運算堡壘的危機與防線
~ 以NIST SP 800-223高效能計算的安全架構窺見資安新戰場攻防

Presentation by **唐雍為 執行董事**
April 2025

唐雍為　執行董事
資誠 / 風險及控制服務

☎(02) 2729 6093
yung-wei.w.tang@pwc.com

經歷

資誠聯合會計師事務所 風險管理及內部控制服務部 副總經理
資誠聯合會計師事務所 風險管理及內部控制服務部 協理/經理/顧問
中華民國電腦稽核協會 理事
曾任 星展(台灣)商業銀行股份有限公司 資訊安全服務部 協理暨資安長
曾任 中華民國銀行商業同業公會全國聯合會 金融業務電子化委員會 技術分組 委員
國際資訊安全系統專家(CISSP)、國際電腦稽核師(CISA)
國際道德駭客認證(CEH) 、國際滲透測試專家(LPT)
國際資安分析專家(ECSA) 、國際數位鑑識專家(CHFI)
國際加密貨幣專家(CCE)

學歷

英國華威大學資訊管理碩士
交通大學管理科學系(輔修資訊工程、電腦軟體、半導體製程、財務工程)

服務專長

資安風險與資安維運評估與諮詢 / 資安治理與縱深防禦輔導與諮詢
資訊安全檢測與評估服務與諮詢 / 資安事件系統導入與規劃諮詢
資料庫活動管理系統導入與規劃諮詢 / 資訊安全管理制度(ISMS)輔導諮詢
個人資訊管理系統(PIMS)輔導諮詢 / 資訊系統專案管理輔導與諮詢
區塊練應用分析與諮詢 / 加密貨幣發行 / 證券型代幣發行
資訊系統一般控制、應用系統及企業流程之稽核或診斷諮詢
內部控制及作業流程優化 / 企業流程再造及數位轉型

Agenda

1

HPC資安為何重要？

為何關注HPC安全？「運算堡壘」的價值與脆弱

HPC是什麼？

高效能運算（High-performance computing，縮寫：HPC）是指研究人員使用超級電腦和電腦叢集來解決一系列問題。高效能運算擁有更快的計算速度、更大的負載能力和更高的可靠性。高效能計算的每一個單一處理器的計算性都應該足夠強勁，並且還需要整合多個處理器，這些多個處理器構成一個電腦系統，並且多處理器之間還要協同分散式計算、平行計算。運用方向主要為大規模平行處理、高速運算能力，用於解決複雜問題，運用領域主要為半導體設計模擬、生醫研究的基因定序分析、學術界的天氣模擬、金融業的風險模型運算、AI模型訓練...等等。

「運算堡壘」意涵

集中了龐大運算力與極度敏感的資料（研究成果、商業機密、智慧財產權）。但是高價值伴隨高風險，易成為攻擊目標（竊取機密、癱瘓服務、挖礦獲利、當作攻擊跳板）。

HPC與傳統運算有什麼不一樣嗎?

Reference: https://zh.wikipedia.org/zh-tw/%E9%AB%98%E6%80%A7%E8%83%BD%E8%AE%A1%E7%AE%97

HPC 和傳統運算有什麼區別？

HPC（High Performance Computing）與傳統運算的主要差異在於 HPC 能夠處理龐大的資料集和複雜的運算任務，以更少的時間和成本獲得結果。以下是主要的差異

差異領域	高效能運算	傳統運算
處理能力	**用多台計算機和儲存設備組成一個高效運算的集群**，以極高速度處理大量資料。這種方法可以處理對單一電腦而言過於龐大的運算，從而降低完成大型運算的時間。	使用**單一電腦或伺服器**進行運算，通常無法處理龐大的資料集和複雜的運算任務。
運算方式	透過將多台計算機或伺服器互相串連成群組，進行平行運算以提高效能。這種方法可以**將運算任務分配到多個節點上**，並讓每個節點同時執行小型作業，以提高整體的運算速度。	通常使用單一電腦或伺服器進行運算，**無法進行平行運算**，從而限制了運算速度和效率。
應用領域	常見應用包括風險模擬、分子模型製作、計算流體動力學、天氣預測模型、原物料模擬、汽車碰撞模擬、地理空間模擬、流量管理等，**需要處理龐大的資料集和複雜的運算任務**。	**通常用於日常運算**、Office 軟體、遊戲等，無法處理龐大的資料集和複雜的運算任務。

Reference: https://roo.cash/blog/hpc-conceptstock-article/

2

HPC面臨的威脅與風險

HPC 獨特的資安風險 (相較於傳統IT)

