# 取扱説明書(操作用)

ローカル認証局作成支援ソフトウェア

# 形 式 **LCA−SG**

# 目　次

# 1. はじめに

このたびは、弊社のソフトウェアをダウンロードいただき誠にありがとうございます。
ご使用いただく前に下記事項をご確認下さい。

## 1.1. はじめに

SG6 では通信セキュリティ向上のために HTTPS をサポートしています。
本書では、HTTPS を利用するために必要な証明書の作成方法について説明します。

## 1.2. 取扱説明書の対応バージョンについて

本取扱説明書は、下表のバージョン以上に対応しています。

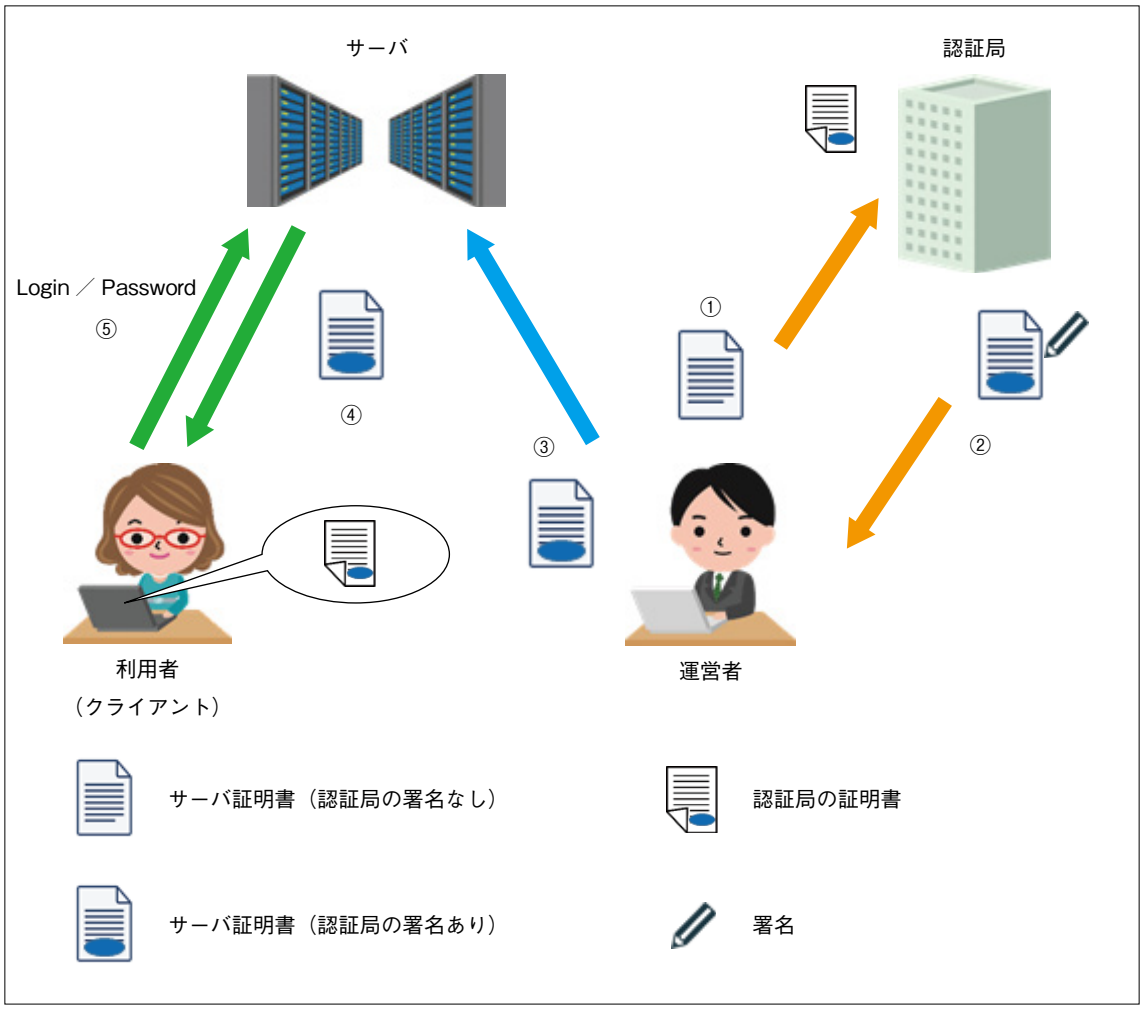
| 形　式 | バージョン |
|---|---|
| LCA－SG | 1.1.0 |
| SG6 | 1.0.8 |

SG6 の詳細はセキュリティゲートウェイ操作用取扱説明書（NM－8591－B）を参照下さい。

# 2. サーバ認証

ここでは、サーバ認証の概要について説明します。ルート CA、中間 CA、電子署名、SSL ／ TLS の詳細等については、各種 Web サイトや書籍等を参照して下さい。

一般的な HTTPS 対応の Web サイト開設時は、おおよそ以下のような手順を経ます。
①運営者は、サーバ証明書を作成して認証局に送付し、署名依頼する。
②認証局は、運営者およびサーバの身元を確認した後 Web サーバ証明書に署名し、運営者に返却する。
③運営者は、サーバ証明書をサーバにインストールする。



