

# Webサイトの常時TLS化

「ホームページにアクセスしたら、『保護されていない通信』と表示されたのですが、大丈夫でしょうか？」

この課題、解決します。

A10ネットワークス株式会社



Reliable Security Always™

# サマリ

# 課題 Webサイトを常時TLS化しないと・・・

常時TLS化するべき理由

## 1. Google Chrome

- HTTPページ(非SSL/TLS)全てに「保護されていない通信」と警告を表示



## 2. 旧暗号方式(RSA)に深刻な問題

- サーバから“秘密鍵”が流出した場合、秘密鍵ですべての暗号データが復号できてしまう

## 3. SSLの脆弱性

- SSLの各バージョンで脆弱性が判明

## 4. WebサイトのSEO対策

- Googleの検索結果において、**SSL/TLS化したサイトを上位へ表示**されるように評価基準を変更

TLS化しないと・・・

- ユーザの不信感
- 経済的損失
- セキュリティ低下
- 企業ブランディング失墜

対策: TLS 1.2、最新の暗号方式 PFSを利用

# 課題 TLS化、PFS対応における負荷問題

## 1. 運用負荷 増大

サーバでSSL/TLS処理を行なっている場合、すべてのサーバでPFS対応が必要

- 暗号ライブラリのアップデート
- サーバ証明書の更新
- Webサーバ設定変更

設定変更が煩雑  
コストがかかる

### PFS対応例

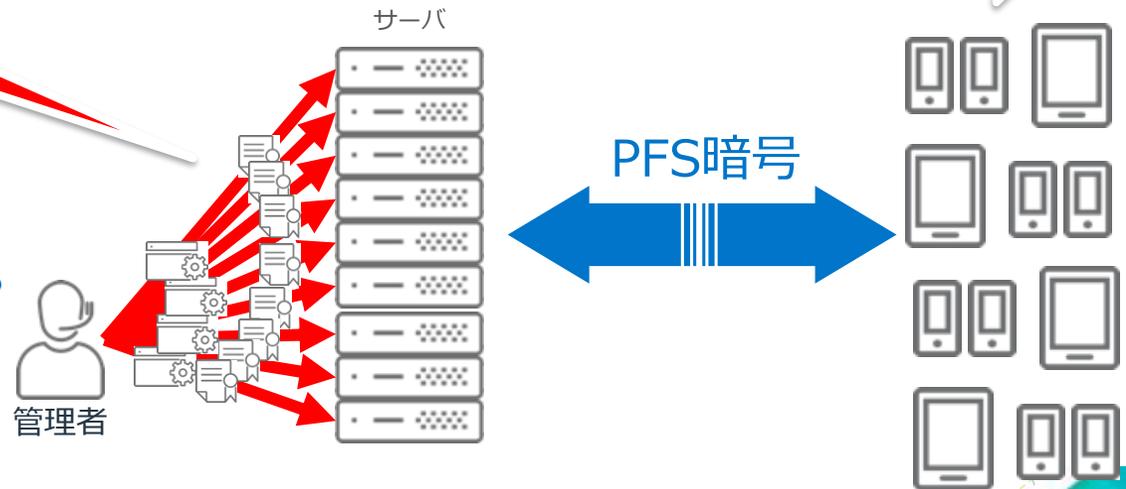
- 暗号ライブラリ(openssl/nss)のアップグレード
- 2048 bit RSA/256bit ECC証明書インストール
- Apache/Nginx/IISのPFS設定追加

