資訊服務採購
資安規定與政策

112年8月

大綱

數位發展部資通安全署
Administration for Cyber Security, moda

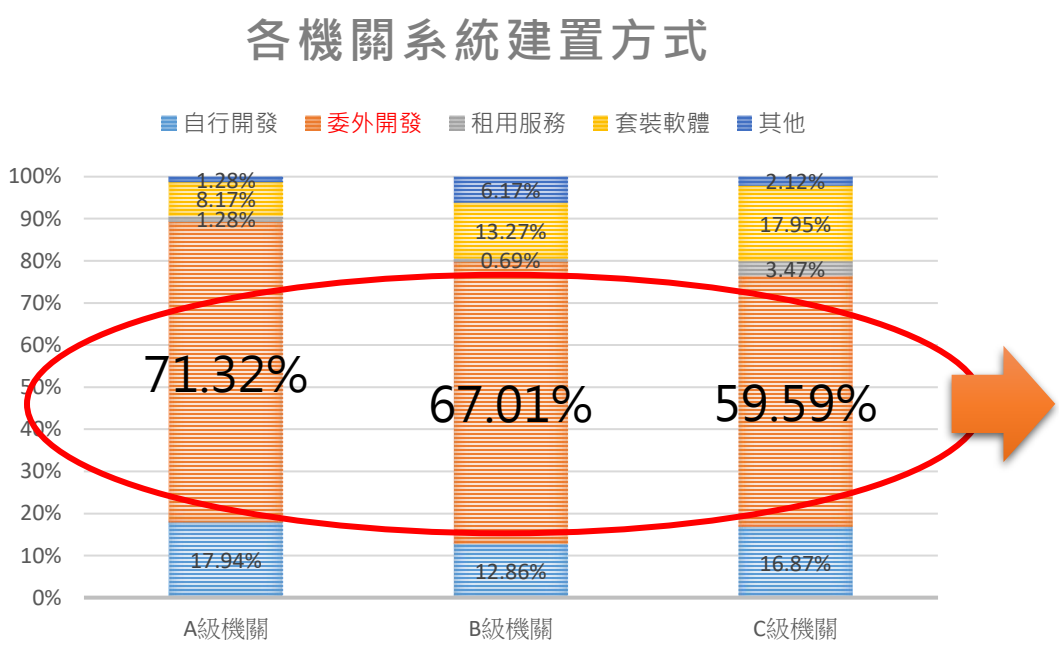
- 前言
- 資通系統委外現況
- 資安事件案例分享
- 防護重點及注意事項
  - 落實資安法委外規定
  - 資通系統籌獲各階段資安強化措施
  - 基於安全的設計
- 總結

前言

- 全球供應鏈安全是重要議題，資訊服務商因資安防護或設計概念不足，資安事件層出不窮。
- 強化供應鏈之安全，避免供應商成為資安破口，一旦發生資安事件，伴隨公私部門的重大影響與衝擊。
- 政府機關因應資安法規要求，逐漸提高自身防禦能量，駭客開始利用供應商之脆弱點，作為攻擊政府機關之跳板，造成連鎖攻擊效應。

