FUJIFILM
Value from Innovation

FUJIFILM Business Innovation
多功能事務機
資訊安全白皮書

2023年 12 月 1 日_2.3 版

FUJIFILM Business Innovation Taiwan Co., Ltd.

目 錄

簡介

多功能事務機的資訊安全措施

FUJIFILM Business Innovation 在開發階段持續透過擴充多功能事務機（Multifunction Printer, MFP）的各式安全功能、加密演算法，以強化資訊安全並確保品質，解決客戶的資安難題。

近年來，不少資安攻擊事件開始利用產品供應鏈的弱點趁機而入，像是將惡意程式注入產品、設備或軟體等等，此類的網路攻擊事件不斷增加；有鑑於此，FUJIFILM Business Innovation率先致力於供應鏈的資訊安全，確保我們的產品及服務在整個生命週期中的安全完整性，協助企業有效防範無所不在的資安威脅。

至始至終，FUJIFILM Business Innovation了解在追求創新和升級產品功能的同時，提升資訊安全的重要性。因此，為了確保多功能事務機的安全可靠性，FUJIFILM Business Innovation 獲得「ISO/IEC 15408」認證，該認證為多功能事務機設計與操作相關的資訊科技安全國際標準，並獲得美國第三方審查機構 Keypoint Intelligence 的安全驗證（BLI 安全標章－裝置滲透測試）。

2020 年 9 月，FUJIFILM Business Innovation 成為日本首家獲得 JaSRO AAAis 最高等級評比，該評比標準為評估符合美國聯邦政府高規資安規範 NIST SP 800-171 （NIST Special Publication 800-171 rev.1）之程度。此外，2022 年12 月，我們也成為日本第一家獲得符合 NIST SP800-171/172 各項安全標準之最高評級 AAA 的企業，表示 FUJIFILM Business Innovation 高度滿足 NIST SP800-172 規範，包含五大項網路安全措施：「識別」、「保護」、「檢測」、「回應」和「恢復」，以及 NIST SP800-171 規範。

此外，為了保護我們的產品及服務免於因產品供應鏈弱點所引發的網路資安攻擊，FUJIFILM Business Innovation 建置完善的資安保護流程，以確保整體產品生命週期的安全完整性。我們也獲得了ISO/IEC 20243 的自我評估認證，該認證為國際標準化的供應鏈安全相關規範。

FUJIFILM Business Innovation 採取進一步措施，在產品和應用服務中，採用尖端科技、高品質管理、快速反饋回應以及專業資安整合服務，以期為企業建造完善的資安環境，降低內外部資安風險。

*欲了解符合規範之產品相關資訊，請與銷售代表洽詢。

https://www.fujifilm.com/fbglobal/eng

本白皮書所陳述內容，皆以製作期間所收集的資訊為依據；本公司將持續加強和優化產品及服務，故白皮書的內容可能會隨時變更。

如欲取得本文件中描述之適用設備與功能的詳細資訊，歡迎與我們聯絡。

企業合規宣言

FUJIFILM Business Innovation 為辦公室多功能事務機製造商及提供各式辦公室解決方案整合服務，嚴謹遵循法規並以公平、誠信原則經營事業；此外，FUJIFILM Business Innovation 及其關係企業，一直以來致力於優化組織安全架構和相關措施，以確保公司內部主管及員工都能在各項業務行動中體現合規準則。

如需了解 FUJIFILM Business Innovation 企業倫理與合規宣言相關資訊，請查詢此連結：
https://holdings.fujifilm.com/en/sustainability/vision/compliance

在與客戶建立信賴關係的同時，FUJIFILM Business Innovation專業團隊亦致力於提升資訊安全層級，從客戶需求出發，站在客戶的角度思考、理解並解決問題，讓客戶安心地使用本公司的產品、服務和解決方案，並將其資訊資產安心地交付予我們。

FUJIFILM Business Innovation及其關係企業已取得第三方機構頒發之資訊安全相關認證，如欲了解詳細資訊，請查詢以下連結。

當然，FUJIFILM Business Innovation將持續加強資訊安全治理，成為客戶最佳的資安典範。
https://www.fujifilm.com/fbglobal/eng/company/public/i_security

多功能事務機之資安威脅與防護措施

以下狀況皆威脅辦公室多功能事務機與企業文件資訊安全：

1. 使用者未經授權的操作
2. 竊取和竄改傳輸資料
3. 未經授權存取管理功能
4. 竄改及未經授權重新寫入軟體
5. 竄改稽核記錄
6. 洩漏儲存在設備內的文件資料（在租賃期滿歸還或報廢裝置時）
7. 因系統管理員或使用者的疏忽而造成資料洩漏

FUJIFILM Business Innovation 的辦公室多功能事務機針對表 1 至表 7 所列之可能資安風險，提供最佳的防護措施。

表 1：辦公室多功能事務機的資安威脅與防護措施

辦公室設備的資安威脅	FUJIFILM Business Innovation 採取資安防護措施
1. 使用者未經授權的操作 當使用者操作設備時，如未確實執行文件保護措施，如資料存取權限管控、設備操作管控等，將可能造成文件資料或儲存於設備中的相關資料遭外洩或竄改。	**A) 使用者身份驗證和存取權限** • **使用者身份驗證** 確認並管理個別使用者。 • **限制操作設備權限** 管理每一位使用者操作設備之權限。 • **自動登出** 避免未登入的使用者，在未經授權情況下使用設備。 • **機密列印／個人列印** 確保設備在無他人使用下，才可執行文件列印，以避免機密文件暴露給第三方。 • **統一的使用者驗證與權限管控** 使用 ApeosWare Management Suite 2 全方位智慧商用整合解決方案，單一平台統一管理使用者、身份驗證與存取權限。 • **單一平台管控機密列印** 透過 ApeosWare Management Suite 2 全方位智慧商用整合解決方案，單一平台整合所有事務機、使用者身份驗證和認證機制，提供安全的列印環境，實現機密列印。

A) 使用者身份驗證和存取權限

認證功能

透過認證功能，可以防止未經授權的使用者操作或存取設備；亦可透過認證功能從完整的操作歷史紀錄中，了解使用者使用設備的情況。

IC 卡驗證

設備可彈性安裝 IC 卡座，即可輕鬆透過 IC 卡完成身份驗證。IC 卡座可串聯整合多種功能，包括管控輸出設備的權限存取，不僅能加強設備資安管理，同時實現更好的使用者體驗。

IC 卡座提供三款形式：內嵌式 IC 卡座、側邊工作檯專用內嵌式 IC 卡座、外接 IC 卡座。

遠端伺服器驗證

透過 Active Directory 或 LDAP* 伺服器登錄 IC 卡使用者資訊，即可在操作設備或印表機時，可藉由伺服器管理的使用者資訊進行身份驗證。

倘若使用者忘記帶 IC 卡，亦可以透過輸入使用者 ID 與密碼使用設備。對於使用 Active Directory 管理各種網路資源的客戶來說，可透過集中管理所有輸出設備，大幅節省時間和人力。

*：LDAP, Lightweight Directory Access Protocol，輕型目錄存取協定

功能存取權限管控

設備功能存取權限管控屬使用者身份驗證的一種，可限制、管控操作 MFP 的所有功能，如複印或傳真。為落實權限管控，僅提供系統管理員透過設備 UI 操作面板或 MFP 設定軟體進行設定。

