

第十五章 網路管理與安全

前言

- ◆ 15-1 網路管理常用的通訊協定
- ◆ 15-2 帳號與權限管理
- ◆ 15-3 資料加密與解密
- ◆ 15-4 數位簽章
- ◆ 15-5 公開金鑰基礎建設 (PKI)
- ◆ 15-6 防火牆
- ◆ 15-7 加強網路層的安全 - IPsec
- ◆ 15-8 資訊安全管理
- ◆ 實作練習：Windows 10/7 的防火牆功能

15-1 網路管理常用的通訊協定

網路管理通訊協定可分為兩類：

- ◆ 第一類是用來修改遠端裝置組態的『遠端組態通訊協定』
- ◆ 另一類則是用來監視網路運作狀態的『網路監控通訊協定』。

15-1 網路管理常用的通訊協定

- ◆ 15-1-1 可用於遠端組態的通訊協定—Telnet 與 HTTP
- ◆ 15-1-2 網路監控通訊協定—SNMP 與 RMON

應用層

表達層

交談層

傳輸層

網路層

鏈結層

實體層

圖 15-1 SNMP 和 Telnet、HTTP 一樣都是應用層的通訊協；至於 RMON 則是 MIB（管理資料庫，後詳）的一種

可用於遠端組態的通訊協定

— Telnet 與 HTTP

- ◆ 讓網管人員可以從遠端查看與修改網路設備的組態設定

Networking
Essentials

15th Edition

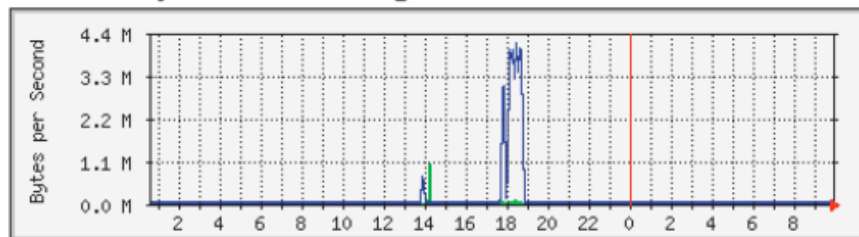
網路監控通訊協定—SNMP 與 RMON

◆ SNMP 協定

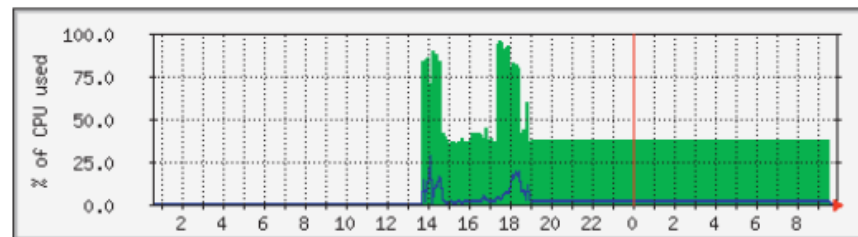
提供一個統一的協定, 方便收集網路設備的狀態, 以便監控各設備的運作情況

MRTG Index Page

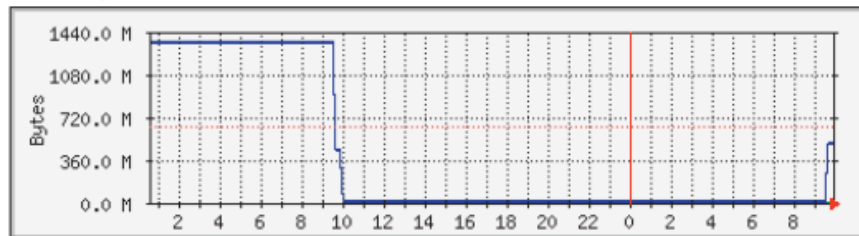
Traffic Analysis for 2 -- free.flag.com.tw



