4 用語集

通番	用　語	解　説
1	CP/CPS (Certificate Policy / Certification Practice Statement)	認証局の運用方式、信頼性・安全性を対外的に示す文書のこと。 CPは認証局が電子証明書を発行する際の運用方針を定めた証明書ポリシーを指し、CPSは運用方針の実施手順を定めた認証局運用規程を指す。
2	e-文書法	“e-Japan重点計画2004”での「IT 規制改革の推進」政策を受け、2005年に施行された規制緩和の法律。従来、書面による保存が義務付けられていた書類を、原則、電子で保存することを容認した法律。関連分野は、税務、医療、建築、会社法など広範囲に及び、300本以上の法律が関係するが、特に、国税、医療関連文書などのスキャナー保存の容認が有名。通則法となる「民間事業者などが行う書面の保存などにおける情報通信の技術の利用に関する法律」と、その整備などに関する法律の２本からなる。「電子文書法」ともいう。
3	IT基本法	正式名称を「高度情報通信ネットワーク社会形成基本法」といい、情報施策に対する国および地方公共団体の責務を定めた法律。
4	IT書面一括法	正式名称を「書面の交付などに関する情報通信の技術の利用のための関係法律の整備に関する法律」といい、書面の交付や書面による手続きを義務付けている法律を改正し、電子的手段（電子メールやWebなど）も認めることで電子商取引の促進を狙った法律。 ただし、特定の法律（公正証書が必要なものなど）については従来どおり書面を必要とする規制が残っているものもある。
5	PDF (Portable Document Format)	アドビシステムズ社が開発したファイルフォーマット。作成したドキュメントを異なるパソコン環境で元のレイアウトどおりに表示・印刷可能な特性を持つ。2008年７月に国際規格（ISO32000-1）として認定されている。
6	PL法	正式名称を「製造物責任法」といい、製造物の欠陥により人の生命、身体又は財産に係る被害が生じた場合における製造業者などの損害賠償の責任について定めた法律。
7	RSA1024 / RSA2048	公開鍵暗号方式であるRSA暗号において処理の際に用いる鍵のデータ長の規格の一つ。 鍵のデータ長が長いほど暗号の強度が高く安全とされ、RSA1024からRSA2048への移行が進められている。

通番	用　語	解　説
8	S / MIME	公開鍵暗号方式による電子メールの暗号化と電子署名に関する標準規格。
9	SHA-1 / SHA-2	暗号処理の際に使用されるハッシュ関数（一方向関数）の一つ。SHA-1の生成するハッシュ値は160ビット、SHA-2の場合は224 ～ 512ビットである。 一般的にハッシュ値が長いほど安全とされ、SHA-1からSHA-2への移行が進められている。 なお、SHA-2はSHA-224、SHA-256、SHA-384、SHA-512の４種類の総称である。
10	SSL	インターネット上でデータを暗号化して通信する技術、取り決め。通信者は電子証明書を参照することによって通信先を確認することができ、通信データは電子証明書による暗号化通信によって第三者からの盗聴や改ざんから守られる。
11	XML （Extensible Markup Language）	属性と値で構成された論理性と拡張性に優れたファイルフォーマット。コンピュータ側で処理することに適した特性を持つ。
12	クライアント証明書	特定の個人や機器などに発行される電子証明書。ユーザー認証や電子署名の付与、データの暗号化などに利用される。
13	サーバ証明書	サーバを対象に発行される電子証明書。サーバ証明書によって、サーバの正当性を証明するとともに、サーバとクライアントPC間で情報を送信する際の暗号化通信にも利用される。Webサイトで利用されるSSLサーバ証明書が代表例。
14	タイムスタンプ	ある時刻にある電子データが存在していたことを証明する「存在証明」と、ある時刻以降電子データの内容が改ざんされていないことを証明する「完全性証明」を実現する仕組みのこと。この証明となる電子データをタイムスタンプトークンというが、これをタイムスタンプと略して呼ぶことも多い。「時刻認証」ともいう。
15	タイムスタンプ局	電子署名などの手段でタイムスタンプの付与およびタイムスタンプの有効性を保証する機関。電子データの「存在証明」と「完全性証明」を実現する上で重要な役割を果たす。 「時刻認証局」ともいう。
16	ハッシュ値	数値や文字列のデータをハッシュ関数によって一定の長さに変換した値。 ハッシュ関数とは擬似乱数を生成する一方向関数で、ハッシュ値の逆算や偽造は極めて困難とされる。

