No.	監査項目	監査資料の例	監査実施方法	箕面市情報セキュリティ対策基準の番号	留意事項
1	**ⅱ）機器の取付け** 情報システム管理者によって、サーバ等の機器の取付けを行う場合、火災、水害、埃、振動、温度等の影響を可能な限り排除した場所に設置し、容易に取り外せないように固定するなどの対策が講じられている。	□機器設置基準/手続 □建物フロアレイアウト図 □管理区域（情報システム室等）のレイアウト図 □機器設置記録 □情報資産管理台帳	監査資料のレビューと情報システム管理者へのインタビュー及び管理区域の視察により、サーバ等の機器が設置されているか確かめる。	4.1.(1)	・情報資産管理台帳などに、機器の設置場所や設置状態などを明記しておくことが望ましい。
2	**ⅲ）サーバ障害対策基準** 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、メインサーバに障害が発生した場合の対策基準及び実施手順が定められ、文書化されている。	□サーバ障害対策基準 □サーバ障害対応実施手順書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、サーバに障害が発生した場合の対策基準及び実施手順が文書化され、正式に承認されているか確かめる。	4.1.(2)②	
3	**ⅱ）サーバ等の機器の定期保守** 情報システム管理者によって、サーバ等の機器の定期保守が実施されている。	□機器保守・修理基準/手続 □保守機器管理表 □保守体制図 □作業報告書 □障害報告書 □機器保守点検記録	監査資料のレビューと情報システム管理者へのインタビューにより、保守対象機器、保守実施時期、保守内容、保守担当が明確になっているか、保守が適切に行われているか確かめる。また、実際にサーバ等機器の障害が発生している場合は、保守に問題がなかったか確かめる。	4.1.(5)①	
4	**ⅲ）電磁的記録媒体を内蔵する機器の修理** 電磁的記録媒体を内蔵する機器を外部の事業者に修理させる場合、情報システム管理者によって、情報が漏えいしない対策が講じられている。	□機器保守・修理基準/手続 □保守機器管理表 □保守体制図 □作業報告書 □機密保持契約書	監査資料のレビューと情報システム管理者へのインタビューにより、電磁的記録媒体を内蔵する機器を事業者に修理させる場合にデータを消去した状態で行わせているか確かめる。データを消去できない場合は、修理を委託する事業者との間で守秘義務契約を締結し、秘密保持体制等を確認しているか確かめる。	4.1.(5)②	
5	**ⅲ）管理区域への立ち入り制限機能** 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、管理区域への許可されていない立ち入りを防止するための対策が講じられている。	□建物フロアレイアウト図 □敷地図面 □管理区域（情報システム室等）のレイアウト図	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及び管理区域の視察により、外部へ通じるドアを必要最低限とし、鍵、監視機能、警報装置等が設けられているか確かめる。	4.2.(1)②	・外部へ通じるドアを必要最小限とするにあたり、消防法に違反しないよう留意する必要がある。
6	**ⅱ）管理区域への入退室制限** 情報システム管理者によって、管理区域への入退室が制限され管理されている。	□管理区域入退室基準/手続 □管理区域入退室記録 □認証用カード管理記録	監査資料のレビューと情報システム管理者へのインタビュー及び管理区域の視察により、入退室管理基準に従って管理区域への入退室を制限しているか確かめる。 また、ICカード、指紋認証等の生体認証や入退室管理簿への記録による入退室管理を行っているか、及びICカード等の認証用カードが管理・保管されているか確かめる。	4.2.(2)①	・ 入退室手続に業者名、訪問者名等の個人情報を記述しているような場合は紛失、覗き見等が生じないように管理する。 ・ICカードや指紋等生体認証の入退管理システムを導入した場合、故障等により入退に支障が生じるのを未然に防止するため、定期的に保守点検することが望ましい。 ・必要以上の入退室や通常時間外の入退室など、不信な入退室を確認する必要がある。
7	**ⅷ）通信回線のセキュリティ対策** 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、伝送途上の情報が破壊、盗聴、改ざん、消去等が生じないよう、通信回線として利用する回線に対策が実施されている。	□ネットワーク管理基準	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、伝送途上の情報が破壊、盗聴、改ざん、消去等が生じないように保護されているか確かめる。また、適切なアクセス制御が実施されているか、及び業務遂行に必要な回線が確保されているか確かめる。	4.3.⑤	・通信回線の断線、通信機器の故障のための装置、ケーブル類の予備在庫をもつことが望ましい。 ・可用性の観点から必要な通信回線を確保することが望ましい。

8	**ⅳ）ログイン認証設定** 情報システム管理者によって、情報システムへのログイン時に認証情報を入力をするよう設定されている。	□パソコン等管理基準	監査資料のレビューと情報システム管理者へのインタビュー及び執務室等のパソコン等のサンプリング確認により、パソコン等にログインする時に認証情報を入力をするよう設定されているか確かめる。	4.4.②	・パスワードの管理及び取扱いについては、No.135～141、238～240も関連する項目であることから参考にすること。 ・ログイン時のシステム設定については、No.237も関連する項目であることから参考にすること。
