# RICOH Interactive Whiteboard
# セキュリティーホワイトペーパー(V1.0)

<対象機種>
RICOH Interactive Whiteboard A6500-Edu

株式会社リコー

2022 年 3 月 2 日

# 目次

# 1 はじめに

このホワイトペーパーでは、RICOH Interactive Whiteboard（以下、RICOH IWB）が提供するセキュリティー対策とその仕組みについて、概要を説明します。

# 2 RICOH IWB について

RICOH IWBは、ホワイトボードアプリケーションを起動して手書き入力したり、コンピューターを含む外部映像機器の映像を表示したりできるシステムです。本章ではRICOH IWB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 IWBのホワイトボードアプリケーションが搭載されているシステムの構成、RICOH IWBが接続されるネットワークの構成について説明します。

## 2.1 RICOH IWB の使用シーン

RICOH IWBは、手書き入力できるシステムです。また、コンピューターを含む外部映像機器の映像を表示して、手書き入力もできます。RICOH IWBで作成したホワイトボードのページはUSBメモリーやクラウド型ストレージ上に保存する事ができます。また、様々なアクセスは管理者によって、アクセスを制限することができます。図1にRICOH IWBの使用シーンを示します。

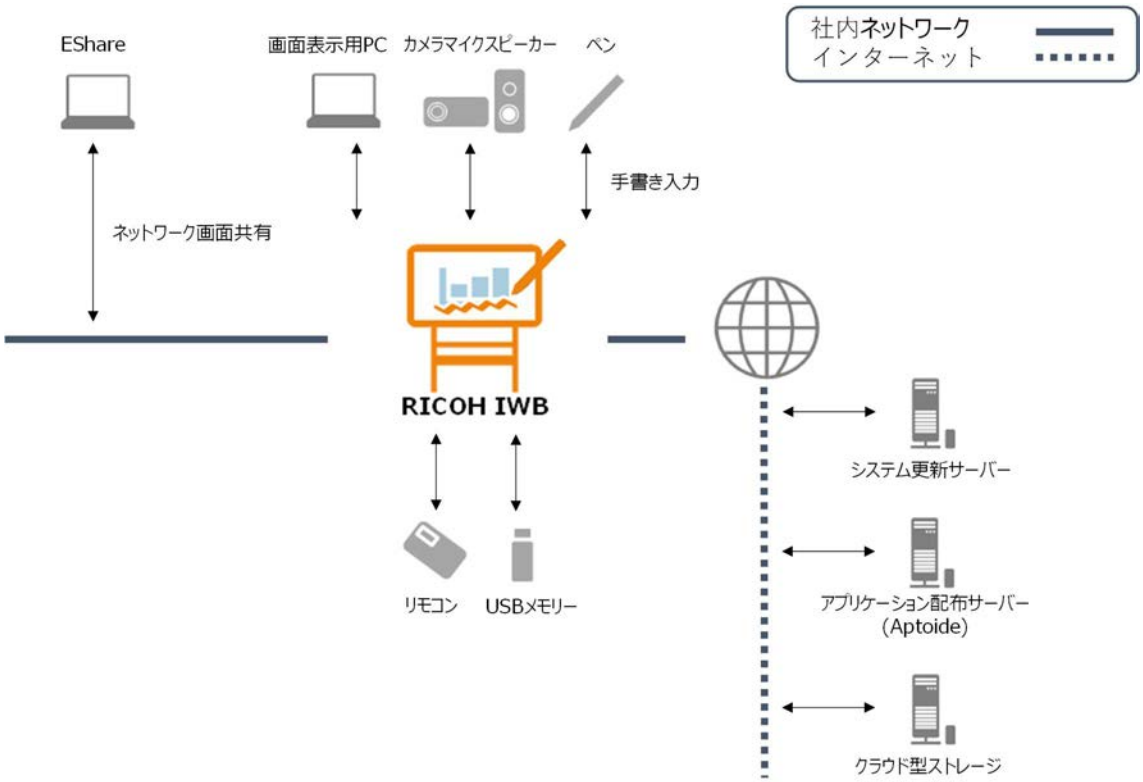


図 1 RICOH IWB 使用シーン

## 2.2 ユーザーが使用できる機能

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。

- ホワイトボード機能
- バージョン情報表示
- ホワイトボードページの保存/読み込み機能

  RICOH IWB 内のストレージに一時保存できます。また、USB メモリーやクラウド型ストレージを利用することもできます。
- EShare

  ネットワーク経由でPC/スマートフォン/タブレットの画面をホワイトボードに表示できます。また、ホワイトボードからPC/スマートフォン/タブレット画面の操作もできます。
- アプリケーションの追加

