SophosUTM
SHA-1 証明書廃止に伴う注意点

2016.06

ネクスト・セキュリティ 株式会社

はじめに

平素より SophosUTM 製品をご利用いただきまして、誠にありがとうございます。

HTTPS の通信に使われる証明書の署名アルゴリズムの一つに「SHA-1」があります。この「SHA-1」は近年のコンピューターの計算速度の進化等により安全性が低下しました。これに伴いマイクロソフト Internet Explorer、グーグル Chrome、Mozilla FireFox といった主要な Web ブラウザでは SHA-1 の証明書を使った HTTPS の通信をブロックする予定であることが発表されています。SophosUTM では特定のバージョン以前でセットアップされた機器では SHA-1 の証明書が使用されているため、**WebAdmin やユーザポータル、Web フィルタリングのアクセスがブロックされる可能性がございます**。これを回避するためには証明書を手動で再生成する必要がございます。本書では影響を受ける機器の見分け方と証明書の再生成方法につきましてご案内致します。

Web ブラウザ各社の対応につきましては流動的になっておりますが **2016 年 7 月以降**でブロックすることも検討されているため**早めに対応することをお勧めします**。詳しくは各社の発表をご確認いただきますようお願い致します。

この資料は Web ブラウザ各社からの発表に基づき作成しておりますが現段階(2016 年 6 月)では実機で動作を確認する手段がないため実際の動作と異なる可能性があることをご了承下さい。

マイクロソフト

https://blogs.technet.microsoft.com/jpsecurity/2015/11/02/faq-sha-1-sha-2/

Google

https://security.googleblog.com/2015/12/an-update-on-sha-1-certificates-in.html

Mozilla

https://blog.mozilla.org/security/2015/10/20/continuing-to-phase-out-sha-1-certificates/

<参考>各社の対応をまとめているサイト

https://jp.globalsign.com/blog/2016/ssl_sha1_sha2_transition.html

https://www.cybertrust.ne.jp/sureserver/productinfo/sha1ms.html

1　影響を受ける機能

Web ブラウザの動作変更に伴い通信が**ブロックされ、アクセスを続行することができなくなる**可能性のある機能は以下になります。

1. **WebAdmin へのアクセス**
2. **ユーザポータルを利用している場合、ユーザポータルへのアクセス**
3. **Web フィルタリングを利用している場合、HTTPS の通信(※)**

   ※Web フィルタリングについては設定により影響範囲が変わります。

   [Web プロテクション] >> **[Web フィルタリング]** >> **[HTTPS]** 及び **[Web プロテクション]** >> **[Web フィルタプロファイル]** >> **[フィルタプロファイル]** にて個別のプロファイルを作成している場合は各プロファイルの**[HTTPS]**タブにおいて

   - **[URL フィルタリングのみ] を選択している場合又は[以下を復号化してスキャン] においてスキャン対象となっていないサイト**

     UTM の URL フィルタリング機能でブロックした場合等、UTM のメッセージ表示に切り替わる部分がブロックされます。
   - **[復号化してスキャン] を選択している場合又は[以下を復号化してスキャン] においてスキャン対象となっているサイト**

     対象の HTTPS 通信全てがブロックされます。

   以下の設定の場合は影響を受けません。

   [Web プロテクション] >> **[Web フィルタリング]** >> **[グローバル]** 及び **[Web プロテクション]** >> **[Web フィルタプロファイル]** >> **[フィルタプロファイル]** にて個別のプロファイルを作成している場合は各プロファイルの**[Web フィルタプロファイル]**タブにおいて**[オペレーションモード:]** を **[透過モード]** に設定し、且つ**[Web プロテクション]** >> **[Web フィルタリング]** >> **[HTTPS]** 及び **[Web プロテクション]** >> **[Web フィルタプロファイル]** >> **[フィルタプロファイル]** にて個別のプロファイルを作成している場合は各プロファイルの**[HTTPS]**タブにおいて**[透過モードで HTTPS トラフィックをプロキシしない]** にチェックが入っている場合

   ※透過モードに設定している場合でも Web ブラウザ側のプロキシ設定で SophosUTM を指定している場合は標準モードでの動作となります。上記影響を受けない条件に当てはまらなくなりますので先の HTTPS のスキャン設定に従い通信に影響が出ます。

