RICOH eWhiteboard
セキュリティホワイトペーパー

Rev. 1.0

改版履歴

Revision	日付	改定概要	作成者
1.0	2021/07	新規作成	
改訂内容			改訂理由

Table of Contents

1 はじめに

本文書では、「RICOH eWhiteboard」（以下、eWhiteboard、本サービス）のセキュリティ情報の概要を説明します。

1.1セキュリティへの取組み

リコーのセキュリティに対する取り組みは、以下の URL から情報を取得することができます。本書は eWhiteboard 特有のセキュリティ情報のみを扱っています。
リコーのセキュリティ： https://jp.ricoh.com/security/

1.2 用語定義

本書では以下の定義に従って用語を利用します。

用語	定義	補足
Empowering Digital Workplaces（EDW） プラットフォーム	リコーが提供する、エッジデバイスとアプリケーションのためのクラウドサービス、プラットフォーム。以前は Ricoh Smart Integration と呼ばれていた。	

2 システム概要

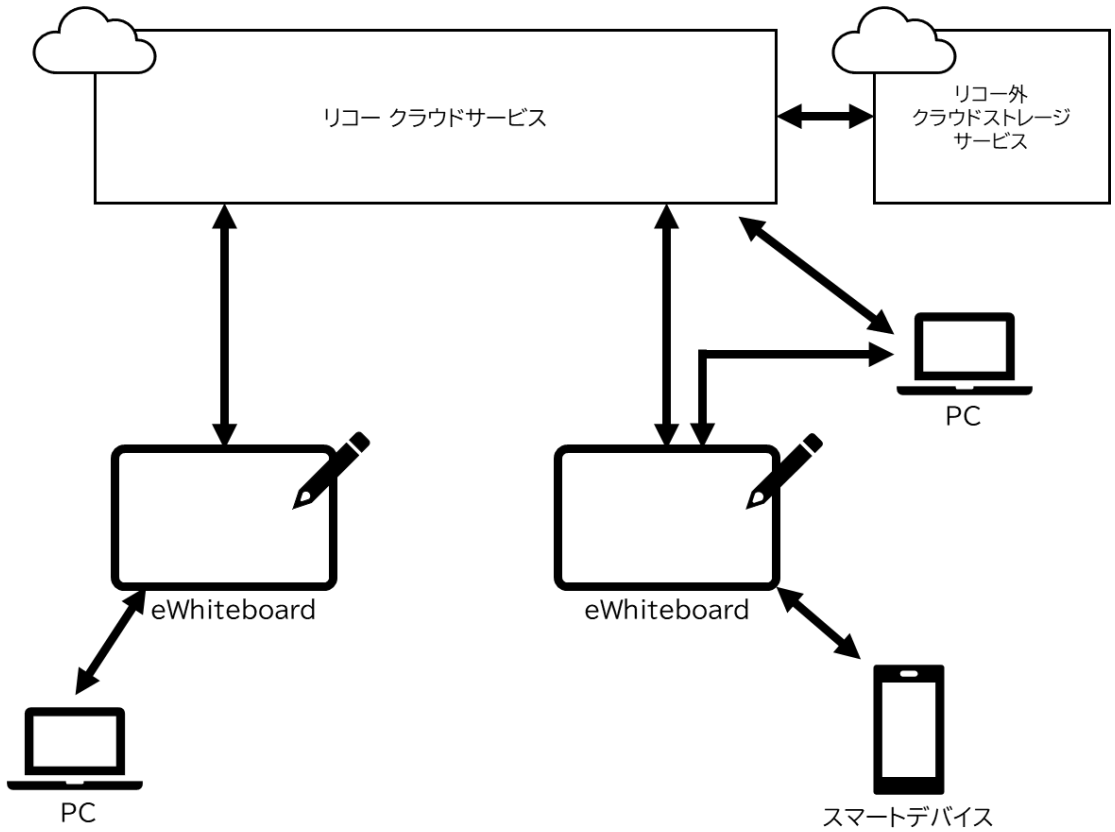

図 1 システム構成

eWhiteboard は電子ペーパーを用いたデジタル・ホワイトボードで、オフィスや現場などのワークプレイスでの紙・手書きのデジタル化をすることができます。

eWhiteboard に付属のペンを用いて絵や文字を書く、PC やスマートデバイスから eWhiteboard の画面を見るといったことができるほか、リコークラウド（米国）やリコー外クラウドストレージサービスとつながることで遠隔地にある複数台の eWhiteboard で図面などを共有する、外部のオンラインストレージサービスにある文書を連携する、といったことができるようになります。

2.1 システム構成の要素

2.1.1 PC・スマートデバイス

PC・スマートデバイスは、Web ブラウザーを用いて eWhiteboard の Web ページにアクセスして設定やファイルのアップロード/ダウンロードをする、リコークラウドの設定画面にアクセスしアクティベーションをする、リコー外クラウドストレージサービスにアクセスする、などのために用います。

2.1.2 eWhiteboard

PC・スマートデバイスの Web ブラウザーやペンを用いた操作の他、一部の機能はインターネットを介してリコークラウド（米国）と接続する必要があります。

2.1.3 リコー クラウドサービス