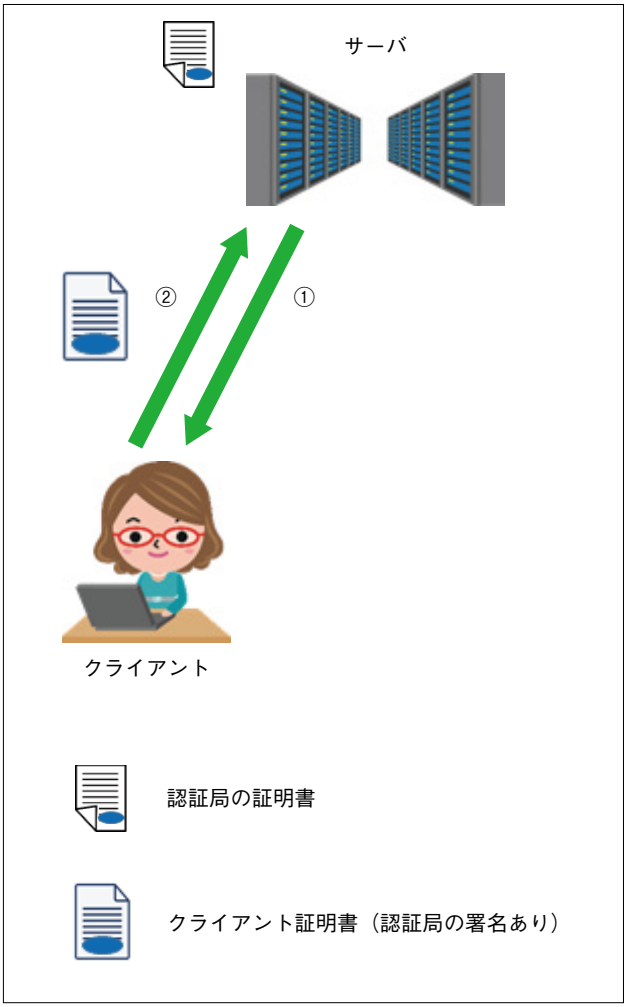

利用者がブラウザを用いてサーバにアクセスすると、HTTPS 接続時に認証局の署名付きサーバ証明書がダウンロードされます（図中④）。この署名の真偽確認には署名した認証局の証明書が必要ですが、主要な認証局の証明書はブラウザにプリインストールされているため、すぐに確認処理を行います。正しい署名であることが確認できれば、接続したサーバは信頼できる認証局により身元確認済みと判断されます。結果として、利用者は目的とした Web サイトに正しく接続できており、悪意のあるなりすましサイトに接続している訳ではないことを認識できます。
さらに、サーバ証明書には暗号に関する情報も含まれており、これを用いてサーバと利用者のブラウザは暗号通信を行います。よって、通信データの盗み見や改ざんを防ぐことができます。

以上のようにして、HTTPS では通信セキュリティを確保しています。この場合、クライアントとなる利用者はサーバ証明書により接続したサーバを認証（サーバ認証）します。一方、Web サーバは接続してくる利用者をログイン名とパスワード（図中⑤）で認証します。

このログイン名とパスワードの送信は暗号化されるため、盗聴の可能性は低くなります。しかし、推測やブルートフォースアタック（総当たり攻撃）等により不正にログインされてしまうリスクが存在します。

# 3. クライアント認証

前述のサーバ認証とは反対に TLS ではサーバがクライアントに対して証明書を要求（図中①）することもできます。クライアントはクライアント証明書をサーバに送信（図中②）し、これを受け取ったサーバは署名確認できたクライアントの接続を許可します。したがって、この証明書にはサーバが認めた認証局による署名が必要となります。

