《安全與情報研究》 第六卷第二期 中華民國 112 年 7 月
Security and Intelligence Studies, Vol. 6, No. 2. July 2023

以數位韌性概念探討近期臺韓個資外洩事件之應處

黃予璿
淡江大學國際事務與戰略研究所碩士生

林穎佑
淡江大學國際事務與戰略研究所助理教授

摘 要

隨著個人資料基於電子化政府政策，陸續上架至雲端系統趨勢下，數位韌性此概念更加重要。數位韌性是透過結合不同數位工具，讓系統、組織在非理想環境能抵抗、吸收威脅，並維持關鍵性服務的能力。本文將先定義數位韌性與相關衡量指標，隨後點出兩國個資外洩事件保護法制和應處作為，驗證我國、韓國在法規、程序等方面韌性，接著探究駭客論壇兜售個資跟中國駭客組織攻韓行動兩案例，指出威脅建模、事後復原機制等未竟之處，最後揭示改善方針，確保國家安全利益。

關鍵詞： 數位韌性、個人資料保護法制、駭客論壇、國家安全

The Response to Recent Personal Data Breach Incidents in Taiwan and South Korea with the Perspective of Digital Resilience

Yu-Hsuan Huang

Graduate Student, Graduate Institute of International Affairs and Strategic Studies, Tamkang University

Ying-Yu Lin

Assistant Professor, Graduate Institute of International Affairs and Strategic Studies, Tamkang University

Abstract

With the trend of personal data being gradually uploaded to cloud systems based on the digitization of government policies, the concept of digital resilience has become more important. Digital resilience is achieved by combining different digital tools to enable systems and organizations to resist and absorb threats in non-ideal environments while maintaining the ability to provide critical services. This article first defines digital resilience and related measurement indicators. It then highlights the legal framework and contingency measures for personal data breaches in Taiwan and South Korea, and the resilience of both countries in terms of regulations and procedures. Next, it will discuss two cases - the sale of personal

data on hacker forums and the cyberattacks on South Korea by Chinese hacker organizations. The article will point out the unfinished aspects of threat modeling and post-mortem recovery mechanism. Finally, it will provide improvement strategies to ensure national security interests.

Keywords: Digital Resilience, Legal System of Personal Data Protection, Hacker Forums, National Security

壹、前言

隨著電子化政府計畫推行，保存在各部會個人資料如個人戶籍、戶政國民身分證影像、勞保投保、財產、個人所得、車駕籍等 31 項資料將陸續放上雲端系統，藉由數位服務個人化 (MyData) 平臺下載。[1] 除了政府機關外，各大電商平台及購票系統也會保存數千、數萬個資，倘若資料遭到他人或第三方外洩至中國駭客組織常交換情資的社交工程資料庫 (Social Engineering Data)，不只存有資料被盜賣、濫用疑慮，[2] 更會降低民眾對政府機關、民間企業信任。[3] 近期臺灣及個資保護嚴謹，我國法務部、國家發展委員會曾研析的韓國，都發生相關案例。

2022 年 10 月 21 日，名為 OKE 的中國籍人士於駭客論壇「違紀論壇」(Breach Forums) 兜售 20 萬筆戶役政資料，宣稱資料來自內政部戶政司。[4] 此外 2023 年初，中華航空會員列表、兵籍資料、國家中山科學研究院職員名單、軍事情報局機密文件、微風集團內部資料等資訊皆被兜售。[5] 韓國案例則是因應中國解封，

---

1 國家發展委員會國會及新聞聯絡中心，〈我的資料，我作主，MyData 平臺試營運上線了！〉，《國家發展委員會》，2020 年 7 月 29 日，< https://www.ndc.gov.tw/nc_27_34301>。

2 黑客，〈S 級黑客離不開的武器，社工庫〉，《知乎》，2016 年 10 月 4 日，<https://zhuanlan.zhihu.com/p/22754953>。

3 彭文暉，《數位時代個資外洩事故之通知機制研究》（臺北：立法院法制局，2021 年 4 月），頁 3。

4 法務部調查局公共事務室，〈法務部調查局資安工作站偵辦戶役政資料遭竊案新聞稿〉，《法務部調查局》，2023 年 2 月 24 日，<https://www.mjib.gov.tw/news/Details/1/839>。

5 劉宇珊，〈賴清德、林志玲等人驚傳個資外流！資料庫疑遭駭，華航回應了〉，《上報》，2023 年 1 月 14 日，<https://www.upmedia.mg/news_info.php?Type=24&SerialNo=163971>。

為預防國內疫情升溫，所以限制中國人民短期簽證，[6] 且韓國明星徐玄拜年文章不符合中國人期望。[7] 這兩件事驅使中國駭客組織「曉騎營」入侵韓國境內 12 個學術機構網站，散布包含檢警、智庫、重工業等 161 位人員資料。[8]

上述事件促使韓國國家情報院在 1 月 25 日和韓國科學技術情報通信部、韓國網路振興院共同展開調查。[9] 另外，我國於 2022 年 8 月新成立的「數位發展部」下設的「國家資通安全研究院」，於 3 月 29 日表示將協助中央目的事業主管機關，針對個資外洩事件施作行政檢查、鑑定程序，探詢資訊外洩根因。[10] 由於目前各國正推動數位韌性 (Digital Resilience)，為探討兩國是否能抵擋威脅且從個資外洩事件快速恢復，[11] 本文將先定義數位韌性此概念及其衡量指標，隨後點出兩國個資外洩事件保護法制與應處作

---

[6] 方璇，〈南韓暫停發中國入境短簽，駐中使領館逾 6 成人感染〉，《壹蘋新聞網》，2022 年 12 月 31 日，<https://tw.nextapple.com/international/20221231/D65134E018FF7FA82ACA859A293EB896>。

[7] 綜合報導，〈Chinese/Lunar New Year 掀戰，中國網友出征〉，《華視新聞網》，2023 年 1 月 24 日，<https://news.cts.com.tw/cts/international/202301/202301242135066.html >。

[8] 張沛元，〈挑農曆新年開戰，中國駭客猛攻南韓網站〉，《自由時報》，2023 年 1 月 26 日，<https://news.ltn.com.tw/news/world/paper/1564013>。

[9] 趙成美，〈中國駭客組織駭入 12 個學術團體和研究機構，甚至攻擊政府機構〉，《韓國聯合通訊社》，2023 年 1 月 25 日，<https://www.yna.co.kr/view/AKR20230125034053017?section=search&fbclid=IwAR1kOLS4O76rQ6XKmAW1qA1RlKjURUIyUHfngoTtOWZ8Y8kjeN87CdokNm8>。

