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－RGP**

目　次

1. はじめに

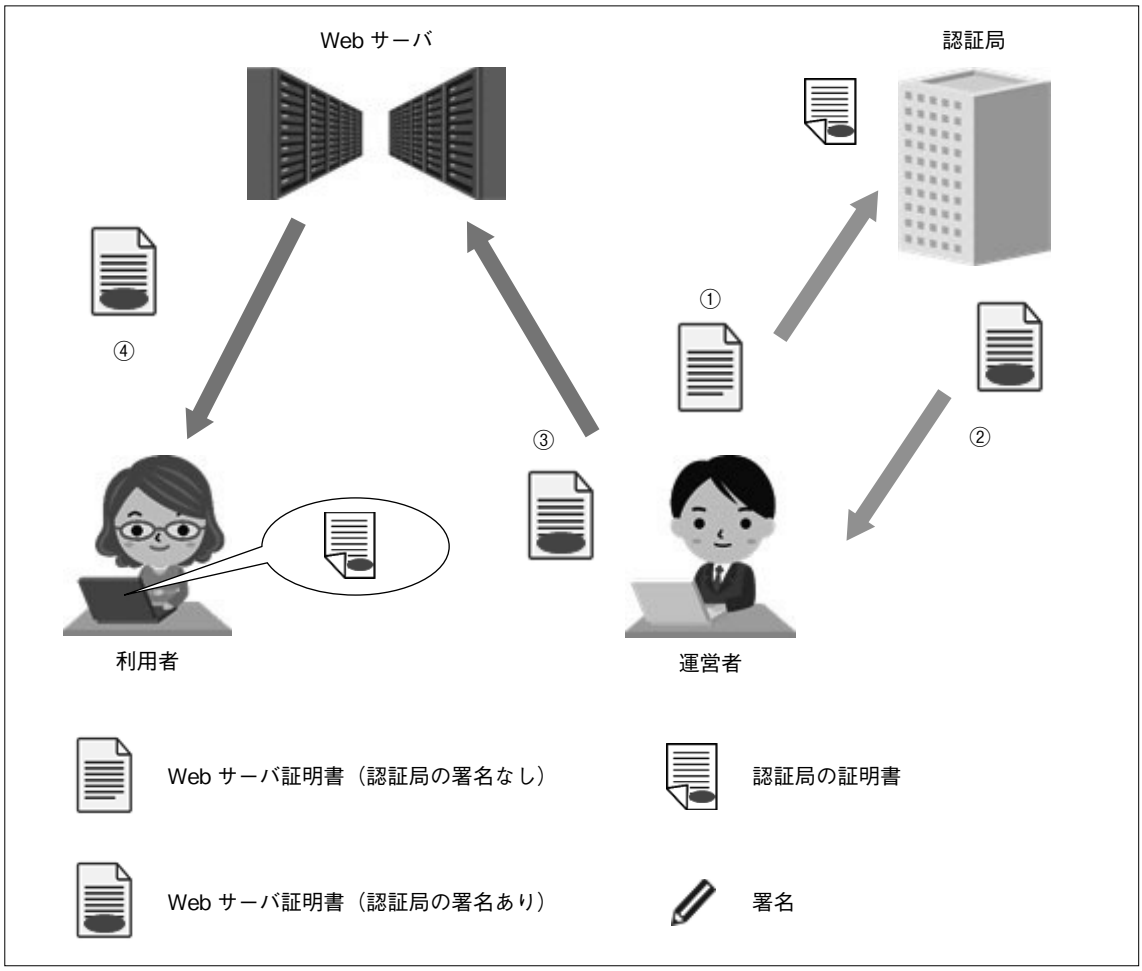
RGP □は通信セキュリティ向上のため、HTTPS をサポートしています。
本書では、HTTPS を利用するために必要な証明書の作成方法について説明します。

注）HTTPS を使用するために RGP30 Ver. 1.1 以上または RGP6 Ver. 1.0 以上が必要です。
RGP30 Ver. 1.0 をご使用の場合は Ver. 1.1 以上に更新して下さい。

2. Web サーバ証明書概要

ここでは、Web サーバ証明書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ください。

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、Web 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 Web 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、Web サーバ証明書を Web サーバにインストールする。



