數位發展部數位產業署

114 年「資安產業跨域聯防推動計畫-推動資安服務團與資安診斷服務」

資安診斷服務申請須知

一、目的

數位發展部數位產業署為促進產業資安防護能力提升，推動產業資安檢測診斷服務，透過「企業資安評級」、「主機系統弱點掃描」、「目錄伺服器或設備組態檢視」、「網路封包側錄分析」、「惡意程式或檔案檢視」及「防火牆連線設定檢視」等檢測項目，協助受測企業掌握組織內部資安防護現況，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：申請受測企業須為依我國公司法設立，經主管機關核准登記之本國公司，以數位產業(如數位內容、數位商務及數位娛樂等)或資訊服務業為重點推動產業。

三、檢測項目及費用

(一)資安檢測診斷服務由數位發展部數位產業署部分補助，受測企業自行負擔金額為新台幣 3 萬 5 千元。

(二)本年度檢測範圍 IP 數[1]及檢測項目如下：

項次	檢測範圍 IP 數	檢測作業項目	經費(新台幣)
1	21~100	1.企業資安評級 2.主機系統弱點掃描 3.目錄伺服器或設備組態檢視 4.網路封包側錄分析 5.惡意程式或檔案檢視 6.防火牆連線設定檢視	每案總價 14 萬元 說明：政府補助 10 萬 5 千元、受測企業自負 3 萬 5 千元 (本檢測市場價值超過 30 萬元)

[1] IP 數計算方式：檢測團隊每針對一臺設備(如主機)執行一項檢測作業，得視為一個 IP 數。

(三)受測企業應於申請通過後，立即將自負款匯入以下帳戶，手續費或匯費由受測企業自行負擔，未繳交費用者，計畫執行單位有權拒絕受理；匯款後請將繳費證明掃描或截圖 email 至 security@cisanet.org.tw

- 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

四、申請方式

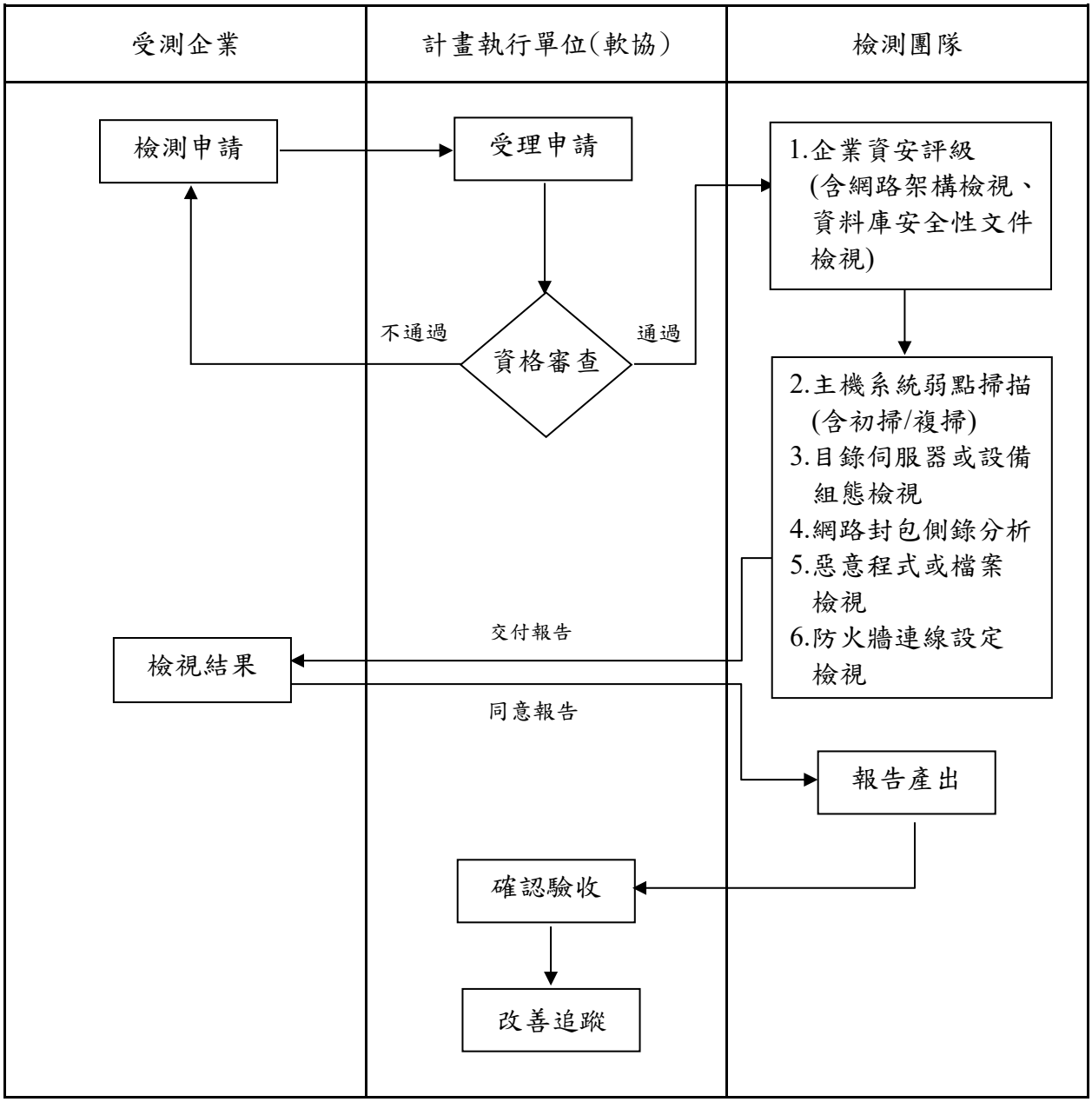
填寫「資安檢測診斷服務申請暨切結書」(如附件一)，並完成公司大小章用印後，將正本郵寄至 104427 臺北市中山區中山北路 3 段 22-1 號新設工大樓 5 樓 C 區、中華民國資訊軟體協會(大同辦公室)資安服務處，註明「申請資安檢測診斷服務」。

