公的個人認証サービス

利用者クライアントソフト API 仕様書

【個人認証サービス AP C 言語インターフェース編】

第１.１版

公的個人認証サービス　指定認証機関

財団法人　自治体衛星通信機構

変更履歴

版数	変更内容
1.0 版	新規作成
1.1 版	Windows XP SP2 対応に伴い表 1(2 頁)のプラットホームを追加

－ 目次 －

第１章　はじめに

利用者クライアントソフトにおける個人認証サービス AP は、以下の機能を実現するための Application Program Interface(以下、API)を提供する。

- 証明書表示機能
- 基本 4 情報取得機能
- 官職証明書検証機能

以降、本書では個人認証サービス AP のうち、C 言語インターフェースの API 仕様について説明する。

第２章　ドキュメント体系

利用者クライアントソフトのドキュメント体系図を以下に示す。本書は以下の体系図の網掛け部分に該当する。

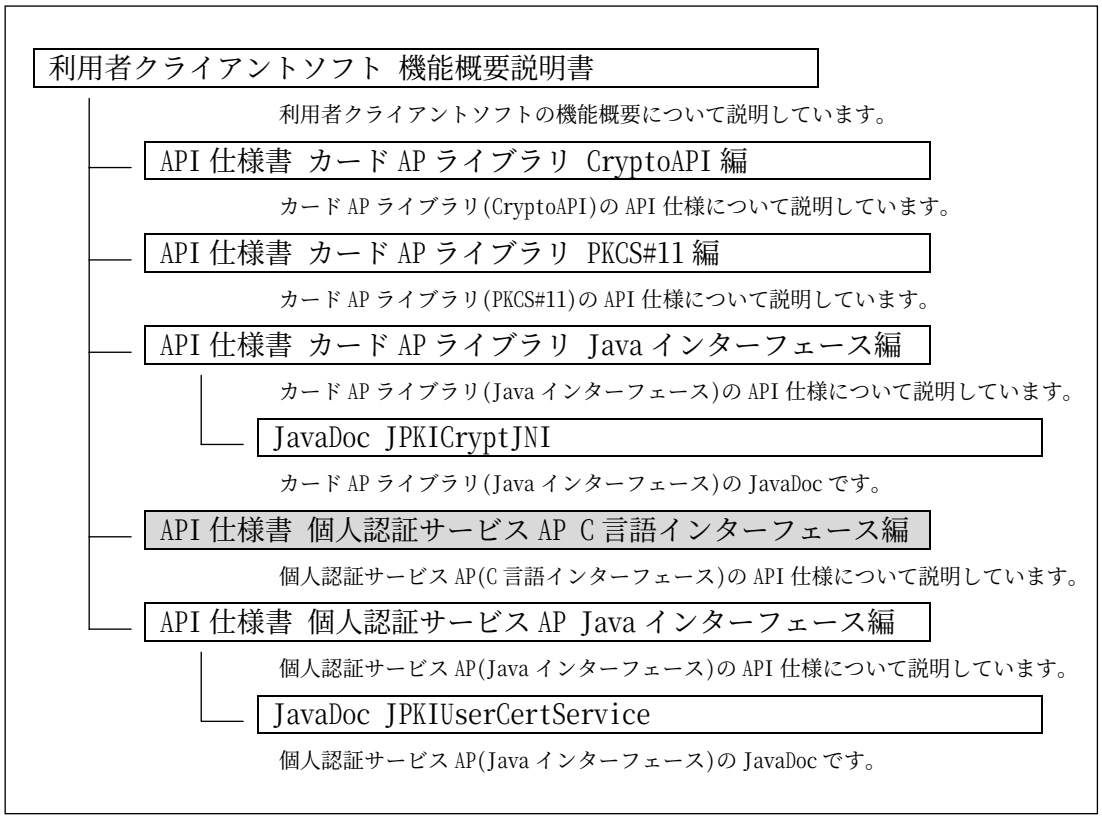


図 1 ドキュメント体系図

第３章　動作環境

個人認証サービス AP(C 言語インターフェース)の動作環境は以下の通りとする。

表 ３.１ 動作環境

項目	条件
プラットフォーム	Windows98 Second Edition(※1) Windows Millennium Edition(※1) WindowsNT4.0 ServicePack6a(※2) Windows2000 ServicePack2 Windows2000 ServicePack3 Windows2000 ServicePack4 WindowsXP ServicePack1 WindowsXP ServicePack2
Web ブラウザ(※3)	Internet Explorer5.5 ServicePack2(※4) Internet Explorer6 ServicePack1(※4) Netscape6.1 Netscape6.2.3 Netscape7.02 Netscape7.1
IC カード	公的個人認証サービスカードアプリケーションを搭載し、公的個人認証サービスの電子証明書が格納されたICカードとする。
IC カードリーダライタ	以下の条件を満たす IC カードリーダライタとする。(「適合性検証済み IC カードリーダライター一覧」を参照のこと。) ・ IC カードのインターフェース(非接触型、接触非接触両対応型)に対応していること ・ USB や RS-232C など、パソコンに接続するためのインターフェースを有すること ・ IC カードリーダライタと通信するためのドライバソフトウェアが提供されていること ・ ICカードの搬送方式が手動挿入/手動排出タイプまたは自動挿入/自動排出タイプであること ・ ICカードを挿入するスロットの数は1つとし、1度に挿入できるICカードは1枚であること

※1 証明書表示機能において補助漢字(JIS X 0212)の表示に一部制限あり。

※2 OS に補助漢字をサポートするフォントがインストールされている必要あり。

※3 Web ブラウザにて利用者証明書の基本情報を表示する場合にいずれかが必要になる。

※4 暗号機能等の利用のため、Internet Explorer5.5 ServicePack2 もしくは Internet Explorer6 ServicePack1 が必要になる。

