資料3-2

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　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)(案)
1.0版

令和5年8月
厚生労働省

(C)　Ministry of Health, Labour and Welfare

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。
・デジタル署名生成サービスの一般ポリシー要求事項
・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（デジタル署名生成サービス）

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
「デジタル署名生成サービスの一般ポリシー要求事項」								
-	5 Risk assessment		5 リスクアセスメント					
1	OVR-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5項に規定されている要件が適用されるものとする(SHALL)。					監査報告書リスト番号78項～82項参照
-	6 Policies and practices		6.ポリシーと運用規程					
-	6.1 Trust service practice statement		6.1 トラストサービス運用規程					
2	OVR-6.1-01	○	「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節に規定されている要件が適用されるものとする(SHALL)。さらに、以下の特定の要件が適用される。					監査報告書リスト番号83項～96項参照
3	OVR-6.1-02 [CONDITIONAL]	○	SCASCがデジタル署名にタイムスタンプトークンを含めることをサポートしている場合、SCASC運用規程はどのTSAが使用されているかを列挙するものとする(SHALL)。					
4	OVR-6.1-03	○	SCASC運用規程は、サポートされているすべての署名生成ポリシーを指定するものとする(SHALL)。					
5	OVR-6.1-04	○	SCASC運用規程は、サポートされているすべての署名フォーマットを指定するものとする(SHALL)。					
6	OVR-6.1-05	○	SCASC運用規程は、サポートされているすべての署名クラス(B、T、LT、LTA)を指定するものとする(SHALL)。					
7	OVR-6.1-06	○	SCASPは、適用可能なポリシーと実務を含む、そのサービスを支援するすべての外部組織の義務をSCASC運用規程の中で識別するものとする(SHALL)。					
-	6.2 Terms and Conditions		6.2利用規約					
8	OVR-6.2-01	○	「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6.2節に規定されている要件を適用するものとする(SHALL)。加え、以下の特定の要件が適用される。					監査報告書リスト番号97項～102項参照
9	OVR-6.2-02	○	適用されているトラストサービスポリシーを特定するために、SCASC利用規約は、それが適合するサポートされているSCASCポリシーを列挙または参照し（例えばOIDを通して）、そして簡潔に説明するものとする(SHALL)。					
10	OVR-6.2-06	○	利用規約はSCASPと署名者の権利と義務を示すものとする(SHALL)。					
11	OVR-6.2-07	○	利用規約は、サービスによってサポートされているオプションを記述するものとする(SHALL)。少なくとも以下を記述するものとする(SHALL)：					
12	a)	○	a） サポートされている署名フォーマット 例： CAdES、XAdES、またはPAdES。					
13	b)	○	サポートされている署名パラメータ					
14	c)	○	署名対象の文書がハッシュとしてのみ提供される場合					
15	d)	○	サポートされている利用者の環境の署名生成装置（SCDev）、またはサポートされている署名者のデジタル署名値を生成するSSASC。					
16	OVR-6.2-08	○	利用規約は、サービス可用性に関するサービスレベル合意（SLA）の要素、および該当する場合は応答時間などの他のSLA情報を含むものとする(SHALL)。					
17	OVR-6.2-09	○	利用規約は、SLAが、署名に使用される証明書を発行するCAやタイムスタンプに使用されるTSAのようなSCASPの管理下にない他のTSPの運用、ポリシー、SLAによって影響を受ける可能性があることを通知するものとする(SHALL)。					
18	OVR-6.2-10	○	利用規約はSCASPがどのように個人データを処理するかを説明するものとする(SHALL)。					
-	6.3 Information security policy		6.3情報セキュリティポリシー					
19	OVR-6.3-01	○	「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6.3節に規定されている要件を適用するものとする(SHALL)ことに加えて、以下の特定の要件が適用される。					監査報告書リスト番号103項～112項参照
20	OVR-6.3-02	○	セキュリティポリシーは、個人データを保護するために実装されたセキュリティとプライバシーの管理を文書化するべきである(SHOULD)。 注： SCASPが署名対象のデータにアクセスできる場合、これには個人情報だけでなく機密情報も含まれる可能性がある。					
-	7 Signature creation application service management and operationon		7 デジタル署名生成サービスの管理と運用					
-	7.1 Internal organization		7.1内部組織					
21	OVR-7.1-01	○	「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節に規定されている要件が適用されるものとする(SHALL)。					監査報告書リスト番号113項～123項参照
-	7.2 Human resources		7.2人的資源					
22	OVR-7.2-01	○	「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7.2項に規定されている要件が適用されるものとする(SHALL)。					監査報告書リスト番号124項～143項参照
-	7.3 Asset managemen		7.3資産管理					
23	OVR-7.3-01	○	「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7.3項に規定されている要件が適用されるものとする(SHALL)。					監査報告書リスト番号144項～148項参照
-	7.4 Access control		7.4アクセス制御					
