T - 技術的措置及び組織的措置（TOM） 確認項目及び管理項目

次の基準は、取り扱う個人データを保護するために設定された技術的及び組織的措置に対処することを目的とする。参照文書を含む「検証手段の提案」は、本基準を充足するか否かの判断するために十分な証拠が収集されるまで、基準に基づき評価されなければならない。

参照ID	申請者	特定 / 一般	レベル	タイトル	評価対象に適用可能な基準（規定条項）	実施ガイダンス（更新の対象となる情報提供条項）	提案された検証手段	GDPR		
T.1				**コア安全性要件** 申請者は、個人データを保護し、その機密性、完全性及び可用性を確保するために十分な措置を講じなければならない。						
T.1.1				**データアクセスの制限**						
T.1.1.1	CP	S	A	アクセス制御方針及び登録簿	A) 申請者は、役割及び責任を中心に定義され、個人データの取扱いを考慮したアクセス制御方針を策定し、文書化しなければならない。 【AND】 B) 当該アクセス制御方針は、少なくとも次の事項を明確にしなければならない。 b.1) 最小アクセス権限の原則に従い、役割に基づき誰がデータにアクセスし利用する必要があるか b.2) 【AND】個人データへの電子的及び物理的アクセスに関する情報 b.3) 【AND】個人データを含む情報分類体系に関連するセキュリティ要件 b.4) 【AND】アクセス制御の責任に関する情報 【AND】 C) 申請者は、個人データにアクセス可能な労働者のアクセス権に関する最新の台帳を維持しなければならない。 【AND】 D) 申請者は、次の事項を実施するための手順、方針又は仕組みを整備しなければならない。 d.1) ユーザーのアクセス権のレジストリを定期的に見直すこと d.2) 【AND】個別の変更及びより広範なシステムに関するアクセス権の変更を記録すること d.3) 【AND】アクセス権の設定、付与又は取消しを含め、アクセス権を定期的に監査すること d.4) 【AND】ユーザーの登録及び登録解除を行うこと 【AND】	申請者は、役割及び責任に基づいて定義された包括的なアクセス制御ポリシーを有しているのが望ましい。これは、アクセス権のレジストリによって補完され、最小権限の原則を遵守するのが望ましい。対応するポリシー又はレジストリは、各労働者のカテゴリー又は各労働者に付与されたアクセス権について、適切な正当化を提供するのが望ましい。 アクセス権のレジストリ、並びに、アクセス権の付与及び取消しに関する管理手順を提示する必要がある。 ISOなどの標準化された管理項目は、当該認証の基準を充足していることを示すため申請者に関連し得る。	アクセス権台帳 調査 CISO、DPO若しくは労働者、又は、その複数との面談	32	1	12
T.1.1.2	CP	G	A	アクセス権の最小化（最小特権）	A) アクセス権は、「最小特権」原則に従い、必要に応じて限定され、付与されなければならない。 【AND】 B) 最小特権方針は、次の事項を含まなければならない。 b.1) データを取扱う施設及びシステムへの物理的アクセス b.2) データを取扱うシステム及びアプリケーションへの一般的なアクセス b.3) 特定のデータアクセス	データへのアクセス権は最小限に抑え、データにアクセスする必要がある労働者と、その業務を遂行するために必要なデータに限定するのが望ましい。申請者は、システム管理者のような高特権プロファイルに適用可能な追加のセキュリティ対策も講じるのが望ましい。 アクセス権方針は、次の3つの異なる要素を考慮に入れるのが望ましい。 1. データを取扱う施設及びシステムへの（物理的）アクセス（T.1.1.4参照） 2. データを取扱うシステム及びアプリケーションへの一般的なアク	アクセス権台帳及び規則 特権アクセス管理ツール（該当する場合） 調査	25, 32	1	4
T.1.1.3	CP	G	A	パスワード方針	A) パスワードの信頼性を確保するため、最小文字数、複雑性要件及び更新頻度（又は代替措置）を規定したパスワード方針が整備されなければならない。 【AND】 B) 法で要求される場合、記録保存されたデータにアクセスするためのパスワード方針は、国内法及び規制を遵守しなければならない。	申請者は、個人データにアクセスするために十分な強度の認証を要求する方針を策定しなければならない。パスワード方針は、国家の方針、ガイドライン及び義務の対象となる場合がある。ENISAなどの組織は、パスワード管理及び方針に関する有用なガイドラインを提供しており、参考ガイドラインとして利用できる。整備される方針又は仕組みは、サーバーにアクセスするための十分な認証方法の使用を強制するものであるのが望ましい。必要に応じて、サーバーにアクセスするためのパスワードの変更を強制する方針を整備するのが望ましい。定期的な間隔でのパスワードの更新を強制することは推奨されるが、必須とはみなされないのが望ましい。	文書レビュー 調査及び証明 パスワード方針の適用に関する構成レビュー及び技術的評価 アクセス制御メカニズムの試験	32	1	2