[10] 林曉慧、陳昌維，〈數位發展部下設資通安全研究院，個資事件查處列重點〉，《公視新聞網》，2023 年 3 月 29 日，<https://news.pts.org.tw/article/629803>。

[11] Domo，〈何謂數位韌性〉，《Domo 的日常隨筆》，2022 年 10 月 21 日，<https://vocus.cc/article/6348be2dfd89780001088e2b>。

為，驗證我國、韓國在法規、程序等方面韌性，接著探究駭客論壇兜售個資跟中國駭客組織攻韓行動兩案例，指出韌性不足之處和案例差異，最後揭示改善方針。

貳、數位韌性定義與衡量指標

一、數位韌性定義

「數位韌性」(Digital Resilience) 此一概念，在國內外文獻中定義不一，吳明璋認為「數位韌性」是承受資安事件的非理想環境下，系統與組織維持關鍵性資訊服務以及管理系統的能力，由失敗平均時間、復原平均時間兩者作出綜合性衡量，為注重復原速度的連續性架構。[12] 我國數位發展部認定的數位韌性，是利用不同數位工具，在國家遇到各種不利狀況時，不僅可承受損害，還能從事件迅速恢復，並且從中學習，強化自身體質。[13] 另外，國家發展委員會是以具韌性特質的政府治理模式詮釋，提出關鍵基礎設施在面臨風險時能持續運作、導入公私協力機制促使政府機能不中斷、精進災難先期預警能力等面向。[14] 綜上所述，國內文獻說法都把數位韌性，當成系統與組織面臨風險時，能夠迅速恢復、適應的能力。

---

[12] 吳明璋，《鋼索上的管理課：駭客、災變與多變動時代的韌性管理學》（臺北：大寫出版有限公司，2018 年 9 月 20 日），頁 213-214。

[13] 數位發展部，〈數位發展部的核心理念是「強化全民數位韌性」，什麼是「數位韌性」？〉，《數位發展部》，2022 年 9 月 21 日，< https://moda.gov.tw/press/clarification/2512>。

[14] 謝翠娟、蔡君微，〈後疫情時代韌性智慧政府運作思維〉，《國土與公共治理季刊》，第 8 卷第 4 期，2020 年 12 月，頁 10-11。

國外的勤業眾信會計師事務所 (Deloitte & Touche)、英國網路安全委員會 (UK Council for Internet Safety, UKCIS)、歐盟議會 (European Parliament)、美國電機電子工程師學會 (Institute of Electrical and Electronics Engineers, IEEE) 則存在其他觀點。勤業眾信認為數位韌性不只是系統或組織應對威脅而且減緩損害的能力，也是不斷發展的方法。此方法會結合戰略甚至動態領導，付諸於人員、技術平台，以便預測及快速響應網路環境的突發事件。[15] 英國網路安全委員會表示數位韌性乃自數據產生的動態資產，讓相關單位積極投入潛在機會甚或挑戰，而非逃避或採取安全行為。[16] 此外歐盟議會內金融部門數位韌性法規和修訂條例，要求金融部門需建構、維護擁有數位韌性的資通訊系統最大限度減緩風險，持續識別潛在威脅，建立保護和預防措施，更須訂立營運持續計畫及資通安全事件通報及應變管理程序。[17] 最後系統在可能導致中斷的過度壓力下仍持續服務，那麼就具備美國電機電子工程師學會眼中的數位韌性，而政府機關、私營部門、個人

[15] Deloitte, "Ramping Resilience in theDigital Age", Deloitte, 2018. <https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/Ramping%20Resilience%20in%20Digital%20Age_Final%20web.pdf>.

[16] UK Council for Internet Safety, "Digital Resilience Framework", UK Council for Internet Safety, 12 September 2019. <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/831217/UKCIS_Digital_Resilience_Framework.pdf>.

[17] European Parliament, "Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations," 2020, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595>.

必須分擔責任，開發和維護在困難時期及時提供服務的能力。[18] 括而言之，數位韌性是建構結合戰略、動態領導、人員、數位工具等因素的方法，同時實踐先期預警，以便從非理想環境恢復、適應的能力。

二、數位韌性衡量指標

數位韌性的衡量指標，主要的 ISO 國際標準是《資訊安全管理系統》的 ISO 27001、《營運持續管理系統》的 ISO 22301、《風險管理》的 ISO 30001。[19] ISO 27001 注重的衡量指標為企業內的機密性 (Confidentiality)、完整性 (Integrity)、可行性 (Availability) 三大原則，又被稱為 CIA 三大要素：機密性是保障所有資訊不被未經授權者取得，並存取在正確的時間、地點、裝置；完整性是確保所有企業、使用者資訊不被未經授權篡改；可行性是確立企業、使用者資訊在系統內流暢度，讓已授權使用者能及時取得，不被任何不利因素中斷。[20] ISO 22301 重視的是企業遭逢惡劣氣候、天災、系統中斷、恐怖攻擊等重大營運衝擊事件，仍能順利營運，因此需規劃企業持續營運計畫、優先營運項目、風險評估、災害緊急應變計畫等面向。[21] ISO 30001 則透過溝通、諮詢確認

---

[18] IEEE, *White Paper - Digital Resilience IC Activity: Foundational Principles for Digital Resilience Framework*, December 1, 2021, p. 8.

[19] 吳明璋，《鋼索上的管理課：駭客、災變與多變動時代的韌性管理學》，頁 214-215。

[20] UPAS 內網安全，盡在掌握，〈從根本認識 ISO 27001，各行各業都適用的資安架構介紹〉，《UPAS 內網安全，盡在掌握》，2020 年 12 月 15 日，<https://reurl.cc/4QqGpR>。

[21] 李志鴻，〈疫情時代，談營運持續管理 (ISO 22301) 之重要性〉，《中小企業綠色環保資訊網》，2021 年 3 月 22 日，<https://green.pidc.org.tw/

企業內、外部環境，隨後進行風險鑑別、評估、分析，接著研擬風險處置方式，以及後續監督和審查流程。[22]

除了上述三種國際標準，韋萊韜悅與英國「經濟學人智庫」(Economist Intelligence Unit, EIU) 共同發表的《解構企業資安應變力》調查報告，指出從資安事件學到教訓、填補資安人才短缺、培養職場資安能力等項目，乃企業依舊缺乏的數位韌性能力。[23] 歐盟網路安全局 (European Union Agency for Cybersecurity, ENISA) 的數位韌性衡量指標，著重在可行性和安全性。可行性包含系統穩定性、網路服務性能、重大事故後平均修復時間、事件響應時間、重大事件數量等樣態；安全性為增加安全漏洞修補、定期紅隊演練等層面。[24] 總而言之，數位韌性衡量指標涵蓋機密性、完整性、可行性三大核心要素，還有企業持續營運計畫、系統穩定性、系統修復時間、風險評估、事件響應等細項。經由上述數位韌性概念、衡量指標，本文將進一步考證我國及韓國個人資料保護法制、資通安全事件應處作為，是否符合數位韌性要義。

