# AudioCodes Services

*The Voice Experts @ Your Service*

Live Platform

# Data Flows, Connectivity and Security Measures

# 目次

**改訂履歴**

| 改訂日 | 改訂内容 | 改訂責任者 |
|---|---|---|
| 2024年6月16日 | 初版発行 | Ofir Nakar |
| 2024年6月25日 | カスタマーポータルに関する情報を追加 | Ofir Nakar |
| 2024年7月18日 | - セキュアクラウドに関する記載を追加<br>- Add Voca as Serviceに関する記載を追加<br>- サービス提供場所一覧表を更新 | Ofir Nakar |
| 2024年7月21日 | - SOC2–Type2に関する記載を追加<br>- プライバシー関連規制に関する記載を追加 | Ofir Nakar |
| 2024年9月21日 | - オンプレミスSBC向け Central Syslog Serviceに関する記載を追加 | Ofir Nakar |
| 2024年9月25日 | - Meeting InsightsにおけるAI技術に関する記載を更新 | Ofir Nakar |
| 2024年11月24日 | - Interaction Recording Serviceの名称を「Interaction Insights」に変更<br>- APAC地域における共通サービス提供場所を更新 | Ofir Nakar |
| 2024年11月25日 | - Central Syslog Serviceの送信トラフィックに関して、顧客側で許可すべきサブネット情報を追加 | Ofir Nakar |
| 2024年12月10日 | - MIAaaSおよびInteraction Insightsに関するAPAC地域の提供場所を更新 | Ofir Nakar |
| 2024年12月10日 | - MIAaaSおよびInteraction Insightsに関するAPAC地域の提供場所を更新 | Ofir Nakar |
| 2025年2月19日 | - Central Debug Recording Serviceに関する記載を追加 | Ofir Nakar |
| 2025年3月19日 | - WebSocketに関するDNSアクセス情報を更新<br>- ISO27032に関する記載を更新 | Ofir Nakar |

# 1 はじめに

本書は、AudioCodes Liveプラットフォームにおける接続オプション、データの流通、およびサービスおよび情報の保護に関するセキュリティ対策について説明することを目的としています。

AudioCodes Ltd.（以下「当社」といいます）は、サービスプロバイダーおよび企業向けに、先進的なVoIP（Voice over IP）および統合型VoIP・データネットワーキング製品およびアプリケーションを設計・開発・販売しています。

当社は、世界中のサービスプロバイダーおよび企業に対し、統合型VoIPおよびデータソリューションを提供する革新的なリーディングサプライヤーとなることを目指しています。

当社の本社はイスラエルに所在します。

当社は、従業員、パートナー、顧客および取引先の情報を含む、保有または処理するすべてのデータの機密性、完全性および可用性を保護することに尽力しています。この取り組みの一環として、当社の経営陣は、情報セキュリティマネジメントシステム（ISMS）を確立・維持するため、ISO-27001規格の採用および実施を決定しました。

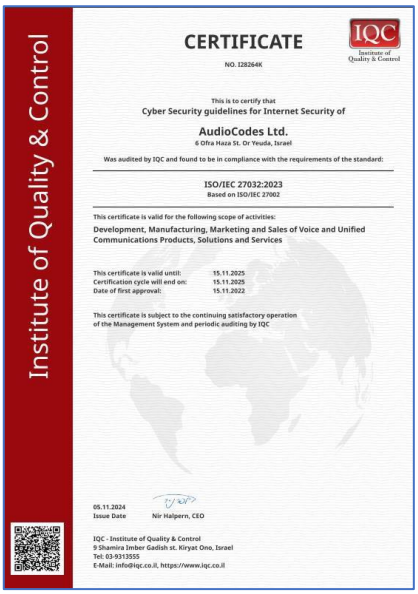
当社は、各国の情報セキュリティおよびプライバシーに関する法令の適用を受けており、当社の全従業員は、これらの法令を遵守する責任を負います。

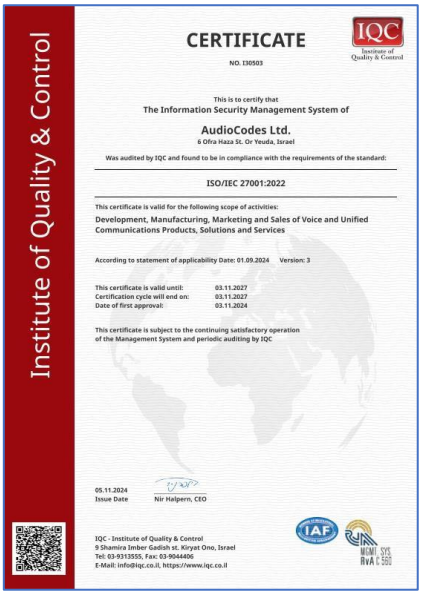
当社は、厳格なセキュリティおよびプライバシー基準を有する世界有数の企業に対してサービスを提供しており、長年にわたり、貴重なデータ資産の取扱いに関して信頼を獲得してまいりました。参考情報については、別途ご請求により提供可能です。

## 1.1 ISO 27001, ISO 27032について

ISO 27001およびISO 27032は、情報セキュリティマネジメントシステム（ISMS）の要件を定めた国際的に広く認知された規格であり、AudioCodesはこれらの規格に基づく十数種類の方針および手続を活用し、顧客情報、財務データ、知的財産、従業員情報、ならびに第三者から委託された情報等、各種資産のセキュリティ管理を実施しています。


IQC
Institute of Quality & Control
CERTIFICATE
NO. 128264
This is to certify that
the Information Security Management System- Cyber Security Techniques of
AudioCodes Ltd.
1 Ha-Yarden St. Lod, Israel
Was audited by IQC and found to be in compliance with the requirements of the standard:
ISO/IEC 27001:2022 – ISO/IEC 27032:2023
This certificate is valid for the following scope of activities:
Manufacturing, marketing and sales of voice and unified communications solutions and services
According to statement of applicability Date: 14.08.2023 Version: 2
This certificate is valid until: 15.11.2025
Certification cycle will end on: 15.11.2025
Date of first approval: 15.11.2022
This certificate is subject to the continuing satisfactory operation of the Management System and periodic auditing by IQC
14.11.2023 Issue date
Nir Halpern, CEO
Institute of Quality & Control Ltd.
6 Ravnitzky St., Petah Tikva 4900017, Israel
Tel: 03-9313555, Fax: 03-9044406
E-Mail: info@iqc.co.il, www.iqc.co.il


Institute of Quality & Control
CERTIFICATE
NO. 128264K
This is to certify that
Cyber Security guidelines for Internet Security of
AudioCodes Ltd.
6 Ofra Haza St. Or Yeuda, Israel
Was audited by IQC and found to be in compliance with the requirements of the standard:
ISO/IEC 27032:2023
Based on ISO/IEC 27002
This certificate is valid for the following scope of activities:
Development, Manufacturing, Marketing and Sales of Voice and Unified Communications Products, Solutions and Services
This certificate is valid until: 15.11.2025
Certification cycle will end on: 15.11.2025
Date of first approval: 15.11.2022
This certificate is subject to the continuing satisfactory operation of the Management System and periodic auditing by IQC
05.11.2024 Issue Date
Nir Halpern, CEO
IQC - Institute of Quality & Control
9 Shamira Imber Gadish st. Kiryat Ono, Israel
Tel: 03-9313555
E-Mail: info@iqc.co.il, https://www.iqc.co.il


Institute of Quality & Control
CERTIFICATE
NO. 130503
This is to certify that
The Information Security Management System of
AudioCodes Ltd.
6 Ofra Haza St. Or Yeuda, Israel
Was audited by IQC and found to be in compliance with the requirements of the standard:
ISO/IEC 27001:2022
This certificate is valid for the following scope of activities:
Development, Manufacturing, Marketing and Sales of Voice and Unified Communications Products, Solutions and Services
According to statement of applicability Date: 01.09.2024 Version: 3
This certificate is valid until: 03.11.2027
Certification cycle will end on: 03.11.2027
Date of first approval: 03.11.2024
This certificate is subject to the continuing satisfactory operation of the Management System and periodic auditing by IQC
05.11.2024 Issue Date
Nir Halpern, CEO
IQC - Institute of Quality & Control
9 Shamira Imber Gadish st. Kiryat Ono, Israel
Tel: 03-9313555, Fax: 03-9044406
E-Mail: info@iqc.co.il, https://www.iqc.co.il

## 1.2 プライバシー関連規制への対応

AudioCodesは、GDPR（一般データ保護規則）、CCPA（カリフォルニア州消費者プライバシー法）、CPRA（カリフォルニア州プライバシー権利法）、LGPD（ブラジル一般データ保護法）その他のプライバシー関連規制に準拠しています。

これらの規制は、GDPRを基盤としており、GDPRは数十ページにわたる規定を有し、個人データの収集、処理、取扱いおよび保存に関するほぼすべての側面において、企業および組織に厳格な義務を課しています。同時に、GDPRは、データ主体が自身の個人データの収集および利用方法を管理する権利を強化しており、救済措置についてもGDPRの文言により定義されています。

当社および当社の顧客におけるデータ取扱いがGDPRに準拠するよう、継続的にコンプライアンス対応を実施しています。当社は、BDO（コンサルタント）と連携し、GDPRへの準拠を確保するための一連の手順および方針を策定しました。

策定された手順には、以下を含み、これらに限定されるものではありません：

- プライバシーポリシー
- 第三国への個人データの移転
- 個人データの記録保持
- データの保存期間、返還および削除
- 個人情報の開示
- データ主体の権利

## 1.3 SOC 2 – Type 2

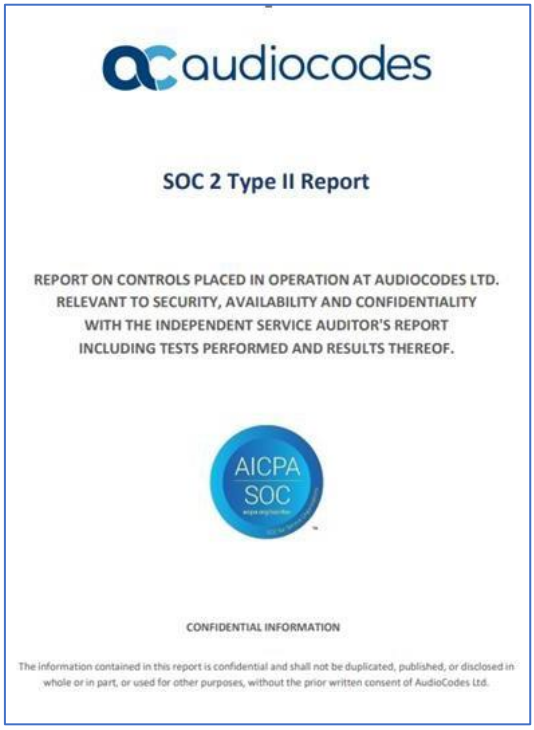
SOC 2監査は、SSAE 18（米国公認会計士協会基準書）に基づき、
AICPA（米国公認会計士協会）のTSC（信頼サービス基準）に照らして、
サービス提供事業者のセキュリティ、可用性、処理の完全性、
機密性に関する統制を評価するものです。

**対象製品およびサービス**

AudioCodes Live Platformは、Azure上で提供されるサービス提供型プラットフォームであり、
UCaaS（Unified Communications as a Service）およびCCaaS（Contact Center as a Service）
環境向けに、以下のような各種サービスを含んでいます：

PSTN接続, コンタクトセンター機能, 録音機能, AIを活用した会議インサイト, デバイス管理,
ユーザー管理,その他音声コミュニケーションの提供を効率化するためのサービス

本プラットフォームは、世界100か国以上に展開する当社のパートナーネットワークを
通じて販売されています。
SOC 2 タイプ2監査報告書は、秘密保持契約（NDA）締結後にご請求に応じて提供いたします。


audiocodes

SOC 2 Type II Report

REPORT ON CONTROLS PLACED IN OPERATION AT AUDIOCODES LTD.
RELEVANT TO SECURITY, AVAILABILITY AND CONFIDENTIALITY
WITH THE INDEPENDENT SERVICE AUDITOR'S REPORT
INCLUDING TESTS PERFORMED AND RESULTS THEREOF.