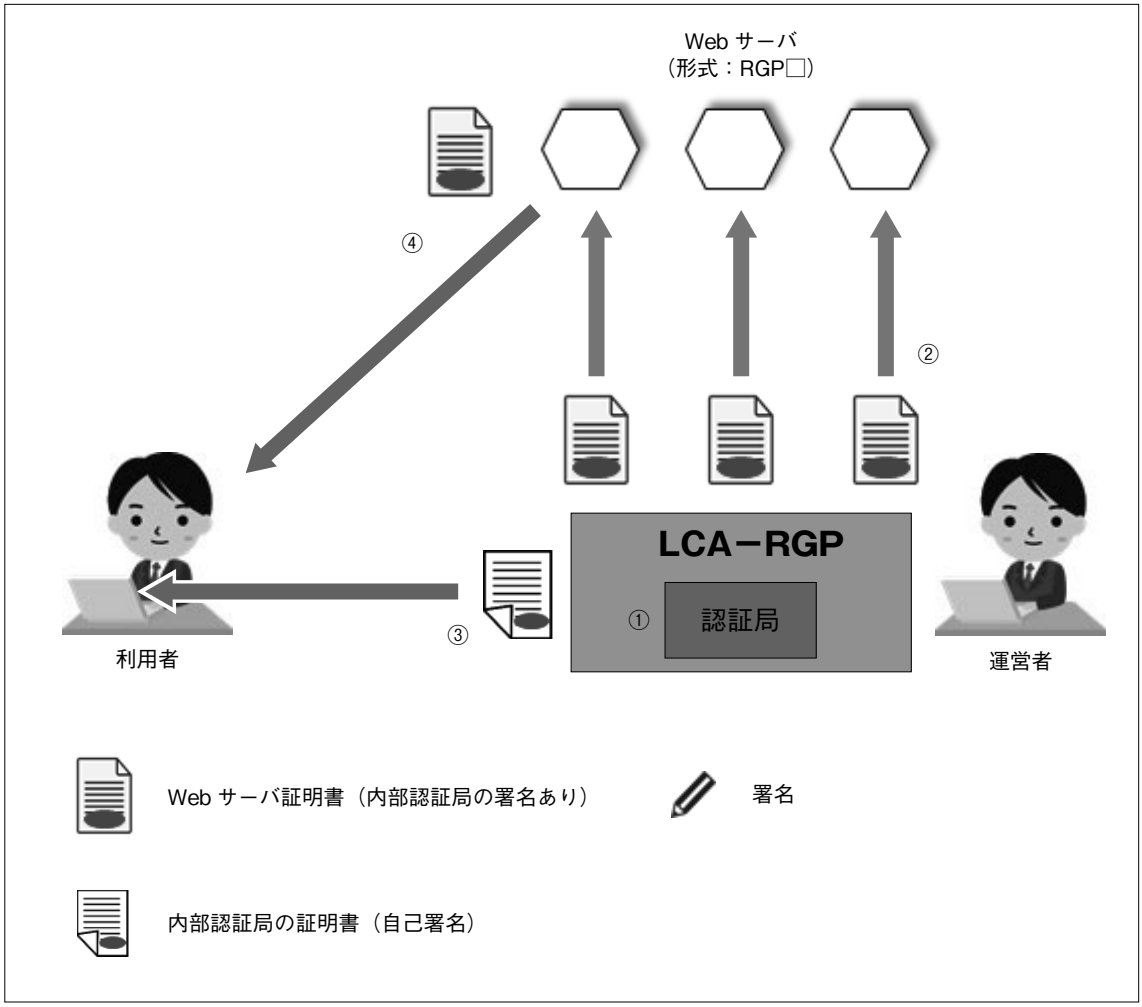
利用者がブラウザを用いて Web サーバにアクセスすると、HTTPS 接続時に認証局の署名付き Web サーバ証明書がダウンロードされます（図中④）。この署名の真偽確認には署名した認証局の証明書が必要ですが、主要な認証局の証明書はブラウザにプリインストールされているため、すぐに確認処理を行います。正しい署名であることが確認できれば、接続した Web サーバは信頼できる認証局により身元確認済みと判断されます。結果として、利用者は目的とした Web サイトに正しく接続できており、悪意のあるなりすましサイトに接続している訳ではないことを認識できます。
さらに、Web サーバ証明書には暗号に関する情報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