---

detail.php?lang=tw&type=4&id=297>。

[22] 領導力企業管理顧問有限公司，〈ISO 31000 風險管理系統原理及指導綱要 Risk Management-Principles and Guidelines〉，《領導力企業管理顧問有限公司》，2016 年 11 月 2 日，<https://www.isoleader.com.tw/home/iso-coaching-detail/ISO31000>。

[23] 韋萊韜悅，〈全球數位韌性調查報告：能力與資源盤點〉，《韋萊韜悅》，2019 年 7 月 11 日，<https://www.wtwco.com/zh-TW/Insights/2019/07/digital-resiliency-report>。

[24] European Union Agency for Cybersecurity, *Resilience Metrics and Measurements: Challenges and Recommendations*, February 1, 2011, pp. 19-21.

參、針對個資外洩事件之我國法制與應處作為

一、我國個人資料保護法制

我國為預防個人資料外洩，同時兼顧數位韌性的個人資料保護法制，分成《個人資料保護法》、《中央主管機關訂定之個資檔案安全維護相關辦法》、《行政院及所屬各機關落實個人資料保護聯繫作業要點》。個人資料在《個人資料保護法》第 2 條定義是「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。」公務機關涉及個人資料外洩的法規是《個人資料保護法》第 18 條：「公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。」還有第28條:「公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。」非公務機關的規範是《個人資料保護法》第 27 條：「非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。」以及第 48 條：「非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣市政府限期改正，屆期未改正者，按次處新臺幣二萬元以上二十萬元以下罰鍰。」最後是第 12 條：「公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。」

統合上述法規，可知無論是公務機關、非公務機關只要不慎洩漏個人資料，便有相干刑責且要通知當事人。至於《中央主管機關訂定之個資檔案安全維護相關辦法》，出自於《個人資料保護法》不設立主管機關原則，直接由中央主管機關如內政部、教育部、經濟部等單位，遵循《個人資料保護法施行細則》第 12 條，對轄下各企業、學校制訂個人資料檔案安全維護管理辦法。[25] 另外《行政院及所屬各機關落實個人資料保護聯繫作業要點》認定中央目的事業主管機關接獲非公務機關通報或副知，抑或非因通報、副知知悉個資外洩案件，應於 72 小時內填列監督通報紀錄表，通報國發會。於此同時，對非公務機關實施監督管理措施。[26]

統合上述規範，《個人資料保護法》及相關辦法，是要求主管機關善盡監管職責，此外公務機關、非公務機關須辦理安全維護事項、事發後限期改正、通知當事人等作為，皆符合數位韌性最根本的機密性、完整性、可行性要素，其餘意涵體現於我國資通安全事件應處作為。

二、我國資通安全事件應處作為

除了《個人資料保護法》呼應的機密性、完整性、可行性要素外，風險評估、企業持續營運計畫、系統穩定性、事件響應、系統修復時間等數位韌性意涵，也存有相應的資通安全事件防護措施。而個資外洩於本文視作資通安全事件來由，是依據《資通

[25] 行政院，《中央主管機關訂定（修正）之個資檔案安全維護相關辦法》，2017 年 3 月 3 日，頁 1。

[26] 行政院，《行政院及所屬各機關落實個人資料保護聯繫作業要點》，2021 年 8 月 11 日，頁 3。

安全事件通報及應變辦法》第 2 條把「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、嚴重洩漏」一事，視為第三級、第四級資通安全事件，由於政府機關多以密件處理個資，[27] 故沿用此概念，探討資通安全事件之事前、事中、事後等應處作為。[28]

事前安全防護自《資通安全管理法》第 7 條，表示「主管機關應衡酌公務機關、特定非公務機關業務之重要性與機敏性、機關層級、保有或處理之資訊種類、數量、性質、資通系統之規模及性質等條件，訂定資通安全責任等級之分級。」與其配合的《資通安全責任等級分級辦法》於第 2 條分出 A 到 E 級的資通安全責任等級，也在 11 條明示「各機關應依其資通安全責任等級，辦理附表一至附表八之事項」。事項包含第三方驗證、資通安全稽核、業務持續運作演練、資安治理成熟度評估、安全性檢測等面向。除了實行應辦事項，《資通安全管理法》第 10 條、第 17 條提出公務機關、特定非公務機關「應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。」第 14 條第 1 項、第 18 條第 1 項，更另外訂立因應資通安全事件的「通報及應變機制」。至於資通安全維護計畫，除了維護實體與環境安全跟監控系統、訂定資通安全事件通報應變及演

[27] 參見李志強，〈公務員保密範圍探討〉，《清流月刊》，第 23 卷第 8 期（2015 年 2 月），頁 31-32。

[28] 林軒宇，〈資通安全事件通報應變推動淺談（上）〉，《跨域資安強化產業推動計畫網站》，2019 年 7 月 15 日，<https://www.acw.org.tw/Events/Detail.aspx?id=33>。

練相關機制之外，也要求公務機關、特定非公務機關加密、備份核心資通系統資料，作業頻率應滿足復原時間要求，並執行異地存放，每季確認核心資通系統資料備份有效性。[29]

配合上述需求的國家層級資安風險評估，就國家資通安全研究院評估方法，是擬定特定領域風險情境，先把情境發生可能性 (p) 參數，置於情境內可能性評估欄位，接著在衝擊評估一欄把影響類型 (n)、影響類型適用數量 (k)、衝擊程度 (x_n)、威脅重要性百分比 (C)、威脅係數 (t)、整體衝擊評估 (I) 等項，以 $I = t \times ((\sum_{n=1}^{k} x_n)/k)$ 公式計算事件發生後的整體衝擊值。[30]

事中緊急應變遵循《資通安全事件通報及應變辦法》的第 4 條、第 5 條、第 11 條內容，也就是事發機關知悉資通安全事件後，1 小時內通報主管機關，事件等級變更時續行通報，隨後主管機關須在 2 小時到 8 小時內審核事件等級。事後復原核心便是災害復原計畫 (Disaster Recovery Plan, DRP)。依據《電腦機房異地備援機制參考指引》，指出營運持續關鍵在於災害復原計畫的資訊回復點 (Recovery Point Objective, RPO)、營運復原時間 (Recovery Time Objective, RTO)、營運復原水準 (Recovery Level Objective,

