RICOH Meeting 360 本体

セキュリティホワイトペーパー

Ver.1.0

作成 ： 2023年10月10日

株式会社リコー

目次

1. はじめに

このホワイトペーパーでは、RICOH Meeting 360 V1が提供するセキュリティ対策とその仕組みについて、概要を説明します。

2. RICOH Meeting 360 V1 について

RICOH Meeting 360 V1は、360°カメラ搭載一体型のマイクスピーカーです。360°カメラで会議室全体の様子を映し出すとともに、発言者を自動認識しクローズアップして表示することができます。
本章では、RICOH Meeting 360 V1の使用シーン、ユーザーが使用できる機能、管理者が設定/実行できる機能、RICOH Meeting 360 V1のネットワーク設定について説明します。

2.1. RICOH Meeting 360 V1 の使用シーン

RICOH Meeting 360 V1のシステムは、RICOH Meeting 360 V1の機器本体と、RICOH Meeting 360 V1にUSBケーブルで接続されたコンピューターで構成されます。
RICOH Meeting 360 V1は360°カメラで撮影した映像とマイクで集音した音声を、接続されたコンピューターに送信します。また、接続されたコンピューターの音声をRICOH Meeting 360 V1のスピーカーから流します。
RICOH Meeting 360 V1用のコンピューター向けアプリケーション「RICOH Meeting 360 Apps for Windows」（以下、PCアプリ）をコンピューターにインストールすると、PCアプリからRICOH Meeting 360 V1のカメラやネットワークの設定ができたり、RICOH Meeting 360 V1で撮影した映像のプレビュー表示を見たりすることができます。
RICOH Meeting 360 V1にネットワークを接続すると、機器のファームウェアをアップデートすることもできます。
図1にRICOH Meeting 360 V1の使用シーンを示します。

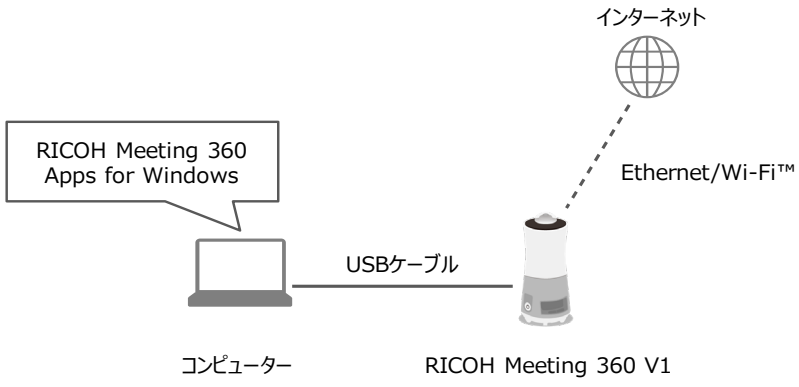

図 1　RICOH Meeting 360 V1 使用シーン

2.2. ユーザーが使用できる機能

ユーザーはRICOH Meeting 360 V1の以下機能を使用することができます。
各機能の詳細やここに記載されていない機能についてはユーザーマニュアルをご参照ください。

- 360°カメラ機能
- マイクスピーカー機能
- 発言者クローズアップ表示機能
- 映像レイアウト変更機能
- 機器・PCアプリのログの保存

2.3. 管理者が設定/実行できる機能

管理者は PC アプリを使用して RICOH Meeting 360 V1 の以下機能を設定/実行することができます。各設定の詳細やここに記載されていない設定についてはユーザーマニュアルをご参照ください。

- 機器名設定
- 操作音設定
- ネットワーク設定（有線ネットワーク設定、無線ネットワーク設定、自動構成/プロキシサーバー、ネットワーク診断）
- 機器ファームウェア更新
- 管理者パスワード設定
- 機器の設定の初期化

2.4. RICOH Meeting 360 V1 のネットワーク設定

RICOH Meeting 360 V1は、有線ネットワーク（Ethernet）、無線ネットワーク（Wi-Fi™）に接続し、LAN経由でインターネットにアクセスできます。インターネットアクセスを行うのは、以下の機能です。

