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

須賀 祐治[1,a)]

概要：SSL および TLS プロトコルに対してメッセージをインジェクション可能な中間者攻撃が 2009 年に指摘され，結果的に RFC5746 が発行され仕様上の問題は解決されていると認識されている．しかし後方互換性を維持しない対策であることから対応していないサイトは未だに多く残されている．加えてブラウザ主導の Renegotiation 機能は DoS 攻撃を誘発することが知られており，ユーザフレンドリな攻撃ツールの存在も確認されている．また 2012 年 8 月にマイクロソフトが公開した 1024 ビット未満の証明書を受け入れない対策や同年 11 月には NISC により電子政府システムにおいてより安全な RSA2048 への移行スケジュールが改定・明確化されたこと等に見られるように 1024 ビット以下の RSA 鍵は利用すべきでないという共通認識が広まりつつある．さらに 2012 年 11 月には圧縮機能における辞書長の違いから平文を推測する CRIME 攻撃も公開されており，今後も新しい手法を用いた攻撃が登場することが予想される．このように SSL/TLS サーバの運用においては考慮すべき対策が存在する．上記脆弱性の対策状況について 2012 年度と 2013 年度に SSLyze を用いてクローリングを行った．本稿にて比較・考察について報告する．

キーワード：SSL/TLS, Renegotiation 機能, CRIME 攻撃, 暗号世代交代, 移行工学

Comparisons and observations of FY2012 and FY2013 about the SSL setting status of web sites in Japan

Yuji Suga[1,a)]

Abstract: In 2009, researchers released details of a vulnerability in the SSL and TLS protocols that could allow Man-in-the-Middle attacks to be carried out. IETF published countermeasures with unprecedented speed as RFC5746, however server-side implementations are not deployed because of problems in business such as the loss of opportunities and backward compatibilities. An efficient DOS attack tool using this vulnerability launched by hacker group. Also, an update that blocks RSA keys less than 1024 bits, which it is recognized should only be used by those understanding the risks involved distributed in August 2012. In November 2012, NISC published a concrete transitioning plan on government systems. Thus measures to be considered are present in the handling of SSL/TLS servers. I went crawling using SSLyze the status of measures above vulnerabilities in 2012 and 2013. This paper shows comparisons and observations.

Keywords: SSL/TLS, Renegotiation function, CRIME attacks, Transitioning of cryptographic algorithms, Transition engineering

1. はじめに

地方自治体および大学のサイトについて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[1][2] の設定状況を把握する先行研究がある [3]．今回，2012 年 5 月に

[1] 株式会社インターネットイニシアティブ
Internet Initiative Japan Inc., Jinbocho Mitsui Bldg. 1-105 Kandajinbo-cho, Chiyoda-ku, Tokyo, 101-0051, Japan
[a)] suga@iij.ad.jp

実施されたクローリングと同じサーバ群に対して対策状況がどのように変化しているのかを把握するために再調査を行った．また 2012 年 11 月に公開された CRIME 攻撃を受け，東証一部・二部上場企業のサイトの対策状況 [4] についてクローリングしている．今回，この対策状況に変化があるかについても調査した．本稿にて 2012 年度と 2013 年度の結果の比較・考察について報告する．

1.1 調査項目

調査項目は以下の 5 点である．

1.1.1 THC-SSL-DOS 対策

ブラウザ主導の Renegotiation 機能は DoS 攻撃を誘発することが知られている [6]．Renegotiation 機能はブラウザ-サーバ間で共有した鍵を再度作り直すことが必要であり，これを何度も繰り返すことでサーバに負荷を与える単純な方法である．DDoS 攻撃のツールも公開されており Anonymous が推奨する DoS ツールのひとつに挙げられていたことが確認されている [7]．

