

# FIPS対応TLSライブラリ

TLS Library for FIPS

## OpenSSLの脆弱性対策のご提案

### Point

- 信頼性が高く軽量なTLSライブラリ(GUARD FIPS Security Toolkit)
- FIPS 140-2認証取得済み暗号ライブラリを実装
- OpenSSLから移行するためのOpenSSL互換ライブラリを付属
- 車載向けにMISRAに準拠
- IoT向けに軽量(10KB以下)なTiny Editonも用意

POODLE

FREAK

OpenSSLの脆弱性で困ってませんか?

Heartbleed

INSIDE Secure セキュリティ製品で解決!

最新の暗号に対応

- TLS プロトコル  
TLS 1.0, 1.1, 1.2, TLS Extensions
- 暗号アルゴリズム  
FIPS 140-2 認証暗号ライブラリ

MISRA 対応

車載向けに MISRA 対応した  
コードの提供

SSL → Internet

FIPS 140-2 認証済み暗号ライブラリ

FIPS 140-2 認証取得の暗号ライブラリなので安全、安心

OpenSSL 互換ライブラリ

OpenSSL 互換ライブラリを利用する事で、OpenSSL を  
利用しているアプリケーションからの移行が容易になります。

アプリケーション

OpenSSL

→

アプリケーション

OpenSSL  
互換ライブラリ  
GUARD FIPS  
Security Toolkit

### 利用例

◆プリンタ ◆車載 ◆ゲーム機 ◆ネットワーク機器

東芝情報システム株式会社