通番	用　語	解　説
17	パブリック認証局／ パブリック証明書	不特定多数の広範囲に電子証明書を発行する電子認証局のこと。利用者または電子証明書を受け取った相手は公開されているCP/CPSの内容を確認し、信頼できる電子認証局か判断し利用する。 電子署名法上の特定認証業務の認定制度やWebtrust制度など外部機関の監査を受けることで電子認証局としての信頼性は高くなる。
18	フィンガープリント	電子証明書の正当性を証明するデータ。電子証明書内のフィンガープリント（拇印）と別途認証局側で公開しているフィンガープリントを照合し一致すれば正しい証明書と確認できる。
19	プライベート認証局／ プライベート証明書	企業内などの限られた場所や特定の相手など限られた範囲に電子証明書を発行する電子認証局のこと。対象者内でルールを守って利用されればよいためCP/CPSを公開しない場合もある。
20	ブリッジ認証局	政府認証基盤（GPKI）や地方公共団体組織認証基盤（LGPKI）を構成する認証局の一つで、行政機関側認証局と外部の認証局との中間に位置し、それぞれと相互認証することで橋渡しを行う電子認証局のこと。
21	ヘルスケアPKI	厚生労働省が保健医療福祉分野で用いる電子証明書を標準化するために推進する公開鍵基盤。医療従事者の国家資格属性を証明書に記入することができるので、“医師が電子署名したもの”であることなどが検証可能となる。
22	リポジトリ	電子認証局を構成する要素の一つであり、CP/CPSや失効リストなどの情報公開を行うサービス。
23	ルート証明書 （自己署名証明書）	ルート認証局が自身の正当性を証明するために発行する電子証明書で自己署名証明書ともいう。 利用者の電子証明書内部にはルート証明書への経路情報が存在し、利用者の電子証明書の信頼性を確認する場合にルート証明書によって確認する。 なお、この時信頼の起点となるルート証明書のことをトラストアンカーと呼ぶ。
24	ルート認証局	他の上位の認証局から証明書を受けない最上位の認証局。利用者の証明書の認証パスの最上位に位置し、トラストアンカーとなるルート証明書を発行したり、他の中間認証局に対して証明書を発行する。ルート認証局は利用者証明書の信頼の拠り所になるため、信頼するに足りるセキュリティの高い運用を行い、その基準をCP/CPSなどで開示して証明書利用者の信頼を得る必要がある。 なお、InternetExplorerなどのブラウザーに証明書が格納されているルート認証局をパブリックルート認証局と呼ぶこともある。

通番	用　語	解　説
25	暗号アルゴリズム	暗号化する際の手順・方式。
26	原本性保証	複製ではなく本人が作成し以後改ざんされていない原本であることを保証すること。 電子文書においては電子署名とタイムスタンプを組み合わせることにより、本人が作成し以後改ざんされていないことを証明できる。
27	公開鍵	公開鍵暗号方式で使用される一対の鍵の一つで、一般に公開される鍵。公開鍵は秘密鍵とは異なり、他人に知られても悪用されるおそれはない。秘密鍵で暗号化されたデータは一対の公開鍵でのみ復号可能となるので、電子署名の検証に用いる。一方、公開鍵で暗号化されたデータは一対の秘密鍵でのみ復号可能となるので、特定の人にだけデータを渡す際の暗号化に用いられる。
28	公的個人認証サービス（JPKI）	住民基本台帳に記載されている者（日本国内に住所のある日本国民）を対象に、各都道府県から住民基本台帳カードに格納される形で電子証明書が発行される。 電子証明書は政府機関や各地方公共団体への電子申請・届出などの行政手続に利用できる。
29	公的個人認証法	正式名称を「電子署名に係る地方公共団体の認証業務に関する法律」といい、申請・届出などの行政手続をオンラインでできるようにするための公的個人認証サービス（JPKI）制度を規定した法律。
30	失効リスト	電子証明書の失効情報を掲載するリストで「ARL（Authority Revocation List）」と「CRL（Certificate Revocation List）」の２種類ある。 ARLは認証局自身の電子証明書の失効情報を掲載し、CRLは認証局が発行した電子証明書の失効情報を掲載する。
31	商業登記電子証明書	法人を対象に、法務省の電子認証登記所の登記官から発行される電子的な証明書。 従来の印鑑証明書・資格証明書によって確認している「本人性」、「法人格の存在」、「代表権限の存在」に代わるもので、印鑑登録された社印と同等の法的有効性が認められている。
32	商業登記法	商法や会社法の規定されている登記すべき事項の手続について定めた法律。 2000年４月に商業登記に基づく電子認証制度のための改正が行われた。
33	署名検証	電子署名の有効性を確認する行為。「電子署名が付与された電子データが改ざんされていないこと」「電子証明書が有効であること」「電子証明書の信頼性が確認されていること」などを確認する。

