Internet Week流Security Bootcamp

常識変化に向き合おう

TLS1.3時代の新常識

ヤフー株式会社

大津 繁樹

2018年11月27日

Internet Week 2018

自己紹介

大津 繁樹

- ヤフー株式会社 サイトオペレーション本部
- CDNチーム, Node.js Support
- Node.js Collaborator

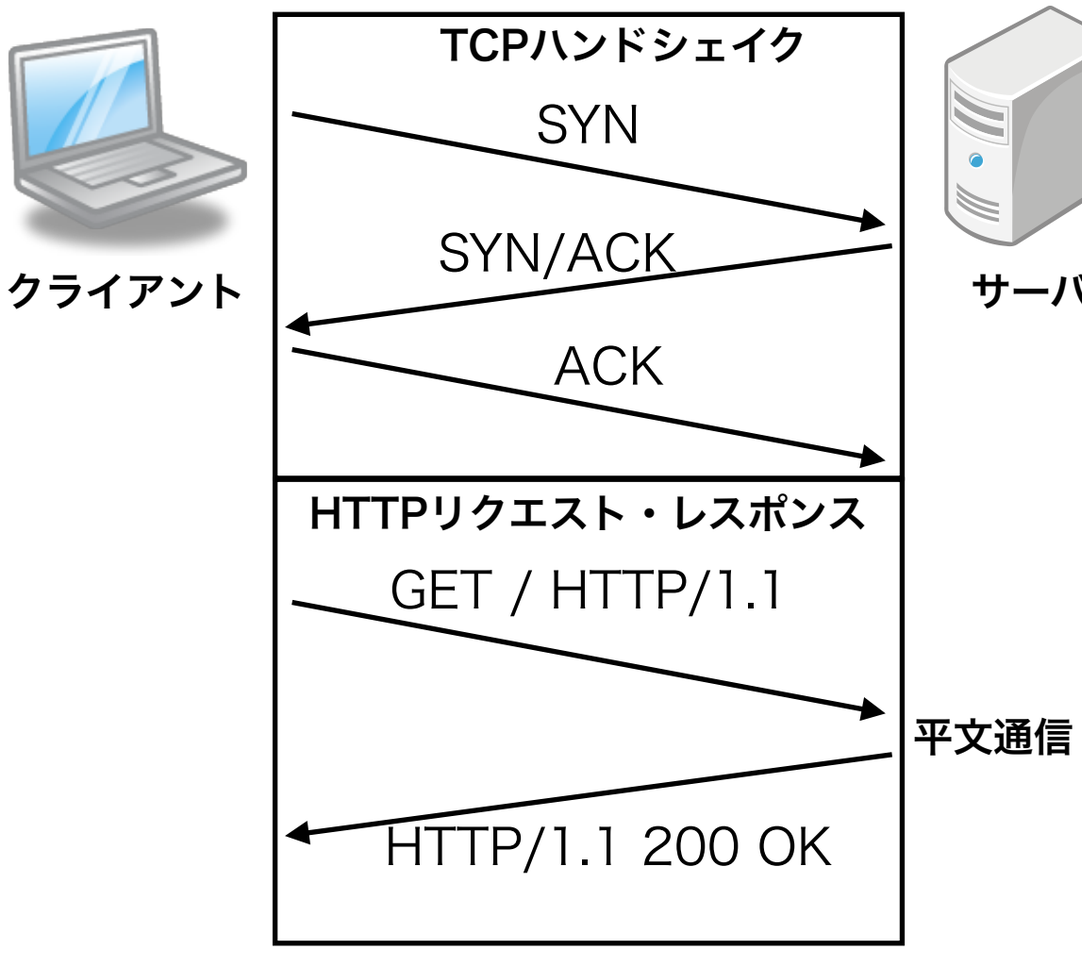
内容

- TLS/HTTPSの基礎(TLS1.3ベースで説明)
- 常識変化と向き合う

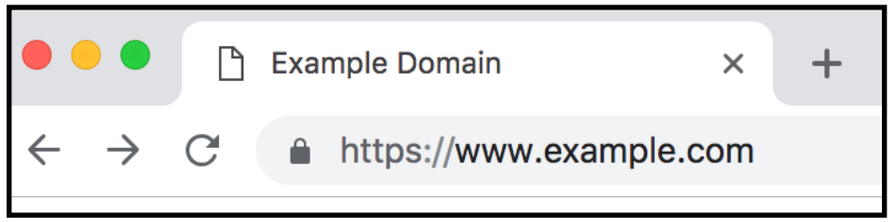
1. 全てをHTTPS化
2. 古いものを捨てる
3. TLS関連の設計が不要に
4. HTTPSと通信先の信頼は別

