OPEN SQUARE

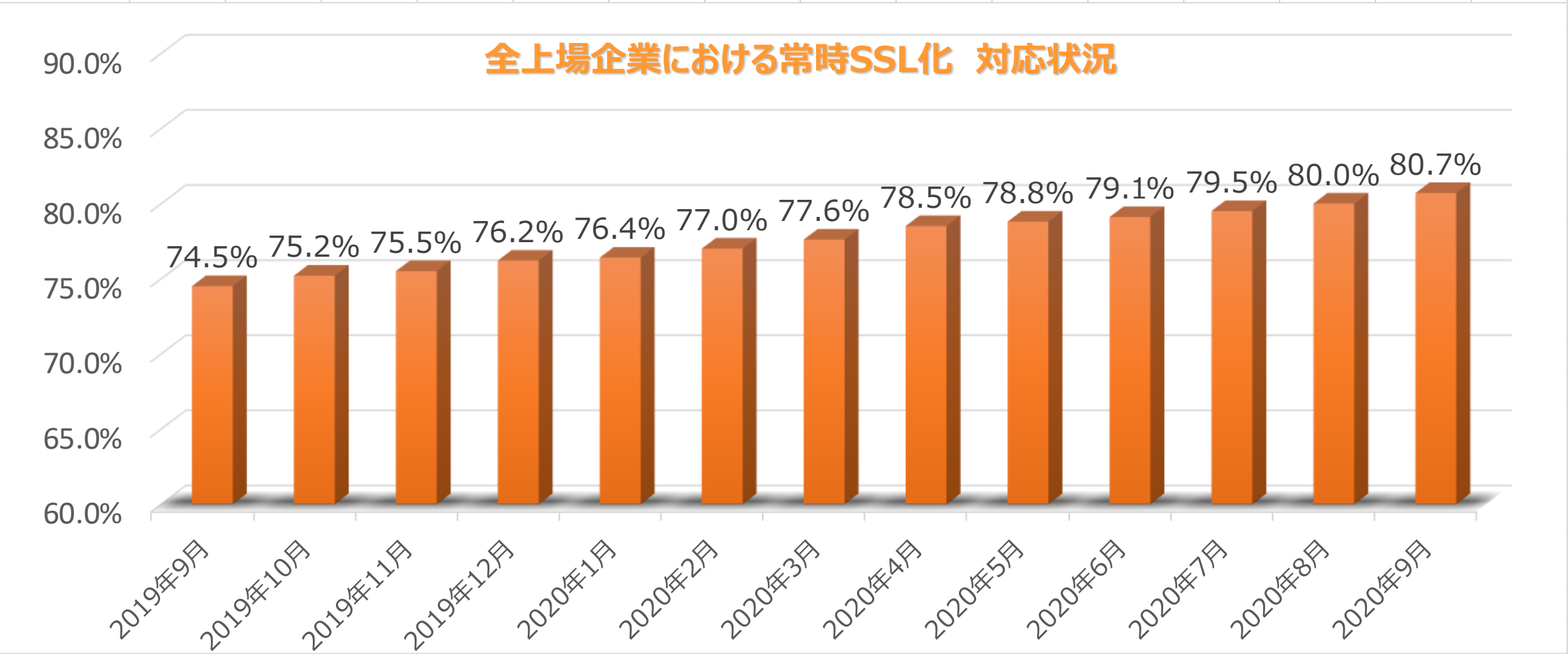
より安全なSSL通信の実現

貴方のサイトでもTSL1.2、TLS1.3を利用しませんか？

株式会社OPENスクエア
田中　昭造

常時SSL化はどれくらい普及しているの？

2014年8月、Googleが”検索結果（SEO）にhttpsサイト（SSL化したサイト）を優遇する”と発表して以来、常時SSL化の対応が進められています。



出展：株式会社フィードテイラー　https://www.feedtailor.jp/report_aossl

今さらながら常時SSL化とは何？

SSLとは「Secure Socket Layer」の略で、インターネットなどのネットワークで送受信されるデータを暗号化する手順（プロトコル）です。

「常時SSL」とは、クレジットカードの番号などの個人情報を入力するフォームだけではなく、全てのコンテンツがSSLによって暗号化されたサイトをさします。

最近はSSLの同意語として“TLS”が使われています。
SSL・TLS区別なくSSLと呼んだり、「SSL/TLS」と並べて表記したりされていますが、本来は異なるものです。

