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(平成30年9月版)

> 平成15年12月25日 策 定 平成30年 9月25日 改 定

> > 総 務 省

### 目 次

第1章 総則	2
1.1. 本ガイドラインの目的	2
1.2. 本ガイドライン策定の経緯	
1.3. 情報セキュリティ監査の意義と種類	
1.4. 本ガイドラインとポリシーガイドラインの関係	
1.5. 本ガイドラインの構成	
第2章 情報セキュリティ監査手順	
2.1. 監査手順の概要	11
2.2. 監査手順	12
2.2.1. 準備	12
2.2.2. 監査計画	16
2.2.3. 監査実施	18
2.2.4. 監査報告	22
2.2.5. 監査結果への対応等	24
2.2.6. 監査結果の公開	25
2.2.7. フォローアップ監査	26
2.3. 外部監査人の調達	27
第3章 情報セキュリティ監査項目	32
3.1. 組織体制	34
3.2. 情報資産の分類と管理	
3.3. 情報システム全体の強靭性の向上	37
3.4. 物理的セキュリティ	39
3.4.1. サーバ等の管理	
3.4.2. 管理区域(情報システム室等)の管理	44
3.4.3. 通信回線及び通信回線装置の管理	47
3.4.4. 職員等の利用する端末や電磁的記録媒体等の管理	49
3.5. 人的セキュリティ	51
3.5.1. 職員等の遵守事項	51
3.5.2. 研修・訓練	57
3.5.3. 情報セキュリティインシデントの報告	59

3.5.4.	ID 及びパスワード等の管理	60
3.6. 技	術的セキュリティ	63
3.6.1.	コンピュータ及びネットワークの管理	63
3.6.2.	アクセス制御	73
3.6.3.	システム開発、導入、保守等	77
3.6.4.	不正プログラム対策	82
3.6.5.	不正アクセス対策	86
3.6.6.	セキュリティ情報の収集	88
3.7. 運	用	89
3.7.1.	情報システムの監視	89
3.7.2.	情報セキュリティポリシーの遵守状況の確認	90
3.7.3.	侵害時の対応等	92
3.7.4.	例外措置	93
3.7.5.	法令遵守	94
3.7.6.	懲戒処分等	95
3.8. 外	部サービスの利用	96
3.8.1.	外部委託	96
3.8.2.	約款による外部サービスの利用	98
3.8.3.	ソーシャルメディアサービスの利用	98
3.9. 評	価・見直し	99
	監査	
3.9.2.	自己点検	100
3.9.3.	情報セキュリティポリシー及び関係規程等の見直し	102

#### 【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)

# 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。

「地方自治情報管理概要」(平成30年3月公表)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42団体(89.4%)、市区町村では774団体(44.5%)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。

前回の改定においては、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り組みが示された。

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、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

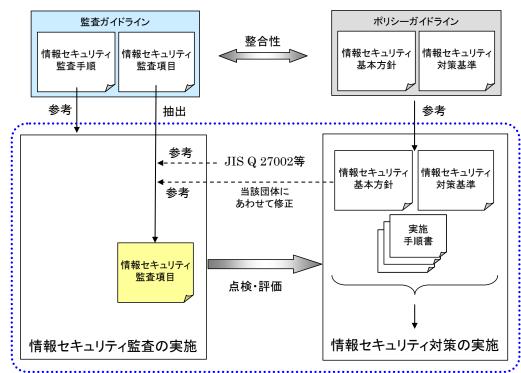
#### 1.4. 本ガイドラインとポリシーガイドラインの関係

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

地方公共団体の取組範囲

#### 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、352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

#### <u>第2</u>章 情報セキュリティ 監査手順

- ・基準
- ・監査計画 ・監査実施
- ・監査報告 ・フォローアップ監査
- ・調達

### 情報セキュリティ監査項目(352項目)

- ・監査項目
- 必須区分
- ・監査資料の例 ・監査実施の例
- ・ポリシーガイドラインNo.
  ・JIS Q 27002 No.
- 1.組織体制
- 2.情報資産の分類と管理 3.情報システム全体の強靭性の向上
- 4.物理的セキュリティ
- 5 人的セキュリティ 6.技術的セキュリティ
- 8 外部サービスの利用 9.評価・見直し

#### 付録

- ・監査資料一覧/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実施委託契約書(例)

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 用頂きたい(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	JISQ27002	留意事項
4. 物理的 セキュ リティ	サーバ	(1)機器の 取付け	29		1)機器の設置に関わる基準及び手続 統括情報セキュリティ責任者又は情報シス 天力管理者によって、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総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グビューにより、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)	11.1.4 11.2.1	
			30	0	II)機器の取付け 情報システム管理者によって、サーバ等の機 誘の取付ける行う場合、火災、水害、族、接 動、温度等の影響を可能な限功排除した場 所に設置し、容易に取外せないように固定す るなどの対策が講じられている。	□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)	11.1.4 11.2.1	・情報資産管理台帳などに、 機器の設置場所や設置状態 などを明記しておくことが望ま しい。
		(2)サーバ の冗長化	31		1)サーイア異化基準 総括情報やより子貴任者又は情報ンス 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	窓変質料のレビューと総括情報セキュリティ責任者又は何 雑システルを開業者へのパンタビューに取り、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	では、広義 の意味で	・サーバの冗長化には、ハードウェア・ハップトクーアが二重に 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 の影響度台・セ十分に検討したうえで、冗長化を行か否か を判断することが望ましい。
			32		■】蓋幹サーバの元長化 情報システム管理者によって、蓋幹サーバ (重索情報を格納しているサーバ、セキュリ ティサーバ、民間テ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 □システム構成図	監査資料のレビュー上情報システム管理者へのインガビュー により、基幹サーイが冗長化され、同一データが保持され ているか確かめる。	4.1.(2)①	12.3.1 ※注意 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	0	■)サーバ障害対策基準 統括情報セキュリティ責任者又は情報シス テム管理者によって、メインサーバに障害が 発生した場合の対策基準及び実施手順が 定められ、文書化されている。		監査資料のレビューと総括情報セキュリティ責任者又は情報システル合理者へのルクがよーに決り、サーベに稼ぎ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)	12.3.1 16.1.2	

## 第2章

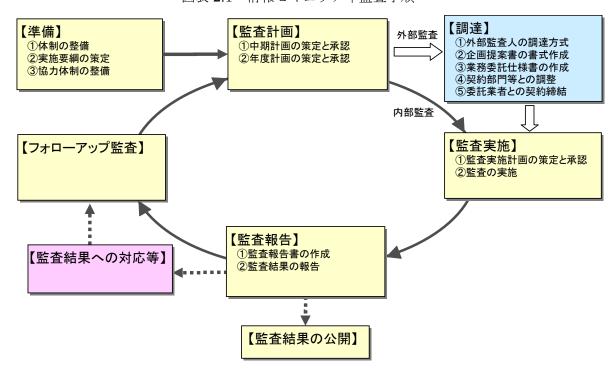
情報セキュリティ監査手順

#### 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

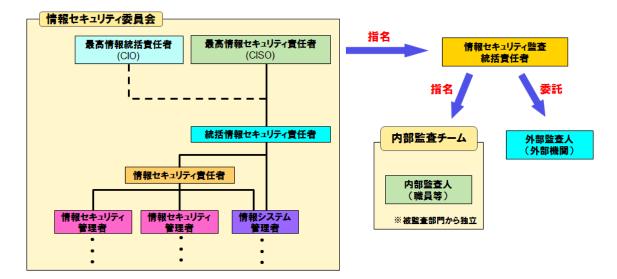
・観察 : 立ち合い監査等により、知識及び技能を評価する・試験 : 筆記試験を行い、行動、知識及び技能を評価する

・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

	項目	内容	
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	意見の相違や対立があっても、進んで責任を	
	動する	もち、倫理的に行動できる	
11	改善に対して前向きで	進んで状況から学び、よりよい監査結果のた	
	ある	めに努力する	
12	文化に対して敏感であ	被監査者の文化を観察し、尊重する	
	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
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

区分	項目
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)。

 
 計画段階
 実施段階

 中期計画
 年度計画

 3年程度の期間の 監査方針や活動 計画
 中期計画に基づく 年度の計画
 個別の監査業務に ついての実施計画

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。

	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			

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)

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
- 個人情報保護条例

#### v) 他の基準・規程類の参照

その他、JIS Q 27002、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

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。

項目 内容 監査目的 監査を実施した目的 1 監査の具体的なテーマや重点監査事項 監査テーマ 3 監査範囲 監査対象の業務、情報システムなどの範囲 被監査部門 監査の対象とした部門 4 監査方法 5 監査で適用した監査技法 監査実施日程 監査の計画から報告までの日程 6 監査実施体制 監査を実施した担当者 7 監查項目 8 監査で確認した大項目 適用基準 監査で適用した基準等 9 監査結果概要 (総括) 監査結果の総括 10 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 改善勧告 指摘事項を踏まえて、改善すべき事項 13 (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

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)

#### (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を指示する。また、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。

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り組みも行われてい 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、外部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。

外部監査の外部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、外部委託事業者による監査に責任を持つ 必要がある。外部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外部 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			
		i )目的			
		ii)本業務の対象範囲			
		iii)準拠する基準			
		iv)監査のポイント 等			
3	監査内容	i)事前打合せ			
		ii ) 事前準備依頼事項			
		・事前の提出資料			
		・アンケート等の有無等			
		iii)監査実施計画書作成			
		iv)予備調査			
		v)本調査			
		※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			
		vi)監査報告書作成			
		vii)監査報告会			
4	監査スケジュー	上記3の概略スケジュール			
	ル	※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・アドバイザ等の役割、			
		氏名を含む監査体制図			
		ii)当該団体との役割分担			
6	監査品質を確保	i)監査品質管理責任者・監査品質管理者等の役割、氏名を			
	するための体制	含む監査品質管理体制図			
		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			
		※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)、情報セキュリティ			
		監査企業台帳への登録等			
		ii)監査メンバの保有資格・技術スキル・地方公共団体を含む			
		実務経験等			
8	監査報告書の目	監査報告書の目次体系(章立て)			
	次体系	i)総括			
		ii)情報セキュリティ監査の実施の概要			
		iii)評価できる事項			
		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)			
		v)監査結果の詳細			
		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			

#### (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。

	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		

図表 2.9 業務委託仕様書に記載する事項(例)

#### (4) 契約部門等との調整

外部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) 外部委託事業者との契約締結

外部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。外部委託事業者は、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。

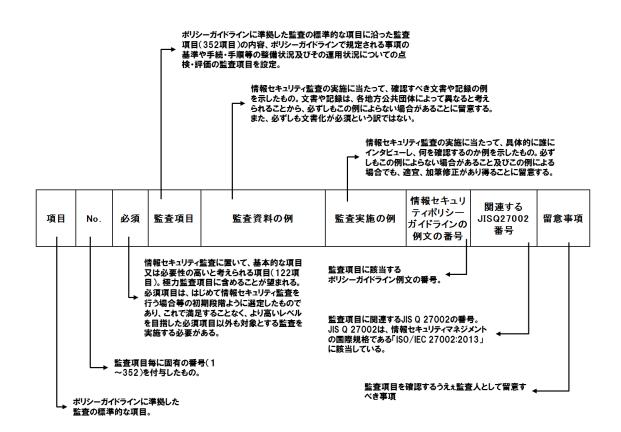
監査を継続的に行うときは、毎回業務委託契約を締結する方法と、業務委託基本 契約と業務委託個別契約に分けて契約を締結する方法がある。毎回契約を締結す る方法が一般的であると考えられ、付録の契約書例もこの形態を想定している。後 者の基本契約と個別契約に分けて契約を締結する方法によるときは、契約書例の 中から、毎回共通する事項を抜き出して基本契約として締結し、毎回定めるべき事 項を個別契約で合意する。

## 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、総務省が平成30年X月に 一部改定した「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。

	1	I	<u> </u>	1
<b>留意事項</b>		<ul> <li>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イ委員会以外に丁騰や幹 部会議等全位置づけること 可能である。</li> </ul>		
関連する j JISQ27002   番号	7.2.1	I	1	6.1.3 6.1.4 16.1.1 16.1.2 16.1.3 16.1.3
情報セキュリ 関連する ティポリシーガ JIS 02 7002 イドラインの例 番号 文の番号	1.(1)~(6), (8) 6.1.1 7.2.1	1.(7)©	1.(7)@	1.(9)
監査実施の例	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 グビュー(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。	□情報セキュリティボリンー 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 □情報セキュリティ表員会設 グビュー(よい) 情報セキュリティボリン一等、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) が設置されているが確かめる。	□情報セキュリティボリシー 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 □情報セキュリティ委員会設 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 アィ委員会が毎年度開催され、リスケ情報の共有や情報セ □情報セキュリティ委員会議 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 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(より、CSIRTが設置されており、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。
監査資料の例	□情報セキュリティボリシー □権限・責任等一覧	<ul><li>□情報セキュリティボリンー □情報セキュリティ委員会設 置要縮</li></ul>	<ul><li>□情報セキュリティボリシー</li><li>□情報セキュリティ委員会設置要綱</li><li>□情報セキュリティ委員会議事録</li></ul>	□情報セキュリティボリシー □CSIRT設置要綱
監査項目	1)組織体制、権限及び責任 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。	1)情報セキュリティ委員会の設置 CISO(によって、情報セキュリティボリン一等、 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。	ii)情報セキュリテイ委員会の開催情報セキュリテイ委員会が毎年度開催され、 情報セキュリテイ教演の改善計画を策定し、 その実施状況が確認されている。	<b>iii ) CSIRTの設置</b> 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。
冷	0	0		0
Š	-	2	т	4
項目	1.     (1)組織体 組織体 制 権限及 制       前     び責任	(2)情報セ キュリティ 奏員会 参		

留意事項				・分類の表示について、情報 システムに記録される情報の 分類をか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ろ。			
				<ul><li>・分類の表 システムに 分類をあり</li><li>注や、表う 類する方</li></ul>			
関連する JISQ27002 番号	8.2.1	8.1.2	8.1.1	8.2.2	8.2.3	8.2.3	8.2.3
情報セキュリティポリシーガイドラインの例文の番号	2.(1)	2.(2)	2.(2)⊕	2.(2)@	2.(2)③	2.(2)⊕	2.(2)⑤
監査実施の例	監査資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て取扱いが文書化され、正式に承認されているか確かめる。	# C C	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)が作成され、定期的に見直されているが確かめる。	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が痛かめる。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。	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 へのイングビューにより、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。	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 へのインがビューにより、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が働かめる。 ます、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。	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 へのインダビューにより、情報資産に、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 にいないか確かめる。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。
監査資料の例	□情報セキュリティボリンー □情報資産分類基準	□情報セキュリティポリシー □情報資産管理基準	□情報資産管理 □情報資産管理台帳	□情報資産管理基準 □情報資産管理台帳	□情報資産管理基準 □情報資産管理台帳	□情報資産管理基準 □情報資産管理台帳	□情報資産管理基準 □情報資産管理合帳
監查項目	1)情報資産の分類に関わる基準 都括情報で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 単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。	1)情報資産の管理に関わる基準 総括情報セキュリンイ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。	11)情報資産管理合機の作成 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合帳(情報資産管理台帳) が作成されている。	II.)情報資産の分類の表示 情報資産に分類が表示されている。	▶ 情報の作成 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。	V)情報資産の入手 情報資産を入手に集合、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ている。	41)情報養産の利用 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。
	0	0	0				
Š	rs	9	7	∞	6	01	=
順	<ol> <li>(1)情報資 情報資 産の分類 産の分類 種の分類 理理</li> </ol>	(2)情報資産の管理					

				۲.	
				・完全性とは、情報が破壊、 改ざん又は消去されていな! 状態を確保することをいう。	
8.2.3	8.2.3 13.2.3	8.2.3 8.3.3	8.2.3	8.2.3	8.3.2 8.3.2
2.(2)@	2.(2) <i>@</i>	2.(2)®	2.(2)@ (77)~(47)	2.(2)@ ( <del>7</del> )	2.(2)@
4 27		441 1	監査資料のレビューと情報セネュリティ管理者及び職員等 へのインケニーにより、機器を供の高い情報管産や利用に指 使する場合、情報セネュリティ管理者の第可を得た上で、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が確 かめる。	311	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 へのインチェーにより、情報電を発棄する場合、情報セキュリテイ管理者の許可を得た上で廃棄され、行った処理に シェ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が確 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 で確かめる。
□情報資産管理基準 □情報資産管理合帳	□情報資産管理告帳 □情報資産管理合帳	□情報資産管理基準□情報資産管理台帳	□情報資産管理台帳□情報資産管理台帳	□情報資産管理基準 □情報資産管理台帳	□情報資産管理基準 □情報資産管理台帳 □情報資産廃棄記録
(4) <b>情報者の保管</b> 開催化キュリテイ管理者又は情報システム管 理者によって、情報管座の分類に従い、情報管産が適切に保管されている。	<b>哺)情報の送信</b> 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。	以 / 情報養産の運搬 車両等にか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、必要に応じ機付きのケース等に 格納し、暗号化又はバ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。	x)情報養産の提供 機能性の高小滑解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 で、必要に応じ暗号化又はバスワードの設 定が行われている。	xi)情報資産の公表 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。	xi)情報養産の廃棄 情報資産必應乗する場合。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。
12	13	41	15	16	17
<ol> <li>(2)情報資 情報資 産の管理 産の分 類と管 埋方法</li> </ol>					
	(2)情報資 産の管理 産の管理 (2)情報資産の発生 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。 (3)情報資産の分類に従い、情報資産の分類に従い、情報資産を理与帳 電切に保管されているか確かめる。必要に応じ、職員等 へのアンケート調査を実施して確かめる。	(2)情報資 (4)情報資 (2)情報資産管理基準 監査資料のレニーと情報でキュリテイ管理者、情報システ (2)⑥ 指報資産管理 (4) (4) (4) (4) (4) (4) (4) (4) (4) (4)	(2)情報資 (4)16 (4) (4) (4) (4) (4) (4) (4) (4) (4) (4)	(3)情報資	12

