

## JKK東京(東京都住宅供給公社) 電子入札システムの操作手順について ~1. クライアント証明書(電子証明書)インポート編~

## 令和6年1月

JKK東京(東京都住宅供給公社)





1. クライアント証明書は1年に1回更新が必要です	P.2~
2. クライアント証明書をダウンロード ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	P.3~
3. クライアント証明書のインポート ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	P.7~
4. クライアント証明書のインポート(別の手順) ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	P.12~
5. 電子入札システムへのログインを試す(クライアント証明書によるアクセス)・・	P.20~
その他 旧クライアント証明書を削除する方法 困った時は・・・ 事象1 事象2 クライアント証明書が正しくインポートされているかの確認方法	P.25~ P.26 P.30~ P.31 P.34 P.35
解決しない場合は	P.39

#### 【利用しているパソコンの環境】

下記以外の環境は、サポート及び問合せの対象外です

- (1) Windows8.1(日本語版)/Chrome
- (2) Windows10(日本語版、64bit版)/Chrome

Internet Explorer11は、2022年06月にMicrosoft社のサポートが終了しました。 このため、電子入札システムの利用推奨ブラウザは、Chromeとなります。

## 1. クライアント証明書は1年に1回更新が必要です



※電子入札システムは、本システム専用のクライアント証明書がないとログイン画面が表示されません。 (クライアント証明書とは、電子入札システムを利用するユーザーの信用性を保証する電子証明書のことです)

※クライアント証明書の有効期間は、4/1~翌年3/31までの1年間です。 このため、クライアント証明書は毎年入れ替え作業が必要になります。

※クライアント証明書の入れ替え期間は、毎年1月中旬~3月末です。

クライアント証明書の準備が整い次第、対象の事業者には、登録されているメールアドレス宛に、

「更新のお知らせ」メールを送信します。

(特に、委託業者の場合は、3年に一度の更新情報が整い次第、「更新のお知らせ」メールを送信しますので、 タイミングは変動します)

なお、更新忘れ防止のために、「更新のお知らせ」メールは1月中旬~3月末の間、数回送付いたします。 すでにその年のクライアント証明書の入れ替え作業を実施済みの場合は、2回目以降のメールは無視してください。

※本手順は、クライアント証明書の更新、新規登録のどちらも同じ手順となります。

※この作業は、パソコンにログインしているユーザは管理者権限(クライアント証明書の登録可能な権限)で行ってください。 ※インストールする台数に制限はありません。



(1)クライアント証明書の「更新のお知らせ」メールを確認してください。

件名:【電子入札システム】更新のお知らせ
内容: 電子入札システムのクライアント証明書を発行しました。 以下のサイトからクライアント証明書をダウンロードして、 電子入札システムを利用するパソコンにインポート(登録)してください。
インポートしない場合、XXXX/4/1から電子入札システムにアクセスできなくなりますので ご注意ください。 ※本メールは年度内に複数回、自動送信しています。 すでにXXXX年度用の電子入札システムのクライアント証明書をインポート済の方は、 このメールは無視してください。
https://e-bid.to-kousya.or.jp/XXXXXXXXXX

※メールは、JKK東京の入札参加申請で登録 しているメールアドレス宛に送付します。 ※登録メールアドレスの変更が必要な場合は、 変更手続きを行うようお願いいたします。

#### (2)メール内に記載されているURLをコピーし、



を開いて、アクセスしてください。

Det.(6Leboth) JKK東京	
電子入札システムを利用するためのクライアント証明書取得のために ワンタイム/(スワードを発行してください。 電子入札システムの「ログインID」「/(スワード」を入力し、 ワンタイム/(スワード発行ボタンを押してください。 ログインID: 	
重子入札システムのパスワードを忘れた方はこちら	

「クライアント証明書ダウンロードのワンタイムパスワード 発行」画面が開きます。 電子入札システムのログインID及びパスワードを入力し、 [ワンタイムパスワード発行]ボタンをクリックします。