1.1.2 RFC5746 対応

2009 年 11 月に Marsh Ray, Steve Dispensa, Martin Rex によって SSL/TLS プロトコルの脆弱性が公表された [8]．本脆弱性は CVE-2009-3555[9] および JVNVU#120541 で管理されている．SSL/TLS は IP 層とアプリケーション層の間に位置し，アプリケーションデータの暗号化とデータ完全性を保証し，通信相手ノードを X.509 公開鍵証明書に拠り認証する機能を提供する．HTTP, SMTP, POP などのアプリケーション層の通信プロトコルと併用して用いられるため，本脆弱性は多くのアプリケーションやシステムに影響を及ぼすと考えられていた [10]．本脆弱性は実装の問題ではなく，SSL/TLS プロトコル仕様そのものの問題に起因する．TLS 仕様を策定した IETF においてもその認識があり，対策を講じた RFC 化を目指してインターネットドラフトが異例の速さで RFC5746[11] として発行された．根本的な対処方法は問題のある仕様をアップデートし，新仕様にあわせた実装に移行することである．しかし後方互換性を持っていないことによる機会損失を嫌がるためか対応されていないサイトは未だに残されている．

1.1.3 証明書の受け入れ対応

サーバ証明書の主要ブラウザの受け入れ状況，つまりトラストアンカーから証明書が辿れるかについてはユーザに証明書が受け入れられるかどうかという観点において重要である．CommonName の同一性（証明書内に含まれる FQDN と接続サイトの FQDN が同一かどうか），CA リポジトリへの内包性（オレオレ証明書を利用していないかどうか）は，一般ユーザが警告メッセージやブラウザでの鍵マークが出るなどの U/I の変化で知ることができる．

1.1.4 RSA 鍵長

今年 8 月にマイクロソフトが公開した 1024 ビット未満の証明書を受け入れない対策 [12][13] に見られるように，1024 ビット以下の RSA 鍵は利用すべきでないという共通認識が広まりつつある [14][15]．

1.1.5 CRIME 攻撃対策

CRIME 攻撃は Juliano Rizzo, Thai Duong によって Ekoparty security conference [16] にて詳細が公開された．CRIME 攻撃の着目したのは TLS の Compression method である．TLS 仕様としては null つまり圧縮処理をしない値だけを規定している．TLS の Compression method の拡張規定として RFC3749 で定義されているアルゴリズムが DEFLATE(RFC1951) であり，gzip compressor と互換性があり，DEFLATE にはハフマン符号が使われている．このとき，例え同じ長さのデータを圧縮したとしても，圧縮前に同じ文字を含むかどうかで辞書の長さが変わるという事実を用いて攻撃を行い Cookie を搾取するデモが公開されている [17]．対処方法は SSL Compression, SPDY を無効にすることが知られているが，SPDY は SSL と HTTP の間に位置していて Web latency を下げるために圧縮する機能をオプションとして持っており，SSL を利用する際には SSL Compression を利用するため単に無効化できない課題が整理されつつある [18]．

今回 (FY2013) は前回 (FY2012) との比較については前回クローリングした 2012 年 5 月以降に CRIME 攻撃が公開されているため，5 月のクローリング結果ではなく 11 月に行った結果 [4] を比較対象とする．

1.2 サーバのあるべき姿

以上のことから SSL/TLS サーバは下記の状態であることが望ましいと考えられる：

- クライアント主導の Renegotiation を Disable にしている
- RFC5746 に対応している
- ブラウザのトラストアンカーから証明書が辿れる状態である
  - FQDN マッチングが取れている
  - 有効期限が切れていない
- 証明書に含まれる RSA 公開鍵は 2048 ビット以上である
- Compression method を Disable にしている

これらの対策・対応が SSL/TLS サイトにおいて満たされるべき必要条件ではあるが，十分条件ではない．そのほかの項目としては CipherSuites の対応状況や BEAST 攻撃への対策（CBC モード，TLS1.1/1.2 対応）などが挙げられる．これらの項目については今後の課題とする．

1.3 従来の関連調査について

同様の調査としては Web チェック方式 [19][20] が知られており，当該サイトをスコアリングする仕組みが提供

されている．公開鍵暗号で用いられる鍵長だけでなく各 CipherSuites つまり共通鍵暗号で用いられる暗号アルゴリズムの鍵長についての設定状況についても知ることができる．また独自の指標を用いており，それぞれのスコアリング基準に基づいてサイトの点数化が行われている．しかし当該サイトの情報が閲覧できるのみで，全体的に対策がどのくらい進められているかなどの統計的な情報を得ることはできない．

公開鍵証明書の大規模収集という観点では，EFF SSL Observatory[21] や PsQs [22], RwWr[23] 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 [22] 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．

