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　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）
1.0版

令和5年8月
厚生労働省

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（鍵管理（署名値生成）サービス）

監査実施にあたって

本監査報告書の記入にあたり「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」に従って監査を実施し記入をすること

本監査報告書は下記の3パートで構成されており、全てのパートの監査を実施する必要がある。
・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
・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
・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

本監査報告書において監査対象は〇の表示がされている項目のみを対象とする。

本監査報告書で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

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報告書（鍵管理（署名値生成）サービス）

監査報告書リスト番号	要求識別子	監査対象	要求事項	措置状況	確認したエビデンス	監査エビデンス(具体的な確認事項／方法)	トラストサービスプロバイダー監査者評価およびコメント	専門家会議評価およびコメント
「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」								
-	**5**		**5 運用規定とポリシーに関する一般規定**					
-	5.1 Practice statement requirements		5.1 運用規定の要求事項					
1	OVR-5.1-01	○	「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」 の 6.1 項に規定される一般要求事項を適用するものとする(SHALL)。加えて、以下の特定の要件を適用する。 注1：TSPは、特定のSSASCポリシー要件に関連する実務を、主要な運用規程とは別に文書化することができる。					監査報告書リスト番号258項～271項参照
2	OVR-5.1-02	○	TSP の運用規程には、適用される署名アルゴリズムおよびパラメータ、鍵ペア生成に適用されるアル ゴリズム、ならびに SSASC 運用のセキュリティにとって重要なその他のアルゴリズムおよびパラメータを 含むものとする(SHALL)。					
3	OVR-5.1-03	○	TSP は、24 時間 365 日利用可能なオンライン手段を通じて、自己の運用規程を公開するものとする(SHALL)。 注2: TSPは、機密情報を含むいかなる側面も開示する義務はない。					
4	OVR-5.2-01	○	SCP(SSASCのポリシー） に変更があり、適用性に影響がある場合は、ポリシー識別子を変更するべきである(SHOULD)。					
5	OVR-5.3.1-01	○	SSASP は、サービスの一部を提供するために他の当事者を利用することができるが（MAY)、SSASP は常に全体的な責任を維持し、本書で特定されるポリシー要件が満たされていることを保証するものとする(SHALL)。					
-	6		6 トラストサービスプロバイダの運用					
-	6.1 Publication and repository responsibilities		6.1公開とリポジトリの責任					
6	OVR-6.1-01	○	TSP は、署名鍵の使用に関して、適用される SCP群、運用規程、利用規約を加入者及び依拠当事者に提供 するものとする(SHALL)。					
7	OVR-6.1-02	○	適用される利用規約は、与えられた署名鍵または関連する証明書について容易に特定可能でなければならない(SHALL)。					
8	OVR-6.1-03	○	上記OVR-6.1-01 及び OVR-6.1-02 で特定された情報は、24時間365日利用可能であるものとする(SHALL)。 システム障害、サービス、その他トラストサービスプロバイダーの管理下にない要因が発生した場合、トラストサービスプロバイダーは、SSASC運用規程に示される最長期間を超えてこの情報サービスが利用できないことがないよう最善の努力をするものとする(SHALL)。					
9	OVR-6.1-04	○	上記OVR-6.1-01で特定された情報は、一般的に利用可能とすべきである(SHOULD)。					
-	6.2 Signing key initialization		6.2 署名鍵の初期化					
-	6.2.1 Signing key generation		6.2.1 署名鍵の生成					
10	GEN-6.2.1-01 [LSCP]	○	「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」 の SRG_KM.1.1 項（署名鍵の環境に関する規定）を適用するものとする(SHALL)。					監査報告書リスト番号160項～162項参照
11	GEN-6.2.1-02 [NSCP]	対象外	「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」の SRA_SKM.1.1 項(署名鍵の環境に関する規定)を適用するのとする(SHALL)。					監査報告書リスト番号238項参照
12	GEN-6.2.1-03	○	「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」 の SRG_KM.1.2 項（暗号アルゴリズムと鍵長を規定）を適用するものとする(SHALL)。					監査報告書リスト番号163項,164項参照
13	GEN-6.2.1-04	○	「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」 の SRG_KM.1.3 項(鍵の保護に関する規定）を適用するのとする(SHALL)。					監査報告書リスト番号165項参照
14	GEN-6.2.1-05	○	「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」 の SRG_KM.1.4 項（デバイスの初期化に関する規定）を適用するのとする(SHALL)。					監査報告書リスト番号166項参照
15	GEN-6.2.1-06	○	「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」 の SRC_SKS.1.1 項（アルゴリズムパラメータを規定）を適用するのとする(SHALL)。					監査報告書リスト番号209項参照
16	GEN-6.2.1-07	○	「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」 の SRC_SKS.1.3 項（生成時間に関する規定）を適用するものとする(SHALL)。					監査報告書リスト番号211項参照
17	GEN-6.2.1-08 [CONDITIONAL]:	○	SSASC と証明書生成サービスコンポーネントが別々に管理される場合、SSASC は ETSI EN 319 411-1 [2] の REG-6.3.1-01 項で定義された要件をサポートするものとする(SHALL)。 例：秘密鍵にリンクされた署名者の認証のアサーションを提供することによって。 EN 319 411-1 [2] の REG-6.3.1-01 サブジェクトの鍵ペアがCAによって生成されていない場合、証明書申請プロ セスは、サブジェクトが認証のために提示された公開鍵に関連する秘密鍵を所有または管理していることを確認するものとする。					
18	GEN-6.2.1-09 [LSCP+] [CONDITIONAL]:	○	SSASC と証明書生成サービスコンポーネントが別々に管理される場合で、サブジェクトの鍵ペアがCAによって生成されている場合、SSASC は 国に認定された信頼できるCAから直接、安全に署名鍵をインポートするものとする（SHALL)。 （例）CAから直接安全に署名鍵をインポートする手段は、以下が考えられる ・インターネットとの接合点は持たないセキュアな回線を用いる サブジェクトの署名鍵を格納する暗号モジュールは、「保健医療福祉分野PKI 認証局署名用証明書ポリシ1.9版　6.2.11 暗号モジュールの評価」の基準を満たすものとする。 保健医療福祉分野PKI 認証局署名用証明書ポリシ1.9版 6.2.11　暗号モジュールの評価 CA私有鍵を格納する暗号モジュールは、 FIPS 140 2 レベル 3 と同等以上のものを使用する。 エンドエンティティの加入者の私有鍵を格納する暗号モジュールは、FIPS 140 2 レベル 1 と同等以上のものを使用する。					
-	6.2.2　eID means linking		6.2.2 電子識別手段のリンキング					
19	LNK-6.2.2-01	○	「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」 の SRC_SA.1.1 項（登録(enrolment)）に関する規定）が適用されるものとする(SHALL)。					監査報告書リスト番号214項参照

監査報告書リスト番号	要求識別子	監査対象	要求事項	措置状況	確認したエビデンス	監査エビデンス(具体的な確認事項／方法)	トラストサービスプロバイダー監査者評価およびコメント	専門家会議評価およびコメント
20	LNK-6.2.2-02 ［NSCP］[CONDITIONAL]	○	署名者が自然人の場合、「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」 の SRA_SAP.1.1 項（登録(enrolment)）に関する規定）を適用するものとする(SHALL)。					監査報告書リスト番号223項参照
21	LNK-6.2.2-03	○	SSASP は、署名鍵を適切な署名者の eID 手段の参照情報とリンクさせるものとする(SHALL)。					
22	LNK-6.2.2-04	○	SSASP は eID 手段の参照情報を生成し、対応する eID 手段を署名者に提供することができる （MAY)。 (6.2.4項参照)。					
23	LNK-6.2.2-05	○	SSASP は、eID の手段参照にリンクされた人物識別データが、関連する証明書のサブジェクトにリンク されたものと同一であることを保証するものとする(SHALL)。 注1：電子識別手段のリファレンスが証明書登録サービス発行元の TSP である場合、本要件への適合性があると見なすことができる					
24	LNK-6.2.2-06	○	署名者の eID手段の参照情報 は、権限のある（外部の）当事者が提供してもよい （MAY)。					
25	LNK-6.2.2-07 ［LSCP］[CONDITIONAL]	○	認証プロセスの全部または一部が外部に委任される場合、SSASP は、その外部が LNK-6.2.2-01 に規定される要件を満たすことを保証するものとする(SHALL)。 注2： 外部当事者が、公的個人認証法第17条の4号の届け出もしくは5号、6号の認定事業者の場合、国により認められた、もしくは国際的な評価基準への適合性が独立した監査機関により認められた事業者の場合要求されるレベルへの適合性を仮定することが可能である。					
26	LNK-6.2.2-08 [NSCP] [CONDITIONAL]	○	認証プロセスの全部または一部が外部に委任される場合、SSASP は、その外部が LNK-6.2.2-02 および LNK-6.2.2-03 に規定される要件を満たすことを保証するものとする(SHALL)。					
27	LNK-6.2.2-09 [NSCP] [CONDITIONAL]	○	認証プロセスのすべてまたは一部が外部に委譲される場合、SSASP は以下を確認するものとする(SHALL)。 -外部当事者が、本文書の関連する全ての要求事項及び適用される規制要件に従った登録の要求事項を満たしている事、又は 外部当事者に委任された認証プロセスが、公的個人認証サービスの下で発行された電子的識別手段を使用すること。 注3： 外部当事者が、公的個人認証法第17条の4号の届け出もしくは5号、6号の認定事業者の場合、国により認められた、もしくは国際的な評価基準への適合性が独立した監査機関により認められた事業者の場合要求されるレベルへの適合性を仮定することが可能である。					
28	LNK-6.2.2-10	○	SSASP は、署名者の署名鍵とその eID の参照手段との間のリンクの完全性を保護するものとする(SHALL)。					
-	6.2.3 Certificate linking		6.2.3 証明書のリンキング					
29	LNK-6.2.3-01	○	「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」 の SRC_SKS.1.2 項（証明書のリンキングに関する規定）は、SSASC に適用されるものとする(SHALL)。					監査報告書リスト番号210項参照
30	LNK-6.2.3-02	○	「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」 の SRC_SKS.1.4 項、（証明書のリンキングに関する規程）は、SSASC に適用されるものとする(SHALL)。					監査報告書リスト番号212項参照
31	LNK-6.2.3-03	○	「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」 の SRC_SKS.1.5 項（リンクの保護に関する吉衛） は、SSASC に適用されるものとする(SHALL)。					監査報告書リスト番号213項参照
-	6.2.4 eID means provision		6.2.4 電子識別手段の提供					
32	EID-6.2.4-01 ［CONDITIONAL］	○	SSASP が署名者の eID 手段を提供する場合、eID 手段は署名者に安全に渡されるものとする(SHALL)。					
33	EID-6.2.4-02 ［CONDITIONAL］	○	SSASP が署名者の eID 手段を関連するユーザ活性化データ（例：PIN コード）でパーソナライズする場合、活性化データは署名者の eID 手段とは別に安全に準備・配布されるものとする。					
-	6.3 Signing key life-cycle operational requirements		6.3 署名鍵のライフサイクル運用要件					
-	6.3.1 Signature activation		6.3.1 署名活性化					
34	SIG-6.3.1-01	○	「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」 の SRC_SA.1.2 項（認証に関する規定）が適用されるものとする(SHALL)。					監査報告書リスト番号215項参照
35	SIG-6.3.1-02	○	「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」 の SRC_SA.1.3 項（プロトコルセキュリティの規定）を適用する(SHALL)。					監査報告書リスト番号216項参照
36	SIG-6.3.1-03	○	「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」 の SRC_SA.1.4 項（アクセス制御を規定）を適用するものとする(SHALL)。					監査報告書リスト番号217項参照
37	SIG-6.3.1-04	○	「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」 の SRC_SA.1.5 項（署名鍵管理に関する規定）を適用するものとする(SHALL)。					監査報告書リスト番号218項参照
38	SIG-6.3.1-05 [NSCP]	対象外	「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」 の SRA_SKM.2.1 項（署名鍵の活性化に関する規定）を適用するものとする(SHALL)。					監査報告書リスト番号245項参照
39	SIG-6.3.1-06 ［NSCP］	対象外	「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」 の SRA_SAP.1.2 項（プロトコルセキュリティに関する規定）を適用するものとする(SHALL)。					監査報告書リスト番号224項参照
40	SIG-6.3.1-07 ［NSCP］	対象外	「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」 の SRA_SKM.2.5 項（署名鍵の管理に関する規定）を適用するものとする(SHALL)。					監査報告書リスト番号249項参照
41	SIG-6.3.1-08	○	SSASP は、対応する署名鍵を使用する前に、公開鍵証明書が有効であることを確認するべきである(SHOULD)。 注：有効＝有効期間切れでない、失効していない、一時停止していない、一時停止を使用しない場合は DEL-6.3.2-01 を適用することにより満たすことができる 。					
42	SIG-6.3.1-09	○	署名鍵は、署名者の同意が得られた場合のみ使用できるものとする(SHALL)。					
43	SIG-6.3.1-10	○	「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」 の SRC_DSC.1.1 項（署名生成のアルゴリズムパラメータを規定）を適用するものとする(SHALL)。					監査報告書リスト番号222項参照

