Chapter 2

資訊中心管理與實體安全

2.1 前言

- 資訊中心的主要任務就是提供高品質的服務，以輔助各單位能妥善利用電腦設備，有效率地協助工作推展。
- 實體安全 (Physical Security) 是資訊中心安全管理重要的一環，亦是電腦系統的基本外在安全需求。基於人力、經濟，以及其他因素的考量，各機關的資訊中心之安全防護措施不盡相同。實體安全的重要任務就是保護資訊系統外在的環境安全。

2.2 人力資源的安全管理

- 依據《資通安全管理法施行細則》（ 以下簡稱為施行細則 ）第 6 條所示，於母法第 10 條、第 16 條第 2 項或第 17 條第 1 項所定之資通安全維護計畫，應包括下列事項：

  1.核心業務及其重要性。

  2.資通安全政策及目標。

  3.資通安全推動組織。

  4.專責人力及經費之配置。

  5.公務機關資通安全長之配置。

  6.資通系統及資訊之盤點，並標示核心資通系統及相關資產。

  7.資通安全風險評估。

2.2 人力資源的安全管理

8.資通安全防護及控制措施。

9.資通安全事件通報、應變及演練相關機制。

10.資通安全情資之評估及因應機制。

11.資通系統或服務委外辦理之管理措施。

12.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。

13.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。

- 此外，金管會為強化公司資訊安全管理機制，修訂了《公開發行公司建立內部控制制度處理準則》並發布相關令釋。
- 指派資訊安全長並設置資訊安全專責單位。

2.2 人力資源的安全管理

1.資訊安全管理相關證照

證照	說明	證照內容
CISM 管理資訊安全專業人員	CISM 是由全球資訊系統稽核和控制協會 (Information Systems Audit and Control Association, ISACA) 所推出的專業資訊安全管理師證照，具有國際認可性，以企業的資訊安全需求為導向，測試持證人在資訊安全管理領域的知識與技能。	CISM 內容主要是資訊安全策略、風險管理、資訊安全監控、資訊安全事件管理等方面的知識。資訊安全經理、資訊安全主管、風險管理專員等職位可能會用到此證照。
CISPP 資訊系統安全專業人員	CISPP 是由國際資訊系統安全認證聯盟 (International Association of Computer Security Professionals, IACSP) 所提供的專業資訊安全考試，以企業資安需求為導向，針對資訊安全專業人員的職業能力進行評鑑，藉此提供企業客觀的選才與評分標準。	CISPP 內容主要是資訊安全管理、資訊風險管理、資訊安全技術等方面的知識。資訊安全部門、安全分析師、網路安全專家等職位可能會用到此證照。

這張證照適合資訊安全經理、資訊安全主管以及風險管理專員等職位，表明持證人具備企業所需的資訊安全知識與技能

這張證照對資訊安全部門、安全分析師、網路安全專家等職位特別有用，能為企業提供客觀的選才與評分標準

2.2 人力資源的安全管理

證照	說明	證照內容
CRISC 風險與資訊系統控制	CRISC 是由全球資訊系統稽核和控制協會 (Information Systems Audit and Control Association, ISACA) 所推出的 IT 領域的專業證照。它以企業風險管理和資訊系統控制為基礎，針對資訊系統控制和資訊風險管理的四個相關領域，進行鑑定。	CRISC 內容主要是風險評估、風險管理、風險監控、資訊系統控制等方面的知識。風險經理、資訊系統經理、IT 審計師、合規性主管等職位可能會用到此證照。
CGEIT 國際企業資訊治理師認證	CGEIT 是由全球資訊系統稽核和控制協會 (Information Systems Audit and Control Association, ISACA) 所推出的 IT 治理專業資格考試，以提高其在 IT 治理領域的能力和價值。	CGEIT 內容主要是企業級 IT 治理、風險管理、合規性等方面的知識。高層管理人員、IT 治理、風險和合規性專家等職位可能會用到此證照。
iPAS 資訊安全工程師	iPAS 由經濟部發證，教育部認可，產業界支持之專業工程師考試。以企業用人能力需求為導向規劃鑑定內容，並推動企業認同優先面試／聘用／加薪獲證者，以提供企業客觀的選才與評分標準。	iPAS 內容主要是網路安全、資料庫安全、應用程式安全、系統安全等方面的知識。資安工程師、系統安全工程師、網路安全工程師等職位可能會用到此證照。

這張證照適合風險經理、 IT 審計師、合規性主管等職位，是評鑑資安控制和風險管理的四個相關領域的專業認證

適合高階管理人員、 IT 治理與風險專家等職位

此證照可作為企業優先面試、聘用或加薪的依據，適合資安工程師、系統安全工程師、網路安全工程師等職位

2.2 人力資源的安全管理

2.資安標準內容相關證照

證照	說明	證照內容
ISO27001 LAC	ISO27001 LAC 由 ISO/IEC 標準認證組織認可的資訊安全管理系統審核員認證考試，目的是評估個人在資訊安全管理體系 (ISMS) 方面的專業知識和技能，包括 ISO 27001 的要求、評審方法、溝通技巧和審核技巧等，以確保對資訊安全管理體系進行有效的評審和審核。	ISO27001 LAC 內容主要是 ISMS 的設計、實施、監視、評估和改進。資訊安全經理、資訊技術稽核師、資訊安全管理系統內部稽核師、資訊安全管理系統供應商和資訊安全管理系統外部審核師等職位可能會用到此證照。

