簡介歐盟資通安全規則

黃意晴 編譯

摘要

今（2019）年 4 月 17 日歐洲議會與歐盟理事會共同簽署資通安全規則。本規則有兩大要點：（一）賦予歐盟網路與資訊安全局更多任務與資源以強化其功能，如協助執委會及各成員國資通安全政策的發展與執行等；（二）為資通訊科技產品、服務及程序，建立自願性的歐盟資通安全認證框架，經認可之符合性評估機構所發行的認證將受到所有歐盟成員國的承認，藉此提高受認證產品之信賴度。另外，資通安全規則之實施亦能鼓勵企業在設計及預設原廠設定的階段，達到安全、簡單及值得信賴的程度。最後，資通安全規則亦可加強歐盟與其他國家以及國際組織在資安方面之合作。

（取材自：Mar Negreiro, *ENISA and a New Cybersecurity Act*, EUROPEAN PARLIAMENT THINK TANK (Feb. 26, 2019), http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/614643/EPRS_BRI(2017)614643_EN.pdf.）

歐盟執委會（European Commission，以下簡稱執委會）於 2017 年 9 月 13 日提出「網路與資訊安全局暨資通訊科技之資通安全認證規則（Regulation of the Parliament and of the Council on ENISA and on Information and Communication Technology Cybersecurity Certification，以下簡稱資通安全規則）」之草案[1]。該草案於今（2019）年 4 月 17 日由歐盟理事會（Council of the European Union）與歐洲議會（European Parliament）共同簽署[2]。

本篇所編譯之歐洲議會智庫報告，雖是撰寫於規則通過前，惟其所根據之草案版本與上述簽署版本並無不同，故其研析仍具參考價值。以下將依之簡介資通安全規則之立法進程與重點，並說明可能帶來的影響。

壹、資通安全規則之立法進程

2017 年 9 月，執委會通過一資通安全套案，採取新的措施以進一步改善歐

[1] *Commission Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and Repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification ("Cybersecurity Act")*, COM (2017) 477 final (Sept. 13, 2017) [hereinafter Proposal of Cybersecurity Act].

[2] EUR-Lex, *Procedure 2017/0225/COD*, https://eur-lex.europa.eu/procedure/EN/2017_225 (last visited May 9, 2019).

盟網路之防護、對威脅之嚇阻（deterrence），以及自身的防禦力[3]。作為上述新措施之一部，執委會提出資通安全規則草案，以強化歐盟網路與資訊安全局（European Union Agency for Network and Information Security, ENISA）之功能[4]。

2016 年「網路與資訊系統安全指令（Directive 2016／1148）」通過後[5]，原預期 ENISA 將在歐盟資通安全領域扮演更廣泛之角色，但其卻受到現有權限與資源之限制。對此，執委會提出一個具有企圖心的改革草案，包含賦予 ENISA 永久性權限，確保其不僅可以一如既往地提供專業建議，亦能夠執行營運型任務[6]。該規則草案亦預計為資通訊科技（Information and Communication Technology, ICT）產品建立首個自願性的歐盟資通安全認證框架（以下簡稱資安認證框架），而 ENISA 也將於其中扮演重要角色[7]。

2018 年 12 月，歐洲議會、歐盟理事會以及執委會，就執委會上述所提出之資通安全規則草案達成非正式的政治性協議[8]。今年 3 月 12 日，歐洲議會通過其一讀立場[9]，而歐盟理事會亦於 4 月 9 日通過該規則[10]。雙方並於 4 月 17 日共同簽署，此規則將於公布 20 天後生效[11]。

貳、資通安全規則主要內容

如前所述，資通安全規則將加強 ENISA 之功能，並建立一個自願性的 ICT 資安認證框架，以下分述這些變革內容。

---

[3] *Commission Joint Communication to the European Parliament and the Council ─Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU*, JOIN (2017) 450 final (Sept. 13, 2017).

[4] Proposal of Cybersecurity Act, at 2.

[5] Directive 2016/1148, of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union, 2016 O.J. (L 194) 1.

[6] Proposal of Cybersecurity Act, at 6.

[7] Regulation of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act), art. 4.6, EUR. COUNCIL DOC. PE-CONS 86/1/18 REV 1 (Apr. 17, 2019), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:PE_86_2018_REV_1&from=EN [hereinafter Cybersecurity Regulation]; 由於截至本篇發刊日為止，該規則尚未刊登於歐洲公報，故以歐洲議會與歐盟理事會共同簽署之文件為引註來源。

[8] European Commission Press Release IP/18/6759, EU Negotiators Agree on Strengthening Europe's Cybersecurity (Dec. 10, 2018).

[9] European Parliament Legislative Resolution of 12 March 2019 on the Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and Repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification (“Cybersecurity Act”), EUR. PARL. DOC. P8_TA-PROV (2019) 0151, http://www.europarl.europa.eu/doceo/document/TA-8-2019-0151_EN.pdf.

[10] Council of the European Union Press Release 281/19, Legislative Acts Adopted by the General Affairs Council (Apr. 9, 2019), https://www.consilium.europa.eu/en/press/press-releases/2019/04/09/legislative-acts-adopted-by-the-general-affairs-council/pdf.

[11] Cybersecurity Regulation, art. 69.1.