規模與複雜度
數千節點、特殊高速網路（如InfiniBand）、平行檔案系統（如Lustre），管理與防護難度高。

共享資源模型
多使用者/多專案環境，需確保資源與資料的嚴格隔離，防止交叉感染或竊取。

特殊軟硬體
作業系統（常為Linux客製版）、排程器（Slurm、PBS）、科學計算函式庫等，可能存在特定漏洞。

資料生命週期安全
強調保護資料不僅在靜態儲存或傳輸，計算過程中的記憶體保護也是挑戰。

運算環境特性
學術研究常需協作與開放性，與嚴格的資安管制有時會產生衝突。產業環境常需強調速度，也會形成衝突。

新戰場攻防
~HPC常見攻擊手法

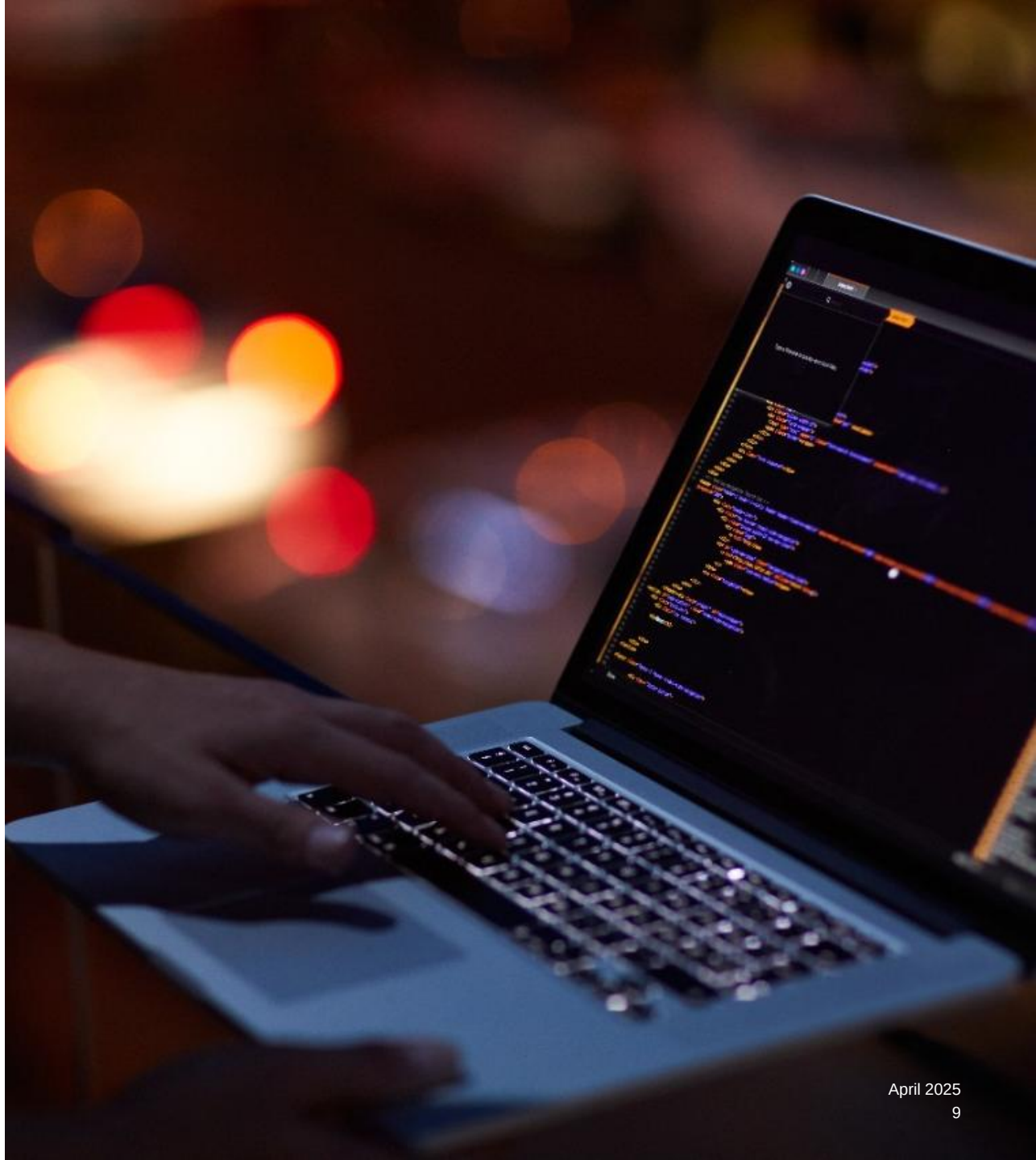
惡意程式
最常見的是加密貨幣挖礦（Cryptojacking），其次是勒索軟體或間諜程式。如何植入？（透過竊取憑證登入、利用系統漏洞、提交惡意任務）。

