Vol.2017-IOT-36 No.17
2017/3/3

ブラウザにおける検索窓問題と対処方法

須賀 祐治[1,a)]

概要：2014 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た．さらに証明書に着目すると，最近ブラウザの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．この問題と同様の状況として，本来安全であるのに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「検索窓問題」について詳細な調査を行った．今回調査対象としたのは，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 サイトである．一般的に紙媒体などで広くアナウンスされている Top FQDN の SSL/TLS サイトについて調査したところ半数程度は正常動作であったものの FQDN ミスマッチなどの問題を抱えていることが分かった．さらに Top FQDN の HTTP（not HTTPS）サーバからユーザログインページに辿り着くパスについていくつかのパターン分けを行い，上記「検索窓問題」の影響について手動で調査した結果も示す．最後に，この問題を解決するための対策方法として HTTP/HTTPS サイトの設計指針についても触れる．

キーワード：検索窓問題, SSLyze, EVSSL 証明書

The browser's "search form" issues and countermeasures

Yuji Suga[1,a)]

Abstract: From 2014, we are conducting fixed point observation to crawl SSL/TLS sites using .jp domain URL list extracted from Alexa Top Sites, and investigation on improvement of usage rate of SSL/TLS versions and Export-grade encryption algorithms. Furthermore, paying attention to the server side certificates, since the notation policy of the browser security indicator had recently changed, the green bar is displayed in the URL notation part originally although it uses the EVSSL certificate, it is "not safe" though sites that are judged were also found. As a situation similar to this issue, a detailed investigation was conducted on the browser's "search form" issues which are originally described to be safe although it is said to be unsafe due to inadequate site-contents. In this paper, the survey targeted are the websites of regular members belonging to the association which is planning and managing settlement systems and the like in "a certain" industry. We investigated SSL/TLS sites of Top FQDN which are widely announced on paper medium etc, so it was found that about half of them were in normal situation but half had problems such as FQDN mismatch. Moreover we also show the result of manually investigating the influence of the above "search form" issues by carrying out some pattern classification on the path reached from the HTTP (not HTTPS) server of the Top FQDN to the user login page. Finally, the design guideline of HTTP/HTTPS sites is mentioned as one of countermeasures against this kind of problems.

Keywords: Search Box Issues, SSLyze, Extended Validation Certificate

[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

1. はじめに

2014 年 10 月に発覚した POODLE 攻撃 [1] によりメッセージの暗号化に CBC 暗号モードを利用した場合に Padding Oracle 攻撃が可能になることが分かり，現在は SSL3.0 の利用は危険であるという認識が広がっている [2]．また SSL2.0 についても以前より危険であることが知られており利用しないことが推奨されている．SSL の後継である TLS は現在 3 つのバージョン：TLS1.0（1999 年策定），TLS1.1（2006 年策定），TLS1.2（2008 年策定） [3] があり，いずれも未だに広く利用されているプロトコルである．TLS1.0 が SSL3.0 をベースに IETF で策定された後，TLS1.1 にて CBC 暗号モード利用時に露呈する BEAST 攻撃やその亜種への対策などを予め仕様に組み入れるなどの安全性強化がなされている．さらに TLS1.2 では認証暗号（AEAD：Authenticated Encryption with Associated Data）[4] の利用が可能となった．

しかし TLS プロトコルに対しても，ここ数年で多くの攻撃がなされている．2015 年 2 月に発行された RFC7457[5] は 2014 年頃までに公知となった TLS に対する攻撃の歴史がまとめられている．この RFC では RC4 ストリーム暗号に関する脆弱性が取り上げられているほか，利用者の想定よりも低い TLS バージョンを使用させるダウングレード攻撃や，圧縮機能を有効にしている場合に起こるタイミング攻撃など多岐にわたる既知の攻撃が取り上げられている．また，それ以降についての SSL/TLS の主な脆弱性のポータルサイトとしては CELLOS[6] などで参照できるが，それぞれの攻撃に対して知識を積み上げ，その都度対処していくことは大変難しい状況になったとも言える．例えば，サーバ運用者がどのように判断して CipherSuites（SSL/TLS で利用する暗号アルゴリズムの組）を決定すべきか判断に悩む事例がある．

