

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7年2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・・・ 現象1 (「選択したクライアント証明書が不正です」「管理者に問い合わせください」などが表示される) 現象2 (「クライアント証明書の選択画面が出てこない」「電子入札システムのログイン画面が表示されない」など) 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 解決したい場合は	P.25~ P.26 P.30~ P.31 P.34 P.35 P.30
ኵ 仄 し な い ' 物 ロ は	P.39

【利用しているパソコンの環境】

下記以外の環境は、サポート及び間合せの対象外です

- (1) Windows10 Home/Pro(日本語版、64bit版)、Chrome
- (2) Windows11 Home/Pro(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。
※現在使用中のパソコン以外に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場合、
更新メールのURLが必要になりますので、削除せずに保存をお願いします。

※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/XXXXXXXXXXX

※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。

Chrome (Google Chrome)

	Google Chrome
^{kk.(9L} &&>たか() KK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 ワンタイムバ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」「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押してください。
	ログインID:
	パスワード:

クライアント証明書インポート主順調

電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。

※パスワードを忘れてしまった方は、パスワードの再発行が 必要です。

「電子入札システムのパスワードを忘れた方はこちら」を クリック後の操作手順は、

別紙「電子入札システム操作手順書(パスワード変更編)」 の「3. パスワードを忘れた場合」(2)~(4)を参照ください。



(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。

Det.(GUEBoth), JKK東京	
この画面は閉じずに、メールを確認	忍してください。
クライアント証明書グンロード用のフンク 登録流みのメールアドレスに送信 メールに記載されているワンタイムパスワ クライアント証明書グラウンロードオジン グライアント証明書がタウンロードできる	イムパスワードを ました。 ードを入力して、 見てください。 らうになります。
ワンタイムパスワード :	
クライアント証明書ダウンロー	:
電子入札システムにアクセスするためには、クライ 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/ インポート手順は「クライアント証明書インボート手	アント証明書が必要です。 ソコンにインボート(登録)してください。 頁書」を参照してください。
クライアント証明書インポート考	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。
閉じる	

(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:XXXX/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(30分)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。

	Ð	20	٤	Ξ	\⊕	$\overline{\mathbf{h}}$	e
ダウンロード			þ	Q		\checkmark	
ファイルを開く	.pfx						
もっと見る							



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 ファイル ホーム 共有 表示 			- 0	× ~ ?
← → * ↑ ↓ > PC > ダウンロード		▼ ^で	検索	
■ 3D オブジェクト ↓ ダウンロード ■ フィンアップ 言ドキュメント	Y 今日 (1) → pfx	更新日時 2021/11/25 11:28	種類 ^ Personal Informati	ť ^
■ ピクチャ				~
■ ビギナ 106 個の項目 1 個の項目を選択 984 バイト			and the second se	

※拡張子pfxが表示されていない場合は、以下の手順で拡張子を表示させてご確認ください。

・Windows10の場合 🚬 | 🔃 📃 = | エクスプローラー エクスプローラーを開きます。 共有 「表示」をクリックします。 大アイコン 📰 大アイコン 🛛 中アイコン 🔲 プレビュー ウィンドウ 開 小アイコン BB 一覧 目二 詳細 前列の追加、 ナビゲーション III 詳細ウィンドウ ウィンドウ・ 並べ替え ■ 並べて表示 目目 コンテンツ 「ファイル名拡張子」にチェックを付けます。 🔜 すべての列のサイズを自動 ・Windows11の場合 エクスプローラーを開きます。 「表示」をクリックします。 \square > PC > 8二 表示 rO (Ā) ↑↓ 並べ替え (表示内の)「表示」をクリックします。 デスクトップ ~ デバイスとドライブ 特大アイコ 大アイコン 中アイコン 「ファイル名拡張子」にチェックを付けます。 ローカル ディスク (C:) > 合市-ム 小アイコン 空き領域 160 GB/237 G ▶ ギャラリー 詳細 ~ ネットワークの場所 > 🞍 ダウンロード 並べて表示 コンテンツ 8= > 🧾 デスクトップ (1) 詳細ウィンド > 📑 F==X2F



