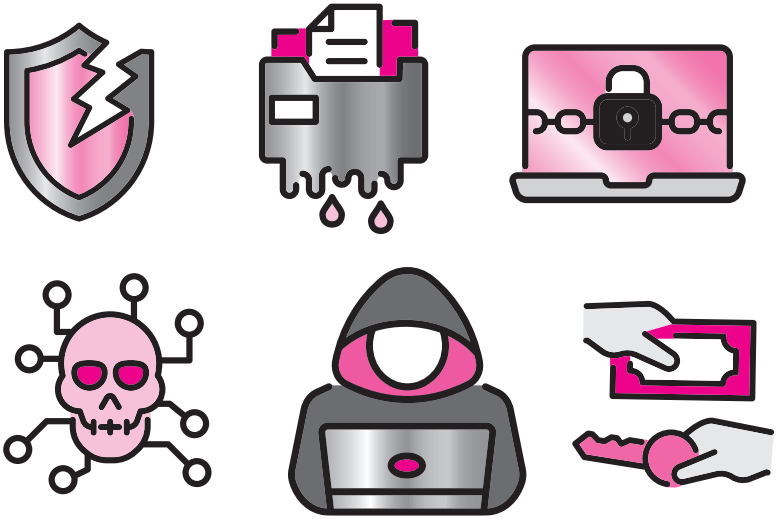
超圖解

網路安全入門

從基本觀念、網路攻擊手法到資安防護，一本全掌握！



大久保隆夫／著　陳識中／譯

前言

網際網路從1990年代開始迅速普及，如今已成為現代人生活中不可缺少的重要基礎建設。資訊網路就和水電與瓦斯一樣，已經是我們日常生活中不能沒有的必需品。平時幾乎不用手機看社群網路、不跟親朋好友聯絡聊天、不上網購物……像上述這樣不使用資通訊功能的人，近年應該非常少見了。而網路雖然為我們的生活帶來莫大的便利性，卻也讓我們**暴露在網路攻擊的風險之下**。

聽到網路安全四個字，可能很多人都會以為那是專家懂就好的東西。然而，其實所有使用網路的人隨時都暴露在遭受網路攻擊的風險中。而本書正是為了那些並非專家的普通人，也就是**平時會用手機刷社群網路、工作或唸書時會用到電腦，這些極其普通的一般人士**所寫，書中統整了**所有人都應該知道，有助於降低遭到網路攻擊風險的知識**。

說到最廣為人知的網路安全對策，相信很多人腦中都會浮現「不要使用簡單的詞語當作密碼或使用重複的密碼」、「隨時讓作業系統（OS）保持在最新版本」等常識。然而，對於「駭客具體是如何破解密碼，大概需要多少時間破解」、「為什麼作業系統廠商會定期發布更新，不更新的話又會遇到何種危險」等更進一步的問題，能夠答得出來的人卻不多。如果可以搞懂這些更深一層的問題，就能更好地保護自己。

在本書中，首先會介紹我們的日常生活有哪些必須防範的網路攻擊，以及它們實際上造成了哪些損害，接著會解說防範這類攻擊的安全策略與代表性的技術。但本書的最終目的終究只是**幫助一般的網路使用者獲得充足的知識**，如果你想獲得的是有助於通過檢定考試的進階安全知識，建議可以參考更進階的書籍。

相反地，如果你是想要學習資安知識來提升自身的資訊素養，或是任職於公司的網路安全部門卻不知道該怎麼對一般員工講解網路安全知識，那麼本書就非常適合你。另外，本書也很適合剛擁有第一支智慧型手機或第一台電腦的學生族，以及他們的家長。

現實中發生的網路犯罪和資訊洩漏事件，其中固然有一部分是由複雜的駭客程式引起，但更多的案例其實是由普通人或一般員工不起眼的小失誤或習慣所導致。**只要每個人都稍微提高資安意識或改變網路使用習慣，就可以避免大部分的資安事故**。希望你在讀完本書後，也能重新檢視自己生活中的資安對策，並加以落實。

從本書可學到的事

- 對一般網路使用者而言充足夠用的網路安全知識
- 盡可能讓網路攻擊者無機可乘的方法和網路安全觀念
- 網路安全的基本術語和技術概要

本書的目標讀者

- 日常生活中會使用智慧型手機的學生、社會人士
- 會在學校或公司使用電腦的學生、社會人士
- 想要到IT公司就職或想轉行到IT公司的人
- 負責對一般員工講解資安知識的資訊部門員工
- 需要教導孩子如何安全使用智慧型手機或平板電腦的家長、教職人員
- 曾經讀過其他網路安全的入門書籍，但因為內容太難懂而放棄的人