(3)「クライアント証明書ダウンロード画面」が開きます。 本画面は閉じずに、メールを確認してください。

DEE.(GLEBOTR) JKK東京
この画面は閉じずに、メールを確認してください。
クライアント証明書ダウンロード用のワンタイムパスワードを 登録添みのメールアドレスに送信しました。 メールに記載されているワンタイムパスワードを入力して、 クライアント証明書ダウンロードボタンを押してください。 クライアント証明書がダウンロードできるようになります。
ワンタイムパスワード:
電子入札システムにアクセスするためには、クライアント証明書が必要です。 ダウンロードしたクライアント証明書を電子入札システムを使うハンコンにインボート(登録)してください。 インボート手順は「クライアント証明書インボート手順書」を参照してください。 クライアント証明書インボート手順書
クライアント証明書をダウンロードしたらこの画面は閉じてください。
間じる

(4)クライアント証明書の「更新用ワンタイムパスワードのお知らせ」メールが送付されます。

件名:【電子入札システム】更新用ワンタイムパスワードのお知らせ 内容: 電子入札システムのクライアント証明書をダウンロードするために、 以下のワンタイムパスワードを画面に入力してください。 入力すると、クライアント証明書のダウンロードが可能になります。 ワンタイムパスワード:XXXXXXX 有効期限:XXX/XX/XX XX:XX

※メールは、JKK東京の入札参加申請で登録 しているメールアドレス宛に送付します。 ※ワンタイムパスワードの有効期限が経過し 無効となった場合は、再度クライアント証明書 の案内メールからワンタイムパスワードを発行 してください。

※ワンタイムパスワードには、有効期限があります。期限内に次の操作を行ってください。

本メールに記載されている「ワンタイムパスワード」を

上記の画面の「ワンタイムパスワード」欄に入力し、[クライアント証明書ダウンロード]ボタンをクリックします。



(5)画面下部に、クライアント証明書のダウンロードが表示されますので、 自分のパソコンの「ダウンロード」フォルダにクライアント証明書をダウンロード(保存)します。 クライアント証明書をダウンロード(保存)したら、閉じるボタンをクリックして、本画面は閉じてください。



※ブラウザによっては、ダウンロードしたクライアント証明書は、画面上部に表示される場合もあります。





#### この場合は、ダウンロードフォルダにクライアント証明書が保存されている状態になりますので、 そのまま閉じるボタンをクリックして画面を閉じ、次の手順に進んでください。

💺   🛃 📙 🗢   ダウンロード				- 0	×
ファイル ホーム 共有 易	<del>【</del> 示				~ ?
← → ~ ↑ 🕹 > PC > ダ	ウンロ−ド		✓ Ö  ✓ ダウンロード	の検索	
<u></u> 3D オブジェクト	▲ 名前		更新日時	~ 種類	ť
↓ ダウンロード	> 5 B (1)	x	2021/11/25 11:28	Personal Informati.	
					Ŷ
ID6 個の項目 1 個の項目を選択	<b>∀</b> <				> 

3. クライアント証明書のインポート



※この手順がうまくいかなかった場合は、12ページの「4. クライアント証明書のインポート(別の手順)」を確認してください。

(1)ダウンロードしたクライアント証明書(拡張子が.pfxのファイル)をダブルクリックします。



(2)「次へ」ボタンをクリックします

←   夢 証明書のインボート 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。	
保存場所 ● 現在のユーザ−(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(N) キャンセ)	IL I
	<ul> <li>✓ ジ 証明書のインボートウィザードの開始</li> <li>このウィザードでは、証明書、証明書信頼リスト、および証明書大効リストをディスクから証明書ストアにコピーします。</li> <li>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ています。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。</li> <li>保存場所         <ul> <li>● 現在のユーザー(C)</li> <li>● ローカル コンピューター(L)</li> </ul> </li> <li>続行するには、[次へ]をクリックしてください。</li> <li>次へ(N) キャンセ/</li> </ul>



(3)「次へ」ボタンをクリックします。

€ 3	F 証明書のインボートウィザード
	インポートする証明書ファイル
	インポートするファイルを指定してください。
	ファイル名(F): <u> </u>
	注意:次の形式を使うと1つのファイルに複数の証明書を保管できます:
	Personal Information Exchange- PKCS #12 (.PFX,.P12)
	Cryptographic Message Syntax Standard- PKCS #7 証明會 (.P7B)
	Microsoft シリアル化された証明書ストア (.SST)



