Vol.2016-CSEC-75 No.3
2016/12/1

SSL/TLSサーバにおける検索窓問題とその対策（速報）

須賀 祐治[1,a)]

概要：Alexa 提供の URL リストのうち.jp ドメインのものを抽出し 2016 年 10 月 24 日から 25 日にかけてクローリングを行った．当初はすでに脆弱であると認識されている SSL2.0/3.0 や Export-grade 暗号アルゴリズムの利用率改善に関する現状を確認するために広域調査を行ったが，本来使われてはいけない証明書が配備されている事例が多く存在することが分かったため速報として報告を行う．また，2016 年 10 月にアップデートされた一部のブラウザにおいてセキュリティインディケータの表記方針が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．本稿はこの「検索窓問題」について，ある特定の分野での状況報告と Web サイトタイプの分類，対策方法について報告する．

キーワード：検索窓問題, SSLyze, EVSSL 証明書

Search box issues and their countermeasures on SSL/TLS servers (Rapid survey)

Yuji Suga[1,a)]

Abstract: We were crawling .jp domain SSL/TLS servers in the URL list by Alexa through October 24 and 25, 2016. We have surveillance in order initially to confirm the current status related to improving use rate of SSL2.0 / 3.0 and the Export-grade encryption algorithms. There are many server certificates that actually deployed, these cases should not be used inherently, so we report as a breaking news. Further the notation policy of security indicators in a certain browser that have been updated in October 2016 has been changed. Although the URL representation portion should be green when using EV SSL certificate, the sites determined not to be safe were found here and there. This paper points out "search box issues" and also reports status about SSL/TLS sites and countermeasures against this kind of this problems.

Keywords: Search Box Issues, SSLyze, Extended Validation Certificate

1. はじめに

2014 年 10 月に発覚した POODLE 攻撃を発端に SSL3.0 以下のプロトコルの利用は危険であるという認識が広がっている．さらに 2016 年 3 月には，たとえ最新のクライアント（ブラウザ）を利用しているケースにおいても SSL2.0 に対応しているサーバが存在した場合に中間者攻撃が可能であるという DROWN attack が公開された．しかしこのような状況においても，未だに設定不備のサイトも散見されている．本稿では SSL/TLS のバージョン対応状況に関する定点観測の結果と，ブラウザの表示ポリシー変更によって新たな問題が発覚していることを報告する．特に，EVSSL 証明書を利用していたとしても，ブラウザ上では安全であるとは表示されておらず EVSSL 証明書をうまく活用されていない事例を取り上げ「検索窓問題」と呼ばれる問題について報告し，対処方法について紹介する．

[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

2. 観測環境

地方自治体および大学のサイトについて上記脆弱性の対策状況についてクローリングすることで SSL/TLS の設定状況を把握する先行研究がある [20]．これらの研究では，THC-SSL-DOS 対策, RFC5746 対策, 証明書の受け入れ対策, RSA 鍵長対策, CRIME 攻撃対策について調査対象となっていたが，実際に利用されるアルゴリズムについての調査は対象となっていなかった．

今回の調査対象は [33] と同様に以下の通りである．今回クローリングに際し利用したソースはすべて Alexa [21] 提供のリストから抽出したものである．

- (α) Alexa top sites の上位 20000 サイト
- (β) .jp ドメイン 17988 サイト
- (γ) ある業界の協会における正会員 120 サイト

ここで SSL/TLS 接続が確立したとしても共用サーバの利用など意図せず SSL を有効にしているケースが見受けられるため，サーバ証明書の FQDN マッチングが OK なもののみを取り上げた． これは通常のブラウザにおいてエラーを起こさないように設定されており，実際に SSL/TLS が利用されていると考えられるサーバのみを調査対象とすることで，より現実的な状況把握を行うことを目指した．公開鍵証明書の大規模収集という観点では，EFF SSL Observatory[22] や PsQs [23],RwWr[24] などの調査が存在する．このクローリング方式においては IP アドレスベースの調査のためテストサイトなど実際に利用されていない証明書を収集してしまうデメリットがある．実際 Heninger らの調査 [23] においては 60%以上のサイトがほかのサイトと秘密鍵ペアを意図せず共有しているという調査結果が報告されており，これは実際に正しく運用されていないサイトをカウントしている点や，同じ FQDN に対して複数の IP アドレスが割り振られている点などの事情をうまく汲み取れていないと考えられる．