RC4 に対する一連の鍵解読攻撃 [7] は RC4 が生成するストリーム鍵の僅かな不均衡（バイアス）から平文を復元する方法であり，具体的な脅威としてはブラウザ上で不正な JavaScript を動かせることによって大量の暗号文を生成するという手法 [8] がある．IETF としてもアカデミアによる複数の研究結果を鑑み，現実的な脅威として捉え 2015 年 2 月に RC4 を排除する旨の RFC[9] が発行されている．また TripleDES を含む CipherSuites の利用は脆弱であると再認識された SWEET32 攻撃 [10] [11] は，暗号アルゴリズムそのものに対する攻撃手法ではなく，SSL/TLS にて CBC 暗号モードを利用する際に起こり得る潜在的な攻撃であり，完全に防ぐことはできない．そのため各ベンダーの対策も TripleDES の利用を制限もしくは格下げするというアナウンスがなされている．

これら上記 2 つの暗号アルゴリズムに関連した脆弱性において，その実現可能性まで熟知した上で当該 CipherSuites の利用判断を行っているケースは非常に少ないと考えられる．特に TripleDES や CBC 暗号モードは，未だに CRYPTREC 暗号リストのうち電子政府推奨暗号リスト [12] に掲載されながらも，この「安全な」2 つのプリミティブを同時に利用したために脆弱になるという状況を引き起こしている点は興味深い事例である．暗号アルゴリズムのレイヤでの直接的な復元攻撃とは異なり，タイミング攻撃・サイドチャネル攻撃などにカテゴライズされる手法においても研究の進展があり，結果として TLS1.0 及び TLS1.1 では使用できない AEAD に対応するため TLS1.2 への移行が望まれている．これは CBC 暗号モードを利用していたとしても TLS1.1 以上のバージョンを利用することで BEAST 攻撃やその亜種への対策が可能と考えられてきた一方で，TLS1.2 に対してもタイミング攻撃が可能な Lucky13 攻撃 [13] が登場したことも AEAD 利用に拍車をかけることとなった．

CipherSuites の選択としては公開鍵暗号アルゴリズムとして Forward Secrecy 対応のアルゴリズムを選ぶことが望まれている点も考慮すべきである．加えて Export-grade 暗号の設定についても注意が必要である．クライアント（ブラウザ）を最新に保つことにより，サーバ側の CipherSuites 選択時に「より強い暗号アルゴリズム」が選ばれることが通常の挙動であるため，かつて使われていた弱い CipherSuites を設定上残しておいたとしてもそれらは使われることはないだろうと考えられていた．しかし 2015 年 1 月の FREAK 攻撃や同年 5 月の Logjam 攻撃の発表 [14] により Export-grade な暗号アルゴリズムを設定しているがために起こってしまう攻撃が発覚している．さらに 2016 年 3 月には DROWN 攻撃 [15] が公開され，Export-grade な暗号アルゴリズムを利用しない環境においても SSL2.0 を有効にしてしまっている状況下では，128 ビット暗号アルゴリズムを利用時にも復元攻撃が可能であることが判明した．

以上の状況を鑑みるに外部情報から，つまり脆弱性攻撃の公開ごとに対処するタイミングを逸しているためか，未だに設定不備のサイトが多く散見されている．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」と呼ばれるこの問題について報告し，対処方法の一部について示す．

2. 予備調査

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 [18]．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 [31] 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 [19] 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

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[20] や PsQs [21],RwWr[22] 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 [21] 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 (重複があることに注意) 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

3 点目である (γ) は，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 サイトである．利用した URL は協会にリストされているものであり，紙媒体などにも掲載されるような電話番号というところの大代表番号にあたる FQDN である．本稿ではこれを Top FQDN と呼び，実際にサービスが運用されている FQDN(s) とは異なるものであると考えられる．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

version	2014-04	2014-11	2015-01	2015-06	2016-10
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	2014-11	2015-01	2015-06	2016-10
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

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

(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 において (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ことが数字上では見て取れる．これは機会損失を回避するために広めに対応バージョンを取っていることに起因すると考えられるが，サーバのリプレースのインターバルが広い可能性もある．

広いユーザ層にサービス提供するサイトを擁していると考えられる (γ) ある業界の協会に属するサーバ群は一般的な .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．これも古いアルゴリズムやバージョンを利用することによるリスクを受容して，多くのデバイスから広くアクセスを許容するために行われていると考えられる．

2.2 Export-grade な暗号アルゴリズム利用状況

表 4 のとおり徐々にではあるが Export-grade な暗号アルゴリズムの利用が排除されていることが分かる． (γ) ある業界の協会に属するサーバ群では 115 のサイトのうち 40 ビット暗号アルゴリズム利用サイトは 9（7.8 %），56 ビット暗号アルゴリズム利用サイトは 25（21.7 %）であること