9	**ⅵ）多要素認証の利用** 情報システム管理者によって、多要素認証が行われている。	□パソコン等管理基準	監査資料のレビューと情報システム管理者へのインタビュー及び執務室等のパソコン等のサンプリング確認により、多要素認証が行われているか確かめる。	4.4.③	・多要素認証はマイナンバー利用事務系では必須事項、LGWAN接続系では推奨事項とする。
10	**ⅷ）電磁的記録媒体の暗号化** 情報システム管理者によって、データ暗号化機能を備える電磁的記録媒体が利用されている。	□パソコン等管理基準	監査資料のレビューと情報システム管理者へのインタビュー及び執務室等の電磁的記録媒体のサンプリング確認により、データ暗号化機能を備える電磁的記録媒体が利用されているか確かめる。		
11	**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)	・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。
12	**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)	・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。 ・業務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。
13	**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り扱われている。	□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	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。
14	**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	

15	**ⅱ）バックアップの実施** 情報システム管理者によって、ファイルサーバ等に記録された情報について定期的なバックアップが実施され、バックアップ媒体が適切に保管されている。	□バックアップ基準 □バックアップ手順書 □バックアップ実施記録 □リストア手順書 □リストアテスト記録	監査資料のレビューと情報システム管理者へのインタビュー及び管理区域あるいは執務室の視察により、ファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、必要に応じて定期的にバックアップが実施されているか確かめる。また、バックアップ処理の成否の確認、災害等による同時被災を回避するためバックアップデータの別施設等への保管、リストアテストによる検証が行われているか確かめる。	6.1.(2)	・サーバの冗長化については、No.31～34も関連する項目であることから参考にすること。
16	**ⅱ）ログ等の取得及び保存** 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、各種ログ及び情報セキュリティの確保に必要な記録が取得され、保存されている。	□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、各種ログ及び情報セキュリティの確保に必要な記録が取得され、一定期間保存されているか確かめる。	6.1.(6)①	
17	**ⅳ）ログ等の点検、分析** 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、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意のある第三者からの不正侵入、不正操作等の有無について点検又は分析を行っている。	□システム運用基準	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、悪意のある第三者による不正なアクセスや不正操作が行われていないか確認するために、ログ等を定期的に点検、分析を行っているか確かめる。	6.1.(6)③	
18	**ⅱ）障害記録の保存** 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、障害記録が適正に保存されている。	□障害対応基準 □障害報告書 □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、職員等からのシステム障害の報告、システム障害に対する処理結果又は問題が記録され、適正に保存されているか確かめる。	6.1.(7)	
19	**ⅱ）ファイアウォール、ルータ等の設定** 統括情報セキュリティ責任者によって、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等が設定されている。	□ネットワーク設定基準 □ネットワーク構成図	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、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しているか確かめる。	6.1.(8)①	・設定の不整合とは、例えば、通信機器間で通信経路の設定や通信パケットの通過ルールに齟齬がある等の場合をいう。
20	**ⅲ）ネットワークのアクセス制御** 統括情報セキュリティ責任者によって、ネットワークに適切なアクセス制御が施されている。	□ネットワーク設定基準	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、不正アクセスを防止するため、ネットワークに適切なアクセス制御を施しているか確かめる。	6.1.(8)②	