CPU utilization for HOST SERVERTYPE



Memory Statistics for HOST SERVERTYPE



Online Users

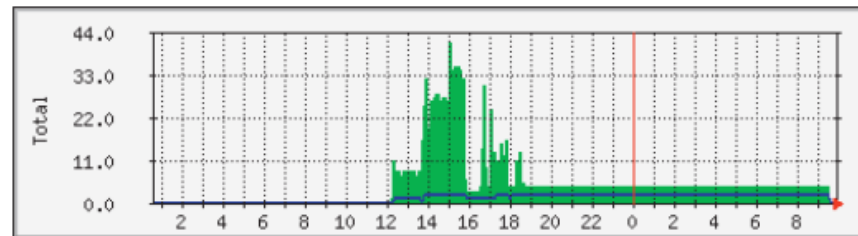


圖 15-2 MRTG 網管軟體使用 SNMP 協定收集並記錄各設備的狀態

網路監控通訊協定—SNMP 與 RMON

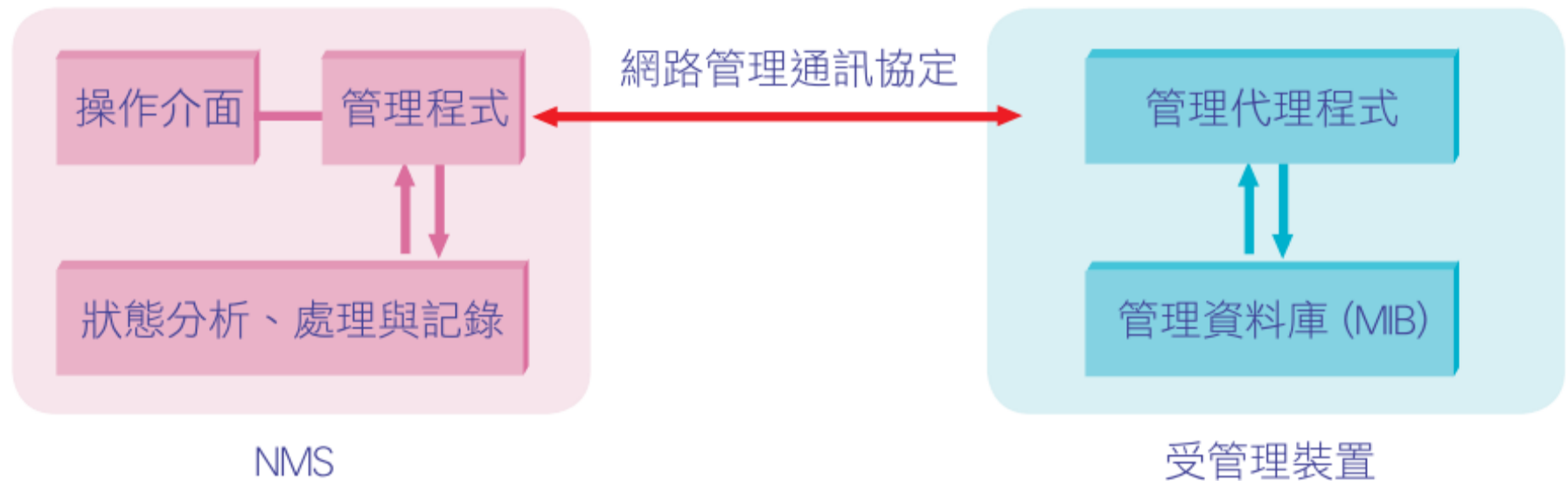


圖 15-3 SNMP 通訊協定運作架構

網路監控通訊協定—SNMP 與 RMON

◆ RMON 管理資料庫

RMON 制定出一組標準的 MIB, 讓所有的網路設備與管理站皆能互通, 規格中還增列了許多有用的網路傳輸狀態資訊

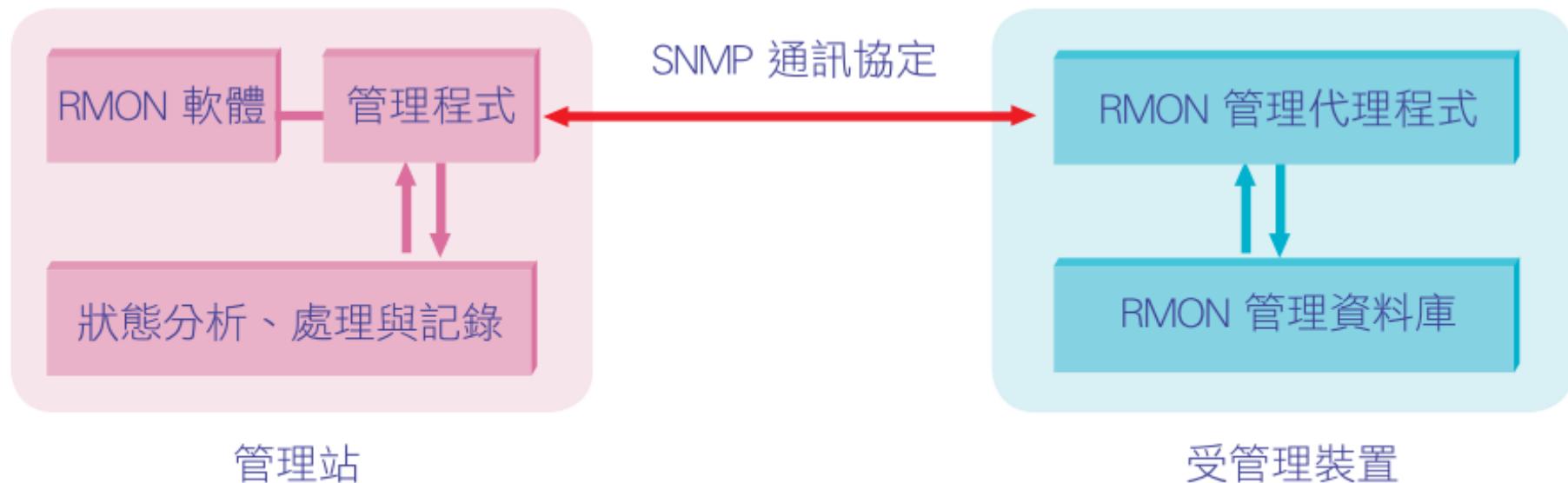


圖 15-4 RMON 運作架構

15-2 帳號與權限管理

『讓必要的人員存取相關的資源, 將不相干的人員排除在外』是確保網路安全的執行方針

◆ 共享層級 (Share Level) 的管理方式



圖 15-5 透過密碼來管理分享資源

帳號與權限管理

◆ 使用者層級 (User Level) 的管理方式



C:\F9453

JJones 帳號可以讀取此資料夾的檔案

Alice 帳號可以讀取並修改此資料夾的檔案

Publish1 帳號可以讀取並修改此資料夾的檔案

圖 15-6 每個共享資源都可以依據帳號賦予不同的存取權限

帳號與權限管理

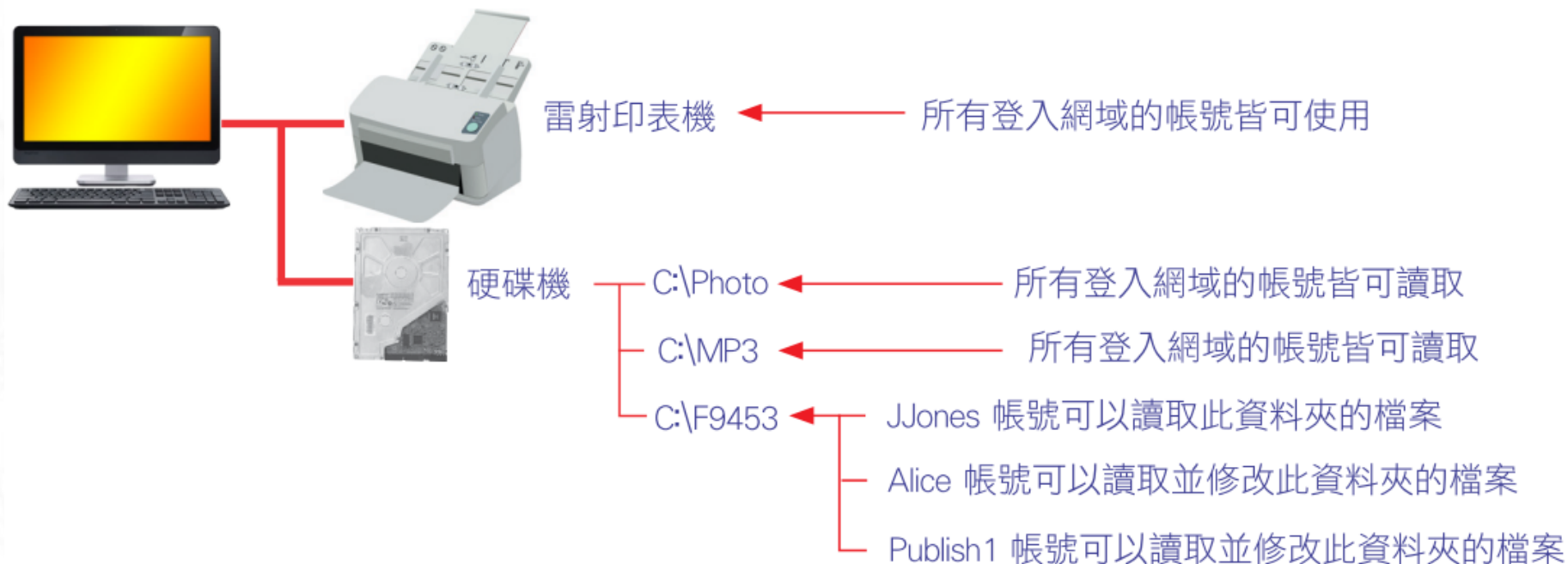


圖 15-7 Windows 作業系統透過帳號來設定資源存取權限

15-3 資料加密與解密

- ◆ 15-3-1 資料安全機制的目標
- ◆ 15-3-2 不可還原的編碼函數
- ◆ 15-3-3 對稱金鑰加解密函數
- ◆ 15-3-4 非對稱金鑰加解密函數
- ◆ 15-3-5 雜湊函數

15-3-1 資料安全機制的目標

1. 完整無誤 (Integrity)

確認從網路收到的資料是正確的, 途中沒有被篡改或變造。

2. 身分驗證 (Authentication)

確認資料發送者的身分, 使發送者無法假冒他人身分發送資料。

3. 不可否認 (Nonrepudiation)

使發送者無法否認這份資料是他所發出的。

4. 資訊保密 (Confidentiality)

確保資料在網路上傳遞時不會被他人竊知內容。

15-3-2 不可還原的編碼函數

- ◆ 若不想在傳輸途中洩密, 則最好將資訊經過編碼處理, 產生另一段編碼過的資訊。

表 15-1 最簡單的編碼函數對照表

加密編碼程序	解密編碼程序
A → Z	Z → A
B → W	W → B
C → X	X → C
D → E	E → D
K → H	H → K

不可還原的編碼函數

- ◆ 編碼函數所產生的編碼資料與原始資料的



圖 15-8 不可還原編碼函數的保護威力

不可還原的編碼函數

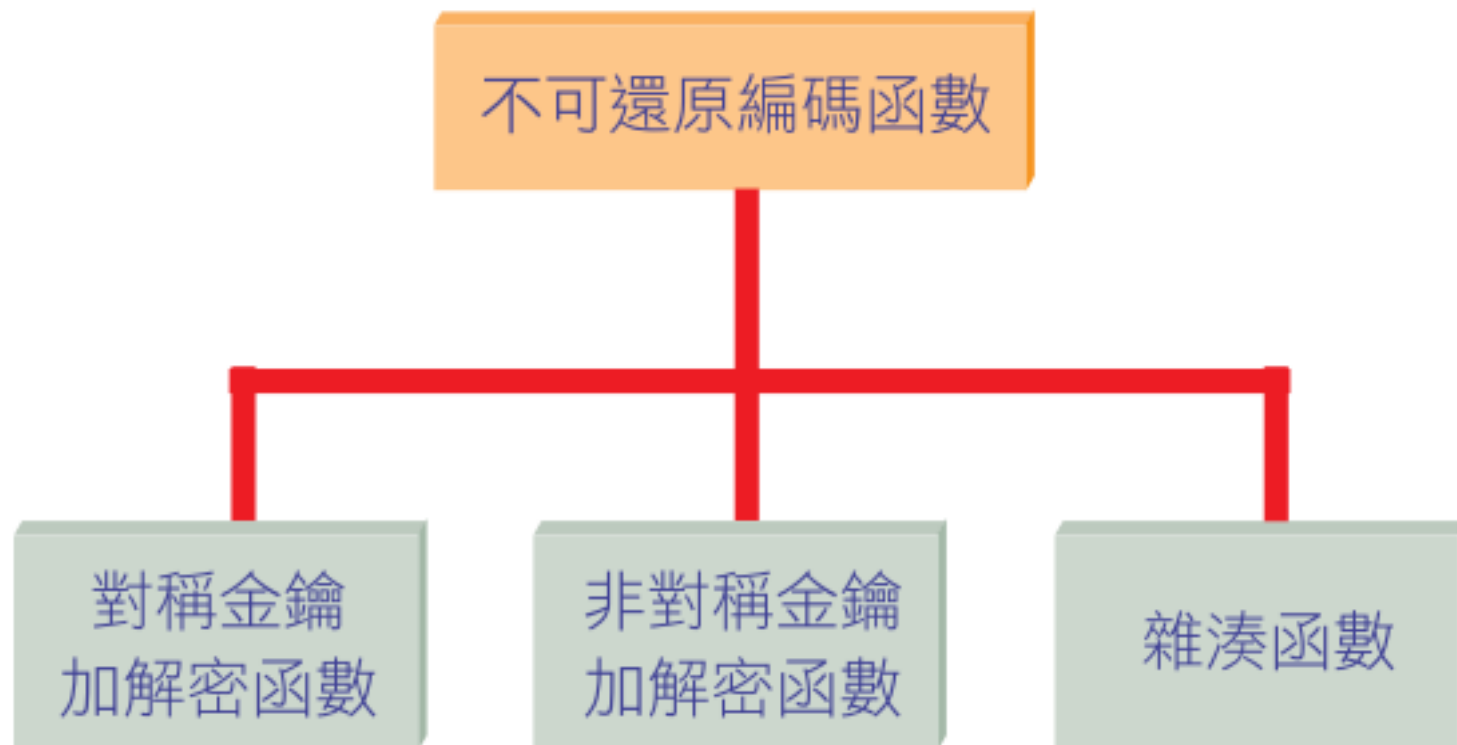
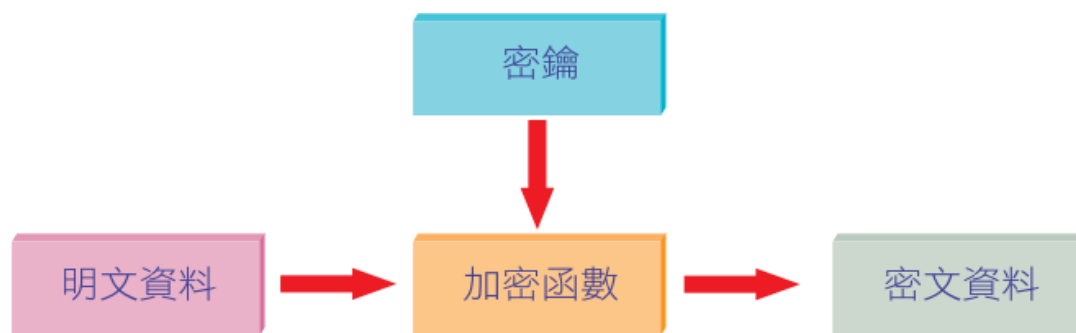


