IDC MarketScape

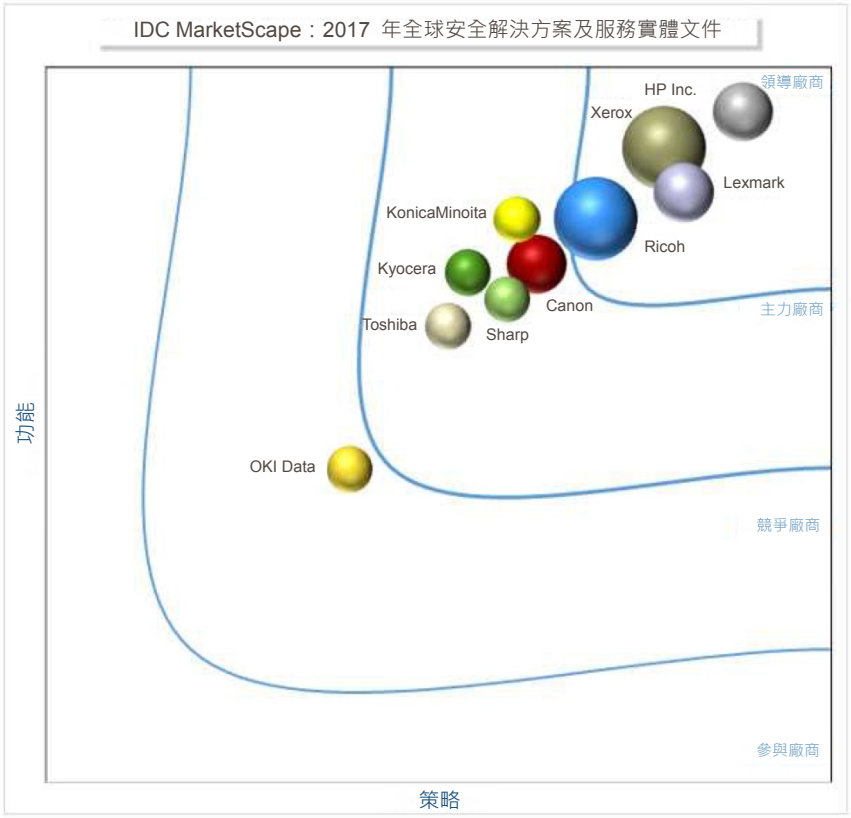
IDC MarketScape：2017 年全球安全解決方案及服務實體文件廠商評估

Robert Palmer Allison Correia

IDC MARKETSCAPE 圖片

圖 1

IDC MarketScape 全球安全解決方案及服務實體文件廠商評估



資料來源：2017 年，IDC

詳細的研究方法、市場定義和評分標準請參閱附錄。

IDC 觀點

本 IDC 研究透過 IDC MarketScape 模型，針對所選定的實體文件廠商，對其列印與文件安全解決方案及服務的市場進行評估。本次評估會同時針對質與量的特徵進行討論，探討讓廠商得以在此重要市場上取得成功的要素。本次 IDC MarketScape 涵蓋多家不同的實體文件廠商，以全方位框架為基礎進行評估，對象為在使用管理型列印與文件服務 (MPDS) 的情境下，以獨立功能及解決方案的形式所提供的安全防護能力，以及非 MPDS 的專業管理型服務的安全防護能力。許多實體文件製造商是以維護現有的管理型列印與文件服務客戶價值的方式，來提供列印與文件安全解決方案及服務，但也會發展獨立於 (或相鄰於) 其管理型服務產品的實用領域。若採用 IDC MarketScape 對列印與文件安全解決方案進行評估，企業可辨識出擁有強大產品及整合良好業務策略的廠商，這類廠商致力於保持長久的可行性和競爭力。本研究在功能及策略上所發現的成功因素包括：

- 現行的解決方案產品組合、裝置層級的功能、管理型服務、專業服務，以及其他針對列印與文件基礎架構的安全性考量的功能性
- 足以應對威脅層次的評估、偵測及風險修補等核心競爭力的能力
- 用於應對與保護列印與文件基礎架構的特定終端使用者困境的部署計畫
- 可協助客戶達到並維持安全合規性並符合業界中心標準的功能和策略
- 可透過直接和間接通路提供水平和垂直的安全解決方案及服務的全方位作法
- 專注維持優良的經營運作和服務提供能力，包括於本地、地區和全球層面提供穩定一致的服務
- 持續擴展至新的地理範圍、垂直產業和業務線 (LOB) 應用情境
- 靈活的服務供應、訂價和計費模型，以及對內部部署、私人、公共雲端產品的支援能力

IDC MARKETSCAPE 廠商涵蓋條件

本文件對 10 家主要的實體文件設備製造商進行分析，這幾家廠商均有豐富多樣的硬體產品，主打辦公室工作群組/部門內的列印環境，規模遍及全球。基於此種方式，Brother 與 Epson 這類廠商以全球營收來看屬於頂尖的印表機硬體商，但其主要產品線在設計上針對的是桌上型電腦和小型工作團隊的環境，因此會將之排除在外。本研究亦會排除 IT 外包公司、業務流程委外 (BPO) 供應商、軟體製造商這類將列印、文件和安全服務當作 IT 服務的一環，或是將這類服務轉包給實體文件廠商的公司。實體文件設備製造商的間接通路合作夥伴亦排除在本研究之外。

技術採購建議

無論業務規模大小，安全性已然是 IT 最優先的考量重點。然而 IDC 研究顯示，大多數企業的列印安全解決方案及服務的推行遠遠落後於整體的 IT 安全防護。列印環境的安全防護確實常常被遺漏在全面的 IT 安全策略之外。

與此同時，需要更有效率地管理資訊存取權限的考量也日漸增加。朝第三方平台技術 (包括行動和雲端工作流程) 的持續轉移，改變了公司處理文件和關鍵業務內容的方式。員工、客戶和其他知識工作者如今需要能夠全天候隨時存取公司防火牆內外部的資訊。資訊長和 IT 部門所面對的壓力日漸增加，必須對資訊管理有更好的掌控能力。

