SSLサーバ証明書

SHA-1から SHA-2への移行

GlobalSign®
GMO INTERNET GROUP

目次

概要

SHA-1ハッシュ関数の危殆化を背景に、NIST(アメリカ国立標準技術研究所)は、2010年までにSHA-2へ移行することを勧告していましたが、SHA-2ハッシュ関数の普及が進まず2011年に"非推奨"という表現に変更しました。

その後2013年11月に、Microsoft社はSHA-1ハッシュ関数を用いたSSLサーバ証明書の受け入れを2017年1月以降不可とする『SHA-1廃止ポリシー』を発表しました。
※2016年5月現在、Microsoft社によるSHA-1 SSLサーバ証明書の受け入れ終了日は、2017年2月14日と発表されています。

グローバルサインでは、ご利用中のSSLサーバ証明書のSHA-2への移行を推奨しております。

SHA-1廃止ポリシー

1) 認証局は2016年1月1日までに新たなSHA-1　SSLサーバ証明書の発行をやめなければならない。

2) SSLサーバ証明書については、Windowsは2017年2月14日までにSHA-1証明書の受け入れを中止する。

※上記は弊社による部分訳です。詳細は以下の原文をご確認ください。
FAQ: SHA-1 廃止/SHA-2 移行に関するマイクロソフトのポリシー

本件に関するこれまでの経緯と今後の動き

2004年	NISTが「SHA-1は2010年までに運用を終了し、SHA-2(SHA-224、SHA-256、SHA-384、SHA-512の総称)に移行する」計画を発表
2011年	NISTがSHA-2への移行が進んでいない実情を容認する形で、「非推奨であることを認識する」「リスクを認識したうえで利用する」ことを前提に、2013年末までのSHA-1利用の許容
2013年	MicrosoftがSHA-1廃止ポリシーを発表
2014年4月	グローバルサインにてSHA-2(SHA256)証明書の提供開始
2015年12月	グローバルサインでは2015年12月31日をもってSHA-1SSLサーバ証明書の発行を停止
2015年12月	主要ブラウザ(Microsoft Internet Explorer、Google Chrome、Mozilla Firefox)では、2017年1月1日をもってWindows製品でのSHA-1証明書受け入れを停止
2016年4月	Microsoft社がSHA-1廃止ポリシーを更新し、SHA-1証明書の受け入れ終了日を2017年2月14日へ延期

SHA-1・SHA-2とは

SHA-1・SHA-2とは、ハッシュ関数の種類で、改ざん検知に利用される署名アルゴリズムのことです。
ハッシュ関数とは、テキストデータから別の固定長のテキストデータ(ハッシュ値)を生成する関数であり、生成されたハッシュ値を比較することでデータの改ざんを確認することができます。SHA-1とSHA-2でハッシュ値の長さが異なり、SHA-1は160ビット、SHA-2は224ビット・256ビット・384ビット・512ビットです。

SHA-2は、SHA-224・SHA-256・SHA-384・SHA-512の総称です。

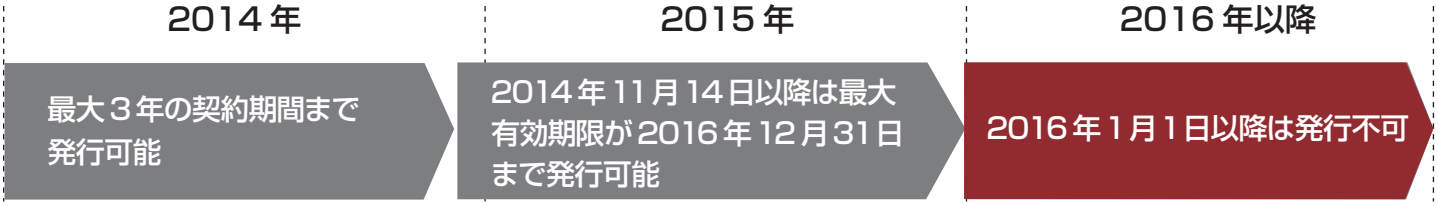
SHA-1証明書を使い続けるリスク

ハッシュ関数による改ざん検知は、同じデータから生成されるハッシュ値が一様であることを前提に成り立っています。ハッシュ値が短いと同一のハッシュ値を持つデータが発見される可能性が高くなり、安全性が低下します。コンピュータの計算能力の向上により、SHA-1の安全性が危ぶまれるようになったため、よりハッシュ値の長いSHA-2の利用が推奨されます。

