別紙3

# 地方公共団体における
# 情報セキュリティ監査に関する
# ガイドライン(令和７年３月改定)

平成15年12月25日　　策　　定
令和７年３月28日　　改　　定

総　務　省

別紙3

# 目　次

**別紙3**

【付録】

監査資料例一覧／索引

情報セキュリティ監査実施要綱（例）

情報セキュリティ監査実施計画書（例）

情報セキュリティ監査報告書（例）

情報セキュリティ監査業務委託仕様書（例）

情報セキュリティ監査業務委託契約書（例）

別紙3

# 第１章

# 総則

# 第1章 総則

## 1.1. 本ガイドラインの目的

現在、ほとんどの地方公共団体は、組織内の情報セキュリティを確保するための方針、体制、対策等を包括的に定めた文書である情報セキュリティポリシーを策定している。

地方公共団体の情報セキュリティ対策は、情報セキュリティポリシーに従って実施され、また情報システムの変更や新たな脅威の出現等を踏まえて、対策の見直しを行うことで、情報セキュリティ対策の水準が向上していく。このため、情報セキュリティ対策全般の実効性を確保するとともに、情報セキュリティポリシーの見直しを行うことが重要であるが、そのための有効な手法となるのが「情報セキュリティ監査」である。

「自治体 DX・情報化推進概要」（令和５年４月発表）によれば、情報セキュリティ監査を実施している地方公共団体は、都道府県においては 46 団体（97.9%）、市区町村では 1000 団体（57.4%）であり、今後もさらに多くの地方公共団体で情報セキュリティ監査が実施されるよう、推進していく必要がある。

本ガイドラインは、情報セキュリティ監査の標準的な監査項目と監査手順を示すものであり、地方公共団体が情報セキュリティ監査を実施する際に活用されることを期待して作成している。

もとより、本ガイドラインに記述した構成や項目等は参考として示したものであり、各地方公共団体が必要に応じて独自の情報セキュリティ監査項目を追加設定したり、監査方法を修正するなど各団体の実情に応じた変更を加えて、情報セキュリティ監査を実施することを妨げるものではない。

## 1.2. 本ガイドライン策定の経緯

総務省では、地方公共団体における情報セキュリティ対策について、これまでも、情報セキュリティポリシーの策定や情報セキュリティ監査の実施を要請するとともに、その参考としてガイドライン等を策定してきた。平成 13 年 3 月に「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」（以下「ポリシーガイドライン」という。）を、また、平成 15 年 12 月に「地方公共団体における情報セキュリティ監査に関するガイドライン」（以下「監査ガイドライン」という。）を策定した。

平成 18 年 2 月に政府の情報セキュリティ政策会議は「第 1 次情報セキュリティ基本計画」を決定し、地方公共団体向けの重点施策として、地方公共団体における情報セキュリティ確保に係るガイドラインの見直しや情報セキュリティ監査実施の推進が掲げられた。これを踏まえ、総務省では、地方公共団体の情報セキュリティ水準の向上を推進するため、平成 18 年 9 月にポリシーガイドラインを、平成 19 年 7 月に監査ガイドラインを全部改定した。

平成 21 年 2 月に情報セキュリティ政策会議によって「第 2 次情報セキュリティ基本計画」が決定され、地方公共団体に関して、小規模な地方公共団体も含め、全ての地方公共団体において、望ましい情報セキュリティ対策が実施されることを目指し、対策の促進を行うこととされたこと、平成 22 年 5 月に情報セキュリティ政策会議によって「国民を守る情報セキュリティ戦略」及び「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定にあたっての指針（第 3 版）」が決定されたこと、平成 22 年 7 月に「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定にあたっての指針　対策編」が策定されたこと等を踏まえ、平成 22 年 11 月にポリシーガイドラインと監査ガイドラインを一部改定した。

平成 25 年 6 月に政府の IT 総合戦略本部が策定した「世界最先端 IT 国家創造宣言」（平成 25 年 6 月 14 日閣議決定、平成 26 年 6 月 24 日改定）や、平成 25 年 5 月 24 日に成立し、平成 25 年 5 月 31 日に公布された社会保障・税の分野における給付と負担の公平化や各種行政事務の効率化のための「行政手続における特定の個人を識別するための番号の利用等に関する法律」、平成 26 年 11 月 6 日に成立し、平成 26 年 11 月 12 日に公布されたサイバーセキュリティに関する施策を総合的かつ効果的に推進することを目的とした「サイバーセキュリティ基本法」等の新たに成立した法令等を踏まえ、平成 27 年 3 月 27 日にポリシーガイドライン、監査ガイドラインの一部改定を行った。また、平成 27 年度には、自治体情報セキュリティ対策検討チームを構成し、地方公共団体の情報セキュリティに関わる抜本的な対策の検討が行われた。「新たな自治体情報セキュリティ対策の抜本的強化について」（平成 27 年 12 月 25 日総行情第 77 号　総務大臣通知）にて、地方公共団体でのセキュリティ対策の抜本的強化への取組が示された。

平成 30 年 9 月 25 日には、政府機関の情報セキュリティ対策のための統一基準、自治体情報セキュリティ対策検討チーム報告等を踏まえて、地方公共団体の情報セキュリティ水準の向上及び情報セキュリティ対策の抜本的強化が実施されたため、ポリシーガイドライン及び監査ガイドラインを一部改定した。

令和 2 年 5 月 22 日には、「クラウド・バイ・デフォルト原則」、行政手続のオンライン化、働き方改革、サイバー攻撃の増加といった新たな時代の要請や「三層の対策」の課題を踏まえた「自治体情報セキュリティ対策の見直しについて」がとりまとめられた。同とりまとめ及び平成 30 年 7 月の政府機関の情報セキュリティ対策のための統一基準の改定等を踏まえて、令和 2 年 12 月 28 日にポリシーガイドライン及び監査ガイドラインを一部改定した。

令和 3 年度には、「デジタル庁設置法」、「デジタル社会形成基本法」、「地方公共団体情報システムの標準化に関する法律」等のデジタル改革関連法が成立・施行され、国及び地方のデジタル・トランスフォーメーション（DX）が推し進められることとなった。総務省では、これらの地方公共団体におけるデジタル化の動向や令和 3 年 7 月の政府機関のサイバーセキュリティ対策のための統一基準の改定を踏まえて、令和 4 年 3 月 25 日に一部改定を行った。

標準化法により、地方公共団体において、標準化基準（標準化法第 6 条第 1 項及び第 7 条第 1 項に規定する標準化のために必要な基準をいう。以下同じ。）に適合する基幹業務システム（以下「標準準拠システム」という。）の利用が義務付けられ、標準準拠システムについてガバメントクラウド（デジタル社会形成基本法（令和 3 年法律第 35 号）第 29 条に規定する「全ての地方公共団体が官民データ活用推進基本法第 2 条第 4 項に規定するクラウド・コンピューティング・サービス関連技術に係るサービスを利用することができるようにするための国による環境の整備」としてデジタル庁が整備するものをいう。以下同じ。）を利用することが努力義務とされた。

また、令和 4 年 10 月に、標準化法第 5 条第 1 項に基づき、地方公共団体情報システムの標準化の推進を図るための基本的な方針として、「地方公共団体情報システム標準化基本方針」が閣議決定された。当該方針のサイバーセキュリティに係る事項において「地方公共団体が利用する標準準拠システム等の整備及び運用に当たっては、総務省が作成する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を参考にしながら、セキュリティ対策を行うものとする。」とされたところである。なお、地方公共団体においては、クラウドサービス上での標準準拠システム等の整備及び運用を開始するまでに、第 4 編「地方公共団体におけるクラウド利用等に関する特則」に示された対策基準（例文及び解説）の内容を参考にセキュリティポリシーの見直しを行う必要がある。

総務省では、これらの状況を踏まえ、今般、ポリシーガイドライン及び監査ガイドラインを改定したものである。

## 1.3. 情報セキュリティ監査の意義と種類

（1） 情報セキュリティ監査の意義

情報セキュリティ監査とは、情報セキュリティを維持・管理する仕組みが組織において適切に整備・運用されているか否かを点検・評価することである。

また、監査の結果は、情報セキュリティに関する管理及び対策が適切であるか否かを示すとともに、情報セキュリティ上の問題点の指摘と改善の方向性の提言をまとめたものである。ただし、監査業務は、あくまで改善の方向性を示すものであり、具体的な解決策を提示するコンサルティング業務とは異なる。

なお、監査業務には、改善を勧告した事項について、後日、フォローアップする業務も含まれる。

（2） 内部監査と外部監査

情報セキュリティ監査には、地方公共団体内の職員自らが監査を行う内部監査と外部に委託して監査を行う外部監査がある。なお、内部監査の場合も被監査部門から独立した監査人等が監査を行うことが必要であり、情報システム等を運用する者自らによる検証を行う場合は、監査ではなく自己点検になる。

内部監査は、外部に委託する経費を要しないほか、監査の実施を通じて内部職員の情報セキュリティに対する意識を高めることができるという長所がある。他方、外部監査は、第三者の視点による客観性や専門性を確保できるという長所がある。地方公共団体の業務は公共性が高く、住民の権利等を守るという目的があることから、内部監査に加え、外部監査を行うことが望ましい。

外部監査を行う場合、監査実施の全部を外部監査するほか、特定の監査テーマについてのみ外部監査とし、それ以外は内部監査とすることも考えられる。

本ガイドラインは、自己点検、内部監査、外部監査を実施する際の点検項目や監査項目を検討する上で参照できる内容となっている（図表 1.1）。

（3） 助言型監査と保証型監査

外部監査の形態には、当該地方公共団体に対し、情報セキュリティ対策の改善の方向性を助言することを目的とする助言型監査と、住民や議会等に対し、情報セキュリティの水準を保証することを目的とする保証型監査がある。

どちらの型の外部監査を行うかは地方公共団体の判断次第であるが、一般的には、情報セキュリティ対策の向上を図るため、最初は継続的な内部監査と併せて助言型監査を行い、必要に応じて保証型監査を行うことが考えられる。

（4） 準拠性監査と妥当性監査

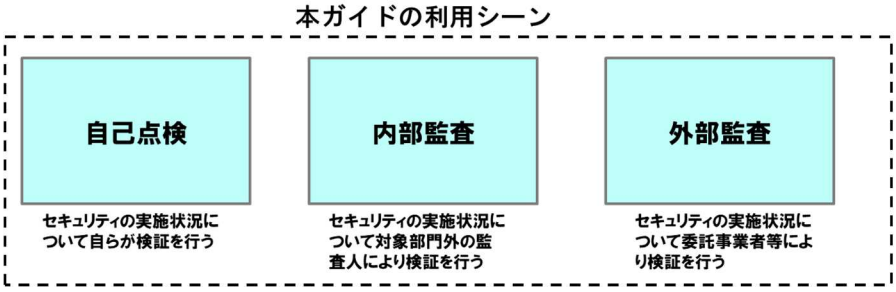
情報セキュリティ監査では、準拠性監査と妥当性監査がある。

準拠性監査においては、当該団体の情報セキュリティポリシーというルールに従って情報セキュリティ対策が実施されているか否かを点検・評価する。

一方、妥当性監査においては、当該団体の情報セキュリティポリシーというルールそのものが、ポリシーガイドラインをはじめ、JIS Q 27002 等の基準や当該団体の情報セキュリティを取り巻く状況等に照らし妥当なものかどうかを点検・評価する。

どちらの型の外部監査を行うかは地方公共団体の判断次第であるが、一般的には、最初は点検・評価のしやすい準拠性監査を行い、必要に応じて妥当性監査を行うことが多いと考えられる。

図表 1.1　情報セキュリティ監査の種類



## 1.4. 本ガイドラインとポリシーガイドラインの関係

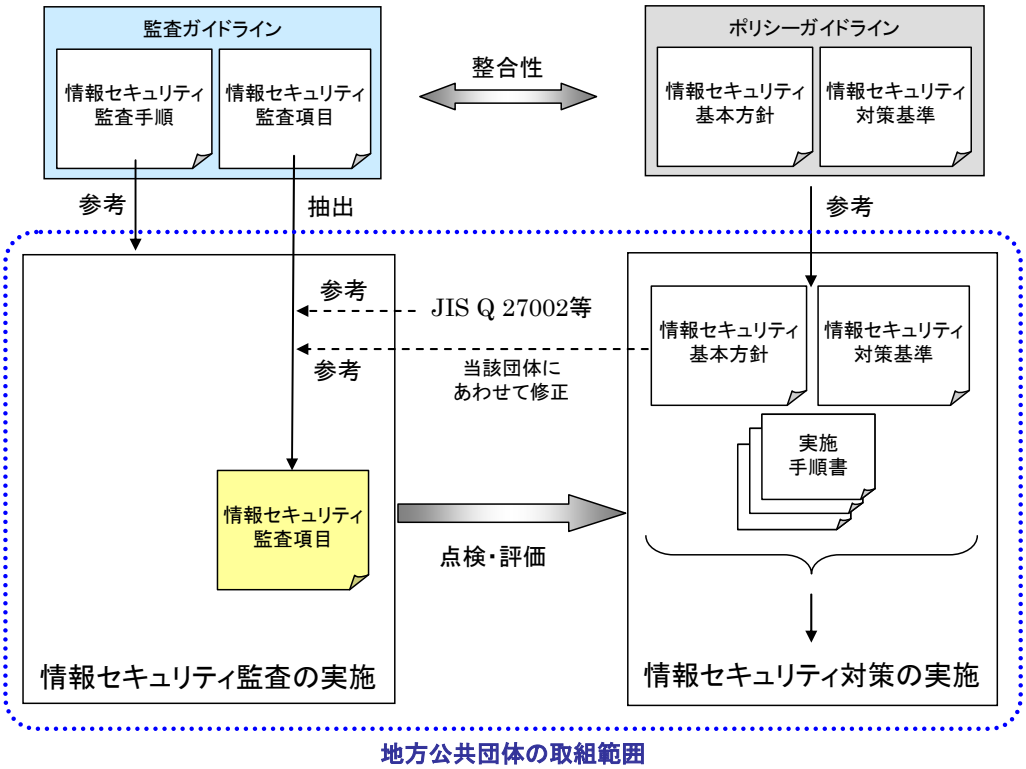
総務省では、監査ガイドラインとポリシーガイドラインを策定しているが、両者は内容的に整合性を図っている。特に、監査ガイドラインの情報セキュリティ監査項目は、ポリシーガイドラインにおける対策基準に即して構成している。

地方公共団体は、ポリシーガイドラインを参考にして、情報セキュリティポリシー（情報セキュリティ基本方針及び情報セキュリティ対策基準）や実施手順書を策定して、情報セキュリティ対策を実施している。

情報セキュリティ監査は、情報セキュリティポリシーの実施状況を点検･評価するものであり、各地方公共団体は、監査ガイドラインを参考にして、情報セキュリティ監査を実施する。この際、監査項目の設定においては、当該団体の情報セキュリティポリシーを踏まえて、監査テーマに応じた監査項目を情報セキュリティ監査項目から抽出することで、各地方公共団体が策定している情報セキュリティポリシーの内容と情報セキュリティ監査項目の対応付けや読み替えなどの工数を削減することができるようになっている。

なお、情報セキュリティ監査の実施においては、監査ガイドライン以外に、必要に応じて、JIS Q 27002 等も参考にするとよい（図表 1.2）。

図表 1.2　監査ガイドラインとポリシーガイドラインの関係

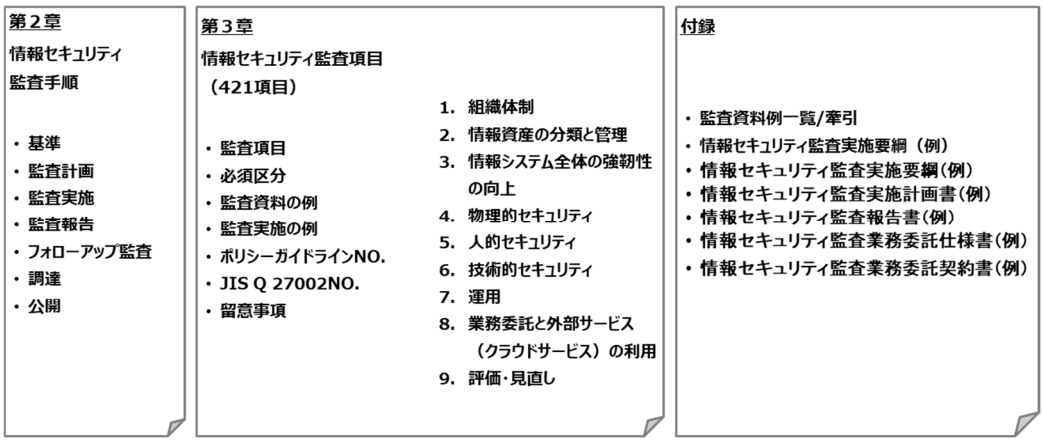


## 1.5. 本ガイドラインの構成

次章より、情報セキュリティ監査の具体的内容を扱うが、第 2 章の「情報セキュリティ監査手順」においては、情報セキュリティ監査の標準的な手順を、第 3 章の「情報セキュリティ監査項目」においては、385 項目の監査項目と項目毎に確認すべき内容や方法を記載している。また、「付録」として、監査資料一覧など情報セキュリティ監査を実施する際に参考となる資料をつけている（図表 1.3）。

監査資料例一覧は、情報セキュリティ監査項目に挙げた監査資料の例を 50 音順に一覧にしたものであり、それぞれの監査資料の内容について解説を記載している。

図表 1.3　監査ガイドラインの構成




なお、監査を効率的に行えるよう、情報セキュリティ監査項目に監査結果や確認した監査資料、指摘事項、改善案の記入欄を追加した監査チェックリストの例を電子データで作成しているので、監査を実施する際に各団体の実情に応じて加工して活用いただきたい（図表 1.4）。

図表 1.4　情報セキュリティ監査チェックリストの例

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|
| 4.物理的セキュリティ | 4.1.サーバ等の管理 | (5)機器の定期保守及び修理 | 43 | | **Ⅰ)機器の保守・修理に関わる基準及び手続**<br>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、サーバ等の機器の定期保守・修理に関わる基準及び手続が定められ、文書化されている。 | □機器保守・修理基準/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、サーバ等の機器の保守・修理に関わる基準及び手続が文書化され、正式に承認されているか確かめる。 | 4.1.(5) | 11.2.4 | |
| | | | 44 | ○ | **Ⅱ)サーバ等の機器の定期保守**<br>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<br>□保守機器管理表<br>□保守体制図<br>□作業報告書<br>□障害報告書<br>□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 | 11.2.4 | |
| | | | 45 | ○ | **Ⅲ)電磁的記録媒体を内蔵する機器の修理**<br>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<br>□保守機器管理表<br>□保守体制図<br>□作業報告書<br>□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 | 15.1.2<br>11.2.4<br>18.1.1<br>18.2.2 | |
| | | (6)庁外への機器の設置 | 46 | | **Ⅰ)庁外への機器設置に関わる基準及び手続**<br>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、庁外にサーバ等の機器を設置する場合の基準及び手続が定められ、文書化されている。 | □機器設置基準/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、庁外にサーバ等の機器を設置する場合の基準及び手続が文書化され、正式に承認されているか確かめる。 | 4.1.(6) | 11.2.5<br>11.2.6 | ・地方公共団体の庁外の装置を保護するために、十分な措置が取られていることが望ましい。<br>・損傷、盗難、傍受といったセキュリティリスクを考慮し、それぞれの場所に応じた最も適切な管理策を導入することが望ましい。 |
| | | | 47 | | **Ⅱ)庁外への機器の設置の承認**<br>統括情報セキュリティ責任者及び情報システム管理者は、庁外にサーバ等の機器を設置する場合、CISOの承認を得ている。 | □機器設置基準/手続<br>□庁外機器設置申請書/承認書<br>□情報資産管理台帳 | 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、庁外に設置しているサーバ等の機器がCISOに承認されているか確かめる。<br>また、情報資産管理台帳を確認し、庁外に設置していることが記載されているか確かめる。 | 4.1.(6) | 11.2.5<br>11.2.6 | |

別紙3

# 第２章

# 情報セキュリティ監査手順

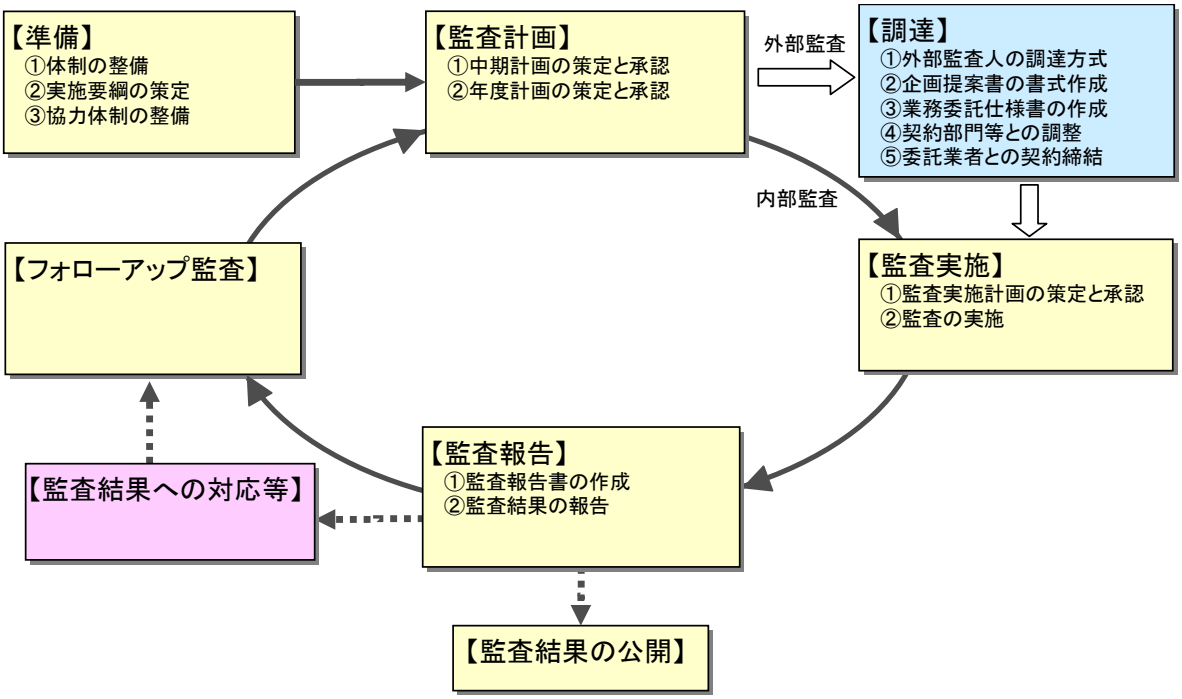
# 第2章 情報セキュリティ監査手順

## 2.1. 監査手順の概要

情報セキュリティ監査は、基本的に「準備」、「監査計画」、「監査実施」、「監査報告」、「監査結果の公開」及び監査結果への対応等に対する「フォローアップ監査」の手順により実施される。内部監査の場合は、この手順に基づいて実施されるが、外部監査の場合は、この手順に「外部監査人の調達」が加わる（図表 2.1）。

本章では、「2.2 監査手順」において、監査の基本的な手順を、「2.3 外部監査人の調達」において、外部監査人に委託する場合の手順について記述する。

図表 2.1　情報セキュリティ監査手順



## 2.2. 監査手順

### 2.2.1. 準備

（1） 体制の整備

情報セキュリティ監査を実施するにあたり、まず、最高情報セキュリティ責任者（CISO: Chief Information Security Officer、以下「CISO」という。）は、「情報セキュリティ監査統括責任者」を指名し、情報セキュリティ監査を実施する責任者を明確にする（図表 2.2）。情報セキュリティ監査統括責任者は、情報セキュリティ監査に関わる責任と権限を有する。情報セキュリティ監査統括責任者は、組織の監査全体に責任を負うため、地方公共団体の長に準じる権限と責任を有する者とすることが望ましい。情報セキュリティ監査統括責任者は、監査計画及びそれに付随するリスクを効果的かつ効率的に管理するのに必要な資質並びに次の領域における知識及び技能を有することが望ましい。ただし、必要な資質、知識及び技能を有することが困難な場合は、外部の専門家をあてて能力を補完することも考えられる。

- 監査の原則、手順及び方法に関する知識
- マネジメントシステム規格及び基準文書に関する知識
- 被監査部門の活動、製品及びプロセスに関する知識
- 被監査部門の活動及び製品に関し適用される法的並びにその他の要求事項に関する知識
- 該当する場合には、被監査部門の利害関係者に関する知識

また、情報セキュリティ監査統括責任者は、監査計画を管理するのに必要な知識及び技能を維持するために適切な専門能力の継続的開発・維持活動に積極的に関わることが望ましい。

情報セキュリティ監査統括責任者は、内部監査人を指名して内部監査チームの編成や、外部監査人への委託により、情報セキュリティ監査の体制を整備する。

内部監査人は、公平な立場で客観的に監査を行うことができるように、被監査部門（監査を受ける部門）から独立した者を指名しなければならない。また、監査及び情報セキュリティについて、専門的知識を有する者でなければならない。そのため、必要に応じ内部監査人として必要な知識について研修を実施したり、外部で行われる研修に派遣することが適当である。さらに、監査プロセスや目的を達成するための能力は、内部監査人の資質に依存する（図表 2.3）。そのため、内部監査人としての資質を満たしているかを評価することが求められる。

なお、内部監査人には、通常監査担当部門の職員をあてるが、情報システムを所管する課の職員に他の情報システム所管課の内部監査を行わせる方法（相互監査）も有効である。

内部監査人の評価の方法については、以下のような方法から複数を組み合わせ

て行うことが望ましい。

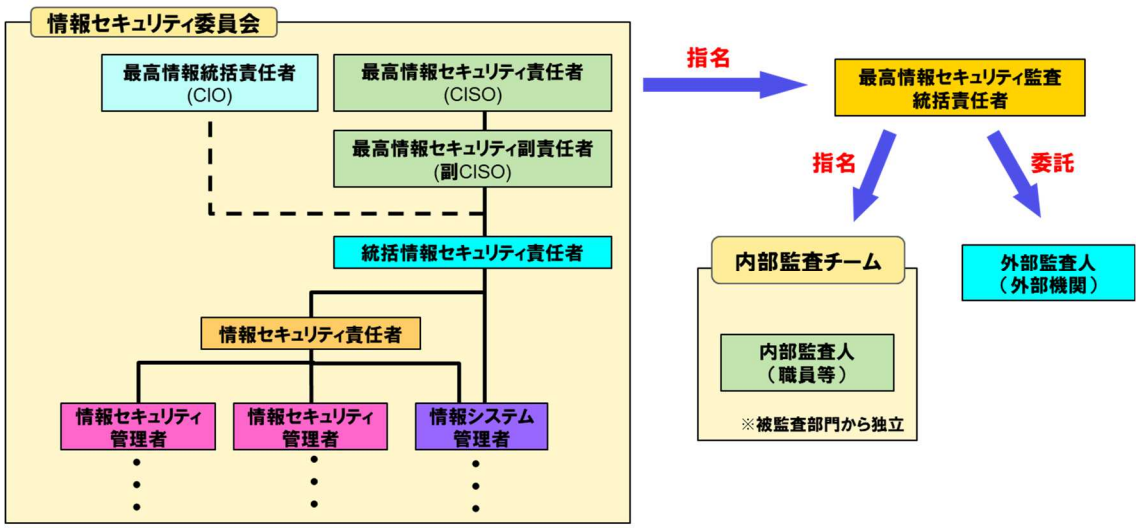
・記録のレビュー　　：教育等の記録を確認し、監査人の経歴を検証する
・フィードバック　　：監査パフォーマンスに関する苦情等の情報を与える
・面接　　：監査人と面接し、監査人の情報を得る
・観察　　：立ち会い監査等により、知識及び技能を評価する
・試験　　：筆記試験を行い、行動、知識及び技能を評価する
・監査後のレビュー　：監査報告書等をレビューし、強み、弱みを特定する

なお、小規模の地方公共団体等においては、CISO が情報セキュリティ監査統括責任者を兼務したり、内部監査チームの職員等も他の業務と兼務せざるを得ないことも考えられる。この場合においても、監査を実施する者は、自らが直接担当する業務やシステムの監査を実施させないなど、監査における客観性の確保を図る必要がある。

その他、外部監査人に監査を依頼する場合は、適切な監査が実施できることをあらかじめ確認しておく必要がある。具体的には以下の事項が考えられる。

・外部監査人の過去の実績、経歴及び保有資格の確認
・過去の監査報告書の構成及び報告内容の確認　など

図表 2.2　情報セキュリティ監査の実施体制（例）



図表 2.3　内部監査人に必要な資質

| | 項目 | 内容 |
|---|---|---|
| 1 | 倫理的である | 公正であり、正直である |
| 2 | 心が広い | 別の考え方や視点を取り入れることができる |
| 3 | 外交的である | 人と上手に接することができる |
| 4 | 観察力がある | 周囲の状況や活動を積極的に観察する |
| 5 | 知覚が鋭い | 状況を察知し、理解できる |
| 6 | 適応性がある | 異なる状況に容易に合わせることができる |
| 7 | 粘り強い | 根気があり、目的の達成に集中する |
| 8 | 決断力がある | 論理的な理由付けや分析により、結論に到達することができる |
| 9 | 自立的である | 他人とやりとりしながらも独立して行動し、役割を果たすことができる |
| 10 | 不屈の精神をもって行動する | 意見の相違や対立があっても、進んで責任をもち、倫理的に行動できる |
| 11 | 改善に対して前向きである | 進んで状況から学び、よりよい監査結果のために努力する |
| 12 | 文化に対して敏感である | 被監査者の文化を観察し、尊重する |
| 13 | 協働的である | 他人と共に効果的に活動する |

（2） 実施要綱の策定

情報セキュリティ監査統括責任者は、情報セキュリティ委員会の承認を得て監査に関する基本的事項を定めた「情報セキュリティ監査実施要綱」を策定する（図表 2.4)。

なお、「情報セキュリティ監査実施要綱」に基づき、内部監査人が監査を実施する際の具体的な手順を記述した「情報セキュリティ監査実施マニュアル」や「情報セキュリティ監査実施の手引き」等を作成し、要綱にこれらを位置付けることもある。

図表 2.4　情報セキュリティ監査実施要綱に記載する事項（例）

| 区分 | 項目 |
|---|---|
| 1.総則 | (1)目的 |
| | (2)監査対象 |
| | (3)監査実施体制 |
| | (4)監査の権限 |
| | (5)監査人の責務 |
| | (6)監査関係文書の管理 |

| 区分 | 項目 |
|---|---|
| 2.監査計画 | (1)監査計画 |
| | (2)中期計画及び年度計画 |
| | (3)監査実施計画 |
| 3.監査実施 | (1)監査実施通知 |
| | (2)監査実施 |
| | (3)監査調書 |
| | (4)監査結果の意見交換 |
| 4.監査報告 | (1)監査結果の報告 |
| | (2)監査結果の通知と改善措置 |
| 5.フォローアップ | (1)フォローアップ監査の実施 |

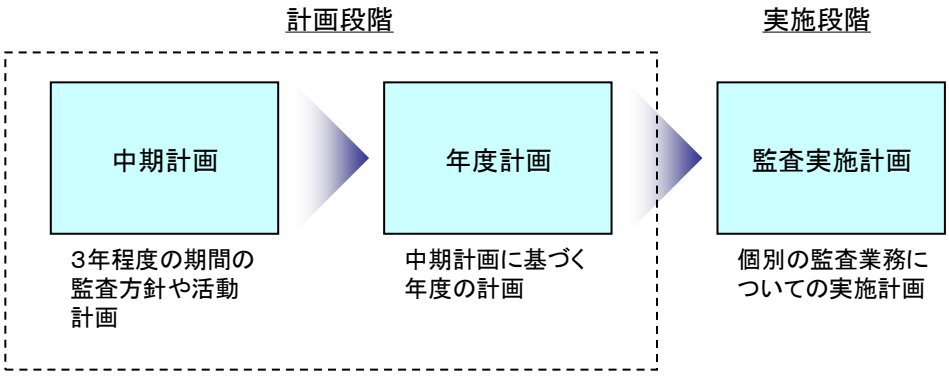
（3） 協力体制の整備

被監査部門は、情報セキュリティ監査に協力する義務を負うが、監査を円滑に実施するとともに、監査の効果をあげるためには、組織内の理解を得ておくことが重要である。とりわけ、被監査部門に対して監査資料の提示や担当者へのインタビュー、執務室の視察等を求めることを考えると、監査の実施に被監査部門の担当者の理解と協力が必要である。また、外部の専門家の支援を受けたり、外部監査人に委託する場合には予算措置が必要となるので、幹部、財政担当部門等の理解を得ておく必要がある。

### 2.2.2. 監査計画

情報セキュリティ監査を効率的かつ効果的に行うために、情報セキュリティ監査を実施する計画を策定する。一般に、監査計画には、「中期計画」、「年度計画」、及び個々の「監査実施計画」がある。計画段階では、中期計画及び年度計画を策定する（図表 2.5）。

図表 2.5　情報セキュリティ監査計画策定の流れ




（1）　中期計画の策定と承認

情報セキュリティ監査の対象は広範囲に及ぶことから、一回の監査や単年度内で全てを網羅することはできない。したがって、一定の期間（例えば、３年程度）を見据えた計画が必要となる。中期計画は、この期間における情報セキュリティ監査の方針や実施目標、監査範囲、大まかな実施時期等の項目を記述した文書であり、情報セキュリティ監査に関する中期的な方針を示すものである。この計画には、一定の期間内での監査の頻度についても記述しておく。

なお、期間中であっても、地方公共団体の置かれている環境の変化や監査実施計画自体の進捗状況により、見直しを行う必要がある。中期計画は策定・見直しの都度、情報セキュリティ委員会の承認を得る必要がある。

また、小規模の地方公共団体等においては、監査の対象規模が相対的に大きくないことから、年度計画のみを作成するなど簡素化することも考えられる。

（2）　年度計画の策定と承認

年度計画は、中期計画に基づいて年度当初に策定されるものであり、各年度の監査重点テーマや実施回数、監査対象、実施時期等を記述した文書である。年度計画は、当該年度の監査目標を遂行するための計画なので、誰が（実行責任者）、いつ（実施時期）、何を（実施内容）、いくら（予算）で実施するのかを明確に定める必要がある。監査テーマの選定においては、情報資産やネットワーク及び情報システム等の重要度や脆弱性、情報システムの変更等の視点から検討し、より重要性、緊

急性、リスク等の高いものから選定する。

　年度計画についても、中期計画同様、情報セキュリティ委員会の承認を得る必要がある。

### 2.2.3. 監査実施

（1） 監査実施計画の策定と承認

情報セキュリティ監査統括責任者は、年度計画に基づいて、内部監査人又は外部監査人に指示して具体的な監査実施計画を策定する（図表 2.6）。

内部監査の場合、内部監査人の資質や業務負荷を考慮した監査実施時期に配慮して実施計画を立てることが望ましい。

監査実施計画書中、監査項目は、例えば、本ガイドライン「第 3 章　情報セキュリティ監査項目」の大分類や中分類のレベルを記載するとよい。また、適用基準には、例えば、付録の「情報セキュリティ監査業務委託仕様書（例）」の適用基準を参考に記載するとよい。

図表 2.6　情報セキュリティ監査実施計画書に記載する事項（例）

| | 項目 | 内容 |
|---|---|---|
| 1 | 監査目的 | 監査を実施する目的 |
| 2 | 監査テーマ | 監査の具体的なテーマや重点監査事項 |
| 3 | 監査範囲 | 監査対象の業務、情報システム等の範囲 |
| 4 | 被監査部門 | 監査の対象となる部門 |
| 5 | 監査方法 | 監査で適用する監査技法 |
| 6 | 監査実施日程 | 監査の計画から報告までの日程 |
| 7 | 監査実施体制 | 監査担当者 |
| 8 | 監査項目 | 監査で確認する大項目 |
| 9 | 適用基準 | 監査で適用する基準等 |

情報セキュリティ監査統括責任者は、監査実施計画書を、組織として受け入れ、監査実施の責任と権限を明確にするため、情報セキュリティ委員会による承認を得る。また、情報セキュリティ委員会の承認を得た後に、被監査部門に対して十分に説明する機会を設け、監査スケジュールを被監査部門へ伝え、担当者の選出、監査資料の準備等の事項の依頼など、効率的に監査を実施するための調整を行う。

（2） 監査の実施

①監査チェックリストの作成

監査人は、監査を効率的かつ効果的に実施するため、次の手順を参考にして、確認すべき具体的な項目を事前に選定して、監査チェックリストを作成する。

ｉ）監査項目の選定

監査テーマに該当する項目を本ガイドライン「第 3 章　情報セキュリティ監査項目」から選定する。なお、「第 3 章　情報セキュリティ監査項目」で必須項目となっているものは、監査において基本的な項目又は必要性の高い項目であることから、極力、監査項目に含めることが望まれる。必須項目は、はじめて情報セキュリティ監査を行う場合等の初期段階用

に選定したものであり、これで満足することなく、より高いレベルを目指した必須項目以外も対象とする監査を実施する必要がある。

監査項目の選定後は、当該地方公共団体の情報セキュリティポリシーに合わせた表現とするなど、必要に応じて項目中の文言を当該団体にとって適切な表現に修正する。なお、本ガイドラインの監査項目はポリシーガイドラインに準拠しているので、ポリシーガイドラインに対する妥当性を監査する場合には表現の修正は行わなくてもよい。

ⅱ）当該地方公共団体に必要と思われる項目の追加

監査項目を選定し、適宜表現を修正した後、当該地方公共団体にとって必要と考えられる項目を追加する。特に、監査範囲内において非常に重要な情報資産が存在し、脅威の発生頻度が高く、脅威が発生した場合の被害が大きい場合には、通常の情報セキュリティ対策に加えて、より厳格な対策を追加することを検討すべきである。

ⅲ）当該地方公共団体が定める条例、規則、規程等との整合性の確保

当該地方公共団体が定める条例、規則、規程等との整合性を図り、矛盾が生じないように監査項目を修正する。

ⅳ）関連法令の参照

関連する法令の要求する事項の中で特に重要と考えられる事項について追加する。

関連する主な法令としては、例えば、以下のようなものが考えられる。

- 地方公務員法
- 著作権法
- 不正アクセス行為の禁止等に関する法律
- 個人情報の保護に関する法律
- 行政手続における特定の個人を識別するための番号の利用等に関する法律
- サイバーセキュリティ基本法
- 個人情報保護法施行条例

ⅴ）他の基準・規程類の参照

その他、JIS Q 27002、JIS Q 27017、ISO/IEC TR 13335（GMITS）、情報システム安全対策基準（通商産業省告示第 536 号）、コンピュータウイルス対策基準（平成 9 年通商産業省告示第 952 号）、コンピュータ不正アクセス対策基準（平成 12 年通商産業省告示第 950 号）等、情報セキュリティ対策の実施に参考となる基準を適時参照して、必要があれば、項目の追加、修正をする。

②監査の実施

監査人は、監査チェックリストに基づいて情報セキュリティ監査を実施し、監査調書を作成する。主な監査技法には、レビュー、インタビュー、視察、アンケートがある。これらの監査技法は、被監査部門の所在場所にて実施する現地監査のほか、被監査部門の所在場所に行かずに行うリモート監査でも用いることができる。

・レビュー　　：文書や記録等の監査資料を入手し、内容を確認する
・インタビュー　：担当者等に質問し、状況を確認する
・視察　　：業務を行っている場所や状況を見て確認する
・アンケート　　：質問書への回答から実態を確認する

具体的な監査方法については、本ガイドラインの「第 3 章　情報セキュリティ監査項目」の監査チェックリストにおいて、監査項目毎に、監査資料の例、監査実施の例を示している。また、レビューで確認すべき文書や記録等については、付録に「監査資料例一覧／索引」としてとりまとめているので、参考にされたい。

情報セキュリティ監査の実施中、情報セキュリティ監査統括責任者は、監査人による監査業務の実施状況について随時報告を求める等、適切な管理を行う必要がある。また、監査人が作成した監査調書は、脆弱性の情報などが漏えいした場合には、当該地方公共団体の情報セキュリティに脅威となる情報も含むことから、情報セキュリティ監査統括責任者は、紛失等が生じないように適切に保管する必要がある。

また、監査人は、監査業務上知り得た情報や監査内容について、その情報が関係者以外に漏えいしないように対策をとる必要がある。

③監査結果の取りまとめ

情報セキュリティ監査統括責任者は、実施した監査の内容を踏まえて、監査結果、確認した監査証拠、指摘事項、改善案等の監査結果を取りまとめる。具体的には、例えば、図表 1.5 の監査チェックリストに記入する。

また、監査結果については、必要に応じ、事実誤認がないかどうかを被監査部門に確認する。

④監査結果の評価

情報セキュリティ監査統括責任者は、監査基準に照らして監査結果を評価する。監査結果では、監査基準に対して適合又は指摘事項のいずれかを示すことができる。個々の監査結果には、根拠となる証拠及び改善の機会並びに被監査部門に対する提言とともに適合性及び優れた実践を含めることが望ましい。

指摘事項については、監査証拠が正確であること及び指摘事項の内容が理解されたかどうか、被監査部門に確認することが望ましい。

また、指摘事項がある場合、個々のセキュリティ対策の有効性のほか、監査におけるマネジメントシステム全体の有効性についても考察した上で監査結論を作成することが望ましい。

### 2.2.4. 監査報告

（1） 監査報告書の作成

情報セキュリティ監査統括責任者は、監査調書に基づいて、被監査部門に対する指摘事項や改善案を含む監査報告書を作成する（図表 2.7）。

また、詳細な監査結果や補足資料等がある場合は、監査報告書の添付資料としてもよい。監査報告書では、監査項目への適合の程度や、図表 2.1 にあるセキュリティ監査手順の運用サイクルが有効に機能しているかの観点を取り入れることが望ましい。

図表 2.7　情報セキュリティ監査報告書に記載する事項（例）

| | 項目 | 内容 |
|---|---|---|
| 1 | 監査目的 | 監査を実施した目的 |
| 2 | 監査テーマ | 監査の具体的なテーマや重点監査事項 |
| 3 | 監査範囲 | 監査対象の業務、情報システムなどの範囲 |
| 4 | 被監査部門 | 監査の対象とした部門 |
| 5 | 監査方法 | 監査で適用した監査技法 |
| 6 | 監査実施日程 | 監査の計画から報告までの日程 |
| 7 | 監査実施体制 | 監査を実施した担当者 |
| 8 | 監査項目 | 監査で確認した大項目 |
| 9 | 適用基準 | 監査で適用した基準等 |
| 10 | 監査結果概要（総括） | 監査結果の総括 |
| 11 | 監査結果 | 監査で確認した事実（評価できる事項を含む） |
| 12 | 指摘事項 | 監査結果に基づき、問題点として指摘する事項 |
| 13 | 改善勧告 | 指摘事項を踏まえて、改善すべき事項<br>（緊急改善事項、一般的改善事項） |
| 14 | 特記事項 | その他記載すべき事項 |

（2） 監査結果の報告

情報セキュリティ監査統括責任者は、監査結果を情報セキュリティ委員会に報告する。

また、被監査部門に対して監査報告会を開催し、監査人から直接、監査結果の説明を行う。監査報告会では、被監査部門に対して次の事項を説明することが望ましい。

・集められた監査証拠は入手可能な情報のサンプルによること。

・監査報告の方法

・監査後の活動について（是正処置の実施、監査結果に対する意見対応等）

監査人は、指摘事項をより具体的に分かりやすく説明し、必要に応じて「監査調書」の内容等、監査証拠に基づいた改善のための方策等を助言する。

また、指摘事項の説明だけではなく、被監査部門において、優れた実践活動が認められる場合は、報告会で評価することが望ましい。

### 2.2.5. 監査結果への対応等

情報セキュリティ監査は、その結果を今後の情報セキュリティ対策に反映させることが必要である。情報セキュリティ対策に反映することで、情報セキュリティ対策の実施サイクル（PDCA サイクル）がはじめて回転していくことになる。

このため、CISO は、監査結果を踏まえ、監査の指摘事項を所管する被監査部門に対し、改善計画書の作成などの対処（改善計画の策定等）を指示する。また、措置が完了していない改善計画は、定期的に進捗状況の報告を指示しなければならない。

さらに、CISO は、その他の部門に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。また、庁内で横断的に改善が必要な事項については、統括情報セキュリティ責任者に対し、当該事項への対処（改善計画の策定等）を指示しなければならない。

なお、措置が完了していない改善計画は、定期的に進捗状況の報告を指示しなければならない。

指示を受けた部門は、監査結果の指摘事項について、緊急性、重要性、費用等も考慮して、必要な改善措置を検討し、CISO に対して、対応措置を報告する。

なお、緊急性が高いと判断される指摘事項については、速やかに改善措置を検討・実施するとともに、その実施状況を報告するものとし、それ以外の指摘事項については、監査終了後、半年から１年毎に実施されるフォローアップ監査で確認する。

また、情報セキュリティ委員会においては、監査結果を情報セキュリティポリシーの見直しやその他情報セキュリティ対策の見直し時に活用する。

### 2.2.6. 監査結果の公開

情報セキュリティ監査の結果については、行政の透明性確保、住民に対する説明責任遂行の観点からは積極的に公開することが望まれる。特に、行政は住民の個人情報を含め、大量の情報を扱っていること、電子自治体の取組を進めていく上で住民の信頼が必要であることに鑑みれば、情報セキュリティ監査の結果を住民に示すことは重要である。

他方、情報セキュリティ監査の成果物には、情報資産やネットワーク及び情報システム等の脆弱性に関する情報が含まれており、情報セキュリティ確保の観点からは、全てを公開することは適当ではない場合もある。

したがって、一律に公開、非公開とすることはいずれも適当ではなく、各地方公共団体の制定する情報公開条例の「不開示情報」の取扱いなどを踏まえ、適切な範囲で公開していく必要がある。

### 2.2.7. フォローアップ監査

監査報告書で指摘した改善事項について、被監査部門の対応状況を確かめるため、監査終了後、半年から 1 年毎にフォローアップ監査を実施する。フォローアップ監査は個別の監査として実施してもよいし、次回の監査の中で実施してもよい。

個別の監査として実施する場合、改善事項に対する被監査部門の対応措置が、対象監査項目を満たすものになっていることの確認及び対応措置の有効性の検証を行う必要がある。

次回の監査の中で実施する場合は、通常の監査項目に加え、前回監査における改善事項のフォローアップを行う場を設け、個別のフォローアップ監査の場合と同様、対応措置の確認と有効性の検証を行う。

なお、情報セキュリティ監査では、セキュリティ監査手順の運用サイクルが有効に機能するためにも、指摘された改善事項への対応が非常に重要となるため、フォローアップ監査を確実に実施する必要がある。