提供三大面向權限管控：

1. **設備權限存取管控**

可管控 UI 操作面板之操作，如當 MFP 啟動時，UI 面板顯示要求登入之訊息。

2. **功能服務權限存取管控**

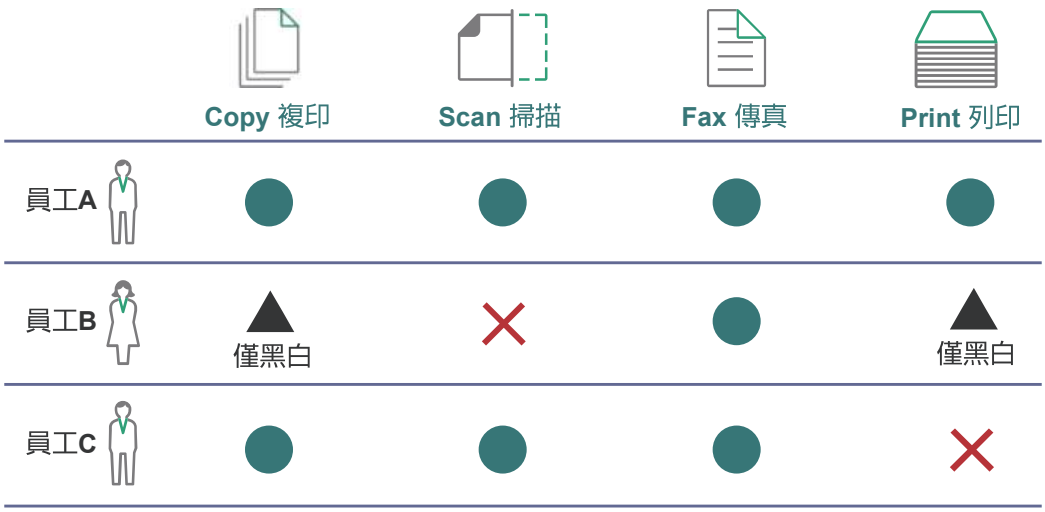
可管控以下功能服務，亦可將功能服務設定為隱藏模式：

- 複印
- 傳真／網路傳真
- 掃描至資料夾
- 掃描至PC
- 掃描至電子郵件
- 資料夾操作
- 執行項目之流程
- 從USB列印
- 外部存取
- 列印

3. **使用者權限存取管控**

可以依據每名使用者之需求設定功能存取、列印和複印的印量配額管控。系統管理員可透過設備 UI 操作面板或 MFP 設定軟體，依據各使用者之權限，設定複印和印量配額的限制。

當列印或複印量超過設定的張數時，使用者將無法繼續使用該功能。系統管理員可清除已計算的張數。



上圖：不同使用者權限存取管控

資料夾文件存取管控

為儲存在 MFP 中掃描或傳真文件的資料夾設定密碼以保護文件。亦可使用驗證模式識別使用者身份，以管控未經授權的使用者，避免其存取資料夾內的文件資料。

自動登出

自動登出功能可避免其他使用者以前一位使用者的身份登入、使用 MFP。當設備閒置一定時間，則會強制自動登出，並回到初始狀態。

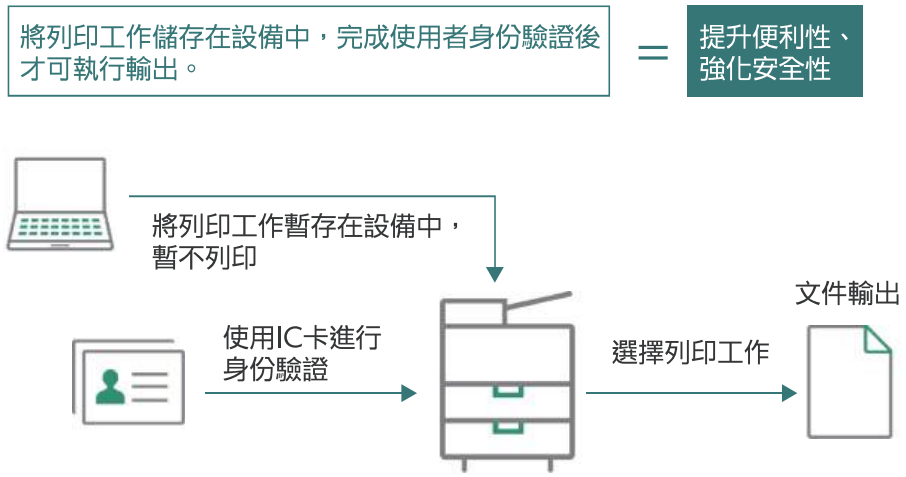
機密列印

機密列印功能可在使用者輸入密碼前，先將執行項目 (Job) 保留在設備中，以避免未經授權者檢視或存取文件。

可透過 Print Driver Customization Tool（免費使用），設定機密列印驅動程式的設定值。

個人列印

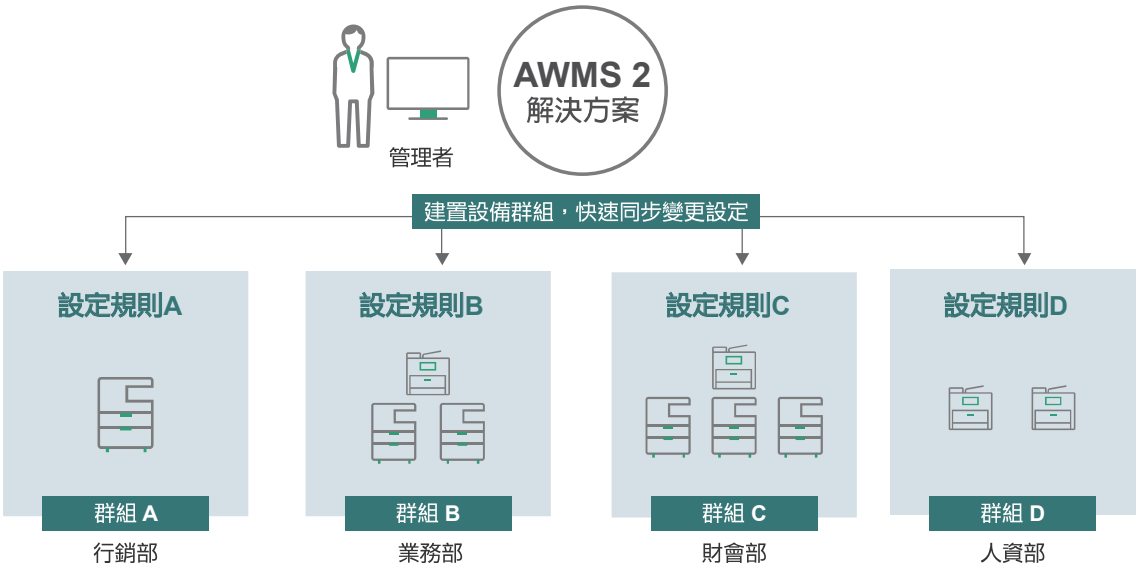
將列印工作保留在設備的儲存裝置中，完成身份驗證後，才可執行輸出；此功能可避免文件無人領取或錯誤輸出。此外，仍可變更列印設定，例如複印份數、雙面／單面、彩色／黑白（僅可將彩色改為黑白），以減少錯誤列印與浪費紙張，有助於降低 TCO 總體擁有成本。



* 須在驗證模式下操作。

統一的使用者驗證與權限控制

ApeosWare Management Suite 2 全方位智慧商用整合解決方案屬架設於伺服器的資安管理軟體，透過單一平台集中管理多台設備、多名使用者身份驗證和存取權限，大幅減輕系統管理員工作負擔。



單一平台管控機密列印

ApeosWare Management Suite 2 全方位智慧商用整合解決方案亦可提供在執行驗證後，安全執行列印工作的功能；此功能可以避免無人領取設備上的列印文件或錯誤輸出。透過伺服器管理，系統管理員可同時管理多台設備設定，依據功能類別設置群組，同步更新設備設定。

