Updated !!

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）～

インターネットビジネスにSSL/TLSは必須なので導入しましたよ
・・・　ちょっと待って、その暗号設定は大丈夫ですか？
ぜひ「暗号設定ガイドライン」をご活用ください！

CRYPTRECがまとめた
SSL/TLSを安全に使う
ためのベストプラクティス

安全性と相互接続性の
バランスを取った推奨設定
をガイダンス

CRYPTREC
Cryptography Research and Evaluation Commitees

CRYPTRECとは
総務省・経済産業省・NICT・IPAが実施している暗号技術評価プロジェクト。暗号技術の専門家により安全性と実装性に優れると判断されたCRYPTREC暗号リストを作成・公表している。

安全なSSL/TLSサーバ構築に必要な暗号設定

安全性と相互接続性のバランスをどう取るか

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

バランスに応じた推奨設定とは何か

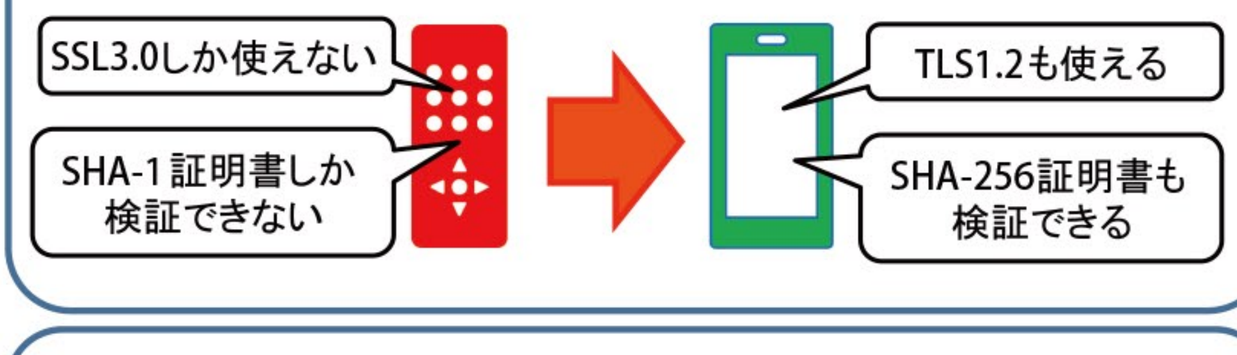
- プロトコルバージョン・・・不必要なバージョンを利用させない設定
- サーバ証明書 ・・・ サーバ証明書を不正利用させない設定
- 暗号スイート ・・・ 弱い暗号を利用させない設定

必要な推奨設定項目の設定確認をどうやるか

- チェックリスト ・・・ 必要な推奨設定項目の設定忘れの防止策

3年間の動向を踏まえ、暗号設定の要件をアップデート！

モバイル端末の更新



民間認証局でのSHA-1証明書発行終了

セキュリティ例外型の利用制限を強化
「短期的な利用」⇒「早期移行」

高セキュリティ型の適用範囲の拡大
「限定的利用」⇒「一般的利用」

TLS1.3の情報提供

本ガイドラインとチェックリストは IPA と CRYPTREC のホームページからダウンロードできます
(IPA) https://www.ipa.go.jp/security/vuln/ssl_crypt_config.html
(CRYPTREC) http://www.cryptrec.go.jp

IPA 独立行政法人 情報処理推進機構
Information-technology Promotion Agency, Japan