資料２－１

保健医療福祉分野における
リモート署名サービスの評価基準(案)

目次

1. 総則

1.1 本評価基準の位置づけ

本評価基準は、保健医療福祉分野におけるリモート署名サービスの評価基準を定めるものである。本書では、1.4 節の図 1 で示すリモート署名サービスを構成する独立した複数のコンポーネントに対してそれぞれの要求事項を定めているため、評価基準は複数の文書から構成される。また、電子処方箋におけるリモート署名サービスのシステム構成と、図 1 との関係を同節の図 2 にて解説した。

1.2 本書のスコープ

本書は、リモート署名サービスを運営するトラストサービスプロバイダー（TSP）に対して、一般的に適用されるポリシーとセキュリティ要件を示し、これに基づいて保健医療福祉分野におけるリモート署名サービスの要件を規定した。なお、トラストサービスやリモート署名サービスのサービスコンポーネントを提供する事業者をトラストサービスプロバイダー（TSP）と呼ぶ。

本書の規定は 1.4 節で示したリモート署名サービスを構成する以下の2つのサービスコンポーネントのいずれにも適用される。

・サーバー署名アプリケーションサービスコンポーネント（SSASC）
　　サーバー署名アプリケーション（SSA）機能をサポートするサービスコンポーネント。
・デジタル署名生成アプリケーションサービスコンポーネント（SCASC）
　　デジタル署名生成アプリケーション（SCA）をサポートするサービスコンポーネント。

1.3 本書の目的

本書は、サーバー署名アプリケーションサービスコンポーネント（SSASC）、およびデジタル署名生成サービスコンポーネント（SCASC）のいずれか、または両方を提供する TSP が信頼できることを評価する適合性評価の基礎として、独立した組織が使用することを目的とする。

1.4 リモート署名サービスのアーキテクチャー

リモート署名サービスとは、リモート署名事業者のサーバーに署名者の署名鍵を設置・保管し、署名者の指示に基づきリモート署名サーバー上で自ら（署名者）の署名鍵で電子署名を行うサービス[1]であり、下記のコンポーネントから構成される。

① サーバー署名アプリケーション（SSA: Server Signing Application）
署名者の署名鍵を内蔵し署名演算を実施する署名値生成装置等（SCDev）を運用し、デジタル署名値を生成するアプリケーション。SSA は、署名者の直接の指示やデジタル署名生成アプリケーション（SCA）により仲介された指示により機能する。また、SSA は、署名者の認証情報や署名に用いる署名鍵を特定する情報、署名対象データのハッシュ値などを含む署名活性化データに基づきデジタル署名値を生成する。 SSA は電子署名値の生成に使用する署名鍵の生成、保持、ライフサイクル管理、使用などの機能を有する。署名者視点から見た場合、署名値生成装置等はリモート環境に設置されるため、リモート署名値生成装置等と呼ぶ場合がある。SSASC は、署名対象データのハッシュ値に基づいて生成された署名値を署名者または他アプリケーションに配信することを目的とする。SSA の機能を提供するサービスをサーバー署名アプリケーションサービスと呼ぶ。

② デジタル署名生成アプリケーション（SCA: Signature Creation Application）
CAdES/XAdES/PAdES 等、標準フォーマットに準拠したデジタル署名を構築するアプリケーション。署名者からの署名リクエストを受け取り、SSA に署名者、署名鍵、署名対象文書等を特定する情報（署名活性化デ

[1] 日本トラストテクノロジー協議会（JT2A）「リモート署名ガイドライン」より

ータ)を引き渡し、SSA によって生成されたデジタル署名値を利用してデジタル署名を生成する機能を有する。SCA の機能を提供するサービスをデジタル署名生成サービスと呼ぶ。

③ 本人認証サービス(Identification Authentication Service)
利用者の身元確認を実施し、必要に応じて電子識別手段(認証用秘密鍵やこれを格納する IC カードなどのデバイスなど)を発行し、オンラインで本人認証(Authentication)や認可(Authorization)を行うサービス。SSA 内に設置する場合と、外部事業者のサービスを利用する場合がある。

