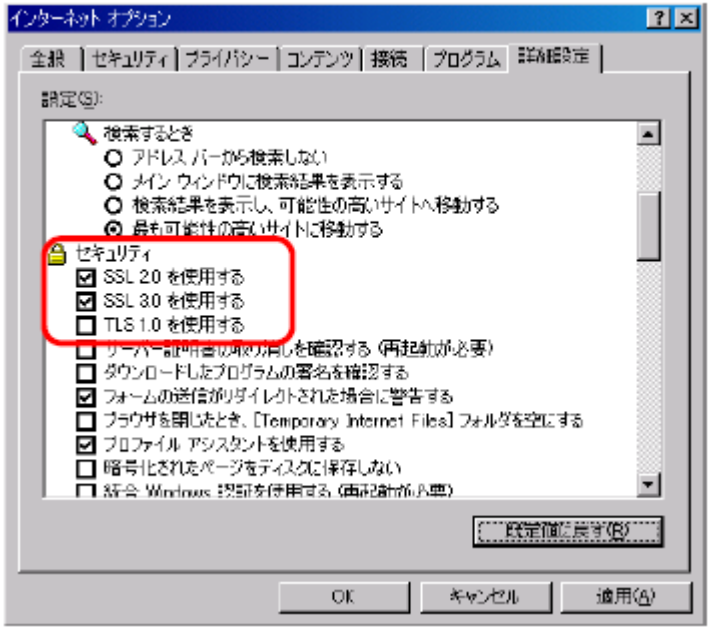
2014 年 10 月 16 日
アーティス株式会社

【SSL3.0 の脆弱性（POODLE）対策について】

10 月 14 日に SSL3.0 に存在する脆弱性(POODLE：Padding Oracle On Downgraded Legacy Encryption)が公表されました。
当社におきましては、eラーニングサービス等で利用しているサーバに影響することから情報を読み取られてしまう危険性を回避するために該当するサーバに対して SSL3.0 による接続を無効とする設定を行いました。
なお、Internet Explorer（IE）の設定で「TLS 1.0」が有効でない場合、アクセスができなくなります。
IE7 以降のブラウザではデフォルトで有効になっていますが、IE6 ではデフォルトで無効となっています。
「TLS 1.0」が無効となっている場合、インタネットオプション⇒詳細設定⇒セキュリティ項目の「TLS 1.0 を使用する」にチェックで有効化することができます。

＜初期設定（デフォルト設定）＞



＜SSL3.0の脆弱性対策後（サーバ側でSSL3.0の接続を無効）＞