ログイン時の画面について





長崎県電子入札システム WEBサーバ 証明書入れ替えのお知らせ

長崎県電子入札システムではWEBサーバ証明書の入替えを行いました。 インストールがされていない場合は接続確認画面が表示されます。(P1の上図参照) 以下手順を参考にインストール作業を行ってください。



1. パソコンにインストールする自己署名証明書のダウンロード

※自己署名証明書をインストールする必要があるパソコンは電子入札システムを 利用するパソコンのみとなります。 アプリケーションCA G4 の自己署名証明書をダウンロードします。 下記URLにアクセスしダウンロードを行ってください。

【ダウンロードサイト(外部リンク)】 https://www.lgpki.jp/CAInfo/install.htm

(1)ダウンロードサイトにアクセスします。(アクセス先の画面です。)



(2)対象の証明書をダウンロードします。

①「LGPKIにおけるアプリケーションCA G4 Rootの自己署名証明書ダウン ロード」が表示されていることを確認します。



「AppCAG4Root.cer」ファイルを任意の場所へ保存します。

A REAL PROPERTY AND A REAL		×
C () () () () () () () () (↑ ★	Ø
ファイル(E) 編集(E) 表示(Y) お気に入り(A) ツール(I) ヘルプ(H)		
		~
	×	
	~	
整理 ▼ 新しいフォルダー 二部 ● (0	
▲ 🚖 お気に入り		
▲ 😭 ライブラリ		
▶) ミュージック		
·		
ファイル名(<u>N</u>): AppCAG4Root.cer	-	
ノアイルの/理境(上): ビキュリティ証明書 (*.cer)		
	_	
● フォルダーの非表示 保存(S) キャンセル		
LGPKIにおけるアブリケーションCA G4 Subの下位CA証明書ダウンロード		
LGPKIにおけるWEBサーバ証明書等を発行する アブリケーションCA G4 Sub (第四世代) の下位CA証明書です。		
- インストール方法について		
証明書のインストール方法は、使用するアプリケーションによって異なりますので、 インストール方法につきましては、ブラウザ等のアプリケーション提供示へお問い合		
わせください。		

これで、ダウンロードは完了です。 2.フィンガープリントの確認(P6)へお進みください。

2. フィンガープリントの確認(印刷またはメモ帳等に控えておきます)

 (1) "1. パソコンにインストールする自己署名証明書のダウンロード"で 証明書ファイルをダウンロードしたサイトです。(P1参照) このページの
 「■LGPKIアプリケーション認証局自己署名証明書のフィンガープリント について」のフィンガープリント一覧をクリックします。

and a second sec		x
(↑ ★	¢.
ファイル(E) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)		
 GDK/ICおける白戸粟夕証明書		
■ ダウンロードについて		
LGPKIでは、次の自己署名証明書を公開しております。		
L <u>GPKIにおけるブリッジCAの自己署名証明書ダウンロード</u> LOPKIDに発行さわた弊書証明書のトラフトマンカー(信頼ら)であるブリッジ		
フリッシCAは、半 <mark>球26年9月13日</mark> にCA鍵へアの更新を実施し、 <mark>新暗号</mark> の新し いCA鍵へアにより発行した自己署名証明書です。		
CA鍵ベア更新前の自己署名証明書は <u>こちら</u>		
LGPKIにおける組織CAへの中間CA証明書ダウンロード		
中間CA証明書は、LGPKIから発行されたブリッジCAから組織CAへの相互認 証証明書で、新時号でのCA鍵々での再新に代し、平時20年1月13日(新し		
CA鍵ペア更新則の中間CA語出明書は <u>こちら</u>		
LGPKIにおけるアプリケーションCA G3 Rootの自己署名証明書ダウンロード		
LGPKILのいる自己者名証明書及び下位のA証明書を発行するアプリー ションCA G3 Root(第三世代)の自己署名証明書です。		
」の以口におけるアプリケーションへん なっ ちょの下位でん 証明まなか ンロード		
LGPKIにおけるWEBサーバ証明書等を発行するアプリケーションCA G3 Sub		
(第二世代)の下位CA証明書です。		
LGPKIにおけるアプリケーションCA G4 Rootの自己署名証明書ダウンロード		
LGPKILのいる日に者名証明書及び下位のA証明書を発行するアプアー ションCA G4 Root(第四世代)の自己署名証明書です。		
0.00/1におけるアブリケーションへん 0.4 Sukの下位へが明明実がウンロード		
LGPKIにおけるWEBサーバ証明書等を発行するアプリケーションCA G4 Sub		
(第四世代)の下位CA証明書です。		
■ インストール方法について 評明書のインストール方法は、使用するアプリケーションによって異なりますので		
インストール方法につきましては、ブラウザ等のアブリケーション提供元へお問い合		
- LOPKIアブリケーション認証局白フ署名証明書のフィンガーブリントについて		
自己署名証明書をインストールする際には、自己署名証明書が改ざんされていな		
コールファーフリンドー見ーないに1000120フィンパーフリンドに作り通びです。1000年10001日 コの表任においてイン		
ハームハーンのはいい地力公共回降雨秋ンステム機柄(J-US)のハームハーンの <u>フィンガーブリント一覧</u> においても確認できます。		
		\checkmark
	100%	
	af 100%	