通番	用　語	解　説
		狭義の意味では、「電子署名が付与された電子データが改ざんされていないこと」のみ確認することを指し、「電子証明書が有効であること」「電子証明書の信頼性が確認されていること」は証明書検証として分けて扱われる。
34	政府認証基盤 （GPKI）	政府が運用する認証基盤で、官職認証局、アプリケーション認証局、ブリッジ認証局の３つの電子認証局から構成される。各認証局からは職責証明書、サーバ証明書、相互認証証明書などがそれぞれ発行される。
35	耐タンパ性	内部情報を不正に読み取られる・改ざんされることに対する耐性のこと。IC カードなど耐タンパ性が高い媒体は不正アクセスに対する強度が高いといえる。
36	地方公共団体組織 認証基盤 （LGPKI）	地方公共団体の認証基盤で、組織認証局、アプリケーション認証局、ブリッジ認証局の３つの電子認証局から構成される。各認証局からは職責証明書、サーバ証明書、相互認証証明書などがそれぞれ発行される。
37	中間認証局	ルート認証局が発行する電子証明書にて自身の正当性を証明する認証局。認証局としての信頼性がルート証明書によって示される点でルート認証局と異なる。
38	長期署名フォーマット	電子署名とタイムスタンプを組み合わせることで電子署名の検証期間を長期間に渡り維持する仕組み。 署名対象毎に 「CAdES（CMS Advanced Electronic Signatures）」、 「XAdES（XML Advanced Electronic Signatures）」、 「PAdES（PDF Advanced Electronic Signatures）」 の３種類あり、それぞれISO14533-1、ISO14533-2、ISO32000-2として国際規格化が進められている。
39	電子証明書	利用者の公開鍵が本人に帰属していることを証明するために認証局が発行する電子的な証明書。 「公開鍵証明書」ともいう。
40	電子署名	電子証明書を利用した暗号技術により、本人が作成したことを表し、かつ改ざんの有無が確認できるよう本人の秘密鍵で暗号措置された電子的な署名データ。
41	電子署名法	正式名称を「電子署名及び認証業務に関する法律」といい、電子署名の定義、電磁的記録の真正な成立の推定、特定認証業務の認定制度について定めた法律。 電子文書に対する電子署名が紙文書に対する署名や押印と同等の法的効力を持つと規定されている。

通番	用　語	解　説
42	電子帳簿保存法	正式名称を「電子計算機を使用して作成する国税関係帳簿書類の保存方法等の特例に関する法律」といい、従来紙での保存が義務付けられていた国税関係帳簿書類を、一定の要件を満たすことによって電子データとして保存することを容認した法律。
43	電子認証	インターネット等ネットワークを利用したやり取りにおいて、電子証明書を用いて本人性を証明する技術のこと。
44	電子認証局 （CA）	電子証明書の発行と失効を行う機関のことで、「CA（Certificate Authority）」ともいう。 登録局（RA）、発行局（IA）、リポジトリなどから構成される。
45	登録局 （RA）	電子認証局を構成する要素の一つであり、電子証明書発行ための審査・登録を行う機関のことで、「RA（Registration Authority）」ともいう。
46	特定認証業務	電子署名法上の技術的基準に準拠した認証業務のこと。
47	認証パス	利用者の電子証明書からルート証明書までの信頼の経路。 電子署名の有効性を検証する場合、この経路を元に電子証明書の信頼性を確認する。
48	認定認証業務	電子署名法上の技術的基準、設備基準、業務方法に関する基準などをクリアし、国が指定した調査機関の審査を受け認定された認証業務のこと。
49	発行局 （IA）	電子認証局を構成する要素の一つであり、電子証明書を発行する機関のことで、「IA（Issuing Authority）」ともいう。
50	秘密鍵	公開鍵暗号方式で使用される一対の鍵の一つで、利用者本人のみが保有し一般に公開されない鍵。秘密鍵が他人に知られると悪用されるおそれがあるため、厳重に管理する必要がある。秘密鍵は本人のみが所持するものなので電子署名に用いられる。 「私有鍵」ともいう。
51	復号	暗号化された暗号文を解いて元の平文に戻すこと。