選目	ģ	必	日東 草温	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. (I)マイナン 情報ン バー利用 バー利用 ネケム 事務系 全体の 強韧性 の向上	8-	0	4× ( )	<ul><li>□ オットワーク管理基準</li><li>□ 通信回線敷設図</li><li>□ 結線図</li></ul>	離査資料のレビューとCISO又は総括情報セキュリティ責任者へのイングビューにより、マイナンバー利用事務系と他の観視が分離されており、通信でさないよりになっているか確さかめる。	3.(1)①	13.1.3	
	6	0	1)マイナンバー利用毒素系と外部との GISOXは液活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、通信路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より、か の外部接続やはインターネットへ接続してい ない。	□ネットワーク管理基準 □通信回線敷設図 □結線図 □対線図	監査資料のレドューとCISOスは総括指輪セキュリティ責任者へのイングェューにより、ペイレン・利用事務系の外部との通信は、通信総略の限定及びアプリケーションロドコルレ・シャ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抜続していないが高かめる。	3.(1)D	13.1.3	マイナンバー利用事務系と他 の関係を通信でない、ただし、マ なければならない、ただし、マ イナンバー和用事務系と外部 台ンの信をする必要がある場 台に限りは、通信路路の限定 及びアブリケーションプトコ ルのレベルでの限定を行わな ければならない。
	20	0	端末における情報アウセス対策 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、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斡務金等のパンプン等のサンプリンが確認により、パスワード以外に指紋認証等の生体認証が併用されているが確かめる。	3.(1)@	9.2.4	
	21		間) 業務毎の専用端末化 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斡務金等のパンプン等のサンプリンが確認により、マイナンバー利用事務系の端末が専用端末でわるが確かめる。	3.(1)@	1	
	22	0	N)電磁的記録媒体による情報待ち出し の不可数定 職員等がマインバー利用事務系の端末から電磁的高級條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 及び執務金等のパソコン等のサンプリンが確認により、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)@	11.2.5	

1 ケジト 存組 たい 旧 甲セン	CISO人は総括情報セキュリアイ責任者に
■   ## 6   14   ☆ ★ 15   ☆ ★ 12	よって、インターネント接続米に高度な情報 セキュリテイ機器を導入している。 1回1 情報セキュリティ運用監視 CISO又は結括情報セキュリティ責門人材による高 水準な運用監視を行っている。 N ) 自治体情報セキュリティ方でとる。 整義 (SISO又は結結情報セキュリティファンティ とって、「市内のインターネット接続口を推修し はいて、自治体情報セキュリティが経過でも維約した。

リ 関連する -ガ uSq27002       例 番号   留意事項	11.1.4	11.1.4 ・情報資産管理台帳などに、 11.2.1 榛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。	12.3.1   ・・サーバの冗長化には、ハー   ※注意   ドルエア・ソアルエが二重に	12.3.1 ※注意 JISQ27002 では、広義 の意味で バッケアップ 全般を規定 している。	12.3.1 16.1.2
情報セキュリティボッシーガイドラインの倒文の番号	4.1.(1)	4.1.(1)	4.1.(2)(D	<del>3.4</del> .1.(2)①	4.1.(2)@
配合実施の金	監査資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。	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、サーベ等の機器が設置されているが確かめる。 こので確かめる。	監査資料のレビューと総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ダビューにより、サーバの元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。	艦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、基幹サースが冗長化され、同一データが保持されているか確かめる。	監査資料のレビューと総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がエューにより、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。
監査資料の例	□機器設置基準/手続	□機器設置基準/手続 	ロサーバ元長化基準	<ul><li>□サーバ元長化基準</li><li>□システム構成図</li></ul>	□サーバ障害対策基準 □サーバ障害対応実施手 順
	1)機器の設備に関わる基準及び手続 総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。	11)機器の取付け 情報ン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 調・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 るなどの対策が講じられている。	1)サーバ元長化基準 都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。	11)基幹サーバの冗長化 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 ディサーバ、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。	Ⅲ)サーバ障害対策基準 総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、メインサーバに修書が 第生世報者によって、メインサーバに修書が 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。
必		0			0
o N	29	30	15	32	33
曹	4. (4.1. (1)機器の 物理的 サーバ 取付け セキュ 等の管 リティ 理		(3)サーバ の元県化		

思急事項	・定場保守等で予備機への 切替試験等各実施し、その記 場を確認することが望まし、。 ・の解を注こいでは、 No.34~35も関連する項目で あろことが必参考にすること。		- 設置した予備電源が、サー バ等の強設に対して十分な 通力供給能力があるのかを定 増的に確認しておくことが望 ましい。	
関連する JISQ27002 番号	16.1.2	11.2.1	11.2.1 11.2.2 16.1.2	11.2.1 11.2.2 16.1.2
情報セキュリ 関連する アイポリシーガ JISQ27002 イドラインの例 番号 文の番号	4.1.(2)@	4.1.(3)①	4.1.(3)①	4.1.(3)@
監査実施の例	監査資料のレビューと情報システム管理者へのインダビュー におり、サーン「職業時にセカング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、いるが確かめる、実際にサーン「職者が発生している場合は、対策が有効に機能しているが確かめる。	監査資料のレビューと統括情報セキュリティ責任者又は情報とネースインを指導に備えた、例のインのインのエーにより、存電等に備えた、一備電源の設置基準や、終電等の電源異常からサーベ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。	監査資料のレビューと情報システム管理者へのイングビュー及び管理を必要を開展、より、USS、無停電電源装備、たどの子機の関係がといるが確かめる。また、停電時や瞬時に最適し、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が確かめる。	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医域の指揮による過電流からサース等の機器を保護するために、確信設備やでVCF(定電圧定周波装置)を設置するために、確信設備やでの下(定電圧がある。
監査資料の例	□サーバ障害対策基準 □サーバ障害対応実施手 順 順審機告書	□機器電源基準	<ul><li>○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○</li></ul>	<ul><li>一機器電源基準</li><li>一次ステム構成図</li><li>一機器設置記録</li><li>「障害報告書</li></ul>
器	<ul> <li>ト)サーバ等書が策 権報ン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。</li> </ul>	1)機器の電源に関わる基準 指指情報とよりが実性を対しては テム管理者によって、停電や落電等からサー 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。	1) 子編編版報画の数階及び点数 情報システン学理者によって、序画等による 電源供給の停止に備えた子権電源が備え 付けられ、定期的に点換されている。	■ 過電路放棄 情報ンダンは間重によって、落雷等による 過電流からサーベ等の機器を保護する設備 が備えられている。
冷			0	
o Ž	34	35	36	37
質	4. (2)サーバ 物理的 サーバ の万長化 セキュ 等の管 リティ 理	(3)機器の		

更量		・情報処理設備に接続する通信ケープル及び電源ケープルは、可能ならば施設内の地下に重要するか又はそれに代わる十分な保護手段を施・ナンとが望まい。 ケーブルの損傷等を放止するために、顕線収納管全使用するとが望ましい。 等)で分離して配線するでとが望まし、また、通信をうかに、直信レーでを表して正確がするとが、望まし、また、通信をしている場合は、それぞれを別ルートで配線することが望ましい。			
01		情情になった。 サーケななす・ サークななかがい。 なったない。 サークなない。 サークなない。 サークない。 サークない。 ファックには、 サークない。			
関連する JISQ27002 番号	11.2.3	11.2.4	11.2.3	11.2.1	11.2.3
情報セキュリー ドイポリシーガ、 イドレインの倒 女の番号	4.1.(4)©	4.1.(4)①	4.1.(4)②	4.1.(4)③	4.1.(4)@
監査実施の例	監査資料のレビューと統括情報セキュリティ責任者又は情報ンステム管理者、のイグビューにより、通信ケーブルや電源ケーブルの配線基準やネットワーケ接続口(ハブのボー等)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が確かめる。	監査資料のレビューと統括情報セキュリティ責任者又は情報ンステム管理者へのイングに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。	監査資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ダヒューにより、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。	□通信ケーブル等配線基準 監査資料のレビューと総括情報セキュリティ責任者又は情報・手続 ・手続 ・の視察により、ネットワーク接続ロ(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。	監査資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外部委託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。
監査資料の例	<ul><li>□通信ケーブル等配線基準 /手続</li></ul>	<ul><li>□ 通信ケーブル等配線基準</li><li>「手続</li></ul>	□通信ケーブル等配線基準  手続  □障害報告書	□通信ケーブル等配線基準 /手続 □通信回線敷設図	<ul><li>□通信ケーブル等配線基準 /手統</li><li>□作業報告書</li></ul>
	1)通信ケーブル等の配線に関わる基準 及び手機 総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総が定められ、文書化されている。	1) 通信ケーブル等の保護 維括情報セキュリテ、責任者及び情報シス 大一グ単型者によって、通信ケーブルや電源 ケーブルの損傷等を抗止するための対策が 講じられている。	前)ケーブル障害対策 総括情報セキュリデ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。	N) ネットワーク接続口の設置場所 デム格性報セキュリテ、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 プのボート等)が他者が容易に接続できたい。 場所に設置されている。	V)配線変更・追加の制限 総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。
冷		0			
Š	89	88	40	14	42
<b>画</b>	4. (4)通信 物理的 サーバ ケーブル等 セキュ 等の管 の配線 リティ 理				

項目	Š.	必	<b></b> <b>1</b>	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 j JISQ27002   番号	習意事項
4. (5)機器の 物理的 サーバ 定期保守 セキュ 等の管 及び修理 リティ 理	43		1)機器の保守・修理に関わる基準及び 手続 総括情報セキュリティ責任者又は情報シス デム管理者によって、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ダビューにより、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	0	<b>の定数保守</b> によって、サーバ等の機 されている。	□機器保守・修理基準/手 続 門保守機器管理表 □保守休期図 □作業報告書 □障害報告書 □機器保守点檢記錄	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、保守担当が開催になっているが、保守が適切に行われているが確かし、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が確かめる。	. 4.1.(5)①	11.2.4	
	45	0	・   電磁的配線媒体を内蔵する機器の格   電電路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、情報ンステム管理  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 続守機器管理表 □保守権器官 □保存権器 □作業報告書 □機密保持契約書	監査資料のレビューと情報システム管理者へのイングビュー により、電飲的配験媒体を対像する機器を外部委託の事業 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。データを消まできない場合は、修理を委託中 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)@	15.1.2 11.2.4 18.1.1 18.2.2	
(6) (7) (4) (6) (4) (4) (4) (4) (4) (4) (4) (4) (4) (4	46		1)庁外への機器設置に関わる基準及 [ び年線 が活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総括情報セキュリティ責任者又は情報とネーステム学組者へのインダビュー「こじ)、「予外にサーバ等級と大場全投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が通りめる。	4.1.(6)	11.2.6	・地方公共団体の庁外の装 借電が取られていることが望 出し。 キャリティングを考慮し、 ・キッリティングを考慮し、そ れぞれの場所に応じた長も適 切な管理策を導入することが 望ましい。
	47		<b>ii )庁外への機器の設置の承認</b> 総括情報と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 	監査資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ダビューには)、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。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が確かめる。	<del>3.4</del> .1.(6)	11.2.5 11.2.6	

画	Š.	冷	監査項目	監査資料の例	監査実施の例	情報セキュリ 関連する ティボリシーガ JISQ27002 イドラインの例 番号 文の番号	関連する JISQ27002 番号	思意事項
4. (6)庁外へ 物理的 サーバ の機器の セキュ 等の管 設置 リティ 理	8 4		ii) 庁外の機器の設置状況確認 統指情報セキュリテ、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 □外部委託事業者訪問記 「外部委託事業者監査報 「外部委託事業者監査報 告書 「外部委託事業者における 「ISO/IEC27001認証取得状 ぶ	監査資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グビュー「CLP、「予外に製産された機器へのイクリン・「大学、ご期的に確認されているか確かめる。	4.1.(6)	11.2.5 11.2.6 18.2.2	
(7) 機器(2)	49		1)機器の廃棄等に関わる基準及び手 総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(1)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。	<ul><li>□機器廃棄・リース返却基準</li><li>□機器廃棄・リース返却手</li><li>○機器廃棄・リース返却手</li></ul>	監査資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グビュー(により、機器名統乗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)	11.2.7	・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。
	20	0	1)配信装置の情報消去 情報システム管理者によって、廃棄又はリース返却子後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 ■機器廃棄・リース返却手 続 門情報資産管理台帳 □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 4.1.(7)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)	11.2.7	・委託契約等により、サービス・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・

情報セキュリ   関連する   ティボリシーガ JISQ27002   イドラインの例 番号   文の番号	者又は情 4.2.(1)① 11.1.1 ・管理区域の中に特にセキュ Swの構造 かめる。	者 又は情 4.2.(1)② 11.1.1 ・管理区域の存在そのも必外 数の視察に 11.1.4 餅の者から分からないように いか、外壁 表示等を明示しないことが望 ましい。	者 又は情 4.2.(1)③ 11.1.1 ・外部〜通じるドアを必要最 70.2.(1)③ 11.1.1 ・外部〜通じるドラシ、消防法 現機能、警 に達反したい 大空館 する心 要がある。	者又は情 4.2.(1)④ 11.1.1 でよん論の が実施さ が実施さ	者又は情 4.2.(1)⑤ 11.1.1 成の視察に Aで塞がれ	
監査実施の例	監査資料のレビューと総括情報セキュリティ責任者又は情報ングスケム管理者へのイングニーに対い、管理区域の構造と 基準が文書化され、正式に承認されているが確かめる。 また、様報ンステム章や電磁的記録媒体の保管順が管理 区域に指定されているが確かめる。	監査資料のレビューと統括情報セキュリティ責任者又は情報ンステム管理国本へのイングビュー及び管理区域の協築により、管理区域が地階又は1階に設けられていないが、外壁が無態になっているが確かめる。	配査資料のレビューと総括情報セキュリティ責任者又は情報となったイングインタイン。 難ンスナる管理をかのインダアコー及び管理区域の視察に は、外部へ通じるドアを必要最低限とし、鍵、配視機能、警 無装置等が設けられているか確かめる。	配査資料のレビューと総括指輪セキュリテイ責任者又は指揮システム管理をファイングビュー及び指輪システム船の場象に対象に計算、防火、防水等の対策が実施されているが縮かめる。	監査資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となったイグを理と域の視察にない、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が確かめる。	
監査資料の例	□管理区域構造基準 □独物フロアレイブウト図 □敷地図面 □管理区域(情報ンステム 室等)のレイアウト図	□雑物フロアレイアウト図 □敷札図面 □管型区域 (情報ンステム   至等) のレイアウト図	□ 建物フロアレイアウト図 □ 敷 地図面 □ 管理区域 (情報システム : 室等) のレイアウト図	<ul><li>□ 種物フェアレイアウト図</li><li>□ 繁地図面</li><li>□ 管理区域 (情報ンステム</li><li>□ 室等) のレイアウト図</li></ul>	□ 建物フロアレイアウト図 ・□ 敷地図面 □ 管理区域 (情報システム 室等) のレイアウト図	
監査項目	1)管理区域の構造基準 総括情報セキュリティ責任者及び情報シス デム管理者によって、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。	11)管理区域の配置 市が指揮地で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。	管理区域への立ち入り衝職機能 総括情報セキュリティ責任者及び情報シス ラム管理者によって、管理区域への許可さ 対でいないなら入りを防止するための対策が 講じられている。	N)信報システム室内の機器の影響、防火、防火水鉄 然店情報セキュリティ責任者又は情報シス が店情報でキュリティ責任者又は情報シス 早等に耐震、防火、防水等の対策が施されている。	v)管理区域の構造 総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わている。	11、我自己认为"一"
冷			0	0		
è	51	52	53	54	55	
画	4. 物理的 管理区 管理区域 セキュ 域(情 の構造等 リティ 薄シス デム室 等)の 管理区域					

		5.41課目 証しこ出検 な			<del>                                     </del>
習意事項		入退室手続に業者名、訪 前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い管理 する。 の入退管理シアルを導入した の入退管理シアルを導入した 支障が生じるの念未然に訪止 するため、定期的に保守点検 するため、定期的に保守点検 は一下を必入とのえたがにが するため、定期的に保守点検 は一下をのる本然にが を関したの入退室上、。 心理以上の入退室や道常 時間外の入退室企道、不信な がは全途確認する必要がある。 る。			
関連する JISQ27002 番号	11.1.2	11.1.2	11.1.2	11.1.2	11.1.5
情報セキュリ ティポリシーガ イドラインの例 文の番号	4.2.(2)	4.2.(2)①	4.2.(2)©	4.2.(2)③	4.2.(2)(£)
監査実施の例		監査資料のレビューと情報システム管理者へのイングビュー及び管理を嫌の機器により、入遺室管理基準に従って管理 区域への入遺室を制限しているか確かめる。 また、「ぴカード、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、及びMCカード等の	監査資料のレビューと情報システム管理者へのイングビュー及び管理区域の視察により、職員等及び外部委託事業者の身分証明書の機構状況や、身分証明書等を機構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。	監査資料のレビューと情報システム管理者へのイングビュー及び管理医域の視察により、外部からの訪問者が管理医域に入る場合、立ち入り医域の制限や、当該医域への入退室合すでおいているが職員の同行、ネームブレート等の着用を行っているか確かめる。	監査資料のレビューと情報システム管理者へのイングビューにより、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、まと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。
監査資料の例	□管理区域入退室基準/手 続	□管理区域入进室基準/手 続 □管理区域入退室記録 □認計用カード管理記録	□管理区域入退室基準/手 続	口管理区域入退室基準/手 続 口管理区域入退室記録	□管理区域入退室基準/手 続 □管理区域入退室記録
監査項目	1)管理区域への入遠室に関わる基準 及び手機 施行情報セネリアイ責任者又は情報システム管理権によって、管理区域への入退室 に関わる基準及び手続が定められ、文書化されいる。	ii)管理区域への入退室制限 情報システム管理者によって、管理区域へ の入退室が制限され管理されている。	旧)身分配明春等の携帯 情報システム管理者によって、職員等及び 外部委託事業者が管理区域に入金する際 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。	N)外部訪問者の立ち入り区域制限及び 区別 外部訪問者が管理区域に入る場合、情報シ 外が訪問者によって、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。	(4)管理区域への機器等の持込み制限 情報システム管理者によって、機密性の高い 情報資産を扱ジン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。
必須		0			0
No.	57	8 9	59	09	19
画	4. (2) (2) 物理的 管理区域 セキュ 域(情 の入退室 リティ 報シス 管理等 テム室 等の 音楽等				

