Orchestrating a brighter world

NEC

SecureWare/Credential Lifecycle Manager

WebAPI リファレンス

2022 年 6 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

2022 年 6 月　第五版

目次

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・パスワード認証
ID/PWD 入手	ID･パスワード発行	POST	/SWCLM/IDInfo	ID・パスワードを生成する。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/IDInfo?keyid=<ID>	ID・パスワード発行で生成した ID・パスワードを取得する。	○	
ID/PWD 照合(認証)	ID･パスワード照合	POST	/SWCLM/IDInfo	ID・パスワードを照合(認証)する。	○	○
ID/PWD 削除	ID･パスワード削除	POST	/SWCLM/IDInfo	ID・パスワード発行で生成した ID・パスワードを削除する。	○	○
証明書発行・取得	証明書発行	POST	/SWCLM/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/CredInfo	CA 証明書、公開鍵証明書を取得する。	○	○
証明書更新・失効	証明書更新	POST	/SWCLM/CredInfo	公開鍵証明書を更新する。	○	○
	証明書失効	POST	/SWCLM/CredInfo	公開鍵証明書を失効する。	○	○
共通鍵発行・取得	共通鍵発行	POST	/SWCLM/KeyInfo	共通鍵を発行する。	○	○
	共通鍵取得	POST	/SWCLM/KeyInfo	共通鍵を取得する。	○	○
共通鍵更新・削除	共通鍵更新	POST	/SWCLM/KeyInfo	共通鍵を更新する。	○	○
	共通鍵削除	POST	/SWCLM/KeyInfo	共通鍵を削除する。	○	○
共通鍵照合(認証)	共通鍵照合	POST	/SWCLM/KeyInfo	共通鍵を照合(認証)する。	○	○
一括処理	共通鍵一括取得	POST	/SWCLM/KeyInfo	共通鍵を一括取得する。	○	○

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・パスワード認証

CLM の WebAPI は、一部の WebAPI を除き、WebAPI 実行時に ID・パスワード認証を行います。

認証に使用する ID・パスワードは、ID・パスワード発行 API で発行します。

また、ID・パスワード認証が必要な 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
https://<サーバ名>/SWCLM/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」を指定します。
tenanted	必須	テナント ID を指定します。「TenantA」固定です。
alias	必須	ID・パスワードに付与する Alias を指定します。 最大文字列長は 64byte です。

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、「7.1 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・パスワードを取得します。

リクエスト URL　　メソッド

https://<サーバ名>/SWCLM/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 を指定します。

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、「7.1 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・パスワード情報。 取得可能な ID・パスワードが存在しない、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・パスワードと、CLM に登録されている ID・パスワードが一致するかを照合(認証)します。

リクエスト URL	メソッド
https://<サーバ名>/SWCLM/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。「auth」を指定します。
keyid	必須	ID・パスワード発行 API で発行した ID を指定します。
key	必須	ID・パスワード発行 API で発行した ID のパスワードを指定します。

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": "0000000001",
    "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、「7.1 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・パスワードを削除します。

リクエスト URL	メソッド
https://<サーバ名>/SWCLM/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。「delete」を指定します。
keyid	必須	削除対象 ID を指定します。 ID・パスワード発行 API で発行した ID を指定します。
key	必須	削除対象 ID のパスワードを指定します。 ID・パスワード発行 API で発行した ID のパスワードを指定します。

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": "0000000001",
    "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、「7.1 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 でどの機器(デバイス・エッジ・サーバなど)に発行するかの紐づけを行い、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 秘密鍵	CA 証明書
CA 証明書		pem、der			○ ※1
公開鍵証明書					
	サーバ証明書	pem、der	○	○ ※2	○ ※3
	クライアント証明書	pem、der	○	○ ※2	○ ※3
		PKCS#12(chain なし)	○	○ ※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: 秘密鍵の形式は、pem です。der 形式の証明書を発行した場合も、秘密鍵は 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: 秘密鍵は、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/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」を指定します。
keyid	必須	ID・パスワード発行 API で発行した ID を指定します。
key	必須	ID・パスワード発行 API で発行した ID のパスワードを指定します。
deviceid	任意	デバイス ID を指定します。 どの機器(デバイス・エッジ・サーバなど)に発行するかを CLM が管理・判別するために指定します。 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「deviceid」値を本パラメータに指定してください。
devicename	必須	デバイス名を指定します。 どの機器(デバイス・エッジ・サーバなど)に発行するかを CLM が管理・判別するために指定します。 キッティング済みエッジ GW では、既に devicename は CLM にエッジ ID で登録されていますので、エッジ ID を指定します。 最大文字列長は、64byte です。
certmode	必須	取得する証明書の種別を指定します。 以下のいずれかを指定してください。 caonly： CA 証明書を取得 client ： サーバ証明書、クライアント証明書を取得
catype	必須	証明書を発行する認証局の名称を指定します。 以下のいずれかを指定してください。 CA: リクエストパラメータ certmode が「caonly」である場合 ca1: リクエストパラメータ certmode が「client」である場合
cacerttype	任意	CA 証明書の種別を指定します。 以下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
clientcerttype	任意	サーバ証明書、クライアント証明書の種別を指定します。 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)