④ 署名者インタラクションコンポーネント(SIC: Signer Interaction Component)
署名者が SCA や SSA 等を利用してデジタル署名の生成を指示するためのユーザーインターフェースを提供するコンポーネント。

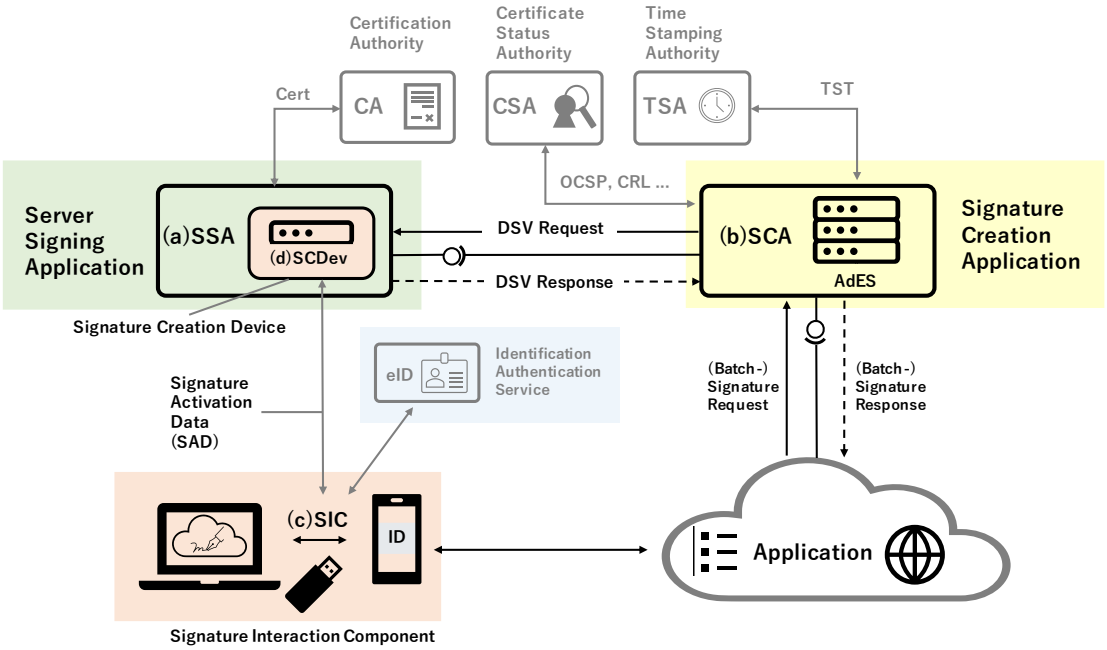

図1　リモート署名サービスのアーキテクチャー
（ETSI TS 119 432 V1.1.1　Figure2 を基に作成）

(a)　SSA：サーバー署名アプリケーション
(b)　SCA：デジタル署名生成アプリケーション
(c)　SIC：署名者インタラクションコンポーネント
(d)　SCDev:署名値生成装置等

上記の独立したアプリケーション（機能群）を実装するコンポーネントが事業者によりサービスとして提供される場合にはサービスコンポーネント（SC）と呼ぶ。また、それぞれのサービスコンポーネントは事業者により、単独または、複数組み合わせて提供される場合がある。このようなサービスコンポーネントを提供する事業者をサービスプロバイダー（SP）と呼び、ここで対象とするサービスプロバイダーは信頼ある第三者機関として一定のトラストサービスプロバイダーの要件を満たす必要がある。本基準群は SC および TSP の要件を定めるものである。