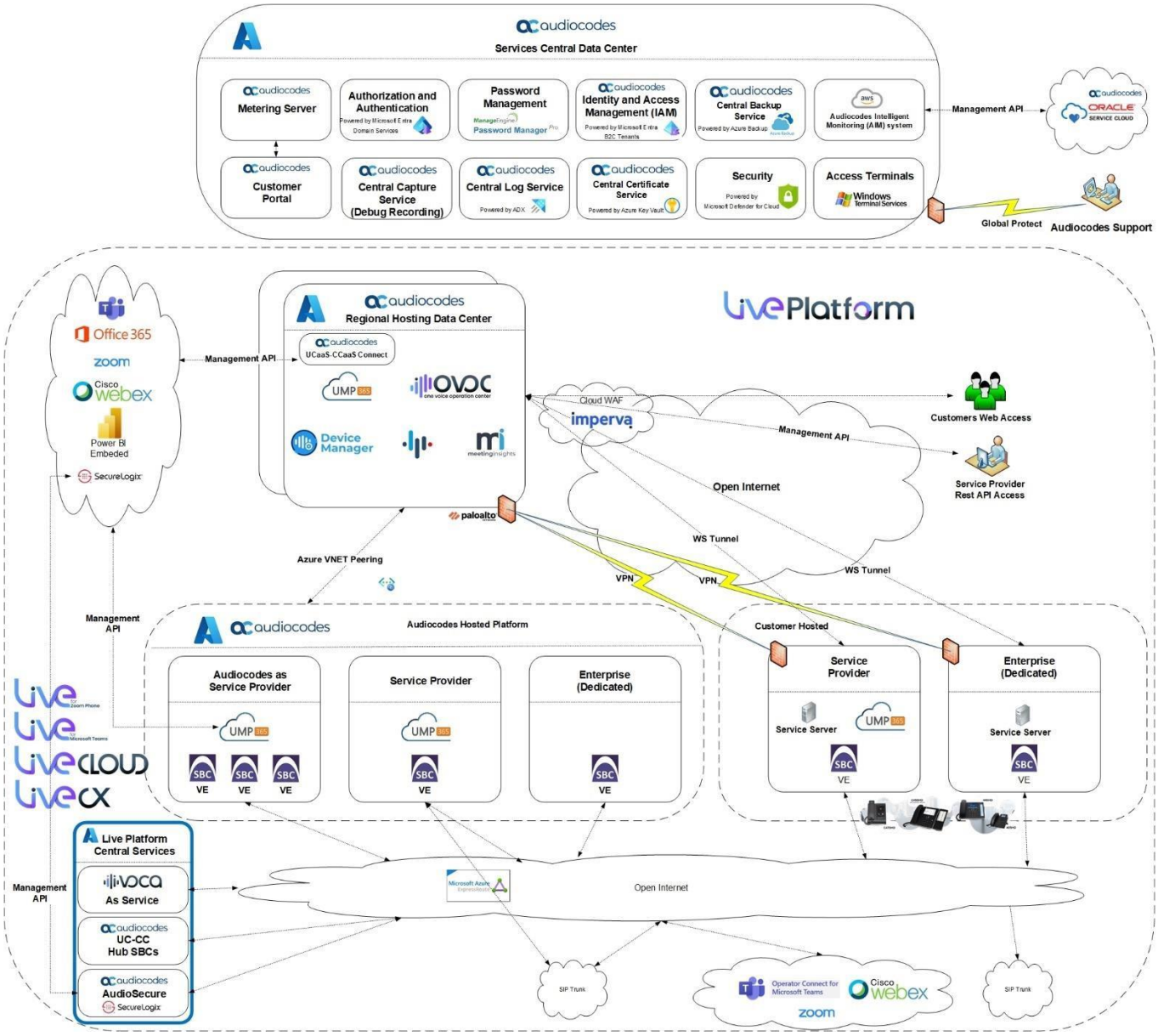
AICPA SOC

CONFIDENTIAL INFORMATION

The information contained in this report is confidential and shall not be duplicated, published, or disclosed in whole or in part, or used for other purposes, without the prior written consent of AudioCodes Ltd.

# 2 Live Platformの構成

以下の図は、Live Platformの構成を示しています。



## 2.1 主要構成要素

- Mediant Virtual Edition (VE) SBC：サービスレベルに応じて、高可用性構成または　地理的冗長構成での導入が可能なセッションボーダーコントローラー
- UMP 365 - AudioCodes' User Management Pack 365：AudioCodesによるユーザー管理パッケージ
- Audiocodes UCaaS-CCaaS Connect：統合コミュニケーションおよびコンタクトセンターサービスとの接続機能
- Audiocodes Voca as Service：音声認識・AI機能を活用したクラウドサービス
- Live Platform Portal - One Voice Operations Center (Live OVOC)：運用管理ポータル
- AudioCodes Intelligent Monitoring service (AIM)：インテリジェント監視サービス
- AudioCodes Central Log Service：統合ログ管理サービス
- Password Management Pro (PMP)：パスワード管理ツール
- AudioCodes Identity and Access Management (IAM)：認証・認可管理サービス
- Access Terminals：AudioCodesサービス担当者がアクセス可能なWindowsターミナルサーバー
- Central Certificate Service：Liveサービス用証明書の保存リポジトリ
- Service Server：Syslogおよびデバッグ用のローカルサーバー
- Oracle Service Cloud ：AudioCodesのサポートチケット管理システム（Oracle Service Cloudを使用）

## 2.2 Live Platformおよびサービス提供拠点

本項では、Microsoft Azure上におけるLive Platformポータルのグローバルなホスティング拠点について説明するとともに、各地域において提供されるサービスの内容を明示します。

Azureの拠点およびデータの所在に関する詳細情報については、以下をご参照ください：
Data Residency in Azure | Microsoft Azure

| Service | | Regional Live Platform Portal (Live OVOC, UCaaS-CCaaS, UMP) Azure region | | | | |
|---|---|---|---|---|---|---|
| | | **Americas USA** (East US) | **Americas Canada** (Central Canada) | **EMEA** (West Europe) | **APAC** (Australia East) | **India** (Central India) |
| Meeting Insights | Azure region (Service) | West US 2 | X | North Europe | Australia East | X |
| Device Manager | | East US | Central Canada | West Europe | Australia East | Central India |
| Interaction Insights | | West US 2<br>West Central US (Double Recording Region) | X | North Europe<br>West Europe (Double Recording Region) | Australia East | X |
| Live CX – HA SBCs (Shared) | | Americas [1]<br>East US<br>West US<br>EMEA: Germany West Central<br>APAC [1]<br>Southeast Asia,<br>Korea Central | X | Americas:<br>East US<br>EMEA:<br>West Europe<br>Germany West Central<br>APAC:<br>Southeast Asia | Americas<br>West US<br>APAC<br>East Asia<br>Australia East<br>Australia Southeast | X |
| Live for Teams -HA SBCs (Shared) | | Americas [1]<br>East US<br>West US<br>EMEA:<br>Germany West Central<br>APAC [1]<br>Southeast Asia,<br>Korea Central | X | Americas:<br>East US<br>EMEA:<br>West Europe<br>Germany West Central<br>APAC:<br>Southeast Asia | Americas<br>West US<br>APAC<br>East Asia<br>Australia East | X |
| Live for Zoom -HA SBCs (Shared) | | Americas [1]<br>East US<br>West US<br>EMEA:<br>Germany West Central<br>APAC [1]<br>Southeast Asia,<br>Korea Central | X | Americas:<br>East US<br>EMEA:<br>West Europe<br>Germany West Central<br>APAC:<br>Australia East | Americas<br>West US<br>APAC<br>East Asia<br>Australia East<br>Australia Southeast | X |
| Live Platform for Channels (Global Service – Provide to all regions) | | | | Americas:<br>West US 2<br>EMEA:<br>West Europe<br>South Africa North<br>APAC:<br>Australia East | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Live for WebEx Cisco | | TBD | TBD | TBD | TBD | TBD |
| Hybrid Entities | | TBD | TBD | TBD | TBD | TBD |
| Voca as Service [2] | | Web and SBC:<br>East US 2<br>IVRs:<br>East US 2<br>North Central US | X | Web and SBC:<br>West Europe<br>IVRs:<br>West Europe<br>UK South | Web and SBC:<br>Australia East<br>IVRs:<br>Australia East<br>Australia Central | Web and SBC:<br>Central India<br>IVRs:<br>Central India<br>South India |
| AudioSecure | | East US<br>West US | SIP can be connected via US site | X | X | X |
| Live Cloud DR (Dedicated) | | Per demand [3] | Per demand [3] | Per demand [3] | Per demand [3] | Per demand [3] |
| Operator Connect (Dedicated) | | Per demand [4] | Per demand [4] | Per demand [4] | Per demand [4] | Per demand [4] |
| Live CX (Dedicated) | | Per demand [5] | Per demand [5] | Per demand [5] | Per demand [5] | Per demand [5] |
| Live Dedicated | | Per demand [6] | Per demand [6] | Per demand [6] | Per demand [6] | Per demand [6] |

[1] Geo-Redundant option available.

[2] SIP cross connection between regions is allow.