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を指定します。 「/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を指定します。 最大文字列長は、128byte です。 使用可能文字種は、ASCII 0x21～0x7E です。
keyfilepath	必須	パスワード保存ファイルパスを指定します。 CLM の管理情報として使用します。 「/tmp/key」を指定します。
cafilepath	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を指定します。 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を指定します。 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 アドレスを指定します。
macaddress	任意	デバイスの MAC アドレスを指定します。 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

<table>
<tr>
<td>ext_data</td>
<td>任意</td>
<td>拡張情報を指定します。
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。
既定で指定可能な拡張情報は、次の通りです。
また、以下以外に、任意の拡張情報も指定可能です。
<table><tr><th>項目名</th><th>説明</th></tr><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>memorysize</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></table></td>
</tr>
</table>

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",
    "cafilepath": "/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", "memorysize":"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、「7.1 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": "1234567890abcdefghijklmnopqrstuvwxyxz",
    "cacert":"-----BEGINCERTIFICATE-----¥nMIIDtDCCApygAwIBAgIJAL2XwoalwjiIMA0GCSqGSIb
3DQEBCwUAMFUxCzAJBgNV¥n＜省略＞¥n-----END CERTIFICATE-----",
    "cacerttype": "pem",
    "cakeynumber": "3",
    "caserial": "863542E528A722EE",
    "clientcert":"-----BEGINCERTIFICATE-----¥nMIIDgDCCAmigAwIBAgIJAL2XwoalwjiDMA0GCSq
GSIb3DQEBCwUAMFUxCzAJBgNV¥n＜省略＞¥n-----END CERTIFICATE-----",
    "clientcerttype": "pem"
    "clientkeynumber": "2",
    "clientserial": "863542E528A7233F",
    "privatekey":"-----BEGINPRIVATE KEY-----¥nMIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwgg
SjAgEAAoIBAQC4kT9F6a0EOAG0¥n＜省略＞¥n-----END PRIVATE KEY-----¥n"
}
```

4.2 証明書取得 API

証明書取得 API は、証明書発行 API、証明書更新 API で発行・更新した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 でどの機器(デバイス・エッジ・サーバなど)から取得されたかの紐づけを行い、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 秘密鍵	CA 証明書
CA 証明書		pem、der			○ ※1
公開鍵証明書					
	サーバ証明書	pem、der	○	○ ※2	
	クライアント証明書	pem、der	○	○ ※2	
		PKCS#12(chain なし)	○	○ ※3	

※1: CLM が連携する CA の CA 証明書を取得します。

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

※3: 秘密鍵は、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/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」を指定します。
keyid	必須	ID･パスワード発行 API で発行した ID を指定します。
key	必須	ID・パスワード発行 API で発行した ID のパスワードを指定します。
deviceid	必須	デバイス ID を指定します。
devicename	必須	デバイス名を指定します。 どの機器(デバイス・エッジ・サーバなど)から取得されるかを CLM が判別するために指定します。 キッティング済みエッジ GW では、既に devicename は CLM にエッジ ID で登録されていますので、エッジ

		ID を指定します。 最大文字列長は、64byte です。
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を指定します。
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を指定します。
catype	必須	取得対象証明書を発行した認証局の名称を指定します。 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を指定します。 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を指定します。 最大文字列長は、128byte です。 使用可能文字種は、ASCII 0x21～0x7E です。
filepath	必須	取得対象証明書保存ファイルパスを指定します。 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、「7.1 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-----¥nMIIDgDCCAmigAwIBAgIJAL2XwoalwjiDMA0GCSqGSIb3DQEBCwUAMFUxCzAJBgNV＜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-----¥nMIIDgDCCAmigAwIBAgIJAL2XwoalwjiDMA0GCSqGSIb3DQEBCwUAMFUxCzAJBgNV＜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可能です。

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 でどの機器(デバイス・エッジ・サーバなど)から更新されたかの紐づけを行い、管理します。

リクエスト URL	メソッド
https://<サーバ名>/SWCLM/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」を指定します。
keyid	必須	ID・パスワード発行 API で発行した ID を指定します。
key	必須	ID・パスワード発行 API で発行した ID のパスワードを指定します。
deviceid	必須	デバイス ID を指定します。
devicename	必須	デバイス名を指定します。 どの機器(デバイス・エッジ・サーバなど)から更新されるかを CLM が判別するために指定します。 キッティング済みエッジ GW では、既に devicename は CLM にエッジ ID で登録されていますので、エッジ ID を指定します。 最大文字列長は、64byte です。
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を指定します。
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を指定します。

newkeynumber	任意	更新後の証明書の鍵番号を指定します。 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を指定します。 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を指定します。 「ca1」を指定します。
certtype	任意	更新後の証明書の種別を指定します。 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を指定します。 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。 最大文字列長は、128byte です。 使用可能文字種は、ASCII 0x21～0x7E です。 [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を指定します。 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を指定します。 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、「7.1 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-----¥nMIIDNjCCAh6gAwIBAgIJAN6 6ttSoJXygMA0GCS
qGSIb3DQEBCwUAMBwxwUAMB＜省略＞¥n-----END CERTIFICATE-----¥n",
    "clientcerttype": "pem",
    "clientkeynumber": "55",
    "clientserial":"DEBAB6D4A8257CA0",
    "privatekey":"-----BEGIN PRIVATE KEY-----¥nMIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcw
ggSjAgEAAoIBAQDPnN0iBxqrAA＜省略＞¥n-----END PRIVATE KEY-----¥n"
}
```