本書的結構

- **Chapter 1　為什麼需要網路安全？**
- **Chapter 2　認識網路攻擊的手法**
- **Chapter 3　網路安全的基本觀念**
- **Chapter 4　認識保護資訊的技術**
- **Chapter 5　認識網路攻擊的原理**

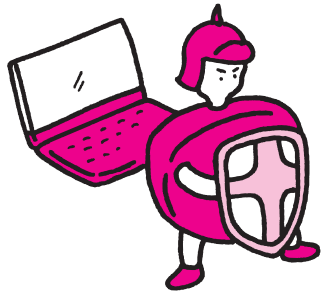
在Chapter 1中，我們會介紹典型的網路攻擊被害案例。在Chapter 2中，我們會深入淺出地講解網路攻擊是如何進行的，以及攻擊者常用的手法。在Chapter 3中，我們會說明「網路安全」的定義，以及基本的觀念。在Chapter 4中，我們會介紹實現安全狀態的具體技術，例如加密等技術的原理。最後在Chapter 5中，我們會介紹幾個典型的網路攻擊手法，講解其原理和防禦它們的方法。

CONTENTS

Chapter 1 為什麼需要網路安全？

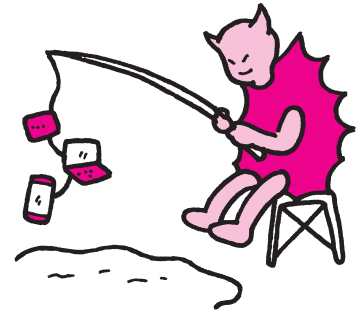
1 現代人的生活與網路空間相連 …… 2
2 透過網路盜走銀行存款 …… 4
3 綁架資料勒索贖金 …… 6
4 顧客的個資外洩 …… 8
5 攻擊公共運輸機構 …… 10
6 網路商店被癱瘓 …… 12
7 心臟節律器被人操控 …… 14
專欄 | 1 遠距辦公的安全對策 …… 16





Chapter 2 認識網路攻擊的手法

8 攻擊的第一步是欺騙 …… 18
9 典型的手法① 社交工程 …… 20
10 典型的手法② 釣魚 …… 24
11 典型的手法③ 惡意軟體 …… 26
12 什麼是駭入？ …… 30
13 什麼是漏洞？ …… 32
專欄 | 2 感染惡意軟體會發生什麼事？ …… 35
14 利用漏洞進行的攻擊 …… 36
15 支撐著網際網路的協定 …… 38
16 TCP/IP帶來的好處與壞處 …… 42
專欄 | 3 如何挑選防毒軟體 …… 44

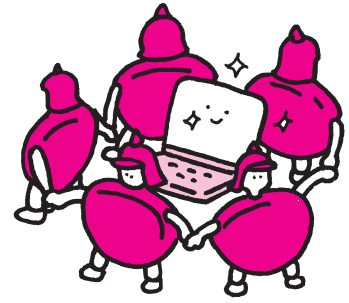


Chapter 3 網路安全的基本觀念

17 資訊安全與網路安全 …… 46
18 CIA＝機密性、完整性、可用性 …… 50
19 機密性 …… 52
20 完整性 …… 54
21 可用性 …… 56
22 什麼是驗證？ …… 58
23 驗證的種類 …… 60
24 驗證與授權的差異 …… 63
25 授權（存取控制）的種類 …… 65
26 什麼是加密？ …… 68
27 什麼是監控？ …… 70
專欄 | 4 網路安全的各種資格證照 …… 73
28 偵測攻擊並加以阻斷的系統 …… 74
29 管理組織與人 …… 76
30 法律與制度的制約 …… 78
31 什麼是最小權限原則？ …… 80
32 多層防禦與多重防禦 …… 82
33 分析威脅 …… 84
34 光藏起來並不安全 …… 87

Chapter 4 認識保護資訊的技術

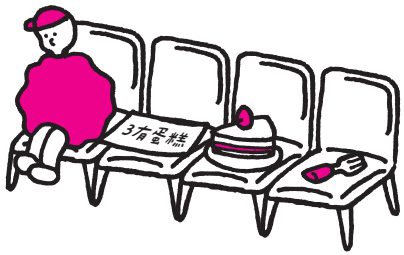
35 我們的通訊都有加密保護 …… 90
36 現代加密的原理 …… 92
37 各種加密的種類 …… 94
38 密文永遠都不會被破解嗎？ …… 96
39 防止外部篡改的設備 …… 98
40 絕對可信的原初基點 …… 100
41 什麼是安全作業系統？ …… 102
42 用於找出漏洞的測試 …… 104
專欄 | 5 個人資訊與特定個人資訊 …… 107
43 黑箱測試的手法 …… 108
44 找找看有無沒上鎖的入口 …… 110
45 偵測惡意檔案 …… 114
46 偵測來自網路的攻擊 …… 116
專欄 | 6 網路的構造與防禦系統 …… 118



