

軟體物料清單 (SBOM) 白皮書

建構可信賴的軟體供應鏈安全防線

日期：2026 年 9 月

白皮書摘要

隨著數位轉型加速與開源軟體 (Open Source Software, OSS) 的廣泛應用，軟體供應鏈安全 (Software Supply Chain Security) 已成為全球組織或企業資安防禦的核心議題。觀察商用軟體高度依賴第三方元件，任何微小的開源元件弱點都可能演變成系統性風險。為提供安全軟體架構與服務，網擎資訊 (Openfind) 積極回應軟體供應鏈資安政策，已落實導入軟體物料清單 (Software Bill of Materials, SBOM) 管理機制，關注軟體第三方元件風險，結合持續監控與資安治理框架，建構可信賴的軟體供應鏈安全防線。

供應鏈安全的挑戰

軟體第三方元件風險

軟體開發隨技術的演進，開源套件與第三方函式庫提供了快入功能擴充性與開發能力。然而，根據國際權威市調機構 Gartner 統計與預測，全球近半數 (45%) 組織正面臨軟體供應鏈攻擊的直接威脅，供應鏈風險管理已成企業首要挑戰。根據非營利組織 Linux 基金會 (Linux Foundation) 與 OpenSSF 調查顯示，商用軟體中 70% 至 90% 皆由開源及第三方元件構成，且超過 80% 的應用程式存在間接相依性 (Transitive Dependencies)，導致多數漏洞隱藏間接相依元件的安全盲點。而帶來的資安風險主要來自三個層面：

1) 元件已知或零日 (Zero Day) 漏洞

軟體開發過程中，開發者直接引用未經過濾或包含安全缺陷的第三方元件，將使系統暴露於高度資安風險中，攻擊者利用公開的漏洞資料庫 (如 CVE) 針對舊版本發動攻擊。而當開源套件因年代久遠，原廠或原作者已停止維護支援，導致漏洞無法修補。

2) 軟體供應鏈遭惡意攻擊或勒索

攻擊者入侵第三方套件的官方資料庫、釋出版本或維護者帳號，植入惡意後門或勒索程式。讓開發者誤載名稱相似的惡意套件，或是透過自動化建置與更新流程載入外部元件時遭到攔截或竄改。

3) 缺乏識別風險範圍與管理機制

軟體開發商或建置團隊無法完整盤點系統內的所有元件安全狀況，同時在漏洞發生時，無法在期望時間內確認損害範圍，甚至軟體版本管理缺乏持續監控與更新機制。

外部攻擊面風險

從外部攻擊面管理（ External Attack Surface Management, EASM ）角度，透過實際的檢測調查發現，許多企業在部署與維運資安系統時，面臨嚴重的「風險盲點」問題：

