

IETF/W3C/etc De-facto STD Overview (in My Case)

株式会社レピダム 林 達也 (@lef)
HAYASHI, Tatsuya / Lepidum Co. Ltd.
IETF標準化セミナー
(2015/3/11)



Speaker's Position



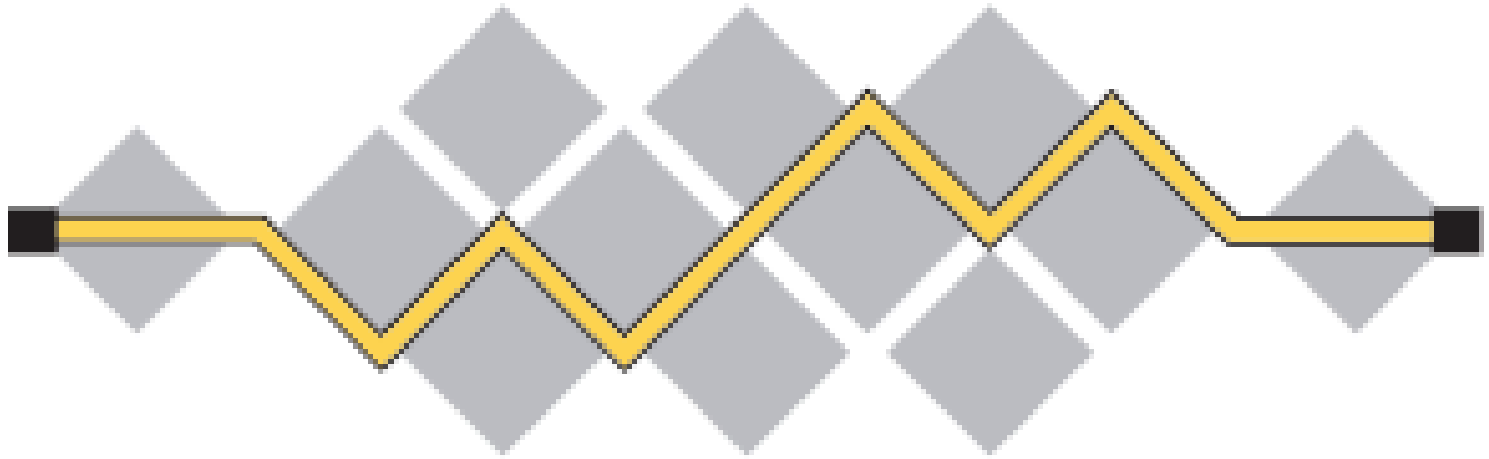
- Lepidum Co. Ltd. (<https://lepidum.co.jp/>)
 - President, Founder and Owner
- Internet Society Japan Chapter
 - Online Identity Working Group Chair
 - Program Committee Member (2013-2015)
- OpenID Foundation Japan
 - Executive Director
- Identity Conference (#idcon)
 - Organizer
- Keio University
 - Visiting Researcher, Keio Research Institute at SFC



World Wide Web Consortium



Internet Engineering Task Force



I E T F[®]



De-facto STD Overview

ABOUT HTTP/2



HTTP/1.1

```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 06 Mar 2013 03:41:55 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
Set-Cookie: CG=US:TX:San+Antonio; path=/
Last-Modified: Wed, 06 Mar 2013 03:41:03 GMT
Vary: Accept-Encoding
Cache-Control: max-age=60, private
Expires: Wed, 06 Mar 2013 03:42:48 GMT
Content-Encoding: gzip
```



