インターネット接続系に主たる業務端末・システムを配置するB′モデルを採用する場合の追加監査項目を、次頁以降に示す。

項目			No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
3. 情報システム全体の強靭性の向上		技術的対策	1	○	**ⅰ）無害化処理** CISO又は統括情報セキュリティ責任者によって、LGWAN接続系にインターネット接続系からファイルを取り込む際に、以下の対策が実施されている。 ・ファイルからテキストのみを抽出 ・ファイルを画像PDFに変換 ・サニタイズ処理 ・インターネット接続系において内容を目視で確認するとともに、未知の不正プログラム検知及びその実行を防止する機能を有するソフトウェアで危険因子の有無を確認	□システム構成図 □システム設計書 □機器等の設定指示書 □運用手順書	監査資料のレビューとCISO又は統括情報セキュリティ責任者へのインタビューにより、LGWAN接続系にインターネット接続系からファイルを取り込む際に、ファイルからテキストのみを抽出、ファイルを画像PDFに変換、サニタイズ処理、インターネット接続系において内容を目視で確認するとともに、未知の不正プログラム検知及びその実行を防止する機能を有するソフトウェアで危険因子の有無を確認するなどの対策が実施されているか確かめる。	3.(3)	－	・無害化の処理方法が複数ある場合は、それぞれの方法について実施状況を確認する。
			2	○	**ⅱ）LGWAN接続系の画面転送** CISO又は統括情報セキュリティ責任者によって、以下の対応が全て実施されている。 ・インターネット接続系の業務端末からLGWAN接続系のサーバや端末を利用する場合は、仮想化されたリモートデスクトップ形式で接続されている。 ・LGWAN接続系からインターネット接続系へのデータ転送(クリップボートのコピー&ペースト等)が禁止されている。ただし、LGWANメールやLGWANからの取り込み、業務で必要となるデータの転送については、中継サーバやファイアウォール等を設置し、通信ポート、IPアドレス、MACアドレス等で通信先を限定することで可能とされている。	□システム構成図 □システム設計書 □機器等の設定指示書 □運用手順書	監査資料のレビューとCISO又は統括情報セキュリティ責任者へのインタビューにより、インターネット接続系の業務端末からLGWAN接続系のサーバや端末を利用する場合は、仮想化されたリモートデスクトップ形式で接続されていることを確認する。さらに、LGWAN接続系からインターネット接続系へのデータ転送(クリップボートのコピー&ペースト等)が原則禁止されており、通信先を限定されたLGWANメールやLGWANからの取り込み、業務で必要となるデータの転送のみが許可されていることを確かめる。	3.(3)	－	

項目			No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
			3	○	**ⅲ）未知の不正プログラム対策（エンドポイント対策）** 統括情報セキュリティ責任者及び情報システム管理者により、パターンマッチング型の検知に加えて、セキュリティ専門家やSOC等のマネージドサービスの運用によって、以下の対応が全て実施されている。 ・端末等のエンドポイントにおけるソフトウェア等の動作を監視し、未知及び既知のマルウェア等による悪意ある活動を示す異常な挙動を監視・検出・特定する。 ・異常な挙動を検出した際にプロセスを停止、ネットワークからの論理的な隔離を行う。 ・インシデント発生時に発生要因の詳細な調査を実施する。	□システム構成図 □システム設計書 □機器等の設定指示書 □運用手順書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、パターンマッチング型の検知に加えて、セキュリティ専門家やSOC等のマネージドサービスの運用によって、端末等のエンドポイントにおけるソフトウェア等の動作の監視がされていること、未知及び既知のマルウェア等の異常な挙動を監視・検知・特定ができるようになっていること並びに異常な挙動を検出した際のプロセスの停止、異常な挙動が検知された端末等に対してネットワークからの隔離ができるようになっていること及びインシデント発生要因の詳細な調査が実施できるようになっていることを確かめる。	3.(3)	―	