[29] 數位發展部資通安全署，〈資通安全維護計畫範本〉，2019 年 1 月 30 日，頁 21、24。

[30] 國家層級資安風險評估方法的操作形式為設定特定情境，之後以情境發生可能性 (p) 的 1(極低) 至 5(極高) 參數，決定事件發生可能性。影響類型 (n)、影響類型適用數量 (k) 兩者，是用於判定情境內風險範疇影響類型和影響類型總數。衝擊程度 (x_n) 由 $((\sum_{n=1}^{k} x_n)/k)$ 計算出 1(極小) 到 5(極大) 的衝擊程度總分。威脅係數 (t) 則是代入威脅重要性百分比 (C) 參數，憑藉公式決定。最後透過 $I = t \times ((\sum_{n=1}^{k} x_n)/k)$ 公式算出整體衝擊評估 (I) 一值。請參閱：行政院國家資通安全會報技術服務中心，《國家層級資安風險評估方法簡介》，2022 年 5 月，頁 16-19。

RLO) 等評估項目，確保復原時可取得最新資料，以最快速度恢復必要服務，使業務持續營運，同時考量資安事件後設備、服務、系統的復原水準。[31]

復原時程參考《資通安全事件通報及應變辦法》第 6 條，第 13 條指示，事發機關按照資通安全事件等級，於 36 小時到 72 小時內完成損害控制或復原作業。執行細項依〈公務機關資通安全事件通報及應變管理程序〉、〈特定非公務機關資通安全事件通報及應變管理程序〉敘述，為負責應變之權責人員或緊急處理小組，依循本機關事前擬定之緊急計畫，完成資通安全事件衝擊及損害控制、造成損害之復原、相關鑑識及其他調查、調查與處理及改善報告、後續發展及與其他事件關聯性等作業，最後於資安事件通報紀錄單留存應變紀錄，受承辦之權責人員、資安長簽核，更修正或調整管理程序、人力配置或其他事項。[32]

綜上所述，事前安全防護的資通安全維護計畫、異地備援、國家層級資安風險評估，切合數位韌性內系統穩定性、風險評估等要素，事中緊急應變的《資通安全事件通報及應變辦法》滿足事件響應，事後復原的災害復原計畫合乎企業持續營運計畫、系統修復時間。探究完我國吻合數位韌性的個人資料保護法制跟資通安全事件應處作為後，能辨析管轄公務機關、特定非公務機關的主責機關。參照《行政院國家資通安全會報設置要點》知悉公務機關由行政院國家資通安全會報資通安全防護組主政，執行單

[31] 財團法人國家實驗研究院國家高速網路與計算中心，《電腦機房異地備援機制參考指引》，2014 年 3 月，頁 55-59。

[32] 數位發展部資通安全署，《公務機關資通安全事件通報應變程序範本》，2018 年 11 月 21 日，頁 6。

位為數位發展部資通安全署。[33] 而非統籌國家資通安全政策的行政院資安長，[34] 或是專注於技術研究發展的資通安全研究院。[35] 特定非公務機關則在關鍵資訊基礎設施安全管理組內分成通訊傳播、衛生醫療、金融服務、交通事業、能源及水資源、科技園區、數位政府等組，受到相關部會抑或數位政府司、韌性建設司管轄。[36] 基於韓國近期也被公開檢警、智庫、重工業等工作人員資料，便能以同一衡量標準，探究其個人資料保護法制以及資通安全事件應處作為，是否也遵從數位韌性。

肆、針對個資外洩事件之韓國法制與應處作為

一、韓國個人資料保護法制

韓國的個人資料保護法制，奠基於「個人情報保護法」（개인정보보호법）、「信用情報法」（신용정보법）及「情報通信網法」（정보통신망법）。[37]《個人情報保護法》是採取合

[33] 行政院國家資通安全會報，《行政院國家資通安全會報設置要點》，2023 年 2 月 22 日，<https://moda.gov.tw/ACS/nicst/establishment/660>。

[34] 行政院新聞傳播處，〈行政院資安長由副院長兼任，統籌國家整體資通安全政策〉，《行政院》，2019 年 2 月 15 日，<https://www.ey.gov.tw/Page/9277F759E41CCD91/f25d6bc3-9c6d-4d40-91da-a7998fbc8c1a>。

[35] 邱倢芯，〈數位部有資安署又有資安院，兩者怎麼分？〉，《科技新報》，2023 年 3 月 29 日，<https://technews.tw/2023/03/29/moda-nics-2/>。

[36] 行政院國家資通安全會報，〈行政院國家資通安全會報組織架構〉，《數位發展部資通安全署》，2023 年 6 月 2 日，<https://moda.gov.tw/ACS/nicst/organization/662>。

[37] 葉奇鑫，《韓國個人資料保護法制因應 GDPR 施行之調適委託研究計畫結案報告（計畫編號：PG10903-0166）》（臺北：國家發展委員會，2020 年），頁 1。

併規範模式，除特定情形外，同時規範公務機關還有非公務機關。並且在第 2 條定義個人資料：「尚生存之個人的相關資料，包括姓名、身分證字號和影像等可辨識個人資料，包含單一資料無法識別，但與其他資料結合可辨識者。」經由法規的模糊空間，可使總統藉由自身職權，增減《個人情報保護法》內敏感性資料所涵蓋範圍。接著第 29 條要求個人資料管理人應採取總統令所訂之必要措施，諸如內部管理計畫及保存存取紀錄等技術性、管理性、物理性措施，以防止個人資料發生遺失、遭竊、外洩、變造和毀損之情事，且於第 31 條指定個人資料保護專責人員，應建立、實施個人資料保護計畫，更存有個人資料外洩罰則，和告知資訊被外洩當事人的義務。[38] 第 39 條第 4 項則是規定網際網路服務提供者知悉個人資料遭洩漏，應於 24 小時內執行。第 10 項為網際網路服務提供者收到保護委員會跟總統令指定之專門機關請求，應刪除、阻斷遭受外洩之個人資料。[39] 上述法條皆被隸屬總統的「個人資料保護委員會」(Personal Information Protection Committee, PIPC)，管轄。[40]

《信用情報法》的定位則圍繞在金融交易時，得以判斷他人信用的必要資訊，好比是信用評分；好比是交易能力；好比是交易內容等情資的蒐集、調查、處理、流通、利用、管理行為做出

[38] 林秀蓮、李世德，《考察南韓、新加坡個人資料保護法制及相關專責機關》（臺北：法務部法律事務司，2014 年 11 月 14 日），頁 8-9。

[39] 葉奇鑫，《韓國個人資料保護法制因應 GDPR 施行之調適委託研究計畫結案報告》，頁 90、93。

[40] 林秀蓮、李世德，《考察南韓、新加坡個人資料保護法制及相關專責機關》，頁 30。

規範，保障當事人公告權、同意權、閱覽權、更正權、刪除權。[41]

