RICOH THETA / RICOH360 THETA

Security White Paper

Security Threats and Countermeasures for RICOH THETA / RICOH360 THETA

2025.12.01 ver.1.2

RICOH360

Table of Contents

Overview of Security Functions against Various Threats

The various threats surrounding the RICOH THETA / RICOH360 THETA include the following.

Network security

The RICOH THETA / RICOH360 THETA communicates with computers, smartphones and servers over a network. If communications are not protected, important information may be maliciously altered or stolen. To protect important information from unauthorized access via the network, please take advantage of the following features. This section describes wireless LAN, wired LAN, LTE, and Bluetooth.

Please refer to the user manual for details on each of these functions.

Wireless LAN Communication

By operating the WLAN button on the side of the main unit (RICOH THETA Z1, RICOH360 THETA A1) or the main unit touch panel (RICOH THETA X), you can select OFF, AP (Access Point) mode, or CL (Client) mode.

AP (Access Point) mode connection

By using the RICOH THETA / RICOH360 THETA in AP (Access Point) mode, you can directly connect and control the THETA with a computer or smartphone. Communications in AP (Access Point) mode are encrypted using WPA2-PSK (AES) or WPA3-SAE (AES).

You can enhance security by modifying the following settings.

For details, please refer to the user manual of the respective model.

SSID (network name)

The default value is THETA + serial number (2 letters + 8 digits) + .OSC.

By changing the network name from the default value (ASCII printable characters can be used), it can be made less obvious that the THETA is being used.

Encryption key (passphrase)

The default value is 8 characters, but can be changed from 8 to 63 characters.

The security strength can be increased by increasing the number of characters and character types (ASCII printable characters can be used). Be sure to manage your encryption key securely.

CL (Client) mode connection / Wired LAN connection (WebAPI control)

RICOH THETA / RICOH360 THETA can be controlled via a router from a computer or smartphone by using CL (Client) mode. The security intensity can be changed by changing the following settings.

Ensure the access point is a trusted access point when using this service.

For details, please refer to the user manual of the respective model.

Authentication method

Digest authentication is used.

Digest Authentication User Name

The default value is THETA + serial number (2 alphabetic characters + 8 digits), but it can be changed from 1 to 32 characters.

You can increase the security level by using longer passphrases with more diverse character types (ASCII printable characters can be used).

Digest Authentication Password

If Digest Authentication is used, it must be set first; it can be set to between 8 and 63 characters.

The security strength can be increased by increasing the number of characters and character types (ASCII printable characters can be used).

Encryption method

When connecting the RICOH THETA / RICOH360 THETA in CL (Client) mode, the router information must be registered with the RICOH THETA / RICOH360 THETA.

At this time, you can select from WEP, WPA/WPA2-PSK, and WPA3-SAE according to the specifications of the router to be connected. (Some models do not support WPA3.)

Select the appropriate one for your environment. WPA2-PSK or WPA3-SAE is recommended unless there is a special reason.

Some public wireless LAN services provided by public institutions may not encrypt communications, and in such cases, the contents of communications may be intercepted by a third party.

Avoid using WebAPI control when connected to unencrypted public networks. Communication with RICOH360 Cloud Service is encrypted, so there is no problem.

CL (Client) mode connection (RICOH360 Cloud Control)

Communication with RICOH360 Cloud Service is encrypted using TLS1.2/1.3 to address risks such as eavesdropping of information.

Reference: Information Security

CL (Client) mode connection (live streaming control)

In preparation

Mobile Network Control

SORACOM's line, which is supported, cannot be directly accessed from outside.

RICOH THETA Z1 does not support mobile network communication.

For details, please refer to the user manual of the respective model.

Bluetooth communication

The models that support Bluetooth are compatible with Bluetooth Low Energy and can operate as either a Central or a Peripheral. When connected as Peripheral, various controls are possible via Bluetooth API.

When used as a Peripheral, it is necessary to make a connection from a terminal such as a smartphone (hereinafter referred to as "terminal").

Supported security level varies depending on the model. At least RICOH THETA / RICOH360 THETA and the terminal can be connected as long as they can be operated directly, and the connection can be made without confirmation by RICOH THETA, so please be very careful when handling.

Depending on the version, Bluetooth is enabled by default and can be disabled via the API or by operating the device.

For details, please refer to the user manual of the respective model.

Function	RICOH THETA Z1	RICOH THETA X	RICOH360 THETA A1
Shooting with Bluetooth connection/GPS function (RICOH THETA Application)	With authentication, no encryption	Not supported	Not supported
WLAN connection via Bluetooth (RICOH THETA Application or RICOH360 Application)	Not supported	With authentication, no encryption *1	Not supported
Automatic upload setting (RICOH360 Application)	Without authentication and encryption *2	With authentication and encryption	With authentication and encryption

*1 Please be mindful of your surroundings when using the smartphone application to automatically connect THETA X to a WLAN.

*2 Please be mindful of your surroundings when registering THETA Z1 for use with the RICOH360 Cloud via the smartphone application.

Interface Security

The RICOH THETA / RICOH360 THETA can access images and videos stored on the RICOH THETA / RICOH360 THETA through a physical cable connection or by operating the unit.

Depending on the usage environment, there is a possibility that important information may be maliciously altered or stolen. To protect important information, please use the following functions. This section describes the USB terminal and main unit operation buttons.

USB communication

RICOH THETA / RICOH360 THETA supports MTP (Media Transfer Protocol). Some models also support MSC (Mass Storage Class).

For models that support MSC, you can choose whether to operate with MSC or MTP when

connecting to a terminal via USB.

In either case, please handle the device with care, as you can freely access the stored images and videos simply by connecting it to the terminal with a USB cable. For details, please refer to the user manual of the respective model.

Main Unit Operation

WLAN ON/OFF and power ON/OFF can be performed by operating the main unit.

Depending on the model, a microSDXC card can be used, but the card cover cannot be locked.

Depending on the model, it is also possible to format the internal memory.

Depending on the model, it is possible to prohibit button operation by using the API.

For details, please refer to the user manual of the respective model.

Device Security

Firmware tampering prevention

RICOH THETA / RICOH360 THETA has built-in software called firmware that controls the operation of the device. If the firmware is improperly altered by a malicious person, the device may not operate properly, and there is a risk of intrusion into the network using the device as a stepping stone or destruction of the device by an unauthorized program.

Follow the official procedure when updating firmware to ensure device integrity.

Still image and video files (image information) stored in the internal memory

These data include image information, location information, user input information, and device configuration information. If this information is stolen in some way, information leaks may occur.

The built-in storage of the RICOH THETA / RICOH360 THETA is not encrypted. The stored image information can be freely accessed when connected via USB as mentioned above. Please be careful with the environment in which the RICOH THETA / RICOH360 THETA is used and managed.

Do not use files that are not created by the RICOH THETA / RICOH360 THETA using MSC or microSDXC.

Batch erasure of data

When disposing of the RICOH THETA / RICOH360 THETA, please erase the stored data.
Depending on the model, initialization may be performed via the device interface.
For details, please refer to the user manual of the respective model.