21	**ⅱ）外部ネットワーク接続の申請及び許可** 情報システム管理者が所管するネットワークを外部ネットワークと接続する場合、CISO及び統括情報セキュリティ責任者から許可を得ている。	□外部ネットワーク接続基準 □外部ネットワーク接続手続 □外部ネットワーク接続申請書/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システム管理者へのインタビューにより、情報システム管理者が所管するネットワークを外部ネットワークと接続する場合、CISO及び統括情報セキュリティ責任者から許可を得ているか確かめる。	6.1.(10)①	
22	**ⅲ）外部ネットワークの確認** 情報システム管理者によって、所管するネットワークと外部ネットワークを接続しようとする場合には、接続しようとする外部ネットワークが調査され、庁内ネットワークや情報資産に影響が生じないことが確認されている。	□外部ネットワーク接続基準 □外部ネットワーク接続手続 □外部ネットワーク調査結果	監査資料のレビューと情報システム管理者へのインタビューにより、接続しようとする外部ネットワークのネットワーク構成、機器構成、セキュリティ技術等が調査され、庁内の全てのネットワーク、情報資産に影響が生じないことが確認されているか確かめる。	6.1.(10)②	・外部ネットワークの調査とは、例えば、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を調査することをいう。
23	**ⅴ）ファイアウォール等の設置** ウェブサーバ等をインターネットに公開している場合、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、外部ネットワークとの境界にファイアウォール等が設置されている。	□ネットワーク管理基準 □通信回線敷設図 □結線図	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、ウェブサーバ等をインターネットに公開する場合、庁内ネットワークへの侵入を防御するため、外部ネットワークとの境界にファイアウォール等が設置されたうえで接続されているか確かめる。	6.1.(10)④	
24	**ⅵ）外部ネットワークの遮断** 接続した外部ネットワークのセキュリティに問題が認められる場合、情報システム管理者によって、統括情報セキュリティ責任者の判断に従い、速やかに当該外部ネットワークが物理的に遮断されている。	□外部ネットワーク接続基準 □外部ネットワーク接続手続 □障害報告書	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システム管理者へのインタビューにより、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、統括情報セキュリティ責任者の判断に従い、速やかに当該外部ネットワークが物理的に遮断されているか確かめる。	6.1.(10)⑤	

25	**ⅱ）無線LAN利用時の暗号化及び認証技術の使用** 無線LANを利用する場合、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、暗号化及び認証技術が使用されている。	□ネットワーク管理基準 □ネットワーク設計書	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、無線LANを利用する場合には解読が困難な暗号化及び認証技術が使用され、アクセスポイントへの不正な接続が防御されているか確かめる。	6.1.(13)①	
26	**ⅲ）機密性の高い情報を扱うネットワークの暗号化等の対策** 統括情報セキュリティ責任者によって、機密性の高い情報を扱うネットワークには暗号化等の措置が講じられている。	□ネットワーク管理基準 □ネットワーク設計書	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、情報の盗聴等を防ぐため、機密性の高い情報を扱うネットワークには暗号化等の措置が講じられているか確かめる。	6.1.(13)②	
27	**ⅰ）アクセス制御に関わる方針及び基準** 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、文書化されている。	□アクセス制御方針 □アクセス管理基準	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、所管するネットワーク又は情報システムの重要度に応じたアクセス制御方針や、業務上の必要性や権限に応じた許可範囲等のアクセス管理基準が文書化され、正式に承認されているか確かめる。	6.2.(1)①	・開発、運用等を委託しており、重要な情報資産へのアクセスを許可している場合は、アクセス制御方針やアクセス管理基準等に委託に関するアクセス制御の事項が記述されていることが望ましい。
28	**ⅰ）利用者IDの取扱いに関わる手続** 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、利用者IDの登録、変更、抹消等の取扱いに関わる手続が定められ、文書化されている。	□利用者ID取扱手続 □利用者ID登録・変更・抹消申請書 □利用者ID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、利用者IDの登録、変更、抹消等の取扱いに関わる手続が文書化され、正式に承認されているか確かめる。	6.2.(1)② (ア)	