3. ローカル認証局（LCA－RGP）

先述した通り、不特定多数の利用者を想定する一般の Web サイトにおいては、第三者の認証局による Web サーバの身元確認が必須となります。しかし、産業機器に搭載された簡易 Web サーバの運用においては、多くの場合はユーザーが運営者と利用者を兼ねます。つまり、自ら設置した機器に自らがアクセスする使い方になります。このような用途においては、第三者の認証局による身元確認を簡略化しても、大きな問題にはならないとも考えられます。

ローカル認証局支援ツール（形式：LCA－RGP）を用いると、この身元確認の簡略化を容易に実現できます。
LCA－RGP は、弊社のホームページ（HTTPS サイト）よりダウンロードできます。

この場合はユーザーが認証局をも兼ねることになり、以下の手順となります。
① LCA－RGP をインストール後の初回起動時、その PC 内部に認証局が作成される。
② LCA－RGP を用いて機器毎に Web サーバ証明書を作成し転送する。このとき署名は自動で行われる。
③ LCA－RGP 内部認証局の証明書を、利用者端末の OS・ブラウザに手動でインストールする。



LCA－RGP 内部認証局は主要な認証局ではないため、その証明書はブラウザにプリインストールされていません。
このため、図中③の処理が必要になりますが、それ以外については一般的な HTTPS と全く変わりありません。

以上より、LCA－RGP を用いると HTTPS に必要な身元確認を簡略化できます。LCA－RGP は LAN 環境にも対応しているため、ローカルネットワークにおいても簡単に HTTPS 化が可能です。

注意事項
LCA－RGP 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。
RGP □の HTTPS サーバおよび LCA－RGP は、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。

4. LCA－RGP の使い方

4.1. システム要件

LCA－RGP 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 OS	下記 OS が動作する PC／AT 互換機 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 空き容量	10 MB 以上 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

4.2. 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」を実行してください。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ください。

4.3. 内部認証局の作成

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。*1

＊1、初回設定時以外は確認ダイアログが表示されません。組織名称を再設定する場合は、19 ページの「4.7. 認証局の再構築」にて内部認証局を再構築してください。

図 4.1　Organization Name 画面

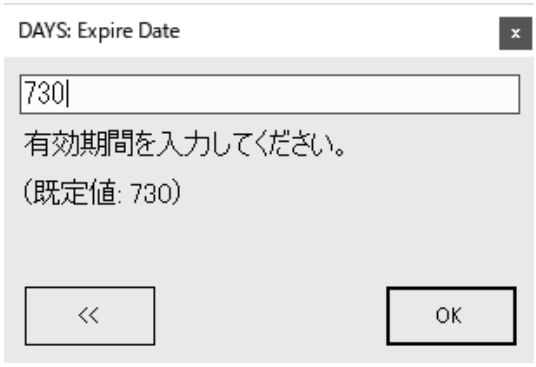


図 4.2　Expire Date 画面

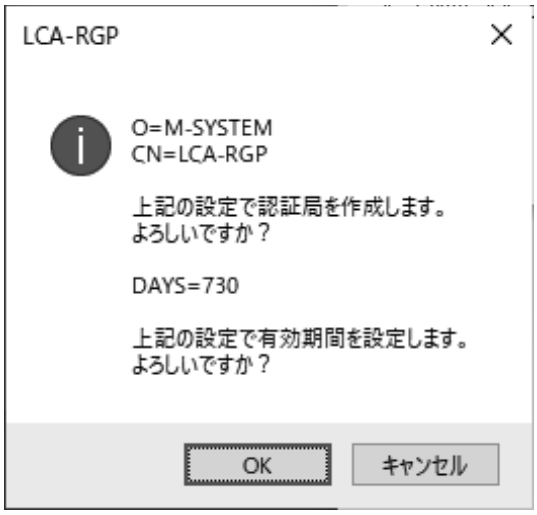


図 4.3　確認ダイアログ

項　目	内　容
Organization Name	会社名等の組織名称設定してください。LCA－RGP 内部認証局の組織名称となります。 入力可能文字 1 文字目: 半角英字、‘_’ 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。 作成・転送時点からの日数となります。

