

SecureWare/Credential Lifecycle Manager

WebAPI リファレンス

2017年10月
日本電気株式会社

はしがき

本書は、SecureWare/Credential Lifecycle Manager(以下、CLM と称します)が提供します WebAPI について説明したものです。

本書の構成は以下のとおりです。

章	タイトル	内容
1	WebAPI 一覧	WebAPI の一覧と概要の説明
2	WebAPI の認証	WebAPI 使用時に行う認証についての説明
3	ID・パスワード管理 API	ID・パスワード管理 API についての説明
4	証明書管理 API	証明書管理 API についての説明
5	共通鍵管理 API	共通鍵管理 API についての説明
6	CLM 管理 API	CLM 管理 API についての説明

◎付録

付録	タイトル	内容
1	エラーコード一覧	WebAPI が返却するエラーコードの一覧

2017 年 10 月 第一版

目次

1	WebAPI 一覧	4
2	WebAPI の認証	5
2.1	ライセンスキー認証	5
2.2	ID・パスワード(事前共有キー)認証	5
3	ID・パスワード管理 API	6
3.1	ID・パスワード発行 API	6
3.2	ID・パスワード取得 API	8
3.3	ID・パスワード照合 API	10
3.4	ID・パスワード削除 API	12
4	証明書管理 API	14
4.1	証明書発行 API	14
4.2	証明書取得 API	20
4.3	証明書更新 API	24
4.4	証明書失効 API	28
5	共通鍵管理 API	31
5.1	共通鍵発行 API	31
5.2	共通鍵取得 API	35
5.3	共通鍵更新 API	37
5.4	共通鍵削除 API	40
6	CLM 管理 API	43
6.1	WebAPI サーバ稼動状態確認 API	43
7	付録	44
7.1	エラーコード一覧	44

1 WebAPI 一覧

CLM で提供する WebAPI を表 1-1 示します。

表内のライセンスキー認証と ID・パスワード(事前共有キー)認証については、2 章をご覧ください。

表 1-1 CLM WebAPI 一覧

	API 名	メソッド	URI	説明	認証方式	
					ライセンスキー認証	ID・パスワード(事前共有キー)認証
ID/PWD (事前共有キー) 入手	ID・パスワード 発行	POST	/SWCLM/v10/IDInfo	ID・パスワード(事前共有キー)を生成する。パスワードの複雑さはサーバ側の設定に従う。	○	
	ID・パスワード 取得	GET	/SWCLM/v10/IDInfo[?keyid=<ID>]	ID・パスワード発行で生成した ID・パスワード(事前共有キー)を取得する。	○	
ID/PWD (事前共有キー) 照合(認証)	ID・パスワード 照合	POST	/SWCLM/v10/IDInfo	ID・パスワード(事前共有キー)を照合(認証)する。	○	○
ID/PWD (事前共有キー) 削除	ID・パスワード 削除	POST	/SWCLM/v10/IDInfo	ID・パスワード発行で生成した ID・パスワード(事前共有キー)を削除する。	○	○
証明書発行・取得	証明書発行	POST	/SWCLM/v10/CredInfo	公開鍵証明書を発行する。CA 証明書を取得する。	○	○
	証明書取得	POST	/SWCLM/v10/CredInfo	CA 証明書、公開鍵証明書を取得する。	○	○
証明書更新・失効	証明書発行	POST	/SWCLM/v10/CredInfo	公開鍵証明書を更新する。	○	○
	証明書取得	POST	/SWCLM/v10/CredInfo	公開鍵証明書を失効する。	○	○
共通鍵発行・取得	証明書発行	POST	/SWCLM/v10/KeyInfo	共通鍵を発行する。	○	○
	証明書取得	POST	/SWCLM/v10/KeyInfo	共通鍵を取得する。	○	○
共通鍵更新・削除	共通鍵更新	POST	/SWCLM/v10/KeyInfo	共通鍵を更新する。	○	○
	共通鍵削除	POST	/SWCLM/v10/KeyInfo	共通鍵を削除する。	○	○

2 WebAPI の認証

本章では、WebAPI を利用する際に行う認証について説明します。

2.1 ライセンスキー認証

WebAPI を使用するには、ライセンスキー認証を行います。

CLM ではライセンスキー認証として Basic 認証を使用します。WebAPI を実行すると、Basic 認証 (ID/Password の入力)が要求されますので、表 2-1 に示す ID/Password を入力します。

表 2-1 Basic 認証の ID/Password

ID	Password
secureware-clm	セットアップカード記載のライセンスキー

2.2 ID・パスワード(事前共有キー)認証

CLM の WebAPI は、一部の WebAPI を除き、WebAPI 実行時に ID・パスワード(事前共有キー)認証を行います。

認証に使用する ID・パスワード(事前共有キー)は、ID・パスワード発行 API で発行します。

また、ID・パスワード(事前共有キー)認証が必要な WebAPI を実行する際には、WebAPI のリクエストパラメータに ID・パスワード発行 API で発行した ID・パスワード(事前共有キー)を指定します。

3 ID・パスワード管理 API

本章では、WebAPI で提供する「ID・パスワード発行・取得・照合・削除」API について説明します。

3.1 ID・パスワード発行 API

ID・パスワード発行 API は、エッジなどのデバイスをクラウド環境に接続する際に、エッジとクラウド間の通信を安全に行うための ID・パスワード(事前共有キー)を発行します。

パスワードの複雑さは CLM の設定に従います。

リクエスト URL	メソッド
<a href="https://<サーバ名>/SWCLM/v10/IDInfo">https://<サーバ名>/SWCLM/v10/IDInfo	POST

リクエストパラメータ

パラメータ	必須/任意	説明
mode	必須	実行モード。「create」を指定してください。
tenanted	必須	テナント ID。
alias	必須	ID・パスワードに付与する Alias 名。

リクエストパラメータの例を以下に示します。

表 3-1 ID・パスワード発行 API リクエストパラメータ(例)

```
{  
  "mode": "create",  
  "tenantid": "tenant01",  
  "alias": "DemoKey1"  
}
```

レスポンスコード

レスポンスコード	説明
201 Created	発行成功
400 Bad Request	リクエスト情報不正
500 Internal Server Error	内部エラー

レスポンスパラメータ

パラメータ	説明
errorcode	エラーコード。 詳細は、「付録. エラーコード一覧」を参照してください。
keyid	生成した ID。
key	生成したパスワード。
alias	ID・パスワードの Alias 名。
expiration	有効期限。 1970/1/1 00:00:00 (UTC) からの経過時間(単位: ミリ秒)で表します。

レスポンスパラメータの例を以下に示します。

表 3-2 ID・パスワード発行 API レスポンスパラメータ(例)

```
{  
  "errorcode": 0,  
  "keyid": "0000000001",  
  "key": "cGFzc3dv",  
  "alias": "DemoKey1",  
  "expiration" :"4645682569766"  
}
```

