RICOH THETA / RICOH360 THETA

セキュリティホワイトペーパー

RICOH THETA / RICOH360 THETA におけるセキュリティ上の脅威と対策について

2025.07.01 ver.1.0

RICOH360

Copyright © Ricoh Co., Ltd. All Rights Reserved.

目次

様々な脅威に対するセキュリティ機能概要 3

ネットワークセキュリティ 3
- 無線 LAN 通信 3
- AP（アクセスポイント）モード接続 3
- CL（クライアント）モード接続・有線 LAN 接続（WebAPI 制御） 3
- CL（クライアント）モード接続（RICOH360 クラウド制御） 4
- CL（クライアント）モード接続（ライブストリーミング制御） 4
- モバイルネットワーク制御 5
- Bluetooth 通信 5

インタフェースセキュリティ 5
- USB 通信 5
- 本体操作 5

デバイスセキュリティ 6
- ファームウェアの改ざん防止 6
- 内蔵メモリに保存される静止画・動画ファイル（画像情報） 6
- データの一括消去 6

Copyright © Ricoh Co., Ltd. All Rights Reserved.

様々な脅威に対するセキュリティ機能概要

RICOH THETA / RICOH360 THETA を取り囲む脅威には次のようなものがあります。

ネットワークセキュリティ

RICOH THETA / RICOH360 THETA はネットワークを介してコンピューターやスマートフォン、サーバーと通信を行います。通信が保護されていない場合、重要な情報が悪意を持って改ざん・窃取される可能性があります。 ネットワークを介した不正アクセスから重要な情報を守るため、以下の機能を活用してください。ここでは無線 LAN、有線 LAN、LTE、Bluetooth について記載します。
それぞれの機能の内容については使用説明書を参照してください。

無線 LAN 通信

本体側面の WLAN ボタン（RICOH THETA Z1、RICOH360 THETA A1）、もしくは本体タッチパネル（RICOH THETA X）を操作することで、OFF、AP（アクセスポイント）モード、CL（クライアント）モードを選択することができます。

AP（アクセスポイント）モード接続

RICOH THETA / RICOH360 THETA を AP（アクセスポイント）モードで利用することで、コンピューター、スマートフォンと THETA を直接接続して制御することが可能です。
AP（アクセスポイント）モードの通信は WPA2-PSK（AES）で暗号化されています。
以下の設定を変更することでセキュリティ強度を変えることができます。
詳細はそれぞれの機種の使用説明書を参照してください。

SSID（ネットワーク名）

初期値は THETA＋製造機番（英字 2 文字＋数字 8 桁）＋.OSC となっています。
ネットワーク名を初期値から変更（ASCII 印字可能文字を利用可能）することで、THETA を利用していることを分かりにくくすることができます。

暗号化キー（パスフレーズ）

初期値は 8 文字ですが、8 文字以上 63 文字以内で変更することができます。
文字数や文字種類を増やす（ASCII 印字可能文字を利用可能）ことで、セキュリティ強度を上げることができます。暗号化キーの管理には充分注意してください。

CL（クライアント）モード接続・有線 LAN 接続（WebAPI 制御）

RICOH THETA / RICOH360 THETA を CL（クライアント）モードで利用することで、コンピューター、スマートフォンからルーター経由で制御することが可能です。 以下の設定を変更することでセキュリティ強度を変えることができます。

Copyright © Ricoh Co., Ltd. All Rights Reserved.

使用する場合は信頼できるアクセスポイントであることを確認してください。
詳細はそれぞれの機種の使用説明書を参照してください。

認証方式

ダイジェスト認証を採用しています。

ダイジェスト認証ユーザー名

初期値は THETA＋製造機番（英字 2 文字＋数字 8 桁）ですが、1 文字以上 32 文字以内で変更することができます。
文字数や文字種類を増やす（ASCII 印字可能文字を利用可能）ことで、セキュリティ強度を上げることができます。

ダイジェスト認証パスワード

ダイジェスト認証を使用する場合は最初に設定する必要があります。8 文字以上 63 文字以内で設定することができます。
文字数や文字種類を増やす（ASCII 印字可能文字を利用可能）ことで、セキュリティ強度を上げることができます。

暗号化方式

RICOH THETA / RICOH360 THETA を CL（クライアント）モードで接続する場合、ルーターの情報を RICOH THETA / RICOH360 THETA に登録する必要があります。
このとき接続するルーターの仕様に合わせて WEP, WPA/WPA2-PSK, WPA3-SAE から選択することができます。（WPA3 に対応していない機種もあります）
環境に合わせて適切なものを選択してください。特別な理由がない限り WPA2-PSK もしくは WPA3 の選択を推奨します。