内部認証局を作成すると次の画面が表示されます。これが LCA－RGP のメイン画面になります。

図 4.4　メイン画面

4.4. Web サーバ証明書の作成・転送

RGP □用の Web サーバ証明書を作成し、本体に転送します。
メイン画面の【新規証明書】をクリックすると次のダイアログが表示されますので、RGP □の簡易 Web サーバの IP アドレスまたはドメイン名を入力してください。

図 4.5　証明書情報編集画面

項　目	内　容
ドメイン名	インターネット経由で RGP □に Web アクセスするためのドメイン名を、半角英数字で設定してください。 (日本語ドメインには対応していません) 最大 8 個まで登録可能です。
IP アドレス	インターネットもしくは LAN で RGP □に Web アクセスするための IP アドレスを、半角英数字で設定してください。 (IPv6 には対応していません) 最大 8 個まで登録可能です。
CN	入力可能文字 1 文字目: 半角英字、'_' 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】ボタンをクリックすると、次の転送ダイアログが表示されます。

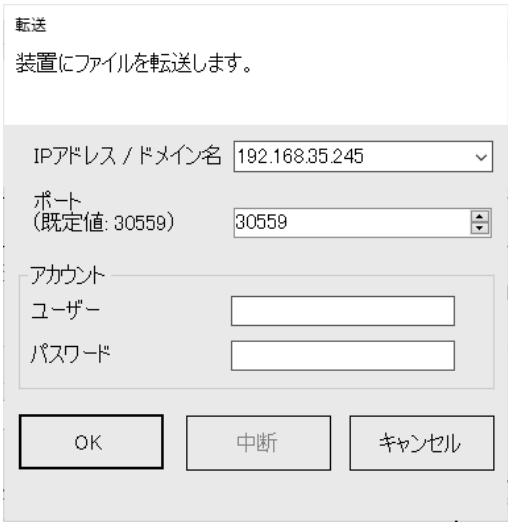


図 4.6　転送画面

RGP－Designer での作画データ転送時と同様、RGP □に接続するためのパラメータを入力し【OK】ボタンをクリックしてください。RGP □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。RGP □が複数台ある場合は、同じ作業を台数分行ってください。また、証明書は同じ認証局で複数作成することができます。「新規証明書（C)」をクリックして追加してください。既に表示されている証明書を作成・転送したい場合は、証明書を指定し、右クリックして「作成・転送」を選択してください。
登録した認証局や証明書は、LCA－RGP を終了し、再度起動しても削除しないかぎり表示されます。もし、不要な証明書を削除したい場合は、削除したい証明書を指定し、右クリックして「削除」を選択してください。

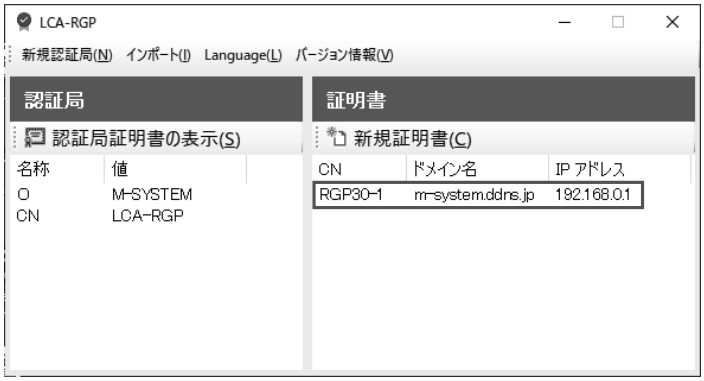


図 4.7　証明書情報

注意事項
RGP □本体への証明書転送時には、本体への Web アクセスは行わないでください。
ドメイン名と IP アドレスについては、間違いのないよう慎重に入力してください。間違いがある場合は、HTTPS アクセス時にセキュリティ警告画面が表示されます。

4.5. 認証局証明書のインストール

4.5.1. 概要

6 ページの「4.3. 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 RGP □にアクセスする全端末について行ってください。この作業を実施せずに RGP □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。

4.5.2. LCA－RGP からインストールする場合

4.5.2.1. Windows（Chrome、Edge）

① LCA－RGP 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ください。「証明書のインポートウィザード」が開始します。

