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?

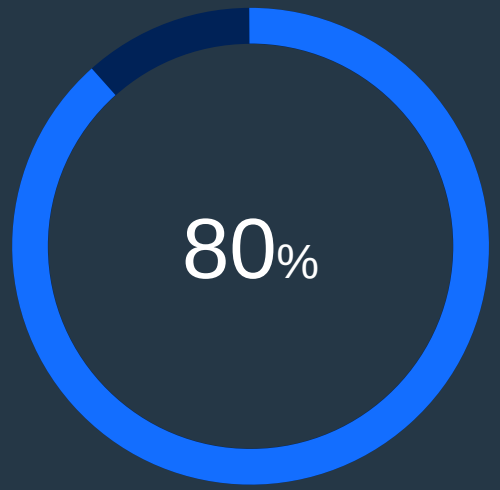
フォーティネットジャパン　コンサルティングSE 杉井義久

本セッションにあたって

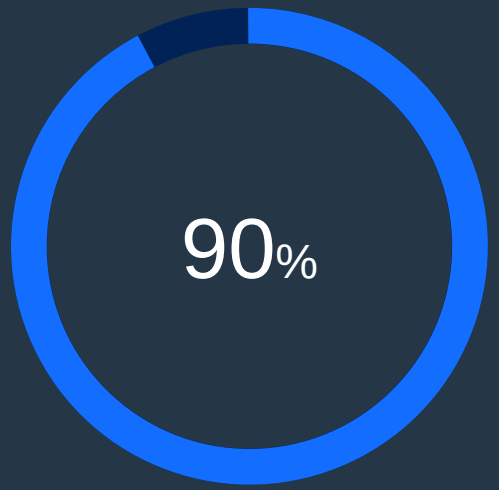
- 個人的な所感ですが、インターネットはできる限り自由であるべきだと考えています。
- もしも自分が所属組織ネットワークセキュリティの運用・管理をまかされたら、という前提で聞いて頂けると幸いです。
- わかりやすさを優先し、本セッションでは“SSL”というタームを利用しますが、厳密にはSSL3.0の利用は禁止され、TLSへ移行しております。

