参考資料

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

2015年 12月更新

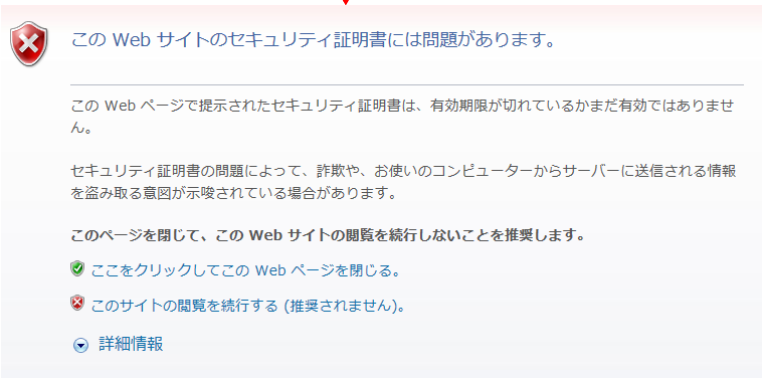
2016年 4月更新

合同会社シマンテック・ウェブサイトセキュリティ

本件に関するお問合せ先 : 合同会社シマンテック・ウェブサイトセキュリティ　テクニカルサポート
Email : server_info_jp@symantec.com
電話 : 03-5114-4135（音声ガイダンス後、2番を選択してください）（平日9時30分～17時30分）

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		
署名ｱﾙｺﾞﾘｽﾞﾑ	SHA-1		SHA-2
利用日	～2016/12/31	2017/1/1～	-
Internet Explore			



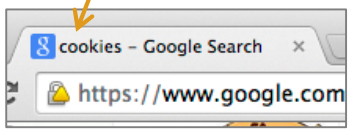
画面サンプル
※実際の表示は異なる場合がございます。

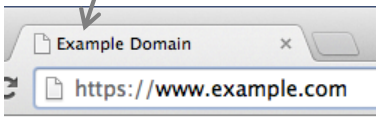
ご参考）
~~2016年6月1日以降、SHA-1版SSLサーバ証明書を利用しているサイトに対して警告画面を表示することを検討しています。~~(2016年4月時点前倒しはなくなりました)
http://social.technet.microsoft.com/wiki/contents/articles/32288.windows-enforcement-of-authenticode-code-signing-and-timestamping.aspx

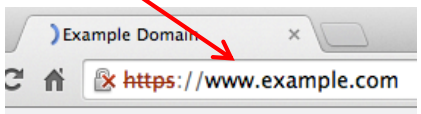
ご注意ください）
本資料は2015年11月時点の情報をもとに作成しています。各ブラウザベンダの仕様に関する詳細は各社へお問い合わせください。

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

	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
証明書有効期間終了日	～2015/12/31	2016/1/1～2016/5/31	2016/6/1～2016/12/31	2017/1/1～	-
Chrome 39 (2014/11/18リリース)					
Chrome 40 Chrome 41					
Chrome 42～ (2015/4/28リリース)					
Chrome 46～ (2015/10/13リリース)					

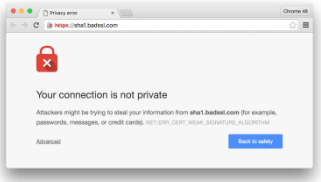
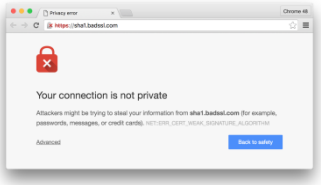






ご注意ください） 本資料は2015年12月時点の情報をもとに作成しています。各ブラウザベンダの仕様に関する詳細は各社へお問い合わせください。

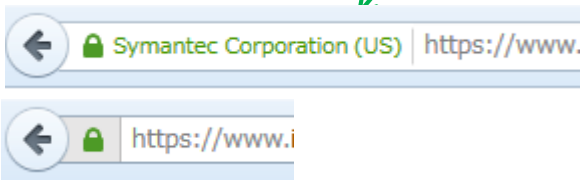
Google Chromeにおける SHA-1のSSLサーバ証明書に対する警告表示 (2)

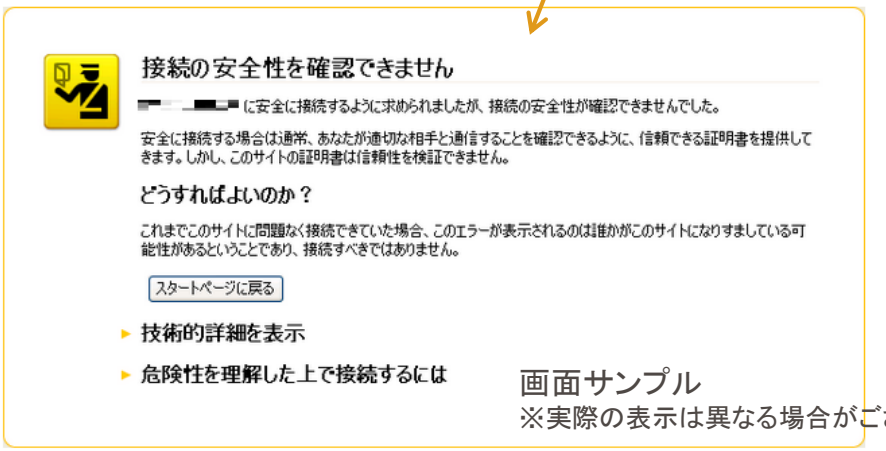
<table>
<tr><th></th><th colspan="4">ウェブサイトでご利用中のSSLサーバ証明書の署名アルゴリズムと有効期間</th></tr>
<tr><td>署名ｱﾙｺﾞﾘｽﾞﾑ</td><td colspan="3">SHA-1</td><td>SHA-2</td></tr>
<tr><td rowspan="3">Chrome 48～
(2016年ﾘﾘｰｽ予定)</td><td colspan="3">証明書有効期間終了日</td><td>-</td></tr>
<tr><td>～2015/12/31</td><td>2016/1/1～
2016/5/31</td><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 XX～
(2016年ﾘﾘｰｽ予定)</td><td colspan="4">・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></tr>
</table>

ご参考） Google社では、2016年7月1日以降、SHA-1版SSLサーバ証明書を利用しているサイトに対してエラーを表示することを検討しています。
https://googleonlinesecurity.blogspot.jp/2015/12/an-update-on-sha-1-certificates-in.html

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-1** 2017/1/1※～ （証明書の発行日に関わらず）	**SHA-2** -
証明書の発行日	～2015/12/31	2016/1/1～		
～Firefox 42			Untrusted connection	
Firefox 43～		Untrusted connection	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。

※ 適用日を2016年7月1日以降に前倒しすることを検討しています。
https://blog.mozilla.org/security/2015/10/20/continuing-to-phase-out-sha-1-certificates/

ご注意ください）
本資料は2015年11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。