# 經濟部工業局 110 年「跨域資安強化產業推動計畫」
# 資訊安全檢測診斷服務申請須知

一、目的

資安事件層出不窮，產業鏈上下游的安全防護已成為國際重要議題，企業除了加強自身的資安防護能力，對於合作廠商及供應商的資安防護能力亦需加以重視，以確保商品生產或服務提供過程的各個環節都受到妥善的防護。為提升國內產業資安防護能力，經濟部工業局推動產業資訊安全檢測診斷服務，並透過供應鏈串聯產業上下游，鼓勵供應鏈或集團連鎖企業完善整體資安防護，進而促進供應鏈生態系統資安防護能力。資安檢測診斷服務包含「資訊安全風險現況評估」、「伺服主機弱點掃描檢測」、「資訊設備組態基準檢測」、「網路封包側錄分析」、「惡意程式檢視檢測」及「防火牆檢測」等健診項目，協助受測企業掌握自身資安管理與防護現況，並了解如何強化、改善缺失及進一步建立預防措施。

二、申請資格

(一) 申請受測企業須為依我國公司法設立，並由中央主管機關核准登記之本國公司，如資通訊製造/服務、智慧機械、智慧製造或智慧應用等業者。

(二) 為強化供應鏈資安，歡迎邀請合作夥伴或供應商一同申請，將優先受理申請。

三、檢測項目

受測企業依檢測項目及檢測範圍 IP 數分為四類。

(一) A、B 類受測企業檢測項目包含：資訊安全風險現況評估、伺服主機弱點掃描檢測、資訊設備組態基準檢測及網路封包側錄分析，共四項。

(二) C、D 類受測企業檢測項目包含：資訊安全風險現況評估、伺服主機弱點掃描檢測、資訊設備組態基準檢測、網路封包側錄分析、惡意程式檢視檢測及防火牆檢測，共六項。

四、申請費用及繳費方式

資訊安全檢測診斷服務由經濟部工業局部分補助，受測企業須交付自籌款如下：

(一) A 類受測企業(檢測範圍於 101 IP~200 IP)，每案新臺幣 126,000 元（政府補助 84,000 元、受測企業自負 42,000 元）

(二) B 類受測企業(檢測範圍於 20 IP~100 IP)，每案新臺幣 74,550 元（政府補助 64,050 元、受測企業自負 10,500 元）

(三) C 類受測企業(檢測範圍於 101 IP~200 IP)，每案新臺幣 177,450 元（政府補助 126,000 元、受測企業自負 51,450 元）

(四) D 類受測企業(檢測範圍於 20 IP~100 IP)，每案新臺幣 115,500 元（政府補助 94,500 元、受測企業自負 21,000 元）

(五) 受測企業選定類別後，請將自負款匯款至以下帳戶，匯款後請將收據掃描 Email 至 kevin@cisanet.org.tw 或傳真至(02) 2553-1319，請註明「資訊安全檢測診斷服務－○○○企業自負款」字樣。

匯款銀行：玉山銀行中山分行(銀行代號 808)

銀行帳號：0417-968-097989

匯款戶名：中華民國資訊軟體協會

**(六) 繳費所產生之手續費或郵資，皆由受測企業自行負擔，並應於申請通過後立即支付，未繳交費用者，計畫執行單位有權拒絕受理。**

五、申請方式

請檢附下列資料，Email 並將正本寄送至 103445 臺北市大同區承德路二段 239 號 6 樓 中華民國資訊軟體協會；請於信封上註明「申請資訊安全檢測診斷服務」字樣。