《情報通信網法》是在電信網路架構中，明訂個人情報之蒐集暨取得、利用暨提供之限制、使用者管理、個人資料侵害事件的紛爭調停等機制。[42] 總結上所言，韓國《個人情報保護法》、《信用情報法》、《情報通信網法》和我國驗證結果相同，契合數位韌性內 CIA 三大要素。

二、韓國資通安全事件應處作為

韓國的資通安全事件應處作為，根據北大西洋公約組織「合作網路防禦卓越中心」(Cooperative Cyber Defense Centre of Excellence, CCDCOE) 出版的《國家網路安全組織：大韓民國》(National Cybersecurity Organisation: Republic of Korea) 一書，是由總統秘書室主責，如出現包括資通安全在內的國家安全問題。總統秘書室就可舉行國家安全保障會議。相關細項自〈韓國網路安全和數據韌性政策〉(Korean Policies of Cybersecurity and Data Resilience) 專文，明瞭公務機關受國家情報院旗下的國家網路安全中心所管轄，私部門由科學技術情報通信部管理，軍方主管機關為國防部網路司令部。[43]

---

[41] 葉奇鑫，《韓國個人資料保護法制因應 GDPR 施行之調適委託研究計畫結案報告》，頁 5。

[42] 葉奇鑫，《韓國個人資料保護法制因應 GDPR 施行之調適委託研究計畫結案報告》，頁 4。

[43] So Jeong Kim and Sunha Bae, "Korean Policies of Cybersecurity and Data Resilience," *Carnegie Endowment for International Peace*, August 17, 2021, <https://carnegieendowment.org/2021/08/17/korean-policies-of-cybersecurity-and-data-resilience-pub-85164>.

關涉的國家網路危機預警等級及事件響應原則，是參照國家情報院公布的《國家網路危機管理標準手冊》，將預警等級分成「輕度警報、中度警報、嚴重警報、關鍵性警報」等階段：輕度警報是入侵偵測系統的網路攻擊情資；中度警報是關鍵基礎設施的部分網路系統故障、些許機構受到攻擊、惡意活動擴散到其他機構的情資；嚴重警報是多個網際網路服務供應商或政府骨幹網路出現障礙，大量政府機關被攻陷的情資；關鍵性警報是針對整個國家的網路攻擊抑或是大規模破壞情資。並會在國家情報院與科學技術情報通信部、國防部情資共享後發布警報，當中度以上警報發布時，各機構便會開展相應的預防、應對和恢復活動。[44]

除了上述預警等級，《國家網路安全管理條例》（국가사이버안전관리규정）也規定中央主管機關、廣域地方自治團體及基礎地方自治團體若獲知資通安全事件或相關徵兆，應採取減緩損害措施，隨即向國家安全保障廳廳長、國家情報院廳長還有中央主管機關通報。簡而言之，韓國的資通安全事件應處作為，是以總統府秘書室及國家情報院主導，制定近似於《資通安全事件通報及應變辦法》的《國家網路安全管理條例》，訂出資通安全事件等級，和列出各單位通報辦法，交由國家網路安全中心、科學技術情報通信部、國防部網路司令部執行，這些程序合於事件響應，卻缺乏系統修復時間、企業持續營運計畫、系統穩定性的詳盡準則，所以韓國個人資料保護法制、資通安全事件應處作為乃有限度數位韌性。

[44] Sungbaek Cho, *National Cybersecurity Organisation: Republic of Korea*, June 2022, p. 20.

伍、臺灣與韓國個資外洩案例之比較分析

一、臺灣個資外洩案例：駭客論壇兜售個資

縱使我國《個人資料保護法》及相關辦法切合數位韌性，也導入《資訊安全管理系統》的 ISO 27001 國際標準至 240 家企業，[45] 但實務依然有未竟之處，所以個案分析由事件內容、事件中攻擊手法、不足之處三種層面構成。事件內容是 2019 年 6 月 22 日，銓敘部接獲五眼聯盟情資，有 24 萬筆中央及地方機關公務人員歷史資料被中國駭客組織 APT12 洩漏至 Raidforums 駭客論壇，[46] 以及 2022 年 10 月 21 日起，於 Breach Forums 駭客論壇逐步外洩的戶役政資料、兵籍資料、國家中山科學研究院職員名單、中華航空客戶列表、軍情局機密文件、微風集團內部資料。這些事件皆能視為駭客後續實施「變臉詐騙」(Business Email Compromise) 與「假旗行動」(false flag operations) 之前兆。

上述事件視作變臉詐騙、假旗行動等攻擊手法來由，可從定義、駭客鎖定目標、資料用途、相關案例等項論述。定義上變臉詐騙是指歹徒冒充主管身份發送訊息，欺騙其員工、客戶或合作夥伴。[47] 假旗行動則是偽裝成敵方，向己方發動攻擊，誤導外

[45] 數位時代，〈2020 資訊治理年會登場！ SGS 揭露第一手資安趨勢觀察〉，《數位時代》，2020 年 12 月 9 日，<https://www.bnext.com.tw/article/60209/sgs-202012>。

[46] 劉榮、林俊宏，〈【情報員個資洩光光】銓敘部遭駭手法曝光，與中國網軍「攻美護主」模式雷同〉，《鏡週刊》，2019 年 7 月 3 日，<https://www.mirrormedia.mg/story/20190703inv007>。

[47] Asaf Cidon, "Threat Spotlight: Barracuda Study of 3,000 Attacks Reveals BEC Targets Different Departments," *Barracuda*, August 30, 2018, <https://

界，進一步合理化我方作為。[48] 之後從駭客鎖定目標來看，資料遭外洩對象，涉及敏感性或國安含資安疑慮之業務範疇，好比是銓敘業務相關系統；好比是戶役政作業管理相關系統；好比是民航場站維運相關系統，[49] 足以發覺駭客組織有意鎖定我國敏感性系統，而且釋出部分樣本使當事機關懷疑現有系統韌性，並受相當罰則。有關被駭資料之用途，依據《天下雜誌》的報導，認為 Breach Forums 駭客論壇上 20 萬筆設籍宜蘭的商品樣本來自 2018 年 4 月前的真實資料，但駭客會變造些許內容。[50]

假若洩漏資料為真，能用於社交工程攻擊，甚至引發國安事件。隨後相關案例為俄國總參謀部情報總局曾假扮成伊斯蘭國襲擊法國電視國際五台、俄國駭客組織 Turla 控制伊朗駭客組織 Oilrig 系統、[51] 中國籍人士假冒誠品書局市調電話，對使用者散布統戰言論、[52] 臺灣工程師偽造越南公安部門、泰國民事法院官

blog.barracuda.com/2018/08/30/threat-spotlight-barracuda-study-of-3000-attacks-reveals-bec-targets-different-departments/>.