資通系統委外現況

- 各機關111年度維護計畫實施情形，公務機關委外辦理資通系統建置之統計

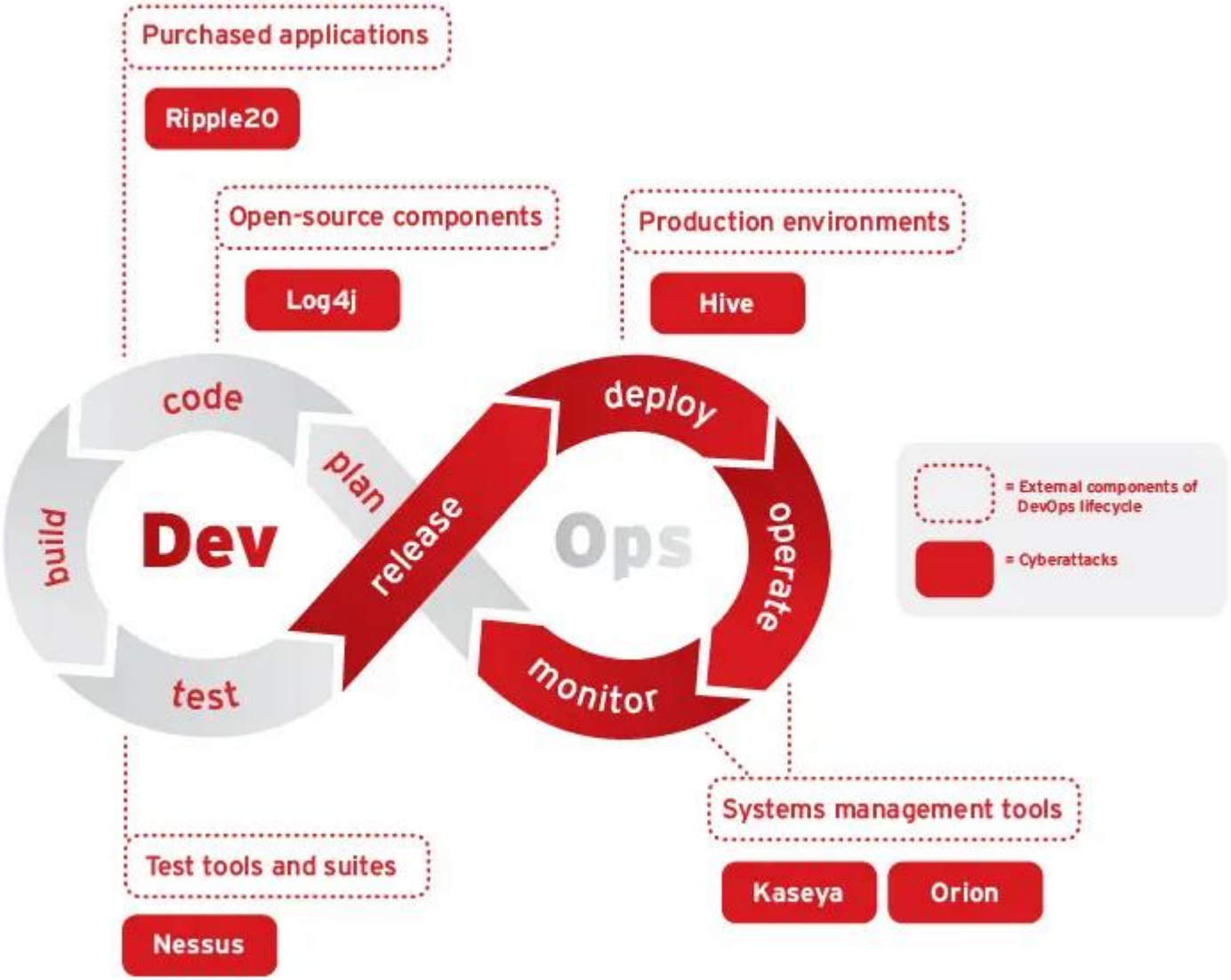


委外廠商	委託機關數	維運系統數
A廠商	93	183
B廠商	78	188
C廠商	70	90
D廠商	64	122
E廠商	60	124
F廠商	58	60
G廠商	57	173
H廠商	45	128
I廠商	43	107

