RICOH Interactive Whiteboard
セキュリティーホワイトペーパー(V4.5/V3.10)

<対象機種>
RICOH Interactive Whiteboard Controller Type3a / Type3 / Type2

株式会社リコー
2023年9月11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、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。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プリンターで印刷することや、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、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。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。

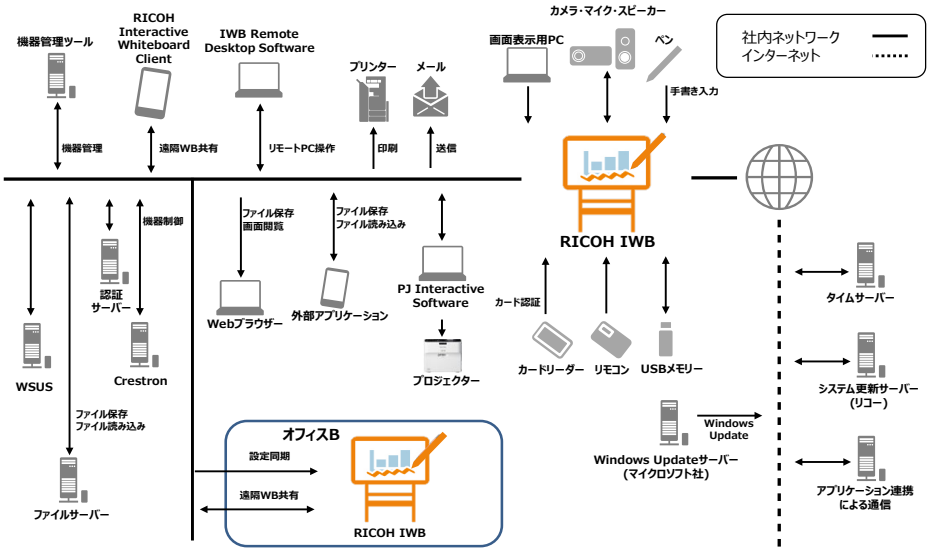

図 1 RICOH IWB 使用シーン

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/著作権情報表示
- ホワイトボードページのメール送信、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内のストレージに一時保存でき、PCからWebブラウザー経由でPDFファイルとしてダウンロードできます。また、USBメモリーや共有フォルダーを利用することもできます。
- 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
  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、直接書き込みができます。
- 外部アプリケーション接続機能
  外部アプリケーションを使用してネットワーク経由でホワイトボードを共有できます。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。
- ユーザー認証機能
  リコー 個人認証システム AE2[1]/SLNX[2]/AD/LDAP 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。
- Bluetooth接続機能
  Bluetooth でマイク・スピーカーと接続できます。

[1] V4.2/V3.8 時点でリコー個人認証システム AE2 V1.5.4 に対応しています。

[2] V4.2/V3.8 時点で、RICOH Streamline NX V3.4 に対応しています。

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
- セキュリティー設定
- ネットワーク設定（有線/無線）
- 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暗号化設定
- 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
- 設定の初期化
- 自動システム更新
- Windows Update
- Windows Defenderによるウィルススキャン
- ルート証明書のアップロード
- クライアント証明書のアップロード
- サーバー証明書のアップロード
- WebブラウザーとRICOH IWB間のSSL/TLS通信設定
- SNMP設定
- SSD暗号化[1]

[1] V3.1-V3.x のみ。V4.0 以降は設定を持たず、常時暗号化されている。

2.4 ネットワークの構成

RICOH IWBは社内ネットワークに閉じて使用することを前提としています。
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[1]
25/TCP	OUT
53/UDP	OUT
67/UDP	OUT
68/UDP	IN
80/TCP	IN
80/TCP	OUT
123/TCP	OUT
161/UDP	IN
389/TCP	OUT
443/TCP	IN
443/TCP	OUT
445/TCP	OUT
515/TCP	OUT
5355/UDP	OUT
9100/TCP	OUT
18080[2]/TCP	OUT
18443/TCP	OUT
41794/TCP	IN/OUT
45000/TCP	IN/OUT
45010/TCP	IN/OUT
50000/TCP	IN/OUT
50001/TCP	IN/OUT
50002/TCP	IN/OUT
50003/TCP	IN
50004/TCP	IN/OUT
50005/TCP	IN/OUT
50006/TCP	IN/OUT
50010/TCP	IN/OUT
61616/TCP	IN/OUT
49513～65535[3]/TCP	IN/OUT

