Cente Technical Information

発行番号	006-0013	Rev	第1版	発行日	2025/01/31
題名	TLS1.3で接続できない場合がある				
情報分類	障害情報				
適用製品	・Cente Compact SSLc Ver.1.50 - Ver.1.52				
関連資料	なし				

【該当するユーザ環境】
Cente Compact SSLc Ver.1.50 - Ver.1.52でTLS1.3を使用しているユーザ。

【障害内容】
以下の設定で運用されているサーバにTLS1.3で接続すると接続に失敗します（以下のいずれかが該当すると失敗します）。
1) ミドルボックス互換モードでない(サーバがChange Cipher Specを送らない)。
2) レコードパディングが有効。

※ミドルボックス互換モードはTLS1.3のハンドシェイクをTLS1.2のハンドシェイクのように似せて接続性を高める機能です。
※レコードパディングはTLS レコードにパディングしてデータ長をわからなくする機能です。

【発生理由】
1) サーバからChange Cipher Specが送られてくることを前提とした実装となっていたため、Change Cipher Specが送られてこない場合、ハンドシェイクが進まず接続が失敗となっていました。
2) レコードパディングの対応が不十分だったため、パディングされている場合に正しくハンドシェイクパケットの解釈ができず接続が失敗となっていました。

【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_XXXatmarkXXX_cente.jpまでお問い合わせください(_XXXatmarkXXX_は@にしてください)。

以上