

Part2. プログミング

はじめに

1) サンプルプログラム

- TLSプロトコル
- 暗号アルゴリズム
- 公開鍵とPKI

2) OpenSSL/wolfSSL

これらのサンプルソースコードは特に断りのない限り、OpenSSL, wolfSSLの両者で同様の動作をします。

3) ヘッダーファイル

本書で紹介するサンプルプログラムでは下記のヘッダーファイルをインクルードします。この中には角プログラムで共通に使われるロジックが含まれています。

Examples/include/example_common.

- C言語標準ライブラリーのためのヘッダーファイル
- BSD Socketライブラリーのためのヘッダーファイル
- TLS1.3のセッション鍵をえるためのコールバック 使い方は「Part4 付録1 プログラミング環境 2) デバッグツール」を参照。

4) ビルド方法

ビルド方法は「Part4 付録1 プログラミング環境 1) サンプルプログラムのビルド」を参照。