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-DL30**

目 次

1. はじめに ・・・・・・3
2. Web サーバ証明書概要······3
3. ローカル認証局(LCA-DL30)・・・・・・・・・・・・4
4. LCA-DL30 の使い方・・・・・5
 4.1. システム要件・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
5. ライセンス ・・・・・ 21

1.はじめに

DL30-Gバージョン 2.0 以降で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。

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-DL30)

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-DL30)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-DL30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-DL30 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-DL30 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-DL30 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-DL30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-DL30を用いると HTTPS に必要な身元確認を簡略化できます。LCA-DL30 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。

<mark>注意事項</mark> LCA-DL30 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。 DL30-G の HTTPS サーバおよび LCA-DL30 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。

4.1. システム要件

LCA-DL30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	下記 OS が動作する PC/AT 互換機	
OS	Windows10 32/64bit、Windows11 64bit	
OS 以外	DOT.NET Framework 4 以上	
メモリ	2 GB 以上	
ハードディスク	60 MB 以上	
空き容量	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

LCA-DL30 インストール後の初回起動時には、図 4.1 のダイアログが表示されますので、会社名等の組織名称を入力 してください。これが、LCA-DL30 内部認証局の組織名称になります。

ここでは例として、「M- TEM」と入力しています。【OK】ボタンをクリックすると図 4.2 の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ください。*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。

O: Organization Name x	
M-SYSTEM	lca X
会社名を入力してください。	O=M-SYSTEM CN=LCA-DL30
, ДЛЛуў; MESYSTEMICO.,LTD.	上記の設定で認証局を作成します。 よろしいですか?
ОК	OK キャンセル
図 4.1 Organization Name 画面	図 4.2 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-DL30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)

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-DL30 のメイン画面になります。

💡 LCA-DL30			- 🗆	×
新規認証局(<u>N</u>) インポート(<u>l</u>) Language(<u>L</u>) バージョン情報(<u>V</u>)			
認証局	証明書			
🖾 認証局証明書の表示(S)	1 新規証明	書(<u>C</u>)		
名称 値 O M-SYSTEM *2 CN LCA-DL30 *3	CN K	メイン名	IP アドレス	

図 4.3 メイン画面

- *2、一度新規作成して登録した認証局の組織名は変更できません。組織名の変更等により内部認証局の再設定が必要な場合は、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。
- * 3、「LCA-DL30」は表示のみで削除・変更はできません。

4.4. Web サーバ証明書の作成・転送

DL30-G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、DL30-GのIPアドレスまたはド メイン名を入力してください。

証明書情報編集	×
ドメイン名 m-system.ddns.jp	IP アドレス 192.168.0.1
追加 編集 削除 装置のドメイン名を入力します。 入力例:www.m-system.co.jp	追加 編集 削除 装置の IP アドレスを入力します。 (ループバックアドレスは自動的に登録されます) 入力例:192.168.0.1
CN DL30-G 装置名等を入力します。 入力例:DL30-G	OK

図 4.4 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 DL30-G 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 DL30-G 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。

置にファイルを転送します	ţ.			
	Network		O USB	
IP アドレス	192.168.0.1 ~	ポート		\sim
ポート (既定値: 30341)	30341			
- アカウント - フーザー				
ユーリー パスワード				
ОК				キャンセル

図 4.5 転送画面

DL30GCFG での設定データ転送時と同様、DL30-G に接続する方法を「Network」/「USB」から選択し、DL30-G 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。DL30-G への証明書転送を開始します。

LCA-DL30

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。DL30-G 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-DL30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。

💡 LCA-DL30)			_		×
新規認証局(<u>N</u>) インポート(<u>I</u>) Language(<u>L</u>)	バージョン情報(⊻)				
認証局		証明書				
: 🗐 認証局	品証明書の表示(<u>S</u>)	: 約 新規詞	正明書(<u>C</u>)			
名称 O CN	値 M-SYSTEM LCA-DL30	CN DL30-G	ドメイン名 m-system.ddns.jp	IP アドレ 192.168	<u>ノス</u> 3.0.1	

