RICOH Cloud Whiteboard Service

セキュリティーホワイトペーパー

Ver.1.0.1

作成 ： 2022年05月19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 Cloud Whiteboard Service をお客様に安心してご利用いただくために、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

本書は、RICOH Cloud Whiteboard Service で利用しているサーバー、RICOH Interactive Whiteboard(以下、「機器」)と PC で利用される RICOH Cloud Whiteboard Service 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。

クラウドサービス事業者がクラウドサービスを提供する際に実施することが望ましい情報セキュリティー対策について、以下のガイドラインが公開されています。

- クラウドサービス提供における情報セキュリティー対策ガイドライン[2] (第 3 版)

これは「クラウドサービス提供における情報セキュリティー対策ガイドライン(第 2 版) 」(2018 年 7 月)をもとに、ISMAP 管理基準、ISO/IEC27017(2016)および NIST SP800-53 Rev.5 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・改定されたものであり、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、情報セキュリティーマネジメントに取り組んでいます[3]。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、本書の対象外とし、主に物理的・技術的対策にフォーカスして説明しています。

---

[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 2021 年 9 月
https://www.soumu.go.jp/main_content/000771515.pdf

[3] 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

以下の章目次に示す通り、まずシステムの概要を把握いただくため、2 章でシステム構成、ユースケース、データフロー、通信プロトコルについて説明しています。そして、3～6 章でシステム全般および、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

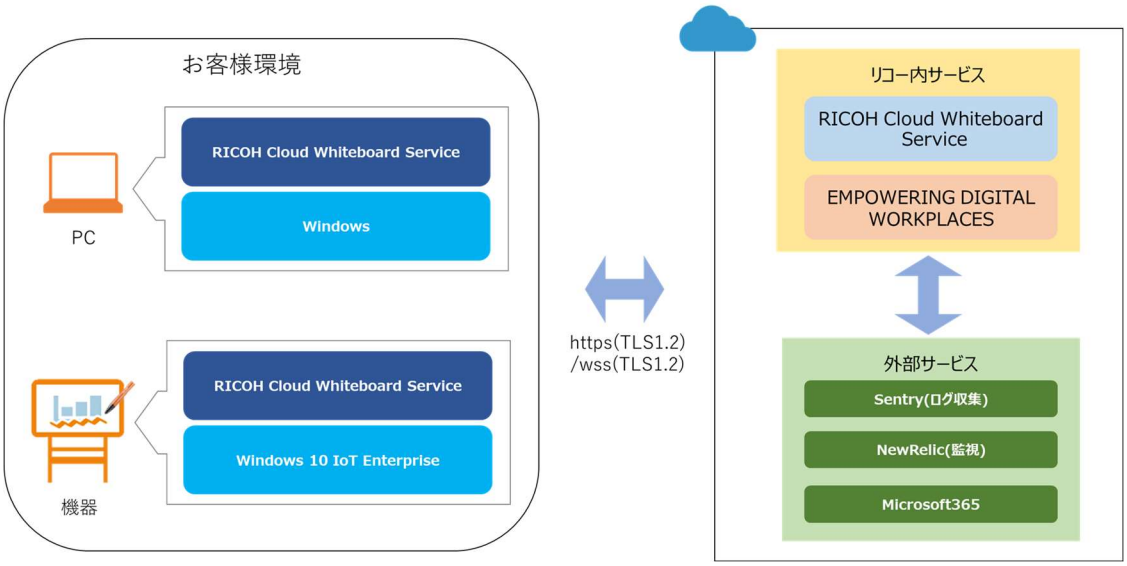

図 1 RICOH Cloud Whiteboard Service システム構成図

RICOH Cloud Whiteboard Service は、お客様環境[4]と、インターネット上に存在する RICOH Cloud Whiteboard Service、EMPOWERING DIGITAL WORKPLACES プラットフォームで構成されるホワイトボード機能を有するオンライン画面共有サービスです。EMPOWERING DIGITAL WORKPLACES プラットフォームは、アプリサーバー[5]と、バックエンドサーバー[6]から構成され、RICOH Cloud Whiteboard Service はアプリサーバー[7]と、バックエンドサーバー[8]から構成されます。PC または機器上で動作するアプリは、バックエンドサーバーと通信し、RICOH Cloud Whiteboard Service の機能提供を行います。

また、RICOH Cloud Whiteboard Service は外部サービスである Sentry によりデバッグログの収集と NewRelic によりサーバーのパフォーマンス監視を行っています。

[4] PC、PC ブラウザまたは機器、お客様ネットワーク等により構成されます。

[5] ユーザー管理サイトにより構成されます。

[6] ID 管理(Microsoft 365 連携含)、認証、RICOH Cloud Whiteboard Service の機能提供用バックエンドサービス、RICOH Cloud Whiteboard Service の機器および会議情報管理バックエンドサービスにより構成されます。

