SONY
說明指南

ILME-FX6
安全注意事項

本說明指南介紹使用本裝置進行檔案傳輸和串流時的安全注意事項。

5-075-083-01(1) Copyright 2026 Sony Corporation

ILME-FX6
安全注意事項

安全注意事項

本主題介紹將本裝置連接到網路時的注意事項。

- 通訊內容可能會在您不知情的情況下遭到訊號附近的第三方人士擅自攔截。使用無線 LAN 通訊時，請採取適當安全措施以保護通訊內容。
- 如果您將 [Security] 無線區域網路設定為 [None] 並連接到存取點，攝影機和存取點之間的無線通訊將不會加密，可能會被訊號範圍內的第三方攔截。使用 WPA2 或 WPA3 安全協定以增強安全性。
- SONY 對於因未針對傳輸裝置採取適當安全措施、因傳輸規格造成無法避免的資料洩漏，或是任何安全問題所導致的任何損壞一概不負責。
- 視操作環境而定，網路上的第三方人士可能可以擅自存取本機。本機連接至網路時，請確認網路受到安全防護。
- 本產品連接到網路時，透過可提供保護功能的系統（例如，路由器或防火牆）進行連接。如果在沒有此類保護的情況下連線，則可能會發生安全問題。

TP1002274614

5-075-083-01(1) Copyright 2026 Sony Corporation

ILME-FX6
安全注意事項

網際網路連接注意事項

本主題介紹將本裝置連接到網際網路時的注意事項。

- 本裝置無法透過無線區域網路連接到僅使用 WEP 或 WPA 的存取點，因為這些安全方法有漏洞。
- 本裝置不是網路裝置（例如路由器或交換式集線器）。強烈建議您將本裝置連接到可以適當配置和管理網路設定的網路，以防止基於網路的攻擊，例如 DoS 攻擊（拒絕服務攻擊）。
- 將本裝置連接到網路時，請透過經過適當配置和管理的路由器進行連接，或將其連接到具有相同功能的區域網路連接埠。如果在沒有這種保護的情況下進行連接（例如使用免費 Wi-Fi 時），可能會出現安全性問題。如果配置正確，路由器可以提供足夠的保護，防止 DoS 攻擊或網路裝置功能喪失。如果您發現任何異常，請立即中斷攝影機與網路的連接。

TP1002274615

5-075-083-01(1) Copyright 2026 Sony Corporation

網路功能相關注意事項

本主題介紹本裝置網路功能的注意事項。

- 如果偵測到未經授權的存取，攝影機可能無法接受通訊。如果發生這種情況，請從頭重新連接。
- 按下 [Network] 狀態畫面上的 [Show Authentication] 按鈕，以顯示連接到本裝置的驗證資訊。請注意，不要讓他人看見您的畫面或複製 QR 碼影像。
- 使用者名稱和密碼在購買時自動產生並在攝影機上設定。設定使用者名稱和密碼時，請確保其他人看不到這些設定。設定使用者名稱和密碼，如下所示。

[User Name]	– 設定一個包含 1 至 16 個字元的使用者名稱。 – 原廠預設將此項設定為“admin”。 – 下列是有效的輸入字元。 字母字元（大寫和小寫）、數字字元、符號 (! % + , - . = _)
[Password]	– 設定一個包含 8 至 16 個字元的密碼，其中至少包含 1 個或多個字母字元以及 1 個或多個數字字元。 – 下列是有效的輸入字元。 字母字元（大寫和小寫）、數字字元、符號 (! % + , - .= _)