## 2. サーバ負荷 増大

PFS対応の暗号スイートは従来より負荷がかかり低速になってしまう

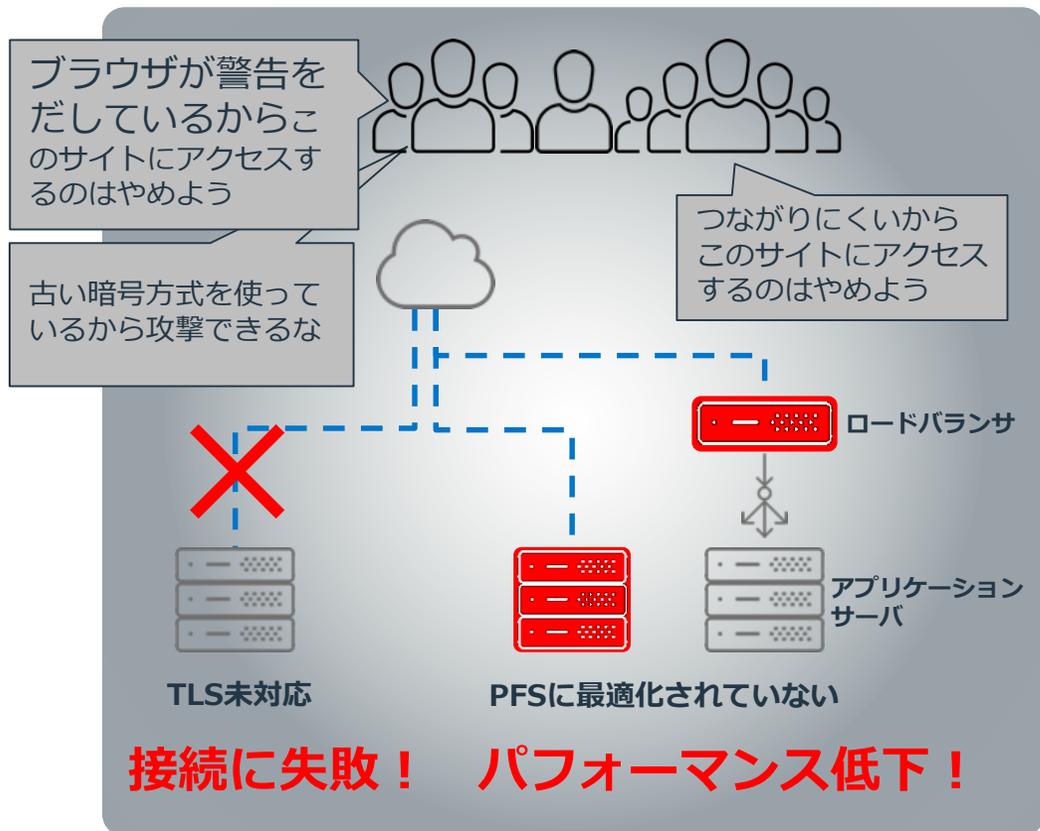
高負荷処理により  
CPU高騰

表示されるのが遅い  
通信が切れる

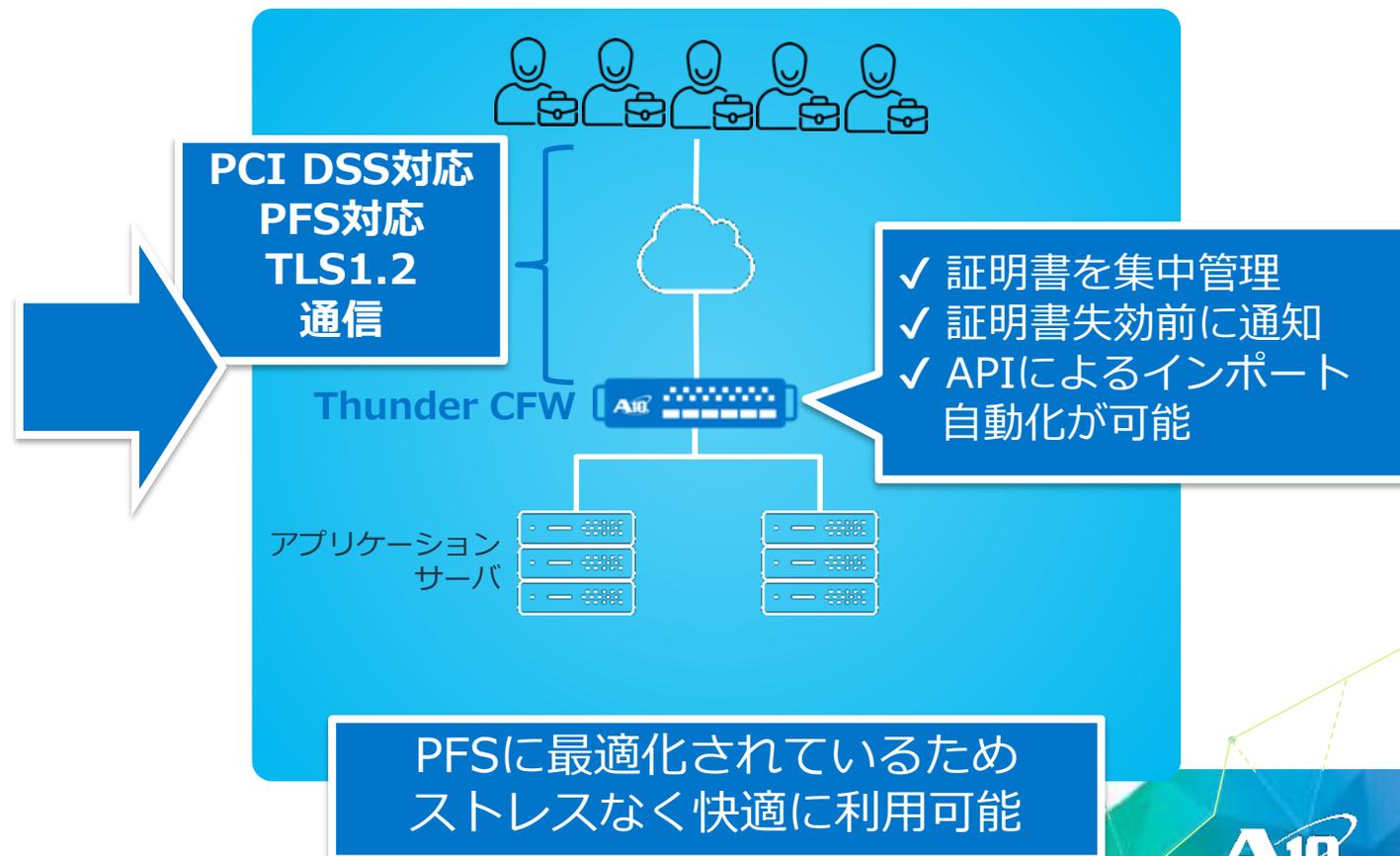


