プレスリリース
2020 年 7 月 7 日
独立行政法人情報処理推進機構

サーバーの構築者、管理者等向けの「TLS 暗号設定ガイドライン」を公開

～TLS1.3 の採用・SSL3.0 の禁止を盛りこみ、TLS サーバーでの要求設定を全面改訂～

IPA（独立行政法人情報処理推進機構、理事長：富田 達夫）セキュリティセンターは、2015 年以降の SSL/TLS (*1) 通信の規格化およびサポートの状況を踏まえ、2020 年 3 月時点における TLS 通信での安全性と相互接続性のバランスを考慮したウェブサーバーでの TLS 暗号設定方法をまとめた「TLS 暗号設定ガイドライン」を本日公開しました。

URL：https://www.ipa.go.jp/security/vuln/ssl_crypt_config.html

各種インターネットサービスでは、安全に通信する仕組み（プロトコル）として SSL/TLS 通信が標準的に利用されています。その SSL/TLS 通信は 1994 年のプロトコル開発以来、その時々のセキュリティ対策を組み込んだ結果、複数のバージョンが作られてきました。よって、一口に SSL/TLS 通信といっても、ウェブサーバーとブラウザーの設定次第で実現される安全性が異なるという問題がありました。

IPA ではこれまでに SSL/TLS 暗号設定ガイドラインを 2 版公開 (*2) していますが、第 2 版の発行後、記載内容に大きく影響する SSL/TLS 通信の規格化が相次いで行われ、改訂が望まれていました。

本日公開の「TLS 暗号設定ガイドライン」は、前述の問題と技術環境の変化を反映させるため、暗号技術評価プロジェクト CRYPTREC (*3) が記載内容の全面的な見直しを行ったものです。サーバーの構築者および管理者、サーバーの構築を発注するシステム管理者を想定読者としています。

● ガイドラインの特長

（1） 2020 年 3 月時点における TLS 通信での実現すべき安全性と必要となる相互接続性とのトレードオフを考慮した、3 つの設定基準 (*4) を提示（別紙参照）。

（2） 設定基準に対応するプロトコルバージョン、サーバー証明書、暗号スイートの詳細な要求設定 (*5) を提示。

（3） 要求設定に基づいたサーバー設定を支援するチェックリスト及び参考ガイドを用意

● 従来の暗号設定ガイドライン（Ver.1、2）との差異

（1） TLS1.3 の採用及び SSL3.0 の禁止に伴い、一段高い安全性を各設定基準に要求

（*1）SSL(Secure Socket Layer)/TLS（Transport Layer Security）：インターネット通信を暗号化する技術

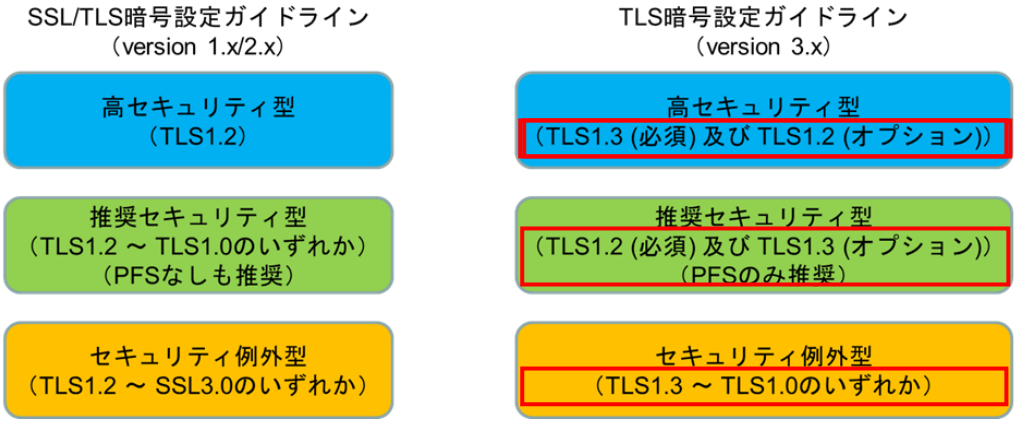
（*2）2015 年 5 月に Ver.1、2018 年 5 月 Ver.2。https://www.ipa.go.jp/security/vuln/ssl_crypt_config.html

（*3） CRYPTREC（クリプトレック）総務省及び経済産業省が共同で運営する暗号技術検討会と、国立研究開発法人情報通信研究機構（NICT）及び独立行政法人情報処理推進機構（IPA）が共同で運営する暗号技術評価委員会及び、暗号技術活用委員会で構成される。https://www.cryptrec.go.jp/about.html

（*4）「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」の区分け基準のこと

（*5）設定基準で選択した区分けに必要な、設定すべき具体的な要求事項のこと

既存の SSL/TLS 暗号設定ガイドラインを利用している場合は、最新版の要求設定に基づいた見直しを行い、必要に応じた設定変更を推奨します。



（2） 要求設定において、従来の「遵守項目」に「推奨項目」を追加

これまでの、必ず満たさなければならない「遵守項目」に加え、よりよい安全性を実現するために満たすことが望ましい「推奨項目」を追加しました。それは、サーバーによっては「遵守項目」であるにも関わらずその通りに設定できない事例が多数あり、こうしたケースを推奨項目と位置付けたためです。これにより現実的かつ実効性が高い要求設定が可能になります。

（3） チェックリスト及び参考ガイドの改訂

・チェックリスト

「選択した設定基準に対応した要求設定項目の設定忘れの防止」と「サーバー構築の作業受託先が適切に要求設定項目を設定したことを確認」するためのリストを改訂

・参考ガイド：サーバー設定編・暗号スイート設定編

主要なオープンソースを利用したサーバーでの具体的な設定を支援するためのガイドで、見直された要求設定に準拠する具体的な設定方法を解説。

「TLS 暗号設定ガイドライン」、「チェックリスト」、及び参考ガイド（「TLS 暗号設定 サーバ設定編」と「TLS 暗号設定 暗号スイート編」）は以下の URL からダウンロードできます。

URL：https://www.ipa.go.jp/security/vuln/ssl_crypt_config.html

本ガイドライン、チェックリストおよび参考ガイドが広く活用され、ウェブサーバーで適切な TLS 暗号設定が行われることにより、安全なインターネット社会の実現の一助となることを期待しています。

■本件に関するお問い合わせ先
IPA　セキュリティセンター　暗号グループ　神田、橋本
Tel: 03-5978-7545　　E-mail: isec-info@ipa.go.jp
■報道関係からのお問い合わせ先
IPA　戦略企画部　広報戦略グループ　白石
Tel: 03-5978-7503　　E-mail: pr-inq@ipa.go.jp