

資安推動小組  
全校資通安全內部稽核  
自我檢核說明會  
暨啟始會議

日期：114/07/14、23、28

ISMS.NTUT.EDU.TW





# 大綱

1	依據國立大專校院資通安全維護作業指引
2	國立臺北科技大學 資通安全推動委員會
3	7-8月內部稽核前應辦項目
4	全校性資安制度第三~四季規劃
5	全校單位「資通安全內部稽核作業」
6	團隊組成
7	受稽核單位-實地稽核
8	稽核方式
9	稽核範圍
10	稽核計畫
11	資通安全防護巡迴研討會摘要
12	資安新聞、報告結束



# 依據國立大專校院資通安全維護作業指引

二、各校依資通安全管理法第 10 條訂定、修正及實施資通安全維護計畫，適用範圍應涵蓋全校各系、院、所教學單位及各行政單位（以下簡稱全校各單位），並應注意下列事項：

- （一）**資通安全長之配置**：各校置資通安全長，宜指派主任秘書以上人員兼任，以落實推動及監督校內資通安全相關事務。
- （二）**資通安全推動組織**：各校資通安全推動組織宜由資通安全長召集全校各單位主管或副主管組成，每年至少召開會議一次。

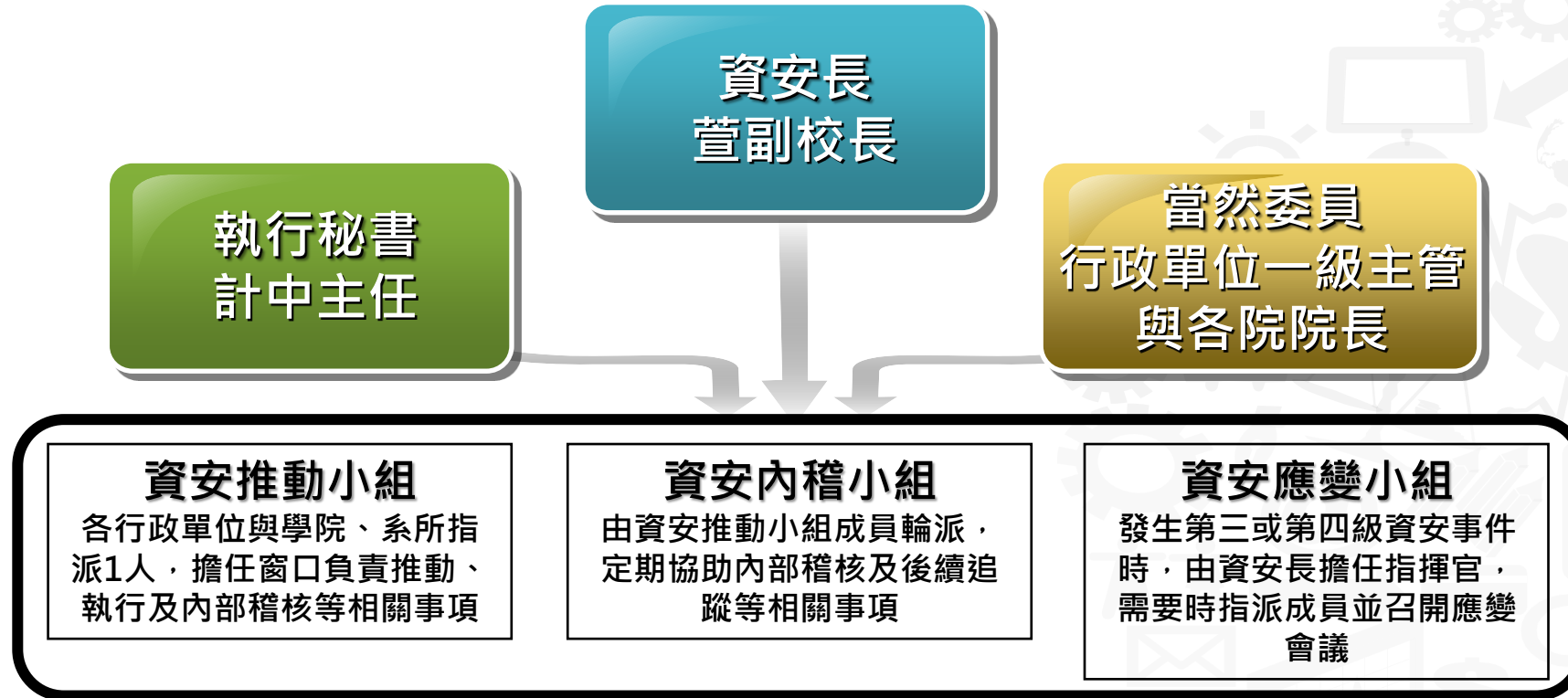


- 系統及資訊之盤點，  
提交之「資通系統資  
、或使用各校網域名  
安全稽核，稽核範圍  
(保有個人資料)風  
後順序，分年分階段  
計畫。



# 國立臺北科技大學 資通安全推動委員會

113年4月30日 112學年度第2學期第5次行政會議修正通過