			4	○	**ⅳ）業務システムログ管理** 統括情報セキュリティ責任者及び情報システム管理者によって、インターネット接続系の業務システムのログの収集、分析、保管が実施されている。	□システム運用基準 □ログ □システム稼動記録 □障害時のシステム出力ログ	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、インターネット接続系の業務システムに関するログが適切に収集、分析、保管されていることを確かめる。	3.(3)	―	・ログの取得及び保管についてはNo.159～162も関連する項目であることから参考にすること。
			5	○	**ⅴ）情報資産単位でのアクセス制御** 統括情報セキュリティ責任者又は情報システム管理者によって、アクセス制御に関わる方針及び基準が定められ、文書化されており、基準に従ってアクセス制御されている。文書を管理するサーバ等は課室単位でのアクセス制御を実施している。	□アクセス制御方針 □アクセス管理基準 □システム設計書 □機器等の設定指示書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、情報資産の機密性レベルに応じて業務システム単位でのアクセス制御が行われていること、文書を管理するサーバ等で課室単位でのアクセス制御が実施されていることを確かめる。	3.(3)	―	・アクセス制御についてはNo.221～247も関連する項目であることから参考にすること。

項目			No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
			6	○	**ⅵ）脆弱性管理** 統括情報セキュリティ責任者及び情報システム管理者によって、OSやソフトウェアのバージョンなどが漏れなく資産管理され、脆弱性の所在が効率的に把握されており、深刻度に応じて修正プログラムを適用し、ゼロデイ攻撃等のソフトウェアの脆弱性を狙った攻撃に迅速に対応されている。	□情報セキュリティ関連情報の通知記録 □脆弱性関連情報の通知記録 □サイバー攻撃情報やインシデント情報の通知記録 □脆弱性対応計画	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、OSやソフトウェアのバージョンなどが漏れなく資産管理され、脆弱性の所在が効率的に把握されており、深刻度に応じて修正プログラムを適用し、ゼロデイ攻撃等のソフトウェアの脆弱性を狙った攻撃に迅速に対応できるようになっているか確かめる。	3.(3)	―	・脆弱性管理についてはNo.320～324も関連する項目であることから参考にすること。
		組織的・人的対策	7	○	**ⅰ）セキュリティの継続的な検知・モニタリング体制の整備** 職員等の標的型攻撃訓練や研修等の受講状況や結果を確認し、セキュリティ対策の浸透状況や効果が測定されており、その結果がフィードバックされている。	□研修・訓練実施基準 □研修・訓練実施計画 □研修・訓練受講記録 □研修・訓練結果報告書 □研修・訓練に関するアンケート	監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、標的型攻撃訓練や研修等の受講状況や結果を確認し、セキュリティ対策の浸透状況や効果が測定されており、その結果がフィードバックされているか確かめる。	3.(3)	―	・標的型訓練についても計画に含めることが望ましい。
			8	○	**ⅰ）住民に関する情報をインターネット接続系に保存させない規定の整備** 住民に関する情報資産は特に重要な情報資産であるため、インターネット接続系のファイルサーバに保存させないことや、一時的に保存したとしても直ちに削除すること等が規定として定められており、その規定に従い、運用がされている。	□情報資産管理基準 □実施手順書	監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、住民情報に関する情報の取扱いについて文書化され、運用されており、実際に住民情報に関する情報がインターネット接続系のファイルサーバ等に保存されていないことを確かめる。	3.(3)	―	
			9	○	**ⅲ）情報セキュリティ研修、標的型攻撃訓練、セキュリティインシデント訓練の受講** 職員等が情報セキュリティ研修、標的型攻撃訓練を年1回以上受講しており、情報システム管理者、情報システム担当者がセキュリティインシデントが発生した場合の訓練を年1回以上受講している。	□研修・訓練実施基準 □研修・訓練実施計画 □研修・訓練受講記録 □研修・訓練結果報告書 □研修・訓練に関するアンケート	監査資料のレビューと統括情報セキュリティ責任者及び職員等へのインタビューにより、職員等が情報セキュリティ研修、標的型攻撃訓練を年1回以上受講していること及び情報システム管理者、情報システム担当者がセキュリティインシデントが発生した場合の訓練を年1回以上受講していることを確かめる。	3.(3)	―	