每家公司各有其本身獨特的列印環境，是以數位和紙本兩種形式管理資料、文件和資訊的中心地。若未多加監督列印與文件環境，則公司會因為韌體受到入侵、網路和文件儲存庫未經保護、資訊/資料洩漏等原因，而在資料和裝置層級出現漏洞。最終會導致要花費大量的員工時間和成本去處理漏洞、罰款以及商譽的損害。若忽略列印環境的安全防護同為整體 IT 策略的一環，會使得企業無力招架嚴重的內外網路威脅。

因此，企業應考量以下幾點：

- **判斷未來三年在列印及文件安全防護上預計的複雜度等級。**在接下來數年內，為列印裝置提供端點安全防護的內建功能會變得越來越普遍。但就希望開發全方位的列印基礎架構安全防護策略的企業而言，其所追求的解決方案和服務應當超越裝置的保護範圍。
- **瞭解當前環境。**評估現有的列印與文件基礎架構，找出安全威脅和漏洞所在。
- **將列印安全防護整合至整體 IT 安全策略環境。**發展長程規劃，納入各種持續監控和管理列印與文件安全程式的措施。多家廠商提供豐富的裝置和資料層級防護服務，其中許多在設計上可和現有的文件管理及企業內容管理 (ECM) 系統相整合，以提供進一步防護，也能處理政府法規上的合規性問題。
- **尋求現有的實體文件廠商。**在評估列印與文件安全防護需求時，務必將公司現有的實體文件廠商納入考量。這些廠商很有可能擁有極具吸引力的安全解決方案和服務，有清晰的規劃可結合各種技術來滿足成長中的業務需求。
- **判別特定產業的功能。**安全需求和法規遵循問題會因垂直市場的不同而有大幅差異。在列印與文件工作流程、內容管理和安全列印服務的核心競爭力方面，要尋找能符合公司特定產業需求的廠商。

廠商資料摘要

本節會簡短說明 IDC 觀點對於 IDC MarketScape 中的廠商定位的觀察結果。各家廠商均按附錄所列的標準經過評估，而本節會精簡介紹各家廠商的優點與面對的挑戰。

Canon

Canon 在 IDC MarketScape 全球列印與文件安全解決方案報告中的分類為主力廠商。Canon 為立足於東京的電子設備暨成像公司，創立於 1937 年，於歐洲、亞太地區、日本及美洲等地全球化經營。

Canon 致力於讓安全防護策略與客戶的需求一致，注重保護整體辦公室的文件生態系統，而非僅是保護裝置。Canon 提供針對水平和垂直兩方的安全解決方案，主要是隨著公司三大緊密相連的軟體解決方案構建而成：NTware 的 uniFLOW 負責列印、掃描和裝置管理，IRIS 處理進階的擷取選項、轉換和文件管理解決方案，因此為資訊管理、工作流程、業務分析解決方案。Canon 以第三代 imageRUNNER ADVANCE 裝置來強化裝置防護及端點安全性。Canon 也提供各種列印與文件基礎架構安全防護的評估與服務，目標在於找出客戶的需要和需求、瞭解當前的安全政策和不同法規的影響、挑選足以達成客戶安全目標的軟硬體和服務、透過安全策略文件和政策來實作和管理。

優點

在成像市場中，Canon 與其他競爭對手的不同之處在於，Canon 擁有豐富多樣的技術業務，並持續研發投資關鍵的技術領域，例如擴增實境和虛擬實境、光學與成像、專業軟體應用程式等。加上與第三方解決方案供應商建立了重要的合作關係，這類投資有助於強化 Canon 的產品並使之與眾不同。與此同時，Canon 也積極尋求收購，以進一步擴展功能、技術與知識，以求讓產品和解決方案更為豐富多樣。裝置層級的安全防護功能可以提供一個平台，讓客戶得以立即應對各式各樣的端點安全威脅，而整合式解決方案平台可提供更高一級的防護層，以處理內容和資料保護相關的更多需求。

Canon 的優點在於建立了公司的第三方平台架構，並在固有的裝置安全防護之外保護辦公資料的安全，且持續運用自家發展的技術和合作關係，將安全防護能力擴展到企業和中小企業雙邊領域。Canon 解決方案的作法對客戶相當有助益，支援各種重要業界標準和安全認證，包括 IEEE 2600 Common Criteria Certification 以及其他多種公司與政府所訂定的規範。

挑戰

IDC 認為，Canon 的供應模式策略還能有所增進，可運用該公司在雲端基礎架構上的投資來強化安全解決方案及服務的部署，藉以擴大市場。積極推動行銷也對 Canon 有益，可提高對列印及文件安全防護相關問題的意識和思想領導能力。

考量 Canon 的時機

若客戶需要具備深入且全方位的列印及文件安全防護方法的廠商，即可將 Canon 列入考量。Canon 的印表機開箱即有強大的端點防護能力，且該公司有能力和其他軟硬體合作夥伴緊密合作，因此可以提供客製化的解決方案，足以應對在列印安全、內容防護和法規遵循上的全面問題。

HP Inc.

HP Inc. 在 IDC MarketScape 全球列印與文件安全解決方案報告中屬於領導廠商。HP Inc. 總部位於加州帕羅奧圖，是一家上市公司。2016 年 9 月，HP Inc. 以 10.5 億美元併購了 Samsung 的列印業務部門，進一步擴大該公司在列印與文件服務合約市場的勢力。

HP Inc. 引領所有實體文件廠商前進，提高對於列印和文件安全考量的意識和能見度，且以擁有全世界最強大的安全合作夥伴為號召。HP Inc. 的安全防護措施是將列印和文件基礎架構全盤納入考量，從鎖定裝置開始，一路擴展到裝置的使用和內容防護等所有層面。HP Inc. 豐富的列印與文件安全解決方案融合了自有技術和合作夥伴所提供的功能性，分為四大主要領域：HP JetAdvantage Security Manager、HP Inc. 擷取列印解決方案、HP Inc. 資料防護功能、HP Inc. 安全防護服務。

HP JetAdvantage Security Manager 可讓客戶建立全方位的列印安全防護政策，並按照政策來評估和修補裝置，還可根據預先定義的準則進行審核和回報。HP Inc. 提供各式各樣的擷取列印解決方案，足以符合客戶特定環境和資料防護解決方案的需求，可協助企業偵測並防止資料經由印表機遺失。