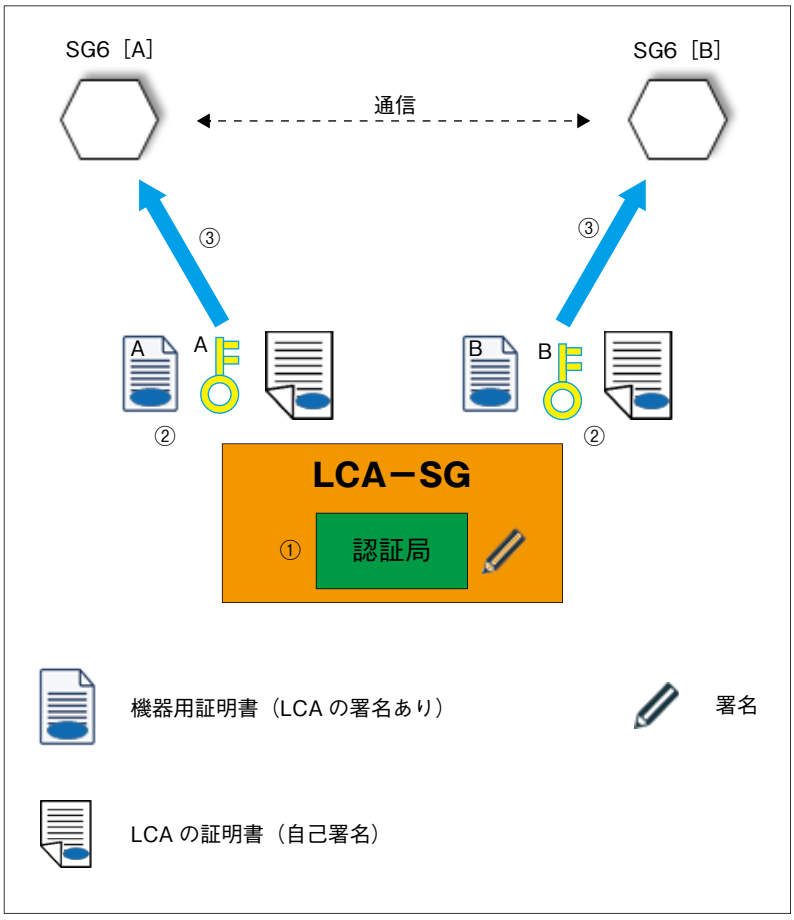


# 4. ローカル認証局（LCA）

SG6 はサーバ認証・クライアント認証の両方を使用した相互認証により接続相手を認証します。これらは、Web サーバのように広く公開する使い方をしないため、この相互認証が可能になります。またこの場合、認証局もローカル環境に構築した方が使いやすくなります。これに対応するためのソフトウェアとして、ローカル認証局支援ツール（形式：LCA－SG）をご用意しています。

LCA－SG を用いて、以下の作業を行うことができます。

① LCA－SG をインストールした PC 内に、ローカル認証局（LCA）を構築する。このとき同時に LCA の証明書も生成される。
② LCA－SG により、機器毎に証明書および秘密鍵を作成する。この証明書はサーバ証明書／クライアント証明書共通となり、LCA の署名が入る。
③①で作成した LCA の証明書、②で作成した機器用の証明書および秘密鍵を機器に転送する。




SG6 同士が通信するためには、同じ LCA に署名された証明書を持つ必要があります。LCA－SG を再インストールしたり、LCA を再構築したりした状態で通信ネットワークに SG6 を追加する場合には、全 SG6 に新しい LCA の署名がついた証明書を再転送する必要があります。ご注意下さい。

**注意事項**
LCA－SG が生成するファイルには、セキュリティを確保上、重要なものが含まれています。取扱いには十分な配慮をお願いします。
SG6 および LCA－SG は、完全なセキュリティの確保を保証するものではありません。
お客様の責任において運用をお願いします。

# 5. LCA－SG の使い方

## 5.1. システム要件

LCA－SG の動作に必要なパソコンの条件を以下に示します。

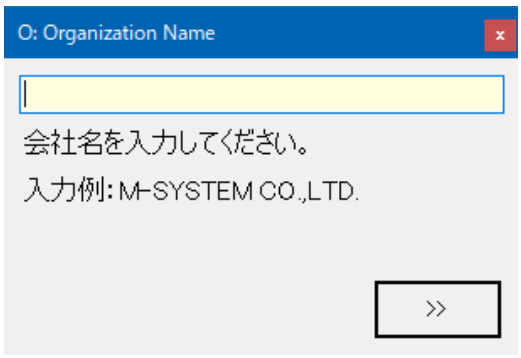
| 項　目 | 内　容 |
|---|---|
| パソコン<br>OS | 下記 OS が動作する PC／AT 互換機<br>Windows10 32／64bit 版の Home、Professional、Enterprise エディション |
| OS 以外 | DOT.NET Framework 4 以上 |
| メモリ | 2 GB 以上 |
| ハードディスク<br>空き容量 | 60 MB 以上<br>注）別途ユーザーデータの保存領域が必要 |
| ディスプレイ解像度 | XGA（1024 × 768）以上 |
| 言語 | 日本語 |

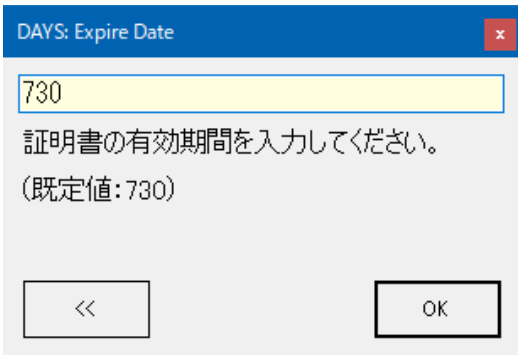
## 5.2. インストール

ダウンロードしたファイルを同一フォルダに格納し、「Setup.exe」を実行して下さい。一般的な Windows インストーラにてインストールを行います。
インストール中に、セキュリティ警告画面が表示される場合があります。
インストーラ関連ファイルが弊社の HTTPS サイトよりダウンロードされたものであることを確認の上、インストールを継続して下さい。

## 5.3. 内部認証局の作成

LCA－SG インストール後の初回起動時に、会社名等の組織名称と証明書の有効期間を設定します。
起動時に表示されるダイアログに会社名などの組織名称を入力して下さい。これが、認証局の組織名称になります。
証明書の有効期間を設定するダイアログが表示されますので、30 ～ 3653 日の範囲内で入力して下さい。これが、証明書の作成時点からの有効期間となります。
すべての入力を完了すると、確認ダイアログが表示されるので、「O=」に登録した組織名称と入力した有効期間が表示されていることを確認後【OK】ボタンをクリックして下さい。




| 項　目 | 内　容 |
|---|---|
| Organization Name | 会社名等の組織名称設定して下さい。<br>入力可能文字<br>1 文字目: 半角英字、‘_’<br>2 文字目以降: 半角英数字、‘_’、‘.’、‘,’、‘-‘、‘ ’( 空白 ) |
| Expire Date | 機器用証明書の有効期間を 30～3653 日の範囲で設定して下さい。<br>作成・転送時点からの日数となります。 |

