マンガ海賊版サイト
最新動向レポート（2024夏）

LINEヤフー株式会社
政策企画本部メディア部・コマース部
セキュリティエンジニアリング本部サイバーセキュリティ分析部脅威情報分析対応チーム

宮内 秀輔

LINEヤフー

発表者担当者について

- **宮内 秀輔（みやうち しゅうすけ）**

- **LINEヤフー株式会社**
  - **政策企画本部メディア部**
    政策企画本部コマース部
  - **セキュリティエンジニアリング本部**
    サイバーセキュリティ分析部脅威情報分析対応チーム
    （通称：Digital Crime Unit）

フィッシング・偽サイト、海賊版、不正取引、誹謗中傷・偽情報などなど
インターネットサービスにおける犯罪・不正全般について、
セキュリティ領域エンジニア、企業法務、両面の立場で社内外の対策推進を担当。

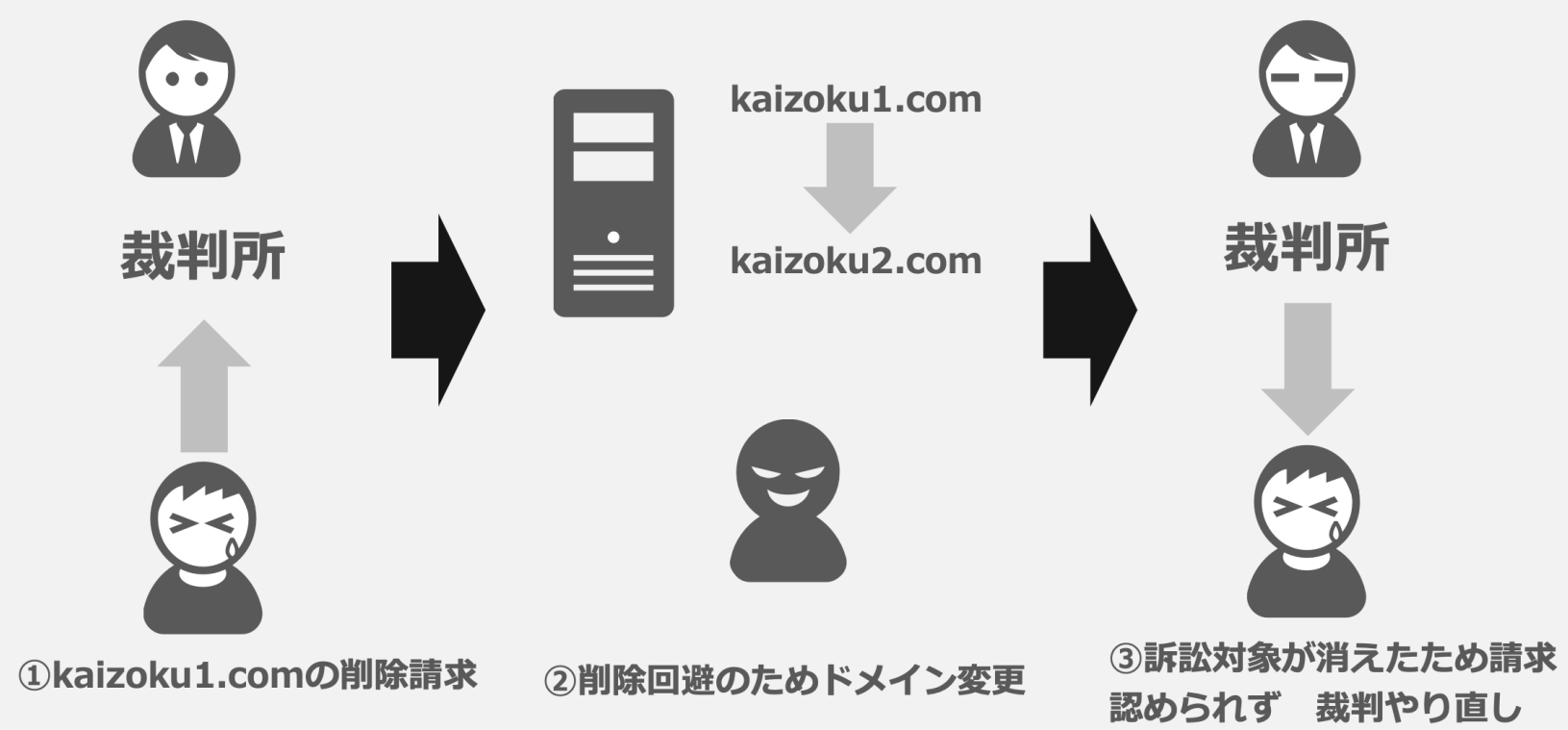
このパートについて

海賊版サイトの運営動向について過去の発表も振り返りつつ
直近1年における新たな観測事項をご報告します

- 日本向けマンガ海賊版サイトの新たな動き
- ベトナム人向けマンガ海賊版サイトの調査報告

日本向けマンガ海賊版サイトの新たな動き

振り返り：海賊版サイト対策の悩みその１
ドメインホッピング



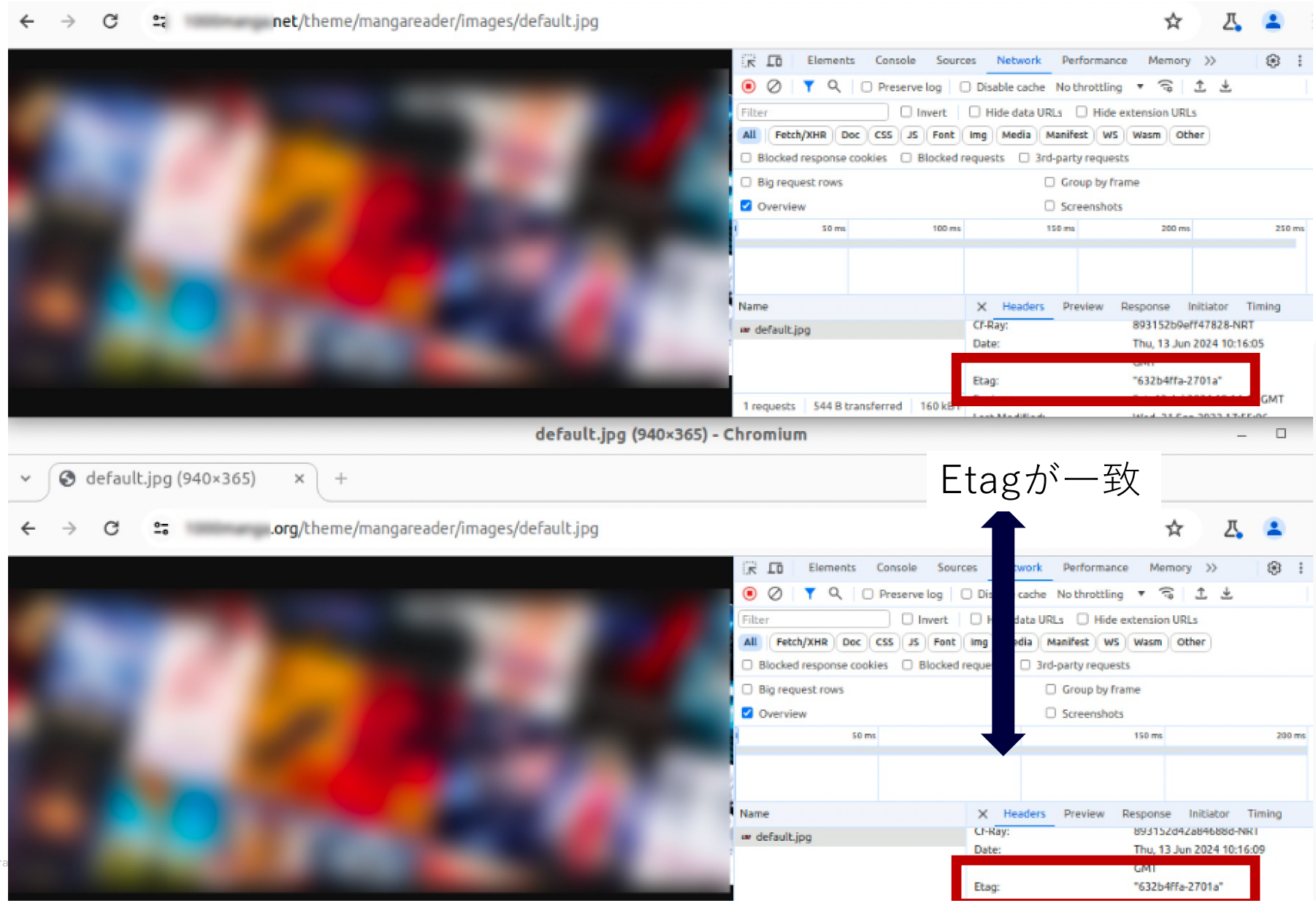
※JANOG50発表資料より

新しい動き1：同一フロントエンドサーバに対して100ドメイン以上を紐づける海賊版サイトが登場

サイト名はドメイン名、IPアドレスもCDN利用のため別々

もっとも、以下の要素から同一オリジンのフロントエンドサーバで運営していると推測

- サイト名以外のデザイン・パス構成が全て一致
- 表示されるマンガ画像の配信元ドメインが全て同一
- フロントエンドサーバから配信される画像のレスポンスヘッダーのEtagが一致


net/theme/mangareader/images/default.jpg
Elements
Console
Sources
Network
Performance
Memory
Preserve log
Disable cache
No throttling
Filter
Invert
Hide data URLs
Hide extension URLs
All
Fetch/XHR
Doc
CSS
JS
Font
Img
Media
Manifest
WS
Wasm
Other
Blocked response cookies
Blocked requests
3rd-party requests
Big request rows
Group by frame
Overview
Screenshots
50 ms
100 ms
150 ms
200 ms
250 ms
Name
Headers
Preview