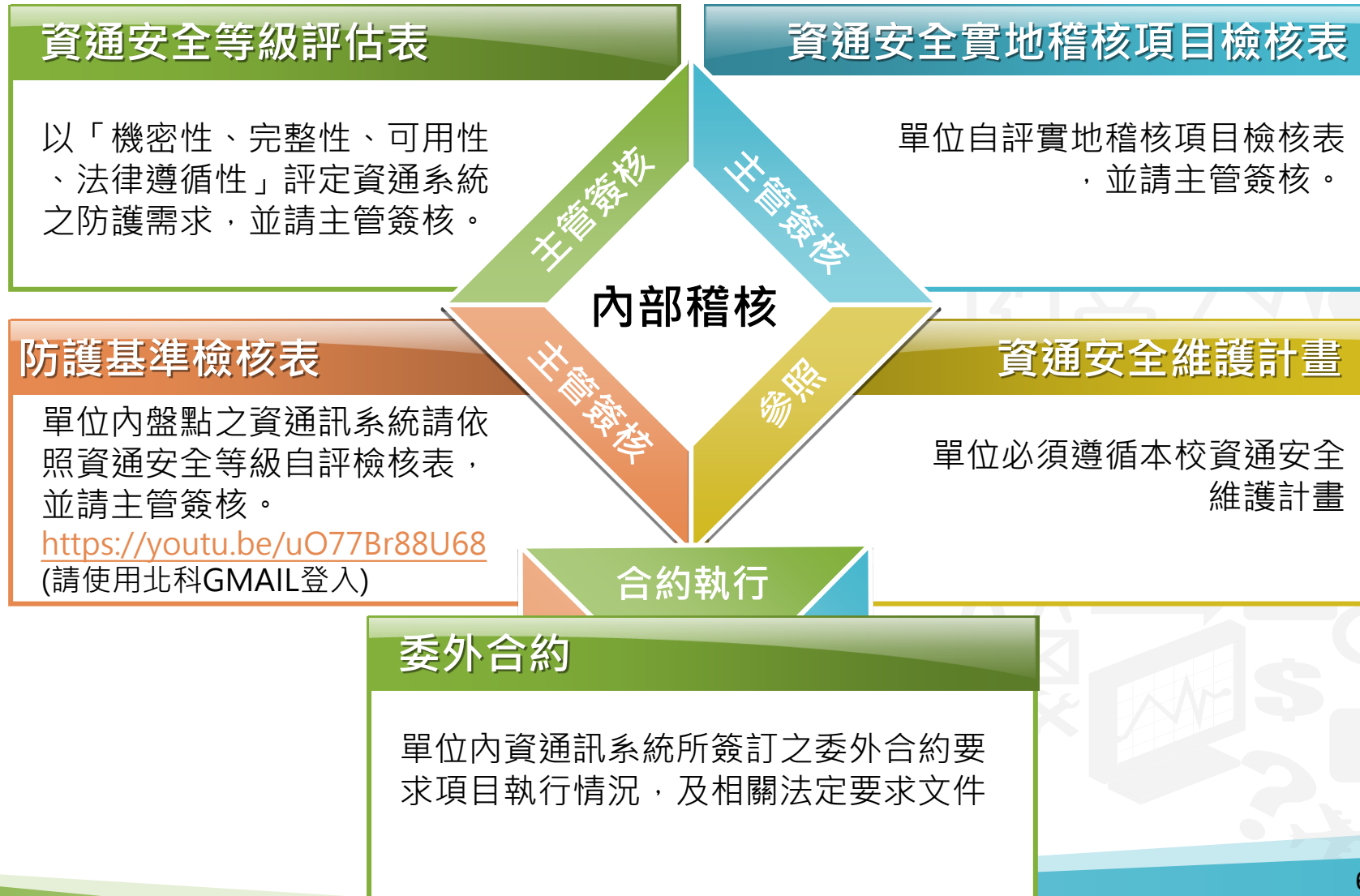


依據北科大資通安全維護計畫執行

檔案位置：校園入口網站/雲端文件夾/00資通安全管理文件/北科大資通安全維護計畫



# 7-8月內部稽核前應辦項目







## 全校性資安制度第三~四季規劃

期程	預計辦理事項及落實方案	執行進度
5-6月	<ul style="list-style-type: none"><li>● 教育訓練-全校導入資訊安全管理制度教育訓練<ol style="list-style-type: none"><li>1. 5/19(一)10時~12時-共同科館三樓-313教室</li><li>2. 5/20(二)10時~12時-共同科館三樓-312教室</li></ol></li><li>● 資通系統與服務資產盤點盤點回收<ol style="list-style-type: none"><li>1. 6/30(一)前回傳盤點資訊</li></ol></li></ul>	已完成
7月	<ul style="list-style-type: none"><li>● 教育訓練-113年全校資通系統自我檢核說明<ol style="list-style-type: none"><li>7/14(一)、7/23(三)、7/28(一) 09:30~12:30 共科三樓-312教室</li></ol></li><li>● 教育部委教育體系資安檢測技術服務中心進行機關資安攻防演練到9月</li></ul>	進行中