1.4.1 電子処方箋におけるリモート署名サービスのシステム構成

電子処方箋におけるリモート署名サービスのシステム構成との関係を示した図を以下に示す。

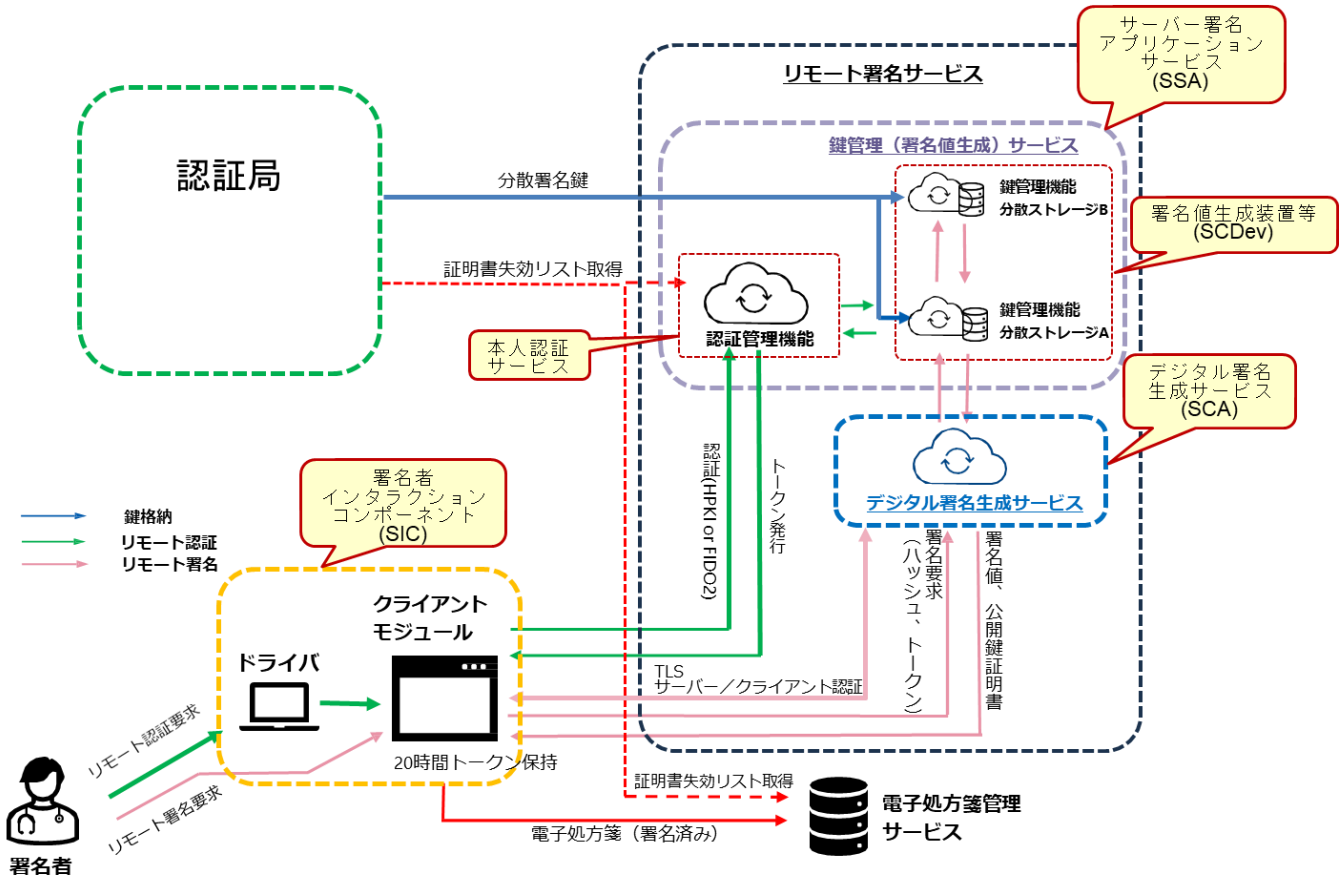

図 2　電子処方箋におけるリモート署名サービスのシステム構成

電子処方箋におけるリモート署名サービスの構成を前述した①～④と対応付けて説明する。

(1)　鍵管理(署名値生成)サービス:

署名値生成装置等に相当する「鍵管理機能　分散ストレージ A」と「鍵管理機能　分散ストレージ B」を内包し、デジタル署名生成サービスに中継された署名者の署名要求(署名対象のハッシュ値と認証により得られたトークンを含む SAD に相当するデータ)に基づき、署名値を生成するサービスで、「①サーバー署名アプリケーション」を管理・運用するサービス(サーバー署名アプリケーションサービス)に相当する。「鍵管理機能　分散ストレージ A」と「鍵管理機能　分散ストレージ B」は、認証局によって分散された署名鍵をそれぞれ保持し、まず A 側の分散署名鍵で署名対象のハッシュ値に演算を施すことによって署名値の分散片を生成し、次に A 側で生成した分散片に対して B 側の分散署名鍵で演算を施すことによって署名値を生成する。

