



そろそろSSL通信に本気出して 向き合ってみる

How should we treat SSL traffic?

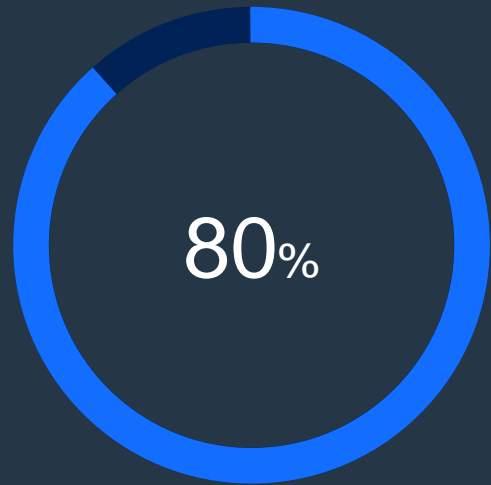
フォーティネットジャパン コンサルティングSE 杉井義久

本セッションにあたって

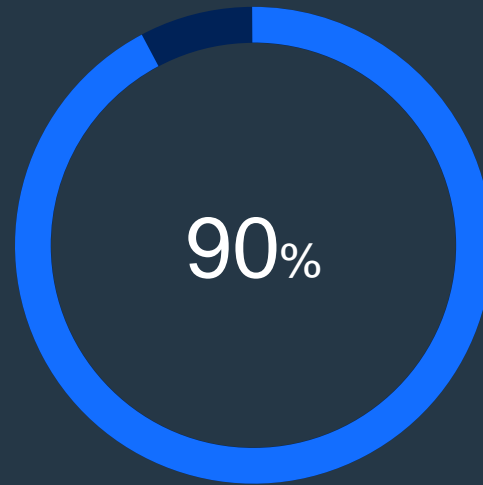
- 個人的な所感ですが、インターネットはできる限り自由であるべきだと考えています。
- もしも自分が所属組織ネットワークセキュリティの運用・管理をまかされたら、という前提で聞いて頂けると幸いです。
- わかりやすさを優先し、本セッションでは“SSL”というタームを利用しますが、厳密にはSSL3.0の利用は禁止され、TLSへ移行しております。

SSL通信の現状を探ってみる

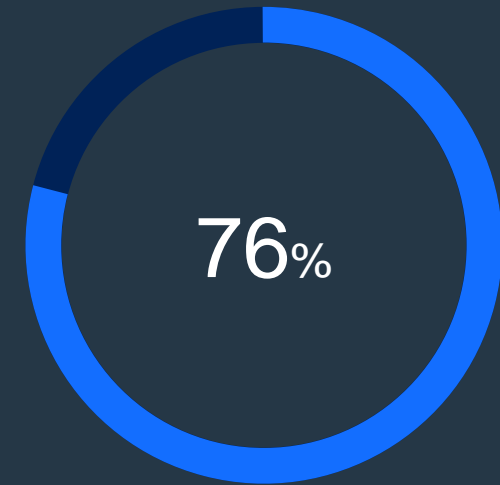
SSL通信の現状を探ってみる



Mobile

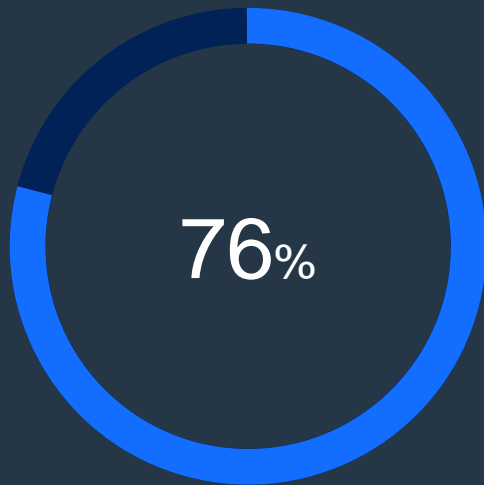


Google



Enterprise

SSL通信の現状を探ってみる

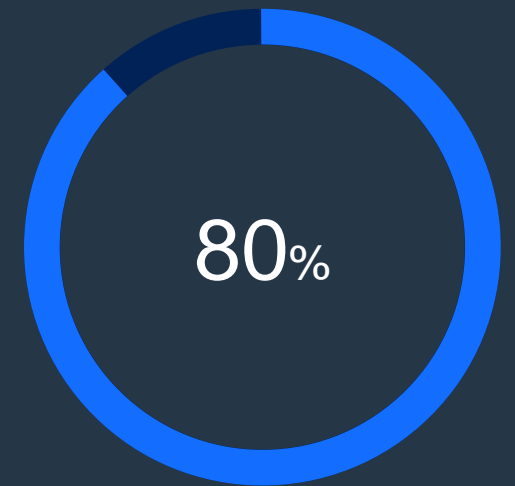
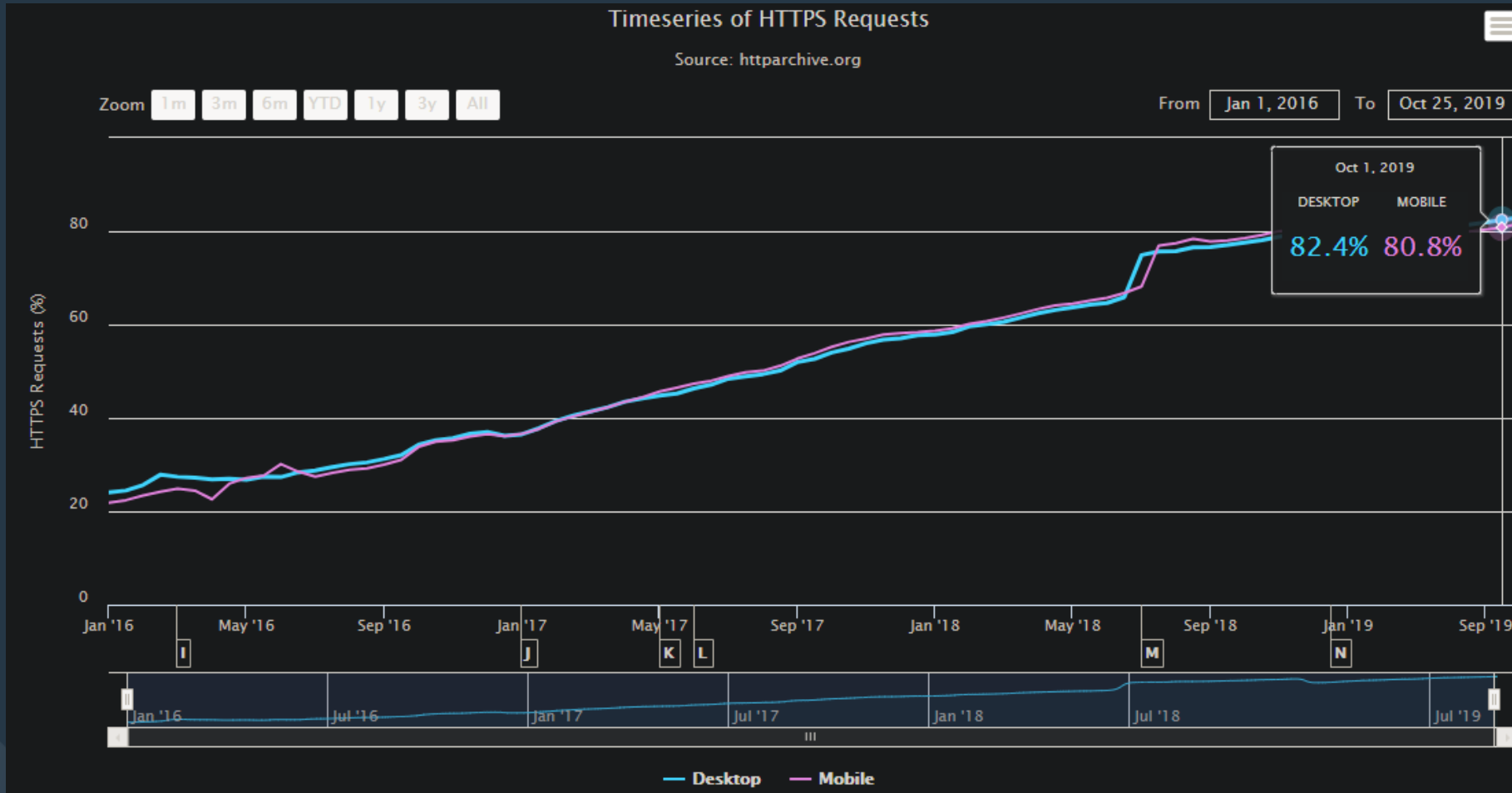


全上場企業における
常時SSL化対応状況
(2019年12月)

常時SSL化 対応済み	76.2% (2810社)
常時SSL化 未対応	23.8% (880社)

引用元: feedtailor社: 国内上場企業Webサイト常時SSL化対応状況レポート
https://www.feedtailor.jp/report_aossl

SSL通信の現状を探ってみる

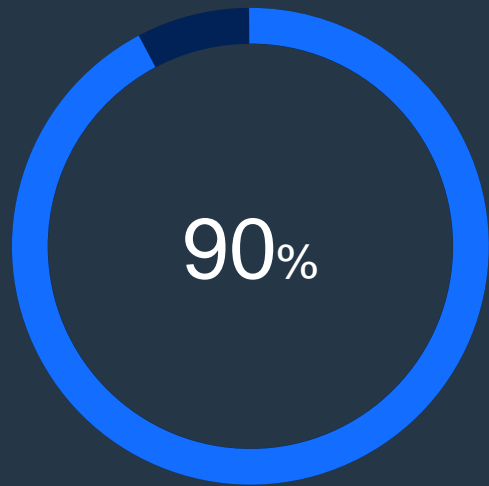


HTTPSリクエストの割合

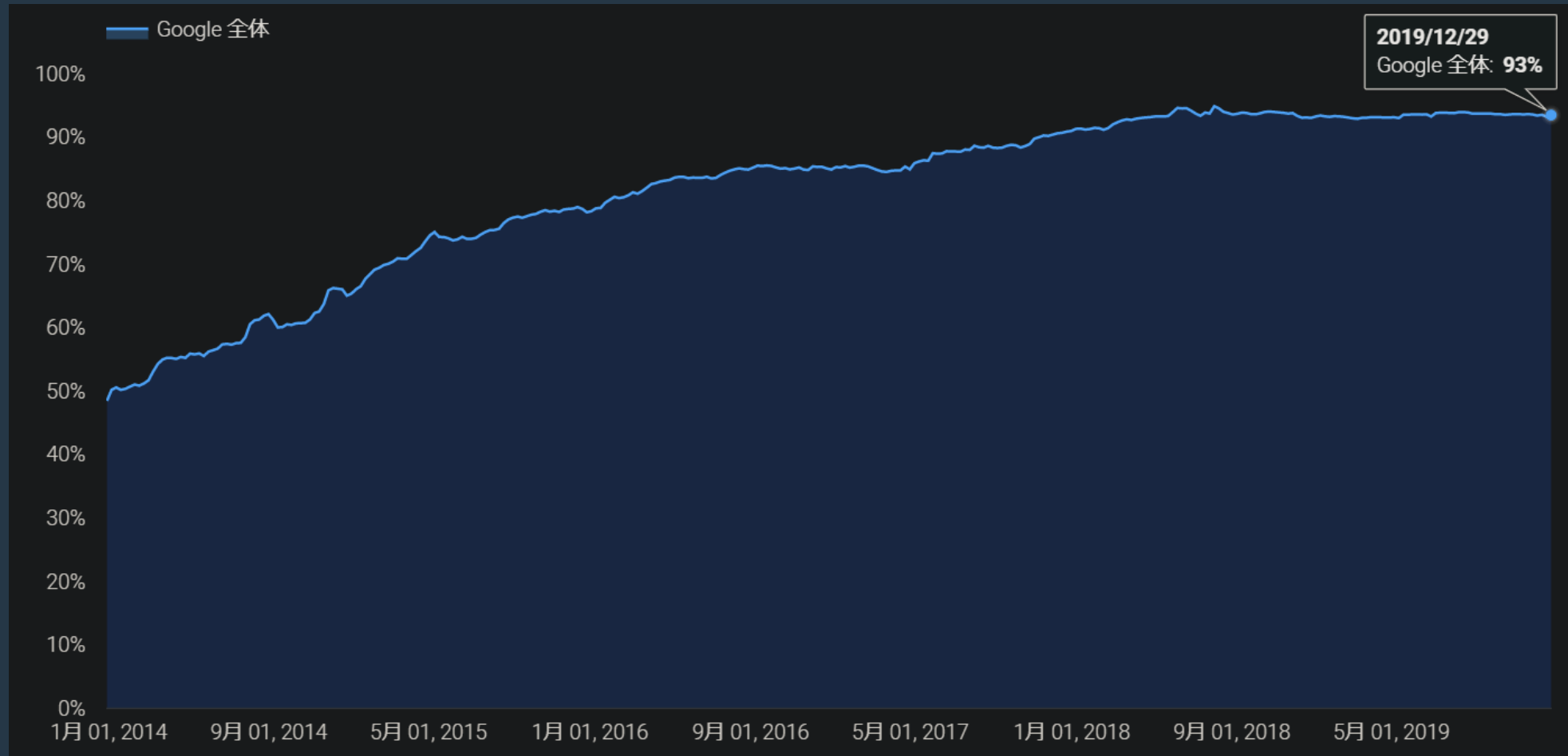
引用元: [http archive: State of Web](http://httparchive.org)

<https://httparchive.org/reports/state-of-the-web>

SSL通信の現状を探ってみる



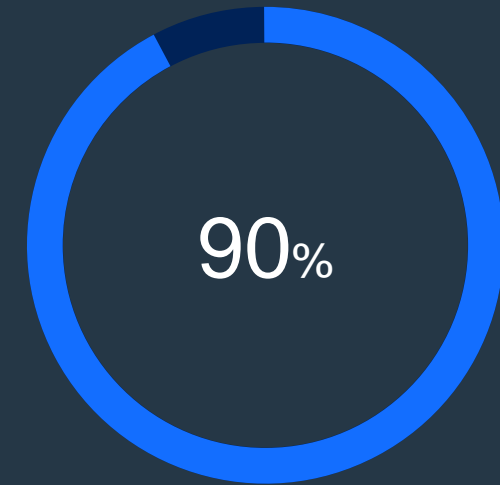
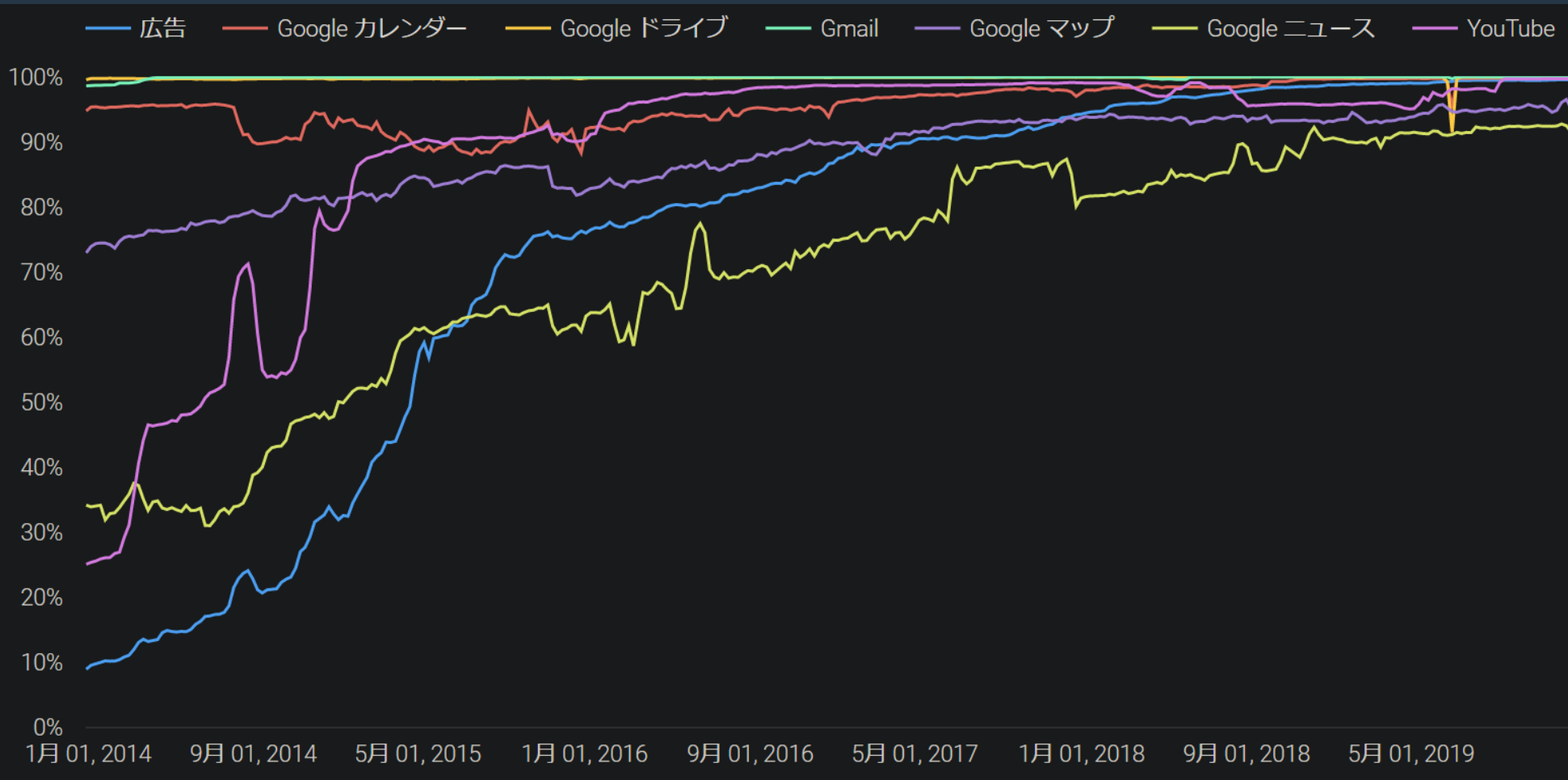
Googleサービス