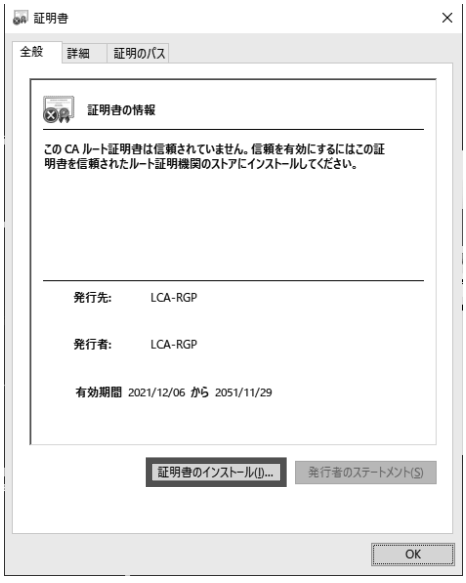


図 4.8　認証局証明書の表示画面（全般）

②「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ください。

図 4.9　証明書のインポートウィザード画面

③「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ください。

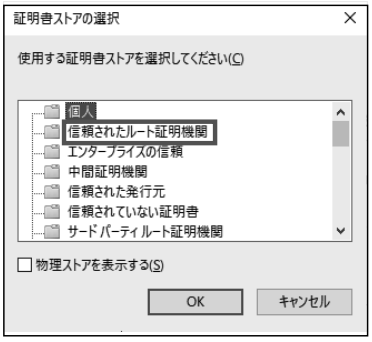


図 4.10　証明書ストアの選択画面

④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－RGP 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、登録してください。

4.5.2.2. Windows（Firefox）

① LCA－RGP メイン画面の【認証局証明書の表示】をクリックして証明書を表示し、「詳細」タブの【ファイルにコピー】ボタンをクリックしてください。

図 4.11　認証局証明書の表示画面（詳細）

②「証明書のエクスポートウィザード」が開始しますので、【次へ】ボタンをクリックしてください。「エクスポートファイルの形式」で【Base 64 encoded X.509 (.CER)】を選択し、次へ進んでください。