## (4)「パスワード」欄にインポートパスワードを入力します。「次へ」ボタンをクリックします。 ※パスワードは「jkkCT333」です。

← 🐶 証明書のインポート ウィザード	×
秘密キーの保護 セキュリティを維持するために、秘密キーはパスワードで保護されています。	
秘密キーのパスワードを入力してください。	
- パスワード(P): 「jkkCT:	333」を入力
□ パスワードの表示(D)	
<ul> <li>インポートオプション(I):</li> <li>□ 秘密キーの保護を強力にする(E) このオプションを有効にすると、秘密キーがアプリケーションで使われるたびに確認を求められます。</li> </ul>	
□ このキーをエクスポート可能にする(M) キーのバックアップやトランスポートを可能にします。	
○ 仮想化ベースのセキュリティを使用して秘密キーを保護する(エクスポート不可)(P)	
☑ すべての拡張プロパティを含める(A)	
次へ(N) キャンセル	



(5)「証明書を全て次のストアに配置する」を選択します。 「参照」ボタンをクリックし、「証明書ストア」欄に「個人」を選択します。

「次へ」ボタンをクリックします。





(6)「完了」ボタンをクリックします。

Ļ	🍜 証明書のインボート ウィザード		×
	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	インボートされます。	
	次の設定が指定されました:		
	ユーサーが選択した証明書ストア 内容	個人 DFX	
	ファイル名	Ci¥Users¥ciana a client(	
	<		
		完了(F) キャンセ	μ

### (7)「OK」ボタンをクリックします。



<u>この画面が出たら、クライアント証明書のインストールは完了です。</u> 20ページの「5. 電子入札システムへのログインを試す(クライアント証明書 によるアクセス)に進んでください。

※この手順で、クライアント証明書がインストールできなかった場合は、 次ページ「4. クライアント証明書のインポート(別の手順)」を確認してください。



前述(3. クライアント証明書のインポート)の手順でうまくいかなかった場合は、以下の手順でインストールしてください。

ダウンロードしたクライアント証明書は、以下の手順でインポートしてください。

(1) Chrome (Google Chrome)
 起動します。
 右上のGoogle Chromeの設定→「設定」
 を選択します。



#### (2)「プライバシーとセキュリティ」を選択します。





#### (3)「セキュリティ」を選択します。

(4)「証明書の管理」(もしくは 「デバイス証明書の管理」)を選択します。



	v	- 🗆 ×
$\leftarrow$ $\rightarrow$ $C$ $\odot$ Chrome   chrome://settin	s/security	\$ <b>* *</b> :
設定	Q、設定項目を検索	
▲ Googleの設定 自動1カ	Chrome では、定期的にパスワードをオンライン上の公開リストと照合し、確認しています。 その際、パスワードとユーザー名は Google を含め離も読み取ることができないよう暗号化さ れます。この機能は Google アカウントにログインすると有効になります。	
	保護なし(推員されません) ○ 危険なウェブサイト、ダウンロード、拡張機能から保護されていません。セーフブラウジングによる保 譲は、Gmal や Google 検索など他の Google サービスで利用可能な場合は、引き続き有効です。	
<ul> <li>Q、検索エンジン</li> <li>回、既定のブラウザ</li> <li>(1) お物時</li> </ul>	詳細設定 常に安全な接続を使用する 波給生を HTTPS (「アップグリード」, HTTPS をサポート」、ていないサイトは読み込む前に警告を実	
詳細設定 •		
拡張機能 🖸 Chrome について	証明書の管理 HTTPS / SSL の証明書と設定を管理します	1
	Google の高度な保護領統プログラム 個人の Google アカウントを標約型双駆から保護します	



(5)「個人」タブを選択します。「インポート」ボタンをクリックします。

証明書							
目的(N):		<ট\\(\(\)					
個人	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		
				2120/03/1 2020/09/0 2028/04/0	6 <なし> 7 <なし> 1 <なし>		
インポート	(I) 目的	エクスポート(E)	削除(R)			詳細設定(A	4)
暗号化フ	ァイル シス	ŦĿ				表示(V)	
						閉じる(C)	)



(6)「次へ」ボタンをクリックします。

÷	☞ 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、[次へ] をクリックしてください。		
	次へ(N) キャンセノ		



(7)「参照」ボタンをクリックし、さきほどクライアント証明書をダウンロードした「ダウンロード」フォルダを開いてください。 「すべてのファイル」を選択してください。