所	Š	必	監査項目	監査資料の例	監査実施の例	情報セキュリ 関連する ティポリシーガ JISQ27002 イドラインの例 番号 文の番号	関連する JISQ27002 番号	留意事項
4.2. (3) 物理的 管理区 機器等の セキュ 域 (情 機入出 リティ 難シス 等型 管理	62		1)管理区域への機器等の搬入出に関 わる機器及び手機 総括情報セキュリティ責任者又は情報シス アム管理者によって、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。	口機器搬入出基準/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ンテント管理者へのイングビューにより、管理区域への機器等の機入出に関わる基準及び手続が文書化され、正式に乗認されているが確かめる。	4.2.(3)	11.1.5	・可能であれば許可されてい 花パアンセスを織けるために、 搬入口は管理区域から離す ことが望ましい。
	63		用)機器等の搬入 情報ンストが開出者によって、機器等の搬 力の際は、あらがじか職員又は支託した業 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	艦査資料のアピューと情報システム管理者へのインタピュー 4.2.(3)① により、職員又は発射した業者が搬入する機器等が現存の 情報システムに影響を与えないが確認しているが確かめる。	. 4.2.(3)①	11.1.5	
	64	0	III)機器等の搬入出時の立会い 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、職員を立ち合わせ ている。	口機器搬入出基準/手続 口管理区域入退室記錄 口機器搬入出記錄	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 4.2.(3)②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)@	11.1.5	

			のとな様		. 10	<b>紫</b> 媛。
留意事項			・通信回線敷設図、結線図の モナア・イルについてもアッ セス制限やパングロード設定な と、外部への満えい防止対策 を講じる必要がある。		・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。	・例えば、機密性の高い情報 資産を扱う場合には、専用総 カルドN回線等を用いること。
囲			・通信回線敷設図、電子ファイルについてス制限やパスワーセス制限やパスワービ、外部への漏えいをが、外部への漏えいを講じる必要がある。		ら理的な理 E C、集約された。 。	列えば、機密 『産を扱う場合 3V PN 回線等
2005			い価もどを		. 10	<b>・</b> 御ぐ
関連する JISQ27002 番号	9.1.2	9.1.2	9.1.2	9.1.2	I	9.1.2
情報セキュリティポッシーガイドラインの倒文の番号	4.3.	4.3.①	4.3.①	4.3.@	4.3.3	4.3.4
· · · ·	監査資料のレビューと統括情報セキュリティ責任者又は情。 報ンステム管理者へのインダビューにより、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 されているが確かめる。	配直資料のDCピューと統括情報セキュリティ責任者又は情。 報ングテム管理者へのインダビューにより、通信回線及び通信回線技職、管理状況について確かめる。 活の線技職、管理状況について確かめる。 大に、熱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。	監査資料のDCビューと統括情報セキュリティ責任者又は情。 機ンズテム管理者へのインダビュー及び文書保管場所の提 繋により、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。	配査資料のレビューと総括信頼セキュリティ責任者又は情。 機ン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が確かめ る。	監査資料のレビューと統括情報セキュリティ責任者又は情・ 機ンズナム管理者へのインダビューにより、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。	監査資料のDレビューと総括情報セキュリティ責任者又は情。 機ンズラム管理者へのインダビューにより、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避択されてい るか確かめる。
監査資料の例	ロネットワーク管理基準	□ネットワーク管理基準 □通信回線敷設図 □結線図	<ul><li>□ ネットワーク管理基準</li><li>□ 通信回線敷設区</li><li>□ 結線区</li></ul>	□ネットワーケ管理基準 □通信回線敷設図 □結線図	□ネットワーク管理基準 □通信回線敷設図 □結線図	<ul><li>□ネットワーク管理基準</li><li>□通信回線敷設区</li><li>□結線区</li></ul>
	1)通信回線及び通信回線装置に関わる基準 各基準 総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、庁内の通信回線及ス 所の音信回線装置の管理基準が定められ、文書化されている。	11)通信回線及び通信回線装信の管理 施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。	Ⅲ)通信回線及び通信回線接信に関する文書の保管 各文書の保管 総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。	N)外部ネットワーク機能ポイントの監察 維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。。	<ul> <li>ソト存扱系ネットワークの集的 総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ケ が総合行政ネットワーク(LGWAN)に集約されている。</li> </ul>	4) 通信回線の選択 維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 産を取り扱い方様以ンチンムに接続している面 信回線がある場合、適切な回線が選択され でいる。
冷		0				
Š.	65	99	67	89	69	70
		<b>.</b>		<u> </u>	<b>.</b>	
西	4.3. 譲及び 適信回 線接置 の管理					
	4. 物理的 ルキュュ リティ リティ ※ ※					

質	o N	冷	監査項目	監査資料の例	監査実施の例	情報セキュリ 関連する ティポリシーガ JISQ27002 イドラインの例 番号 文の番号	関連する JJSQ27002 番号	更重
4. 4.3. 物理的 通信回 セキュ 線及び リティ 通信回 線装置 の管理	17		(4) 法受債権の暗号化 総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 □ 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.( <del>+</del> )	9.1.2	・暗号化については、No.184~186も関連する項目であることから参考にすること。
	72		備) 通信回義のセキュリティ対策 予は情報セネュリテノ責任者又は情報ンス 予は管理者によって、伝送途上の情報が破 泰、密範、収さん、消失等が生じたいよう。 信回線として利用する回線に対策が実施さ れている。	ロネットワーク管理基準	監査資料のレビューと総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グビューにより、伝送後上の情報が破壊、盗職、政営人、消失等が生じないように保護されているが、流かるが確かめる。また、適切なアクセス相側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が確認する。	4.3.6	13.1.2 13.1.2	・通信回線の断線、通信機器 の故障のための装置、ケーブ 小類の予備在庫をもっことが 望まし、 ・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。
	73		は)通信回線の可用性 株型は一般が指摘や表現が 性型以上の情報を取り扱う情報システムが接 総される通信回線は、雑念的が運用を可能 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、同用性2以上の背積を取り扱う情報を対象が情報やステムが接続される値回線について、継続的な運用を可能とする回線が選択されているか痛かめる。対し、必要に応じ、回線を冗長構成にする等の指置が講じられているか痛かめ る。	4.3.©	13.1.2 17.2.1	

道目	No.	必		監査資料の例		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
4.4. 物理的 職員等 セキューの利用 リテイ 末や鮨 稼や配	74		1)パリコン等の端末の管理基準 総括情報とキュリティ責任者文は情報シス 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ンステム管理者へのインタビューにより、執務宣等のハショ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.	11.2.1	・定期的に端末管理台帳と実 被を点検し、紛失、盗難等の 情報セキュリティインシデント ロ早期発見に努めることが望 ましい。
	75		ii ハベリコン等の端末の盗難防止対策 情報システム管理者によって、執務監等の 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グビュー及び執務室等の損禁により、ベ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録保管等の盗難防止の対策が講じられているが確かめる。	4.4.①	11.2.1	
	76		)電磁的記録媒体の登離防止対策  情報システム管理者によって、電磁的記録 媒体の盗雛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、電磁的記錄媒体について、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が確かめる。	4.4.①	11.2.1	
	7.1	0	<b>*ソログイン緩距粉定</b> 情報システム管理者によって、情報システム そ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。	□ベンコン等管理基準	監査資料のレド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ンコン等のサンプリング権認により、パンコン等により、インコン等にはア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.©	9.2.1 9.2.2 9.4.2 9.4.3	・・・スワードの管理及び取扱 131、219~220も関連する項 目であることから参考にするこ と。 ・ログイン時のシステム設定に っいては、No.218も関連する 項目であることから参考にす
	78		<b>v)パスワードの併用</b> 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 ドディスケパスワード等)の併用が行われてい る。	□バソコン等管理基準	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ン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	9.2.4	・管理用バスワードは必要最小限の者で管理されること。 ・担当変更等が実施された場合は、同時にバスワードを変更するとが望まい。
	79	0	って、多要素認証	□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	9.2.1 9.2.2	・多要素認証はマイナンバー 利用事務系では必須事項、 LCWAN接続系では推奨事 項とする。
	80		■・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	□バソコン等管理基準	監査資料のレニューと情報システム管理者へのインタビュー及び執務監禁のパンコン等のサンプリング権認により、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が確かめる。	4.4.©	10.1.1	

思意事項		
関連する JISQ27002 番号	10.1.1	8.3.1 8.3.2 11.2.6
情報セキュリ 関連する ティポリシーガ JISQ27002 イドラインの例 番号 文の番号	4.4.⑤	4.4.6
監査実施の例	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 4.4.⑤ 及び執務差等の電磁的記録媒体のサンプリン/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。	離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 4.4.⑥ 及びモベイル端末のサンプリング確認により、遠隔消去機能 が利用されているが確かめる。
監査資料の例	□パソコン等管理基準	□パソコン等管理基準
監查項目	<b>哺)電磁的記録媒体の暗号化</b> 構報ンオ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。	k)遠隔溝去機能の利用 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。
心通		
ġ	28	82
圏	4. 物理的 職員等 セキュ OA別用 リアイ 末や電 旅的記 森的記	なみます 他の離 単

1			17イボ 認及 5.292 である		
1.	<b></b> ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・		報セキュー 状況の確 いては、N. する項目・ さすること		
1.	图		損等の情 一の遵守 対処につい 100も関連 から参考(		
(1)	002		・ 最少なり 8.3		
1) 情報セキュリティポリシー等選号の	関連する JISQ270 番号	5.1.1	5.1.1	I	I
1) 情報セキュリティポリシー等選号の	情報セキュリ ティポリシーガ イドラインの例 文の番号	5.1.(1)⊕	5.1.(1)@	5.1.(1)@	5.1.(1)@
(1) (1) (4) (1) (4) (4) (5) (5) (6) (7) (7) (7) (7) (7) (7) (7) (7) (7) (7	監査実施の例	監査資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ピューにより、職員等の情報セキュリティがリン一及び実施手順の遵守や、情報セキュリティが策について不明な点及び遵守が困難な上債券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。主た、承認された文書が職員等に周知されているか確かめる。	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 へのインダビューにより、情報セキュリティボリシー及び実施 手順の適等中状況を振かめる。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、指示を何 等が速やかに情報セキュリティ管理者に相談し、指示を何 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。	監査資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ダビューにお、職員等の業務以外の目的での情報資産の特ち出し、情報ンケラムへのアッセス、電子メールアドレスの使用及びインダーネット・のアッセスの禁止について文書化され、正式に承認されているが確かめる。	
(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	監査資料の例		□情報セキュリティボリンー □実施手順	<ul><li>□情報セキュリティボリシー □情報資産取扱基準 □ネットワーク利用基準 □電子メール利用基準</li></ul>	□編末ログ □電子メール送受信ログ □ファイアウォートログ
(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	監査項目	1)情報セキュリティポリシー等選令の 明記 総括情報セキュリティ責任者又は情報セキュリ リティ青任者によって、職員等が情報セキュリ ティポリシー及び実施手順を選守しなければ ならないことが定められ、文書化されている。	11)情報セキュリティポリシー等の適中 職員等は、情報セキュリティポリシー及び実 施手順念遵守するとともに、精報セキュリティ 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。	1)情報資産等の利用基準 総括情報と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特ち出し、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。	11)情報資産等の業務以外の目的での 使用業止 職員等による業務以外の目的での情報資産 の特ち出し、情報ン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。
( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( )	必須	0	0		0
	No.	83	84	85	98
		) () () () () () () () ()	_	) (画等 (重要の (重要の) (世間の) (正用の)	
Lici 巻 の h	項目			い職選の業のの禁	
5.5 10 10 10 10 10 10 10 10 10 10		N1			

通	o Z	必	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	田彦事項
(1) 機員等の適子等に (1) 機員等 機員等の (1) を (1	87			□端末等特出・特込基準/ 手続 連/手続 準/手続	監査資料のレビューと統括情報でキュリティ責任者又は情報を登り、 報セキュリティ責任者へのインタビューにより、機密性足以 L、可用性2。元全性2の情報資産を外部で処理する場合 いるか確かめる。	5.1.(1)⊚	6.2.1 6.2.2 11.2.6	・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
	88	0	用)情報資産等の外部特出制限 職員等かモイハ始末、電磁的記線媒体、 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。	<ul><li>「端末等特出・持込基準/ 手続 「「斤水での情報処理作業基準/手続 単一手続 「端末等特出・持込申請書 /承設書</li></ul>	口端末等特出・特込基準/ 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 手続 つのイングビューにより、職員等がモッイルでは、電磁的記 口庁林での情報処理作業基 鏡媒体、情報登底及びソフトウェアを外部に持ち出す場 音、情報セキュリティ管理者から許可を得ているか確かめ 口端末等特出・持込申請書 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 承認書	(-7) (-7)	6.2.1 6.2.2 11.2.6	・紛失、盗難による情報漏え、 必必むセイるため、暗号化等 の適切な処置をして持出すこ とが望ましい。
	68	0	Ⅲ)外部での情報処理業務の制限 職員等が外部で情報処理作業を行う場合 は、情報セキュリテイ管理者による許可を得ている。	□庁外での情報処理作業基 準 手続 □庁外作業申請書/承認書	□庁外での情報処理作業基盤査資料のDとコーと情報をネュリティ管理者及び職員等 へのイングビューにより、職員等が外部で情報処理作業を行 □庁外作業申請書/承認書 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)	6.2.1 6.2.2 11.2.6	・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) (1) (1) (1) (1) (2) (3) (4) (4) (5) (6) (7) (7) (7) (7) (7) (7) (7) (7) (7) (8) (8) (9)	06	0	1)支給以外のパンコン、モバイル端末 及び電磁的配像媒体の業務利用基準及 化子機 総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 以外のパンコ、エイグル端末及び電磁的 記縁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。	□端末等特出・特込基準/ 手続 □支給以外のパンコン等使 用申請書/承認書	監査資料のレビューと総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、文格以外のパンソン、モ・インが指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が確かめる。	5.1.(1)⊕	8.2.3 11.2.1	

留意事項				・記録を定期的に点検し、紛失、盗難が発生していないか 権設することが望ましい。
05				·記錄を 失、盜巢 確認す?
関連する JISQ27002 番号	6.2.1 6.2.2 11.2.1 11.2.6	13.1.2	11.2.5	11.2.5
情報セキュリティポリシーガイドラインの倒 女で番号	€1(J)⊕	5.1.(1)@	5.1.(1)⑤	5.1.(1)⑤
監査実施の例	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グビューにより、職員等が情報処理作業を行う際に支給以外のバンコン、モバイル端末及び電磁的記録媒体を用いる場合、あるいは广付ネットワーツに接続する場合、情報セキュリティ管理者の許可を得ているが確かめる。また、端末ロックが行われていることや、端末ロック機能が利用できること、機密性3の可能能が行われていることや、端末ロック機能が利用できること、機密性3のが情報で変化が「透陽消失機能が利用できること、機密性3のが情報を確かの情報処理作業を行っていないこと、支給2人のの端末 のセキュリティに関する数号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痛かめる。	□庁外での情報処理作業基 監査資料のレビューと情報でキュリティ管理者及び職員等へのインダビューにより、支給以外のパンコン、セバイが結果 □支給以外のパンコン等使 及び電磁的記念機体を行わネットワーグに接続することを計画 日申請書/展認書 □する場合は、シンクライアント環境やセキュアブウザの □支給以外のパンコン等使 使用、ファイル暗号化機能を持つアブリケーでの接続 のみを許可する等の情報議え、対策が講じられているが確 市基準 「高かめる。必要に応じて、職員等へのアンケート調査を実施し 「確かめる。	監査資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グビューにより、端未等の持ち出し及び特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。	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、保管されているが確かめる。
監査資料の例	□支給以外のパソコン等使 用申請書、承認書 □支給以外のパソコン等使 用基準	□庁外での情報処理作業基 増・手続 □支給以外のパソコン等使 用申請・所認書 □支給以外のパソコン等使 □技能以外のパソコン等度 用基準	□端末等特出·特込基準/ 手続	□端末等特出·特込基準/ 手続 □端末等特出·特込申請書 /承認書
監査項目	1) 支給以外のパソコン、モバイル端末 及び電路的記憶媒体の利用側隔 職員等が指輪処理作業を行際に支給以外 のパソコン、モバイル端末及び電廠的記録 媒体を用いる場合、あるいは庁内ネットワー がに接続する場合、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 による許可を得ている。また、機密性の高い 端末及び電廠的記録媒体による情報とエックボ 端末及び電廠的記録媒体による情報処理作 業は行われていない。	用)支給以外のパンコン、モバイル端末 及び電磁的記録媒体の庁内ネットワーク 機構 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、情報編表い対策が講じられている。	i)端末等の特出・特込基準及び手機 総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総が定められ、文書化されている。	前)端末等の特出・持込配録の作成 情報セキュリティ管理者によって、端末等の 持ち出し及び持ち込みの記録が作成され、 保管されている。
必須	0	0		0
o Z	-6	92	ဗ	94
曹	5. 5.1. (1) 人的な 職員等 職員等の キュリ の遵守 議中事項 (4) 中事項 (4) チィー 事項 (5) 女治以外 のパンコン・ボーバイン・ボーバイン・ボーバイン い間 (4) を開発 (5) を開発		(1) 職員等の 選中事項 ⑤ 特ち出し及 び持ち込 みの記録	