T.1.1.4	CP	G	A	物理的アクセスの制限	A) 申請者は、次の措置を実施しなければならない。 a.1) 個人データが記録保存され、又は、その他の方法でアクセス若しくは取り扱われる場所及びデバイスの特定 a.2) 【AND】各場所及びデバイスのカテゴリに対するリスクの評価 a.3) 【AND】かかるリスクを低減するための効果的なアクセス制御メカニズムの実装	個人データを記録保存、取扱い、アクセスするために意図された場所及びデバイスは、効果的なアクセス制御を備えた物理的に安全な環境に配置されるのが望ましい。これは、サーバー、ハードウェア、リムーバブルメディア、印刷物などに及ぶ。 リスクの特定及び評価は、基準G.6.2.4のリスクアセスメントに含まれることが期待される。	物理的アクセス制御及び物理的アクセス規則の調査 施設管理者との面談 ソーシャルエンジニアリングアプローチ又はレッドチーム演習による試験	25, 32	1	3
T.1.1.5	CP	G	A	アクセスログ及び移転ログ	A) 申請者は、次の措置を実施しなければならない。 a.1) 実施したリスクアセスメントに基づくログとして記録する必要のある情報の特定 a.2) 【AND】暗号化を含むログを保護するためのセキュリティ対策の実装 a.3) 【AND】データ最小化の要件に従ったログ保持期間の決定 【AND】 B) 申請者は、次の事項のログを記録し、保管するための監視システム、仕組み又は手続を整備しなければならない。 b.1) データの目的及び使用 b.2) 【AND】申請者の労働者及び代理人による個人データ及びデータを含むシステムへのアクセス b.3) 【AND】EEA域内及び第三国からの個人データ及び関連システムへのリモートアクセス b.4) 【AND】組織内及び組織と他の当事者間におけるあらゆる種類の個人データ移転に関する移転規則の情報	監視システムは、データ主体の権利及び自由を保護するために、技術の最先端に関して信頼性が高く、十分に強力である必要がある。 リスクの特定及び評価は、基準G.6.2.4のリスクアセスメントに含まれることが期待される。	調査 アクセスログ及び移転ログ CISO又はDPOとの面談	32	1	8
T.1.1.6	CP	G	A	BYOD（Bring Your Own Device） 方針	A) 申請者は、次の措置を講じるための書面による規則又は方針を整備しなければならない。 a.1) アクセス可能なデータを特定すること a.2) 【AND】許可されたデバイスを特定すること a.3) 【AND】データ主体のリスクを制限するため、個人のモバイルデバイスの適切な使用を規定すること a.4) 【AND】データが保護されるのを確保するため、モバイルデバイスの使用に関するアクセス制御及び制限を規定すること a.5) 【AND】特定されたリスクに対応するたにデータを保護するセキュリティ対策を含めること a.6) 【AND】サーバーへのアクセス権限を有する労働者に認識されること 【AND】 B) 申請者は、次の事項のための手順又は仕組みを整備しなければならない。 b.1) 当該方針の実装 b.2) 【AND】使用されるデバイス及びこれに対応するアクセス権を文書化すること b.3) 【AND】特定されたリスクに対応するために講じられているセキュリティ対策を文書化すること	方針は、個人データが記録保存されているサーバーへのモバイルデバイス（スマートフォン、ノートパソコン、USBメモリなど）によるアクセスを制御及び制限するために適用されるのが望ましい。明確な書面による方針が採用及び実施され、並びに、データにアクセスする労働者に認識されている望ましい。該当する場合、検査が実施されるのが望ましい。該当する場合、USBポートは無効にされるのが望ましい。BYOD方針には、OS及びソフトウェアの更新管理も含まれる場合がある。その他のセキュリティ対策には、暗号化、デバイスのリモートブロックなどが含まれる場合がある。 方針は最新の技術水準に準拠しているのが望ましい。 リスクの特定及び評価は、基準G.6.2.4のリスクアセスメントに含まれることが期待される。	方針 調査（デバイスのBYO方針へ遵守を含む） 労働者との面談	32	1	10
T.1.1.7	CP	G	A	セッションの自動ログアウト	A) 個人データの取扱いに使用されるシステムへのアクセスは、セッションの自動ログアウトのメカニズムによって保護されなければならない。 【AND】 B) 申請者は、特定されたリスクに対応するため、セッションが終了されるまでの時間を文書化し、正当化しなければならない。	ユーザーの非活動時に自動的にログアウトし、セッションを終了させるためのメカニズムが整備されているのが望ましい。 リスクの特定及び評価は、基準G.6.2.4のリスクアセスメントに含まれることが期待されている。	調査及び証明 アクセス制御メカニズムのテスト	25, 32	1	2
