RICOH Interactive Whiteboard Add-on Service

セキュリティーホワイトペーパー

Ver.1.4

作成 ： 2019 年 05 月 10 日

改定 ： 2021 年 10 月 14 日

株式会社リコー

<目次>

<図表目次>

1. はじめに

1.1. 目的

本書では、RICOH Interactive Whiteboard Add-on Service をお客様に安心してご利用頂くために、本システムのセキュリティー対策と仕組みについて説明することを目的としています。

1.2. 本書説明の対象となる範囲

本書では、RICOH Interactive Whiteboard Add-on Service で利用しているクラウドサーバー(EMPOWERING DIGITAL WORKPLACES プラットフォーム)と機器(RICOH Interactive Whiteboard)上で動作する RICOH Interactive Whiteboard Add-on Service App のセキュリティー対策を説明対象としています。なお、機器(RICOH Interactive Whiteboard)本体におけるセキュリティー対策に関しては、『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[1]』で開示している内容と重複するため、本書説明の対象外としています。

クラウドサービスの情報セキュリティー対策のあり方に関しては以下のガイドラインが公開されています。

① ASP・SaaS における情報セキュリティー対策ガイドライン[2]
② クラウドサービス利用のための情報セキュリティーマネジメントガイドライン[3]
③ クラウド事業者による情報開示の参照ガイド[4]

①/②は JIS Q 27001(ISMS)、27002(実践のための規範)を参考にして、クラウドサービス提供事業者が実施すべき情報セキュリティー対策を整理したものであり、次章より説明する本システムのセキュリティー対策も上記ガイドラインに即したものとなっています。

また、リコーグループではお客様に安心してご利用いただける製品・サービスを提供していくための不可欠な要素として、ISMS 認証の取得と継続的な外部審査をはじめとする情報セキュリティーマネージメント[5]に取り組んでいます。この取り組みにより上記ガイドラインの組織・運用面での対策についてはその多くが網羅できているため、本書における説明の対象外とし、主に物理的・技術的対策にフォーカスし説明しています。

本書は③に準じて必要な情報を開示・提供するものです。

---

1 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 (適宜更新)
http://ext.ricoh.co.jp/iwb/swp/

2 総務省、2008 年 1 月 30 日
http://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/chousa/asp_saas/

3 経済産業省
http://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudsec2013fy.pdf

4 IPA、2011 年 4 月 25 日
http://www.ipa.go.jp/security/cloud/tebiki_guide.html

5 リコーグループの情報セキュリティー(適宜更新)
http://jp.ricoh.com/security/management/

1.3. 本書の構成

以下章目次に示す通り、まずシステムの概要を把握頂くため、2 章でシステム構成、データフロー、通信プロトコルについて説明しています。3～6 章でシステム全般及び、各項目のセキュリティー対策について説明しています。

2 章 システム構成
3 章 システム全般のセキュリティー対策
4 章 データのセキュリティー対策
5 章 ネットワークのセキュリティー対策
6 章 データセンターのセキュリティー対策