引用元: Google: 透明性レポート

<https://httparchive.org/reports/state-of-the-web>

SSL通信の現状を探ってみる

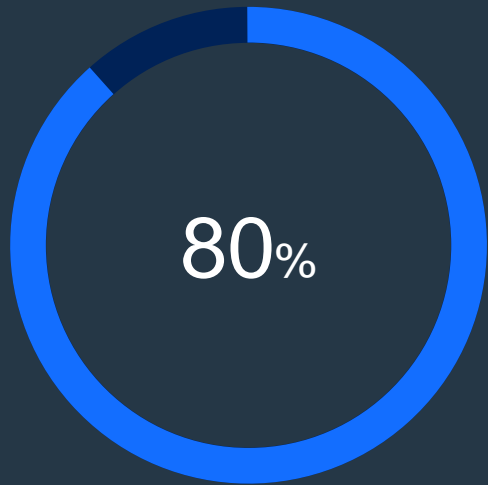


Googleサービス

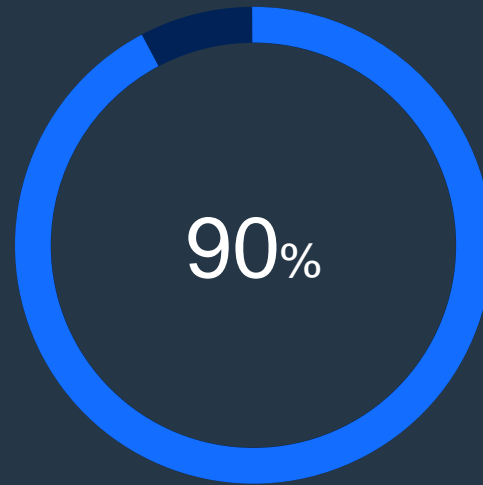
引用元: Google: 透明性レポート

<https://httparchive.org/reports/state-of-the-web>

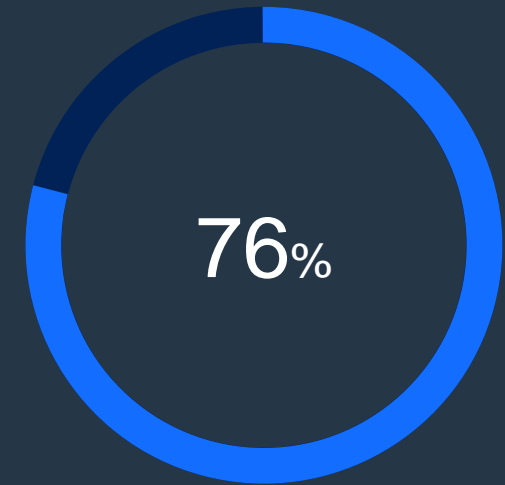
常時SSL化 - ざっくり8割



Mobile



Google



Enterprise

SSLについておさらいしてみる



実在証明



暗号化通信

実在証明



実在証明



申請者

確認します



認証局

実在証明



申請者

確認中



認証局

実在証明



申請者

確認中



実在証明



申請者

確認とれました



認証局

実在証明



認証局から発行された証明書だと



The screenshot shows the homepage of the Japan Network Operators' Group (JANOG). The browser address bar displays <https://www.janog.gr.jp>. The website header includes the JANOG logo and the text "Japan Network Operators' Group" and "日本ネットワーク・オペレーターズ・グループ". A navigation menu contains links for HOME, General Information, Meetings, Mailing List, Archive, Resource, Sponsors, and English Page. The main content area features a large banner with the text "Japan Network Operators' Group" and a background image of green fiber optic cables. To the right, there is a promotional image for "JANOG45 in Sapporo" with a night cityscape background. Below the banner, there is a section titled "下記の日程にて、JANOG45 Meeting を開催します。" (The JANOG45 Meeting will be held on the following schedule.) followed by details: "開催日程: 2020年1月22日(水)~24日(金)", "開催場所: 北海道札幌市", "参加費: 無料(本会議)・有料(懇親会)", and "ホスト: 北海道総合通信網株式会社・株式会社ネクステック". There are also links for "[JANOG45 Meeting Webサイト]" and "[JANOG45 若者支援プログラムについてはこちら]". On the right side, a text block states: "JANOG45は [北海道総合通信網株式会社](#)・[株式会社ネクステック](#) のホストにより開催します。"

認証局から発行された証明書だと



認証局から発行された証明書だと



認証局から発行された証明書だと

証明書

*.janog.gr.jp

JPRS Domain Validation Authority - G2

Subject Name _____

Common Name *.janog.gr.jp

Issuer Name _____

Country JP

Organization Japan Registry Services Co., Ltd.

Common Name JPRS Domain Validation Authority - G2

Validity _____

Not Before 2019/1/28 16:15:57 (Asia/Tokyo)

Not After 2021/1/31 23:59:59 (Asia/Tokyo)

Subject Alt Names _____

DNS Name *.janog.gr.jp

DNS Name janog.gr.jp

認証局から発行された証明書だと

証明書マネージャー



あなたの証明書

個人証明書

サーバー証明書

認証局証明書

*.janog.gr.jp

認証局を識別するため以下の証明書が登録されています

証明書名と発行者名

セキュリティデバイス

JPRS Domain Validation Authority - G2

Software Security Device

KDDI Web Communications Certification Authority 2

Software Security Device

KDDI Web Communications Certification Authority

Software Security Device

NII Open Domain CA - G5

Software Security Device

NII Open Domain CA - G4

Software Security Device

FujiSSL Public Certification Authority - G2

Software Security Device

FujiSSL Public Certification Authority - G1

Software Security Device

Security Communication RootCA2

Builtin Object Token

KDDI Web Communications Certification Authority 3

Software Security Device

FujiSSL Public Validation Authority - G3

Software Security Device

表示...

信頼性を設定...

インポート...

エクスポート...

削除または信頼しない..

OK

信頼された認証局を通していない証明書(=オレオレ証明書)だと



The screenshot shows the homepage of the Japan Network Operators' Group (JANOG). The browser address bar displays <https://jan0g.gr.jp>. The website header includes the JANOG logo and the text "Japan Network Operators' Group" and "日本ネットワーク・オペレーターズ・グループ". A navigation menu contains links for HOME, General Information, Meetings, Mailing List, Archive, Resource, Sponsors, and English Page. The main content area features a large banner with the text "Japan Network Operators' Group" and a background image of fiber optic cables. To the right, there is a smaller banner for "JANOG45 in Sapporo". Below the main banner, there is a text block announcing the "JANOG45 Meeting" with details on dates, location, fees, and hosts. A link to the meeting website is provided. To the right of this text, there is a small text block explaining that the event is hosted by Hokkaido Integrated Communications Network Co., Ltd. and NextStack Co., Ltd.

JANOG
Japan Network Operators' Group
日本ネットワーク・オペレーターズ・グループ

HOME | General Information | Meetings | Mailing List | Archive | Resource | Sponsors | English Page

Japan Network Operators' Group

JANOG45 in Sapporo

下記の日程にて、**JANOG45 Meeting** を開催します。

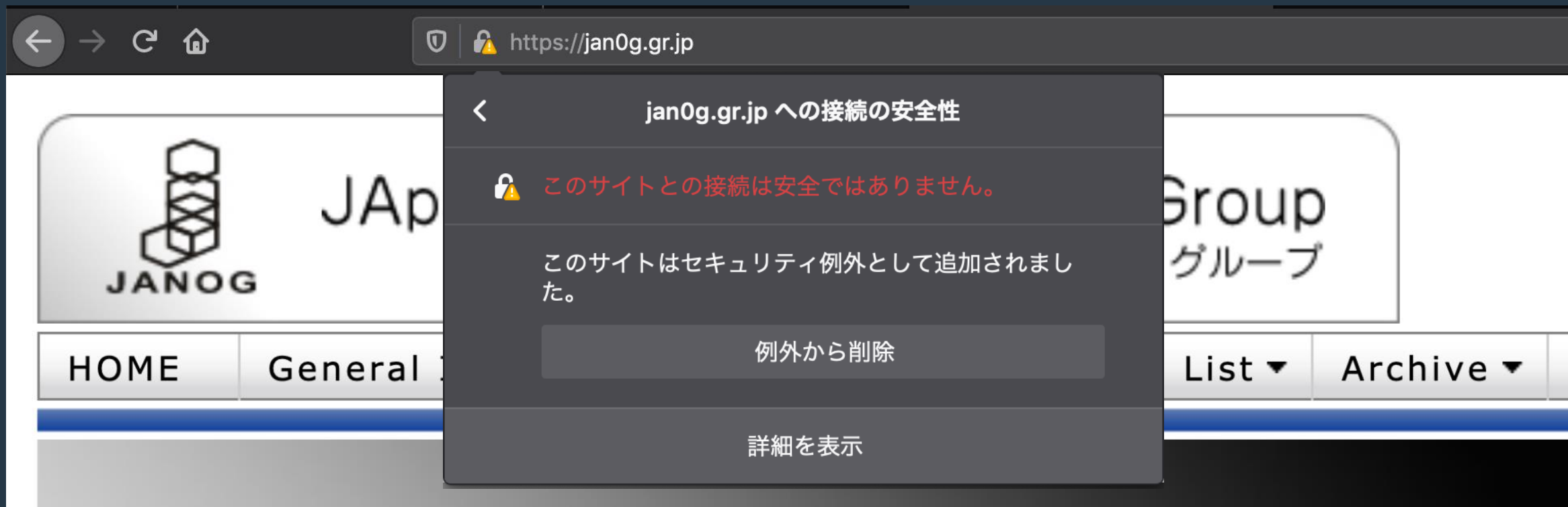
開催日程: 2020年1月22日(水)~24日(金)
開催場所: 北海道札幌市
参加費: 無料(本会議)・有料(懇親会)
ホスト: 北海道総合通信網株式会社・株式会社ネクステック
[\[JANOG45 Meeting Webサイト\]](#)

JANOG45は [北海道総合通信網株式会社](#)・[株式会社ネクステック](#) のホストにより開催します。

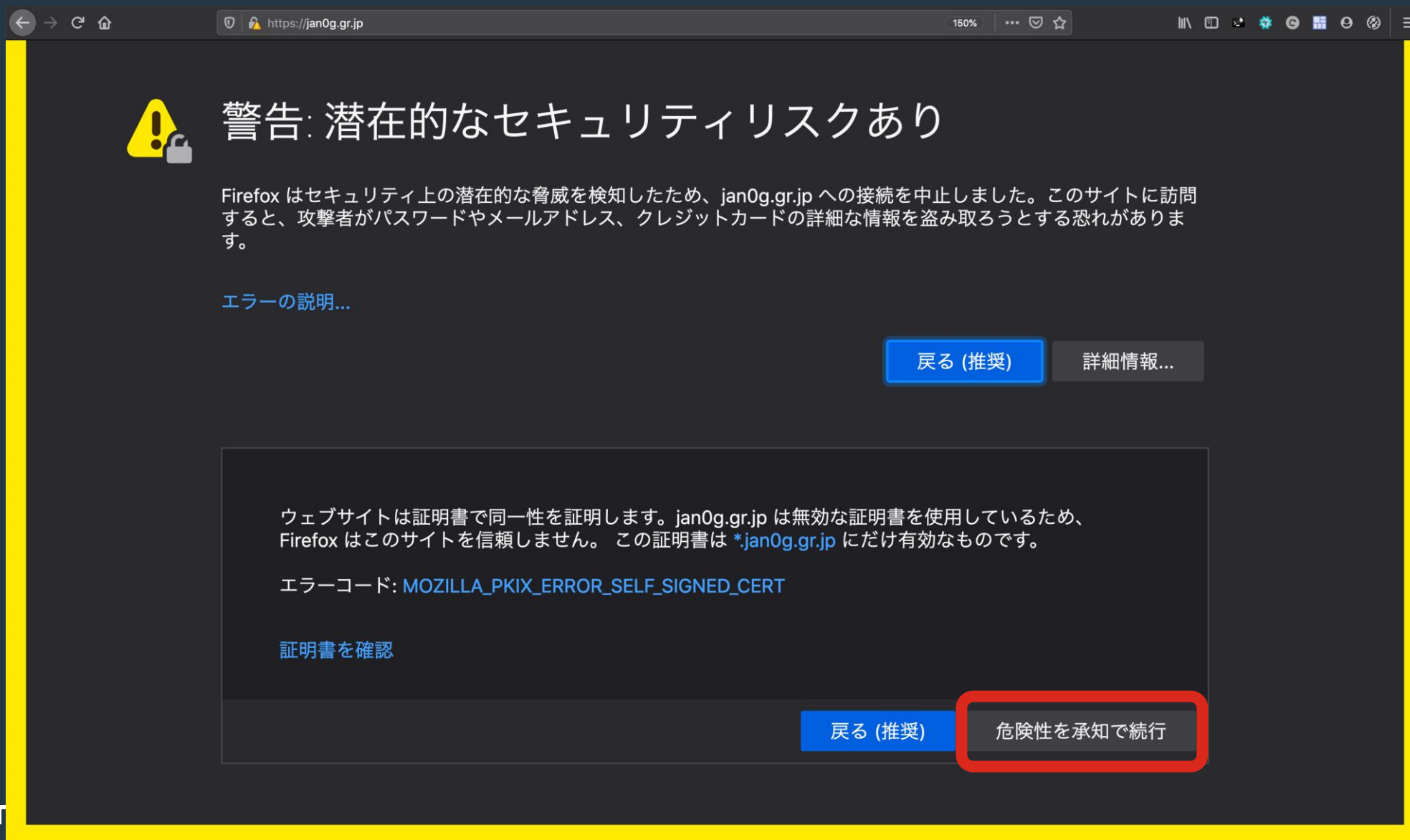
信頼された認証局を通していない証明書(=オレオレ証明書)だと



信頼された認証局を通していない証明書(=オレオレ証明書)だと



信頼された認証局を通していない証明書(=オレオレ証明書)だと



The screenshot shows a Firefox browser window with a security warning. The address bar shows the URL `https://jan0g.gr.jp`. The warning message is in Japanese and explains that the site is not trusted because it uses a self-signed certificate. The error code is `MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT`. There are two buttons: "戻る (推奨)" (Back - Recommended) and "危険性を承知で続行" (Proceed with awareness of risk), the latter of which is highlighted with a red box.

