專題

公文電子交換系統之資訊安全改善建議

Suggestions for Improvement on Information Security of the Electronic Official Document Exchange System

■ 賴國旺 Jeff Lai
財團法人資訊工業策進會創新應用服務研究所組長
Section Manager,
Innovative DigiTech-Enabled Applications & Services Institute, Institute of Information Industry

摘要

公文電子交換系統緣起於行政院研究發展考核委員會推動「數位臺灣」（e-Taiwan）計畫，全面建構政府公文電子交換資訊環境，讓政府與各界可隨時隨地經由安全認證之電子公文往返，快速傳遞公務訊息。現行公文電子交換系統由財團法人資訊工業策進會開發與維運，迄今已建置 58 個公文統合電子交換中心，並提供 15,000 多個政府機關 / 單位 / 學校及 5,000 多家公司行號加入參與公文電子交換應用，是為我政府重要資訊高速公路。

公文電子交換系統為我政府資訊傳遞的核心系統，應特別強化資訊安全防護與管理，以確保系統充分滿足機密性（Confidentiality）、完整性（Integrity），與可用性（Availability）的三大資訊系統安全目標，以對抗日新月異的駭客攻擊手法。本研究將深入探討現有公文電子交換網路系統資訊安全強化之長、中、短期可能之做法，深入系統技術架構之整體調整規劃，俾利各機關建置穩定、安全之公文電子交換強固環境。

ABSTRACT

The electronic official document exchange system was initiated from Digital Taiwan Project by the former Research, Development and Evaluation Commission, Executive Yuan. Taiwan government intended to construct a comprehensive environment for exchanging official documents electronically among agencies, so that all level of government agencies were able to transmit their official documents rapidly in a secured way using digital signature technologies. For this reason, Institute of Information Industry contracted by our government has been responsible for maintaining the system since then. The system consisting of 58 document exchange centers for about 15,000 government agencies and 5,000 non-

government organizations has become one of the most important services for our government in the information highway.

Since the system is a core function of our government information delivering mechanism, confidentiality, integrity and availability in its information security framework become more important. This article is to examine feasible solutions for establishing a more robust official document exchanging environment, including different approaches for goals in short-, middle- and long-term.

關鍵字：公文電子交換、資訊安全

Keywords：electronic official document exchange, information security

壹、前言

行政院研究發展考核委員會（民國 [以下同]103 年 1 月與行政院經濟建設委員會等機關合併，改制為國家發展委員會）依據行政院推動公文電子交換公文 2000 工作計畫，實施公文電子交換推廣計畫（註 1），以網路傳輸公文，取代郵寄及人工傳送，加速公文傳遞效率。自 89 年 7 月起，分 3 階段將公文電子交換推廣至各級政府機關，藉由政府資訊化服務提升行政效能。自此公文電子交換系統之發展，歷經公文電子閘道系統架構、E-mail 傳遞、點對點交換（Peer to Peer）等不同交換技術沿革，至 98 年起創新建置第 4 代公文電子交換統合中心系統，迄今已建置 58 個統合公文電子交換中心（以下簡稱統合交換中心），並提供 15,099 個政府機關 / 單位 / 學校及 5,000 多家公司行號加入參與公文電子交換應用，是為我政府重要資訊高速公路。

公文電子交換系統為我政府資訊傳遞的核心系統，應特別強化資訊安全防護與管理，以確保能充分滿足機密性（Confidentiality）、完整性（Integrity），與可用性（Availability）的三大資訊系統安全目標，以對抗日新月異的駭客攻擊手法。尤其是國際上資安威脅已從個別、單純的炫耀，演變成有組織、以經濟或政治等特定利益為目的的入侵行為，而我國更因為政經情勢特殊，近年屢遭駭客以進階持續性攻擊（Advanced Persistent Threat，簡稱 APT）（註 2）方式，企圖竊取公務、國防及商業機密。現有公文電子交換統合中心系統已建置多年，面對日益嚴峻的新型態資訊安全挑戰，急需持續強化系統資訊安全架構與管理，無論是機密性、完整性及可用性的要求皆必須採高標準控制措施，提高防護目標水準，才能確保系統能通過外部有計畫組織的進階持續性攻擊。

依據國家發展委員會檔案管理局（以下簡稱檔案局）102 年 7 月 10 日提報行政院，有關「公文電子交換系統資安事故檢討與加強防範措施報告」之中長期強化措施，以及行政院國家資通安全會報辦公室於 102 年 8 月 30 日會議建議公文電子交換系統交換層，可評估集中化做法等建議，將深入探討現有公文電子交換網路系統資訊安全強化之長、中、短期可能之做法，擬深入系統技術架構之整體調整規劃，俾利各機關建置穩定、安全之公文電子交換強固環境。預期技術架構改善之資安

強化目標如下：

一、強化 G2B2C 中心系統（含統合中心系統與 eClient）之系統軟體資訊安全，降低資訊安全風險發生機率及尋求快速應變與災害復原能力。

二、強化各統合中心自主管理能量，進一步防範駭客計畫性偽冒攻擊，提升統合中心系統安全，協助各統合交換中心與終端交換層提升資安管理及防禦能力。

三、強化資訊安全防護縱深，從系統與軟體防護層深化為全面資料防護管制，確保系統及業務資訊資產之機密性、完整性與可用性之最高要求。

貳、系統現況摘要

行政院自 89 年 7 月實施公文電子交換推廣計畫，以網路傳輸公文，取代郵寄及人工傳送，加速公文傳遞效率，歷經變革之後，由第 1 代公文交換前置處理器（Front End Processor，簡稱 FEP）、第 2 代公文交換之公文電子閘道系統、第 3 代公文交換採用公文 G2B2C 前置處理交換器（XML-Box）以點對點方式交換等，一直到現在第 4 代公文電子交換統合中心系統架構。現行公文電子交換機制分為以下三類：

