

# Signed HTTP Exchanges

## (SXG) とはなにか

SXGの仕組みからAMP連携の導入まで

大津 繁樹

SXG Study

2019年5月28日

# 内容

1. SXGのしくみ
2. SXG/AMPシステム事例
3. amppackagerについて
4. SXG導入振り返り

SXGのしくみ

# 問題1：何が違う？

1. Signed HTTP Exchanges
2. Signed Exchange
3. SXG

# 解答1

1. Signed HTTP Exchanges: 仕様の正式名称
2. Signed Exchange: 話している時みんな使っている言葉
3. SXG : 拡張子もしくは略称表記

# 問題2: どっちがSXG?

A

https://travel.yahoo.co.jp/amp/dhote

Y! トラベル Y!

品川・高輪・五反田

品川プリンスホテル

★★★★★ 3.76

1,283人中 861人が満足

口コミ1,283件

詳細・アクセス 宿泊プラン 写真ギャラリー Yahoo! 地図

B

https://www.google.com/amp/s/trav

travel.yahoo.co.jp

Y! トラベル Y!

品川・高輪・五反田

品川プリンスホテル

★★★★★ 3.76

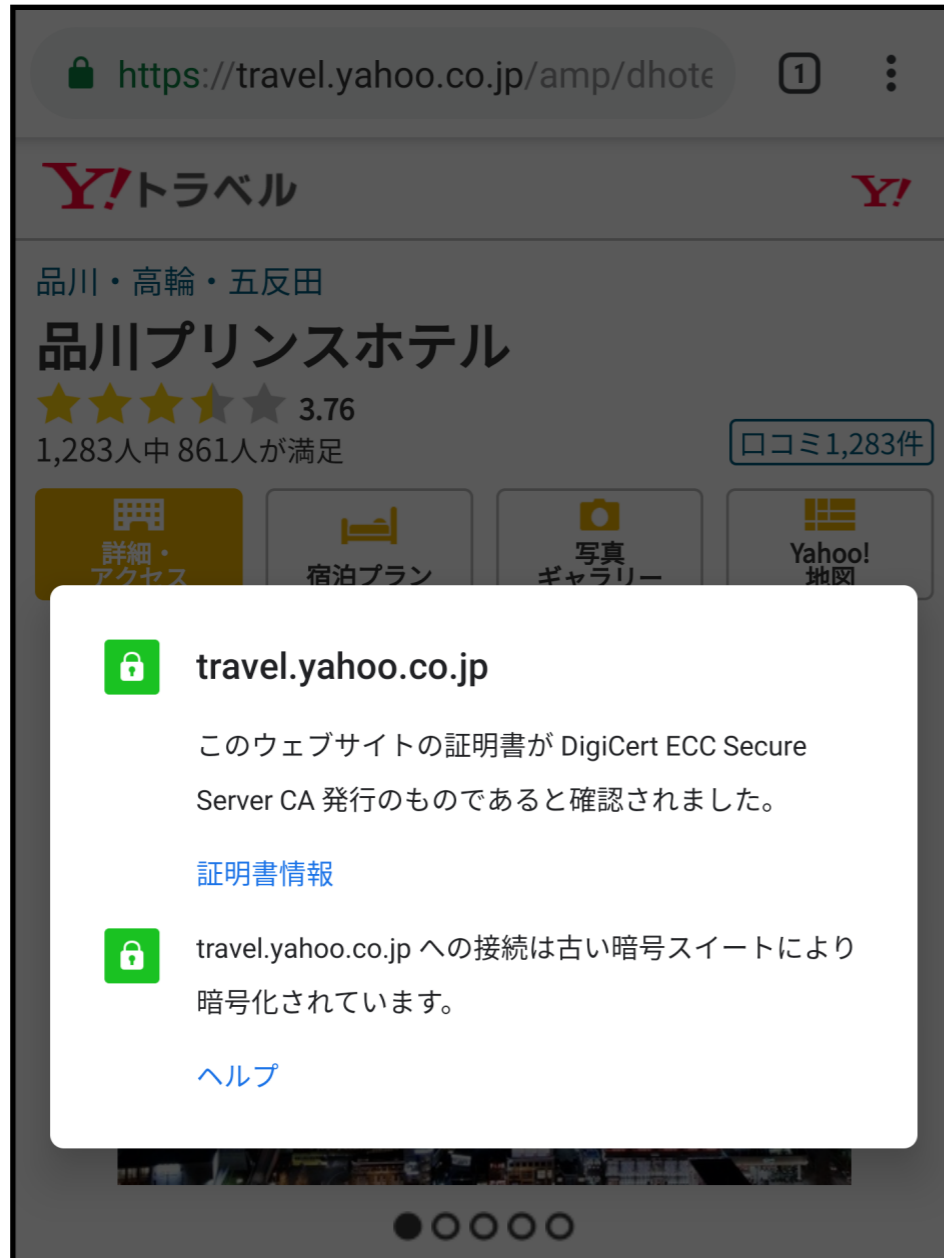
1,283人中 861人が満足

口コミ1,283件

詳細・アクセス 宿泊プラン 写真ギャラリー Yahoo! 地図

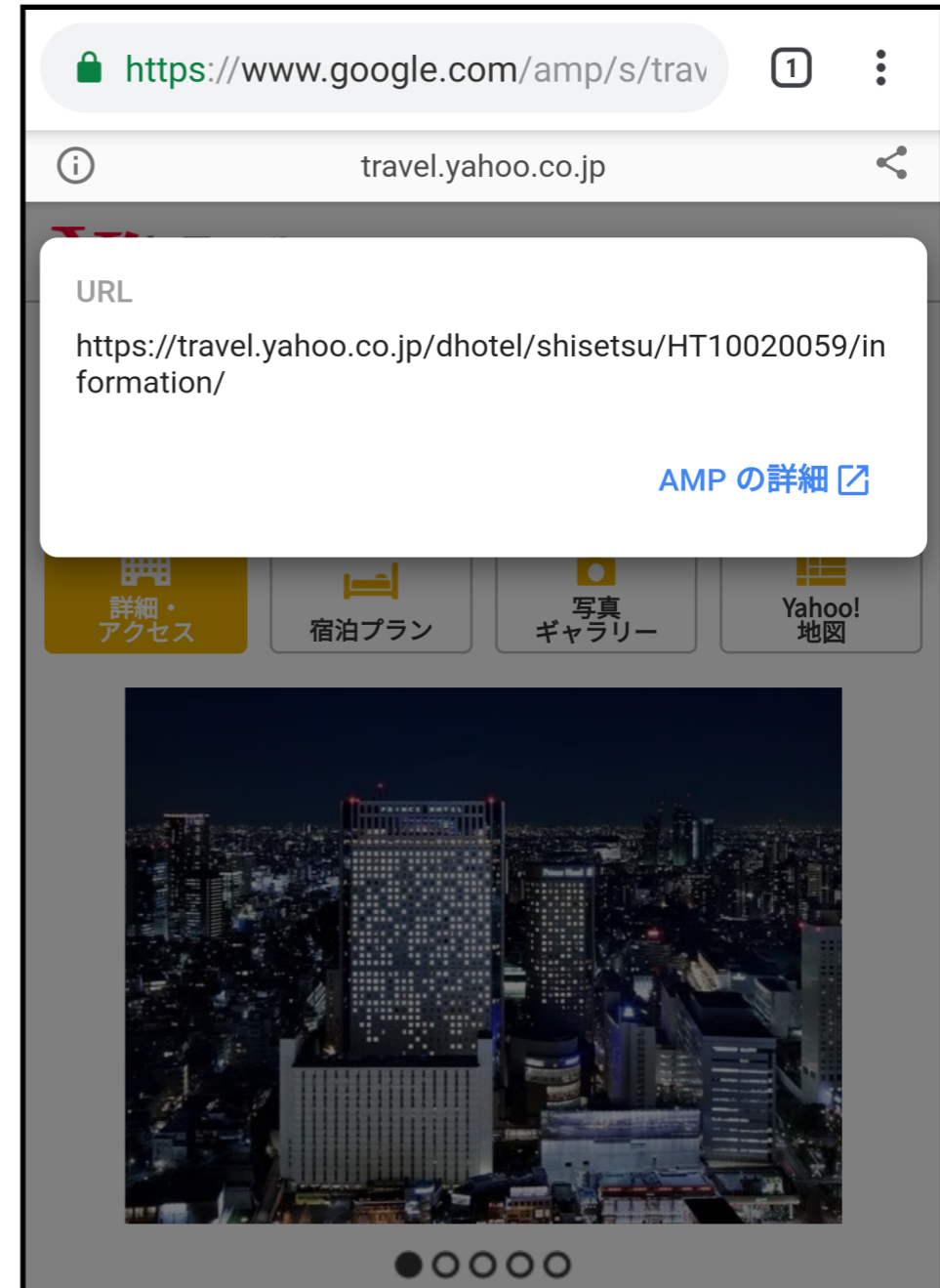
# 解答2

A



SXG

B



AMP

# 問題3: どっちがSXG?

A

https://travel.yahoo.co.jp/amp/dhote

Y!トラベル Y!

品川・高輪・五反田

## 品川プリンスホテル

★★★★☆ 3.76  
1,283人中 861人が満足

口コミ1,283件

詳細・アクセス 宿泊プラン 写真ギャラリー Yahoo!地図



●○○○○

B

https://travel.yahoo.co.jp/amp/dhote

Y!トラベル Y!