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。

	×
←	
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 ④ 現在のユーザー(C)	
○ □-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) キャンセノ	٢
	 ✓ ■ 証明書のインボートウイザードの開始 広のケバナードでは、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よです。 ごのウバガードでは、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なたたかりトワーク接続を提供するための情報を含んています。証明書カバスドをされるシステムとの領域です。 保存場所 ● 現在のユーザー(C) ● ローカル コンビューター(L) 株行するには、「次へ」をクリックしてください。 次へ(N) ない (次へ) (ない)



(3)「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
	インボ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): を 研(R)… 参照(R)…
	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 証明書 (.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。	
バスワード(P): ●●●●●●●●● 「jkkC	57333」を入力
□ パスワードの表示(D)	
インポート オプション(I):	
□ 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)	
☑ 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。

÷	☞ 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	ザードの完了
	[完了]をクリックすると、証明書	き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	7 個人
	ファイル名	CVUsersVersion and a second se
	<	>
		完了(F) キャンセル

(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。





(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。



🌣 19	定 · セキュリティ × +			~	-	0		×
\leftarrow -	C Chrome chrome://settin	igs/secur	iity		☆	*	-	:
設定			設定項目を検索					
: 6	Google の設定 自動入力		Chrome では、定期的に「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、バ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。					ľ
?	プライバシーとセキュリティ デザイン	0	保護なし(推奨されません) 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。 譲は、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				
م ا	検索エンジン 既定のブラウザ 起動時	詳細! 常に! 移動!	^{設定} 安全な接続を使用する 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					
詳細調		示し! セキ: この!	ます ユア DNS を使用する 段定は管理対象のブラウザでは無効です	0				
拡張 Chror	機能 【2] me について	証明 HTTF	書の管理 SS / SSL の証明書と設定を管理します	Ø]			
		Goog 個人(le の高度な保護機能プログラム ⑦ Google アカウントを標的型攻撃から保護します	Z				

(5)「ユーザの証明書」を選択します。 「Windowsからインポートした証明書 を管理する」を選択します。

★ 設定・セキュリティ × 月 証明書 日	Rネージャ × +	-	0	×
← → C () Chrome chrome://certificate-m	hanager/clientcerts	☆	-	:
◎ 証明書マネージャ				
🛄 ローカル証明書	ユーザーの証明書			
🗷 ユーザーの証明書	クライアント証明書は、他のサーバーに対してユーザーの認証を行う証明書です。			
Ohrome Root Store	管理者方治加	^		
	証明書がありません			
	ウィンドウ			
	Windows からインボートした証明書を表示する	•		
	Windows からインボートした証明書を管理する	Ø		

(6)「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):	<রু\(৴					~
C	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		1
			1	2120/03/	16 <なし>		Ш
	.			2020/09/	07 <なし>		Ш
				2028/04/	01 <なし>		Ш
							-
Г							
L	インボート(I) エクン	スポート(E)	削除(R)			詳細設定(A	()
	証明書の目的						
	暗号化ファイル システム						
						表示(V)	
						問!!ろ(0)	
						(C)	

JKK東京



(7)「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) キャンセル	



(8)「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 · · · · · · · · · · · · · · · · · · ·	υ	ダウンロードの検索
	整理 ▼ 新しいフォルダー		· · · · · · · · · · · · · · · · · · ·
	✓ 素 クイック アクセス ^ヘ 名前		更新日時 人
← ジジ 証明書のインボートウィザード	■ デスクトップ オ		マイルルを選択
			「へ COD JAIN」を送入
インボートする証明書ファイル	▼ (1), (1), (1), (1), (1), (1), (1), (1),		
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(N):	~ すべての	リアイル (*.*) ~
		開	<(O) キャンセル
ファイル名(F):			
CiUsersVet 11, 11, 4 Andrew and Andrew and Andrew	参照(R)		
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 証明書 (.P	7B)		
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。



