2010 年 8 月

お客様各位

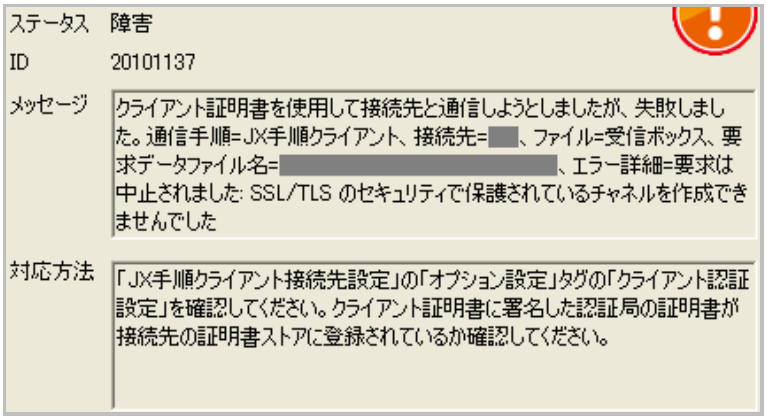
株式会社データ・アプリケーション

# ACMS Lite Neo の JX 手順における SSL 通信時の通信エラーと回避方法について

ACMS Lite Neo の JX 手順クライアントにて、SSL 通信時にエラーが発生する現象がおきましたので、以下にその現象の詳細と回避方法をお知らせ致します。

## 1. 現象

JX 手順クライアントにて、SSL 通信時に障害ログ ID20101137 により通信エラーになる。




[ログ詳細画面]

## 2. 発生条件

（1）対象となる ACMS Lite Neo のバージョンは、1.2.0、1.2.1、1.3.0、1.3.1。

（2）接続先のサーバーが SSL バージョン「TLS 1.0」を未サポートの場合。

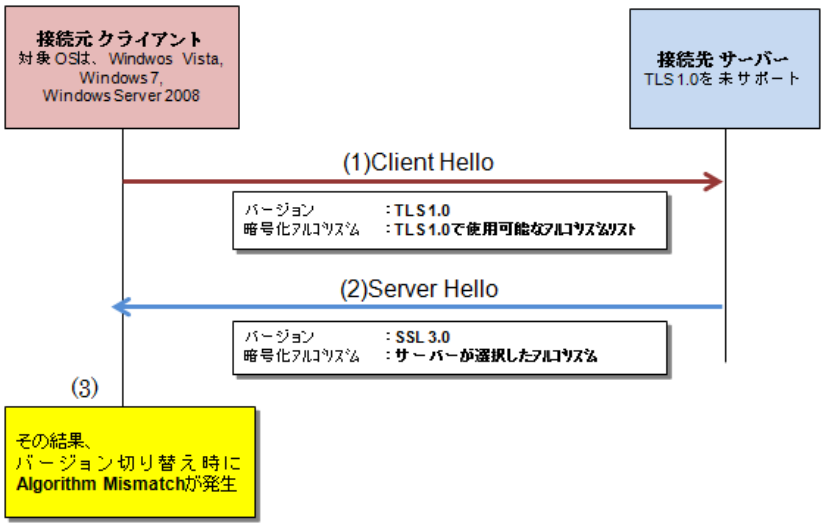
（3）ACMS Lite Neo の稼働 OS が Windows Vista、Windows 7、Windows Server 2008 の場合。

## 3. 現象の詳細説明

ACMS Lite Neo は、SSL 接続を確立する際、最初に TLS 1.0 による接続を試みます。次に、サーバーからの返信にて TLS 1.0 より下位バージョンである SSL 3.0 が指定された場合は、下位バージョンに切り替えて接続を試みます。本現象は、下位バージョンへの切り替え処理が行われ際に、.NET Framework からエラーが返され通信エラーとなります。

**【シーケンス図による現象の説明】**

発生条件に該当する環境にて SSL 通信した場合、以下の流れにより通信エラーが発生します。




(1) Client Hello

クライアント側（ACMS Lite Neo）が以下の情報をサーバーへ送信します。

・**バージョン「TLS 1.0」**

・**暗号化アルゴリズム「TLS 1.0 で使用可能な暗号化アルゴリズムリスト」**

(2) Server Hello

サーバー側は以下の情報をクライアント側へ返信します。

・**バージョン「SSL 3.0」**

・**暗号化アルゴリズム「サーバーが選択したアルゴリズム」**

サーバーにて下位のバージョン「SSL 3.0」が指定される。また「TLS 1.0 で使用可能な暗号化アルゴリズムリスト」の中から任意のアルゴリズムが指定される（通常セキュリティの高いものが指定される）