五、資安檢測診斷服務團隊派案原則：

(一)本年度將受理 20 家符合資格之企業申請，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。

(二)檢測團隊將與受測企業簽訂保密切結書，以利本計畫執行。

六、資安檢測診斷服務申請及執行流程



七、企業資安評級評估作業

(一)檢測團隊將訪談受測企業並協助填寫資安整合服務平台(SECPAAS)資安評級問卷，並提供改善建議及相關做法。

(二)檢測團隊將依據受測企業填寫之「資料庫安全性檢視表」(如附件二，以核心業務資料庫為主)，提供「企業資安評級評估報告」(含網路架構檢視、資料庫安全性文件檢視)。

八、資訊安全技術檢測作業

(一)主機系統弱點掃描：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的設定、帳號密碼設定及管理方式等進行弱點掃描，至少包含以下掃描項目且須符合 Common Vulnerabilities and Exposures (CVE)發布的弱點內容(最新版)：

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掃描
7. 網路通訊埠掃描

本項作業包含初掃及複掃，得各別計算 IP 數，執行方式如下：

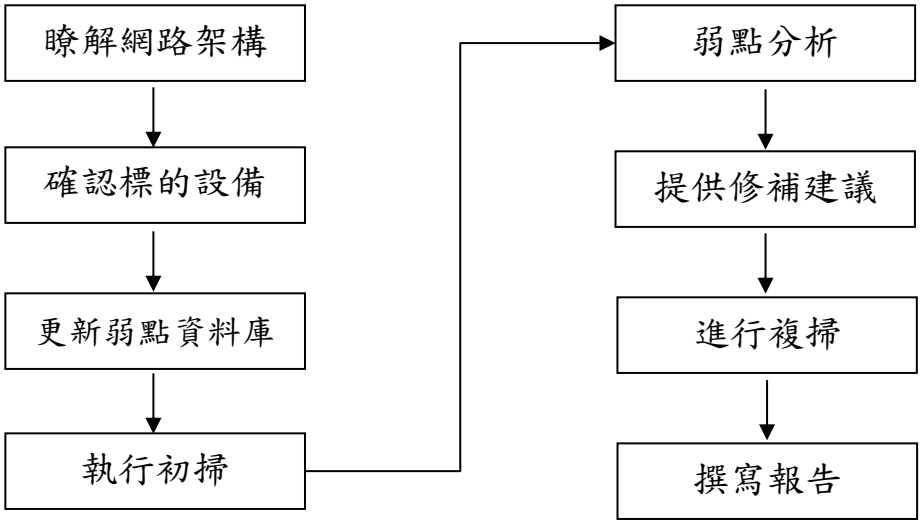


圖1 ：主機系統弱點掃描作業流程圖

(二)目錄伺服器或設備組態檢視：參考國家資通安全研究院，官方網站「政府組態基準」專區所公布安全性檢視內容，確認受測企業目錄伺服器或設備組態

設定情形，並至少完成下列組態檢視項目。

表 1：組態檢視項目表

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
帳戶原則	8	重設帳戶鎖定計數器的時間間隔	15 分鐘以上
	9	帳戶鎖定期間	15 分鐘以上
	10	帳戶鎖定閾值	5 次以下不正確的登入嘗試，但須大於 0 次
密碼原則	11	最小密碼長度	8 個字元以上
	12	密碼最長使用期限	90 天以下，但須大於 0 天
	13	密碼最短使用期限	1 天
	14	強制執行密碼歷程記錄	3 個以上記憶的密碼
	15	使用可還原的加密來存放密碼	停用
	16	密碼必須符合複雜性需求	啟用
螢幕保護	17	啟用螢幕保護裝置	啟用
	18	螢幕保護裝置逾時	啟用，900 秒以下，但須大於 0 秒
	19	以密碼保護螢幕保護裝置	啟用
互動式	20	在密碼到期前提示使用者變更密碼	14 天以上

項目	選項	說明	方式
登入	21	不要求按 CTRL+ALT+DEL 鍵	停用
	22	不要顯示上次登入	啟用
附件管理員	23	開啟附件時通知防毒程式	啟用
	24	隱藏移除區域資訊的機制	啟用
	25	不要保留檔案附件的區域資訊	停用
Windows 元件	26	關閉自動播放	啟用，所有磁碟機