結果として本稿では以下の SSL/TLS サーバ (重複あり) について調査を行っている．

- (α) Alexa top sites 6835 サイト
- (β) .jp ドメイン 5668 サイト
- (γ) ある業界の協会における正会員 115 サイト

それぞれのサーバ群に対して SSL/TLS バージョン対応状況の推移について報告を行う．以下の結果は 2016 年 10 月 24 日から 25 日にかけてクローリングによるものである．

2.1 SSL/TLS バージョン対応状況

(α) Alexa top sites，(β) .jp ドメインともに SSL 利用率が下がっていることが分かる．一方で，同日に調査した結果である表 3 を見ると (α) Alexa top sites と比べると (β) .jp ドメインでは対応が大幅に遅れている．広いユーザ層にログイン機能を提供するサイトをそれぞれ擁している (γ) 某協会は一般的な .jp ドメインよりも強固な対策が行われていると考えられていたが，これを見ると分かるように .jp ドメインの傾向とほぼ一致している．

version	2014-04-27	2014-11-26	2015-01-07	2015-06-27	2016-10-24
SSL2.0	05.23	01.73	01.62	01.23	00.4
SSL3.0	98.57	37.42	33.78	23.67	09.3
TLS1.0	99.48	99.69	99.75	99.39	97.1
TLS1.1	56.66	72.66	74.46	80.83	90.8
TLS1.2	60.66	76.42	78.37	83.98	93.4

表 1 SSL/TLS バージョン対応状況 - (α) Alexa top sites

version	2014-04-27	2014-11-26	2015-01-07	2015-06-27	2016-10-24
SSL2.0	24.08	12.91	12.12	09.30	04.2
SSL3.0	99.91	62.32	57.44	49.89	30.6
TLS1.0	99.86	98.84	98.63	99.64	99.2
TLS1.1	15.61	27.27	28.94	36.96	62.8
TLS1.2	17.86	29.98	31.67	40.36	65.9

表 2 SSL/TLS バージョン対応状況 - (β) .jp ドメイン

3. 検索窓問題

SOUPS2016 [34] においてセキュリティインディケータについての議論が行われている．1300 を超えるユーザにアンケートを行い，40 種（8 型 5 色）の表記方法に関してどう感じ取るか調査し最適なものを導出し，実際のブラウザに展開するという研究である．実際に適用される対象となったアイコンは以下の 6 種類のうち 4 つであった．

- (採用) コネクション-”Valid HTTPS”
- (採用) コネクション-”HTTPS with minor errors”
- (採用) コネクション-”HTTPS with major errors”
- コネクション-”HTTP”
- (採用) トラスト-”EV (Extended Validation) HTTPS”
- トラスト-”Malware and phishing”

”major errors”は証明書ストアから当該証明書に辿れないことや有効期限を過ぎているなどのエラーを指し示している．また，”minor errors”は HTTPS で返却された HTML コンテンツに HTTP で指し示された画像がある等を示しており，具体的には HTTP でアクセスしたときと同様のアイコンが利用されている．そのため HTTPS でアクセスしているにも関わらず安全でないと表記されてしまう．これは EVSSL 証明書を利用している場合でも同様であり，ここに EVSSL 証明書をうまく利用できていない事例が発生する余地を残していることとなる．