適合資訊安全經理、資訊技術稽核師、內部及外部稽核師等職位 。

2.2 人力資源的安全管理

3.供應鏈安全相關證照

證照	說明	證照內容
SCS-CP 資訊安全 技術專業	SCS-CP 是由台灣資通安全協會 (Taiwan Information Security Association, TISA) 發證，國際供應鏈安全協會所認證的供應鏈安全專業證照，以供應鏈安全相關的法規、風險評估、安全監控等主題為核心，以確保企業能夠有效保護供應鏈中的貨物、人員及設施不受到任何潛在的威脅或危害。	SCS-CP 內容主要是電腦科學、資訊系統、資料庫、網路、軟體工程、人工智慧等領域的技能和知識。軟體開發工程師、資訊系統管理員、網路安全分析師、資料分析師、人工智慧工程師和項目經理等職位可能會用到此證照。

適用於軟體開發工程師、資訊系統管理員及網路安全分析師等職位。

2.2 人力資源的安全管理

4.網路安全相關證照

證照	說明	證照內容
CCNA Security 思科認證網路工程師	CCNA Security 是由思科公司 (Cisco Systems, Inc., CISCO) 開發的認證考試，旨在評估參加考試者對網路安全的理解和能力。該考試內容包括網路安全基礎知識、安全傳輸技術、安全基礎架構、安全儲存等方面的內容。	CCNA Security 證照的內容主要是網路安全基礎、VPN、防火牆、入侵檢測和防範、安全路由等方面的技能和知識。網路安全工程師、網路工程師、安全分析師、安全顧問和技術支援人員等職位可能會用到此證照。
CompTIA Security+	CompTIA Security+ 是由電腦技術工業協會 (Computing Technology Industry Association, CompTIA) 所認證的資安專業證照。該證照由經濟部之資訊工業策進會引進台灣，並受到教育部認可。這項證照以企業用人能力需求為導向，規劃鑑定內容，並得到產業界的支持。	CompTIA Security+ 證照的內容主要是網路安全、軟體安全、加密、身分驗證和授權、防範威脅、風險管理等方面的技能和知識。網路安全工程師、網路和系統管理員、安全分析師、安全顧問和技術支援人員等職位可能會用到此證照。

內容涵蓋網路安全基礎、 VPN 、防火牆、入侵偵測與防範等。

內容包括資安漏洞掃描、弱點分析及事件分析等。

2.2 人力資源的安全管理

證照	說明	證照內容
CEH 駭客技術 專家認證	CEH 是由國際電腦調查協會(International Association of Computer Investigative Specialists, IACIS) 發證，是通過對駭客手法的理解和應用，幫助認證人了解和熟悉網路和系統安全的最新技術和方法，核心概念是「道德駭客」。	CEH 證照的內容主要是網路和系統安全、滲透測試、漏洞掃描和測試等方面的技能和知識。網路安全工程師、滲透測試工程師、安全分析師、安全顧問等職位可能會用到此證照。
CHFI 資安鑑識調查專家認證	CHFI 是由國際電腦調查協會(International Association of Computer Investigative Specialists, IACIS) 發證，此證照得到許多企業和政府機構的支持與認可，強調以調查為導向，培養具備高度專業素養的電腦調查專業人才。	CHFI 證照的內容主要是電子證據蒐集、鑑識分析、審計追蹤、線上調查等方面的技能和知識。資訊安全分析師、資訊安全工程師、資料分析師、鑑識調查師等職位可能會用到此證照。
ECSA 專業安全分析師	ECSA 是由國際電腦調查協會(International Association of Computer Investigative Specialists, IACIS) 發證，是全球公認的資安專業證照之一，受到產業界廣泛認可與支持。考試內容以企業用人能力需求為導向，是一個實戰性強、實用性高的資安證照。	ECSA 證照的內容主要是滲透測試的各個階段，包括情報蒐集、足跡追蹤、漏洞掃描、漏洞利用等技能和知識。滲透測試工程師、安全分析師、資訊安全工程師、系統管理員等職位可能會用到此證照。