SSL通信の現状を探ってみる

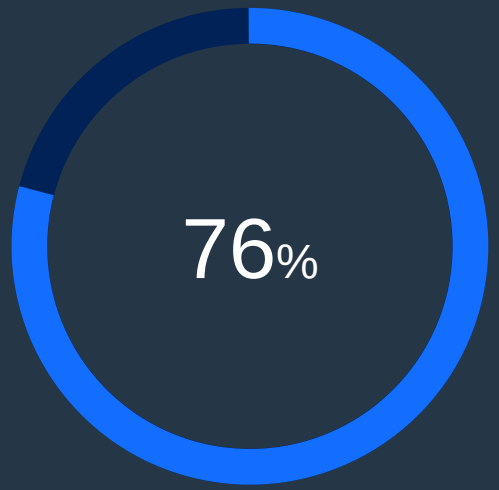
SSL通信の現状を探ってみる



Mobile

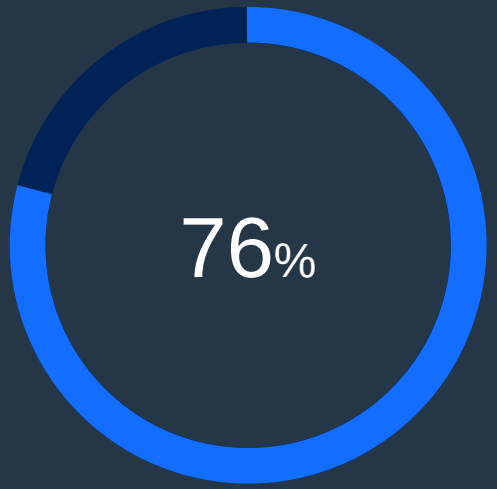


Google



Enterprise

SSL通信の現状を探ってみる

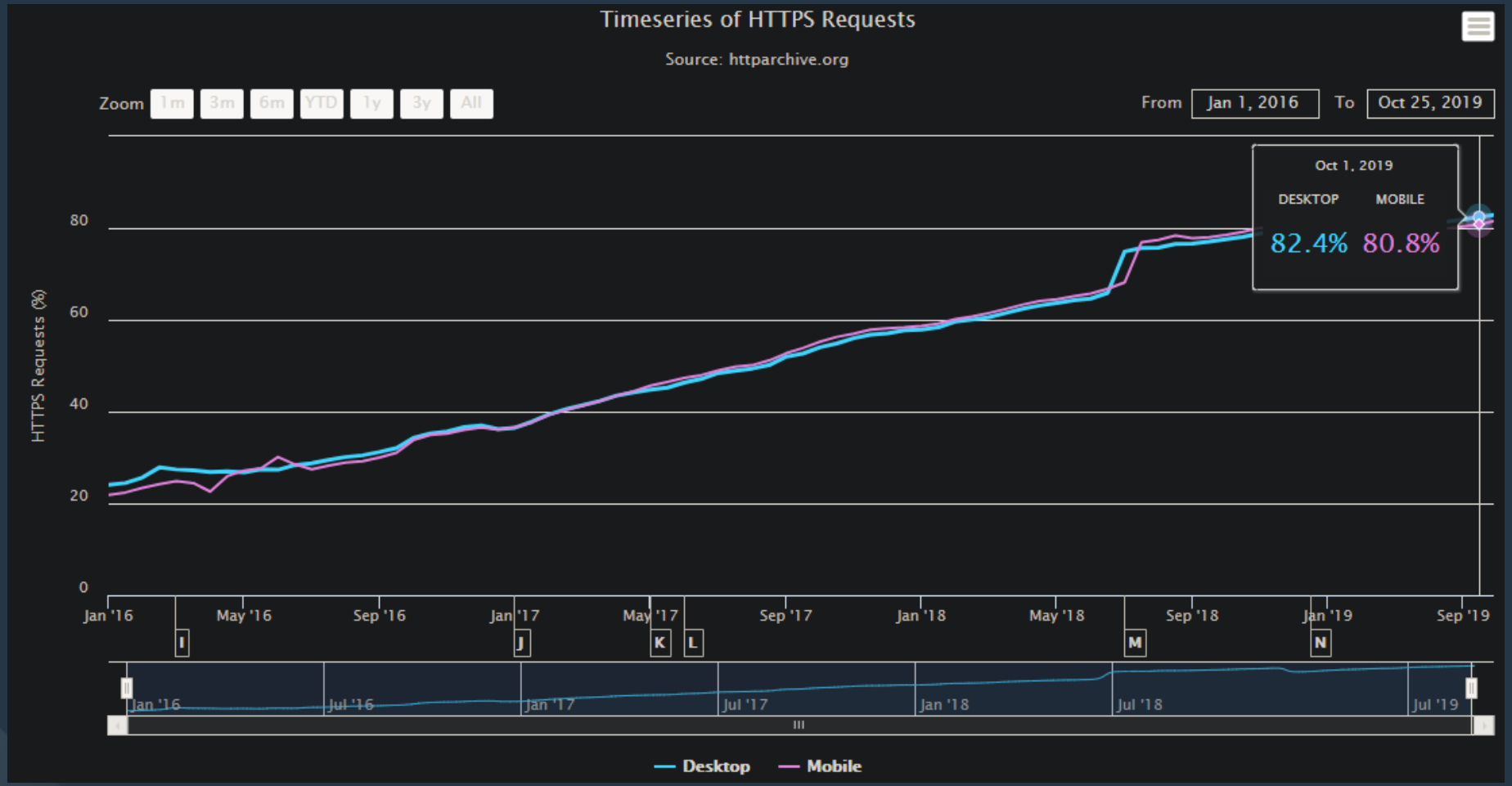


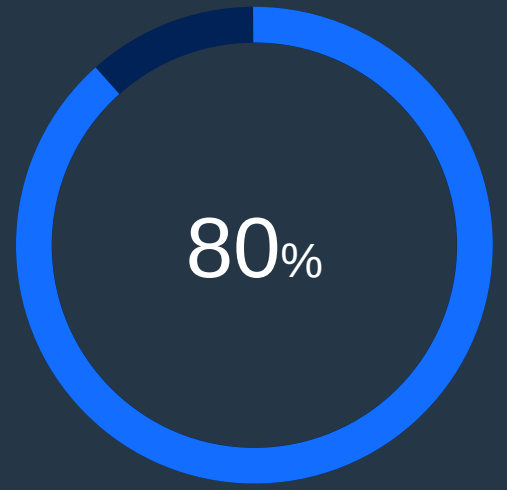
全上場企業における
常時SSL化対応状況
（2019年12月）

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

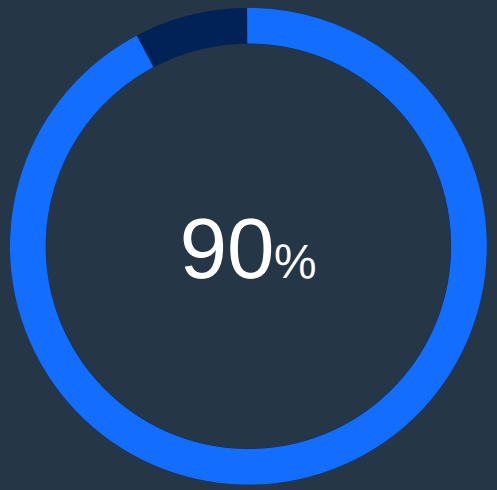




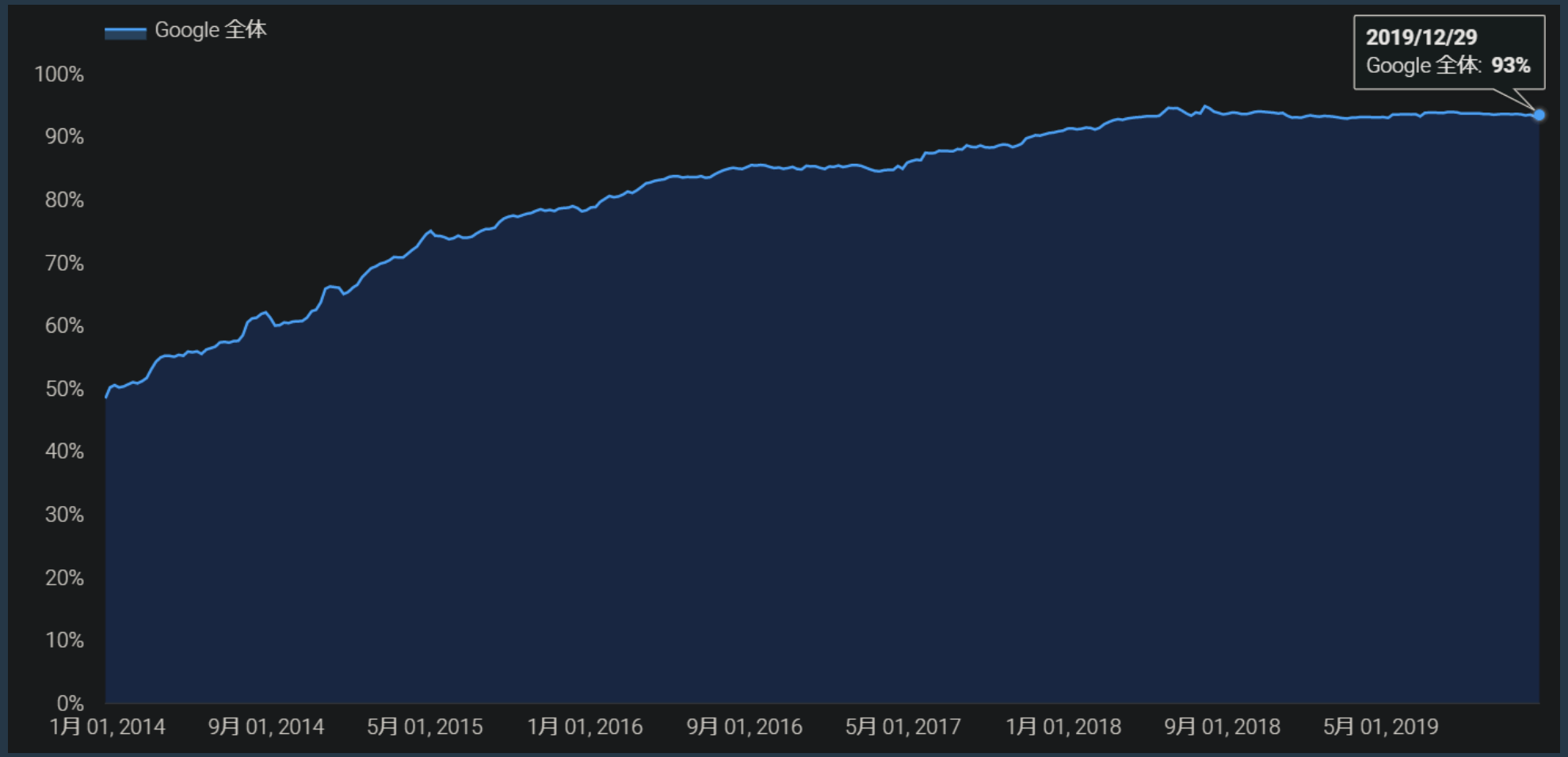
HTTPSリクエストの割合

引用元：http archive: State of Web
https://httparchive.org/reports/state-of-the-web

SSL通信の現状を探ってみる

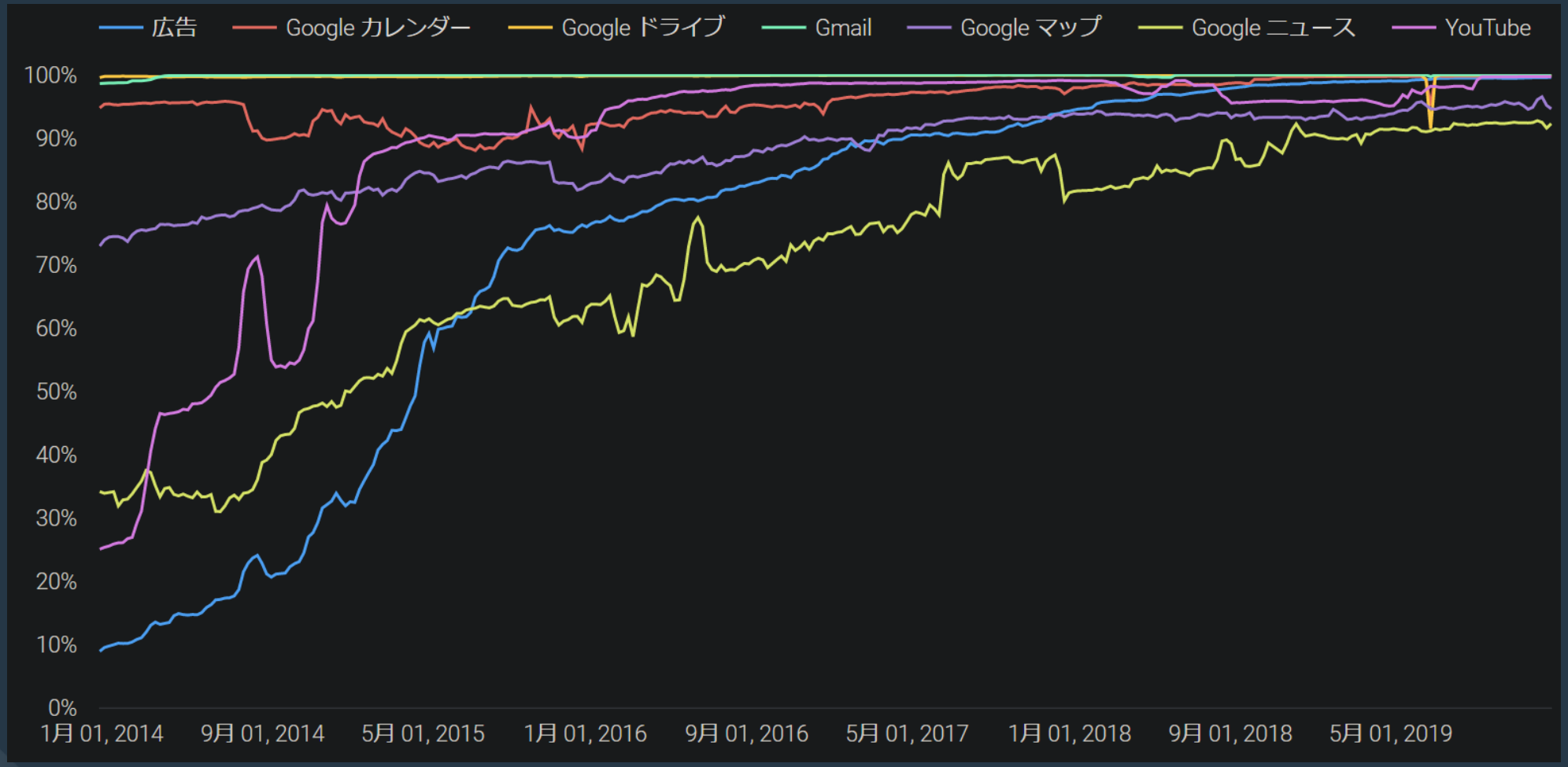


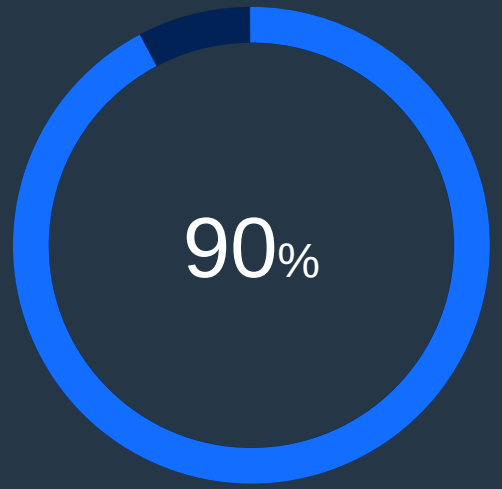
Googleサービス



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



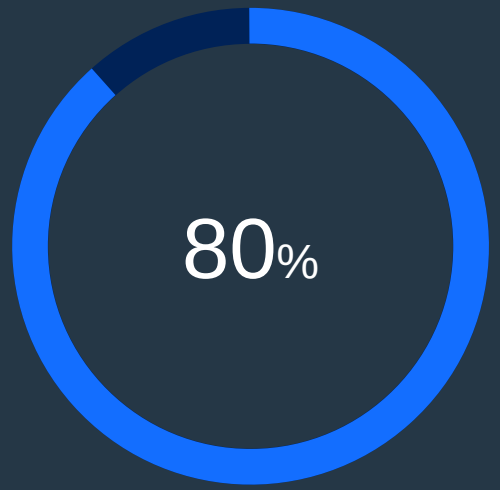


Googleサービス

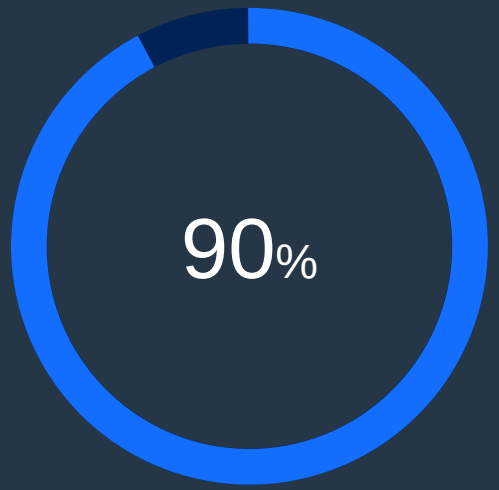
引用元：Google: 透明性レポート
https://httparchive.org/reports/state-of-the-web

FORTINET

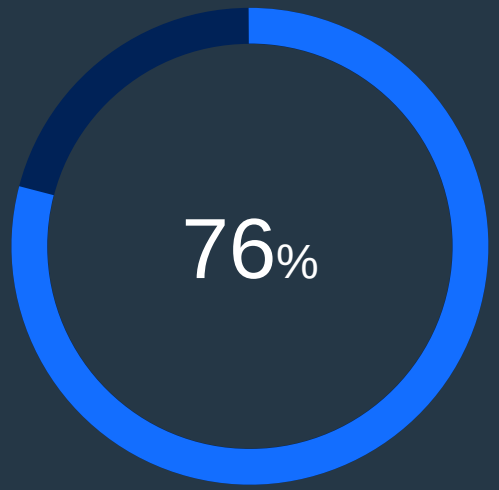
常時SSL化 - ざっくり8割



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

申請者

認証局

実在証明

申請者

確認します

認証局

実在証明

申請者

認証局

実在証明

申請者

認証局

実在証明

申請者

確認とれました

認証局

実在証明

申請者

認証局

認証局から発行された証明書だと

https://www.janog.gr.jp 170%

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

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。

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 若者支援プログラムについてはこちら]

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)

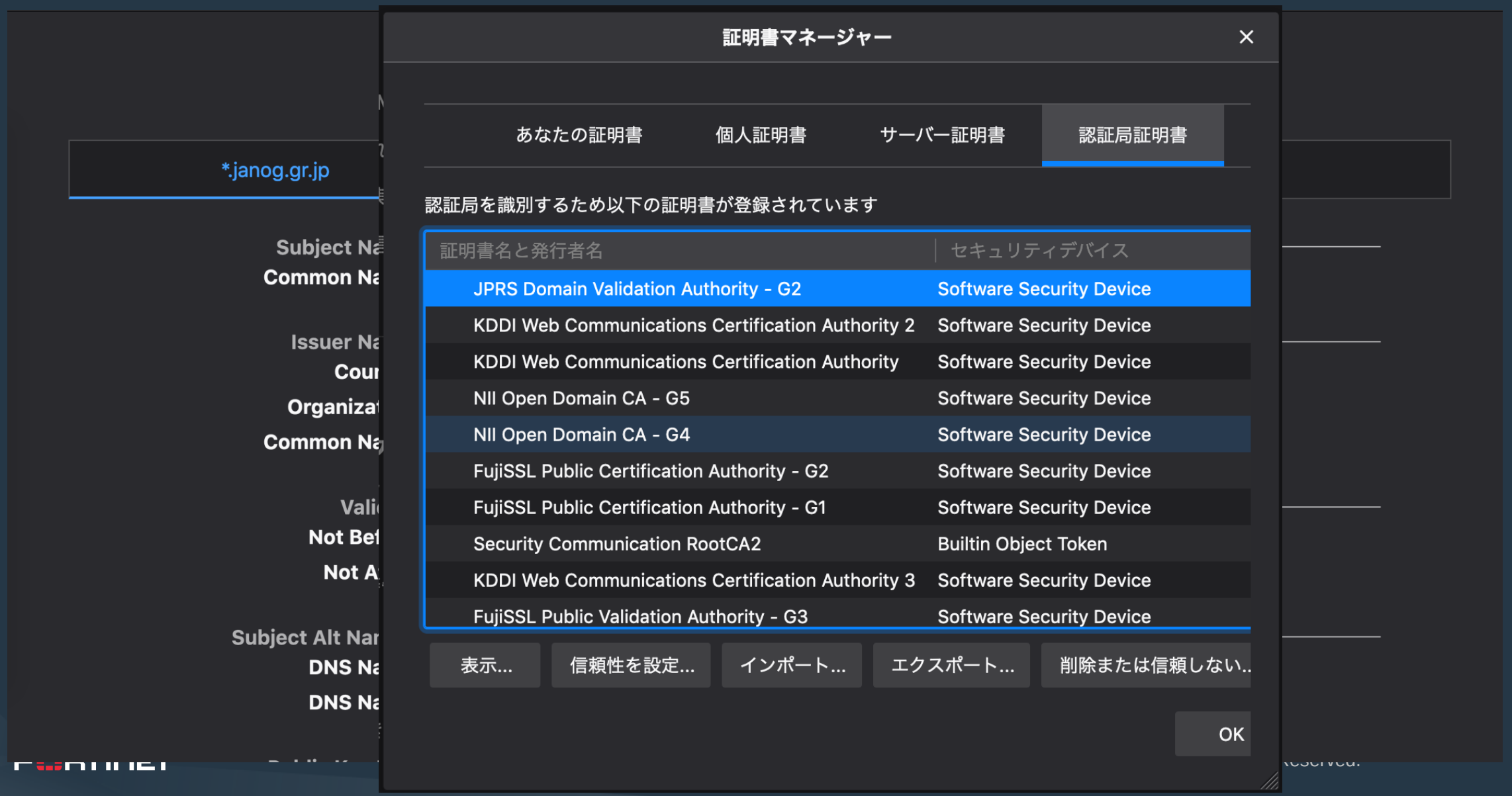
Not After 2021/1/31 23:59:59 (Asia/Tokyo)

Subject Alt Names

DNS Name *.janog.gr.jp

DNS Name janog.gr.jp

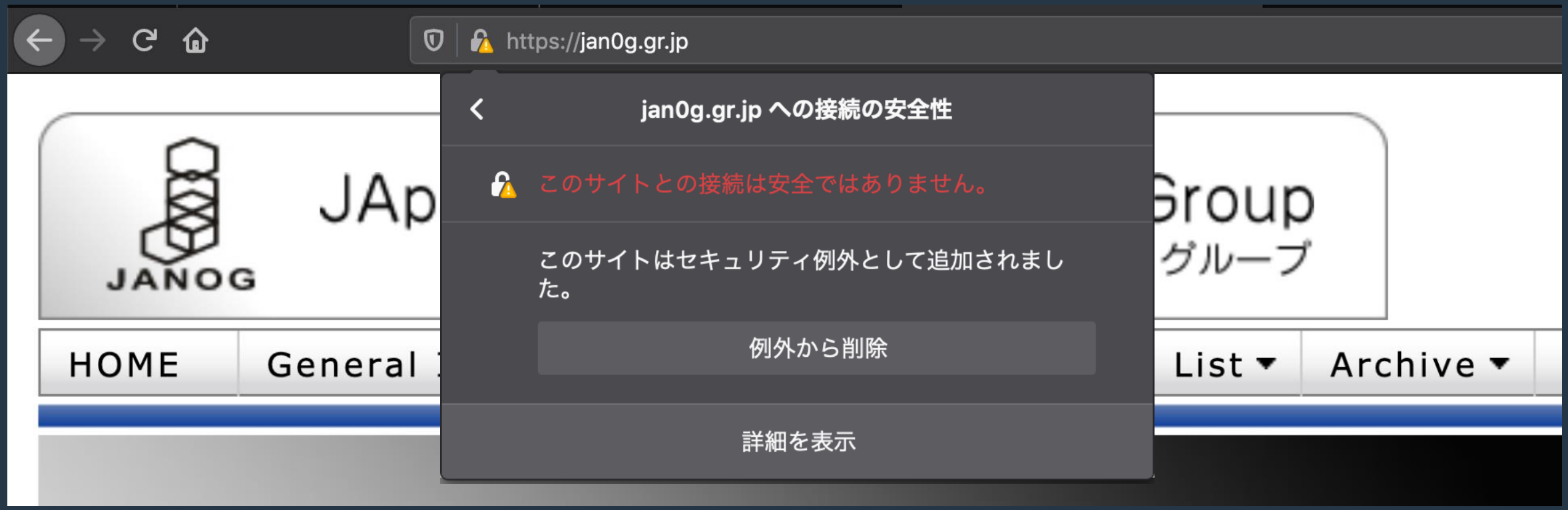
認証局から発行された証明書だと



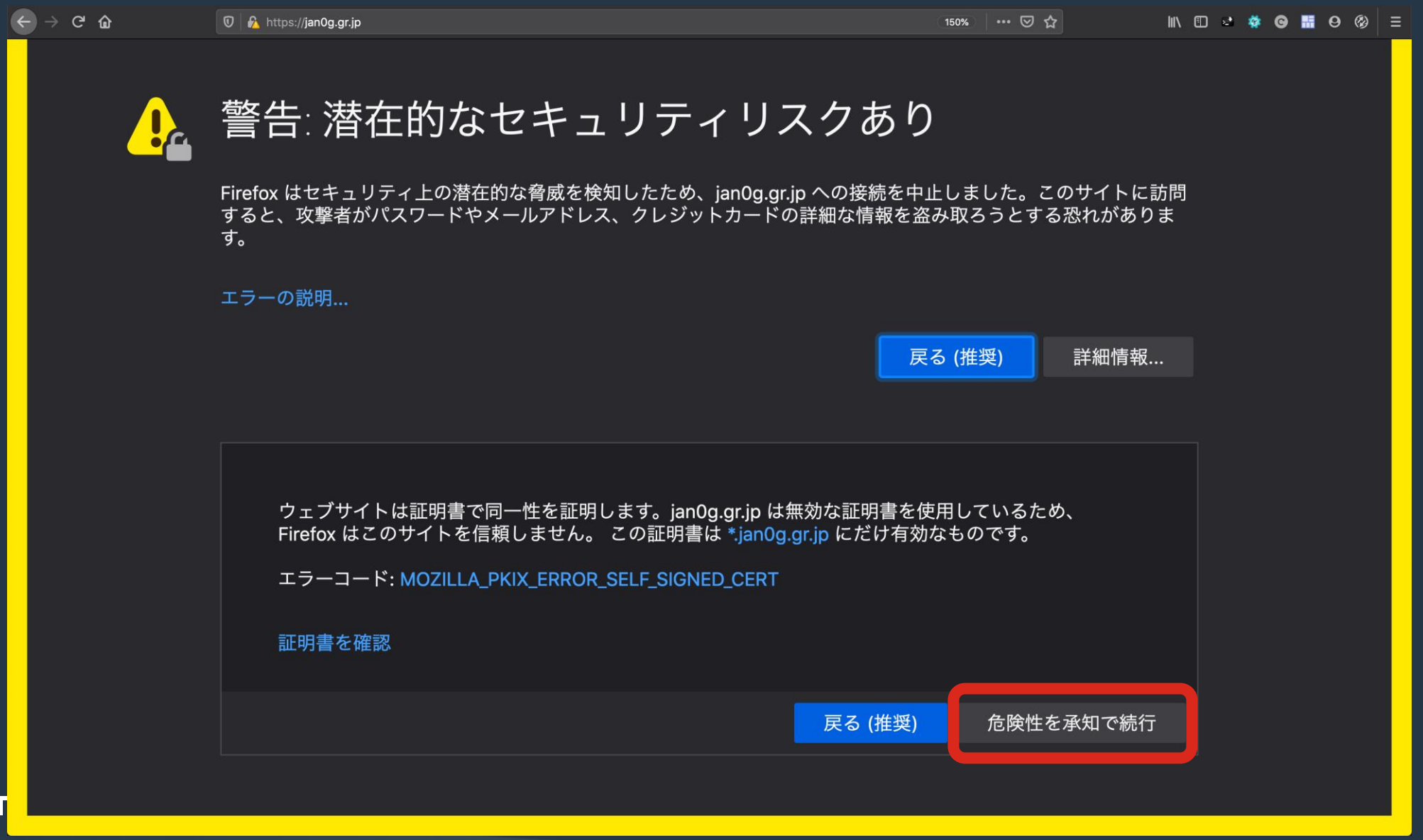
信頼された認証局を通していない証明書（＝オレオレ証明書）だと

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



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

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/Bowser 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証明書との更なる差別化が図られている。

