TLS1.3意外と普及してる？

～TLS1, 1.1の終焉に向けて

2023-11-07 JPAAWG 6th GM Open Round Table

JPAAWG / Vade Japan(株)

平野善隆

自己紹介

名前　　平野 善隆

所属　　Vade Japan 株式会社
　　Principal Messaging Engineer

学歴　　奈良先端科学技術大学院大学
情報科学研究科　自然言語処理学

趣味　　長距離の自転車大会(2,000kmとか)
バンド演奏

主な活動 M³AAWG
JPAAWG
Audax Randonneurs Nihonbashi

もくじ

- TLSの歴史
- 調べてみよう
- OpenSSLとの関連性
- まとめ

TLSの歴史

- SSLv3 draft-ietf-tls-ssl-version3-00 (1996年11月)
- TLSv1.0 RFC2246 (1999年1月) (RFC4346により廃止)
- TLSv1.1 RFC4346 (2006年4月) (RFC5246により廃止)
- TLSv1.2 RFC5246 (2008年8月) (RFC8446により廃止)
- TLSv1.3 RFC8446 (2018年8月)

- STARTTLS RFC3207 (2002年2月)

RFC8996の登場

- 2021年3月 RFC8996が登場しました

Deprecating TLS 1.0 and TLS 1.1

TLS 1.0, 1.1の使用禁止

4. Do Not Use TLS 1.0

TLS 1.0 **MUST NOT** be used. Negotiation of TLS 1.0 from any version of TLS **MUST NOT** be permitted.

5. Do Not Use TLS 1.1

TLS 1.1 **MUST NOT** be used. Negotiation of TLS 1.1 from any version of TLS **MUST NOT** be permitted.

調べてみた

調査方法

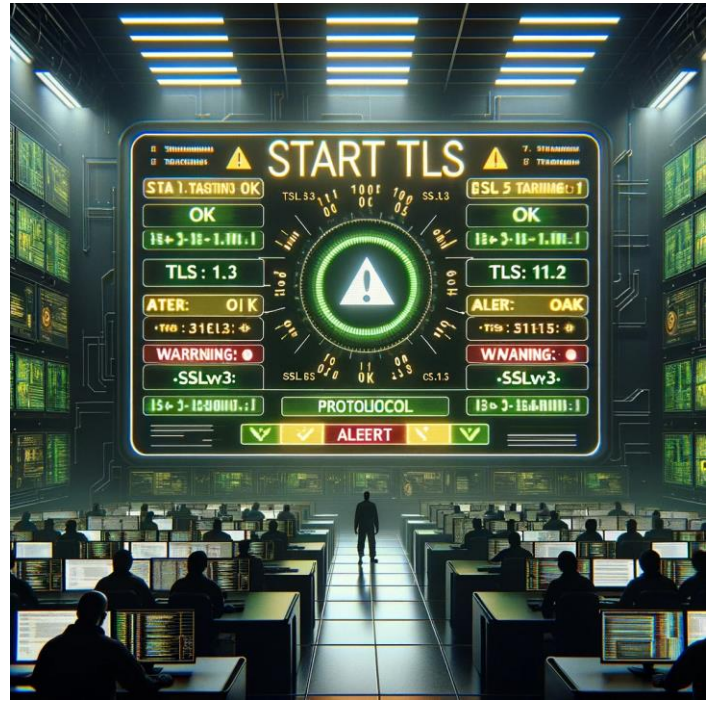
telnet to port 25:
- STARTTLS with TLS1.3
- STARTTLS with TLS1.2
- STARTTLS with TLS1.1
- STARTTLS with TLS1.0
- STARTTLS with SSLv3