迁					認証用のIC 1返還させ 5遵守につい 310も関連す から参考に	
图意事項					・退職時等には、認証用のIC カード等を確実に返還させ る。その他の法令強守につい では、No.309~31の場遇 必項目でかることから参考に すること。	
関連する JISQ27002 番号	12.1.2	12.1.2	11.2.9	11.2.9	8.1.4	8.1.4
情報セキュリ ティポリシーガ イドラインの例 文の番号	5.1.(1)@	5.1.(1)@	5.1.(1)©	<del>3.</del> 5.1.(1)◎	5.1.(1)®	5.1.(1)®
監査実施の例	監査資料のレビューと総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。	□セキュリティ設定変更申請 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 「クライングビューにより、バンコンやモバイン様来におげるセ キュリティ関での変更が必要な場合は、情報セキュリティ管 単者の許 コを得ているが編めめる。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。	監査資料のレビューと総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グビュー「により、離席時のパツコン、モバイル端末、電磁的配線媒体、文書等の取扱基準が文書化され、正式に承認されているが確かめる。	監査資料のDCコ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、パンコン、モバイル端大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て、場形では、場所のの第三者使用又は情報ない。場所への保管といった、情報資産の第三者使用又は情報をは、出了イ管理者の許可な、情報資産の第三者使用又は情報が閲覧される。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がる。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がる。	<u>監査資料のレビューと統括情報セキュリティ責任者</u> スは情報セキュリティ責任者へのイングビューにより、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が確かめる。	配着資本のレビューと情報セキュリティ管理者及び職員等 へのイングビューにより、異動、起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認する。主た、異動、 場職後も業務上知り得た情報を溜らさないように周知されているか確認する。また、民動、 いるか確かめる。
監査資料の例	□端末等セネュリティ設定変更基準/手続	□セキュリティ設定変更申請 書/承認書	<u> ロッリアデスク・クリアスク</u> リーン基準	ロクリアデスク・クリアスク リーン基準	<b>口職務規</b> 程	口職務規程
監查項目	1)パンコンやモバイル端末におけるセキュリティ股店変更基準及び手機 総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と以情報をキュリティ責任者とは情報セキュリティ責任者によって、パソコンやセ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。	1)パンコンやモバイル端末におけるセキュリティ版が変 側腕 特報とキュリティ管理者による許可な、パッ 日本のでもよくれい端末におけるセキュリティ形 定は変更されていない。	1)和上の端末等の取扱基準 指指情報とキュリティ責任者又は情報とキュ リティ責任者によって、離席時のペシコン、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。	1) 加上の端末等の取扱 動能解析には、パソコン、モバイル端末、電磁 的配象媒体、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指置が講 じられている。	1) 温醂時等の選令事項 計算報告キュ リティ責任者によって、異動、退職等により業 務を離れる場合の選守事項が定められ、文 書化されている。	1) 過職時等の情報資産の取扱い 職員等が、異物、短端等に少素的を開れる 場合、利用していた情報資産が返却されて いる。 おた、異動、退職をも業務上知の得た 情報を涌らさないよう職員等へ周知されている。
冷				0		
ò	95	96	97	86	66	100
町	5. 5.1. (1) 人的セ 職員等 職員等のキュリ の遵守 議任事項 ・ 事項 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	更の禁止	(1) 職員等の 職件等の (7) (1) 大作の端 用来等の管		(1) 機両等の 機子毒項 ⑥ 迅速離時等 の強件中等 質	

情報セキュリ 関連する ティポリシーガ JISQ27002 イドラインの例 番号 文の番号	(4)	7.4.2.0     7.1.2     ・情報セキュリティに関する研 (*) 1.2.2     修 訓練については、No.100 ~109も関連する項目である ことがら参考にすること。       ELて     ことから参考にすること。	7.9 5.1.(2)② 7.1.2 ・同意書への署名は必須で 1内なく、業務の内容に応じ て、必要と判断される場合に 行う。	5.1.(2)© 9.2.2
監査実施の例	監査資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グビューにより、情報セキュリティに関し非常勤及び臨時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が確かめる。	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、情報セキュリティオリン・等のうち、採用時に 非常動及び踏時職員に理解させた事項が、非常勤及び額 時職員によって実施、遵守されているか確かめる。必要にた でて、非常勤及び額時職員へのアンケート調査を実施して 確かめる。	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、非常勤及び臨時職員採用時に、業務の内容に応じて、情報セキュリティがリシー等を遵守する旨の同意書への署名を求ているか確かめる。	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勢務室の視察により、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非常勤及び臨時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。
監査資料の例	□非常勤及び臨時職員 ~ の対応基準	□研修·訓練奖施基準 □研修奖施報告書	<b>柳</b> 凝叵口	□ネットワーク管理基準 □電子メール利用基準
監査項目	1)非常勤及び臨時票員への対応基準 □非常勤及 総括情報と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 リティ責任者によって、情報セキュリティに関 リティ責任者によって、情報とキュリティに関 「非常勤及び臨時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。	1)非常数及び臨時職員の情報セキュリ □研修・副練実施基準 「一大化リシー等の選中 情報セキュリティ管理者「た」って、非常勤及 び臨時職員を採用する際、情報セキュリティ ポリシー等のうち当該職員が選中すへき事 項を理解させ、実施、遵守させている。	1)非常勤及び臨時票員の情報セキュリ ライボリシー等の連令に対する同意 情報セキュリテイ管理者によって、非常勤及 (で臨時職員採用時に、業務の内容に応じ て、情報セキュリティボリン・等を遵守する旨 の同意書への署名を求めている。	1)非常勤及び臨時職員のインターキット及び電子メール使用制限 情報セネリティ管理者によって、非常勤及 で臨時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。
· 必	_	C.		_
ė Ž	0	102	103	104
極	5.     5.1.     (2)       人的セ 職員等 非常勤及キュリ の遵守 び臨時職ティー 事項 再項 店への対 た	(2) ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	(2) 非消失 (2) (3) (4) (5) (6) (6) (6) (7) (7) (4) (7) (4) (7) (4) (7) (4) (7) (4) (7) (7) (7) (7) (7) (7) (7) (7	#活動及 び臨時職 での臨時職 (6) (6) (7) (7) (7) (7) (7) (7) (7) (7

			<b>.</b>	
野田				・再奏記は原則禁止である が、例外的に再奏形を認める 動をしば、再会形事業者に おける情報セキョリテ、対策 が十分取られており、外部奏 下井業者と同等の水準である こと確認した上で許可しな ければたらない。 ・外部奏託事業者に対して、 ・外部委託事業者に対して、 ・外部委託をはいて必要 に応じ立ち入り検査を実施す ること。 ・外部委託に関する事項つい では、No.315~318を開連す る項目であることから参考に すること。
関連する JISQ27002 番号	5.1.1	5.1.1	15.1.2	15.1.2
情報セキュリティポリシーガイドラインの例 メアラインの例 文の番号	5.1.(3)	5.1.(3)	5.1.(4)	5.1.(4)
監査実施の例	離査資料のレビューと総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グビューにより、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ある。という文書化され、正式に承認されているか確かめる。	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 ビュー及び物務室の視察により、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。	監査資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、ネッドワーク及(特報システムの開発・保守等 を発せする外間委託事業者及び外部委託事業者から再委 所を受ける事業者に対して、情報セキュリティボリンー等のうち外部委託事業者等が守るされての場で、 お外部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。	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・保守総を発行する分割を発行する分割を発行事業者の名の組織を指える場合のでは、情報セキュリティボリン・等のうち外部委託事業者等が守るくまりなの適中及びその機の事項が説明されているか確かめる。
監査資料の例	□情報セキュリティボリンー	□職員等~の周知記録	□情報セキュリティボリシー	□ 樂務委託製約書 □ 外部委託管理基準
器	1)情報セキュリティポリシー等の公妻 総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 キュリティボリシー及び実施手順必認覧でき るように掲示することが定められ、文書化され ている。	i)情報セキュリティポリシー等の掲示 情報セキュリティ管理者によって、職員等が 常に最新の情報セキュリティポリシー及び実 施手順を閲覧できるように掲示されている。	1)外部委託事業者の情報セキュリティ ポリシー等連中の設明義務 ネッドンーク及び情報システムの開発・保中 報を外部委託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、外部委託事業者及び外部 委託事業者から再委託を受ける事業者及び外部 なに、「構化セキュリティがリシー等の55外部 の機密事項会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。	1)外部委託事業者に対する情報セキュリティボリシー等進中の説明 ネットアーグ及(特報システムの開発・保中等を外部委託業者に発在する場合、情報セキュリティが理者によって、情報セキュリティがリー・等のうち、外部委託事業者及び外部委託者から再委託を受ける事業者が明まれている。
今		0		0
ė	105	106	107	801
町	5.1. (3) 人的セ 職員等 情報セキュキュリ の遵守 リティボリ ライ 事項 シー等の 掲示		(4) 外部 参託 神 本 本 本 本 本 本 本 本 本 本 本 正 の 語 の 記 の 記 の 記 の 記 の 記 の 記 の 記 の 記 の 記	

情報セキュリ 関連する ティボリシーガ JISQ27002 (路の例 イドラインの例 番号 文の番号	報セキュリティ責任者へのイン 5.2.(1)~(4) 7.2.2 アイに関する研修: 訓練の実施 承認されているか確かめる。	戦セキュリティ責任者へのイン 5.2.(1) 7.2.2 tセキュリティご関する研修・訓 る。	報セキュリティ責任者へのイン 5.2.(2)① 7.2.2 ・研修計画には情報セキュリティに関する研修計画の策定と ティ人材の育成も含まれていているが確かめる。ま ることが望ましい。 よいないでいるが確かめる。	報セキュリティ責任者へのイン 5.2.(2)② 7.2.2 いて、職員等が毎年度景低1 2講できるように計画されてい	報セキュリティ責任者へのイン 5.2.(2)③ 7.2.2 員等を対象に、情報セキュリ でいるが確かめる。	報セキュリティ責任者へのイン 5.2.(2)④ 7.2.2 ・研修内容は、毎回同じ内容 ではなく、内部監査の結果や 情報セキュリティ責任 「下内外での情報セキュリティ 「下内外での情報セキュリティ 「アム担当者及びその他職員等 インケデントの第生状況等を 内容 ではない。 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。
監査実施の例	監査資料のレビューと総括情報セキュリティ責任者へのイングビューにより、情報セキュリティに関する呼称・訓練の実施について文書化され、正式に承認されているが確かめる。	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。	<ul> <li>□研修・訓練実施基準</li> <li>□が6・訓練実施基準</li> <li>○アケーにより、情報セネュリティに関する研修計画の策定と □情報セネュリティを員会議 実施体制の構築が定期的に行われているが確かめる。また、情報セネュリティ委員会に承認されているが確かめる。また、情報セネュリティ委員会に承認されているが確かめる。</li> </ul>	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 Y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。	監査資料のレビューと総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が確かめる。	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、情報とキュリティ管任義、特報とキュリティ管理者、情報システム管理者、情報システム管理者、情報システム性当者及びその他番(ドガして、自己の責任、義務・権限を理解できるように、それの役割、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。
監査資料の例	□研修・訓練実施基準	□研修・訓練実施基準 □研修実施報告書 □訓練実施報告書		□研修·訓練実施基準 □研修·訓練実施計画	□研修·訓練実施基準 □研修実施報告書	□研修·訓練実施基準 □研修·訓練実施計画
監査項目	i)情報セキュリティに関する研修・関線 の実施基準 CISOによって、定期的にセキュリティに関す る所修・副線を実施したければならないこと が定められ、文書化されている。	) 情報セキュリティ研修・訓練の実施 CISOによって、定期的にセキュリティに関す る研修・訓練が実施されている。	1)母修計画の策定及び承認 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。	ii)情報セキュリティ研修計画 職員等が毎年度最低1回は情報セキュリティ 研修を受講できるように計画されている。		N)情報セキュリティ研修の内容の設定 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。
必須		0				
Š.	109	110	Ξ	112	113	114
	(1) 情報セキュ リティに関 する研修・ 訓練		(2) 研修計画 の策定及 び実施			•
断	5.2. 雪春					
	5. 人 ホト アイ イ					

質	No.	冷	監査項目	監査資料の例	監査実施の例	情報セキュリ 関連する ティポリシーガ JISQ27002 イドラインの例 番号 文の番号	関連する JISQ27002 番号	留意事項
5. (3) 人的セ 研修・緊急時対 キュリ 訓練 応訓練 ティ	校   116		1) 緊急時対応訓練の実施計画 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 □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が確かめる。また、訓練計画には、ネットワーケや債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が確かめる。	5.2.(3)	7.2.2	
	117		ii)緊急時対応回線の実施 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 □訓練実施報告書	監査資料のレアューン統括情報セキュリアイ責任者へのイン 5.2.(3) ダバューにより、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が確かめる。	5.2.(3)	7.2.2	・緊急時対応計画について は、No.301~304も関連する 項目であることから参考にす ること。
(4) 研修・訓練 への参加	訓練 1118		<ul><li>1) 研修・監像への参加</li><li>すべての職員等が定められた研修・訓練に参加している。</li></ul>	□研修・訓練実施基準 □研修実施報告書 □訓練実施報告書	監査資料のレビューと総括情報セキュリティ責任者へのイン 5.2.(4) タビューにより、幹部を含めたす、ペイ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)	7.2.2	