圖 15-9 不可還原編碼函數的發展

15-3-3 對稱金鑰加解密函數

- ◆ 利用相同的密鑰與加解密函數, 以執行加密與解密的動作

加密：



解密：

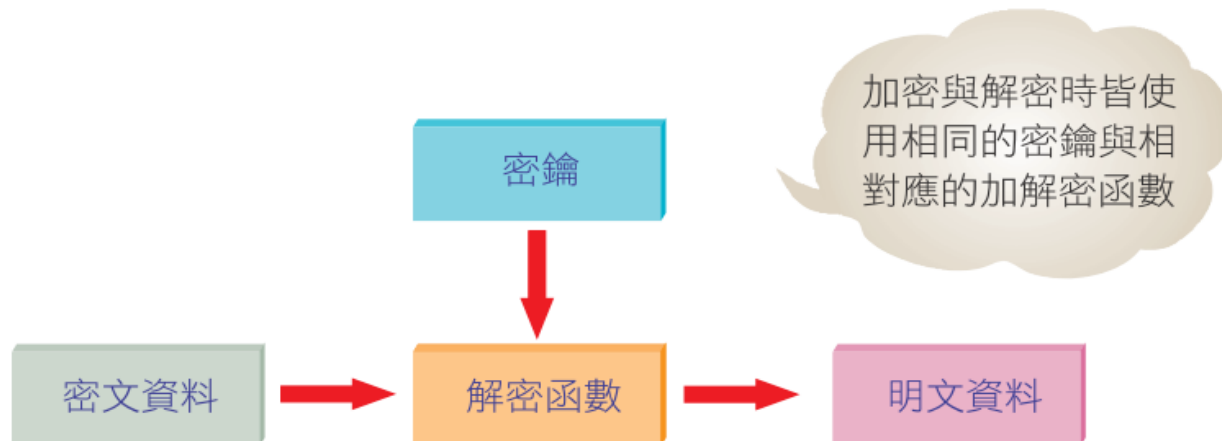


圖 15-10 對稱式加解密系統的原理

對稱金鑰加解密函數

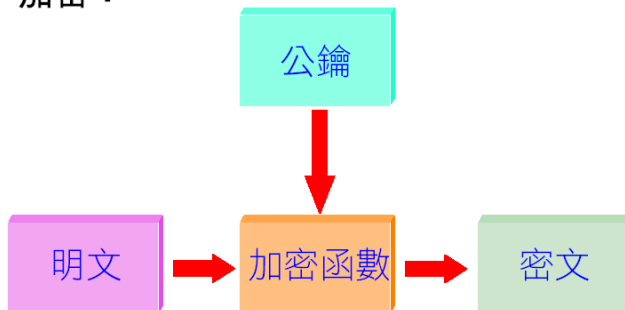
- ◆ A、B 兩位使用者各自擁有一把相同的 K 密鑰, 且 A、B 互信對方不會將 K 密鑰分送給他人。
- ◆ A 利用 K 密鑰將一段明文文字加密為加密文字, 然後將加密文字送給尚未驗證身份的 X 使用者。若 X 可用 K 密鑰將加密文字解密為明文文字, 則 A 即可相信 X 就是 B。

15-3-4 非對稱金鑰加解密函數

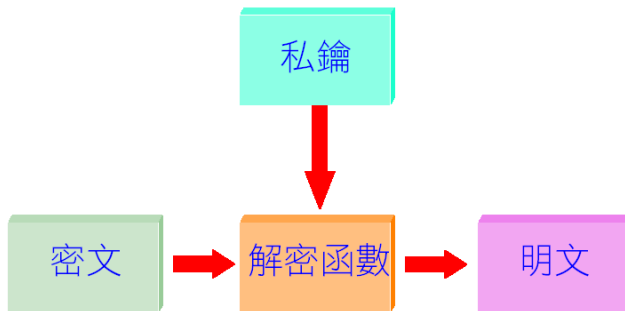
- ◆ 利用不同的公鑰 (Public Key) 與私鑰 (Private Key) 搭配加解密函數, 以執行加密與解密的動作。
- ◆ 用私鑰加密是為了確認身分；用公鑰加密則是為了保密

15-3-4 非對稱金鑰加解密函數

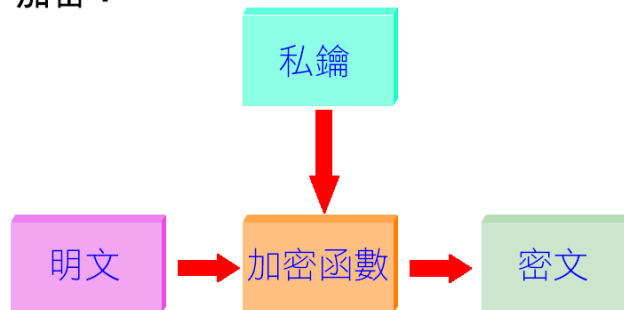
加密：



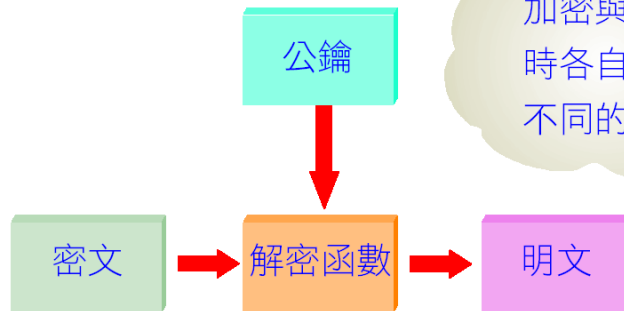
解密：



加密：



解密：



加密與解密
時各自使用
不同的金鑰

圖 15-11 非對稱式加解密系統的原理

15-3-5 雜湊函數

- ◆ 雜湊函數主要用來產生雜湊值 (Hash Value)



圖 15-12 雜湊函數的運作架構

雜湊函數

- ◆ 輸入雜湊函數的資料沒有長度的限制。
- ◆ 雜湊值的長度固定。
- ◆ 雜湊函數的運算不會太複雜, 亦即電腦在執行時不會耗費太多 **CPU** 資源。
- ◆ 雜湊函數具有單向特性, 因此實務上無法利用雜湊值來求出輸入的原始資料。
- ◆ 即使輸入的資料僅有一個位元不同, 產生的雜湊值卻會有很大的差異。

15-4 數位簽章

- ◆ 15-4-1 數位簽章的產生流程
- ◆ 15-4-2 數位簽章與電子簽章的差異

Networking
Essentials

15th Edition

15-4-1 數位簽章的產生流程

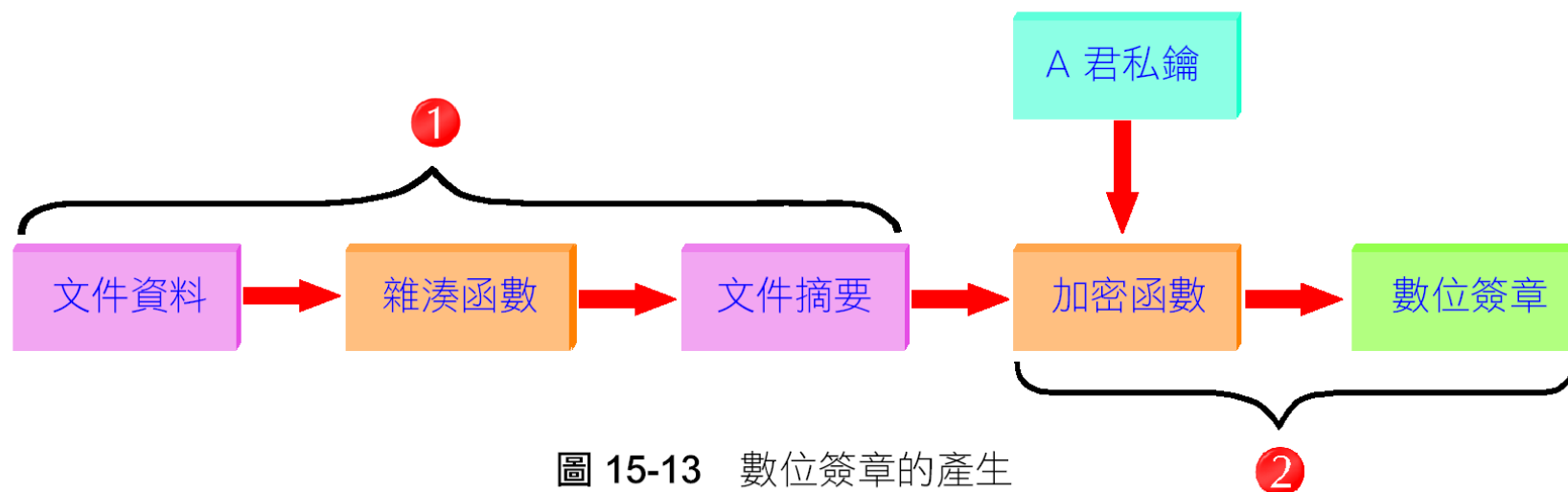


圖 15-13 數位簽章的產生

數位簽章的產生流程

- ① 首先將電子文件經過雜湊函數處理, 產生一份文件摘要 (也就是 15-3-5 節所指的雜湊值)。
- ② 再以傳送者的私鑰對摘要加密, 所產生的結果便是數位簽章。