警告: 潜在的なセキュリティリスクあり

Firefox はセキュリティ上の潜在的な脅威を検知したため、jan0g.gr.jp への接続を中止しました。このサイトに訪問すると、攻撃者がパスワードやメールアドレス、クレジットカードの詳細な情報を盗み取ろうとする恐れがあります。

[エラーの説明...](#)

[戻る \(推奨\)](#) [詳細情報...](#)

ウェブサイトは証明書で同一性を証明します。jan0g.gr.jp は無効な証明書を使用しているため、Firefox はこのサイトを信頼しません。この証明書は `*jan0g.gr.jp` にだけ有効なものです。

エラーコード: `MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT`

[証明書を確認](#)

[戻る \(推奨\)](#) [危険性を承知で続行](#)

信頼された認証局を通していない証明書(=オレオレ証明書)だと

証明書

*.jan0g.gr.jp

Subject Name _____
Country JP
State/Province AAA
Locality LLL
Organization Test
Organizational Unit develop
Common Name *.jan0g.gr.jp

Issuer Name _____
Country JP
State/Province AAA
Locality LLL
Organization Test
Organizational Unit develop
Common Name *.jan0g.gr.jp

Validity _____
Not Before 2020/1/23 0:33:26 (Asia/Tokyo)
Not After 2030/1/20 0:33:26 (Asia/Tokyo)

Subject Alt Names _____
DNS Name *.jan0g.gr.jp



実在証明

DV (Domain Validated) 証明書	ドメイン名の所在のみを確認して証明書を発行。
OV (Organization Validation) 証明書	組織の所在(実在性)を確認をして証明書を発行。
EV (Extended Validation) 証明書	CA/Browser Forum で規定された手順に則り証明書を発行。ブラウザでURL記載部分が緑色になるなど、DV/OV証明書との異なる差別化が図られている。

IJ, IIRvol.30, 1.4.2 Let's Encryptプロジェクトと証明書自動発行のためのACMEプロトコル
http://www.ij.ad.jp/company/development/report/iir/030/01_04.html



EVSSL証明書が泣いている「検索窓問題」 ～ブラウザのセキュリティインディケータを 意識していますか～



保護された通信 | <https://www.ij.ad.jp/>



須賀祐治
2017-01-20

Ongoing Innovation

保護された通信 | <https://www.cellos-consortium.org>

Cryptographic protocol Evaluation toward Long-Lived
Outstanding Security Consortium (CELLOS)

SSLについておさらいしてみる



実在証明



暗号化通信

← SSL → 暗号化通信



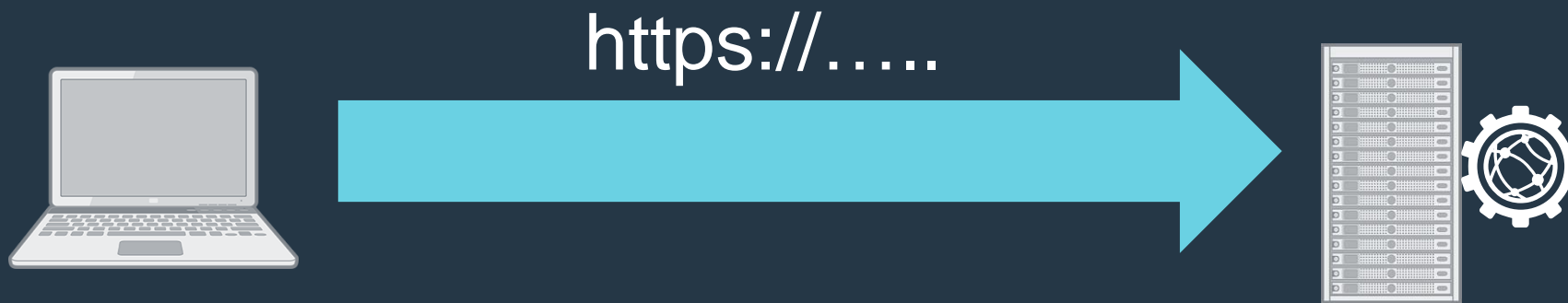
HTTP(暗号化無し)でのアクセスだと

暗号化通信

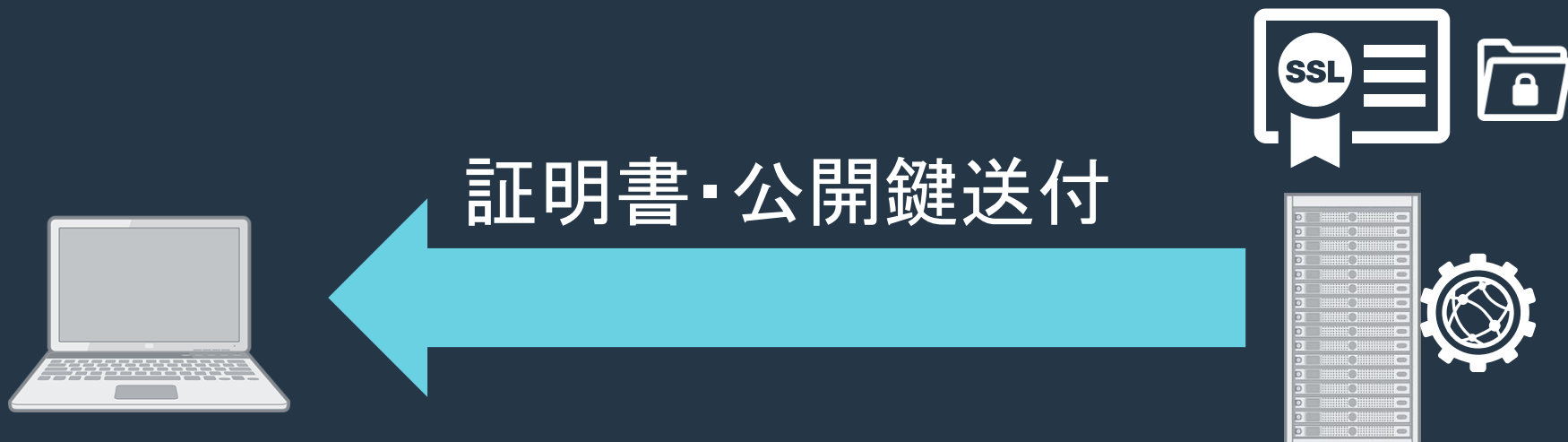
End to End 暗号化



暗号化通信



暗号化通信

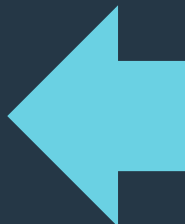


暗号化通信



証明書・公開鍵送付





ルート証明書と照合

証明書マネージャー

あなたの証明書 個人証明書 サーバー証明書 **認証局証明書**

認証局を識別するため以下の証明書が登録されています

証明書名と発行者名	セキュリティデバイス
▼ AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
▼ AC Camerfirma SA CIF A82743287	
Camerfirma Chambers of Commerce Root	Builtin Object Token
Camerfirma Global Chambersign Root	Builtin Object Token
▼ ACCV	
ACCVRAIZ1	Builtin Object Token
▼ Actalis S.p.A./03358520967	
Actalis Authentication Root CA	Builtin Object Token
▼ AddTrust AB	
AddTrust Low-Value Services Root	Builtin Object Token
AddTrust External Root	Builtin Object Token
COMODO ECC Certification Authority	Software Security Device
COMODO RSA Certification Authority	Software Security Device

表示... 信頼性を設定... **インポート...** エクスポート... 削除または信頼しない...

OK

暗号化通信



共通鍵を作成



暗号化通信



公開鍵で共通鍵を
暗号化



暗号化通信



暗号化通信



暗号化通信



秘密鍵で共通鍵を解錠

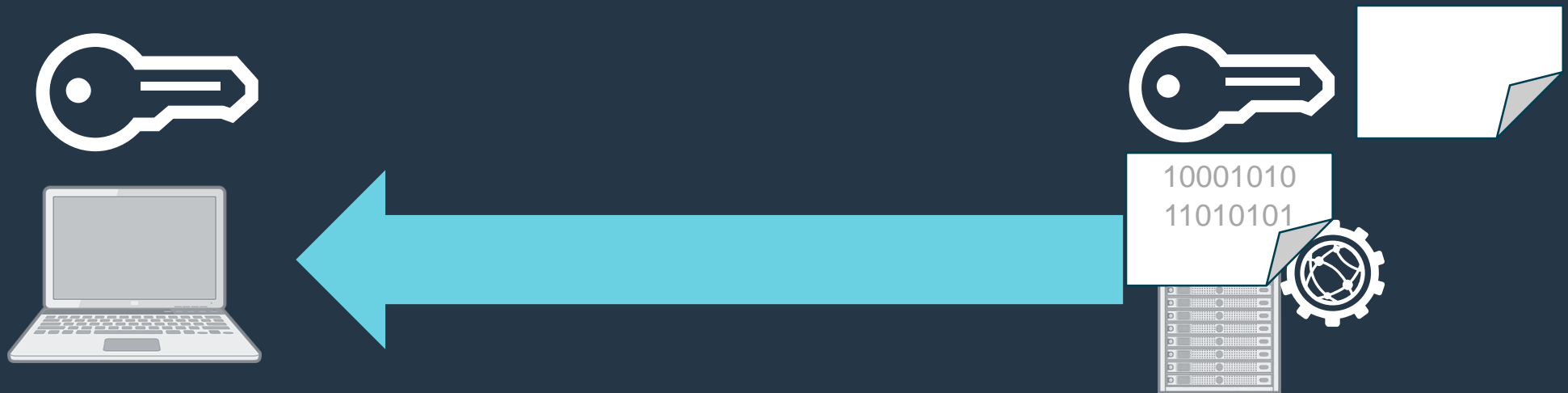
暗号化通信



共通鍵の交換完了！

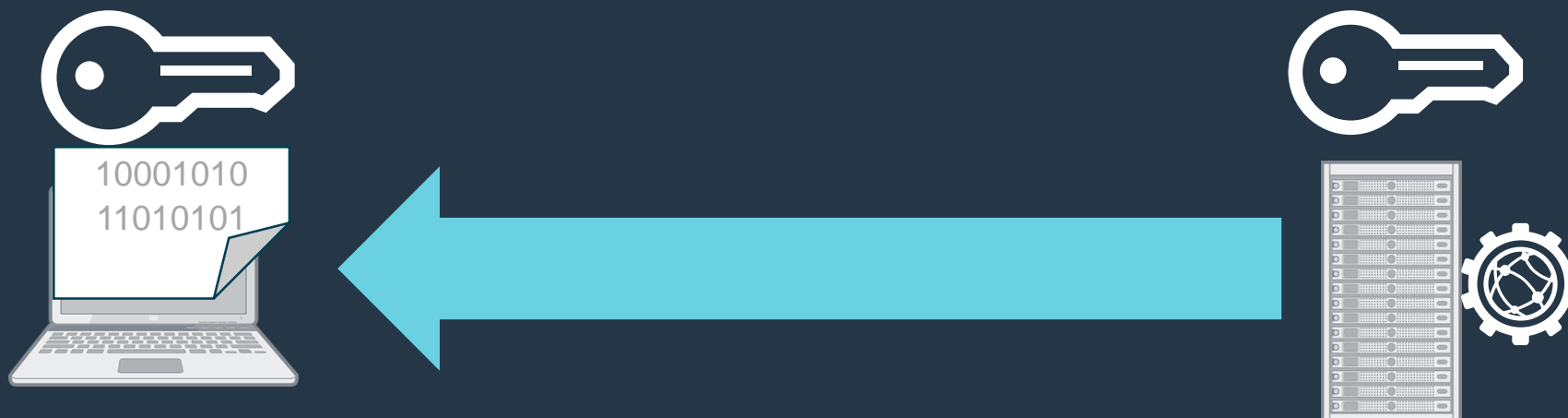


暗号化通信



共通鍵で暗号化して送信

暗号化通信



共通鍵で暗号化して送信

暗号化通信



共通鍵で復号化



暗号化通信



盗聴・改ざん不可



ダークサイド of SSL

鍵マークがあれば本当に安心なのか？

鍵マークがあれば本当に安心なのか？

The screenshot shows the homepage of JP Bank (ゆうちょ銀行). At the top, there is a search bar and navigation links for "よくあるご質問", "お問い合わせ", "サイトマップ", and "English". Below this is a horizontal menu with categories like "個人のお客さま", "法人のお客さま", "株主・投資家のみなさま", "ゆうちょ銀行について", and "採用情報". A secondary menu lists services: "店舗・ATM", "貯金", "送金・支払・海外関連", "給与・年金受取り", "カードサービス", "資産運用・確定拠出年金", "ローン・貸付け".

The main content area features a large banner for "ゆうちょダイレクト" with buttons for "ログイン", "総合口座をお持ちでないお客さま" (総合口座開設), and "投資信託をはじめ" (投資信託口座開設). Below the banner is a grid of service icons: "店舗・ATM", "貯金", "送金・支払・海外関連", "給与・年金受取り", "カードサービス", "資産運用・確定拠出年金", "ローン・貸付け", and "相続".

On the left side, there are utility links: "手数料・料金一覧", "金利一覧", "店舗・ATM検索", and "各種お申込みお手続き". Below these is a section for "他の金融機関との振込" (振込用の店名、口座番号のご案内はこちら) and a warning "金融犯罪にご注意ください!". At the bottom left, there is a link for "カード・通帳等の紛失盗難のお問い合わせ先".

The right side of the page has a "キャンペーン" section with a banner for "資産形成 抽選で5,000円プレゼント!" and "新生活応援 キャンペーン". Below this is "お役立ち情報" with links for "各種ご請求用紙のダウンロード" and "iDeCo (イデコ) 各種ご請求用紙のダウンロード". At the bottom right, there is a section for "株式・IR関連情報" with a link for "株主・投資家のみなさまへ".

鍵マークがあれば本当に安心なのか？

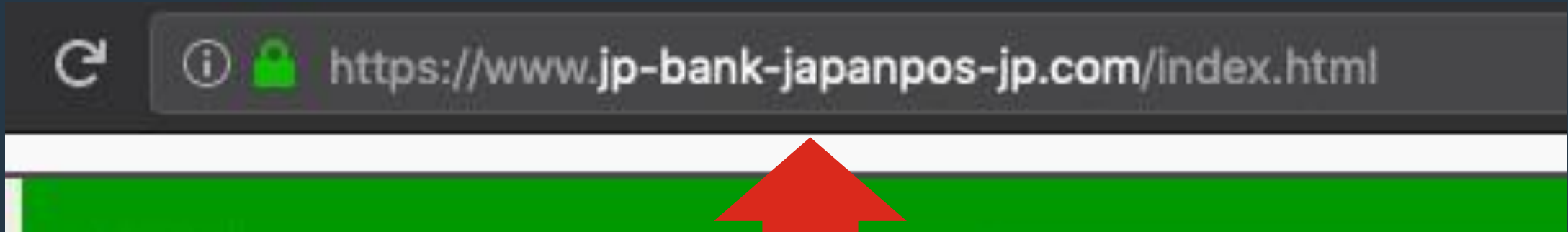
The screenshot shows the homepage of JP Bank (ゆうちょ銀行). At the top left is the JP Bank logo and the slogan "そばにいるから、できることがある。" (Because we are nearby, we can do things). To the right is a search bar with the text "検索キーワードを入力" and a "検索" button. Below the search bar are links for "よくあるご質問", "お問い合わせ", "サイトマップ", and "English". A "金融機関コード: 9900" is displayed on the left. A navigation bar includes "個人のお客さま", "法人のお客さま", "株主、投資家のみなさま", "ゆうちょ銀行について", and "採用情報". Below this is a menu with "店舗・ATM", "貯金", "送金・支払・海外関連", "給与・年金受取り", "カードサービス", "資産運用・確定拠出年金", and "ローン、貸付け". The main content area features a blurred image of staff and three prominent buttons: "ゆうちょダイレクト ログイン", "総合口座をお持ちでないお客さま 総合口座開設", and "投資信託をはじめる 投資信託口座開設".