Chapter 5 認識網路攻擊的原理

47 大家都在淘汰密碼驗證 …… 120
48 暴力破解 …… 122
專欄 | 7 為什麼變更密碼這麼麻煩？ …… 125
49 字典攻擊 …… 126
50 撞庫攻擊 …… 128
51 DoS攻擊與DDoS攻擊 …… 130
52 DDoS攻擊的對策 …… 134
53 什麼是注入攻擊？ …… 136
專欄 | 8 等「有需要再學」就太遲的理由 …… 139
54 資料庫與OS用的語言 …… 140
55 注入攻擊的原理 …… 142
56 注入攻擊的對策 …… 144
57 記憶體的運作原理 …… 146
58 緩衝區溢位① 異常中止 …… 148
59 緩衝區溢位② 改寫位址 …… 150
60 緩衝區溢位的對策 …… 152

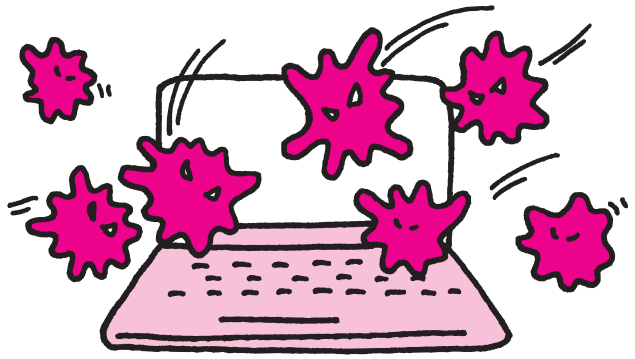
結語 …… 154
INDEX …… 161



Chapter 1

為什麼需要網路安全？

一般人常以為網路安全只有專家需要懂，但其實對一般人而言，網路安全並非毫無關係的知識。在本章中，我們會先解釋為什麼一般網路使用者也應該具備網路安全的知識，接著再介紹那些與你我切身相關的被害案例。



網際網路 IoT

1 現代人的生活與網路空間相連



在現代社會，我們周遭的各種事物都與**網際網路**（Internet）相連著。西元2000年以後出生的人可能很難想像，以前要是想查資料就必須上圖書館，不知道路怎麼走時只能去派出所問路，也沒有任何方法可以即時聯絡到外出的人。

然而在現代，這些事情只要一支智慧型手機就能全部辦到。不僅如此，各種家電、汽車，甚至是電網和自來水等社會基礎建設，也都開始連上網路。

這些機器或系統可以利用網際網路即時地分享資訊，或是透過網路來進行遠端控制。這種將我們生活中的各種事物都連上網路的資訊系統，就稱為**IoT**（Internet of Things，物聯網）。

IoT已經是一種相當普及常見的技術，日漸融入我們的生活，就連一些大家平常沒注意到的東西可能也是IoT的一部分。而且不只是肉眼可見的產品，就連肉眼不可見的系統和能源等也都開始連上網路，讓這個世界變得愈來愈方便。

然而很遺憾的是，這世間的萬物都有兩面性。機器和系統連上網路，就意味著可以從網路上的任何地方與這些機器或是系統通訊。換句話說，**惡意人士有可能透過網路攻擊這些設備**，而且**現實中也已經出現這樣的案例**。近幾年針對電力和自來水設備的網路攻擊就一度成為新聞焦點，而這些都是社會基礎設施連上網路之前不曾發生過的事件。

既然我們生活中的各種事物都如此依賴網路，那所有人就都跟網路安全脫不了關係。你可能會以為「維護網路安全不是專家的工作嗎？」但即使是為了消遣或工作而使用手機或電腦（PC）的一般人，也應該了解網路安全的知識，才能保護自己、家人，以及公司的資產。

本書的內容主要在解說有助於各位讀者保護自身的網路安全知識。首先，為了讓大家認識**為什麼網路安全這麼重要**，下面先來看看幾個**實際發生過的被害和攻擊案例**吧。

網路攻擊 釣魚

2 透過網路盜走銀行存款



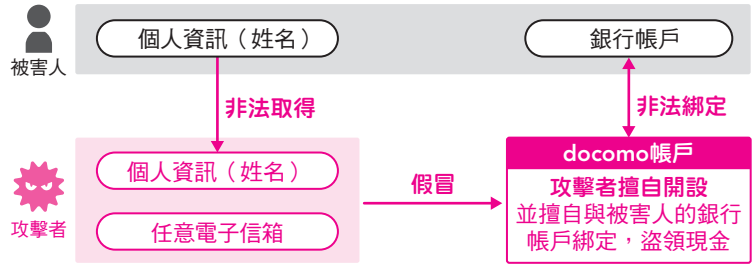
具惡意的第三方透過網路對他人造成損害的行為，就稱為**網路攻擊**。與我們切身相關的網路攻擊案例之一，便是**透過網路駭入非法盜取銀行存款**。