監査報告書リスト番号	要求識別子	監査対象	要求事項	措置状況	確認したエビデンス	監査エビデンス(具体的な確認事項／方法)	トラストサービスプロバイダー監査者評価およびコメント	専門家会議評価およびコメント
-	6.3.2 Signing key deletion		6.3.2 鍵の消去					
44	DEL-6.3.2-01	○	「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」 の SRG_KM.7.1 項を適用するものとする(SHALL)。					監査報告書リスト番号181項参照
45	DEL-6.3.2-02	○	SSASP は、署名者から要求された場合、署名鍵を破棄するものとする(SHALL)。					
46	DEL-6.3.2-03	○	「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」 の SRG_KM.7.2 項（セッション管理に関する規定）が適用されるものとする(SHALL)。					監査報告書リスト番号182項参照
47	DEL-6.3.2-04	○	「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」 の SRG_KM.7.3 項（鍵のバックアップの削除を規定）が適用されるものとする(SHALL)。					監査報告書リスト番号183項参照
-	6.4 Facility, management, and operational controls		6.4 施設、管理、および運用管理					
-	6.4.1 General		6.4.1 概要					
48	OVR-6.4.2-01	○	「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」 の 7.6 項に規定される要求事項を適用するものとする(SHALL)。さらに、以下の特別な要件が適用される。					監査報告書リスト番号336項～340項参照
49	OVR-6.4.2-02	○	ETSI EN 319 411-1 [2]の OVR-6.4.2-02 項から OVR-6.4.2-10 項(　物理的セキュリティ管理)で規定される要件は、					
-	6.4.3　Procedural controls		6.4.3 手続き上のコントロール					
50	OVR-6.4.3-01	○	「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」 の要求事項 REQ-7.4-04 から REQ-7.4-09 が適用されるものとする(SHALL)。					監査報告書リスト番号328項～333項参照
-	6.4.4　Personnel controls		6.4.4 人的コントロール					
51	OVR-6.4.4-01	○	「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」 7.2 項に規定される要求事項を適用するものとする(SHALL)。					監査報告書リスト番号299項～318項参照
-	6.4.5　Audit logging procedures		6.4.5 監査の記録手順					
52	OVR-6.4.5-01	○	「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」 7.10 項に規定される要求事項が適用されるものとする(SHALL)。					監査報告書リスト番号382項～389項参照
53	OVR-6.4.5-02	○	セキュリティポリシーに関する変更、システムの起動・停止、システムクラッシュ及びハードウェア障害、ファイアウォール及びルータの動作、SSASCシステムアクセスの試行など、すべてのセキュリティイベントを記録するものとする(SHALL)。					
54	OVR-6.4.5-03	○	「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」 SRG_AA.1項 （監査データ生成に関する規定）を適用するものとする(SHALL)。					監査報告書リスト番号186項,187項参照
55	OVR-6.4.5-04	○	「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」 SRG_AA.2項 （監査データの利用可能性に関する規定）を適用するものとする(SHALL)					監査報告書リスト番号188項～191項参照
56	OVR-6.4.5-05	○	「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」 SRG_AA.3項 （監査データのパラメータに関する規定）を適用するものとする(SHALL)。					監査報告書リスト番号192項参照
57	OVR-6.4.5-06	○	「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」 SRG_AA.7項 （監査データの完全性に関する規定）を適用するものとする(SHALL)。					監査報告書リスト番号197項,198項参照
58	OVR-6.4.5-07	○	「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」 の SRG_AA.8 項 （監査データのタイミングに関する規定）を適用するものとする(SHALL)。					監査報告書リスト番号199項参照
-	6.4.6		6.4.6 記録保管					
59	OVR-6.4.6-01	○	SSASP は、監査データの記録を、これらの記録に基づく証明書が効力を失った後、少なくとも 7 年間、 適用される法律の制約の範囲内で、保持するものとする(SHALL)。					
-	6.4.7		6.4.7 鍵更新					
60	-	対象外	規程しない					
-	6.4.8		6.4.8 危殆化と災害復旧					
61	OVR-6.4.8-01	○	「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」 の 7.9 項と 7.11 項で特定された要件が適用されるものとする(SHALL)。					監査報告書リスト番号370項～381項,390項,391項参照
-	6.5		6.5 技術的なセキュリティ管理					
-	6.5.1		6.5.1 システム及びセキュリティ管理					
62	OVR-6.5.1-01	○	「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」 の SRG_M.1 項に規定された要件が適用されるものとする(SHALL)。					監査報告書リスト番号122項～141項参照
-	6.5.2		6.5.2 システムと運用					
63	OVR-6.5.2-01	○	「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」 の SRG_SO.1 項に規定された要求事項を適用するものとする(SHALL)。					監査報告書リスト番号142項～149項参照
64	OVR-6.5.2-02	○	「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」、SRG_SO.2 項で特定された要求事項を適用するものとする(SHALL)。					監査報告書リスト番号150項～152項参照
-	6.5.3		6.5.3 コンピュータセキュリティコントロール					
65	OVR-6.5.3-01	○	「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」 の要件、REQ-7.4-01、REQ-7.4-02、REQ-7.4-03 および REQ-7.4-10 が適用されるものとする(SHALL)。 注：信頼できるシステムの要件は、例えば、「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」に準拠するシステム、またはISO/IEC 15408 [i.6]に従って定義される適切な保護プロファイル（またはプロファイル）を使用して確保することができる。					監査報告書リスト番号324項～326項,334項参照
66	OVR-6.5.3-02	○	「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」 のSRG_AA.6.1項 （システム監視に関する規定）を適用するものとする(SHALL)。					監査報告書リスト番号196項
-	6.5.4		6.5.4 ライフサイクルセキュリティコントロール					
67	OVR-6.5.4-01	○	「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」 の 7.7 項で特定された要件が、すべてのサービス・コンポーネントに適用されるものとする(SHALL)。					監査報告書リスト番号341項～349項参照
-	6.5.5		6.5.5 ネットワークセキュリティコントロール					
68	OVR-6.5.5-01	○	「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」 の 7.8 項で特定された要件が適用されるものとする(SHALL)。					監査報告書リスト番号350項～369項参照
-	6.6		6.6 コンプライアンス監査およびその他の評価					
69	-	対象外	注：ETSI EN 319 403 [i.3]を参照。					
-	6.7		6.7 その他のビジネスおよび法的事項					
-	6.7.1		6.7.1手数料					
70	-	対象外	これらのポリシー要件は、TSP のサービスに対する課金に関する制限を意味するものではない。					
-	6.7.2		6.7.2 財政的責任					

監査報告書リスト番号	要求識別子	監査対象	要求事項	措置状況	確認したエビデンス	監査エビデンス(具体的な確認事項／方法)	トラストサービスプロバイダー監査者評価およびコメント	専門家会議評価およびコメント
71	OVR-6.7.2-01	対象外	無効 注：財務的責任については、本書 6.8.1 項の OVR-6.8.1-01 に記載されています。					
-	6.7.3		6.7.3 業務情報の守秘義務					
72	-	対象外	規程しない					
-	6.7.4		6.7.4 個人情報の保護					
73	OVR-6.7.4-01	○	「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」 で特定された要件 REQ 7.13-05 が適用されるものとする(SHALL)。					監査報告書リスト番号407項参照
-	6.7.5		6.7.5 知的財産権					
74	-	対象外	規程しない					
-	6.7.6		6.7.6 表明と保証					
75	OVR-6.7.6-01	○	「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」 に規定されている要件 REQ-6.3-05 および REQ-6.3-06 が適用されるものとする(SHALL)。 注：SSASP は、SSASP の機能がアウトソーサーによって引き受けられる場合でも、本ポリシーに規定された手順への適合に責任を有する。					監査報告書リスト番号282項,283項参照
-	6.7.7		6.7.7 保証の免責事項					
76	-	対象外	6.7.6項を参照。					
-	6.7.8		6.7.8 責任の制限					
77	-	対象外	責任の限定は、6.8.4 項のとおり、利用規約でカバーされます。					
-	6.7.9		6.7.9 免責事項					
78	-	対象外	規程しない					
-	6.7.10		6.7.10 期間と終了					
79	-	対象外	規程しない					
-	6.7.11		6.7.11 参加者への個別通知と連絡					
80	-	対象外	規程しない					
-	6.7.12		6.7.12 修正					
81	-	対象外	規程しない					
-	6.7.13		6.7.13 紛争解決手続き					
82	OVR-6.7.13-01	対象外	無効 注：紛争解決手続きは、本書 6.8.1 項および 6.8.1 項の OVR-6.8.1-01 および OVR-6.8.4-04 でカバーされます。					
-	6.7.14		6.7.14 準拠法					
83			本文書の対象外。					
-	6.7.15		6.7.15 適用される法律の遵守					
84	OVR-6.7.15-01	対象外	「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」 に規定される要件 REQ-7.13-01 および REQ-7.13-02 が適用されるものとする(SHALL)。					監査報告書リスト番号403項,404項参照
-	6.7.16		6.7.16 雑則					
85	-	対象外	規程しない					
-	6.8		6.8 その他の規定					
-	6.8.1		6.8.1 組織的要件					
86	OVR-6.8.1-01	○	「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」 の 7.1 項に規定される要求事項を適用するものとする(SHALL)。					監査報告書リスト番号288項～297項参照
-	6.8.2		6.8.2 追加試験					
87		対象外	ポリシーの要件なし。					
-	6.8.3		6.8.3 障害					
88	OVR-6.8.3-01	○	「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」 で特定された要求事項 REQ-7.13-03 および REQ-7.13-04 が適用されるものとする(SHALL)。					監査報告書リスト番号405項,406項参照
-	6.8.4		6.8.4 利用規約					
89	OVR-6.8.4-01	○	「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」 の 6.2 項に規定される要求事項を適用するものとする(SHALL)。					監査報告書リスト番号272項～277項参照
-	**7**		7. 本書を基に構築されたSSASCポリシーを定義するためのフレームワーク					
90	OVR-7-01 [CONDITONAL]	○	本文書で定義された要求事項から SCP を構築する場合、ポリシーは条項 5 から 6 で特定されたすべての要求事項を組み込むか、さらなる制約条件を組み込むものとする(SHALL)。					
91	OVR-7-02 [CONDITONAL]	○	本文書に定義された要求事項から SCP を構築する場合，ポリシーは，適用することを選択したあらゆる差異を特定するものとする(SHALL)。					
92	OVR-7-03 [CONDITONAL]	○	本文書で定義された要件から SCP を構築する場合、契約者は、利用規約を締結する一環として、特定のポリシーが本文書で定義されたポリシーの要件に追加する、あるいはさらに制約する方法について知らされるものとする(SHALL)。					
93	OVR-7-04 [CONDITONAL]	○	本文書で定義された要件から SCP を構築する場合、ポリシーを規定し承認する最終的な権限と責任を 持つ機関（例えば、ポリシー管理権限者）が存在するものとする(SHALL)。					
94	OVR-7-05 [CONDITONAL]	○	本文書で定義された要件から SCP を構築する場合、ビジネス要件を評価し、明記されたコミュニティ及び適用可能性のためにポリシーに含めるべきセキュリティ要件を決定するために、リスクアセスメントを実施するものとする(SHALL)。					
95	OVR-7-06 [CONDITONAL]	○	本文書で定義された要件から SCP を構築する場合、ポリシーを維持する責任を含む、定義されたレビュープロセ スに従って、ポリシーの承認と修正を行うべきである(SHOULD)。					
96	OVR-7-07 [CONDITONAL]	○	本文書で定義された要件から SCP を構築する場合，方針が実務の記述によって裏付けられていることを確 認するために，定義されたレビュープロセスが存在すべきである。					
97	OVR-7-08 [CONDITONAL]	○	本文書で定義された要件から SCP を構築する場合、TSP は、TSP がサポートするポリシーをその利用者コ ミュニティに公開すべきである(SHOULD)。					
98	OVR-7-09 [CONDITONAL]	○	本文書に定義された要件から SCP を構築する場合、TSP がサポートするポリシーの改訂をサブスクライバに公開すべきである(SHOULD)。					
99	OVR-7-10 [CONDITONAL]	○	本文書で定義された要件から SCP を構築する場合，ポリシーについて一意のオブジェクト識別子（OID または URI など）を取得するものとする(SHALL)。					
-	Annex A (normative):		eIDAS規則に関連する特定の要求事項					
100	A.1　SSASP as a Qualified TSP	対象外	本付属書は、リモートQSCDを操作するサービス・コンポーネントを実装する適格TSPに一般的に適用されるポリシーおよびセキュリティ要件を規定する。					

監査報告書リスト番号	要求識別子	監査対象	要求事項	措置状況	確認したエビデンス	監査エビデンス(具体的な確認事項／方法)	トラストサービスプロバイダー監査者評価およびコメント	専門家会議評価およびコメント
101	OVR-A.1-01 [EUSCP]:	対象外	［EUSCP］に準拠する。SSASP は、規則 (EU) No 910/2014 [i. 1] に定義される Qualified TSP であるものとする(SHALL)。 注1：規則（EU）No 910/2014［i.1］の現在の一般的な解釈は、SSASP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）のみを操作するための資格を得ることはできないということである。QSCDを管理するSSASPは、規則（EU）No 910/2014［i.1］に定義されるように、適格トラストサービスの一部として使用することが要求される。 注2：トラストサービスの定義については、Regulation (EU) No 910/2014 [i.1] 第3条 (16) を参照のこと。					
102	A.2　Policy name and identification [EUSCP]:	対象外	本文書に従うSSASPは、以下の特定のトラストサービスポリシーOIDを介して、本文書への準拠を主張することができる。 a)☒USCP: EU SSASCポリシー itu-t(0) identified-organization(4) etsi(0) SIGNATURE CREATION SERVICE-policies(19431) ops (1) policy-identifiers(1) eu-remote-qscd (3)					
-	A.3　General requirements		一般的要求事項					
103	OVR-A.3-01 [EUSCP]:	対象外	[EUSCP]:[NSCP]に規定された全ての要求事項を適用するものとする(SHALL)。					
104	OVR-A.3-02 [EUSCP]:	対象外	[EUSCP]: TSP の運用規定には、規則(EU)No 910/2014[i.1] 附属書 II の要求事項に対して QSCD が採用した証明書への言及を含めるものとする(SHALL)。					
-	A.4　Signing key generation		署名鍵の生成					
105	GEN-A.4-01 [EUSCP]:	対象外	[ESCP]:署名者の署名鍵は、QSCD で生成されるものとする(SHALL)。					
106	GEN-A.4-02 [EUSCP]:	対象外	[EUSCP]:QSCDは、適切な認証ガイダンス文書に記載された構成で、または同じセキュリティ目的を達成する同等の構成で運用されるものとする(SHALL)。					
-	A.5　Signature activation		署名活性化					
107	SIG-A.5-01 [EUSCP]:	対象外	[EUSCP]:署名者の署名鍵は、QSCDで使用されるものとする(SHALL)。					
108	SIG-A.5-02 [EUSCP]:	対象外	[EUSCP] QSCDは、適切な認証ガイダンス文書に記載された構成で、または同じセキュリティ目的を達成する同等の構成で運用されるものとする(SHALL)。					
109	SIG-A.5-03 [EUSCP]:	対象外	[EUSCP]:「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」 の SRA_SAP.1.3 項（暗号強度の規定）を適用するものとする(SHALL)。					
110	SIG-A.5-04 [EUSCP]:	対象外	[Euscp]:「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」 の SRA_SAP.1.4 項 （脅威の軽減に関する規定）を適用しするものとする(SHALL)。					
111	SIG-A.5-05 [EUSCP]:	対象外	[EUSCP]:「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」 の SRA_SAP.1.5 項（環境保護に関する規定）を適用するものとする(SHALL)。					
112	SIG-A.5-06 [EUSCP]:	対象外	[EuscP]:「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」 の SRA_SAP.1.6 項 （改ざんに対する保護規定）を適用するものとする(SHALL)。					
113	SIG-A.5-07 [EUSCP]:	対象外	[EuscP]:「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」 の SRA_SAP.1.7 項 （攻撃者に対する防御規定）を適用するものとする(SHALL)。					
-	A.6　Signature activation data management		署名活性化データの管理					
114	SIG-A.6-01 [EUSCP]:	対象外	[EUSCP]：「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」 の SRA_SAP.2.1項 （署名活性化					
115	SIG-A.6-02 [EUSCP]:	対象外	[EUSCP]：「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」 の SRA_SAP.2.2 項（ 署名活性化データの収集と生成に関する規定）を適用するものとする(SHALL)。					
116	SIG-A.6-03 [EUSCP]:	対象外	[EUSCP]：「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」 の SRA_SAP.2.3項（署名活性化データのパラメータに関する規定 ）を適用するものとする(SHALL)。					
117	SIG-A.6-04 [EUSCP]:	対象外	[EUSCP]：「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」 の SRA_SAP.2.4 項（ 署名活性化データの使用法に関する規定）を適用するものとする(SHALL)。					
118	SIG-A.6-05 [EUSCP]:	対象外	[EUSCP]：「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」 の SRA_SAP.2.5 項（ 署名活性化データの提出先に関する規定する）を適用するものとする。					
119	SIG-A.6-06 [CONDITONAL] [EUSCP]:	対象外	[EUSCP] ：「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」　SRA_SAP.2.6項（ 署名者が自然人の場合の署名活性化データの収集と保護に関する規定）を適用するものとする(SHALL)。					
120	SIG-A.6-07 [CONDITONAL]	対象外	[EUSCP] ：「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」 のSRA_SAP.2.7項（署名者が自					
121	SIG-A.6-08 [EUSCP]:	対象外	[EUSCP]：「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」 のSRA_SAP.2.8項（ 活性化後の署名活性化データ保護に関する規定）を適用するものとする(SHALL)。					
「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」								
-	6 Security requirements		6 セキュリティ要件					
-	6.1 General		6.1 一般事項					
-	6.2 General security requirements (SRG)		6.2 一般的なセキュリティ要件 (SRG)					
-	6.2.1 Management (SRG_M)		6.2.1 管理 (SRG_M)					
-	6.2.1.1 General		6.2.1.1 一般事項					
-	6.2.1.2 Systems and security management (SRG_M.1)		6.2.1.2 システムとセキュリティ管理 (SRG_M.1)					
122	SRG_M.1.1	○	SSASCは異なる特権を持つロールをサポートするものとする(SHALL)。					
123	SRG_M.1.2	○	SSASCは最低限、下記のロールをサポートするものとする(SHALL):					
124	-	○	セキュリティオフィサー: セキュリティポリシー、セキュリティプラクティスの実施を管理する全体的な責任を持ち、セキュリティ関連情報へアクセスできるロール。					