3.2 ID・パスワード取得 API

ID・パスワード取得 API は、ID・パスワード発行 API で発行した ID・パスワード(事前共有キー)を取得します。

リクエスト URL

メソッド

`https://<サーバ名>/SWCLM/v10/IDInfo?keyid=<ID>` GET

リクエストパラメータ

パラメータ	必須/任意	説明
keyid	任意	ID・パスワード発行 API で発行した ID。

レスポンスコード

レスポンスコード	説明
200 OK	取得成功
400 Bad Request	リクエスト情報不正
500 Internal Server Error	内部エラー

レスポンスパラメータ

パラメータ	説明
errorcode	エラーコード。 詳細は、「付録. エラーコード一覧」を参照してください。
keyid	リクエストパラメータ の keyid に指定した ID。
keyinfo	取得した ID・パスワード(事前共有キー)情報。 取得可能な ID・パスワード(事前共有キー)が存在しない、または ID が無効である場合は、空の配列。
keyid	取得した ID。
key	取得したパスワード。
alias	取得した ID・パスワードの Alias 名。
tenantid	テナント ID。
expiration	有効期限。 1970/1/1 00:00:00 (UTC) からの経過時間(単位: ミリ秒)で表します。

レスポンスパラメータの例を以下に示します。

表 3-3 ID・パスワード取得 API レスポンスパラメータ(例)

```
{  
  "errorcode": 0,  
  "keyinfo": [  
    {"keyid": "0000000001",  
     "key": "cGFzc3dv",  
     "alias": "DemoKey1",  
     "tenantid": "tenant01",  
     "expiration" : "4645682569766"}  
  ]  
}
```

3.3 ID・パスワード照合 API

ID・パスワード照合 API は、リクエスト送信元デバイスが所有している ID・パスワード(事前共有キー)と、CLM に登録されている ID・パスワード(事前共有キー)が一致するかを照合(認証)します。

リクエスト URL

`https://<サーバ名>/SWCLM/v10/IDInfo`

メソッド

POST

リクエストパラメータ

パラメータ	必須/任意	説明
mode	必須	実行モード。「auth」固定。
keyid	必須	ID・パスワード発行 API で発行した ID。
key	必須	ID・パスワード発行 API で発行した ID のパスワード。

リクエストパラメータの例を以下に示します。

表 3-4 ID・パスワード照合 API リクエストパラメータ(例)

```
{  
  "mode": "auth",  
  "keyid": "00000000001",  
  "key": "cGFzc3dv"  
}
```

レスポンスコード

レスポンスコード	説明
200 OK	照合成功
400 Bad Request	リクエスト情報不正
403 Forbidden	認証エラー
404 Not Found	照合失敗
500 Internal Server Error	内部エラー

レスポンスパラメータ

パラメータ	説明
errorcode	エラーコード。 詳細は、「付録. エラーコード一覧」を参照してください。
keyid	照合を行った ID。

レスポンスパラメータの例を以下に示します。

表 3-5 ID・パスワード照合 API レスポンスパラメータ(例)

```
{  
  "errorcode": 0,  
  "keyid": "0000000001"  
}
```

3.4 ID・パスワード削除 API

ID・パスワード削除 API は、ID・パスワード発行 API で発行した ID・パスワード(事前共有キー)を削除します。

リクエスト URL

https://<サーバ名>/SWCLM/v10/IDInfo

メソッド

POST

リクエストパラメータ

パラメータ	必須/任意	説明
mode	必須	実行モード。「delete」を指定してください。
keyid	必須	ID・パスワード発行 API で発行した ID。
key	必須	ID・パスワード発行 API で発行した ID のパスワード。

リクエストパラメータの例を以下に示します。

表 3-6 ID・パスワード削除 API リクエストパラメータ(例)

```
{  
  "mode": "delete",  
  "keyid": "00000000001",  
  "key": "cGFzc3dv"  
}
```

レスポンスコード

レスポンスコード	説明
200 OK	削除成功
400 Bad Request	リクエスト情報不正
403 Forbidden	認証エラー
404 Not Found	削除失敗
500 Internal Server Error	内部エラー

レスポンスパラメータ

パラメータ	説明
errorcode	エラーコード。 詳細は、「付録. エラーコード一覧」を参照してください。
keyid	削除した ID。

レスポンスパラメータの例を以下に示します。

表 3-7 ID・パスワード削除 API レスポンスパラメータ(例)

```
{  
  "errorcode": 0,  
  "keyid": "0000000001"  
}
```

4 証明書管理 API

4.1 証明書発行 API

証明書発行 API は、証明書を発行・取得します。

発行した証明書は、CLM でリクエスト送信元デバイスとの紐づけを行い、管理します。本 API で発行・取得可能な証明書は、次の通りです。

表 4-1 証明書発行 API 発行・取得可能な証明書一覧

発行・取得可能な証明書	証明書形式	証明書	証明書 密鑑	CA 証明書
CA 証明書	pem、der			<input type="radio"/> ※1
公開鍵証明書				
サーバ証明書	pem、der	<input type="radio"/>	<input type="radio"/> ※2	<input type="radio"/> ※3
クライアント証明書	pem、der	<input type="radio"/>	<input type="radio"/> ※2	<input type="radio"/> ※3
	PKCS#12(chain なし)	<input type="radio"/>	<input type="radio"/> ※4	

※1: 証明書発行 API で「CA 証明書の発行」を行うと、CLM が連携する CA の CA 証明書を取得します。

※2: 密鑑の形式は、pem です。der 形式の証明書を発行した場合も、密鑑は pem 形式となります。

※3: 証明書を発行した CA の CA 証明書を取得します。証明書発行で取得する CA 証明書は、「CA 証明書の発行」で取得する CA 証明書と同一です。

※4: 密鑑は、証明書に同梱されています。

リクエスト URL

メソッド

<https://<サーバ名>/SWCLM/v10/CredInfo>

POST

リクエストパラメータ

パラメータ	必須/任意	説明
mode	必須	実行モード。 「create」を指定してください。
keyid	必須	ID・パスワード発行 API で発行した ID。
key	必須	ID・パスワード発行 API で発行した ID のパスワード。
deviceid	任意	デバイス ID。 リクエスト送信元デバイスから CLA や WebAPI、クライアントライブラリを使用して証明書発行や共通鍵発行を行ったことがない場合、本パラメータは省略してください。