24	OVR-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」 の7.4節に規定されている要件が適用されるものとする(SHALL)。					監査報告書リスト番号149項～159項参照
-	7.5 Cryptographic controls		7.5暗号制御					
25	OVR-7.5-01	○	「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7.5項に規定されている要件が適用されるものとする(SHALL)。					監査報告書リスト番号160項参照
-	7.6 Physical and environmental security		7.6物理的および環境的安全					
26	OVR-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」 の7.6項に規定されている要件に加え、以下の特定の要件が適用されるものとする(SHALL)。					監査報告書リスト番号161項～165項参照
27	OVR-7.6-02	○	ETSI TS 119 101の5.2節に規定されている以下の要求事項がSCAに適用されるものとする(SHALL)：GSM 1.4。 GSM 1.4： 対応する標準に対してテストされた暗号ライブラリを使用すること。確立されたライブラリを使用すべきである(SHOULD)。					
-	7.7 Operation security		7.7運用セキュリティ					
28	OVR-7.7-01	○	「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項に規定されている要件に加え、以下の特定の要件が適用されるものとする(SHALL)。					監査報告書リスト番号166項～174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
29	OVR-7.7-02	○	ETSI TS 119 101の5.2節に規定されている以下の要求事項がSCAに適用されるべきである(SHOULD)：GSM 1.2およびGSM 1.3。 GSM 1.2: 最新のアプリケーション環境（管理されたソフトウェア環境）は、最新のセキュリティフィックスを含めて使用されるべきである(SHOULD)。 GSM 1.3: 標準化されたプロトコルとライブラリの実装は、十分にテストされ、レビューされたものを使用するものとする(SHALL)。					
30	OVR-7.7-03	○	ETSI TS 119 101の5.2節に規定されている以下の要求事項がSCAに適用されるものとする(SHALL)：GSM 2.4。 GSM 2.4：SCA/SVA/SAAは、公開アプリケーション環境の場合であっても、ユーザーから提供された全ての情報、およびアプリケーションとユーザーの間を流れる全てのデータの完全性と機密性を維持するものとする(SHALL)。					
-	7.8 Network security		7.8ネットワークセキュリティ					
31	OVR-7.8-01	○	「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7.8項に規定されている要件が適用されるものとする(SHALL)。					監査報告書リスト番号175項～194項参照
-	7.9 Incident management		7.9インシデント管理					
32	OVR-7.9-01	○	「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節に規定されている要件が適用されるものとする(SHALL)。					監査報告書リスト番号195項～206項参照
-	7.10 Collection of evidence		7.10証拠の収集					
33	OVR-7.10-01	○	「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7.10項に規定されている要件に加え、以下の特定の要件が適用されるものとする(SHALL)。					監査報告書リスト番号207項～214項参照
34	OVR-7.10-02	○	この情報が知られているときは、デジタル署名生成操作は、加入者の識別とともに記録されるものとする(SHALL)。					
35	OVR-7.10-03	○	イベントログはイベントの時刻でマークされるものとする(SHALL)。					
36	OVR-7.10-04	○	処理頻度、保存期間、保護、収集システムのバックアップ手順、アーカイブ手順、およびイベントログの脆弱性評価は、SCASC運用規程に文書化されるものとする(SHALL)。					
37	OVR-7.10-05	○	要件OVR-7.10.1およびOVR-7.10.2の実装は、適用されるプライバシー要件を考慮に入れるものとする(SHALL)。					
38	OVR-7.10-06	○	イベントログには、イベントの種類、イベントの成功または失敗、およびそのようなイベントの発生源となる人物および/またはコンポーネントの識別子を含めるものとする(SHALL)。					
-	7.11 Business continuity management		7.11事業継続マネジメント					
39	OVR-7.11-01	○	「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7.11節に規定されている要件が適用されるものとする(SHALL)。さらに、利用規約に指定されているとおりに事業継続性を提供するために、以下に示す要件が適用される。					監査報告書リスト番号215項,216項参照
40	OVR-7.11-02	○	ユーザーまたは第三者の意図的または意図的でない行動によるサービスの中断を回避するための対策が実施されるべきである(SHOULD)。					
41	OVR-7.11-03 [CONDITIONAL]	○	署名にタイムスタンプを追加するとき、SCASPのSLAは対応するTSAのSLAを考慮に入れるべきである(SHOULD)。					
-	7.12 Termination and termination plans		7.12終了および終了計画					
42	OVR-7.12-01	○	「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7.12項に規定されている要件が適用されるものとする(SHALL)。					監査報告書リスト番号217項～227項参照
-	7.13 Compliance and legal requirements		7.13コンプライアンスと法的要件					
43	OVR-7.13-01	○	「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7.13項に規定されている要件に加え、以下の特定の要件が適用されるものとする(SHALL)。					監査報告書リスト番号228項～232項参照
44	OVR-7.13-02	○	個人データが第三者によって処理される場合、法律により必要とされる場合は、個人データの第三者処理者が個人データを保護するための技術的、組織的および法的措置の実施を含む法的要件を遵守することを確実にするために、個人データの第三者処理者と適切な契約を結ぶものとする(SHALL)。 注1： 署名されるデータは個人データと見なされる。					