鍵マークがあれば本当に安心なのか？



鍵マークがついている！

鍵マークがあれば本当に安心なのか？



URLはヘンテコだがそれっぽい！

鍵マークがあれば本当に安心なのか？

https://www.jp-bank-japanpos-jp.com/index.html 偽物

https://www.jp-bank.japanpost.jp 本物

JP BANK ゆうちょ銀行

そばにいるから、できることがある。

金融機関コード：9900

よくあるご質問 お問い合わせ サイトマップ English

文字サイズ変更 小 中 大

個人のお客さま 法人のお客さま 株主・投資家のみなさまへ ゆうちょ銀行について 採用情報

店舗・ATM 貯金 送金・支払・海外関連 給与・年金受取り カードサービス 資産運用・確定拠出年金 ローン・貸付け

⚠️ 令和元年台風第19号に関するお知らせ

⚠️ フィッシングメール、偽ショートメッセージ（SMS）による詐欺被害にご注意ください

⚠️ 「長期間ご利用がない貯金のご確認のお願い」を送付しています

ゆうちょダイレクト

ログイン

新規申込・サービス内容

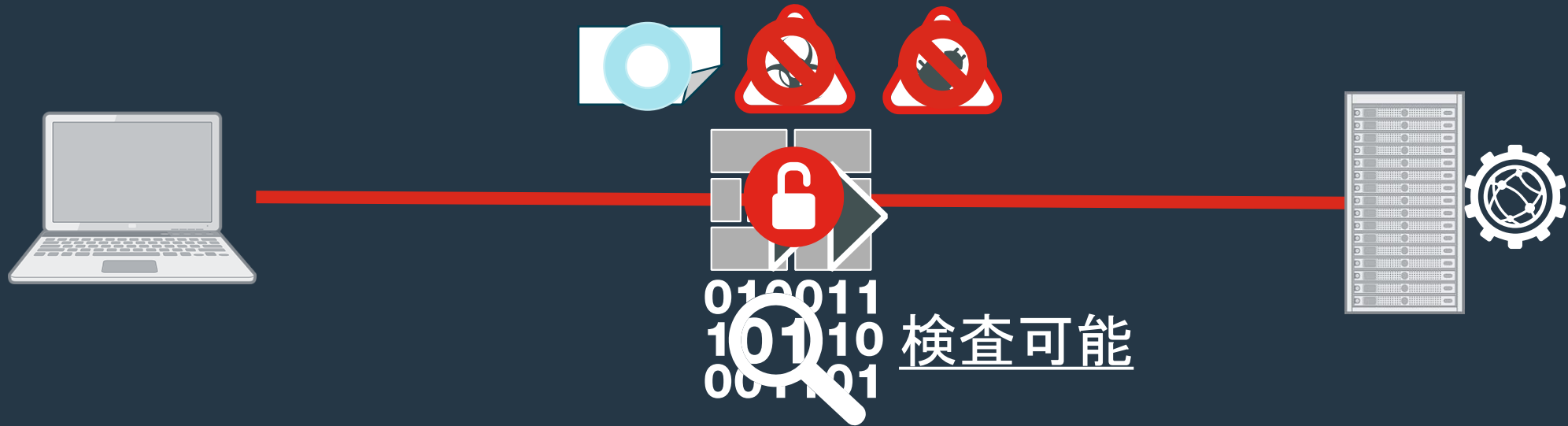
ダイレクトについて質問する

総合口座をお持ちでないお客さま

総合口座開設

ネットワークセキュリティ装置が手出し出来ない

ネットワークセキュリティ装置が手出し出来ない



HTTP(暗号化無し)でのアクセスだと

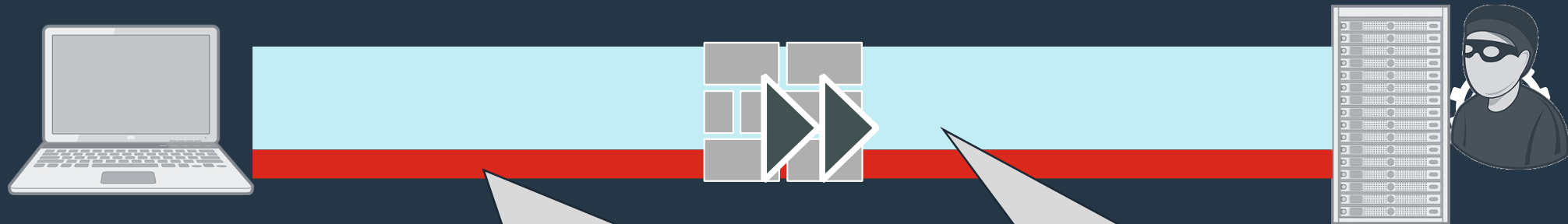
ネットワークセキュリティ装置が手出し出来ない



HTTPS(暗号化)でのアクセスだと

ネットワークセキュリティ装置が手出し出来ない

HTTPS通信が8割以上の現実



2割しかセキュリティ
対策が取れない

8割素通し。。。

ダークサイド of SSL

実在証明



コンテンツの安全性は
証明していない

暗号化通信



ネットワークセキュリティ
装置の無力化

ネットワークレベルでの対抗策

ネットワークレベルでの対抗策

- 証明書インスペクション
- SSL Deepインスペクション(インターセプト)

証明書インスペクション

- 証明書のCNを見る

証明書インスペクション

▼ Secure Sockets Layer

▼ TLSv1.2 Record Layer: Handshake Protocol: Certificate

Content Type: Handshake (22)

Version: TLS 1.2 (0x0303)

Length: 2727

▼ Handshake Protocol: Certificate

Handshake Type: Certificate (11)

Length: 2723

Certificates Length: 2720

▼ Certificates (2720 bytes)

Certificate Length: 1538

▼ Certificate: 308205fe308204e6a00302010202087dd5b0fdb70a9c5730... (id-at-commonName=*.janog.gr.jp)

▶ signedCertificate

▶ algorithmIdentifier (sha256WithRSAEncryption)

Padding: 0

encrypted: 75d37a00a286d1a7c9f4fa84c5b01d7b24d7f852b4971c3e...

Certificate Length: 1176

証明書インスペクション

- 証明書のCNを見る
- CLIENT HELLOのSNIを見る

証明書インスペクション

- 証明
- CLIENT

```
▼ Secure Sockets Layer
  ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 512
  ▼ Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 508
    Version: TLS 1.2 (0x0303)
    ▶ Random
    Session ID Length: 32
    Session ID: 4f4080be84c33491a0cb10996d226f6e1b418fbee96a7fb5...
    Cipher Suites Length: 36
    ▶ Cipher Suites (18 suites)
    Compression Methods Length: 1
    ▶ Compression Methods (1 method)
    Extensions Length: 399
  ▼ Extension: server_name
    Type: server_name (0x0000)
    Length: 20
  ▼ Server Name Indication extension
    Server Name list length: 18
    Server Name Type: host_name (0)
    Server Name length: 15
    Server Name: www.janog.gr.jp
```

証明書インスペクション

- 証明書のCNを見る
- CLIENT HELLOのSNIを見る
- あくまで証明書のHOST名レベル

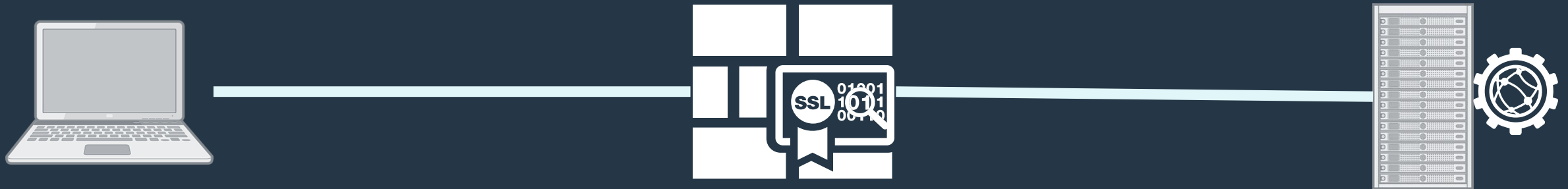
ネットワークレベルでの対抗策

- 証明書インスペクション
- SSL Deepインスペクション(インターセプト)

