~~JANOG40 LightnigTalk~~

JANOG BoF & LT Night #2

国産CDNのSSL負荷対策

2017/09

株式会社Ｊストリーム
CDNext推進室　佐藤 太一

© J-Stream Inc. All Rights Reserved.

自己紹介（佐藤 太一）

- 経歴
  - 1980/09　山口県光市　生
  - 2003/03　鹿児島大学　卒
  - 2003/04　Jストリーム（AS24253）に入社
    ～新卒で入社してそのまま、現在も在籍

- 業務内容
  - セールス兼インフラエンジニア
  - CDNのインフラ全般の構築・運用・管理
  - CDN情報サイト：　https://tech.jstream.jp/

- その他
  - インターネットコミュニティ活動も積極的に実施中
    JANOG36@北九州　LAスタッフ,LightLightnigTalk登壇
    JANOG37@名古屋　LAチェア
    JANOG38@沖縄　　実行委員長
  - 趣味：楽器(ファゴット)

© J-Stream Inc. All Rights Reserved.

常時SSL化の状況

※本資料ではSSL/TLSをまとめてSSLとして表記しています

© J-Stream Inc. All Rights Reserved.

常時SSL(AOSSL)とは？

- WebサイトのHTTPサイトを閉鎖しHTTPSのみで閲覧可能にする事
  - HTTPの接続はHTTPSへのリダイレクトのみ許可
  - HSTS(HTTP Strict Transport Security)とかもありますね
- AOSSLとも言います
  - Always on SSL
- 大手Webサイトは軒並み対応済
  - Google,Youtube,Facebook,Twitter 他
  - 米国連邦機関の全サイトをSSL化済
  - Yahoo! Japanは2017/3月末までに完了
    - https://about.yahoo.co.jp/info/aossl/

© J-Stream Inc. All Rights Reserved.

