# リコーインタラクティブホワイトボード
# セキュリティーホワイトペーパー(V2.3)

株式会社リコー
2018 年 10 月 15 日

## 目次

# 1 はじめに

このホワイトペーパーでは、RICOH Interactive Whiteboard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 全体概要

RICOH Interactive Whiteboard（以下、RICOH IWB）は、コンピューターを含む外部映像機器の映像をホワイトボードに表示して手書き入力できるシステムです。このホワイトボードは、プリンターで印刷することができ、PDFファイルに変換してメール送信、USBメモリーや共有フォルダーに保存することができ、ネットワークで接続した別のRICOH IWBや専用ソフトウェアをインストールしたコンピューターと共有することができます。コンピューターのWebブラウザーを使うとホワイトボードをネットワーク経由で閲覧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。

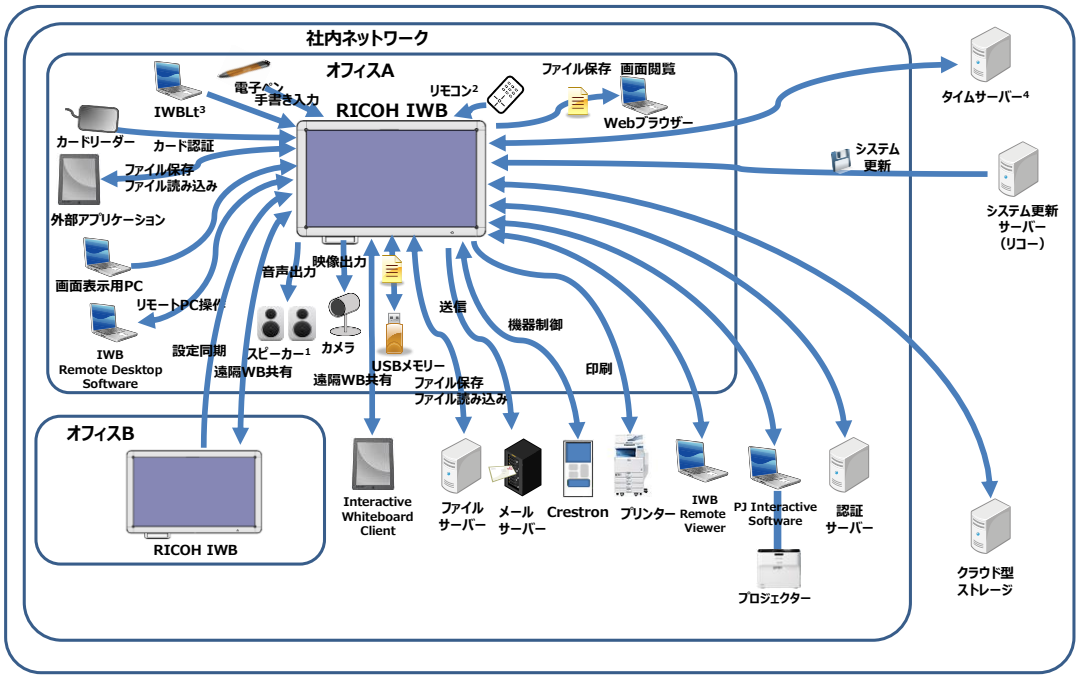


図 1 RICOH IWB 使用シーン

[1] RICOH IWB D5520/D6510は内蔵のマイク・スピーカー（音声入出力）です。

[2] RICOH IWB D5510を除く。

[3] RICOH IWB D5520/D6500/D6510/D8400に限って使えます。一部機能に限って利用できます。

[4] 日付と時刻の設定で「インターネット時刻サーバーと同期する」の設定を有効にしたときのみアクセスします。

RICOH IWBは、ファイヤーウォール内の社内ネットワークに接続して使用することを前提に設計されています。

## 2.1 ユーザーが使用できる機能

ユーザーは以下の機能を使用できます。

- ホワイトボード機能
- バージョン情報表示
- 著作権情報表示
- ホワイトボードページのメール送信機能、印刷機能
- 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（一時保存）
    PCのWebブラウザーからPDFファイルとしてダウンロードできます。
  - USBメモリー
  - クラウド型ストレージ
- 遠隔ホワイトボード共有機能
- PCのWebブラウザーからのホワイトボード閲覧
- IWB Remote Desktop Software：
  本ソフトウェアをPCにインストールすると、ネットワーク経由でPC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画面の操作もできます。
- RICOH Interactive Whiteboard Client（以下、IWB Client）：
  本ソフトウェアをインストールしたPCやタブレット端末からホワイトボードを閲覧、直接書き込みできます。
- 外部アプリケーション接続機能：
  RICOH カンタン入出力などの外部プリケーションと接続できる機能です。
  また、本機能を使用するアプリケーションを開発しホワイトボードを共有および制御ができます。
- RICOH Interactive Whiteboard Lt for Windows：
  RICOH IWB D5520/D6500/D6510/D8400に本ソフトウェアをインストールしたPCを接続することにより、簡易版RICOH IWBの機能を使用できます。
- ユーザー認証機能：
  リコー 個人認証システム AE2[1]を使ったユーザー認証ができます。