資料外洩
竊取敏感研究資料、模擬結果、訓練好的AI模型等智慧資產。（直接存取未受保護的儲存區、利用網路漏洞傳輸）。

阻斷服務 (DoS/DDoS)
癱瘓排程器、耗盡儲存空間、塞爆網路頻寬，目標是中斷研究。

橫向移動/權限提升
從單一被駭帳號擴散至更多節點，甚至取得管理員權限。

供應鏈攻擊
針對HPC使用的第三方軟體、函式庫或管理工具下手。



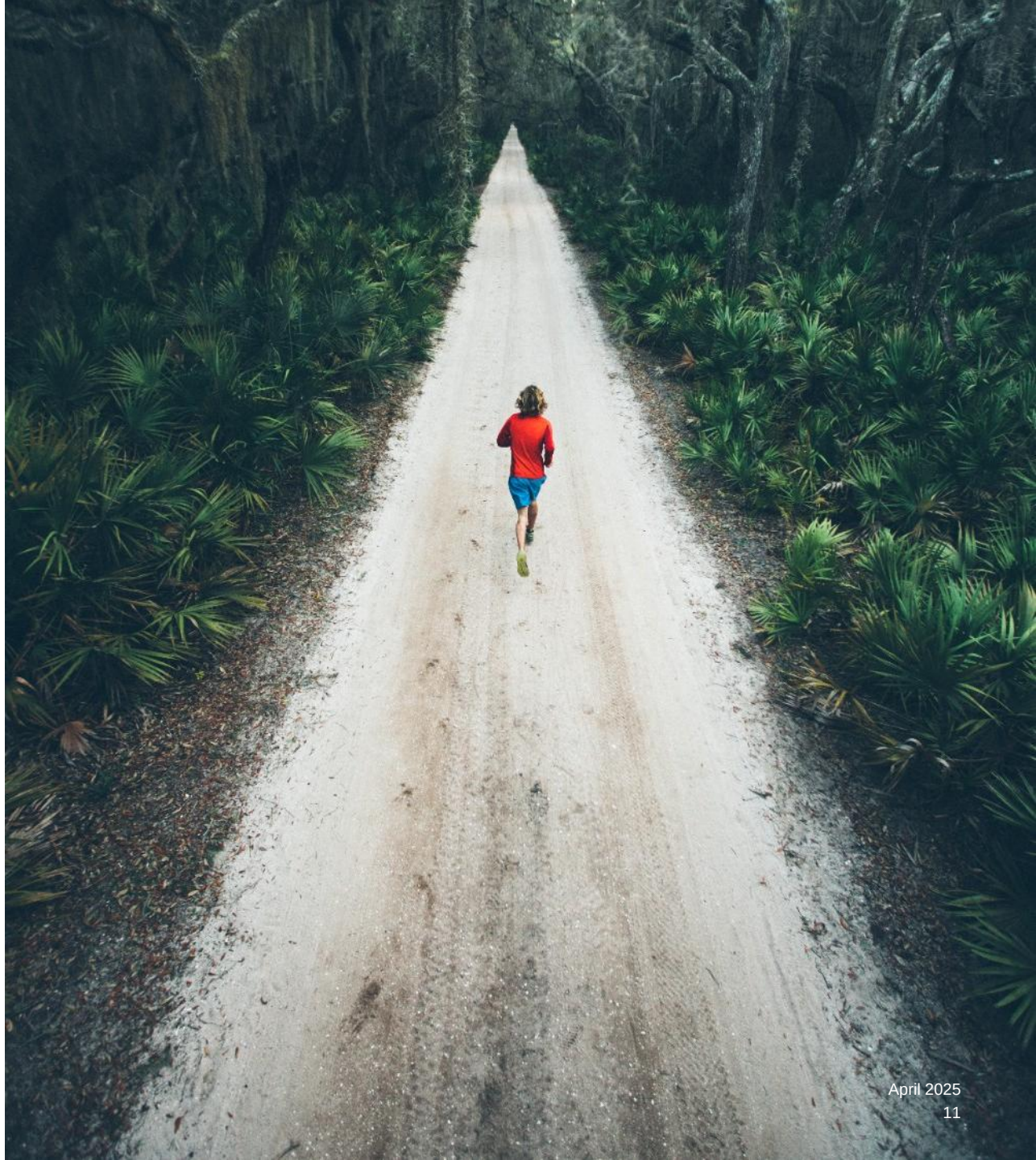
3

NIST SP 800-223 概覽

指引明燈
NIST SP 800-223 概覽

NIST Special Publication 800-223 是一份針對高效能計算（HPC）系統安全的指南，涵蓋了架構、威脅和對策。此文件旨在幫助組織識別和應對HPC環境中的安全挑戰。