# 解決 常時TLS化 = A10 Thunder ストレスフリーのTLS通信を実現

常時TLS化 未対応  
PFS暗号処理 最適化していない



**A10** Thunderシリーズの場合  
(PFS/ATSに対応)



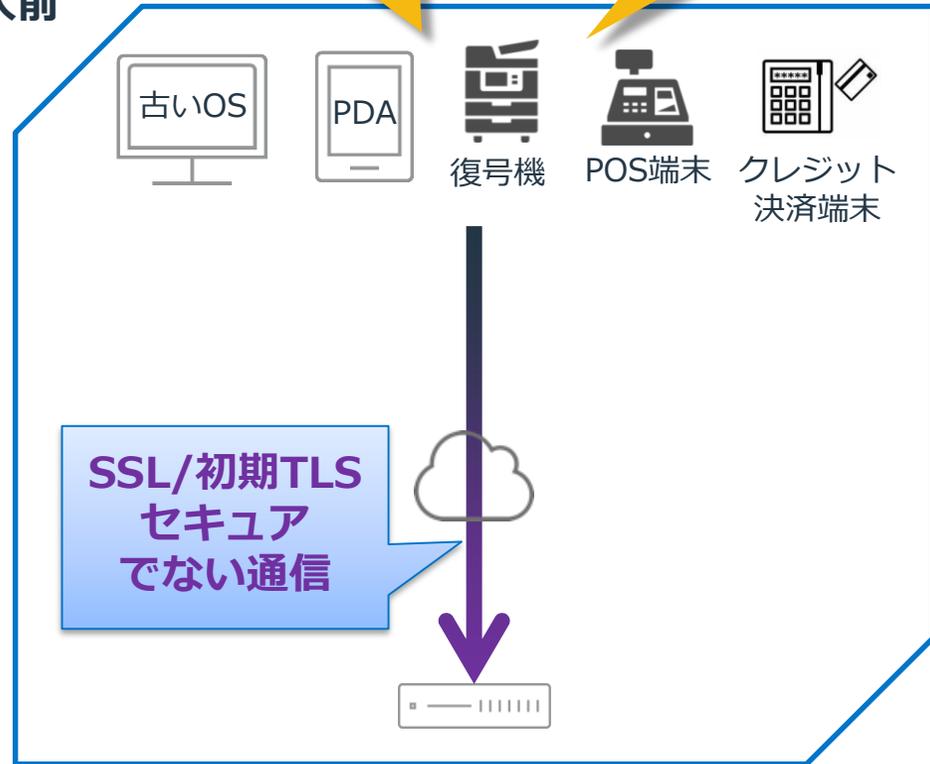