核心概念為「道德駭客」，內容包括網路與系統安全、滲透測試、漏洞掃描及測試。適合網路安全工程師、滲透測試工程師及安全顧問等職位

此證照特別適合需要處理數位鑑識相關工作的職位，例如資安分析師、資訊安全工程師、資料分析師及鑑識調查師等。

適合擔任滲透測試工程師、資安研究員、資訊安全工程師及系統管理員等職位。

2.2 人力資源的安全管理

證照	說明	證照內容
OSCE	OSCE 是由 Offensive Security 發證的高級安全專業考試，著重於提高駭客攻擊技能和解決複雜的安全挑戰，該考試得到產業界的廣泛支持和認可，並以其嚴格性和實用性聞名。	OSCE 證照的內容主要是針對漏洞利用和測試的高級技術和知識，包括漏洞利用、反殺式測試、編程技巧等等。滲透測試專家、安全分析師、資訊安全工程師、系統安全架構師等職位可能會用到此證照。
OSCP	OSCP 是由 Offensive Security 公司提供的專業測試，是一種進階的資訊安全認證，主要目的是測試考生對網路測試和攻擊技能的掌握能力。	OSCP 證照的內容主要是針對漏洞利用和測試的技術和知識，包括滲透測試方法、漏洞利用、編程技巧等。滲透測試工程師、安全研究員、資訊安全工程師、系統安全分析師等職位可能會用到此證照。

適合擔任滲透測試專家、安全分析師、資訊安全工程師及系統安全架構師等職位

擔任滲透測試工程師、安全研究員、資訊安全工程師及系統安全分析師等職位 。

2.2 人力資源的安全管理

5.應用程式安全相關證照

證照	說明	證照內容
CompTIA CySA+ 威脅情報分析家	CompTIA CySA+ 是由電腦技術工業協會 (Computing Technology Industry Association, CompTIA) 所認證的專業資安考試，以企業用人能力需求為導向規劃鑑定內容。考試涵蓋網路及系統安全、弱點與漏洞管理、威脅與漏洞評估等主題。	CompTIA CySA+證照的內容主要是涵蓋安全威脅檢測、分析、回應等方面的技能和知識，包括資安漏洞掃描、弱點分析、事件分析等。資安分析師、安全操作中心分析員、安全工程師、網路安全工程師等職位可能會用到此證照。
CSSLP 認證安全軟體生命週期專家	CSSLP 是由國際資訊安全認證聯盟 (International Information System Security Certification Consortium, Inc., ISC) 所提供的專業工程師考試，在於證明擁有軟體安全相關知識和技能的專業人士，能夠有效地保護軟體免受各種內部和外部威脅。	CSSLP 證照的內容主要是軟體開發生命週期中的安全性、安全性需求、設計和代碼實現、軟體測試、驗證和驗收、軟體部署、維護和更新等方面的知識。軟體安全工程師、應用程序開發人員、軟體測試工程師、軟體架構師、系統工程師、資訊安全專家等可能會用到此證照。

資安分析師、安全操作中心分析師、安全工程師及網路安全工程師等職位

軟體安全工程師、應用程序開發人員、軟體測試工程師及軟體架構師等職位

2.2 人力資源的安全管理

證照	說明	證照內容
GSSP-JAVA 全球安全專業 -Java 語言編程證照	GSSP-JAVA 是由國際資訊安全認證聯盟 (International Information System Security Certification Consortium, Inc., ISC) 發行的專業認證，以驗證應該具備的 Java 安全編程技能，包括如何避免常見的安全漏洞和攻擊。	GSSP-JAVA 證照的內容主要是 Java 編程語言的安全漏洞、攻擊和防禦方法。Java 開發人員、軟體測試人員、應用程式安全工程師等可能會用到此證照。
GSSP-.NET 全球安全性專業認證 - .NET 平台	GSSP-.NET 是由國際資訊安全認證聯盟 (International Information System Security Certification Consortium, Inc., ISC) 發行的專業認證，以驗證對於使用 .NET 技術開發 Web 應用程式的安全性進行測試、審核、監控及維護等方面的知識和技能水平，考試內容主要涵蓋 .NET 平台的安全設計、代碼編寫、調試和應用安全測試等方面。	GSSP-.NET 證照的內容主要是 Web 和 Windows 應用程式的安全漏洞檢測和防禦，包括 ASP.NET Web 應用程式、Windows 桌面應用程式等 .NET 開發人員、Web 開發人員、安全分析師、應用程式測試人員等可能會用到此證照。

Java 開發人員、軟體測試人員以及應用程式安全工程師等職位

.NET 開發人員、 Web 開發人員、安全分析師與應用程式測試人員等職位

2.2 人力資源的安全管理

6.資料庫安全相關證照

證照	說明	證照內容
Oracle Database Security 資料庫安全	Oracle Database Security 是由 Oracle 公司推出的專業認證考試，此證照獲得了經濟部的認證，並獲得了教育部的認可。該證照的鑑定內容以企業用人能力需求為導向，考試內容包括但不限於資料庫安全管理、安全測試和實施資料庫安全策略等方面。	Oracle Database Security 證照的內容主要是 Oracle 資料庫安全的基礎知識、使用 Oracle 資料庫安全功能進行資料庫保護和漏洞修補、使用 Oracle 資料庫安全工具進行資料庫監視和日誌分析，資料庫管理員、資安專家、資訊安全分析師、資訊安全工程師等可能會用到此證照。
GCPM Google Cloud 平台管理員	GCPM 是由台灣國際專案管理師學會 (Project Management Institute Taiwan Chapter, PMI Taiwan Chapter) 發證，是 Google 提供的管理 Google Cloud 平台的證照。測試持有人如何設置和配置 Google Cloud 環境，管理網路資源、應用程序和服務，以及設定安全性和訪問控制。	GCPM 證照的內容主要是 Google Cloud 平台的架構設計、部署、監控和優化等方面的知識，GCP 的管理員、資料庫管理員、資訊安全工程師等可能會用到此證照。