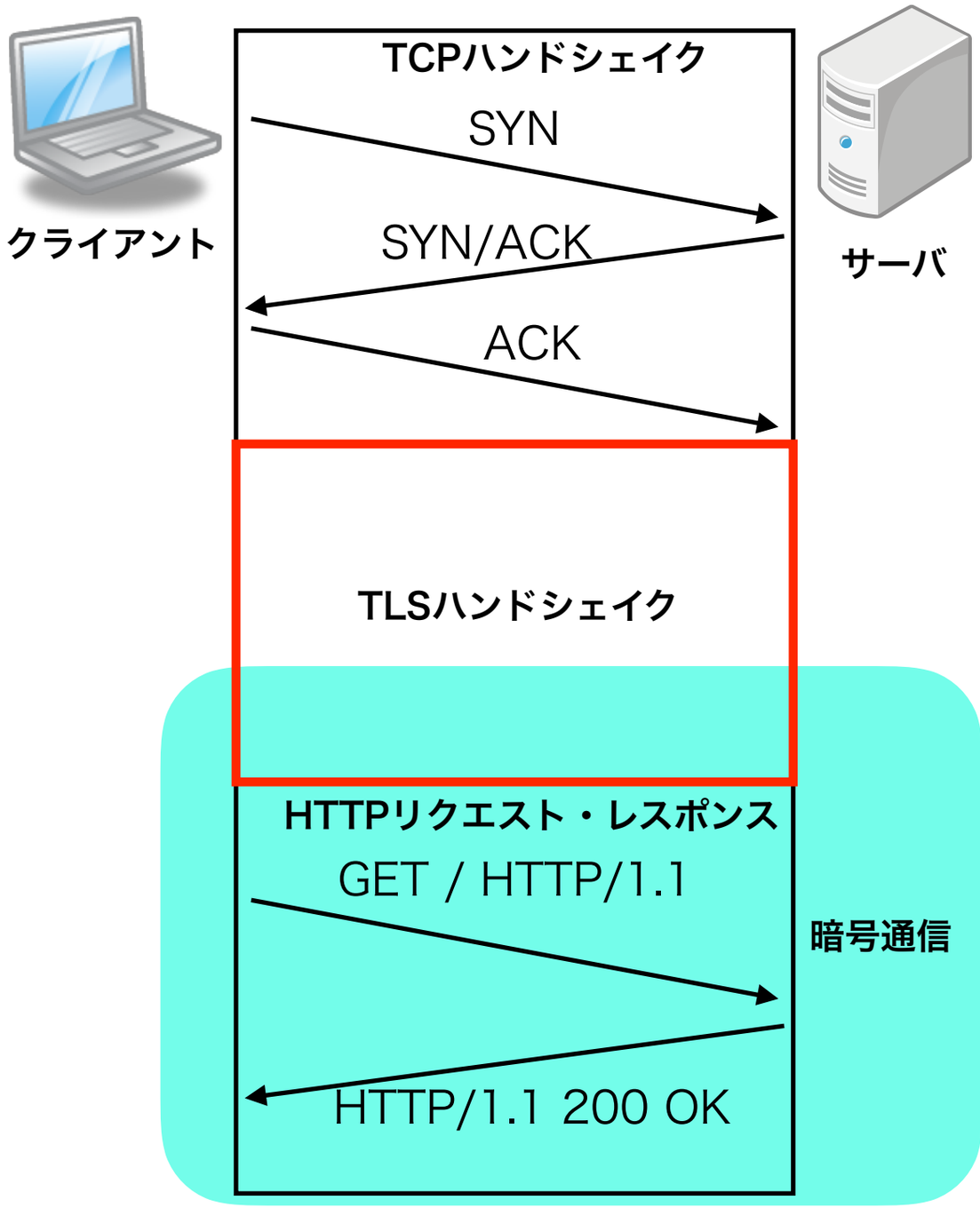
HTTPとHTTPS通信の違い

HTTP通信

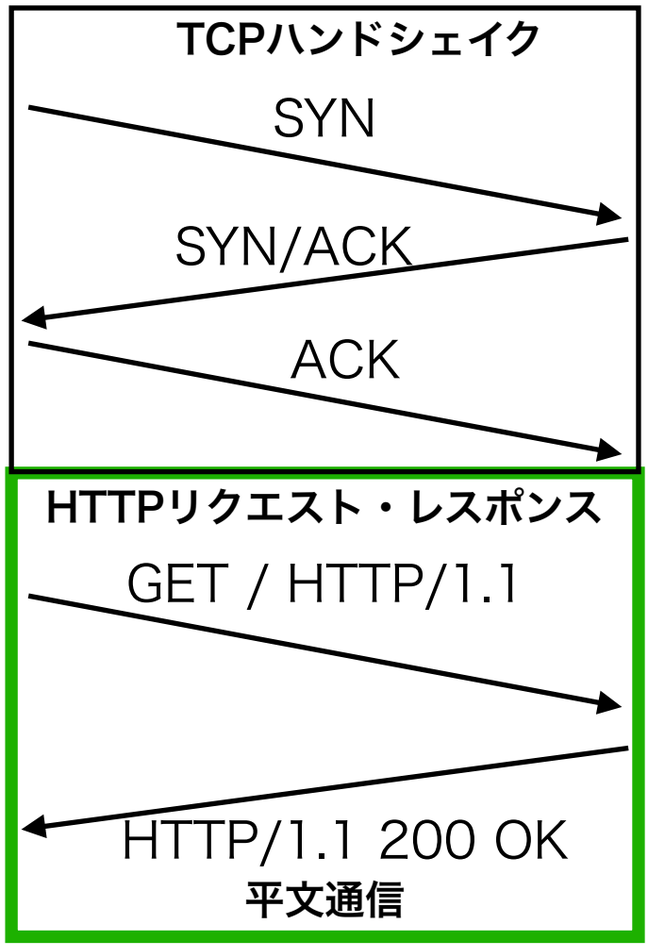


HTTPS通信





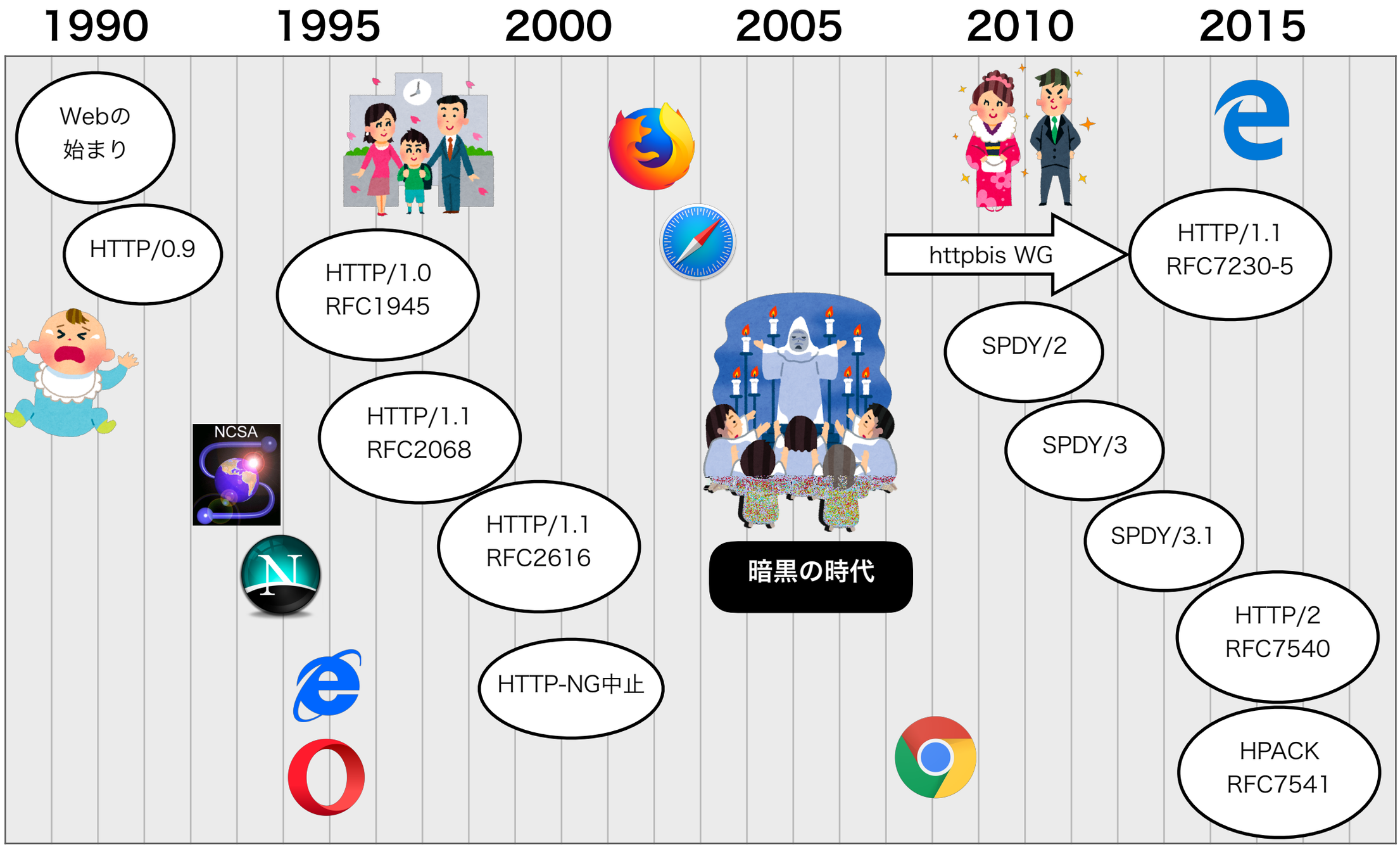
HTTPパケットの中身



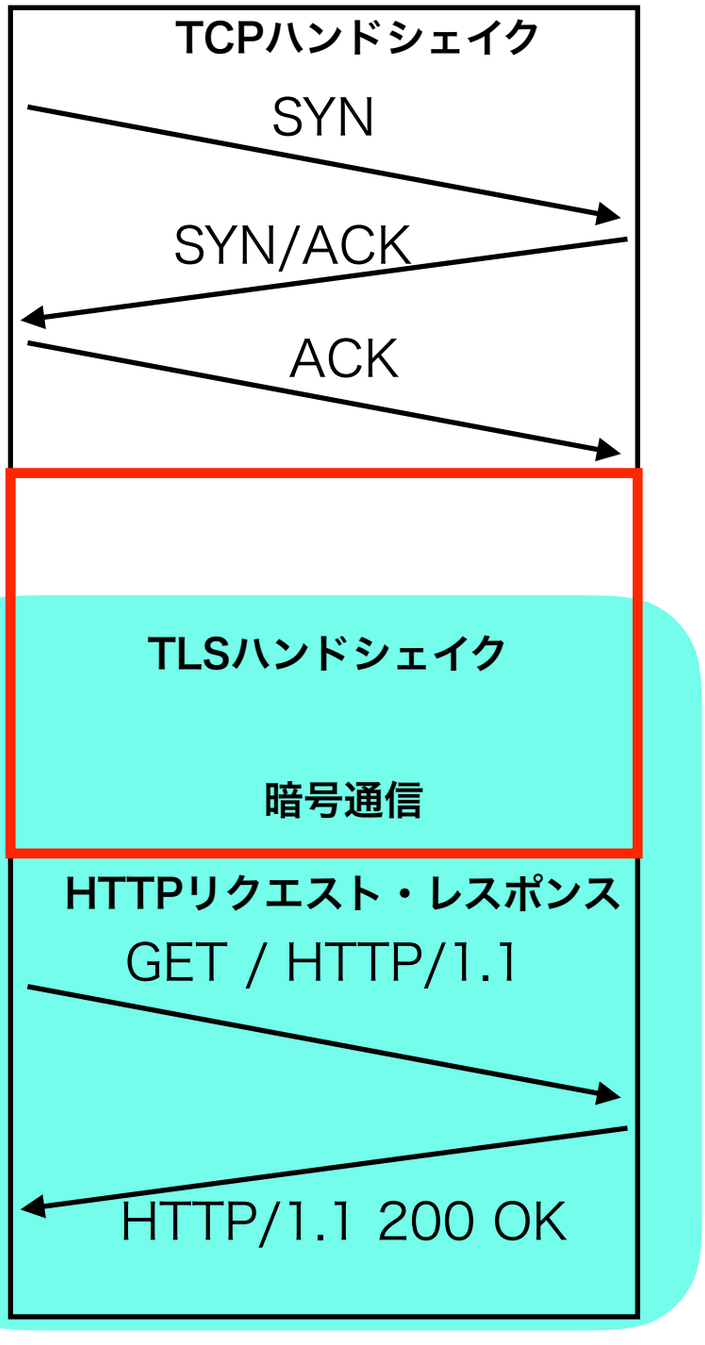
イーサネットヘッダ	IPヘッダ	TCPヘッダ	HTTP
宛先MACアドレス 送信元MACアドレス	宛先IPアドレス 送信元IPアドレス	宛先ポート 送信元ポート	リクエスト レスポンス