服務多家政府機關之廠商，倘未落實資安管理，將形成資安破口，而造成連鎖之攻擊效應

資安事件案例分享

軟體供應鏈的網路資安

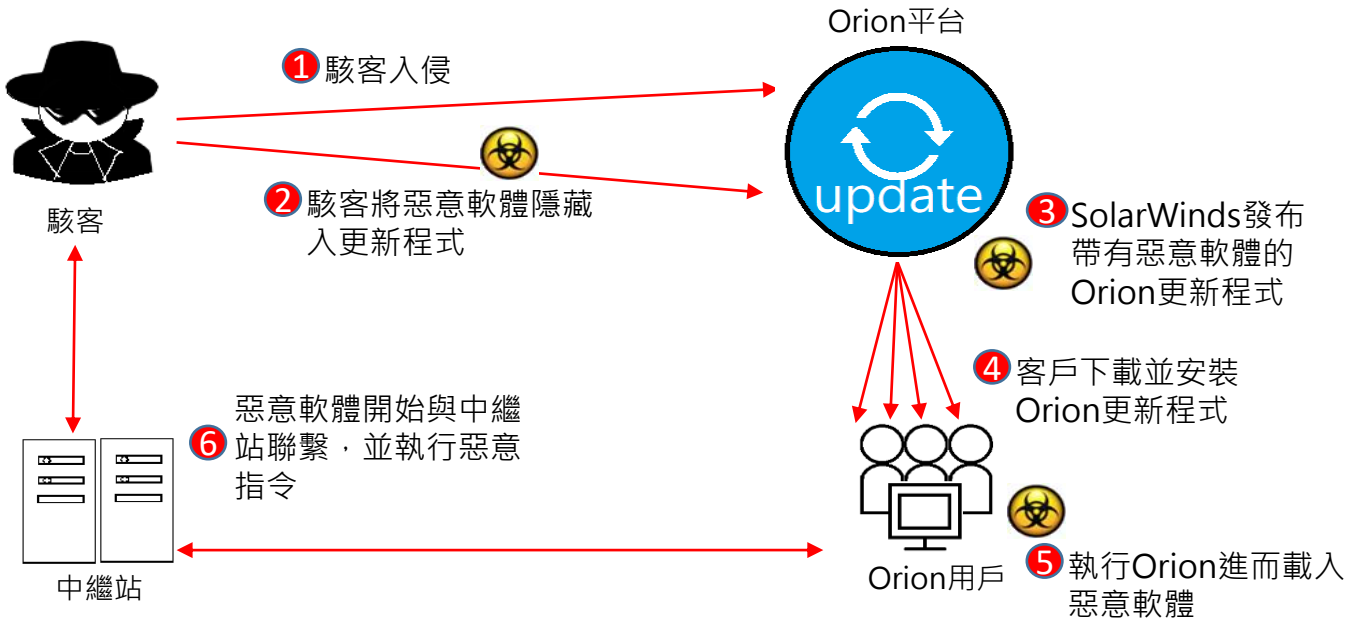


https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=10063

國外供應鏈攻擊案例

案情概要

- SolarWinds Orion平台是美國政府機構和企業廣為使用之整合式網路管理工具，109年12月發生國家級駭客利用該平台之重大漏洞植入惡意軟體，並藉由更新機制進行散播，進而攻擊美國財政部與商務部及其他民間企業。