數位簽章的產生流程

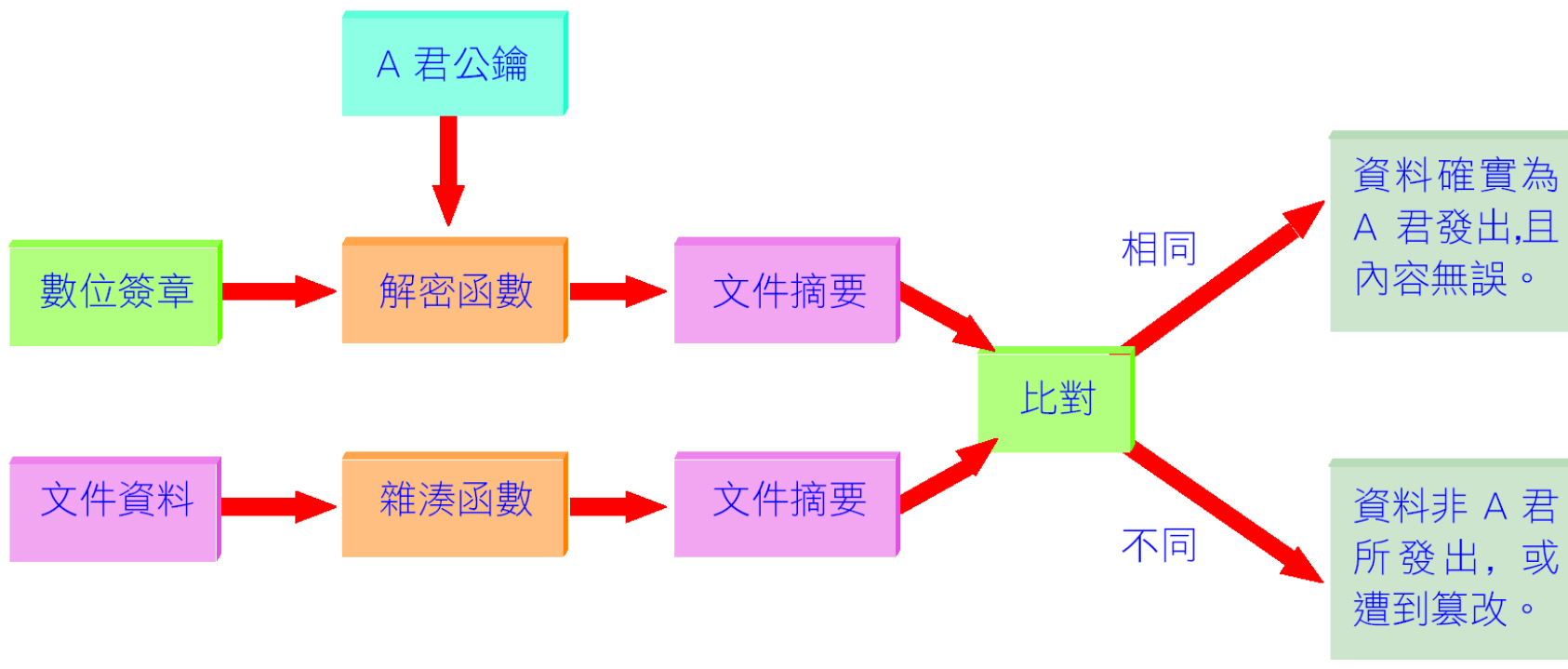


圖 15-14 接收端以數位簽章驗證身分與文件內容的流程

數位簽章的產生流程

- ◆ 發送者根本不是 A 君, 所以用 A 君的公鑰解密(編碼) 而得的 D1 不是正確的摘要。
- ◆ 文件資料遭竄改, 以致於 D2 並非正確的摘要。

Networking
Essentials

15th Edition

15-4-2 數位簽章與電子簽章的差異

◆ 數位簽章 (Digital Signature)

指對於電子文件以數學或其他方式, 轉換為特定長度的數位資料 (也就是前文所述的『文件摘要』), 再以簽署人私鑰對該資料加密而形成數位簽章, 並得以簽署人公鑰加以驗證者。

◆ 電子簽章 (Electronic Signature)

則包括了數位簽章, 及使用指紋、聲紋、視網膜、DNA、靜脈紋路等等生物辨識技術所製作的資料。

數位簽章與電子簽章的差異

1. 電子簽章必須依附在電子文件上。
2. 必須能利用電子簽章辨識簽署人的身分。
3. 必須能利用電子簽章辨識電子文件的真偽。

Networking
Essentials

15th Edition

15-5 公開金鑰基礎建設 (PKI)

- ◆ 15-5-1 公鑰憑證
- ◆ 15-5-2 政府 PKI 的架構與發展
- ◆ 15-5-3 民間 PKI 的發展

*Networking
Essentials*

15th Edition

公開金鑰基礎建設 (PKI)

- ◆ 既然可以將公鑰公布給大眾知道, 那麼應該將公鑰存放在哪部電腦? 又該透過什麼管道公布呢? 難道得自己架設一部 24 小時不關機的網站, 並在各大媒體刊登廣告, 通知大家來下載嗎?
- ◆ 如何防止某乙以自己的公鑰冒充某甲的公鑰? 如果多個網站都有某甲的公鑰, 如何辨識哪一把才是正牌的公鑰?

15-5-1 公鑰憑證

- ◆ 在實作上, 發鑰機構在發布公鑰時, 為了防止偽造, 會將公鑰與申請人姓名、發放日期、序號、有效期限、發鑰機構名稱和發鑰機構的數位簽章等等資訊整合在一起, 成為一份公鑰憑證 (Public Key Certificate), 又稱為數位憑證 (Digital Certificate), 通常簡稱為憑證 (Certificate)。

15-5-2 政府 PKI 的架構與發展

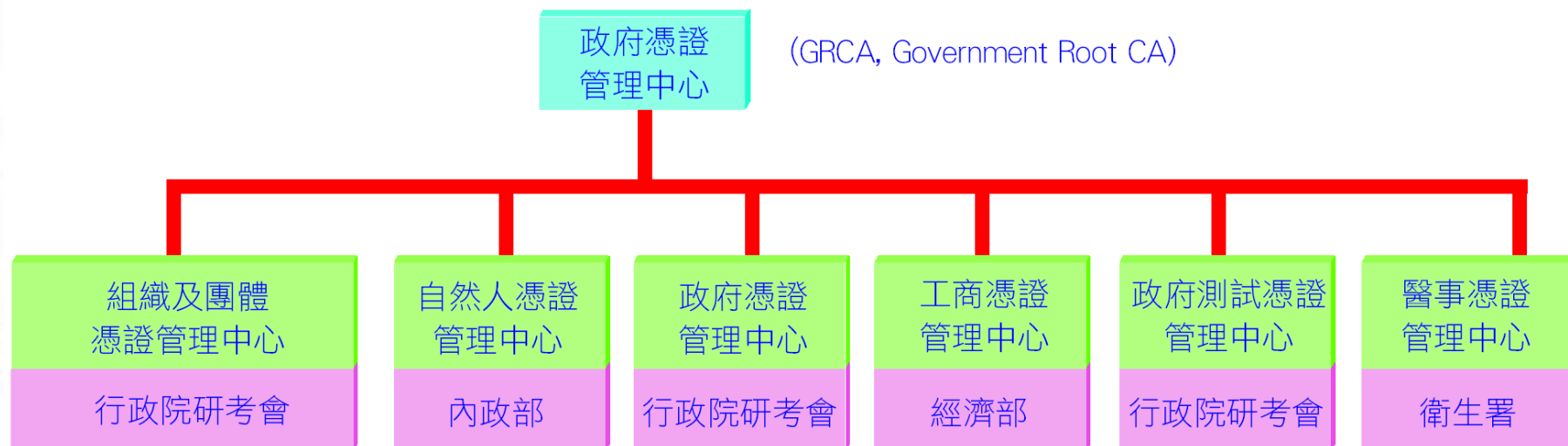


圖 15-15 政府機關公開金鑰基礎建設 (GPKI, Government PKI)

政府 PKI 的架構與發展

要讓自然人憑證發揮功用, 必須具備兩項條件：

- ◆ 一是有讀卡機
- ◆ 二是能上網



圖 15-16

(上圖) 自然人憑證及使用手冊
(下圖) 自然人憑證需插入支援晶片卡的讀卡機中使用

政府 PKI 的架構與發展



MOICA內政部憑證管理

moica.nat.gov.tw/link_1.html

內政部憑證管理中心

訪客

首頁 > 應用服務 > 應用系統網站連結

應用服務 Service

- ▶ 應用系統網站連結
- ▶ Hisecure程式開發套件
- ▶ 身分確認服務申請
- ▶ API問題/障礙申告
- ▶ 人次登錄系統
- ▶ 回首頁

應用系統網站連結

有了自然人憑證，您就可利用網路享受目前各政府機關所提供的自然人憑證應用服務系統，【少用馬路，多用網路】的便捷性與高安全性。未來將配合電子化政府提供更多項的網路服務，詳細內容，請參閱各政府機關網站說明。

應用服務名稱	主管機關
全民健康保險個人健保資料網路服務作業	衛生福利部中央健康保險署
健康存摺-下載個人就醫資訊	衛生福利部中央健康保險署
食品業者登錄平台	食品藥物管理署
臺中市政府服務e櫃台	臺中市政府
測繪圖資整合資料查詢申購入口網	內政部國土測繪中心
財政部稅務入口網	財政部

圖 15-17 目前自然人憑證所能應用的服務, 都可以從這個網頁連結過去

15-5-3 民間 PKI 的發展

- ◆ 基本上,台灣民間 PKI 業者的發展是呈現『多頭馬車』的局面。各自引進國外不同的技術核發不同的憑證,而這些憑證彼此互不相容。
- ◆ 換言之, A 憑證管理中心核發的憑證,不能用於 B 憑證管理中心；而 B 憑證管理中心所核發的憑證,也不被 A 憑證管理中心所承認。

15-6 防火牆

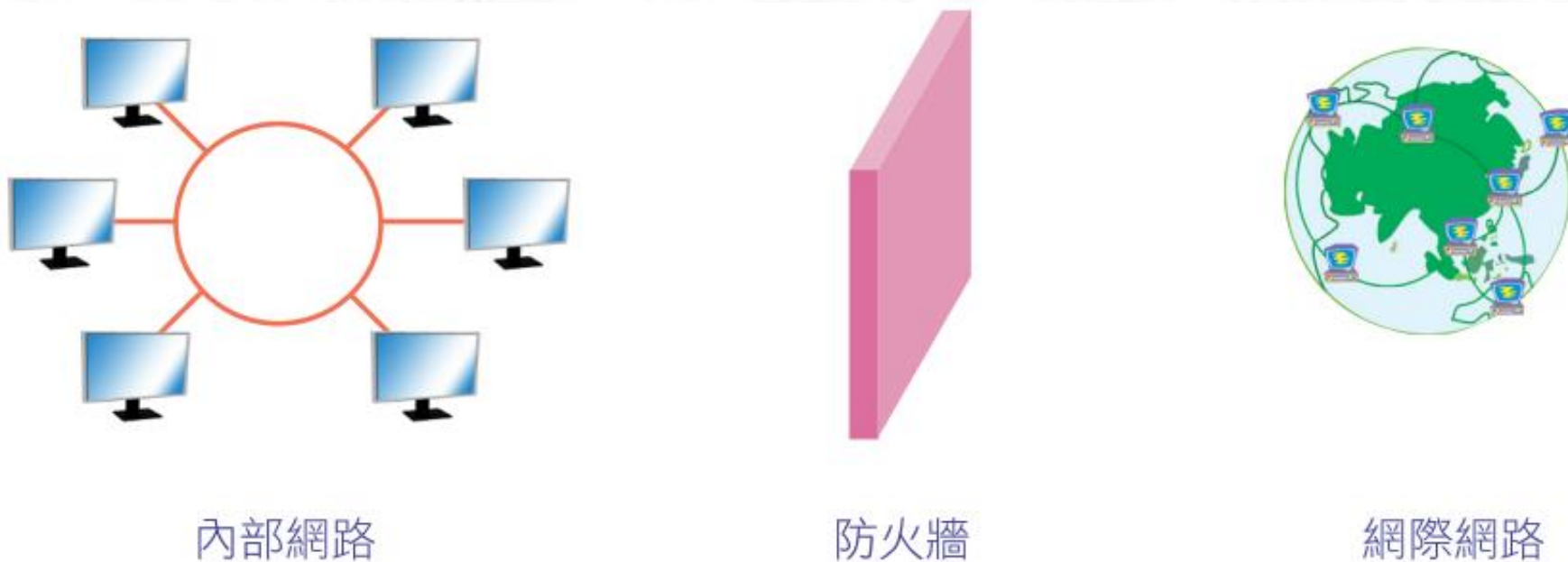


圖 15-18 防火牆將內部網路和網際網路分開, 以達到保護內部網路的目的

防火牆

◆ 封包過濾 (Packet Filter)

