‖ AI 是 Mercedes-Benz 轉型的推動力 ‖ 生成式 AI 七大商業用例 ‖ 求才策略 — 裁撤職位而非人員 ‖

CIO IT 經理人
BUSINESS TECHNOLOGY LEADERSHIP

ESG帶來企業變革契機

資訊長主動處理或協同合作，以嶄新方式促進 IT 與整個商業營運的永續性。

行政院公共工程委員會副主委葉哲良 Page 42

逢甲大學企管系講座教授佘日新 Page 46

美律實業資訊長暨資安長梁坤棠 Page 50

11月號 | 2023・No.149 | 定價240

ISSN 2223-4519

67 特別報導／

軟體供應鏈安全：探索SSDF與SBOM趨勢

供應鏈對於軟體資安要求逐步昇高，SBOM 與 SSDF 也受到關注與研究，掌握其發展趨勢將是製造業、網通業、資服業、軟體業等資安部門與雲端 SaaS、AI 應用的重要課題。

72 特別報導／

政府科技採購大翻新

九月甫上線《資訊服務採購作業指引》，除了保障公家單位、資訊服務商能在對等的條件下合作，更重要的是未來政府單位的「資安預算」應獨立編列，以及杜絕「回饋項目」風氣。

74 特別報導／

後疫情時代智慧醫療科技展望與未來(七)

科技產業、學界與醫療院所進行醫療人工智慧發展，本次會分析整個 AI 導入的政策期、場域驗證期、臨床應用期與擴散複製期等進行各層心法探討。

CIO IT經理人雜誌 美國IDG集團CIO雜誌獨家授權台灣版

中文版發行人 施威銘 ／ 總經理 林振輝 ／ 執行副總編輯 王家佩 ／
法律顧問 張孝詳律師 ／ 產業顧問 左大川 盛敏成 張玉雲 章光祖 ／
編輯部 總編輯 林振輝 ／ 總主筆 施鑫澤 ／ 主編 何信達 ／ 特約編輯 林裕洋 楊迺仁 柳林緯／ 美術編輯 葉芳妮 ／
整合行銷部 副總經理 張靜慧 ／ 協理 戴承恩 ／ 廣告專線 (02)2321-4335分機634 ／
產業行銷部 執行副總編輯 王家佩 ／ 活動企劃 蔡麗君 謝沛婕 ／ 行政助理 李佳軒／
讀者專線 (02)2321-4335分機118 (服務時間：週一-週五 9:00-12:20 13:30-18:00) ／ 讀者傳真 (02)2321-9730 ／
發行所 旗訊科技股份有限公司 ／ 地址 台北市杭州南路一段15-1號19樓 ／ 網址 www.cio.com.tw (歡迎多加利用線上服務表單) ／
電話 (02)2321-4335 ／ 傳真 (02)2321-9730 ／ 劃撥帳號 17615050 ／ 戶名 旗訊科技股份有限公司 ／
零售經銷商 一般書店及海外地區 旗標科技股份有限公司 ／ 地址 台北市杭州南路一段15-1號19樓 ／ 電話 (02)2396-3257分機314或331 ／
中華郵政北臺字第828號執照登記為(雜誌)交寄 ／ 製版、印刷 文聯實業有限公司 ／

軟體供應鏈安全的要角與良方

探索 SSDF 與 SBOM 之趨勢發展

有鑑於供應鏈對於軟體資安要求逐步昇高，SBOM 與 SSDF 也受到關注與研究，掌握其發展趨勢將是製造業、網通業、資服業、軟體業等資安部門與雲端 SaaS、AI 應用的重要課題。

文／梁日誠

在 2020 年末的 SolarWinds 事故與 2021 年末的 Log4j 攻擊行為之後，供應鏈風險管理中的軟體供應鏈安全漸漸成為有感的資安議題，軟體供應鏈的全球化特性也使得美國所推動的 Enhancing Software Supply Chain Security（Sec.4 EO14028）成為美國與國際盟友間的合作要項，而其中的安全軟體發展框架（Secure Software Development Framework，SSDF）與軟體物料清單（Software Bill of Materials，SBOM）因此成為舞台的要角及解惑的良方，要角需要識英雄的慧眼、良方則見效於微恙的苦主。

