3E-3

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

須賀 祐治 *
株式会社インターネットイニシアティブ

あらまし 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．THC-SSL-DOS対策，RFC5746対応，証明書の受け入れ対応，RSA鍵長，CRIME攻撃対策の5つに対する対策状況について設定状況を把握する先行研究がある．今回，最新の状況を把握し，地理的・業種別リージョンごとの統計情報を可視化する方式について提案する．特にサーバ証明書の鍵長，公開鍵使いまわし問題，FQDNミスマッチ，有効期限切れや自己署名証明書の利用などについて把握できるツールを実装したので報告する．

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

1 はじめに

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[1]．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[2]．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[3]．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[4]も公開されており，今後も様々なセキュアプロトコルに対して新たな攻撃手法が登場することが予想される．

1.1 サーバのあるべき姿

上記脆弱性の対策状況を鑑み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
- RFC5746に対応
- ブラウザのトラストアンカーから証明書が辿れる
  - 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
- Compression methodをDisable

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以外の暗号モード利用，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であり，現在準備中である．

2 可視化方法の提案

大局的（マクロ）もしくは局所的（ミクロ）な表現の両方を行えることを目指す．前者のマクロ的表現とは地域や業種など同じ属性を持つサイト群の状況について統計情報のみを示すことを意味する．一方でミクロ的表現は各サイト個々のサイト設定状況について表現することである．

2.1 可視化の目的

本稿にて可視化を行う大きな目的はサーバ管理者への情報提供である．他サイトと比較して自サイトの対応状況についてランク付けを行うことで対策の進度を知ることができる．同様の先行事例としてWebチェック方式[6]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．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．また平均的な対策がどの程度であるかについての指標が無く，移行が妥当であるかどうかの判断基準（例えば，現在稼働しているサーバをストップしてでも対策すべき問題であるかの判断基準）が分からないという課題もある．

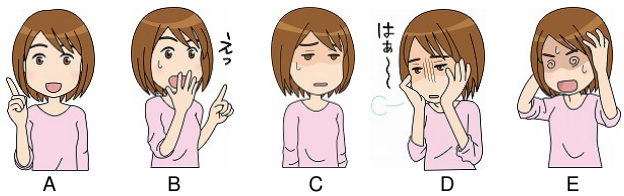

図 1: サーバの状態に関する平易な表現例

このように「横並び意識」を利用することでサーバ設定の見直しと安全な状況への速やかな移行を促すきっか

* Visualization of SSL setting status in Japan such as the FQDN mismatch, Yuji SUGA, Internet Initiative Japan Inc., Jinbocho Mitsui Bldg. 1-105 Kandajinbo-cho, suga@iij.ad.jp

けとなれば幸いである．実際，特定地域のサーバ群の対策状況を情報政策を司る部署に連絡することで，問題が解決した事例も存在する [5]．このとき実際に提示した数値やログなどは詳細に精査されなかった．そこで図 1 のように平易な表現を用いる方法を採ることが必要であると考え，今回利用している．詳細な情報よりも直感的な表現で伝達した方が通知側・被通知側ともにメリットが大きい．

2.2 可視化の対象データ

1 章で示した脆弱性の対策状況について，地方自治体，大学および東証一部・二部上場企業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 の設定状況を把握する先行研究がある [5, 7]．さらにアジア地域に範囲を拡げて調査されている [8]．本稿はこれらのデータを利用して可視化を行う．

2.3 マクロ的表現

アジア地域に範囲を拡げて調査した結果 [8] を用いてマクロ的表現を行う方法を検討した．今回スマートフォンの AR アプリケーションを通して状況を確認する手法を採用している．アジア地域の地図に国旗を併記しておき，図 2 のように，その国旗をスマートフォン越しに閲覧することで，その国に属する ccTLD を持つサーバ群の対応状況を知ることができる．

図 2: 国旗にかざした際の表示例

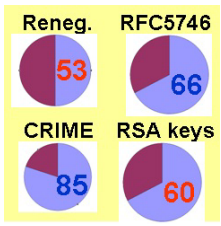

図 3: サーバ群の大局的な状態の表示例

サーバ群の対応状況は，図 3 のように各項目に対して対策進度を円グラフで表現した．他国と比較して対策が進んでいることを青色の数字で，進んでいないことを赤色の数字で，対策されているサーバの割合を示し，対策の進度を容易に確認することを可能にした．

2.4 ミクロ的表現

前節のマクロ表現とは異なり，各サイトの対策状況 [5, 7] を示す際の方法を検討する．以下の項目に基づいて各サイトの脆弱性にポイント付けを行い，加算したポイントについて表 1 における A(0),B(1-2),C(3-4),D(5-7),E(8-) にランク付けする方式を採用した．

1	圧縮機能が有効 (CRIME 攻撃の対策なし) RFC5746 不対応 クライアント主導の Renegotiation が有効
2	1024 ビット以下の RSA 鍵を利用 FQDN マッチングが取れていない 証明書の有効期限切れ
4	サーバ証明書が自己署名証明書
8	他サイトと秘密鍵を共有

表 1: 各脆弱性のスコアリング

図 4 は地方自治体サイトの状況について実際に地図上に配置したものである．容易にその地域のサイトがどのような状況であるかを把握することが可能である．

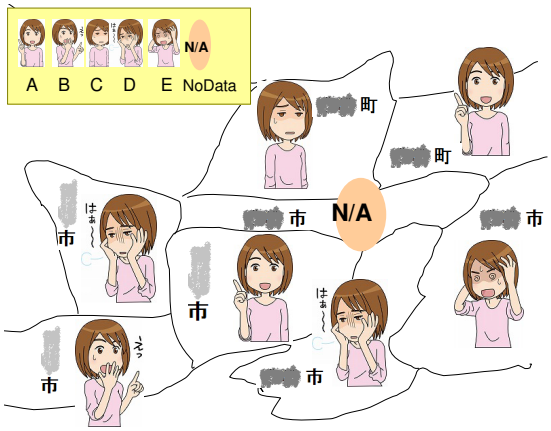

図 4: 実際の地図への配置例

参考文献

[1] E. Rescorla, M. Ray, S. Dispensa, N. Oskov, Transport Layer Security (TLS) Renegotiation Indication Extension, 2010. http://www.ietf.org/rfc/rfc5746.txt

[2] THC-SSL-DOS, http://www.thc.org/thc-ssl-dos/

[3] IIJ, IIR vol.8, Year 2010 Issues on Cryptographic Algorithms, http://www.iij.ad.jp/en/development/iir/pdf/iir_vol08_infra_EN.pdf

[4] http://www.ekoparty.org/eng/2012/thai-duong.php

[5] Y. 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).

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

[7] 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.

[8] 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).