都市銀行におけるSSL/TLSサーバの暗号アルゴリズム設定状況調査

米澤 祥子[1]　菅野 哲[1]

概要：近年、RC4 や SHA-1 等の暗号アルゴリズムが危殆化し、米 NIST や日本 CRYPTREC では安全性に問題のある暗号アルゴリズムを使用しないよう勧告している。大手ブラウザベンダーは SHA-1 を使用したサーバ証明書の取扱いを 2017 年内に停止することを発表しており（暗号の 2017 年問題）、SSL/TLS 通信を扱うサービスにも対応が求められる。本稿では、日本国内の都市銀行においてインターネットバンキングで利用されている SSL/TLS サーバの設定状況を調査し、安全性を満たす設定がされているかを調査する。さらに、SSL/TLS サーバの適切な設定方法に関する提言も行う。

キーワード：SSL/TLS, 暗号アルゴリズム, 危殆化, SHA-1

Settings for Cryptographic Algorithms on SSL/TLS servers of Major Banks

Shoko YONEZAWA[1]　Satoru KANNO[1]

Abstract: Cryptographic algorithms such as RC4 and SHA-1 are compromised these days. NIST, CRYPTREC and other national organizations advise to stop using such vulnerable algorithms. Major browser vendors announced that they stop supporting server certificates using SHA-1, which requires web services using SSL/TLS connections to adapt such settings. In this paper, we check the settings of SSL/TLS servers in online banking services of main banks in Japan and examine the adaptation for the secure settings. Futhermore, we propose the appropriate settings for SSL/TLS servers.

Keywords: SSL/TLS, cryptographic algorithms, compromise, SHA-1

1. はじめに

今日、インターネットは我々の生活にとって必要不可欠なものとなっている。それに伴い、インターネットの安全性についても注目が集まっている。インターネットの安全性を確保する方法として SSL/TLS と呼ばれる通信プロトコルが存在する。SSL は Netscape によって開発された通信プロトコルで、IETF (Internet Engineering Task Force) での標準化に伴い TLS と名称変更された。TLS は 1999 年に Version 1.0 [1]、2006 年に Version 1.1 [2]、2008 年に Version 1.2 [3] が公開され、現在 Version 1.3 の策定が進められている [4]。従来 SSL/TLS はクレジットカード情報などの個人情報を送信する際に利用されていたが、最近は Google が「HTTPS Everywhere」を掲げるなど、常時 SSL/TLS 化 (Always on SSL/TLS) の流れができている。このような動きは、インターネットにおいて SSL/TLS が重要な基盤となっていることを表している。

SSL/TLS 通信での安全性を担保するために、RFC においてさまざまな暗号アルゴリズムが規定されているが、近年数々の暗号アルゴリズムが危殆化している。米国の NIST (National Institute of Standards and Technology) では、等価安全性の文脈において 112bit 以下の安全性を有する暗号アルゴリズムを廃止する流れとなっている。また日本においても、NISC（内閣サイバーセキュリティセンター）

[1] 株式会社レピダム
Lepidum Co. Ltd.

や CRYPTREC において、安全性の低い暗号アルゴリズムから安全性の高い暗号アルゴリズムへの移行指針が示されている。また、Google, Microsoft, Mozilla 等の大手ブラウザベンダーは、2017 年中に SHA-1 を用いて発行された証明書を無効にする方針を発表している（暗号の 2017 年問題）。しかし、現在公開されている Web サイトの中には、ユーザの観点から高い安全性が要求されるサイトであっても、SSL/TLS において安全性に問題のある設定を採用しているものが多く見受けられる。

本稿では、高い安全性が要求されると期待される銀行の Web サイトに対し、SSL/TLS サーバの設定状況を調査しその安全性を考察する。本稿ではまず、SSL/TLS の推奨設定の調査結果を示す。次に、金融機関に対するセキュリティガイドラインを調査し、暗号アルゴリズムや SSL/TLS の設定に関する基準を確認する。さらに、都市銀行のインターネットバンキングサイトにおける SSL/TLS サーバの設定状況を調査し、推奨設定を満たしているかどうかを確認する。最後に、SSL/TLS の安全性を高めるための考察を行う。

2. SSL/TLS の推奨設定

本章では、各種組織において公開されている SSL/TLS の推奨設定を示す。

2.1 IETF

IETF では Best Current Practice (BCP) が公開されており、安全性の観点で推奨される SSL/TLS のプロトコルバージョンや暗号アルゴリズムが記載されている [5]。

