2013 年 10 月 3 日

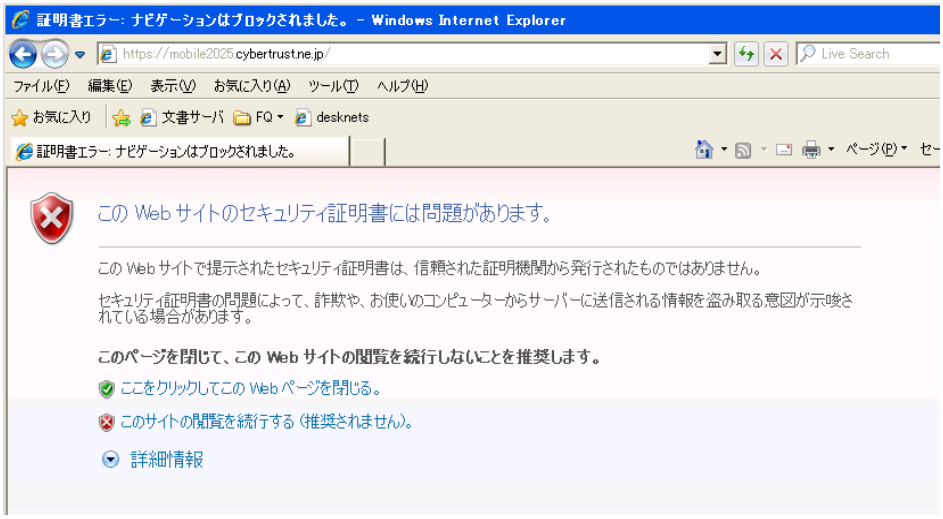
お客様各位

日経テレコン SSLサーバー証明書の更新について

日本経済新聞デジタルメディア

日経テレコンは SSL によるセキュアな接続を提供するために、サービス用サーバーに SSL サーバー証明書（以下、サーバー証明書）を利用しています。安全性を保証し続けるために証明書は1～3年に1度、更新の必要があります。

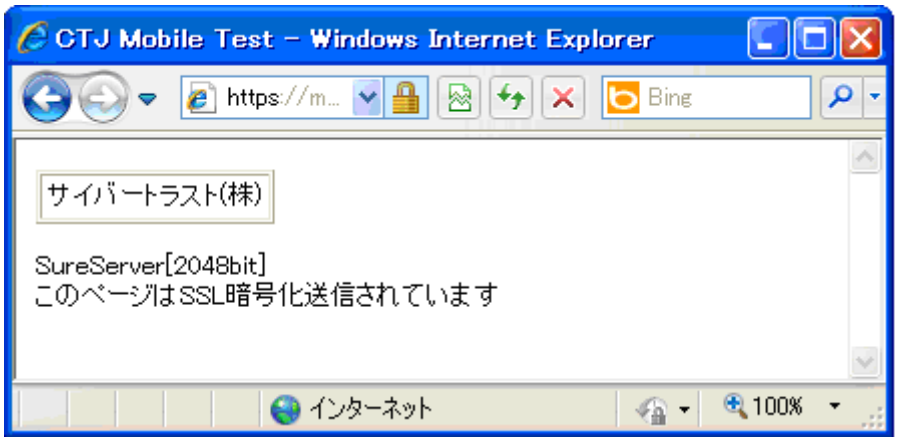
2013 年 10 月 21 日（月）未明に日経テレコンのサーバー証明書を更新する予定です。新しい証明書は、より安全性を強化し、鍵長が 2048bit になります※注。パソコンがウィンドウズアップデートを適用していれば、何の影響もありません。しかし、ウィンドウズアップデートの状況（長い間アップデートしていない、など）によっては日経テレコンに SSL 接続すると以下のようなセキュリティ警告が発生することになります。



(1)事前にパソコンに影響がないか確認する方法

パソコンから下記の URL にアクセスして、以下の画面が表示されるかどうか確認します。

https://mobile2025.cybertrust.ne.jp/



上記画面が表示されれば新しいサーバー証明書に対応済みですので、問題ありません。上記 URL はサイバートラスト社が、2048bit サーバー証明書の確認用に一般公開しているページです。

(2)前ページの画面が表示されない場合、またはサーバー証明書更新後にSSL接続でセキュリティ警告が発生した場合は、以下の対策でのご対応をお願い致します。

https://www.cybertrust.ne.jp/ssl/support/faq/tech_faq01.html#19

Q.「条件や対策方法について」

Q. 条件や対策方法について

A.

2014年以降、Microsoft社がSureServer(1024bit)のルート証明書「GTE CyberTrust Global Root」をはじめとした世の中の1024bitのルート証明書の利用を終了させることを弊社では想定しております。
様々な条件を想定して弊社で調査を実施したところ、**Web訪問者のPCが以下複数の条件にすべて一致する場合にセキュリティ警告が発生することを確認しております。**

- SureServer[2048bit]用クロスルート方式、もしくはSureServer EV[2048bit]をご利用の場合
- Web訪問者のPCがWindows XPで、かつ、Internet Explorer 、Chrome、Safari を利用している場合
- Web訪問者のPCにルート証明書が搭載されていない場合
- Microsoft社がWindows Updateにおいて「KB2607712」「KB2718704」相当の更新プログラムを提供した場合

※携帯電話やスマートフォンなどの携帯端末、Windows 7やMac OSなどのWindows XP以外のOS、Firefox などのその他ブラウザではセキュリティ警告は発生しません。

そのため弊社では、セキュリティ警告発生回避のため、お客様への事前対策について以下にご案内いたします。

No	対策		対応者
1	クロスルート方式から3階層へ変更する(※)		サーバ運営者
2	予め2048bitルート証明書をPC環境へインストールする	1. マイクロソフト提供のrootsupd.exeを実行する	Web訪問者
		2. 2048bitルート証明書のファイルを開く ・SureServer[2048bit] のルート証明書 ・SureServer EV[2048bit]のルート証明書	Web訪問者
		3. Webサイトへ「Root Upgrader」を掲載する	サーバ運営者

※携帯端末の非対応機種が増加いたしますが、時間経過とともに非対応機種の実質アクセス率の低下が予測されます。
また、弊社では実質アクセス率の調査を定期的に実施しており、随時お知らせいたします。

注)米国標準技術研究所(NIST)が 2005 年に定めた米政府系システムで使用する暗号の基準(SP 800-57)で、2011 年以降は2048bit 以上の RSA 鍵長を用いた証明書を使用することを推奨しています。
日経テレコンで採用している SSL 証明書の発行元であるサイバートラスト社でも 1024bit の証明書の提供は 2014 年以降は行わない方針となっています。