HP Inc. 運用其多樣的解決方案產品，提供豐富的安全服務組合，包括 Security Audit Advisory Services、Implementation Service 和 Advisory Retainer Service。HP Inc. 以獨立程式的方式供應安全防護服務，但所有安全解決方案服務產品也可透過 HP Inc.的 Managed Print Services (MPS) 產品取得。HP Inc. 建立了強勁的管理型列印服務實作方式，以安全防護能力為骨幹，而根基立於其「作為服務」的全球基礎架構投資之上。HP Inc. 實際上將其 MPS 計畫作為「Secure MPS」來行銷，一部分是單純推銷，但同時也顯現出這類核心功能已經成為 HP Inc. MPS 系列標準安全防護元件。

優點

HP Inc. 的優點在於強大的 IT 服務和能力，能實現工作流程領域方面的擴張和整合能力，在技術堆疊上有一致性，並可促成跨 IT 基礎架構的全方位整合安全防護策略。HP Inc. 在世界各地勢力範圍廣闊，可在不同的地理區域為跨國公司和國際組織提供一致的服務。HP Inc. 在安全防護上的經歷，加上電腦和印表機一同進入市場，使之有別於其他競爭對手。

挑戰

IDC 認為 HP Inc. 的訂價結構模式有進步空間，可改善其人頭式計費模式，尋求直接訂約或符合合作夥伴需求的合約。HP Inc. 整體的行銷策略也可再改善，可和名聲響亮的網路資安公司建立更加正式的聯合開發和促銷計畫。

考量 HP Inc. 的時機

若對公司業務運作而言，列印和文件基礎架構的持續性威脅監控和風險修補的重要性無可比擬，即應將 HP Inc. 列入考量。若使用者尋求的是跨國的一致性，希望方案實行時有健全的功能集，且想要將列印與文件安全防護作為整體 IT 安全和公司管理計畫的一環，那麼 HP Inc. 應當也會出現在最終名單上。

Konica Minolta

Konica Minolta 在 IDC MarketScape 全球列印與文件安全解決方案報告中的分類為主力廠商。Konica Minolta 總部位於日本東京，於全世界擁有 43,000 名以上員工，於 150 個不同國家販售產品及服務。

Konica Minolta 的列印與文件安全防護策略是採取無一不包的形式，將裝置、文件、網路和實體環境均納入保護之下。Konica Minolta 具備各種解決方案和服務，可提供 MFP 型的安全防護能力，功能涵蓋使用者驗證與授權、裝置與列印安全管理、資料加密 (靜態及傳輸)、裝置惡意軟體防護、BIOS 與作業系統防護、韌體更新與密碼管理、硬碟廢棄、映像複寫、卸除式儲存媒體防護、防毒與防惡意軟體/間諜軟體、稽核追蹤、網路防護。

以豐富的解決方案產品為基礎，Konica Minolta 提供各式各樣的安全防護服務，在世界各地均能以各種不同的供應方式取得服務和擴張。服務包括 All Covered Security Assessment、Security Information Event Monitoring、Active Directory Security Event Management、HIPAA Consulting Services、PCI Consulting Services、Mobile Device Management、Unified Threat Management、Managed Vulnerability Scanning、Managed Print Services、內容服務、Information Rights Management。該公司的服務是以多種實施方式和供應模式來提供：一次性評估、內部部署、訂閱/雲端供應。

優點

Konica Minolta 的優點在於該公司的直接服務組織、間接通路合作夥伴、IT 服務功能、以及跨垂直產業與業務功能的強大解決方案整合能力。Konica Minolta 是少數幾家成功殺入 IT 服務市場的實體文件廠商。幾次關鍵性的併購 (如 All Covered) 對其成功有決定性的影響，但 Konica Minolta 也展現出其運用整合併購企業的重要資產能力，有助於推動本身核心的成像業務。該公司在 IT 方面的優點，搭配其在工作流程、文件管理、數位轉型等領域的技能，有助於和其他競爭對手作出區隔。

挑戰

IDC 認為 Konica Minolta 的供應模式策略還可再作改善，可朝雲端和訂閱型的模式轉換，進一步實現間接通路，並可應對中小企業區塊不斷成長的市場需求。此外，Konica Minolta 也可透過增加促銷活動以及舉辦更多與列印和文件安全相關的客戶和通路活動的方式，改善行銷方面的策略。

考量 Konica Minolta 的時機

若客戶在列印與整體 IT 基礎架構間需要穩定性和相互整合，應可將 Konica Minolta 列入考量。若所需的是針對法律、教育和金融業的特定安全解決方案和服務，也應考慮選擇 Konica Minolta。

Kyocera

Kyocera 在 IDC MarketScape 全球列印與文件安全解決方案報告中的分類為主力廠商。Kyocera 為總部設在日本京都的電子設備暨製造綜合公司。該公司於 2017 年 3 月 31 日止的會計年度報告在世界各地擁有超過 70,000 名員工。

Kyocera 安全策略的基本作法是以幾項關鍵要素來保護列印與文件基礎架構：裝置層級防護、使用者驗證、內容管理、合規/標準、諮詢服務。Kyocera 提供多種裝置層級的端點防護功能，並有各種方案，具備安全開機、安全資訊與活動管理 (SIEM) 整合、信任平台模組 (TPM) 支援等內建功能。

為了在文件和內容方面提供更豐富的防護，Kyocera 透過多種不同的供應模式和平台，提供各式各樣的安全解決方案和服務。Kyocera 自有的軟體 nscale 是一款內容管理平台，可作為雲端解決方案或內部部署解決方案使用。nscale 的設計是為了在公司自有的 ECM 系統中授予使用者存取權限，提供一個可安全有效率地管理文件的平台，無須使用存取控制清單 (ACL)。

Kyocera 所提供的安全服務包括模擬客戶電腦系統遭受攻擊的滲透測試，會嘗試取得系統功能和資料的存取權限，以找出安全防護上的弱點。Kyocera 以專業服務的形式提供 BPM 諮詢服務，以找出客戶的困難點所在，協助客戶達成合規性目標，並改善實用性和程序。

