經濟部工業局 107 年「新興資安產業生態系推動計畫」
資訊安全檢測診斷服務團隊遴選須知

一、目的

經濟部工業局為協助產業資安防護能力提升，於 107 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，以利受測企業掌握組織之資安防護狀況，並了解如何強化、改善及建立預防措施。

為遴選國內優秀資安業者協助提供資安檢測診斷服務，特訂定此遴選須知，邀請具備資格及服務能量之業者參加。

二、申請日期：依正式公告文件為準。

三、檢測期間：自受測企業申請通過並派案執行起，至 107 年 10 月 31 日前完成報告交付。

四、檢測服務團隊申請資格

(一)依我國公司法設立，中央主管機關經濟部核准登記之本國公司，請附團隊所有成員證明影本一份。

(二)每一檢測團隊之組成至少包含 2 家(含)以上公司，檢測團隊成員應包含專案主持人、專案經理、資安風險現況評估人員及資安檢測診斷服務人員等，檢測團隊及服務人員應具備下列資格條件，以確保服務水準。具備技能說明如下：請填具附件一申請表並附證明文件一份。

1. 檢測團隊須提供近 3 年內執行本案所訂四類資安檢測作業達 5 案(含)以上實績，四類至少各 1 件(含)以上。

2. 資訊安全風險現況評估人員，需具備 CNS/ISO 27001 主導稽核員

或課程完訓證明。

3. 資訊安全技術檢測作業人員，須具備以下資安相關證照或相關課程訓練證明至少 2 式，並註明證明文件之有效期間：

(1)證照：CISSP(Certified Information Systems Security Professional)、GIAC 、 CompTIA Security 、 SSCP(Systems Security Certified Practitioner)、CEH (Council Ethical Hacking)、OSCP(Offensive Security Certified Professional) 、 ECSA(EC-Council Certified Security Analyst)等相關資安證照。

(2)課程訓練：接受過 CISSP(Certified Information Systems Security Professional)、CEH (Council Ethical Hacking)、GIAC、CompTIA Security 等相關資安課程訓練。