Response
Initiator
Timing
default.jpg
CF-Ray:
893152b9eff47828-NRT
Date:
Thu, 13 Jun 2024 10:16:05
Etag:
"632b4ffa-2701a"
GMT
1 requests
544 B transferred
160 kB
default.jpg (940×365) - Chromium
default.jpg (940×365)
Etagが一致
.org/theme/mangareader/images/default.jpg
Elements
Console
Sources
Performance
Memory
Preserve log
No throttling
Filter
Invert
Hide extension URLs
All
Fetch/XHR
Doc
CSS
JS
Font
Manifest
WS
Wasm
Other
3rd-party requests
Big request rows
Group by frame
Overview
Screenshots
50 ms
150 ms
200 ms
Name
Headers
Preview
Response
Initiator
Timing
default.jpg
Date:
Thu, 13 Jun 2024 10:16:09
GMT
Etag:
"632b4ffa-2701a"

振り返り：海賊版サイト対策の悩み　その２
登録容易なCDNの悪用

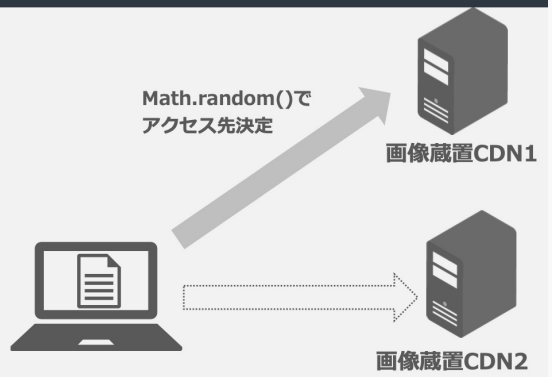
フロントエンドでのルーティング処理も発見

```
var imgDefer = document.getElementsByTagName('img');
    for(i+1; i<imgDefer.length; i++){
        if(imgDefer[i].getAttribute('onload') == 'xxxt(-1)'){
            var image_cdn1_url = imgDefer[i].getAttribute('cdn-src');
            var image_cdn2_url = imgDefer[i].getAttribute('data-src');
            var image_cdn_url = Math.random() >=2 && image_cdn1_url ? image_cdn1_url : image_cdn2_url;
            imgDefer[i].setAttribute('src', image_cdn_url);
            imgDefer[i].setAttribute('onload','xxxt(' + i+')');
        }
    }
```