除此之外，也會以入門級的評估形式為客戶提供網路威脅評估，檢查客戶網路的健全狀態、評估可能的威脅、以及目前使用的應用程式風險。Kyocera 提供兩種類型的評估服務：列印與文件基礎架構安全性評估，以及更加針對 IT/技術作法設計的評估服務。列印與文件基礎架構安全性評估方面，Kyocera 的著眼點在於網路存取權限、不受控制的裝置、外界勢力、法規規範、裝置與應用程式。IT 評估則因產業而異，因為合規性和法規會因市場而不同。Kyocera 著重的產業包括政府機關、金融業、製藥業、教育界和媒體業。

優點

Kyocera 的優點在於以自有技術為基礎的深度安全解決方案產品和合作夥伴解決方案支援能力。近來對 Ceyoniq 和 DataBank 的併購是 Kyocera 的策略行動之一，讓該公司得以強化 ECM 領域的產品，以應對特定垂直市場和業務線應用程式的需求。Kyocera 也建立了強大且忠誠的間接通路計畫，對於提供中小企業市場的列印與文件安全防護服務大有助益。

挑戰

IDC 認為 Kyocera 的供應模式策略還可進一步強化，可以提高公司安全解決方案和服務產品在全世界的一致性。此外，Kyocera 整體的產品也可以再改善，可加入裝置層級的支援服務，以提供特定的基本功能，如安全開機和 SIEM 工具整合等，兩者均已有規劃。

考量 Kyocera 的時機

若整體的文件生態系統需要整合式安全防護策略，則 Kyocera 應當列入考量。若需要針對政府機關、金融業、製藥業、教育界和媒體業的特定安全解決方案和服務，也應將 Kyocera 納入廠商的最終名單之列。

Lexmark

Lexmark 在 IDC MarketScape 全球列印與文件安全解決方案報告中屬於領導廠商。Lexmark 總部位於肯塔基州的萊辛頓。Lexmark 的客戶遍布 170 個國家，全球將近有 14,000 名員工。

Lexmark 提供全系列的列印與文件安全防護服務，十分瞭解從工具、服務、資料、裝置、網路、使用者、應用程式乃至解決方案等各種環境要件。在裝置層級方面，Lexmark 提供多種功能和解決方案，可鎖定裝置，並保護在列印與為文件生態系統之中移動的內容資訊。這些功能包括安全輸出與使用者驗證、硬碟安全防護、資料防護、裝置/機群管理工具、安全文件監控、網路防護功能。

Lexmark 具有豐富的安全防護服務和解決方案，包括專有的技術和來自合作夥伴的軟體。該公司開發出一個解決方案生態系統，可讓硬體和其他第三方前後端應用程式無縫整合。Lexmark 的連接器，如 Cloud Solution Framework (CSF)、Embedded Solutions Framework (eSF)、Lexmark Document Distributor (LDD)，能夠順暢連接裝置、雲端、第三方嵌入式解決方案和文件。

Lexmark 在列印與文件安全解決方案與服務的部署和供應上善加運用雲端服務。Lexmark Professional Services 包含全球各地雄厚的諮詢專業人員、現場系統工程師和領域專家，擁有安全防護方面的特定技能、訓練和認證。Lexmark 的 Professional Services 組織是由自家強大的管理型列印服務實作經驗成長而成，致力於保持與客戶環境有緊密的知識連結，如此可找出客戶的困難所在，並根據客戶的特定需求來排列回應的優先順序。Lexmark 的安全領域專家有能力執行複雜度更高的諮詢工作，而全球實作安全防護的業主則能開出可供實作的方法、標準和策略。

優點

Lexmark 持續採取垂直形式進入市場，並以垂直產業的方式來處理銷售、支援和人力提供。Lexmark 的上層垂直產業包括零售業、銀行業、製造業、醫療照護業、政府機關、教育界和保險業。此種垂直作法加上 Lexmark 豐富的安全解決方案產品組合和專業服務人員，讓 Lexmark 為客戶提供同級最佳安全防護的地位屹立不搖。靈活的供應選項、建立完成的全球基礎架構、擴大合作夥伴強化安全產品的決心，在在都是該公司的重要優點。

挑戰

雖然 Lexmark 形成了數個新聯盟，IDC 仍認為 Lexmark 的銷售/經銷策略還有改善空間，可以依靠更多打入市場的聯盟和互補的服務供應商與軟體公司來加強。若持續投資創新以維持該公司的競爭地位和差異化，也有助於 Lexmark 的整體成長策略。

考量 Lexmark 的時機

若企業需要在全球各地擁有一致性，且想要注重輸出/文件安全性的穩健專案功能集，則應考慮 Lexmark。若解決方案的廣度和深度是優先事項，也應該將 Lexmark 加入最終名單內。

OKI Data

OKI Data 在 IDC MarketScape 全球列印與文件安全解決方案報告中屬於競爭廠商。OKI Data 為 OKI Electric 企業集團旗下的公司，以獨立公司的模式經營，在全球 100 多個國家運作，包括以下各地的製造站點：日本福島、泰國、英國、中國。

OKI Data 提供裝置、內容和網路的安全防護解決方案與服務。OKI Data 的安全解決方案融合了自有的智慧財產 (IP) 和第三方應用程式。其解決方案包括擷取與文件管理、列印管理、列印追蹤、計費功能。至於使用者驗證和安全列印方面，OKI Data 的 MFP 具備的 Smart Extendable Platform 可支援以下兩種功能，提供進階的裝置安全防護能力：私人列印與保留列印。OKI Data 也和多家第三方解決方案供應商合作，以支援安全列印和使用者驗證功能。PaperCut MF 提供安全的列印允許功能，可讓管理員鎖定無線列印功能，僅供經過核准的使用者使用。SENDYS Output Manager 則可設定安全政策，要求使用者透過 Microsoft Active Directory、PIN 碼、感應卡或行動裝置等方式驗證，才可取得文件。

安全防護也是 OKI Data 的 Managed Print Services 產品的要素之一。透過其 MPS 計畫和 Smart Managed Print Services，OKI Data 可協助企業應對各種變數，進一步保護列印與文件基礎架構，例如裝置與韌體更新、密碼防護、使用者存取控制與限制、安全列印功能等。

優點

OKI Data 擁有穩健的安全解決方案和服務，可合作為客戶提供安全的列印環境。OKI Data 持續努力將自身的列印技術從傳統的辦公室市場轉變為辦公室解決方案、專業服務和高速工業列印。

