Vol.2018-CSEC-81 No.8
Vol.2018-IOT-41 No.8
2018/5/17

仮想通貨交換業者が提供するWebサイトに関する一考察

須賀 祐治[1,a)]

概要：2017 年 4 月に改正資金決済法が施行され，それまで特に規制のなかった仮想通貨を取り扱う業者に対して登録制が導入され，金融庁から仮想通貨交換業者登録一覧が公開されている．本稿は仮想通貨交換業者登録一覧に記載の各交換業者が消費者向けにサービス提供している Web サーバに着目する．本発表の目的は個々の交換業者の優劣をつけることではなく，仮想通貨を扱う業界全体として「フロントエンドである SSL/TLS サーバ」が消費者にとって安心と安全を与えるサーバ設定になっているかどうかについて調査を行うものである．

キーワード：Virtual Currency Exchanges, 仮想通貨交換業者登録一覧，SSL/TLS, EVSSL 証明書

A consideration about web sites of virtual currency exchanges

Yuji Suga[1,a)]

1. はじめに

2017 年 4 月に改正資金決済法が施行され，それまで特に規制のなかった仮想通貨を取り扱う業者に対して登録制が導入された．2017 年 11 月 1 日に 11 業者が仮想通貨交換業者登録一覧 [1] に掲載され，当時 19 社が継続審査中というステータスであった．その後 12 月 5 日に 15 業者に増加し，さらに 2018 年 1 月 17 日に公開されたリストが執筆時 (2018 年 4 月 10 日) において最新版であり 16 業者が登録されている．金融庁は一定の条件をクリアした「仮想通貨交換業者」のリストを作成して国民に周知することで当該業者にお墨付きを与え，仮想通貨を扱う消費者を保護している．消費者保護の観点では，無登録で仮想通貨交換業を行う業者に対して警告 [2] を行っており，消費者はこれらの情報や注意喚起 [3] からあくまで自己責任で仮想通貨への投資を行う構図となっている．

NEM 流出事件を発端に登録業者 16 業者およびみなし業者 16 業者 [4] に対し立ち入り検査を強化しており，一部の業者に対して業務停止命令・改善命令が発出されている．みなし業者のうちすでに数社は金融庁の提示する条件をクリアできないと判断して登録申請を取り消し廃業に追い込まれていること，上記 32 業者以外にも 100 以上の業者が申請を行っており審査に時間がかかっているなどの報道がなされており「仮想通貨交換業者」リスト更新は先が見えない状況である．リストに列挙されている，いわゆるライセンスは持ってはいるが業務を開始していない業者もあり，それらの業者が他の企業に買収されるなどの報道も見受けられる．消費者にとっては，この業界全体の行方，さらには仮想通貨そのものに対してどのように信頼していくかについて困惑している．

これらの状況のもと，交換業者は自主規制団体を立ち上げ，速やかに金融庁の認定団体として認められるよう自助努力を行っているように見受けられる．業界全体として信頼を獲得していくためのひとつの方策と考えられる．本稿は仮想通貨交換業者登録一覧に記載の各交換業者が消費者向けにサービス提供している Web サーバに着目する．本発表の目的は個々の交換業者の優劣をつけることではなく，仮想通貨を扱う業界全体として「フロントエンドである SSL/TLS サーバ」が消費者にとって安心と安全を与えるサーバ設定になっているかどうかについて調査を行うものである．ただし前述したように仮想通貨交換業者登録一

[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

覧には掲載されており広報用 Web サイトは公開しているが，顧客登録や実サービスを行っていないサイトについては調査対象から除外している．

2. 従来の SSL/TLS 調査の実例

2.1 プロトコル・暗号アルゴリズムの脆弱性

2014 年 10 月に発覚した POODLE 攻撃 [5] 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 [6]．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） [7] 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）[8] 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[9] 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[10] 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．

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 [11] 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 [12] 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．

2.2 検索窓問題

SOUPS2016 [15] 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．

2.3 Mixed Contents エラー

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 [16] [17] [18] [19]．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．

2.4 Alexa top sites における調査事例

(α) Alexa top sites [21] 上位 20000 サイトと，(γ) ある業界の協会における正会員 115 サイトにおける定点観測結果を列挙する [20], [22].