上記は海賊版サイトの最大グループで一時期みられたJavaScriptコード。

JavaScript上で画像配信CDNのプログラムルーティングを行っている。

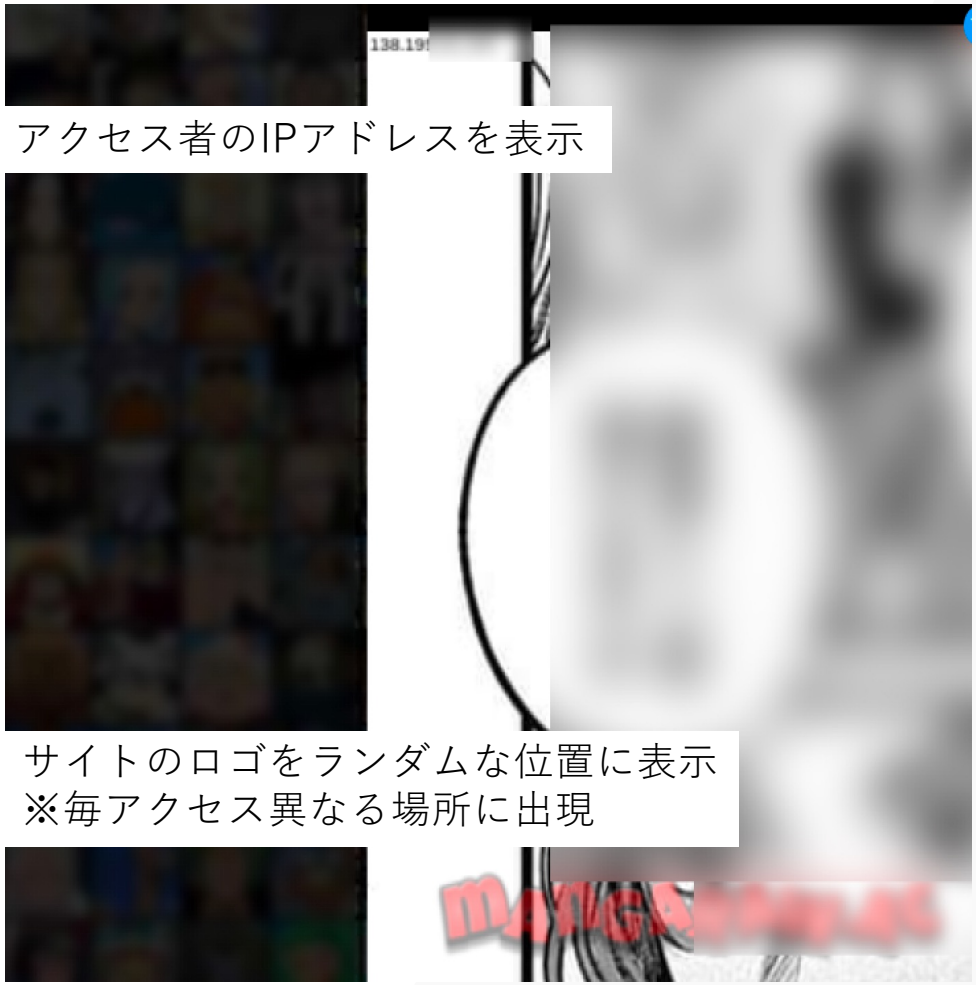
※よくみるとMath.random()のところにバグがあり実際は機能しない。
　そのためか、最近はこのコードが使われる形跡はない。