(一) 資訊安全檢測診斷服務申請暨切結書（格式如附件一）。

(二) 資訊安全檢測診斷服務自負費用繳費證明。

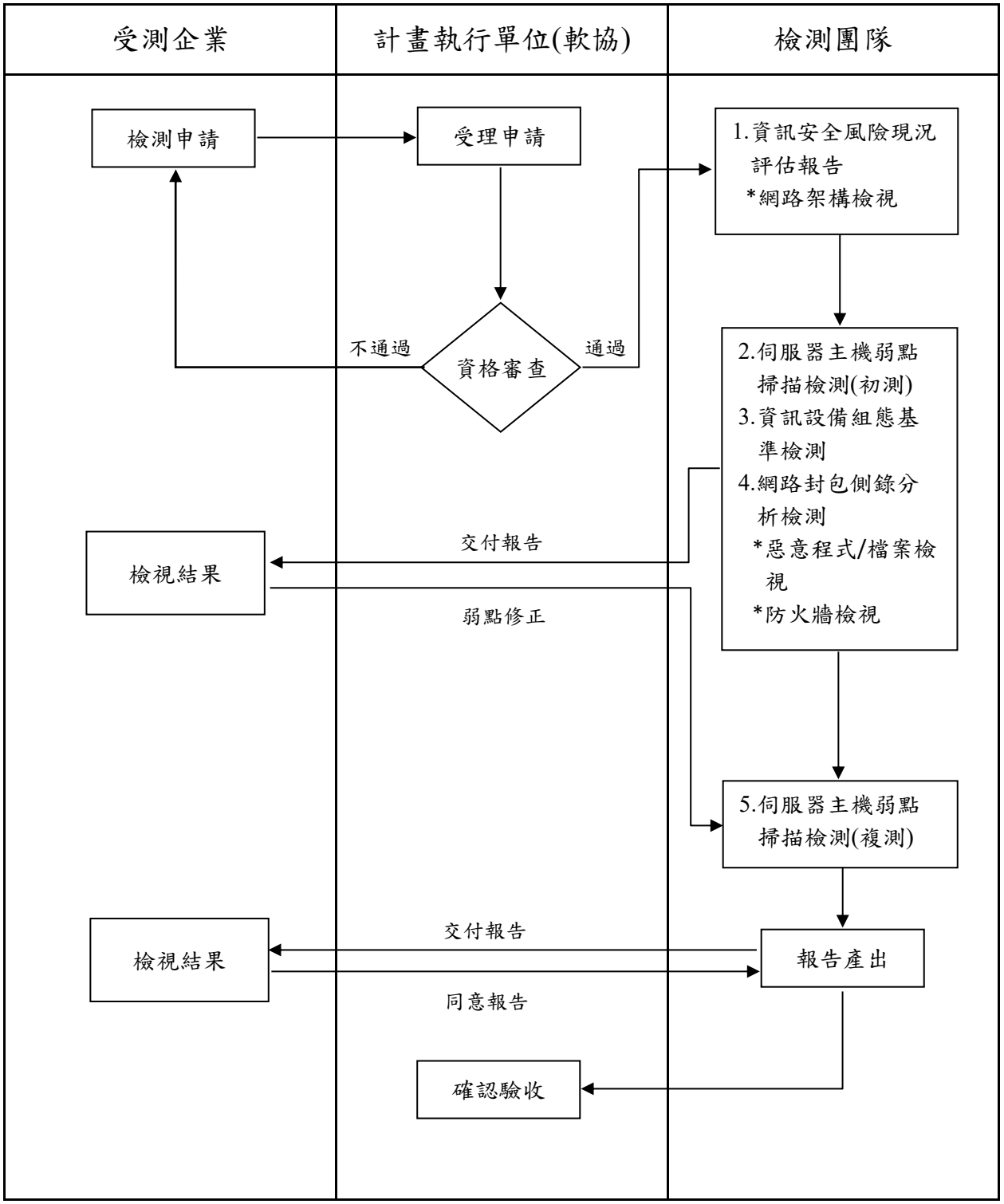
六、檢測診斷服務團隊派案原則：

本服務將受理 40 家符合資格之企業申請，包含 A 類 3 家、B 類 15 家、C 類 10 家及 D 類 12 家，依申請先後順序額滿為止。檢測診斷服務團隊與受測企業須簽保密切結書，以利專案進行。

(一) 檢測團隊推薦之受測企業，優先派案予推薦該受測企業之檢測團隊執行。

(二) 受測企業可於本計畫遴選合格檢測團隊中，提出指定檢測團隊申請，未指定或團隊檢測數量已額滿，由計畫執行單位依序派案。

七、資安檢測診斷服務申請及執行流程




*註：網路架構檢視、惡意程式/檔案檢視、防火牆檢視為C、D類受測企業檢測項目。

八、資訊安全風險現況評估作業

(一) 檢測團隊將參採資訊安全管理標準 ISO 27002 研擬「訪談分析紀錄表」，依訪談結果產出「資訊安全風險現況評估報告」；C、D 類「資訊安全風險現況評估報告」另含「網路架構檢視報告」，做為資訊安全技術檢測之參考資料。