平文

HTTPプロトコルの年表



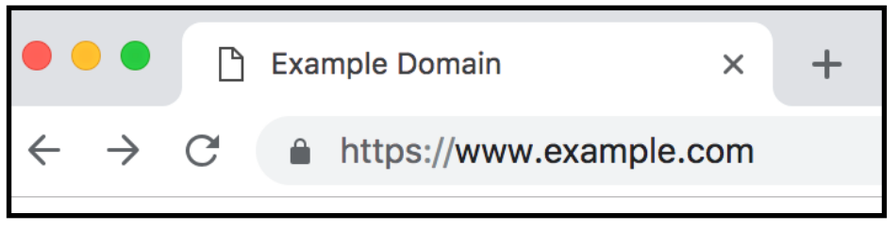
HTTPSパケットの中身



TLSハンドシェイクデータパケット

イーサネットヘッダ	IPヘッダ	TCPヘッダ	TLS	
			TLSレコード	TLSハンドシェイク
宛先MACアドレス 送信元MACアドレス	宛先IPアドレス 送信元IPアドレス	宛先ポート 送信元ポート		

途中まで平文



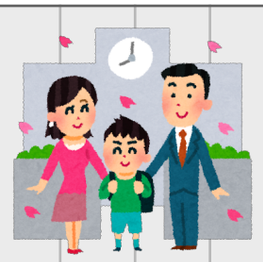
TLSアプリケーションデータパケット

イーサネットヘッダ	IPヘッダ	TCPヘッダ	TLS	
			TLSレコード	暗号データ
宛先MACアドレス 送信元MACアドレス	宛先IPアドレス 送信元IPアドレス	宛先ポート 送信元ポート		

SSL/TLSプロトコルの年表

1990 1995 2000 2005 2010 2015

Webの
始まり



SSL2.0

SSL3.0
RFC6101

TLS1.0
RFC2246

TLS1.1
RFC4346

TLS1.2
RFC5246

PCT

2018年8月発行

TLS1.3
RFC8446

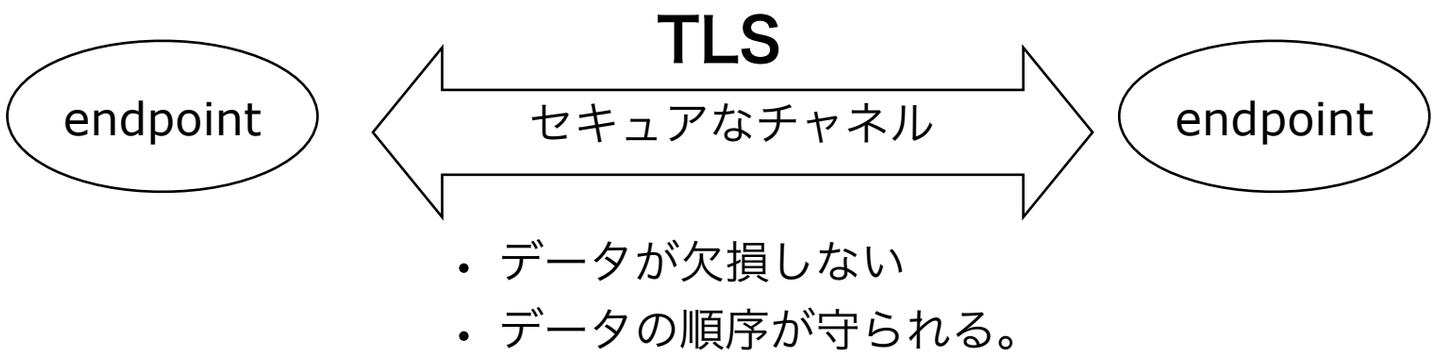
TLSの目的

RFC8446 The Transport Layer Security (TLS) Protocol Version 1.3

1. Introduction

The primary goal of TLS is to provide a **secure channel** between two communicating peers; the only requirement from the underlying transport is a

- TLSプロトコルの最重要なゴールは、通信する２点間で**セキュアチャネル**を提供することである。通信経路に求められる要件は、通信欠損のなく(reliable)、データ順序が守られることである。



セキュアチャネルとは？

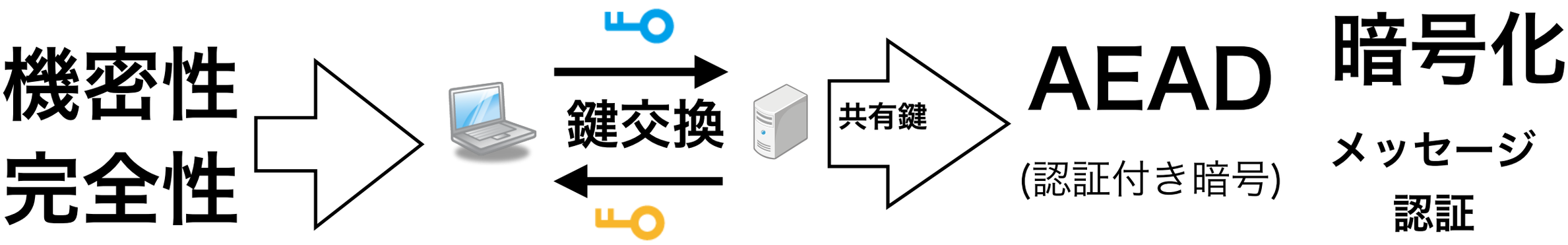
- 認証(Authentication): サーバを認証する。クライアントの認証はオプション。通信相手の認証と信頼は別物(後述)

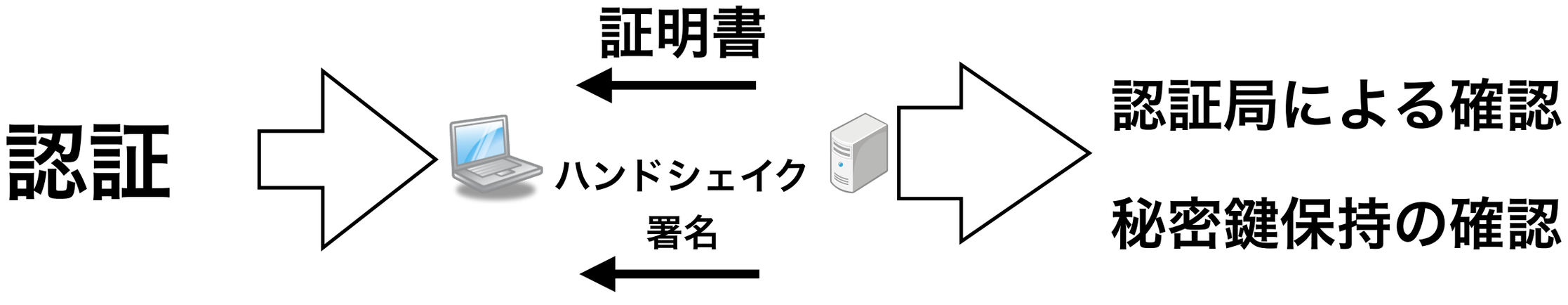
- 機密性(Confidentiality)：通信相手以外がデータの内容を見えないようにする。

- 完全性(Integrity)：通信経路途中でデータの改変ができない。

相手の顔が見えないインターネット上で安全な通信を確立する

セキュアチャネルを
TLSで実現するには?

