圖 1-1 攻擊目的的變化

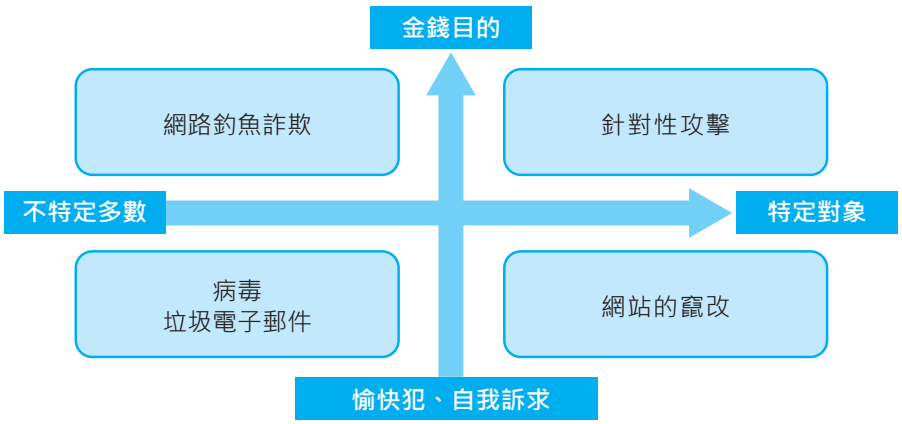
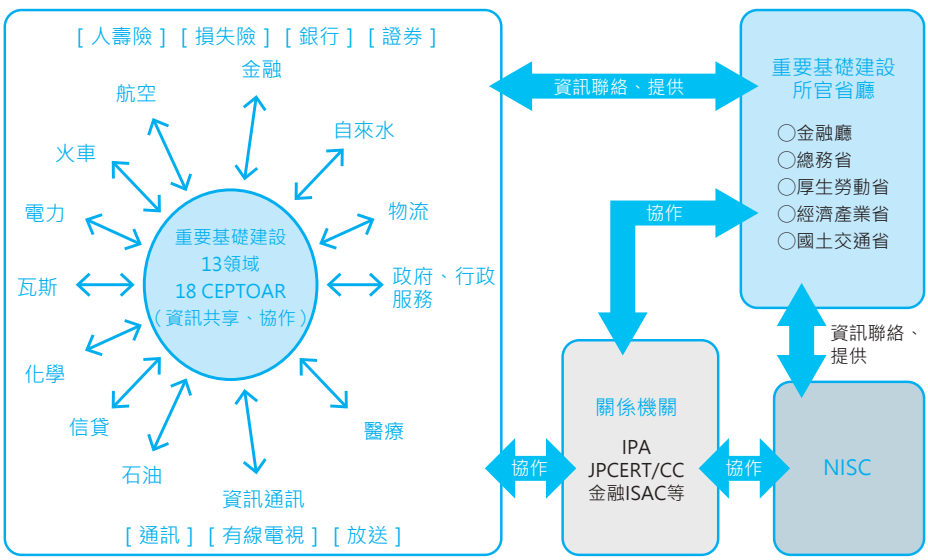


圖 1-2 重要基礎建設之安全體制



出處：內閣網路安全中心（NISC）「2017年度跨領域演習」（URL：https://www.nisc.go.jp/conference/cs/ciip/dai11/pdf/11shiryou03.pdf）

Point

- 瞭解攻擊者的目的，找出該保護的對象並實施對策
- 應該清楚認識到自己的公司或自己本身都是會遭受攻擊的對象
- 對網路恐怖主義的影響程度有所理解

» 資訊安全三要素

資訊安全的 CIA（三要素）

在與資訊安全管理系統（ISMS）相關之國際標準的日文版 JIS Q 27000 之中，是將「資訊安全」定義為「維持資訊的**機密性**（Confidentiality）、**完整性**（Integrity）及**可用性**（Availability）一事」，取其開頭字母，有時也會被稱作**資訊安全的 CIA**。

經授權者才可使用的「機密性」

被設計成只有經過授權者才可使用，這樣的方式可說是具有很高的「機密性」。在這裡，經授權「者」並不侷限於人而已。對於像電腦等裝置，也需要給予適度的**存取授權**（**權限**）（**圖 1-10**）。

