Cente Technical Information

発行番号	006-0005	Rev	第1版	発行日	2012/09/20
題名	SSL3.0のみに対応しているサーバに接続できないことがある現象について				
情報分類	障害情報				
適用製品	・Cente Compact SSL Ver.1.00				
関連資料	なし				

【該当するユーザ環境】
Cente Compact SSL Ver.1.00を使用し、SSL3.0のみに対応しているサーバに接続するユーザ。

【障害内容】
ssl_set_version()を使うと、サーバに通知する使用可能SSLバージョンを指定することができます。このAPIでTLS1.0/SSL3.0の両方を指定（デフォルト）すると、送信するClient Helloのバージョンは TLS1.0となります。接続先がSSL3.0だけに対応しているサーバだった場合、SSL3.0にバージョンを変更してネゴシエーションを続けます（ロールバック機能）。ここで、使用するサーバによっては「Bad Record MAC」のAlertが送信されて接続が失敗することがあります。

【発生理由】
クライアントから送信するKey Exchangeメッセージで使用する鍵（プリマスタシークレット）を作成する際にSSLバージョンを使用します。Cente Compact SSLではロールバック後のバージョンを使用していましたが、正しくはClient Helloと同じバージョンを使用する必要がありました。OpenSSLなど、この点を厳しくチェックするサーバの場合、「Bad Record MAC」のAlertが送信されて接続が失敗します。

【回避方法】
ソースコードを修正し、Client Helloと同じバージョンを使用するよう変更する必要があります。
（改変箇所については、営業担当またはsupport@cente.jpまでお問い合わせください。）

以上