Vol.2021-IOT-52 No.34
2021/3/2

TLSバージョン移行とEV証明書利用に関する局所的調査（FY2020 4Q）

須賀 祐治[1,a)]

概要：ある特定の分野における TLS サーバ設定に関する定点観測に関する調査報告を行う．主に 2020 年主要ブラウザが TLS1.0/1.1 サポートを中止した影響について報告する．あわせて TLS バージョン対応と利用アルゴリズムについての局所的調査の結果も報告する．

キーワード：SSL/TLS, 移行工学, EVSSL 証明書，ROBOT 攻撃, RC4

A local survey on transitioning of TLS versions and EV Certificates Usage (FY2020 4Q)

Yuji Suga[1,a)]

Abstract: This paper reports on a survey of fixed-point observations of TLS server configurations in a particular field. We mainly report on the impact of the discontinuation of TLS1.0/1.1 support by major browsers in 2020. We also report the results of topical surveys of TLS version support and usage algorithms.

Keywords: SSL/TLS, Transition Engineering, EV SSL Certificates, ROBOT Attacks, RC4

1. はじめに

2012 年より Alexa Top Sites から .jp ドメインを抽出した URL リストを利用して SSL/TLS サーバのクローリングを行う定点観測を行っており，SSL/TLS バージョンや Export-grade 暗号アルゴリズムの利用率改善に関する調査を行ってきた [1], [2], [3]．特に証明書に着目すると，ブラウザのセキュリティインディケータの表記方針が大きく変更になったことから，本来 URL 表記部分に緑のバーが表示される EVSSL 証明書を利用しているにも関わらず安全ではないと判断されるサイトも散見された．これは，本来安全であるにも関わらずコンテンツ不備により安全ではないと表記されてしまう問題であり，コンテンツ管理を適切に行えば改修できる．

一方で 2017 年 3 月にブラウザのバグとして取り上げられた問題においてはサーバ証明書の構造に応じて正しい表記になっていない状況が約 1 ヶ月続いていた [4], [5]．証明書ベンダーからサーバ証明書の再発行が可能であることがアナウンスされていたが EVSSL 証明書の差し替えを行っていない，もしくはこの問題に気がついていなかったサイトが多く見られた．

この状況について，ある業界の決済システム等の企画・運営を行っている協会に属する正会員の Web サイトを調査対象として 2017 年に報告が行われている [6]．この報告によると，広報用に広く公開された FQDN（これを Top FQDN と呼ぶ）で SSL-enable なサイトは 115 であり，このうち脆弱であると認識されてい SSL2.0 が未だに有効となっているサイトは 4.3%，SSL3.0 が有効なサイトは 34.8%も存在した．

[1] 株式会社インターネットイニシアティブ
Internet Initiative Japan Inc., Iidabashi Grand Bloom, 2-10-2 Fujimi, Chiyoda-ku, Tokyo 102-0071, Japan
[a)] suga@iij.ad.jp

一方で顧客向けにのみ提供されるログインを必要とするサイトにおける調査では Top FQDN と比較して芳しい結果が得られており組織側の自助努力が垣間見られた．具体的には SSL2.0 有効サイトは無く SSL3.0 有効サイトは 3 サイトのみであった．このとき Top FQDN としては 115 サイトが存在したが，アウトソーシングサービスを利用しているため同じ FQDN に複数の組織のログインサービスが提供されているため，トータルで 58 の FQDN が調査対象となっており 58 全てのサーバにおいて EVSSL 証明書が配備されていた．そのうち 53 の証明書は同一商用認証機関から発行されており，このまま使い続けると近々，ある特定のブラウザにおいて脆弱であると判断され，EV 証明書として本来機能するべきグリーンバーが表示されないことが指摘されていた．

2018 年 10 月，主要ブラウザが同時に TLS1.0/1.1 のサポート排除を 2020 年前半に予定しているとのアナウンスがなされた [7] ．アップデート頻度も高く，最新版に更新される仕組みが整っている TLS クライアント（ブラウザ）においては，サーバに接続できない等の不具合が起こると考えられ，サーバサイドでの対応が必要であると認識されていた [8], [9]．この低いプロトコルバージョンの排除対策に呼応して SSL/TLS サイトランクにおいては TLS1.0 または TLS1.1 に対応しているサーバをランク B に下落させる計画が事前にアナウンスが行われ，正式に 2020 年 1 月 31 日よりその措置が取られている [17]．その影響により一時的なランク低下が見られたが，ランク付けポリシー変更実施後の 10 日程度後の時期に TLS1.0 および TLS1.1 の無効化措置が行われ，ランクサイトに対抗していた [10]．本稿は 2021 年 1 月 15 日に行った追調査の報告を行う．

