「SSL 3.0」で発見された脆弱性への対応について

インターネットで通信内容の保護に使われている暗号化方式「SSL 3.0」につきまして深刻な脆弱（ぜいじゃく）性が発見されました。保護すべき通信内容の一部が漏えいする可能性があるというものです（詳細は情報処理推進機構の「SSL 3.0 の脆弱性対策について（https://www.ipa.go.jp/security/announce/20141017-ssl.html）」をご参照ください）。

この脆弱性に対応するため、統合電子認証システムおよび東北大学ポータルシステムでは SSL 3.0 の使用を順次停止し、SSL を基に強化・開発された暗号化方式「TLS」だけを通信に用いるように切り替えを実施いたします。**最近のウェブブラウザーは** TLS に標準で対応しているため、システム側で旧式化した SSL 3.0 使用を停止しても**サービスのご利用に影響はございません。**

しかし一部の古いブラウザーや、ブラウザーの通信設定によっては、東北大学ポータルシステムにアクセスできなくなる場合がありますのでご注意ください。その場合は、新しいブラウザーにアップデートしてご利用いただくか、Internet Explorer の場合には以下の通信設定の例をご参照の上、設定変更をお願いいたします。

なお、Chrome および Firefox は最新バージョンで既にこの問題に対応済みとなっております。そのほかのブラウザーの開発元も対応策をそれぞれ発表しておりますので、開発元の情報をご確認ください。

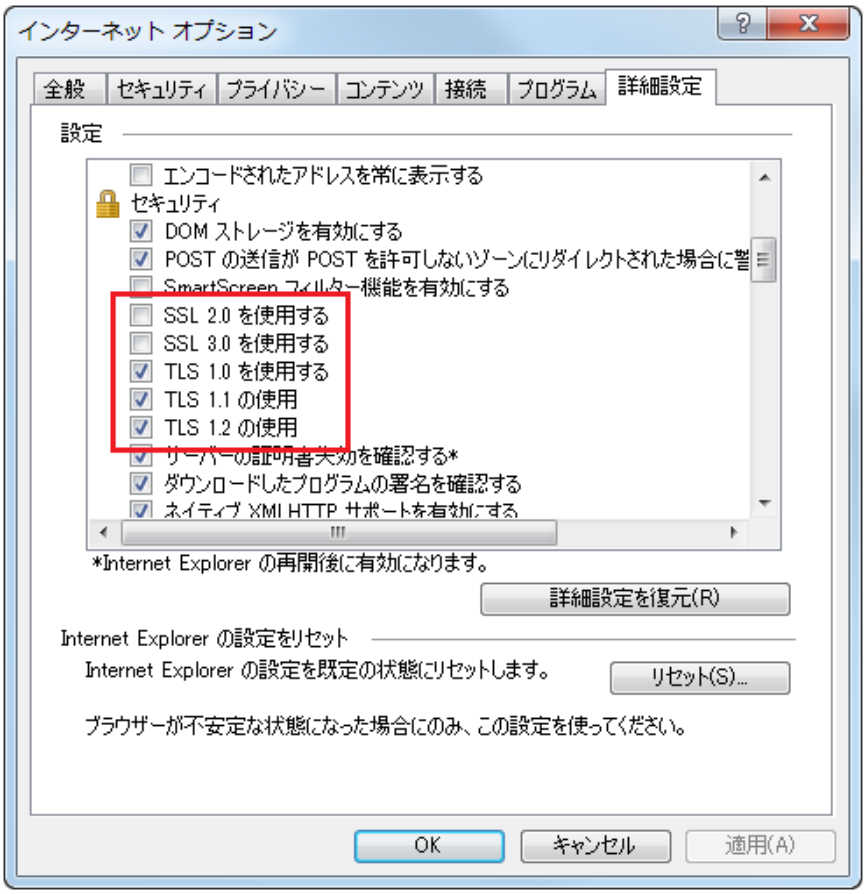
SSL 3.0 無効化作業日程

- 東北大学ポータルサイト　　平成 26 年 12 月 18 日　12:00 ～ 13:00
- 教職員グループウェア　　平成 26 年 12 月 19 日　12:00 ～ 13:00
- 統合電子認証システム　　平成 27 年 1 月（予定）

ブラウザーの通信設定の例

「Internet Explorer」を例に通信設定の方法をご説明します。

1. Internet Explorer のウインドウ上部のメニュー「ツール」から（メニューが表示されていない場合は右上の歯車のマークから）「インターネット オプション」を開く
2. 「インターネット オプション」のウインドウの上部にあるタブの中から「詳細設定」をクリックする
3. 「設定」に表示された項目のうち「セキュリティ」のブロックが表示されるまでスクロールする



4. 「SSL 2.0 を使用する」と「SSL 3.0 を使用する」のチェックを外し、一方で「TLS 1.0 を使用する」「TLS 1.1 の使用」「TLS 1.2 の使用」の 3 カ所にチェックを入れた状態にする
5. 「適用」のボタンをクリックし、「OK」をクリック
6. Internet Explorer を一度閉じ、再起動する