「ファイル名」欄にダウンロードしたクライアント証明書(拡張子が.pfxのファイル)を選択します。

※自分のパソコンが拡張子を表示しない設定の場合は、ファイル名の最後が「\_cert」のファイルであることを確認してください。

		~
	← → ~ ↑ ↓ > PC > ダウンロード	<ul> <li>✔ ダウンロードの検索</li> </ul>
	整理 ▼ 新しいフォルダー	III - 🔟 🕐
	✓ ★ クイック アクセス <sup>▲</sup> 名前	更新日時 ~ ^
証明書のインボート ウィザード	<ul> <li>デスクトップ</li> </ul>	_cert.pfx
		(「すべてのファイル」を選択
インボートする証明書ファイル		
インボートするファイルを指定してください。	ファイル名(N):	
		開く(O) キャンセル
ファイル-名(ド):		
CiVUsersVel	● III(R)	
When you are additional additional additional additional additional additional additional additional and a second additional addit		
注意:次の形式を使うと1つのファイルに複数の証明書を	· #まちで苦泉	
Personal Information Exchange- PKCS #12 (.PFX,	P12)	
Cryptographic Message Syntax Standard- PKCS #	7 証明書 (.P78)	
Microsoft シリアル化された証明書ストア (.SST)		
	次へ(N) キャンセル	

「次へ」ボタンをクリックします。



## (8)「パスワード」欄にインポートパスワードを入力します。「次へ」ボタンをクリックします。 ※パスワードは「jkkCT333」です。

÷	≫ 証明書のインポート ウィザード	
	秘密キーの保護 セキュリティを維持するために、秘密キーはパスワードで保護されています。	
	秘密キーのパスワードを入力してください。	
	「パスワード(P): 「jkkCT333」を	专入力
	□ パスワードの表示(D)	
	<ul> <li>インポートオブション(I):</li> <li>□ 秘密キーの保護を強力にする(E) このオプションを有効にすると、秘密キーがアプリケーションで使われるたびに確認を求められます。</li> </ul>	
	<ul> <li>このキーをエクスポート可能にする(M)</li> <li>キーのバックアップやトランスポートを可能にします。</li> </ul>	
	<ul> <li>□ 仮想化ペースのセキュリティを使用して秘密キーを保護する(エクスポート不可)(P)</li> <li>☑ すべての拡張プロパティを含める(A)</li> </ul>	
	次へ(N) キャンセル	



(9)「証明書を全て次のストアに配置する」が選択されていること、 「証明書ストア」欄に「個人」が選択されていることを確認します。

「次へ」ボタンをクリックします。

÷	☞ 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)	
	<ul> <li>         ・証明書をすべて次のストアに配置する(P)         証明書ストア:         個人         </li> </ul>	
	次へ(N) キャンセ)	ŀ



#### (10)「完了」ボタンをクリックします。

÷	夢 証明書のインボートウィザード			×
	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	「インボートされます。		
	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	個人		7
	内容	PFX	Sector and the sector of the s	
	c		>	
			完了(F) キャン	セル

## (11)「OK」ボタンをクリックします。



<u>この画面が出たら、クライアント証明書のインストールは完了です。</u> 20ページの「5. 電子入札システムへのログインを試す(クライアント証明書 によるアクセス)に進んでください。 5. 電子入札システムへのログインを試す (クライアント証明書によるアクセス) (1)JKK東京ホームページ(入札・契約情報)にChrome(Google Chrome)  $\mathbf{P}$ でアクセスします。 Google Chrom https://www.to-kousya.or.jp/keiyaku/nyusatu/index.html 「インポート済み電子証明書によるログイン」をクリックします。 電子入札ログイン 証明書を取得済みの方はこちらからログインしてください。 インポート済み電子証明書による [→ ログイン ログインできない方はこちら ▼ 下記のような表示が出た場合は、 選択したクライアント証明書が不正です。 正しいクライアント証明書を選択した上で、 電子入札サイトにアクセスしてください。 閉じる 31・32・33ページ「キャッシュをクリアする」を行って ください。

JKK東京





[OK]ボタンをクリックします。

<表示されているクライアント証明書が、電子入札システムのクライアント証明書ではない、 有効期限が切れている等で他のクライアント証明書を選択したい場合は・・・>

・複数のクライアントが表示されていますので、
 該当するクライアント証明書を選択してください。
 [OK]ボタンをクリックします。

証明書の選択			×
e-bid.to-kousya.or.jp:443 での認証に使用す	る証明書を選択してください		
件名	発行元	シリアル番号	^
	Contraction of the Contraction		
bidTMHSC.to-kousya.or.jp	bidTMHSC Japan CA	6A00000AA976DDFA	32 🗸
<			>
証明書情報		OK キャンセ	ll I



