現在利用されている SSL/TLS 通信の危険性についての調査

山田　道洋

明治大学総合数理学部先端メディアサイエンス学科

1　はじめに

近年，インターネット上でのクレジットカードを利用した買い物や，個人情報の入力が行われる機会が非常に増えている．こういった重要な情報の通信を行う際に通信を暗号化するために SSL/TLS 証明書が利用されている．

しかし，古い仕様である SSL3.0 の BC モードにおいて暗号化通信が解読されてしまう中間者攻撃“POODLE Attack”の脆弱性が指摘されている[1]．

加えて、SHA-1 アルゴリズムによって署名をされた TLS 証明書は中間者攻撃などを実行される危険性があるとして，Microsoft 社は 2016 年 1 月 1 日以降の SHA-1 による署名の証明書の発行の停止と，2017 年 1 月 1 日以降には SHA-1 による署名の証明書での TLS 通信を Windows クライアントで拒否することを決定した[2][3]．

そこで，本研究では，現在利用されている SSL/TLS 通信のリスクを評価するために，2015 年 11 月 29 日～12 月 3 日に利用されている SSL/TLS を用いた WEB サイトについて調査した結果を報告する．

2　実験

2.1　データ収集方法

Google にて“https://”をキーワードに検索を行い，検索された上位 100 サイトを対象に，Google Chrome を利用して，証明書情報を記録した．

2.2　データ形式

データに含まれる要素は，URL，サイト運営者の業種，署名アルゴリズム，SSL/TLS のバージョン，暗号化モード，有効期限の開始日，有効期限の終了日，証明書の発行者である．署名アルゴリズムは証明書作成時に利用されたアルゴリズム，業種はサイト運営者の業務内容などから日本標準産業分類［4］を参考に分類した．

2.3　調査結果

各業種の署名アルゴリズムの件数を表 1 に示す．運送業では 6 つの証明書の内 5 つが SHA1 を使用しているが，そのうち 3 つは JR 系列の会社が運営しているサイトであった．

表 1 業種と署名アルゴリズムの件数

業種	SHA1	SHA256	総計	業種内SHA1
通信	5	31	36	14%
サービス	4	20	24	17%
小売り	4	7	11	36%
運送	5	1	6	83%
飲食	1	4	5	20%
公務	0	3	3	0%
宿泊	0	3	3	0%
装飾	1	1	2	50%
福祉	1	1	2	50%
医療	0	2	2	0%
教育	0	2	2	0%
金融	0	2	2	0%
製造	0	2	2	0%
総計	**21**	**79**	**100**	**21%**

発行認証局と署名アルゴリズムの件数を表 2 に示す．VerySign 社の発行数が最も多く，SHA1 証明書の割合も最も高い．

表 2　証明書発行認証局と署名アルゴリズムの件数

認証局	SHA1	SHA256	総計	SHA1割合
VeriSign	16	22	38	42%
GeoTrust	1	19	20	5%
GlobalSign	0	18	18	0%
CyberTrust	3	5	8	38%
DigiCert	0	5	5	0%
AddTrust	0	3	3	0%
Security Communication	1	2	3	33%
Starfield	0	2	2	0%
Go Daddy	0	1	1	0%
RapidSSL	0	1	1	0%
thawte	0	1	1	0%
総計	**21**	**79**	**100**	**21%**

SHA1 証明書の発行年と期限終了年の件数を表 3 に示す．Windows で SHA-1 署名を利用した証明書の利用が禁止される 2017 年中も有効な証明書が 2 つ確認された．しかし，2013 年に発行された証明書の発行日は，Microsoft のルート証明書についてのポリシーの変更を発表した 2013 年 11 月よりも以前のものであった．また，2016 年までの利用の証明書も含め，ポリシー変更後の 2014 年にも SHA-1 署名による証明書が 16 件発行

“Investigation into about the risk SSL/TLS communication used now”
Michihiro Yamada
Department of Frontier Media Science, Faculty of Interdisciplinary Mathematic Science , Meiji University

されていることも確認された.

表 3　SHA-1 署名による証明書有効期限開始年と終了年の件数

開始年/終了年	2015年	2016年	2017年	総計
2013年	2	2	1	5
2014年	2	3	1	6
2015年	0	10	0	10
総計	**4**	**15**	**2**	**21**

SSL/TLS 通信の通信方式と暗号化の利用モードの件数を表 4 に示す. 本調査対象とした 100 サイトでは, SSL 方式での通信は行われておらず, TLS 方式での通信を利用しているため, “Poodle Attack”に対する脆弱性は存在しない.

表 4　通信方式と暗号化モードの件数

利用モード	TLS1.0	1	2	総計
CBC	12	1	27	40
GCM	1	0	59	60
総計	**13**	**1**	**86**	**100**

3　おわりに

本調査では, VerySign 社の SHA1 による署名の証明書の発行数が多いことが示された. しかし, データ数が小さかったため, 業種による区分での有用なデータを得ることはできなかった. これはデータの収集を手動で行ったがゆえの問題である. このため, データの収集の自動化によるデータサイズの拡大を検討中である.

参考資料

[1] Bodo Möller, Thai Duong, Krzysztof Kotowicz
“This POODLE Bites: Exploiting The SSL 3.0 Fallback” Google September 2014
[2]Microsoft TechNet マイクロソフト セキュリティ アドバイザリ 2880823
(https://technet.microsoft.com/ja-jp/library/security/2880823.aspx
/2015-12-21 参照)
[3]Microsoft TechNet Windows Enforcement of Authenticode Code Signing and Timestamping
(http://social.technet.microsoft.com/wiki/contents/articles/32288.windows-enforcement-of-authenticode-code-signing-and-timestamping.aspx
/2015-12-21 参照)
[4]総務省　日本標準産業分類（平成 25 年 10 月改定）（平成 26 年 4 月 1 日施行）
(http://www.soumu.go.jp/toukei_toukatsu/index/seido/sangyo/02toukatsu01_03000022.html
/2015-11-29 参照)