eWhiteboard 用のクラウドサービスは、リコーが提供する Empowering Digital Workplaces プラットフォーム（以下 EDW プラットフォーム）を利用して提供します。eWhiteboard へ認証・ファイル一覧取得/アップロード/ダウンロードの機能を提供するほか、クラウドストレージサービスと接続を行います。

3 システム全体のセキュリティ対策

3.1 稼働監視、障害監視、パフォーマンス監視

eWhiteboard 用リコークラウドの機能は 24 時間 365 日でネットワーク、サーバー、アプリケーションなどの稼働状況、パフォーマンスを監視しており、不具合が発生した場合には迅速な対応を行う体制となっています。またキャパシティ管理 を行い、十分な可用性を確保しています。

3.2 脆弱性情報の定期収集と対応

脆弱性情報の収集と対応は、リコー社内で定められたプロセスに従って運用しています。

3.3 脆弱性診断と対応

eWhiteboard 用リコークラウドおよび eWhiteboard 本体の Web アプリケーション、ネットワーク機能や他の脆弱性については、リコーで定められた脆弱性調査ツール（AppScan, InsightVM）を 3 ヵ月に 1 回およびアップデートを実施する際に使用して、既知の脆弱性が残されていないことを確認しています。

3.4 ログ

3.4.1 eWhiteboard 用リコークラウド

eWhiteboard から eWhiteboard 用リコークラウドへのアクセスログおよび操作ログを、サーバー内に保持しています。上記のログに含まれる情報はイベントの情報、テナント ID、デバイス ID、ユーザーID、ファイル ID、ステータスや外部サービスとの通信結果や中間処理の実行結果があります。これらのログ情報は、サーバーに対して適切なアクセス制限を行うことで、社内外からの不正アクセスを防いでいます。

なお、個人情報（PIN コード、氏名、メールアドレス 等）および企業情報、業務データ（ファイル名、ファイル内容も含む 等）の情報に関しては、ログへの出力を禁止しています。

3.4.2 eWhiteboard 本体

eWhiteboard 内のアプリケーションの状態、実行結果、IP アドレス、MAC アドレスや機器やネットワークの状態を本体に継続的に記録しており、電源を切っても情報が保持される領域に保存しています。eWhiteboard 内 Web ページの管理者設定からは eWhiteboard 内のアプリケーションのログを取得することができますが、暗号化されており、リコーの限られたメンバーのみが参照できます。

なお、個人情報（PIN コード、氏名、メールアドレス 等）および企業情報、業務データ（ファイル名、ファイル内容も含む 等）の情報に関しては、ログへの出力を禁止しています。