國內供應鏈攻擊案例

案情概要

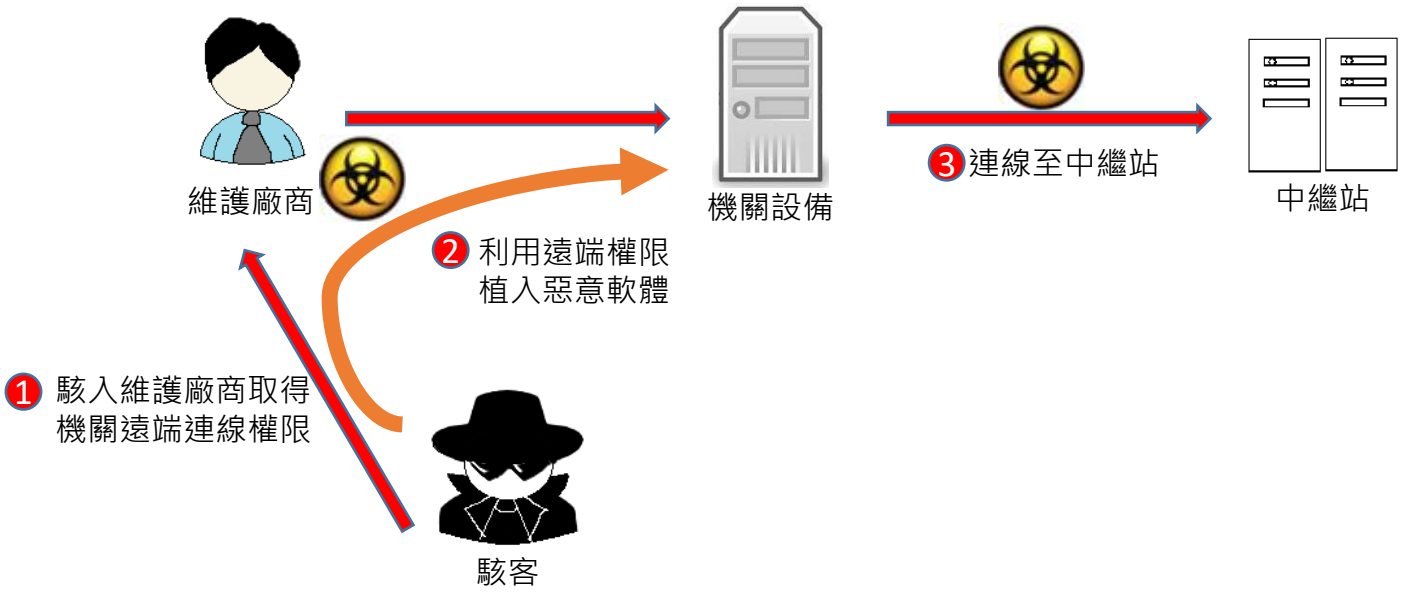
- 駭客入侵機關資訊服務廠商，並透過VPN將勒索病毒感染至機關內部，導致機關內部電腦無法正常運作，惟未造成資料外洩
- 透過實地查核發現，機關VPN管理機制待加強，VPN內部未設置存取控管機制，且針對資訊服務業者之資安防護未有要求，亦未限制資訊服務業者連線範圍

防護建議：應採原則禁止機關委外廠商進行遠端維護資通系統

國內供應鏈攻擊案例

案情概要

- 機關發現設備於夜間時有異常連線，連線IP經辨識為來自維護廠商IP，以VPN帳號連至跳板機存取後，該設備即遭植入惡意程式，並連至中繼站。經機關與廠商確認，當時並無人員進行遠端設備維護作業。



防護建議：應採原則禁止機關委外廠商進行遠端維護資通系統

防護重點及注意事項

防護重點及注意事項

1.落實資安法委外規定 (1/3)

數位發展部資通安全署
Administration for Cyber Security, moda

甲方

委外辦理資通系統之建置、維運或資通服務之提供，應考量廠商之專業能力與經驗、委外項目之性質及資訊安全需求，選任適當之廠商，並監督其資通安全維護情形

資通安全管理法第9條

乙方

委外廠商應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員

資通安全管理法施行細則第4條第1項第2款

甲方

委託關係終止或解除時，應確認委外廠商返還、移交、刪除或銷毀履行委託契約而持有之資料

資通安全管理法施行細則第4條第1項第7款

乙方

受託業務涉及國家機密者，執行受託業務之廠商相關人員應接受適任性查核，並依國家機密保護法之規定，管制其出境

資通安全管理法施行細則第4條第1項第4款

1.落實資安法委外規定 (2/3)

數位發展部資通安全署
Administration for Cyber Security, moda

乙方

受託業務包括客製化資通系統開發者，受託者應提供該資通系統之安全性檢測證明

資通系統屬委託機關之核心資通系統，或委託金額達新臺幣一千萬元以上者，委託機關應自行或另行委託第三方安全性檢測證明

涉及利用非自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明

資通安全管理法施行細則第4條第1項第5款

1. 安全性檢測建議包含弱點掃描、滲透測試、源碼掃描等
2. 依資通安全責任等級分級辦法附表十資通系統防護基準，針對系統與服務獲得之構面防護需求為高之系統，需執行源碼掃描、滲透測試及弱點掃描，要求；防護需求為中或普等級之系統，至少需執行弱點掃描。

