀的議題：如何確保這些應變能力持續有效且不斷進步？這正是資安事件處理計畫的核心目的。一個完善的計畫不僅是靜態的文件，更是一個持續發展的體系，需要不斷投入資源與精力來維護與強化，以確保組織能夠適應不斷變化的威脅環境，從而實現所有處理目的。以下為資安事件處理計畫的四大重點：

(1) 定期重新審查計畫文件：資安威脅、技術環境、組織架構及業務流程都在不斷變化。如果計畫文件長期不更新，就會與實際脫節，導致應變失靈。

◆ 更新內容：

- **人員異動：**應變團隊成員、聯絡方式或職責變更時，需立即更新。
- **技術變遷：**組織採用新技術或系統升級時，應變流程及工具可能需要相應調整。
- **業務流程：**核心業務流程的異動也可能影響資安事件的應變優先順序。

(2) 教育訓練：

再好的計畫，也需要有能力的人來執行。訓練是提升團隊及個人應變能力的根本途徑。

- ◆ **訓練內容：**應涵蓋組織分工與權責、資安技能、危機處理、數位鑑識、調查技巧及溝通能力等關鍵面向。

(3) 財務支持：

資安不是成本中心，而是維護業務連續性及品牌聲譽的必要投資。缺乏足夠的財務支持，再好的計畫也無法有效落地。



- ◆ **支持項目：**包括預算編列、額外設備、專業人員配置、以及員工薪資與訓練費用等。

(4) 持續演練：

演練是驗證資安事件處理計畫是否可行、是否有效的最終手段。光有計畫而不演練，就像有地圖卻從不實際走一遍。

- ◆ **目的：**

- **定期驗證：**透過定期模擬資安事件，測試應變流程、人員技能、技術工具的實用性及有效性。
- **修正作業流程：**每次演練後，都應進行事後檢討，找出計畫中的不足、流程的瓶頸或人員的失誤，並據此修正及優化作業流程與計畫文件，這是一個持續改進的循環。

資安事件處理計畫是一個有機體，必須透過**持續審查**、**教育訓練**、**財務支持**及**持續演練**這四大支柱來共同維護與強化。如此，組織才能從「被動應對」轉變為「主動準備」，真正建立起面對不斷演進的資安威脅的強大韌性。

9.6.3 資安事件 - 處理程序

在討論資安事件的處理目的及處理計畫後，我們現在將聚焦於事件處理的核心程序。這是一個業界普遍採用的資安事件處理生命週期，通常包含 6 個關鍵階段：「準備、識別、封鎖、根除、復原、經驗學習」。此系統性框架指導應變團隊從事件發生前到事件結束後的整個處理過程。

(1) 準備：

這是資安事件應變的基石，指在事件發生前所進行的一切準備工作。

- ◆ **內容：**建立資安政策與程序、組建資安應變小組、配置所需工具與技術、進行人員訓練、定期演練應變計畫、以及執行風險評估等。
- ◆ **目標：**確保組織在面對資安事件時，能有足夠的資源、能力與準備，迅速有效地應對

(2) 識別：

指的是檢測到可能的資安事件，並進行驗證與分析，以確認事件是否真實發生，以及其初步的性質與影響範圍。

- ◆ **內容：**監控系統日誌、入侵偵測系統警報、使用者回報異常行為、進行初步的衝擊與範圍評估。

- ◆ **目標：**準確判斷資安事件的真偽、類型及初步嚴重程度，避免資源浪費於誤報，並及時啟動後續應變流程。

(3) 封鎖：

一旦確認事件發生，此階段的目標是限制資安事件的擴散範圍，阻止損害進一步蔓延。

- ◆ **內容：**隔離受感染的系統或網路區段、暫時性阻擋惡意流量、變更被入侵的憑證、實施臨時補丁或修復。
- ◆ **目標：**阻止攻擊者繼續控制系統、竊取資料或造成更多破壞，為後續的根除與復原爭取時間。

(4) 根除：

在封鎖後，此階段的目標是徹底清除惡意軟體、攻擊者留下的後門、以及導致事件發生的根本原因。

- ◆ **內容：**移除惡意程式、修補已知的安全漏洞、重新配置受損的系統、刪除惡意創建的帳號、在必要時重建受感染的系統。
- ◆ **目標：**確保威脅已被完全消除，攻擊者無法輕易再次入侵。

(5) 復原：完成根除後，此階段的目標是將受影響的系統及服務恢復到正常或接近正常的運作狀態。

- ◆ **內容：**從乾淨的備份中恢復資料、重新啟用系統與服務、進行功能測試與驗證、持續監控以確保穩定性。
- ◆ **目標：**降低對業務與網路服務的中斷時間，確保業務連續性。這也包括達成事先訂定的 RTO、RPO 及 MTPD 值。

(6) 經驗學習：

這是一個承上啟下的關鍵階段，旨在從資安事件中汲取教訓，避免未來再次發生類似事件。

- ◆ **內容：**召開事件後檢討會議、進行根本原因分析、識別安全控制措施的不足、更新資安政策與程序、強化資安教育訓練、改進監控與偵測能力，並將這些經驗反饋到「準備」階段。
- ◆ **目標：**提升組織的整體資安防護能力和應變韌性，使資安管理成為一個不斷學習和進步的循環過程

這 6 個階段構成了一個完整的資安事件處理循環，從預防到解決，再到優化。



(1) 資安事件 - 處理程序之準備

我們已了解資安事件處理的 6 個關鍵階段，其中第一步也是最關鍵的步驟，便是「準備」。資安事件成功處理的關鍵，在於事前的充分準備。以下為準備階段的六大核心要素：

- ◆ **組織資安事件處理小組：**資安應變絕非單打獨鬥，而需跨部門協作。應明確定義小組的組織架構、成員角色、職責分工與權限。這將確保每位成員在危機發生時，都能清楚自身的定位與職責。
- ◆ **建立資安事件處理策略：**此為戰略層面的考量，用以定義組織處理資安事件的總體方針與優先順序。例如，是優先快速恢復服務 (RTO)，還是優先進行數位鑑識以追溯攻擊者？此策略必須與組織整體的資通安全維護計畫目標一致。
- ◆ **設計資安事件處理程序：**這是將策略轉化為可執行步驟的關鍵。應為各類資安事件（如惡意程式感染、資料外洩、阻斷服務攻擊）設計詳細的標準作業程序。這些程序應涵蓋識別、封鎖、根除、復原等各階段的具體行動，並確保其清晰、具可操作性。
- ◆ **建立溝通管道與方式：**有效的溝通在資安事件中至關重要。應建立對內（管理階層、受影響部門）與對外（客戶、監管機構、媒體）的溝通流程、訊息發布權限、指定發言人，並確立使用的溝通工具與方式。
- ◆ **蒐集所需資源：**沒有足夠的資源，再好的計畫也只是空談。這包括人力資源（資安專業人員）、技術工具（如數位鑑識工具、SIEM 系統）及充足的財務支持（預算、緊急採購權限）。
- ◆ **練習、練習及再練習：**熟能生巧，這是準備階段最實用也最核心的一點。應定期進行各類資安演練，透過反覆練習，驗證計畫可行性，找出弱點，並修正作業流程，使應變團隊在真實事件發生時能有效執行任務。
- ◆ **資安事件處理小組之組成：**

