

# 2017年以降のSHA-1のサーバー証明書に対する エラーや警告について



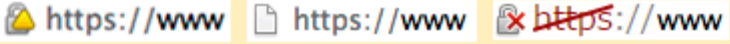


---

サイバートラスト株式会社  
2017年05月12日

## 【！】本資料の内容に関するご注意

- 本資料は「2017年5月時点」の各ブラウザベンダの情報を元に作成しています。
- 本資料に掲載されている内容と実際の動作は異なる場合があります。
- 本資料は動作を保証するものではなく、この資料内に誤りがあった場合、サイバートラスト株式会社は一切の責任を負いません。
- 本資料は予告なく変更される場合があります、サイバートラスト株式会社はその内容に対して責任を負うものではありません。

## 2. 各ブラウザにおける影響

ブラウザ	SHA-1のサーバー証明書に対する エラーや警告																							
	2016年												2017年											
	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12
<b>Microsoft</b> Microsoft Edge Internet Explorer 11	警告やエラーなし							2016年8月2日～ アドレスバーから鍵アイコンを外す 					2017年5月9日(米国時間)～ 信頼しないサイトとして警告 											
<b>Google</b> Chrome	2014年11月～ アドレスバーのアイコンを段階的に変更 											2017年1月31日～ (Chrome56) 警告表示 												
<b>Mozilla</b> Firefox	警告やエラーなし											2017年3月7日～ (Firefox52) 「信頼されない接続」としてエラー 												
<b>Apple</b> Safari	警告やエラーなし											2017年4月～ (macOS 10.12.4/iOS 10.3～) 安全でない接続として Safari に表示												

SHA-1証明書をご利用中の場合は、外部規制やSHA-2証明書の対応状況をご確認のうえ、お早めにSHA-2へ移行を進めてくださいますようお願いいたします。

## ■ 概要

### ■ SHA-1廃止に関するロードマップの最新情報

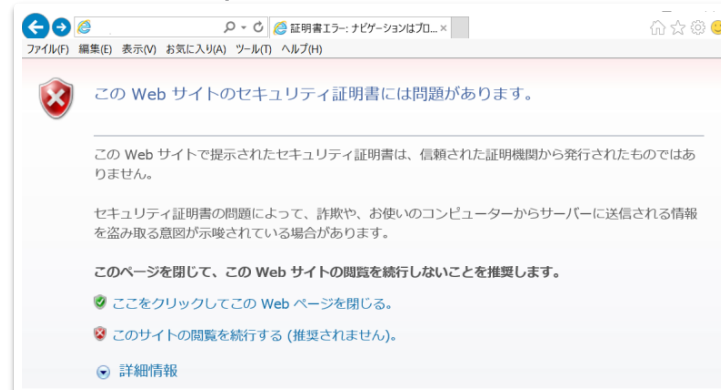
- 2017年5月9日(米国時間)より、SHA-1のTLSサーバー証明書を利用するウェブサイトを、Microsoft Edge および Internet Explorer 11 で閲覧した場合、**信頼しないサイトとして警告表示**

【警告画面】

#### ・ Microsoft Edge



#### ・ Internet Explorer 11



### ■ 対象

- ウェブサーバーにて、SHA-1のTLSサーバー証明書を利用している
- マイクロソフトルート証明書更新プログラムに参加しているルート証明機関から発行された証明書である

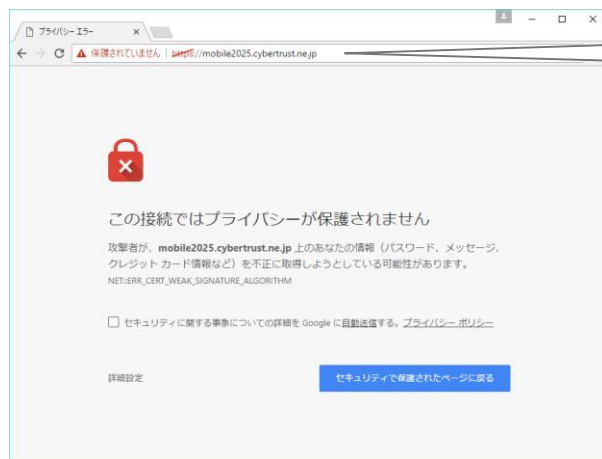
## 概要

### SHA-1 Certificates in Chrome

- 2017年1月31日にリリースされた Chrome56 から、SHA-1証明書のサポートを削除
- SHA-1証明書を使用しているWebサイトにアクセスする場合、警告表示