  Aptoide ストアから各種アプリケーションを追加できます。

  サードパーティー製のアプリのダウンロード、およびアプリの使用については、アプリの提供元をよく確認のうえ、お客様の責任で行ってください。

  本機を使用する環境によっては、不特定のユーザーが許可なくアプリをインストールしてしまう可能性があります。アプリの追加を制限するため、システム設定でアプリの追加を無効にしてご利用ください。（製品の初期値では、アプリ追加は無効になっています）

  ダウンロードしたソフトウェアの利用に際しては、お客様がご利用になる地域の法律に準拠してご利用ください。
- QR コード によるブラウザアクセス(閲覧)
- ブラウザによる、インターネットへの接続/WEBサービスの利用

## 2.3 管理者が設定/実行できる機能

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。

- 各種機能の有効/無効
- 管理者パスワード設定
- スーパーパスワード設定
- 画面ロックパスワード設定
- セキュリティー設定
- ネットワーク設定（有線/無線）
- 表示言語設定
- 日付と時刻設定
- 電源設定
- PC画像入力設定
- オーディオ設定
- 壁紙設定
- システム更新
- 工場出荷状態へのリセット

## 2.4 ネットワークの構成

ネットワークに接続する場合は以下のポートを使用します。詳細は表1のポートをご参照ください。なお、RICOH IWBではユーザーによるポートの開閉は許可されていません。

表 1 RICOH IWB 使用ポート一覧

| ポート番号 | 通信方向 |
|---|---|
| 4660/TCP | IN/OUT |
| 5555/TCP | IN/OUT |
| 8000/TCP | IN/OUT |
| 8121/TCP | IN/OUT |
| 25123/TCP | IN/OUT |
| 25123/UDP | IN/OUT |
| 39980/UDP | IN/OUT |
| 48689/UDP | IN/OUT |
| 54000/UDP | IN/OUT |
| 55954/UDP | IN/OUT |
| 56789/TCP | IN/OUT |
| 57395/TCP | IN/OUT |

# 3 セキュリティーの仕組み

RICOH IWBを使用する上で、以下のようなセキュリティーに対する脅威が想定されます。RICOH IWBではこれらの脅威について対策しています。なお対策詳細は3.1、3.2章をご参照ください。

- 情報漏洩

  脅威：

  記録・保存したデータに不正アクセスできてしまい、第三者に情報が漏洩してしまう。

  対策：

  RICOH IWBではスクリーンロック機能を用いて、第三者への情報漏洩を防いでいます。

- マルウェアの感染

  脅威：

  USBメモリーや、ネットワークを介して、不正なプログラムが実行されたり、インストールされたりする。RICOH IWBを仲介して、ネットワーク上の他の機器に不正アクセスしマルウェアが配布されてしまう。

  対策：

  RICOH IWBではセキュリティー対策ソフトウェアのインストールによりマルウェアの駆除を実行することができます。

- なりすまし

  脅威：

  管理者になりすまし、悪意をもってシステムを改竄したり、第三者に情報を漏洩したりする。

  対策：

  RICOH IWBではアクセス制限のある情報を取得するためには認証が必要です。情報にアクセス可能なユーザーにのみ認証情報を通知することで、意図せぬユーザーのシステム・情報へのアクセスを制限することができます。

- 改竄

  脅威：

  不正に改竄されたプログラムがシステムに悪意ある操作を実施し、情報漏洩やウィルスが実行・配布されてしまう。

  対策：

  システム更新時において、正しい更新ファイルであることを検証した上で適用しています。

  ※サードパーティー製アプリケーションの改竄検証は行いませんので、アプリケーションのダウンロード、およびアプリの使用については、アプリの提供元をよく確認のうえ、お客様の責任で行ってください。

- 脆弱性(セキュリティーホールを突いた悪意ある攻撃)