Oracle 資料庫管理員、資安專家、資訊安全分析師與資訊安全工程師等。

GCP 管理員、資料庫管理員與資訊安全工程師等職位

2.2 人力資源的安全管理

7.雲端安全相關證照

證照	說明	證照內容	
CompTIA Cloud+ 電腦技術工業協會雲端技術專業認證	CompTIA Cloud+ 是由 (Computing Technology Industry Association, CompTIA) 電腦技術工業協會發行的專業雲端計算證照，目的是證明持有人在規劃、設計、運營、管理和保護雲端解決方案方面的能力。	CompTIA Cloud+ 證照的內容主要是針對有意從事雲端技術相關職位的 IT 專業人員。它考核雲端計算的核心概念、技術、架構和安全，以及在公有、私有和混合雲環境中實施、維護和管理雲端解決方案的能力，雲端架構師、雲端系統工程師、雲端運維工程師、雲端解決方案顧問等可能會用到此證照。	**雲端架構師、雲端系統工程師、雲端運維工程師及雲端解決方案顧問等**
CCSP 雲端安全專業認證	CCSP 是一種由國際資訊安全認證聯盟 (International Information System Security Certification Consortium, Inc., ISC) 所提供的雲端安全證照，目的是為了確認個人對於雲端安全的知識和技能，以及確保個人能夠設計、管理和保護各種雲端服務，包括軟體即服務 (SaaS)、平台即服務 (PaaS) 和基礎架構即服務 (IaaS)。	CCSP 證照的內容主要是雲端資訊安全、架構和設計、雲端資料安全、雲端平台和基礎設施安全、遵循和合規性等相關議題，雲端架構師、雲端安全顧問、雲端運營管理、企業資訊安全專員、網路安全工程師等可能會用到此證照。	**雲端架構師、雲端安全顧問、雲端運營管理及資訊安全專員等職位**

2.2 人力資源的安全管理

8.無線網路安全相關證照

證照	說明	證照內容
CWSP	CWSP 是由國際資訊安全認證聯盟(International Information System Security Certification Consortium, Inc., ISC) 所發行，目的是驗證專業人士對無線網路安全的知識和技能，包括無線網路安全架構、安全協議和技術、漏洞分析和解決方案等方面的能力。	CWSP 證照的內容主要是安全標準、加密和驗證技術、無線 LAN 架構和協議、漏洞掃描和風險評估，無線網路安全專家、網路安全工程師、網路管理員等可能會用到此證照。

資安專家、網路安全工程師及網路管理員等

優先考取證照

- iPAS 資訊安全工程師：這是一項由台灣政府及產業支持的認證，適合初學者入門。相較於其他國際證照，它更貼近台灣的業界需求，能幫助您快速建立基礎。

- CISSP（資訊系統安全專業人員）：被譽為資安界「黃金證照」，證明個人具備資安專業知識。儘管難度較高，但其國際認可度極高，對職涯發展有重大助益。

進階證照

- CISM（管理資訊安全專業人員）：此證照專注於資安管理，適合有一定工作經驗的資安經理人。與 CISSP 相比，它更偏重於管理與風險控制。

- OSCP（專業認證）：這張證照強調實戰，需要動手操作來通過考試，因此難度相當高。適合希望專攻滲透測試與攻擊技術的專業人士。

據職涯方向考取特定領域證照

- CHFI（資安鑑識調查專家認證）：若您對數位鑑識有興趣，這張證照能提供您所需的專業知識。
- CWSP（無線網路安全專業認證）：如果您專注於無線網路安全領域，此證照能證明您具備相關技術。
- CCSP（雲端安全專業認證）：隨著雲端技術日益普及，這張證照對於想在雲端安全領域發展的人來說至關重要。
- GSSP-JAVA (全球安全專業 — Java 語言證照)