第４章　機能仕様

第１節　ソフトウェア構成図

本仕様書では、利用者クライアントソフトのうち、下図の太枠に示す個人認証サービス AP(C 言語インターフェース)の仕様をまとめる。

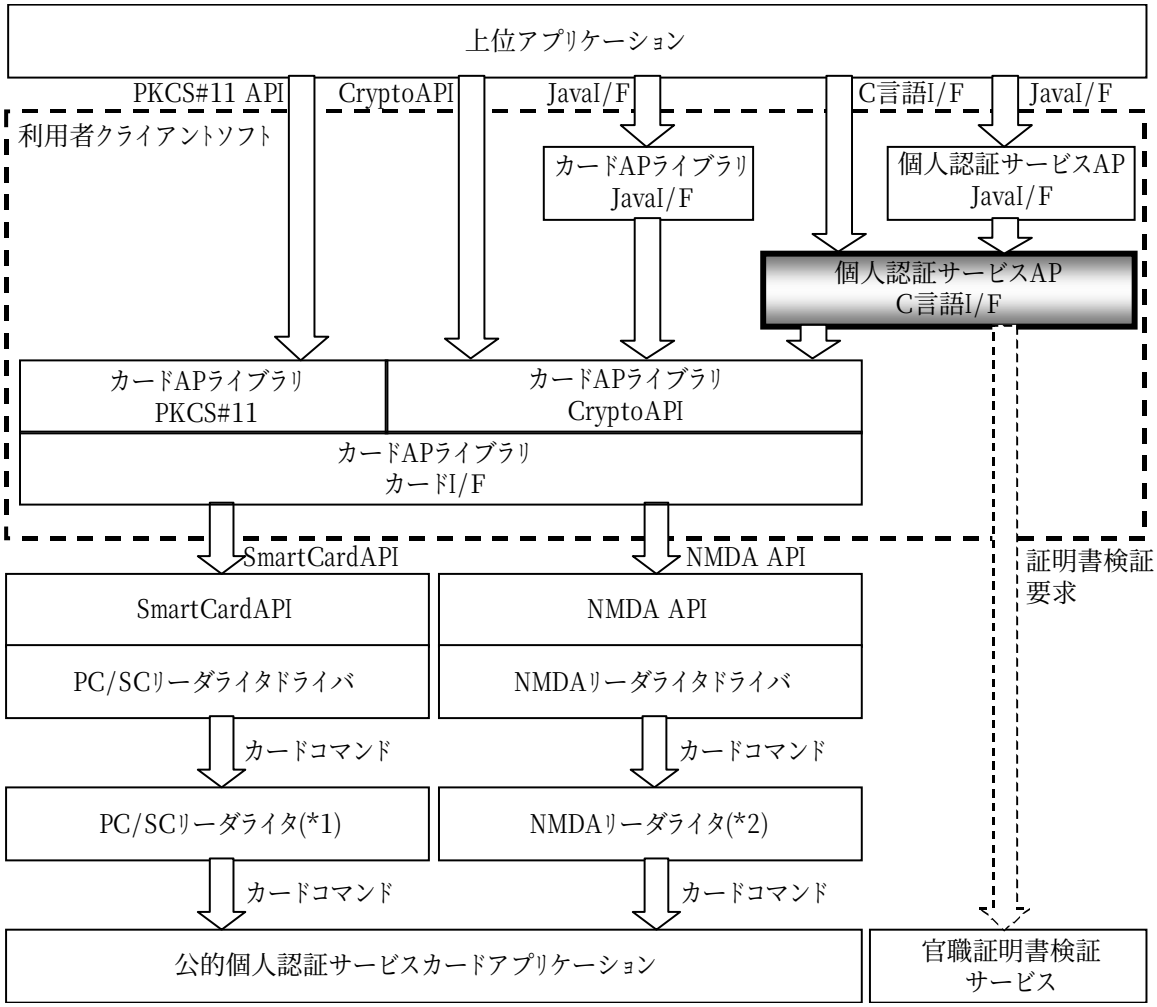


図 ４.１ ソフトウェア構成図

*1 Personal Computer/Smart Cardの略。Microsoft社等のワーキンググループが推進する、Windows環境におけるICカード利用のための統一規格(PC/SC規格)に対応したICカードリーダライタのことを指す。

*2 New Media Development Associationの略。(財)ニューメディア開発協会「IT装備都市研究事業 リーダライタ共通インターフェース仕様書 1.1 版[平成 14 年 5 月 29 日]」に対応したICカードリーダライタのことを指す。

第２節　実現可能な機能の一覧

個人認証サービス AP(C 言語インターフェース)で実現可能な機能の一覧を表 ４.１に示す。

表 ４.１ 実現可能な処理の一覧

NO	機能	概要
1	証明書表示	電子証明書を証明書 Viewer で表示する。
2	基本 4 情報取得	利用者証明書から基本 4 情報(氏名、住所、性別、生年月日)を取得する。
3	官職証明書検証	官職証明書や職責証明書の証明書検証を行うため、公的個人認証サービスの都道府県センターにある官職証明書検証サービスに対して証明書検証要求を発行する。

第５章　　API 仕様

第１節　サポート API 一覧

サポート API 一覧を表 ５.１に示す。

表 ５.１ サポート API 一覧

NO	API 名	概要
1	JPKICertViewDialog	電子証明書を表示する。
2	JPKIGetBasicData	利用者証明書から基本４情報を取得する。
3	JPKICertValid	官職証明書の証明書検証を行う。
4	JPKIFreeBasicData	基本４情報の格納領域を解放する。

第２節　サポート API 仕様詳細

（1）　JPKICertViewDialog

API 名	JPKICertViewDialog		
概要	電子証明書を表示する。		
関数インターフェース	int JPKICertViewDialog (　　JPKI_CertBinaryData　　*certData);		
	値		内容
戻り値	JPKI_USER_TRUE		正常終了。
	JPKI_USER_FALSE_INVALID_PARAM		引数に不正な値が設定されていた。
	JPKI_USER_FALSE_MEMORY		メモリが不足している。
	JPKI_USER_FALSE_DECODE_CERT		証明書のデータの解析に失敗した。
	JPKI_USER_FALSE_SHOW_VIEWER		ダイアログの表示に失敗した。
	JPKI_USER_FALSE_OTHER		その他システムエラーが発生した。
	型	I/O	内容
引数	JPKI_CertBinaryData *	IN	電子証明書データ(DER 形式)

（2）　JPKIGetBasicData

API 名	JPKIGetBasicData		
概要	利用者証明書から基本４情報を取得する。		
関数インターフェース	int JPKIGetBasicData (　　JPKI_CertBinaryData　　*certData, 　　JPKI_BasicData　　*basicData);		
	値		内容
戻り値	JPKI_USER_TRUE		正常終了。
	JPKI_USER_FALSE_INVALID_PARAM		引数に不正な値が設定されていた。
	JPKI_USER_FALSE_MEMORY		メモリが不足している。
	JPKI_USER_FALSE_DECODE_CERT		証明書のデータの解析に失敗した。
	JPKI_USER_FALSE_OTHER		その他システムエラーが発生した。
	型	I/O	内容
引数	JPKI_CertBinaryData *	IN	利用者証明書データ(DER 形式)
	JPKI_BasicData *	OUT	基本４情報

（3） JPKICertValid

API 名	JPKICertValid		
概要	官職証明書の証明書検証を行う。		
関数インターフェース	int JPKICertValid (JPKI_CertBinaryData *certData, int *certPathStatus, int *responseStatus);		
戻り値	int（表 5.2 検証結果コード（戻り値）参照）		
	型	I/O	内容
引数	JPKI_CertBinaryData *	IN	検証対象証明書データ(DER 形式)
	int *	OUT	証明書検証（認証パスの構築および検証）の結果コード (表 5.3 検証結果コード（certPathStatus）参照)
	int *	OUT	OCSP レスポンスステータス (表 5.4 検証結果コード（responseStatus）参照)

表 5.2 検証結果コード（戻り値）

#	Define シンボル(定義名)	区分※1	意味
1	JPKI_CVS_OK	-	証明書検証に成功した。 この戻り値を返却する場合､以下の値が設定される。 certPathStatus … 0（有効） responseStatus … 0（OCSP Request が正しく処理された）
2	JPKI_CVS_NG	-	証明書検証に失敗した。 この戻り値が返却された場合、certPathStatus に CVS 証明書検証サーバが返却した検証結果コードが設定される。
3	JPKI_CVS_FALSE_CL_MEMORY	C	メモリの確保に失敗した。
4	JPKI_CVS_FALSE_CL_INVALID_PARAM	C	引数に設定した値が間違っている。
5	JPKI_CVS_FALSE_CL_OTHER	C	システム関数起因によるエラーが発生。
6	JPKI_CVS_FALSE_CL_CREATE_REQUEST	C	OCSP Request および拡張情報の生成に失敗した。または、リクエスト署名の生成に失敗した。
7	JPKI_CVS_FALSE_CL_HTTP	C	HTTP または HTTPS 通信で失敗した。
8	JPKI_CVS_FALSE_SV_DECODE	S	OCSP Response(ASN.1 エンコード形式)のデコードに失敗した。
9	JPKI_CVS_FALSE_SV_RESPONSE_EXCEPTION	S	OCSP レスポンダで例外が発生した。 この戻り値が返却された場合、responseStatus に OCSP レスポンダが返却したステータスが設定される。
10	JPKI_CVS_FALSE_SV_SIGN_VERIFY_SIGNATURE	S	OCSP レスポンダから受信した OCSP Response(ASN.1 エンコード形式)の署名検証に失敗した。

#	Define シンボル(定義名)	区分※1	意味
11	JPKI_CVS_FALSE_SV_NONCE	S	Request送信時に付与したnonceとResponseに含まれるnonce※2が一致しない場合に返却する。
12	JPKI_CVS_FALSE_SV_CERT_VERYFY	S	CVS 証明書の証明書検証に失敗した。
13	JPKI_CVS_FALSE_SV_ANALYZE	S	証明書検証結果の解析に失敗した。
14	JPKI_CVS_FALSE_CL_CVSURL	C	接続先証明書検証サーバのＵＲＬが不正の場合に返却する。
15	JPKI_CVS_FALSE_CL_GETCERT	C	IC カードリーダから証明書(利用者証明書または、CA 証明書)の取得に失敗した。

