



Seminar

OpenSSLアプリケーションのスムーズな移行のために

wolfSSL Japan合同会社
エンジニア
松尾 卓幸
2021年4月21日



Outline

0

wolfSSLを知る

1

OpenSSL互換レイヤーとは何か？

2

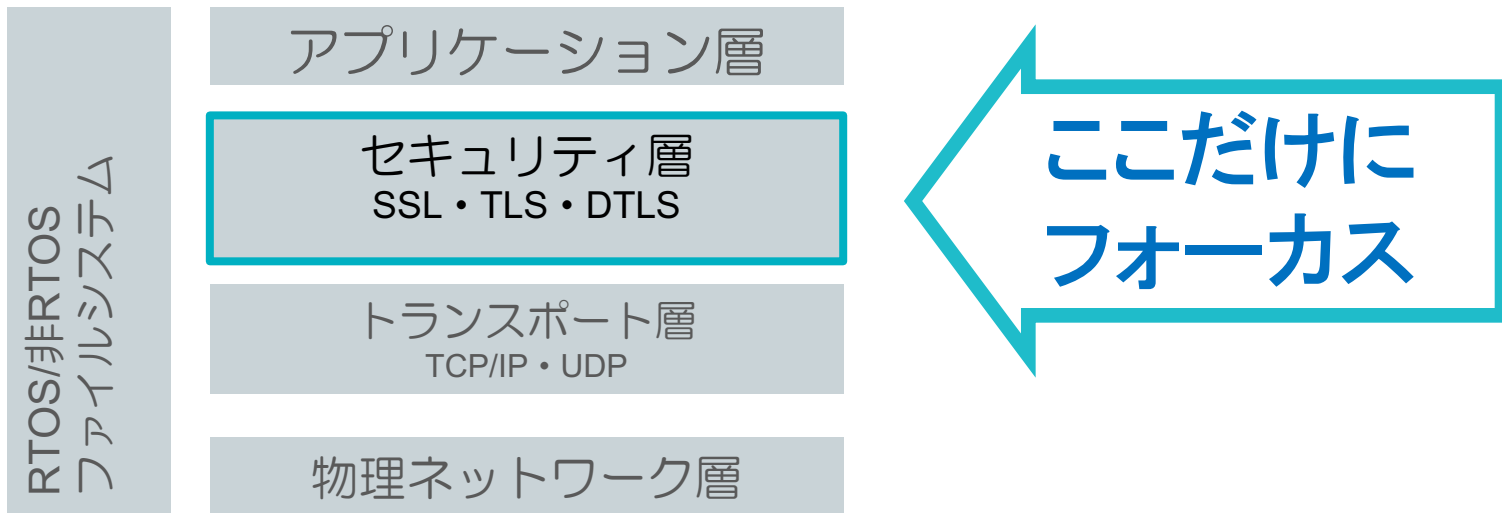
OpenSSL互換レイヤーの仕組み

3

サンプルアプリをwolfSSLに移行してみる

4

wolfSSLでビルドしてみた著名なアプリ



ネットワークセキュリティ、暗号技術の専門チームです

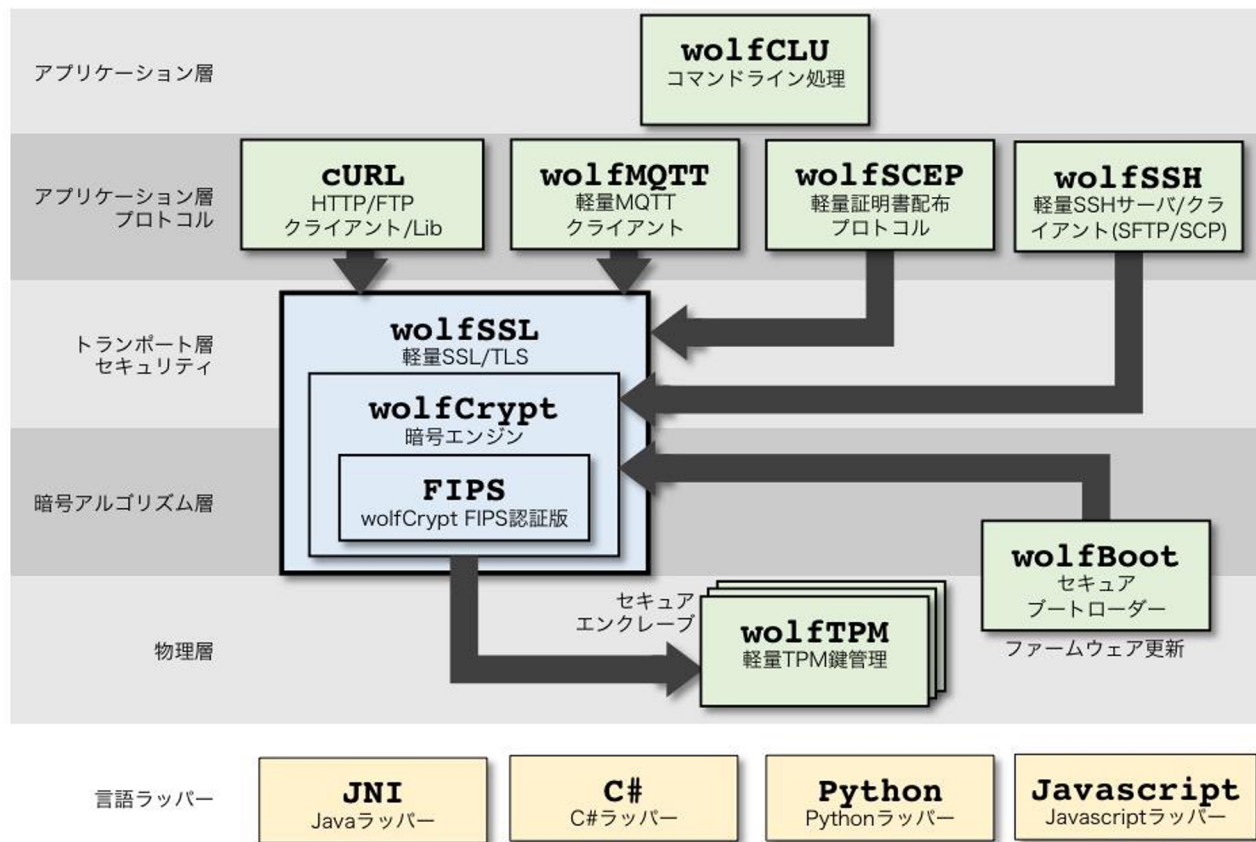
本社はシアトル



世界中のお客様に
安全な通信をお届けしています



wolfSSLの製品



適用事例



スマート工場



病院：検査機器



車載：インフォティメント



電力：スマードグリッド



署名用ペンタブレット



オフィス機器

写真はイメージです

適用事例：ホーム



写真はイメージです

wolfSSLのフォーカス分野

- 高い信頼性
- 長期間安定した運用サポート

産業/ビジネス機器:

- 金融決済端末
- スマートファクトリ
- FA機器、産業用ロボット
- 電力監視
- ビル管理
- 複合機、プリンタ
- アプライアンスボックス

医療機器:

- 内視鏡
- CT検査装置
- 見守りベッド

自動車/鉄道関係:

- 車載AV
- エンジン制御
- 車両テスト/計測機器
- 配車システム
- 信号システム

家庭/一般機器:

- デジタルカメラ
- 掃除ロボット
- 健康機器
- スマートライト
- ドアホン/キー
- AV機器
- 太陽光発電
- パソコンソフト
- スマホアプリ/ゲーム

