

第十四點附錄 7(修正後)

附錄 7：公文電子交換系統之各機關權責辦理資通安全相關事項

為管理公文電子交換環境正常運作，確保公文電子交換系統(下稱交換系統)之機密性、完整性及安全性，本附錄適用於依機關公文電子交換作業辦法規定進行文書傳遞交換作業之各機關(構)。

一、交換系統之資通安全事項，除資通安全管理法及其相關子法另有規定外，應依本附錄規定辦理。

二、交換系統架構，區分為四個層級，說明如下：

(一)管理層：係由國家發展委員會檔案管理局(以下簡稱檔案局)主管之電子文書檔案服務中心。

(二)交換層：係由中央部會及直轄市政府、縣(市)政府等主管之公文統合交換中心(以下簡稱交換中心)。依開發維運型態，分為下列三種交換中心：

1. 共用中心：係由檔案局開發公文交換程式，並建置硬體設備環境、負責設備維運及軟體使用管理，提供使用機關(構)進行公文電子交換者。

2. 自管中心：係使用檔案局開發之公文交換程式，自行建置硬體設備環境、負責設備維運及軟體使用管理，提供使用機關(構)進行公文電子交換者。

3. 自建中心：係自行或委外開發公文交換程式，自行建置硬體設備環境、負責設備維運及軟體使用管理，提供使用機關(構)進行公文電子交換者。

(三)機關層：係負責公文管理系統或其他應用系統且與交換層介接，以進行電子公文傳遞作業者。

(四)終端層：係由各機關(構)使用交換系統進行公文電子交換收發文作業之終端用戶。

三、各機關(構)應依交換系統架構之層級辦理下列事項：

(一)共通性安全事項：

1. 應定期檢查主機安裝之伺服器應用軟體憑證效期，並於憑證過期前更新憑證，以確保交換系統正常運作。

2. 應依各機關(構)業務需求，定期登入系統收發公文，以確保公文電子交換作業正常運作。

(二)管理層機關：負責規劃、推動交換系統發展與維護等安全管理事項，確保業務永續運作，包括：

1. 對交換層及機關層主機之作業環境建立標準組態列表，包括作業系統版本、套件版本及相關組態設定等作為系統安全維護設定之準則。

2. 配合各交換層主機 IP 位址之變動，更新交換主機 IP 位址清單，並據以修正防火牆白名單設定，同時通知各交換層機關。
3. 訂定交換系統安全傳輸協定，確保傳遞過程全程加密，並建立收發文確認機制，防止未經授權之資料存取及竄改。
4. 應依資通安全責任等級分級辦法附表十所定資通系統防護基準中級以上之控制措施辦理交換系統維護作業。

(三) 交換層機關：負責交換層交換中心之運作與督導所屬機關層及終端層使用者交換作業等安全管理事項，包括：

1. 配合管理層發布之作業系統更新及漏洞修補通知，排定更新及修補時程，並儘速完成更新及風險控管。
2. 接獲管理層發布之交換層主機系統更版通知時，配合預定更版時程，盡速完成系統更新。
3. 交換系統各項主機應專機專用，不得安裝非必要軟體，並以防火牆及其他必要安全設施管控與其他主機間之資料傳輸及資源存取，非必要應禁止與網際網路進行連線。
4. 依據管理層通知之交換主機 IP 位址清單進行防火牆白名單設定，並以一對一固定 IP 位址為原則，有交換主機 IP 位址異動需求者，應通知管理層辦理連線異動事宜。
5. 交換層機關應以防火牆白名單控管機關層及網頁版公文收發模組用戶連線作業，並以一對一固定 IP 位址為原則，有 IP 位址異動需求者，應通知交換層辦理連線異動事宜；確有一對多或非固定 IP 位址之需求者，應向交換層機關申請核准，並應建立 IP 位址與機關（構）名稱對照表，以供追蹤及查檢之用。
6. 交換層機關提供網頁版公文收發模組介接使用交換系統，應依本附錄之要求辦理管理作業，若交換層機關未提供網頁版公文收發模組，則本項目檢核為不適用。
7. 應依資通安全責任等級分級辦法附表十所定資通系統防護基準中級以上之控制措施辦理交換系統維護作業，委外作業應依資通安全管理法施行細則第七條規定辦理。
8. 交換層機關對於非所業管機關（構）參與交換系統服務之請求，應本行政協助原則予以協助，非有正當理由，不得拒絕。倘無法為收容，應與其他交換層機關協商，協力完成收容作業。

(四) 機關層機關(構)：負責機關層公文交換相關軟硬體設施之安全管理，包括：

1. 於接獲交換系統發布之更版通知時，配合預定更版時程，盡速完成系統更新。
2. 機關層主機應專機專用並採用固定 IP 位址，並提報交換層機關備查，因特殊理由未能遵行者，應採取必要之監管措施，並提報交換層機關