(三)團隊各成員需與主提案廠商簽署合作協議書一份。

五、檢測服務團隊遴選數量及派案原則

(一)本計畫原則預計遴選 4 個團隊,團隊成員需承諾於年底結案前通過檢測項目之資安服務機構能量登錄。

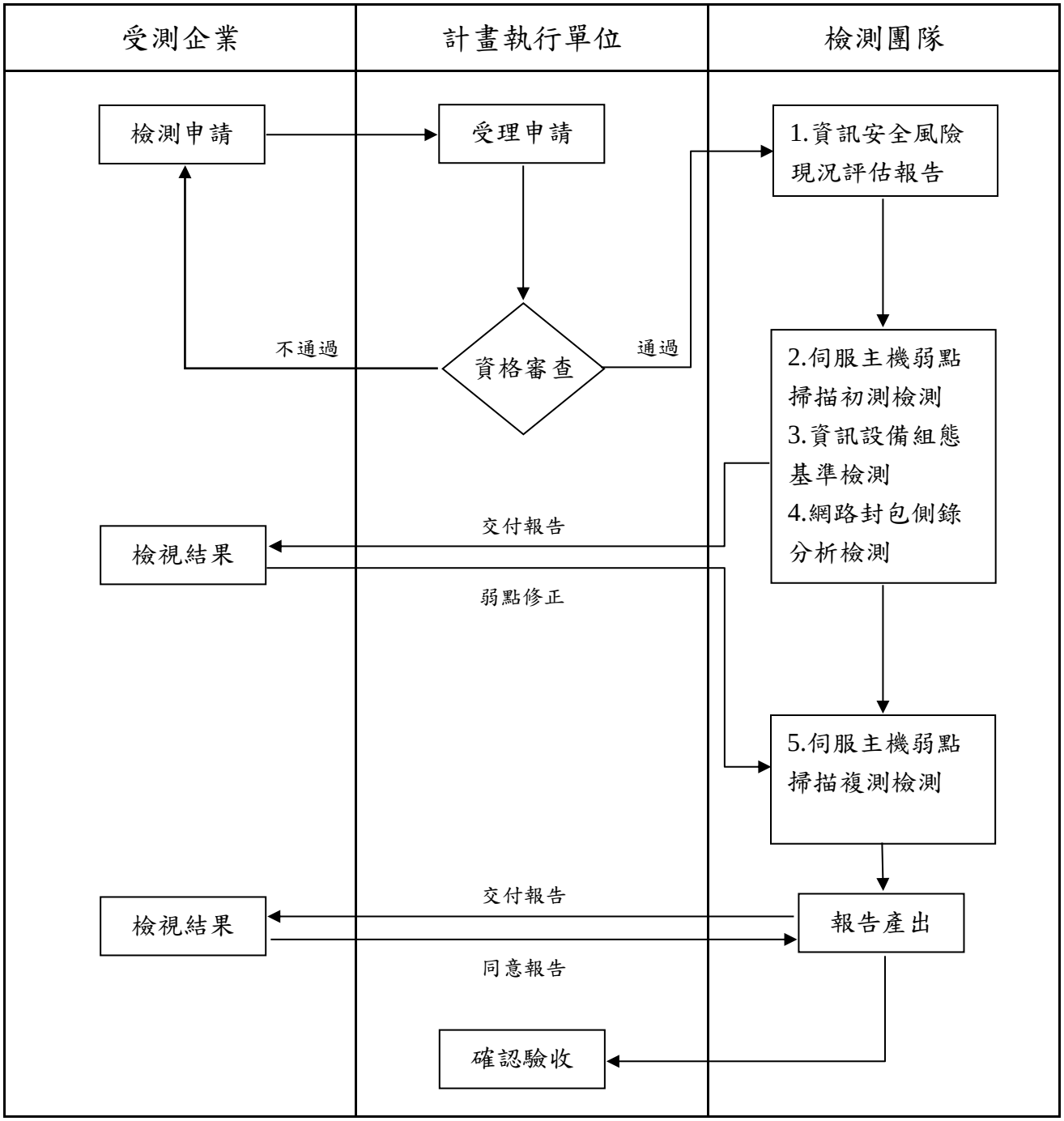
(二)每一團隊執行量：

1. 4 件 A 類企業(101 IP 以上~200 IP 以內)，每案 14 萬元(政府補助 10 萬、受測企業自籌款 4 萬)。

2. 6 件 B 類企業(20 IP 以上~100 IP 以內)，每案 9 萬元(政府補助 8 萬、受測企業自籌款 1 萬)。

(三)派案原則：由受測企業提出申請，可指定檢測團隊，未指定或團隊檢測數量已額滿，由計畫執行單位依序派案。

六、資安檢測診斷服務申請及執行流程：



七、資安檢測執行規範

參與資安檢測診斷團隊必須簽訂專案合約及保密切結書，藉此保障雙方之權益，檢測團隊成員皆需遵循，內容如下：

(一)與計畫執行單位:檢測團隊主提案單位需與計畫執行單位簽訂合約及保密切結書。

(二)與受測企業：檢測團隊須向受測企業簽訂保密切結書，保證檢測過程中所取得之資料，絕不會以任何方式透露給任何第三方。

八、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「資訊安全風險控制建議報告」。