T.1.1.8	CP	S	A	多要素認証	A) 申請者は、次の措置を実施しなければならない。 a.1) データ取扱いに関連するリスクを考慮し、多要素認証を導入する必要性を評価すること a.2) 【AND】必要と判断される場合、労働者、代理人及びその他のユーザーのために多要素認証を導入すること	個人データを記録保存、取扱い及びアクセスするための場所及びデバイスへのアクセスは、適切な認証メカニズムを通じて制御されるのが望ましい。かかるメカニズムは、保護される資産の価値に適合し、低価値の場合には十分に安全なパスワードを含み、多要素認証を含むのが望ましい。リスクの特定及び評価は、基準G.6.2.4のリスクアセスメントに含まれることが期待される。	個人データを記録保存するサーバーへのアクセスは、適切な認証メカニズムを通じて制御されるのが望ましい。メカニズムは、保護される資産の価値に応じたものであって、低価値の場合には十分に安全なパスワード、多要素認証が用いられ	32	1	2
T.1.2				**データ暗号化、仮名化及び匿名化**						

T.1.2.1	CP	S	A	暗号化	【IF】申請者のリスクアセスメントにおいて、個人データの取扱いが自然人の権利及び自由にもたらすリスクに対処すべくセキュリティレベルを確保するため、データ暗号化が必要であると結論付けられた場合、【THEN】次のとおりとする。 A) 電子データへの不正アクセスのデータ主体へのリスクは、次の要件を充足する報告書において、特定及び評価されなければならない。 a.1) 自然人の権利及び自由に対する不正アクセス（公的機関によるものを含む）のリスクを考慮すること a.2)【AND】データ送信及び保存に関連するリスクを考慮すること a.3)【AND】暗号鍵への不正アクセス又は誤用に関連するリスクを考慮すること a.4)【AND】特定されたリスクに応じて、必要な暗号化の水準及び範囲を決定すること a.5)【AND】取り扱われるデータの暗号化方針を規定すること a.6)【AND】残存リスク及びそれに対処するための措置を特定すること 【AND】 B) 次の事項を確保するための方針、手順又は仕組みが整備されなければならない。 b.1) 暗号化アルゴリズムが既知の脆弱性のない最新のソフトウェアによって実装されることを確保すること b.2)【AND】暗号鍵を保護し、暗号化されたデータとは別に保管すること b.3) 【AND】最小特権アクセス権原則に基づき、暗号鍵へのアクセス権の記録を維持すること b.4) 【AND】補完的措置について、少なくとも年に1回の見直しを行い、最新の技術水準に適合していることを確保すること 【AND】 C) データは、規定された暗号化方針に従って暗号化されなければならない	該当する場合、申請者は、httpsを用いて、ウェブインターフェース上で収集又は表示される個人データを含む、施設外での個人データの電子的な移転及び通信を暗号化するのが望ましい。 申請者は、暗号化に関する適用可能な規制、暗号化の技術的実現可能性及び暗号化方針で定義された暗号化メカニズムを考慮し、最新の技術水準に準拠することを確保するのが望ましい。 静止データ（保存データ）は、不正アクセスのリスクが示される場合に暗号化されるのが望ましく、これにはエンドユーザーのデバイス、共有システム又は第三者のインフラストラクチャに保存されたデータも含まれる。クライアントオペレーティングシステムのストレージ暗号化は、関連する場合に有効にされるのが望ましく、その設定は暗号化方針に文書化されるのが望ましい。 送信は、公的又は共有ネットワークを介したものや、申請者の組織的管理外の処理者又は取得者を含む移転をカバーするのが望ましい。 暗号化措置は、申請者の暗号化方針に従い、暗号鍵が適切に保護され、暗号化されたデータとは別に管理されるように実施されるのが望ましい。 個人データが申請者の施設又は組織的管理外の処理者、パートナー又は取得者に移転される場合、第三国の文脈を含め、申請者は、暗号化が特定されたリスクを効果的に低減するか否か、暗号鍵へのアクセスが適切に制限されているか否かを評価するのが望ましい。 個人データの収集、取扱い若しくは共有、又は、その複数がまだ開始されていない場合、監査人は、技術的及び組織的措置の効率を試験及び検証するために非個人データの使用を要求するのが望ましい。 リスクの特定及び評価は、基準GI.6.2.4のリスクアセスメントに含	調査 サンプル分析 文書レビュー	32.1.a	1	12
T.1.2.2	CP	G	A	バックアップの暗号化	【IF】申請者のリスクアセスメントにおいて、個人データの取扱いが自然人の権利及び自由にもたらすリスクに対処すべくセキュリティレベルを確保するため、バックアップの暗号化が必要であると結論付けられた場合、【THEN】次のとおりとする。 A) 個人データを含むバックアップファイルは、暗号化されなければならない。	サーバーOSのストレージ暗号化が有効にされるのが望ましく、暗号化の設定は暗号化方針に文書化されるのが望ましい。 リスクの特定及び評価は、基準G.6.2.4のリスクアセスメントに含まれることが期待される。	調査及び証明 サンプル分析	25, 32	1	1