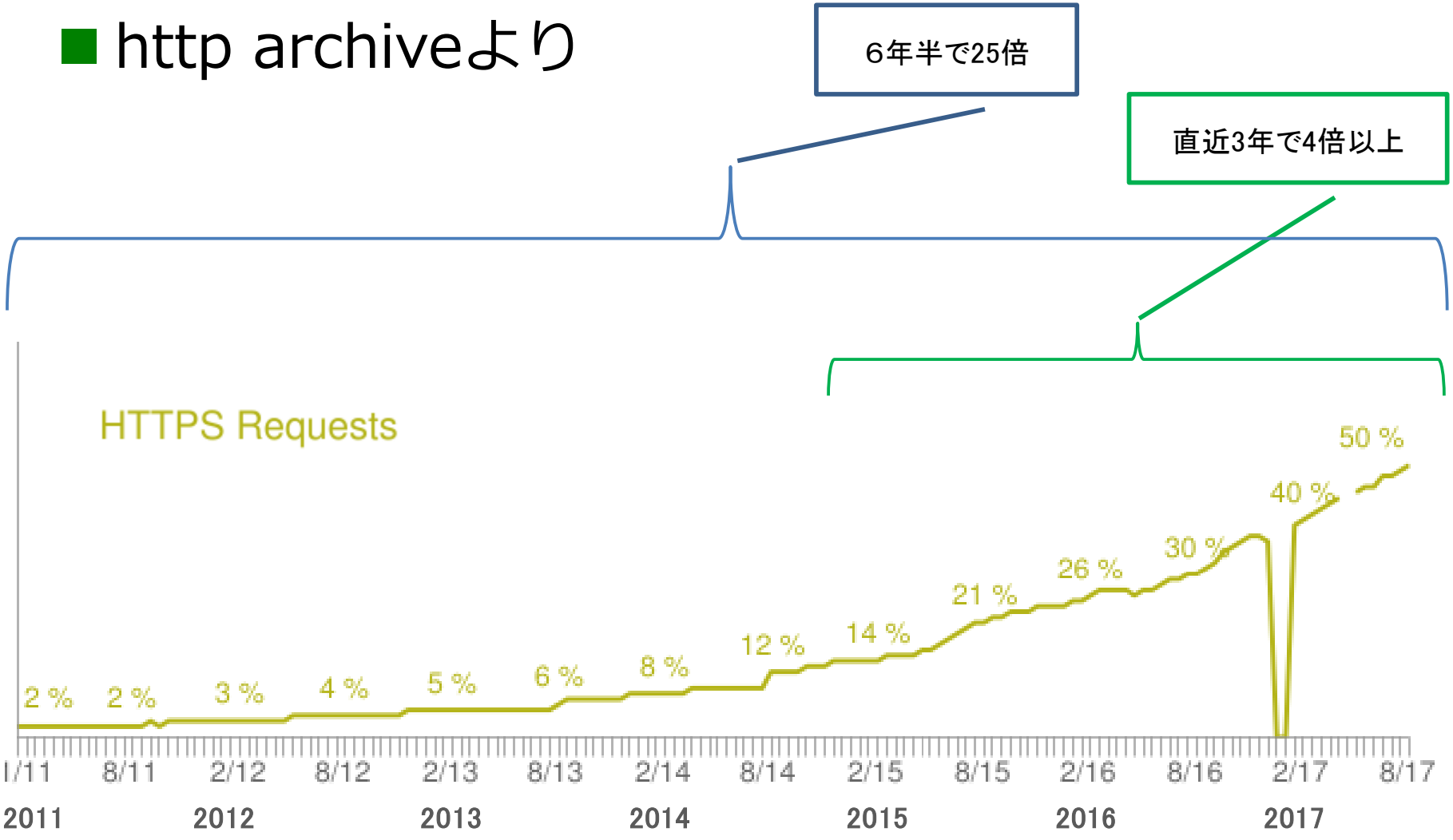
なぜ常時SSL化するのか？

- ユーザー保護
  - フリーWifiスポット等で万が一情報を盗み見られた場合でも、せめて自社のWebサイトへアクセスしてきたユーザーの通信は守れるように
- マーケター視点
  - SEO対策(常時SSL化がランクアップ要素に)
  - リファラ取得(https->httpサイトに遷移時はリファラ情報が取れない)
- Webサイト表示高速化
  - HTTP/2を利用するためにはSSL化が必須
  - HTTP/2にすると、概ね10%～20%の表示速度UP
- ATS(App Transport Securiy)対応
  - iOS9以降のiOSアプリ内通信は基本的に全てSSLで
  - TLS1.2+ Forward Secrecy必須

© J-Stream Inc. All Rights Reserved.

で、実際のところどうなの？ (Global ①)

- http archiveより



http://httparchive.org/trends.phpより

© J-Stream Inc. All Rights Reserved.

で、実際のところどうなの？ (Global ②)

- Alexaランキング Top 50 (Global) の常時SSL対応状況 **76%**

	FQDN	常時SSL	status
1	www.google.com	on	302
2	www.youtube.com	on	301
3	www.facebook.com	on	301
4	www.baidu.com	off	○
5	www.wikipedia.org	on	301
6	www.yahoo.com	on	301
7	www.reddit.com	on	301
8	google.co.in	on	302
9	www.qq.com	off	×
10	www.amazon.com	on	301
11	world.taobao.com	on	301
12	www.google.co.jp	on	301
13	twitter.com	on	301
14	www.tmall.com	on	301
15	vk.com	on	302
16	login.live.com	on	301
17	www.instagram.com	on	301
18	www.sohu.com	off	○
19	www.sina.com.cn	off	○
20	www.jd.com	off	○
21	weibo.com	off	○
22	www.360.cn	on	301
23	www.google.de	on	302
24	www.google.co.uk	on	302
25	www.google.ru	on	302
26	www.google.fr	on	302
27	google.com.br	on	302
28	www.linkedin.com	on	301
29	list.tmall.com	on	301
30	www.google.com.hk	on	302
31	www.yandex.ru	on	302
32	www.netflix.com	on	302
33	www.google.it	on	302
34	www.yahoo.co.jp	on	301
35	www.google.es	on	302
36	t.co	off	○
37	www.pornhub.com	on	301
38	www.ebay.com	on	301
39	imgur.com	off	○
40	www.google.ca	on	302
41	www.twitch.tv	on	301
42	www.alipay.com	on	301
43	www.google.com.mx	on	302
44	www.bing.com	off	○
45	www.xvideos.com	off	○
46	www.youth.cn	off	○
47	www.msn.com	off	○
48	www.tumblr.com	on	301
49	www.aliexpress.com	on	301
50	ok.ru	on	301

で、実際のところどうなの？ (Japan)

- Alexaランキング Top 50 (Japan) の常時SSL対応状況

66%

No	FQDN	常時SSL	status
1	www.google.co.jp	on	301
2	www.google.com	on	302
3	www.youtube.com	on	301
4	www.yahoo.co.jp	on	301
5	www.amazon.co.jp	on	301
6	www.nicovideo.jp	off	×
7	twitter.com	on	301
8	www.facebook.com	on	301
9	www.rakuten.co.jp	on	301
10	fc2.com	on	301
11	www.wikipedia.org	on	301
12	t.co	off	○
13	kakaku.com	off	×
14	ameblo.jp	on	301
15	2ch.net	off	○
16	www.baidu.com	off	○
17	www.livedoor.com	off	×
18	matome.naver.jp	on	301
19	hatenablog.com	off	×
20	blog.jp	off	×
21	www.livedoor.com	off	×
22	www.goo.ne.jp	on	301
23	github.com	on	301
24	www.amazon.com	on	301
25	www.hatena.ne.jp	off	○
26	www.instagram.com	on	301
27	www.qq.com	off	×
28	www.dmm.co.jp	off	○
29	www.microsoft.com	on	301
30	www.chatwork.com	off	○
31	login.live.com	on	301
32	www.apple.com	on	301
33	qiita.com	on	301
34	tabelog.com	on	301
35	world.taobao.com	on	301
36	www.weblio.jp	off	○
37	www.xvideos.com	off	○
38	www.pornhub.com	on	301
39	www.yahoo.com	on	301
40	www.reddit.com	on	301
41	www.post.japanpost.jp	off	○
42	www.tmall.com	on	301
43	www.msn.com	off	○
44	stackoverflow.com	on	301
45	www.buyma.com	on	301
46	www.doorblog.jp	on	301
47	www.tumblr.com	on	301
48	www.nikkei.com	on	301
49	www.office.com	on	301
50	sakura.ne.jp	on	301