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：

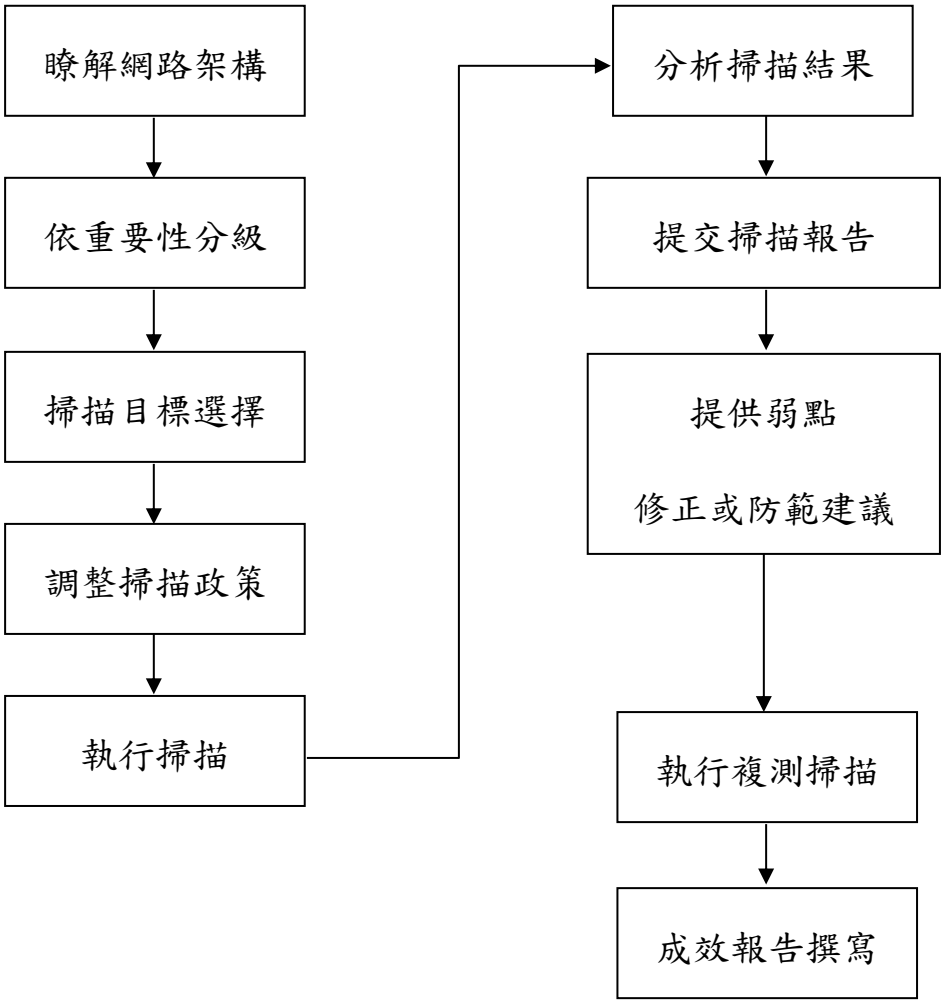


圖1　伺服主機弱點掃描檢測作業流程圖

(二)資訊設備組態基準檢測作業：本項作業係透過合法授權之商用軟硬體，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
	1	帳戶：Administrator 帳戶狀態	停用

項目	選項	說明	方式
安全性選項	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
	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 分鍾
	11	帳戶鎖定期間	15 分鍾
	12	帳戶鎖定閾值	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	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

項目	選項	說明	方式
員	30	不要保留檔案附件的區域資訊	停用

(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) 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。