T.1.2.3			A	仮名化	【IF】申請者のリスクアセスメントにおいて、個人データの取扱いが自然人の権利及び自由にもたらすリスクに対処すべくセキュリティレベルを確保するため、データの仮名化が必要であると結論付けられた場合、【THEN】次のとおりとする。 A) 個人データは仮名化されなければならない。 【AND】 B) 申請者は、次の事項を含め、仮名化プロセスを文書化しなければならない。 b.1) 使用される技術及びその選択の正当化理由 b.2)【AND】設定パラメータ b.3)【AND】再識別キー及びルックアップテーブルの保存及び保護措置 b.4)【AND】予想される残存リスク及びそれを低減するための追加措置 【AND】 C) 申請者は、次の事項を証明しなければならない。 c.1) 導入された仮名化技術が、追加情報へのアクセスなく、復元不可能な出力を生成すること c.2) 【AND】合理的に想定される方法によっても、再識別キーなく、仮名から自然人への再識別ができないこと c.3) 【AND】適用される技術が、個人データの各カテゴリに関連するリスクに照らして適切であること 【AND】 D) 再識別キーは、仮名化されたデータとは別に保管されなければならない。 【AND】 E) 申請者は、仮名化プロセス及び残存リスクについて、少なくとも技術的措置に変更が講じられる場合には、定期的に見直し及び更新を行うための手順、規則又は方針を整備しなければならない。	該当する場合、申請者は個人データを仮名化するのが望ましい。 申請者は、仮名化措置がEDPBの仮名化に関するガイドライン1/2025などのスタンダード及びガイドラインで設定された要件と整合していることを確保するか、又は、評価時点での最新技術と整合する同等若しくはそれ以上のセキュリティレベルを証明するのが望ましい。受け入れ可能な仮名化は、少なくとも次を確保する。 - リンク不可：仮名化されたデータセットは、追加情報を使用せずに特定の個人に帰属させることができない - キー／追加情報の分離：再識別を可能にする追加情報は、異なるセキュリティ及びアクセス制御の下で別々に保存される - 文脈的堅牢性：選択された方法は、文脈、データタイプ及び可能性のある外部データセットを考慮した再識別に対して堅牢である - 再識別リスクのスケーラビリティ：データセットが他の合理的にアクセス可能なデータセットと結合されるときに、再識別のリスクは実際には増加しない - 透明性及び文書化：申請者は仮名化技術、その実施、及び、講じられている保護措置を文書化する - レビュー及び適応: 措置は、技術的及び法的な進展を反映するために定期的にレビューされる。 個人データの収集、取扱い若しくは共有、又は、その複数がまだ開始されていない場合、監査人は、技術的及び組織的措置の効率を試験及び確認するために非個人データの使用を要求するのが望ましい。 申請者は、次の項目を含む仮名化プロセスを文書化するのが望ましい。 - 使用された技術 - 当該技術を選択した理由	調査 サンプル分析 文書レビュー	32	1	10

T.1.2.4			A	匿名化	【IF】申請者のリスクアセスメントにおいて、個人データの取扱いが自然人の権利及び自由にもたらすリスクに対処すべくセキュリティレベルを確保するため、データの匿名化が必要であると結論付けられた場合、【THEN】次のとおりとする。 A) 個人データは匿名化されなければならない。 【AND】 B) 申請者は、再識別に使用されると合理的に想定されるあらゆる手段を考慮に入れ、匿名化されたデータがいかなるデータ主体にも結び付けられないことを確保しなければならない。 【AND】 C) 申請者は、次の事項を含め、匿名化プロセスを文書化しなければならない。 c.1) 使用される技術及びその選択の正当化理由 c.2) 【AND】予想される残存リスク及びそれを低減するための追加措置 【AND】 D) 申請者は、匿名化されたデータセットが、次の方法によるデータ主体の再識別を防止していることを証明しなければならない。 d.1) 個々のデータ主体の特定 d.2) 【AND】データセット内又は異なるデータセット間におけるレコードの連結可能性 d.3) 【AND】センシティブ又はユニークな属性の推定 【AND】 E) 申請者は、匿名化プロセス及び残存リスクについて、少なくとも技術的措置に変更が加えられた場合には、定期的に見直し及び更新を行うための手順、規則又は方針を整備しなければならない。	申請者は、匿名化が不可逆性を達成し、その後に自然人の識別が合理的に使用される手段を用いて不可能になることを確保するのが望ましい。 匿名化プロセスは体系的で文書化されるのが望ましく、次の内容を含むのが望ましい。 - 適用された技術 - 当該技術を選択する理由 - 匿名化前後の再識別リスクの評価 - データの使用、開示及びアクセス可能性の文脈 堅牢性の基準を充足するため、匿名化は次の事項を防ぐのが望ましい。 - 特定（データセット内で個人を孤立させることができないこと） - リンク可能性（レコードが異なるデータセット間で同じ人物にリンクできないこと） - 推測（センシティブ又は識別可能な属性が信頼性を持って推測できないこと） 申請者は、データのリリース又は再利用の前に、残余リスクを文書化し評価するのが望ましい。 個人データの収集及び/又は取扱い及び/又は共有がまだ開始されていない場合、監査人は、実施されている技術的及び組織的措置の効率をテスト及び検証するために非個人データの使用を要求するのが望ましい。 リスクの特定及び評価は、基準ISO/IEC 27005のリスクアセスメントに合	調査 サンプル分析 文書レビュー	25、 Rec 26	1	8
T.1.2.5	CP	G	A	暗号化方針	【IF】ToEにおけるデータが暗号化手法によって保護されている場合、【THEN】次のとおりとする。 A) 申請者は、次の事項を規定した暗号化方針を整備しなければならない。 a.1) データの各カテゴリーに使用する暗号アルゴリズム（その決定の正当性理由） a.2) 【AND】鍵の生成、更新、配布（該当する場合）、インストール、使用、分離、エスクロー及び失効（破棄） a.3) 【AND】適切な鍵長の要件 a.4) 【AND】鍵を変更しなければならない期間又は鍵ローテーションを実施しなければならない条件 a.5) 【AND】鍵の保管要件 a.6) 【AND】バックアップを含む鍵の保護措置 a.7) 【AND】鍵へのアクセス権 【AND】 B) 当該暗号化方針が最新の技術水準に適合していることを確保するため、少なくとも年1回見直しを行うための手順、規則又は仕組みを整備しなければならない。 【AND】 C) 申請者は、自らの暗号化方針の実施状況を文書化しなければならない。	暗号化方針は明示的、具体的かつ完全でなければならない。使用される全てのアルゴリズムのリストを編纂し、その目的（静止時の暗号化、転送中の暗号化、整合性保護など）を含む必要がある。本方針は、認められた技術標準及び関連機関からのガイダンスに基づいて、最新の技術水準を考慮に入れるのが望ましい。 申請者は、明確な暗号化方針を定義し、その効果的な尊重及び実施を確保することが期待される。 申請者は、暗号化方針に少なくとも次の事項が含まれることを確保するのが望ましい。 - 鍵を変更する必要がある時間間隔又は条件、及び、鍵をローテーションしなければならない条件（疑わしい侵害、アルゴリズムの廃止、又は、リスク若しくは取扱い状況の変更など）の仕様 - 暗号鍵の安全な保管及びアクセス制御要件の記述、権限のある要員のみが当該鍵にアクセス、変更又は使用できることを確保し、アクセス権の定義及び管理、並びに、適切な場合には職務の分離 - 関連する場合、鍵がどのように生成、配布、アクティブ化、保管、ローテーション、アーカイブ（該当する場合）及び取消し（又は破棄）されるかの仕様（鍵のライフサイクル全体をカバーする） 鍵管理手順は、侵害され、又は、廃止された鍵が迅速に交換され、安全に取り消されることを確保し、かかる事象が文書化されることを確保しなければならない。 暗号化方針の遵守を証明するため、適切なログ又は監査証跡が維持されるのが望ましい。 暗号関数（鍵なしハッシュ関数、対称アルゴリズム及び非対称アルゴリズムなど）は、データの性質、目的、範囲などに基づいて異なるデータの種類に使用される可能性がある。	暗号化方針のレビュー 定期的な設定の調査	32	1	9
T.1.3				**インターネットアクセスの接続性チェック** 条件: 【IF】評価対象にインターネットアクセスが含まれている場合、【THEN】次のとおりとする。						
T.1.3.1	CP	G	A	HTTPS有効化	A) ウェブインタフェースへのアクセスには、デフォルトでHTTPSを有効にしなければならない。	ウェブインターフェースのコンプライアンスは、証明及び試験されるのが望ましい。ウェブインターフェースには、ユーザーがウェブサイト、その他のオンラインアプリケーション及び技術システムと対話することを可能にするヒューマンマシンインターフェースが含まれる。	調査及び試験 ウェブインターフェースのセキュリティ方針レビュー 設定レビュー及びテスト サンプル試験／分析	32	1	1

T.1.3.2	CP	G	A	SDNS有効化	A) 申請者は、次の事項を実施しなければならない。 a.1) ウェブインターフェースを通じたデータの取扱いに関連するリスクを評価すること a.2) 【AND】 特定されたリスクに対処するための低減措置を講じること（公開ドメイン名の解決における改ざん又は誤誘導を防止するためのセキュアDNS（DNSSEC）を含む）	ウェブインターフェースの遵守は証明及び試験されるのが望ましい。ウェブインターフェースには、ユーザーがウェブサイト、他のオンラインアプリケーション及び技術システムと対話することを可能にするヒューマンマシンインターフェースが含まれる。評価は基準G.6.2.4のリスクアセスメントに含めることができる。	調査 サンプル試験	32	1	2