一方で SSL/TLS サーバが受け入れる公開鍵暗号・共通鍵暗号の鍵長について 300 程度のサーバについて調査した結果が公開されている [24]（クローリングに用いられたツールの詳細については不明である）．本稿では，脆弱性報告としては計測が容易で比較しやすい「鍵長」だけにとらわれることなく，総合的な対策が必要であると考え Renegotiation 機能を用いた DoS 攻撃や CRIME 攻撃への対策などより特化した攻撃への対策状況について調査対象としている．

2. 調査方法・調査対象

今回，前節で取り上げた 5 つの脆弱性（弱鍵を利用している状況も一種の脆弱性として捉える）への対処状況について，対策・対応状況について調査した．調査にて OpenSSL ライブラリの上位に位置する Python コード SSLyze[25] ver 0.5 を利用した．その際に CA リポジトリは添付の Mozilla's CA Store では最新の状況に対処していない，日本国内でよく利用される CA が含まれていないことから以下の証明書群を Trust と判定するように修正を行っている．

- VeriSign Class 3 Secure Server CA - G3 [26]
  5d:eb:8f:33:9e:26:4c:19:f6:68:
  6f:5f:8f:32:b5:4a:4c:46:b4:76
- GlobalSign Domain Validation CA - G2 [27]
  2a:3c:f4:bd:dc:74:cc:aa:48:05:
  58:f9:d8:d1:d2:a0:84:f3:4b:31
- VeriSign Class 3 Secure Server 1024-bit CA - G2 [28]
  7c:95:4a:ca:e1:88:1f:03:ad:3a:
  78:ad:5a:f0:65:ab:fd:18:50:77
- RapidSSL CA [29]
  c0:39:a3:26:9e:e4:b8:e8:2d:00:
  c5:3f:a7:97:b5:a1:9e:83:6f:47
- GlobalSign Domain Validation CA [30]
  66:fb:5d:19:e3:fa:e7:cc:47:a2:
  65:82:c4:8a:94:e4:ab:0e:51:1d
- GeoTrust SSL CA [29]
  78:0a:06:f6:e9:b4:06:1c:ad:0c:
  65:02:71:06:06:eb:53:5f:1c:26
- GeoTrust DV SSL CA [29]
  ba:e3:0b:15:db:b1:54:4c:f1:94:
  d0:76:b7:5b:7b:b9:e3:d6:b7:60
- VeriSign International Server CA - Class 3 [31]
  d5:59:a5:86:66:9b:08:f4:6a:30:
  a1:33:f8:a9:ed:3d:03:8e:2e:a8
- AlphaSSL CA - G2 [32]
  58:24:cf:32:c3:cc:2a:47:44:3d:
  b1:0a:33:bb:e3:ac:8d:e5:24:e1
- GlobalSign Organization Validation CA [33]
  37:b4:46:56:16:40:6a:da:1a:
  52:92:08:cc:7b:e0:70:f6:2b:7b:db
  4b:6c:50:2e:01:47:19:ae:5a:80:
  8f:e8:9c:08:28:fd:38:ef:c1:17
- LGPKI Application CA G2 [34]
  96:83:38:f1:13:e3:6a:7b:ab:dd:
  08:f7:77:63:91:a6:87:36:58:2e

2.1 クローリング対象サーバ

調査対象は以下の通りである．都道府県 Web サイトについては SSL サーバの存在性を確認してから調査を行っている．地方自治体及び大学・専門学校のサイトについては HTTP で接続可能なポータルサイトに対してポート番号 443 で SSL 接続して調査を行っている．そのため以下のサイト数は HTTP でアクセス可能なサイトの総数であり，そのすべてにおいて SSL 接続が可能ではないことに注意されたい．なおクローリング作業は 2013 年 9 月 20 日に行った．

- 都道府県 46 サイト
- 地方自治体 3224 サイト [35]
- 大学・専門学校 532 サイト
- 東証一部・二部上場企業 3228 サイト

調査対象としては Alexa Top Sites[36] のようにアクセス数の多いサイトを選択することが考えられる．しかし，本稿では特定分野における傾向が現れることを想定してクローリングを行ったため，上記のサイトを選択している．なお Alexa Top Sites の情報を用いてアジア地域の ccTLD のサーバ群の調査は別の会議 [37] において発表される予定である．