將內容維持為正確狀態的「完整性」

未經竄改或破壞，內容處於正確的狀態，便稱為保有「完整性」。檔案的內容是否未經不當改寫、經由網路等傳輸之中資訊並沒有遺失等，這些都需要被證明（**圖 1-11**）。

不容易受到故障影響的「可用性」

不容易發生故障、即便發生故障也可將影響減輕到最低、恢復正常所需時間很短等，便稱為「高可用性」。就算機密性及完整性維持得很好，但系統本身無法使用也沒有意義。一旦遭到網路攻擊而導致**系統停止便會降低可用性**，所以必須想辦法避免，以便維持系統隨時都可使用的狀態（**圖 1-12**）。

圖 1-10 維持機密性的案例

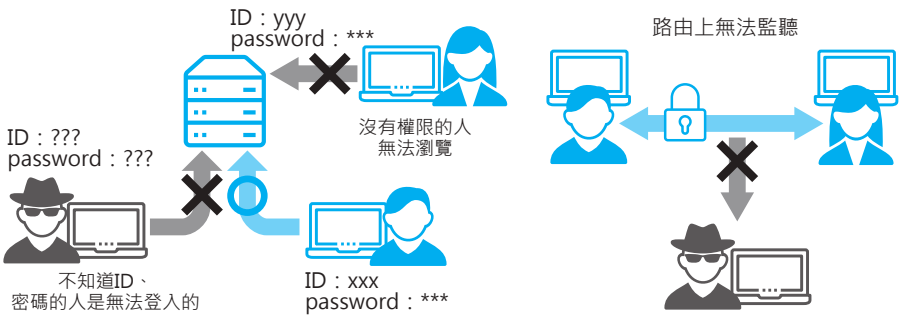


圖 1-11 完整性遭到損壞的案例

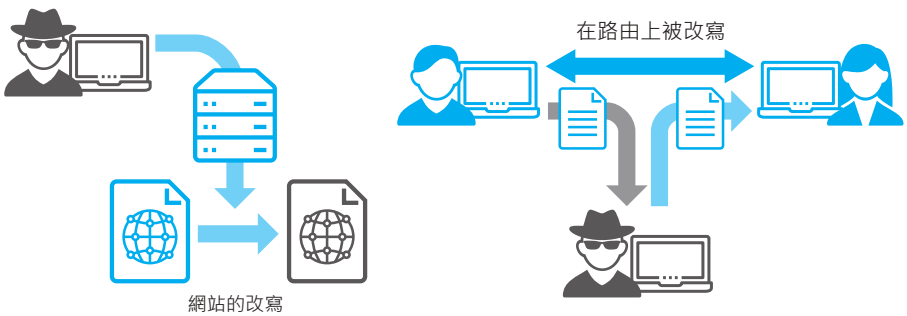
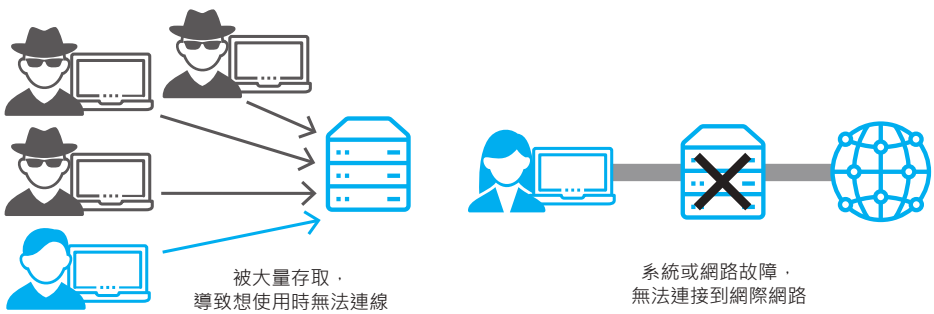