TP1002274616

5-075-083-01(1) Copyright 2026 Sony Corporation

ILME-FX6
安全注意事項

無線區域網路相關注意事項

本主題介紹透過無線區域網路連接本裝置時的注意事項。

- 在本裝置的說明指南中，無線區域網路存取點和中繼區域網路連接的無線區域網路路由器稱為“存取點”。
- [Security]（加密方法）可以設定為 [None]、[WPA2] 或 [WPA3]。使用 [WPA2] 或 [WPA3] 是基於安全考量而建議。當選取 [None] 時，連接前會顯示訊息。為了確保無線區域網路連接的安全，強烈建議連接到具有 WPA2 或 WPA3 安全設定的存取點。
- 依預設，使用 [Manual Register] 註冊無線區域網路存取點時，會選取 WPA2 安全方法。
- 如果您連接到沒有任何安全設定的存取點，您可能會遭受駭客攻擊、惡意第三方存取或漏洞攻擊。除非不可避免的情況，否則不建議進行沒有任何安全設定的連接。
- 配置無線區域網路的安全性非常重要。對於未採取安全措施而造成的任何損害，或因使用無線區域網路時不可避免的情況而發生安全問題，Sony 概不負責。

TP1002274617

5-075-083-01(1) Copyright 2026 Sony Corporation

USB 網際網路共用相關注意事項

本主題介紹透過 USB 網際網路共用連接本裝置時的注意事項。

- 僅使用可信賴的智慧型手機裝置進行網際網路共用。基於安全考慮，不建議連接來源不明的裝置。

TP1002274618

5-075-083-01(1) Copyright 2026 Sony Corporation

關於 FTPES (FTPS) 功能

FTPS 功能支援多種加密演算法，確保檔案傳輸的安全。支援多種加密演算法（其中一些可能不符合目前的安全最佳實務），以便與各種伺服器相容。

FTPS 功能支援的加密演算法

支援下列加密演算法。

- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

建議的加密演算法

根據 NIST 建議（NIST SP 800-57 第 1 部分修訂版 5）及相關安全標準，建議使用下列加密演算法。

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

關於棄用的演算法

FTPS 功能還支援下列演算法以實現相容性，但根據 NIST 建議（NIST SP 800-57 第 1 部分修訂版 5）和相關安全標準，這些演算法已被棄用，並且可能會在未來版本中被移除。

- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

關於連接相容性

FTPS 功能在設計上兼顧安全性和相容性。目前，由於下列原因，支援棄用的演算法，但為了提高安全性，在未來的版本中可能會移除這些演算法。

- 自由攝影師和攝像師需要連接到在各種用戶端上執行的伺服器。
- 需要保持與舊系統和舊伺服器的相容性。

- 並非所有使用者都準備變更為更安全的設定，因為變更伺服器端的加密演算法設定很複雜。
- FTPS 設定通常與其他安全服務共用。任何變更都必須予以審慎考慮，因為這些變更可能會對伺服器上的其他服務產生影響。
- 必須支援多種加密演算法，以確保在不同環境中的互通性。

FTPS 連接期間使用的加密演算法由與目的地伺服器的自動協商決定，因此取決於伺服器設定。在意識到安全風險的同時，目前優先考慮相容性，以滿足使用者的多樣化需求。

安全風險

使用包括 CBC/DHE/RSA/SHA-1 在內的棄用演算法會增加加密資料被攻擊者解密或竄改的風險，從而導致資料在傳輸過程中洩漏。

安全連接建議

使用 FTPS 功能前，請檢查連接目的地伺服器是否支援建議的加密演算法。在伺服器端僅啟用建議的演算法，並停用已棄用的演算法。

使用安全 FTP 上傳

您可以使用顯式模式 (FTPES) 中的 FTPS 以加密的方式上傳檔案，以便連接目的地檔案伺服器。
對於安全 FTP 傳輸，請將檔案傳輸目的地伺服器上的 [Using Secure Protocol] 設定為 [On] 並匯入憑證。

參考資料

- Recommendation for Key Management, Special Publication 800-57 Part 1 Revision 5, NIST, 2020.
- Transitioning the Use of Cryptographic Algorithms and Key Lengths, Special Publication 800-131A Revision 2, NIST, 2019.
- Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, NIST, 2005（包括截至 2016 年 10 月 6 日的更新）。

憑證

將 FTPES (FTPS) 功能所使用的憑證寫入記憶卡的根目錄。設定檔案名稱，如下所示。
certification.pem（PEM 格式）
每個憑證可載入的最大憑證大小為 1 MB。

TP1002274619

5-075-083-01(1) Copyright 2026 Sony Corporation