SHA-1証明書に関する対応状況

SHA-1証明書の発行・再発行に関する弊社の対応

グローバルサインでは、SHA-1 SSLサーバ証明書の発行を終了いたしました。

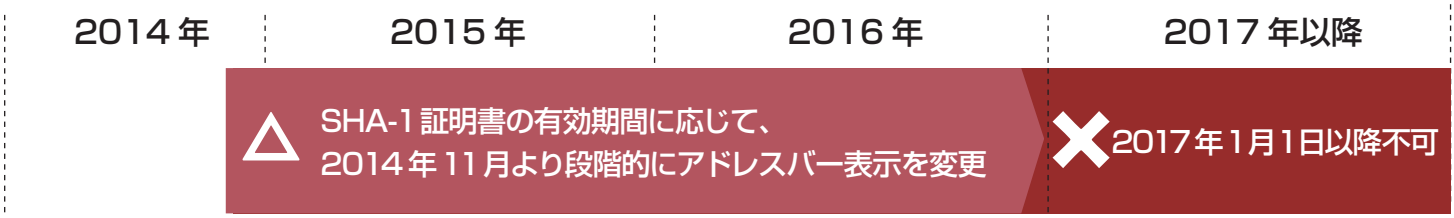


ブラウザ[Internet Explorer]の対応予定

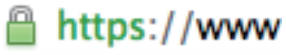
2017年2月13日までご利用可能ですが、2017年2月14日以降は利用できなくなります。

ブラウザ[Google Chrome]の対応予定

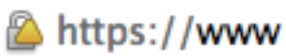
ブラウザのバージョンとSSLサーバ証明書の有効期限により以下の対応となります。



バージョン	証明書の有効期間終了日			
	～2015年12月31日	2016年1月1日～5月31日	2016年6月1日～12月31日	2017年1月1日～
39				
40・41				
42・43・44・45				
46				