2. 追調査の方針

ある業界の協会に属するサーバ群において，より重要情報を扱うためのログインサイトについては，Top FQDN とは異なる FQDN でサービス提供されている．Top FQDN におけるサーバ群では .jp ドメイン全体と同様の傾向があったが，より安全な設定の基でサーバ運用がされていることが既に報告されている．ここでログインサイトは比較的規模の小さい組織においてはアウトソーシングサービスを利用していることが多いため，同じ FQDN で複数組織のログインサービスが提供されているため集約されることになる．2017 年までの報告ではトータルで 58 の FQDN が調査対象であった．2019 年に再調査を行うにあたり利用サービスをひとつひとつ手動で再度調査した結果，55 を調査対象とする判断を行っている．これは (1) 経営統合によりサービス中止したため 1 サイトを比較対象から外す，(2) オンプレミスでサービス構築を行っていたが他組織と同じ FQDN での提供に統合されたため 1 サイトを比較対象が外す，(3) 利用者がログインできる IP アドレス群を制限したためクロールできない 1 サイトを比較対象から外す，という方針のためである．ただし 1 サイトは提供される FQDN が変更されたがオンプレミスでサービス構築を行っていることから比較対象として残すこととしている．

3. 追調査の結果

今回も，独自のクローリング実装を利用せず，あえて読者に再現性を持たせることも考慮して広く利用されている SSL/TLS サーバ評価システムである Qualys SSL Labs [11] を利用した．ランク付けの方針は SSL Server Rating Guide [12] で規定されており，本ガイドラインは年を重ねることによって実情に見合うように見直されている．

表-1 は SSL/TLS バージョン対応状況を示している．本稿では 2020 年 7 月 24 日と 2021 年 1 月 15 日の調査結果が追記されている．

前回 1 年前から比べると TLS1.0 の排除が進んでいることが分かる．また TLS1.3 対応サイトが出現している．

今回利用したランキング手法は A 以上が安全であるとされており要因によって B から F までランク付けされる仕組みである．例えば SSL3.0 利用で C ランク，DES 等の 56 ビット暗号利用で F ランクのように決められている．今回得られた結果は，A ランク 4 サイト（2019 年 6 月調査：3 サイト，2019 年 12 月調査：4 サイト），B ランク 50 サイト（前々回：48 サイト, 前回：47 サイト），C ランク 0 サイト（前々回，前回ともに 2 サイト），F ランク 1 サイト（前々回，前回ともに 2 サイト）であった．大きな変化はないものの C ランクにカテゴライズされたサーバは 0 となり SSL3.0 利用サイトは全て無くなったことを裏付けている．なお 7 月 19 日から 24 日の間にランク C が B ランクに変更されているサイトが存在しており，7 月 20 日はサーバにアクセスできなかったことからメンテナンス期間であったことと，このメンテナンス期間に設定変更が行われ SSL3.0 を排除したと考えられる．

また依然として残されている F ランク 1 サイトは Bleichenbacher 攻撃の亜種である ROBOT 攻撃 [16] に脆弱であると判断されており，この結果は 2019 年 6 月調査時から変化していなかった．ROBOT 攻撃は BEAST や POODLE と同様に何度もトライ＆エラーを繰り返しリクエストを送ることで，過去の暗号メッセージを復元するという類の攻撃である．ROBOT 攻撃のリスクを許容するかどうかは意見が分かれるところではあるが，通常ユーザが気軽にランクを確認できることから，このようなランク表示がされることによりミスリーディングを起こしやすいため，速やかな対策が必要であると考えられる．

version	2016-10	2017-04	2019-01	2019-06	2019-12	2020-07	2021-01
SSL2.0	0	0	0	0	0	0	0
SSL3.0	8	3	2	2	2	1	0
TLS1.0	55	55	55	55	55	50	40
TLS1.1	18	23	23	39	40	39	38
TLS1.2	36	37	53	53	54	55	55
TLS1.3	-	-	0	0	0	0	1

表 1 SSL/TLS バージョン対応状況

次に B ランクへの下落要因の変化について考察する．Forward Secrecy 対応のアルゴリズム [13] に未対応（noFS），TLS1.3 [14] で義務化された AEAD 暗号の未サポート（noAEAD），RC4 [15] の利用（noMoreRC4），鍵長の短い Diffie-Hellman 方式の利用（weakDH）について表 2 にまとめている．

全体的に改善が見られる．特に RC4 排除（脆弱サイト数：21 → 4）と AEAD 対応（未対応サイト数：31 → 6）は大きな改善が見られる．一方でランク B にカテゴライズされている理由の多くは TLS1.0/1.1 に対応したままであることが要因であることが分かった．