[48] 王能斌，〈【新聞辭典】假旗行動〉，《中華民國國防部青年日報社》，2022 年 1 月 16 日，<https://www.ydn.com.tw/news/newsInsidePage?chapterID=1477511&type=universal>。

[49] 國家運輸安全調查委員會，《具敏感性或國安（含資安）疑慮之業務範疇》，2020 年 11 月 10 日，頁 1-3。

[50] 鄭閔聲、史書華，〈15 萬如何買下 2300 萬人？《天下》深入白帽駭客圈，還原個資賤售荒唐錄〉，《天下雜誌》，2023 年 3 月 7 日，<https://www.cw.com.tw/article/5124927>。

[51] Josh Fruhlinger, “What is a False Flag? How State-Based Hackers Cover Their Tracks,” *CSO*, January 9, 2020, <https://www.csoonline.com/article/3512027/what-is-a-false-flag-how-state-based-hackers-cover-their-tracks.html>.

[52] 陳凱俊，〈阿共真的「打來了」！誠品買書竟接「詭異市調」爆個資外洩變統戰〉，《鏡週刊》，2023 年 5 月 14 日，<https://www.mirrormedia.mg/story/20230514edi007/>。

網行騙等事。[53] 此類手法除了妨害企業、政府機關信譽，也存在戰時或國家遭受重大變故，導致通訊系統不若以往那般暢通，已取得可信個資的有心人士，會偽裝我國公職人員，從事電信詐欺或侵擾他國關鍵基礎設施的隱憂。

鑒於國家安全局、國防部會依「資安向前防禦方針」追溯攻擊源頭，[54] 建議個資主管機關與其協作，識破有心人士意圖，確立個資外洩事件的共同威脅樣態，研擬威脅模型，用以補強影響營運持續、事後復原的脆弱點。[55] 除此之外事後復原需克服之處是事發機關處理事件程序應透明化，[56] 依照機密等級由低至高，於他處逐步恢復加密、分割後存放至備援主機資料，同時刪除原處外洩資訊，避免駭客循線獲取數據。

二、韓國個資外洩案例：中國駭客組織攻韓行動

韓國的個資外洩事件內容是 2023 年 1 月 7 日時，中國駭客組織「曉騎營」提出「對韓國進行新一輪行動，會長期造成數據外洩，並同步更新在官方部落格」的「韓國行動」宣言，自 1 月 20 日開始，攻擊大韓建設政策研究院、韓語學會、韓國考古學會、

[53] 社會組，〈詐騙 IT 王 1 ／架假官網、客製「變臉」賣 20 詐團，台工程師成亞洲難波萬〉，《周刊王》，2022 年 12 月 30 日，<https://www.ctwant.com/article/229728>。

[54] 國家安全會議資通安全辦公室，《國家資通安全戰略報告 — 資安即國安 2.0》，2021 年 9 月，頁 30-31。

[55] T.H. Schee，〈大量國民個資外洩是一種持續性的威脅〉，《T.H. Schee》，2023 年 2 月 14 日，<https://blog.schee.info/2023/02/14/massive-data-breach-and-persistent-threat/>。

[56] 財團法人資訊工業策進會，《電子商務個資外洩資安防護參考指引》，2015 年 7 月，頁 100-101。

韓國家長學會、韓國教育大學幼兒教育研究所、韓國基礎健康醫學會、韓國社會科學與教育學會、韓國東西方精神科學會、韓國唇顎裂學會、韓國視覺障礙教育康復學會、濟州大學教育科學研究所、韓國教育原理學會等網站。[57] 依據筆者的觀察，大韓建設政策研究院起初就終止服務，其餘 11 個學術機構於 1 月 24 日晚間網頁遭致置換，隨後在 1 月 25 日早上 10 點再也無法瀏覽。在韓國網路振興院、韓國科學技術情報通信部、韓國國家情報院經由《國家網路安全管理條例》介入本次行動後，「曉騎營」便刪除大量外洩資料。更於 2 月 19 日表示終止韓國行動，將和黑狼駭客組織共同復出。

事件內中國駭客組織「曉騎營」的攻擊手法，是置換韓國學術機構官方網站，接著讓網頁呈現伺服器無法回應的 HTTP 狀態 404，抑或是無法完成請求的 500，再竊取內部資料庫於駭客論壇兜售。此舉為何會洩漏個人資訊，源自駭客登入網站後台，除了更換網頁參數也能讀取受害主機資料。[58] 若駭客向外兜售所獲文件，將衍生個資外洩事件。除此之外從內部數據出售群組，能覺察「曉騎營」和其他駭客組織共享情資：群組內存有我國 2003 到 2021 年的旅館業訂單、試務人員登入資訊、8 千組日本信箱以及 250 萬筆數據，還有用 theHarvester、Nmap 等網路滲透工具偵蒐的法務部網路架構。深入探討後得知以上資料取自另一中國駭客組織「騰蛇」(Teng Snake)。不足之處是法規缺乏修復系統期限

[57] 張沛元，〈挑農曆新年開戰，中國駭客猛攻南韓網站〉。

[58] 臺灣學術網路危機處理中心團隊，《網頁置換攻擊事件分析報告》，2019 年 3 月，頁 8。

跟異地備援機制，[59] 使得遭受攻擊無法運作的學術網站數月後仍不能連線，若補足呼應系統修復時間法規，此外公私部門借助雲端服務備份重要數據，[60] 作為事後復原的備援主機，將完全契合數位韌性內多項可行性準則。

三、兩國個資外洩案例差異之處

兩國個資外洩案例差異之處，能比較個資保護法制管轄重點、個資外洩通報機制、資安事件主責機關、駭客動機、事件嚴重性、數位韌性不足之處等事項。相較我國個資保護法制，韓國更重視金融交易的信用情報、電信網路架構中個人資料，並且不確切定義個資範疇，以便總統增補法規內敏感性情資。此外知曉個人資料外洩的通報機制也有所差異，我國由主管機關實行，韓國為網際網路服務提供者，且雙方通報時限差距甚大。接著資安事件主責機關，我國經由數位發展部資通安全署主政，韓國以總統府秘書室、國家情報院主導。