HTTP/2



HTTP/2

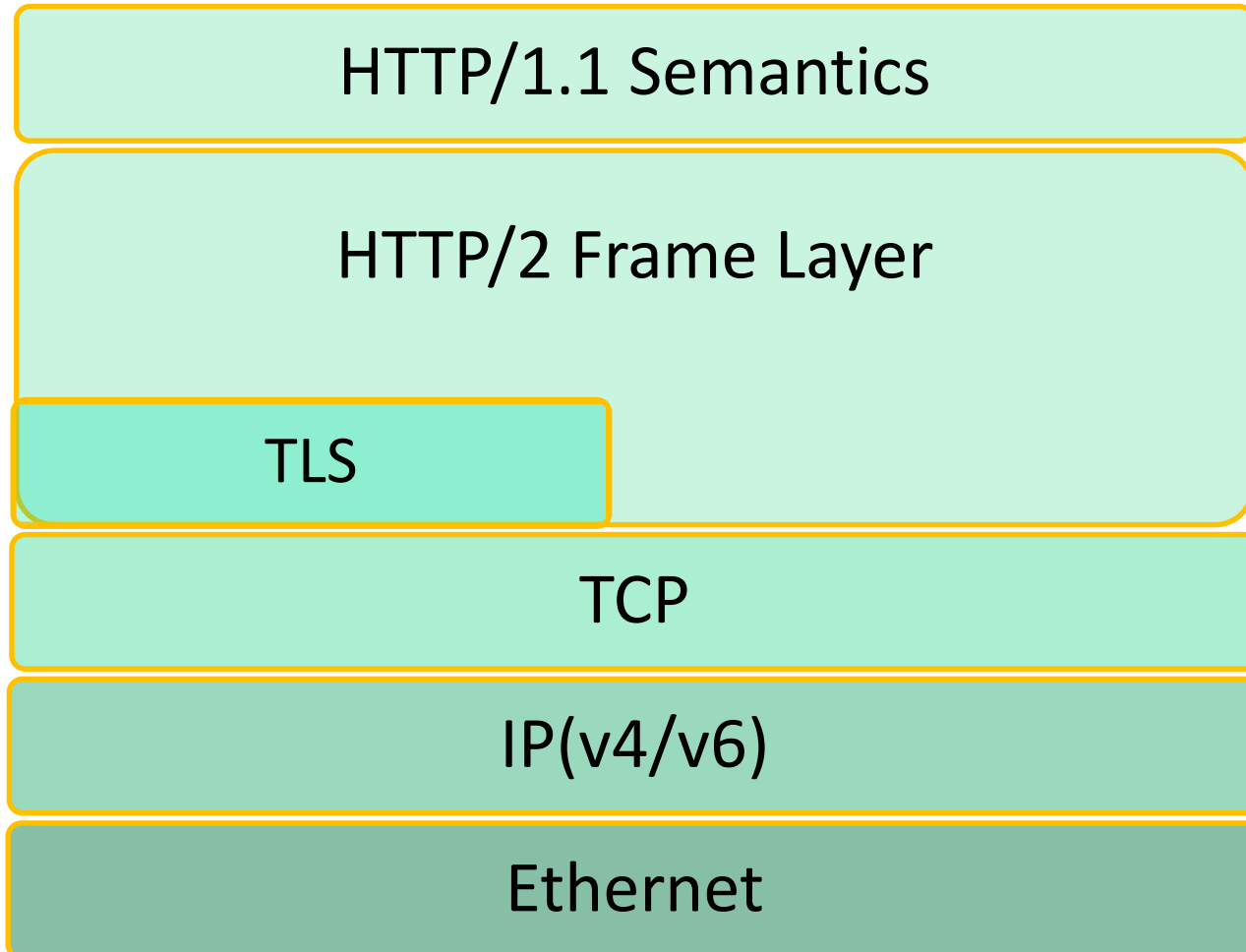
Silent, but **Huge** change
in the world of the Web



- Motivation
 - Efficient network resource usage
 - Performance improvement in any environment
 - Modern security requirement
- Among several proposal, SPDY is chosen as a draft of HTTP/2 discussion
- Now standardization in IETF httpbis Working Group



HTTP/2 Protocol Overview



Difference from HTTP/1.1 to HTTP/2

- Text to Binary
- Header Compression
- Multiplexing
- Prioritizing
- Connection Start Process
- Use policy of TCP Connection
- etc...



Contributors (a part of...)