2.3 空間環境資源的安全管理

- 建立安全無虞且正常運轉的電腦使用環境，是資訊部門的主要任務之一。

1.電腦機房環境不良

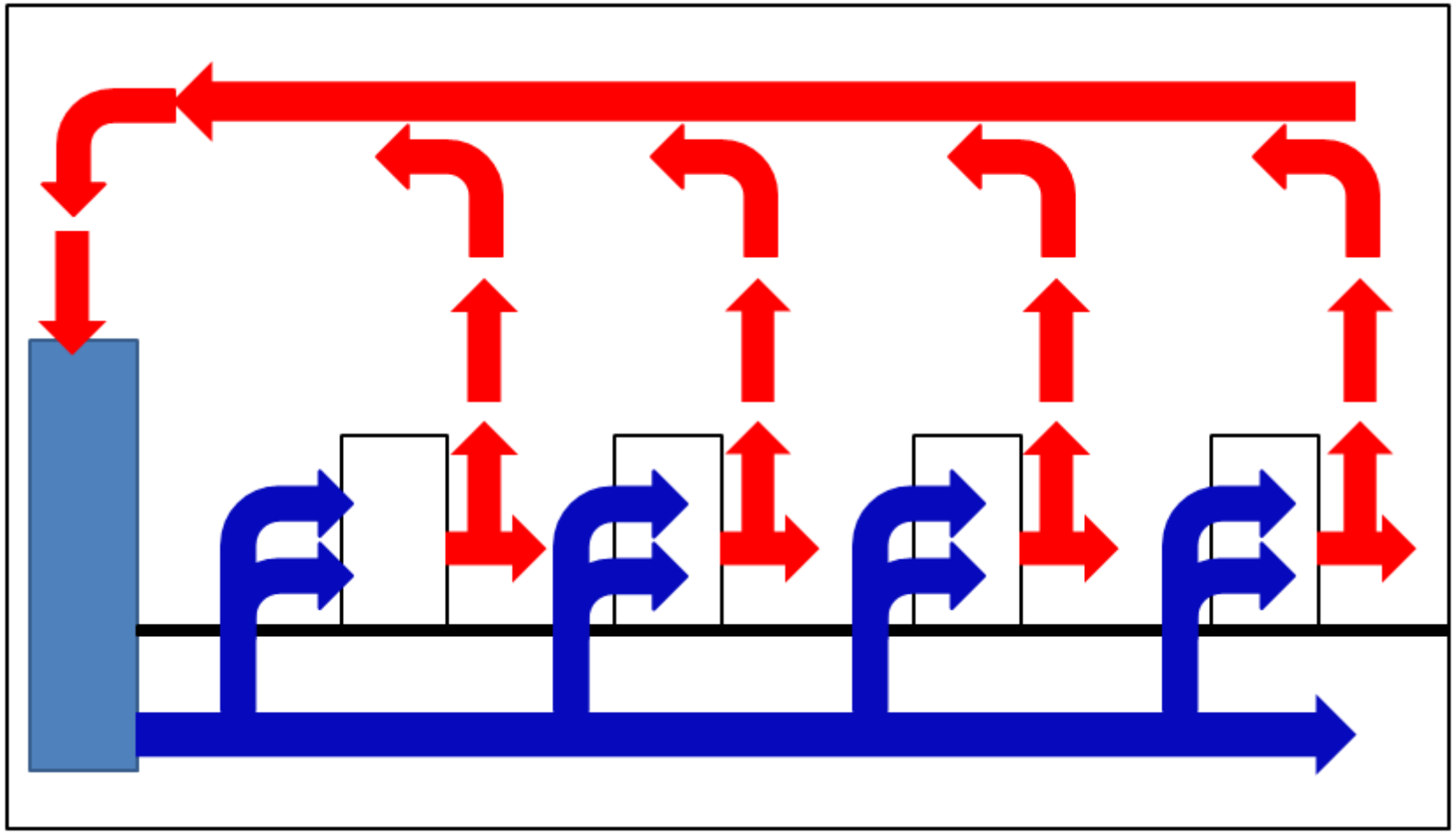
機房環境不良會導致電腦系統故障。這裡所謂的機房環境除了有形的環境衛生外，無形的溫度、濕度及落塵等更為重要。