45	OVR-7.13-03	○	SCASCは、不要なときは処理後に署名者のドキュメントを格納しないものとする(SHALL NOT)。 注2： SCASPが保存サービスと組み合わせて機能する場合、そのようなデータを保存する必要があり得る。					
46	OVR-7.13-04	○	SCASPは、その機能の一部または全部が下請け業者によって行われている場合でも、第5章から第8章に定義された要件を満たすことに対して全体的な責任を負うものとする(SHALL)。					
-	8 Signature creation application service component technical requirements		8デジタル署名生成サービスコンポーネントの技術的要件					
-	8.1 Interface		8.1インターフェース					
47	ASI-8.1-02	○	デジタル署名値の生成に使用されるSCASCとSCDevの間の接続は保護されるものとする(SHALL)。					
48	ASI-8.1-03 [CONDITONAL]	○	SCASCがその文書を署名者に提示するとき、SCASC運用規程の中で、「見たものが署名したもの」であること(WYSIWYS)を保証する方法を記述するものとする(SHOULD)。					
49	ASI-8.1-04 [CONDITONAL]	○	SCASCが文書を変換して署名者に提示するとき、SCASC運用規程はそれが特定のデータをどのように変換するかを明記するものとする(SHALL)。 例： 署名される文書はXMLフォーマットであり、運用規程は、プレゼンテーションにどのソフトウェアが使用されるか、または異なるXMLタグを提示するために従うべき規則を述べている。					
50	ASI-8.1-05 [CONDITONAL]	○	SCASCが文書を署名者に提示するときには、SCASC運用規程または諸条件は、どのコンテンツタイプを正しく提示できるかを述べるものとする(SHALL)。					
51	ASI-8.1-06 [CONDITONAL]	○	SCASCが文書を署名者に提示するとき、データ内容の種類に従ってSDのすべての部分を正確に提示できない場合、インタフェースは署名者に警告するものとする(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
52	ASI-8.1-07 [CONDITONAL]	○	SCASCがクライアントにグラフィカルユーザインタフェースを提供するときは、ETSI TS 119 101の要件UI 1とUI 2が適用されるべきである(SHOULD)。 UI 1：ユーザーインターフェースは以下の通りであるべきである(SHOULD)： a) SCA/SVA/SAA の使用方法、および該当する場合、システムのインストールと設定に関する明確なユーザーガイダンスを提供すること； b) 各ダイアログステップがシステムからのフィードバックにより容易に理解できる程度に自己記述的であるか、または要求に応じてユーザに説明されること； c) 入力に明らかなエラーがあるにもかかわらず、最小限の修正動作で意図した結果を達成できる場合、エラーに寛容であること； d) ユーザーを前進させるために、有益なエラー報告を行う； e) 利用者が行った操作が正しい（または正しくない）ことを確認するためのフィードバックを提供する； f) 色表示を使用する場合、エラーには赤を、ゴー/プロシードには緑を使用する； g) いつでも、現在の操作をキャンセルしてメインメニューに戻ること、またはシステ ムを完全に終了することができること； h) 例えば、ユーザーインターフェイスにおいて、情報を他人がアクセスできないようにするなど、個人のプライバシーを保護すること； そして i) ユーザの重要な決定や選択について確認を求める。 UI 2：SCA/SVA/SAAは、署名の生成、補強、検証のプロセスを通じて、初めてのユーザーを導く詳細なユーザーズガイドを提供するものとする(SHALL)。					
53	ASI-8.1-08 [CONDITONAL]	○	SCASCが文書を署名者に提示するときには、署名者が文書の署名に同意することが署名者に明白であるワークフローであるものとする(SHALL)。					
54	ASI-8.1-09 [CONDITONAL]	○	SCASCが文書を署名者に提示するとき、ETSI TS 119 101のSCP 13とSCP 47が適用されるものとする(SHALL)。 SCP 13:SDが署名者に提示された場合、SCAは署名者に提示されたSDが署名プロセスで署名される SDと同一であることを保証するものとする(SHALL)。 SCP47:ビジネスプロセスに署名者への DTBS または SD の提示が含まれる場合、SCA は DTBS または SD が署名者に提示された後にのみ署名を計算するものとする(SHALL)。 注：一括署名の場合、署名者が全ての署名を取得するとは限らない					
55	ASI-8.1-10 [CONDITONAL]	○	SCASCが文書を署名者に提示するとき、SCASCは署名される文書のダウンロードを許可すべきである(SHOULD)。					
56	ASI-8.1-11 [CONDITONAL]	○	SCASCが文書を署名者に提示するとき、SCASCは文書が署名者に提示された期間を記録するものとする(SHALL)。					
57	ASI-8.1-12 [CONDITONAL]	○	SCASCが文書を署名者に提示し、文書がダウンロードされたとき、SCASCはそのようなイベントをログに記録するべきである(SHOULD)。					
-	8.2 AdES digital signature creation		8.2 デジタル署名の生成					
58	OVR-8.2-01	○	SCASCは受け取った情報の完全性と機密性を保証するものとする(SHALL)。					
59	OVR-8.2-02	○	使用される暗号アルゴリズムは、Cryptrecの「電子政府推奨暗号リスト」によって推奨されているアルゴリズムから選択されるべきである(SHOULD)。					
60	OVR-8.2-03	○	適用される暗号アルゴリズムは、運用規程や利用規約などで定義されているとおりであるものとする(SHALL)。					
61	OVR-8.2-04	○	ETSI TS 119 101のSCP 14、SCP 31、SCP 37およびSCP 61が適用されるものとする(SHALL)。 SCP 14: DAは、署名のために署名者が選択したSD が、署名のためにSCAに提供されたSDと同一であることを保証するものとする(SHALL)。 SCP 31：署名者が複数の署名証明書を使用できる場合、DAは署名者が署名を生成するために使用する証明書を選択できるものとする(SHALL)。DAは、ユーザにデフォルトの選択を提供することができる。選択可能なものが 1 つしかない場合、このステップは省略できる(MAY)。 SCP 37：SCAは、署名が生成された後、署名内の署名証明書への参照または署名証明書のコピ ーが検知されずに置き換えられないように保護するものとする(SHALL)。 注3：これは通常、このデータを文書とともに署名し、署名フォーマットの認証済み属性セ クションなどに格納することで実現される。 SCP 61：署名者の認証データがSCAを通過する際、SCAは認証データの機密性と完全性を維 持し、不要になり次第（例えば、署名者の代替や署名者の登録が削除された場合）、安全に消去するものとする(SHALL)。					