IIJ, 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.iij.ad.jp/company/development/report/iir/030/01_04.html

https://www.janog.gr.jp/meeting/janog39/program/evssl.html

SSLについておさらいしてみる

実在証明

暗号化通信

暗号化通信

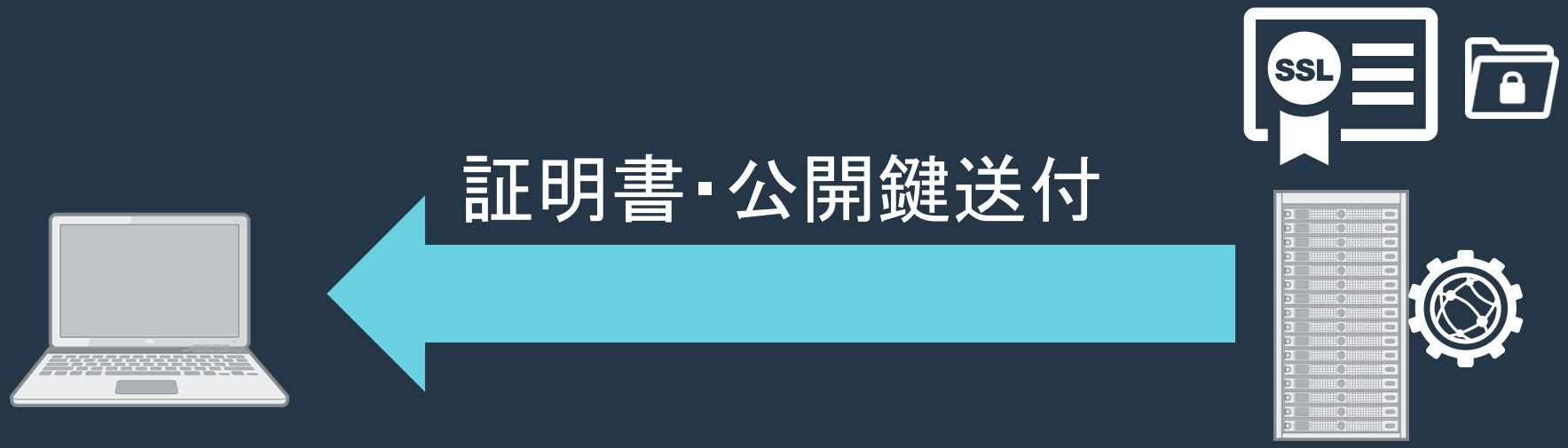
HTTP(暗号化無し)でのアクセスだと

暗号化通信

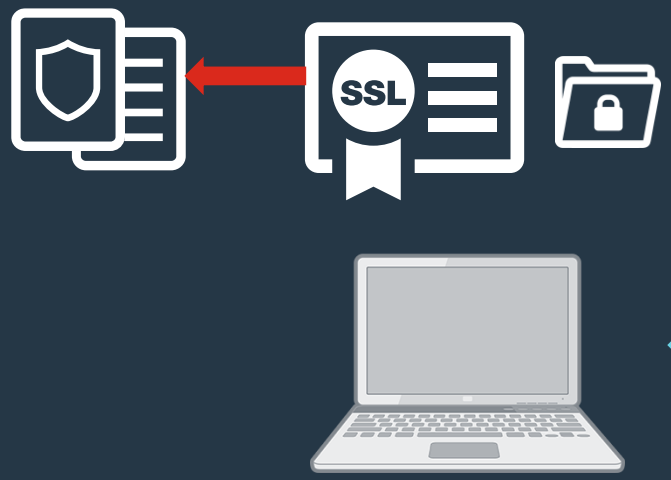
End to End 暗号化

暗号化通信

暗号化通信



暗号化通信



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

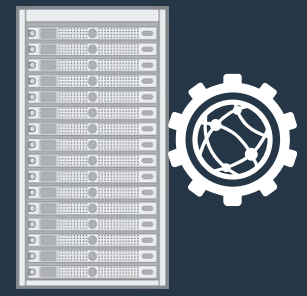
表示... | 信頼性を設定... | インポート... | エクスポート... | 削除または信頼しない...