它詳細介紹了HPC系統的特殊架構需求，包括計算能力、網絡設置和資料存儲等方面。報告分析了潛在的安全威脅，如惡意軟件攻擊、資料洩露和未經授權訪問等。為了減輕這些風險，NIST提供了一系列安全對策，如加強身份驗證措施、使用加密技術、監控異常活動和定期進行安全評估。該指南旨在促進HPC系統的安全性和可靠性，以支持科學研究和商業應用。



Reference: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-223.pdf

NIST SP 800-223 關鍵安全概念

HPC具有以下獨特的安全特徵與需求

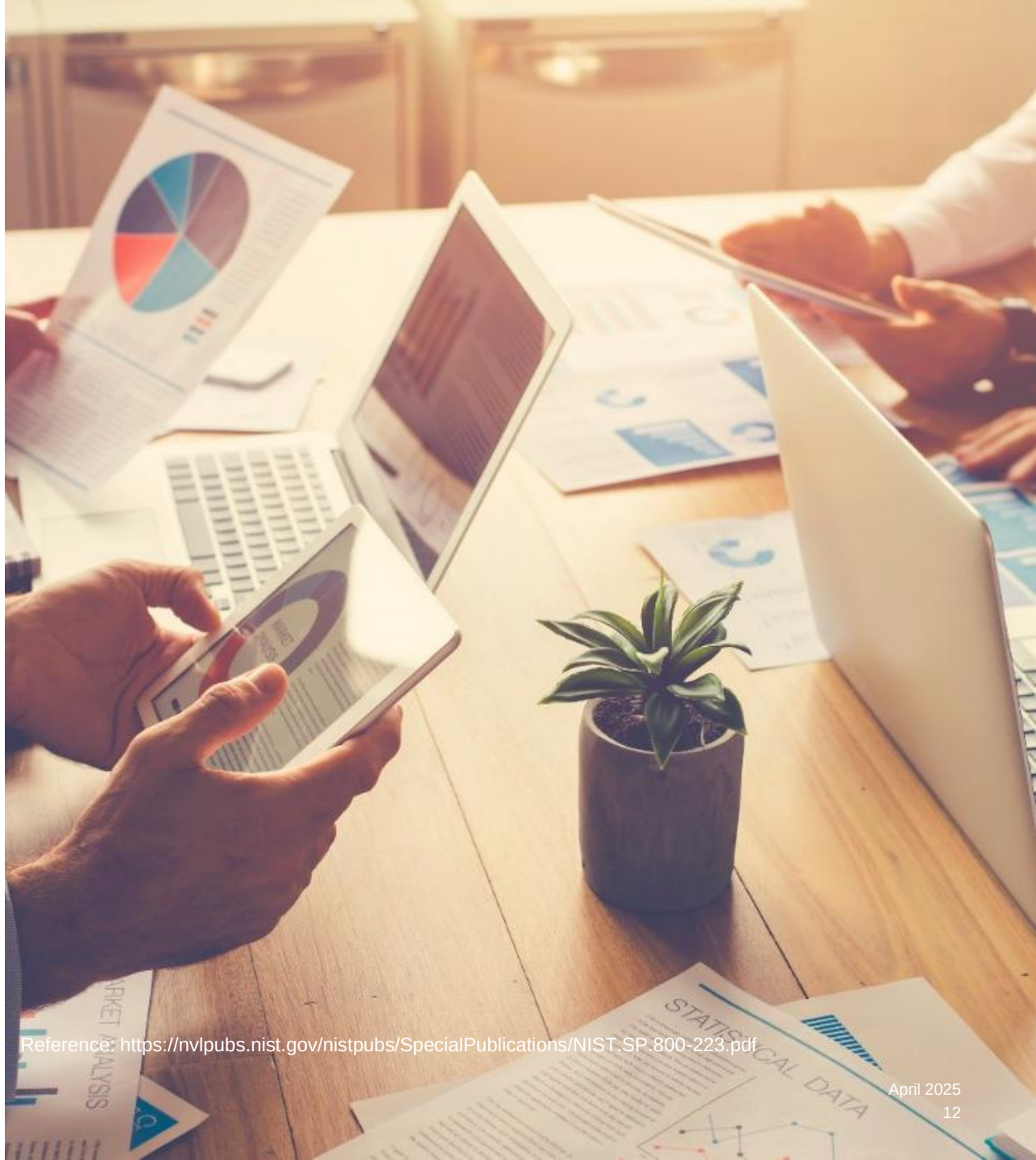
性能與安全的衝突
HPC用戶重視安全性，但不希望其影響系統性能或研究進行。

不同應用的安全需求
不同平台、項目和資料有不同的安全敏感性，需同時執行多個安全政策。

安全工具資源有限
HPC系統多將資源集中於提升性能，鮮少考量安全工具。

開源及自行開發軟體
開源軟體易受供應鏈威脅，自行開發軟體則可能因安全品質不佳而易受攻擊。

資料庫存取控制的顆粒度
不同團隊需不同資料存取權限，控制需求需隨實驗或應用結果調整。



NIST SP 800-223 關鍵安全概念 ~ 管制區的潛在威脅(1)

高效能計算區域威脅

此區域提供核心計算功能，多用戶共享節點，易受邊信道攻擊等多租戶環境威脅。其他風險包括配置錯誤、用戶軟件錯誤和系統濫用。若使用虛擬化技術，可能遭遇容器逃逸和拒絕服務攻擊。HPC應用運行於用戶空間，但安全測試不足，難以監控可疑活動。

資料存儲區域威脅

資料存儲區域需確保資料的機密性、完整性和可用性。惡意資料刪除和污染可損害資料完整性；用戶誤操作可能影響機密性。HPC文件系統提供高速和大容量，但硬盤故障及備份挑戰是潛在威脅，尤其是默認不備份的用戶資料。存儲的敏感資料需遵循安全標準，應用隱私保護技術需平衡性能和可用性。

Reference: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-223.pdf

NIST SP 800-223 關鍵安全概念 ~ 管制區的潛在威脅(2)

訪問區域威脅

