

5Gプライベートセル ラーネットワークはどの ように機能しますか？

3月 2026

概要

産業のデジタル化の加速とIoT（モノのインターネット）接続デバイスの急増は、5Gプライベートセルラーネットワーク（5G PCN）への需要の高まりを直接的に生み出しています。

5G PCNは、信頼性が高く、安全で高性能な無線接続が不可欠な組織や業界にとって、特に有益です。このネットワークにより高度なアプリケーションの利用が可能となり、産業オートメーションの需要拡大にも適応します。

5G PCNは、Wi-Fi®と比較して屋外カバレッジに優れ、より高い容量を備え、従来のモバイルネットワーク（3G/4G）よりも多くのデバイスを処理できます。また、ユーザーは自らのシステムを所有し、特定のワークフローに合わせて設計することが可能になります。5G PCNは大規模な投資を要しますが、有線設備と比較すると、トレンチングの不要化や運用効率の向上によりコスト削減を実現できます。

セルラーネットワークは長年にわたり発展してきており、世代を重ねるごとに、モバイルデバイスの容量および接続性において急速な進化を遂げてきました。

目次

1	はじめに	4
2	5Gプライベートセルラーネットワークのメリット	6
3	5Gプライベートセルラーネットワークのユースケースと用途	7
4	プライベートセルラーネットワークとパブリックセルラーネットワークの違い	8
5	5Gプライベートセルラーネットワークにおけるセキュリティおよびプライバシーに関する考慮事項	9
6	5Gと映像監視	10

1 はじめに

本ホワイトペーパーでは、プライベートセルラーネットワークを、独自のコアを有し、特定の場所においてセルラー技術を用いて接続性を提供するネットワークとして定義します。コアネットワークはPCNのインテリジェントな制御中枢として機能し、例えばデータトラフィックの管理、認証、ユーザーセッション、セキュリティ、およびサービス提供を担います。

モバイルネットワーク事業者（MNO）によって運用され、一般向けに提供されるパブリックセルラーネットワークとは異なり、プライベートセルラーネットワークは組織の特定のニーズを満たすために専用に設計されています。認可されたユーザーのみがプライベートセルラーネットワークにアクセスできます。