(※1) 区分　C:クライアント側エラー　S:サーバ側エラー

（※2）nonce

検証サーバに検証を依頼するために送信した Request とその結果として返ってきた Response が真に対応しているかどうかを確認する為に、送信時に Request に付与する 1 から 33 バイトの乱数。Request に付与した nonce と、Response に含まれる nonce が一致すれば送信した Request に対する Response であると確認される。

表 5.3 検証結果コード（certPathStatus）

#	Define シンボル(定義名)	値	内容	解説
1	JPKI_CVS_GOOD	0	有効	認証パスの構築が成功し検証結果が正しい
2	JPKI_CVS_INTERNAL_PATH_CONSTRUCTION_ERROR	101	認証パス構築不可	認証パス構築ができない
3	JPKI_CVS_SIGNATURE_VERIFICATION_FAILURE	202	署名不正	認証パスに署名が不正である証明書が含まれる
4	JPKI_CVS_ONE_OR_MORE_CERTIFICATES_ARE_REVOKED	203	失効証明書を含む	認証パスに失効した証明書が含まれる
5	JPKI_CVS_POLICY_MAPPING_ERROR	204	ポリシ不一致	認証パスにポリシが一致しない証明書が含まれる
6	JPKI_CVS_CONSTRAINTS_ERROR	205	制約違反	認証パスに制約に違反している証明書が含まれる
7	JPKI_CVS_CERTSTATUS_OF_OCSP_RESPONSE_IS_UNKNOWN	206	OCSP での証明書検証確認不正	認証パスに OCSP での certStatus が unknown と応答される証明書が含まれる
8	JPKI_CVS_REJECTED_A_REQUEST	901	要求受付け拒否	証明書検証サーバ(CVS)側で要求の受け付けを拒否した
9	JPKI_CVS_VALIDATION_TIMEOUT	902	タイムアウト	要求がタイムアウトとなった

表 5.4 検証結果コード（responseStatus）

#	Define シンボル(定義名)	値	内容	解説
1	JPKI_CVS_RESSTATUS_SUCCESSFUL	0	成功	OCSP Request が正しく処理された
2	JPKI_CVS_RESSTATUS_MALFORMEDREQUEST	1	エラー	OCSP Request のフォーマットエラー
3	JPKI_CVS_RESSTATUS_INTERNALERROR	2	エラー	内部エラー
4	JPKI_CVS_RESSTATUS_TRYLATER	3	エラー	一時的な解答不能
5	JPKI_CVS_RESSTATUS_SIGREQUIRED	5	エラー	OCSP Request への署名が必要
6	JPKI_CVS_RESSTATUS_UNAUTHORIZED	6	エラー	クライアントが認証されていない

（4） JPKIFreeBasicData

API 名	JPKIFreeBasicData		
概要	基本４情報の格納領域を解放する。		
関数インターフェース	int JPKIFreeBasicData (JPKI_BasicData *basicData);		
	値		内容
戻り値	JPKI_USER_TRUE		正常終了。
	JPKI_USER_FALSE_INVALID_PARAM		引数に不正な値が設定されていた。
	型	I/O	内容
引数	JPKI_BasicData *	IN	基本４情報

第３節　構造体仕様

（1）　JPKI_CertBinaryData

構造体名		JPKI_CertBinaryData		
概要		電子証明書情報を格納する構造体。		
NO	変数名	型	値	備考
1	len	unsigned long	電子証明書データ長	
2	data	unsigned char *	電子証明書データの格納先ポインタ	DER 形式とする。

（2） JPKI_BasicData

構造体名		JPKI_BasicData		
概要		基本４情報を格納する構造体。		
NO	変数名	型	値	備考
1	name	wchar_t *	氏名	UNICODE
2	address	wchar_t *	住所	UNICODE
3	gender	char *	性別	性別コード。 1:男　2:女　3:不明
4	dateOfBirth	char *	生年月日	9 桁のコード（EYYYYMMDD)。 E　：年号コード。 (1:明治　2:大正 3:昭和　4:平成) YYYY：西暦年 MM　：月 (01～12:1 月～12 月 00:不明　A1:春 A2:夏　A3:秋　A4:冬) DD　：日 (01～31:1 日～31 日 00:不明　A1:上旬 A2:中旬　A3:下旬)
5	substituteCharacterOfName	char *	代替文字の使用（氏名）	name と同じ文字数の文字列。代替文字と同じ位置に 1、その他に 0 が入る。
6	substituteCharacterOfAddress	char *	代替文字の使用（住所）	address と同じ文字数の文字列。代替文字と同じ位置に 1、その他に 0 が入る。

第４節　コーリングシーケンス

「第４章　第２節　実現可能な機能の一覧」を実現するためのコーリングシーケンスを以下に示す。上位アプリケーションは、このコーリングシーケンスに沿って実装すること。

（1） 証明書表示処理

電子証明書を DER 形式で取得	
↓	
JPKICertViewDialog	電子証明書の表示 certData: 電子証明書格納領域アドレス

（2） 基本４情報取得処理

利用者証明書を DER 形式で取得	
↓	
JPKIGetBasicData	基本４情報の取得 certData: 利用者証明書格納領域アドレス basicData: 基本 4 情報格納領域アドレス
↓	
basicData から必要情報の取得	
↓	
JPKIFreeBasicData	基本４情報格納領域の解放 basicData: 基本 4 情報格納領域アドレス

（3） 官職証明書検証処理

官職証明書や職責証明書を DER 形式で取得	
↓	
JPKICertValid	官職証明書や職責証明書の証明書検証 certData: 電子証明書格納領域アドレス certPathStatus: 証明書検証（認証パスの構築および検証）の結果コード格納領域アドレス responseStatus: OCSP レスポンスステータス格納領域アドレス
↓	
結果コードの解析	

第６章　画面仕様
第１節　画面一覧

表 ６.１ 画面一覧

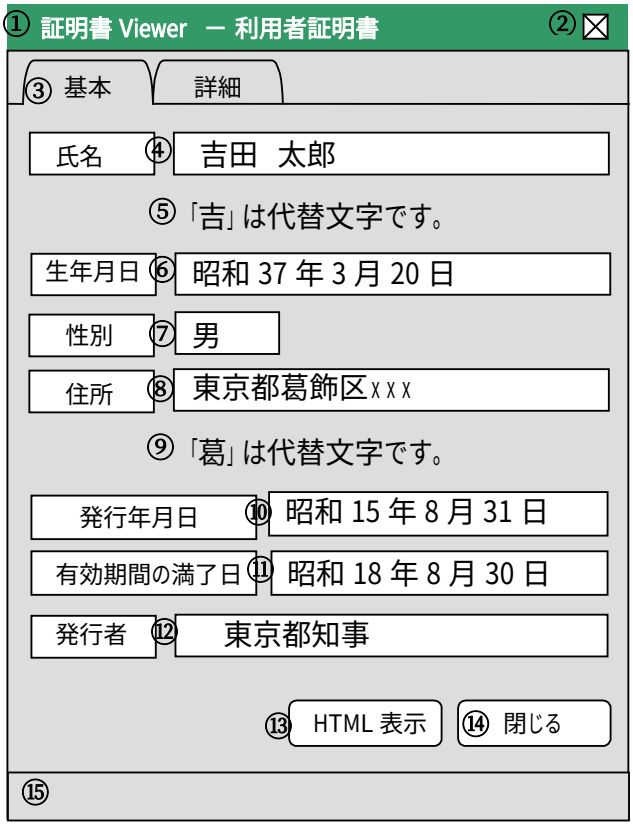
NO	機能名	画面名		概要
1	証明書表示機能	基本画面	利用者証明書	利用者証明書の基本情報を表示する。 [HTML 表示]ボタン押下により、利用者証明書基本情報画面(HTML)を表示する。
2			CA 証明書	CA 証明書(ルート CA 証明書,リンク証明書,下位 CA 証明書,相互認証証明書,自己署名証明書等)の基本情報を表示する。
3			電子証明書（官職／職責／その他証明書の場合）	上記以外の証明書の基本情報を表示する。 [証明書検証]ボタン押下により、証明書の検証を行う。
4		詳細画面		電子証明書内の全ての記載事項を表示する。 官職／職責／その他証明書の電子証明書の詳細画面にて、[証明書検証]ボタン押下により、証明書の検証を行う。
5		官職証明書・職責証明書画面		官職／職責／その他証明書の電子証明書（基本／詳細）画面にて、[証明書検証]ボタンを押下し、証明書検証を行い、証明書検証結果を表示する。
6		利用者証明書基本情報画面(HTML)		利用者証明書基本画面での[HTML 表示]ボタンを押下により、ブラウザ上に利用者証明書基本情報を表示する。

