

---

# RICOH Interactive Whiteboard セキュリティホワイトペーパー(V1.1)

---

<対象機種>

RICOH Interactive Whiteboard A6510 / A7510

株式会社リコー  
リコーデジタルプロダクツ BU エッジデバイス事業本部 SC 事業部 エッジデバイス事業推進室

2024 年 10 月 09 日

## 目次

---

|                               |    |
|-------------------------------|----|
| 1 はじめに .....                  | 3  |
| 2 RICOH IWB について .....        | 4  |
| 2.1 RICOH IWB の使用シーン .....    | 4  |
| 2.2 ユーザーが利用できる機能 .....        | 5  |
| 2.3 管理者が設定/実行できる機能 .....      | 6  |
| 2.5 ネットワークの構成 .....           | 7  |
| 3 セキュリティーの仕組み .....           | 8  |
| 3.1 本体でのセキュリティー対策 .....       | 10 |
| 3.2 ネットワーク使用時のセキュリティー対策 ..... | 11 |
| 3.3 機能ごとのセキュリティーに関する留意点 ..... | 12 |
| 4 安全にお使いいただくために .....         | 14 |
| 参考資料 .....                    | 15 |
| 改訂履歴 .....                    | 16 |
| 使用している固有名詞 .....              | 17 |

## 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製品本体やUSBメモリーに保存する事ができます。また、Webブラウザを利用したインターネット接続やWebサービスを利用することもできます。さらに、様々なアクセスは管理者によって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。

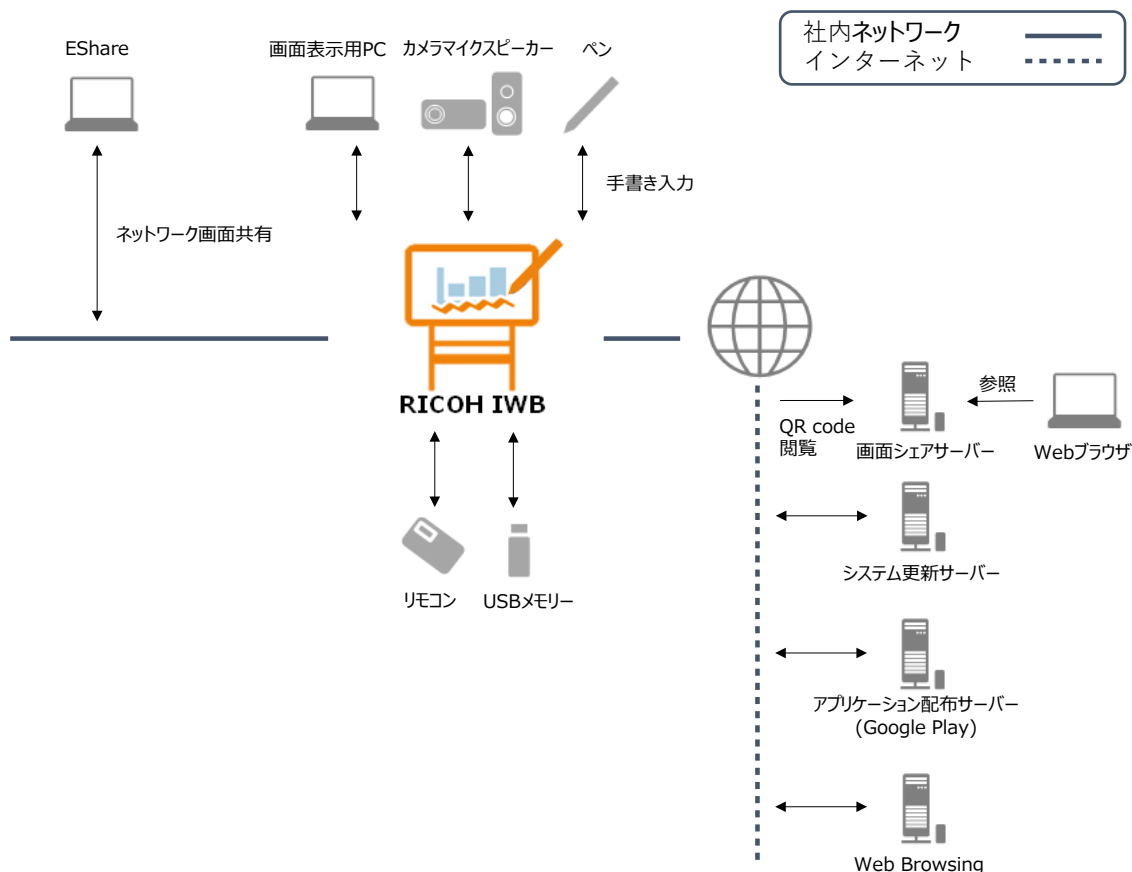


図 1 RICOH IWB 使用シーン

## 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
- 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

Google Play 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、インストールロック設定を有効にしてご利用ください。（製品の初期値では、インストールロック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 によるホワイトボード／アノテーション画面共有（閲覧）