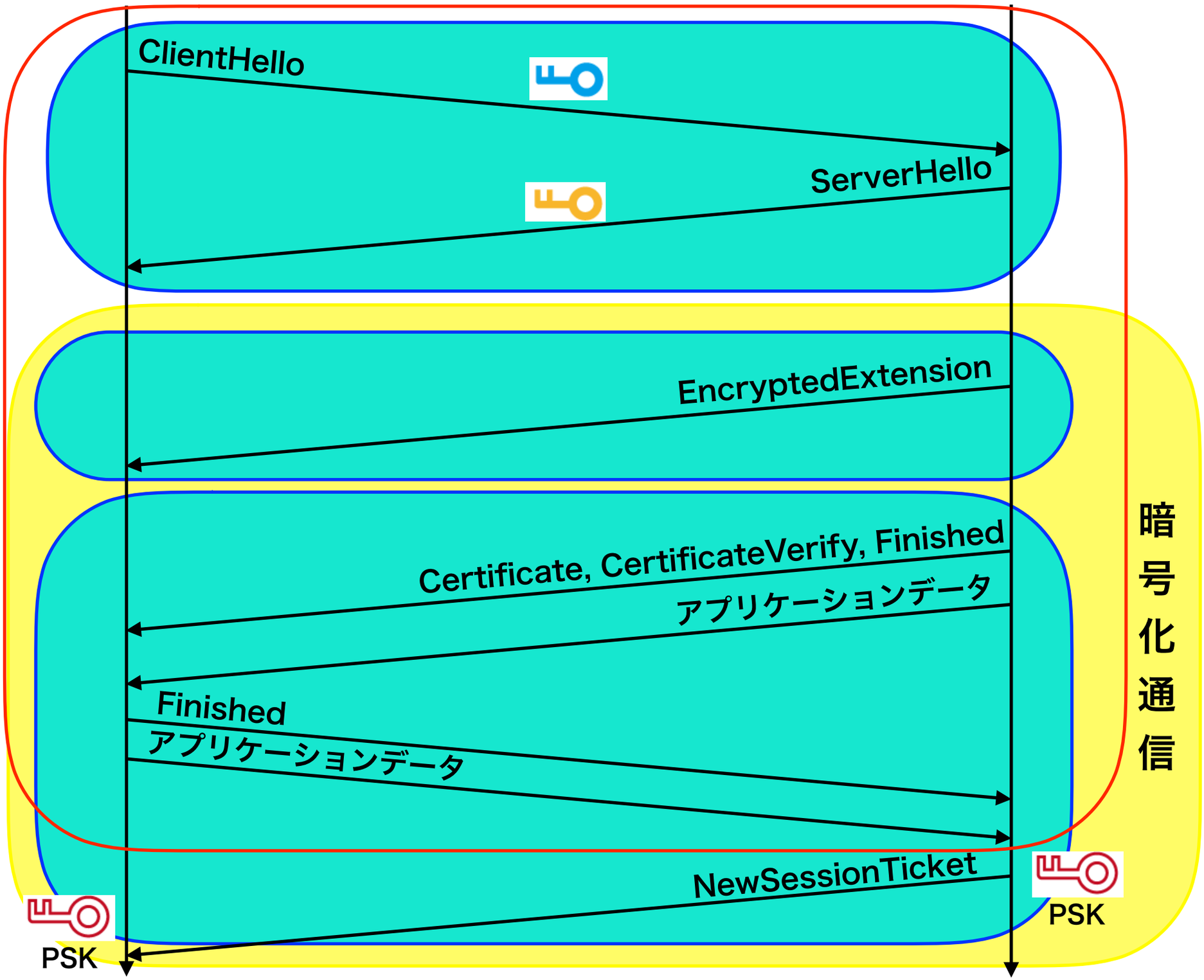




TLS1.3のハンドシェイク
1-RTT 初期接続

クライアント

サーバ



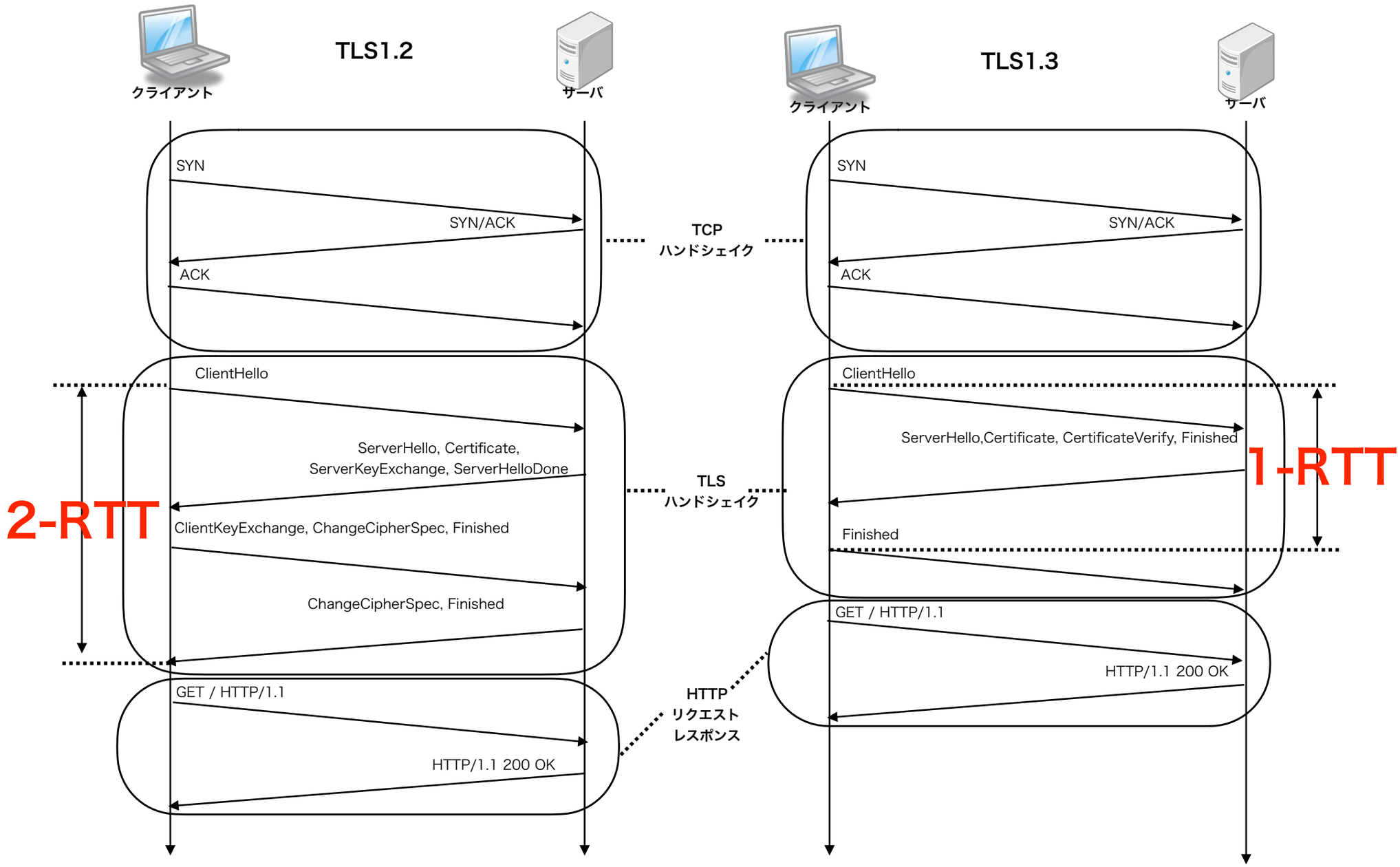
1. クライアントパラメータの送付と鍵交換

2. サーバパラメータの送付

3. サーバ認証、ハンドシェイクの改ざんチェック、アプリケーションデータの送受信

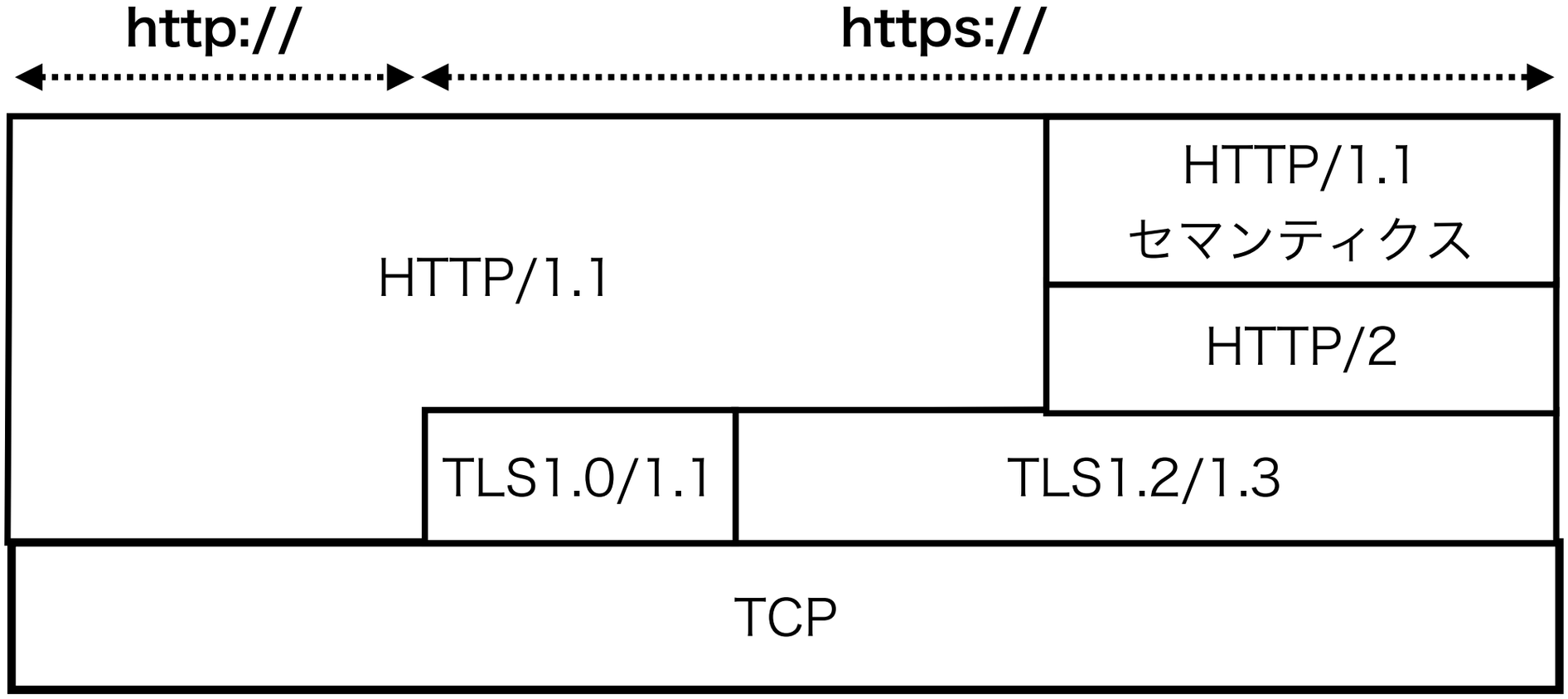
4. 再接続用チケットの送付

TLS1.3の高速化



速いハンドシェイク

2018年8月の
Webプロトコル・スタック



- **2018年8月11日 TLS1.3(RFC8446)発行**
- 2018年6月30日 PCI-DSS(*)でTLS1.0利用禁止、TLS1.1非推奨

PCI-DSS: クレジットカード情報を扱う国際的なセキュリティ基準

常識変化に向き合う#1
「全てをHTTPS化」

昔

パスワードやクレジットカード情報など大事な情報を扱う部分だけをHTTPSで提供する。