OK

FORTINET

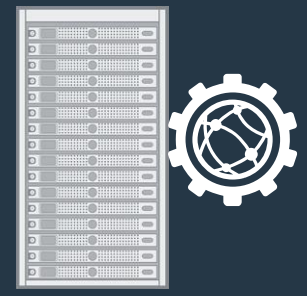
暗号化通信

共通鍵を作成

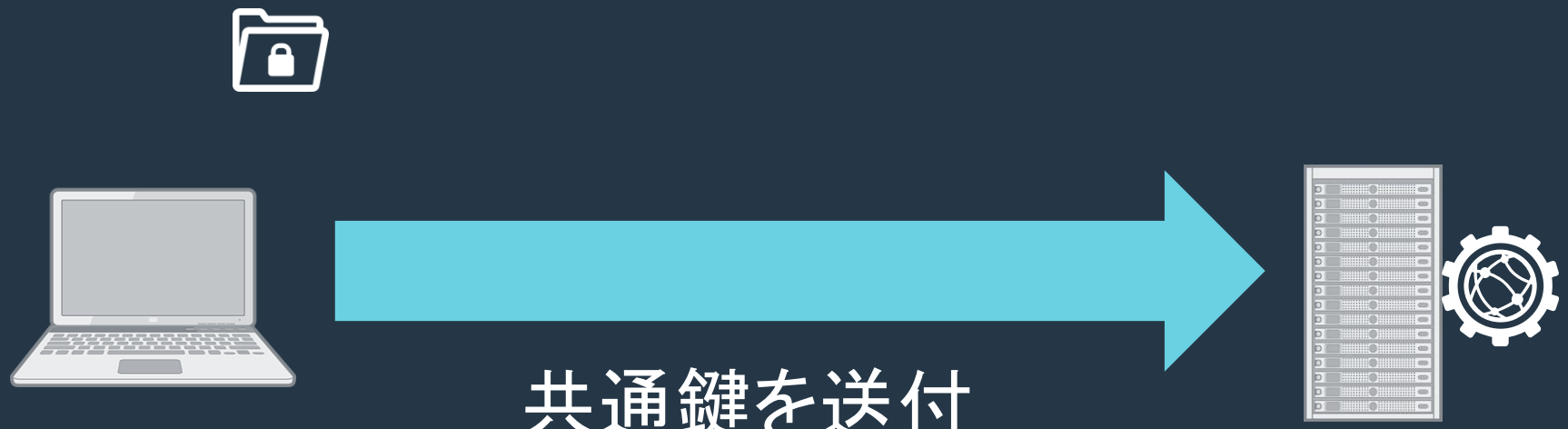


暗号化通信

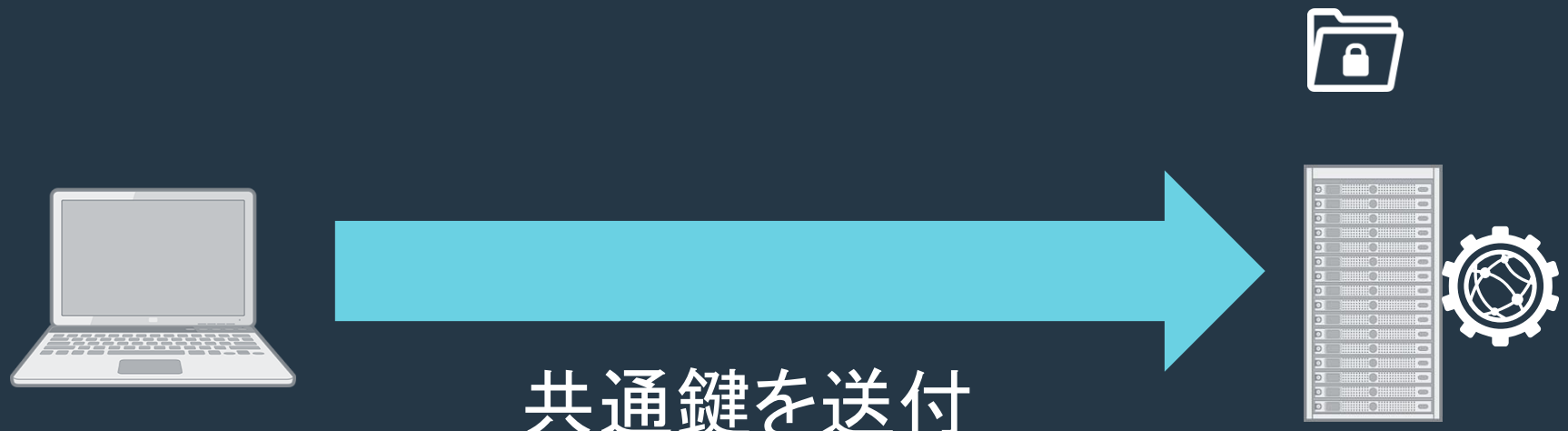
公開鍵で共通鍵を
暗号化



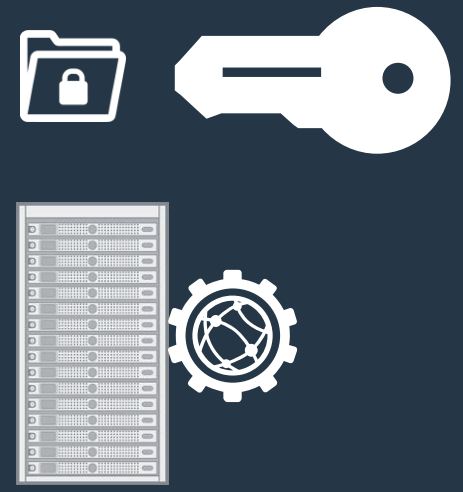
暗号化通信



暗号化通信



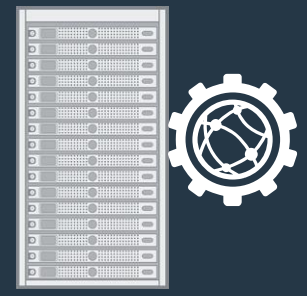
暗号化通信



秘密鍵で共通鍵を解錠

暗号化通信

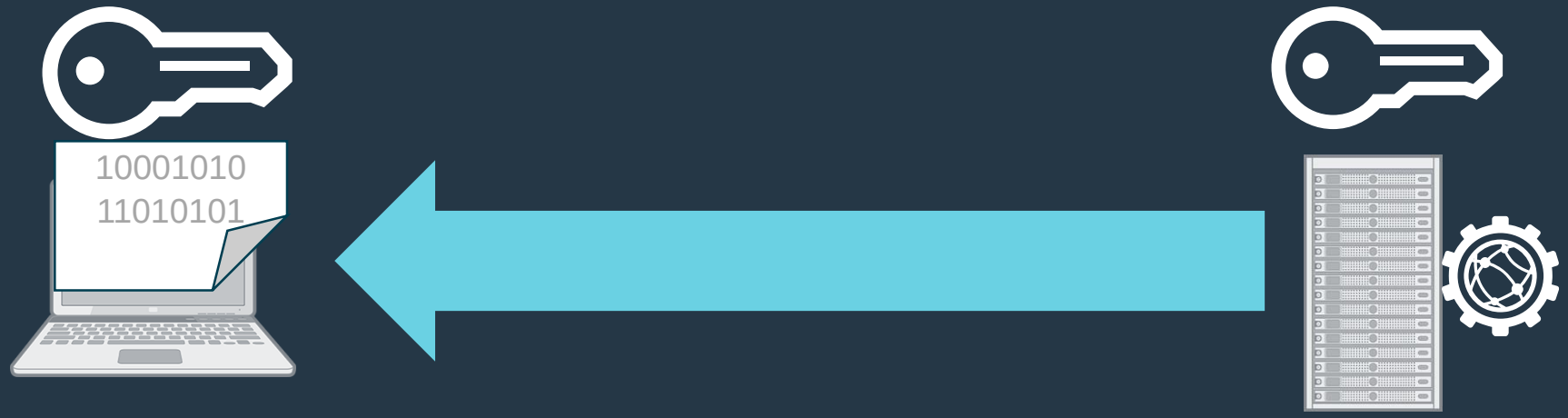
共通鍵の交換完了！



暗号化通信

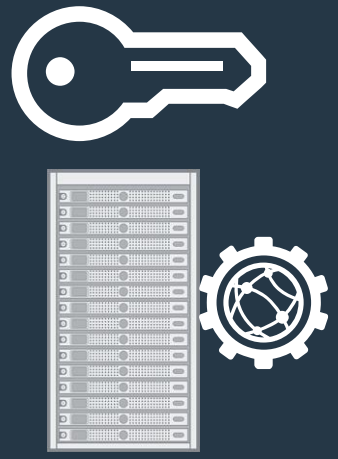
共通鍵で暗号化して送信

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

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？

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？

鍵マークがついている！

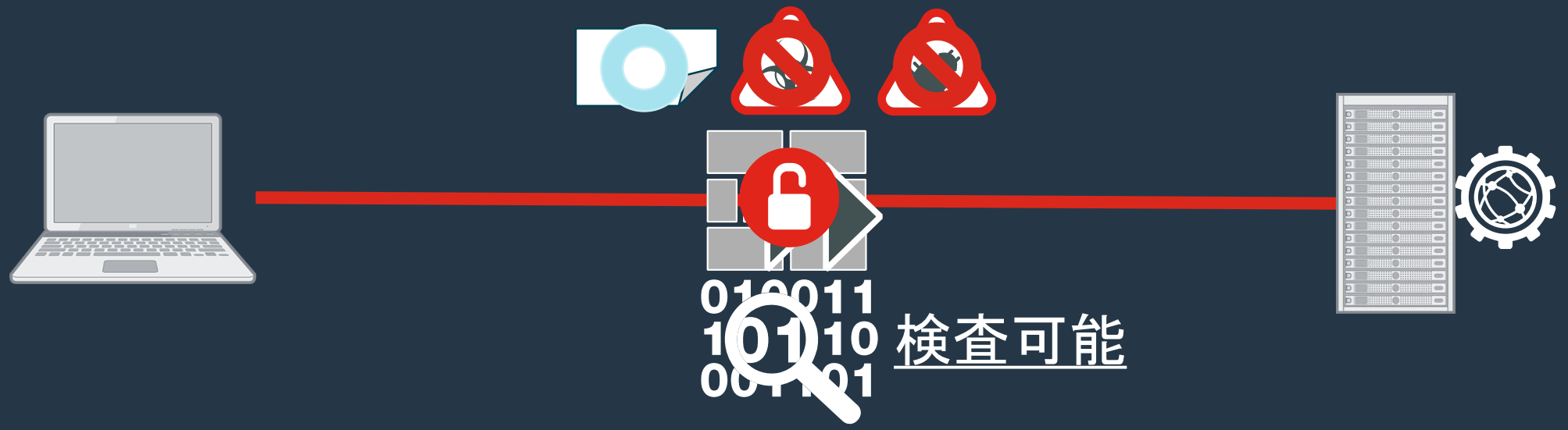
鍵マークがあれば本当に安心なのか？

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？

