RICOH Meeting 360

セキュリティーホワイトペーパー

Ver.1.0

作成 ： 2023年3月7日

株式会社リコー

＜目次＞

＜図表目次＞

1. はじめに

1.1. 目的

本書は、RICOH Meeting 360 をお客様に安心して頂くためご利用いただくために、本システムのセキュリティ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 Meeting 360 で利用しているサーバ、機器と PC で利用されるアプリケーションのセキュリティ対策を説明対象としています。

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対策ガイドライン[1]（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対策ガイドライン（第 2 版）」(2018 年 7 月)を基に、ISMAP 管理基準、ISO/IEC27017(2016)及び 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対策を整理し/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、情報セキュリティマネージメントに取り組んでいます[2]。この取り組みにより、上記ガイドラインの組織・運用面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。

リコーグループの情報セキュリティに関しては、リンクをご参照ください。

1.3. 用語定義

RICOH Meeting 360 V1：360°映像録画できるカメラマイクスピーカーデバイス

RICOH Meeting 360 Apps for Windows：RICOH Meeting 360 V1 と接続して利用するアプリケーション

RICOH Meeting 360 Add-on Service for カンタン議事録：アプリケーションと連携して会議・記録機能を提供するバックエンドサービス

---

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

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

1.4. 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対策
4 章 データのセキュリティ対策
5 章 ネットワークのセキュリティ対策
6 章 データセンターのセキュリティ対策

2. システム構成

2.1. 全体構成

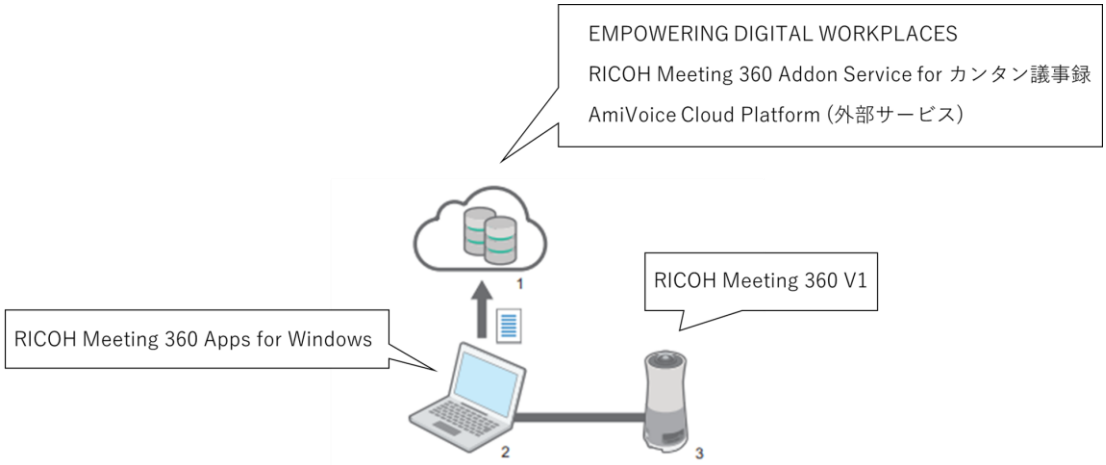

図 1 RICOH Meeting 360 システム構成図

RICOH Meeting 360 は、お客様環境の PC 上で動作するアプリ(RICOH Meeting 360 Apps for Windows)と、インターネット上に存在する RICOH Meeting 360 Add-on Service for カンタン議事録、EMPOWERING DIGITAL WORKPLACES プラットフォーム、機器(RICOH Meeting 360 V1)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（ユーザ管理サイト）と、バックエンドサーバ(ID 管理(Microsoft 365 連携含)、認証、会議情報管理バックエンドサービス)から構成され、RICOH Meeting 360 Add-on Service for カンタン議事録はアプリサーバ（Microsoft 365 連携、テナント設定）と、バックエンドサーバ(RICOH Meeting 360 の機能提供用バックエンドサービス)から構成されます。PC アプリは、バックエンドサーバと通信し、RICOH Meeting 360 の機能提供を行います。

※ 本サービスは NIST SP800-171 には準拠していません

2.2. 通信プロトコル

2.2.1. お客様環境から本サービスプラットフォームへの通信

RICOH Meeting 360 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 及び RICOH Meeting 360 Add-on Service for カンタン議事録への通信については、以下の表 1 をご確認ください。

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	*.accounts.ricoh.com *.cs.rinfra.ricoh.com	443/TCP	HTTPS

2.2.2. 本サービスプラットフォームからインターネット環境への通信

RICOH Meeting 360 を利用する場合の、EMPOWERING DIGITAL WORKPLACES プラットフォーム及び PC アプリからのインターネット環境への通信は、基本 HTTPS のプロトコルにより接続します。
また、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。

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[3]、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[4]。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。

[3] 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。

[4] 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、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[5]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、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。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、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[6]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。

[5] 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。

[6] 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 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、全てのログにおいてパスワード情報は出力しておりません。
個人情報に関わる情報は、別途 RICOH Meeting 360 Add-on Service for カンタン議事録の利用規約を参照してください。

4. データのセキュリティ対策

4.1　データアクセス制御

図 1 の 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、Amazon Web Services (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 共通）

図 1 の 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(図 1 の 2 から 1 へのアクセス)。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 5 回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ています。

ユーザーは、ユーザーサイトから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えい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)。

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。

5　ネットワークのセキュリティ対策

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。

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に接続して行っています。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にアクセスすることはできません。また、センターサーバ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(OS)のアクセス制御

サーバ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。サーバ管理者に対しては、事前にセキュリティ教育を実施し、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

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。センターのサーバ証明書には、ACM[7]を利用しており、暗号化にはAWSのセキュリティポリシー[8]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

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

[8] 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対策

サーバ群は、AWS の上に構成されます。データセンターのセキュリティ対策は AWS のセキュリティ対策によって行われています。[9]AWS 上のデータベースサーバーは、Multi-AZ で構成されており、障害が発生してもサービスを継続できるように設計されています。AWS 上のデータベース、ストレージで保存されるデータは、暗号化されております。

[9] 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

- Windows®、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、AWS、Powered by AWS ロゴ、[およびかかる資料で使用されるその他の AWS 商標] は、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。

変更履歴

Rev.	改版日	改版内容
1.0	-	初版作成