品川・高輪・五反田

## 品川プリンスホテル

★★★★☆ 3.76  
1,283人中 861人が満足

口コミ1,283件

詳細・アクセス 宿泊プラン 写真ギャラリー Yahoo!地図



●○○○○



# 解答3

A

https://travel.yahoo.co.jp/amp/dhote

Y!トラベル

品川・高輪・五反田

品川プリンスホテル

★★★★☆ 3.76

1

**travel.yahoo.co.jp**

このウェブサイトの証明書が Cybertrust Japan Public CA G3 発行のものであると確認されました。

[証明書情報](#)

**travel.yahoo.co.jp** への接続は新しい暗号スイートにより暗号化されています。

この接続には TLS 1.2 を使用しています。

接続は AES\_128\_GCM を使用して暗号化および認証されており、ECDHE\_RSA が鍵交換メカニズムとして使用されています。

[ヘルプ](#)

HTTPS

B

https://travel.yahoo.co.jp/amp/dhote

Y!トラベル

品川・高輪・五反田

品川プリンスホテル

★★★★☆ 3.76

1,283人中 861人が満足

□コミ1,283件

詳細・アクセス

宿泊プラン

写真ギャラリー

Yahoo! 地図

**travel.yahoo.co.jp**

このウェブサイトの証明書が DigiCert ECC Secure Server CA 発行のものであると確認されました。

[証明書情報](#)

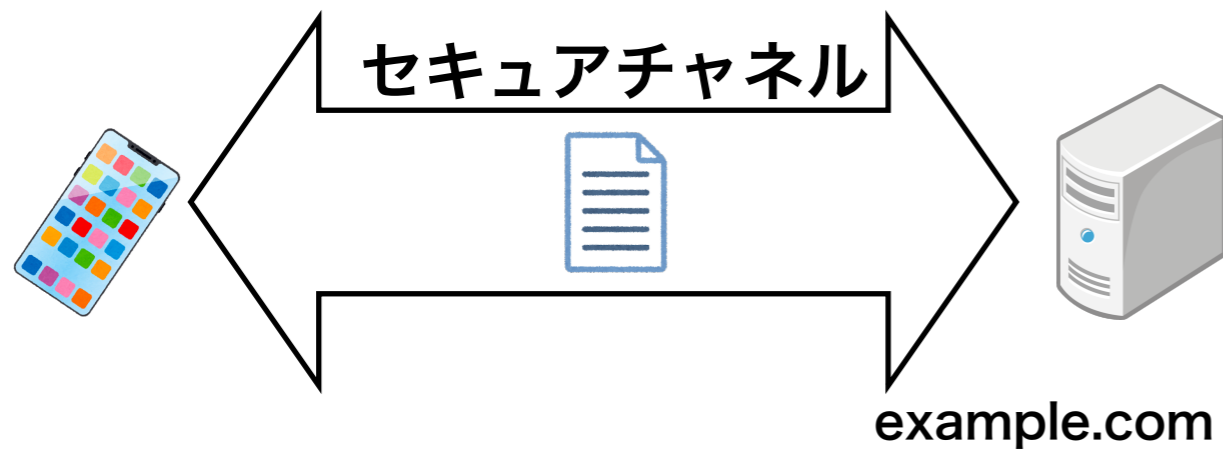
**travel.yahoo.co.jp** への接続は古い暗号スイートにより暗号化されています。

[ヘルプ](#)

SXG

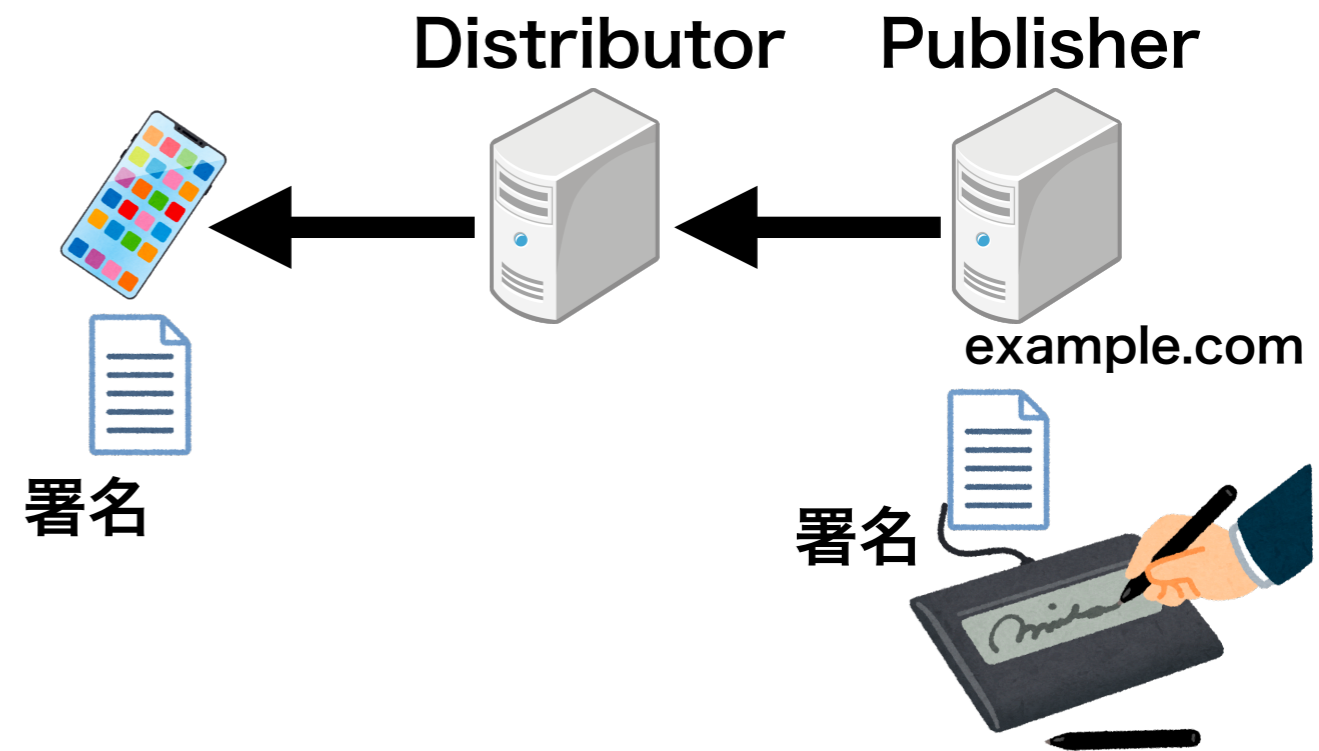
# HTTPSとSXGの違い#1

## HTTPS



通信を守る

## SXG



コンテンツを守る  
publisherのoriginで表示

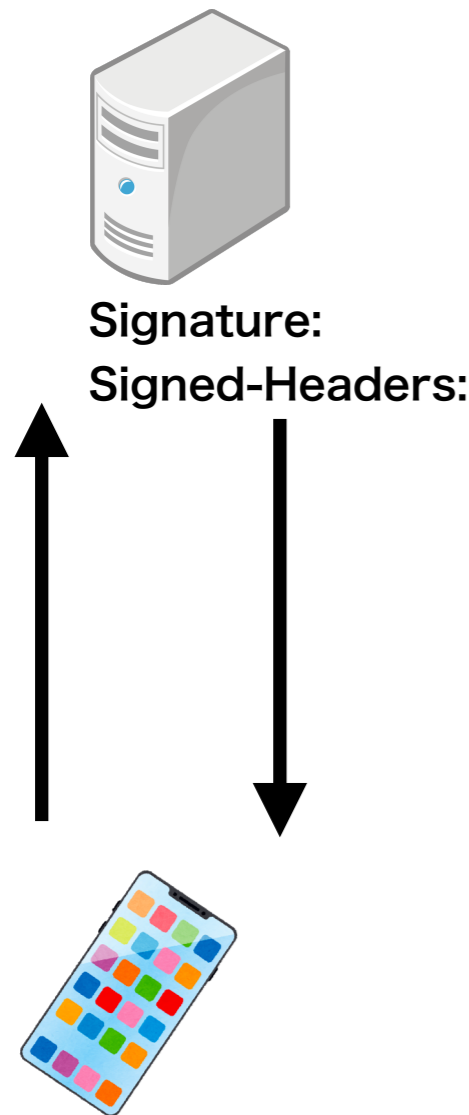
# HTTPSとSXGの違い#2

	HTTPS	SXG
機密性	✓	N/A
完全性	✓	✓
認証	✓	✓
否認防止	N/A	✓
Origin	接続先	Publisher
保護している時間	通信している間 (数百ミリ秒程度)	署名の有効期間 (最大7日間)
HTTPの制限	N/A	キャッシュ可能なコンテンツ限定 (GET限定、禁止ヘッダ有)

