經濟部工業局108年「新興資安產業生態系推動計畫」
資訊安全檢測診斷服務申請須知

一、目的

經濟部工業局為協助產業資安防護能力提升，於108年「新興資安產業生態系推動計畫」，推動產業資訊安全檢測診斷服務，透過「資訊安全風險現況評估」，實施「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」檢測作業，以利受測企業掌握該組織之資安防護現況，並了解如何強化、改善及建立預防措施。

二、申請資格

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，並屬資通訊製造、雲端物聯網、金融服務、中小企業、智慧應用等營運項目者。

三、申請費用

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類企業(101 IP以上~200 IP以內)，每案費用新台幣16萬元(政府補助11萬元、受測企業自負款5萬元)。

(二)B類企業(20 IP以上~100 IP以內)，每案費用新台幣9萬元(政府補助7萬元、受測企業自負款2萬元)。

(三)繳費方式，請匯款至以下帳戶，匯款後請將收據掃描 email 至 betty.hsu@mail.cisanet.org.tw 或傳真至 (02)2553-1319 徐佩君小姐

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

匯款手續費用: 由受測企業支付。

四、申請方式

請檢附下列資料，email/傳真並將正本寄送至 103 台北市大同區承德路二段 239 號 6 樓中華民國資訊軟體協會收。請於信封上註明「申請資訊安全檢測診斷服務」字樣。