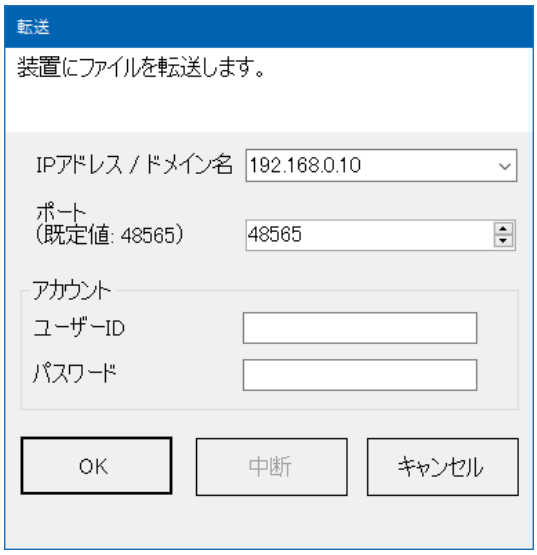
認証局が作成されると下図画面が表示され、これが LCA－SG のメイン画面になります。

## 5.4. 機器用証明書・秘密鍵の作成・転送

続いて、SG6 用の証明書を作成し、本体に転送します。
メイン画面の【新規証明書】をクリックすると下図ダイアログが表示されるので、SG6 にアクセスするための情報を入力して下さい。


| 項　目 | 内　容 |
|---|---|
| ドメイン名 | インターネット経由で SG6 に接続するときのドメイン名を半角英数字で設定して下さい。<br>ドメイン名を使わない場合は、設定不要です。<br>(日本語ドメインには対応していません)<br>最大 16 個まで登録可能です。<br>入力可能文字<br>1 文字目: 半角英字、'_'<br>2 文字目以降: 半角英数字、'_'、'.'、','、'-'、' '( 空白 ) |
| IP アドレス | インターネットもしくは LAN で SG6 に Web アクセスするための SG6 サーバと SG6 クライアント両方の IP アドレスを、半角英数字で設定して下さい。<br>(IPv6 には対応していません)<br>最大 16 個まで登録可能です。<br>設定する IP アドレスを減らしたい場合は次のものを設定しますが、SG6 サーバと SG6 クライアント両方を設定しても問題ありません。<br>標準モードで接続する場合: SG6 サーバの IP アドレス<br>逆接続モードで接続する場合: SG6 クライアントの IP アドレス |
| CN | SG6 を識別するための名称を設定して下さい。<br>入力可能文字<br>1 文字目: 半角英字、'_'<br>2 文字目以降: 半角英数字、'_'、'.'、','、'-'、' '( 空白 ) |

入力後、【OK】ボタンをクリックすると確認ダイアログが表示されます。
【はい】をクリックすると、下図の転送ダイアログが表示されます。




SG6 の設定画面にログインするためのユーザー ID、パスワードを入力し【OK】ボタンをクリックして下さい。SG6 への証明書転送を開始します。
作成した証明書に関する情報は、メイン画面の「証明書」に記録されます。SG6 が複数台ある場合は、同じ作業を台数分行うか、記録された証明書を右クリックし、「作成・転送」を選択して下さい。
SG6 クライアントと SG6 サーバの両方に、証明書を転送します。
転送後は、SG6 を再起動させて下さい。


**注意事項**
・機器への転送は、LAN 環境下にて行って下さい。
・ドメイン名と IP アドレスについては、間違いがないよう慎重に入力して下さい。

# 5.5. 認証局証明書を Web 接続する端末にインストール

## 5.5.1. 概要

Web ブラウザから Web サーバに接続するときに、SG6 を経由して HTTPS で接続するときは、8 ページの「5.3. 内部認証局の作成」で作成した認証局の証明書を Web 接続する端末にインストールします。
この作業は、この認証局の署名付き証明書を持つ SG6 にアクセスする全端末について行って下さい。この作業を実施せずに SG6 に HTTPS 接続すると、ブラウザにセキュリティ関連の警告画面が表示されます。
接続する端末によってインストール可能な方法が異なります。

## 5.5.2. LCA－SG からインストールする場合

### 5.5.2.1. Windows（Chrome、Edge）

① LCA－SG メイン画面の【認証局証明書の表示】をクリックすると次のダイアログが表示されますので、【証明書のインストール】ボタンをクリックして下さい。
「証明書のインポートウィザード」が開始します。