## 2.3. 外部監査人の調達

ここでは、外部監査を行う場合における外部監査人の調達方法について説明する。なお、県と県内市町村など、複数の地方公共団体が共同で外部監査人の調達を行うことによって、調達を効率化する方法もあり、実際にこのような取組も行われている。

（1） 外部監査人の調達方式

外部監査人の調達は、当該地方公共団体の調達基準や手続にしたがって行われるが、特に、監査の客観性、公正性等の観点から、委託事業者の決定の透明性と公平性の確保には特に留意する必要がある。

外部監査の委託事業者の調達方式には、次のような方式があり得る。

- 公募型プロポーザル方式（企画提案書を評価して判断して事業者を選定）
- 総合評価入札方式（価格と技術的要素を総合的に判断して事業者を選定）
- 一般競争入札方式（最も安価な価格を提示した事業者と契約）
- 条件付き一般競争入札方式（一定の条件を満たす事業者の中で、最も安価な価格を提示した事業者と契約）

（2） 企画提案書の書式作成

公募型プロポーザル方式により情報セキュリティ監査に関する企画提案を求める場合は、「企画提案書」を作成する。企画提案書には、情報セキュリティ監査業務の受託を希望する提案者が、業務委託仕様書に基づいて、当該監査に関する考え方、実施方法、実施体制等の具体的な内容を記述する（図表 2.8）。また、委託業務内容に加えて、費用の見積りに必要となる事項も併せて記載する。例えば、ネットワークへの侵入検査を行う場合には、対象サーバ数や IP アドレス数などの対象、範囲、実施の程度等の詳細な記載があれば、企画提案者の費用積算は精緻なものになり、より正確な見積りが期待できる。

情報セキュリティ監査統括責任者は、委託事業者による監査に責任を持つ必要がある。委託事業者による監査を情報セキュリティポリシーの見直しにつなげていくためにも、企画提案書の内容を確認し、監査の品質を担保できる委託事業者を選定することが求められる。

図表 2.8　企画提案書に記載する事項（例）

| | 項目 | 内容 |
|---|---|---|
| 1 | 監査期間 | 委託する監査の期間 |
| 2 | 監査実施内容 | 委託する監査業務の内容<br>ⅰ)目的<br>ⅱ)本業務の対象範囲<br>ⅲ)準拠する基準<br>ⅳ)監査のポイント　　等 |
| 3 | 監査内容 | ⅰ)事前打合せ<br>ⅱ)事前準備依頼事項<br>・事前の提出資料<br>・アンケート等の有無　等<br>ⅲ)監査実施計画書作成<br>ⅳ)予備調査<br>ⅴ)本調査<br>※機器又は情報システムに対して情報システム監査ツールを使用する場合はその名称も記載<br>ⅵ)監査報告書作成<br>ⅶ)監査報告会 |
| 4 | 監査スケジュール | 上記 3 の概略スケジュール<br>※詳細は監査人決定後に求める。 |
| 5 | 監査実施体制 | ⅰ)監査責任者・監査人・監査補助者・アドバイザー等の役割、氏名を含む監査体制図<br>ⅱ)当該団体との役割分担 |
| 6 | 監査品質を確保するための体制 | ⅰ）監査品質管理責任者・監査品質管理者等の役割、氏名を含む監査品質管理体制図<br>ⅱ）監査品質管理に関する規程　等 |
| 7 | 監査人の実績等 | ⅰ)組織としての認証資格等<br>※例えば、ISMS 認証やプライバシーマーク認証、情報セキュリティサービス基準適合サービスリスト（うちセキュリティ監査サービスに係る部分）への登録等<br>ⅱ)監査メンバーの保有資格・技術スキル・地方公共団体を含む実務経験等　（※注１） |
| 8 | 監査報告書の目次体系 | 監査報告書の目次体系（章立て）<br>ⅰ)総括<br>ⅱ)情報セキュリティ監査の実施の概要<br>ⅲ)評価できる事項<br>ⅳ)改善すべき事項(緊急改善事項・一般的改善事項のまとめ)<br>ⅴ)監査結果の詳細<br>ⅵ)添付資料（補足資料等） |
| 9 | 成果物 | 最終成果物（納品物）一覧 |
| 10 | その他 | 会社案内、パンフレット等必要な添付書類 |

（※注１）監査メンバーの保有資格は、以下を参照することが望ましい。

独立行政法人 情報処理推進機構（https://www.ipa.go.jp/index.html）

・システム監査技術者

・情報処理安全確保支援士

特定非営利活動法人 日本セキュリティ監査協会（https://www.jasa.jp/）

・公認情報セキュリティ監査人

ISACA（https://engage.isaca.org/japanesechapters/aboutus）

・公認情報システム監査人

・公認情報セキュリティマネジャー

一般財団法人 日本要員認証協会（https://www.jrca-jsa.or.jp/）

・ISMS 審査員

特定非営利活動法人 日本システム監査人協会（https://www.saaj.or.jp/）

・公認システム監査人

国際情報システムセキュリティ認証コンソーシアム（https://japan.isc2.org/）

・公認情報システムセキュリティ専門家

（３） 業務委託仕様書の作成

入札方式による場合、事前に業務委託の内容を業務委託仕様書としてまとめ、入札に応じる民間事業者、団体等に提示する。また、業務委託仕様書の添付資料に選定基準の概要や提案書の評価基準を開示するとよい。

業務委託仕様書には、監査目的、監査対象、適用基準等の記載に加えて、当該地方公共団体が実施する情報セキュリティ監査に関する方針、実施条件等、どのような監査を実施したいかを正確かつ具体的に記載することが重要である（図表 2.9）。

なお、付録に「情報セキュリティ監査業務委託仕様書」の例を挙げているので参照されたい。

図表 2.9 業務委託仕様書に記載する事項（例）

| | 項目 | 内容 |
|---|---|---|
| 1 | 業務名 | 委託する業務の名称 |
| 2 | 監査目的 | 監査を実施する目的 |
| 3 | 発注部署 | 監査を委託する部署名 |
| 4 | 監査対象 | 監査対象の業務、情報システムなどの範囲 |
| 5 | 業務内容 | 委託する監査業務の内容 |
| 6 | 適用基準 | 監査を行う際、準拠すべき基準や参考とする基準を記載 |
| 7 | 監査人の要件 | 受託者及び監査人の要件 |
| 8 | 監査期間 | 委託する監査の期間 |
| 9 | 監査報告書の様式 | 監査報告書の作成様式、宛名 |

| | | |
|---|---|---|
| 10 | 監査報告書の提出先 | 監査報告書を提出する部署 |
| 11 | 監査報告会 | 監査結果を報告する会議等の内容 |
| 12 | 監査成果物と納入方法 | 委託した監査業務の成果物と納入の方法 |
| 13 | 成果物の帰属 | 成果物及びこれに付随する資料の帰属 |
| 14 | 委託業務の留意事項 | 再委託、資料の提供、秘密保持等の留意事項 |
| 15 | その他 | その他の事項 |

（4） 契約部門等との調整

委託事業者の決定までの間に、調達事務を行う契約部門、出納部門等と調整し、委託業務契約書に盛り込む事項や個人情報保護に関する措置等を検討する。

特に、外部監査人は、地方公共団体の情報セキュリティにおける脆弱性を知ることになるので、情報資産に関する守秘義務等を契約書上どのように規定するか十分な検討が必要である。

なお、外部監査人が個人情報を扱うことが想定される場合には、個人情報保護法施行条例に従い、個人情報の適切な管理のため必要な措置を講じなければならない。

（5） 委託事業者との契約締結

委託事業者が決定すれば、地方公共団体と外部委託事業者との間で契約を締結することになる。委託事業者は、監査対象と直接の利害関係がないことを確認して選定する必要がある。

契約に当たっての主な合意事項は下記のとおりである。業務委託契約書の記載例については、付録の「情報セキュリティ監査業務委託契約書(例)」を参照されたい。

・目的、対象、範囲を含む監査内容に関する事項
・成果物（納品物）に関する事項
・監査報告書の記載内容に関する事項

契約には、監査人が監査業務上知り得た情報や監査内容を関係者以外に開示したり、監査人から情報が漏えいしないよう、監査人の守秘義務に係る規定や監査人における監査結果の管理方法についても規定を明記しなければならない。

また、契約の適正な履行を確保するため、監査目的、監査対象、監査方針、実施条件、計画、実施、報告を含む主たる実施手順、準拠規範、監査技法、収集すべき監査証拠の範囲等の監査品質、対価の決定方法、金額と支払の時期、支払方法、中途終了時の精算、負担すべき責任の範囲等を明確に定め、監督、検査の判断基準を明確にすることが必要である。なお、地方公共団体が契約保証金の納付を求めた場合、「契約の相手方が契約上の義務を履行しないとき」、すなわち、監査品質が所定の水準に達しないときは、契約において別段の定めをしない限り契約保証金は地

方公共団体に帰属する。

付録の「情報セキュリティ監査業務委託契約書（例）」では、情報セキュリティ監査特有の部分のみを取り上げている。その他の事項である履行方法、契約保証人、保証契約、前払い金、損害賠償、権利義務の譲渡禁止、再委託、一括下請けの禁止、監督員、貸与品の処理、作業の変更中止、履行期間の延長、成果物の納品と検査、所有権の移転時期、請負代金の支払時期や支払方法、瑕疵担保、委託完成保証人の責任、甲乙の解除権、解除に伴う措置、秘密保持、その他は、既に各地方公共団体にある請負契約約款（準委任とするときは準委任契約約款）を用いることができる。

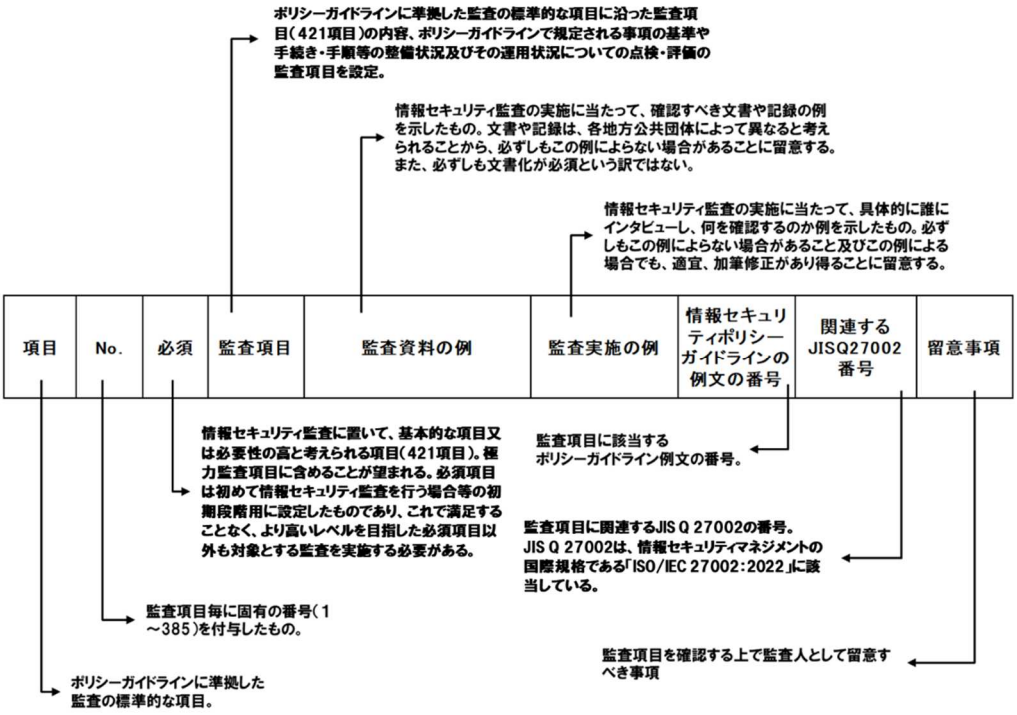
監査を継続的に行うときは、毎回業務委託契約を締結する方法と、業務委託基本契約と業務委託個別契約に分けて契約を締結する方法がある。毎回契約を締結する方法が一般的であると考えられ、付録の契約書例もこの形態を想定している。後者の基本契約と個別契約に分けて契約を締結する方法によるときは、契約書例の中から、毎回共通する事項を抜き出して基本契約として締結し、毎回定めるべき事項を個別契約で合意する。

# 第3章

# 情報セキュリティ監査項目

# 第3章 情報セキュリティ監査項目

情報セキュリティ監査項目は、以下の構成となっている。




（注）監査項目の趣旨や運用上の留意点を理解するため、総務省が令和７年 3 月の「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」の解説を併せて確認されたい。

実際の情報セキュリティ監査項目を、次頁以降に記載する。

| 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 | | (1)組織体制、権限及び責任 | 1 | ○ | **ⅰ)組織体制、権限及び責任**<br>CISOによって、情報セキュリティ対策のための組織体制、権限及び責任が定められ、文書化されている。 | □情報セキュリティポリシー<br>□権限・責任等一覧 | 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、情報セキュリティ対策に係る権限、責任、連絡体制、兼務の禁止が文書化され、正式に承認されているか確かめる。 | 1.(1)～(6)、(8) | 5.2<br>5.4 | |
| | | (2)情報セキュリティ委員会 | 2 | ○ | **ⅰ)情報セキュリティ委員会の設置**<br>CISOによって、情報セキュリティポリシー等、情報セキュリティに関する重要な事項を決定する機関(情報セキュリティ委員会)が設置されている。 | □情報セキュリティポリシー<br>□情報セキュリティ委員会設置要綱 | 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、情報セキュリティポリシー等、情報セキュリティに関する重要な事項を決定する機関(情報セキュリティ委員会)が設置されているか確かめる。 | 1.(7)① | ― | ・情報セキュリティに関する意思決定機関として情報セキュリティ委員会以外に庁議や幹部会議等を位置づけることも可能である。 |
| | | | 3 | | **ⅱ)情報セキュリティ委員会の開催**<br>情報セキュリティ委員会が毎年度開催され、情報セキュリティ対策の改善計画を策定し、その実施状況が確認されている。 | □情報セキュリティポリシー<br>□情報セキュリティ委員会設置要綱<br>□情報セキュリティ委員会議事録 | 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、情報セキュリティ委員会が毎年度開催され、リスク情報の共有や情報セキュリティ対策の改善計画を策定し、その実施状況が確認されているか確かめる。 | 1.(7)② | ― | |
| | | (3)CSIRTの設置・役割 | 4 | ○ | **ⅰ)CSIRTの設置・役割の明確化**<br>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<br>□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<br>5.6<br>5.24<br>5.25<br>5.26<br>6.8 | |
| 2. 情報資産の分類と管理 | | (1)情報資産の分類 | 5 | ○ | **ⅰ)情報資産の分類に関わる基準**<br>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、機密性・完全性・可用性に基づく情報資産の分類と分類に応じた取扱いが定められ、文書化されている。 | □情報セキュリティポリシー<br>□情報資産分類基準 | 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セキュリティ責任者へのインタビューにより、機密性・完全性・可用性に基づく情報資産の分類と分類に応じた取扱いが文書化され、正式に承認されているか確かめる。 | 2.(1) | 5.12 | |
| | | (2)情報資産の管理 | 6 | ○ | **ⅰ)情報資産の管理に関わる基準**<br>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、情報資産の管理に関わる基準が定められ、文書化されている。 | □情報セキュリティポリシー<br>□情報資産管理基準 | 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セキュリティ責任者へのインタビューにより、情報資産の管理に関わる基準が文書化され、正式に承認されているか確かめる。 | 2.(2) | 5.9<br>5.10 | |
| | | | 7 | ○ | **ⅱ)情報資産管理台帳の作成**<br>情報セキュリティ管理者によって、重要な情報資産について台帳(情報資産管理台帳、情報システム台帳)が作成されている。 | □情報資産管理基準<br>□情報資産管理台帳<br>□情報システム台帳 | 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、重要な情報資産について台帳(情報資産管理台帳、情報システム台帳)が作成され、定期的に見直されているか確かめる。 | 2.(2)① | 5.9 | |

| 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 |
|---|---|---|---|---|---|---|---|---|
| | 8 | | **ⅲ）情報資産の分類の表示**<br>情報資産に分類が表示されている。 | □情報資産管理基準<br>□情報資産管理台帳 | 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へのインタビュー、執務室及び管理区域の視察により、情報資産に分類が表示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。 | 2.(2)② | 5.13 | ・分類の表示について、情報システムに記録される情報の分類をあらかじめ規定する方法や、表示の有無によって分類する方法などもありうる。 |
| | 9 | | **ⅳ）情報の作成**<br>情報の作成時に情報資産の分類に基づき、当該情報の分類と取扱制限が定められている。 | □情報資産管理基準<br>□情報資産管理台帳 | 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、情報の作成時に情報資産の分類に基づき、当該情報の分類と取扱制限が定め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。 | 2.(2)③ | 5.10 | |
| | 10 | | **ⅴ）情報資産の入手**<br>情報資産を入手した場合、情報資産の分類に基づき情報資産が取扱われている。また、情報資産の分類が不明な場合は、情報セキュリティ管理者に判断を仰いでいる。 | □情報資産管理基準<br>□情報資産管理台帳 | 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、情報資産を入手した場合、情報資産の分類に基づき情報資産が取扱われているか確かめる。また、情報資産の分類が不明な場合は、情報セキュリティ管理者に判断を仰いでいるか確かめる。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。 | 2.(2)④ | 5.10 | |
| | 11 | | **ⅵ）情報資産の利用**<br>情報資産は、情報資産の分類に応じて適切に取り扱われており、業務以外の目的に利用されていない。 | □情報資産管理基準<br>□情報資産管理台帳 | 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、情報資産は、情報資産の分類に応じて適切に取り扱われており、業務以外の目的に利用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。 | 2.(2)⑤ | 5.10 | |
| | 12 | | **ⅶ）情報資産の保管**<br>情報セキュリティ管理者又は情報システム管理者によって、情報資産の分類に従い、情報資産が適切に保管されている。 | □情報資産管理基準<br>□情報資産管理台帳 | 監査資料のレビューと情報セキュリティ管理者、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情報資産の保管場所の視察により、情報資産の分類に従い、情報資産が適切に保管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。 | 2.(2)⑥ | 5.10 | |
| | 13 | | **ⅷ）情報の送信**<br>機密性の高い情報を送信する場合、必要に応じ暗号化又はパスワード設定が行われている。 | □情報資産管理基準<br>□情報資産管理台帳 | 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、機密性の高い情報を送信する場合、必要に応じ暗号化又はパスワード設定等、情報の漏えいを防止するための措置が講じられているか確かめる。 | 2.(2)⑦ | 5.10<br>5.14 | 電子メール等により情報を送信する場合の暗 号化に用いるパスワード については、ポリシーガイドライン 第3編第2章 2.2.情報資産の管理 の解説(注7)も参照されたい。 |
| | 14 | | **ⅸ）情報資産の運搬**<br>車両等により機密性の高い情報資産を運搬する場合、情報セキュリティ管理者の許可を得た上で、必要に応じ鍵付きのケース等に格納し、暗号化又はパスワードの設定を行う等、情報資産の不正利用を防止するための措置がとられている。 | □情報資産管理基準<br>□情報資産管理台帳 | 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、情報資産の運搬元の視察により、機密性の高い情報資産を外部に提供する場合、情報セキュリティ管理者の許可を得た上で、必要に応じ暗号化又はパスワードの設定が行われているか確かめる。 | 2.(2)⑧ | 5.10<br>7.10 | |

別紙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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | 15 | | **ⅹ）情報資産の提供**<br>機密性の高い情報資産を外部に提供する場合、情報セキュリティ管理者の許可を得た上で、必要に応じ暗号化又はパスワードの設定が行われている。 | □情報資産管理基準<br>□情報資産管理台帳 | 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、機密性の高い情報資産を外部に提供する場合、情報セキュリティ管理者の許可を得た上で、必要に応じ暗号化又はパスワードの設定が行われているか確かめる。 | 2.(2)⑨<br>(ア)～(イ) | 5.10 | |
| | | | 16 | | **ⅺ）情報資産の公表**<br>情報セキュリティ管理者によって、住民に公開する情報資産について、完全性が確保されている。 | □情報資産管理基準<br>□情報資産管理台帳 | 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、住民に公開する情報資産について、完全性が確保されているか確かめる。 | 2.(2)⑨<br>(ウ) | 5.10 | ・完全性とは、情報が破壊、改ざん又は消去されていない状態を確保することをいう。 |
| | | | 17 | | **ⅻ）情報資産の廃棄**<br>情報資産を廃棄する場合、情報セキュリティ管理者の許可を得た上で廃棄され、行った処理について、日時、担当者及び処理内容が記録されている。 | □情報資産管理基準<br>□情報資産管理台帳<br>□情報資産廃棄記録 | 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、情報資産を廃棄する場合、情報セキュリティ管理者の許可を得て、情報の機密性に応じて適切な処理をした上で廃棄され、行った処理について、日時、担当者及び処理内容が記録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。 | 2.(2)⑩ | 5.10<br>7.10 | |
| 3.<br>情報システム全体の強靭性の向上 | | (1)マイナンバー利用事務系 | 18 | ○ | **ⅰ）マイナンバー利用事務系と他の領域との分離**<br>CISO又は統括情報セキュリティ責任者によって、マイナンバー利用事務系と他の領域が分離されており、通信できないようになっている。 | □ネットワーク管理基準<br>□通信回線敷設図<br>□結線図 | 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、マイナンバー利用事務系と他の領域が分離されており、通信できないようになっているか確かめる。 | 3.(1)① | 8.22 | |
| | | | 19 | ○ | **ⅱ）マイナンバー利用事務系と外部との接続**<br>CISO又は統括情報セキュリティ責任者によって、マイナンバー利用事務系と外部との通信は、通信経路の限定及びアプリケーションプロトコルレベルでの限定を行っており、かつ外部接続先はインターネットへ接続していない。なお、十分に安全性が確保された外部接続先との通信については、必要な対策が実施されている。 | □ネットワーク管理基準<br>□通信回線敷設図<br>□結線図 | 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、マイナンバー利用事務系と外部との通信は、通信経路の限定及びアプリケーションプロトコルレベルでの限定を行っており、かつ外部接続先はインターネットへ接続していないか確かめる。なお、十分に安全性が確保された外部接続先と通信については、必要な対策がとられているか確かめる。 | 3.(1)① | 8.22 | マイナンバー利用事務系と他の領域を通信できないようにしなければならない。ただし、マイナンバー利用事務系と外部との通信をする必要がある場合に限りは、通信経路の限定及びアプリケーションプロトコルのレベルでの限定を行わなければならない。 |
| | | | 20 | ○ | **ⅲ）端末における情報アクセス対策**<br>職員等がマイナンバー利用事務系の端末を利用する際に、二つ以上を併用する認証（多要素認証）が導入されている。 | □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、二つ以上の認証手段が併用されているか確かめる。 | 3.(1)② | 5.17<br>8.5 | |
| | | | 21 | | **ⅳ）業務毎の専用端末化**<br>マイナンバー利用事務系の端末は業務毎に専用端末化されている。 | □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、マイナンバー利用事務系の端末が専用端末であるか確かめる。 | 3.(1)② | － | |
| | | | 22 | ○ | **ⅴ）電磁的記録媒体による情報持ち出しの不可設定**<br>職員等がマイナンバー利用事務系の端末から電磁的記録媒体により情報を持ち出すことができないように設定がされている。 | □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、電磁的記録媒体により情報を持ち出すことができないように設定がされているか確かめる。 | 3.(1)② | 7.10 | |

別紙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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | (2)LGWAN接続系 | 23 | ○ | **ⅰ）LGWAN接続系とインターネット接続系の分割①**<br>CISO又は統括情報セキュリティ責任者によって、LGWAN接続系とインターネット接続系の通信環境は分離され、必要な通信のみ許可するようになっている。 | □ネットワーク管理基準<br>□通信回線敷設図<br>□結線図 | 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接続系とインターネット接続系の通信環境は分離され、必要な通信のみ許可するようにしているか確かめる。 | 3.(2)① | 8.22 | |
| | | | 24 | ○ | **ⅱ）LGWAN接続系とインターネット接続系の分割②**<br>CISO又は統括情報セキュリティ責任者によって、インターネット接続系のメールやデータをLGWAN接続系に取り込む場合は無害化通信を行っている。 | □システム構成図<br>□ネットワーク管理基準 | 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メールやデータをLGWAN接続系に取り込む場合は無害化通信を行っているか確かめる。 | 3.(2)① | 8.22 | |
| | | (3)インターネット接続系 | 25 | ○ | **ⅰ）サーバ等の監視**<br>CISO又は統括情報セキュリティ責任者によって、インターネット接続系の監視対象としてWebサーバ等のログを取得している。 | □システム構成図 | 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監視対象としてWebサーバ、メールリレーサーバ、プロキシサーバ、外部DNSサーバのログが取得されているか確かめる。 | 3.(3)① | 8.20<br>8.21 | |
| | | | 26 | ○ | **ⅱ）情報セキュリティ機器の導入**<br>CISO又は統括情報セキュリティ責任者によって、インターネット接続系に高度な情報セキュリティ機器を導入している。 | □システム構成図 | 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に高度な情報セキュリティ機器が導入されているか確かめる。 | 3.(3)① | 8.8<br>8.15<br>8.20<br>8.21 | 高度なセキュリティ機器とは、通信パケットの監視及び破棄、通信ポートの制御、不正なプログラムの検知、不審なメールの検知及び遮断、不審なURLへのアクセス遮断、ログ監視、コンテンツの改ざん検知等の機能を持った機器のことを指す。 |
| | | | 27 | | **ⅲ）情報セキュリティ運用監視**<br>CISO又は統括情報セキュリティ責任者によって、情報セキュリティ専門人材による高水準な運用監視を行っている。 | □保守体制図<br>□作業報告書 | 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は情報セキュリティ専門人材による運用監視が行われているか確かめる。 | 3.(3)① | 8.20<br>8.21 | 高水準な運用監視とは、予兆を含めた早期検知、常駐する専門人材による早期判断、及び運用委託先による24時間365日有人での集中監視のことを指す。 |
| | | | 28 | | **ⅳ）自治体情報セキュリティクラウドとの接続**<br>CISO又は統括情報セキュリティ責任者によって、庁内のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドと接続している。 | □システム構成図<br>□通信回線敷設図<br>□結線図 | 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、庁内のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドと接続しているかを確かめる。 | 3.(3)② | 8.22 | |

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|
| 4.物理的セキュリティ | 4.1.サーバ等の管理 | (1)機器の取付け | 29 | | **ⅰ)機器の設置に関わる基準及び手続**<br>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、サーバ等の機器の取付けを行う場合の基準及び手続が定められ、文書化されている。 | □機器設置基準/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、機器の設置に関わる基準及び手続が文書化され、正式に承認されているか確かめる。 | 4.1.(1) | 7.5<br>7.8 | |
| | | | 30 | ○ | **ⅱ)機器の取付け**<br>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<br>□建物フロアレイアウト図<br>□管理区域(情報システム室等)のレイアウト図<br>□機器設置記録<br>□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) | 7.5<br>7.8 | ・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)サーバの冗長化 | 31 | | **ⅰ)サーバ冗長化基準**<br>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、サーバを冗長化する基準が定められ、文書化されている。 | □サーバ冗長化基準 | 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、サーバの冗長化に関する基準が文書化され、正式に承認されているか確かめる。 | 4.1.(2)① | 8.13<br>※注意<br>JISQ27002では、広義の意味でバックアップ全般を規定している。 | ・サーバの冗長化には、ハードウェア・ソフトウェアが二重に必要となる等、多額の費用を要する。冗長化にかかる費用とサーバ等の停止による損失の影響度合いを十分に検討したうえで、冗長化を行うか否かを判断することが望ましい。 |
| | | | 32 | | **ⅱ)基幹サーバの冗長化**<br>情報システム管理者によって、基幹サーバ(重要情報を格納しているサーバ、セキュリティサーバ、住民サービスに関するサーバ及びその他の基幹サーバ)が冗長化されている。 | □サーバ冗長化基準<br>□システム構成図 | 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、基幹サーバが冗長化され、同一データが保持されているか確かめる。 | 4.1.(2)① | 8.13<br>※注意<br>JISQ27002では、広義の意味でバックアップ全般を規定している。 | |
| | | | 33 | ○ | **ⅲ)サーバ障害対策基準**<br>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<br>□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 | 6.8<br>8.13 | |
| | | (2)サーバの冗長化 | 34 | | **ⅳ)サーバ障害対策**<br>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に、システムの運用停止時間を最小限にする対策が講じられている。 | □サーバ障害対策基準<br>□サーバ障害対応実施手順書<br>□障害報告書 | 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により、サーバ障害時にセカンダリサーバが起動され、システムの運用停止時間が最小限になるような対策が講じられているか確かめる。実際にサーバ障害が発生している場合は、対策が有効に機能しているか確かめる。 | 4.1.(2)② | 6.8<br>8.13 | ・定期保守等で予備機への切替試験等を実施し、その記録を確認することが望ましい。<br>・定期保守については、No.43～44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 |
|---|---|---|---|---|---|---|---|---|
| (3)機器の電源 | 35 | | **ⅰ)機器の電源に関わる基準**<br>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、停電や落雷等からサーバ等の機器を保護する基準が定められ、文書化されている。 | □機器電源基準 | 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、停電等に備えた予備電源の設置基準や、落雷等の電源異常からサーバ等の機器を保護するための基準が文書化され、正式に承認されているか確かめる。 | 4.1.(3)① | 7.8<br>7.11 | |
| | 36 | ○ | **ⅱ)予備電源装置の設置及び点検**<br>情報システム管理者によって、停電等による電源供給の停止に備えた予備電源が備え付けられ、定期的に点検されている。 | □機器電源基準<br>□システム構成図<br>□機器設置記録<br>□機器保守点検記録<br>□障害報告書 | 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及び管理区域の視察により、UPS(無停電電源装置)などの予備電源が設置されているか確かめる。また、停電時や瞬断時に起動し、当該機器が適切に停止するまでの間に十分な電力を供給できる容量があるかなど、定期的に点検されているか確かめる。 | 4.1.(3)① | 6.8<br>7.8<br>7.11 | ・設置した予備電源が、サーバ等の増設に対して十分な電力供給能力があるのかを定期的に確認しておくことが望ましい。 |
| | 37 | | **ⅲ)過電流対策**<br>情報システム管理者によって、落雷等による過電流からサーバ等の機器を保護する設備が備えられている。 | □機器電源基準<br>□システム構成図<br>□機器設置記録<br>□障害報告書 | 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及び管理区域の視察により、落雷等による過電流からサーバ等の機器を保護するために、避雷設備やCVCF(定電圧定周波装置)を設置するなどの措置が講じられているか確かめる。 | 4.1.(3)② | 6.8<br>7.8<br>7.11 | |
| (4)通信ケーブル等の配線 | 38 | | **ⅰ)通信ケーブル等の配線に関わる基準及び手続**<br>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、通信ケーブル等の配線に関わる基準及び手続が定められ、文書化されている。 | □通信ケーブル等配線基準/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、通信ケーブルや電源ケーブルの配線基準やネットワーク接続口(ハブのポート等)設置基準、配線申請・変更・追加等の手続が文書化され、正式に承認されているか確かめる。 | 4.1.(4)① | 7.12 | |
| | 39 | ○ | **ⅱ)通信ケーブル等の保護**<br>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、通信ケーブルや電源ケーブルの損傷等を防止するための対策が講じられている。 | □通信ケーブル等配線基準/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及び執務室や管理区域の視察により、通信ケーブルや電源ケーブルが配線収納管に収納されるなど、損傷から保護されているか確かめる。 | 4.1.(4)① | 7.12<br>7.13 | ・情報処理設備に接続する通信ケーブル及び電源ケーブルは、可能ならば施設内の地下に埋設するか又はそれに代わる十分な保護手段を施すことが望ましい。<br>・ケーブルの損傷等を防止するために、配線収納管を使用することが望ましい。<br>・ケーブル用途(電源、通信等)で分離して配線することが望ましい。また、通信ケーブルを二重化している場合は、それぞれを別ルートで配線することが望ましい。 |
| | 40 | | **ⅲ)ケーブル障害対策**<br>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、通信ケーブル及び電源ケーブルの損傷等への対応が行われている。 | □通信ケーブル等配線基準/手続<br>□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、通信ケーブルや電源ケーブルの損傷等に対し、施設管理部門と連携して対応しているか確かめる。 | 4.1.(4)② | 6.8<br>7.12 | |

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | 41 | | **ⅳ）ネットワーク接続口の設置場所**<br>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、ネットワーク接続口（ハブのポート等）が他者が容易に接続できない場所に設置されている。 | □通信ケーブル等配線基準/手続<br>□通信回線敷設図 | 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執務室や管理区域の視察により、ネットワーク接続口（ハブのポート等）が他者の容易に接続できない場所に設置されているか確かめる。 | 4.1.(4)③ | 7.8<br>7.12 | |
| | | | 42 | | **ⅴ）配線変更・追加の制限**<br>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、配線の変更及び追加が許可された者だけに制限されている。 | □通信ケーブル等配線基準/手続<br>□作業報告書 | 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、統括情報セキュリティ責任者、情報システム管理者、情報システム担当者及び契約した委託事業者だけが配線の変更及び追加の作業を行っていることを確かめる。 | 4.1.(4)④ | 7.12<br>8.32 | |
| | | (5)機器の定期保守及び修理 | 43 | | **ⅰ）機器の保守・修理に関わる基準及び手続**<br>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、サーバ等の機器の定期保守・修理に関わる基準及び手続が定められ、文書化されている。 | □機器保守・修理基準/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、サーバ等の機器の保守・修理に関わる基準及び手続が文書化され、正式に承認されているか確かめる。 | 4.1.(5) | 7.13 | |
| | | | 44 | ○ | **ⅱ）サーバ等の機器の定期保守**<br>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<br>□保守機器管理表<br>□保守体制図<br>□作業報告書<br>□障害報告書<br>□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 | 7.13 | |
| | | | 45 | ○ | **ⅲ）電磁的記録媒体を内蔵する機器の修理**<br>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<br>□保守機器管理表<br>□保守体制図<br>□作業報告書<br>□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 | 5.20<br>5.31<br>5.36<br>7.13 | |
| | | (6)庁外への機器の設置 | 46 | | **ⅰ）庁外への機器設置に関わる基準及び手続**<br>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、庁外にサーバ等の機器を設置する場合の基準及び手続が定められ、文書化されている。 | □機器設置基準/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、庁外にサーバ等の機器を設置する場合の基準及び手続が文書化され、正式に承認されているか確かめる。 | 4.1.(6) | 7.9<br>7.10 | ・地方公共団体の庁外の装置を保護するために、十分な措置が取られていることが望ましい。<br>・損傷、盗難、傍受といったセキュリティリスクを考慮し、それぞれの場所に応じた最も適切な管理策を導入することが望ましい。 |
| | | | 47 | | **ⅱ）庁外への機器の設置の承認**<br>統括情報セキュリティ責任者及び情報システム管理者は、庁外にサーバ等の機器を設置する場合、CISOの承認を得ている。 | □機器設置基準/手続<br>□庁外機器設置申請書／承認書<br>□情報資産管理台帳 | 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、庁外に設置しているサーバ等の機器が、CISOに承認されているか確かめる。<br>また、情報資産管理台帳を確認し、庁外に設置していることが記載されているか確かめる。 | 4.1.(6) | 7.9<br>7.10 | |



別紙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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | 48 | | **ⅲ）庁外の機器の設置状況確認**<br>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、庁外に設置しているサーバ等の機器への情報セキュリティ対策状況が定期的に確認されている。 | □機器設置基準/手続<br>□委託事業者訪問記録<br>□委託事業者監査報告書<br>□委託事業者におけるISO/IEC27001認証取得状況 | 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、庁外に設置された機器への情報セキュリティ対策状況が、定期的に確認されているか確かめる。 | 4.1.(6) | 5.36<br>7.9<br>7.10 | |
| | | (7)機器の廃棄等 | 49 | | **ⅰ）機器の廃棄等に関わる基準及び手続**<br>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、機器の廃棄又はリース返却等を行う場合の基準及び手続が定められ、文書化されている。 | □機器廃棄・リース返却基準<br>□機器廃棄・リース返却手続 | 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、機器を廃棄又はリース返却する場合の基準及び手続が文書化され、正式に承認されているか確かめる。 | 4.1.(7) | 7.14 | ・委託契約等により、サービス提供を受けている業務においても留意する必要がある。 |
| | | | 50 | ○ | **ⅱ）記憶装置の情報消去**<br>情報システム管理者によって、廃棄又はリース返却する機器内部の記憶装置からすべての情報が消去され、復元が不可能な状態にされている。 | □機器廃棄・リース返却基準<br>□機器廃棄・リース返却手続<br>□情報資産管理台帳<br>□記憶装置廃棄記録 | 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、機器内部の記憶装置からすべてのデータが復元が不可能なように消去されているか確かめる。 | 4.1.(7) | 7.14 | ・委託契約等により、サービス提供を受けている業務においても留意する必要がある。 |
| | 4.2.<br>管理区域(情報システム室等)の管理 | (1)<br>管理区域の構造等 | 51 | | **ⅰ）管理区域の構造基準**<br>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、管理区域の構造についての基準が定められ、文書化されている。 | □管理区域構造基準<br>□建物フロアレイアウト図<br>□敷地図面<br>□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により、管理区域の構造基準が文書化され、正式に承認されているか確かめる。<br>また、情報システム室や電磁的記録媒体の保管庫が管理区域に指定されているか確かめる。 | 4.2.(1)① | 7.1 | ・管理区域の中に特にセキュリティ要求事項の高い領域が存在するときは、他の領域との間に、物理的アクセスを管理するための障壁及び境界を追加することが望ましい。 |
| | | | 52 | | **ⅱ）管理区域の配置**<br>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、管理区域が自然災害の被害から考慮された場所であって、かつ外部からの侵入が容易にできない場所に設けられている。 | □建物フロアレイアウト図<br>□敷地図面<br>□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、管理区域が地階又は1階に設けられていないか、外壁が無窓になっているか確かめる。 | 4.2.(1)② | 7.1<br>7.5 | ・管理区域の存在そのものを外部の者から分からないように表示等を明示しないことが望ましい。 |
| | | | 53 | ○ | **ⅲ）管理区域への立ち入り制限機能**<br>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<br>□敷地図面<br>□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)③ | 7.1 | ・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。 |
| | | | 54 | ○ | **ⅳ）情報システム室内の機器の耐震、防火、防水対策**<br>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、情報システム室内の機器等に耐震、防火、防水等の対策が施されている。 | □建物フロアレイアウト図<br>□敷地図面<br>□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情報システム室の視察により、機器等に耐震、防火、防水等の対策が実施されているか確かめる。 | 4.2.(1)④ | 7.1<br>7.5 | |



別紙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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | 55 | | **ⅴ）管理区域の構造**<br>統括情報セキュリティ責任者及び情報セキュリティ管理者によって、管理区域を囲む外壁等の床下開口部が塞がれている。 | □建物フロアレイアウト図<br>□敷地図面<br>□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、管理区域を囲む外壁等の床下開口部がすべて塞がれているか確かめる。 | 4.2.(1)⑤ | 7.1<br>7.5 | |
| | | | 56 | | **ⅵ）管理区域の消火機器**<br>統括情報セキュリティ責任者及び情報セキュリティ管理者によって、管理区域に配置する消火薬剤や消防用設備等が、機器等及び電磁的記録媒体に影響を与えないようにされている。 | □建物フロアレイアウト図<br>□敷地図面<br>□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、管理区域に配置する消火薬剤や消防用設備等が、機器等及び電磁的記録媒体に影響を与えないように配慮されているか確かめる。 | 4.2.(1)⑥ | 7.5 | ・管理区域に配置する消火薬剤は、発泡性のものを避けるべきである。また、情報システム機器等に水がかかる位置にスプリンクラーを設置してはならない。 |
| | | (2)<br>管理区域の入退室管理等 | 57 | | **ⅰ）管理区域への入退室に関わる基準及び手続**<br>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、管理区域への入退室に関わる基準及び手続が定められ、文書化されている。 | □管理区域入退室基準／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、管理区域への入退室の基準及び手続が文書化され、正式に承認されているか確かめる。 | 4.2.(2) | 7.2 | |
| | | | 58 | ○ | **ⅱ）管理区域への入退室制限**<br>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<br>□管理区域入退室記録<br>□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。<br>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 | 7.2 | ・ 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。<br>・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。<br>・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。 |
| | | | 59 | | **ⅲ）身分証明書等の携帯**<br>情報システム管理者によって、職員等及び委託事業者が管理区域に入室する際は、身分証明書等を携帯させ、求めに応じて提示させている。 | □管理区域入退室基準／手続 | 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、職員等及び委託事業者の身分証明書の携帯状況や、身分証明書等を携帯していない者への身分証明書等の提示を促しているか確かめる。 | 4.2.(2)② | 7.2 | |

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | 60 | | **ⅳ）外部訪問者の立ち入り区域制限及び区別**<br>外部訪問者が管理区域に入る場合、情報システム管理者によって、必要に応じて立ち入り区域が制限され、当該区域への入退室を許可されている職員が同行するとともに外見上職員等と区別できる対策が講じられている。 | □管理区域入退室基準/手続<br>□管理区域入退室記録 | 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、外部からの訪問者が管理区域に入る場合、立ち入り区域の制限や、当該区域への入退室を許可されている職員の同行、ネームプレート等の着用を行っているか確かめる。 | 4.2.(2)③ | 7.2 | |
| | | | 61 | ○ | **ⅴ）管理区域への機器等の持込み制限**<br>情報システム管理者によって、機密性の高い情報資産を扱うシステムを設置している管理区域に当該情報システムに関連しない、または個人所有である機器等を持ち込ませていない。 | □管理区域入退室基準/手続<br>□管理区域入退室記録 | 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、機密性2以上の情報資産を扱うシステムを設置している管理区域への入室の際、当該情報システムに関連しない、又は個人所有であるコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等を持ち込ませていないか確かめる。 | 4.2.(2)④ | 7.6 | |
| | | (3)<br>機器等の搬入出 | 62 | | **ⅰ）管理区域への機器等の搬入出に関わる基準及び手続**<br>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、管理区域に機器等を搬入出する場合の基準及び手続が定められ、文書化されている。 | □機器搬入出基準/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、管理区域への機器等の搬入出に関わる基準及び手続が文書化され、正式に承認されているか確かめる。 | 4.2.(3) | 7.2<br>7.6 | ・可能であれば許可されていないアクセスを避けるために、搬入口は管理区域から離すことが望ましい。 |
| | | | 63 | | **ⅱ）機器等の搬入**<br>情報システム管理者によって、機器等の搬入の際は、あらかじめ職員又は委託した業者に既存の情報システムに与える影響について確認させている。 | □機器搬入出基準/手続 | 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、職員又は委託した業者が搬入する機器等が既存の情報システムに影響を与えないか確認しているか確かめる。 | 4.2.(3)① | 7.2<br>7.6 | |
| | | | 64 | ○ | **ⅲ）機器等の搬入出時の立会い**<br>情報システム管理者によって、管理区域への機器の搬入出の際は、職員を立ち会わせている。 | □機器搬入出基準/手続<br>□管理区域入退室記録<br>□機器搬入出記録 | 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、機器等の搬入出の際に職員が立会っているか確かめる。 | 4.2.(3)② | 7.2<br>7.6 | |
| | 4.3.<br>通信回線及び通信回線装置の管理 | | 65 | | **ⅰ）通信回線及び通信回線装置に関わる基準**<br>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、庁内の通信回線及び通信回線装置の管理基準が定められ、文書化されている。 | □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、庁内の通信回線及び通信回線装置の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。 | 4.3. | 5.15<br>8.20 | |
| | | | 66 | ○ | **ⅱ）通信回線及び通信回線装置の管理**<br>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、庁内の通信回線及び通信回線装置が管理基準に従って管理されている。 | □ネットワーク管理基準<br>□通信回線敷設図<br>□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、通信回線及び通信回線装置の管理状況について確かめる。<br>また、執務室や管理区域の視察により、ネットワークの配線状況を確かめる。 | 4.3.① | 5.15<br>8.20 | |



別紙3

別紙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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | 67 | | **iii）通信回線及び通信回線装置に関する文書の保管**<br>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、庁内の通信回線及び通信回線装置に関連する文書が適切に保管されている。 | □ネットワーク管理基準<br>□通信回線敷設図<br>□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及び文書保管場所の視察により、通信回線及び通信回線装置に関連する文書が適切に保管されていることを確かめる。 | 4.3.① | 5.15<br>8.20 | ・通信回線敷設図、結線図の電子ファイルについてもアクセス制限やパスワード設定など、外部への漏えい防止対策を講じる必要がある。 |
| | | | 68 | | **iv）通信回線装置のセキュリティ対策**<br>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、情報システムのセキュリティ要件として策定した情報システムのネットワーク構成に関する要件内容に従い、通信回線装置に対して適切なセキュリティ対策が実施されている。 | □ネットワーク管理基準<br>□通信回線敷設図<br>□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、通信回線装置に対するセキュリティ対策が適切に実施されていることを確かめる。 | 4.3.② | 7.8 | |
| | | | 69 | | **v）外部ネットワーク接続ポイントの制限**<br>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、外部ネットワークへの接続ポイントが必要最低限に限定されている。 | □ネットワーク管理基準<br>□通信回線敷設図<br>□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、必要以上に外部ネットワークへの接続ポイントが設けられていないか確かめる。 | 4.3.③ | 5.15<br>8.20 | |
| | | | 70 | | **vi）行政系ネットワークの集約**<br>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、行政系のネットワークが総合行政ネットワーク（LGWAN）に集約されている。 | □ネットワーク管理基準<br>□通信回線敷設図<br>□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、行政系のネットワークが総合行政ネットワーク（LGWAN）に集約されているか確かめる。 | 4.3.④ | － | ・合理的な理由がある場合は、集約されないこともありうる。 |
| | | | 71 | | **vii）通信回線の選択**<br>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、機密性の高い情報資産を取り扱う情報システムに接続している通信回線がある場合、適切な回線が選択されている。 | □ネットワーク管理基準<br>□通信回線敷設図<br>□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、機密性2以上の情報資産を取り扱う情報システムに通信回線を接続する場合、セキュリティ水準に見合った適切な回線が選択されているか確かめる。 | 4.3.④ | 5.15<br>8.20 | ・例えば、機密性の高い情報資産を扱う場合には、専用線かVPN回線等を用いること。 |
| | 4.3.<br>通信回線及び通信回線装置の管理 | | 72 | | **viii）送受信情報の暗号化**<br>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、機密性の高い情報を送受信する場合、必要に応じ、情報の暗号化が行われている。 | □ネットワーク管理基準<br>□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、機密性2以上の情報を送受信する場合、必要に応じ、情報の暗号化が行われているか確かめる。 | 4.3.④ | 5.15<br>8.20 | ・暗号化については、No.198～201も関連する項目であることから参考にすること。 |
| | | | 73 | | **ix）通信回線のセキュリティ対策**<br>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、不正な通信の有無を監視する等の対策が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。 | 4.3.⑥ | 8.20<br>8.21 | ・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。<br>・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。 |