3. 調査結果と考察

3.1 都道府県 Web サイト

前回のクローリング [3] では 2 つのドメインにおいて, SSL 対応のサイトがゼロであったため調査対象は 45 であった. 広報されているメインサイトで SSL 接続ができない場合には同ドメイン配下の別のサーバを利用している. その際には, 特定のサイトを選択することを避けるために Google 検索結果を利用した. 例えば `www.pref.dokka.lg.jp` が SSL に対応していないことを確認した場合, `pref.dokka.lg.jp` と `https` をキーワードにして最も上位に記された SSL サーバをクローリング対象としている.

また, 前回対象となっていたサーバが SSL 接続ができなくなっているケースが見受けられた. そのため FY2012 と FY2013 の比較ができるサイト数は 41 である. 以下集計結果について記載する. 各項目において FY2012 → FY2013 でのサイト数が記されている.

(1) Client-initiated renegotiation

Rejected	32 → 32
Honored	9 → 9

(2) Secure renegotiation supported

Supported	23 → 28
Not supported	18 → 13

(3) RSA key length

2048	21 → 28
1024	20 → 13

3.1.1 考察

クライアント主導の Renegotiation を Disable にしているサイト数に変更は無かったが, 1 サイト Rejected → Honored に設定変更しているサーバが存在している. RFC5746 対応および RSA2048 ビット証明書への移行は改善が見受けられる. 特に RSA2048 への移行状況は約半分の対応だったものが 2/3 程度まで占める結果となった. 一方で RSA1024 ビット証明書の発行元は LGPKI[34] 配下のものが大半を占めていた.

自己署名証明書がサーバ証明書に用いられているサイトは 1 件見つかっている. localdomain 証明書 [4][5]（OpenSSL のデフォルト設定のまま発行された証明書）がテスト用に発行され, その証明書が設定されたまま SSL/TLS が Enable な状態になっていると考えられる.

またブラウザが受け入れる証明書ではあるが FQDN マッチングに失敗するケースが前述の localdomain 証明書を除き 7 件見つかっている. これらの設定ミスは以下 3 種類に分類できる.

[広報されているドメイン名が複数存在] 例 : 地域型 JP ドメイン名と LG.JP ドメイン名を併用しているのに片方の証明書しか存在しない [38]

[ドメイン名は一致するがサーバ FQDN が異なる] 例 : www.hoge.org にて ssl.hoge.org という他サイトの証明書が反応してしまう

[共用サーバでの設定ミス] 例 : IP アドレスを共用しているため証明書に含まれる FQDN が異なる

3.2 地方自治体 Web サイト

前回 SSL 接続できた 1067 サイトから今回 1073 サイトと微増している. 総数が合わない箇所はクローリング時にエラー処理されサーバの状況が判別できなかったサーバが存在することを意味する.

(1) Client-initiated renegotiation

Rejected	623 → 695
Honored	440 → 326

(2) Secure renegotiation supported

Supported	587 → 751
Not supported	476 → 268

(3) RSA key size

4096	2 → 0
2048	676 → 825
1024	383 → 247
512	2 → 1

3.2.1 考察

いずれにおいても改善されていることが分かる. 特に RFC5746 対応の比率は 55%から 73%に上昇しており（アップデート時なども含み）製品への普及が進められた結果が現れている.

一方でブラウザで受け入れない証明書を提示したサイトは 225 件と 20% 以上存在する. そのうち自己署名証明書は約 3/4 にあたる 179 件, localdomain 証明書は約半分の 109 件見つかっている.

3.3 大学・専門学校 Web サイト

前回 SSL 接続できた 344 サイトから今回 376 サイトと 10% 弱増加している. なお調査対象サーバのリストについては前回の報告 [3] に記載されている.

3.3.1 考察

地方自治体 Web サイトの対策状況と同じく, いずれにおいても改善されている. 一方, ブラウザで受け入れない証明書を提示したサイトは 61 件と約 1/6 存在する. うち半数は localdomain 証明書であり, これも地方自治体 Web サイトの対策状況と同じ傾向にある.