圖 1-12 可用性較低的案例



Point

- 此三要素若無法全數維護，就資訊安全而言可說是有所不足，容易產生風險的狀況
- 依據這三要素來進行檢視，便可徹底地實施對策

» 添加負荷類型的攻擊

藉由大量的通訊來讓網路癱瘓的攻擊

藉由讓大量的通訊暫時產生，以造成對象網路癱瘓的攻擊，被稱為 **DoS**（Denial of Service）**攻擊**或**阻斷服務攻擊**。各位可以想像成「有太多的惡作劇騷擾電話，而使得必要的電話沒辦法被接聽到的狀態」應該會比較容易理解。

如網路伺服器這樣對外部公開的情況，不論其規模大小都會成為攻擊的對象。DoS 攻擊是來自一台電腦的攻擊，而多台的電腦對一台電腦進行攻擊的則稱為 **DDoS**（Distributed Denial of Service）**攻擊**。

若是屬於 DoS 攻擊，只需要對來自該電腦的通訊加以阻擋即可；至於 DDoS 攻擊，由於是來自多台的電腦，一一加以阻擋實在不是一個很實際的作法。

透過電腦劫持來發動 DDoS 攻擊

發動 DDoS 攻擊需要很多台的電腦，所以攻擊者除了自己準備這些電腦之外，還有劫持他人電腦來予以濫用的方法存在。遭到病毒等感染，而變得可藉由來自外部透過網際網路的指令以進行操控狀態的電腦，稱之為**機器人**（**Bot**），而這些可被操控的電腦的集合，則稱為**殭屍網路**（**Botnet**）（**圖 2-16**）。使用者可能會在沒有察覺的情況下被加入殭屍網路，**不知不覺間成為加害者**。

以大量的電子郵件塞滿收件匣的「電子郵件炸彈」

電子郵件炸彈是屬於垃圾電子郵件的一種，意指傳送大量的電子郵件以耗盡電子郵件信箱的容量（**圖 2-17**）。因垃圾電子郵件的過濾功能越來越強大、電子郵件信箱的大容量化等，最近較少看到這種攻擊方式。

圖 2-16 殭屍網路所發動的 DDoS 攻擊

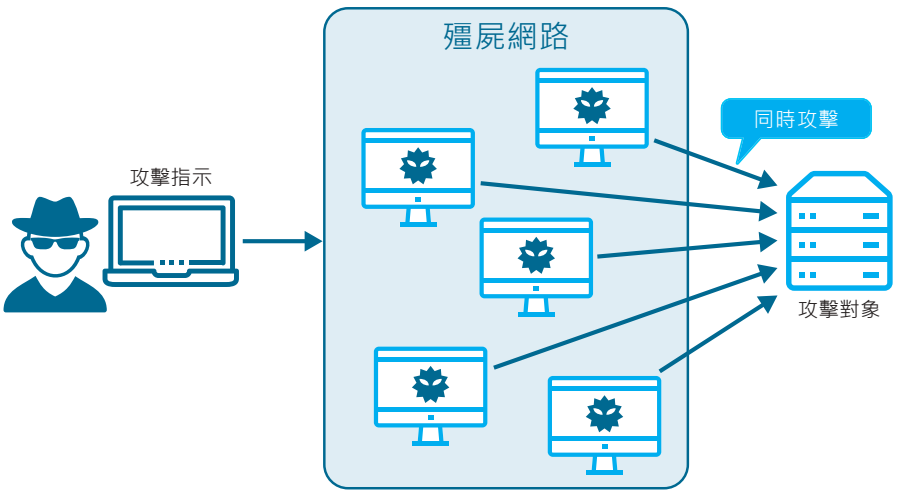
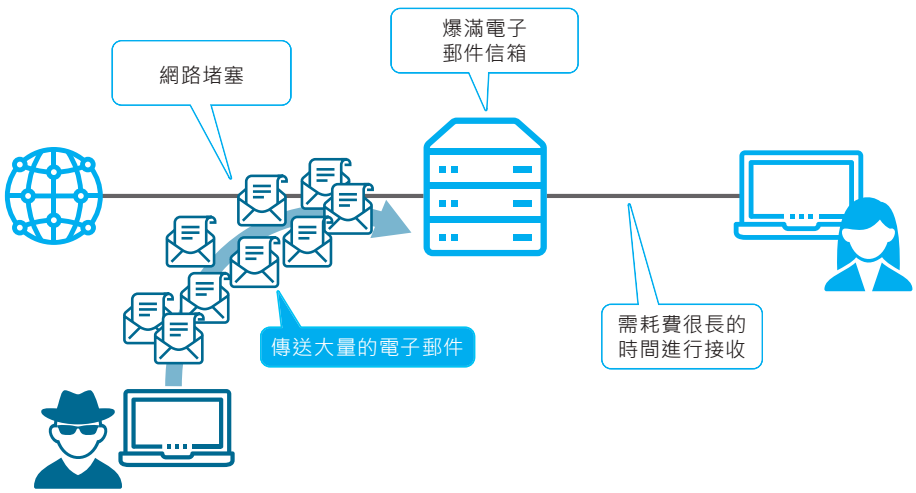