example.jp

example.com

example.net

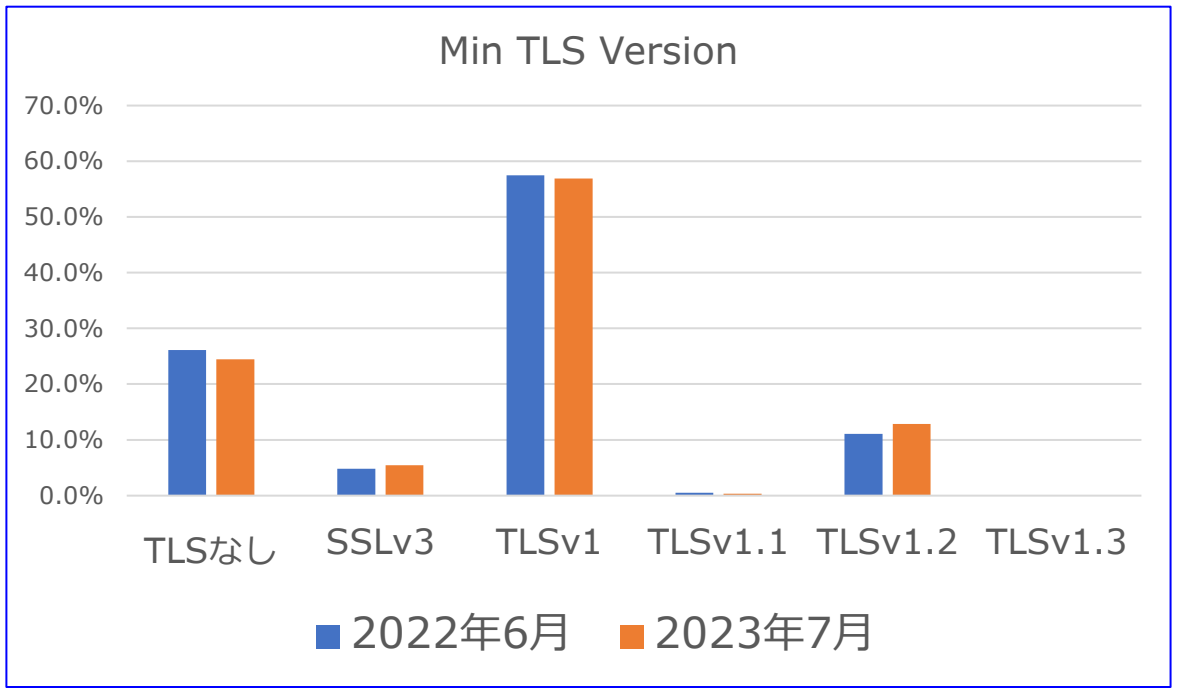
example.org

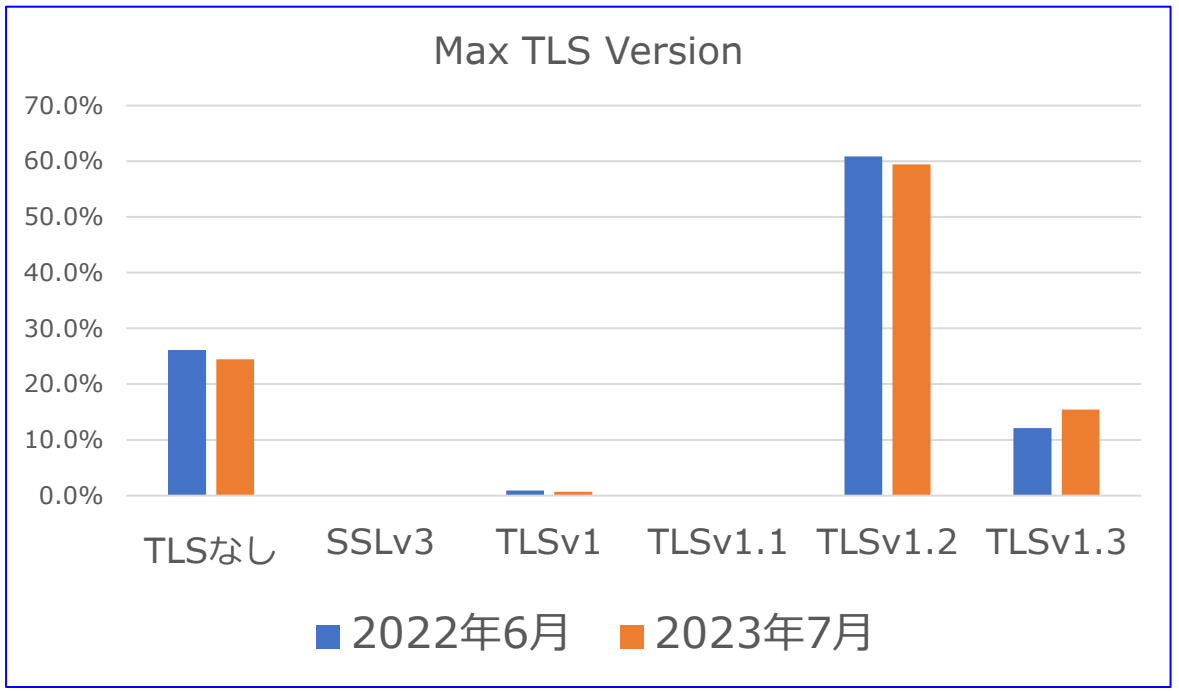


ラボの様子 (イメージ)