資安事件的影響是全面性的，處理小組需涵蓋多方專業，以應對技術、業務、法律等多重挑戰。一個完整的應變小組通常包含以下核心角色：

- **技術部門** (IT、資通安全及系統管理者)：作為應變的先鋒部隊與執行核心，負責事件的偵測、分析、封鎖、根除與復原等技術性操作。
- **管理人員：**提供策略指導，授權必要的應變措施，調度資源，並做出影響業務連續性的關鍵決策。

- **法務部門**：提供法律諮詢，確保應變過程符合法規（如個資法），並指導數位證據的保全以維護監管鏈。
- **數位鑑識專家**：專責數位證據的收集、保全與分析，以釐清事件起因、攻擊路徑與損害程度，為後續調查提供可靠依據。公共關係部門：資安事件對組織聲譽的衝擊可能很大，需要專責的公共關係部門。
- **公共關係部門**：負責對外發言與媒體應對，處理客戶與合作夥伴的溝通，確保發布資訊的精準與及時，以維護組織聲譽。
- **人力資源部門**：處理人員管理與支援，包括內部威脅調查、員工隱私問題、懲戒措施，並在應變期間提供員工支援。
- **實體安全與維護部門**：在有實體關聯的事件中，協助控制實體進出，確保機房安全，並提供基礎設施維護。
- **通訊部門**：確保在主要通訊系統受損時，備援通訊管道的暢通，並建立緊急通訊聯絡網。

(2) 資安事件 - 處理程序之識別

在完成「準備」階段後，我們進入流程的第二步：「識別」。資安防護的現實是：儘管我們投入大量資源預防，但沒有任何系統是絕對安全的。因此，「資安事件無法完全防制，但必須被偵測」，及早識別是將損害降到最低的關鍵。以下說明識別階段的核心工作與判斷：

◆ 確認事件真實性與影響範圍

- **識別意圖**：判斷事件起源是惡意攻擊（如駭客入侵）或無意的內部錯誤（如設定失誤）。
- **確認範圍**：這是識別階段的關鍵。必須快速精確地判斷「哪些系統」、「哪些人員」及「資訊資產」受到影響。這為後續的封鎖與復原提供準確依據，避免盲目應變。

◆ 偵測可疑事件的指標

資安事件的偵測通常依賴於多種可疑指標。應特別關注以下異常現象：

- **異常的帳號與檔案活動**：攻擊者常用來建立持續性或隱蔽行動的手段，如新增非授權帳號、出現來源不明的新檔案或關鍵系統檔案被修改。可透過系統日誌、檔案監控系統或 SIEM 系統進行發現。
- **入侵偵測系統與防火牆警訊**：網路邊界防禦設備發出的直接警訊，包括入侵偵測 / 防禦系統 (IDS/IPS) 的警報、防火牆日誌顯示的異常連線嘗試等。



- **系統效能異常**：這是事件對業務衝擊最直接的體現，如系統效能變差、服務無回應或系統不穩定，這可能是阻斷服務攻擊或惡意軟體耗盡資源的跡象。
- **監聽進行中的攻擊**：資安團隊應主動透過 SIEM 系統、端點偵測及應變機制 (EDR) 或網路封包分析，來追蹤與分析正在發生的攻擊行為。

◆ 數位證據的取得與監管

識別出事件後，**保留可靠的證據**是至關重要的原則。這不僅是後續分析的基礎，也與法律程序息息相關。

- **數位證據的正確取得**
 - ✓ **採用經認可的磁碟映像複製工具**：應對儲存媒體（如硬碟）進行完整的位元級複製，確保所有資料（包括已刪除資料）都被完整擷取。
 - ✓ **配合雜湊函數進行驗證**：在複製過程中，必須使用雜湊函數（如 SHA-256）來驗證原始資料與複製映像檔的一致性，確保證據未經竄改。
 - ✓ **配合錄影紀錄採證過程**：透過錄影紀錄系統關機前的螢幕狀態，以及數位證據收集的完整過程，以證明採證操作的規範性與證據的可信度。
- **維護證據的監管鏈**

監管鏈是證明數位證據從發現、儲存到移交的整個過程皆受到嚴格控制、未曾遭受污染或竄改的書面紀錄。其完整性直接影響證據的法律效力。

 - ✓ **明確的保管人**：每一項證據從被發現起，都必須由可證明身分的人員負責保管，以確保來源清晰、責任明確。
 - ✓ **詳細的交接紀錄**：任何時候證據從一位保管人轉移至另一位，都必須有詳細的書面紀錄，包括交接時間、地點、人員與簽名，避免監管鏈中斷。
 - ✓ **安全的儲存保護**：被收集的證據必須存放於安全受控的環境中，並採取實體門禁、邏輯存取控制及寫入保護等措施，確保其在儲存期間的完整性。

(3) 資安事件 - 處理程序之封鎖

在完成「準備」及「識別」階段後，我們進入流程的第三步：「封鎖」。在確認資安事件已發生，並初步建立監管鏈後，首要任務是封鎖入侵來源，

避免災害擴大。這是一個與時間賽跑的階段，目標是盡快控制住局面，為後續的根除與復原爭取寶貴時間。以下說明封鎖階段的核心考量：

- ◆ **識別可信任來源：**在執行任何封鎖行動前，必須先明確界定哪些是「可信任」的網路來源、設備與使用者。此舉旨在避免在緊急應變中，因誤判而影響到正常的業務運作。
- ◆ **避免驚動入侵者以避免證據被銷毀：**過於倉促或激烈的封鎖行動，可能會驚動攻擊者，導致其立即刪除日誌或銷毀證據，從而大幅增加後續調查的難度。因此，在進行封鎖的同時，必須審慎考慮證據的保全問題。
- ◆ **開始進行證據分析與數位鑑識：**封鎖與鑑識並非獨立步驟，而是應同步展開。在執行封鎖行動的同時，數位鑑識團隊應立即著手收集及分析證據，以利於了解攻擊者的入侵路徑、手法與最終目的。
- ◆ **減緩攻擊的封鎖行動：**封鎖的核心目標是「減緩」攻擊，而非完全阻斷所有連線。過於粗暴的封鎖手段可能導致正常業務中斷，因此應採取分層次的策略性行動。
 - **變更通行碼與權限：**一旦確認攻擊者已取得某些帳號的控制權，應立即變更所有受影響的帳號通行碼與權限，涵蓋使用者帳號、系統管理員帳號及服務帳號等。
 - **變更主機名稱與 IP 位址：**在特定情況下，可透過變更受感染主機的名稱及 IP 位址，增加攻擊者重新鎖定目標的難度。此為一種暫時性的應變措施。
 - **將可疑的流量導到不存在的位址：**透過網路設定，將可疑的惡意流量導向不存在的位址（黑洞），藉此觀察攻擊者的行為模式，並收集更多情報。
 - **阻擋攻擊來源 IP 或網段：**當已明確識別攻擊來源的 IP 位址或網段時，直接在防火牆上進行阻擋是最有效的封鎖手段，但須謹慎操作以避免誤擋正常流量。
 - **在類似系統上更新修補程式：**若攻擊是利用某個已知的漏洞，則應立即在所有具有相同漏洞的系統上套用修補程式，以防範類似攻擊在其他系統上發生。
 - **關閉服務：**在某些情況極為嚴重的狀況下，為了防止更大的損失，可能需要暫時性關閉受影響的服務。儘管這是一個艱難的決定，但在維護整體系統安全時是必要的手段。