無線アクセスネットワーク（RAN）は、無線信号を用いてユーザーデバイスを5Gプライベートセルラーネットワークに接続します。

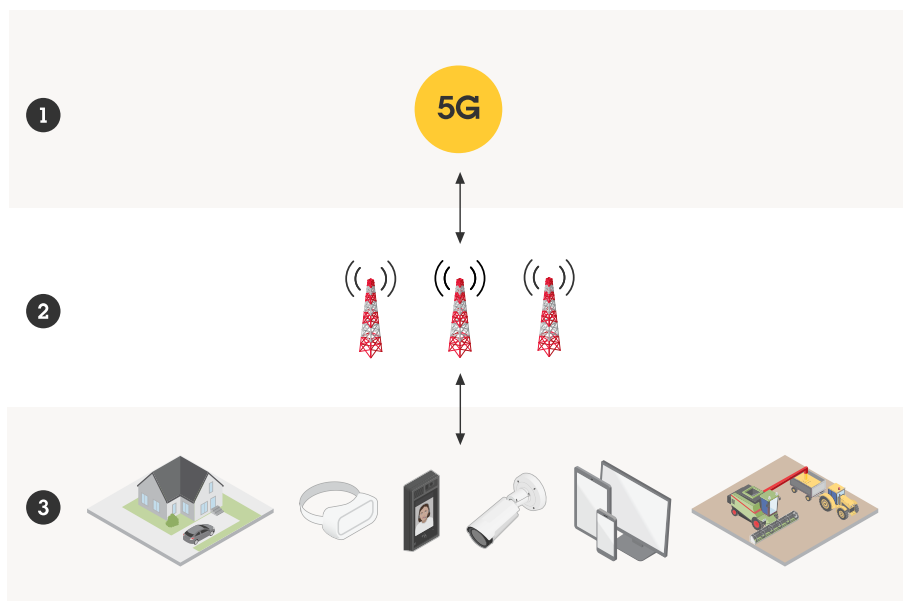


図 1.1 1: 5Gコアネットワーク 2: 無線アクセスネットワーク（RAN） 3: ユーザー機器（UE）

5Gは、従来の世代と比べてより広い周波数帯域をサポートしています。高帯域、中帯域、低帯域の3つの周波数帯に対応しています。

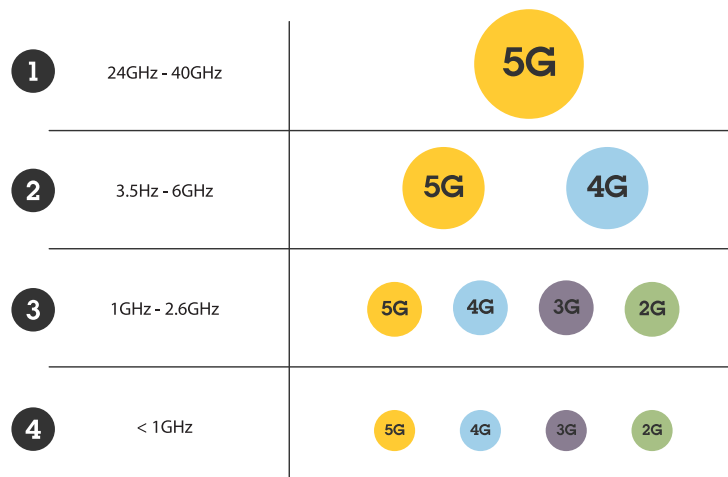


図 1.2 1: 高帯域 2と3：中帯域 4：低帯域

- 高帯域は、約1ミリ秒という超低遅延で超高速通信を実現します。
- ミッドバンドは、モバイルデバイス向けに高速かつ低遅延を提供し、高信頼性と大規模接続を伴う高精細な動画ストリーミング、仮想現実（VR）・拡張現実（AR）、クラウドゲームを可能にします。
- 低周波帯は広範なカバレッジと優れた屋内浸透性を提供します。

これらの5G周波数帯は、サブ6GHz帯およびミリ波（24GHz～40GHz）とも呼ばれ、ネットワークのカバレッジ、容量、速度に影響を与えます。

5Gは第5世代のセルラーネットワーク技術であり、従来世代と比較して、より高速なデータ通信、低遅延、そして大容量を実現するよう設計されています。理論上、最大ダウンロード速度は20Gbps、最大アップロード速度は10Gbpsに達します。実際のユーザーが体感する通信速度はこれより低くなるのが一般的ですが、多くの場合100Mbpsを超えます。これらのピーク速度は主にミリ波帯域によって実現され、4G LTEの約100倍のトラフィック容量をサポートするよう設計されています。このデータレートにより、大容量コンテンツのストリーミング、ダウンロード、アップロードがよりスムーズかつ高速に行えます。