4.4 証明書失効 API

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

リクエスト URL	メソッド
https://<サーバ名>/SWCLM/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。「revoke」を指定します。
keyid	必須	ID・パスワード発行 API で発行した ID を指定します。
key	必須	ID・パスワード発行 API で発行した ID のパスワードを指定します。
deviceid	必須	デバイス ID を指定します。
devicename	必須	デバイス名を指定します。 どの機器(デバイス・エッジ・サーバなど)から失効されるかを CLM が判別するために指定します。 キッティング済みエッジ GW では、既に devicename は CLM にエッジ ID で登録されていますので、エッジ ID を指定します。 最大文字列長は、64byte です。
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を指定します。
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を指定します。
catype	必須	失効対象証明書を発行した認証局の名称を指定します。 「ca1」を指定します。
filepath	任意	失効対象証明書の保存ファイルパスを指定します。 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": "0000000001",
    "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、「7.1 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 でどの機器(デバイス・エッジ・サーバなど)に発行するかの紐づけを行い、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	メソッド
https://<サーバ名>/SWCLM/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。「create」を指定します。
keyid	必須	ID・パスワード発行 API で発行した ID を指定します。
key	必須	ID・パスワード発行 API で発行した ID のパスワードを指定します。
deviceid	任意	デバイス ID を指定します。 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「deviceid」値を本パラメータに指定してください。
devicename	必須	デバイス名を指定します。 どの機器(デバイス・エッジ・サーバなど)に発行するかを CLM が管理・判別するために指定します。 キッティング済みエッジ GW では、既に devicename は CLM にエッジ ID で登録されていますので、エッジ

<table>
<tr><td></td><td></td><td>ID を指定します。
最大文字列長は、64byte です。</td></tr>
<tr><td>alias</td><td>必須</td><td>共通鍵に付与する Alias を指定します。
最大文字列長は、64byte です。</td></tr>
<tr><td>keylength</td><td>任意</td><td>発行する共通鍵の長さ(単位: bit)を指定します。
省略時の既定値は 128(bit)です。
keytype に「AES」を指定する場合、「128」または「256」のみ指定可能です。
keytype に「TWINE」を指定する場合、「80」または「128」のみ指定可能です。</td></tr>
<tr><td>keytype</td><td>必須</td><td>鍵を利用する暗号化方式を指定します。
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</td></tr>
<tr><td>keyfilepath</td><td>必須</td><td>パスワード保存ファイルパスを指定します。
CLM の管理情報として使用します。
「/tmp/key」を指定します。</td></tr>
<tr><td>commonkeyfilepath</td><td>必須</td><td>共通鍵保存ファイルパスを指定します。
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。</td></tr>
<tr><td>ipaddress</td><td>任意</td><td>デバイスの IP アドレスを指定します。</td></tr>
<tr><td>macaddress</td><td>任意</td><td>デバイスの MAC アドレスを指定します。
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</td></tr>
<tr><td>ext_data</td><td>任意</td><td>拡張情報を指定します。
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。
既定で指定可能な拡張情報は、次の通りです。
また、以下以外に、任意の拡張情報も指定可能です。
<table><tr><th>項目名</th><th>説明</th></tr><tr><td>osname</td><td>OS 名</td></tr><tr><td>osversion</td><td>OS バージョン</td></tr></table></td></tr>
</table>

