

# 有助於網路防禦的 20 個關鍵資安控制項 ( 稽核參考指引 )

資訊人員對於規劃資訊安全作業常有不知道從何下手的困擾。現在 SANS Institute 推出新版 ( 版本 : 2.3 ) 的關鍵資安控制項指引, 提供一份集結各方資安專家(包含 NSA, US Cert, DoD JTF-GNO 與其他官方/民間的團體)意見作為行動準則, 亦可當作稽核的依據。

## 20 個關鍵資安控制項 - 版本 2.3

- [20 個關鍵資安控制項 - 介紹](#)
- [關鍵控制項 1: 授權與未授權之裝置的清點](#) Inventory of Authorized and Unauthorized Devices
- [關鍵控制項 2: 授權與未授權之軟體的清點](#) Inventory of Authorized and Unauthorized Software
- [關鍵控制項 3: 筆記型電腦、工作站 \( 桌上型電腦 \)、伺服器之安全組態](#) Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
- [關鍵控制項 4: 網路裝置如防火牆、路由器與交換器的安全組態](#) Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- [關鍵控制項 5: 網路邊界防禦](#) Boundary Defense
- [關鍵控制項 6: 稽核記錄的維護、監控與分析](#) Maintenance, Monitoring, and Analysis of Audit Logs
- [關鍵控制項 7: 應用軟體安全](#) Application Software Security
- [關鍵控制項 8: 使用管理者權限的控管](#) Controlled Use of Administrative Privileges
- [關鍵控制項 9: 以 Need to know 為原則的存取控制](#) Controlled Access Based on Need to Know
- [關鍵控制項 10: 持續的弱點評估與矯正](#) Continuous Vulnerability Assessment and Remediation
- [關鍵控制項 11: 帳號的監視與控制](#) Account Monitoring and Control
- [關鍵控制項 12: 防護惡意程式](#) Malware Defenses
- [關鍵控制項 13: 網路埠、通訊協定與服務的限制與管制](#) Limitation and Control of Network Ports, Protocols, and Services
- [關鍵控制項 14: 無線網路裝置控管](#) Wireless Device Control
- [關鍵控制項 15: 資料外洩防護](#) Data Loss Prevention

可以協助完成上述控制項的自動化 [使用者審核工具](#)

## 更多的控制項

以下五項亦為重要的控制項, 但無法完全自動化或進行持續的監控, 須輔以人工的方式加以評估落實的程度。

- [關鍵控制項 16: 安全網路工程](#) Secure Network Engineering
- [關鍵控制項 17: 滲透測試與攻擊演練](#) Penetration Tests and Red Team Exercises
- [關鍵控制項 18: 事件應變處理能力](#) Incident Response Capability
- [關鍵控制項 19: 資料回覆能力](#) Data Recovery Capability
- [關鍵控制項 20: 資訊安全技能評量與合適的教育訓練以補不足](#) Security Skills Assessment and Appropriate Training to Fill Gaps

## 參考資料

- [SANS \(SysAdmin, Audit, Network, Security\) Institute](#)

Last update: 2009/12/23 10:51 security:guideline:twenty\_critical\_security\_controls [https://net.nthu.edu.tw/netsys/security:guideline:twenty\\_critical\\_security\\_controls](https://net.nthu.edu.tw/netsys/security:guideline:twenty_critical_security_controls)

---

- [Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines](#)
- [SANS新版關鍵資安控制項目出爐 - 資安人雜誌網站](#)

From: <https://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link: [https://net.nthu.edu.tw/netsys/security:guideline:twenty\\_critical\\_security\\_controls](https://net.nthu.edu.tw/netsys/security:guideline:twenty_critical_security_controls)

Last update: **2009/12/23 10:51**