2. システム構成

2.1. 全体構成

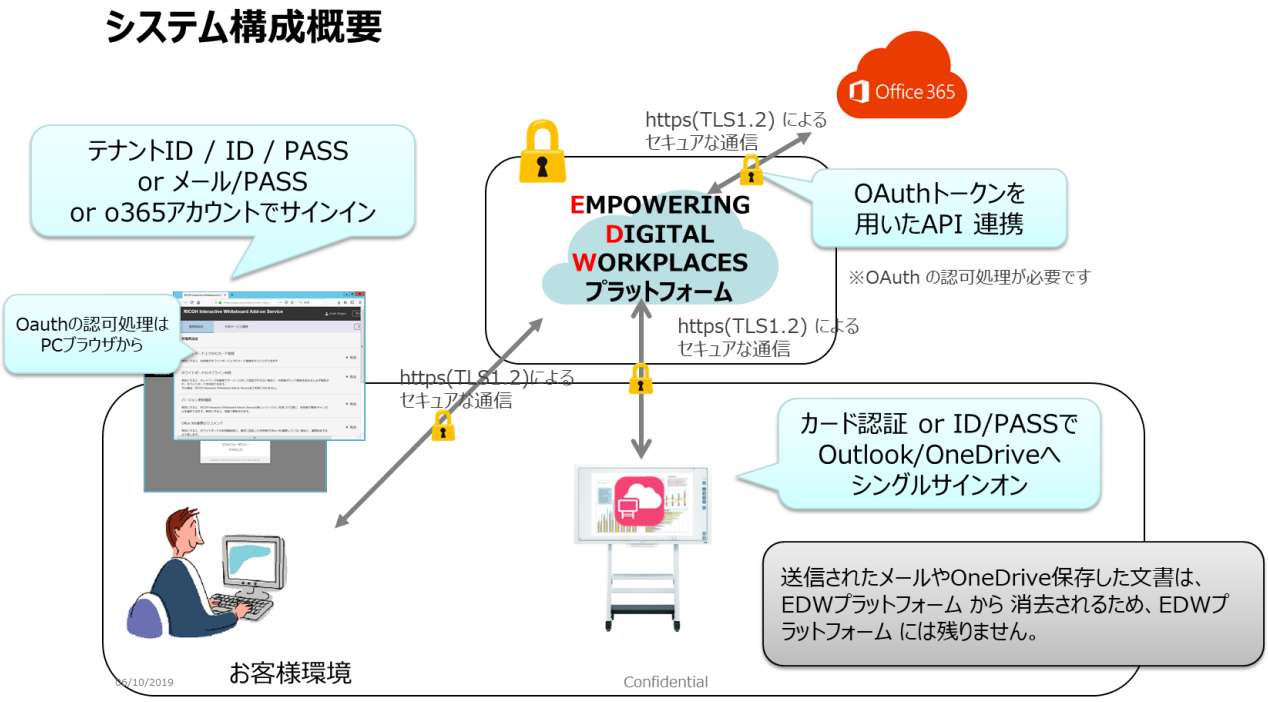

図 1 RICOH Interactive Whiteboard Add-on Service システム構成図

RICOH Interactive Whiteboard Add-on Service は、お客様環境[6]と、インターネット上に存在する EMPOWERING DIGITAL WORKPLACES プラットフォームで構成されます。EMPOWERING DIGITAL WORKPLACES プラットフォームは、アプリサーバー[7]と、バックエンドサーバー[8]から構成され、機器(RICOH Interactive Whiteboard)上で動作する RICOH Interactive Whiteboard Add-on Service App は、バックエンドサーバーと通信し、RICOH Interactive Whiteboard Add-on Service の機能提供(Microsoft 365/BOX 連携機能を含む)を行います。

6 PC ブラウザ、機器(RICOH Interactive Whiteboard)、お客様ネットワーク等により構成されます。

7 ユーザー管理サイト、RICOH Interactive Whiteboard Add-on Service 連携サイト等により構成されます。

8 ID 管理(Office365 連携含)、認証、メール送信、RICOH Interactive Whiteboard Add-on Service の機能提供用バックエンドサービス、RICOH Interactive Whiteboard Add-on Service の機器、会議情報管理バックエンドサービス等により構成されます。

2.2. 通信プロトコル

2.2.1. RICOH Interactive Whiteboard Add-on Service を利用する場合の、お客様環境から EMPOWERING DIGITAL WORKPLACES プラットフォームへの通信

表 1 お客様環境から EMPOWERING DIGITAL WORKPLACES プラットフォームへの通信

機能	通信先ホスト	ポート	プロトコル
PC ブラウザから EMPOWERING DIGITAL WORKPLACES プラットフォームへの接続	*.accounts.ricoh.com *.smart-integration.ricoh.com	443/TCP	HTTPS
IWB から EMPOWERING DIGITAL WORKPLACES プラットフォームへの接続	*.smart-integration.ricoh.com	443/TCP	HTTPS

2.2.2. RICOH Interactive Whiteboard Add-on Service を利用する場合の、EMPOWERING DIGITAL WORKPLACES プラットフォームからインターネット環境(外部サービス)への通信