項目			No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
			10	○	**ⅳ）情報セキュリティ研修計画** 職員等が毎年度最低1回は情報セキュリティ研修を受講できるように計画されている。	□研修・訓練実施基準 □研修・訓練実施計画	監査資料のレビュー又は統括情報セキュリティ責任者へのインタビューにより、研修計画において、職員等が毎年度最低1回は情報セキュリティ研修を受講できるように計画されているか確かめる。	5.2.(2)②	6.3	・αモデルにおいては推奨事項だが、β・β’モデルにおいては必須事項となる。
			11	○	**Ⅴ）実践的サイバー防御演習（CYDER）の確実な受講** CISOによって、実践的サイバー防御演習（CYDER）を受講しなければならないことが定められ、受講計画が策定されており、また、受講計画に従い、職員等が受講してい る	□研修・訓練実施計画 □研修・訓練受講記録 □研修・訓練結果報告書	監査資料のレビュー又は統括情報セキュリティ責任者へのインタビューにより、実践的サイバー防御演習（CYDER）の受講計画について文書化され、正式に承認されているか確かめる。 また、職員等が適切に受講しており、その受講記録が取られていることを確かめる。	3.(3)	―	
			12	○	**Ⅵ）演習等を通じたサイバー攻撃情報やインシデント等への対策情報共有** 職員等が以下の演習やそれに準ずる演習を受講している。 ・インシデント対応訓練（基礎/高度） ・分野横断的演習	□研修・訓練実施計画 □研修・訓練受講記録 □研修・訓練結果報告書	監査資料のレビュー又は統括情報セキュリティ責任者へのインタビューにより、職員等がインシデント対応訓練（基礎/高度）、分野横断的演習又はそれに準ずる演習を受講しているか確かめる。	3.(3)	―	
			13	○	**Ⅶ）自治体情報セキュリティポリシーガイドライン等の見直しを踏まえた情報セキュリティポリシーの見直し** 自治体情報セキュリティポリシーガイドライン等の見直し踏まえて、適時適切に情報セキュリティポリシーの見直しがされている。	□情報セキュリティポリシー	監査資料のレビュー又は統括情報セキュリティ責任者へのインタビューにより、情報セキュリティポリシーが自治体情報セキュリティポリシーガイドライン等の見直しを踏まえて、適時適切に見直しがされていることを確かめる。	9.3	―	・情報セキュリティポリシーの策定・遵守については、No.334～342、No.403～413、No.420～421も関連する項目であることから参考にすること。

※α’・β・β’モデルを採用する場合、「地方公共団体における情報セキュリティポリシーに関するガイドライン」対策基準（例文）記載の組織的・人的対策を確実に実施する必要があるため、以下の監査項目を再掲

項目			No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
1. 組織体制		(3)CSIRTの設置・役割	4	○	**ⅲ）CSIRTの設置・役割の明確化** CSIRTが設置され、部局の情報セキュリティインシデントについてCISOへの報告がされている。また、CISOによって、CSIRT及び構成する要員の役割が明確化されている。	□情報セキュリティポリシー □CSIRT設置要綱	監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、CSIRTが設置されており、規定された役割に応じて情報セキュリティインシデントのとりまとめやCISOへの報告、報道機関等への通知、関係機関との情報共有等を行う統一的な窓口が設置されているか確かめる。また、監査資料のレビューとCISO又は構成要員へのインタビューにより、CSIRTの要員構成、役割などが明確化されており、要員はそれぞれの役割を理解しているか確かめる。	1.(9)	5.5 5.6 5.24 5.25 5.26 6.8	