# 端末をまとめてTLS 1.2化

## 課題

端末が全国に点在  
台数が多すぎてUpgradeに  
時間とコストがかかる

端末が古すぎて  
最新の暗号方式に  
対応していない

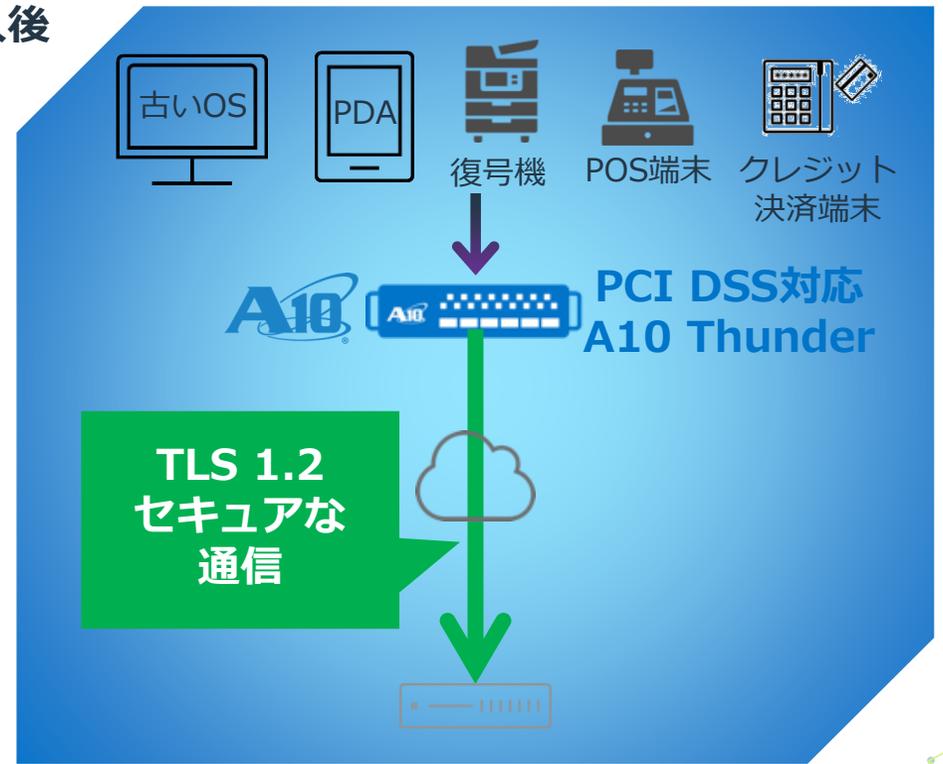
導入前



