GeoTrust®

ジオトラスト

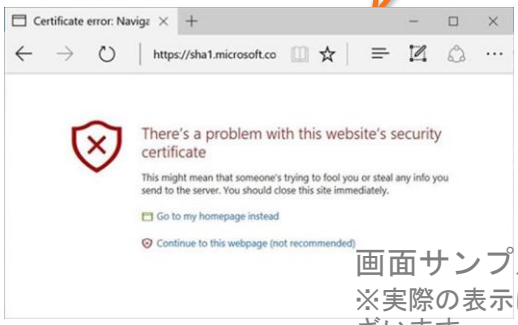
ブラウザベンダにおけるSHA-1版証明書に対する警告表示について

2016年10月（更新）

日本ジオトラスト株式会社

Microsoft Internet Explorerにおける SHA-1のSSLサーバ証明書に対する警告表示

	ウェブサイトでご利用中のSSLサーバ証明書の 署名アルゴリズムと有効期間		
署名ｱﾙｺﾞﾘｽﾞﾑ	SHA-1		SHA-2
証明書発行日	～2016/12/31	2017/1/1～	-
Internet Explore 11 ～　2017/2/13	鍵マークなし	鍵マークなし	
Internet Explore 11 2017/2/14　～	警告画面	警告画面	



画面サンプル
※実際の表示は異なる場合がございます。

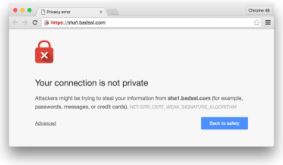
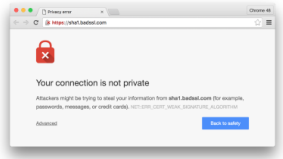
ご参考）
Windows Enforcement of SHA1 Certificates

http://social.technet.microsoft.com/wiki/contents/articles/32288.windows-enforcement-of-authenticode-code-signing-and-timestamping.aspx

ご注意ください）
本資料は2016年10月時点の情報をもとに作成しています。各ブラウザベンダの仕様に関する詳細は各社へお問い合わせください。

GeoTrust®

Google Chromeにおける SHA-1のSSLサーバ証明書に対する警告表示 (2)

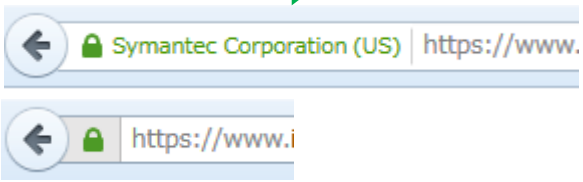
<table>
<tr><th></th><th colspan="4">ウェブサイトでご利用中のSSLサーバ証明書の署名アルゴリズムと有効期間</th></tr>
<tr><td>署名ｱﾙｺﾞﾘｽﾞﾑ</td><td colspan="3">SHA-1</td><td>SHA-2</td></tr>
<tr><td rowspan="3">Chrome 48～
(2016/1/20 ﾘﾘｰｽ)</td><td colspan="3">証明書有効期間終了日</td><td>-</td></tr>
<tr><td>～
2015/12/31</td><td>2016/1/1～
2016/5/31</td><td>2016/6/1～
2016/12/31</td><td>2017/1/1～</td></tr>
<tr><td>  </td><td>  </td><td>  </td><td>  </td><td rowspan="2">  </td></tr>
<tr><td colspan="3">証明書有効期間開始日
2016/1/1～
  </td></tr>
<tr><td>Chrome 56～
(2017年1月予定)</td><td colspan="3">・End-Entity証明書、または中間CA証明書にSHA-1を利用している、または
・2016年1月1日以降に発行されている
・Public ルートにチェーンする証明書（※）
※ローカルに保存されているルート証明書にチェーンするSHA-1版証明書を利用している場合はブラウザ上エラー表示にはしないがネットワークエラー（鍵マークのアイコン）として表示する。
  </td><td></td></tr>
</table>

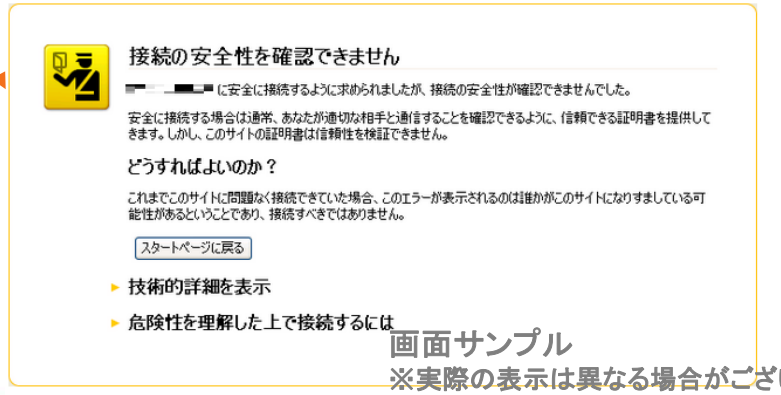
ご参考）
A further update on SHA-1 certificates in Chrome
https://www.chromium.org/Home/chromium-security/education/tls/sha-1

ご注意ください）
本資料は2016年10月時点の情報をもとに作成しています。各ブラウザベンダの仕様に関する詳細は各社へお問い合わせください。

Firefox における SHA-1のSSLサーバ証明書に対する警告表示

	ウェブサイトでご利用中のSSLサーバ証明書の署名アルゴリズムと有効期間		
署名ｱﾙｺﾞﾘｽﾞﾑ	SHA-1 ～2016/12/31		SHA-2 -
証明書の発行日	～2015/12/31	2016/1/1～	
Firefox 45			
Firefox 51～	Untrusted connection		





画面サンプル
※実際の表示は異なる場合がございます。

※1 参考）
SHA-1版証明書を利用したサイトへの警告表示は段階的に行う旨を告知しています。
Phasing Out SHA-1 on the Public Web
https://blog.mozilla.org/security/2016/10/18/phasing-out-sha-1-on-the-public-web/

ご注意ください）
本資料は2016年10月時点の情報をもとに作成しています。各ブラウザベンダの仕様に関する詳細は各社へお問い合わせください。

GeoTrust