[1] OUT のポート番号は宛先ポート番号を示します。
[2] 初期設定でのポート番号であり、変更されることもあります。
[3] 記載のエフェメラルポートのうち空いているポートを自動的に使用します。

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。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**
  - 『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。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や他者になりすましてアクセスされ第三者に情報が漏洩してしまう。』
  - RICOH IWBではユーザー認証を用いて、第三者への情報漏洩を防いでいます。また、万が一情報が漏洩した場合を考慮し、SSDの暗号化[1]に加えて、記録・保存したデータ単体でも暗号化しています。

- **マルウェアの感染**
  - 『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。』
  - RICOH IWBでは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、許可されたアプリケーションのみ動作します。また、万が一許可されていないマルウェアが保存・インストールされた場合、ブラックリスト方式のセキュリティー対策ソフトウェアによりマルウェアの駆除が実行されます。

- **なりすまし**
  - 『意図せぬユーザーがRICOH IWBを使用した結果、意図せずシステム変更されたり、第三者に情報が漏洩したりする。』
  - 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**
  - 『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。』
  - RICOH IWBでは実行プログラムが不正に改竄されていないか検証します。また、不正なプログラムへの改竄を抑制するために、プログラムを難読化しています。

- **脆弱性(セキュリティーホールを突いた悪意ある攻撃)**
  - 『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。』
  - 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やWindows Update機能などを用いて対策する体制を整えています。

[1] SSD 暗号化が有効な場合（V3.1-V3.x）

3.1 本体でのセキュリティー対策

- **システムの保護**

  システムの保護では、なりすまし・マルウェアの脅威に対策しています。

  RICOH IWBは専用のシステムであるため、ユーザーの操作はホワイトボード・アプリケーションに限定しています。さらに、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不正なプログラムの実行もできません。万が一ウィルスが進入してもブラックリスト方式のセキュリティー対策ソフトウェアにより駆除されます。

- **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 [1]。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。

  ホワイトボードのページはPDFファイルに変換してメール送信、保存することができます。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。

  ユーザー認証機能を使用すると、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。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。

  ホワイトボードのページは、本体のSSDに一時保存することができます。一時保存したページ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上に保存されているPDFファイルは暗号化が施されており、SSDから直接PDFファイルを読み込んでもPDFファイルを開くことはできません。

  RICOH IWBは、コントローラーに装着されているTrusted Platform Module(TPM)を使用してSSDが暗号化されています。このため、万が一意図せずSSDが転用されてもSSD内のデータが読み取られることはありません。（ただし、V3.1-V3.xでは既定では暗号化されていません。管理者用設定でSSD暗号化を有効にする必要があります。V3.1-V3.xでSSD暗号化を有効にした場合、回復キーを確認することができます。この回復キーは、お客様が故障時の解析をリコーに依頼する場合、TPMが破損して自動復号に失敗した場合、Windowsの構成変更が発生した場合の回復手段として必要です。例えば、Windows UpdateなどによりWindowsの構成変更が意図せずに起きることがあります。その場合は、回復キーを入力しない限りRICOH IWBが利用できなくなることがありますので、回復キーは必ず控えるようにしてください。）

[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。

- **マルウェア対策**

  マルウェア対策では、マルウェアの脅威に対策しています。

  RICOH IWBでは、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のみ起動、インストールが可能です。ホワイトリストにはOSのソフトウェアとRICOH IWBの実行に必要なアプリケーションのみを登録しています。アプリケーションの実行制御をすることで外部からのマルウェア実行、不正なアクセスによるファイル変更を防止することができます。