	27	設定 AutoRun 的預設行為	啟用，不執行任何 AutoRun 命令
	28	指定記錄檔大小上限(KB)(安全性)	啟用，81,920KB 以上
	29	指定記錄檔大小上限(KB)(安裝)	啟用，32,768KB 以上
	30	指定記錄檔大小上限(KB)(系統)	啟用，32,768KB 以上

資料來源：國家資通安全研究院「政府組態基準」專區，參考網址 https://www.nics.nat.gov.tw/core_business/cybersecurity_defense/GCB

(三)網路封包側錄分析：

1. 網路封包側錄分析：在受測企業有線網路(內網、外網、DMZ 區或 N 個網段)適當位置架設側錄設備，進行封包側錄至少以 6 小時為原則並以 3 台電腦為限，觀察內部電腦或設備是否有對外之異常連線或 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。發現異常連線之電腦或設備需確認使用狀況與用途。
2. 網路設備紀錄檔分析：檢視網路與資安設備(如防火牆、入侵偵測/防護系統等)紀錄檔，分析過濾內部電腦或設備是否有對外之異常連線紀錄，發現異常連線之電腦或設備需確認使用狀況與用途。

(四)惡意程式或檔案檢視：

1. 使用者端電腦檢視：

(1) 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。

(2) 針對使用者電腦進行作業系統更新檢視；使用者電腦安裝之應用程式安全性更新，包含 Office 應用程式、Adobe Acrobat、及 Java 應用程式更新檢視；檢視使用者電腦是否使用已經停止支援之作業系統或軟體(如 Windows XP、Windows Vista、Windows 7、Windows 8、Office 2003、Office 2007、Office 2010、Office 2013、Adobe Flash Player 等，依使用作業系統或軟體之官網公告資訊為主)；針對使用者電腦防毒軟體安裝、更新及定期全系統掃描狀況進行檢視。

2. 伺服器主機檢視：

(1) 針對伺服器主機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。

(2) 針對伺服器主機進行作業系統更新檢視；檢視伺服器主機安裝之應用程式安全性更新，包含 Office 應用程式、Adobe Acrobat、及 Java 應用程式更新；檢視伺服器是否使用已經停止支援之作業系統或軟體(如如 Windows XP、Windows Vista、Windows 7、Windows 8、Office 2003、Office 2007、Office 2010、Office 2013、Adobe Flash Player 等，依使用作業系統或軟體之官網公告資訊為主)；檢視伺服器是否使用不合宜之作業系統(如使用 Windows 10 等)；針對伺服器主機防毒軟體安裝、更新及定期全系統掃描狀況進行檢視。