監査報告書リスト番号	要求識別子	監査対象	要求事項	措置状況	確認したエビデンス	監査エビデンス(具体的な確認事項／方法)	トラストサービスプロバイダー監査者評価およびコメント	専門家会議評価およびコメント
125	-	○	システム管理者：SSASCのインストール、設定、保守を行う権限を持つが、セキュリティ関連情報へのアクセスは制御されるロール。					
126	-	○	システムオペレーター：SSASCの日常的な運用に責任を持ち、システムのバックアップとリカバリーを実行する権限を持つロール。					
127	-	○	システム監査人：セキュリティポリシーに沿ったシステムの運用を監査する目的で、SSASCのアーカイブや監査ログの閲覧の権限を持つロール。					
128	-	○	セキュリティオフィサーとシステム管理者は特権システムユーザーである。					
129	-	○	システムオペレーターとシステム監査人は特権を持つが、					
130	SRG_M.1.3	○	SSASCは最低限、下記の非特権ロールをサポートするものとする(SHALL):					
131	-	○	署名者: 文書またはDTBS/Rに署名するために、SADを渡すことにより、SSASCを使用する権限を持つロール。					
132	-	○	SCA: 署名者が署名するために、SSASCにDTBS/R要求を送信する権限を有するロール。					
133	-	○	RA: 証明書発行要求に応じて公開鍵証明書をSSASCに送信する権限を持つロール。					
134	SRG_M.1.4	○	一人の特権ユーザーが全ての特権ロールを担えないものとし(SHALL NOT)、一つ以上の特権ロールを担えるべきではない(SHOULD NOT)。					
135	SRG_M.1.5	○	特権ロールを割り当てられたユーザには、非特権ロールを割り当てないものとする(SHALL NOT)。					
136	-	○	非特権ロールを割り当てられたユーザには、特権ロールを割り当てないものとする(SHALL NOT)。					
137	SRG_M.1.6	○	SSASCは、セキュリティオフィサーのロールを担う権限を持つユーザが、システム監査人のロールを担う権限を持たないことを確実にすることができるものとする(SHALL)。					
138	SRG_M.1.7	○	SSASCは、システム管理者及び/又はシステムオペレータのロールを担う権限を持つユーザが、システム監査人及び/又はセキュリティオフィサーのロールを担う権限を持たないことを確実にすることができるものとする(SHALL)。					
139	SRG_M.1.8	○	特権システムユーザのグループの一員である個人は、指名され、訓練された要員であるものとする(SHALL)。					
140	SRG_M.1.9	○	特権システムユーザーのみが、ハードウェアへ物理的にアクセスでき、SSASCを管理することができるものとする(SHALL)。					
141	SRG_M.1.10	○	特権システムユーザのみが、関連する全てのアプリケーションとインタフェースを通してSSASCを管理する広範な特権を持つものとする(SHALL)。					
-	6.2.2 Systems and operations (SRG_SO)		6.2.2 システムと運用 (SRG_SO)					
-	6.2.2.1 Operations management (SRG_SO.1)		6.2.2.1 運用管理 (SRG_SO.1)					
142	SRG_SO.1.1	○	SSASC構築事業者は、SSASC が下記が実施できるための指示事項が提供されることを確実にするものとする(SHALL):					
143	-	○	— 正しく、安全に運用する。					
144	-	○	— システム障害リスクを最小化する方法でデプロイする。					
145	-	○	— システムと処理する情報の完全性を確実にするためにウィルスや悪意のあるソフトウェアに対して保護する。					
146	SRG_SO.1.2	○	SSASC構築事業者は、SRG_M.1.2で言及した4つの特権ロールの責任をカバーするシステム文書を提供するものとする(SHALL)。それは以下を含むべきである(SHOULD):					
147	-	○	— インストールガイド					
148	-	○	— 管理ガイド					
149	-	○	— ユーザーガイド					
-	6.2.2.2 Time synchronization (SRG_SO.2)		6.2.2.2 時刻同期 (SRG_SO.2)					
150	SRG_SO.2.1	○	SSASC構築事業者は、SSASCの時刻精度とそれを確実にする方法を表明するものとする(SHALL)。					
151	SRG_SO.2.2	○	監査対象事象の時刻精度を確保するため、標準時と適切に同期した時刻ソースを使用するべきである(SHOULD)。					
152	SRG_SO.2.3	○	証明書が有効期限切れかどうかを確認するために、協定世界時UTCと適切に同期した時刻ソースを使用するものとする(SHALL)。					
-	6.2.3 Identification and authentication (SRG_IA)		6.2.3 識別と認証 (SRG_IA)					
-	6.2.3.1 General		6.2.3.1 一般事項					
-	6.2.3.2 Authentication for privileged and non-privileged roles other than signer (SRG_IA.1)		6.2.3.2 署名者以外の特権および非特権ロールのための認証 (SRG_IA.1)					
153	SRG_IA.1.1	○	SSASCは、各ユーザが、そのユーザまたはそのユーザが担					
154	SRG_IA.1.2	○	ログアウト後の再認証は必須であるものとする(SHALL)。					
155	SRG_IA.1.3	○	認証データの組み合わせを使用する場合、予測不可能であるものとする(SHALL)。					
156	SRG_IA.1.4	○	特権ユーザに対して、ユーザの入力デバイスが放置された場合、認証されたユーザセッションが乗っ取られるリスクを低減するためのメカニズム(例えば、所定のアイドル時間後にユーザセッションを終了させるなど)が実装されるものとする(SHALL)。					
-	6.2.3.3 Authentication failure		6.2.3.3 認証失敗 (SRG_IA.2)					
157	SRG_IA.2.1	○	同一ユーザーからの認証失敗回数が最大許容回数に達した場合、SSASC は、一定時間内または管理者がユーザーのブロックを解除するまで、さらなるユーザー認証試行を防止するものとする(SHALL)。					
-	6.2.4 System access control		6.2.4 システムアクセス制御 (SRG_SA)					
-	6.2.4.1 General		6.2.4.1 一般事項					
-	6.2.4.2 Right management (SRG_SA.1)		6.2.4.2 権限管理 (SRG_SA.1)					
158	SRG_SA.1.1	○	SSASCは、特定された個人が所有または責任を負うシステムまたはユーザーオブジェクトへのアクセスを制御し、制限する機能を提供するものとする(SHALL)。					
159	SRG_SA.1.2	○	SSASCは、機密性の高い残留情報へのアクセス制御を確実に提供するものとする(SHALL)。					
-	6.2.5 Key management (SRG_KM)		6.2.5 鍵管理 (SRG_KM)					
-	6.2.5.1 General		6.2.5.1 一般事項					
-	6.2.5.2 Keys generation (SRG_KM.1)		6.2.5.2 鍵生成 (SRG_KM.1)					
160	SRG_KM.1.1	○	秘密鍵もしくは共通鍵はSCDev内で生成し使用すべきである(SHOULD)。					

監査報告書リスト番号	要求識別子	監査対象	要求事項	措置状況	確認したエビデンス	監査エビデンス(具体的な確認事項／方法)	トラストサービスプロバイダー監査者評価およびコメント	専門家会議評価およびコメント
161	-	○	— 使用されるSCDevは、AVA_VAN.5で補強されたISO/IEC 15408 EAL 4以上が確実にされた、もしくは同等の国内もしくは国際的に認知されたITセキュリティの評価基準が確保された信頼できるシステムであるべきである(SHOULD)。これは、リスク分析に基づき、物理的及びその他の非技術的なセキュリティ対策を考慮した上で、本文書の要求事項を満たすセキュリティターゲットもしくはプロテクションプロファイルであるものとする(SHALL)。					
162	-	○	— 使用されるSCDevは、ISO/IEC 19790 またはFIPS PUB 140-2レベル3で特定される要件を満たすべきである(SHOULD)。					
163	SRG_KM.1.2	○	SCDevは、システム設計中に特定されたセキュリティ要求を満たす適切なセキュリティレベルに対応する暗号アルゴリズム及び鍵長をサポートするものとする(SHALL)。					
164	-	○	(例えば署名鍵のバックアップなど)機密性または完全性保護サービスが必要な場合には、同等以上の暗号強度を持つ暗号アルゴリズムおよびアルゴリズムパラメータのみを使用するものとする(SHALL)。					
165	SRG_KM.1.3	○	(署名者署名鍵、インフラストラクチャ鍵、制御鍵を含め)秘密鍵または共通鍵がSCDevの外部で保持される場合、これらの鍵は鍵の機密性と完全性を確実にするために保護されるものとする(SHALL)。					
166	SRG_KM.1.4	○	SCDevは、署名鍵を生成または格納する前に、少なくとも2					
-	6.2.5.3 Keys storage, backup and recovery (SRG_KM.2)		6.2.5.3 鍵の保管、バックアップ、リカバリ (SRG_KM.2)					
167	SRG_KM.2.1	○	全ての秘密鍵または共通鍵は(署名者署名鍵、インフラストラクチャ鍵、制御鍵を含め)、安全に保管されるものとする(SHALL)。即ち、保護されていない状態で保管してはならな					
168	SRG_KM.2.2	○	(署名者署名鍵、インフラストラクチャ鍵、制御鍵を含め)任意の秘密鍵もしくは共通鍵が当該SCDevからエクスポートされる場合、SCDevに内と同等以上のセキュリティレベルで機密性と完全性を確実にするために、その鍵は保護されるものとする(SHALL)。					
169	-	○	秘密鍵/共通鍵が暗号化により保護される場合は、同等以上の暗号強度を持つ暗号アルゴリズムおよびアルゴリズムパラメータのみを使用するものとする(SHALL)。					
170	SRG_KM.2.3	○	SSASCは、(署名者署名鍵、インフラストラクチャ鍵、制御鍵を含め)秘密鍵もしくは共通鍵のバックアップ、保管、リカバリが、認可された要員によってのみ行われることを確実にするものとする(SHALL)。ユーザー鍵および作業鍵の両方を保護するために使用するマスター鍵は、少なくとも複数人制御の下でバックアップ、保管、リロードされるものとする(SHALL)。SCDevの外部では、当該マスターキーは、保護された形でのみ保有されるものとする(SHALL)。					
-	6.2.5.4 Key usage (SRG_KM.3)		6.2.5.4 鍵の利用 (SRG_KM.3)					
171	SRG_KM.3.1	○	秘密鍵と共通鍵は(署名者署名鍵、インフラストラクチャ鍵、制御鍵を含め)その意図された目的のためだけに使用されるものとする(SHALL)。					
172	SRG_KM.3.2	○	秘密鍵と共通鍵は(署名者署名鍵、インフラストラクチャ鍵、制御鍵を含め)その目的に満たすために必要な場合を除いて、共有はされないものとする(SHALL NOT)。					
173	SRG_KM.3.3	○	アクセス制御は、(署名者署名鍵、インフラストラクチャ鍵、制御鍵を含め)鍵のアクセスと利用が保護された場所で行われるものとする(SHALL)。					
174	SRG_KM.3.4	○	署名鍵は唯一の署名者および、唯一の公開鍵証明書に紐付けられるものとする(SHALL)。					
-	6.2.5.5 Key distribution (SRG_KM.4)		6.2.5.5 鍵の配布 (SRG_KM.4)					
175	SRG_KM.4.1	○	(インフラストラクチャ鍵及び制御鍵を含む)秘密鍵もしくは共通鍵は、送信する必要がある場合、安全に送信されるものとする(SHALL)。					
176	SRG_KM.4.2	○	送信中に他の秘密鍵/共通鍵を保護するために使用される全ての鍵は、送信される鍵と(少なくとも)同程度の強度であるものとする(SHALL)。					
-	6.2.5.6 Key renewal/update/change (SRG_KM.5)		6.2.5.6 鍵の更新と変更 (SRG_KM.5)					
177	SRG_KM.5.1	○	インフラストラクチャ鍵および制御鍵は、リスク評価に基づく頻度で定期的に変更すべきである(SHOULD)。					
178	SRG_KM.5.2	○	鍵アルゴリズムもしくは鍵長が不適切になったと判断した場合、そのアルゴリズムに基づく鍵は直ちに変更されるものとする(SHALL)。					
179	SRG_KM.5.3	○	鍵の危殆化、もしくは危殆化が疑われる場合、直ちにその鍵を変更するべきである(SHOULD)。					
-	6.2.5.7 Key archiving (SRG_KM.6)		6.2.5.7 鍵のアーカイブ (SRG_KM.6)					
180	SRG_KM.6.1	○	署名鍵はアーカイブされないものとする(SHALL NOT)。					
-	6.2.5.8 Key deletion (SRG_KM.7)		6.2.5.8 鍵の削除 (SRG_KM.7)					
181	SRG_KM.7.1	○	署名鍵は、公開鍵証明書の有効期限が切れた後、もしくは署名者にとって不必要になった場合、破棄されるものとする(SHALL)。					
182	SRG_KM.7.2	○	署名鍵と署名者の間のリンクが署名操作セッションの後に維持されない場合、署名鍵は署名操作セッションの終了時に破棄されるものとする(SHALL)。					
183	SRG_KM.7.3	○	署名鍵破壊の仕組みと手順では、破壊された署名鍵の全てのバックアップもまた破壊され、残っている情報が署名鍵を再構築するために使用できないことを確実にすべきである(SHOULD)。					
184	-	対象外	注: この推奨事項は、バックアップ中の一つの鍵を指定した削除が現実的ではない場合には適用されない。					
-	6.2.6 Auditing (SRG_AA)		6.2.6 監査(SRG_AA)					
-	6.2.6.1 Audit data generation (SRG_AA.1)		6.2.6.1 監査データの生成（SRG_AA.1）					
185	-	対象外	各サービスには、これらの一般的な要件に加え、さらに特定の監査要件があり、これに対処するものとする（SHALL）。					
186	SRG_AA.1.1	○	最低限、以下のイベントは記録されるものとする（SHALL）：					