62	OVR-8.2-05	○	SCASCは、署名者にコミットメントタイプ(署名の意図・目的)を知らせるものとする(SHALL)。 注2： この情報は署名ポリシー、運用規程、利用規約の中で与えることができる。					
63	OVR-8.2-06	○	SCASCは、署名証明書チェーンを署名に含めるべきである(SHOULD)。					
64	OVR-8.2-07	○	署名者は、どの署名生成ポリシーが適用されるのかを知ることができるものとする(SHALL)。					
65	OVR-8.2-08	○	署名者は、特定の署名を生成するときにどの署名生成ポリシーが適用されたかを知ることができるものとする(SHALL)。 例1： どの署名生成ポリシーが特定の署名に適用されるか、または適用されたかに関する情報は、署名者のユーザーアカウントから知ることができる。 例2： 署名生成ポリシーを署名済み属性として署名に追加できる。 例3： SCASPは各時点で有効な署名生成ポリシーを1つだけ持ち、署名の時点からどのバージョンが適用されるのかが明確になる。 例4：運用規程や利用規約などによって署名生成ポリシーを示すことができる。					
66	OVR-8.2-08A	○	SCASCは署名者に署名を提供するべきである(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
67	OVR-8.2-09 [CONDITIONAL]	○	SCASCが署名付きデータにアクセスできる場合、署名付きデータと署名者を署名者に提供すべきである(SHOULD)。 注3： 署名が署名されたデータで包まれているか包み込まれている場合、OVR-8.2-09はOVR-8.2-08から直接続く。					
-	9 Framework for definition of signature creation application service component policy built on the present document		9 本書を基に構築された署名生成アプリケーションサービスコンポーネントポリシーの定義のためのフレームワーク					
68	OVR-9-01A [CONDITIONAL]	○	本書で定義されたトラストサービスポリシーの上にSCASCポリシーを構築する場合、SCASCポリシーは、本書で定義されたトラストサービスポリシーのどの項目を採用したかを示すものとする(SHALL)。					
69	OVR-9-02 [CONDITIONAL]	○	本書で定義された要件に基づいてSCASCポリシーを構築する場合、ポリシーは、適用することを選択したあらゆるバリエーションを明らかにするものとする(SHALL)。					
70	OVR-9-03 [CONDITIONAL]	○	本書で定義された要件に基づきSCASCポリシーを構築する場合、契約者は、利用規約の実施の一部として、特定のポリシーが本書で定義されたポリシーの要件を追加する、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)。					
71	OVR-9-04 [CONDITIONAL]	○	本書で定義された要件に基づきSCASCポリシーを構築する場合、ポリシーの規定と承認について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)。					
72	OVR-9-05 [CONDITIONAL]	○	本書で定義された要件に基づいてSCASCポリシーを構築する場合、ビジネス要件を評価し、明記されたコミュニティと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べきである(SHOULD)。					
73	OVR-9-06 [CONDITIONAL]	○	本書で定義された要件に基づいてSCASCポリシーを構築する場合、ポリシーを維持するための責任を含め、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ものとする(SHALL)。					
74	OVR-9-07 [CONDITIONAL]	○	本書で定義された要件に基づいてSCASCポリシーを構築する場合、ポリシーが運用規程に裏付けられていることを確実にするために、定義されたレビュー プロセスが存在するものとする(SHALL)。					
75	OVR-9-08 [CONDITIONAL]	○	本書で定義された要件に基づいてSCASCポリシーを構築する場合、TSPは、TSPがサポートするポリシーをそのユーザーコミュニティに公開すべきである(SHOULD)。					
76	OVR-9-09 [CONDITIONAL]	○	本書で定義された要件に基づいてSCASCポリシーを構築する場合、TSPがサポートするポリシーの改訂は加入者が利用できるようにすべきである(SHOULD)。					
77	OVR-9-10 [CONDITIONAL]	○	本書で定義された要件に基づいてSCASCポリシーを構築する場合、そのポリシーに対して一意なオブジェクト識別子（OID や URI など）を取得するものとする(SHALL)。					
「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					
78	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]					
79	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。					
80	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]					
81	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]					
82	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					
83	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]					
84	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]					
85	• REQ-6.1-03	対象外	廃止					
86	• 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。					
87	• 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]					
88	• REQ-6.1-05	対象外	廃止					
89	• 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。					
90	• 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。 ☒HALL]					
91	• REQ-6.1-07	○	TSPの管理者は業務を実装するものとする。[SHALL]					
92	• 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。					
93	• REQ-6.1-09	対象外	廃止					

