JCCH・セキュリティ・ソリューション・システムズ

プライベート CA Gléas

証明書のダイジェストアルゴリズム SHA-2 への変更手順

Ver.1.0

2015 年 6 月

Copyright by JCCH Security Solution Systems Co., Ltd., All Rights reserved

・ JCCH・セキュリティ・ソリューション・システムズ、JS3 およびそれらを含むロゴは日本および他の国における株式会社 JCCH・セキュリティ・ソリューション・システムズの商標または登録商標です。Gléas は株式会社 JCCH・セキュリティ・ソリューション・システムズの商標です。
・ その他本文中に記載されている製品名および社名は、それぞれ各社の商標または登録商標です。
・ Microsoft Corporation のガイドラインに従って画面写真を掲載しています。

Copyright by JCCH Security Solution Systems Co., Ltd., All Rights reserved

目次

1. はじめに

1.1. 本書について

Gléas 電子証明書のダイジェストアルゴリズムについてのデフォルト設定を SHA-1 から SHA-2 への変更する方法について解説いたします。

SHA-1 ハッシュ関数の脆弱性が指摘され、米国の国立標準技術研究所は、SHA-2 への移行を勧告しました。また 2013 年に Microsoft 社はルート証明書プログラムでの SHA-1 ハッシュアルゴリズムの廃止が発表されました。それによると Windows 環境において、SHA-1 の SSL サーバ証明書が 2017 年 1 月 1 日以降利用することが出来なくなります。

このような背景で、弊社ではご利用中の電子証明書を SHA-2 への移行を推奨しており、本書でその方法を解説致します。

1.2. 本書を利用時の注意点

本書の手順をおこなうとそれ以降に発行するすべての証明書の鍵長が RSA2048bit、ダイジェストアルゴリズムが SHA-2 となるので、発行する証明書によりこれを変更したい場合などは、グループ機能をご利用ください。
（詳細は製品付属の標準マニュアルをご参照ください）

2. 移行についての操作手順

2.1. 手順概要

SHA-1 から SHA-2 への変更に関しては、次のような操作の流れになります。

1. Gléas RA にログイン
2. [スタート]ページ　→　テンプレートを選択
3. [テンプレート]概要　→　テンプレート一覧を選択
4. [テンプレート]一覧　→　認証局情報のデフォルト設定を選択
5. [テンプレート]詳細　→　編集を選択
6. [テンプレート]詳細　→　ダイジェストアルゴリズムが（SHA1 であれば）右側の削除[-]を選択

7. [テンプレート]詳細　→　鍵長が(1024bit であれば)右側の削除[-]を選択
8. [テンプレート]詳細　→　下のドロップボックスより[ダイジェストアルゴリズム]を選択し、次に[SHA256]を選択し追加[+]を選択
9. [テンプレート]詳細　→　下のドロップボックスより[鍵長]を選択し、次に[2048bit]を選択して追加[+]を選択
10. 以上が済んだら[保存]を選択

