

# N日でできる! TLS 1.3 自作入門

@tex2e

セキュリティ・キャンプ全国大会 2019 LT 大会

# 今日のお話

## TLS 1.3

# TLS とは

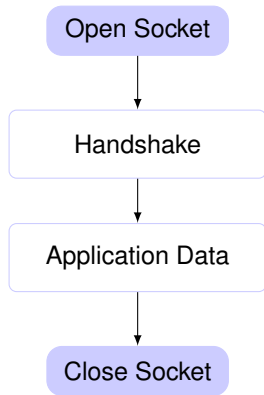
通信する2人はこれまでに**会ったことがなく**、  
**安全ではない**通信路を使ったとしても、  
**安全に**やりとりができる

# 安全な通信路とは...

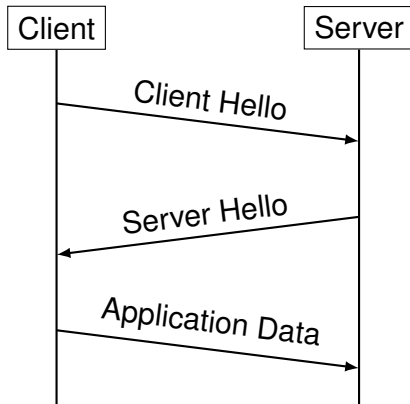
- 真正性
  - 通信相手が本物であることを確認できる
  - (サーバ証明書による **認証** ... X.509 Cert, PKI)
- 機密性
  - 権限を持つ人だけがアクセスできる
  - (通信内容の **暗号化** ... AES, ChaCha20)
- 完全性
  - 改ざんされない
  - (認証付き暗号による **改ざん検知** ... AEAD)

# TLS のハンドシェイク

- Handshake
  - どの暗号スイートを使うか決める
  - **公開鍵暗号**を用いて鍵共有する
  - 証明書を使って認証する
- Application Data
  - **共通鍵暗号**を用いて暗号化する
  - HTTP を暗号化したデータなど



# TLS 1.3のやりとり



# プログラマの3大「嗜み」

- 自作 OS
- 自作コンパイラ (プログラミング言語)
- 自作プロトコルスタック (TCP/IP, TLS)

※諸説あり

# TLS どうやって作るの？

## RFCを読む



# TLS 1.3 (RFC 8446)

[\[Docs\]](#) [\[txt|pdf\]](#) [\[draft-ietf-tls-...\]](#) [\[Tracker\]](#) [\[Diff1\]](#) [\[Diff2\]](#) [\[IPR\]](#) [\[Errata\]](#)

PROPOSED STANDARD

**Errata Exist**

E. Rescorla

Mozilla

August 2018

Internet Engineering Task Force (IETF)

Request for Comments: 8446

Obsoletes: [5077](#), [5246](#), [6961](#)

Updates: [5705](#), [6066](#)

Category: Standards Track

ISSN: 2070-1721

## The Transport Layer Security (TLS) Protocol Version 1.3

### Abstract

This document specifies version 1.3 of the Transport Layer Security (TLS) protocol. TLS allows client/server applications to communicate over the Internet in a way that is designed to prevent eavesdropping, tampering, and message forgery.

This document updates RFCs 5705 and 6066, and obsoletes RFCs 5077, 5246, and 6961. This document also specifies new requirements for TLS 1.2 implementations.

### Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has

# 構造体とバイト列の相互変換

復元

```
▼ Secure Sockets Layer
  ▼ TLSv1.3 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 512
  ▼ Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 508
    Version: TLS 1.2 (0x0303)
    Random: e6fd60bfdc54078d0d9969e7ede6475f2ddbccc7e0c545117...
    Session ID Length: 32
    Session ID: 07958723fa38848fb730317ab4fdb018eb2862edb25d76a8...
    Cipher Suites Length: 8
    ▶ Cipher Suites (4 suites)
0010 02 39 00 00 40 00 40 06 c1 d9 c0 a8 0b 02 9f 45 9·@·@· .....E
0020 0b f6 c6 9a 01 bb 2b 72 a6 87 08 19 91 3e 80 18 .....+r .....>..
0030 08 0a 4b 96 00 00 01 01 08 0a 11 0e 02 ac 98 ee ...K·...· .....
0040 c5 b5 16 03 01 02 00 01 00 01 fc 03 03 e6 fd 60 .....· .....
0050 bf dc 54 07 8d 0d 99 69 e7 ed e6 47 5f 2d db cc ...T·...i ...G_...
0060 7e 0c 54 51 17 99 13 6c 1e 9a 03 d3 f1 20 07 95 ~TQ·...l .....
0070 87 23 fa 38 84 8f b7 30 31 7a b4 fd b0 18 eb 28 #·8·...0 1z·...·(
0080 62 ed b2 5d 76 a8 bf bc ae 98 5b 6a 94 58 00 08 b·]v·...·[j·X·
0090 13 02 13 03 13 01 00 ff 01 00 01 ab 00 00 00 18 ...tls 13.pinte
00a0 00 16 00 00 13 74 6c 73 31 33 2e 70 69 6e 74 65
00b0 72 6a 61 6e 6e 2e 69 73 00 0b 00 04 03 00 01 02 rjann.is .....·
```

