ILME-FX6

보안 주의 사항

본 도움말 안내는 장치를 사용한 파일 전송 및 스트리밍 시의 보안 주의 사항에 대해 설명합니다.

ILME-FX6
보안 주의 사항

보안 주의 사항

이 항목에서는 장치를 네트워크에 연결할 때의 주의사항에 대해 설명합니다.

- 신호 대역이 비슷한 제3자가 무단으로 통신 내용을 가로챌 수 있습니다. 무선 LAN 통신을 사용할 때는 통신 내용을 보호하기 위한 적절한 보안 수단을 시행하십시오.
- [Security] 무선 LAN 설정을 [None]으로 지정하고 액세스 포인트에 연결할 경우, 카메라와 액세스 포인트 간의 무선 통신은 암호화되지 않아 신호 범위 내의 제3자가 통신을 가로챌 수 있습니다. 보안을 강화하려면 WPA2 또는 WPA3 보안 프로토콜을 사용하십시오.
- SONY는 전송 장치에 대한 적절한 안전 대책 구축 실패로 인해 발생하는 어떤 종류의 피해, 전송 사양에 따른 불가피한 데이터 누출 또는 어떠한 종류의 보안 문제에 대해서도 책임을 지지 않습니다.
- 운영 환경에 따라 승인되지 않은 제3자가 네트워크를 통해 제품에 액세스할 수 있습니다. 제품을 네트워크에 연결할 때 네트워크가 안전하게 보호되고 있는지 확인하십시오.
- 이 제품을 네트워크에 연결할 때는 라우터나 방화벽과 같은 보호 기능이 있는 시스템을 통해 연결하십시오. 이러한 보호 기능 없이 연결하면 보안 문제가 발생할 수 있습니다.

TP1002274638

ILME-FX6
보안 주의 사항

인터넷 연결 주의사항

이 항목에서는 장치를 인터넷에 연결할 때의 주의사항에 대해 설명합니다.

- 이 장치는 취약점이 있는 보안 방법인 WEP 또는 WPA만을 사용하는 액세스 포인트에 무선 LAN을 통해 연결할 수 없습니다.
- 이 장치는 네트워크 장치(예: 라우터 또는 스위칭 허브)가 아닙니다. DoS 공격(서비스 거부 공격)과 같은 네트워크 기반 공격으로부터 보호하기 위해 네트워크 설정을 적절하게 구성하고 관리할 수 있는 네트워크에 장치를 연결하는 것이 강력히 권장됩니다.
- 장치를 네트워크에 연결할 때는 적절하게 구성되고 관리되는 라우터를 통해 연결하거나 동일한 기능을 갖춘 LAN 포트에 연결합니다. 이러한 보호 기능 없이 연결할 경우(예: 무료 Wi-Fi 사용) 보안 문제가 발생할 수 있습니다. 라우터를 적절하게 구성하면 DoS 공격이나 네트워크 내 장치의 기능 손실로부터 충분한 보호 기능을 제공합니다. 이상한 점이 발견되면 즉시 카메라를 네트워크에서 분리하십시오.

TP1002274639

ILME-FX6
보안 주의 사항

네트워크 기능과 관련된 주의사항

이 항목에서는 장치의 네트워크 기능에 대한 주의사항을 설명합니다.

- 무단 접근이 감지되면 카메라가 통신을 수신할 수 없게 될 수 있습니다. 이런 현상이 발생하면 처음부터 다시 연결하십시오.
- [Network] 상태 화면에서 [Show Authentication] 버튼을 눌러 장치에 연결하기 위한 인증 정보를 표시합니다. 다른 사람이 이 화면을 보거나 QR 코드 이미지를 복사할 수 없도록 주의하십시오.
- 사용자 이름과 암호는 구매 시 자동으로 생성되어 카메라에 설정됩니다. 사용자 이름과 암호를 설정할 때, 해당 설정이 다른 사람에게 보이지 않도록 주의하십시오. 사용자 이름과 암호를 다음과 같이 설정합니다.

[User Name]	– 1~16자로 구성된 사용자 이름을 설정합니다. – 공장 기본값은 "admin"입니다. – 유효한 입력 문자는 다음과 같습니다. 알파벳 문자(대문자와 소문자), 숫자, 기호(! % + , - . = _)
[Password]	– 알파벳 문자 1개 이상과 숫자 1개 이상을 포함하는 8~16자의 암호를 설정합니다. – 유효한 입력 문자는 다음과 같습니다. 알파벳 문자(대문자와 소문자), 숫자, 기호(! % + , - . = _)

TP1002274640

ILME-FX6
보안 주의 사항

무선 LAN과 관련된 주의사항

이 항목에서는 무선 LAN을 통해 장치를 연결할 때의 주의사항에 대해 설명합니다.