外部サービスとの連携は、外部サービスの仕様に従います。また、基本的には HTTPS のプロトコルにより接続します。

2.2.3. マルチテナント対応

EMPOWERING DIGITAL WORKPLACES プラットフォームは複数の企業・組織に対してサービスを提供します。企業・組織など、サービスを提供する対象をテナントと呼び[9]、複数のテナントの情報を同一ハードウェア上で管理しています。システムは論理的にテナント間でのデータを分離しており、テナント間の独立性を確保しています[10]。データアクセスに関しては、4.1 データアクセス制御に記載しています。

テナントは、エンドユーザーが自身の属するテナントにライセンスされた EMPOWERING DIGITAL WORKPLACES プラットフォーム上のアプリケーションを利用するためのもので、他テナントの情報を参照することはできません。

9 複数の企業が合同で契約するような利用形態があるため、「企業」ではなく「テナント」と言う用語を使用しています。

10 このようなシステム構成は、「マルチテナントアーキテクチャ」と呼ばれます。

3. システム全般のセキュリティー対策

3.1. 稼動監視、障害監視、パフォーマンス監視

24 時間 365 日、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、万一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[11]を行い十分な可用性を確保しています。

3.2. 脆弱性情報の定期的収集とパッチ適用

脆弱性情報の収集と対応は、事前通知を管理する社内組織からの提言をもとに社内で定められたプロセスに従って運用しています。OS やミドルウェア等に対するセキュリティーパッチは重要性とシステムへの影響を判断した上で、開発環境にて検証後、実運用環境への実施を計画し適用しています。

また、Vuls[12]を使用して各サーバーで動作しているパッケージの脆弱性を自動検知しています。さらに、動作しているパッケージの脆弱性情報を JVNDB[13]で確認し、パッケージ毎にサービスへの影響度と対応有無を調査・管理しています。

[11] テナント、ユーザー、機器、ライセンス、ジョブの想定数に対して、十分なストレージ容量を割り当て、また実際の使用量の監視を行っています。

[12] VULnerability Scanner の略称。システムの脆弱性をスキャンするためのソフトウェアです。

[13] IPA により提供される脆弱性対策情報データーベース

3.3. 脆弱性診断

Web アプリケーションの脆弱性評価ツールとして IBM 社の AppScan を使用して、以下の項目について 3 ヶ月に 1 度確認を行い、既知の脆弱性が残されていないことを確認しています。

表 2 AppScan の脆弱性分類と対応する項目例

検査分類	具体的な検査項目	
認証	・総当り攻撃	・不適切な認証
認可	・インデクシング/セッションの推測 ・セッションの固定	・不適切なセッション期限 ・不適切な許可
アプリケーション	・プライバシーテスト	・品質テスト
クライアント側攻撃	・クロスサイトスクリプティング	・コンテンツの成りすまし
コマンドの実行	・LDAP インジェクション ・OS 命令 ・SQL インジェクション ・SSL インジェクション	・XPath インジェクション ・バッファオーバーフロー ・書式文字列攻撃
情報の開示	・ディレクトリインデクシング ・パストラバーサル	・情報遺漏 ・推測可能なリソース
論理攻撃	・サービスの拒否攻撃	・機能の悪用

さらに、第三者評価として、Web アプリケーションの脆弱性評価ツールとして米 Rapid7 社の InsightVM を 3 ヶ月に 1 回適用し、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. システム共通

サーバーのアプリケーションログは統合的に収集を行い、不正アクセス、システム障害の解析を一元的に行えるようにしており、各サーバー内のシステムログを含め、定期的にバックアップを行っています。また、全てのサーバーは NTP で時刻同期を行っています。なお、収集されるログ情報はリコー社内のルールに従って内容を適切に判断しており、全てのログにおいてパスワード情報の収集は行っておりません。

4. データのセキュリティー対策

4.1　データアクセス制御

EMPOWERING DIGITAL WORKPLACES プラットフォームで利用されるデータは、ユーザーやテナント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、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。認証チケットによってアクセスできるデータを制御しているので、別ユーザーの保存文書や別企業のユーザー情報が目にふれることはありません。
EMPOWERING DIGITAL WORKPLACES プラットフォームで管理するデータは、AWS 上に存在し、インターネットから直接アクセスすることはできず、EMPOWERING DIGITAL WORKPLACES プラットフォーム内に存在するエンドポイントを経由しない限りアクセスできません。
また、AWS にアクセスできるアカウントに対して AWS IAM でアクセス権限を設定しており、内部からも業務上必要な範囲以外のデータにはアクセスできないようになっています。