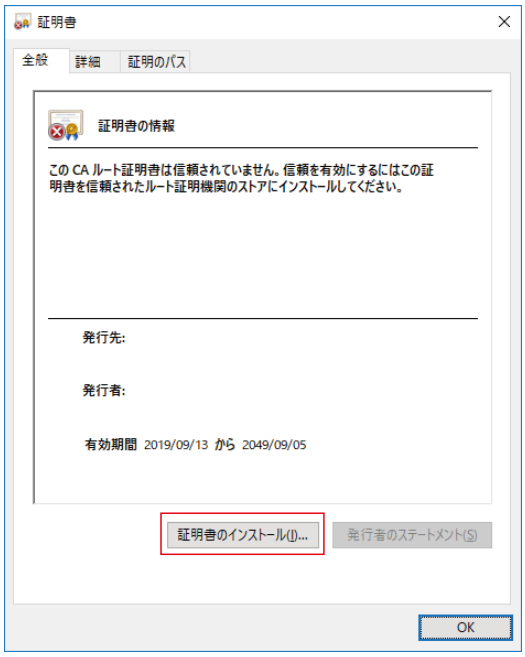



図　認証局証明書の表示画面（全般）

②「証明書のインポートウィザードの開始」の画面が表示されると「保存場所」を【現在のユーザー】を選択し、【次へ】ボタンをクリックして下さい。

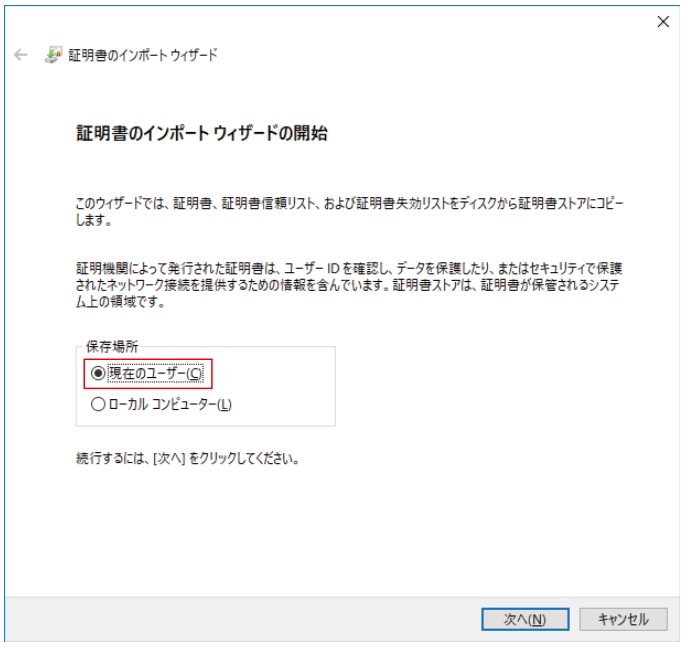



図　証明書のインポートウィザードの開始画面

③「証明書ストア」の画面が表示されると、【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て下さい。

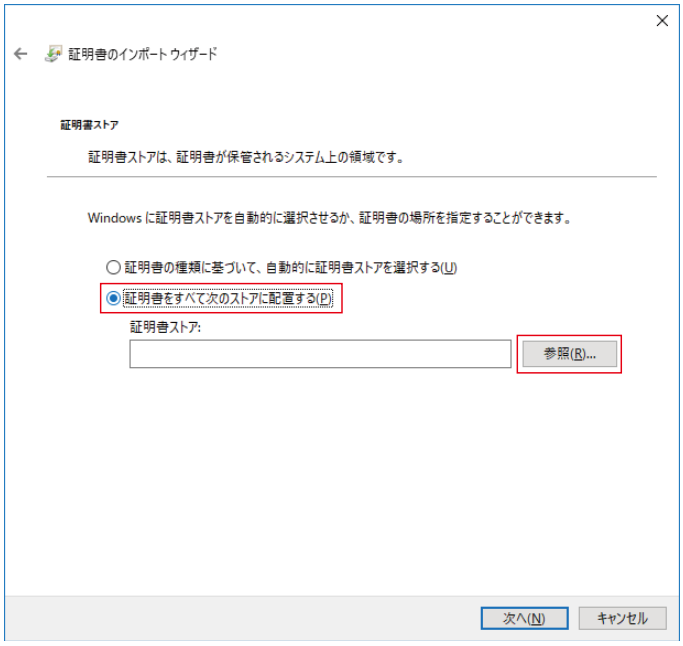



図　証明書ストア画面

④「証明書ストアの選択」ダイアログが表示されますので、ここで【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て下さい。

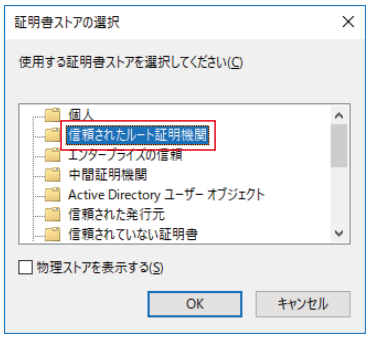



図　証明書ストアの選択画面

⑤ウィザードの途中で、Windows がセキュリティ警告を出す場合があります。
LCA－SG は、お客様自身がルート証明機関となるソフトウェアです。警告内容を熟読して問題ないことを確認の上、登録して下さい。

## 5.5.3. 認証局証明書ファイルを使用する場合

### 5.5.3.1. Windows（Chrome、Edge）

① 20 ページの「5.6. 認証局証明書の保存」の方法で認証局証明書を保存します。
②保存した認証局証明書ファイルをダブルクリックすると証明書ダイアログが表示されます。
【証明書のインストール】をクリックすると、「証明書のインポートウィザード」が開始します。
以降は、11 ページの「5.5.2.1. Windows（Chrome、Edge）」と同様の手順になります。
なお、LCA－SG をインストールしていない端末でも、同様の手順となります。