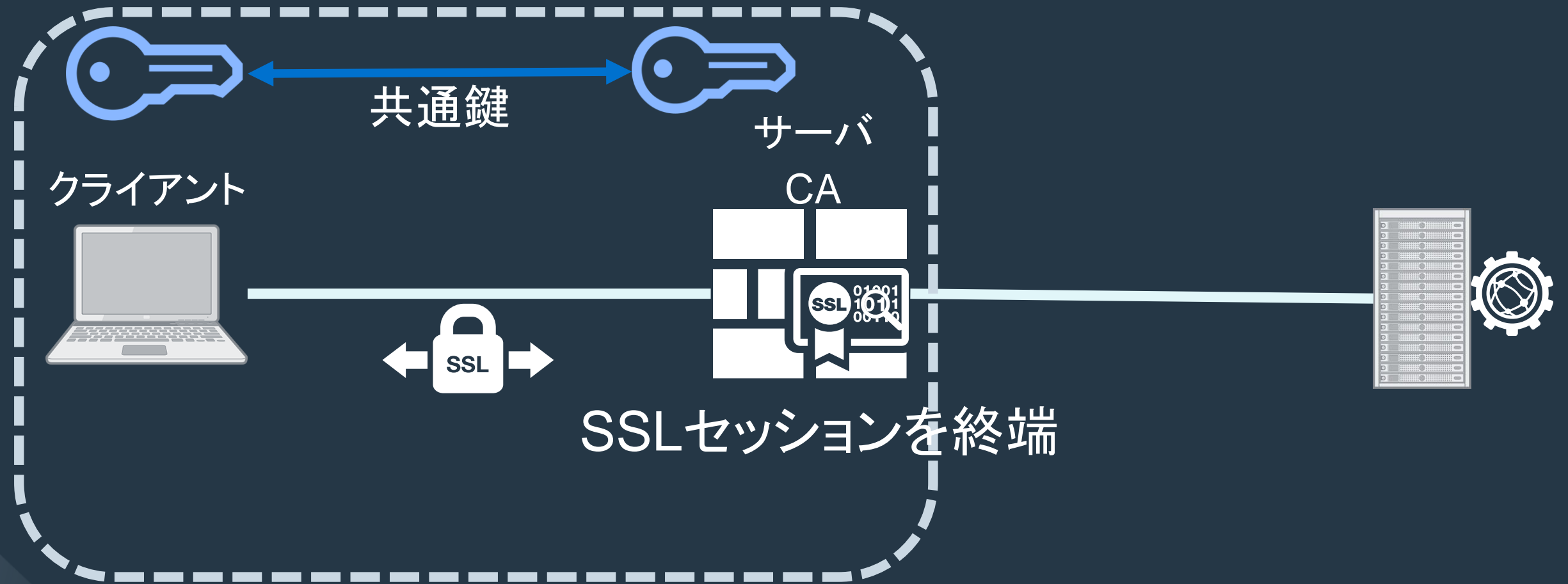
SSL Deepインスペクション

SSL Deepインスペクション

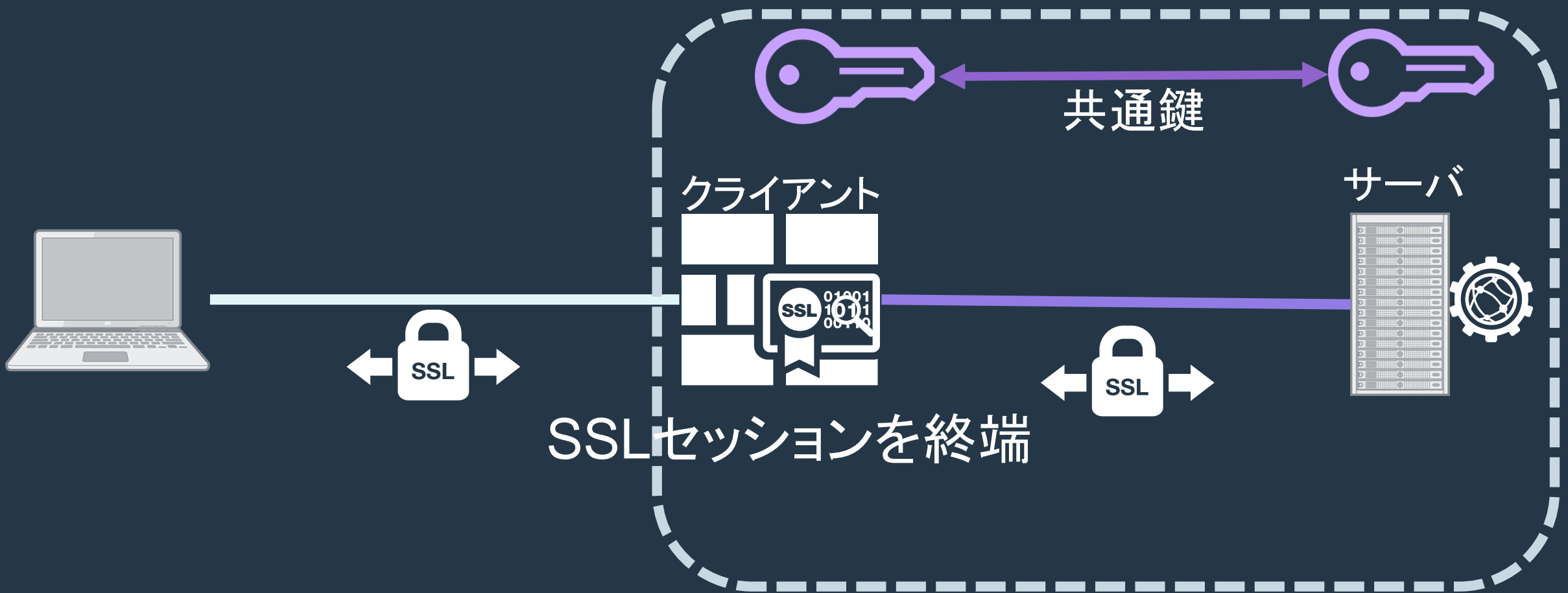
ファイアウォール、プロキシ



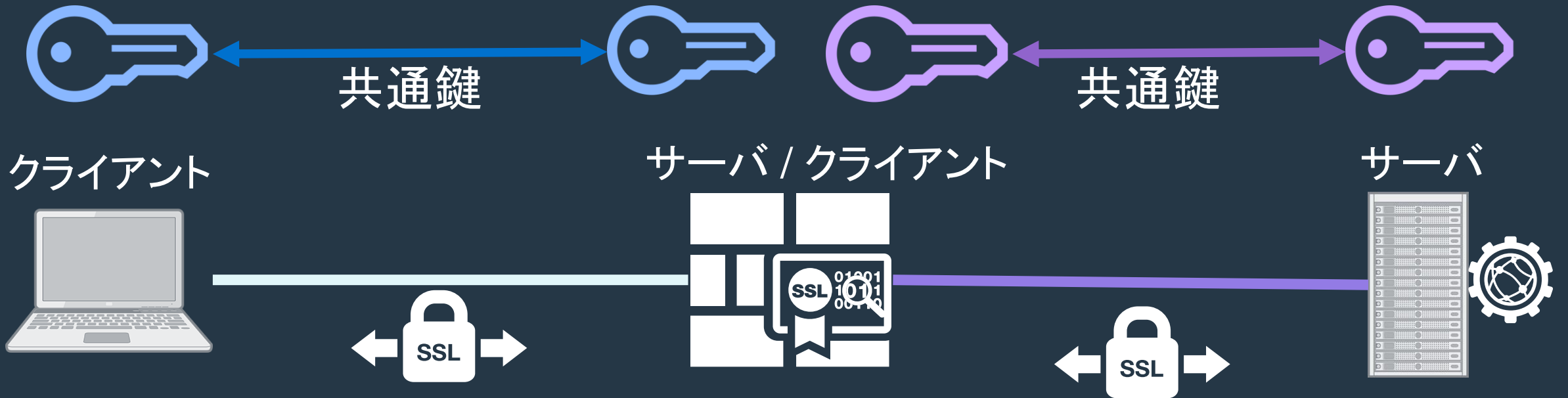
SSL Deepインスペクション



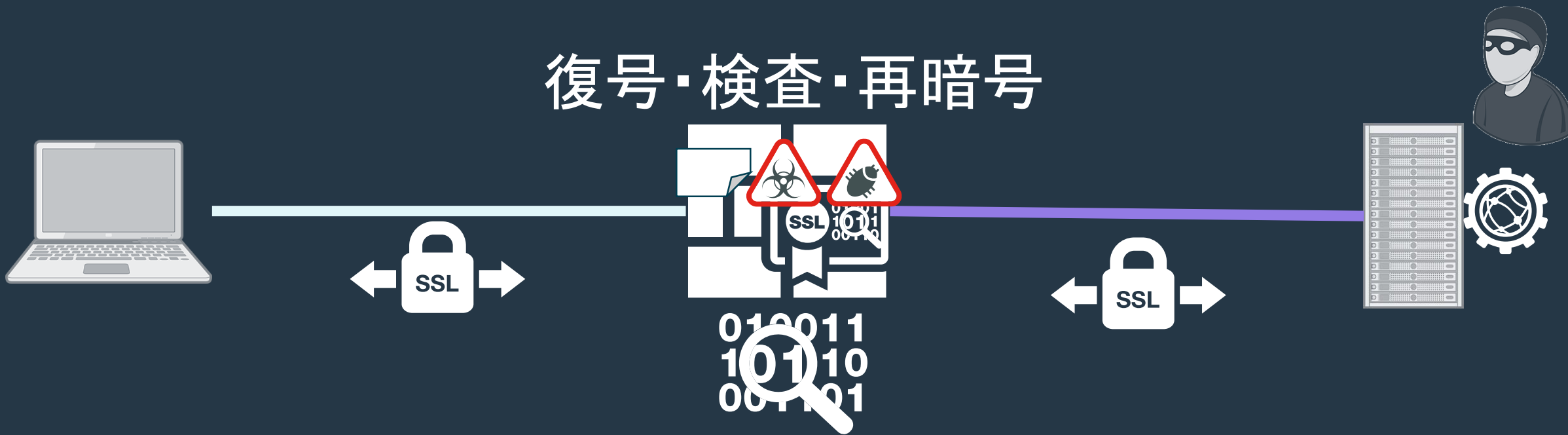
SSL Deepインスペクション



SSL Deepインスペクション



SSL Deepインスペクション



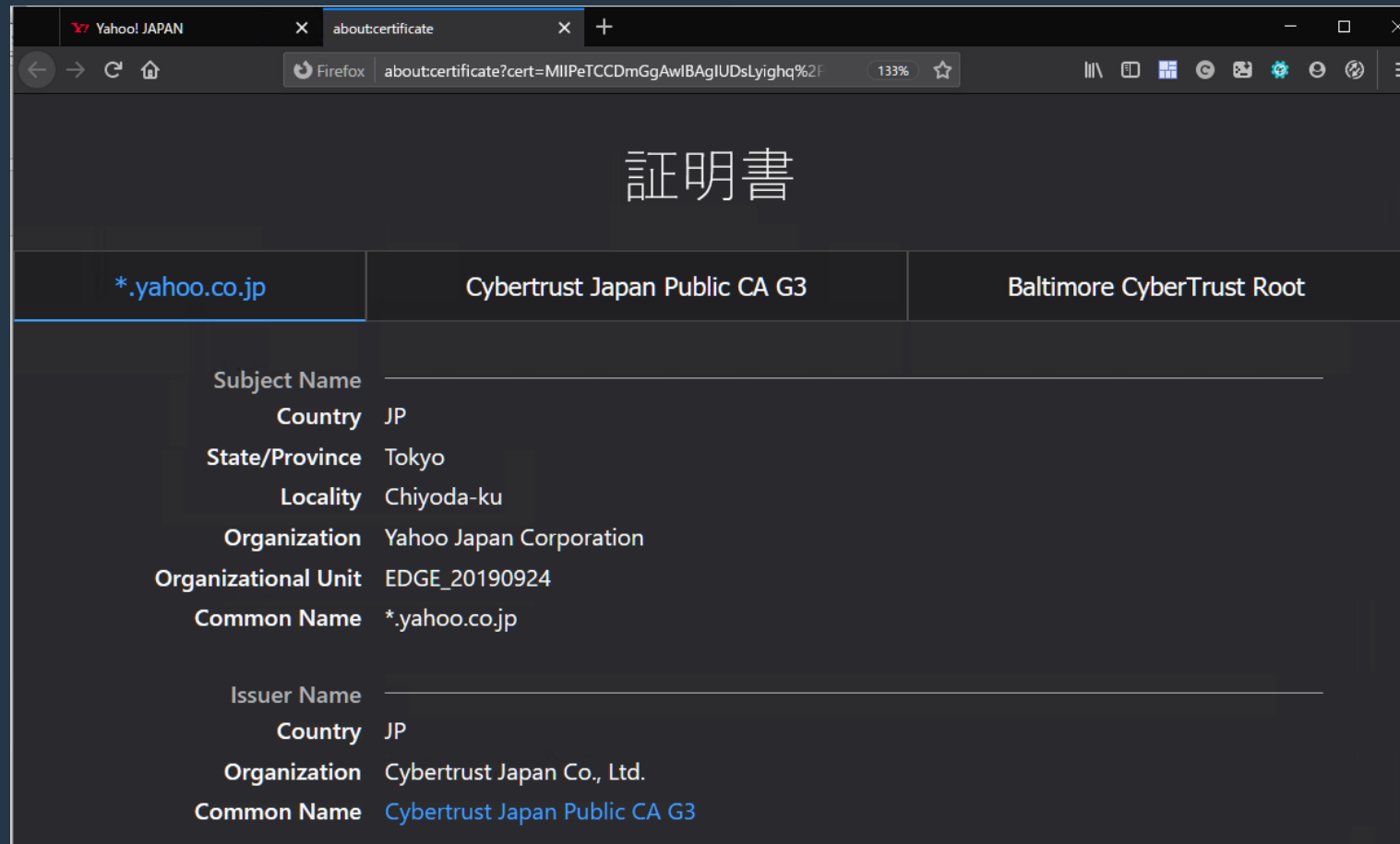
SSL Deepインスペクション

- ようは、Man In The Middle
- 証明書エラーの対処が必要

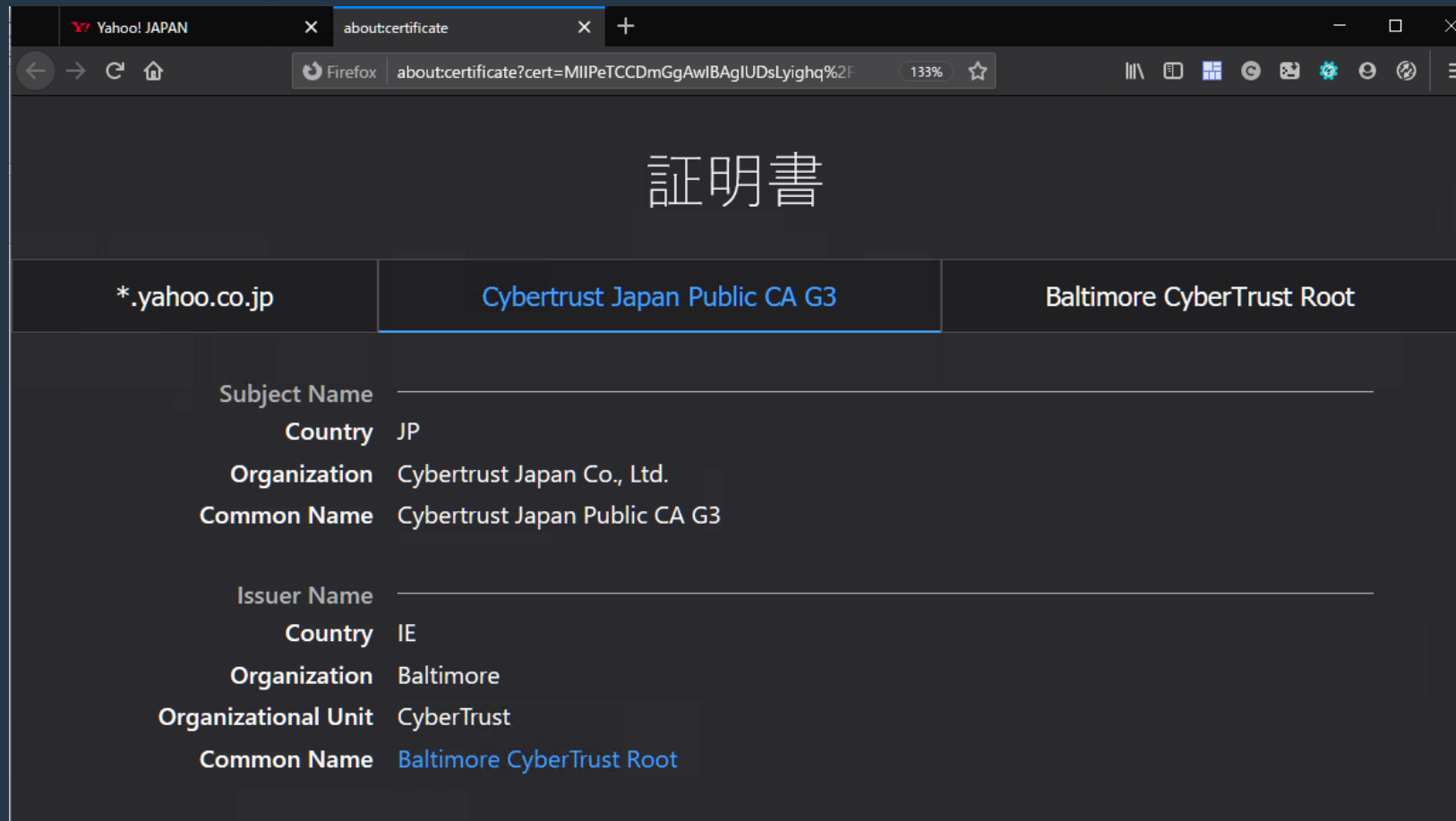
普通にアクセスすると



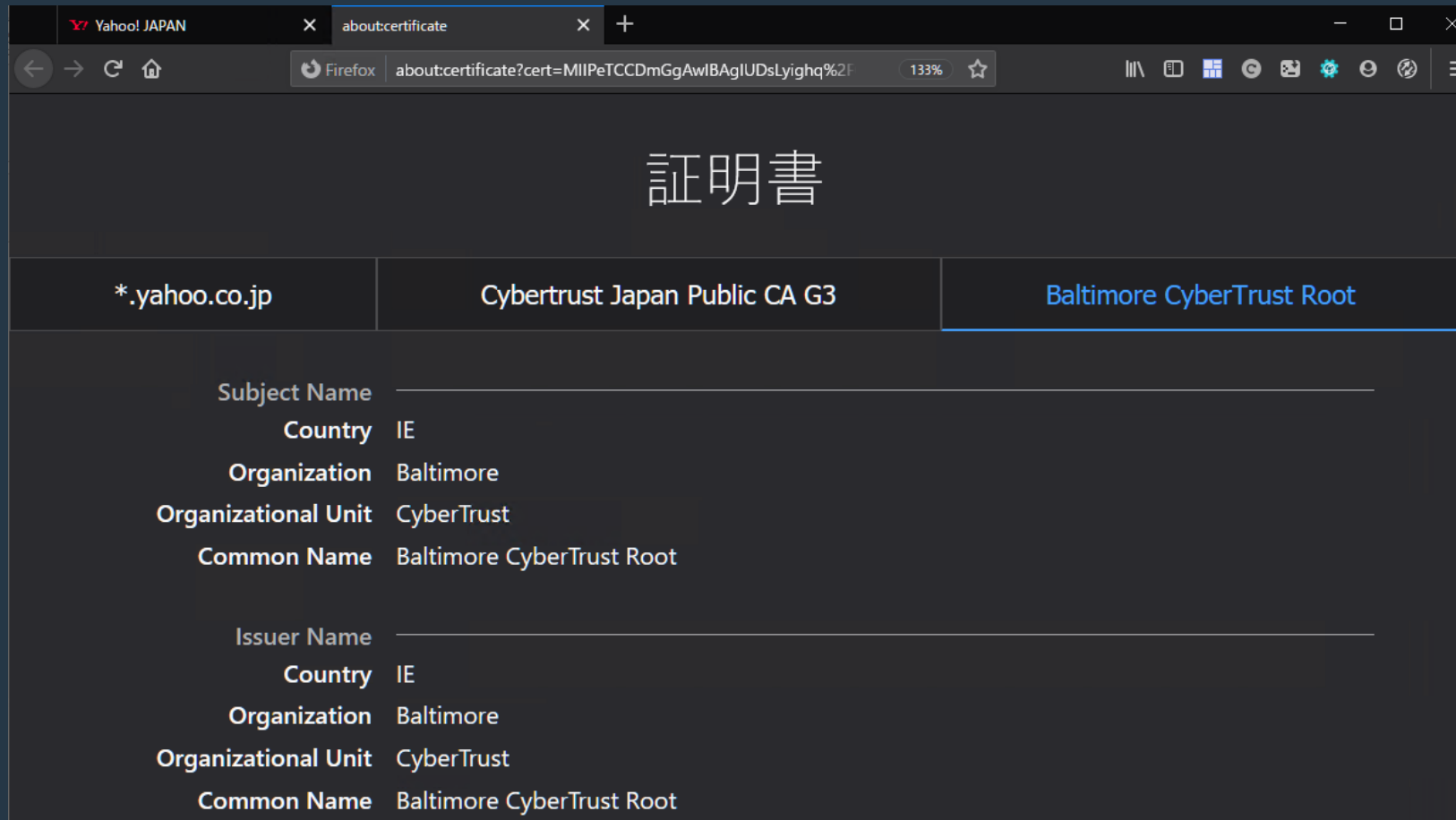
普通にアクセスすると



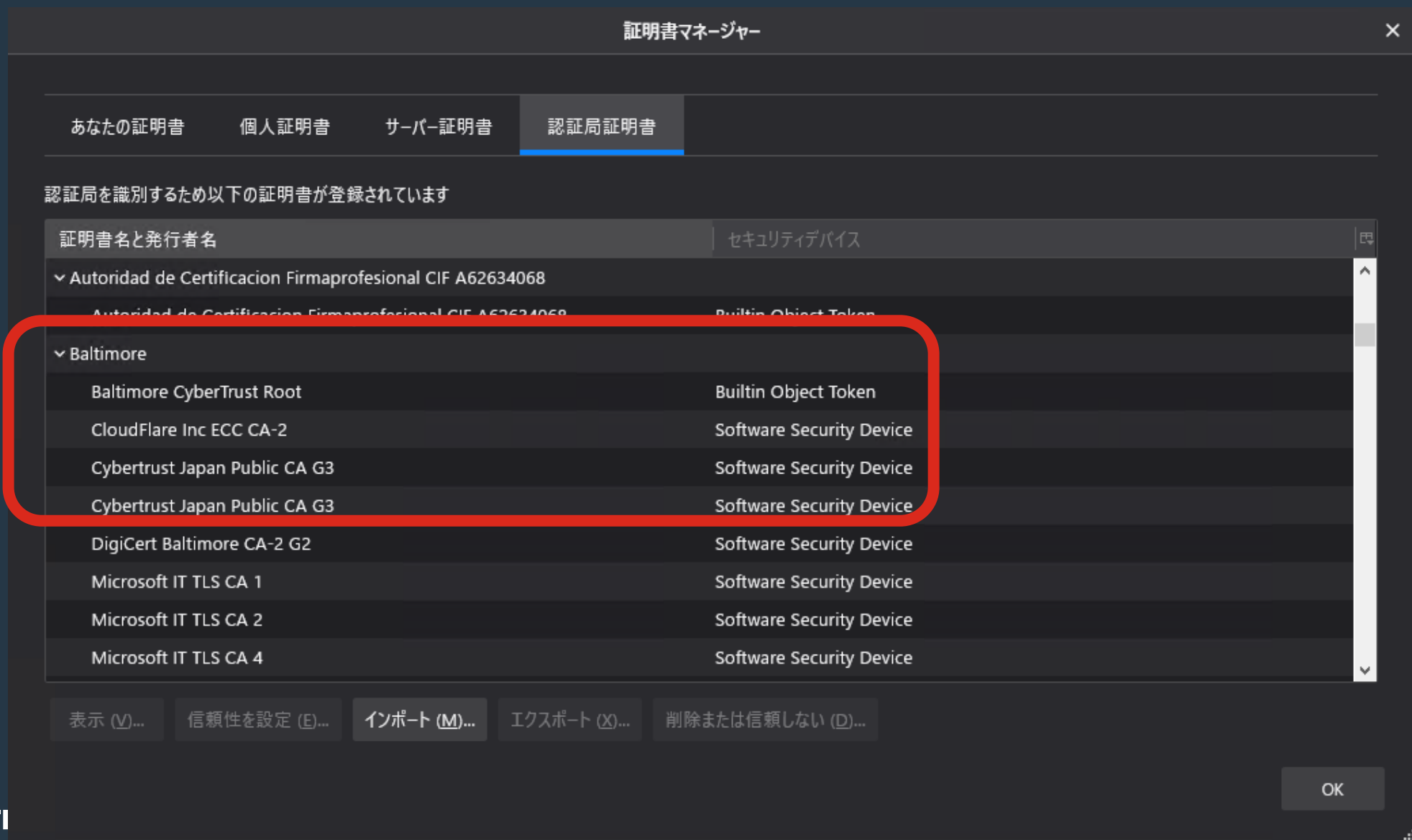
普通にアクセスすると



普通にアクセスすると

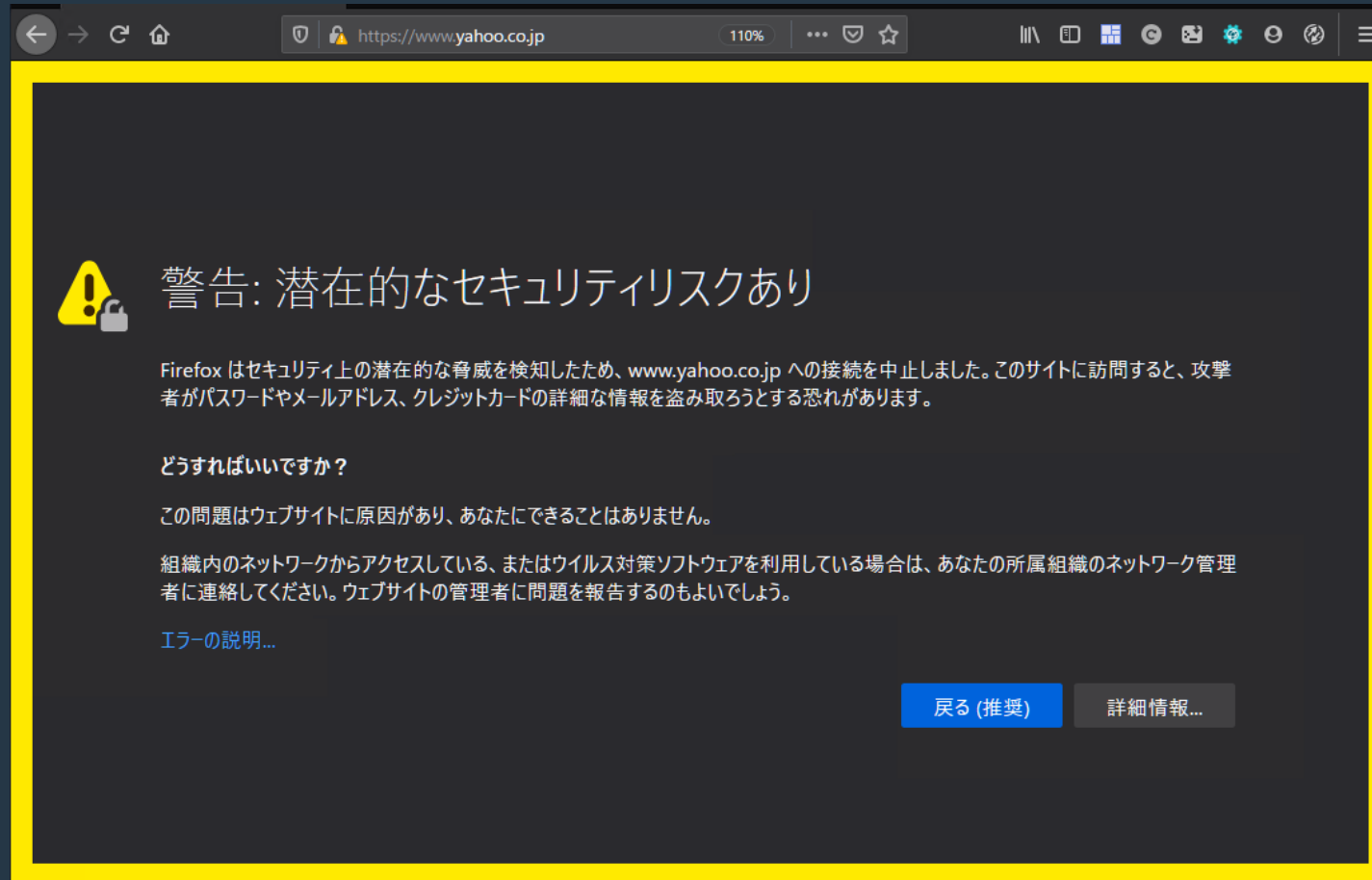


ブラウザ(Firefox)にインストール済み



SquidでSSLインスペクションをすると

SquidでSSLインスペクションをすると



SquidでSSLインスペクションをすると

この問題はウェブサイトの原因があり、あなたにできることはありません。

組織内のネットワークからアクセスしている、またはウイルス対策ソフトウェアを利用している場合は、あなたの所属組織のネットワーク管理者に連絡してください。ウェブサイトの管理者に問題を報告するのもよいでしょう。

[エラーの説明...](#)

[戻る \(推奨\)](#)

[詳細情報...](#)

誰かがこのサイトに偽装しようとしている可能性があります。続行しないでください。

ウェブサイトは証明書で同一性を証明します。証明書の発行者が不明、証明書が自己署名、またはサーバーが正しい中間証明書を送信していないため、Firefox は www.yahoo.co.jp を信頼しません。

エラーコード: [SEC_ERROR_UNKNOWN_ISSUER](#)

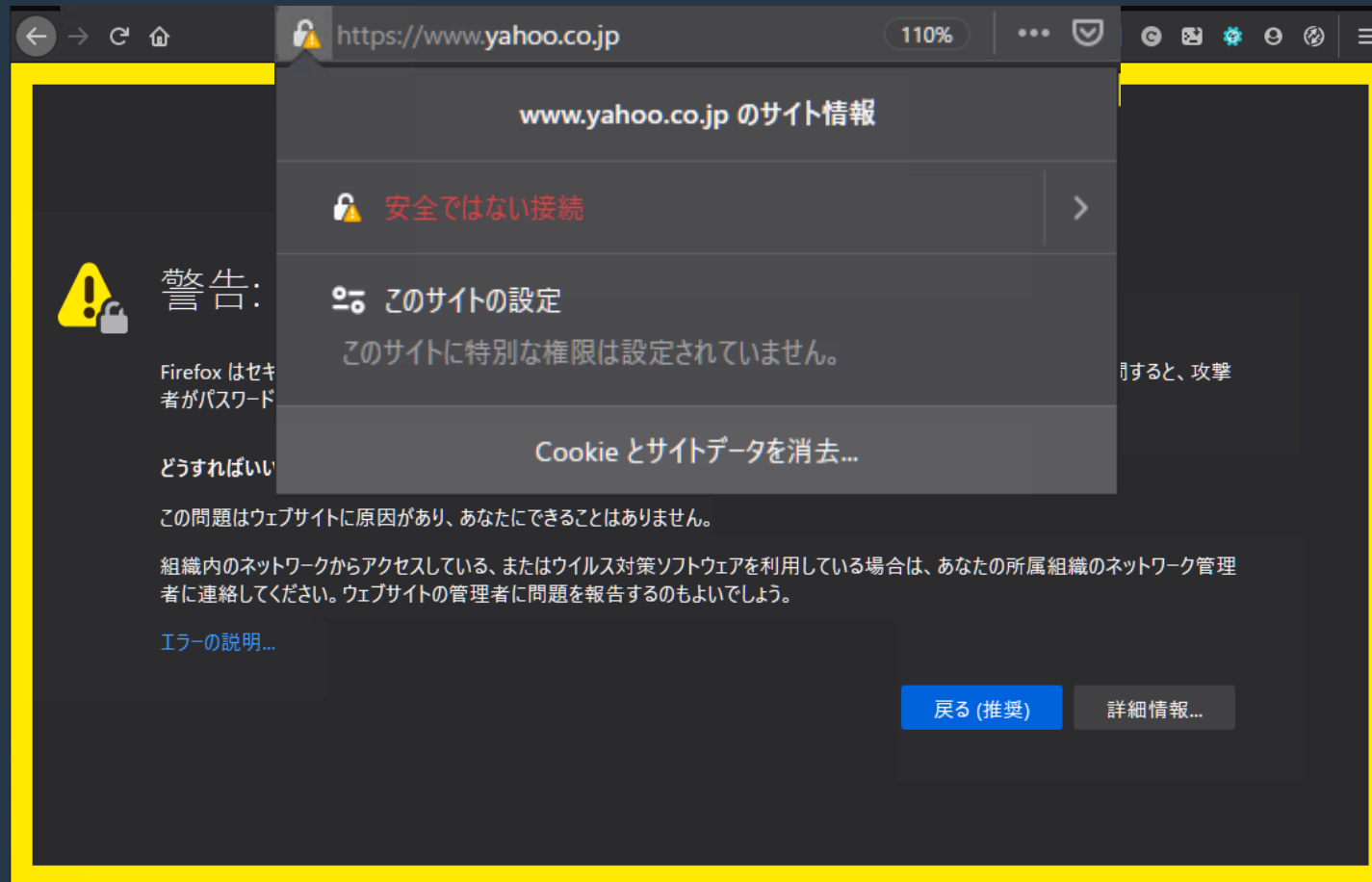