BCP において、暗号アルゴリズムおよび SSL/TLS の利用について以下の内容が示されている。

SSL/TLS のプロトコルバージョン

- SSL 2.0 と SSL 3.0 の使用禁止
- TLS 1.0 の非推奨
- TLS 1.1 は基本的に非推奨で、上位バージョンが使えないときのみ使用許可
- TLS 1.2 のサポート必須
- 上位バージョンが非対応で接続できるバージョンまで変更する場合 (fallback)、SSL 3.0 より前のバージョンの使用禁止

暗号アルゴリズム

- RC4 の使用禁止
- 112bit 安全性より弱い暗号スイートの使用禁止（export-level encryption を含む）
- 128bit 安全性より弱い暗号スイートの非推奨
- static RSA の非推奨（Forward Secrecy を満たさないため）
- Forward secrecy を満たす暗号スイート（DHE や ECDHE など）のサポートと利用必須
- SHA-256 の使用推奨
- Trancated HMAC extension の使用禁止
- 2048bit 以上 DH 鍵の使用推奨
- 192bit 未満 ECDH 鍵の使用禁止
- 2048bit 以上 RSA 鍵の使用推奨

以上を踏まえて、以下の暗号スイートの使用が推奨されている。

- `TLS_DHE_RSA_WITH_AES_128_GCM_SHA256`
- `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`
- `TLS_DHE_RSA_WITH_AES_256_GCM_SHA384`
- `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`

2.2 CRYPTREC

CRYPTREC により作成され IPA から発行された「SSL/TLS 暗号設定ガイドライン Ver.1.1」 [6] において、SSL/TLS の推奨設定が公開されている。本ガイドラインでは、要求設定項目として「高セキュリティ型」「推奨セキュリティ型」「セキュリティ例外型」の 3 つの設定基準を提示し、それぞれの要求を満たす SSL/TLS のプロトコルバージョンや暗号アルゴリズムを示している。本ガイドラインにおいて金融サービスは「推奨セキュリティ型」の利用例として挙げられている。

2.2.1 高セキュリティ型

「高セキュリティ型」の設定基準において、SSL/TLS のプロトコルバージョンは以下の設定が推奨されている。

- TLS1.2 を設定有効にする
- TLS1.1 以前を設定無効（利用不可）にする

利用する暗号アルゴリズムについては以下の条件が要求されている。

- CRYPTREC 暗号リストに掲載されているアルゴリズムのみで構成される
- 暗号化として 128bit 安全性以上を有する
- 安全性向上への寄与が高いと期待されることから、認証付暗号利用モードを採用する
- Perfect Forward Secrecy の特性を満たす [*1]
- DSA を含む暗号スイートは選定しない

以上を踏まえて、本ガイドラインでは以下の暗号スイートの利用が推奨されている。暗号スイートのグループのうち、グループ α は 256bit 安全性を有する暗号スイート、グループ β は 128bit 安全性を有する暗号スイートであり、より安全性の高いグループ α を優先して設定するよう推奨されている。

グループ α

- `TLS_DHE_RSA_WITH_AES_256_GCM_SHA384`
- `TLS_DHE_RSA_WITH_CAMELLIA_256_GCM_SHA384`

[*1] [6] の文脈における Perfect Forward Secrecy は [5] の文脈における Forward Secrecy と同等であるが、[6] にて Perfect Forward Secrecy で統一されているため、本稿でも採用した。

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384

グループ β

- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_CAMELLIA_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256

ここで、DHE の鍵長は 2048bit 以上、ECDHE の鍵長は 256bit 以上を必須とする。

なお、本ガイドラインにおいて、 ECDSA を採用する際にはパテントリスクの存在を考慮するよう求められているが、ECDSA の特許は 2017 年 4 月 18 日に有効期限が切れていることに注意したい [7]。

2.2.2 推奨セキュリティ型

「推奨セキュリティ型」の設定基準において、SSL/TLS のプロトコルバージョンは以下の設定が推奨されている。

- SSL3.0 及び SSL2.0 を設定無効（利用不可）にする
- TLS1.1 及び TLS1.2 については、実装されているのであれば設定有効にする
- プロトコルバージョンの優先順位が設定できる場合には、設定有効になっているプロトコルバージョンのうち、最も新しいバージョンによる接続を最優先とし、接続できない場合に順番に一つずつ前のプロトコルバージョンで接続するように設定することが望ましい

利用する暗号アルゴリズムについては以下の条件が要求されている。

- CRYPTREC 暗号リストに掲載されているアルゴリズムのみで構成される
- 暗号化として 128bit 安全性以上を有する
- DSA を含む暗号スイートは選定しない