監査報告書リスト番号	要求識別子	監査対象	要求事項	措置状況	確認したエビデンス	監査エビデンス(具体的な確認事項／方法)	トラストサービスプロバイダー監査者評価およびコメント	専門家会議評価およびコメント
187	SRG_AA.1.2	○	TSPは、外部ストレージへの監査情報の転送が失敗した場合に何を行うか（すなわち、取られる措置）を明示するものとする（SHALL）。					
-	6.2.6.2 Guarantees of audit data availability (SRG_AA.2)		6.2.6.2 監査データの利用可能性の保証（SRG_AA.2）					
188	SRG_AA.2.1	○	SSASCは、監査データを維持し、すべての監査データを保存するための措置を講じることを確実にするものとする（SHALL）。					
189	SRG_AA.2.2	○	監査機能は、情報を追加するだけであるものとする（SHALL）。					
190	SRG_AA.2.3	○	SSASCは、監査証跡に保存された監査記録を、権限を伴わない削除から保護するものとする（SHALL）。					
191	SRG_AA.2.4	○	監査記録は、外部ストレージにアーカイブすれば、内部からは削除できる（MAY）。					
-	6.2.6.3 Audit data parameters (SRG_AA.3)		6.2.6.3 監査データパラメータ (SRG_AA.3)					
192	SRG_AA.3.1	○	すべての監査記録（サービス固有の監査ログを含む）は、以下のパラメータを含むものとする（SHALL）： - イベントの日時 - イベントのタイプ - アクションに責任を持つエンティティ（ユーザー、管理者、プロセスなど）のアイデンティティ； - 監査イベントの成否。					
-	6.2.6.4 Selectable audit review (SRG_AA.4)		6.2.6.4 選択可能な監査レビュー(SRG_AA.4)					
193	SRG_AA.4.1	○	SSASCは、イベントの日付、イベントのタイプ、及び/又はユーザーのアイデンティティに基づいて、監査ログ内のイベントを検索できるようにするものとする（SHALL）。					
194	SRG_AA.4.2	○	監査記録は、処理可能な形式であり、システム監査人が情報を解釈するのに適した方法で提示されるものとする（SHALL）。					
-	6.2.6.5 Restricted audit review (SRG_AA.5)		6.2.6.5 制限付き監査レビュー (SRG_AA.5)					
195	SRG_AA.5.1	○	SSASCは、デフォルトで、明示的に読み取り権限を付与されたユーザー（例：システム監査の役割を持つユーザー）を除き、監査記録への全てのユーザーの読み取りアクセスを拒否するものとする（SHALL）。					
-	6.2.6.6 Generation of warning (SRG_AA.6)		6.2.6.6 警告の生成(SRG_AA.6)					
196	SRG_AA.6.1	○	SSASCは、署名サーバーシステムが本規定で特定されるセキュリティ要件を満たす能力に影響を及ぼしうる異常なイベントを適時に通知する警告を生成するものとする（SHALL）。 異常なイベントが検出されるたびに警告を発する機構を実装すべきである（SHOULD）。警告は、関連する管理者に通知するトリガーとなるべきである（SHOULD）。 警告は、攻撃される可能性のある経路を遮断するなど、攻撃の可能性に対応するためのさらなる行動のトリガーとすることができる(MAY)。 ユーザー活動に関連する異常事態の例としては、以下のようなものが考えられる（ただし、これらに限定されない）： - 標準的な利用時間外のユーザーの行為。 - 異常な速度で実行されるユーザーアクション（人間以外の介入を検出するため）。 - 定義されたプロセス内の標準的なアクティビティをスキップするユーザーアクション。 - 重複するユーザーセッション。					
-	6.2.6.7 Guarantees of audit data integrity (SRG_AA.7)		6.2.6.7 監査データの完全性の保証（SRG_AA.7）					
197	SRG_AA.7.1	○	SSASCは、監査データの完全性を確実にするものとする（SHALL）。					
198	SRG_AA.7.2	○	SSASCは、監査データの完全性を検証する機能を提供するものとする（SHALL）。					
-	6.2.6.8 Guarantees of audit timing (SRG_AA.8)		6.2.6.8 監査時刻の保証 (SRG_AA.8)					
199	SRG_AA.8.1	○	監査対象イベントの時刻の精度を確実にするため、要求事項SRG_SO.2.2を適用する。					
-	6.2.7 Archiving (SRG_AR)		6.2.7 アーカイビング（SRG_AR）					
-	6.2.7.1 Archive data generation (SRG_AR.1)		6.2.7.1 アーカイブデータ生成 (SRG_AR.1)					
200	SRG_AR.1.1	○	TSPは、外部メディア上にアーカイブを生成することができるものとする（SHALL）。 このメディアは、保存とその後の処理に適切であり、デジタル署名のサポートに必要な法的証拠を提供できるものであるべきである（SHOULD）。 注 これらのポリシー要件は、適切な規格が利用可能になった時点でその規格に移行される予定である。					
201	SRG_AR.1.2	○	すべての監査ログは、アーカイブされるものとする（SHALL）。					
202	SRG_AR.1.3	○	各アーカイブエントリは、アーカイブが発生した時刻を含むものとする（SHALL）。					
203	SRG_AR.1.4	○	アーカイブは、SSASCユーザーパスワードのような機密性の高いセキュリティパラメータを含まないものとする（SHALL NOT）。					
-	6.2.7.2 Integrity of archived data (SRG_AR.2)		6.2.7.2 アーカイブデータの完全性 (SRG_AR.2)					
204	SRG_AR.2.1	○	アーカイブの各エントリーの権限を伴わない改変を防止するものとする（SHALL）。権限を伴わない改変を検出するために、完全性を検証する機構を設けるものとする（SHALL）。					
-	6.2.8 Backup and recovery (SRG_BK)		6.2.8 バックアップとリカバリー（SRG_BK）					
-	6.2.8.1 General		6.2.8.1 一般事項					
-	6.2.8.2 Integrity and confidentiality of backup information (SRG_BK.1)		6.2.8.2 バックアップ情報の完全性及び機密性 (SRG_BK.1)					
205	SRG_BK.1.1	○	バックアップは、バックアップ情報の完全性を検証すること					
206	SRG_BK.1.2	○	機密性の高いセキュリティパラメータやその他の機密情報は、機密性と完全性を確実にするために、保護された形で保存されるものとする（SHALL）。					
-	6.2.8.3 Recovery (SRG_BK.2)		6.2.8.3 リカバリー（SRG_BK.2）					
207	SRG_BK.2.1	○	SSASCは、バックアップからシステムの状態を復元することができるリカバリー機能を含むものとする（SHALL）。					

監査報告書リスト番号	要求識別子	監査対象	要求事項	措置状況	確認したエビデンス	監査エビデンス(具体的な確認事項／方法)	トラストサービスプロバイダー監査者評価およびコメント	専門家会議評価およびコメント
208	SRG_BK.2.2	○	十分な権限を持つロールにリンクされたユーザは、バックアップからオンデマンドで復旧機能を呼び出すことが可能であるものとする（SHALL）。					
-	6.3 Core components security requirements (SRC)		6.3 コアコンポーネントのセキュリティ要求事項(SRC)					
-	6.3.1 Signing key setup (SRC_SKS) - Cryptographic key (SRC_ SKS.1)		6.3.1 署名鍵設定（SRC_SKS） - 暗号鍵（SRC_SKS.1）					
209	SRC_SKS.1.1	○	信頼できるシステムによる署名生成に使用する☒ルゴリズムパラメータは、署名者の証明書のライフタイムの間、耐えられるよう選択されるものとする（SHALL）。 注 Cryptrecの電子政府推奨暗号リストを参照することを推奨する。					
210	SRC_SKS.1.2	○	SSASCは、署名者の署名鍵を、適切な署名者の公開鍵証明書とリンクさせるものとする（SHALL）。					
211	SRC_SKS.1.3	○	署名者の署名鍵は、事前に生成することができる(MAY)（すなわち、公開鍵証明書と連動しない）。					
212	SRC_SKS.1.4	○	署名鍵は、その公開鍵証明書がSSASCによってリンクされる前に使用されるべきではない（SHOULD NOT）。 注：この勧告は、署名鍵が証明書を取得するための所有証明の署名に使用される場合は適用されない。					
213	SRC_SKS.1.5	○	SSASCは、署名者の署名鍵と公開鍵の間のリンクの完全性を保護するものとする（SHALL）。					
-	6.3.2 Signer authentication (SRC_SA)		6.3.2 署名者認証（SRC_SA）					
-	6.3.2.1 Signer authentication for SCAL1 (SRC_SA.1)		6.3.2.1 SCAL1 の署名者認証（SRC_SA.1）					
214	SRC_SA.1.1	○	署名者の登録の保証レベルは、別表AのA.1に規定される「低」あるいはそれ以上であるものとする（SHALL）。 電子識別手段の特性および設計の保証レベルは、別表AのA.2.1に規定される「低」あるいはそれ以上であるものとする（SHALL）。 認証メカニズムの保証レベルは、別表AのA.2.2に規定される「低」あるいはそれ以上であるものとする（SHALL）。					
215	SRC_SA.1.2	○	SSASCは、署名鍵の単独制御に影響を与える可能性のある行為を許可する前に、各署名者の識別と認証に成功することを要求するものとする（SHALL）。					
216	SRC_SA.1.3	○	使用するプロトコルは、中間者攻撃、リプレイ攻撃、より一般的には悪意のあるユーザが自分のものではない認証情報を使用することができるあらゆる形態の攻撃を防止するものとする（SHALL）。					
217	SRC_SA.1.4	○	アクセス制御は、署名者が機密性の高いシステムオブジェクトや、他の署名鍵の制御をユーザに与える機能へのアクセス権を持たないことを確実にするものとする(SHALL)。					
218	SRC_SA.1.5	○	SSASCは、署名者の制御下で提供されるDTBS/Rが、この署名者に属する署名鍵によってのみ署名されることを確実にするものとする（SHALL）。					
-	6.3.2.2 Authentication failure handling (SRC_SA.2)		6.3.2.2 認証失敗時の対応（SRC_SA.2）					
219	SRC_SA.2.1	○	与えられた署名者について、SSASCは、定義された回数の連続した認証失敗が発生した場合、それを検知するものとする(SHALL)。					
220	SRC_SA.2.2	○	所定の署名者について、定義された認証失敗回数に至った場合、SSASCは、妥当な期間、または管理者の役割によりユーザーのブロックを解除するまで、このユーザーのアクセスをブロックするものとする（SHALL）。					
-	6.3.2.3 Signer authentication delegated to external system (SRC_SA.3)		6.3.2.3 外部システムに委任された署名者認証（SRC_SA.3）					
221	SRC_SA.3.1	○	署名者認証が外部システムに委任される場合、TSPは、SRC_SA.1節およびSRC_SA.2節に規定される要件が外部システムによって満たされることを確実にするものとする（SHALL）。					
-	6.3.3 Digital signature creation (SRC_DSC) - Cryptographic operation (SRC_DSC.0)		6.3.3 電子署名生成（SRC_DSC） - 暗号操作（SRC_DSC.1）					
222	SRC_DSC.1.1	○	信頼できるシステムによる署名生成に使用されるアルゴリズムパラメータは、署名者の証明書の有効期間中に耐えられるように選択されるものとする（SHALL）。 注 Cryptrecの電子政府推奨暗号リストを参照するとよい。					
-	6.4 Additional security requirements for SCAL2 (SRA)		6.4 SCAL2に対する追加セキュリティ要求事項（SRA）					
-	6.4.1 General		6.4.1 一般事項					
-	6.4.2 Signature activation protocol and signature activation data (SRA_SAP)		6.4.2 署名活性化プロトコル及び署名活性化データ (SRA_SAP)					
-	6.4.2.1 Threat resistance (SRA_SAP.1)		6.4.2.1 脅威への耐性（SRA_SAP.1）					
223	SRA_SAP.1.1	○	署名者の登録保証レベルは別表AのA.1に規定される「十分」以上であるものとする（SHALL）。 電子識別手段の特性及び設計の保証レベルは、別表AのA.2.1に規定される「十分」以上であるものとする（SHALL）。 認証メカニズムの保証レベルは、別表AのA.2.2に規定される「十分」以上であるものとする（SHALL）。					
224	SRA_SAP.1.2	対象外	SADおよびSAD使用に関する以下の脅威（オンライン推測、オフライン推測、クレデンシャル複製、フィッシング、盗聴、リプレイ、セッションハイジャック、中間者、クレデンシャル盗難、スプーフィング、マスカレード攻撃）に対抗するため、リスクアセスメントにより必要とされるコントロールを提供するものとする（SHALL）。					
225	SRA_SAP.1.3	対象外	SAPは、プロトコルの脅威や信頼できる第三者のなりすまし攻撃による侵害から認証要素を保護する暗号強度のメカニズムを提供するものとする（SHALL）。					
226	SRA_SAP.1.4	対象外	SAPは、署名者とリモートSCDev間のリプレイ、バイパス、偽造攻撃に対して保護される（例えば、nonce、タイムスタンプ、セッショントークンを使用）ものとする（SHALL)。					

