CTONE

Securing Connectivity in O-RAN systems

進化するO-RAN環境の新たなアタックサーフェィスをセキュアに

グローバルにおけるOpen Radio Access Network (O-RAN)市場は、2022 年から2027年の間に11億ドルから156 億ドルへと増加し、70.5%という驚くべきCAGRで急成長すると予測されています。* この成長は、独自もしくはクローズドな無線アクセスネットワークアーキテクチャから、オープンで相互運用可能なシステムへとシフトしたO-RAN アーキテクチャの移行と密接に関係しています。

O-RANはマルチベンダー環境における相互運用性の実現と、無線アクセスネットワークの導入と管理における柔軟性を向上するため、オープン化されたインターフェイス、Software-Defined Networking (SDN)および仮想化の採用を重視しています。O-RANを採用することで、通信事業者やシステム インテグレータはベンダーロックインを回避、イノベーションを促進し、よりオープンで競争力のある通信エコシステムを実現することができます。

* Open Radio Access Network (Open RAN) Market Size, Industry Share Forecast (marketsandmarkets.com)

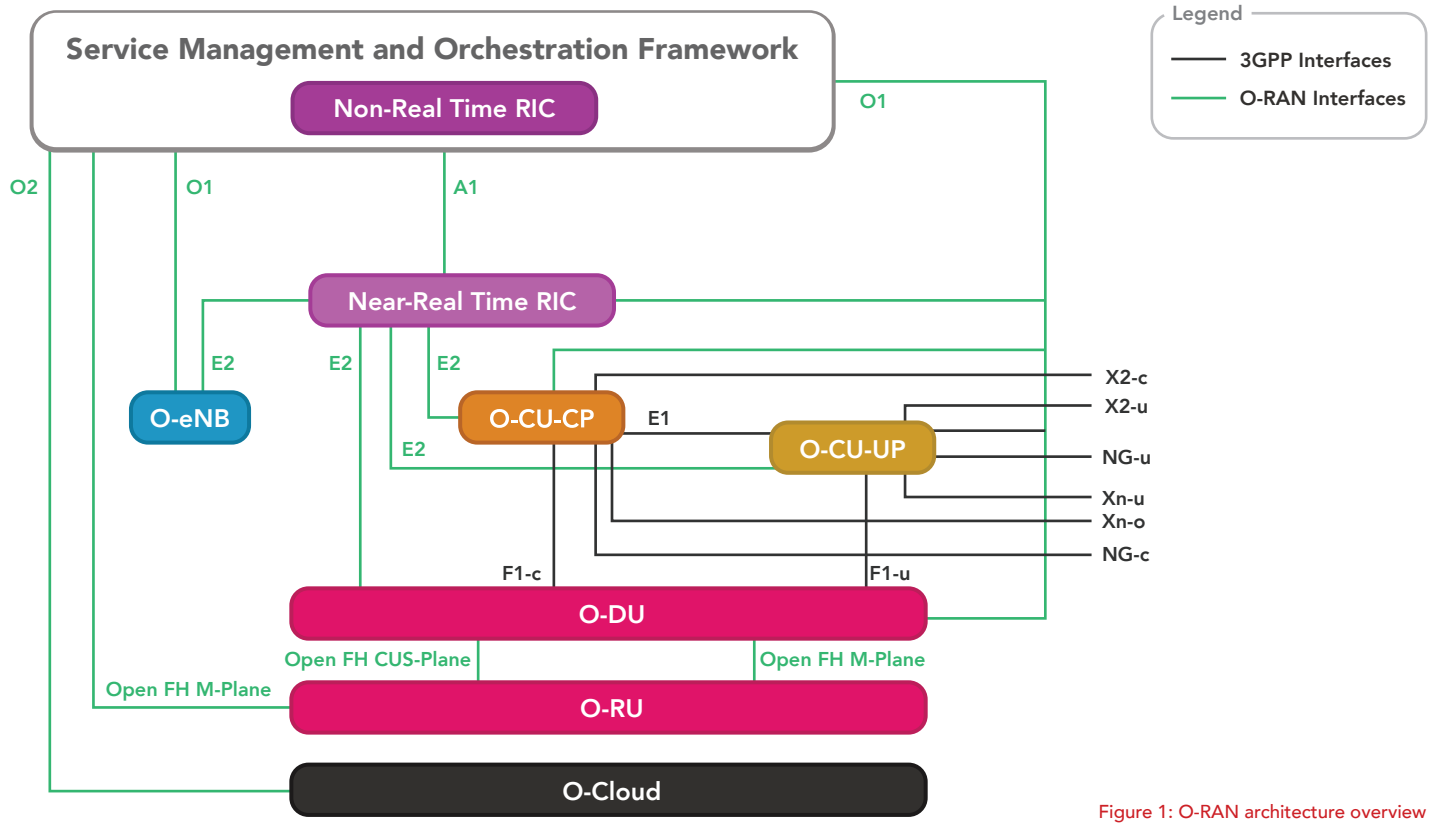


Figure 1: O-RAN architecture overview

O-RANセキュリティとは

O-RANにおけるセキュリティとは、ネットワークインフラ、コンポーネントおよびデータを不正アクセスや悪意のある攻撃、潜在的な脆弱性から保護するための対策と手法を指します。セキュリティ対策は、ネットワークの完全性、機密性、可用性を確保する上で極めて重要な役割を果たすため、O-RANの展開において不可欠な要素といえます。