2 5Gプライベートセルラーネットワークのメリット

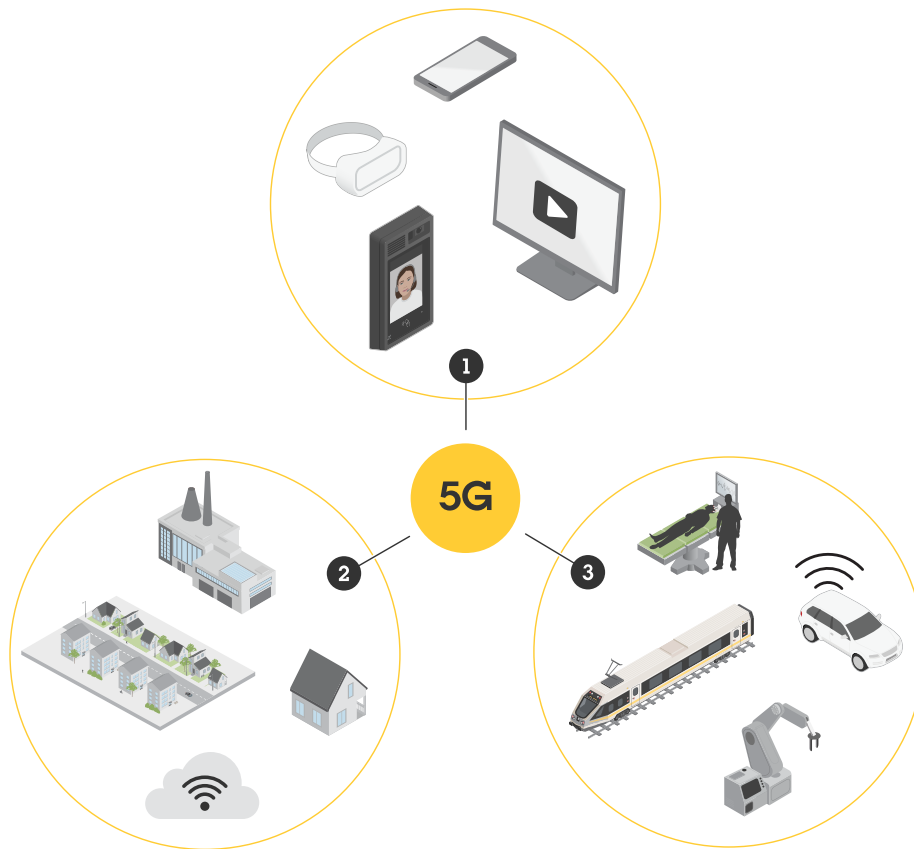


図 2.1 1：パフォーマンスの高いモバイルブロードバンド2：大規模マシンタイプ通信 3：信頼性の高い低遅延通信

1 パフォーマンスの高いモバイルブロードバンド：5Gプライベートセルラーネットワークを利用することで、接続ニーズに応じて、建物や特定のエリア内でネットワーク帯域を割り当て、制御し、分配することができます。ネットワークスライシングを可能にし、物理インフラ内で異なる性能特性を持つ複数の仮想ネットワークを作成できます。これにより、組織は特定のユースケースに合わせてネットワークを最適化することができます。例えば、PCNを運用する空港は、従来のWi-Fiやパブリックネットワークよりも高いセキュリティで、航空会社に対して自社PCNの一部をネットワークスライスとして専用ネットワークとして提供することができます。

5GはWi-Fiに比べて干渉の影響を受けにくく、より高いセキュリティを提供します。また、ネットワークがプライベートであるため、データトラフィックに対するセキュリティと制御性が強化されます。これは、機密情報を取り扱う組織にとって重要です。また、パブリックネットワークから独立して動作するため、一般利用者によるネットワーク混雑や、組織の管理外にあるシステム障害による影響を受けません。

2 大規模マシンタイプ通信 IoTやマシンツーマシン（M2M）通信にも対応しており、これらは現代の産業およびエンタープライズ用途において不可欠です。4Gと比較してより広いカバレッジを提供でき、より多くの接続デバイスをサポート可能です。IoTやM2Mを利用するデバイスの増加は、5Gの必要性が高まっていることを示しています。

3 高信頼・低遅延通信：5Gネットワークは遅延が低く、これはデータパケットが送信元から宛先まで到達するのに要する時間を指します。オンラインゲーム、自動運転車、遠隔手術など、リアルタイム性が求められる用途には、より低遅延のセルラーネットワークが必要です。

プライベート5Gネットワークは大規模な投資を要しますが、コスト削減の可能性もあります。コスト削減は、導入コストの直接的な削減や運用効率の向上で実現されます。例えば、空港においては、PCNは次のような形でコスト削減に寄与します：

- 費用対効果の高い周辺設備の導入：広大なフェンス周辺でのトレンチング（溝掘り）は非常に高コストですが、PCNは電源が確保されていればトレンチングを必要としません。
- より迅速で柔軟な導入：新たな接続インフラストラクチャーを必要とせずにカメラを設置できます。トレンチングやケーブルの敷設は、建物を含む空港のさまざまな部分に望ましくない影響を及ぼす可能性があります。また、これらの有線設備は、環境の美観を損なうことが多く、好ましい外観にはなりません。トレンチング、掘削、ケーブル敷設などの必要な工事作業は、時間を要し、騒音や道路の遮断を引き起こすため、組織の日常業務に支障や妨げを生じる可能性があります。
- PCNは既存インフラストラクチャーを補完します：容量を増やすために既存の有線インフラを新しいものに置き換えるのではなく、PCNはネットワークを補完し、トラフィックをオフロードすることができます。また、新たなデバイスの追加も可能になります。
- 一時的な接続性：PCNはモビリティの利点を有しており、有線ネットワークでは移動する車両の接続管理が困難であるのに対し、柔軟に対応できます。空港の滑走路、顧客向けの展示会、キャンパス内の建設現場、屋内外のイベントなど、一時的に接続が必要となるさまざまな場面で有効です。