4.1.1 ユーザー認証

ログイン(PC ブラウザ、機器共通)

EMPOWERING DIGITAL WORKPLACES プラットフォームにアクセスするには、テナント ID、ユーザー名、パスワード、または、メールアドレス、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。認証に成功しない限り、続く操作やデータへアクセスすることはできない様になっています。

テナント ID は 10 桁の数字列で、業務システムにより発行され、利用お申し込み後にお客様に割り当てられます。ユーザー名は 1 文字以上 128 文字以下の文字列として登録することができます。更に、最小登録文字数の制限や英数に加えて記号の使用、再利用回数を規定することで登録パスワードの強度を高める事ができます

パスワードは、最大 128 文字(最小 6 文字)の任意のアスキー文字列として設定でき、ログイン時にパスワードを連続で間違えるとそのアカウントはロックされる為、ブルートフォース攻撃(総当たり攻撃)や辞書攻撃に対し十分な耐性を有しており、不正な認証突破によるデータアクセスが防止されます。アカウントがロックされた場合、管理者がユーザー管理画面から有効化するか、ユーザーがパスワードをリセットするか、24 時間後にシステムによって自動解除されるまでログインすることはできません。

登録されているテナント ID、ユーザー名、メールアドレス等のアカウント情報は、上述の通りデータへのアクセスが制御され漏洩することはないため、リバースブルートフォース攻撃に対する耐性も有します。

ユーザーはユーザーサイトからログインしパスワードを変更することができますが、センター側ではパスワードのハッシュ値のみを保存しているので、リコーはお客様のパスワードを入手することはできず、センター側からパスワードの文字列が漏えいすることもありません。なお、ハッシュ値やユーザー情報のデータアクセスに関しても、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(5.1 節参照)。加えて、パスワードに有効期限を設定し定期的なパスワードの変更をユーザーへ促すことで、より安全性を高めることができます。

外部サービスのアカウントを利用したシングルサインオン(ログイン)機能も備えていますが、外部サービスのアカウント情報はリコー側では管理されません。

機器(Interactive Whiteboard)からのログイン

機器(RICOH Interactive Whiteboard)からのログインは、ログイン(PC ブラウザ、機器共通)に記載の方法の他に、IC カードログイン、または、機器(RICOH Interactive Whiteboard)が連携している認証サーバー(Active Directory 等)のアカウント(ID/パスワード)でログインすることができます。これらのログインは登録された機器(RICOH Interactive Whiteboard)からのみ利用できるため、PC などの他のクライアントデバイスからログインすることはできません。

機器を利用するためには、初回アプリ起動時に管理者の権限でログインを実施しセンターサーバーに機器を登録する必要があります。登録された機器では、ユーザー認証時にログインユーザーのテナントチェックを行っており、他テナントのユーザー情報ではログインすることは出来ません。

機器登録時に、TPM(Trusted Platform Module)を用いて、キーペアが生成されます。登録されたテナントの情報にアクセスするためには、キーペアの秘密鍵が必要となるため、他のデバイスで成りすましてのテナント情報への不正アクセスもできなくなります。

EMPOWERING DIGITAL WORKPLACES プラットフォームを認証サーバーとした際の IC カード(所持要素)によるログインでは、PIN コード(記憶要素)を組み合わせた多要素認証(Multi-Factor Authentication)を設定することができ、より高度に不正アクセス/なりすましを防止することができます。

外部サービスへのシングルサインオン

機器(RICOH Interactive Whiteboard)にログインすると、外部サービスにアクセスできるようになります。例えば、Office 365 の OneDrive for Business や Outlook(Exchange Online)のスケジュールにアクセスできるようになります。
シングルサインオンは、予め、RICOH Interactive Whiteboard Add-on Service 連携設定サイトで、Office 365 のアカウントと、EMPOWERING DIGITAL WORKPLACES プラットフォームのアカウントを紐づけておく必要があります。紐づけは、OAuth 認可を用いて行われます。
機器にログインした EMPOWERING DIGITAL WORKPLACES プラットフォームアカウントは、OAuth で認可されている範囲のデータにしかアクセスできません。
一般的にアカウントの紐づけ(SSO 設定)は外部サービスのアカウントを有するユーザーが自身のアカウントにログインし、認可されるデータの範囲を確認し承認することで行われます。