(3)電子入札システムのログイン画面が表示されます。





(4) 電子入札システムへのログインを行います。

電子入札システムログイン画面でログインID(受付番号)及びログインIDに対応したパスワードを入力し、 [ログイン]ボタンをクリックします。



※ ログインID及び初期パスワードはJKK東京から送付した書類でご確認ください。

※ パスワードは任意に変更できます。

※ ログインIDは半角数字7桁です。

なお、ログインID またはパスワードを連続して5回間違えてログインを行うと、それ以降はログインができなくなります。 その場合は、JKK 東京契約課までご連絡ください。



(5)電子入札システムの「メインメニュー画面」が開きます。

の72 第件で	ServerTime 2016/12/ パンスアルク ニュアル も ログアウト	16 1
のインストー	-ラはこちら 	
xx 于八1	15216月11日豆稣有刈州政(安記).2017/03/31	
SWH 77	18650866014C99 入札案件一覧 JV入札案件一覧	
入礼•状况	確認はこちら	
案件状態	<ul> <li>□入礼特案件(入礼期限前の案件)</li> <li>☑入礼中案件(入礼期間中の案件)</li> <li>□開礼案件(開札演み、落礼一時保留中の案件)</li> <li>□厚礼案件(福礼業者が確定した案件)</li> <li>□中止案件(中止となった案件)</li> <li>□ 不調案件(不調となった案件)</li> <li>※必ず一つり上のチェックボックスを獲択してください。</li> </ul>	
案件区分	委託 ∨	1
登録業種	<u>金て                                    </u>	1
入礼締切日		1
検索条件を設	起して、【検索】ボタンをクリックしてください 検索	1
会社情報	まこちら パスワード変更 変更した場合、電子入札システムに 会社情報確認 / 変更申請	
和武・仕様	ログインし直してください 書等はこちら 各種様式等ダウンロード 各種仕様書等ダウンロード	]

#### この画面が表示されたら、正しくログインできています。

次に、STSインストール手順に進んでください。ただし、STSをすでにインストールしている方は対応不要です。 (STSはインストール済であれば、更新作業は不要です)



# その他



## 【旧クライアント証明書を削除する方法】

(1) Chrome(Google Chrome)を起動します。
 右上のGoogle Chromeの設定→「設定」
 を選択します。



#### (2)「プライバシーとセキュリティ」を選択します。





#### (3)「セキュリティ」を選択します。

(4)「証明書の管理」(もしくは 「デバイス証明書の管理」)を選択します。



	v	- 🗆 ×
$\leftarrow$ $\rightarrow$ $C$ $\odot$ Chrome   chrome://settin	s/security	\$ <b>* *</b> :
設定	Q、設定項目を検索	
▲ Googleの設定 自動1カ	Chrome では、定期的にパスワードをオンライン上の公開リストと照合し、確認しています。 その際、パスワードとユーザー名は Google を含め離も読み取ることができないよう暗号化さ れます。この機能は Google アカウントにログインすると有効になります。	
	保護なし(推員されません) ○ 危険なウェブサイト、ダウンロード、拡張機能から保護されていません。セーフブラウジングによる保 譲は、Gmal や Google 検索など他の Google サービスで利用可能な場合は、引き続き有効です。	
<ul> <li>Q、検索エンジン</li> <li>回、既定のブラウザ</li> <li>(1) お物時</li> </ul>	詳細設定 常に安全な接続を使用する 波給生を HTTPS (「アップグリード」, HTTPS をサポート」、ていないサイトは読み込む前に警告を実	
詳細設定 •		
拡張機能 🖸 Chrome について	証明書の管理 HTTPS / SSL の証明書と設定を管理します	1
	Google の高度な保護領統プログラム 個人の Google アカウントを標約型双駆から保護します	



(5)「個人」タブを選択します。

「発行先」が「bidTMHSC.to-kousya.or.jp xxxxxx」の「有効期限」が切れているクライアント証明書を選択します。

(「発行先」が「bidTMHSC.to-kousya.or.jp xxxxxx」のクライアント証明書が複数ある場合は、

有効期限が短い方を選択します)