ファイヤーウォールによりインターネットへの接続が制限されている環境では、この機能を利用することができない場合があります。
- 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
- Google アプリケーション

本製品はGoogle EDLA認証(Enterprise Devices Licensing Agreement)を取得していますので、YouTubeやChromeなど多様なGoogleアプリケーションを利用する事ができます。

## 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
- ・ アプリロックパスワード設定
- ・ インストール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

## 2.5 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   |
|-----------|--------|
| 8000/TCP  | IN/OUT |
| 8121/TCP  | IN/OUT |
| 8600/TCP  | IN/OUT |
| 8700/TCP  | IN/OUT |
| 25123/TCP | IN/OUT |
| 25124/TCP | IN/OUT |
| 51010/TCP | IN/OUT |
| 51020/TCP | IN/OUT |
| 51030/TCP | IN/OUT |
| 51040/TCP | IN/OUT |
| 51060/TCP | IN/OUT |
| 52020/TCP | IN/OUT |
| 52025/TCP | IN/OUT |
| 52030/TCP | IN/OUT |
| 53000/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、Google Play プロテクトによりアプリやデバイスが有害な動作を引き起こさないかチェックしています。また、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もできます。

- 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。認証に必要な情報をアクセス許可されたユーザーにのみ通知することで、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は、Google Play プロテクトにより安全性を確認した上でインストールする仕組みを搭載しておりますが、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。（要確認）

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、パスワード認証を設定する事ができます。これにより、機器を安全に利用していただくことができます。

### マルウェア対策

セキュリティ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を担保するものではありません。）。

### 機能制限

設定メニューのAdvanced設定では、ユーザーのセキュリティ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起動や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。

自動システム更新は、インターネット経由でシステム更新用サーバーからシステム更新用ファイルを取得します。更新用サーバーとの通信路は暗号化されているため、不正に通信内容を傍受されることはありません。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

RICOH IWB では、無線セキュリティとして 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。

外部サーバーとの通信を行うアプリケーション（EShare、ホワイトボード、アノテーション、など）は、全て https による暗号化通信を行っているため、安全にご利用いただく事ができます。

### 3.3 機能ごとのセキュリティに関する留意点

以下の機能を使用する上で、セキュリティに対する脅威が想定されます。必ず以下に記載の運用方法を守ってください。

#### アプリケーション追加機能

追加するアプリケーションによっては、RICOH IWB機器内部のファイルにアクセスできる場合があります。この場合は、RICOH IWB機器内の情報保護は保証されませんので、RICOH IWB機器内に情報を残さない、利用者を限定するなど、RICOH IWB機器内の情報が流出しないように運用してください。

また、追加するアプリケーションが大量のデータを保存するアプリケーションである場合、ファイルの保存によりディスク使用量などに影響が出て、システムが正常に動作しなくなる可能性があります。大量のデータを保存するアプリケーションを使用する場合はシステムの動作は保証されませんので、大量のデータが本体に保存されないように運用してください。

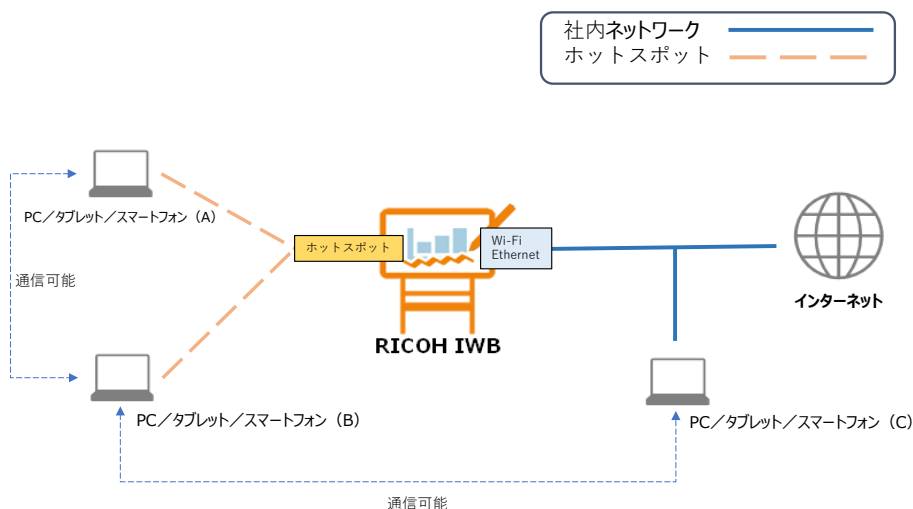
また、追加するアプリケーションがインターネット通信を行うアプリケーションである場合、通信が暗号化されていない可能性がありますので、アプリケーションの仕様をご確認の上で運用してください。