今

全てのページをHTTPS化する。

なぜ全部HTTPSにしないといけないの？

2013年6月： エドワード・スノーデン事件

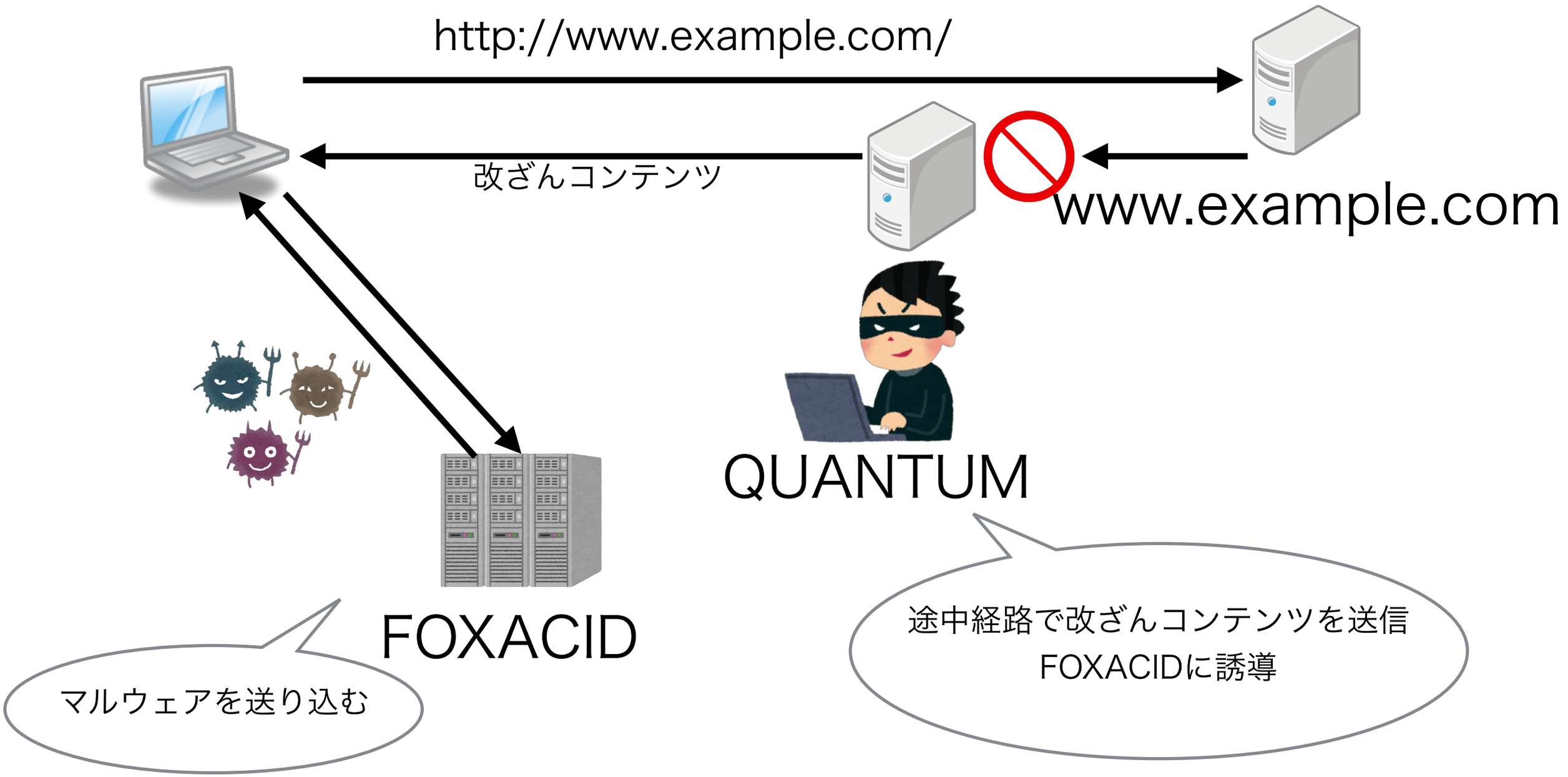
- NSA, CGHQによる国家レベルの広範囲な盗聴行為が明らかに

- 通信キャリアと協力し、DC内やインターネットバックボーンに盗聴・改ざんの仕掛けを配置

- 平文通信をMiTMで改ざんし未知のマルウェアを感染させる

- 暗号の標準化仕様にバックドアを仕掛けているとの話も

NSAによるサイバー攻撃の一例



https://www.schneier.com/blog/archives/2013/10/how_the_nsa_att.html

IAB(*)によるインターネットの信頼性に関する宣言(2014/11)

- 新しくプロトコルを設計する際には、**暗号化機能を必須**とすべき。

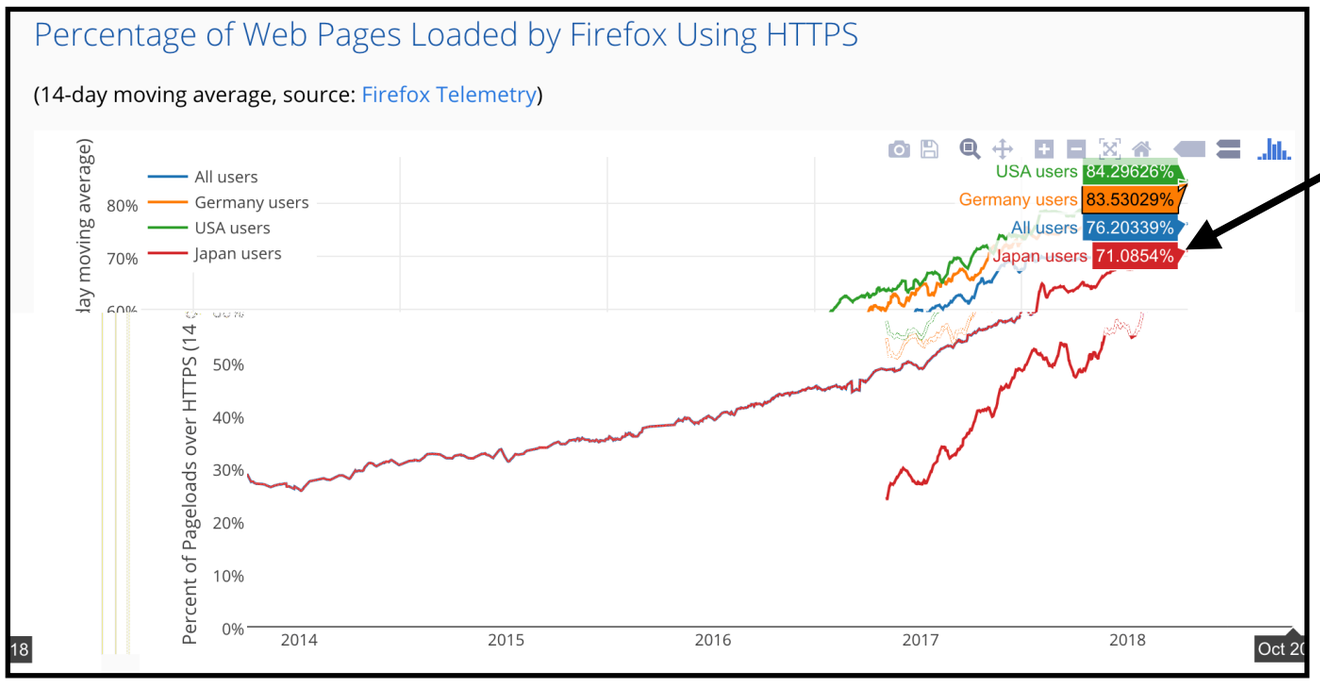
- ネットワーク運用者やサービス提供者に**暗号化通信の導入を推進**するよう強く求める。