鍵長分布において RSA512 ビット証明書が消滅している

(1) Client-initiated renegotiation

Rejected	203 → 262
Honored	141 → 103

(2) Secure renegotiation supported

Supported	197 → 270
Not supported	147 → 95

(3) RSA key size

4096	1 → 2
2048	246 → 323
1024	96 → 51
512	1 → 0

ことが分かる．かつて RSA512 ビット証明書が利用されていたサーバは Web メール用に準備されていた．現在も URL が変更され RSA2048 ビット証明書で運用されていることが確認できた．しかし証明書の中に含まれる FQDN は当該サーバとは異なるものであり，しかもサーバ証明書は自己署名証明書である．ブラウザ・OS に事前に別の手段で安全に証明書ストアに格納する運用がされているかどうかは確認できなかった．

3.4 東証一部・二部上場企業サイト

前回 SSL 接続できた 2235 サイトから今回 2228 サイトとほぼ横ばいであった．結果を表 1 (FY2012) および表 2 (FY2013) に示す．

各業種ごとに以下を満たすサーバ数が列挙されている．

Survey	調査対象全体
SSL	SSL 接続可能
Rej	クライアント主導の Renegotiation を排除
Hon	クライアント主導の Renegotiation を受入
Sup	RFC5746 に対応
nSup	RFC5746 に非対応
Dis	Compression method を Disable
Ena	Compression method を Enable
Tru	ブラウザのトラストアンカーから証明書が辿れる
nTru	ブラウザのトラストアンカーから証明書が辿れない
Self	[nTru] のうち 自己署名証明書
loc	[nTru] のうち localdomain 証明書
exp	[nTru] のうち 有効期限切れ
Mis	[nTru] のうち FQDN マッチングが取れていない
512	RSA512 ビット鍵
1024	RSA1024 ビット鍵
2048	RSA2048 ビット鍵
4096	RSA4096 ビット鍵

3.4.1 考察

CRIME 攻撃対策としては，2012 年 11 月に攻撃手法が公開された直後 820 サイト（36.6 %）が圧縮機能を有効にしていたが，今回は 662 サイト（29．7%）と若干減少していることが分かる．THC-SSL-DOS 対策，RFC5746 対応は大学のサイトと同程度の改善が見られた．ここでとくに特定の業種のサイトに特定の対策が行われた傾向は見られず，全般的に対策が行われていた．一方で証明書の FQDN マッチングと有効期限の問題については業種間で開きがあり，建設・化学・卸売・小売・通信の業種では証明書切れや FQDN ミスマッチが放置される傾向にあり FY2013 も同様である．この傾向は鍵長対策にも若干見受けられる．

鍵長対策については RSA512 ビット証明書が 10 から 1 に激減しており，RSA2048 ビット（以上）証明書への移行は 79.1 % から 89.8 % へと大きな改善が見られた．残り約 1 割の移行が早急に行われることが望まれる．

4. まとめ

地方自治体および大学のサイトについて脆弱性の対策状況についてクローリングした結果，前回 (FY2012) に比べ，THC-SSL-DOS 対策，RFC5746 対応，RSA2048 ビット証明書への移行の全てにおいて改善が見られることが分かった．しかし意図せず SSL 接続も可能にしている設定ミスが一定量（localdomain 証明書が公開されているケースは全体の約 1/12）あることも露呈した．これは，証明書の内容に関する真偽に拠らず，必要ないにも関わらず SSL 接続を許可しているために SSL プロトコル経由 DoS 攻撃を可能にしてしまう状況の方が問題と考えられる．また東証一部・二部上場企業のサイトについて CRIME 攻撃への対策も同時に調査し，緩やかながらも対策が進められていることが判明した．

今後も定期的な定点観測を行うが，調査対象サーバの範囲を拡大するとともに 1.2 節で取り上げられていない他の設定状況についても調査項目として対応していく．特に CipherSuites の対応状況と BEAST 攻撃への対策（CBC モード，TLS1.1/1.2 対応）などを予定している．