3 5Gプライベートセルラーネットワークのユースケースと用途

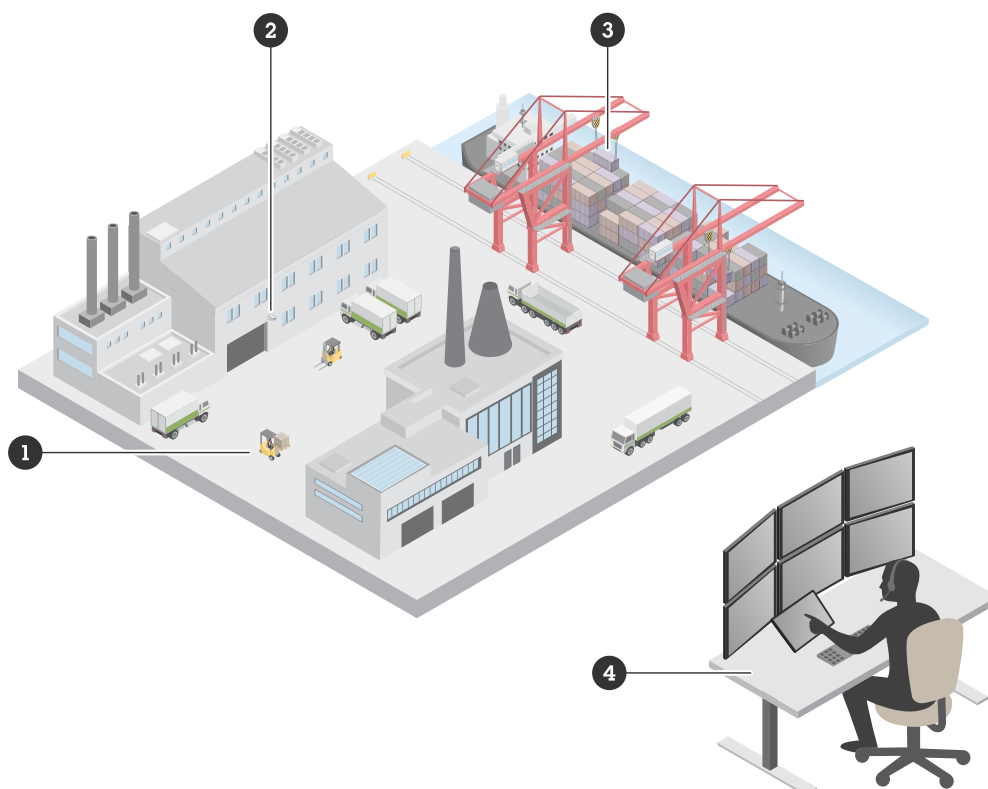


図 3.1 1: リアルタイム作業状況の追跡2: 映像監視3: 機器のテレメトリ4: 監視モニタリングおよび遠隔操作

5Gプライベートセルラーネットワークは、大規模で複雑かつ動的な環境で運用され、安全で信頼性の高いモバイル接続を必要とする組織に最適です。

- 1 **リアルタイム作業状況の追跡:** 5G PCNによりリアルタイムでの追跡が可能になります。例えば、製造業や工場では、資産の正確な位置や状態を把握するために、リアルタイムでの追跡が必要となる場合があります。これを実現するには、5Gが提供する超低遅延かつ高信頼な接続が必要です。病院においても、プライベート5Gは、生命に関わる医療機器の信頼性の高い接続、低遅延の遠隔医療診療、遠隔手術、さらに点滴ポンプや車椅子などの移動機器の追跡に活用でき、大規模な施設内におけるデータセキュリティとネットワーク性能の確保に寄与します。
- 2 **映像監視:** クレーン、トラック、作業員が行き交う港湾のような動的な環境では、屋内外にわたるシームレスな映像監視が求められます。5G PCNは広範なカバレッジとシームレスなハンドオーバーを提供し、資産の追跡、自動運転車の管理、そして円滑な運用の維持を可能にします。
- 3 **機器のテレメトリ:** 機器の保守時期の予測や運用分析、さらには遠隔制御を行うには、当該機器からの継続的なデータ取得が必要です。このようなデータには、スプレッドの位置、荷重、モーター温度などが含まれます。例えば、大型の岸壁クレーンは完全に接続されたデジタルアセットとして機能させることができます。プライベート5G接続は、壊れやすく保守負担の大きい光ファイバーケーブルリールに代わり、重要な情報を無線で電子的に伝送します。同時に、同じ接続を利用してクレーンに設置されたカメラからの映像をストリーミングし、オペレーターにコンテナやその周囲の状況を明確に把握させることができます。
- 4 **監視モニタリングおよび遠隔操作:** 重要なインフラ施設（エネルギー、公益事業、鉱業）や大規模施設（空港、スタジアム）では、施設の監視や機器の遠隔操作が求められることが多くあります。例えば、公共事業会社は自社のグリッドセンサーを監視する必要があります。プライベート5G接続は、拠点の監視と機器の操作の両方に対応でき、重要な運用トラフィックに対して効率的な性能を確保します。