MXのある約20万ドメイン

Version別 TLS普及率 1年前との比較



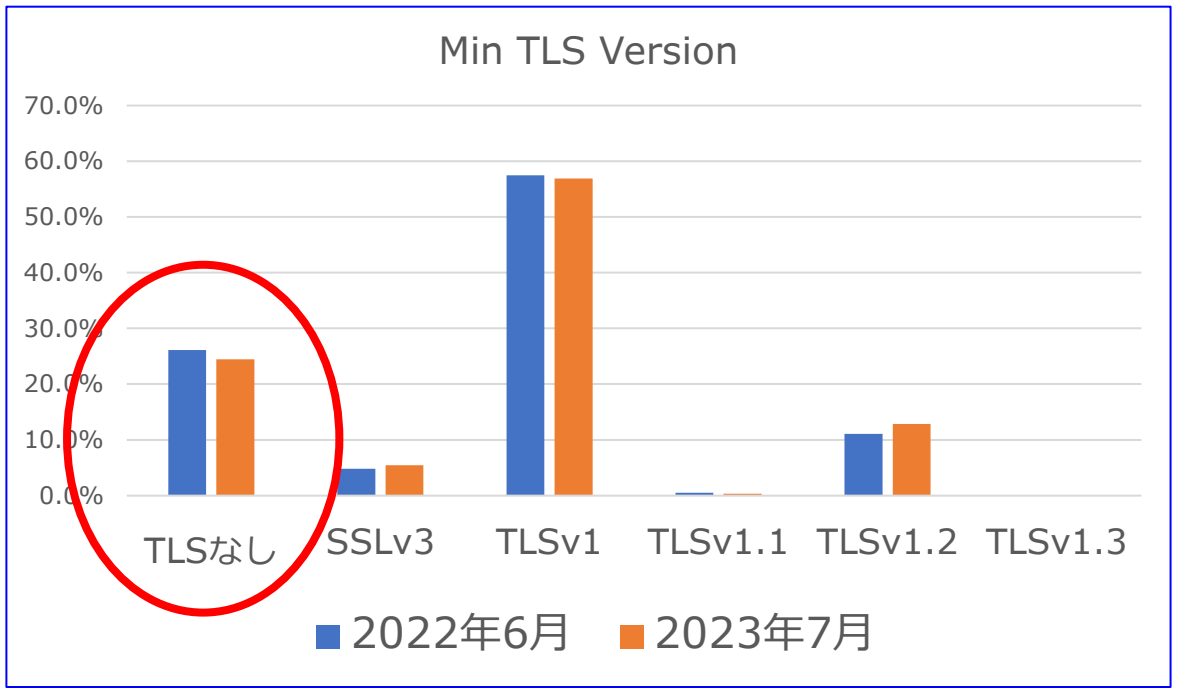


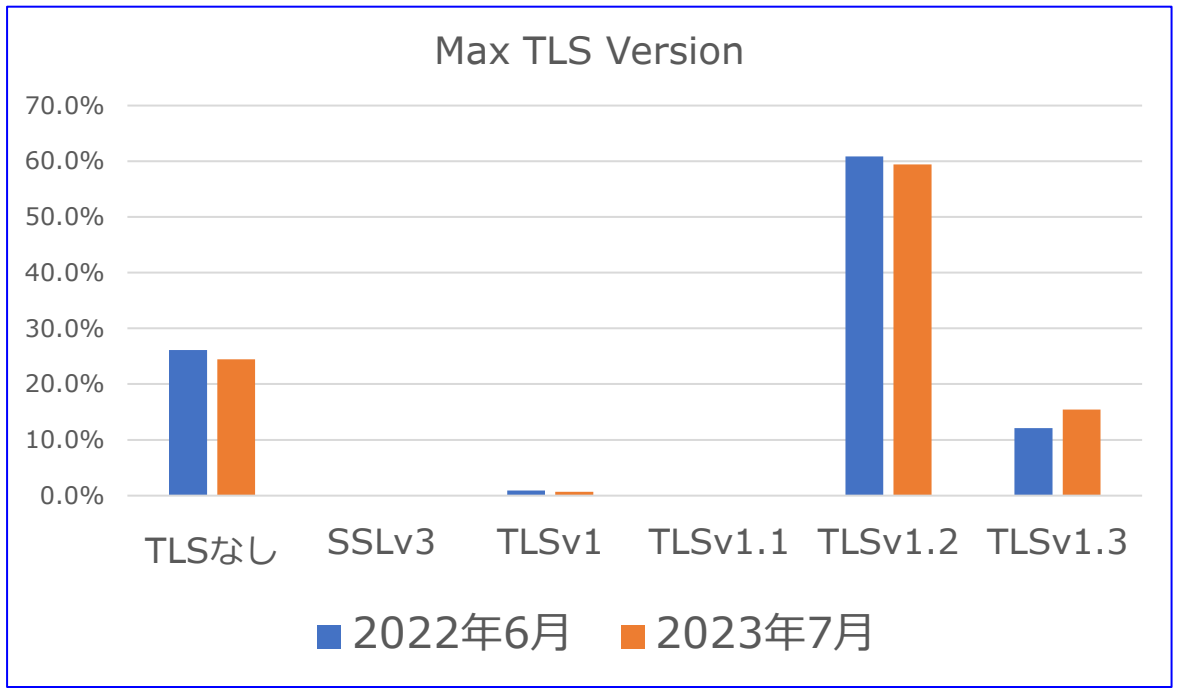
version	2022年6月	2023年7月	2022年6月	2023年7月
TLSなし	56227	52588	26.1%	24.4%
SSLv3	10373	11754	4.8%	5.5%
TLSv1	123642	122389	57.5%	56.9%
TLSv1.1	1080	758	0.5%	0.4%
TLSv1.2	23779	27620	11.1%	12.8%
TLSv1.3	40	12	0.019%	0.006%
合計	215141	215121	100.0%	100.0%

version	2022年6月	2023年7月	2022年6月	2023年7月
TLSなし	56227	52588	26.1%	24.4%
SSLv3	0	3	0.0%	0.0%
TLSv1	1984	1508	0.9%	0.7%
TLSv1.1	13	13	0.0%	0.0%
TLSv1.2	130881	127808	60.8%	59.4%
TLSv1.3	26036	33201	12.1%	15.4%
合計	215141	215121	100.0%	100.0%