「封鎖」是一個高強度、高壓力的應變階段，需要快速決策與精確執行。其核心目標是在控制損害的同時，為後續的「根除」與「復原」工作創造有利條件。

(4) 資安事件 - 處理程序之根除

在成功完成「準備」、「識別」與「封鎖」階段後，我們進入流程的第四步：「根除」。顧名思義，此階段的目標是從系統或網路中完全移除惡意程式，並消除所有攻擊者留下的痕跡。這不僅僅是隔離，更是要將病灶徹底切除，確保環境的潔淨。

一旦資安事件已被控制，接下來說明根除階段的核心決策與行動：

◆ 決定採用移除或回存方式：

這是根除階段一個非常關鍵的決策點，需依據事件的複雜度、影響範圍及業務需求來判斷。

• 是否可以完全移除乾淨？

對於簡單的惡意程式，可能可透過工具或手動清除。但對於複雜入侵（如 rootkit），徹底清除極為困難且風險極高。若無法百分之百確定能完全清除，則重建系統（從乾淨備份恢復或全新安裝）是更安全、更徹底的選擇。

• 備份資料中是否有惡意程式？

若決定回存系統，則必須確保所使用的備份資料是乾淨、未受感染的。在恢復前，應對備份資料進行嚴格的掃描及驗證，甚至可在隔離環境中進行試恢復，以確認其安全性。

◆ 強化防禦機制：

根除不僅是清除當前威脅，更重要的是強化防禦機制，防止未來類似事件再次發生。

- **建立額外的偵測與防禦方法：**依據本次事件暴露出的弱點，部署新的安全工具（如 EDR、網路流量分析 (NTA)），強化現有安全控制（如更新防火牆規則），並實施更精細的網路分段。

- **提升稽核紀錄的詳細程度：**調整系統、應用程式、網路設備的日誌設定，以提供更詳細、更全面的數據，為未來的識別與分析提供基礎。

- **在其他系統中尋找已發現的惡意程式：**利用本次事件中收集到的惡意程式特徵，在組織內的其他系統中進行主動排查，以尋找潛在的感染或入侵跡象。

- **更嚴謹控管存取來源：**許多資安事件與弱點存取控制或被竊取的憑證有關。應實施多因子鑑別 (MFA)、強化密碼策略、定期審查權限，並限制網路內部橫向移動。

(5) 資安事件 - 處理程序之復原

我們已經完成了資安事件的「準備」、「識別」、「封鎖」與「根除」階段，成功清除了威脅。現在，我們進入流程的第五步：「復原」。

本階段的核心是：「一旦威脅被根除，接下來應開始將業務與服務恢復至正常運作狀態」。此目標不僅是讓系統重新上線，更重要的是確保業務流程能夠安全、穩定地恢復，並為應對未來可能的攻擊做好準備。

◆ 業務與服務的復原

- **優先順序與時效性：**在復原過程中，無法一次性恢復所有系統和服務。必須依據業務連續性計畫中定義的復原時間目標 (RTO) 與復原點目標 (RPO)，優先恢復對組織營運最關鍵的系統及服務。這與事件處理目標中「降低對業務與網路服務的中斷時間」緊密相關
- **徹底驗證：**在將系統重新連接到生產網路之前，必須進行徹底的功能性測試和安全驗證。確保系統功能正常、資料完整，並且沒有任何殘留的惡意程式或後門。
- **溝通與協調：**持續與相關利害關係人（包括業務部門、客戶、主管機關）溝通復原進度、預計的服務恢復時間，提供精準與及時的資訊。

◆ 加強監控以偵測攻擊是否再發生：

復原階段並非資安應變的終點。事實上，在系統恢復初期，環境仍可能存在潛在風險，或是攻擊者可能試圖再次入侵。因此，強化監控是確保復原成功及防止事件再次發生的關鍵。

• 客製化入侵偵測及防禦規則：

- ✓ **目的：**通用的入侵偵測及防禦系統 (IDS/IPS) 規則可能無法捕捉到本次攻擊中使用的特定戰術、技術及程序。
- ✓ **行動：**依據從「識別」及「根除」階段分析所得的入侵指標 (Indicators of Compromise, IOCs) 及攻擊模式，設計並實施更具針對性的入侵偵測及防禦規則。這將大大提高我們再次發現類似攻擊的能力，是「經驗學習」成果應用的一個具體體現。
- **在網路、主機及應用程式中，額外實作更詳細的稽核紀錄：**
 - ✓ **目的：**提升日誌的詳細程度，能為未來的安全監控、事件識別及數

位鑑識提供更豐富的數據支持。

- ✓ **行動：**重新審視並配置關鍵系統（如網路設備、伺服器、應用程式）的日誌紀錄級別，確保能捕捉到所有重要的安全事件及異常行為。這些詳細的日誌是資安分析的基礎，也有助於完善我們的「準備」階段。

「復原」不僅是技術操作，更是一個業務與安全的平衡點。它要求我們在追求效率的同時，不犧牲安全性。而持續且加強的監控，是確保復原成果，並將本次事件的經驗轉化為組織未來防禦能力的關鍵。

(6) 資安事件 - 處理程序之經驗學習

我們已循序漸進地探討了資安事件處理的各個階段：從事前的「準備」、到事件的「識別」、控制與「封鎖」、徹底「根除」威脅，以及將業務與服務「復原」至正常狀態。

現在，我們來到整個循環的終點，也是下一個循環的起點：「經驗學習」。這個階段的精髓在於將每一次資安事件視為寶貴的學習機會，從中汲取教訓，以不斷優化我們的防禦與應變能力。這完整體現了資安事件處理閉環流程的本質。

◆ 召開經驗學習會議：

資安事件處理完成後，應儘速召開會議，以確保在**相關處理人員記憶猶新的情況下**，進行深入的檢討與反思。此會議能更準確地回顧事件細節、應變挑戰與關鍵決策，與會者應涵蓋所有核心應變小組成員及相關利害關係人。相關回顧與反思說明如下：

- **成功經驗：**識別並記錄在事件處理中發揮關鍵作用的應變措施、流程或技術，並將其列為值得推廣的最佳實務。
 - **不足之處：**誠實面對應變過程中暴露出的問題，例如識別延遲、封鎖不徹底、復原因難或溝通障礙等，以作為未來改進的依據。
 - **根因分析：**深入探究事件發生的深層原因，而不僅止於表面現象。例如，是組態錯誤、漏洞未修補、員工資安意識不足，或是第三方供應鏈風險所致？
 - **證據鑑識回顧：**評估數位證據的取得及監管鏈維護是否符合規範，並從中學習提升鑑識效率的方法。
- ◆ **建議修改相關政策或程序，以利未來安全防護機制實作時，可避免重蹈覆轍：**