写真はイメージです

wolfSSLの特徴



スクラッチから書いたコード



オープンソースと商用のライセンスモデル



FIPS140-2認証実績（FIPS140-3を今秋取得予定）

Outline

0

wolfSSLを知る

1

OpenSSL互換レイヤーとは何か？

2

OpenSSL互換レイヤーの仕組み

3

サンプルアプリをwolfSSLに移行してみる

4

wolfSSLでビルドしてみた著名なアプリ

OpenSSL互換レイヤーとは何か？



OpenSSL APIのサブセットをwolfSSLのAPIにマッピング



OpenSSL依存のAppをwolfSSLに簡単に移行できるよう設計



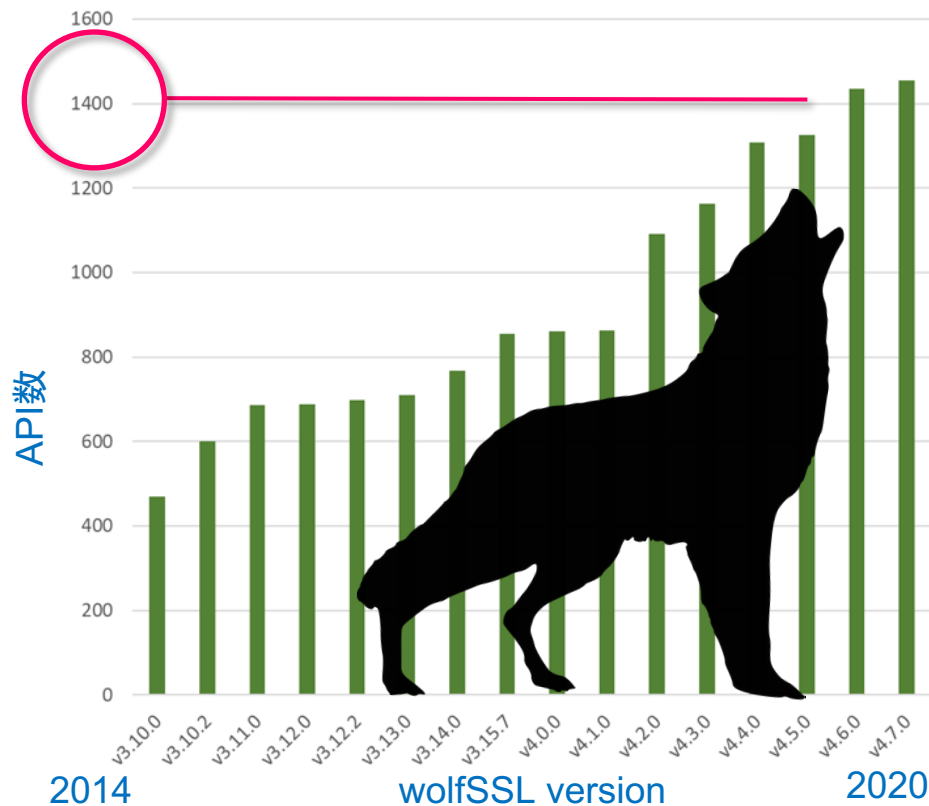
1400以上の互換APIを用意



構造体、enumもwolfSSLにマッピング

OpenSSL互換レイヤー

1400以上



互換API群



TLS関連



証明書/鍵/署名/ハッシュ



暗号化/復号



Encode/Decode

APIグループ	互換API数
SSL_*	275
X509_*	187
EVP_*	175
BIO_*	85
BN_*	55
PEM_*	48
ASN1_*	41
EC_*	41
RSA_*	37
ERR_*	37
sk_X509_*	34
その他	482
計	1497