※JANOG52発表資料より

新しい動き2:マンガページ画像表示方式の変化

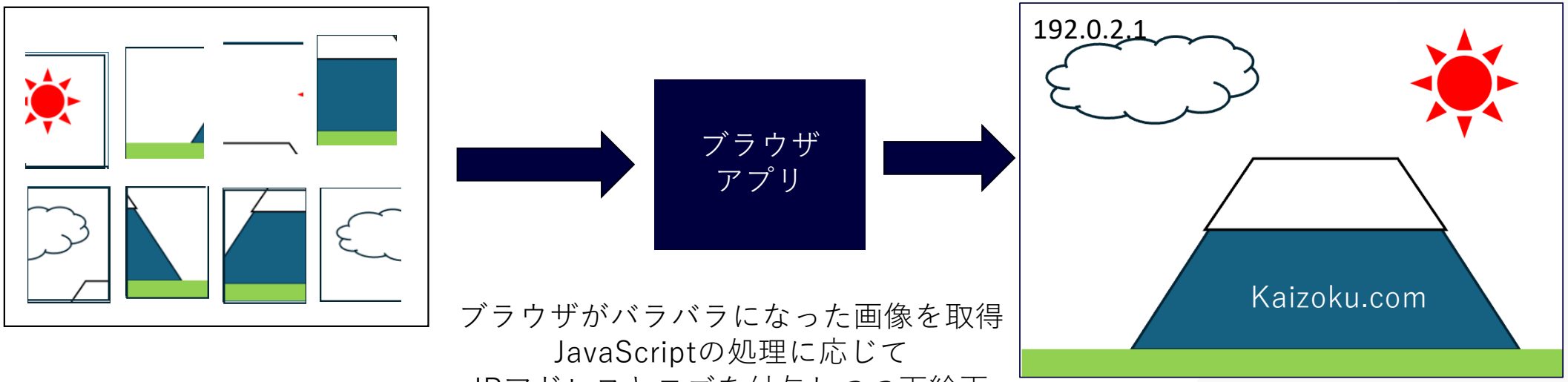
マンガのページ画像は
１６分割バラバラにされた状態で配信



アクセス者のIPアドレスを表示

サイトのロゴをランダムな位置に表示
※毎アクセス異なる場所に出現

どのようにマンガページを表示しているのか



ブラウザがバラバラになった画像を取得
JavaScriptの処理に応じて
IPアドレスとロゴを付与しつつ再絵画

その他の変化：リサーチャーへの嫌がらせ
ブラウザ開発者ツール利用妨害

```
359   if (config.f12) {
360     var _0x6e63 = [
361           "getTime",
362           "debugger",
363           "constructor",
364           "href",
365           "location",
366           "https://google.com",
367           "script",
```

```
389     devtoolsOpen = !1;
390   function _time() {
391     var e = new Date()[_0x6e63[0]]();
392     (function () {}[_0x6e63[2]](_0x6e63[1])(),
393       new Date()[_0x6e63[0]]() - e >= 200 &&
394         (window[_0x6e63[4]][_0x6e63[3]] = _0x6e63[5]));
395   }
```

- ブラウザ開発者ツール利用の状態でアクセスした場合、デバッガーが起動
- デバッガー起動により、ページのレンダリング処理遅延を検知すると、google.comにリダイレクトする

その他の変化：リサーチャーへの嫌がらせ ソースコード難読化

comic-view.bundle.js

```
var KjmBbY = [], y1s73U7 = 0x0, PNzRD_ = fHPxn2(()=>{
    var KjmBbY = ['#2hGmx?H7!ZKpE', '?7y171wC6Li', '!70HJkcYMO"(w8RbAEf<z#zH&PZ'
        7l@Jk4U:>S9', '#fXxy+nNJR&/#6mYQ8*K', 'RP)a+iIYD8{89Ebq+lXcl4b1KOeU^CYdC
        .wn/,3KSK%?Z_DN', 'dP(gt@mC', '44!fP[A', ']DwJb', ',z_1Z', 'BE)=l/A', '9
         '2X01nvoC', 'PP)Fd', 'dPef{*UC', '*zbgmvaC', '$zo/5+UC', 'hrZ2b', 'XPAJ
        'w5zg7=YC', 'a852b,uC', 'CE(gt@MC', '[%XJ>[aC', '#Xlf&.aC', '*zbgb', 'SP
        &zmf=[geE$=#},`o', ']D%2x)wC', 'xoTgp@1B', 'tl$G', 'Hujg6=SC', 'CE(gt@7*
        /yC', 'drzgl)RvG', '9oefB.cC', 'ZP;I', '(zH<8zCIR#y', '[i/2s)AIDT@4ZE',
        BEU=t)MI"U9uhE', '^D(gFpp;M!30HC<mI=MfN[~jQJ^5ba?b3%+,My8{u4*Bj+adoX3c9.
        tFHs4*BLO{WwDWc[tFHrL+B<7{WwDWc[tFHs4*BLO{WwDWc[t!Ms4rHLO0c0DWc[tHHb7,BL
        tFHs4*BLO{WwDWc[tFHs4*BLO{WwDWc[tFHs4*Bn6ArQ,YGg>L1e&sO&[2o%JX/<3+Ms4HQ&
        5^`<4_8LO{W{qQzX7Eu7L,&*[!QTUQ2hhsS&5#IIb8QbXj.P0mkf1#Z{[&ZfuOE2_n`?5"F=
        148GtIk<+[=T.D1f6.:oO7PYyZgYmU>HCu]0m6&=pQEY6,I;N546v4OXYv{Weuncd/{M~%bi
        yIiVN~!ow2l!Ynz)aR0<u@#&=KF(Z3U?xe/W6TM[IN.Im?R.G?y9dy8[#TO.moRQ2&iY0<Rf
        06OP?DPVjFSHh9_>oL%LXuZcp"7Cgnxy6GN"dfaiY]ijdA89d+Ncz![Arg8Dd1#[HAP:ulwn
```