で、実際のところどうなの？(Jストリーム)

- Jストリームのhttp/httpsトラフィック比率
  - ATSの影響で動画(HLS)も軒並みHTTPsに
  - 今年に入ってWebサイトの常時SSL化をしたいという問い合わせが急に増えた印象（体感値）
    - 顧客カスタムドメイン/持込SSL証明書なら、追加料金がからない
  - 具体的な数値は口頭のみでm(_ _)m

© J-Stream Inc. All Rights Reserved.

ＪストリームのSSL負荷対策

※本資料ではSSL/TLSをまとめてSSLとして表記しています

© J-Stream Inc. All Rights Reserved.

JストリームのSSL負荷対策　要点

- ロードバランサにSSL処理をさせない
  - LBのCPUでやっていたら追いつかないのでサーバ側で処理させる
  - L3 DSR(Direct Server Return)を積極利用
- Webサーバ側での対応
  - ChiperSuiteの優先制御(Server preferredモード)
  - HTTP/2 onによる負荷軽減
- ハードウェアの力を借りる
  - Intel Quick Assist Adapter(QAT)

© J-Stream Inc. All Rights Reserved.

ロードバランサにSSL処理をさせない

- LBのCPUでやっていたら追いつかないのでサーバ側で処理させる
  - SSL高性能なLBはスケールさせにくい。サーバー増設のほうが導入・運用・保守コストパフォーマンスが良い　＝　LBのSSLアクセラレータはコストパフォーマンスが悪い
  - そこに余っているCPUがあるのになぜ使わない！？
- L3 DSR(Direct Server Return)を積極利用
  - SSLに限らず、通常の通信もですが・・・
  - Ｊストリームは10年以上、L3 DSRです

© J-Stream Inc. All Rights Reserved.

Webサーバ側でのカスタマイズ

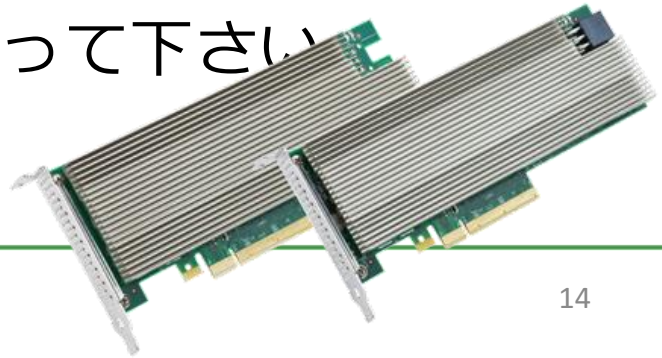
- ChiperSuiteの優先制御(Server preferredモード)
  - OpensslにはSSLv3/TLS利用時、サーバ側が示したChiperSuiteを優先して適用される事が出来る
  - 優先順位も指定する事が可能
  - 適切な暗号強度を持った中でサーバCPU負荷が低いものを選んで、クライアントに掲示を行う
  - DHEよりECDHE

- HTTP/2 onによる負荷軽減
  - セッションを張る部分（ネゴシエーション部分）でCPUコストが一番かかる
  - １度セッション張ったら、中で適当に処理してくれるHTTP/2の方がCPUコストを下げる事が出来る
  - Webサイトの場合は表示速度改善にも貢献

© J-Stream Inc. All Rights Reserved.

ハードウェアの力を借りる

- Intel Quick Assist Adapter (QAT)
  - 昔良く見かけたサーバにincludeするタイプのハードウェアSSLアクセラレータ
  - 適切にセッティングすると、SSL負荷の部分をそれなりにオフロード出来る
  - チップ的にはIntel,caviumが２強？
  - Intelの次期サーバ向けチップセット(Purley、ハイエンド向けのみ)に同機能が内蔵されると告知あり
  - 現在、絶賛開発中
  - 詳細はQAT intel Purley等でググって下さい



© J-Stream Inc. All Rights Reserved.

www.stream.co.jp

CDNext推進室　佐藤 太一

© J-Stream Inc. All Rights Reserved.