表 2：辦公室多功能事務機的資安威脅與防護措施

辦公室設備的資安威脅	FUJIFILM Business Innovation 採取資安防護措施
2. 傳輸通訊遭竊聽竊取或資料遭竄改 用來操作設備（列印、掃描等）的 PC 或檔案伺服器，在網路裝置間傳輸資料時，可能會發生資料遭竊聽竊取或竄改等事件。	**B) 加密通訊與資料保護** • **SSL/TLS 與 IPSec** 將 PC／檔案伺服器與 MFP 之間的資料傳輸安全加密，以保護資訊。 • **SMB v3、SFTP** 將 PC／檔案伺服器與 MFP 之間的資料傳輸安全加密，以保護資訊。 • **FIPS 140-2** 啟用 FIPS 140-2 聯邦資訊處理標準，以符合美國聯邦密碼模組安全性要求。 • **數位憑證確認** 確認憑證鏈結、憑證註銷與有效期限。可將由管理員手動更新的憑證（包含新發放的憑證）和相關更新的設定進行自動化更新。 • **關閉未使用的網路協定或連接埠** 避免未經授權存取和外洩資料。 • **加密掃描文件** 使用密碼／公開金鑰以避免資料外洩。 • **直接列印加密文件** 可將加密後的 DocuWorks 檔案和 PDF 檔案解密後直接列印。 • **電子郵件的加密與數位簽章** 降低電子郵件在傳輸過程中，資料被竊聽竊取或竄改。 • **避免不同傳輸管道之間的資料洩漏** 避免經由傳真線路、第二乙太網路介面、無線網路、USB 連接埠或 USB 記憶體中的惡意程式，攻擊 MFP 或內部網路。

B) 加密通訊與資料保護

伺服器或用戶端 PC 與 MFP 之間的加密通訊（SSL / TLS / IPSec）

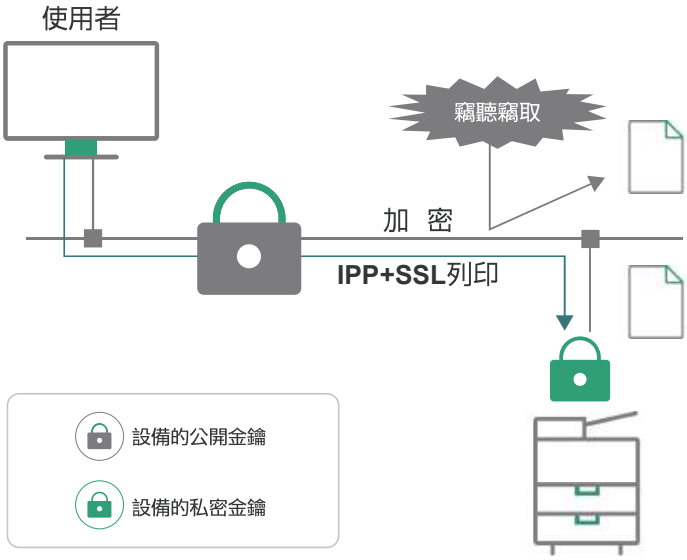
您可透過加密通訊傳輸，來防止他人試圖在未經授權的狀況下存取網路，避免設備與伺服器或客戶端 PC 傳輸資料過程，資料遭竊取、竄改或外洩。

以下為可被加密之傳輸通訊：預設為 TLS 1.2*。亦可變更設定為 TLS1.3。

*：TLS 1.0 / TLS 1.1 / TLS 1.3 預設為停用。

• 使用 IPP 連接埠列印工作（列印）

將傳輸列印資料的 IPP（網際網路列印協定）通訊路徑進行加密，以防止竊取驗證資訊和列印資料。

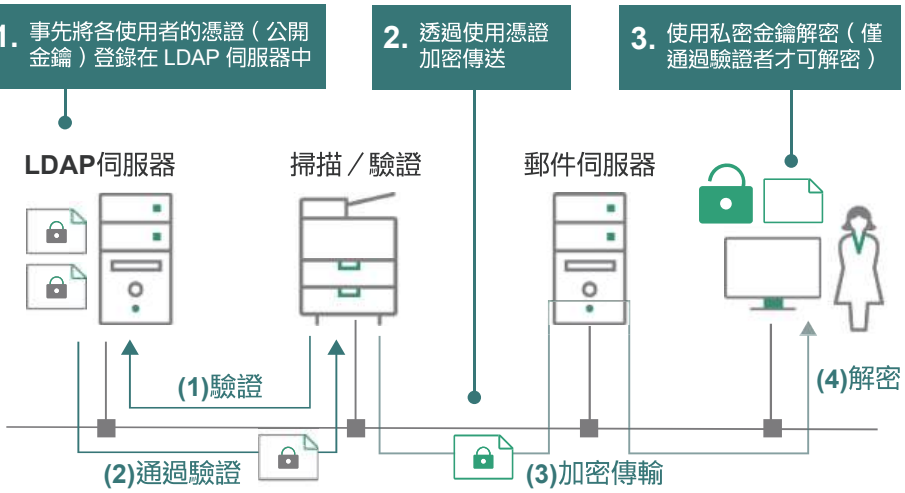


• 採用 HTTP 安全傳輸協定

從您的 PC 存取 MFP 上的網路服務，或從 MFP 存取外部伺服器時，請使用安全的 HTTP 通訊。

• 採用 **LDAP** 伺服器傳輸通訊（搜尋通訊簿／驗證）

透過 LDAP 伺服器加密通訊路徑中所傳輸的資料，避免驗證資料和通訊簿裡的資料遭竊聽竊取。



• 採用 **SMTP** 伺服器的傳輸通訊（電子郵件）

透過 SMTP（電子郵件傳輸）伺服器加密通訊路徑中所傳輸的資料，避免驗證資料和通訊簿裡的資料遭竊聽竊取。

• 採用 **POP** 伺服器的傳輸通訊（電子郵件）

透過 POP（電子郵件接收）伺服器加密通訊路徑中所傳輸的資料，避免驗證資料和通訊簿裡的資料遭竊聽竊取。

• 採用 **SFTP** 的通訊（掃描／檔案傳輸）

在工作流程中，透過 FTP 將資料傳送至伺服器時，使用 Secure Shell 方法執行通訊路徑加密／驗證，避免驗證資料遭竊聽竊取。

• 採用 **SMB** 的傳輸通訊（掃描／檔案傳輸）

在 SMB v3 中，新增通訊加密功能，確保將檔案安全地傳送至目的地。

• 透過 IPsec 加密 IP 傳輸通訊

您可以避免在配置IPsec連線的設備間，以IP資料封包為單位進行竄改與竊聽竊取。在使用憑證的客戶通訊中，SSL 伺服器驗證與 IPSec PKI 驗證可以防止詐騙。

• 透過 IEEE 802.1x 驗證進行網路裝置驗證

屬於一種驗證標準；當設備在網路上相互連接時，用於規定連接至網路之裝置連線的驗證標準。由於其支援 IEEE 802.1x 驗證，因此可以將 MFP 安全地連接至受連線裝置限制的網路。

FIPS 140 標準

FIPS 140（聯邦資訊處理標準）是指具體指明與密碼模組之安全性要求有關的美國聯邦標準。將 FIPS140-2 憑證模式設定至 [啟用]，即可允許使用符合 FIPS 140 的模組執行操作。

數位憑證的驗證

憑證的驗證是確認通訊中使用之憑證的功能，例如憑證鏈結、註銷確認及憑證的有效期限。可使用信賴起點憑證管理功能，執行可靠的驗證與憑證管理。

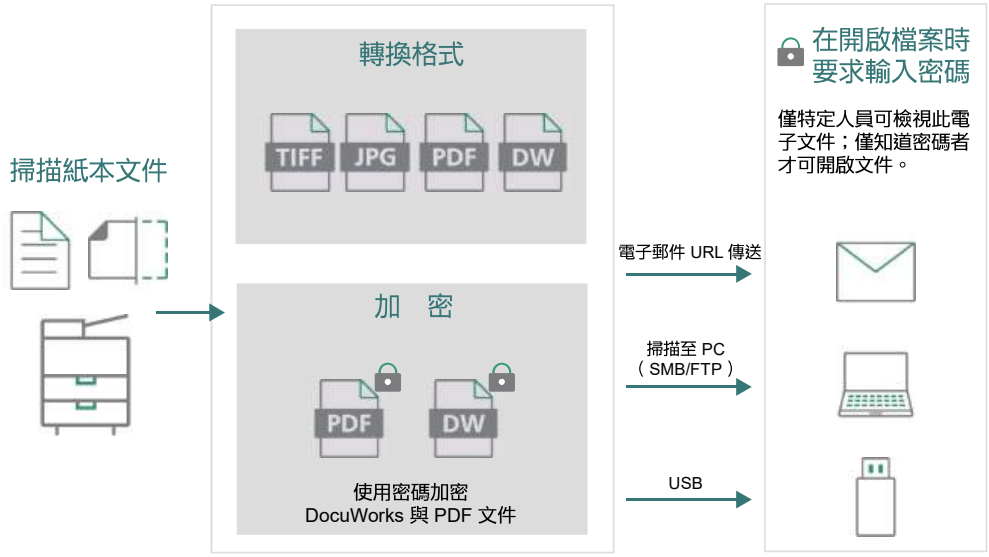
支援 Windows Server 之網路裝置登記服務（Network Device Enrollment Service，NDES）提供的自動憑證派送功能。可以使用 SCEP（簡易憑證註冊協定：Simple Certificate Enrollment Protocol），將由管理員手動執行的憑證更新（包括新發放的憑證）和相關設定更新自動化。