監査報告書リスト番号	要求識別子	監査対象	要求事項	措置状況	確認したエビデンス	監査エビデンス(具体的な確認事項／方法)	トラストサービスプロバイダー監査者評価およびコメント	専門家会議評価およびコメント
227	SRA_SAP.1.5	対象外	SAMは、以下のような改ざん防止された環境で使用されるものとする（SHALL）： - これは、ISO/IEC 15408、またはITセキュリティに関する国内もしくは国際的に認知された同等の評価基準に従い、EAL 4以上が確保された信頼できるシステムである。これは、リスク分析に基づき、物理的及びその他の非技術的なセキュリティ対策を考慮した上で、本文書の要件を満たすセキュリティターゲット又はプロテクションプロファイルに対するものとする（SHALL）。 注 1 ISO/IEC 15408に準拠したTSP暗号モジュールのコモンクライテリア プロテクションプロファイルを規定する規格は、現在CEN内でCEN/TS 419221-2, CEN/TS 419221-3, CEN/TS 419221-4, または EN 419221-5 として開発中である。 - あるいは、ISO/IEC 19790またはFIPS PUB 140-2レベル3で特定される要件を満たす。 注2 ISO/IEC 15408を満たす機器が一般に普及したことで、ISO/IEC 19790やFIPS 140-2のレベル3は通用しなくなることが予想される。					
228	SRA_SAP.1.6	対象外	SAPは、攻撃可能性の高い攻撃者に対して、SADが複製や改ざんから常に確実に保護されていると仮定できるように設計されるものとする（SHALL）。					
229	SRA_SAP.1.7	対象外	SAPは、攻撃可能性の高い攻撃者に対して、署名者がSADによる署名鍵の活性化を常に確実に保護できるように設計されるものとする（SHALL）。					
-	6.4.2.2 SAD Management (SRA_SAP.2)		6.4.2.2 SAD管理（SRA_SAP.2）					
230	SRA_SAP.2.1	○	SADは、データの集合とすることもできるし、以下に示す必須パラメータを用いた暗号操作の結果とすることもできる(MAY)。					
231	SRA_SAP.2.2	○	SADは、署名者の環境の中のSICにより、または署名者の制御下にあるSICを使用して遠隔に収集または生成できる（MAY）。					
232	SRA_SAP.2.3	対象外	SADは、少なくとも以下のパラメータを高い信頼性でリンクするものとする（SHALL）： - 与えられたDTBS/RまたはDTBS/Rの集合、 - 認証された署名者を識別するための項目、および - デフォルトまたは選択された署名鍵 サポートされている場合、法的に許可されていない文脈では、複数のDTBS/Rの使用を無効化することが可能であるものとする（SHALL）。					
233	SRA_SAP.2.4	○	署名者認証に成功した場合のみ、SADを使用して署名鍵を活性化するものとする（SHALL）。 (認証に成功した後にSADを計算すること、または他の暗号化の手段によって）。					
234	SRA_SAP.2.5	対象外	SADは、SAPのSAMに渡されるものとする（SHALL）。					
235	SRA_SAP.2.6	対象外	SADは、以下をすべて満足するものとする（SHALL）： - 署名者の管理下にある方法で、高い信頼性をもって収集されること、 - デバイス内に保持される鍵が安全であるように保護されていること、そして - SRA_SAP.1.4 で定義されているように、使用される秘密（一回限りまたは長期的なもの）を保護すること。					
236	SRA_SAP.2.7	対象外	SAPは、SAMがSADを受領した場合、SADが署名者の単独制御のもと、署名者が所有する手段により提出されたと想定できるように設計されるものとする（SHALL）。					
237	SRA_SAP.2.8	対象外	SADは、攻撃可能性の高い攻撃者による推測、盗聴、リプレイ、通信操作などの行為によって、署名活性化のための認証が破られる可能性が極めて低いことを検証するものとする（SHALL）。					
-	6.4.3 Signing key management (SRA_SKM)		6.4.3 署名鍵管理(SRA_SKM)					
-	6.4.3.1 Signing key generation (SRA_SKM.1)		6.4.3.1 署名鍵生成 (SRA_SKM.1)					
238	SRA_SKM.1.1	対象外	署名者の署名鍵を以下のSCDevで生成し使用するものとする（SHALL）： - ISO/IEC 15408に準拠したAVA_VAN.5で補強されたEAL 4以上、またはITセキュリティに関する国内もしくは国際的に認知された同等の評価基準で確保された信頼できるシステムである。これは、リスク分析に基づき、物理的及びその他の非技術的なセキュリティ対策を考慮した上で、本文書の要求事項を満たすセキュリティターゲット又はプロテクションプロファイルに対するものであるものとする（SHALL）。 注 1 ISO/IEC 15408 に準拠した TSP暗号モジュールのコモンクライテリアプロテクションプロファイルを規定する規格は、現在CEN内で CEN/TS 419221-2, CEN/TS 419221-3, CEN/TS 419221-4, または EN 419221-5 として開発中である。 - あるいは、ISO/IEC 19790 または FIPS PUB 140-2 レベル3で特定される要件を満たす。 注2⊠O/IEC 15408に適合する機器の一般的な普及に伴い、ISO/IEC 19790またはFIPS 140-2のレベル3は受け入れられなくなることが予想される。					
239	SRA_SKM.1.2	○	このSCDev は、署名生成サービスに必要な暗号機能（乱数生成や、場合によってはサーバー署名をサポートする暗号化も含む）のサポート専用であるものとする（SHALL)。					
240	SRA_SKM.1.3	対象外	署名鍵の生成に使用するSCDevが署名操作に使用するSCDevと異なる場合、署名鍵の転送はSRG_KM.4.1を要求するものとする（SHALL）。					
241	SRA_SKM.1.4	○	SCDevは、同じ署名者及び異なる署名者のための複数の署名鍵を含むことができる(MAY)。 同一署名者または異なる署名者の複数の署名鍵がSCDevに含まれる場合、鍵の使用に関する管理の分離を確実にするものとする（SHALL)。					
242	SRA_SKM.1.5	対象外	署名者の署名鍵は、SAPが提供する手段により、その署名者に高い信頼性でリンクされるものとする（SHALL）。					
243	SRA_SKM.1.6	○	署名者の署名鍵は、その署名者がSSASCによってリンクされる前に使用されないものとする（SHALL NOT）。					
244	SRA_SKM.1.7	対象外	SSASCは、署名鍵を活性化するために、いくつかの異なるSAPとSADのメカニズムをサポートしてもよい(MAY)。 ただし、1つの署名鍵は、1つのSADおよびSAP機構にのみリンクされるものとする（SHALL）。					

監査報告書リスト番号	要求識別子	監査対象	要求事項	措置状況	確認したエビデンス	監査エビデンス(具体的な確認事項／方法)	トラストサービスプロバイダー監査者評価およびコメント	専門家会議評価およびコメント
-	6.4.3.2 Signing key activation (SRA_SKM.2)		6.4.3.2 署名鍵の活性化 (SRA_SKM.2)					
245	SRA_SKM.2.1	対象外	SSASCは、署名者を認証し、署名鍵を活性化するために、署名者がSAMに対してSADを提示することを要求するものとする（SHALL)。					
246	SRA_SKM.2.2	対象外	SAPは、署名鍵が高い信頼性で署名者の制御下にあることを保証する方法で、SADのSAMへの転送を制御するものとする（SHALL)。					
247	SRA_SKM.2.3	○	署名者の署名鍵は、リモートSCDevでの使用のためにのみ活性化されるものとする（SHALL）。					
248	SRA_SKM.2.4	○	署名者の署名鍵は、署名者の認証要素を用いて生成されたSADにより、正しい鍵へのリファレンスで活性化されるものとする（SHALL）。					
249	SRA_SKM.2.5	対象外	活性化された署名鍵は、SAPによって認可されたDTBS/Rのみに署名するために使用されるものとする（SHALL）。					
250	SRA_SKM.2.6	○	SADのDTBS/RがSCAから来る場合、そのソースは認証されるものとする（SHALL)。					
251	SRA_SKM.2.7	○	特権ユーザは、署名者に割り当てられた署名鍵を使用することができないものとする（SHALL NOT)。					
252	SRA_SKM.2.8	○	署名鍵の活性化とデジタル署名の生成後、署名者のSADをSSASCが保護されない状態で保存しないものとする（SHALL NOT)。					
「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」								
-	5 Risk Assessment		5 リスク評価					
253	REQ-5-01	○	TSPは、ビジネスおよび技術的な問題を考慮して、トラストサービスのリスクを特定、分析、評価するためのリスクアセスメントを実施するものとする。[SHALL]					
254	REQ-5-02	○	TSPは、リスクアセスメント結果を考慮して、適切なリスク対応策を選択するものとする。リスク対応策は、セキュリティのレベルがリスクの程度に見合ったものであることを保証するものとする。[SHALL] 注:情報セキュリティマネジメントシステムの一部としての情報セキュリティリスクマネジメントに関するガイダンスについては、ISO/IEC 27005:2018 [i.5]を参照のこと。					
255	REQ-5-03	○	TSPは、情報セキュリティポリシーおよびトラストサービス業務規程(第6章を参照)に文書化されているように、選択したリスク対応策を実装するために必要なすべてのセキュリティ要件と運用手順を決定するものとする。[SHALL]					
256	REQ-5-04	○	リスクアセスメントは定期的に見直され、改訂されるものとする。[SHALL]					
257	REQ-5-05	○	TSPの経営陣はリスクアセスメントを承認し、特定された残留リスクを受け入れるものとする。[SHALL]					
-	6 Policies and practices		6 方針と実践					
-	6.1 Trust Service Practice statement		6.1 トラストサービス業務規程					
258	REQ-6.1-01	○	TSPは、提供する信頼サービスに適した一連のポリシーと業務を指定するものとする。[SHALL]					
259	REQ-6.1-02	○	一連のポリシーと業務は、経営陣によって承認され、公開され、関連する従業員や外部関係者に伝達されるものとする。[SHALL]					
260	• REQ-6.1-03	対象外	廃止					
261	• REQ-6.1-03A	○	TSPは、TSPが特定した適用可能なトラストサービスポリシーのすべての要件に対処するために使用される業務と手順の記述を持つものとする。[SHALL] 注1:この文書は、トラストサービス業務規程の構造に関していかなる要件も設けていない。					
262	• REQ-6.1-04	○	TSPのトラストサービス業務規程は、適用されるポリシーと業務を含む、TSPのサービスをサポートするすべての外部組織の義務を特定するものとする。[SHALL]					
263	• REQ-6.1-05	対象外	廃止					
264	• REQ-6.1-05A	○	TSPは、トラストサービスポリシーへの準拠を証明するために必要に応じて、その業務規程およびその他の関連文書を利用者および依拠当事者に提供するものとする。[SHALL] 注2:TSPは、利用者および依拠当事者に提供されるドキュメント内の機密情報を含む側面を開示する必要はない。					
265	• REQ-6.1-06	○	TSPは、TSPの業務規程を承認する最終権限を持つ、TSPに対する全体的な責任を負う管理機関を持つものとする。[SHALL]					
266	• REQ-6.1-07	○	TSPの管理者は業務を実装するものとする。[SHALL]					
267	• REQ-6.1-08	○	TSPは、TSPの業務規程を維持する責任を含む業務のレビュープロセスを定義するものとする。[SHALL] 注3:変更の予告には変更の詳細を記載する必要はない。予告はTSPのリポジトリで公開できる。					
268	• REQ-6.1-09	対象外	廃止					
269	• REQ-6.1-09A [CONDITIONAL]	○	TSPが、対象者、利用者、または依拠当事者によるサービスの受け入れに影響を与える可能性のあるトラストサービス実施声明の変更を行おうとする場合、利用者および依拠当事者に変更について適切に通知するものとする。注3:変更予告通知には変更の詳細を記載する必要はない。通知はTSPのリポジトリで公開できる。[SHALL]					
270	• REQ-6.1-10	○	TSPは、上記REQ-6.1-06の承認後、上記REQ-6.1-05の要求に応じて、修正されたトラストサービス業務規程を直ちに利用できるようにするものとする。[SHALL]					
271	• REQ-6.1-11	○	TSPは、サービスの終了に関する規定をその業務規程の中で明記するものとする(第7章第12項を参照)。[SHALL]					
-	6.2 Terms and Conditions		6.2 利用規約					
272	REQ-6.2-01	○	TSPは、そのサービスに関する契約条件をすべての利用者および依拠当事者が利用できるようにするものとする。[SHALL]					