T.1.3.3	CP	G	A	SSL	A) セキュアでないSSLは使用してはならない。	SSL 2.0は禁止され、SSL 3.0はセキュアでない。暗号ツール方針に反映されるのが望ましく、該当する場合は試験されるのが望ましい。	調査 サンプル試験	32	1	1
T.1.3.4	CP	G	A	TLS	A) セキュアでないTLSは使用してはならない。	TLS 1.1はセキュアでなく、個人データを適切に保護するためには認められない。サイバーコミュニティによって十分にセキュアであるとみなされる場合は、より高いバージョンのTLS（すなわちTLS 1.2）を使用することができる。TLSを使用する場合は、適切に設定され、暗号化方針に記載されるのが望ましい。該当する場合は、試験されるのが望ましい。	調査 サンプル試験	32	1	1
T.1.3.5	CP	G	A	SSH	A) セキュアでないSSHは使用してはならない。	SSH1はセキュアでなく、個人データを適切に保護するためには認められない。SSHの高いバージョン（SSH-2）は、サイバーセキュリティコミュニティによって十分にセキュアであるとみなされる場合に使用できる。SSHを使用する場合は、適切に構成され、暗号化方針に記載されるのが望ましい。該当する場合は、試験されるのが望ましい。	調査 サンプル試験	32	1	1
T.1.3.6	CP	G	A	下位非互換性	A) セキュアでないSSL又はTLSバージョンとの下位互換性は無効にされなければならない。	レガシークライアントが拒否されることを示すテストプロトコルの構成を実施するのが望ましい。	調査 サンプル試験	32	1	1
T.1.3.7	CP	G	A	無線通信ネットワーク	A) 無線通信ネットワークへの接続はパスワードによって保護されなければならない。 【AND】 B) 訪問者がアクセス可能な無線通信ネットワークは、内部目的で使用されるWiFiネットワークから分離されなければならない。	無線通信ネットワークのアクセスポイントは、ハッカーにとってネットワークへの脆弱な侵入点を構成し、適切に保護されなければならない。無線ネットワークへの認証方法は実施及び強制されることが期待される。 無線ネットワークのアクセス及びセキュリティの設定は、最新の技術水準に沿ったものでなければならない。	調査 サンプル試験	32	1	2
T.1.4				**その他のセキュリティ対策**						
T.1.4.1	CP	G	A	機密性、完全性、可用性及びレジリエンス	A) 申請者は、次の目的のため、セキュリティインシデント発生時において、ToEにおける個人データの可用性及び完全性、並びに、取扱いシステム及びサービスのレジリエンスを確保するための継続計画を整備しなければならない。 a.1) 個人データの継続的な可用性及び完全性を確保するため a.2) 【AND】取扱いシステム及びサービスのレジリエンスを確保するため 【AND】 B) 当該計画には、少なくとも次の情報を含めなければならない。 b.1) 計画の目的及び適用範囲 b.2) 【AND】申請者の組織内における役割及びそれに対応する各責任 b.3) 【AND】重要なプロセス及びシステム b.4) 【AND】データの機密性、完全性、可用性、並びに、取扱いシステム及びサービスのレジリエンスに関連するリスクに対処するための措置 b.5) 【AND】セキュリティインシデントへの対応手順 b.6) 【AND】データ復旧手順 【AND】 C)	申請者は、サイバー攻撃、ランサムウェア、ハードウェアのクラッシュなどのセキュリティインシデントが発生した場合にデータの可用性を回復するための継続性計画を策定するのが望ましい。サービス拒否攻撃の事例において、申請者は、特定の閾値、制御措置、リスク低減措置を備えた専用の措置を講じるのが望ましい。標準化された管理項目（ISOなど）は、申請者が本認証の基準を充足していることを示すのに関連する可能性がある。継続性を確保するための措置は、所轄機関のガイドライン（EDPB及びENISAを含む）に準拠し、最新の技術水準に準拠しているのが望ましい。 リスクの特定及び評価は、基準G.6.2.4のリスクアセスメントに含まれることが期待される。	セキュリティに関する規則及び方針 継続計画 労働者、CISO及びDPOとの面談	32	1	9