1) 未監控的第三方元件比例偏高

實測顯示許多企業內部伺服器運行的軟體，有超過 60% 無法清楚列出其引用的開源套件版本與來源，形成資安防守盲區。

2) 漏洞修復時程延滯：

當國際發布高風險 CVE 漏洞時，企業往往缺乏元件清單，平均需要花費 2 至 4 週的時間進行人工清查與影響評估，錯失資安關鍵防禦時機。

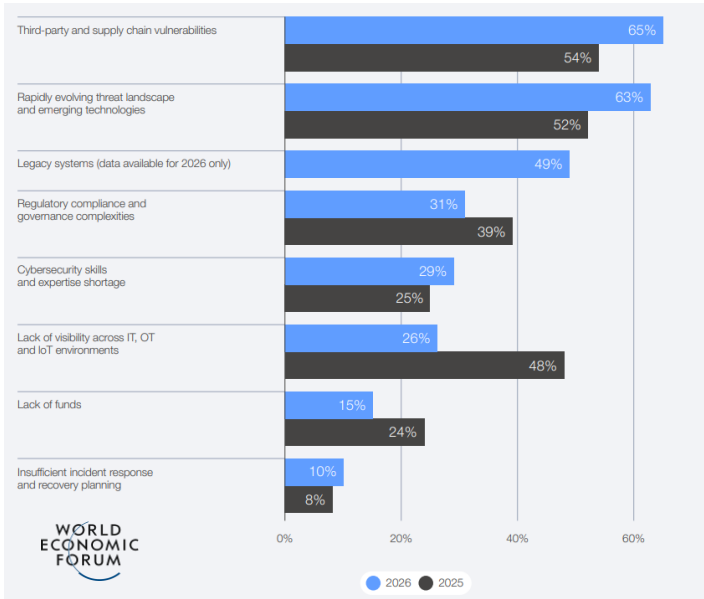
3) 外部攻擊面管理（ EASM ）缺口：

外部資安掃描工具能偵測暴露的服務端口，但無法掌握軟體內部的隱性函式庫漏洞，導致「外部無告警、內部已滲透」的風險。

組織韌性與供應鏈安全

世界經濟論壇（ WEF ）《2026 年全球網路安全展望》指出，地緣政治仍是影響全球網路風險的首要因素。約 64% 的組織已將具地緣政治動機的網路攻擊納入風險考量，例如關鍵基礎設施破壞與網路間諜活動。在組織網路安全韌性方面，供應鏈安全的重要性持續上升。調查顯示，「第三方與供應鏈脆弱性」已成為大型企業面臨的主要障礙，比例由 2025 年的 54% 上升至 2026 年的 65%，顯示企業的資安風險已不再侷限於自身環境，整體供應鏈的防護能力，正逐漸成為企業網路安全韌性的關鍵。