(1) 溫度：電腦系統對於溫度非常敏感。溫度維持在攝氏 20 至 25 度間。

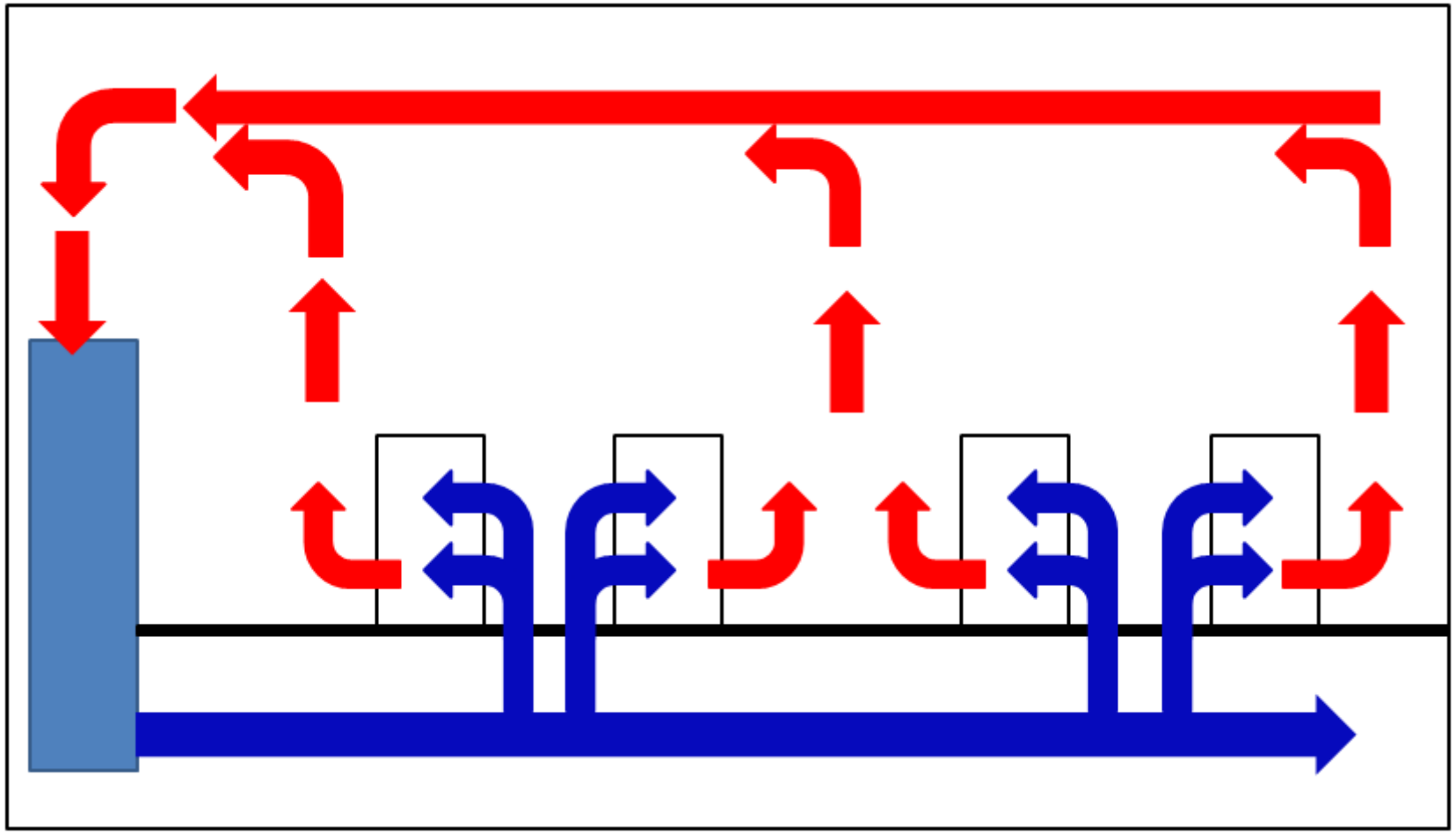
(2) 濕度：潮濕環境往往造成電路板快速腐蝕。一般電腦機房之濕度應維持在 40% 至 60% 之間。

(3) 落塵：購置空氣清淨機，以防落塵飄散電腦機房。

溫度控制



冷熱通道（熱對流）



2.3 空間環境資源的安全管理

2.停電

電腦需要穩定的電源，若遇到停電或電力系統故障，電腦就會立刻停止運作。

現在的電腦機房大多設置不斷電供應系統 (UPS) ，以應付停電時的處理。

3.機房位置規劃不當

電腦機房位置應遠離受電磁場干擾的地方。

機房內更要避免鋪設地毯，除了容易藏污納垢外，也會產生靜電。

2.3 空間環境資源的安全管理

4.火災

火比水更難解決，因為反應時間較少。

實施異地備份或者透過雲端服務備份，更可以完全避免因火災造成資料之毀損。

目前許多電腦機房都使用二氧化碳滅火器或自動噴氣系統來抑制火災擴散。

5.雷擊

雷擊會產生超強電流，若不引導到地表，很容易發生火災及燒毀設備。

2.3 空間環境資源的安全管理

電腦的電源線是三線式（ 三個插孔之插座 ），分別是火線、 空線及接地線。 接地線的用途即是在保護電腦設備，避免因閃電雷擊所產生超強電流，而燒毀電腦設備及電器用品。

6.地震

對於電腦機房及設備之防震能力，應格外重視。

7.水災

水災會帶來泥沙及石礫。

資訊中心工作人員必須在最短的時間將重要的資料搬至較地面更高的地方。

2.4 硬體設備資源的安全管理

- 針對發生資通安全事件導致電腦硬體設備與系統不能正常使用有網路斷線、不正常使用或電腦系統故障等主要原因，這些都是屬於「可用性」構面。

2.4.1 電腦系統故障

- 許多電腦廠商皆有備援的電腦系統，並能在 24 小時內移送到發生災害的地點，或者直接從生產線運送而來。
- 而沒有資訊應用系統及資料，必須在最短時間內，將所有應用軟體及資料安裝完成，以恢復電腦正常的運轉。
- 規劃電腦設備時就必須考慮採用容錯系統 (Fault Tolerance) ，亦即有兩套系統同時運轉，一旦有一套系統發生故障時，將由另外一套系統接替，使進行的作業不會中斷。