公共機関などに用意されている公衆無線 LAN サービスの中には通信を暗号化していない場合があり、このような場合通信内容を第三者に盗み見られる可能性があります。
このような接続を利用する場合には、WebAPI による制御を利用しないことを推奨します。
RICOH360 クラウドサービスとの通信は暗号化されているので、問題ありません。

CL（クライアント）モード接続（RICOH360 クラウド制御）

RICOH360 クラウドサービスとの通信は TLS1.2/1.3 で暗号化することで、情報の盗聴等のリスクに対処しています。
参考：情報セキュリティ

CL（クライアント）モード接続（ライブストリーミング制御）

準備中

Copyright © Ricoh Co., Ltd. All Rights Reserved.

モバイルネットワーク制御

サポートしている SORACOM 社の回線は、外部から直接アクセスすることはできません。
※RICOH THETA Z1 はモバイルネットワーク通信に非対応です。
詳細はそれぞれの機種の使用説明書を参照してください。

Bluetooth 通信

Bluetooth に対応している機種では Bluetooth Low Energy に対応しており、Central としても、Peripheral としても動作することが可能です。Peripheral として接続した場合、BluetoothAPI によって色々な制御が可能です。
Peripheral として使用する場合は、スマートフォンなどの端末（以降端末とします）から接続を行う必要があります。
機種により対応しているセキュリティレベルは異なります。 少なくとも RICOH THETA / RICOH360 THETA と端末が直接操作できる状態であれば接続できますし、RICOH THETA での確認なしで接続できてしまうので、取り扱いには充分注意してください。
なお、バージョンにもよりますが Bluetooth は初期状態で有効になっています。API や本体操作で無効にすることができます。
詳細はそれぞれの機種の使用説明書を参照してください。

インタフェースセキュリティ

RICOH THETA / RICOH360 THETA は物理的なケーブル接続、本体操作により、RICOH THETA / RICOH360 THETA に保存されている画像･動画にアクセスすることが可能です。使用環境によっては、重要な情報が悪意を持って改ざん・窃取される可能性があります。重要な情報を守るため、以下の機能を活用してください。 ここでは USB 端子、本体操作ボタンについて記載します。

USB 通信

RICOH THETA / RICOH360 THETA は MTP (Media Transfer Protocol)に対応しています。また、機種によっては MSC (Mass Storage Class)にも対応しています。
MSC に対応している機種の場合、USB で端末と接続したときに MSC で動作するか、MTP で動作するかを選択することができます。
いずれの場合でも、USB ケーブルで端末と接続するだけで保存されている画像・動画に自由にアクセスできてしまうので、本機の取り扱いには充分注意してください。 詳細はそれぞれの機種の使用説明書を参照してください。

本体操作

本体操作により、WLAN の ON/OFF や電源 ON/OFF を行うことができます。

Copyright © Ricoh Co., Ltd. All Rights Reserved.

機種により、microSDXC カードを利用することも可能ですが、カードの蓋をロックすることはできません。
機種により、内蔵メモリのフォーマットを行うことも可能です。
機種により、API を利用することでボタン操作を禁止することも可能です。
詳細はそれぞれの機種の使用説明書を参照してください。

デバイスセキュリティ

ファームウェアの改ざん防止

RICOH THETA / RICOH360 THETA にはその機器の動作をつかさどるファームウェアと呼ばれるソフトウェアが内蔵されています。 このファームウェアが悪意を持った者により不当に改ざんされると正常な動作ができず、それらの機器を踏み台としたネットワーク内部への侵入や、不正なプログラムによる機器の破壊などが行われる危険性が発生します。
ファームウェアのアップデートは正しい手順で実施してください。

内蔵メモリに保存される静止画・動画ファイル（画像情報）

これらのデータには、画像情報、位置情報、ユーザーが入力した情報、デバイス構成情報などが含まれています。こういった情報が何らかの方法で窃取されることにより、情報漏えいが発生する可能性があります。
RICOH THETA / RICOH360 THETA の内蔵ストレージは暗号化されていません。また、保存されている画像情報は、前述のように USB で接続すると自由にアクセスできるので、RICOH THETA / RICOH360 THETA の使用環境や管理には充分注意してください。
また、MSC や microSDXC などを利用して、RICOH THETA / RICOH360 THETA で作成されないファイルを使用しないでください。

データの一括消去

RICOH THETA / RICOH360 THETA を廃棄する場合は保存したデータを消去してください。
機種により、本体操作で初期化することも可能です。
詳細はそれぞれの機種の使用説明書を参照してください。

Copyright © Ricoh Co., Ltd. All Rights Reserved.