Cente Technical Information

発行番号	006-0007	Rev	第1版	発行日	2014/01/20
題名	乱数用のエントロピー提供関数rand_add_entropy()の呼び出しが無効な場合がある				
情報分類	障害情報				
適用製品	・Cente Compact Crypto Ver.1.00 – Ver1.11 なお、このモジュールが含まれるパッケージは以下の通りです。 ・Cente Compact SSLc Ver.1.00 – Ver.1.20 ・Cente Compact SSLd Ver.1.00				
関連資料	なし				

【該当するユーザ環境】
Cente Compact SSLc、Cente Comapct SSLdを使用しているユーザ。またはCente Compact Cryptoに含まれる乱数取得関数rand_get()を直接使用しているユーザ。

【障害内容】
rand_get()で得られる値のランダム性を向上させるため、ユーザは乱数用のエントロピー提供関数rand_add_entropy()を適宜呼び出すこととしています。ここで、機器の電源投入後最初のrand_get()の呼び出しの前にrand_add_entropy()を呼び出してもrand_get()が必ず同じ値になっていました。SSLを使用している場合、機器の電源投入後最初のSSLハンドシェイク実行時に生成する乱数が毎回同じ値になります。なお、その後はrand_add_entropy()の呼び出しによってエントロピーが更新されます。

【発生理由】
初期化後、最初にrand_get()を呼んだ場合に使用するエントロピーが
rand_add_entropy()の呼び出しに関わらず固定値になっていました。

【回避方法】
・機器の電源投入後、一度ダミーでrand_get()を呼び出し、その後rand_add_entropy()を呼び出してエントロピーを提供する。
・ソースコードを修正し、rand_add_entropy()で正しくエントロピーを提供できるようにする。
（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