網路銀行（**線上銀行**）就是透過網路提供金融交易服務的銀行。只要登入銀行的網頁，便能確認自己帳戶的存款餘額，或是進行匯款或匯兌。

隨著網路銀行普及，現在紙本存摺逐漸遭到淘汰，愈來愈多銀行只提供電子存摺。客戶不用親自跑到銀行的櫃檯或ATM也能辦理各種手續，是一套非常便利的系統。

然而，網路銀行雖然方便，卻也是**網路攻擊者**（以下簡稱**攻擊者**）眼中的絕佳標的。舉例來說，近年日本便頻頻發生「明明沒有進行匯款，戶頭裡的錢卻在不知不覺間被匯給陌生帳戶」的案例。

2021年，日本發生數起透過NTT docomo電子支付服務「docomo帳戶」非法盜取存款的事件，受害的總金額約1800萬日圓。



▲docomo帳戶非法盜領事件的概要

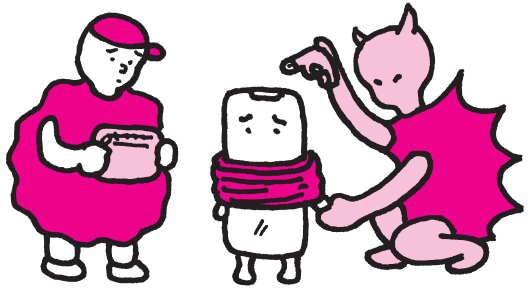
在這起案件中，攻擊者先非法取得了被害人的個人資料，接著再利用被害人的姓名開設docomo帳戶，然後與被害人的銀行帳戶綁定連結。

至於為什麼攻擊者可以做到這件事，這是因為docomo帳戶只要有本人的姓名和電子信箱就能申請，不需要確認本人的身分。換句話說，**申請者可以未經本人允許，冒用他人名義開戶**。攻擊者便是利用這種申請機制，非法將被害人銀行帳戶的錢轉移到自己的docomo帳戶中。

網路銀行的攻擊事件，主要是透過**釣魚**這種詐欺手法進行。關於釣魚的手法，我們會在⑩中詳細解說。

勒索軟體 / WannaCry

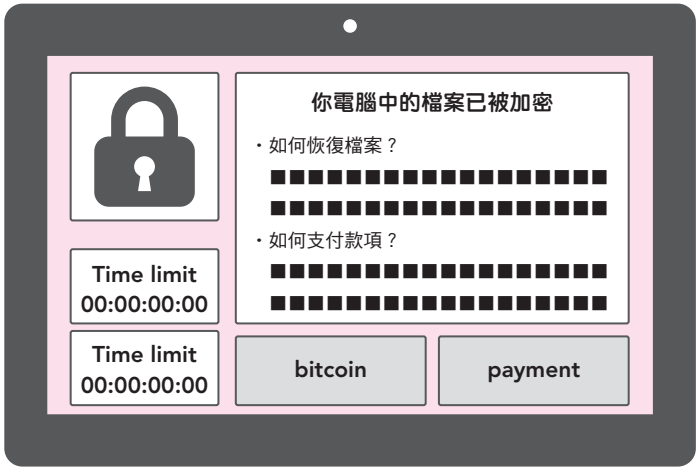
3 綁架資料勒索贖金



網路世界也跟現實世界一樣，存在著「綁架人質要求贖金」的犯罪。那便是**勒索軟體**（**Ransomware**）的攻擊。Ransom便是「贖金」的意思。

勒索軟體不綁架人，而是**用資料或電腦當作人質**（**物質**）。代表性的例子就是2017年時，一度在全球流竄的**WannaCry**病毒。這個勒索軟體感染了全球超過150個國家、23萬台的電腦，造成了嚴重的問題。

電腦一旦被勒索軟體感染，就會跳出如右頁插圖的畫面。畫面上除了「你電腦中的檔案已被加密」的警告文字外，還會顯示「如果你希望取回檔案，就將現金或比特幣匯入以下帳戶」。



▲感染勒索軟體的電腦畫面範例

要防止電腦感染勒索軟體，就必須落實「**不輕易點開陌生電子郵件中的附加檔案**」和「**不啟用巨集**※1」等對策。同時，為了預防萬一真的遭到感染，平時還應該**定期備份重要資料**。只要做好備份，就算檔案損壞了也能隨時復原。

勒索軟體通常會要求支付贖金來復原檔案，但本書建議不要同意攻擊者的要求。萬一遇到攻擊，在台灣可以向法務部調查局或內政部刑事警察局「勒索軟體報案專用窗口」報案；在香港可以到香港警務處官網電子報案中心的「舉報科技罪案及騙案」報案。