N=MXのある約20万ドメイン

TLSの利用率は増えた



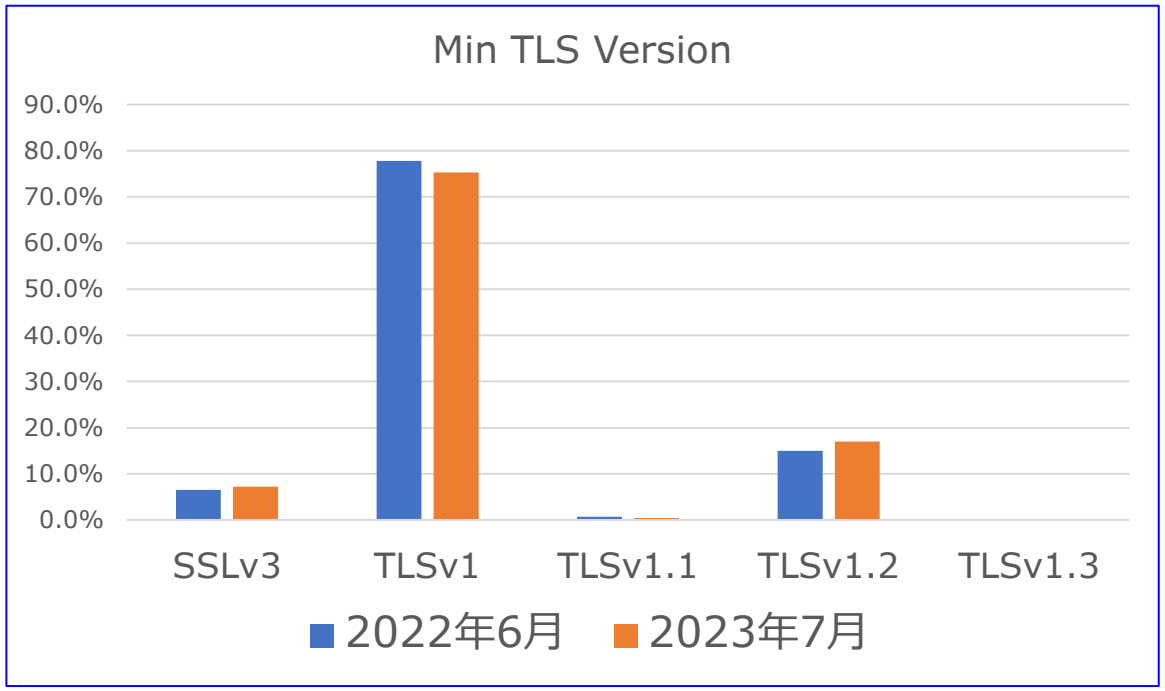


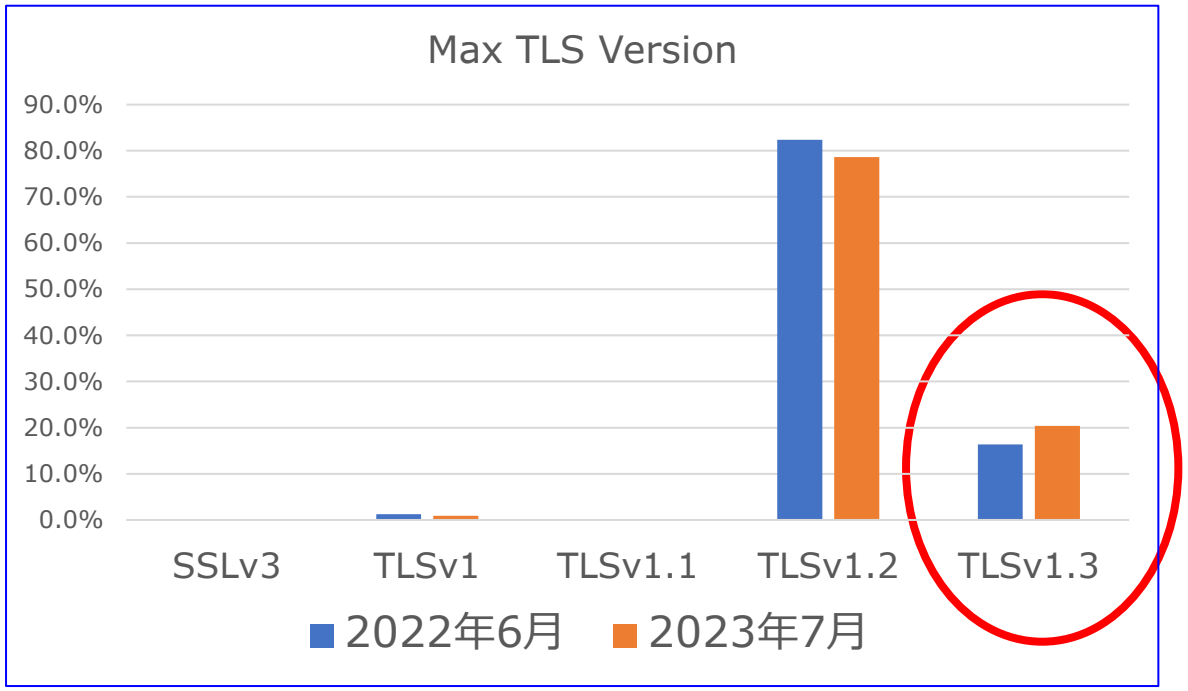
version	2022年6月	2023年7月	2022年6月	2023年7月
TLSなし	56227	52588	26.1%	24.4%
SSLv3	10373	11754	4.8%	5.5%
TLSv1	123642	122389	57.5%	56.9%
TLSv1.1	1080	758	0.5%	0.4%
TLSv1.2	23779	27620	11.1%	12.8%
TLSv1.3	40	12	0.019%	0.006%
合計	215141	215121	100.0%	100.0%

version	2022年6月	2023年7月	2022年6月	2023年7月
TLSなし	56227	52588	26.1%	24.4%
SSLv3	0	3	0.0%	0.0%
TLSv1	1984	1508	0.9%	0.7%
TLSv1.1	13	13	0.0%	0.0%
TLSv1.2	130881	127808	60.8%	59.4%
TLSv1.3	26036	33201	12.1%	15.4%
合計	215141	215121	100.0%	100.0%