這是經驗學習階段最重要的產出，因為學習的最終目的是為了改進，以避免未來重蹈覆轍。這些改進措施包括：

- **更新資安事件處理計畫與程序：**依據學習到的經驗，修訂「資安事件處理計畫」中的人員、科技、業務流程，以及具體的處理程序。
- **強化防禦機制：**針對發現的漏洞及弱點，實施新的安全控制措施，例如更新系統修補程式、客製化入侵偵測規則、提升稽核紀錄詳細程度，並更嚴謹地控管存取。
- **加強訓練與演練：**依據事件中暴露出的知識或技能缺口，調整資安訓練內容及演練情境，確保團隊的能力持續提升。
- **資源優化：**評估所需的財務支持及技術資源是否充足，並進行相應調整。

「經驗學習」是資安應變的最終階段，但它同時也是「準備」階段的起點，形成一個永續改進的循環。一個成熟的組織，不會讓資安事件的教訓白費。透過系統性的經驗學習，組織能夠不斷提升其資安防護的韌性、應變的速度及效率，從而在不斷變化的威脅環境中保持領先。

(7) 資安事件 - 處理個資外洩

我們已探討資安事件的通用處理程序。本節將特別聚焦於一個影響層面廣、法律風險高且對組織聲譽具毀滅性打擊的事件類型：「個人資料外洩」。處理個資外洩事件，除了遵循標準的「準備、識別、封鎖、根除、復原、經驗學習」六大步驟外，更需考量其涉及的法律責任與社會觀感。本節將針對不同階段的特殊要求進行闡述。

◆ 在「識別」與「封鎖」階段：

- **應確定個人資料外洩的範圍：**在個資外洩事件的「識別」階段，我們需進行更精確的範圍確認，這不僅限於受影響的系統，更包含：
 - ✓ **外洩資料的類型：**釐清外洩了哪些具體的個人資料，例如姓名、身分證字號、聯絡方式、病歷或財務資訊等。
 - ✓ **受影響的個資主體數量與身分：**確認涉及了多少人，並盡可能識別出具體的受影響對象，以便後續通知。
 - ✓ **外洩方式：**查明資料是如何被外洩的，例如是被竊取、誤傳或惡意公開等。

目的：精確的範圍確認是後續「封鎖」措施的基礎，也直接影響到法律上的通報義務及對個資主體的通知內容。此階段需要技術部門與



數位鑑識專家的緊密合作。

◆ 在「復原」階段：

- 依「個人資料保護法」要求，應主動通知個資被外洩的對象。
 - ✓ 這是處理個資外洩最核心的法定義務之一。當個人資料被侵害時，公務或非公務機關負有告知當事人的義務。通知內容通常需包含事件發生時間、外洩資料類型、可能造成的損害、已採取的應變措施，以及受害者可採取的保護行動。此步驟高度呼應了「提供精準與及時的資訊」這一處理目標。提供改善方案，以防止個資外洩對象進一步的損害。
 - ✓ **提供改善方案以防止進一步損害：**告知受害者只是第一步。作為資料管理者，組織有責任採取措施，盡可能降低外洩對個資主體造成的「進一步損害」。改善方案範例如下：
 - 提供身分盜用監控服務（例如信用監測）
 - 建議受害者更改相關密碼並啟用多因子鑑別。
 - 提醒受害者警惕釣魚郵件或詐騙電話。
 - 設立專屬諮詢熱線或網站，回答受害者疑問。

處理個資外洩事件，不僅是技術層面的應變，更是一場對組織法律合規、社會責任及聲譽的嚴峻考驗。從事件發生初期的精確識別，到後續的主動告知與損害預防，每一步都必須嚴謹且符合法規要求。

9.7

數位證據及數位鑑識

在前面的章節中，我們多次強調了資安事件處理過程中「保留證據」及「維持監管鏈」的重要性。本節將深入探討這些被保留與管理的對象 - 「數位證據」，以及如何科學地處理它們 - 「數位鑑識」。在現代社會，幾乎所有資安事件都會留下數位痕跡，這些痕跡是釐清真相、追究責任的關鍵。

9.7.1 數位證據的定義與特性

數位證據的定義包含 4 個核心要件：

(1) 由電腦來儲存或是傳送的資料：

數位證據的範圍廣泛，涵蓋任何以數位形式存在或傳輸的資訊，例如硬碟中的檔案、網路設備的日誌、電子郵件、聊天紀錄，甚至是記憶體中的「揮發性資料」。與傳統證據不同，數位證據具有易變性、隱匿性與無形性等特點，使得其收集與保全更具挑戰性。

(2) 該資料可以用來進行後續的偵查：

數位證據是重建事件時間軸、分析攻擊手法、識別入侵來源與影響範圍的可靠依據。在資安事件處理的「識別」與「根除」階段，透過分析系統日誌、網路流量等，可以逐步還原事件全貌。

(3) 偵查的目的是用來確認或是否定反駁有關犯罪的推斷陳述：

數位證據不僅用於建立對事件的「推斷」，更重要的是，它能夠確認這些推斷是否正確，或否定錯誤的陳述。這要求數位證據的採集與分析過程必須嚴謹、科學、客觀。

(4) 該資料在法庭上具有具體的用途：

這是數位證據與一般資料最本質的區別。當資安事件涉及犯罪行為或民事賠償時，合規收集及保存的數位證據，就能在法庭上作為關鍵的呈堂證供。前提是，必須嚴格遵循「取得規範」及「監管鏈要求」，以證明其未經竄改且來源可靠，這也是「讓法務單位可對惡意者提起訴訟」的基石。

數位證據是資安事件調查的靈魂，從事件的發生到最終的法律追訴，都扮演著不可或缺的角色。



9.7.2 數位鑑識

「數位鑑識」是將抽象的數位資料，轉化為可信賴、可追溯、可呈堂證供的過程，是資安事件調查的科學大腦。

(1) 數位鑑識的核心概念：

- ◆ **數位鑑識是鑑識科學的領域之一：**數位鑑識必須遵循標準化、科學化的方法論，使用經科學驗證的技術與工具，確保分析過程的客觀性、完整性與重現性。
- ◆ **探討與電腦犯罪相關證物的處理與調查：**數位鑑識涵蓋從證據識別、妥善保全、複製採集、分析到最終報告撰寫的整個生命週期，旨在重建事件發生過程，找出攻擊者的「誰、何時、何地、如何、為什麼」。
- ◆ **可運用在法庭上支持或是否定犯罪的推論：**當事件涉及法律訴訟時，數位鑑識提供的報告與結論，是支持或反駁犯罪推論的有力證據。這前提是，整個過程必須維持完整的「監管紀錄」。
- ◆ **可運用在一般場合提供資安事件的調查：**對於不涉及法律訴訟的事件，數位鑑識依然能幫助我們理解事件根源，找出防護弱點，進而反饋到「根除」與「經驗學習」階段，不斷提升整體安全水位。