#### ホットスポット機能

RICOH IWBはホットスポット機能を搭載しています。

ホットスポットはネットワークブリッジとして動作しますので、以下のネットワーク接続が可能になります。ご利用にあたっては十分にご注意いただき、不要な場合は設定をOFFにして運用してください。

- ・ホットスポットを用いて接続した機器同士： 下図の(A)と(B)
- ・ホットスポットを用いて接続した機器と社内ネットワークに接続している機器： 下図の(B)と(C)
- ・ホットスポットを用いて接続した機器とインターネット： 下図の(A) or (B)とインターネット



## LANポート

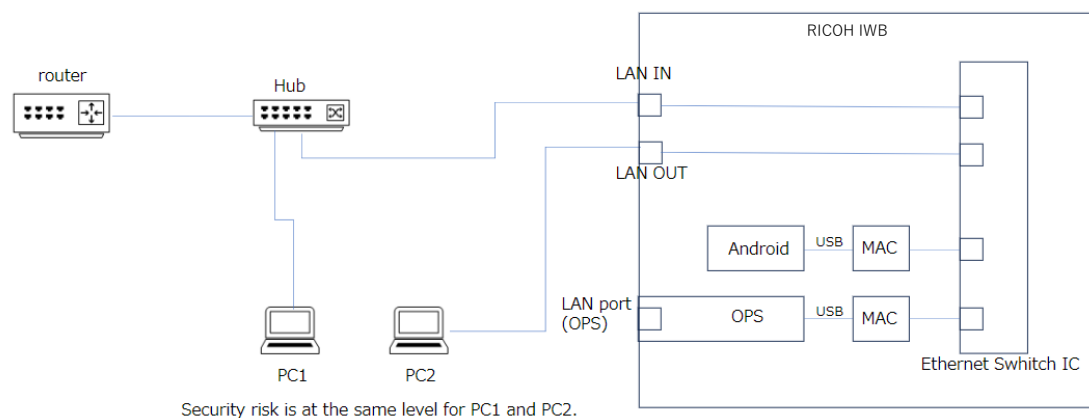
RICOH IWBは標準で2つのLANポートを搭載しています。

※OPSを装着されている場合は、さらにもう1つのLANポートを利用することができます。

LAN IN と LAN OUT のポートは、名称は異なりますが同一機能を備えています。そのため、どちらのポートを利用してネットワーク接続することができます。

OPS用のLANポートは、LAN IN / LAN OUT ポートとは独立しているため、どちらかを選択して利用することができます。

LAN IN / LAN OUT / LAN PORT(OPS)、いずれを利用する場合でも、ネットワークセキュリティは同一レベルとなります。※いずれかのポートのみセキュリティリスクが大きくなることはありません。



## 4 安全にお使いいただくために

---

機器の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. 最新のアプリケーションを利用する。
3. 設定アプリにパスワードロックをかける。
4. 推測されにくいパスワードを設定する。
5. 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。
6. 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。
7. 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。
8. 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
9. マルウェア対策/フィルタリング/などのセキュリティ対策アプリを導入する
10. ホットスポット機能を利用されない場合は、設定を無効にしてご利用ください。

## 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>

## 改訂履歴

---

### V1.1

---

| 年月日        | 改訂概要                                                      |
|------------|-----------------------------------------------------------|
| 2024-10-09 | 外部サーバー、ホットスポット機能、LAN ポート機能に関する記載を追加。<br>PMT レビューの指摘事項を反映。 |
|            |                                                           |
|            |                                                           |

### V1.0

---

| 年月日        | 改訂概要 |
|------------|------|
| 2024-05-20 | 新規作成 |
|            |      |
|            |      |



## 使用している固有名詞

---

- Android
- Google
- WPA2
- EShare
- McAfee
- QR コード
- ウイルスバスター
- Trend Micro
- YouTube
- Amazon