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | 74 | | **ｘ）通信回線装置の脆弱性対応**<br>統括情報セキュリティ責任者によって、通信回線装置が動作するために必要なソフトウェアに関する事項を含む実施手順が定められており、必要なソフトウェアの状態等が調査されている。また、認識した脆弱性等について対策を講じている。 | □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へのインタビューにより、通信回線装置が動作するために必要なソフトウェアに関する事項を含む実施手順が定められていることを確認する。また、必要なソフトウェアの状態等が調査され、認識した脆弱性等について対策が実施されているかを確認する。 | 4.3.⑦ | 8.8 | |
| | | | 75 | | **ⅺ）通信回線の可用性**<br>統括情報セキュリティ責任者によって、可用性2以上の情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線が選択されている。 | □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へのインタビューにより、可用性2以上の情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線が選択されているか確かめる。また、必要に応じ、回線を冗長構成にする等の措置が講じられているか確かめる。 | 4.3.⑧ | 8.14<br>8.21 | |
| | 4.4.<br>職員等の利用する端末や電磁的記録媒体等の管理 | | 76 | | **ⅰ）パソコン等の端末の管理基準**<br>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、執務室等のパソコン等の端末の管理基準が定められ、文書化されている。 | □パソコン等管理基準 | 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、執務室等のパソコン等の端末の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。 | 4.4. | 7.8 | ・定期的に端末管理台帳と実数を点検し、紛失、盗難等の情報セキュリティインシデントの早期発見に努めることが望ましい。 |
| | | | 77 | | **ⅱ）パソコン等の端末の盗難防止対策**<br>情報システム管理者によって、執務室等のパソコン等の端末に盗難防止対策が講じられている。 | □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視察により、パソコン等の端末のワイヤー固定、モバイル端末及び電磁的記憶媒体の使用時以外の施錠保管等の盗難防止の対策が講じられているか確かめる。 | 4.4.① | 7.8 | |
| | | | 78 | | **ⅲ）電磁的記録媒体の盗難防止対策**<br>情報システム管理者によって、電磁的記録媒体の盗難防止対策が講じられている。 | □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視察により、電磁的記録媒体について、情報が保存される必要がなくなった時点で記録した情報が消去されているか確かめる。 | 4.4.① | 7.8 | |
| | | | 79 | ○ | **ⅳ）ログイン認証設定**<br>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 | 5.16<br>5.17<br>5.18<br>8.5 | ・パスワードの管理及び取扱いについては、No.137～143、244～246も関連する項目であることから参考にすること。<br>・ログイン時のシステム設定については、No.243も関連する項目であることから参考にすること。 |



別紙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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | 80 | | **v）パスワードの併用**<br>情報システム管理者によって、端末の電源起動時のパスワード（BIOSパスワード、ハードディスクパスワード等）の併用が行われている。 | □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、BIOSパスワード、ハードディスクパスワード等が併用されているか確かめる。 | 4.4.③ | 5.17 | ・管理用パスワードは必要最小限の者で管理されること。<br>・担当変更等が実施された場合は、同時にパスワードを変更することが望ましい。 |
| | | | 81 | ○ | **vi）多要素認証の利用**<br>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。 | 4.4.④ | 5.16<br>5.18 | ・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。 |
| | | | 82 | | **vii）暗号化機能の利用**<br>情報システム管理者によって、パソコン等の端末の暗号化機能又は端末に搭載されているセキュリティチップの機能が有効に利用されている。 | □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パソコン等のサンプリング確認により、データの暗号化機能又は端末に搭載されているセキュリティチップの機能が有効に利用されているか確かめる。 | 4.4.⑤ | 8.24 | |
| | | | 83 | | **viii）電磁的記録媒体の暗号化**<br>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。 | 4.4.⑤ | 8.24 | |
| | | | 84 | | **ix）遠隔消去機能の利用**<br>情報システム管理者によって、モバイル端末の庁外での業務利用の際に、遠隔消去機能等の措置が講じられている。 | □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モバイル端末のサンプリング確認により、遠隔消去機能が利用されているか確かめる。 | 4.4.⑥ | 7.9<br>7.10 | |
| 5.<br>人的セキュリティ | 5.1.<br>職員等の遵守事項 | (1)<br>職員等の遵守事項<br>①<br>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**<br>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<br>□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**<br>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<br>□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。 |

| 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)<br>職員等の遵守事項<br>②<br>業務以外の目的での使用の禁止 | 87 | | **ⅰ)情報資産等の利用基準**<br>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を禁止することが定められ、文書化されている。 | □情報セキュリティポリシー<br>□情報資産取扱基準<br>□ネットワーク利用基準<br>□電子メール利用基準 | 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、職員等の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の禁止について文書化され、正式に承認されているか確かめる。 | 5.1.(1)② | － | |
| | 88 | ○ | **ⅱ)情報資産等の業務以外の目的での使用禁止**<br>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<br>□電子メール送受信ログ<br>□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 | － | |
| (1)<br>職員等の遵守事項<br>③<br>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 | 89 | | **ⅰ)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基準及び手続**<br>CISOによって、機密性、可用性、完全性の高い情報資産を外部で処理する場合の安全管理措置の基準及び手続が定められ、文書化されている。 | □端末等持出・持込基準/手続<br>□庁外での情報処理作業基準/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セキュリティ責任者へのインタビューにより、機密性2以上、可用性2、完全性2の情報資産を外部で処理する場合の安全管理措置について文書化され、正式に承認されているか確かめる。 | 5.1.(1)③ | 6.7<br>7.9<br>8.1 | ・損傷・盗難・傍受といったセキュリティリスクを考慮し、作業場所に応じた最も適切な管理策を導入することが望ましい。<br>・外部で業務を行うために端末等を使用する場合の情報セキュリティ対策は、庁内の安全対策に加え、安全管理に関する追加的な措置をとることが望ましい。 |
| | 90 | ○ | **ⅱ)情報資産等の外部持出制限**<br>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<br>□庁外での情報処理作業基準/手続<br>□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<br>(イ) | 6.7<br>7.9<br>8.1 | ・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**<br>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<br>□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<br>(ウ) | 6.7<br>7.9<br>8.1 | ・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。 |

別紙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 |
|---|---|---|---|---|---|---|---|---|---|
| | (1)<br>職員等の遵守事項<br>④<br>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**<br>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<br>□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<br>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**<br>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<br>□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 | 6.7<br>7.8<br>7.9<br>8.1 | |
| | | 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**<br>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<br>□支給以外のパソコン等使用申請書/承認書<br>□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<br>8.21 | |
| | (1)<br>職員等の遵守事項<br>⑤<br>持ち出し及び持ち込みの記録 | 95 | | **ⅰ）端末等の持出・持込基準及び手続**<br>統括情報セキュリティ責任者又は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に関わる基準及び手続が定められ、文書化されている。 | □端末等持出・持込基準/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セキュリティ責任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に関わる基準及び手続が文書化され、正式に承認されているか確かめる。 | 5.1.(1)⑤ | 7.1 | |
| | | 96 | ○ | **ⅱ）端末等の持出・持込記録の作成**<br>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<br>□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。 |

| 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 ⑥ パソコンやモバイル端末におけるセキュリティ設定変更の禁止 | 97 | | **ⅰ)パソコンやモバイル端末におけるセキュリティ設定変更基準及び手続**<br>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、パソコンやモバイル端末におけるセキュリティ設定変更に関わる基準及び手続について定められ、文書化されている。 | □端末等セキュリティ設定変更基準/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セキュリティ責任者へのインタビューにより、パソコンやモバイル端末におけるセキュリティ設定を変更する場合の基準及び手続が文書化され、正式に承認されているか確かめる。 | 5.1.(1)⑥ | 8.32 | |
| | 98 | | **ⅱ)パソコンやモバイル端末におけるセキュリティ設定変更制限**<br>情報セキュリティ管理者による許可なく、パソコンやモバイル端末におけるセキュリティ設定は変更されていない。 | □セキュリティ設定変更申請書/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、パソコンやモバイル端末におけるセキュリティ設定の変更が必要な場合は、情報セキュリティ管理者の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)⑥ | 8.32 | |
| (1) 職員等の遵守事項 ⑦ 机上の端末等の管理 | 99 | | **ⅰ)机上の端末等の取扱基準**<br>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、離席時のパソコン、モバイル端末、電磁的記録媒体、文書等の取扱基準が文書化されている。 | □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、離席時のパソコン、モバイル端末、電磁的記録媒体、文書等の取扱基準が文書化され、正式に承認されているか確かめる。 | 5.1.(1)⑦ | 7.7 | |
| | 100 | ○ | **ⅱ)机上の端末等の取扱**<br>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 | |
| (1) 職員等の遵守事項 ⑧ 退職時等の遵守事項 | 101 | | **ⅰ)退職時等の遵守事項**<br>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、異動、退職等により業務を離れる場合の遵守事項が定められ、文書化されている。 | □職務規程 | 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、異動、退職等により業務を離れる場合の遵守事項が文書化され、正式に承認されているか確かめる。 | 5.1.(1)⑧ | 5.11<br>6.5 | ・退職時等には、認証用のICカード等を確実に返還させる。その他の法令遵守については、No.351～352も関連する項目であることから参考にすること。 |
| | 102 | | **ⅱ)退職時等の情報資産の取扱い**<br>職員等が、異動、退職等により業務を離れる場合、利用していた情報資産が返却されている。また、異動、退職後も業務上知り得た情報を漏らさないよう職員等へ周知されている。 | □職務規程 | 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、異動、退職等により業務を離れる場合に情報資産が返却されているか確かめる。また、異動、退職後も業務上知り得た情報を漏らさないように周知されているか確かめる。 | 5.1.(1)⑧ | 5.11<br>6.5 | |

別紙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 |
|---|---|---|---|---|---|---|---|---|
| (2)<br>臨時・非常勤職員への対応 | 103 | | **ⅰ)臨時・非常勤職員への対応基準**<br>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、情報セキュリティに関し臨時・非常勤職員への対応に関わる基準が定められ、文書化されている。 | □臨時・非常勤職員への対応基準 | 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、情報セキュリティに関し臨時・非常勤職員への対応に関わる基準が文書化され、正式に承認されているか確かめる。 | 5.1.(2)<br>①～③ | 5.2 | |
| (2)<br>臨時・非常勤職員への対応<br>①<br>情報セキュリティポリシー等の遵守 | 104 | | **ⅰ)臨時・非常勤職員の情報セキュリティポリシー等の遵守**<br>情報セキュリティ管理者によって、臨時・非常勤職員を採用する際、情報セキュリティポリシー等のうち当該職員が遵守すべき事項を理解させ、実施、遵守させている。 | □研修・訓練実施基準<br>□研修実施報告書 | 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、情報セキュリティポリシー等のうち、採用時に臨時・非常勤職員に理解させた事項が、臨時・非常勤職員によって実施、遵守されているか確かめる。必要に応じて、臨時・非常勤職員へのアンケート調査を実施して確かめる。 | 5.1.(2)① | 6.2<br>6.3 | ・情報セキュリティに関する研修・訓練については、No.111～122も関連する項目であることから参考にすること。 |
| (2)<br>臨時・非常勤職員への対応<br>②<br>情報セキュリティポリシー等の遵守に対する同意 | 105 | | **ⅰ)臨時・非常勤職員の情報セキュリティポリシー等の遵守に対する同意**<br>情報セキュリティ管理者によって、臨時・非常勤職員採用時に、業務の内容に応じて、情報セキュリティポリシー等を遵守する旨の同意書への署名を求めている。 | □同意書 | 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臨時・非常勤職員採用時に、業務の内容に応じて、情報セキュリティポリシー等を遵守する旨の同意書への署名を求めているか確かめる。 | 5.1.(2)② | 6.2 | ・同意書への署名は必須ではなく、業務の内容に応じて、必要と判断される場合に行う。 |
| (2)<br>臨時・非常勤職員への対応<br>③<br>インターネット接続及び電子メール使用等の制限 | 106 | | **ⅰ)臨時・非常勤職員のインターネット及び電子メール使用制限**<br>情報セキュリティ管理者によって、臨時・非常勤職員のインターネット及び電子メールの使用が必要最小限に制限されている。 | □ネットワーク管理基準<br>□電子メール利用基準 | 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及び執務室の視察により、インターネット及び電子メールの使用が業務上必要ない臨時・非常勤職員には使用できないように制限されているか確かめる。 | 5.1.(2)③ | 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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | (3)<br>情報セキュリティポリシー等の掲示 | 107 | | **ⅰ）情報セキュリティポリシー等の公表**<br>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、職員等が常に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することが定められ、文書化されている。 | □情報セキュリティポリシー | 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、職員等が常に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することが文書化され、正式に承認されているか確かめる。 | 5.1.(3) | 5.1 | |
| | | | 108 | ○ | **ⅱ）情報セキュリティポリシー等の掲示**<br>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)<br>委託事業者に対する説明 | 109 | | **ⅰ）委託事業者の情報セキュリティポリシー等遵守の説明義務**<br>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、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、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を説明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<br>□委託管理基準 | 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セキュリティ責任者、情報システム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を説明しなければならないことが文書化され、正式に承認されているか確かめる。 | 5.1.(4) | 5.19<br>5.20 | |
| | | | 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**<br>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<br>□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<br>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。<br>・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。<br>・業務委託に関する事項ついては、No.357～402も関連する項目であることから参考にすること。 |



別紙3

別紙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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | 5.2.<br>研修・訓練 | (1)<br>情報セキュリティに関する研修・訓練 | 111 | | **ⅰ)情報セキュリティに関する研修・訓練の実施基準**<br>CISOによって、定期的にセキュリティに関する研修・訓練を実施しなければならないことが定められ、文書化されている。 | □研修・訓練実施基準 | 監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、情報セキュリティに関する研修・訓練の実施について文書化され、正式に承認されているか確かめる。 | 5.2.(1)～(4) | 6.3 | |
| | | | 112 | ○ | **ⅱ)情報セキュリティ研修・訓練の実施**<br>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<br>□研修実施報告書<br>□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 | |
| | | (2)<br>研修計画の策定及び実施 | 113 | | **ⅰ)研修計画の策定及び承認**<br>CISOによって、情報セキュリティに関する研修計画の策定と実施体制の構築が定期的に行われ、情報セキュリティ委員会で承認されている。 | □研修・訓練実施基準<br>□研修・訓練実施計画<br>□情報セキュリティ委員会議事録 | 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、情報セキュリティに関する研修計画の策定と実施体制の構築が定期的に行われているか確かめる。また、情報セキュリティ委員会に承認されているか確かめる。 | 5.2.(2)① | 6.3 | ・研修計画には情報セキュリティ人材の育成も含まれていることが望ましい。 |
| | | | 114 | | **ⅱ)情報セキュリティ研修計画**<br>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<br>□研修・訓練実施計画 | 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 | |
| | | | 115 | | **ⅲ)採用時の情報セキュリティ研修の実施**<br>新規採用の職員等を対象に、情報セキュリティに関する研修が実施されている。 | □研修・訓練実施基準<br>□研修実施報告書 | 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、新規採用の職員等を対象に、情報セキュリティに関する研修が実施されているか確かめる。 | 5.2.(2)③ | 6.3 | |
| | | | 116 | | **ⅳ)情報セキュリティ研修の内容の設定**<br>研修の内容は、職員等の役割、情報セキュリティに関する理解度等に応じたものになっている。 | □研修・訓練実施基準<br>□研修・訓練実施計画 | 監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、研修の内容が、統括情報セキュリティ責任者、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、情報システム担当者及びその他職員等に対して、自己の責任・義務・権限を理解できるように、それぞれの役割、情報セキュリティに関する理解度等に応じたものになっているか確かめる。 | 5.2.(2)④ | 6.3 | ・研修内容は、毎回同じ内容ではなく、内部監査の結果や庁内外での情報セキュリティインシデントの発生状況等を踏まえ、継続的に更新することや、職員等が具体的に行動すべき事項を考慮することが望ましい。 |
| | | (2)<br>研修計画の策定及び実施 | 117 | | **ⅴ)情報セキュリティ教育実施状況の記録及び報告**<br>情報セキュリティ管理者によって、教育の実施状況が記録され、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対して報告されている。 | □研修・訓練実施計画<br>□研修・訓練受講記録<br>□研修・訓練結果報告書<br>□研修・訓練に関するアンケート | 教育の実施記録、受講記録をもとに、教育の実施状況が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報告されているか確かめる。 | 5.2.(2)⑤ | 6.3 | |

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | 118 | | **vi）情報セキュリティ教育実施状況の分析、評価及び報告**<br>統括情報セキュリティ責任者によって、教育の実施状況が分析、評価され、CISOに情報セキュリティ対策に関する教育の実施状況について報告されている。 | □研修・訓練受講記録<br>□研修・訓練結果報告書<br>□研修・訓練に関するアンケート | 統括情報セキュリティ責任者により教育・訓練結果に対して分析が行われ、分析結果のフィードバックが行われているか確認する。また、分析結果やフィードバック内容などが教育・訓練の実施状況とともにCISOに報告されているか確かめる。 | 5.2.(2)⑥ | 6.3 | |
| | | | 119 | | **vii）情報セキュリティ研修の実施報告**<br>CISOによって、情報セキュリティ研修の実施状況について、情報セキュリティ委員会に報告されている。 | □研修・訓練実施基準<br>□研修実施報告書<br>□情報セキュリティ委員会議事録 | 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、職員等の情報セキュリティ研修の実施状況について、毎年度1回、情報セキュリティ委員会に報告されているか確かめる。 | 5.2.(2)⑦ | 6.3 | ・幹部を含めた全ての職員等が参加しているかの確認が必要である。 |
| | | (3)<br>緊急時対応訓練 | 120 | | **ⅰ）緊急時対応訓練の実施計画**<br>CISOによって、緊急時対応を想定した訓練計画について定められ、文書化されている。 | □研修・訓練実施基準<br>□研修・訓練実施計画 | 監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、緊急時対応を想定した訓練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、訓練計画には、ネットワークや各情報システムの規模等を考慮して実施体制、実施範囲等が定められているか確かめる。 | 5.2.(3) | 6.3 | |
| | | | 121 | | **ⅱ）緊急時対応訓練の実施**<br>CISOによって、緊急時対応を想定した訓練が実施されている。 | □研修・訓練実施基準<br>□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、緊急時対応を想定した訓練計画が定期的かつ効果的に実施されているか確かめる。 | 5.2.(3) | 6.3 | ・緊急時対応計画については、No.343～346も関連する項目であることから参考にすること。 |
| | | (4)<br>研修・訓練への参加 | 122 | | **ⅰ）研修・訓練への参加**<br>すべての職員等が定められた研修・訓練に参加している。 | □研修・訓練実施基準<br>□研修実施報告書<br>□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、幹部を含めたすべての職員等が定められた研修・訓練に参加しているか確かめる。 | 5.2.(4) | 6.3 | |
| | 5.3.<br>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**<br>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)<br>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**<br>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<br>□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 | |



別紙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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | (2)<br>住民等外部からの情報セキュリティインシデントの報告 | 125 | | **ⅰ）住民等外部からの情報セキュリティインシデントの報告**<br>住民等外部からネットワーク及び情報システム等の情報資産に関する情報セキュリティインシデントについて報告を受けた場合、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<br>□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、住民等外部からネットワーク及び情報システム等の情報資産に関する情報セキュリティインシデントについて報告を受けた場合、報告手順に従って遅滞なく報告されているか確かめる。 | 5.3.(2)①～③ | 6.8 | |
| | | | 126 | | **ⅱ）情報セキュリティインシデントの窓口設置**<br>CISOによって、情報システムの情報セキュリティインシデントについて住民等外部から報告を受けるための窓口設置及び、当該窓口への連絡手段について定められ、公表されている。 | □情報セキュリティインシデント報告手順書<br>□住民に対する広報記録 | 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、情報システム等の情報セキュリティインシデントについて住民等外部から報告を受けるための窓口設置及び当該窓口への連絡手段が文書化され、公表されているか確かめる。 | 5.3.(2)④ | 6.8 | |
| | | (3)<br>情報セキュリティインシデントの原因究明・記録、再発防止等 | 127 | | **ⅰ）情報セキュリティインシデントの原因究明・記録、再発防止等**<br>統括情報セキュリティ責任者及び情報セキュリティインシデントを引き起こした部門の当該責任者によって、情報セキュリティインシデントの発生から対応までの記録が作成、保存されている。また、同様の情報セキュリティインシデントが別の情報システムにおいても発生している可能性を検討し、必要に応じて当該情報システムを所管する情報システム管理者へ確認が指示されている。 | □情報セキュリティインシデント報告手順書<br>□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へのインタビューにより、情報セキュリティインシデントの原因究明が行われ、発生から対応までの記録が作成、保存されているか確かめる。<br>また、情報セキュリティインシデントが起きたときに迅速に行動したか、報告内容等は適切であったかどうかを確かめる。<br>同様の情報セキュリティインシデントが別の情報システムにおいても発生している可能性を検討し、必要に応じて当該情報システムを所管する情報システム管理者へ確認が指示されているかを確かめる。<br>原因究明結果から、再発防止策が検討され、CISOに報告されているか確かめる。 | 5.3.(3) | 5.25<br>5.26<br>6.8 | ・情報セキュリティインシデントの分析結果は、情報セキュリティポリシー等の見直しに活用されることが望ましい。<br>・他部門も含めて同様の情報セキュリティインシデントの再発を防止するために全庁横断的に再発防止策を検討する必要がある。 |
| | 5.4.<br>ID及びパスワード等の管理 | (1)<br>ICカード等の取扱い | 128 | | **ⅰ）認証用ICカード等の取扱いに関わる基準及び手続**<br>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、認証用ICカード等の取扱いに関わる基準及び手続が定められ、文書化されている。 | □ICカード等取扱基準 | 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、認証用のICカードやUSBトークンの取扱いに関わる基準と手続が文書化され、正式に承認されているか確かめる。 | 5.4.(1)①<br>～③ | 5.16<br>5.18 | |
| | | | 129 | | **ⅱ）認証用ICカード等の共有禁止**<br>認証用ICカード等は職員等間で共有されていない。 | □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により、認証用のICカードやUSBトークンなどが職員等間で共有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.(1)①<br>(ア) | 5.16<br>5.18 | |
| | | | 130 | ○ | **ⅲ）認証用ICカード等の放置禁止**<br>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<br>(イ) | 5.16<br>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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | 131 | ○ | **ⅳ）認証用ICカード等の紛失時手続**<br>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<br>□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<br>(ウ) | 5.16<br>5.18 | |
| | | | 132 | ○ | **ⅴ）認証用ICカード等の紛失時対応**<br>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<br>□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<br>5.18 | |
| | | | 133 | ○ | **ⅵ）認証用ICカード等の回収及び廃棄**<br>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<br>□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<br>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。 |
| | | (2)<br>IDの取扱い | 134 | | **ⅰ）職員等のID取扱基準**<br>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、職員等のIDの取扱いに関わる基準が定められ、文書化されている。 | □ID取扱基準 | 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、IDの取扱基準が文書化され、正式に承認されているか確かめる。 | 5.4.(2) | 5.16<br>5.18 | ・利用者IDの取扱いについては、No.222～225も関連する項目であることから参考にすること。 |
| | | | 135 | | **ⅱ）職員等のID貸与禁止**<br>職員等に個人毎に付与されているIDを他人に利用させていない。 | □ID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により、職員等が利用するIDを他人に利用させ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.(2)① | 5.16<br>5.18 | |
| | | | 136 | | **ⅲ）共用IDの利用制限**<br>共用IDを利用する場合は、共用IDの利用者以外の利用が制限されている。 | □ID取扱基準<br>□ID管理台帳 | 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、共用IDの利用者が特定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.(2)② | 5.16<br>5.18 | |
| | | (3)<br>パスワードの取扱い | 137 | | **ⅰ）職員等のパスワードの管理基準**<br>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、職員等のパスワードの取扱いに関わる基準が定められ、文書化されている。 | □パスワード管理基準 | 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。 | 5.4.(3) | 5.17 | ・パスワードに関する情報の管理については、No.244～246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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | 138 | ○ | **ⅱ）パスワードの取扱い**<br>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 | 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**<br>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 | |
| | | | 140 | | **ⅳ）同一パスワードの使用禁止**<br>機密性の非常に高い複数の情報システムを扱う職員等のパスワードが~~は、~~当該情報システム間で異なるように設定されている。 | □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、機密性の非常に高い複数の情報システムを扱う職員等が、当該情報システム間で同一パスワードを使用し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)⑤ | 5.17 | |
| | | | 141 | | **ⅴ）仮パスワードの変更**<br>仮パスワードは、最初のログイン時に変更されている。 | □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、仮パスワードが最初ログイン時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。また、サンプリングにより仮パスワードが残っていないかを確かめる。 | 5.4.(3)⑥ | 5.17 | 仮パスワードの中には初期パスワードを含んでいることに留意する。 |
| | | | 142 | ○ | **ⅵ）パスワード記憶機能の利用禁止**<br>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 | |
| | | | 143 | | **ⅶ）パスワードの共有禁止**<br>職員間でパスワードが共有されていない。 | □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により、職員間でパスワードが共有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)⑧ | 5.17 | ただし、共有IDのパスワードは除く。 |
| 6.<br>技術的セキュリティ | 6.1.<br>コンピュータ及びネットワークの管理 | (1)<br>文書サーバの設定等 | 144 | | **ⅰ）文書サーバに関わる設定基準**<br>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、文書サーバに関わる設定基準が定められ、文書化されている。 | □文書サーバ設定基準 | 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、文書サーバに関わる設定基準が文書化され、正式に承認されているか確かめる。 | 6.1.(1) | 5.15<br>8.3 | |
| | | | 145 | | **ⅱ）文書サーバの容量設定と職員等への周知**<br>情報システム管理者によって、職員等が使用できる文書サーバの容量が設定され、職員等に周知されている。 | □文書サーバ設定基準<br>□職員等への周知記録 | 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、職員等が使用できる文書サーバの容量が設定され、職員等に周知されているか確かめる。 | 6.1.(1)① | － | |

| 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 |
|---|---|---|---|---|---|---|---|---|
| | 146 | ○ | **ⅲ）文書サーバの構成**<br>情報システム管理者によって、文書サーバが課室等の単位で構成され、職員等が他課室等のフォルダ及びファイルを閲覧及び使用できないように設定されている。 | □文書サーバ設定基準 | 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パソコン等の端末からの操作により、文書サーバが課室等の単位で構成され、職員等が他課室等のフォルダ及びファイルを閲覧及び使用できないように設定されているか確かめる。 | 6.1.(1)② | 5.15<br>8.3 | |
| | 147 | ○ | **ⅳ）文書サーバのアクセス制御**<br>情報システム管理者によって、特定の職員等しか取り扱えないデータについて、担当外の職員等が閲覧及び使用できないような措置が講じられている。 | □文書サーバ設定基準 | 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パソコン等の端末からの操作により、住民の個人情報や人事記録といった特定の職員等しか取扱えないデータについて、担当外の職員等によって閲覧及び使用できないよう、別途ディレクトリを作成する等のアクセス制御が行われているか確かめる。 | 6.1.(1)③ | 5.15<br>8.3 | |
| (2)<br>バックアップの実施 | 148 | | **ⅰ）バックアップに関わる基準及び手順**<br>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、業務システムのデータベースやファイルサーバ等に記録された情報についてのバックアップに関わる基準及び手順が定められ、文書化されている。 | □バックアップ基準<br>□バックアップ手順書<br>□リストア手順書 | 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、ファイルサーバ等に記録された情報のバックアップ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。 | 6.1.(2) | 8.13 | |
| | 149 | ○ | **ⅱ）バックアップの実施**<br>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<br>□バックアップ手順書<br>□バックアップ実施記録<br>□リストア手順書<br>□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かかわらず、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)① | 8.13 | ・サーバの冗長化については、No.30～33も関連する項目であることから参考にすること。 |
| | 150 | ○ | **ⅲ）サーバ装置、通信回線装置のバックアップ**<br>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、重要な情報を取り扱うサーバ装置は、適切な方法でバックアップが取得されている。また、通信回線装置は、運用状態を復元するために必要な設定情報等のバックアップを取得し、保管されている。 | □バックアップ基準<br>□バックアップ手順書<br>□バックアップ実施記録<br>□リストア手順書<br>□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により、サーバ装置および通信回線装置のバックアップが取得されているか確かめる。また、バックアップデータの保管方法、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)②③ | 8.13 | |
| (3)<br>他団体との情報システムに関する情報等の交換 | 151 | | **ⅰ）他団体との情報システムに関する情報等の交換の取扱いに関わる基準**<br>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及び情報システム管理者によって、他団体との情報システムに関する情報及びソフトウェアを交換する場合の取扱いに関わる基準が定められ、文書化されている。 | □情報及びソフトウェアの交換基準 | 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、他の団体との情報システムに関する情報及びソフトウェアを交換する場合の取扱いに関わる基準が文書化され、正式に承認されているか確かめる。 | 6.1.(3) | 5.14<br>5.20 | |

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | 152 | | **ⅱ）他団体との情報システムに関する情報等の交換**<br>他団体と情報システムに関する情報及びソフトウェアを交換する場合、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及び情報セキュリティ責任者の許可を得ている。 | □情報及びソフトウェアの交換基準<br>□情報及びソフトウェアの交換に関する契約書（覚書）<br>□他の組織との間の情報及びソフトウェアの交換に関する申請書 | 監査資料のレビューと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、他の団体との情報システムに関する情報及びソフトウェアを交換する場合、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の許可を得ているか確かめる。 | 6.1.(3) | 5.14<br>5.20 | ・必要に応じて、他団体との間において契約を取り交わすことが望ましい。この契約におけるセキュリティの扱いは、関連する業務情報の重要度やリスクを低減させる管理策を盛り込むことが望ましい。 |
| | | (4)<br>システム管理記録及び作業の確認 | 153 | | **ⅰ）システム管理記録及び作業の確認に関わる基準**<br>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、所管する情報システムの運用及び変更等の作業記録、確認に関わる基準が定められ、文書化されている。 | □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、所管する情報システムの運用及び変更等の作業内容を記録し管理することや、システム変更等の作業を確認することなどの基準が文書化され、正式に承認されているか確かめる。 | 6.1.(4) | 5.3<br>5.37<br>8.15<br>8.19<br>8.32 | |
| | | | 154 | ○ | **ⅱ）情報システム運用の作業記録作成**<br>情報システム管理者によって、所管する情報システムの運用において実施した作業記録が作成されている。 | □システム運用基準<br>□システム運用作業記録 | 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、所管する情報システムの運用において実施した作業記録が作成され、管理されているか確かめる。 | 6.1.(4)① | 8.15 | |
| | | | 155 | | **ⅲ）システム変更等作業の記録作成及び管理**<br>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、所管するシステムの変更等の作業記録が作成され、管理されている。また、運用・保守によって機器の構成や設定情報等に変更があった場合は、情報セキュリティ対策が適切であるか確認し、必要に応じて見直されている。 | □システム運用基準<br>□システム変更等作業記録 | 監査資料のレビューと統括情報セキュリティ責任者及び情報システム管理者へのインタビューにより、所管するシステムの変更等の作業記録が作成され、詐取、改ざん等されないよう管理されているか確かめる。<br>機器構成や設定情報等の変更がある場合は、情報セキュリティ対策が適切であるか確認し、必要に応じて見直しされているかを確かめる。 | 6.1.(4)② | 8.15<br>8.19<br>8.32 | |
| | | | 156 | | **ⅳ）システム変更等作業の確認**<br>システム変更等を行う場合は、2名以上で作業し、互いにその作業が確認されている。 | □システム運用基準<br>□システム変更等作業記録 | 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、統括情報セキュリティ責任者、情報システム管理者又は情報システム担当者及び操作を認められた委託事業者がシステム変更等を行う場合は、2名以上で作業し、互いにその作業内容を確認しているか確かめる。 | 6.1.(4)③ | 5.3<br>5.20<br>5.22<br>8.15 | |
| | | (5)<br>情報システム仕様書等の管理 | 157 | | **ⅰ）情報システム仕様書等の管理基準**<br>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、情報システムに関する文書の管理に関わる基準が定められ、文書化されている。 | □情報システム関連文書管理基準 | 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、ネットワーク構成図、情報システム仕様書等の情報システム関連文書の管理に関わる基準が文書化され、正式に承認されているか確かめる。 | 6.1.(5) | ― | |



別紙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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | 158 | ○ | **ⅱ）情報システム仕様書等の管理**<br>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、情報システム仕様書等が管理されている。 | □情報システム関連文書管理基準<br>□システム仕様書等<br>□プログラム仕様書等 | 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、ネットワーク構成図、情報システム仕様書等の情報システム関連文書を業務上必要でない者からの閲覧や、紛失等がないよう、施錠したキャビネットへの保管やフォルダへのアクセス制限などによって管理されているか確かめる。 | 6.1.(5) | － | |
| | | (6)<br>ログの管理取得等 | 159 | | **ⅰ）ログ等の取得及び管理に関わる基準**<br>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、ログ等の取得及び管理に関わる基準が定められ、文書化されている。 | □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、ログ等の取得及び管理に関わる基準が文書化され、正式に承認されているか確かめる。 | 6.1.(6) | 8.15 | |
| | | | 160 | ○ | **ⅱ）ログ等の取得及び保存**<br>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<br>□ログ<br>□システム稼動記録<br>□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 | 8.15 | |
| | | | 161 | | **ⅲ）ログ等の改ざん、誤消去等の防止**<br>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、ログとして取得する項目、保存期間、取扱方法及びログが取得できなくなった場合の対処等について定め、ログを適切に管理している。 | □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、ログ等が仕様どおりに取得され、詐取、改ざん、誤消去等されないように必要な措置が講じられているか確かめる。 | 6.1.(6)② | 8.15 | |
| | | | 162 | | **ⅳ）ログ等の点検、分析**<br>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 | 8.15 | |
| | | (7)<br>障害記録 | 163 | | **ⅰ）障害記録の記録及び保存に関わる基準**<br>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、障害記録の記録及び保存に関わる基準が定められ、文書化されている。 | □障害対応基準 | 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等の記録及び保存に関わる基準が文書化され、正式に承認されているか確かめる。 | 6.1.(7) | 8.15 | |
| | | | 164 | ○ | **ⅱ）障害記録の保存**<br>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<br>□障害報告書<br>□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) | 8.15 | |



別紙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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | (8)<br>ネットワークの接続制御、経路制御等 | 165 | | **ⅰ)ネットワークの接続制御、経路制御等に関わる基準**<br>統括情報セキュリティ責任者によって、ネットワークの接続制御、経路制御等に関わる基準が定められ、文書化されている。 | □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、ネットワークの接続制御、経路制御等に関わる基準が文書化され、正式に承認されているか確かめる。 | 6.1.(8) | 5.15<br>8.20 | |
| | | | 166 | ○ | **ⅱ)ファイアウォール、ルータ等の設定**<br>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<br>□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 | 8.20<br>8.21 | ・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。 |
| | | | 167 | ○ | **ⅲ)ネットワークのアクセス制御**<br>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 | 5.15<br>8.20<br>8.21 | |
| | | | 168 | | **ⅳ)リモートメンテナンスのセキュリティ確保**<br>統括情報セキュリティ責任者によって、保守又は診断のために、外部の通信回線から内部の通信回線に接続された機器等に対して行われるリモートメンテナンスに係る情報セキュリティが確保されている。また、情報セキュリティ対策について、定期的な確認により見直しされている。 | □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、リモートメンテナンスに係る情報セキュリティが確保されているか確かめる。また、情報セキュリティ対策について、定期的な確認により見直しされているか確かめる。 | 6.1.(8)③ | 6.7 | |
| | | (9)<br>外部の者が利用できるシステムの分離等 | 169 | | **ⅰ)外部の者が利用できるシステムの分離等に関わる基準**<br>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、外部の者が利用できるシステムの分離等に関わる基準が定められ、文書化されている。 | □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、外部の者が利用できるシステムについて、不正アクセス等を防御するために他のネットワークと切り離す等の基準が文書化され、正式に承認されているか確かめる。 | 6.1.(9) | 5.15<br>8.22 | |
| | | | 170 | | **ⅱ)外部の者が利用できるシステムの分離**<br>情報システム管理者によって、外部の者が利用できるシステムについて、必要に応じ他のネットワーク及び情報システムと物理的に分離する等の措置が講じられている。 | □ネットワーク管理基準<br>□通信回線敷設図<br>□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、外部の者が利用できるシステムについて、不正アクセス等を防御するために他のネットワーク及び情報システムと物理的に分離する等の措置が取られているか確かめる。 | 6.1.(9) | 8.22 | |



別紙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)<br>外部ネットワークとの接続制限等 | 171 | | **ⅰ)外部ネットワークとの接続に関わる基準及び手続**<br>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、所管するネットワークと外部ネットワークとの接続に関わる基準及び手続が定められ、文書化されている。 | □外部ネットワーク接続基準<br>□外部ネットワーク接続手続 | 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、所管するネットワークと外部ネットワークとを接続する場合の基準及び手続が文書化され、正式に承認されているか確かめる。 | 6.1.(10) | 5.15<br>5.20<br>5.24<br>8.22 | |
| | | | 172 | ○ | **ⅱ)外部ネットワーク接続の申請及び許可**<br>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<br>□外部ネットワーク接続手続<br>□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 | 5.15 | |
| | | | 173 | | **ⅲ)外部ネットワークの確認**<br>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<br>□外部ネットワーク接続手続<br>□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。 |
| | | | 174 | | **ⅳ)外部ネットワークの瑕疵による損害賠償責任の担保**<br>接続した外部ネットワークの瑕疵による損害賠償責任が契約上担保されている。 | □外部ネットワーク接続基準<br>□外部ネットワーク接続手続<br>□サービス契約書 | 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、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任が契約上担保されているか確かめる。 | 6.1.(10)③ | 5.2 | |
| | | | 175 | ○ | **ⅴ)ファイアウォール等の設置**<br>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、セキュリティ対策が実施されている。 | □ネットワーク管理基準<br>□通信回線敷設図<br>□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、次のセキュリティ対策が実施されているか確かめる。<br>・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<br>・ウェブサーバが備える機能のうち、必要な機能のみを利用しているか<br>・ウェブサーバからの不用意な情報漏えいを防止するための措置を講じているか<br>・ウェブコンテンツの編集作業を行う主体を限定しているか<br>・全ての情報に対する暗号化及び電子証明書による認証の対策を講じているか | 6.1.(10)④ | 8.22 | |
| | | | 176 | | **ⅵ)外部ネットワークの遮断**<br>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<br>□外部ネットワーク接続手続<br>□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 | 5.24 | |



別紙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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | (11)<br>複合機のセキュリティ管理 | 177 | | **ⅰ）複合機のセキュリティに関わる基準及び手続**<br>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、複合機の調達、運用に関わる基準及び手続が定められ、文書化されている。 | □複合機管理基準<br>□複合機管理手続 | 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、複合機の調達、運用に関わる基準及び手続が文書化され、正式に承認されているか確かめる。 | 6.1.(11) | 5.21<br>7.8<br>7.13 | |
| | | | 178 | | **ⅱ）複合機の調達要件**<br>統括情報セキュリティ責任者によって、複合機の調達におけるセキュリティ要件が定められている。 | □複合機管理基準<br>□複合機管理手続 | 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、複合機の調達時に、複合機の機能、設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適切なセキュリティ要件が定められているか確かめる。 | 6.1.(11)① | 5.21 | |
| | | | 179 | | **ⅲ）複合機のセキュリティ設定**<br>統括情報セキュリティ責任者によって、複合機の設定が適切に行われ、複合機の情報セキュリティインシデント対策が講じられている。 | □複合機管理基準<br>□複合機管理手続 | 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、複合機の情報セキュリティインシデントに対する対策として、複合機の設定が適切に行われているか確かめる。 | 6.1.(11)② | 5.21<br>7.8<br>7.13 | |
| | | | 180 | | **ⅳ）複合機の情報の抹消**<br>複合機の運用を終了する場合、統括情報セキュリティ責任者によって、複合機の電磁的記録媒体の全ての情報が抹消する又は再利用できないような対策が講じられている。 | □複合機管理基準<br>□複合機管理手続 | 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、複合機の運用を終了する場合に複合機の電磁的記録媒体の全ての情報が抹消する又は再利用できないような対策が講じられているか確かめる。 | 6.1.(11)③ | 7.14 | |
| | | (12)<br>IoT機器を含む特定用途機器のセキュリティ管理 | 181 | | **ⅰ）特定用途機器のセキュリティ対策**<br>統括情報セキュリティ責任者によって、特定用途機器の特性に応じたセキュリティ対策が実施されている。 | □特定用途機器管理基準<br>□特定用途機器管理手続 | 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、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により脅威が想定される場合には、当該機器の特性に応じたセキュリティ対策が実施されているか確かめる。 | 6.1.(12) | 5.21<br>7.8<br>7.13 | |
| | | (13)<br>無線LANのセキュリティ対策及びネットワーク盗聴対策 | 182 | ○ | **ⅰ）無線LAN利用時の暗号化及び認証技術の使用**<br>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<br>□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管理者、ユーザとも強固な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 | 5.15<br>8.22 | |
| | | | 183 | ○ | **ⅱ）無線端末同士の通信の防止**<br>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、無線端末間同士の通信が行われないよう適切な設定を行う。 | □ネットワーク管理基準<br>□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、無線端末間同士の通信が行われないよう適切な設定が講じられているか確かめる。 | 6.1.(13) | | |
| | | | 184 | | **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**<br>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<br>□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 | 5.15<br>8.24 | |



別紙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 |
|---|---|---|---|---|---|---|---|---|
| (14) 電子メールのセキュリティ管理 | 185 | | **ⅰ）電子メールのセキュリティ管理に関わる基準**<br>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、電子メールのセキュリティ管理に関わる基準が定められ、文書化されている。 | □電子メール管理基準 | 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、メールサーバのセキュリティ対策等、電子メールのセキュリティ管理に関わる基準が文書化され、正式に承認されているか確かめる。 | 6.1.(14) | 5.14<br>5.20 | |
| | 186 | ○ | **ⅱ）電子メール転送制限**<br>統括情報セキュリティ責任者によって、電子メールサーバによる電子メール転送ができないように設定されている。 | □電子メール管理基準 | 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、権限のない者による外部から外部への電子メール転送（電子メールの中継処理）が行えないよう、電子メールサーバの設定が行われているか確かめる。 | 6.1.(14)① | 5.14 | |
| | 187 | | **ⅲ）メールサーバ運用の停止**<br>大量のスパムメール等の送受信を検知した場合、統括情報セキュリティ責任者によって、メールサーバの運用が停止されている。 | □電子メール管理基準<br>□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、大量のスパムメール等の送受信を検知した場合にメールサーバの運用が停止されているか確かめる。 | 6.1.(14)② | 5.14 | |
| | 188 | | **ⅳ）電子メール送受信容量制限**<br>統括情報セキュリティ責任者によって、電子メールの送受信容量が制限されている。 | □電子メール管理基準 | 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、電子メールの送受信容量の上限が設定され、上限を超える電子メールの送受信ができないよう設定されているか確かめる。 | 6.1.(14)③ | 5.14 | |
| | 189 | | **ⅴ）電子メールボックス容量制限**<br>統括情報セキュリティ責任者によって、職員等が使用できる電子メールボックスの容量が制限されている。 | □電子メール管理基準<br>□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システム管理者へのインタビューにより、職員等が使用できる電子メールボックスの容量の上限が設定され、それを超えた場合の対応が職員等に周知されているか確かめる。 | 6.1.(14)④ | 5.14 | |
| | 190 | | **ⅵ）委託事業者の電子メールアドレス利用についての取り決め**<br>委託事業者の作業員が庁内に常駐している場合、統括情報セキュリティ責任者によって、電子メールアドレス利用について、委託先との間で利用方法が取り決められている。 | □電子メール管理基準<br>□業務委託契約書 | 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、委託事業者の作業員の電子メールアドレス利用について、委託先との間で利用方法が取り決められているか確かめる。 | 6.1.(14)⑤ | 5.14<br>5.20 | |
| | 191 | | **ⅶ）電子メールによる情報資産無断持ち出し禁止**<br>統括情報セキュリティ責任者によって、職員等が電子メールの送信等により情報資産を無断で外部に持ち出すことができないよう措置が講じられている。 | □電子メール管理基準 | 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、職員等が電子メールの送信等により情報資産を無断で外部に持ち出すことができないように、フィルタリングソフトウェア等の利用によって添付ファイルを監視する等、システム上において措置が講じられているか確かめる。 | 6.1.(14)⑥ | 5.14 | |
| (15) 電子メールの利用制限 | 192 | | **ⅰ）電子メールの利用に関わる基準**<br>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、電子メールの利用に関わる基準が定められ、文書化されている。 | □電子メール利用基準 | 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、電子メールの利用に関わる基準が文書化され、正式に承認されているか確かめる。 | 6.1.(15) | 5.14 | ・宛先メールアドレスのTOに限らず、CC、BCCにも留意しているか確認する必要がある。 |
| | 193 | | **ⅱ）電子メール転送禁止**<br>電子メールの自動転送機能を用いた転送は行われていない。 | □電子メール利用基準<br>□電子メール送受信ログ | 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、不正な情報の持ち出しを防止する観点から、自動転送機能を用いて電子メールを転送し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。 | 6.1.(15)① | 5.14 | |