- アプリケーション連携機能：
  RICOH IWBに追加したアプリケーションを使用できます。

[1] V2.3 時点でリコー個人認証システム AE2 V1.4.000 に対応しています。

- Bluetooth接続機能[1]：
  Bluetoothでマイク・スピーカーと接続できます。

## 2.2 管理者が設定/実行できる機能

管理者は、管理者用設定メニューを使用して以下の設定、実行ができます。

- 各種機能の有効/無効
- 管理者用パスワード設定
- セキュリティー設定
- ネットワーク設定（有線/無線[2]）
- 一時保存設定
- 自動一時保存ファイルの管理
- 印刷、メールサーバー設定
- メールアドレス帳設定
- 公開アドレス帳設定
- ライセンス設定
- 遠隔ホワイトボードのコンタクトリスト設定
- デバイス管理設定（Bluetooth）
- 共有フォルダーリスト設定
- Crestron制御システム設定
- ユーザー認証設定
- 機器設定同期設定
- 機器設定のインポートとエクスポート
- ログの収集
- システム更新
- 工場出荷時状態への初期化

[1] RICOH IWB D5520/D6510 のみ対応しています。

[2] RICOH IWB D5520/D6500/D6510/D8400 のみ対応しています。

# 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。

- 情報漏洩

  記録・保存したデータに不正アクセスできてしまい、第三者に情報が流出してしまう。あるいは、遠隔ホワイトボード時に、共有画面に不正にアクセスできたり、他者になりすましてアクセスし、第三者に情報が流出してしまう。

- マルウェア（悪意のあるソフトウェア）の実行

  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。あるいは、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たり、ウィルスが配布されてしまう。

ここでは、RICOH IWBの本体と遠隔ホワイトボードにて実施しているセキュリティー対策について、それぞれ説明します。

## 3.1 本体でのセキュリティー対策

**情報漏洩防止**

ホワイトボードのページは、ホワイトボードを終了するか、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、消去されます[1]。ホワイトボードのページはPDFファイルに変換して送信、保存することができますが、PDFファイルには権限パスワード、開くパスワード、編集禁止を設定できます。ただし、開くパスワード、編集禁止、印刷禁止が設定されたPDFはホワイトボードに読み込むことはできません。

ホワイトボードのページは、本体のSSDにファイルとして一時保存することができます。一時保存したファイルは、一時保存時に指定した会議コードを入力すると、ホワイトボードに読み込むことができます。管理者用設定メニューで設定された保存期間を過ぎると一時保存ファイルは自動的に消去されます。RICOH IWBは、関係者しか入ることのできない社内で使用することを前提に設計されているため、盗難に対する対策であるSSDのパスワードは設定されていません。

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。管理者用設定メニューで登録されたすべてのパスワードは、暗号化されて本体のSSDに保存されます。さらに、プログラムの解析により暗号化方式などのセキュリティー情報が漏洩するのを防止するために、ホワイトボード内部のプログラムを難読化しています。