- 機器ファームウェア更新
- ネットワーク診断
- 機器の時刻同期（必要に応じて自動的に実行されます）

また、RICOH Meeting 360 V1とコンピューターをUSBケーブルで接続すると、Ethernet over USBによって、コンピューターから機器搭載Webサーバーへのアクセスが可能となります。これは、以下の機能で使用します。

- PCアプリからの機器操作/設定
- コンピューターのWebブラウザからの機器搭載ソフトライセンス情報表示

RICOH Meeting 360 V1で使用可能なポートは、各ネットワークインターフェース（Ethernet、Wi-Fi™、Ethernet over USB）で必要とするものに限定されており、ユーザーによるポートの開閉はできません。使用可能ポートの詳細は表1、表2をご参照ください。
また、機器を経由した通信は禁止されており、コンピューターから機器を経由してインターネットにアクセスするようなことはできません。

表 1 RICOH Meeting 360 V1 使用ポート一覧（Ethernet、Wi-Fi™）

ポート番号	通信方向	説明
53/UDP・TCP	OUT	DNSサーバーアクセス
67/UDP	OUT	DHCPサーバーアクセス
68/UDP	IN	DHCPクライアントアクセス(レスポンス)
123/UDP	OUT	タイムサーバーアクセス(NTP)
443/TCP	OUT	機器ファームウェア配布サーバーアクセス(HTTPS)
-	IN	ICMPv4(Ping応答)

表 2 RICOH Meeting 360 V1 使用ポート一覧（Ethernet over USB）

ポート番号	通信方向	説明
80/TCP	IN	機器搭載Webサーバーアクセス(HTTP)
-	IN	ICMPv4(Ping応答)

3. RICOH Meeting 360 V1 のセキュリティ対策

RICOH Meeting 360 V1は、想定されるセキュリティ脅威に対し、以下のような対策を行っています。

- ネットワーク経由の攻撃防止
  ネットワーク機能を持つ機器は、ネットワーク経由で様々な攻撃を受ける可能性があります。
  RICOH Meeting 360 V1 は、ファイアウォールによって許可された必要最小限のネットワークアクセス以外は全てブロックして攻撃を防いでいます。

- 通信からの情報漏洩防止
  RICOH Meeting 360 V1 は、機器からのインターネットアクセスを行う際、HTTPS による通信の暗号化を行っており、盗聴を防いでいます。
  また、機器から送信するデータはファームウェア配布サーバーとの通信を確立するために必要な最小限の機器情報のみであり、映像・音声・ユーザーの個人情報・ログなどは含まれません。

- ファームウェア改竄防止
  機器のファームウェアが改竄されると、マルウェアが混入されたり、カメラ・マイクを使った会議ののぞき見など、機器の機能を悪用される可能性があります。
  RICOH Meeting 360 V1 は、ファームウェア更新を行う際、通信先が正規のファームウェア配布サーバーであることを検証した上で、暗号化された通信によって新しいファームウェアをダウンロードするので、改竄されたファームウェアを使った更新が行われることはありません。
  また、万一機器のファームウェアが改竄されたとしても、セキュアブート機能により改竄を検知して起動を停止するので、悪用されることはありません。

- 脆弱性対策
  RICOH Meeting 360 V1 に搭載されたソフトウェアについては、脆弱性情報の収集・確認を常時行っています。もし、外部からの攻撃が想定される脆弱性が発見された場合は、速やかに対策版ファームウェアのリリース、アドバイザリーの公開など適切な対応を行います。

4. 安全にお使いいただくために

セキュリティを確保するため以下の点に注意し、設置および設定を適切に行ってください。

1. 最新のファームウェアを適用する。
2. 最新のPCアプリを利用する。
3. 推測されにくいパスワードを設定する。
4. ファイアウォールで守られたネットワーク内で利用する。

改訂履歴

Version	改訂日	改訂内容
1.0	2023/10/10	新規作成

使用している固有名詞

●Windows は、米国 Microsoft Corporation の米国およびその他の国における商標または登録商標です。

●Ethernet は富士フイルムビジネスイノベーション株式会社の登録商標です。

●Wi-Fi™は、Wi-Fi Alliance の商標です。

●その他の会社名および製品名は、それぞれ各社の商号、商標または登録商標です。