(3) SSL バージョンを切り替え

クライアント側は SSL バージョンの切り替え処理を行います。このとき**「Algorithm Mismatch」**が発生します。

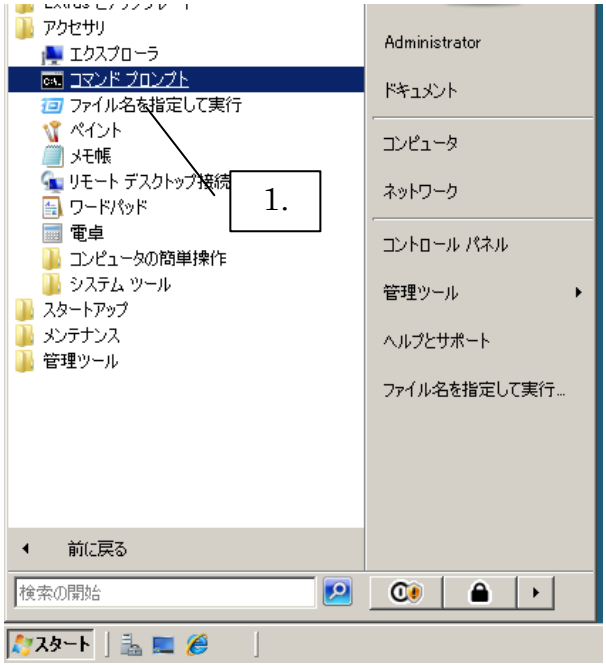
## 4. 通信エラーの原因

発生条件に該当する OS では、サーバーが選択した暗号化アルゴリズム（確認されているアルゴリズムとしては「TLS_RSA_WITH_AES_128_CBC_SHA」） を「SSL 3.0」がサポートしていません。このため、ACMS Lite Neo が使用している.NET Framework にて SSL バージョンと暗号化アルゴリズムの組み合わせエラー（Algorithm Mismatch）が発生し通信エラーとなります。

## 5. 回避方法

(1)「Administrator」権限のユーザーでログインします。

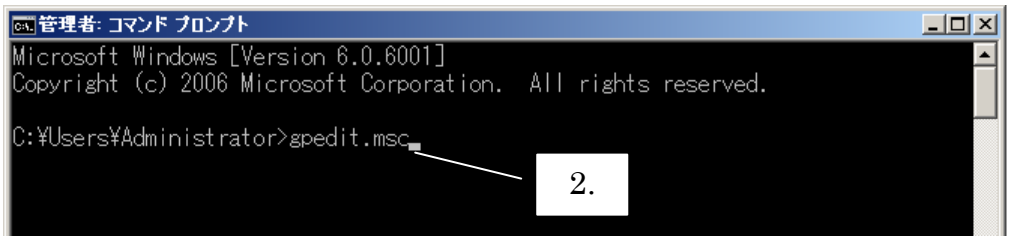
「スタート」メニューから、「すべてのプログラム」-「アクセサリ」-「コマンド プロンプト」を選択して下さい。




[Windows 7 の場合]