【警告画面 (Chrome56)】

【アドレスバーの表示】



保護されていません | ~~https://~~mobile2025.cybertrust.ne.jp

### 対象

- SHA-1のサーバー証明書・中間CA証明書

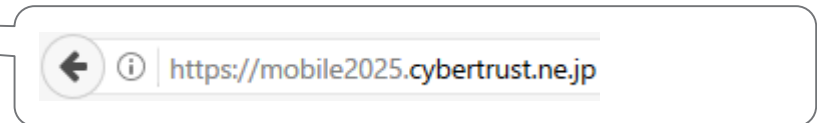
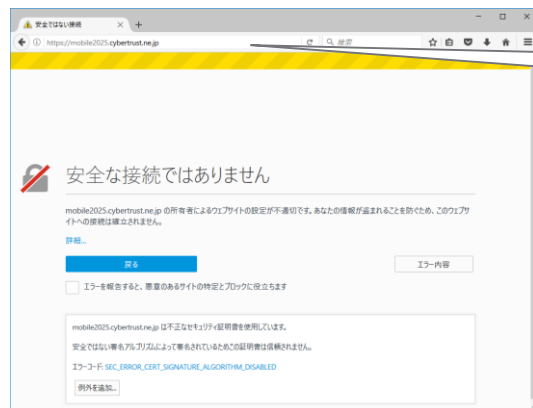
※2017年3月リリース予定の Chrome57 以降、ローカルにインストールされたルート証明書につながる証明書は「[EnableSha1ForLocalAnchors](#)」ポリシーのセットが必要となり、本機能は2019年1月に削除される予定

## ■ 概要

- Phasing Out SHA-1 on the Public Web
- The end of SHA-1 on the Public Web
- 2017年3月7日にリリースされた Firefox52 から、SHA-1証明書を使用しているWebサイトにアクセスする場合、「信頼されない接続」としてエラーを表示

【エラー画面 (Firefox52)】

【アドレスバーの表示】

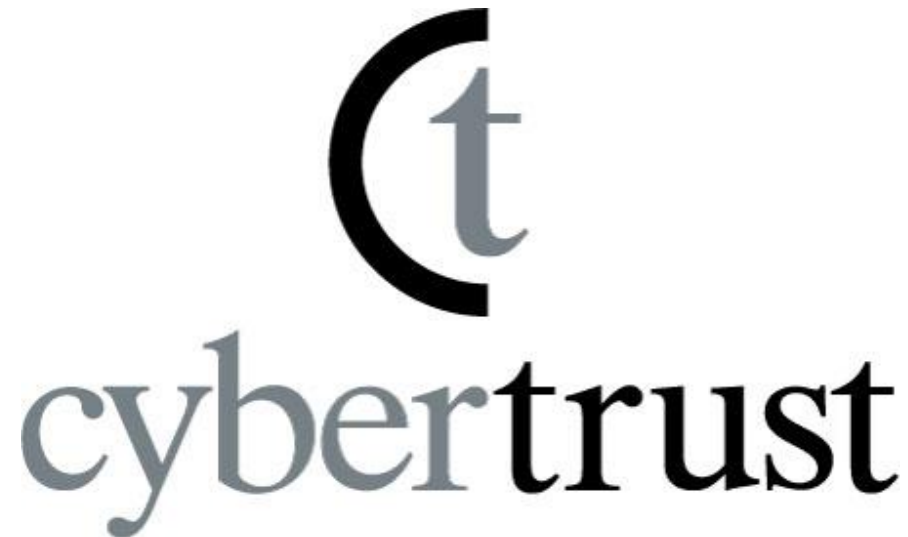


## ■ 対象

- Mozilla's CA Certificate Program に参加しているルート証明書につながる SHA-1 証明書

## ■ 概要

- Safari および WebKit での SHA-1 証明書のサポート終了について
  - **2017 年 4 月** のセキュリティアップデートの適用後、SHA-1 署名証明書を使って TLS 接続を確立しようとする Web ページにアクセスすると、Safari に通知が表示。クリックしないとサイトが読み込まれず、読み込み後、サイトは**安全でない接続**として Safari に表示
- 対象
  - macOS Sierra 10.12.4、iOS 10.3、tvOS 10.2、watchOS 3.2 ~
  - オペレーティングシステムのデフォルトのトラストストアに保存されている、ルート認証局 (CA) が発行したすべてのSHA-1証明書
    - [Lists of available trusted root certificates in macOS](#)
    - [Lists of available trusted root certificates in iOS](#)
    - [Lists of available trusted root certificates in tvOS](#)
    - [Lists of available trusted root certificates in watchOS](#)



<https://www.cybertrust.ne.jp>

詳細は下記まで、お問い合わせください。

**0120-957-975**

電話受付時間 平日 9:00 ~ 18:00

✉ [servicedesk@cybertrust.ne.jp](mailto:servicedesk@cybertrust.ne.jp)