監査報告書リスト番号	要求識別子	監査対象	要求事項	措置状況	確認したエビデンス	監査エビデンス(具体的な確認事項／方法)	トラストサービスプロバイダー監査者評価およびコメント	専門家会議評価およびコメント
273	REQ-6.2-02	○	利用規約では、TSPによってサポートされる各トラストサービスポリシーについて少なくとも次の内容を指定するものとする。 [SHALL] a)適用されているトラストサービスポリシー。 b)制限を超えたサービスの使用から生じる損害の制限を含む、提供されるサービスの使用に関する制限。 例1:公開鍵証明書の有効期間。 c)利用者の義務（ある場合）。 d)トラストサービスに依存する依拠当事者向けの情報。 例2:トラストサービストークンを検証する方法、トラストサービストークンに関連付けられた有効期間に考えられる制限。 e)TSPのイベントログが保持される期間。 f)責任の制限。 g)適用される法制度。 h)苦情および紛争解決の手順。 i)TSPのトラストサービスがトラストサービスポリシーに準拠していると評価されているかどうか、準拠している場合はどの準拠評価スキームによって評価されるか。 j)TSPの連絡先情報。 k)可用性に関するあらゆる約束。					
274	REQ-6.2-03	○	利用者およびトラストサービスに依存する依拠当事者は、契約関係を締結する前に、上記の項目を含む正確な契約条件を知らされるものとする。[SHALL]					
275	REQ-6.2-04	○	利用規約は、耐久性のある通信手段を通じて入手できるものとする。[SHALL]					
276	REQ-6.2-05	○	利用規約は、容易に理解できる言語で提供されるものとする。[SHALL]					
277	REQ-6.2-06	○	契約条件は電子的に送信される場合があってもよい。[MAY]					
-	6.3 Information security policy		6.3 情報セキュリティポリシー					
278	REQ-6.3-01	○	TSPは、経営陣によって承認され、情報セキュリティを管理する組織のアプローチを規定する情報セキュリティポリシーを定義するものとする。[SHALL]					
279	REQ-6.3-02	○	情報セキュリティポリシーの変更は、該当する場合、第三者に通知されるものとする。これには、利用者、依拠当事者、評価機関、監督機関、またはその他の規制機関が含まれます。[SHALL]					
280	• REQ-6.3-03	○	TSPの情報セキュリティポリシーは、サービスを提供するTSPの施設、システム、情報資産のセキュリティ管理と運用手順を含め、文書化、実装、維持されるものとする。 [SHALL]					
281	• REQ-6.3-04	○	TSPは、情報セキュリティポリシーを公開し、そのポリシーの影響を受けるすべての従業員に伝達するものとする。 [SHALL] 注1:ガイダンスについては、ISO/IEC 27002:2022 [i.3]の条項5.1.1を参照のこと。					
282	• REQ-6.3-05	○	TSPは、TSPの機能が委託先によって引き受けられる場合でも、情報セキュリティポリシーに規定された手順への準拠について全体的な責任を負うものとする。[SHALL]					
283	• REQ-6.3-06	○	TSPは委託先の責任を定義し、委託先がTSPが要求するあらゆる管理を実施する義務を負うことを保証するものとする。 [SHALL]					
284	• REQ-6.3-07	○	TSPの情報セキュリティポリシーおよび情報セキュリティ資産の目録(第7.3項を参照)は、計画された間隔で、または重大な変更が発生した場合に、継続的な適合性、適切性、および有効性を確保するために見直されるものとする。[SHALL]					
285	• REQ-6.3-08	○	提供されるセキュリティのレベルに影響を与える変更は、REQ-6.1-07で参照される管理機関によって承認されるものとする。[SHALL]					
286	• REQ-6.3-09	○	TSPシステムの構成は、TSPのセキュリティポリシーに違反する変更がないか定期的にチェックされるものとする。 [SHALL]					
287	• REQ-6.3-10	○	2つのチェック間の最大間隔は、トラストサービス業務規程に文書化されるものとする。[SHALL] 注2:さらに具体的な推奨事項は、CA/Browser Forumネットワークセキュリティガイド[i.7]の項目1に記載されています。					
-	7 TSP management and operation		7 TSPの管理と運用					
-	7.1 Internal organization		7.1 内部組織					
-	7.1.1 Organization reliability		7.1.1 組織の信頼性					
288	REQ-7.1.1-01	○	TSP組織は信頼できるものでなければならないものとする。 [SHALL]					
289	• REQ-7.1.1-02	○	TSPが運営するトラストサービスの業務は、差別的であってはならないものとする。[SHALL]					
290	• REQ-7.1.1-03	○	TSPは、その活動が事業分野に該当し、TSPの利用規約に指定されている義務を遵守することに同意するすべての申請者がそのサービスにアクセスできるようにするべきである。 [SHOULD]					
291	• REQ-7.1.1-04	○	TSPは、運用および/または活動から生じる責任をカバーするために、適用法に従って、十分な財源を維持し、および/または適切な賠償責任保険を利用するものとする。[SHALL]					
292	• REQ-7.1.1-05	○	TSPは、このポリシーに従って運営するために必要な財務的安定性とリソースを備えているものとする。[SHALL]					
293	• REQ-7.1.1-06	○	TSPは、サービスの提供またはその他の関連事項に関して顧客または他の依拠当事者から受け取った苦情および紛争を解決するためのポリシーと手順を持つものとする。[SHALL]					
294	• REQ-7.1.1-07	○	TSPは、サービスの提供に下請け、外部委託、またはその他の第三者の取り決めが含まれる場合、文書化された合意および契約関係を整備するものとする。[SHALL]					
295	• REQ-7.1.1-08 [CONDITIONAL]	○	TSPが、下請け、外部委託、またはその他の第三者の取り決めを通じてサービスの一部を提供するために、トラストサービスコンポーネントプロバイダーを含む他の第三者を利用する場合、TSPは、トラストサービスポリシーにおいて規定された要件に適合するための全体的な責任を維持するものとする。[SHALL]					

監査報告書リスト番号	要求識別子	監査対象	要求事項	措置状況	確認したエビデンス	監査エビデンス(具体的な確認事項／方法)	トラストサービスプロバイダー監査者評価およびコメント	専門家会議評価およびコメント
296	• REQ-7.1.1-09 [CONDITIONAL]	○	TSPが別の当事者によって提供されたトラストサービスコンポーネントを利用する場合、コンポーネントインターフェイスの使用がトラストサービスコンポーネントプロバイダーによって指定された要件を満たすことを保証するものとする。[SHALL]					
297	• REQ-7.1.1-10 [CONDITIONAL]	○	TSPが別の当事者によって提供されたトラストサービスコンポーネントを利用する場合、トラストサービスコンポーネントによって要求されるセキュリティと機能が、該当するポリシーの適切な要件を満たしていることを保証するものとする。[SHALL]					
-	7.1.2 Segregation of duties		7.1.2 職務の分離					
298	REQ-7.1.2-01	○	TSPの資産の不正または意図しない変更または悪用の機会を減らすために、職務および責任領域は適切に分離されるものとする。[SHALL]					
-	7.2 Human resources		7.2 人材					
299	REQ-7.2-01	○	TSPは、従業員と請負業者がTSPの業務の信頼性をサポートすることを保証するものとする。[SHALL] 注1:ガイダンスとしてISO/IEC 27002: 2022 [i.3]の条項6.1.1および7を参照のこと。					
300	• REQ-7.2-02	○	TSPは、必要な専門知識、信頼性、経験、資格を有し、提供されるサービスと仕事の機能に適切なセキュリティと個人データ保護規則に関するトレーニングを受けたスタッフを雇用し、場合によっては下請け業者を使用するものとする。[SHALL]					
301	• REQ-7.2-03	○	TSPの担当者は、正式なトレーニングと資格、実際の経験、またはその2つの組み合わせを通じて、「専門知識、経験、資格」の要件を満たすべきである。[SHOULD]					
302	• REQ-7.2-04	○	これには、新しい脅威と現在のセキュリティ慣行に関する定期的(少なくとも12か月ごと)の更新が含まれるべきである。[SHOULD] 注2:TSPによって雇用される要員には、TSPのサービスをサポートする機能の実行に契約上従事する個々の要員が含まれる。TSPのサービスの監視に関与できる担当者は、TSPの要員である必要はない。					
303	• REQ-7.2-05	○	TSPのポリシーまたは手順に違反した職員には、適切な懲戒処分が適用されるものとする。[SHALL] 注3:ガイダンスについては、ISO/IEC 27002:2022 [i.3]の条項7.2.3を参照のこと。					
304	• REQ-7.2-06	○	TSPの情報セキュリティポリシーで指定されているセキュリティの役割と責任は、職務記述書または関係者全員が利用できる文書に文書化されているものとする。[SHALL]					
305	• REQ-7.2-07	○	TSPの運営のセキュリティが依存する信頼された役割は、明確に識別されているものとする。[SHALL]					
306	• REQ-7.2-08	対象外	廃止					
307	• REQ-7.2-09	対象外	廃止					
308		○	注4:役割と責任を確立する際の管理責任に関する詳細なガイダンスについては、ISO/IEC 27002:2022 [i.3]の条項7.2.1を参照のこと。					
309	• REQ-7.2-10	○	TSPの職員(臨時および常駐)は、職務とアクセスレベル、経歴審査、従業員のトレーニングと意識に基づいてポジションの機密性を決定する、職務の分離と最小限の権限(7.1.2項を参照)で果たされる役割の観点から定義された職務記述書を持つものとする。[SHALL]					
310	• REQ-7.2-11	○	必要に応じて、職務記述書は一般的な職務とTSPの特定の職務を区別するものとする。これらには、スキルと経験の要件を含める必要がある。注5:役割と責任を確立する際の管理責任に関する詳細なガイダンスについては、ISO/IEC 27002:2022 [i.3]の条項7.2.1を参照のこと。[SHALL]					
311	• REQ-7.2-12	○	担当者は、TSPの情報セキュリティ管理手順に沿った管理および管理手順およびプロセスを実行するものとする。[SHALL] 注6:役割と責任を確立する際の管理責任に関する詳細なガイダンスについては、ISO/IEC 27002:2022 [i.3]の条項7.2.1を参照のこと。					
312	• REQ-7.2-13	○	管理者は、提供されるトラストサービスに関する経験またはトレーニング、セキュリティ責任を負う担当者のセキュリティ手順に精通し、管理機能を実行するのに十分な情報セキュリティとリスクアセスメントの経験を有しているものとする。[SHALL]					
313	• REQ-7.2-14	○	信頼される役割にあるすべてのTSP職員は、TSPの運営の公平性を損なう可能性のある利益相反を起こさないものとする。[SHALL] 注7:ガイダンスについては、ISO/IEC 27002:2022 [i.3]の条項6.1.2を参照のこと。					
314	• REQ-7.2-15	○	信頼された役割には、次の責任を伴う役割が含まれるものとする。[SHALL] a)セキュリティ責任者:セキュリティ慣行の実装を管理する全体的な責任。 b)システム管理者:サービス管理のためにTSPの信頼できるシステムをインストール、構成、保守する権限を与えられる。 注8:これにはシステムのリカバリが含まれる。 c)システムオペレータ:TSPの信頼できるシステムを日常的に運用する責任を負う。システムバックアップを実行する権限を与えられている。 d)システム監査人:TSPの信頼できるシステムのアーカイブと監査ログを表示する権限を与えられる。 注9:特定の信頼サービスには、追加のアプリケーション固有の役割が必要になる場合がある。					
315	• REQ-7.2-16	対象外	廃止					
316	• REQ-7.2-16A	○	TSPの職員は、セキュリティを担当する上級管理者によって信頼される役割に正式に任命されるものとする。[SHALL]					
317	• REQ-7.2-16B	○	信頼された役割は、その役割を果たすために任命された人によって受け入れられるものとする。[SHALL]					
318	• REQ-7.2-17	○	職員は、必要なチェックが完了するまで、信頼できる機能にアクセスしないものとする。[SHALL] 注10:一部の国では、TSPが従業員候補者の同意なしに過去の有罪判決に関する情報を入手することは不可能です。					
-	7.3 Asset management		7.3 資産管理					
-	7.3.1 General requirements		7.3.1 一般要件					

監査報告書リスト番号	要求識別子	監査対象	要求事項	措置状況	確認したエビデンス	監査エビデンス(具体的な確認事項／方法)	トラストサービスプロバイダー監査者評価およびコメント	専門家会議評価およびコメント
319	REQ-7.3.1-01	○	TSPは、情報資産を含む資産の適切なレベルの保護を確保するものとする。注1:ガイダンスについては、ISO/IEC 27002:2022 [i.3]の第8章を参照のこと。[SHALL]					
320	• REQ-7.3.1-02	○	TSPは、すべての情報資産の目録を維持し、リスクアセスメントと一致する分類を割り当てるものとする。[SHALL] 注2:ガイダンスについては、ISO/IEC 27002:2022 [i.3]の条項8.1.1を参照のこと。					
-	7.3.2 Media handling		7.3.2 メディアの取り扱い					
321	REQ-7.3.2-01	○	すべてのメディアは、情報分類スキームの要件に従って安全に取り扱われなければならない。機密データを含むメディアは、不要になった場合は安全に廃棄するものとする。[SHALL]					
322	REQ-7.3.2-02	○	TSPのシステム内で使用されるメディアは、メディアを損傷、盗難、不正アクセス、陳腐化から保護するために安全に取り扱うものとする。[SHALL]					
323	REQ-7.3.2-03	○	メディア管理手順は、記録を保持する必要がある期間内のメディアの陳腐化および劣化を防止するものとする。[SHALL] 注:ガイダンスについては、ISO/IEC 27002:2022 [i.3]の条項8.3を参照のこと。					
-	7.4 Access control		7.4 アクセス制御					
324	REQ-7.4-01	○	TSPのシステムへのアクセスは、許可された個人に限定するものとする。[SHALL]					
325	• REQ-7.4-02	対象外	廃止					
326	• REQ-7.4-03	対象外	廃止					
327	• REQ-7.4-04	対象外	廃止					
328	• REQ-7.4-04A	○	TSPは、アクセス権限を設定する際に「最小限の権限」の原則を適用して、オペレータ、管理者、およびシステム監査人のユーザーアクセスを管理するものとする。注1:これは通常、REQ-7.2-16に従って信頼された役割に任命された担当者に適用される。[SHALL]					
329	• REQ-7.4-05	○	管理には、ユーザーアカウントの管理とアクセスの適時の変更または削除が含まれるものとする。[SHALL]					
330	• REQ-7.4-06	○	情報およびアプリケーションシステム機能へのアクセスは、アクセス制御ポリシーに従って制限されるものとする。[SHALL]					
331	• REQ-7.4-07	○	TSPのシステムは、セキュリティ管理機能と運用機能の分離を含め、TSPの業務で特定された信頼できる役割を分離するための十分なコンピュータセキュリティ制御を提供しなければならない。特に、システムユーティリティプログラムの使用を制限、管理するものとする。[SHALL]					
332	• REQ-7.4-08	○	TSPの要員は、サービスに関連する重要なアプリケーションを使用する前に識別および認証されるものとする。[SHALL]					
333	• REQ-7.4-09	○	TSPの職員は、自らの活動に対して責任を負うものとする。・例:イベントログを保持する。[SHALL]					
334	• REQ-7.4-10	○	機密データは、権限のないユーザーがアクセスできる再利用されたストレージオブジェクト(削除されたファイルなど)またはメディア(第7.3.2項を参照)を通じて漏洩しないように保護されるものとする。[SHALL] 注2:ガイダンスについては、ISO/IEC 27002:2022 [i.3]の第9章を参照のこと。 注3:認証に関するさらなる推奨事項は、CA/Browser Forum ネットワークセキュリティガイド[i.7]、第2章に記載されている。					
-	7.5 Cryptographic controls		7.5 暗号コントロール					
335	REQ-7.5-01	○	ライフサイクル全体を通じて、あらゆる暗号キーおよびあらゆる暗号デバイスを管理するために、適切なセキュリティ管理を実施するものとする。[SHALL] 注:ガイダンスについては、ISO/IEC 27002:2022 [i.3]の第10章を参照のこと。					
-	7.6 Physical and environmental security		7.6 物理的および環境的セキュリティ					
336	REQ-7.6-01	○	TSPは、セキュリティが信頼サービスの提供にとって重要であるTSPシステムのコンポーネントへの物理的アクセスを制御し、物理的セキュリティに関連するリスクを最小限に抑えるものとする。[SHALL] 注1:ガイダンスについては、ISO/IEC 27002:2022 [i.3]の第11章を参照のこと。					
337	• REQ-7.6-02	○	セキュリティが信頼サービスの提供にとって重要であるTSPシステムのコンポーネントへの物理的アクセスは、許可された個人に限定されるものとする。[SHALL] 注2:重要度は、リスクアセスメントを通じて、またはアプリケーションのセキュリティ要件を通じて、セキュリティ保護が必要であると特定される。					
338	• REQ-7.6-03	○	資産の損失、損傷、侵害、および事業活動の中断を回避するために管理を実施するものとする。[SHALL]					
339	• REQ-7.6-04	○	情報および情報処理施設の侵害または盗難を回避するための制御を実装するものとする。[SHALL]					
340	• REQ-7.6-05	○	トラストサービスの安全な運用に重要なコンポーネントは、侵入に対する物理的保護、セキュリティ境界を介したアクセスの制御、および侵入を検出するアラームを備えた保護されたセキュリティ境界に配置されるものとする。[SHALL] 注3:安全な領域に関するガイダンスについては、ISO/IEC 27002:2022 [i.3]、11.1項を参照のこと。					
-	7.7 Operation security		7.7 運用上のセキュリティ					
341	REQ-7.7-01	○	TSPは、改変から保護された信頼できるシステムと製品を使用し、それらによってサポートされるプロセスの技術的安全性と信頼性を確保するものとする。[SHALL] 注1:ガイダンスについては、ISO/IEC 27002:2022 [i.3]の第12章を参照のこと。 注2:システムの取得、開発、および保守に関するガイダンスについては、ISO/IEC 27002:2022 [i.3]の第14章を参照のこと。 注3:サプライヤーとの関係に関するガイダンスについては、ISO/IEC 27002:2022 [i.3]の第15章を参照のこと。					

