ストリーミングのTLS(SSL)化
JANOG 35.5

2015年4月17日

鍋島　公章
株式会社Jストリーム

Rev9:20150416

自己紹介

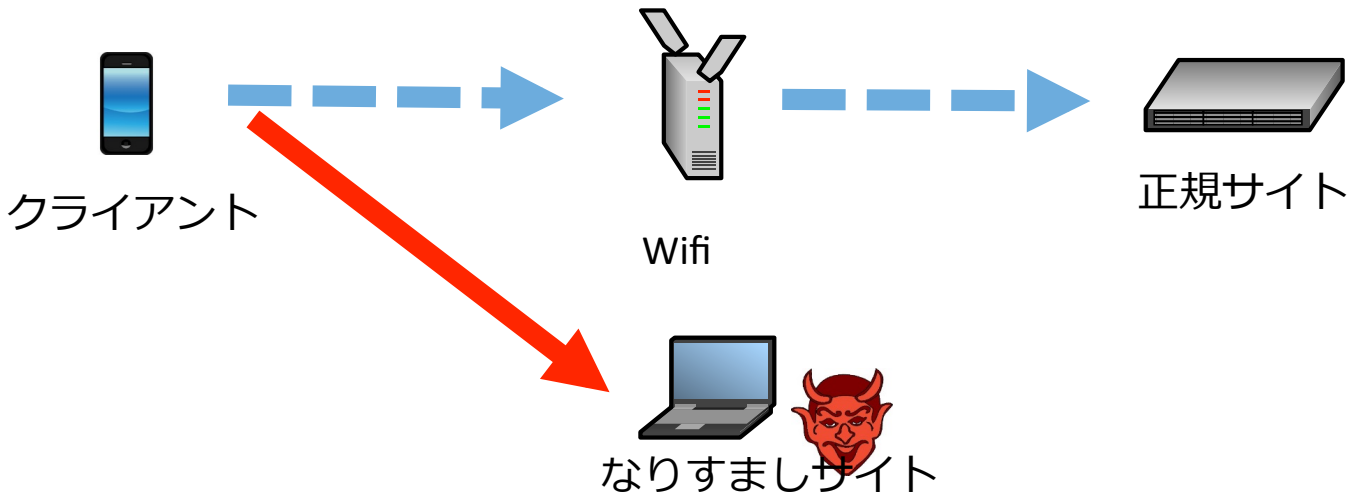
- 鍋島　公章
  - 配信屋（CDNのみならずライブチャットからデジタルシネマまで）
  - 株式会社Ｊストリーム（国産CDNを作っています）
- 過去のJANOGプレゼンテーション
  - JANOG 1
    - 大規模WWWキャッシュサーバについて
  - JANOG 3
    - Proxy Cacheを透かして見た風景～透過型 Proxy Cache による影響～
  - JANOG 30
    - スマートフォン時代のコンテンツ配信とトラフィック取引

はじめに

- ビデオストリーミング
  - 2018年には全トラフィックの75%を占めると予想される
    - 出典：Cisco VNI Service Adoption Forecast 2013–2018 White Paper
  - 現在、HTTP化さらにはTLS化が進行中
    - ネットワークオペレータにも影響あるはず←発表の動機
- 目次
  - 復習：TLS
  - ストリーミングのHTTP化
  - ストリーミングのTLS化
  - 影響の考察

復習:TLSへのニーズ（サイトのなりすまし）

- モバイル（Wifi）環境は危険
  - **サイトのなりすまし**、盗聴
    - 中間者攻撃(ARP Poisoning, ICMP Redirect)



復習：企画屋、マーケター視点の動向

- 主要サイト（既に常時SSL化済）からのリファラ取得不可
  - HTTPの規定(HTTPSサイトからHTTPサイトに移動した時にはリファラを付けない)
- 2014年8月：Google検索のランクダウン
- 2014年9月：無料SSL CDNの登場
  - 制約あり（SNI+ECC）
- 2015年1月：Chromeベータ版
  - 非HTTPSサイトを危険なサイトとして表示するオプションを追加