至於駭客動機，我國面臨的是變臉詐騙、假旗行動前兆，韓國視角為中國駭客組織訴諸民族主義。事件嚴重性因我國軍方、情報機關個資被多次變賣，比起韓國學術機構遭駭更加嚴重。最後我國不足之處為事發機關應透明化處理程序，同時在他處根據機密等級逐步恢復資料。韓國因缺乏異地備援機制，需導入雲端服務備份公私部門重要數據，當成事後復原的備援主機。

---

[59] 俞伯翰，〈【觀點】一場 Kakao 之亂讓韓國停擺！企業怎麼防範？營運永續計畫 BCP 是什麼？〉，《數位時代》，2022 年 11 月 29 日，<https://www.bnext.com.tw/article/72786/company-bcp-plan>。

[60] 同上註。

陸、結論

個人資料逐漸上架至雲端系統的趨勢下，如何讓社會運作不因多次資通安全事件失衡，已變得更加重要。數位韌性此概念，可讓國家結合戰略、動態領導、人員、數位工具等因素，使系統、組織於逆境時足以抵抗、吸收威脅，維持關鍵服務。細部衡量指標涵蓋機密性、完整性、可行性等核心要素以及企業持續營運計畫、系統穩定性、系統修復時間、風險評估、事件響應等細項。

我國和韓國的個人資料防護法制、資通安全事件應處作為皆合於數位韌性。兩國個人資料防護法制相同點在於公務機關、非公務機關須指定專人負責個人資料安全維護，防止資料被盜取、竄改、毀損、滅失或外洩，若資料外洩，事發機關需承擔損害賠償責任，並告知權益遭損害當事人。相異點是韓國注重金融交易的信用情報、電信網路中的個人資料保護。此外知悉個人資料外洩的通報機制這部分，我國由主管機關實行，韓國為網際網路服務提供者，雙方通報時限差距甚大。至於韓國不確切定義個人資料範疇，是便於總統增補法規內敏感性情資。

有關資通安全事件應處作為，我國係由數位發展部資通安全署主責，透過行政院國家資通安全會報資通安全防護組、關鍵資訊基礎設施安全管理組管轄公務機關、特定非公務機關，分「出事前安全防護」、「事中緊急應變」、「事後復原」等程序，同時導入國家層級風險評估。韓國由總統秘書室主導，制定預警等級及事件響應原則。預警等級劃分成輕度、中度、嚴重、關鍵性警報，發布警報後各機構開展相應的預防、應對、恢復活動。法規要求中央及地方主管機關若獲知資通安全事件，應採取減緩損

害措施，且通報國家安全保障廳及國家情報院。

近期兩國個人資料外洩事件，驗證出個人資料防護法制、資通安全事件應處作為之於數位韌性未竟之處。我國是事發機關處理事件程序應透明化，也在系統他處依機密等級逐步恢復資料，除了維持營運更中止駭客攻擊。韓國的《國家網路安全管理條例》則沒寫明修復系統時限、異地備援機制將使事發機關於數月後無意修復遭攻擊網站，另外案例差異包含駭客動機、事件嚴重性。動機存有變臉詐騙需求和民族主義差別，至於事件嚴重性因我國軍方、情報機關個資被多次變賣，比起韓國學術機構遭駭更嚴重。最後雙方改善方針，建議我國個資主管機關與國家安全局、國防部協作，藉由個資外洩的威脅模型，補強影響營運持續、事後復原的脆弱點。韓國需補足呼應系統修復時間法規跟各部門導入雲端服務備份重要數據等可行性項目，強化數位韌性。（投稿：2023 年 4 月 16 日；修訂：2023 年 6 月 27 日；接受：2023 年 7 月 5日）

參考文獻

一、中文部分

（一）專書

吳明璋，2018。《鋼索上的管理課：駭客、災變與多變動時代的韌性管理學》。臺北：大寫出版有限公司。

（二）期刊論文

李志強，2015/02。〈公務員保密範圍探討〉，《清流月刊》，第 23 卷第 8 期，頁 31-35。

謝翠娟、蔡君微，2020/12。〈後疫情時代韌性智慧政府運作思維〉，《國土與公共治理季刊》，第 8 卷第 4 期，頁 8-19。

（三）官方文件

行政院，2017/03/03。《中央主管機關訂定（修正）之個資檔案安全維護相關辦法》。

行政院，2021/08/11。《行政院及所屬各機關落實個人資料保護聯繫作業要點》。

行政院國家資通安全會報，2023/02/22。《行政院國家資通安全會報設置要點》。

行政院國家資通安全會報技術服務中心，2022/05。《國家層級資安風險評估方法簡介》。

林秀蓮、李世德，2014/11/14。《考察南韓、新加坡個人資料保護法制及相關專責機關》。臺北：法務部法律事務司。

財團法人國家實驗研究院國家高速網路與計算中心，2014/03。《電腦機房異地備援機制參考指引》。

財團法人資訊工業策進會，2015/07。《電子商務個資外洩資安防護參考指引》。

國家安全會議資通安全辦公室，2021/09。《國家資通安全戰略報告 — 資安即國安 2.0》。

國家運輸安全調查委員會，2020/11/10。《具敏感性或國安（含資安）疑慮之業務範疇》。

彭文暉，2021/04。《數位時代個資外洩事故之通知機制研究》。臺北：立法院法制局。

臺灣學術網路危機處理中心團隊，2019/03。《網頁置換攻擊事件分析報告》。

數位發展部資通安全署，2018/11/21。《公務機關資通安全事件通報應變程序範本》。

（四）研究計畫

葉奇鑫，2020。《韓國個人資料保護法制因應 GDPR 施行之調適委託研究計畫結案報告（計畫編號：PG10903-0166）》。臺北：國家發展委員會。

（五）網際網路

2022/12/30。〈詐騙 IT 王 1 ／架假官網、客製「變臉」賣 20 詐團，台工程師成亞洲難波萬〉，《周刊王》，<https://www.ctwant.com/article/229728>。

2023/01/24。〈Chinese/Lunar New Year 掀戰，中國網友出征〉，《華視新聞網》，<https://news.cts.com.tw/cts/international/202301/202301242135066.html >。

Domo，2022/10/21。〈何謂數位韌性〉，《Domo 的日常隨筆》，<https://vocus.cc/article/6348be2dfd89780001088e2b>。

T.H. Schee，2023/02/14。〈大量國民個資外洩是一種持續性的威脅 〉，《T.H. Schee》，<https://blog.schee.info/2023/02/14/massive-data-breach-and-persistent-threat/>。

UPAS 內網安全，盡在掌握，2020/12/15。〈從根本認識 ISO 27001，各行各業都適用的資安架構介紹〉，《UPAS 內網安全，盡在掌握》，<https://reurl.cc/4QqGpR>。