5. 人的セキュリティ	5.1. 職員等の遵守事項	(1) 職員等の遵守事項① 情報セキュリティポリシー等の遵守	85	○	**ⅰ）情報セキュリティポリシー等遵守の明記** 統括情報セキュリティ責任者又は情報セキュリティ責任者によって、職員等が情報セキュリティポリシー及び実施手順を遵守しなければならないことが定められ、文書化されている。	□情報セキュリティポリシー □職員等への周知記録	監査資料のレビューと統括情報セキュリティ責任者又は情報セキュリティ責任者へのインタビューにより、職員等の情報セキュリティポリシー及び実施手順の遵守や、情報セキュリティ対策について不明な点及び遵守が困難な点等がある場合に職員等がとるべき手順について文書化され、正式に承認されているか確かめる。また、承認された文書が職員等に周知されているか確かめる。	5.1.(1)①	5.1	
			86	○	**ⅱ）情報セキュリティポリシー等の遵守** 職員等は、情報セキュリティポリシー及び実施手順を遵守するとともに、情報セキュリティ対策について不明な点や遵守が困難な点等がある場合、速やかに情報セキュリティ管理者に相談し、指示を仰げる体制になっている。	□情報セキュリティポリシー □実施手順書	監査資料のレビューと情報セキュリティ管理者及び職員等へのインタビューにより、情報セキュリティポリシー及び実施手順の遵守状況を確かめる。また、情報セキュリティ対策について不明な点及び遵守が困難な点等がある場合、職員等が速やかに情報セキュリティ管理者に相談し、指示を仰げる体制が整備されているか確かめる。必要に応じて、職員等へのアンケート調査を実施し、周知状況を確かめる。	5.1.(1)①	5.1	・職員等の情報セキュリティポリシーの遵守状況の確認及び対処については、No.334～342も関連する項目であることから参考にすること。
		(1) 職員等の遵守事項② 業務以外の目的での使用の禁止	88	○	**ⅱ）情報資産等の業務以外の目的での使用禁止** 職員等による業務以外の目的での情報資産の持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスは行われていない。	□端末ログ □電子メール送受信ログ □ファイアウォールログ	監査資料のレビューと情報システム管理者及び職員等へのインタビューにより、業務以外の目的での情報資産の持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスが行われていないか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	5.1.(1)②	－	

項目			No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
		(1) 職員等の遵守事項③ モバイル端末や電磁的記録媒体の持ち出し及び外部における情報処理作業の制限	90	○	**ⅱ）情報資産等の外部持出制限** 職員等がモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合、情報セキュリティ管理者により許可を得ている。	□端末等持出・持込基準/手続 □庁外での情報処理作業基準/手続 □端末等持出・持込申請書/承認書	監査資料のレビューと情報セキュリティ管理者及び職員等へのインタビューにより、職員等がモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合、情報セキュリティ管理者から許可を得ているか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	5.1.(1)③ (イ)	8.1 6.7 7.9	・紛失、盗難による情報漏えいを防止するため、暗号化等の適切な処置をして持出すことが望ましい。
			91	○	**ⅲ）外部での情報処理業務の制限** 職員等が外部で情報処理作業を行う場合は、情報セキュリティ管理者による許可を得ている。	□庁外での情報処理作業基準/手続 □庁外作業申請書/承認書	監査資料のレビューと情報セキュリティ管理者及び職員等へのインタビューにより、職員等が外部で情報処理作業を行う場合、情報セキュリティ管理者から許可を得ているか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	5.1.(1)③ (ウ)	8.1 6.7 7.9	・情報漏えい事故を防止するため、業務終了後は速やかに勤務地に情報資産を返却することが望ましい。