エンドツーエンドのモバイルネットワークの領域においてO-RANが広く活用されることは、オープンで相互運用可能なシステムの導入が広まることを意味します。しかし、ベンダーがプライベートもしくはパブリックなネットワーク環境を構築する際、このアプローチではある種の脆弱性を生ずる可能性があることを認識することは重要です。結果として新たなアタックサーフェイスが出現する可能性があるため、ネットワークを展開する前に革新的なO-RANセキュリティソリューションの導入を検討すべきと考えます。これらの懸念に積極的に対処することで、企業組織はモバイルネットワークインフラの安全性とレジリエンスを確保することができます。

O-RANにおける新たなアタックサーフェイスの出現

O-RANのセキュリティと完全性を確保するためには、以下の課題に対処することは極めて重要です。

1. **クローズドシステムからオープンシステムへの移行**
   O-RANのアーキテクチャは、攻撃者がO-RANシステムを標的とする潜在的な攻撃ベクトルや経路を拡大し、セキュリティリスクを増大させます。
2. **新しいO-RANインターフェース**
   よりオープンなシステム構成において、A1、E2、O1などのO-RANインターフェースは新たな攻撃対象になり得ます。
3. **サプライチェーンリスク**
   単一ベンダーへの依存からマルチベンダーのサプライチェーンへの移行は、攻撃や侵害のリスクを増大させます。
4. **IT化が進むCT (Communication Technology)環境**
   COTS(Commercial Off-The-Shelf)サーバー上での仮想化技術やオープンソースソフトウェアの普及により、IT技術に起因するセキュリティリスクが高まっています。
5. **オープンソースの活用**
   オープンソースコンポーネントの透過性やアクセシビリティにより、O-RANシステムは未知の状況下で脆弱性にさらされます。