		リクエスト送信元デバイスから CLA や WebAPI、クライアントライブラリを使用して証明書発行や共通鍵発行を行ったことがある場合は、証明書発行や共通鍵発行を行った際に取得したレスポンスパラメータの「devieid」値を本パラメータに指定してください。
devicename	必須	<p>デバイス名。</p> <p>最大文字列長は、256byte です。</p> <p>リクエスト送信元デバイスから CLA や WebAPI、クライアントライブラリを使用して証明書発行や共通鍵発行を行ったことがない場合、本パラメータにリクエスト送信元デバイスを特定可能な名称(デバイス名)を指定してください。</p> <p>リクエスト送信元デバイスから CLA や WebAPI、クライアントライブラリを使用して証明書発行や共通鍵発行を行ったことがある場合は、初回発行時に指定したデバイス名を指定してください。</p>
certmode	必須	<p>取得する証明書の種別。</p> <p>以下のいずれかを指定してください。</p> <p>caonly : CA 証明書を取得</p> <p>client : サーバ証明書、クライアント証明書を取得</p>
catype	必須	<p>証明書を発行する認証局の名称。</p> <p>以下のいずれかを指定してください。</p> <p>CA: リクエストパラメータ certmode が「caonly」である場合</p> <p>ca1: リクエストパラメータ certmode が「client」である場合</p>
cacerttype	任意	<p>CA 証明書の種別。</p> <p>以下いずれかを指定してください。</p> <p>pem: pem 形式の証明書 (本パラメータ省略時の既定値)</p> <p>der : der 形式の証明書</p>
clientcerttype	任意	<p>サーバ証明書、クライアント証明書の種別。</p> <p>以下のいずれかを指定してください。</p> <p>pem: pem 形式の証明書 (本パラメータ省略時の既定値)</p> <p>der : der 形式の証明書</p> <p>p12 : PKCS#12 形式の証明書(chain なし)</p>

clientsubject	任意 ※certmode が 「client」の場合は 必須です。	サーバ証明書、クライアント証明書のサブジェクト。 「/C=国別コード/ST=都道府県名/L=市区町村名/O=部 門名/OU=組織名/CN=コモンネーム」 の形式で指定してください。 「/CN=コモンネーム」以外は省略可能です。 最大文字列長は、512byte です。
passphrase	任意 ※clientcerttype が 「p12」の場合は必須で す。	サーバ証明書、クライアント証明書の秘密鍵のパスフ レーズ。 最大文字列長は、128byte です。 クライアント証明書の種別に「p12」が指定された場合、 PKCS#12 形式に変換する際のパスフレーズにも利用 します。
keyfilepath	必須	パスワード保存ファイルパス CLM の管理情報として使用します。 「/tmp/key」を指定してください。
caffilepath	任意 ※以下のいずれかに該当 する場合は必須です。 certmode が「caonly」。 clientcerttype が「pem」。	CA 証明書保存ファイルパス。 最大文字列長は、1024byte です。 リクエスト送信元デバイス上のファイルパスを指定し てください。
clientfilepath	任意 ※certmode が「client」 の場合は必須です。	サーバ証明書、クライアント証明書保存ファイルパス。 最大文字列長は、1024byte です。 リクエスト送信元デバイス上のファイルパスを指定し てください。
ipaddress	任意	デバイスの IP アドレス。
macaddress	任意	デバイスの MAC アドレス。 以下のいずれかの形式で指定してください。 12:34:56:78:90:12 12-34-56-78-90-12 123456789012

ext_data	任意	<p>付加情報。</p> <p>項目名と項目値を配列で指定してください。</p> <p>項目名の最大文字列長は、128byte です。また項目値の最大文字列長は、256byte です。</p> <p>既定で指定可能な付加情報は、次の通りです。</p> <p>また、以下以外に、任意の付加情報も指定可能です。</p> <table border="1"> <thead> <tr> <th>項目名</th><th>説明</th></tr> </thead> <tbody> <tr> <td>osname</td><td>OS 名</td></tr> <tr> <td>osversion</td><td>OS バージョン</td></tr> <tr> <td>architecture</td><td>アーキテクチャ</td></tr> <tr> <td>cpuname</td><td>CPU 名</td></tr> <tr> <td>memoriesize</td><td>メモリサイズ</td></tr> <tr> <td>hostname</td><td>ホスト名</td></tr> <tr> <td>computername</td><td>コンピュータ名</td></tr> </tbody> </table>	項目名	説明	osname	OS 名	osversion	OS バージョン	architecture	アーキテクチャ	cpuname	CPU 名	memoriesize	メモリサイズ	hostname	ホスト名	computername	コンピュータ名
項目名	説明																	
osname	OS 名																	
osversion	OS バージョン																	
architecture	アーキテクチャ																	
cpuname	CPU 名																	
memoriesize	メモリサイズ																	
hostname	ホスト名																	
computername	コンピュータ名																	

リクエストパラメータの例を以下に示します。

表 4-2 証明書発行 API リクエストパラメータ(例・クライアント証明書(pem 形式)を発行)

```
{
  "mode": "create",
  "keyid": "0000000001",
  "key": "cGFzc3dv",
  "devicename": "nec-edge-0001",
  "certmode": "client",
  "catype": "ca1",
  "clientsubject": "/C=JP/L=Tokyo/O=NEC/CN=AP1",
  "keyfilepath": "/tmp/key",
  "cafepath": "/etc/opt/nec/swclm/keyfile/cacert.pem",
  "clientfilepath": "/etc/opt/nec/swclm/keyfile/clcert.pem",
  "ipaddress": "192.168.0.1",
  "macaddress": "aa:aa:aa:aa:aa:aa",
  "ext_data": {"osname": "CentOS", "osversion": "6.8", "memoriesize": "2048MB", "flag": "1"}
}
```

レスポンスコード

レスポンスコード	説明
201 Created	登録成功
400 Bad Request	リクエスト情報不正
403 Forbidden	認証エラー
404 Not Found	発行エラー
500 Internal Server Error	内部エラー

レスポンスパラメータ

パラメータ	説明
errorcode	エラーコード。 詳細は、「付録 エラーコード一覧」を参照してください。
deviceid	デバイス ID。 リクエストパラメータ deviceid 未指定時は、CLM が採番した値。 リクエストパラメータ deviceid 指定時は、リクエストパラメータ deviceid と同じ値。
devicekey	デバイスキー。 リクエストパラメータ deviceid 未指定時の場合は、CLM が採番した値。 上記以外である場合は、レスポンスパラメータ省略。
cacert	CA 証明書。 証明書形式が der 形式である場合は Base64 エンコードした文字列。
cacerttype	CA 証明書の種別(pem、der のいずれか)。
cakeynumber	証明書の鍵番号。
caserial	証明書のシリアル番号。
clientcert	証明書(サーバ証明書またはクライアント証明書)。 証明書形式が der 形式、PKCS#12 形式である場合、Base64 エンコードした文字列。
clientcerttype	証明書の種別(pem、der、p12 のいずれか)。
clientkeynumbe	証明書の鍵番号。
clientserial	証明書のシリアル番号。
privatekey	証明書の秘密鍵。pem 形式。