 安全なHTTPSページ

 HTTPとマイナーエラーを含むHTTPSページ

 マイナーなエラーのあるHTTPSページ

 問題のあるSSLサーバ証明書を利用しているなど破損しているHTTPSページ

EV SSLの場合は、緑色の鍵アイコンにウェブサイトの運営組織が表示されます。

ブラウザ[Mozilla Firefox]の対応予定

以下の対応となります。

2016年1月1日以前に発行された証明書の場合	警告表示
2017年1月1日以降	すべてのSHA-1 SSLサーバ証明書が利用不可

※ 各ブラウザの対応状況は、2015年12月1日時点の情報に基づき作成しています。各社の対応時期等は変更される場合があります。

ライブラリ・モバイル(携帯)端末対応状況 ※2014年12月調べ

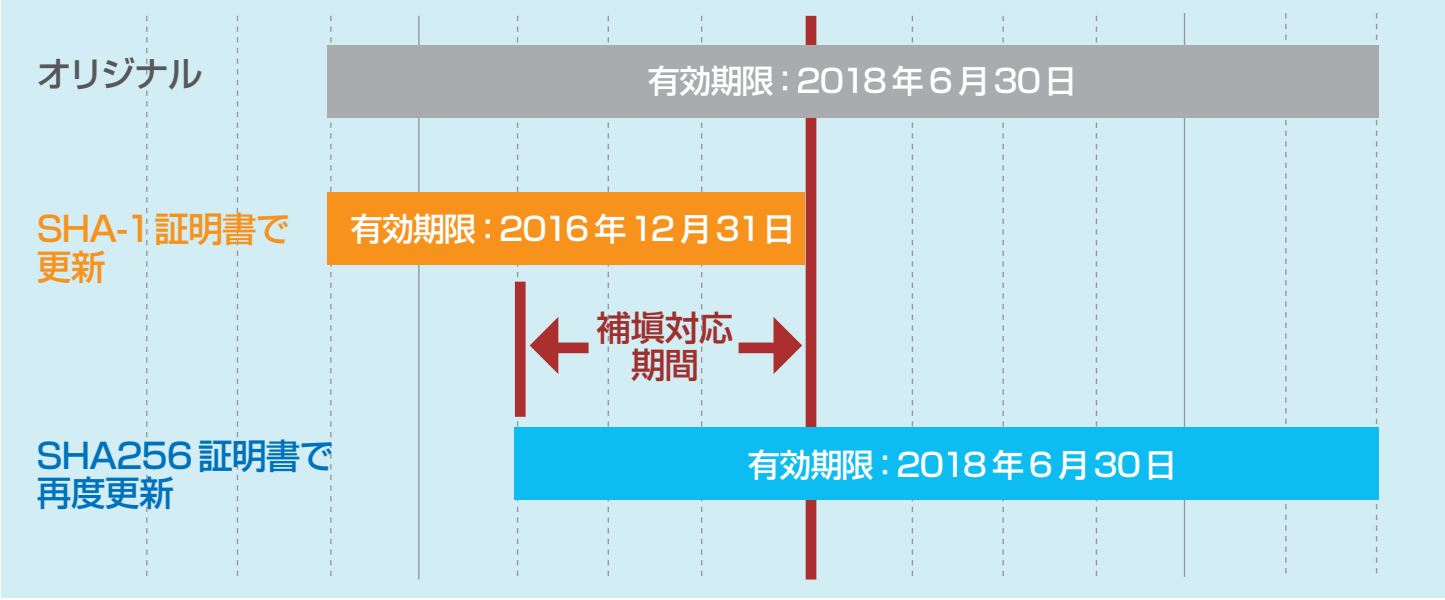
SHA-1証明書	【ライブラリ】 ・ORACLE JRE (1.7.0 以降、1.6.0_10 以降、1.5.0_16 以降、1.4.2_18 以降) ・NSS 3.11.10 以降 ・SeaMonkey 2 以降 【フィーチャーフォン】 ・2009年冬モデル以降 【スマートフォン】 ・100%対応
SHA256(SHA-2)証明書	【ライブラリ】 ・OpenSSL Project OpenSSL 0.9.8o 以降※ ・GnuTLS 1.7.4 以降 ・Oracle JRE (1.7.0 以降、1.6.0_17 以降、1.5.0_22 以降、1.4.2_19以降) ・ Mozilla NSS 3.11.10 以降 ・ Microsoft .NET 3.5 SP1 以降 ※ハッシュアルゴリズムのSHA256は、OpenSSL 0.9.8より搭載されておりますが、標準で有効になったのは0.9.8oからです。 【フィーチャーフォン】 ・2010年夏モデル以降 【スマートフォン】 ・iOS 4以降、Android 2.3以降対応

現在SHA-1 SSLサーバ証明書をご利用中のお客様へ

有効期限が2017年1月1日以降の場合、ご利用中に利用不可になる場合がございますので、2016年12月31日までにSHA256証明書での再発行（無償）のお手続きが必要です。

SHA-1 SSLサーバ証明書にて再発行をご希望のお客様へ

再発行（無償）可能な期間が2015年12月31日までとなります。
※2016年12月31日を超える残期間を有する証明書を2014年11月14日 18:00以降に再発行の手続きを行った場合は、有効期限が2016年12月31日までに短く変更のうえ再発行されます。
再発行により有効期間が短くなった証明書は、再度SHA256証明書にて再発行の手続きを行っていただくことにより、当初の有効期限までの証明書を発行いたします。