挑戰

IDC 認為 OKI Data 整體的安全防護和解決方案產品可再進一步改善，投資擴大公司的安全產品，並更將重心放在處理印表機導致的端點風險上。OKI Data 提供的服務範圍也可再增強，加入安全評估和審計功能以擴大，可作為獨立服務提供，也可作為管理型列印服務合約的一部分。

考量 OKI Data 的時機

若公司需要針對特定專案的穩健功能集，即可考慮 OKI Data。若希望在列印與文件基礎架構上的投資發揮應有的價值，也可考慮 OKI Data。

Ricoh

Ricoh 在 IDC MarketScape 全球列印與文件安全解決方案報告中屬於領導廠商。Ricoh 總部位於日本東京，於全世界擁有超過 109,000 名員工。

Ricoh 的安全解決方案從裝置核心一路擴展到使用者介面、嵌入式應用程式、網路、伺服器和各種服務。Ricoh 專注於三大關鍵領域，致力減少列印環境中的風險：列印安全、資訊安全、網路安全。Ricoh 也採取了多項步驟來應對客戶對於安全合規需求與日俱增的擔憂，包括風險與合規評估產品的擴展，以及切合客戶特定需求的評估型解決方案。

Ricoh 提供多種內建功能，屬於辦公室級 MFP 型號的標準配備。這些功能包括可信任平台模組保護的加密金鑰、韌體簽章認證、未授權影印防護功能、使用者驗證與存取限制 (包括 LDAP 驗證和 Windows 驗證)、驗證密碼加密、使用者鎖定功能、掃描文件 PDF 密碼保護、鎖定列印、硬碟加密設備、以及 DataOverwriteSecurity System (DOSS)。Ricoh 的多款特定產品也具備 ISO/IEC 15408 Common Criteria 的 IEEE 2600.2 認證。

Ricoh 亦提供豐富多樣的安全解決方案與服務，設計注重協助企業找出弱點空隙、緩解安全風險、維持對政府機關和業界規範的合規性。Ricoh 有多種管理型安全服務負責處理端點與網路的安全防護、身分存取管理、電子郵件安全性等。Ricoh 的網路安全方案則是根據深度防禦範例所開發，且 Ricoh 的各種安全防護服務直接對應至不同法規規範的需求，例如 HIPAA、PCI 及 Gramm-Leach-Bliley Act。Ricoh 也提供專門協助公司管理印表機的卸除和廢棄工作的服務。

優點

Ricoh 的安全解決方案產品結合了其在管理型服務、基礎架構服務、工作流程服務、軟體開發等方面的核心能力，有助於該公司獲得領導廠商的地位，有足夠的能力處理列印及文件環境內的安全防護。Ricoh 的全球服務供應模式讓公司得以提供一致的標準化諮詢服務，因此能在多家競爭對手中脫穎而出。

挑戰

IDC 認為 Ricoh 整體的供應情況可再改善，打入市場的直接和間接策略兩者間可以更趨於一致。Ricoh 的行銷策略也有進步空間，可以再多加闡述如何運用創新來推動技術上的規劃，也可以籌劃對外活動來增加知名度並提高公司在列印與文件安全領域的領導地位。

考量 Ricoh 的時機

公司尋求的是豐富多樣的解決方案和服務組合，注重網路安全更甚於裝置防護，且希望有平衡的全球服務供應模式，則可考慮採用 Ricoh。若使用者希望擁有持續來往的真正合作夥伴，以對不斷演進的技術和合規性的變化即時處置對應，則 Ricoh 也應當在最終的考量名單上。

Sharp

Sharp Corp. 在 IDC MarketScape 全球列印與文件安全解決方案報告中的分類為主力廠商。Sharp 為日本的跨國公司，總部位於日本大阪。

Sharp 提供多層次的安全防護佈建，以硬體為起點，再擴大納入內容與網路的防護功能，能協助緩解更大範圍的安全措施遭受的威脅。在列印與文件安全防護方面，Sharp 採取從頭到尾全包式作法，包括觀察、評估、部署、遠端監控與管理 (RMM)、裝置使用、韌體更新，直至最終的硬體除役。

Sharp 的 Security Suite 由四大要素組成：Standard MFP Security Features、Data Security Kit (Commercial/Common Criteria Certified)、Printer Drive and Application Security Features、Sharp Partner Program Member Applications。

Standard MFP Security Features 包括使用者驗證和授權、Sharp Remote Device Manager (SRDM) 提供的安全裝置與列印管理、資料加密、裝置惡意軟體防護、BIOS 與作業系統防護、韌體更新與密碼管理、硬碟廢棄、映像複寫、無需伺服器的內建基本擷取列印功能、稽核追蹤支援、電子郵件與傳真防護。

Sharp 提供豐富多樣的安全解決方案，組成包括 Sharp 自有的 IP，再加上地區和全球的合作夥伴一齊提供的第三方應用程式。結合 Sharp 的軟硬體解決方案後，還可提供多樣的管理型 IT 服務和管理型列印服務。Sharp 的安全服務可以為所有領域的列印與文件基礎架構提供更廣泛的保護措施，還能夠延伸至伺服器監控與照護、網路與安全評估、行動裝置管理等層面。Sharp 亦相當注重協助企業滿足各式各樣的產業標準和政府法規。

優點

由於鴻海企業的影響力加持，且鴻海堅決擴大在 IT 服務市場的勢力，Sharp 處於絕佳定位，可協助客戶處理範圍廣大的安全性挑戰。在實體文件領域中，Sharp 轉向 IT 服務市場和該公司的 IT 服務評估價值主張模式，在某種程度上相當獨特，得以讓 Sharp 對網路、周邊、行動、工作流程方面的安全性展開分析。

挑戰

IDC 認為 Sharp 在功能性或產品策略/規劃上還有改善空間，應當更加專注於引進新的安全防護措施來滿足公司成長中的需求。Sharp 的行銷策略也可再加強，可推出以安全功能和憑證為主打的方案。

考量 Sharp 的時機

若企業需要能夠對網路、周邊、行動、工作流程的安全性進行分析的 IT 服務供應商，即可考慮 Sharp。使用者若在尋找的是多種不同的垂直特定解決方案，也可將 Sharp 列入最終名單。

Toshiba

Toshiba 在 IDC MarketScape 全球列印與文件安全解決方案報告中的分類為主力廠商。Toshiba 總部位於日本東京，於北美洲、拉丁美洲、歐洲、亞太地區各地均有營運。