*欲了解符合規範之產品相關資訊，請與銷售代表洽詢。

https://www.fujifilm.com/fbglobal/eng

使用密碼為掃描文件加密

透過此功能，在將掃描文件儲存至 PC、或藉由電子郵件傳送掃描文件時，不僅能將文件轉換成 DocuWorks 文件或 PDF 檔案，且能使用密碼進行「文件加密」。同時亦可支援應用程式的安全功能，例如列印與編輯限制，當然還可以設定以密碼來開啟檔案。此功能可減少掃描文件的資料外洩與竄改風險。



附註：加密的 DocuWorks 或 PDF 檔案，需使用 DocuWorks Viewer Light 或 Acrobat Reader / Adobe Reader 開啟。無法以較舊的版本開啟新版文件，因此請使用最新版本的 DocuWorks Viewer Light 與 Acrobat Reader。

掃描文件的數位簽章與公開金鑰加密

將憑證與私密金鑰輸入 MFP，即可在傳送 DocuWorks、PDF 或 XML 文件規格（XPS）格式的掃描文件時，使用數位簽章功能，並允許偵測第三方竄改的資料。此外，由於 DocuWorks 文件可以使用 PKI 加密，因此能擁有比密碼加密強度更高的安全性，並可建立僅允許特定使用者存取的文件。

* 僅 ApeosPort 及 Apeos 機型支援此功能。

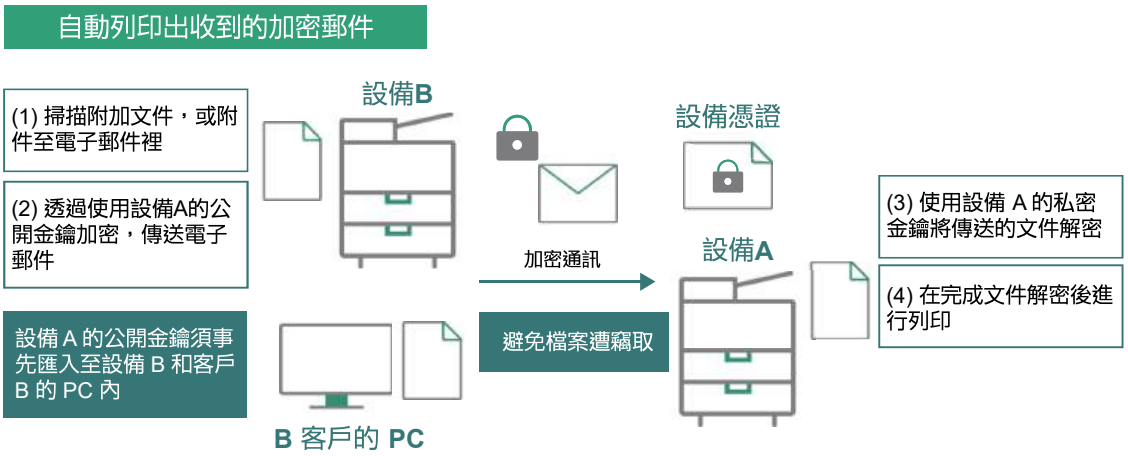
直接列印加密文件

使用事先登錄在 MFP 的密碼，即可解密並直接列印儲存在 USB、Working Folder 中的加密 DocuWorks 與 PDF 檔案。此外，也可以支援使用 Contents Bridge 公用程式，同時傳送含密碼的 DocuWorks 或 PDF 檔案。

電子郵件加密與數位簽章

電子郵件加密（S/MIME）：電子郵件（包括附加文件）是以使用者的數位憑證加密，因此僅有收件者可以開啟。此方式可以減少在電子郵件傳送過程中，資料遭竊聽竊取和洩漏的風險。

電子郵件的數位簽章（S/MIME）：在傳送電子郵件（包括附加文件）時，使用MFP的數位憑證內附加使用者的數位簽章。此方式可以減少電子郵件傳送過程中遭竄改的風險，且作為寄件人的客觀憑證，讓收件者能安心使用。

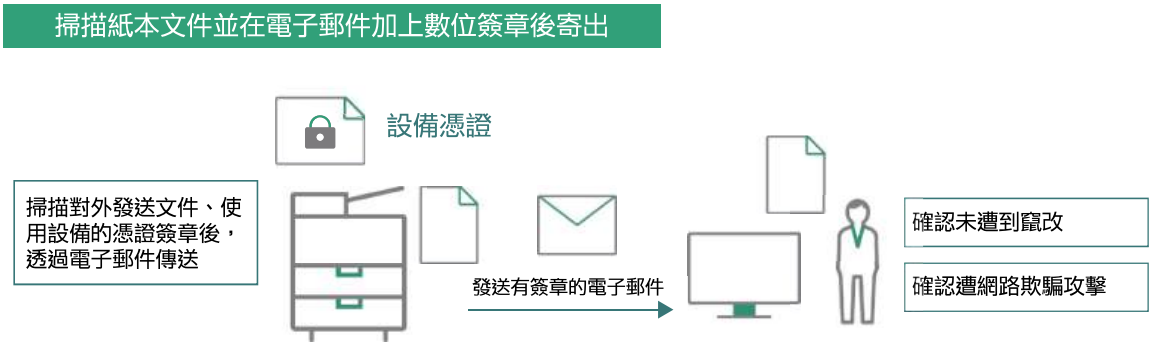


防止經由傳真線路的資安攻擊、資料外洩和竊聽竊取

經由傳真線路（電話線路）存取的安全防護，採用僅接受傳真協定通訊進行安全把關。如此一來，傳真的資料若含有惡意軟體，就不會危害到 MFP 作業，也不會執行未經授權的命令。

接收的所有資料，皆是使用傳真圖像格式的資料進行處理。若有不符合傳真協定標準的變形資料，將會視為圖像資料錯誤進行處理，例如解碼錯誤。

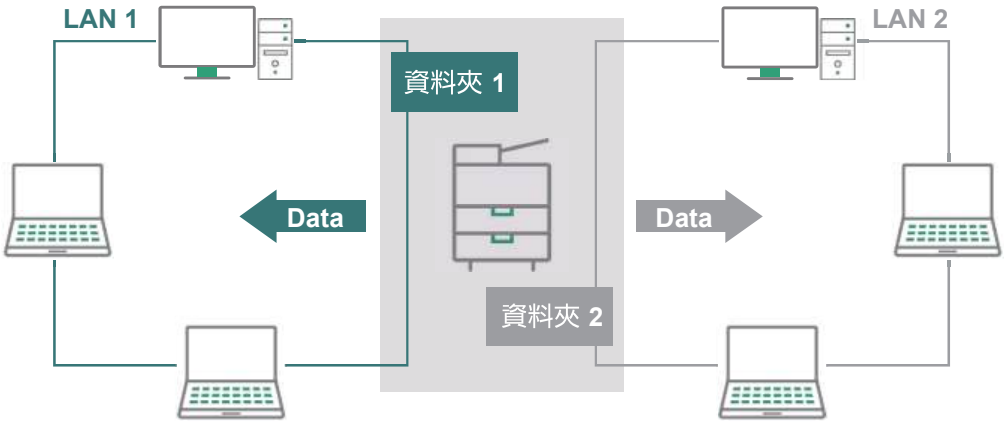
儲存在 MFP 資料夾的圖像和原始文件，可透過遠端站台以通訊的方式擷取；然而，倘若對 MFP 資料夾執行嚴格的密碼管控，即不會發生未經授權的資料擷取（洩漏）事件。



