Cente Technical Information

発行番号	006-0012	Rev	第1版	発行日	2020/10/16
題名	複数の証明書を送ってくるサーバに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】
TLS1.3で接続してサーバが複数の証明書を送ってくる場合に本障害が発生する場合があります。
サーバからの一つ目の証明書の検証が失敗して、二つ目の証明書の検証をしようとした際、証明書の内容に関わらず必ず検証に失敗していました。
ただし以下のいずれかの場合は問題が発生しません(または問題が発生しても接続に失敗しません)。
・TLS1.3で接続しない場合。
・一つ目の証明書で検証が成功した場合。
・証明書検証モード設定「ssl_set_verify_mode()」でSSL_VERIFY_NONEを設定している場合。
・証明書検証モード設定「ssl_set_verify_mode()」でSSL_VERIFY_OPTIONALを設定している場合。
　(ただし証明書検証結果取得「ssl_get_verify_result()」の戻り値がSSLERR_CERT_BAD_FORMATとなります。)

【発生理由】
サーバ証明書の検証は一つ目の証明書から順番に行われ検証が成功した時点で検証完了となります。
一つ目の証明書の検証が失敗した場合、二つ目の証明書の検証を行いますが、このときの証明書チェインのパース処理に間違いがあり二つ目の証明書の検証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