

Cente Technical Information

発行番号	012-0001	Rev	第1版	発行日	2020/01/10
題名	サーバ証明書チェーンを正しく送信できない				
情報分類	障害情報				
適用製品	・ Cente Compact SSLd Ver. 1.00				
関連資料	なし				
<p>【該当するユーザ環境】 サーバ証明書1枚だけではなく、サーバ証明書・それに署名するCA証明書・その上位のCA証明書のように、複数の証明書(以下サーバ証明書チェーン)をクライアントへ送信するユーザ。 サーバ証明書1枚のみを送信する場合は、該当しません。</p> <p>【障害内容】 サーバ証明書チェーンの長さを不正な内容で送信していました。 それを受信したSSLクライアントの動作は、クライアントの仕様によります。 一般には、不正な内容とみなして切断すると思われます。</p> <p>【発生理由】 証明書は、長さで証明書自体を1枚1枚個別に送信する必要がありますが、複数の証明書をまとめて1つの長さにして送信していました。</p> <p>【回避方法】 以下の2点の修正が必要です。 1. ソースコードの修正 2. サーバ証明書チェーンデータの修正 なお、サーバ証明書1枚のみを送信する場合は、問題ありません。</p> <p>詳細については、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)。 (2020/10/01 発行番号の誤り(008-0001)を、012-0001に修正しました)</p> <p style="text-align: right;">以上</p>					