防止經由第二乙太網路介面的資安攻擊、資料外洩和竊聽竊取

第二乙太網路卡（選購）與主要乙太網路（標配）是各自建立通訊（TCP/IP）。由於此功能已停用，因此 MFP 將不會在兩個網路介面之間執行路由通訊（TCP/IP），亦無法透過 MFP 的功能在兩個網路間存取。

網路存取限制可以附加在 MFP 資料夾上。針對各 MFP 資料夾，可以將來自網路的顯示／文件儲存／傳輸至 MFP 資料夾的文件，限定在主要乙太網路或第二乙太網路。因此，可以避免因為來自其他網路之未授權存取，而造成 MFP 資料夾內之文件的資訊外洩。同時，必須管理好 MFP 資料夾的密碼。



第二乙太網路介面允許使用下列掃描功能：

- 使用掃描至資料夾，透過 Internet Services 擷取文件
- 從 MFP 資料夾開始工作流程（SMB 傳送）
- AirPrint 掃描

與 MFP 資料夾有關之功能可受到網路存取限制的保護。在進行 AirPrint 掃描時，僅有從第二乙太網路接收到掃描指示，才會傳輸至第二乙太網路端。因此，可以避免未經授權使用第二乙太網路而造成資訊外洩。

防止經由無線區域網路（**Wi-Fi**）埠的資安攻擊、資料外洩和竊聽竊取

選購的無線區域網路轉換器是連接有線區域網路纜線的無線終端機。無線區域網路套件、無線套件和無線套件 2 是在連接至 MFP 時，執行無線區域網路通訊的無線終端機。

這些無線終端機支援稱為 KRACKs 的 WPA / WPA2 漏洞對策。無線區域網路套件 2 支援 Wi-Fi Alliance 於 2018 年 6 月制定的 WPA3-SAE，讓使用者可以安全地使用設備。

此外，由於這些無線終端機不具備路由功能，無法在各個網路介面（TCP/IP）之間執行通訊。

存取 MFP 資料夾以及未經授權存取的反制措施，皆與第二乙太網路相同。因此，可以避免未經授權使用無線終端機導致的資訊外洩。

防止經由 **USB** 連接埠的資安攻擊、資料外洩和竊聽竊取

透過 USB 連接埠輸入列印工作時的資料，是視為印表機工作語言（PJL）與圖像資料進行處理。若接收到 PJL 與圖像資料以外的資料時，將會因為發生工作錯誤而暫停工作。

此外，在此情況下也不會執行轉接功能，以致無法與通訊線路建立連線，包括來自 USB 連接埠的網路與傳真線路。

防止經由 **USB** 隨身碟中感染病毒之檔案的資安攻擊、資料外洩和竊聽竊取

基於以下原因，在使用 USB 隨身碟執行掃描與列印工作時，連接至 MFP 的網路 MFP 與 PC 都不會有病毒。

1. 在執行掃描工作時，將不會嘗試存取 USB 隨身碟中的檔案。
   因此，即使 USB 隨身碟中的檔案遭到病毒感染，也不會感染 MFP。

2. 在執行列印工作時，是將 USB 隨身碟中的檔案當作圖像資料處理。
   若檔案遭到病毒感染時，將會因為檔案不符合圖像資料格式而產生圖像處理錯誤，導致列印工作暫停。將不會自動執行惡意程式。

3. 如上所述，由於 MFP 不會受到病毒感染，因此網路上的 PC 也不會經由 MFP 遭到感染。

4. 不會執行直接從 USB 隨身碟連接至網路 PC 的通訊方法。

表 3：辦公室多功能事務機的資安威脅與防護措施

辦公室設備的資安威脅	FUJIFILM Business Innovation 採取資安防護措施
3. 未經授權存取「系統管理功能」 若用於識別授權使用者身份驗證的功能，無法為待處理的文件資料和管理設備的使用者資訊，依照規定（資訊安全準則）執行身份驗證，將會有未經授權操作的狀況發生。	**C) 保護「系統管理功能」** • **系統管理員的密碼** 在使用預設值操作時，將顯示警告訊息，提醒您更改密碼。 • **帳戶鎖定** 在管理員連續登入失敗時，將執行帳戶鎖定。 • **客服工程師操作限制功能** 避免因 MFP 設定變更而遭受安全攻擊。 • **集中管理使用者設定檔** ApeosWare Management Suite 2 全方位智慧商用整合解決方案可根據設備的安裝地點或企業據點進行存取管控。 • **依據企業位置或安裝地點，集中控制使用者權限** ApeosWare Management Suite 2 可依據設備單位或安裝地點的配置，進行管控使用者存取權限。

C) 保護「系統管理功能」

針對預設系統管理員 ID 與密碼的安全警示訊息

為了能在使用設備時，擁有更高的安全性，當系統管理員在系統管理員模式下，以預設的系統管理員 ID 及密碼登入系統時，將顯示提醒變更密碼的警示訊息。

管理員連續登入失敗將鎖定帳戶

此功能為當系統管理員驗證失敗後，進行系統安全保護功能，並在登入系統管理員模式之前執行。若系統管理員在超過預定的登入次數後，仍無法登入時，在重新啟動設備之前，將會禁止再次嘗試登入。

客服工程師操作限制

系統管理員可透過配置設定，限制僅由具備特別權限的客服工程師執行操作。可設定為必須使用密碼才能登入客服工程師模式，以避免他人冒充客服工程師進行未經授權存取設備。

針對組織部門或設備安裝位置的集中權限管控

ApeosWare Management Suite 2 全方位智慧商用整合解決方案可將使用者設定檔集中管理，以進行權限管控，且可以根據以使用者群組為單位的組織部門或以設備群組為單位，套用使用者設定檔。使用者設定檔亦可透過安全層級或 ApeosWare Management Suite 2 提供的服務，設定存取權限。

此外，也可以在安裝 ApeosWare Management Suite 2 Mobile 應用程式的行動裝置及其他裝置上，使用存取設定檔。

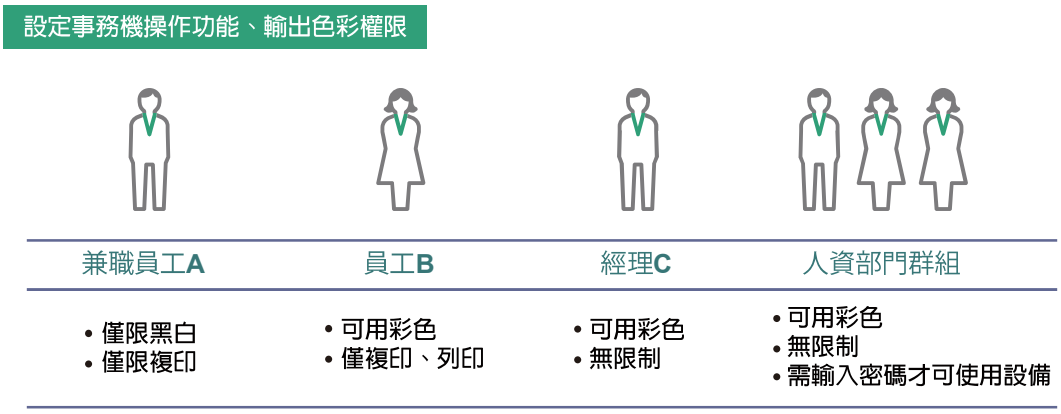


表 4：辦公室多功能事務機的資安威脅與防護措施

辦公室設備的資安威脅	FUJIFILM Business Innovation 採取資安防護措施
4. 軟體遭竄改 倘若軟體遭到竄改，則無法落實安全準則之規範。 由於缺乏明確的機制驗證軟體是否符合最新版本的情況下，使用者可能會上傳未經授權的軟體或系統檔案，將導致加密功能失去功用，或安裝非法程式，進而影響設備及文件檔案之安全。	**D) MFP 軟體的安全完整性** • **偵測漏洞、更新軟體** 設備主動定期偵測韌體是否遭竄改，同時定期更新軟體至最新版本。 • **更新軟體並確保安全完整性** 避免未經授權的控制軟體與附加應用程式安裝在 MFP 上。 • **確保設備啟動時的安全完整性** 避免設備啟動時，執行未經授權的控制軟體。 • **確保操作期間的安全完整性** 根據白名單進行設備操作管控，以避免未經授權的操作。