  脅威：

  一般に明らかになった脆弱性を放置することにより、悪意ある第三者から脆弱性を突いた攻撃が実施され、システムに悪影響を及ぼす可能性がある。

  対策：

  RICOH IWBではこれらの脆弱性が発覚した場合は、ファームウェアアップデートを用いて対策する体制を整えています。

  また、RICOH社内にて脆弱性情報を収集する体制を整えています。

## 3.1 本体でのセキュリティー対策

**情報漏洩防止**

情報漏洩防止では、情報漏洩・なりすましの脅威に対策しています。

ホワイトボードのページは、意図せず保存されることは無く、スタンバイ状態になると自動消去されます。ユーザーが電源ボタンを押下するか、ホワイトボードを使用しないで自動スタンバイ時間が経過すると、スタンバイ状態へ移行します。

スクリーンロック機能を使用すると、RICOH IWBの利用者を限定することができます。

システムの各種設定を実施する管理者用設定メニューに入るには、パスワード認証が必要です。

**マルウェア対策**

セキュリティー対策ソフトウェアをインストールすることにより、ウィルス定義ファイルに記載されているウィルスの駆除が実行されます。

**なりすまし対策**

適切にパスワードを設定・管理していただく事で、意図せぬユーザーのシステム・情報へのアクセスを制限することができます。登録されたパスワードは外部から参照できないように記録されます。

**不正改竄防止**

不正改竄防止では、改竄の脅威に対策しています。

システム更新時において、正しい更新ファイルであることを検証した上で適用しています。

**脆弱性対策**

脆弱性対策では、脆弱性の脅威に対策しています。

RICOH IWBは十分セキュアに設計されておりますが、もしもRICOH IWBに組み込んでいるシステムで脆弱性が発見された場合には、リコーはファームウェアのアップデートを速やかに提供します。（お客様が構築されたITシステム（PC、ソフトウェアなど）に関してはセキュリティーを担保するものではありません。）。

**機能制限**

管理者用設定メニューのセキュリティー設定では、ユーザーのセキュリティーポリシーに合わせた運用ができるようにアプリケーションの追加に関して機能制限をかけることができます。

## 3.2 ネットワーク使用時のセキュリティー対策

**情報漏洩防止**

情報漏洩防止では、情報漏洩・なりすましの脅威に対策しています。

ネットワーク通信に関する設定として、RICOH IWBの動作に必要なポートを除くインバウンド通信をすべて閉じております。

自動システム更新ではシステム更新用ファイルのみを取得しており、RICOH IWB内の個人情報やユーザーが作成したデータを送信することはありません。

**不正改竄防止**

不正改竄防止では、改竄の脅威に対策しています。

RICOH IWBでは自動システム更新の際、システム更新ファイルの正当性を検証し更新ファイルが改竄されていないか確認します。

**不正アクセス防止**

不正アクセス防止では、情報漏洩・なりすましの脅威に対策しています。

RICOH IWBでは、既定の初期管理者パスワードは設定されておらず、初回起動時に必ず管理者パスワードを設定させることにより、既定パスワードを用いた不正アクセスを防止しています。

**ネットワークセキュリティー**

RICOH IWB では、無線セキュリティーとして WPA2-PSK に対応しています。WPA2 では認証による接続制限に加えて、高度な暗号化通信により、盗聴/傍受/改竄の対策もされます。

QR コード によるブラウザアクセス(閲覧)を利用する際は、通信経路が暗号化されていませんので、機密情報を扱わないように運用ください。

**機能制限**

アクセス制限されたProxy サーバーと組み合わせて運用していただくことで、意図せぬ外部サイトにアクセスする事を防止できます。

## 4 安全にお使いいただくために

機器のセキュリティー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. 最新のアプリケーションを利用する。
3. 推測されにくいパスワードを設定する。
4. ファイヤーウォールで守られたネットワーク内で利用する。
5. 消し忘れによる情報漏洩を防ぐため、使用後はホワイトボードアプリを終了する。
6. のぞき見による情報漏洩を防ぐため、利用時は周囲に配慮する。
7. 追加するアプリケーション/利用するWEBサービスの仕様(認証/通信の暗号化強度等)を十分に確認する
8. マルウェア対策/フィルタリング/などのセキュリティー対策アプリを導入する

## 参考資料

Interactive Whiteboard を安全にご利用いただくために
https://www.ricoh.co.jp/iwb/security

製品・サービスを安全にお使いいただくために
https://jp.ricoh.com/security/products

## 使用している固有名詞

- Android は Google LCC.の商標です。
- WPA2 は Wi-Fi Alliance の商標です。
- QR コードは(株)デンソーウェーブの登録商標です
- その他、本ドキュメントに記載の会社名および製品名・ロゴマークはそれぞれ各社の商号、商標または登録商標です。