N=MXのある約20万ドメイン

TLSv1.3の利用が増加



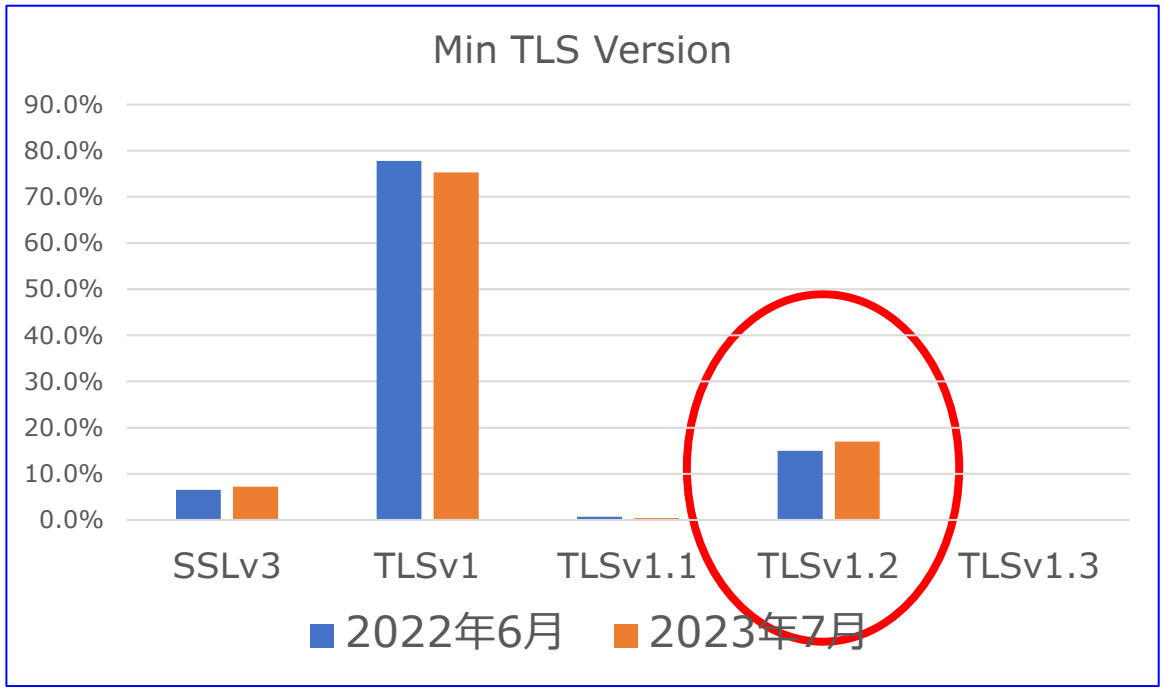


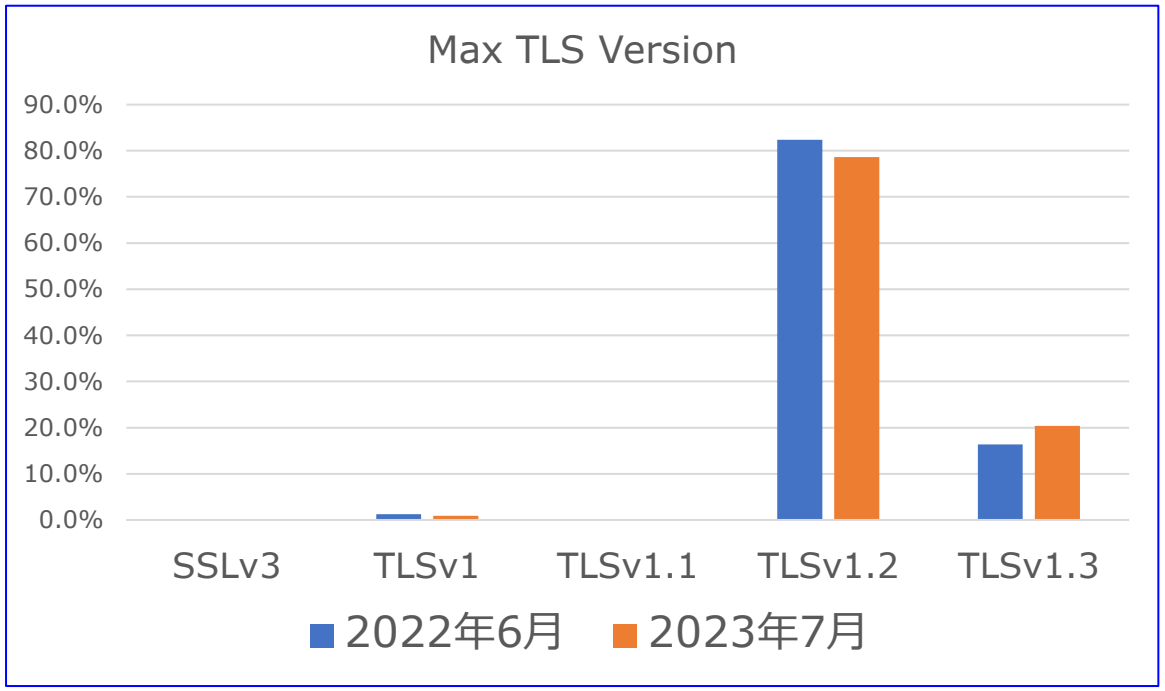
version	2022年6月	2023年7月	2022年6月	2023年7月
SSLv3	10373	11754	6.5%	7.2%
TLSv1	123642	122389	77.8%	75.3%
TLSv1.1	1080	758	0.7%	0.5%
TLSv1.2	23779	27620	15.0%	17.0%
TLSv1.3	40	12	0.025%	0.007%
合計	158914	162533	100.0%	100.0%

version	2022年6月	2023年7月	2022年6月	2023年7月
SSLv3	0	3	0.000%	0.002%
TLSv1	1984	1508	1.2%	0.9%
TLSv1.1	13	13	0.008%	0.008%
TLSv1.2	130881	127808	82.4%	78.6%
TLSv1.3	26036	33201	16.4%	20.4%
合計	158914	162533	100.0%	100.0%