変換

# 実装の流れ

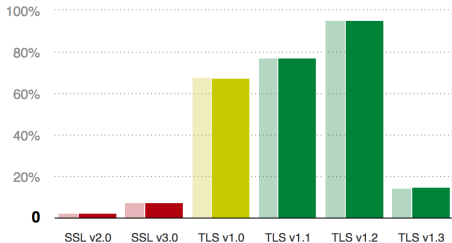
TLS のやりとりの実装：

1. ソケット通信
2. メッセージの構造体とバイト列の相互変換

TLS のやりとりの中身の実装：

1. 楕円曲線 Diffie-Hellman 鍵共有
2. HKDF による鍵スケジューリング
3. 認証付き暗号 (AEAD)
4. X.509 証明書

# TLS 1.3 の最新動向 (Server/Client)

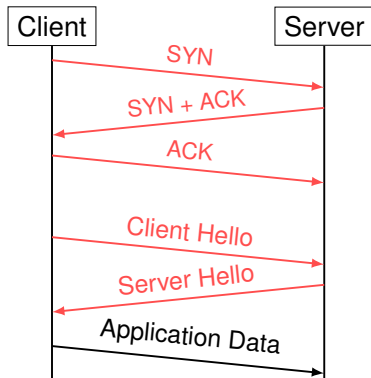


IE	Edge *	Firefox	Chrome	Safari	iOS Safari *	Opera Mini *	Chrome for Android
			74				
	17	67	75		12.1		
11	18	68	76	12.1	12.3	all	75
	76	69	77	13	13		
		70	78	TP			
			79				

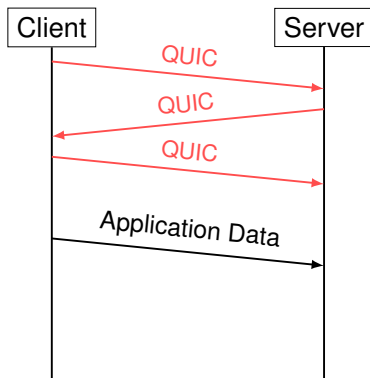
# TLS 1.3の最新動向 (QUIC)

UDP でコネクション確立と TLS 1.3 確立を同時に行う

TCP + TLS 1.3



QUIC (HTTP/3)



# TLS 1.3 自作は楽しいけど難しい






- 文書はほとんど**英語**
- 暗号技術の基盤となる**数学**の知識
- **ネットワーク**技術の知識
- **RFC** は入門書ではないので初学者には厳しい

# 30日で TLS 1.3 は 作れないよ

おわり



## 参考文献 I

-  RFC 8446: The Transport Layer Security (TLS) Protocol Version 1.3. IETF, August 2018.
-  Andy Brodie: Overview of TLS v1.3. OWASP, 2017. URL [https://www.owasp.org/images/d/d3/TLS\\_v1.3\\_Overview\\_OWASP\\_Final.pdf](https://www.owasp.org/images/d/d3/TLS_v1.3_Overview_OWASP_Final.pdf)
-  SSL Labs: SSL Pulse. Qualys, Inc, June 2019. URL <https://www.ssllabs.com/ssl-pulse/>
-  @Fyrd, @Lensco: Can I use... URL <https://caniuse.com/>
-  IETF Draft: "QUIC: A UDP-Based Multiplexed and Secure Transport". URL <https://tools.ietf.org/html/draft-ietf-quic-transport-22>

## 参考文献 II

-  Alessandro Ghedini: The Road to QUIC. Cloudflare, Inc, 2018. URL <https://blog.cloudflare.com/the-road-to-quic/>
-  雅也 山本: TCP/IP プロトコルスタック自作入門. KLab Inc, 2018. URL <https://www.slideshare.net/pandax381/tcpip-105857327>
-  Ivan Ristić 著, 齋藤孝道 監訳: プロフェッショナル SSL/TLS. ラムダノート, 2018.