		architecture	アーキテクチャ	
		cpuname	CPU 名	
		memorysize	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(例)

```
{
    "mode": "create",
    "keyid": "0000000001",
    "key": "cGFzc3dv",
    "devicename": "nec-edge-0001",
    "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", "memorysize":"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、「7.1 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に示します。

表 5-2 共通鍵発行 API レスポンスパラメータ(例)

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

5.2 共通鍵取得 API

共通鍵取得 API は、共通鍵発行 API、共通鍵更新 API で発行・更新した共通鍵を取得します。

取得した共通鍵は、CLM でどの機器(デバイス・エッジ・サーバなど)から取得されたかの紐づけを行い、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。

なお、取得する共通鍵は、次の方法で指定することが可能です。

- 共通鍵の鍵番号を指定して取得
  指定した鍵番号に該当する共通鍵を取得します。
- 共通鍵発行・更新時に共通鍵に付与した Alias を指定して取得
  指定した Alias が付与された共通鍵を取得します。
  指定 Alias が付与された共通鍵が CLM 上に複数存在する場合、指定 Alias が付与された共通鍵のうち鍵番号が最大である共通鍵を取得します。

リクエスト URL	メソッド
https://<サーバ名>/SWCLM/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」を指定します。
keyid	必須	ID・パスワード発行 API で発行した ID を指定します。
key	必須	ID・パスワード発行 API で発行した ID のパスワードを指定します。
deviceid	必須	デバイス ID を指定します。
devicename	必須	デバイス名を指定します。 どの機器(デバイス・エッジ・サーバなど)から取得されるかを CLM が判別するために指定します。 キッティング済みエッジ GW では、既に devicename は CLM にエッジ ID で登録されていますので、エッジ ID を指定します。 最大文字列長は、64byte です。
keynumber	任意 ※alias を指定しない	取得対象共通鍵の鍵番号を指定します。 リクエストパラメータ alias と同時に指定した場合は、

	場合は必須です。	本パラメータを優先し、リクエストパラメータ alias は無視します。
filepath	必須	共通鍵保存ファイルパスを指定します。 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。
alias	任意 ※keynumber を指定しない場合は必須です。	取得対象共通鍵に付与されている Alias を指定します。 最大文字列長は、64byte です。 リクエストパラメータkeynumberと同時に指定した場合は、リクエストパラメータ keynumber を優先し、本パラメータは無視します。
expiredkey	任意	有効期限が切れた共通鍵を取得するかどうかを指定します。 以下のいずれかを指定してください。省略時は、有効期限切れの鍵を取得しません。 true ： 有効期限切れの共通鍵を取得する false ： 有効期限切れの共通鍵は取得しない

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 共通鍵を鍵番号指定で取得)

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

表 5-4 共通鍵取得 API リクエストパラメータ(例 共通鍵を Alias 指定で取得)

```
{
    "mode": "get",
    "keyid": "0000000001",
    "key": "cGFzc3dv",
    "deviceid": "0000000001",
    "devicename": "nec-edge-0001",
    "alias": "iotgatewaytest cmkey",
    "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、「7.1 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 5-5 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": "1234567890abcdefghijklmnopqrstuvwxyxz",
    "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、新しい共通鍵を取得します。

更新した共通鍵は、CLM でどの機器(デバイス・エッジ・サーバなど)から更新されたかの紐づけを行い、管理します。

本 API で更新可能な共通鍵については、5.1 章をご覧ください。

更新対象の共通鍵は、次の方法で指定することが可能です。

- 共通鍵の鍵番号を指定して更新

  指定した鍵番号に該当する共通鍵を更新します。
- 共通鍵発行・更新時に共通鍵に付与した Alias を指定して更新

  指定した Alias が付与された共通鍵を更新します。

  指定 Alias が付与された共通鍵が CLM 上に複数存在する場合､次の条件に当てはまる共通鍵のうち、鍵番号が最大である共通鍵を更新します。

  ・共通鍵は、指定 Alias が付与されている

  ・共通鍵は、リクエストパラメータ devicename に指定したデバイス名に紐づいている

また、更新後の共通鍵は、以下のいずれかから選択可能です。

- 共通鍵を新規発行し、更新後の共通鍵とする

  共通鍵更新 API 実行時に、新規に共通鍵を発行します。発行した鍵を更新後の共通鍵として取得します。

  共通鍵の鍵長は、変更することが可能です(例: 128bit で発行した共通鍵を 256bit で更新)。
- 既存の共通鍵を更新後の共通鍵とする

  CLM 上に既に存在する共通鍵を、更新後の共通鍵として扱い、取得します。

  更新後の共通鍵として、更新対象共通鍵と異なる鍵長の共通鍵を指定することが可能です(例: 128bit で発行した共通鍵を既存の 256bit の共通鍵で更新)。

リクエスト URL　　メソッド

https://<サーバ名>/SWCLM/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」を指定します。
keyid	必須	ID・パスワード発行 API で発行した ID を指定します。