(二) 「資訊安全風險現況評估報告」將整合伺服主機弱點掃描檢測、資訊設備組態基準檢測與網路封包側錄分析結果，提供受測企業「總體資安風險評估報告」。

九、資訊安全技術檢測作業

(一) 伺服主機弱點掃描檢測作業：針對作業系統的弱點、網路服務的弱點、作業系統或網路服務設定、帳號密碼設定及管理方式等進行弱點檢測，系統弱點掃描的檢測項目須符合 Common Vulnerabilities and Exposures (CVE)發布的最新版本弱點內容，並參採 CVE 評分系統 CVSS (Common Vulnerability Scoring System)給予嚴重(Critical)、高(High)、中(Medium)、低(Low)及無(None)之弱點等級評分。檢測項目至少包含以下項目：

1. 作業系統未修正的弱點掃描。
2. 常用應用程式弱點掃描。
3. 網路服務程式掃描。
4. 木馬、後門程式掃描。
5. 帳號密碼破解測試。
6. 系統之不安全與錯誤設定檢測。
7. 網路通訊埠掃描。

此項檢測需完成初、複測作業，其流程圖如下所示：

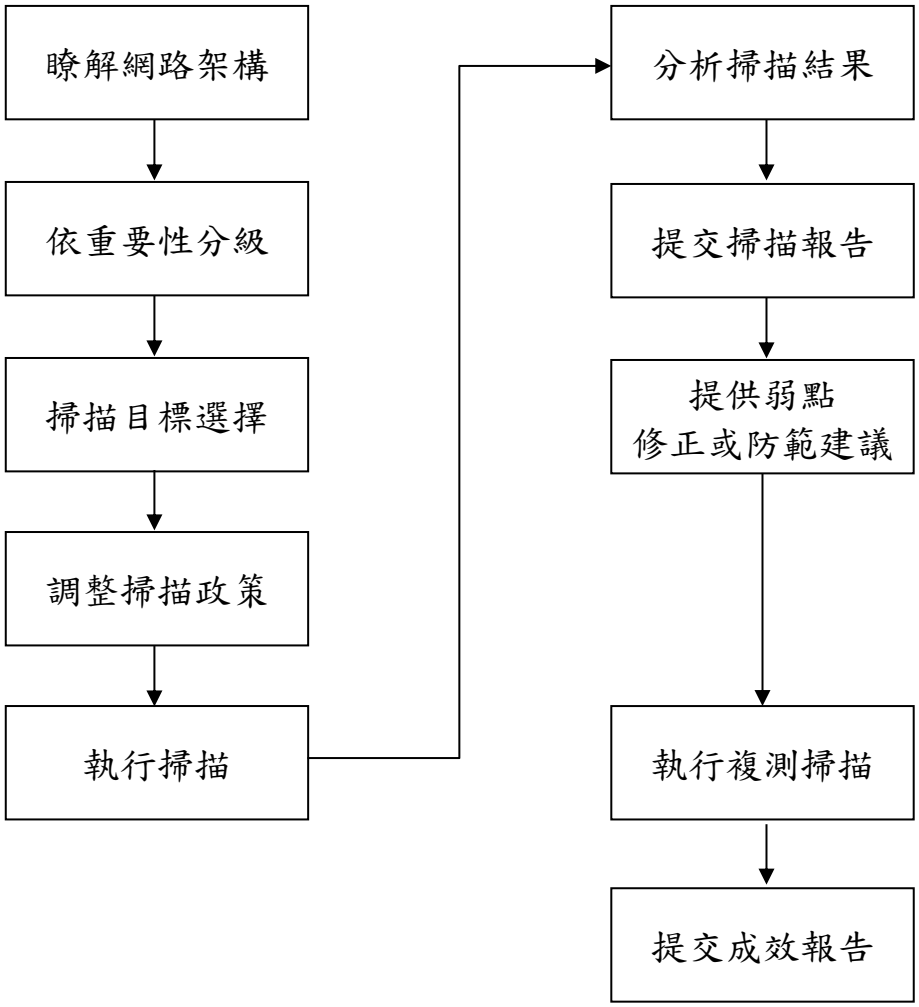



圖 1：伺服主機弱點掃描檢測作業流程圖

(二) 資訊設備組態基準檢測作業：本項作業係針對資通訊終端設備之資訊安全組態基準是否達到一致性的安全設定狀態檢測。資訊設備組態基準設定值請參考政府組態基準(GCB)做為依據。組態基準檢測項目至少包含以下共通檢測項目，如下表列：