圖 2-17 電子郵件炸彈



Point

- 以殭屍網路來發動的 DDoS 攻擊是難找出發動攻擊者的
- 傳送大量電子郵件的電子郵件炸彈攻擊，雖然會對業務造成很大影響，但由於防堵垃圾電子郵件的功能越來越強大，最近已經減少了很多

» 防毒軟體的技術

在網際網路上設置誘餌

雖然防毒軟體加上了行為偵測的功能，不過對於防毒軟體而言最重要的還是病毒碼。為了製作病毒碼，防毒軟體商必須收集病毒。

這時會用到的就是**蜜罐**（**Honeypot**）。也就是將所謂的「誘餌」設置在網際網路上，同時讓它看起來像是實際上使用的電腦，且設定成很容易受到病毒或不當存取的攻擊（圖 3-5）。

由於是屬於易於攻擊的環境，病毒製作者及攻擊者會視為目標來發動攻勢。像這樣，讓實際上並未使用的環境看起來像是「真正的系統」，然後對**遭受到的攻擊或病毒進行收集**，來幫助病毒碼的製作。

用以確認程式行為舉動的「沙盒」

為了進行行為偵測，如果不想在實際的電腦上進行，有時會採用虛擬的方式，準備一個可執行程式的環境，這樣的環境就稱為**沙盒**（**Sandbox**）（圖 3-6）。

Sandbox 也可譯做「沙坑」，就如同小孩在公園的沙坑遊玩一樣，意指準備一個安全的場所。在沙盒內的執行結果，不會影響原本的電腦，如果所執行的程式是病毒，可降低損害。

藉由對在這裡被執行的程式具有什麼樣的行為舉動進行確認，便可運用在病毒的偵測上。有些防毒軟體甚至內建這樣的功能，在下載軟體時，可以直接放置於沙盒環境執行，確認其安全性。

圖 3-5 蜜罐

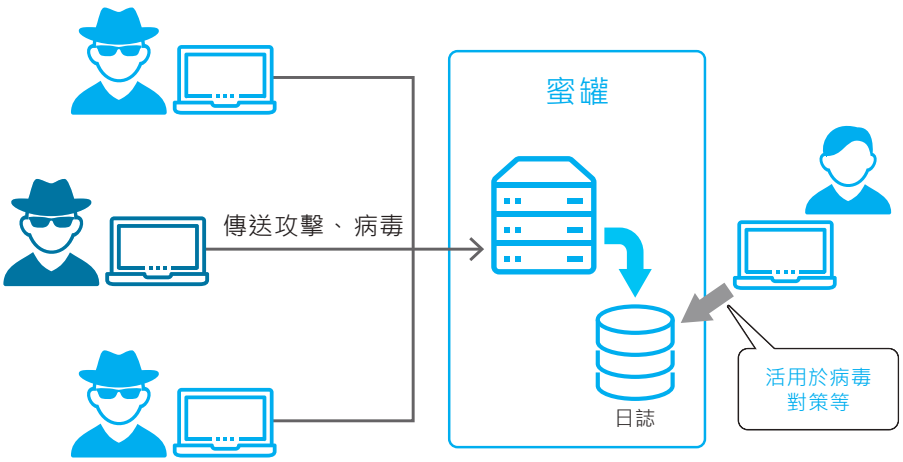
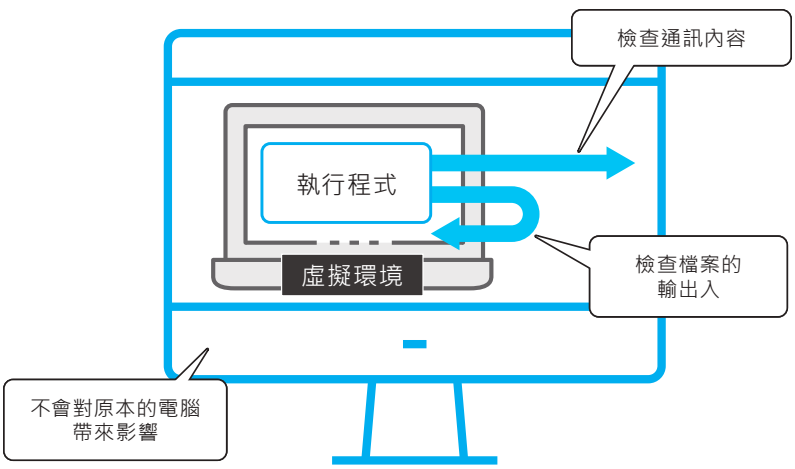