## 解決 A10 Thunderで

## 端末をTLS1.2化

導入後



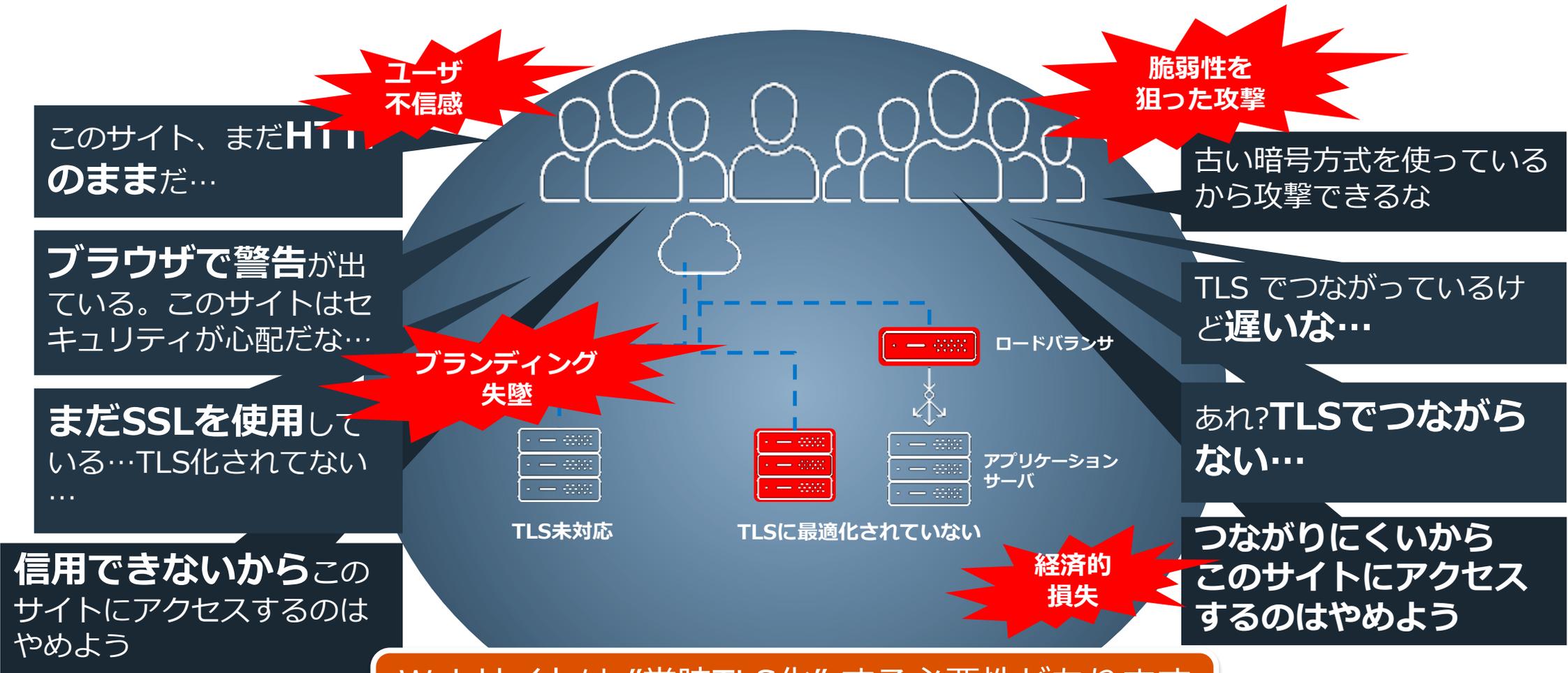
# A10 THUNDERによる WEBサイト常時TLS化詳細

- セキュア ハイパフォーマンス 運用コスト削減

A10ネットワークス株式会社



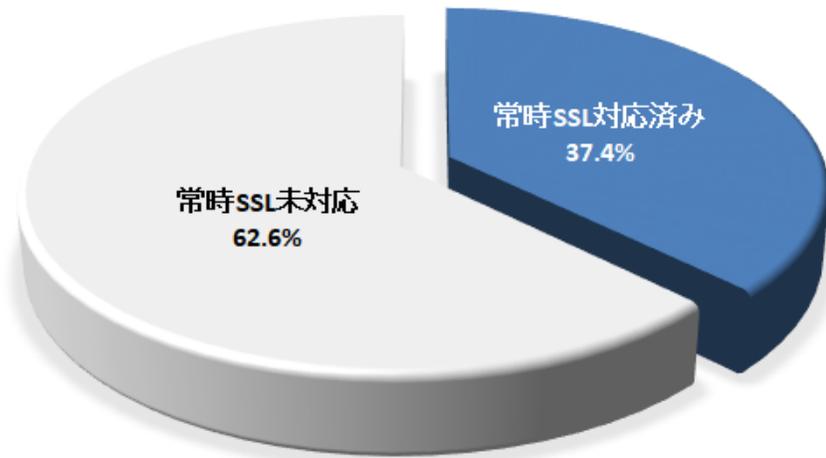