十、檢測團隊應配合作業規定事項

(一)檢測團隊於需求訪談階段，需先就受測企業之網路架構及標的設備進行了解，如設備廠牌、系統版本等，以利後續進行弱點或漏洞分析及修補建議。

(二)檢測團隊應與受測企業協調取得適當時間進行檢測作業，並依排定之日期執行資安檢測。

(三)檢測期間若可能影響系統運作時，需提前通知本計畫執行單位及受測企業專案聯絡人，以因應緊急突發狀況。

(四)檢測期間若檢測團隊發現重大安全弱點或漏洞，應立即告知受測企業。

(五)執行資安檢測期間，檢測團隊若發現網路線上有駭客入侵行為或跡象

時，應立即告知受測企業。

(六)專案合約終止時,檢測團隊應將有關資安檢測過程中處理之任何形式資訊，整理歸檔後交還受測企業，並留存交還紀錄以供備查。

(七)檢測工具應為取得合法授權之商用軟體，並應於每次檢測作業前，將工具之弱點資料庫更新至最新版本，並提供佐證資料，以確保本項服務之正確性。

(八)資安檢測作業執行前，須提出受測目標備份建議，避免發生非預期資料損毀或遺失等情形。作業執行期間，若需執行具侵入性質的檢測作業，需與受測企業進行確認，並於雙方議定之適當時間且具備應變措施與風險評估後，方能進行檢測作業。

(九)資安檢測作業執行期間,應避免執行具破壞系統可用性與完整性的檢測作業，如刪除、更改資料及更動原系統設定等行為。如為新增資料行為，該資料應明顯可識別為本次測試所產生，並通知受測系統相關人員。

(十)因執行資安檢測作業造成軟硬體設備服務中斷時,檢測團隊應立即停止測試工作,協助受測企業恢復正常運作,並調整測試之方法與策略,以確保系統無受影響，並經受測企業同意後繼續進行。