2　影響を受ける機器の見分け方

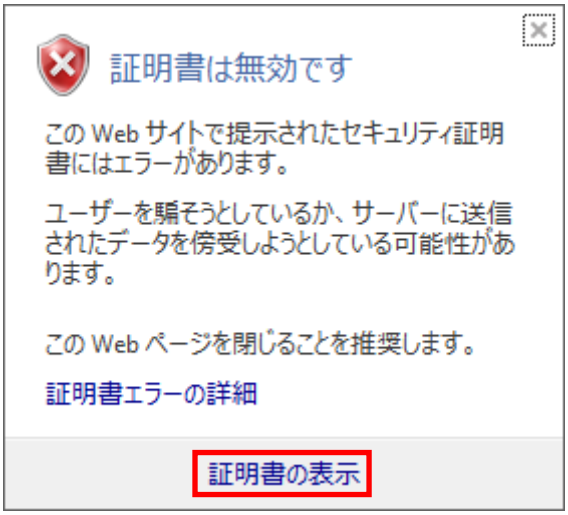
9.313 以前のファームウェアバージョンで初回セットアップを行った機器全てが対象となります。現在ご利用中のファームウェアバージョンではなく初回セットアップ時点でのバージョンであることにご注意下さい。ハードウェアをリプレースしたがバックアップは以前の機器のものを引き継いだといった場合は以前に使用されていた機器の初回セットアップ時点のファームウェアバージョンで判断することになります。

初回セットアップ時点のファームウェアバージョンが不明の場合は次の「2-1 証明書から署名アルゴリズムを確認する方法」を参照して直接証明書をご確認下さい。

2-1 証明書から署名アルゴリズムを確認する方法

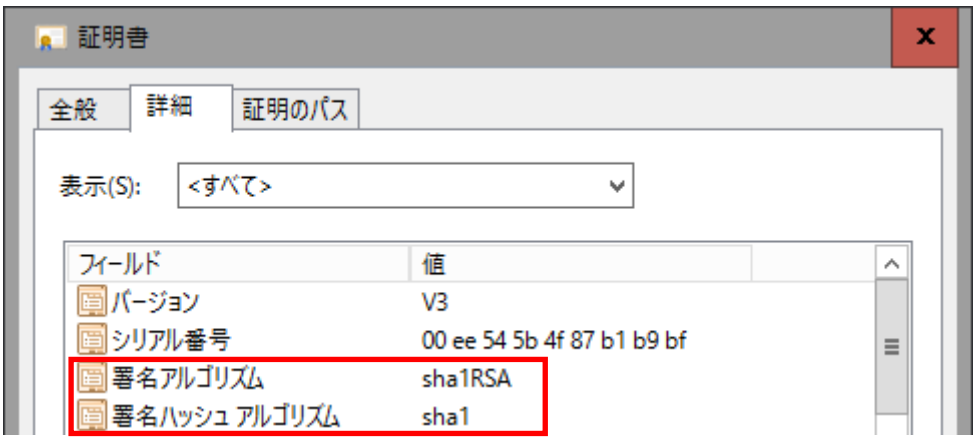
1. Internet Explorer を起動し WebAdmin にアクセスします。
2. アドレスバーの右側にある**[証明書のエラー]**又は**[鍵マークのアイコン]**をクリックします。

