（案）

資料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
1.00 版

令和 6 年 11 月

厚生労働省

改定履歴

版数	日付	内容
初版	令和6年11月	初版発行

目次

1. 総則 4
1.1 本書の目的、スコープ 4
1.2 リモート署名サービスのアーキテクチャーの要件 4
1.3 リモート署名サービスを利用可能な情報サービスの要件 8
2. 用語と定義 9

1. 総則

1.1 本書の目的、スコープ

厚生労働省は、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（以下「評価基準」という。）による適合性評価（以下「適合性評価」という。）を行っている。本書は、適合性評価の対象となる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）の範囲をさだめるものであり、適合性評価の対象を本書で規定される要件（アーキテクチャーの要件及び情報サービスの要件）を満たすものに限定することにより利用者に対して安全な電子署名環境を提供することを目的とする。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。

適合性評価は、1.2 および 1.3 に定められた要件を満たしたリモート署名サービスを対象とし、評価基準は、かかる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に適用される。

・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。

1.2 リモート署名サービスのアーキテクチャーの要件

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、下記のアプリケーションから構成される。

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

[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

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 はデジタル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は、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。SSA 視点では自らが運用するため“リモート”を省略し署名値生成装置等と記載する。SSA は、署名対象データのハッシュ値に基づいて生成されたデジタル署名値を署名者または、次の②に記載するデジタル署名生成アプリケーションに配信することを目的とする。

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。

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。

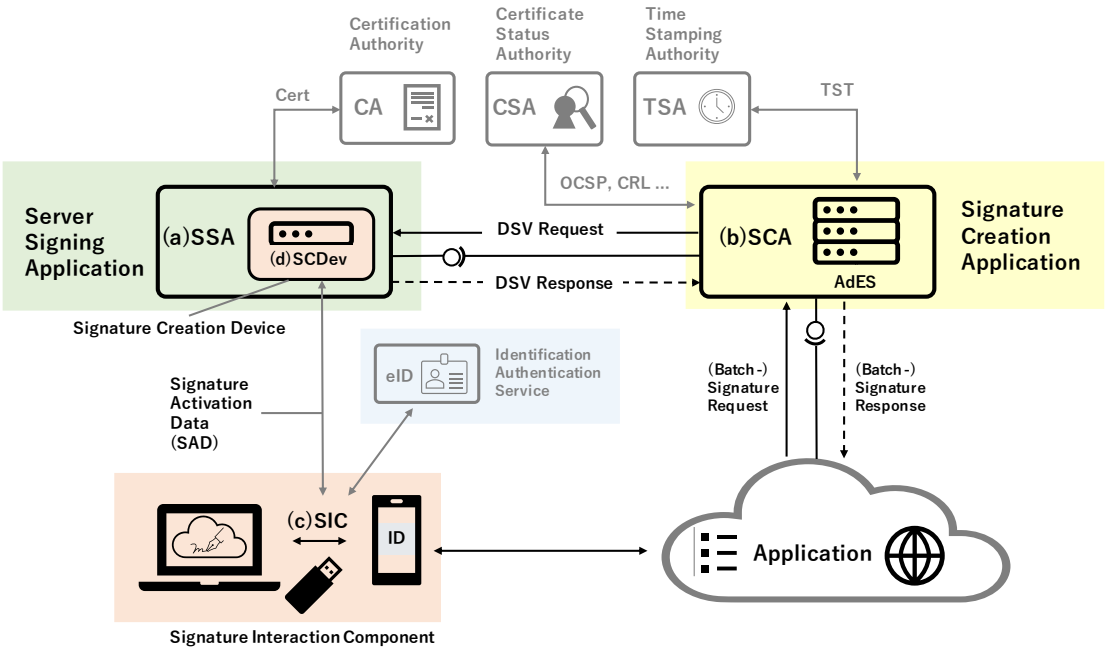

図1　リモート署名サービスのアーキテクチャー

（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（TSP）の要件を満たす必要がある。

リモート署名サービスの利用登録のフロー

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(HPKI の証明書ポリシーにおける、Private Key をいう。)、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(デジタル署名値生成)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。