封包過濾防火牆運作於 TCP/IP 的網路層與傳輸層，可以針對 IP 位址、通訊埠號、TCP/UDP 協定等網路層與傳輸層屬性進行過濾。

應用層

表達層

交談層

傳輸層

網路層

鏈結層

實體層

圖 15-19 封包過濾型的防火牆主要在網路層及傳輸層運作；應用層過濾型及代理器防火牆則是在應用層運作

防火牆

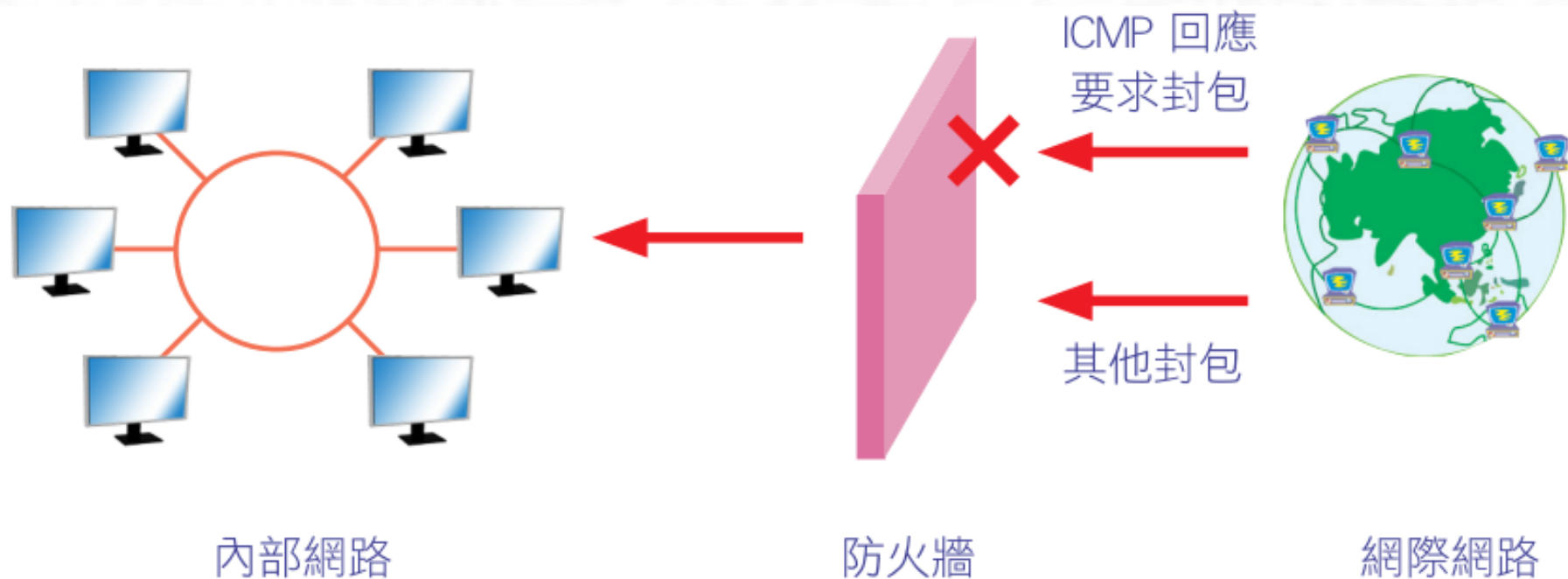


圖 15-20 使用封包過濾阻擋外部網路 ping 內部網路的主機

防火牆

◇ 應用層過濾 (Application Layer Filter)

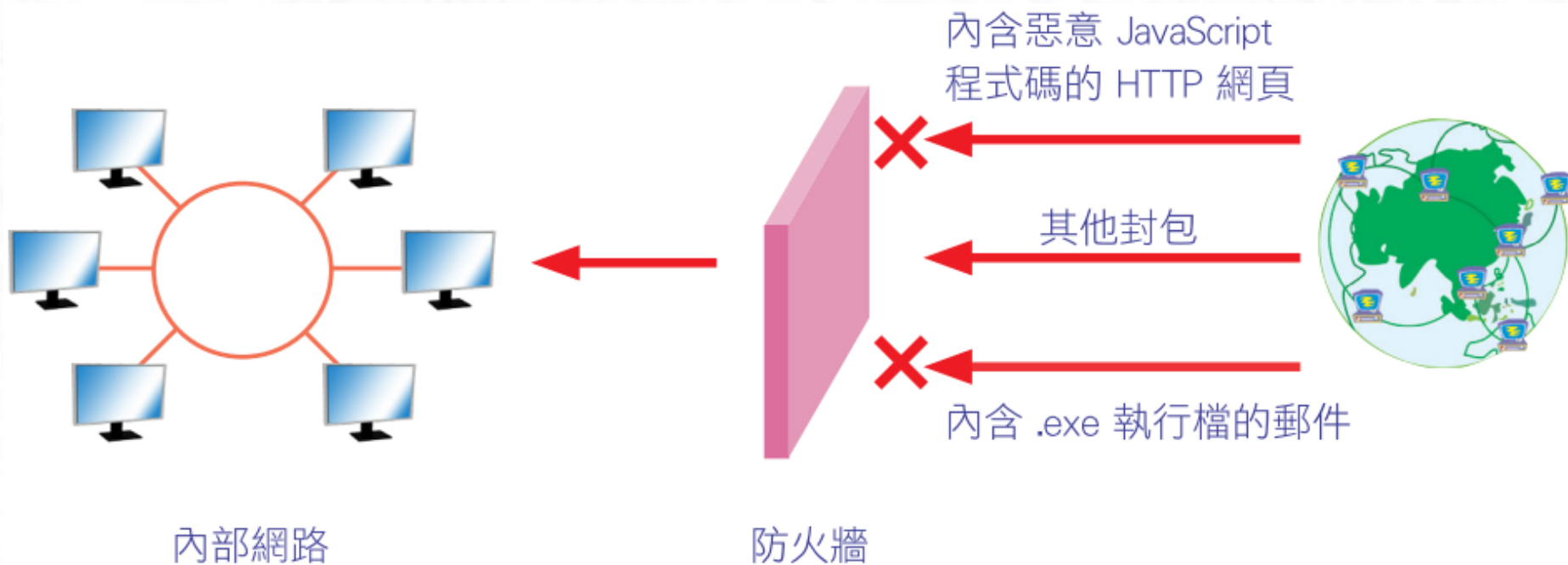


圖 15-21 應用層過濾防火牆

防火牆

- ◆ 代理器(Proxy)：代理器防火牆將內外網路完全隔絕,所有連線都必須透過代理器防火牆來完成。



圖 15-22 Windows 的 Proxy 設定

15-7 加強網路層的安全- IPsec

IPsec 協定包含了以下 3 種主要協定：

- ◆ ISAKMP (Internet Security Association and Key Management Protocol) 協定

主要用來決定加密與解密時所使用的密鑰 (Secret Key)。

- ◆ AH (Authentication Header) 協定

主要用來執行『身份驗證』與『完整性檢查』(Integrity Check) 兩項工作。

- ◆ ESP (Encapsulating Security Payload) 協定

主要用來執行『身份驗證』和『資料加密』兩項工作。

15-8 資訊安全管理

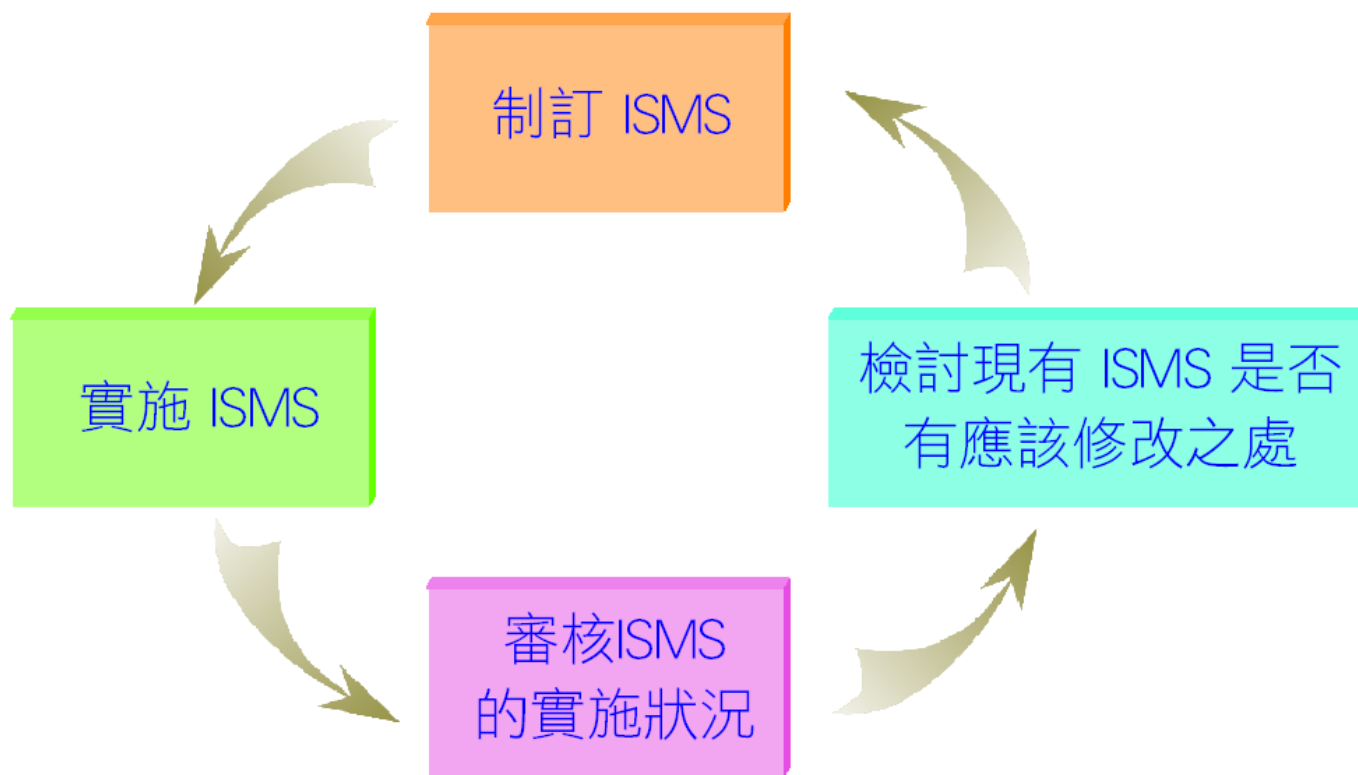


圖15-23

資訊安全管理

◆ BS 7799

- ◆ Part 1 : The Code of Practice For Information Security management
- ◆ Part 2 : Specification For Information Security Management System
- ◆ Part 3 : Guidelines for information security risk management