[証明書を確認](#)

[戻る \(推奨\)](#)

[危険性を承知で続行](#)

警告が出た

SquidでSSLインスペクションをすると



警告が出た

SquidでSSLインスペクションをすると

証明書

*.yahoo.co.jp	*.ftntjp.com	*.ftntjp.com
---------------	--------------	--------------

Subject Name _____

Country JP

State/Province Tokyo

Locality Chiyoda-ku

Organization Yahoo Japan Corporation

Organizational Unit EDGE_20190924

Common Name *.yahoo.co.jp

Issuer Name _____

Country JP

State/Province TOKYO

Locality MINATOKU

Organization FTNT

Organizational Unit CSE

Common Name *.ftntjp.com

SquidでSSLインスペクションをすると

証明書

*.yahoo.co.jp	*.ftntjp.com	*.ftntjp.com
---------------	--------------	--------------

Subject Name _____
Country JP
State/Province Tokyo
Locality Chiyoda-ku
Organization Yahoo Japan Corporation
Organizational Unit EDGE_20190924
Common Name *.yahoo.co.jp

Issuer Name _____
Country JP
State/Province TOKYO
Locality MINATOKU
Organization FTNT
Organizational Unit CSE
Common Name *.ftntjp.com

Issuerが認証局証明書リストにないため

SquidでSSLインスペクションをすると

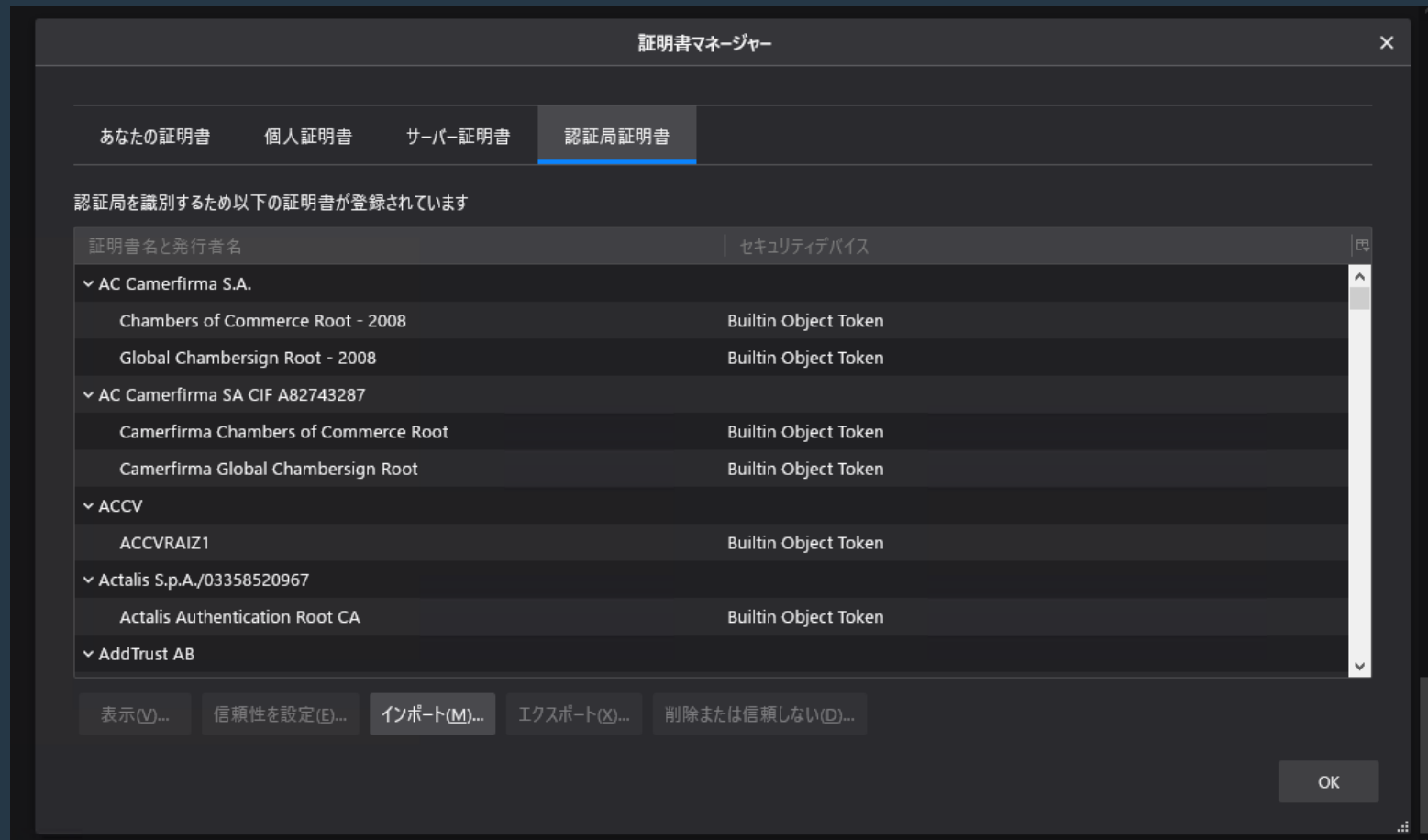
証明書

*.yahoo.co.jp	*.ftntjp.com	*.ftntjp.com
---------------	--------------	--------------