# Webサイトのセキュリティ 適切な暗号化、暗号処理が最適化されていないと…



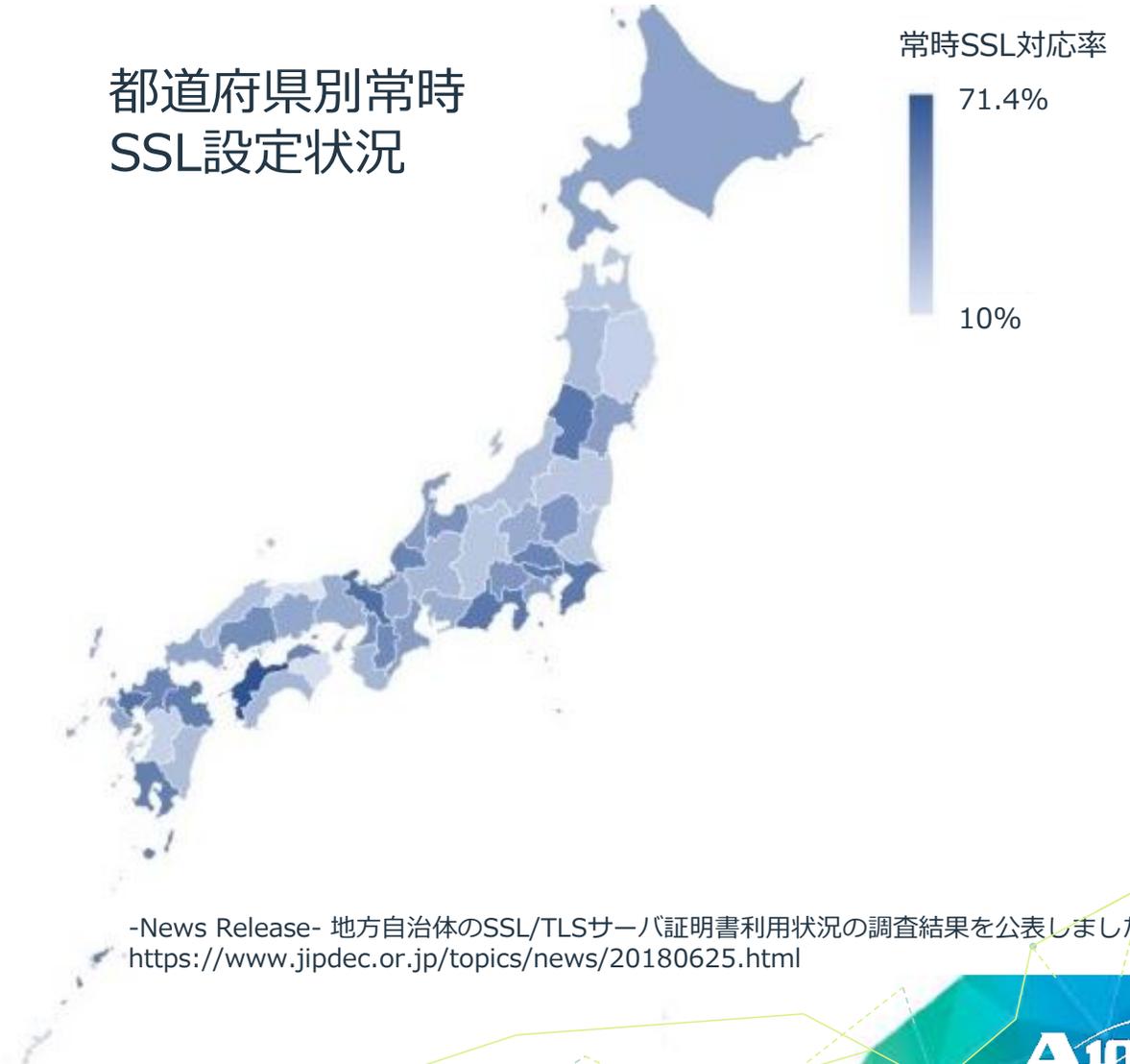
Webサイトは“常時TLS化”する必要があります  
(常時TLS化 = 最新の暗号方式を使用して全webページ暗号化)

