簡介歐盟網路韌性法案

陳楷勛 編譯

摘要

歐盟執委會於今（2022）年 9 月 15 日提出「具備數位元素產品之水平網路安全要件與修訂第 2019/1020 號規則草案」，旨在提高具備數位元素產品於歐盟境內之網路安全與處理監管架構之問題。該規則草案規範於歐盟進出口或銷售之具備數位元素的產品，需要進行網路風險之評估，並於系爭產品的規劃、設計、開發、生產、運送及維護階段，考慮評估結果，以確保於系爭產品交付時沒有任何已知且可利用之漏洞，最後分別課予製造商、進口商、經銷商具體義務。為符合相關規定，該規則可能帶給中小型企業壓力並對其技術創新產生影響，亦可能阻礙整體數位市場的技術性進步，因此，立法者需於技術發展與監管之間建立合理之平衡。此規則草案目前仍在審查階段，其後續發展值得我們持續關注。

（取材新聞：Eduardo Ustaran et al., *The EU Cyber Resilience Act: What to Expect*, HOGAN LOVELLS (Oct. 4, 2022), https://www.engage.hoganlovells.com/knowledgeservices/viewContent.action?key=Ec8teaJ9VapDyLsVcvQMB17eOOGbnAEFKCLORG72fHz0%2BNbpi2jDfaB8lgiEyY1JAvAvaah9lF3dzoxprWhI6w%3D%3D&nav=FRbANEucS95NMLRN47z%2BeeOgEFCt8EGQ0qFfoEM4UR4%3D&emailtofriendview=true&freeviewlink=true; Scott Ikeda, *EU Cyber Resilience Act Primarily Aimed at Beefing Defenses of "Smart" Connected Devices*, CPO MAG. (Sept. 26, 2022), https://www.cpomagazine.com/cyber-security/eu-cyber-resilience-act-primarily-aimed-at-beefing-defenses-of-smart-connected-devices/.）

歐盟執委會於今（2022）年 9 月 15 日提出「具備數位元素產品之水平網路安全要件與修訂第 2019/1020 號規則草案（Proposal for a Regulation of the European Parliament and of the Council on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulation (EU) 2019/1020）」，即「網路韌性法案（EU Cyber Resilience Act）」（以下簡稱規則草案），旨在提高歐盟確保具備

數位元素的產品之網路安全與處理監管架構問題[1]。

由於全球多數國家未針對具備數位元素之產品，例如智慧與網路連線設備，設有管制，因此該類產品於全球流通時，其長久安全性相對被忽略[2]。此導致市場上充斥未受密碼保護之設備、無法更改之預設密碼、當漏洞出現時無法更新韌體或軟體設備、以及其他嚴重之安全漏洞，此均顯示該些設備在原始設計層面上缺乏對產品之長久安全性的重視。

再者，智慧與網路連線設備近年來越來越容易受到網路攻擊，至 2021 年，全球每年因網路犯罪所造成的損失預計達到 5.5 兆歐元[3]。因此，歐盟執委會推出「網路韌性法案」以強化此類設備之防禦機制[4]。

以下簡介規則草案的主要內容，接著評析本規則草案，最後作一結論。

壹、規則草案內容

以下分別介紹規則草案的規範範圍、草案規範之製造商、進口商與經銷商的具體義務、以及在規則草案下的執法措施。

一、規範範圍

規則草案對受規範之產品給予非常廣泛的定義：其指任何以連接至網路為目的或預期將連接至網路之軟體或硬體[5]。惟本規則草案亦排除特定產品之適用，例如受醫療器材法規範之醫療器材、或是專為國家安全或軍事目的開發之產品[6]。

二、製造商、進口商與經銷商之具體義務

規則草案之核心目的係為軟體與硬體產品之開發，制定一最低網路安全標準，並課予供應鏈之不同參與者相關的具體義務，其中包括製造商、進口商與經銷商

---

[1] European Commission Press Release IP/22/5374, State of the Union: New EU Cybersecurity Rules Ensure More Secure Hardware and Software Products (Sept. 15, 2022); *Proposal for a Regulation of the European Parliament and of the Council on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulation (EU) 2019/1020*, COM (2022) 454 final (Sept. 15, 2022) [hereinafter *Proposal for Cybersecurity Requirements for Products with Digital Elements*].

[2] *Proposal for Cybersecurity Requirements for Products with Digital Elements, supra* note 1, Explanatory Memorandum at 1.

[3] *Id*. Explanatory Memorandum at 1.

[4] European Commission Press Release, *supra* note 1.

[5] *Proposal for Cybersecurity Requirements for Products with Digital Elements*, *supra* note 1, art. 2(1).

[6] *Id*. arts. 2(2), 2(5).

