SONY

Manuel d’aide

MPC-2610

Mesures de sécurité

Ce manuel d’aide décrit les mesures de sécurité à prendre pour le transfert de fichiers et la diffusion en continu à l’aide de l’appareil.

MPC-2610
Mesures de sécurité

Mesures de sécurité

Cette rubrique décrit les précautions à prendre lors de la connexion de l’appareil à un réseau.

- Le contenu des communications peut être intercepté à votre insu par des tiers non autorisés à proximité des signaux. Lors de communications LAN sans fil, appliquez des mesures de sécurité adaptées pour protéger le contenu des communications.
- Si vous réglez le réglage [Security] du LAN sans fil sur [None] et que vous vous connectez à un point d’accès, la communication entre la caméra et le point d’accès ne sera pas chiffrée. Elle pourra donc être interceptée par un tiers se trouvant dans la zone de couverture du signal. Utilisez le protocole de sécurité WPA2 ou WPA3 pour une sécurité renforcée.
- SONY NE PEUT ÊTRE TENUE RESPONSABLE DE TOUT DOMMAGE, DE QUELQUE NATURE QUE CE SOIT, RÉSULTANT D’UNE INCAPACITÉ À METTRE EN PLACE DES MESURES DE SÉCURITÉ ADAPTÉES POUR LES DISPOSITIFS DE TRANSMISSION, DE FUITES DE DONNÉES INÉVITABLES DUES AUX SPÉCIFICATIONS DE TRANSMISSION OU DE TOUT AUTRE PROBLÈME DE SÉCURITÉ.
- Selon l’environnement d’exploitation, il est possible que des tiers non autorisés sur le réseau puissent accéder à l’appareil. Avant de connecter l’appareil au réseau, vérifiez que le réseau est bien protégé.
- Lorsque vous connectez ce produit à un réseau, connectez-le via un système fournissant une fonction de protection, tel qu’un routeur ou un pare-feu. Si vous vous connectez sans cette protection, des problèmes de sécurité pourraient survenir.

TP1002220992

MPC-2610
Mesures de sécurité

Précautions concernant la connexion Internet

Cette rubrique décrit les précautions à prendre lors de la connexion de l’appareil à Internet.

- L’appareil ne peut pas se connecter en LAN sans fil à un point d’accès utilisant uniquement WEP ou WPA, car ces méthodes de sécurité présentent des vulnérabilités.
- L’appareil n’est pas un périphérique réseau (par exemple, un routeur ou un commutateur réseau). Il est fortement recommandé que vous connectiez l’appareil à un réseau dont vous pouvez configurer et gérer les réglages réseau de manière appropriée, afin de le protéger contre les attaques réseau, telles que les attaques DoS (attaques par déni de service).
- Lorsque vous connectez l’appareil à un réseau, utilisez de préférence un routeur correctement configuré et sécurisé, ou un port LAN disposant des mêmes fonctionnalités. Une connexion sans ce type de protection (par exemple via un réseau Wi-Fi public) peut entraîner des risques de sécurité. Lorsqu’ils sont correctement configurés, les routeurs fournissent une protection suffisante contre les attaques DoS ou la perte de fonctionnalité des appareils du réseau. Si vous observez un comportement anormal, déconnectez immédiatement la caméra du réseau.

TP1002220993

MPC-2610
Mesures de sécurité

Précautions relatives à la fonction réseau

Cette rubrique décrit les précautions à prendre concernant la fonction réseau de l’appareil.

- Si un accès non autorisé est détecté, la caméra risque de ne plus pouvoir accepter les communications. Dans ce cas, reconnectez-vous depuis le début.
- Les informations d’authentification permettant de se connecter à l’unité s’affichent lorsque vous utilisez [Network] – [Network Setup] – [Show Authentication]. Veillez à ce que l’écran ne puisse pas être visualisé et que l’image du code QR ne puisse pas être copiée par d’autres personnes.
- Un nom d’utilisateur et un mot de passe doivent être définis au moment de l’achat. Lorsque vous définissez votre nom d’utilisateur et votre mot de passe, assurez-vous que les réglages ne sont pas visibles par d’autres personnes. Réglez le nom d’utilisateur et le mot de passe comme suit.

[User Name]	– Réglez un nom d’utilisateur comprenant 1 à 16 caractères. – Ceci est réglé sur « admin » par défaut. – Les caractères suivants sont valides. Caractères alphabétiques (majuscules et minuscules), caractères numériques, symboles (! % + , - . = _)
[Password]	– Réglez un mot de passe comprenant 8 à 16 caractères contenant au moins 1 ou plusieurs caractères alphabétiques et 1 ou plusieurs caractères numériques. – Les caractères suivants sont valides. Caractères alphabétiques (majuscules et minuscules), caractères numériques, symboles (! % + , - . = _)

TP1002220994

MPC-2610
Mesures de sécurité

Précautions relatives au LAN sans fil

Cette rubrique décrit les précautions à prendre lors de la connexion de l’appareil via un LAN sans fil.