29	**ⅱ）利用者IDの登録・権限変更の申請** 業務上においてネットワーク又は情報システムにアクセスする必要あるいは変更が生じた場合、当該職員等によって、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当該利用者IDを登録又は権限を変更するよう申請されている。	□利用者ID登録・変更・抹消申請書 □利用者ID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及び職員等へのインタビューにより、ネットワーク又は情報システムにアクセスする業務上の必要あるいは権限変更が生じた場合、当該職員等によって、利用者IDの登録、権限変更を申請しているか確かめる。	6.2.(1)② (ア)	・単に利用者IDの登録及び変更の手続の有無を確認するのではなく、承認者の妥当性などを確認することが望ましい。
30	**ⅲ）利用者IDの抹消申請** 業務上においてネットワーク又は情報システムにアクセスする必要がなくなった場合、当該職員等によって、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当該利用者IDを抹消するよう申請されている。	□利用者ID登録・変更・抹消申請書 □利用者ID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及び職員等へのインタビューにより、ネットワーク又は情報システムにアクセスする業務上の必要がなくなった場合、当該職員等によって、利用者IDの抹消を申請しているか確かめる。	6.2.(1)② (イ)	・単に利用者IDの抹消の手続の有無を確認するのではなく、承認者の妥当性などを確認することが望ましい。
31	**ⅳ）利用者IDの点検** 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、利用されていないIDが放置されてないか点検されている。	□利用者ID棚卸記録 □利用者ID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、人事管理部門と連携し、利用者IDを定期的に棚卸して、必要のない利用者IDが登録されてないか、過剰なアクセス権限を付与していないかなどを定期的に点検しているか確かめる。	6.2.(1)② (ウ)	
32	**ⅰ）特権IDの取扱いに関わる手続** 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、管理者権限等の特権を付与されたIDの取扱いに関わる手続が定められ、文書化されている。	□特権ID取扱手続 □特権ID認可申請書 □特権ID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、管理者権限等の特権を付与されたIDの取扱いに関わる手続が文書化され、正式に承認されているか確かめる。	6.2.(1)③	
33	**ⅱ）特権ID及びパスワードの管理** 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、特権IDを付与する者が必要最小限に制限され、当該ID及びパスワードが厳重に管理されている。	□特権ID取扱手続 □特権ID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、必要以上に特権IDを付与していないか、当該ID及びパスワードが厳重に管理されているか確かめる。	6.2.(1)③ (ア)	
34	**ⅴ）特権IDの委託事業者による管理の禁止** 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、特権を付与されたID及びパスワードの変更を委託事業者には行わせていない。	□特権ID取扱手続	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、委託事業者に特権ID及びパスワードの変更を行わせていないか確かめる。	6.2.(1)③ (エ)	

35	**vi）特権ID及びパスワードのセキュリティ機能強化** 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、特権IDのパスワード変更や入力回数制限等のセキュリティ機能が強化されている。	□ネットワーク設計書 □システム設計書 □特権ID取扱手続 □特権ID・パスワード変更記録	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システム管理者へのインタビューにより、特権ID及びパスワードについて、利用者IDのパスワードよりも頻繁かつ定期的に変更する機能や、入力回数を制限する機能が組み込まれているか確かめる。	6.2.(1)③ (オ)	
36	**vii）特権IDのID変更** 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、特権IDは初期値以外のものに変更されている。	□特権ID取扱手続	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、特権IDを利用する際は、IDを初期値以外のものに変更しているか確かめる。	6.2.(1)③ (カ)	
37	**ⅰ）外部からのアクセスに関わる方針及び手続** 統括情報セキュリティ責任者によって、外部から内部のネットワーク又は情報システムにアクセスする場合の方針及び手続が定められ、文書化されている。	□リモートアクセス方針 □リモート接続手続	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、外部からのアクセスに関わる方針及び手続が文書され、正式に承認されているか確かめる。	6.2.(2)	