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
94	• 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]					
95	• 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]					
96	• 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					
97	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]					
98	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。					
99	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]					
100	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]					
101	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]					
102	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					
103	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]					
104	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]					
105	• 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]					
106	• 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。					
107	• 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]					
108	• 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]					
109	• 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]					
110	• 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]					
111	• 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]					
112	• 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					
113	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]					
114	• 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]					
115	• 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]					
116	• 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]					
117	• 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]					

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
118	• 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]					
119	• 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]					
120	• 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]					
121	• 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]					
122	• 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					
123	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					
124	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。					
125	• 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]					
126	• 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]					
127	• 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。					
128	• 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。					
129	• 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]					
130	• 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]					
131	• REQ-7.2-08	対象外	廃止					
132	• REQ-7.2-09	対象外	廃止					
133		○	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。					
134	• 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]					
135	• 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]					
136	• 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。					
137	• 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]					
138	• 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。					
139	• 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。					
140	• REQ-7.2-16	対象外	廃止					

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
141	• 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]					
142	• 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]					
143	• 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					
144	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]					
145	• 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					
146	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]					
147	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]					
148	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					
149	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]					
150	• REQ-7.4-02	対象外	廃止					
151	• REQ-7.4-03	対象外	廃止					
152	• REQ-7.4-04	対象外	廃止					
153	• 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]					
154	• 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]					
155	• 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]					
156	• 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]					
157	• 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]					
158	• 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]					
159	• 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					
160	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					
161	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。					
162	• 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。					
163	• 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]					
164	• 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]					
165	• 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					