[3] SBC HA (Appliance or SW SBC) and UMP can be hosted on any Customer's Cloud or on Premises

[4] SBCs HA (Appliance or SW SBC) and UMP can be hosted on any Customer's Cloud or on Premises

[5] SBC (Appliance or SW SBC) can be hosted on any Customer's Cloud or on Premises

[6] Some Solution Components can be hosted on any Customer's Cloud or on Premises

# 3 構成要素の接続性およびセキュリティ対策

## 3.1 アクセス管理

以下の内容は、AudioCodes サービスのユーザーライフサイクルを説明したもので、サービスおよびオンプレミスシステム（およびそのデータ）へのアクセスは、世界各地に所在するAudioCodesの認定サービスエンジニアのみに制限されていることを示すものである。

- **オンボーディングAPI:** 新たに従業員が加わった際、その情報はAudioCodesのOracle HRシステムに登録される。これにより、APIを通じて、権限やグループに属さないユーザーが企業のActive Directoryに作成される。
- **ディレクトリの分離:** AudioCodes Global Services（AudioCodes.com）は、AudioCodes Corporate（AudioCodes-corp.com）とは別のActive Directoryを管理している。
- **アクセス制御:** AudioCodesサービスの本番環境テナントへのアクセスは、AudioCodes Corp Active Directoryのサービス用配信グループのメンバーに限定される。以下の配信グループの所有者（地域マネージャー）は、対象者をメンバーとして追加する責任を有する。
  - ServicesEMEA – for EMEA region
  - ServicesAmericas – for America's region
  - ServicesAPAC – for APAC region
- **ユーザー同期:** APIは、すべての現行AudioCodesユーザーとAudioCodes Corp Active Directoryサービス配信リストのメンバーを比較する。新規ユーザーが配信グループに追加された場合、APIはAudioCodes上に新規ユーザーを作成する。
- **退職処理:** HRがOracleに退職日を設定すると、APIは企業のActive Directory上で当該ユーザーを無効化する。
- **比較プロセス:** APIはAudioCodes Corp Active Directoryサービス配信グループからメンバーリストを取得し、AudioCodes上の全ユーザーと比較する。
- **ユーザー検証:** AudioCodes上で検出された各ユーザーについて、APIは当該ユーザーがAudioCodes Corp Active Directoryサービス配信リストに存在するかを確認する。存在しない場合、当該ユーザーはAudioCodes上で無効化される。
- **Comparison Process:** APIはすべての無効化されたユーザーを識別し、60日以上無効化されたユーザーを削除する。
- **即時退職処理:** 高権限ユーザーの即時退職が必要な場合、企業IT部門は当該ユーザーを即時に無効化する権限を有し、これによりAudioCodes上でも無効化される。
- **職務変更:** ユーザーがAudioCodesサービス組織外の職務に異動した場合、地域マネージャーは当該ユーザーをAudioCodes Corp Active Directoryサービス配信グループから削除し、これによりAudioCodes上でも無効化される。
- **AudioCodesサービスデータセンターへのアクセス:** AudioCodesのサービスデータセンターへのアクセスは、AudioCodesaaS Active Directoryによる認証に基づく多要素認証（MFA）を用いたクライアントからサーバーへのIPSec VPNトンネルを通じて提供される。

- **パスワード要件:** AudioCodesのサービス用Active Directoryにおけるパスワードは、エンジニアの場合は8文字以上、管理者の場合は12文字以上とし、英大文字、英小文字、数字（0～9）、特殊文字（例：!, #, $）、Unicode文字のうち、少なくとも3種類の文字を含むものとする。また、パスワードにはユーザー名からの文字を2文字以上含めてはならず、過去24回分のパスワードは再利用できないものとする。さらに、ユーザーは90日ごとにパスワードを変更する義務を負うものとする。

## 3.2 環境セキュリティ

以下は、世界各地に所在するAudioCodesの認定サービスエンジニアのみに限定された、サービスおよびオンプレミスシステム（並びにそれらのデータ）への排他的アクセスに関するセキュリティ対策について記載するものである。

- AudioCodesサービスエンジニアによるアクセス端末サーバーおよびUMPへの認証は、AudioCodesのサービス用Active Directoryを通じて行われるものとする。
- SBC（セッションボーダーコントローラー）への認証は、Secure LDAPを用いたAudioCodesサービス用Active Directory認証により実施される。
- Live Platformポータルへの認証は、Azure Entra IDを用いた多要素認証（MFA）に基づくものとする。
- （任意）AudioCodesのデータセンター内の端末サーバー（Windows Server 2019）から、RDPを用いてAudioCodesオンプレミスのサービスサーバーへアクセスする場合、サイト間VPNを通じて、ローカルまたはドメインユーザーの資格情報（パスワードは有効期限なし）を用いるものとする。
- AudioCodes Live Platformソリューションコンポーネントの内部インターフェース（RDP（3389）、CLI（SSH））へのアクセスは、AudioCodesのデータセンター内のアクセス端末サーバー（Windows Server 2019）または（任意で）オンプレミスのサービスサーバーからのみ許可される。
- Live PlatformポータルのWebインターフェース（HTTPS（443））へのアクセスは、Imperva製のクラウドWAFにより保護されたパブリックインターネット経由で行われ、多要素認証（MFA）が必須とされる。
- サービスがAudioCodesにより完全にホスティングされる場合、該当する専用サービスについては、Live顧客向けソリューションコンポーネントを実装するために、専用のAzureサブスクリプションが割り当てられ、論理的な分離が確保される。
- 共有サービスにおいては、論理的なアプリケーション構成により、論理的な分離が実現される。
- AudioCodesのデータセンターと顧客拠点間には、以下のデフォルトパラメータに基づくサイト間IPsec VPNトンネルが構成されるものとする。

| PHASE | ATTRIBUTE | Default Values |
|---|---|---|
| **IKE version** | **IKEv2** | |
| **Route/Policy based** | **Route-based** | |
| **Phase 1: ISAKMP - Main Mode** | SA Timeout (seconds) | 86400 |
| | Hash Algorithm | SHA-256 |
| | Encryption Algorithm | AES-256 |
| | Diffie-Hellman (DH) Group | Group 5 |
| **Phase 2: IPSec - Quick Mode** | SA Timeout (seconds) | 28800 |
| | Hash Algorithm | SHA-256 |
| | Encryption Algorithm | AES-256 |
| | PFS DH Group | Group 5 |
| | Encrypted Hosts/Subnets | Should include AudioCodes devices, Service Server. |

## 3.3 Password Manager Pro (PMP)

Password Manager Pro(PMP)は、認証情報、機密情報その他のデジタルアイデンティティを安全に保管・管理するために設計されたセキュアなパスワード管理ツールであり、Fortune 500企業を含む世界中の多数の企業により信頼され、導入されている。Password Manager Proは、企業向けパスワード管理を自動化する機能を有する。

AudioCodes Servicesは、Password Manager Proを使用して、SBC、OVOC、UMP等のソリューションコンポーネントに関するローカルユーザー認証情報など、共有される機密情報の保管および管理を行っている。

詳細は右記を参照 - ManageEngine - Password Manager Pro

## 3.4 Microsoft Defender for Cloud

Microsoft Defender for Cloudは、クラウドベースのアプリケーションを各種のサイバー脅威および脆弱性から保護するために設計された、クラウドネイティブなアプリケーション保護プラットフォーム（CNAPP）である。

Microsoft 365 Defenderポータルは、クラウドリソース、デバイス、アイデンティティに対する攻撃をセキュリティチームが調査するための支援を行うものであり、クラウド環境において発生する疑わしい事象および悪意のある事象を含む攻撃の概要を提供する。Microsoft 365 Defenderは、クラウドにおけるアラートおよびインシデントを含むすべてのアラートおよびインシデントを相関分析することにより、これを実現する。

AudioCodesは、Azure Services Platformに対するセキュリティ評価および脆弱性スキャンを実施するために、Defender for Cloudを有効化している。
詳細は右記を参照 - Microsoft Defender for Cloud | Microsoft Learn

## 3.5 Cloud WAF - Imperva

Imperva Cloud WAFは、業界を代表するWebアプリケーションセキュリティファイアウォールであり、最も高度なセキュリティ脅威に対して、エンタープライズレベルの保護を提供する。Imperva Cloud WAFは、Impervaが提供する市場をリードするフルスタック型アプリケーションセキュリティソリューションの主要構成要素であり、多層防御（Defense-in-Depth）を新たな次元へと引き上げるものである。

クラウドベースのWAFとして、Live PlatformのWebサイトインターフェースが、あらゆる種類のアプリケーション層に対するハッキング試行から常時保護されることを保証する。WAFの管理は、AudioCodes Servicesのコアエンジニアのみが行うものとする。

クライアント署名は、Impervaにより必要に応じて随時更新される。すべてのクライアント署名および最終更新日は、以下のリンクに記載：

https://docs.imperva.com/bundle/cloud-application-security/page/settings/client-classification.htm

AudioCodes Live Platformにより使用されるすべてのサービスのWebインターフェースおよびREST APIインターフェースは、当該WAFを利用するものとする。
詳細は右記を参照 - Imperva Web Application Firewall (WAF) | App & API Protection

## 3.6 Central Syslog Service

Central Log Serviceは、Azure Data Explorer（ADX）を基盤とする社内ログ管理システムであり、SBC（MP1288、Mediant 500/500L/800/1000/2600/3100/4000/90xx/SW-SBC）から送信されるSyslogおよびCDR/SDR等のログ情報を一元的に保管するものである。これらの情報は、デバッグ、サービス分析および課金目的に使用される。

当該データには、RFC3261に基づき、個人を識別し得る以下の情報が含まれる場合がある：

- 発信者および／または着信者の氏名
- 発信者および／または着信者の電話番号
- 発信者および／または着信者のURI

本サービスは、AudioCodesのエンジニアに対し、以下の機能を備えたCentral Log Serviceを提供する：

- **データの所在:** セントラルトポロジーは、以下の3つのサポート地域に分散された3つの独立したクラスタで構成される：:
  - Americas: West US 2
  - EMEA: West Europe
  - APAC: Southeast Asia
- ソリューションコンポーネントのログ／Syslogメッセージは、Kafkaプロトコル（ポート9093）を使用し、TLSv1.3により保護されたSSL経由でパブリックネットワークを通じて、地域別Azure EventHubへ安全に送信される.
- 顧客拠点にホストされたSBCの場合、Syslogはインターネット経由で、SSLにより保護されたポート9093を使用して、地域別Azure EventHubへ安全に送信される。
- SBCのSyslogへのアクセスは、行レベルセキュリティ（Row Level Security Access：RLS）に基づくロールベースアクセスにより管理される。
- アクセスはAudioCodesサービス組織内の担当者に限定され、Azure MFAにより保護される。
- セントラルログサービスにおける異常動作は検出される。
- データは削除または改ざんできず、自動保持期間は30日間とする。
- SBCがSyslogの送信を停止した場合、自動的にアラートが生成される。

| Personal Data Type | On Transit | At Rest | View |
|---|---|---|---|
| Personal Data Encryption | Yes | Yes | Full details |
| Personal Data pseudonymization | No | No | Full details, View Personal Data pseudonymization can be enable on demand |