(2) 數位鑑識之原則：

為確保數位證據在偵查、分析及法律程序中有效且可信，必須依賴三大基本原則：

- ◆ **物證的監管鏈：**「監管鏈」是一份詳盡的書面紀錄，記載了數位證據自被發現、扣押、蒐集、保管到最終運送、分析及呈堂的每一個環節。它明確了「誰」在「何時」、「何地」、「為何」持有或處理了這份證據。其核心目標是「確保資料的一致性與完整性」。沒有完整的監管鏈，證據的有效性可能被質疑。
- ◆ **數位證據的完整性：**要求保證數位證據自採集那一刻起，內容未發生任何變動。我們透過雜湊函數（如 SHA-256）為資料產生獨特的「數位指紋」，以驗證其在監管鏈各階段的完整性。
- ◆ **客觀性：**要求鑑識過程必須保持中立、公正，不受任何主觀偏見影響。鑑識人員的職責是讓證據說話，而不是支持預設結論。這要求鑑識人員具備專業操守，遵循標準流程，並允許結果被第三方複查。

「監管鏈」、「完整性」及「客觀性」是數位鑑識的三大支柱，共同確保了數位證據的可靠性、法律效力與調查結果的說服力。

9.8

社交工程

在前面的課程中，詳細討論了資安事件的處理程序，以及數位證據與數位鑑識的重要性。然而，再完善的技術防禦，也可能因為人為因素而功虧一簣。

本節將探討「社交工程」，這是一種利用「人」這個最難防範的弱點的攻擊方式。它並非技術攻擊，而是一種心理操縱，能繞過精心部署的軟硬體安全防護，對組織造成巨大損害。

9.8.1 何謂社交工程

社交工程的定義與特點可歸納為以下 3 點：

(1) 利用人性弱點，以及應用簡單的溝通與欺騙伎倆，遂行其非法的存取與破壞行為：

- ◆ **本質：**社交工程的核心是心理學與人際互動的藝術。攻擊者利用人性的弱點，例如：信任、恐懼、貪婪、好奇、同情、權威崇拜，甚至只是疲勞或匆忙，來進行欺騙。
- ◆ **手段：**它不依賴複雜的程式碼或系統漏洞，而是透過簡單的「溝通」和「欺騙伎倆」，誘使受害者自願洩露敏感資訊或執行惡意行為，進而達成「非法的存取與破壞行為」。

(2) 繞過技術防護，騙取機敏資料：

攻擊者不需要具備頂尖的電腦專業技術，只要受害方對於防範詐騙沒有足夠的認知，就可以輕易的避過企業的軟硬體安全防護，騙取到帳號、通行碼、身分證號碼或其他機敏資料。

- ◆ **最大威脅：**這是社交工程最可怕之處。即使企業投入巨資建立層層技術防護，如防火牆、入侵偵測系統，若員工缺乏對詐騙手法的警覺性，則這些技術防線就可能被輕易「避過」。
- ◆ **攻擊目標：**攻擊者能直接從受害者手中「騙取帳號、通行碼、身分證號碼或其他機敏資料」，這些資料可直接用於入侵系統、竊取資料或勒索。這點凸顯了資安培訓與人員資安意識提升的重要性，與「資安事件 - 處理計畫」中強調的「訓練」緊密相關。



(3) 善於偽裝，利用時事與日常情境：

利用目前備受矚目的重大事件與新聞做為誘餌，也可能利用日常活動做為誘餌，例如線上理財、投資、帳單管理以及購物等。

- ◆ **誘餌設計：**成功的社交工程攻擊善於偽裝，讓受害者難以察覺。攻擊者會利用當前大眾關注的「重大事件與新聞」（如疫情、選舉、熱門話題）來編造欺詐情境，增加可信度。
- ◆ **日常情境：**更普遍的是，攻擊者會模仿受害者熟悉的「日常活動」，例如「線上理財、投資、帳單管理以及購物」等，使受害者更容易放鬆警惕。
- ◆ **應對策略：**針對社交工程的訓練必須結合最新的攻擊趨勢及日常工作場景，並定期進行「社交工程演練」，以提高員工的識別能力。

社交工程是考驗「人」這個要素的終極戰場。再堅固的技術防線也無法完全阻擋利用人性的攻擊。因此，提升全體員工的資安意識及反詐騙能力，是應對社交工程攻擊最重要且最根本的防線。

9.8.2 社交工程常見的攻擊手法

社交工程是一種利用人性弱點進行的心理操縱，其可怕之處在於，無需高深的技術即可突破企業層層的軟硬體防護。以下將逐一介紹最常見的社交工程攻擊手法，以作為建立「人」這道防線的第一步。

(1) 網路釣魚 (Phishing)：

- ◆ **定義：**攻擊者偽裝成可信賴的實體（如銀行、政府機關、知名企業或公司內部同事），透過電子郵件或其他電子通訊方式發送虛假訊息。
- ◆ **運作方式：**資訊內容通常會製造一種「緊急性」、「威脅性」或「誘惑性」，例如帳戶異常、中獎通知、公司政策變更等，誘騙收件人點擊惡意連結、開啟帶有惡意軟體的附件，或直接在偽造網站上輸入敏感資訊。
- ◆ **案例：**您收到一封看似來自您銀行官方的電子郵件，通知您的帳戶因安全問題已被凍結，並要求您點擊連結「立即驗證」身分。點擊後進入的網站外觀與銀行官網一模一樣，但實為釣魚網站，您輸入的帳號密碼會被立即竊取。

(2) 釣魚簡訊 (Smishing)：

- ◆ **定義：**Phishing 的簡訊變體 (SMS + Phishing)。攻擊者透過手機簡訊發送惡意連結或詐騙訊息。

- ◆ **運作方式：**簡訊內容常偽裝成包裹遞送通知、銀行交易警示、會員點數兌換、或假冒公務機關的通知，誘導收件人點擊連結、回撥詐騙電話，或下載惡意應用程式。由於簡訊內容通常較短，且人們對手機訊息的警惕性可能較低，使其更具欺騙性。
- ◆ **案例：**您收到一則簡訊：「您的包裹已抵達指定地點，請點擊連結填寫收貨資訊：[惡意連結]」。點擊連結後，您的手機可能被植入監控軟體，或被要求輸入個人銀行資訊。

(3) 電話詐騙 (Vishing)：

- ◆ **定義：**Phishing 的語音變體 (Voice + Phishing)。攻擊者透過電話，冒充特定機構（如銀行客服、電信公司、技術支援人員、執法機關），進行詐騙。
- ◆ **運作方式：**攻擊者利用語音對話，製造急迫、恐懼、或權威氛圍，誘導受害者提供敏感資訊（如帳號、密碼、OTP 驗證碼），執行轉帳操作，或授予遠端桌面控制權限。他們可能會使用變聲器或預錄音檔來增加真實感。
- ◆ **案例：**您接到一通自稱是「地檢署」或「健保局」的電話，聲稱您的身分被盜用或涉嫌洗錢，要求您將名下資金轉入「安全帳戶」以供監管。