	mi <sup>A</sup> J				ンュ活 報再酬の
鬥	・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。				・情報セキュリティインンデントの分析結果は、情報セキューリの分析結果は、情報セキューサーボリン・等の見直しに活用されることが望まし、。・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機断的に再発防止策を検討する必要がある。
留意事項	- トレは、E - トと整合 : ある。				・情報セキュリティインジトの分析結果は、情報セリティインジトの分析結果は、情報セリティインン・学のり屋間であることが選ました。・他部門も含めて同様のセキュリティイン・デント 落を妨止するために全げる 発表が上するために全がから、必要がある。
	<ul><li>報告ルートは 決定ルートと が重要である。</li></ul>				・情報セキ- トの分析結 リティボリン ・他部門もこ ・在キュリティ 発を防止す 一般に再発防 的に再発防 必要がある。
関連する JISQ27002 番号	5. 6.	6; 6;	2, 6;	6; e;	ं धं सं एं
	16.1.3	16.1.2	3 16.1.3	16.1.3	16.1.2 16.1.3 16.1.4 16.1.5
情報セキュリティポリシーガイドラインの倒 メドラインの倒 文の番号	5.3.(1)~(3)	5.3.(1)	5.3.(2)①~③ 16.1.2 16.1.3	5.3.(2)⊕	5.3.(3)
	又は情 等が情 民等外 場合の 8されて	Mm v	及は清 外部が、 する情 か、報	スは情 /メケム ・部から 重絡手	ペークイン パープ が でいる できるる。 に報告
	監査資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テブーを認知した場合、又は住民等外額から指揮セキュリティインテア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。	監査資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、情報ンステム管理者、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。	監査資料のレビューと統括情報セキュリテイ責任者又は情報セキュリテイ責任者、情報セキュリテイ責任者、情報とキュリテイ管理者、情報シアコーにより、住民等外部からな管理者、能員等へのイングでコーにより、住民等外部からネットワーク及び情報ンステム等の信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・事順に従って連帯なく報告されているか確かめる。	監査資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グビューにより、情報システム等の情報セキュリティイン・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文書化され、公表されているが確かめる。	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 が確かめる。 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がを確かめる。 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。
9	キュリテューによった場合 フた場合 トの報告 され、正	キュリテ、 リティ管 ューにより 働かめる。	キュリティ リティ管 ユーにより この情報登 て報告を ているか	キュリティーによい こうしん にっしん にっしん にっしい でんしい ていい は 数 窓 にっしゃん いんかい にっちゃん しょうしゃん しょうしゃん しょうしゃん しょうしゃん しょうしゃん しょうしゃん しょうしゃん しょうしょく しょくしょく しょくしょく しょく しょくしょく しょくしょく しょく	キュリテン ンシデン が作成、 が起きた ったかど 後割され
監査実施の例	帝 帝 か た か が が が 大 が が が が が が が が が が が が が が が	括情報と呼ばなくなく	括情報セキューイングビック・アングレーングランダーングデンタデンをしたいった。 報告され	括情報で ウインタに ・シェント ・シェント ・ショント ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	括情報センリアイイ での記録 ベンゲン/ 適切でな 誘力に策決
組	ューと落 活	ューと統 任者、情 員等への 報告され、	ューと結 (布本、福 の事やへので情報な アツボン	1	ューと総 情報セキ ら対応ま 内容等は ら、再楽 いめる。
	監査資料のレビ 報セキュリティ責 報セキュリティイ 部から情報セキ 報告ルート及び いるか確かめる。	監査資料のレビューと総括情報セキュリテー解セキュリティ責任者、情報セキュリティ管・アエ管理者、職員等へのインタビューにより従って連帯なく報告されているか確かめる。	本のアア エリケイ書 田者、職 フーク及 エリティイ	キのアプライ書 報セキュ 敬けるたい ひけるたい ひけるたい いて 女神	監査資料のレビューと グビューにより、情報セ 行われ、発生から対応 行われ、発生から対応 対応かめる。 また、情報セキュリティ 動したか、報告内容等 原因究明結果から、再 原因究明結果から、再 きれているか確かめる。
	麗報 報 報 は な い の か い り り り り り り り り り り り り り り り り り り	開本 アンス (3) (2) (3) (4) (4) (4) (4) (4) (5) (5) (6) (7) (7) (7) (7) (7) (7) (7) (7) (7) (7	開報 で と と な な な な の の の の の の の の の の の の の	監報等報段値との生に強や情をつい	騰益資料の タビューによ 行われ、発名 か確かめる。 かでは、 かでは、 がでいた。 原口である。 原因究明結 されているが
<b>室</b>	7-7-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1	5 5 17 17 14 14	\$ \$ } } ! !	報記録	5 5 > >  }
監査資料の例	キュリティ 調頂	キュリティ 訓順 キュリティ	キュリティ 調度 キュリティ	キュリティ 訓順 対する広:	キュリティ 画 ・キュリティ
帽	□情報でキュリティインシゲント報告手順 ント報告手順	□情報セキュリティインンデント報告手順 □情報セキュリティインンデント報告書 ント報告書	□情報でキュリティインシデント数音手順 ント数音手順 □情報でキュリティインシデント報告書	□情報セキュリティインシデ ント報告手順 □住民に対する広報記録	□情報セキュリティインシブ ント報告手順 □情報セキュリティインシブ ント報告書
	<b>の報告</b> (、情報 場合の報 る。	i) 庁内での情報セキュリティインシデントの報告 庁内で情報セキュリティインシデントが認知さ けた場合、報告手順に従って関係者に報告 されている。	<b>リティ</b> 報システ リティイ ら、報告 る。	9 関ロ	<b>の原因</b> 報セキュ 引の当該 ンシデン 、保存さ
	インシデントの報告 責任者によって、情報 トを認知した場合の第一書化されている。	キュリティインシデントが認知さ イインシデントが認知さ こ従って関係者に報告	1) 住民等外部からの信報セキュリティインテナトの場合 インテナトの場合 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を完まっプティイン等の情報を定に関する情報セキュリティインツ・アナ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を受けている。	ii) 情報セキュリティンシデントの窓口 数値 が iii) では、「情報システムの情報セキュリ アイインシデントについて住民等外部から報 音を受けるための窓口製置及び、当該窓口 への連絡手段について定められ、公表され でいる。	1)情報セキュリティインシデントの原因 初明・記録・再等的止等 総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 いの発生から対応までの記録が作成、保存さ れている。
語 香項目	<b>ルイン</b> アイ ガンン ド 大学 ・ 大学 ・ 大学	<b>報セキュ</b> リティイン 順に従っ		報システーク・ハイ仲のの日報画のいて「たる」	<b>ルイイン</b> 7 <b>5 イ東任等</b> アイ黄任等 書類セキ・ までの記録 までの記録
₩7	<b>i)情報セキュリティ 手順</b> 然指情報セキュリティ ビキュリティインシデン 告手順が定められ、文	i) 庁内での情報セ ・の報告 - 方がで情報セキュリテ でた場合、報告手順に されている。	<ul> <li>(1) 体民等が部からイン・ポントの報告</li> <li>イン・ポントの報告</li> <li>主民等が密からネットな等の情報資産に関・アンデントについて報イン・アデントになって関係者に関います順に従って関係者に</li> </ul>	) <b>信報セキュリテイ教育</b>	1)情報セキュリティ 労畑・配像、再発防」 然品情報をキュリティ アティケン・アントを引 責任者によって、情報 いの発生から対応まで たている。
	1)権報セキュリティインシデントの報告 手順 総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。	<ul> <li>1) 庁内での情報セトの報告 F内で情報セキュリテ れた場合、報告手順に されている。</li> </ul>	<ul><li>1) 住民等外部から インシボントの報由</li><li>住民等外部からネット ム等の情報資産に関 ンシボントについて報 手順に従って関係者!</li></ul>	間)情報セキュリティインンデントの第日 数値 ではこました、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製産及び、当該窓口への連絡手限について定められ、公表されている。	1   情報セキュリティインシデントの原因 労略・記録・再等的止等 対象を表す。 対象を表すが一番では、情報セキュリティアンデントを引き起こした部門の当該 関任者によって、情報セキュリティインシデントの発生がら対応までの記録が作成、保存されている。 れている。
冷	0	0			
Š	119	120	121	122	123
		(1) 庁内での 情報セキュ リティイン シデントの 報告	(2) 能ならの情 報なキュリ ティインシ デントの報 告		(3) 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
通	記事キテンンと報 おフィントは報子 もファット				
	5. 人的セ ティン				

留意事項						・回収時の個数を確認し、紛失・弦離が発生していないが、確実に確認することが望ましい。
関連する JISQ27002 番号	9.2.1 9.2.2	9.2.1 9.2.2	9.2.1 9.2.2	9.2.1 9.2.2	9.2.1 9.2.2	9.2.2
情報セキュリ ティポリシーガ イドラインの例 文の番号	~ @ ~	5.4.(1)⊕ (₹)	(√) (√)	5.4.(1)① ( <del>7</del> )	5.4.(1)@	5.4.(1)③
監査実施の例	監査資料のレビューと統括情報セキュリティ責任者又は情報ンステム管理者へのインタビューにより、認証用の1CカードやUSBトークンの取扱いに関わる基準と手総が文書化され、正式に承認されているが確かめる。	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 インガビューにより、認証用のICカードやUSBトーゲンなどが 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。	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 5.4.(1)① インチビュー及び報務室の損象により、業務上不要な場合 (イ) にカードリードペキシンジ等の端末のスロッド等から認証 用のICカードペセSBトーツ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。	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を大き、アナイ責任者及び情報を大力が立た。 できいSBトーツンが紛失した場合は、建やかに統括情報と 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。	監査資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テステム管理者へのインタビューにより、紛失した認正用網ンステムを受けると、シリンカードやUSBトーツ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。	監査資料のレビューと総括情報セキュリティ責任者又は情報システム管理者、のイングニーにより。認証用のにカードやUSBトーツを切り替える場合に切替え前のにカードやUSBトーケンが回収され、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かる。
監査資料の例	□ICカード等取扱基準	□ICカード等取扱基準	□ICカード等取扱基準	□1Cカード等取扱基準□1Cカード紛失届書	□ICカード等取扱基準 □ICカード等管理台帳	□ICカード等取扱基準 □ICカード等管理台帳
監査項目	1)認証用にカード等の取扱いに関わる 基準及び手縛 総括情報セキュリティ責任者又は情報シス アム管理者によって、認証用にカード等の取 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。	<b>ii )認証用ICカード等の共有禁止</b> 認証用ICカード等は職員等間で共有されて b v2c v。	<b>                                  </b>	N)医証用にカード等の効失時手続 認証用にフード等の対象性かは場合は、速や かだ然指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。	V) 認証用にカード等の紛失時対応 認証用につード等の紛失性緒がからだ場 合、統括情報セキュリティ責任者及び情報ン ステム管理者によって、当該にグード等の不 正使用を妨止する対応がたられている。	4) 認証用にカード等の回収及び膨業 ICカード等を切り落える場合、統括情報セキュリフィ責任者及び情報なアの情報でスト全種理者に 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。
必須			0	0	0	0
No.	124	125	126	127	128	129
通目	5. 5.4. (1) 人的セ ID及び ICカード等 キュリ バス の取扱い ティ 等の管 理					

	Š	冷	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 JUSQ27002 番号	恩章章
L .	130		1)職員等のID取扱基準 総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取极基準	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ダビューにより、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)	9.2.1 9.2.2	・利用者IDの取扱いについて は、No.198~2015関連する 項目であることから参考にす ること。
L.	131		ii)職員等のID賞与禁止 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取极基準	監査資料のレビューと情報システム管理者及び職員等~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~のアンケート調査を実施して確かめる。	5.4.(2)⊕	9.2.1	
L.	132		iii) 共用IDの利用制限 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覧扱基準 □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が確 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)@	9.2.1	
L	133		<ul> <li>・ 職員等のパスワードの管理基準 総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。</li> </ul>	□バスワード管理基準	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、職員等のバ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)	9.3.1	・バスワードに関する情報の 管理については、No.219~ 220も関連する項目であること から参考にすること。
	134	0	<b>用)バスワードの取扱い</b> 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。	ロバスワード管理基準	監査資料のレビューと情報システム管理者及び厳員等へのイングビューにより、職員等のシスワードについて照会等に応じたり、他人が登りため、他会をおけなて学列に設定したりしたいように取扱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)Û~© 9.3.1	9.3.1	・最短6文字以上で、次の条件を満たしていることが望ましい。 ・ の当人の開連情報(例えば を前、電話番号、誕生日等) から、他の者が容易に推測できる事質又は表別に相当できる事質又は表別に相当で きる事項に基づかないこと。 の連続した同一文字又は数 中ではす出くはアルファベット だけの文字列でないこと。
I I	135	0	<b>川)パスワードの不正使用防止</b> 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 培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が確かめる。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)⊕	9.3.1	

重	ò	必	監査項目	監査資料の例	監査実施の例	情報セキュリ 関連する ティポリシーガ JISQ27002 イドラインの例 番号 文の番号	関連する JISQ27002 番号	田意事項
5. 5.4. (3) 人的セ ID及 パスワード キュリ びパス の取扱い ディ ワード 等の管 理	136		▶)同一パスワードの使用業止機密性の非常に高い複数の情報システムを投源。 投源、事等のパスワードは、当該情報システムをA間で異なるように設定されている。	□バスワード管理基準	<u>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 5.4.(3)⑤</u> 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バスワードを使用していない分離かめる。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。		9.3.1	
	137		<b>v)仮パスワードの変更</b> 仮パスワードは、最初のログイン時に変更されている。	□バスワード管理基準	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 5.4.(3)⑥ 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。		9.3.1	仮ベスワードの中には初期バスワードを含んでいることに留意する。
	138	0	<b>リンズスワード記憶機能の利用禁止</b> サーバ、ネットワーグ機器及びヘンコン等の 端末にブ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 5.4(3)② イングレー、 サルフェー、 サルスをの指表の の場式にい、サーバ、ネッドワーが機 野及 びゃいコン等の端末に、 3.70 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。		9.3.1	
	139		<b>哨)パスワードの共有禁止</b> 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 5.4.(3)③ 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。		9.3.1	ただし共有IDのパスワードは 除る

野士場田						・サーバの冗長化について は、No.22~25も関連する項 目であることから参考にすること。 と。
関連する JISQ27002 番号	9.4.1	I	9.1.1	9.4.1	12.3.1	12.3.1
情報セキュリティポリシーガイドラインの例 メデッスの例 文の番号	6.1.(1)	6.1.(1)⊕	6.1.(1)@	6.1.(1)③	6.1.(2)	6.1.(2)
監査実施の例	監査資料のレビューと総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ダビューにより、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。	監査資料のレビューと情報システム管理者へのイングビュー 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が確かめる。	監査資料のレビューと情報システム管理者へのイングビュー 及びベンコン等の連携オからの場合により、表書サーベが課 登等の単位で構成され、職員等が他課金等のアメルダ及び 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。	監査資料のレビューと情報ンステム管理者へのインダビュー 及びペソコン等の端末からの練員等により、在民の個人情報 や人事記録といった特定の議員等にか取扱えないデータに ついて、担当体の議員等によって閲覧及び使用できないよ う、別途ディレグリを作成する等のアッセス制御が行われて いるか流かめる。	監査資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ダビューにより、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。	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 バ等に記録された音報について、サーバの元長化対策に 関わらず、必要に応じて定期的にベックアップが実施され にいるか確認いめる。また、バックアップが建成され 記、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。
監査資料の例	□文書サーバ設定基準	<ul><li>□ 文書サーバ設定基準</li><li>□ 職員等への周知記録</li></ul>	□文書サーバ設定基準	□文書サーバ設定基準	□バックアップ基準 □バックアップ手順 □リストア手順	<ul><li>□バックアップ基準</li><li>□バックアップ手順</li><li>□バックアップ美施記録</li><li>□リストア手順</li><li>□リストアテスト記録</li></ul>
監査項目	1)文書サーバに関わる数定基準 総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。		<ul> <li>II)文書サーバの構成</li> <li>III)文書サーバが 機様ンズテム提唱者によって、文書サーバが 課業等の単位で構成され、職員等が他票室 等のフォルダ及びアイルを閲覧及び使用できないように設定されている。</li> </ul>	▶)文書サーバのアクセス制御 権限ンデン管理者によって、特定の職員 等しか取扱えいデーダニンいて、担当外 の職員等が閲覧及び使用できないような指 置が講じられている。	1) バックアップに関わる基準及び手順 が指揮物セキュリティ責任者又は情報シス テム管理者によって、ファイルサーベ等に記 終された情報についてのバッグッグ・プに関わ る基準及び手順が定められ、文書化されている。	■)パックアップの実施 情報システム管理者によって、ファイルサー パ等に記録された情報について定期的な パックアップが実施され、パッケアップ媒体 が適切に保管されている。
冷			0	0		0
o Z	140	141	142	143	144	145
町	6. 6.1. (1) 技術的 コン 文書サー セキュ ピュー べの設定 リティ タ及び 等 イネット の管理				(2) パッケアッ プの実施	

图意事項		・必要に応じて、他団体との間において契約名取り交わす において契約名取り交わす この契約にお けるセキュリティの扱いは、関 進する業務情報の重要度やリ スクを伝演させる管理策を臨り 込むことが望ましい。				
関連する JISQ27002 番号	13.2.1 13.2.2 15.1.2	13.2.1 13.2.2 15.1.2	6.1.2 12.1.1 12.1.2 12.4.3 12.5.1 14.2.2	12.4.3	12.1.2 12.4.3 12.5.1 14.2.2	6.1.2 12.4.3 15.1.2 15.2.1
情報セキュリ ティポリシーガ イドラインの例 文の番号	6.1.(3)	6.1.(3)	6.1.(4)	6.1.(4)⊕	6.1.(4)@	6.1.(4)©
監査実施の例	監査資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、他の団体との情報ステムに関する情報及びビューにより、他の団体との情報及びいに関わる基準が支帯化され、正式に承認されているが確かめる。	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グビューにより、他の団体との情報システムに関する情報及びツア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ているか確かめる。	監査資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グやエーにより、所管する情報、ステムの運用及び変異等の作業内容を記録し管理すること、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。	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。	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ングニーにより、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。 いよう管理されているか確かめる。	監査資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グビューにより、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 月安 砂線作金級かられて外部変能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。
監査資料の例	□情報及びソフトウェアの交換基準	□情報及びソフトウェアの交 換基準 □信報及びソフトウェアの交 「信報及びソストウェアの会 「日報及の別の情報及 「一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	<b>□システム運用基準</b>	□システム連用基準 □システム運用作業記録	□システム運用基準 □システム変更等作業記録	□システム運用基準 □システム変更等作業記録
監査項目	1)他団体との情報システムに闘する情報等の交換の取扱いに闘わる基準 事等の交換の取扱いに闘わる基準 地が開催やセンド・責任者 文は情報を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シア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。	11)他団体との情報システムに関する情報を含な 機等の交換 他団体と情報システムに関する情報及びツァウェアを交換する場合、情報システム管 エ書によって統括情報セキュリティ責任者 び情報セキュリティ責任者の許可を得ている。	1)システム管理記録及び作業の確認 「四部力る基準 総括情報センニリテ責任者又は情報システムを増増さいこの、所管する情報システムを増増さいこので、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。	■)情報システム運用の件集記録作成 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。	<ul> <li>II)システム変更等作業の配験作成及 化管理 総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。</li> </ul>	<b>ト)システム変更等作業の確認</b> システム変更等を行う場合は、2名以上で作業し、互いごその作業が確認されている。
必				0		
Š	146	147	148	149	150	151
野	6. 6.1. (3) 技術的コン 他団体との セキュ ピュン 情報システ リティ タびひ ば親する メット 情報等の ワーク 交換		(4) システム管 単記録及 び作業の 確認			

画						
思き事項						
関連する JISQ27002 番号	1	1	12.4.1	12.4.1	12.4.2	12.4.2
情報セキュリ ティポリシーガ イドラインの例 文の番号	6.1.(5)	6.1.(5)	6.1.(6)	6.1.(6)⊕	6.1.(6)@	6.1.(6)③
監查実施の例	監査資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、情報システム保護等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。	監査資料のレビューと統括情報セキュリティ責任者又は情報となって大生登車と並の損業に表して大力と登車となりは業に入り、メアハチの中では、大手に対しては、大手の一時には、一般では、大手の関連文書を業務上が要でない。者からの関策や、紛失等がない、よう、施錠したキャビネットへの保管やアオ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。	監査資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が確かめる。	監査資料のレビューと統括情報や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。	監査資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グビューにより、ログ等が仕様とおりに取得され、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。	監査資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が確認するために、ログ等を定期的に点検、分析を行っているが確かめる。
監査資料の例	□情報システム関連文書管 理基準	□情報システム関連文書管 理整準 □システム仕様書等 □プログラム仕様書等	□システム運用基準	<ul><li>□システム運用基準</li><li>□ログ</li><li>□ンステム稼動記録</li><li>□解音時のシステム出力ログ</li></ul>	ロシステム運用基準	ロシステム運用基準
監查項目	<ul> <li>1)情報システム仕様書等の管理基準 総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。</li> </ul>	<ul> <li>1)情報システム仕様書等の管理 総括情報セキュリティ責任者文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。</li> </ul>	1)ログ等の取得及び管理に関わる基準 総括指揮とスークで責任を受び情報シス 子と管理者によって、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。	<ul> <li>1)口グ等の取得及び保存</li> <li>総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アイの確保に必要な記録が取得され、保存されている。</li> </ul>	間)口分等の改さん、観消去等の防止 総括情報と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。	N) ログ等の点検、分析 総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、取得したログを理的 にに係及は分析する機能を設け、必要に応じて悪質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。
冷		0		0		
o Z	152	153	154	155	156	157
町	6. (5.) 技術的 コン 情報システ セキュ ピュー ム仕様書 リティ タ及び 等の管理 ネット の管理		(6) ログの管理 取得等			