2.4.2 網路斷線與網路的品質監測

- 如何維持網路暢通是資訊部門最基本的任務之一。這裡所謂的網路暢通，包括網路正常連線沒有斷線、網路正常流通沒有阻塞以及網路正常傳輸沒有雜訊。
- 網路的品質一直是使用者對資訊部門服務品質的一項重要指標。資訊部門除了可以使用網路分析儀來規劃及監視網路品質外，另外還有一種更簡便的方法可以測試網路品質，亦即使用網路所提供的「 ping 」公用程式。

2.4.2 網路斷線與網路的品質監測

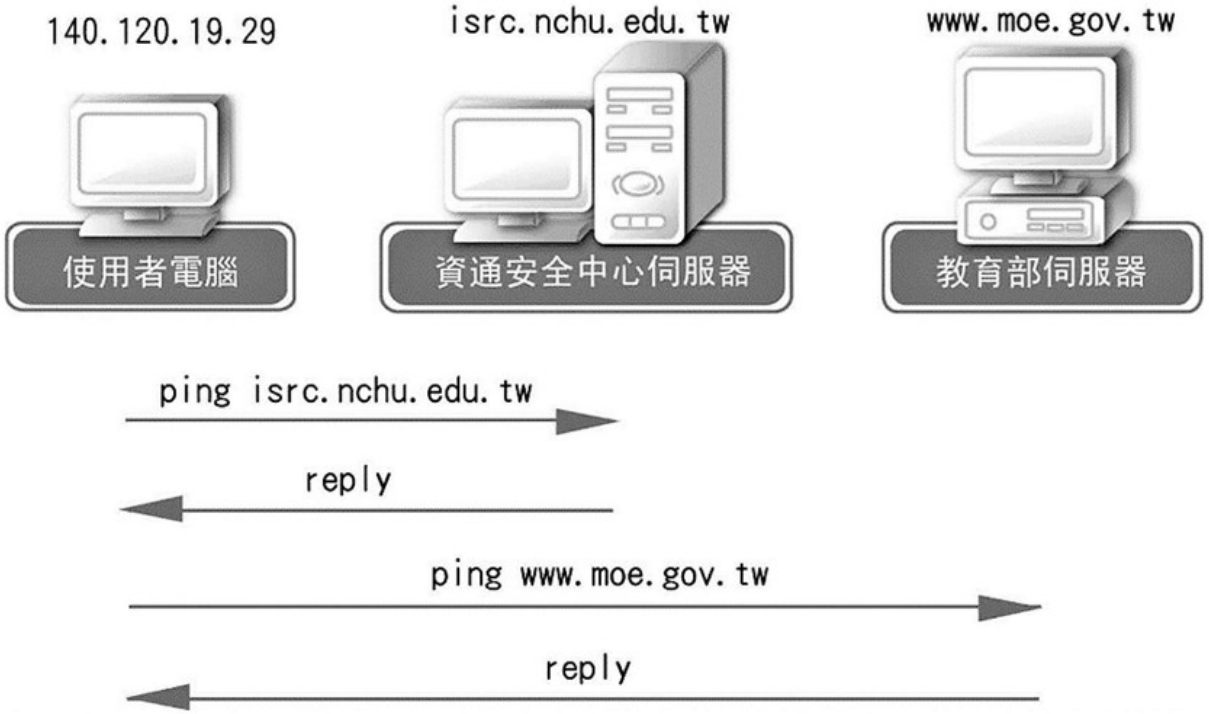


圖 2.1　使用 ping 測試網路品質

2.4.2 網路斷線與網路的品質監測

- > ping isrc.nchu.edu.tw [Enter]

  Pinging isrc.nchu.edu.tw [140.120.1.20] with 32 bytes of data:

  Reply from 140.120.1.20: bytes=32 time<1ms TTL=242

  Reply from 140.120.1.20: bytes=32 time<1ms TTL=242

  Reply from 140.120.1.20: bytes=32 time<1ms TTL=242

  Reply from 140.120.1.20: bytes=32 time<1ms TTL=242

2.4.2 網路斷線與網路的品質監測

- 當 ping 之網路位址不存在時，則回應錯誤訊息

  > ping www.nchu.com.jp [Enter]

  Bad IP address www.nchu.com.jp

2.4.2 網路斷線與網路的品質監測

Request timed out

- 表示兩個網站間之傳輸時間已超過預定的 1,000 毫秒，可能的原因有下列三種：

  1.兩個網站間的路徑或網站目前正處於堵塞或故障狀況。

  2.對方網站目前是關機或故障狀況。

  3.對方網站目前忙碌。

2.5 軟體設備資源的安全管理

2.5.1 軟體程式的安全管理

- 對於作業系統安全管理，資訊中心必須隨時注意記憶體的使用情況。記憶體是否被非法使用或藏入病毒程式，或其他系統資源是否被非法盜用等都需加以預防。
- 公用程式或工具提供使用者更方便地使用電腦系統，而有些公用程式或工具可以直接或間接存取系統資源。資訊中心對於系統提供哪些公用程式或工具，以及有哪些權限必須加以了解，並做妥善之安全管理。