(五)防火牆連線設定檢視：檢視受測企業防火牆(設備數量以 2 臺以內為原則)的連線設定規則(如外網對內網、內網對外網、內網對內網)是否有安全性弱點，確認來源與目的 IP 與通訊埠連通的適當性(包含設置「Permit All/Any」與「Deny All/Any」等 2 項防火牆檢測規則確認)。

九、受測企業配合事項

(一)受測企業應確實填寫「資安檢測診斷服務申請暨切結書」(如附件一)，以便

檢測團隊了解受測環境，及早準備，並避免影響正常營運。

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

(三) 受測企業應配合執行改善建議，並於主機系統弱點初掃發現企業網路潛在的安全威脅後，儘速進行弱點修補，以進行複掃，初掃與複掃間隔期間不得超過三個月為限。

十、聯絡資訊

計畫執行單位聯絡方式，電話：02-2553-3988 轉分機 812，

電子信箱：security@cisanet.org.tw。

附件一

資安檢測診斷服務申請暨切結書

<table>
<tr><th colspan="6">公 司 基 本 資 訊</th></tr>
<tr><td>公司中文全名</td><td colspan="2"></td><td>負 責 人</td><td colspan="2"></td></tr>
<tr><td>核准設立日期</td><td colspan="2">民國　　年　　月　　日</td><td>統一編號</td><td colspan="2"></td></tr>
<tr><td>公 司 資 本 額</td><td colspan="5"></td></tr>
<tr><td>公司聯絡地址</td><td colspan="5"></td></tr>
<tr><td rowspan="4">公 司 聯 絡 人</td><td>姓名</td><td colspan="2"></td><td>職稱</td><td></td></tr>
<tr><td>電話</td><td colspan="4"></td></tr>
<tr><td>行動電話</td><td colspan="4"></td></tr>
<tr><td>E-mail</td><td colspan="4"></td></tr>
<tr><td rowspan="2">公 司 規 模</td><td>總員工數</td><td colspan="4"></td></tr>
<tr><td>資訊部門
(人數)</td><td colspan="4">☐ 資訊部門人數：　　人
☐ 委外管理
☐ 無專責資訊部門</td></tr>
<tr><td colspan="6">本公司已詳細閱讀過申請暨切結書內容及作業配合事項，並同意遵守。

公司印章：＿＿＿＿＿＿＿＿　負責人印章：＿＿＿＿＿＿＿＿

中 華 民 國　　年　　月　　日</td></tr>
</table>

網 路 基 本 資 訊	
資訊環境調查	1. 防火牆廠牌及型號： 2. 入侵防禦系統廠牌及型號： 3. 防毒系統廠牌及型號： 4. 網路交換器廠牌及型號： 支援Port Mirror功能 □是 □否 5. 檢測標的網路環境具備Windows AD □是 □否 AD伺服器作業系統及版本：
作業配合事項	1. 企業資安評級：請提供網路架構圖、資安管理文件等，並填寫「資料庫安全性檢視表」，並安排相關人員接受訪談。 2. 主機系統弱點掃描：請提供掃描服務範圍設備清單或相關資訊。 3. 目錄伺服器或設備組態檢視及惡意程式/檔案檢視： (1)請提供檢測服務範圍設備清單。 (2)執行「使用者端電腦檢視」及「伺服器主機檢視」須以高權限角色(Admin / Power User)才能獲取精確檢測數據，如對AD權限有特別管制，請協助暫時開放。 (3)同上，或設定一組測試帳號並賦予Admin或Power User權限，待作業完成再行復原。 4.網路封包側錄分析：因應網路封包側錄需求，請協助針對內、外網段及DMZ區設定流量Mirror，以利封包分析作業。 5.為達成有效檢測之目的，申請檢測建議最低設備需求如下： (1)使用者端電腦及伺服器主機合計20臺(含)以上。 (2)防火牆1臺。 (3)Switch或Core Switch 1台，並具備Port Mirror功能，請安排工程師或廠商協助配合設定。 (4)受測設備須具備log匯出功能，並有工程師或廠商協助配合設定。

檢 測 服 務 申 請 資 訊	
檢 測 團 隊	請安排_____執行本公司申請之資安檢測診斷服務；若檢測團隊檢測數量已額滿，由計畫執行單位指派檢測團隊。
進階檢測服務	本公司有興趣與檢測團隊商議加購「進階檢測服務」，請提供相關資訊： □資料庫安全檢視(實機檢測) □其他：_____ □暫時不需要

