ILME-FX6

セキュリティに関するご注意

このヘルプガイドは、本機のファイル転送やストリーミングのセキュリティについての注意事項を説明しています。

5-075-080-01(1) Copyright 2026 Sony Corporation

ILME-FX6
セキュリティに関するご注意

セキュリティに関するご注意

本機をネットワークに接続する場合の注意点です。

- 利用者が気付かないうちに、電波が届くところから意図せぬ第三者に通信内容を盗み見られてしまうおそれがあります。無線LAN通信を利用する際は、通信内容を保護するために、適切なセキュリティ対策をしてください。
- 本機の無線LANの設定で［Security］を［None］にしてアクセスポイントと接続すると、カメラとアクセスポイント間の無線通信が暗号化されないため、電波の届く範囲にいる第三者に内容を盗み取られる可能性があります。より安全なセキュリティ方式であるWPA2またはWPA3を使用してください。
- 通信を行う機器でセキュリティ対策を行わなかった結果、または、通信仕様上の、やむを得ない事情により、データ漏洩等、セキュリティ上の問題が発生した場合、弊社ではそれによって生じたあらゆる損害に対する責任を負いかねます。
- 使用環境によってはネットワーク上の意図せぬ第三者から製品にアクセスされる可能性があります。本機をネットワークに接続する際には、セキュアなネットワークであることをご確認の上ご使用ください。
- 本製品のネットワークへの接続には、ルーターやファイアウォールなどの保護機能を通して接続をしてください。このような接続をしない場合、セキュリティ上の問題が生じる可能性があります。

TP1002220827

5-075-080-01(1) Copyright 2026 Sony Corporation

ILME-FX6
セキュリティに関するご注意

インターネット接続時のご注意

本機をインターネットに接続する場合の注意点です。

- 本機は無線LANを用いて、脆弱性が懸念されるセキュリティ方式であるWEPまたはWPAのみを使用するアクセスポイントとは接続できません。
- 本機はネットワーク機器（例えばルーター、スイッチング・ハブ）ではありません。DoS攻撃（サービス妨害攻撃）などのネットワーク経由での攻撃に対して、適切な設定と管理を行うことができるネットワークに本機を接続することを強く推奨します。
- 本機のネットワークへの接続には、適切な設定と管理が行われたルーターを介した接続、もしくは同機能を有したLANポートへの接続をしてください。このような接続をしない場合（例えばFree Wi-Fiなど）、セキュリティ上の問題を生じる可能性があります。ルーターは適切な設定をすることにより、ネットワーク内の機器へのDoS攻撃または機器の機能喪失に対する十分な保護を提供します。何か異常を感じた場合は、すぐにカメラをネットワーク接続から遮断してください。

TP1002220828

5-075-080-01(1) Copyright 2026 Sony Corporation

ILME-FX6
セキュリティに関するご注意

ネットワーク機能に関するご注意

本機のネットワーク機能についての注意点です。

- 不正なアクセスが検出された場合、カメラが通信を受け付けない状態になることがあります。その際は再度初めから接続し直してください。
- ［Network］ステータス画面の［Show Authentication］ボタンを押すと、本機に接続するための認証情報が表示されます。画面を盗み見られたりQRコードの画像を流出させないようにご注意ください。
- ユーザー名やパスワードは、お買い上げ時にカメラが自動で生成し設定されます。任意のユーザー名とパスワードを設定する際は、他者に盗み見られないようご注意ください。ユーザー名、パスワードは、以下のように設定してください。

［User Name］	– 1文字以上16文字以下の任意のユーザー名を設定してください。 – 出荷時は「admin」に設定されています。 – 入力可能文字は下記です。 英字（大文字、小文字）、数字、記号（！% + , - . = _ ）
［Password］	– 英字・数字をそれぞれ1文字以上含む、8文字以上16文字以下の任意のパスワードを設定してください。 – 入力可能文字は下記です。 英字（大文字、小文字）、数字、記号（！% + , - . = _ ）