key	必須	ID・パスワード発行 API で発行した ID のパスワードを指定します。
deviceid	必須	デバイス ID を指定します。
devicename	必須	デバイス名を指定します。 どの機器(デバイス・エッジ・サーバなど)から更新されるかを CLM が判別するために指定します。 キッティング済みエッジ GW では、既に devicename は CLM にエッジ ID で登録されていますので、エッジ ID を指定します。 最大文字列長は、64byte です。
keynumber	任意 ※oldalias を指定しない場合は必須です。	更新対象共通鍵の鍵番号を指定します。
oldalias	任意 ※keynumber を指定しない場合は必須です。	更新対象共通鍵の Alias を指定します。 最大文字列長は、64byte です。
newkeynumber	任意	更新後の共通鍵の鍵番号を指定します。 既存の共通鍵を更新後共通鍵としたい場合に指定してください。
newalias	任意	更新後の共通鍵の Alias を指定します。 最大文字列長は、64byte です。 本パラメータで指定した Alias が付与された既存の共通鍵を更新後共通鍵としたい場合に指定してください。
alias	任意	更新後の共通鍵に付与する Alias を指定します。 最大文字列長は、64byte です。 更新後の共通鍵に、更新対象共通鍵と異なる Alias を付与したい場合に指定してください。
keylength	任意	更新後の共通鍵の長さ(単位: bit) を指定します。 省略時の既定値は 128(bit)です。 更新対象共通鍵の keytype が「AES」である場合、「128」または「256」を指定します。 更新対象共通鍵の keytype が「TWINE」である場合、「80」または「128」を指定します。
filepath	必須	更新対象共通鍵保存ファイルパスを指定します。 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を指定します。 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 5-6 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)

```
{
    "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"
}
```

表 5-7 共通鍵更新 API リクエストパラメータ(例 共通鍵を Alias 指定で更新)

```
{
    "mode": "update",
    "keyid": "0000000001",
    "key": "cGFzc3dv",
    "deviceid": "0000000001",
```

```
    "devicename": "nec-edge-0001",
    "oldalias": "iotgatewaytest cmkey",
    "filepath": "/etc/opt/nec/swclm/keyfile/cmkey",
    "keylength": "128",
    "newfilepath": "/etc/opt/nec/swclm/keyfile/cmkey_upd"
}
```

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、「7.1 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 5-8 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": "1234567890abcdefghijklmnopqrstuvwxyxz",
    "keynumber": "66",
    "commonkey":"3Q1EmpN9ItHBCKkWkaRASA¥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	メソッド
https://<サーバ名>/SWCLM/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。「delete」を指定します。
keyid	必須	ID・パスワード発行 API で発行した ID を指定します。
key	必須	ID・パスワード発行 API で発行した ID のパスワードを指定します。
deviceid	必須	デバイス ID を指定します。
devicename	必須	デバイス名を指定します。 どの機器(デバイス・エッジ・サーバなど)から削除されるかを CLM が判別するために指定します。 キッティング済みエッジ GW では、既に devicename は CLM にエッジ ID で登録されていますので、エッジ ID を指定します。 最大文字列長は、64byte です。
keynumber	必須	削除対象共通鍵の鍵番号を指定します。
commonkey	必須	削除対象共通鍵を指定します。 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 5-9 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、「7.1 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 5-10 共通鍵削除 API レスポンスパラメータ(例)

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

5.5 共通鍵照合 API

共通鍵照合 API は、リクエスト送信元デバイスが所有している共通鍵と、CLM に登録されている共通鍵が一致するかを照合(認証)します。

本 API で照合可能な共通鍵と照合可能な形式は、次の通りです。

表 5-11 共通鍵照合 API 照合可能な共通鍵・形式一覧

共通鍵(暗号化方式)		CLM 管理共通鍵との照合	軽量暗号 TWINE を用いた照合
AES		○	
TWINE			
	80 bit	○	
	128 bit	○	○

