

(案)

資料 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
1.01 版

令和 6 年 11 月

厚生労働省

(C) Ministry of Health, Labour and Welfare

改定履歴

版数	日付	内容	
初版	令和 5 年 9 月	初版発行	
1.01 版	令和 6 年 11 月	1.1 本評価基準の位置づけ	評価基準と要件の文書を切り離すにあたり、要件該当部分を削除し、要件を定義した文書について記載を追加した。
		1.2 本書のスコープ	評価基準と要件の文書を切り離すにあたり、要件該当部分を削除了。
		1.4 リモート署名サービスの評価基準の文書体系	評価基準と要件の文書を切り離すにあたり、旧版での 1.4 項目(リモート署名サービスのアーキテクチャー) を削除し 1.5 を繰り上げした。

目次

1.	総則	4
1.1	本評価基準の位置づけ	4
1.2	本書のスコープ	4
1.3	本書の目的	4
1.4	リモート署名サービスの評価基準の文書体系	5
1.5	評価基準の文書における法助動詞	7
2.	用語と定義	7
3.	記号・略語	10
4.	参照規格	11

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、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、具体的な評価基準はそれぞれのコンポーネントに対応する別紙に記載される。なお、本基準に基づき厚生労働省が実施する適合性評価の対象は「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による適合性評価の対象となるリモート署名サービスの適用要件」に記載のアーキテクチャ要件及び情報サービス要件を満たすサービスに限られる。

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参考とし、「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による適合性評価の対象となるリモート署名サービスの適用要件」を満たすサービスに対する評価基準を規定した。なお、トラストサービス及び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)
署名者に代わってデジタル署名値を生成するサーバー署名アプリケーション(SSA)を管理・運用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)
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(SCA)を管理・運用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(デジタル署名値生成)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○印が付けられている項目である。鍵管理(デジタル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○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○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: ○印を付けた項目は本評価基準を適用でき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る。たとえば署名者の署名鍵を2つに分散する実装が考えられるが、そのような実装であっても 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エバイスを用いて保持する場合と比べ高いと言える。したがって、このような実装については、本評価基準による評価だけでは不十分であり、安全性に関する付加的な審査が必要である。将来、1.1 で定めたサービス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○印を付すべき項目を再検討し、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○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 (Lightweight SSASC Policy)”、標準的な“NSCP(Normalized SSASC Policy)”および欧州の適格レベルを満たす“EUSCP(EU SSASC Policy)“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。(SCASC) 及び、同サービスコンポーネントを管理・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。

1.5 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ぬ
- 「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ぬ
- 「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	デジタル署名値	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ます。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ます。 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ます。
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	署名者に代わってデジタル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)	署名者に代わってデジタル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、デジタル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	署名者インターフェ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	デジタル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	トラストサービス及び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

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 ト拉斯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