第２節　画面仕様詳細

（１） 利用者証明書

画面名	利用者証明書基本画面
概要	利用者証明書の基本情報を表示する。

画面レイアウト



表示項目と証明書領域の対応は、表　６．２を参照。

画面項目説明

NO	項目名	概要
①	タイトルバー	表示する電子証明書の種類を表示する。 表示テキストは「証明書 Viewer－利用者証明書」とする。
②	終了ボタン	証明書 Viewer を閉じる。
③	タブ	基本画面と詳細画面を切り替える。
④	氏名*1	利用者の氏名を表示する。最大 100 文字まで表示可能。画面上に表示しきれない場合は、カーソルを移動することにより、表示欄のスクロールを可能とする。
⑤	代替文字の使用（氏名）*1	氏名の代替文字を表示する。最大 100 文字まで表示可能。代替文字がない場合は、表示しない。
⑥	生年月日	利用者の生年月日を和暦で表示する。
⑦	性別	利用者の性別（男/女/不明）を表示する。
⑧	住所*1	利用者の住所を表示する。最大 200 文字まで表示可能。画面上に表示しきれない場合は、カーソルを移動することにより、表示欄のスクロールを可能とする。
⑨	代替文字の使用（住所）*1	住所の代替文字を表示する。最大 200 文字まで表示可能。代替文字がない場合は、表示しない。

⑩	発行年月日	電子証明書の発行年月日を和暦で表示する。
⑪	有効期間の満了日	電子証明書の有効期間の満了日を和暦で表示する。
⑫	発行者	電子証明書の発行者を表示する。
⑬	HTML 表示	[HTML 表示]ボタンを押下することによって、Web ブラウザにて利用者証明書の基本情報を表示する。詳細については、「（６）利用者証明書　基本情報画面（HTML）」の画面項目説明を参照。（[HTML 表示]ボタンは、利用者証明書基本画面の場合のみ表示する。）
⑭	閉じるボタン	証明書 Viewer を閉じる。
⑮	ステータスバー	使用せず。

*1：Windows98／Me 版では、氏名または住所に表示できない文字（JIS 補助漢字）が含まれている場合、氏名または住所欄にメッセージ「[HTML 表示]ボタンを押して内容を確認して下さい。表示できない文字(JIS 補助漢字)が含まれています。」を表示する。このとき、代替文字欄には何も表示しない。

表 ６.２ 表示項目と証明書領域の対応（利用者証明書）

項番	項目名	証明書の項目名		表示方法
		上位項目名	項目名	
1	氏名	SubjectAlt-Name	CommonName	設定値をそのまま表示。
2	代替文字の使用(氏名)		Substitute-CharacterOf-CommonName※1	・代替文字を「鍵括弧」付で表示。 ・ 代替文字が複数ある場合は代替文字を続けて表示。 例) 「吉」「郎」は代替文字です。 ・ 同じ代替文字が続いた場合は、繰り返し表示。 例)「吉」「吉」は代替文字です。
3	生年月日		dateOfBirth※2	設定値を和暦に変換して表示。
4	性別		gender※3	設定値を日本語表記に変換して表示。
5	住所		address	設定値をそのまま表示。
6	代替文字の使用(住所)		Substitute-CharacterOf-Address※1	・代替文字を「鍵括弧」付で表示。 ・代替文字が複数ある場合は代替文字を続けて表示。 例) 「葛」「飾」は代替文字です。 ・ 代替文字が続いた場合は、繰り返し表示。 例)「葛」「葛」は代替文字です。
7	発行年月日	Validity	NotBefore	設定値を和暦(明石標準時)に変換して表示。書式は「ＧＧ YY 年 MM 月 DD 日」(ＧＧは元号、時分秒は表示せず。)
8	有効期間の満了日		notAfter	
9	発行者	IssuerAlt-Name	Organizational-UnitName	設定値をそのまま表示。

※1 代替文字の設定ルール

(ｉ) 表記ルール

1. 代替文字を”1”、それ以外を”0”で表現する。
2. スペースも 1 文字として捉え、ルール 1 を適用する。

(ⅱ)表記例

項目名	設定値	代替文字使用位置の値	説明
氏名	吉田△太郎	10000	氏名の長さは 5 文字 1 文字目の「吉」が代替文字
住所	東京都葛飾区ｘｘｘ	000100000	住所の長さは 9 文字 4 文字目の「葛」が代替文字

△は全角スペース

※2 生年月日の設定ルール

(ｉ) コード体系

英数字型 9 桁 EYYYYMMDD

E ：年号コード 1 桁（1:明治 2:大正 3:昭和 4:平成）

YYYY ：西暦年 4 桁

MM ：月 2 桁（01～12:1 月～12 月 00:不明 A1:春 A2:夏 A3:秋 A4:冬）

DD ：日 2 桁（01～31:1 日～31 日 00:不明 A1:上旬 A2:中旬 A3:下旬）

(ⅱ) 表記例

例	生年月日の値	表 記
通常	420030401	平成 15 年 4 月 1 日
年号のはざまの日	219261225	大正 15 年 12 月 25 日
	319261225	昭和元年 12 月 25 日
年月日不明	000000000	
月日不明	319260000	昭和元年
	31926A100	昭和元年春
日不明	319261200	昭和元年 12 月
	3192612A2	昭和元年 12 月中旬

※3 性別の設定ルール

(ｉ) コード体系

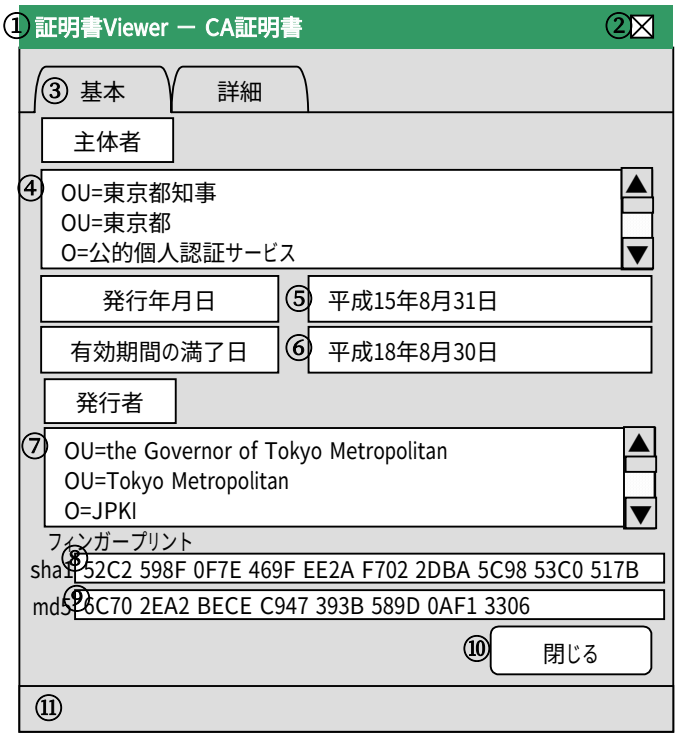
英数字型 1 桁 X

X ：性別コード 1 桁 (1:男 2:女 3:不明)