(4) 即時通訊詐騙 (Instant Messaging Scams)：

- ◆ **定義：**攻擊者透過即時通訊軟體（如 Line, WhatsApp, Telegram, Facebook Messenger）進行的詐騙
- ◆ **運作方式：**攻擊者可能盜用受害者親友或同事的帳號，或創建虛假帳號，以緊急借錢、代買點數卡、投票請求、或分享惡意連結等名義進行欺詐。由於即時通訊通常建立在信任關係上，受害者更易輕信。
- ◆ **案例：**您收到一個來自您朋友 Line 帳號的訊息：「我手機壞了，急需一筆錢，可以先幫我轉帳到這個帳戶嗎？」或收到公司主管在 Teams 上傳來的訊息：「幫我點擊這個連結登入，緊急審批一份文件」。

(5) 冒充 (Pretexting)：

- ◆ **定義：**攻擊者事先編造一個虛假但看似合理的故事或情境 (Pretext)，以獲取目標信任，從而套取資訊或促使對方執行某項操作。
- ◆ **運作方式：**這種攻擊通常會進行前期偵察，蒐集目標資訊以建立可信的「藉口」。攻擊者可能冒充為 IT 技術支援人員、審計員、供應商或客戶，編造出需要特定資訊（如密碼重設、系統配置細節、內部流程）的理由，



讓受害者在不知情的情況下提供。這往往是更複雜攻擊的前奏。

- ◆ **案例：**駭客冒充公司 IT 部門人員致電某員工，聲稱正在進行「系統維護及安全更新」，需要該員工的用戶名及密碼來「檢查」其帳戶狀態。

(6) 誘餌 (Baiting)：

- ◆ **定義：**攻擊者透過提供具有吸引力的「誘餌」，引誘受害者上鉤，從而達到攻擊目的。
- ◆ **運作方式：**誘餌可以是實體的，如將帶有惡意軟體的 USB 隨身碟丟棄在公共場所；也可以是數位的，如在線提供免費但帶毒的電影下載。一旦受害者啟用誘餌，惡意軟體便會植入其系統。
- ◆ **案例：**您在公司茶水間發現一個標註為「2025 年員工薪資」的 USB 隨身碟。出於好奇，您將其插入電腦，結果電腦立即感染了勒索軟體。

(7) 尾隨 (Tailgating)：

- ◆ **定義：**攻擊者透過實體欺騙，跟隨合法授權的人員進入受限制區域。
- ◆ **運作方式：**攻擊者利用受害者的善意、禮貌或不警惕，假裝手持大量物品或講電話，趁門還未關閉時溜入。
- ◆ **案例：**一名陌生人手持物品，跟在員工身後，當員工刷卡進入大樓時，此人輕聲示意並請員工扶門，便無需刷卡即可進入。

(8) 蜜罐陷阱 (Honeytrap)：

- ◆ **定義：**攻擊者利用浪漫或其他情感關係作為誘惑，誘使目標落入圈套，以獲取敏感資訊或進行勒索。
- ◆ **運作方式：**攻擊者在社交媒體上建立虛假身分，與目標建立信任關係，然後利用情感依賴，誘導目標透露個人的敏感資訊（如財務、職場機密），或引導其執行特定動作（如安裝遠端控制軟體）。
- ◆ **案例：**某公司高層在線上結識一位異性，在信任建立後，對方誘使該高層透露了公司新產品的研發細節，最終用於商業間諜活動。

這些攻擊手法千變萬化，但萬變不離其宗，都是利用了人的信任、好奇、恐懼或善意。認識這些手法是提高個人與組織資安意識的第一步。

9.8.3 社交工程演練作業流程（以電子郵件為例）

為了提升組織的「人」這道防線，我們需要從被動的事件應變，轉向主動的預防與訓練。社交工程演練便是其中一項關鍵的「準備」工作，它是一種模

擬攻擊，旨在評估員工的資安意識並加以強化。

(1) 計畫與準備：

- ◆ **確立目標與設計場景：**這是演練的基礎。應明確本次演練的目標，例如評估員工對釣魚郵件的識別能力或回報效率。接著，依據目標設計逼真的攻擊場景，包括製作模擬釣魚郵件範本（如偽裝成 IT 部門的帳號通知或人資部門的薪資調整信），並設定發送者身分、主旨、內容與誘騙點擊後的「假性」惡意網站。精準的規劃直接關係到演練的真實性與效果。

(2) 執行模擬攻擊：

- ◆ **發送郵件與記錄反應：**依據事先規劃好的攻擊場景，將模擬釣魚郵件發送給目標員工群體。同時，詳細記錄員工的反應，包括開啟郵件、點擊連結、下載檔案、輸入帳號密碼，以及正確回報可疑郵件的人數。這些數據是後續分析與評估的關鍵依據。

(3) 評估與分析：

- ◆ **分析結果與識別弱點：**在模擬攻擊結束後，需對收集到的數據進行全面分析，計算各項反應率。找出哪些部門、哪些類型的員工更容易上當，以及哪種攻擊手法最具欺騙性。最關鍵的是識別薄弱環節，這不僅限於個人，也可能包括現有的技術控制（如郵件過濾系統的不足）或培訓內容的缺失。

(4) 回饋與教育：

- ◆ **提供回饋與組織培訓：**這是演練達到教育目的的核心環節。對於在演練中上當的員工，應提供具體回饋，解釋其受騙原因並指導正確處理方式。更進一步，應組織培訓課程，結合本次演練發現的弱點，對所有員工進行資安意識強化，教導他們辨識各種社交工程手法及正確的回報管道。

(5) 持續改進：

- ◆ **改進策略與定期演練：**資安防禦是一個持續的過程。依據演練結果與培訓回饋，我們需要改進安全策略，例如更新郵件過濾規則、加強終端防護或優化事件回報流程。最後，這個循環會回到「定期演練」，確保組織能持續適應不斷變化的社交工程威脅，並維持員工高度的資安警覺性。

社交工程演練不僅是對員工的「考試」，更是一個極具價值的「教育」與「改進」過程。透過這種模擬實戰，組織能發現潛在的人為弱點，並針對性地強化資安意識培訓與防護機制。



9.8.4 社交工程 - 案例

前面我們討論了社交工程的定義與多種常見攻擊手法。現在，我們將透過一個實際案例，具體理解這些手法在真實世界中的運用，以及其對政府機關及企業造成的潛在威脅。

(6) 案例描述：

這是一個真實發生過的案例，攻擊者利用學術網路的帳號，冒充「監察院名義」，向政府機關人員及企業發送了含有惡意附件的社交工程電子郵件，如圖 67 社交工程電子郵件案例。