4.2 データ管理

4.2.1 機器(Interactive Whiteboard)

センターサーバーに機器登録する際に、契約時に発行されたテナント ID と、ユーザー名、パスワード、もしくは、メールアドレス、パスワードを入力します。入力されたテナント ID は機器内に保存されますが、管理者のユーザー名、メールアドレス、パスワードは機器内に保存されません。

5　ネットワークのセキュリティー対策

5.1　アクセス制御

5.1.1　ネットワークのアクセス制御

インターネットから直接アクセスできるサーバーにはお客様のアップロードした文書やパスワードなどの機密情報は置かず、4.1 章の通りの AWS アカウント限定でアクセスできる場所に保管されます。インターネットからサーバーに対して直接ログインできないようにしているほか、AWS のセキュリティーグループ(仮想ファイアウォール)で通信を許可するポート番号を設定することにより外部からの不正アクセスを防止しています。

サーバー保守業務は、リコーの社内 LAN からインターネット回線でセンターサーバーに接続して行われます。AWS のセキュリティーグループ(仮想ファイアウォール)で通信を許可する IP アドレス、および、ポート番号を設定することで、センターサーバーへのアクセスを、リコー社内 LAN からのみ、かつ特定プロトコルでの暗号化通信に限定していますので、第三者がインターネットから接続して、保守業務装いセンターサーバーにアクセスすることはできません。また、センターサーバーへの接続はパスワードではなく SSH 秘密鍵を使用しており、リコー社内からの接続者を、公開鍵を作成した関係者に限定することで、保守業務における顧客情報の漏洩や攻撃を防いでいます。

5.1.2　サーバー(OS)のアクセス制御

サーバーに登録するアカウントは社内にて権限を認められた最小人数に限定し、担当者の異動時に権限をメンテナンスするだけでなく、社内規定に準じて半年毎に棚卸しを行うことで、権限を持たない人からの不正アクセスを防止しています。また、アカウントのパスワードは容易に推測されないようパスワードポリシーを定めています。

サーバーで保存しているデータについては種類によって適切なアクセス範囲を決め、業務上必要な範囲以外のデータにアクセスできないように AWS IAM でアカウントやサーバー毎にアクセス権限を設定しています。更に、データアクセスに関する取り扱い手順を定めており、手順に従って承認を得た上でアクセスが行なわれます。サーバー管理者に対しては、事前にセキュリティー教育を実施し、また定期的に取り扱い手順の確認/徹底を行っています。

5.2　通信経路の暗号化

PC(ブラウザ)、機器(RICOH Interactive Whiteboard)とセンターサーバー間の通信は、メールを除き、すべて HTTPS で通信経路を暗号化されています。センターのサーバー証明書には、第三者認証局の発行する、公開鍵 RSA 2048 ビット、拇印アルゴリズム SHA-2 の証明書を使用しています。HTTPS で用いるプロトコルとそのバージョンは、TLS 1.2 のみとしています。

5.3　メール送信

システムからの全てのメール送信には SMTP を用いており、暗号化は行っていませんが、送信したメールのなりすまし防止として SPF(Sender Policy Framework)、ドメイン認証技術として DKIM(Domain Keys Identified Mail)を適用しています。SPF、および、DKIM で使用する DNS レコードは全て、高いセキュリティー性を有する AWS Route53 で管理されています。

6　データセンターのセキュリティー対策

サーバー群は、AWS の上に構成されています。データセンターのセキュリティー対策は AWS のセキュリティー対策によって行われております。[14]

[14] AWS セキュリティプロセスの概要
日本語：https://d0.awsstatic.com/International/ja_JP/Whitepapers/AWS%20Security%20Whitepaper.pdf
英語　：https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf

7　商標

- Office 365®、OneDrive®、Outlook®は Microsoft 社の米国および、その他の国における商標または登録商標です。
- Office 365®の一部のプランでは 2020 年 4 月 21 日から Microsoft 365®に名称が変更されています。
- 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。
- InsightVM は.Rapid7 社の米国その他の諸国における商標または登録商標です。