Cente Technical Information

発行番号	006-0004	Rev	第1版	発行日	2012/09/20
題名	正当性が確認できない証明書を受信した場合も接続が成功してしまう現象について				
情報分類	障害情報				
適用製品	・Cente Compact SSL Ver.1.00				
関連資料	なし				

【該当するユーザ環境】
Cente Compact SSL Ver.1.00を使用し、SSLサーバから受信する証明書を検証する環境で運用するユーザ。

【障害内容】
ssl_set_verify_mode()を使うと、SSLサーバから送信されてきた証明書の検証を行うことができます。しかし、内容が改ざんされたルートCA証明書が送信された場合や、不正な証明書と正しいルートCA証明書の2つが送信された場合、不正な証明書と検出できていませんでした。これによって、本来接続が完了すべきでない、不正なサーバに対して接続できてしまうことがあります。

【発生理由】
以下のケースで、証明書が不正と判断できていませんでした。
(A) 署名が不正なルートCA証明書が送信された場合
(B) 署名が不正なサーバ証明書と正しいルートCA証明書が送信された場合

【回避方法】
ソースコードを修正し、上記のケースは「検証失敗」と判断できるようにする必要があります。
（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