4 データのセキュリティ対策

4.1 データアクセス制御

4.1.1 ユーザー認証（eWhiteboard 本体）

eWhiteboard の操作は本体画面および Web 画面から行います。

本体「メンテナンス」機能と Web「管理者設定」ページにアクセスするには管理者パスワードが必要です。

4.1.2 ユーザー認証（eWhiteboard 用リコークラウド）

4.1.2.1 設定画面へのユーザー認証

本サービスの機能を利用するためには、ユーザーID、パスワードによるログイン（ユーザー認証）を行う必要があります。

ログインに成功しない限り、続く操作を実行することはできない様になっています。ログインに使用するアカウントは EDW プラットフォームから発行され、認証に関する下記要件については、EDW プラットフォームの仕様に準じています。

- 初期アカウント
- パスワード要件
- 二要素認証対応
- パスワード検証
- ユーザー登録時のメッセージ
- アカウントロックポリシー

ログインに失敗した場合は、失敗理由に応じて下記のメッセージが表示されます。メッセージの文言は、用語の見直しにより変更になる場合があります。

発生条件	メッセージ
登録されていないユーザーID、またはパスワードが指定された。	ID またはパスワードが違います。
本サービスの利用権限を持たないユーザーの ID、パスワードが指定された。	指定されたユーザーは機能を利用できません。管理者による機能の利用割り当てが必要です。

本サービスで利用するデータは、EDW プラットフォームにおけるユーザーやテナント（契約した企業・グループの単位）単位で管理されており、各データにアクセスするためには、ログイン後（ユーザー認証成功後）に発行される認証チケットが必要となります。認証チケットの有効期限はログイン後 8 時間であり、有効期限が切れると再ログインするまで本サービスの機能は利用できません。

また OAuth 認証では、お客様が RSI から認可された情報として、上記の認証チケットを本サービスのログイン情報に利用するため、ログインに用いるパスワードが eWhiteboard 用リコークラウドに保存されることはありません。

4.1.2.2 サービス利用へのユーザー認証

eWhiteboard から eWhiteboard 用リコークラウドを利用するための認証方式は、クライアント認証およびユーザコード認証（PIN 認証）の組み合わせとします。クライアント認証（所有）と PIN 認証（知識）の多要素になっています。

4.1.3 クライアント認証

AWS IoT のクライアント証明書の「AWS IoT によって生成された X.509 証明書」を利用し、eWhiteboard 内に安全に保管します。

4.2 データ管理(eWhiteboard 本体)

eWhiteboard にアップロード・ダウンロードされた文書データ(画像含む)や管理者パスワードなどの認証情報、遠隔画面共有データなどの eWhiteboard 用のデータは、暗号化・ハッシュ化され保存されます。

オンラインアップデートファイルをダウンロードする際はサーバー証明書情報の確認およびファイルの改ざん検知を実施します。

eWhiteboard が保有するサーバー証明書(digital-wb.com)は、公開鍵はアルゴリズムが RSA でキーサイズが 2048、署名アルゴリズムは SHA-256です。

4.3 データ管理(eWhiteboard 用リコークラウド)

4.3.1 認証情報

本サービスで作成したユーザー情報は保存せずに、ステートレスなトークン認証をしています。セッションを一時管理していますが、時間経過で自動削除する仕組みとなっています。なお、トークン情報に関しては、暗号化しています。

セッション情報の適切な破棄に関しては、以下の通りです。

- サインイン時に生成され、サインアウト時に破棄されます。
- 一定時間経過後に自動で破棄されます。
- セッション情報破棄時に、トークン情報も併せて破棄します。
- セッション情報以外に管理する機微データはありません。

5 アクセス制御

5.1 アクセス制御

5.1.1 通信プロトコル

インターネットを経由して eWhiteboard がクラウドサービスを利用する際は、HTTPS、MQTTS プロトコルによりサーバーの正当性の確認がされ、通信は暗号化されます。
eWhiteboard とクラウドサービスは、以下の通りに通信します。