経年変化として危険と認識されているバージョンは排除され，より上位のプロトコルに移行していることが分かる．

以下，リダイレクトについて (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列挙する．

2.4.1 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．

2.4.2 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．

2.5 ある業界のオンラインログインサイトに関する調査

(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（注：広報用サイトとは異なる会員用サイト）については，Top FQDN（広報用サイトの 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報告されている．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．

2016 年 10 月 24 日に調査後，半年で若干の改善が見られる (2017 年 4 月 14 日に再調査) ことがわかるが，ログインサイトでさえ，未だに SSL3.0 に対応したサイトが 3 サイト存在していることが露見している．これはフィーチャーフォンなどのレガシーなデバイスからのアクセスをブロックしてしまうことを機会損出と捉える，つまりリスク受容を行っていると考えられる [22].

2.5.1 EVSSL 証明書の利用

ログインサイトにおいて EVSSL 証明書の利用は全てのケースにおいて対応していたが，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．

2.5.2 サーバ証明書の分布

58 のサーバ証明書のうち発行元を示す CA ベンダーは以下の通りである：

- A 社発行 53
- B 社発行 2
- C 社発行 1
- D 社発行 1
- E 社発行 1

このようにこの業界においては圧倒的なシェアを A 社が握っていることが分かる．この事実は次節に示すようにブ

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	(γ) Top FQDN	(γ) Login 2016-10	(γ) Login 2017-04
SSL2.0	04.3	00.0	00.0
SSL3.0	34.8	13.8	05.2
TLS1.0	100.0	100.0	100.0
TLS1.1	67.0	31.0	43.1
TLS1.2	69.6	62.1	62.1

表 2 ログインサイトにおける SSL/TLS バージョン対応状況

ラウザにおける表記不備問題の影響が大きかった．

2.5.3 証明書不備による表記バグの問題

2017 年 3 月，ブラウザのバグとして取り上げられた問題 [24] 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．2016 年 1 月にサーバ証明書の Policy OID の変更についてアナウンスされ，CA/Browser Forum が OID 指定する 2.23.140.1.1 の利用が始まり，現在は過渡期で発行業者が持つ OID と併記されていることが多い．

今回複数の OID が並んでいるケースにおいてその処理を誤ったことから URL 表記部分が緑色にならないバグが存在していた．前述の 58 サイトにおいて，ある発行ベンダーに集中していたため影響が大きかった．58 のうち 53 サイトが問題が発生していたベンダーであり，そのうち 25 サイトで不備が起こっていた．一部のサイトでは複数の組織の個別サイトがアウトソースされていた．最大で 45 組織の個別サイトがアウトソースされていたことからも依頼者側でも留意すべきであった事例である．これは，証明書ベンダーから再発行も可能とのアナウンスをなされていたが 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い依頼者・サーバ管理者が多かったことも示している．

2.5.4 Mixed Contents エラーなど軽微な設計ミス

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．

3. 仮想通貨交換業者サイトの調査

調査対象となるサーバ群は一般的なサイト構成に基づき，1 業者に対して以下の 3 種類サイトを取り扱う

- 広報用サイト（例：http://www.vircurr.jp/）
- 口座開設サイト（例：http://account.vircurr.jp/）
- ログインサイト（例：http://login.vircurr.jp/）

本稿では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もたせるために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 LabsSSL [25] を利用する．本稿は 12 月 6 日から 7 日に得たデータに基いて報告する．

3.1 総合評価

図 1 に SSL Server Test における総合評価結果を示す．ランク付けの方針は SSL Server Rating Guide [26] 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．

横軸は仮想通貨交換業者登録一覧 [1] に記載の 16 業者を任意に並べており，それぞれの業者において 3 種類のサイトを調査している．灰色の箇所は当該サイトが存在しないことを意味する．また矢印やセル統合されている箇所は異なる用途を同じ FQDN で運用されていることを示している．ランク付けの主要因は以下の節で事例紹介を行う．

3.2 評価下落の主要因

図 2 はランク下落要因を示している．詳細は以下の通りである：

- FS(Forward Secrecy) 未対応 (A-ランク)
- DES3 利用 (B ランク)
- RC4 利用 (B ランク)
- DH1024 利用 (B ランク)
- SSL3.0 利用 (C ランク)
- 56 ビット暗号利用 (F ランク)

