

---

# Securing Enterprise Private Mobile Networks



## CT セキュリティ： サーバーセキュリティ最前線

5Gは、その長所や利点の活用により企業のデジタルトランスフォーメーション(以下、DX)における重要な役割を担います。しかし、CT (Communication Technology:通信技術)は攻撃者にとっては不正侵入や機密データを盗む出すための新たな攻撃手法になり得えます。5Gは他の無線通信技術よりも安全と言われている一方で、ネットワーク機能の仮想化、オープンソースソフトウェア、5G規格のオープン性、および無防備な多数のIoTデバイスによって、5Gは様々な脆弱性やセキュリティ攻撃にさらされることとなります。そのため今後のセキュリティ対策は、従来のITやOTだけでなくCTも網羅し、企業のデジタルインフラのあらゆる側面を総合的に保護する必要があります。

5Gの活用は企業に成長とイノベーションへの道を拓きます。安定性と信頼性の高い5G無線ネットワークにより、例えば企業は多様な顧客ニーズに対して、より迅速で柔軟な生産ラインの展開が可能になります。CTは、ITとOTのネットワークを紐づける極めて重要な役割を果たし、5G技術の活用を通じて企業内のシームレスなDX化を可能にします。しかし、至るところに存在しながら目には見えない無線通信は、OTネットワークとITネットワークの間の明確な境界を破壊し、設計、管理、保護が不十分な5Gプライベートモバイルネットワークを経由してセキュリティ脅威が伝搬することを許してしまいます。

## 企業5Gセキュリティの最適化： 重要資産の保護



### プライベートモバイルネットワーク内でのアプリケーション実行

プライベートモバイルネットワークを利用する様々な業界において、AR/VR/MLといった無停止運用されるアプリケーションの安全を保障し、攻撃者による運用停止や妨害から保護することが重要です。



### 通信の安全性

4G、5GおよびWi-Fiなどの無線技術には攻撃対象となり得る脆弱性が存在するため、通信の安全性を確保することが極めて重要です。これらの無線通信はDDoS攻撃、マルウェアの侵入、ランサムウェアなどの一般的なセキュリティ脅威の攻撃方法として利用される可能性があります。



### 企業の機密データ

無線ネットワーク内の通信セキュリティとプライバシーの確保対象には、機密情報、デジタル資産、企業秘密、従業員や顧客の個人情報、その他送信・保存される機密データなどが含まれます。



### O-RAN システム

Open RANによるクローズドアーキテクチャからオープンアーキテクチャへの移行は、無線ネットワークを構築する上で、より柔軟でコスト効率の高いアプローチとなる一方で、新たな攻撃対象やSBOM(Software Bill of Materials: ソフトウェア部品表)による脆弱性管理の必要性が生じます。



### プライベートネットワーク内の重要インフラ

標準x86サーバーおよび仮想化・クラウド環境によるIT化の進展に伴い、IT特有のセキュリティ脅威が無線ネットワーク内にも発生します。プライベートモバイルネットワーク内のインフラおよび重要コンポーネントの保護は重要な課題です。

# アプリケーションからセキュリティを考える： プライベートモバイルネットワークセキュリティが期待される業界



スマート  
工場



スマート  
物流



スマート  
ヘルスケア



エネルギー・  
公益事業



軍事・  
防衛

## CTOneソリューション： 特長と提供価値

CTOneのソリューションは、企業や通信事業者が即時利用可能なモバイルネットワークセキュリティを提供します。4G/LTEおよび5Gネットワークにおける多様で進化するセキュリティ脅威に対して、堅牢な保護を提供します。

### 1 テーラーメイド・ソリューション

ITとCTドメインの統合し、プライベートモバイルネットワーク全体をカバーするテーラーメイドのセキュリティソリューションです。

### 2 ゼロトラストとジョイントディフェンスによるエンドツーエンドの保護

エンドポイント、RAN、MEC、5GCをカバーするこの包括的なサイバーセキュリティソリューションは、ゼロトラスト&ジョイントディフェンスによるセキュリティ対策が可能です。