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | 194 | | **ⅲ）電子メールの業務外利用の禁止**<br>業務以外の目的で電子メールを利用していない。 | □電子メール利用基準<br>□電子メール送受信ログ | 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、業務上必要のない送信先に電子メールを送信し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。 | 6.1.(15)② | 5.14 | |
| | | | 195 | | **ⅳ）電子メール送信先開示の禁止**<br>職員等が複数人に電子メールを送信する場合、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにして送信されている。 | □電子メール利用基準<br>□電子メール送受信ログ | 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、複数人に電子メールを送信する場合、BCCに送信先を入力するなど、他の送信先の電子メールアドレスが分からないように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。 | 6.1.(15)③ | 5.14 | |
| | | | 196 | | **ⅴ）電子メール誤送信の報告**<br>職員等が重要な電子メールを誤送信した場合、情報セキュリティ管理者に報告されている。 | □電子メール利用基準 | 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により、重要な電子メールを誤送信した場合、情報セキュリティ管理者に報告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。 | 6.1.(15)④ | 5.14<br>5.24 | |
| | | | 197 | ○ | **ⅵ）フリーメール、ネットワークストレージサービス等の使用禁止**<br>ウェブで利用できる電子メール、ネットワークストレージサービス等は使用されていない。 | □電子メール利用基準 | 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、外部への不正な情報の持ち出し等を防止するため、ウェブで利用できる電子メール、ネットワークストレージサービス等が使用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。 | 6.1.(15)⑤ | 5.14 | |
| | | (16)<br>電子署名・暗号化 | 198 | | **ⅰ）電子署名・暗号化等に関わる基準**<br>CISOによって、外部に送るデータの電子署名・暗号化等に関わる基準が定められ、文書化されている。 | □電子署名・暗号化利用基準 | 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、外部に送るデータの電子署名・暗号化又はパスワードに関わる基準が文書化され、正式に承認されているか確かめる。 | 6.1.(16) | 5.14<br>8.24 | |
| | | | 199 | | **ⅱ）電子署名、暗号化又はパスワード設定**<br>外部に送るデータの機密性又は完全性を確保することが必要な場合、CISOが定めた電子署名・暗号化又はパスワード設定の方法を使用して送信されている。 | □電子署名・暗号化利用基準 | 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、外部に送るデータの機密性又は完全性を確保することが必要な場合、CISOが定めた電子署名、暗号化又はパスワード設定の方法を使用して送信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。 | 6.1.(16)① | 5.14<br>8.24 | |
| | | | 200 | | **ⅲ）暗号化方法及び暗号鍵管理**<br>外部に送るデータを暗号化する場合、CISOが定める方法により暗号化され、暗号鍵が管理されている。 | □電子署名・暗号化利用基準 | 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、外部に送るデータを暗号化する場合、CISOが定める方法により暗号化され、暗号鍵が管理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。 | 6.1.(16)② | 5.14<br>8.24 | |
| | | | 201 | | ⅳ）**電子署名の正当性検証手段の提供**<br>**CISOによって、**付与した電子署名の正当性が確認できる情報又は手段が提供されている。 | □電子署名・暗号化利用基準 | 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、電子署名の正当性を確認する情報又は手段が提供されていることを確かめる。必要に応じて、提供された情報又は手段により検証可能であることを確かめる。 | 6.1.(16)③ | 5.14<br>8.24 | |
| | | (17)<br>無許可ソフトウェアの導入等の禁止 | 202 | | **ⅰ）ソフトウェアの導入に関わる基準及び手続**<br>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、ソフトウェアの導入に関わる基準及び手続が定められ、文書化されている。 | □ソフトウェア導入基準/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、ソフトウェアの導入に関わる基準及び手続が文書化され、正式に承認されているか確かめる。 | 6.1.(17) | 8.7 | |



別紙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 |
|---|---|---|---|---|---|---|---|---|---|
| | | 203 | ○ | **ⅱ）ソフトウェアの無断導入の禁止**<br>パソコンやモバイル端末に無断でソフトウェアが導入されていない。 | □ソフトウェア導入基準/手続 | 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、パソコンやモバイル端末の確認により、パソコンやモバイル端末に許可なくソフトウェアが導入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。 | 6.1.(17)① | 8.7 | |
| | | 204 | ○ | **ⅲ）ソフトウェア導入の申請及び許可**<br>業務上必要なソフトウェアがある場合、統括情報セキュリティ責任者及び情報システム管理者の許可を得て、ソフトウェアが導入されている。 | □ソフトウェア導入基準/手続<br>□ソフトウェア導入申請書/承認書 | 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、業務上必要なソフトウェアがある場合、統括情報セキュリティ責任者及び情報システム管理者の許可を得て、ソフトウェアが導入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。 | 6.1.(17)② | 8.7 | |
| | | 205 | ○ | **ⅳ）不正コピーソフトウェアの利用禁止**<br>不正にコピーされたソフトウェアは利用されていない。 | □ソフトウェア導入基準/手続 | 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、不正にコピーされたソフトウェアが利用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。 | 6.1.(17)③ | 5.32<br>8.7 | ・不正コピーはライセンス違反や著作権法違反であることを認識させる必要がある。 |
| | (18)<br>機器構成の変更の制限 | 206 | | **ⅰ）機器構成の変更に関わる基準及び手続**<br>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、パソコンやモバイル端末の機器構成の変更に関わる基準及び手続が定められ、文書化されている。 | □端末構成変更基準/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、職員等がパソコンやモバイル端末に対し機器の構成を変更する場合の基準及び手続が文書化され、正式に承認されているか確かめる。 | 6.1.(18) | 8.32 | |
| | | 207 | | **ⅱ）機器の改造及び増設・交換の禁止**<br>パソコンやモバイル端末に対し機器の改造及び増設・交換が無断で行われていない。 | □端末構成変更基準/手続 | 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、パソコンやモバイル端末に対し許可なく機器の改造及び増設・交換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。 | 6.1.(18)① | 8.32 | |
| | | 208 | ○ | **ⅲ）機器の改造及び増設・交換の申請及び許可**<br>業務上パソコンやモバイル端末に対し機器の改造及び増設・交換の必要がある場合、統括情報セキュリティ責任者及び情報システム管理者の許可を得て行われている。 | □端末構成変更基準/手続<br>□端末構成変更申請書/承認書 | 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、業務上パソコンやモバイル端末に対し機器の改造及び増設・交換の必要がある場合、統括情報セキュリティ責任者及び情報システム管理者の許可を得て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。 | 6.1.(18)② | 8.32 | |
| | (19)<br>無許可でのネットワーク接続の禁止 | 209 | ○ | **ⅰ）ネットワーク接続の禁止**<br>統括情報セキュリティ責任者の許可なく、パソコンやモバイル端末がネットワークに接続されていない。 | □ネットワーク利用基準 | 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及び職員等へのインタビュー、執務室及び管理区域の視察により、統括情報セキュリティ責任者の許可なく、職員等や委託事業者がパソコンやモバイル端末をネットワークに接続し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。 | 6.1.(19) | 8.2 | |

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | (20)<br>業務以外の目的でのウェブ閲覧の禁止 | 210 | ○ | **ⅰ）業務以外の目的でのウェブ閲覧禁止**<br>業務以外の目的でウェブが閲覧されていない。 | □ネットワーク利用基準 | 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、業務以外の目的でウェブが閲覧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。 | 6.1.(20)① | 5.15 | |
| | | | 211 | | **ⅱ）業務以外の目的でのウェブ閲覧発見時の対応**<br>職員等のウェブ利用について明らかに業務以外の目的でウェブを閲覧していることが発見された場合、統括情報セキュリティ責任者によって、情報セキュリティ管理者に通知され、適切な措置が求められている。 | □ネットワーク利用基準<br>□通知書 | 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管理者へのインタビューにより、職員等が明らかに業務以外の目的でウェブを閲覧していることが発見された場合、情報セキュリティ管理者に通知され、適切な措置が求められ、対応されているか確かめる。 | 6.1.(20)② | 5.28<br>6.8 | |
| | | (21)<br>Web会議サービスの利用時の対策 | 212 | ○ | **ⅰ）Web会議の利用手順**<br>統括情報セキュリティ責任者によってWeb会議の利用手順が定められている。 | □Web会議利用手順書 | 監査資料のレビューと統括情報セキュリティ責任者及び職員等へのインタビューにより、Web会議の利用手順が定められ、文書化されていることを確かめる。 | 6.1(21)① | － | |
| | | | 213 | ○ | **ⅱ）Web会議の情報セキュリティ対策の実施**<br>職員等によりWeb会議の利用手順に従って、セキュリティ対策が実施されている。 | □Web会議利用手順書 | 監査資料のレビューと統括情報セキュリティ責任者及び職員等へのインタビューにより、Web会議の参加者や取り扱う情報に応じたセキュリティ対策が実施されていることを確かめる。 | 6.1(21)② | － | |
| | | | 214 | ○ | **ⅲ）Web会議に無関係の者を参加させない**<br>職員等によりWeb会議の利用手順に従って、Web会議に無関係の者が参加できないように対策が実施されている。 | □Web会議利用手順書 | 監査資料のレビューと統括情報セキュリティ責任者及び職員等へのインタビューにより、Web会議の利用手順に従ってWeb会議に無関係の者が参加できないように対策が実施されていることを確かめる。 | 6.1(21)③ | － | |
| | | | 215 | | **ⅳ）外部からのWeb会議への招待**<br>統括情報セキュリティ責任者によって職員等が外部からWeb会議に招待された場合の利用手順が定められている。 | □Web会議利用手順書 | 監査資料のレビューと統括情報セキュリティ責任者及び職員等へのインタビューにより、職員等が外部からWeb会議に招待された場合の利用手順が定められていることを確かめる。 | 6.1(21)④ | － | |
| | | (22)<br>ソーシャルメディアサービスの利用 | 216 | ○ | **ⅰ）自組織が管理するアカウントでのソーシャルメディアサービスの利用**<br>情報セキュリティ管理者によって本市が管理するアカウントでソーシャルメディアサービスを利用する場合の情報セキュリティ対策に関する事項を記載した運用手順が定められている。 | □ソーシャルメディアサービス運用手順書 | 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、職員等が自組織が管理するアカウントでソーシャルメディアサービスを利用する場合、以下の事項を含めたソーシャルメディアサービス運用手順が定められていることを確かめる。<br><br>・当該アカウントによる情報発信が、実際の当該アカウントのものであることを明らかにするために、自組織の自己管理ウェブサイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を実施する。<br><br>・パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（ICカード等）等を適正に管理するなどの方法で、不正アクセス対策を実施する。 | 6.1(22)① | － | |

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | 217 | ○ | **ⅱ）機密性２以上の情報のソーシャルメディアサービスでの発信**<br>情報セキュリティ管理者によって機密性2以上の情報をソーシャルメディアサービスで発信しないよう、利用手順が定められている。 | □ソーシャルメディアサービス運用手順書 | 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、職員等が自組織が管理するアカウントでソーシャルメディアサービスを利用する場合、機密性2以上の情報を発信しないよう定められていることを確かめる。 | 6.1(22)② | － | |
| | | | 218 | ○ | **ⅲ）利用するソーシャルメディアサービスごとの責任者を定める**<br>利用するソーシャルメディアサービスごとの責任者が定められている。 | □ソーシャルメディアサービス運用手順書 | 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、利用するソーシャルメディアサービスごとに責任者が定められていることを確かめる。 | 6.1(22)③ | － | |
| | | | 219 | ○ | **ⅳ）アカウント乗っ取りに対する措置**<br>なりすましや不正アクセスを確認した場合の対処と手順が定められている。 | □ソーシャルメディアサービス運用手順書 | 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、なりすましや不正アクセスを確認した場合の対処と手順が定められていることを確かめる。 | 6.1(22)④ | － | |
| | | | 220 | ○ | **ⅴ）可用性２の情報の提供時の措置**<br>可用性2の情報の提供にソーシャルメディアサービスを用いる場合は、本市の自己管理ウェブサイトに当該情報を掲載して参照可能となっている。 | □ソーシャルメディアサービス運用手順書 | 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及び自己管理Webサイトの情報を確認することにより、ソーシャルメディアサービスで提供する可用性2の情報が掲載され参照可能となっていることを確かめる。 | 6.1(22)⑤ | － | |
| 6.<br>技術的セキュリティ | 6.2.<br>アクセス制御 | (1)<br>アクセス制御<br>(ア)<br>アクセス制御 | 221 | ○ | **ⅰ）アクセス制御に関わる方針及び基準**<br>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<br>□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 | 5.15<br>5.16<br>5.17<br>5.18<br>8.2 | ・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。 |
| | | (1)<br>アクセス制御<br>(イ)<br>利用者IDの取扱い | 222 | ○ | **ⅰ）利用者IDの取扱いに関わる手続**<br>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<br>□利用者ID登録・変更・抹消申請書<br>□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<br>(ア) | 5.16<br>5.18 | |
| | | | 223 | ○ | **ⅱ）利用者IDの登録・権限変更の申請**<br>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<br>□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<br>(ア) | 5.16<br>5.18 | ・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。 |

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | 224 | ○ | **ⅲ）利用者IDの抹消申請**<br>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<br>□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<br>(イ) | 5.16<br>5.18 | ・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。 |
| | | | 225 | ○ | **ⅳ）利用者IDの点検**<br>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。また、主体から対象に対する不要なアクセス権限が付与されていないか定期的に確認されている。 | □利用者ID棚卸記録<br>□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<br>(ウ)(エ) | 5.18 | |
| | | (1)<br>アクセス制御<br>(ウ)<br>特権を付与されたIDの管理等 | 226 | ○ | **ⅰ）特権IDの取扱いに関わる手続**<br>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<br>□特権ID認可申請書<br>□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 | 5.18<br>8.2 | |
| | | | 227 | ○ | **ⅱ）特権ID及びパスワードの管理**<br>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<br>□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<br>(ア) | 5.18<br>8.2 | |
| | | | 228 | | **ⅲ）特権IDの被害最小化**<br>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、管理者権限の特権を持つ主体の識別コード及び主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置、及び内部からの不正操作や誤操作を防止するための措置を講じられている。 | □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、窃取された際の被害最小化や内部からの不正操作や誤操作を防止のための措置が講じられているか確認する。 | 6.2.(1)③<br>(イ) | 8.2 | |
| | | | 229 | | **ⅳ）特権代行者の指名**<br>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、統括情報セキュリティ責任者及び情報システム管理者の特権を代行する者が指名され、CISOに承認されている。 | □特権代行者承認書 | 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、統括情報セキュリティ責任者及び情報システム管理者の特権を代行する者が指名され、CISOに承認されているか確かめる。 | 6.2.(1)③<br>(ウ) | 5.18<br>8.2 | |
| | | | 230 | | **ⅴ）特権代行者の通知**<br>CISOによって、統括情報セキュリティ責任者及び情報システム管理者の特権代行者が速やかに関係者（統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者及び情報システム管理者）に通知されている。 | □特権代行者通知書 | 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、CISOによって、統括情報セキュリティ責任者及び情報システム管理者の特権代行者が関係者（統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者及び情報システム管理者）に通知されているか確かめる。 | 6.2.(1)③<br>(エ) | 5.18<br>8.2 | |

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | 231 | ○ | **ⅵ）特権IDの委託事業者による管理の禁止**<br>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<br>(オ) | 5.18<br>8.2 | |
| | | | 232 | | **ⅶ）特権ID及びパスワードのセキュリティ機能強化**<br>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<br>□システム設計書<br>□特権ID取扱手続<br>□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<br>(カ) | 5.18<br>8.2 | |
| | | | 233 | | **ⅷ）特権IDのID変更**<br>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<br>(キ) | 5.18<br>8.2 | |
| | | (2)<br>職員等による外部からのアクセス等の制限 | 234 | ○ | **ⅰ）外部からのアクセスに関わる方針及び手続**<br>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<br>□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) | 5.15<br>8.1<br>8.24 | |
| | | | 235 | ○ | **ⅱ）外部からのアクセスの申請及び許可**<br>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 | 5.15 | ・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。 |
| | | | 236 | | **ⅲ）外部からのアクセス可能者の制限**<br>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を許可された者が必要最小限に限定されている。 | □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へのインタビューにより、外部からのアクセスを許可された者が必要最小限に限定されているか確かめる。 | 6.2.(2)② | 5.15 | |
| | | | 237 | ○ | **ⅳ）外部からのアクセス時の本人確認機能**<br>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<br>□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 | 5.15 | |
| | | | 238 | | **ⅴ）外部からのアクセス時の暗号化等**<br>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、通信データの暗号化等が行われている。 | □ネットワーク設計書<br>□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、通信途上の盗聴等による情報漏えいを防御するために通信データの暗号化等が行われているか確かめる。 | 6.2.(2)④ | 8.24 | |



別紙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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | 239 | ○ | **vi）外部からのアクセス用端末のセキュリティ確保**<br>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 | 8.1 | |
| | | | 240 | ○ | **vii）外部から持ち込んだ端末のウイルス確認等**<br>外部から持ち込んだ端末を庁内ネットワークに接続する場合、当該職員等によって、接続前にコンピュータウイルスに感染していないことや、パッチの適用状況等が確認され、情報セキュリティ管理者の許可を得るか、もしくは情報セキュリティ管理者によって事前に定義されたポリシーに従って接続されている。 | □端末接続時手続 | 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、外部から持ち込んだ端末を庁内ネットワークに接続する場合、接続前に当該端末がコンピュータウイルスに感染していないことや、セキュリティホールや不正プログラムに対する適切なパッチが適用されていることが確認され、情報セキュリティ管理者の許可を得るか、もしくは情報セキュリティ管理者によって事前に定義されたポリシーに従って接続されているか確かめる。 | 6.2.(2)⑥ | 8.1 | |
| | | | 241 | ○ | **viii）公衆通信回線の接続**<br>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、公衆通信回線等の庁外通信回線を庁内ネットワークに接続する場合の情報セキュリティ確保のために必要な措置が管理されている。 | □端末接続時手続 | 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、公衆通信回線等の庁外通信回線を庁内ネットワークに接続する場合には、統括情報セキュリティ責任者の許可を得ることや、アクセス範囲を必要最小限とし、アクセスログを取得していること等の情報セキュリティ対策を講じ、情報セキュリティが確保されていることを管理しているか確かめる。 | 6.2.(2)⑦ | 5.8<br>8.20 | |
| | | (3)<br>自動識別の設定 | 242 | | **ⅰ）自動識別の設定**<br>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、外部からのネットワークへの接続を許可する機器を自動的に識別するよう設定されている。 | □ネットワーク設計書<br>□接続許可端末一覧 | 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、機器を自動識別するよう設定（例えば、電子証明書やIPアドレス、MACアドレスによる識別情報の取得等）されているか確かめる。 | 6.2.(3) | 8.2 | |
| | | (4)<br>ログイン時の表示等 | 243 | | **ⅰ）ログイン時のシステム設定**<br>情報システム管理者によって、正当なアクセス権をもつ職員等がログインしたことを確認できる機能が設定されている。 | □システム設計書<br>□ログイン画面 | 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、ログイン時におけるメッセージ及びログイン試行回数の制限、アクセスタイムアウトの設定、ログイン・ログアウト時刻の表示等、ログイン時のシステム設定があるか確かめる。 | 6.2.(4) | 8.5 | ・ログイン手順では、許可されていない利用者に助けとなるようなメッセージ（例えば、IDは職員番号であることを表示する等）を表示していないかを確認することが望ましい。 |
| | | (5)<br>認証情報の管理 | 244 | ○ | **ⅰ）認証情報ファイルの管理**<br>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<br>□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 | 5.17 | ・職員等によるパスワードの取扱いについては、No.137～143も関連する項目であることから参考にすること。 |



別紙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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | 245 | | **ⅱ）仮パスワードの変更**<br>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<br>□アクセス管理基準<br>□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 | 5.17 | |
| | | | 246 | | **ⅲ） 認証情報の不正利用防止**<br>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、職員等の認証情報の不正利用を防止するための対策が定められ、文書化されている。 | □アクセス制御方針<br>□アクセス管理基準<br>□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、認証情報の不正利用を防止するための対策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。 | 6.2.(5)③ | 5.18 | |
| | | (6)<br>特権による接続時間の制限 | 247 | | **ⅰ）特権による接続時間の制限**<br>情報システム管理者によって、特権によるネットワーク及び情報システムへの接続時間が必要最小限に制限されている。 | □アクセス制御方針<br>□アクセス管理基準<br>□ネットワーク設計書<br>□システム設計書 | 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、特権によるネットワーク及び情報システムへの接続時間が必要最小限に制限されているか確かめる。 | 6.2.(6) | 8.5 | ・外部ネットワークとの接続制限については、No.171～176も関連する項目であることから参考にすること。 |
| | 6.3.<br>システム開発、導入、保守等 | (1)<br>機器等の調達に係る運用規程の整備 | 248 | | **ⅰ）機器等の選定基準**<br>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、機器等の選定基準が運用規程として文書化されている。また、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続が整備されている。 | □機器等の選定基準<br>□納入時の確認・検査手続 | 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、機器等の選定基準を運用規程や、機器等の納入時の確認・検査手続が整備され、文書化されているか確認する。また、選定基準の一つとして、機器等の開発等のライフサイクルで不正な変更が加えられないような対策が含まれているか確かめる。 | 6.3.(1) | 8.29 | |
| | | (2)<br>情報システムの調達 | 249 | | **ⅰ）情報システムの調達における情報セキュリティに関わる基準**<br>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、情報システムの調達における情報セキュリティに関わる基準が定められ、文書化されている。 | □情報システム調達基準 | 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、情報システムの開発、導入、保守等の調達における情報セキュリティに関わる基準が文書化され、正式に承認されているか確かめる。 | 6.3.(2) | 5.8<br>8.30 | |
| | | | 250 | ○ | **ⅱ）セキュリティ機能の明記**<br>情報システムを調達する場合、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、必要とする技術的なセキュリティ機能が調達仕様書に明記されている。 | □調達仕様書 | 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、情報システム開発、導入、保守等の調達にあたり、アクセス制御機能やパスワード設定機能、ログ取得機能、データ暗号化等、必要とする技術的なセキュリティ機能が調達仕様書に明記されているか確かめる。 | 6.3.(2)① | 5.8<br>8.30 | |
| | | | 251 | | **ⅲ）セキュリティ機能の調査**<br>機器及びソフトウェアを調達する場合、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、セキュリティ機能が調査され、安全性が確認されている。 | □調達仕様書<br>□セキュリティ機能調査結果 | 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、機器及びソフトウェアの調達にあたり、セキュリティ機能が調査され、安全性が確認されているか確かめる。 | 6.3.(2)② | 5.8<br>8.30 | |
| | | (3)<br>情報システムの開発 | 252 | | **ⅰ）システム開発に関わる基準**<br>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、情報システムの開発に関わる基準が定められ、文書化されている。 | □システム開発基準 | 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、情報システムの開発に関わる基準が文書化され、正式に承認されているか確かめる。 | 6.3.(3) | 5.8<br>8.27<br>8.30 | |

| 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 |
|---|---|---|---|---|---|---|---|---|
| | 253 | ○ | **ⅱ）システム開発における責任者及び作業者の特定**<br>情報システム管理者によって、システム開発の責任者及び作業者が特定され、システム開発の規則が確立されている。 | □システム開発体制図<br>□システム開発規則 | 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、システム開発の責任者及び作業者が特定されているか確かめる。<br>あわせて、システム開発の規則が定められているか確かめる。 | 6.3.(3)① | 5.8<br>8.27<br>8.30 | |
| | 254 | | **ⅲ）システム開発用IDの管理**<br>情報システム管理者によって、システム開発の責任者及び作業者が使用する開発用IDが管理されている。 | □開発用ID登録・削除手続<br>□開発用ID登録・削除申請書<br>□開発用ID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により、システム開発の責任者及び作業者が使用する開発用IDが管理され、開発完了後は削除されているか確かめる。 | 6.3.(3)②(ア) | 5.15<br>5.16<br>5.18<br>8.2 | |
| | 255 | ○ | **ⅳ）システム開発の責任者及び作業者のアクセス権限設定**<br>情報システム管理者によって、システム開発の責任者及び作業者のアクセス権限が設定されている。 | □アクセス権限設定書<br>□開発用ID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により、システム開発の責任者及び作業者のアクセス権限が設定されているか確かめる。 | 6.3.(3)②(イ) | 5.15<br>5.16<br>5.18<br>8.2<br>8.4 | |
| | 256 | | **ⅴ）システム開発に用いるハードウェア及びソフトウェアの特定**<br>情報システム管理者によって、システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアが特定されている。 | □システム開発・保守計画 | 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、システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアが特定されているか確かめる。 | 6.3.(3)③(ア) | 8.19 | |
| | 257 | | **ⅵ）許可されていないソフトウェアの削除**<br>利用が認められていないソフトウェアが導入されている場合、情報システム管理者によって、当該ソフトウェアがシステムから削除されている。 | □システム開発・保守計画 | 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、利用が認められていないソフトウェアが導入されている場合、当該ソフトウェアをシステムから削除しているか確かめる。 | 6.3.(3)③(イ) | 8.19 | |
| | 258 | | **ⅶ）脆弱性の排除**<br>情報システム管理者によって、ウェブアプリケーションの開発時には、セキュリティ要件として定めた仕様に加えて、既知の種類のウェブアプリケーションの脆弱性を排除するための対策が講じられている。 | □システム開発・保守計画 | 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、定めた仕様に加え、既知の種類のウェブアプリケーションの脆弱性を排除するための対策が講じられているか確かめる。 | 6.3.(3)④ | 8.29 | |
| (4)<br>情報システムの導入 | 259 | | **ⅰ）情報システムの導入に関わる基準**<br>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、情報システムの導入に関わる基準が定められ、文書化されている。 | □情報システム導入基準 | 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、情報システムの導入に関わる基準が文書化され、正式に承認されているか確かめる。 | 6.3.(4) | 8.29<br>8.31 | |
| | 260 | | **ⅱ）開発環境と運用環境の分離**<br>情報システム管理者によって、システム開発、保守及びテスト環境とシステム運用環境が分離されている。 | □情報システム導入基準 | 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、管理区域の視察により、システム開発、保守及びテスト環境とシステム運用環境が分離されているか確かめる。 | 6.3.(4)①(ア) | 8.31 | |

| 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 |
|---|---|---|---|---|---|---|---|---|
| | 261 | | **ⅲ）移行手順の明確化**<br>情報システム管理者によって、システム開発・保守及びテスト環境からシステム運用環境への移行について、システム開発・保守計画策定時に手順が明確にされている。 | □システム開発・保守計画<br>□移行手順書 | 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、システム開発・保守及びテスト環境からシステム運用環境への移行について、システム開発・保守計画策定時に手順が明確にされているか確かめる。 | 6.3.(4)①<br>(イ) | 8.29 | |
| | 262 | | **ⅳ）移行に伴う情報システム停止等の影響の最小化**<br>システム移行の際、情報システム管理者によって、情報システムへの影響が最小限になるよう措置が移行前に検討されている。 | □システム開発・保守計画<br>□移行手順書 | 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、システム移行の際、情報システムに記録されている情報資産の保存を確実に行い、情報システムの停止等の影響が最小限になるよう、移行前に検討されているか確かめる。 | 6.3.(4)①<br>(ウ) | 8.29 | |
| | 263 | | **ⅴ）情報システム導入時の可用性確認**<br>システム導入の際、システムやサービスの可用性が確保されていることを確認した上で、導入がされている。 | □情報システム導入基準<br>□移行手順書 | 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、システム導入の際、障害によるシステム停止や広域災害時に備え、システムの冗長性や可用性が確保されていることを確認した上で、システム導入を行っているか確かめる。 | 6.3.(4)①<br>(エ) | 5.20<br>5.21<br>8.14<br>8.27 | |
| | 264 | ○ | **ⅰ）導入前のテスト実施**<br>新たに情報システムを導入する場合、情報システム管理者によって、既に稼動している情報システムに接続する前に十分なテストが行われている。 | □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により、新たに情報システムを導入する場合、既に稼動している情報システムに接続する前に十分なテストが行われているか確かめる。 | 6.3.(4)②<br>(ア) | 8.29 | |
| | 265 | | **ⅱ）擬似環境での操作確認**<br>運用テストを行う場合、情報システム管理者によって、あらかじめ擬似環境による操作確認が行われている。 | □システムテスト計画書／報告書<br>□ユーザテスト計画書／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により、運用テストを実施する場合、あらかじめ擬似環境による操作確認が行われているか確かめる。 | 6.3.(4)②<br>(イ) | 8.29 | |
| | 266 | ○ | **ⅲ）個人情報及び機密性の高い生データの使用禁止**<br>個人情報及び機密性の高い生データは、テストデータとして使用されていない。 | □システムテスト計画書／報告書<br>□ユーザテスト計画書／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により、個人情報及び機密性の高い生データを、テストデータとして使用していないか確かめる。 | 6.3.(4)②<br>(ウ) | 8.29<br>8.33 | |
| | 267 | | **ⅳ）独立した受け入れテスト**<br>受け入れテストを行う場合、開発した組織と導入する組織が、それぞれ独立したテストを実施する。 | □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により、他組織で開発された情報システムを受け入れる場合、開発した組織と導入する組織が、それぞれ独立したテストを実施しているか確かめる。 | 6.3.(4)②<br>(エ) | 8.29<br>8.33 | |
| | 268 | | **ⅴ）委託事業者の監督**<br>業務システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮したテスト計画を策定し、確実に検証が実施されるよう、必要かつ適切に委託事業者の監督が行われている。 | □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により、確実に検証が実施されているか確かめる。 | 6.3.(4)②<br>(オ) | 8.29 | |



別紙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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | 269 | | **vi）情報システムの受入れ時の確認・検査**<br>情報システム管理者によって、機器等の納入時又は情報システムの受入れ時の確認・検査において、調達仕様書等で定められた検査手続に従い、情報セキュリティ対策に係る要件が満たされていることが確認されている。 | □調達仕様書 | 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、調達仕様書等で定められた検査手続に従って、情報セキュリティ対策に係る要件が満たされていることが確認されているか確かめる。 | 6.3.(4)③(ア) | 8.29 | |
| | | | 270 | | **vii）情報システムが構築段階から運用保守段階へ移行する際**<br>情報システム管理者によって、当該情報システムの開発事業者から運用保守事業者へ引継がれる項目に、情報セキュリティ対策に必要な内容が含まれていることが確認されている。 | □情報システム引継書 | 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、開発事業者から運用保守事業者へ引継がれる項目に、情報セキュリティ対策に必要な内容が含まれていることを確認されているか確かめる。 | 6.3.(4)③(イ) | 8.30 | |
| | | (5)<br>情報システムの基盤を管理又は制御するソフトウェア導入時の対策 | 271 | | **ⅰ）端末、サーバ装置、通信回線装置等及びソフトウェアの保護**<br>情報システム管理者によって、情報セキュリティの観点から情報システムの基盤を管理又は制御するソフトウェアを機器等及びソフトウェア自体を保護するための措置が講じられている。 | □情報システム調達基準 | 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により、情報システムの基盤を管理又は制御するソフトウェアを導入する端末、サーバ装置、通信回線装置等及びソフトウェア自体を保護するための措置が講じられているか確かめる。 | 6.3.(5)① | 8.18 | |
| | | | 272 | | **ⅱ）実施手順の整備**<br>情報システム管理者によって、利用するソフトウェアの特性を踏まえた実施手順が整備され、文書化されている。 | □情報セキュリティ水準の維持に関する手順<br>□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、情報システムの基盤を管理又は制御するソフトウェアの情報セキュリティ水準の維持に関する手順、及び情報システムの基盤を管理又は制御するソフトウェアで発生した情報セキュリティインシデントを認知した際の対処手順が文書化されているか確かめる。 | 6.3.(5)② | 8.19 | |
| | | (6)<br>情報システムの基盤を管理又は制御するソフトウェア運用時の対策 | 273 | | **ⅰ）セキュリティ対策の実施**<br>情報システム管理者によって、情報システムの基盤を管理又は制御するソフトウェアを運用・保守する場合にセキュリティ対策が実施されている。 | □情報セキュリティ水準の維持に関する手順<br>□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情報システム管理者へのインタビューにより、導入時に定めた実施手順に従いセキュリティ対策が実施されているか確かめる。 | 6.3.(6)① | 8.32 | |
| | | | 274 | | **ⅱ）ソフトウェアの定期的な確認**<br>情報システム管理者によって、利用を認めるソフトウェアが定期的に確認され、見直しが行われている。 | □ソフトウェア管理台帳 | 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により、利用を認めるソフトウェアが定期的に確認され、見直しが行われているか確かめる。 | 6.3.(6)② | 5.9 | |

別紙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 |
|---|---|---|---|---|---|---|---|---|---|
| | (7) システム開発・保守に関連する資料等の整備・保管 | 275 | | **ⅰ)システム開発・保守に関連する資料等の整備・保管に関わる基準**<br>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、システム開発・保守に関連する資料等の整備・保管に関わる基準が定められ、文書化されている。 | □システム開発・保守に関連する資料等の保管基準 | 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、システム開発・保守に関連する資料等の整備・保管に関わる基準が文書化され、正式に承認されているか確かめる。<br>情報システム台帳のセキュリティ要件に係る内容を記録し、統括情報セキュリティ責任者に報告しているか確かめる。<br>情報システムを構成するサーバ装置及び端末関連情報や情報システムを構成する通信回線及び通信回線装置関連情報を含む情報システム関連文書が整備されているか確かめる。<br>情報システム構成要素ごとの情報セキュリティ水準の維持、情報セキュリティインシデントを認知した際の対処、及び情報システムが停止した際の復旧を含む実施手順が整備されているか確かめる。 | 6.3.(7) | ― | |
| | | 276 | ○ | **ⅱ)資料等の保管**<br>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正に整備・保管されている。 | □システム開発基準<br>□システム仕様書等<br>□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.(7)① | ― | |
| | | 277 | ○ | **ⅲ)テスト結果の保管**<br>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<br>□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.(7)② | ― | |
| | | 278 | ○ | **ⅳ)ソースコードの保管**<br>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<br>□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.(7)③ | 8.4 | |
| | (8) 情報システムにおける入出力データの正確性の確保 | 279 | | **ⅰ)データの入力処理時の正確性の確保**<br>情報システム管理者によって、データ入力時のチェック機能が組み込まれるように情報システムが設計されている。 | □システム仕様書等<br>□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、データの入力処理時における範囲、妥当性のチェック機能及びデータの不正な文字列等の入力を除去する機能が組み込まれた設計となっているか確かめる。 | 6.3.(8)① | ― | |
| | | 280 | | **ⅱ)ウェブアプリケーションやウェブコンテンツのセキュリティ対策**<br>情報システム管理者によって、ウェブアプリケーションやウェブコンテンツのセキュリティ対策が実施されている。 | □システム仕様書等<br>□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、利用者の情報セキュリティ水準の低下を招かぬアプリケーション及びウェブコンテンツの提供方式の見直し、定期的な脆弱性対策状況の確認、脆弱性が発覚した際の措置、データの内部処理時に起こるおそれのあるデータ抽出条件の誤りやデータベース更新処理時の計算式のミスなど、故意又は過失による情報の改ざん又は漏えいを検出するチェック機能を組み込んだ情報システムが設計されているか確かめる。 | 6.3.(8)② | ― | |
| | | 281 | | **ⅲ)データの出力処理時の正確性の確保**<br>情報システム管理者によって、データが出力処理される際に情報の処理が正しく反映され、出力されるように情報システムが設計されている。 | □システム仕様書等<br>□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、データの出力処理時に情報の処理が正しく反映され、出力されるように情報システムが設計されているか確かめる。 | 6.3.(8)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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | (9)<br>情報システムの変更管理 | 282 | | **ⅰ)システムの変更管理に関わる基準**<br>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、情報システムを変更した場合の変更管理に関わる基準が定められ、文書化されている。 | □システム変更管理基準 | 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、情報システムを変更した場合の変更管理に関わる基準が文書化され、正式に承認されているか確かめる。 | 6.3.(9) | 8.32 | |
| | | | 283 | ○ | **ⅱ)変更履歴の作成**<br>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<br>□システム仕様書等<br>□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.(9) | 8.32 | |
| | | (10)<br>開発・保守用のソフトウェアの更新等 | 284 | | **ⅰ)開発・保守用ソフトウェアの更新等**<br>情報システム管理者によって、開発・保守用のソフトウェア等を更新、又はパッチの適用をする場合、他の情報システムとの整合性が確認されている。 | □システム開発基準<br>□ソフトウェア管理台帳 | 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により、運用環境のシステム保守状況を踏まえて、開発・保守用のソフトウェア等を更新、又はパッチの適用をする場合、他の情報システムとの整合性が確認されているか確かめる。 | 6.3.(10) | 8.8<br>8.29<br>8.32 | |
| | | (11)<br>システム更新又は統合時の検証等 | 285 | | **ⅰ)システム更新又は統合時の検証等**<br>情報システム管理者によって、システム更新又は統合時に伴うリスク管理体制の構築、移行基準の明確化及び更新・統合後の業務運営体制の検証が行われている。 | □統合時影響検討書<br>□システム統合手順書<br>□異常時復旧手順 | 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、システム更新・統合に伴うリスクの事前検証を実施し、リスクに応じたシステム更新・統合手順及び異常事態発生時の復旧手順が策定されているか確かめる。 | 6.3.(11) | 8.29 | |
| | | (12)<br>情報システムについての対策の見直し | 286 | | **ⅰ)システム更新又は統合時の検証等**<br>情報システム管理者によって、対策の推進計画等に基づき情報システムの情報セキュリティ対策を適切に見直しされている。また、本市内で横断的に改善が必要となる情報セキュリティ対策の見直しによる改善指示に基づき、情報セキュリティ対策を適切に見直ししている。 | □情報システム推進計画 | 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、対策の推進計画等に基づいた情報システムの情報セキュリティ対策が適切に見直しされているか確かめる。<br>本市内で横断的に改善が必要となる情報セキュリティ対策の見直しは、改善指示に基づき、情報セキュリティ対策がを適切に見直しされているか確かめる。<br>なお、措置の結果については、統括情報セキュリティ責任者へ報告しているか確かめる。 | 6.3.(11) | 8.32 | |
| | 6.4.<br>不正プログラム対策 | - | 287 | ○ | **ⅰ)不正プログラム対策に関わる基準及び手順**<br>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<br>□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. | 8.7<br>8.20 | |
| | | (1)<br>統括情報セキュリティ責任者の措置事項 | 288 | | **ⅰ)外部ネットワークから受信したファイルのチェック**<br>統括情報セキュリティ責任者によって、インターネットのゲートウェイで外部ネットワークから受信したファイルに不正プログラムが含まれていないかどうかチェックされている。 | □不正プログラム対策基準<br>□不正プログラム対策手順書<br>□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により、不正プログラムのシステムへの侵入を防止するために、外部ネットワークから受信したファイルがインターネットのゲートウェイで、不正プログラムが含まれていないかどうかチェックされているか確かめる。 | 6.4.(1)① | 8.7 | |

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | 289 | | **ⅱ）外部ネットワークへ送信するファイルのチェック**<br>統括情報セキュリティ責任者によって、インターネットのゲートウェイで外部ネットワークへ送信するファイルに不正プログラムが含まれていないかチェックされている。 | □不正プログラム対策基準<br>□不正プログラム対策手順書<br>□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により、不正プログラムの外部への拡散を防止するために、インターネットゲートウェイで、外部ネットワークへ送信するファイルに不正プログラムが含まれていないかどうかチェックされているか確かめる。 | 6.4.(1)② | 8.7 | |
| | | | 290 | | **ⅲ）職員等への注意喚起**<br>統括情報セキュリティ責任者によって、コンピュータウイルス等の不正プログラム情報が収集され、必要に応じ職員等に注意喚起されている。 | □不正プログラム対策基準<br>□不正プログラム対策手順書<br>□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、コンピュータウイルス等の不正プログラム情報が収集され、必要に応じ職員等に注意喚起されているか確かめる。 | 6.4.(1)③ | 8.7 | |
| | | | 291 | | **ⅳ）不正プログラム対策ソフトウェアの常駐**<br>統括情報セキュリティ責任者によって、所掌するサーバ及びパソコン等の端末に、不正プログラム対策ソフトウェアを常駐させている。 | □不正プログラム対策基準<br>□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、所掌するサーバ及びパソコン等の端末に、不正プログラム対策ソフトウェアを常駐させているか確かめる。 | 6.4.(1)④ | 8.7 | |
| | | | 292 | ○ | **ⅴ）パターンファイルの更新**<br>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<br>□不正プログラム対策手順書<br>□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 | 8.7<br>8.8 | |
| | | | 293 | ○ | **ⅵ）不正プログラム対策ソフトウェアの更新**<br>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<br>□不正プログラム対策手順書<br>□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、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.(1)⑥ | 8.7<br>8.8<br>8.32 | |
| | | | 294 | ○ | **ⅶ）サポート終了ソフトウェアの使用禁止**<br>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<br>□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 | － | |
| | | (2)<br>情報システム管理者の措置事項 | 295 | | **ⅰ）不正プログラム対策ソフトウェアの常駐**<br>情報セキュリティ管理者によって、所掌するサーバ及びパソコン等の端末に、不正プログラム対策ソフトウェアを常駐させている。 | □不正プログラム対策基準<br>□不正プログラム対策手順書 | 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、サーバ及びパソコン等の確認により、所掌するサーバ及びパソコン等の端末に、不正プログラム対策ソフトウェアを常駐させているか確かめる。 | 6.4.(2)① | 8.7 | |

| 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 |
|---|---|---|---|---|---|---|---|---|
| | 296 | ○ | **ⅱ）パターンファイルの更新**<br>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<br>□不正プログラム対策手順書<br>□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 | 8.7<br>8.8 | |
| | 297 | | **ⅲ）不正プログラム対策ソフトウェアの更新**<br>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<br>□不正プログラム対策手順書<br>□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 | 8.7<br>8.8<br>8.32 | |
| | 298 | | **ⅳ）インターネット接続していないシステムにおける不正プログラム対策**<br>インターネットに接続していないシステムにおいて電磁的記録媒体を使う場合、情報セキュリティ管理者によって、不正プログラム対策が実施されている。 | □不正プログラム対策基準<br>□不正プログラム対策手順書<br>□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により、インターネットに接続していないシステムにおいて電磁的記録媒体を使う場合、管理外電磁的記録媒体の使用禁止、不正プログラム対策ソフトウェア導入、ソフトウェア及びパターンファイルの定期的な更新等、不正プログラム対策が実施されているか確かめる。 | 6.4.(2)④ | 8.7 | |
| | 299 | | **ⅴ）不正プログラム対策ソフトウェアの一括管理**<br>情報システム管理者によって、不正プログラム対策ソフトウェア等の設定変更権限が一括管理されており、職員等に当該権限を付与されていない。 | □不正プログラム対策基準<br>□不正プログラム対策手順書<br>□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、情報システム管理者へのインタビュー及び実際の設定を確認することにより、不正プログラム対策ソフトウェアの設定権限が一括管理されているか確かめる。 | 6.4.(2)⑤ | 8.7<br>8.8 | |
| (3)<br>職員等の遵守事項 | 300 | | **ⅰ）不正プログラム対策ソフトウェアの設定変更の禁止**<br>パソコン、モバイル端末に不正プログラム対策ソフトウェアが導入されている場合、職員等によって、不正プログラム対策ソフトウェアの設定が変更されていない。 | □不正プログラム対策基準<br>□不正プログラム対策手順書<br>□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、職員等がパソコン、モバイル端末に導入されている不正プログラム対策ソフトウェアの設定を変更し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。 | 6.4.(3)① | 8.7 | |
| | 301 | ○ | **ⅱ）データ等取り入れ時のチェック**<br>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<br>□不正プログラム対策手順書<br>□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 | 5.14<br>8.7 | |
| | 302 | ○ | **ⅲ）出所不明なファイルの削除**<br>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<br>□不正プログラム対策基準<br>□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 | 5.14<br>8.7 | |
| | 303 | ○ | **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**<br>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<br>□不正プログラム対策手順書<br>□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 | 8.7 | |

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | 304 | | **ⅴ）ファイル送受信時のチェック**<br>添付ファイルが付いた電子メールを送受信する場合、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及び無害化処理が行われている。 | □不正プログラム対策基準<br>□不正プログラム対策手順書<br>□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、添付ファイルが付いた電子メールを送受信する場合、不正プログラム対策ソフトウェアによるチェック及び無害化処理が行われているか確かめる。 | 6.4.(3)⑤ | 5.14<br>8.7 | 無害化に関してはNo.24にて記載 |
| | | | 305 | | **ⅵ）ウイルス情報の確認**<br>統括情報セキュリティ責任者から提供されるウイルス情報が職員等によって、常に確認されている。 | □不正プログラム対策基準<br>□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、統括情報セキュリティ責任者から提供されるウイルス情報が常に確認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)⑥ | 6.8<br>8.7 | |
| | | | 306 | ○ | **ⅶ）不正プログラムに感染した場合の対処**<br>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<br>□不正プログラム対策手順書<br>□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 | 5.24 | ・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.343～346も関連する項目であることから参考にすること。 |
| | | (4)<br>専門家の支援体制 | 307 | | **ⅰ）専門家による支援体制の確保**<br>実施している不正プログラム対策では不十分な事態が発生した場合に備えて、統括情報セキュリティ責任者によって、外部の専門家の支援が受けられるようになっている。 | □不正プログラム対策基準<br>□不正プログラム対策手順書<br>□業務委託契約書 | 監査資料のレビューと統括情報セキュリティ責任者、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、実施している不正プログラム対策では不十分な事態が発生した場合に備えて、外部の専門家の支援が受けられるようになっているか確かめる。 | 6.4.(4) | 5.6 | ・不正プログラム対策に関する情報については、外部の専門家から支援を受けるほか、公的なセキュリティ機関、定評のある刊行物、信頼できるインターネットサイト等からも収集することが望ましい。 |
| | 6.5.<br>不正アクセス対策 | | 308 | | **ⅰ）不正アクセス対策に関わる基準及び対応手順**<br>統括情報セキュリティ責任者によって、不正アクセス対策に関わる基準及び対応手順が定められ、文書化されている。 | □不正アクセス対策基準<br>□不正アクセス対応手順書 | 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、不正アクセス対策に関わる基準及び対応手順が文書化され、正式に承認されているか確かめる。 | 6.5. | 5.24<br>5.25<br>5.26<br>5.27<br>5.28<br>5.29<br>6.8 | ・ネットワークの管理については、No.165～168、171～176も関連する項目であることから参考にすること。 |
| | | (1)<br>統括情報セキュリティ責任者の措置事項 | 309 | | **ⅰ）未使用ポートの閉鎖**<br>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<br>□ネットワーク管理記録<br>□ファイアウォール設定<br>□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.175～176も関連する項目であることから参考にすること。 |
| | | | 310 | | **ⅱ）不要なサービスの削除又は停止**<br>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<br>□不正アクセス対応手順書<br>□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 | － | |