- **台灣法務部調查局** service@mjib.gov.tw
- **台灣刑事警察局** cib.noransom@cib.npa.gov.tw
- **香港警務處** www.police.gov.hk/ppp_tc

勒索軟體仍然在不斷進化當中，直到今天對我們而言依然是一個巨大的威脅。

※1 巨集（Macro）是Word和Excel等軟體中，將複雜處理過程自動化的功能。該功能預設為關閉的狀態。

4 顧客的個資外洩



在網路商店購物時，通常需要先註冊會員。註冊時只要預先登錄住址、姓名、信用卡號等個人資訊，下次購物時就能直接套用，不用重新輸入，非常方便。

很多服務都會收集並保管顧客的個人資訊。然而，有時這些資料會因為網路攻擊而外洩，對顧客造成**信用卡遭人盜用**等損害。

2021年，Facebook公司（現改名Meta）承認自家有超過5億5000萬名使用者的個人資料外洩。該公司解釋背後原因是Facebook提供的某個功能遭到濫用，令攻擊者可以利用此功能取得第三者的資訊。

這類「可以被攻擊者利用的系統缺陷」，一般就稱為**漏洞**（**Vulnerability**）。從Facebook的這起案例便能得知，由於攻擊者會利用軟體或系統的漏洞來發動攻擊，因此要強化資訊安全就必須盡可能消除軟體或系統的漏洞。關於漏洞的部分，本書會在⑬中詳細說明。

個人資料的外洩通常是因為針對漏洞的攻擊，以及我們會在⑨中介紹的社交工程等導致。但要注意的是，有**非常多的個資外洩案例都是沒有做好適當的資訊管理所致**，甚至比網路攻擊導致的案例更多。

舉例來說，日本常常發生因為把裝有筆記或電子設備的包包忘在電車上，才導致資料被拿走而外洩的案例。還有，直接用便條紙寫上密碼後貼在電子設備上，這種不當管理導致第三者侵入系統的例子也層出不窮。

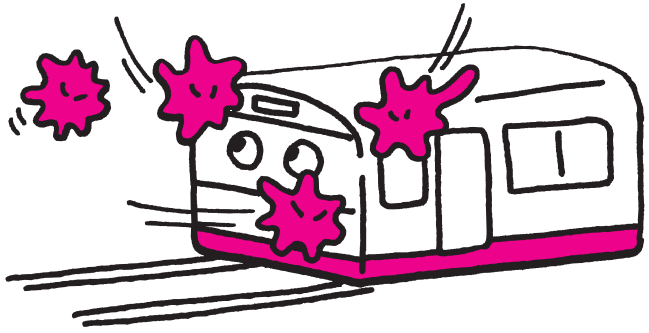


▲丟失儲存裝置或密碼的不當管理導致資料外洩

日本的《個人資料保護法》規定，「事業者必須適當管理顧客的個人資料」。萬一顧客的個資外洩，將有可能違反《個人資料保護法》，顧客也有權利要求該公司賠償損失。

駭入 勒索軟體

5 攻擊公共運輸機構



在影集或電影中，有時會看到「公車、電車、汽車等交通工具遭人駭入，奪走控制權」的橋段。這種事情在現實中真的有可能辦到嗎？

所幸，直到2023年為止，現實社會中還沒有發生過這種案例。然而，國外曾有鐵路公司遭到網路攻擊，並確實造成了損害。

舉例來說，2016年美國舊金山城市鐵路的**車站設備和售票機就曾感染勒索軟體，導致售票機停擺**，只好暫時讓乘客**免費搭乘**的事件。攻擊者向舊金山交通局要求7萬3000美元的贖金，但舊金山市政府拒絕支付。

除了這起案件之外，2017年德國和日本的鐵路公司（JR東日本）也都發生過電腦被WannaCry（參照③）感染的事件。當時WannaCry不只攻擊鐵路公司，也同時攻擊了各種不同的組織，向每名受害者勒索約300美元左右的贖金。在JR東日本的案例中，該公司發現設置在車站內**供民眾上網查詢的電腦遭到感染**，但是由於該電腦沒有連接到車輛運行等所使用的網路，因此對運行沒有造成影響。

不只是鐵路，汽車也有可能受到攻擊。在國際資訊安全會議※2上，許多專家們都展示了透過有線或無線網路，**利用車載系統的漏洞奪取車輛控制權**的可能性。在重現駭入過程的影片中，可以看到駭客成功奪取了汽車的方向盤，駕駛明明沒有碰觸方向盤，車子也能向左或向右轉。一旦汽車的方向盤和油門的控制權遭到奪取，駕駛將沒辦法自由控制車子，可能會偏離車道或突然加減速，很可能引發交通事故。