以上を踏まえて、本ガイドラインでは以下の暗号スイートの利用が推奨されている。暗号スイートは、安全性と実用性とのバランスでグループ A からグループ F まで分けられており、グループ C 以降の暗号スイートは選択しなくてもよいこととされている。以下に、グループ A およびグループ B に含まれる暗号スイートを示す。

グループ **A**

- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_CAMELLIA_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

グループ **B**

- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA

ここで、DHE の鍵長は 1024bit 以上、RSA の鍵長は 2048bit 以上、ECDHE の鍵長は 256bit 以上を必須とする。

「高セキュリティ型」と同様、「推奨セキュリティ型」においても ECDSA を採用する際のパテントリスクの存在が指摘されている。

3. 金融機関におけるセキュリティ基準

本章では、銀行に対して策定されているセキュリティ基準において、SSL/TLS のプロトコルバージョンおよび暗号アルゴリズムの推奨設定を調査する。銀行に対するセキュリティ基準として、財団法人金融情報システムセンター (FISC) による基準（FISC ガイドライン）を取り扱う。また比較のため、同じ金融機関向けセキュリティ基準として、クレジットカード業界におけるセキュリティ基準である PCI DSS (Payment Card Industry Data Security Standard) の内容も取り扱う。

3.1 FISC ガイドライン

財団法人金融情報システムセンターは、金融機関等のコンピュータシステムの安全対策の共通的なよりどころとして「金融機関等コンピュータシステムの安全対策基準・解説書」を策定した [8]。

最新版である第 8 版は 2011 年 3 月に発行され、基準項目数は 305 項目（設備基準 138 項目、運用基準 114 項目、技術基準 53 項目）に上る。また、第 8 版追補改訂が 2015 年 6 月に発行されている [9] ほか、2018 年 3 月にはさらなる改訂版の発行が予定されている。

暗号アルゴリズムについては技術基準にて言及されており、128bit 安全性を満たすような暗号アルゴリズムの使用が推奨されている。ただし、SSL/TLS のような暗号プロトコルに関する基準は記載されていない。

3.2 PCI DSS

PCI DSS (Payment Card Industry Data Security Standard) は、カード会員データのセキュリティを強化し均一なデータセキュリティ評価基準の採用をグローバルに推進するために、PCI SSC (Payment Card Industry Security Standards Council) によって策定された。最新版は 2016 年 4 月に発行された Version 3.2 である [10]。

PCI DSS では最低 112bit 安全性を有する暗号アルゴリズムを「強力な暗号化技術 (Strong Cryptography)」として定義し、利用を推奨している。Version 3.2 では例として以下の暗号アルゴリズムが挙げられている。

- AES（128bit 以上）
- TDES/TDEA（3 倍長キー）
- RSA（2048bit 以上）
- ECC（224bit 以上）
- DSA/D-H（2048/224bit 以上）

また、新しい実装では最低 128bit 安全性を有する暗号アルゴリズムを使用するよう推奨されている。

PCI DSS では SSL/TLS の設定に関する補助資料も公開されている [11]。補助資料には以下の内容が記載されている。

- SSL と初期の TLS を使ってはならない。最低限 TLS1.1 を適用し、TLS1.2 が強く奨励される。
- 2016 年 6 月 30 日までに安全な TLS サービスを提供しなければならない。
- 2018 年 6 月 30 日以降、SSL と初期の TLS の利用を停止し、安全なバージョンのプロトコルのみを使用しなければならない。
- 2018 年 6 月 30 日より以前に、SSL と初期の TLS を使用している実装は、公式の Mitigation and Migration Plan を持たなければならない。
- SSL と初期の TLS による攻撃を受けていないと検証された POS POI 端末は、2018 年 6 月 30 日以降も使用してよい。

4. 推奨設定の比較

各基準・ガイドラインにおける SSL/TLS 設定の一覧を表 1 に示す。全ての基準・ガイドラインにおいて、128bit 安全性を満たす暗号アルゴリズムの使用が推奨されていることが分かる。SSL/TLS のプロトコルバージョンについては、TLS 1.1 以上の使用が推奨されている。日本の基準・ガイドラインでは、使用できる暗号アルゴリズムとして CRYPTREC 暗号リストが参照されている。

*2 上位バージョンが使用できない場合のみ

5. 都市銀行における SSL/TLS サーバ設定状況

本章では、都市銀行における SSL/TLS サーバの設定状況を調査した結果を示す。調査対象は日本国内の都市銀行でインターネットバンキングのログインサイトとして公開されているサーバとし、個人向けサイトと法人向けサイトそれぞれを調査した。客観性を担保するために、調査には Qualys SSL Labs の SSL Server Test [12] を利用した。