Outline

0

wolfSSLを知る

1

OpenSSL互換レイヤーとは何か？

2

OpenSSL互換レイヤーの仕組み

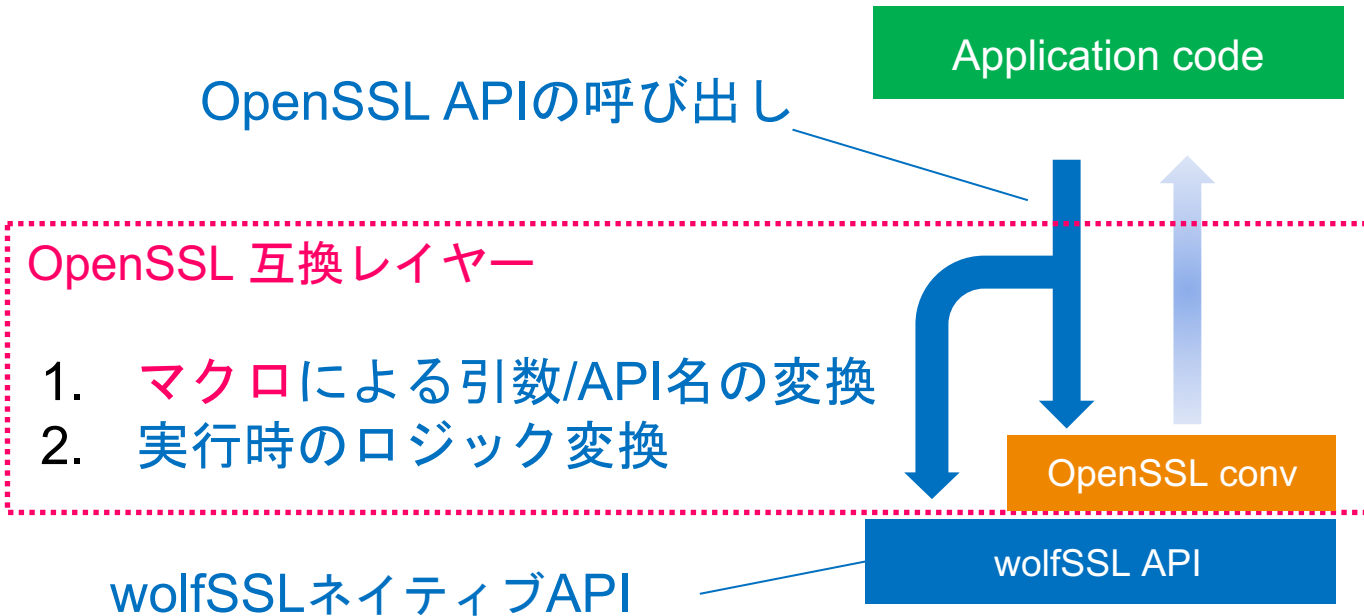
3

サンプルアプリをwolfSSLに移行してみる

4

wolfSSLでビルドしてみた著名なアプリ

OpenSSL 互換レイヤーの仕組み -1-



OpenSSL 互換レイヤーの仕組み -2-

wolfSSL の型

```
typedef WOLFSSL_EVP_PKEY  
typedef WOLFSSL_BIO  
typedef WOLFSSL_BIO_METHOD  
typedef WOLFSSL_CIPHER  
typedef WOLFSSL_X509_LOOKUP  
typedef WOLFSSL_X509_LOOKUP_METHOD  
typedef WOLFSSL_X509_CRL
```



OpenSSL の型

```
EVP_PKEY;  
BIO;  
BIO_METHOD;  
SSL_CIPHER;  
X509_LOOKUP;  
X509_LOOKUP_METHOD;  
X509_CRL;
```

OpenSSL 関数名

```
#define SSL_CTX_new  
#define SSL_new  
#define SSL_set_fd  
#define SSL_get_fd  
#define SSL_connect  
#define SSL_clear
```