O-RAN環境をセキュアに: CTOne RAN Protection

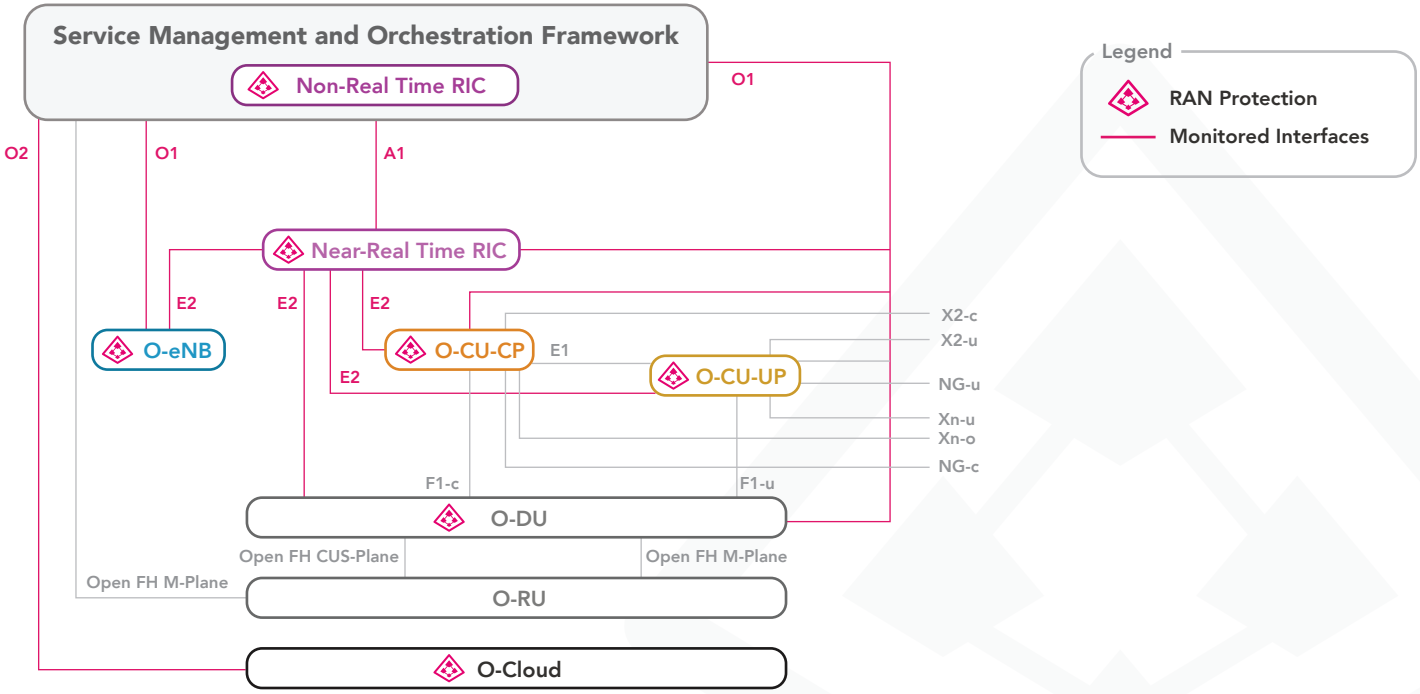
CTOne RAN Protectionは、O-RANシステム向けに特化したITとCTの両領域をカバーするサイバーセキュリティソリューションであり、O-RANシステムの主要な要素を保護するためにO-Cloudプラットフォーム上に展開されます。ホストサーバーとO-RANインターフェースの両方を監視し、O-RANシステムのSBOM(Software Bill of Materials)交換可能データを生成することで、サードパーティのSBOM管理システムとのシームレスな連携を可能にし、セキュリティ規制の遵守を保証します。

O-RANシステムの可視化

SBOMプロファイリングは、透過性、脆弱性管理、コンプライアンス、インシデント対応、情報に基づいた意思決定のために不可欠であり、ソフトウェアセキュリティを強化、リスクを低減、システム全体のレジリエンスを向上させます。
CTOne RAN Protectionは、SBOM交換可能なデータと脆弱性エクスプロイト情報を生成し、O-RANシステムで利用されているソフトウェアの全体像を把握可能にします。可視性を高め、サードパーティのSBOM管理システムとの連携を促進し、セキュリティ規制への準拠を保証します。

リアルタイム保護

CTOne RAN Protectionは、O-RANシステム向けに特化したITとCTの両領域をカバーするサイバーセキュリティソリューションであり、O-RANシステムの主要な要素を保護するためにO-Cloudプラットフォーム上に展開されます。ホストサーバーとO-RANインターフェースの両方を監視し、O-RAN環境をリアルタイム保護するとともに、O-RANシステムのSBOM(Software Bill of Materials)を生成し、O-RANシステムで利用されているソフトウェアの可視化を支援します。



総合的なモバイルネットワークセキュリティによるコネクティビティ強化

CTOneは、完全なプライベート5Gセキュリティソリューションを提供し、IIoTエンドポイントデバイス、O-RANシステム、エッジコンピューティングアプリケーション、コアネットワークなどを含むネットワーク全体を保護します。この迅速に導入可能なソリューションは、多額の投資や管理コストを必要とせずとも包括的なセキュリティ保護を提供できるように設計されています。CTOneはITとCTの間のギャップを埋めることで、ネットワークとエンドポイントの両レイヤーのセキュリティを確保し、4G/LTEおよび5Gネットワークのビジネス利用おいて、企業が直面するセキュリティ脅威の増大に対処します。

“Empowering Secure Connectivity in an Open World”

About CTOne

CTOne は、グローバルにおける通信技術のサイバーセキュリティリーダーであり、次世代ワイヤレスネットワーク向けのセキュリティソリューションを企業へ提供しております。トレンドマイクロの子会社でもあるCTOne は、企業のデジタルトランスフォーメーションを支え、通信技術のレジリエンス強化に貢献いたします。vvv

www.ctone.com