圖 3-6 沙盒



Point

- 蜜罐可用在收集攻擊手法及病毒上
- 透過沙盒，便可在不影響原本的電腦前提下，確認程式的行為舉動

» 記憶體區域溢位之濫用

在程式執行時要確保的記憶體區域

在執行程式時，就電腦的內部運作來說，會在記憶體劃分一部分區域來存放資料，對程式輸入的資料也會被存放在這裡，如果輸入資料過大，便會超出在設計階段所設定好的區域來嘗試進行存放（圖 4-17）。

開發人員在設計程式時，只要注意一下資料大小並設下限制以防止超出即可，如果不做這樣的處理，任何字串都有可能以輸入的形式塞到這個區域上。如果攻擊者寫入帶有惡意的程式碼，任何程式都有可能被執行。

超出保留區域時會發生的問題

對 C/C++ 等程式設計語言所開發的程式來說，記憶體的使用需由程式設計師適切地加以管理。如果沒有妥善管理，便會發生**堆疊溢位**（**Stack overflow**）、**堆積溢位**（**Heap overflow**）、**整數溢位**（**Integer overflow**）等問題。這些都是稱為**緩衝區溢位**（**Buffer overflow**）漏洞的一種，會在超出預設區域進行存取時發生（圖 4-18）。

當緩衝區溢位時，也就是可以寫入到準備好的區域之外的地方，如果處於這樣的狀態，就有可能會遇到如之前所提到過的，攻擊者所準備好的惡意程式碼遭到執行的情況發生。

最近的網頁應用程式許多是以 Java、PHP、Ruby 等程式設計語言來進行實作的，而以這些語言製作出來的程式，幾乎不會有記憶體使用上的漏洞產生。但是，這些程式語言所用到的 **Framework 或中介軟體之中，也有些是以 C 語言或 C++ 等程式語言來進行實作的，需要注意**。