- 2015年：SSL証明書の無料化（現状でも数千円/年程度）
  - 2015年中には無料発行組織が発足

復習：技術屋志向の動向

- HTTP/2ではTLS必須に（実装上）
  - “HTTP://～”のブラウザ実装は未定

	プロトコル選択	ブラウザ実装
HTTP://～	HTTP/1.1 Upgrade	？（実装されるか未定）
HTTPS://～	TLS拡張（NPN、 ALPN)	Chrome 40，Firefox 36，IE11 on Windows 10

- TLS運用は大変
  - 安全でない環境の切捨て判断
  - IPアドレスの不足
  - サーバ負荷の増加
  - 脆弱性への対応

復習：TLS比の動向

- 常時SSL
  - HTTPサイトを閉鎖（HTTPSへのリダイレクトのみ許可）HTTPSのみとする
    - Google、Facebook、米国主要銀行等
- 普及率

指標	状況
SSLサイト率（グローバル）	約13%（過去2年間で2.6倍）
上位5銀行	米国（すべて常時SSL化済み） 日本（4社がSSLエラー）
日本のTOP20サイト	約半分はSSLエラー（未対応）

SSLサイト率 出典：http://httparchive.org

ここから本題

- TLSトラフィック比率（流量ベース）
  - 北米
    - 固定19%、モバイル26%+α　（鍋島調べ、詳細は後で）
  - 国内
    - 公表されている資料なし（JANOGな方には既知でしょうが）
      - たぶん北米と同じぐらい？
      - 非公式な場所では、いろいろ聞きます
        - HTTPトラフィックの半分ぐらいがTLS？
        - TLSトラフィック比率30%？
- TLSトラフィックの急激な増加は、ストリーミングのTLS化が原因
  - ストリーミング屋として、この背景を説明します
    - ただし、国内ではまだストリーミングのTLS化は始まっていません、国内ストリーミング屋のグローバルな動向に対する考察です

動画のHTTP化

- 専用プロトコルは先細り

方式	状況	補足
Real Media	×	サーバビジネスから撤退（2015年）
Windows Meida (mms)	×	SilverLightへ移行、 WMT DRM (WS2003)終了
Flash Media (rtmp)	↓	PC向けでは全盛だが、Android、 iOSでFlash Playerは動かない

- HTTPへの移行
  - 専用プロトコル
    - Apple HLS↑、Microsoft Smooth Streaming (SilverLight)→、Adobe HDS↓
  - 標準プロトコル(Apple除く）
    - MPEG-DASH

ブラウザの対応状況

▶対応状況（2015年4月暫定版）

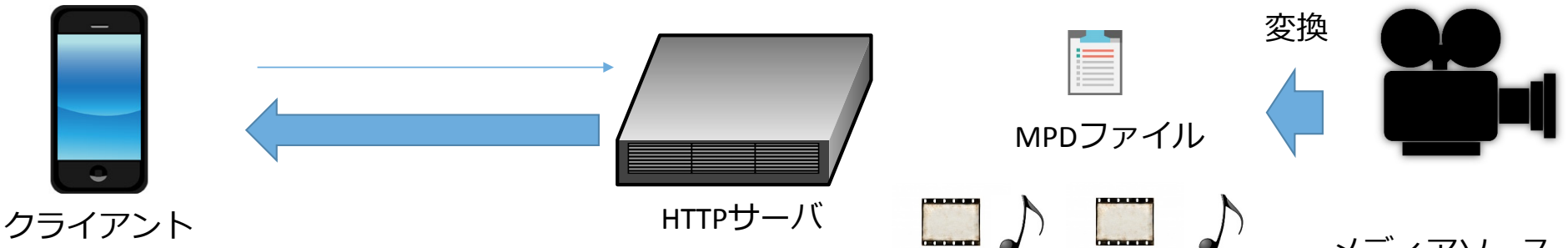
OS	ブラウザ	Apple HLS	MPEG-DASH
Windows 7	IE	×	×
	Chrome	×	○
	Firefox	×	×
Windows 8.1	IE	×	○
	Chrome	×	○
	Firefox	×	×
MacX	Safari	○	○
	Chrome	×	×
	Firefox	×	×
iOS	Safari	○	×
Android4.4	Chrome	○	○