以下，(γ) ある業界の協会における正会員 115 サイトに対して調査した結果をまとめておく．

3.1 リダイレクト状況

3.1.1 HTTPS → HTTP

HTTPS で Top FQDN(紙媒体などで広くアナウンスされた当該サイトの FQDN) にアクセスした場合の状況を以下に示す．

- 200 - 61 件
- 302 で HTTP にフォワード - 18 件
- 403 or 404 - 19 件
- FQDN ミスマッチ - 13 件

ここで Top FQDN に HTTPS でアクセスした場合に，Top FQDN とは異なるサーバ証明書を返却するケースが 10%見受けられた．これは設定ミスであるケースも見受けられるが CDN サービスを用いているためにクラウド側のサーバ証明書が反応するケースもあった．このようなケースでは検索サイトなどからアクセスする場合にがこの問題は発生せず，わざわざユーザが http を https と打ち直す場合において生じる軽微な問題とも言える．しかし，ブラウザにおいては証明書ストアからと辿れない，もしくは FQDN ミスマッチのエラーが発生することからこれも回避しておくべきだと考えられる．また 403 や 404 が返却されるケースもあるが，これも同様にユーザから見たときには少なくともエラーが返却されており，回避しておくべきであろう．

一方で HTTP にフォワードするケースもある．これらのケースにおいては Top FQDN の正規証明書が利用されており，ユーザにエラーが返却されることなくアクセス可能としている．そのためだけに証明書を利用することはコスト高になることから，ユーザにデータ入力させる，例えば顧客問い合わせのようなページにおいて利用することが望ましいと言える．

version	(α) Alexa top sites	(β) .jp ドメイン	(γ) 某協会
SSL2.0	00.4	04.2	04.3
SSL3.0	09.3	30.6	34.8
TLS1.0	97.1	99.2	100.0
TLS1.1	90.8	62.8	67.0
TLS1.2	93.4	65.9	69.6

表 3 2016-10-24 における各カテゴリごとの SSL/TLS バージョン対応状況

3.1.2 HTTP → HTTPS

7 サイトが HTTP でのアクセスを許可せず HTTPS サイトにフォワードされている．常時 SSL/TLS を利用するトレンドに迎合していると考えられる．しかし，このケースにおいて「コネクション-”HTTPS with minor errors”」のように HTTPS サイトに HTTP コンテンツが内包しているために前述したように HTTPS が安全でないと表示される場合が存在する．具体的には，HTTPS で返却されるコンテンツのうち.js ファイルの一部に HTTP でアクセスする「検索窓」がヘッダ部分に含まれているために上記のように安全でないと判断されている事例が複数存在する．これを「検索窓問題」と呼ぶこととする．

3.2 理想的な HTTP/HTTPS サイト設計

上記を踏まえ，よりよいサーバ設計について示唆しておく．ここで Top FQDN とは紙媒体などで広くアナウンスされた当該サイトの FQDN を指す．

- Top FQDN で HTTP でアクセスされた場合，HTTPS にフォワードする場合にはブラウザエラーを発生しないように正しい証明書を返却するべきである
- Top FQDN の HTTPS サイトは HTTP サイトとコンテンツを分離するべきである
- Top FQDN で HTTPS でアクセスされた場合，HTTP にリダイレクトするケースでは Top FQDN の証明書はブラウザの証明書ストア配下に置かれるべきである（エラーメッセージは発生しないようにする）
- ログインサイトへのリンクは HTTPS ページから行われるべきである
- ログインページの EVSSL 証明書はアウトソーシング先の業者名ではなく，当該サイトの正式名称が表記されるべきである