由此可見，一旦有心人士對運輸機構發動網路攻擊，不只普通人上班或上學等日常生活會受到影響，**還可能造成人身事故等物理性的損害**。

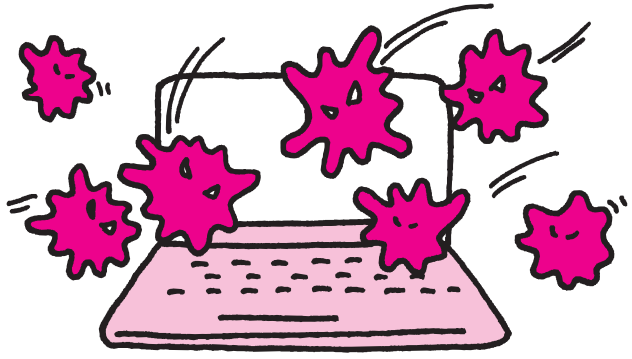
截至2023年為止，還沒有傳出網路攻擊對運輸機構造成物理性損害的報告。此外，鐵路等系統的運行網路也沒有與外網連接，所以很難進行網路攻擊。

話雖如此，我們仍無法斷言這種事情未來絕對不會發生。因此平時就要收集資安的相關訊息，思考身邊可能會發生哪些事故，這點也變得更加重要。

※2 白帽駭客（參照⑫）們公開市售產品尚未被人發現的漏洞調查結果的會議。較知名的有在美國舉行的國際資訊安全會議（DEFCON）和黑帽大會（Black Hat）。

DoS攻擊 伺服器

6 網路商店被癱瘓



如今的時代，不只是書籍，就連生活用品和各種家電也都可以在網路上購買。而且還可以直接在手機上下訂，快的話隔天就能送達。包含網路購物在內的各種網路服務，正逐漸成為現代人日常生活的必需品。

然而，我們**每隔一陣子就會遇到某個網路商店或服務暫時故障無法使用的情況**。發生這類故障的其中一個原因，便是**伺服器**※3**被DoS攻擊癱瘓而無法連接**。

※3 伺服器（Server）即是指負責提供服務的電腦。一旦伺服器當機或是癱瘓，網路服務就會跟著中斷。



▲ DoS攻擊的結構

DoS（Denial of Service）**攻擊**又叫做**阻斷服務攻擊**，是代表性的網路攻擊手法。這種攻擊的原理是對攻擊目標的伺服器給予大量工作負載，使伺服器的網路頻寬或運算資源超載，導致伺服器當機或無法正常被使用者連接。使伺服器超載最簡單易懂的方法，包含一次寄送大量電子郵件的**郵件轟炸**，以及快速連按重新整理網頁的快捷鍵F5的**F5攻擊**。

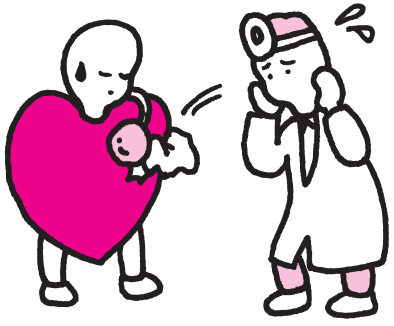
DoS攻擊可以透過屏蔽送出大量連接請求的連入者來進行防禦。然而，如果是一次有大量攻擊者的話，就另當別論了。同時透過大量設備發動的DoS攻擊稱為**DDoS攻擊**，這種攻擊無法光靠屏蔽特定通訊來源來防禦。

DDoS攻擊的代表性案例是2022年發生的雲端服務業者攻擊事件。這次攻擊導致了DeepL、Discord、Spotify等許多知名網路服務暫時中斷。

DoS攻擊癱瘓伺服器的行為，不只會造成網路服務使用者的不便，也會對服務業者造成**機會損失**，**發生財務上的損害**。不僅如此，**有時還可能導致品牌形象受損**。關於DoS攻擊，我們會在51中詳細介紹。

非法操作 個資外洩

7 心臟節律器被人操控

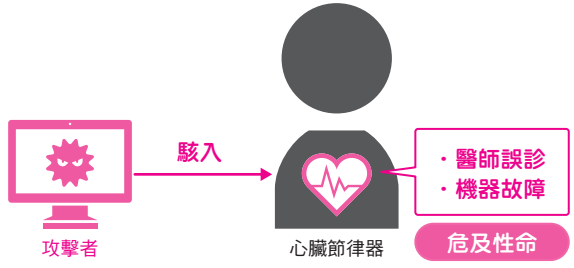


近年來，不需要醫生在場，可以連接網路從遠端治療或確認病患狀況的醫療器材日益增加。這類設備雖然很方便，但也跟其他IT系統或IoT機器一樣，遭受網路攻擊的風險也隨之提高。而且針對醫療器材的網路攻擊還有一個特徵，那就是**潛在的損害非常嚴重**。

