僅供委員問政所需參考
不代表本院意見或立場

編號：2711

議題研析

一、 題目：澳洲 2024 年網路安全法簡介

二、 議題所涉法規

資通安全管理法

三、 背景說明（緣起）

據報載[1]，除馬偕醫院 114[2]年 2 月 9 日遭勒索軟體攻擊，檔案被大規模加密，導致患者病歷資料無法開啟等情形外，彰化基督教醫院近日亦發生駭客攻擊，病毒取得主機管理權限後造成當機，致使院外掛號系統短暫失靈。

四、 問題爭點

我國資通安全管理法（下稱資安法）規範對象主要為公務機關，非公務機關部分，僅限於經中央目的事業主管機關核定之關鍵基礎設施提供者、公營事業及政府捐助之財團法人（下稱特定非公務機關）[3]。依資安法規定，公務機關知悉資通安全事件時，應通報上級或監督機關及主管機關[4]，特定非公務機關則應通報中央目的事業主管機關[5]。而一般企業因不在資安法適用範圍，發生資通安全事件並無通報義務。查澳洲 2024 年 11 月通過之 2024 年網路安全法（Cyber Security Act 2024，下稱網路安全法）則針對包括企業等實體

[1] 曾以寧，彰基遭駭客攻擊 衛福部：資安專家進駐、將報案，中央社，114 年 3 月 3 日。
[2] 本文有關年分之使用，原則以民國紀年表述，惟涉及外國法制或立法例部分，改採西元紀年表述。
[3] 資通安全管理法第 3 條、第 7 條第 1 項、第 16 條第 1 項規定參照。
[4] 資通安全管理法第 14 條第 2 項。
[5] 資通安全管理法第 18 條第 2 項。

（entity[6]）遭受勒索軟體攻擊且支付贖金者，賦予提交報告之義務[7]，爰簡介該規範重點，以供我國法制之參考。

五、探討研析

（一）澳洲網路安全法之立法背景與目的

澳洲為因應針對關鍵基礎設施之網路攻擊事件，於 2018 年制定 2018 年關鍵基礎設施安全法（The Security of Critical Infrastructure Act 2018），規定關鍵基礎設施發生網路安全事件時具有通報義務[8]；後為因應日益增長之網路安全威脅並補充現行法規範不足之處，遂依據 2023-2030 澳洲網路安全策略（2023-2030 Australian Cyber Security Strategy）之 7 項倡議陸續制定、修正相關法律，2024 年通過之網路安全法即為其中之一[9]。

（二）遭勒索軟體攻擊而支付贖金者應提出相關報告

考量遭遇勒索軟體攻擊時，支付贖金並未能保證資料之復原，爰澳洲政府雖未禁止支付贖金，惟明定一定規模之實體倘支付贖金，則應就該攻擊事件提交報告[10]。

1. 應提出報告之實體類型

依網路安全法第 26 條第 2 項、第 3 項及第 27 條第 1 項、第 5

---

[6] 依澳洲網路安全法第 8 條有關 entity 之定義，包括：個人、公司、合夥、設有管理機構之非法人團體、信託、關鍵基礎設施之責任實體。Section 8：” entity means any of the following：(a) an individual; (b) a body corporate;(c) a partnership;(d) an unincorporated association that has a governing body;(e) a trust;(f) an entity that is a responsible entity for a critical infrastructure asset.

[7] 李思萱，澳洲通過 2024 年網路安全法，期望強化社會整體網路安全保障，資訊工業策進會科技法律研究所，114 年 2 月，網址：https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&d=9296，最後瀏覽日期：114 年 3 月 10 日。

[8] 郭又華，首設部長級資安首長，澳洲如何用資安政策發揮國際影響力，iTHOME，111 年 11 月 22 日，網址：https://www.ithome.com.tw/news/154345，最後瀏覽日期：114 年 3 月 11 日。

[9] Australian Government Department of Home Affairs, Introduction of landmark Cyber Security Legislation Package, 9 Oct. 2024, website：https://www.homeaffairs.gov.au/news-media/archive/article?itemId=1247, last visited：Mar. 11 2025.

[10] 李思萱，同註 7。

項規定，澳洲政府要求於境內經營業務，且前一年度營業額達特定門檻[11]之實體，或符合 2018 年關鍵基礎設施安全法 2B 部分（Part 2B of the Security of Critical Infrastructure Act 2018）規定之關鍵基礎設施責任實體（responsible entity），倘於遭受勒索軟體攻擊時選擇支付贖金，應於支付或知悉支付贖金之 72 小時內向指定之聯邦機關（designated Commonwealth body）提出付贖報告（ransomware payment report），違反規定之實體將被處民事制裁金（civil penalty）。

2.付贖報告應包括之內容

依網路安全法第 27 條第 2 項規定，付贖報告應包括該支付贖金之實體之詳細資訊[12]及聯繫窗口（倘若贖金係由其他實體支付，則應提供該實體之相關資料）、敘明所發生之網路安全事件及對實體之

[11] 依 2025 年 2 月 27 日發布之網路安全（付贖報告）規則〔Cyber Security（Ransomware Payment Reporting）Rules 2025〕（下稱付贖報告規則）第 6 條規定，該營業額門檻為 300 萬澳幣，倘該實體前一年之營業並非完整年度，則依該條規定之公式計算門檻。Section 6：”(1) For the purposes of paragraph 26(3)(b) of the Act, the amount of turnover threshold for a business for the previous financial year is $3 million.(2)For the purposes of paragraph 26(3)(a) of the Act, if a business has been carried on for only part of the previous financial year, the turnover threshold for the business for the previous financial year is worked out using the formula：

$$\$3\text{ million} \times \frac{\text{Number of days in the part}}{\text{Number of days in the previous financial year}}\text{”}$$

[12] 依付贖報告規則第 7 條第 2 項及第 3 項規定，該資訊應包括地址，且該實體如有公司編號（Australian Business Number, ABN）應一併提供。Section 7：”(2)The reporting business entity’s contact and business details given for the purposes of paragraph 27(2)(a) of the Act must include the entity’s ABN (if any) and address.(3)The other entity’s contact and business details given for the purposes of paragraph 27(2)(b) of the Act must include the entity’s ABN (if any) and address.”