以 2023 年 9 月美國政府所公布的「各類資訊（服務）採購之共通性資通安全基本要求參考一覽表」為例，其中陳述了「安全軟體發展生命週期（Secure Software Development Life Cycle，SSDLC）」與 SBOM 的相關要求，SSDF 為展現 SSDLC 的具體方法，並有 NIST Special Publication 800-218（SP800-218）做為依據，SBOM 則有對應的 ISO 國際標準支撐，均具備高度的可行性，在 2021 年 5 月的 EO14028 「改善國家資通安全（Improving the Nation’s Cybersecurity）」總統令中，零信任架構（Zero Trust Architecture，ZTA）與 SSDF 常為人討論，ZTA 的直接受眾為聯邦政府機構，SSDF 則主要針對廣大的全球供應鏈，國際間的現行做法，包括合規面與應用面，均可為我們借鏡的對象。

認識SSDF與SBOM

SSDF 的主旨在應對「軟體發展生命週期（Software Development Life Cycle，SDLC）」中的軟體脆弱性（Vulnerabilities）的風險，SBOM 則提供軟體透通性（Transparency）、軟體完整性（Integrity）、軟體身份（Identity）的實作機制，SBOM 並為 SSDF 的任務（Task）之一（任務編號 PS.3.2）。

依據SP800-218，SSDF分為四個群組（Groups），群組下包含了實作（Practice）、任務（Tasks）、參考案例（Notional Implementation Examples）與參考指引（References），SSDF 的群組、實作、任務歸納於**<表A>**。

SBOM 的最低所需元素定義於 NTIA（National Telecommunications and Information Administration）的「The Minimum Elements For a Software Bill of Materials（SBOM）」文件中，包含**資料欄位、自動化支援、實作與流程**三大類。

其中，SPDX（Software Package Data eXchange，Source：The Linux Foundation）、CycloneDX（Source：OWASP）、SWID（Software Identification）Tag（Source：ISO、NIST）是自動化支援所列舉的三種可接受的資料格式，自動化支

援亦包含了自動產生與機器可讀性；實作與流程定義了 SBOM 請求、產生與使用，包含：頻率、深度、已知的未知、分送與交付、存取控制、錯誤調解（Accommodation of Mistakes）等；基線資料欄位及與資料格式的關係，列舉於**<表B>**（參考 NTIA 的「Survey of Existing SBOM Formats and Standards」文件）。

元素 / 群組	群組名稱	實作	任務
PO	組織的準備 Prepare the Organization	PO.1 ~ PO.5	PO.1.1 ~ PO.1.3 PO.2.1 ~ PO.2.3 PO.3.1 ~ PO.3.3 PO.4.1 ~ PO.4.2 PO.5.1 ~ PO.5.2
PS	保護軟體 Protect the Software	PS.1 ~ PS.3	PS.1.1 PS.2.1 PS.3.1 ~ PS.3.2
PW	產出安全完善的軟體 Produce Well-Secured Software	PW.1 ~ PW.9	PW.1.1 ~ PW.1.3 PW.2.1 PW.4.1,4.2,4.4 PW.5.1 PW.6.1 ~ PW.6.2 PW.7.1 ~ PW.7.2 PW.8.1 ~ PW.8.2 PW.9.1 ~ PW.9.2
RV	回應脆弱點 Respond to Vulnerabilities	RV.1 ~ RV.3	RV.1.1 ~ RV.1.3 RV.2.1 ~ RV.2.2 RV.3.1 ~ RV.3.4
數量	4	20	42

表A

SBOM 三種可被接受的資料格式中，SPDX 已經成為國際標準 ISO／IEC 5962：2021，SWID Tag 則成為國際標準 ISO／IEC 19770-2：2015。SBOM 發展至今，主要的雲端服務提供商（包括 AWS、Google Cloud、Azure 等）、原始碼代管服務平台（如 GitHub）、網通產品製造商（如 CISCO）都對 SBOM 提供了支持與解決方案。