留意事項				・設定の不整合とは、例え に、通信機器間で通信格路 の設定や通信ペケットの通過 ルールに齟齬がある等の場合 む、う。	
				<ul><li>設定の不 ば、通信様 の設定や記 アールに をいう。</li></ul>	
関連する JISQ27002 番号	12.4.1	12.4.1	9.1.2	13.1.1	9.1.2 13.1.1 13.1.2
情報セキュリティボリンーガイドラインの倒 メドラインの倒 女の番号	6.1.(7)	6.1.(7)	6.1.(8)	6.1.(8)⊕	6.1.(8)@
監査実施の例	監査資料のレビューと統括情報セキュリティ責任者又は情報となって大工を理者へのインタビューにより、職員等からのシアンが立確害の対する処理結果又は問系等の対象の記録をび採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。	監査資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機告、システム障害に対する処理結果又は問題が記録され、適切に保存されているか確かめる。	監査資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グビューにより、ネッレフークの接続制御、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が確かめる。	監査資料のレビューと総括情報セキュリティ責任者又は情報ン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ケーティングトランで、設定の不整合が発生しないように、フィイアサール、ルーク等の通信ソントウェア等を設定しているか確かめる。	監査資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が確かめる。
監査資料の例	□障害対応基準	□障害対応基準 □障害報告書 □障害時のシステム出力ロ グ	口ネットワーク設定基準	□ネットワーク設定基準 □ネットワーク構成図	ロネットワーク設定基準
路香源目	1)障害記録の記録及び保存に関わる 基準 基準 所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。	1)障害記録の保存 総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、障害記録が記録され、保存されている。	1)キットワークの接続制御、経路制御 総に開わる基準 総括情報セキュリティ責任者によって、ネット フークの接続制御、施路船舶等に関わる基 準が定められ、文書化されている。	前プライアウォール、ルータ等の設定 総括書報セキュリア・責任者によって、フィル グ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びに、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。	III) ネットワークのアクセス制御 総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。
今		0		0	0
Š	158	159	160	161	162
町	6.1. (7) 技術的コン 障害記録 セキュニピュー リティ タ及び オット ワーク		(8) ネットワー クの接続制 御、落路制 創等		

						情報セキュリ ティポリシーガ	関連する JISQ27002	
項目	No.	心須	監査項目	監査資料の例	監査実施の例	イドラインの例 文の番号	番号	留意事項
6. (5.1. (9) 技術的 コン 外部の者 セキュ ビュー が利用でき リティ タ及び めンダナー ネット の分離等 の管理	163		<ul> <li>1)外都の者が利用できるシステムの分 機能に関わる基準 総括情報セキュリテイ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。</li> </ul>	ロネットワーク管理基準	艦査資料のレビューと総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ダニーにより、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任めネッ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)	9.1.2 13.1.3	
	164		11)外部の者が利用できるシステムの分 機構システム管理者によって、外部の者が利 情報システムではついて、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。	<ul><li>□ネットワーク管理基準</li><li>□通信回線敷設区</li><li>□結線区</li></ul>	監査資料のレビューと総括情報セキュリティ責任者又は情報ンステム管理者へのイングビュー「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任のネットワーク及び情報ン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)	13.1.3	
(10) ケ部ネット ワークとの 機器制限 線器制限	165			□外部ネットワーク接続基準 □外部ネットワーク接続手続	□外部ネットワーク接続基準 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 □外部ネットワーク接続手続 報ンステム管理者へのイングビュー「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。 が文書化され、正式に承認されているが確かめる。	6.1.(10)	9.1.2 13.1.3 15.1.2 16.1.1	
	166	0	11.)外部ネットワーク接続の申請及び許可 可 情報システム管理者が所管するネットワーク 告外部ネットワークと接続する場合、CISO及 び結括情報セキュリティ責任者から許可を得 ている。	<ul><li>□外部ネットワーグ接続基準</li><li>□外部ネットワーグ接続手続</li><li>□外部ネットワーグ接続申請</li><li>書/承認書</li></ul>	□外部ネットワーク接続基準 監査資料のDレビューと統括情報セキュリティ責任者又は情 □外部ネットワーク接続手続 報システム管理者へのイングビュー「Cより、情報システム管 □外部ネットワーク接続申請 理者が可管するネットワークを外部ネットワークと接続する場 書/承認書  一人CISO及び総括情報セキュリティ責任者から許可を得て してSOか確かめる。	6.1.(10)©	9.1.2	
	167		間)外都ネットワークの確認 情報ンステム停車者によって、所管するネッ トワークと外部ネットワークを接続しようとする 場合には、接続しようとする外部ネットワーク が調査され、庁内ネットワークや情報資産に 影響が生じないことが確認されている。	□外部ネットワーク接続基準 □外部ネットワーク接続手続 □外部ネットワーク調査結果	□外部ネットワーク接続基準 監査資料のルビューと情報システム管理者へのイングビュー □外部ネットワーク接続手続により、接続にようとする外部ネットワークのネットワーク □外部ネットワーク調査結果 成 機器構成、セキュリティ技術等が調査され、庁内の全て ログネットワークのネットワーグ、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。	©.	I	・外部ネットワークの調査と が別えば、複称しようとする 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 とむい。
	168		<b>iv ) 外部ネットワークの現底による損害 暗境責任の担保</b> 接続にた外部ネットワークの瑕疵による損害 暗償責任が契約上担保されている。	<ul><li>□外部ネットワーク接続基準</li><li>□外部ネットワーク接続手続</li><li>□サービス契約書</li></ul>	□外部ネットワーク接続基準 監査資料のDレビューと情報システム管理者へのイングビュー □外部ネットワーク接続手続 により、接続した外部ネットワークの発売によう業務への影響 レ、破壊、改さ人スはシステムゲウン等による業務への影響 が生じた場合に対して対してあり、当該水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	15.1.2	

留意事項							
图							
関連する JISQ27002 番号	13.1.3	16.1.1	11.2.1 11.2.4 15.1.3	15.1.3	11.2.1 11.2.4 15.1.3	11.2.7	11.2.1 11.2.4 15.1.3
情報セキュリ ティポリシーガ イドラインの例 文の番号	6.1.(10)⊕	6.1.(10)⑤	6.1.(11)	6.1.(11)⊕	6.1.(11)@	6.1.(11)®	6.1.(12)
監査実施の例	監査資料のレビューと統括情報セキュリティ責任者又は情報・大スケム管理者へのイングニーにより、ウェブサーバ等をインケース・インケーネットに公開する場合、「片内ネットワークへの長入を 防御するため、外部ネットワークとの境界にファイアウォール 等が設置されたうえで接続されているか補かめる。	□外部ネットワーク接続基準 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 □外部ネットワーク接続手続報システム管理者へのインダニーにより、接続した外部 オ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規定される場合には、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。	監査資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ネステム管理者へのイングビューにより、複合機の調産、運用に関わる基準及び手継が文書化され、正式に承認されているが確かめる。	監査資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、複合機の構能、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。	監査資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ン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。	監査資料のレビューと統括情報セキュリティ責任者又は情報ンチスト管理者へのイングビューにより、複合機の運用を報ンする場合に複合機の電磁的配線媒体の全ての情報が採消又は再利用できないような対策がとられているが確かめる。	監査資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。
監査資料の例	<ul><li>□ ネットワーク管理基準</li><li>□ 通信回線敷設図</li><li>□ 結線図</li></ul>	□外部ネットワーク接続基準 □外部ネットワーク接続手続 □障害報告書	□複合機管理基準□複合機管理手続	□複合機管理基準 □複合機管理手続	□複合機管理基準 □複合機管理手続	□複合機管理基準 □複合機管理手続	□ 特定 用途機器管理基準 □ 特定 用途機器管理手続
監査項目	(4)ファイアウォール等の設置 ウェブサーバ等をインターネットに公開してい ウェダー、結構情報セキュリティ責任者又は情報システム管理者によって、外部ネットワーク との境界にファイブウォール等が設置されている。	Ⅵ・外部ネットワークの遮断 接続した外部ネットワークのセキュリティに問題が認められる場合、情報システム管理者 [によって、統括情報セキュリティ責任者の判断に従い、速やかに当該外部ネットワークが 物理的に進断されている。	1)権合機のセキュリティに関わる基準 及び手機 総括情報セキュリティ責任者又は情報シス アム管理者によって、複合機の調整、運用に 関わる基準及び手統が定められ、文書化さ れている。	<ul><li>1)複合機の調達要件 総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。</li></ul>	Ⅲ)複合機のセキュリティ散定 総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。	▶)複合機の情報の抹消 複合機の運用を下する場合、結括情報セ 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又は再利用 できないような対策がとられている。	<ul> <li>1)特定用途機器のセキュリティ対策 総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。</li> </ul>
必	0						
No.	169	170	17.1	172	173	174	175
道目	6. (5.1. (10) 技術的 コン 外部ネット セキュ ピュー ワークとの リティ タ及び 接続制限 ネット 等 ワーク の管理		(11)   後の義の   本かまり   アイ帝国				(12) 特定用途 機器のセ キュリティ 管理

重							
留意事項							
関連する 「JISQ27002 番号	9.1.2 10.1.1 13.1.1 13.1.3	9.1.2 13.1.3	9.1.2 10.1.1	13.2.1 13.2.3 15.1.2	13.2.1 13.2.3	13.2.1	13.2.1
情報セキュリティポリシーガイドラインの倒 女の番号	6.1.(13)	6.1.(13)⊕	6.1.(13)@	6.1.(14)	6.1.(14)⊕	6.1.(14)@	6.1.(14)③
監査実施の例	監査資料のレビューと総括情報セキュリティ責任者又は情報とステム管理者へのイングビューにより、無線LAN及びネシトワーッの路聴対策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。	監査資料のレビューと総括情報セキュリティ責任者又は情報ンオテム管理者へのインタビューにより、無線LANを利用する場合には解読が困難な暗号化及び認証技術が使用され、アクセスポイントへの不正な接続が防御されているか確かめる。	監査資料のレビューと総括情報セキュリティ責任者又は情報ンのインダニュー(より、情報の盗職等を財ぐため、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が確かめる。	監査資料のレビューと総括情報セキュリティ責任者又は情報ン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。	監査資料のレビューと統括情報セキュリティ責任者又は情報ン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。	監査資料のレビューと統括情報セキュリティ責任者又は情報ンステム管理者へのインタビューにより、大量のスペスメール等の法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。	監査資料のレビューと統括情報セキュリティ責任者又は情報ンステム管理者へのインダビューにより、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。
監査資料の例	ロネットワーク管理基準	□ネットワーク管理基準 □ネットワーク設計書	□ネットワーク管理基準 □ネットワーク設計書	□電子メール管理基準	□電子メール管理基準	□電子メール管理基準 □障害報告書	□電子メール管理基準
監查項目	) #機LAN及びネットワークの登職対 雑に関わる基準 総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LAN及びネット ワークの盗聴対策に関わる基準が定められ、 文書化されている。	11)無線LAN利用時の暗号化及び認証 技術の使用 無線LANを利用する場合、統括情報セキュリ イ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。	II) 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 終活情報セキュリティ責任者によって、機密 性の高い情報を数分ネットワークには暗号化 等の措置が講じられている。	1)電子メールのセキュリテイ管理に副 わる基準 総括情報とネュリティ責任者又は情報システム管理者によって、電子メールのドキュリ ティ管理に関わる基準が定められ、文書化されている。	1)電子メール転送制限 総括情報セキュリティ責任者者によって、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。	Ⅲ)メールサーバ連用の停止 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。	iv)電子メール送受信容量制限 総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。
		0			0		
ò	176	7.7.1	178	179	180	181	182
断	6. (5.1. (13) 技術的 コン 無線LAN セキュ ピュー 及びネット リティ タ及び ワールの盆 ネット 聴対策 ワール			(14) 無子メール のセキュリ ァイ衛用			

必須 監査項目 監査項目 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
V   <b>電子メールボックス等重制器</b>
<b>i ) 外都委託事業者の電子メールアドレ</b>   電子メール学理基準   ス利用についての取り決め   □業務委託契約書   外間委託事業者の作業員が行内に推胜して 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。
M)電子メールによる情報資産無断移ち   口電子メール管理基準   出し業止   総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信報資産を   無断で外部に持ち出すことができないよう指   置が講じられている。
<b>1)電子メールの利用に関わる基準</b>   口電子メール利用基準
<ul><li>前)電子メール和送業</li><li>電子メールの自動転送機能を用いた転送は □電子メール送受信ログ行われていない。</li></ul>
<b>    電子メールの業務が利用の禁止</b>
<ul> <li>iv)電子メール送信先期示の禁止</li> <li>□電子メール利用基準 職員等が複数人に電子メールを送信する場 □電子メール送受信ログ 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。</li> </ul>

图意事項							
関連する JISQ27002 番号	13.2.1 13.2.3 16.1.1	13.2.1 13.2.3	10.1.1 10.1.2 13.2.1 13.2.3	10.1.1 10.1.2 13.2.1 13.2.3	10.1.1 10.1.2 13.2.1 13.2.3	12.2.1	12.2.1
情報セキュリーティボリシーガ・イドラインの倒になる番号	6.1.(15)&		6.1.(16)	6.1.(16)©	6.1.(16)@	6.1.(17)	
監査実施 OA例	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グビューにより、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。	監査資料のレビューと情報システム管理者及び職員等~の $6.1.(15)$ ③ インタビューにより、外部~の不正な情報の持ち出し等を妨止するため、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が確かめる。必要に応じて、職員等~のアンケート調査を実施して確かめる。	監査資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・暗号化又はパネ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が確かめる。	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能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、暗号化又はバ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。	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喰かる。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。	監査資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グビューにより、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。	監査資本のレビューと情報システム管理者及び職員等~の 6.1.(17)① インタビュー、パンコンやモバイル端末の職器により、パンコンやアインが場上ですった。アンテイルが導入されていないや中バイル場はに許可なペンフトウェアが導入されていないをからない必要に応じて、職員等~のアンケート調査を実施して確かめる。
監査資料の例	電子メール利用基準	□電子メール利用基準	□電子メール利用基準□電子メール送受信ログ	□電子メール利用基準	□電子メール利用基準	□ソフトウェア導入基準/手続	□ソフトウェア導入基準/手続
監査項目	<ul> <li>V)電子メール観送信の報告</li> <li>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。</li> </ul>	<b>n)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</b> 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。	1)電子号名・暗号化等に関わる基準 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。	前)電子書名、暗号化又はバスワード数 が が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・暗号化又はバスワード設定の方法 を使用して送信されている。	) <b>暗号化方法及び暗号鍵管理</b> 外部に送るデータを暗号化する場合、GISO が定める方法により暗号化され、暗号機が管理されている。	i)ソフトウェアの導入に関わる基準及び 手機 総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。	ii )ソフトウェアの集断導入の禁止 バ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。
※ ※ ※ ※ ※ ※ ※ ※ ※ ※ ※ ※ ※ ※ ※ ※ ※ ※ ※		0					0
Š	190	191	192	193	194	195	196
野	6. 6.1. (15) 技術的コン 電子メール セキュ ピュー の利用制 リティ ネシト ワーク	財長()	(16) 瞻子署名· 暗号化			(17) 無許可ソフ ドウェアの 導入等の 禁止	

題意事項		・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。				
関連する JISQ27002 番号	12.2.1	12.2.1 ·不正 18.1.2 や著( 認識:)	12.1.2	12.1.2	12.1.2	13.1.1
情報セキュリ 関 ドイボリシーガ リ イドラインの例 番 文の番号	6.1.(17)@ 1.		6.1.(18)	6.1.(18)① 1.	6.1.(18)@ 1.	6.1.(19)
監査実施の例	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 イングレニーにより、業券上必要がフトレデルがある場合、 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評 可を得て、ソアウエ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。	監査資料のアビューと情報システム管理者及び職員等への (6.1.(17)③ インタビュー(より、不正にコピーな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。	監査資料のレビューと統括情報セキュリティ責任者又は情報ンステム管理者へのイングビュー「より、職員等がバソコンやモバイル結果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。	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が痛かめる。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。	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 イングビューにより、業務とパンペキンイル協案に対し 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会得で行 われているが確かめる。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。	監査資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又は情報とメテム管理者及び職員等へのインダビュー、勢務室及び呼阻反域の組築により、統括情報セキュリティ責任者の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指すが、職員等や外部委託事業者がインコンやキャイル端末をネットワークに接続していないが確かめる。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。
監査資料の例	<ul><li>□ソフトウェア導入基準/手続</li><li>続</li><li>□ソフトウェア導入申請書/承認書</li></ul>	□ソフトウェア導入基準/手続	□端末構成変更基準/手続 1	□端末構成変更基準/手続 1	□編末構成変更基準/手続 □端末構成変更申請書/承 認書	□ネットワーク利用基準
監査項目	間ソフトウェア導入の中請及び許可 業務上と要なソフトウェアがある場合、結合 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。	N) 不正コピー・ソフトウェアの利用禁止 不正にコピーされたソフトウェアは利用されていない。	1)機器構成の変更に関わる基準及び 手機 総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。	11)機器の改造及び増設・交換の禁止 バン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。	間)機器の改造及び増設・交換の申請及 び幹可 業務上パンニ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。	1)キットワーク接続の兼止 総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。
必須	0	0			0	0
Š.	197	198	199	200	201	202
野	6.1. (17) 株務的 コン 無許可ソフ セキュ ビュートウェアの リティ タ及び 導入等の ネット 禁止 ワーケー の管理		(18) 機器構成 の変更の 制限			(19) 無許可で のネット ワーク接続 の禁止