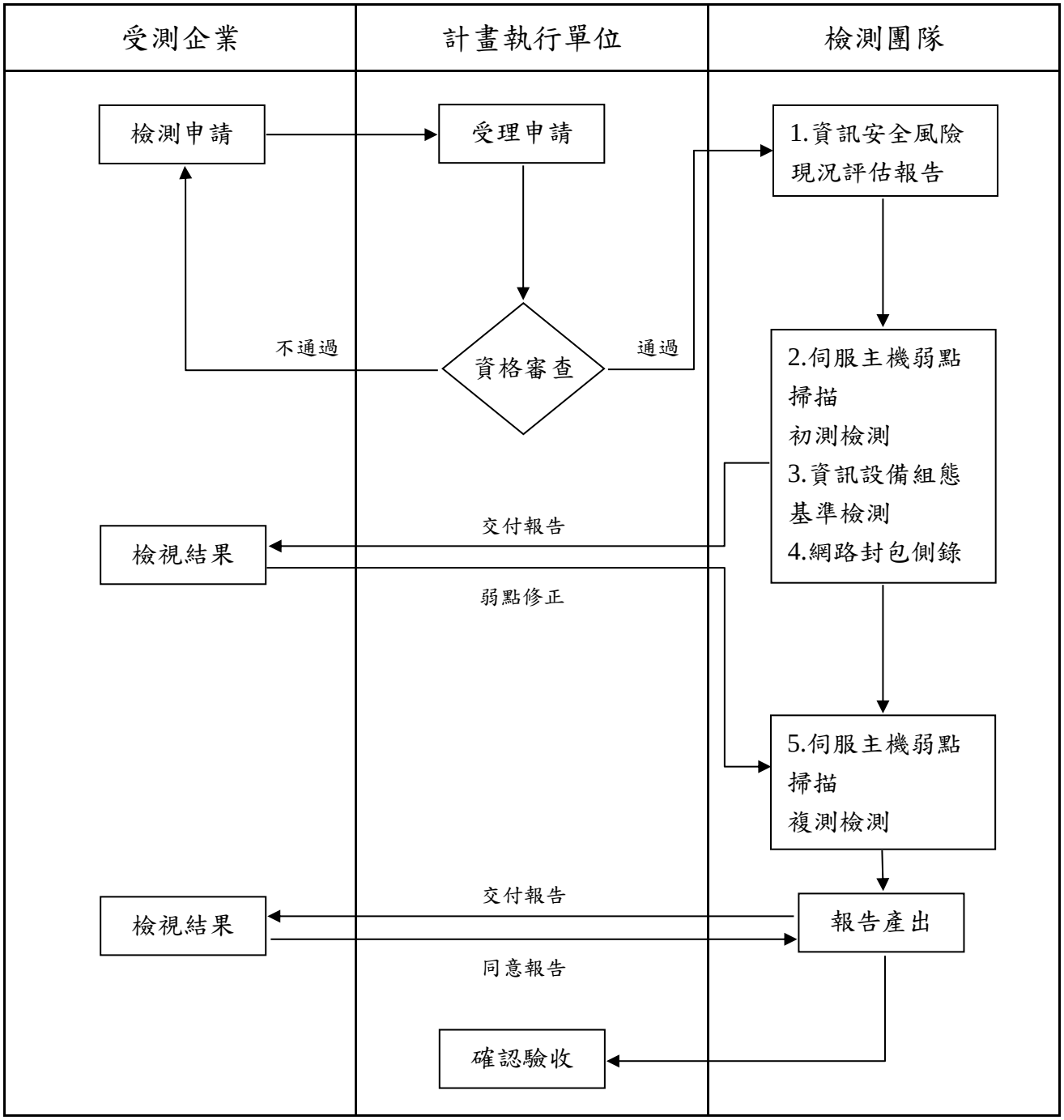
(一)資訊安全檢測診斷服務申請暨切結書（格式如附件一）。

(二)資訊安全檢測診斷服務自籌款繳費證明。

五、檢測診斷服務團隊派案原則：

本服務將受理 60 家符合資格之企業申請，包含 20 家 A 類企業、40 家 B 類企業，依申請先後順序額滿為止，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。檢測診斷服務團隊與受測企業須簽密切結書，以利專案進行。

六、資安檢測診斷服務申請及執行流程



七、資訊安全風險現況評估作業

(一)參採資訊安全管理標準 ISO 27002 研擬「訪談分析紀錄表」，檢測團隊進行訪談後應產出「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。

(二)「資訊安全風險現況評估報告」應與伺服主機弱點檢測、資訊設備組態基準檢測與網路封包側錄分析檢測結果整合，提供受測產業「總體

資安風險評估報告」

八、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)發布的弱點內容(最新版) ，檢測結果需參採CVE評分系統CVSS (Common Vulnerability Scoring System)進行嚴重(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：