7-11月	<ul style="list-style-type: none"><li>● 辦理全校資通系統內部稽核<ol style="list-style-type: none"><li>1. 上傳稽核作業自我檢核檔案</li><li>2. 安排稽核日期並輪派資安窗口填選可參加的稽核隊伍</li><li>3. 委請中華電信主導稽核員偕同計網中心輔導「資安推動小組」成員進行「資通安全內部稽核作業」</li></ol></li></ul>	進行中
10月30日	<ul style="list-style-type: none"><li>● 教育部偕同教育機構驗證中心對本校進行資通安全實地稽核<ol style="list-style-type: none"><li>召集本校資通安全推動委員會與會，抽檢各單位資通安全執行情況</li></ol></li></ul>	規劃中
12月	<ul style="list-style-type: none"><li>● 召開全校資通安全管理審查會<ol style="list-style-type: none"><li>匯整全校資料進行報告，檢討各單位執行成效與各項稽核缺失。</li></ol></li></ul>	規劃中



# 全校單位「資通安全內部稽核作業」

- 稽核範圍：全校各單位(分年分階段)
- 時程：114年09月1日~11月28日
- 稽核員：由中華電信主導稽核員偕同計網中心輔導「資安推動小組」成員。
- 因接觸各單位機敏感性資訊，請配合填寫保密切結書。