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | 311 | | **ⅲ）ウェブページ改ざんの検知**<br>不正アクセスによるウェブページの改ざんを検出した場合、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通報するよう設定されている。 | □不正アクセス対策基準<br>□不正アクセス対応手順書<br>□システム監視手順書<br>□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システム管理者へのインタビューにより、不正アクセスによるウェブページのデータの書換えを検出し、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するよう設定しているか確かめる。 | 6.5.(1)③ | 6.8 | |
| | | | 312 | | **ⅳ）システム設定ファイルの検査**<br>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<br>□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)④ | 6.8 | |
| | | | 313 | | **ⅴ）連絡体制の構築**<br>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)⑤ | 5.24<br>6.8 | |
| | | (2)<br>攻撃への対処 | 314 | | **ⅰ）攻撃に対する措置**<br>サーバ等に攻撃を受けた場合又は攻撃を受けるリスクがある場合は、CISO及び統括情報セキュリティ責任者によって、必要な措置が講じられるとともに、関係機関から情報が収集されている。 | □緊急時対応計画<br>□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システム管理者へのインタビューにより、サーバ等に攻撃を受けた場合又は攻撃を受けるリスクがある場合、システムの停止等の適切な措置が講じられ、関係機関から情報が収集されているか確かめる。 | 6.5.(2) | 5.5<br>5.6<br>5.29 | |
| | | (3)<br>記録の保存 | 315 | | **ⅰ）記録の保存**<br>サーバ等に犯罪の可能性がある攻撃を受けた場合、CISO及び統括情報セキュリティ責任者によって、攻撃の記録が保存されるとともに、警察及び関係機関と連携・調整し、事案に対して適切に対応している。 | □緊急時対応計画<br>□情報セキュリティインシデント報告書<br>□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、サーバ等に対し不正アクセス禁止法違反等犯罪の可能性がある攻撃を受けた場合、攻撃の記録が保存され、警察及び関係機関と連携・調整し、事案に対して適切に対応しているか確かめる。 | 6.5.(3) | 5.5<br>5.6<br>5.28 | ・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。<br>・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.342～ |
| | | (4)<br>内部からの攻撃 | 316 | | **ⅰ）内部からの攻撃の監視**<br>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、職員等及び委託事業者が使用しているパソコン等の端末からの庁内のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視し、有線の端末間で通信が行われない設定が可能であれば講じられている。 | □端末ログ<br>□監視記録<br>□ネットワーク管理基準<br>□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、職員等及び委託事業者が使用しているパソコン等の端末からの庁内のサーバ等や外部のサイトに対する攻撃が監視され、有線の端末間で通信が行われない設定が可能であればされているか確かめる。 | 6.5.(4) | 6.8 | ・情報システムの監視については、No.325～332も関連する項目であることから参考にすること。 |
| | | (5)<br>職員等による不正アクセス | 317 | | **ⅰ）職員等の不正アクセスに対する処置**<br>職員等による不正アクセスが発見された場合、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、当該職員等が所属する課室等の情報セキュリティ管理者に通知され、適切な処置が求められている。 | □情報セキュリティインシデント報告書<br>□通知書 | 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管理者及び情報システム管理者へのインタビューにより、職員等による不正アクセスが発見された場合、当該職員の所属課室等の情報セキュリティ管理者に通知され、適切な処置が求められているか確かめる。 | 6.5.(5) | 6.4 | ・職員等の違反行為に対する対応については、No.354～356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)<br>サービス不能攻撃 | 318 | | **ⅰ)サービス不能攻撃に対する対策**<br>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、システムに対するサービス不能攻撃を防ぐため、情報システムの可用性を確保する対策が講じられている。 | □不正アクセス対策基準<br>□不正アクセス対応手順書<br>□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セキュリティ管理者及び情報システム管理者へのインタビューにより、サービス不能攻撃対策として、以下の管理策が実施されていることを確かめる。<br>・情報システムの技術的な対策<br>・通信事業者サービスの利用による対策<br>・情報システムの監視及び監視記録の保存<br>さらに、上記対策のモニタリングの実施の有無を確かめる。 | 6.5.(6) | － | |
| | | (7)<br>標的型攻撃 | 319 | | **ⅰ)標的型攻撃に対する対策**<br>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、標的型攻撃対策として人的対策や入口対策、内部対策が講じられている。 | □不正アクセス対策基準<br>□不正アクセス対応手順書<br>□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セキュリティ管理者及び情報システム管理者へのインタビューにより、標的型攻撃対策として、以下の管理策が実施されていることを確かめる。<br>・標的型攻撃メール対策としての人的対策<br>・電磁的記録媒体経由での攻撃対策となる入口対策<br>・ネットワークの通信を監視し外部との不正通信を検知して対処する等の内部対策及び出口対策<br>・不正な通信がないか、ログを確認する等の事後対策<br>さらに、上記対策のモニタリングの実施有無を確かめる。 | 6.5.(7) | － | |
| | 6.6.<br>セキュリティ情報の収集 | | 320 | | **ⅰ)セキュリティホールや不正プログラム等の情報収集に関わる基準**<br>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、サーバ装置、端末及び通信回線装置等におけるセキュリティホールや不正プログラム等の情報収集に関わる基準が定められ、文書化されている。 | □セキュリティ情報収集基準 | 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、セキュリティホールや不正プログラム等の情報収集に関わる基準が文書化され、正式に承認されているか確かめる。 | 6.6. | 8.8 | |
| | | (1)<br>セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等 | 321 | | **ⅰ)セキュリティホールの情報収集及び共有**<br>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、サーバ装置、端末及び通信回線装置等におけるセキュリティホールに関する情報が収集され、関係者間で共有されている。 | □セキュリティホール関連情報の通知記録 | 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に関する情報が収集され、情報システムを所管する部署等の関係者間で共有されているか確かめる。 | 6.6.(1) | 8.8 | ・セキュリティホールに関する情報の収集先は、1ヵ所ではなく、複数から収集していることが望ましい。 |
| | | | 322 | ○ | **ⅱ)ソフトウェアの更新**<br>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、サーバ装置、端末及び通信回線装置等における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<br>□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) | 8.8 | |
| | | (2)<br>不正プログラム等のセキュリティ情報の収集・周知 | 323 | | **ⅰ)不正プログラム等のセキュリティ情報の収集及び周知**<br>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、不正プログラム等のセキュリティ情報が収集され、必要に応じ対応方法について、職員等に周知されている。 | □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システム管理者へのインタビューにより、不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について、職員等に周知しているか確かめる。 | 6.6.(2) | 8.8 | ・不正プログラムの対策については、No.287～307も関連する項目であることから参考にすること。 |



別紙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)<br>情報セキュリティに関する情報の収集及び共有 | 324 | | **ⅰ)情報セキュリティに関する情報の収集及び共有**<br>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、情報セキュリティに関する情報が収集され、関係者間で共有されている。 | □情報セキュリティ関連情報の通知記録 | 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技術の動向や変化について情報を収集し、必要に応じ関係者で共有され、新たな脅威への対応方法について検討しているか確かめる。 | 6.6.(3) | 8.8 | |
| 7.<br>運用 | 7.1.<br>情報システムの監視 | (1)<br>情報システムの運用・保守時の対策 | 325 | | **ⅰ)情報システムの監視に関わる基準**<br>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、ネットワーク及び情報システムの稼動状況の監視に関わる基準が定められ、文書化されている。 | □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、情報システムに実装された監視を含むセキュリティ機能を適切に運用するため、ネットワーク及び情報システムの稼動状況の監視対象や監視体制、サーバの時刻設定等、情報システムの監視に関わる基準が文書化され、正式に承認されているか確かめる。 | 7.1.(1)① | 8.15 | ・監視の方法には、侵入検知システム(IDS)等の監視の専用システムを用いる方法の他に、対象システムのログによる監視がある。 |
| | | | 326 | | **ⅱ)監視の運用**<br>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、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しされている。また、危機的事象発生時に適切な対処が行えるよう運用されている。 | □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、監視運用の状況を踏まえ見直しされているか、また危機的事象発生時に適切な対処が行えるよう準備・運用されているか確かめる。 | 7.1.(1)②③ | 8.16 | |
| | | (2)<br>情報システムの監視機能 | 327 | | **ⅰ)監視機能の実装**<br>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、情報システム運用時の監視に係る運用管理機能要件が策定され、監視機能を実装・運用されている。 | □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、監視機能が実装されているか、また適切に運用されているか確かめる。 | 7.1.(2)①② | 8.15<br>8.16 | |
| | | | 328 | | **ⅱ)監視機能の定期的な見直し**<br>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、情報システムにおける監視の対象や手法が定期的に見直しされている。 | □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、新たな脅威の出現、運用の状況等を踏まえ、監視の対象や手法が定期的に見直しされているか確かめる。 | 7.1.(2)③ | 8.16 | |
| | | | 329 | | **ⅲ)サーバ装置の監視**<br>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、サーバ装置上での情報セキュリティインシデントの発生を監視されているか。 | □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、サーバ装置上での情報セキュリティインシデントの発生を監視するため、当該サーバ装置を監視するための措置が講じられているか確かめる。 | 7.1.(2)④ | 8.16 | |
| | | (3)<br>情報システムの監視 | 330 | | **ⅱ)情報システム及びネットワークの常時監視**<br>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、セキュリティに関する事案を検知するため、ネットワーク及び情報システムが常時監視されている。 | □システム運用基準<br>□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、セキュリティに関する事案を検知するため、ネットワーク及び情報システムが常時監視されているか確かめる。 | 7.1.(3)① | 8.15 | ・監視結果は定期的に見直し、不正なアクセスなどの情報セキュリティインシデントの予兆がないか点検することが望ましい。 |

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | 331 | | **ⅲ）時刻の同期**<br>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、重要なアクセスログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期が行われている。 | □システム運用基準<br>□時刻設定手順書 | 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、アクセスログ等の証拠として正確性を確保するため、重要なアクセスログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期が行われているか確かめる。 | 7.1.(3)② | 8.17 | |
| | | | 332 | ○ | **ⅳ）外部接続システムの常時監視**<br>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<br>□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)③ | 5.22 | |
| | | | 333 | | **ⅴ）通信データの再暗号化**<br>暗号化された通信データを監視のために復号することの要否が判断され、要すると判断された場合、当該通信データを復号する機能及び必要な場合はこれを再暗号化する機能が導入されている。 | □通信データ暗号化基準<br>□通信データ監視基準 | 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、通信データを復号することが基準どおり判断されているか、また適切に復号、再暗号化がされているか確かめる。 | 7.1.(3)④ | 5.31 | |
| | 7.2.<br>情報セキュリティポリシーの遵守状況の確認 | (1)<br>遵守状況の確認及び対処 | 334 | | **ⅰ）情報セキュリティポリシーの遵守状況の確認及び問題発生時の対応に関わる基準**<br>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、情報セキュリティポリシーの遵守状況についての確認及び問題発生時の対応に関わる基準が定められ、文書化されている。 | □情報セキュリティポリシー<br>□システム運用基準<br>□情報セキュリティインシデント報告手順書<br>□自己点検実施基準 | 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の遵守状況についての確認及び問題発生時の対応に関わる基準が文書化され、正式に承認されているか確かめる。 | 7.2.(1) | 5.24<br>5.36<br>6.8 | |
| | | | 335 | | **ⅱ）情報セキュリティポリシーの遵守状況の確認**<br>情報セキュリティ責任者及び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の遵守状況についての確認が行われ、問題が認められた場合には、速やかにCISO及び統括情報セキュリティ責任者に報告されている。 | □情報セキュリティポリシー<br>□システム運用基準<br>□情報セキュリティインシデント報告手順書<br>□情報セキュリティインシデント報告書<br>□自己点検実施基準<br>□自己点検結果 | 監査資料のレビューと情報セキュリティ責任者及び情報セキュリティ管理者へのインタビューにより、情報セキュリティポリシーの遵守状況についての確認が行われ、問題が認められた場合には、速やかにCISO及び統括情報セキュリティ責任者に報告されているか確かめる。 | 7.2.(1)① | 5.24<br>5.36<br>6.8 | |
| | | | 336 | ○ | **ⅲ）発生した問題への対処**<br>CISOによって、情報セキュリティポリシー遵守上の問題に対して、適切かつ速やかに対処されている。 | □情報セキュリティインシデント報告手順書<br>□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へのインタビューにより、CISOに報告された情報セキュリティポリシー遵守上の問題に対して、適切かつ速やかに対処されているか確かめる。 | 7.2.(1)② | 5.24<br>5.36 | |
| | | | 337 | ○ | **ⅳ）システム設定等における情報セキュリティポリシーの遵守状況の確認及び問題発生時の対処**<br>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、システム設定等における情報セキュリティポリシーの遵守状況について定期的に確認が行われ、問題が発生していた場合には適切かつ速やかに対処されている。 | □情報セキュリティポリシー<br>□システム運用基準<br>□情報セキュリティインシデント報告手順書<br>□情報セキュリティインシデント報告書<br>□自己点検実施基準<br>□自己点検結果 | 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、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について定期的に確認が行われ、問題が発生していた場合には適切かつ速やかに対処されているか確かめる。 | 7.2.(1)③ | 5.24<br>5.36<br>6.8 | |

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | (2) パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査 | 338 | | **ⅰ）パソコン、モバイル端末及び電磁的記録媒体等の利用状況の調査に関わる基準**<br>CISO及びCISOが指名した者によって、パソコン、モバイル端末及び電磁的記録媒体等のログ、電子メールの送受信記録等の利用状況の調査に関わる基準が定められ、文書化されている。 | □情報セキュリティポリシー<br>□利用状況調査基準 | 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セキュリティ責任者へのインタビューにより、不正アクセス、不正プログラム等の調査のために、CISO及びCISOが指名した者による職員等の使用しているパソコン、モバイル端末及び電磁的記録媒体等のログ、電子メールの送受信記録等の利用状況の調査に関わる基準が文書化され、正式に承認されているか確かめる。 | 7.2.(2) | 8.15 | |
| | | | 339 | | **ⅱ）パソコン、モバイル端末及び電磁的記録媒体等の利用状況の調査**<br>不正アクセス、不正プログラム等の調査のために、CISO及びCISOが指名した者によって、パソコン、モバイル端末及び電磁的記録媒体等のログ、電子メールの送受信記録等の利用状況が必要に応じて調査されている。 | □利用状況調査結果 | 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、不正アクセス、不正プログラム等の調査のために、CISO及びCISOが指名した者によって、職員等が使用しているパソコン、モバイル端末及び電磁的記録媒体等のログ、電子メールの送受信記録等の利用状況が必要に応じて調査されているか確かめる。 | 7.2.(2) | 8.15 | |
| | | (3) 職員等の報告義務 | 340 | | **ⅰ）情報セキュリティポリシー違反発見時の対応に関わる手順**<br>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、情報セキュリティポリシーに対する違反行為を発見した場合の対応に関わる手順が定められ、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ポリシーに対する違反行為を発見した場合の対応に関わる手順が文書化され、正式に承認されているか確かめる。 | 7.2.(3) | 5.24 | |
| | | | 341 | ○ | **ⅱ）情報セキュリティポリシー違反発見時の報告**<br>情報セキュリティポリシーに対する違反行為が発見された場合、職員等によって、直ちに統括情報セキュリティ責任者及び情報セキュリティ管理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<br>□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管理者、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に対する違反行為が発見された場合、直ちに統括情報セキュリティ責任者及び情報セキュリティ管理者に報告されているか確かめる。 | 7.2.(3)① | 5.24 | |
| | | | 342 | ○ | **ⅲ）発見された違反行為に対する対処**<br>情報セキュリティポリシーに対する違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると統括情報セキュリティ責任者が判断した場合、統括情報セキュリティ責任者によって、緊急時対応計画に従った対処が行われている。 | □情報セキュリティインシデント報告手順書<br>□情報セキュリティインシデント報告書<br>□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及び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に対する違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると統括情報セキュリティ責任者が判断した場合、緊急時対応計画に従った対処が行われているか確かめる。 | 7.2.(3)② | 5.24 | ・緊急時対応計画については、No.343～346も関連する項目であることから参考にすること。 |
| | 7.3. 侵害時の対応等 | | 343 | | **ⅰ）緊急時対応計画に関わる基準**<br>統括情報セキュリティ責任者によって、情報資産に対するセキュリティ侵害が発生した場合又は発生するおそれのある場合の緊急時対応計画に関わる基準が定められ、文書化されている。 | □情報セキュリティポリシー | 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、情報セキュリティインシデント、情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合又は発生するおそれのある場合の緊急時対応計画に関わる基準が文書化され、正式に承認されているか確かめる。 | 7.3. | 5.29 | ・緊急時対応計画の策定においては、自然災害、事故、装置の故障及び悪意による行為の結果などの情報セキュリティインシデント発生時における住民からの問合せ方法・窓口は常に明確にしておくことが望ましい。 |

| 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)<br>緊急時対応計画の策定<br><br>(2)<br>緊急時対応計画に盛り込むべき内容 | 344 | ○ | **ⅱ）緊急時対応計画の策定**<br>CISO又は情報セキュリティ委員会によって、緊急時対応計画が定められている。 | □緊急時対応計画<br>□情報セキュリティ委員会議事録 | 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、緊急時対応計画が定められているか確かめる。 | 7.3.(1)～(2) | 5.24<br>5.29 | |
| | | (3)<br>業務継続計画との整合性確保 | 345 | | **ⅰ）業務継続計画との整合性確保**<br>業務継続計画を策定する場合、業務継続計画と情報セキュリティポリシーの整合性が確保されている。 | □業務継続計画<br>□情報セキュリティポリシー<br>□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セキュリティ責任者へのインタビューにより、業務継続計画と情報セキュリティポリシーの整合性が確保されているか確かめる。 | 7.3.(3) | － | |
| | | (4)<br>緊急時対応計画の見直し | 346 | | **ⅰ）緊急時対応計画の見直し**<br>CISO又は情報セキュリティ委員会によって、必要に応じて緊急時対応計画の規定が見直されている。 | □緊急時対応計画<br>□情報セキュリティ委員会等の議事録 | 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、情報セキュリティ委員会によって、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて緊急時対応計画の規定が見直されているか確かめる。 | 7.3.(4) | 5.29 | |
| | 7.4.<br>例外措置 | | 347 | | **ⅰ）例外措置に関わる基準及び対応手続**<br>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、例外措置を講じる場合の基準及び対応手続が定められ、文書化されている。 | □例外措置対応基準/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セキュリティ責任者へのインタビューにより、例外措置を講じる場合の基準及び対応手続が文書化され、正式に承認されているか確かめる。 | 7.4. | － | |
| | | (1)<br>例外措置の許可 | 348 | ○ | **ⅰ）例外措置の申請及び許可**<br>情報セキュリティ関係規定の遵守が困難な状況で行政事務の適正な遂行を継続しなければならない場合、情報セキュリティ管理者及び情報システム管理者によって、CISOの許可を得たうえで例外措置が講じられている。 | □例外措置申請書/許可書<br>□例外措置実施報告書 | 監査資料のレビューと情報セキュリティ管理者又は情報システム管理者へのインタビューにより、情報セキュリティ関係規定の遵守が困難な状況で行政事務の適正な遂行を継続しなければならない場合、遵守事項とは異なる方法を採用すること又は遵守事項を実施しないことについて合理的な理由がある場合に限り、CISOの許可を得たうえで例外措置が講じられているか確かめる。 | 7.4.(1) | － | ・例外措置は単に適用を排除するだけでなく、リスクに応じて代替措置を定めていることを確認することが望ましい。 |
| | | (2)<br>緊急時の例外措置 | 349 | ○ | **ⅰ）緊急時の例外措置**<br>行政事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、情報セキュリティ管理者及び情報システム管理者によって、事後速やかにCISOに報告されている。 | □例外措置実施報告書 | 監査資料のレビューと情報セキュリティ管理者又は情報システム管理者へのインタビューにより、行政事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、例外措置実施後速やかにCISOに報告されているか確かめる。 | 7.4.(2) | － | |
| | | (3)<br>例外措置の申請書の管理 | 350 | | **ⅰ）例外措置の申請書の管理**<br>CISOによって、例外措置の申請書及び審査結果が保管され、定期的に申請状況が確認されている。 | □例外措置申請書/許可書<br>□例外措置実施報告書 | 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、CISOによって、例外措置の申請書及び審査結果が保管され、定期的に申請状況が確認されているか確かめる。 | 7.4.(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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | 7.5.<br>法令遵守 | | 351 | | **ⅰ）遵守すべき法令等の明確化**<br>統括情報セキュリティ責任者によって、職員等が職務の遂行において遵守すべき情報セキュリティに関する法令等の一覧が定められ、文書化されている。 | □関連法令等一覧 | 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、職員等が職務の遂行において遵守すべき情報セキュリティに関する法令等の一覧が定められているか確かめる。 | 7.5. | 5.31<br>5.32<br>5.33<br>5.34 | |
| | | | 352 | | **ⅱ）法令遵守**<br>職員等が職務の遂行において遵守すべき情報セキュリティに関する法令等を遵守している。 | □関連法令等一覧 | 監査資料のレビューと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、職員等が職務の遂行において遵守すべき情報セキュリティに関する法令等を遵守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。 | 7.5. | 5.31<br>5.32<br>5.33<br>5.34 | |
| | 7.6.<br>懲戒処分等 | (1)<br>懲戒処分 | 353 | ○ | **ⅰ）懲戒処分の対象**<br>統括情報セキュリティ責任者によって、情報セキュリティポリシーに違反した職員等及びその監督責任者が地方公務員法による懲戒処分の対象となることが定められ、文書化されている。 | □情報セキュリティポリシー | 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、情報セキュリティポリシーに違反した職員等及びその監督責任者が、その重大性、発生した事案の状況等に応じて、地方公務員法による懲戒処分の対象となることが文書化され、正式に承認されているか確かめる。 | 7.6.(1) | 6.4 | |
| | | (2)<br>違反時の対応 | 354 | | **ⅰ）違反時の対応手順**<br>統括情報セキュリティ責任者によって、職員等による情報セキュリティポリシーに違反する行動が確認された場合の対応手順が定められ、文書化されている。 | □情報セキュリティポリシー<br>□情報セキュリティ違反時の対応手順書 | 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、職員等による情報セキュリティポリシーに違反する行動が確認された場合の対応手順が文書化され、正式に承認されているか確かめる。 | 7.6.(2) | 5.24<br>5.28<br>5.36<br>6.4<br>6.8 | |
| | | | 355 | | **ⅱ）関係者への通知**<br>職員等による情報セキュリティポリシーに違反する行動が確認された場合、関係者に通知し、適切な措置を求めている。 | □情報セキュリティ違反時の対応手順書<br>□通知書 | 監査資料のレビューと統括情報セキュリティ責任者、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へのインタビューにより、職員等による情報セキュリティポリシーに違反する行動が確認された場合、関係者に通知し、適切な措置を求めているか確かめる。 | 7.6.(2)①<br>～② | 5.24<br>5.28<br>5.36<br>6.4 | |
| | | | 356 | | **ⅲ）情報システム使用の権利の制限**<br>情報セキュリティ管理者等の指導によっても改善がみられない場合、統括情報セキュリティ責任者によって、当該職員等のネットワーク又は情報システムを使用する権利を停止又は剥奪し、関係者に通知されている。 | □情報セキュリティ違反時の対応手順書<br>□通知書 | 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及び情報セキュリティ管理者へのインタビューにより、情報セキュリティ管理者の指導によっても改善がみられない場合、統括情報セキュリティ責任者によって当該職員等のネットワーク又は情報システムを使用する権利が停止又は剥奪され、CISO及び当該職員等の所属課室等の情報セキュリティ管理者に通知されているか確かめる。 | 7.6.(2)③ | 5.24<br>5.28<br>5.36<br>6.4<br>6.8 | |

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|
| 8.業務委託と外部サービス(クラウドサービス)の利用 | 8.1.業務委託 | (1)業務委託に係る運用規程の整備 | 357 | | **ⅰ)業務委託に係る運用規程の整備**<br>統括情報セキュリティ責任者によって、業務委託を行う場合の情報セキュリティに関わる基準が定められ、文書化されている。 | □委託判断基準<br>□委託事業者選定基準 | 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セキュリティ責任者へのインタビューにより、業務委託を行う場合の情報セキュリティに関わる基準が文書化され、正式に承認されているか確かめる。 | 8.1.(1)①② | 5.20<br>5.22<br>8.30 | ・情報セキュリティポリシー等遵守事項の委託事業者に対する説明義務については、No.109～110も関連する項目であることから参考にすること。<br>・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。 |
| | | (2)業務委託実施前の対策 | 358 | | **ⅰ)業務委託実施前の対策**<br>情報セキュリティ管理者又は情報システム管理者によって、業務委託の実施までに仕様の確定、契約締結等の必要事項が実施されている。 | □委託判断基準<br>□委託事業者選定基準<br>□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管理者又は情報システム管理者へのインタビューにより、業務委託の実施までに、委託する業務内容の特定、委託事業者の選定条件を含む仕様の策定、仕様に基づく委託事業者の選定、情報セキュリティ要件を明記した契約の締結、委託事業者に重要情報を提供する場合には秘密保持契約(NDA)の締結が行われているか確かめる。 | 8.1.(2)① | 5.19 | |
| | | | 359 | ○ | **ⅱ)委託事業者との契約**<br>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等に係る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等に係る要件が明記されているか確かめる。<br>・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<br>・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<br>・提供されるサービスレベルの保証<br>・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<br>・委託事業者の従業員に対する教育の実施<br>・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<br>・業務上知り得た情報の守秘義務<br>・再委託に関する制限事項の遵守<br>・委託業務終了時の情報資産の返還、廃棄等<br>・委託業務の定期報告及び緊急時報告義務<br>・委託元団体による監査、検査<br>・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<br>・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)① | 5.2 | ・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。<br>・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。 |
| | | | 360 | | **ⅲ)委託事業者への要求**<br>情報セキュリティ管理者又は情報システム管理者によって、業務委託の実施までに委託の前提条件を委託事業者に求めている。 | □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管理者又は情報システム管理者へのインタビューにより、業務委託の実施までに、仕様に準拠した提案、契約の締結、重要情報を取り扱う場合は、秘密保持契約(NDA)の締結が求められているかを確かめる。 | 8.1.(2)② | 5.20 | |

| 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)<br>業務委託実施期間中の対策 | 361 | | **ⅰ）業務委託実施期間中の対策**<br>情報セキュリティ管理者又は情報システム管理者によって、業務委託の実施期間に履行状況の定期的な確認等が実施されている。 | □委託管理基準<br>□作業報告書<br>□改善要望書<br>□改善措置実施報告書 | 監査資料のレビューと統括情報セキュリティ責任者又は情報セキュリティ責任者へのインタビューにより、業務委託の期間中に、委託判断基準に従った重要情報の提供、情報セキュリティ対策の履行状況の定期的な確認及び措置、統括情報セキュリティ責任者へ措置内容の報告、情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合の委託事業の一時中断が実施されているか確かめる。 | 8.1.(3)① | 5.22 | ・委託事業者の情報セキュリティポリシー等の遵守事項については、No.109～110も関連する項目であることから参考にすること。<br>・契約事項の遵守状況のほか、十分なセキュリティ対策がとられていることを確認する必要があり、特に、再委託の制限、情報の持ち出しの禁止、業務終了後のデータの返還・廃棄、支給以外のパソコンの使用について、違反がないか確認することが必要である。 |
| | | | 362 | | **ⅱ）委託事業者への要求**<br>情報セキュリティ管理者又は情報システム管理者によって、業務委託の実施期間にて実施する対策を委託事業者に求めている。 | □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管理者又は情報システム管理者へのインタビューにより、業務委託の実施期間に、情報の適正な取扱いのための情報セキュリティ対策、情報セキュリティ対策の履行状況の定期的な報告、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合の委託事業一時中断等が求められているかを確かめる。 | 8.1.(3)② | 5.20 | |
| | | (4)<br>業務委託終了時の対策 | 363 | | **ⅰ）業務委託終了時の対策**<br>情報セキュリティ管理者又は情報システム管理者によって、業務委託の終了に際して対策が実施されている。 | □委託管理基準<br>□作業完了報告書<br>□返却／廃棄・抹消証明 | 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、業務委託の終了に、セキュリティ対策が適切に実施されたことの確認を含む検収、委託事業者において取り扱われた情報が確実に返却、廃棄又は抹消されたことの確認が行われているか確かめる。 | 8.1.(4)① | 5.22 | |
| | | | 364 | | **ⅱ）委託事業者への要求**<br>情報セキュリティ管理者又は情報システム管理者によって、業務委託の終了時にて実施する対策を委託事業者に求めている。 | □委託管理基準<br>□作業完了報告書<br>□返却／廃棄・抹消証明 | 監査資料のレビューと情報セキュリティ管理者又は情報システム管理者へのインタビューにより、業務委託の終了時に、セキュリティ対策が適切に実施されたことの報告を含む検収の受検、委託業務において取り扱った情報の返却、廃棄又は抹消を求められているかを確かめる。 | 8.1.(4)② | 5.22 | |
| | 8.2.<br>情報システムに関する業務委託 | (1)<br>情報システムに関する業務委託における共通的対策 | 365 | | **ⅰ）業務委託における共通的対策**<br>情報システム管理者によって、情報システムに関する業務委託の実施までに、情報システムに本市の意図せざる変更が加えられないための対策に係る選定条件を委託事業者の選定条件に加え、仕様が策定されている。 | □委託事業者選定基準<br>□仕様 | 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、情報システムに関する業務委託の実施までに、本市の意図せざる変更が情報システムに加えられないための対策を委託事業者の選定条件に加え、仕様が策定されているかを確かめる。 | 8.2.(1) | 5.19 | |

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | (2)<br>情報システムの構築を業務委託する場合の対策 | 366 | | **ⅰ)情報システムの構築**<br>情報システム管理者によって、契約に基づいた対策の実施を委託事業者に求めている。 | □業務委託契約書 | 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、情報システムの構築を業務委託する場合、情報システムのセキュリティ要件の適切な実装、情報セキュリティの観点に基づく試験の実施、情報システムの開発環境及び開発工程における情報セキュリティ対策を委託事業者に求められているか確かめる。 | 8.2.(2) | 8.30 | |
| | | (3)<br>情報システムの運用・保守を業務委託する場合の対策 | 367 | | **ⅰ)情報システムの運用・保守**<br>情報システム管理者によって、契約に基づいた対策の実施を委託事業者に求めている。 | □委託判断基準<br>□委託事業者選定基準 | 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により、情報システムの運用・保守を業務委託する場合、情報システムに実装されたセキュリティ機能が適切に運用されるための要件を委託事業者に求められているか確かめる。<br>また、対策を実施するうえで情報システムに変更内容が生じた場合には、契約に基づいた速やかな報告を求められているか確かめる。 | 8.2.(3) | 8.30 | |
| | | (4)<br>本市向けに情報システムの一部の機能を提供するサービスを利用する場合の対策 | 368 | | **ⅰ)委託事業者の選定**<br>情報システム管理者又は情報セキュリティ管理者によって、業務委託サービスを利用する場合の業務委託において、委託事業者の選定条件に業務委託サービスに特有の選定条件が加えられている。 | □委託判断基準<br>□委託事業者選定基準 | 監査資料のレビューと情報システム管理者又は情報セキュリティ管理者へのインタビューにより、業務委託サービスを利用する場合の業務委託において、委託事業者の選定条件に業務委託サービスに特有の選定条件が加えられているか確かめる。 | 8.2.(4)① | 5.19 | |
| | | | 369 | | **ⅱ)業務委託サービスの選定**<br>情報システム管理者又は情報セキュリティ管理者によって、業務委託サービスに係るセキュリティ要件を定め、業務委託サービスを選定している。 | □業務委託サービス選定基準 | 監査資料のレビューと情報システム管理者又は情報セキュリティ管理者へのインタビューにより、業務委託サービスに係るセキュリティ要件を定め、業務委託サービスを選定しているか確かめる。 | 8.2.(4)② | 5.19 | |
| | | | 370 | | **ⅲ)委託事業者の評価・判断**<br>情報システム管理者又は情報セキュリティ管理者によって、委託事業者の信頼性が十分であることを総合的・客観的に評価し判断されている。 | □委託判断基準<br>□委託事業者選定基準 | 監査資料のレビューと情報システム管理者又は情報セキュリティ管理者へのインタビューにより、委託事業者の信頼性が十分であることを総合的・客観的に評価し判断しているか確かめる。 | 8.2.(4)③ | 5.22 | |
| | | | 371 | | **ⅳ)業務委託サービスの利用申請**<br>情報システム管理者又は情報セキュリティ管理者によって、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当該サービスの利用申請が行われている。 | □利用申請 | 監査資料のレビューと情報システム管理者又は情報セキュリティ管理者へのインタビューにより、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当該サービスの利用申請を行っているか確かめる。 | 8.2.(4)④ | － | |
| | | | 372 | | **ⅴ)利用申請の審査と記録**<br>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、業務委託サービスの利用申請を受けた場合は、当該利用申請を審査し、利用の可否を決定されている。また、業務委託サービスの利用申請を承認した場合は、承認済み業務委託サービスとして記録し、業務委託サービス管理者を指名している。 | □利用申請審査結果<br>□利用委託業務サービス記録 | 監査資料のレビューと情報システム管理者又は情報セキュリティ管理者へのインタビューにより、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は、業務委託サービスの利用申請を受けた場合は、当該利用申請を審査し、利用の可否を決定しているか確かめる。また、業務委託サービスの利用申請を承認した場合は、承認済み業務委託サービスとして記録し、業務委託サービス管理者を指名しているか確かめる。 | 8.2.(4)⑤⑥ | － | |



別紙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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | 8.3. 外部サービス(クラウドサービス)の利用(機密性2以上の情報を取り扱う場合) | (1) クラウドサービスの選定に係る運用規程の整備 | 373 | ○ | **ⅰ)クラウドサービスの選定に係る運用規程の整備**<br>統括情報セキュリティ責任者によって、クラウドサービスの選定(機密性2以上の情報を取り扱う場合)に関する基準が定められ、文書化されている。 | □クラウドサービス利用判断基準<br>□クラウドサービス提供者の選定基準 | 監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、クラウドサービスの選定に関する基準が文書化され、正式に承認されていることを確かめる。<br>また、基準には以下の事項が定められていることを確かめる。<br>・クラウドサービスが利用可能な業務及び情報システムの範囲や情報の取扱いを許可する場所を判断する基準<br>・クラウドサービス提供者の選定基準<br>・クラウドサービスの利用申請の許可権限者と利用の手順<br>・クラウドサービス管理者とクラウドサービスの利用状況管理の内容 | 8.3.(1) | 5.20<br>5.21<br>5.22 | |
| | | (2) クラウドサービスの利用に係る運用規程の整備 | 374 | | **ⅰ)クラウドサービスの利用に係る運用規程の整備**<br>統括情報セキュリティ責任者によって、クラウドサービスの利用(機密性2以上の情報を取り扱う場合)に関する基準が定められ、文書化されている。 | □クラウドサービス運用規程 | 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、クラウドサービスの利用に関する基準が文書化され、正式に承認されていることを確かめる。<br>また、基準には以下の事項が定められていることを確かめる。<br>・クラウドサービスを利用して情報システムを導入・構築する際のセキュリティ対策の基本方針<br>・クラウドサービスを利用して情報システムを運用・保守する際のセキュリティ対策の基本方針<br>・クラウドサービスの利用を終了する際のセキュリティ対策の基本方針(情報の廃棄、アカウントの廃棄を含む) | 8.3.(2) | 5.23 | |
| | | (3) クラウドサービスの選定 | 375 | | **ⅰ)クラウドサービスの利用判断基準**<br>情報セキュリティ責任者によって、クラウドサービス利用判断基準に従って、業務に係る影響度等を検討した上でクラウドサービスの利用可否が判断されている。 | □クラウドサービス運用規程<br>□クラウドサービス利用判断基準<br>□クラウドサービス提供者の選定基準 | 監査資料のレビューと情報セキュリティ責任者へのインタビューにより、クラウドサービス利用の際、規定や判断基準に従って利用の可否が判断されていることを確かめる。 | 8.3.(2)① | － | |
| | | | 376 | | **ⅱ)クラウドサービスの選定条件①**<br>情報セキュリティ責任者によって、クラウドサービス提供者の選定基準に従ってクラウドサービス提供者が選定されている。 | □クラウドサービス運用規程<br>□クラウドサービス利用判断基準<br>□クラウドサービス提供者の選定基準 | 監査資料のレビューと情報セキュリティ責任者へのインタビューにより、クラウドサービス利用の際、規定や判断基準に従ってクラウドサービス、クラウドサービス提供者が選定されていることを確かめる。<br>また、クラウドサービス提供者の選定条件として、以下の項目が含まれていることを確認する。<br>・クラウドサービスの利用を通じて自組織が取り扱う情報のクラウドサービス提供者における目的外利用の禁止<br>・クラウドサービス提供者における情報セキュリティ対策の実施内容及び管理体制<br>・クラウドサービスの提供に当たり、クラウドサービス提供者若しくはその従業員、再委託先又はその他の者によって、自組織の意図しない変更が加えられないための管理体制<br>・クラウドサービス提供者の資本関係・役員等の情報、クラウドサービスの提供が行われる施設等の場所、クラウドサービス提供に従事する者の所属・専門性(情報セキュリティに係る資格・研修実績等)・実績及び国籍に関する情報提供<br>・情報セキュリティインシデントへの対処方法<br>・情報セキュリティ対策その他の契約の履行状況の確認方法<br>・情報セキュリティ対策の履行が不十分な場合の対処方法 | 8.3.(2)② | － | |



別紙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 |
|---|---|---|---|---|---|---|---|---|
| | 377 | | **iii）クラウドサービスの選定条件②**<br>情報セキュリティ責任者によるクラウドサービスの選定条件に、クラウドサービスの中断や終了時に円滑に業務を移行するための対策が含まれている。 | □クラウドサービス運用規程<br>□クラウドサービス利用判断基準<br>□クラウドサービス提供者の選定基準 | 監査資料のレビューと情報セキュリティ責任者へのインタビューにより、クラウドサービス利用の際、規定や判断基準に従ってクラウドサービス、クラウドサービス提供者が選定されていることを確かめる。<br>また、クラウドサービス提供者の選定条件として、以下の項目が含まれていることを確認する。<br>・クラウドサービスの中断や終了時に円滑に業務を移行するための対策（代替サービス、情報のバックアップなど） | 8.3.(2)③ | － | |
| | 378 | | **iv）クラウドサービスの選定条件③**<br>情報セキュリティ責任者によるクラウドサービス提供者の選定条件に、クラウドサービスの利用を通じて取り扱う情報の格付等を勘案し、必要に応じて情報セキュリティ監査の受け入れやサービスレベルの保証がクラウドサービス提供者の選定条件に含まれている。 | □クラウドサービス運用規程<br>□クラウドサービス利用判断基準<br>□クラウドサービス提供者の選定基準 | 監査資料のレビューと情報セキュリティ責任者へのインタビューにより、クラウドサービス利用の際、規定や判断基準に従ってクラウドサービス、クラウドサービス提供者が選定されていることを確かめる。<br>また、クラウドサービス提供者の選定条件として、以下の項目が含まれていることを確認する（含まれていない場合はその理由を確認）。<br>・情報セキュリティ監査の受入れ<br>・サービスレベルの保証 | 8.3.(2)④ | － | |
| | 379 | | **v）クラウドサービスの選定条件④**<br>情報セキュリティ責任者によるクラウドサービスの選定条件に、クラウドサービスの利用を通じて本市が取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクを評価してクラウドサービス提供者を選定し、必要に応じて本市の情報が取り扱われる場所及び契約に定める準拠法・裁判管轄が選定条件に含まれている。 | □クラウドサービス運用規程<br>□クラウドサービス利用判断基準<br>□クラウドサービス提供者の選定基準 | 監査資料のレビューと情報セキュリティ責任者へのインタビューにより、クラウドサービス利用の際、規定や判断基準に従ってクラウドサービス、クラウドサービス提供者が選定されていることを確かめる。<br>また、クラウドサービス提供者の選定条件として、以下の項目が含まれていることを確認する（含まれていない場合はその理由を確認）。<br>・クラウドサービスの利用を通じて自組織が取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクの評価<br>・自組織の情報が取り扱われる場所及び契約に定める準拠法・裁判管轄 | 8.3.(2)⑤ | － | |
| | 380 | | **vi）クラウドサービスの選定条件⑤**<br>情報セキュリティ責任者によるクラウドサービスの選定条件に、クラウドサービス提供者がその役務内容を一部再委託する場合の条件や、再委託承認可否について含まれている。 | □クラウドサービス運用規程<br>□クラウドサービス利用判断基準<br>□クラウドサービス提供者の選定基準 | 監査資料のレビューと情報セキュリティ責任者へのインタビューにより、クラウドサービス利用の際、規定や判断基準に従ってクラウドサービス、クラウドサービス提供者が選定されていることを確かめる。<br>また、クラウドサービス提供者が役務内容を一部再委託する場合の承認に、以下の項目が考慮されていることを確認する。<br>・再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、クラウドサービス提供者の選定条件で求める内容をクラウドサービス提供者に担保させる<br>・再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報の自組織への提供<br>・クラウドサービス利用判断基準及びクラウドサービス提供者の選定基準に従った再委託の承認の可否判断 | 8.3.(2)⑥ | － | |
| | 381 | | **vii）クラウドサービスの選定条件⑥**<br>情報セキュリティ責任者によるクラウドサービスの選定条件に、取り扱う情報の格付及び取扱制限に応じてセキュリティ要件を定め、クラウドサービスを選定することや、クラウドサービスのセキュリティ要件としてセキュリティに係る国際規格等と同等以上の水準を求めることが含まれている。 | □クラウドサービス運用規程<br>□クラウドサービス利用判断基準<br>□クラウドサービス提供者の選定基準 | 監査資料のレビューと情報セキュリティ責任者へのインタビューにより、クラウドサービス利用の際、規定や判断基準に従ってクラウドサービス、クラウドサービス提供者が選定されていることを確かめる。<br>また、クラウドサービス提供者に求めるセキュリティ要件として、セキュリティに係る国際規格等と同等以上の水準が求められていることを確認する。<br>【推奨される規格等】<br>・ISO/IEC27017の認証取得状況<br>・ISMAPの管理基準を満たすことの確認<br>・SOC報告書の活用　など | 8.3.(2)⑦ | － | |

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | 382 | | **viii）クラウドサービスに要求するセキュリティ要件**<br>情報セキュリティ責任者によって、情報の流通経路全般を見渡した形でセキュリティ設計を行った上で、情報セキュリティに関する役割及び責任の範囲を踏まえたセキュリティ要件が定められている。 | □クラウドサービス運用規程<br>□クラウドサービス利用判断基準<br>□クラウドサービス提供者の選定基準 | 監査資料のレビューと情報セキュリティ責任者へのインタビューにより、クラウドサービスで利用する情報の流通経路全般でセキュリティ設計がなされていることを確かめる。また、クラウドサービスの提供者との間で情報セキュリティに関する役割や責任を踏まえて以下のセキュリティの要件が定められていることを確認する。<br>・クラウドサービスに求める情報セキュリティ対策<br>・クラウドサービスで取り扱う情報が保存される国・地域及び廃棄の方法<br>・クラウドサービスに求めるサービスレベル | 8.3.(2)⑧ | － | |
| | | | 383 | | **ix）クラウドサービス提供者の信頼性**<br>統括情報セキュリティ責任者によって、情報セキュリティ監査の報告書や認定・認証制度の適用状況等からクラウドサービス提供者の信頼性が判断されている。 | □クラウドサービス運用規程<br>□クラウドサービス利用判断基準<br>□クラウドサービス提供者の選定基準 | 監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、クラウドサービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、クラウドサービス及び当該クラウドサービス提供者の信頼性が判断されていることを確かめる。 | 8.3.(2)⑨ | － | ・ISO/IEC27017認証、SOC報告書及びISMAPなどを活用することが考えられる。 |
| | | (4)<br>クラウドサービスの利用に係る調達・契約 | 384 | | **ⅰ）クラウドサービスの利用に係る調達仕様書**<br>情報セキュリティ責任者によって、調達仕様書にクラウドサービス提供者の選定基準及び選定条件並びにクラウドサービスの選定時に定めたセキュリティ要件が含まれている。 | □クラウドサービス運用規程<br>□クラウドサービス利用判断基準<br>□クラウドサービス提供者の選定基準<br>□クラウドサービス利用時のセキュリティ要件<br>□クラウドサービスの利用に係る調達仕様書 | 監査資料のレビューと情報セキュリティ責任者へのインタビューにより、調達仕様書にクラウドサービス提供者の選定基準及び選定条件並びにクラウドサービスの選定時に定めたセキュリティ要件が含まれていることを確かめる。 | 8.3.(4)① | － | |
| | | | 385 | | **ⅱ）クラウドサービスの利用に係る契約**<br>情報セキュリティ責任者によって、クラウドサービス提供者及びクラウドサービスが調達仕様書を満たすことが契約締結までに確認されており、利用承認を得ている。また、調達仕様書の内容が契約書にも盛り込まれている。 | □クラウドサービスの利用に係る調達仕様書<br>□クラウドサービスの利用に係る契約書 | 監査資料のレビューと情報セキュリティ責任者へのインタビューにより、クラウドサービスの契約までに、クラウドサービス提供者及びクラウドサービスが調達仕様書を満たすことが契約締結までに確認されており、利用承認を得ている。また、調達仕様書の内容が契約書にも盛り込まれていることを確かめる。 | 8.3.(4)② | － | |
| | | (5)<br>クラウドサービスの利用承認 | 386 | | **ⅰ）クラウドサービスの利用申請**<br>情報セキュリティ責任者によって、クラウドサービスの利用申請の許可権限者に許可申請がされている。 | □クラウドサービス運用規程<br>□クラウドサービス利用申請書 | 監査資料のレビューと情報セキュリティ責任者へのインタビューにより、クラウドサービスの利用申請が利用許可権限者に対して申請されていることを確かめる。 | 8.3.(5)① | － | |
| | | | 387 | | **ⅱ）クラウドサービスの利用可否判断**<br>利用申請の許可権限者は、クラウドサービスの利用申請を審査し、利用の可否を判断している。 | □クラウドサービス運用規程<br>□クラウドサービス利用申請書<br>□クラウドサービス利用審査結果 | 監査資料のレビューと利用申請の許可権限者へのインタビューにより、クラウドサービスの利用申請が審査を経て承認されていることを確かめる。 | 8.3.(5)② | － | |
| | | | 388 | | **ⅲ）クラウドサービス管理者の指名**<br>利用申請の許可権限者は、クラウドサービスの利用申請を承認した場合、クラウドサービス管理者を指名している。 | □クラウドサービス運用規程 | 監査資料のレビューと利用申請の許可権限者へのインタビューにより、クラウドサービスの利用申請を承認した場合にクラウドサービス管理者を指名していることを確かめる。 | 8.3.(5)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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | (6) クラウドサービスを利用した情報システムの導入・構築時の対策 | 389 | | **ⅰ)クラウドサービスを利用した情報システムを構築する際のセキュリティ対策**<br>統括情報セキュリティ責任者によって、クラウドサービスを利用した情報システムを構築する際のセキュリティ対策が規定されている。 | □クラウドサービスセキュリティ対策規程 | 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、クラウドサービスを利用した情報システムを構築する際のセキュリティ対策が規定されていることを確かめる。<br>また、セキュリティ対策として、以下の項目が考慮されていることを確認する。<br>・不正アクセスを防止するためのアクセス制御<br>・取り扱う情報の機密性保護のための暗号化<br>・開発時におけるセキュリティ対策<br>・設計・設定時の誤りの防止 | 8.3.(6)① | － | |
| | | | 390 | | **ⅱ)クラウドサービス利用の記録**<br>クラウドサービス管理者によって、情報システムにおいてクラウドサービスを利用する際には、情報システム台帳及び関連文書に記録又は記載されている。なお、情報システム台帳に記録又は記載した場合は、統括情報セキュリティ責任者へ報告されている。 | □情報システム台帳 | 監査資料のレビューとクラウドサービス管理者へのインタビューにより、クラウドサービスを利用する際には、情報システム台帳及び関連文書に記録又は記載されているか確かめる。なお、情報システム台帳に記録又は記載した場合は、統括情報セキュリティ責任者へ報告されているか確かめる。 | 8.3.(6)② | 5.23 | |
| | | | 391 | | **ⅲ)クラウドサービス実施手順の整備**<br>クラウドサービス管理者によって、クラウドサービスの情報セキュリティ対策を実施するために必要となる文書として、クラウドサービスの運用開始前までに実施手順が整備されている。 | □クラウドサービス運用規程 | 監査資料のレビューとクラウドサービス管理者へのインタビューにより、クラウドサービスの情報セキュリティ対策を実施するために必要となる文書として、クラウドサービスの運用開始前までに以下の実施手順が整備されているか確かめる。<br>・クラウドサービスで利用するサービスごとの情報セキュリティ水準の維持に関する手順<br>・クラウドサービスを利用した情報システムの運用・監視中における情報セキュリティインシデントを認知した際の対処手順<br>・利用するクラウドサービスが停止又は利用できなくなった際の復旧手順 | 8.3.(6)③ | 5.23 | |
| | | | 392 | | **ⅳ)クラウドサービス管理者による確認・記録**<br>クラウドサービス管理者によって、クラウドサービスを利用した情報システム構築時のセキュリティ対策状況が定期的に確認・記録されている。 | □クラウドサービス構築状況確認記録 | 監査資料のレビューとクラウドサービス管理者へのインタビューにより、クラウドサービスを利用した情報システムの構築において、セキュリティ対策の状況が定期的に確認・記録されているか確かめる。 | 8.3.(6)④ | － | |
| | | (7) クラウドサービスを利用した情報システムの運用・保守時の対策 | 393 | | **ⅰ)クラウドサービスを利用した情報システムを運用する際のセキュリティ対策**<br>統括情報セキュリティ責任者によって、クラウドサービスを利用した情報システムを構築する際のセキュリティ対策が規定されている。 | □クラウドサービスセキュリティ対策規程 | 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、クラウドサービスを利用した情報システムを運用する際のセキュリティ対策が規定されていることを確かめる。<br>また、セキュリティ対策として、以下の項目が考慮されていることを確認する。<br>・クラウドサービス利用方針の規定<br>・クラウドサービス利用に必要な教育<br>・取り扱う資産の管理<br>・不正アクセスを防止するためのアクセス制御<br>・取り扱う情報の機密性保護のための暗号化<br>・クラウドサービス内の通信の制御<br>・設計・設定時の誤りの防止<br>・クラウドサービスを利用した情報システムの事業継続 | 8.3.(7)① | － | |