SSLとTLSはどんな関係なの？

TLS(Transport Layer Security)はSSLを元にして策定されたプロトコルです。SSLと云う名称が広く知られていたことから、明確に区別する場合を除いてTLSもSSLと呼ばれることがあります。

SSL 1.0 ➡ **SSL 2.0** ➡ **SSL 3.0**

- **SSL 1.0**
  ネットスケープコミュニケーションズ社がSSLの最初のバージョンとして設計していたが、大きな脆弱性が発見され、リリースされなかった。

- **SSL 2.0　1994年リリース**
  2011年3月に使用禁止

- **SSL 3.0　1995年リリース**
  2014年に脆弱性「POODLE」が発見
  2015年6月に使用禁止

1996年5月
SSLをNetscape社からIETFへ移管するために、
TLSワーキンググループが結成

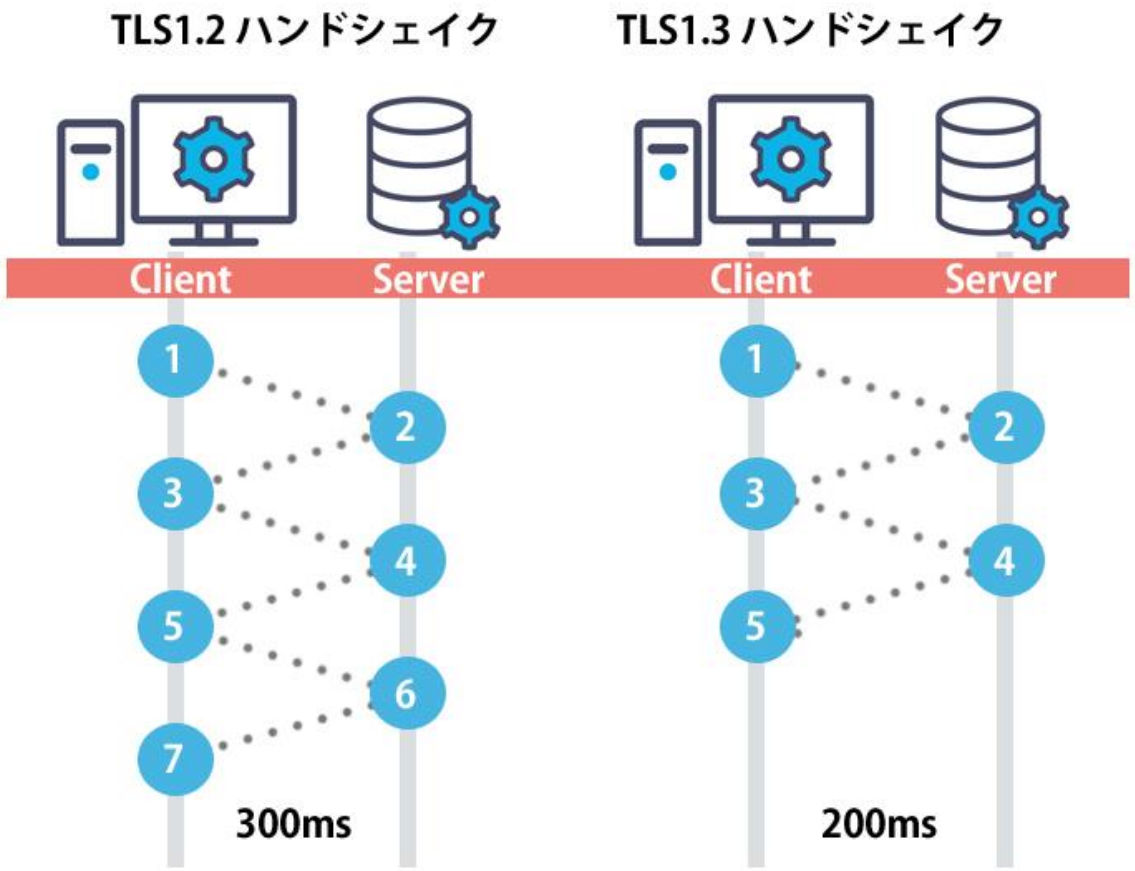
- **TLS 1.0**　1999年リリース
- **TLS 1.1**　2006年リリース
- **TLS 1.2**　2008年リリース
- **TLS 1.3**　2018年リリース

