## 二、零信任架構概念

零信任架構的主要精神，是基於「永不信任、持續驗證」的方式，透過持續、多種類的驗證手段，持續強化對系統或資料存取控制的安全性。目前主要參考文件如下：

(一)2020 年美國國家標準技術研究院(NIST)發布SP 800-207 文件[1]，提出身分鑑別、設備鑑別及信任推斷等 3 大核心組件，並且以身分鑑別為優先導入範圍。

(二)2021 年美國總統發布指令[2]，要求美國聯邦政府採用零信任架構，作為資通安全現代化策略之一。2022 年 1 月，美國預算與管理辦公室制定備忘錄[3]，要求各機構在 2024 財年(FY) 年底前，於身分識別、設備、網路、應用程式與工作負載、資料等 5 個面向滿足特定的安全標準和目標。

(四)2023 年 4 月美國網路安全暨基礎設施安全局(Cybersecurity and Infrastructure Security Agency, CISA)發布零信任成熟度模型 2.0[4]，依身分識別、設備、網路、應用程式與工作負載、資料等五支柱；至自動化與協調、可視性及分析則內含於各支柱中。因應逐步漸進之導入過程，區分傳統、起始、進階、最佳化等四個等級。

(五)我國行政院第六期「國家資通安全發展方案(110 年至 113 年)」之推動策略，數位部資安署將發展零信任網路資安防護環境，並優先推動A級公務機關導入試辦。規劃自 111 年起，分年依序導入身分鑑別、設備鑑別、信任推斷等階段，並陸續訂定身分鑑別、設備鑑別、信任推動等產品標準並受理廠商申請產品驗測[5]。

[1] https://csrc.nist.gov/pubs/sp/800/207/final
[2] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[3] https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf
[4] https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf
[5] https://www.nics.nat.gov.tw/ZeroTrustMain.htm?lang=zh