Google

 Microsoft

 Akamai

Canon



from "HTTP/2.0: Challenges and Opportunities
Mark Nottingham (@mnot)"

<http://www.mnot.net/talks/http2-challenges/#/4>



Roadmap

- | | | |
|------------|----------------|---------------------|
| ■ Mar 2012 | IETF83 | - Paris, France |
| ■ Jul 2012 | IETF84 | - Vancouver, CA |
| ■ Nov 2012 | IETF85 | - Atlanta, US |
| ■ Jan 2013 | Interim | - Tokyo, JP |
| ■ Mar 2013 | IETF86 | - Orlando, US |
| ■ Jun 2013 | Interim | - San Francisco, US |
| ■ Jul 2013 | IETF87 | - Berlin, DE |
| ■ Aug 2013 | Interim | - Hamburg, DE |
| ■ Oct 2013 | Interim | - Seattle, US |
| ■ Nov 2013 | IETF88 | - Vancouver, CA |
| ■ Jan 2014 | Interim | - Zurich, CH |
| ■ Mar 2014 | IETF89 | - London, UK |
| ■ Mar 2014 | Interim | - London, UK |
| ■ Jun 2014 | Interim | - New York, US |
| ■ Jul 2014 | IETF90 | - Toronto, CA |
| ■ Nov 2014 | IETF91 | - Honolulu, US |



about
3 years



De-facto STD Overview

ABOUT SPDY AND QUIC (HTTP/2 BACKGROUND)



SPDY

- Real world deployment.
 - Google, Facebook ,Twitter, etc...
 - Chrome(Chromium),
Firefox, Opera, IE11, etc...
 - Jetty, Apache, nginx, etc...
- Source of Next Web Protocol (HTTP/2, QUIC)
- Mandatory Encryption(TLS/HTTPS)
- SPDY4 $\doteq$ HTTP/2
- SPDY5? = Next SPDY?



Why do we get a SPDY?

Mobile
Friendly

Optimization

Fast

Quick



Why now HTTP/2 ?

Interoperability

More
Optimization

Standard

Implementation



What is happening Now ?

Vulnerability
(CRIME, HeartBleed)

Header
Compression

HPACK

Pervasive Monitoring
(PRISM)

End to End
Encryption

Perfect
Forward
Secrecy

Challenge
(SPDY, HTTP/2, QUIC)

Max
Optimization

Mandatory
Encryption



QUIC: "Quick UDP Internet Connections"

- New UDP Base transport layer protocol
- Implemented Chrome(and Chromium)
- Real world deployment. but Google only
- main use: SPDY over QUIC
- TCP and TLS layer replacement
- Userland Impl.
 - Not Kernel mode, Not Network Stack
- QUIC project is cloaked...
 - "Quick UDP Internet Connections Multiplexed Stream Transport over UDP" in IETF88 tsvarea
 - Chromium source code
 - blog article, design doc, etc...



Cite: "Experimenting with QUIC" from Chromium blog

- "High security similar to TLS"
- "Fast (often 0-RTT) connectivity similar to TLS Snapstart combined with TCP Fast Open"
- "Packet pacing to reduce packet loss"
- "Packet error correction to reduce retransmission latency"
- "UDP transport to avoid TCP head-of-line blocking"
- "A connection identifier to reduce reconnections for mobile clients"
- "A pluggable congestion control mechanism"



What is happening Future ?

More Optimization !

- QUIC
- etc...

More Security !

- HTTPS, TLS 1.3
- etc...

More Function !

- Server Push, Flow Control
- Priority Forest
- etc...



De-facto STD Overview

DE-FACTO / FORUM STD ACTIVITY EXAMPLE



De-Facto / Forum STD Body (My Case)

- Internet Engineering Taskforce (IETF)
- World Wide Web Consortium (W3C)
- Internet Society / Internet Society Japan Chapter
 - ISOC-JP Program Committee (2013-2015)
 - ISOC-JP Online Identity Working Group
- OpenID Foundation / OIDF Japan



Protocols

- WebSocket
- WebRTC
- HTTP/2
- OAuth2
- OpenID Connect
- etc...



My Step

• HTTP Mutual Authentication [IETF]

• OAUTH [IETF]

• OpenID Connect [OIDF]

• [#idcon]

• [OIDF-J]

• [W3C]

• HTTPAUTH [IETF]

[ISOC-JP]

• HTTP/2 [IETF]

• [#http2study]

WEBPUSH, JOSE,
etc...