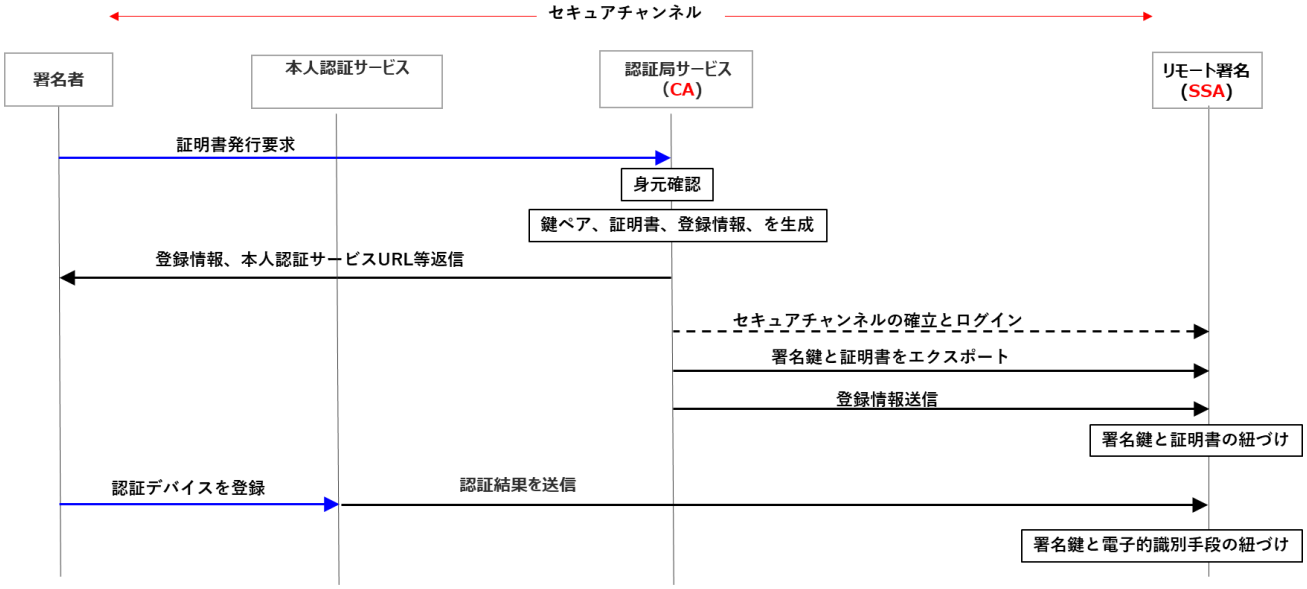

図 3　本評価基準を適用できるリモート署名サービスの利用登録(認証局が利用者の鍵ペアを生成し SSA に送信する場合)の例

1.3　リモート署名サービスを利用可能な情報サービスの要件

適合性評価の対象となるリモート署名サービスは、以下の要件を満たした情報サービスで利用するものに限るものとする。

① 情報サービスの運営主体

国、社会保険診療報酬支払基金または公益財団法人国民健康保険中央会であること。

② 情報サービスの対象者

電子署名を付す電子処方箋、診療情報提供書等、本要件の対象とする文書のやりとりは、本要件が対象とする評価基準の評価結果に従って対象ごとのリスク分析を行い、情報サービスの運営主体による運用規程等で定められた組織間および基盤間のみで運用されること。

③ 情報サービスの利用基盤

情報サービスの運営主体が運用する認証局から発行されたクライアント証明書をインストールしている許可された端末・サーバーからのみアクセスできること。本要件が対象とする評価基準を満たした基盤を使用していること。

④ 情報サービスのネットワーク要件

情報サービスの運営主体と情報サービスの対象者間の電子署名を付す電子処方箋、診療情報提供書等、本要件の対象とする文書のやりとりは閉域 IP 網を利用した IP-VPN 接続、または、オープンなネットワークにおいては IPsec と IKE を組み合わせた接続を利用していること。

⑤ 情報サービスのセキュリティ対策

運営主体及び、情報サービスを利用する組織は、厚生労働省が公開している「医療情報システムの安全管理に関するガイドライン」の最新版に準拠した対策を実施していること。運営主体の情報サービスを提供するサーバーはネットワークに接続した組織に対し、ネットワークを介した不正アクセスや提供データの改ざん等が生じないセキュリティ対策が講じられていること。主なセキュリティ対策の概要を付録Aに示す。

2. 用語と定義

表記	内容
電子署名	「電子署名及び認証業務に関する法律」(平成 12 年法律第 102 号) 第 2 条第 1 項に規定する 電子署名
認証局	電子証明書を発行する組織
クライアント証明書	ユーザーのデバイスにインストールされる認証局より発行される電子証明書

付録A：主なセキュリティ対策の概要[1)]

主なセキュリティ対策	概要
アクセス、利用制限	情報資産へのアクセスを許可された者のみに限定するため、利用する主体（職員、システム運用要員、医療機関・薬局）を識別するための認証を行う。 管理者に対するアクセス制御を検討し、内部の要員によるデータ漏えいを防止する仕組みを実現する。
セキュリティリスク分析、セキュリティ診断、セキュリティリスク管理	設計、開発するソフトウェアの緊急性の高いセキュリティパッチなどの適用を適宜正確かつ迅速に行う。脆弱性が生じないよう留意して設計、開発し、定期的な検査を通じた確認により修正を適用できるようにする。
マルウェア対策	アンチウイルスソフトウェア等の導入によりマルウェアへの対策を講ずるための機能を備える。 外部ネットワークからのマルウェアの侵入や、万が一、マルウェアに侵入された場合の外部ネットワークへの不正な通信等を監視し、侵入の検知、防止及び当該マルウェアによる通信の遮断等を行う。
データの秘匿	情報の窃取や漏えいを防止するため、保護すべき情報に対してアクセス制御を行うことに加えて、保存された情報及び情報にアクセスするための通信回線を暗号化する機能を備える。
不正アクセス、 内部不正対策	ネットワーク機器及びサーバ機器への不正アクセス等による被害を極小化するため、全てのサーバ、ネットワーク機器を対象に、ネットワーク及びサーバー機器への不正アクセスの防止や万が一侵入された場合の検知、通知を行う。 正当な権限を持つ内部職員による内部不正や、外部攻撃によるセキュリティインシデントの放置を防止するため、ログ等の証跡に対し、当該事象を特定できるようにする。
ネットワーク対策	通信回線を介した不正を防止するため、不正アクセス及び許可されていない通信プロトコルを通信回線上で遮断する機能を備える。不正な通信、サービス停止攻撃等に対し通信の遮断や通信量の抑制、レピュテーション情報を活用したセキュリティ監視等により、サービス停止の脅威を軽減する機能（自動的に遮断する仕組みも含める。）を備える。
Web 対策	L7レイヤーまでのセキュリティ対策（Cookie、パラメータの改ざん、URL の改ざんなどへの対応）を行う。 DDoS 攻撃を回避する仕組みを設ける。新たに発見された脅威に対し、速やかに対応する必要がある場合、WAF の導入による対策が必要。WAF を導入した場合に、WAF を経由した攻撃等にも対処を実施する。

1）電子処方箋管理サービスの導入に関するシステムベンダ向け技術解説書　表 19 電子処方箋管理サービスにおける主なセキュリティ対策　より抜粋