図 4.6 証明書情報

注意事項

DL30-G 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。

Web サーバ証明書の有効期限は証明書を転送してから 730 日(約2年)です。有効期限を過ぎるとブラウザは DL30-Gに HTTPS プロトコルで接続できません。有効期限が過ぎる前に定期的に Web サーバ証明書の再転送を行なってください。

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 DL30-G 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 DL30-G 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-DL30 からインストールする場合

4.5.2.1. Windows (Chrome, Edge)

① LCA-DL30 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。

68	証明書	×
全원	段 詳細 証明のパス	
	証明書の情報	
	この CA ルート証明書は信頼されていません。信頼を有効にするにはこの証	
	明書を信頼されたルート証明機関のストアにインストールしてください。	
	發行去・ ICA_DI30	
	有効期間 2019/09/13 から 2049/09/05	
	証明書のインストール(」) 発行者のステートメント(S)	
	ОК	

図 4.7 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ください。

÷	☞ 証明書のインポート ウィザード	×	
	証明書のインポート ウィザードの開始		
	このウィザードでは、証明書、証明書信頼リスト、および証明書失効リストをディスクから証明書ストアにコピー します。		
	証明機關によって発行された証明書は、ユーザーIDを確認し、データを保護したり、またはセキュリティで保護 されたネットワーク接続を提供するための情報を含んでいます。証明書ストアは、証明書が保管されるシステ ム上の領域です。		
	保存場所 ● 開左のユーザー(C) ○ ローカルコンピューター(L)		
	続行するには、「次へ」をクリックしてください。		
	次へ(<u>N</u>) キャンセル	١	

図 4.8 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 クしてください。

	×
←	
証明書ストア	
証明書ストアは、証明書が保管されるシステム上の領域です。	
Windows に証明書ストアを自動的に選択させるか、証明書の場所を指定することができます。	
○ 証明書の種類に基づいて、自動的に証明書ストアを選択する(山)	
 証明書をすべて次のストアに配置する(P) 	
証明書ストア:	
参照(<u>R</u>)	
次へ(<u>N</u>) キャンセ	μ

図 4.9 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 ンをクリックしてください。



図 4.10 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-DL30 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-DL30 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。

🛺 証明書		×
全般 詳細 証明のパス		
表示(5)・ マオバアト	~	
32/1/2/		
フィールド	値	^
🥅 パージョン	V3	
回 シリアル番号	00c686570b4f675f3b	
📴 署名アルゴリズム	sha256RSA	
🥅 署名ハッシュ アルゴリズム	sha256	
🌐 発行者	LCA-DL30, M-SYSTEM, Osak	
□ 有効期間の開始	2019年9月13日 14:36:44	
□ 有効期間の終了	2049年9月5日 14:36:44	
191919F	LCA-DL30, M-SYSTEM, Osak	~
1		
	プロパティの編集(E) ファイルにコピー	-(<u>C</u>)
		OK

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。

エクス	ボート ファイルの形式 さまざまなファイル形式で証明書をエクスボートできます。
	使用する形式を選択してください:
	O DER encoded binary X.509 (.CER)(<u>D</u>)
	Base 64 encoded X.509 (.CER)(S)
	〇 Cryptographic Message Syntax Standard - PKCS #7 証明書 (.P7B)(<u>C</u>)
	□ 証明のパスにある証明書を可能であればすべて含む(!)
	O Personal Information Exchange - PKCS #12 (.PFX)(P)
	□ 証明のパスにある証明書を可能であればすべて含む(U)
	□ 正しくエクスポートされたときは秘密キーを削除する(K)
	□ すべての拡張プロパティをエクスポートする(<u>A</u>)
	□ 証明書のプライパシーを有効にする(E)
	○ Microsoft シリアル化された証明書ストア (.SST)(<u>T</u>)

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。

		×
~	☞ 証明書のエクスポート ウィザード	
	エクスボートするファイル	
	エクフポーレオスコッノルの夕前をユカレアノださい	
	エノスホートするノナールの石前を入力してへんとい	
	フラノリック (5)。	
	ファイル/4(E): 参照(R)	
	₽ m(77)	
	次へ(N) キャンセ ル	,