情報セキュリ 関連する ティボリシーガ JISQ27002 イドラインの例 番号 文の番号	(C 0.1.(20)① 9.1.2 (C 1.1.(20)① 9.1.(20)① 9.1.(20) (C 1.1.(20)① 9.1.(20) (C 1.1.(20)① 9.1.(20) (C 1.1.(20) (C	青 6.1.(20)② 16.1.2 引充 流	6 6.2.(1)①     9.1.1     ・ 開発、運用等を外部委託しており、重要な情報資産への9.2.2     アクセスを許可している場合り2.3     オンセスを許可している場合が、アクセス制御方角やアフかスが登出。       カン     9.2.3     セス管理基準等に外部委託り、に関するアクセス制御の事項が終まれていることが望ました。       か。     か。記述されていることが望ました。       り。     か。	青 6.2.(1)② 9.2.1 (ア) 9.2.2 対	育 6.2.(1)②     9.2.1     ・単に利用者Dの登録及び       ツ (ア)     9.2.2     変更の手続の有無を確認する       必     そのではなべ、承認者の妥当者の発当を確認することが望ましてい。       む。     し、。	情 (6.2.(1)②     9.2.1     ・単に利用者IDの抹消の手続か。       ッ (イ)     9.2.2     の有無を確認するのではないない。       ペない     人 承認者の娶当性などを確認するのとが望ましい。
監査実施の例	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。	監査資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グビューにより、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、対応されているが確かめる。	監査資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スは精験ンステムの重要度に応じたアクセス制御分針や、業務上の必要性や権限に応じた許可範囲等のアクシを管理基準が文書化され、正式に承認されているが確かめる。	監査資料のレビューと総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1Dの登録、変更、技消等の取扱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。	監査資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、ネットワークス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が確かめる。	監査資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グビューにより、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
監査資料の例	ロネットワーク利用基準	□ネットワーク利用基準 □通知書	□アクセス制御方針 □アクセス管理基準	□利用者1D敬极手続 □利用者1D登録・変更・抹消申請書 □利用者1D管理合帳	□利用者1D登錄·変更·抹消申請書 □利用者1D管理台帳	□利用者ID登録・変更・抹 消申請書 □利用者ID管理台帳
監查項目	<ul><li>1)業務以外の目的でウェブが閲覧されていな 業務以外の目的でウェブが閲覧されていない。</li></ul>	ii)業務以外の目的でのウェブ閲覧発見 時の対応 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。	<ul> <li>1)アクセス創御に関わる方針及び基準 総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。</li> </ul>	i)利用者IDの取扱に関わる手機 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、抹消等の取扱に関わる手続が定められ、文書化されている。	ii)利用者iDの登録・権限変更の申請 業務上においてネットワークスは情報システ ムにアクセスする必要あるいは変更が出た 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。	III)利用者IDの抹消申請業務上においてネットワーク又は情報システムにアクセスする必要がなくなった場合、当該職員等によって、統括情報セキュリティ責
心須	0		0	0	0	0
No.	203	204	205	206	207	208
斯	6. (6.1. (20) 技術的 コン 業務以外 セキュ ピュー の目的で リティ タ及び のウェブ関 ネット 覧の禁止	の管理	6.2. (1) アクセ アクセス制 X制御 第 X 対 アクセス制 アクセス制	(1) アクセス制 御 (イ) 利用者:D の取扱い		

留 記事 通						
関連する JISQ27002 番号	9.2.5	9.2.3	9.2.3	9.2.3	9.2.3	9.2.3
情報セキュリ ティポリシーガ イドラインの例 文の番号	6.2.(1)© ( <del>7)</del>	6.2.(1)③	6.2.(1)③ (7)	(4) (4)	(7) (7)	(E)
監査実施の例	監査資料のレビューと統括情報セキュリティ責任者又は情報ンテスト登重者へのインタニーにより、事管理部門と連携し、利用者口を定期的に開卸して、必要のない利用者口が登録されてないが、通剰なアクセス権限を付与していないがなどを定期的に点検しているか確かめる。	監査資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。	配査資料のレビューと統括情報セキュリティ責任者又は情報ン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を付与していないが、当該ID及びバスワードが厳重に管理されているが確かめる。	監査資料のレビューと統括情報セキュリティ責任者又は情報や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に承認されているが確かめる。	監査資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グビューにより、CUSOによって、統括情報セキュリティ責任者及び情報ン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、情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ資配者)に通知されているが確かめる。	監査資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、外部委託事業者に特権ID及びペスワードの変更を行わせていないが確かめる。
監査資料の例	□利用者ID衛朗記錄 □利用者ID管理台帳	□特権ID取扱手続 □特権ID認可申請書 □特権ID管理台帳	□特権ID敬母終 □特権ID管理台帳	□特權代行者承認書	□特權代行者通知書	□特権ⅠD政扱手続
田 町 棹 湖	<ul> <li>N 利用者1Dの点後 結括情報とネージャイ責任者及び情報シス 子上管理者によって、利用されていない1Dが 放置されてないか。点検されている。</li> </ul>	1)特権10の取扱に関わる手機 総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110の取扱に関わる手続が定め られ、文書化されている。	1) 特権D及びパスワードの管理 統括情報セキュリア・責任者及び情報シス 大名質理者によって、特権Dを付与する者が 必要最小限に制限され、当該D及びバス ワードが厳重に管理されている。	m)特権代行者の指名 総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、総括情報セキュリティ 育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。	N)特権代音の通知 CISOによって、統括情報セキュリティ責任者 及び情報システン管理者の特権代行者が述 からに関係者(統括情報セキュリティ責任 者、情報セキュリティ責任者、情報セキュリティ首任者、情報セキュリティ首任者、情報セキュリティ省世名、は対して表しる。	v)特権10の外部委託事業者による管理 の禁止 総括権権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10な びパスワードの変更を外部委託事業者には 行わせていない。
必	0	0	0			0
Š	209	210	211	212	213	214
蜃	6.2 (1) 投稿的 アクセ アクセス制 セキュ ス制網 網 リティ 利用者 ID の取扱い	(1) アクセス制 御 (ワ) ち権を付 与されたID の香粗等				

車通				7セスを認める 外部から下 接続するが することが望			
图 意				・外部からのアクセスを認める 場合であっても、外部から斤 レネットワーグに接続する必 要性などを確認することが望 ましい。			
関連する JISQ27002 番号	9.2.2 9.2.3	9.2.2 9.2.3	6.2.1 9.1.2 10.1.1	9.1.2	9.1.2	9.1.2	10.1.1
情報セキュリティポリンーガイドラインの例 メドラインの例 文の番号	6.2.(1)© (A7)	6.2.(1)③ (次)	6.2.(2)	6.2.(2)①	6.2.(2)@	6.2.(2)③	6.2.(2)⊕
監査実施の例	監査資料のレビューと総括情報セキュリティ責任者又は情報となった人を理者へのイングビューにより、特権D及びバスワードについて、利用者IDのバスワードよりも頻繁かつ定期のに変更する機能や、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。	監査資料のレビューと総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Dを利用する際は、Dを初期値以外のものに変更しているか確かめる。	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ダビューにより、外額のも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。	監査資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ダビューにより、職員等が外部から行行をかけて力で変のある場合、統括情報セキュリティ責任者及び当該情報システム管理者の許可を得ているか確かめる。	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。	酷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 ダビューにより、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。	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 ダビューにより、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妨御するために通信データの 暗号化等が行われているが確かめる。
監査資料の例	<ul><li>□ ネットワー/設計書</li><li>□ システム設計書</li><li>□ 特権ID取扱手続</li><li>□ 特権ID取扱手続</li><li>録</li></ul>	□特権D取扱手続	□リモートプセス方針 □リモート接続手続	□リモート接続許可申請書/許可書	□リモート接続許可申請書/許可書	□メットワーク設計書 □システム設計書	□ネットワーク設計書 □システム設計書
監査項目	<b>4) 特権D及びバスワードのセキュリティ 機能強化</b> 総括情報セキュリティ責任者及び情報シス デム管理者によって、特権Dのパスワード変 更や入力回数制膜等のセキュリティ機能が 強化されている。	41)特権10の10変更 総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1Dは初期値以外 のものに変更されている。	1)外部からのアクセスに関わる方針及 び手機 総括情報セキュリティ責任者によって、外部 がお信頼やキュリティ責任者によって、外部 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。	11)外部からのアクセスの申請及び許可 外部から庁内ネットワーグに接続する必要の ある場合、当該随口等によって、総括情報セ キュリティ責任者及び当該情報ンテムを管理する情報システム管理者の許可を得てい	III.)外報からのアクセス可能者の創機 総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。	N)外部からのアクセス時の本人確認機能 機 外部からのアクセスを認める場合、総括情報 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。	v)外部からのアクセス特の暗号化等 外部からのアクセスを認める場合、総括情報 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。
冷			0	0		0	
ö Z	215	216	217	218	219	220	221
順	6.2. (1) 技術的 アクセ アクセス制 セキュ ス制鋼 鋼 (ウ) リティ 特権を付 与されたID の管理等		(2) 職員等によ 必外部から のアケ部から のアウセス 等の制限				

No.	必	<b>万項目</b> カノ田総士のムナ-	監査資料の例		情報セキュリー ドイボリシーガ、イドラインの例 女の番号 (2000)	関連する JISQ27002 番号	昭彦華通
222	0	<b>セス用端末のセキュ</b> 利用するパソコン等の する場合、統括情報セ 情報システム管理者に (保の措置が講じられて	□リモート接続手続		6.2.(2)(6)	6.2.1	
223	0	個)外部から持ち込んだ端末のウイルス [ 機関等 格部から特ち込んだ端末を庁内ネットワーク ド接続する場合、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ている。	口端末接続時手続		6.2.(2)©	6.2.1	
224	0	画)公衆通信回線の接続 総括情報セキュリティ責任者及が情報シス 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グ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。	口端末接続時手続	監査資料のレビューと総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~のイクダビュー(より、公衆通信回線を)下が予ルトワーツ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積ること、、アクセス値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が策を講じ、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が確かめる。	6.2.(2)®	13.1.1 14.1.1	
225		1)自動業別の設定 総括指揮セキュリイ責任者及び情報シス [5 子と管理者によって、外類のキのネットワークの接続を許可する機器を自動的に識別するよう訳定されている。	□本小ワーク設計書□接総許可端末一覧	離査資料のレビューと総括情報セキュリティ責任者又は情報とネースが大力と増生ーへのインダニー「こだ)、最終を目動職別するよう設定(例えば、電子証明書やIPアドレス、MACアドレスによる観別情報の取得等)されているか確かめる。	6.2.(3)	13.1.1	
226		1)ログイン時のシステム散定 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。	□ンステム設計書 □セグイン園面	監査資料のレビューと情報システム管理者へのイングビューにより、ログイン時におけるメッセーシ及びログイン試行回数の制限、アケモスタイムアけの設定、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)	9.4.2	<ul> <li>ログイン手順では、許可され</li> <li>になたが目者に助けとなるようなかッセージ(例えば、ID</li> <li>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た。</li> </ul>

断		o N	必	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 イドラインの倒 女の番号	関連する JISQ27002 番号	田野寺
6.2. (5) 技術的 アグセ 認証 セキュ ス制御 の管 リティ	(5) 認証情報 の管理	227	0	1) <b>認証情報ファイルの書題</b> 統括情報セキュリティ責任者又は情報システム管理者によって、職員等の認証情報ファイルが厳重に管理されている。	□アクセス制御方針 □アクセス管理基準	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタにューにより、職員等のバ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)⊕	9.4.3	・職員等によるパスワードの取扱いについては、No.124~ 131も関連する項目であることから参考にすること。
		228	20° 0', we 1///	前) 仮パスワードの変更 総括情報セキュリティ責任者又は情報システム管理者によって発行された仮パスワードは、職員等によって、初回ログイン後直ちに変更されている。	□アクセス制御方針 □アクセス管理基準 □利用者1D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が確かめる。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)@	9.2.4	
		229	21K 3) : [/ 21K	前)酸配情報の不正利用防止 総括情報と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 不正利用名的比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 □アクセス管理基準 □利用者1D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グビュー「にお」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信かめ、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)@	9.2.5	
(6) 特権に 接続時 放続時 の制限	大 間 間	230	- 1 K	1)特権による接線時間の制限 情報システム管理者による 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。	<ul><li>□アクセス制御方針</li><li>□アクセス管理基準</li><li>□ネットワーク設計書</li><li>□システム設計書</li></ul>	監査資料のレビューと情報システム管理者へのイングビューにより、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)	9.4.2	・外部ネットワークとの接続制限については、No.157~62 も関連する項目であることから参考にすること。
6.3. ム第 ム署 ム署 人文文 本 神 総 本 様 本 本 本 本 本 本 本 本 本 本 本 本 本	調達	231	** 300 (0) (1) (2) (0.00)	1)権機システムの関連における情報セキュリティに関わる基準 総括情報セキュリティ責任者及び情報システムを理理とによって、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ンステム管理者へのインダビューにより、情報ンステムの開発、導入、保守等の調塞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.(1)	14.1.1	
		232	0	ii) セキュリティ機能の明記 情報システムを調達する場合、総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開報システム管理者へのインダビューにより、情報システム開発、導入、保守等の調査にあたり、アクセス制御機能やペスワード設定機能、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.(1)⊕	14.1.1	
		233	* - H 40	(ii) セキュリティ機能の調査 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 □セキュリティ機能調査結果	□調達仕様書 監査資料のレビューと総括情報セキュリティ責任者又は情 □セキュリティ機能調査結果 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.(1)@	14.1.1	

留意事項						
関連する JISQ27002 番号	14.1.1 14.2.5 14.2.7	14.1.1 14.2.5 14.2.7	9.1.1 9.2.1 9.2.2 9.2.3 9.2.6	9.1.1 9.2.1 9.2.2 9.2.3 9.4.5	12.5.1	12.5.1
情報セキュリティポリシーガイドラインの例文の番号	6.3.(2)	6.3.(2)⊕	6.3.(2)@ (7)	6.3.(2)@ (A)	6.3.(2)③ ⟨₹)	6.3.(2)® (~f)
監査実施の例	監査資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が確かめる。	艦査資料のレビューと情報システム管理者へのインダビュー 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が確かめる。 あか確かめる。 あわせて、システム開発の規則が定められているが確かめ る。	監査資料のレビューと情報システム管理者へのイングビューにより、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。	監査資料のレビューと情報システム管理者へのイングビューにより、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が確かめる。	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。	監査資料のレビューと情報システム管理者へのイングビュー により、利用が認められていないソフトウェブ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備か める。
監査資料の例	ロシステム開発基準	ロシステム開発体制図 ロシステム開発 規則	□開発用ID登録・削除手続 □開発用ID登録・削除申請 書 □開発用ID管理台帳	□アクセス権限設定書 □開発用ID管理台帳	□システム開発・保守計画	ロシステム開発・保守計画
監査項目	1)システム開発に関わる基準 総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。	#)システム開発における責任者及び作業者のの特定 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。	III)システム開発用IDの管理 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。	N)システム開発の責任者及び作業者 のアクセス権服設股 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。	V)システム開発に用いるハードウェア 及びンアトウェアの特定 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。	<b>4) 許可されていないソフトウェアの削除</b> 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。
冷		0		0		
O	234	235	236	237	238	239
通目	6.3. (2) 技術的システ 情報システ セキュム A開 Aの開発 リティ 発 導 中等					

原	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 関連する ティポリシーガ JISQ27002 イドラインの例 番号 文の番号	関連する JISQ27002 番号	盟急事項
6.3. (3) システ 情報システ ム開 ムの導入 発、導 (ア) 入、保 開発環境と 守等 通用環境	240	7.2.7.	<b>) 情報システムの導入に関わる基準</b>	□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学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が 確かめる。	6.3.(3)	12.1.4 14.2.8 14.2.9	
	241		) 開発環境と運用環境の分離    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ソステム運用環境    次分離されている。	□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.(3)⊕ (₹)	12.1.4	
	242			□システム開発・保守計画 □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ダビューにより、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.(3)⊕ (~)	14.2.8	
	243	71 010	N)移行に伴う情報システム停止等の影 [ 春の最小化 システム移行の際、情報システム管理者に よって、情報ン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。	ロシステム開発・保守計画 口移行手順書	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.(3)( <del>(7)</del>	14.2.8	
	244	72 5710	<ul> <li>*)情報システム導入時の可用性確認</li> <li>*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。</li> </ul>	□情報システム導入基準 □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ダビューにより、システム導入の際、障害によるシステム導ルや広域、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が確かめる。	6.3.(3)⊕ (≖)	14.2.5 15.1.2 15.1.3 17.2.1	