4. まとめ

本稿は執筆時点 (2016 年 11 月 7 日) でも速報をまとめているが 3 ヶ月以内により詳細な報告を行う予定である．

参考文献

[1] NIST, "SUPPLEMENTAL ITL BULLETIN FOR SEPTEMBER 2013", http://csrc.nist.gov/publications/nistbul/itlbul2013_09_supplemental.pdf
[2] ArsTechica, "Stop using NSA-influenced code in our products, RSA tells customers", http://arstechnica.com/security/2013/09/stop-using-nsa-influencecode-in-our-product-rsa-tells-customers/?comments=1&post=25330407#comment-25330407
[3] Dan Shumow, Niels Ferguson, "On the Possibility of a Back Door in the NIST SP800-90 Dual Ec Prng", Rump session in CRYPTO2007, http://rump2007.cr.yp.to/15-shumow.pdf
[4] Debian Security Advisory, "DSA-1571-1 openssl – predictable random number generator", http://www.debian.org/security/2008/dsa-1571
[5] IIJ, IIR Vol.17, "1.4.1 SSL/TLS, SSH で利用されている公開鍵の多くが他のサイトと秘密鍵を共有している問題, http://www.iij.ad.jp/development/iir/pdf/iir_vol17.pdf
[6] bitcoin.org, "Android Security Vulnerability", http://bitcoin.org/en/alert/2013-08-11-android
[7] Joppe W. Bos, J. Alex Halderman, Nadia Heninger, Jonathan Moore, Michael Naehrig, Eric Wustrow, "Elliptic Curve Cryptography in Practice", https://eprint.iacr.org/2013/734
[8] 須賀, "Bitcoin の ECDSA 署名生成時にポカしたら現金搾取される", 4A1-3, SCIS2014.
[9] IETF Blog, "We Will Strengthen the Internet", http://www.ietf.org/blog/2013/11/we-will-strengthen-the-internet/
[10] CA Security COUNCIL Blog, "IETF 88 - Pervasive Surveillance, https://casecurity.org/2013/11/26/ietf-88-pervasive-surveillance/
[11] IETF 88 Technical Plenary: Hardening The Internet, https://www.youtube.com/watch?v=oV71hhEpQ20
[12] The TLS Protocol Version 1.0http://www.ietf.org/rfc/rfc2246.txt
[13] Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security(TLS), http://www.ietf.org/rfc/rfc4492.txt
[14] Google Online Security Blog, "Protecting data for the long term with forward secrecy", http://googleonlinesecurity.blogspot.jp/2011/11/protecting-data-for-longterm-with.html
[15] Facebook Engineering, "Secure browsing by default", https://www.facebook.com/notes/facebook-engineering/secure-browsing-by-default/10151590414803920
[16] The Twitter Engineering Blog, "Forward Secrecy at Twitter", https://blog.twitter.com/2013/forward-secrecy-at-twitter-0
[17] The GitHub Blog, "Introducing Forward Secrecy and Authenticated Encryption Ciphers", https://github.com/blog/1727-introducing-forward-secrecy-andauthenticated-encryption-ciphers
[18] Electronic Frontier Foundation, "UPDATE: Encrypt the Web Report: Who's Doing What", https://www.eff.org/deeplinks/2013/11/encrypt-web-reportwhos-doing-what#crypto-chart
[19] Qualys Community, "Configuring Apache, Nginx, and OpenSSL for Forward Secrecy", https://community.qualys.com/blogs/securitylabs/2013/08/05/configuringapache-nginx-and-openssl-for-forward-secrecy
[20] Yuji Suga, SSL/TLS status survey in Japan - transitioning against the renegotiation vulnerability and short RSA key length problem, The 7th Asia Joint Conference on Information Security (AsiaJCIS 2012).
[21] http://www.alexa.com/topsites
[22] Electronic Frontier Foundation, The EFF SSL Observatory, https://www.eff.org/observatory
[23] Nadia Heninger, Zakir Durumeric, Eric Wustrow, J. Alex Halderman, "Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices", USENIX Security'12.
[24] Arjen K. Lenstra, James P. Hughes, Maxime Augier, Joppe W. Bos, Thorsten Kleinjung, Christophe Wachter "Public Keys", CRYPTO2012.
[25] The Heartbleed Bug, http://heartbleed.com/
[26] OpenSSL Security Advisory [07 Apr 2014], "TLS heartbeat read overrun (CVE-2014-0160)", https://www.openssl.org/news/secadv_20140407.txt
[27] https://freakattack.com
[28] https://freakattack.com/vulnerable.txt
[29] https://weakdh.org
[30] DROWN attack, https://drownattack.com/
[31] 須賀, SSL/TLS サーバにおける Forward Secrecy への対応状況について（+速報版 Heartbleed Bug 発覚後の状況変化, 第 65 回 CSEC 研究発表会, 2014.
[32] 須賀, POODLE attack 公開後の SSL/TLS サーバのバージョン移行状況, IPSJ 第 77 回全国大会, 2015.
[33] 須賀, Export-grade な暗号アルゴリズムを用いたダウングレード攻撃に対する SSL/TLS サーバの対処状況について, FIT2015.
[34] Adrienne Porter Felt, Robert W Reeder, Alex Ainslie, Helen Harris, Max Walker, Chris Thompson, Mustafa Acer, Elisabeth Morant, Sunny Consolvo, "Rethinking Connection Security Indicators", SOUPS2016, http://research.google.com/pubs/pub45366.html