一、以 XML-Gateway 系統介接交換

屬於早期的自建交換中心型式，其自建交換中心內部使用自行定義的交換機制，與統合交換中心使用的 eClient 交換方式並不相同，但是透過 XML-Gateway 轉接後，可與其他自建交換中心或統合交換中心順利交換以 DI（註 3）檔為交換格式的電子公文。

二、以 e-Gateway 系統介接交換

屬於新型的自建交換中心介接系統，e-Gateway 除具有傳統 XML-Gateway 功能外，也能交換新型態以信封檔為交換格式的電子公文，因此也具備能應用信封檔機制，產生較為廣泛的功能。

三、以統合交換中心交換（eCenter）（註 4）

即目前檔案局委託公文 G2B2C 資訊服務中心維運的應用系統軟體，目前共建置有 58 個統合交換中心，包含大部份中央及地方政府機關，為主要公文電子交換資訊環境。其交換機制同時包含傳統 DI 電子公文交換及新型態信封檔交換機制，為目前使用交換的主流。

由於統合交換中心為主要之現有公文電子交換資訊環境，以下將詳細說明統合交換中心架構：

（一）統合交換中心運作架構

以檔案局目前委託公文 G2B2C 資訊服務中心所負責的以統合交換中心交換架構而言，其公文電子交換運作的架構分為三層，包括管理層（公文 G2B2C 資訊服務中心機房）、交換層（各統合交換中心）及終端層（eClient），如下頁圖 1。

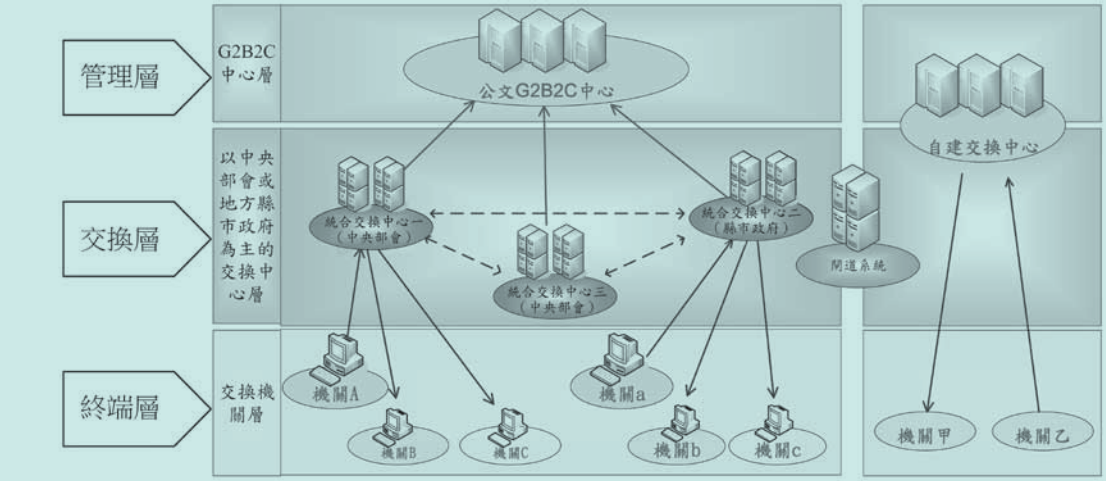

圖 1：統合交換中心三層式架構隸屬

資料來源：作者繪製

1. 管理層（公文 G2B2C 資訊服務中心機房）

管理層主要是用來支援交換層及終端層的運作，以集中式管理處理分散的交換機制，讓系統更具有彈性及強固性，其功能包括地址簿更新下載、eClient 版本更新、Server 端交換主機版本更新、交換 Log 收集等相關管理工作，並不經手公文電子交換工作。主要設備位於行政院共構機房。

2. 交換層（各統合交換中心）

交換層則用來提供部會或縣市政府公文電子交換之作業需求，建置於部會或縣市政府指定機房，負責統合交換中心內部及跨統合交換中心間的公文電子交換作業，一方面協調整合所屬機關進行公文電子交換訊息介接，所屬機關即可取得相關通知及線上接收上級機關轉辦之公文，另一方面提供對其它統合交換中心，或不同公文電子交換機制之公文電子交換訊息介接，加速轉文辦理時間。

3. 終端層（eClient）

終端層則是統合交換中心交換架構中最終端的系統環境，由各收發文用戶機關提供個人電腦安裝 eClient 軟體，透過 GCA 或支援的相關憑證進行公文簽發，與機關所隸屬的統合交換中心搭配，共同完成公文電子交換服務。eClient 同時也做為和各機關公文管理系統主要界接的地方，將公文以目錄收發方式轉接給公文管理或公文製作系統。

（二）統合交換中心運作流程

為使龐大數量的公文在不同的統合交換中心或其他公文電子交換架構中安全有效的順利運行，負責公交轉發傳遞機制的統合交換中心運作流程作業相當複雜，簡要概述如下：

1. 公文電子交換流程

發文時由終端層（eClient）將公文傳送到交換層，經格式查驗，查詢地址簿資訊，加簽章後將公文傳送到收文方所屬的統合交換中心。收文時由終端層（eClient）定期到交換層詢問是否有待收的公文，如有則驗明簽章，確認非假造後下載，並回傳確認訊息。