**注意事項:** **顧客拠点にホストされているSBCに関しては、以下のFQDNへのインターネットアウトバウンド通信をポート9093で許可する必要があり、通話開始ごとに概算で250Kbpsの帯域幅が必要となる**

**EMEA**: Syslog-EMEA-EH.servicebus.windows.net
**Americas**: Syslog-America-EH.servicebus.windows.net
**APAC**: Syslog-APAC-EH.servicebus.windows.net

また、以下のファイルに記載されたサブネットについて、顧客はアウトバウンド通信を許可する必要がある。
Date source: Download Azure IP Ranges and Service Tags – Public Cloud from Official Microsoft Download Center

## 3.7 Central Debug Recording Service

SBC（セッションボーダーコントローラー）は、デバッグ録音（Debug Recording：DR）パケットをセントラルDRサーバーへ送信することができる。DRが有効化されると、当該機器はすべてのネットワークメッセージを複製し、セントラルDRストレージへ送信する。

DRは、RTP/RTCP、T.38、ISDN、CAS、SIPなど、複数の種類のトラフィックに対して実施可能である。

DRは、内部メッセージや信号の解析が必要な高度なデバッグに有用であり、ハブやポートミラーリングが利用できない環境におけるネットワークトラフィックの記録、または同一機器内の2つのエンドポイント間の内部トラフィックの記録にも有効である。

DRは初期状態では無効化されており、サービス品質の確保を目的としたトラブルシューティングのためにのみ有効化されるものとする（初期設定では1時間後に自動的に無効化される）。RTPストリームの記録は、音声品質に関する問題への対応を目的として顧客からの要請があった場合に限り実施されるものであり、顧客は録音された音声通話に個人情報または機微情報が含まれないよう十分に留意するものとする。

本サービスは、AudioCodesのエンジニアに対し、以下の機能を備えたセントラルDRサービスを　　提供する：

- **データの所在: セントラルトポロジーは、以下の3つのサポート地域に分散された3つの独立したストレージアカウントで構成される：**
  - Americas: Central US
  - EMEA: West Europe
  - APAC: Southeast Asia
- AudioCodesがホストするSBCの場合、DRパケットは、Azureネットワークを通じて、　ポート443によるHTTPSストリーミングを用い、TLSv1.3により保護された状態で地域別Azureストレージアカウントへ安全に送信される。
- 顧客拠点にホストされるSBCの場合：DRは、同様にポート443による HTTPSストリーミングを用い、TLSv1.3により保護された状態で地域別 Azureストレージアカウントへ安全に送信される。
- アクセスはAudioCodesサービス組織内の担当者に限定され、Azure MFAと統合されている。
- DRファイルは、Azureストレージ上に保存された後、3日間で自動的に削除されるものとする。

| Personal Data Type | On Transit | At Rest | View |
|---|---|---|---|
| Personal Data Encryption | Yes | Yes | Full details |
| Personal Data pseudonymization | No | No | Full details |

**注意事項:** Central Debug Recording serviceを利用するにあたり、顧客は以下のFQDNへのアウトバウンド通信をポート443にて許可する必要があり、通話開始ごとに概算で250Kbpsの帯域幅が必要となる。

**EMEA:** emeadrstorageaccount.blob.core.windows.net
**Americas:** amerdrstorageaccount.blob.core.windows.net
**APAC**: apacdrstorageaccount.blob.core.windows.net

また、以下のファイルに記載されたサブネットについて、顧客はアウトバウンド通信を許可する必要がある。

Date source: Download Azure IP Ranges and Service Tags – Public Cloud from Official Microsoft Download Center

上記要件は、以下のSBCに適用されるものとする：Mediant 9000 / 9030 / 9080,　Mediant SBCs (VE, CE, SE)

## 3.8 Central Certificate Service

Central Certificate Serviceは、Azure Key VaultおよびAzure Web Appを基盤とする社内リポジトリシステムであり、SBC、OVOC、UMP、WAF等、証明書の使用を要するソリューションコンポーネントに対して、Liveサービス用の証明書を管理するために設計されたものである。当該サービスは、証明書の運用に関する一連のプロセスを包括的に取り扱う：

- 必要なパラメータを含むCSR（証明書署名要求）の発行
- 公的認証局により証明書が署名された後、PFX形式の証明書スイートを作成し、パスワードにより保護された状態でKey Vaultに保存
- PFXファイル内の証明書（PMPに保存されたパスワードにより保護）については、復旧または運用上の必要が生じた場合に取得可能

Central Certificate Serviceは、いかなる個人情報も保存しないものとする。また、当該サービスへのアクセスはAudioCodesサービス組織内の担当者に限定され、Azure MFAにより保護される。

## 3.9 Metering Server

Metering Serviceは、各種AudioCodesの'reporting entities" (例:SBC) から、消費（利用）情報をAudioCodesのクラウドベースのメータリングアプリケーションへ報告することを可能にするものである。

SBCは、通話時間の消費量および同時セッションの使用状況を、AudioCodesメータリングアプリケーションへ報告する。報告は、Rest APIを用いてHTTPS経由で毎分送信される（当該期間中にセッションが発生していない場合でも報告は行われる）。

メータリングサーバーは、いかなる個人情報も保存せず、報告された情報は以下の目的で使用される：

- 顧客への課金
- 顧客が契約容量を超過しているかの測定
- 顧客が自身の利用状況をポータル上で確認するための提供

Metering Serviceは、AzureのWest Europeリージョンに設置されており、以下のポータルを通じてアクセス可能である。 https://metering1.audiocodes.com

## 3.10 Customer Metering Portal

Customer Metering Serviceは各種AudioCodesの'reporting entities" (例:SBC)からの報告を受け付けるものであり、VoiceAI ConnectおよびLive CXの顧客向けに、顧客ポータルが提供される

当該ポータルは、Liveプロジェクトごとに以下の情報を提供する：

- Oracleから取得する情報：顧客が契約したセッション数／通話時間（分）および契約期間に関する情報
- メータリングアプリケーションから取得する情報：実際に消費された通話時間（分）および同時セッション数に関する報告

顧客メータリングポータルは、通話内容に関する情報を一切保存せず、ログインユーザーに関する以下の個人情報のみを保存する：

- ユーザーの氏名
- ユーザーの電子メールアドレス
- ユーザーの電話番号

## 3.11 AudioCodes Intelligent Monitoring (AIM) System

AIMシステムは、米国AWS（北バージニアリージョン）に設置されており、管理対象機器から発生するアラームおよびイベントを分析・検査し、AudioCodes Managed Servicesがどのように対応すべきかを判断するものである。当該システムは、サービスコンポーネントの実際のパフォーマンスを分析し、運用レポートを発行することにより、サービスコンポーネントをインテリジェントに運用するためにAudioCodesが使用する。

サービスコンポーネントの一部として、顧客は連絡先情報を共有する義務を負うものとし、当該情報は、管理対象機器から発生するアラームやサイト間VPNに関連する問題について、AudioCodes AIMが顧客のヘルプデスクと連絡を取るために使用される。

この目的のため、AIMシステムは以下の情報をデータベースに保存する：

- NOC / ヘルプデスクの電話番号
- NOC / ヘルプデスクの電子メールアドレス

上記情報へのアクセスは、HTTPS（TCPポート443）によるWeb GUIを通じて行われ、AudioCodesマネージドサービス管理者グループのみに許可される。

AIMシステムは、Amazon RDSサービス上のMySQLデータベースエンジン／インスタンスを使用している。また、当該データベースはNOCサービス専用で使用され、管理者ユーザーおよびパスワードにより保護されている。

# 4 Service's Components Connectivity and Security Measures

次のセクションでは、サービスに接続して保護するために講じられる接続及びセキュリティ対策について説明します

## 4.1 Live Platform Portal

Live OVOCは、AudioCodes社が提供するサービス管理のために使用される、マルチテナント型のWebベース音声ネットワーク管理ソリューションであり、音声ネットワーク機器の管理機能と、ユーザー体験の品質監視機能を統合した、直感的な操作が可能な単一のWebアプリケーションとして構成されています。Live OVOCは、TLSポート5001を介したAudioCodes独自のQoEセキュアプロトコルを使用して、SBC（Session Border Controller）から通話関連情報を収集・保存します。収集される通話データには、個人を識別可能な情報が含まれる場合があり、通話件数に応じて最大1年間保存されます。

- 保存される情報は以下のとおりです：
- 発信者名
- 発信者の電話番号
- 発信者のURI
- 着信者名
- 着信者の電話番号
- 着信者のURI
- SIPメッセージの完全なコールフロー

本ソリューションの各構成要素は、SNMPv3プロトコル（SBC）を使用して、Live Platform Portalへアラームおよび／またはイベントを送信します。これにより、各構成要素上で生成されたトラップがセキュアに送信されます。なお、UMPに関してはSNMPv2プロトコルが使用されます。Live Platformにおけるアラームの保持ポリシーは、全テナントを対象として最大1,000万件のアラーム、または保持期間1年間のいずれか早い方に達した時点で、保持を終了するものとします。Live Platform Portalは、その運用の一環として、Azure PostgreSQLおよびCassandra Azureデータベースを使用します。これらのデータベースは、別個の仮想ネットワーク上に構成されており、外部の第三者によって直接アクセスされることはありません。Live Platform Portalは、すべての顧客に対して単一のPostgreSQLデータベースを使用して運用されており、サービスプロバイダー／テナントごとにスキーマ単位でのマルチテナンシー方式が実装されています。この構成は、同一データベース内において顧客間の分離を実現するための有効かつ推奨されるベストプラクティスであり、各顧客のデータの独立性およびセキュリティを確保するものです。各サービスプロバイダー／Live Platform Portalのテナントは、それぞれ固有のデータベーススキーマを使用します。これにより、テナント識別子は当該データベーススキーマそのものとなります。各顧客には自身のスキーマへのアクセス権のみが付与されるため、顧客データの分離が確保されます。Live Platform PortalのPostgreSQLデータベースは、個人データを保存するために使用されます。当該データベースには、非個人情報（トポロジー構成要素、プロファイルテーブル、設定テーブル等）を含むメインスキーマと、各サービスプロバイダーテナントごとに構成された個別スキーマが存在します。個別スキーマには、デバイス情報、ユーザー情報、QoE（Quality of Experience）、通話情報等の個人情報が含まれます。