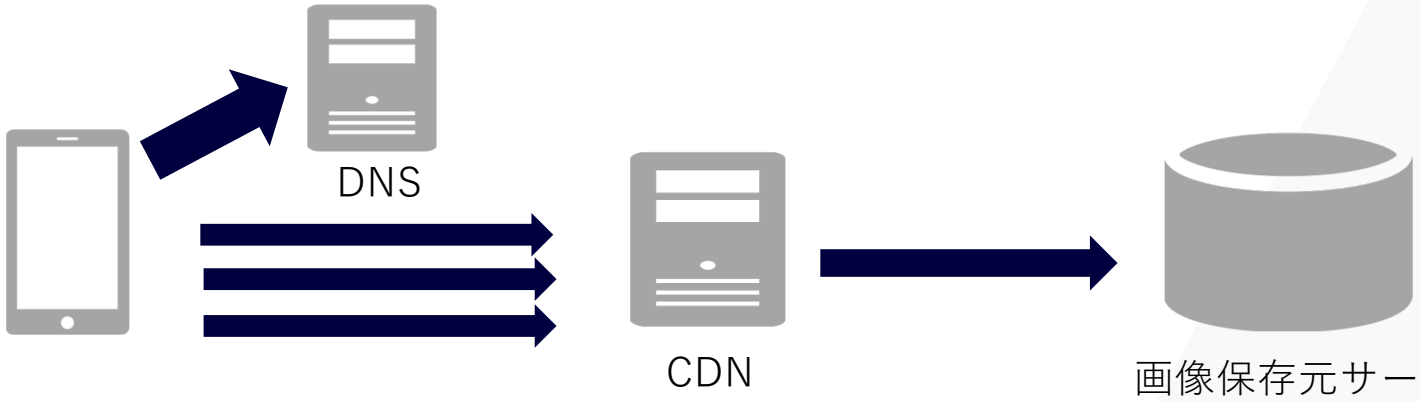
ソースコードが難読化、解析がしづらくなった

新たな動きに対する考察

マンガ海賊版サイト対策に対する国内外の動き、それに付随する調査活動が行われていることについて、運営者も自覚して対策を考え始めている

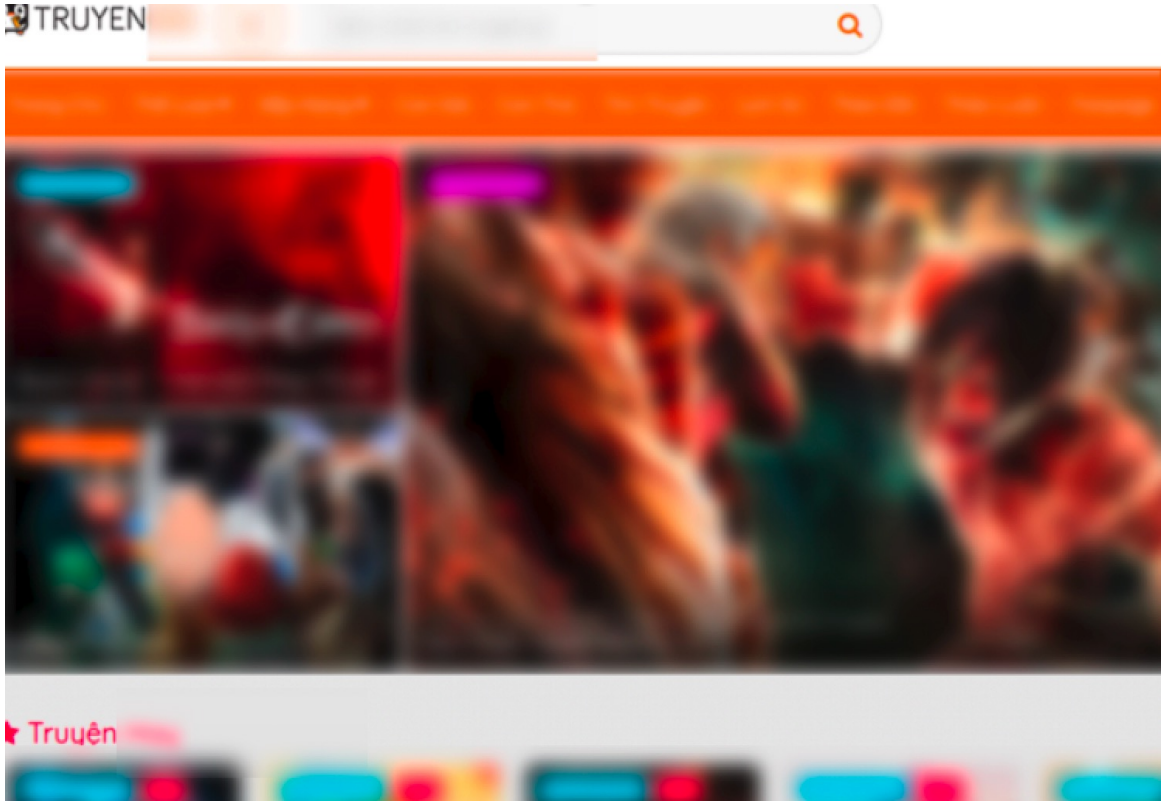