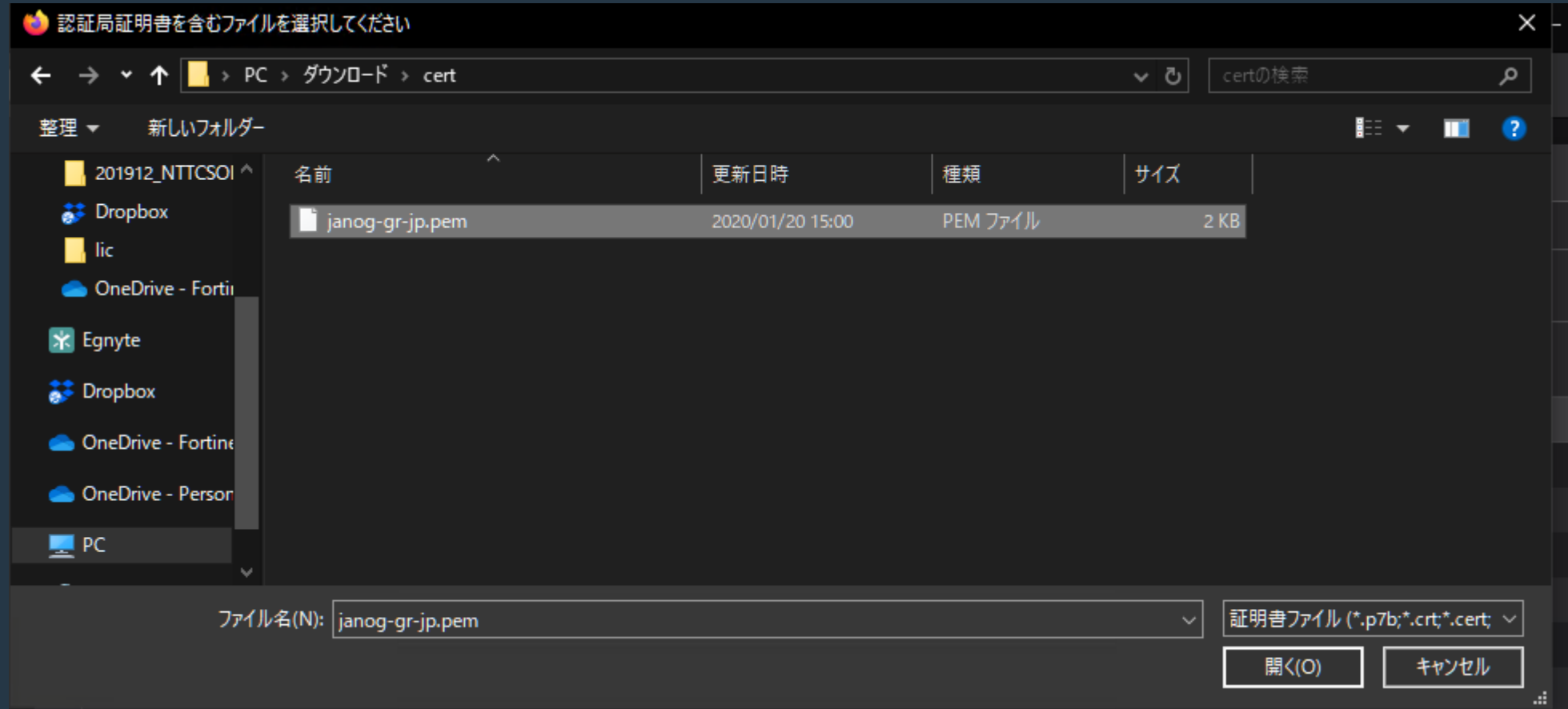
Subject Name _____
Country JP
State/Province TOKYO
Locality MINATOKU
Organization FTNT
Organizational Unit CSE
Common Name *.ftntjp.com
Email Address ysugii@fortinet.com

Issuer Name _____
Country JP
State/Province TOKYO
Locality MINATOKU
Organization FTNT
Organizational Unit CSE
Common Name *.ftntjp.com

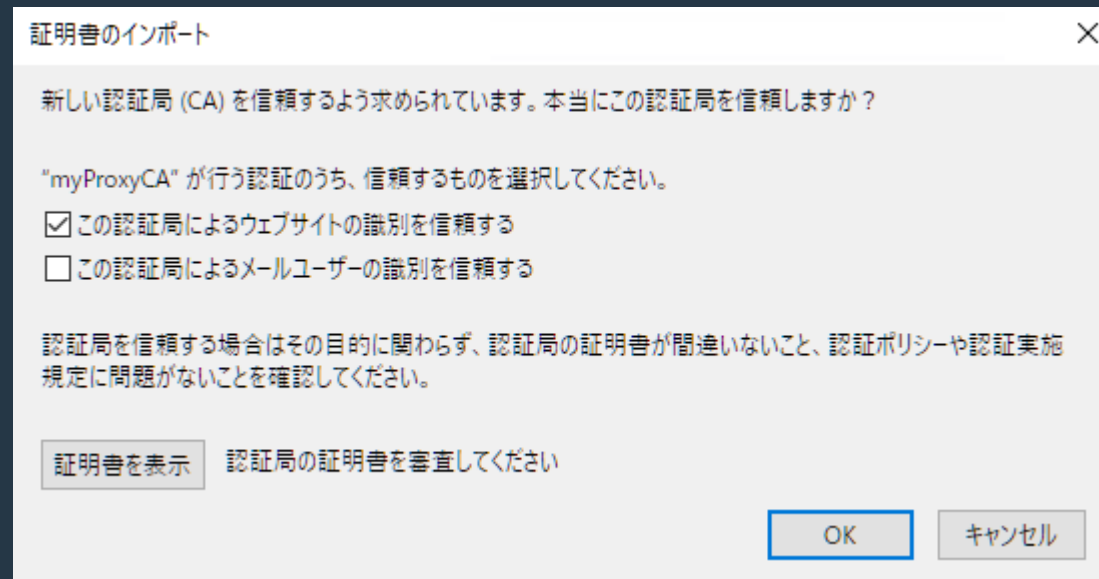
SquidでSSLインスペクションをすると



SquidでSSLインスペクションをすると



SquidでSSLインスペクションをすると



SquidでSSLインスペクションをすると



SquidでSSLインスペクションをすると



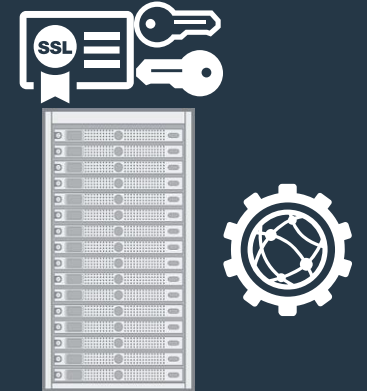
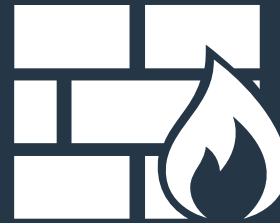
警告は消えたが、、、

余談:SSL オフロードとの違い

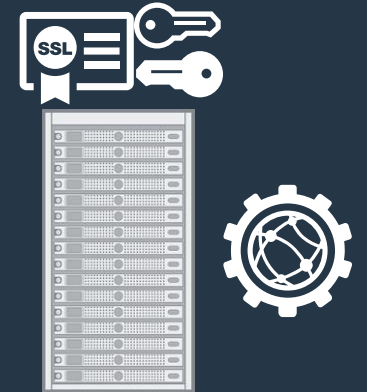


ロードバランサ

WAF

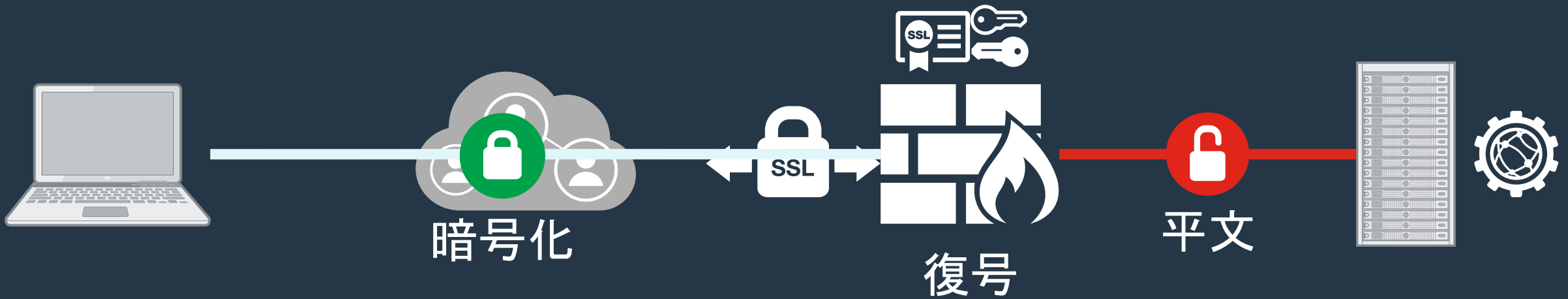


余談: SSL オフロードとの違い



サーバの証明書・秘密鍵を
LB・WAFにインポート

余談:SSL オフロードとの違い



SSLインスペクション

- 不特定多数へのアクセス
- LAN側の保護

SSLオフロード

- 特定サーバへのアクセス
- WANサービス側の保護

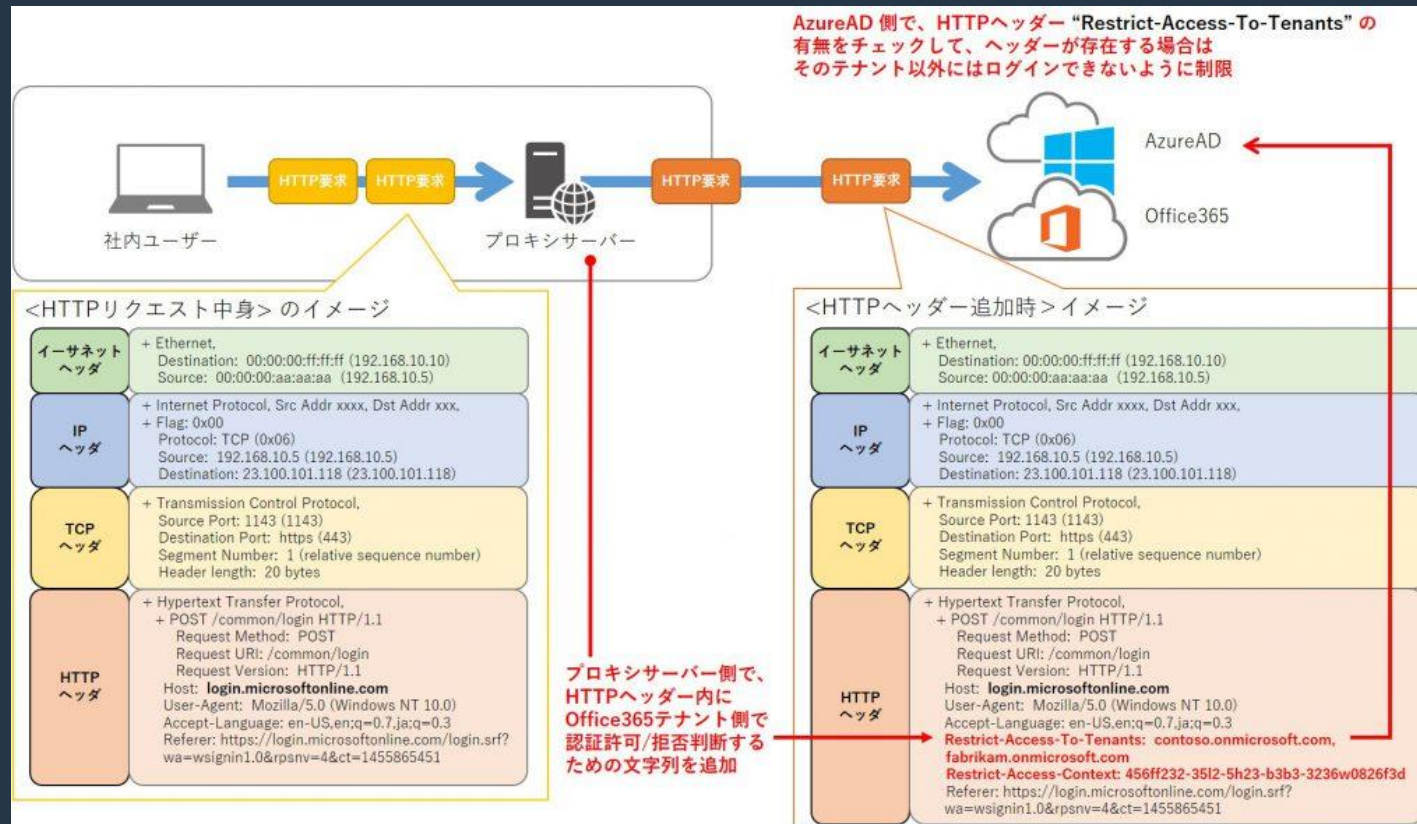
SSLインスペクションが必要なもう一つの理由 ～シャドーITどうしゃどう～

- サービスレベルでのブロックならどうにかなる
 - Dropbox -> NG
 - Onedrive -> OK
- ISDB(IPベース or FQDNベース)での宛先制御, 証明書インスペクションでのHost名制御で実現可能
- でも野良one driveどうしよう



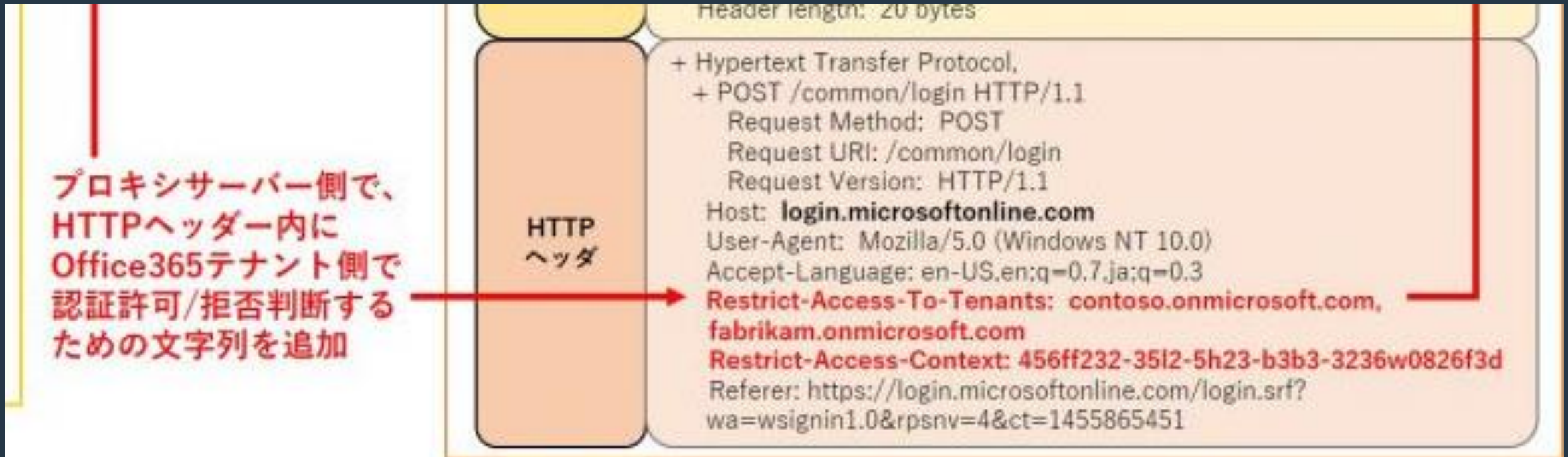
O365のテナント管理はどうにかやりたい

- Proxy + SSLインスペクションの導入が必須



O365のテナント管理はどうにかやりたい

- Proxy + SSLインスペクションの導入が必須



参照: 自社テナント以外へのアクセス制御 – “テナントの制限” 機能 (Tenant Restrictions)

FAQ: API型CASBではダメなのか？

- あくまで自社契約サービス(=テナント)内でのコントロール
- テナント管理はスコープ外
- テナント管理にはIn-line Proxyを導入する必要がある



SSLインスペクションに踏み切れない理由

- 運用負荷 (CA証明書の配布)
- 適切な除外リストのメンテナンス
- パフォーマンス

SSLインスペクションに踏み切れない理由

• 進
• 進
• ノ

The screenshot shows a Microsoft Docs page in Japanese. The browser address bar shows the URL: https://docs.microsoft.com/ja-jp/windows-server/identity/ad-fs/deployment/distribute-certificates-to-client-co. The page title is 'グループポリシーを使用してクライアントコンピューターに証明書を配布する' (Distributing certificates to client computers using group policy). The page content includes a breadcrumb trail: Docs / Windows Server / ID およびアクセス / Active Directory フェデレーション サービス (AD FS) / AD FS 展開 / Windows Server 2012 AD FS の展開ガイド / パートナー組織の構成 / グループ ポリシーを使用してクライアント コンピューターに証明書を配布する. The main heading is 'グループポリシーを使用してクライアントコンピューターに証明書を配布する'. The article text starts with '次の手順を使用して、)を使用して、アカウントフェデレーションサーバー、リソースフェデレーションサーバー、および Web サーバーのアカウントフェデレーションサーバー、リソースフェデレーションサーバー、および Web サーバーの信頼されたルートグループポリシーにチェーンされている適切な Secure Sockets Layer (SSL) 証明書 (または同等の証明書をプッシュダウンすることができます。' and continues with 'この手順を実行するには、Domain adminsまたはEnterprise adminsのメンバーシップ、またはそれと同等の Active Directory Domain Services (AD DS) が最低限必要です。適切なアカウントとグループメンバーシップの使用に関する詳細については、(http://go.microsoft.com/fwlink/?)を参照してください。LinkId=83477)。

SSLインスペクションに踏み切れない理由

- 運用負荷 (CA証明書の配布)
 - Windows Server + ADで頑張る
- 適切な除外リストのメンテナンス
 - コツコツメンテナンス
- パフォーマンス
 - ??????