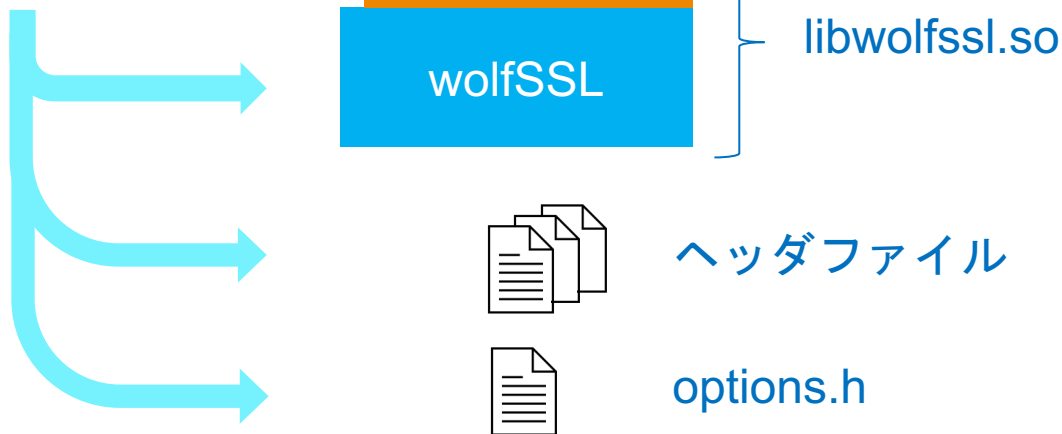
wolfSSL 関数名

```
wolfSSL_CTX_new  
wolfSSL_new  
wolfSSL_set_fd  
wolfSSL_get_fd  
wolfSSL_connect  
wolfSSL_clear
```

OpenSSL 互換レイヤーの仕組み -3-

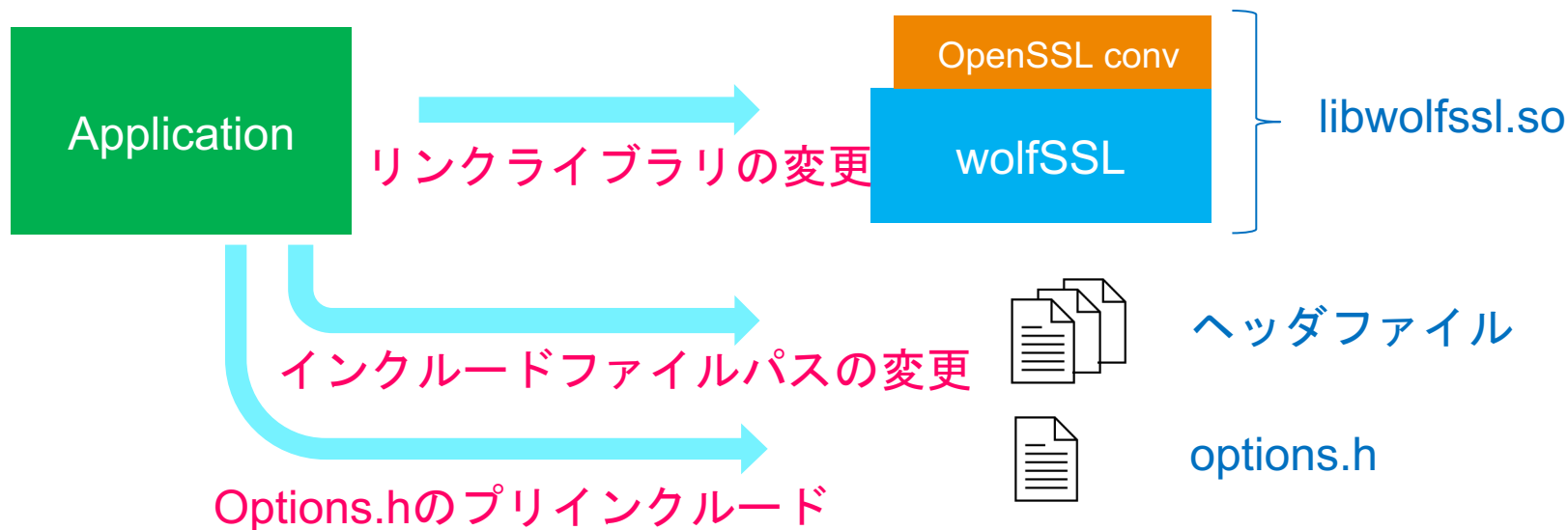
wolfSSL ライブラリ生成時のオプションにより互換レイヤーを付加

```
$ ./configure --enable-opensslextra  
$ make  
$ make install
```