Toshiba 從四大角度來看安全性：裝置、存取、文件、生命終期。 Toshiba 整體的安全防護方案與產品組合名為 SecureMFP，由豐富多樣的自有 IP 和第三方解決方案共同組成。Toshiba 的策略聯盟夥伴包括 Nuance、PaperCut、Lexmark、Pharos、HP Inc. 及 PrinterLogic。Toshiba 透過各式各樣的第三方解決方案來提供裝置層級和使用者型的重要安全追蹤功能，包括終端使用者驗證和安全列印允許功能、資料監控與存取控制、規則式列印政策等。Toshiba 也有自己的產品：e-BRIDGE CloudConnect、e-BRIDGE Multi-Station Print、e-BRIDGE Fleet Management System。Toshiba 的 e-BRIDGE Multi-Station Print 是一款不需使用其他專用伺服器的隨身列印解決方案。

Toshiba 還提供許多安全防護實作和諮詢服務。Toshiba 會透過安全性評估找出客戶目前的安全漏洞，根據當前與未來的需求，與客戶一起合作建立正式的安全防護計畫，並將公司現有的安全防護政策一併納入考量。Toshiba 會持續提供多種服務，以修補目前的漏洞、強化或替換目前的產品、建立實施生命終期政策、設立好數位權限管理，藉此完善保護公司的智慧財產。

優點

Toshiba 已建立全面一致的方式來保護直接和間接的管道，有豐富的解決方案組合，足以涵蓋整個列印與文件基礎架構。Toshiba 的間接管道深植於中小企業，且 Toshiba 也致力以培訓和教育的方式，將工作流程和安全解決方案能力轉移給合作夥伴。

挑戰

IDC 認為 Toshiba 整體的產品策略還有改善空間，應善用技術與合作夥伴的產品，進一步超越公司當前以列印為重的作法。Toshiba 的服務範圍和供應策略也可再加強，可考慮拓展公司在安全評估和稽核方面的能力。

考量 Toshiba 的時機

若企業的列印與文件基礎架構需要全方位的防護，即可將 Toshiba 納入考量。若希望有值得信賴的合作夥伴能力和資源，Toshiba 也應當會出現在最終名單上。

Xerox

Xerox 在 IDC MarketScape 全球列印與文件安全解決方案報告中屬於領導廠商。Xerox 是一家上市公司，總部位於康乃狄克州諾沃克。Xerox 勢力遍布超過 180 個國家，擁有 130,000 名以上的員工。

Xerox 以工具、方法論和服務的形式，提供豐富的列印與文件安全解決方案組合，設計上專門用於滿足客戶在 IT 策略上的需求，包括資料、文件、裝置、規則、法規控管商用或個人使用案例。Xerox 的 Secure Print Manager Suite 可支援公司自行製作或第三方解決方案，如此能夠達到客戶在裝置驗證、擷取列印、安全行動列印和資料防護方面的需求。Xerox 也提供其他多種內容與協作工具 (即 DocuShare 7、DocuShare Flex、Hyland's OnBase)，以提供安全的資訊管理解決方案，同時也確保關鍵業務的文件和重要的商業機密處於公司的監管與政策下保持安全無虞。

Xerox 對於列印與文件環境的方法論所採取的是分層式作法，從裝置層級開始，進一步擴大深入至客戶的應用程式和 IT 基礎架構。這種分層式作法可以讓 Xerox 妥善處理保護 PDM 基礎架構時的三大要素：裝置、文件、資料防護。

Xerox 提供豐富多樣的安全服務，專門用來協助客戶找出安全漏洞、修補目前的漏洞、持續管理並遵守公司安全性政策和準則。作為 MPS 產品組合的一環，Xerox 也提供多種安全服務，以保障其管理型列印服務產品內的主動式管理、回報、安全事件修復能力，入侵偵測系統與防火牆的全天候監控與管理即為其中之一。

優點

Xerox 對列印與文件安全防護所採取的分層式作法，讓客戶擁有一組強大的基本功能，同時也提供一條移轉的路徑，可以透過進階的解決方案與服務，加入其他裝置防護功能和內容。Xerox 的全球服務供應能力和靈活的訂價方式，能夠為不同的地理區域、產業、各種規模的公司提供一致性和擴充能力。Xerox 所提供的 MPS 方案是業界中涵蓋範圍最廣的方案之一，有多種不同的入口，也就是無論何種公司規模或垂直產業，均可針對客戶的需求，量身打造出合適的安全列印解決方案與服務以供使用。

挑戰

IDC 認為，Xerox 的供應模式策略還能有所增進，可強化公司的雲端服務基礎架構，藉以改善解決方案的佈建方式，加強處理業務上和合作夥伴的需求。在列印與文件基礎結構方面，若提升市場名聲的活動增加，有明智的領導能力、獲得全新的品牌認知，都對 Xerox 當前的行銷能力有益。

考量 Xerox 的時機

若公司在尋找的是範圍廣大的產品組合以及豐富的諮詢與實作服務，還要注重既有的 ID 基礎架構與框架，Xerox 即可列入考慮。若優先追求靈活的訂價選項和精準的專案管理，則 Xerox 也應當列為最終名單之內。

IDC MarketScape 圖表閱讀方式

為本次分析目的，IDC 將可能的成功關鍵指標分為兩大類：能力與策略。

Y 軸的位置代表廠商目前的能力和服務項目，以及廠商之於客戶需求的符合程度。能力類別所關注的是公司目前即刻的能力。在此類別中，IDC 的分析師會觀察廠商在建立/提供能讓公司實行所選市場策略能力時的表現。

X 軸也就是所謂的策略軸，代表的是廠商的未來策略是否足以搭配客戶未來三至五年需求的程度。策略類別著重的是高等級的決策，以及未來三至五年內對產品、客戶市場區分、業務計畫與上市計畫等的基本假設。