一部のサイトで脆弱な暗号アルゴリズムやプロトコルバージョンを利用されていることが分かる．特に 56 ビット暗号は Export-grade（輸出可能な弱い）暗号としても知られており 2015 年 3 月に公開された FREAK Attack [27] 等を誘発することが知られており即座に利用停止すべき暗号アルゴリズムであると認識されている．

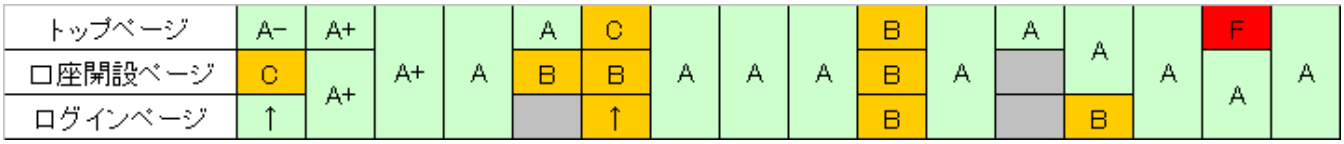

図 1　総合評価

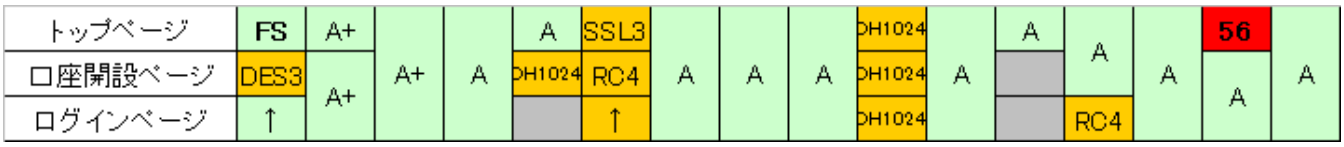

図 2　評価下落の主要因

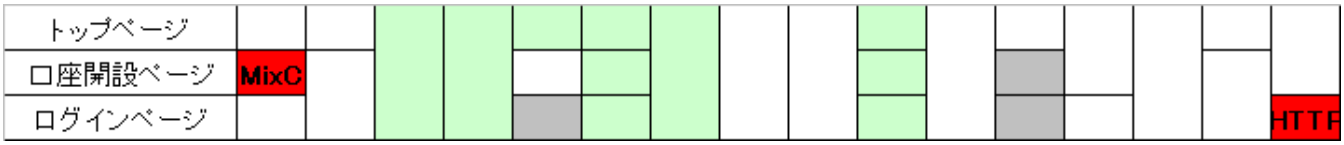

図 3　コンテンツ不備

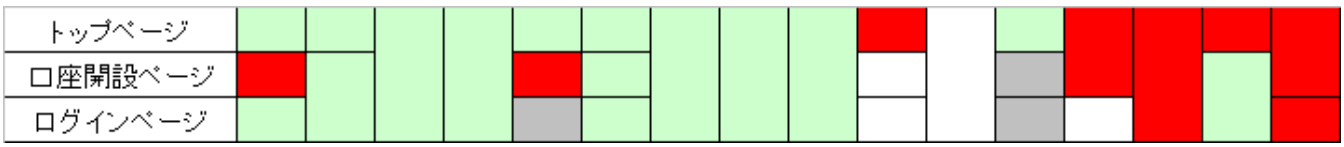

図 4　リダイレクト不備

これらの古い暗号アルゴリズムやプロトコルバージョンを利用しているサイトは，総じて新規参入ではなく既存システムで仮想通貨を扱おうとしている「老舗」サイトで多く見受けられた．これは利用機材の古さや，機会損出防止のため広めに拾いがちという思想に基いているためと推測できる．

3.3 コンテンツ不備

図 3 はコンテンツ不備の有無を示している．1 サイトで Mixed Contents エラーが検出されているが，favicon 画像が HTTP でリンクされている事例であり軽微な修正で済むことが分かる．また 1 サイトで HTTPS ではなく HTTP でログインサイトが運用されている事例が見られた．これは本稿執筆時（2018 年 4 月 10 日）においても修正が行われておらず，当該サイトの利用者は意図せずユーザ ID 及びパスワードが流出する危険性が存在したままとなっている．

3.4 リダイレクト不備

図 4 にて HTTP でアクセスした場合の挙動について示す．薄緑色の箇所は HTTP → HTTPS に正しくリダイレクトされており正しい挙動がなされていると言える．白色の箇所はそもそも HTTP サーバが運用されておらず，これも正しい運用形態であるとも捉えられる．