（2） CA 証明書

画面名	CA 証明書基本画面
概要	CA 証明書の基本情報を表示する。

画面レイアウト



表示項目証明書領域の対応は、表 ６．３を参照。

画面項目説明

NO	項目名	概要
①	タイトルバー	表示する電子証明書の種類を表示する。 表示テキストは「証明書 Viewer－CA 証明書」とする。
②	終了ボタン	証明書 Viewer を閉じる。
③	タブ	基本画面と詳細画面を切り替える。
④	主体者	主体者を表示する。 設定値が１行で収まらない場合は、折り返して表示する。
⑤	発行年月日	電子証明書の発行年月日を和暦で表示する。
⑥	有効期間の満了日	電子証明書の有効期間の満了日を和暦で表示する。
⑦	発行者	電子証明書の発行者を表示する。 設定値が１行で収まらない場合は、折り返して表示する。
⑧	sha1	電子証明書の「sha1」ハッシュ値を表示する。
⑨	md5	電子証明書の「md5」ハッシュ値を表示する。
⑩	閉じるボタン	証明書 Viewer を閉じる。
⑪	ステータスバー	使用せず。

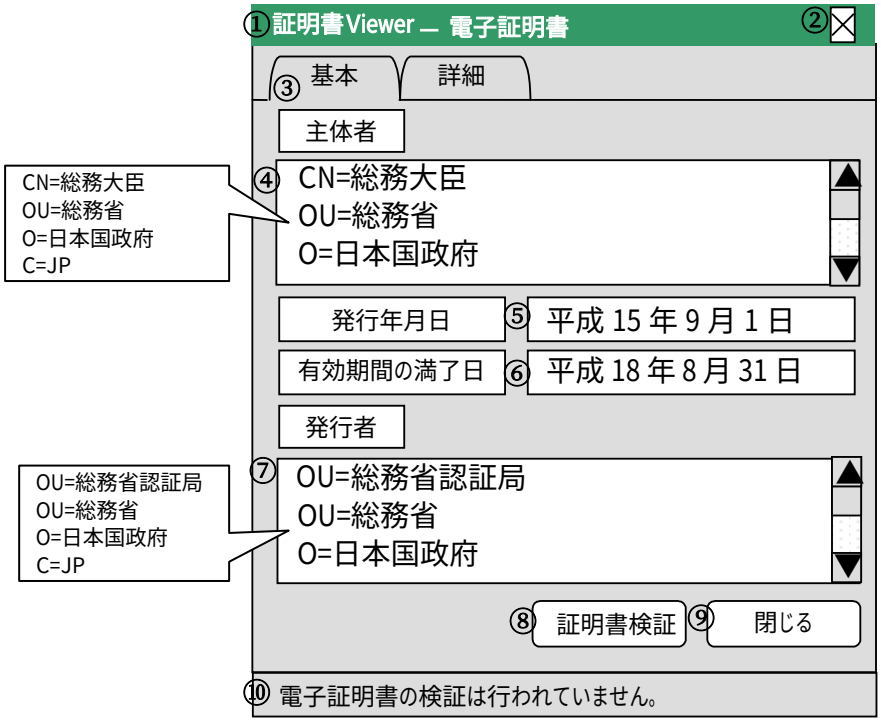
表 6.3 表示項目と証明書領域の対応（CA 証明書）

項番	項目名	証明書の項目名		表示方法
		上位項目名	項目名	
1	主体者	SubjectAlt-Name または Subject	CountryName OrganizationName OrganizationalUnitName OrganizationalUnitName 例) 都道府県知事の自己署名証明書の場合	SubjectAltName の DN を全て表示。DN は属性毎に改行して表示し、「(属性名の略語)＝(設定値)」にて表記。 subjectAltName に記述がない場合は subject を表示。
2	発行年月日	Validity	notBefore	設定値を和暦(明石標準時)に変換して表示。書式は「ＧＧ YY 年 MM 月 DD 日」(ＧＧは元号、時分秒は表示せず。)
3	有効期間の満了日		notAfter	
4	発行者	IssuerAlt-Name または Issuer	CountryName OrganizationName OrganizationalUnitName OrganizationalUnitName 例) 都道府県知事の自己署名証明書の場合	IssuerAltName の DN を全て表示。DN は属性毎に改行して表示し、「(属性名の略語)＝(設定値)」にて表記。 issuerAltName に記述がない場合は issuer を表示。
5	フィンガープリント	－	－	電子証明書のハッシュ値を計算して表示。ハッシュ関数は「sha1」と「md5」を使用する。

（3） 電子証明書

画面名	電子証明書基本画面
概要	利用者証明書、CA 証明書以外の電子証明書の基本情報を表示する。

画面レイアウト



表示項目と証明書領域の対応は、表 ６.４を参照。

画面項目説明

NO	項目名	概要
①	タイトルバー	表示する電子証明書の種類を表示する。 表示テキストは「証明書 Viewer－電子証明書」とする。
②	終了ボタン	証明書 Viewer を閉じる。
③	タブ	基本画面と詳細画面を切り替える。
④	主体者	主体者を表示する。 設定値が１行で収まらない場合は、折り返して表示する。(単語途中であっても折り返しを行う仕様とする。)
⑤	発行年月日	電子証明書の発行年月日を和暦で表示する。
⑥	有効期間の満了日	電子証明書の有効期間の満了日を和暦で表示する。
⑦	発行者	電子証明書の発行者を表示する。 設定値が１行で収まらない場合は、折り返して表示する。(単語途中であっても折り返しを行う仕様とする。)
⑧	証明書検証ボタン[*1]	[証明書検証]ボタンを押下することによって、公的個人認証サービス AP の官職証明書検証機能を呼び出し、官職証明書検証サービスに証明書検証の問い合わせを行う。 官職証明書検証機能の戻り値を判断して官職証明書・職責証明書検証ダイアログを表示する。
⑨	閉じるボタン[*1]	証明書 Viewer を閉じる。

⑩	ステータスバー	証明書検証状態を以下のように表示する。 検証前：電子証明書の検証は行われていません。 検証後：証明書検証結果「有効」 証明書検証結果「無効（xxx)」 証明書検証結果「検証失敗（xxx)」 「xxx」は原因を示すエラーコード。詳細は、表 ６.７、表 ６.８を参照。

（＊１）証明書検証処理中は、非活性状態となる。

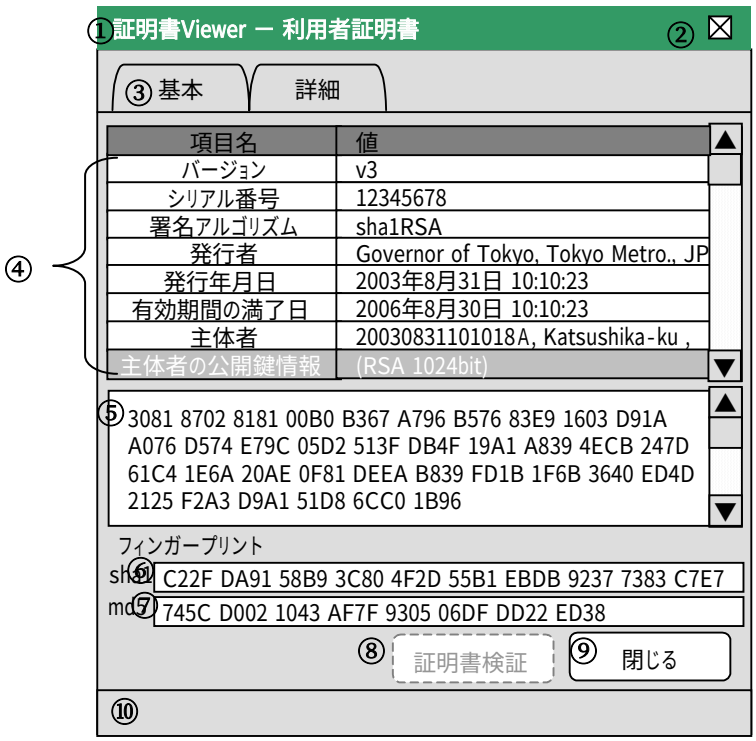
表 ６.４ 表示項目と証明書領域の対応（官職証明書／職責証明書／その他の証明書）