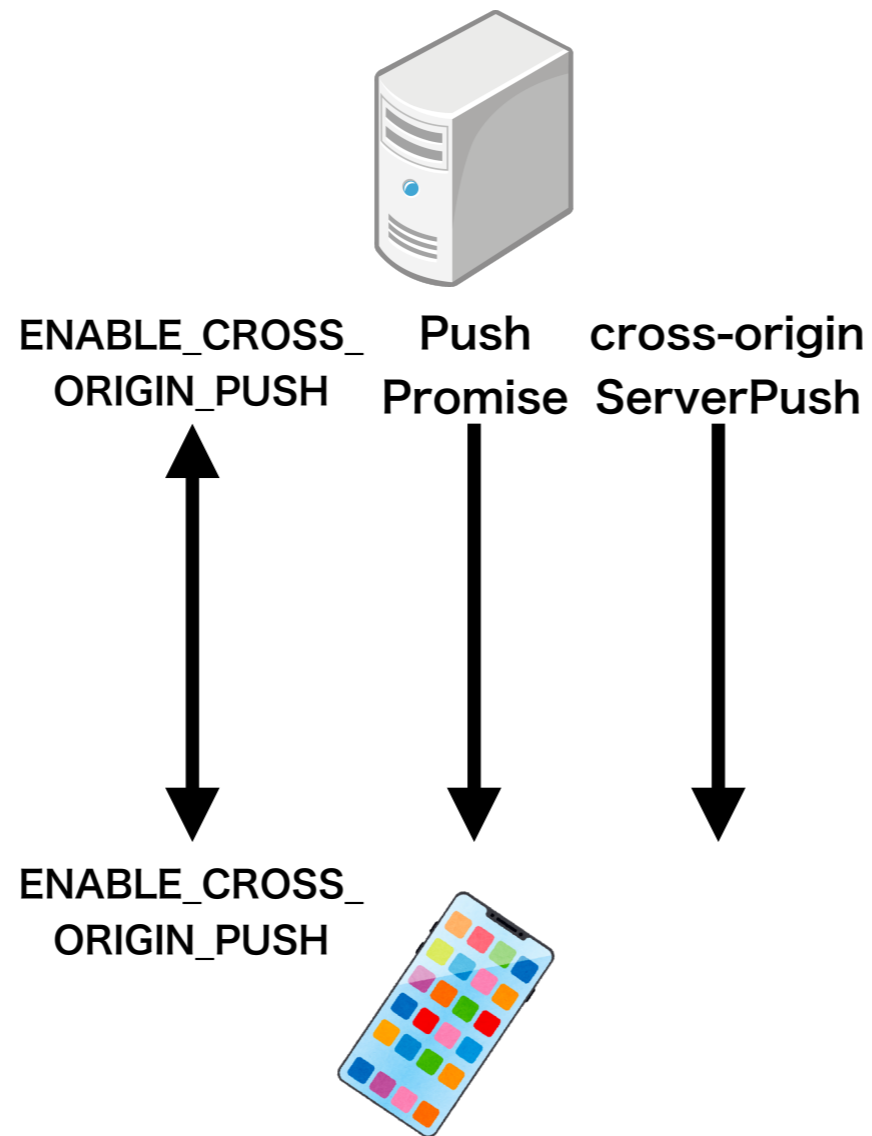
# SXGのやり取り方法3種

今日の話

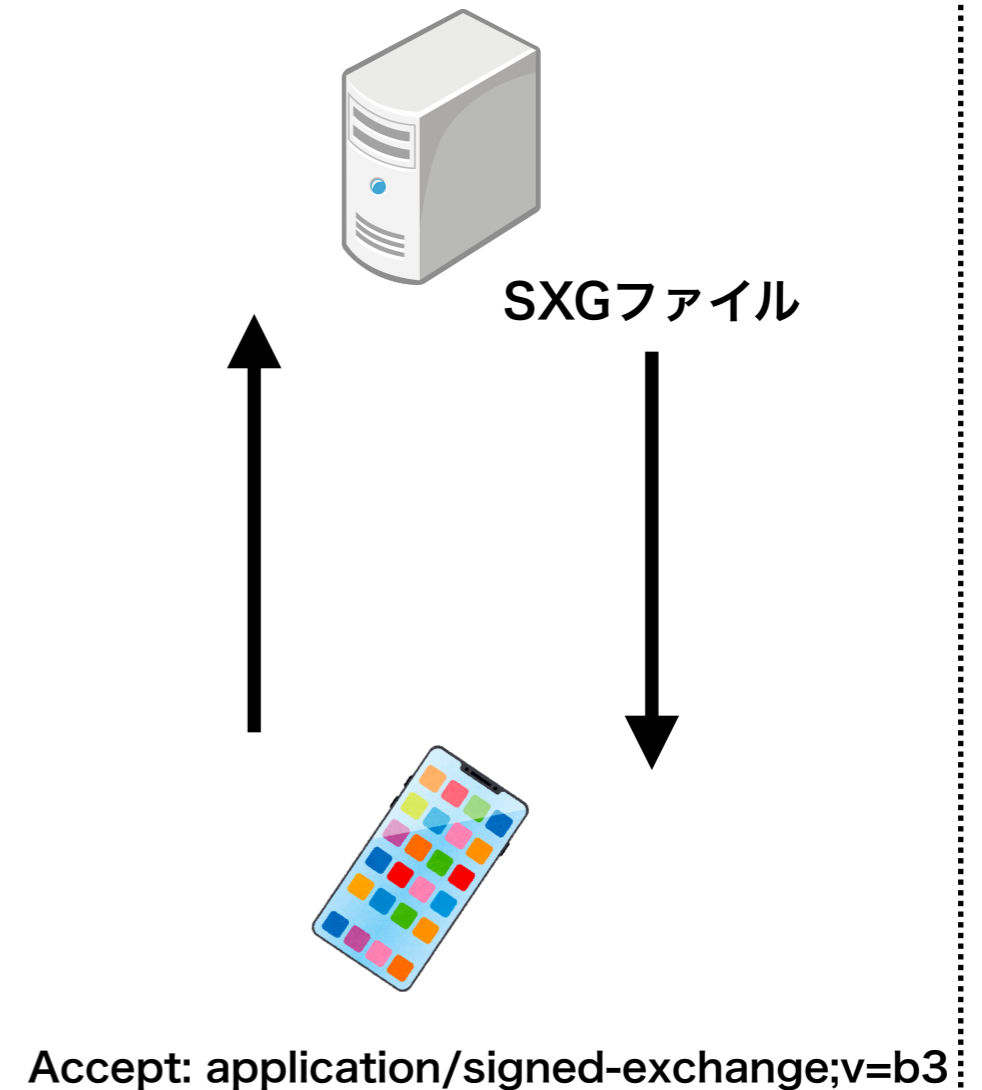
## 1. Same-Origin



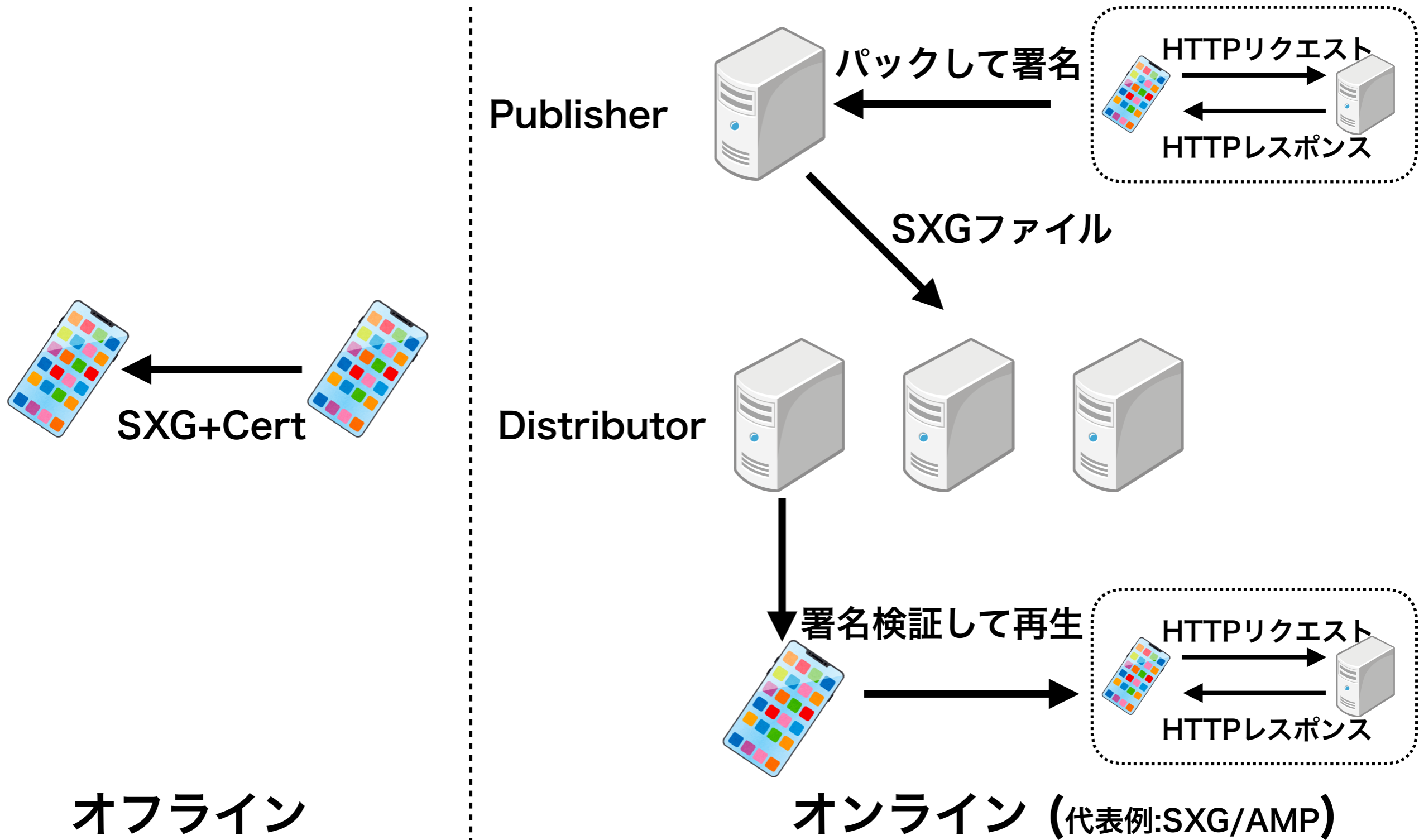
## 2. cross-origin Server Push



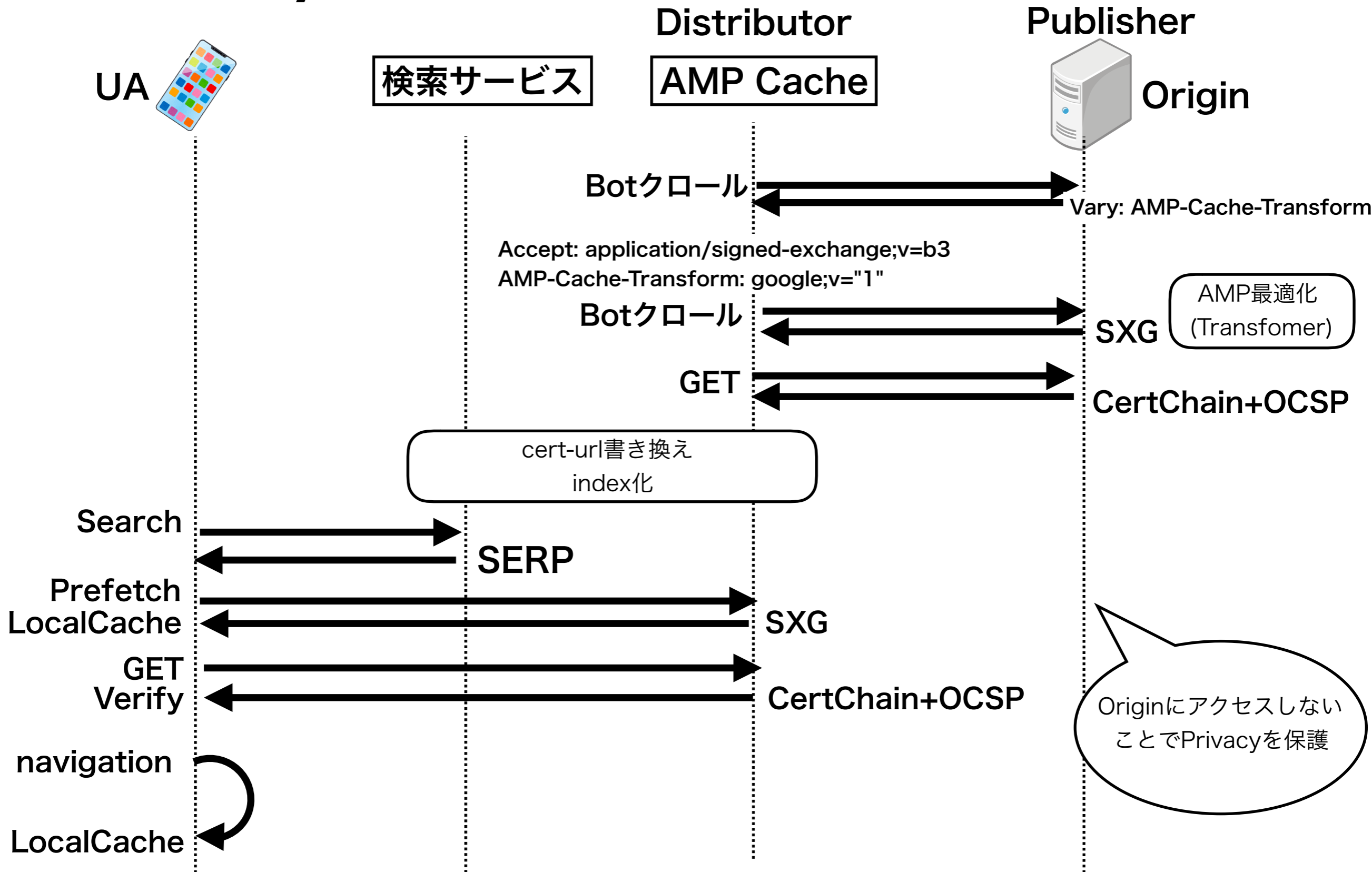
## 3. application/ signed-exchange フォーマット



# 代表的なSXGのユースケース



# SXG/AMPシーケンス図



# 検索結果 (SERP) から SXGをPrefetch

Pixel 2 XL 411 x 823 150%

Elements Console Sources Network Performance Memory Application Security Audits

Filter Hide data URLs All XHR JS CSS Img Media Font Doc WS Manifest Other

Name	Status	Protocol	Domain	Remote Address	Type	Initiator
gen_204?s=web&t=...	204	http/2+quic/43	www.google.com	172.217.24.132:443	fetch	serviceworker?pwa=search&hl=ja...
gen_204?atyp=i&ct=rfl&...	200	http/1.1	www.google.com		text/plain	search?q=ホテル+information+sit...
gen_204?atyp=i&ct=...	204	http/2+quic/43	www.google.com	172.217.24.132:443	fetch	serviceworker?pwa=search&hl=ja...
?usqp=mq331AQRKAG...	200	http/2+quic/43	travel-yahoo-co-jp.cdn.ampproject...	172.217.31.129:443	signed-exchange	search?q=ホテル+information+sit...
rs=ACT90oE_LfZUBZIM...	200	http/1.1	www.google.com		script	search?q=ホテル+information+sit...
rs=ACT90oE_LfZUBZIM...	200	http/1.1	www.google.com		script	search?q=ホテル+information+sit...
rs=ACT90oE_LfZUB...	200	http/2+quic/43	www.google.com	172.217.24.132:443	fetch	serviceworker?pwa=search&hl=ja...
rs=ACT90oE_LfZUB...	200	http/2+quic/43	www.google.com	172.217.24.132:443	fetch	serviceworker?pwa=search&hl=ja...
rs=ACT90oE_LfZUB...	200	http/2+quic/43	www.google.com	172.217.24.132:443	fetch	serviceworker?pwa=search&hl=ja...
m=rQSi2?xjs=s1	200	http/1.1	www.google.com		script	rs=ACT90oE_LfZUBZIMaFuDp0...
m=rQSi2?xjs=s1	200	http/2+quic/43	www.google.com	172.217.24.132:443	fetch	serviceworker?pwa=search&hl=ja...
search?q&cp=0&client=...	200	http/2+quic/43	www.google.com	172.217.24.132:443	xhr	rs=ACT90oE_LfZUBZIMaFuDp0...
home_icon.svg	200	http/2+quic/43	www.gstatic.com	172.217.25.227:443	svg+xml	search?q=ホテル+information+sit...
save_icon.svg	200	http/2+quic/43	www.gstatic.com	172.217.25.227:443	svg+xml	search?q=ホテル+information+sit...
manage_searches_icon...	200	http/2+quic/43	www.gstatic.com	172.217.25.227:443	png	search?q=ホテル+information+sit...