SHA-1 SSLサーバ証明書にて更新をご希望のお客様へ

SHA-1 SSLサーバ証明書でのお申し込み可能な最大契約期間、及び最大有効期限につきましては、以下をご確認ください。

	お申し込み可能な契約期間	発行可能な証明書の最大有効期限
クイック認証SSL・企業認証SSL	半年・1年	2016年12月31日
EV SSL	1年	2016年12月31日

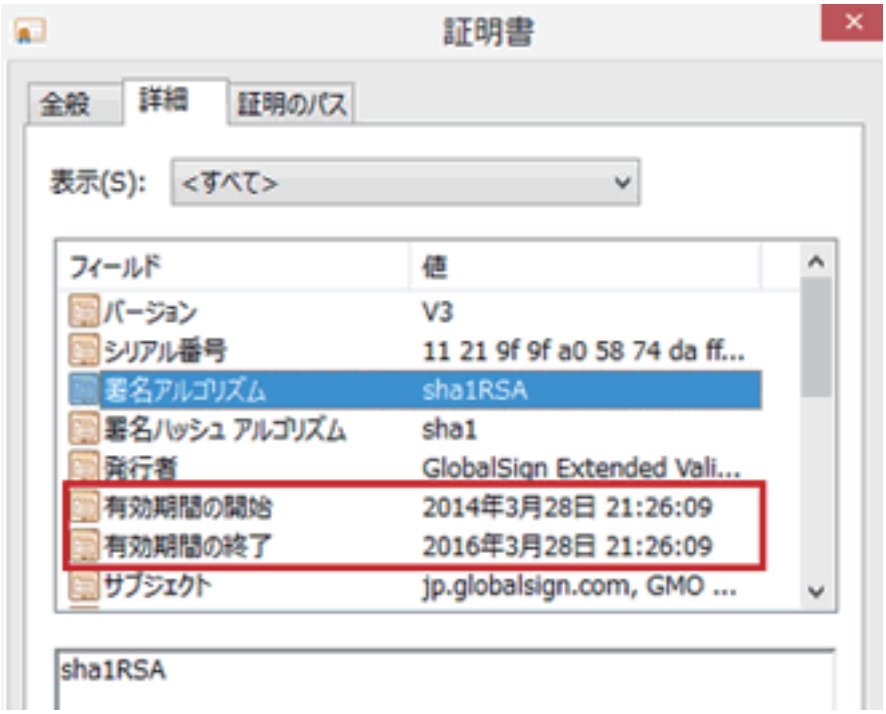
※SHA-1 SSLサーバ証明書の最大有効期限は2016年12月31日までとなるため、「更新」や「乗り換え」等において有効期限の延長期間が短くなる場合がございます。
※2014年11月17日以降に発行されるSHA-1 SSLサーバ証明書は、有効期間が2016年12月31日に制限されております。

