

SHA-1証明書の受付終了(2015年12月)とSHA-2証明書への移行について

署名アルゴリズムを「SHA-1」とするSSLサーバー証明書(以下、SHA-1証明書とします。)の受付終了と、署名アルゴリズムを「SHA-2」とするSSLサーバー証明書(以下、SHA-2証明書とします。)への移行についてご案内します。

1. SHA-1証明書に関する指針について

「SHA-1」のSSLサーバー証明書に関するブラウザベンダの指針は以下です。

※SHA-1の中間CA証明書も下記指針の対象です。

※2014年9月時点の情報に基づく内容のため、今後変更される可能性がございます。あらかじめご了承ください。

■各ベンダのSHA-1証明書に対する指針スケジュール

SHA-1証明書における指針		2014年	2015年	2016年	2017年～
Microsoft	WindowsにおけるSHA-1証明書サイトへのSSL通信	~2016年12月31日までOK			SSL通信拒否
Google	ChromeによるSHA-1証明書サイトへのSSL通信	OK	SHA-1証明書の有効期間に応じて(2017年1月以降、2016年7月以降)、2014年11月から段階的にアドレスバー表示を変更		
Mozilla	FirefoxによるSHA-1証明書サイトへのSSL通信	OK	2015年早期から有効期間が2017年以降の証明書で警告		SSL通信拒否

◆Microsoft社の指針

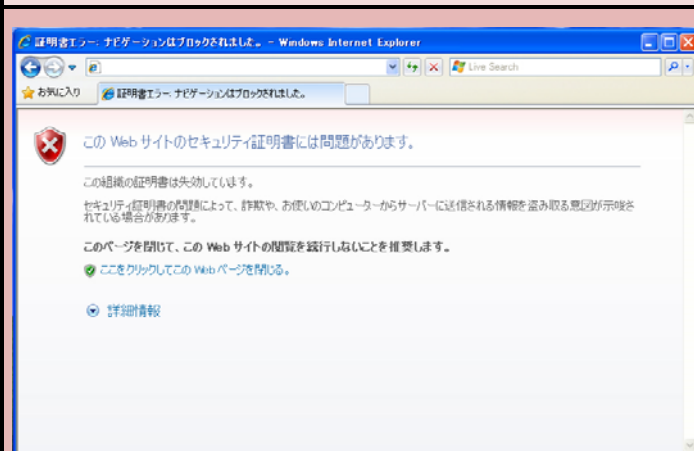
Microsoft社は2013年11月に発表した「Windows Root Certificate Program - Technical Requirements version 2.0」において、SHA-1証明書に関する下記の指針を表明しました。

- ・ 認証局は、2016年1月1日までに新しいSHA1 SSLおよびコード署名証明書の発行を停止しなければならない。
- ・ Windowsは2017年1月1日でSHA1証明書でのSSL通信を拒否する。

■影響

SSLサーバー証明書を発行する認証局は上記指針に従い、2015年12月31日までにSHA-1証明書の発行を停止する必要があります。また、2017年1月1日以降、SSLサーバー証明書の発行元に関わらず、Windows製品でSHA-1証明書のSSL通信が拒否されます。

<セキュリティ警告表示例(予定)>



※選択肢がなく、次の画面へ遷移できません。

<通常のセキュリティ警告表示例>



※選択肢があり、続行すると次の画面へ遷移できます。


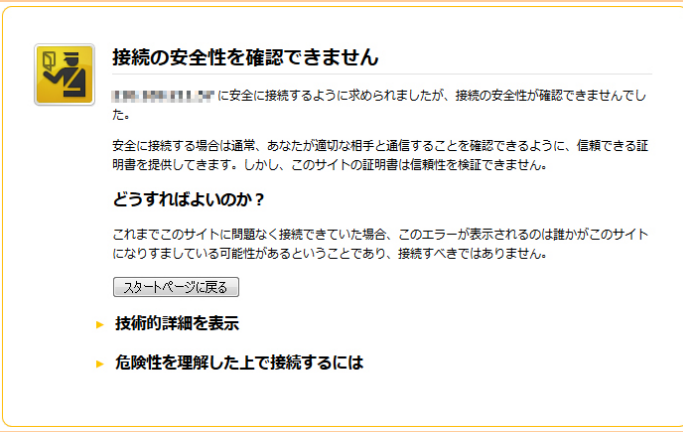
◆Googleの指針

Googleは2014年9月にChromium Blogにて発表した「Gradually Sunsetting SHA-1」において、SHA-1証明書が使用されているWEBサイトへのSSL接続において、これからリリース予定のChrome39 ~ 41で段階的にアドレスバーの表示を変化させることを表明しました。