N=MXのある約20万ドメイン

最小VerがTLSv1.2に



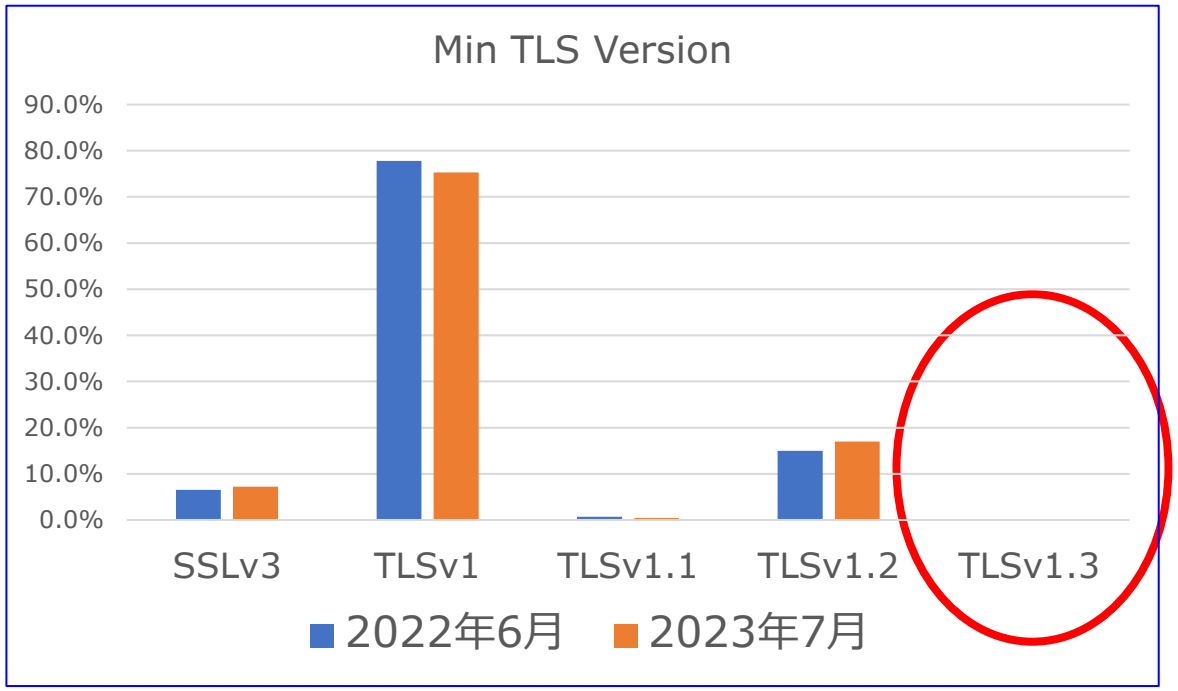


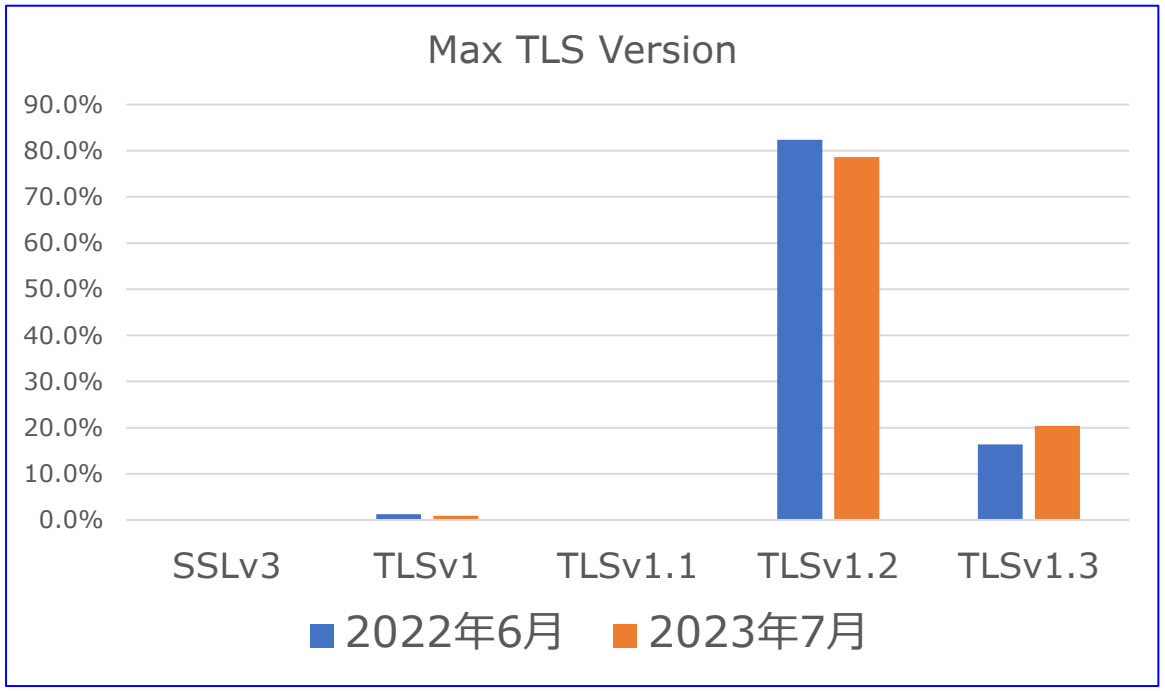
version	2022年6月	2023年7月	2022年6月	2023年7月
SSLv3	10373	11754	6.5%	7.2%
TLSv1	123642	122389	77.8%	75.3%
TLSv1.1	1080	758	0.7%	0.5%
TLSv1.2	23779	27620	15.0%	17.0%
TLSv1.3	40	12	0.025%	0.007%
合計	158914	162533	100.0%	100.0%

version	2022年6月	2023年7月	2022年6月	2023年7月
SSLv3	0	3	0.000%	0.002%
TLSv1	1984	1508	1.2%	0.9%
TLSv1.1	13	13	0.008%	0.008%
TLSv1.2	130881	127808	82.4%	78.6%
TLSv1.3	26036	33201	16.4%	20.4%
合計	158914	162533	100.0%	100.0%

N=MXのある約20万ドメイン

さすがに時期尚早でやめた?