# 團隊組成

各受稽核單位&抽該單位資通系統





# 受稽核單位-實地稽核

1. 資安窗口配合檢視收集  
相關**文件化資訊**之簽核文件

1. 單位  
資安窗口  
全程陪同

2. 單位內所有同仁之  
個人電腦設定、教育訓練  
時數進行抽檢稽核

4. 單位內  
物聯網  
設備

**抽檢  
稽核**

2. 單位內  
所有同仁

4. 單位內所有印表機、  
NAS、監視系統、刷卡系  
統進行抽檢稽核

3. 單位內  
資通系統  
與服務

3. 單位內所有資通系統與  
服務及委外廠商進行抽檢  
稽核如合約、應用系統、  
SERVER等



# 稽核方式

內部稽核小組  
資通安全實地稽核項目  
檢核表紀錄佐證

受稽單位  
資安窗口

檢視1.資通系統與服務資產清冊、2.資訊系統安全等級評估表、3.資通系統防護基準檢核表、4.資通安全實地稽核項目檢核表

個人電腦  
設備和文件

檢視個人電腦帳號密碼原則、GCB+VANS、防毒軟體→異常軟體、個人教育訓練資安時數證明

資通訊系  
統與服務

配合1.資通系統與服務資產清冊、2.資訊系統安全等級評估表、3.資通系統防護基準檢核表、4.委外合約，檢核相關文件化資訊執行狀況

委外廠商  
法規要求

除配合上述委外合約要求之相關文件化資訊執行狀況，廠商保密協議、廠商資通安全管理措施或通過第三方驗證、廠商資安教育訓練、擁有資安證照或具有資安業務經驗資安人員

物聯網  
設備

檢視相關物聯網設備密碼原則、安全性設定



內部資通安全稽核：各校辦理內部資通安全稽核，稽核範圍應包含全校各單位。各校得就資通系統（保有個人資料）風險高低、教學單位特性評估訂定推動先後順序，分年分階段規劃辦理，並明訂於各校資通安全維護計畫。**(今年主要的稽核範圍只有教學單位)**

## 教學單位(窗口)

- (管理學院)工業工程與管理系-陳冠翰
- 經營管理系(114年第一順位)-陳柏瑄
  - (設計學院)互動設計系-傅子恒
  - 工業設計系-林志昇
- (人文與社會科學學院)技術及職業教育研究所-蔡銘修
  - 智慧財產權研究所-郭宏杉
  - 文化事業發展系-吳欣怡
  - 師資培育中心-蔡銘修



# 稽核計畫

近期會再請受稽單位安排日期並請各單位窗口回填可參加之隊伍

單位	稽核日期	主稽	副稽	觀察員	觀察員	觀察員
能源與冷凍空調工程系-周義翔		中華電信	計網中心			
太空系統工程研究所-黃思瑋		中華電信	計網中心			
自動化科技研究所-胡念祖		中華電信	計網中心			
五年制專科部智慧自動化工程 科-李昭德		中華電信	計網中心			
分子科學與工程系-劉俊宏		中華電信	計網中心			
化學工程與生物科技系-陳韻文		中華電信	計網中心			
材料及資源工程系-邱家吉		中華電信	計網中心			
資源工程所-邱家吉		中華電信	計網中心			
(管理學院)工業工程與管理系- 陳冠翰		中華電信	計網中心			
經營管理系-陳柏瑄		中華電信	計網中心			



# 稽核計畫

近期會再請受稽單位安排日期並請各單位窗口回填可參加之隊伍

單位	稽核日期	主稽	副稽	觀察員	觀察員	觀察員
(設計學院)互動設計系-傅子恒		中華電信	計網中心			
工業設計系-林志昇		中華電信	計網中心			
(人文與社會科學學院)技術及 職業教育研究所-蔡銘修		中華電信	計網中心			
智慧財產權研究所-郭宏杉		中華電信	計網中心			
文化事業發展系-吳欣怡		中華電信	計網中心			
師資培育中心-蔡銘修		中華電信	計網中心			
計算機與網路中心-李亮宏 (每年)		中華電信	計網中心			







# 資通安全防護巡迴研討會摘要-資安署



## 資安事件案例-供應商遭駭

駭客利用**廠商VPN帳號**登入後，再透過機關人員帳號進入系統查詢病患資料，致個資外洩，通報3級資安事件。



### 建議防範措施

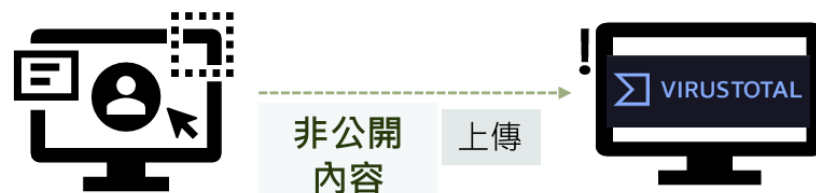
- 對於每一種允許之遠端存取類型，均應**先取得授權，建立使用限制、組態需求、連線需求及文件化**。
- 機關應加強遠端存取控制機制，依「**原則禁止、例外允許**」方式辦理
- 若需允許外部遠端維護，應加強防護措施，如採VPN並啟用**多因子認證機制**等，以強化遠端登入身分鑑別。



