RICOH Remote Concierge System

セキュリティ ホワイトペーパー（Ver1.0）

RICOH
imagine. change.

株式会社 リコー

2019年12月

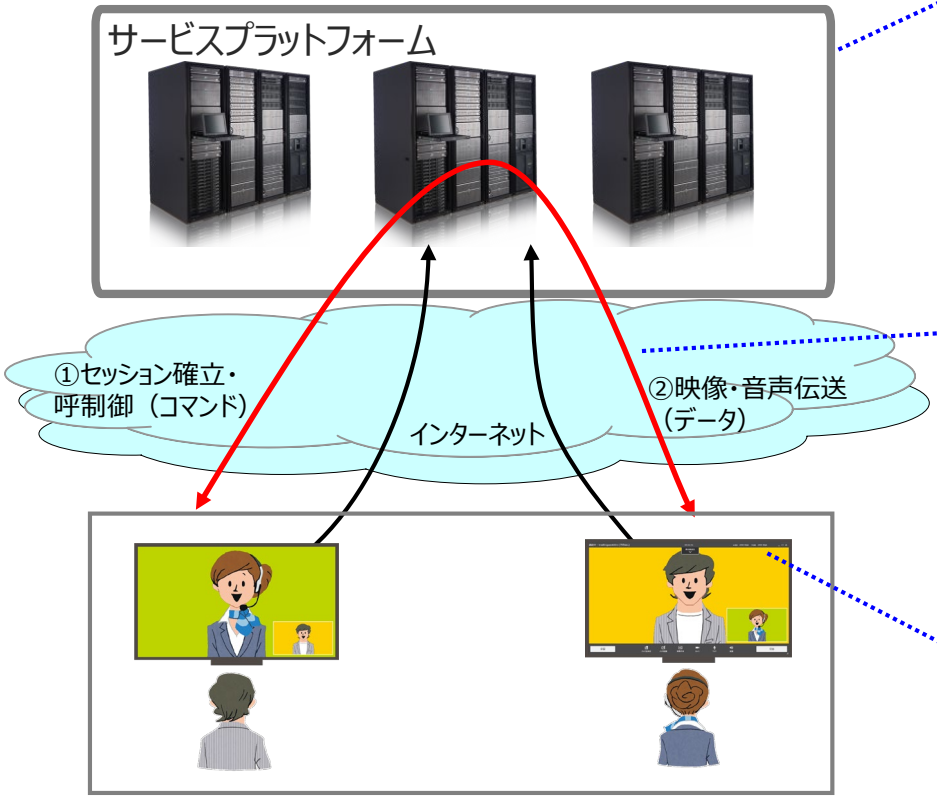
変更履歴

RICOH
imagine. change.

日付	バージョン	前バージョンからの変更
2019年12月	1.0	初版発行

全体概要

Ricoh Remote Concierge System（以降、リモートコンシェルジュとする）は、クラウド上に構築されたサービスプラットホームを介して通信を行う。サービスプラットホームは端末同士の接続を制御するとともに、映像・音声データを中継する。