MPEG-DASH

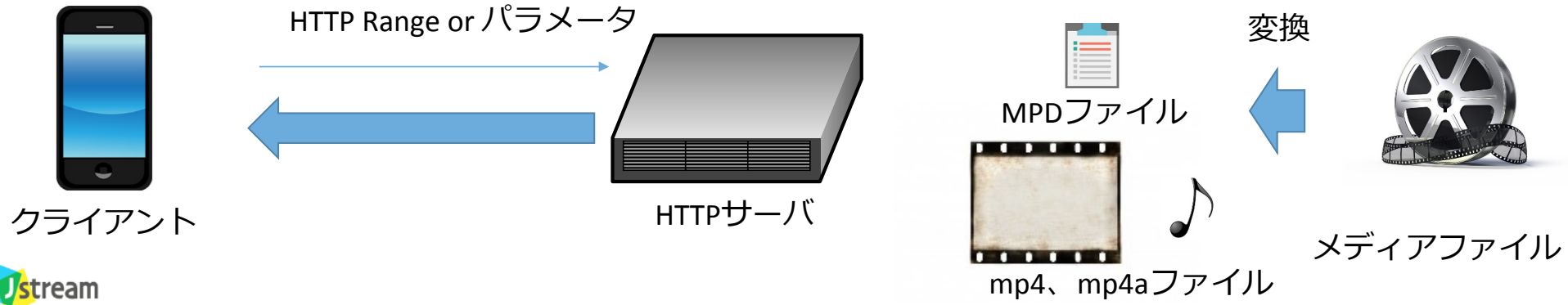
- Dynamic Adaptive Streaming over HTTP
  - 特徴
    - 旧来のアドホックなHTTPクローキング・プログレッシブダウンロードでない
    - HTTPできちんとストリーミング
      - クライアント側でいろいろ操作
    - 機能
      - オンデマンド、ライブ、タイムシフト
      - アダプティブビットレート
      - 映像、音声トラックの動的切り替え（例：英語、日本語切替）
      - 広告挿入
      - 字幕対応

MPEG-DASH

- ライブ



- オンデマンド



MPEG-DASH

- 配信へのインパクト
  - 普通のWebサーバで動画配信可能
    - サーバライセンス不要
    - ストリーミングサーバより高性能（負荷対策はWeb用CDN）
      - サーバ1台でＸ～Ｘ0Gbps程度は配信
  - MPD、mp4ファイルはHTTPキャッシュ可能
    - 付加機能
      - ライブのスプリット、ライブのタイムシフト再生
    - ライブスプリッタの展開が容易に
      - オンデマンドサーバのX倍のパフォーマンス
        - オンメモリキャッシュ

MPEG-DASH

- ＣＰ側の組織内（含むISP）キャッシュへの対応
  - 組織内キャッシュで複製されるのはＣＰ・配信屋としては困る

項目	補足
高付加価値の無償提供	タイムシフト再生
売り上げ減（配信屋）	配信量の減少
CPのCDNキャッシュ展開を阻害	コンテンツ・コントロール権の維持

  - ＣＰ側のキャッシュ不可指定
    - ワンタイムURL
    - Cache-Controlでキャッシュを禁止

復習：HTTPプロトコル (RFC2616)

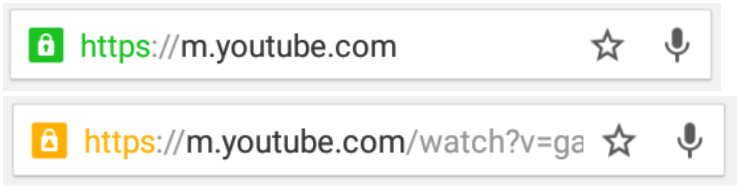
- Cache Control
  - Public
    - MAY be cached by any cache
  - **Private**
    - **MUST NOT be cached by a shared cache**
  - No-Cache
    - MUST NOT use the response to satisfy a subsequent request without successful revalidation
  - No-store
    - MUST NOT store any part of either this response or the request