(十一) 本計畫檢測團隊應接受執行單位實地稽核，確保檢測團隊於服務期間與合約終止時之資料安全、設備管理及其他安全維護事項已採取必要措施。

(十二) 檢測團隊應協助受測企業解讀報告及建議後續處理方式。

十一、履約期間內檢測團隊應配合事項

(一)檢測團隊須於遴選通過當月起,每月 20 日前(如遇假日則順延一個工作日)提出當月之書面工作報告，送交審核或備查。

(二)檢測團隊須配合參加工作會議，提供進度報告。

(三)本案服務內容涉及敏感資訊,檢測團隊不得轉包或分包予其他業者執

行。

十二、驗收項目

每完成一案(受測企業)需交付以下報告：

(一)與受測企業簽訂之保密切結書。

(二)啟動會議簡報及會議紀錄。

(三)資訊安全風險現況評估報告(包含訪談分析紀錄表)。

(四)資訊設備組態基準檢測報告。

(五)伺服主機弱點掃描檢測初、複測各一份報告。

(六)網路封包側錄分析報告。

(七)將所有檢測報告，彙整一份「總體資安風險評估」報告。

(八)結案會議簡報及會議紀錄

十三、申請時應檢具之文件

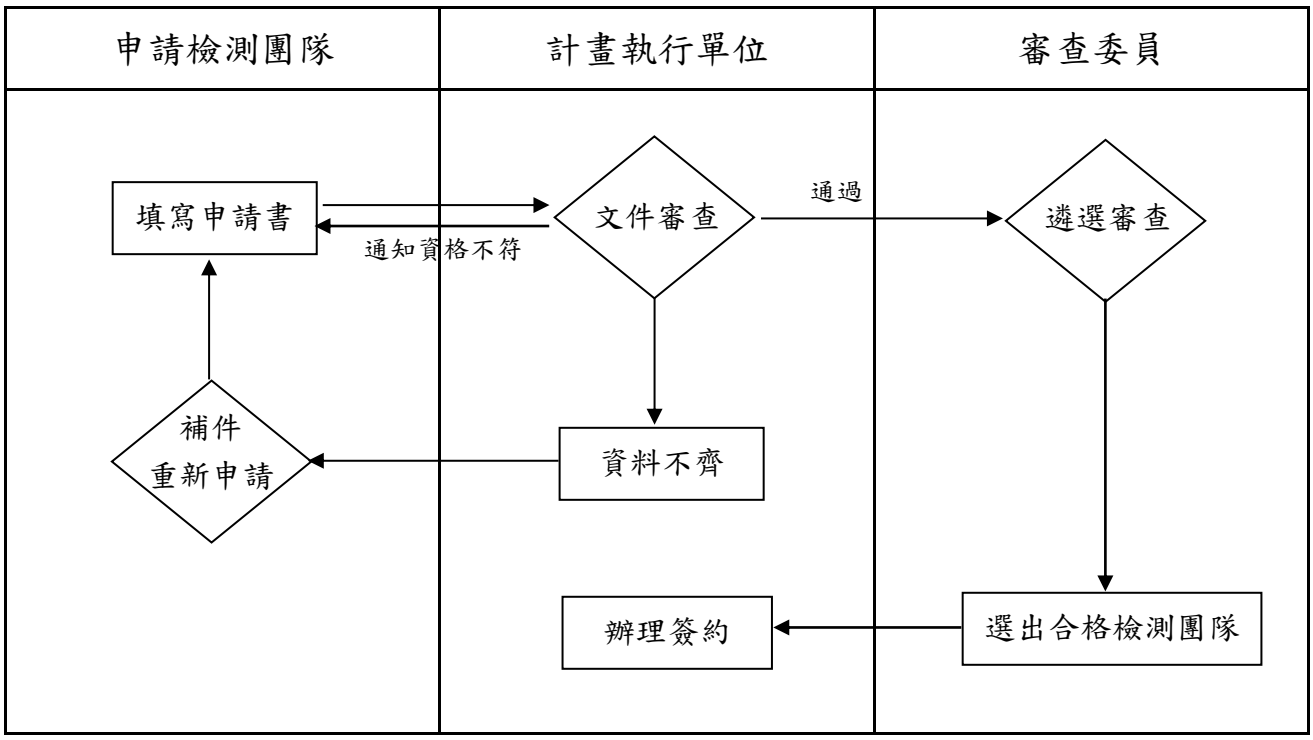
檢附「資訊安全檢測診斷服務團隊」申請書，請參見附件一。

十四、申請方式

須完整填寫「資訊安全檢測診斷服務團隊申請書」及完成公司大小章用印後，將正本於期限內郵寄至台北市承德路二段 239 號 6 樓-中華民國資訊軟體協會，註明資訊安全檢測診斷服務團隊申請書，或先 mail 掃描電子檔，再後補文件正本，提供予本案聯絡人鄭佩君專員 livia.cheng@mail.cisanet.org.tw，聯絡電話：(02)2553-3988 分機 387。

十五、遴選審查流程及評分標準

本計畫成立遴選委員會，由審查委員依申請單位之書面資料及評分項目進行遴選，遴選審查流程詳如下圖所示，並說明如下：



(一)第 1 階段：文件資格審查

本計畫執行單位依據本遴選須知進行資格及申請書文件資料正確性審核，經審核結果若有申請資格不符者，敘明原因後做退件處理；若僅為提供之書面資料未齊備時，限期於 3 個工作日內重新申請，逾時視同資格不符。

(二)第 2 階段：召開遴選會議審查評選

針對符合遴選資格之企業，將召開遴選會議，並外聘具專業背景審查委員 3~5 名進行複審及評選。

(三)評選標準(採序位法)

審查委員依下列各評選項目及配分，予以評選。

審查委員就個別團隊各評選項目及子項分別評分後予以加總，並依加總分數高低轉換為序位，分數最高者為序位 1，餘依分數排序，依序位較低者優先，原則選出 4 個團隊，出席委員評分平均低於 70 分者，為不合格團隊。

表 2 評選項目及配分表

項次	評選項目	比例
1	檢測團隊規模與人力能量	30%
2	資安檢測實績與相關技術經驗	30%
3	資訊安全風險現況評估、伺服主機弱點掃描方法、資訊設備組態、網路封包側錄分析，包含需求確認、分析規劃、資訊蒐集、執行方式、工具等作業方法與程序	40%
合計		100%

十六、遴選審查結果將以 email 方式通知申請團隊聯絡人。