- コンテンツフィルターやIDS等平文通信が必要な機能については将来的に代替技術の開発に取り組む。

(* Internet Architecture Board)
https://www.iab.org/2014/11/14/iab-statement-on-internet-confidentiality/

HTTPSの導入状況(読み込みページ割合)

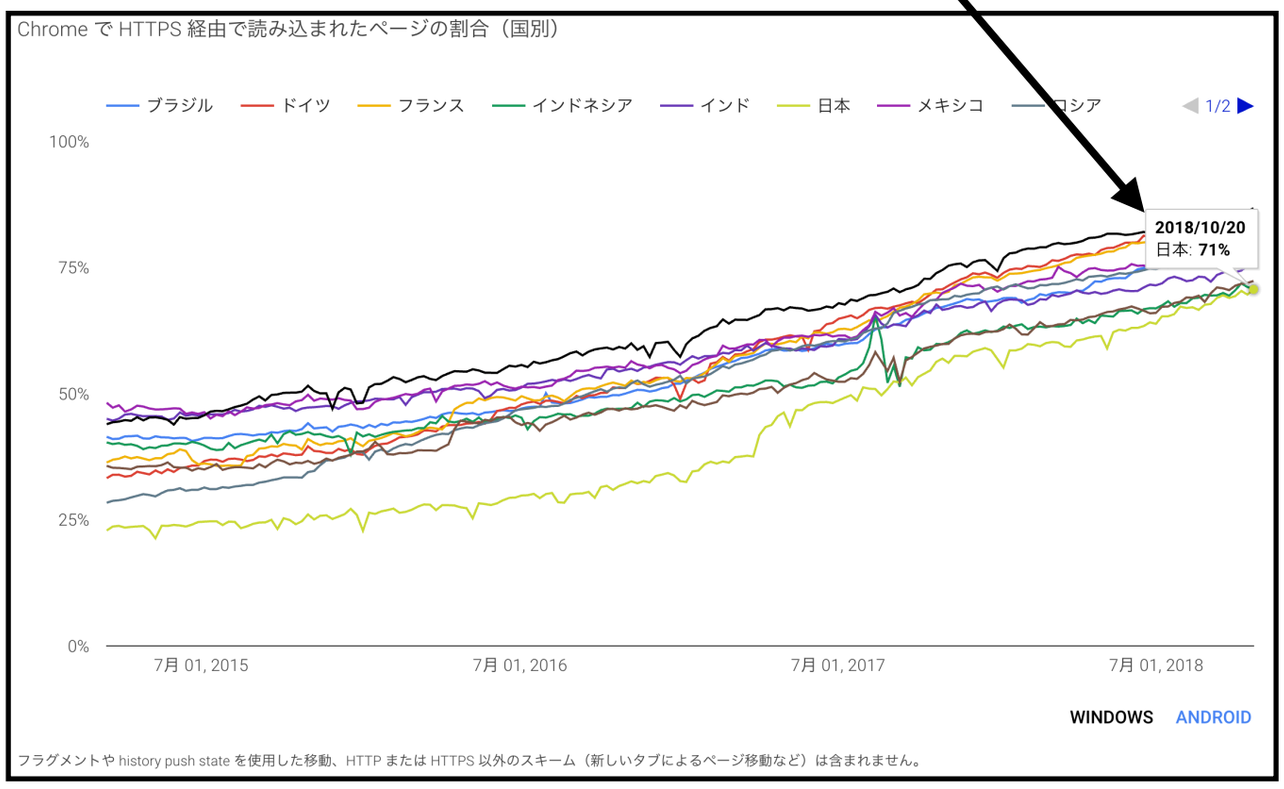
Firefox



Japan: 71.1%

Japan: 71%

Chrome



https://letsencrypt.org/stats/#percent-pageloads

https://transparencyreport.google.com/https/overview

常識変化に向き合う#2
「古いものを捨てる」

昔

SSL3.0は、脆弱性が発見されて使うのは危険だけど、ガラケーが使えなくなるから残しておかないと。

今

将来的な安全性を確保するためTLS1.0/1.1のサポートをやめよう。

主要ブラウザにおける TLS1.0/1.1のサポート廃止

Firefox

Mozilla Security Blog

OCT 15 2018

Removing Old Versions of TLS

Martin Thomson

In March of 2020, Firefox will disable support for TLS 1.0 and TLS 1.1.

IE11/Edge

OCTOBER 15, 2018 6:35 AM

Modernizing TLS connections in Microsoft Edge and Internet Explorer 11

By Kyle Pflug / Senior Program Manager, Microsoft Edge

SHARE TWEET SHARE SHARE SKYPE

Today, we're announcing our intent to disable Transport Layer Security (TLS) 1.0 and 1.1 by default in supported versions of Microsoft Edge and Internet Explorer 11 in the first half of 2020.

Chrome

In line with these industry standards, Google Chrome will deprecate TLS 1.0 and TLS 1.1 in Chrome 72. Sites using these versions will begin to see deprecation warnings in the DevTools console in that release. TLS 1.0 and 1.1 will be disabled altogether in Chrome 81. This will affect users on early release channels starting January 2020. Apple, Microsoft, and Mozilla have made similar announcements.

Safari

WebKit Blog Downloads Feature Status Reporting Bugs Co

Deprecation of Legacy TLS 1.0 and 1.1 Versions

Oct 15, 2018
by Christopher Wood

This is a guest post from Apple's Secure Transports team about TLS protocol version deprecations. This announcement may require changes for your websites.

TLSプロトコルの比較

	策定	ブロック暗号の 初期ベクトル	CBC モード	AEAD	PRF/MAC
SSL 2.0 SSL 3.0	脆弱性があるため使用禁止				
TLS1.0	1999年	なし	有	なし	SHA1, MD5
TLS1.1	2006年	有	有	なし	SHA1, MD5
TLS1.2	2008年	有	有	有	SHA256以上
TLS1.3	2018年	廃止	廃止	必須	HKDF, SHA256以上