なお、電子処方箋では③本人認証サービスに相当する認証管理機能も鍵管理(署名値生成)サービスに内包される。

(2)　デジタル署名生成サービス:

署名者からの要求に基づき、電子処方箋に対応する XAdES 形式のデジタル署名関連データを構築するサービスで、「②デジタル署名生成アプリケーション」を管理・運用するサービス(デジタル署名生成サービス)に相当する。このとき、デジタル署名値の生成は鍵管理(署名値生成)サービスに、上記 SAD に相当する署名要求を送付することにより要求する。また、電子処方箋のコンテンツと XAdES 形式のデジタル署名関連データの結合は、クライアントモジュールで行われる。

(3)　認証管理機能:

SSA 内に設置されるタイプの③本人認証サービスに相当する。Healthcare Public Key Infrastructure(以下、HPKI)によるユーザー認証と FIDO2 によるユーザー認証を行い、認証に成功した場合、電子処方箋の署名生成の

ための要求を 20 時間維持するトークンを発行する。また、署名生成の要求があった場合のトークンの検証も実施する。

なお、FIDO2 とは、パスワードを使わずに認証を行う認証方式の標準化を推進する業界団体である FIDO Alliance が 2018 年に制定した技術規格。指紋や顔、虹彩などを用いた生体認証を用いて認証器(Authenticator)と呼ばれる FIDO 対応デバイスで認証を行い、認証結果をサービス側で持つ FIDO サーバーへ送信することでログインを行う方式である。

(4) クライアントモジュール(及びドライバ):

署名者が電子処方箋に署名を付与するための指示を行うモジュールで、④署名者インタラクションコンポーネントに相当する。クライアントモジュールそのものの TLS によるクライアント認証、HPKI あるいは FIDO2 によるユーザー認証、発行されたトークンの保持、署名要求の送付、XAdES 形式のデジタル署名関連データの受信、XAdES 形式のデジタル署名関連データとコンテンツを結合することによる署名付電子処方箋の構築等を実施する。

1.4.2 電子処方箋における利用登録のフロー

署名者がリモート署名サービスの利用申し込みを行い、登録が終了するまでのエンロールメントプロセスについて FIDO2 認証を用いる場合を例にとり下記のシーケンス図に示す。ここでは、次の 2 種類の鍵ペアを用いる。

主鍵ペア :HPKI 認証局により生成され、IC カード(HPKI カード)に格納される署名用、認証用の私有鍵、および、対応する証明書に格納される公開鍵。

2nd 鍵ペア:HPKI 認証局により生成され、鍵管理(署名値生成)サービスにエキスポートされる署名用の私有鍵(以下、署名鍵)と対応する証明書に格納される公開鍵。リモート署名に用いられる。