やっぱり気になるパフォーマンス

- SSLインスペクションするとどれくらい劣化するのか？
- Webプロキシ/Squidで実測してみました

試験条件

- SquidでSSLインスペクション(SSL Bump)を有効化
- プレーンHTTP vs. HTTPS
- GET - 21KB Text を x 1 トランザクション
 - 1 HTTP(s)トランザクション / 1 TCP セッション
 - HTTPS – 2048bit RSA証明書 (Sha256)
- 負荷をランプアップさせ、最大スループットを見てみる

Webプロキシ/Squidで実測

• ハードウェア

- Dell R630
- Xeon(R) E5-2620 v3 x 2 Socket
 - 6 Cores + 6 Cores
 - HyperThreadは無効化
- 64GB RAM
- ST300MM0008 (300GB)
- Intel 82599ES 10G Ether

• ソフトウェア

- Ubuntu 19.10 server (eoan)
- Squid Version 4.8
 - SSL bumpを有効化して rebuild
 - Worker x 11を設定
 - CPU affinityで固定

すこし苦勞話を

- SSL Bumpが使えない

=> Rebuildしないと使えなかった_orz

- 性能が出ない(CPUを使い切れない)

=> Workersを設定しないとシングルプロセスで動く_orz

- それでも性能が安定しない

=> Hyper ThreadをOFFするのか_orz

試験構成(物理)

Webプロキシ / Squid



Dell R630

L2スイッチ



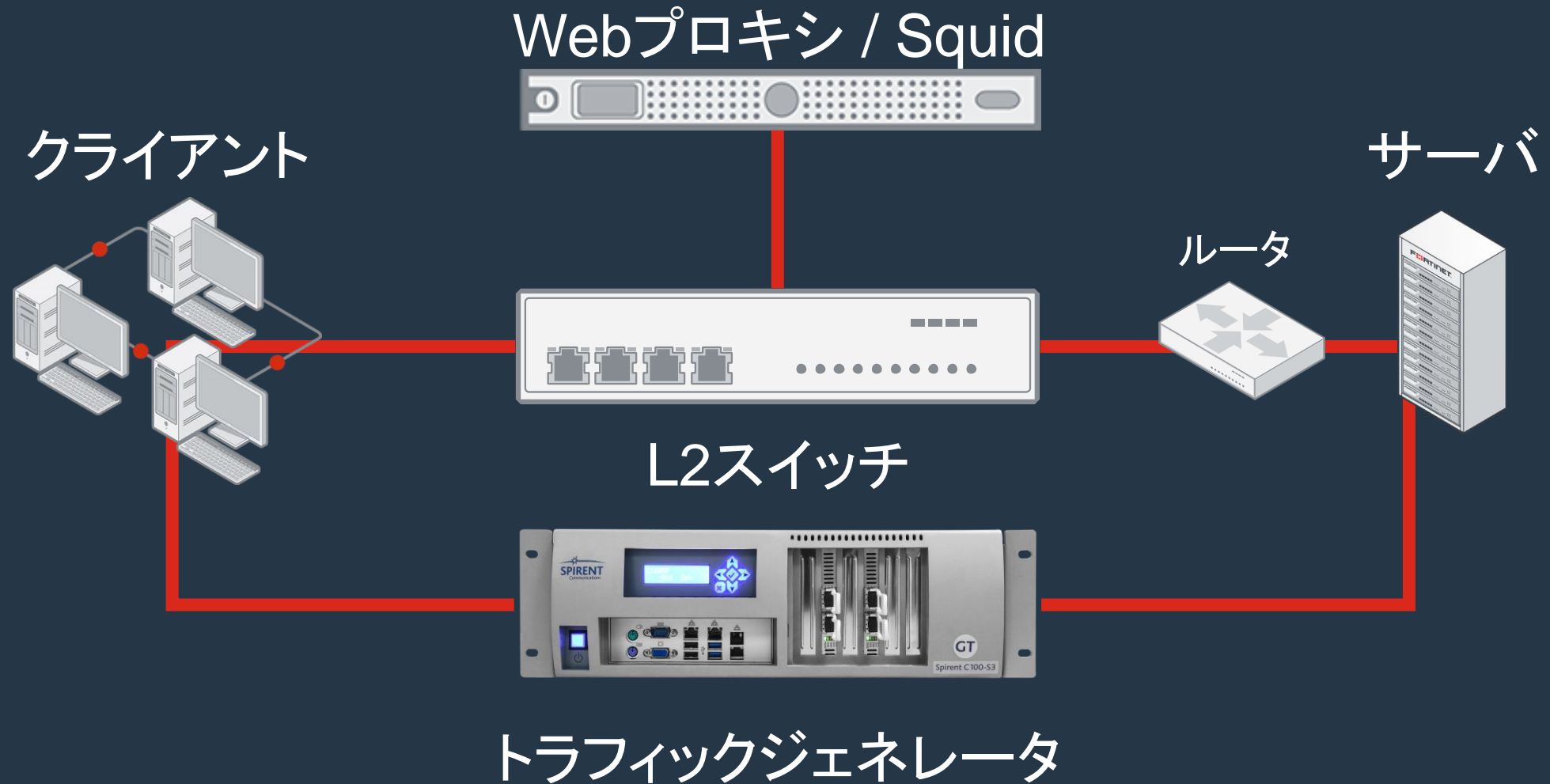
Cisco Nexus7706

トラフィックジェネレータ

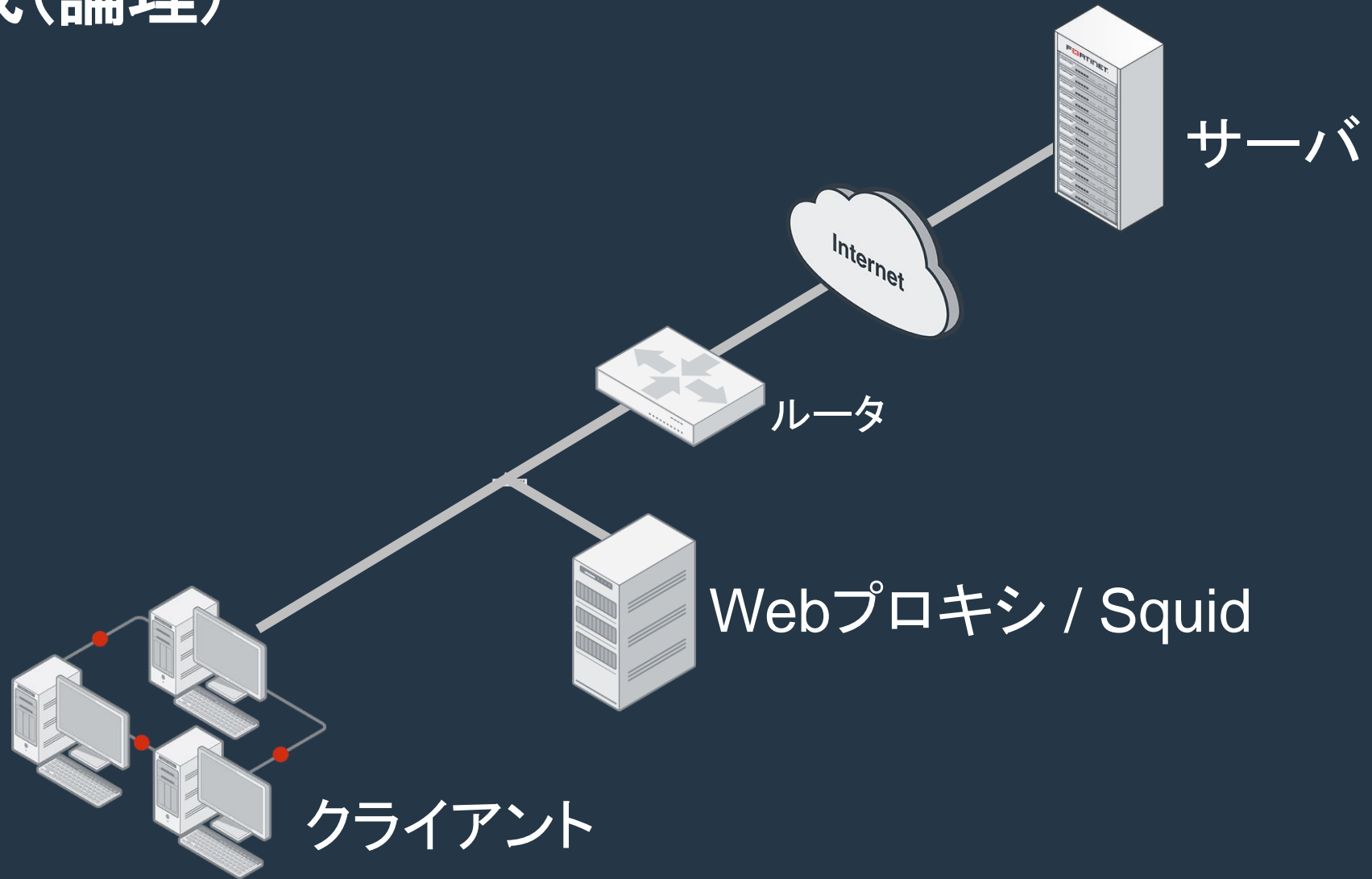


Spirent Avalanche
Model C100-S3-MP

試験構成(物理)



試験構成(論理)

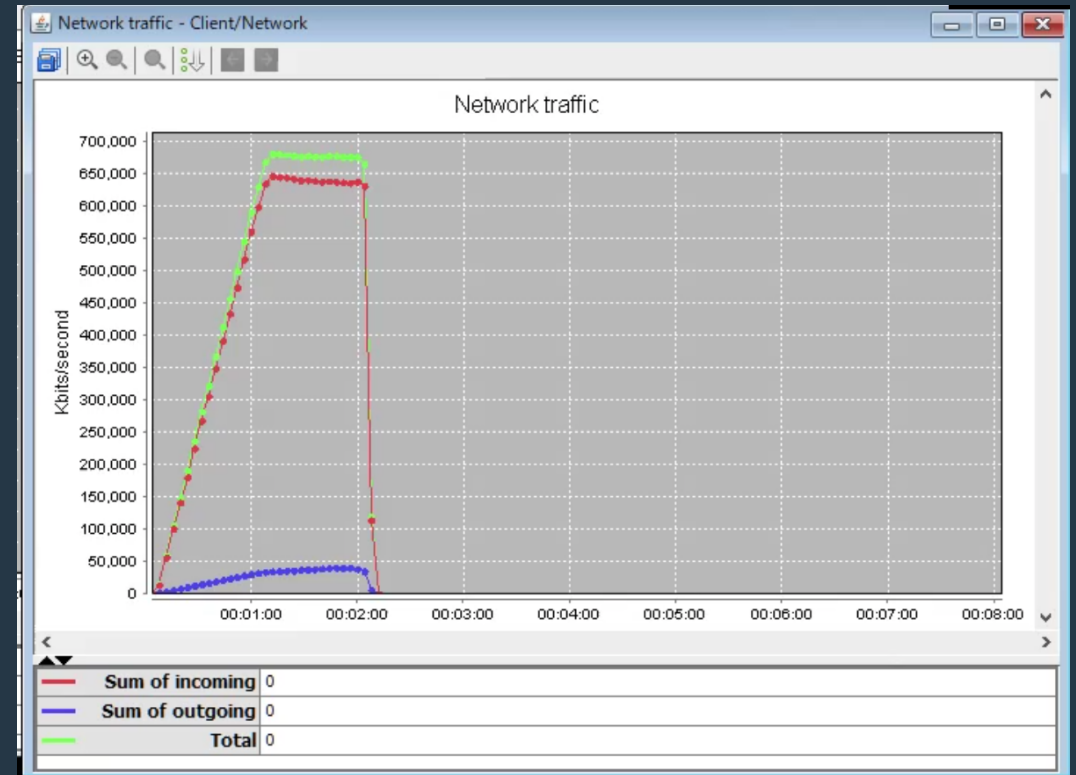
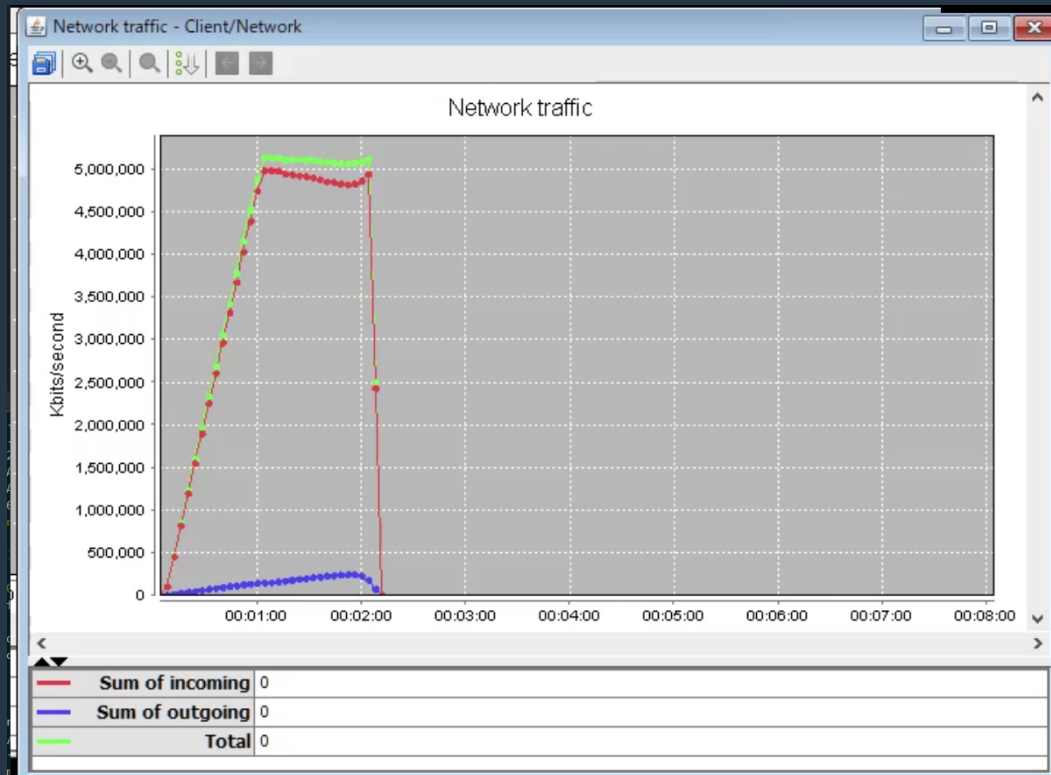


試験結果

1/8に低下!

HTTP 21KB – 5,100Mbps

HTTPS 21KB – 680 Mbps



そろそろSSL通信に本気出して向き合ってみる

- Webトラフィックの8割が暗号化されている
- SSLインスペクションは避けては通れない？
- 組織ネットワークセキュリティの見直しが必要
- どこまで？どのように？

FORTINET[®]