レスポンスパラメータの例を以下に示します。

表 4-3 証明書発行 API レスポンスパラメータ(例)

```
{  
    "errorcode": 0,  
    "deviceid": "1234567890abcdefghijklmnopqrstuvwxyz",  
    "cacert": "-----BEGIN CERTIFICATE-----\nMIIDtDCCApAgAwIBAgIJAL2XwoalwjiIMA0GCSqGSIb  
3DQEBCwUAMFUxCzAJBgNV\n<省略>\n-----END CERTIFICATE-----",  
    "cacerttype": "pem",  
    "cakeynumber": "3",  
    "caserial": "863542E528A722EE",  
    "clientcert": "-----BEGIN CERTIFICATE-----\nMIIDgDCCAmigAwIBAgIJAL2XwoalwjiDMA0GCSq  
GSIb3DQEBCwUAMFUxCzAJBgNV\n<省略>\n-----END CERTIFICATE-----",  
    "clientcerttype": "pem"  
    "clientkeynumber": "2",  
    "clientserial": "863542E528A7233F",  
    "privatekey": "-----BEGIN PRIVATE KEY-----\nMIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwgg  
SjAgEAAoIBAQc4KT9F6a0EOAG0\n<省略>\n-----END PRIVATE KEY-----\n"  
}
```

4.2 証明書取得 API

発行済みの証明書を取得します。

取得の際、証明書の形式を変換することが可能です(例: pem 形式で発行した証明書を der 形式で取得)。

取得した証明書は、CLM でリクエスト送信元デバイスとの紐づけを行い、管理します。

本 API で取得可能な証明書は、次の通りです。

表 4-4 証明書取得 API 取得可能な証明書一覧

発行・取得可能な証明書	証明書形式	証明書	証明書 密鑑	CA 証明書
CA 証明書	pem、der			<input type="radio"/> ※1
公開鍵証明書				
サーバ証明書	pem、der	<input type="radio"/>	<input type="radio"/> ※2	
クライアント証明書	pem、der	<input type="radio"/>	<input type="radio"/> ※2	
	PKCS#12(chain なし)	<input type="radio"/>	<input type="radio"/> ※3	

※1: CLM が連携する CA の CA 証明書を取得します。

※2: 密鑑の形式は、pem です。der 形式の証明書を取得した場合も、密鑑は pem 形式となります。

※3: 密鑑は、証明書に同梱されています。

リクエスト URL

メソッド

https://<サーバ名>/SWCLM/v10/CredInfo

POST

リクエストパラメータ

パラメータ	必須/任意	説明
mode	必須	実行モード。「get」を指定してください。
keyid	必須	ID・パスワード発行 API で発行した ID。
key	必須	ID・パスワード発行 API で発行した ID のパスワード。
deviceid	必須	デバイス ID。
devicename	必須	デバイス名。
keynumber	任意 ※certserial を指定しない場合は必須です。	取得対象証明書の鍵番号。
certserial	任意 ※keynumber を指定しない場合は必須です。	取得対象証明書のシリアル番号。

catype	必須	取得対象証明書を発行した認証局の名称。 以下のいずれかを指定してください。 CA: CA 証明書を取得したい場合 ca1: 公開鍵証明書を取得したい場合
certtype	任意	取得対象証明書の種別。 以下のいずれかを指定してください。 pem: pem 形式の証明書 (本パラメータ省略時の既定値) der : der 形式の証明書 p12 : PKCS#12 形式の証明書(chain なし)
passphrase	任意 ※certtype が「p12」で、 発行済みの証明書の形式 が PKCS#12 ではない場 合は必須です。	発行済みの証明書の形式を PKCS#12 に変換する際に 使用するパスフレーズ。
filepath	必須	取得対象証明書保存ファイルパス。 最大文字列長は、1024byte です。 リクエスト送信元デバイス上のファイルパスを指定 してください。

リクエストパラメータの例を以下に示します。

表 4-5 証明書取得 API リクエストパラメータ(例 CA 証明書をシリアル番号指定で取得)

```
{
  "mode": "get",
  "keyid": "0000000001",
  "key": "cGFzc3dv",
  "deviceid": "0000000001",
  "devicename": "nec-edge-0001",
  "certserial": "863542E528A7233F",
  "catype": "CA",
  "certtype": "pem",
  "filepath": "/etc/opt/nec/swclm/keyfile/cacert.pem"
}
```

表 4-6 証明書取得 API リクエストパラメータ(例 クライアント証明書を鍵番号指定で取得)

```
{  
  "mode": "get",  
  "keyid": "0000000001",  
  "key": "cGFzc3dv",  
  "deviceid": "0000000001",  
  "devicename": "nec-edge-0001",  
  "keynumber": "2",  
  "catype": "ca1",  
  "certtype": "pem",  
  "filepath": "/etc/opt/nec/swclm/keyfile/clcert.pem"  
}
```

レスポンスコード

レスポンスコード	説明
200 OK	取得成功
400 Bad Request	リクエスト情報不正
403 Forbidden	認証エラー
404 Not Found	取得エラー
500 Internal Server Error	内部エラー

レスポンスパラメータ

パラメータ	説明
errorcode	エラーコード。 詳細は、「付録. エラーコード一覧」を参照してください。
deviceid	デバイス ID。 リクエストパラメータ deviceid 未指定時は、CLM が採番した値。 リクエストパラメータ deviceid 指定時は、リクエストパラメータ deviceid と同じ値。
cacert	CA 証明書。証明書形式が der 形式である場合は Base64 エンコードした文字列。
cacerttype	CA 証明書の種別(pem、der のいずれか)。
cakeynumber	証明書の鍵番号。
caserial	証明書のシリアル番号。

clientcert	証明書(サーバ証明書またはクライアント証明書)。 証明書形式が der 形式、PKCS#12 形式である場合、Base64 エンコードした文字列。
clientcerttype	証明書の種別(pem、der、p12 のいずれか)。
clientkeynumbe	証明書の鍵番号。
clientserial	証明書のシリアル番号。
privatekey	証明書の秘密。pem 形式。

レスポンスパラメータの例を以下に示します。

表 4-7 証明書取得 API レスポンスパラメータ(例 CA 証明書をシリアル番号指定で取得)

```
{
  "errorcode": 0,
  "deviceid": "0000000001",
  "cacert": "-----BEGIN CERTIFICATE-----\nMIIDgDCCAmigAwIBAgIJAL2XwoalwjiDMA0GCSqG
SIb3DQEBCwUAMFUxCzAJBgNV<省略>\n-----END CERTIFICATE-----\n",
  "cacerttype": "pem",
  "cakeynumber": "2",
  "caserial": "863542E528A7233F"
}
```

表 4-8 証明書取得 API レスポンスパラメータ(例 クライアント証明書を鍵番号指定で取得)

```
{
  "errorcode": 0,
  "deviceid": "0000000001",
  "clientcert": "-----BEGIN CERTIFICATE-----\nMIIDgDCCAmigAwIBAgIJAL2XwoalwjiDMA0GCS
qGSIB3DQEBCwUAMFUxCzAJBgNV<省略>\n-----END CERTIFICATE-----\n",
  "clientcerttype": "pem",
  "clientkeynumber": "2",
  "clientserial": "863542E528A7233F",
  "privatekey": "-----BEGIN PRIVATE KEY-----\nMIIDgDCCAmigAwIBAgIJAL2XwoalwjiDMA0GCS
qGSIB3DQEBCwUAMFUxCzAJBgNV<省略>\n-----END PRIVATE KEY-----\n"
}
```