TP1002220830

5-075-080-01(1) Copyright 2026 Sony Corporation

ILME-FX6
セキュリティに関するご注意

無線LANに関するご注意

本機を無線LANで接続する場合の注意点です。

- 本機のヘルプガイドでは、LAN接続を中継する無線LANアクセスポイントや無線LANルーターなどを「アクセスポイント」と表記しています。
- ［Security］（暗号化方式）は［None］、［WPA2］、［WPA3］から選択できます。セキュリティの観点から、暗号化される［WPA2］または［WPA3］の利用を推奨します。［None］を選択した場合は、接続する前に警告メッセージが表示されます。セキュアな無線LAN接続を実現するために、セキュリティ設定がWPA2またはWPA3のアクセスポイントを使用することを、強く推奨します。
- ［Manual Register］で無線LANアクセスポイントを登録する場合のセキュリティ方式は初期状態でWPA2が選択されています。
- セキュリティ設定なしのアクセスポイントに接続すると、ハッキングや悪意ある第三者からのアクセス、脆弱性への攻撃を受ける可能性があります。特別な理由がある場合以外は、セキュリティ設定なしでの使用は推奨しません。
- 無線LANではセキュリティの設定をすることが非常に重要です。セキュリティ対策を施さなかった場合、あるいは無線LANの使用上やむを得ない事情により、セキュリティの問題が発生してしまった場合、弊社ではこれによって生じたあらゆる損害に対する責任を負いかねます。

TP1002220831

5-075-080-01(1) Copyright 2026 Sony Corporation

ILME-FX6
セキュリティに関するご注意

USBテザリングに関するご注意

本機をUSBテザリングで接続する場合の注意点です。

- テザリングを行うスマートフォンは、信頼できるデバイスのみを使用してください。セキュリティ上安全ではないため、素性が不明なデバイスとの接続は推奨しません。

TP1002220832

5-075-080-01(1) Copyright 2026 Sony Corporation

FTPES（FTPS）機能について

FTPS機能は、安全なファイル転送を実現するために様々な暗号化アルゴリズムをサポートしています。幅広いサーバーとの互換性を確保するため、複数の暗号化アルゴリズムに対応していますが、その中には現在のセキュリティベストプラクティスに適合しないものも含まれています。

FTPS機能がサポートする暗号化アルゴリズム

以下の暗号化アルゴリズムをサポートしています。

- 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

推奨される暗号化アルゴリズムについて

NIST勧告（NIST SP 800-57 Part 1 Revision 5）および関連するセキュリティ標準に基づき、以下の暗号化アルゴリズムが推奨されています。

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

非推奨アルゴリズムについて

FTPS機能は互換性のため以下のアルゴリズムもサポートしていますが、NIST勧告（NIST SP 800-57 Part 1 Revision 5）および関連するセキュリティ標準に基づき非推奨とされており、将来のバージョンでは削除される可能性があります。

- 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

接続互換性について

FTPS機能は、セキュリティと互換性のバランスを考慮して設計されています。現時点では、以下の理由から非推奨アルゴリズムもサポートしていますが、将来のバージョンではセキュリティ強化のためこれらのアルゴリズムを削除する可能性があります。

- フリーランスのフォトグラファーやビデオグラファーは、様々なクライアントが運用するサーバーに接続する必要があります。
- 古いシステムやレガシーサーバーとの互換性を維持する必要があります。
- サーバー側での暗号化アルゴリズムの設定変更は複雑であり、すべてのユーザーが安全な設定に変更できるとは限りません。
- FTPSのサーバー設定は、他のセキュアサービスと共有されることが多く、サーバー上の他サービスへの影響を考慮する必要があり容易に変更できるとは限りません。
- 様々な環境での相互運用性を確保するため、幅広い暗号化アルゴリズムのサポートが必要です。

FTPS接続時に使用される暗号化アルゴリズムは接続先サーバーとの自動ネゴシエーションによって決定されるため、サーバー側の設定に依存します。セキュリティリスクを認識しつつも、ユーザーの多様なニーズに応えるため、現時点では幅広い互換性を優先しています。

セキュリティリスク

CBC/DHE/RSA/SHA-1を含む非推奨アルゴリズムを使用すると、暗号化されたデータが攻撃者によって解読または改ざんされるリスクが高まり、転送中のデータが漏洩する危険性があります。

安全な接続のための推奨事項

FTPS機能を使用する際は、接続先サーバーが推奨暗号化アルゴリズムをサポートしているか事前に確認してください。サーバー側では推奨アルゴリズムのみを有効にし、非推奨アルゴリズムを無効化することをお勧めします。

セキュアなFTP転送を行うには

ファイル転送先サーバーとの接続にFTPSのExplicitモード（FTPES）を使用することで、ファイルを暗号化して転送することができます。
セキュアなFTP転送を行うには、ファイル転送先サーバーの設定で、［Using Secure Protocol］を［On］に設定し、証明書の読み込みを行います。

参考資料

- 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 (includes updates as of 10/06/2016).

証明書

FTPES（FTPS）機能で利用する証明書はメモリーカードのルートディレクトリに書き込んでください。ファイル名は以下に設定してください。
certification.pem（PEM形式）
読み込める証明書サイズは1証明書辺り最大1MBです。

TP1002220833

5-075-080-01(1) Copyright 2026 Sony Corporation