変化があったのはソフトウェア上の処理や設定だけ

登録が容易なドメイン・CDN悪用という全体インフラ構成は変化がない



ベトナム人向けマンガ海賊版サイト調査報告

今回の調査対象：ベトナム人向けマンガ海賊版サイト



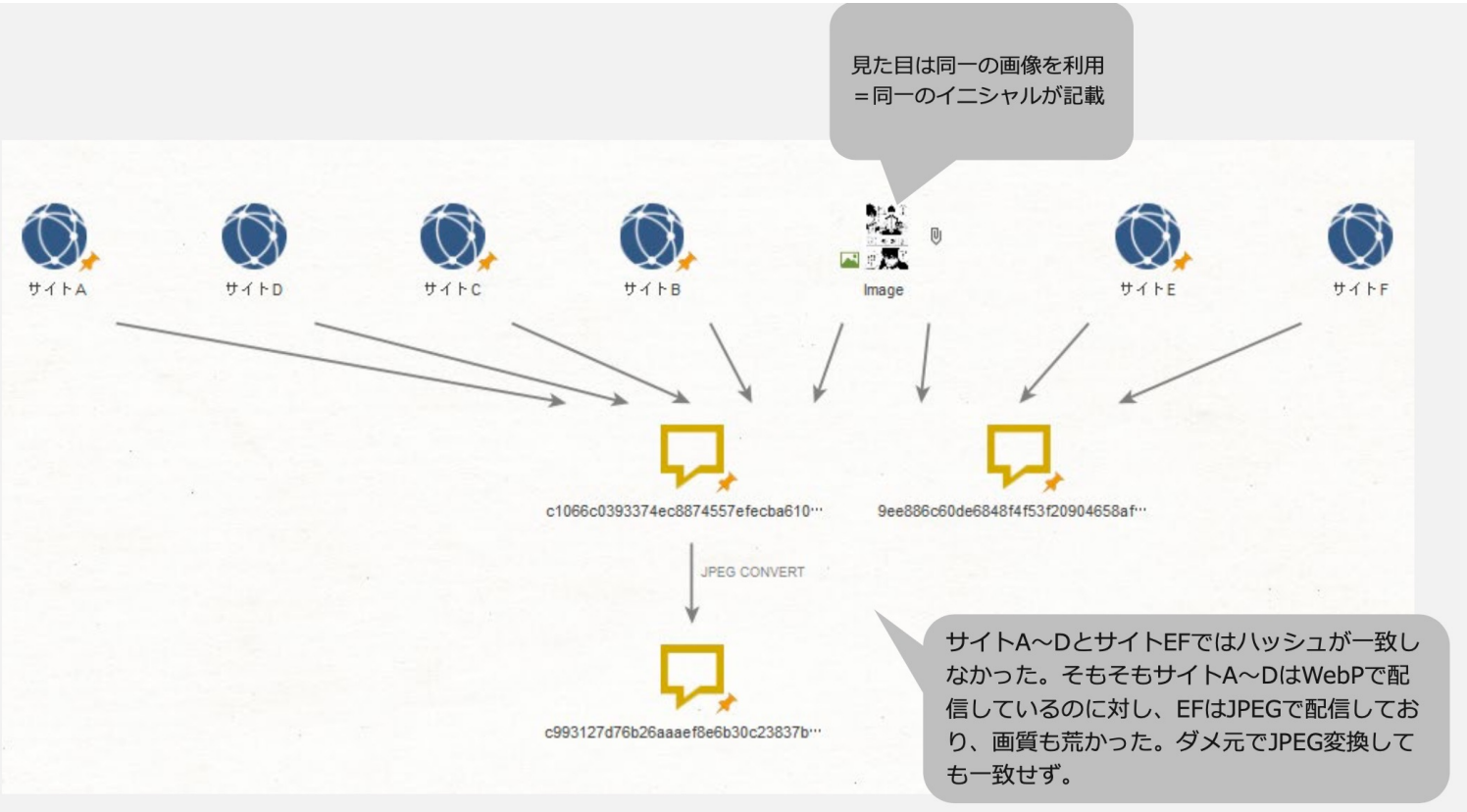
ドメインやサイト名において「truyện（チュイエン）」という
ベトナム語で「物語」を意味する語句が使われる