証明書の有効期限・署名アルゴリズムの調べ方

証明書の有効期限の調べ方

Internet Explorerで確認

ブラウザの鍵マークをクリック後、「証明書の表示」をクリックしてください。



「詳細」タブをクリックし、「有効期間の終了」欄をご確認ください。

証明書の有効期限の調べ方

Firefox で確認

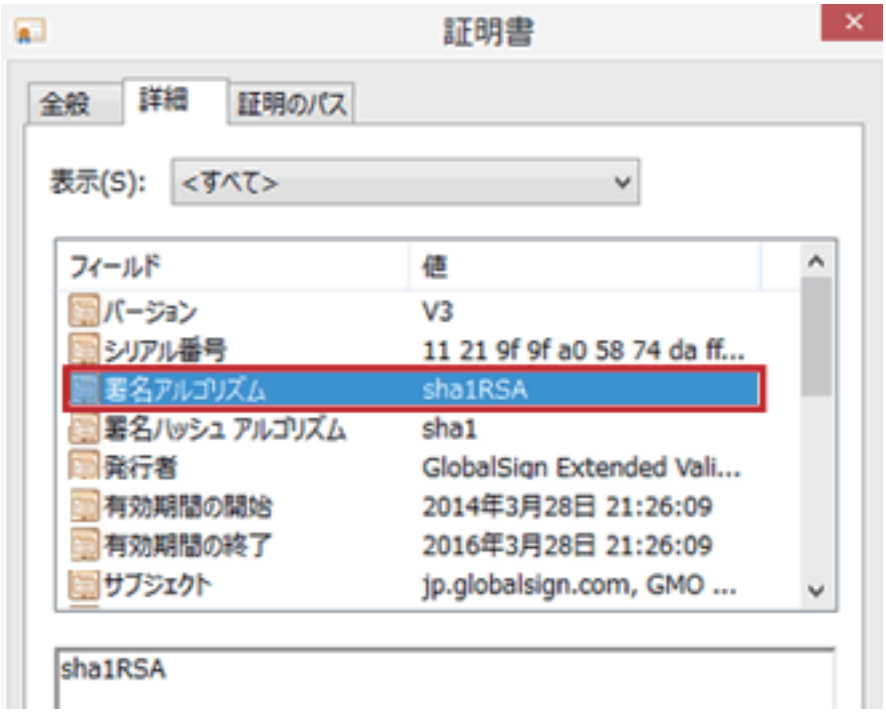
ブラウザの鍵マークをクリック後、「詳細を表示」をクリックしてください。

「一般」タブの「証明書の有効期間」欄をご確認ください。

署名アルゴリズムの調べ方

Internet Explorerで確認

ブラウザの鍵マークをクリック後、「証明書の表示」をクリックしてください。



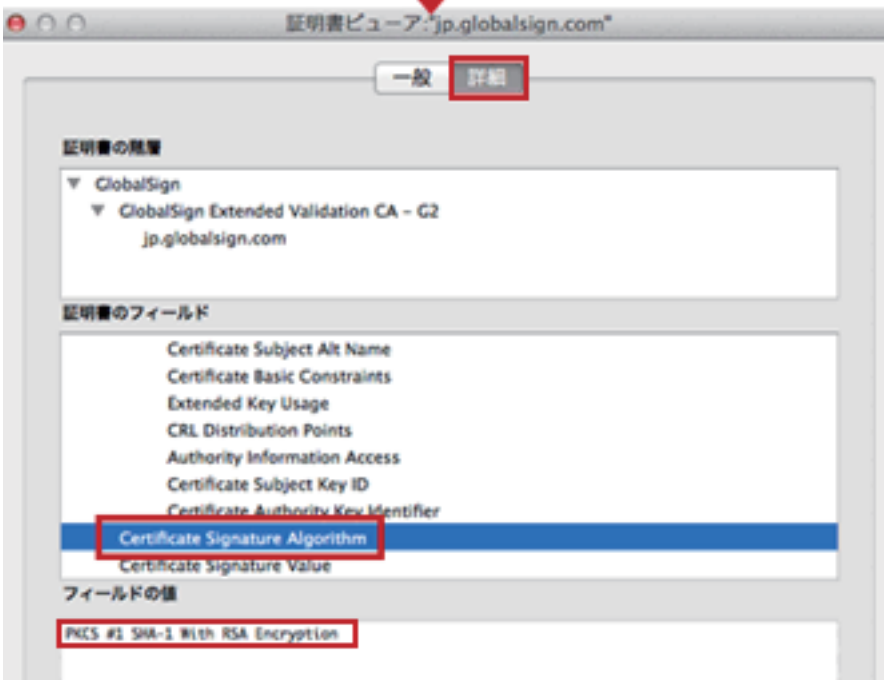
「詳細」タブをクリックし、「署名ハッシュアルゴリズム」欄をご確認ください。

署名アルゴリズムの調べ方

Firefox で確認

ブラウザの鍵マークをクリック後、「詳細を表示」をクリックしてください。

「詳細」タブの「Certificate Signature Algorithm」欄をご確認ください。



SHA-2証明書への移行手続きについて

再発行の手続きの流れ

SHA-2(SHA256)への移行期限(2016年12月31日)より証明書の有効期限が長い場合は、移行期限前に証明書の再発行のお手続きが必要となります。

1 事前準備	CSR(スキップ申し込みサービスをご利用の場合は不要)や審査に必要な書類を準備してください。
↓	
2 証明書再発行お申し込み	GSパネルにログイン後、対象の証明書を選択して、再発行のお申し込みをしていただきます。
↓	
3 署名ハッシュアルゴリズム選択	「SHA256」を選択してください。
↓	
4 再発行する証明書の確認	再発行ではディスティングイッシュネームを変更することができません。
↓	
5 証明書発行・インストール	発行された証明書をサーバにインストールしていただきます。