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

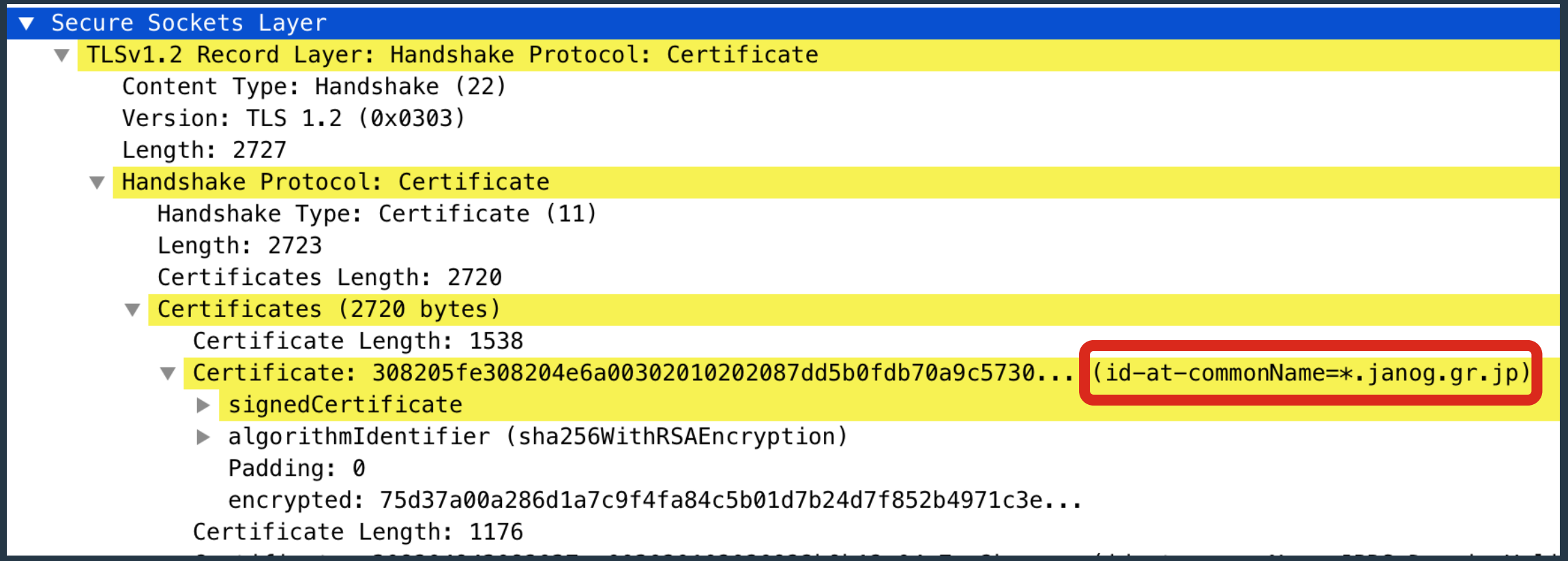
ネットワークレベルでの対抗策

- 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

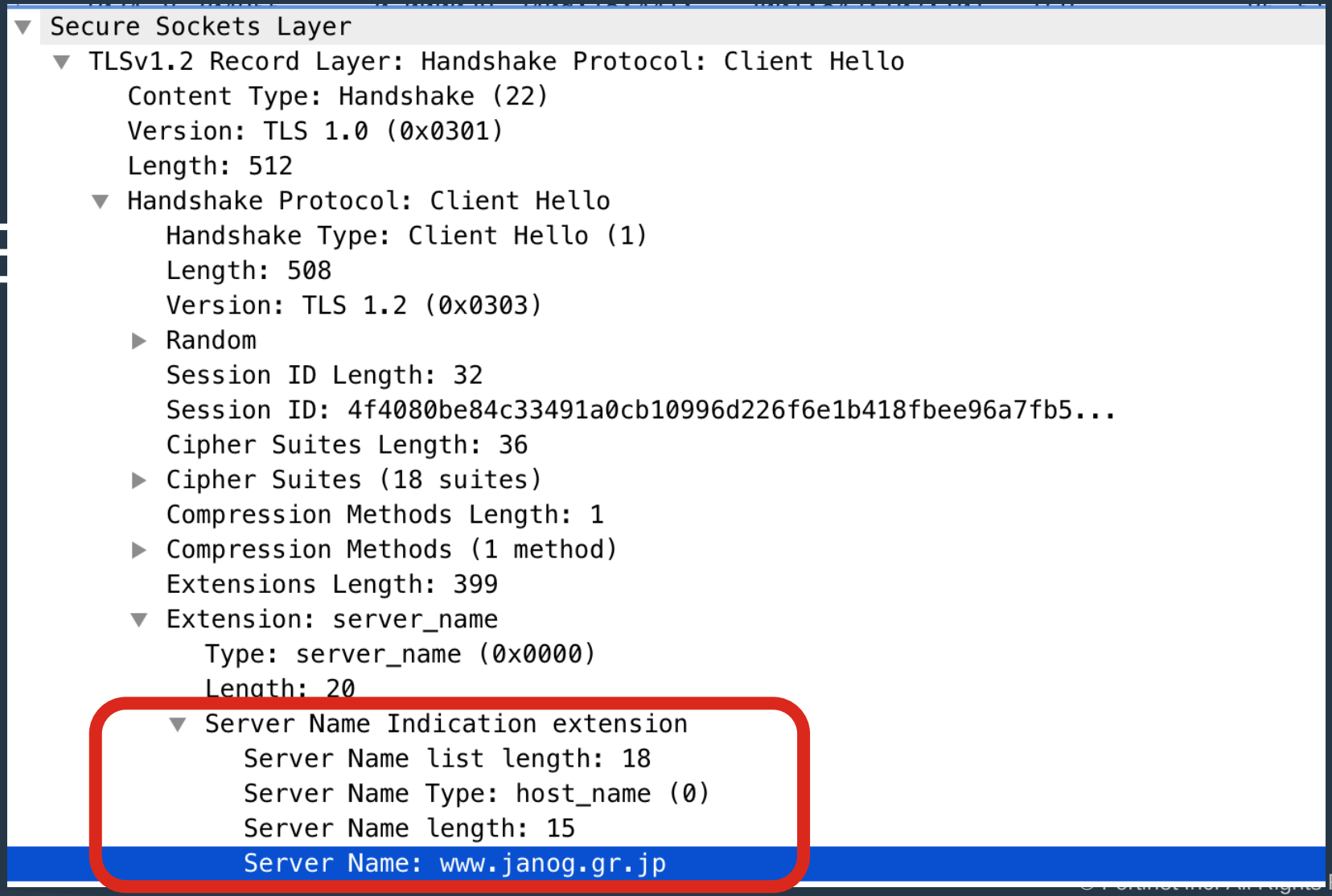


証明書インスペクション

- 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
- CLIE



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

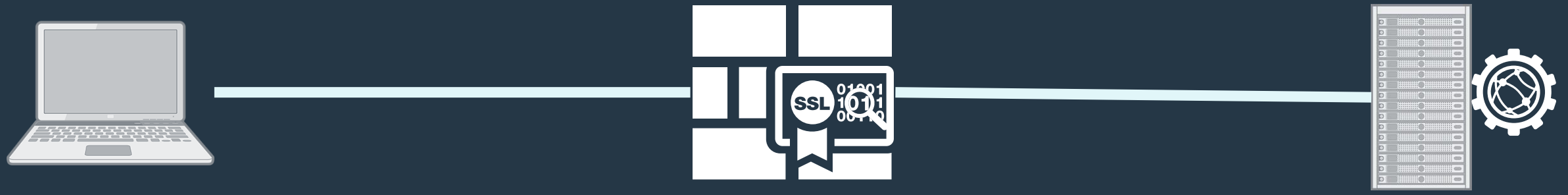
ネットワークレベルでの対抗策

- 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）

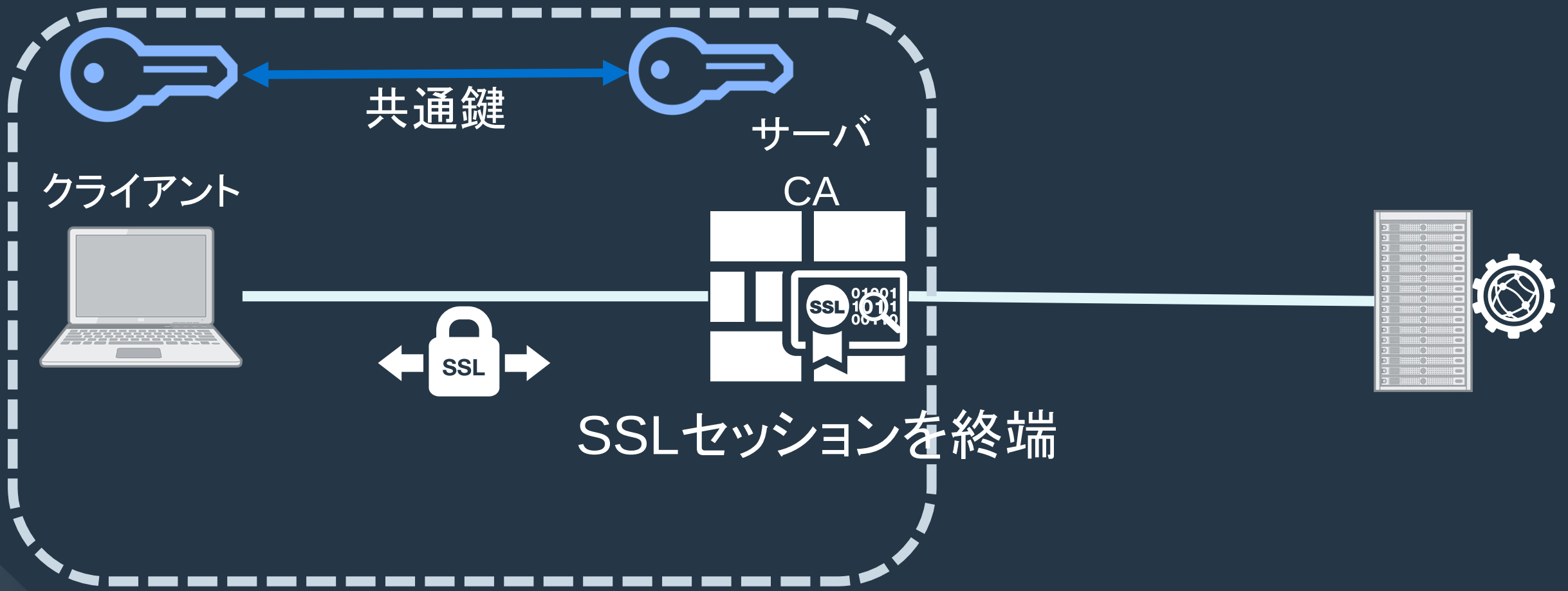
SSL Deepインスペクション

SSL Deepインスペクション

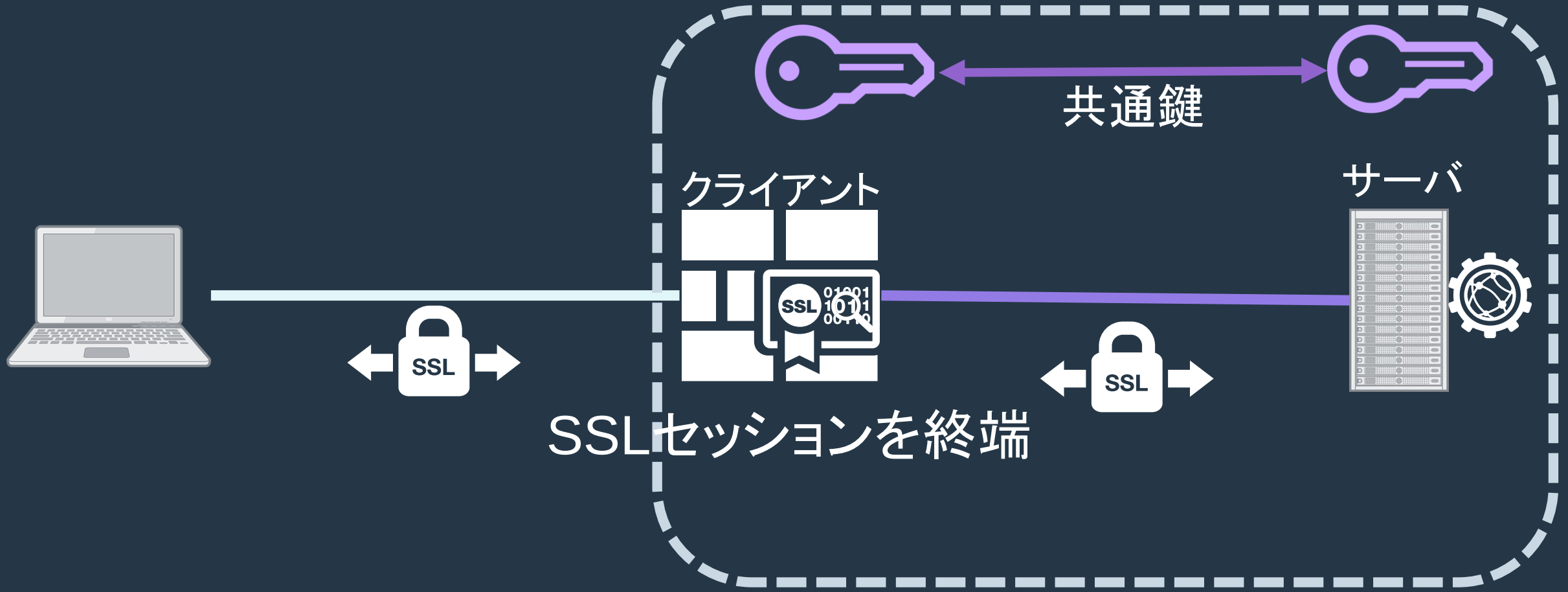
ファイアウォール、プロキシ



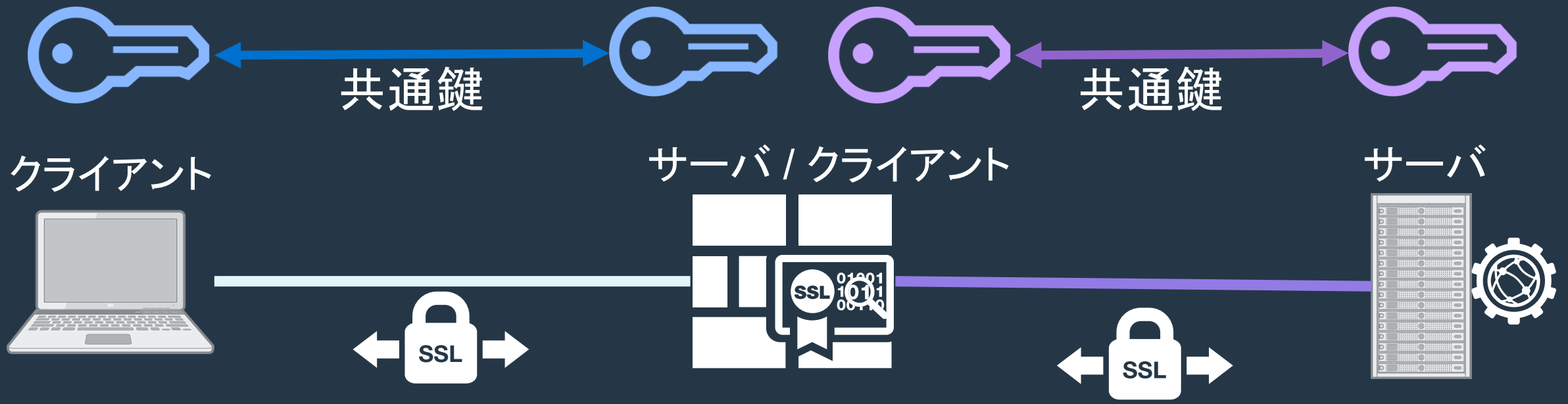
SSL Deepインスペクション