ベトナム向けサイトの特徴　その１
CDN悪用観点は同一

サイト名	フロントエンド	ドメインレジストラ
サイトA	CDN　米国系C社	ベトナム系P社
サイトB	CDN　米国系C社	米国系N社
サイトC	CDN　米国系C社	米国系N社
サイトD	CDN　米国系C社	米国系C社
サイトE	CDN　米国系C社	ベトナム系M社

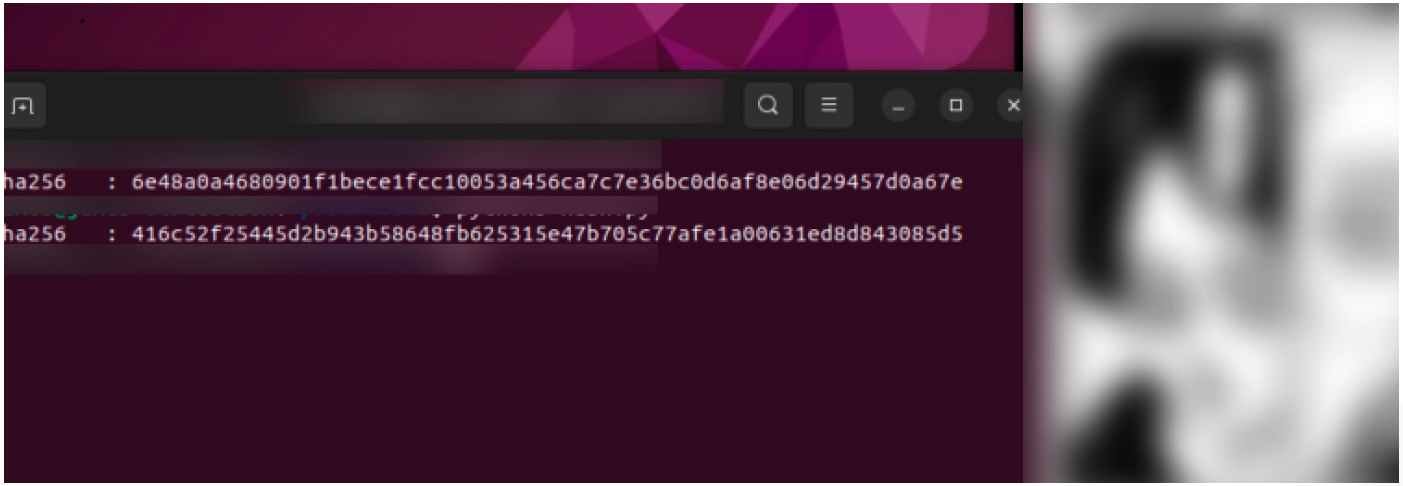
※調査データは2023年夏～秋時点のものです

振り返り：日本向サイトは画像ファイルが一致



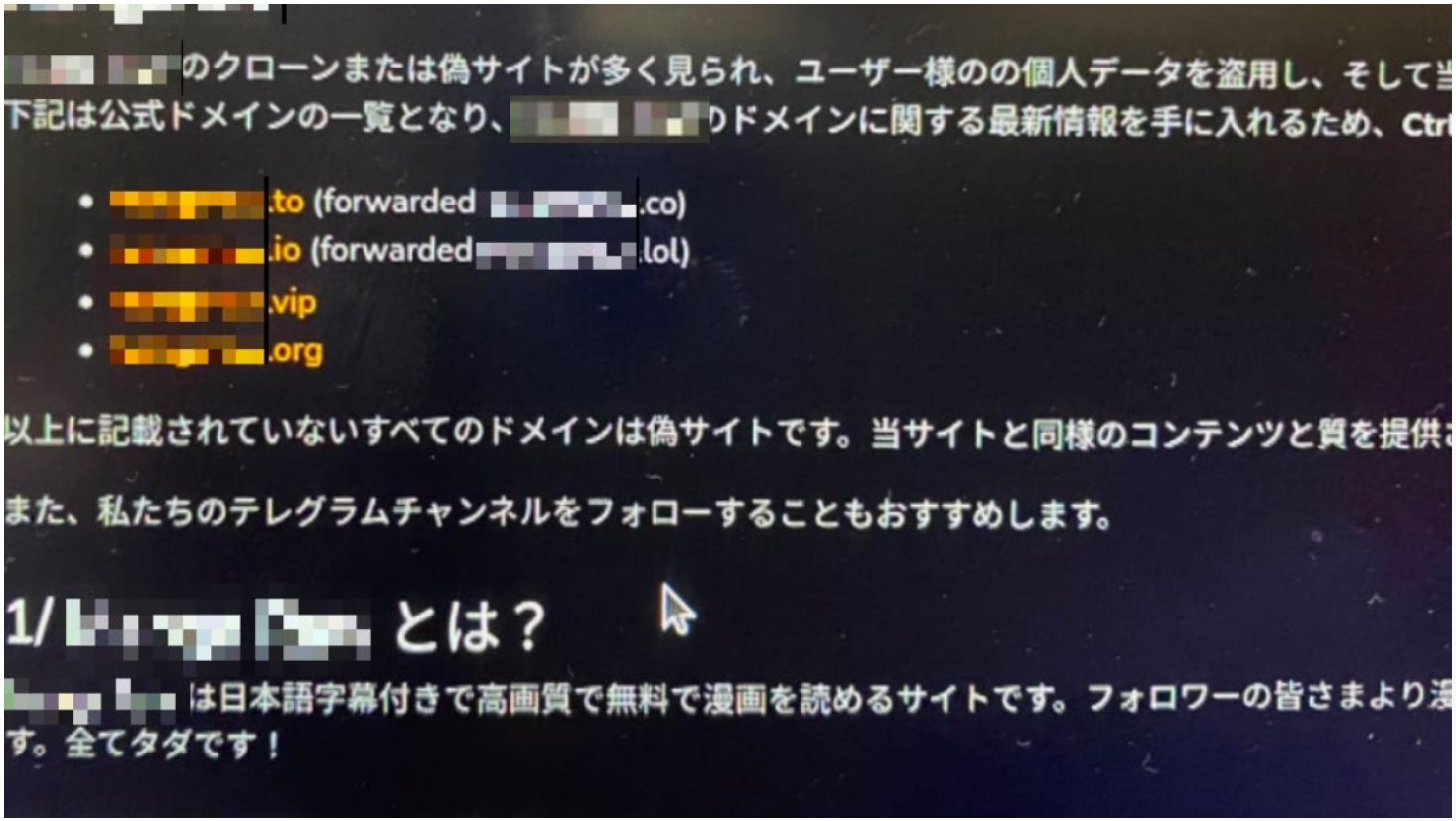
※JANOG52発表資料より

ベトナム向けサイトの特徴　その２
サイトごとの画像のハッシュ値が一致しない



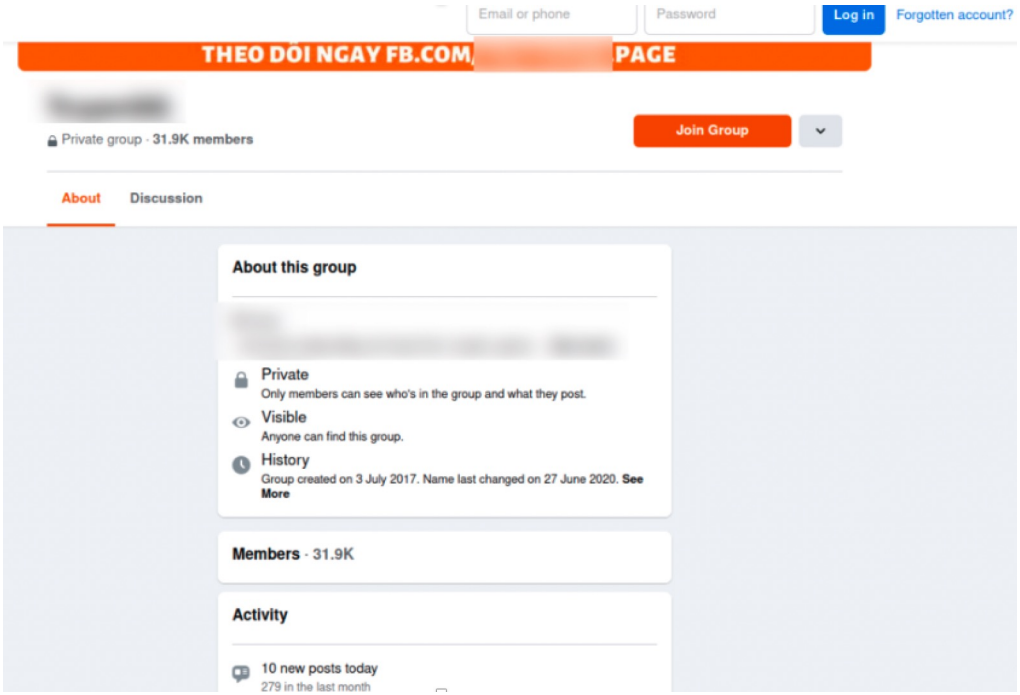
大手サイト同士でも画像のハッシュ値が一致しない
目視レベルでもドットに違いが見られる
サイト運営者ごとに自前で用意している可能性