管理者がデバッグまたは不具合修正の目的でデータベース内容にアクセスする必要がある場合、二重の保護層が適用されます。認証されたアクセスサーバへの接続は、ドメインログインおよびAzure Key Vaultに暗号化された状態で保存された管理者認証情報により保護されます。加えて、OVOCデータベースへのアクセスは、OVOCマシン上のルートユーザーのみに限定されます。

| Personal Data Type | On Transit | At Rest | View |
|---|---|---|---|
| 個人データの暗号化 | 有 | 有 | 詳細表示可能 |
| 個人データ仮名化 | 無 | 無 | オペレータ権限レベルでマスキング |

## 4.2 Mediant Virtual Edition (VE) SBC

Mediant Virtual SBCは、企業およびサービスプロバイダーのVoIPネットワーク間の接続性およびセキュリティを実現するために設計された純粋なソフトウェアソリューションです。

本SBCは、悪意あるVoIP攻撃から企業を保護するための境界防御を提供します。また、音声信号の仲介および正規化を行い、任意のIP-PBXと任意のサービスプロバイダーとの接続を可能にし、サービス品質および管理性を確保します。さらに、SBCは「サバイバビリティ（可用性）」機能を提供し、中央集約型SIPベースのIPセンターサーバーまたは支店における独立したシステム運用により、接続障害時にも企業のサービス継続性を確保します。

SBCは、Live Microsoft Teams、Lync Ev、Zoom Phone Communicationサービス、Broadsoft Hosted PBX（BroadCloud）、および顧客のクラウドまたはオンプレミス環境でのAvayaに利用されます（この場合、SBCのモデルは異なる場合があります）。

音声暗号化に関しては、SBCはVoIPのセキュアプロトコル（SIP over TLS、Secure RTP）を使用するようにデフォルトで設定されており、非セキュアなVoIPプロトコル（TCP/RTP）は、必要な場合に限り使用されます。これらはセキュアプロトコルをサポートまたは実装していないためです。

デフォルト設定に基づき、SBCはSIPプロトコル（RFC3261）に基づいて以下の情報をSyslogサーバへ送信します。これらの情報は個人を識別可能な情報に該当する場合があります：

- 発信者および／または着信者の氏名
- 発信者および／または着信者の電話番号
- 発信者および／または着信者のURI

| 個人データの種類 | 転送中 | 保存時 | 表示 |
|---|---|---|---|
| 個人データの暗号化 | 有 | 有 | 詳細表示可能 |
| 個人データの仮名化 | 任意 | Optional | Full details |

## 4.3 User Management Pack (UMP)

AudioCodesが提供するユーザーマネジメントパック（以下「UMP」という）は、Microsoft 365 Teamsにおけるオンボーディングの自動化を目的としたソフトウェアアプリケーションであり、MACD（移動、追加、変更、削除）操作およびMicrosoft Teams Direct Routingならびにオペレーター接続機能に関するポリシー管理のライフサイクルを簡素化するものとします。

UMPは、Live Platform REST APIを通じて外部に公開されており、開発者がDirect Routingおよびオペレーター接続サービスを自社ソリューションに統合し、管理および設定作業を実行することを可能にします。

UMPは、Live Microsoft Teamsサービスにおいて使用されるものであり、AudioCodesが提供するホスティングプラットフォーム（Azure）上、または顧客のクラウド環境もしくはオンプレミス環境にてホストされるものとします。

UMPは、Microsoft Teamsから取得した顧客データを、テナントごとに専用のSQLデータベースへ同期するものとします。

UMPは、HTTPSプロトコルを介してREST APIを使用し、以下の関連情報を含む形でLive Platform Portalを更新します：

- ユーザー名
- ユーザーの電話番号
- ユーザーのメールアドレス
- その他関連情報

これらの情報は、ライフサイクル管理の目的で使用され、当該ユーザーが退職するか、テナントから削除されるまでの間、サービス期間中保持されるものとします。

| 通信/ポート/プロトコル | 転送中 | 保存時 | 表示 |
|---|---|---|---|
| 個人データの暗号化 | 有 | 有（ディスクレベル） | 詳細表示可能 |
| 個人データの疑似匿名化 | 無 | 無 | 詳細表示可能 |

## 4.4 AudioSecure Cloud

SecureLogix社およびAudioCodes社は提携し、企業およびコンタクトセンター向けに包括的な通話認証および不正検出機能を提供する「AudioSecure Cloudサービス」（以下「本サービス」という）を提供します。本サービスはLive Platformを基盤として運用され、顧客が本サービスを導入することにより、AudioSecure Cloudに接続されるものとします。なお、顧客の通話動作は受信されますが、デフォルト設定において通話プロファイルは変更されません。

本サービスは、通話の方向（着信または発信）に応じてスコアリングを行う機能を有しており、着信通話においては発信元番号に対するスコアが、発信通話においては宛先番号に対するスコアがそれぞれ取得されます。

本サービスの一部として、AudioCodes製SBC（Session Border Controller）が使用され、VoIP通信においてはSIP over TLSおよびSecure RTP等の安全なプロトコルのみが使用されるように構成されています。安全性の確保のため、その他の非セキュアなVoIPプロトコルは使用されません。

SecureLogix社のデータセンターとの接続には、REST APIが使用されます。

管理アクセス権限は、AudioCodesサービス組織内の認定担当者に限定されており、第三者によるアクセスは許可されません。

なお、デバッグ目的に限り、SBCからSyslogサーバーへ送信される情報には以下の内容が含まれる場合があります（SIPプロトコル（RFC3261）に基づく）：

- 発信者および／または着信者の氏名
- 発信者および／または着信者の電話番号
- 発信者および／または着信者のURI

| 個人データの種類 | 転送中 | 保存時 | 表示 |
|---|---|---|---|
| 個人データの暗号化 | 有 | 有 | 詳細表示可能 |
| 個人データの仮名化 | 任意 | 任意 | 詳細表示可能 |

## 4.5 Voca as Service

Voca as Service（以下「本サービス」という）は、企業とのインタラクションを円滑にする次世代のサービス体験を提供する、クラウドベースのコンタクトセンターサービスである。本サービスは、従業員、エージェントおよび内部ユーザーがサービスワークフロー内で相互に連携するために、先進的な行動ルーティング技術および会話型AI技術を活用するものとする。本サービスのWebインターフェースは、Web Application Firewall（WAF）により保護されており、Web GUIへのアクセスはLive Platform Portalを経由して行われ、直接のアクセスは許可されないものとする。本サービスの一部として、AudioCodes製SBC（Session Border Controller）が使用され、VoIP通信においては、SIP over TLSおよびSecure RTP等の安全なプロトコルを使用するようデフォルトで構成されている。非セキュアなVoIPプロトコル（TCP/RTP）は許可されず、ファイアウォールおよびIPS（侵入防止システム）も安全なプロトコルのみをサポートする。管理用サポートプロトコルとしては、HTTPS、SSHおよびSNMPv3が使用され、アクセス権限はAudioCodesサービス組織内の特定の職員に限定されるものとする。

デバッグ目的に限り、SBCはSyslogサーバーに対して以下の情報を送信する（SIPプロトコルRFC3261に基づく）。これらの情報は、個人を識別可能な情報に該当する場合がある：

- 発信者または着信者の氏名
- 発信者または着信者の電話番号
- 発信者または着信者のURI

本サービスは、上記情報を一時的に保存し、保存日から起算して21日後に自動的に削除されるものとする。

ユーザー情報の取扱いについて

本サービスは、Azure Entraを介してHTTPS経由で顧客のAzure Entra環境と接続し、Graph APIを利用して組織の連絡先情報と統合することが可能である。取得される情報には、サービス内容および顧客のニーズに応じた活動情報が含まれる場合があり、組織連絡先データには以下の情報が含まれることがある：

- 氏名
- 役職
- 電話番号
- 携帯電話番号
- メールアドレス
- 所属部門

通話情報の取扱いについて

通話情報は、一定期間VocaのMySQLサーバーに保存され、当該期間の経過後、自動的に削除されるものとします。削除後であっても、当該データはVoca顧客テナントの管理者により復元可能な状態に保持されます

保存される通話情報には、以下の項目が含まれます：

- 通話番号
- 通話日時

これらの情報は、サービス提供期間中保持され、サービスの終了または顧客テナントから当該ユーザーが削除されるまでの間、保持されるものとします。

インポートされた個人ユーザー情報を消去するためには、Vocaカスタマーテナントの管理者がActive Directoryとの接続を終了し、Voca Web Managementインターフェース上にて、すべてのユーザーおよびその個人データを手動で削除することが可能です。

| 個人データの種類 | 転送中 | 保存中 | 表示 |
|---|---|---|---|
| 個人データの暗号化 | 有 | 有 | 詳細表示可能 |

]

## 4.6 Device Manager

Live Device Manager（以下「本モジュール」といいます）は、Live Platformのユーザーインターフェースを通じてアクセス可能なデバイス管理用アプリケーションモジュールであり、Microsoft Azureより直接提供されるSaaS（Software as a Service）として構成されております。

本モジュールは、企業IPネットワーク内において中断のない高品質な電話および会議体験を保証することを目的として、広範な種類のデバイスに対応した管理機能を提供いたします。

Device Managerは、Live Platform PortalのPostgreSQLデータベースを利用しており、当該データベースには以下の情報が含まれております：

Device Managerは、Live Platform PortalのPostgreSQLデータベースを利用しており、当該データベースには、非個人情報（トポロジー構成要素、プロファイルテーブル、設定テーブル等）を含むメインスキーマと、各サービスプロバイダーテナントごとに構成された個別スキーマが存在します。個別スキーマには、デバイス（IP電話機器）、ユーザー、QoE（Quality of Experience）、通話情報等の個人情報が含まれております。

保存される個人情報には、以下の項目が含まれる場合があります

- ユーザー名
- ユーザーの電話番号
- ユーザーのメールアドレス
- その他関連情報

これらの情報は、ライフサイクル管理の目的で使用され、当該顧客が退職するか、顧客テナントから削除されるまでの間、サービス提供期間中保持されるものとします。

| 個人データの種類 | 転送中 | 保存中 | 表示 |
|---|---|---|---|
| 個人データの暗号化 | 有 | 有 | 詳細表示可能 |
| 個人データの仮名化 | 無 | 無 | 詳細表示可能 |

以下の表は、Teamsアクセス要件の一環として、デバイスがパブリックインターネットへアクセスするために必要なファイアウォール設定を示すものです：

| 通信/ポート/プロトコル | AudioCodes Device Manager-> デバイス (IP Phone) | デバイス (IP Phone) -> AudioCodes Device Manager (クラウド) |
|---|---|---|
| TCP 443 (HTTPS) | | X |