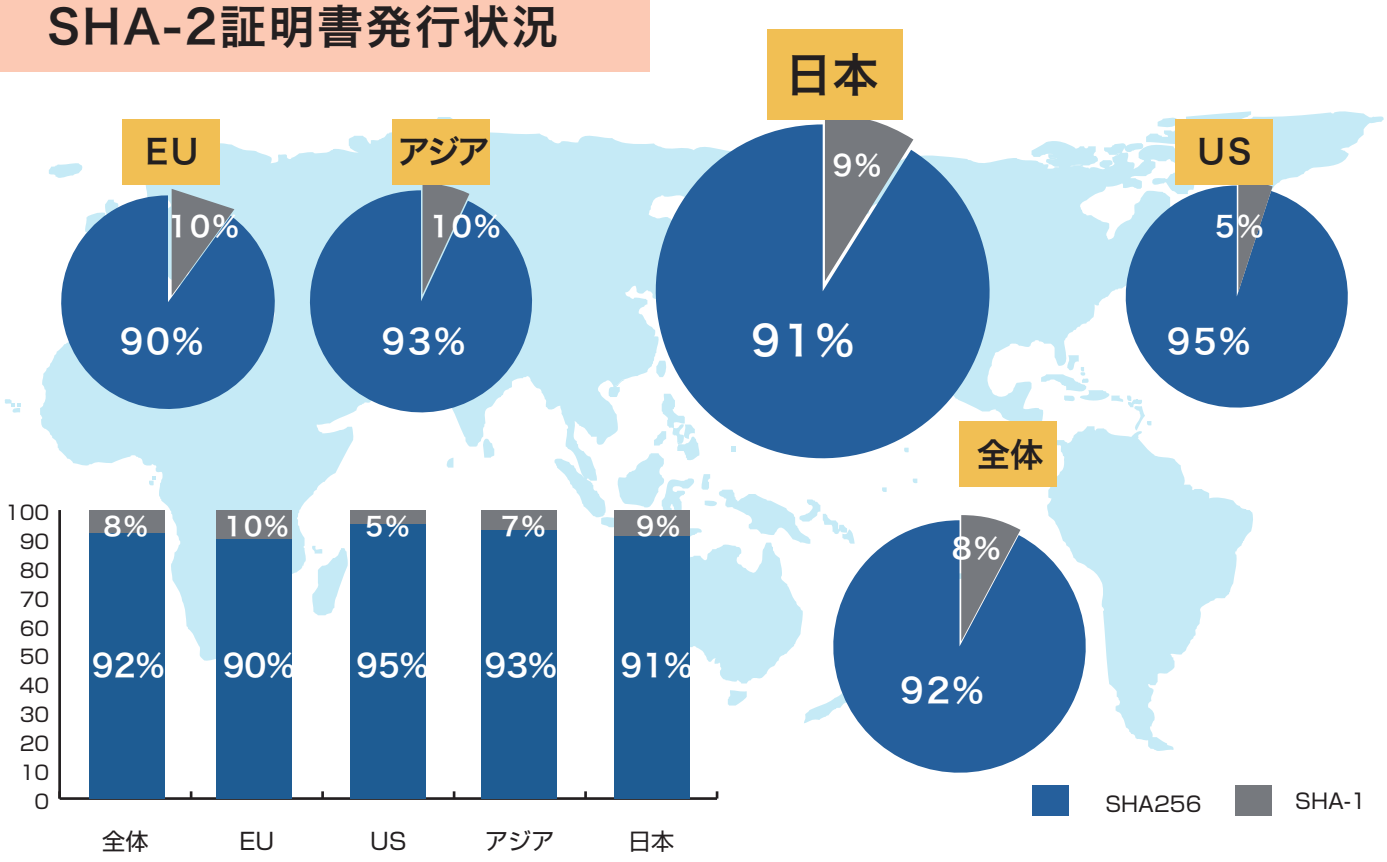
更新の手続きの流れ

SHA-2(SHA256)への移行期限前に更新を迎える場合は、証明書の更新時に署名ハッシュアルゴリズムの選択欄でSHA-2(SHA256)を選択してください。

1 事前準備	CSR(スキップ申し込みサービスをご利用の場合は不要)や審査に必要な書類を準備してください。
↓	
2 証明書更新お申し込み	GSパネルにログイン後、更新対象の証明書を選択してください。
↓	
3 署名ハッシュアルゴリズム選択	「SHA256」を選択してください。
↓	
4 証明書発行・インストール	発行された証明書をサーバにインストールしていただきます。

SHA-2証明書発行状況
よくある質問

SHA-2証明書発行状況



よくある質問

Q. 現在利用している証明書のハッシュ関数および有効期限を調べる方法を教えてください。

A. 本資料「証明書の有効期限・署名アルゴリズムの調べ方」をご参照ください。

Q. ハッシュ関数が判明したら、どのような対応を行えばいいでしょうか？

A. ご利用中の電子証明書がSHA256の場合は、何もご対応いただく必要はございません。
引き続きご利用ください。
ご利用中の電子証明書がSHA-1の場合、有効期間中に利用不可になる場合がございますので、その場合はSHA256証明書の再発行（無償）が必要です。

Q. ハッシュ関数の違いにより対応環境（ブラウザ、携帯端末など）の違いはありますか？

A. SHA-1とSHA256では対応環境が異なります。

Q. ハッシュ関数の違いにより証明書の設定方法に違いはあるのでしょうか？