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | 394 | | **ⅱ）クラウドサービス利用の記録**<br>クラウドサービス管理者によって、クラウドサービスの運用・保守時に情報セキュリティ対策を実施するために必要となる項目等で修正又は変更等が発生した場合には、情報システム台帳及び関連文書が更新又は修正されている。なお、情報システム台帳を更新又は修正した場合は、統括情報セキュリティ責任者へ報告されている。 | □情報システム台帳 | 監査資料のレビューとクラウドサービス管理者へのインタビューにより、クラウドサービスの運用・保守時に情報セキュリティ対策を実施するために必要となる項目等で修正又は変更等が発生した場合には、情報システム台帳及び関連文書に記録又は記載されているか確かめる。なお、情報システム台帳に記録又は記載した場合は、統括情報セキュリティ責任者へ報告されているか確かめる。 | 8.3.(7)② | 5.23 | |
| | | | 395 | | **ⅲ）クラウドサービスの情報セキュリティ対策の見直し**<br>クラウドサービス管理者によって、クラウドサービスの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置が講じられている。 | □クラウドサービス運用規程 | 監査資料のレビューとクラウドサービス管理者へのインタビューにより、クラウドサービスの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置が講じられているか確かめる。 | 8.3.(7)③ | 5.23 | |
| | | | 396 | ○ | **ⅳ）クラウドサービスで発生したインシデントの対応手順**<br>情報セキュリティ責任者によって、クラウドサービスで発生したインシデントの対処手順が整備されている。 | □クラウドサービスインシデント対応手順書 | 監査資料のレビューと情報セキュリティ責任者へのインタビューにより、クラウドサービスでインシデントが発生した場合の対応手順が整備されているか確かめる。 | 8.3.(7)④ | － | |
| | | | 397 | | **ⅴ）クラウドサービス管理者による確認・記録**<br>クラウドサービス管理者によって、クラウドサービスを利用した情報システムの運用・保守時のセキュリティ対策やインシデント対応状況が定期的に確認・記録されている。 | □クラウドサービス運用状況確認記録 | 監査資料のレビューとクラウドサービス管理者へのインタビューにより、クラウドサービスを利用した情報システムの運用・保守において、セキュリティ対策やインシデント対応の状況が定期的に確認・記録されているか確かめる。 | 8.3.(7)⑤ | － | |
| | | (8)<br>クラウドサービスを利用した情報システムの更改・廃棄時の対策 | 398 | | **ⅰ）クラウドサービスを利用した情報システムを終了する際のセキュリティ対策**<br>統括情報セキュリティ責任者によって、クラウドサービスを利用した情報システムを終了する際のセキュリティ対策が規定されている。 | □クラウドサービスセキュリティ対策規程 | 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、クラウドサービスを利用した情報システムを終了する際のセキュリティ対策が規定されていることを確かめる。<br>また、セキュリティ対策として、以下の項目が考慮されていることを確認する。<br>・クラウドサービスの利用終了時における対策<br>・クラウドサービスで取り扱った情報の廃棄<br>・クラウドサービスの利用のために作成したアカウントの廃棄 | 8.3.(8)① | － | |
| | | | 399 | | **ⅱ）クラウドサービス管理者による確認・記録**<br>クラウドサービス管理者によって、クラウドサービスを利用した情報システム終了時のセキュリティ対策状況が定期的に確認・記録されている。 | □クラウドサービス構築状況確認記録 | 監査資料のレビューとクラウドサービス管理者へのインタビューにより、クラウドサービスを利用した情報システムの終了において、セキュリティ対策の状況が確認・記録されているか確かめる。 | 8.3.(8)② | － | |



別紙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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | 8.4. 外部サービス(クラウドサービス)の利用(機密性2以上の情報を取り扱わない場合) | (1) クラウドサービスの利用に係る規定の整備 | 400 | ○ | **ⅰ)クラウドサービスの利用に係る規定の整備**<br>統括情報セキュリティ責任者によって、クラウドサービスの利用(機密性2以上の情報を取り扱わない場合)に関する基準が定められ、文書化されている。 | □クラウドサービス運用規程<br>□クラウドサービス利用判断基準<br>□クラウドサービス提供者の選定基準 | 監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、クラウドサービスの利用可否に関する基準が文書化され、正式に承認されていることを確かめる。<br>また、基準には以下の事項が定められていることを確かめる。<br>・クラウドサービスを利用可能な業務の範囲<br>・クラウドサービスの利用申請の許可権限者と利用手続<br>・クラウドサービス管理者の指名とクラウドサービスの利用状況の管理<br>・クラウドサービスの利用の運用手順 | 8.4.(1) | 5.20<br>5.21<br>5.22 | |
| | | (2) クラウドサービスの利用における対策の実施 | 401 | | **ⅰ)クラウドサービスの利用申請**<br>職員等は、利用のリスクが許容できることを確認して申請している。また、指名されたクラウドサービス管理者は、利用に当たり適切な措置を講じている。 | □クラウドサービス運用規程<br>□クラウドサービス利用申請書<br>□クラウドサービス利用審査結果 | 監査資料のレビューとクラウドサービスの利用申請した職員等と指名されたクラウドサービス管理者へのインタビューにより、リスクの確認内容や利用に必要な措置を講じていることを確かめる。 | 8.4.(2)① | ― | |
| | | | 402 | | **ⅱ)クラウドサービスの利用審査・承認**<br>情報セキュリティ責任者によって、申請されたクラウドサービスの利用可否が決定されており、承認されたクラウドサービスが記録されている。 | □クラウドサービス運用規程<br>□クラウドサービス利用申請書<br>□クラウドサービス利用審査結果 | 監査資料のレビューと情報セキュリティ責任者へのインタビューにより、クラウドサービスの利用可否が決定されており、利用が承認されたクラウドサービスが記録されているか確かめる。 | 8.4.(2)② | ― | |
| 9. 評価・見直し | 9.1. 監査 | | 403 | | **ⅰ)情報セキュリティ監査に関わる基準及び手順**<br>統括情報セキュリティ責任者によって、情報セキュリティ監査の実施に関わる基準及び手順が定められ、文書化されている。 | □情報セキュリティ監査実施要綱<br>□情報セキュリティ監査実施マニュアル | 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、情報セキュリティ監査の実施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。 | 9.1. | 5.20<br>5.22<br>5.35<br>8.34 | |
| | | (1) 実施方法 | 404 | | **ⅰ)監査の実施**<br>CISOによって、情報セキュリティ監査統括責任者が指名され、毎年度及び必要に応じて情報セキュリティ監査が行われている。 | □情報セキュリティ監査実施要綱<br>□情報セキュリティ監査実施マニュアル<br>□監査実施計画<br>□監査報告書 | 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、CISOによって情報セキュリティ監査統括責任者が指名され、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、毎年度及び必要に応じて監査が行われているか確かめる。 | 9.1.(1) | 5.35<br>8.34 | |
| | | (2) 監査を行う者の要件 | 405 | | **ⅰ)監査人の独立性**<br>情報セキュリティ監査統括責任者によって、被監査部門から独立した者に対して監査の実施が依頼されている。 | □情報セキュリティ監査実施要綱<br>□情報セキュリティ監査実施マニュアル<br>□監査実施計画<br>□監査報告書 | 監査資料のレビューと情報セキュリティ監査統括責任者へのインタビューにより、被監査部門から独立した者に監査が依頼され、公平な立場で客観的に監査が実施されているか確かめる。 | 9.1.(2)① | 5.35<br>8.34 | |
| | | | 406 | | **ⅱ)監査人の専門性**<br>情報セキュリティ監査は、監査及び情報セキュリティに関する専門知識を有する者によって実施されている。 | □情報セキュリティ監査実施要綱<br>□情報セキュリティ監査実施マニュアル<br>□監査実施計画<br>□監査報告書 | 監査資料のレビューと情報セキュリティ監査統括責任者へのインタビューにより、監査及び情報セキュリティに関する専門知識を有する者が情報セキュリティ監査を実施しているか確かめる。 | 9.1.(2)② | 5.35<br>5.36 | |

| 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)<br>監査実施計画の立案及び実施への協力 | 407 | | **ⅰ)監査実施計画の立案**<br>情報セキュリティ監査統括責任者によって、監査実施計画が立案され、情報セキュリティ委員会の承認を得ている。 | □情報セキュリティ監査実施マニュアル<br>□監査実施計画<br>□情報セキュリティ委員会議事録 | 監査資料のレビューと情報セキュリティ監査統括責任者へのインタビューにより、監査実施計画が立案され、情報セキュリティ委員会の承認を得ているか確かめる。 | 9.1.(3)① | 5.35<br>8.34 | |
| | 408 | | **ⅱ)監査実施への協力**<br>監査実施に際し、被監査部門による協力が得られている。 | □情報セキュリティ監査実施マニュアル<br>□監査報告書 | 監査資料のレビューと情報セキュリティ監査統括責任者へのインタビューにより、被監査部門が監査の実施に協力しているか確かめる。 | 9.1.(3)② | 5.35 | |
| (4)<br>委託事業者に対する監査 | 409 | | **ⅰ)委託事業者に対する監査**<br>情報セキュリティ監査統括責任者によって、委託事業者(再委託事業者を含む)に対する情報セキュリティポリシーの遵守についての監査が定期的又は必要に応じて行われている。 | □情報セキュリティ監査実施要綱<br>□情報セキュリティ監査実施マニュアル<br>□監査実施計画<br>□監査報告書 | 監査資料のレビューと情報セキュリティ監査統括責任者へのインタビューにより、委託事業者(再委託事業者を含む)に対する情報セキュリティポリシーの遵守についての監査が定期的又は必要に応じて行われているか確かめる。 | 9.1.(4) | 5.20<br>5.35<br>5.36 | ・セキュリティポリシー遵守について委託事業者に対する説明は、No.109～110も関連する項目であることから参考にすること。 |
| (5)<br>報告 | 410 | | **ⅰ)監査結果の報告**<br>情報セキュリティ監査統括責任者によって、監査結果が取りまとめられ、情報セキュリティ委員会に報告されている。 | □情報セキュリティ監査実施マニュアル<br>□監査報告書<br>□情報セキュリティ委員会議事録 | 監査資料のレビューと情報セキュリティ監査統括責任者へのインタビューにより、監査結果が取りまとめられ、情報セキュリティ委員会に報告されているか確かめる。 | 9.1.(5) | 5.35 | ・監査報告書は、監査証拠に裏付けられた合理的な根拠に基づくものであることを要する。従って監査報告書中に、監査意見に至った根拠とそれを導く証拠が記載され、これを第三者が評価できるように整然と、かつ明瞭に記載することが望ましい。 |
| (6)<br>保管 | 411 | | **ⅰ)監査証拠及び監査調書の保管**<br>情報セキュリティ監査統括責任者によって、監査証拠及び監査調書が適切に保管されている。 | □情報セキュリティ監査実施マニュアル<br>□監査調書 | 監査資料のレビューと情報セキュリティ監査統括責任者へのインタビュー、保管場所の視察により、監査実施によって収集された監査証拠及び監査報告書作成のための監査調書が紛失しないように保管されているか確かめる。 | 9.1.(6) | 5.33<br>5.35 | |
| (7)<br>監査結果への対応 | 412 | | **ⅰ)監査結果への対応**<br>CISOによって、監査結果を踏まえた指摘事項への対処(改善計画の策定等)が関係部局に指示されている。また、指摘事項を所轄していない部局においても同種の課題がある可能性が高い場合には、当該課題及び問題点の有無を確認させている。また、庁内で横断的に改善が必要な事項については、統括情報セキュリティ責任者に対し、当該事項への対処(改善計画の策定等)を指示されている。<br>なお、措置が完了していない改善計画は、定期的に進捗状況の報告が指示されている。 | □情報セキュリティ委員会議事録<br>□改善指示書<br>□改善計画 | 監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、CISOによって、監査結果を踏まえた指摘事項への対処(改善計画の策定等)が関係部局に指示され、また、指摘事項を所轄していない部局においても同種の課題がある可能性が高い場合には、当該課題及び問題点の有無を確認させているか確かめる。また、庁内で横断的に改善が必要な事項については、統括情報セキュリティ責任者に対し、当該事項への対処を指示されているか確かめる。<br>なお、措置が完了していない改善計画は、定期的に進捗状況の報告が指示されているか確かめる。 | 9.1.(7) | 5.35 | |

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | (8)<br>情報セキュリティポリシー及び関係規程等の見直し等への活用 | 413 | | **ⅰ)情報セキュリティポリシー及び関係規程等の見直し等への活用**<br>情報セキュリティ委員会によって、監査結果が情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直しに活用されている。 | □情報セキュリティ委員会議事録<br>□情報セキュリティポリシー | 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、監査結果が情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直しに活用されているか確かめる。 | 9.1.(8) | 5.1 | ・情報セキュリティポリシーの見直しについては、No.420～421も関連する項目であることから参考にすること。 |
| | 9.2.<br>自己点検 | | 414 | | **ⅰ)情報セキュリティ対策の自己点検に関わる基準及び手順**<br>統括情報セキュリティ責任者によって、情報セキュリティ対策の実施状況の自己点検に関わる基準及び手順が定められ、文書化されている。 | □情報セキュリティ自己点検基準<br>□情報セキュリティ自己点検実施手順書 | 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、情報セキュリティ対策の実施状況の自己点検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。 | 9.2. | 5.36 | |
| | | (1)<br>実施方法 | 415 | ○ | **ⅰ)ネットワーク及び情報システムに関わる自己点検の実施**<br>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、所管するネットワーク及び情報システムについて、毎年度及び必要に応じて自己点検が行われている。 | □自己点検実施計画<br>□自己点検結果報告書 | 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、所管するネットワーク及び情報システムについて、毎年度及び必要に応じて自己点検が行われているか確かめる。 | 9.2.(1)① | 5.36 | |
| | | | 416 | ○ | **ⅱ)各部局の自己点検の実施**<br>情報セキュリティ責任者及び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に沿った情報セキュリティ対策状況について、毎年度及び必要に応じて自己点検が行われている。 | □自己点検実施計画<br>□自己点検結果報告書 | 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セキュリティ管理者へのインタビューにより、情報セキュリティポリシーに沿った情報セキュリティ対策状況について、毎年度及び必要に応じて自己点検が行われているか確かめる。 | 9.2.(1)② | 5.36 | |
| | | (2)<br>報告 | 417 | ○ | **ⅰ)自己点検結果の報告**<br>統括情報セキュリティ責任者、情報システム管理者及び情報セキュリティ責任者によって、自己点検結果と自己点検結果に基づく改善策が取りまとめられ、情報セキュリティ委員会に報告されている。 | □自己点検結果報告書<br>□改善計画<br>□情報セキュリティ委員会議事録 | 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及び情報セキュリティ責任者へのインタビューにより、自己点検結果と自己点検結果に基づく改善策が取りまとめられ、情報セキュリティ委員会に報告されているか確かめる。 | 9.2.(2) | 5.36 | |
| | | (3)<br>自己点検結果の活用 | 418 | | **ⅰ)権限の範囲内での改善**<br>職員等によって、自己点検の結果に基づき、自己の権限の範囲内で改善が図られている。 | □自己点検結果報告書<br>□改善計画 | 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、自己点検の結果に基づき、自己の権限の範囲内で改善が図られているか確かめる。 | 9.2.(3)① | 5.36 | |
| | | | 419 | | **ⅱ)情報セキュリティポリシーの見直しへの活用**<br>情報セキュリティ委員会によって、自己点検結果が情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用されている。 | □情報セキュリティ委員会議事録<br>□情報セキュリティポリシー | 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、自己点検結果が情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用されているか確かめる。 | 9.2.(3)② | 5.1<br>5.36 | |

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | 9.3.<br>情報セキュリティポリシー及び関係規程等の見直し | | 420 | | **ⅰ）情報セキュリティポリシー及び関係規程等の見直しに関わる基準**<br>情報セキュリティポリシー及び関係規程等の見直しに関わる基準が定められ、文書化されている。 | □情報セキュリティポリシー | 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、情報セキュリティポリシー及び関係規程等の見直しに関わる基準が文書化され、正式に承認されているか確かめる。 | 9.3. | 5.1 | |
| | | | 421 | ○ | **ⅱ）情報セキュリティポリシー及び関係規程等の見直し**<br>情報セキュリティ委員会によって、情報セキュリティ監査及び自己点検の結果や情報セキュリティに関する状況の変化等を踏まえ、情報セキュリティポリシー及び関係規程等の見直しが行われている。<br>なお、横断的に改善が必要となる情報セキュリティ対策の運用見直しについて、内部の職制及び職務に応じた措置の実施又は指示し、措置の結果についてCISOに報告されている。 | □情報セキュリティポリシー<br>□情報セキュリティ委員会議事録<br>□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へのインタビューにより、情報セキュリティ委員会において、情報セキュリティ監査及び自己点検の結果や情報セキュリティに関する状況の変化等を踏まえ、毎年度及び重大な変化が発生した場合にリスク評価を行い、必要に応じて情報セキュリティポリシー及び関係規程等の改善が行われているか確かめる。また、改善された場合に、その内容が職員等や委託事業者に周知されているか確かめる。<br>なお、横断的に改善が必要となる情報セキュリティ対策の運用見直しについて、内部の職制及び職務に応じた措置の実施又は指示し、措置の結果についてCISOに報告されているか確かめる。 | 9.3. | 5.1 | |



別紙3

# 別紙3

市区町村において独自に自治体情報セキュリティクラウドの調達を行った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.<br>情報システム全体の強靭性の向上 | | (3)インターネット接続系（セキュリティクラウドの監査項目例） | 1 | ○ | **ｉ）標準要件に基づいた機能と運用**<br>統括情報セキュリティ責任者、情報システム管理者及び情報セキュリティ責任者によって、クラウドの機能や運用が標準要件に基づいて実装・利用・運用されている。 | □システム構成図<br>□システム設計書<br>□機器等の設定指示書<br>□運用手順書<br>□サービス利用契約書 | 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、自組織又は外部サービス提供者により、「次期自治体情報セキュリティクラウドの標準要件について」（令和2年8月18日総行情第109号　総務省自治行政局地域情報政策室長通知）における標準要件（機能要件一覧、要件シート等）に基づいたセキュリティクラウドの機能を有していること及び運用がされていることを確かめる。 | 3.(3) | ー | ・「3.情報システム全体の強靭性の向上 (3)インターネット接続系」における監査項目に加えて、左記の監査項目も合わせて確認する。<br>・外部サービス（クラウドサービス）については、No.357～402も関連する項目であることから参考にすること。 |



別紙３

# 別紙3

α’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）接続先のクラウドサービスの証明書による認証**<br>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、以下の対策が実施されている。<br>・接続先のクラウドサービスが本物であるか否か、正当性を確認する。 | □システム構成図<br>□システム設計書<br>□機器等の設定指示書<br>□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、LGWAN接続系からパブリッククラウドサービスに接続するさい、接続先が本物であるか否か、正当性を確認する対策が実施されているか確かめる。 | ― | ― | |
| | | | 2 | ○ | **ⅱ）マルウェア対策ソフト**<br>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方式や、不審な動作を行うコードが含まれていることを検出する振る舞い検知などにより、不正プログラム対策が実施されている。 | □システム構成図<br>□システム設計書<br>□機器等の設定指示書<br>□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方式や、不審な動作を行うコードが含まれていることを検出する振る舞い検知などにより、不正プログラム対策が実施されているか確かめる。 | ― | ― | |
| | | | 3 | ○ | **ⅲ）パッチ適用**<br>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、脆弱性を修正するパッチを速やかに適用し、脆弱性を解消する対策が実施されている。 | □システム構成図<br>□システム設計書<br>□機器等の設定指示書<br>□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、脆弱性を修正するパッチを速やかに適用し、脆弱性を解消する対策が実施されているか確かめる。 | ― | ― | |
| | | | 4 | ○ | **ⅳ）接続先制限**<br>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、LGWAN接続系から外部へのアクセス先をLGWAN-ASP及び利用が許可されたクラウドサービスのみに限定する対策が実施されている。 | □システム構成図<br>□システム設計書<br>□機器等の設定指示書<br>□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、LGWAN接続系から外部へのアクセス先をLGWAN-ASP及び利用が許可されたクラウドサービスのみに限定する対策が実施されているか確かめる。 | ― | ― | |
| | | | 5 | ○ | **ⅴ）ローカルブレイクアウトテナントアクセス制御**<br>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、団体専用テナントを利用時は、利用するクラウドサービスへのアクセスを自らの団体が利用するテナントのみに制限する対策が実施されている。 | □システム構成図<br>□アクセス制御方針<br>□アクセス管理基準<br>□システム設計書<br>□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、団体専用テナントを利用時は、利用するクラウドサービスへのアクセスを自らの団体が利用するテナントのみに制限していることを確かめる。 | ― | ― | |

| 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）メール無害化/ファイル無害化**<br>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。<br>・ファイルからテキストのみを抽出<br>・ファイルを画像PDFに変換<br>・サニタイズ処理<br>・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<br>□システム設計書<br>□機器等の設定指示書<br>□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、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を確かめる。 | ― | ― | |
| | | | 7 | ○ | **vii）権限管理**<br>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、不正行為（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、管理者、ユーザの権限関連する属性に応じて適切に管理する対策が実施されている。 | □システム構成図<br>□システム設計書<br>□機器等の設定指示書<br>□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、不正行為（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、管理者、ユーザの権限関連する属性に応じて適切に管理していることを確かめる。 | ― | ― | |
| | | | 8 | ○ | **viii）アクセス制御**<br>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、不正アクセス（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、権限に応じた認可に基づき、アクセスの許可または拒否を行う対策が実施されている。 | □アクセス制御方針<br>□アクセス管理基準<br>□システム設計書<br>□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、不正アクセス（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、権限に応じた認可に基づき、アクセスの許可または拒否が実施されていることを確かめる。 | ― | ― | ・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。 |
| | | | 9 | ○ | **ix）IDS/IPS**<br>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、ネットワーク上の通信パケットを収集・解析し、不正な通信の検知及び遮断する対策が実施されている。 | □システム構成図<br>□システム設計書<br>□機器等の設定指示書<br>□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、ネットワーク上の通信パケットを収集・解析し、不正な通信の検知及び遮断する対策が実施されていることを確かめる。 | ― | ― | |

| 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 | | **ｘ）DDoS対策**<br>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、サービス不能攻撃の一つであるDDoS（Distributed Denial of Service）攻撃による被害を最小化するために、以下の対策が実施されている。<br>・DDoS対策機器の導入<br>・DDoS対策サービスの利用によって、高負荷攻撃への耐性を向上<br>・負荷分散装置（ロードバランサ）による耐性向上 | □システム構成図<br>□システム設計書<br>□機器等の設定指示書<br>□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、DDoS対策として、DDoS対策機器の導入、DDoS対策サービスの利用による高負荷攻撃への耐性の向上、負荷分散装置（ロードバランサ）による耐性の向上などの対策が実施されているかを確かめる。 | － | － | |
| | | | 11 | ○ | **ⅺ）通信路暗号化**<br>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、通信路上の盗聴・改ざんによる被害を最小化するために、以下の対策が実施されている。<br>・暗号技術を用いて通信路上のデータを暗号化する<br>・通信路上のデータ漏えいが発生しても、暗号化により攻撃者にとって無意味なものとする | □システム構成図<br>□システム設計書<br>□機器等の設定指示書<br>□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、通信路上の盗聴・改ざんによる被害を最小化するため、暗号技術を用いて通信路上のデータを暗号化する、通信路上のデータ漏えいが発生しても、暗号化により攻撃者にとって無意味なものとする対策が実施されているかを確かめる。 | － | － | |
| | | | 12 | | **ⅻ）クラウドサービスからファイルダウンロード制限**<br>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、必要性に応じクラウドサービス上から業務端末へのファイルダウンロードを制限する**する対策が実施されている。** | □システム構成図<br>□システム設計書<br>□機器等の設定指示書<br>□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、必要性に応じ、クラウドサービス上から業務端末へのファイルダウンロードを制限するする対策が実施されているかを確かめる。 | － | － | |
| | | 組織的・人的対策 | 13 | ○ | **ⅰ）手続・規定**<br>クラウドサービスを利用開始する場合の申請、承認等に係る規定を整備するとともに、運用を徹底している。 | □クラウドサービス事業者選定基準<br>□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へのインタビューにより、クラウドサービス事業者選定の際、利用するクラウドサービスのアプリケーションや、格納する情報資産など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。 | － | － | |

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | 14 | ○ | **ⅱ）情報セキュリティ研修計画**<br>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<br>□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) | 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。 |
| | | | 15 | ○ | **ⅲ）実践的サイバー防御演習（CYDER）の確実な受講**<br>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<br>□研修・訓練受講記録<br>□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。<br>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。 | ― | ― | |
| | | | 16 | ○ | **ⅳ）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**<br>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。<br>・インシデント対応訓練（基礎/高度）<br>・分野横断的演習 | □研修・訓練実施計画<br>□研修・訓練受講記録<br>□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。 | 5.2.(2) | ― | |
| | | | 17 | ○ | **ⅴ）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**<br>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.<br>組織体制 | | (3)CSIRTの設置・役割 | 4 | ○ | **ⅲ）CSIRTの設置・役割の明確化**<br>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<br>□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<br>5.6<br>5.24<br>5.25<br>5.26<br>6.8 | |
| 5.<br>人的セキュリティ | 5.1.<br>職員等の遵守事項 | (1)<br>職員等の遵守事項①<br>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**<br>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<br>□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**<br>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<br>□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)<br>職員等の遵守事項②<br>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**<br>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<br>□電子メール送受信ログ<br>□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 | － | |



別紙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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | (1)<br>職員等の遵守事項③<br>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**<br>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<br>□庁外での情報処理作業基準/手続<br>□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<br>(イ) | 8.1<br>6.7<br>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**<br>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<br>□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<br>(ウ) | 8.1<br>6.7<br>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)<br>職員等の遵守事項④<br>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**<br>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<br>□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<br>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**<br>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<br>□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<br>6.7<br>7.8<br>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**<br>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<br>□支給以外のパソコン等使用申請書/承認書<br>□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<br>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)<br>職員等の遵守事項⑤<br>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**<br>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<br>□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)<br>職員等の遵守事項⑦<br>机上の端末等の管理 | 100 | ○ | **ⅱ)机上の端末等の取扱**<br>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)<br>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**<br>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)<br>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**<br>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<br>□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<br>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。<br>・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。<br>・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.<br>研修・訓練 | (1)<br>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**<br>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<br>□研修実施報告書<br>□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.<br>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**<br>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)<br>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**<br>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<br>□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.<br>ID及びパスワード等の管理 | (1)<br>ICカード等の取扱い | 130 | ○ | **ⅲ）認証用ICカード等の放置禁止**<br>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<br>(イ) | 5.16<br>5.18 | |
| | | | 131 | ○ | **ⅳ）認証用ICカード等の紛失時手続**<br>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<br>□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<br>(ウ) | 5.16<br>5.18 | |
| | | | 132 | ○ | **ⅴ）認証用ICカード等の紛失時対応**<br>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<br>□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<br>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**<br>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<br>□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<br>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)<br>パスワードの取扱い | 138 | ○ | **ⅱ）パスワードの取扱い**<br>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**<br>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**<br>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 | |

# 別紙3

インターネット接続系に主たる業務端末を配置するβ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.<br>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**<br>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。<br>・ファイルからテキストのみを抽出<br>・ファイルを画像PDFに変換<br>・サニタイズ処理<br>・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<br>□システム設計書<br>□機器等の設定指示書<br>□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を確かめる。 | 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**<br>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。<br>・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。<br>・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アドレス等で通信経路を限定することで可能とされている。 | □システム構成図<br>□システム設計書<br>□機器等の設定指示書<br>□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）**<br>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。<br>・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、外部からの侵入や、未知及び既知のマルウェア等による悪意ある活動（データの持ち出しや外部との通信等）を示す異常な挙動を監視・検出・特定する。<br>・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。<br>・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<br>□システム設計書<br>□機器等の設定指示書<br>□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**<br>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、LGWAN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<br>□ログ<br>□システム稼動記録<br>□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、LGWAN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）脆弱性管理**<br>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<br>□脆弱性関連情報の通知記録<br>□サイバー攻撃情報やインシデント情報の通知記録<br>□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。 |

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | 組織的・人的対策 | 6 | ○ | **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**<br>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<br>□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) | － | |
| | | | 8 | ○ | **ⅲ）実践的サイバー防御演習（CYDER）の確実な受講**<br>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<br>□研修・訓練受講記録<br>□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。<br>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) | － | |
| | | | 9 | ○ | **ⅳ）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**<br>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。<br>・インシデント対応訓練（基礎/高度）<br>・分野横断的演習 | □研修・訓練実施計画<br>□研修・訓練受講記録<br>□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) | － | |
| | | | 10 | ○ | **ⅴ）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**<br>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。 |



別紙３

※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.<br>組織体制 | | (3)CSIRTの設置・役割 | 4 | ○ | **ⅲ）CSIRTの設置・役割の明確化**<br>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<br>□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<br>5.6<br>5.24<br>5.25<br>5.26<br>6.8 | |
| 5.<br>人的セキュリティ | 5.1.<br>職員等の遵守事項 | (1)<br>職員等の遵守事項①<br>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**<br>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<br>□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**<br>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<br>□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)<br>職員等の遵守事項②<br>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**<br>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<br>□電子メール送受信ログ<br>□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 | － | |



別紙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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | (1)<br>職員等の遵守事項③<br>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**<br>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<br>□庁外での情報処理作業基準/手続<br>□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<br>6.7<br>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**<br>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<br>□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<br>6.7<br>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)<br>職員等の遵守事項④<br>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**<br>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<br>□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<br>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**<br>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<br>□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<br>6.7<br>7.8<br>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**<br>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<br>□支給以外のパソコン等使用申請書/承認書<br>□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<br>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)<br>職員等の遵守事項⑤<br>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**<br>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<br>□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)<br>職員等の遵守事項⑦<br>机上の端末等の管理 | 100 | ○ | **ⅱ)机上の端末等の取扱**<br>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)<br>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**<br>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)<br>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**<br>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<br>□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<br>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。<br>・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。<br>・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.<br>研修・訓練 | (1)<br>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**<br>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<br>□研修実施報告書<br>□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.<br>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**<br>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)<br>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**<br>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<br>□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.<br>ID及びパスワード等の管理 | (1)<br>ICカード等の取扱い | 130 | ○ | **ⅲ）認証用ICカード等の放置禁止**<br>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<br>(イ) | 5.16<br>5.18 | |
| | | | 131 | ○ | **ⅳ）認証用ICカード等の紛失時手続**<br>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<br>□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<br>(ウ) | 5.16<br>5.18 | |
| | | | 132 | ○ | **ⅴ）認証用ICカード等の紛失時対応**<br>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<br>□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<br>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**<br>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<br>□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<br>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)<br>パスワードの取扱い | 138 | ○ | **ⅱ）パスワードの取扱い**<br>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**<br>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**<br>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 | |

# 別紙3

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β′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。

別紙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.<br>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**<br>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。<br>・ファイルからテキストのみを抽出<br>・ファイルを画像PDFに変換<br>・サニタイズ処理<br>・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<br>□システム設計書<br>□機器等の設定指示書<br>□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**<br>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。<br>・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。<br>・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アドレス等で通信経路を限定することで可能とされている。 | □システム構成図<br>□システム設計書<br>□機器等の設定指示書<br>□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) | － | |

別紙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）**<br>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。<br>・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、外部からの侵入や、未知及び既知のマルウェア等による悪意ある活動（データの持ち出しや外部との通信等）を示す異常な挙動を監視・検出・特定する。<br>・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。<br>・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<br>□システム設計書<br>□機器等の設定指示書<br>□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**<br>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<br>□ログ<br>□システム稼動記録<br>□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**<br>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。<br>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<br>□アクセス管理基準<br>□システム設計書<br>□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**<br>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<br>□脆弱性関連情報の通知記録<br>□サイバー攻撃情報やインシデント情報の通知記録<br>□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**<br>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<br>□研修・訓練実施計画<br>□研修・訓練受講記録<br>□研修・訓練結果報告書<br>□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**<br>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<br>□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**<br>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<br>□研修・訓練実施計画<br>□研修・訓練受講記録<br>□研修・訓練結果報告書<br>□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**<br>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<br>□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**<br>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<br>□研修・訓練受講記録<br>□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。<br>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**<br>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。<br>・インシデント対応訓練（基礎/高度）<br>・分野横断的演習 | □研修・訓練実施計画<br>□研修・訓練受講記録<br>□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**<br>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.<br>組織体制 | | (3)CSIRTの設置・役割 | 4 | ○ | **ⅲ）CSIRTの設置・役割の明確化**<br>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<br>□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<br>5.6<br>5.24<br>5.25<br>5.26<br>6.8 | |
| 5.<br>人的セキュリティ | 5.1.<br>職員等の遵守事項 | (1)<br>職員等の遵守事項①<br>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**<br>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<br>□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**<br>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<br>□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)<br>職員等の遵守事項②<br>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**<br>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<br>□電子メール送受信ログ<br>□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 | － | |



別紙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 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | (1)<br>職員等の遵守事項③<br>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**<br>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<br>□庁外での情報処理作業基準/手続<br>□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<br>6.7<br>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**<br>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<br>□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<br>6.7<br>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)<br>職員等の遵守事項④<br>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**<br>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<br>□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<br>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**<br>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<br>□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<br>6.7<br>7.8<br>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**<br>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<br>□支給以外のパソコン等使用申請書/承認書<br>□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<br>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)<br>職員等の遵守事項⑤<br>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**<br>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<br>□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)<br>職員等の遵守事項⑦<br>机上の端末等の管理 | 100 | ○ | **ⅱ）机上の端末等の取扱**<br>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)<br>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**<br>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)<br>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**<br>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<br>□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<br>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。<br>・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。<br>・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.<br>研修・訓練 | (1)<br>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**<br>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<br>□研修実施報告書<br>□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.<br>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**<br>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)<br>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**<br>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<br>□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.<br>ID及びパスワード等の管理 | (1)<br>ICカード等の取扱い | 130 | ○ | **ⅲ）認証用ICカード等の放置禁止**<br>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<br>(イ) | 5.16<br>5.18 | |
| | | | 131 | ○ | **ⅳ）認証用ICカード等の紛失時手続**<br>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<br>□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<br>(ウ) | 5.16<br>5.18 | |
| | | | 132 | ○ | **ⅴ）認証用ICカード等の紛失時対応**<br>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<br>□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<br>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**<br>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<br>□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<br>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)<br>パスワードの取扱い | 138 | ○ | **ⅱ）パスワードの取扱い**<br>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**<br>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**<br>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 | |

# 別紙3

マイナンバー利用事務系で無線 LAN を利用する場合の監査項目を、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 |
|---|---|---|---|---|---|---|---|---|---|---|
| 6.技術的セキュリティ | 6.1.コンピュータ及びネットワークの管理 | (13)無線LANのセキュリティ対策及びネットワーク盗聴対策 | 1 | ○ | **ⅰ）無線セキュリティ規格**<br>統括情報セキュリティ責任者によって、無線LAN通信の強度の高い暗号化により盗聴対策(WPA2又はWPA3)が行われている。 | □ネットワーク管理基準<br>□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され、盗聴に対し防御されているか確かめる。 | 6.1.(13) | 5.15<br>8.22 | |
| | | | 2 | ○ | **ⅱ）認証方式**<br>統括情報セキュリティ責任者によって、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、認めた端末のみ接続を許可するための認証技術が使用されている。 | □ネットワーク管理基準<br>□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EAP-TLS等の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) | 5.15<br>8.22 | |
| | | | 3 | ○ | **ⅲ）アクセスログの取得・確認**<br>統括情報セキュリティ責任者によって、無線LANへのアクセスログの取得とアクセスログの確認を行う。 | □ネットワーク管理基準<br>□ネットワーク設計書<br>□ログ<br>□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、無線LANへのアクセスログの取得及びログの確認に関わる基準が文書化され、正式に承認されているか確かめる。 | 6.1.(13) | 8.15 | |
| | | | 4 | ○ | **ⅳ）ファームウェア、OS等の最新化**<br>統括情報セキュリティ責任者によって、無線LANを構成する機器のファームウェア、OS等の最新化する。 | □パッチ適用情報<br>□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ファームウェア、OSが更新されているか確かめる。 | 6.1.(13) | 8.8 | |
| | | | 5 | | **ⅴ）電波調整・設定**<br>統括情報セキュリティ責任者によって、電波の伝搬範囲の適切な設定をする。また、電波状況を監視する。 | □ネットワーク管理基準<br>□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、、電波の伝搬範囲の適切な設定をする、また、電波状況を監視しているか確かめる。 | 6.1.(13) | | |
| | | | 6 | ○ | **ⅵ）アクセスポイントの管理**<br>統括情報セキュリティ責任者によって、アクセスポイントの管理者パスワードを適切に設定する。 | □ネットワーク管理基準<br>□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、アクセスポイントの管理者パスワードを適切に管理されているか確かめる。 | 6.1.(13) | 5.17 | |
| | | | 7 | ○ | **ⅶ）無線端末同士の通信の防止**<br>統括情報セキュリティ責任者によって、無線端末間同士の通信が行われないよう適切な設定を行う。 | □ネットワーク管理基準<br>□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、無線端末間同士の通信が行われないよう適切な設定を行っているか確かめる。 | 6.1.(13) | | |
| | | | 8 | | **ⅷ）端末の設定**<br>統括情報セキュリティ責任者によって、端末に許可されたアクセスポイントのSSIDのみを表示する設定を行う。 | □ネットワーク管理基準<br>□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、許可されたアクセスポイントのSSIDのみを表示する設定を行っているか確かめる。 | 6.1.(13) | | |
| | | | 9 | ○ | **ⅸ）正規利用者の管理・不正アクセスの防止**<br>統括情報セキュリティ責任者によって、事務取扱担当者のリスト化、無線LAN利用を許可する者のリスト化を行う。 | □事務取扱担当者一覧 | 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、事務取扱担当者のリスト化、無線LAN利用を許可する者のリスト化を行っているか確かめる。 | 6.1.(13) | | |

| 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 | ○ | **x）事務取扱端末の保護**<br>統括情報セキュリティ責任者によって、事務取扱担当者の端末は執務エリア（特定個人情報を取り扱う事務を行う区域であり、支所を含む）から原則持ち出しをしない運用ルールの徹底を行う。 | □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、事務取扱担当者の端末は執務エリア（特定個人情報を取り扱う事務を行う区域であり、支所を含む）から原則持ち出しをしない運用ルール化を行っているか確かめる。 | 6.1.(13) | | |
| | | | 11 | ○ | **xi）事務取扱担当者と他部門の分離**<br>統括情報セキュリティ責任者によって、事務取扱担当者の庁内の執務エリア（部署単位）をまとめ、執務室を分ける、パーティションの設置等、特定個人情報が他部門に見えないよう分離する。 | □フロアレイアウト | 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、事務取扱担当者の庁内の執務エリア（部署単位）をまとめ、執務室を分ける、パーティションの設置等、特定個人情報が他部門に見えないよう分離を行っているか確かめる。 | 6.1.(13) | | |
| | | | 12 | ○ | **xii）機器の物理的な保護**<br>統括情報セキュリティ責任者によって、無線LANアクセス時の認証システムや、無線LANのアクセスポイントは、第3者の手が届かない場所に設置する。 | □フロアレイアウト | 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アクセス時の認証システムや、無線LANのアクセスポイントは、第3者の手が届かない場所に設置していることを確かめる。 | 6.1.(13) | 7.8 | |
| | | | 13 | ○ | **xⅲ）特権管理者・保守端末の管理**<br>統括情報セキュリティ責任者によって、無線LANの保守は、業務端末とは分けた専用の保守端末で実施する。 | □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、無線LANの保守は、業務端末とは分けた専用の保守端末で実施することが文書化され、正式に承認されているか確かめかる。 | 6.1.(13) | | |

# 別紙3

参考　市区町村においてクラウドサービス上で標準準拠システム等を整備及び運用する場合の追加監査項目を、次頁以降に示す。

別紙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JISQ27017番号 | 留意事項 |
|---|---|---|---|---|---|---|---|---|---|---|
| 1.<br>組織体制 | | (10)クラウドサービス利用における組織体制 | 1 | ○ | **ⅰ)クラウドサービス利用における組織体制**<br>①統括情報セキュリティ責任者によって、クラウドサービスを利用する際には、必要な連絡体制が構築されている。また、クラウドサービス利用における情報セキュリティ対策に取り組む十分な組織体制が確立されている。 | □情報セキュリティポリシー<br>□権限・責任等一覧 | 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、クラウドサービス利用における情報セキュリティ対策に係る複数の事業者の存在・責任の所在を確認し、複数の事業者が存在する場合は、必要な連絡体制が構築されているか確かめる。また、クラウドサービス利用における情報セキュリティ対策に取り組む十分な体制が確立されていることを確かめる。 | 1.(10)① | 6.1.1<br>6.1.3<br>7.2.1 | |
| 2.<br>情報資産の分類と管理 | | (2)情報資産の管理 | 2 | ○ | **ⅰ)管理責任**<br>情報セキュリティ管理者によって、クラウドサービスの環境に保存される情報資産についても情報資産の分類に基づき管理されている。また、クラウドサービスを更改する際の情報資産の移行及びこれらの情報資産の全ての複製のクラウドサービス事業者からの削除の記述を含むサービス利用の終了に関する内容について、サービス利用前に文書での提示を求め、又は公開されている内容を確認している。 | □情報セキュリティポリシー<br>□情報資産分類基準<br>□クラウドサービス事業者の情報の取扱いに関する文書 | 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、情報資産の管理に関わる基準が文書化され、正式に承認されているか確かめる。クラウドサービス事業者からの削除の記述を含むサービス利用の終了に関する内容について記載された文書を確かめる。 | 2.(2)①(ウ) | 8.1.1<br>8.2.2 | |
| | | | 3 | ○ | **ⅱ)情報資産の廃棄等**<br>クラウドサービスで利用する全ての情報資産について、クラウドサービスの利用終了時期を確認し、クラウドサービスで扱う情報資産が適切に移行及び削除されるよう管理されている。 | □情報資産管理基準<br>□情報資産管理台帳<br>□情報資産廃棄記録 | 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により、情報資産を廃棄する場合、情報セキュリティ管理者の許可を得て、情報の機密性に応じて適切な処理をした上で廃棄され、行った処理について、日時、担当者及び処理内容が記録されているか確かめる。 | 2.(2)⑩(エ) | 8.2.3<br>8.3.2 | |
| | | (1)マイナンバー利用事務系 | 4 | ○ | **ⅰ)マイナンバー利用事務系と接続されるクラウドサービス上での情報システムの扱い**<br>マイナンバー利用事務系の端末・サーバ等と専用回線により接続されるガバメントクラウド上の情報システムの領域については、マイナンバー利用事務系として扱い、本市の他の領域とはネットワークを分離している。 | □ネットワーク管理基準<br>□通信回線敷設図<br>□結線図 | 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、マイナンバー利用事務系と他の領域が分離されており、通信できないようになっているか確かめる。 | 3.(1)③ | 13.1.3 | |

| 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JISQ27017番号 | 留意事項 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | 5 | ○ | **ⅱ）マイナンバー利用事務系と接続されるクラウドサービス上での情報資産の取扱い**<br>マイナンバー利用事務系の情報システムをガバメントクラウドにおいて利用する場合は、暗号による対策を実施している。<br>また、クラウドサービス事業者が暗号に関する対策を行う場合又はクラウドサービス事業者が提供する情報資産を保護するための暗号機能を利用する場合、クラウドサービス事業者が提供するそれらの機能や内容について情報を入手している。 | □ネットワーク管理基準<br>□通信回線敷設図<br>□結線図 | 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、マイナンバー利用事務系をガバメントクラウドにおいて利用する場合に適切な暗号方式が利用されていることを確認する。また、クラウドサービス事業者の提供する暗号に関する対策を利用する場合もそれらの機能及び内容について、情報の入手や確認を行っているか確かめる。 | 3.(1)④ | 10.1.1<br>10.1.2 | |
| | | (2)<br>LGWAN接続系 | 6 | ○ | **ⅰ）LGWAN接続系と接続されるクラウドサービス上での情報システムの扱い**<br>LGWAN接続系の情報システムをクラウドサービス上へ配置する場合は、その領域をLGWAN接続系として扱い、マイナンバー利用事務系とネットワークを分離し、専用回線を用いて接続しなければならない。 | □ネットワーク管理基準<br>□通信回線敷設図<br>□結線図 | 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接続系とマイナンバー利用事務系の通信環境は分離されていることを確かめる。また、クラウドサービスとは専用回線で接続されていることを確かめる。 | 3.(2)② | 13.1.3 | |
| 4.<br>物理的セキュリティ | | (7)機器の情報の廃棄 | 7 | ○ | **ⅰ）機器の廃棄等**<br>クラウドサービス事業者が利用する資源（装置等）の処分（廃棄）をする者は、セキュリティを確保した対応となっているか、クラウドサービス事業者の方針及び手順について確認している。<br>なお、当該確認にあたっては、クラウドサービス事業者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用している。 | □情報資産管理基準<br>□情報資産管理台帳<br>□情報資産廃棄記録<br>□クラウドサービスの監査報告書<br>□第三者認証文書／登録証 | 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、情報資産を廃棄する場合、クラウドサービス管理者の許可を得て、情報の機密性に応じて適切な処理をした上で廃棄され、行った処理について、日時、担当者及び処理内容が記録されているか確かめる。 | 4.1(7)② | 11.2.7 | |

| 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JISQ27017番号 | 留意事項 |
|---|---|---|---|---|---|---|---|---|---|---|
| 5.<br>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<br>⑨クラウドサービス利用時等の遵守事項 | 8 | ○ | **ⅰ)クラウドサービス利用時等の遵守事項**<br>職員等は、クラウドサービスの利用にあたっても情報セキュリティポリシー を遵守し、クラウドサービスの利用に関する自らの役割及び責任を意識している。 | □情報セキュリティポリシー<br>□職員等への周知記録 | 監査資料のレビューと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が遵守されているか確かめる。 | 5.1.(1)⑨ | CLD6.3.1 | |
| | 5.2. 研修・訓練 | (1)情報セキュリティに関する研修・訓練 | 9 | ○ | **ⅰ)クラウドサービスを利用する職員等の教育・研修**<br>CISOは、定期的にクラウドサービスを利用する職員等の情報セキュリティに関する意識向上、教育及び訓練を実施するとともに、委託先を含む関係者については、委託先等で教育、訓練が行われていることを確認している。 | □教育・研修実施基準<br>□教育実施報告書<br>□研修実施報告書<br>□クラウドサービスの監査報告書<br>□第三者認証文書／登録証 | 監査資料のレビューとCISOへのインタビューにより、定期的にクラウドサービスを利用する職員等の情報セキュリティに関する教育・研修が実施されているか確かめる。また、委託先を含む関係者については、委託先等で教育、訓練が行われていることを確認していることを確かめる。 | 5.2.(1)② | 7.2.2 | |
| | 5.3.情報セキュリティインシデントの報告 | (1)庁内での情報セキュリティインシデントの報告 | 10 | ○ | **ⅰ) クラウドサービス利用に関する情報セキュリティインシデントの報告**<br>情報セキュリティ責任者は、クラウドサービス利用における情報セキュリティインシデントの報告について連絡体制の対象者に報告している。 | □情報セキュリティインシデント報告手順書<br>□情報セキュリティインシデント報告書<br>□緊急連絡網/体制図 | 監査資料のレビューと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周知されているか確かめる。 | 5.3.(1)⑤ | 16.1.2<br>16.1.3 | |
| | | (2)住民等外部からの情報セキュリティインシデントの報告 | 11 | ○ | **ⅰ) クラウドサービス事業者が検知したインシデントの追跡**<br>統括情報セキュリティ責任者は、クラウドサービス事業者が検知した情報セキュリティインシデントの報告や情報セキュリティインシデントの状況を追跡する仕組みの構築を契約等で取り決めている。 | □クラウドサービスの仕様書/基本契約書及び利用規約<br>□クラウドサービスの監査報告書<br>□情報セキュリティインシデント報告手順書<br>□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へのインタビューにより、情報セキュリティインシデントの報告や情報セキュリティインシデントの状況を追跡する仕組みの構築が契約等で取り決められているか確かめる。 | 5.3.(2)⑤ | 16.1.2<br>16.1.3<br>16.1.4<br>16.1.5 | |



