TLS暗号設定ガイドライン　v.3.1の改訂内容について

2024年2月19日

独立行政法人情報処理推進機構
セキュリティセンター　セキュリティ技術評価部

IPA Better Life with IT

改訂の背景

■ 「TLS暗号設定ガイドライン」の改訂(v3.0.1からv3.1)の背景は以下のとおり

- 「CRYPTREC暗号リスト（電子政府推奨暗号リスト）」の改定（2012年版から2022年版に改定）
  - CRYPTREC暗号リストには「電子政府推奨暗号」「推奨候補暗号」「運用監視暗号」の３つのカテゴリーがある
  - 「電子政府推奨暗号」への昇格：EdDSA, SHA-512/256, SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256, XTS, ChaCha20-Poly1305, ISO/IEC 9798-4
  - 「運用監視暗号」への降格：3key-Triple DES
  - 「運用監視暗号」からリスト外への降格：RC4, SC2000

  ※下線のアルゴリズムはIANA TLS registryに登録されているもの
- 「暗号強度要件に関する設定基準」の策定（2022年3月）
  - CRYPTREC暗号リストに掲載の暗号技術を利用する際の鍵長の選択方法を規定
  - 「ビットセキュリティ基準」を導入し、これに基づいてアルゴリズムごとに強度要件を規定

改訂内容

- TLS暗号設定ガイドラインv3.1の改訂内容のうち、「TLS暗号設定ガイドライン参考文書の更新業務」に関わる部分は以下の通り

	対象となるセキュリティ型	改訂内容
1	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	鍵交換にECDHEを利用する場合に128ビットセキュリティ以上を満たす曲線の使用を規定。これによりx25519を明示的に利用可能とした
2	高セキュリティ型 推奨セキュリティ型	鍵交換にてECDHE鍵/DHE鍵に付与する署名の推奨アルゴリズムにEdDSA（ed25519及びed448）を追加
3	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	暗号スイートでの利用禁止アルゴリズムにSM2_signature(署名), SM3(ハッシュ関数), SM4(共通鍵ブロック暗号)を追加

- TLS暗号設定ガイドラインv3.1では上記以外の改訂も行っているが、いずれも「TLS暗号設定ガイドライン参考文書の更新業務」には関係しない内容である

「TLS暗号設定ガイドライン参考文書の更新業務」に関わる TLS暗号設定ガイドラインV3.1の影響

	TLS暗号設定ガイドラインV3.1内容	更新作業への影響
1	【改訂あり】CRYPTREC暗号リスト改定に伴ったTLSでの利用可能／利用禁止暗号アルゴリズム	「TLS暗号設定ガイドライン」の現行版において、既にChaCha20-Poly1305は暗号スイートでの利用推奨アルゴリズムとして、また3key-Triple DESとRC4は利用禁止アルゴリズムとして、それぞれ指定されており、この改訂による影響なし EdDSAを暗号スイートでの推奨アルゴリズムに指定したことの影響あり(以下の3)
2	【改訂あり】鍵交換にECDHEを利用する場合に128ビットセキュリティ以上を満たす曲線の使用を規定。これによりx25519を明示的に利用可能とした	「サーバ設定編」および「暗号スイートの設定例」の現行版において、既にx25519の設定例が示されているため、同等の設定ができていればよい
3	【改訂あり】鍵交換にてECDHE鍵/DHE鍵に付与する署名の推奨アルゴリズムにEdDSA（ed25519及びed448）を追加	現状、パブリック認証局の発行するサーバ証明書ではEdDSAを公開鍵として設定できず、鍵交換の署名としてEdDSAを利用できないため、今回の更新作業においては対応不要とする
4	【改訂あり】暗号スイートでの利用禁止アルゴリズムにSM2_signature(署名), SM3(ハッシュ関数), SM4(共通鍵ブロック暗号)を追加	「暗号スイートの設定例」の現行版では、利用禁止アルゴリズムを明示的に除外するのではなく、利用するアルゴリズムを指定する設定例で示されているため、この改訂による影響なし
5	【改訂なし】TLS1.2以前及びTLS1.3における暗号スイートの推奨セット及び優先順位には変更なし（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全て）	暗号スイートの設定は「サーバ設定編」および「暗号スイートの設定例」の現行版と同等の設定ができていればよい
6	【改訂なし】TLSプロトコルバージョン及びサーバ証明書の推奨設定には変更なし（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全て）	TLSプロトコルバージョン及びサーバ証明書は「サーバ設定編」および「暗号スイートの設定例」の現行版と同等の設定ができていればよい

TLS暗号設定ガイドラインv3.1の発行について

- 現在、TLS暗号設定ガイドラインv3.1はドラフト段階。3月上旬のCRYPTREC暗号技術活用委員会にて発行が承認される予定