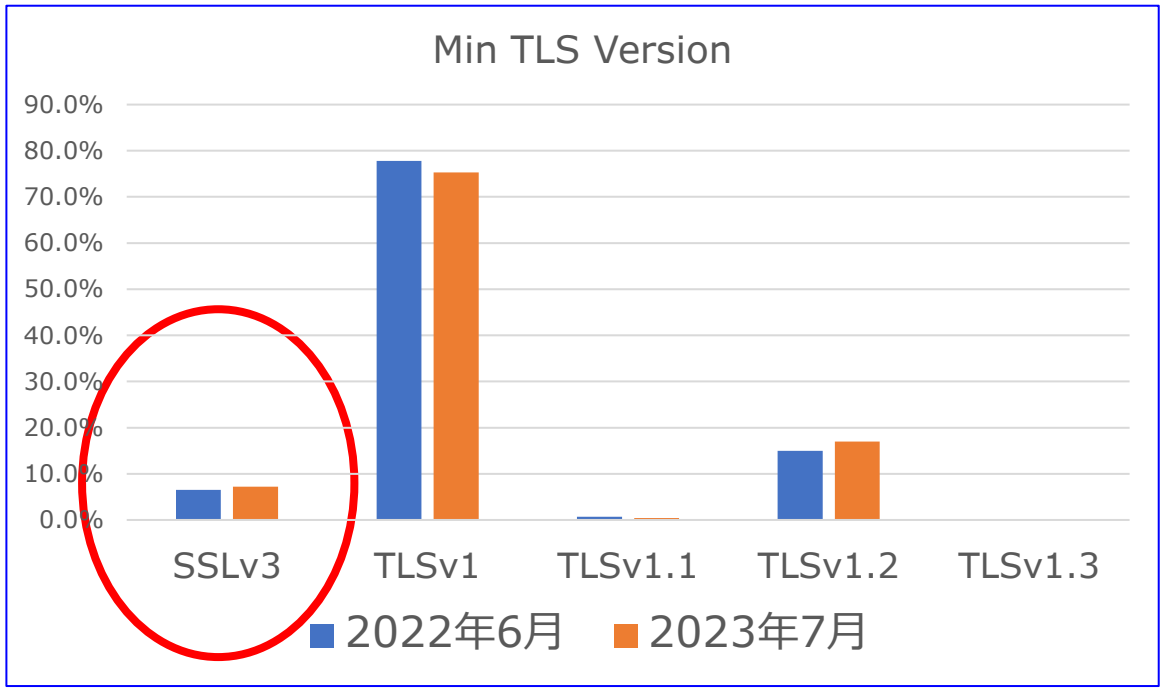


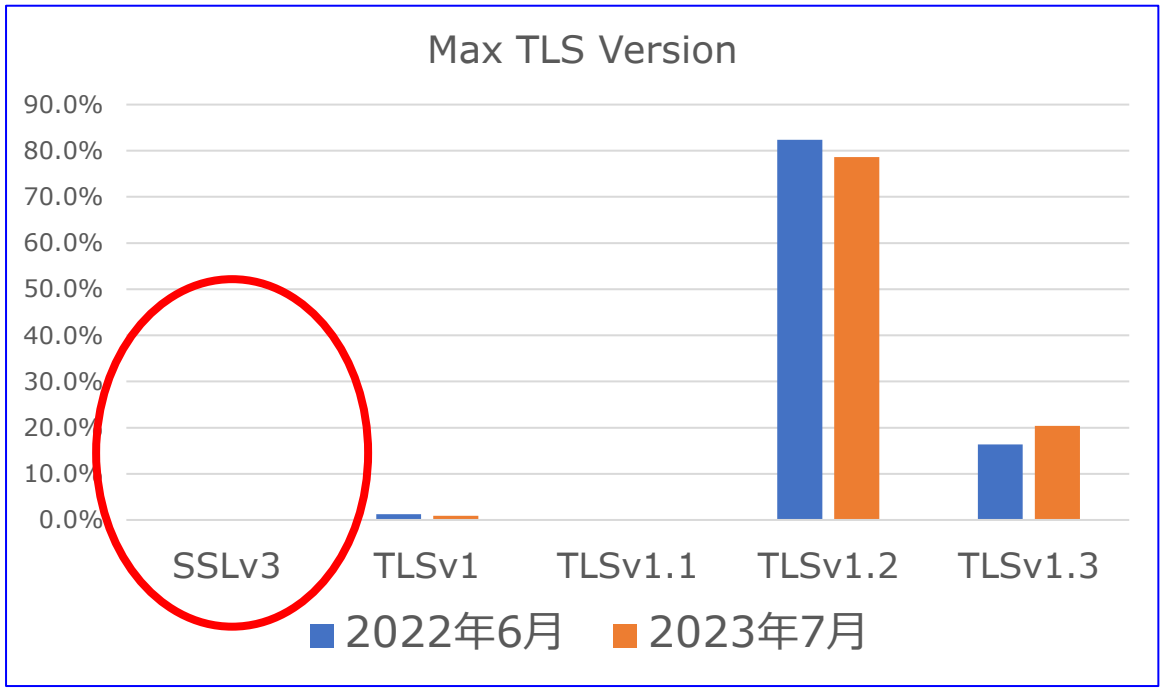
version	2022年6月	2023年7月	2022年6月	2023年7月
SSLv3	10373	11754	6.5%	7.2%
TLSv1	123642	122389	77.8%	75.3%
TLSv1.1	1080	758	0.7%	0.5%
TLSv1.2	23779	27620	15.0%	17.0%
TLSv1.3	40	12	0.025%	0.007%
合計	158914	162533	100.0%	100.0%

version	2022年6月	2023年7月	2022年6月	2023年7月
SSLv3	0	3	0.000%	0.002%
TLSv1	1984	1508	1.2%	0.9%
TLSv1.1	13	13	0.008%	0.008%
TLSv1.2	130881	127808	82.4%	78.6%
TLSv1.3	26036	33201	16.4%	20.4%
合計	158914	162533	100.0%	100.0%