# 資通安全防護巡迴研討會摘要-資安署

## 資安事件案例-機敏資訊上傳公開網站致外洩

某縣政府接獲協力廠商告知該府SOC月報疑似遭上傳至VirusTotal網站，內容包含該府網段資訊等機敏資訊，經查為該府SOC廠商不慎將該報告上傳至網站上，致機敏資料外洩，爰通報3級資安事件。



### 強化措施參考

- 確認資料機敏性資料，**避免將機敏資訊上傳至公開系統**。
- 如需檢測是否為惡意檔案，建議**優先使用我國自有之VirusCheck**，如需使用VirusTotal，應**透過檔案Hash值檢查**。
- **針對文件機敏性分級**，如設置TLP (Traffic Light Protocol)分級。
- 注意廠商委外管理，針對機敏資訊應加強管理與防護。



# 資通安全防護巡迴研討會摘要-資安署



## 工程會訂定「採購契約範本附記條款特別聲明」

### 工程會函釋

工程會114.5.20工程企字第1140100189號函訂定「採購契約範本附記條款特別聲明」

機關辦理各類採購時，契約如約定須交付書面履約成果者，應將「採購契約範本附記條款特別聲明」納入採購契約，重點摘述如下：

◆ **履約禁用DeepSeek(含禁止廠商使用DeepSeek製作書面履約成果)**：於特別聲明明定，契約如約定廠商須交付書面履約成果者，應禁止使用DeepSeek 製作，並增訂通案之生成式AI使用條款，包含：「履約禁用中國大陸廠牌資通訊產品」、「不得提供公務機密予AI」、「使用AI履約須報機關同意」，**並輔以切結書規範廠商責任**。

◆ 廠商如違反上述禁用條款，機關得終止或解除契約。

### 【切結書範本】

使用資通訊產品禁制事項同意書/切結書  
(得標後檢附)

本廠商(得標廠商)履行(採購機關)辦理之(標的名稱)案，已充分瞭解並遵行本特別聲明所定資通訊產品之禁制事項規範，於履約過程及履約標的均無違反前述禁制事項，如有違反，願賠償一切因此所生之損害，並擔負相關民、刑事責任。

立書人

投標廠商： (蓋章)

負責人： (蓋章)

中華民國 年 月 日



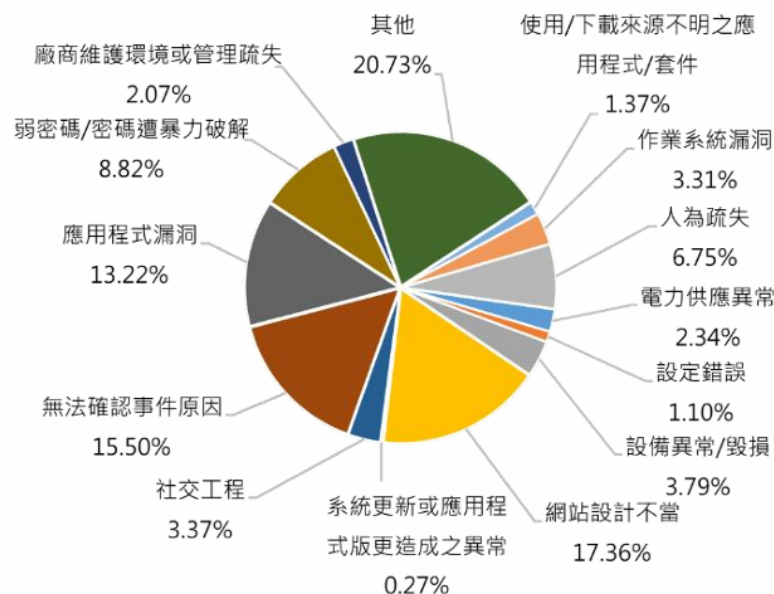
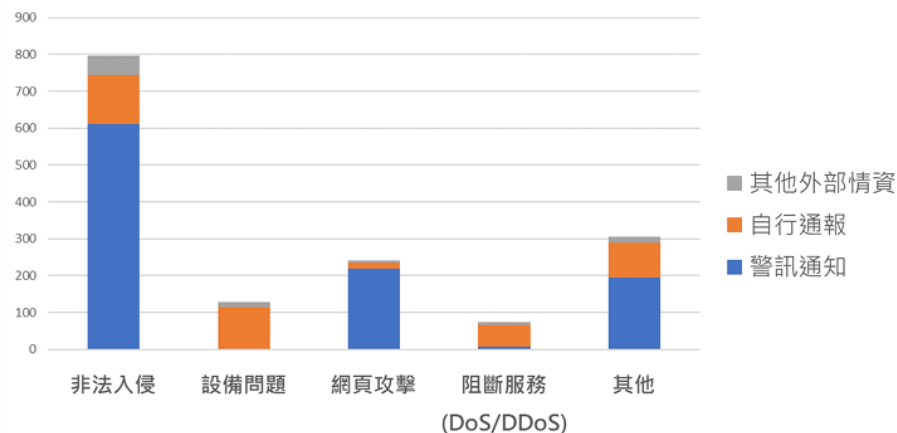
# 資通安全防護巡迴研討會摘要-資安院