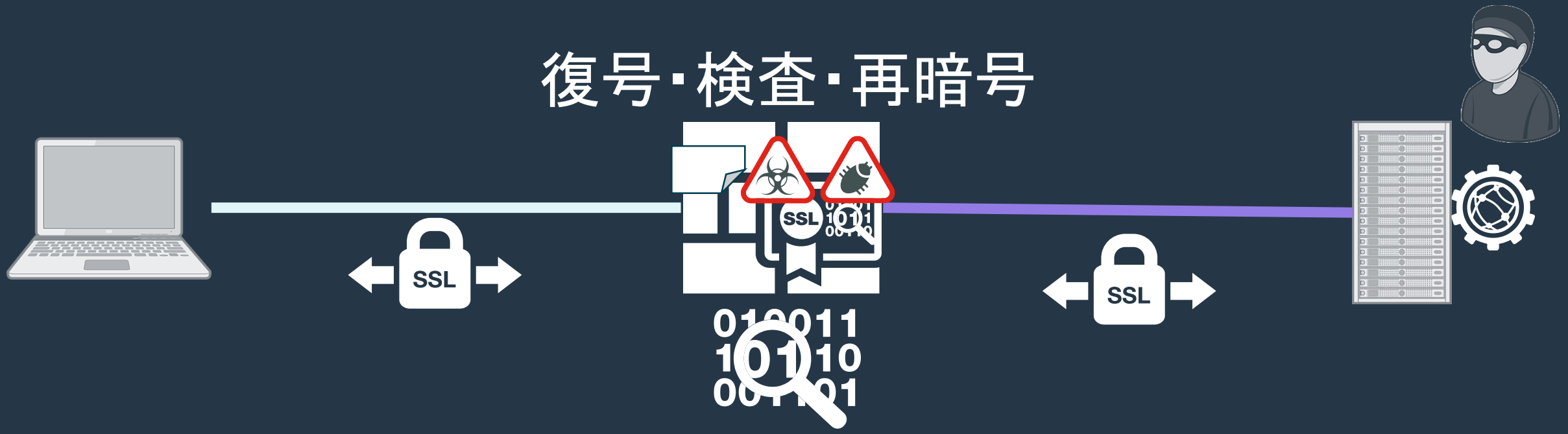
SSL Deepインスペクション



SSL Deepインスペクション



SSL Deepインスペクション

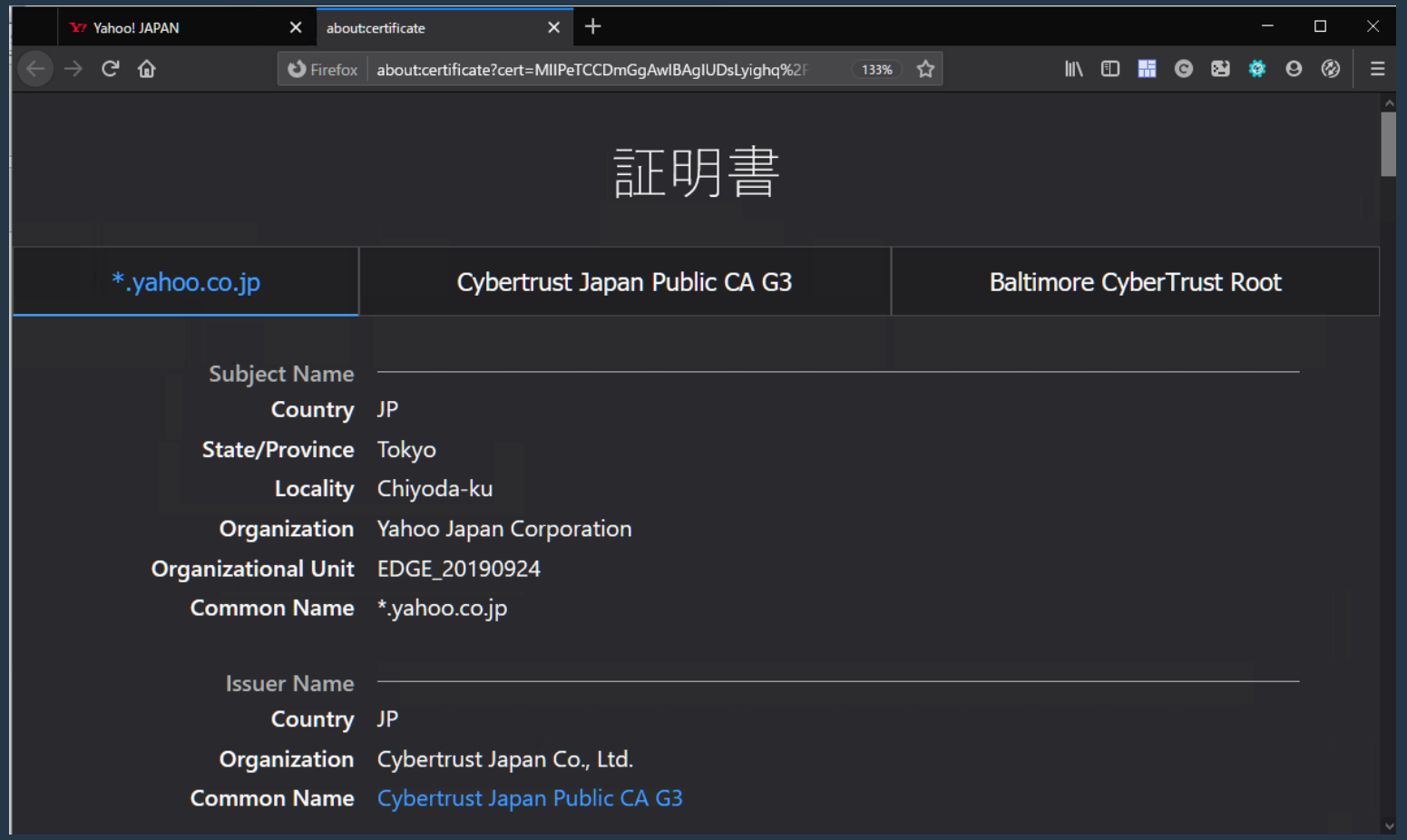


SSL Deepインスペクション

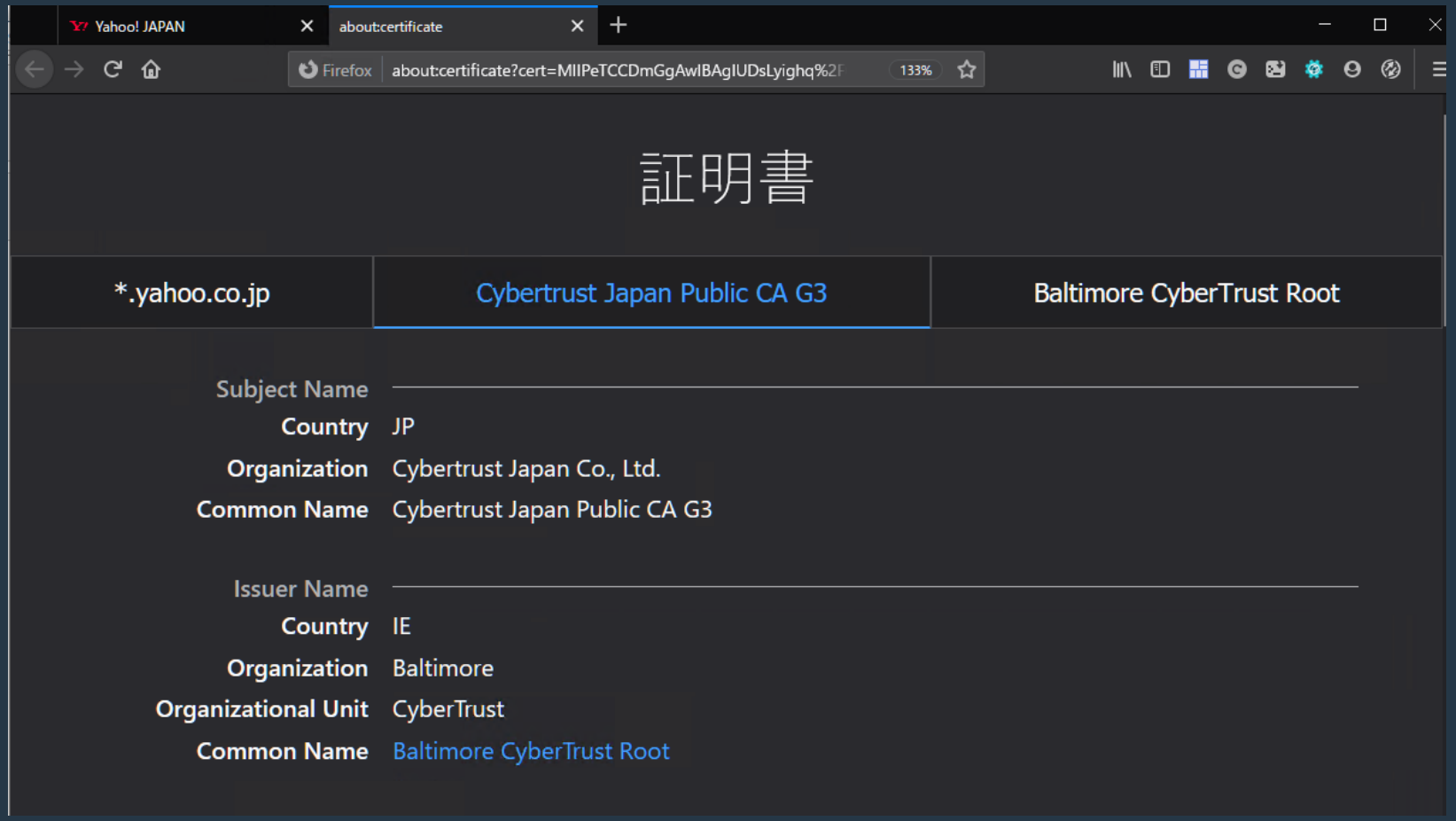
- ようは、Man In The Middle
- 証明書エラーの対処が必要

普通にアクセスすると

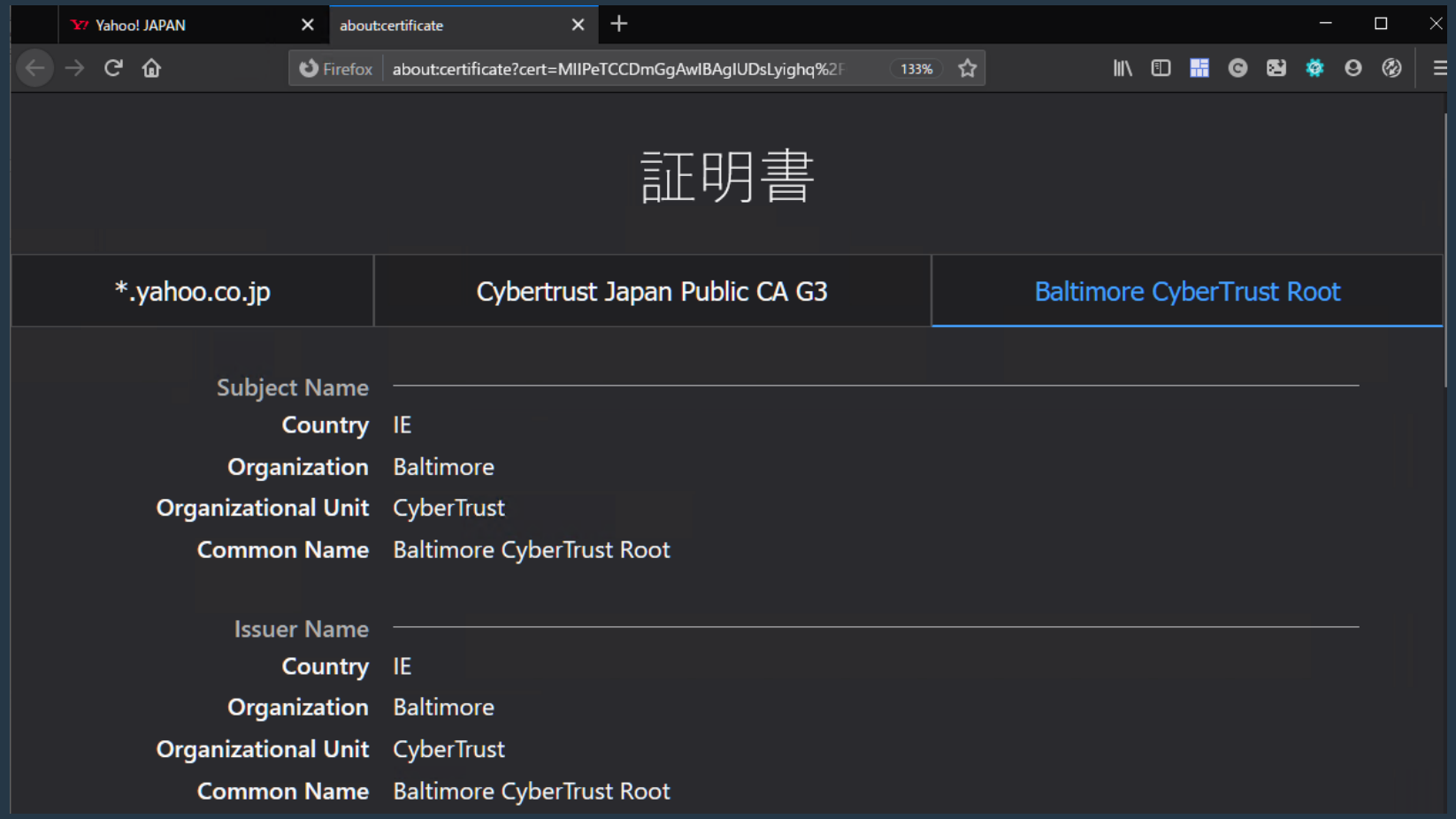
普通にアクセスすると



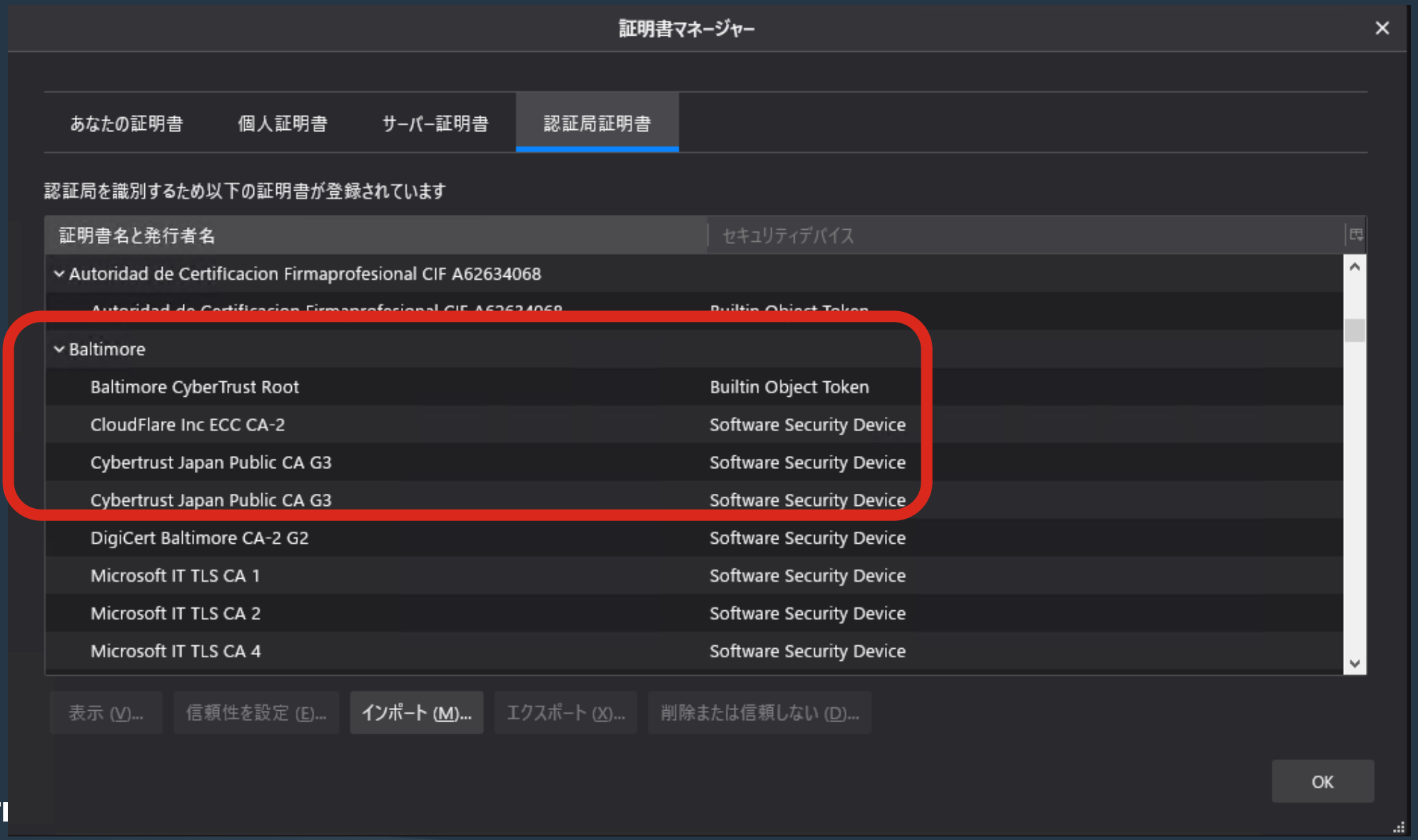
普通にアクセスすると



普通にアクセスすると

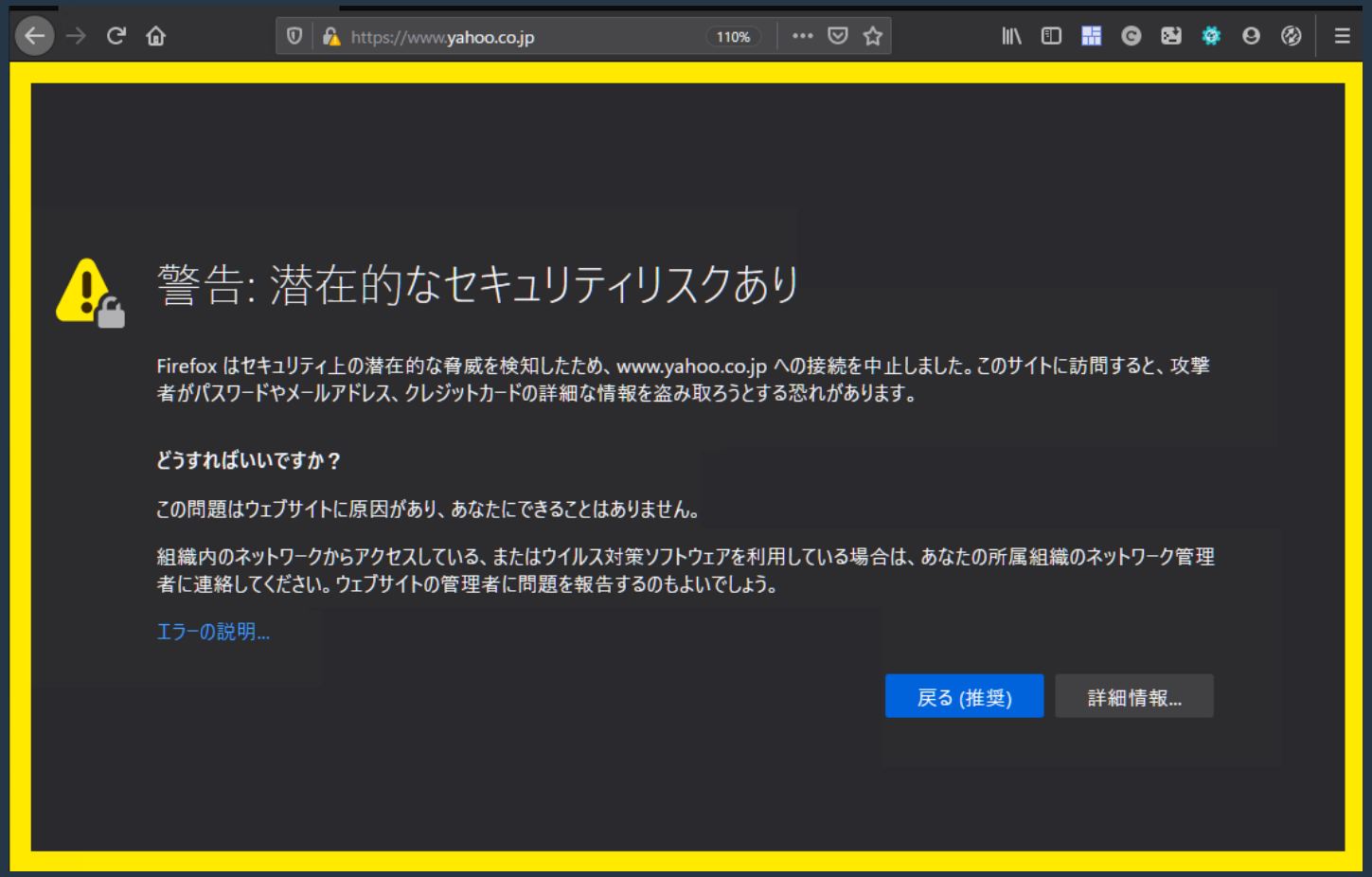


ブラウザ（Firefox）にインストール済み



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

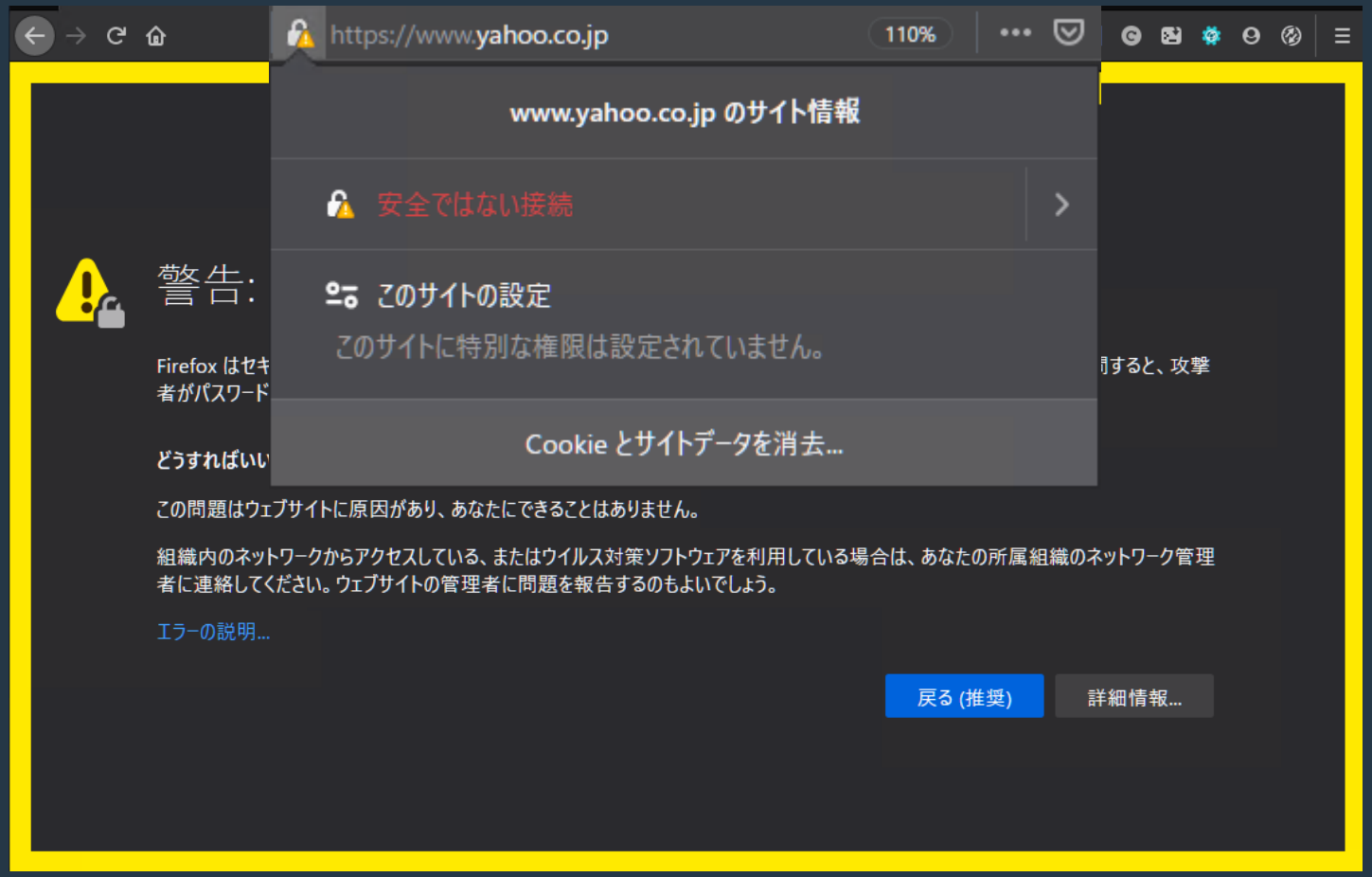


警告が出た

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



警告が出た

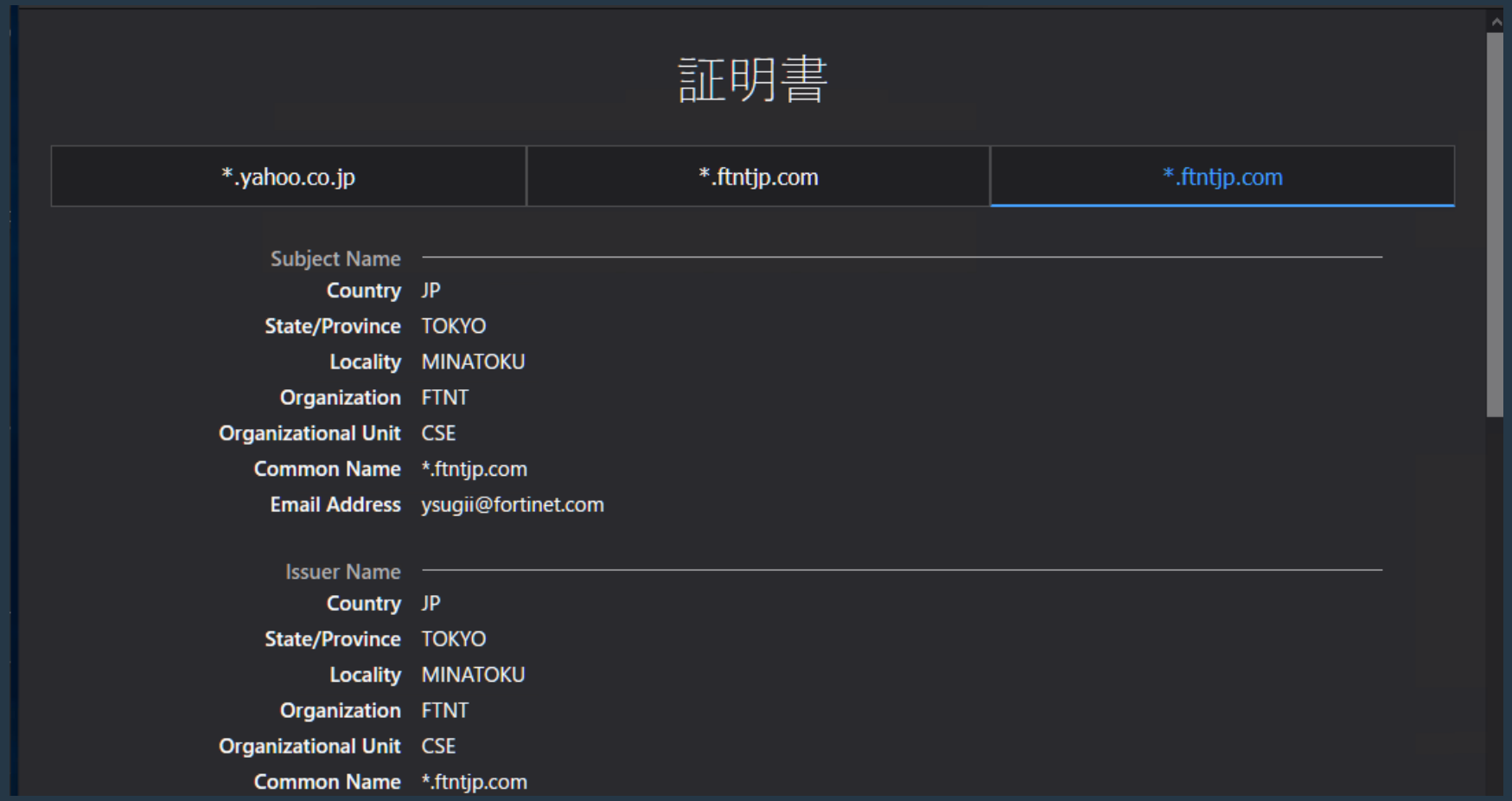
SquidでSSLインスペクションをすると