訪問區域是外部用戶進入HPC系統的入口，負責身份驗證和授權，因直接連接外部網絡，易受拒絕服務、網絡掃描、身份驗證攻擊和會話劫持等威脅。特定的軟件堆疊可能遭篡改和代碼注入。建議使用多因素身份驗證以減少未授權訪問風險。此區域支持有限計算，易被濫用，並常被多用戶共享，可能導致活動曝光，一般IT安全工具可加固此區域。

管理區域威脅

管理區域負責HPC系統管理，連接內部網絡，運行管理軟件，易受特權提升攻擊影響。用戶通常依賴POSIX文件系統權限來隔離特權，僅有特權的管理員可登錄，但惡意用戶可能嘗試入侵。若管理區域基於雲服務，需考慮雲相關風險。

Reference: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-223.pdf

NIST SP 800-223 關鍵安全概念 ~ 其他潛在威脅(1)

環境及物理威脅

包括對設施（如電力、冷卻系統、水源）的物理或網絡攻擊、未經授權的實體訪問和自然災害（如火災、洪水、地震、颶風等）。

性能優先下的漏洞

HPC設計中優先考慮性能，可能導致系統不夠冗餘，增加了如拒絕服務攻擊的風險。備份系統因成本高而常被忽視，數據存儲缺乏備份。

Reference: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-223.pdf

NIST SP 800-223 關鍵安全概念 ~ 其他潛在威脅(2)

供應鏈威脅

HPC供應鏈可能遭遇從專有信息盜竊到硬件攻擊和軟件操控等威脅。供應商數量有限，導致技術支持人力短缺和多樣性不足。

內部威脅

來自內部人員的威脅，分為意外/無意和惡意/有意兩類。無意威脅源自正常活動的意外結果，而惡意內部人員可能故意上傳惡意代碼。

Reference: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-223.pdf

NIST SP 800-223 關鍵安全概念 ~ 可落地的管理關鍵（舊瓶新酒的意味濃厚）

安全域 (Security Domains)

將HPC環境依功能/信任等級劃分區域（如登入節點、計算節點、儲存系統、管理網路），施加不同安全控制。

資料敏感性分級 (Data Sensitivity)

將資料分類（公開、內部、機密、極機密），依等級實施不同的存取控制、加密等保護措施。

存取控制 (Access Control)