参考：著作権法（文化庁、文部科学省）

- H21年の改正（複製してよい範囲を拡大）
  - 第４７条の５：送信の障害の防止等のための複製
    - 配信側におけるミラー、バックアップ、CDN化等
      - 明示的に許可
    - ISP側における複製（キャッシュサーバ）
      - 法文の解釈として許可
  - HTTP Cache-Controlを無視するようなISPキャッシュ
    - 著作権侵害だと思われる（鍋島意見）
  - ISP側におけるコンテンツ改変
    - 著作権侵害だと思われる（鍋島意見）

動画のTLS化

- 背景
  - HTML5
    - 動画再生もブラウザ単体で完結
  - HTTPSサイトにおいて動画コンテンツをHTTP（非HTTPS）で配信するとワーニング表示
    - トップページ
    - 再生ページ



- TLS化のニーズ
  - 前記ワーニングの解消
  - コンテンツ保護は別のストーリー（ブラウザのEncrypted Media Extensions）
    - TLS化されていても各種ツールで動画のダウンロード可能
    - 組織内キャッシュ等によるコピー回避は可能

動画のTLS化

- ストリーミングのTLSサーバ運用
  - 基本的に、通常サイト用のTLS CDNと同じく各種負荷が増加
  - サーバ負荷の目安

対象		負荷増加
通常配信（ショートコンテンツ）		10倍
ストリーミング配信	普通のチューニング	数倍ぐらい
	カーネル改造	1.2倍？

  - ポイント
    - ECC (かつ動画は1セッションが長いので楽)
    - AES NI (CPUのAES用命令セット)
    - Kernel Sendfileが使えないのは痛い

ストリーミングのHTTP、HTTPS化の状況

- 米国の状況
  - 代表的な常時SSLサイトの動画配信方式

サイト	PC向け	モバイル向け (Nexsus7+Wifi+Yahoo! ADSL)	
	ブラウザ	ブラウザ	アプリ
Youtube	HTML5 + **HTTPS**	HTML5 + HTTP	**HTTPS**
Facebook	Flash + ？ + **HTTPS**	HTML5 + **HTTPS**	**HTTPS**
Yahoo!	Flash + ？ + **HTTPS**	HTML5 + **HTTPS**	非検証

  - 注意点
    - 一般的にCPは、モバイル向け配信において、端末・ISPにより方式を変える
      - 遅いCPU、遅いISP
        - 軽いコーデック
        - 意図的なHTTP配信

TLS比率：北米

- TLSトラフィック比率（北米2014年下期）

固定：19.16%		モバイル：26.15%	
Netflix	34.89	Youtube	19.75
Youtube	14.04	Facebook	19.05
その他HTTP	8.62	その他HTTP	11.44
Facebook	2.98	その他MPEG	6.32
BitTorrent	2.80	Netflix	4.51
iTunes	2.77	Instagram	4.49
MPEGその他	2.66	SSL	4.03
Amazon Video	2.58	iTunes	3.20
SSL	2.14	Google Cloud	3.07
Hulu	1.41	Pandora Radio	2.72

- 出展
  - トラフィック比率：Sandvine’s Global Internet Phenomena Report 2H 2014
    - https://www.sandvine.com/trends/global-internet-phenomena/
  - 黄色枠がけ・TLSトラフィック比率算出：鍋島

影響

- 事業者別
  - 動画配信事業者
    - TLS CDNに本気
- 機能別
  - 強制（トランスペアレント）キャッシュ⇒終了
  - 強制トランスコード⇒終了
  - 帯域制御⇒不可能ではないが困難
    - いろいろ制限が付く
    - TCP Proxy型による制御⇒影響なし
    - ビデオペーシング⇒終了 or 高度な処理が必要