(2) LGPKIにおけるフィンガープリント一覧が表示されます。



3. 自己署名証明書のインストール及び目的の設定

(1) ダウンロードしたファイルをダブルクリックします。



左図は「AppCAG4Root.cer」となっていますが パソコン設定により「.cer」が表示されない場合が あります。

(2) 証明書 が開きます。下部にある【証明書のインストール】ボタンを押下します。

証明		
全	般 詳細 証明のパス	
	証明書の情報	
	この証明書の目的: ・データが現在の時刻で署名できるようにする ・電子メールを保護する ・ソフトウェアがソフトウェア発行者の送信であるか確認する ・公開後のソフトウェアの変更を禁止する	
	発行先: Application CA G4 Root	
	発行者: Application CA G4 Root	
	有効期間 2017/02/16 から 2037/02/15	
	正明書のインストール(D 発行者のステートメント(S) 正明書の詳細について表示します。	
	ОК	

(3)証明書のインポートウィザードが表示されます。【次へ】ボタンを押下します。

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。	
	証明機関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。	
	続行するには、D欠へ]をクリックしてください。	
	< 戻る(B) (XA(N)) キャンセル	

(4)「証明書をすべて次のストアに配置する」を選択し【参照】ボタンを押下します。

証明書のインポート ウィザード
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(U) ◎ 証明書をすべて大のストア(ご配置する(P))
計四月書人下/?: 参照(<u>R</u>)
<u>証明書ストアの詳細を表示します</u>
< 戻る(B) 次へ(N) > キャンセル

(5)証明書ストアの選択 画面が開きます。 「信頼されたルート証明機関」を選択し、【OK】ボタンを押下します。



(6) 証明書ストア 欄に「信頼されたルート証明機関」と表示されていることを確認し 【次へ】ボタンを押下します。



(7) 完了画面が表示されます。表示されている内容を確認し 【完了】ボタンを押下します。

証明書のインポート ウィサ	β β
	証明書のインポート ウィザードの完了
	[完了] をクリックすると、証明書がインポートされます。
	次の設定が指定されました: ユーザーが選択した証明書ストア 信頼されたルート証明機関 内容 証明書
	 ユーザーが選択した証明書ストア 信頼されたルート証明機関 内容 …明書 と表示されていることを確認。
	(反る(日) 完了 キャンセル
セキュリティ警告 発行者が次であると主き ルしようとしています: Application CA G4 Ro 証明書が実際に "Applic を検証できません。"A 窓する必要があります。 拇印 (sha1): 21DACE4 A89D4C1D 警告: このルート証明書をインストールする。 クリックすると、このが この証明書をインストー この証明書をインストー	を考 な な な な な な な な の の の の た の と 、 この CA に た い に な た な い な い な い な い な い な い な い な い な い
	(まし)(Y) ししえ(N)

(8) インポートされました。【OK】ボタンを押下します。



証明書のインストールは完了です。 【OK】ボタンを押下します。 次は証明書の目的の設定を行います。 (9)へお進みください。 (9)証明書の目的の設定及びフィンガーを行います。 Internet Explorer を開き、インターネットオプションを開きます。

※ Internet Explorerを開く際は必ず「管理者として実行」を行ってください。



(10)「管理者として実行」でインターネットを開いたら 「ツール」→「インターネットオプション」の順で開きます。



(11)インターネットオプションが開きます。「コンテンツ」タブを選択し 【証明書】ボタンを押下します。



(12)証明書 画面が開きます。

- ①「信頼されたルート証明機関」タブを選択します。
- ② 発行先の欄に表示された「Application CA G4 Root」を選択します。
- ③【表示】ボタンを押下します。

II	明				×
Γ	١	的(N): <<すべて>	(1)		•
	ſ	1人 (ほかの人)中間証明機関 (言頼されたル	ート証明機関 信頼された	発行元 信頼さ	れない発行元
		発行先	発行者	有効期限	フレンドリ名 🔺
		🔄 ANCERT Certificados Notariales V2	ANCERT Certificados	2030/05/26	ANCERT (
		🔄 ANCERT Corporaciones de Derecho Pu	ANCERT Corporacion	2024/02/12	ANCERT (
		🔄 ANF Server CA	ANF Server CA	2021/12/01	ANF AC
(2)	🔄 Application CA G2	Application CA G2	2016/03/31	Japan Loc
		En Application CA 20 Pool	Application Of Go R	2004/00/00	(141)
		🙀 Application CA G4 Root	Application CA G4 R	2037/02/15	<なし>
		ApplicationCA	ApplicationCA	2017/12/13	Jananese
					•
		インポート(D) [エクスポート(E)] 削除(F	0		詳細設定(A)
		明書の目的			
	<	(すべて)			
				3	表示(V)
	11	明書の詳細について表示します。			開じる(C)