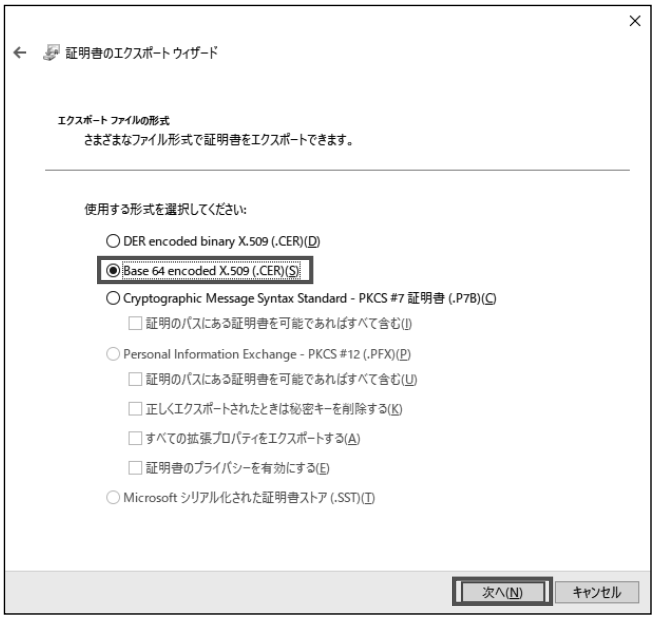


図 4.12　証明書のエクスポートウィザード画面（エクスポートファイルの形式）

③デスクトップ等に適当なファイル名で保存し、証明書ダイアログを閉じてください。

図 4.13　証明書のエクスポートウィザード画面（ファイル名）

④ 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】を選択してください。オプションタブが開きます。

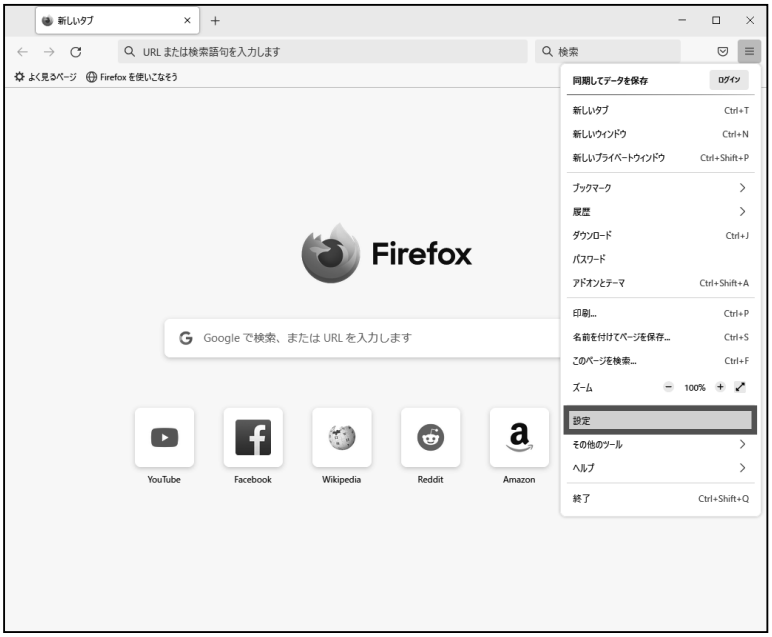


図 4.14　Firefox ブラウザ

⑤【プライバシーとセキュリティ】をクリックしてください。

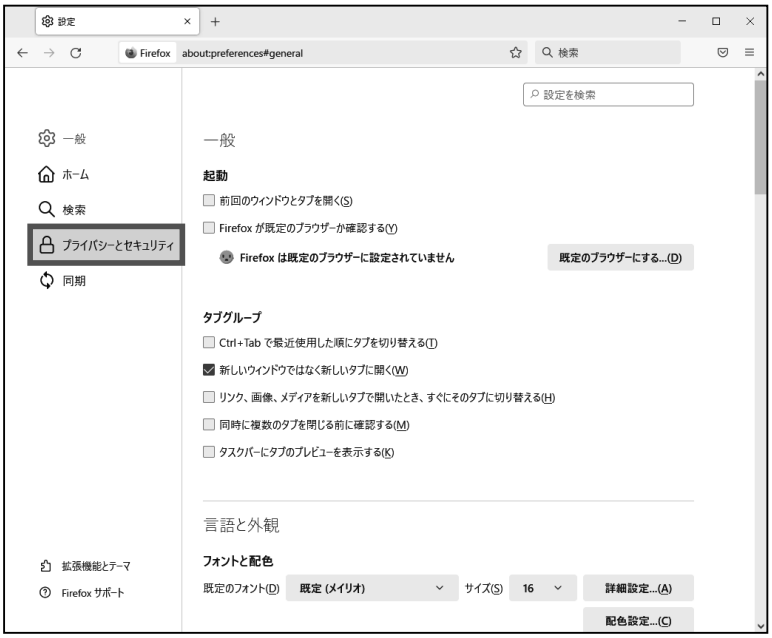


図 4.15　Firefox オプション画面

⑥「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ください。

図 4.16　Firefox プライバシーとセキュリティ画面

⑦「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ください。

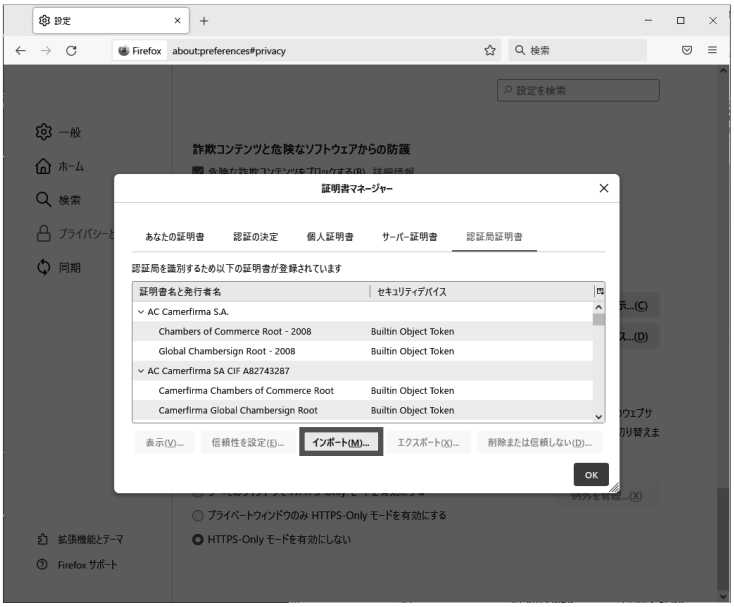


図 4.17　Firefox 証明書マネージャー画面

⑧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（.CER）を選択してください。

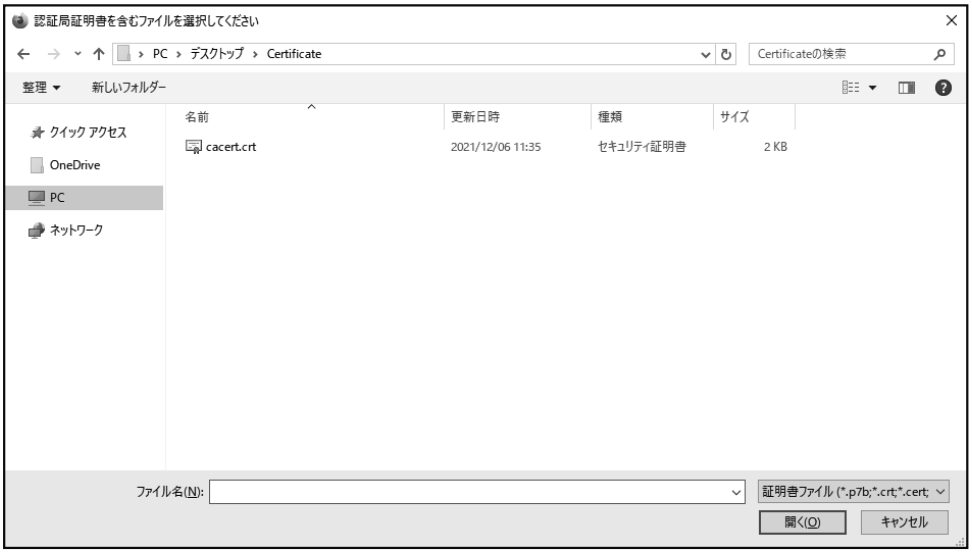


図 4.18　Firefox 認証局証明書ファイル選択画面