圖：Large companies' greatest barriers to cyber resilience, 2025–2026

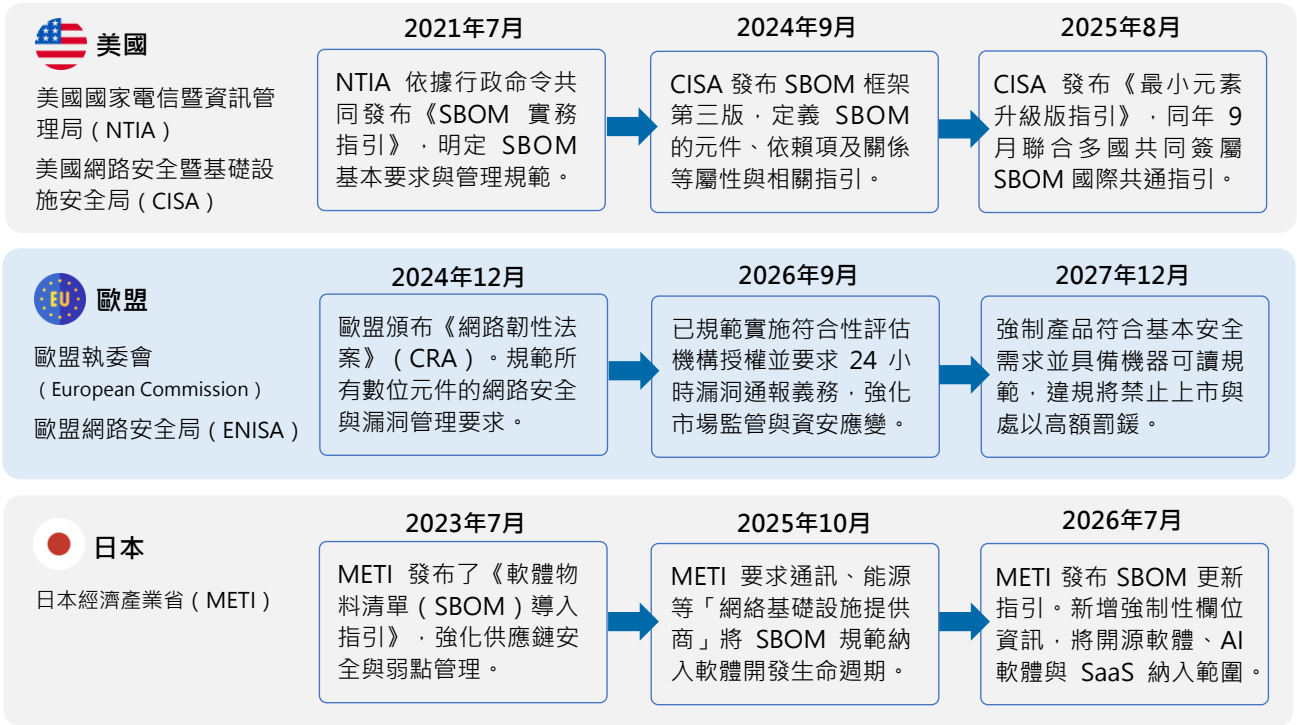


企業資安防護邊界已從「保護自己」逐步延伸至「確保供應鏈安全與韌性」。隨著企業軟體開發與服務架構日益複雜，第三方元件、開源軟體及外部服務已陸續成為企業供應鏈的重要環節。一旦供應鏈中的元件存在漏洞或遭受攻擊，風險可能快速擴散至下游產品與客戶。因此，企業除了強化自身防禦能力，也需要建立完整的供應鏈風險管理機制，透過 SBOM 掌握軟體組成與依賴關係，搭配弱點掃描、持續監控及安全軟體開發管理，提升漏洞發現、影響評估與修復效率，進一步強化整體資安韌性。

軟體物料清單規範

國際政策的推動

全球主要國家已相繼提升軟體供應鏈安全至國家安全層級，將 SBOM 列為軟體採購與資安合規的強制要求，觀察美國、歐盟與日本政策如下：



資料來源：Openfind 整理

台灣政策的引導

台灣政府為強化國家數位韌性，由數位發展部 (MODA) 數位產業署與財團法人資訊工業策進會 (III) 帶頭推動軟體供應鏈安全政策，並將 SBOM 納入實務管理機制。

國家資通安全發展方案 (2025-2028)

國際接軌 × SBOM導入

導入 SSDLC 與 SBOM、強化軟體透明度與安全、與美日歐共享資安情資。

國家資通安全戰略 (2025)

供應鏈安全 × 主動防禦

建立主動防禦體系、推動「信任供應鏈」、接軌美國、歐盟 CRA。

政府共同供應契約 (2026)

SBOM 強制要求

中/高風險系統需提供 SBOM、作為採購與驗收必要文件。

- 1) 數位發展部數位產業署「軟體資安品質指引」

指引中特別強調，採購單位應優先選用在開發階段落實安全軟體開發流程，且具備標準化 SBOM 產出與管理能力之軟體服務商，以落實軟體元件透明度管理，有效降低潛在的供應鏈安全風險。
- 2) 財團法人資訊工業策進會「軟體產品元件表規範」

遵循國際 NTIA 與 CycloneDX/SPDX 標準，建立國內軟體元件表欄位規範，要求供應商揭露組件名稱、版本、供應商與授權證明，輔導企業建立供應鏈透明度，落實 SBOM 管理規範。

遵循與落實

Openfind 全面將 SBOM 建立與維護機制融入安全軟體開發生命週期 (Secure Software Development Life Cycle, SSDLC) 確保所有交付給客戶的軟體均具備透明性與可追溯性。