### 5.5.3.2. Windows（FireFox）

① 20 ページの「5.6. 認証局証明書の保存」の方法で認証局証明書を保存します。
② Firefox ブラウザを起動し、右上のメニューボタンをクリックし、【オプション】を選択して下さい。
オプションタブが開きます。

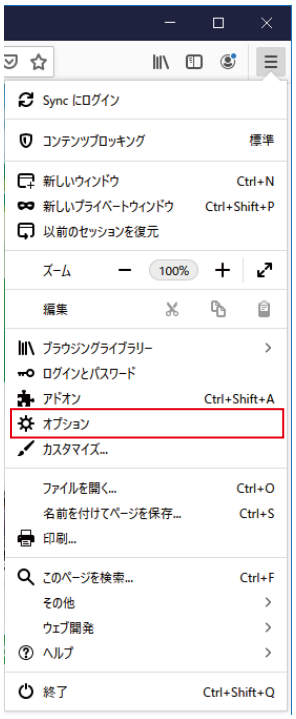



図　Firefox ブラウザ

③【プライバシーとセキュリティ】をクリックして下さい。


図　Firefox オプション画面

④「ブラウザープライバシー」が表示されますので【証明書を表示】ボタンをクリックして下さい。


図　Firefox プライバシーとセキュリティ画面

⑤「証明書マネージャー」が表示されますので【インポート】ボタンをクリックして下さい。

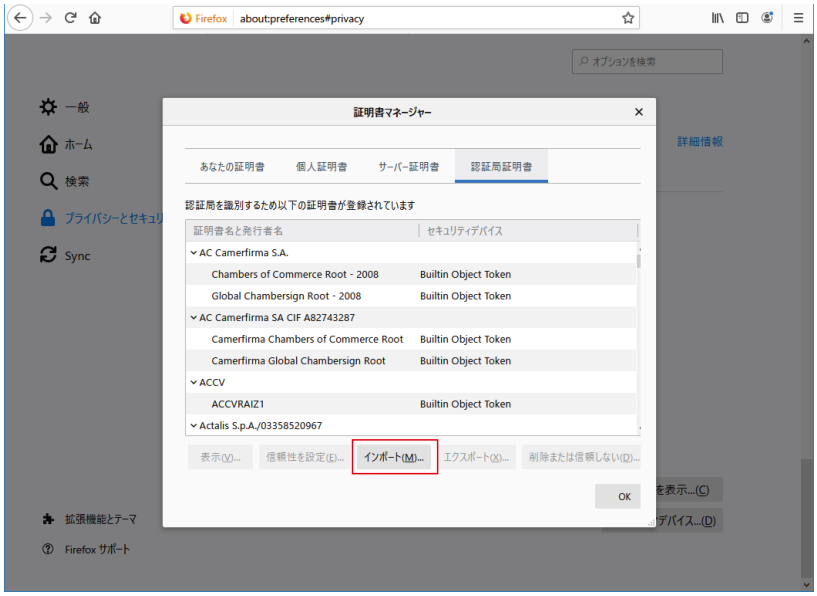



図　Firefox 証明書マネージャー画面

⑥ファイル選択画面が表示されますので③で保存したファイル（cacert.crt）を選択して下さい。

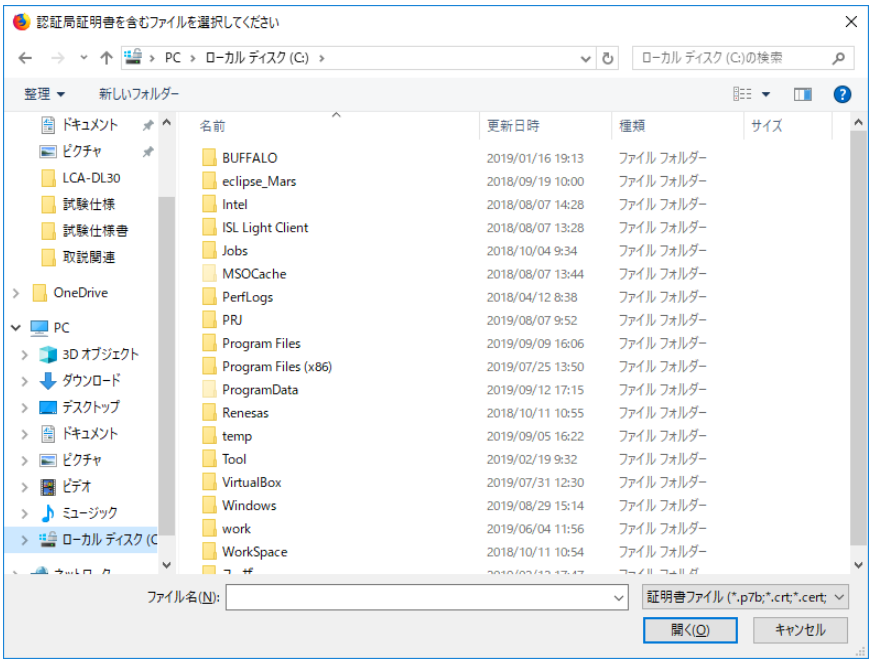



図　Firefox 認証局証明書ファイル選択画面

⑦「証明書のインポート」が表示されますので【この認証局によるウェブサイトの識別を信頼する】にチェックを入れ、【OK】ボタンをクリックして下さい。

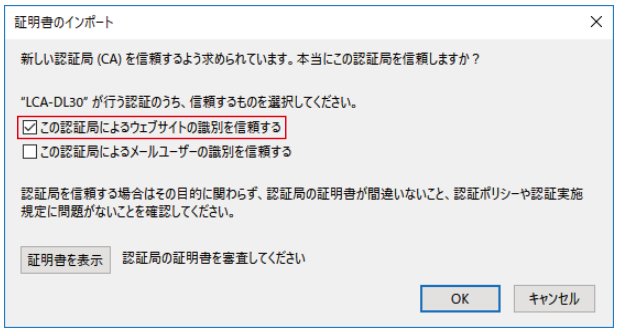



図　Firefox 証明書のインポート画面

⑧これで、LCA－SG 内部認証局の証明書が Firefox に登録されました。Firefox を閉じて下さい。

## 5.5.4. SG6 からインストールする場合

### 5.5.4.1. Windows（Chrome、Edge、FireFox）

① SG6 のシステム設定画面にログインし、「Maintenance」の「Download CA Certificate File」から認証局証明書をダウンロードします。