D) MFP 軟體的安全完整性

定期掃描漏洞和更新軟體

定期透過弱點掃描以防止設備遭受惡意攻擊，並在更新設備軟體的同時，採取防範措施。

為確保設備之安全，FUJIFILM Business Innovation 在開發新產品階段，透過多個弱點掃描進行漏洞驗證；當發現漏洞時，將即刻執行安全修補程式等措施。在弱點掃描面向，由於每天都會更新漏洞資訊和資料庫，因此，可確保當執行偵測漏洞，皆以最新的資料庫進行弱掃驗證。

此外，將定期驗證和支援現有產品，並視情況執行軟體更新。此外，像是禁止安裝 SSH 等遠端連線的功能，可避免從外部執行未經授權的設備操作。

更新軟體並確保安全完整性

當更新設備的控制器軟體或附加應用程式 (Add-on application) 時，透過數位簽章驗證功能，可避免該軟體或程式遭改寫成未經授權軟體或程式。當偵測到竄改，自動將竄改事件記錄在稽核記錄中，並暫時停止啟動 MFP。

當安全性層級提升後，可透過網路停用軟體更新功能，避免經由網路進行未經授權更新軟體。

此外，無法經由傳真線路更新軟體（韌體）。

確保設備啟動時的安全完整性（設備啟動自動偵測竄改功能）

在啟動 MFP 時，自動驗證設備控制器軟體的電子簽章，若偵測到偽造，則會從 Golden Master（復原）自動還原初始設定！使用安全穩固的端點設備，才能真正落實資安防護。

確保操作期間的安全完整性（使用白名單防止操作期間遭竄改）

根據白名單進行設備操作管控，避免執行可疑的應用程式，以保護一般應用程式和防止未經授權的操作；同時，可使用 IP 位址過濾功能，以管控網路通訊的位址，以封鎖在未預期內之存取。

表 5：辦公室多功能事務機的資安威脅與防護措施

辦公室設備的資安威脅	FUJIFILM Business Innovation 採取資安防護措施
5. 竄改稽核記錄 若未保護、追蹤未經授權的稽核記錄，則該記錄可能會遭到竄改或刪除。	**E) 稽核記錄、保護記錄以及其他記錄的相關功能** • **稽核紀錄** 透過查看稽核紀錄，以追蹤設備的操作項目和歷程，如設備的啟動／停止、設定變更或工作進度狀態等等。 • **保護稽核記錄** 可禁止未經授權人員檢視、編輯及刪除稽核記錄。 • **整合 SIEM 稽核記錄** 透過 Syslog 通訊協定，將 MFP 的稽核記錄與 SIEM 安全性資訊事件管理系統整合，即可集中管理和分析稽核記錄。 • **限制執行項目資訊顯示** 亦可將其他使用者的執行紀錄設定為隱藏。 • **列印文件專屬識別碼「UUID」** 若有資料洩漏狀況發生，可透過 UUID 識別碼，追蹤特定使用者。 • **執行項目異動的可追蹤性** 可透過 ApeosWare Management Suite 2 全方位智慧商用整合解決方案與 ApeosWare Image Log Management 文件影像備份管理系統，進行追蹤使用者的工作執行項目。

E) 稽核記錄、保護記錄以及其他記錄的相關功能

稽核記錄

您可以透過網頁瀏覽器，從 Internet Services 下載「稽核記錄」。此記錄會顯示出詳細的歷史資料，包括系統資料變更、使用者登入／登出、電源開啟／關閉，以及工作進度狀態，以協助改善系統管理，並追蹤非預期變更的歷程。稽核記錄也有助於提升使用者的安全意識。

稽核記錄會記錄與以下設備相關之操作資訊：

- 狀態變更：設備的電源開啟／關閉、使用者啟動／結束操作的時間等等。
- 登入狀態：使用者登入／登出、系統管理員的驗證鎖定等
- 工作狀態：工作完成等。
- 設定變更：時間設定、安全設定變更、使用者資訊設定、開啟資料夾等等。
- 資料變更：憑證變更、通訊簿變更等
- 配置變更：儲存設備更換、ROM 版本變更等。
- 通訊結果：通訊錯誤等。

保護稽核記錄

稽核紀錄不可因任何目的，被第三方檢視／編輯／刪除紀錄。

以下為稽核紀錄的保護措施：

- 沒有操作介面得以編輯／刪除稽核記錄。
- 僅管理員有權存取。必須使用 SSL / TLS 加密通訊，才可下載稽核記錄。
- 同時，可使用儲存裝置加密功能保護稽核記錄，即使從 MFP 更換或移除儲存裝置，仍可以持續提供保護。

整合 **SIEM** 稽核紀錄

透過 Syslog[*1] 通訊協定，將 MFP 的稽核紀錄傳送至外部 SIEM[*2] 系統，以利集中管理、分析 MFP 的稽核紀錄，確保提早偵測並分析資安威脅。

*1：Syslog 是屬於標準通訊協定，可以透過IP網路傳送時間序列記錄。

*2：SIEM（Security Information and Event Management：安全資訊與事件管理）是屬於安全性軟體／服務，可以集中儲存和管理設備和軟體操作狀態的記錄，以及迅速偵測與分析引起安全性威脅的事件。

限制執行項目資訊顯示

此功能可藉由設定來限制資訊的顯示，例如讓未驗證使用者無法檢視執行中、等候中或完成後的執行項目（Job）資訊。

同時可以針對驗證使用者設定顯示限制，確保他們僅能檢視自己的執行項目，無法檢視其他使用者的執行項目（Job）。於此情形下，不僅能保護隱私，亦能避免資料外洩。

列印工作記錄識別碼 **UUID**

此功能可在複印、列印或傳真文件上，列印「通用唯一識別碼（UUID）」的文件專屬識別碼。可透過此識別碼搜尋或辨別特定文件。識別碼會顯示出處理文件的「時間」、「執行者」與「方式」資訊以供確認，因此當發生資料洩漏時，可藉由此資訊找出該文件的使用者。

執行項目異動的可追溯性

ApeosWare Management Suite 2 全方位智慧商用整合解決方案，可收集執行異動的執行工作項目資訊（Job），並允許系統管理員從報表追蹤處理過程。

同時，亦可使用伺服器式的軟體，追蹤執行項目的文件影像，例如 **ApeosWare Image Log Management 文件影像備份管理系統**，將文件的影像資料和使用者資訊儲存在裝置中，或使用 UUID 功能。ApeosWare Image Log Management 也可以監控影像紀錄；當使用者違反安全設定規則時，系統將自動通知系統管理員進行外洩追蹤。

表 6：辦公室多功能事務機的資安威脅與防護措施

辦公室設備的資安威脅	FUJIFILM Business Innovation 採取資安防護措施
6. 儲存在設備內的文件資料外洩（當設備租賃期滿歸還或報廢設備時） 列印、複印或傳真的文件資料會暫時或永久儲存在儲存裝置中，但當設備租賃期滿歸還、或設備報廢時，如未妥善處理儲存裝置，可能導致資料外洩。儘管表面顯示無法存取此文件資料，但倘若無實際刪除，亦可還原儲存在裝置裡的資料。	**F) 保護儲存在裝置內的文件資料** • **為儲存裝置裡的資料加密** 避免第三方解析、存取從 MFP 移除的儲存裝置。 • **批次刪除 MFP 儲存空間裡的資料** 當 MFP 租賃期滿移轉至另一個單位使用時，或報廢處理時，可透過批次刪除設定和刪除文件資訊，以確保儲存在 MFP 中的資料不會外洩。