項番	項目名	証明書の項目名		表示方法
		上位項目名	項目名	
1	主体者	SubjectAlt-Name または Subject	CountryName OrganizationName OrganizationalUnitName CommonName 例)官職証明書の場合	SubjectAltName の DN を全て表示。 DN は属性毎に改行して表示し、「(属性名の略語)＝(設定値)」にて表記。subjectAltName に記述がない場合は subject を表示。
2	発行年月日	Validity	notBefore	設定値を和暦(明石標準時)に変換して表示。書式は「ＧＧ YY 年 MM 月 DD 日」(ＧＧは元号、時分秒は表示せず。)
3	有効期間の満了日		notAfter	
4	発行者	IssuerAlt-Name または Issuer	CountryName OrganizationName OrganizationalUnitName OrganizationalUnitName 例)官職証明書の場合	IssuerAltName の DN を全て表示。 DN は属性毎に改行して表示し、「(属性名の略語)＝(設定値)」にて表記。issuerAltName に記述がない場合は issuer を表示。

（4） 詳細画面

画面名	詳細画面
概要	電子証明書内の全ての記載事項を表示する。

画面レイアウト



表示項目と証明書領域の対応は、表 ６．５、表 ６．６を参照。

画面項目説明

NO	項目名	概要
①	タイトルバー	表示する電子証明書の種類を表示する。 表示テキストは「証明書 Viewerー利用者証明書／CA 証明書／電子証明書」とする。
②	終了ボタン	証明書 Viewer を閉じる。
③	タブ	基本画面と詳細画面を切り替える。
④	設定値の簡易表記	電子証明書内の記載事項を表示する。 フィールドにて、表示しきれないものは、縦スクロールバー、横スクロールバーを移動することによって表示する。 フィールド名と値の詳細は、「表 ６．５ 項目名と証明書基本領域との対応」と「表 ６．６ 項目名と証明書標準拡張領域との対応」の簡易表記を参照。
⑤	設定値の詳細表記	選択したフィールドの設定値を表示する。 折り返し表示とし、横スクロールバーは表示しない。 フィールド名と値の詳細は、「表 ６．５ 項目名と証明書基本領域との対応」と「表 ６．６ 項目名と証明書標準拡張領域との対応」の詳細表記を参照。
⑥	sha1	電子証明書の「sha1」ハッシュ値を表示する。
⑦	md5	電子証明書の「md5」ハッシュ値を表示する。

⑧	証明書検証ボタン	電子証明書の場合のみ表示する。 （証明書検証機能については、（３）電子証明書の画面項目説明を参照。）
⑨	閉じるボタン	証明書 Viewer を閉じる。
⑩	ステータスバー	電子証明書の場合のみ表示する。 （ステータスバーの概要については、（３）電子証明書の画面項目説明を参照。）

表 ６.５ 項目名と証明書基本領域との対応

NO	項目名	証明書の項目名		表示方法	
		上位項目名	項目名	簡易表記	詳細表記
1	バージョン	version		Version 表記。Version3 は“V3”とする。	
2	シリアル番号	serialNumber		設定値をそのまま表示。	
3	署名アルゴリズム	signature	algorithm parameters	algorithm の OID を RFC の規定値に変換した値。	
4	発行者	issuer	countryName organizationName organizationalUnitName 等	DN をカンマ区切り表示。「(設定値)，(設定値),･･･」。	DN を属性毎に改行。各行は「(属性の略語)=(設定値)」にて表記。 <属性の略語> 「countryName」 →C 「organizationName」 →O 「organizationalUnitName」 →OU
5	発行年月日	Validity	notBefore	設定値を西暦（明石標準時）で表示。書式は「YYYY 年 MM 月 DD 日 hh 時 mm 分 ss 秒」。	
6	有効期間の満了日		notAfter		
7	主体者[*1]	subject	countryName localityName commonName 等	DN をカンマ区切り表示。「(設定値)，(設定値)，･･･」。 commonName が 発行要求発生時刻の場合は、設定値をそのまま表示。	DN を属性毎に改行。各行は「(属性の略語)=(設定値)」にて表記。 <属性の略語> 「countryName」 →C 「localityName」 →L 「commonName」 →CN commonName が 発行要求発生時刻の場合は、設定値をそのまま表示。
8	発行申請送信時刻[*1]	subject	commonName	CN のみを表示対象とする。CN の発行申請送信時刻を設定値のまま表示。	

9	受付端末識別記号*1			CN のみを表示対象とする。CN の受付端末番号を設定値のまま表示。	
10	主体者の公開鍵情報	subjectPublicKeyInfo	algorithm	暗号アルゴリズムと鍵長を表示。書式は「(algorithm の OID を RFC の規定値に変換した値)＋(鍵長)Bits」。	SubjectPublicKey の設定値（１６進数）をそのまま表示。
			subjectPublicKey		
11	発行者ユニーク識別子	issuerUniqueID		設定値をそのまま表示。	
12	主体者ユニーク識別子	subjectUniqueID		設定値をそのまま表示。	

*1：利用者証明書の場合、commonName を「発行申請送信時刻」／「受付端末識別記号」に分けて表示する。利用者証明書以外は、「主体者」で表示する。

表 ６.６ 項目名と証明書標準拡張領域との対応

NO	項目名	証明書の項目名		表示方法	
		上位項目名	項目名	簡易表記	詳細表記
1	認証局鍵識別子	AuthorityKeyIdentifier	keyIdentifier authorityCertIssuer authorityCertSerialNumber	AuthorityKeyIdentifier の情報を項目毎にカンマ区切り表示。なお、表示の際は以下のルールを適用する。 ・項目名は英語のまま。 ・OID は RFC の規定値に変換。	AuthorityKeyIdentifier の情報を項目毎に階層表示。なお、表示の際は以下のルールを適用する。 ・項目名は英語のまま。 ・OID は RFC の規定値に変換。 ・DN は属性毎に改行。
2	鍵用途	KeyUsage	digitalSignature nonRepudiation keyEncipherment dataEncipherment keyAgreement keyCertSign cRLSign encipherOnly decipherOnly	KeyUsage の情報を項目毎にカンマ区切り表示。なお、表示の際は以下のルールを適用する。 ・項目名は英語のまま。 ・OID は RFC の規定値に変換。 ・KeyUsage のビット列は、鍵用途の英語名に変換してカンマ区切り表示。	KeyUsage の情報を項目毎に階層表示。なお、表示の際は以下のルールを適用する。 ・項目名は英語のまま。 ・OID は RFC の規定値に変換。 ・KeyUsage のビット列は、鍵用途の英語名に変換してカンマ区切り表示。