2020年
主要ブラウザで
TLS1.0/1.1
を無効化を実施

TLS1.0/TLS1.1での接続時の警告はご存知ですか？

TLS1.2 / TLS1.3は何が違うの？

TLS 1.3 速度向上



参照：https://lpeg.info/webworks/tls_ssl.html

TLS 1.3 セッキュリティ向上

古くて安全でない暗号化アルゴリズムなど削除

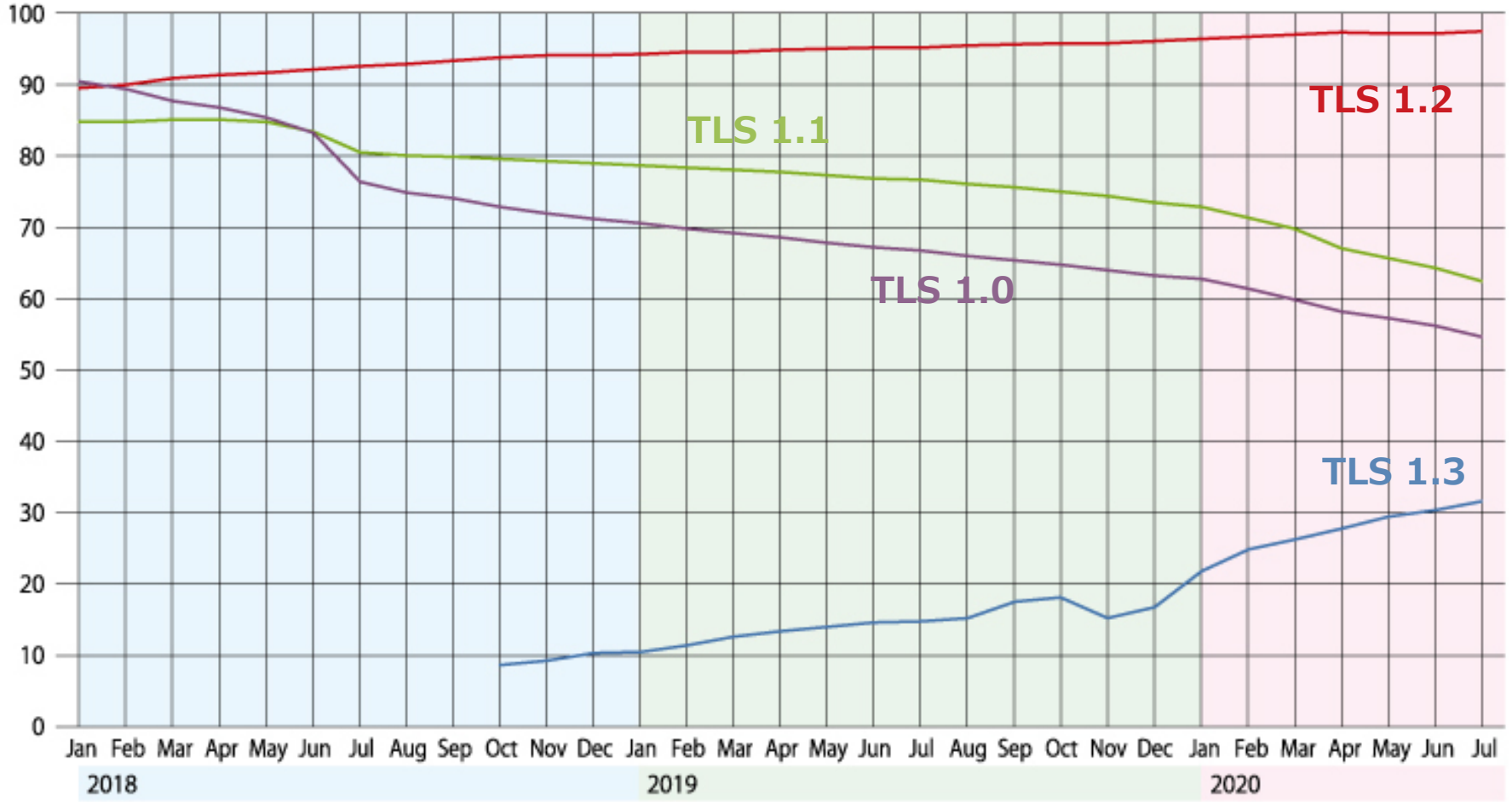
- SHA-1
- RC4
- DES
- 3DES
- AES-CBC
- MD5