settings_icon.svg	200	http/2+quic/43	www.gstatic.com	172.217.25.227:443	svg+xml	search?q=ホテル+information+sit...
privacy_advisor_icon.svg	200	http/2+quic/43	www.gstatic.com	172.217.25.227:443	svg+xml	search?q=ホテル+information+sit...
help_icon.svg	200	http/2+quic/43	www.gstatic.com	172.217.25.227:443	svg+xml	search?q=ホテル+information+sit...
feedback_icon.svg	200	http/2+quic/43	www.gstatic.com	172.217.25.227:443	svg+xml	search?q=ホテル+information+sit...
m=IM1CJf,MB3mMb,N...	200	http/1.1	www.google.com		script	rs=ACT90oE_LfZUBZIMaFuDp0...
m=IM1CJf,MB3mM...	200	http/2+quic/43	www.google.com	172.217.24.132:443	fetch	serviceworker?pwa=search&hl=ja...
bgasy?ei=wnbpXLqPN...	200	http/2+quic/43	www.google.com	172.217.24.132:443	xhr	rs=ACT90oE_LfZUBZIMaFuDp0...
preconnect.gif?0.69452...	200	http/2+quic/43	cdn.ampproject.org	172.217.31.129:443	gif	m=IM1CJf,MB3mMb,NBZ7u,Rqx...
Lp7pseFL264qrw_KcQ...	200	http/2+quic/43	travel-yahoo-co-jp.cdn.ampproject...	172.217.31.129:443	cert-chain+cbor	travel-yahoo-co-jp.cdn.ampprojec...
preconnect.gif?crossori...	200	http/2+quic/43	cdn.ampproject.org	172.217.31.129:443	gif	m=IM1CJf,MB3mMb,NBZ7u,Rqx...
information/	200	http/1.1	travel.yahoo.co.jp		text/html	travel-yahoo-co-jp.cdn.ampprojec...

https://travel.yahoo.co.jp › shisetsu

## ビジネスホテル シーズン - 【Yahoo!トラベル】 - Yahoo! JAPAN

ビジネスホテル シーズンの宿泊・予約情報。ビジネスホテル シーズンの宿泊予約はYahoo!トラベル。  
19/05/03 にこのページにアクセスしました。

評価  
2.9 ★★★★★ (8)

https://travel.yahoo.co.jp › shisetsu

## CALENDAR HOTEL - 【Yahoo!トラベル】 - Yahoo! JAPAN

10月、JR大津駅舎リニューアル！大津を変えるビッグプロジェクト始動！人々が集う大型複合施設にスタイリッシュなカプセル型ホテルがオープン！もちろん、施設内全てFREE Wi-Fi完備！  
19/05/19 にこのページにアクセスしました。

評価  
3.7 ★★★★★ (49)

# SXG Verifyの状況

The image shows a browser window displaying a hotel page for '品川プリンスホテル' (Shinagawa Prince Hotel) on Yahoo! Travel. The page includes a search bar, hotel details, and a promotional banner. The developer tools network panel is open, showing a 'Signed HTTP exchange' for a specific URL. The response headers and signature are visible, confirming the SXG status.

**品川・高輪・五反田**  
**品川プリンスホテル**  
★★★★☆ 3.76  
1,287人中 863人が満足

詳細・アクセス | 宿泊プラン | 写真ギャラリー | Yahoo! 地図

**宿おすすめ ツイン**  
【72時間タイムセール】ポイント最大20倍! 6月までのご宿泊に (室料のみ)  
定員1~2名 なし  
最大1300ポイント  
大人1名 1部屋 1泊 (税込) **6,563円~**  
プレミアム会員になれば、今すぐ1,495ポイント分割引OK!

