

日本內閣府研議「網路資訊安全判斷基準草案」並將作為未來機關處理共同標準



日本內閣府網路安全戰略本部（サイバーセキュリティ戰略本部）於2017年7月13日第14次會議中提出對2020年後網路安全相關戰略案之回顧（2020年及びその後を見据えたサイバーセキュリティの在り方（案）－サイバーセキュリティ戰略中間レビュー－），針對網路攻擊嚴重程度，訂立網路安全判斷基準（下稱本基準）草案。對於現代網路攻擊造成之嚴重程度、資訊之重要程度、影響範圍等情狀，為使相關機關可以做出適當之處理，進而可以迅速採取相應之行動，特制訂強化處理網路攻擊判斷基準草案。其後將陸續與相關專家委員討論，將於2017年年底發布相關政策。

本基準設置目的：為了於事故發生時，具有視覺上立即判斷標準，以有助於事故相關主體間溝通與理解，並可以做為政府在面對網路侵害時判斷之基準，成為相關事件資訊共享之體制與方法之基準。

本基準以侵害程度由低至高，分為第0級至第5級。第0級（無）為無侵害，乃對國民生活無影響之可能性；第1級（低）為對國民生活影響之可能性低；第2級（中）為對國民生活有影響之可能性；第3級（高）為明顯的對國民生活影響，並具高可能性；第4級（重大）為顯著的對國民生活影響，並具高可能性；第5級（危機）為對國民生活廣泛顯著的影響，並具有急迫性。除了對國民及社會影響，另外在相關系統（システム）評估上，在緊急狀況時，判斷對重要關鍵基礎設施之安全性、持續性之影響時，基準在第0級至第4級；平常時期，判斷對關鍵基礎設施之影響，只利用第0級至第3級。

本次報告及相關政策將陸續在一年內施行，日本透過內閣府網路安全戰略本部及總務省、經濟產業省與相關機構及單位之共同合作，按照統一之標準採取措施，並依據資訊系統所收集和管理之資料作出適當的監控及觀測，藉由構建之資訊共享系統，可以防止網路攻擊造成重大的損失，並防止侵害持續蔓延及擴大，同時也將為2020年東京奧運會之資訊安全做準備。我國行政院國家資通安全會報目前公布了「國家資通安全通報應變作業綱要」，而日本以國民生活之影響程度標準列成0至5等級，其區分較為精細，且有區分平時基準及非常時期基準等，日本之相關標準可作為綱要修正時之參考。

相關連結

- [1.日本內閣府，內閣サイバーセキュリティセンター](#)
- [2.內閣サイバーセキュリティセンター，2020年及びその後を見据えたサイバーセキュリティの在り方～サイバーセキュリティ戰略中間レビュー～，頁6](#)

你可能會想參加

- 製造業及技術服務業個資保護及資安落實－經濟部工業局112年企業個人資料保護暨資訊安全宣導說明會
- 【已額滿】2023科技研發法制推廣活動－科專個資及反詐騙實務講座
- 供應鏈資安國際法制與政策趨勢分享會
- 【實體】數位發展部數位經濟相關產業個資安維辦法說明會（南部場）
- 【線上】數位發展部數位經濟相關產業個資安維辦法說明會（南部場）
- 商業服務業個資保護宣導說明會
- 【實體】2024科技研發法制推廣活動－科專個資及反詐騙實務講座
- 【直播】2024科技研發法制推廣活動－科專個資及反詐騙實務講座
- 數位發展部數位產業署113年資訊服務業者個資安維辦法宣導說明會

蕭仁豪

法律研究員 編譯整理

上稿時間：2017年08月

資料來源：

- 1.日本内閣府，内閣サイバーセキュリティセンター，<http://www.nisc.go.jp/conference/cs/>（最後瀏覽日：2017/08/14）。
- 2.内閣サイバーセキュリティセンター，2020年及びその後を見据えたサイバーセキュリティの在り方～サイバーセキュリティ戦略中間レビュー～，頁6，<http://www.nisc.go.jp/conference/cs/taisaku/ciso/dai13/pdf/13shiryu01.pdf>（最後瀏覽日：2017/08/14）。

文章標籤

推薦文章