表 1 クラウドサービスとの通信

機能	通信先ホスト	ポート	プロトコル	TLS ver.
REST-API	api.iot.na.smart-integration.ricoh.com	443	HTTPS	1.2
MQTT	（利用の際にホスト名を API から取得します）	443/8883	MQTTS	1.2
Workflow Application API	www.na.smart-integration.ricoh.com	443	HTTPS	1.2
Online Update	auto-ds1.support-download.com	443	HTTPS	1.2

- クラウドサービスが提供される IP アドレスは公開していません。現在サービスを提供している IP アドレスにおいて、将来にわたってサービスが提供される保証はありません。

また eWhiteboard は IPv4 のみに対応しており、使用する TCP/UDP ポートは以下の通りです。

表 2 使用通信ポート一覧

ポート番号	説明
53/TCP, UDP	DNS、クエリ応答や管理者用ネットワークチェックツール
67/UDP	DHCP
68/UDP	DHCP
80/TCP	HTTP, Web ブラウザーからの Web ページアクセス
123/TCP	NTP, 時刻同期
443/TCP	HTTPS, MQTTS、Web ブラウザーからの Web ページアクセスやリコークラウドとの通信
8883/TCP	MQTTS
ICMPv4	ICMP

5.1.2 無線 LAN 機能と独自 DNS サーバー

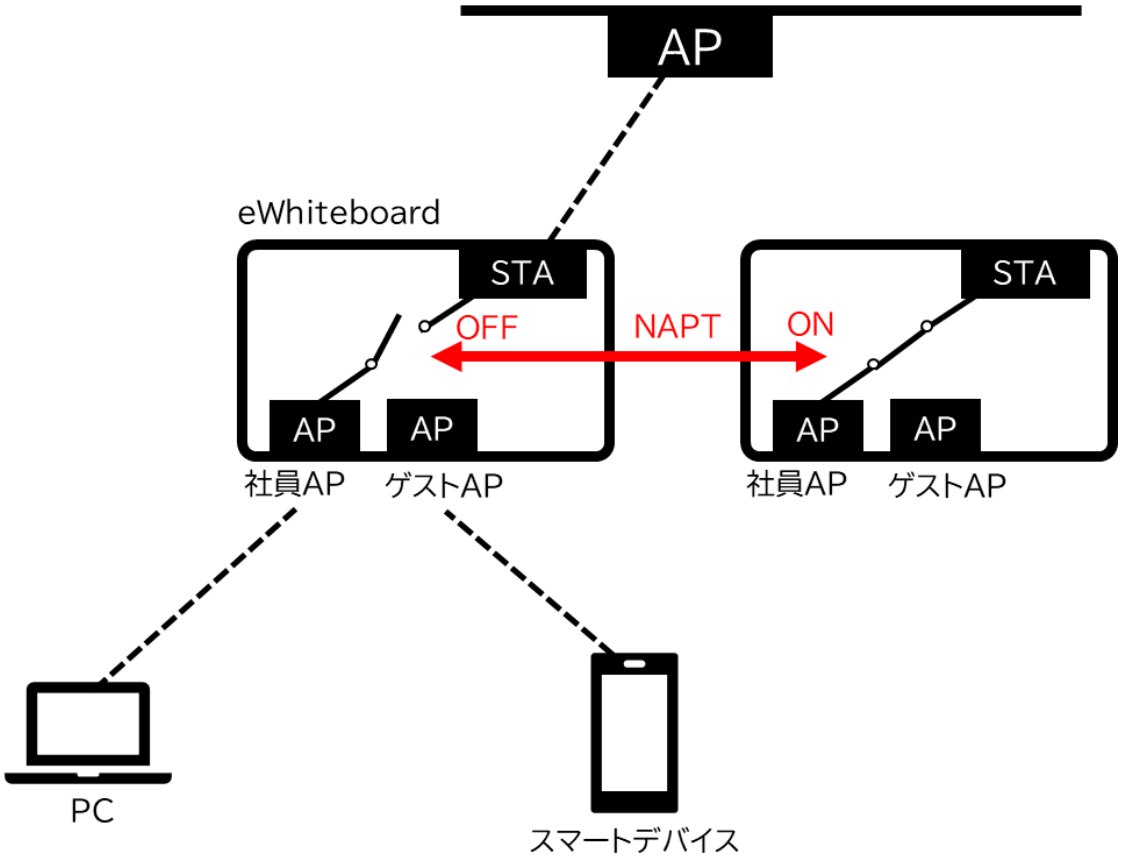

図 2 無線 LAN 機能概要図

eWhiteboard には 2 つの無線 LAN アクセスポイント(AP)機能、1 つの無線 LAN ステーション(STA)機能があります。AP には、AP 側のネットワークと STA 側のネットワークとを NAPT(Network Address Port Translation)機能によりつなぐことのできる社員 AP と、それができないゲスト AP とがあります。

なお、NAPT 機能の ON と OFF の切り替えは eWhiteboard の管理者用 Web ページから設定することができます。

また eWhiteboard の AP に接続された端末から「digital-wb.com」についての DNS クエリが出されると、eWhiteboard は自身の IP アドレスを返答します。これは上記端末から eWhiteboard の Web 画面にアクセスするときに使います。また eWhiteboard は Captive Portal 機能のため端末からの特定の URL についての DNS 問い合わせに応答します。

