別紙

■安全性と相互接続性についての比較

安全性の確保と相互接続の必要性のトレードオフにより、「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 段階の設定基準を設けています。実際にどの設定基準を採用するかは、安全性の確保と相互接続の必要性の両面を鑑みて、サーバー管理者等が最終的に決定すべきことですが、特段の要求がなければ「推奨セキュリティ型」の採用を強く推奨します。

設定基準	概要	安全性	相互接続性の確保
高セキュリティ型	**※ 高い安全性の確保を必要とする利用を想定した設定** 情報が漏えいした際、組織の運営や資産、個人の資産やプライバシー等に悪影響を及ぼすと予想される情報を、安全性を優先して TLS 通信を行うような場合に採用する設定基準 ＜利用例＞ • 特にセキュリティが重要視されるシステムを構築する場合	本ガイドライン作成時点（2020 年 3 月）において、標準的な水準を大きく上回る高い安全性水準を達成している	本ガイドラインで対象とするブラウザが搭載されている PC、スマートフォン等であれば相互接続性を確保できると期待される。
推奨セキュリティ型	**※ほぼすべての一般的な利用形態で使うことを想定した設定** 情報が漏えいした際、組織の運営や資産、個人の資産やプライバシー等に悪影響を及ぼすと予想される情報を、安全性確保と利便性（相互接続性）の実現をバランスさせて TLS 通信を行うための標準的な設定基準 ＜利用例＞ • 電子申請など、企業・国民と役所等との電子行政サービスを提供する場合 • 金融サービスや電子商取引サービス、多様な個人情報の入力を必須とするサービス等を広範囲（不特定多数）に提供する場合 • 新規に社内システムを構築する場合	本ガイドライン作成時点（2020 年 3 月）における標準的な安全性水準を実現している	本ガイドラインで対象とするブラウザが搭載されている PC、スマートフォンを含め、多くの製品・システムで相互接続性を確保できると期待される。 ※サポートが終了しているバージョンが古い OS やブラウザ、発売開始から長期間経過している古い機器、IoT 用途などの一部の機器類については接続できない可能性がある。
セキュリティ例外型	**※推奨セキュリティ型への移行完了までの暫定運用を想定した設定** 脆弱なプロトコルバージョンや暗号が使われるリスクを受容したうえで、**安全性よりも相互接続性に対する要求をやむなく優先**させて TLS 通信を行う場合に採用する設定基準 ＜利用例＞ • 利用するサーバーやクライアントの実装上の制約、又は既存システムとの相互接続上の制約により、推奨セキュリティ型（以上）の設定が事実上できない場合	本ガイドライン作成時点（2020 年 3 月）において、標準的な安全性水準を満たしていないプロトコルバージョンや暗号スイート等が使用される可能性があることを認識する必要がある	既存システムを含め、ほぼすべての機器に対して相互接続性が確保されると期待される。