[7]，以下分別簡介之：

（一）製造商

相關產品之製造商（包括開發商）承擔最主要之義務，其被要求確保產品滿足必要的網路安全要件，主要包含一系列之技術標準以及與之並行的其它組織與治理要件[8]。

具體來說，根據規則草案：製造商首先必須確保其產品接受與產品相關的網路安全風險評估[9]。第二，製造商須在產品的規劃、設計、開發、生產、運送及維護階段，考慮到前述所進行之風險評估結果，以盡量降低網路安全風險，並預防網路安全事件之發生及降低相關事件之影響[10]。第三，製造商須於產品交付時確保沒有任何已知可利用之漏洞，並具備適當之政策與程序以檢測與修復潛在漏洞[11]。第四，製造商須提供產品之安全資訊與說明，為其使用者提供透明之資訊[12]。

此外，製造商尚須執行符合性評估程序，而根據產品的類型、是否遵循調和標準、及通用規範或歐洲網路安全驗證規範，將適用不同的符合性評估程序[13]。再者，製造商須確保其產品具備 CE 標誌，並在使用來自第三方零件之情況，記錄其措施並對供應商進行盡職調查[14]。

最後，為確保產品生命週期之安全性，製造商必須具備處理安全漏洞的程序，包含解決與修復漏洞、以及向歐盟網路與資訊安全局（European Union Agency for Cybersecurity）與用戶報告其檢測到之漏洞或安全事件[15]。

（二）進口商

[7] *Id*. Explanatory Memorandum at 9.
[8] *Id*. art. 10(1).
[9] *Id.* art. 10(2).
[10] *Id.* art. 10(2).
[11] *Id*. art. 10(6).
[12] *Id.* art. 10(10).
[13] *Id*. arts. 10(7), 24(1)-(3).
[14] 「CE 標誌」係指製造商用來表明相關產品符合歐盟規定之安全、健康及環境保護要件的標誌。*CE Marking*, EUR. COMM'N, https://ec.europa.eu/growth/single-market/ce-marking_en (last visited Nov. 25, 2022); *Proposal for Cybersecurity Requirements for Products with Digital Elements*, *supra* note 1, arts. 10(4)-(5), 10(7).
[15] *Id.* arts. 10(6), 11(1), 11(4).

進口商僅能進口符合最低要求之產品[16]，其須驗證製造商是否進行符合性評估、是否具備正確之技術文件、與產品是否具備正確之認證[17]。

（三）經銷商

經銷商應謹慎行事以符合規則草案之要件，其負有驗證產品是否具備 CE 標誌之義務，且需確認製造商與進口商是否遵循其義務[18]。

三、執法措施

不遵守關鍵網路安全要件之經濟營運商將被處以最高 1500 萬歐元、或其前一財政年度全球總營業額之 2.5%的行政罰鍰，並以前述較高者為計算標準[19]。

規則草案之監督與執行預計由各歐盟成員國指定之主管機關負責[20]。該些機關在遇有產品不合規的狀況時，得要求相關營運商採取適當改善措施以符合規則草案之要件、將產品於市場中下架、或於合理期限內將其從市場召回[21]。

貳、評析

倘若歐洲議會與理事會通過此規則草案，製造商將需調整全球產品線以符合歐盟的必要標準，此舉可能會使其它地區的使用者從中受益。

雖然規則草案並非第一個專為連接裝置立法之規則，但先前立法，像是 2018 年要求智慧設備啟用安全密碼的加州法律，傾向於解決特定漏洞，而非於產品設計原型時訂定「安全設計」之方法[22]。因此，與先前關於連接裝置之立法對比，如果規則草案通過，其將是目前全球最強而有力且全面之規則。

另一方面，有論者認為，規則草案距離通過依舊遙遠，因規則草案可能為中小型企業帶來不成比例之壓力，並可能對技術創新產生影響。

---

16 *Id.* art. 13(1).
17 *Id.* art. 13(2).
18 *Id.* art. 14(2).
19 *Id.* art. 53(3).
20 *Id.* art. 41(2).
21 *Id.* art. 47(2).
22 CAL. CIV. CODE §1798.91.04 (b) (2018); Tim Sandberg, *California SB-327: The Security of Connected Devices*, GALEN DATA (Sept. 26, 2022), https://www.galendata.com/california-sb-327-the-security-of-connected-devices/.

歐盟立法者針對連接至歐盟市場之裝置或網路的所有硬體與軟體產品制定規則，並適用於所有歐盟成員國為一合理之舉。倘若任一此類產品存有安全漏洞，其將影響歐盟針對網路攻擊所作之防禦的有效性。

儘管人們需要強而有力且具一致性之網路安全標準以減少數位產品之漏洞，但因中小型企業必須滿足規則草案之嚴格要件方得將數位產品引入歐盟市場，故為符合規則草案所致之合規成本可能會使其等難以於數位市場競爭。此外，規則草案可能將阻礙技術進步。是故，立法者需於監管中取得一適當平衡以確保網路安全免受威脅，並同時允許及鼓勵新興且不斷進步之數位產品開發。

歐盟議會與理事會將審查規則草案並討論其可能之修正案[23]。一旦歐盟立法者同意並通過本規則草案，其將於兩年後實施，惟關於漏洞通知義務則例外地將在法案通過一年後開始適用[24]。此外，過渡規則將適用於某些產品上，包括已獲網路安全要件之證明或核可之產品、適用其他歐盟立法之產品、或是在本法案適用前已銷售於歐盟市場之產品[25]。

參、結論

規則草案為具備數位元素產品之網路安全與監管之一大進展，歐盟透過制定一最低網路安全標準，以及課予供應鏈之不同參與者相關的具體義務，以期強化該些產品之網路防禦機制，減少網路犯罪之問題發生。然而，規則草案所規範之要件相當嚴苛，對中小型企業來說，合規成本勢必會增加，使其等難以於數位市場競爭，此為歐盟立法者應考量之事項。本規則草案尚須經歐盟議會與理事會正式批准後方能生效，而在正式生效以前，規則草案之規範內容是否有所變動，值得持續關注。

[23] European Commission Press Release IP/22/5374, *supra* note 1.
[24] *Proposal for Cybersecurity Requirements for Products with Digital Elements*, *supra* note 1, art. 57.
[25] *Id.* arts. 55(1)-(2).