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。

	33 M	I-Syste	em - '	Total Compone	ents X	+															
$\left(\boldsymbol{\leftarrow} \right)$	\rightarrow	G, i	ŵ		(i) 🖲	https:	/www. m	n-syste	₂m.co.jp	р					•••	⊚ 1	ን		II\ E	:	E
			5	and					-				-		1	ø	Sync にログイン				
					- 1	EAA		3	1				£		-	Ø	コンテンツブロッ	キング			標準
				Total Co	ompo tioners.	nents S	upplie	er foi	r PA/	/FA/	/ BA	~		~	3	□ ≈ ₽	新しいウィンドウ 新しいプライベー 以前のセッション	トウイン /を復う	ドウ 5	Ctrl+S	Ctrl+N hift+P
				Paperless Re	ecording	System, Ind	cators, E	lectric	Actuato	tors							ズーム	- (100%	+	4 2
														-			編集		ж	Ъ	Đ
				Select Yo 日本語 王内朝 中文 한국이 Copyright © 2011	our Lang 语 ish (简体) 어	quage 4-System.Co.,	td. Al rig	this rese	erved.				I KORA		#xtât	■ ** * * *	ブラウジングライ ログインとパスワ アドオン オブション カスタマイズ ファイルを聞く 名前を付けてべ 印刷 このページを検索 その他 ウェブ開発 ヘルプ	ブラリー -ド -ジを作	转	Ctrl+S	> hift+A Ctrl+O Ctrl+S Ctrl+F > >
																Ċ	終了			Ctrl+S	hift+Q

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。

	8	M-System - Total Compone	ents X 🕏 オブション X 🕇			-		Х
¢	\rightarrow	C' û	Sirefox about:preferences		☆	III\ 🗉	3	≡
				¥ م	プションを検索			^
	₽	一般	一般					
	۵	ホーム	起動					
	Q 4	検索 プライバシーとセキュリテ	 前回のセッションを復元する(S) ブラウザーを終了するときは確認する デイ Firefox が既定のプラウザーか確認する(Y) 					
	Ĵ	Sync	🥺 Firefox は既定のブラウザーに設定されていません	既	そこのブラウザーにする…(<u>(D</u>)		
			タブグループ					
			✓ Ctrl+Tab で最近使用した順にタブを切り替える(I)					
			✓ 新しいウィンドウではなく新しいタブに開く(W)					
			リンクを新しいタブで開いたとき、すぐにそのタブに切り替える(H)					
			タスクパーにタブのブレビューを表示する(K)					
			言語と外観					
	*	拡張機能とテーマ	フォントと配色					
	?	Firefox サポート	既定のフォント(D) 既定 (メイリオ) ・ サイズ(S)	16 🗸	詳細設定(<u>A</u>)			
					配色設定(C)			~

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。

🔣 M-System - Total Componer	is x 🛱 л7эву x 🕂				×
← → ♂ ☆	V Firefox about:preferences#privacy	☆	lii\ 🗊	٢	≡
	E	♀ オブションを検索			^
✿ 一般	証明書マネージャー	×			
ⓑ ^{肃−ム}	本なたの証明会 個人証明会 サーバー証明会 認証局証明表		詳細情報		
Q、検索					
🔒 プライバシーとセキュリ	認証局を識別するため以下の証明書が登録されています 証明書名と発行者名 セキュリティデバイス				
Sync	← AC Camerfirma S.A.				
	Chambers of Commerce Root - 2008 Builtin Object Token				
	Global Chambersign Root - 2008 Builtin Object Token				
	✓ AC Camerfirma SA CIF A82743287				
	Camerfirma Chambers of Commerce Root Builtin Object Token				
	Camerfirma Global Chambersign Root Builtin Object Token				
	~ ACCV				
	ACCVRAIZ1 Builtin Object Token				
	✓ Actalis S.p.A./03358520967				
	表示(<u>V</u>) 信頼性を設定(<u>E</u>) 1ンボート(<u>M</u>) エクスポート(<u>X</u>) 削除または信	言頼しない(<u>D</u>)…			
		ок	表示(C)		
▶ 拡張機能とテーマ			「バイス…(<u>D</u>)		
⑦ Firefox サポート					~