PCI DSS3.1
禁止 2018/6～
ブラウザ
サポート廃止

推奨

常識変化に向き合う#3
「TLS関連の設計が不要に」

昔

HTTPSサーバのTLS設計は、暗号ガイドラインに従って危険なものを除外して、他も危険な設定を残していないかちゃんとチェックしておく。

今

アプリケーションは最新にしてあるし、最新バージョンのTLSも使っているから大丈夫(*)。

(*) ただし古いプロトコルの利用が残っている場合は、古いプロトコル用の設計が必要です。

TLS1.3が求められた背景

1. 常時HTTPS時代を迎えるにあたって、しっかりしたプロトコルが必要
2. TLS1.2の限界
    - 様々な技術負債の蓄積

長期に使えるより安全で高性能なTLSプロトコルを作る

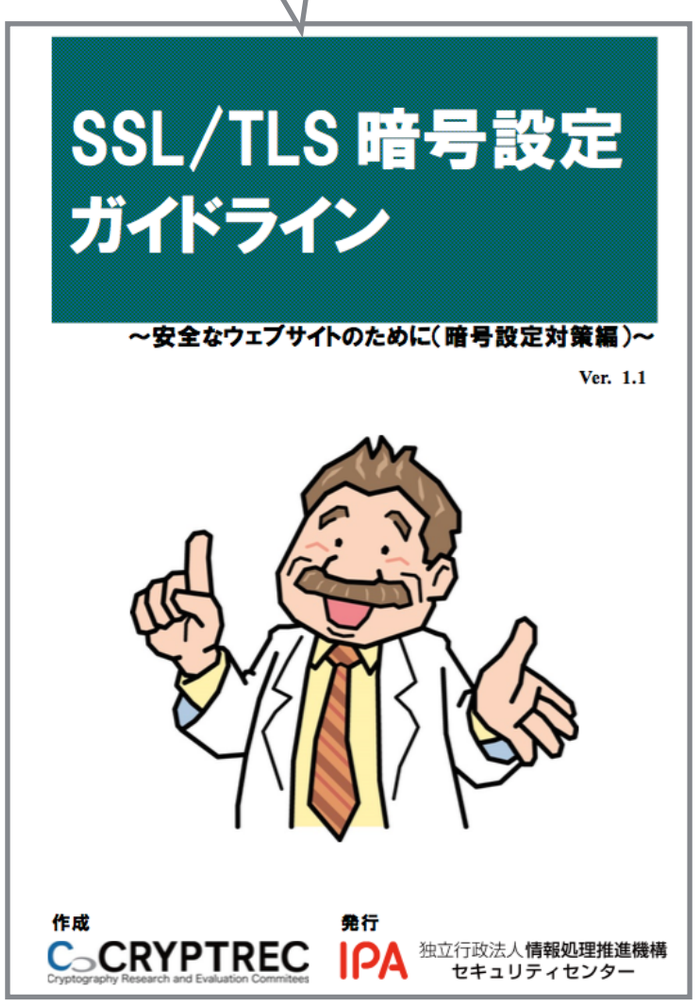
TLS1.2の限界

- 現在のTLS1.2で定義されている機能の一部は、既に利用すると危険である。

- 過去様々なTLSの攻撃手法や脆弱性が公開され、その都度対策が取られてきた。

- しかし一時的な対応で根本的・抜本的な対策になっていないものも多い。

本来このようなガイドラインがなくて済むのが望ましい



https://www.ipa.go.jp/security/vuln/ssl_crypt_config.html

TLS1.3の特徴

1. 様々な機能、項目の見直し・廃止

   時代に合わなくなったもの、より効率的に変更修正できるものをTLS1.2から機能・項目を数多く廃止

2. よりセキュアに

   平文通信が必要な部分を極力少なくして情報を秘匿

   これまで攻撃対象となった機能を極力排除し将来的な攻撃に備える

3. 性能向上

   初期接続の短縮による性能向上

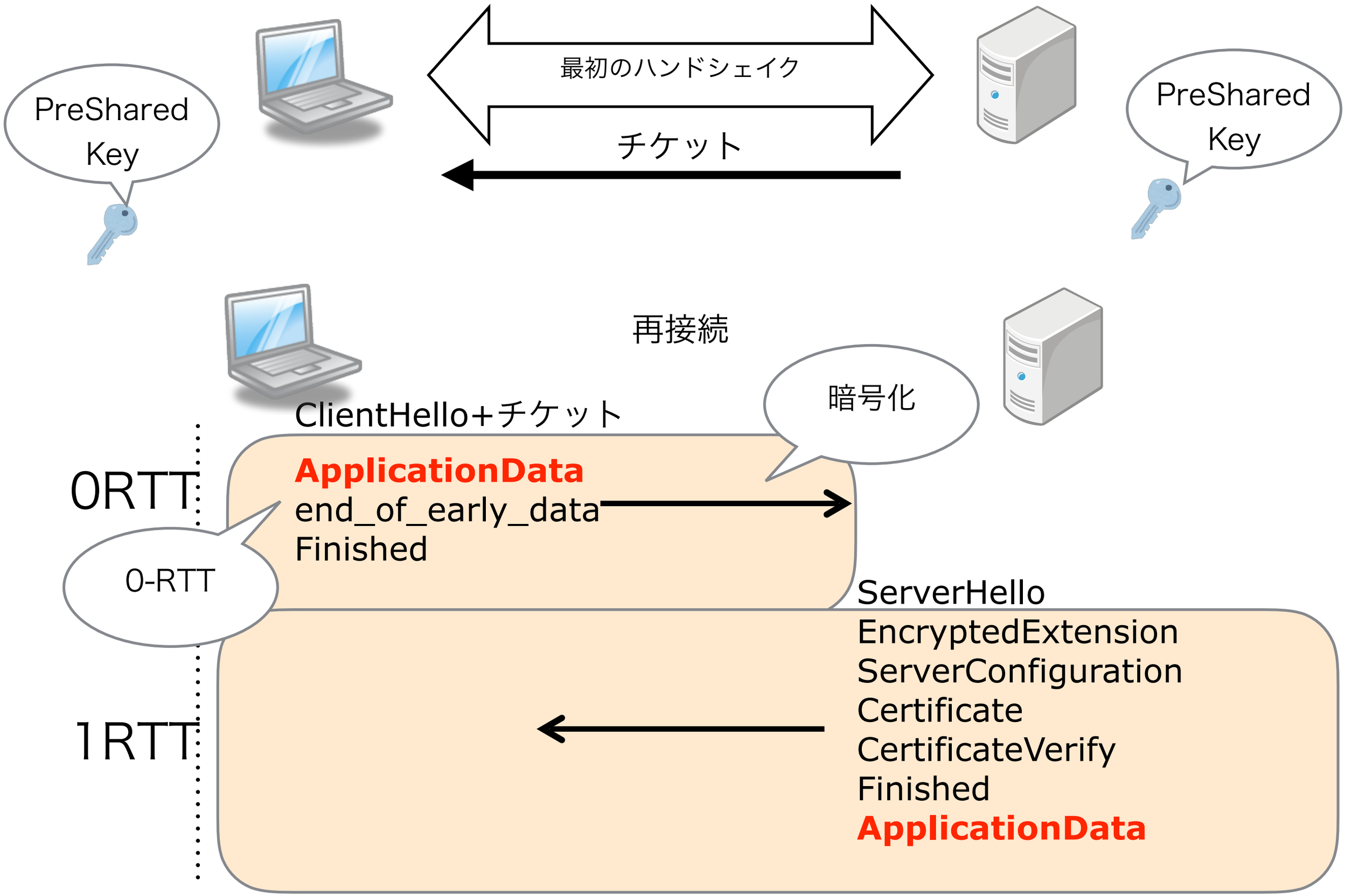
TLS1.3で注意しないといけないこと
0-RTT

- TLS1.3ではハンドシェイク時にPSK(Pre Shared Key)を作成し、再接続時にハンドシェイクとデータを同時に送信する 0-RTT 機能が目玉として定義されている。

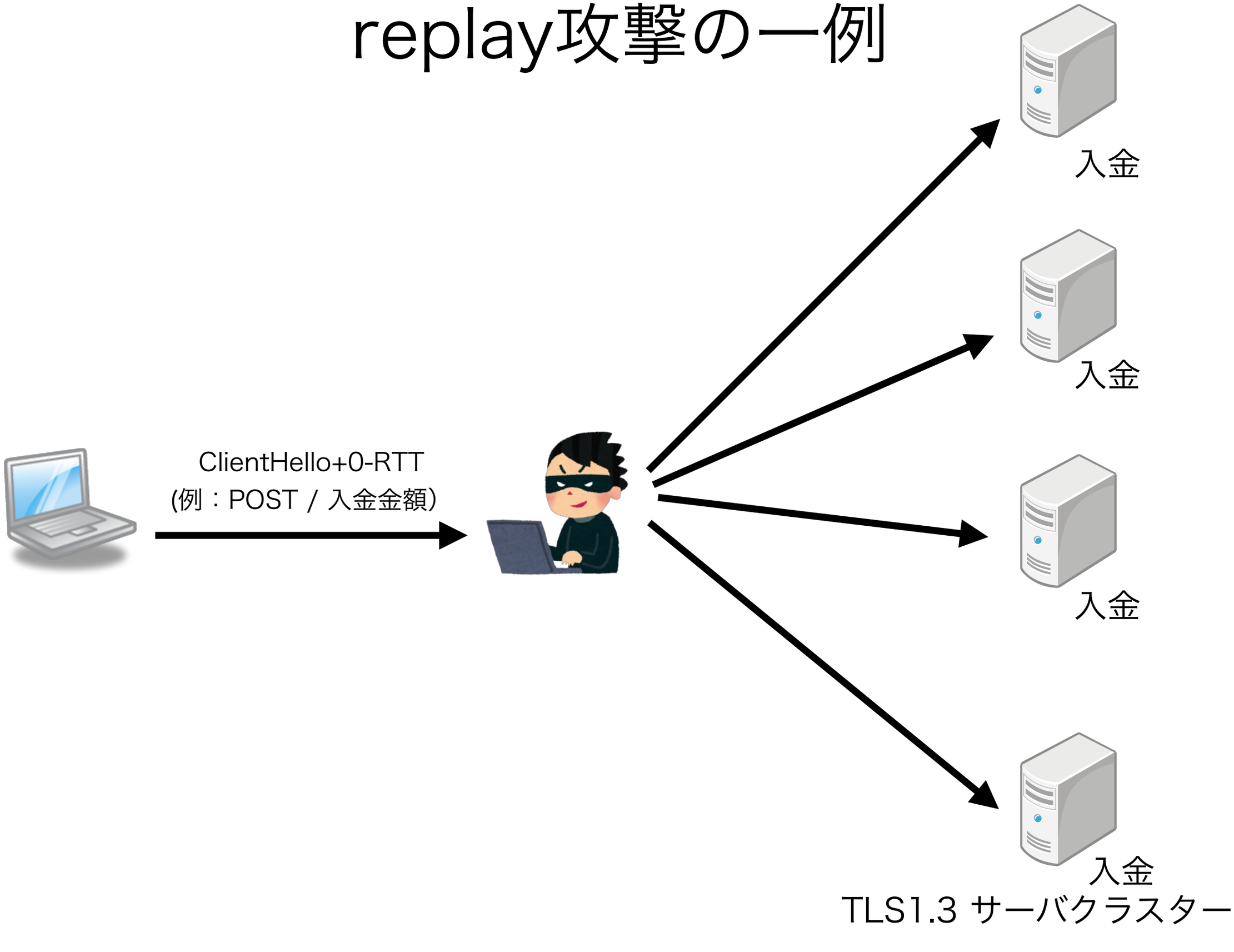
- 0-RTT機能によるデータ通信の高速化が期待されているが、0-RTTのデータを中間攻撃者が複製してサーバに送信するReplay攻撃に弱いという弱点が存在する。