(9)「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」	を入力
	□ パスワードの表示(D)	
	インポート オプション(I): 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。 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) ☑ すべての拡張プロパティを含める(A) 	
	次へ(N) キャンセル	



(10)「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)	_
	 ● 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 参照(R) 	
		_
	77 A (AD) + + + > 1+	



(11)「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サ	fードの完了	
	[完了] をクリックすると、証明書が	ゲ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	
	内容	PFX	
	<	>	
		完了(F) キャンセル	1

(12)「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 Chrome 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 件名	る証明書を選択してくたさい 発行元	シリアル番号	^
			:
bidTMHSC.to-kousya.or.jp	bidTMHSC Japan CA	6A00000AA976DDFA3	2 🗸
<		2	
証明書情報		วห キャンセル	,



(3)電子入札システムのログイン画面が表示されます。

1)電子入札 システム	4 - Micros	oft Internet	Explorer			-0
774110日 編集()	D 表示()/	890C入()(8)	7-8D	V154R		_
ログイン田(羊	角入力)					
パスワード(牛	角入力)					
					NEE (cl tabata)	
リセット						
					JICICARAN	
			_	-		
			電子	入札シ	·ステム	1
			00月	×802100	~2400はメンラナンスのためご利用できなくなります。	
			2,818	をおかけ聞し	ますが、ご協力のほどをよろしくお願い吹します。	
			1			



(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(入札参加登録時にJKK東京から送付したもの)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。

	ServerTime 2016/12/16 パニュアル 3 ログアウト
のインスト	ーラはこちら
競争入	礼参加資格登録有効期限(委託):2017/03/31
参加中込	指名確認はこちら
	入札案件一覧 JV入札案件一覧
入札•扶汤	は言語はこちら
案件状態	□入礼特案件(入礼期駅前の案件) ☑入礼申案件(入礼期間中の案件) □開礼案件(開礼演み、落礼一時保留中の案件) □洋礼案件(塔札業者が確定した案件) □中止案件(中止となった案件) □不調案件(不調となった案件) □水調案件(不調となった案件)
案件区分	委託 マ
登錄業種	<u><u>कि</u>र ∨</u>
入礼締切日	からまたで※半角数字で入力してください。どちらか一方のみの指定も可能です。 入力例:[2010/01/20]から[2010/03/03]まで
検索条件を設	定して、【検索】ボタンをクリックしてください 検索
会社情報	はこちら
	パスワード変更 変更した場合、電子入札システムに ログインし直してください
様式・仕様	/書等はこちら
	名類様式第月かいロード 名類件様変第月かいロード

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。



\$ 19	定 · セキュリティ × +			~	-	0		×
\leftarrow -	C Chrome chrome://settin	ngs/secu	rity		☆	*	-	÷
設定			設定項目を検索					
: 8	Google の設定 自動入力		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紹合し、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。	>				
€	プライバシーとセキュリティ デザイン	0	何種なし(推乗されません) 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 猫は、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。	5保				
م ا	検索エンジン 既定のブラウザ 起動時	詳細 常に 移動	設定 安全な接続を使用する 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					
詳細調		示し セキ この	ます ユア DNS を使用する 設定は管理対象のブラウザでは無効です	>				
Chror	mme (こついて	証明 HTTI	書の管理 PS / SSL の証明書と設定を管理します	Z				
		Goog 個人	yle 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				



(6)「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)
 ※xxxxxxxには、業者コード が表示されます。

KK東京

28

「削除」ボタンをクリックします。

※異なる証	E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)
	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-kouse or in	発行者 有効期限 5 A	
	bidTMHSC.to-kousya.or.jp	bidTMHSC Japan CA 2021/04/01	
bidTM である	IHSC.to-kousya.or.jp ことを確認	有効期限が切れている(また は期限が短い)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)	:



(7)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。

E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 bidTMHS	C.to-kousya.or.jp		発行者 bidTMHSC Japan CA	有効期限 5 个 2050/04/01 <
<				×
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)



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	



32

【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。

(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。

(1) Chrome(Google Chrome)を起動します。
 右上のGoogle Chromeの設定→「閲覧履歴データを削除」
 を選択します。

(3)「安全チェック」の[安全チェックに移動]ボタン をクリックします。



🥖 入札 | JKK東京 × + ← → C ③ Chrome chrome://settings/clearBrowserData ☆ 😩 : 設定 Q、設定項目を検索 閲覧履歴データを削除 G Google の設定 基本設定 詳細設定 On 自動入力とパスワード 期間 1 時間以内 9 閲覧履歴 @ パフォーマンス 検索ボックスなどの履歴を削除します Cookie と他のサイトデータ ほとんどのサイトからログアウトします Q 検索エンジン キャッシュされた画像とファイル ロ 既定のブラウザ 最大で 188 MB を解放します。サイトによっては、次回アクセスする際に \sim 読み込みに時間がかかる可能性があります。 (¹) 記動時 ☆ 言語 ダウンロード データを削除 キャンセル ユーザー補助機能 × 💠 設定 - プライバシーとセキュリティ × + 🥖 入札|JKK東京 _ × ← → C ③ Chrome chrome://settings/privacy ☆ 😩 : 設定 0 Q、設定項目を検索 ■ お使いのブラウザは組織によって管理されています G Google の設定 安全チェック ◎ 自動入力とパスワード ♥ プライバシーとセキュリ ティ 安全に関する推奨事項をご確認ください 0 安全チェックに移動 パスワード @ パフォーマンス



(4-1)「安全に関する概要」に 「Chromeは最新の状態です」が表示されている 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)



(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。 そのあとに改めて、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。

\$ 段	定	× +			~	-]	×
$\leftarrow \rightarrow$	C 💿 Chrome	chrome://set	tings/priv	acy		☆	*	-	:
設定				設定項目を検索					
•	Google の設定			お使いのブラウザは組織によって管理されています					Â
Ê	自動入力		安全確	82					
•	プライバシーとセキュ!	リティ	0	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		プライ	パシーとセキュリティ					
日 し	既定のブラウザ 起動時		Ĩ	関覧履歴データの削除 閲覧履歴、Cookie、キャッシュなどを削除します	÷				
詳細調	没定	•	۵	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	Þ				
拡張権	度推		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競定	Þ				
Chron	ne (20117		#	サイトの設定 サイトが使用、表示できる情報(位置情報、カメラ、ポップアップなど)を制御します	•				
			x	プライバシー サンドボックス 試用板機能はオンになっています	Z				ł

现定		0	动士语曰永处表		
DX JC		~			
Goo	gle の設定		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		
Ê 自動	入力		れます。 この機能は Google アカウントにロクインすると有効になります。		
😯 75	イバシーとセキュリティ	0	保護なし(推奨されません) 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		
🌳 デザ	イン		纏は、Gmail や Google 検索など他の Google サーヒスで利用可能な場合は、引き続き有効です。		
Q、 検索	エンジン	*¥ \$8	設定		
□ 既定	のブラウザ	PT-19	incac.		
し 起動	時	常に 移動 示し	安全な機能を使用する 洗を 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		
詳細設定	*	174	ニュア DNS を使用する		
抗張繼能	[2]	この	設定は管理対象のブラウザでは無効です		
Autroane について		証明 HTT	1書の管理 PS / SSL の証明書と設定を管理します		
		Goo 個人	gle の高度な保護機能プログラム の Google アカウントを使め里攻部から保護します		





(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] a					\times
全般	詳細	証明のバス				
- 129	月のパス(P)					- 1
	ibidTMH	ISC Japan CA MHSC.to-kou	sya.or.jp 💭			
				証明	書の表示(V)	
証明	書の状態()	5);				- 1
201	199日は国	認めりよせん。				
					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