F) 保護儲存在設備內的文件資料

為儲存裝置裡的資料加密*1

當資料寫入儲存裝置後，採用進階的加密*2 方法保護資料，以避免儲存的資料遭未經授權存取。此外，亦能在使用 MFP 時，避免資料遭到第三方解析。

此密碼編譯金鑰不會儲存在非揮發性記憶體（non-volatile memory）中，而是在每一次 MFP 開機時產生並提供使用。因此，即使從儲存裝置移除非揮發性記憶體，此金鑰亦無外洩之疑慮。此外，在部份多功能事務機機型中，為儲存裝置資料加密的加密金鑰，亦會使用獨立於儲存裝置之安全性晶片（TPM：可信任平台模組）內部的根加密金鑰進一步加密。由於 TPM 可防止遭竄改，使根加密金鑰受到安全保護，無法從外部讀取。

*1 HDD 與 SSD。*2 AES-256

如需了解各 MFP 機型之相關加密詳細資訊，請至以下網站的「Security Target」查詢

https://www.fujifilm.com/fbglobal/eng　　*欲了解符合規範之產品相關資訊，請與銷售代表洽詢。

覆蓋儲存在 HDD 硬碟裡的資料

覆蓋硬碟功能*可清除儲存在HDD硬碟裡的暫存資料，防止經由影印、傳真、掃描和列印的內容外洩到設備之外。此功能需要額外選購硬碟覆寫組件。

*覆蓋硬碟功能，可選擇覆蓋次數：一次（以二進制零覆蓋資料）或三次（以二進制零、隨機數覆寫數據，然後進行驗證）。

批次刪除儲存在 **MFP** 中的資料*1

當 MFP 要移轉至另一個單位使用或報廢處理時，管理員可刪除儲存在 MFP 中的記錄、設定等所有資訊，以避免 MFP 中的資料遭外洩。

在配備有 HDD 的設備中，安裝選購的資料安全套件或數位管理套件後，將會覆寫（批次刪除）HDD 儲存空間中的資料。僅有未安裝選購配件的設備可以初始化（格式化）。

配備 SSD 的設備，可透過格式化（安全清除）清除資料。當 SSD 儲存空間中的資料經由加密時，也可執行批次刪除，以刪除加密金鑰。在刪除加密金鑰之後，即無法解碼（讀取）SSD 儲存空間的加密資料，因此其效果與刪除資料本身（清除密碼編譯）相同。

*1 HDD（安全刪除）、SSD（安全清除）

表 7：辦公室多功能事務機的資安威脅與防護措施

辦公室設備的資安威脅	FUJIFILM Business Innovation 採取資安防護措施
7. 因系統管理員或使用者的疏忽而造成資料洩漏 即使管理員或使用者自認為已正確地完成設定或執行操作，但是人為疏失仍會導致資料意外洩漏。	**G) 避免配置設定／操作錯誤，提高文件處理的資安意識** • **針對全域IP位址的安全警示訊息** 建議管理員變更 IP 位址或採用使用者驗證模式。 • **將掃描文件傳送／儲存至固定位址** 透過將通訊目的地（包括傳真）限制在特定的位址，防止使用者將資料傳送至錯誤的位址或洩露資料。 • **防止錯誤的傳真輸出** 透過重複輸入號碼、手動重新撥號等方式，以防止誤傳。 • **封鎖傳真接收** 避免惱人的廣告傳真文件。 • **設定禁止列印時段** 可避免無人看管列印文件的狀況發生。 • **防止列印文件外洩** 提供註解、複印管理輸出（類似浮水印功能）和安全浮水印(數位管理)功能。

G) 保護「系統管理功能」

避免配置設定／操作錯誤，提高文件處理的資安意識

若將全域 IP 位址指派給 MFP，並將 [登入類型] 設定為 [無須登入] 時，當系統管理員登入時，即會顯示警示訊息。此功能建議系統管理員更換 IP 位址，或使用使用者驗證模式。

掃描至固定位址

此功能允許將目的地位址或寄件人，自動儲存在驗證使用者本人的電子郵件地址中。可透過此設定，有效避免電子郵件傳送錯誤及傳送至外部電子郵件收件人。

文件的儲存位置可指定使用者 PC 的特定資料夾；此外，將掃描文件儲存在設備上，可透過電子郵件傳送檔案連結給通過驗證的使用者。此功能可減少網路或郵件伺服器的負荷，並可確保將郵件傳送給通過驗證的使用者。

* 須在驗證模式下操作。

避免使用者傳真錯誤

將文件傳真至錯誤的位址是每個人都會出現的疏失，但此人為疏失將造成嚴重的後果。透過以下功能可避免傳送錯誤的狀況發生；且這些功能符合「FASEC 1*」，為針對商務用途的傳真安全功能準則。

- 重新輸入傳真位址：重複輸入傳真位址兩次，以進行驗證
- 手動重新撥號：在傳真時，從傳送歷史清單中選擇目的地

- 重複輸入傳真號碼
  透過輸入兩次傳真號碼，進行驗驗以避免輸入錯誤號碼。

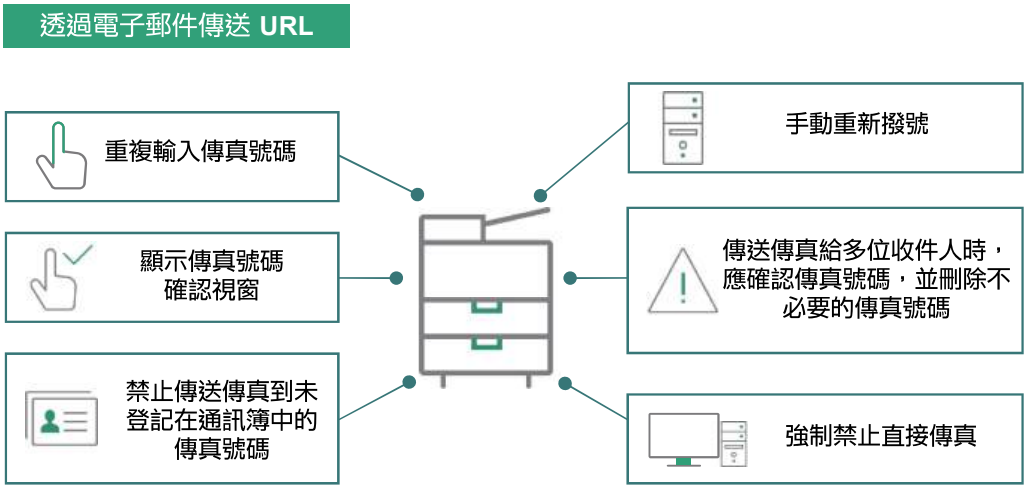
- 禁止傳送傳真到未列在通訊簿中的傳真號碼
  限制使用者將傳真傳送至未登記於通訊簿中的號碼。

- 強制禁止直接傳真 (Direct fax)
  禁止從PC發送傳真。

- 顯示傳真號碼的確認視窗
  在傳送傳真前，會跳出確認畫面進行再次確認，亦可允許使用者刪除錯誤的目的地。

- 傳送傳真給多位收件人時，應確認傳真號碼，並刪除不必要的傳真號碼
  允許使用者刪除或修正傳真號碼。

- 手動重新撥號
  在傳真傳送至目的地後，記錄傳真位址，並事先傳送一封文字傳真，以確定傳真傳送正確。



* 由日本 Communications and Information Network Association, CIAJ 制定，以促進改善電話線傳真通訊的安全功能。

