

R-Car プロアクティブなパートナー ソリューション



## 信頼可能な実行環境

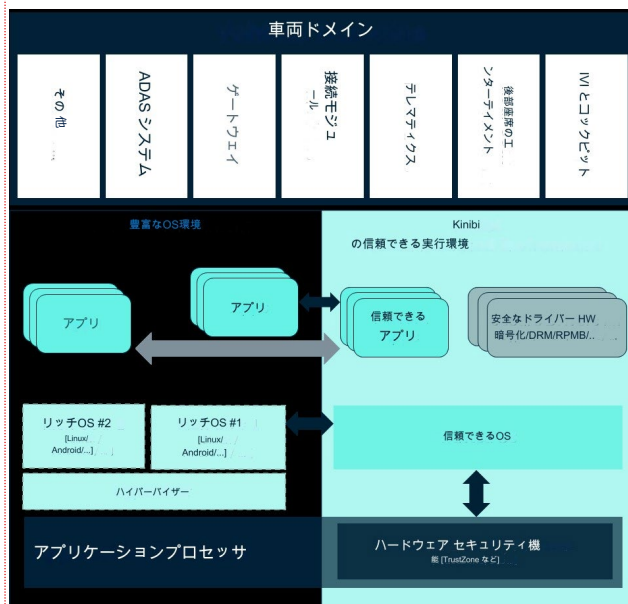
### 解決概要

信頼可能な実行環境 (TEE) は、セキュリティ操作を実行するためのSecure Enclaveを提供します。TEEは、カスタムコードとデータを世界中の通常OS (Linux, QNX など) から分離して保護します。

### 特徴と利点

- Art Teeのステート
- 幅広い脅威軽減策
- 高性能暗号化
- 信頼可能なアプリケーションとその信頼可能なアプリケーションの開発
- QEMUバージョンを含む完全なSDK

### 図／グラフィックス



### 対象市場とアプリケーション

- IVI システム / 統合デジタルコックピット / リアスクリーンエンターテインメント
- ネットワークゲートウェイ
- ADAS システム

5. <https://www.trustonic.com/secure-os/>

## 技術的な利点

- 複数のリッチオペレーティングシステムとハイパーバイザーのサポート
- 保護メカニズムの充実セット、つまり
  - サイドチャネル保護
  - アンチロールバック保護
  - その他 となる
- 追加のセキュリティ、パフォーマンス、安定性を提供するマイクロカーネル アーキテクチャ
- ポスト量子暗号に対応した更新可能な暗号ライブラリ
- 複数の安全なストレージオプションのサポート
- グローバルプラットフォームAPIのサポート
- Widevine レベル 1 DRM をサポート
- ARM V9 バージョンが利用可能
- すべての標準TEEサービスを追加

## エコシステム

- SDKサービスとパートナーの完全なエコシステムが利用可能。
- 利用可能な SDK/DDK の QEMU バージョン
- トレーニングサービス
- Android への完全な準拠のサポート
- 建築コンサルティング
- 専門能力開発サービス

## サポートとメンテナンス

- 長期サポートとメンテナンス
- 5年、10年、15年のオプションがある

## 規制とコンプライアンス

- 世界的な規制準拠のための共通基準 EAL5+ の認証を取得
- 利用可能なサポートドキュメント
- シンプルな SBOM を備えた独自の IP ソリューション (サードパーティの依存関係なし)
- Vulnerability Responseサービス