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
166	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。					
167	• 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]					
168	• 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]					
169	• 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。					
170	• 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]					
171	• REQ-7.7-06	対象外	廃止					
172	• REQ-7.7-07	対象外	廃止					
173	• 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]					
174	• 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					
175	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]					
176	• 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]					
177	• 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]					
178	• 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]					
179	• 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]					
180	• 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]					
181	• 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]					
182	• 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]					
183	• 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]					
184	• 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]					
185	• REQ-7.8-11	対象外	廃止					
186	• 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]					
187	• 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]					
188	• 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]					
189	• 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]					
190	• 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]					
191	• 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]					
192	• 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]					
193	• 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]					
194	• 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					

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
195	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。					
196	• 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]					
197	• 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。					
198	• 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。					
199	• 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]					
200	• 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]					
201	• 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。					
202	• 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]					
203	• 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]					
204	• 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]					
205	• 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。					
206	• 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					
207	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。					
208	• 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]					
209	• 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]					
210	• 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]					
211	• 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]					
212	• 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]					
213	• 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]					
214	• 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					
215	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]					
216	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					
217	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]					

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
218	• 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。					
219	- 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]					
220	- 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]					
221	- 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]					
222	- 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]					
223	- 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]					
224	- 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]					
225	• 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]					
226	• 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。					
227	• 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					
228	・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]					
229	• 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]					
230	• 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]					
231	• 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]					
232	• 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。					