※xxxxxxには、業者コード が表示されます。

「削除」ボタンをクリックします。

※異なる証明書を削除しないようにご注意ください。(他サイトが利用できなくなるなどの問題が発生してしまうことがあります)

	証明書			×	
	目的(N):	<すべて>		~	
Г	個人 いかの人 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	言頼されない発行元	
_	発行先		発行者	有効期限 5 ^	
_	bidTMHSC.to-k	ousya.or.jp	bidTMHSC Japan CA	2050/04/01 <	
	bidTMHSC.to-k	ousya.or.jp	bidTMHSC Japan CA	2021/04/01	
			and the second second		
bidTMHS であること	SC.to-kousya.or.j ☆確認	p		有効は期	)期限が切れている(また)  限が短い)ことを確認
	<			>	
	インポート(I) エク	'スポート(E) 削除(R)		詳細設定(A)	
	証明書の目的				
	クライアント認証				
				表示(V)	
				閉じる(C)	



(6)下記のメッセージが表示されます。「はい」ボタンをクリックします。



さきほど、選択したクライアント証明書が削除されたことを確認します。 「閉じる」ボタンをクリックします。

明書				
目的(N):	<すべて>			
個人 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 国bidTMHSC to	-kousva orin		発行者 bidTMHSC Japan CA	有効期限 こへ
	Keusyalonjp .			
<				>
インポート(I) 1	Eクスポート(E)	削除(R)		詳細設定(A)
証明書の目的				
クライアント認証				<b>.</b>
				表示(V)



## 困った時は・・・



## 【現象1】

- ・(クライアント証明書の選択が表示されず、)すぐに "選択したクライアント証明書が不正です~"の メッセージが表示される
- ・"管理者に問い合わせください。のメッセージが表示される

などのメッセージが出て、電子入札システムのログイン 画面が表示されてない場合は、 次ページの操作を行ってみてください。 状況が改善されるかご確認ください。



管理者に問い合わせください。	
閉じる	



## 【現象1の対処方法】

・キャッシュをクリアするために、以下の手順を行ってください。

(1) Chrome(Google Chrome)を起動します。
 右上のGoogle Chromeの設定→「その他のツール」
 →「閲覧履歴を消去」を選択します。



(2)「キャッシュされた画像とファイル」を選択します。

[データを削除]ボタンをクリックします。





(3)「安全確認」の「Chromeでデータ侵害や不正な拡張機能 などの脅威から保護されているか確認します」の [今すぐ確認]ボタンをクリックします。

(4-1)「更新 Chromeは最新の状態です」 が表示された場合は、 (5)に進んでください。

(4-2)「更新 アップデートが適用されました。更新を 完了するにはChromeを再起動してください。」が 表示された場合は、「再起動」ボタンをクリックします。 ※Chromeのみが再起動します。

(パソコンが再起動されるわけではありません)



🗘 設定 🗙 🗙	+			-		
← → C ③ Chrome   chrom	me://settings/privacy	Ŀ	☆		1	:
② 設定     ③	Q、 設定項目を検索					
Google の設定	▲					
自動入力	安全確認					
♥ プライバシーとセキュリ ティ	⊘ 安全確認を数分前に実行しました	G				
デザイン	✓ 更新 Chrome は最新の状態です					



(5)Chromeを全て閉じてください。

IEやEdgeなどのChrome以外のブラウザで開いている画面がある場合はそれも全て閉じてください。 そのあどに改めて、Chromeで電子入札システムにアクセスしてください。