此外，免費與付費的 SBOM 管理工具也於市場中可供選用，近期在 SBOM 的主要推動機構-美國 CISA 的討論中，也提出了 AI 為軟體系統的詮釋。SBOM 的持續發展包含了以下的工作，來支持 SBOM 在各項現有使用案例的成功：

- Recommended Data Fields：Hash of the Component、Lifecycle Phase、Other Component Relationships、License Information
- Cloud-based Software and Software-as-a-Service
- SBOM Integrity and Authenticity
- Vulnerabilities and SBOM
- Vulnerability and Exploitability in Dependencies
- Legacy Software and Binary Analysis
- Flexibility vs Uniformity in Implementation

政府推動與法規遵循

SSDF 與 SBOM 的發展進度，與以美國政府為首而帶頭推動的國際政府與行業（包括歐盟、英國、荷蘭、加拿大、日本、韓國等）合作有很大的關係，由美國 EO14028 總統令開始，輔以主責與協同機構（如 DHS CISA、NTIA、Department of Energy、Department of Defense、GSA、NASA、FDA、NIST）的規範制定，相關的法制化活動展開，使得國際間的軟體供應鏈的廠家們正視即將面臨的法規遵循要求，自詡以軟實力為優勢的台灣軟體業，不妨同時以風險與機會的角度看待 SSDF 與 SBOM 的法遵要求發展。

‖ 美國聯邦政府對SSDF要求的法制化

於 2023 年 4 月，美國國土安全部（DHS）之下的 CISA 依 EO14028 總統令與 M-22-18 文件「Enhancing the Security of the Software Supply Chain through Secure Software Development Practices」，公布「Secure Software Development Attestation Common Form」來徵求意見文件（Docket No. CISA - 2023 - 0001，法制化進行中）。

因此，對於軟體產製者，要求於 2022-09-14

年後開發的軟體、於2022-09-14後產生主要版本變更的現有軟體、軟體產製者對軟體碼持續進行變更的軟體（如：SaaS 或使用持續交付／持續佈署），應執行自我具結（Self-Attestation），具結的要求依據 EO14028 與 SSDF（依據SP800-218）相關的實作與任務，以上不包含政府自行開發的軟體及政府自由取得的軟體;政府亦可要求如：SBOM 或第三方評鑑員的附加具結證明文件；於 M-22-18文件中定義軟體包含：韌體（Fireware）、作業系統(Operating systems)、應用(Applications)、應用服務(Application services，如:Cloud-based software)、包含軟體的產品(Products containing software)等。若適用時，自我具結亦包含第三方評鑑機構評鑑員依相關NIST指引對所指軟體的確認，此法制化工作賦予美國聯邦政府機構對軟體供應商依據SSDF所進行的自我具結(包含第三方評鑑、SBOM等要求)要求的責任。

‖ 美國聯邦採購法規對SBOM要求的法制化

於 2023 年 10 月，美國國防部（DoD）、GSA、NASA 共同提出聯邦採購法規（Federal Acquisition Regulation，FAR）「Cyber Threat and Incident Reporting and Information Sharing」（Docket No. FAR - 2021 - 0017，目前法制化進行中），其中包含合約商對 SBOM 的產生、維護與提供的相關要求，要求的依據為 NTIA 的「The Minimum Elements For a Software Bill of Materials」文件。此法制化工作要求聯邦政府的合約商對執行合約所涉及的軟體均應符合 SBOM 要求，由此法規也可窺見美國聯邦政府對SBOM與資通安全威脅、事故與資訊分享等關係的重視程度。

‖ 美國醫療領域的SBOM資安要求

美國食品藥物管理局（Food and Drug Administration，FDA）已經完成法制化，公布「Cybersecurity in Medical Devices：Quality

