

# 組込み機器に搭載可能な軽量TLSライブラリと、 リアルタイム改ざん検出

## GUARD FIPS Security Toolkit / Core / WhiteBox

### Point

1 FIPS 140-2認証取得済みの暗号ライブラリ、  
TLSは1.2に対応  
(GUARD FIPS Security Toolkit)

### Point

2 IoT機器を守るリアルタイム改ざんチェック(Core)と、  
機密データ保護(WhiteBox)

### Point

3 セキュリティベンダーとして実績のある  
インサイドセキュア社の製品

脅威に合わせた複数の対策をご提案

マルウェア  
IDなりすまし  
リバースエンジニアリング  
サービス不能攻撃／DoS

データ改ざん  
のぞき見スパイ行為  
パスコード解除  
情報漏洩

ネットワーク経由の脅威にTLS  
標準で使用されているTLSプロトコルを  
IoT機器でも利用

内部からの脅威に難読化・改ざん検知  
IoT機器にアクセスされた場合を想定して  
ソフトウェア自体を保護

インサイドセキュア社のTLS、暗号ライブラリの特徴

- 組込み機器に最適な小さなコードサイズ
- Intel AES\_NI, ARMv8インストラクション対応
- ハードウェア処理対応や暗号アルゴリズムの取り外しが容易
- メモリの使用量を制限可能
- 高スループット・低レイテンシー

インサイドセキュア社の難読化・改ざん検知ツールの特徴

- 改ざん行為の検知:
  - アプリケーションが自律的に防御を埋め込み、コードの変更を防ぐ
- コードの難読化:
  - リバース・エンジニアリング防御
- 機密データの保護:
  - 機密性の保たれた暗号機能とデータ保護を提供

適用例

- IoT機器 ● 車載 ● ゲーム機 ● ネットワーク機器 など