監査報告書リスト番号	要求識別子	監査対象	要求事項	措置状況	確認したエビデンス	監査エビデンス(具体的な確認事項／方法)	トラストサービスプロバイダー監査者評価およびコメント	専門家会議評価およびコメント
342	• REQ-7.7-02	○	セキュリティ要件の分析は、ITシステムにセキュリティが組み込まれていることを確認するために、TSPまたはTSPの代理で実施されるシステム開発プロジェクトの設計および要件仕様の段階で実行されるものとする。[SHALL]					
343	• REQ-7.7-03	○	変更管理手順は、運用ソフトウェアのリリース、修正、緊急ソフトウェア修正、およびTSPのセキュリティポリシーを適用する構成の変更に適用されるものとする。[SHALL]					
344	• REQ-7.7-04	○	手順には変更の文書が含まれるものとする。[SHALL] ?注4:ガイダンスについては、ISO/IEC 27002:2022 [i.3]の第14章を参照のこと。					
345	• REQ-7.7-05	○	TSPのシステムと情報の完全性は、ウイルス、悪意のあるソフトウェア、および無許可のソフトウェアから保護されるものとする。[SHALL]					
346	• REQ-7.7-06	対象外	廃止					
347	• REQ-7.7-07	対象外	廃止					
348	• REQ-7.7-08	○	サービスの提供に影響を与えるすべての信頼できる管理役割に対して手順を確立し、実施するものとする。[SHALL]					
349	• REQ-7.7-09	○	TSPは、以下を確実にするための手順を指定し、適用するものとする。[SHALL] a)セキュリティパッチは、入手可能になってから適切な期間内に適用される。 b)セキュリティパッチを適用するメリットを上回る追加の脆弱性または不安定性が導入される場合、セキュリティパッチは適用されない。 c)セキュリティパッチを適用しない理由が文書化されている。 注5:さらに具体的な推奨事項は、CA/ブラウザフォーラムのネットワークセキュリティガイド[i.7]、項目1lに記載されている。					
-	7.8 Network security		7.8 ネットワークセキュリティ					
350	REQ-7.8-01	○	TSPは、そのネットワークとシステムを攻撃から保護するものとする。[SHALL]					
351	• REQ-7.8-02	○	TSPは、信頼できるシステムとサービス間の機能的、論理的、物理的(場所を含む)関係を考慮したリスクアセスメントに基づいて、システムをネットワークまたはゾーンに分割するものとする。[SHALL]					
352	• REQ-7.8-03	○	TSPは、同じゾーン内に同じ場所にあるすべてのシステムに同じセキュリティ制御を適用するものとする。[SHALL]					
353	• REQ-7.8-04	○	TSPは、ゾーン間のアクセスおよび通信を、TSPの運営に必要なものに制限するものとする。[SHALL]					
354	• REQ-7.8-05	○	TSPは、不要な接続およびサービスを明示的に禁止または非アクティブ化するものとする。[SHALL]					
355	• REQ-7.8-06	○	TSPは、確立されたルールセットを定期的にレビューするものとする。[SHALL]					
356	• REQ-7.8-07	○	TSPは、TSPの運営にとって重要なすべてのシステムを1つ以上のセキュアゾーンに保持するものとする。[SHALL]					
357	• REQ-7.8-08	○	TSPは、ITシステム管理用の専用ネットワークとTSPの運用ネットワークを分離するものとする。[SHALL]					
358	• REQ-7.8-09	○	TSPは、セキュリティポリシー実装の管理に使用されるシステムを他の目的で使用しないものとする。[SHALL]					
359	• REQ-7.8-10	○	TSPは、TSPのサービスのための実稼働システムを、開発およびテストで使用されるシステム(例:開発、テスト、ステージングシステム)から分離するものとする。[SHALL]					
360	• REQ-7.8-11	対象外	廃止					
361	• REQ-7.8-11A	○	TSPは、他の通信チャネルから論理的、暗号的、または物理的に分離され、エンドポイントの確実な識別とチャネルデータの変更または開示からの保護を提供する信頼できるチャネルを通じてのみ、別個の信頼できるシステム間の通信を確立するものとする。[SHALL]					
362	• REQ-7.8-12	○	トラストサービスへの外部アクセスの高レベルの可用性が必要な場合、単一障害の場合でもサービスの可用性を確保するために、外部ネットワーク接続を冗長化するものとする。[SHALL]					
363	• REQ-7.8-13	○	TSPは、TSPによって識別されたパブリックおよびプライベートIPアドレスに対して定期的な脆弱性スキャンを受けるか実行し、各脆弱性スキャンがスキル、ツール、熟練度、コードおよび信頼できるレポートを提供するために必要な倫理と独立性を備えた個人または団体によって実行されたという証拠を記録するものとする。[SHALL]					
364	• REQ-7.8-13A	○	REQ-7.8-13によって要求された脆弱性スキャンは四半期に1回実行されるべきである。[SHOULD]					
365	• REQ-7.8-14	○	TSPは、セットアップ時、およびTSPが重要であると判断したインフラストラクチャまたはアプリケーションのアップグレードまたは変更後に、TSPのシステムに対して侵入テストを受けるものとする。[SHALL]					
366	• REQ-7.8-14A	○	REQ-7.8-14で要求される侵入テストは、少なくとも年に1回実行するべきである。[SHOULD]					
367	• REQ-7.8-15	○	TSPは、信頼できるレポートを提供するために必要なスキル、ツール、習熟度、倫理規定、および独立性を備えた個人または団体によって各侵入テストが実行されたという証拠を記録するものとする。[SHALL]					
368	• REQ-7.8-16	○	制御(ファイアウォールなど)は、TSPの内部ネットワークドメインを利用者や第三者によるアクセスを含む不正アクセスから保護するものとする。[SHALL]					
369	• REQ-7.8-17	○	TSPの運営に必要のないすべてのプロトコルとアクセスを防止するようにファイアウォールを構成するべきである。[SHOULD]					
-	7.9 Incident management		7.9 インシデント管理					
370	REQ-7.9-01	○	ITシステムへのアクセス、ITシステムの使用、およびサービス要求に関するシステムアクティビティは監視されるものとする。[SHALL] 注1:ガイダンスについては、ISO/IEC 27002:2022 [i.3]の第16章を参照のこと。					
371	• REQ-7.9-02	○	モニタリング活動では、収集または分析される情報の機密性を考慮するべきである。[SHOULD]					
372	• REQ-7.9-03	○	TSPのネットワークへの侵入を含む、潜在的なセキュリティ違反を示す異常なシステム活動は、検出され、アラームとして報告されるものとする。[SHALL] 注2:異常なネットワークシステムアクティビティには、(外部)ネットワークスキャンやパケットドロップが含まれる場合がある。					

監査報告書リスト番号	要求識別子	監査対象	要求事項	措置状況	確認したエビデンス	監査エビデンス(具体的な確認事項／方法)	トラストサービスプロバイダー監査者評価およびコメント	専門家会議評価およびコメント
373	• REQ-7.9-04	○	TSPは次のイベントを監視するものとする。[SHALL] a)ロギング機能の起動と停止。 b)TSPのネットワークで必要なサービスの可用性と利用。					
374	• REQ-7.9-05	○	TSPは、インシデントに迅速に対応し、セキュリティ侵害の影響を制限するために、タイムリーかつ調整された方法で行動するものとする。[SHALL]					
375	• REQ-7.9-06	○	TSPは、潜在的に重大なセキュリティイベントのアラートをフォローアップし、関連するインシデントがTSPの手順に従って確実に報告されるように、信頼できる担当者を任命するものとする。[SHALL]					
376	• REQ-7.9-07	○	TSPは、侵害が特定されてから24時間以内に提供されるトラストサービスおよびそこで維持される個人データに重大な影響を与えるセキュリティ違反または完全性の喪失について、該当する規制規則に従って適切な関係者に通知する手順を確立するものとする。[SHALL] 注3:適切な監督機関および/またはその他の管轄当局に連絡することができる。					
377	• REQ-7.9-08	○	セキュリティの侵害または完全性の喪失が、信頼できるサービスが提供されている自然人または法人に悪影響を与える可能性がある場合、TSPはまた、その自然人または法人に過度な遅延なくセキュリティの侵害または完全性を失うことを通知するものとする。[SHALL]					
378	• REQ-7.9-09	○	TSPのシステムは、監査ログを処理し、起こり得る重大なセキュリティイベントについて担当者に警告するための自動メカニズムを実装して、悪意のある活動の証拠を特定するために、監査ログの監視または定期的なレビューを含めて監視されるものとする。[SHALL]					
379	• REQ-7.9-10	○	TSPは、TSPによって対処されていない重大な脆弱性を発見後48時間以内に対処するものとする。[SHALL]					
380	• REQ-7.9-11	○	あらゆる脆弱性について、潜在的な影響を考慮して、TSPは以下を少なくとも一つ選択するものとする。[SHALL] -脆弱性を軽減する計画を作成して実装する。 -脆弱性は修復する必要がないとTSPが判断した事実に基づく根拠を文書化する。 例:TSPは、潜在的な影響のコストが軽減のコストを正当化できない場合、脆弱性を修復する必要がないと判断できる。 注4:さらなる推奨事項は、CA/ブラウザフォーラムのネットワークセキュリティガイド[i.7]項目4 f)に記載されている。					
381	• REQ-7.9-12	○	インシデントの報告と対応手順は、セキュリティインシデントや機能不全による損害が最小限に抑えられるような方法で採用されるものとする。[SHALL]					
-	7.10 Collection of evidence		7.10 証拠の収集					
382	REQ-7.10-01	○	TSPは、特に法的手続きにおける証拠、およびサービスの継続性を確保する目的で提供する目的で、TSPが発行および受信したデータに関するすべての関連情報を、TSPの活動停止後を含む適切な期間記録し、アクセス可能な状態に保つものとする。[SHALL] NOTE:See requirement REQ-7.13-05. 注:要件REQ-7.13-05を参照のこと。					
383	• REQ-7.10-02	○	サービスの運用に関する現在およびアーカイブされた記録の機密性と完全性は維持されるものとする。[SHALL]					
384	• REQ-7.10-03	○	サービスの運用に関する記録は、開示された商習慣に従って完全かつ機密にアーカイブされるものとする。[SHALL]					
385	• REQ-7.10-04	○	サービスの運用に関する記録は、法的手続きの目的でサービスの正しい運用の証拠を提供する目的で必要な場合に利用可能にされるものとする。[SHALL]					
386	• REQ-7.10-05	○	重要なTSPの環境イベント、鍵管理イベント、およびクロック同期イベントの正確な時刻が記録されるものとする。[SHALL]					
387	• REQ-7.10-06	○	監査ログに必要なイベントの記録に使用される時刻は、少なくとも1日に1回UTCと同期されるものとする。[SHALL]					
388	• REQ-7.10-07	○	サービスに関する記録は、必要な法的証拠を提供するために適切な期間、TSPの利用規約で通知されているとおりに保持されるものとする(第6.3項を参照)。[SHALL]					
389	• REQ-7.10-08	○	イベントは、保持が必要な期間内に簡単に削除または破棄できない方法で記録されるものとする(長期メディアに確実に転送される場合を除く)。[SHALL] 例:これは、たとえば、書き込み専用メディアの使用、使用された各リムーバブルメディアの記録、およびオフサイトバックアップの使用を通じて、または複数(たとえば2つまたは3つ)の独立した場所で情報を並行して保存することによって実現できる。					
-	7.11 Business continuity management		7.11 事業継続管理					
390	REQ-7.11-01	○	TSPは、災害時に実施する継続計画を定義および維持するものとする。[SHALL]					
391	REQ-7.11-02	○	秘密鍵の漏洩やTSPのその他のクレデンシャルの漏洩などの災害が発生した場合、災害の原因に対処した上で、再発する可能性（セキュリティ上の脆弱性など）に対して適切な修復手段を講じ、継続計画で定められた遅延時間内に運用を復元するものとする。[SHALL] 注1:災害時のガイダンスについては、ISO/IEC 27002:2022 [i.3]の第17章を参照のこと。 注2:その他の災害状況には、ハードウェアやソフトウェアを含む、TSPの信頼できるシステムの重要なコンポーネントの障害が含まれる。					
-	7.12 TSP termination and termination plans		7.12 TSP の終了と終了計画					
392	REQ-7.12-01	○	TSPサービスの停止の影響である利用者および依拠当事者に対する潜在的な混乱を最小限に抑え、特にトラストサービスの正確性を検証するために必要な情報の継続的な保守が提供されるものとする。[SHALL]					
393	• REQ-7.12-02	○	TSPは最新の終了計画を持っているものとする。[SHALL] TSPがサービスを終了する前に、少なくとも次の手順が適用される。					
394	- REQ-7.12-03	○	TSPがサービスを終了する前に、TSPは以下に終了を通知するものとする:すべての利用者およびTSPと契約またはその他の形式の確立された関係を結んでいる他のエンティティ(依拠当事者、TSPおよび監督機関などの関連当局)[SHALL]					
395	- REQ-7.12-04	○	TSPがサービスを終了する前に、TSPは他の依拠当事者が終了の情報を利用できるようにするものとする。[SHALL]					