以降は、13 ページの「5.5.3. 認証局証明書ファイルを使用する場合」と同様の手順になります。

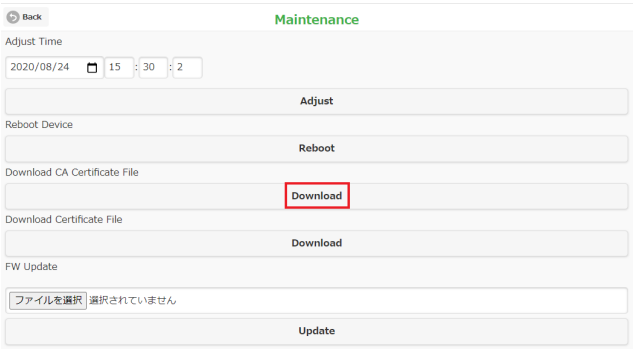



図　CA 証明書ダウンロード画面

#### 5.5.4.2. iPadOS（Safari）

① SG6 のシステム設定画面にログインし、「Maintenance」の「Download CA Certificate File」をタップすると、下図のメッセージが表示されますので［許可］をタップし、ダウンロードします。


図　iPadOS メッセージ画面

②ダウンロード完了後は、ホーム画面に戻り、歯車マークの［設定］をタップし“プロファイルがダウンロードされました”をタップします。

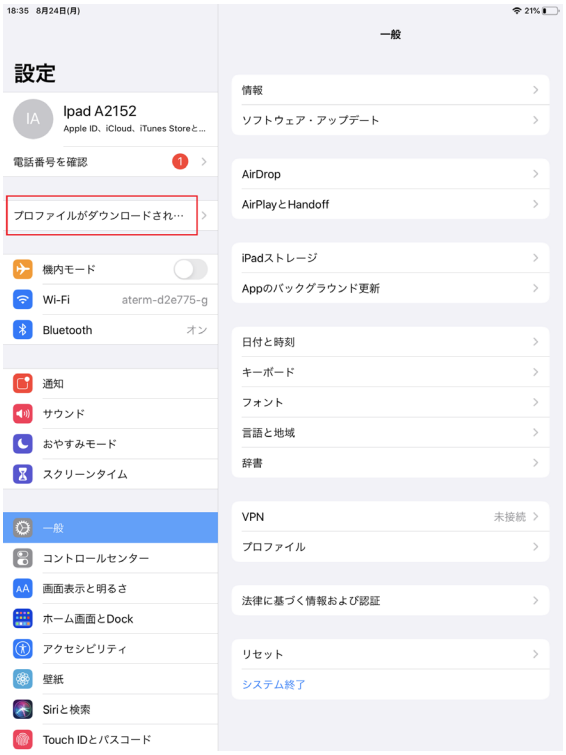



図　iPadOS 設定画面

③ダウンロードしたプロファイルをタップし、プロファイルの詳細を表示します。
表示されたプロファイルの詳細右上の［インストール］をタップし、端末にプロファイルをインストールします。
途中、警告が表示されますが再度［インストール］をタップしてインストールを続行して下さい。


図　インストール画面

④インストールが完了後は、［設定］→［一般］→［情報］→［証明書信頼設定］とタップし［証明書信頼設定］を開き、「ルート証明書を全面的に信頼する」の項目に表示されているプロファイルを有効にします。

#### 5.5.4.3. Android（Chrome）

① SG6 のシステム設定画面にログインし、「Maintenance」の「Download CA Certificate File」をタップし、認証局証明書をダウンロードします。


