MPC-2610

安全注意事项

本帮助指南介绍使用本机进行文件传输和流媒体传输时的安全注意事项。

MPC-2610
安全注意事项

安全注意事项

本主题介绍将本机连接到网络时的注意事项。

- 通信内容可能会在不知情的情况下被信号附近的第三方拦截。使用无线LAN通信时，请采取适当的安全措施以保护通信内容。
- 如果将[安全]无线LAN设置设为[无]并连接至接入点，摄像机与接入点之间的无线通信不会被加密，可能会被信号范围内的第三方截获。为增强安全性，请使用WPA2或WPA3安全协议。
- SONY不对任何因传输设备安全措施操作不当、传输规格导致不可避免的数据泄露或任何种类的安全问题造成的损坏负责。
- 视操作环境而定，网络上未经授权的第三方可能可以访问本装置。将本装置连接到网络时，必须确认网络有安全保护。
- 将本产品连接到网络时，请通过具有保护功能的系统（例如路由器或防火墙）进行连接。如果在没有此类保护的情况下进行连接，可能会发生安全问题。

TP1002220936

MPC-2610
安全注意事项

互联网连接注意事项

本主题介绍将本机连接到互联网时的注意事项。

- 本机无法通过无线LAN连接至仅使用WEP或WPA的接入点，因为这些都是存在漏洞的安全加密方式。
- 本机并非网络设备（例如路由器或交换式集线器）。强烈建议将本机连接至可对网络设置进行适当配置和管理的网络，以防范基于网络的攻击，例如DoS攻击（拒绝服务攻击）。
- 在将本机连接至网络时，请通过经过适当配置和管理的路由器进行连接，或者将其连接至具有相同功能的LAN端口。如果在没有此类保护的情况下（例如在使用免费Wi-Fi时）进行连接，可能会出现安全问题。若配置得当，路由器能够提供足够的防护，防范DoS攻击或设备在网络中丧失功能。如果发现任何异常情况，请立即断开摄像机与网络的连接。

TP1002220937

MPC-2610
安全注意事项

网络功能相关注意事项

本主题介绍本机网络功能相关注意事项。

- 如果检测到未经授权的访问，摄像机可能无法接受通信。如果发生这种情况，请从头开始重新连接。
- 通过[网络] – [网络状态] – [显示接入验证设置]操作时，系统会显示连接本机所需的身份验证信息。请注意，不要让其他人看到屏幕，且不要让其他人复制二维码图像。
- 必须在购买时设置用户名和密码。在设置用户名和密码时，确保设置内容不会被他人看到。按如下方式设置用户名和密码。

[用户名]	– 设置一个由1至16个字符组成的用户名。 – 此项在出厂时默认设置为“admin”。 – 以下皆为有效输入字符。 字母数字字符（大写和小写）、数字字符、符号(！% + , - .= _)
[密码]	– 设置一个由8至16个字符组成的密码，其中至少包含1个或以上的字母字符和1个或以上的数字字符。 – 以下皆为有效输入字符。 字母数字字符（大写和小写）、数字字符、符号(！% + , - .= _)

TP1002220938

MPC-2610
安全注意事项

无线LAN相关注意事项

本主题介绍通过无线LAN连接本机时的注意事项。

- 在本机的帮助指南中，无线LAN接入点和中继LAN连接的无线LAN路由器统称为“接入点”。
- [安全]（加密方法）可设为[无]、[WPA2]或[WPA3]。出于安全考虑，推荐使用[WPA2]或[WPA3]。选择[无]时，系统会在建立连接前显示一条消息。为实现安全的无线LAN连接，强烈建议连接至采用WPA2或WPA3安全设置的接入点。
- 使用[手动注册]方式注册无线LAN接入点时，默认选择的安全方法为WPA2。
- 如果连接至没有任何安全设置的接入点，可能会遭受黑客攻击或第三方恶意访问，也可能会因漏洞而遭受攻击。除非不可避免，否则不建议连接至没有任何安全设置的接入点。
- 对无线LAN进行安全配置非常重要。对于因未采取安全措施而造成的任何损害，或因使用无线LAN时出现不可避免的情况而发生安全问题，Sony概不负责。

TP1002220939

MPC-2610
安全注意事项

USB网络共享相关注意事项

本主题介绍通过USB网络共享连接本机时的注意事项。

- 仅使用可信任的智能手机设备进行网络共享。出于安全考虑，不建议连接来源不明的设备。

TP1002220940

关于FTPES (FTPS)功能

为了确保文件传输的安全，FTPS功能支持多种加密算法。为了兼容各种服务器，该功能支持多种加密算法，其中一些算法可能不符合当前的安全最佳实践。

FTPS功能支持的加密算法

支持以下加密算法。

- 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

推荐加密算法

根据NIST建议（NIST SP 800-57第1部分修订版5）以及相关安全标准，推荐使用以下加密算法。

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

关于已弃用的算法

为了保证兼容性，FTPS功能也支持以下算法，但根据NIST的建议（NIST SP 800-57第1部分修订版5）以及相关安全标准，这些算法已被弃用，并且可能会在未来的版本中被移除。

- 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

关于连接兼容性

FTPS功能旨在在安全性和兼容性之间寻求平衡。目前，由于以下原因，我们支持一些已弃用的算法，但为了提高安全性，未来版本可能会移除这些算法。

- 自由摄影师和摄像师需要连接至运行在各种客户端上的服务器。
- 需要保持与旧系统和遗留服务器的兼容性。
- 并非所有用户都准备好切换到更安全的设置，因为在服务器端更改加密算法设置很复杂。
- FTPS设置通常会与其他安全服务共享。任何更改都必须谨慎考虑，因为它们可能会对服务器上的其他服务产生影响。
- 为了确保在不同环境中的互操作性，必须支持多种加密算法。

在FTPS连接期间使用的加密算法由与目的地服务器的自动协商确定，因此取决于服务器设置。虽然意识到存在安全风险，但目前优先考虑兼容性，以便满足用户的多样化需求。

安全风险

使用已弃用的算法（包括CBC/DHE/RSA/SHA-1）会增加加密数据被攻击者解密或篡改的风险，导致数据在传输过程中遭到泄露。

安全连接建议

使用FTPS功能之前，先检查连接目的地服务器是否支持推荐的加密算法。服务器端仅允许启用推荐的算法，禁止使用已弃用的算法。

使用安全FTP进行上传

可以使用显式模式FTPS (FTPES)上传文件，加密与目的地文件服务器之间的连接。
针对安全FTP传输，将文件传输目的地服务器上的[使用安全协议]设为[开]，并导入认证。

参考资料

- 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日的更新内容）。

认证

将FTPES (FTPS)功能使用的认证写入存储卡的根目录。按如下方式设置文件名称。
certification.pem（PEM格式）
每个认证可加载的最大认证大小为1 MB。

TP1002220941