影響[13]、勒索者之要求[14]（包括贖金或其他）、贖金支付情形[15]、與勒索者間關於該事件、要求及贖金支付等之交涉情形與內容[16]。

3.付贖報告僅於特定情形下得予揭露或使用

依網路安全法第 29 條第 1 項及第 2 項規定，為保護該付贖或被勒索之實體，除為調查涉及違反本法與刑法之規定外，該報告不得作為調查該實體是否違反其他法律規定之用，且付贖報告內容僅於以下情形始得揭露或使用：

（1）為協助該付贖或被勒索之實體回應、緩解或解決該網路安全事件；

（2）涉及刑法第 137.1 條及第 137.2 條有關虛假與誤導性資訊及文件訴訟或第 149.1 條有關妨礙聯邦公職人員執行職務訴訟；

---

[13] 依付贖報告規則第 7 條第 4 項規定，該資訊應包括網路安全事件發生或可能發生之時間、受影響之實體知悉該事件的時間、對於實體之基礎建設與客戶之影響、受哪些勒索軟體或惡意軟體攻擊、該攻擊係利用實體之哪些漏洞、可協助聯邦或州機關解決或緩解該網路安全事件之資訊等。Section 7：”(4) The information about the cyber security incident, including its impact on the reporting business entity, given for the purposes of paragraph 27(2)(c) of the Act must include the following：(a) when the incident occurred or is estimated to have occurred; (b) when the reporting business entity became aware of the incident; (c) the impact of the incident on the reporting business entity’s infrastructure; (d) the impact of the incident on the reporting business entity’s customers; (e) what variants (if any) of ransomware or other malware were used; (f) what vulnerabilities (if any) in the reporting business entity’s system were exploited; (g) information that could assist the response to, mitigation or resolution of the cyber security incident by a Commonwealth body or State body.”

[14] 依付贖報告規則第 7 條第 5 項規定，該資訊應包括要求之金額、支付方式，倘若勒索者之要求並非金錢，則敘明要求之內容及交付方式。Section 7：”(5) The information about the demand made by the extorting entity given for the purposes of paragraph 27(2)(d) of the Act must include：(a) the amount or quantum of the ransomware payment demanded, or if the ransomware payment demanded is a non monetary benefit, a description of the ransomware payment demanded; and (b) the method of provision demanded.

[15] 依付贖報告規則第 7 條第 6 項規定，該資訊應包括實際支付之金額、支付方式，倘若勒索者之要求並非金錢，則敘明實際交付之內容及方式。Section 7：”(6) The information about the ransomware payment given for the purposes of paragraph 27(2)(e) of the Act must include: (a) the amount or quantum of the ransomware payment, or if the ransomware payment is a non monetary benefit, a description of the ransomware payment; and (b) the method of provision.”

[16] 依付贖報告規則第 7 條第 7 項規定，該資訊應包括彼此間溝通之性質與時間、溝通內容之簡要描述及相關協商過程之簡要說明。Section 7：”(7) The information about communications with the extorting entity relating to the incident, the demand and the ransomware payment given for the purposes of paragraph 27(2)(f) of the Act must include：(a) the nature and timing of any communications between the entity and the extorting entity; and (b) a brief description of those communications (if any); and (c) a brief description of any pre-payment negotiations undertaken in relation to the demand or the ransomware payment.”

（3）聯邦、州機關或國家網路安全協調員（National Cyber Security Coordinator）為履行有關網路安全事件之回應與解決等職務；

（4）向聯邦部長通報或提出網路安全事件建議；

（5）情報機關為執行其職務。

（三）比較法之借鏡及修法建議

隨網路科技發展，駭客攻擊手法亦日新月異，致使各種資安事件頻傳，其中政府機關及保有機敏資料、營業秘密或大量個人資料之企業或團體，更容易成為網路攻擊對象，主管機關倘能適時取得相關資訊，協助止損、或防止其他機關、企業或團體遭受類似攻擊，將有助於我國整體資安提升。查個人資料保護委員會籌備處已預告修正個人資料保護法，草案第 12 條規劃增訂非公務機關知悉發生個人資料侵害事故時，通報主管機關之義務[17]，考量網路安全事件並非皆涉及個人資料，爰建議主管機關參考澳洲網路安全法等相關規定，研議修正資安法，賦予一定規模以上企業如遭受勒索軟體攻擊而付贖等類型之重大網路安全事件時，應通報中央目的事業主管機關或主管機關之可行性，以促進我國整體資通安全保護。

撰稿人：陳育靖

[17] 公共政策網路參與平台，預告修正「個人資料保護法」部分條文，113 年 12 月 20 日，網址：https://join.gov.tw/policies/detail/4b6fdd7e-c73e-4028-b293-64a3b2427556，最後瀏覽日期：114 年 3 月 11 日。