参考文献

[1] Alan O. Freier, Philip Karlton, Paul C. Kocher, ”The SSL Protocol Version 3.0”, Internet Draft, November 1996.
[2] Dierks, T. and E. Rescorla, ”The Transport Layer Security (TLS) Protocol Version 1.2”, RFC 5246, August 2008. http://www.ietf.org/rfc/rfc5246.txt
[3] 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).
[4] 須賀, SSL/TLS サイトの脆弱性・弱鍵対策はそのサイトが属する業界に左右されるのか？, 信学技報, vol. 112, no. 315, ICSS2012-56, 2012.
[5] 須賀, SSL/TLS サイトの脆弱性・弱鍵対策はそのサイトが属する業界に左右されるのか？ (2), SCIS2013, 3D4-4, 2013.
[6] THC-SSL-DOS, http://www.thc.org/thc-ssl-dos/
[7] WEAPONS v.0.1, http://pastebin.com/twrDM9kZ

表 1 The Tokyo Stock Exchange companies sites (FY2012)

Category of business	Survey	SSL	Rej	Hon	Sup	nSup	Dis	Ena	Tru	nTru	Self	loc	exp	Mis	512	1024	2048	4096
Construction	216	126	62	61	77	46	77	48	110	15	10	2	1	50	0	26	100	0
Food and Beverages	151	105	55	48	60	43	64	41	95	10	5	1	3	32	0	21	84	0
Chemicals	222	156	79	75	83	71	102	53	128	27	19	8	1	63	1	35	120	0
Metals	101	67	42	22	31	33	43	23	51	15	7	4	1	25	3	10	54	0
Machinery	251	154	77	71	88	60	95	58	125	28	15	8	5	58	1	39	114	0
Electrical Machinery	312	214	116	90	117	89	142	70	190	23	11	4	6	65	0	45	169	0
Transportation	106	72	37	33	41	29	41	30	57	14	7	3	3	29	1	12	59	0
Precision Machinery	53	32	15	13	23	5	20	11	29	2	1	1	0	8	0	2	30	0
Electric and Gas	25	19	7	11	11	7	16	2	18	0	0	0	0	5	0	4	15	0
Communication	367	255	99	146	161	84	149	104	223	31	15	4	13	64	0	66	188	1
Wholesaling	381	267	139	121	144	116	167	99	213	53	24	11	10	104	3	54	208	2
Retail sale	394	291	155	123	149	129	187	103	250	40	26	10	8	105	1	56	233	1
Bank	106	89	39	47	51	35	54	34	87	1	0	0	0	15	0	15	74	0
Insurance	15	9	5	4	4	5	8	1	9	0	0	0	0	2	0	1	8	0
Real Estate	142	97	58	34	49	43	65	31	87	9	4	0	4	22	0	17	80	0
Service	386	282	142	136	147	131	171	112	256	26	13	5	9	88	0	56	226	0
SUM	3228	2235	1127	1035	1236	926	1401	820	1928	294	157	61	64	735	10	459	1762	4

表 2 The Tokyo Stock Exchange companies sites (FY2013)

Category of business	Survey	SSL	Rej	Hon	Sup	nSup	Dis	Ena	Tru	nTru	Self	loc	exp	Mis	512	1024	2048	4096
Construction	216	125	62	59	78	43	93	31	111	13	9	3	0	51	0	10	115	0
Food and Beverages	151	105	54	49	64	39	77	28	95	10	5	1	4	34	0	9	95	1
Chemicals	222	160	65	92	100	57	111	48	132	27	17	8	2	64	1	21	138	0
Metals	101	63	37	25	34	28	45	17	51	11	5	2	2	22	0	3	60	0
Machinery	251	160	70	83	100	53	109	50	132	27	16	7	5	61	0	20	140	0
Electrical Machinery	312	211	104	101	134	71	152	58	194	16	8	2	3	62	0	18	193	0
Transportation	106	70	32	36	46	22	49	20	60	9	6	3	1	27	0	6	64	0
Precision Machinery	53	32	15	15	25	5	25	6	30	1	0	0	0	8	0	1	31	0
Electric and Gas	25	19	8	10	13	5	17	1	18	0	0	0	0	5	0	3	16	0
Communication	366	246	92	149	168	73	170	76	220	25	14	4	10	64	0	27	219	0
Wholesaling	381	266	117	144	172	89	185	80	213	52	22	9	11	100	0	33	232	1
Retail sale	394	290	129	146	173	102	199	90	245	44	29	11	10	101	0	36	253	1
Bank	106	89	33	54	63	24	60	28	86	2	0	0	1	12	0	4	85	0
Insurance	15	9	3	6	5	4	9	0	9	0	0	0	0	2	0	0	9	0
Real Estate	142	95	50	36	50	36	65	28	87	7	4	0	2	23	0	8	87	0
Service	387	288	130	155	183	102	188	101	263	25	14	5	8	93	0	26	262	0
SUM	3228	2228	1001	1160	1408	753	1554	662	1946	269	149	55	59	729	1	225	1999	3