■Chrome 39 (2014年11月中旬リリース)	
満了日が2017年1月1日以降のSHA-1証明書	
	
※黄色マーク付き鍵アイコンが表示されます	
■Chrome 40 (2015年1月頃リリース予定)	
満了日が2016年6月1日から2016年12月31日のSHA-1証明書	満了日が2017年1月1日以降のSHA-1証明書
	
※黄色マーク付き鍵アイコンが表示されます	※鍵アイコンなし、http 同等
■Chrome 41 (2015年3月頃リリース予定)	
満了日が2016年1月1日から2016年5月31日のSHA-1証明書	満了日が2017年1月1日以降のSHA-1証明書
	
※黄色マーク付き鍵アイコンが表示されます	※赤いXマーク付き鍵アイコンとhttps取り消し線が表示されます

◆Mozillaの指針

Mozillaは2014年9月にMozilla Security Blogにて発表した「Phasing Out Certificates with SHA-1 based Signature Algorithms」において、SHA-1証明書の発行と利用の非推奨、およびSSL接続時の表示変更に関する以下の指針を表明しました。

■2015年初期にリリース予定のFirefox	■2015年初期のリリース後に追加が計画されている動作
<p>・満了日が2017年1月1日以降のSHA-1証明書</p> <p>※アドレスバーに混合コンテンツ同様の警告</p> 	<p>・2016年1月1日以降、新たに発行されたSHA-1証明書 ・満了日が2017年1月1日以降におけるすべてのSHA-1証明書</p> <p>※「信頼されない接続」である旨のエラーを表示</p> 

※2017年以降のある時点において、コンテンツを表示できない(エラーを無視できない)状況にする可能性有り

◆ご利用中のサーバについて

各ブラウザの警告表示を回避するには、適正な期限までにSSL証明書を運用されているサーバにて現在ご利用中のSHA-1証明書から次世代のSHA-2証明書に入れ替えて頂く必要があります。

ご利用中のサーバのOSによりサーバ側の対応状況が異なって参ります。対応方法をそれぞれ記載致しますので下記詳細をご確認ください。

○RHEL5以降をご利用のお客様 ⇒ [RHEL5、RHEL6、CentOS6] SHA-2対応OS

- ・SHA-2証明書を取得し、対象サーバにインストールする事で対応可能です。
- ・SHA-2証明書へ切り替える際、各端末(フューチャーフォン、PHS)やブラウザの対応状況異なってまいりますので注意が必要です。
対応状況については後述の『SHA-2対応版SSL証明書 PCブラウザ・モバイル・サーバー対応について(予定)』をご参照ください。

○RHEL4を含むレガシーOSをご利用中のお客様 ⇒ [RHEL ES4、RHEL ES3、etc...] ※SHA-2非対応OS

- ・対象のOS(サーバ)はハッシュアルゴリズムSHA-2に対応しておらず、インストールする事ができません。
SHA-1証明書が使用可能な**2016年12月末までに、SHA-2に対応した現行OSへサーバをリプレース**し、SHA-2証明書をインストールする必要があります。

※注意: SHA-1証明書を2016年12月末まで使用される場合、前述のとおり各ブラウザにて警告表示がされます。

◆SHA-2対応版SSL証明書 PCブラウザ・モバイル・サーバー対応について(予定)

※SSL証明書認証局調べ

クライアントカバレッジ(PCブラウザ)

PC

OS		ブラウザ	SHA-2対応	備考
Microsoft Windows	XP SP3 以降で対応	Internet Explorer	○	IE ver.6以降
		Google Chrome	○	Chrome 1.0以降
		Opera	○	Opera 9.5以降
	OSのバージョン問わず	Mozilla Firefox	○	Firefox 1.0.0以降
Mac OS X		Safari	○	Safari2.0以降
		Mozilla Firefox	○	Firefox 1.0.0以降

携帯電話(フューチャーフォン)

OS	ブラウザ	SHA-2対応	備考
フューチャーフォン	標準搭載ブラウザ	約7割	※アクセスシェアベース ⇒端末全てに対する割合ではございません

スマートフォン

OS	ブラウザ	SHA-2対応	備考
Android	標準搭載ブラウザ(Android)	○	IE ver.6以降
iOS	標準搭載ブラウザ(Safari)	○	Chrome 1.0以降
Windows Phone	標準搭載ブラウザ(IE Mobile)	○	Opera 9.5以降
Blackberry	標準搭載ブラウザ(Blackberry)	○	Firefox 1.0.0以降

サーバ

	備考	SHA-2対応
Apache	Openssl 0.9.8以降	○
Windows Server	IIS6.0 以降 (IIS6.0の場合KB938397/KB968730要)	○

※重要: ロードバランサーに SSL 証明書をインストールされている場合は、対象機器が SHA-2 証明書に対応しているか確認する必要があります。