資訊安全管理

◆ ISO 27000 系列

- ◆ 最近幾年 ISO 組織推出了 ISO 27000 系列標準, 是資訊安全管理領域的專用標準, 因此爾後只要看到編號為 **27XXX** 的 ISO 標準, 便可以確定那是一個關於資安的國際標準。

資訊安全管理

◆ CNS 27002

- ◆ 台灣雖然是資訊產品的大國,可是在資安方面的起步晚,又無重量級的機構或廠商在推動資安標準,因此只能跟著國際的腳步前進。
- ◆ 行政院經濟部標準檢驗局便根據 ISO 17799 和 ISO 17800 制訂了CNS 17799『資訊安全管理之作業要點』和 CNS 17800『資訊安全管理系統規範』,可以說是將 ISO 版予以中文化,賦予了統一的中文名稱。

實作練習：Windows 10/7 的防火牆功能

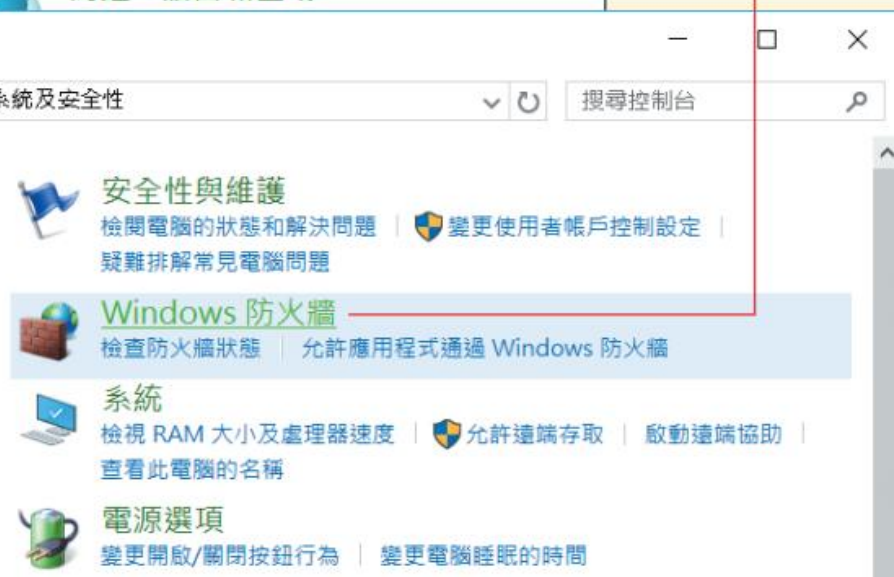
- ◆ 查看 Windows 防火牆狀態
- ◆ 查看與修改網路位置
- ◆ 防火牆的警告交談窗
- ◆ 修改例外清單