5.1.3 アクセス制御(eWhiteboard 本体)

管理者の認証は、4.1.1 に記載の内容で実施しています。また、本体画面からは文書ごとにロックコードが設定可能で、文書にアクセスするのに必要になります。

5.1.4 アクセス制御(eWhiteboard 用リコークラウド)

5.1.4.1 所有権に応じたアクセス制御

ユーザー認証は、4.1.2 に記載の内容で実施しています。ユーザーのアクセス方法は eWhiteboard からの入力のみとなります。

5.1.4.2 アクセス制御失敗時の記録

サービス利用時のエラーメッセージ表示に対応しています。

5.2 通信路の暗号化

5.2.1 通信路の暗号化(eWhiteboard 本体)

eWhiteboard と eWhiteboard 用リコークラウドとの通信路(アプリケーションレイヤー)は上記の通り暗号化されています。

また、無線 LAN のレイヤーでは、対応している認証・暗号化方式は以下の通りです。

- AP
  - Open
  - WEP
  - WPA-PSK TKIP
  - WPA-PSK AES
  - WPA2-PSK TKIP
  - WPA2-PSK AES(デフォルト)
- STA
  - WPA/WPA2-PSK
  - WPA2-EAP-PEAP
  - WPA2-EAP-TLS

最後に、Web ページへは eWhiteboard の STA 側ネットワークからは HTTP もしくは HTTPS でアクセスできるよう設定可能です。

5.2.2 通信路の暗号化(eWhiteboard 用リコークラウド)

AWS IoT を用いた MQTT 通信(TLS1.2)を実施しています。

5.3 データセンター(eWhiteboard 用リコークラウド)のセキュリティ対策

本サービスのサーバー群は、Amazon Web Services の上に構成されています。このデータセンターのセキュリティ対策は Amazon Web Services のセキュリティ対策によって行われています。

6 商標

- Amazon Web Services、“Powered by Amazon Web Services”ロゴ、[およびかかる資料で使用されるその他の AWS 商標]は、米国その他の諸国における、Amazon.com, Inc.またはその関連会社の商標です。
- Wi-Fi, WPA, WPA2 は Wi-Fi Alliance の商標または登録商標です。

その他の製品名、名称は各社の商標または登録商標です。
これらは本書の説明および所有者の権利のために使用され、使用により所有者の権利を侵害するものではありません。