リクエスト URL　　メソッド

https://<サーバ名>/SWCLM/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。「auth」を指定します。
keyid	必須	ID・パスワード発行 API で発行した ID を指定します。
key	必須	ID・パスワード発行 API で発行した ID のパスワードを指定します。
deviceid	必須	デバイス ID を指定します。
devicename	必須	デバイス名を指定します。 どの機器(デバイス・エッジ・サーバなど)を認証するかを CLM が判別するために指定します。 キッティング済みエッジ GW では、既に devicename は CLM にエッジ ID で登録されていますので、エッジ ID を指定します。 最大文字列長は、64byte です。
keynumber	必須	照合する共通鍵の鍵番号を指定します。
commonkey	任意 ※encdata を指定しない場合は、必須です。	照合する共通鍵を指定します。 共通鍵は、Base64 エンコードした文字列で指定します。

encdata	任意 ※認証に使用する共通鍵が以下に該当する場合、指定可能です。 ・keytype: TWINE ・keylength: 128	暗号化した認証用データを指定します。 認証用データは、Base64 エンコードした文字列で指定します。 認証用データについては、後述「認証用データについて」をご覧ください。
filepath	必須	共通鍵保存ファイルパスを指定します。 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 5-12 共通鍵照合 API リクエストパラメータ(例)

```
{
    "mode": "auth",
    "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	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、「7.1 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	照合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 5-13 共通鍵照合 API レスポンスパラメータ(例)

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

認証用データについて

encdata パラメータに指定する認証用データとは、devicename に指定するデバイス名を軽量暗号 開発キット同梱の暗号コマンドと、照合する共通鍵を使用して暗号化した結果、得られるデータです。
以下の手順でデータを生成し、encdata に指定します。
軽量暗号 開発キット同梱の暗号コマンドの詳細については、軽量暗号 開発キットのマニュアルをご覧ください。

1. 暗号コマンドの共通鍵ファイル生成機能を使用して、共通鍵ファイルを生成します。
   コマンド実行時の引数「暗号鍵」には、共通鍵照合で照合する共通鍵を指定します。

> lightcipher -create_key_file <照合する共通鍵> <共通鍵ファイル名>

2. 暗号コマンドのファイル暗号機能を使用して、暗号文を生成します。
   コマンド実行時の引数「平文ファイル名」には、デバイス名を保存したファイルのパスを指定します。
   また、共通鍵ファイル名には、上述 1.で生成した共通鍵ファイル名を指定します。
   > lightcipher -enc -mode TWINE-OTR <平文ファイル名> <共通鍵ファイル名>
3. 上述 2.を実行した結果、暗号文がファイルに出力されます。
   暗号文を Base64 エンコードし、encdata パラメータに指定します。

5.6 共通鍵一括取得 API

共通鍵一括取得 API は、デバイスに紐づく共通鍵を一括取得します。

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。

共通鍵取得 API と異なり、どの機器(デバイス・エッジ・サーバなど)から一括取得取得されたかの紐づけは行いません。

なお、共通鍵一括取得中にエラーが発生した場合は、当該デバイスに関する処理をスキップし、次のデバイスの登録処理を行います。

なお、取得する共通鍵は、次の方法で指定することが可能です。

- 共通鍵の鍵番号を指定して取得

  指定した鍵番号に該当する共通鍵を取得します。

  なお、同一デバイス・同一鍵番号を複数指定した場合は、指定した分の鍵情報を取得します。

- 共通鍵発行・更新時に共通鍵に付与した Alias を指定して取得

  指定した Alias が付与された共通鍵を取得します。

  指定 Alias が付与された共通鍵が CLM 上に複数存在する場合、指定 Alias が付与された共通鍵のうち鍵番号が最大である共通鍵を取得します。

リクエスト URL	メソッド
https://<サーバ名>/SWCLM/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。「getlist」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。

<table>
<tr><td>deviceinfo</td><td>必須</td><td>共通鍵を保有しているデバイスの情報。
以下の項目を、配列で指定します。
<table><tr><th>パラメータ</th><th>必須/任意</th><th>説明</th></tr><tr><td>deviceid</td><td>必須</td><td>共通鍵を保有しているデバイスのデバイス ID を指定します。</td></tr><tr><td>devicename</td><td>必須</td><td>共通鍵を保有しているデバイスのデバイス名を指定します。
キッティング済みエッジ GW では、既に devicename は CLM にエッジ ID で登録されていますので、エッジ ID を指定します。
最大文字列長は、64byte です。</td></tr><tr><td>keynumber</td><td>必須</td><td>デバイスが保有している共通鍵の鍵番号を指定します。配列で指定します。</td></tr></table></td></tr>
</table>

リクエストパラメータの例を以下に示します。

表 5-14 共通鍵一括取得 API リクエストパラメータ(例)