核准。有主機 IP 位址異動需求，亦應通知交換層機關以進行白名單之設定。

(五) 終端層機關(構)：負責終端用戶本身之公文交換相關軟硬體設施之安全管理，包括：

1. 機關(構)有資訊異動(例如機關(構)代碼、機關(構)名稱、電子憑證 IC 卡等)或機關(構)裁撤情形，應依管理層發布之程序辦理連線異動事宜。

2. 系統登錄註冊之電子憑證 IC 卡應專卡專用，並指定專人妥善保管。未使用時應妥善收存以防止遺失，並定期檢查憑證效期，在憑證過期前更新憑證 IC 卡。

四、使用共用中心、他機關自管中心或自建中心者，所屬中央部會或直轄市政府、縣(市)政府對交換系統資通安全要求事項應盡管理及督導之責。

五、管理層及交換層機關應將交換系統納入年度資通安全稽核計畫，並至檔案局指定網站完成交換系統資通安全自評及稽核結果彙整資料填報作業。

六、交換層機關經評估資通安全風險程度，得對所屬機關層及終端層機關(構)進行定期稽核，對於不符合事項應要求即時改善及追蹤改善情形。對嚴重不符事項或特殊資通安全事件，應不定期進行專案稽核作業。

七、各機關(構)應依自評及稽核結果，對執行交換系統資通安全工作績優或缺失人員，予以適當獎懲。管理層及交換層機關得對執行交換系統資通安全工作績優或缺失之各機關(構)人員(含所屬機關(構))，予以適當之獎懲建議。

八、管理層及交換層機關因資通安全需求，請使用機關(構)配合調查或辦理事項，使用機關(構)應於期限內完成。各機關(構)發生下列情形之一者，所屬交換層機關或管理層機關得中止對該機關(構)之系統服務：

(一)發生資通安全事件通報應變及演練辦法所定第三級或第四級資通安全事件。

(二)電子憑證 IC 卡遺失或未使用加解密模組。

(三)未將交換系統納入機關內部或參採所隸上級機關(構)之資訊安全管理系統(ISMS)管理。

(四)交換層機關未將交換系統納入 ISMS 第三方認證範圍及資通安全監控中心(SOC)監控範圍防護。

(五)未依規定辦理交換系統資通安全自評或未對所屬機關層及終端層機關(構)進行定期稽核。

(六)發送廣告性質電子公文經交換層機關警告後仍未改善。

(七)其他未依本規範規定執行工作權責且情節重大。

修正說明：

一、附錄序號變更。

二、修正公文電子交換架構，並增訂交換系統之各機關(構)權責資通安全相關事項。

三、其餘未修正。

第十四點附錄 9(修正前)

附錄 9：公文電子交換架構

現行公文電子交換整體交換架構如圖 9，使用單位得透過共用/自管中心或自建中心進行公文傳遞交換，其名詞定義如下：

- 1、共用/自管中心：前者指由國家發展委員會檔案管理局開發公文交換程式，並建置硬體設備環境、負責設備維運及軟體使用管理，提供使用機關(構)進行公文電子交換；後者指使用國家發展委員會檔案管理局開發之公文交換程式，自行建置硬體設備環境、負責設備維運及軟體使用管理，提供使用機關(構)進行公文電子交換者。
- 2、自建中心：指自行或委外開發公文交換程式，自行建置硬體設備環境、負責設備維運及軟體使用管理，提供使用機關(構)進行公文電子交換者。