3. ポップアップしたメッセージの最下部にある**[証明書の表示]**をクリックします。

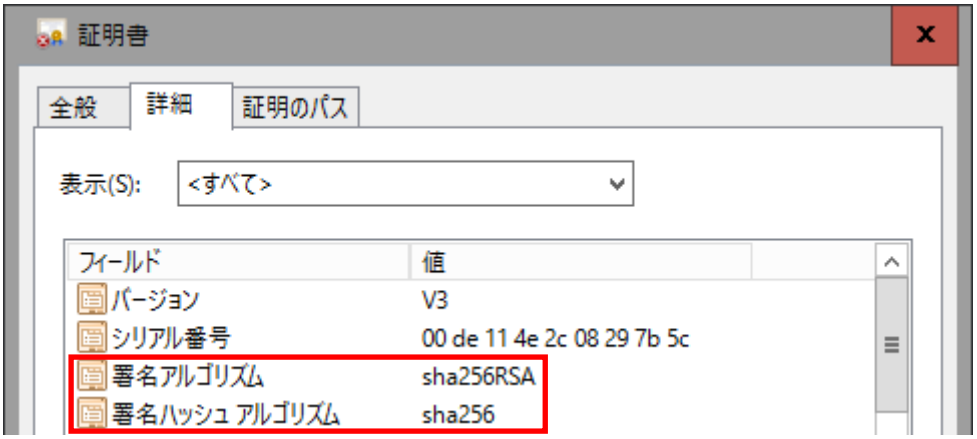


4. **[詳細]**タブを開き、**[署名アルゴリズム]**や**[署名ハッシュアルゴリズム]**を確認します。この値が**[sha1RSA、sha1]**や**[md5RSA、md5]**の場合、影響が出る可能性のある機器となります。**[sha256RSA、sha256]**の場合は影響ありません。

<影響が出る可能性のある証明書>



<影響の無い証明書>


証明書
全般
詳細
証明のパス
表示(S):
<すべて>
フィールド
値
バージョン
V3
シリアル番号
00 de 11 4e 2c 08 29 7b 5c
署名アルゴリズム
sha256RSA
署名ハッシュ アルゴリズム
sha256

3　証明書の再生成方法

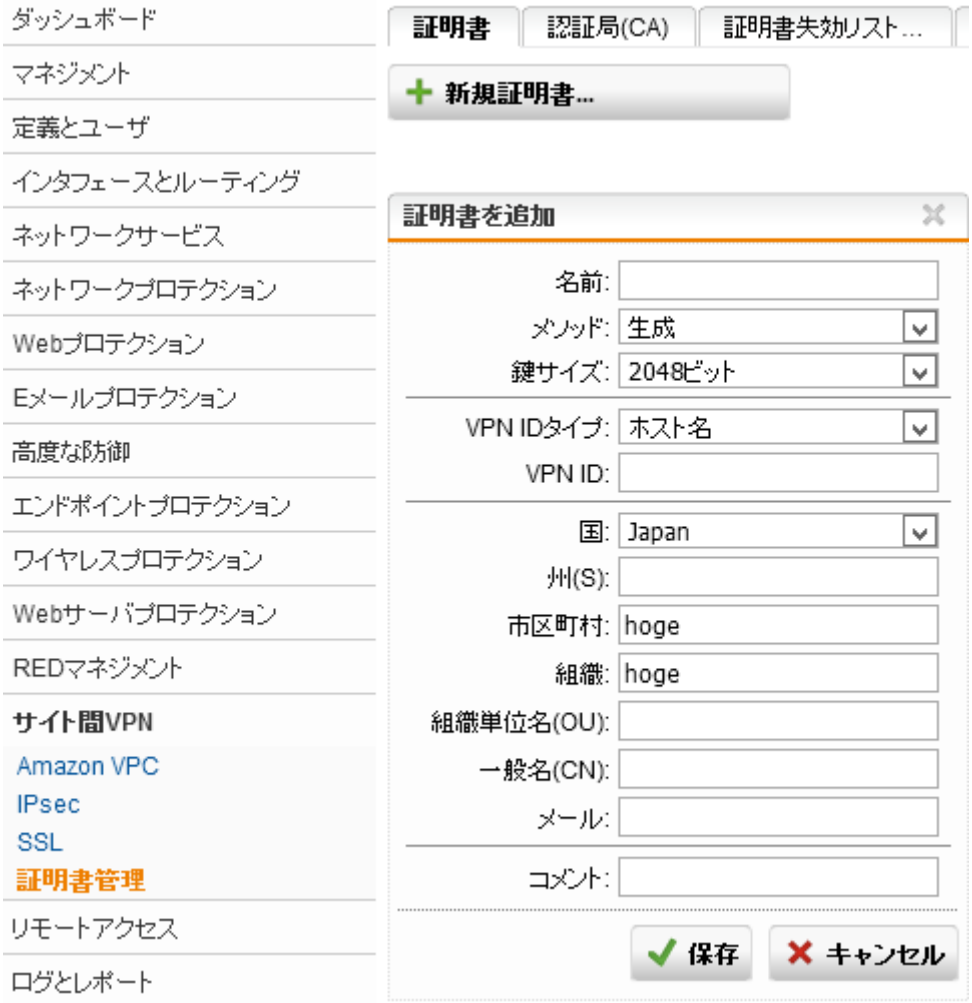
影響を受ける機器の場合**ファームウェアバージョンを 9.314 以上**にアップデートした上で証明書を再生成します。ファームウェアのアップデートは**[マネジメント] >> [Up2Date] >> [概要]**より行います。詳しくは機器に同梱されている CD に収録されている「SophosUTM9 運用ガイド」をご参照下さい。