振り返り：日本向けサイトのコミュニティはTelegram



※JANOG52発表資料より

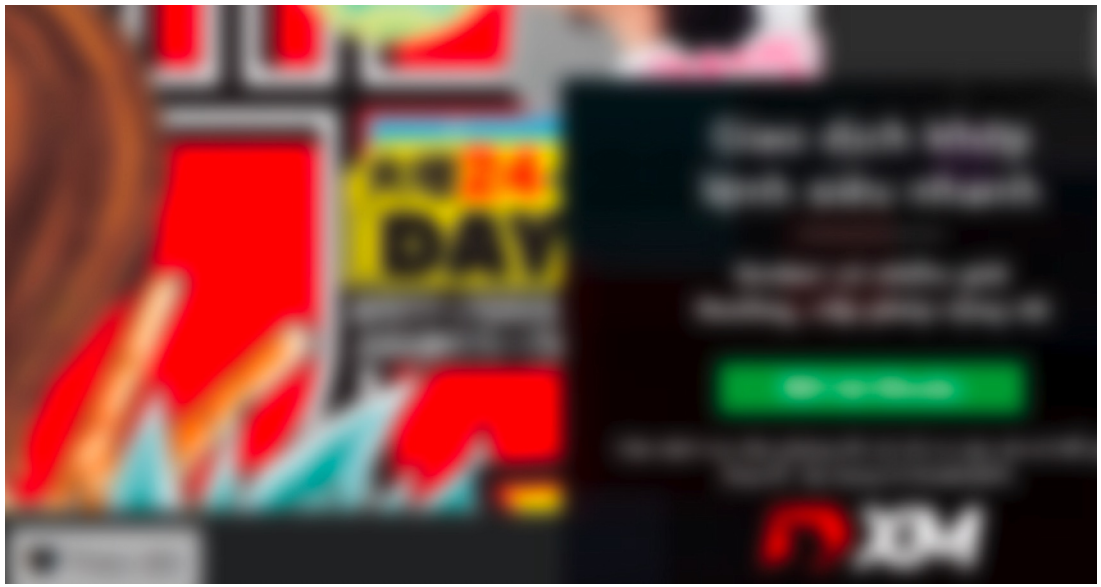
ベトナム向けサイトの特徴　その３
大手SNSに3万人のコミュニティ



サイトにリンクされる形で大手SNSに参加者3万人以上のコミュニティを発見

Activityに1日で10投稿とあり、活動も活発と推察

ベトナム向けサイトの特徴　その４
オーバーグラウンド広告が配信

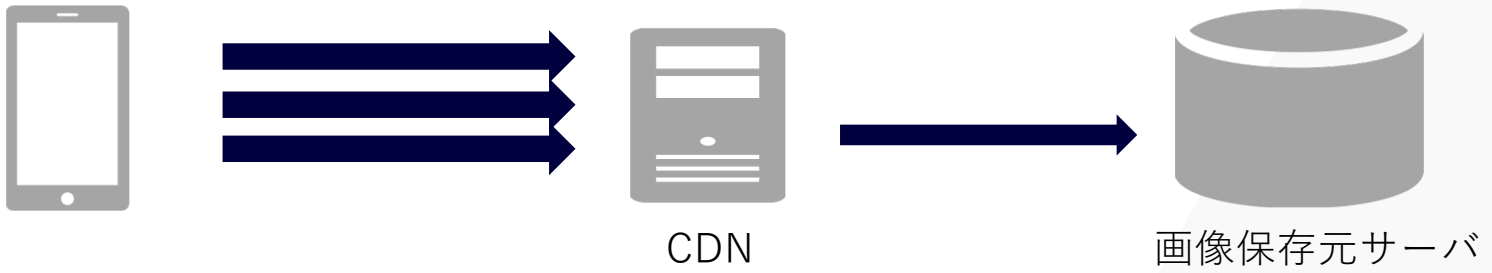


- 日本や海外一般サイトでも表示される外資系FXサービスのベトナム語広告が表示
  ※日本向けサイトはアダルト・カジノなどのアンダーグラウンド広告が配信
- 海外ニュースが流れる広告モジュールも出現
  →　パブリッシャー審査において**著作権侵害サイトという認識ができていない**可能性

ベトナム向けサイトに対する考察

- 運営者・利用者・関連事業者含め、悪意を感じられない
  ➡ ベトナム人向けの著作権啓発の必要性

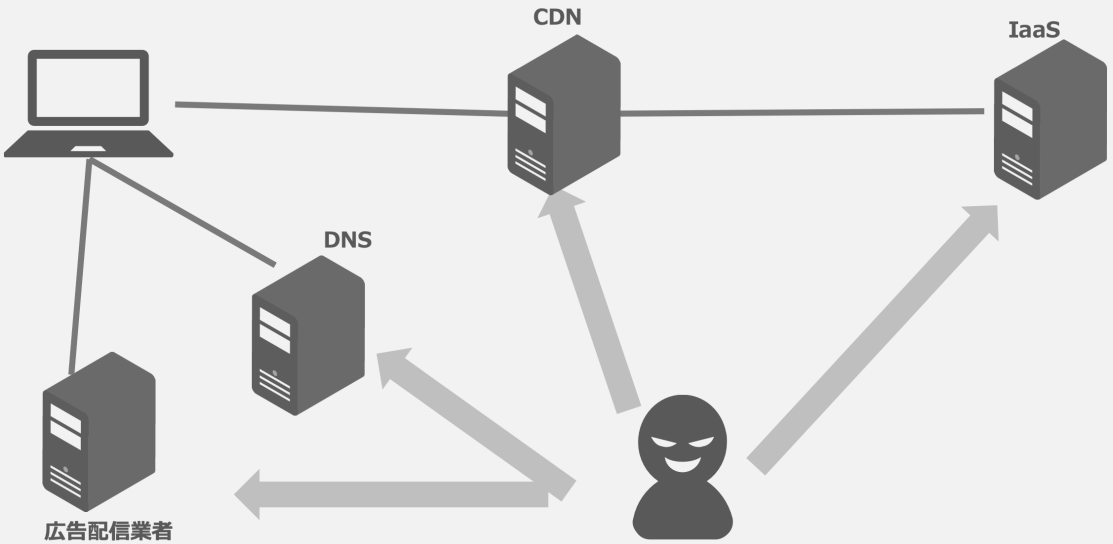
- CDN悪用というインフラ観点は日本と変わらない
  ➡ インフラ悪用対策は国内対策と共通する課題



このパートのまとめ

このパートのまとめ：２つの調査共通にいえること

安価or無料で身元確認の弱いインフラの活用



※JANOG52発表資料より

インフラ構成は他国向けでも同一・国内向けも過去と現在で変化がない

➡ インフラ領域における悪用対策は引き続き課題である

LINEヤフー