以上の操作により次に発行する証明書は SHA-2/RSA2048bit になります。

2.2. 手順詳細

1. Gléas RA にログイン
2. [スタート]ページ　→　テンプレートを選択

3. [テンプレート]概要　→　テンプレート一覧を選択

4.［テンプレート］一覧　→　認証局情報のデフォルト設定を選択

5.［テンプレート］詳細　→　編集を選択

6. [テンプレート]詳細　→　ダイジェストアルゴリズムが（SHA1 であれば）右側の削除[−]を選択

7. [テンプレート]詳細　→　鍵長が(1024bit であれば)右側の削除[-]を選択

8. [テンプレート]詳細　→　下のドロップボックスより[ダイジェストアルゴリズム]を選択し、次に[SHA256]を選択し追加[+]を選択


作業名 ： タスク12
管理者 ： admin2015
プライベートCA Gléas RA
[テンプレート]> 詳細
認証局 ログ 管理者 ヘルプ ログアウト
サイドバー
クイックナビ
ユーザ証明書
マシン証明書
サーバ証明書
認証局証明書
アカウント Account
グループ Group
証明書 Certificate
認証デバイス Device
テンプレート Template
テンプレート操作
テンプレート一覧
テンプレート詳細一覧
テンプレート新規作成
テンプレート
一覧に戻る
デフォルト設定
テンプレート情報
タイムライン
概要
テンプレート名 ： デフォルト設定
テンプレートID ： __DEFAULT__
作成日 ： 2015/04/10 14:18
削除日 ：
認証局 ： Evaluation CA
詳細
元に戻す 保存 取り消し
証明書の属性
データベースの項目
暗号アルゴリズム
RSA暗号
有効日数
1ヶ月
鍵用途
電子署名
鍵用途
鍵の暗号化
拡張鍵用途
SSLクライアント認証
組織名
JCCH Security Solution Systems
発行局
Evaluation CA
Netscape 拡張
有効
ダイジェストアルゴリズ
SHA1
保存
ドック
アカウント (0)
証明書 (0)
グループ情報
ユーザグループ
なし
ロールグループ
グローバルグループ
操作履歴 プライベートCA Gléas
Copyright (C)2010-2013 JCCH Security Solution Systems Co.,Ltd. All rights reserved.


作業名 ： タスク12
管理者 ： admin2015
プライベートCA Gléas RA
[テンプレート]> 詳細
認証局 ログ 管理者 ヘルプ ログアウト
サイドバー
クイックナビ
ユーザ証明書
マシン証明書
サーバ証明書
認証局証明書
アカウント Account
グループ Group
証明書 Certificate
認証デバイス Device
テンプレート Template
テンプレート操作
テンプレート一覧
テンプレート詳細一覧
テンプレート新規作成
テンプレート
一覧に戻る
デフォルト設定
テンプレート情報
タイムライン
概要
テンプレート名 ： デフォルト設定
テンプレートID ： __DEFAULT__
作成日 ： 2015/04/10 14:18
削除日 ：
認証局 ： Evaluation CA
詳細
元に戻す 保存 取り消し
証明書の属性
データベースの項目
暗号アルゴリズム
RSA暗号
有効日数
1ヶ月
鍵用途
電子署名
鍵用途
鍵の暗号化
拡張鍵用途
SSLクライアント認証
組織名
JCCH Security Solution Systems
発行局
Evaluation CA
Netscape 拡張
有効
ダイジェストアルゴリズ
SHA1
SHA2
SHA256
SHA384
SHA512
DSS1
MD5
保存
ドック
アカウント (0)
証明書 (0)
グループ情報
ユーザグループ
なし
ロールグループ
グローバルグループ
操作履歴 プライベートCA Gléas
Copyright (C)2010-2013 JCCH Security Solution Systems Co.,Ltd. All rights reserved.

9. [テンプレート]詳細　→　下のドロップボックスより[鍵長]を選択し、次に[2048bit]を選択して追加[+]を選択


作業名 ： タスク12
管理者 ： admin2015
プライベートCA Gléas RA
[テンプレート]> 詳細
認証局 ログ 管理者 ヘルプ ログアウト
アカウント
グループ
証明書
認証デバイス
テンプレート
テンプレート操作
テンプレート一覧
テンプレート詳細一覧
テンプレート新規作成
テンプレート
一覧に戻る
デフォルト設定
テンプレート情報
タイムライン
概要
テンプレート名 ： デフォルト設定
テンプレートID ： __DEFAULT__
作成日 ： 2015/04/10 14:18
削除日 ：
認証局 ： Evaluation CA
詳細
元に戻す 保存 取り消し
証明書の属性
データベースの項目
暗号アルゴリズム
RSA暗号
有効日数
1ケ月
鍵用途
電子署名
鍵用途
鍵の暗号化
拡張鍵用途
SSLクライアント認証
組織名
JCCH Security Solution Systems
発行局
Evaluation CA
Netscape 拡張
有効
ダイジェストアルゴリズム
SHA256
鍵長
512bit
証明書ポリシ
別名(電子メール)
Netscape 拡張
ダイジェストアルゴリズム
有効日数
CA証明書
所属名
critical
終了日
一般名
メールアドレス
別名(プリンシパル名)
鍵用途
鍵長
発行局
別名(DNS)
別名(コンピュータ名)
組織名
CRL 配布点
暗号アルゴリズム
発行局の別名
拡張鍵用途
開始日
OCSP
ドメインコントローラ
グループ情報
ユーザグループ
なし
ロールグループ
グローバルグループ
サイドバー
クイックナビ
ユーザ証明書
マシン証明書
サーバ証明書
認証局証明書
保存
ドック
アカウント (0)
証明書 (0)
操作履歴 プライベートCA Gléas
Copyright (C)2010-2013 JCCH Security Solution Systems Co.,Ltd. All rights reserved.