⑨「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ください。

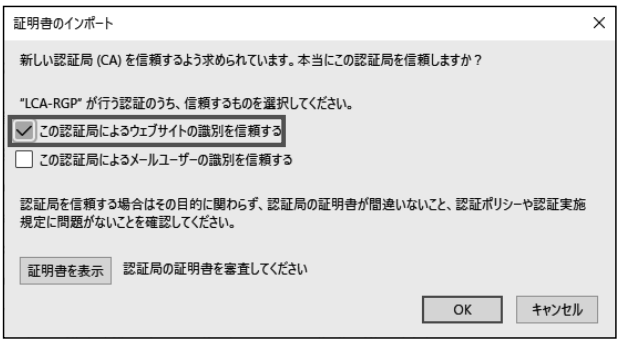


図 4.19　⑩これで、LCA－RGP 内部認証局の証明書が Firefox に登録されました。Firefox を閉じてください。

4.5.3. 認証局証明書ファイルを使用する

4.5.3.1. Windows（Chrome、Edge）

①認証局証明書ファイルを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、9 ページの「4.5.2.1. Windows（Chrome、Edge)」と同様の手順になります。

4.5.3.2. Windows（FireFox）

① 11 ページの「4.5.2.2. Windows（Firefox)」の④以降と同様の手順になります。

4.5.4. RGP □からインストールする場合

4.5.4.1. Windows（Chrome、Edge、FireFox）

① LCA－RGP で証明書を作成し転送した場合、RGP □の証明書ダウンロードサイト（RGP □の IP アドレスが初期設定の場合、http://192.168.0.1/SSL になります）を開き「Certificate_file」をクリックすると認証局証明書ファイルをダウンロードできます。ダウンロード後は、15 ページの「4.5.3. 認証局証明書ファイルを使用する」と同様の手順になります。
RGP □のシステム設定でダウンロードレベルが設定されている場合、ユーザー、パスワードを求められます。RGP－Designer で転送したユーザーアカウント設定のログイン名、パスワードを入力してください。