		(1) 職員等の遵守事項④ 支給以外のパソコン、モバイル端末及び電磁的記録媒体の業務利用	92	○	**ⅰ）支給以外のパソコン、モバイル端末及び電磁的記録媒体の業務利用基準及び手続** 統括情報セキュリティ責任者又は情報セキュリティ責任者によって、職員等が業務上支給以外のパソコン、モバイル端末及び電磁的記録媒体を利用する場合の基準及び手続について定められ、文書化されている。	□端末等持出・持込基準/手続 □支給以外のパソコン等使用申請書/承認書	監査資料のレビューと統括情報セキュリティ責任者又は情報セキュリティ責任者へのインタビューにより、支給以外のパソコン、モバイル端末及び電磁的記録媒体利用手順が文書化され、正式に承認されているか確かめる。	5.1.(1)④	5.10 7.8	
			93	○	**ⅱ）支給以外のパソコン、モバイル端末及び電磁的記録媒体の利用制限** 職員等が情報処理作業を行う際に支給以外のパソコン、モバイル端末及び電磁的記録媒体を用いる場合、当該端末の業務利用の可否判断をCISOが行った後に、業務上必要な場合は、統括情報セキュリティ責任者の定める実施手順に従い、情報セキュリティ管理者による許可を得ている。また、機密性の高い情報資産の支給以外のパソコン、モバイル端末及び電磁的記録媒体による情報処理作業は行われていない。	□支給以外のパソコン等使用申請書/承認書 □支給以外のパソコン等使用基準/実施手順書	監査資料のレビューと情報セキュリティ管理者及び職員等へのインタビューにより、職員等が情報処理作業を行う際に支給以外のパソコン、モバイル端末及び電磁的記録媒体を用いる場合、情報セキュリティ管理者の許可を得ているか確かめる。また、端末のウイルスチェックが行われていることや、端末ロック機能及び遠隔消去機能が利用できること、機密性3の情報資産の情報処理作業を行っていないこと、支給以外の端末のセキュリティに関する教育を受けた者のみが利用しているか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。また、手順書に基づいて許可や利用がされているか確かめる。	5.1.(1)④	8.1 6.7 7.8 7.9	
			94	○	**ⅲ）支給以外のパソコン、モバイル端末及び電磁的記録媒体の庁内ネットワーク接続** 職員等が支給以外のパソコン、モバイル端末及び電磁的記録媒体を庁内ネットワークに接続することを許可する場合、統括情報セキュリティ責任者又は情報セキュリティ責任者によって、情報漏えい対策が講じられている。	□庁外での情報処理作業基準/手続 □支給以外のパソコン等使用申請書/承認書 □支給以外のパソコン等使用基準/実施手順書	監査資料のレビューと情報セキュリティ管理者及び職員等へのインタビューにより、支給以外のパソコン、モバイル端末及び電磁的記録媒体を庁内ネットワークに接続することを許可する場合は、シンクライアント環境やセキュアブラウザの使用、ファイル暗号化機能を持つアプリケーションでの接続のみを許可する等の情報漏えい対策が講じられているか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	5.1.(1)④	8.20 8.21	

項目	No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
(1) 職員等の遵守事項⑤ 持ち出し及び持ち込みの記録	96	○	**ⅱ）端末等の持出・持込記録の作成** 情報セキュリティ管理者によって、端末等の持ち出し及び持ち込みの記録が作成され、保管されている。	□端末等持出・持込基準/手続 □端末等持出・持込申請書/承認書	監査資料のレビューと情報セキュリティ管理者へのインタビューにより、端末等の持ち出し及び持ち込みの記録が作成され、保管されているか確かめる。	5.1.(1)⑤	7.1	・記録を定期的に点検し、紛失、盗難が発生していないか確認することが望ましい。
(1) 職員等の遵守事項⑦ 机上の端末等の管理	100	○	**ⅱ）机上の端末等の取扱** 離席時には、パソコン、モバイル端末、電磁的記録媒体、文書等の第三者使用又は情報セキュリティ管理者の許可なく情報が閲覧されることを防止するための適切な措置が講じられている。	□クリアデスク・クリアスクリーン基準	監査資料のレビューと情報セキュリティ管理者及び職員等へのインタビュー、執務室の視察により、パソコン、モバイル端末の画面ロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管といった、情報資産の第三者使用又は情報セキュリティ管理者の許可なく情報が閲覧されることを防止するための適切な措置が講じられているか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	5.1.(1)⑦	7.7	