強調最小權限原則、角色為基礎的存取控制(RBAC)、以及對使用者與管理者採用強認證機制(建議MFA)。

作業排程安全 (Job Scheduling Security)

保護排程器本身、驗證提交任務的合法性、防止任務間的干擾或權限擴張、監控資源濫用。

監控與稽核 (Monitoring & Auditing)

需要收集並分析系統、網路、應用程式及任務執行的日誌，部署入侵偵測系統(IDS)，定期審閱稽核紀錄。

配置管理 (Configuration Management)

維護作業系統、函式庫、應用程式的安全基準配置，及時進行弱點掃描與修補。

4

訂閱者的風險與責任


The Supply chain stuff is really tricky.
Elon Musk

HPC生態圈的各種角色
~如何確保您的研究資料、成果或商業機密在生態系中是安全的？

角色 (Player)	主要職責與互動對象 (Primary Role & Key Interactions)
HPC 服務提供者 (HPC Provider)	定位：提供計算、儲存基礎設施與平台服務 執行任務：管理資料中心物理安全、核心網路、底層作業系統與中介軟體 互動對象： 訂閱者、軟硬體供應商、網路服務商
訂閱者 / 使用者 (Subscriber / User)	定位：使用 HPC 資源進行計算與分析 執行任務：上傳、下載、處理資料、開發或執行應用程式/計算、管理自身團隊的存取權限 互動對象： HPC服務提供者、資料擁有者、應用軟體供應商
資料擁有者 (Data Owner)	定位：擁有被處理資料的所有權 執行任務： 設定資料使用與處理的政策規範(可能與訂閱者是同一單位) 互動對象： 訂閱者 (主要)、HPC服務提供者 (關於資料處理規範)
軟體供應商 (Software Vendor)	定位：提供作業系統、排程器、函式庫、編譯器、應用軟體等 執行任務：提供軟體更新與修補程式 互動對象： HPC服務提供者、訂閱者 (應用軟體)
硬體供應商 (Hardware Vendor)	定位：提供伺服器、CPU/GPU、儲存設備、高速網路設備等 執行任務：提供韌體更新與修補程式 互動對象： HPC服務提供者 (主要)
網路服務商 (Network Provider)	定位與執行任務：提供對外網路連線 (Internet 或 學術研究網路，如：TWAREN) 執行任務：維持網路可用之狀態 互動對象： HPC服務提供者 (主要)
系統整合商 (System Integrator) - **(選擇性)**	定位與執行任務：協助設計、建置、整合 HPC 系統 互動對象： HPC服務提供者、軟硬體供應商
資安服務商 (Security Service Provider) - **(選擇性)**	定位與執行任務：提供專業的 HPC 資安監控、顧問或事件應變服務 互動對象： HPC服務提供者、訂閱者

訂閱者面臨的風險樣貌

智慧財產權/機密資料外洩
研發成果、演算法、客戶資料、基因序列等敏感資料被竊。

資料完整性遭破壞
輸入資料或計算結果被惡意竄改，導致研究結論錯誤或產品設計失敗。

服務可用性衝擊
因供應商遭攻擊導致HPC停擺，研究中斷、錯失時效性機會(Time-to-market)。

法規遵循風險
使用的HPC環境未能滿足特定法規（如個資法、GDPR、特定領域規範）對資料處理的要求。

商譽損害
若使用的供應商爆發重大資安事件，訂閱者聲譽可能連帶受損。

在HPC情境下，供應商安全管理是指訂閱者對於所使用的HPC服務提供者，進行持續性的安全風險評估與管理過程。計算可以外包，但風險與責任無法完全轉嫁。訂閱者有責任確保供應商的安全水準符合自身需求。供應商管理是訂閱者實踐其在責任共擔模型中應盡義務的關鍵手段。

供應商盡職調查（Due Diligence）

安全框架 / 安全認證 / 稽核報告
是否參考NIST SP 800-53或其他標準？對NIST SP 800-223的認知程度？是否通過 ISO 27001 / ISO27701 / BS10012？是否有 SOC 2 Type II 報告 (關注安全性、可用性、機密性原則)？

法規遵循能力
能否滿足特定行業或地區的法規要求？

安全政策文件
可否檢閱其存取控制、資料處理、加密、事件應變等政策？

技術控制措施
詢問網路隔離、加密機制（傳輸中/靜態）、日誌記錄能力、弱點管理作法。

營運持續/災難備援
了解供應商如何應對服務中斷。

合約規範與服務等級協議 (SLA)

