

概要

WEBサーバのSSLを更新後、クライアントからの接続時にサーバー認証でエラーが発生する。(ブラウザの場合は警告ダイアログ、自動送受信パックの場合はエラーとなる)

【現象詳細】

WEBサーバのSSLの更新を行ったところ、取引先の自動送受信パックでエラーが発生するようになります。

ERROR: Server 認証

HTTPエラーが発生しました。

エラー番号: 12045

メッセージ: サーバの証明書を発行した認証局が不明です。

また、ブラウザからログインする場合も、不正なSSLとして警告ダイアログが表示されます。

【対象リリース】

BACREXサーバ全ての製品

【発生原因】

SSLの更新により、1024bitから2048bitの証明書に変更された場合、WEBサーバ側のルート証明書と、クライアント側のルート証明書の整合性が取れなくなることで、エラーが発生します。

【発生条件】

以下2つの条件を満たす場合

- ① WEBサーバで1024bitから2048bitの証明書に更新した場合。
- ② クライアントPCでWindows Updateにて、「ルートCA証明書の更新」を行っていない場合。

【回避策】

以下2つの方法があります。

- ① Windows Updateから、「ルートCA証明書の更新」を行う。
 - ※ 「ルートCA証明書の更新」をするには、[コントロールパネル]-[プログラムの追加と削除]-[Windowsコンポーネントの追加と削除]にて、「ルート証明書の更新」チェックボックスをオンにしてください。(Windows XPの場合)
- ② 正常にログインできる(「ルートCA証明書の更新」を行った)PCより「ルートCA証明書」をエクスポートし、エラーが発生するPCにインポートします。
 - エクスポートするルート証明書は、WEBサーバで使用しているSSL発行元にマッチしたルート証明書をエクスポートします。
 - ※ 警告の発生しないPC上でIEを起動します。
 - [ツール]-[インターネット オプション]-[コンテンツ]タブ-[証明書]-[信頼されたルート証明機関]タブで該当するルート証明書をエクスポートします。
 - エクスポートしたファイルを指定して、警告が発生するPC上でインポートします。

例) 以下はWEBサーバがインテック社EINS/PKIパブリック証明書を利用している場合にエクスポートする際の例です。