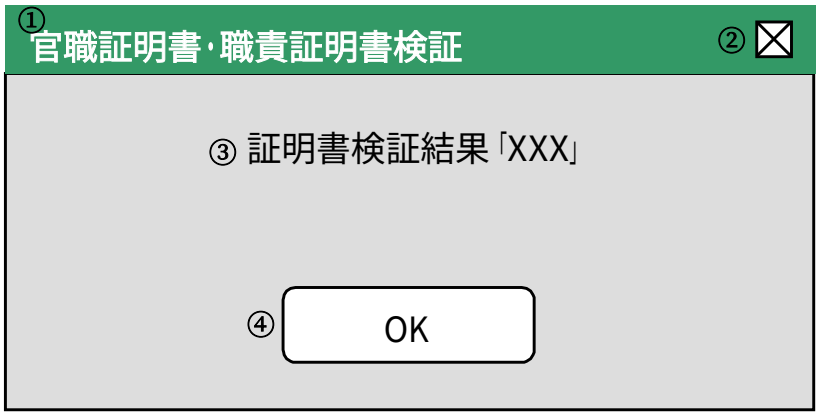
3	主体者代替名	SubjectAltName	countryName organizationName organizationalUnitName 等	SubjectAltName の情報を項目毎にカンマ区切り表示。なお、表示の際は以下のルールを適用する。 ・項目名は英語のまま。 ・OID は RFC の規定値に変換。	SubjectAltName の情報を項目毎に階層表示。なお、表示の際は以下のルールを適用する。 ・項目名は英語のまま。 ・OID は RFC の規定値に変換。
4	発行者代替名	issuerAltName	countryName organizationName organizationalUnitName 等	issuerAltName の情報を項目毎にカンマ区切り表示。なお、表示の際は以下のルールを適用する。 ・項目名は英語のまま。 ・OID は RFC の規定値に変換。	issuerAltName の情報を項目毎に階層表示。なお、表示の際は以下のルールを適用する。 ・項目名は英語のまま。 ・OID は RFC の規定値に変換。
5	基本制約	BasicConstrains	cA pathLenConstraint	BasicConstrains の情報を項目毎にカンマ区切り表示。なお、表示の際は以下のルールを適用する。 ・項目名は英語のまま。 ・OID は RFC の規定値に変換。	BasicConstrains の情報を項目毎に階層表示。なお、表示の際は以下のルールを適用する。 ・項目名は英語のまま。 ・OID は RFC の規定値に変換。
6	CRL 分配点	CRLDistributionPoints	countryName organizationName organizationalUnitName 等	CRLDistributionPoints の情報を項目毎にカンマ区切り表示。なお、表示の際は以下のルールを適用する。 ・項目名は英語のまま。 ・OID は RFC の規定値に変換。	CRLDistributionPoints の情報を項目毎に階層表示。なお、表示の際は以下のルールを適用する。 ・項目名は英語のまま。 ・OID は RFC の規定値に変換。 ・DN は属性毎に改行。
7	証明書ポリシー	CertificatePolicies	policyIdentifier policyQualifiers	CertificatePolicies の情報を項目毎にカンマ区切り表示。なお、表示の際は以下のルールを適用する。 ・項目名は英語のまま。 ・OID は RFC の規定値に変換。	CertificatePolicies の情報を項目毎に階層表示。なお、表示の際は以下のルールを適用する。 ・項目名は英語のまま。 ・OID は RFC の規定値に変換。

8	主体者鍵識別子	SubjectKeyIdentifier	keyIdentifier	SubjectKeyIdentifier の情報を項目毎にカンマ区切り表示。なお、表示の際は以下のルールを適用する。 ・項目名は英語のまま。 ・OID は RFC の規定値に変換。	SubjectKeyIdentifier の情報を項目毎に階層表示。なお、表示の際は以下のルールを適用する。 ・項目名は英語のまま。 ・OID は RFC の規定値に変換。
9	拡張鍵用途	ExtKeyUsage	serverAuth clientAuth codeSigning emailProtection ipsecEndSystem ipsecTunnel ipsecUser timeStamping	ExtKeyUsage の情報を項目毎にカンマ区切り表示。なお、表示の際は以下のルールを適用する。 ・項目名は英語のまま。 ・OID は RFC の規定値に変換。	ExtKeyUsage の情報を項目毎に階層表示。なお、表示の際は以下のルールを適用する。 ・項目名は英語のまま。 ・OID は RFC の規定値に変換。

（５） 官職証明書・職責証明書検証画面

画面名	官職証明書・職責証明書検証画面
概要	電子証明書（基本／詳細）画面にて、[証明書検証]ボタンを押下し、証明書検証を行い、証明書検証結果を表示する。

画面レイアウト



画面項目説明

NO	項目名	概要
①	タイトルバー	表示する電子証明書の種類を表示する。 表示テキストは「官職証明書・職責証明書検証」とする。
②	終了ボタン	官職証明書・職責証明書検証画面を閉じる。
③	証明書検証結果	証明書検証が終了した場合、以下のメッセージを表示する。 証明書が有効の場合：証明書検証結果「有効」 証明書が無効の場合：証明書検証結果「無効（xxx）」 （無効の場合とは、証明書検証結果が失敗した場合を示す。） 証明書検証処理が失敗した場合 ：証明書検証結果「検証失敗（xxx）」 （検証失敗とは、証明書検証が行えなかった場合を示す。） 「xxx」は原因を示すエラーコード。詳細は、表 ６.７、表 ６.８を参照。
④	ＯＫボタン	官職証明書・職責証明書検証画面を閉じる。

＜メッセージの詳細＞

表 6.7 証明書検証結果「無効」の場合のエラーコード一覧

NO	エラーコード	内容	意味
1	100101	認証パス構築不可(101)	認証パス構築ができないこと。
2	100202	署名不正(202)	認証パスに署名が不正である証明書が含まれていること。
3	100203	失効証明書を含む(203)	認証パスに失効した証明書が含まれていること。
4	100204	ポリシ不一致(204)	認証パスにポリシが一致しない証明書が含まれていること。
5	100205	制約違反(205)	認証パスに制約に違反している証明書が含まれていること。
6	100206	OCSP での証明書検証確認不正(206)	認証パスに OCSP での certStatus が unknown と応答される証明書が含まれていること。
7	100901	要求受付け拒否(901)	証明書検証サーバ側で要求の受け付が拒否されたこと。

注：( )中のコードは certPathStatus を示す。

表 6.8 証明書検証結果「検証失敗」の場合のエラーコード一覧

NO	エラーコード	内容	意味
1	100902	タイムアウト(902)	要求がタイムアウトとなったこと。( )中のコードは certPathStatus を示す。
2	200100	署名検証失敗	受信した OCSP レスポンスデータが改竄されていること。
3	200200	証明書が改竄または、有効期限切れ	OCSP レスポンスに付与されている電子証明書が改竄または有効期限切れである。
4	300100	接続失敗	ネットワークの問題で通信できなかった。 LAN 環境からプロキシサーバを使用している場合は、Internet Explorer の LAN の設定又は、環境設定ファイルのプロキシ情報の指定に誤りがある。
5	300200	拡張領域の解析に失敗	証明書検証サーバ（CVS）に接続していない。 環境設定ファイルの CVS 接続先 URL をもう一度見直してください。
6	300300	その他のエラー発生のため証明書検証の確認不可	・ 環境設定ファイルに CVS 接続先 URL が指定されていない又は、環境設定ファイルが存在しない。 ・ その他の内部エラーが発生。
7	300400	証明書の取得失敗	・ IC カードの PIN 入力でキャンセルされた場合。 ・ IC カードリーダライタに IC カードがセットされていない場合。 ・ IC カードリーダライタが PC に接続されて

NO	エラーコード	内容	意味
			いない場合。
8	400001	OCSP Request のフォーマットエラー(1)	レスポンダで例外が発生 ・ 検証要求を行う証明書検証サーバ（CVS）の検証依頼者認証が必要であるか確認してください。 ・ 署名に使用した電子証明書が X.509 バージョン 3 の電子証明書であるかを確認してください。
9	400002	内部エラー (2)	
10	400003	一時的な解答不能(3)	
11	400005	OCSP Request への署名が必要(5)	
12	400006	クライアントが認証されていない(6)	