4. まとめ

ある業界の決済システム等の企画・運営を行っている協会に属する正会員の Web サイトのログインサイトについて調査を行った．2019 年 12 月に調査を行った前回の報告では 55 サイトのうち 1 サイトは SSL3.0/TLS1.0 しか対応していなかった．そのため，主要ブラウザの「TLS1.0/1.1 排除」が行われた場合には当該サイトにはアクセスできないため速やかに対応する必要があったが，無事に対応されていることを確認できた．

最も最新バージョンである TLS1.3 への対応サイトが 1 つ観測されており，一部のクラウドサービスが牽引して今後普及していくことが予想される．また，前回報告において 2 サイトが Padding Oracle 攻撃の 1 種である ROBOT 攻撃に対応していないことが指摘されており重大な脆弱性としてレーティングされているためランクが非常に低くなっており，依然として対応が必要であることが分かった．またランクサイトの評価としては B ランクではあるが，その要因について調査したところ，RC4 排除（脆弱サイト数：21 → 4）と AEAD 対応（未対応サイト数：31 → 6）は大きな改善が見られており，ランク低下の主要因は TLS1.0/1.1 が理由であることが判明している．

今後も継続して報告を行う予定であるが .jp ドメインなどに拡大して調査することも視野に入れて検討を行う．

reason	2019-01	2019-06	2019-12	2020-07	2021-01
noFS	44	41	40	28	27
noAEAD	35	33	31	15	6
noMoreRC4	22	21	21	5	4
weakDH	8	9	10	9	8

表 2 B ランク下落要因の変化

参考文献

[1] 須賀, 国内 Web サイトの SSL 設定状況に関する 2012 年度と 2013 年度の比較・考察, 第 6 回インターネットと運用技術シンポジウム, 2013.
[2] Y. Suga, SSL/TLS status survey in Asia region - Transitioning against the renegotiation vulnerability, CRIME attacks and untrusted X.509 certificates, Internet Technologies & Society 2013 Conference (ITS 2013).
[3] 須賀, 国内 SSL サイトにおける証明書 FQDN ミスマッチ状況等の可視化，情報処理学会第 76 回全国大会, 2014.
[4] Google Chrome57 のバグにより EV SSL 証明書の組織名がグリーン表示されない事象について, https://knowledge.symantec.com/jp/support/ssl-certificates-support/index?vproductcat=V_C_S&vdomain=VERISIGN.JP&page=content&id=INFO4287&actp=RSS&viewlocale=ja_JP&locale=ja_JP&redirected=true
[5] EV SSL サーバ証明書の Policy OID の変更について, https://knowledge.symantec.com/jp/support/ssl-certificates-support/index?vproductcat=V_C_S&vdomain=VERISIGN.JP&page=content&actp=CROSSLINK&id=ALERT1955&locale=ja_JP&redirected=true
[6] 須賀, ”EVSSL 証明書利用時の表示不備に関する調査”, 第 18 回 インターネットテクノロジーワークショップ, 2017.
[7] https://blogs.technet.microsoft.com/jpsecurity/2018/10/16/tlsdeprecation/
[8] 須賀, TLS バージョン移行に関する局所的調査（FY2019 1Q）, IPSJ 第 81 回全国大会, 2019.
[9] 須賀, TLS バージョン移行と EV SSL 証明書利用に関する局所的調査（FY2019 2Q）, FIT2019, 2019.
[10] 須賀, TLS バージョン移行と EV SSL 証明書利用に関する局所的調査（FY2019 4Q）, ICSS2019-86, 2020.
[11] Qualys SSL Labs, SSL Server Test, https://www.ssllabs.com/ssltest/
[12] Qualys SSL LabsSSL, SSL Server Rating Guidehttps://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide
[13] Y. Suga, SSL/TLS Servers Status Survey about Enabling Forward Secrecy, 17th International Conference on Network-Based Information Systems (NBiS), 2014.
[14] RFC8446: The Transport Layer Security (TLS) Protocol Version 1.3, https://tools.ietf.org/html/rfc8446
[15] Mathy Vanhoef, Frank Piessens and iMinds-DistriNet, RC4 NOMORE, https://www.rc4nomore.com/
[16] The ROBOT Attack, https://robotattack.org
[17] Qualys SSL Labs, SSL Labs Grade Change for TLS 1.0 and TLS 1.1 Protocols, https://blog.qualys.com/ssllabs/2018/11/19/grade-change-for-tls-1-0-and-tls-1-1-protocols