影響：帯域制御

- アプリケーション別（ストリーミング、P2P、通常Web等）
  - プロトコルによる識別は不可能
  - セッションの振舞い（流量、使用帯域、頻度）識別のみ可能
- IPアドレス or SNIホスト別
  - リスト管理は結構大変

方式	
IPアドレス	かなり困難（CDN屋は多くのIPアドレスを変更しながら使用，CP側のマルチCDN（複数CDNの切り替え使用）利用も進む）
SNIホスト名	特定のCPのみなら可能、TLS1.3からは取得不可（ドラフト）

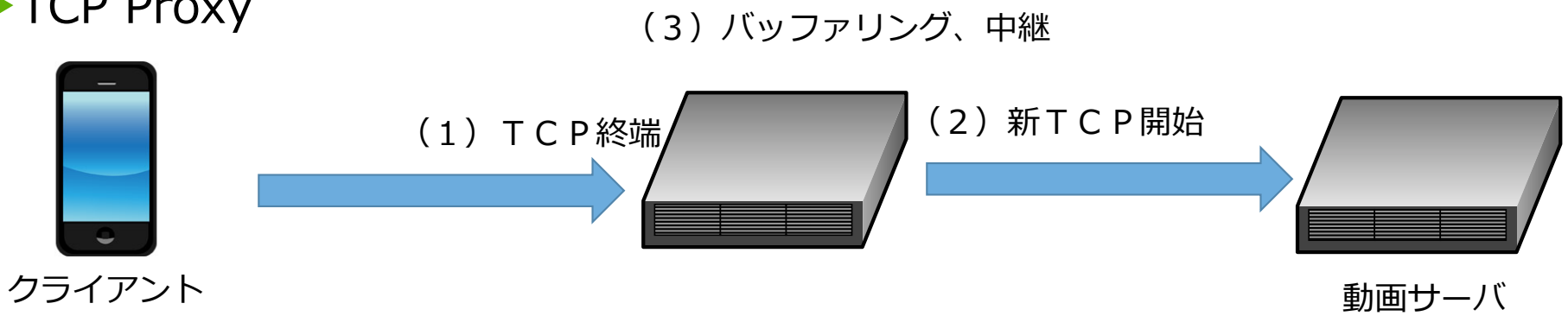
  - 利用の公平（ISPが特定のCPのみ帯域を制御する）問題
    - アプリケーション単位での制御は問題とならないが、特定ＣＰとなると電気通信事業者法に抵触すると思われる（鍋島意見）

参考：電気通信事業法（総務省）

- 第六条：利用の公平
  - 電気通信事業者は、電気通信役務の提供について、不当な差別的取扱いをしてはならない
- 帯域制御の運用基準に関するガイドライン
  - 日本インターネットプロバイダー協会、電気通信事業者協会、テレコムサービス協会、日本ケーブルテレビ連盟、MVNO協議会
  - 帯域制御の対象
    - 特定のアプリケーション
    - 特定のユーザ
- 課題
  - 特定のCP（ドメイン、IPアドレス）に対する帯域制御

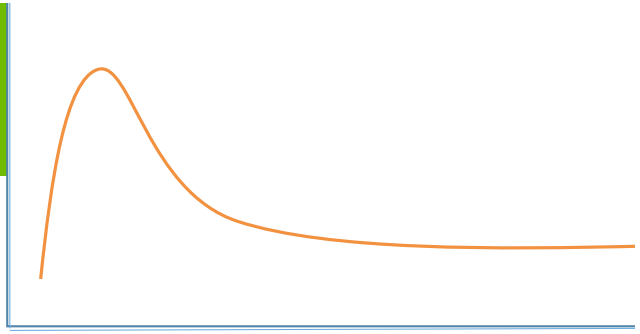
影響：TCP Proxyによる制御

- TCP Proxy



  - TCP Proxyの振舞い
    - （１）クライアントからのTCPセッションを終端
    - （２）動画サーバに新規にTCPセッションを開始
    - （３）TCPペイロードをバッファリング・中継
  - 影響
    - TCPペイロード（TLS通信）への影響なし
    - クライアントに対してはモバイル網向けのTCPアルゴリズム、帯域制御を使用できる
    - TCP Fast Openは未対応？