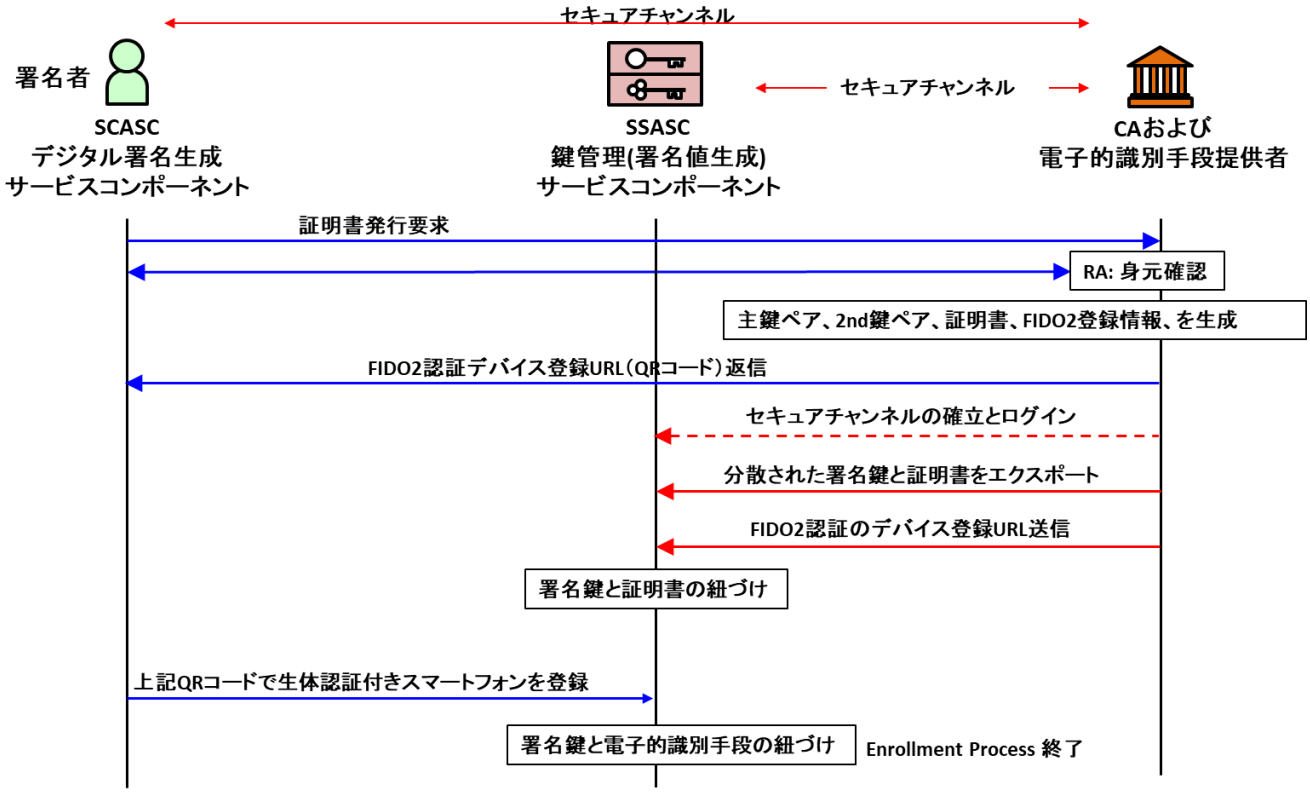

図 3 電子処方箋における利用登録のフロー

1.5　リモート署名サービスの評価基準の文書体系

保健医療福祉分野のリモート署名サービスの評価基準は、「保健医療福祉分野におけるリモート署名サービスの評価基準」（本書）及び、次に示す本書の2件の別紙（以下、これらを「別紙1」「別紙2」という。）により構成される。

別紙1：保健医療福祉分野におけるリモート署名サービス評価基準準拠性監査報告書様式（鍵管理（署名値生成）サービス）
別紙2：保健医療福祉分野におけるリモート署名サービス評価基準準拠性監査報告書様式（デジタル署名生成サービス）

保健医療福祉分野のリモート署名サービスの監査に用いる具体的な要求事項は、別紙1及び別紙2の監査対象の欄に〇印が付けられている項目である。鍵管理（署名値生成サービス）は SSASC に該当しており、別紙1の要求事項の〇印を付けた項目に従って監査を行う。同様にデジタル署名生成サービスは SCASC に該当しており、別紙2の要求事項に〇印を付けた項目に従って監査を行う。
なお、実際の監査に当たっては、別紙1及び別紙2を用いて、監査に用いるチェック表（保健医療福祉分野におけるリモート署名サービス評価基準準拠性監査報告書）を作成して実施するものとする。

注：〇印を付けた項目は電子処方箋におけるリモート署名サービスの基準として現在の実装を評価するためのものであり、署名者の秘密鍵を 2 つに分散しているとはいえ、SSASC の外に署名鍵の 2 つの断片がともに持ち出されるリスクは耐タンパーデバイスを用いて保持する場合と比べ高いと言える。将来、電子処方箋以外の医療文書のリモート署名に用いる場合は、対象文書の重要度に応じて〇印の項目を再評価し、署名鍵の漏洩リスクを物理的な SCDev などを用いて十分に低減するか、または、たとえ漏洩した場合であっても署名者以外が署名できないような必要な管理策を検討すべきである。