4.3 証明書更新 API

証明書更新 API は、発行済みの公開鍵証明書を更新し、発行済みの公開鍵証明書と同一の Subject を持つ新しい公開鍵証明書を取得します。

取得の際、新しい公開鍵証明書を発行せず、既存の公開鍵証明書を更新後の公開鍵証明書として取得することができます。

また、証明書の形式を変換することも可能です(例: pem 形式で発行した証明書を der 形式で更新)。

更新した公開鍵証明書は、CLM でリクエスト送信元デバイスとの紐づけを行い、管理します。

リクエスト URL

メソッド

<https://<サーバ名>/SWCLM/v10/CredInfo>

POST

リクエストパラメータ

パラメータ	必須/任意	説明
mode	必須	実行モード。「update」を指定してください。
keyid	必須	ID・パスワード発行 API で発行した ID。
key	必須	ID・パスワード発行 API で発行した ID のパスワード。
deviceid	必須	デバイス ID。
devicename	必須	デバイス名。
keynumber	任意 ※certserial を指定しない場合は必須です。	更新対象証明書の鍵番号。
certserial	任意 ※keynumber を指定しない場合は必須です。	更新対象証明書のシリアル番号。
newkeynumber	任意	更新後の証明書の鍵番号。 既存の証明書を更新後証明書としたい場合に指定してください。
newcertserial	任意	更新後の証明書のシリアル番号。 既存の証明書を更新後証明書としたい場合に指定してください。

catype	必須	更新対象証明書を発行した認証局の名称。 「ca1」を指定してください。
certtype	任意	更新後の証明書の種別。 以下のいずれかを指定してください。 pem: pem 形式の証明書 (本パラメータ省略時の既定値) der : der 形式の証明書 p12 : PKCS#12 形式の証明書(chain なし)
passphrase	任意 ※[条件]に該当する場合は必須(右記の説明内を参照してください)。	更新後の証明書の秘密鍵のパスフレーズ。 certtype に「p12」が指定された場合、PKCS#12 形式に変換する際のパスフレーズにも利用します。 [条件] 以下のいずれかに該当する場合、passphrase の指定は必須です。 ・ newkeynumber または newcertserial を指定しない場合 ・ newkeynumber または newcertserial を指定、かつ certtype が「p12」で、 newkeynumber または newcertserial に該当する証明書の形式が PKCS#12 ではない場合
filepath	必須	更新対象証明書保存ファイルパス。 最大文字列長は、 1024byte です。 リクエスト送信元デバイス上のファイルパスを指定してください。 ・ 証明書発行 API で発行した証明書を更新する場合は、証明書発行 API のリクエストパラメータ clientfilepath で指定したファイルパスを指定してください。 ・ 証明書取得 API で取得した証明書を更新する場合は、証明書取得 API のリクエストパラメータ filepath で指定したファイルパスを指定してください。
newfilepath	必須 ※filepath と値が同じである場合は任意です。	更新後証明書の保存ファイルパス。 最大文字列長は、 1024byte です。 リクエスト送信元デバイス上のファイルパスを指定してください。

リクエストパラメータの例を以下に示します。

表 4-9 証明書更新 API リクエストパラメータ(例)

```
{  
  "mode": "update",  
  "keyid": "0000000001",  
  "key": "cGFzc3dv",  
  "deviceid": "0000000001",  
  "devicename": "nec-edge-0001",  
  "keynumber": "54",  
  "catype": "ca1",  
  "certtype": "pem",  
  "filepath": "/etc/opt/nec/swclm/keyfile/clcert.pem",  
  "newfilepath": "/etc/opt/nec/swclm/keyfile/clcert_upd.pem"  
}
```

レスポンスコード

レスポンスコード	説明
200 OK	取得成功
400 Bad Request	リクエスト情報不正
403 Forbidden	認証エラー
404 Not Found	取得エラー
500 Internal Server Error	内部エラー

レスポンスパラメータ

パラメータ	説明
errorcode	エラーコード。 詳細は、「付録. エラーコード一覧」を参照してください。
deviceid	リクエストパラメータに指定したデバイス ID。
clientcert	更新後の証明書。 証明書形式が der 形式、または PKCS#12 形式である場合、Base64 エンコードした文字列。
clientcerttype	更新後の証明書の種別(pem、der、p12 のいずれか)。
clientkeynumber	更新後の証明書の鍵番号。
clientserial	更新後の証明書のシリアル番号。

privatekey	更新後の証明書の秘密鍵。pem 形式。
------------	---------------------

レスポンスパラメータの例を以下に示します。

表 4-10 証明書更新 API レスポンスパラメータ(例)

```
{  
  "errorcode": 0,  
  "deviceid": "0000000001",  
  "clientcert": "-----BEGIN CERTIFICATE-----  
  MIIDNjCCAh6gAwIBAgIJAN6 6ttSoJXygMA0GCS  
  qGSIb3DQEBCwUAMBwxwUAMB <省略>  
  -----END CERTIFICATE-----  
  ",  
  "clientcerttype": "pem",  
  "clientkeynumber": "55",  
  "clientserial": "DEBAB6D4A8257CA0",  
  "privatekey": "-----BEGIN PRIVATE KEY-----  
  MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcw  
  ggSjAgEAAoIBAQDPnN0iBxqrAA <省略>  
  -----END PRIVATE KEY-----  
 }
```

4.4 証明書失効 API

証明書失効 API は、証明書発行 API、証明書取得 API、証明書更新 API で発行・取得・更新した公開鍵証明書を失効します。

リクエスト URL

https://<サーバ名>/SWCLM/v10/CredInfo

メソッド

POST

リクエストパラメータ

パラメータ	必須/任意	説明
mode	必須	実行モード。「revoke」を指定してください。
keyid	必須	ID・パスワード発行 API で発行した ID。
key	必須	ID・パスワード発行 API で発行した ID のパスワード。
deviceid	必須	デバイス ID。
devicename	必須	デバイス名。
keynumber	任意 ※ certserial を指定しない場合は必須です。	失効対象証明書の鍵番号。
certserial	任意 ※ keynumber を指定しない場合は必須です。	失効対象証明書のシリアル番号。
catype	必須	失効対象証明書を発行した認証局の名称。 「ca1」を指定してください。
filepath	任意	失効対象証明書の保存ファイルパス。最大文字列長は、1024byte です。 リクエスト送信元デバイス上のファイルパスを指定してください。 ・証明書発行 API で発行した証明書を失効する場合は、証明書発行 API のリクエストパラメータ clientfilepath で指定したファイルパスを指定してください。 ・証明書取得 API で取得した証明書を失効する場合は、証明書取得 API のリクエストパラメータ filepath で指定したファイルパスを指定してください。 ・証明書更新 API で更新した証明書を失効する場合は、