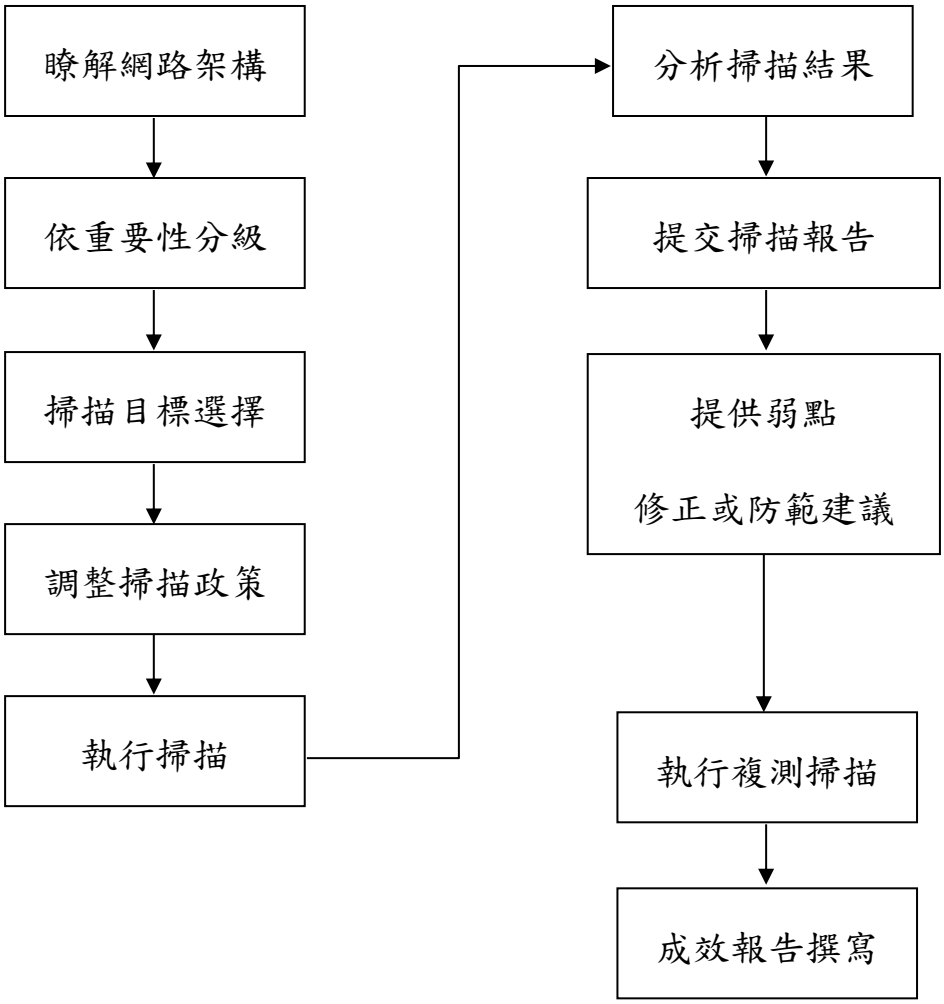


圖1　伺服主機弱點掃描檢測作業流程圖

(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 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

項目	選項	說明	方式
	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
	9	AutoRun 的預設行為	啟用
帳戶原則	10	重設帳戶鎖定計數器的時間	15 分鐘
	11	帳戶鎖定期間	15 分鐘
	12	帳戶鎖定閥值	5
密碼原則	13	最小密碼長度	8 碼以上
	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	900 秒
	21	以密碼保護螢幕保護裝置	啟用
	22	記錄檔大小上限(KB)(安全性)	81920
	23	記錄檔大小上限(KB)(安裝)	81920
	24	記錄檔大小上限(KB)(系統)	32768
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

- 資料來源參考依據:行政院國家資通安全會報技術中心，政府組態基準 GCB_Windows 設定對照表_V1.3(2018/1/30)

https://www.nccst.nat.gov.tw/GCBDownloadDetail?lang=zh&seq=1043

(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：以電腦設備至組織網路適當位置架設側錄點(如:側錄核心交換器流量封包) 進行監聽，監聽軟體採用如: Tcpdump、Wireshark 等工具，進行至少 7 天之網路封包監聽藉以分析，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匯整與研究，撰寫於報告書。

九、受測企業配合項目及效益

(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。

(四)檢測效益

項次	檢測項目		效益說明
1	資訊安全風險現況評估作業		本項作業係以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。
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	使用者端電腦惡意程式或檔案檢視	個人電腦是否存在惡意程式或檔案進行檢視，檢視項目包含活動中潛藏惡意程式、駭客工具程式及異常帳號與群組，降低遭受入侵的風險。
		伺服器主機惡意程式或檔案檢視	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，降低遭受入侵的風險。
		主機更新檢視	作業系統、Office 應用程式、防毒軟體、Adobe Reader 及 Adobe flash player、Java 應用程式更新檢視，降低遭受入侵的風險。
4	網路封包側錄分析作業	封包監聽與分析	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)或有符合惡意網路行為的特徵。
		網路設備紀錄檔分析	檢視防火牆、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，降低遭受入侵的風險。
5	檢測結果分析與建議	資訊安全風險控制建議報告	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」。

十、聯絡方式

本案聯絡人徐佩君資深專員 betty.hsu@mail.cisanet.org.tw，聯絡電話：(02)2553-3988 分機 313。