**Network Panel:**  
Name: %3Fusqp=mq331AQNKAGYAeDs94r5wuS5fQ%253D%...  
Signed HTTP exchange  
Request URL: https://travel.yahoo.co.jp/amp/dhotel/shisetsu/HT10020059/information/  
Response code: 200  
Response headers:  
age: 2  
content-encoding: mi-sha256-03  
content-length: 39685  
content-security-policy: default-src \* blob: data;;report-uri https://csp-collector.appspot.com/csp/amp;script-src blob: https://cdn.ampproject.org/rtv/ https://cdn.ampproject.org/v0/ https://cdn.ampproject.org/viewer/;style-src 'unsafe-inline' https://cdn.materialdesignicons.com https://cloud.typography.com https://fast.fonts.net https://use.typekit.net;object-src 'none'  
content-type: text/html; charset=UTF-8  
date: Sat, 25 May 2019 14:24:23 GMT  
digest: mi-sha256-03=F0168RVz7CNehY5UVLbsMwMRYa4cgNEtq7Myiftt7w8=  
link: <https://cdn.ampproject.org/v0.js>;rel=preload;as=script,<https://cdn.ampproject.org/v0/amp-analytics-0.1.js>;rel=preload;as=script,<https://cdn.ampproject.org/v0/amp-carousel-0.1.js>;rel=preload;as=script,<https://cdn.ampproject.org/v0/amp-iframe-0.1.js>;rel=preload;as=script  
p3p: policyref="http://privacy.yahoo.co.jp/w3c/p3p\_jp.xml", CP="CAO DSP COR CUR ADM DEV TAI PSA PSD IVAI IVDI CONI TELO OTPI OUR DELI SAMI OTRI UNRI PUBI IND PH L HEA PRE GOV"  
server: ATS  
vary: Accept-Encoding  
x-content-type-options: nosniff  
x-ua-compatible: IE=Edge  
Signature  
Label: label  
Signature:  
30 44 02 20 58 C8 50 7D 06 22 02 0A 18 E3 39 27 6D 32 87 9E B5 FB 70 55 0D 0F 93 4D 28 22 A5 DB E7 DD 0C C6 02 20 10 A4 7C 14 6E 73 55 A6 D6 1F AA 74 71 31 25 29 89 CA  
Certificate URL: https://travel-yahoo-co-jp.cdn.ampproject.org/crt/s/travel.yahoo.co.jp/amppkg/cert/Lp7pseFL264qrw\_KcQKmuu2GWrLM7LLr-I6YCb\_o6OE  
Integrity: digest/mi-sha256-03  
Certificate SHA256:  
2E 9E E9 B1 E1 4B DB AE 2A AF 0F CA 71 02 A6 BA ED 86 5A B2 CC EE 52 EB F8 8E 98 09 BF E8 E8 E1  
Validity URL: https://travel.yahoo.co.jp/amppkg/validity  
Date: Fri, 24 May 2019 14:24:24 GMT  
Expires: Fri, 31 May 2019 14:24:24 GMT  
Certificate  
Subject: travel.yahoo.co.jp  
Valid from: Wed, 06 Feb 2019 00:00:00 GMT  
Valid until: Thu, 01 Aug 2019 12:00:00 GMT  
Issuer: DigiCert ECC Secure Server CA

devtool上ネットワークパネルのPreviewで確認できます



# SXGの状況

- ChromeM73より default で enable (バージョン:b3)
- iOS版は非対応。現状モバイル環境でSXGが使えるのは Android Chromeのみ
- MacOS版IE Edge(Chromiumベース)でもSXG動作確認済
- Google Searchで4月中旬よりSXG/AMPを正式対応
- CloudflareもSXG機能提供開始(GUIベース)
- 標準化… まだわかりません。DISPATCH->ESCAPE  
Workshop

# Web Packaging仕様概要

Binary JSONの  
シリアライズ

HTTPボディの  
Hash Digest

より扱いやすいHTTP  
ヘッダの記述書式

WHATWG  
Fetch

RFC7049  
CBOR

draft-thomson-  
http-mic

draft-ietf-httpbis-  
header-structure

Loading Signed  
Exchanges

draft-yasskin-wpack-  
bundled-exchanges

draft-yasskin-http-origin-  
signed-response

Fetchに対する  
モンキーパッチ

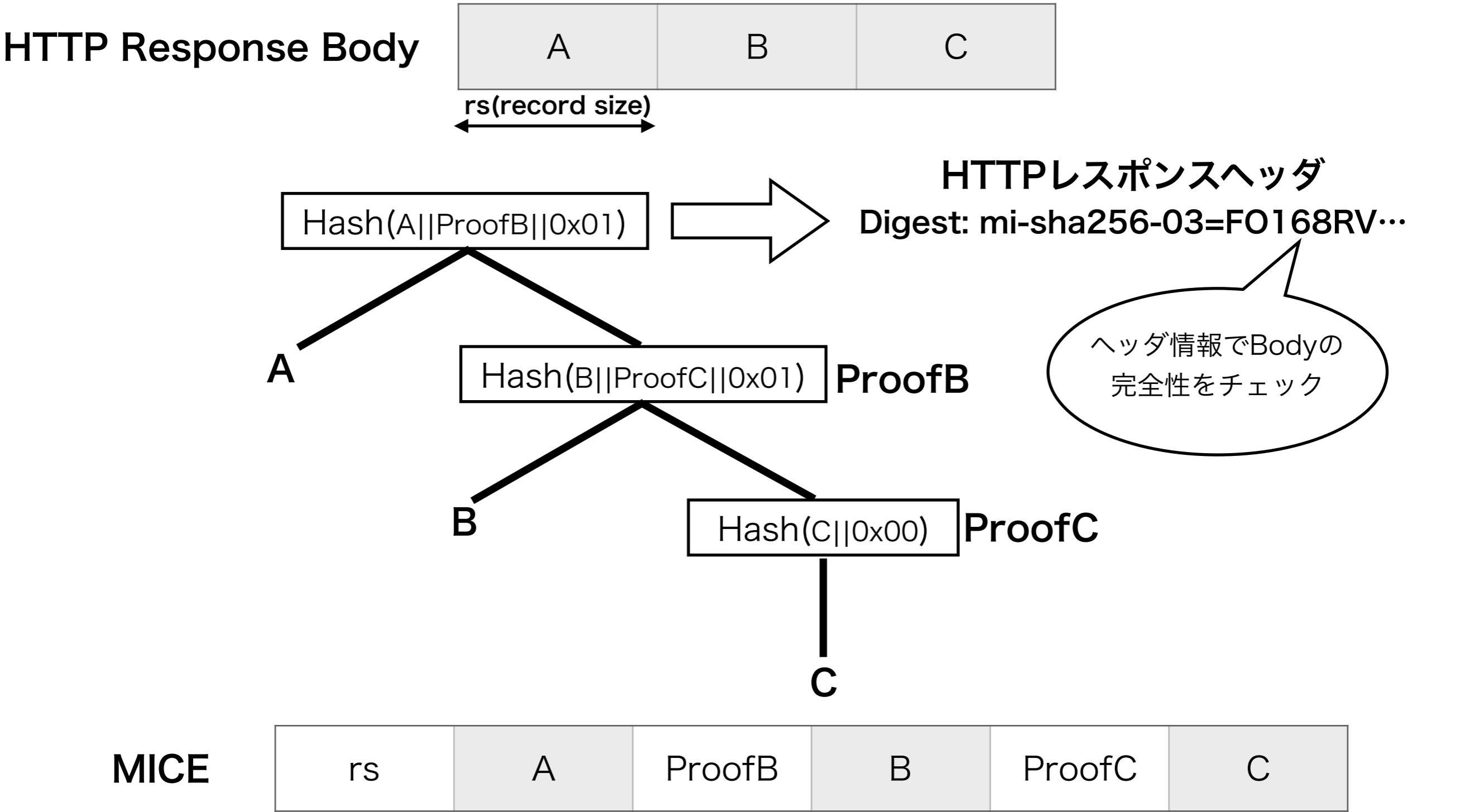
Bundle

SXG

(b3:2019年5月時点)

Web Packaging仕様

# Merkle Integrity Content Encoding



SXG仕様では record sizeは 16KB以下に制限

# SXGファイルの中身 (b3)

sxg1-b3 (8)	fallbackUrl length (2)	fallbackURL	sigLength (3)	headerLength (3)	signature	signedHeaders	payload body
----------------	------------------------------	-------------	------------------	---------------------	-----------	---------------	-----------------

sxg1-b3	マジック
fallbackURL	SXG検証が失敗した場合にアクセスするURL
signature	署名データ
signedHeaders	HTTPレスポンスヘッダ (CBOR形式)
payload body	HTTPレスポンスのボディ (MICE形式)

sig	署名値
integrity	HTTPレスポンスボディのハッシュアルゴリズム
validity-url	新しい署名データを取得URL (現在未実装)
cert-url	証明書データのURL (署名対象外)
cert-sh256	証明書データのハッシュ値
ed25519key	署名検証する公開鍵 (現在未実装)
date	署名した時間
expire	署名の有効期限 (最大7日間)

# SXGで署名しているデータ

0x20,0x20,0x20.....0x20 (64)	
HTTP Exchange 1(15)	
0x00(1)	
cert-sha256(32)	
validity-url len (8)	validity-url
date(8)	
expires(8)	
requestUrl len(8)	requestUrl
responseHeaders len(8)	responseHeaders

b3からrequestヘッダは除外

- SXG証明書の秘密鍵を使って ecdsa-with-SHA256(secp256r1) で署名
- SXG証明書の公開鍵を使って署名を Verify
- 署名のVerifyが成功してレスポンスボディのMICEチェックができたならSXGがvalid



# SXGの中身2

```
ohtsu@opro:~$ dump-signedexchange -i shinagawa_prince.sxg
format version: 1b3
request:
  method: GET
  uri: https://travel.yahoo.co.jp/amp/dhotel/shisetsu/HT10020059/information/
  headers:
response:
  status: 200
  headers:
    P3p: policyref="http://privacy.yahoo.co.jp/w3c/p3p_jp.xml", CP="CA0 DSP COR CUR ADM DEV TAI PSA PSD IV
    Content-Type: text/html; charset=UTF-8
    Content-Length: 39685
    X-Ua-Compatible: IE=Edge
    Server: ATS
    Content-Encoding: mi-sha256-03
    X-Content-Type-Options: nosniff
    Age: 0
    Date: Sat, 25 May 2019 17:39:18 GMT
    Link: <https://cdn.ampproject.org/v0.js>;rel=preload;as=script,<https://cdn.ampproject.org/v0/amp-anal
    ject.org/v0/amp-carousel-0.1.js>;rel=preload;as=script,<https://cdn.ampproject.org/v0/amp-iframe-0.1.js>;r
    Vary: Accept-Encoding
    Digest: mi-sha256-03=F0168RVz7CNehY5UVLbsMwMRYa4cgNEtq7Myiftt7w8=
    Content-Security-Policy: default-src * blob: data:;report-uri https://csp-collector.appspot.com/csp/am
    n.ampproject.org/viewer/;style-src 'unsafe-inline' https://cdn.materialdesignicons.com https://cloud.typog
    ro.fontawesome.com https://use.fontawesome.com https://use.typekit.net;object-src 'none'
    signature: label; sig=*MEUCIQDKYCYzUX/ia0KFsCh/9T568s0dkcI39Ld8r5LhSnvaSAIgmIzfLG9ebiLe16jK+ifc07PyhbhZ0c1
    /travel.yahoo.co.jp/amppkg/cert/Lp7pseFL264qrw_KcQKmuu2GWrLM7LLr-I6YCb_o60E"; cert-sha256=*Lp7pseFL264qrw/
    payload [39757 bytes]:
    @<!doctype html><html i-amhtml-layout i-amhtml-no-boilerplate lang=ja transformed="google;v=1" ⚡><head>
```