註：本計畫遴選通過之檢測團隊名單，以計畫執行單位(軟協)網站公告為主。

附件二

資料庫安全性檢視表

資料庫基本資訊		
1.1 資料庫名稱(類型)		
1.2 資料庫版本		
1.3 官方預設帳戶		
資料庫帳戶管理		
2.1 啟用帳戶鎖定次數	□是，於錯誤____次後鎖定	□否 (請跳至2.3)
2.2 啟用帳戶鎖定時間	□是，將鎖定____分鐘	□否
2.3 啟用「通行碼複雜度」原則 (可複選)	□英文 □數字 □大小寫 □特殊符號	□否
2.4 啟用「最小通行碼長度」原則	□是，長度至少____字元	□否
2.5 啟用「資料庫管理帳戶的通行碼最長有效期限」原則	□是，最長有效期為____日	□否
2.6 是否停用或變更官方預設帳戶	□是	□否
資料庫資料保護機制		
3.1 是否具備資料保護機制 (可複選)	□使用資料庫加密 □資料表欄位內容加密 □資料表欄位內容遮罩 □其他，請補充說明：	□否
3.2 是否採用第三方加解密工具	□是，工具名稱：	□否
資料庫備份管理機制		
4.1 資料庫備份週期	□每天 □每週 □每月 □其他：	□否

4.2 資料庫備份執行方式 (可複選)	□完整備份 □差異備份 □增量備份 □其他：	□否
4.3 資料庫備份儲存方式 (可複選)	□本地備份 □異地備份 □其他：	□否
4.4 資料庫備份保護方式	□備份檔案加密 □硬體加密 □實體保護(如儲存資料櫃上鎖) □其他：	□否
4.5 資料庫備份回復測試	‧ 測試頻率： □每季 □每半年 □每年 □其他： ‧ 最近一次執行日期： 年 月 日	□否
資料庫弱點管理機制		
5.1 執行資料庫主機弱點掃描	‧ 弱點掃描執行頻率： □每週 □每月 □每季 □其他： ‧ 最近一次掃描日期： 年 月 日 ‧ 掃描工具：	□否
5.2 定期修補資料庫主機弱點	‧ 弱點修補頻率： □每月 □每季 □每半年 □其他： ‧弱點修補門檻： □僅修補高風險弱點 □修補中風險以上弱點 □修補低風險以上弱點	□否

5.3 定期修補資料庫主機安全性更新項目	▪ 更新方式： □集中管控、派送(如中控台) □管理者手動更新 □其他： ▪ 更新頻率： □每月 □每兩週 □每週 □每天 □其他： ▪ 最近更新日期： 年 月 日	□否
資料庫存取與授權		
6.1 限制資料庫主機服務埠	□是，僅開啟下列服務埠：	□否
6.2 限制遠端存取的IP來源	□是，僅允許下列來源IP可存取資料庫：	□否
6.3 限制遠端存取的帳戶	□是，僅允許下列帳戶可遠端存取資料庫：	□否
6.4 禁止管理者帳戶透過遠端存取	□是，限制管理者帳戶直接透過遠端連線進行操作	□否
6.5 資料庫帳戶權限最小化原則	□是，依照職務區隔限制資料庫帳戶所需權限	□否
6.6 資料庫連線傳輸安全機制	□是，連線傳輸安全機制如下：	□否
資料庫稽核與紀錄		
7.1 啟用資料庫帳戶變更稽核	□是，針對資料庫的帳戶變動(新增、刪除、修改)，留存相關紀錄	□否
7.2 啟用資料庫存取稽核	□是，針對資料庫的帳戶登出/登入行為，留存相關紀錄	□否
7.3 啟用資料庫結構變更稽核	□是，針對資料庫結構新增、刪除、修改等行為，留存相關紀錄	□否
7.4 建立稽核紀錄備份週期	□每週 □每月 □每季 □其他：	□否

7.5 稽核紀錄備份儲存方式	□本機備份 □異地備份 □其他：	□否
7.6 設定資料庫主機校時	□是，校時主機IP如下：	□否
7.7 定期分析稽核紀錄	‧ 分析稽核紀錄執行頻率： □每週 □每月 □每季 □其他： ‧ 最近一次分析日期： 年 月 日 ‧ 分析工具：	□否

資料來源：國家資通安全研究院，資料庫技術檢測執行方法