別紙１及び別紙2の参考資料として次の資料を挙げておく。別紙1については（1）、（2）及び（4）の、別紙2については（3）及び（4）の、それぞれの要求事項に〇印を付けた項目を参照されたい。

（１）リモート署名生成装置等を運用する TSP の一般ポリシー要求事項、および
リモート署名生成装置等を運用する TSP の一般ポリシー要求事項解説
（ETSI TS 119 431-1 を参考に作成）
ここでは、リモート署名生成装置（SCDev）を操作するサーバー署名アプリケーションサービスコンポーネント（SSASC）を管理・運用する“トラストサービスプロバイダー（TSP）”に対して、適用されるポリシーとセキュリティ要件を規定した。この SSASC に対するセキュリティ要件の一部は次の（3）を引用している。ポリシーレベルは、署名者の鍵ペアを SCDev の中で生成する際の3つのポリシー、すなわち簡易的な″LSCP″、標準的な″NSCP″および欧州の適格レベルを満たす″EUSCP“の 3 レベルに加え、署名者の鍵ペアを認証局が生成して SCDev にインポートするポリシー″LSCP+″を規定した。

（２）サーバー署名アプリケーションサービスの一般セキュリティ要求事項、および
サーバー署名アプリケーションサービスの一般セキュリティ要求事項解説
（EN 419 241-1 を参考に作成）
ここではサーバー署名アプリケーションサービスを提供する信頼できる SSASC に対するセキュリティ要件を規定した。
SSA は、承認された署名者の制御下で SCDev を使用するため、認可（Authorization）された署名者による独占的な制御（単独制御）が保証されなければならない。単独制御レベルを SCAL（Sole Control Level）と定義し、信頼度により SCAL1（低）と SCAL2（高）の 2 つの基準が示されている。

（３）デジタル署名生成サービスの一般ポリシー要求事項、および
デジタル署名生成サービスの一般ポリシー要求事項解説
（ETSI TS 119 431-2 を参考に作成）
ここでは、デジタル署名の生成をサポートするサービスコンポーネント（SCASC）及び、SCASC

を管理・運用するサービスプロバイダー(SCASP)のポリシー及びセキュリティ要件を規定した。

（４） トラストサービスプロバイダーに共通するポリシー要求事項、および
トラストサービスプロバイダーに共通するポリシー要求事項解説
（ETSI EN 319 401 を参考に作成）
ここでは、トラストサービスプロバイダー(TSP)の種類を問わず、TSP の管理及び運用の実施に関する一般的なポリシー要件を定義する。特定の種類の TSP については、別の文書によって評価基準、要求事項等が追加される場合がある。

なお、上記（1）～（4）は、保健医療福祉分野に特化したものではなく広く一般のリモート署名基準に用いることを前提に作成している。保健医療福祉分野からは参考資料としての位置づけとなることに留意されたい。

1.6　評価基準の文書における法助動詞

この評価基準においては，各評価基準項目への準拠性の対応内容を明確にするため英語の法助動詞を添えて下記の表現を用いている。
「するものとする」，(SHALL) 実施が義務付けられる
「しないものとする」，(SHALL NOT)実施しないことが義務付けられる
「すべきである」，(SHOULD) 実施しない場合、合理的な理由を示さなければならない
「すべきでない」，(SHOULD NOT) 実施する場合、合理的な理由を示さなければならない
「してもよい」，(MAY) 実施することが許容される
「する必要がない」，(NEED NOT) 実施することが求められていない