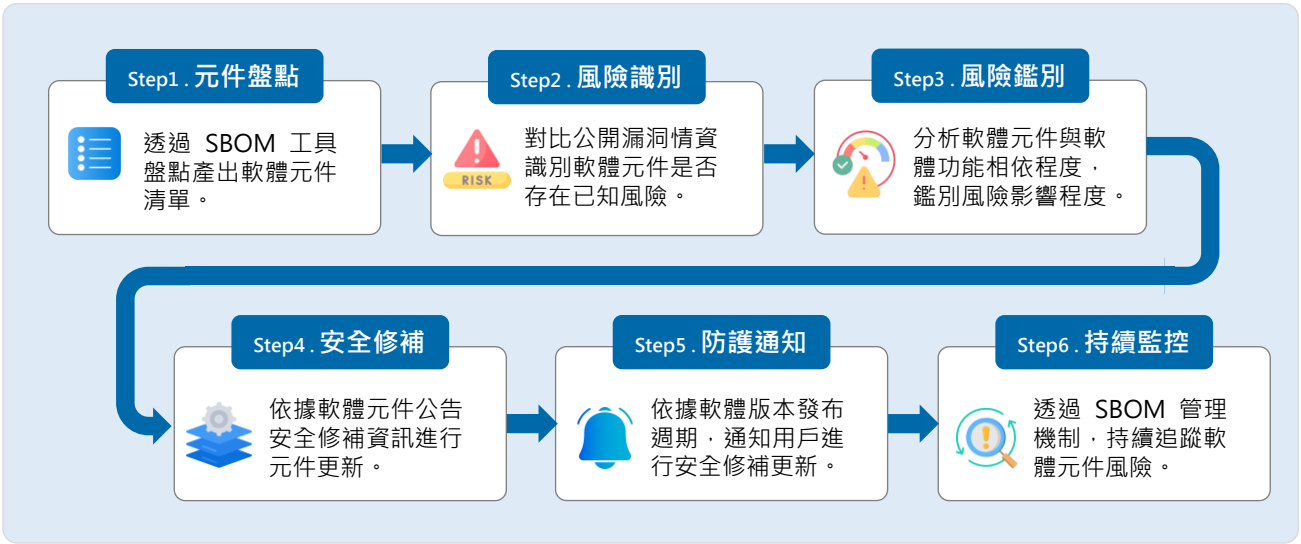
揭露原則與交換格式

軟體物料清單之資訊揭露機制，遵循數位發展部數位產業署《軟體資安品質相關指引》並參考財團法人資訊工業策進會《軟體產品元件表規範》，提供元件名稱、使用版本、元件來源、授權類型以及風險說明。資料交換格式支援 CycloneDX 、SPDX 等國際標準規範。

欄位名稱 (Field Name)	範例與說明 (Example Description)
元件名稱 (Library Name)	揭露完整名稱，例如：Apache HTTPD
使用版本 (Version)	揭露版本號碼，例如：2.4.68
元件來源 (Package Source)	揭露來源，例如：https://downloads.apache.org
授權類型 (License Type)	揭露授權，例如：Apache-2.0
風險說明 (Risk Status)	揭露安全性，例如：穩定安全版本，於 2026 年 6 月 8 日發布

軟體元件風險管理流程

組織建立風險管理流程，遵循管理循環 (PDCA) 從盤點、驗證、改善到持續監控，確保軟體供應鏈安全。首先，透過自動化 SBOM 工具進行全面盤點，產出對應的軟體物料清單，隨後進入風險識別與風險鑑別。技術團隊依據公開的漏洞情資，識別是否存在已知風險，並深度分析軟體元件與整體功能的相依程度，鑑別風險的實質影響範圍。確認風險後，隨即啟動安全修補，進行元件更新與弱點修復。修補完成後，配合軟體版本的發布週期，主動通知用戶進行安全修補更新，並透過常態化管理機制，持續追蹤軟體元件風險。



軟體元件安全評估

當技術團隊偵測到第三方元件存在安全性漏洞 (CVE) 時，將立即啟動「軟體元件可利用性評估機制」進行深度分析。本機制的核心在於透過嚴謹的「識別 (Identification)」與「鑑別 (Triage & Analysis)」程序，精準判定該漏洞是否會對產品的實際執行環境造成實質資安風險，進而評估其「漏洞可利用性 (Exploitability)」。在實務分析中，評估流程將區分為兩大路徑：

1) 驗證與風險排除

若經技術團隊驗證，該漏洞在產品現有的系統架構與業務邏輯中，完全無法被外部觸發，或者產品本身已具備完善的隔離與防護機制，則該漏洞將被判定為「無實質威脅」。團隊會將該軟體元件版本標註為「穩定安全版本」，產品安全不受影響，避免客戶產生警報疲勞。