サービスプラットフォーム（クラウド）

冗長化による可用性確保
サービスプラットフォームを構成するF/W、ネットワーク機器、サーバは全て冗長化されている。

アクセス制限
ファイアウォールによるアクセス制限を行なっている。

脆弱性対策
ツールを用いた脆弱性評価を3ヶ月毎に実施している。脆弱性が発見された場合には、５営業日以内に対応を実施している。

システム監視
サービスプラットホーム内部での監視に加えて、外部から通話が正常に行われることを確認している。

通信

①セッション確立・呼制御
セッション確立後、呼制御に必要な情報はTLS により暗号化されている。

②映像・音声伝送
映像・音声、PC画面共有データは全て暗号化されている。ストリーミングデータ転送方式SRTP

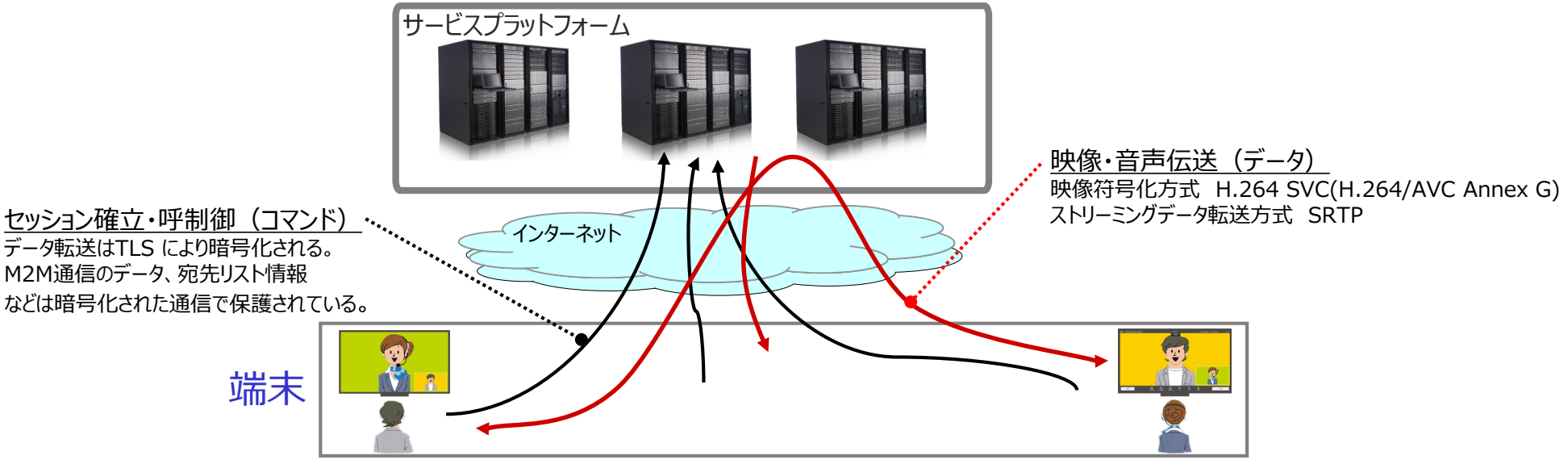
端末

脆弱性対策
ソフトウェアに脆弱性が発見された場合は、対策を講じたソフトウェアをインターネット経由でアップデートさせる仕組みを提供している。

不正利用防止
ご利用中のアカウントを紛失・盗難された時は、そのアカウントを指定して管理コンソールまたはリコー側で利用を停止することで、アカウントの不正利用を防止することができる。アカウントの指定は、ログインIDで行う。本サービス向けアプリケーションはログインIDとパスワードのセットで認証を行い利用できる仕組みとしている。

通信相手の制限
想定外の相手からの通信を制限するため、事前に設定された同一企業（テナント）内の端末からのコール（通話要求）しか許可されない仕組みとしている。このため、本サービスを利用している別テナントからのコールは発生しない。

システムのセキュリティについて



セッション確立・呼制御（コマンド）
データ転送はTLS により暗号化される。
M2M通信のデータ、宛先リスト情報
などは暗号化された通信で保護されている。

映像・音声伝送（データ）
映像符号化方式　H.264 SVC(H.264/AVC Annex G)
ストリーミングデータ転送方式　SRTP

セッション確立・呼制御
リモートコンシェルジュはアプリを起動するとまず、サービスプラットフォームへ接続し、待ち受け画面が表示される。
起動した後、データ転送は全てTLSにより暗号化される。
SRTP(Secure RTP)と呼ばれる映像・音声データを暗号化する通信方式を利用する。これにより映像・音声データを盗聴・保存されても暗号化されているため復元はできない。

インターネットからサービスプラットフォームへのアクセス制限
F/Wにより、管理コンソールによるブラウザからのHTTPSアクセスと、認証に成功したリモートコンシェルジュ端末からの指定ポートを使用したアクセスのみ受け付ける。また、ツールを用いた脆弱性評価を３ヶ月毎に実施している。

システムの監視
監視ソフトウェアを用いて、CPUやメモリ、ネットワーク帯域などのリソース監視やログ監視を行っている。
また専用ソフトウェアを外部に複数配置し、通話の開始及び実行が正常に行われることを監視している。

サービスプラットフォームのセキュリティについて

RICOH
imagine. change.

サービスプラットフォーム全体について

サービスプラットフォームは複数のデータセンターで構成されており、天災や大規模な障害などによって一つのデータセンターが利用不可能になったとしても、それ以外のデータセンターを自動的に利用しサービス継続するように設計されている。
各データセンターはいずれもISO27001認証を取得している。