- 이 장치의 도움말 안내에서는 LAN 연결을 중계하는 무선 LAN 액세스 포인트와 무선 LAN 라우터를 "액세스 포인트"라고 합니다.
- [Security](암호화 방법)을 [None], [WPA2] 또는 [WPA3]으로 설정할 수 있습니다. 보안 관점에서 [WPA2] 또는 [WPA3]의 사용을 권장합니다. [None]이 선택된 경우, 연결하기 전에 메시지가 표시됩니다. 안전한 무선 LAN 연결을 위해 WPA2 또는 WPA3 보안 설정이 적용된 액세스 포인트에 연결하는 것이 강력히 권장됩니다.
- [Manual Register]를 사용하여 무선 LAN 액세스 포인트를 등록할 때 기본적으로 WPA2 보안 방법이 선택되어 있습니다.
- 보안 설정이 없는 액세스 포인트에 연결할 경우, 해킹, 악의적인 제3자의 접근 또는 취약점에 대한 공격을 받을 수 있습니다. 불가피한 경우를 제외하고 보안 설정 없이 연결하는 것은 권장되지 않습니다.
- 무선 LAN에서 보안을 구성하는 것은 매우 중요합니다. Sony는 보안 조치를 취하지 않아 발생한 손해나 무선 LAN 사용 시 불가피한 상황으로 인해 보안 문제가 발생한 경우 책임을 지지 않습니다.

TP1002274641

ILME-FX6
보안 주의 사항

USB 테더링과 관련된 주의사항

이 항목에서는 USB 테더링을 통해 장치를 연결할 때의 주의사항에 대해 설명합니다.

- 테더링에는 신뢰할 수 있는 스마트폰 기기만 사용하십시오. 보안 문제로 인해 출처를 알 수 없는 장치에 연결하는 것은 권장되지 않습니다.

TP1002274642

FTPES(FTPS) 기능 정보

FTPS 기능은 다양한 암호화 알고리즘을 지원하여 안전한 파일 전송을 보장합니다. 다양한 서버와의 호환성을 위해 여러 암호화 알고리즘이 지원되며, 이 중 일부는 현재 보안 모범 사례를 준수하지 않을 수 있습니다.

FTPS 기능이 지원하는 암호화 알고리즘

다음 암호화 알고리즘이 지원됩니다.

- 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

권장 암호화 알고리즘

다음 암호화 알고리즘은 NIST 권장 사항(NIST SP 800-57 1부 5차 개정판) 및 관련 보안 표준을 기반으로 권장됩니다.

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

사용되지 않는 알고리즘 정보

FTPS 기능은 호환성을 위해 다음과 같은 알고리즘도 지원하지만, NIST 권장 사항(NIST SP 800-57 1부 5차 개정판) 및 관련 보안 표준에 따라 더 이상 사용되지 않으며, 향후 버전에서 제거될 수 있습니다.

- 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

연결 호환성 정보

FTPS 기능은 보안과 호환성의 균형을 맞춰 설계되었습니다. 현재 사용되지 않는 알고리즘은 다음과 같은 이유로 지원되지만, 보안을 개선하기 위해 향후 버전에서 제거될 수 있습니다.

- 프리랜서 사진 작가와 비디오 작가는 다양한 클라이언트에서 실행되는 서버에 연결해야 합니다.
- 구형 시스템 및 레거시 서버와의 호환성을 유지해야 합니다.

- 서버 측의 암호화 알고리즘 설정을 변경하는 것은 복잡하기 때문에 모든 사용자가 더 안전한 설정으로 변경할 준비가 되어 있지는 않습니다.
- FTPS 설정은 종종 다른 보안 서비스와 공유됩니다. 변경 사항은 서버의 다른 서비스에 영향을 미칠 수 있으므로 신중하게 고려해야 합니다.
- 다양한 환경에서의 상호 운용성을 보장하기 위해 다양한 암호화 알고리즘이 지원되어야 합니다.

FTPS 연결 중에 사용되는 암호화 알고리즘은 대상 서버와의 자동 협상을 통해 결정되므로 서버 설정에 따라 달라집니다. 보안 위험을 인지하면서도, 현재는 사용자의 다양한 요구를 충족하기 위해 호환성이 우선시되고 있습니다.

보안 위험

사용되지 않는 알고리즘(CBC/DHE/RSA/SHA-1 포함)을 사용하면 암호화된 데이터가 공격자에 의해 해독되거나 변조될 위험이 높아지고 전송 중에 데이터가 노출될 수 있습니다.

안전한 연결을 위한 권장 사항

FTPS 기능을 사용하기 전에 연결 대상 서버가 권장 암호화 알고리즘을 지원하는지 확인하십시오. 서버 측에서 권장되는 알고리즘만 활성화하고, 사용되지 않는 알고리즘은 비활성화합니다.

보안 FTP를 사용하여 업로드

대상 파일 서버와의 연결을 위해 Explicit 모드(FTPES)에서 FTPS를 사용하여 암호화된 파일을 업로드할 수 있습니다.
보안 FTP 전송의 경우 파일 전송 대상 서버에서 [Using Secure Protocol]을 [On]으로 설정하고 인증서를 가져옵니다.

참고문헌

- 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 (2016년 10월 6일 기준 업데이트 포함).

인증서

FTPES(FTPS) 기능에서 사용하는 인증서를 메모리 카드의 루트 디렉터리에 기록합니다. 파일 이름을 다음과 같이 설정합니다.
certification.pem(PEM 형식)
로드할 수 있는 최대 인증서 크기는 인증서당 1MB입니다.

TP1002274643