Cente Technical Information

発行番号	006-0008	Rev	第1版	発行日	2014/01/31
題名	DTLSの再ハンドシェイクができない現象について				
情報分類	障害情報				
適用製品	・Cente Compact DTLSc SSLオプション Ver.1.00				
関連資料	なし				

【該当するユーザ環境】
Cente Compact DTLSc SSLオプション Ver.1.00を使用し、再ハンドシェイク機能を使用しているユーザ。

【障害内容】
SSLcでは、ssl_connect()を呼び出して初回のハンドシェイク確立後、通信中にssl_handshake()を呼び出すと再ハンドシェイクを行うことができます(SSLdから再ハンドシェイクが要求される場合もあります)。しかし、DTLScで再ハンドシェイクを実行すると正しく処理されず、DTLS通信が継続できなくなります。
(デフォルトでは2分後に再ハンドシェイクがSSLERR_IO_TIMEOUTエラーを返します。)
DTLS通信を再開するには、再度dtls_init()の呼び出しから始める必要があります。

【発生理由】
DTLSc内部では、DTLSdとのパケット送受信の対応にシーケンス番号を使っています。初回ハンドシェイク完了後にシーケンス番号を初期化する必要がありますが、これが正しく処理できていませんでした。そのため、再ハンドシェイク時にDTLSdから受信するハンドシェイクパケットのシーケンス番号と、Cente Compact DTLScが期待するシーケンス番号が異なり、DTLSdから受信したパケットを全て破棄していました。

【回避方法】
DTLSc、DTLSdともに再ハンドシェイクを利用しない環境であれば、本障害は影響がありません。サーバから再ハンドシェイクのリクエストを受けた場合、一旦切断し、ssl_connect()を使用して新しいDTLS接続を行う場合も影響がありません。
再ハンドシェイクを行う場合、シーケンス番号の初期化処理を修正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