2.　用語と定義

英語表記	日本語表記	内容
authentication	認証	主張されたエンティティの同一性の保証の提供 （注） ISO/IEC 18014-2 で定義されているとおり。
authentication factor	認証ファクター	ある実体の同一性識別の認証、または検証のために使用される情報の断片および/またはプロセス
Coordinated Universal Time (UTC)	協定世界時	勧告 ITU-R TF.460-6 に定義されている秒を基準とした時間スケール。
data to be signed representation (DTBS/R)	署名対象データレプレゼンテーション	デジタル署名値を算出するために署名対象文書から生成されるデータ（ハッシュ値など）
(AdES)digital signature	デジタル署名	CAdES 署名、PAdES 署名、XAdES 署名のいずれかであり、デジタル署名値とその検証に必要な情報等を含んでいる電子データ。電子データの受信者が当該データの出所と完全性を証明し、受信者などによる偽造から保護できるようにするもの。
digital signature value	署名値	署名対象データのハッシュ値を署名者の秘密鍵により暗号変換して得られる値。
eIDAS Regulation	eIDAS 規則	EU 内部市場において、電子署名指令（1999/93/EC）を上書きする電子取引のための電子識別及びトラストサービスに関する欧州議会及び理事会の規則（EU）No 910/2014。
electronic identification (eID)	電子識別(eID)	自然人や法人、または法人を代表する自然人等を一意に表す電子的な個人識別データを用いて、オンライン・サービスなどで電子的に当該自然人等を識別するプロセス。
electronic identification means	電子識別手段（eID 手段）	個人識別データを含む電子形式のデータもしくは、それを格納した物理トークン。オンライン・ サービスの認証に使用されるもの。

electronic identification means reference	電子識別手段の参照	署名者を認証するために、電子識別手段の参照として SSASC で使用されるデータ。 （例） 電子識別手段が非対称鍵を使用する場合、公開鍵を参照とすることができる。 署名者の認証に成功した後に署名付きアサーションが生成される場合、アサーション署名者 ID およびユーザー ID を参照とすることができる。 電子識別手段が秘密鍵（ワンタイム・パスワード・ジェネレータなど）を使用する場合、秘密鍵を 参照とすることができる。
person identification data	個人識別データ	自然人もしくは法人、または法人を代表する自然人の身元を確認することを可能にするデータの集合。本人のみが所持または知りえる秘密情報を含む。
relying party	依拠当事者	電子証明書またはトラストサービスに依拠する自然人または法人をいう。 （注） 依拠当事者には、公開鍵証明書を使用してデジタル署名を検証する当事者が含まれる。
remote signature creation device	リモート署名生成装置	署名者の視点からリモートで使用され、署名者に代わって署名操作を制御する署名生成装置等。
server signing application (SSA)	サーバー署名アプリケーション	署名者に代わって署名値を生成するために署名生成装置等を使用するアプリケーション。
server signing application service component (SSASC)	サーバー署名アプリケーションサービスコンポーネント（SSASC）	署名者に代わって署名値を生成するサーバー署名アプリケーションを管理・運用するサービスコンポーネント。
server signing application service provider (SSASP)	サーバー署名アプリケーションサービスプロバイダー（SSASP）	サーバー署名アプリケーションサービスコンポーネントを管理・運用する TSP。
signature activation data (SAD)	署名活性化データ	SAP が収集するデータのうち、署名者に代わって暗号モジュールによって実行される所定の署名操作を高レベルの信頼性で制御するために使用されるデータ。署名者の単独制御下にあるもの。
signature activation module (SAM)	署名活性化モジュール	署名鍵が署名者の単独制御で使用されることを高レベルの信頼性で保証するために、SAD を使用するよう構成されたソフトウェア。
signature activation protocol (SAP)	署名活性化プロトコル	署名者の署名鍵を用いて、DTBS/R の署名操作を制御するために使用される SAD を収集するプロトコル。
signature applicability rules	署名適用性規則	1 つまたは複数のデジタル署名に適用され、署名が特定のビジネス目的または法的目的に適しているかどうかを判断するための要件を定義する一連の規則。 （注） 署名適用可能性規則は、暗黙的である場合もあれば、人間が読み取り可能な文書および/または機械が処理可能な文書