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。

● 認証局証明書を含むファイルを	選択してください				×			
← → × ↑ ≌ > PC >	← → 、 ↑ 🍰 > PC > □-カルディスク(C) > 、 、 び □-カルディスク							
整理 ▼ 新しいフォルダー		•	?					
🚔 F#1X7F 🛛 🖈 ^	名前 ^	更新日時	種類	サイズ	^			
📰 ピクチャ 🛛 🖈	BUFFALO	2019/01/16 19:13	ファイル フォルダー					
LCA-DL30	eclipse_Mars	2018/09/19 10:00	ファイル フォルダー					
試験仕様	Intel	2018/08/07 14:28	ファイル フォルダー					
試験仕様書	ISL Light Client	2018/08/07 13:28	ファイル フォルダー					
取説闡連	Jobs	2018/10/04 9:34	ファイル フォルダー					
	MSOCache	2018/08/07 13:44	ファイル フォルダー					
> OneDrive	PerfLogs	2018/04/12 8:38	ファイル フォルダー					
✓ ■ PC	PRJ	2019/08/07 9:52	ファイル フォルダー					
▲ 3D オブジェクト	Program Files	2019/09/09 16:06	ファイル フォルダー					
	Program Files (x86)	2019/07/25 13:50	ファイル フォルダー					
>	ProgramData	2019/09/12 17:15	ファイル フォルダー					
> 🔜 テスクトップ	Renesas	2018/10/11 10:55	ファイル フォルダー					
> 🛗 ドキュメント	temp	2019/09/05 16:22	ファイル フォルダー					
> 📰 ピクチャ	Tool	2019/02/19 9:32	ファイル フォルダー					
> 📕 ビデオ	VirtualBox	2019/07/31 12:30	ファイル フォルダー					
> <u>)</u> ミュージック	Windows	2019/08/29 15:14	ファイル フォルダー					
> #≙ ローカル ディフク (C	work	2019/06/04 11:56	ファイル フォルダー					
	- WorkSpace	2018/10/11 10:54	ファイル フォルダー					
 →…L□ h 	¬ +f	2010/02/12 17:47	7-71 7-11 8		· ·			
ファイル名	(<u>N</u>):		~ 証明書ファイル	/ (*.p7b;*.crt;*.cer	rt; ~			
			開く(<u>O</u>)	キャンセノ	IV .			

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。

証明書のインポート	×
新しい認証局 (CA) を信頼するよう求められています。本当にこの認証局を信頼しますか?	
"LCA-DL30" が行う認証のうち、信頼するものを選択してください。 ☑ この認証局によるウェブサイトの識別を信頼する □ この認証局によるメールユーザーの識別を信頼する	
認証局を信頼する場合はその目的に開わらず、認証局の証明者が間違いないこと、認証ポリシーや認証実施 規定に問題がないことを確認してください。	j
証明書を表示 認証局の証明書を審査してください	
OK キャンセル	

図 4.19 Firefox 証明書のインポート画面

⑩これで、LCA-DL30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)

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. DL30-G からインストールする場合

DL30-GのWEBのプロトコルをHTTPSに設定してから以降の操作を行ってください。

4.5.4.1. Windows (Chrome, Edge, FireFox)

 LCA-DL30 で証明書を作成し転送した場合、DL30-G に HTTP 接続を行いダウンロードします。 「http://<DL30G-IP アドレス >」を入力すると認証局証明書ファイル (cacert.crt)がダウンロードされます。ダウンロー ド後は、16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。

4.5.4.2. iOS (Safari)

① LCA-DL30 で証明書を作成し転送した場合、DL30-G に HTTP 接続を行いダウンロードします。

「http://<DL30G-IP アドレス >」を入力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 4.20 iOS 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。