		証明書更新 API のリクエストパラメータ newfilepath で指定したファイルパス(newfilepath 省略時は filepath で指定したファイルパス)を指定してください。
--	--	--

リクエストパラメータの例を以下に示します。

表 4-11 証明書失効 API リクエストパラメータ(例)

{ "mode": "revoke", "keyid": "00000000001", "key": "cGFzc3dv", "deviceid": "0000000001", "devicename": "nec-edge-0001", "keynumber": "54", "catype": "ca1", "filepath": "/etc/opt/nec/swclm/keyfile/clcert.pem" }
--

レスポンスコード

レスポンスコード	説明
200 OK	失効成功
400 Bad Request	リクエスト情報不正
403 Forbidden	認証エラー
404 Not Found	失効エラー
500 Internal Server Error	内部エラー

レスポンスパラメータ

パラメータ	説明
errorcode	エラーコード。 詳細は、「付録. エラーコード一覧」を参照してください。
deviceid	リクエストで指定したデバイス ID。
clientkeynumber	失効した公開鍵証明書の鍵番号。
clientserial	失効した公開鍵証明書のシリアル番号。

レスポンスパラメータの例を以下に示します。

表 4-12 証明書失効 API レスポンスパラメータ(例)

```
{  
  "errorcode": 0,  
  "deviceid": "0000000001",  
  "clientkeynumber": "55",  
  "clientserial": "DEBAB6D4A8257CA0"  
}
```

5 共通鍵管理 API

5.1 共通鍵発行 API

共通鍵発行 API は、共通鍵を発行します。

発行した共通鍵は、CLM でリクエスト送信元デバイスとの紐づけを行い、管理します。

本 API で発行可能な共通鍵は、下記の通りです。

- AES 用の鍵(鍵長 128bit、256bit)
- TWINE 用の鍵(鍵長 80bit、256bit)

リクエスト URL

<https://<サーバ名>/SWCLM/v10/KeyInfo>

メソッド

POST

リクエストパラメータ

パラメータ	必須/任意	説明
mode	必須	実行モード。「create」を指定してください。
keyid	必須	ID・パスワード発行 API で発行した ID。
key	必須	ID・パスワード発行 API で発行した ID のパスワード。
deviceid	任意	デバイス ID。 リクエスト送信元デバイスから CLA や WebAPI、クラシアントライブラリを使用して証明書発行や共通鍵発行を行ったことがない場合、本パラメータは省略してください。 リクエスト送信元デバイスから CLA や WebAPI、クラシアントライブラリを使用して証明書発行や共通鍵発行を行ったことがある場合は、証明書発行や共通鍵発行を行った際に取得したレスポンスパラメータの「devieid」値を本パラメータに指定してください。
devicename	任意	デバイス名。 最大文字列長は、256byte です。 リクエスト送信元デバイスから CLA や WebAPI、クラシアントライブラリを使用して証明書発行や共通鍵発行を行ったことがない場合、本パラメータにリクエスト送信元デバイスを特定可能な名称(デバイス名)を指定してください。

		リクエスト送信元デバイスから CLA や WebAPI、クライアントライブラリを使用して証明書発行や共通鍵発行を行ったことがある場合は、初回発行時に指定したデバイス名を指定してください。												
alias	必須	共通鍵に付与する Alias。最大文字列長は、64byte です。												
keylength	任意	発行する共通鍵の長さ(単位: bit)。 省略時の既定値は 128(bit)です。												
keytype	必須	鍵を利用する暗号化方式。 以下のいずれかを指定してください。 AES : AES で利用する TWINE: TWINE で利用する												
keyfilepath	必須	パスワード保存ファイルパス(Max: 1024 byte)。 CLM の管理情報として使用します。 「/tmp/key」を指定してください。												
commonkeyfilepath	必須	共通鍵保存ファイルパス。最大文字列長は、1024byte です。 リクエスト送信元デバイス上のファイルパスを指定してください。												
ipaddress	任意	デバイスの IP アドレス。												
macaddress	任意	デバイスの MAC アドレス。 以下のいずれかの形式で指定してください。 12:34:56:78:90:12 12-34-56-78-90-12 123456789012												
ext_data	任意	付加情報。 項目名と項目値を配列で指定してください。 項目名の最大文字列長は、128byte です。また項目値の最大文字列長は、256byte です。 既定で指定可能な付加情報は、次の通りです。 また、以下以外に、任意の付加情報も指定可能です。												
		<table border="1"> <thead> <tr> <th>項目名</th><th>説明</th></tr> </thead> <tbody> <tr> <td>osname</td><td>OS 名</td></tr> <tr> <td>osversion</td><td>OS バージョン</td></tr> <tr> <td>architecture</td><td>アーキテクチャ</td></tr> <tr> <td>cpuname</td><td>CPU 名</td></tr> <tr> <td>memoriesize</td><td>メモリサイズ</td></tr> </tbody> </table>	項目名	説明	osname	OS 名	osversion	OS バージョン	architecture	アーキテクチャ	cpuname	CPU 名	memoriesize	メモリサイズ
項目名	説明													
osname	OS 名													
osversion	OS バージョン													
architecture	アーキテクチャ													
cpuname	CPU 名													
memoriesize	メモリサイズ													

hostname	ホスト名
computername	コンピュータ名

リクエストパラメータの例を以下に示します。

表 5-1 共通鍵発行 API リクエストパラメータ

{
"mode": "create",
"keyid": "00000000001",
"key": "cGFzc3dv",
"devicename": "device01",
"ipaddress": "192.168.0.1",
"macaddress": "aa:aa:aa:aa:aa:aa",
"alias": "iotgatewaytest cmkey",
"keyfilepath": "/tmp/key",
"keylength": "128",
"keytype": "AES",
"commonkeyfilepath": "/etc/opt/nec/swclm/keyfile/cmkey",
"ext_data": {"osname": "CentOS", "osversion": "6.8", "memsize": "2048MB", "flag": "1"}
}

レスポンスコード

レスポンスコード	説明
201 Created	発行成功
400 Bad Request	リクエスト情報不正
403 Forbidden	認証エラー
404 Not Found	発行エラー
500 Internal Server Error	内部エラー

レスポンスパラメータ

パラメータ	説明
errorcode	エラーコード。 詳細は、「付録 エラーコード一覧」を参照してください。
deviceid	デバイス ID。

	リクエストパラメータ deviceid 未指定時は、CLM が採番した値。 リクエストパラメータ deviceid 指定時は、リクエストパラメータ deviceid と同じ値。
devicekey	デバイスキー。 リクエストパラメータ deviceid 未指定時の場合は、CLM が採番した値。 上記以外である場合は、レスポンスパラメータ省略。
commonkey	共通鍵。Base64 エンコードした文字列。
keynumber	共通鍵の鍵番号。
alias	共通鍵の Alias 名。
expiration	有効期限。 1970/1/1 00:00:00 (UTC) からの経過時間(単位: ミリ秒)で表します。