4.5.4.2. iOS（Safari）

① LCA－RGP で証明書を作成し転送した場合、RGP □の証明書ダウンロードサイト（RGP □の IP アドレスが初期設定の場合、http://192.168.0.1/SSL になります）を開き「Certificate_file」をクリックすると認証局証明書ファイルをダウンロードできます。

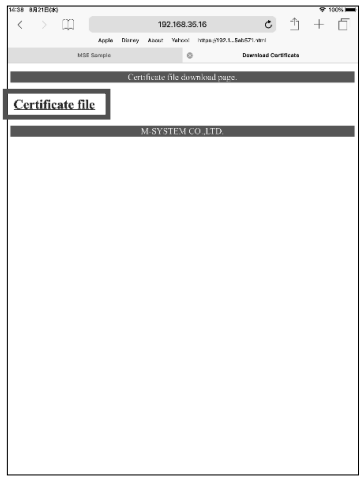


図 4.20　iOS Certificate_file 画面

②次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 4.21　iOS メッセージ画面

③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 4.22　iOS 設定画面

④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ください。

図 4.23　iOS インストール画面

⑤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。

4.5.4.3. Android（Chrome）

① iOS と同様に認証局証明書をダウンロードします。

図 4.24　Android Certificate_file 画面

②ダウンロードした認証局証明書を開きます。

図 4.25　Android Certificate_file 画面（開く）

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 4.26　Android 証明書インストーラー画面

4.6. 証明書のインポート

LCA－RGP 内部認証局を用いずに、一般的な HTTPS 対応 Web サイト開設時と同様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－RGP を経由して証明書ファイルと秘密鍵ファイルを RGP □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。

図 4.27　証明書のインポート（PEM 形式）

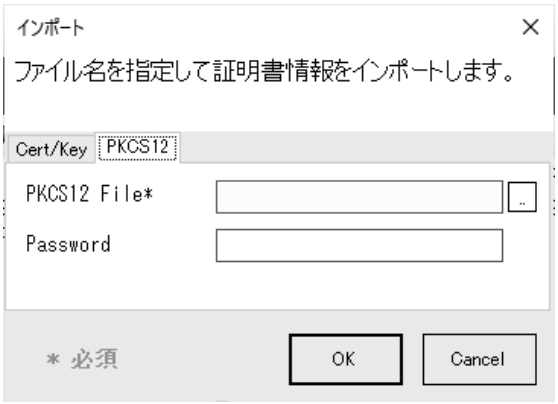


図 4.28　証明書のインポート（PKCS12 形式）

フォーマットは、PEM 形式（.crt、.key）と PKCS12 形式（.pfx、.p12）に対応しています。
ファイルを選択後【OK】ボタン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、当社ではお答えすることができません。
ご了承ください。

4.7. 認証局の再構築

内部認証局は LCA－RGP 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。
ただし、再構築が必要な場合は、メイン画面の【新規認証局】から行ってください。
認証局の再構築後は、OS・ブラウザへの認証局証明書登録が再度必要となります。

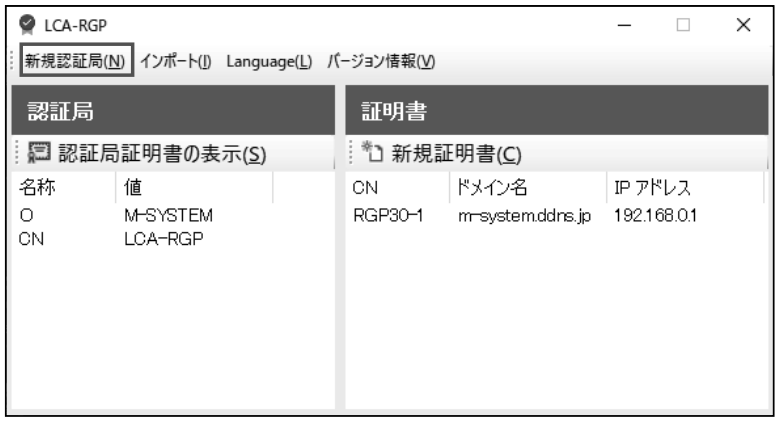


図 4.29　認証局の再構築

4.8. 表示言語の切替え

LCA－RGP 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－RGP を再起動すると画面の言語が切替わります。

図 4.30　表示言語の切替え

5. 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.