IDC MarketScape 中，個別廠商圖示的大小則代表各家廠商在受評估的特定市場區塊中的市佔率。

IDC MarketScape 方法

IDC MarketScape 的挑選準則、權重以及廠商評分，代表的是 IDC 對市場和特定廠商詳加研究後的判斷。針對市場領導廠商、相關人員和終端使用者進行有結構的討論、調查、訪談後，IDC 分析師量身制訂出標準特徵的範疇。市場權重所根據的是使用者訪談、買家調查以及各市場中 IDC 專家審查委員會提出的資訊。至於各家廠商的評分以及廠商在 IDC MarketScape 上的最終落點，IDC 分析師所依據的是各家廠商的詳盡調查和訪談、公開取得的資訊、終端使用者的體驗，以求能夠對各家廠商的特徵、行為和能力提出準確且一致的評估。

市場定義

針對 2017 全球列印安全服務 IDC MarketScape，IDC 對列印與文件安全之定義為「用於處理應對列印與文件基礎架構安全問題的解決方案與服務，包括裝置層級的功能性、軟體解決方案、具有威脅層級評估、偵測、修復功能等核心能力的專業管理型服務」。

本 IDC MarketScape 會對裝置層級的資料/內容端點安全與防護兩方面的措施進行評估。其功能包括但不必然限定於：

- 使用者驗證與授權
- 裝置管理
- 裝置惡意軟體防護
- BIOS、作業系統、韌體更新與密碼管理
- 硬碟及卸除式儲存媒體防護
- 防毒與防惡意軟體/間諜軟體
- 安全事件管理

- 侵入偵測系統與防火牆的全天候監控與管理功能
- 修補程式的管理與更新監督
- 安全性評估與安全性稽核的執行
- 內容安全、隱私權、資料完整性 (軟硬體)
- 設備的安裝、設定與使用
- 遠端、BYOD、行動列印

實體文件廠商所提供的安全解決方案的範圍涵蓋軟硬體及管理型服務或專業服務的任何搭配組合。

安全服務包括諮詢服務與實行服務 (專業管理型)，涵蓋列印與文件的安全評估及稽核、安全事件與政策管理、侵入偵測系統與防火牆的持續監控與管理、修補程式的管理與更新監督、內容安全、隱私權、資料完整性 (靜態資料與傳輸資料)設備的安裝、設定與使用、遠端、BYOD、行動列印的安全系統。對傳統商用系統的整合以及對目前及未來的法規遵循政策的支援能力也會納入考量。

策略與能力準則

表 1 與表 2 為實體文件廠商成功提供列印與文件安全解決方案與服務的關鍵策略與能力指標。

表 1

成功的關鍵策略指標：全球安全解決方案與服務實體文件廠商

策略標準	成功標準	子標準權重 (%)
特定的產品規劃	此項展現的是廠商如何規劃解決方案與服務的擴展與開發工作，以應對列印與文件基礎架構的安全性。廠商會採用各式各樣不同的作法，以確保提高功能性和產業所需的能力，包括市場感知能力、產品強化、策略性聘僱與培訓。應著重於負責處理裝置層級與內容層級安全防護問題的策略性規劃。規劃計畫應提出產品在 IDC 第三方平台 (雲端、行動、社交、巨量資料、分析) 技術方面進展情況的特定資訊，也要應對法規合規性和垂直市場專業的成長需求。	15.0
於核心領域引進新解決方案的比率	此項特別注重廠商執行規劃的方式。針對列印與文件安全所引進的新功能性規劃比率為何？此項會對透過獨立軟體解決方案、專業管理型服務於裝置層級嵌入的功能進行評估。廠商也應當要注重系統整合與彼此間的互操作性，包括目前和已規劃的第三方軟體解決方案支援。	15.0

表 1

成功的關鍵策略指標：全球安全解決方案與服務實體文件廠商

策略標準	成功標準	子標準權重 (%)
跟上成長中業務需求的能力	為了確保發揮最大效果，企業必須強化能力，以製作出足以應對文件安全考量的產品，其中需考慮到多種要素，包括偵測、修復、法規合規性等。產品目前的發展會關係到未來三到五年內的客戶，也對客戶極具吸引力。此外，有效率的公司一定要有穩健的策略，需顯現出未來的客戶需求，也要述明符合客戶成長需求的規劃策略。	15.0
實作方法	準備好各種計畫以支援服務供應與計費的模式，以配合未來五年中客戶採納/消費偏好的轉變。計畫應要找出並處理在不同的列印與文件安全解決方案與服務供應模式下，目前出現的漏洞和可趁之機，運用策略來處理目標產品/客戶市場區塊，著重於多種不同的服務供應模式 (如套裝軟體和 SaaS)。	10.0
雲端供應	廠商應找出列印與文件安全解決方案與服務移轉至雲端供應模式 (公開、私人、混合) 的當前規劃和未來規劃。注重運用雲端供應模式來加快軟體佈建並改善服務供應能力的方案計畫。	10.0
本地與全球資源	此供應模式的策略應要述明廠商打算如何跨國拓展列印與文件的安全功能、解決方案與專業服務，以及廠商打算在哪些地區供應這類功能。運用與拓展合作通路的策略，也要注重用於處理特定產業與客戶市場區塊的解決方案與服務。	10.0
整體成長策略	成長策略涵蓋任務、方向和目標，廠商透過策略可獲得列印與文件安全解決方案與服務可取得的總市場中的成長率。此類別評估的是需清晰且有說服力地說明廠商的定位、市場機會以及增加廠商在總體可取得市場中的市佔率的機會。	15.0
整體研發策略	公司的創新模式可將公司的潛能發揮到極致，產生出列印與文件基礎架構防護方面的市場價值。廠商已展現出理解到若要提高產品的功能性，不但要深入內部開發資源，也要和其他公司合作，以將有所差異而創新的功能帶進市場。廠商未來三到五年內，對研發投資以及於美國及世界各地的合作計畫有清楚的策略。	10.0
總計		100.0