資料欄位 \ 資料格式	SPDX	CycloneDX	SWID Tag
Supplier Name	PackageSupplier	Supplier publisher	<Entity> @role (softwareCreator/publisher), @name
Component Name	PackageName	name	<softwareIdentity> @name
Version of the Component	PackageVersion	version	<softwareIdentity> @version
Other Unique Identifiers	DocumentNamespace combined with SPDXID	bom/serialNumber component/bom-ref	<softwareIdentity> @tagID
Dependency Relationship	Relationship: DESCRIBES; CONTAINS	(Inherent in nested assembly/ subassembly and/or dependency graphs)	<Link> @rel, @href
Author of SBOM Data	Creator	metadata/authors/ author	<Entity> @role (tagCreator), @name
Timestamp	Created	metadata/timestamp	<Meta>

表B

System Considerations and Content of Premarket Submissions」文件，文件中對 SBOM 的要求包含安全風險管理報告中須包含 SBOM、SBOM 須涵蓋於設備組態管理之中、SBOM 須與 NTIA「Multistakeholder Process on Software Component Transparency document Framing Software Component Transparency: Establishing a Common Software Bill of Materials」一致，對於有意進入或維持美國醫療市場的廠家須即時關注。

‖ 美國國際採購需求納入SBOM要求

於 2023 年 8 月，美國政府採購網站 System for Award Management（SAM）發布了一項國際性車輛採購需求（Notice ID 191V1023Q0028），需求中納入 SBOM 相關要求，以與其他合約商分享 SBOM 資訊，做為對應已知脆弱點之用途，此要求適用於合約商與其分包商，要求中也可見對於通報軟體脆弱點的 Vulnerability Exploitability exchange（VEX）格式的使用。

應用與使用案例

‖ SSDF 的應用狀況

SSDF 的主旨在應對 SDLC 的軟體脆弱性（Vulnerabilities）的風險，這體現在 Secure SDLC 的資安實作，適用於 Waterfall、Spiral、Agile、Agile combined with Software Development and IT Operations （DevOps）、DevSecOps（DevOps integrated with Security）、CI/CD、Life Cycle Model for Software Domain（ISO/IEC/IEEE 24748-1：2018 Guidelines for life cycle management）等方法與模型的資安管理。於業界常見的 SLSA（Supply-chain Levels for Software Artifacts）Supply Chain Model、ESF（Enduring Security Framework）的開發者、供應者、用戶間的關係，亦適用於 SSDF 的應用。

以 DoD 的 "Unfolded" DevSecOps Lifecycle Phases為例，展現 SSDF 與各現行應用，包括 DevOps、DevSecOps、CI／CD、Continuous Operations、Continuous Build 間的關係。

此外，SLSA 中列舉的供應鏈威脅，包含Source Threats、Dependency Threats、Build Threats及ESF 中所列舉的開發者與供應者的威脅（包含 On-Premises 與 SaaS），均可採用 SSDF 的各項實作與任務來應對，以適當的管理風險；SLSA v1.0 的 Security Levels（L1 ~ L3）也可進一步對應到 SSDF Attestation 的準備作業上。

至於，SSDF 與 SBOM 對應到業界常用的 SDLC 與 SSDLC 相關的國際標準、行業標準與法規，包括 BSAFSS、BSIMM、CNCFSSCP、EO14028、IDASOAR、IEC62443、IR8397、ISO27034、ISO29147、ISO30111、MSSDL、NISTCSF、NISTLABEL、OWASPASVS、OWASPMASVS、OWASPSAMM、OWASPSCVS、PCISSLC、SCAGILE、SCFPSSD、SCSIC、SCTPC、SP800-53、SP800-160、SP800-161、SP800-181 等，則具備較高的兼容性，也降低了進入門檻。

‖ SBOM 的使用案例

爰引 CISA、DoE、NTIA 等機構發布的 SBOM 相關文件，可綜合整理 SBOM 流程，包括，產生、發現、存取、傳送、使用等階段。各階段的使用案例舉例如下：