影響：ビデオペーシング（概要）



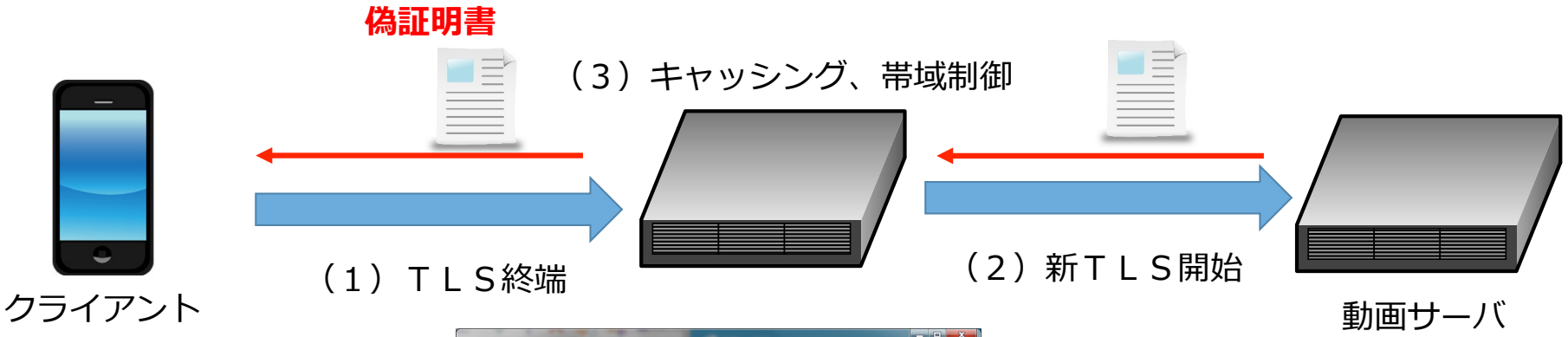
- ビデオストリーミングに対する網側の帯域制御
  - 最初：無制限
  - 一定時間後：帯域制限（動画のビットレートに合わせた処理）
  - 効果
    - 流量（使用帯域帯域）の（網の状態に合わせた最適な）削減
      - 多くのビデオは最後まで見られない⇒無駄な流量の排除
- 課題
  - クライアント側リクエスト処理とのバッティング
    - 最初：大目（映像ビットレートのＸ倍）にビデオ取得
    - 一定時間後：映像ビットレート＋αでビデオ取得
    - アダプティブビットレート：ビデオ取得ができないとビットレートを下げる
  - クライアントより高度な処理ができないと視聴に影響

影響：ビデオペーシング（TLS化の影響）

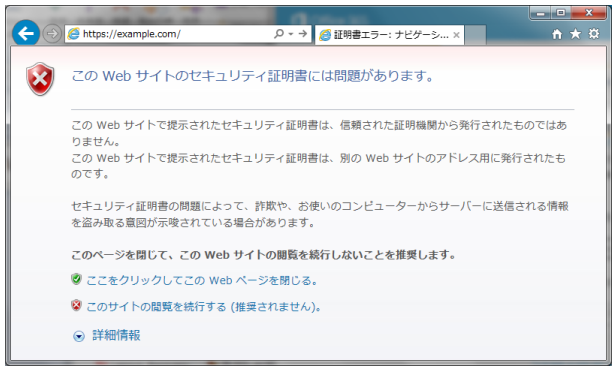
- アプローチ１
  - TLSストリーミングに対してはビデオペーシングを諦める
    - 動画のビットレートを取得できない⇒適正な適用は困難
- アプローチ２
  - 無理やり適応（流量の多いセッションをビデオと仮定し、全適用する）
    - 非ビデオ（例：ゲーム、アプリ）に対するビデオペーシング適用の可能性
      - ダウンロードに時間がかかる
    - もともと難しい帯域管理がより困難に
      - 適正な帯域の決定は無理⇒視聴に悪影響を与える