レスポンスパラメータの例を以下に示します。

表 5-2 共通鍵発行 API レスポンスパラメータ

<pre>{ "errorcode": 0, "alias": "iotgatewaytest cmkey", "expiration": "4655086987524", "deviceid": "1234567890abcdefghijklmnopqrstuvwxyz", "keynumber": "66", "commonkey": "3Q1EmpN9ItHBCKkWkaRASA¥u003d¥u003d" }</pre>

5.2 共通鍵取得 API

共通鍵取得 API は、発行済みの共通鍵を取得します。

取得した共通鍵は、CLM でリクエスト送信元デバイスとの紐づけを行い、管理します。

本 API で取得可能な共通鍵については、5.1 章をご覧ください。

リクエスト URL	メソッド
https://<サーバ名>/SWCLM/v10/KeyInfo	POST

リクエストパラメータ

パラメータ	必須/任意	説明
mode	必須	実行モード。「get」を指定してください。
keyid	必須	ID・パスワード発行 API で発行した ID。
key	必須	ID・パスワード発行 API で発行した ID のパスワード。
deviceid	必須	デバイス ID。
devicename	必須	デバイス名。
keynumber	必須	取得対象共通鍵の鍵番号。
filepath	必須	共通鍵保存ファイルパス。 最大文字列長は、1024byte です。 リクエスト送信元デバイス上のファイルパスを指定してください。

リクエストパラメータの例を以下に示します。

表 5-3 共通鍵取得 API リクエストパラメータ(例)

```
{
  "mode": "get",
  "keyid": "0000000001",
  "key": "cGFzc3dv",
  "deviceid": "0000000001",
  "devicename": "nec-edge-0001",
  "keynumber": "66",
  "filepath": "/etc/opt/nec/swclm/keyfile/cmkey"
}
```

レスポンスコード

レスポンスコード	説明
200 OK	取得成功
400 Bad Request	リクエスト情報不正
403 Forbidden	認証エラー
404 Not Found	取得エラー
500 Internal Server Error	内部エラー

レスポンスパラメータ

パラメータ	説明
errorcode	エラーコード。 詳細は、「付録. エラーコード一覧」を参照してください。
deviceid	リクエストで指定したデバイス ID。
commonkey	共通鍵。Base64 エンコードした文字列。
keynumber	共通鍵の鍵番号。
alias	共通鍵の Alias 名。
expiration	有効期限。 1970/1/1 00:00:00 (UTC) からの経過時間(単位: ミリ秒)で表します。

レスポンスパラメータの例を以下に示します。

表 5-4 共通鍵取得 API レスポンスパラメータ(例)

```
{  
  "errorcode": 0,  
  "alias": "iotgatewaytest cmkey",  
  "expiration": "4655086987524",  
  "deviceid": "1234567890abcdefghijklmnopqrstuvwxyz",  
  "keynumber": "66",  
  "commonkey": "3Q1EmpN9ItHBCKkWkaRASA¥u003d¥u003d"  
}
```

5.3 共通鍵更新 API

共通鍵更新 API は、発行済みの共通鍵を更新し、新しい共通鍵を発行・取得します。

取得の際、新しい共通鍵を発行せず、既存の共通鍵を更新後の共通鍵として取得することが可能です。

また、共通鍵の鍵長を変更することも可能です(例: 128bit で発行した共通鍵を 256bit で更新)。

更新した共通鍵は、CLM でリクエスト送信元デバイスとの紐づけを行い、管理します。

リクエスト URL

メソッド

https://<サーバ名>/SWCLM/v10/KeyInfo

POST

リクエストパラメータ

パラメータ	必須/任意	説明
mode	必須	実行モード。「update」を指定してください。
keyid	必須	ID・パスワード発行 API で発行した ID。
key	必須	ID・パスワード発行 API で発行した ID のパスワード。
deviceid	必須	デバイス ID。
devicename	必須	デバイス名。
keynumber	必須	更新対象共通鍵の鍵番号。
newkeynumber	任意	更新後の共通鍵の鍵番号。
alias	任意	共通鍵に付与する Alias。最大文字列長は、64byte です。
keylength	任意	更新後の共通鍵の長さ(単位: bit)。 省略時の既定値は 128(bit)です。
filepath	必須	更新対象共通鍵保存ファイルパス。 最大文字列長は、1024byte です。 リクエスト送信元デバイス上のファイルパスを指定してください。 <ul style="list-style-type: none">・共通鍵発行 API で発行した共通鍵を更新する場合は、 共通鍵発行 API のリクエストパラメータ commonkeyfilepath で指定したファイルパスを指定してください。・共通鍵取得 API で取得した共通鍵を更新する場合は、 共通鍵取得 API のリクエストパラメータ filepath で指定したファイルパスを指定してください。・共通鍵更新 API で更新した共通鍵を更新する場合は、 共通鍵更新 API のリクエストパラメータ newfilepath

		で指定したファイルパス (newfilepath 省略時は filepath で指定したファイルパス)を指定してください。
newfilepath	必須 ※filepath と値が同じ である場合は任意です。	更新後の共通鍵保存ファイルパス。 最大文字列長は、1024byte です。 リクエスト送信元デバイス上のファイルパスを指定してください。

リクエストパラメータの例を以下に示します。

表 5-5 共通鍵更新 API リクエストパラメータ(例 共通鍵(AES 鍵長 128bit)を更新)

<pre>{ "mode": "update", "keyid": "0000000001", "key": "cGFzc3dv", "deviceid": "0000000001", "devicename": "nec-edge-0001", "keynumber": "66", "filepath": "/etc/opt/nec/swclm/keyfile/cmkey", "keylength": "128", "newfilepath": "/etc/opt/nec/swclm/keyfile/cmkey_upd" }</pre>
--

レスポンスコード

レスポンスコード	説明
200 OK	更新成功
400 Bad Request	リクエスト情報不正
403 Forbidden	認証エラー
404 Not Found	更新エラー
500 Internal Server Error	内部エラー

レスポンスパラメータ

パラメータ	説明
errorcode	エラーコード。 詳細は、「付録. エラーコード一覧」を参照してください。

deviceid	デバイス ID。
commonkey	共通鍵。Base64 エンコードした文字列。
keynumber	共通鍵の鍵番号。
alias	共通鍵の Alias 名。
expiration	有効期限。 1970/1/1 00:00:00 (UTC) からの経過時間(単位: ミリ秒)で表します。