T.1.4.2	CP	G	A	バックアップ方針及び復旧テスト	A) 次の事項を定めたバックアップポリシーが整備されなければならない。 a.1) バックアップの頻度 a.2) バックアップ対象のデータ a.3) データ最小化要件に従ったバックアップ方法 a.4) バックアップデータの保存場所 a.5) バックアップファイルを不正アクセスから保護するための措置 【AND】 B) 少なくとも年1回、データ復旧テストを実施するための手順が整備されなければならない。 【AND】 C) 復旧テストにおいて対処すべき問題が特定された場合、申請者は当該問題に対して必要な措置を講じなければならない。	バックアップファイルに基づくデータ復旧システムは、過去12か月間に成功裏に試験されているのが望ましい。復旧テストの要件は、データ主体に対する特定のリスクを考慮するものとする。例えば、病院が個人データを保有している場合、データ主体に対するリスクが高いため、復旧時間を厳格に最小化する必要がある。一方、パン屋の顧客リストの復旧はデータ主体に対する影響が少ない。原則として、成功したバックアップ復旧テストは、48時間以内に99%以上のデータを復元することを要求するのが望ましい。試験の頻度は、高いリスクのデータ取扱いの場合には適応され、増加されるのが望ましい。同様に、重要なデータを含む取扱いの場合には、地理的に分離されたオフラインバックアップが特に考慮されるのが望ましい。	バックアップ・リカバリテスト報告書 CISOとの面談 調査 サンプル試験	32	1	7
T.1.4.3	CP	S	A	バックアップの義務	A) 申請者は、セキュリティインシデント発生時に、個人データの可用性及びアクセスを適時に復旧できる間隔で、かつ、少なくとも週1回、個人データのバックアップを実施しなければならない。 【AND】 B) バックアップは、次の要件を充足しなければならない。 b.1) 安全な場所に保管されていること	申請者は、バックアップからデータセットを復元する能力をバックアップし、定期的にテストするのが望ましい。 個人データの収集、取扱い若しくは共有、又は、その複数がまだ開始されていない場合、監査人は技術的及び組織的措置の効率を試験及び検証するために非個人データの使用を要求するのが望ましい。バックアップ方針には明確な保持方針を含めるのが望ましい。	調査 サンプル分析 バックアップ復元試験報告書	32.1.c	1	3
T.1.4.4	CP	G	A	サーバーデバイス及びシステムの定期的な更新	A) 申請者が次の措置を確実に実施するための手順、設定又は仕組みを整備しなければならない。 a.1) 個人データの取扱い又は保存に使用されるサーバー、デバイス及びシステムについて、関連するリスクに基づきアップデートのの必要性を評価すること a.2) 【AND】 これらに対して定期的にパッチを適用すること a.3) 【AND】 各プロバイダーによって発行される重要なセキュリティパッチを監視し、重要なセキュリティパッチが利用可能な場合には不当な遅滞なくインストールすること	これらの試験の文書を作成する必要がある。カバレッジメトリクスを適用する必要がある。 申請者は、更新（セキュリティ又はより一般的なもの）が生産に影響を与え、その結果データの可用性に影響を及ぼす場合に備えて、回帰テストを実施することを検討するのが望ましい。これは、取扱いに依存するデータ主体にとって高いリスクを意味する可能性がある。 データ保護を確保するには、これらのデータにアクセスするために使用されるネットワーククライアント（デバイス）のセキュリティも考慮する必要がある。 セキュリティの更新及びパッチは、最新の技術水準に準拠するのが望ましい。 リスクの特定及び評価は、基準G.6.2.4のリスクアセスメントに含まれることが期待される。	規則及び手順の文書レビュー（パッチ適用方針を含む） 試験報告書 調査 サンプル試験 DPO及び労働者との面談	32	1	3
T.1.4.5	CP	G	A	データの継続性	A) かかるリスクが存在する場合、個人データが記録保存又は取り扱われる物理的及び論理的環境（サーバー、デバイス及びコピーを含む）を保護し、データの継続性を確保するための保護措置が講じられなければならない。 【AND】 B) 当該措置は、次の条件を充足しなければならない。 b.1) 申請者が実施した文書化されたリスクアセスメントに基づくこと b.2) 【AND】データの可用性、完全性及び機密性に対する予見可能な脅威（火災、洪水、停電及びその他の関連するインシデントを含む）に対処していること b.3) 【AND】影響を受けたシステム及びデータの適時の復旧を支援するため、災害復旧及び事業	申請者は、個人データの物理的な保管に関連するリスクを評価に含めるのが望ましい。かかるリスクが存在する場合、データの破壊から保護し、データの継続性を確保するための措置を実施するのが望ましい。 かかる措置には、火災及び洪水から保護されたサーバーに個人データを記録保存することが含まれる。火災及び煙の検知器を設置しなければならない。電力供給の不足も考慮し、防止するのが望ましい。 これらの試験の文書を作成する必要がある。カバレッジメトリクスを適用する必要がある。 リスクの特定及び評価は、基準G.6.2.4のリスクアセスメントに含まれることが期待される。	火災及び洪水対策の調査 施設管理者との面談 サンプル試験	32	1	4