[8] Marsh Ray, Steve Dispensa, "Renegotiating TLS", November 2009. http://extendedsubset.com/Renegotiating_TLS.pdf
[9] CVE-2009-3555, http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3555
[10] Thierry Zoller, TLS & SSLv3 renegotiation vulnerability, http://www.g-sec.lu/practicaltls.pdf
[11] E. Rescorla, M. Ray, S. Dispensa, N. Oskov, Transport Layer Security (TLS) Renegotiation Indication Extension, 2010. http://www.ietf.org/rfc/rfc5746.txt
[12] RSA keys under 1024 bits are blocked http://blogs.technet.com/b/pki/archive/2012/06/12/rsa-keys-under-1024-bits-are-blocked.aspx
[13] Microsoft Security Advisory (2661254), Update For Minimum Certificate Key Length http://technet.microsoft.com/ja-jp/security/advisory/2661254
[14] IIJ, IIR vol.8, Year 2010 Issues on Cryptographic Algorithms, http://www.iij.ad.jp/en/development/iir/pdf/iir_vol08_infra_EN.pdf
[15] Transition Guidelines concerning the Cryptographic Algorithms SHA-1 and RSA1024 Adopted by Government Agencies (in Japanese), http://www.nisc.go.jp/conference/seisaku/dai20/pdf/20siryou0502.pdf
[16] http://www.ekoparty.org/eng/2012/thai-duong.php
[17] http://www.youtube.com/watch?v=gGPhHYyg9r4
[18] B. Kihara, K. Shimizu, Considerations for Protocols with Compression over TLS (work in progress) https://datatracker.ietf.org/doc/draft-kihara-compression-considered-harmful/
[19] Qualys SSL Labs: SSL Server Test, https://www.ssllabs.com/ssltest/index.html
[20] COMODO SSL Analyzer, https://sslanalyzer.comodoca.com/
[21] Electronic Frontier Foundation, The EFF SSL Observatory, https://www.eff.org/observatory
[22] 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.
[23] Arjen K. Lenstra, James P. Hughes, Maxime Augier, Joppe W. Bos, Thorsten Kleinjung, Christophe Wachter "Public Keys", CRYPTO2012.
[24] 独立行政法人情報処理推進機構,「SSL サーバ設定状況等の調査」報告書 http://www.ipa.go.jp/security/fy24/reports/cryptrec/ssl-server/index.html
[25] SSLyze, https://github.com/iSECPartners/sslyze
[26] https://www.verisign.co.jp/repository/intermediate/secureserverCAg3.html
[27] https://www.globalsign.com/support/intermediate/domain_bundle2011.php
[28] https://www.verisign.co.jp/repository/intermediate/2009_secureg21024.html
[29] https://www.geotrust.co.jp/resources/repository/intermediate.html
[30] https://www.globalsign.com/support/intermediate/domainssl_intermediate.php
[31] https://www.verisign.co.jp/repository/intermediate/2009_global.html
[32] http://www.alphassl.com/support/install-root-certificate.html
[33] https://www.globalsign.com/support/intermediate/organizationssl_intermediate.php
[34] https://www.lgpki.jp/CAInfo/fingerprint.htm
[35] National Diet Library, Japan Web Archiving Project, http://warp.da.ndl.go.jp/search/archivesearch/WE00-ToWE09.do
[36] http://www.alexa.com/topsites
[37] 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).
[38] 地域型 JP ドメイン名再構築検討部会, 都道府県の地域型 JP ドメイン名と LG.JP ドメイン名の利用状況調査 http://jprs.jp/geo-wg/2010-06-02/shiryo_e.html