データセンター内のインフラ構成について

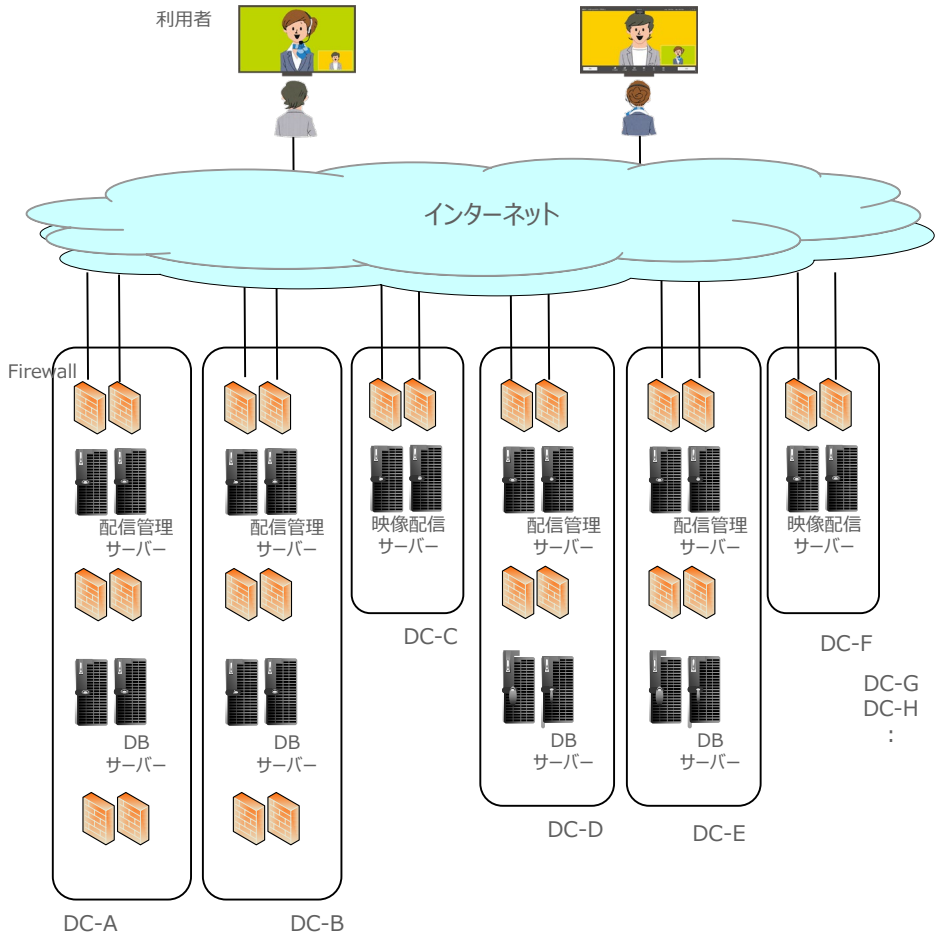
F/W、ネットワーク機器、データベース、アプリケーションサーバは全て冗長化している。映像配信サーバも冗長化され、利用者数の増加に合わせてスケールアウトし常に十分なリソースを確保している。
重要なデータを格納するデータベースは、二重のF/Wの内側にのみ配置し、情報流出を防止している。
またインターネットとの接続も冗長化されている。

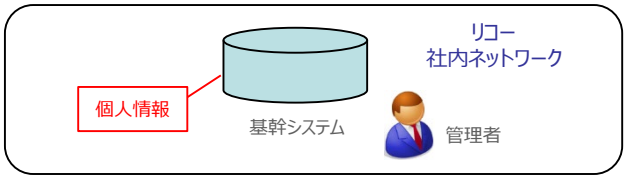
お客様の個人情報について

契約時に頂く個人情報は本サービスプラットフォーム内には記録しておらず、リコーネットワーク内の基幹システムでのみ管理されている。

脆弱性対策について

ツールを用いた脆弱性評価を３ヶ月毎に実施している。
脆弱性が発見された場合には、対応を５営業日以内に実施している。





端末セキュリティ
（店舗・コンシェルジュ向けアプリケーション）

RICOH
imagine. change.

情報漏洩防止

１）ユーザー情報

アプリケーション内で利用されるユーザーや環境に関わる情報は、クライアント端末内で暗号化し、Windowsのプロファイルフォルダに保存されている。

２）アプリケーションログ情報

Windowsのプロファイルフォルダに保存されており、他ユーザーからアクセスできない。

３）プログラム内情報

アプリケーション内の重要な情報を暗号化処理することで、情報漏洩の危険性を低減している。

プログラム不正改竄防止

インストーラにコードサイニング署名を施して配布しているため、リコーが配布するインストーラに改竄や変更が加えられていないことが確認できる。

端末レポート送信

本サービス利用時に発生した問題について、端末側で起こっていたことを解析に用いるため、端末側より情報（レポート）を送信する機能を提供している。なお、収集したレポートはソフトウェアおよびハードウェアの問題を診断するためにリコーが利用する。これ以外の目的で利用することはない。