---

[1] [起動時に前回のホワイトボードを復元する]機能を有効にした場合、指定した時間以内に RICOH IWB を起動するとホワイトボードのページは復元されます。

**ウィルス対策**

ホワイトリスト方式のセキュリティー対策ソフトウェアにより、信頼されたプログラム以外の起動やインストールはできません。外部からのマルウェアを実行しようとしても、ホワイトリストにないため実行できません。USBメモリーを接続した場合も、USBメモリーの自動起動をオフにしているためUSBメモリー上のプログラムが勝手に起動することはありませんし、USBメモリー上からプログラムを起動しようとしてもRICOH IWB上にファイルがコピーされてもホワイトリストに登録されていないプログラムは起動することができません。

**使用履歴**

使用履歴を記録し、ログとして出力する機能を提供しています。システムの起動・停止や動作記録、遠隔ホワイトボードの開始・終了などの記録を保存しています。ログは管理者のみが収集できます。

**セキュリティーポリシー**

管理者用設定メニューのセキュリティー設定では、メール送信、パスコード、遠隔ホワイトボード、Webブラウザー接続、USBメモリーに関しRICOH IWB本体に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**

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 NetBIOS over TCP/IP は無効にしています。RICOH IWB は社内ネットワークに接続して使用することを前提に設計されているため、遠隔ホワイトボード中の通信や本体 Web サーバーアクセスの通信は社内ネットワーク外に出ることはなく、ネットワーク通信上の脅威はないものとし、暗号化処理はしていません。遠隔ホワイトボードの開催端末は、参加端末でのファイル保存、印刷、メール送信、一時保存を禁止でき、遠隔ホワイトボード終了時には、参加端末のホワイトボードを消去できます[1]。遠隔ホワイトボード参加時は、不正なユーザーからのアクセスを抑制するためパスコードによる認証方式を提供しています。

パスコードは、本体画面にのみ表示され、会議に参加した人しか知ることはできません。パスコードは、会議セッション毎（ホワイトボードの終了やスタンバイ/電源オフ毎）に生成されるランダムな4桁～10桁の数字を使用できます。

[1] 遠隔ホワイトボード開催オプションで[参加ホワイトボードの機能を制限する]機能を有効にした場合のみです。

IWB Clientによる遠隔ホワイトボードへの参加、Webブラウザーによる遠隔ホワイトボードの閲覧、IWB Remote Desktop SoftwareによるPC表示・操作においても、パスコードによる認証が必要です。

メール送信は、SMTP認証とSTARTTLS方式に対応しています。

自動システム更新は、インターネット経由でリコーが管理する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。システム更新用ファイルは暗号化され、HTTPSプロトコルにより通信路も暗号化されているため、なりすまし、または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取得のみをおこなっており、RICOH IWB内の情報を送信することはありません。システム更新用サーバーは専用サーバーを使用しており、リコー製品以外はアクセスすることができません。

**不正改竄防止**

自動システム更新では、ホワイトボード・アプリケーション起動時に、リコーが管理しているシステム更新用サーバーをチェックします。システム更新用ファイルがある場合には自動的にダウンロードし、ユーザーにはシステム更新するか否かを確認します。自動システム更新の際、システム更新用ファイルの正当性がチェックされます。管理者は、管理者用メニューより、自動システム更新を無効にすることができます。

**Webブラウザーからの管理者用設定メニューのアクセス権管理**

誤ってインターネット回線に接続される事故を想定して、工場出荷時と同じ管理者用パスワードの場合はWebブラウザーからの管理者用設定メニューが使用できないよう設計されています。使用する場合は、工場出荷時から管理者用パスワードを変更することが必要です。

## 使用している固有名詞

●Windows, Active Directory, Windows Defender, Windows Update 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。
●Adobe PDF は、アドビシステムズ社の米国ならびに他の国における商標または登録商標です。
●Bluetooth は、米国 Bluetooth SIG, INC.の米国ならびにその他の国における商標または登録商標です。
●Crestron は、米国 Crestron Electronics, Inc.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。