[7] Microsoft 365 連携により構成されます。

[8] RICOH Cloud Whiteboard Service の機能提供用バックエンドサービスにより構成されます。

2.2. 通信プロトコル

2.2.1. RICOH Cloud Whiteboard 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、RICOH Cloud Whiteboard Service およびその他サービスへの通信

表 1 お客様環境からの通信

接続元	通信先ホスト	ポート	プロトコル
PC ブラウザ	*.accounts.ricoh.com	443/TCP	HTTPS
PC アプリ、機器アプリ共通	*.accounts.ricoh.com *.smart-integration.ricoh.com	443/TCP	HTTPS
	*.smart-integration.ricoh.com	443/TCP	WSS
	*.activation.airserver.com *.api.airserver.com	443/TCP[9]	HTTPS
機器アプリ	*.iot.us-west-2.amazonaws.com	443/TCP	HTTPS
	*.iot.us-west-2.amazonaws.com	443/TCP	WSS

2.2.2. RICOH Cloud Whiteboard 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 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[10]、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[11]。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 AirServer の初回アクティベート時のみインターネット通信します。

10 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。

11 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、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。加えて、不正なパケットや攻撃等も監視/検知する体制があります。またキャパシティ管理[12]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、開発環境で検証後、実運用環境への実施を計画し適用しています。

また、パッケージの脆弱性を自動検知している。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。

[12] 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。

[13] JPCERT/CC と 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 HCL Technologies 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 ・不適切なセッション期限	・セッションの固定 ・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 ・SQL インジェクション ・XPath インジェクション ・書式文字列攻撃	・OS 命令 ・SSL インジェクション ・バッファオーバーフロー
情報の開示	・ディレクトリインデクシング ・情報遺漏	・パストラバーサル ・推測可能なリソースの
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 1 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。なお、出力情報はリコー社内のルールに従って出力内容を適切に判断しており、すべ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。

3.5. アプリのプログラムの難読化

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の難読化を行っています。

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、ユーザー認証で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ができず、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なっています。

4.1.1 ユーザー認証

ログイン（ブラウザ、PC、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、続く操作を実行することはできないようになっています。

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。

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ため、ブルートフォース攻撃や辞書攻撃に対し、十分な耐性を有しています。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、情報として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変更できます。また、センター側で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洩することはありません。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することで定期的なパスワードの変更をユーザーへ促し、より安全性を高めることができます。
また、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機能も備えています。

機器からのログイン

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[14]を登録する必要があります。登録された機器では、起動時にテナントチェックを行っており、他テナントでは利用することが出来きません。

機器登録時に付与された認証情報を使用し、アクセスするため、他のデバイスで成りすましての不正アクセスはできません。認証情報は、TPM(Trusted Platform Module)を用いて、保護しています。

4.2 データ管理

4.2.1 機器,PC

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。

また、ホワイトボードの情報が機器/PC 内に残ることもありません。

[14] リコーで適切に製造された RICOH Interactive Whiteboard のみが登録されます。

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ます。また、AWS のセキュリティグループ（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う。AWS のセキュリティグループ（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。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。合わせて、定期的な監査により管理/運営が適切に行われていることを確認しています。

5.2　通信経路の暗号化

ブラウザ、PC、機器とセンター間の通信は、すべて HTTPS で通信経路を暗号化しています。センターのサーバー証明書には、ACM[15]を利用しており、暗号化には AWS のセキュリティポリシー[16]のうち ELBSecurityPolicy-FS-1-2-Res-2020-10 を利用しています。HTTPS で用いるプロトコルとそのバージョンは、以下のものをサポートしています。

- TLS 1.2

[15] AWS Certificate Manager
https://aws.amazon.com/jp/certificate-manager/

[16] AWS のセキュリティポリシー
https://docs.aws.amazon.com/ja_jp/elasticloadbalancing/latest/application/create-https-listener.html#describe-ssl-policies

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 の上に構成される。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います。[17]

ホワイトボードの情報を扱うサーバーは日本国内にあり、日本国内の法律および条令が適応されるよう対策されています。

[17] AWS セキュリティプロセスの概要
日本語: https://d1.awsstatic.com/whitepapers/ja_JP/Security/AWS_Security_Whitepaper.pdf
English: https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf

7　商標

- Microsoft 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。
- Amazon Web Services、“Powered by Amazon Web Services”ロゴ、AWS、［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。
- AppScan は HCL Technologies 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。
- SENTRY は Functional Software 社の米国および、その他の国における登録商標です。
- New Relic は New Relic 社の米国および、その他の諸国における商標または登録商標です。
- 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。