4 プライベートセルラーネットワークとパブリックセルラーネットワークの違い

プライベートセルラーネットワークは特定の組織専用であるのに対し、パブリックセルラーネットワークは一般利用者によって共有・利用されます。いずれもネットワーク接続を提供しますが、両者にはいくつかの違いがあります。以下は、その一例です。

機能	プライベートネットワーク	パブリックネットワーク
所有権	<p>専用のプライベートネットワークは、公衆が運用するモバイルネットワークから分離されています。特定の組織のために専用で運用されます。</p> <p>ネットワーク、デバイス、およびセキュリティポリシーに対する完全な制御を組織に提供できるようになります。</p>	<p>モバイルネットワーク事業者（MNO）によって所有・運用されており、エンドユーザーが持つ制御は限られています。</p>
設定の柔軟性	<p>PCNは、ネットワーク、デバイス、およびセキュリティポリシーに対する完全な制御を組織に提供します。</p>	<p>サブスクリプションでは、特定のネットワーク構成に関して利用できる選択肢が限られています。</p> <p>すべての構成変更は、MNOの管理を通じて行う必要が</p>

	組織は、アップリンクおよびダウンリンクの無線リソースを設定できるほか、QoSレベルの設定、ネットワークスライスの構成、さらには必要に応じたネットワークの拡張を行うことができます。	あります。ただし、MNOのネットワーク上に仮想サブネットワーク（ネットワークスライス）を構築し、プライベートネットワークのように動作させることは可能です。この場合、自社でネットワーク機器を保有する代わりに、MNOのコアおよびネットワークノードを利用します。
コストモデル	ハードウェアの購入および導入、ならびにネットワークの維持には多額の投資が必要です。ただし、これは一度きりの投資であり、それによりデータ通信を無制限に利用できます。	MNOは政府から認可を受けており、特定の規制に従う必要があります。MNOに対してサブスクリプション料金を支払う必要があります。
セキュリティ	セキュリティを直接管理でき、データをオンプレミスに保持できるほか、公共インターネットやMNOのネットワークを安全に経由できるため、高いセキュリティを確保できます。プライベートSIMカードは、設定されている場合、SIM PINによって追加のセキュリティ層を提供します。	データのセキュリティやポリシーを第三者に委ねる必要があります。また、データはMNOが共有するインフラストラクチャーを通じて伝送されます。
アクセスと対象範囲	接続およびアクセスが認可されたデバイスだけに制限され、組織が必要とする場所に展開されるため、低遅延かつ広域なカバレッジを実現します。各デバイスごとに、使用できるデータ量やサービス品質（QoS）を個別に制御できます。	カバレッジが限定されており、ネットワークの混雑が発生する可能性があります。これは、お使いのデバイスが他の多くのデバイスと同様に共有リソースを競合して使用しており、誰がデータをどれだけ使用するかについて、ユーザーが制御できないためです。

まとめると、パブリックネットワークはシンプルなサブスクリプション型モデルであり、十分な性能で問題ない場合に適しています。一方で、性能、セキュリティ、信頼性が組織の運用において極めて重要であり、妥協できない場合にはプライベートネットワークが必要です。

5 5Gプライベートセルラーネットワークにおけるセキュリティおよびプライバシーに関する考慮事項

プライベートセルラーネットワークは、組織に対して安全でプライベートな接続を提供します。また、プライベートセルラーネットワークでは、組織が自らのデータに対する所有権と管理権を有します。

SIMカードによるネットワークアクセスの保護に加え、エンドツーエンド暗号化により、運用データおよび個人データの双方が保護されます。ネットワークへのアクセスは、承認されたユーザー、デバイス、アプリケーション、およびシステムに限定されるべきです。