```
{
    "mode": “getlist",
    "keyid": "0000000001",
    "key": "cGFzc3dv",
    “deviceinfo”: [{
        "deviceid": "0000000001",
        "devicename": "nec-edge-0001",
        "keynumber":["1", "3","4"]
    },{
         "deviceid": "0000000002",
        "devicename": "nec-edge-0002",
        "keynumber":["10"]
    }]
}
```

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、別紙「WebAPI リファレンス」の「付録. エラーコード一覧」を参照してください。 エラーが複数発生した場合は、最後に発生したエラーのエラーコードを格納します。
deviceinfo		取得した共通鍵の情報。以下の項目をデバイス単位で配列に格納します。
	errorcode	エラーコード。
	deviceid	共通鍵を保有しているデバイスのデバイス ID。
	devicename	共通鍵を保有しているデバイスのデバイス名。
	keyinfo	取得した共通鍵の鍵情報(配列)。 **パラメータ** / **説明** keynumber / 共通鍵の鍵番号。 commonkey / 共通鍵。Base64 エンコードした文字列。 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。 keyalias / 共通鍵の Alias 名。
	errorkeylist	取得できなかった鍵番号のリスト。

レスポンスパラメータの例を以下に示します。

表 5-15 共通鍵一括取得 API レスポンスパラメータ(例)

```
{
  "errorcode": 0,
  "deviceinfo":[
    {"errorcode": 0, "deviceid":"0000000001", "devicename":"nec-edge-0001",
     "keyinfo":[
       {"keynumber":1, "commonkey":"QhWPjdyC8vks¥/4LR1oSBfA==",
```