查看 Windows 防火牆狀態

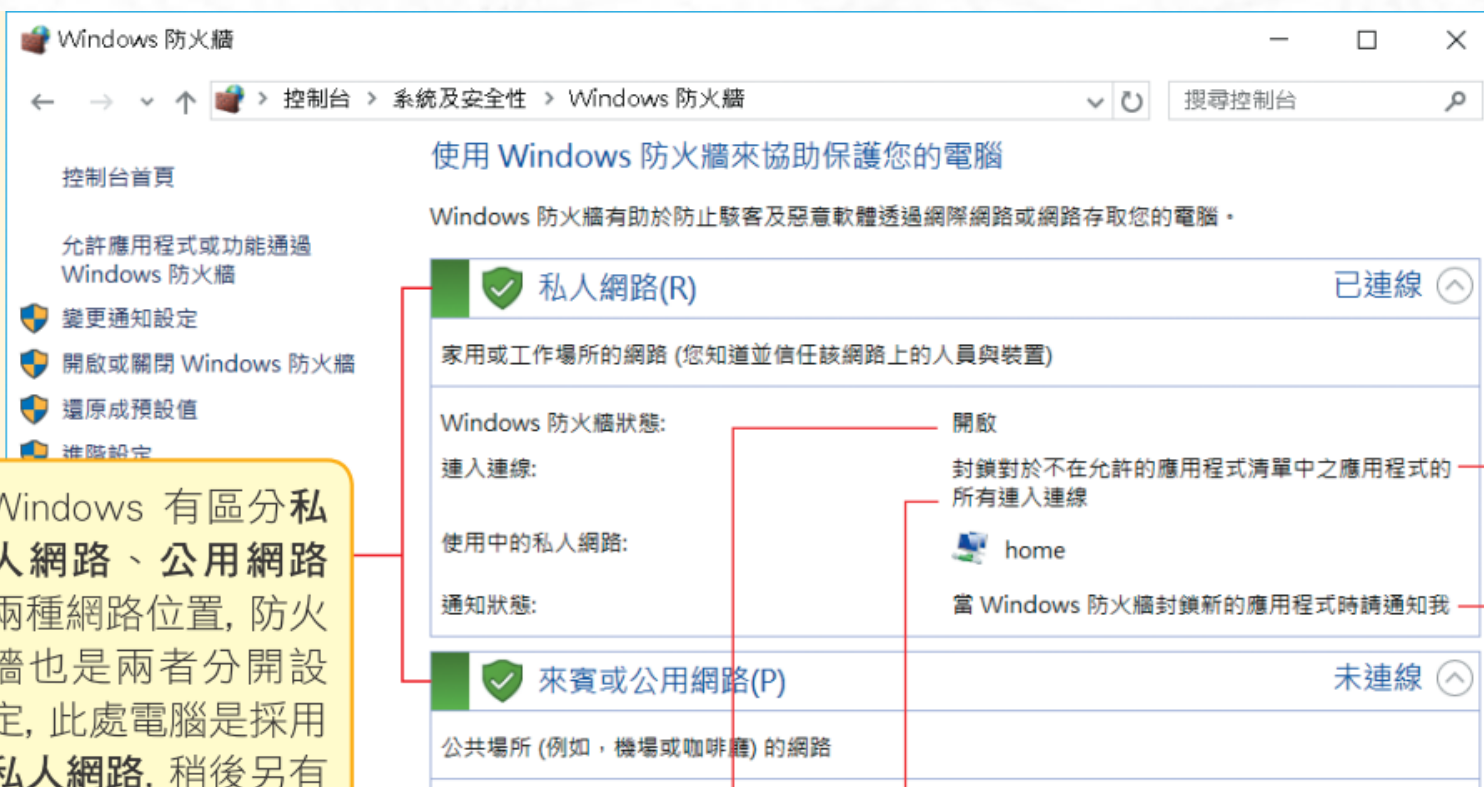
1 按系統及安全性項目



2 按 Windows 防火牆項目



查看 Windows 防火牆狀態



Windows 有區分**私人網路**、**公用網路**兩種網路位置, 防火牆也是兩者分開設定, 此處電腦是採用**私人網路**, 稍後另有詳細說明

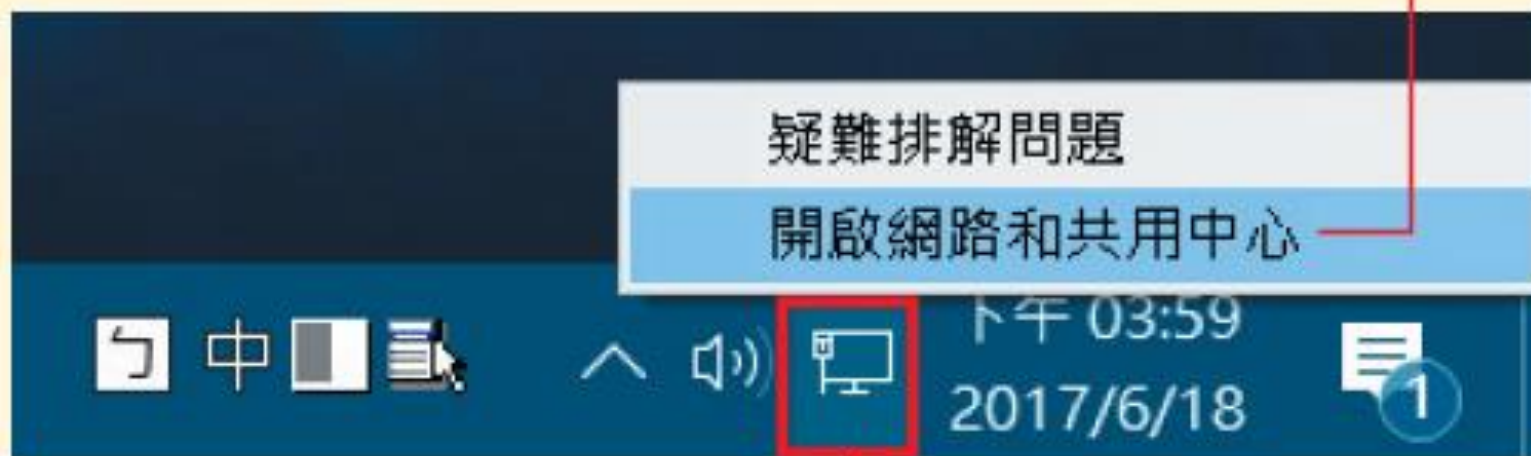
預設會封鎖所有的對內連線
當程式被封鎖時會顯示通知

防火牆功能已經開啟

使用中的網路

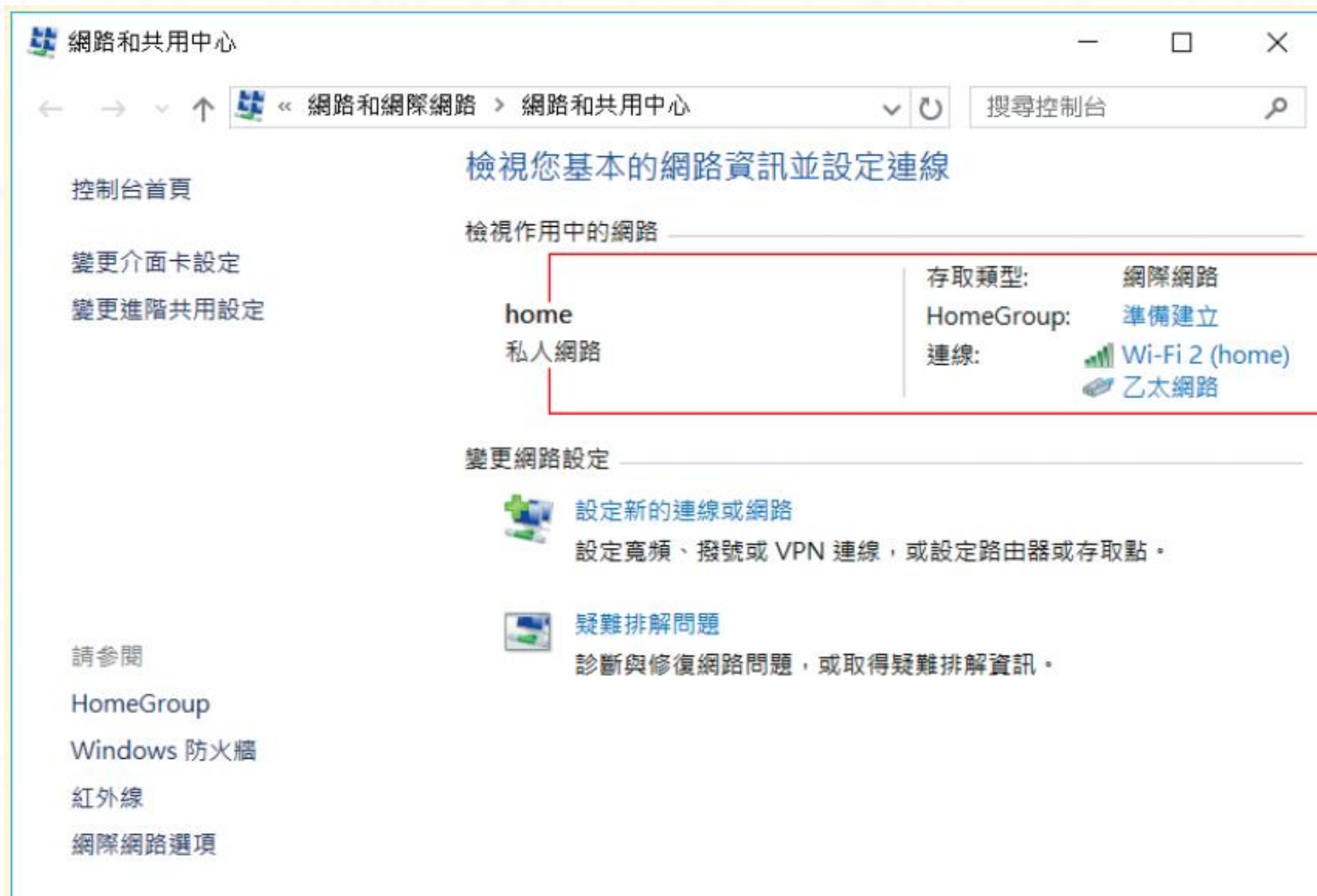
查看與修改網路位置

2 選擇此項開啟網路共用中心



1 在通知區域的網路圖示上按右鈕

查看與修改網路位置



此為網路名稱

此處會顯示目前的網路位置設定

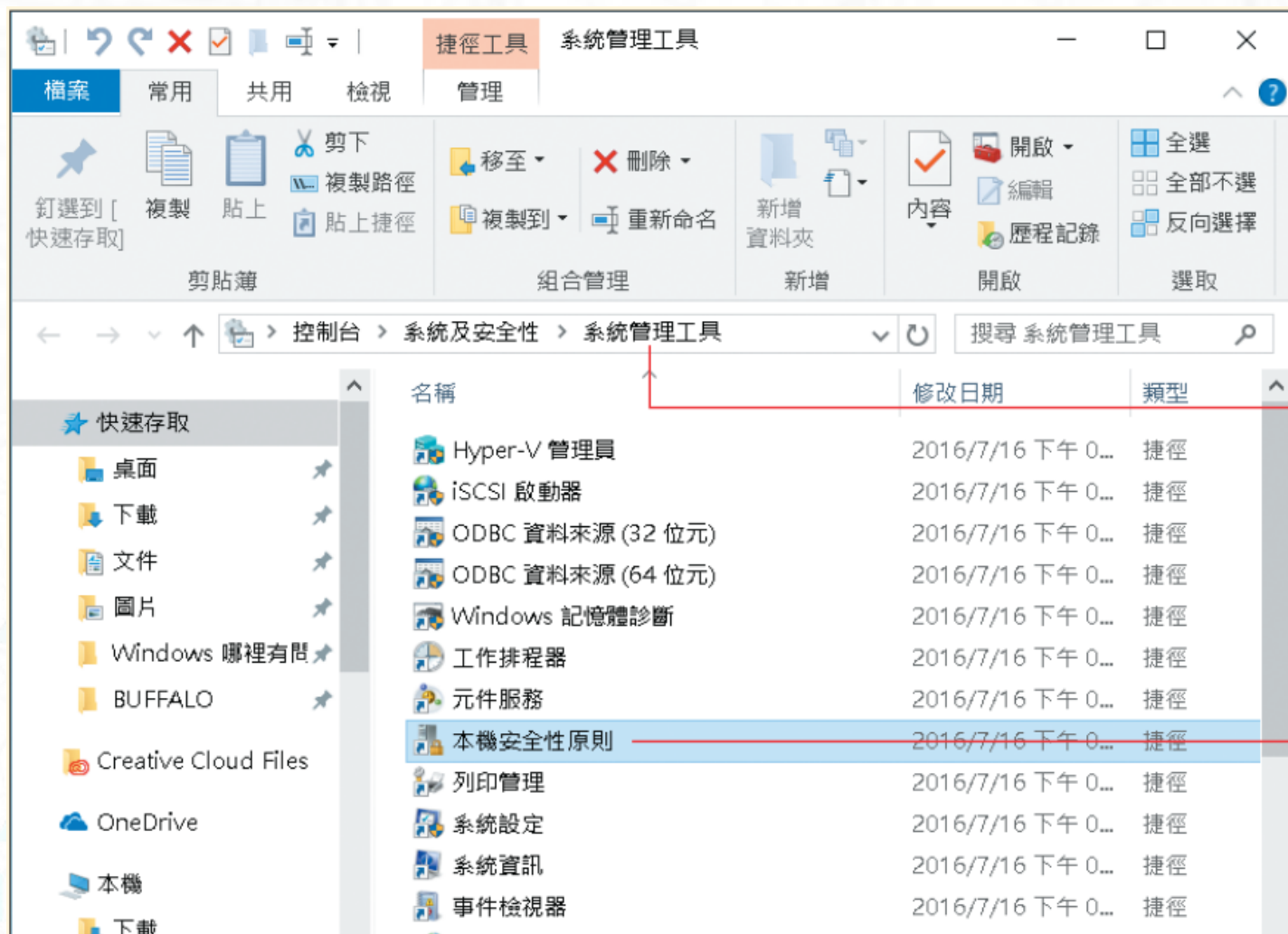
查看與修改網路位置

網路位置	網路探索功能	連出連線	連入連線
私人網路	開啟	放行	僅開放核心網路功能
公用網路	關閉	放行	僅開放核心網路功能

Networking
Essentials

15th Edition

查看與修改網路位置

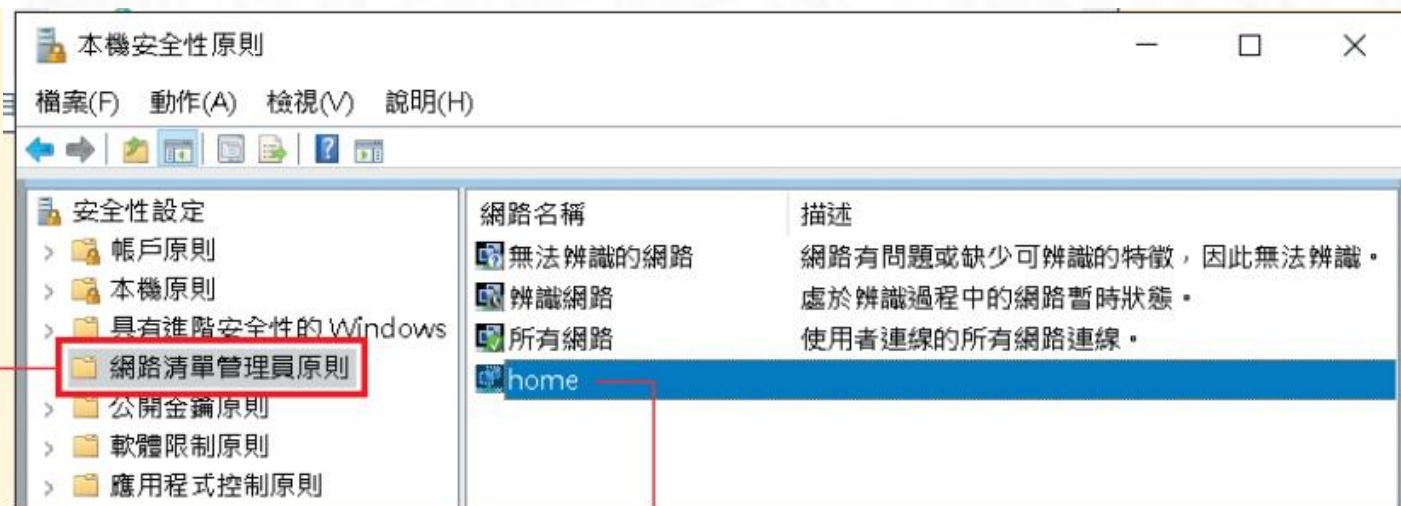


1 開啟『控制台 / 系統與安全性 / 系統管理工具』

2 選擇本機安全性原則

查看與修改網路位置

3 在左邊選擇網路清單管理員原則



4 在右邊雙按目前連線的網路名稱

Essentials
15th Edition

查看與修改網路位置

The screenshot shows the 'Network Location' tab in the Windows Network and Sharing Center. The window title is 'home - 內容'. The 'Network Location' tab is selected and highlighted with a red box, with a red line pointing to it from the annotation '5 切換到網路位置頁次'. Below the tabs, there is a descriptive text: '網路位置可識別電腦所連線的網路類型，並且可自動為該位置設定適當的防火牆設定。'