## 通報事件分析(2/2)

- 事件類型以 **非法入侵** 為大宗，其中又以 **機關接獲資安院警訊通知** 後進行通報為主

- 可識別之事件原因

- 「網站設計不當」 17.36%
- 「應用程式漏洞」 13.22%
- 「弱密碼/密碼遭暴力破解」 8.82%





# 資通安全防護巡迴研討會摘要-資安院

## 廠商供應鏈橫向移動

機關**供應鏈廠商遭駭**，橫向移動機關內部，DNS Tunnel報到



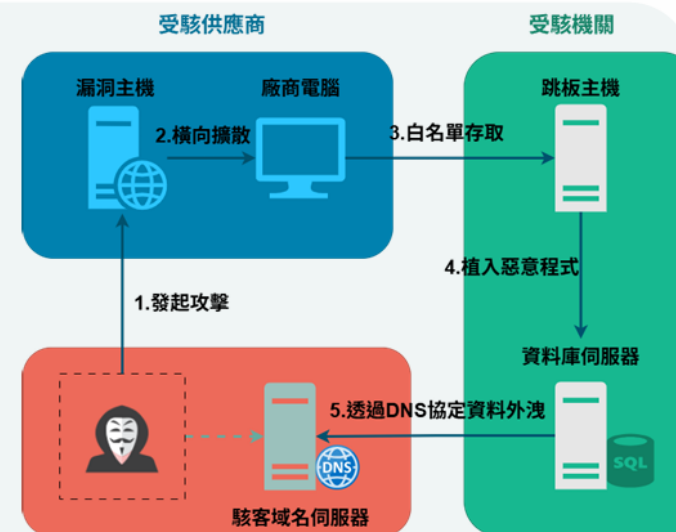
案情提要

- 駭客利用**供應商端主機漏洞**作為入侵起點，避開直接攻擊受駭機關的防線
- 供應商內部進行**橫向移動**，逐步掌握更多資源並尋找對外可用跳板，藉由跳板機對機關進行白名單連線，**躲避監控與偵測**
- 成功滲透至內部網路後入侵資料庫伺服器，部署惡意程式建立持續控制
- 駭客使用**偽冒chatgpt網域**透過**DNS Tunnel**進行資料外洩



防護建議

- 強化第三方存取管控與跳板機連線驗證機制，僅提供廠商必要性權限帳號存取
- 部署相關防護偵測機制，監控和限制橫向移動工具的使用，部署端點與內網攻擊偵測機制，針對應盡速處理告警，減輕受駭程度





## 資安新聞

- 每年駭進消防系統3千萬次搶生意 救護車還沒來殯葬業者已到
- <https://www.ettoday.net/news/20250701/2988075.htm>



報告結束

 CNC 計算機與網路中心  
COMPUTER & NETWORK CENTER

感謝您的參與推動  
敬祝平安順利

ISMS.NTUT.EDU.TW

