セキュリティホワイトペーパー

RICOH スマート予約サービス for 会議室

Version 1.0.1

目次

1. はじめに

1.1. 目的

本書は、RICOH スマート予約サービス for 会議室（以下、本サービスと記載）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

本書では、本サービスで利用しているサーバーおよびタブレットアプリケーションのセキュリティー対策を説明対象としています。

クラウドサービスの情報セキュリティー対策の実施に関して、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[1]
2. クラウドサービス利用のための情報セキュリティマネジメントガイドライン[2]

これらは 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[3]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] 総務省、2018 年 7 月
https://www.soumu.go.jp/main_content/000566969.pdf
[2] 経済産業省、2013 年
https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudsec2013fy.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

以下の章の通り、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

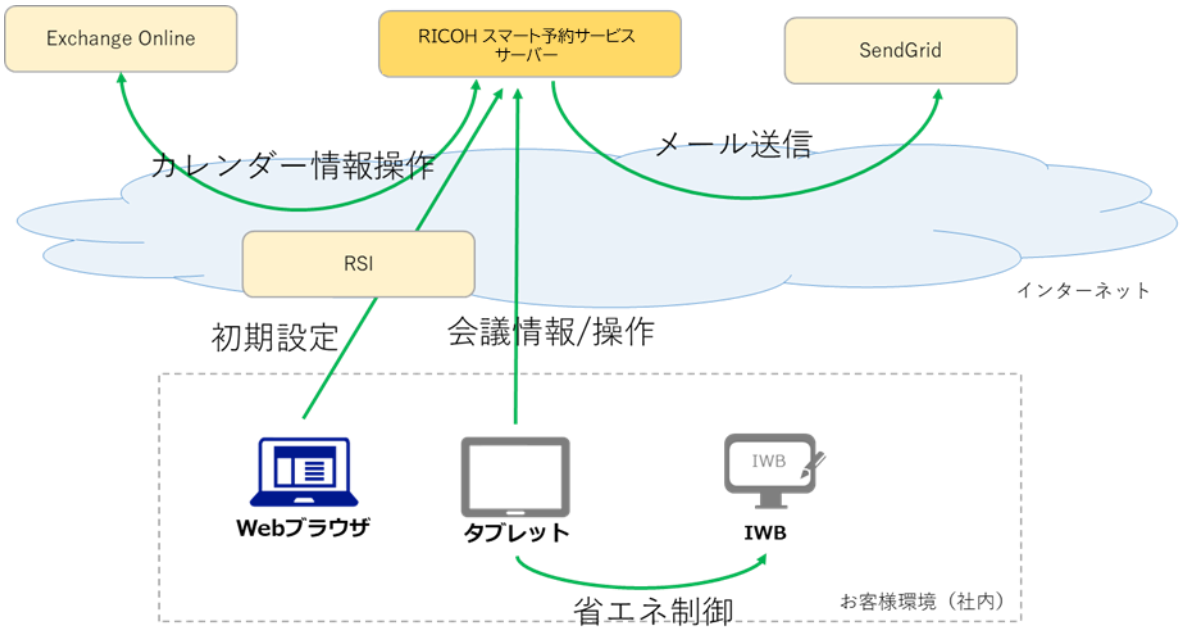

図 1 本サービスのシステム構成図

本サービスは、お客様環境とインターネット上に存在するサービス(具体的には Exchange Online サービス(O365)、SendGrid サービス、RICOH Smart Integration(RSI))から構成されます。本サービスは Exchange Online サービスと通信し、カレンダー情報を取得することで本サービスの機能提供を行います。

2.1.1. 通信プロトコル

2.1.2. お客様環境から本サービスへの通信

表 1 お客様環境から本サービスへの通信

機能	ポート	プロトコル	暗号化	認証
Web ブラウザからの初期設定	443/TCP	HTTPS	TLSv1.2	OAuth 2.0 認証
タブレットアプリケーションからの会議情報取得および操作	443/TCP	HTTPS	TLSv1.2	独自認証(API キーおよびテナント ID)

2.1.3. お客様環境(ローカルネットワーク)内での通信

表 2 お客様環境(ローカルネットワーク)内での通信

機能	ポート	プロトコル	暗号化	認証
タブレットアプリケーションからの RICOH Interactive Whiteboard の省エネ制御	50005/TCP	HTTPS	自己署名	Basic 認証

2.1.4. 本サービスからインターネット環境への通信

表 3 本サービスと外部サービスの通信

機能	ポート	プロトコル	暗号化	認証
Exchange Online(O365)のカレンダー情報操作	443/TCP	HTTPS	TLSv1.2	OAuth 2.0 認証
SendGrid 経由でのメール送信	443/TCP	HTTPS	TLSv1.2	独自認証(API キー)

2.1.5. マルチテナント対応

本サービスは複数の企業・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[4]、複数のテナントの情報を同一の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[5]。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、エンドユーザーが本サービス上のサービス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。