表 1：資訊設備組態基準共通檢測項目表

| 項目 | 選項 | 說明 | 方式 |
|---|---|---|---|
| 安全性選項 | 1 | 帳戶：Administrator 帳戶狀態 | 停用 |
| | 2 | 帳戶：重新命名系統管理員帳戶 | Renamed_Admin |
| | 3 | 帳戶：Guest 帳戶狀態 | 停用 |
| | 4 | 帳戶：重新命名來賓帳戶名稱 | Renamed_Guest |
| | 5 | 網路存取：允許匿名 SID/名稱轉譯 | 停用 |
| | 6 | 網路存取：不允許 SAM 帳戶和共用的匿名列舉 | 啟用 |
| | 7 | Microsoft 網路用戶端:傳送未加密的密碼到其他廠商的 SMB 伺服器 | 停用 |
| | 8 | 關閉自動播放 | 啟用<br>所有磁碟機 |
| | 9 | AutoRun 的預設行為 | 啟用/不執行任何 Autorun 命令 |
| 帳戶原則 | 10 | 重設帳戶鎖定計數器的時間 | 15 分鍾 |
| | 11 | 帳戶鎖定期間 | 15 分鍾 |
| | 12 | 帳戶鎖定閥值 | 5 次不正確的登入嘗試 |
| 密碼原則 | 13 | 最小密碼長度 | 8 個字元以上 |
| | 14 | 密碼最長使用期限 | 90 天以下 |
| | 15 | 密碼最短使用期限 | 1 天 |
| 密碼原則 | 16 | 強制執行密碼歷程記錄 | 3 次以上 |
| | 17 | 使用可還原的加密來存放密碼 | 停用 |
| | 18 | 密碼必須符合複雜性需求 | 啟用 |
| 螢幕保護 | 19 | 啟用螢幕保護裝置 | 啟用 |
| | 20 | 螢幕保護裝置逾時 | 啟用，900 秒 |
| | 21 | 以密碼保護螢幕保護裝置 | 啟用 |

| 項目 | 選項 | 說明 | 方式 |
|---|---|---|---|
| | 22 | 記錄檔大小上限(KB)(安全性) | 啟用，81920(KB) |
| | 23 | 記錄檔大小上限(KB)(安裝程式) | 啟用，32768(KB) |
| | 24 | 記錄檔大小上限(KB)(系統) | 啟用，32768(KB) |
| 互動式登入 | 25 | 互動式登入：在密碼到期前提示使用者變更密碼 | 14 天 |
| | 26 | 互動式登入：不要求按 CTRL+ALT+DEL 鍵 | 停用 |
| | 27 | 互動式登入：不要顯示上次登入的使用者名稱 | 啟用 |
| 附件管理員 | 28 | 開啟附件時通知防毒程式 | 啟用 |
| | 29 | 隱藏移除區域資訊的機制 | 啟用 |
| | 30 | 不要保留檔案附件的區域資訊 | 停用 |

資料來源：行政院國家資通安全會報技術服務中心，政府組態基準(GCB) Windows 設定對照表 V1.7 (2020/7/20)，網址如下：https://www.nccst.nat.gov.tw/GCBDownloadDetail?lang=zh&seq=1078

(三) 網路封包側錄分析作業：本項作業係透過網路封包監聽，了解組織網路是否有異常連線狀態。檢測作業分為「網路封包側錄分析」及「網路設備記錄檔分析」。

1. 網路封包側錄分析：以電腦設備至受測企業網路適當位置架設側錄點(如：側錄核心交換器流量封包)，監聽軟體採用如：Tcpdump、Wireshark 等工具，進行至少 7 天之網路封包監聽並分析，分析重點在於有無異常連線、是否連線已知惡意 IP，協助受測產業發現異常連線。
2. 網路設備記錄檔分析：將針對防火牆、入侵偵測防護系統等網路設備紀錄檔，分析過濾異常連線紀錄。網路設備紀錄檔分析以 1 個月