T.1.4.6	CP	G	A	ネットワークセキュリティ方針	A) 申請者は、次の要件を充足するネットワークセキュリティ方針を整備しなければならない。 a.1) 個人データが取り扱われ又は記録保存されるサーバー、デバイス及びシステムを特定し、それらに関連するリスクに基づき、ネットワークセキュリティ方針が必要となる対象を特定していること a.2) 【AND】当該リスクに対処するために必要なネットワークセキュリティコントロール（ファイアーウォール、侵入検知及び侵入防止メカニズム）を特定していること	ネットワークセキュリティ方針は、データ管理者（又は処理者）の個人データに関連するICTインフラストラクチャを保護するために策定されるのが望ましい。当該方針は、最新の技術水準に準拠したものであるのが望ましい。 リスクの特定及び評価は、基準G.6.2.4のリスクアセスメントに含まれることが期待される。	ファイアウォール設定のレビュー 調査 サンプル試験 CISOとの面談	25, 32	1	3
T.1.4.7	CP	G	A	アンチウイルスのアップデート	A) 評価対象において取扱いに使用されるサーバー、モバイル及び端末デバイスを保護するため、少なくともアンチウイルスアプリケーションを含むセキュリティソリューションが導入されていなければならない。 【AND】 B) 当該セキュリティソリューションが最新の状態に維持されることを確保にするための方針、手順又は仕組みを整備しなければならない	セキュリティソリューション（アンチウイルス及びアンチスパイウェアソリューションを含む）は、データ管理者又は処理者によって個人データの取扱いに使用されるサーバー及び端末デバイスを保護するために整備されるのが望ましい。これには、申請者の要員が使用するサーバー及びデバイスが含まれる。	調査 サンプル試験 アンチウイルスの最終更新日 更新ログのレビュー 侵害指標（IOC）レビュー	32	1	2

T.1.4.8	CP	G	A	ペンテスト又は同等のもの	【IF】申請者のリスクアセスメントにおいて、個人データの取扱いが自然人の権利及び自由にもたらすリスクに対処すべくセキュリティレベルを確保するため、ペネトレーションテスト（ペンテスト）又は同等のものが必要であると結論付けられた場合、【THEN】次のとおりとする。 A) 必要となるテストの性質、範囲及び頻度は、特定されたリスク及びセキュリティインシデントの監視に基づいて決定され、かつ、正当化されなければならない（T.1.4.9を参照）。 【AND】 B) 申請者は、次の措置を実施しなければならない。 a.1) データ侵害への曝露を評価するため、決定された頻度（少なくともセキュリティに影響を及ぼし得る重要な変更後） に従ってのテストを実施すること a.2) 【AND】当該テストの結果を文書化すること a.3) 【AND】当該テストの結果に対して対応が行われることを確保するための手順を整備していること	試験が必要か否かを判断するために、申請者は次の事項を考慮するのが望ましい。 - 取扱われるデータの種類及びその性質 - データ主体の種類 - データ取扱いの文脈 - 取扱いに使用される技術インフラストラクチャ - データ主体に対するリスク - 過去の試験結果 ペネトレーションテスト、敵対者シミュレーション又は自動化されたIS脆弱性スキャンなどの定期的なテストは、個人データ侵害につながる可能性のあるリスク及び弱点を特定するために定期的に実施されるのが望ましい。考慮すべき攻撃には、SQLインジェクション、スクリプト、クロスサイトスクリプティング、バッファオーバーフロー攻撃、中間者攻撃、リプレイ攻撃などが含まれる。情報システムがインターネットにさらされていない場合は、侵害を想定した演習及び敵対者シミュレーションなど、より広範な攻撃的セキュリティアプローチを考慮するのが望ましい。 リスクの特定及び評価は、基準G.6.2.4のリスクアセスメントに含まれることが期待される。	ペネトレーションテスト	*32*				
T.1.4.9	CP	G	A	侵入検知	A) 申請者は、セキュリティインシデントを検知、報告及び是正するための方針、規則、手順又は仕組みを整備しなければならない。	侵入及び攻撃などのセキュリティインシデントを監視することは、セキュリティの重要な要素である。かかるインシデントを記録するため、専用の組織的及び技術的措置を講じるのが望ましい。 侵入検知のリスクに対処するため、机上演習演習（TTX）、セキュリティインシデントシミュレーション、サイバーセキュリティインシデント対応計画（CSIRP）などの多様なアプローチを活用することができる。 セキュリティインシデント計画は、T.1.4.1の継続計画の一部になる可能性がある。	文書レビュー 調査 CISOとの面談 セキュリティインシデントシミュレーション報告書	*32*				

									1	4
									1	1
									0	0

基準の略語	
C	管理者にのみ適用される。
P	処理者にのみ適用される。
CP	管理者及び処理者の両方に適用される。
S	評価対象ごとに特定かつ明確である。
G	評価対象に共通する一般的なものである。
A	全てに対する必須要件である。
B	単純なデータ取扱いには必要とされないが、
E	例外。