38	**ⅱ）外部からのアクセスの申請及び許可** 外部から庁内ネットワークに接続する必要のある場合、当該職員等によって、統括情報セキュリティ責任者及び当該情報システムを管理する情報システム管理者の許可を得ている。	□リモート接続許可申請書／許可書	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、職員等が外部から庁内ネットワークに接続する必要のある場合、統括情報セキュリティ責任者及び当該情報システムを管理する情報システム管理者の許可を得ているか確かめる。	6.2.(2)①	・外部からのアクセスを認める場合であっても、外部から庁内ネットワークに接続する必要性などを確認することが望ましい。
39	**ⅳ）外部からのアクセス時の本人確認機能** 外部からのアクセスを認める場合、統括情報セキュリティ責任者によって、外部からのアクセス時の本人確認機能が設けられている。	□ネットワーク設計書 □システム設計書	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、外部からのアクセスを認める場合、本人確認機能が設けられているか確かめる。	6.2.(2)③	
40	**vi）外部からのアクセス用端末のセキュリティ確保** 外部からのアクセスに利用するパソコン等の端末を職員等に貸与する場合、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、セキュリティ確保の措置が講じられている。	□リモート接続手続	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、外部からのアクセスに利用するパソコン等の端末を職員等に貸与する場合、セキュリティ確保の措置が講じられているか確かめる。	6.2.(2)⑤	
41	**ⅰ）認証情報ファイルの管理** 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、職員等の認証情報ファイルが厳重に管理されている。	□アクセス制御方針 □アクセス管理基準	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、職員等のパスワードの暗号化やオペレーティングシステム等のセキュリティ強化機能等で認証情報ファイルが厳重に管理されているか確かめる。	6.2.(5)①	・職員等によるパスワードの取扱いについては、No.135～141も関連する項目であることから参考にすること。
42	**ⅱ）仮パスワードの変更** 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発行された仮パスワードは、職員等によって、初回ログイン後直ちに変更されている。	□アクセス制御方針 □アクセス管理基準 □利用者ID取扱手続	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及び職員等へのインタビューにより、仮パスワードが速やかに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。	6.2.(5)②	
43	**ⅱ）資料等の保管** 情報システム管理者によって、システム開発・保守に関連する資料及びシステム関連文書が適切に保管されている。	□システム開発基準 □システム仕様書等 □プログラム仕様書等	監査資料のレビューと情報システム管理者へのインタビュー又は管理区域及び執務室の視察、ファイルサーバ等の確認により、システム開発・保守に関連する資料及びシステム関連文書が紛失したり改ざん等されないように保管されているか確かめる。	6.3.(4)①	
44	**ⅲ）テスト結果の保管** 情報システム管理者によって、テスト結果が一定期間保管されている。	□システム開発基準 □システムテスト計画書／報告書	監査資料のレビューと情報システム管理者へのインタビュー又は管理区域及び執務室の視察、ファイルサーバ等の確認により、テスト結果が一定期間保管されているか確かめる。	6.3.(4)②	
45	**ⅳ）ソースコードの保管** 情報システム管理者によって、情報システムに係るソースコードが適切に保管されている。	□システム開発基準 □ソースコード	監査資料のレビューと情報システム管理者へのインタビュー又は管理区域及び執務室の視察、サーバ等の確認により、情報システムに係るソースコードが誤消去や改ざん等されないような方法で保管されているか確かめる。	6.3.(4)③	
46	**ⅱ）変更履歴の作成** 情報システム管理者によって、情報システムを変更した場合、プログラム仕様書等の変更履歴が作成されている。	□システム開発基準 □システム仕様書等 □プログラム仕様書等	監査資料のレビューと情報システム管理者へのインタビューにより、情報システムを変更した場合、システム仕様書やプログラム仕様書等の変更履歴が作成されているか確かめる。	6.3.(6)	

47	**ⅰ）不正プログラム対策に関わる基準及び手順** 統括情報セキュリティ責任者及び情報セキュリティ責任者によって、不正プログラム対策に関わる基準及び手順が定められ、文書化されている。	□不正プログラム対策基準 □不正プログラム対策手順書	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、不正プログラム対策に関わる基準及び手順が文書化され、正式に承認されているか確かめる。	6.4.	
