HazardFilter で使用しているサーバ証明書の確認方法

株式会社 YE DIGITAL

【 質問 】

HazardFilter で使用しているサーバ証明書の確認方法を教えてください。

【 回答 】

HazardFilter で使用する証明書(認証局証明書)の取得手順は、以下のとおりです。

	連氏のパーク	
ミマルミノコ バス、	イロカメイタリーとこと	

1. [共通アクセス管理] → [HTTPS 規制設定]を選択します。

HazardFil	ter Ver3.1 Build1600 on Linux 64bit	ログインユーザ: root	⊖ ログアウト
ホーム グループ/ユーザ管理 🗸	共通アクセス管理・ 個別アクセス管理・ 規制解除申請管理・ サーバ管理・ 読定情報管理・	ログ管理 👻	
共通アクセス管理 >			
HTTPS規制設定	HTTPSU9エストをディレクトリ単位で規制します。		
			保存
▶ 認証局設定			
認証局証明書	認証局証明書のダウンロード 証明書サブジェクト CNHinterSafe WebFilter Sensice OAO=#ALPS SYSTEM INTEGRATION OD XILTD, ST=Tokyo,O=、P		
	ファイルの選択ファイルが選択されていません		
認証局変更	PKCS#12パスワード		
	※指定可能なファイル形式はFKCS#12です。秘密鍵と証明書のペアを含みパスワードが設定されている必要があります。		
▶ サーバデコード方式			
иттре≓⊐⊸К	▲ HTTPS通信は情報が暗号化されますが、 この暗号を一時的にデコードして、フィルタリングおよびアクセス履歴の保存を行います。		
HITEST F	☑ HTTPS解析機能の申込規約と上記注意事項に同意し、HTTPSデコード機能を使用する		
	◎ システム一括		
設定単位	全てのグループ/ユーザで機能を有効化する 〇 グリューブ毎		
	(グループ/ユーザ管理Hグループ管理Hネットワーク設定]で個別に機能の有効/無効を選択する		
施生而而迅宁	☑ HTTPSデコード処理の実行前に、ユーザへ警告画面を表示する		
吉古國國政定	警告画面の再表示問隔: 6時間 🗸		
	○ 対象ホストをHTTPSデコード対象にする。		
対象ホスト設定	動物の中では、「「「「「「「」」」、「「」」、「「」」、「「」」、「」、「」、「」、「」、「		
	▶ 対象ホスト一覧へ		
除外カテゴリ設定	▶ 除外力テゴリ設定へ		
POSTログ出力設定	▶ [ログ管理]-[ログ設定] でPOSTログ出力が無効に設定されています。		
パス部ログ出力設定	▶ パス部ログ出力設定へ		
HazardFilter			

2. 「HTTPS 規制設定」画面で、「認証局証明書のダウンロード」をクリックします。 「cacert.cer」ファイルがダウンロードされます。

3. 取得した証明書をクリックします。

■ 証明書	× 😱 証明書	×
全般 詳細 証明のパス	全般 詳細 証明のパス	
正明書の情報 この証明書の目的: ・すべての発行ポリシー ・すべてのアプリケーションポリシー	表示(S): <すパて> フィールド 値 ③ パージョン V3 ③ ジリアル番号 389a05b4 圖 署名アルゴリズム sha256RSA 圖 署名パッジュアルゴリズム sha256 ③ 発行者 HazardFilter, YE DIGITAL Cor 圖 有効期間の開始 2022年3月8日 8:45:07	^
	□ 有効期間の終了 2047年3月8日 8:45:07 □ サブジェクト HazardFilter, YE DIGITAL Cor	~
発行者: HazardFilter		
有効期間 2022/03/08 から 2047/03/08		
証明書のインストール(J) 発行者のステートメント(S)	プロパティの編集(<u>E</u>) ファイル	lt⊐k°−(<u>C</u>)
ОК		OK

4. [証明書のインストール] ボタンをクリックすると、証明書のインストールが行えます。
 保存場所を選択後、[次へ] ボタンをクリックします。

←	×
証明書のインポート ウィザードの開始	
このウィザードでは、証明書、証明書信頼リスト、および証明書夫効リストをディスクから証明書ストアにコピー します。	
証明機関によって発行された証明書は、ユーザーIDを確認し、データを保護したり、またはセキュリティで保護 されたネットワーク接続を提供するための情報を含んでいます。証明書ストアは、証明書が保管されるシステ ム上の領域です。	
 保存場所 ○現在のユーザー(C) ◎□-カルコンビューター(L) 	
続行するには、 [次へ] をクリックしてください。	
	セル

4. [証明書をすべて次のストアに配置する]を選択し、[参照]ボタンをクリックします。

_	×
←	
証明書ストア	
証明書ストアは、証明書が保管されるシステム上の領域です。	_
Windows に証明書ストアを自動的に選択させるか、証明書の場所を指定することができます。	
○ 証明書の種類に基づいて、自動的に証明書ストアを選択する(凹)	
・ 証明書をすべて次のストアに配置する(P)	٦
証明書ストア:	
参照(<u>R</u>)	
次へ(<u>N</u>) キャンセル	

5.「証明書ストア」の選択で、「信頼されたルート証明機関」を選択し、 [OK] ボタンをクリックします。



6. [次へ] ボタンをクリックします。

÷	夢 証明者のインポート ウィザード	×
	証明書ストァ 証明書ストアは、証明書が保留されるシステム上の領域です。	
	Windowsに証明書ストアを自動的に選択させるか、証明書の場所を指定することができます。	
	○ 証明書の種類に基づいて、自動的に証明書ストアを選択する(U)	
	 ・ 血分白をすべく次の入りたに差すった) 証明會入トア: 信頼されたルート証明機関 参照(B) 	
	次へ(N) キャンセ	μ

7. [完了] ボタンをクリックします。

← 緑 証明者のインポート ウィザード		×
証明書のインポート ウィザードの完了		
[完了]をクリックすると、証明書がインポートされます。		
次の設定が指定されました:		
ユーザーが選択した証明書ストア 信頼されたルート証明機関 内容 証明書		
	完了(<u>F</u>)	キャンセル

以上