サーバリスト種別	(α) Alexa top sites		(β) .jp ドメイン		
観測日	2015-01-07	2015-06-27	2015-01-07	2015-06-27	2016-10-24
(40 ビット暗号アルゴリズム総計)	808	255	1444	970	475
DES-CBC-SHA	943	709	2648	2267	1609
DES-CBC-MD5	122	71	682	509	220
EDH-RSA-DES-CBC-SHA	408	276	2277	1960	1416
(56bits 暗号アルゴリズム総計)	947	711	2648	2268	1609

表 4 Export-grade な暗号アルゴリズムの SSL/TLS サーバにおける対応状況

が判明した．

これは前節の SSL/TLS バージョンの対応状況の結果とは少々事情が異なるように見受けられる．リスク受容をしてても「多くのデバイスから広くアクセスを許容する」意図が見て取れないためである．先に紹介した FREAK や Logjam 攻撃にように Export-grade な暗号アルゴリズムに対応したままのサーバに対する攻撃が存在することから早急に見直しが必要な要件であると考えられる．

3. 検索窓問題

SOUPS2016 [32] において，ブラウザのセキュリティインディケータ（URL 記載エリアの近くに配備されることが多く，押下することでより詳細な情報得られるためのトリガーボタンの役割も持ちあわせている）の表記方法に関する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．その結果，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 3 つであった．EVSSL 証明書を正しく利用している場合には CA Browser Forum で規定されているようにグリーンバーによる差別化が行われている．

- (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”
- 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「安全ではない」とも読み取れる表記がなされてしまう．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．

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 Mixed Contents エラー

前節で紹介したように HTTPS コンテンツに HTTP コンテンツが混じり込んでいる状況において主要ブラウザではこれをエラーの 1 種として扱うようになっている．そのためサーバ管理者およびコンテンツ管理者は早急な対策を要している．

主要ブラウザベンダーは 2013 年からこの類いの対応を行っており，いくつかの対処方法に関するドキュメントが公開されている [33] [34] [35] [36]．しかし SOUPS2016 での結果が実際のブラウザ実装に反映されはじめたため，決してセキュリティリテラシの高くないユーザ層からではなくとも，明らかに何らかの問題が生じているようなユーザインターフェイスを持つこととなってしまった．そのためサーバ管理者およびコンテンツ管理者の両者は，この Mixed Contents エラーを解消する必要がある．

しかしそれぞれのロールに属するスタッフは自身の責任範囲（カバレッジ）に気がついておらず，問題発覚およびその解消に時間を要している状況ではないかと予測される．さらにブラウザベンダーからは解決のために十分な情報の開示や検査ツールの提示が公開されているとは言い難く状況である．さらに誤検知と見られる事例もあり，検査ロジックのさらなる精度向上が必要であると言える．

3.3 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. ログインサイトに絞った追調査

前述した (γ) 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 (γ) のサーバ総数は 58 と大幅に低下しているのは，自社サーバで管理せずにアウトソーシングしているケースが多数あったためである．以下の数字は傾斜を設けずに純粋に 58 サーバを母数としたものである点に留意する．

version	(α)	(β) .jp	(γ) Top FQDN	(γ) Login
SSL2.0	00.4	04.2	04.3	00.0
SSL3.0	09.3	30.6	34.8	13.8
TLS1.0	97.1	99.2	100.0	100.0
TLS1.1	90.8	62.8	67.0	31.0
TLS1.2	93.4	65.9	69.6	62.1

表 5 ログインサイトにおける SSL/TLS バージョン対応状況

またログインサイトにおいては Mixed Contents エラーを生じるサイトは皆無であった．また Top FQDN に HTTP でアクセスしてログインサイトに辿るパスを全て検証したが，NonSSL(HTTP) サイトからログイン情報を入力させる 1 件の事例を除いては，概ね正しく設計されていた．ログインサイトにおいて EVSSL 証明書の利用がなされているものがほとんどであったが，アウトソースされた SIer が表記される事例が多く散在された．一方で，この問題を正しく解決しており，アウトソーシングしていても当該サービス提供企業の証明書が配備されている事例も見受けられた．ユーザニーズを正しく捉えているいい好例であると考えられる．

5. まとめ

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た．さらに本来安全であるのに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「検索窓問題」について追調査を行った．今回調査対象としたのは，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 サイトであった．一般的に紙媒体などで広くアナウンスされている Top FQDN の SSL/TLS サイトについて調査したところ半数程度は正常動作であったものの FQDN ミスマッチなどの問題を抱えていることが分かった．一方，重要情報を扱うログインを要するサービスサイトにおいては，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．