2.5.2 資料的備份

- 所謂資料備份就是複製全部或部分檔案，萬一系統毀損或檔案遺失，可還原檔案，使系統盡可能地回復到損壞前的狀態。
- 資料備份的範圍依資料的擁有者，可以大致區分為企業組織的資料備份及個人的資料備份。

2.5.2 資料的備份

企業組織的資料備份

- 企業組織的資料備份是指企業或組織針對其資訊系統所產生的資料來做備份。
- 企業資料備份的策略依資料備份的頻率來區分，可以分為日備份 (Daily Backup)、週備份 (Weekly Backup)、月備份 (Monthly Backup)、隔月備份 (Bimonthly Backup)、季備份 (Quarterly Backup) 或年備份 (Yearly Backup) 等等。
- 日備份就是每天對企業內部的資料做備份；週備份是每週做一次備份；月備份是每月進行一次備份；隔月備份就是每兩個月進行一次備份；季備份是每季進行一次備份；而年備份則是每年進行一次備份。

2.5.2 資料的備份

1.完整備份 (Completely Backup)

完整備份是將電腦系統所有檔案（ 包括資料、應用系統程式、作業系統及系統程式等 ），不管這些檔案是否有被標記「已備份」，均要完整地複製至儲存媒體上。

完整備份的優點是只需一份儲存媒體來備份所有檔案。缺點則由於資料量很大，並不適合每天都做完整備份，通常間隔一段較長的時間才做完整備份。

2.5.2 資料的備份

2.選擇式備份 (Selective Backup) 或差異備份 (Different Backup)

有別於完整備份將資料完整地複製一份，差異備份只在第一次備份時做完整性備份，之後要備份時只把從上次完整備份到目前有改變的檔案（ 新增及更新 ）進行資料備份。值得注意的是，差異備份後並不清除存檔屬性，亦即還是保留新增或更新之「未備份」屬性，以便下次做差異備份時，此檔案還是會再被重複備份。

這種備份只有某些有更改過的檔案才必須做備份，所以這一類型的備份方式可以縮短備份的時間，但需要二份儲存媒體空間，一份用來保管完整備份檔案，另外一份則用來儲存差異備份資料。

2.5.2 資料的備份

3.增量備份 (Incremental Backup)

增量備份只在第一次備份時做完整性備份，之後要備份時，只把從上次備份到目前有改變的檔案（ 新增及更新 ）進行資料備份。有別於差異備份，增量備份後將清除存檔屬性，亦即將此新增或更新檔案之存檔屬性更改為「已備份」屬性，所以下次再做增量備份時，此檔案並不會再被重複備份。

需要二份以上儲存媒體空間，一份用來保管完整備份檔案，其他則用來儲存每日之增量備份資料。

2.5.2 資料的備份

增量備份另外一個缺點是可靠度較差，一旦某一次增量備份（設當月 6 日）的儲存媒體毀損或遺漏，系統將只能回復到當月 5 日以前之檔案資料，6 日至 20 日的檔案資料都將遺失。

- 企業資料備份的策略依資料備份的儲存地點來區分，可以分為同地備份 (Local Backup) 及異地備份 (Remote Backup)。
- 同地備份就是所備份的儲存媒體與原資料儲存體是在同一地點。
- 異地備份就是所備份的儲存媒體與原資料儲存體是在不同地點。

2.5.2 資料的備份

- 異地備援是希望當資訊系統的原所在地發生災難，而造成系統無法復原的損壞時，可以在最短的可接受時間內，讓異地的備援系統能部分或完全地回復原系統所能提供的服務，將災難對使用者的影響降至最低。
- 異地備援有以下兩個重要的特性。

1.異地存放

為了避免災難造成原設備及備援設備同時損壞，所以備援設備必須放置在離原設備之安全間距以上。

2.同步傳輸

由於原設備與備援設備是異地存放，所以兩者之間的資料傳輸必須透過專線或高速網路來進行。

2.5.2 資料的備份

- 在建置異地備援機制時還必須考量：
  1.資料備份儲存系統必須不耗用主機系統資源及效能。
  2.資料在網路上傳輸時必須做適當的安全防護措施。

2.5.2 資料的備份

個人的資料備份

- 在備份個人資料時，我們多半會採用完整備份的策略，將所需備份的資料存放在行動碟或光碟等儲存媒介上。至於執行備份的頻率則是視個人需要而異，可以是日備份、週備份或月備份等等。
- 公共雲端服務 (Public Cloud Service) 就是提供給使用者一個網路儲存空間來儲存個人資料，使用者只要透過網路便可以存取個人資料。
- 網路儲存機制同樣也需要安全的控管機制。

2.5.3 敏感媒體的處理

- 有很多重要資料均儲存在各種媒體上，一旦這些媒體因故要丟棄時，必須先將媒體上的資料銷毀，否則會有洩漏機密之疑慮。銷毀各種媒體常用的設備如下：

  1.碎紙機

  2.水銷

  3.磁性資料的清除

  4.消磁物體

- 隨身碟 (USB) 及行動碟大都是使用快閃記憶體 (Flash Memory)，丟棄前應先將其以鐵鎚擊碎破壞。