2. 地址簿更新流程

機關異動需向維運辦公室申請，由維運辦公室加入地址簿。定期（每天）將地址簿由管理層（公文 G2B2C 中心機房）下載到交換層供各統合交換中心使用。

3. eClient 版本更新流程

eClient 每次登入時會向版本更新主機傳送版本資訊，並詢問是否為最新版本，如果不是最新版，系統則會主動啟動更新作業。

4. 交換主機版本更新流程

交換主機也會定期向 Subversion(SVN) 版本更新主機詢問是否有最新版本，如有則會啟動交換主機的版本更新機制。

5. 交換 Log 收集流程

由各統合交換中心將公文交換的 Log 紀錄 (此為應用系統的 Log，並非網路或應用主機的 Log)，傳送到公文 G2B2C 中心機房彙整保存。

參、系統架構改善建議

現行公文交換網路系統雖承襲過去電子交換系統推行的成果與經驗，但自 97 年研發暨維運至今已 6 年之久，面對與日俱增的資訊安全威脅，對於系統資訊安全強化有強烈的急迫性，是以規劃短、中、長期之整體系統強化與改善建議。短期規劃著重於現有系統的資訊安全管理強化措施，中期規劃為虛擬化集中管理與資料全程加密保護機制，並針對架構性系統全面調整做為長期研發規劃，發展公文雲端應用服務架構，整體發展規劃如表 1。

表 1　公文電子交換系統架構資安改善建議

短期	中期	長期
■ 強化現有系統資訊安全管理 ➢ 多層式作業系統更新 ➢ 軟體版本數位簽章防護更新機制 ➢ 中心端網頁程式亂碼化 ➢ API 介面參數亂碼化	■ 導入虛擬化技術 ➢ 集中小型統合交換中心為共用交換中心，提升整體資安偵防水準。 ➢ 配合虛擬化系統特點，強化系統資訊安全管理，提升整體系統安全管理效率。 ■ 啟用交換環境全程加密 ➢ 協調各自建中心配合導入全程加密技術，運用加密技術全程確保系統機密性。	■ 發展雲端公文系統 ➢ 導入雲端自動擴展與資料分散運算技術，規劃整體公文系統架構 ➢ 重新開發雲端公文電子交換系統與 API 模組 ➢ 重新開發雲端公文管理與製作整合交換 API 系統 ➢ 導入雲端虛擬桌面技術，讓公文電子檔全程不落地

資料來源：作者整理

一、強化現有系統資訊安全管理

有鑑於網路攻擊手法不斷翻新，駭客善於利用社交攻擊模式，偽冒入侵系統事件頻傳，規劃系統軟體強化措施包括作業系統更新機制強化、應用軟體更新機制強化以及應用程式混淆化、應用介面（API）傳遞參數混淆化，隱藏程式作業方式與路徑等，重新定義連線參數與溝通方式，強化軟體安全。相關規劃說明如下：

（一）多層式作業系統更新

作業系統為主機的基礎服務，也是主機資訊安全防護的第一道防線，隨著時間與技術的更新，作業系統的弱點或漏洞會陸續被公布，無論是 Microsoft、IBM、Redhat 等商業版本作業系統，亦或是本專案使用之 CentOS，其官方網站都會持續維護作業系統之資安更新資訊，以確保作業系統安全。因此，定期執行作業系統更新是系統維運的重要任務。

現有公文交換系統中心端 CentOS 作業系統之更新作業，依據檔案局資訊安全管理手冊要求，強化作業系統及套裝軟體變更應遵循下列控制措施：

1. 作業系統在升級進行修補程式或套裝軟體進行修改之前，由應用系統負責人評估其對應用系統的影響。
2. 審視應用系統的控制和整合程序，以確保不會造成應用系統無法正常運作。
3. 審視是否取得合法使用權。
4. 變更前事先通知並保留足夠的時間，供應用系統負責單位進行審查和測試。

據此將規劃多層式作業系統更新機制，以建立正式營運系統之作業系統更新之測試與評估，並配合各統合交換中心之自主管理機制，提供不同的作業系統更新配套服務，整體架構如圖 2。

