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*** フリーアドレス

Version 1.0.0

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 フリーアドレス(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、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. 本書の説明対象となる範囲

本サービスで利用しているサーバー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す。
次章より説明する本サービスのセキュリティー対策も上記ガイドラインに則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に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に準し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、（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。

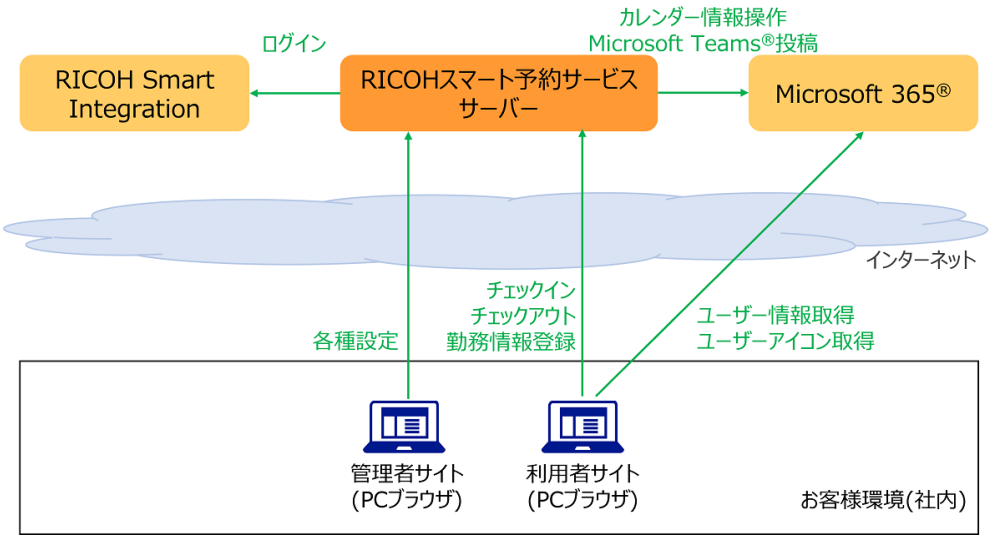
2章 システム構成
3章 システム全般のセキュリティー対策
4章 データのセキュリティー対策
5章 ネットワークのセキュリティー対策
6章 データセンターのセキュリティー対策

2. システム構成

2.1. 全体構成

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下記サービスから構成されます。

- RICOHスマート予約サービスサーバー
- RICOH Smart Integration
- Microsoft 365®



2.2. 通信プロトコル

2.2.1. お客様環境からスマート予約サービスサーバーへの通信

機能	ポート	プロトコル	暗号化	認証
管理者サイトの利用	443/TCP	HTTPS	TLSv1.2	OAuth 2.0認証 Cookie認証
利用者サイトの利用	443/TCP	HTTPS	TLSv1.2	OAuth 2.0認証 Cookie認証

ログイン時はOAuth 2.0認証でRICOH Smart Integrationに対するログインを実施し、ログインに成功するとスマート予約サービスサーバーでセッションCookieを発行します。
セッションの有効期限が切れるまではスマート予約サービスサーバーへのアクセスはCookieにより認証します。
ログイン中にRICOH Smart Integrationの利用権限が無くなった場合は、セッションの有効期限内でもスマート予約サービスサーバーにアクセスできなくなります。
RICOH Smart Integrationの利用権限が無くなってからスマート予約サービスサーバーにアクセスできなくなるまで、数分程度のタイムラグが発生する場合があります。

2.2.2. お客様環境から**Microsoft 365®**への通信

機能	ポート	プロトコル	暗号化	認証
Microsoft 365®からの情報取得	443/TCP	HTTPS	TLSv1.2	OAuth 2.0認証

Microsoft 365®連携設定が実施されていない場合は、本通信は発生しません。

2.2.3. スマート予約サービスサーバーからインターネット環境への通信

機能	ポート	プロトコル	暗号化	認証
RSIの認証	443/TCP	HTTPS	TLSv1.2	OAuth 2.0認証
Microsoft 365®のカレンダー情報操作	443/TCP	HTTPS	TLSv1.2	OAuth 2.0認証
Microsoft Teams®投稿	443/TCP	HTTPS	TLSv1.2	OAuth 2.0認証

Microsoft 365®連携設定が実施されていない場合は、Microsoft 365®に対する通信は発生しません。

2.3. 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 、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。
データアクセスに関しては、データアクセス制御 に記載しています。
テナントは、ユーザーが本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。
なお、本サービスではユーザーが所属するRICOH Smart Integrationのテナントが同一の場合は同一テナント、RICOH Smart Integrationのテナントが異なる場合は他テナントとみなします。
ユーザーが本サービスを利用して登録したデータは、登録を行ったユーザーが所属するテナントに属します。

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。
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HCL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、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

スマート予約サービス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、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。

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テナントのユーザー情報が目にふれることはありません。

4.2. ユーザー認証

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、パスワードを利用した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、RICOH Smart Integrationのパスワードがスマート予約サービスサーバーに送信、保存されることはありません。

4.3. 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、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れます。
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きます。
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が行えます。
運用管理者は、お客様テナントに属するフロアの追加・変更・削除を行えます。また、フロアごとの運用設定が行えます。
なお、利用者サイトの各機能の利用は、全てのユーザーが行えます。

4.4. Microsoft 365®連携

Microsoft 365®と連携するための権限委譲の設定が可能です。
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。

4.5. データ管理

4.5.1. ブラウザ

ブラウザ内のアプリケーション固有領域のストレージに保存するため、他のアプリケーションからアクセスすることはできません。

4.5.2. サーバー

各種設定情報はスマート予約サービス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。

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、多要素認証の設定およびパスワードは容易に推測されないようにするための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)とサーバー間の通信は、すべてHTTPSで通信経路の暗号化がされています。
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

6. 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®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. 商標

- Microsoft®、Azure®、Microsoft 365®、Microsoft Teams®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。
- 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。この使用によって所有者の権利を侵害するものではありません。