# CertChain+CBORの中身

U+F4DC 📜 Scroll  
U+26D3 🗉 Chains

```
[ [ '🗉',  
  { cert:  
    <Buffer 30 82 04 f1 30 82 04  
  obsp:  
    <Buffer 30 82 01 34 0a 01 00  
  { cert:  
    <Buffer 30 82 03 ac 30 82 02
```

CBOR形式

```
ohtsu@opro:~$ dump-certurl -i shinagawa_prince.cert  
Certificate #0:  
Subject: travel.yahoo.co.jp  
Valid from: 2019-02-06 00:00:00 +0000 UTC  
Valid until: 2019-08-01 12:00:00 +0000 UTC  
Issuer: DigiCert ECC Secure Server CA  
Embedded SCT:  
  LogID: u9nfvB+KcbWTlCOXqpJ7RzhXlQqrUugakJZkNo4e0YU=  
  LogID: h3W/51l8+IxDmV+9827/Vo1HVjb/SrVgwbTq/16ggw8=  
Has canSignHttpExchangesDraft extension  
OCSP response:  
Status: 0 (good)  
ProducedAt: 2019-05-24 05:44:53 +0000 UTC  
ThisUpdate: 2019-05-24 05:44:53 +0000 UTC  
NextUpdate: 2019-05-31 04:59:53 +0000 UTC  
Certificate #1:  
Subject: DigiCert ECC Secure Server CA  
Valid from: 2013-03-08 12:00:00 +0000 UTC  
Valid until: 2023-03-08 12:00:00 +0000 UTC  
Issuer: DigiCert Global Root CA
```

90日以内、現在有効??

CT  
ログ有?

SXG拡張有?

現在の時刻  
で有効?

rootCAまで  
署名検証



# SXG禁止HTTPヘッダ

## Hop-by-Hopレスポンスヘッダ

Connection
Keep-Alive
Proxy-Connection
Trailer
Transfer-Encoding
Upgrade

## Statefulレスポンスヘッダ

Authentication-Control
Authentication-Info
Clear-Site-Data
Optional-WWW-Authenticate
Proxy-Authenticate
Proxy-Authenticate-Info
Public-Key-Pins
Sec-WebSocket-Accept
Set-Cookie
Set-Cookie2
SetProfile
Strict-Transport-Security
WWW-Authenticate

**SXG化するAMPサーバからのレスポンスに上記ヘッダが入っていないか注意する  
amppkgではErrorOnStatefulHeadersの設定で制御できます。**

# amppackager

## について

[github.com/ampproject/amppackager/](https://github.com/ampproject/amppackager/)

release branch: Production用ブランチ

master branch: 開発ブランチ

# amppackager 提供コマンド

- `cmd/amppkg/` amppkg本体
- `cmd/amppkg_dl_sxg/` SXGと証明書をダウンロード
- `cmd/amppkg_test_cache/` SXGを提供する簡易キャッシュサーバ
- `cmd/gateway_server/` gRPCでSXGを生成するゲートウェイサーバ
- `cmd/transform/` AMP最適化を行うコマンド

# amppkg.toml(master)

Port	Listenポート (default:8080)		
LocalOnly	localhostでListenすることを強制 (default: false)		
CertFile	SXG証明書のファイル(サーバ証明書,中間証明書, PEM形式)		
KeyFile	SXG証明書の秘密鍵ファイル(PEM形式)		
OCSPCache	OCSPデータのキャッシュファイルのパス		
ForwardedRequestHeader	fetchする際に転送するリクエストヘッダ		
[[URLSet]]			
	[URLSet.Sign]	署名用の設定(必須)	
		Domain	署名するドメイン
		PathRE	署名を許可するPath(default: .*)
		PathExcludeRE	署名を許可しないPath
		QueryRE	署名を許可するQueryパラメータ (default: "")
		ErrorOnStatefulHeader	statefulヘッダがあったらproxyさせるか削除するか
		MaxLength	URLの最大長(default: 2000)
	[URLSet.Fetch]	AMPコンテンツをFetchする設定(オプション)	
		Scheme	fetchを許可するschema (default: https)
		SamePath	署名と同じpathでfetchすることを強制させる
		DomainRE	fetchを許可するドメインのパターン
		Domain	fetchするドメイン
		PathRE	fetchを許可するPATH (default:*.*)
		QueryRE	fetchを許可するQueryパラメータ (default: "")

# amppkg

## コマンドラインフラグ

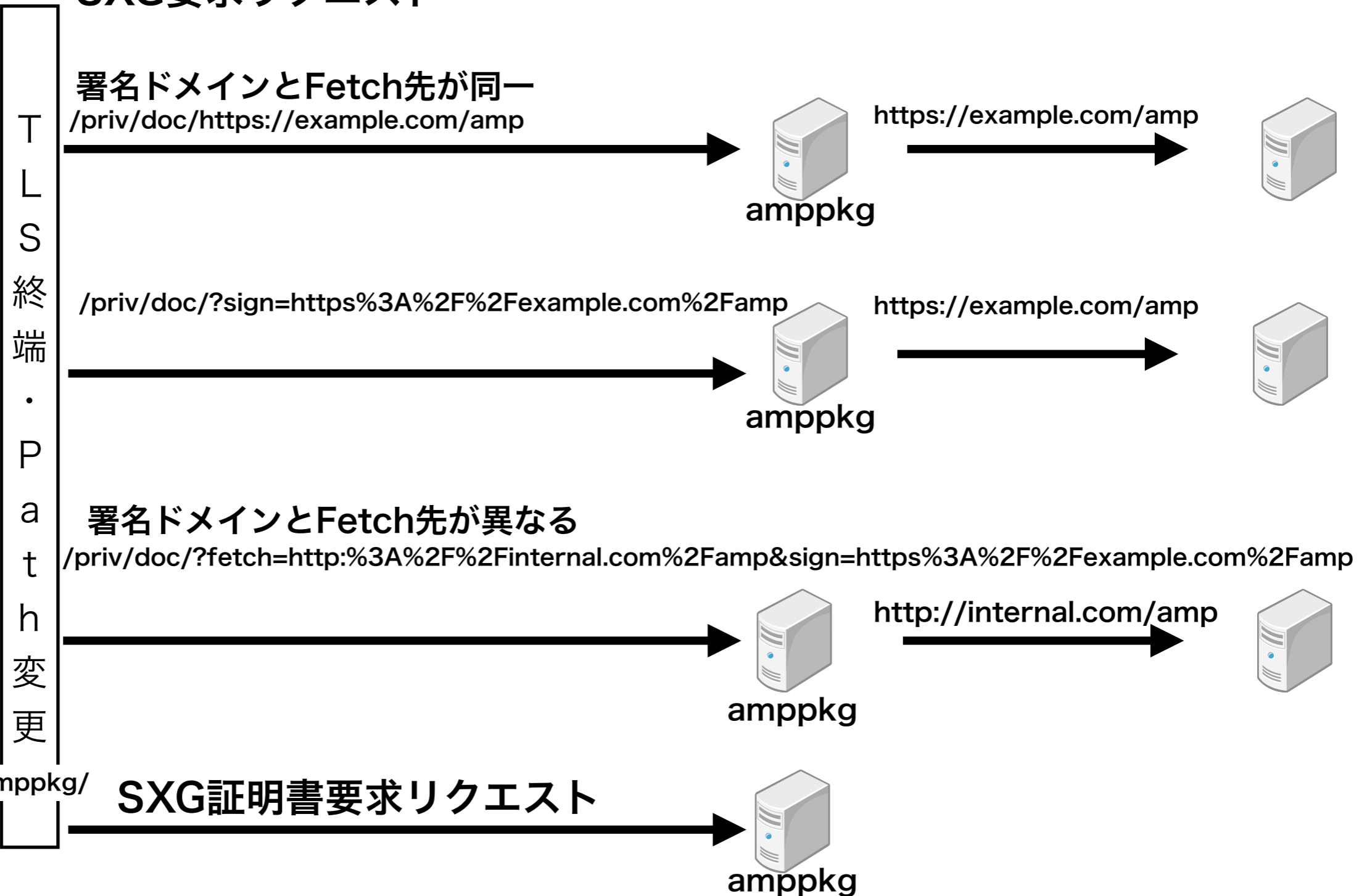
-config	configファイルの指定
-development	<ul style="list-style-type: none"><li>• CanSignHTTPExchange拡張がない証明書の利用を許可する</li><li>• localhost宛のURLだけ許可</li><li>• AMP-Cache-Transform/Acceptヘッダは必要ない</li></ul>
-invalidcert	CanSignHTTPExchange拡張がない証明書の利用を許可する