N=MXのある約20万ドメイン

えっ?!





version	2022年6月	2023年7月	2022年6月	2023年7月
SSLv3	10373	11754	6.5%	7.2%
TLSv1	123642	122389	77.8%	75.3%
TLSv1.1	1080	758	0.7%	0.5%
TLSv1.2	23779	27620	15.0%	17.0%
TLSv1.3	40	12	0.025%	0.007%
合計	158914	162533	100.0%	100.0%

version	2022年6月	2023年7月	2022年6月	2023年7月
SSLv3	0	3	0.000%	0.002%
TLSv1	1984	1508	1.2%	0.9%
TLSv1.1	13	13	0.008%	0.008%
TLSv1.2	130881	127808	82.4%	78.6%
TLSv1.3	26036	33201	16.4%	20.4%
合計	158914	162533	100.0%	100.0%

N=MXのある約20万ドメイン

過去一年間のTLS Versionの変化

最小TLS Version

2022 ＼ 2023	なし	SSLv3	TLSv1	TLSv1.1	TLSv1.2	TLSv1.3
なし	42080	3752	4302	151	5928	3
SSLv3	552	7677	1327	26	787	1
TLSv1	4695	259	114063	146	4468	8
TLSv1.1	47	5	57	421	549	0
TLSv1.2	5196	61	2620	14	15886	0
TLSv1.3	18	0	20	0	2	0

最大TLS Version

2022 ＼ 2023	なし	SSLv3	TLSv1	TLSv1.1	TLSv1.2	TLSv1.3
なし	42080	2	62	0	11433	2639
SSLv3	0	0	0	0	0	0
TLSv1	248	1	1444	0	224	67
TLSv1.1	0	0	0	12	1	0
TLSv1.2	9447	0	0	1	115533	5893
TLSv1.3	813	0	2	0	617	24602

OpenSSLとTLSのバージョン

OpenSSLで使用できるTLSのバージョン

OpenSSL version	最小 TLS version	最大 TLS version	リリース日	EOL
0.9.8	???	1.0	2005/7/5	2015/12/31
1.0.1	???	1.2	2012/3/14	2016/12/31
1.0.2(LTS)	SSLv2?	1.2	2015/1/22	2019/12/31
1.1.0	1.0	1.2	2016/8/25	2019/9/11
1.1.1(LTS)	1.0	1.3	2018/9/11	2023/9/11
3.0(LTS)	1.2	1.3	2021/9/7	2026/9/7
3.1	1.2	1.3	2023/3/14	2025/3/14

OpenSSLとOSとTLSのバージョン

OpenSSL version	最小 TLS version	最大 TLS version	EOL	OS	Full support ends	Maintenance support1 ends	Maintenance support2 ends	Extended life cycle support (ELS) add-on ends
0.9.8	???	1.0	2015/12/31	RHEL5	2013/1/8	2014/1/31	2017/3/31	2020/11/30
1.0.1	???	1.2	2016/12/31	RHEL6	2016/5/10	2017/5/10	2020/11/30	2024/6/30
1.0.2(LTS)	SSLv2?	1.2	2019/12/31	RHEL7	2019/8/6	2020/8/6	2024/6/30	2028/6/30
1.1.0	1.0	1.2	2019/9/11					
1.1.1(LTS)	1.0	1.3	2023/9/11	RHEL8	2024/5/31		2029/5/31	2032/5/31
3.0(LTS)	1.2	1.3	2026/9/7	RHEL9	2027/5/31		2032/5/31	2035/5/31
3.1	1.2	1.3	2025/3/14					

https://access.redhat.com/support/policy/updates/errata

議論のお時間

大切なお約束

- 意見と人格は切り離してください
- 意見を批判するのは大歓迎ですが
  意見を言った人を批判しないでください
- あなたの言った意見が批判されるかも知れません
  しかし、それはあなたが批判されたわけではありません

まとめ

TLS 1.3の採用状況

- 大手を中心にTLS 1.3が採用され、ORT参加者の中ではTLS 1.0/1.1は3,4社で廃止されていた

TLS 1.0/1.1廃止の課題と対策

- サーバやアプリケーションの制約で進まない
- 廃止を成功させたところは、平文にフォールバックしても通信は可能なのでよいと判断
- セキュリティ診断で高得点を得るために廃止できた

平文通信と古いTLSの比較

- 平文にはセキュリティリスクが存在し、TLS 1.0/1.1はダウングレード攻撃のリスクがある
- TLS通信が極端に遅い送信先があり(100通/分)、TLSに対応させられない
- セキュリティ上の問題として、ダウングレードされるTLS 1.0/1.1を公開するより平文の方がまし

まとめ (Cont'd)

TLSのバージョンとアップデートの問題点

- TLS 1.1が少ない理由は、OpenSSLのTLSのmaxが1.1であるバージョンが存在しないから

WebのTLSバージョンは新しいのになぜメールは古いのか

- ブラウザのアップデートは容易
- ブラウザに警告が出るのでサーバーはバージョンアップせざるを得ない

見える化による意識改革

- Webブラウザはセキュリティ警告でユーザーにリスクを通知できるが、メールは送受信後でないと安全性が確認できない
- Gmailの鍵マークなどの見える化により、TLSバージョンアップのモチベーションが高まる可能性がある

今後の展望とアクションプラン

- OSやアプリケーションのバージョンアップを通じてTLSバージョンアップを促進
- セキュリティ基準(PCIDSS)や新しいメールセキュリティ技術(DANE/MTASTS)がTLS 1.2以上を要求しているため、アップデートが不可欠
- 見える化を促進し、バージョンアップしないといけない機運を高める

詳細な議事録

詳しくはWebで！

https://qiita.com/hirachan/items/a7c87ae44453f30f2f37