圖 4-17 記憶體的配置

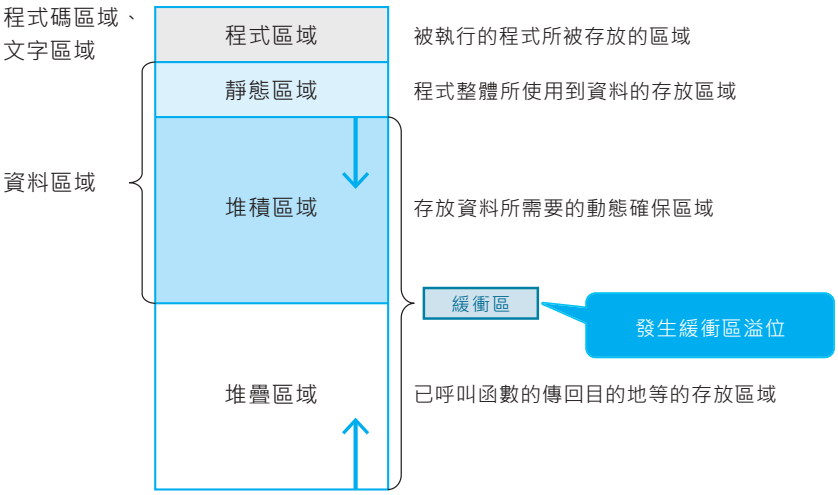
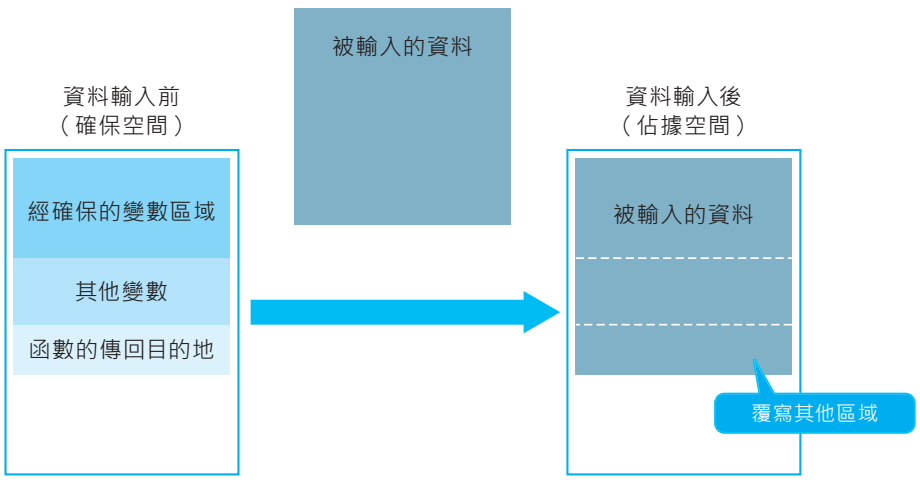


圖 4-18 緩衝區溢位



Point

- 使用需要由程式設計師來管理記憶體使用的程式語言進行開發，就有可能發生緩衝區溢位漏洞
- 就最近的腳本語言來說，記憶體使用方面的漏洞幾乎是不會發生的，但如果使用到第三方函式庫，還是有可能遇到漏洞問題

» 檢查是否有漏洞

站在攻擊者的立場來調查漏洞

幾乎所有的漏洞，都是在軟體開發階段就已經存在。不過，攻擊者會採取開發人員料想不到的方法來進行入侵，所以開發人員可能根本沒有察覺到有漏洞存在。

因此，為了檢查是否有漏洞，必須進行**漏洞診斷（圖 4-19）**。現在市面上可以找到免費的漏洞診斷工具，可針對一般攻擊手法來做調查。不過，當然也有工具無法發現的漏洞存在，所以許多企業會由專家以手動作業的方式來進行診斷。

然而，**即便是漏洞診斷沒有找到問題，也無法斷定漏洞並不存在**。需注意到，這是「僅限於以該調查方式對實施的範圍內，並無漏洞存在」的確認。

如果被判斷為漏洞存在，會針對該漏洞進行攻擊，以具體確認會有什麼樣的損害發生。

針對網路上的電腦，利用已知的技術來嘗試進行入侵，以確認系統是否有漏洞的測試手法，稱為**滲透測試**（**Penetration test**）或**入侵測試**。

對通訊埠編號進行存取即可調查出弱點

對於網路上的電腦，只要調查通訊埠編號是否可被存取，便可得知該電腦所使用的通訊協定。舉例來說，以 FTP 這個通訊協定來進行通訊的電腦，FTP 的通訊埠是開啟的。

攻擊者會實施一種針對有哪些通訊埠是開啟的，從外部來收集資訊而被稱為**通訊埠掃描**的檢測方式**（圖 4-20）**。開啟中的通訊埠一旦被得知，便可針對該通訊協定的弱點來擬定攻擊的策略。通常的預防措施，就是關閉不會使用到的通訊埠。