ログは標準出力のみ

# amppkgへのリクエスト

https://example.com/amp

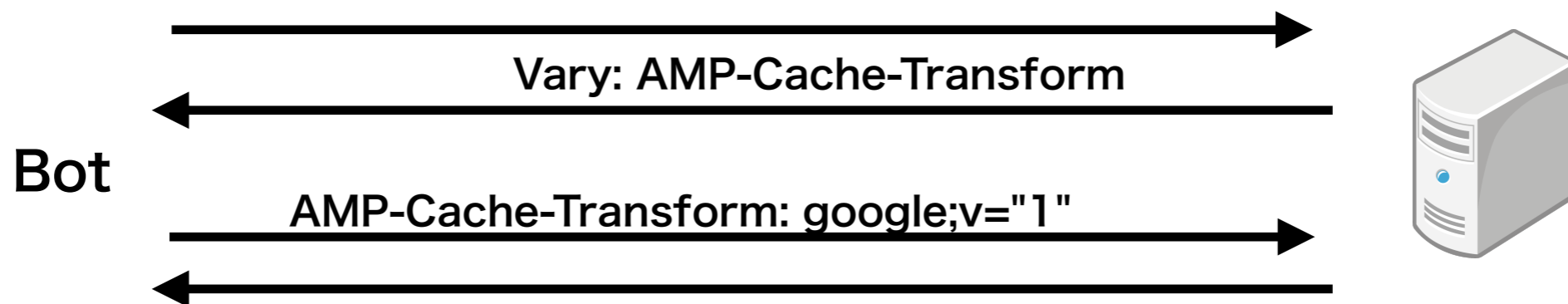
SXG要求リクエスト



amppkg前段でTLS終端をして、外部から直接/priv/docに接続させないこと

# Transformer

- これまでAMP CacheでGoogleがAMP最適化処理を行ってきた(AMPのrun time valueの入れ込みやinline化 etc)
- SXGでは署名した後では最適化が不可能。SXG化の前にやる必要がある。
- Transformerの指定をAMP-Cache-Transformerヘッダでネゴシエーションする。バージョンは6-8週間で上がる予定
  - AMP-Cache-Transform: google;v="1..3,5"
  - AMP-Cache-Transform: any



# SXG証明書

- SXGをサービスで提供するために必要不可欠
- 通常のECC証明書(secp256)にSXG拡張が付いたもの
- 通常のHTTPSサーバ用途の証明書に使うことは禁止
- 現在Digicert社のみ発行
- 2019年5月1日より
  - 証明書の有効期限を90日に制限
  - DNSCAAレコード登録を必須化

SXG拡張



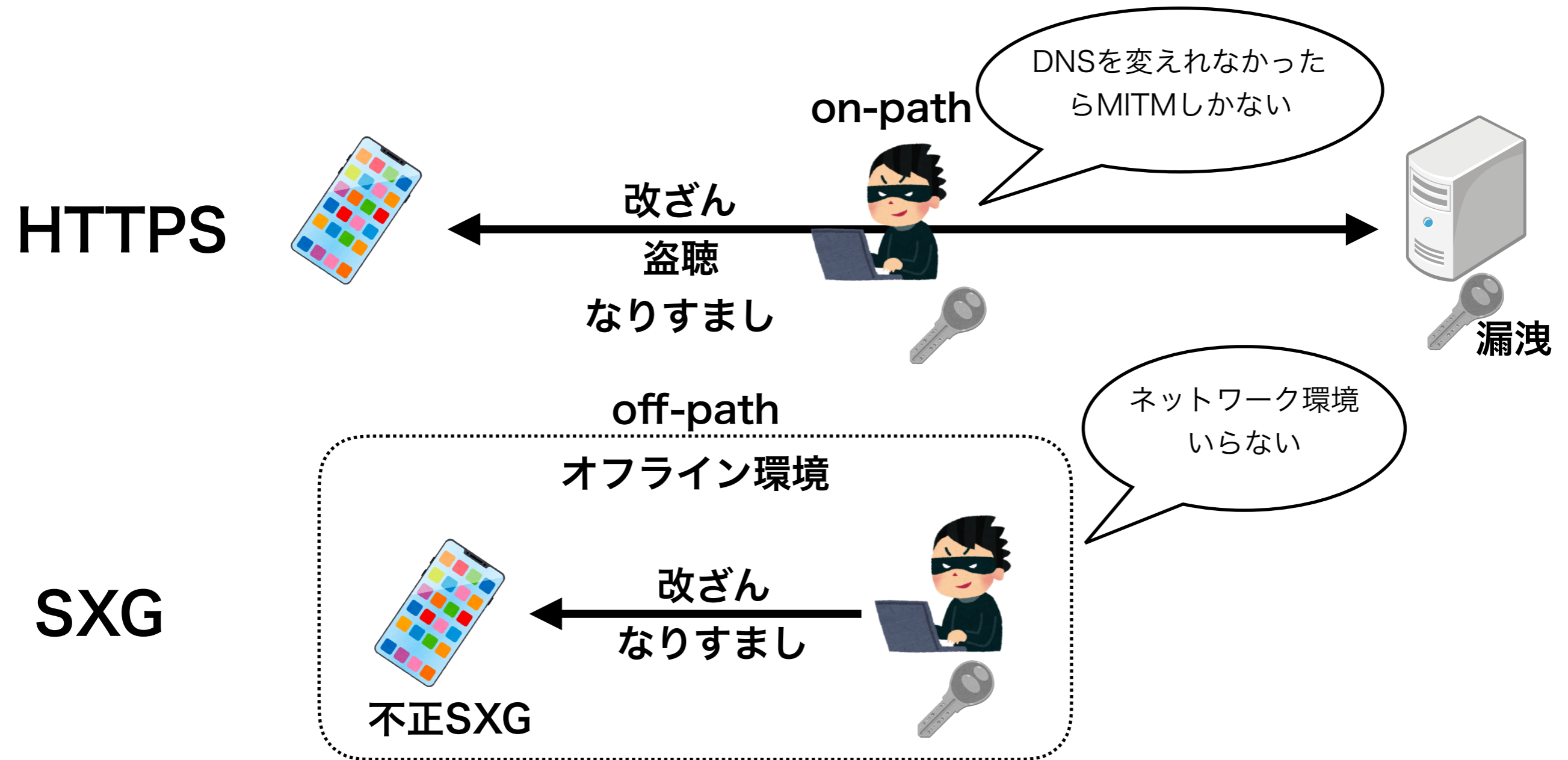
```
X509v3 Basic Constraints: critical
CA:FALSE
1.3.6.1.4.1.11129.2.1.22:
..
CT Precertificate SCTs:
Signed Certificate Timestamp:
```