方璇，2022/12/31。〈南韓暫停發中國入境短簽，駐中使領館逾 6 成人感染〉，《壹蘋新聞網》，<https://tw.nextapple.com/international/20221231/D65134E018FF7FA82ACA859A293EB896>。

王能斌，2022/01/16。〈【新聞辭典】假旗行動〉，《中華民國國防部青年日報社》，<https://www.ydn.com.tw/news/newsInsidePage?chapterID=1477511&type=universal>。

行政院國家資通安全會報，2023/06/02。〈行政院國家資通安全會報組織架構〉，《數位發展部資通安全署》，<https://moda.gov.tw/ACS/nicst/organization/662>。

行政院新聞傳播處，2019/02/15。〈行政院資安長由副院長兼任，統籌國家整體資通安全政策〉，《行政院》，<https://www.ey.gov.tw/Page/9277F759E41CCD91/f25d6bc3-9c6d-4d40-91da-a7998fbc8c1a>。

李志鴻，2021/03/22。〈疫情時代，談營運持續管理 (ISO 22301) 之重要性〉，《中小企業綠色環保資訊網》，<https://green.pidc.org.tw/detail.php?lang=tw&type=4&id=297>。

林軒宇，2019/07/15。〈資通安全事件通報應變推動淺談（上）〉，《跨域資安強化產業推動計畫網站》，<https://www.acw.org.tw/Events/Detail.aspx?id=33>。

林曉慧、陳昌維，2023/03/29。〈數位發展部下設資通安全研究院，個資事件查處列重點〉，《公視新聞網》，<https://news.pts.org.tw/article/629803>。

法務部調查局公共事務室，2023/02/24。〈法務部調查局資安工作站偵辦戶役政資料遭竊案新聞稿〉，《法務部調查局》，<https://www.mjib.gov.tw/news/Details/1/839>。

邱倢芯，2023/03/29。〈數位部有資安署又有資安院，兩者怎麼分？〉，《科技新報》，<https://technews.tw/2023/03/29/moda-nics-2/>。

俞伯翰，2022/11/29。〈【觀點】一場 Kakao 之亂讓韓國停擺！企業怎麼防範？營運永續計畫 BCP 是什麼？》，《數位時代 》，<https://www.bnext.com.tw/article/72786/company-bcp-plan>。

韋萊韜悅，2019/07/11。〈全球數位韌性調查報告：能力與資源盤點〉，《韋萊韜悅》，<https://www.wtwco.com/zh-TW/Insights/2019/07/digital-resiliency-report>。

國家發展委員會國會及新聞聯絡中心，2022/07/29。〈我的資料，我作主，MyData 平臺試營運上線了！〉，《國家發展委員

會》，<https://www.ndc.gov.tw/nc_27_34301>。

張沛元，2023/01/26。〈挑農曆新年開戰，中國駭客猛攻南韓網站〉，《自由時報》，<https://news.ltn.com.tw/news/world/paper/1564013>。

陳凱俊，2023/05/14。〈阿共真的「打來了」！誠品買書竟接「詭異市調」爆個資外洩變統戰〉，《鏡週刊》，<https://www.mirrormedia.mg/story/20230514edi007/>。

黑客，2016/10/04。〈S 級黑客離不開的武器，社工庫。〉，《知乎》，<https://zhuanlan.zhihu.com/p/22754953>。

趙成美，2023/01/25。〈中國駭客組織駭入 12 個學術團體和研究機構，甚至攻擊政府機構〉，《韓國聯合通訊社》，<https://www.yna.co.kr/view/AKR20230125034053017?section=search&fbclid=IwAR1kOLS4O76rQ6XKmAW1qA1RlKjURUIyUHfngoTtOWZ8Y8kjeN87CdokNm8>。

領導力企業管理顧問有限公司，2016/11/02。〈ISO 31000 風險管理系統原理及指導綱要 Risk management–principles and guidelines〉，《領導力企業管理顧問有限公司》，<https://www.isoleader.com.tw/home/iso-coaching-detail/ISO31000>。

劉宇珊，2023/01/14。〈賴清德、林志玲等人驚傳個資外流！資料庫疑遭駭，華航回應了〉，《上報》，<https://www.upmedia.mg/news_info.php?Type=24&SerialNo=163971>。

劉榮、林俊宏，2019/07/03。〈【情報員個資洩光光】銓敘部遭駭手法曝光，與中國網軍「攻美護主」模式雷同〉，《鏡週刊》，<https://www.mirrormedia.mg/story/20190703inv007>。

數位發展部，2022/09/21。〈數位發展部的核心理念是「強化全民數位韌性」，什麼是「數位韌性」？〉，《數位發展部》，<https://moda.gov.tw/press/clarification/2512>。

鄭閔聲、史書華，2023/03/07。〈15 萬如何買下 2300 萬人？《天下》深入白帽駭客圈，還原個資賤售荒唐錄〉，《天下雜誌》，<https://www.cw.com.tw/article/5124927>。

二、 英文部分

（一）官方文件

Cho, Sungbaek, 2022/07. *National Cybersecurity Organisation*: *Republic of Korea.*

European Union Agency for Cybersecurity, 2011/02/11. *Resilience Metrics and Measurements: Challenges and Recommendations.*

IEEE, 2021/12/01. *White Paper - Digital Resilience IC Activity: Foundational Principles for Digital Resilience Framework.*

（二）網際網路

Cidon, Asaf, 2018/08/30. “Threat Spotlight: Barracuda Study of 3,000 Attacks Reveals BEC Targets Different Departments,” *Barracuda*, <https://blog.barracuda.com/2018/08/30/threat-spotlight-barracuda-study-of-3000-attacks-reveals-bec-targets-different-departments/>.

Deloitte, 2018. “Ramping Resilience in the Digital Age,” <https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/Ramping%20Resilience%20in%20Digital%20Age_Final%20

web.pdf>.

European Parliament, 2020. “Proposal for a Regulation of the European Parliament and of the Council on Digital Operational Resilience for the Financial Sector and Amending Regulations,” <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595>.

Fruhlinger, Josh, 2020/01/09. “What is a False Flag? How State-Based Hackers Cover Their Tracks,” CSO, <ttps://www.csoonline.com/article/3512027/what-is-a-false-flag-how-state-based-hackers-cover-their-tracks.html>.

Kim, So Jeong, and Sunha Bae, 2021/08/17. “Korean Policies of Cybersecurity and Data Resilience,” *Carnegie Endowment for International Peace*, <https://carnegieendowment.org/2021/08/17/korean-policies-of-cybersecurity-and-data-resilience-pub-85164>.

UK Council for Internet Safety, 2019/09/12. “Digital Resilience Framework,” <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/831217/UKCIS_Digital_Resilience_Framework.pdf>.