(13)「詳細」タブを選択し、下部にある【プロパティの編集】ボタンを クリックします。

ſ	2.50 IFAII IFAIIII IFAII IFAIII	•	※注意事項 Internet F	i※ Fxplorerを「管理者と
	フィールド 第バージョン シリアル番号 第名アルゴリズム 第名スパッシュアルゴリズム	値 V3 31 a5 f3 ca 90 ea 23 ac d2 9 sha256RSA sha256	して実行」 【プロパテ ことがあり 開けなかっ し起動しな	で起動しなかった場合 マの編集】が開けない ます。 た場合はP11を参照 おして下さい。
	 第行者 有効期間の開始 有効期間の終了 	Application CA G4 Prot. LGF 2017年2月16日 200:00 2037年2月15日 23:59:59	-	
			2011年1月11日1日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日	「プロパティの編集(E)」 マ ァイルにコピー(C) 」 こ
	証明書の詳細とついて表示します。	ブロパティの編集(E)	⊐ピー(©	
		(OK	14

(14)「全般」タブの証明書の目的を下記のように設定し【OK】ボタンを押下します。

証明書のプロパティ	
全般 クロス調理書 OCSP EV (Extended Validation)	
フレンドリ名(E):	
	,
証明書の目的(U) 「の次の目的にけを有効にする」にチェックする)°
○この証明者の目的をすべて無効にする(2)	
 ◎ 次の目的だけを有効にする(Q) 	
/注意・証明の/ハスと計判された証明者の目的のが編集できない場合があります。 す。	
●サーバー認証	
□ 0-71/2018200 □ 1-F署名 □ 1-F署名 □ 1-F署名	
⑦ 電子メールの保護 ■電子メールの保護 ■ 電子メールの保護 ■ ロイムフロンプ	
□ Microsoft 信頼) ストの署名 以上、4項目にチェックをする。	
Microsoft & 1 & 2827	
目的の追加(巴)	
証明書のプロパティの詳細を表示します。	
OK 適用(<u>A</u>)	

- (15) 画面が「詳細」タブに戻ります。そのまま拇印(フィンガープリント)の 確認を行います。
 - スクロールバーを下へおろします。
 - ②「拇印」を選択しフィンガープリントの確認をします。
 - ③ 確認が終わったら【OK】ボタンを押下します。

		証明書		×	
	全般 詳細 証明のパ 表示(S): <すべて> フィールド	2 (D
. [6e dc 0a 35 1f 20 c KeyID=6e dc 0a 35 Certificate Signing, Subject Type=CA, Jud 21 da ce 4c 2c 34 e			
2	21 da ce 4c 2c 34 e6	54 68 ee 06 31 4d b0 55 a(♥ a8 9d 4c 1d] •	P6 [2 フィンガー
		プロパティの編集(E).	ファイルにコピー(<u>C</u>)		リントの確認」をご確認 ださい※
			Зок		15

(15) 画面が証明書一覧に戻ります。画面下部にある「証明書の目的」欄に設定した とおりに表示されていることを確認し【閉じる】ボタンを押下する。

副人 ほかの人 中間証明機関 信頼されたル	ート証明機関(信頼された	発行元 信頼さ	れない発行元
発行先	発行者	有効期限	フレンドリ名 ^
Application CA G2	Application CA G2 Application CA G3 B	2016/03/31	Japan Loc
Application CA G4 Root	Application CA G4 R	2037/02/15	(ない)
ApplicationCA2 Root	ApplicationCA2 Root Arge Daten Oesterrei ATHEX Root CA	2033/03/13 2009/02/12 2030/10/18	GPKI Appl Austrian S Athex Roo 🚽
インボート(D_ 」 [エクスボート(E)_] 削除(F	0		』詳細』设定(A
=0月音の日回り 2イム スタンプ、電子メールの保護、コード署名、サー	-//-1211E		表示(V)
四書 キニします。			開じる(C)

インターネット オプション	? 🗙
全般 セキュリティ ブライバシー コンテンツ 接続 プログラム 詳細設定 ファミリー セーフティ	
閲覧できるインターネットのコンテンツを指 ファミリー セーフティ(F 定します。	:)
証明書	
暗号化された接続と識別のための証明書を設定します。	
SSL 状態のクリア(S) 証明書(C) 発行元(B)	
オートコンプリート	
オートコンプリートによって、Web ページで前回 入力した内容を、入力中に補完できます。	
フィードと Web スライス	
フィードと Web スライスは、Web サイトの更新 されたコンテンツを Internet Explorer やその 他のプログラムで表示します。	
	商用(<u>A</u>)



※ " 1. パソコンにインストールする自己署名証明書のダウンロード" でインストールした証明書ファイルは削除してください。



インストール作業は完了です。開いているブラウザを全て閉じログインしてください。 ご協力ありがとうございました。

ログインボタン押下後、下記のように画面が表示されればインストールは正常に 行われています。

