L-034

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

SSL/TLS servers status survey against down-grade attacks with export-grade cipher algorithm

須賀 祐治 *
Yuji SUGA

あらまし 2015 年 3 月および 5 月に暗号アルゴリズムの輸出規制があった時代に規定されていた Export-grade（輸出可能な弱い）暗号アルゴリズムを使わせる中間者攻撃が立て続けに発表された．本稿ではこれらの攻撃に対するサーバ側の対処状況について報告する．

キーワード SSL/TLS, 暗号輸出規制, 中間者攻撃, FREAK 攻撃, Logjam 攻撃, OpenSSL

1 調査背景

2015 年 3 月および 5 月に SSL/TLS において中間者攻撃が立て続けに発表された．3 月に公開された FREAK 攻撃 [1] は暗号アルゴリズムの輸出規制があった時代に規定されていた Export-grade（輸出可能な弱い）暗号アルゴリズムを利用させることで，情報を筒抜けにする中間者攻撃である．FREAK 攻撃の概要を図 1 に示す．

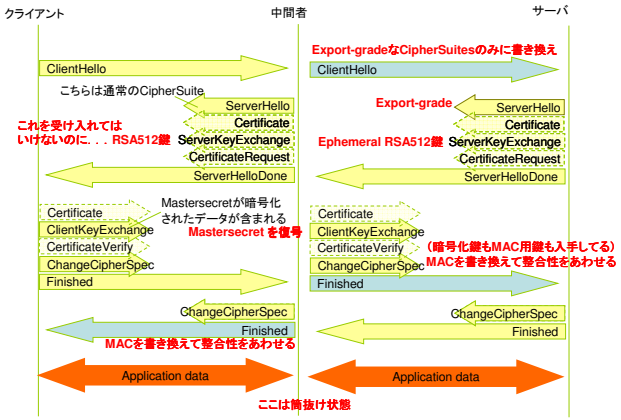

図 1: FREAK 攻撃のメッセージフロー概要

本攻撃は SSL/TLS のプロトコル仕様の問題ではなく，CVE-2015-0204 の脆弱性を持つクライアント製品を利用する場合，かつ，サーバ側に Export-grade 暗号を利用している場合にのみ成立する．この観点においては，サーバ側の暗号設定対策，具体的には Export-grade 暗号を利用しないようにすることで防ぐことができた．そのため，サーバ設定の不備に関するサーベイサイト [2] が登場し，ブラックリストのように扱われたことからサーバ設定の見直しが行われた．約 15 年前の輸出規制時代の CipherSuites をサポートすることは後方互換性の確保のため，という理由にはならないと考えられたことも移行を後押ししたと考えられる．

FREAK 攻撃では RSA512 ビット鍵をサーバ・クライントに意図せず使わせることで情報を筒抜けにする攻撃であった．一方で 5 月に改めて問題が指摘された Logjam 攻撃 [3] は DH 鍵に対する同様の問題に起因している．これもサーバ設定の不備として分類することもできるが Non Export-grade 暗号を利用しているケースでも 512 ビット程度の素数が利用可能なため仕様上の問題としても認識されている．いずれにせよサーバ設定の問題を解消することでこの問題を回避することができる．

本稿では以上のケースのうち Export-grade 暗号の設定状況の推移について調査した．また POODLE 攻撃に起因して脆弱であると認識されるようになった SSL3.0 仕様の移行状況についての続報も報告する．

2 観測環境とその結果

今回の調査対象は以下の通りである．今回クローリングに際し利用したソースはすべて Alexa [4] 提供のリストから抽出したものである．なお今回のクローリングは 2015 年 6 月 27 日から 28 日にかけて行われたものを集計している．

- Alexa top sites の上位 20000 サイト
- .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

* 株式会社インターネットイニシアティブ，〒 102-0071 東京都千代田区富士見 2-10-2 飯田橋グラン・ブルーム，Internet Initiative Japan Inc., Iidabashi Grand Bloom, 2-10-2 Fujimi, Chiyoda-ku, Tokyo, 102-0071 Japan, suga@iij.ad.jp

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
EXP-RC2-CBC-MD5	756	230	1414	932
EXP-RC4-MD5	802	251	1437	962
EXP-EDH-RSA-DES-CBC-SHA	182	96	1128	779
EXP-EDH-DSS-DES-CBC-SHA	0	0	0	0
EXP-DES-CBC-SHA	771	229	1293	853
EXP-RC2-CBC-MD5	756	230	1414	932
EXP-RC4-MD5	802	251	1437	962
(40 ビット暗号アルゴリズム総計)	808	255	1444	970
DES-CBC-SHA	943	709	2648	2267
DES-CBC-MD5	122	71	682	509
EDH-RSA-DES-CBC-SHA	408	276	2277	1960
(56bits 暗号アルゴリズム総計)	947	711	2648	2268

表 1: 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

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[5] や PsQs [6],RwWr[7] 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 [6] 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．

以上を鑑み，本稿では (α) Alexa top sites 6835 サイト 及び (β) .jp ドメイン 5668 サイトの SSL/TLS サーバ (重複あり) についてクローリング調査を行った．これらのサーバリスト (α), (β) は，2014 年 4 月の Heartbleed bug 発覚時のサーバ設定調査結果 [8] 及び POODLE 攻撃発覚後の調査結果 [9] と同一なリストであり，クロール環境・方式も従来方式に準じている．ただし同じ対象サーバリストを利用しているため，SSL-enable なサイト数は若干減少しており，今回のクローリングにおいては，最終的に SSL-enable サイトは (α) Alexa top sites 6431 サイト，(β) .jp ドメイン 5518 サイトであった．

2.1 Export-grade な暗号アルゴリズムの対応状況

FREAK 攻撃 [1] や Logjam 攻撃 [3] の発表により注意喚起がなされ，一定数のサーバが設定変更を行ったことが見受けられる．しかし依然として表 1 に示すように 40bits/56bits 暗号アルゴリズムが有効なままになったいることが判明した．40bits 暗号アルゴリズムが利用可能なままのサーバが (α) Alexa top sites で 4.0%，(β) .jp ドメイン で 17.6%の割合で残っていることが判明した．

2.2 SSLv3 無効化と TLS への移行状況調査

調査対象は前述の通りである．表の数値は各バージョンの対応比率をパーセンテージをあらわしており，サーバサイドでの SSLv3 無効化と TLS1.1 及び 1.2 への対応が加速していることが分かった．

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

表 2: SSL/TLS バージョン対応状況 - (α) .jp ドメイン

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

表 3: SSL/TLS バージョン対応状況 - (β) Alexa top sites

参考文献

[1] https://freakattack.com

[2] https://freakattack.com/vulnerable.txt

[3] https://weakdh.org

[4] http://www.alexa.com/topsites

[5] Electronic Frontier Foundation, The EFF SSL Observatory, https://www.eff.org/observatory

[6] 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.

[7] Arjen K. Lenstra, James P. Hughes, Maxime Augier, Joppe W. Bos, Thorsten Kleinjung, Christophe Wachter "Public Keys", CRYPTO2012.

[8] 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.

[9] 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.