2008年在日本的一場學術會議上，便有團隊發表研究指出，某款心臟節律器（心臟起搏器）和ICD（植入式去顫器）**存在著被駭客篡改病患資料、診療資訊及機器設定的可能性**。

該機種原本就可以透過網路遠端調閱或變更上述資訊。而攻擊者也同樣可以透過網路竊取設備上的資料，或在未經授權下變更機器的設定。

擅自變更病患的資料，可能會讓負責管理ICD的醫師誤診。同時，變更機器上的設定也可能引發設備意外故障，危及病患的性命。



▲ 攻擊者對醫療器材的非法操作

隨後在2012年，又有研究者在學術會議上發表報告，指出攻擊者可以透過網路攻擊讓心臟節律器或ICD**發出電壓高達830V的電流**。根據東京技能者協會的研究，**25～50V的電壓就足以致人於死**，因此**830V是一個非常危險的數字**。

所幸直到2023年為止，還沒有發生過這一類的攻擊事件。然而，一旦有心人士透過網路攻擊實際奪取了醫療器材的控制權，就有可能危及人命。

從本章的介紹可知，**網路攻擊造成的損害種類繁多**。有些光靠個人的努力無法防範，例如針對公共運輸機構的攻擊；也有些只要個人的一個簡單行動就能夠防止，例如物理性因素導致的個資外流等等。

在Chapter 2中，為了更進一步深化大家對於網路安全的相關知識，並確實預防可以防止的損害，我們會一一檢視攻擊者的各種攻擊手法。

專欄｜1 遠距辦公的安全對策

遠距辦公具有各式各樣的好處，但在資訊安全方面，也有幾個應該注意的要點。

首先，假如你跟家人住在一起，請記得**將工作用的電腦設定成只有自己才能使用**。就算家人沒有惡意，意外也可能會發生。在工作時間之外，電腦應該關閉電源並加上**物理鎖**，防止被人帶出家中；而在工作中暫時離席時，請記得將作業系統切換到**鎖定畫面**（Windows的話請按**Win鍵**＋**L鍵**）。為了防止意外發生，即使不是遠距辦公也請養成離席時鎖定電腦的習慣。

其次，請**不要使用公共的無線網路**。因為有些公共無線網路的安全措施做得很差，存在被人竊聽或資料外洩的危險性。即便是自家的Wi-Fi，如果你從來沒有檢查過路由器設定的話，也請記得「限制連接設備或設定密碼」、「換掉出廠時預設的帳號或密碼」。

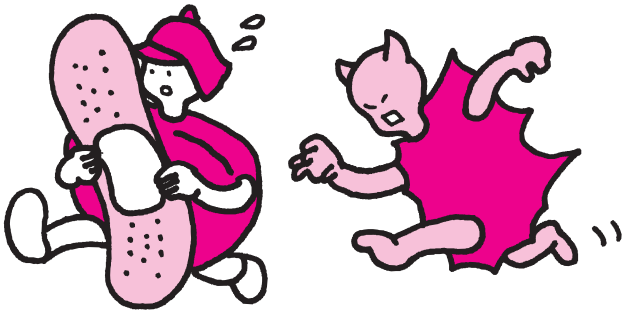
最後，請**不要將私人的儲存裝置連接至工作用的設備**。無論是哪種儲存裝置都存在資料外洩的風險。關於遠距辦公的資訊安全策略，一些政府機構的官網上都有詳細的資料，建議大家可以上去看看。

- **遠距、居家辦公的資安防護重點（台灣）**
  cs.hl.gov.tw/Upload/20220530173927039508l.pdf
- **遠距辦公資安（台灣）**
  www.cic.police.ntpc.gov.tw/cp-755-73432-28.html
- **網絡安全資訊站—遙距工作的保安（香港）**
  www.cybersecurity.hk/tc/learning-remote-working.php
- **資訊安全網—遙距工作的保安（香港）**
  www.infosec.gov.hk/tc/best-practices/person/remote-working

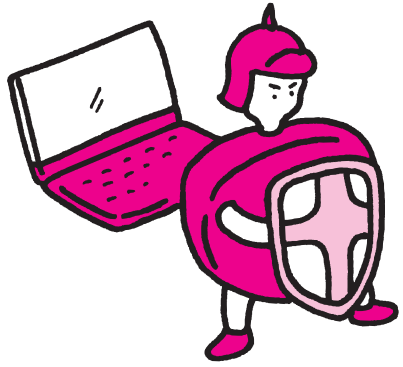
Chapter

2 認識網路攻擊的手法

網路攻擊有幾種典型的手法。在本章中，我們會先介紹這些手法，再一一講解它們攻擊時所針對的**漏洞**。同時，我們也會稍微介紹網際網路的原理，作為**Chapter 3**之後技術部分的預習。