1.落實資安法委外規定 (3/3)

數位發展部資通安全署
Administration for Cyber Security, moda

甲方

具敏感性或國安(含資安)疑慮之業務範疇，於招標文件載明不允許投審會公告之陸資資訊服務業者參與

行政院秘書長
109年11月9日院臺護字第1090195928號函

乙方

委外廠商辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證

資通安全管理法施行細則第4條第1項第1款

乙方

委外廠商辦理受託業務得否複委託、得複委託之範圍與對象，及複委託之受託者應具備之資訊安全維護措施

資通安全管理法施行細則第4條第1項第3款

甲方

委託機關應定期或於知悉委外廠商發生可能影響受託業務之資安事件時，以稽核或其他適當方式確認受託業務之執行情形

資通安全管理法施行細則第4條第1項第9款

乙方

受託者執行受託業務，違反資通安全相關法令或知悉資通安全事件時，應立即通知委託機關及採行補救措施

資通安全管理法施行細則第4條第1項第6款

2.資通系統籌獲各階段資安強化措施

- 行政院111年5月26日院臺護字第1110174630號函「**資通系統籌獲各階段資安強化措施**」

請參閱本署網站https://s.moda.gov.tw/tDpfZWdziw4z

需求階段

- **系統**防護需求**等級標註**(普、中、高)
- **資安**作業**經費5%**
- 受託者**資安作業應納入評選**項目(10%)
- **資安**評選**委員**

建置階段

- **核心**資通**系統**則應聘請**外部資安專家**協助檢視資安管理作為
- **核心**資通**系統**且委託金額達**1千萬元以上**，應**評估**獨立驗證與認證(IV&V)

維運階段

- 請**資安人員二線**協助**確認**系統維運之**資安**作業
- 應對**高**防護**等級**之資通系統**廠商**辦理資安**稽核**
- **受託業務**發生**重大**資安**事件**，機關應辦理**廠商**資安**稽核**，並將**結果送交**主管機關

為瞭解各機關辦理現況，已通函請各機關於112年9月1日前提供施行意見，俾利後續檢討評估相關措施

3.基於安全的設計(1/2)

- 基於安全的設計(Security by Design)也稱為設計安全，在軟體工程中，指軟體的設計基礎包含資訊安全的觀點：
  - 軟體的惡意行為視為必然
  - 資安漏洞被發現時，減少對軟體的衝擊
  - 軟體開發設計階段，列出**安全需求**、**辨識安全風險**及**套用控制措施**
  - 建立後續**安全功能驗證**的基礎
- 落實安全的軟體發展生命週期(SSDLC)，從設計先期著手整體資訊系統安全。導入好的軟體設計措施，可減少開發過程中可能造成資安漏洞的風險

3.原則禁止遠端存取(2/2)

◘ 行政院資安處110年3月2日院臺護字第1100165761號函

各機關開放內部同仁及委外廠商進行遠端維護資通系統，應採「**原則禁止、例外允許**」方式辦理，若機關因地理限制、處理時效及專案特性等因素，須開放前揭人員自遠端存取資通系統時，應至少辦理下列防護措施：

1.依資安法遠端存取相關規定辦理

2.以短天期為限

3.建立異常行為管理機制

4.結束遠端存取期間後，應確實關閉網路連線，並更換遠端存取通道(如VPN)登入密碼

總結

- 資訊服務採購安全，應**落實法遵**及**軟體安全設計**，以達成委託及受託雙贏局面
- 依資通安全需求與機關ISMS相關規定，建立**安全管控制**度與執行**資安計畫**
- 完善資通安全管理措施或通過**第三方驗證**；人員應受訓取得證照，具備**資安專業**及類似業務經驗
- **原則禁止遠端連線**，確實評估**潛在風險**，以明確資通安全需求
- 受託業務**發生資安事件**時，應立即通知委託機關及採行補救措施

數位發展部資通安全署

Administration for Cyber Security, moda

資安是持續精進的風險管理