		に記載されている場合もある。ETSI TS 119 172-1 はこの目的に使用できる。
signature creation application (SCA)	デジタル署名生成アプリケーション	CAdES/XAdES/PAdES 等、標準フォーマットに準拠したデジタル署名を構築するアプリケーション。
signature creation application service component (SCASC)	署名生成アプリケーションサービスコンポーネント	デジタル署名生成アプリケーションを管理・運用するサービスコンポーネント。
signature creation application service provider (SCASP)	署名生成アプリケーションサービスプロバイダー	署名生成アプリケーションサービスコンポーネントを管理・運用する TSP。
signature creation constraint	署名生成制約	デジタル署名を生成する際に使用される規則。
signature creation device (SCDev)	署名生成装置等	署名者の署名鍵を保持し、署名値を生成するために使用されるソフトウェアまたはハードウェア。
signature creation policy	署名生成ポリシー	SCA によって処理される署名生成制約のセット。
signature policy	署名ポリシー	同一の署名または署名の集合に適用される、署名生成や検証に関わるポリシー。
signer	署名者	デジタル署名の生成者となるエンティティ（自然人または法人）
signer's interaction component	署名者インタラクションコンポーネント	署名者が SAP をサポートするために使用するソフトウェアおよび/またはハードウェアコンポーネント
signing key	署名鍵	署名値を生成するために使用される非対称暗号アルゴリズムにおける秘密鍵。
subscriber	加入者	トラストサービスプロバイダーとの契約により指定された加入者義務に拘束される法人または自然人
trust service practice statement	トラストサービス運用規程	TSP がトラストサービスを提供する際に採用する実務を記述したもの。
trust service provider (TSP)	トラストサービスプロバイダー	1 つ以上のトラストサービスを提供するエンティティ

3. 記号・略語

CA	Certification Authority（認証局）
CC	Common Criteria, ISO/IEC 15408, Evaluation criteria for IT security
CEN	Comité Européen de Normalization (European Committee for Standardization)
DTBS/R	Data To Be Signed Representation（署名対象データ表現）
EAL	Evaluation Assurance Level
eID	electronic Identification（電子識別）
ETSI	European Telecommunications Standards Institute
EUSCP	EU SSASC Policy
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
ISSS	Information Society Standardization System
LSCP	Lightweight SSASC Policy
NSCP	Normalized SSASC Policy
OID	Object Identifier（オブジェクト識別子）
SAD	Signature Activation Data （署名活性化データ）
SAM	Signature Activation Module（署名活性化モジュール）
SAP	Signature Activation Protocol（署名活性化プロトコル）
SCA	Signature Creation Application（署名生成アプリケーション）
SCAL	Sole Control Assurance Level（署名者唯一による署名鍵の制御。単独制御）
SCASC	Signature Creation Application Service Component（署名生成アプリケーションサービスコンポーネント）
SCASP	Signature Creation Application Service Provider（署名生成アプリケーションサービスプロバイダー）
SCDev	Signature Creation Device（署名生成装置等）
SCP	SSASC Policy
SD	Signer's Document（署名者のドキュメント）
SIC	Signer's Interaction Component
SLA	Service-Level Agreement（サービスレベルアグリーメント、サービス品質保証、サービスレベル合意書）
SSA	Server Signing Application
SSASC	Server Signing Application Service Component（サーバー署名アプリケーションサービスコンポーネント）

SSASP	Server Signing Application Service Provider（サーバー署名アプリケーションサービスプロバイダー）
TSA	Time-Stamping Authority（タイムスタンプ局）
TSP	Trust Service Provider

4. 参照規格

- ETSI EN 319 401 トラストサービスプロバイダーの一般的ポリシー要求
  General Policy Requirements for Trust Service Providers
- EN 419 241-1 サーバー署名の一般セキュリティ要求
  Trustworthy Systems Supporting Server Signing – Part 1: General System Security Requirements
- EN 419 241-2 サーバー署名で用いる適格署名生成装置の Protection profile
  Trustworthy Systems Supporting Server Signing – Part 2: Protection profile for QSCD for Server Signing
- ETSI TS 119 431-1 リモート QSCD/SCDev のポリシー要求事項
  Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev
- ETSI TS 119 431-2 AdES デジタル署名生成を提供する TSP のポリシー要求事項
  Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation (remote signing)
- ETSI TS 119 432 リモートデジタル署名生成プロトコル
  Protocols for remote digital signature creation