また、SophosUTM では SophosUTM 自身のセキュリティに関する更新を随時ファームウェアのアップデートにて行っておりますので最新の推奨バージョンまでアップデートすることをお勧めします。推奨バージョンにつきましては随時更新されますので弊社サポートセンター(SophosUTM@nextit.jp、0570-081777)までお問い合わせ下さい。

本書ではファームウェアを 9.314 以上にアップデートされている前提で証明書の再生成方法をご案内します。

3-1　WebAdmin、ユーザポータル用の証明書の再生成

1. WebAdmin にアクセスし、**[サイト間 VPN] >> [証明書管理] >> [証明書]** を開きます。
2. **[新規証明書...]** をクリックします。
3. **[証明書を追加]**ペインが表示されるので各項目に値を入力します。



- **[名前:]**
  証明書に付ける任意の名前を入力
- **[メソッド:]**
  「生成」を選択

- **[鍵サイズ:]**
  2048 以上を選択することを推奨
- **[VPN ID タイプ:]**
  「ホスト名」を選択
- **[VPN ID:]**
  SophosUTM のホスト名([マネジメント] >> [システム設定] >> [ホスト名])を入力
- **[国:]**
  「Japan」を選択
- **[州(S)～組織単位(OU)までの各項目:]**
  入力は任意。使用可能文字は半角の英数字及び半角記号のスペース、 '(アポストロフィ)、 -(ハイフン)、 ,(カンマ)、 =(イコール)、 /(スラッシュ)、 ()(括弧)、 .(ピリオド)、 :(コロン)
- **[一般名(CN):]**
  SophosUTM のホスト名([マネジメント] >> [システム設定] >> [ホスト名])を入力
- **[メール:]**
  入力は任意。入力する場合は管理者のメールアドレスを入力
- **[コメント:]**
  入力は任意

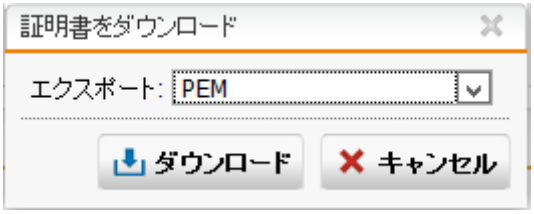
4. 値の入力が終わったら**[保存]**をクリックして証明書を生成します。
5. **[マネジメント] >> [WebAdmin 設定] >> [HTTPS 証明書]** を開きます。

6. **[WebAdmin/ユーザポータル証明書を選択してください]**の項目にある**[証明書:]**にて先ほど作成した証明書を選択します。
7. 右下の**[適用]**アイコンをクリックして設定を保存します。
8. **「2-1 証明書から署名アルゴリズムを確認する方法」**を参照して**[署名アルゴリズム]**や**[署名ハッシュアルゴリズム]**が**[sha256RSA、sha256]**になった事を確認します。

3-2 Web フィルタリング用の証明書の再生成

1. [Web プロテクション] >> [フィルタリングオプション] >> [HTTPS CA] を開きます。

2. **[署名 CA]** の項目の**[再生成]**をクリックします。
3. 各ユーザが利用されている端末に署名 CA を取り込んでいる場合は再生成した証明書を再度取り込み直します。
4. 再生成した証明書を再度取り込み直す場合や署名アルゴリズムを確認する場合は**[ダウンロード]**をクリックします。
5. **[証明書をダウンロード]**ペインが表示されるので**[エクスポート:]**の値を**[PEM]**にして**[ダウンロード]**をクリックします。



6. 証明書を任意のフォルダにダウンロードします。
7. ダウンロードした証明書をダブルクリックして開きます。
8. **[詳細]**タブを開き、**[署名アルゴリズム]**や**[署名ハッシュアルゴリズム]**が**[sha256RSA、sha256]**になっている事を確認します。
9. 各ユーザが利用されている端末に署名 CA を取り込む場合はダウンロードした署名 CA を配布して下さい。