(3) 情報セキュリティポリシー等の掲示	108	○	**ⅱ）情報セキュリティポリシー等の掲示** 情報セキュリティ管理者によって、職員等が常に最新の情報セキュリティポリシー及び実施手順を閲覧できるように掲示されている。	□職員等への周知記録	監査資料のレビューと情報セキュリティ管理者へのインタビュー及び執務室の視察により、職員等が常に最新の情報セキュリティポリシー及び実施手順を閲覧できるよう、イントラネット等に掲示されているか確かめる。	5.1.(3)	5.1	
(4) 外部委託事業者に対する説明	110	○	**ⅱ）委託事業者に対する情報セキュリティポリシー等遵守の説明** ネットワーク及び情報システムの開発・保守等を委託事業者に発注する場合、情報セキュリティ管理者によって、情報セキュリティポリシー等のうち、委託事業者及び再委託事業者が守るべき内容の遵守及びその機密事項が説明されている。	□業務委託契約書 □委託管理基準	監査資料のレビューと情報セキュリティ管理者へのインタビューにより、ネットワーク及び情報システムの開発・保守等を発注する委託事業者及び再委託事業者に対して、情報セキュリティポリシー等のうち委託事業者等が守るべき内容の遵守及びその機密事項が説明されているか確かめる。	5.1.(4)	5.19 5.20	・再委託は原則禁止であるが、例外的に再委託を認める場合には、再委託事業者における情報セキュリティ対策が十分取られており、委託事業者と同等の水準であることを確認した上で許可しなければならない。 ・委託事業者に対して、契約の遵守等について必要に応じ立ち入り検査を実施すること。 ・委託に関する事項ついては、No.337～366も関連する項目であることから参考にすること。

項目			No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
	5.2. 研修・訓練	(1) 情報セキュリティに関する研修・訓練	112	○	**ⅱ）情報セキュリティ研修・訓練の実施** CISOによって、定期的にセキュリティに関する研修・訓練が実施されている。	□研修・訓練実施基準 □研修実施報告書 □訓練実施報告書	監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、定期的に情報セキュリティに関する研修・訓練が実施されているか確かめる。	5.2.(1)	6.3	
	5.3. 情報セキュリティインシデントの報告		123	○	**ⅰ）情報セキュリティインシデントの報告手順** 統括情報セキュリティ責任者によって、情報セキュリティインシデントを認知した場合の報告手順が定められ、文書化されている。	□情報セキュリティインシデント報告手順書	監査資料のレビューと統括情報セキュリティ責任者又は情報セキュリティ責任者へのインタビューにより、職員等が情報セキュリティインシデントを認知した場合、又は住民等外部から情報セキュリティインシデントの報告を受けた場合の報告ルート及びその方法が文書化され、正式に承認されているか確かめる。	5.3.(1)～(3)	6.8	・報告ルートは、団体の意思決定ルートと整合していることが重要である。
		(1) 庁内での情報セキュリティインシデントの報告	124	○	**ⅰ）庁内での情報セキュリティインシデントの報告** 庁内で情報セキュリティインシデントが認知された場合、報告手順に従って関係者に報告されている。	□情報セキュリティインシデント報告手順書 □情報セキュリティインシデント報告書	監査資料のレビューと統括情報セキュリティ責任者又は情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者、職員等へのインタビューにより、報告手順に従って遅滞なく報告されているか確かめる。また、個人情報・特定個人情報の漏えい等が発生していた場合、必要に応じて個人情報保護委員会へ報告されていることを確かめる。	5.3.(1)	6.8	