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

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

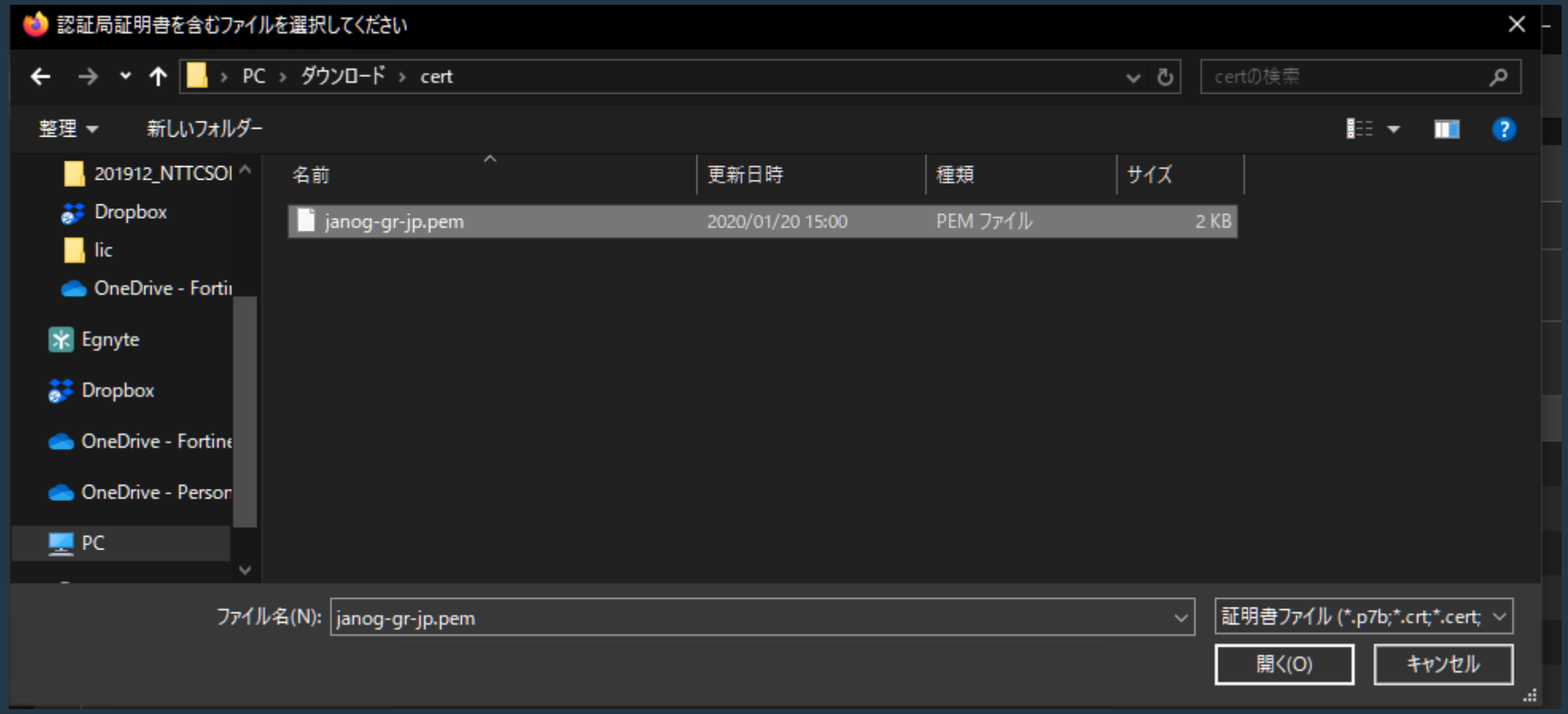


Issuerが認証局証明書リストにないため

SquidでSSLインスペクションをすると

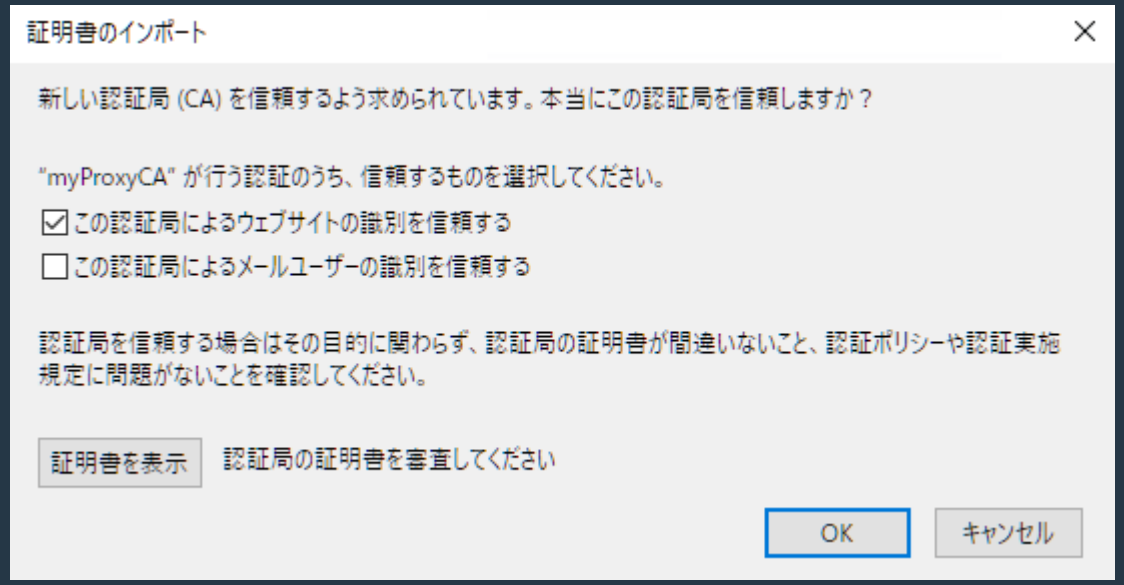
CA証明書をインポートすると

SquidでSSLインスペクションをすると



CA証明書をインポートすると

SquidでSSLインスペクションをすると



CA証明書をインポートすると

SquidでSSLインスペクションをすると

警告は消えたが、、、

SquidでSSLインスペクションをすると

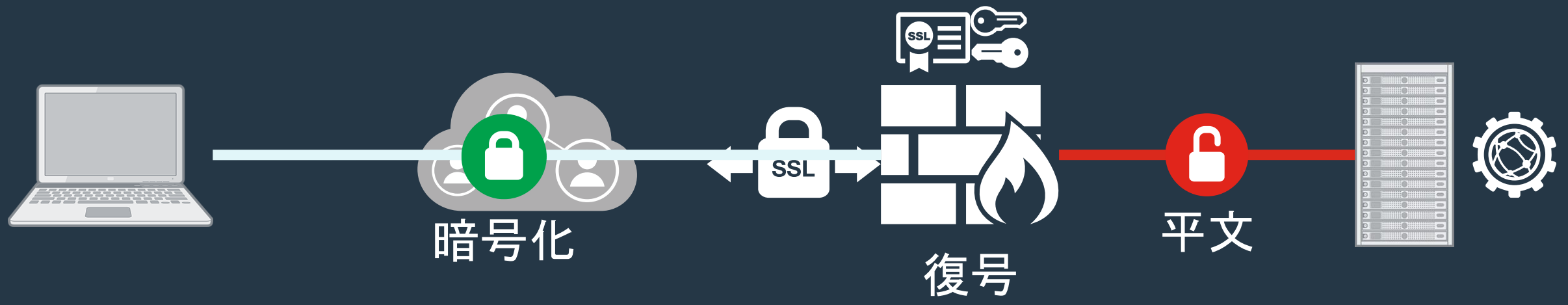
警告は消えたが、、、

余談：SSL オフロードとの違い

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

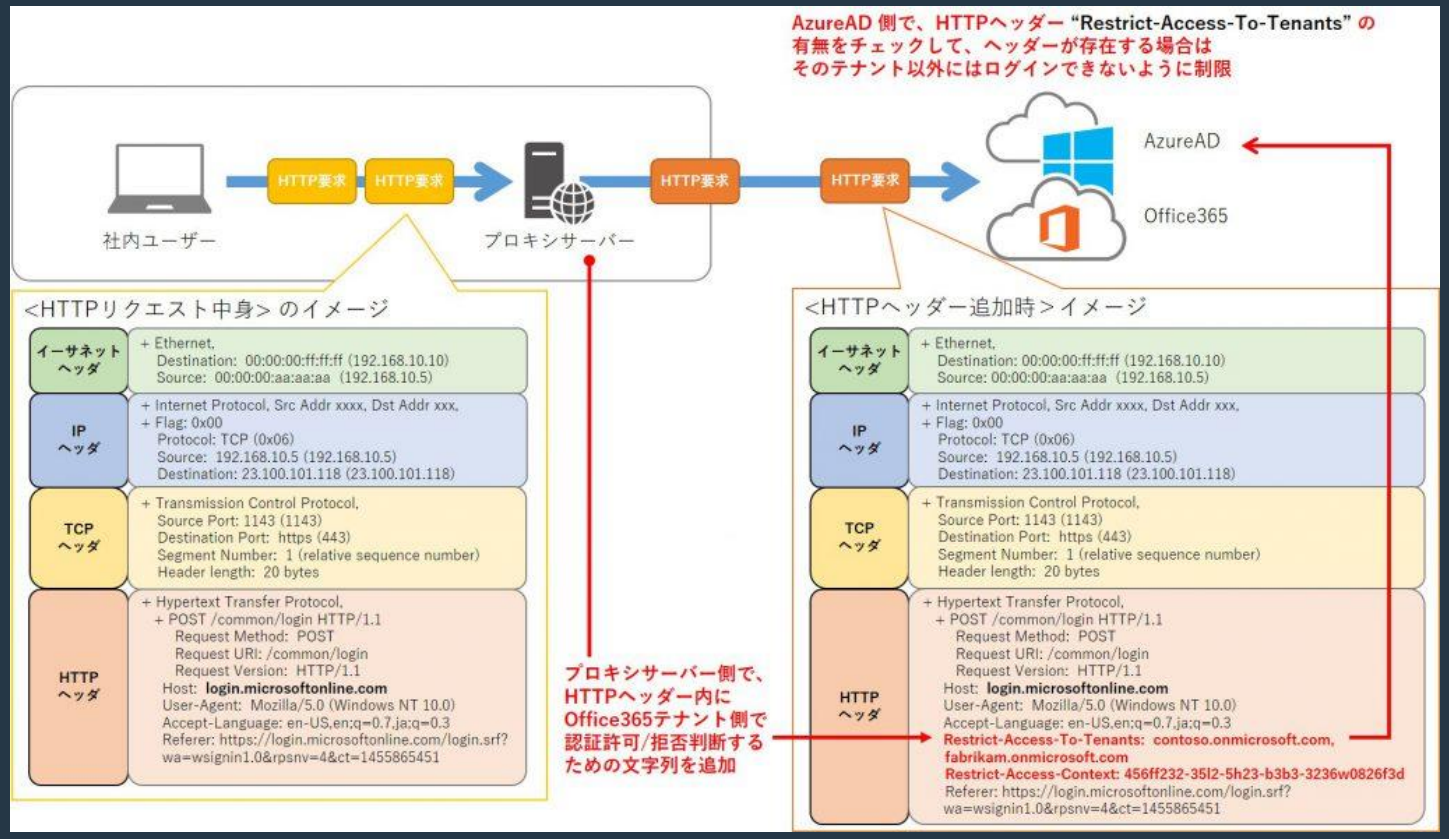
SSLインスペクションが必要なもう一つの理由 ～シャドーITどうしゃどう～

- 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

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)