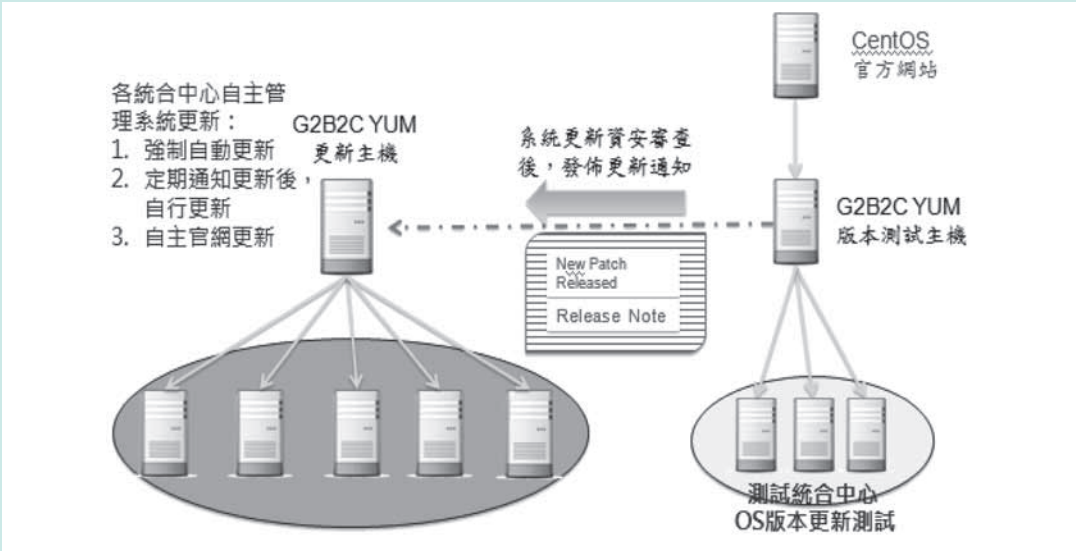

圖 2：多層式統合中心作業系統更新機制

資料來源：作者繪製

1. G2B2C 中心 Yellow Dog Updater Modified（YUM）版本測試作業

第一層版本 YUM 更新測試主機將建置於公文 G2B2C 中心，負責從 CentOS 官方網站將最新更新 Patch 封裝檔下載，由系統維護人員執行更新 Release note 判讀與分析，評估更新內容及更新測試作業，據以評估測試相關更新對系統的資安與運作影響，彙整為更新評估與測試紀錄。

2. 審查系統更新資安作業與發佈更新訊息

作業系統更新套件經由應用系統維運人員，完成對應用系統的影響評估與測試後，將彙整相關更新資訊（Release note）與測試報告，提報檔案局審查，經檔案局審查通過後，再由 G2B2C 中心正式發布作業系統更新資訊予各統合交換中心管理人員，由各統合交換中心依據自主管理評估與更新。

3. G2B2C 營運更新主機作業

G2B2C 中心營運更新 YUM 主機擔任各統合中心更新之中介主機，負責將版本 YUM 更新測試主機測試通過之更新 Patch，下載到營運更新 YUM 主機做為各統合交換中心作業系統統一版更新來源。

4. 統合交換中心更新作業

為配合各統合交換中心自主管理需求，本案統合交換中心作業系統更新機制將提供包括：強制統一更新、定期通知後自行更新或自主式官網下載更新等不同服務，以配合各統合交換中心之實際管理需求。

（二）軟體版本數位簽章防護更新機制

在軟體版本管理強化機制方面，將程式開發與測試、營運隔離，建立 Clean Room 環境，淨化程式來源。程式以原始碼形式進入測試區編譯為執行碼後進行測試，完成測試之程式將依據檔案局資安手冊要求，進行應用系統變更審查。為將風險降到最低，作業中應用系統的變更除需遵守變更管理程序外，程式上線應符合檔案局資訊安全管理系統所規定之相關資安審查（Code review, Virus Scan, Changes review 等程序），系統執行檔測試成功後，相關測試紀錄，呈報審核通過後始申請上線更新。

除上述管理機制強化外，在技術架構上，交換系統之軟體更新機制將新增執行碼資安保全機制（Token 簽章），確保軟體來源辨識與完整性（授權、識別、一致）。統合中心軟體及終端用戶 eClient 軟體；經完成測試及資安審查後，將送交專案承辦人或營運權責人員，使用指定註冊之憑證卡執行程式碼簽章控管，以嚴格管制版本項目與來源；軟體更新機制則增加版本驗簽機制，確保更新之程式皆通過驗證，相關作業示意如下頁圖 3。