レスポンスパラメータの例を以下に示します。

表 5-6 共通鍵更新 API レスポンスパラメータ(例 共通鍵(AES 鍵長 128bit)を更新)

```
{
  "errorcode": 0,
  "alias": "iotgatewaytest cmkey",
  "expiration": "4655086987524",
  "deviceid": "1234567890abcdefghijklmnopqrstuvwxyz",
  "keynumber": "66",
  "commonkey": "3Q1EmPn9ItHBCkWkaRASA¥u003d¥u003d"
}
```

5.4 共通鍵削除 API

共通鍵削除 API は、共通鍵発行 API、共通鍵更新 API で発行・更新した共通鍵を削除します

リクエスト URL

`https://<サーバ名>/SWCLM/v10/KeyInfo`

メソッド

POST

リクエストパラメータ

パラメータ	必須/任意	説明
mode	必須	実行モード。「delete」を指定してください。
keyid	必須	ID・パスワード発行 API で発行した ID。
key	必須	ID・パスワード発行 API で発行した ID のパスワード。
deviceid	必須	デバイス ID。
devicename	必須	デバイス名。
keynumber	必須	削除対象共通鍵の鍵番号。
commonkey	必須	削除対象共通鍵。 Base64 エンコードした文字列を指定してください。
filepath	必須	削除対象共通鍵の保存ファイルパス。最大文字列長は、1024byte です。 リクエスト送信元デバイス上のファイルパスを指定してください。 ・共通鍵発行 API で発行した共通鍵を削除する場合は、共通鍵発行 API のリクエストパラメータ commonkeyfilepath で指定したファイルパスを指定してください。 ・共通鍵取得 API で取得した共通鍵を削除する場合は、共通鍵取得 API のリクエストパラメータ filepath で指定したファイルパスを指定してください。 ・共通鍵更新 API で更新した共通鍵を削除する場合は、共通鍵更新 API のリクエストパラメータ newfilepath で指定したファイルパス (newfilepath 省略時は filepath で指定したファイルパス)を指定してください。

リクエストパラメータの例を以下に示します。

表 5-7 共通鍵削除 API リクエストパラメータ(例)

```
{  
  "mode": "delete",  
  "keyid": "0000000001",  
  "key": "cGFzc3dv",  
  "deviceid": "0000000001",  
  "devicename": "nec-edge-0001",  
  "keynumber": "66",  
  "filepath": "/etc/opt/nec/swclm/keyfile/cmkey"  
  "commonkey": "3Q1EmpN9ItHBCKkWkaRASA¥u003d¥u003d"  
}
```

レスポンスコード

レスポンスコード	説明
200 OK	削除成功
400 Bad Request	リクエスト情報不正
403 Forbidden	認証エラー
404 Not Found	削除失敗
500 Internal Server Error	内部エラー

レスポンスパラメータ

パラメータ	説明
errorcode	エラーコード。 詳細は、「付録. エラーコード一覧」を参照してください。
deviceid	リクエストで指定したデバイス ID。
keynumber	削除した共通鍵の鍵番号。

レスポンスパラメータの例を以下に示します。

表 5-8 共通鍵削除 API レスポンスパラメータ(例)

```
{  
  "errorcode": 0,  
  "deviceid": "0000000001",  
  "keynumber": "66"  
}
```

6 CLM 管理 API

6.1 WebAPI サーバ稼動状態確認 API

CLM(WebAPI サーバ)が正常稼動しているかどうか、状態を取得します。

リクエスト URL

メソッド

`https://<サーバ名>/SWCLM/v10/SystemStatus`

GET

レスポンスコード

レスポンスコード	説明
200 OK	正常稼働
500 Internal Server Error	内部エラー

レスポンスパラメータ

パラメータ	説明
errorcode	エラーコード。 詳細は、「付録. エラーコード一覧」を参照してください。

レスポンスパラメータの例を以下に示します。

表 6-1 WebAPI サーバ稼動状態確認 API レスポンスパラメータ(例 DB 接続エラーの場合)

```
{  
  "errorcode": 1601  
}
```

7 付録

7.1 エラーコード一覧

レスポンスパラメータ `errorcode` の値は、下表の通りです。

エラーコード	エラーコード返却時 HTTPステータス	説明
1001	500	CLM の設定不正。
1002	500	設定ファイルの読み込みに失敗。
1101	400	JSON 構文エラー。
1102	400	必須パラメータが指定されていない。
1103	400	パラメータの指定方法誤り。
1104	400	パラメータの諸元誤り。
1201	403	パスワードが不一致。
1202	403	パスワードのステータスが有効ではない。
1203	403	パスワードが有効期限切れ。
1204	404	データベース上に ID・パスワード(事前共有キー)情報が見つからない。
1205	500	keyID 番号が keyID 長の最大値をオーバー。
1301	404	証明書情報が取得できない(keynumber または certserial の値が不正)。
1302	404	CA 局名称が不正でテーブル情報が取得できない(パラメータ catype の値が不正)。
1303	404	紐付け情報が取得できない(証明書とデバイス情報の組み合わせが不正)。
1304	403	keynumber または certserial の証明書のステータスが有効ではない。
1305	403	keynumber または certserial の証明書が有効期限切れ。
1306	403	keynumber または certserial の証明書がすでに失効または更新済み。
1307	403	newkeynumber または newcertserial の証明書のステータスが有効ではない。
1308	403	newkeynumber または newcertserial の証明書が有効期限切れ。
1309	404	証明書ファイルが見つからない。

1401	500	openssl コマンド実行エラー。
1402	500	openssl コマンド実行結果の形式異常。
1403	500	ロックタイムアウト。
1501	404	共通鍵情報が取得できない(keynumber の値が不正)。
1502	404	共通鍵情報が取得できない(newkeynumber の値が不正)。
1503	404	紐付け情報が取得できない (keynumber と deviceid の組み合わせが不正)。
1504	403	keynumber の共通鍵がすでに失効または更新済み。
1505	403	newkeynumber の共通鍵の status が有効ではない。
1506	403	newkeynumber の共通鍵が有効期限切れ。
1507	400	keynumber の暗号化方式と newkeynumber の暗号化方式が異なる。
1508	400	リクエスト中の共通鍵値と DB の共通鍵値が一致しない
1601	500	データベース接続エラー。
1602	500	データベースアクセスエラー。
1603	500	カラム情報不正。
1604	500	データベースのデータ異常。
1701	400	deviceid が、登録済みの情報と一致しない。
1702	400	デバイス名が既に登録済み。
1703	403	デバイスキーが一致しない。
1704	403	デバイスのステータスが有効でない。
1705	403	デバイスが有効期限切れ。
1706	404	デバイス情報が見つからない。
1707	500	スクリプト実行エラー。
1901	500	ログ初期化失敗。
2001	500	初期化処理で異常発生。
2002	500	暗号化処理で異常発生。
2003	500	復号化処理で異常発生。
2004	500	SecureWare/開発キットの API 呼び出しで異常発生。
9901	500	システムエラー。