圖 4-19 漏洞診斷

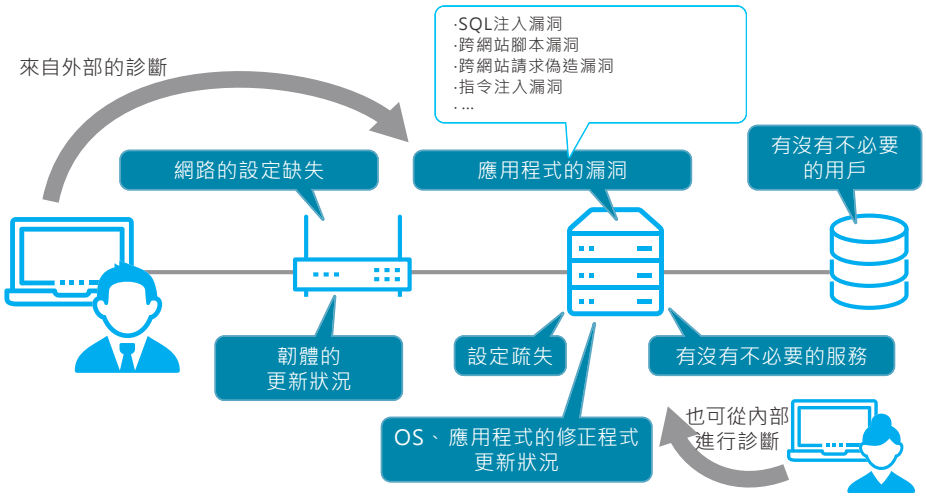
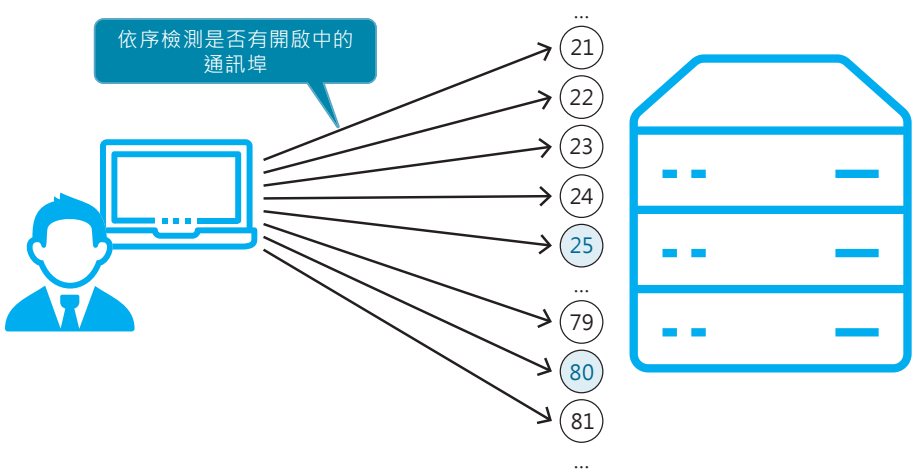


圖 4-20 通訊埠掃描



Point

- 實施漏洞診斷來檢測是否有漏洞存在一事，對於目前的軟體開發來說是必須的
- 實施對網路上的通訊埠是否可供存取的檢測，也就是通訊埠掃描，即可調查出電腦的弱點

圖 7-1　個人資訊的定義

個人資訊

基本4資訊	個人識別代碼	敏感性個人資訊
· 姓名 · 出生年月日 · 住址 · 性別	· DNA · 指紋、聲紋 · 護照編號 · 駕照編號 · 住民票代碼 · …	· 人種 · 宗教信仰 · 社會身份 · 病歷 · 前科 · …

圖 7-2　個人資訊、個人資料、擁有個人資料的不同之處

個人資訊

可用以識別存活中特定個人的資訊
包含能夠輕易地與其他資訊進行對照，結果為能用以識別特定個人的資訊

個人資料

由體型方面所組成可用以搜尋特定個人的資料
（個人資訊資料庫等）之內所含帶的個人資訊

擁有個人資料

具有公開、訂正、刪除等權限，並且擁有超過6個月者

出處：依據經濟產業省「各位業者!! 這樣的處理方式沒問題嗎？“ 個人資訊”」（URL：http://www.meti.go.jp/policy/it_policy/privacy/100401_pamphlet_meti.pdf）所製作

Point

- 個人資訊保護法經修正後，個人資訊的定義已明確化
- 個人資訊需遵守僅於使用目的之範圍內使用