公文交換系統程式可運用憑證簽章機制，充分確保線上可執行程式的來源與完整性，各運行版本原始碼及執行碼則統一由檔案局版本管理系統控管。

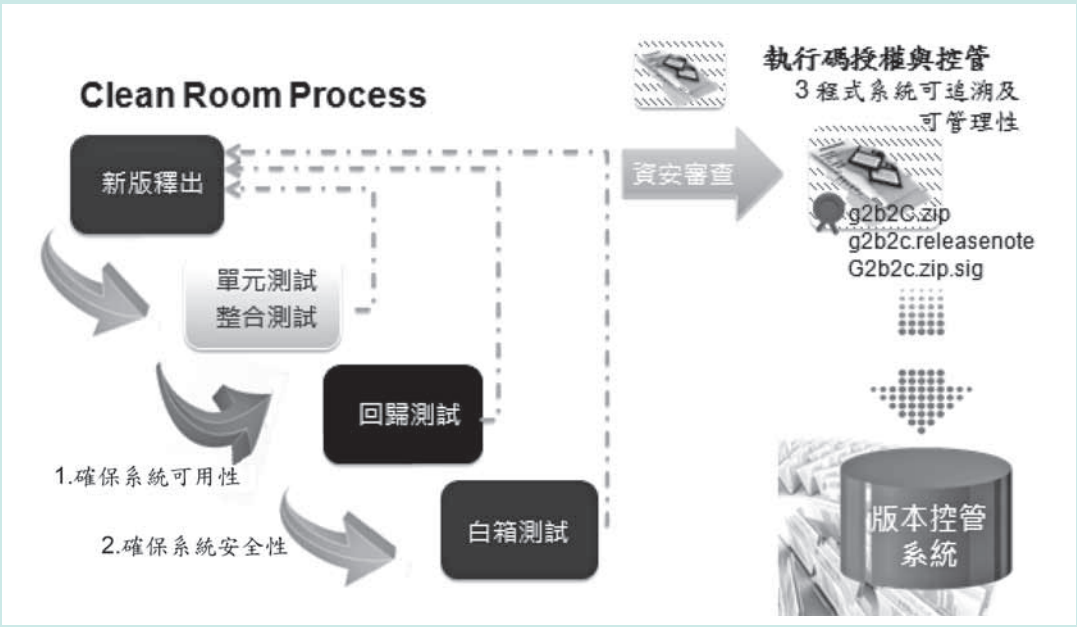

圖 3：版本管理數位簽章防護機制

資料來源：作者繪製

各統合中心之軟體更版及公文交換前端軟體 eClient 更版機制說明如下：

1. 統合交換中心更版作業

各統合中心版本更新管理由統合中心權責機關自主控管，如圖 4 。

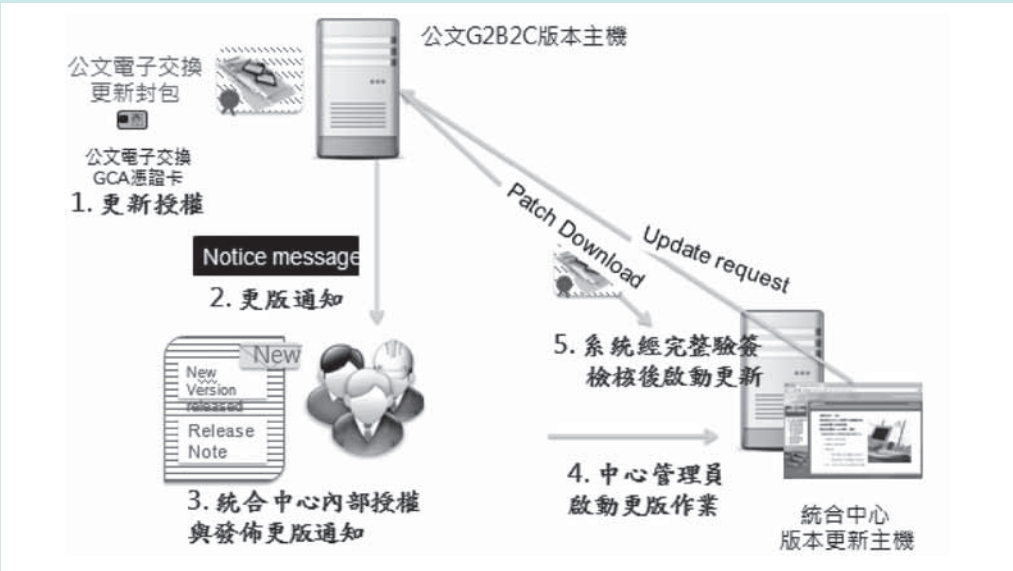

圖 4：統合中心端版本更新防護機制

資料來源：作者繪製

當新軟體版本簽章上傳至公文 G2B2C 版本主機後，系統將發送版本更新資訊予各統合交換中心管理人員；統合交換中心管理人員則將版本更新資訊，依據內部資訊安全管理要求，進行資訊安全審查；通過版本更新審查後，再由統合中心更新主機自行操作新版本下載與更新作業，此時新版本才會下載至統合中心更新主機，經過驗簽通過後進行軟體更新。本項強化修改機制無論統合中心主機或 eClient 軟體都將以統合交換中心更新主機為限，採內部更新，阻絕內部主機及用戶端對外連線的威脅。

2. 更版作業程序

整體更版程序分為三個階段：

(1) 第一階段：更版前期，為加強整體更版機制之嚴謹程度，更版程式將於釋版前進行白、黑箱測試且修改完成確認無誤後，才呈報檔案局更版需求，依指示進行上版動作。

(2) 第二階段：版本釋出時將以 E-mail 通知方式，通報各統合交換中心管理者釋版內容及更新版本，而不直接進行自動更版，待統合交換中心管理者確認後方可執行。

(3) 第三階段：eManager 網頁更版功能，eManager 提供更版畫面供中心管理者選擇更新中心端程式或 eClient 程式，待管理者確認更版後，更版機制才會由版本中心取得最新版程式，並進行 token 驗簽確認其檔案之合法性及完整性。

（三）中心端網頁程式混淆化

為強化系統網頁程式之 Hypertext Preprocessor（PHP）語言程式碼，將採用商用 PHP 程式編碼器（PHP Encoder），透過程式混淆器將交換程式及參數混淆化，避免被惡意攻擊者掌握應用程式運作機制及各項資料與參數內容，並持續遵循最新程式混淆更新機制，確保本項機制之防護有效性。以下將說明本強化機制之優點：

SourceGuardian（註 5）是目前市面上最先進的 PHP Encoder，具有完整的 ground-up rewrite、功能強大的 GUI 涵蓋了最新版本的 PHP 程式編碼混淆相容性。透過 SourceGuardian for PHP 可以達到快速又安全地編碼、編譯，將 PHP 文件進行加密，不僅能保護智慧財產權不被侵犯，還可防止資料庫密碼被盜取。

SourceGuardian 可以限制 scripts、IP 和鎖定網域或是使用內建的授權機制。

使用 SourceGuardian for PHP 的優點有：

1. 保護 PHP 應用程式，以便可以用類似的方式被部署到一個正式的應用程式上，而不用部署原始碼。
2. 鎖定 PHP Scripts 在某 1 臺機器上，這樣應用程式就不會被竊取或挪用到公司以外的工作人員，防止智慧財產權被侵犯。
3. 保護資料庫密碼：保護應用程式中的某一個部分，讓大多數的文件可以被開啟或改變，但