# HTTPSとSXGのセキュリティの違い

## 秘密鍵が漏洩した場合



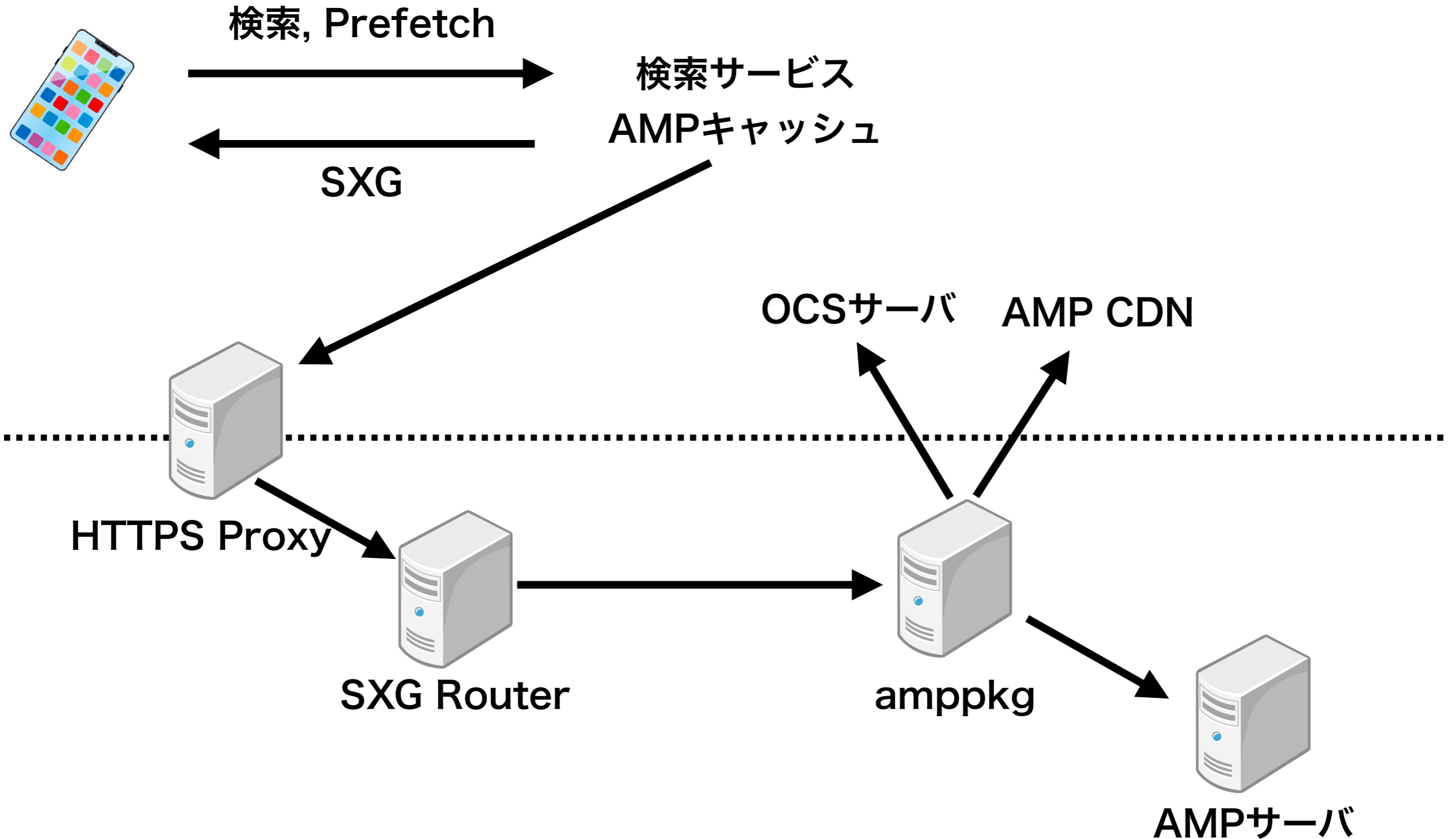
CAAで証明書の不正発行・誤発行を防ぎ

短期間(90日)のSXG証明書で危殆化時のリスクを低減

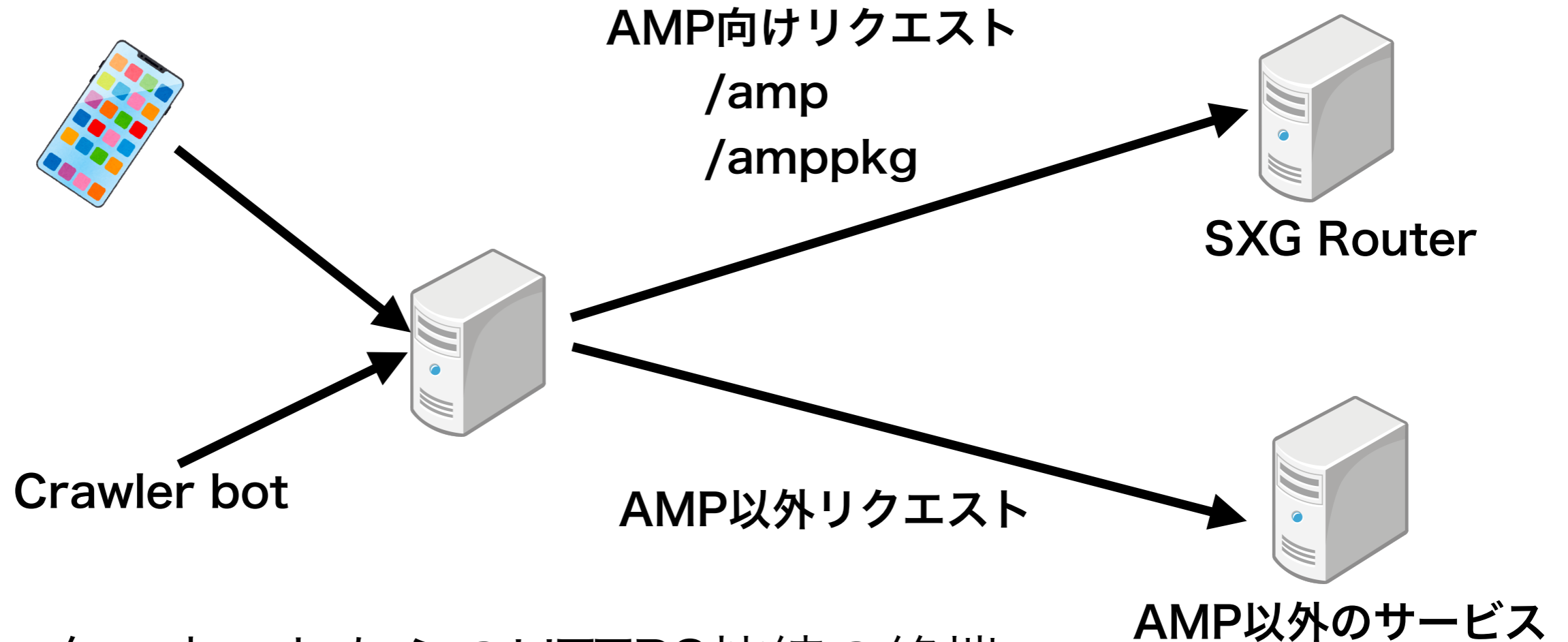
SXG/AMP

システム事例

# AMP/SXGシステム概要

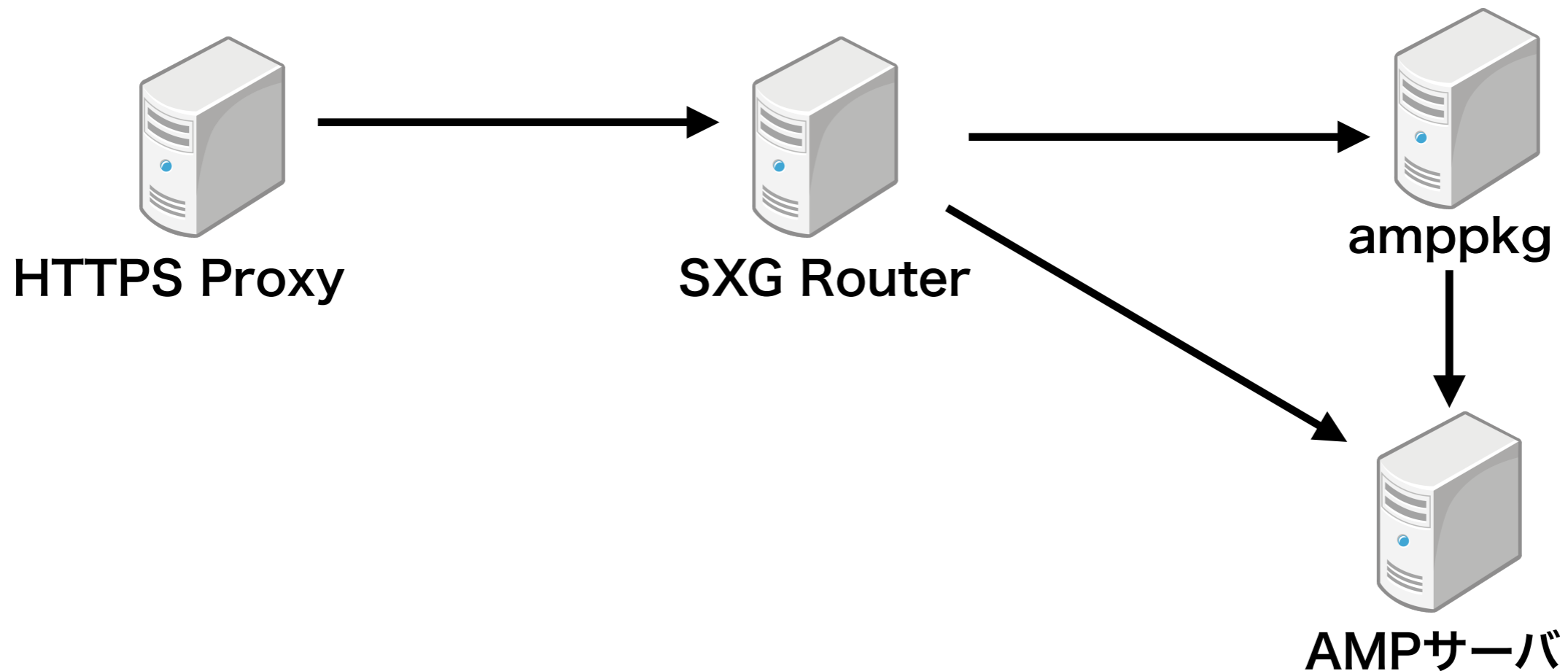


# HTTPS Proxy



- インターネットからのHTTPS接続の終端
- キャッシュ機能
- 内部サービスへの振り分け (/amp AMPサービス, /amppkg SXG証明書取得)

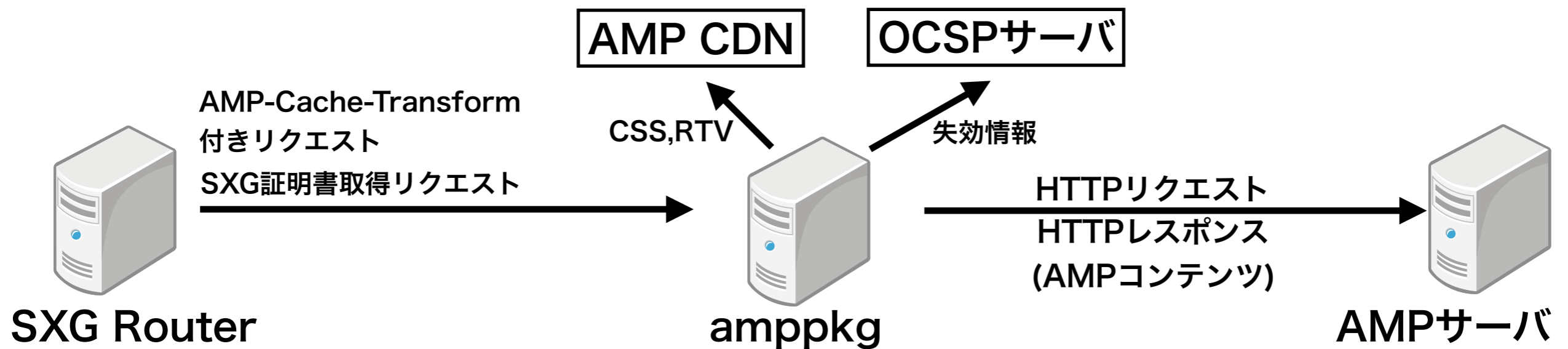
# SXG Router



- CrawlerにSXG対応であることを知らせる(Vary: AMP-Cache-Transform)
- SXG取得リクエスト(AMP-Cache-Transform: google;v=..)が来たらamppkgにふる。
- リクエストを amppkg用のquery parameterに変更

# amppkg

<https://github.com/ampproject/amppackager>



- AMPコンテンツからSXGを生成し提供する(最大4MB)
- クライアントの時間ずれを考慮して署名期間は1日前から6日後
- SXG生成時にAMP最適化(Transform)を行う
- SXG証明書とOCSPをまとめたデータ(cert+cbor)を生成し、提供する
- パブリックキャッシュに適さないヘッダのチェックや削除を行う
- statusCode 200以外は基本スルー(proxy)

SXG導入振り返り



# SXG/AMPシステム導入、振り返り

1. 既存インフラへの影響を最小限にして、導入が可能だった。
2. ユーザへの直接リクエストの影響をあまり気にせずにした(主要リクエストがBotのクローリングであったため)
3. 事前にStaging環境でのテストが限定的だった。BotクローラやAMPキャッシュ化の試験はリリース後にしかできない。

# SXG/AMPシステム導入に関する する注意事項

- キャッシュ可能なコンテンツか？ (SXG禁止ヘッダ)
- 個人情報やセキュリティ情報が入っていないか？
- Same Originになったらエラーにならないか？ (e.g. AMP-iframe)
- Soft404(not foundを200で返す)とかしていないか？

# まとめ

originを入れ替えるSigned HTTP Exchangesは、これまでのWebプロトコルの概念を根本的に変える技術です。

この技術によって Publisher/Distributor それぞれの関係が将来大きく変わる可能性があります。

今後、SXGが天使となるのか、それとも悪魔となるのか、皆さんでその影響をよく考えた上でSXGを判断して下さい。