付　　録

(γ) におけるバージョン対応状況 - 1:対応/0:非対応

SSL2.0	SSL3.0	TLS1.0	TLS1.1	TLS1.2
0	0	1	1	1
0	0	1	1	1
0	1	1	1	1
0	0	1	1	1
0	0	1	1	1
0	0	1	1	1
0	1	1	0	0
0	1	1	1	1
0	0	1	0	0
0	1	1	1	1
0	1	1	0	0
0	1	1	0	0
0	0	1	0	0
0	0	1	1	1
0	1	1	1	1
0	1	1	1	1
0	1	1	0	0
0	0	1	1	1
1	1	1	1	1
0	0	1	1	1
0	1	1	1	1
0	1	1	0	0
0	0	1	1	1
0	1	1	1	1
0	0	1	1	1
0	1	1	1	1
0	0	1	1	1
0	0	1	0	0
0	0	1	0	0
0	0	1	1	1
0	0	1	1	1
0	0	0	0	0
0	0	1	1	1
0	1	1	1	1
0	0	1	0	0
0	0	1	1	1
0	0	1	1	1
0	0	1	1	1
0	1	1	1	1
0	1	1	0	1
0	0	1	0	0
0	1	1	1	1
0	0	1	1	1
0	0	1	1	1
0	1	1	0	0
0	1	1	1	1
0	0	1	0	0
0	0	1	1	1
0	0	1	1	1

SSL2.0	SSL3.0	TLS1.0	TLS1.1	TLS1.2
0	1	1	0	0
0	1	1	1	1
0	0	1	1	1
1	1	1	0	0
0	0	1	1	1
0	1	1	0	0
1	1	1	1	1
0	0	1	1	1
0	0	1	1	1
0	0	1	1	1
0	0	1	1	1
0	0	1	0	1
0	0	1	1	1
0	1	1	1	1
0	0	1	1	1
0	0	1	0	0
0	0	1	1	1
0	0	1	0	0
0	0	1	1	1
0	0	1	1	1
1	1	1	0	0
0	0	0	0	0
0	0	1	1	1
0	0	0	0	0
0	0	1	1	1
0	0	1	0	0
0	0	1	0	0
0	0	1	0	0
0	0	0	0	0
0	0	1	0	0
0	0	1	1	1
0	1	1	1	1
0	0	1	1	1
0	0	1	1	1
0	1	1	1	1
0	1	1	0	0
0	0	1	0	0
0	0	1	1	1
0	0	1	0	1
0	0	1	0	0
0	1	1	1	1
0	0	1	1	1
0	0	1	1	1
0	0	1	0	0
0	0	1	1	1
0	1	1	1	1
0	0	1	1	1
0	1	1	0	0
0	0	1	1	1
0	0	1	0	0
0	0	1	1	1
0	1	1	0	0
0	0	1	0	0

SSL2.0	SSL3.0	TLS1.0	TLS1.1	TLS1.2
0	1	1	1	1
1	1	1	0	0
0	0	1	1	1
0	1	1	0	0
0	0	1	1	1
0	1	1	0	0
0	0	1	1	1
0	0	0	0	0
0	0	1	1	1
0	0	1	1	1
0	0	1	1	1
0	0	1	1	1
0	0	1	0	0
0	1	1	1	1
0	0	1	1	1
0	0	1	1	1
0	0	1	1	1