---

[4] 複数の企業が合同で契約するようなテナントも考えられるため、「企業」ではなく「テナント」と言う用語を使用している。

[5] 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」と呼ばれる。

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。またキャパシティ管理[6]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

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

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、既知の脆弱性が残されていないことを確認しています。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 ヵ月に 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. サーバー

サーバーではアプリケーションログと、実行した全ての操作のログを、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、会議室 ID、ユーザー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。また、障害解析のためメールアドレスも含まれています。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。

3.4.2. タブレット

タブレットで動作するタブレットアプリは、サーバーとの通信ログ（入退室や延長等の操作で発生したエラーログ）はタブレット本体に出力しています。ログは、iOS の機能である sandbox を用いてアプリケーションの専用領域に保存されているため、他アプリケーションからアクセスできません。

---

[6] 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う。

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

本サービスで利用するデータは、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、別ユーザーの設定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。

4.1.1. ユーザー認証

ログイン
本サービスのユーザーサイトにアクセスするには、ユーザーID、パスワードによる OAuth 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様になっています。

ユーザーID やパスワードは、RICOH Smart Integration から発行されるアカウントです。
OAuth では、お客様が認可された情報を本サービスのログイン情報として利用するため、RSI のパスワードが本サービス側に送信、保存されることはありません。

4.1.2. ロールとテナント間のアクセス制御

本サービスで利用するユーザーのロールにはシステム管理者ロール、アカウント管理者ロールと運用管理者ロール、一般ロールの 4 種類があります。

RICOH Smart Integration の企業管理者ロールのユーザーが、自動的に本サービスのシステム管理者のユーザーとして設定さます。システム管理者は、次に記載するアカウント管理者、運用管理者両方の権限をもち、操作を行うことがでます。
アカウント管理者は、お客様テナントに所属する管理者ユーザーの管理および次の章に記載するカレンダーサービス連携が行えます。
運用管理者は、お客様テナントに属する会議室の追加・変更・削除を行えます。また、会議室ごとの運用設定が行えます。

4.1.3. カレンダーサービス連携

前記アカウント管理者(もしくは、システム管理者)により、カレンダーサービスと連携するための権限委譲（接続情報）の設定を行います。連携のために必要な認証情報を外部に取り出すインターフェイスは存在せず、システムは OAuth 認証によるサービス連携を使用します。

4.2. データ管理（タブレット側）

4.2.1. アプリケーション

アプリケーションは iOS の機能である sandbox を用いてアプリケーションの専用領域に保存されており、また iOS 上のアプリケーションには署名が義務付けられているためアプリケーションに改竄や変更が加えられません。

4.2.2. ユーザー情報

アプリケーション内で利用される接続情報等は、アプリケーション内で暗号化しアプリケーション固有の内部ストレージに保存されます。アプリケーション固有領域のため他アプリケーションからアクセスすることはできません。

4.3. データ管理（サーバー側）

4.3.1. イベント情報

カレンダーサービスから取得したイベント情報のデータは本サービスのサーバーに保存されますが、その保存先は Azure のファイアウォールの内側にあること、その保存先へのアクセスはシステム内部に限定していることの 2 つの理由から利用者には外部からアクセスする手段が無いため、データが漏洩することはありません。
また、データを保存するデータベース自体の暗号化は Azure 側の機能により自動で行われます。

4.3.2. 通知先設定情報

各ユーザーが設定した通知先情報のデータは本サービスのサーバーに保存されていますが、その保存先は Azure のファイアウォールの内側にあること、その保存先へのアクセスはシステム内部に限定していることの 2 つの理由から利用者には外部からアクセスする手段が無いため、データが漏洩することはありません。
また、データを保存するデータベース自体の暗号化は Azure 側の機能により自動で行われます。

5. アクセス制御

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、Azure の関数キーと呼ばれる認証機構により、不特定多数のアカウントからアクセスできないように制御を行っています。

5.1.2. サーバーのアクセス制御

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少人数に限定し、担当者の移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、データの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)、タブレットアプリケーションとサーバー間の通信は、メールを除き、すべて HTTPS で通信経路の暗号化がされています。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 RSA2048 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、以下のものをサポートしています。
・TLS 1.2

5.2.1. データセンターのセキュリティー対策

本サービスのサーバー群は、Azure 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 Azure のセキュリティー対策によって行われております。[7]

[7] Microsoft Azure セキュリティーの概要：
https://docs.microsoft.com/ja-jp/azure/security/azure-security-getting-started

6. 商標

- Microsoft、Windows、Windows Server、Azure、Office 365、Outlook、 .NET Framework 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。
- 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。
- SendGrid の名称およびそのロゴは、SendGrid 社の登録商標です。
- AppScan®は、世界の多くの国で登録された HCL Technologies Ltd. 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。
本書の説明および所有者の権利のために使用されます。この仕様によって所有者の権利を侵害するものではありません。