(2)「コマンド プロンプト」画面にて以下のコマンドを実行して下さい。

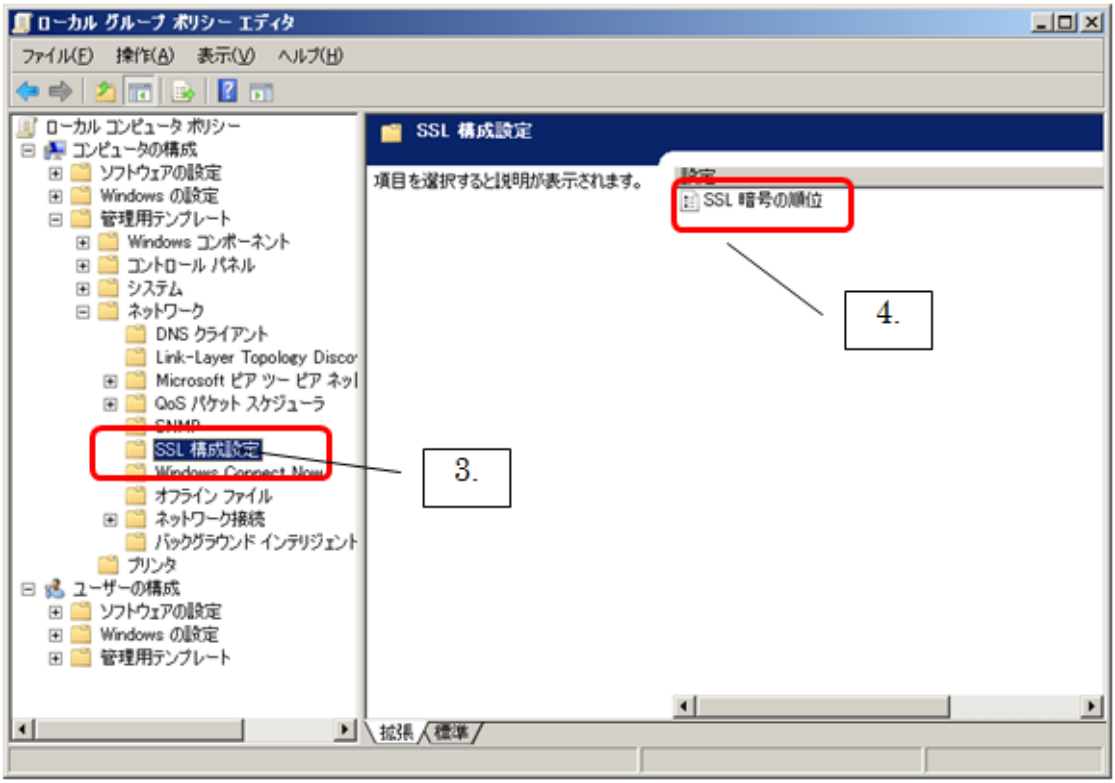
**> gpedit.msc**




[コマンドプロンプト]

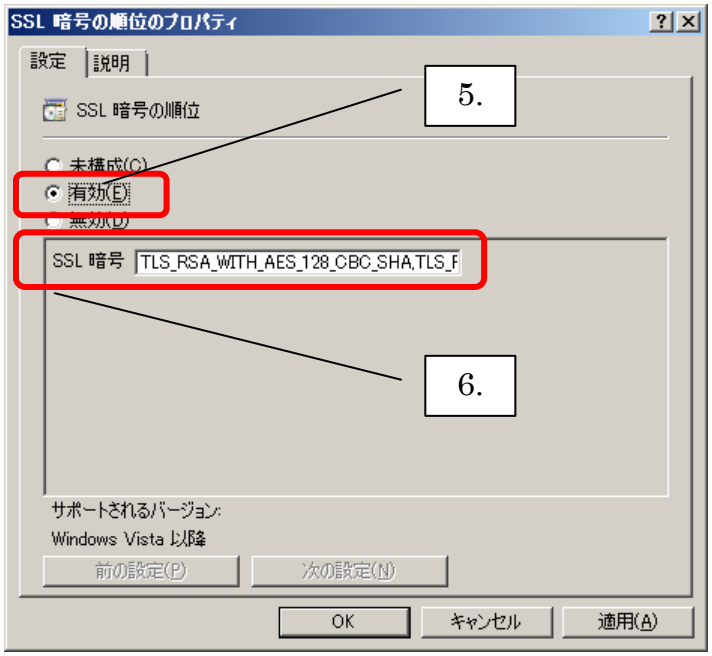
(3)「ローカル グループ ポリシー エディタ」画面が起動します。左側のツリービューから、「コンピュータの構成」-「管理用テンプレート」-「ネットワーク」-「SSL 構成設定」を選択して下さい。

(4)右側の「SSL 暗号の順位」をダブルクリックして下さい。




[ローカル グループ ポリシー エディタ]

(5)「SSL 暗号の順位のプロパティ」画面が起動しますので、「有効」ラジオボタンを選択して下さい。




[SSL 暗号の順位のプロパティ]

(6)「SSL 暗号」が入力できるようになるので、一旦初期値をすべてコピーしメモ帳に保存して下さい。元に戻す場合を考慮し、初期値を保管して下さい。

(7)「SSL 暗号」の初期値をすべて削除し、以下の文字列を新たに入力して「OK」ボタンをクリックして下さい。改行や間にスペースが入らないようご注意下さい。

TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_MD5,TLS_RSA_WITH_NULL_MD5,TLS_RSA_WITH_NULL_SHA

(8）最後に OS を再起動し、通信が正常終了することをご確認下さい。

以上