別紙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JISQ27017番号 | 留意事項 |
|---|---|---|---|---|---|---|---|---|---|---|
| 6.技術的セキュリティ | 6.1.コンピュータ及びネットワークの管理 | (2)バックアップの実施 | 12 | ○ | **ⅰ）クラウドサービス事業者のバックアップ機能の利用**<br>統括情報セキュリティ責任者及び情報システム管理者は、クラウドサービス事業者のバックアップ機能を利用する場合、クラウドサービス事業者にバックアップ機能の仕様を要求し、その仕様を確認している。また、その機能の仕様が本市の求める要求事項を満たすことを確認している。クラウドサービス事業者からバックアップ機能を提供されない場合やバックアップ機能を利用しない場合は、自らバックアップ機能の導入に関する責任を負い、バックアップに関する機能を設け、情報資産のバックアップを行っている。 | □情報セキュリティポリシー<br>□クラウドサービスの仕様書/基本契約書及び利用規約<br>□クラウドサービスの監査報告書<br>□バックアップ基準<br>□バックアップ手順書<br>□クラウドサービスの合意書(SLA)<br>□セキュリティ機能調査結果<br>□バックアップ実施記録 | 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、クラウドサービス事業者のバックアップ機能の仕様が本市の求める要求事項を満たしているか確かめる。<br>クラウドサービス事業者からのバックアップ機能を利用しない場合は、自らバックアップの機能を設け、情報資産のバックアップが行われているか確かめる。 | 6.1.(2)④ | 12.3.1 | |
| | | (6)ログの取得等 | 13 | ○ | **ⅰ）クラウドサービス事業者のログ等の保護**<br>統括情報セキュリティ責任者及び情報システム管理者は、クラウドサービス事業者が収集し、保存する記録(ログ等)に関する保護(改ざんの防止等)の対応について、ログ管理等に関する対策や機能に関する情報を確認し、記録(ログ等)に関する保護が実施されているのか確認している。 | □情報セキュリティポリシー<br>□クラウドサービスの仕様書/基本契約書及び利用規約<br>□システム運用基準<br>□クラウドサービスの合意書(SLA)<br>□セキュリティ機能調査結果 | 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、クラウドサービス事業者が収集するログ等が仕様どおりに取得され、詐取、改ざん、誤消去等されないように必要な措置が講じられているか確かめる。 | 6.1.(6)③ | 12.4.1<br>12.4.2 | |
| | | (6)ログの取得等 | 14 | ○ | **ⅱ）クラウドサービス事業者へのログ等の提出要求**<br>統括情報セキュリティ責任者及び情報システム管理者は、監査及びデジタルフォレンジック に必要となるクラウドサービス事業者の環境内で生成されるログ等の情報(デジタル証拠)について、クラウドサービス事業者から提供されるログ等の監視機能を利用して取得することで十分では無い場合は、クラウドサービス事業者に提出を要求するための手続を明確にしている。 | □クラウドサービスの仕様書/基本契約書及び利用規約<br>□クラウドサービスの監査報告書<br>□システム運用基準<br>□クラウドサービスの合意書(SLA)<br>□ログ等の提出要求手順書 | 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、クラウドサービス事業者の環境内で生成されるログ等の情報(デジタル証拠)について、提出を要求するための手順が定められているか確かめる。 | 6.1.(6)④ | 12.4.1<br>12.4.2<br>CLD.9.5.2 | |

| 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JISQ27017番号 | 留意事項 |
|---|---|---|---|---|---|---|---|---|---|---|
| | 6.4.不正プログラム対策 | (1)統括情報セキュリティ責任者の措置事項 | 15 | ○ | **ⅰ）仮想マシン設定時の不正プログラム対策**<br>仮想マシンを設定する際に不正プログラムへの対策(必要なポート、プロトコル及びサービスだけを有効とすることやマルウェア対策及びログ取得等の実施)を確実に実施している。SaaS 型を利用する場合は、これらの対応が、クラウドサービス事業者側でされているのか、サービスを利用する前に確認している。また、サービスを利用している状況下では、これらのセキュリティ対策が適切にされているのか定期的にクラウドサービス事業者に報告を求めている。 | □クラウドサービスの仕様書/基本契約書及び利用規約<br>□クラウドサービスの監査報告書<br>□ネットワーク設定基準<br>□クラウドサービスの合意書(SLA) | 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、クラウドサービス事業者が不正プログラムへの対策を施しているか定期的に確認しているか確かめる。 | 6.4.(1)⑧ | 9.1.2<br>13.1.1<br>13.1.2<br>CLD.9.5.2 | |
| | 6.5.不正アクセス対策 | (1)統括情報セキュリティ責任者の措置事項 | 16 | ○ | **ⅰ）クラウドサービス利用のアクセス制御ポリシーの遵守**<br>本市が定めたクラウドサービスの利用に関するポリシー(情報セキュリティポリシー)におけるアクセス制御に関する事項が、クラウドサービスにおいて実現できるのか又はクラウドサービス事業者の提供機能等により実現できるのか、利用前にクラウドサービス事業者に確認している。 | □情報セキュリティポリシー<br>□クラウドサービスの合意書(SLA)<br>□セキュリティ機能調査結果<br>□クラウドサービスの監査報告書 | 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、クラウドサービスの利用における不正アクセス防止のためのアクセス制御が施しているか確かめる。 | 6.5.(1)⑥ | 9.1.2<br>13.1.1<br>13.1.2 | |
| | | | 17 | ○ | **ⅱ）クラウドサービス利用の管理者権限の管理**<br>クラウドサービスを利用する際に、委託事業者等に管理権限を与える場合、多要素認証を用いて認証させ、クラウドサービスにアクセスさせている。 | □情報セキュリティポリシー<br>□委託管理基準<br>□クラウドサービスの仕様書/基本契約書及び利用規約 | 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、委託事業者等に管理権限を与える場合、二つ以上の認証手段が併用されているか確かめる。 | 6.5.(1)⑦ | 9.2.3<br>9.2.4<br>9.4.1 | |

| 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JISQ27017番号 | 留意事項 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | 18 | ○ | **iii）クラウドサービス利用時の認証情報の管理**<br>パスワードなどの認証情報の割り当てがクラウドサービス側で実施される場合、その管理手順等が、本市が定めたクラウドサービスの利用に関するポリシー（情報セキュリティポリシー）を満たすことを確認している。 | □情報セキュリティポリシー<br>□クラウドサービスの仕様書/基本契約書及び利用規約<br>□セキュリティ機能調査結果 | 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、クラウドサービス事業者のパスワードなどの管理手順等が本市の求める要求事項を満たしているか確かめる。 | 6.5.(1)⑧ | 9.4.1 | |
| | 6.6.セキュリティ情報の収集 | (1)セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等 | 19 | ○ | **ⅰ）セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等**<br>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、クラウドサービス事業者に対して、利用するクラウドサービスに影響し得る技術的脆弱性の管理内容について情報を求め、本市の業務に対する影響や保有するデータへの影響について特定している。そのうえで、技術的脆弱性に対する脆弱性管理の手順について、クラウドサービス事業者に確認している。 | □クラウドサービスの運用手順書/保守手順書<br>□クラウドサービスの仕様書/基本契約書及び利用規約<br>□クラウドサービスの監査報告書 | 監査資料のレビューと統括情報セキュリティ責任者及び情報システム管理者へのインタビューにより、クラウドサービス事業者に対して、利用するクラウドサービスに影響し得る技術的脆弱性の管理内容について情報を求め、業務に対する影響や保有するデータへの影響について特定していることを確かめる。そして、技術的脆弱性に対する脆弱性管理の手順について、クラウドサービス事業者に確認していることを確かめる。 | 6.6.(1)② | 12.6.1 | |
| 7.運用 | 7.1.情報システムの監視 | (3)情報システムの監視 | 20 | ○ | **ⅰ）クラウドサービス利用における時刻同期**<br>利用するクラウドサービスで使用する時刻の同期について適切にされているのか確認している。 | □クラウドサービスの運用手順書/保守手順書<br>□クラウドサービスの仕様書/基本契約書及び利用規約<br>□クラウドサービスの監査報告書 | 監査資料のレビューと統括情報セキュリティ責任者及び情報システム管理者へのインタビューにより、クラウドサービスで使用する時刻の同期の仕様や手順について確認していることを確かめる。 | 7.1.(3)② | 12.4.4 | |
| | | | 21 | ○ | **ⅱ）クラウドサービス利用におけるリソースの確保**<br>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、必要となるリソースの容量・能力が確保できるクラウドサービス事業者を選定している。また、利用するクラウドサービスの使用において必要な監視機能を確認するとともに監視により、業務継続の上で必要となる容量・能力を予測し、業務が維持できるようにしている。 | □クラウドサービスの選定基準<br>□クラウドサービスの仕様書/基本契約書及び利用規約<br>□クラウドサービスの監査報告書 | 監査資料のレビューと統括情報セキュリティ責任者及び情報システム管理者へのインタビューにより、必要となるリソースの容量・能力が確保できるクラウドサービス事業者を選定していることを確かめる。また、利用するクラウドサービスの使用において必要な監視機能を確認するとともに監視により、業務継続の上で必要となる容量・能力を予測し、業務が維持できるようにしていることを確かめる。 | 7.1.(3)⑤ | 15.1.3<br>CLD.12.4.5 | |

| 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JISQ27017番号 | 留意事項 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | 22 | ○ | **iii）クラウドサービス利用におけるログの取得**<br>統括情報セキュリティ責任者及び情報システム管理者は、イベントログ取得に関するポリシーを定め、利用するクラウドサービスがその内容を満たすことを確認し、クラウドサービス事業者からログ取得機能が提供される場合は、そのログ取得機能が適切かどうか、ログ取得機能を追加して実装すべきかどうかを検討している。 | □クラウドサービスの選定基準<br>□クラウドサービスログ取得基準<br>□クラウドサービスの仕様書/基本契約書及び利用規約<br>□クラウドサービスの監査報告書 | 監査資料のレビューと統括情報セキュリティ責任者及び情報システム管理者へのインタビューにより、イベントログ取得に関するポリシーが定められており、利用するクラウドサービスがその内容を満たすことを確認していることを確かめる。また、クラウドサービス事業者からログ取得機能が提供される場合は、そのログ取得機能が適切かどうか、ログ取得機能を追加して実装すべきかどうかを検討していることを確かめる。 | 7.1.(3)⑥ | 15.1.3<br>CLD.12.4.5 | |
| | | | 23 | ○ | **iv）クラウドサービス利用における手順書の確認**<br>統括情報セキュリティ責任者及び情報システム管理者は、クラウドサービス利用における重大なインシデントに繋がるおそれのある以下の重要な操作に関して、手順化し、確認している。<br>(ア)サーバ、ネットワーク、ストレージなどの仮想化されたデバイスのインストール、変更及び削除<br>(イ)クラウドサービス利用の終了手順<br>(ウ)バックアップ及び復旧 | □クラウドサービスの利用手順書<br>□クラウドサービスの仕様書/基本契約書及び利用規約<br>□クラウドサービスの監査報告書 | 監査資料のレビューと統括情報セキュリティ責任者及び情報システム管理者へのインタビューにより、クラウドサービス利用における重大なインシデントに繋がるおそれのある以下の重要な操作に関して、手順化し、妥当性を確認していることを確かめる。<br>(ア)サーバ、ネットワーク、ストレージなどの仮想化されたデバイスのインストール、変更及び削除<br>(イ)クラウドサービス利用の終了手順<br>(ウ)バックアップ及び復旧 | 7.1.(3)⑦ | 15.1.3<br>CLD.12.1.5 | |
| 7.3.<br>侵害時の対応 | (1)緊急時対応計画の策定 | | 24 | ○ | **ⅰ）クラウドサービス利用におけるインシデント管理の責任と役割**<br>CISO又は情報セキュリティ委員会は、クラウドサービス事業者と情報セキュリティインシデント管理における責任と役割の分担を明確にし、これらを踏まえてクラウドサービスの障害時を想定した緊急時対応計画を定められており、セキュリティ侵害時には当該計画に従って適正に対処している。 | □クラウドサービスの利用手順書<br>□クラウドサービスの仕様書/基本契約書及び利用規約<br>□クラウドサービスの緊急連絡先一覧<br>□クラウドサービスの緊急時対応計画 | 監査資料のレビューとCISO又は情報セキュリティ委員会へのインタビューにより、クラウドサービス事業者と情報セキュリティインシデント管理における責任と役割の分担を明確にし、これらを踏まえてクラウドサービスの障害時を想定した緊急時対応計画を定められている。また、セキュリティ侵害時には当該計画に従って適正に対処していることを確かめる。 | 7.3.(1)② | 16.1.2 | |

| 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JISQ27017番号 | 留意事項 |
|---|---|---|---|---|---|---|---|---|---|---|
| | 7.5.<br>法令遵守 | | 25 | ○ | **ｉ）クラウドサービス利用におけるソフトウェアライセンスの管理**<br>統括情報セキュリティ責任者及び情報システム管理者は、クラウドサービスに商用ライセンスのあるソフトウェアをインストールする（IaaS等でアプリケーションを構築）場合は、そのソフトウェアのライセンス条項への違反を引き起こす可能性があるため、利用するソフトウェアにおけるライセンス規定に従っている。 | □クラウドサービスの利用手順書<br>□クラウドサービスの仕様書/基本契約書及び利用規約<br>□ソフトウェアライセンス管理表 | 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、クラウドサービスに商用ライセンスのあるソフトウェアをインストールする（IaaS等でアプリケーションを構築）場合は、そのソフトウェアのライセンス条項に違反しないように、利用するソフトウェアにおけるライセンス規定に従っていることを確かめる。 | 7.5.(2) | 8.1.1<br>11.2.7<br>18.1.2<br>CLD.6.3.1 | |



別紙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JISQ27017番号 | 留意事項 |
|---|---|---|---|---|---|---|---|---|---|---|
| 8.業務委託と外部サービス(クラウドサービス)の利用 | 8.3.外部サービス(クラウドサービス)の利用(機密性2以上の情報を取り扱う場合) | (1)クラウドサービスの利用に係る規定の整備 | 26 | ○ | **ｉ）クラウドサービス利用における規定の整備**<br>クラウドサービス管理者の指名とクラウドサービスの利用状況が管理されていること。 | □クラウドサービス利用規定<br>□クラウドサービスの仕様書/基本契約書及び利用規約<br>□クラウドサービスに係る体制表/連絡網 | 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、クラウドサービス管理者が指名されていること及びクラウドサービスの利用状況が管理されていることを確かめる。 | 8.3.(1)⑤ | 15.1.1<br>15.1.2 | |
| | | (3)クラウドサービスの選定 | 27 | ○ | **ｉ）クラウドサービス利用における情報セキュリティ対策情報の提供**<br>情報セキュリティ責任者は、情報セキュリティ対策に関する情報の提供を求め、その内容を確認し、利用する外部サービス(クラウドサービス)が、本市が定めたクラウドサービスの利用に関するポリシー(情報セキュリティポリシー)を満たしているか否かを評価している。 | □情報セキュリティポリシー<br>□クラウドサービス利用規定<br>□クラウドサービスの仕様書/基本契約書及び利用規約<br>□クラウドサービスの監査報告書<br>□第三者認証文書／登録証 | 監査資料のレビューと情報セキュリティ責任者へのインタビューにより、情報セキュリティ対策に関する情報の提供を求め、その内容を確認し、利用するクラウドサービスが、本市が定めたクラウドサービスの利用に関するポリシー(情報セキュリティポリシー)を満たしているか否かを評価していることを確かめる。また、情報セキュリティ対策には以下の内容が含まれていることを確かめる。<br><含まれる情報セキュリティ対策><br>(ア)クラウドサービスの利用を通じて本市が取り扱う情報のクラウドサービス提供者における目的外利用の禁止<br>(イ)クラウドサービス提供者における情報セキュリティ対策の実施内容及び管理体制<br>(ウ)クラウドサービスの提供に当たり、クラウドサービス提供者若しくはその従業員、再委託先又はその他の者によって、本市の意図しない変更が加えられないための管理体制<br>(エ)クラウドサービス提供者の資本関係・役員等の情報、クラウドサービス提供に従事する者の所属・専門性(情報セキュリティに係る資格・研修実績等)・実績及び国籍に関する情報提供並びに調達仕様書による施設の場所やリージョンの指定<br>(オ)情報セキュリティインシデントへの対処方法<br>(カ)情報セキュリティ対策その他の契約の履行状況の確認方法<br>(キ)情報セキュリティ対策の履行が不十分な場合の対処方法 | 8.3.(3)③ | 15.1.1<br>15.1.2 | |



別紙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JISQ27017番号 | 留意事項 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | 28 | ○ | **ⅱ）クラウドサービス利用における役割と責任**<br>情報セキュリティ責任者は、クラウドサービス事業者と情報セキュリティに関する役割及び責任の分担について確認している。 | □クラウドサービスの仕様書/基本契約書及び利用規約<br>□クラウドサービス利用に係る体制図 | 監査資料のレビューと情報セキュリティ責任者へのインタビューにより、クラウドサービス事業者と情報セキュリティに関する役割及び責任の分担について確かめる。 | 8.3.(3)⑤ | 15.1.1<br>15.1.2 | |
| | | | 29 | ○ | **ⅲ）クラウドサービス利用におけるSLAの定め**<br>クラウドサービスの利用前に合意した事項があれば、その内容についてサービス合意書（SLA）に定めている。クラウドサービス事業者のサービス利用規約等が変更できない場合は、機密性・完全性・可用性・安全性・個人情報等の扱いに関するクラウドサービス事業者の定める条件を鑑み、その規約内容が本市によって受容可能か判断している。 | □情報セキュリティポリシー<br>□クラウドサービス利用規定<br>□クラウドサービス選定基準<br>□クラウドサービスの仕様書/基本契約書及び利用規約<br>□クラウドサービスの合意書（SLA）<br>□クラウドサービスの監査報告書<br>□第三者認証文書／登録証 | 監査資料のレビューと情報セキュリティ責任者へのインタビューにより、クラウドサービスの利用前に合意した事項があれば、その内容についてサービス合意書（SLA）に定めていることを確かめる。クラウドサービス事業者のサービス利用規約等が変更できない場合は、機密性・完全性・可用性・安全性・個人情報等の扱いに関するクラウドサービス事業者の定める条件を鑑み、その規約内容が本市によって受容可能か判断していることを確かめる。 | 8.3.(3)⑤ | 15.1.1<br>15.1.2 | |
| | | (4)クラウドサービスの利用承認 | 30 | ○ | **ⅰ）クラウドサービス利用の管理者の指名**<br>利用申請の許可権限者は、クラウドサービスの利用申請を承認した場合は、承認済みクラウドサービスとして記録し、クラウドサービス管理者を指名している。（クラウドサービスを利用する場合も同様の措置を行う。） | □クラウドサービスの仕様書/基本契約書及び利用規約<br>□クラウドサービス利用申請書<br>□クラウドサービス利用に係る体制図 | 監査資料のレビューと利用申請の許可権限者へのインタビューにより、クラウドサービスの利用申請を承認した場合は、承認済みクラウドサービスとして記録し、クラウドサービス管理者を指名していることを確かめる。 | 8.2.(4)③ | 6.1.1<br>6.1.3 | |



別紙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JISQ27017番号 | 留意事項 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | (5)クラウドサービスを利用した情報システムの導入・構築時の対策 | 31 | ○ | **ⅰ）クラウドサービス利用におけるユーティリティプログラムのセキュリティ**<br>統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方等を踏まえ、クラウドサービスを利用して情報システムを構築する際のセキュリティ対策を規定している。 | □情報セキュリティポリシー<br>□クラウドサービス利用規定<br>□クラウドサービスの仕様書/基本契約書及び利用規約<br>□クラウドサービスの監査報告書<br>□第三者認証文書／登録証 | 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、クラウドサービスの特性や責任分界点に係る考え方等を踏まえ、クラウドサービスを利用して情報システムを構築する際のセキュリティ対策を規定していることを確かめる。また、情報セキュリティ対策には以下の内容が含まれていることを確かめる。<br>〈含まれる情報セキュリティ対策〉<br>(ア)不正なアクセスを防止するためのアクセス制御<br>(イ)取り扱う情報の機密性保護のための暗号化<br>(ウ)開発時におけるセキュリティ対策<br>(エ)設計・設定時の誤りの防止<br>(オ)クラウドサービスにおけるユーティリティプログラムに対するセキュリティ対策 | 8.2.(5)①(オ) | 9.4.4 | |
| | | | 32 | ○ | **ⅱ）クラウドサービス利用のセキュリティに配慮した構築**<br>クラウドサービス管理者により、クラウドサービスの利用において定められた規定に対し、情報セキュリティに配慮した構築の手順及び実践がされていることの確認及び記録が取られている。 | □情報セキュリティポリシー<br>□クラウドサービス利用規定<br>□クラウドサービスの構築手順書<br>□クラウドサービスの設計書<br>□クラウドサービスの監査報告書 | 監査資料のレビューとクラウドサービス管理者へのインタビューにより、クラウドサービスの利用において定められた規定に対し、情報セキュリティに配慮した構築の手順及び実践がされていることの確認及び記録が取られていることを確かめる。 | 8.2.(5)③ | 14.2.1<br>15.1.1<br>15.1.2 | |



別紙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JISQ27017番号 | 留意事項 |
|---|---|---|---|---|---|---|---|---|
| (6)クラウドサービスを利用した情報システムの運用・保守時の対策 | 33 | ○ | **ⅰ）クラウドサービス利用の設計・設定変更時の管理**<br>統括情報セキュリティ責任者により、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、クラウドサービスを利用して情報システムを運用する際のセキュリティ対策が規定されている。 | □情報セキュリティポリシー<br>□クラウドサービス利用規定<br>□クラウドサービスの設定/設定変更手順書 | 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、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、クラウドサービスを利用して情報システムを運用する際のセキュリティ対策が規定されていることを確かめる。また、情報システムを運用する際のセキュリティ対策には以下の内容が含まれていることを確かめる。<br>＜含まれるセキュリティ対策＞<br>(ア)クラウドサービス利用方針の規定<br>(イ)クラウドサービス利用に必要な教育<br>(ウ)取り扱う資産の管理<br>(エ)不正アクセスを防止するためのアクセス制御<br>(オ)取り扱う情報の機密性保護のための暗号化<br>(カ)クラウドサービス内の通信の制御<br>(キ)設計・設定時の誤りの防止<br>(ク)クラウドサービスを利用した情報システムの事業継続<br>(ケ)設計・設定変更時の情報や変更履歴の管理 | 8.2.(6)①(ケ) | 15.1.1<br>15.1.2 | |
| | 34 | ○ | **ⅱ）クラウドサービス利用の運用・保守状況の確認**<br>クラウドサービス事業者により、利用しているクラウドサービスにおいて情報セキュリティに配慮した運用・保守の手順及び実践がされている。また、クラウドサービス事業者に情報を求め、実施状況を定期的に確認及び記録されている。 | □情報セキュリティポリシー<br>□クラウドサービス利用規定<br>□クラウドサービスの運用手順書/保守手順書<br>□クラウドサービスの監査報告書 | 監査資料のレビューとクラウドサービス管理者へのインタビューにより、情報セキュリティに配慮した運用・保守の手順及び実践がされているか、クラウドサービス事業者に情報を求め、実施状況を定期的に確認及び記録されていることを確かめる。 | 8.2.(6)④ | 15.1.1<br>15.1.2 | |

| 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JISQ27017番号 | 留意事項 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | (7)クラウドサービスを利用した情報システムの更改・廃棄時の対策 | 35 | ○ | **ⅰ）クラウドサービス利用の機密性の高い情報への対策**<br>クラウドサービス管理者により、クラウドサービス上で機密性の高い情報(住民情報等)を保存する場合の暗号化やその情報資産を破棄する際の暗号化した鍵(暗号鍵)の削除など、その情報資産を復元困難な状態としている。 | □クラウドサービスの仕様書/基本契約書及び利用規約<br>□暗号に関する仕様書/暗号化に関する規定(鍵管理手順含む) | 監査資料のレビューとクラウドサービス管理者へのインタビューにより、クラウドサービス上で機密性の高い情報(住民情報等)を保存する場合の暗号化や廃棄する際の暗号化した鍵(暗号鍵)の削除などの情報資産を復元困難な状態とする対策が実施されていることを確かめる。 | 8.2.(7)③ | 15.1.1<br>15.1.2 | |
| 9.<br>評価見直し | 9.1.<br>監査 | (4)委託事業者に対する監査 | 36 | ○ | **ⅰ）クラウドサービス事業者への監査**<br>情報セキュリティ監査統括責任者により、クラウドサービス事業者が自ら定める情報セキュリティポリシーの遵守について、定期的に監査が行われている。 | □クラウドサービスの監査報告書 | 監査資料のレビューとCISOまたは情報セキュリティ監査統括責任者へのインタビューにより、クラウドサービス事業者が自ら定める情報セキュリティポリシーの遵守について、定期的に監査が行われていることを確かめる。クラウドサービス事業者にその証拠(文書等)の提示を求めている場合は、第三者の監査人が発行する証明書や監査報告書等をこの証拠としていることを確かめる。 | 9.1.(4)② | 18.1.1<br>18.2.1 | |

付録

○監査資料例一覧／索引

○情報セキュリティ監査実施要綱（例）

○情報セキュリティ監査実施計画書（例）

○情報セキュリティ監査報告書（例）

○情報セキュリティ監査業務委託仕様書（例）

○情報セキュリティ監査業務委託契約書（例）

別紙3

# 監査資料例一覧／索引

# 別紙3

## 監 査 資 料 例 一 覧 ／ 索 引

（注）情報セキュリティ監査の実施にあたって、確認すべき文書や記録の例を示したもの。文書や記録は、各地方公共団体によって異なると考えられることから、必ずしもこの例によらない場合があることに留意する。また、必ずしも文書化が必須という訳ではない。
なお、該当No.における表示は、自No.：自治体情報セキュリティクラウドの調達を行った場合の追加監査項目、α'No.：α'モデルを採用する場合の追加監査項目、βNo.：βモデルを採用する場合の追加監査項目、β'No.：β'モデルを採用する場合の追加監査項目を表す。

| 索引 | 名称 | 解 説 | 該当No. |
|---|---|---|---|
| あ | ICカード等管理台帳 | 職員等に付与されている認証証のICカードやUSBトークンの発行から廃棄までを管理する文書。 | 132,133 |
| | ICカード等取扱基準 | 認証のために職員等に発行されているICカードやUSBトークンなどの管理、紛失時の対応手順、廃棄時の手続などを記述した文書。 | 128,129,130,131,132,133 |
| | ICカード紛失届書 | 職員等が認証用ICカード等を紛失したことの報告及び、それに対してどのような対応をしたかを記録した文書。 | 131 |
| | ID取扱基準 | 職員等に付与されるIDの登録、変更、抹消等の情報管理、職員等の異動、出向、退職者に伴うIDの取扱い、貸与禁止や共用IDの利用制限など取扱いに関する基準について記述した文書。 | 134,135,136 |
| | アクセス管理基準 | アクセス制御方針に基づき、利用者の権限に応じたアクセス制御を行なう基準を記述した文書。 | 221,244,245,246,247,α'5,α'8,β'5 |
| | アクセス権限設定書 | 参照、更新、削除のアクセス権限範囲の定義を記述した文書。 | 255 |
| | アクセス制御方針 | 情報資産へのアクセスについて、業務上の必要性や禁止事項等の基本的な考えを記述した文書。 | 221,244,245,246,247,α'5,α'8,β'5 |
| | 移行手順書 | システム開発・保守及びテスト環境からシステム運用環境への移行する具体的な手順を記述した文書。 | 261,262,263 |
| | 委託管理基準 | 委託事業者との間で締結する契約の内容、委託業務の運用状況の確認等の基準を記述した文書。 | 109,110,361,363,364 |
| | 委託事業者監査報告書 | 外部に設置された機器の情報セキュリティ対策状況を確認するために行った監査の結果及び改善勧告について記述した文書。 | 48 |
| | 委託事業者訪問記録 | 外部に設置された機器の情報セキュリティ対策状況を確認するために訪問したこと（担当者、訪問日時等）を記録した文書。 | 48 |
| | 委託事業者選定基準 | 委託事業者の選定基準や選定方法等を記述した文書。 | 357,358,365,367,368,370 |
| | 委託事業者における<br>ISO/IEC27001認証取得状況 | 委託事業者のISO/IEC27001認証取得認定書又はこれに類する文書。 | 48 |
| | 委託判断基準 | 委託先への提供を認める情報及び委託する業務の範囲を判断する基準を記述した文書。 | 357,358,367,368,370 |
| | Web会議利用手順書 | Web会議利用時の申請、承認、セキュリティ対策などの手順を記述した文書。 | 212,213,214,215 |
| | 運用手順書 | 情報システムや機器等を運用するにあたりその手順を記述した文書。 | 自1,α'1,α'2,α'3,α'4,α'6,α'7,α'9,α'10,α'11,α'12,β1,β2,β3,β'1,β'2,β'3 |
| か | 改善計画 | 自己点検で問題点となった事項に対する改善計画を記述した文書。 | 412,417,418 |
| | 改善指示書 | 情報セキュリティ監査で明らかになった問題点に対し、当該部局などに対して改善指示を記述した文書。 | 412 |
| | 改善措置実施報告書 | 改善要望への対応結果を記録した委託事業者から提出される文書。 | 361 |

# 別紙3

## 監 査 資 料 例 一 覧 ／ 索 引

| 索引 | 名称 | 解 説 | 該当No. |
|---|---|---|---|
| | 改善要望書 | 不備が確認されたセキュリティ対策に対する改善要望を記述した文書。 | 361 |
| | 開発用ID登録・削除手続 | 開発者向けに発行するIDの登録、変更、抹消等の手続を記述した文書。 | 254 |
| | 開発用ID登録・削除申請書 | 開発用IDの発行、変更、抹消を申請する文書。 | 254 |
| | 開発用ID管理台帳 | 開発用IDを管理するために発行、変更、抹消及びアクセス権限区分を記録した文書。 | 254 |
| | 外部ネットワーク接続基準 | 外部ネットワークに接続する場合の事前調査や、損害賠償責任の担保、ファイアウォールの設置、問題が生じた場合の遮断などの基準を記述した文書。 | 171,172,173,174,176 |
| | 外部ネットワーク接続申請書/承認書 | 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の許可を得るために申請し、承認する文書。 | 172 |
| | 外部ネットワーク接続手続 | 所管するネットワークと外部ネットワークとを接続する場合の申請手続を記述した文書。 | 171,172,173,174,176 |
| | 外部ネットワーク調査結果 | 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の調査結果を記録した文書。 | 173 |
| | 監査実施計画 | 監査テーマ、監査項目、監査対象、監査実施日、監査実施者名、被実施部門名等を記述した文書。 | 404,405,406,407,409 |
| | 監査調書 | 監査人が実施し確認した内容を記録した文書。 | 411 |
| | 監査報告書 | 監査対象、監査結果、確認した監査証拠、指摘事項等を記述した文書。 | 404,405,406,408,409,410 |
| | 監視記録 | ネットワークや情報システムへのアクセスの成功又は失敗等を記録・分析した結果を記録した文書。 | 316,330,332 |
| | 管理区域（情報システム室等）のレイアウト図 | ネットワークの基幹機器や情報システムの設置状況が記載された文書。 | 30,51,52,53,54,55,56 |
| | 管理区域構造基準 | 管理区域の配置や立ち入り制限、管理区域内の機器の保護などの基準を記述した文書。 | 51 |
| | 管理区域入退室基準/手続 | 管理区域への入退室を管理するため、入退室制限や身分証明書等の携帯、職員の同行などの基準や、管理区域への入退室権限の申請や承認などの手続を記述した文書。 | 57,58,59,60,61 |
| | 管理区域入退室記録 | 管理区域への入退室情報（時間・IDナンバー等）を記録した文書や映像。 | 58,60,61,64 |
| | 関連法令等一覧 | 職員等が遵守すべき法令（例えば、地方公務員法第34条-守秘義務-や個人情報保護法施行条例等）を一覧にした文書。 | 351,352 |
| | 記憶装置廃棄記録 | 記憶装置の廃棄手段・方法及び実施内容を記録した文書。 | 50 |
| | 機器設置基準/手続 | サーバ等の機器を庁内あるいは庁外設置する場合に、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、容易に取外せないように固定するなどの基準や、設置する場合の申請や承認などの手続を記述した文書。 | 29,30,46,47,48 |
| | 機器設置記録 | ハードウェアを設置したときにベンダが作成する作業報告。 | 30,36,37 |
| | 機器電源基準 | 停電や瞬断、落雷等による過電流からサーバ等の機器を保護するための基準を記述した文書。 | 35,36,37 |

# 別紙3

## 監 査 資 料 例 一 覧 ／ 索 引

| 索引 | 名称 | 解 説 | 該当No. |
|---|---|---|---|
| | 機器等の設定指示書 | システムを構成するサーバ、端末及びネットワーク機器などの設定を行うため、設定情報を記述した文書。 | 自1,α'1,α'2,α'3,α'4,α'5,α'6,α'7,α'8,α'9,α'10,α'11,α'12,β1,β2,β3,β'1,β'2,β'3,β'5 |
| | 機器等の選定基準 | 対策基準に基づいた調達する機器等の選定基準を記述した文書。 | 248 |
| | 機器廃棄・リース返却基準 | 機器を廃棄する場合やリース返却する場合の基準を記述した文書。 | 49,50 |
| | 機器廃棄・リース返却手続 | 機器を廃棄する場合やリース返却する場合の申請や承認などの手続を記述した文書。 | 49,50 |
| | 機器搬入出基準/手続 | 管理区域への機器の搬入出の基準や、新しい情報システム等導入の際、既存のシステムへの影響を考慮するなどの基準及び管理区域への機器搬入出の申請や承認などの手続を記述した文書。 | 62,63,64 |
| | 機器搬入出記録 | 業者が機器を搬入出した際の作業内容を記録した文書。 | 64 |
| | 機器保守・修理基準/手続 | 機器の保守や修理に関する基準や、機器の保守や修理を行う場合の申請や承認などの手続を記述した文書。 | 43,44,45 |
| | 機器保守点検記録 | ベンダが機器を保守点検したときの作業内容を記録した文書。 | 36,44 |
| | 機密保持契約書 | 職務上知り得た機密情報の取扱いや負うべき義務・責任を定めた文書。 | 45 |
| | 業務委託契約書 | システム開発や運用等を外部の事業者に委託する場合に、委託する作業の内容や期間、支払方法、責任範囲、機密保持、損害賠償等の事項についての取り決めを記述した文書。 | 110,190,307,358,359,360,362,366 |
| | 業務継続計画 | 地震及び風水害等の自然災害等の事態に備えた、情報セキュリティにとどまらない危機管理を規定した文書。 | 345 |
| | 業務委託サービス選定基準 | クラウドサービスを除く情報システムの一部の機能を提供するサービスの委託先の選定基準を記述した文書。 | 369 |
| | 緊急時対応計画 | 情報セキュリティインシデント、情報セキュリティポリシーの違反等により情報資産へのセキュリティ侵害が発生した場合又は発生するおそれのある場合、関係者の連絡、証拠保全、被害拡大の防止、対応措置、再発防止措置の策定等を記述した文書。 | 313,314,315,342,344,345,346 |
| | クラウドサービス運用規程 | クラウドサービスの利用に関する基準を記述した文書。 | 374,375,376,377,378,379,380,381,382,383,384,386,387,388,391,395,400,401,402 |
| | クラウドサービス運用状況確認記録 | クラウドサービスの運用状況を確認したことを記録した文書。 | 397 |
| | クラウドサービス構築状況確認記録 | クラウドサービスの構築状況を確認したことを記録した文書。 | 392,399 |
| | クラウドサービスセキュリティ対策規程 | クラウドサービスの利用に当たり必要なセキュリティ対策を記述した文書。 | 389,393,398 |
| | クラウドサービス利用申請書 | クラウドサービスを利用する場合の許可を得るために申請する文書。 | 386,387,401,402 |

# 別紙3

## 監 査 資 料 例 一 覧 ／ 索 引

| 索引 | 名称 | 解 説 | 該当No. |
|---|---|---|---|
| | クラウドサービス利用審査結果 | クラウドサービスを利用する場合の許可を得るための申請に対する審査結果を記述した文書。 | 387,401,402 |
| | クラウドサービス利用時のセキュリティ要件 | クラウドサービス利用時に必要なセキュリティ対策について記述した文書。 | 384 |
| | クラウドサービス利用判断基準 | クラウドサービスの利用可否を判断するための基準や条件を記述した文書。 | 373,375,376,377,378,379,380,381,382,383,384,400 |
| | クラウドサービス提供者の選定基準 | クラウドサービスの選定に関する基準を記述した文書。 | 373,375,376,377,378,379,380,381,382,383,384,400,α'13 |
| | クリアデスク・クリアスクリーン基準 | パソコン等にある情報を無許可の閲覧から保護するための基準や、使用していない文書及び電磁的記録媒体を適切な場所へ安全に収納する等、机上の情報の消失及び損傷のリスクを軽減するための基準を記述した文書。 | 99,100 |
| | 訓練実施報告書 | 訓練の実施日、内容、参加者、使用テキスト等を記録した文書。 | 112,121,122 |
| | 結線図 | 庁内の通信回線装置間の配線を図に表した文書。 | 18,19,23,28,66,67,68,69,70,71,170,175 |
| | 権限・責任等一覧 | 情報セキュリティに関わる事項について、誰がどのような権限及び責任を持っているかを記述した文書。 | 1 |
| | 研修・訓練結果報告書 | 研修・訓練の実施日、内容、参加者、使用テキスト等を記録した文書。 | 117,118,β8,β9,β'7,β'9,β'11,β'12 |
| | 研修・訓練実施基準 | 情報セキュリティに関する研修や緊急時対応訓練の計画、実施、報告の基準を記述した文書。 | 104,111,112,113,114,115,116,119,120,121,122,α'15,β7,β'7,β'9,β'10 |
| | 研修・訓練実施計画 | 実施する研修・訓練のテーマ、実施予定日、内容、対象者、使用テキスト等を記述した文書。 | 113,114,116,117,120,α'14,α'15,α'16,β7,β8,β9,β'7,β'9,β'10,β'11,β'12 |
| | 研修・訓練受講記録 | 研修・訓練の実施日時、参加者氏名、研修・訓練の内容を記録した文書。 | 117,118,α'15,α'16,β8,β9,β'7,β'9,β'11,β'12 |
| | 研修実施報告書 | 研修の実施日、内容、参加者、使用テキスト等を記録した文書。 | 104,112,115,119,122 |
| | 研修・訓練に関するアンケート | 研修・訓練に対するアンケート及びアンケート結果を記録した文書。 | 117,118,,β'7,β'9 |
| さ | サーバ障害対応実施手順書 | 情報システム個別に作成した具体的なサーバ障害時対応手順を記述した文書。 | 33,34 |
| | サーバ障害対策基準 | サーバ障害時のセカンダリサーバへの切り替え等の対策基準を記述した文書。 | 33,34 |

# 別紙3

## 監 査 資 料 例 一 覧 ／ 索 引

| 索引 | 名称 | 解 説 | 該当No. |
|---|---|---|---|
| | サーバ冗長化基準 | 冗長化すべき対象サーバ、冗長化の方法などの基準を記述した文書。 | 31,32 |
| | サービス契約書 | 外部ネットワークに接続する場合に、利用するサービスの内容や期間、支払方法、責任範囲、機密保持、損害賠償等の事項についての取り決めを記述した文書。 | 174 |
| | サービス利用契約書 | クラウドサービスを利用する場合に、利用するサービスの内容や期間、支払方法、責任範囲、機密保持、損害賠償等の事項についての取り決めを記述した文書。 | 自1 |
| | サイバー攻撃情報やインシデント情報の通知記録 | サイバー攻撃やセキュリティインシデントに関する情報を、関係者に対して通知した記録。 | β5,β'6 |
| | 作業完了報告書 | 業務委託の終了に際し委託事業者に求める委託作業についての実施報告書。 | 363,364 |
| | 作業報告書 | 委託事業者から提出される委託業務（保守作業や配線作業等）の作業状況を記録した文書。 | 27,42,44,45,361 |
| | CSIRT設置要綱 | 情報セキュリティに関する統一的な窓口としてのCSIRTの役割、体制等の取り決めを記述した文書。 | 4 |
| | 敷地図面 | 敷地周辺及び敷地内の施設の配置を記述した文書。 | 51,52,53,54,55,56 |
| | 時刻設定手順書 | コンピュータ内の時計を標準時に合わせるための手順を記述した文書。 | 331 |
| | 自己点検結果 | 情報システム等を運用又は利用する者自らが情報セキュリティポリシーの履行状況を点検、評価した結果を記録した文書。 | 335,337,415,416,417,418 |
| | 自己点検結果報告書 | 点検対象、点検結果、確認した文書、問題点等を記述した文書。 | 415,416,417,418 |
| | 自己点検実施基準 | 情報システム等を運用又は利用する者自らが情報セキュリティポリシーの履行状況を点検、評価するための基準を記述した文書。 | 334,335,337 |
| | 自己点検実施計画 | 点検テーマ、点検項目、点検対象、点検実施日、点検実施者名等を記述した文書。 | 415,416 |
| | システム運用基準 | 情報システムの日常運用や変更等に関する体制、手続、手順等、システムを運用する上で遵守しなければならない基準を記述した文書。 | 72,153,154,155,156,159,160,161,162,325,326,327,328,329,330,331,332,334,335,337 |
| | システム運用作業記録 | 情報システムの運用担当者が作業した内容（作業時刻、作業内容、担当者名、作業結果等）を記録した文書。 | 154 |
| | システム開発・保守計画 | システム開発・保守にあたり、開発・保守体制、スケジュール、作業工程、会議体や開発・保守環境（使用するハードウェア、ソフトウェア）等を記述した文書。 | 256,257,258,261,262 |
| | システム開発・保守に関連する資料等の保管基準 | 資料等やテスト結果、ソースコード等の保管の基準を記述した文書。 | 275 |
| | システム開発基準 | 情報システムを開発する場合の工程、会議体、成果物、セキュリティ要件、変更管理等の基準を記述した文書。 | 276,277,278,283,284 |
| | システム開発規則 | 情報システムを開発する場合の作業者が実施するセキュリティに関するルールを記述した文書。 | 253 |