5.1 個人向けサイト

日本国内の都市銀行において、個人向けインターネットバンキングのログインサイトとして公開されている URL のドメインを抽出し、SSL Server Test の出力結果を調査した。個人向けサイトの調査結果を表 2 に示す。SSL Server Test による評価では、C 銀行が C でそれ以外の 3 銀行は B と判定された。C 銀行は TLS 1.1 および TLS 1.2 に対応していないことで C と評価されている。

5.2 法人向けサイト

日本国内の都市銀行において、法人向けインターネットバンキングのログインサイトとして公開されている URL のドメインを抽出し、SSL Server Test の出力結果を調査した。法人向けサイトの調査結果を表 3 に示す。SSL Server Test による評価では、A 銀行が A、D 銀行が A-と判定される一方、B 銀行は C、C 銀行は F と判定された。両銀行ともに SSL 3.0 を有効にしていることで評価が下がっている。また C 銀行は、56bit 安全性しか満たさない DES を含む暗号スイートをサポートしていることが、評価の低下につながっている。DES は最近の OS や暗号ライブラリでは無効化されている場合が大半であるため、古い OS やライブラリでサービスが行われていると考えられる。

5.3 考察

都市銀行の SSL/TLS サーバ設定状況を Qualys SSL Labs の SSL Server Test によって調査した結果、安全でない（C〜F 判定）とされる設定が残っていることが判明した。原因として以下のようなことが考えられる。

古いソフトウェアの使用

C 銀行の SSL/TLS サーバでは DES が有効とされていた。DES は最近の OS や暗号ライブラリでは無効化されている場合が大半であるため、古い OS やライブラリでサービスが行われていると考えられる。SSL/TLS を安全に利用するためには、最新の OS およびライブラリを利用することが必要である。

相互接続性の確保

SSL 3.0 を有効にしている理由は、Windows XP 上で動作する Internet Explorer 6 を受け入れるためであると推測

表 1　SSL/TLS 推奨設定の比較

組織名	暗号アルゴリズム	SSL/TLS バージョン	SSL/TLS 暗号スイート
IETF [5]	112bit 安全性未満禁止 128bit 安全性未満非推奨	TLS 1.1 *2 TLS 1.2	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
CRYPTREC （高セキュリティ型） [6]	CRYPTREC 暗号リスト掲載 128bit 安全性以上 認証付暗号モード採用 Perfect Forward Secrecy	TLS 1.2	（グループ α のみ） TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 TLS_DHE_RSA_WITH_CAMELLIA_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384
CRYPTREC （推奨セキュリティ型） [6]	CRYPTREC 暗号リスト掲載 128bit 安全性以上	TLS 1.1 TLS 1.2	（グループ A のみ） TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 TLS_DHE_RSA_WITH_CAMELLIA_128_GCM_SHA256 TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
FISC [8], [9]	128bit 安全性以上 CRYPTREC 暗号リスト掲載	-	-
PCIDSS [10], [11]	112bit 安全性以上 新たな実装は 128bit 安全性以上	TLS 1.1 TLS 1.2	-

表 2　都市銀行における SSL/TLS サーバ設定状況（個人向けサイト）

銀行	評価	根拠
A 銀行	B	RC4 の許可 Forward Secrecy の未サポート
B 銀行	B	弱い DH 鍵のサポート
C 銀行	C	SSL3.0 の使用 TLS1.2 への未対応 RC4 の許可 Forward Secrecy の未サポート
D 銀行	B	中間証明書で SHA-1 を使用 RC4 の許可 Forward Secrecy の未サポート

される。中小企業等 OS の移行が進んでいないユーザーのための相互接続性を確保することで、機会損失を回避することはできる。その一方で、安全でない設定を残すことで Web サーバの安全性が低下しており、攻撃を受けることで結果的に金銭的損失が大きくなる可能性も高い。また、安全でない設定を残すことにより、企業としてのセキュリティ対策が十分でないと判断され、企業の評判が落ちる可能性も否定できない。

ガイドラインの不在

FISC ガイドラインにおいて、暗号アルゴリズムの設定に

表 3　都市銀行における SSL/TLS サーバ設定状況（法人向けサイト）

銀行	評価	根拠
A 銀行	A	-
B 銀行	C	POODLE 攻撃に脆弱 中間証明書で SHA-1 を使用 RC4 の許可 Forward Secrecy の未サポート
C 銀行	F	56bit 安全な暗号スイートのサポート POODLE 攻撃に脆弱 弱い DH 鍵のサポート RC4 の許可 Forward Secrecy の未サポート
D 銀行	A-	-