資料權利歸屬與處理地點
明確資料所有權，以及儲存與處理的地理位置限制。

安全標準要求
約定供應商需達到的具體安全控制措施。

安全事件通報
規範通報的時效、流程與內容。

稽核權利
保留訂閱者或委託第三方稽核供應商的權利。

責任歸屬與賠償
界定發生安全事件時的責任與處理方式。

退場機制
約定服務終止時，資料如何安全刪除或返還。

安全相關SLA 量化指標
重大弱點修補時限、安全事件回應時間、系統因安全因素停機的補償等。

供應商持續監控與稽核

定期審閱報告
向供應商索取並檢視最新的稽核報告（如SOC 2）、滲透測試摘要。

安全問卷
定期（如每年）發送問卷，了解供應商安全措施的變化。

定期會議
與供應商召開安全治理會議，討論風險與改善措施。

SLA績效追蹤
監控供應商是否達成安全相關的服務水準承諾。

關注外部情資
留意可能影響供應商的資安威脅情報。

檢視供應商提供的安全儀表板或日誌(若有提供)
若供應商可以透過機制提供系統運作實時狀態，將更可以協助訂閱者掌握第一手的運作狀態。

訂閱者的自主防禦策略 ~強化自身

資料處理安全
在資料上傳至HPC前，進行敏感度分類；對高度敏感資料考慮進行加密、去識別化或遮罩。

存取權限管理
嚴格管理自身團隊成員對HPC服務的存取權限；強制使用強密碼與MFA；落實最小權限原則；及時撤銷離職人員權限。

安全程式開發
若需自行開發程式在HPC上執行，應遵循安全編碼規範（如：驗證輸入、處理錯誤、避免寫死密碼）。

訂閱者的自主防禦策略 ~主動監控與應變

任務執行監控

教育使用者留意自己提交任務的資源使用狀況（CPU、記憶體、執行時間）是否異常。

了解資料流

掌握自己的資料在HPC環境中的存放位置（特定目錄、暫存區）及生命週期，理解各區域的安全保護程度。

制定內部應變計畫

規劃當收到供應商安全事件通知時，訂閱者內部應如何應對（例如：如何快速通知內部利害關係人、評估影響、採取補救措施）。

自主監控意識與應變能力很重要
沒有人會比你更了解你的應用

Case Study
~ 歐洲多國HPC中心遭鎖定 – 挖礦與跳板攻擊事件啟示

情境
2020年曾發生歐洲多個國家級或大型研究機構的高效能計算中心 (包括英國、德國、瑞士、西班牙等地) 在短時間內相繼發現遭到入侵。攻擊者利用竊取的SSH憑證或系統漏洞取得登入權限後，主要目的是部署惡意軟體進行加密貨幣挖礦，濫用龐大的運算資源牟利。部分案例中，攻擊者還試圖利用這些HPC中心作為跳板，對其他網路目標發動攻擊。

衝擊
多個HPC中心被迫暫時關閉服務，進行安全檢查與系統清理，嚴重影響了眾多科學研究計畫的進度 (訂閱者/使用者直接受害)。暴露出HPC環境在身份驗證、存取控制、網路隔離方面可能存在的弱點。引發了對HPC供應鏈安全 (使用的軟體、管理工具) 的擔憂。

供應商管理
此事件凸顯了訂閱者在選擇HPC供應商時，需要評估其安全監控能力、事件應變速度、以及安全基礎建設的強度 (如MFA、入侵偵測系統)。合約中關於服務中斷的補償、安全事件的通報機制變得至關重要。