不會影響到核心功能。

（四）API 介面參數混淆化

API 介面為跨模組程式溝通的必要工具，包括中心端系統模組及用戶端程式，與中心端溝通介面都會使用到各種不同的API介面程式，傳統API之使用方式，多採用明碼傳輸方式，易成為資安防護上的弱點，可能受到駭客利用側錄窺探系統作業模式，甚至進行偽冒等攻擊行為。若強化 API 介面防護能力，將系統 API 介面參數予以編碼混淆化，可避免駭客的窺探或偽冒攻擊行為，將大幅提高駭客攻擊的成本，有效降低威脅發生的機率。本項調整包含傳輸技術調整與參數的混淆化，如圖 5 。

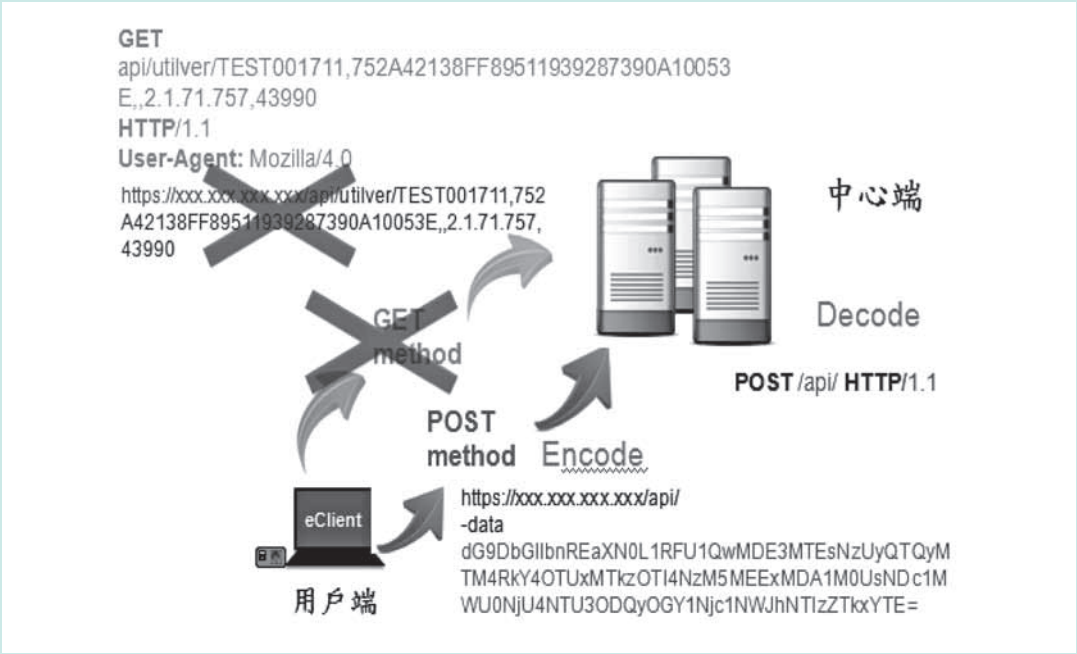

圖 5：API 運作模式與參數混淆化示意

資料來源：作者繪製

介接程式之參數若被截取，容易被複製竄改，本次修改將透過參數亂數加密方式，取代原參數值，並搭配原 SSL 通道加密提高資訊洩漏之門檻。

二、中期規劃統合交換中心虛擬集中化及全程加密

近年來雲端運算相關技術發展已趨成熟，其中以虛擬化技術廣受各類系統所採用，主要原因是短期即可沿用原有應用系統之技術架構，快速達到主機虛擬化後主機資源共用以及維運管理彈性之優點，中長期更可改變應用服務系統整體架構，再配合上應用服務之效能偵測技術、整合虛擬化管理系統所提供之縮放 API（Virtual Machine Scaling Application Programming Interface），即有機會達成依應用服務負載狀況，自動彈性擴展（Auto-Scaling）[註 6] 服務資源之雲端服務系統特性。

另配合行政院組織改造資訊資源向上集中至部會及地方政府之政策，辦理統合交換中心及終端層最適規模虛擬集中化規劃，因應統合交換中心最適經濟規模及終端層集中且分散之管理經濟模式等相關問題，以公文電子交換系統交換層及終端層最適規模虛擬集中化作法，強化交換層之資安強度及透過科技技術簡化管理程序，以提升整體資訊安全強度規劃。

建議採用 iServCloud（註 7）雲端資源管理系統，來負責虛擬化平台之管理系統，以期達成以下所描述之建議解決方案，建立集中虛擬化之統合交換中心共用系統。

（一）提升虛擬化公文交換系統主機維運效率

1. 建立公文交換功能模組虛擬化主機樣版

使用 iServCloud 虛擬化平台將現有公文交換系統，依照各功能模組製成各別虛擬化主機樣版（Virtual Machine Image Template），這樣即可透過虛擬化主機樣版快速建立啟用公文交換模組之虛擬主機。

2. 發展統合交換中心自動部署設定機制

經由虛擬化樣版與服務組合套餐功能所快速建立啟用的公文交換虛擬主機，可縮減掉主機安裝作業系統與公文交換系統的大部分時間，但對於交換系統之參數，以及主機模組間的關聯設定，也應該提供能夠自動佈署設定之機制。因此，整合虛擬主機建立啟用 API（Virtual Machine Provision Application Programming Interface）以及套餐組合建立啟用 API（Package Provision Application Programming Interface），將可達成系統建置部署時之自動設定處理功能，這樣更可簡化對統合交換中心之共用系統維運工作，讓維護多個統合交換中心，所產生大量公文交換虛擬主機，這樣複雜度高的共用系統更容易管理。