監査報告書リスト番号	要求識別子	監査対象	要求事項	措置状況	確認したエビデンス	監査エビデンス(具体的な確認事項／方法)	トラストサービスプロバイダー監査者評価およびコメント	専門家会議評価およびコメント
396	- REQ-7.12-05	○	TSPがサービスを終了する前に、TSPは、トラストサービストークンの発行プロセスに関連する機能をTSPに代わって実行するすべての下請け業者の権限を終了するものとする。[SHALL]					
397	- REQ-7.12-06	○	そのような情報を保持していないことを示さない限り、TSPがサービスを終了する前に、TSPは、TSPの運用の証拠を提供するために必要なすべての情報を合理的な期間維持する義務を信頼できる当事者に移転するものとする。[SHALL]					
398	- REQ-7.12-07	○	TSPがそのサービスを終了する前に、バックップコピーを含むTSPの秘密鍵は、秘密鍵を取得できないようにするために、使用できないように破棄されるか回収されるものとする。[SHALL]					
399	- REQ-7.12-08	○	TSPがサービスを終了する前に、可能な場合、TSPは既存の顧客に対するトラストサービスの提供を別のTSPに移管する手配を行うべきである。[SHOULD]					
400	• REQ-7.12-09	○	TSPは、TSPが破産した場合、またはその他の理由により自力でコストを賄えない場合に備えて、破産に関する法律の適用される制約の範囲内で可能な限り、これらの最低要件を満たすためのコストをカバーする取り決めを持つものとする。[SHALL]					
401	• REQ-7.12-10	○	TSPは、サービスの終了について定められた規定をその実務の中に明記するものとする。これには以下が含まれる。[SHALL] a)影響を受けるエンティティへの通知。 b)該当する場合、TSPの義務を他の当事者に移転する。					
402	• REQ-7.12-11	○	TSPは、公開鍵またはトラストサービストークンを妥当な期間、信頼できる当事者に利用可能にする義務を維持するか、信頼できる当事者に譲渡するものとする。[SHALL]					
-	7.13 Compliance		7.13 コンプライアンス					
403	REQ-7.13-01	○	TSPは、合法かつ信頼できる方法で運営することを保証するものとする。[SHALL]					
404	• REQ-7.13-02	○	TSPは、適用される法的要件をどのように満たしているかに関する証拠を提供するものとする。[SHALL]					
405	• REQ-7.13-03	○	提供されるトラストサービスおよびそれらのサービスの提供に使用されるエンドユーザー製品は、可能な場合には障害のある人もアクセスできるようにするものとする。[SHALL]					
406	• REQ-7.13-04	○	アクセシビリティに関する規格を考慮するべきである。[SHOULD]					
407	• REQ-7.13-05	○	個人データの無許可または違法な処理、および個人データの偶発的な紛失または破壊、損傷に対して、適切な技術的および組織的措置を講じるものとする。[SHALL] 注2:プライバシー情報管理のための27002の拡張に関する要件とガイダンスについては、ISO/IEC 27701:2019 [i.14]を参照のこと。					

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報告書（鍵管理（署名値生成）サービス）別表A

A.1　登録

A.1.1　申請と登録

保証レベル	必要な要素
「低」	1. 電子識別手段の使用に関する条件を申請者が認識していることを確実にする。 2. 電子識別手段に関連する推奨されるセキュリティ上の注意事項を申請者が認識していることを確実にする。 3. 身元確認と検証に必要な関連する同一性識別情報を収集する。
「十分」	レベル「低」と同じ。
「高」	レベル「低」と同じ。

A.1.2　身元確認と検証（自然人）

保証レベル	必要な要素
「低」	1. 申請者は、主張された身元を示している証拠をその人物が所持していると仮定することができる。 2. 証拠が真正である、または信頼できる情報源によって存在すると仮定でき、その証拠は有効であるとみなせる。 3. 主張された身元が存在することが信頼できる情報源によって知られており、その身元を主張する人 が同一人物であると仮定することができる。
「十分」	レベル「低」に加えて、1～4のいずれかの選択肢を満たす必要がある 1. 申請者は、主張された身元を示している証拠をその人物が所持していると検証されている かつ その証拠が真正であることを確認している、または信頼できる情報源によって、その証拠が存在し、実在の人物に関連するものであると知られている かつ 例えば、紛失、盗難、停止、失効または期限切れの証拠のリスクを考慮し、申請人の身元が主張された身元ではないリスクを最小限に抑えるための措置が取られている または 2. 身元証明書が登録手続き中に提示され、その書類が提示した人物に関連するとみなせる かつ 例えば、紛失、盗難、停止、失効または期限切れの証拠のリスクを考慮し、申請人の身元が主張された身元でないリスクを最小限に抑えるための措置が取られていること または 3. 電子識別手段の発行以外の目的で，公的又は私的機関が以前に使用した手順が，保証レベル「十分」について A.1.2 項に規定するものと同等の保証を提供する場合，その同等の保証が，該当する規制要件に準拠した適合評価機関又は同等の機関によって確認されていれば，登録に責任を負う機関は，以前の手順を繰り返す必要がない または 4. 電子識別手段が、保証レベル「十分」または「高」を有する有効な通知済み電子識別手段に基づいて発行され、個人識別データの改変のリスクを考慮する場合、身元確認および検証プロセスを繰り返す必要はない。根拠となる電子識別手段が通知されていない場合、保証レベル「十分」または「高」は、 適用される規制要件（注1参照）に準拠する適合性評価機関または同等の機関によって確認されなけ ればならない。

「高」	1または2のいずれかの要件を満たす必要がある 1.レベル「十分」、かつ、(a)～(c)に掲げる選択肢のうち1つを満たさなければならない (a) 申請者は、主張された身元を示している写真または生体識別証拠を所持していることが確認されている場合、その証拠が信頼できる情報源によって有効であると確認されている かつ 申請者が、1つまたは複数の身体的特徴を信頼できる情報源と比較することにより、主張された本人であると確認される または (b) 電子識別手段の発行以外の目的で，公的又は私的団体が以前に使用した手順が，保証レベル「高」について A.1.2 項に規定するものと同等の保証を提供する場合，その同等の保証が，該当する規制要件に準拠する適合性評価機関（注2参照）又は同等の機関によって確認されていれば，登録に責任を負う機関は，以前の手順を繰り返す必要がない かつ 以前の手順の結果が有効であることを証明するための措置を講じている または (c) 電子識別手段が、保証レベル「高」を有する有効な通知済み電子識別手段に基づいて発行され、 個人識別データの改変のリスクを考慮する場合、身元確認および検証プロセスを繰り返す必要はない。根拠となる電子識別手段が通知されていない場合、適用される規制要件に準拠した適合性評価機関または同等の機関によって、保証レベル「高」が確認されなければならない かつ 通知された電子識別手段の前の発行手続きの結果が有効であることを証明するための措置がとられている または 2.申請者が認められた写真または生体識別証拠を提示しない場合、そのように認められた写真または生体識別証拠を取得するために、国レベルで使用されるものと全く同じ手順が適用される。

A.1.3 身元確認と検証（法人）

保証レベル	必要な要素
「低」	1. 法人の主張する身元は、証拠に基づいて証明される。 2. 証拠が有効であるとみなせ、かつ真正である、または信頼できる情報源に従って存在すると仮定できる。ただし、信頼できる情報源に法人が含まれることは任意であり、法人と信頼できる情報源の間の協定によって規制される。 3. その法人が、その法人として行動することを妨げるような状態にあることを、信頼できる情報源から知らされていないこと。
「十分」	レベル「低」に加えて、1～3のいずれかの選択肢を満たす必要がある 1.電子識別手段の申請が行われた証拠に基づいて、主張された法人のアイデンティティが証明されている。ここには法人の名前、法人形態、登録番号(該当する場合)を含む。 かつ その証拠が真正であることを確認している、あるいは信頼できる情報源に従って既知かどうかが確認されていて、法人がその分野で活動するために信頼できる情報源に法人が含まれることが求められる かつ 例えば、紛失、盗難、停止、失効または期限切れの証憑書類のリスクを考慮し、法人のアイデンティティが主張するアイデンティティと異なるリスクを最小限に抑えるための措置が取られていること

「十分」	または 2.電子識別手段の発行以外の目的で，公的又は私的機関が以前に使用した手順が，保証レベル「十分」について A.1.3 項に規定するものと同等の保証を提供する場合，その同等の保証が，該当する規制要件に準拠する適合評価機関（注1参照）又は同等の機関によって確認されていれば，登録に責任を負う機関は，以前の手順を繰り返す必要がない または 3.電子識別手段が、保証レベル「十分」または「高」を有する有効な通知済み電子識別手段に基づいて発行される場合、電子識別証明および検証プロセスを繰り返す必要はない。根拠となる電子識別手段が通知されていない場合、適用される規制要件に準拠した適合性評価機関 （注1参照）または同等の機関によって、保証レベル「十分」または「高」を確認する必要である。
「高」	レベル「十分」に加えて、1～3のいずれかの選択肢を満たす必要がある 1.主張される法人のアイデンティティは証拠に基づいて証明される。ここには、法人の名前、法人形態、および国内で使用される法人を表す少なくとも 1 つの固有識別子が含まれる。 かつ その証拠が信頼できる情報源に基づき有効であることを確認する または 2.電子識別手段の発行以外の目的で，公的又は私的機関が以前に使用した手順が，保証レベル「高」について A.1.3 節に規定するものと同等の保証を提供する場合，その同等の保証が， 該当する規制要件に準拠する適合性評価機関（注2参照）又は同等の機関によって確認されていれば，登録に責任を負う機関は，以前の手順を繰り返す必要がない かつ この前の手順の結果が有効であることを証明するための措置がとられている または 3.電子識別手段が、保証レベル「高」を有する有効な通知済み電子識別手段に基づいて発行される場合、身元確認および検証プロセスを繰り返す必要はない。根拠となる電子識別手段が通知されていない場合、適用される規制要件に準拠した適合性評価機関 （注2参照）または同等の機関によって、保証レベル「高」が確認されなければならない。 かつ 通知された電子識別手段の前の発行手続きの結果が有効であることを証明するための措置がとられている。

A.1.4 自然人と法人の電子識別手段の紐づけ(バインディング)

保証レベル	必要な要素
「低」	1.法人を代表して行動する自然人の身元確認が、レベル「低」以上で行われたことが確認される。 2.バインディングは、国に認められた手順に基づいて確立されている。 3.自然人が、その人が法人を代表して行動することを妨げるような状態にあることを、信頼できる情報源から知らされていないこと。
「十分」	レベル「低」の3に加え、 1.法人を代表して行動する自然人の身元確認が、レベル「十分」または「高」で行われたことが検証される。 2.バインディングは、国に認められた手続きに基づいて確立され、その結果、信頼できる情報源に登録されたものである。 3.バインディングは、信頼できる情報源からの情報に基づいて確認されている。

「高」	レベル「低」の3、レベル「十分」の2に加え、 1.法人を代表して行動する自然人の身元確認が、レベル「高」で行われたことが検証される。 2.バインディングは、国内で使用される法人を表す固有の識別子、及び信頼できる情報源からの自然人を表す固有の情報に基づいて検証されている。

A.2 電子識別手段と認証

A.2.1 電子識別手段の特性と設計

保証レベル	必要な要素
「低」	1.電子識別手段は、少なくとも1つの認証要素を利用する。 2.電子識別手段が、その電子識別手段を携帯する者の制御下または所有下にある場合のみ使用されることを確認するための合理的な措置を、発行者が講じるように設計されていること。
「十分」	1.電子識別手段は、異なる種類から少なくとも2つの認証要素を利用する。 2.電子識別手段は、その電子識別手段を携帯する者の制御下または所有下にある場合にのみ使用されることが想定できるように設計されていること。
「高」	レベル「十分」に加えて、 1.電子識別手段は、複製や改ざん、さらには攻撃可能性が高い攻撃者から保護する。 2.電子識別手段は、他人の使用に対して、その電子識別手段を携帯する者が確実に保護することができるように設計されている。

A.2.2 認証メカニズム

保証レベル	必要な要素
「低」	1.個人識別データの開示は、電子識別手段とその有効性を確実に確認した上で行う。 2.認証メカニズムの一部として個人識別データが保存される場合、その情報は、紛失や、オフラインでの分析を含む侵害を防ぐために保護されている。 3.認証メカニズムは、基本的な攻撃能力を強化した攻撃者による推測、盗聴、再生、通信操作などの行為が認証メカニズムを破壊する可能性が極めて低いように、電子識別手段の検証のためのセキュリティ制御を実装している。
「十分」	レベル「低」に加え、 1.個人識別データの開示は、動的認証による電子識別手段とその有効性を確実に確認した上で行う。 2.認証メカニズムは、中程度の攻撃力を持つ攻撃者による推測、盗聴、再生、通信操作などの行為が認証メカニズムを破壊する可能性が極めて低くなるように、電子識別手段の検証のためのセキュリティ制御を実装している。
「高」	レベル「十分」に加え、 認証メカニズムは、攻撃力の高い攻撃者による推測、盗聴、再生、通信操作などの行為が認証メカニズムを破壊する可能性が極めて低くなるように、電子識別手段の検証のためのセキュリティ制御を実装している。