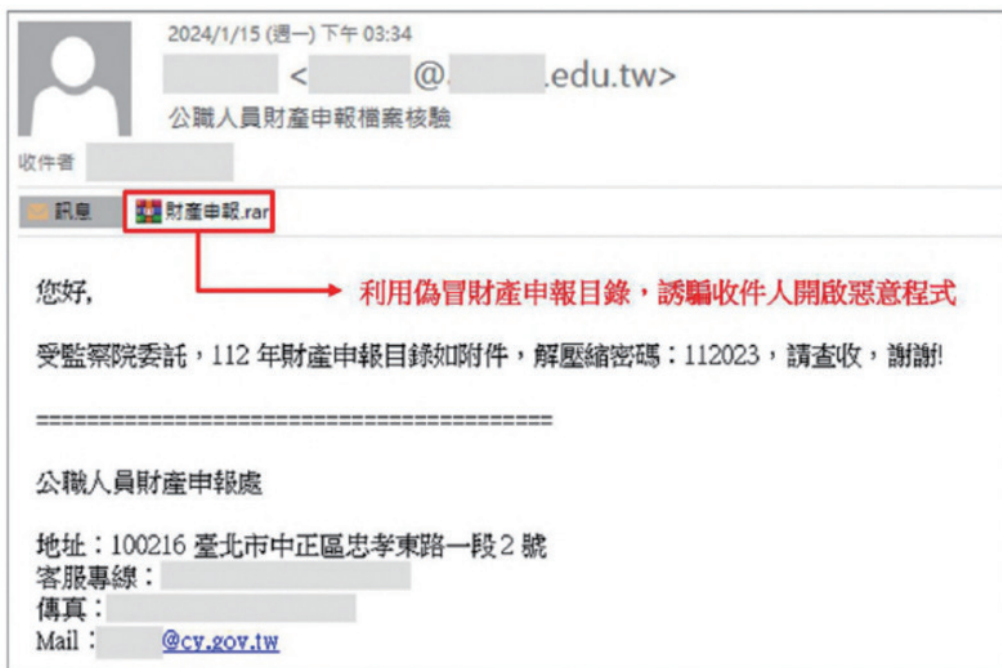


圖 67 社交工程電子郵件案例

- ◆ **郵件內容：**郵件主旨可能偽裝成「公職人員財產申報」或其他具權威性、公務性質的內容，以增加收件人的信任感及開啟意願。
- ◆ **攻擊方式：**郵件內文會誘導收件人開啟附加檔案，例如圖中所示的 財產申報.rar 壓縮檔，並可能提供一個看似「解壓縮密碼」的數字，以降低受害者的戒心。
- ◆ **後果：**一旦收件人開啟惡意壓縮檔內的執行檔，就會觸發惡意程式，導致電腦被植入後門，進而竊取帳號、通行碼等機敏資訊。

(7) 案例中運用到的社交工程手法：

- ◆ **網路釣魚**：透過電子郵件進行攻擊，偽裝成具公信力的機構。
- ◆ **冒充**：精心編造了「公職人員財產申報」這個具說服力的藉口，並冒充監察院的名義，利用公務的敏感性來誘導受害者。
- ◆ **誘餌**：郵件中的「財產申報.rar」壓縮檔本身就是一個誘餌，聲稱是重要的公務文件，引誘收件人開啟並執行其中的惡意程式。

(8) 從案例中學習到的防範重點：

此案例清楚地展示了社交工程如何透過「人」這個環節，繞過傳統技術防禦。為此，我們必須建立多層次防禦體系，其中「人」的防線至關重要：

- ◆ **提升資安意識**：員工的防詐騙認知是技術防護的最後一道防線。
- ◆ **謹慎識別郵件**：仔細檢查發件人完整郵件地址，而非僅看顯示名稱。對不明或不尋常郵件應提高警惕。
- ◆ **不隨意開啟附件或點擊連結**：切勿輕易開啟可疑郵件中的壓縮檔或執行檔。點擊連結前，先確認真實網址。
- ◆ **驗證資訊真實性**：若涉及敏感操作或重要機構通知，則應透過官方管道確認，切勿直接回覆或點擊郵件內連結。
- ◆ **強化技術防護**：確保郵件過濾與端點防護軟體能有效阻擋惡意郵件及程式。
- ◆ **定期資安訓練與演練**：透過定期培訓及社交工程演練，強化員工識別與回報可疑行為的能力。

面對日益複雜的社交工程威脅，我們必須建立一套多層次的防禦體系，其中員工的資安意識及警覺性，是至關重要的一環。

9.8.5 社交工程 - 正確防範觀念

在了解了社交工程的本质與多種攻擊手法後，建立正確的防範觀念至關重要。再好的技術防護，若「人」的環節被突破，也將功虧一簣。本節將提供一系列實用的防範原則，幫助我們共同建構起一道堅不可摧的「人」的防火牆。

(1) 隨時提高警覺，在沒有適當的認證情況下，不應輕信他人，只要出現社交工程攻擊警訊，都應保持小心求證的戒心：

「不輕信」是防範社交工程的首要原則。攻擊者往往利用信任來誘騙受害者，因此在數位世界中，我們必須培養一種零信任的懷疑態度。面對任何



可疑通訊，應保持「小心求證的戒心」，不確定的時候，先問、先查、先證實，而不是立即反應。

(2) 具體而言，包含了以下幾點：

- ◆ **不未經確認即提供資料：**無論對方聲稱是誰、理由多麼緊急，都不要在未經驗證對方身分的情況下，提供任何個人敏感資料、帳號密碼、或一次性驗證碼 (OTP)。
- ◆ **不開啟來路不明的電子郵件及附加檔案：**這是防範網路釣魚的基礎。不認識的寄件人、不尋常的主旨、或與日常工作無關的郵件，都應保持警惕。切勿隨意開啟附件，特別是壓縮檔或可執行檔，因為它們可能攜帶惡意程式。
- ◆ **不連結及登入未經確認的網站：**登入任何網站前，務必仔細檢查網址是否正確，是否有安全憑證 (HTTPS)。若有任何疑慮，則應自行輸入官方網址登入，而非點擊郵件或訊息中的連結。
- ◆ **不下載非法軟體及檔案：**非法軟體或盜版內容常是惡意程式的載體，即使是看似無害的檔案也可能被植入惡意程式。只從官方或可信賴的來源下載。
- ◆ **避免在公共場所使用免費 WiFi 熱點：**公共 WiFi 熱點安全性較低，可能存在中間人攻擊風險。攻擊者可能監聽您的通訊，竊取敏感資料。若需使用，則應搭配 VPN 保護連線。

(3) 任何資訊釋出時都要確認要求者的身分及對方經過授權：

任何內部資訊的釋出或敏感操作的執行，都必須再次確認要求者的身分，並確認其是否具有合法權限。無論是電話、即時通訊，還是面對面的要求，都不要僅憑表面資訊就輕易相信。

(4) 遇到疑似攻擊事件時應向有關單位通報：

「通報」是資安防禦鏈中極為重要的一環。即使您沒有上當，發現任何可疑的社交工程企圖，都應立即向您公司的資安部門或相關主管單位通報。及時的通報能幫助組織採取預防措施，保護更多人不受害。