48	**ⅴ）パターンファイルの更新** 統括情報セキュリティ責任者によって、不正プログラム対策ソフトウェアのパターンファイルが最新のパターンファイルに更新されている。	□不正プログラム対策基準 □不正プログラム対策手順書 □不正プログラム対策ソフトウェアのログ	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セキュリティ責任者へのインタビュー、サーバ及びパソコン等の確認により、不正プログラム対策ソフトウェアのパターンファイルが最新のパターンファイルに更新されているか確かめる。	6.4.(1)⑤	
49	**ⅶ）サポート終了ソフトウェアの使用禁止** 統括情報セキュリティ責任者によって、開発元のサポートが終了したソフトウェアの利用は禁止され、ソフトウェアの切り替えが行われている。	□不正プログラム対策基準 □不正プログラム対策手順書	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、サーバ及びパソコン等の確認により、業務で利用するソフトウェアは開発元のサポートが継続しているソフトウェアであるか確かめる。	6.4.(1)⑦	
50	**ⅱ）パターンファイルの更新** 情報セキュリティ管理者によって、不正プログラム対策ソフトウェアのパターンファイルが最新のパターンファイルに更新されている。	□不正プログラム対策基準 □不正プログラム対策手順書 □不正プログラム対策ソフトウェアのログ	監査資料のレビューと情報システム管理者へのインタビュー、サーバ及びパソコン等の確認により、不正プログラム対策ソフトウェアのパターンファイルが最新のパターンファイルに更新されているか確かめる。	6.4.(2)②	
51	**ⅲ）不正プログラム対策ソフトウェアの更新** 情報セキュリティ管理者によって、不正プログラム対策ソフトウェアが最新のバージョンに更新されている。	□不正プログラム対策基準 □不正プログラム対策手順書 □不正プログラム対策ソフトウェアのログ	監査資料のレビューと情報システム管理者へのインタビュー、サーバ及びパソコン等の確認により、サーバ及びパソコン等の確認により、導入された不正プログラム対策ソフトウェアが最新のバージョンに更新されているか確かめる。	6.4.(2)③	
52	**ⅱ）データ等取り入れ時のチェック** 外部からデータ又はソフトウェアを取り入れる場合、職員等によって、不正プログラム対策ソフトウェアによるチェックが行われている。	□不正プログラム対策基準 □不正プログラム対策手順書 □不正プログラム対策ソフトウェアのログ	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、職員等が外部からデータ又はソフトウェアを取り入れる場合、不正プログラム対策ソフトウェアによるチェックが行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。	6.4.(3)②	
53	**ⅲ）出所不明なファイルの削除** 差出人不明又は不自然に添付されたファイルを受信した場合、職員等によって、速やかに削除されている。	□電子メール利用基準 □不正プログラム対策基準 □不正プログラム対策手順書	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、職員等が差出人不明又は不自然に添付されたファイルを受信した場合、速やかに削除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。	6.4.(3)③	
54	**ⅳ）不正プログラム対策ソフトウェアによるフルチェックの定期的実施** 職員等の使用する端末に対して、職員等によって、不正プログラム対策ソフトウェアによるフルチェックが定期的に実施されている。	□不正プログラム対策基準 □不正プログラム対策手順書 □不正プログラム対策ソフトウェアのログ	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、職員等の使用する端末に対して、不正プログラム対策ソフトウェアによるフルチェックが定期的に実施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。	6.4.(3)④	
55	**ⅶ）不正プログラムに感染した場合の対処** 不正プログラムに感染した場合又は感染が疑われる場合、職員等によって、パソコン等の端末のLANケーブルが即時取り外されている。モバイル端末の通信機能を停止する設定に変更している。	□不正プログラム対策基準 □不正プログラム対策手順書 □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、不正プログラムに感染した場合又は感染が疑われる場合、パソコン等の端末であれば、LANケーブルが即時取り外されているか確かめる。モバイル端末であれば通信機能を停止する設定に変更しているか確認する。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。	6.4.(3)⑦	・情報セキュリティインシデント発生時の対応についてはNo.323～326も関連する項目であることから参考にすること。