などなど、、、、、

TLS1.3の利用がお勧めです。

TLS1.2 / TLS1.3はどれくらい利用されてるの？

SSL Pluseでは毎月約15万の主要サイトを調査して、TLS利用状況などのWebサイトの調査結果を公開しています。（ https://www.ssllabs.com/ssl-pulse/　7月8日時点のデータより）



TLS 1.3が利用できるのサイト
31.7%

TLS 1.2が利用できるのサイト
97.6%

10月4日時点では、TLS1.3が利用できるサイトは**39.8%**に増えています。

参照サイト：https://www.sqat.jp/tag/tls/

TLS1.2 / TLS1.3を利用するには？

TLS 1.2 / 1.3

HTTPS,IMAPS,SMTPS,FTPS・・・

サーバ

主要ブラウザーは
TLS1.2 / 1.3
対応済

各サーバのソフトウェアをTLS1.2 / 1.3対応にバージョンアップと設定、テストが必要です。

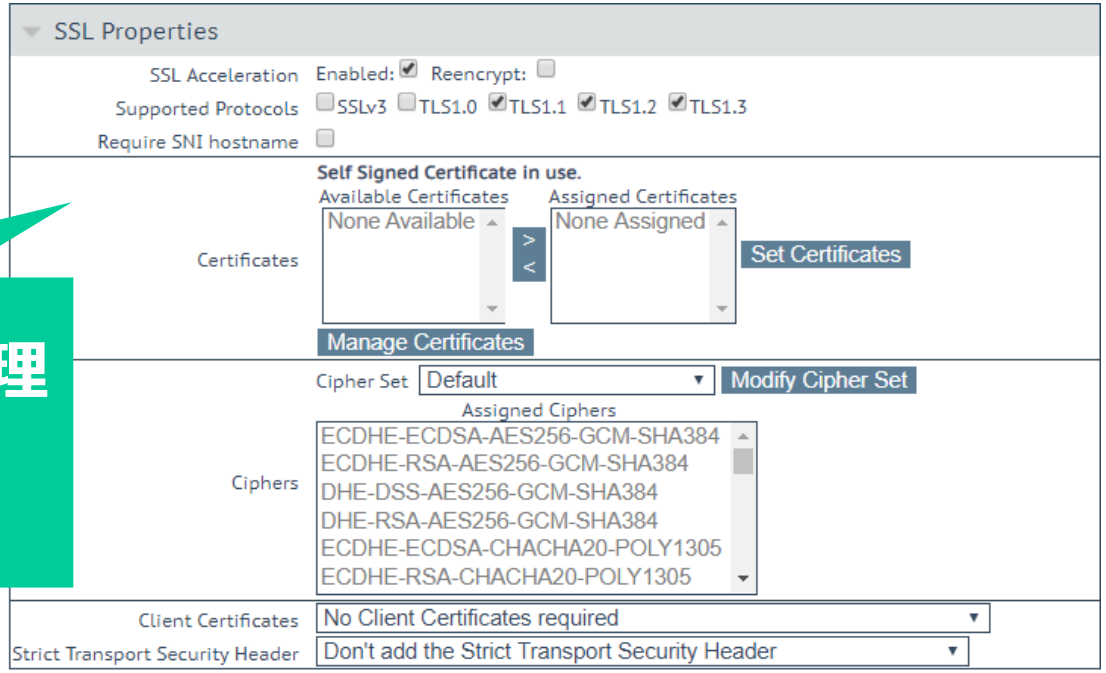
TLS 1.2 / 1.3の利用はLoadMasterで簡単に!!

TLS 1.2 / 1.3

HTTP

サーバ

サーバの設定変更不要



LoadMasterで集中管理
TLS 1.2 / 1.3の選択
SSL証明書も一元管理

無料で使えるLoadMasterもリリースしています。

■Free-VLM　（無償で利用できる仮想版LoadMaster）
- ■スループット　20Mbits（L7）
- ■SSL TPS　50TPS（２K)
- ■HA構成は不可
- ■WAF利用可能(ルール手動設定）

ダウンロードサイト：　https://freeloadbalancer.com/download/

是非、一度お試し下さい。

End