図　Android Maintenance 画面

② Chrome の右上のメニューからダウンロードを開き、保存した認証局証明書をタップします。

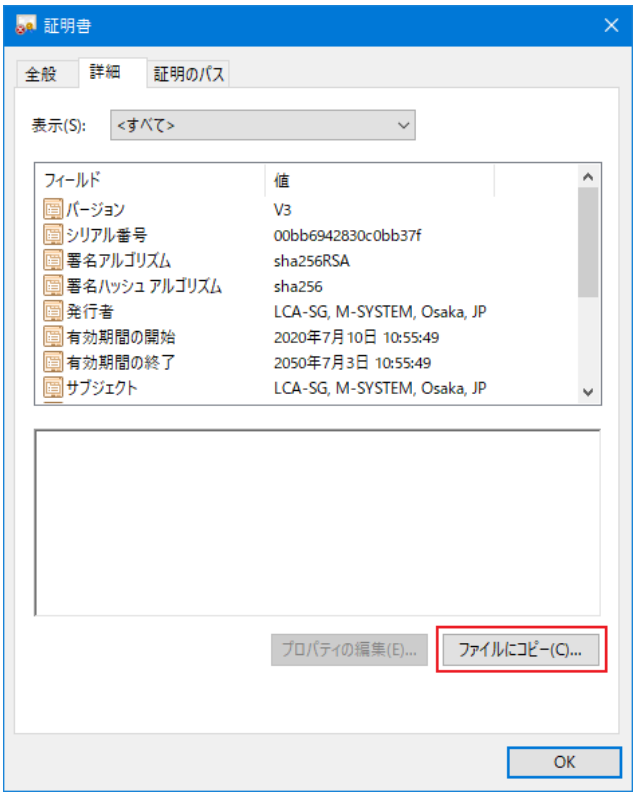

図　ダウンロード画面

③任意の証明書名を入力し［OK］をタップすることで認証局証明書が登録されます。


図　Android 証明書インストーラー画面

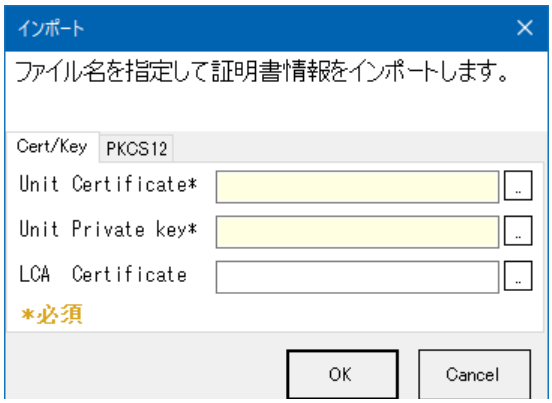
## 5.6. 認証局証明書の保存

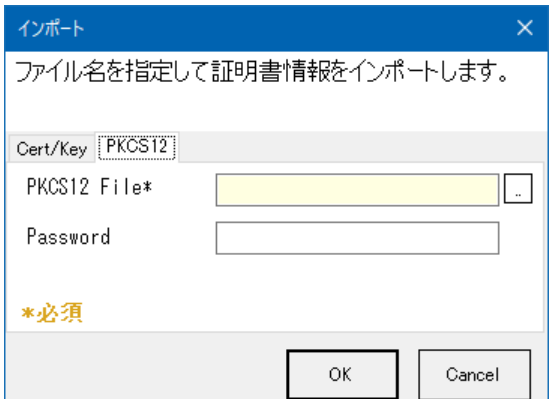
8 ページの「5.3. 内部認証局の作成」で作成した認証局証明書を機器に保存する必要がある場合は、メイン画面の「認証局証明書の表示」をクリックします。表示されるダイアログにある「詳細」タブの【ファイルにコピー】から保存して下さい。



## 5.7. 証明書のインポート

LCA－SG の認証局を用いずに、外部の認証局に署名してもらうことも可能です。この場合は、LCA－SG を経由して証明書ファイルと秘密鍵ファイル、認証局証明書を SG6 本体に転送します。
メイン画面の【インポート】をクリックすると、インポートダイアログが表示されます。




証明書は PEM 形式（.crt、.key）、DER 形式（.der）と PKCS12 形式（.pfx、.p12）に対応しています。
ファイルを選択後【OK】をクリックすると本体への転送を開始します。

**注意事項**
証明書のインポートに関連するご質問については、弊社ではお答えすることができません。
ご了承下さい。

## 5.8. 認証局の再構築

内部認証局は LCA－SG インストール後の初回起動時に作成されるので、通常は再構築の必要はありません。
再構築が必要な場合は、メイン画面の【新規認証局】から行って下さい。
LCA の再構築後は、機器への再転送が必要となります。

## 5.9. 表示言語の切替え

LCA－SG インストール後は OS が日本語の場合は自動的に日本語で表示され、OS が日本語以外の場合は自動的に英語で表示されます。
表示言語を切替えたい場合はメイン画面の【Language】をクリックすると、言語切替えを確認するダイアログが表示されますので【OK】ボタンをクリックしてください。LCA－SG を再起動すると画面の言語が切替わります。

# 6. ライセンス

本製品は OpenSSL v1.0.1r を使用している。(OpenSSL License、Original SSLeay License デュアルライセンス ) 本製品には、以下の Camellia ライセンスの適用を受けるソフトウェアが含まれている。

OpenSSL License
---

==========

Copyright (c) 1998-2018 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:
“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)”

4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:
“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License
---

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).
The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young' s, and as such any Copyright notices in the code are not to be removed.
If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.
This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)." The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:
   "This product includes software written by Tim Hudson (tjh@cryptsoft.com)."

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence].

camellia.c ver 1.2.0

Copyright (c) 2006, 2007
NTT (Nippon Telegraph and Telephone Corporation). All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer as the first lines of this file unmodified.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY NTT "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL NTT BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON
ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.