遠端操作與維護平台連線申請單 Connection application for remote operation and maintenance platform

ISPI-D-047，機密等級 Level of confidentiality：2限閱， 版　　本 Version：2.0

紀錄編號. / NO　　填表日期. / Date.

申請單位 Unit	(校內承辦單位)	**分機 Ext.**	(分機)
申請人 Applicant	(校內承辦人員)	**亞洲網路帳號 Asia Network ID, ANID**	(資安個資事件通報及帳號啟用通知)
服務/合約/專案計畫 Services / Contract / Project	(專案計畫、工程或維護採購合約全名)		
專案執行單位/委外人員			
專案執行單位 Project execution unit	(校內單位或委外公司全名)	**帳號使用人員聯絡電話 Account User Phone**	
帳號使用人員姓名 Account User	(平台主要使用者/工程師)	**帳號使用人員電子郵件 Account User EMAIL**	(資安個資事件通報及帳號啟用通知)

1. **亞洲大學基於資通訊安全與個人資料保護管理之目的，並遵循「個人資料保護法」、「資通安全管理法」、「臺灣學術網路管理規範」辦理，蒐集單位、姓名、電話及電子郵件等個人資料，以在本校地區內，作為資通安全管理紀錄之用。您得以行使請求查閱、補充、更正；請求停止蒐集、處理、利用；請求刪除個人資料等權利。**
2. **帳號使用人員為校外人員(含委外)時，請依合約辦理保密切結作業，並請提供佐證資料查驗。(如、保密切結書)**

來源 IP Source IP	(選填，可多個，資訊安全稽查時提供快速鑑識使用)		
目的伺服器 IP Destination server IP	(經由需連線維運的伺服器 IP，開啟防火牆用，若有多台，請列表作為申請附件)		
目的伺服器管理人員 Destination server administrator	□同申請人 applicant □亞洲大學資訊發展處人員 AU OICT staff □本校其它人員 Other	單位姓名 name	
帳號使用期間 Account permit period (應檢附合約/計畫影本) (掃描電子檔可) (Copy of contract required) (Accept scanned files)	**短期 short term** (短期最長不超過90日 maximum duration of 90 days.) □ 7日.(7day) □ 14日.(14day) □ 28日.(28day) □自申請日起至　　年　　月　　日止，共　　日 From apply Date to　Year　Month　　Day, total　　of days. **長期 long term** (依合約/專案計畫日期辦理 Processed according to the contract/project plan date.) □申請日至當年12月31日 The period extends until December 31st of the year of application. □申請日至次年07月31日 The period extends until July 31 of the following year after the application.		
帳號 Account	(使用者自設帳號) – (公司/單位英文名簡稱)		

帳號說明：

1. 請提供使用者自設帳號與公司/單位英文名縮寫，帳號為兩者合併以供區隔。
   如、單位是 oict 使用者是 junny，VPN 帳號為 junny_oict
2. 亞洲大學遠端操作與運維架構，會同時開通「VPN」與「操作平台」兩個系統的帳號。
3. 目的伺服器管理人員會同時開通核准帳號，每次連線平台的申請由目的伺服器管理人員審核。
   (可含代理人，需要再提供代理人資訊)
4. 提出的連線請求，會以「電子郵件提供連結」、「登入平台」或「TEAMS 通知」(須按裝元件)方式提供目的伺服器管理人員審核。

申請單總共有2頁

維護合約 VPN 帳號 (Maintenance Agreement VPN account)

遠端操作與維護平台連線申請單 Connection application for remote operation and maintenance platform

ISPI-D-047，機密等級 Level of confidentiality：2限閱， 版　　本 Version：2.0

1. 本校遠端維護平台使用 FortiGate VPN +多因子驗證 token 作為第一線驗證程序，已與亞洲大學 SSL-VPN 服務區隔，提供連線本校伺服器區人員使用。
2. 使用方式與架構圖請參閱申請單附件。
3. 同一案件僅提供一組帳號與 token 連線。每間公司只會搭配1組 token，請由主要維護人員使用。
4. 為維護雙方權益，本 VPN 限定週一至周五 07:30-20:00方得連線，其他特殊需求，請統一由伺服器管理員提出。
5. 連線操作設定將與連線帳號開通通知，同時寄送。

特權帳號管理平台 (Privileged Account Management Platform)

1. 本校使用 One Identity 特權帳號管理平台作為第二線安全程序，連線維護平台主機轉伺服器。(以下稱平台)
2. 每次連線需在平台申請，由伺服器管理人員授權後，在允許時間內下載連線檔案使用。
3. 架構圖連線申請與請參閱申請單附件。
4. 帳號與維護合約 VPN 帳號相同，但系統各自獨立，通行密碼請個別變更。
5. 預設密碼於開通後以電子郵件通知，初次使用請變更預設密碼。
6. 通行密碼有效期90天，有效期內可自行登入變更密碼。
7. 同 VPN，平台連線操作設定將與連線帳號開通通知，同時寄送。
8. 平台虛擬主機如何連線至目的伺服器，請洽詢目的伺服器管理人員。