	5.4. ID及びパスワード等の管理	(1) ICカード等の取扱い	130	○	**ⅲ）認証用ICカード等の放置禁止** 認証用ICカード等を業務上必要としないときは、カードリーダーやパソコン等の端末のスロット等から抜かれている。	□ICカード等取扱基準	監査資料のレビューと情報システム管理者及び職員等へのインタビュー並びに執務室の視察により、業務上不要な場合にカードリーダーやパソコン等の端末のスロット等から認証用のICカードやUSBトークンが抜かれているか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	5.4.(1)① (イ)	5.16 5.18	
			131	○	**ⅳ）認証用ICカード等の紛失時手続** 認証用ICカード等が紛失した場合は、速やかに統括情報セキュリティ責任者及び情報システム管理者に通報され、指示に従わせている。	□ICカード等取扱基準 □ICカード紛失届書	監査資料のレビューと統括情報セキュリティ責任者及び情報システム管理者へのインタビューにより、認証用のICカードやUSBトークンが紛失した場合は、速やかに統括情報セキュリティ責任者及び情報システム管理者に通報され、指示に従わせているか確かめる。	5.4.(1)① (ウ)	5.16 5.18	
			132	○	**ⅴ）認証用ICカード等の紛失時対応** 認証用ICカード等の紛失連絡があった場合、統括情報セキュリティ責任者及び情報システム管理者によって、当該ICカード等の不正使用を防止する対応がとられている。	□ICカード等取扱基準 □ICカード等管理台帳	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、紛失した認証用のICカードやUSBトークンを使用したアクセス等が速やかに停止されているか確かめる。	5.4.(1)②	5.16 5.18	

項目			No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
			133	○	**ⅵ）認証用ICカード等の回収及び廃棄** ICカード等を切り替える場合、統括情報セキュリティ責任者及び情報システム管理者によって、切替え前のカードが回収され、不正使用されないような措置が講じられている。	□ICカード等取扱基準 □ICカード等管理台帳	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、認証用のICカードやUSBトークンを切り替える場合に切替え前のICカードやUSBトークンが回収され、破砕するなど復元不可能な処理を行った上で廃棄されているか確かめる。	5.4.(1)③	5.16 5.18	・回収時の個数を確認し、紛失・盗難が発生していないか確実に確認することが望ましい。
		(3) パスワードの取扱い	138	○	**ⅱ）パスワードの取扱い** 職員等のパスワードは当該本人以外に知られないように取扱われている。	□パスワード管理基準	監査資料のレビューと情報システム管理者及び職員等へのインタビューにより、職員等のパスワードについて照会等に応じたり、他人が容易に想像できるような文字列に設定したりしないように取り扱われているか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	5.4.(3)①～③	5.17	内閣サイバーセキュリティセンター(NISC)のハンドブックでは、「ログイン用パスワード」は、英大文字(26種類)小文字(26種類)＋数字(10種類)＋記号(26種類)の計88種類の文字をランダムに使って、10桁以上を安全圏として推奨している。
			139	○	**ⅲ）パスワードの不正使用防止** パスワードが流出したおそれがある場合、不正使用されない措置が講じられている。	□パスワード管理基準	監査資料のレビューと情報システム管理者及び職員等へのインタビューにより、パスワードが流出したおそれがある場合、速やかに情報セキュリティ管理者に報告され、パスワードが変更されているか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	5.4.(3)④	5.17	
			142	○	**ⅵ）パスワード記憶機能の利用禁止** サーバ、ネットワーク機器及びパソコン等の端末にパスワードが記憶されていない。	□パスワード管理基準	監査資料のレビューと情報システム管理者及び職員等へのインタビュー、執務室の視察により、サーバ、ネットワーク機器及びパソコン等の端末にパスワードが記憶されていないか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	5.4.(3)⑦	5.17	