影響：偽証明書

- 概要
  - Squid用語：SSL Peek and Splice、SSL Bump



- クライアント側
  - エラー表示



影響：偽証明書

- 偽証明書の利用
  - 状況

用途	実装	状況
企業用途（FW等）	きちんと（専用ルート証明書の配布）実施	すでに一般化
PC用ウィルススキャン	オプション扱いで実装	これから普及
飛行機内Wifi ISP等	こっそり実施	顧客からクレーム

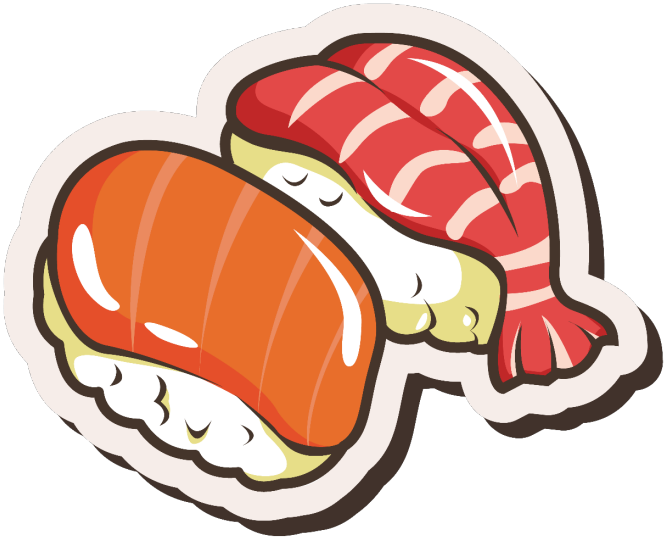
  - ストリーミング配信における可能性
    - 配信側ときちんと握ること（TLS証明書の貸与等）
    - 顧客側ときちんと握ること（専用のルート証明書）
  - 関連法規
    - 不正競争防止法（経産省）

まとめ

- ストリーミングのHTTP化
  - Everything on HTTPの一環
  - HTTPサーバの高性能性を享受
  - ブラウザだけで動画再生（プラグイン排除）
- ストリーミングのTLS化
  - URLバーのワーニング対策
  - コンテンツの濫用（勝手キャッシュ、勝手スプリット）対策
  - コンテンツの改変対策
  - 社会的な要請への対応（プライバシー保護）
- 影響
  - コンテンツ操作（キャッシュ、トランスコード）⇒終了
  - 帯域制御
    - アプリケーション別⇒振舞い認識型（ただし課題多数）を除き終了
    - IPアドレス・SNIベース⇒電気通信事業者法が課題
    - TCP Proxy⇒影響なし
    - ビデオペーシング⇒（基本）終了
  - 偽証明書
    - きちんとした握りが必要

おわりに

- CPとISP・キャリアとの「うまい　にぎり」がより重要に



- ただし、ISP Cacheなアプローチではなく、Open Reverse Cacheが本命

補足

- 事前資料および追記資料
  - J-Stream CDN情報サイト
    - https://tech.jstream.jp/blog/meeting/janog35-5/

補足：ネットワークの中立性議論

- 単純な定義
  - すべてのトラフィックを平等に扱うべきかという議論
- 政策的・経済学的な定義
  - キャリア・ISPがトラフィックの差別的扱いにより、隣接業界（CP等）に影響を与えることを許すべきか（それにより産業全体のプラスになるか）という議論
- 現実的な定義 by 鍋島
  - CP vs キャリア・ISPのパワーゲーム and 国策
    - 産業規模
      - 米国：CP産業規模>キャリア・ISP産業規模
      - 日本：CP産業規模＜キャリア・ISP産業規模
    - 各国における産業政策
    - 経産省 vs 総務省