3. 虛擬主機內僅提供特定路徑可寫入權限

在虛擬化平台運算節點（Compute Node）對啟用之虛擬主機影像檔（Virtual Machine Image）設定成唯讀模式，就能將公文交換模組之運行環境變成無法寫入的狀況，所以對系統需要暫存寫入的路徑，可透過虛擬機開機啟動過程所建立出記憶體磁碟（RAM Disk）（註 8）的技術來解決，對於公文交換檔案資料所存放路徑，則可採外掛虛擬磁碟（Virtual Volume Disk）或網路檔案磁碟（Network File System）（註 9）的技術來因應，如此可降低公文交換系統運行環境遭受入侵，被植入木馬或竄改公文交換模組程式檔案機會。當懷疑公文交換系統運行環境異常時，只需要重新開機啟動該虛擬主機，則能立刻還原成系統乾淨的初始狀態。對於公文交換檔案可存放之外掛虛擬磁碟或網路檔案磁碟，因專屬檔案資料存放區域（或主機），將來亦可快速整合各類第三方資安惡意檔案掃描工具，來提高這部份檔案資料類型之安全檢核等級。

4. 虛擬主機僅安裝各交換模組所需最精簡套件

若將虛擬化平台所提供之精簡虛擬主機 Linux 樣版，已將 Linux 作業系統以最小化安裝並移除非必要之系統套件，因此再將每個運行環境只安裝單一公文交換模組，這樣就能讓虛擬主機變為最精簡最單純的公文交換模組運行環境，如此除提升該公文交換模組在虛擬環境

運行之效能外，也能大幅降低系統漏洞的發生。

（二）公文電子交換全程加密

現行公文電子交換所傳送之公文皆為非密等公文，屬非機敏性資料，在交換系統自始以來都是以明碼方式處理（儲存 / 交換），以資訊安全風險評估檢視，亦是一項資產的弱點，為求嚴實公文電子交換系統整體安全強固性，擬規劃建議將電子公文以密文方式處理，杜絕傳輸過程洩漏之可能性。在技術問題方面，在於過去公文 DI 檔同時存放本文資訊及交換資訊，一旦加密即造成交換傳遞過程無法正常剖析，造成無法正常交換問題，另外加密後的簽章適法性也是需要考慮的問題。

建議運用信封檔封裝觀念處理公文電子交換，將公文本文及附件資訊與交換資訊分開，如此本文即可全程加密。現有統合交換中心系統已經初具此項功能，略作調整及強化即可使用。然而全程加密另需要其他所有公文交換廠商共同配合變更交換程式，以及文書與檔案電腦化作業規範配合調整，此為影響較大部分，後續可透過召開閘道會議來推動。

三、發展雲端公文交換系統

近年來雲端運算相關技術發展已趨成熟，運用雲端技術可以帶來許多實際效益，包括服務彈性與能量的提升、整體服務成本的下降、服務可靠度的提升、無處不在的服務環境等效益。在此技術趨勢下，發展公文雲端服務將是公文系統長期規劃的重要目標，可運用公文交換系統虛擬化集中的基礎架構，配合統合中心最適規模，實體主機仍座落於各統合中心，從各統合交換中心內部公文交換雲端化架構規劃發展出公文雲端化架構，如圖 6。

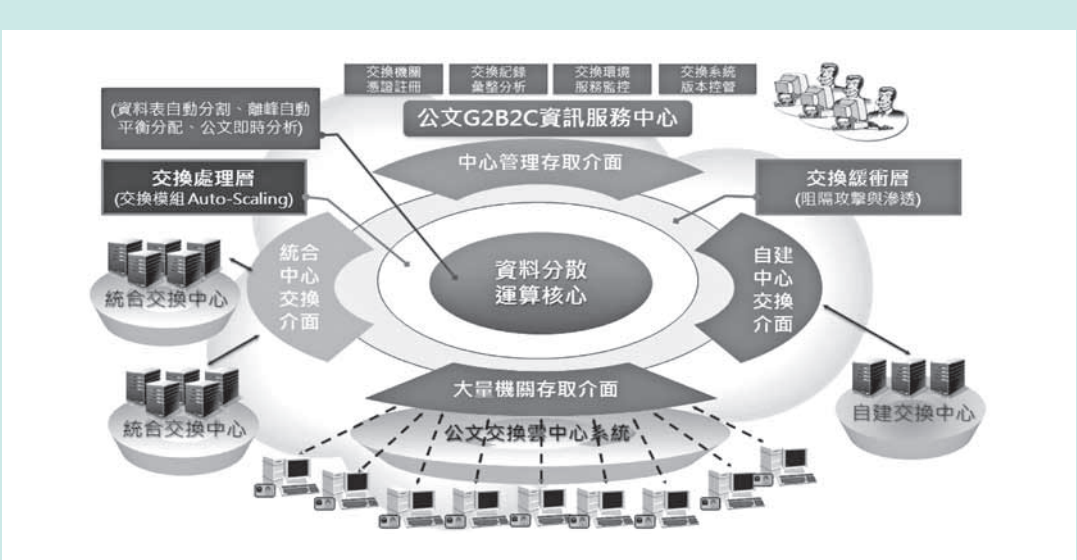

圖 6：公文電子交換雲端架構示意

資料來源：作者繪製

公文交換雲端化架構，著重於簡化公文交換架構，及強化安全管理增加緩衝層為核心防護機制，以阻隔攻擊與滲透，解決交換中心遭受入侵與滲透攻擊，所增加的緩衝層應該置放於動態記憶體虛擬磁碟區，暫存上傳之公文交換訊息檔，以及待下載之公文交換訊息檔，再配合專屬設計之公文檔案驗證機制，讓不合法的檔案無法正常寫入或被自動檢核程式剔除，當發現可疑異常檔時，也能透過重新開機方式快速恢復乾淨的環境，如此將可降低遭受滲透攻擊之風險。