請務必將以上這些防範觀念內化為日常習慣，使「不輕信、多求證、速通報」成為我們的資安座右銘。這不僅保護個人，更保護了整個組織的安全。

參考資料

- (1) 行政院國家資通安全會報
<https://moda.gov.tw/ACS/nicst/551>
- (2) 第七期國家資通安全發展方案
<https://www.ey.gov.tw/Page/448DE008087A1971/a954ca38-9dfb-446b-879a-9e7ed88495a4>
- (3) 數位發展部資通安全署的職涯發展藍圖
<https://moda.gov.tw/ACS/operations/training/654>
- (4) 資通安全管理法
<https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030297>
- (5) 資通安全管理法施行細則，
<https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030303>
- (6) 資通安全責任等級分級辦法
<https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030304>
- (7) 特定非公務機關資通安全維護計畫實施情形稽核辦法
<https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030306>
- (8) 資通安全事件通報及應變辦法，
<https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030305>
- (9) 資通安全情資分享辦法
<https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030307>
- (10) 公務機關所屬人員資通安全事項獎懲辦法
<https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030308>
- (11) 國家機密保護法施行細則
<https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=I0060005>
- (12) 個人資料保護法
<https://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=I0050021>

- (13) 個人資料保護法施行細則
<https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=l0050022>
- (14) 國家資通安全發展方案
<https://www.ey.gov.tw/Page/448DE008087A1971/a954ca38-9dfb-446b-879a-9e7ed88495a4>
- (15) 資通安全安署相關作業規定及指引
<https://moda.gov.tw/ACS/laws/guide/rules-guidelines/904>
- (16) 資通安全安署相關範本文件
<https://moda.gov.tw/ACS/laws/documents/680>
- (17) 國家資通安全研究院 - 共通規範 (資安參考指引、治理指引、保護指引、偵測、應變、復原)
https://www.nics.nat.gov.tw/cybersecurity_resources/reference_guide/Common_Standards/
- (18) GCA 政府憑證入口網
https://gcp.nat.gov.tw/views/about/about_1.html
- (19) 安全控制措施參考指引 (共通規範 - 資安參考指引)
https://www.nics.nat.gov.tw/cybersecurity_resources/reference_guide/Common_Standards/
- (20) 資安治理成熟度評估參考指引 (共通規範 - 治理)
https://www.nics.nat.gov.tw/cybersecurity_resources/reference_guide/Common_Standards/
- (21) 網路架構規劃參考指引 (共通規範 - 保護)
https://www.nics.nat.gov.tw/cybersecurity_resources/reference_guide/Common_Standards/
- (22) Web 應用程式安全參考指引 (共通規範 - 保護)
https://www.nics.nat.gov.tw/cybersecurity_resources/reference_guide/Common_Standards/
- (23) 防火牆建置資安參考指引 (共通規範 - 保護)
https://www.nics.nat.gov.tw/cybersecurity_resources/reference_guide/Common_Standards/

- (24) 政府機關雲端服務應用資安參考指引 (共通規範 - 保護)
https://www.nics.nat.gov.tw/cybersecurity_resources/reference_guide/Common_Standards/
- (25) 入侵偵測與防禦系統建置資安參考指引 (共通規範 - 偵測)
https://www.nics.nat.gov.tw/cybersecurity_resources/reference_guide/Common_Standards/
- (26) 領域 SOC 實務建置指引 (共通規範 - 偵測)
https://www.nics.nat.gov.tw/cybersecurity_resources/reference_guide/Common_Standards/
- (27) 營運持續管理參考指引 (共通規範 - 復原)
https://www.nics.nat.gov.tw/cybersecurity_resources/reference_guide/Common_Standards/
- (28) 弱點掃描服務 RFP 範本 (v4.0) (資安服務需求建議書範本)
https://www.nics.nat.gov.tw/cybersecurity_resources/reference_guide/Information_Security_Service_Requirement_Proposal_Template/
- (29) 滲透測試服務 RFP 範本 (v5.0) (資安服務需求建議書範本)
https://www.nics.nat.gov.tw/cybersecurity_resources/reference_guide/Information_Security_Service_Requirement_Proposal_Template/
- (30) 資安健診服務 RFP 範本 (v4.0) (資安服務需求建議書範本)
https://www.nics.nat.gov.tw/cybersecurity_resources/reference_guide/Information_Security_Service_Requirement_Proposal_Template/
- (31) 社交工程演練服務 RFP 範本 (資安服務需求建議書範本)
https://www.nics.nat.gov.tw/cybersecurity_resources/reference_guide/Information_Security_Service_Requirement_Proposal_Template/
- (32) 政府組態基準 (GCB)
https://www.nics.nat.gov.tw/core_business/cybersecurity_defense/GCB/
- (33) 資通安全弱點通報機制 (VANS)
https://www.nics.nat.gov.tw/core_business/cybersecurity_defense/VANS/

- (34) 端點偵測及應變機制 (EDR)
https://www.nics.nat.gov.tw/core_business/cybersecurity_defense/EDR/
- (35) 國家資安聯防監控中心 (N-SOC)
https://www.nics.nat.gov.tw/core_business/cybersecurity_defense/N-SOC/
- (36) OWASP
<https://owasp.org/Top10/>
- (37) Secure Software Development Framework(SSDF) version 1.1
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf>
The NIST Cybersecurity Framework (CSF) 2.0 , <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>
- (38) Cybersecurity Maturity Model Certification (CMMC) model overview
https://dodcio.defense.gov/Portals/0/Documents/CMMC/ModelOverview_V2.0_FINAL2_20211202_508.pdf
- (39) CNS 27001:2023 (於下列網址之搜尋欄位，輸入 CNS 27001)
<https://www.cnsonline.com.tw/>
- (40) CNS 27002:2023 (於下列網址之搜尋欄位，輸入 CNS 27002)
<https://www.cnsonline.com.tw/>
- (41) CNS 27005：2024 (於下列網址之搜尋欄位，輸入 CNS 27005)
<https://www.cnsonline.com.tw/>
- (42) NIST CSF 2.0
<https://csrc.nist.gov/News/2024/the-nist-csf-20-is-here>
- (43) NIST CMMC 2.0
<https://dodcio.defense.gov/CMMC/About/>
- (44) NIST SP 800-210
<https://csrc.nist.gov/publications/detail/sp/800-210/final#:~:text=This%20document%20presents%20cloud%20access%20control%20characteristics%20and,a%20Service%29%2C%20and%20SaaS%20%28Software%20as%20a%20Service%29.>

(45) ISO/IEC 22301 : 2019

<https://www.iso.org/standard/75106.html>

(46) ISO/IEC 27017 : 2015

<https://www.iso.org/fr/standard/43757.html>

(47) ISO 22300 : 2021

<https://www.iso.org/standard/77008.html>

(48) ISO 22313 : 2020

<https://www.iso.org/standard/75107.html>

(49) ISO/IEC 33020 : 2015

<https://www.iso.org/standard/54195.html>

資通安全概論

編撰者 羅金賢
指導機關 數位發展部
出版機關 數位發展部資通安全署

地 址 臺北市中正區北平東路 2 號
電 話 02-2380-8500

版本日期 中華民國 114 年 11 月

封面 / 美編 菩薩蠻電腦科技有限公司

本教材僅供資通安全職能訓練課程使用，智慧財產權屬數位發展部資通安全署，欲作上述範圍以外之利用，須徵求數位發展部資通安全署之同意，版權所有，翻印必究。

Printed in Taiwan



指導單位

mod^a 數位發展部
Ministry of Digital Affairs

主辦單位



數位發展部資通安全署
Administration for Cyber Security, moda