Cente Technical Information

発行番号	006-0011	Rev	第1版	発行日	2018/12/04
題名	AES-GCMまたはchacha20-poly1305使用時に、再ネゴシエーションが失敗する現象について				
情報分類	障害情報				
適用製品	・Cente Compact SSLc Ver.1.30				
関連資料	なし				

【該当するユーザ環境】
Cente Compact SSLc Ver1.30 + Cente Compact Crypto Plusで、暗号スイートにAES-GCMまたはchacha20-poly1305を使用するユーザ。

【障害内容】
暗号スイートにAES-GCM、chacha20-poly1305を使用している場合に再ネゴシエーションに失敗します。

【発生理由】
再ネゴシエーション時に以下のことが発生していました。
1. AES-GCMまたはchacha20-poly1305使用時のハッシュ計算に誤りがあり、不正なFinishedを送信していました。
2. chacha20-poly1305使用時の暗号処理に誤りがあり、不正なClientHello、ClientKeyExchangeを送信していました。

【回避方法】
ソース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