注：( )中のコードは responseStatus を示す。

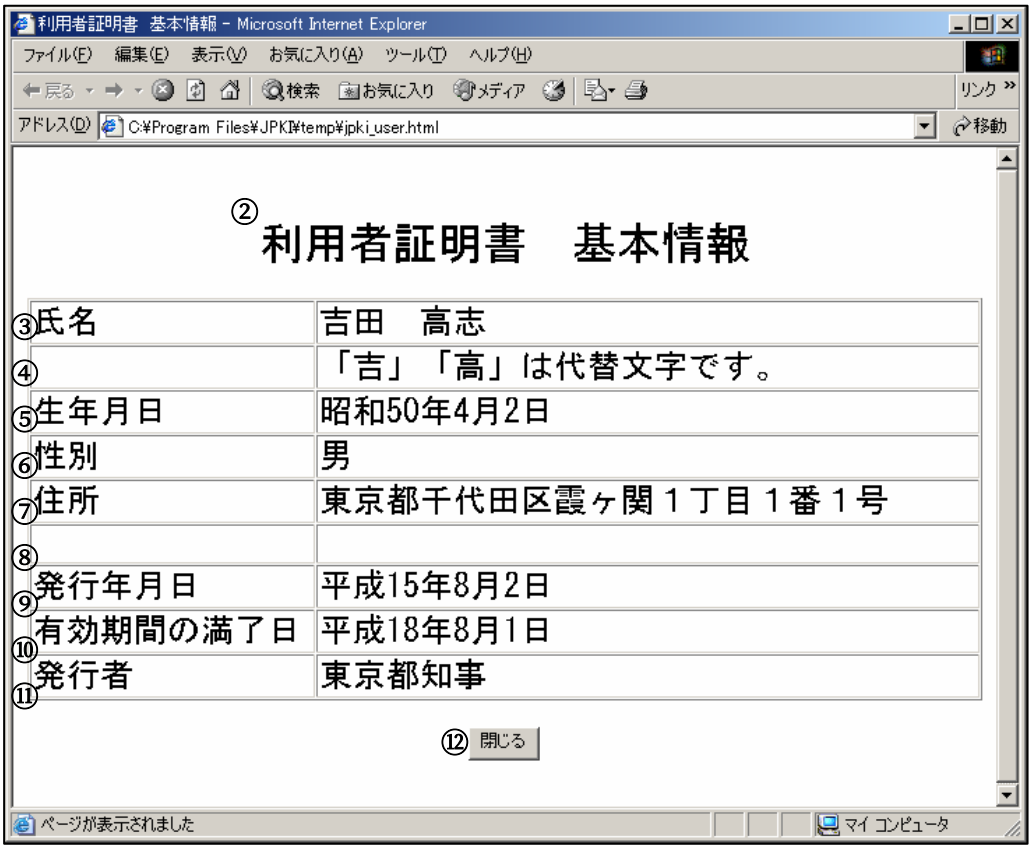
（６） 利用者証明書　基本情報画面（HTML）

画面名	利用者証明書　基本情報画面（HTML）
概要	利用者証明書基本画面にて、[HTML 表示]ボタンを押下した場合、HTML 表示にて利用者証明書基本情報画面を表示する。

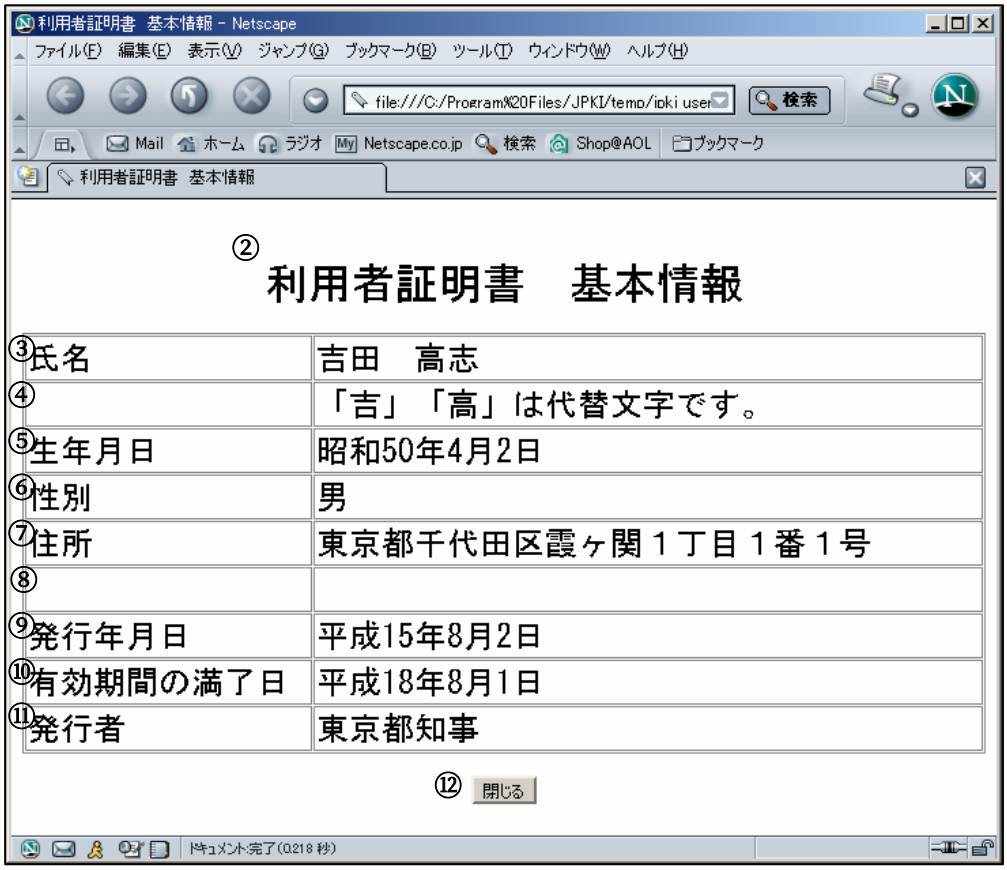
画面レイアウト

＜Internet Explorer の場合＞

①



＜Netscape の場合＞



画面項目説明		
NO	項目名	概要
①	タイトルバー	表示する電子証明書の種類を表示する。 表示テキストは「利用者証明書　基本情報-（ブラウザ名称）」とする。
②	タイトル	タイトルを表示する。 表示テキストは「利用者証明書　基本情報」とする。
③	氏名	利用者の氏名を表示する。最大 100 文字まで表示可能。
④	代替文字の使用（氏名）	氏名の代替文字を表示する。最大 100 文字まで表示可能。代替文字がない場合は、表示しない。
⑤	生年月日	利用者の生年月日を和暦で表示する。
⑥	性別	利用者の性別（男/女/不明）を表示する。
⑦	住所	利用者の住所を表示する。最大 200 文字まで表示可能。
⑧	代替文字の使用（住所）	住所の代替文字を表示する。最大 200 文字まで表示可能。代替文字がない場合は、表示しない。
⑨	発行年月日	電子証明書の発行年月日を和暦で表示する。
⑩	有効期間の満了日	電子証明書の有効期間の満了日を和暦で表示する。
⑪	発行者	電子証明書の発行者を表示する。
⑫	閉じるボタン	ブラウザを閉じる。

表示項目と証明書領域の対応（利用者証明書）については、表 ６．２ 表示項目と証明書領域の対応（利用者証明書）を参照。

禁・無断転載

公的個人認証サービス

利用者クライアントソフト API 仕様書
【個人認証サービス AP C 言語インターフェース編】

第１.１版

（注意事項）

※利用者クライアントソフトの著作権は、総務省が保有しており、国際著作権条約及び日本国の著作権関連法令によって保護されています。

※総務省は、利用者が利用者クライアントソフトを利用したことにより発生した利用者の損害及び利用者が第三者に与えた損害について、一切の責任を負いません。

※利用者クライアントソフトの利用に当たっては、次に掲げる行為を禁止します。

（1） 利用者クライアントソフトを電子申請・届出等の行政手続等以外の目的で利用すること。

（2） 利用者クライアントソフトに対し、総務省に許可なく改造等を行うこと。