参考文献

[1] Bodo Möller, Thai Duong, Krzysztof Kotowicz, "This POODLE Bites: Exploiting The SSL 3.0 Fallback", https://www.openssl.org/~bodo/ssl-poodle.pdf
[2] RFC7568: Deprecating Secure Sockets Layer Version 3.0, https://datatracker.ietf.org/doc/rfc7568/
[3] RFC2246: The TLS Protocol Version 1.0http://www.ietf.org/rfc/rfc2246.txt
[4] RFC5116: An Interface and Algorithms for Authenticated Encryption, https://datatracker.ietf.org/doc/rfc5116/
[5] RFC7457: Summarizing Known Attacks on Transport Layer Security (TLS) and Datagram TLS (DTLS), https://datatracker.ietf.org/doc/rfc7457/
[6] CELLOS consortium, Publication, https://www.cellos-consortium.org/index.php?Publication
[7] Kenneth G. Paterson, "Big Bias Hunting in Amazonia : Large-scale Computation and Exploitation of RC4 Biases", ASIACRYPT2014 Invited Talk.
[8] Mathy Vanhoef, Frank Piessens, "All Your Biases Belong To Us : Breaking RC4 in WPA-TKIP and TLS", https://www.rc4nomore.com/vanhoef-usenix2015.pdf, RC4 NOMORE, https://www.rc4nomore.com/
[9] RFC7465 : Prohibiting RC4 Cipher Suites, https://datatracker.ietf.org/doc/rfc7465/
[10] Sweet32 : Birthday attacks on 64-bit block ciphers in TLS and OpenVPN, https://sweet32.info/
[11] Karthikeyan Bhargavan and Gatan Leurent, "On the Practical (In-) Security of 64-bit Block Ciphers : Collision Attacks on HTTP over TLS and OpenVPN", ACM CCS'16, http://dl.acm.org/citation.cfm?id=2978423&CFID=697886415&CFTOKEN=82935453
[12] CRYPTREC, 電子政府における調達のために参照すべき暗号のリスト, https://www.cryptrec.go.jp/list.html
[13] Nadhem AlFardan, Kenny Paterson, "Lucky Thirteen: Breaking the TLS and DTLS Record Protocols", http://www.isg.rhul.ac.uk/tls/Lucky13.html
[14] 須賀, 暗号と社会の素敵な出会い：2. SSL/TLS と暗号プロトコルの安全性 -恒久的に噴出する脆弱性との戦い-, 会誌「情報処理」Vol.56 No.11, http://id.nii.ac.jp/1001/00145437/
[15] The DROWN Attack, https://drownattack.com/
[16] CRYPTREC, SSL/TLS 暗号設定ガイドライン～安全なウェブサイトのために (暗号設定対策編)～, https://www.ipa.go.jp/security/vuln/ssl_crypt_config.html
[17] 情報処理推進機構, 「SSL/TLS アプライアンス製品の暗号設定方法等の調査報告書」の公開, http://www.ipa.go.jp/security/fy28/reports/crypto_survey/
[18] 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).
[19] http://www.alexa.com/topsites
[20] Electronic Frontier Foundation, The EFF SSL Observatory, https://www.eff.org/observatory
[21] 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.
[22] Arjen K. Lenstra, James P. Hughes, Maxime Augier, Joppe W. Bos, Thorsten Kleinjung, Christophe Wachter "Public Keys", CRYPTO2012.
[23] The Heartbleed Bug, http://heartbleed.com/
[24] OpenSSL Security Advisory [07 Apr 2014], "TLS heartbeat read overrun (CVE-2014-0160)", https://www.openssl.org/news/secadv_20140407.txt
[25] https://freakattack.com
[26] https://freakattack.com/vulnerable.txt
[27] https://weakdh.org
[28] DROWN attack, https://drownattack.com/
[29] 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.
[30] 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.
[31] 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.
[32] 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
[33] https://blog.mozilla.org/tanvi/2013/04/10/mixed-content-blocking-enabled-in-firefox-23/
[34] https://support.mozilla.org/ja/kb/mixed-content-blocking-firefox
[35] https://developers.google.com/web/fundamentals/security/prevent-mixed-content/what-is-mixed-content
[36] https://developers.google.com/web/fundamentals/security/prevent-mixed-content/fixing-mixed-content