平台虛擬主機 至 目的伺服器 間 Between the virtual host and the destination server

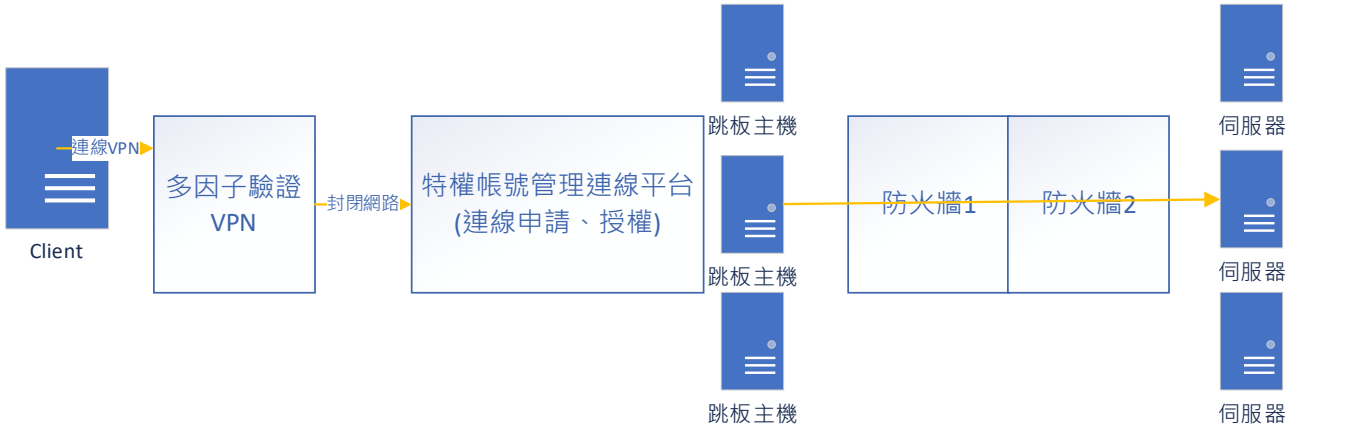
開啟的遠端服務 **Enable remote services**	□Windows Base (Open RDP Service) □Unix Like (Open SSH Service)
防火牆連線埠 (列表) **Firewall port (list)**	(如、1433。維護不需要用到的不用填)

資訊發展處評估事項 OICT Assessment Items

□維護合約/計畫在有效期內，合約資安與個資保護資訊符合本校安全要求
□目的伺服器管理人員明確
□單位/委外公司，具有有效的資安自評表或 ISO27001證明
□有效的使用人員保密切結聲明與資安教育訓練時數證明

申請單位 Unit	資訊發展處 Office of Information and Communication Technology		
	聯合服務櫃檯 Service counter	目的伺服器管理員 Destination server administrator	網路維運組 Network Section
申請人 Applicant	收件日期時間 Received date and time	□同申請人 same as applicant	平台管理員 Platform Administrator
單位主管 Unit Director		權責主管 Unit Director	權責主管 Unit Director

亞洲大學遠端操作與運維架構圖



二階段驗證
Forti Client

特權帳號管理連線平台
1.平台為WEB介面
提供user 端的連線請求，與Server管理員連線授權服務
2.每一連線申請預設值為2小時(可申請4小時)，經授權核准後，可在平台下載RDP連線檔案進行連線，每次中斷要重新下載。連線時間將截止時，可申請授權延長。
3.每一client僅可連線授權指定的跳板主機
4.跳板主機已阻斷對校外連線，有檔案或腳本需置放於跳板主機，請聯絡目的伺服器本校的系統管理員

目的伺服器
1.防火牆僅允許RDP及SSH及申請單上有提出申請的網路埠通過
2.防火牆允許通行的時段為
工作日(週一至周五)08:00-20:00
特殊情況請由伺服器管理員經權責主管同意，以電子郵件等方式提出以資佐證。

使用須知

1. 亞洲大學防火牆內伺服器，**不提供 來自網際網路的**直接**遠端連線服務**(RDP<TCP 3389>及 SSH<TCP 22>)。

亞洲大學防火牆區域伺服器提供兩種類型連線方式

類型	校級伺服器區	代管主機區
說明	本校核心系統伺服器、由資訊發展處人員管理之系統伺服器及資訊機房伺服器。	單位系所、計畫申請之校內專案虛擬主機
校內連線基本要求	校內連線來源主機應具備 EDR 等安全性防護。	應提供校內固定來源主機 IP。
校外人員遠端連線	1. 使用伺服器管理人員主機連線。(如、teams 會議遠端主控) 2. 請使用本申請單申請使用帳號。 3. 每次連線由伺服器管理人員核准。	1. 使用伺服器管理人員主機連線。(如、teams 會議遠端主控) 2. 使用 TWAREN SSL-VPN 服務，請使用「校外人員 VPN 帳號申請單」申請 VPN 帳號。

2. 本架構具備多階段驗證，請配合使用
   (1) 多因子驗證 VPN：使用 FortiGate VPN +多因子驗證 token 作為第一線驗證程序，已與亞洲大學 SSL-VPN 服務區隔。

(2) 特權帳號管理連線平台：使用 One Identity 特權帳號管理平台作為第二線安全程序，連線維護平台主機轉伺服器。

3. 本管理平台具行為側錄功能，若不同意進行側錄，請執行單位人員親至本校，在目的伺服器管理人員監控下進行維運作業。
4. 平台虛擬主機設置有本機防火牆，運維所需使用埠請自行開啟。
   遠端桌面連線埠設置有白名單，請勿任意更動。
5. 平台虛擬主機至目的伺服器之防火牆連線規則，於使用期間到會自動停用(Timer Disable)。
6. 資訊發展處於每年會進行伺服器防火牆規則盤點，若已不再有續期合約檢附，將逕行刪除虛擬主機連線規則，若後續再重新簽訂合約，需重新申請。
7. 本申請單經目的伺服器管理員評估會辦後，由網路維運組評估安全性並進行平台設置作業，啟用後以電子郵件方式通知。
8. 填寫完畢請送交資訊處聯合服務櫃檯，相關問題請連絡分機3515轉接網路維運組。
9. 暫不提供由國外連入，請使用所在地在臺灣的網路連線。