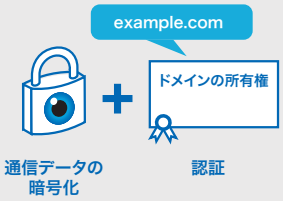
A. 設定方法に違いはありませんが、設定に利用するルート証明書、中間証明書が異なります。
ご利用の証明書に対応するルート証明書、中間証明書を使用するようご注意ください。

Q. SHA-2に環境が対応していないので、SHA-1の証明書を引き続き利用（発行）することは可能でしょうか？

A. SHA-1証明書の発行または利用には期限がございます。期限を過ぎての発行・利用はできません。

グローバルサインのSSLサーバ証明書

クイック認証SSL



・問い合わせフォーム
・会員向けサイトなどにオススメ。

認証レベル	★
認証項目	ドメイン
発行スピード	最短2分

企業認証SSL

・新規ユーザの信頼獲得が必要な会員制サイトなどにオススメ。

認証レベル	★★
認証項目	ドメイン 法的企業実在性
発行スピード	最短即日

EV SSL(強化認証SSL)

・金融機関や、オンライン決済のあるショッピングサイトにオススメ。

認証レベル	★★★
認証項目	ドメイン・ 法的及び物理的企業実在性
発行スピード	10営業日前後

※発行スピードは、一定の条件がございます。

お問い合わせ専用ダイヤル

03-6370-6500

(受付時間：平日10:00～18:00)

グローバルサイン SHA1 SHA2 検索

https://jp.globalsign.com/sha256/

GlobalSign®
GMO INTERNET GROUP

GMOグローバルサイン株式会社
東京都渋谷区桜丘町26-1 セルリアンタワー
グローバルサイン 検索 https://jp.globalsign.com/

GSM160801D-102-0000