Cente Technical Information

発行番号	006-0009	Rev	第1版	発行日	2014/01/31
題名	DTLSdからCertificate Requestを受信するとハンドシェイクに失敗する現象について				
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、通信相手のDTLSdがハンドシェイク時にCertificate Requestを送信する環境で運用しているユーザ。
なお、Certificate Requestを送信しないDTLSdと通信する場合は本障害は影響がありません。

【障害内容】
DTLScではssl_connect()を呼び出してDTLSdとハンドシェイクを行います。ハンドシェイク中にDTLSdからCertificate Requestを受信した場合、ssl_connect()はSSLERR_HS_UNEXPECTED_PACKETエラーで返り、ハンドシェイクに失敗します。

【発生理由】
DTLScがCertificate Requestを受信した際、パケットのパース後に次のハンドシェイクパケットを受信する必要がありますが、正しく受信処理を行っていませんでした。
そのため、Certificate Requestの次のパケットであるServer Hello Doneパケットを処理できず、ハンドシェイクに失敗していました。

【回避方法】
クライアント証明書の確認処理が不要なサーバであれば、Certificate Requestを送信しない設定にすることで本障害を回避することができます。
Certificate Requestを送信するサーバと通信を行う場合はコードの修正が必要です。
（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