. There are two main sections: '位置類型' (Location Type) and '使用者權限' (User Permissions). In the '位置類型' section, the '公用(P)' (Public) radio button is selected and highlighted with a red box, with a red line pointing to it from the annotation '6 選擇要切換的網路位置'. In the '使用者權限' section, the '使用者不可以變更位置(S)' (Users cannot change this location's settings) radio button is selected. At the bottom, the '確定' (OK) button is highlighted with a red box, with a red line pointing to it from the annotation '7 按此鈕確認即可'. The other buttons are '取消' (Cancel) and '套用(A)' (Apply).

home - 內容

網路名稱 網路圖示 **網路位置**

網路位置可識別電腦所連線的網路類型，並且可自動為該位置設定適當的防火牆設定。

位置類型

- ☐ 尚未設定(N)
- ☐ 私人(R)
- ☒ **公用(P)**

使用者權限

- ☐ 尚未設定(O)
- ☐ 使用者可以變更位置(U)
- ☒ 使用者不可以變更位置(S)

確定 取消 套用(A)

5 切換到網路位置頁次

6 選擇要切換的網路位置

7 按此鈕確認即可

防火牆的警告交談窗

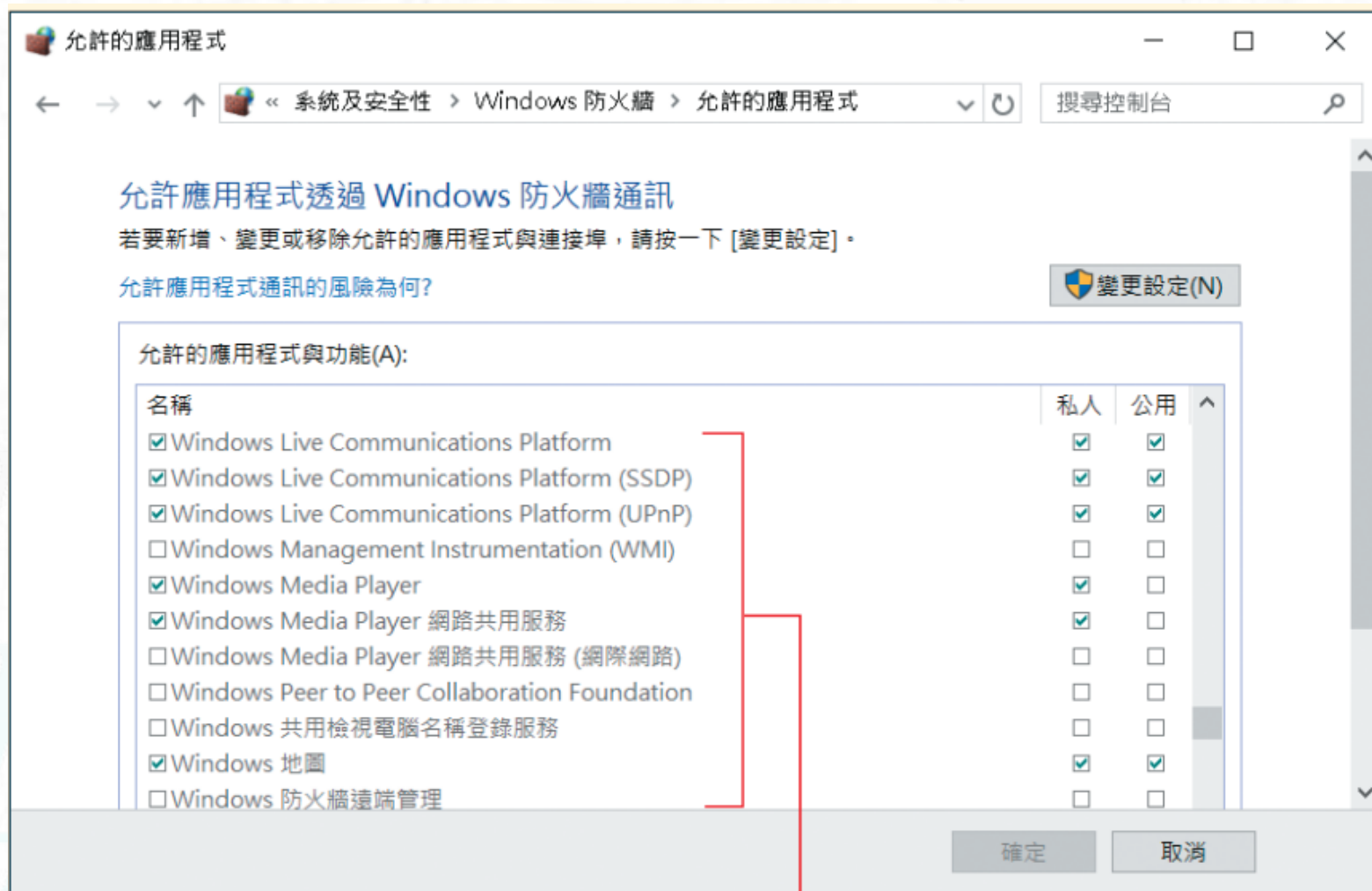


防火牆的警告交談窗

1 按允許程式通過 Windows 防火牆項目



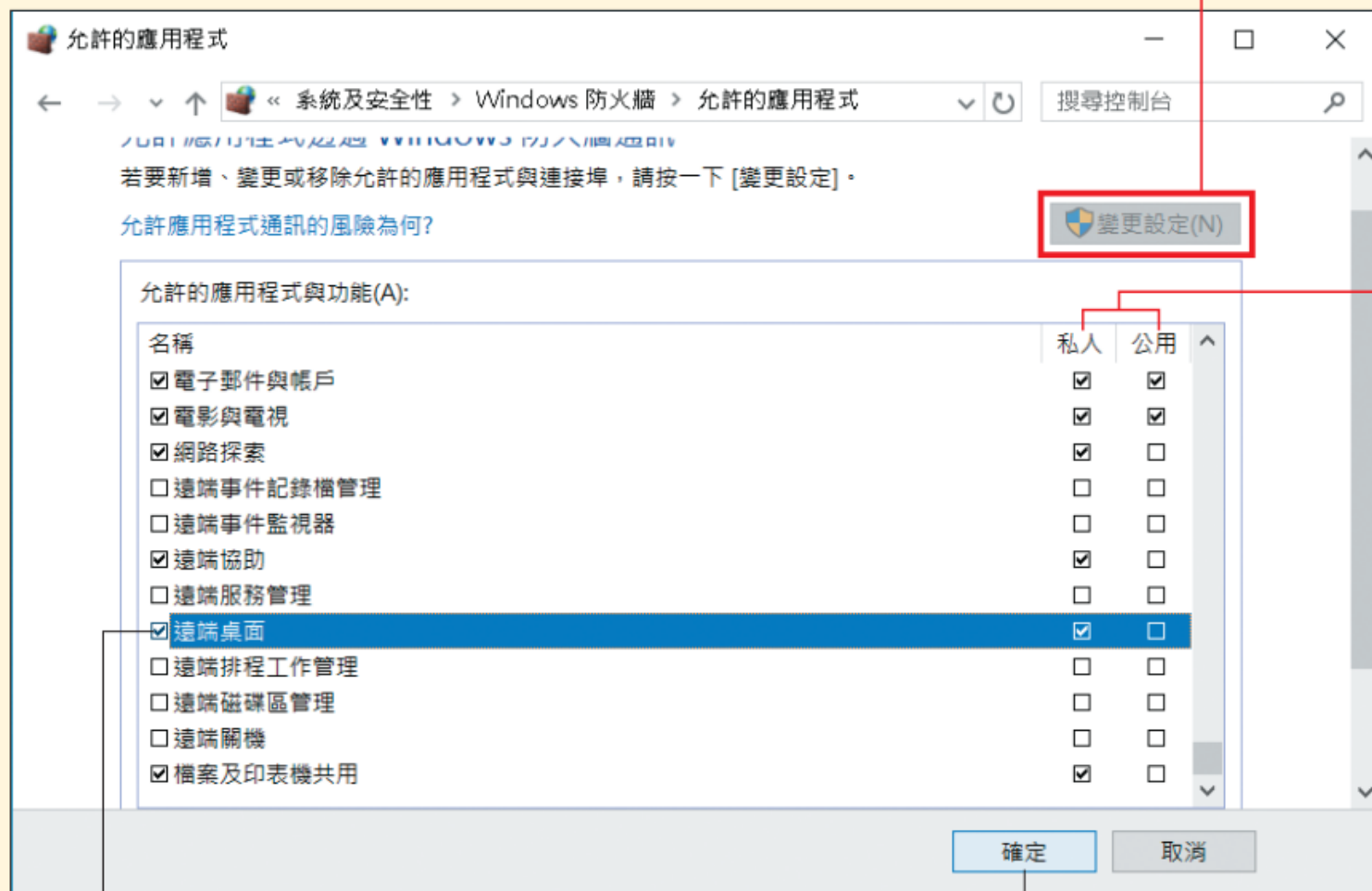
防火牆的警告交談窗



允許通過防火牆的程式會出現在
此例外清單中 (有打勾的才允許)

修改例外清單

1 先按此鈕



此處允許連線的
程式, 私人網路、
公用網路同樣可
以分開設定

2 勾選代表允許遠端桌面

3 按確定鈕即完成設定