此外，對交換服務的各個介面將區分出來，讓每一個介面功能單純化，降低可能出現的弱點風險，簡述如下：

（一）單向式上傳檔案介面（發文介面 / 發訊息介面）

將發文或訊息所上傳之檔案暫存於上傳緩衝層，並在此緩衝層整合或更換各類型資安檢核掃描工具，快速過濾出異常檔案，在進入交換層之前就將異常檔案剔除，並立即回應給傳遞端知道很可能該機關已經遭病毒感染的狀況。因該介面僅能上傳不能下載，異常檔案在未被判斷出來前也不可能被其他機關單位所下載。當交換層處理到該份公文或訊息時，會主動到上傳緩衝層讀取這份上傳檔案，如此可阻絕檔案主動由外傳送到交換層之途徑。

（二）單向式下載檔案介面（收文介面 / 收訊息介面）

交換層完成交換處理程序後，會將收文或訊息待下載之檔案暫存於下載緩衝層，並在此緩衝層整合或更換各類型資安檢核掃描工具，快速過濾出異常檔案，在收文端下載前就可將異常檔案剔除，並可立即回應給中心系統管理者知道，很可能交換層哪臺主機已經有遭病毒感染的狀況。因該介面僅能下載不能上傳，異常檔案也不可能透過外部上傳進來被其他機關單位所下載。

（三）限制式傳遞串流介面（認證介面 / 收命令介面）

收發文系統與交換中心之身分認證與命令溝通，採用加密訊息串流處理，並於訊息串流內增加編碼與干擾訊息，提高滲透者對公文交換系統的入侵攻擊難度。此介面也不允許檔案上傳與下載，阻絕異常檔案上傳下載的可能性。

公文交換雲端化架構之發展除了提升系統架構之防駭設計外，透過 iServCloud 虛擬化整合將各統合交換中心整合，將形成一個強大的公文雲（Hybrid Cloud）資源池，大幅提高系統可用性及整體備援能力。

肆、結語

綜觀本研究提出之短、中、長期規劃項目，涵括公文電子交換系統短期之資訊安全強化作為，以及中期加強資安防禦縱深與公文生命週期長期發展之雲端服務規劃，符合全球雲端化的趨勢及下一階段電子化政府階段發展需求，綜整如下：

一、短期強化系統資訊安全管理

強化措施以提升資安管理防護控制措施，防止駭客偽冒攻擊機會，強化措施包含作業系統更新、應用軟體更新以及程式碼混淆化與 API 參數混淆化等，將有效降低公文交換系統在作業系統與應用軟體層的資安風險。

二、中期虛擬化集中管理與資料全程加密保護機制

公文電子交換系統交換層及終端層最適規模虛擬集中化，搭配 iServCloud 雲端資源管理系統，將有效提升公文交換系統主機維運效率，以樣版及統合中心組合套餐方式，實踐虛擬集中快速管理維護機制。作業系統精簡與公文全程加密，分別針對系統層與資料層強化防護，強化資安防禦縱深，確保系統傳輸資料安全，具體落實滴水不漏的資安要求。

三、長期規劃邁向雲端環境遷移

運用全新的雲端技術架構發展出未來的公文雲為長期規劃建議，透過雲端技術進一步將公文製作、管理、交換與檔管整合，建立完整公文生命週期的雲端服務，建立電子化政府旗艦級雲端服務典範。

註釋

註 1：行政院，《公文電子交換推廣計畫》（民 89 年 2 月 3 日），行政院臺 89 秘字第 03378 號函。

註 2："Advanced persistent threat, APT," *Wikipedia Website,*〈http://en.wikipedia.org/wiki/Advanced_persistent_threat〉（7 Mar. 2014）.

註 3：行政院，《文書及檔案管理電腦化作業規範（99 年 12 月修正版）》（臺北市：行政院，民 99 年 12 月）：頁 5。

註 4：國家發展委員會檔案管理局公文 e 網通網站，〈公文統合交換中心（eCenter）〉。〈http://www.good.nat.gov.tw/〉（10 Mar. 2014）.

註 5："SourceGuardian," *SourceGuardia Website,*〈http://www.sourceguardian.com/〉（10 Mar. 2014）.

註 6："Auto-Scaling," *AmazonWebsit,*〈http://aws.amazon.com/autoscaling//〉（10 Mar. 2014）.

註 7：經濟部雲端開發測試平台，<iServCloud〉。〈http://www.cloudopenlab.org.tw/content4.do/〉（10 Mar. 2014）.

註 8："RAM Disk," *Wikipedia Website,*〈http://zh.wikipedia.org/wiki/RAM_disk〉（10 Mar. 2014）.

註 9："Network File System," *Wikipedia Website,*〈http://en.wikipedia.org/wiki/Network_File_System〉（10 Mar. 2014）.