OpenSSL 互換レイヤーの仕組み -4-

wolfSSL ライブラリ生成時のオプションにより互換レイヤーを付加



Outline

0

wolfSSLを知る

1

OpenSSL互換レイヤーとは何か？

2

OpenSSL互換レイヤーの仕組み

3

サンプルアプリをwolfSSLに移行してみる

4

wolfSSLでビルドしてみた著名なアプリ

TLSサーバーアプリ

testserver.c

OpenSSLの型、APIを使用

```
ssl = SSL_new(ctx);
SSL_set_fd(ssl, fd);

/* SSL_accept */
printf("starting TLS handshake¥n" );
while (1) {
    sslret = SSL_accept(ssl);
    ssl_eno = SSL_get_error(ssl, sslret);
```

アプリケーションをビルド

OpenSSL

```
$ gcc testserver.c -o open.out -lssl -lcrypt
```

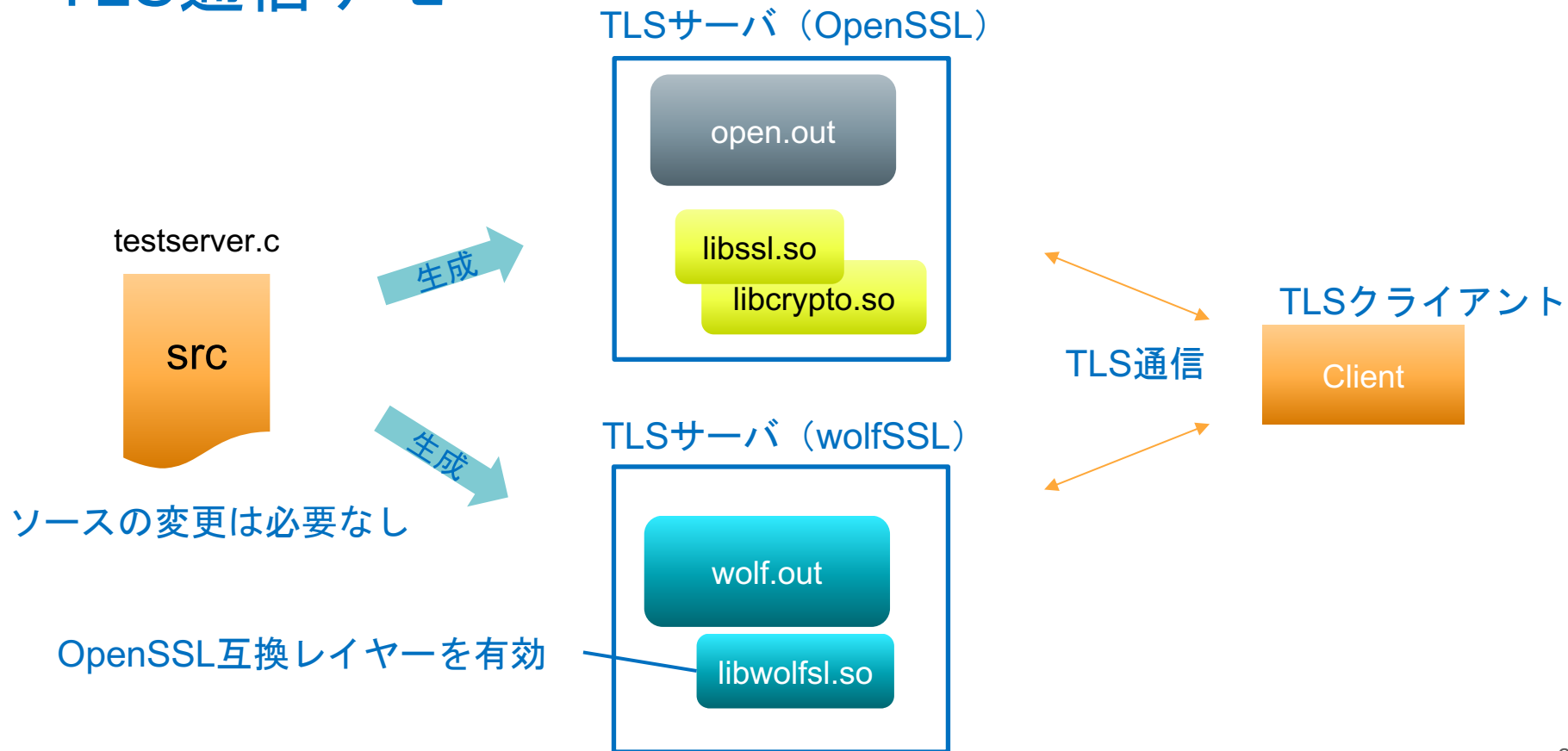
ソースファイル アプリ名 リンクライブラリ インクルードファイルパス

wolfSSL

```
$ gcc testserver.c -o wolf.out -lwolfssl -I<header file path>  
-include wolfssl/options.h
```

プレインクルードファイル

TLS通信デモ



デモ : TLSサーバーアプリビルド～通信

参考 ヒープ使用量の比較

- open.out と wolf.out の実行時にヒープ使用量を計測
- Valgrind + massif



OpenSSL				
n	time(i)	total(B)	useful-heap(B)	extra-heap(B)
50	28,002,940	277,592	212,986	64,606
51	28,091,762	241,752	177,657	64,095
52	28,150,844	188,768	126,649	62,119
53	28,209,996	183,768	123,649	60,119
54	28,269,615	178,488	120,481	58,007