# 未対応62.6%：自治体の常時SSL対応比率

自治体全体の常時SSL対応比率



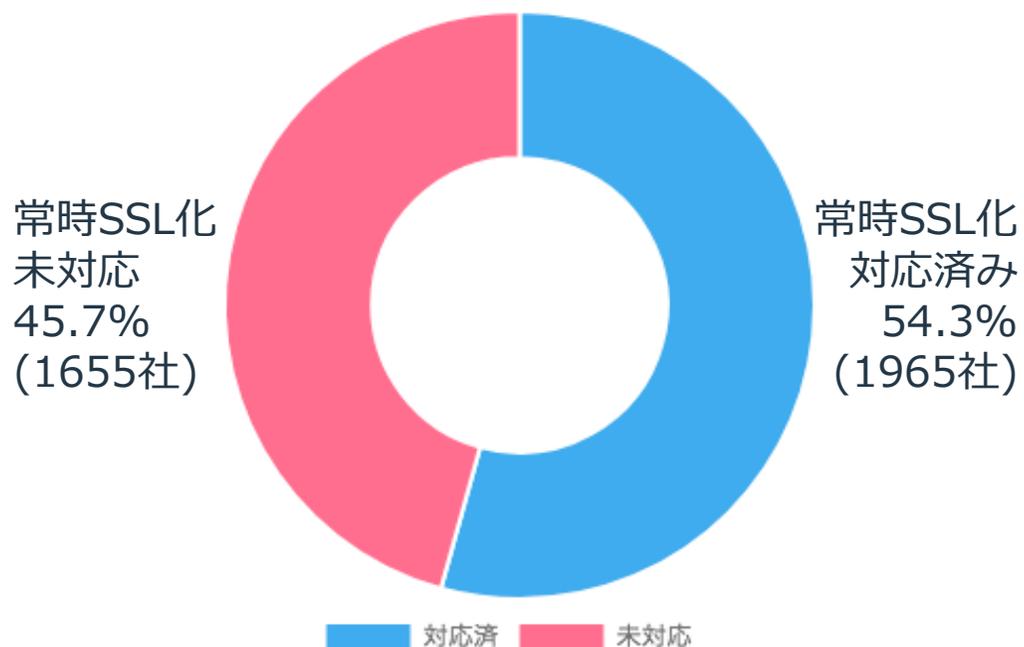
都道府県別常時SSL設定状況



常時SSL/TLS化調査レポート | 自治体サイト対応状況  
[https://itc.jipdec.or.jp/aossil\\_local-government/201806.html](https://itc.jipdec.or.jp/aossil_local-government/201806.html)

# 未対応45.7%：上場企業における常時SSL化対応状況

全上場企業(3620社)における  
常時SSL化対応状況



業種コード別の常時SSL化  
対応状況 (17業種コード)

業種	対応済み	未対応
食品(136社)	58%	42%
エネルギー資源(19社)	41%	59%
建設・資材(314社)	40%	60%
素材・化学(287社)	49%	51%
医薬品(67社)	51%	49%
自動車・輸送機(112社)	42%	58%
鉄鋼・非鉄(80社)	34%	66%
機械(229社)	47%	53%
電機・精密(309社)	55%	45%
情報通信・サービス(949社)	63%	37%
電力・ガス(24社)	49%	51%
運輸・物流(117社)	43%	57%
商社・卸売(320社)	50%	50%
小売(352社)	52%	48%
銀行(84社)	52%	48%
金融(除く銀行)(94社)	53%	47%
不動産(127社)	56%	44%

常時SSL化 調査レポート 上場企業サイト対応状況 (2018年6月版)  
[https://www.feedtailor.jp/report\\_aossl\\_201806/](https://www.feedtailor.jp/report_aossl_201806/)