- Dans le manuel d’aide pour cet appareil, les points d’accès LAN sans fil et les routeurs LAN sans fil qui relaient les connexions LAN sont appelés « points d’accès ».
- [Security] (méthode de chiffrement) peut être réglé sur [None], [WPA2] ou [WPA3]. L’utilisation de [WPA2] ou [WPA3] est recommandée du point de vue de la sécurité. Lorsque [None] est sélectionné, un message s’affiche avant la connexion. Pour une connexion LAN sans fil sécurisée, la connexion aux points d’accès avec un réglage de sécurité WPA2 ou WPA3 est fortement recommandée.
- Par défaut, la méthode de sécurité WPA2 est sélectionnée lors de l’enregistrement d’un point d’accès LAN sans fil à l’aide de [Manual Register].
- Si vous vous connectez à un point d’accès sans aucun réglage de sécurité, vous vous exposez à des risques de piratage, d’accès par des tiers malveillants ou d’exploitation de failles de sécurité. Sauf indication contraire, il est déconseillé d’établir une connexion sans réglage de sécurité.
- La configuration de la sécurité sur un réseau LAN sans fil est très importante. Sony décline toute responsabilité en cas de dommages résultant de l’absence de mesures de sécurité, ou de problèmes de sécurité survenus dans des circonstances inévitables liées à l’utilisation du réseau LAN sans fil.

TP1002220995

MPC-2610
Mesures de sécurité

Précautions relatives au partage de connexion USB

Cette rubrique décrit les précautions à prendre lors de la connexion de l’appareil via un partage de connexion USB.

- Utilisez uniquement des smartphones approuvés pour le partage de connexion. La connexion à des dispositifs d’origine inconnue n’est pas recommandée pour des raisons de sécurité.

TP1002220996

À propos de la fonction FTPES (FTPS)

La fonction FTPS prend en charge divers algorithmes de chiffrement pour garantir un transfert de fichiers sécurisé. Plusieurs algorithmes de chiffrement, dont certains ne sont pas conformes aux meilleures pratiques de sécurité actuelles, sont pris en charge pour la compatibilité avec une large gamme de serveurs.

Algorithmes de chiffrement pris en charge par la fonction FTPS

Les algorithmes de chiffrement suivants sont pris en charge.

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Algorithmes de chiffrement recommandés

Les algorithmes de chiffrement suivants sont recommandés conformément aux recommandations du NIST (NIST SP 800-57 Part 1 Revision 5) et aux normes de sécurité associées.

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

À propos des algorithmes obsolètes

La fonction FTPS prend également en charge les algorithmes suivants à des fins de compatibilité. Cependant, selon les recommandations du NIST (NIST SP 800-57 Part 1 Revision 5) et les normes de sécurité associées, ces algorithmes sont considérés comme obsolètes et pourraient être supprimés dans une version future.

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_GCM_SHA384
- 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

À propos de la compatibilité des connexions

La fonction FTPS est conçue pour offrir un équilibre entre sécurité et compatibilité. Actuellement, les algorithmes obsolètes sont pris en charge pour les raisons suivantes, mais ils peuvent être supprimés dans une version ultérieure afin d'améliorer la sécurité.

- Les photographes et vidéastes indépendants doivent se connecter à des serveurs fonctionnant sur divers systèmes clients.
- La compatibilité avec les anciens systèmes et les serveurs existants doit être maintenue.
- Tous les utilisateurs ne sont pas en mesure de passer à des réglages plus sécurisés, car modifier les réglages de chiffrement côté serveur peut s'avérer complexe.
- Les réglages FTPS sont souvent partagés avec d'autres services sécurisés. Toute modification doit être évaluée avec précaution car elle peut avoir un impact sur d'autres services du serveur.
- Un large éventail d'algorithmes de chiffrement doit être pris en charge pour garantir l'interopérabilité dans différents environnements.

L'algorithme de chiffrement utilisé lors d'une connexion FTPS est déterminé automatiquement par négociation avec le serveur de destination ; il dépend donc des réglages du serveur. Bien que les risques en matière de sécurité soient connus, la priorité est actuellement donnée à la compatibilité, afin de répondre aux besoins hétérogènes des utilisateurs.

Risques de sécurité

L'utilisation d'algorithmes obsolètes, tels que CBC/DHE/RSA/SHA-1, augmente le risque que les données chiffrées soient déchiffrées ou altérées par un attaquant, exposant ainsi les données durant leur transfert.

Recommandation pour une connexion sécurisée

Avant d'utiliser la fonction FTPS, vérifiez que le serveur de destination de la connexion prend en charge l'algorithme de chiffrement recommandé. Activez uniquement les algorithmes recommandés côté serveur et désactivez les algorithmes obsolètes.

Téléchargement à l'aide d'un FTP sécurisé

Vous pouvez charger des fichiers cryptés à l'aide de FTPS en mode Explicit (FTPES) pour la connexion avec le serveur de fichiers de destination.
Pour un transfert FTP sécurisé, réglez [Using Secure Protocol] sur [On] dans le serveur de destination de transfert de fichiers puis importez un certificat.

Références

- 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 (y compris les mises à jour à partir de 10/06/2016).

Certificat

Écrivez le certificat utilisé par la fonction FTPES (FTPS) dans le répertoire racine d'une carte mémoire. Définissez le nom du fichier comme suit.
certification.pem (format PEM)
La taille maximale d'un certificat pouvant être chargée est de 1 Mo par certificat.

TP1002220997