O365のテナント管理はどうにかやりたい

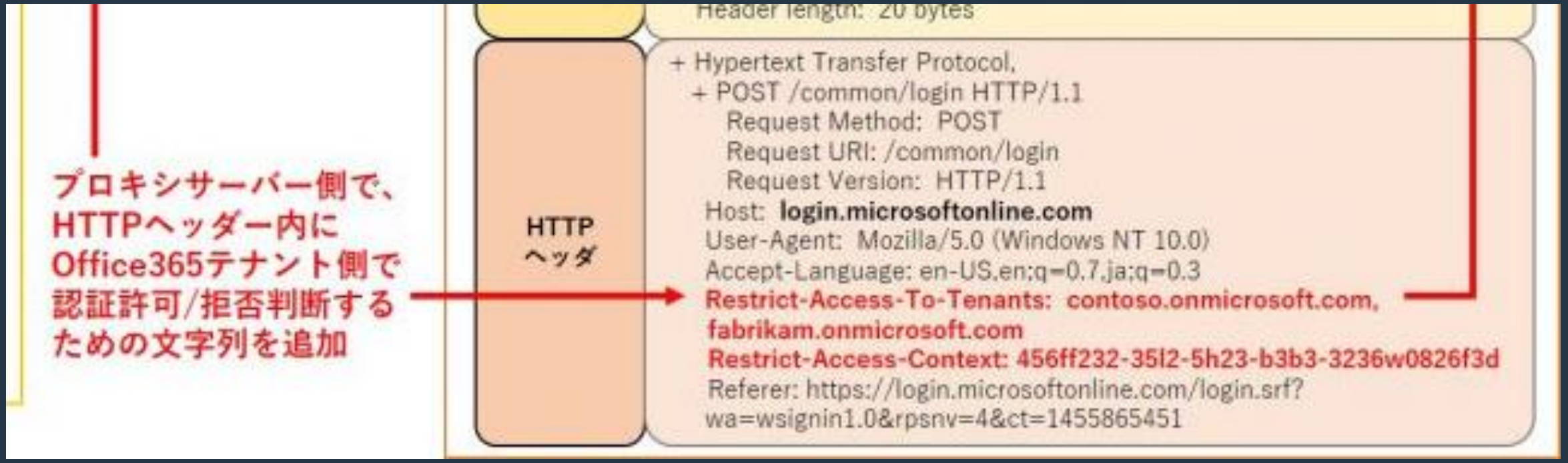
- Proxy + SSLインスペクションの導入が必須



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)

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

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)

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

- 通
- 通
- ノ

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

すこし苦労話を

- 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

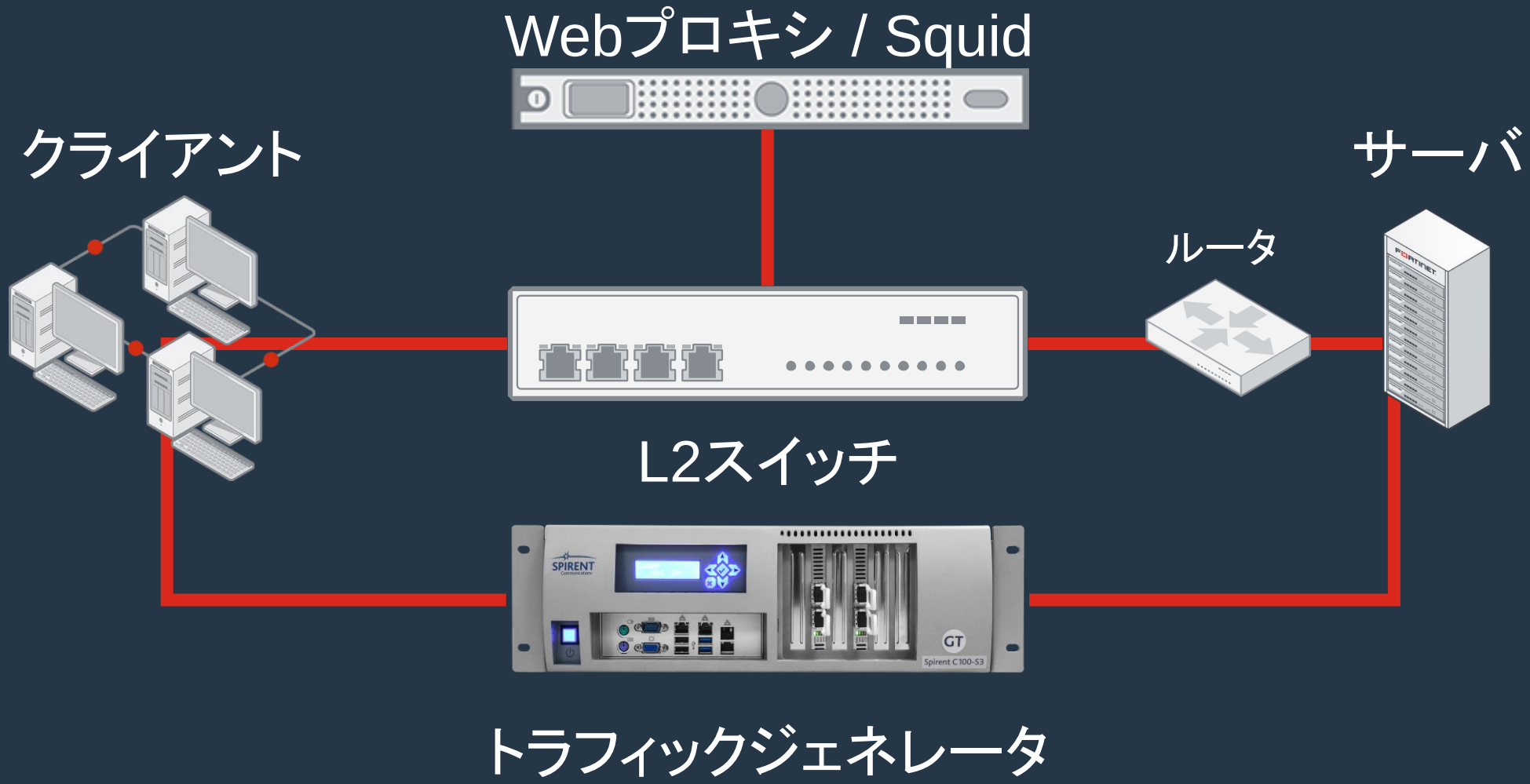
L2スイッチ

Cisco Nexus7706

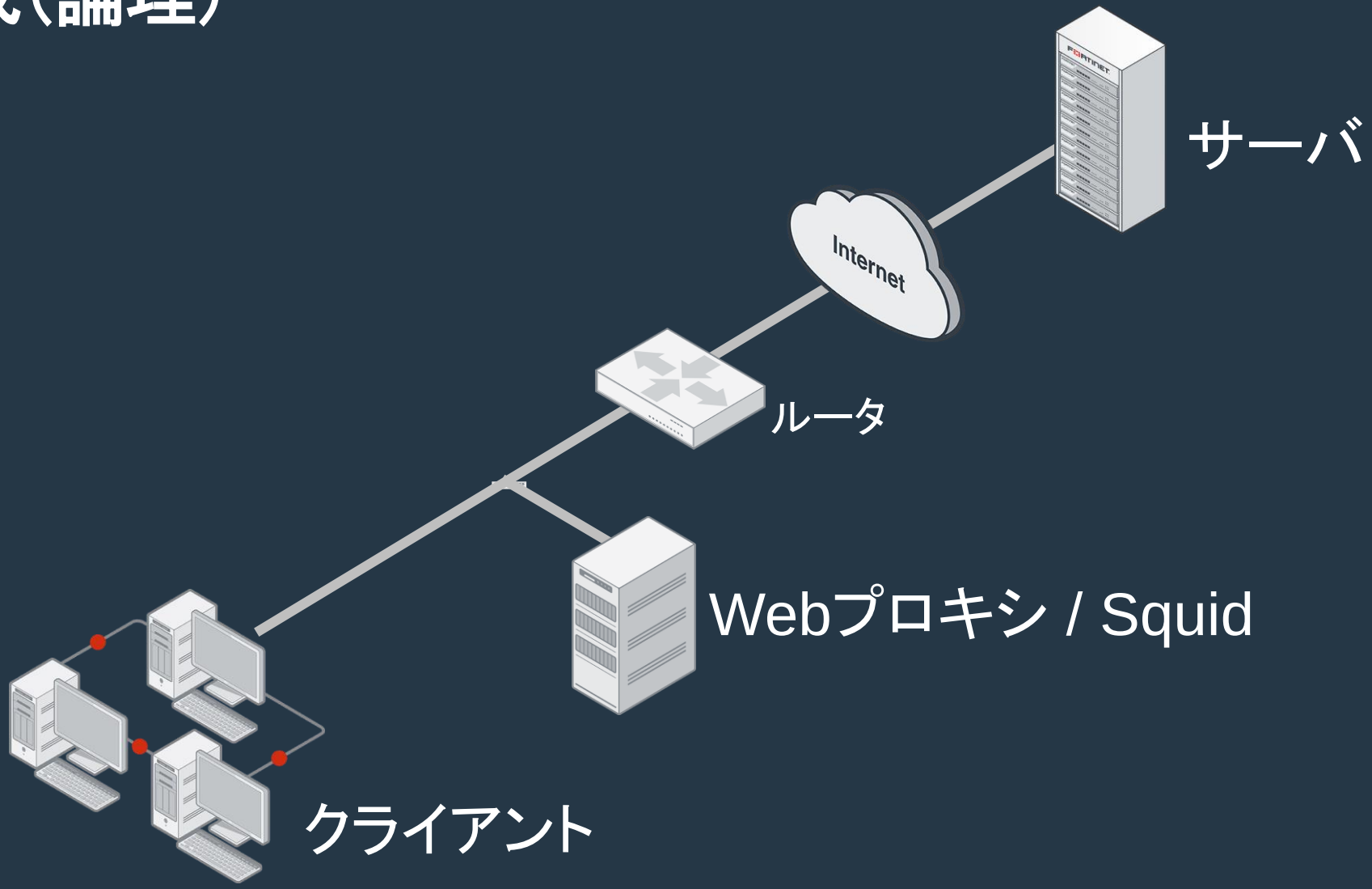
トラフィックジェネレータ

Spirent Avalanche
Model C100-S3-MP

試験構成（物理）



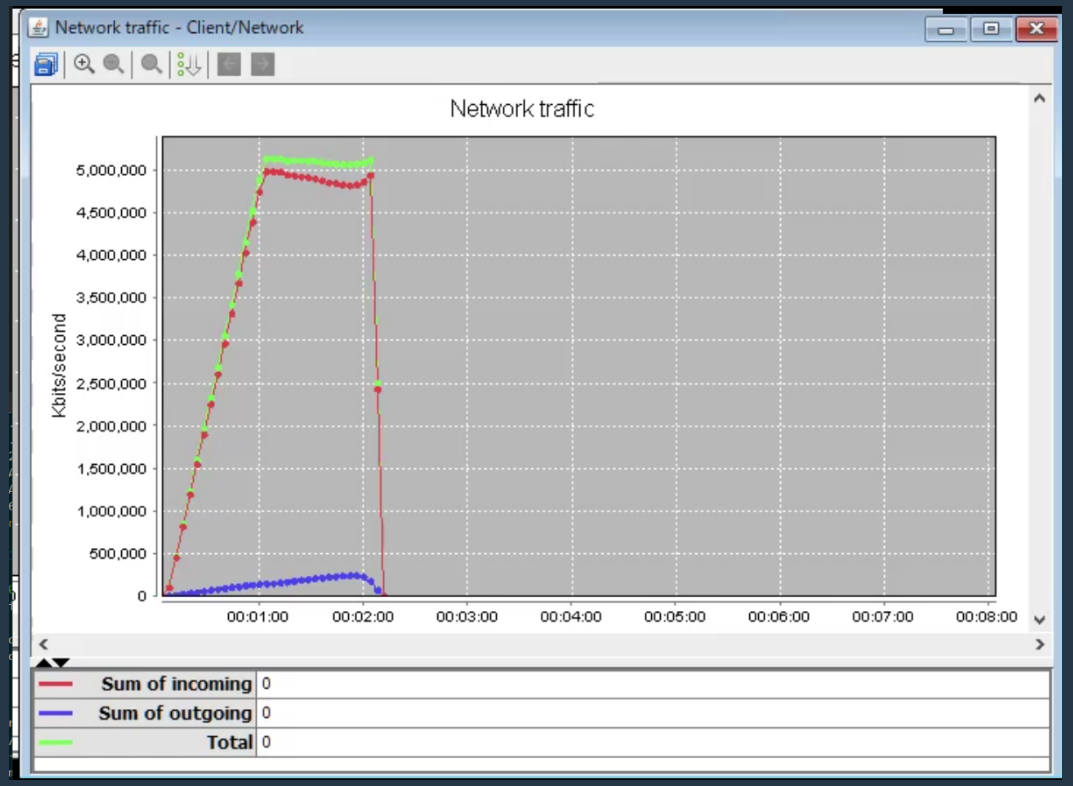
試験構成（論理）



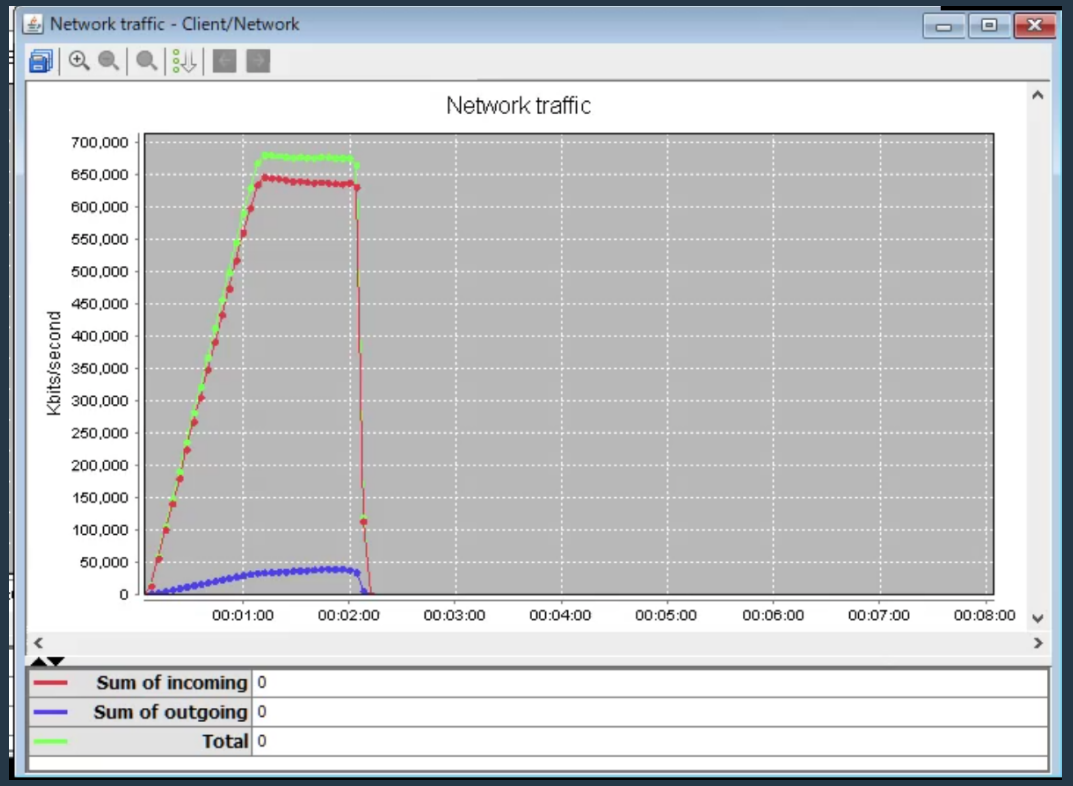
試験結果

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