作業名 ： タスク12
管理者 ： admin2015
プライベートCA Gléas RA
[テンプレート]> 詳細
認証局 ログ 管理者 ヘルプ ログアウト
サイドバー
クイックナビ
ユーザ証明書
マシン証明書
サーバ証明書
認証局証明書
アカウント Account
グループ Group
証明書 Certificate
認証デバイス Device
テンプレート Template
テンプレート操作
テンプレート一覧
テンプレート詳細一覧
テンプレート新規作成
テンプレート
一覧に戻る
デフォルト設定
テンプレート情報
タイムライン
概要
テンプレート名 ： デフォルト設定
テンプレートID ： __DEFAULT__
作成日 ： 2015/04/10 14:18
削除日 ：
認証局 ： Evaluation CA
詳細
元に戻す 保存 取り消し
証明書の属性
データベースの項目
暗号アルゴリズム RSA暗号
有効日数 1ヶ月
鍵用途 電子署名
鍵用途 鍵の暗号化
拡張鍵用途 SSLクライアント認証
組織名 JCCH Security Solution Systems
発行局 Evaluation CA
Netscape 拡張 有効
ダイジェストアルゴリズム SHA256
鍵長
512bit
1024bit
2048bit
4096bit
8192bit
保存
ドック
アカウント (0)
証明書 (0)
グループ情報
ユーザグループ
なし
ロールグループ
グローバルグループ
操作履歴 プライベートCA Gléas
Copyright (C)2010-2013 JCCH Security Solution Systems Co.,Ltd. All rights reserved.


作業名 ： タスク12
管理者 ： admin2015
プライベートCA Gléas RA
[テンプレート]> 詳細
認証局 ログ 管理者 ヘルプ ログアウト
サイドバー
クイックナビ
ユーザ証明書
マシン証明書
サーバ証明書
認証局証明書
アカウント Account
グループ Group
証明書 Certificate
認証デバイス Device
テンプレート Template
テンプレート操作
テンプレート一覧
テンプレート詳細一覧
テンプレート新規作成
テンプレート
一覧に戻る
デフォルト設定
テンプレート情報
タイムライン
概要
テンプレート名 ： デフォルト設定
テンプレートID ： __DEFAULT__
作成日 ： 2015/04/10 14:18
削除日 ：
認証局 ： Evaluation CA
詳細
元に戻す 保存 取り消し
証明書の属性
データベースの項目
暗号アルゴリズム RSA暗号
有効日数 1ヶ月
鍵用途 電子署名
鍵用途 鍵の暗号化
拡張鍵用途 SSLクライアント認証
組織名 JCCH Security Solution Systems
発行局 Evaluation CA
Netscape 拡張 有効
ダイジェストアルゴリズム SHA256
鍵長
2048bit
保存
ドック
アカウント (0)
証明書 (0)
グループ情報
ユーザグループ
なし
ロールグループ
グローバルグループ
操作履歴 プライベートCA Gléas
Copyright (C)2010-2013 JCCH Security Solution Systems Co.,Ltd. All rights reserved.

10. 以上が済んだら[保存]を選択

以上の操作で SHA-1 から SHA-2 へのアルゴリズム変更は完了です。最後に、設定した内容が下記の画面のように示されますので、内容を確認して終了です。

3. 問い合わせ

ご不明な点がございましたら、以下にお問い合わせください。

■株式会社 JCCH・セキュリティ・ソリューション・システムズ
Tel:　050-3821-2195
Mail:　sales@jcch-sss.com