## 4.7 Meeting Insights Service Information

AudioCodes Meeting Insights（以下「本サービス」といいます）は、ユーザーが会議において生成されたコンテンツ（音声および画面共有）を記録し、Microsoft Teams会議の議事録を自動生成す可能とする、AIを活用したエンタープライズ向けソリューションです。本サービスは、会議、ウェビナー、電話会議等のあらゆる側面を記録・書き起こし・整理する機能を有しており、組織全体で容易に共有可能な企業プラットフォームを提供することにより、情報へのアクセスおよびコンテンツ管理の効率化を図るものであります。本サービスは単一機能としてではなく、複数の機能を統合した形で提供されます。

- Meeting Insights Application layer
  - **Virtual Assistant/Teams Bot**

    バーチャルアシスタントが会議に参加し、コンテンツの記録、メモの作成、アクションアイテムの抽出等を行います。
  - **Business logic**

    ビジネスロジックコンテンツの処理、記録およびユーザーインターフェースの提供を行います。
- Meeting Insights Data layer
  - **Media Storage Space**

    顧客ごとにAzure Blob Storageが使用され、当該ストレージはAzureサブスクリプションとして別途購入いただく必要がございます。アクセスは制限されており、顧客の承認を受けた者およびAudioCodesサービス管理者のみが利用可能です。
  - **Data Storage**

    MongoDBとじはユーザー情報（録音メタデータ等）を保存するために使用されるサービスであり、物理的または論理的に分離された環境にて運用されます。

### 4.7.1 Meeting Insights' Metadata

Meeting Insightsは、以下の情報を管理・収集・保存いたします

- **Meeting recording:**Meeting Insightsは、Microsoft Teamsから取得した音声、画面共有等の会議関連情報およびメタデータを記録いたします。これらには以下の情報が含まれます：
  - 会議主催者のユーザー プリンシパル名（UPN）、ログインIDおよび氏名
  - 会議参加者のUPN、ログインIDおよび氏名
  - 会議録画の閲覧者のUPN、ログインIDおよび氏名
  - 外部参加者の氏名または電話番号
  - 会議メディア（音声、コンテンツ共有、画像等）
  - 会議の要約情報（サマリー、メモ、決定事項、アクションアイテム等）
- **User information:** Meeting Insightsは、Microsoft Azure Entraと連携することにより、ユーザー情報へアクセスし、当該情報をMeeting Insightsのデータベースに保存いたします。これらの情報は、会議データと実際のユーザー名との関連付けおよびユーザー認証の目的で使用されます。保存されるユーザーの個人情報には、以下の情報が含まれる場合があり、これらは個人を識別可能な情報に該当する可能性があります：

- 氏名（姓・名）
- アカウントUPN
- 電子メールアドレス
- 音声認証情報（ボイスプリント）ー本システムは、利用者の音声をデジタル形式で生成し、当該情報は暗号化された上で、ユーザー名とは分離して保存されます。

- **ログ情報：**Meeting Insightsのログメッセージは、Meeting Insightsサーバー上に保存され、CDR（通話詳細記録）や会議参加者のユーザー名、電子メールアドレス等の個人情報を含む場合があります。

  Meeting Insightsをサービスとして提供するAzureホスティングリソースを管理するAudioCodesのサポートエンジニアは、これらの情報にアクセス可能です。
- **AI技術の利用：**Meeting Insightsは、音声認識（Speech to Text）、話者識別（Speaker Identification）、生成AI（Generative AI）等のAI技術を活用し、生産性の向上、会議体験の改善、協働の促進を図ります。これにより、会議の要約、アクション項目の一覧、会議の構成などのAIインサイトが自動生成されます。Meeting InsightsのAI処理には、音声のテキスト化、文字起こし、文字起こし内容の分析が含まれます。本サービスは、Microsoft Azure Cognitive Services、Speech、Azure OpenAI Services（OpenAIとは異なるサービス）、またはAmazon Bedrock Anthropicモデルを利用しています。Microsoft Azure OpenAI Serviceには、濫用監視およびコンテンツフィルタリング機能が統合されており、AWS Bedrockには自動濫用検出機能が実装されています。お客様のデータは、他の顧客やAzure OpenAI、Anthropicには提供されず、Azure OpenAIモデル、Anthropicモデル、AudioCodesモデルの改善、またはMicrosoftその他第三者製品・サービスの改善には使用されません。
-

### 4.7.2 View Information via GUI

上記の情報には個人情報が含まれており、顧客はロールベースのユーザーアクセス制御に従って当該情報にアクセスすることができます。

| 個人データの種類 | 転送時の保護 | 保存時の保護 | View via GUI |
|---|---|---|---|
| 個人データの暗号化 | 実施済み | 実施済み（AES-256アルゴリズム） | See above |
| 個人データー仮名化 | 未実施 | 未実施 | See above |

### 4.7.3 Meeting Insights' Meetings Recording Files

Meeting Insightsサーバーは、会議の録音ファイルをAzureストレージアカウント（例：顧客ごとのBlobストレージ）に保存します。デフォルトでは、Azureストレージアカウント上のファイルは保存時に暗号化されます（Azureレベルでの暗号化）。録音された会議ファイルは顧客がアクセス可能であり、会議におけるユーザーの役割または管理者の役割に応じて個人情報を含む場合があります。管理者の役割はユーザーインターフェース（UI）を通じて設定可能であり、管理者はすべての会議録音にアクセスする権限を有します。顧客データへのアクセスは制限されており、顧客の承認およびAudioCodesサービス管理部門の承認がある場合に限り、アクセスが許可されます。

| 個人データの種類 | 転送中の暗号化 | 保存時の暗号化 |
|---|---|---|
| 個人データの暗号化 | 有 | 有 |

| 個人データの種類 | 転送中の状態 | 保存時の状態 |
|---|---|---|
| 個人データの仮名 | No | No |

### 4.7.4 Meeting Insights Teams Bot

Meeting Insights Teams Botは、顧客のTeamsサブスクリプションに接続し、録音対象ユーザーの会議に参加することにより、Teams®コミュニケーションの録音を可能にする機能です。Meeting Insights Teams Botは、Microsoft Media Communication SDKおよびGraph APIを通じて会議データおよびメディアを受信し、その後、メタデータをMeeting Insightsアプリケーションにアップロードします。会議終了後、録音されたメディアは顧客のAzureストレージにアップロードされます。録音中およびアプリケーションまたはストレージへの転送が完了するまでの間、メタデータおよび録音ファイルは一時的にMeeting Insights Teams Bot上に保存されます。当該Botのディスクは暗号化されています。

| 個人データの種類 | 転送中の暗号化 | 保存時の暗号化 |
|---|---|---|
| 個人データの暗号化 | 有 | 有 |
| 個人データの仮名化（疑似匿名化） | 無 | 無 |

## 4.8 Interaction Insights Service Information

AudioCodes Live Interaction Insightsは、Microsoft Teams向けのエンタープライズグレードの録音サービスであり、企業が顧客との通話または社内通話を記録・インデックス化することを可能にし、コンプライアンス遵守、品質管理等の目的に利用されます。本サービスは高可用性を有し、あらゆる規模の企業に適した設計となっております。検索、再生、ダウンロード等の操作が容易であり、ユーザーは通話の種類や日付範囲に基づいて録音された通話を記録・再生・取得することが可能です。
Interaction Insightsサービスは、以下の論理層により構成されます：

- Interaction Insightsアプリケーション層
  - **Teamsコンプライアンス録音Bot**

    Microsoft社により対象ユーザーの通話録音のために呼び出され、通話を録音します。
  - **業務ロジック**

    本アプリケーションは、処理、録音、ユーザーインターフェースの提供等、業務ロジックを担います。
- Interaction Insightsデータ層
  - **メディア保存領域**

    顧客ごとのAzure Blob Storageが、通話音声等の録音メディアの保存に使用されます。これは別のAzureサブスクリプション上に配置されており、顧客データへのアクセスは制限されており、顧客の承認およびAudioCodesサービス管理部門の承認がある場合に限り、アクセスが許可されます。
  - **データ保存領域**

    MongoDBサービスが、ユーザー情報、録音メタデータ等のデータ保存に使用されます。すべての顧客固有のデータは、物理的または論理的に分離されています。
- Office 365テナント：顧客のOffice 365テナントがTeamsを提供し、Interaction Insights BotはTeamsユーザーの通話時に参加し、音声を録音します。

### 4.8.1 Interaction Insights' Metadata

Interaction InsightsはMongoDBサービスを通じて以下の情報を収集・管理・保存します：

- **通話録音情報**：Interaction Insightsは、通話に関連する情報を記録・保存します。通話メタデータには、以下の情報が含まれます
  - 発信者氏名
  - 発信者電話番号
  - 発信者URI
  - 着信者氏名
  - 着信者電話番号
  - 着信者URI
  - 通話ID
  - 着信先氏名

- 応答側当事者のURI
- 転送元当事者の氏名
- 転送先当事者の氏名

■ **ユーザー情報**：Interaction Insightsは、Azure Entraと連携するように構成することが可能であり、ユーザー情報をInteraction Insightsデータベースに取得することができます。これらの情報は、通話データと実際のユーザー名との関連付けに使用されます。取得されるユーザーの個人情報には、以下が含まれます：

- 氏名（名・姓）
- エイリアス（別名）
- 電子メールアドレス
- 組織により定義された追加項目（例：電話番号、Microsoft SIP URI、Tel URI等、録音対象ユーザーの識別に使用される情報）

■ **ログ情報**：Interaction Insightsのログメッセージは、Interaction Insightsサーバーおよび Azure Application Insightsに保存されます。これらのログには、会議参加者のユーザー名や電子メールアドレス等、CDR（通話詳細記録）に関する個人情報が含まれる場合があります。Interaction Insights as a Serviceの一環としてAzureホスティングリソースを管理するAudioCodesのサービス担当者は、これらの情報にアクセスする権限を有します。

### 4.8.2 View Information via GUI

前項に記載された情報には個人情報が含まれており、顧客はロールベースのユーザーアクセス制御に従って当該情報にアクセスすることができます。

| 個人データの種類 | 転送中の暗号化 | 保存時の暗号化（AES-256） | GUI表示によるアクセス |
|---|---|---|---|
| 個人データの暗号化 | 有 | 有 (AES-256 algorithm) | 上記参照 |
| 個人データの仮名化 | 無 | 無 | 上記参照 |

### 4.8.3 Interaction Insights Call Recording Files

Interaction Insightsサーバーは、Azureストレージアカウント（例：Blobストレージ）に通話録音ファイルを保存します。デフォルトでは、Azureレベルにおいて保存時に暗号化が施されます。

