SSL3.0脆弱性（POODLE）への弊社対応状況について

平素は、弊社ネット注文システムをご利用頂き、誠にありがとうございます。

下記、脆弱性について、弊社提供サービスである「パンチネット注文」に関して、
当該サーバへのSSL3.0の無効化を実施致しました。

【脆弱性内容】
SSL 3.0 プロトコルには、通信の一部が第三者に解読可能な脆弱性が存在します。
サーバ、クライアント間の通信において、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があります。
ただし、攻撃には一定の条件が必要になります為、ただちに悪用可能な脆弱性ではありません。

【対策について】
弊社管理サーバにつきましては、SSL3.0の機能を無効化しておりますので、ご安心下さい。

SSL 3.0は十数年前にリリースされた古いバージョンのプロトコルであり、
本脆弱性の影響を受けないTLS1.0等の比較的新しいプロトコルが、多くのウェブブラウザで
ご利用可能であることと、本脆弱性の影響範囲の大きさを考慮し、
弊社ではSSL 3.0の無効化を判断しております。
安全に弊社サービスをご利用頂くための対応ですので、ご理解の程、よろしくお願い致します。

【本件対策における影響について】
ご利用端末がWindowsXPでウェブブラウザがInternetExplorer6等の古いソフトウェアを
ご利用されている場合には、SSLコンテンツが表示できない可能性があります。

＜弊社サイトにアクセスできない場合＞
ウェブブラウザで、弊社サイトにアクセスできなくなってしまった場合は、
以下設定によりTLS 1.0を有効化してください。
■Microsoft Internet Explorerの例
［ツール］→［インターネット オプション］→［詳細設定］において
「TLS 1.0を使用する」のチェックを入れて、ブラウザを再起動してください。

【本件に関するお問い合わせ先】
パンチ工業株式会社　情報システム推進室
担当：　千田、伊藤（義）
TEL：　0197-68-3137
＜ご参考＞
SSLv3 プロトコルに暗号化データを解読される脆弱性（POODLE 攻撃）
http://jvn.jp/vu/JVNVU98283300/