此外，以下功能亦可避免傳真錯誤：

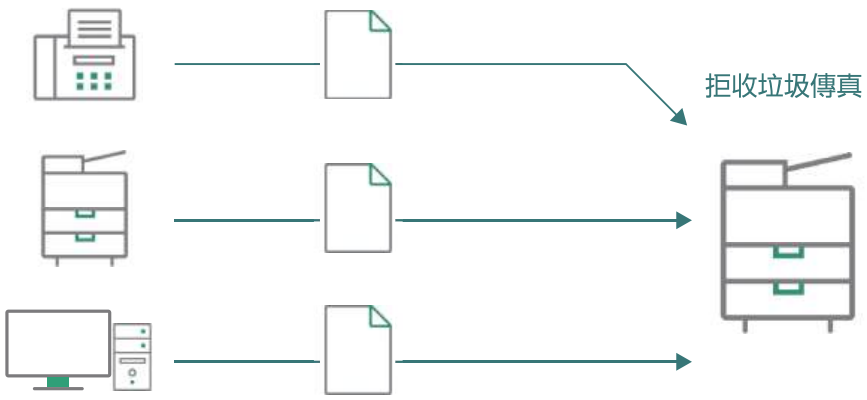
- 可透過禁止多位址傳真，避免造成傳真錯誤。
- 可禁止傳真的中繼與轉傳功能。

封鎖傳真接收

避免騷擾傳真的功能

透過來電拒接功能，避免接收垃圾傳真。
您可以拒絕來自不想接收其傳真之收件人，或來自不明號碼的傳真。避免隨機發送的垃圾傳真，所造成不必要文件列印。

- 封鎖傳真號碼：登錄可拒收傳真的 G3 ID（電話號碼）。可登入高達50組傳真號碼。
- 封鎖未知的傳真號碼：可封鎖未知 G3 ID（電話號碼）的傳真。

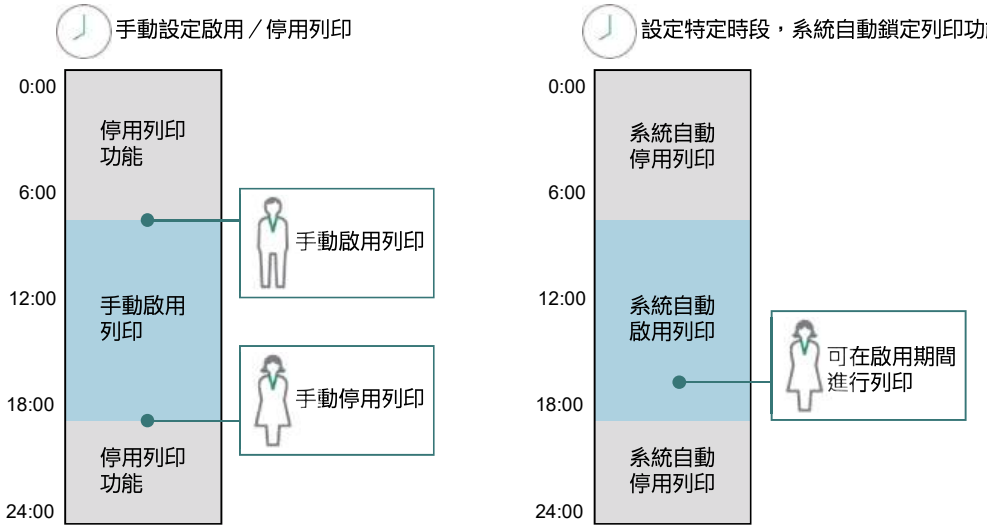


封鎖未登錄在通訊簿的傳真

可透過客服工程師模式設定，封鎖來自 MFP 通訊簿未登錄之送件人的傳真。

禁止列印時段

此功能可設定在特定時段停用列印功能，以避免當辦公室無人時，無人領取列印或傳真文件的情形發生。



在設定自動停用列印的期間，使用者亦可變更為啟用

註解

在複印時，可於文件上加註「不可複印」或其他文字，以提醒他人此文件的重要性。

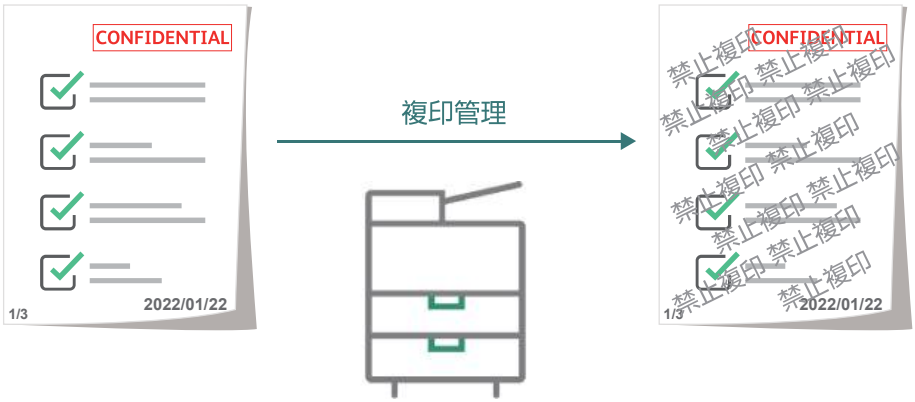
管理強制註解

透過此功能，可強制在複印、列印或收到的傳真文件上，加註列印使用者的 ID、輸出年份／月份／日期等。此功能可以輕鬆辨別輸出文件的「時間」、「輸出者」，並依據列印工作建立彼此的關聯性，進而設定四種範本樣式。在設備上安裝此功能後，無需再安裝其他選購功能，就能輕鬆處理各式紙本文件。

複製管理（類似浮水印功能）

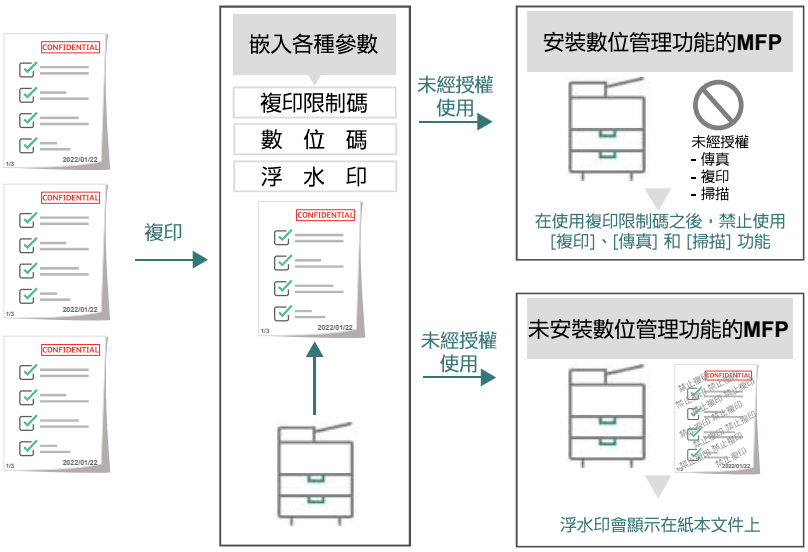
在輸出文件時，可將編號或浮水印印在文件上。在複印文件時，將會出現浮水印，可避免因未經授權進行複印而造成資料外洩。此方式可協助使用者能更謹慎地處理列印文件。

*選購。需有複製管理延伸套件。



安全浮水印 **Secure Watermark Kit**（數位管理）

在列印或複印文件時，可指定是否加入數位碼，例如複印限制碼或執行項目（Job）的資訊。透過安全浮水印可防止文件遭不當複印，亦可紀錄文件的歷程分析。此外，系統管理員可透過此功能強制嵌入數位碼，當資料外洩時，管理員可快速追蹤資訊。



* 安全浮水印 Secure Watermark Kit（數位管理）功能為選購。需有安全浮水印（數位管理）套件。
* 關於限制複印、數位碼分析和浮水印功能之文件資安防範作用，將視原始文件或設定方式不同而有所不同。

備註：

1. 本文件包含由 Xerox Corporation 授權的 Fuji Xerox 產品。產品經銷商為 FUJIFILM Business Innovation Corp.

2. 本文件內容、產品規格與描述將因產品更新而修訂，恕不另行通知。

FUJIFILM

台灣富士軟片資訊股份有限公司
FUJIFILM Business Innovation Taiwan Co., Ltd.

營業本部
地址 | 10551台北市松山區敦化北路88號7樓
電話 | (02) 2731-9099

fujifilm.com/fbtw