## 【現象2】

・クライアント証明書の選択が出てきません。

・電子入札システムのURLにアクセスしましたが、電子入札システムのログイン画面が表示されません。

## 【現象2の対処方法】

次ページの手順でクライアント証明書が正しく入っているか確認してください。



## 【クライアント証明書が正しくインポートされているかの確認方法】

(1)Chrome(Google Chrome)を起動します。
 右上のGoogle Chromeの設定→「設定」
 を選択します。



#### (2)「プライバシーとセキュリティ」を選択します。





### (3)「セキュリティ」を選択します。

## (4) 「証明書の管理」(もしくは 「デバイス証明書の管理」)を選択します。

\$ 設	定	×	+			~	-		I	×
$\leftarrow \rightarrow$	C O C	Chrome   chrom	e://settings	s/privad	γ.		☆	*	-	:
設定					設定項目を検索					
<u>*</u>	Googleの設定	<u>A</u>			■」 お使いのブラウザは組織によって管理されています					-
Ê	自動入力		安	安全確認	2					
۲	プライバシー	とセキュリティ		9	Chrome でデータ侵害や不正な拡張機能などの脅威から保護されているか確認します	今すぐ確認				
۲	デザイン									
Q	検索エンジン		ブ	プライハ	(シーとセキュリティ					
日 山	既定のブラウ 起動時	f		Î	<b>閲覧履歴データの</b> 剤除 閲覧履歴、Cookie、キャッシュなどを削除します	×				
詳細調	设定	•		٩	Cookie と他のサイトデータ シークレット モードでサードパーティの Cookie がブロックされています	×				
拡張権	或前 <u>に</u>	Ľ		0	セキュリティ セーフ ブラウジング(危険なサイトからの保護機能)などのセキュリティ設定	×				
Chron	ne (C 261 C				<b>サイトの設定</b> サイトが使用、表示できる情報(位置情報、力メラ、ポップアップなど)を制御します	•				
				×	プライバシー サンドボックス 試用版職能はオンになっています	Z				
										-

			$\sim$	-	-	×
$\leftarrow$ $\rightarrow$ $C$ $\odot$ Chrome   chrome://settin	ngs/secu	rity		☆	*	:
設定		設定項目を検索				
<ul> <li>Google の設定</li> <li>自動入力</li> </ul>		Chrome では、定期的にパスワードをオンライン上の公開リストと照合し、確認しています。 その際、パスワードとユーザー名は Google を含め誰も読み取ることができないよう暗号化さ れます。 この職能は Google アカウントにログインすると有効になります。	-			
<ul> <li>ブライバシーとセキュリティ</li> <li>デザイン</li> </ul>	0	保護なし(推貨されません) 危険なウェブサイト、ダウンロード、拡張機能から保護されていません。セーフブラウジングによ 踏は、Gmail や Google 検索など他の Google サービスで利用可能な場合は、引き続き有効です。	にる保			
<ul><li>Q 検索エンジン</li><li>□ 限定のブラウザ</li></ul>	詳細	設定 安全な接続を使用する				
<ul> <li>         し</li> <li>         起動時         <ul> <li>             詳細設定             </li> </ul> </li> </ul>	移動示し	先を HTTPS にアップグレードし、HTTPS をサポートしていないサイトは読み込む前に警告を表 ます				
拡張機能 🖸	セキ この	ュア DNS を使用する 設定は管理対象のブラウザでは無効です	)			
Chrome について	証明 HTT	書の管理 PS / SSL の証明書と設定を管理します	Ø			
	Goo 個人	gle の高度な保護機能プログラム の Google アカウントを標的型攻撃から保護します	Z			



(5)「個人」タブを選択します。今登録した証明書を選択して、「表示」ボタンをクリックします。

	証明書				×
	目的(N):	<すべて>			~
Г	個人 いかの人 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	
	bidTMHSC.to-kc	usya.or.jp	bidTMHSC Japan CA	2050/04/01 2028/03/25	
bidTMHSC.to-kousya.or.jp であることを確認					
	<				>
	インポート(I) エク	スポート(E) 削除(I	R)	詳細設定	Ē(A)
	証明書の目的				
	クライアント認証			表示(V)	
				閉じる	(C)



(6)「証明のパス」タブを選択します。

画面下部に「この証明書は問題ありません」が表示されていればOKです。

証明書	×
全般 詳細 証明のバス	
- 証明のバス(P)	
bidTMHSC Japan CA	
証明者の表	<b>π</b> (V)
証明書の状態(S):	
この証明書は問題ありません。	
	OK



## 【解決しない場合は】

現象1の対処(キャッシュのクリア)や現象2の対処(クライアント証明書が正しくインポートされているかの確認)を行っても、 解消しない場合は、自社内のセキュリティ等の制限のために利用できない可能性があります。 自社内のセキュリティ等の確認いただき、セキュリティの設定等を変更してください。

以下のような場合に、ログイン画面が表示されないことがあります。(以下が全てではないため、他のセキュリティ制限等の 確認・設定等の変更をお願いします)

・セキュリティソフトで"クライアント証明書を使うサイトを許可していない"や"クライアント証明書を通過させないようにしている"

・ファイヤーウォールやプロキシ等でブロックしていた