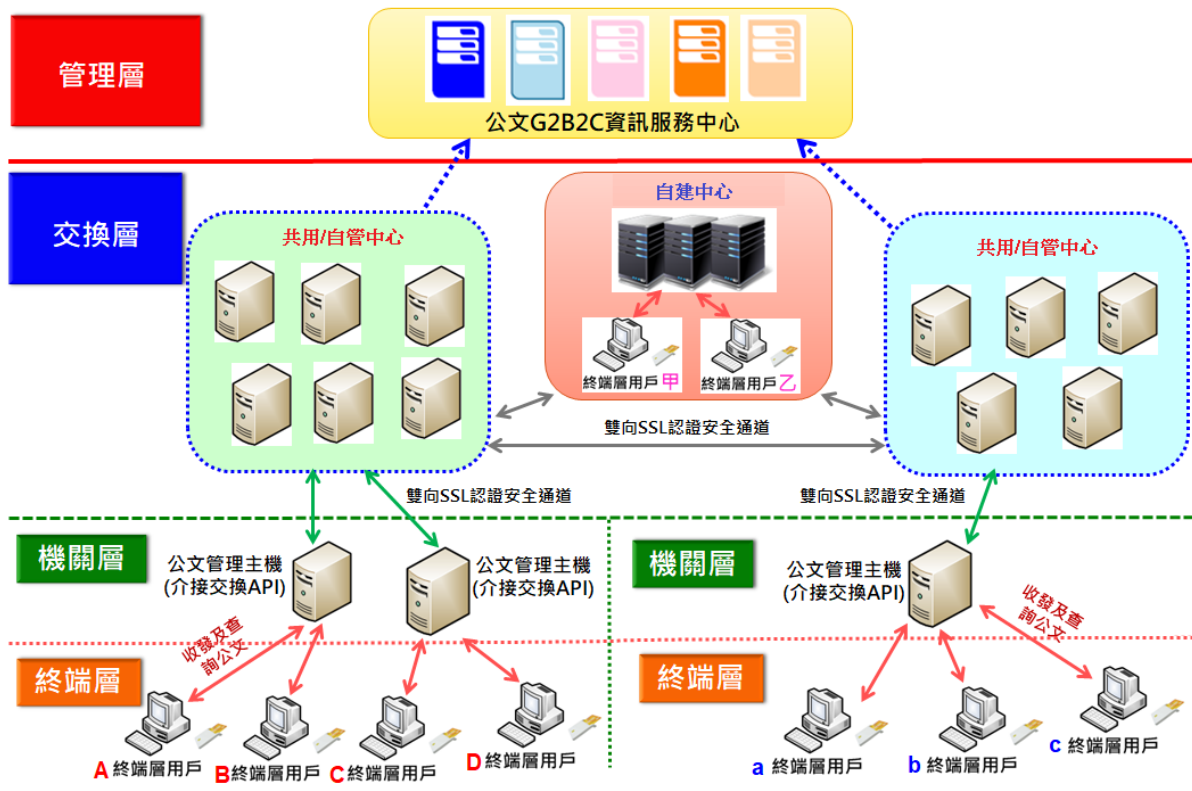


圖 9 公文電子交換架構圖

茲分別說明 2 種模式交換歷程如下：

- 1、共用/自管中心：利用共用/自管中心之公文電子交換系統進行公文傳遞交換。如圖中 A 終端層用戶、B 終端層用戶、C 終端層用戶、D 終端層用戶與 a 終端層用戶、b 終端層用戶、c 終端層用戶等，當進行公文傳遞交換時依據所發送之對象，分為中心內部交換與跨中心交換 2 類，相關作業歷程為：

- (1) 共用/自管中心內部交換

當同一共用/自管中心內部之使用單位進行文書傳遞交換時，如 A 終端層用戶、B 終端層用戶、C 終端層用戶、D 終端層用戶或 a 終端層用戶、b 終端層用戶、c 終端層用戶間，透過圖中各共用/自管中心之機關層系統(與交換 API 介接之公文管理系統)及交換層公文電子交換系統即可內部進行交換作業。

- (2) 與自建中心進行交換

若是由 A 終端層用戶發送公文至屬於自建中心之使用單位時，則由共用/自管中心之公文電子交換系統進行對外傳送作業；如 A 終端層用戶擬發送公文至終端層用戶乙，則由共用/自管中心之公文電子交換系統將公文傳送到自建中心之公文電子交換系統，終端層用戶乙再至該中心公文電子交換系統收取公文，即完成整個公文傳遞交

換作業。

(3) 與其他共用/自管中心進行交換

若是由 A 終端層用戶發送公文至屬於其他共用/自管中心之使用單位時，則由共用/自管中心之公文電子交換系統進行對外傳送作業；如 A 終端層用戶擬發送公文至 a 終端層用戶，則須由共用/自管中心一之公文電子交換系統將公文傳送到共用/自管中心二之公文電子交換系統，再由 a 終端層用戶透過與交換 API 介接之公文管理系統至該中心公文電子交換系統收取公文，完成整個公文傳遞交換作業。

2、自建中心：透過自建中心進行公文傳遞交換。如圖中終端層用戶甲與終端層用戶乙，當進行公文傳遞交換時依據所發送之對象，分為中心內部交換與跨中心交換作業 2 類，相關作業歷程為：

(1) 自建中心內部交換

同一自建中心下之使用單位互相進行交換作業，如終端層用戶甲發送公文至終端層用戶乙時，透過圖中自建中心所屬之公文電子交換系統即可進行內部交換。

(2) 跨中心交換

1、與共用/自管中心進行交換

若是由終端層用戶甲發送公文至屬於共用/自管中心之使用單位時，則由自建中心之公文電子交換系統進行對外傳送作業；如終

端層用戶甲擬發送公文至 B 終端層用戶，則須由自建中心之公文電子交換系統將公文傳送到共用/自管中心一之公文電子交換系統，最後由 B 終端層用戶透過與交換 API 介接之公文管理系統至該中心公文電子交換系統收取公文，完成整個公文傳遞交換作業。

2、與其他自建中心進行交換

若是由終端層用戶甲發送公文至屬於其他自建中心之使用單位時，則由所屬自建中心之公文電子交換系統進行對外傳送作業；如終端層用戶甲擬發送公文至其他自建中心之使用單位，則須由自建中心之公文電子交換系統將公文傳送到其他自建中心之公文電子交換系統，再由收文機關至該中心公文電子交換系統收取公文，完成整個公文收發作業。