資料來源：2017 年，IDC

表 2

成功的關鍵能力指標：全球安全解決方案與服務實體文件廠商

能力標準	成功標準	子標準權重 (%)
整體供應產品	此項會評估廠商的產品組合功能性、解決方案、服務在處理列印與文件基礎架構的安全性考量的程度。此項評估會將廠商的安全防護產品的整體廣度和寬度納入考量，包括裝置層級的功能與支援能力、軟體解決方案、具有威脅評估、偵測、修復功能等核心能力的專業管理型服務。評估也會納入第三方合作夥伴的解決方案和支援產品。	15.0
基本能力	評估廠商對列印與文件安全性關鍵領域的核心市場需求的處理能力，包括使用者驗證與授權、裝置管理、資料加密、裝置惡意軟體防護、BIOS 與作業系統防護、韌體更新與密碼管理、硬碟廢棄、映像複寫、卸除式儲存媒體防護、防毒與防惡意/間諜軟體。對於業界標準和重要安全認證的合規性也會受到評估，包括 Health Insurance Portability and Accountability Act (HIPPA)、Sarbanes-Oxley Act、Gramm-Leach-Bliley Act、FDA 21 CFR Part 11 以及 Common Criteria Certification (ISO/IEC 15408)。	15.0
提供服務範圍	評估廠商的諮詢服務與實作服務 (專業管理型)，以帶給客戶最大效益。優秀程度端看是否提供全面的安全服務，包括列印與文件的安全評估及稽核、安全事件與政策管理、侵入偵測系統與防火牆的持續監控與管理、修補程式的管理與更新監督、內容安全、隱私權、資料完整性 (靜態資料與傳輸資料)設備的安裝、設定與使用、遠端、BYOD、行動列印的安全系統。對傳統商用系統的整合以及對目前及未來的法規遵循政策的支援能力也會納入考量。	15.0
供應方式的合適度和執行	評估廠商透過多種供應模式與平台提供各式各樣的安全解決方案與服務的能力。此項會納入分析師在服務供應、實作、持續管理、目標 SLA 的執行、支援能力等相關領域的評估。特別關注的領域則包括整體的服務供應方式 (內部部署/雲端、本機/遠端、陸上/海上、混合模式)、解決方案與技術部署、與既有系統的互操作性、全球供應狀態、以及持續的計劃管理和支援能力。	15.0

表 2

成功的關鍵能力指標：全球安全解決方案與服務實體文件廠商

能力標準	成功標準	子標準權重 (%)
銷售/經銷	此項顯示廠商的銷售人力分配，並會辨識專用於銷售/支援列印與文件安全解決方案服務的資源。此項會評估廠商銷售人員的專業能力，還有當地和跨國的混合銷售能力、垂直產業的銷售人力分派、銷售人員運用當地資源或國際資源作出決策的能力。也會評估廠商透過合作關係與通路，以本地、跨國和全球交易市場為目標的服務銷售能力。	10.0
行銷	此項會評估廠商在未來 12 到 18 個月內，意識到列印與文件安全解決方案與服務的需求並加以運用的能力。評估也會將直接行銷和專為通路合作夥伴開發的資源納入評估。廠商應對市場傳達出清楚的訊息，表達其有能力和專業可保護列印與文件基礎架構，包括垂直市場特定的計畫與活動以滿足法規合規性。	10.0
支援地理範圍	此項展現出廠商於全球供應列印與文件安全解決方案的能力。此項會評估廠商垂直分配客戶服務的能力，以及是否可跨國服務支援全球的客戶與合作夥伴、展現當地的影響力、滲入既有的客戶群、影響留客率。	10.0
訂價選項總數	此項顯示廠商處理列印與文件安全領域目前與未來客戶需求的訂價、包裝與計費模式的範圍。此項端看廠商對於客戶和通路供應方案及服務所支援的多種訂價與計費模式，包括費用型、人頭型、訂閱型服務、授權模式、SaaS、以及其他訂價/計費模式。	10.0
總計		100.0

資料來源：2017 年，IDC

瞭解詳情

相關研究

- *市場分析觀點：全球與美國管理型列印與文件服務 (Market Analysis Perspective: Worldwide and U.S. Managed Print and Document Services)，2017 年* (IDC #US41988617，2017 年 8 月)
- *IDC MaturityScape 標準：美國的列印與文件管理 (IDC MaturityScape Benchmark: Print and Document Management in the United States)，2017 年* (IDC #US41265117，2017 年 7 月)

- *全球與美國管理型列印與文件服務及基本列印服務預測 (Worldwide and U.S. Managed Print and Document Services and Basic Print Services Forecast)，2017–2021 年* (IDC #US41264717，2017 年 5 月)
- *2016 全球與美國管理型列印與文件服務及基本列印服務市佔率：中型市場成長 (Worldwide and U.S. Managed Print and Document Services and Basic Print Services Market Shares 2016: Growth in the Midmarket)*，(IDC #US41264817，2017 年 5 月)
- *IDC MarketScape：2016 年全球文件工作流程服務實體文件廠商評估 (IDC MarketScape:Worldwide Document Workflow Services Hardcopy 2016 Vendor Assessment)*，(IDC #US40994416，2016 年 9 月)

概要

本 IDC 研究針對頂尖的全球實體文件廠商，對其列印與文件安全解決方案及服務的市場進行評估，並找出其優點及難處。本次評估會同時針對質與量的特徵進行討論，探討讓廠商得以在此重要市場上取得成功的要素。本次 IDC 研究是以全方位的框架為基礎進行評估，對象為在使用 MPDS 的情境下，以獨立功能及解決方案的形式所提供的安全防護能力，以及非 MPDS 的專業管理型服務的安全防護能力。

IDC 成像、列印與文件解決方案部門研究主管 Robert Palmer 表示：「對許多企業而言，在發展全面的 IT 安全策略時，列印與文件安全經常受到忽略。就算採取許多措施保護 IT 基礎架構，缺乏列印環境的可見度以及疏忽，會導致出現脆弱的弱點，讓公司難以抵抗駭客和其他網路安全方面的威脅。」

關於 IDC

IDC 國際數據資訊是全球著名的資訊科技、電信行業和消費科技諮詢、顧問和活動服務專業提供商。IDC 幫助 IT 專業人士、企業主管和投資機構制定以實際研究結果為基礎的技術採購決策以及扎實的企業發展策略。IDC 在全球擁有超過 1100 名分析師，他們具有全球化、區域性和本地化的專業視角，對 110 多個國家的技術發展趨勢和業務行銷機會進行深入分析。在 IDC 超過 50 年的發展歷史中，眾多企業客戶借助 IDC 的策略分析而成功達成關鍵業務目標。IDC 是國際數據集團 (IDG) 的全資子公司，IDG 是全球領先的科技出版、會展服務及研究諮詢公司。

全球總部

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter：@IDC
idc-community.com
www.idc.com