### 3 セキュリティ視覚化・可視化

様々なエンドポイントデバイスを含む包括的で透視的なネットワークトポロジーを提供し、セキュリティ状態を可視化します。

### 4 ユーザーフレンドリーな統合コンソール

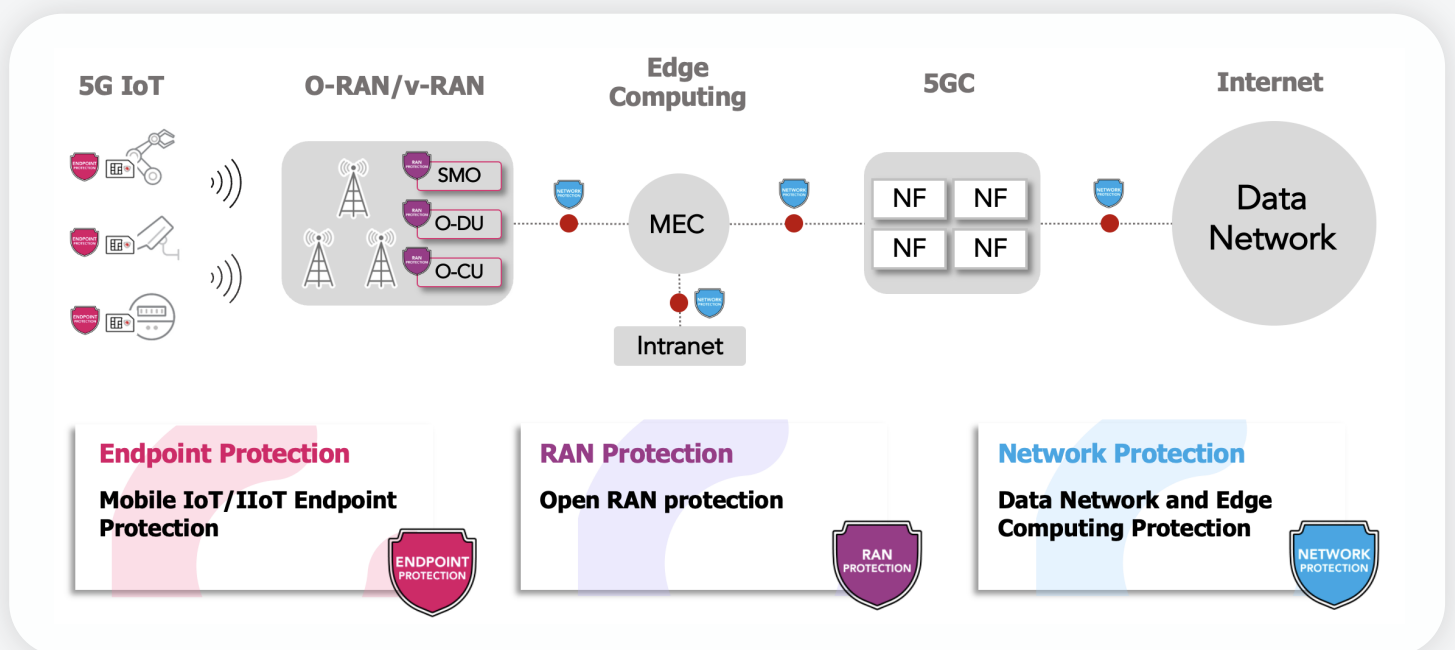
IT技術者や情報セキュリティ担当者にユーザーフレンドリーなコンソールを提供することで、5G技術導入に必要なスキル獲得時間を短縮します。

### 5 透視的かつベンダー非依存な導入

既存の5Gインフラに互換性問題を生ずることなく透視的に導入することが可能です。

# プライベートモバイルネットワークにおけるセキュリティ課題

クローズドアーキテクチャから オープンアーキテクチャへの移行	ネットワーク機能の仮想化
オープンソースソフトウェアの活用	見えにくいセキュリティ状態
異なるネットワーク(IT・OT・CT) 環境	無防備な多数のIoTデバイスの 利用
N3、N6、A1、E2、O1... などの不慣れなCTインタフェース	ITおよび情報セキュリティ管理者の CT知識不足



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、ORAN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において、企業が直面するセキュリティ脅威に対処します。



“

To Protect the Next-Generation Wireless Networks for  
Digital Transformation

”



[www.ctone.com](http://www.ctone.com)

### 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。

© 2023 CTOne All Rights Reserved.