



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

- ・ 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。

プライベート CA Gléas
ダイジェストアルゴリズム変更方法に関するご案内

目次

1. はじめに.....	4
1.1. 本書について.....	4
1.2. 本書を利用時の注意点.....	4
2. 移行についての操作手順.....	4
2.1. 手順概要.....	4
2.2. 手順詳細.....	6
3. 問い合わせ.....	15

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

プライベート CA Gléas
ダイジェストアルゴリズム変更方法に関するご案内

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。

プライベート CA Gléas ダイジェストアルゴリズム変更方法に関するご案内

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

The screenshot shows the 'Start Page' (スタートページ) of the Gléas RA interface. The left sidebar contains a menu with 'テンプレート' (Template) highlighted. The main content area displays 'admin2015 さんのタスク' (Tasks for admin2015) and various sections: 'アカウント情報' (Account Information), '証明書情報' (Certificate Information), and 'CSR発行待ち' (CSR Pending). A 'ヘルプトピック' (Help Topics) section is also visible on the right side of the main content area.

3. [テンプレート]概要 → テンプレート一覧を選択

The screenshot shows the 'Template Overview' (テンプレート概要) page. It includes a 'ヘルプトピック' (Help Topics) section, a '統計' (Statistics) table, and a 'テンプレートの種類' (Template Types) pie chart. The '統計' table lists various attributes and their counts. The 'テンプレートの種類' pie chart shows the distribution of templates across different categories.

属性	数	操作
証明書用途	7	一覧を表示
証明書種別	3	一覧を表示
サブジェクト	2	一覧を表示
属性	7	一覧を表示
暗号	4	一覧を表示
CRL	1	一覧を表示

種類	割合
用途	29%
種別	29%
サブジェクト	4%
属性	17%
暗号	13%
失効	8%

テンプレート名	登録日時	更新日時
デフォルト設定	2015/04/10 14:18	2015/05/29 11:57
デフォルト設定	2015/04/10 14:18	2015/05/29 11:55
デフォルト設定	2015/04/10 14:18	2015/04/10 14:18
OCSPリソルバ	2015/04/10 14:19	2015/04/10 14:19
発行局[Evaluation OTA CA]	2015/04/10 14:19	2015/04/10 14:19

プライベート CA Gléas

ダイジェストアルゴリズム変更方法に関するご案内

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

操作履歴: プライベートCA Gléas

Copyright (C)2010-2013 JOCH Security Solution Systems Co. Ltd. All rights reserved.

5. [テンプレート]詳細 → 編集を選択

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	JOCH 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	SHA2
鍵長	1024bit

操作履歴: プライベートCA Gléas

Copyright (C)2010-2013 JOCH Security Solution Systems Co. Ltd. All rights reserved.

プライベート CA Gléas
 ダイジェストアルゴリズム変更方法に関するご案内

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

操作名 : 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

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

デフォルト設定

テンプレート情報

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

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	SHA2	[-]
鍵長	1024bit	[-]
証明書ポリシー	CPS	[-]

グループ情報

ユーザーグループ

ロールグループ

操作履歴 プライベートCA Gléas

Copyright (C)2010-2015 JCCH Security Solution Systems Co.Ltd. All rights reserved.

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

操作名 : 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

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

デフォルト設定

テンプレート情報

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

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	[-]
鍵長	1024bit	[-]
証明書ポリシー	CPS	[-]

グループ情報

ユーザーグループ

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)2010-2015 JCCH Security Solution Systems Co.Ltd. All rights reserved.

プライベート CA Gléas ダイジェストアルゴリズム変更方法に関するご案内

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

The screenshot shows the 'Template Information' page in the Private CA Gléas interface. The 'Digest Algorithm' dropdown menu is open, displaying a list of available algorithms. 'SHA256' is highlighted in blue, indicating it is the selected option. The current selected algorithm is 'RSA'. The interface also shows other fields like 'Certificate Properties', 'Validity Period', and 'Certificate Usage'.

証明書属性	データベース項目
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
証明書ポリシー	CPS

The screenshot shows the 'Template Information' page in the Private CA Gléas interface. The 'Digest Algorithm' dropdown menu is open, displaying a list of available algorithms. 'SHA256' is highlighted in blue, indicating it is the selected option. The current selected algorithm is 'RSA'. The interface also shows other fields like 'Certificate Properties', 'Validity Period', and 'Certificate Usage'.

証明書属性	データベース項目
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
証明書ポリシー	CPS

プライベート CA Gléas

ダイジェストアルゴリズム変更方法に関するご案内

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

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
デフォルト設定

テンプレート情報

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

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	SHA1

タイムライン

グループ情報

ユーザーグループ
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

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
デフォルト設定

テンプレート情報

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

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	SHA1 SHA2 SHA256 SHA384 SHA512 DSS1 MD5

タイムライン

グループ情報

ユーザーグループ
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.

プライベート CA Gléas

ダイジェストアルゴリズム変更方法に関するご案内

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

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

デフォルト設定

テンプレート情報

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

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

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)2010-2015 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

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

デフォルト設定

テンプレート情報

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

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

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)2010-2015 JCCH Security Solution Systems Co.,Ltd. All rights reserved.

プライベート CA Gléas

ダイジェストアルゴリズム変更方法に関するご案内

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

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

デフォルト設定

テンプレート情報

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

グループ情報

ユーザーグループ

なし

詳細

証明書の属性

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
証明書ポリシー	電子署名
別名(電子メール)	鍵の暗号化
Netscape 拡張	SSLクライアント認証
CA証明書	JCCH Security Solution Systems
所属名	Evaluation CA
critical	有効
終了日	SHA256
一般名	SHA256
メールアドレス	
別名(アンソナル名)	
鍵用途	
発行局	SHA256
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	

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

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

デフォルト設定

テンプレート情報

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

グループ情報

ユーザーグループ

なし

ロールグループ

グローバルグループ

なし

詳細

証明書の属性

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

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.

プライベート CA Gléas

ダイジェストアルゴリズム変更方法に関するご案内

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

テンプレート

デフォルト設定

テンプレート情報

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

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	<input type="text" value="512bit"/> <input type="text" value="1024bit"/> <input style="border: 2px solid red;" type="text" value="2048bit"/> <input type="text" value="4096bit"/> <input type="text" value="8192bit"/>

グループ情報

- ユーザーグループ > 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)2010-2015 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

テンプレート

デフォルト設定

テンプレート情報

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

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	<input type="text" value="512bit"/> <input type="text" value="1024bit"/> <input style="border: 2px solid blue;" type="text" value="2048bit"/> <input type="text" value="4096bit"/> <input type="text" value="8192bit"/>

グループ情報

- ユーザーグループ > 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)2010-2015 JCCH Security Solution Systems Co. Ltd. All rights reserved.

プライベート CA Gléas ダイジェストアルゴリズム変更方法に関するご案内

10. 以上が済んだら[保存]を選択

The screenshot shows the 'デフォルト設定' (Default Settings) page for a Private CA Gléas RA. The page is divided into several sections:

- テンプレート情報 (Template Information):**
 - 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 (Details):** A table showing the mapping of certificate properties to database items.

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

The '保存' (Save) button is located in the top right corner of the main content area.

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。

This screenshot is identical to the previous one, showing the 'デフォルト設定' page. The 'ダイジェストアルゴリズム' (Digest Algorithm) is now set to SHA256, and the '鍵長' (Key Length) is 2048bit. The '保存' (Save) button is highlighted in the top right corner.

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