一、改革歐盟網路與資訊安全局

除了協助成員國發展「電腦安全事件應變小組（Computer Security Incident Response Team, CSIRTs）」以完善網路與資訊系統安全指令賦予其之職責外，ENISA 在如營運上的合作與 ICT 安全認證等領域，亦被賦予新的權限與資源，以反映資通安全之新現實與需求[12]。具體而言，ENISA 將負責六種不同類型的工作：

（一）ICT 資安認證框架下的市場相關任務：包含在專家協助及國家認證機構的密切合作下，準備歐盟資安認證計畫的方案，並將由執委會採納[13]。ENISA 亦將協助 ICT 標準化的政策發展[14]；

（二）政策發展與執行：其目標是在更大程度上協助執委會及成員國發展、執行與檢討一般資通安全政策，以及經網路與資訊系統安全指令所指出如能源、運輸及金融等關鍵策略部門之資通安全政策[15]；

（三）能力建構：ENISA 將加強協助成員國改善如預防與因應事件之能力與專業[16]；

（四）知識與資訊：ENISA 將提供分析與建議並提高資安意識，以便成為歐盟機構與組織中資安資訊的單一窗口[17]；

（五）ENISA 將主管歐盟層級的 CSIRTs 秘書處，且將依成員國之請求協助處理資安事件[18]；

（六）ENISA 將處理大規模的資安事件[19]。

ENISA 改造後的權限、目標與任務將受到定期檢討[20]。同時，ENISA 將舉辦一年一度的泛歐資安演習，且藉由建立資訊共享與分析中心，改善網路威脅情報與知識之分享[21]。除此之外，其也將在即將出爐之關於資安危機合作的資安藍圖中扮演一定的角色，同時也會針對歐盟機構在資安方面的研究需要，提供建議給

12 *Id.* arts. 6.1(d), 7, 8.
13 *Id.* arts. 49.1, 49.5, 49.7.
14 *Id.* art. 8.1(a).
15 *Id.* art. 5.
16 *Id.* art. 6.
17 *Id.* art. 9.
18 *Id.* arts. 7.3, 7.4.
19 *Id.* art. 7.7.
20 *Id.* art. 67.1.
21 *Id.* art. 7.5, recital (29).

歐盟資安研究與技術中心[22]。

二、建立資安認證框架

ENISA 的新權限亦包括協助發展受各成員國承認之自願性歐盟認證框架，此認證之目的係在確認產品與服務是資安無虞的[23]。認證框架將利用一套包含規定、技術性要求、標準及程序的全面性內容，來制定泛歐的認證計畫[24]。這將基於歐盟層級對於特定 ICT 產品或服務之安全屬性的評估協議[25]。由於資通安全規則確立了歐盟層級的認證計畫位階高於各國現行的認證計畫，因此經確認符合上述要求而產生之認證將被所有成員國承認[26]。

歐盟資安認證計畫係由 ENISA 透過「歐洲資安認證小組（European Cybersecurity Certification Group, ECCG）」之協助與專業建議，同時與該小組密切合作下所草擬，且經執委會通過後將逕付執行[27]。當出現資安認證計畫之需求，執委會就會要求 ENISA 為特定 ICT 產品及服務草擬計畫[28]。ENISA 會與 ECCG 中之各成員國認證監理機關代表密切合作，以草擬資安認證計畫[29]。成員國與 ECCG 亦可主動向執委會提議，要求 ENISA 草擬特定產品或服務的資安認證計畫[30]。

一旦某項歐盟資安認證計畫獲得通過，ICT 產品製造商或 ICT 服務供應商將能夠向其自行選擇之符合性評估機構，提交產品或服務認證之申請[31]。符合性評估機構的資格效期最長為五年，但只要其符合要求，便得以相同的條件更新其資格效期[32]。

參、可能的重要影響

歐洲議會對於該規則提出之意見，有些值得注意之處：

（一）資通安全規則提供企業得以在產品設計及開發的最初階段，適用各種自願性安全措施的機會。這將加強 ICT 產品、服務及程序在歐盟所獲得的信賴，而被

[22] *Id.* art. 11(a).
[23] *Id.* art. 8.1.
[24] *Id.* arts. 2(9), 52.4.
[25] *Id.* recitals (68), (69).
[26] *Id.* arts. 53.5, 56.10.
[27] *Id.* art. 49.
[28] *Id.* art. 48.
[29] *Id.* arts. 49.5, 62.2.
[30] *Id.* art. 48.2.
[31] *Id.* recital (97).
[32] *Id.* art. 60.4.

稱為「設計的安全（security by design）」[33]；

（二）資通安全規則也鼓勵企業在預設 ICT 產品、服務及程序的原廠設定時，便讓該等配置達到簡單、值得信賴與安全的程度，使消費者不需具備廣泛的設定知識或技術理解就能使用，此被稱為「預設的安全（security by default）」[34]；

（三）網路威脅為一全球性問題，而更密切的國際性合作對於改善資通安全標準至關重要，此將有賴於採用共同行為準則、資訊共享、使用國際標準及全球規模的合作。因此，在歐盟資通安全規則下，ENISA 的主要任務將是增強歐盟與第三國及國際組織的合作[35]。

[33] *Id.* recital (12).
[34] *Id.* recital (13).
[35] *Id.* recital (43).