2) 應變與安全修補

若評估結果確認該漏洞在產品執行時期存在被惡意利用的實質風險，團隊將立即將其列入「最高優先修補序列」，同步啟動緊急應變與弱點修復流程，發布安全更新，確保客戶端供應鏈韌性。

安全修補與維護更新

將 SBOM 產出整合於軟體開發流程中，透過自動化流程，確保軟體版本的發布 (Release) 皆能提供對應的物料清單檔案，落實供應鏈源頭管理之資安透明度。技術團隊透過持續性監控與主動修補流程，針對軟體元件持續對應全球最新之通用漏洞披露 (CVE) 資料庫。偵測並識別出影響產品元件之高風險或關鍵漏洞，團隊將啟動應變程序，進行漏洞風險評估，產出對應之安全修補程式或更新檔 (Patch)。

依據資安治理規範與客戶維護服務層級協議 (SLA) 之履約承諾，主動向用戶端發布軟體安全修補更新通知，協助客戶即時阻斷潛在威脅，強化數位供應鏈之整體防禦韌性。

安全交付與應變管理

積極落實國家軟體供應鏈安全政策，Openfind 全產品線皆具備標準軟體物料清單 (SBOM) 產出能力，支援客戶於採購驗收、資安風險評估及法規遵循上的揭露需求；並建立專責組織，協助客戶落實政府法規與國際資安標準相關條文規範與應變要求。若因資安稽核需求欲索取軟體物料清單，可透過專屬技術支援管道或業務服務窗口提出申請，提供對應產品版本的物料清單，落實「專案審核與受控交付」原則。

雲端服務 (SaaS) 安全更新



技術團隊產生軟體更新檔後，即時進行雲端環境修補更新。

軟體佈署 (On-Premise) 安全更新



標準版本：管理介面進行更新。
客製版本：依專案約定方式更新。

Openfind 的資安承諾

法規遵循與資安治理

積極響應數位發展部 (MODA) 推動之軟體供應鏈安全政策與《軟體資安品質相關指引》；通過 ISO 27001 資訊安全管理系統 與 ISO 27017 雲端服務資訊安全、ISO 27018 雲服務隱私管理認證。已將 SBOM 管理納入 ISO 27001 的 A.15 (供應商關係) 與 A.14 (系統獲取、開發及維護) 控制措施；同時將 SBOM 機制融入安全軟體開發生命週期 (Secure Software Development Life Cycle, SSDLC) 確保從軟體設計、程式碼編寫、套件引用到雲端運營，均處於可控的資安風險管理之下。

軟體供應鏈安全承諾

網擎資訊始終堅持「品質、安全、可信賴」的品牌價值。未來持續深化軟體安全生命週期與物料清單管理，建構軟體供應鏈安全防線，主動遵循國家資安政策與國際標準，致力協助企業客戶在日益嚴峻的資安威脅中建立堅韌的防禦體系，成為客戶值得信賴的長期資安夥伴。

參考指引與標準

- 數位發展部數位產業署《軟體資安品質相關指引》
- 經濟部《軟體物料清單 SBOM 發展趨勢》
- 財團法人資訊工業策進會《軟體產品元件表規範》
- 國際標準組織 ISO/IEC 5962 (SPDX Specification Standard)
- 美國網路安全暨基礎設施安全局 (CISA)《軟體元件透明度框架》
- 美國網路安全暨基礎設施安全局 (CISA)《軟體物料清單最小要素指引》
- 美國國家電信暨資訊管理局 (NTIA)《軟體物料清單最小要素指引》
- 日本經濟產業省 (METI)《軟體管理之軟體物料清單 (SBOM) 導入指引》
- 歐盟《網路韌性法案》(CRA)



聯絡資訊

網擎資訊軟體股份有限公司 | 永續治理專案辦公室

電子信箱：sustdept@openfind.com.tw

地址：11286 台北市北投區承德路六段 120 號 7 樓

電話：+886 2 2553-2000