関する言及はあるが、SSL/TLS のプロトコルバージョンに関しては言及されていない。銀行は FISC ガイドラインに従ってセキュリティ対策を行うため、ガイドラインに言及のない SSL/TLS の適切な設定について意識されていない可能性がある。2 章に示した通り、IETF や CRYPTREC によって SSL/TLS サーバの推奨設定が公開されているので、そのようなガイドラインに従って設定することが望ましい。また、FISC ガイドラインにおいても SSL/TLS の推奨設定について言及することが求められる。

6. SSL/TLS の安全な設定に向けて

SSL/TLS の安全な設定を浸透させるために、以下のような対策を取ることが望まれる。

6.1 SSL/TLS 推奨設定のガイドラインへの記載

FISC ガイドラインにおいて、暗号アルゴリズムに関する基準は示されているが、SSL/TLS のプロトコルバージョンや暗号スイートに関する基準は示されていない。銀行において暗号アルゴリズムを使用する場面として SSL/TLS は大きな位置を占めるため、FISC ガイドラインにも SSL/TLS の設定に関する記述を設けるべきである。

6.2 SSL/TLS 推奨設定のガイドラインへの記載

FISC ガイドラインにおいて、暗号アルゴリズムに関する基準は示されているが、SSL/TLS のプロトコルバージョンや暗号スイートに関する基準は示されていない。銀行において暗号アルゴリズムを使用する場面として SSL/TLS は大きな位置を占めるため、FISC ガイドラインにも SSL/TLS の設定に関する記述を設けるべきである。

6.3 SSL/TLS 設定ガイドラインの更新

CRYPTREC の SSL/TLS 設定ガイドラインは、最新版である Version 1.1 の発行が 2015 年 8 月である。暗号アルゴリズムの安全性は日進月歩で変わるため、2017 年現在では既に情報が古いと言える。古い情報をそのまま公開し続けることによって、安全でない SSL/TLS 設定が参照され続け結果的にインターネットの安全性が脅かされる恐れがある。そのため、現在の安全性基準に即した内容を反映した最新版の発行が望まれる。

6.4 信頼できる組織による情報発信

現在は情報セキュリティや暗号技術に関する情報が充実し、個人ブログ等でもさまざま解説が公開されている。しかし、一般のユーザにとって、難解な暗号技術に関する情報の真偽を判断することは難しい。そのため、専門家により精査された情報をしかるべき機関から発信することが求められる。

6.5 暗号アルゴリズム移行計画立案の必要性

相互接続性の確保等のため、弱いセキュリティ設定を現在も残している Web サイトは多く存在する。そのような Web サイトでも、今後のセキュリティ確保のために、暗号移行計画を立てるべきである。

7. まとめ

本稿では、暗号 2017 年問題をはじめとする暗号危殆化問題に対し、SSL/TLS の推奨設定がどのように規定されているかを調査した。また、銀行の SSL/TLS サーバ設定を調べ、推奨設定に従わない弱い設定が残されていることを示した。さらに、SSL/TLS サーバ設定を安全にするための方策を提言した。インターネットの安全性を確保するために、国や業界団体において最新の情報を反映した基準・ガイドラインが発信され、企業においても最新の安全性を確保するよう対策することが望まれる。

参考文献

[1] Allen, C. and Dierks, T.: The TLS Protocol Version 1.0, RFC 2246 (1999).
[2] Dierks, T. and Rescorla, E.: The Transport Layer Security (TLS) Protocol Version 1.1, RFC 4346 (2006).
[3] Rescorla, E. and Dierks, T.: The Transport Layer Secu-

rity (TLS) Protocol Version 1.2, RFC 5246 (2008).
[4] Rescorla, E.: The Transport Layer Security (TLS) Protocol Version 1.3 (2017).
[5] Sheffer, Y., Holz, R. and Saint-Andre, P.: Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS), RFC 7525 (2015).
[6] 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）〜 Ver.1.1 (2015).
[7] Mullin, R. and Vanstone, S.: Digital signatures on a smart card, CA Patent 2202566 (2006).
[8] 金融情報システムセンター：金融機関等コンピュータシステムの安全対策基準・解説書第 8 版，金融情報システムセンター (2011).
[9] 金融情報システムセンター：金融機関等コンピュータシステムの安全対策基準・解説書第 8 版追補改訂，金融情報システムセンター (2015).
[10] PCI Security Standards Council: PCI DSS Requirements and Security Assessment Procedures (2016).
[11] PCI Security Standards Council: Migrating from SSL and Early TLS Version 1.1 (2016).
[12] Qualys SSL Labs: SSL Server Test, `https://www.ssllabs.com/ssltest/`.