55	28,328,719	173,808	117,673	56,135
56	28,387,768	119,888	84,825	35,063
57	28,446,839	61,448	49,761	11,687

180 ~ 270KB

wolfSSL				
n	time(i)	total(B)	useful-heap(B)	extra-heap(B)
87	57,677,169	12,384	11,909	475
88	57,867,340	12,136	11,723	413
89	57,871,777	12,080	11,685	395
90	57,890,025	12,216	11,801	415
91	57,907,860	12,200	11,789	411
92	57,914,181	12,336	11,903	433
93	57,921,066	12,296	11,890	406
94	57,924,016	9,920	9,643	277
95	57,928,806	5,664	5,411	253

12KB

Outline

0

wolfSSLを知る

1

OpenSSL互換レイヤーとは何か？

2

OpenSSL互換レイヤーの仕組み

3

サンプルアプリをwolfSSLに移行してみる

4

wolfSSLでビルドしてみた著名なアプリ

OpenSSL互換レイヤーを使用したアプリ



Apache

-- Web サーバー



QT

-- GUIツールキット



NGINX

-- Webサーバー



cURL

-- データ転送ライブラリ



Stunnel

-- 汎用TLSトンネリングサービス



StrongSwan

-- IPsec



OpenVPN

...

wolfSSLに移行するメリット



wolfSSLのH/Wアクセラレーションが利用可
フットプリント、メモリ使用量



TLS 1.3 対応の実績



単純なライセンスモデル



FIPS140-2認証実績（**FIPS140-3**を今秋取得予定）



コード開発エンジニアによる直接サポート

Q & A

ウェビナーへのご参加、
ありがとうございました。
wolfSSL Japan



wolfに関するご要望や追加質問などありましたら、
アンケートにご記入いただければと思います。

あるいは info@wolfssl.jpまでお寄せくださっても結構です。