- 0-RTTのreplay攻撃防御の手法としてはHTTPでは冪等性のあるリクエストに限定するといったようにアプリ側の対応が必要になる見込みである。

TLS1.3のハンドシェイク 0-RTT

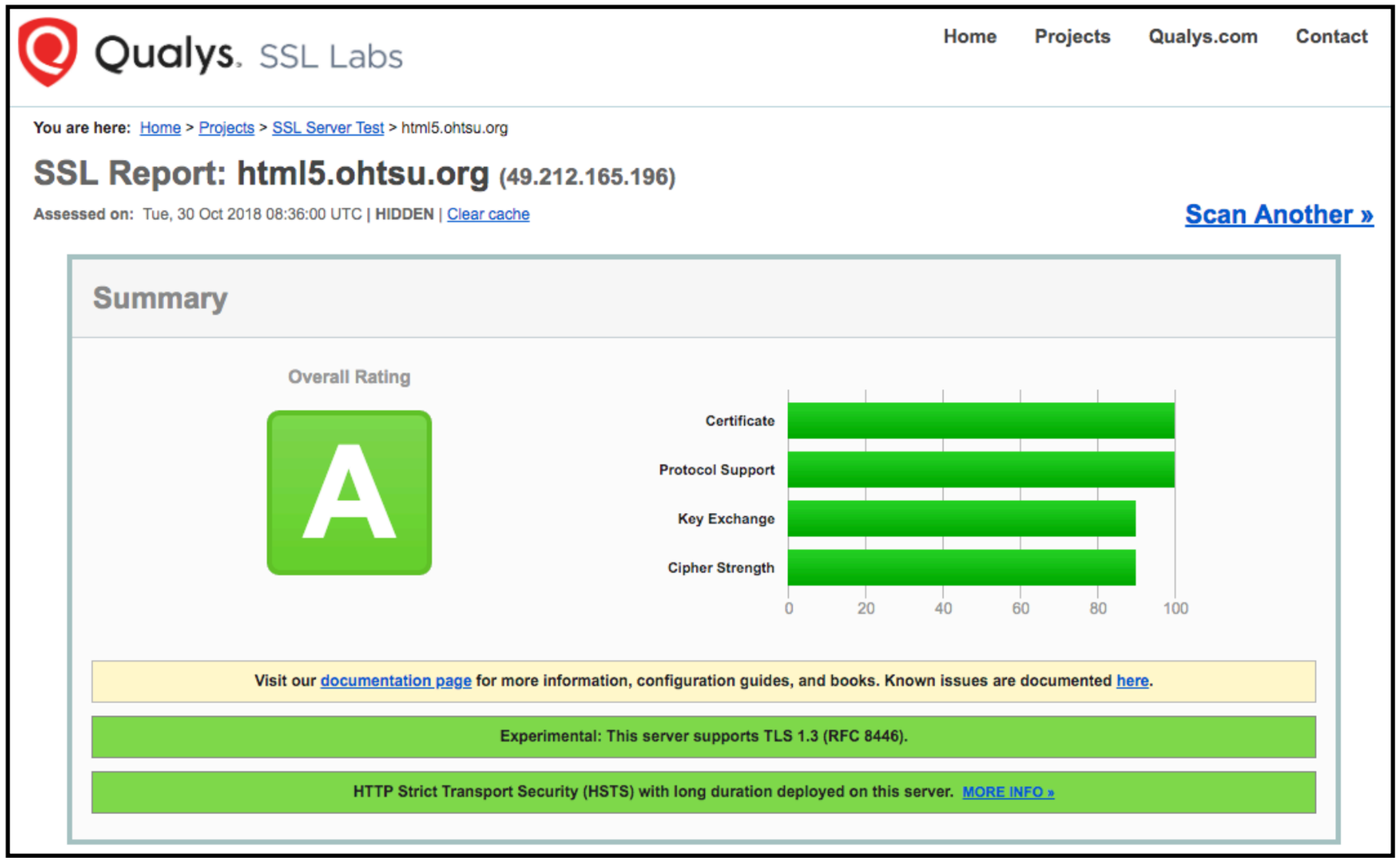


TLS 1.3 0-RTTの脅威
replay攻撃の一例



設計レス

まずは０–RTTを利用せず、TLS1.3にしていれば全て安全



0-RTTの利用は、将来安全に取り扱える環境が整備されるまで待ちましょう。

常識変化に向き合う#4
「HTTPSと通信先の信頼は別」

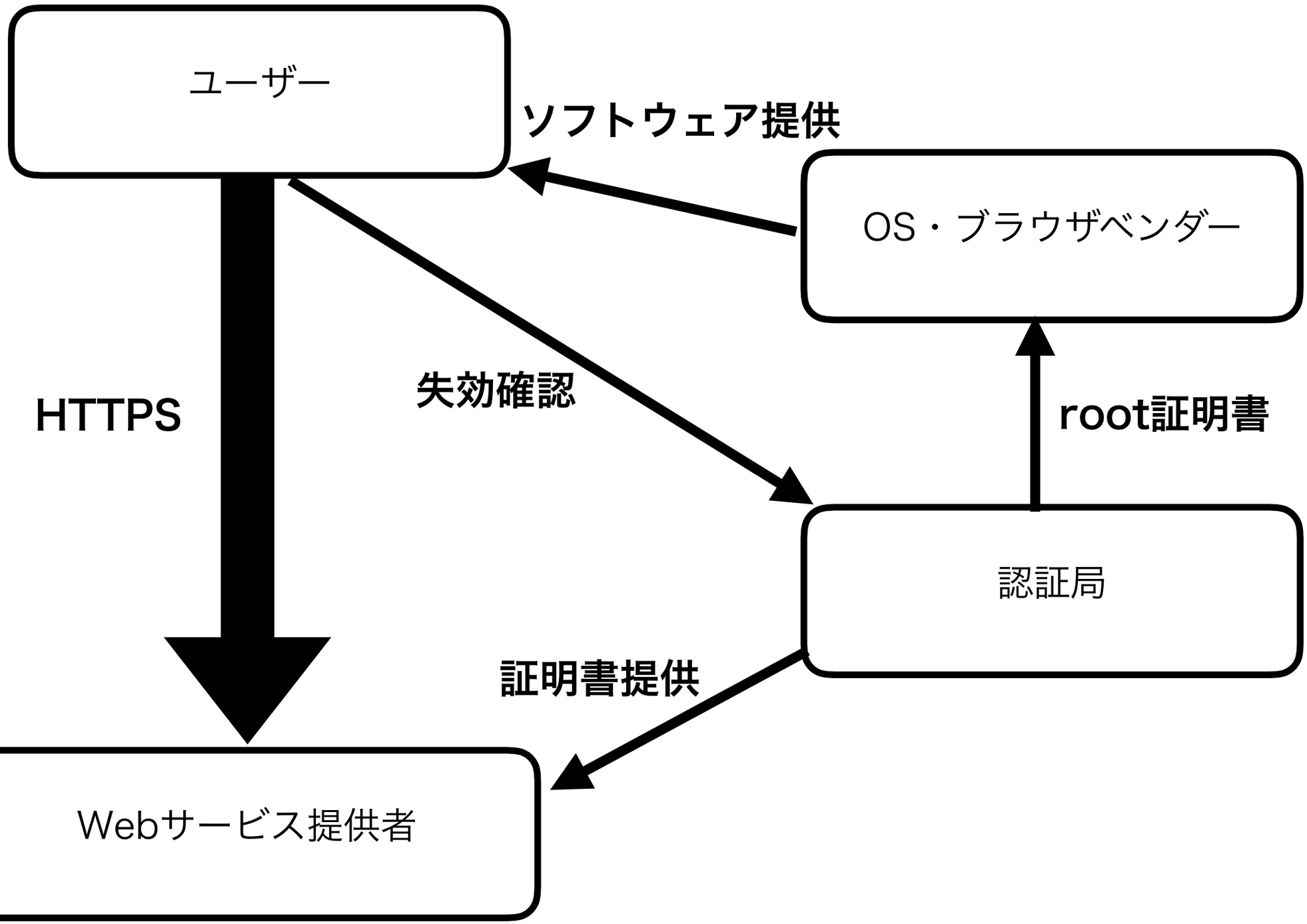
昔

Webブラウザで緑の鍵アイコンだ。HTTPSサイト表示だから信頼できるぞ。

今

詳しくは次の奥田さんの講演で。

HTTPS通信に関連するステークホルダー



HTTPSでは、
証明書の何が検証されるのか？

- サーバ証明書がroot証明書が登録されている認証局発行であること

- 証明書内の記載(期限、用途、失効情報、Certificate Transparency, EVのOID)などが正当なものであること

- アクセス先のホスト名が、証明書のSubject AltNameのリストに登録されていること

HTTPSにおける証明書の検証と信頼は別の話

HTTPSとWebプラウザ表示についてはこの後の発表で