10:33 9月13日(金)		🗢 100% 🔳
	一般	
設定	アクセシビリティ	>
Q. 検索		
	本体値のスイッナの機能:	
	画面の向きをロック	~
Ipad A1474	消音	
Apple ID、iCloud、iTunes Storeと	コントロールセンターから消音にできます。	
2ファクタ認証を有効にする 1 >	iPadストレージ	>
	Appのパックグラウンド更新	>
iPadの設定を完了する 🚺 >		
プロファイルがダウンロードされ… >	日付と時刻	>
	キーボード	>
	言語と地域	>
Wi-Fi aterm-8c075f-g	辞書	>
* Bluetooth オン		
	iTunes WiaFi同期	
通知		
🔊 サウンド	VPN	未接続 >
おやすみモード	プロファイル	3 >
X99-291X	認証	>
O -A	リセット	>
🔋 コントロールセンター	システム終了	
AA 画面表示と明るさ		

図 4.21 iOS 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ください。

10:36 9月13日(金)				
		く一般	プロファイル	
設定		ダウンロード済みプロファ		
Q. 検索		LCA-DL30		
			_	
	キャンセル プロ	コファイルをインストール	インストール	
Арр				
2ファクタ認証	LCA-DL30			
iPadの設定を				
	普泊吉 LCA-DL30 未検証			
フロファイル;	内容 証明書:1			
	詳細		>	
▶ 機内モ-				
🛜 Wi-Fi	ダウンロ	コード済みプロファイルを削	除	
Bluetoc				
(1) 通知				
じ おやする				
🛛 スクリー	271A			
〇 一般				
םאעב 🕄	ールセンター			
▲ 画面表示	と明るさ			

図 4.22 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。

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、ダウンロードした認証局証明書を開きます。

≈ ⊻ <u>₩</u> h	A ≥ 4	92.168.1	13.10/9	gantt. × +		2		11:04
÷	\rightarrow	C		192.168.13.10/gantt.html	2	22	ŧ	:
	0000	rt art [間7	1				~
×	cacer		囲く	J				^

図 4.23 Android cacert.crt を開く画面

②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。

⊚⊻ д ⊭∆		逸 📖 11:05
証明書インスト	-ラ-	
	証明書の名前を指定する	
	証明書名	
	次按律规办使用	
	Wi-Fi O	
	この証明書の発行者は、ご利用の端末における送受信 トラフィックをすべて検査する場合があります。	
	パッケージの内容:CA証明書	
	キャンセル OK	

図 4.24 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-DL30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-DL30を経由して証明書ファイルと秘密鍵ファイルを DL30-G 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。

インポート ×	インポート ×
ファイル名を指定して証明書情報をインポートします。	ファイル名を指定して証明書情報をインポートします。
Cert/Key PKCS12 Unit Certificate*	Cert/Key PKCS12 PKCS12 File*
* 必須 OK Cancel	* 必須 OK Cancel
図 4.25 証明書のインポート(DER 形式)	図 4.26 証明書のインポート(PKCS12 形式)

フォーマットは、DER 形式(.crt、.key、.der)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-DL30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。

💡 LCA-DL30)				-		×
… 新規認証局(<u>N</u>) インポート(J) Language(<u>L</u>) バージョン情報(<u>V</u>)							
認証局			証明書				
: 🗐 認証局	局証明書の表示(<u>S</u>)		🗄 新規訂	[明書 <mark>(C</mark>)			
名称 O CN	値 M - SYSTEM LCA-DL30		CN DL30-G	ドメイン名 m-system.ddns.jp	IP 가 192.1	[×] レス 68.0.1	

図 4.27 認証局の再構築

4.8. 表示言語の切替え

LCA-DL30 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-DL30を再起動すると画面の言語が切替わります。

💡 LCA-DL30	l.				- [Х
新規認証局(<u>N</u>) インポート(J) Language(<u>L</u>) パージョン情報(<u>V</u>)							
認証局			証明書				
🗐 認証局	品証明書の表示 <mark>(S)</mark>		🏻 1 新規訂	E明書 <mark>(C)</mark>			
名称 O CN	値 M - SYSTEM LCA-DL30		CN DL30-G	ドメイン名 m-system.ddns.jp	IP アドレ: 192.168.0	ર 0.1	Í

図 4.28 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.