オンプレミスのコアサーバーや無線装置への物理的アクセスは、制限および管理される必要があります。これは、認可されたアクセス権を持つ者のみがネットワークの物理的なセキュリティ構成要素にアクセスできるようにするためです。

以下に、5Gプライベートセルラーネットワークにおける主なセキュリティリスクを示します：

- **設定ミス**：誤って設定されたネットワークスライスは、共通の制御を迂回する可能性があります。これにより、検知が難しく、悪用されやすいセキュリティ上の脆弱性が生じる可能性があります。
- **サイドチャネル攻撃**：タイミング、電力、メモリ使用量などの間接的な信号から情報が抽出される可能性があります。
- **サービス拒否 (DoS) 攻撃**：攻撃者は、無線アクセスチャネルの妨害、APIの過負荷、またはネットワークスライスへのトラフィックの集中を引き起こす可能性があります。
- **盗聴およびトラフィック分析**：5Gネットワーク内のデータは暗号化されていますが、メタデータは必ずしも暗号化されとは限りません。トラフィックパターンを観測する攻撃者は、ユーザーの行動、位置、またはアプリケーションの種類を推測する可能性があります。
- **中間者 (MITM) 攻撃**：デバイスが5G基地局を装って通信に介入し、機密性および完全性の双方を損なう可能性があります。

6 5Gと映像監視

5GネットワークはIPベースのアーキテクチャを採用していますが、第2層（データリンク層）において大きく異なります。このため、5Gネットワークは有線ネットワークやWi-Fiネットワークとは異なる動作をします。

IPカメラのデフォルトの動作は受動的であり、クライアントからの接続を待機します。VMS (ビデオ管理システム)を通じて、カメラは通常、mDNS (Multicast DNS) やUPnP (Universal Plug and Play) などのプロトコルによって検出されます。これらのプロトコルはデータリンク層に大きく依存しており、5Gネットワークではサポートされていません。Genetec、Milestone、AXIS Camera Stationなどの既存VMSに5G PCN 経由でカメラを接続するには、カメラに既知の固定IPアドレスが設定されている必要があります。VMSからIPアドレス範囲をスキャンすることも可能ですが、その場合でもカメラは既知のIPアドレス範囲内に固定IPアドレスを有している必要があります。

例えば、WebRTCやVPNソリューションを利用することで、クライアントとサーバーが共通の既知のサーバーを介して接続されるため、固定の既知IPアドレスに依存する必要がなくなります。ただし、これはAxisカメラや従来のVMSではネイティブにはサポートされていません。

ミッドバンド（サブ6GHz帯）で動作する5G PCNは最大100MHzの帯域幅をサポートしており、利用可能なビットレートに制限があります。さらに、移動するデバイスでは信号品質が変動する可能性があります。静止しているデバイスであっても、無線環境の変化により信号品質が影響を受け、その結果チャネルで利用可能なビットレートが変動する可能性があります。有線ネットワークと比較すると、5G PCNは利用可能なビットレートがより限定的かつ予測しにくく、そのため混雑の影響を受けやすくなります。

従来の映像ストリームプロファイルは、帯域使用が大きく変動しやすい特性があります。Iフレームは、短時間で伝送する必要のある大量のデータを生成します。帯域幅が不足している場合、バッファの破綻、遅延、フレームドロップ、画質の低下が発生する可能性があります。

有線ネットワークと比較すると、サブ6GHz帯で動作する5G PCNは約10msの追加遅延があります。これはライブビューやパン・チルト・ズーム (PTZ) 制御などの監視用途では問題になりませんが、自動運転車などの用途では重要な要素となります。ネットワークの混雑により、遅延が大幅に増加する可能性があります。

Axis Communicationsについて

Axisは、セキュリティ、安全性、運用効率、ビジネスインテリジェンスを向上させることで、よりスマートでより安全な世界の実現を目指しています。ネットワークテクノロジー企業として、また業界をけん引するリーダーとして、Axisは映像監視、アクセスコントロール、インターコム、音声ソリューションを提供しています。これらのソリューションは、インテリジェントアプリケーションによって強化され、質の高いトレーニングによってサポートされています。

Axisは50ヶ国以上に5,000人を超える熱意にあふれた従業員を擁し、世界中のテクノロジーパートナーやシステムインテグレーションパートナーと連携することで、カスタマーソリューションをお届けしています。Axisは1984年に創業し、本社はスウェーデン・ルンドにあります。