録音された通話ファイルには個人情報が含まれており、Interaction Insights Web GUIを通じて、顧客が定義したセキュリティプロファイルに基づきアクセスが可能です。AudioCodesのサービス担当者は、Interaction Insights as a Serviceへのアクセス権限を有します。

顧客の通話録音ファイルへのアクセスは制限されており、顧客の承認およびAudioCodesサービス管理部門の承認がある場合に限り、アクセスが許可されます。

| 個人データの種類 | 転送中の暗号化 | 保存時の暗号化 |
|---|---|---|
| 個人データの暗号化 | 有 | 有 |
| 個人データの仮名化 | 無 | 無 |

### 4.8.4 Interaction Insights Teams Bot

Interaction Insights Teams Botは、顧客のTeamsサブスクリプションに接続し、録音対象として設定されたユーザーの通話に参加することにより、Teams®コミュニケーションの録音を可能にする機能です。当該Botは、Microsoftのコンプライアンス録音機能およびGraph APIを通じて通話データおよびメディアを受信し、メタデータをInteraction Insightsサーバーにアップロードします。通話終了後、録音されたメディアはメディア保存領域（例：Blobストレージ）にアップロードされます。

録音中およびInteraction Insightsデータベースまたは保存領域への転送が完了するまでの間、メタデータおよび録音ファイルは一時的にInteraction Insights Bot上に保存されます。Interaction Insightsまたは保存領域に起因する通信障害が発生した場合、当該データは最大24時間、または通信が復旧するまで保持される可能性があります。

| 個人データの種類 | 転送中の暗号化 | 保存時の暗号化 |
|---|---|---|
| 個人データの暗号化 | 有 | 有 |
| 個人データの仮名化（疑似匿名化） | 無 | 無 |

## 4.9 UCaaS-CCaaS Connect

AudioCodes UCaaS-CCaaS Connectは、Live Platform上においてUC（ユニファイドコミュニケーション）およびCC（コンタクトセンター）サービス（例：Zoom電話システム、Genesys SIP接続等）を管理するために使用される地域別Webアプリケーションです。

UCaaS Connectは、Rest APIを用いてHTTPS経由でUCアプリケーションと通信し、サービスのライフサイクルの設定および管理を行います。

CCaaS Connectは、コンタクトセンターへのトランク接続を作成し、サービスのルーティングおよび機能を管理します。

この目的のため、UCaaS-CCaaS Connectは以下の情報をデータベースに保存しますが、これらは個人情報には該当しません：

- 会社名
- 会社の担当者名
- 会社の担当者の電子メールアドレス
- 会社の担当者の電話番号

## 4.10 Oracle Service Cloud

マネージドサービスの一環として、顧客はAudioCodesのTAC（テクニカル・アシスタンス・センター）との連絡に使用される連絡先情報（マネージドデバイスのアラームやサイト間VPNの問題に関する対応）を共有する必要があります

この目的のため、Oracle Service Cloudは、AIMシステムのデータベースに以下の情報を保存します：

- 組織名／住所
- 連絡先情報（電話番号、電子メールアドレス）
- サービスリクエスト情報：
  - サービスリクエストの件名
  - シリアル番号
  - 顧客とサービスリクエストに割り当てられたTACエンジニアとの間の通信履歴
  - 顧客またはTACエンジニアが提供した添付ファイル
- 添付ファイルは、チケット発行日から1年以内に削除されます。ただし、チケットの記録（ノート）は削除されません。

Oracleは、Oracle Cloud、コンサルティング、アドバンスト・カスタマー・サポート、テクニカル・サポートのすべての顧客に対し、適切なデータ移転保護措置を提供しており、これにはOracleの「プロセッサー向け拘束的企業準則（BCR-P）」または「EU標準契約条項」が含まれます。

# 5 Personal Data Flows

以下の表は、Live Platformサービスにおける内部ソリューションコンポーネント間の個人データの流れを示すものである。

| 個人データの種類 | 送信元 | 送信先 | プロトコル | 備考 |
|---|---|---|---|---|
| RFC3261に準拠した情報（以下は一部抜粋）：<br>■ 管理対象デバイスのIPアドレス<br>■ 通信事業者SIPトランクのIPアドレス<br>■ 第三者SIPサーバーのIPアドレス<br>■ 発信者氏名<br>■ 発信者電話番号<br>■ 発信者URI<br>■ 着信者氏名<br>■ 着信者電話番号<br>■ 着信者URI<br>■ 通話／セッション詳細記録（CDR／SDR）情報<br>■ 音声コーデック情報 | SBC | 中央ログサービス（インターネット経由） | Syslog (SSL 9093) | Syslogは通話ごとに送信・保存される。 |
| AudioCodes独自プロトコルによるデバッグ録音（以下は一部抜粋）：<br>■ 管理対象デバイスのIPアドレス<br>■ 通信事業者SIPトランクのIPアドレス<br>■ 第三者SIPサーバーのIPアドレス<br>■ 発信者氏名<br>■ 発信者電話番号<br>■ 発信者URI<br>■ 着信者氏名<br>■ 着信者電話番号<br>■ 着信者URI<br>■ 通話／セッション詳細記録（CDR／SDR）情報<br>■ 音声コーデック情報<br>■ RTPストリーム | SBC | 中央DRサービス | AudioCodes Debug Recording (UDP 925) | 情報は必要に応じて送信・保存される。 |

| Personal Data | Source | Destination | Protocol | Comments |
|---|---|---|---|---|
| 制御、メディアデータレポート、およびSIP通話フローに関するメッセージは、以下の情報（抜粋）を含み、XMLベースかつTLSにより保護された通信により送信されます：<br>■ 管理対象デバイスのIPアドレス<br>■ 通信事業者SIPトランクのIPアドレス<br>■ 第三者SIPサーバーのIPアドレス<br>■ 発信者氏名<br>■ 発信者電話番号<br>■ 発信者URI<br>■ 着信者氏名<br>■ 着信者電話番号<br>■ 着信者URI<br>■ SIPのCall-ID<br>■ 通話／セッション詳細記録（CDR／SDR）情報<br>■ 音声コーデック情報<br>■ 音声通話品質情報（成功／失敗したストリーム、最大同時ストリーム数、ストリーム品質の利用分布、平均通話時間（ACD）、MOS、パケット損失、ジッター、遅延、エコー等） | SBC | Live Platform Portal | AudioCodes QoE (TLS 5001) | 通話ごとに送信・保存される |
| Teamsから収集されたユーザー情報：<br>■ ユーザー名<br>■ ・ユーザー電話番号<br>■ ・ユーザー電子メールアドレス | UMP | Live Platform Portal | HTTPS | |
| アラーム／イベント情報：<br>■ 管理対象デバイスのIPアドレス<br>■ 通信事業者SIPトランクのIPアドレス<br>■ 第三者SIPサーバーのIPアドレス<br>■ アラーム／イベント情報 | SBC<br>UMP | Live Platform Portal | SNMP (UDP 162) | 当該情報は、各イベントごとに送信および保存されます。 |
| アラーム／イベント情報：<br>■ 管理対象デバイスのIPアドレス<br>■ 通信事業者SIPトランクのIPアドレス<br>■ 第三者SIPサーバーのIPアドレス<br>■ アラーム／イベント情報 | OVOC | AIM System | SNMP (UDP 162) | 当該情報は、各イベントごとに送信され、保存されます。 |
| アラーム／イベント情報：<br>■ 管理対象デバイスのIPアドレス<br>■ 通信事業者SIPトランクのIPアドレス<br>■ 第三者SIPサーバーのIPアドレス<br>■ アラーム／イベント情報 | AIM System | Oracle Service Cloud | Rest API HTTPS (443) | 当該情報は、各イベントごとに送信されます。 |
| アラーム／イベント情報：<br>■ 管理対象デバイスのIPアドレス<br>■ 通信事業者SIPトランクのIPアドレス<br>■ 第三者SIPサーバーのIPアドレス<br>■ アラーム／イベント情報 | AIM System<br>Oracle Service Cloud | Customer's Helpdesk | SMTP (TCP 25) | 当該情報は、各イベントごとに送信されます。 |

以下の表は、Live Platformサービスにおけるオンプレミスの SBC（セッションボーダーコントローラー）とローカルサービスサーバー間における個人データの流れを示すものである。

| 個人データの種類 | 送信元 | 送信先 | プロトコル | 備考 |
|---|---|---|---|---|
| RFC3261に準拠した情報：<br>Managed Device IP Address<br>■ 管理対象デバイスのIPアドレス<br>■ 通信事業者SIPトランクのIPアドレス<br>■ 第三者SIPサーバーのIPアドレス<br>■ 発信者氏名<br>■ 発信者電話番号<br>■ 発信者URI<br>■ 着信者氏名<br>■ 着信者電話番号<br>■ 着信者URI<br>■ 通話／セッション詳細記録（CDR／SDR）情報<br>■ 音声コーデック情報 | SBC | On Prem Service Server | Syslog (TLS 514)<br>CDR (UDP 514) | Syslogは、各通話ごとに送信および保存されます。<br>CDRは、必要に応じて送信および保存されます。 |
| AudioCodes独自プロトコルによるデバッグ録音：<br>■ 管理対象デバイスのIPアドレス<br>■ 通信事業者SIPトランクのIPアドレス<br>■ 第三者SIPサーバーのIPアドレス<br>■ 発信者氏名<br>■ 発信者電話番号<br>■ 発信者URI<br>■ 着信者氏名<br>■ 着信者電話番号<br>■ 着信者URI<br>■ 通話／セッション詳細記録（CDR／SDR）情報<br>■ 音声コーデック情報 | SBC | On Prem Service Server | AudioCodes Debug Recording (UDP 925) | 当該情報は、必要に応じて送信および保存されます。 |

# 6 Backup and Restore

以下の表は、各種データのバックアップ方法について記載したものである。

| 対象 | 頻度および方法 | 保存先 |
|---|---|---|
| 中央データセンター構成要素 | バックアップを毎日実施 | ドメインコントローラー、AIM、PMPサービスは、インストールされたクラウドサイトおよびリモートクラウドサイトにおいて、14日間保持の暗号化されたバックアップが毎日実施される。 |
| 地域データセンター構成要素 | バックアップを毎日実施 | Live Platformポータル（AKS）－PostgreSQLデータベースは、7日間保持の地理的冗長バックアップを毎日実施。Cassandraデータベースは、2日間保持のバックアップを毎日実施。UMP（仮想マシン）－Azureバックアップを毎日実施。毎日のバックアップは14日間保持。即時リカバリスナップショットは2日間保持。Meeting Insights－MongoDBは4時間ごとにスナップショット取得、14日間保持。Interaction Insights－MongoDBは4時間ごとにスナップショット取得、14日間保持。 |
| SBC | 構成パッケージ、OVOCのバックアップマネージャー | OVOCは、SBCの構成ファイル（ini、conf、cliスクリプトファイル）を自動的に（毎日）バックアップするよう設定されている。バックアップファイルはBackup Managerにより管理され、各管理対象デバイスにつき最新の5件のバックアップファイルが保存される。 |