內的紀錄為原則，依據分析與檢測結果進行彙整與研究，撰寫於報告書。

(四) 惡意活動程式/檔案檢視：

1. 使用者端電腦檢視：使用者端電腦惡意程式或檔案檢視。
2. 伺服器主機檢視：伺服器主機惡意程式或檔案檢視。
3. 安全性設定檢視：網通設備組態設定檢視及設備記錄檔分析、應用程式伺服器主機組態設定檢視、目錄伺服器(如 MS AD)組態設定檢視。

(五) 防火牆檢視：檢視受測企業的防火牆連線設定規則，依據檢視結果分析企業網路之安全性弱點，確認來源/目的 IP 與通訊埠連通的適當性，並撰寫該受測企業「資訊安全技術檢測_防火牆規則檢視分項報告」。

十、受測企業配合項目

(一) 受測企業申請檢測診斷服務時，請詳細填寫附件一、「資訊安全檢測診斷服務」申請暨切結書，以便檢測團隊了解受測環境，及早準備，並避免影響受測企業正常營運。

(二) 受測企業應提供聯絡專人，協助聯繫安排各項訪談、會議時間，及檢測作業時間、場地及設備。

(三) 受測企業應配合檢測團隊執行改善建議，並於伺服主機弱點掃描檢測作業初檢發現企業網路潛在的安全威脅後，儘速進行弱點排除，以進行複測。

十一、 受測項目總表說明

| 項次 | 檢測項目 | 說明 |
|---|---|---|
| 1 | 資訊安全風險現況評估作業 | 本項作業係由資安專業人員實地訪談後產出「資訊安全風險現況評估報告」，做為資訊安全技術檢測之參考資料；C、D 類受測企業之資安風險現況評估報告將增加網路架構檢視。 |
| 2 | 伺服主機弱點掃描檢測作業 | 針對伺服主機或電腦系統進行安全弱點掃描，藉由所發現的系統漏洞，找出受測企業網路潛在的安全威脅並提出改善建議後提供複掃，以確認弱點是否排除，降低遭受入侵的風險。 |
| 3 | 資訊設備組態基準檢測作業 | 規範資通訊終端設備(如個人電腦)的一致性安全設定(如密碼長度、更新期限等)，以降低成為駭客入侵管道之風險。 |
| 4 | 網路封包側錄分析作業 | 觀察資訊環境是否有異常連線或 DNS 查詢，並比對是否連線已知惡意 IP、中繼站(Command and Control，C&C)，找出建立惡意連線的受駭主機，進而加以監控與防護，並提供強化改善建議。 |
| *5 | 惡意活動/程式檔案檢視 | 1. 有線網路惡意程式或檔案檢視：針對個人電腦進行是否存在惡意程式或檔案檢視，檢視項目包含活動中與潛藏惡意程式、駭客工具程式及異常帳號與群組，藉此分析後了解可能的風險。 |

| 項次 | 檢測項目 | 說明 |
| --- | --- | --- |
| | | 2. 伺服主機是否存在惡意程式或檔案進行檢視，檢視項目包含活動中與潛藏惡意程式、駭客工具程式及異常帳號與群組；伺服器更新檢視，檢視範圍包含作業系統、Office 應用程式、防毒軟體、Adobe Acrobat 及 Adobe Flash Player、資料庫(MS SQL)降低遭受入侵的風險。<br>3. 對個人電腦進行是否存在惡意程式或檔案檢視，檢視項目包含活動中與潛藏惡意程式、駭客工具程式及異常帳號與群組。 |
| *6 | 防火牆檢視 | 檢視防火牆連線設定規則是否有安全性弱點，以及確認來源與目的 IP 與通訊埠連通的適當性，是否有安全性弱點。 |
| 7 | 檢測結果分析與建議 | 整合資訊安全風險現況評估、伺服主機弱點檢測、資訊設備組態基準檢測與網路封包側錄分析檢測結果，提供受測企業「總體資安風險評估報告」。 |

*註：其中 5、6 項為 C、D 類之檢測項目。

十二、 聯絡方式

本案聯絡人甘世裕(Kevin)資深專員 kevin@cisanet.org.tw，聯絡電話(02) 2553-3988 分機 371 或 375。