  また、USBメモリー上の実行ファイルが自動実行されることはありません。

  ブラックリスト方式のセキュリティー対策ソフトウェアにより、ウィルス定義ファイル(ブラックリスト)に記載されているウィルスの駆除が実行されます。ブラックリストはWindows Update時に更新されるため、最新のウィルスに対応することができます。

  Windows Updateはマイクロソフト社から新規のWindows Updateが通知されてからリコーで適用検証を実施し、30日後に適用されます。万が一、適用検証時にシステムに致命的問題が発生してすぐに解決できない場合、Windows Updateの自動更新機能を停止するソフトを配信することがあります。このようなケースが発生した場合は、随時リコーホームページにてお知らせ致します。

- **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。

  不正改竄に対しては、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アプリケーションの実行制御をすることで、マルウェアや悪意ある改竄がされたアプリケーションは実行されません。また、不正なプログラムへの改竄を抑制するために、プログラムを難読化しています。

  また、システム更新時においても、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は組み込み機器であり、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。）このRICOH IWBファームウェアアップデートの適用は、「自動システム更新機能による自動更新」もしくは「管理者による手動ファームウェアアップデート」の2種類があり、お客様で手法を選択することが可能です。

  また、RICOH IWBでは動作プラットフォームであるWindowsへの脆弱性対策はWindows Updateにより、実施されます。Windows Updateの適用済みバージョンはログから確認できます。

- **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。また、ユーザー認証が有効になっている場合は、ユーザーのログイン/ログアウト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。

- **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メモリーの使用に関して
  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**

  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NetBIOS over TCP/IPは無効にしています。また、有線・無線の各種ネットワークセキュリティーにも対応していますので、適切にご利用いただくことで安全にネットワークに接続していただくことができます。
  遠隔ホワイトボード中のRICOH IWB同士の通信およびRICOH IWBとRICOH Interactive Whiteboard Client間の通信は、設定で暗号化することが可能です。また、Webブラウザーからの管理者設定メニューへのアクセスも同様に、機器設定や管理者パスワード情報を含むためSSL/TLS通信に切り替えることでより安全性の高い運用も可能です。RICOH IWBでは自己署名証明書を標準でインストールしていますが、必要に応じてお客様が準備したサーバー証明書を利用することもできます[1]。RICOH IWBとIWB Remote Desktop Software間の通信は設定によらず暗号化されます。
  また、遠隔ホワイトボード機能、自動システム更新機能では以下のセキュリティー対策を実施しています。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[2]。
  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、通信路も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内の情報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。RICOH IWBではホワイトボード・アプリケーション起動時に、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。

---

[1] 自己署名証明書を用いた SSL/TLS 通信はブラウザーから警告が表示されることがあります。これは自己署名証明書が信頼された認証局からの署名を付与されていないためです。認証局から署名された証明書はお客様自身がお客様の環境に合わせて作成する必要があります。

[2] 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。

- **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。
  ネットワークからの不正な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。
  RICOH Interactive Whiteboard Clientによる遠隔ホワイトボードへの参加とIWB Remote Desktop SoftwareによるPC表示・操作においては、パスコードによる認証が必要です。RICOH IWB同士の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においては、パスコードによる認証の有効/無効を設定することが可能です。

- **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（パーソナル/エンタープライズ）に対応しています。また、ネットワーク認証として802.1Xに対応しており、認証が必要なネットワークにIWBを参画することが可能です。なお、RICOH IWBでは特定ドメインには参加することはできません。

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。（IWB Remote Desktop Software、RICOH Interactive Whiteboard Client、およびアプリケーション連携機能で追加するアプリケーションなど）
3. 最新のWindows Updateを適用する。
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、会議終了後はホワイトボードを終了する。
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。

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。
- PDFはAdobe PDF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。
- WPA2は、Wi-Fi Allianceの商標です。
- iOSは、米国およびその他の国における商標またはシスコの登録商標であり、ライセンスのもとに使用されます。
- 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。