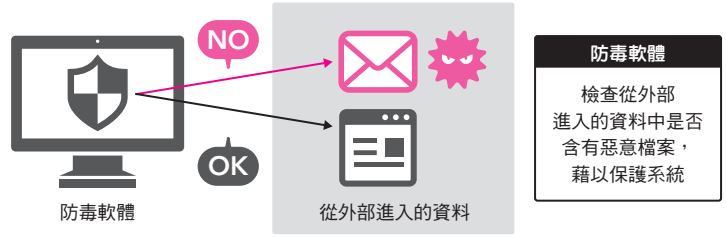
8 攻擊的第一步是欺騙



提到網路攻擊，可能多數人腦中浮現的畫面，都是駭客透過網路運用各種資訊技術發動攻擊。雖然這個印象並沒有錯，但你如果只提防這點，就有可能在意想不到的地方失足。因為網路攻擊的第一步，永遠是從**欺騙對象**開始，而**這個行為並非只依賴於數位途徑**。

在網路攻擊中，「欺騙對象」是非常重要的一步。因為絕大多數的人和企業都不想被攻擊，會設下重重的防備，所以攻擊者必須先突破這些防禦才能成功攻擊。

以我們身邊的事物為例，比如現代人在登入購物網站時都必須先輸入密碼，或是在電腦上安裝**防毒軟體**※4。這些全都是針對惡意或非法連接的防禦手段，而我們平時都會運用這類防禦手段來抵禦攻擊。



▲ 防毒軟體的防禦原理

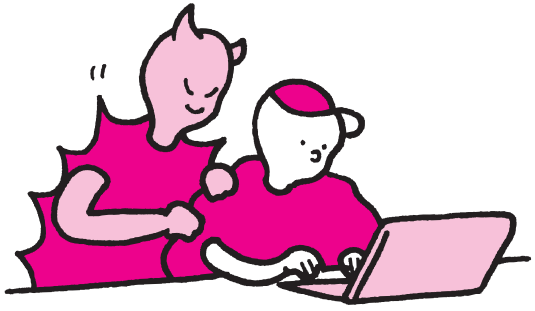
而站在攻擊者的立場來看，這些防禦系統是非常麻煩的。所以攻擊者必須想辦法無效化這些防禦。其中一種無效化的手段，便是運用數位技術攻破，但除了這種方法之外，也可以運用古典的面對面詐欺，或是物理性的盜竊方法。

密碼和防毒軟體都是重要的防禦手段。然而，如果平時只留意這些工具，你就有可能被意想不到的手法解除防禦。所以重要的**不是個別的防禦手段，而是時時提高警覺、提防被騙**。而要做到這點，就**必須先了解攻擊者具體會運用何種手段來解除你的防禦**。

所以從下一節開始，我們就來看看幾個**典型的欺騙手法**吧。

※4 具有預防感染病毒（參照⑪）、殺毒、阻斷未經授權的連接等功能，保護電腦或手機系統的軟體。其他像是安全軟體、殺毒軟體等等，指的也都是相同的東西。後面我們會在**專欄③**詳細說明。

9 典型的手法① 社交工程



網路攻擊的典型例子之一是社交工程。所謂的**社交工程**，就是利用人心或行為習慣的弱點，在不使用數位技術的情況下竊取個人所擁有的資料。日本網路安全協會對社交工程的定義※5如下：

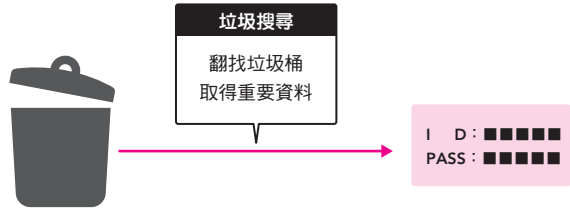
> **不利用電腦技術或網路技術，而使用物理手段（或心理手段）獲取入侵系統所需的帳號、密碼，或企業的機密資料等的行為。**

※5 「什麼是社交工程」日本網路安全協會：
https://www.jnsa.org/ikusei/04/14-01.html

社交工程具體可以分為以下幾種手段。

- **物理性手段**
  - 垃圾搜尋
  - 肩窺
- **心理性手段**

第一種**物理性手段**是**垃圾搜尋**。所謂的垃圾搜尋，就是從辦公處的垃圾桶中取得重要文件或寫有密碼的紙本，是電影中也經常出現的有名手法。



▲ 透過垃圾搜尋取得重要資料

除了紙張之外，**以非法手段取得他人的電腦或手機等電子設備**，並從中汲取個資或信用卡資料，也屬於垃圾搜尋的一種。這類資訊都存在著**透過廢棄設備外洩的危險性**。

想避免有心人士透過廢棄設備取得個人資料的方法大致上有兩種，但兩種都不簡單。

① 完全刪除資料
② 以物理性手段破壞設備