# 別紙3

## 監 査 資 料 例 一 覧 ／ 索 引

| 索引 | 名称 | 解 説 | 該当No. |
|---|---|---|---|
| | システム開発体制図 | 情報システムを開発する場合の責任者、作業者とその役割を記述した文書。 | 253 |
| | システム稼動記録 | 情報システムの稼動状況を記録した文書。 | 160,β4,β'4 |
| | システム監視手順書 | サーバに記録されているファイルのサイズや更新日付等を監視するための手順を記述した文書。 | 310,311,318,319 |
| | システム構成図 | 情報システム個別に作成したサーバ等の機器やソフトウェアの構成を記述した文書。 | 24,25,26,28,32,36,37,α'1,α'2,α'3,α'4,α'5,α'6,α'7,α'9,α'10,α'11,α'12,β1,β2,β3,β'1,β'2,β'3 |
| | システム仕様書等 | データの入力処理、内部処理、出力処理や画面、帳票の仕様などを記述した文書。 | 158,276,279,280,281,283 |
| | システム設計書 | システムの構成や設定などを記述した文書。 | 232,237,238,243,247,α'1,α'2,α'3,α'4,α'5,α'6,α'7,α'8,α'9,α'10,α'11,α'12,β1,β2,β3,β'1,β'2,β'3,β'5 |
| | システム設定検査記録 | システム設定ファイルの変更等の状況を検査した結果を記録した文書。 | 312 |
| | システムテスト計画書／報告書 | 導入前の総合的なテスト項目とその結果を記録した文書。 | 264,265,266,267,268,277 |
| | システム統合手順書 | 情報システムの統合・更新時の具体的な作業手順、作業結果の成否の確認方法、失敗や異常の判定方法等を記述した文書。 | 285 |
| | システム変更管理基準 | プログラムの保守等、情報システムを変更した場合の管理の基準を記述した文書。 | 282 |
| | システム変更等作業記録 | 情報システム変更等の作業に関する内容（作業時刻、変更作業内容、担当者名、作業結果、確認者等）を記録した文書。 | 155,156 |
| | 実施手順書 | 対策基準を具体的な情報システムや手順、手続に展開して個別の実施事項として記述した文書。 | 86,α'13,β6,β'8 |
| | 支給以外のパソコン等使用基準/実施手順書 | 職員等が支給以外のパソコン及び電磁的記録媒体を用いる場合の管理の基準、利用のための手順を記述した文書。 | 93,94 |
| | 支給以外のパソコン等使用申請書/承認書 | 職員等が支給以外のパソコン及び電磁的記録媒体を用いる場合に、作業の目的、内容、支給以外のパソコン及び電磁的記録媒体を用いる理由、期間等を申請し、情報セキュリティ管理者の承認を得たことを記録する文書。 | 93,94 |
| | 住民に対する広報記録 | 『広報誌』『ホームページ』『メールマガジン』『電子掲示板』等、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る窓口及び連絡手段を公表した記録。 | 126 |
| | 障害時のシステム出力ログ | 障害時にどのような事象が発生したのかを記録した文書。 | 160,164,β4,β'4 |

# 別紙3

## 監 査 資 料 例 一 覧 ／ 索 引

| 索引 | 名称 | 解 説 | 該当No. |
|---|---|---|---|
| | 障害対応基準 | 情報システム等の障害が発見された場合の対応体制、手続、手順などを記述した文書。 | 163,164 |
| | 障害報告書 | 情報システム障害等の発生経緯、発生時の状況、原因、暫定対応、恒久対策などを記録した文書。 | 34,36,37,40,44,164,176,187 |
| | 情報及びソフトウェアの交換基準 | 送主、送信、発送及び受領を通知する手順及び管理や責任範囲について記述した文書。 | 151,152 |
| | 情報及びソフトウェアの交換に関する契約書(覚書) | 他団体との間において情報やソフトウェアを交換する際の契約書や覚書。 | 152 |
| | 情報資産管理基準 | 情報資産の管理責任、分類表示、入手から廃棄までの局面ごとの取扱等の基準を記述した文書。 | 6,7,8,9,10,11,12,13,14,15,16,17,β6,β'8 |
| | 情報資産管理台帳 | 情報資産の名称、管理方法、管理責任者等の情報を記録した文書。 | 7,8,9,10,11,12,13,14,15,16,17,30,47,50 |
| | 情報資産取扱基準 | 情報資産の分類に基づく管理方法について記述した文書。 | 87 |
| | 情報資産廃棄記録 | 情報資産を廃棄した日時、担当者及び処理内容を記録した文書。 | 17 |
| | 情報資産分類基準 | 機密性・完全性・可用性に基づく情報資産の分類基準や取扱制限等を記述した文書。 | 5 |
| | 情報システム関連文書管理基準 | ネットワーク構成図や情報システム仕様書等の作成から廃棄までの管理に関わる基準を記述した文書。 | 157,158 |
| | 情報システム推進計画 | 情報システムに対する対策の推進計画の文書。 | 286 |
| | 情報システム台帳 | 情報システムの全容を把握するために必要な事項を整理した台帳。 | 7,390,394 |
| | 情報システム調達基準 | 情報システムの開発、導入、保守、機器及びソフトウェア等の調達に関わる基準を記述した文書。 | 249,271 |
| | 情報システム導入基準 | 開発環境と運用環境の分離、移行、テスト等の基準を記述した文書。 | 259,260,263 |
| | 情報システム引継書 | 情報システムの開発事業者から運用保守事業者へ引継がれる際のセキュリティ対策等の必要事項を記載した文書。 | 270 |
| | 情報セキュリティ委員会議事録 | 情報セキュリティに関する各事項を取り決める、最高情報セキュリティ責任者、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者及び情報システム管理者等で構成された委員会において討議、決定された事項について記録した文書。 | 3,113,119,344,407,410,412,413,417,419,421 |
| | 情報セキュリティ委員会設置要綱 | 構成員、会議、事務局等を規定した文書。 | 2,3 |
| | 情報セキュリティ違反時の対応手順書 | 情報セキュリティ違反の重大性、発生した事案の状況等に応じて、違反した職員等及びその監督責任者への対応手順を記述した文書。 | 354,355,356 |
| | 情報セキュリティ監査実施要綱 | 情報セキュリティ監査の計画、実施、報告等の基本的事項を記述した文書。 | 403,404,405,406,409 |
| | 情報セキュリティ監査実施マニュアル | 情報セキュリティ監査を実施する際の計画、調達、実施、報告等の手順を記述した文書。 | 403,404,405,406,407,408,409,410,411 |
| | 情報セキュリティ関連情報の通知記録 | 情報セキュリティに関連する情報について、関係者に対して通知した記録。 | 324,β5,β'6 |

# 別紙3

## 監 査 資 料 例 一 覧 ／ 索 引

| 索引 | 名称 | 解 説 | 該当No. |
|---|---|---|---|
| | 情報セキュリティ自己点検基準 | 情報セキュリティ対策が整備・運用されていることを自ら点検し、評価するための基準を記述した文書。 | 414 |
| | 情報セキュリティ自己点検実施手順書 | 情報セキュリティ対策が整備・運用されていることを自ら点検し、評価するための実施手順を記述した文書。 | 414 |
| | 情報セキュリティインシデント報告書 | 発生した情報セキュリティインシデントの発見日時、発見者、状況、業務への影響などを記録した文書。 | 124,125,127,306,311,314,315,317,335,336,337,341,342 |
| | 情報セキュリティインシデント報告手順書 | 庁内あるいは住民等外部からの情報セキュリティインシデントの報告ルートとその方法を記述した文書。 | 123,124,125,126,127,272,273,334,335,336,337,340,341,342 |
| | 情報セキュリティ水準の維持に関する手順 | 情報システムの基盤を管理又は制御するソフトウェアの情報セキュリティの維持に関する手順の文書。 | 272,273 |
| | 情報セキュリティポリシー | 組織内の情報セキュリティを確保するための方針、体制、対策等を包括的に定めた文書。 | 1,2,3,4,5,6,85,86,87,107,109,334,335,337,338,343,345,353,354,413,419,420,421,α'17,β10,β'13 |
| | 職員等への周知記録 | 首長等によって承認された決定事項や関係者で共有すべき情報等を職員等に公表・通知した文書。 | 85,108,145,189,290,323,421 |
| | 職務規程 | 職員等の職務について必要な事項を定めた文書。 | 101,102 |
| | 脆弱性関連情報の通知記録 | OSやソフトウェアの脆弱性の概要、攻撃を受けた場合の現象や対処の方法について、関係者に対して通知した記録。 | β5,β'6 |
| | 脆弱性対応計画 | OSやソフトウェアの脆弱性に対する対応計画や修正プログラムの適用計画を記述した文書。 | β5,β'6 |
| | セキュリティ機能調査結果 | 調達する機器及びソフトウェアに必要とする技術的なセキュリティ機能が組み込まれているか調査し、その結果を記録した文書。 | 251 |
| | セキュリティ情報収集基準 | セキュリティホールや不正プログラム等に関する情報を収集・周知するための基準を記述した文書。 | 320 |
| | セキュリティ設定変更基準/手続 | 機器やプログラムなどのセキュリティ設定を変更するための基準や手続を記述した文書。 | 97 |
| | セキュリティ設定変更申請書/承認書 | 所属課室名、名前、日時、変更対象物、理由、管理者の確認印等を記録した文書。 | 98 |
| | セキュリティホール関連情報の通知記録 | セキュリティホールや脆弱性に関連する情報について、関係者に対して通知した記録。 | 321 |
| | 接続許可端末一覧 | 外部から接続することを許可した端末の一覧を記録した文書。 | 242 |
| | ソーシャルメディアサービス運用手順書 | ソーシャルメディアサービスを運用する場合の手順を記述した文書。 | 216,217,218,219,220 |
| | ソースコード | プログラミング言語を用いて記述したプログラムのこと。 | 278 |

# 別紙3

## 監 査 資 料 例 一 覧 ／ 索 引

| 索引 | 名称 | 解 説 | 該当No. |
|---|---|---|---|
| | ソフトウェア管理台帳 | プログラム等のバージョンなどの情報を記録した文書。 | 274,284 |
| | ソフトウェア導入基準/手続 | ソフトウェアを導入する場合の基準や、ソフトウェアの導入許可を得るための手続を記述した文書。 | 202,203,204,205 |
| | ソフトウェア導入申請書/承認書 | 業務上必要なソフトウェアがある場合の導入許可を得るために申請し、承認する文書。 | 204 |
| た | 建物フロアレイアウト図 | 建物の各フロアの構成配列・配置を記述した文書。 | 30,51,52,53,54,55,56 |
| | 端末構成変更基準/手続 | パソコン、モバイル端末等の機器構成を変更する基準や、パソコン、モバイル端末等の機器構成を変更する場合の手続を記述した文書。 | 206,207,208 |
| | 端末構成変更申請書/承認書 | パソコン、モバイル端末等に対し機器の改造及び増設・交換の必要がある場合に許可を得るために申請し、承認する文書。 | 208 |
| | 端末接続時手続 | 外部から持ち込んだ端末を庁内ネットワークに接続する際に実施すべき手続を記述した文書。 | 240,241 |
| | 端末等セキュリティ設定変更基準/手続 | パソコン、モバイル端末等のソフトウェアに関するセキュリティ機能の設定を変更する基準や、セキュリティ機能の設定を変更する場合の手続を記述した文書。 | 97 |
| | 端末等持出・持込基準/手続 | パソコン、モバイル端末や情報資産を庁外に持ち出す場合の基準や、庁外に持ち出す場合の許可を得る手続を記述した文書。 | 89,90,92,95,96 |
| | 端末等持出・持込申請書/承認書 | 職員等がパソコン、モバイル端末及び電磁的記録媒体、情報資産及びソフトウェアを持ち出す場合又は持ち込む場合に、所属課室名、名前、日時、持出/持込物、個数、用途、持出/持込場所、持ち帰り日/返却日、管理者の確認印を記録した文書。 | 90,96 |
| | 端末ログ | 端末の利用状況や操作内容を記録した文書。 | 88,316 |
| | 庁外機器設置申請書／承認書 | 庁外に機器を設置するにあたり、最高情報セキュリティ責任者の承認を得るために申請する文書。 | 47 |
| | 庁外作業申請書/承認書 | 職員等が外部で情報処理作業を行う場合に、作業の目的、内容、期間等を申請し、情報セキュリティ管理者の承認を得たことを記録する文書。 | 91 |
| | 庁外での情報処理作業基準/手続 | 職員等が外部で情報処理作業を行う場合のパソコン、モバイル端末等の持ち出しや庁外で作業する際の注意事項、支給以外のパソコンの使用制限などの基準及び外部で情報処理作業を行う場合の申請や承認などの手続を記述した文書。 | 89,90,91,94 |
| | 調達仕様書 | 調達する情報システムの要件、機能、必要となるセキュリティ機能等の仕様を記述した文書。 | 250,251,269,384,385 |
| | 通信回線敷設図 | 庁内の通信回線の敷設状況を図に表した文書。 | 175 |
| | 通信ケーブル等配線基準/手続 | 電源ケーブルや通信ケーブルを損傷等から保護するための配線基準やネットワーク接続口（ハブのポート等）の設置基準、及び配線や設置に関わる申請や変更・追加等の手続を記述した文書。 | 38,39,40,41,42 |
| | 通信データ暗号化基準 | 通信データの暗号化の要否、利用する暗号方式や鍵の管理など、通信データの暗号化に関する基準を記述した文書。 | 333 |
| | 通信データ監視基準 | 通信データの監視の要否に関する基準を記述した文書。 | 333 |
| | 通知書 | 情報セキュリティポリシーに違反する行動等が確認された場合、関係者に改善のための指示を通知する文書。 | 211,317,355,356 |

# 別紙3

## 監 査 資 料 例 一 覧 ／ 索 引

| 索引 | 名称 | 解 説 | 該当No. |
|---|---|---|---|
| | 電子署名・暗号化利用基準 | 電子署名付与や暗号化実施条件など、電子署名・暗号化の利用に関わる基準を記述した文書。 | 198,199,200,201 |
| | 電子メール管理基準 | 電子メール転送禁止や送受信容量制限、業務外利用禁止など、電子メールの運用・管理に関わる基準を記述した文書。 | 185,186,187,188,189,190,191 |
| | 電子メール送受信ログ | 電子メールの送受信が行われた日時や送受信データの内容などを記録した文書。 | 88,193,194,195 |
| | 電子メール利用基準 | 電子メールを送受信する場合の基準を記述した文書。 | 87,106,192,193,194,195,196,197,302 |
| | 同意書 | 情報セキュリティポリシー等を遵守することを誓約し、署名あるいは記名捺印した文書。 | 105 |
| | 統合時影響検討書 | 情報システムの統合・更新を実施した場合に想定される影響範囲と影響の大きさ及びその対処方針について、検討した結果を記述した文書。 | 285 |
| | 特定用途機器管理基準 | 特定用途機器のセキュリティ設定等の基準を記述した文書。 | 181 |
| | 特定用途機器管理手続 | 特定用途機器を運用する際の具体的な手続きを記述した文書。 | 181 |
| | 特権ID・パスワード変更記録 | 特権IDや特権IDのパスワードの変更したことを記録した文書。 | 232 |
| | 特権ID管理台帳 | 特権IDの付与情報を記録した文書。 | 226,227 |
| | 特権ID取扱手続 | 特権IDの取扱い（登録、変更、抹消等）の認可手続や、パスワードの管理について記述した文書。 | 226,227,228,231,232,233 |
| | 特権ID認可申請書 | 特権ID利用の許可を得るため申請を記録した文書。 | 226 |
| | 特権代行者承認書 | 統括情報セキュリティ責任者及び情報システム管理者の特権を代行者を最高情報セキュリティ責任者が承認したことを記録した文書。 | 229 |
| | 特権代行者通知書 | 統括情報セキュリティ責任者及び情報システム管理者の特権を代行する者を関係者に通知したことを記録した文書。 | 230 |
| な | 認証用カード管理記録 | 入退管理システムで使用する認証用カードの発行状況を記録した文書。 | 58 |
| | ネットワーク管理基準 | ネットワークにおけるデータのセキュリティを確保するための体制、責任、ネットワークに接続したサービスを無認可のアクセスから保護するための基準等、ネットワークの運用、変更などに関する基準を記述した文書。 | 18,19,23,24,65,66,67,68,69,70,71,72,73,74,75,106,169,170,175,182,183,184,312 |
| | ネットワーク管理記録 | ネットワーク管理基準に従って実施した管理作業の実施日、実施者、実施内容等について記録した文書。 | 309 |
| | ネットワーク構成図 | ネットワークの構成を論理的や物理的に記述した文書。 | 166,309 |
| | ネットワーク設計書 | ネットワークの構成や設定などを記述した文書。 | 183,184,232,237,238,242,247 |
| | ネットワーク設定基準 | 個々のネットワーク毎に、どのような通信経路を介して、接続するのかなどを記述した文書。 | 165,166,167,168 |
| | ネットワーク利用基準 | 庁内ネットワークやインターネットを利用する場合の基準を記述した文書。 | 87,209,210,211 |

# 別紙3

## 監 査 資 料 例 一 覧 ／ 索 引

| 索引 | 名称 | 解 説 | 該当No. |
|---|---|---|---|
| | 納入時の確認・検査手続 | 機器等の納入時における確認、検査手続の文書。 | 248 |
| は | パスワード管理基準 | パスワードの選択や変更等、管理の基準を記述した文書。 | 137,138,139,140,141,142,143 |
| | パソコン等管理基準 | パソコン、モバイル端末等の盗難防止対策やパスワード設定、データ暗号化等の基準を記述した文書。 | 20,21,22,76,77,78,79,80,81,82,83,84 |
| | バックアップ基準 | ファイルサーバ等の故障等に備えて実施しておくべきバックアップの基準について記述した文書。 | 148,149,150 |
| | バックアップ実施記録 | バックアップを行った内容（媒体識別番号、実施日時、作業者名、範囲（フルバック、差分バックアップなど））等を記録した文書。 | 149,150 |
| | バックアップ手順書 | バックアップの実施方法や実施間隔、バックアップ媒体の保管方法等について記述した文書。 | 148,149,150 |
| | パッチ適用記録 | パッチをソフトウェアに適用した結果を記録した文書。 | 322 |
| | パッチ適用情報 | セキュリティホールや不正プログラム等に対するパッチの適用情報を記録した文書。 | 322 |
| | 非常勤及び臨時職員への対応基準 | 非常勤及び臨時職員の情報セキュリティポリシー遵守、同意書への署名、インターネット接続及び電子メール使用等の制限などに関する基準について記述した文書。 | 103 |
| | ファイアウォール設定 | ネットワークを分離するために設置したファイアウォールの設定やアクセス制御のためのルール、ポートなどの制御に関するルール等を記述した文書。 | 309 |
| | ファイアウォールログ | 内部から外部ネットワーク、外部から内部ネットワークへの通信が行われた日時や利用したサービス（メール、web等）等を記録した文書。 | 88,309 |
| | 複合機管理基準 | 複合機のセキュリティ設定やデータ抹消等の基準を記述した文書。 | 177,178,179,180 |
| | 複合機管理手続 | 複合機を調達し、運用する際の具体的な手続を記述した文書。 | 177,178,179,180 |
| | 不正アクセス対応手順書 | アクセス制御の導入やIDS,IPSの導入等の手順を記述した文書。 | 308,310,311,318,319 |
| | 不正アクセス対策基準 | 悪意の第三者等の不正アクセスから情報資産を保護するためのアクセス制御の導入や、IDS、IPSなどの導入等の基準を記述した文書。 | 308,310,311,318,319 |
| | 不正プログラム対策基準 | コンピュータウイルスやスパイウェア等の不正プログラムから情報資産を保護するための不正プログラム対策ソフトウェアの導入や定期的なパターンファイル・ソフトウェアのバージョン更新等の基準を記述した文書。 | 287,288,289,290,291,292,293,294,295,296,297,298,299,300,301,302,303,304,305,306,307 |
| | 不正プログラム対策ソフトウェアのログ | 不正プログラム対策ソフトウェアでファイル等をチェックした結果を記録した文書。 | 288,289,292,293,296,297,298,299,300,301,303,304 |
| | 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導入や定期的なパターンファイル・ソフトウェアのバージョン更新等の手順を記述した文書。 | 287,288,289,290,291,292,293,294,295,296,297,298,299,300,301,302,303,304,305,306,307 |

# 別紙3

## 監 査 資 料 例 一 覧 ／ 索 引

| 索引 | 名称 | 解 説 | 該当No. |
|---|---|---|---|
| | プログラム仕様書等 | システム仕様書に基づいてプログラムを開発する際の具体的な仕様を記述した文書。 | 158,276,279,280,281,283 |
| | 文書サーバ設定基準 | 文書サーバの容量や構成、アクセス制御などの設定基準について記述した文書。 | 144,145,146,147 |
| | 返却／廃棄・抹消証明 | 委託業務の終了時に委託事業者において取り扱われた情報が確実に返却、廃棄又は抹消されたことを確認する文書等。 | 363,364 |
| | 他の組織との間の情報及びソフトウェアの交換に関する申請書 | 他団体との間において情報やソフトウェアの交換の許可を得るため申請する文書。 | 152 |
| | 保守機器管理表 | 保守対象機器、保守実施時期、保守内容、保守担当等を一覧表などで記述した文書。 | 44,45 |
| | 保守体制図 | 当該機器の保守依頼の受付窓口や担当者等、体制を記述した文書。 | 27,44,45 |
| や | ユーザテスト計画書／報告書 | 業務に精通している利用部門による操作確認のテスト項目とその結果を記録した文書。 | 265,266 |
| ら | リストア手順書 | 情報システムを正常に再開するためのバックアップ媒体から情報を元に戻す手順を記述した文書。 | 148,149,150 |
| | リストアテスト記録 | バックアップ媒体から正常に情報を元に戻せるかどうかを検証した結果を記録した文書。 | 149,150 |
| | リモートアクセス方針 | 外部から内部のネットワーク又は情報システムへのアクセスに対する方針を記述した文書。 | 234 |
| | リモート接続許可申請書／許可書 | リモート接続の申請と許可を記録した文書。 | 235,236 |
| | リモート接続手続 | 外部から内部のネットワークへ接続する具体的な手続を記述した文書。 | 234,239 |
| | 利用者ID管理台帳 | 利用者IDの付与情報を記録した文書。 | 222,223,224,225 |
| | 利用者ID棚卸記録 | 利用者IDの登録状況及びアクセス権の付与状況を定期的に確認したことを記録した文書。 | 225 |
| | 利用者ID登録・変更・抹消申請書 | 利用者IDを登録、変更又は抹消の申請を記録した文書。 | 222,223,224 |
| | 利用者ID取扱手続 | 利用者IDの取り扱い（登録、変更、抹消等）の認可手続きやパスワードの管理について記述した文書。 | 222,245,246 |
| | 利用状況調査基準 | 職員等の使用しているパソコン、モバイル端末及び電磁的記録媒体のログ、電子メールの送受信記録等の利用状況の調査に関する基準を記述した文書。 | 338 |
| | 利用状況調査結果 | 職員等が使用しているパソコン、モバイル端末及び電磁的記録媒体のログ、電子メールの送受信記録等の利用状況を調査した結果を記録した文書。 | 339 |
| | 例外措置実施報告書 | 許可を得て実施した例外措置の内容を記録した文書。 | 348,349,350 |
| | 例外措置申請書/許可書 | 情報セキュリティ関係規定を遵守することが困難な理由を説明し、最高情報セキュリティ責任者に例外措置を採ることの許可を申請し、許可されたことを記録した文書。 | 348,350 |
| | 例外措置対応基準/手続 | 情報セキュリティ関係規定の遵守が困難な状況で行政事務の適正な遂行を継続しなければならない場合の対応基準や、例外措置の実施について申請、審査、許可に関する手続を記述した文書。 | 347 |

# 別紙3

監 査 資 料 例 一 覧 ／ 索 引

| 索引 | 名称 | 解 説 | 該当No. |
|---|---|---|---|
| | ログ | 情報システムにアクセスした日時、アクセスしたID、アクセス内容等を記録した文書。 | 160,315,β4,β'4 |
| | ログイン画面 | 情報システムのログイン認証の画面。 | 243 |

別紙3

# 情報セキュリティ監査
# 実施要綱（例）

情報セキュリティ監査実施要綱（例）

第１章　総　則

（目　的）

第１条　この要綱は、○○○市における情報セキュリティ監査に関する基本的事項を定め、本市の情報セキュリティの維持・向上に資することを目的とする。

（監査対象）

第２条　情報セキュリティ監査は、○○○市情報セキュリティポリシーに定める行政機関を対象に実施する。

（監査実施体制）

第３条　情報セキュリティ監査は、○○○室が担当する。

２　情報セキュリティ監査は、情報セキュリティ監査統括責任者が指名する監査人によって実施する。

３　外部監査を行う場合は、外部監査人の選定基準に基づき、客観的で公平な手続きに従って調達を行い、外部の専門家により情報セキュリティ監査を実施する。

（監査の権限）

第４条　監査人は、情報セキュリティ監査の実施にあたって被監査部門に対し、資料の提出、事実などの説明、その他監査人が必要とする事項の開示を求めることができる。

２　被監査部門は、前項の求めに対して、正当な理由なくこれを拒否することはできない。

３　監査人は、委託先など業務上の関係先に対して、事実の確認を求めることができる。

４　監査人は、被監査部門に対して改善勧告事項の実施状況の報告を求めることができる。

（監査人の責務）

第５条　監査人は、監査を客観的に実施するために、監査対象から独立していなければならない。

２　監査人は、情報セキュリティ監査の実施にあたり、常に公正かつ客観的に監査判断を行わなければならない。

３　監査人は、監査及び情報セキュリティに関する専門知識を有し、相当な注意をもって

監査を実施しなければならない。
4　監査報告書の記載事項については、情報セキュリティ監査統括責任者及び監査人がその責任を負わなければならない。
5　情報セキュリティ監査統括責任者及び監査人は、業務上知り得た秘密事項を正当な理由なく他に開示してはならない。
6　前項の規定は、その職務を離れた後も存続する。

（監査関係文書の管理）
第６条　監査関係文書は、紛失等が発生しないように適切に保管しなければならない。

第２章　監査計画
（監査計画）
第７条　情報セキュリティ監査は、原則として監査計画にもとづいて実施しなければならない。
２　監査計画は、中期計画、年度計画及び監査実施計画とする。

（中期計画及び年度計画）
第８条　情報セキュリティ監査統括責任者は、中期の監査基本方針を中期計画として策定し、情報セキュリティ委員会の承認を得なければならない。
２　情報セキュリティ監査統括責任者は、中期計画にもとづき、当該年度の監査方針、監査目標、監査対象、監査実施時期、監査要員、監査費用などを定めた年度計画を策定し、情報セキュリティ委員会の承認を得なければならない。

（監査実施計画）
第９条　情報セキュリティ監査統括責任者は、年度計画にもとづいて、個別に実施する監査ごとに監査実施計画を策定し、情報セキュリティ委員会の承認を得なければならない。
２　特命その他の理由により、年度計画に記載されていない監査を実施する場合も、監査実施計画を策定しなければならない。

第３章　監査実施
（監査実施通知）
第１０条　情報セキュリティ監査統括責任者は、監査実施計画にもとづく監査の実施にあたって、原則として○週間以上前に被監査部門の情報セキュリティ管理者に対し、監

査実施の時期、監査日程、監査範囲、監査項目などを文書で通知しなければならない。
2　ただし、特命その他の理由により、事前の通知なしに監査を実施する必要性があると判断した場合には、この限りではない。

（監査実施）
第１１条　監査人は、監査実施計画にもとづき、監査を実施しなければならない。ただし、特命その他の理由によりやむを得ない場合には、情報セキュリティ監査統括責任者の承認を得てこれを変更し実施することができる。

（監査調書）
第１２条　監査人は、実施した監査手続の結果とその証拠資料など、関連する資料を監査調書として作成しなければならない。

（監査結果の意見交換）
第１３条　監査人は、監査の結果、発見された問題点について事実誤認などがないことを確認するため、被監査部門との意見交換を行わなければならない。

第４章　監査報告
（監査結果の報告）
第１４条　情報セキュリティ監査統括責任者は、監査終了後、すみやかに監査結果を監査報告書としてとりまとめ、情報セキュリティ委員会に報告しなければならない。ただし、特命その他の理由により緊急を要する場合は口頭をもって報告することができる。
2　監査報告書の写しは、必要に応じて、被監査部門の情報セキュリティ管理者に回覧又は配付する。
3　情報セキュリティ監査統括責任者は、被監査部門に対して監査報告会を開催しなければならない。

（監査結果の通知と改善措置）
第１５条　最高情報セキュリティ責任者は、情報セキュリティ委員会への監査結果報告後、すみやかに監査結果を被監査部門の情報セキュリティ管理者に通知しなければならない。
2　前項の通知を受けた被監査部門の情報セキュリティ管理者は、改善勧告事項に対する改善実施の可否、改善内容、改善実施時期などについて、最高情報セキュリティ責任者に回答しなければならない。
3　情報セキュリティ委員会は、監査結果を情報セキュリティポリシーの見直し、その他

情報セキュリティ対策の見直し時に活用しなければならない。

（フォローアップ）

第１６条　情報セキュリティ監査統括責任者は、被監査部門における改善勧告事項に対する改善実施状況について、適宜フォローアップしなければならない。

２　前項による確認結果については、適宜とりまとめ、情報セキュリティ委員会に報告しなければならない。

以　上

別紙3

# 情報セキュリティ監査
# 実施計画書（例）

**別紙3**

# 情報セキュリティ監査実施計画書（例）

令和○○年○○月○○日

| | | |
|---|---|---|
| 1 | 監査目的 | ○○業務に関して、情報資産の管理体制が適切に確立されているか確認する。 |
| 2 | 監査テーマ | 庁内設備を利用するに当たって、内外の脅威に対する情報セキュリティ対策が行われているか確認する。 |
| 3 | 監査範囲 | ○○業務<br>○○情報システム |
| 4 | 被監査部門 | ○○○○課（情報システム所管課）<br>○○○○課（原課） |
| 5 | 監査方法 | ア. 規程類、記録類の確認<br>イ. 情報システム、マシン室及び執務室の視察<br>ウ. 職員へのアンケート調査及びヒアリング |
| 6 | 監査実施日程 | 令和○○年○○月○○日～　令和○○年○○月○○日 |
| 7 | 監査実施体制 | 情報セキュリティ監査統括責任者　○○○○<br>監査人　○○○○<br>監査人　○○○○ |
| 8 | 監査項目 | アクセス制御<br>不正プログラム対策<br>不正アクセス対策 |
| 9 | 適用基準 | ・○市 情報セキュリティポリシー<br>・○○○実施手順書 |

別紙3

# 情報セキュリティ監査
# 報告書(例)

**別紙3**

# 情報セキュリティ監査報告書（例）

令和○○年○○月○○日

| | | |
|---|---|---|
| 1 | 監査目的 | ○○業務に関して、情報資産の管理体制が適切に確立されているか確認する。 |
| 2 | 監査テーマ | 庁内設備を利用するに当たって、内外の脅威に対する情報セキュリティ対策が行われているか確認する。 |
| 3 | 監査範囲 | ○○業務、○○情報システム |
| 4 | 被監査部門 | ○○○○課（情報システム所管課）、○○○○課（原課） |
| 5 | 監査方法 | ア．規程類、記録類の確認<br>イ．情報システム、マシン室及び執務室の視察<br>ウ．職員へのアンケート調査及びヒアリング |
| 6 | 監査実施日程 | 令和○○年○○月○○日～　令和○○年○○月○○日 |
| 7 | 監査実施体制 | 情報セキュリティ監査統括責任者　○○○○<br>監査人　○○○○<br>監査人　○○○○ |
| 8 | 監査項目 | アクセス制御<br>不正プログラム対策<br>不正アクセス対策 |
| 9 | 適用基準 | ・○市 情報セキュリティポリシー<br>・○○○実施手順書 |

**１.総括**

××××××××××××××××××××××××××××××××××××××××

**（１）アクセス制御**

**①**××××××××××

**【監査結果】**

××××××××××××××××××××××××××××××××××××××××

**【指摘事項】**

××××××××××××××××××××××××××××××××××××××××

**【改善案】**

××××××××××××××××××××××××××××××××××××××××

**（２）不正プログラム対策**

**①**××××××××××

・
・

別紙3

# 情報セキュリティ監査業務委託仕様書（例）

# 別紙3

情報セキュリティ監査業務委託仕様書（例）

1　業務名

○○市情報セキュリティ監査業務

2　監査目的

本業務は、○○市の情報セキュリティポリシーに基づき実施している情報資産の管理、各種情報システムの保守・運用、職員研修等の情報セキュリティ対策について、第三者による独立かつ専門的な立場から、基準等に準拠して適切に実施されているか否かを点検・評価し、問題点の確認、改善方法等についての検討、助言、指導を行うことによって、○○市の情報セキュリティ対策の向上に資することを目的とする。

3　発注部署

○○市△△部□□課　　担当者：
連絡先〒XXX-XXXX　　○○市××
電話番号：0XXX-XX-XXXX　　FAX：0XXX-XX-XXXX

4　監査対象

○○市行政LAN/WAN上の情報システムを対象とする（具体的な範囲は、別に受託者に指示することとし、個別ネットワークについては、監査対象に含まない。）。

5　業務内容

「地方公共団体情報セキュリティ監査ガイドライン」を基に、○○市の実情にあった監査項目を抽出して、助言型監査を実施すること。なお、技術的検証の実施も含まれることに留意する。

6　適用基準

(1)必須とする基準

ア　○○市情報セキュリティポリシー（基本方針及び対策基準）
イ　○○市△△情報システム実施手順書

(2)参考とする基準

ア　○○市情報セキュリティ監査実施要綱
イ　○○市個人情報保護法施行条例
ウ　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（総務省）
エ　地方公共団体における情報セキュリティ監査に関するガイドライン（総務省）
オ　上記のほか委託期間において情報セキュリティに関し有用な基準等で、○○市と協議して採用するもの

7　監査人の要件

(1)受託者は情報セキュリティサービス基準適合サービスリスト(うちセキュリティ監査サービスに係る部分）に登録されていること。

(2)受託者はISO/IEC27001(JIS Q 27001)認証又はプライバシーマーク認証を取得していること。

(3)監査責任者、監査人、監査補助者、アドバイザー等で構成される監査チームを編成すること。

(4)監査の品質の保持のため監査品質管理責任者、監査品質管理者等の監査品質管理体制をつくること。

(5)監査チームには、情報セキュリティ監査に必要な知識及び経験（地方公共団体における情報セキュリティ監査の実績）を持ち、次に掲げるいずれかの資格を有する者が１人以上含まれていること。

ア　システム監査技術者
イ　公認情報システム監査人（CISA）
ウ　公認システム監査人
エ　ISMS 主任審査員
オ　ISMS 審査員
カ　公認情報セキュリティ主任監査人
キ　公認情報セキュリティ監査人

(6)監査チームには、監査の効率と品質の保持のため次のいずれかの実績（実務経験）を有する専門家が１人以上含まれていること。

ア　情報セキュリティ監査
イ　情報セキュリティに関するコンサルティング
ウ　情報セキュリティポリシーの作成に関するコンサルティング（支援を含む）

(7)監査チームの構成員が、監査対象となる情報資産の管理及び当該情報資産に関する情報システムの企画、開発、運用、保守等に関わっていないこと。

8　監査期間

令和○○年○○月○○日～令和○○年○○月○○日

9　監査報告書の様式

(1)監査報告書の作成様式

ア　Ａ４版縦（必要に応じてＡ３版三つ折も可。Ａ３版三つ折の場合、両面印刷は不可とする。）とし、様式は任意とする。
イ　監査報告書は監査対象についての脆弱点を網羅した非公開の「監査報告書(詳細版)」と公開を前提とした「監査報告書(公開版)」の２種類を作成し、提出すること。

(2)監査報告書の宛名

１部を「○○市長」宛てとし、他を「最高情報セキュリティ責任者」宛てとする。

１０　監査報告書の提出先

○○市△△部□□課とする。

１１　監査報告会

監査対象となった課室の長及び情報セキュリティ責任者、情報システム管理者に対して、監査結果の報告会を実施すること。

１２　監査成果物と納入方法

下記に掲げる監査成果物を書面（Ａ４版縦を基本とし、必要に応じてＡ３版三つ折も可。Ａ３版三つ折の場合、両面印刷は不可とする。）及び電子媒体（CD-R）にて、必要数を提出すること。

(1)監査成果物

ア　監査実施計画書　２部

イ　情報セキュリティ監査報告書（詳細版）　２部

ウ　情報セキュリティ監査報告書（公開版）　２部

(2)納品方法

ア　紙媒体　上記のとおり

イ　電子媒体　１部

１３　成果物の帰属

成果物及びこれに付随する資料は、全て○○市に帰属するものとし、書面による○○市の承諾を受けないで他に公表、譲渡、貸与又は使用してはならない。ただし、成果物及びこれに付随する資料に関し、受託者が従前から保有する著作権は受託者に留保されるものとし、○○市は、本業務の目的の範囲内で自由に利用できるものとする。

１４　委託業務の留意事項

業務の実施にあたっては、以下の事項に留意する。

(1)監査実施計画書の提出

契約締結後、受託者は監査実施計画書を提出し、市及び受託者の協議により委託業務の詳細内容及び各作業の実施時期を決定するものとする。

(2)資料の提供等

本業務の実施にあたり、必要な資料及びデータの提供は○○市が妥当と判断する範囲内で提供する。

なお、受託者は、○○市から提供された資料は適切に保管し、特に個人情報に係るもの及び情報システムのセキュリティに係るものの保管は厳格に行うものとする。また、契約終了後は本件監査にあたり収集した一切の資料を速やかに○○市に返還し、又は破棄するものとする。

(3)技術的検証

技術的検証については、対象情報システム及び行政 LAN/WAN の運用に対し、支障及び損害を与えないように実施するものとする。

(4)再委託

受託者は、本業務の実施にあたり他の業者に再委託することを原則、禁止する。再委託が必要な場合は、○○市と協議の上、事前に書面により○○市の承認を得ること。

(5)秘密保持等

受託者は本業務の実施にあたり、知り得た情報及び成果品の内容を正当な理由なく他に開示し又は自らの利益のために利用してはならない。これは、契約終了後又は契約解除後においても同様とする。

(6)議事録等の作成

受託者は、本業務の実施にあたり○○市と行う会議、打ち合わせ等に関する議事録を作成し、○○市にその都度提出して内容の確認を得るものとする。

(7)関係法令の遵守

受託者は業務の実施にあたり、関係法令等を遵守し業務を円滑に進めなければならない。

(8)報告等

受託者は作業スケジュールに十分配慮し、○○市と密接に連絡を取り業務の進捗状況を報告するものとする。

１５　その他

本業務の実施にあたり、本仕様書に記載のない事項については○○市と協議の上決定するものとする。

以　上

別紙3

# 情報セキュリティ監査業務委託契約書（例）

# 別紙3

情報セキュリティ監査業務委託契約書（例）

自治体　　甲：
事業者　　乙：
（完成保証人　丙：　　）

委託業務名　　：○○市情報セキュリティ監査業務委託

履行場所　　：○○市○○

履行期限　　自　令和○○年○○月○○日
　　至　令和○○年○○月○○日

甲は、乙と、下記のとおり頭書情報セキュリティ監査業務委託契約を締結し、その契約の証として、本書2通（完成保証人がある場合は3通）を作成し、当事者記名の上これを保有する。

第1条（総則）
甲と乙は、以下の内容の請負契約※1を締結する。
1　名　　称　○○市情報セキュリティ監査業務
2　業務の内容※2
別紙業務委託仕様書※3第2項、第4項から第6項まで、第9項から第12項まで記載のとおり、乙が管理する監査チームの監査従事者が、甲の情報セキュリティ監査統括責任者に対し、監査時期において、監査の目的に従い、監査対象を適用基準に照らして評価することを含む監査範囲の監査を行い、その結果を記載した監査報告書を含む監査成果物を定められた納品方法により提出すること。
①監査チームの構成及び監査従事者　別紙監査従事者名簿※4記載のとおり。
②監査時期　　別紙業務委託仕様書第8項記載のとおり。
③監査の目的　　同　　第2項記載のとおり。
④監査対象　　同　　第4項記載のとおり。
⑤業務範囲　　同　　第5項記載のとおり。
⑥適用基準　　同　　第6項記載のとおり。
⑦成果物と納品方法　　同　　第9から12項まで記載のとおり。
⑧成果物の提出期限　令和○○年○○月○○日
⑨評価の基準日　　令和○○年○○月○○日
3　代金及び支払いの時期
xxx万円（監査に要する一切の経費を含む（消費税及び地方消費税込））
支払日：令和○○年○○月○○日

※1　監査契約を請負契約とするものと準委任契約とするものがあり得るが、本件監査では実務上多く存在する請負契約とした。ただし、監査契約が請負契約か準委任契約かその混合契約かの争いを防止するため、請負契約であることを明記した。

※2　仕事の内容のうち、明示されていない事項については、「仕事の内容につき本契約書に明記されていない事項及び本契約書の記載内容に解釈上の疑義を生じた場合には甲乙が協議して定める」という一項を入れることもある。さらに、監督員（地方自治法施行令第

167 条の 15 第 4 項の規定に基づき監督を委託された者をいう）がいる場合は、「ただし軽微なものについては、甲又は監督員の指示に従うものとする。」というただし書きをつける場合もある。

※3　情報セキュリティ監査業務委託仕様書（例）を参照のこと。なお、業務委託仕様書と異なるときはその内容を記載する。

※4　監査従事者名簿は、本件監査に従事する者を特定することにより、監査の品質を裏付けるとともに、監査に関して問題が発生したときの責任の追及を容易にするためのものであるから、監査主体における地位（監査責任者、監査補助者等の監査主体における組織統制上の位置を明らかにする事項）、氏名、生年月日、住所、連絡先、資格などを記載する。記載内容が詳細にわたるため、契約書とは別に監査従事者名簿を作成する。

第２条（監査人の権限）
　乙は、甲に、本契約に定めるセキュリティ監査（以下「本件監査」という。）を実施するため甲に具体的な必要性を説明して、相当な方法をもって、以下の行為を行うことができる。
　１　甲の所有・管理する場所に存する各種の文書類及び資料類の閲覧、収集。
　２　甲の役職員に対する質問及び意見聴取。
　３　甲の施設の現地調査。
　４　監査技法を適用するためのコンピュータ機器の利用。
　５　本件監査の監査報告書を決定する前における乙との意見交換。

第３条（品質管理）※5
　乙は、監査結果の適正性を確保するために、別に定める品質管理を行う。

※5　品質管理の具体例としては、監査人要件、技術的検証の内容、監査ツール、監査結果の管理方法その他が考えられる。監査品質は監査結果とコストに影響するため、その内容を具体的に定めるときは契約時にその内容、方法及び評価の方法を具体的に特定しておくことが望ましい。ただし、その内容には実情に応じて定めるべきであり、契約書例では「別に定める」としている。

第４条（注意義務）※6
　乙は、職業倫理に従い専門職としての相当の注意と○○団体が定めた倫理規則を遵守して誠実に本件監査を実施し、監査従事者全員をして乙の義務を履行させる。

※6　地方公共団体の情報セキュリティ監査には、高い公益性が認められるため、その注意義務の内容は、請負人の一般的な注意義務や善良なる管理者の注意義務以上の厳格なものであるべきである。そこで本条を設けた。契約にあたっては、乙が所属し倫理規範を設けている団体の名称を○○に挿入する。

第５条（監査人の責任）※7
　１　乙は、監査対象事実と適用基準との乖離の有無と程度、その助言の内容を実施することによって乖離の程度が縮小するとの意見を表明する。
　２　乙は、前項の意見が、前条に定める注意義務に照らして合理的に導かれた乙の評価に基づくことについて責任を負う。

※7　第１項は、助言型監査の場合の文例である。保証型監査の場合は、「乙は、監査対象事実と適用基準との乖離の有無の判断を内容とする意見を表明する」となる。

第６条（機密保持）
　乙と監査従事者は、本件監査を行うに際して知り得た秘密※8及び個人情報を正当な理

由なく他に開示し又は自らの利益のために利用してはならない。なお、この契約が終了又は解除された後においても同様とする。

※8　守秘義務の対象を、「秘密」とするときは、乙の契約違反の責任を追及する場合に甲が秘密として管理していることの立証に成功する必要がある。「事実」とするときは、およそ全ての事実であり、甲がこれを秘密として管理していたか否かを問わないし、甲はその立証をする必要はない。なお、特に、個人情報については、地方公共団体の個人情報保護法施行条例においても、個人データの委託先に対して、安全管理のための必要な監督を行う義務を負うことが規定されることが多いため、個人情報については特に守秘条項を記載した。

第７条（監査の手順）
　乙は、監査計画に基づき、予備調査、本調査及び評価・結論の手順により本件監査を実施する。

第８条（監査実施計画書の提出・承認）
　乙は、甲に、予備調査後速やかに※9 以下の事項を含む本件監査の手順及びその実施時期を具体的に記載した監査実施計画書を提出して甲の承認を得た後でなければその後の手順を行ってはならない。なお、乙は、本件監査の目的を達するため、監査実施計画書を、監査の進行に伴い、甲と協議して変更することができる。
１　本調査実施方法の要領
２　調査実施場所毎の監査従事者
３　調査実施場所毎の調査時期
４　収集する監査証拠の範囲
５　監査証拠の収集方法
６　特段の評価方法があるときはその旨
７　評価の日
８　監査の協議の日時・内容
９　監査結果の報告の日時・内容
１０　その他本件監査に必要な事項

※9　具体的な日時を記載することが望ましい

第９条（監査調書の作成と保存）
１　乙は、本件監査を行うにあたり監査調書を作成する。
２　乙は、甲に、監査報告に際し、監査調書及び乙が本件監査にあたり収集した一切の物及び電磁的記録を引き渡し、それらに対する所有権、著作権その他一切の権利を放棄する。

第１０条（監査報告書の記載事項）
　乙は、監査報告書に、実施した監査の対象、監査の内容、証拠に裏付けられた合理的な根拠に基づく意見※10、制約又は除外事項、その他本件監査の目的に照らして必要と判断した事項を明瞭に記載する。

※10　監査報告書は、監査証拠に裏付けられた合理的な根拠に基づくものであることを要する。したがって監査報告書中に、監査意見に至った根拠とそれを導く証拠が記載され、これを第三者が評価できるように整然と、かつ明瞭に記載することが望ましい。

第１１条（監査報告書の開示）
甲は、乙から提出された成果物を、第三者に開示することができる。※11

※11　成果物の開示については、甲乙間でその手続、条件を定めることもある。その際の監査契約書の記載例としては、「甲は、乙の事前の承認を得て、本件監査の成果物を第三者に開示することができる。手続、条件は別途協議して定める」という記載が考えられる。

第１２条（改善指導）
乙は、監査結果に基づいて、別に定めるところにより改善指導を行う。

第１３条（解除）
甲が第１条により乙に支払うべき金員を支払わないときは、乙は、本件監査に関して保管中の書類その他のものを甲に引き渡さないでおくことができる。

第１４条（紛争）
本件に関する紛争は、他に法令の定めがない限り、●●地方裁判所を唯一の第一審合意管轄裁判所とする。

第１５条（その他）
１　本契約に定めのない事項については別添契約約款により、そのいずれにも定めのない事項は甲乙協議して定める。
２　なお、本契約のうち法令に反する部分は無効であり、他の契約又は約款のうち、本契約に反する部分は無効とする。

令和〇〇年〇〇月〇〇日

甲

乙

丙

以　上