訂閱者責任
使用者自身妥善保管登入憑證 (如SSH金鑰) 的重要性被再次強調。若攻擊是從使用者端點發起，則訂閱者機構的內部安全也需檢討。

事件中的入侵手法與NIST SP800-223框架中強調的存取控制、系統監控、配置管理等環節息息相關。

Reference:https://www.ithome.com.tw/news/137666

5

總結與展望

未來挑戰與展望
~資安是動態演變的領域，需保持關注

新興技術風險

- AI/ML在HPC上的應用帶來新威脅（模型竊取、對抗式攻擊）
- 量子計算對現有加密的長遠影響，傳統加密演算法可能無法因應新時代

威脅不斷演變

- 強力攻擊者（國家級駭客、勒索軟體集團）手法持續進化，而且其商業認知也迅速疊加（更了解每個資料的價值），對HPC的覬覦有增無減。

持續努力方向

- 強調「零信任」架構概念的導入，雖然可能犧牲效能
- 加強供應鏈安全，無論自建或訂閱都會面對到這課題
- 促進HPC社群內的威脅情資分享與合作

重點回顧及管理建議

重點回顧

- HPC是高價值的運算堡壘，目前運行的架構面臨不同於傳統運算的嚴重資安威脅。
- NIST SP 800-223提供了應對這些挑戰及威脅的寶貴框架與指引。
- 訂閱者需確保HPC安全管理上扮演關鍵角色，要求服務提供商提高資安層級，訂閱者不能置身事外。
- 有效的「供應商管理」與強化「自主防禦」是大部分的HPC使用者的兩大防線（目前趨勢是訂閱者可能是大宗，自建者可能是少數）。

您的下一步

- 評估： 檢視自身對HPC的依賴程度與潛在風險。
- 檢視： 審閱與HPC供應商的合約及安全措施。
- 強化： 落實訂閱者端的安全基本要求。
- 溝通： 與供應商建立常態的安全溝通管道。

Reference

1. American Institute of Certified Public Accountants (AICPA). (n.d.). *System and Organization Controls (SOC) for Service Organizations*. AICPA. Retrieved April 14, 2025, from https://www.aicpa.org/soc

2. Amazon Web Services (AWS). (n.d.). *AWS Shared Responsibility Model*. AWS. Retrieved April 14, 2025, from https://aws.amazon.com/compliance/shared-responsibility-model/

3. Boyens, J., Paulsen, C., Moorthy, R., & Bartol, N. (2022). *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* (NIST Special Publication 800-161 Rev. 1). National Institute of Standards and Technology. [https://doi.org/10.6028/NIST.SP.800-161r1](https://www.google.com/search?q=https://doi.org/10.6028/NIST.SP.800-161r1)

4. Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide* (NIST Special Publication 800-61 Rev. 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2

5. Claburn, T. (2020, May 18). Euro supercomputers hijacked by cryptocurrency-mining malware gangs after compromising SSH logins. *The Register*. https://www.theregister.com/2020/05/18/european_supercomputers_hacked_crypto_mining/

6. Cloud Security Alliance (CSA). (n.d.). *Consensus Assessments Initiative*. CSA. Retrieved April 14, 2025, from https://cloudsecurityalliance.org/research/consensus-assessments-initiative/

7. Google Cloud. (n.d.). *Security foundations: Exploring the shared responsibility and shared fate models*. Google Cloud Architecture Center. Retrieved April 14, 2025, from https://cloud.google.com/architecture/framework/security/shared-responsibility-shared-fate

8. Intersoft Consulting. (n.d.). *General Data Protection Regulation (GDPR)*. GDPR-info.eu. Retrieved April 14, 2025, from https://gdpr-info.eu/

9. International Organization for Standardization (ISO). (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. ISO. https://www.iso.org/standard/82875.html

10. iThome編輯部. (2020年5月19日)。歐洲超級電腦運算中心爆發大規模攻擊，駭客疑似透過SSH登入植入挖礦程式。 *iThome*. https://www.ithome.com.tw/news/137711

11. Joint Task Force. (2020). *Security and Privacy Controls for Information Systems and Organizations* (NIST Special Publication 800-53 Rev. 5). National Institute of Standards and Technology. [https://doi.org/10.6028/NIST.SP.800-53r5](https://www.google.com/search?q=https://doi.org/10.6028/NIST.SP.800-53r5)

12. Lee, K., Huh, J. H., Ramaswamy, R., Saini, K. K., & Nalla, R. S. (2023). *High Performance Computing (HPC) Security: Architecture, Threats, and Countermeasures* (NIST Special Publication 800-223). National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/sp/800-223/final

13. Microsoft Azure. (n.d.). *Shared responsibility in the cloud*. Microsoft Docs. Retrieved April 14, 2025, from https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

14. OWASP Foundation. (n.d.). *OWASP Secure Coding Practices - Quick Reference Guide*. OWASP. Retrieved April 14, 2025, from https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/

15. OWASP Foundation. (n.d.). *OWASP Top 10*. OWASP. Retrieved April 14, 2025, from https://owasp.org/Top10/

16. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

17. Shilov, A. (2020, May 18). Supercomputers hacked across Europe to mine cryptocurrency. *ZDNet*. https://www.zdnet.com/article/supercomputers-hacked-across-europe-to-mine-cryptocurrency/

18. 法務部. (n.d.). *個人資料保護法*. 全國法規資料庫. 擷取於 2025年4月14日，自 https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=I0050021

Thank you

pwc.com