56	**ⅰ）未使用ポートの閉鎖** 統括情報セキュリティ責任者によって、使用されていないポートが閉鎖されている。	□ネットワーク構成図 □ネットワーク管理記録 □ファイアウォール設定 □ファイアウォールログ	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、使用されていないポートが閉鎖され、不正アクセスによる侵入を防止しているか確かめる。	6.5.(1)①	・ファイアウォールの設置については、No.171～172も関連する項目であることから参考にすること。
57	**ⅱ）不要なサービスの削除又は停止** 統括情報セキュリティ責任者によって、不要なサービスが削除又は停止されている。	□不正アクセス対策基準 □不正アクセス対応手順書 □システム監視手順書	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、使用されていない不要なサービスが削除又は停止され、不正アクセスによる侵入を防止しているか確かめる。	6.5.(1)②	

58	**ⅳ)システム設定ファイルの検査** 統括情報セキュリティ責任者によって、重要なシステムの設定を行ったファイル等について、定期的に当該ファイルの改ざんの有無が検査されている。	□ネットワーク管理基準 □システム設定検査記録	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システム管理者へのインタビューにより、重要なシステムの設定を行ったファイル等について、定期的に当該ファイルの改ざんの有無が検査されているか確かめる。	6.5.(1)③	
59	**ⅴ)連絡体制の構築** 統括情報セキュリティ責任者によって、監視、通知、外部連絡窓口及び適切な対応を実施できる体制並びに連絡網が構築されている。	□緊急時対応計画	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、情報セキュリティに関する統一的な窓口と連携して、CISOへの報告、各部部局への指示、ベンダとの情報共有及び報道機関への通知などの対応が行われているか確かめる。	6.5.(1)④	
60	**ⅱ)ソフトウェアの更新** 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、セキュリティホールの緊急度に応じてパッチが適用され、ソフトウェアが更新されている。	□パッチ適用情報 □パッチ適用記録	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システム管理者へのインタビューにより、セキュリティホールの緊急度に応じてパッチが適用され、ソフトウェアが更新されているか確かめる。	6.6.(1)	
61	**ⅳ)外部接続システムの常時監視** 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、外部と常時接続するシステムが常時監視されている。	□システム運用基準 □監視記録	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システム管理者へのインタビューにより、外部と常時接続するシステムが常時監視されているか確かめる。	7.1.③	
62	**ⅰ)委託事業者の選定基準** 情報セキュリティ管理者によって、委託事業者選定の際、委託内容に応じた情報セキュリティ対策が確保されていることが確認されている。	□委託事業者選定基準 □サービス仕様書(サービスカタログ)	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、委託事業者選定の際、重要な情報資産を取扱う業務を委託する場合など、委託内容に応じた情報セキュリティ対策が確保されていることを確認しているか確かめる。	8.1.(1)①	・委託事業者選定基準には、「コンプライアンスに関してその管理体制、教育訓練等の対策が取られ、従業員が理解しているか」、「委託業務内容に即した技術、要員が確保されているか」などの項目が含まれていることが望ましい。
63	**ⅰ)委託事業者との契約** 情報システムの運用、保守等を業務委託する場合、委託事業者との間で締結される契約書に、必要に応じた情報セキュリティ要件が明記されている。	□業務委託契約書	監査資料のレビューと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、委託事業者との間で締結される契約書に必要に応じて次の情報セキュリティ要件が明記されているか確かめる。 ・情報セキュリティポリシー及び情報セキュリティ実施手順の遵守 ・委託事業者の責任者、委託内容、作業者の所属、作業場所の特定 ・提供されるサービスレベルの保証 ・委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法 ・委託事業者の従業員に対する教育の実施 ・提供された情報の目的外利用及び受託者以外の者への提供の禁止 ・業務上知り得た情報の守秘義務 ・再委託に関する制限事項の遵守 ・委託業務終了時の情報資産の返還、廃棄等 ・委託業務の定期報告及び緊急時報告義務 ・委託元団体による監査、検査 ・委託元団体による情報セキュリティインシデント発生時の公表 ・情報セキュリティポリシーが遵守されなかった場合の規定(損害賠償等) 等	8.1.(2)	・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。 ・契約書において、再委託事業者の監督についても規定されていることが望ましい。