```
          "expiration":"1515971297610", "alias":"devicekey01"},
         {"keynumber":3, "commonkey":"oJ7MUePSQywQLlYu8¥/SaLg==",
          "expiration":"1505971397610", "alias":"devkey02"},
         {"keynumber":4, "commonkey":"MrQXm6+kDNA5ODLTO7i3nQ==",
          "expiration":"1505971397610", "alias":"devkey03"}]
       },
      {"errorcode": 0, "deviceid":"0000000002", "devicename":"nec-edge-0002",
       "keyinfo":[
         {"keynumber":10, "commonkey":"QhWPjdyC8vks¥/4LR1oSBfA==",
          "expiration":"1515971297610", "alias":"devkey10"}]
      }]
}
```

6 CLM 管理 API

6.1 WebAPI サーバ稼動状態確認 API

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

リクエスト URL	メソッド
https://<サーバ名>/SWCLM/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、「7.1 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 サーバ稼働状態確認 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。CLM の設定を確認してください。
1002	500	設定ファイルの読み込みに失敗。CLM の設定を確認してください。
1101	400	JSON 構文エラー。ネットワークの状態を確認してください。
1102	400	必須パラメータが指定されていない。WebAPI で指定したパラメータを確認してください。
1103	400	パラメータの指定方法誤り。WebAPI で指定したパラメータを確認してください。
1104	400	パラメータの諸元誤り。WebAPI で指定したパラメータを確認してください。
1201	403	パスワードが不一致。指定した ID・パスワードを確認し、再実行してください。
1202	403	パスワードのステータスが有効ではない。指定した ID・パスワードを確認し、再実行してください。
1203	403	パスワードが有効期限切れ。指定した ID・パスワードを確認し、再実行してください。
1204	404	データベース上に ID・パスワード情報が見つからない。指定した ID・パスワードを確認し、再実行してください。
1205	500	keyID 番号が keyID 長の最大値をオーバー。CLM の設定を確認してください。
1301	404	証明書情報が取得できない(keynumber または certserial の値が不正)。WebAPI で指定した keynumber または certserial を確認してください。
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)。WebAPI で指定した catype を確認してください。
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)。WebAPI で指定した keynumber や devicename を確認してください。
1304	403	keynumberまたはcertserialの証明書のステータスが有効ではない。WebAPI で指定した keynumber または certserial を確認してください。または、証明書の情報を確認してください。
1305	403	keynumber または certserial の証明書が有効期限切れ。WebAPI で指定した keynumber または certserial を確認してください。または、証明書の情報を確認してください。
1306	403	keynumberまたはcertserialの証明書がすでに失効または更新済み。WebAPI で指定した keynumber または certserial を確認してください。または、証明書の情報を確認してください。
1307	403	newkeynumberまたはnewcertserialの証明書のステータスが有効ではない。WebAPI で指定した newkeynumber または newcertserial を確認してください。または、証明書の情報を確認してください。
1308	403	newkeynumberまたはnewcertserialの証明書が有効期限切れ。WebAPI で指定した newkeynumber または newcertserial を確認してください。または、証明書の情報を確認してください。
1309	404	証明書ファイルが見つからない。CLM のログを確認してください。
1310	500	証明書ファイルのアクセスエラー。CLM のログを確認してください。
1401	500	OpenSSL のコマンド実行エラー。CLM のログを確認してください。
1402	500	OpenSSL のコマンド実行結果の形式異常。CLM のログを確認してください。
1403	500	OpenSSL のコマンドのロックタイムアウト。CLM のログを確認してください。
1501	404	共通鍵情報が取得できない(keynumber の値が不正)。WebAPI で指定した keynumber を確認してください。または共通鍵の情報を確認してください。
1502	404	共通鍵情報が取得できない(newkeynumber の値が不正)。

		WebAPI で指定した keynumber または newkeynumber を確認してください。または共通鍵を更新してください。
1503	404	紐付け情報が取得できない（keynumber、filepath、deviceid の組み合わせが不正）。WebAPI で指定した keynumberやfilepath、devicenameを確認してください。
1504	403	keynumber の共通鍵がすでに失効または更新済み。WebAPI で指定した keynumber を確認してください。または共通鍵の情報を確認してください。
1505	403	newkeynumber の共通鍵の status が有効ではない。WebAPI で指定したnewkeynumberを確認してください。または共通鍵の情報を確認してください。
1506	403	newkeynumberの共通鍵が有効期限切れ。WebAPI で指定した newkeynumber を確認してください。または共通鍵を更新してください。
1507	400	keynumberの暗号化方式とnewkeynumberの暗号化方式が異なる。WebAPI で指定した newkeynumber を確認してください。または共通鍵の情報を確認してください。
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。WebAPI で指定した filepath と keynumber を確認してください。または共通鍵の情報を確認してください。
1509	403	共通鍵のステータスが有効ではない。WebAPI で指定した filepath と keynumber を確認してください。または共通鍵の情報を確認してください。
1510	403	共通鍵が有効期限切れ。WebAPI で指定した filepath と keynumber を確認してください。または共通鍵を更新してください。
1511	500	共通鍵ファイルが見つからない。CLM のログを確認してください。
1512	500	共通鍵ファイルのアクセスエラー。CLM のログを確認してください。
1513	404	更新対象の鍵番号と更新後の鍵番号が一致。WebAPI で指定した keynumber と newkeynumber を確認してください。または共通鍵の情報を確認してください。
1601	500	データベース接続エラー。CLM のリポジトリの状態を確認してください。

1602	500	データベースアクセスエラー。CLM のリポジトリの状態を確認してください。
1603	500	カラム情報不正。CLM のログを確認してください。
1604	500	データベースのデータ異常。CLM のログを確認してください。
1701	400	deviceid が、登録済みの情報と一致しない。WebAPI で指定した devicename を確認してください。
1702	400	デバイス名が既に登録済み。WebAPI で指定した devicename を変更し、異なるデバイス名にしてください。
1703	403	デバイスキーが一致しない。WebAPI で指定した devicename を確認してください。
1704	403	デバイスのステータスが有効でない。WebAPI で指定した devicename を確認してください。
1705	403	デバイスが有効期限切れ。WebAPI で指定した devicename を確認してください。
1706	404	デバイス情報が見つからない。WebAPI で指定した devicename を確認してください。
1707	500	スクリプト実行エラー。CLM のログを確認してください。
1708	404	デバイスのステータスが既に無効状態。
1709	404	デバイスのステータスが既に有効状態。
1710	404	デバイスのステータスが既に削除状態。
1901	500	ログ初期化失敗。CLM のログを確認してください。
2001	500	初期化処理で異常発生。CLM のログを確認してください。
2002	500	暗号化処理で異常発生。CLM のログを確認してください。
2003	500	復号化処理で異常発生。CLM のログを確認してください。
2004	500	SecureWare/開発キットの API 呼び出しで異常発生。CLM のログを確認してください。
2005	500	軽量暗号 開発キットのコマンド呼び出しで異常発生。CLM のログを確認してください。
2201	404	ファイルが見つからない。CLM のログを確認してください。
2202	500	ファイルの読み込みに失敗。CLM のログを確認してください。
2203	500	ファイルの書き込みに失敗。CLM のログを確認してください。

2204	500	ファイルの削除に失敗。CLM のログを確認してください。
2205	500	日付のフォーマット変換 (数値<->文字列) 失敗。CLM のログを確認してください。
9901	500	システムエラー。CLM のログを確認してください。