各構成要素のリストア（復元）作業は、当該サービスにおける内部手続に従って実施されるものとします。

# 7 On Premises Hosting (Optional)

## 7.1 Service Server

サービスサーバーは、顧客施設内に設置されるMicrosoft Windows Serverであり、ローカルリポジトリとして機能します。当該サーバーは、AudioCodesのサービス担当者による障害切り分けおよび詳細レポートの分析支援のため、Syslogファイルを24時間365日収集します。

サービスサーバーに搭載されるアプリケーション（NIXLog Syslog Service、Wireshark、AC INI editor、AC Syslog Viewer、WinSCP、Windows IIS Service、Notepad++等）は、AudioCodesにより提供されます。顧客は、AudioCodesに対して、パスワードの有効期限が無期限の管理者権限を付与する必要があります。なお、当該サーバーは顧客のドメインに属さないスタンドアロン構成とすることが推奨されます。

### 7.1.1 Syslog Information

管理対象デバイスは、TLSポート514を介してSyslogメッセージをサービスサーバー（顧客施設内）に送信し、当該メッセージは「クリアテキスト」形式のtxtファイルとして30日間保存されます。Syslogには、RFC3261に基づき、個人を識別可能な通話関連情報が含まれる場合があります：

- 発信者および／または着信者の氏名
- 発信者および／または着信者の電話番号
- 発信者および／または着信者のURI

| 通信/ポート/プロトコル | 転送中 | 保存時 | 表示 |
|---|---|---|---|
| 個人データの暗号化 | 有 | 有（顧客がオンプレミスサービスサーバー上でBitLocker等により実装・維持する責任を負う） | 全詳細表示可能 |
| 個人データの仮名化 | 無 | 無 | 全詳細表示可能 |

### 7.1.2 Debug Recording Information

管理対象機器は、顧客拠点内に設置されたサービスサーバーに対して、デバッグ録音パケットを送信することができる。

デバッグ録音が有効化された場合、当該機器は自身が送信または受信するすべてのメッセージを複製し、IPアドレスにより定義された外部サーバーへ送信する。

デバッグ録音は、RTP／RTCP、T.38、ISDN、CAS、SIP等、複数の種類のトラフィックに対して実施可能であり、内部メッセージおよび信号の解析が必要とされる高度なデバッグに使用される。

また、ハブやポートミラーリングが利用できない環境においてネットワークトラフィックを記録する場合や、同一機器内の2つのエンドポイント間の内部通信を記録する場合にも有用である。

なお、デバッグ録音は初期状態では無効化されており、サービス品質の確保を目的としたトラブルシューティングに限り、有効化されるものとする。

RTPストリームのキャプチャは、音声品質に関する問題を解決するために顧客からの要請があった場合に限り実施される。顧客は、録音された音声通話に個人情報または機微情報が含まれないよう、適切な管理を行う責任を負うものとする。

| 通信／ポート／プロトコル | 転送中 | 保存時 | 表示内容 |
|---|---|---|---|
| 個人データの暗号化 | 無 | 無 | 全詳細表示可能 |
| 個人データの仮名化（疑似匿名化） | 無 | 無 | 全詳細表示可能 |

### 7.1.3 BitLocker Overview

BitLockerドライブ暗号化は、オペレーティングシステムと統合されたデータ保護機能であり、紛失、盗難、または不適切な廃棄処理が行われたコンピュータからのデータの窃取または漏洩を防止することを目的としています。

BitLockerは、Trusted Platform Module（TPM）バージョン1.2以降と併用することで、最高レベルの保護を提供します。TPMは、近年の多くのコンピュータに搭載されているハードウェアコンポーネントであり、BitLockerと連携してユーザーデータを保護し、システムがオフライン中に改ざんされていないことを保証します。

TPMバージョン1.2以降を搭載していないコンピュータでも、BitLockerを使用してWindowsオペレーティングシステムドライブを暗号化することが可能です。ただし、この場合、コンピュータの起動または休止状態からの復帰時にUSB起動キーの挿入が必要となります。Windows 8以降では、TPM非搭載のコンピュータに対して、オペレーティングシステムボリュームを保護するためのパスワードを使用することが可能です。これらの方法は、TPMと併用したBitLockerが提供する起動前のシステム整合性検証機能を提供しません。

TPMに加えて、BitLockerは、ユーザーが個人識別番号（PIN）を入力するか、起動キーを含むUSBフラッシュドライブ等のリムーバブルデバイスを挿入するまで、通常の起動プロセスをロックするオプションを提供します。これらの追加的なセキュリティ手段は、多要素認証を提供し、正しいPINまたは起動キーが提供されるまでコンピュータが起動または休止状態から復帰しないことを保証します。

以下のリンクは、顧客のIT担当者向けに、Windows Server 2012以降におけるBitLockerの導入方法を説明するものです。BitLockerの実装および維持管理は、顧客の責任となります：

https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-how-to-deploy-on-windows-server

すべてのWindows Serverエディションにおいて、BitLockerはServer ManagerまたはWindows PowerShellのコマンドレットを使用してインストール可能です。BitLockerのインストールには、管理者権限が必要です。

## 7.2 Firewall Requirements

以下の表は、AudioCodes社のデータセンターと顧客のクラウドまたはオンプレミス環境との間に構築されるIPSecサイト間VPNにおいて必要とされる接続マトリックス（プロトコル、ポート、通信方向）を示すものです。これらのファイアウォール設定は、AudioCodes社が顧客側にホストされるソリューション構成要素を管理するために必要なものです。

| 通信種別/ポート/プロトコル | AudioCodes DC -> SBC | SBC-> AudioCodes DC |
|---|---|---|
| TLS 5001 (Secure QoE) | | X |
| TCP 22 (SSH) | X | |
| UDP 161 (SNMPv3) | X | |
| UDP 162 (SNMPv3) | | X |
| TCP 443 (HTTPS) | X | |
| NTP 123 (UDP) | | X |
| TCP 636 (LDAPs) | | X |

| 通信種別/ポート/プロトコル | AudioCodes DC -> UMP | UMP-> AudioCodes |
|---|---|---|
| TCP 80 (http) | X | X |
| TCP 3389 (RDP) | X | |
| UDP 161 (SNMPv2) | X | |
| UDP 162 (SNMPv2) | | X |
| UDP 1161 (KeepAlive) | | X |
| TCP 443 (HTTPS) | X | |
| UMPはプロキシサーバーを介さない「基本的な」直接インターネット接続を必要とする。 | | |

| 通信種別/ポート/プロトコル | AudioCodes DC -> Service Server | Service server-> AudioCodes DC |
|---|---|---|
| TCP 3389 (RDP) | **X** | |
| TCP 636 (LDAPs) - Optional | | **X** |

以下の表は、パブリックインターネットへのアクセスを定義するために必要となります。ファイアウォール設定要件を示すものです。

| 通信種別/ポート/プロトコル | Metering Server (Cloud)-> SBC | SBC-> Metering Server (Cloud) |
|---|---|---|
| TCP 443 (HTTPS) | | X |

Audiocodes社のCentral Syslogサービスを利用する場合、パブリックインターネットへの送信（アウトバウンド）通信を可能とするため、以下のポートを開放する必要があります。

| 通信種別/ポート/プロトコル | Live Platform -> Service Components | Service Components -> Central Syslog service |
|---|---|---|
| TCP 9093 (SSL Kafka) | | X |

WebSocket接続を利用する場合、以下の表は、AudioCodes社のデータセンターと顧客拠点との間において実装すべきプロトコル、ポートおよび通信方向を示す接続マトリックスであります。

WebSocket接続は、SNMP、HTTPS、NTP、QoE等のすべての管理プロトコルをWebSocketトンネル内にカプセル化するものです。

当該接続を開始するためには、機器がインターネット上のパブリックDNSサーバーに対してUDPポート53を使用してクエリを送信できる能力を有している必要があります。

また、以下に示すパブリックIPアドレスからのTCP/HTTPSによるアウトバウンド通信を許可する必要があり、Imperva社のIPアドレスを許可リストに登録し、IP制限ルールを設定することが求められます。

| 通信種別/ポート/プロトコル | Live Platform -> Service Components | Service Components -> Live Platform FQDN |
|---|---|---|
| TCP 443 (HTTPS – WS Tunnel) | | X |

| 通信種別/ポート/プロトコル | Live Platform -> Service Components | Service Components -> Public DNS Server |
|---|---|---|
| UDP 53 (DNS) | | X |

## 7.3 Backup and Restore

以下の表は、各サービス構成要素におけるバックアップ処理の概要を示すものであります。

管理対象機器のリストアは、各サービス構成要素におけるベストプラクティスに従って実施されるものとします。

| 対象機器 | 推奨される頻度及び方法 | 保存期間 | 保管場所 |
|---|---|---|---|
| SBC | Live Platformによるバックアップ | 最新5ファイル | OVOCにより自動（毎日）バックアップされ、構成ファイル（ini、conf、cliスクリプト等）がBackup Managerにより管理され、各管理対象機器につき最新5件のバックアップファイルが保存される。 |
| UMP | 毎日 | 14 days | バックアップおよびリストアは顧客の責任において実施される。 |
| Service Server | 毎日 | 5 Days | バックアップおよびリストアは顧客の責任において実施される。 |

# About AudioCodes

AudioCodes社は、音声という人間のコミュニケーションの根幹に対する揺るぎない使命感を持つ、グローバル企業です。当社は、Voice over IP（VoIP）および統合型VoIP・データネットワーク製品、アプリケーション、ならびにプロフェッショナルサービスの設計、製造、販売を行っており、世界中の大企業、中堅・中小企業、並びに通信事業者に対してソリューションを提供しています。当社の幅広い製品ラインアップには、以下が含まれます。IP電話機, セッションボーダーコントローラー（SBC）, メディアゲートウェイ, モバイルVoIPクライアント, 多機能ビジネスルーター（MSBR）, ルーティングアプリケーション, 通話録音, 音声ダイヤル機能　など

**International Headquarters**
Naimi Park
6 Ofra Haza Street Or Yehuda, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

**AudioCodes Inc.**
80 Kingsbridge Rd
Piscataway, NJ 08854, USA
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: https://www.audiocodes.com/corporate/offices-worldwide
Website: https://www.audiocodes.com