◆ 產生（Generate）階段

✓ 於 Build 時或於 Binary 分析時產生 SBOM，如：

☐ DevOps 可使用自動化工具於 Build 時生成 SBOM。

☐ 使用 Binary 分析工具（如逆向分析工具），分析現有不具備 SBOM 的軟體並生成 SBOM。

✓ 以雜湊（Hashing）、簽章（Signing）方式確保 SBOM 的完整性、真實性。

✓ 於 SBOM 中參考其他 SBOM。

✓ 於合約中要求供應商持續提供SBOM

◆ 發現（Discovery or Advertisement）階段

✓ 告知（如 email、官網公告、隨軟體告知）用戶 SBOM 的存在及存取的方式。

✓ 採用 Sophistication Level（如: Low、Medium、High）方式進行分級處理。

◆ 存取（Access）階段。

✓ 採用存取控制管控 SBOM 或為公開資料。

✓ 選擇傳送的方式。

✓ 採用 Sophistication Level（如: Low、Medium、High）方式進行分級處理。

◆ 傳送（Transport）階段

✓ 用戶接收方式的選擇，如：

☐ 以email或交付物（如隨身碟）進行。

☐ 被包含於 Complied Code 中一併取得，如 PowerShell 模式。

☐ 附加於 Registry，如 Azure Container Registry（ACR）、Amazon Elastic Container Registry（ECR）。

☐ 儲存於線上，如 Digital Bill of Materials（DBoM）、Supply Chain Integrity, Transparency, and Trust（SCITT）、廠家網站。

☐ 儲存於 Repo，如 Conda。

✓ 採用 Sophistication Level（如: Low、Medium、High）方式進行分級處理。

◆ 使用（Use）階段

✓ 用戶接收到 SBOM 的應用，如採用 SBOM 管理工具。

✓ 使用於併購（Mergers & Acquisitions，M&A）的風險評鑑過程中。

✓ 識別供應鏈中的 Malicious OSS。

✓ 識別脆弱點的影響與否，如: Vulnerability Exploitability eXchange（VEX）的 NOT AFFECTED、AFFECTED、FIXED、UNDER INVESTIGATION。

✓ 識別脆弱點及對應的 VDR（Vulnerability Disclosure Report）。

✓ 協助Incident Response。

✓ 識別 License 及智財權風險識別。

✓ 協助國際間、區域性、國家級、各行業的情資分享、威脅管理、脆弱點管理、事故處理等作業。

總之，SSDF 與 SBOM 是兩個高度相關的議題，在現有的法遵考量下，有一定的即時性，對於法制化中或預告實施的法規，則存在及時的特性，不論是將現有的「安全軟體發展生命週期（SSDLC）」作業對應展現 SSDF 或是以 SSDF 建立 SSDLC，都需要一定的準備時間，在準備 SSDF 與 SBOM 的合規過程中，也須留意與現有合規要求的整合或介接，如 ISO 27001：2022 中的 A.8.25 Secure development life cycle，以利有效使用資源並增進準備效率。

此外，CMMC 所依據之一的 NIST SP800-171 標準，目前為 Rev 2 版本，於 Rev 3 版本草案中，也將會見到針對供應鏈風險管理的納入，考量到數個 SSDF 與 SBOM 相關的聯邦層級法規與聯邦採購法規的法制化進行，應該充分考量 SSDF 與 SBOM 的相關實作於 CMMC 的合規準備中。

美國聯邦政府、ISO、NIST、OWASP、The Linux Foundation 等機構，在大力倡議 SSDF 與 SBOM 的同時，也提供相對的資源，包括在工作群組、技術資料、認知宣導、能力培養、工具等。

目前，筆者所服務的 TCIC 卓越中心（CoE）正整備相關資源，將先提供中文授課的 SSDF／SBOM 基礎課程與證照方案，SSDF／SSDLC 第三方 NIST SP800-218 評鑑服務可獨立或合併資通安全相關稽核或評鑑作業進行，有意投入的企業或人員可以多加運用。

作者梁日誠（CISSP/CCISA/CCISM/GPM-b）現為 CMMC PI/CCP/CCA/SME，ISO/IEC JTC1/SC27、SC42、ISO/TC22/SC32、IEC/TC65 技術組委員，ISO 27001／ISO 27701／ISO 22301／ISO 20000-1／IEC 62443-2-1 主導稽核師及講師，TCIC 環奧國際驗證公司全球營運總經理。