平成 26 年 12 月 23 日

「ＳＳＬ３．０」の脆弱性について

１．概要　SSL 3.0 プロトコルにおいて通信の一部が第三者に解読可能な脆弱性
（SSL 3.0 を使用している場合、通信の一部が第三者に漏えいする可能性）

２．対象　SSL 3.0 を使用するサーバ、クライアント
（au や docomo の一部携帯電話、古いバージョンのブラウザなど）

３．対策　暗号化方式「TLS1.0」以降に対応した端末／ブラウザでアクセスしてください。

例：Internet Explorer での設定方法
「ツール」メニュー→「インターネットオプション」の「詳細設定」タブにある「セキュリティ」で
・「SSL 3.0 を使用する」のチェックを外す
・「TLS 1.0 を使用する」「TLS 1.1 の使用」「TLS 1.2 の使用」にチェックを入れる