L-018

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）
Local survey on transitioning of TLS version and EV SSL Certificates Usage

須賀 祐治 *
Yuji SUGA

あらまし ある特定の分野における TLS サーバ設定に関する調査報告を行う．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ている．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ており，サーバサイドでの対応が必要である．本稿では TLS バージョン対応と利用アルゴリズムについて局所的調査を行い報告する．

キーワード SSL/TLS, 移行工学，EV SSL 証明書, ROBOT 攻撃, クロスルート証明書

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 [4]．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．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．本稿は 2019 年 6 月 7 日に行った追調査の報告を行う．

2 ログインサイトに絞った追調査の方針

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，以下に示すように，より安全な設定の基でサーバ運用がされていることが分かった．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 年の報告ではトータルで 58 の FQDN が調査対象であった．今回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た．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た．

3 追調査の結果

今回，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

* 株式会社インターネットイニシアティブ, 〒 102-0071 東京都千代田区富士見 2-10-2 飯田橋グラン・ブルーム, Internet Initiative Japan Inc., Iidabashi Grand Bloom, 2-10-2 Fujimi, Chiyoda-ku, Tokyo, 102-0071 Japan suga@iij.ad.jp

いる SSL/TLS サーバ評価システムである Qualys SSL Labs [5] を利用した．ランク付けの方針は SSL Server Rating Guide [6] 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．

version	2016-10	2017-04	2019-01	2019-06
SSL2.0	0	0	0	0
SSL3.0	8	3	2	2
TLS1.0	55	55	55	55
TLS1.1	18	23	23	39
TLS1.2	36	37	53	53
TLS1.3	-	-	0	0

表 1: SSL/TLS バージョン対応状況

3.1 バージョン移行の考察：TLS1.1 対応の増加

前回の報告 [7] とのバージョン対応状況の変化は図 1 のとおりである．時期的には 5ヶ月しか間隔がないが年度を跨いでいるため念のため変化があるかどうか調査を行ったところ TLS1.1 対応サーバが大きく変化していることが分かった．これは主要ブラウザの「TLS1.0/1.1 排除」[8] による移行促進の影響ではないと考えられる．何故急に TLS1.1 対応が行われたかは今のところ原因は不明である．また，55 サイトのうち 2 サイトは未だに SSL3.0/TLS1.0 しか対応していないため，当該サイトには 2020 年後半以降アクセスできない状況であり速やかに対応する必要がある．

3.2 B ランク下落要因の考察：若干の改善

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．

rank	2019-01	2019-06
A	3	4
B	48	47
C	2	2
D	0	0
F	2	2

表 2: ランクの変化状況

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 [9] に未対応（noFS），TLS1.3 で義務化された AEAD 暗号の未サポート（no AEAD），鍵長の短い Diffie-Hellman 方式の利用（weakDH）について表 3 にまとめている．前者 2 つの要因については若干の改善が見られるが，weakDH については 1 サイトが改悪を行っている．フィーチャーフォンなどの古いデバイス対応，つまり後方互換性の確保などが理由である可能性が高い．また，依然として F ランク 2 サイトは Bleichenbacher 攻撃の亜種である ROBOT 攻撃 [10] に脆弱であると判断されている．

reason	2019-01	2019-06
noFS	44	41
noAEAD	35	33
weakDH	8	9

表 3: B ランク下落要因の変化

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．55 サイトのうち 2 サイトは SSL3.0/TLS1.0 しか対応していないため，2020 年前半に予定されている主要ブラウザの「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状況であり速やかに対応する必要がある．昨年 RFC 化された TLS1.3 への対応はまだ 0 サイトであるが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，今回上記とは異なる 2 サイトにおいて 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，早急な対応が必要であることが分かった．今後も 2020 年に向けて「TLS1.0/1.1 排除」に対処できているかどうか継続して報告を行うが .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．

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] 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.

[5] Qualys SSL Labs, SSL Server Test, https://www.ssllabs.com/ssltest/

[6] Qualys SSL LabsSSL, SSL Server Rating Guidehttps://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide

[7] 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.

[8] https://blogs.technet.microsoft.com/jpsecurity/2018/10/16/tlsdeprecation/

[9] Y. Suga, SSL/TLS Servers Status Survey about Enabling Forward Secrecy, 17th International Conference on Network-Based Information Systems (NBiS), 2014.

[10] The ROBOT Attack, https://robotattack.org