一方で赤色の箇所は HTTPS と同コンテンツを HTTP で提供していることを示している．必ずしも対処すべきではないが，HTTP と HTTPS の両方でコンテンツ管理を行う際にミスが発生する可能性をはらんでいるとも捉えることができる．前節で示した HTTP でサーバでログインページが提供されている事例がそのミスの一つであり，HTTP → HTTPS リダイレクトの設定を行っていれば防げた事例でもある．

4. 今後について

今回，仮想通貨を扱う業界全体として「フロントエンドである SSL/TLS サーバ」が消費者にとって安心と安全を与えるサーバ設定になっているかどうかについて調査を行った．概ね良い結果が得られているが軽微なミスで本来提供すべき安全なサービスが行われていない事例も見受けられた．現在みなし業者の扱いについて混沌としているため調査対象から外しているが，業界全体としてセキュリティ対応の底上げを行って頂くために，より広くかつ継続的な調査を行う予定である．

消費者視点としては安全に取引できる仮想通貨のリストが欲しいのではないだろうか．これは暗号アルゴリズムに対して CRYPTREC 暗号リストと同様のものである．仮想通貨交換業者登録一覧にはお墨付きを与えた業者一覧とともに，それぞれの交換業者が取り扱う仮想通貨もリストされているが，果たしてそれらの通貨は安全であると認識してよいかどうかは消費者にも分からず，さらなる混乱を与えてしまっているのではないかと危惧している．今後の動向に注力したい．

参考文献

[1] 金融庁, 仮想通貨交換業者登録一覧, https://www.fsa.go.jp/menkyo/menkyoj/kasoutuka.pdf
[2] 金融庁, 無登録で仮想通貨交換業を行う者の名称等について, https://www.fsa.go.jp/policy/virtual_currency/kasoutuka_mutouroku.pdf
[3] 金融庁, 仮想通貨の利用者のみなさまへ, https://www.fsa.go.jp/policy/virtual_currency/index.html
[4] 金融庁, コインチェック株式会社に対する立入検査の着手及び仮想通貨交換業者に対する報告徴求命令の発出について, https://www.fsa.go.jp/policy/virtual_currency/09.pdf
[5] Bodo Möller, Thai Duong, Krzysztof Kotowicz, "This POODLE Bites: Exploiting The SSL 3.0 Fallback", https://www.openssl.org/~bodo/ssl-poodle.pdf
[6] RFC7568: Deprecating Secure Sockets Layer Version 3.0, https://datatracker.ietf.org/doc/rfc7568/
[7] RFC2246: The TLS Protocol Version 1.0http://www.ietf.org/rfc/rfc2246.txt
[8] RFC5116: An Interface and Algorithms for Authenticated Encryption, https://datatracker.ietf.org/doc/rfc5116/
[9] RFC7457: Summarizing Known Attacks on Transport Layer Security (TLS) and Datagram TLS (DTLS), https://datatracker.ietf.org/doc/rfc7457/
[10] CELLOS consortium, Publication, https://www.cellos-consortium.org/index.php?Publication
[11] 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/
[12] The DROWN Attack, https://drownattack.com/
[13] 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
[14] 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/
[15] 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
[16] https://blog.mozilla.org/tanvi/2013/04/10/mixed-content-blocking-enabled-in-firefox-23/
[17] https://support.mozilla.org/ja/kb/mixed-content- blocking-firefox
[18] https://developers.google.com/web/fundamentals/security/prevent-mixed-content/what-is-mixed-content
[19] https://developers.google.com/web/fundamentals/security/prevent-mixed-content/fixing-mixed-content
[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] Yuji Suga, Browser's "search form" issues and countermeasures, 19th Asia-Pacific Network Operations and Management Symposium (APNOMS2017), 358-361, 2017
[23] EV SSL サーバ証明書の Policy OID の変更について, 2016 年 1 月, 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
[24] 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, 2017 年 3 月, 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
[25] Qualys SSL LabsSSL, SSL Server Test, https://www.ssllabs.com/ssltest/
[26] Qualys SSL LabsSSL, SSL Server Rating Guidehttps://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide
[27] CELLOS consortium, SSL/TLS への弱い暗号を利用した FREAK Attack について, https://www.cellos-consortium.org/jp/index.php?FreakAttack_20150304_J