留意事項							
関連する JISQ27002 番号	14.2.9	14.2.9	14.2.9 14.3.1	14.2.9	1	1	1
情報セキュリ ドイポリシーガ イドラインの例 文の番号	(F)	©(E).	( <i>c</i> )	6.3.(3)② (エ)	6.3.(4)	6.3.(4)⊕	6.3.(4)@
監査実施の例	監査資料のレビューと情報システム管理者へのイググビューにより、着たに情報システム会導入する場合、既に稼動している情報システムに接続する前に十分な対験が行われているか痛かめる。	監査資料のレビューと情報システム管理者へのインダビュー 6.3 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 (イ) る操作確認が行われているか確かめる。	監査資料のレビューと情報システム管理者へのインダビューにより、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。	配着資料のレビューと情報システム管理者へのイングビューにより、他組織で開発された情報システムを受け入れる場合、開発した組織と対して名組織が、それぞれ独立したテストを実施しているか確かがあ。	監査資料のレビューと総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ダビューにより、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が確かめる。	配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 又は管理反域の行場発発のの関係、ファイルサーバ等の備 割により、ンテム開発・保守に関連する資料及でシステム 関連文書が紛失したり改さん等されないように保管されてい るか備かめる。	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 又は管理区域及び物務室の視察、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。
監査資料の例	□システムテスト計画書/ 報告書	<ul><li>□システムテスト計画書/ 報告書</li><li>□ユーザテスト計画書/報告書</li><li>告書</li></ul>	<ul><li>□システムテスト計画書/ 報告書</li><li>□ユーザテスト計画書/報告書</li><li>告書</li></ul>	□システムテスト計画書/報告書	□ンステム開発・保守に関連する資料等の保管装準 連する資料等の保管装準	<ul><li>□システム開発基準</li><li>□システム仕様書等</li><li>□ブログラム仕様書等</li></ul>	□システム開発基準 □システムテスト計画書/ 報告書
監査項目	1)導入前のラスト実施 新たに信権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試験が 行われている。	<ul><li>1) 凝似環境での操作確認 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権 認が行われている。</li></ul>	<ul> <li>III)個人情報及び機密性の高い生データの使用禁止</li> <li>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。</li> </ul>	N 独立した要け入れテスト 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。	1)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 総括標果セメリティ責任者及び情報シス アム管理者によって、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。	用)資料等の保管 借機シケテル管理者によって、システム開 発発保行関連する資料及びシステム関連 文書が適切に保管されている。	<b>III)テスト結果の保管</b> 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。
必	0		0			0	0
No.	245	246	247	248	249	250	251
道目	6. (3.3. (3) 技術的 システ 情報システ 信報システ でキュ ム陽 ムの導入 リティ 発、導 (イ) 人、保 テスト 中等				(4) ンステム圏 第・4年で 圏 (4:4年で 圏 (4:4年で ) (4:4年で 圏 (4:4年で ) (4:		

图 高事項							
関連する JISQ27002 番号	9.4.5	ı	ı	ı	12.1.2 14.2.2	12.1.2 14.2.2	12.1.2 12.6.1 14.2.2 14.2.4 14.2.9
情報セキュリティポリシーガイドラインの例 メアラインの例 文の番号	6.3.(4)③	6.3.(5)⊕	6.3.(5)@	6.3.(5)®	6.3.(6)	6.3.(6)	6.3.(7)
監査実施の例	監査資料のレビューと情報システム管理者へのイングビュー スは管理区域及で機務室の視線、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製消去や改さん等され ないような方法で保管されているか確かめる。	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。	監査資料のレビューと情報システム管理者へのイングビュー により、データの付割が理時にこちまそれのあるデータ抽 出条件の觀りやデータペース更新処理時の計算式のミスな と、故意又は過失による情報の改さん又は満れたを使出す 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。	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。	監査資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がピューにより、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。	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。	監査資料のレビューと情報システム管理者へのイングビュー により、連用環境のシステム保守状況を被まえて、開発・保 守用のソフトウェブ等を更新、又はバ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が確か める。
監査資料の例	□システム開発基準 □ソースコード	ロシステム仕様書等 □プログラム仕様書等	□システム仕様書等 □アログラム仕様書等 □アログラム仕様書等	□システム仕様書等 □プログラム仕様書等	<b>ロシステム変更管理基準</b>	<ul><li>□ンステム開発基準</li><li>□システム仕様書等</li><li>□プログラム仕様書等</li></ul>	□ンステム開発基準 □ンフトウェア管理台帳
監査項目	<b>ゕ)ッースコードの保管</b> 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。	1)データの入力処理時の正確性の確保 保 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。	前)データの内部処理時の正確性の確保 保証を表示して、、枚意文は過 情報システム管理者によって、、枚意文は過 大による情報の改さん、又は漏えいを検出す る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。	ii) データの出力処理時の正確性の確 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。	1)システムの変更管理に関わる基準 デム格情報セキュリテ、責任者及び情報シス デム管理者によって、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。	<ul><li>1)変更優麗の作成 情報システム管理者によって、情報システム を変更した場合、ブログラム仕様書等の変更 履歴が作成されている。</li></ul>	1)開発・保守用ソフトウェアの更新等 情報ン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、又はメペッチの適用 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。
冷巡	0					0	
ė	252	253	254	255	256	257	258
野	6.3 (4) 技術的システシステム開 セキュム開 発・保守に リティ 祭・薬 関連する 人、保 資料等の 中等 保管	(5) 情報システ ムにおける 入出力 データの正 なおける	# H K		(6) 情報システ ムの変更 管理		(7) 開業後保守 用のソフト ウェブの更 新等

图意事項						
関連する JISQ27002 番号	14.2.9	13.1.1	12.2.1	12.2.1	12.2.1	12.2.1
情報セキュリティポリンーガイドラインの例文の番号	6.3.(8)	6.4.	6.4.(1)⊕	6.4.(1)@	6.4.(1)③	6.4.(1)(4)
監査実施の例	監査資料のレビューと情報システム管理者へのイングビューにより、システム更著・統合に作り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日手順が策定されているか確かめる。	監査資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が確かめる。	監査資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又は情報セキュリティ責任者へのイングビュー「に」」、不正フログラムので大力でしていために、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、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が確かめる。	監査資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がの拡張を受けて、インターネットゲートリュイで、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がどがチェックされているか確かめる。	監査資料のレビューと紡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。	監査資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、所奪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。
監査資料の例	□統合時影響検討書 □システム統合手順 □異常時復旧手順	□不正プログラム対策基準 □不正プログラム対策手順	□不正プログラム対策基準 □不正プログラム対策手順 □不正プログラム対策ソフト ヴェブのログ	□不正プログラム対策基準 □不正プログラム対策手順 □不正プログラム対策ソフト ヴェアのログ	□不正プログラム対策基準 □不正プログラム対策手順 □職員等への周知記録	□不正プログラム対策基準 □不正プログラム対策手順
監査項目	1)システム更新又は統合時の検証等 情報ンタス全種担害によって、システム質新 文は統合時に伴ジスグ管理体制の構築、移 万法第合時に伴ジスグ管理体制の構築、移 登体制の検証が行われている。	1)不正プログラム対策に関わる基準及 び手順 総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。	1)外部ネットワークから受信したファイルのチェック 総括機製セキュリティ責任者によって、イン教と本がのグートウェイで外部ネットワート 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がチェックされて、エッログラムが含まれていないかどが・チェックされている。	11) 外部ネットワークへ送信するファイルのチェック 総括機能セキュリティ責任者によって、イングーネットのゲートウェイで外部ネットワーツ 今一ネットのゲートウェイで外部ネットワーク ・送信するファイルに不正プログラムが含まれていなりがチェックされている。	前)職員等への注意喚起 総括情報セキュリティ責任者によって、コン ビューケケ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。	N) 不正プログラム対策ソフトウェアの常 軽 総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。
必		0				
O	259	260	261	262	263	264
画	6.3. (8) 技術的システシステム更 セキュム A別 新文は統 リティ 第、準 合時の検 八、保 証等	6.4. 不正プ ログラ ム対策	(1) 総括清報 総括清報 トフィオエリ アイオエリ の措置事 国			

留意事項							
受田							
関連する JISQ27002 番号	12.2.1 12.6.1	12.2.1 12.6.1 14.2.2	ı	12.2.1	12.2.1 12.6.1	12.2.1 12.6.1 14.2.2	12.2.1
情報セキュリ ティポリシーガ イドラインの例 文の番号	6.4.(1)⑤	6.4.(1)@	6.4.(1)@	6.4.(2)⊕	6.4.(2)@	6.4.(2)③	6.4.(2)⊕
監査実施の例	監査資料のレビューと総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、サーバ及びベンコン等の確認により、不正プログラム対策ソフトヴェアのバターンファイルが最新のハターンファイルに更新されているか確かめる。	龍査資料のレビューと総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、サーバ及びペン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ヴェアが最新のバージョンに更新されているか。確かめる。	監査資料のレビューと総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又は情報セキュリティ責任者へのインダビュー、サーバ及びベン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確認しているソフトウェアであるか確かめる。	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、サーバ及びバンコン等の確認により、所掌するサー バ及びバンコン等の端末に、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。	館査資料のアドコーと指載システム管理者へのインケアコー、サースのスペンジン等の確認により、木正プログラム対策ソフトウェアのパターンフィイルが最終のパケーンフィイルに関節されているが確かめる。	雅香資料のアビューと指揮システム管理者へのインケアコー、サース及びパンコン等の確認により、サース及びパンコン等の確認により、導入された不正プログラス対策ソフトフェが最新のパージョンに更新されているが確かめる。	監査資料のレビューと情報システム管理者へのインダビュー により、インターネルに接続にていない、システムにおいて着 磁的記録媒体を使う場合、管理外電磁的記録媒体の使用 素比、不正プログラム対策ツアトウェア導入、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。
監査資料の例	<ul><li>□不正プログラム対策基準</li><li>□不正プログラム対策手順</li><li>□不正プログラム対策ソフト</li><li>ウェアのログ</li></ul>	□不正プログラム対策基準 □不正プログラム対策手順 □不正プログラム対策ソフト ヴェアのログ	<ul><li>□不正プログラム対策基準</li><li>□不正プログラム対策手順</li></ul> <li>□不正プログラム対策手順</li>	<ul><li>□不正プログラム対策基準</li><li>□不正プログラム対策手順</li></ul> <li>□不正プログラム対策手順</li>	□不正プログラム対策基準 □不正プログラム対策手順 □不正プログラム対策ソフト ウェアのログ	ロ不正プログラム対策基準 ロ不正プログラム対策手順 ロ不正プログラム対策ソフト ヴェアのログ	ロ不正プログラム対策基準 ロ不正プログラよ対策手順 ロ不正プログラム対策プリ ヴェブのログ
監査項目	<b>ソンペターンファイルの更新</b> 総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。	4) 不正プログラム対像ソフトウェアの更 新 指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パージョ ソに更新されている。	M)サポート終了ソフトウェアの使用禁止 然店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 に禁止され、ソフトウェアの切り替えが行われ ている。	i) 不正プログラム対策ソフトウェアの常 情報セキュリアイ管理者によって、所筆する 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。	# ) バターンファイルの更新 情報セキュリティ管理者によって、不正プログ ラム対策ソフトウェアのバダーンファイルが最 新のパターンファイルに更新されている。	間)不正プログラム対策ソフトウェアの更 新 情報セキュリティ管理者によって、不正プログ 与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。	N)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 インターネットに接続していないシステムによいて、電機的自動媒体を使ぶ場合、情報に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。
冷	0	0	0		0		
Š	265	266	267	268	269	270	271
豐	6. 技術的 不正プ 総括情報 セキュ ログラ セキュリ フテイ ム対策 ティ青任者 の措置事			(2) 情報システ ム管理者 の措置事 項			

					72
留意事項					無害化に関してはNo.24にで記載
四					化に関し、
					記載 記載
関連する JISQ27002 番号	12.2.1	13.2.1 13.2.1	13.2.1 13.2.1	12.2.1	12.2.1 13.2.1
情報セキュリティボリンーガイドラインの例文の番号	6.4.(3)⊕	6.4.(3)@	6.4.(3)③	6.4.(3)4	6.4.(3)⑤
監査実施の例	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、職員等がインコン、モイイル端末に、導入されている不正フログラム対策ソフトウェアの設定を変更していないが高がある。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。	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スはソフト ヴェアを取り入れる場合、不正プログラム対策ソアトウェアに 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。	監査資料のレビューと情報セキュリテイ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が確かめる。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。	監査資本のレビューと情報セキュリテイ管理者及び職員等 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、 不正フレグム対策ソフトウェアによるフルチェックが定期的 に実施されているが確かめる。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。	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、代電子メールを 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。
監査資料の例	ロ不正プログラム対策基準 ロ不正プログラム対策手順 ロ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基準 □不正プログラム対策手順 □不正プログラム対策ソフト ヴェアのログ	<ul><li>□電子メール利用基準</li><li>□不正プログラム対策基準</li><li>□不正プログラム対策手順</li></ul>	ロ不正プログラム対策基準 ロ不正プログラム対策手順 ロ不正プログラム対策ソフト ウェブのログ	□不正プログラム対策基準 □不正プログラム対策手順 □不正プログラム対策プリ ウェアのログ
監査項目	1)不正プログラム対策ソフトウェアの設 だ変更の禁止 ポソコン、モンベル端末に不正プログラム対 パソコン、モンベル端末に不正プログラム対 第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。	<ul> <li>11)データ等取り入れ時のチェック</li> <li>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。</li> </ul>	) <b>山 所 不明なファイルの 削除</b> 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。	N)不正プログラム対策ソフトウェアによ □不正プロンるフルチェックの定義的実施 □不正プロン 職員等の使用する端末に対して、職員等に □不正プロンテップ、不正プログラム対策ソフトウェアによる ウェアのログフルチェックが定期的に実施されている。	<ul> <li>V)ファイル送受信時のチェック</li> <li>添付ファイルが付いた電子メールを送受信す。□不正プロンる場合、職員等によって、不正プログラム対 □不正プログ第ソフトウェアによるチェック及び無害化処理 ウェアのログが行われている。</li> </ul>
冷		0	0	0	
Š	272	273	274	275	276
	(3) 藤貝等の 藤中事項				
一種	6.4. イエプ ログラ ル対策 人本対策				
	6. 技術的 セキュ リティ				

情報セキュリ 関連する ティボリシーガ US227002 イドラインの例 番号 文の番号	12.2.1 16.1.3	16.1.1 ・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.301~304も関連する項目であることが必参考にすること。	6.1.4 ・不正プログラム対策に関する情報については、外部の専 同等から支援を受けるおか、 全的なセキュリテイ機関、定 評のある刊行物、信頼できる インターネットサイ等からも 収集することが望ましい。
情報セキュリ 関連 ティボリシーガ JISQ イドラインの例 番号 文の番号	6.4.(3)@	6.4.(3)(T)	6.4.(4)
監査実施の例	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 へのイングビューにより、総括情報セキュリティ責任者から提供されるティ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。。	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 へのインダビューにより、不正アログラムに感染した場合文 は感染が疑われる場合、ペソコン等の端末であれば、LAN ケーブルが即時取みされているか確かめる。セパル端末 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。	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 6-4.(4) キュリティ責任者又は情報システム管理者へのイングビュー ドより、実施している不正プログラム対策ではスイ・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が確かめる。
監査資料の例	□不正プログラム対策基準 □不正プログラム対策手順	<ul><li>□ 不正プログラム対策基準</li><li>□ 不正プログラム対策手順</li><li>□ 情報セキュリティインシブ</li><li>ント報告書</li></ul>	<ul><li>□不正プログラム対策基準</li><li>□不正プログラム対策手順</li><li>□業務委託契約書</li></ul>
監査項目	<b>が)ウイルス情報の確認</b> 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。	<b>ゴ) 不正プログラムに感染した場合の対象</b> <b>処</b> 不正プログラムに感染した場合又は感染が 形むれる場合、職員等によって、パシコン等 の端末のLANケーブルが即時取外されてい 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。	1)専門家による支援体制の確保 実施している不正プログラム対策では不十分 □不正プログラム対策手順 な事権が発生した場合に備えて、統括情報 □業務委託契約書 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。
必		0	
No.	772	278	279
重	6. 6.4. (3) 技術的 不正づ 職員等の セキュ ログラ 遠守事項 リティ ム対策		(4) 専用家の 支援体制

情報セキュリ  関連する   ティポリシーガ JISQ27002   イドラインの例 番号   留意事項   文の番号   本号	監査資料のレビューと統括情報セキュリティ責任者又は情 6.5. 16.1.1 ・ネットワークの管理について 鞠システム管理者へのイングビューにより、不正プクセス対 第に関わる基準及び対応手順が文書化され、正式に承認 16.1.3 16.2場は・予項目であること されているか確かめる。 16.1.4 から参考にすること 16.1.5 16.1.5 16.1.1 16.1.5 16.1.1 16.1.1 16.1.1 16.1.1 16.1.1 16.1.1 16.1.1 16.1.1 16.1.1 16.1.1 16.1.1 16.1.1 16.1.1 17.1.1 17.1.1	監査資料のレビューと総括指輪セキュリティ責任者又は情 6.5.(1)(1) - ・ファイアウォールの設體につ解システム管理者へのイングビューにより、使用されていないボートが開鎖され、不正アクセスによる侵入を防止しているがある。 にすることのも参考ない確かめる。	監査資料のレビューと統括情報セネュリティ責任者又は情 [6.5.(1)② ー 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。	監査資料のレビューと総括情報セキュリティ責任者又は情 (6.5.(1)③ 16.1.2 郷システム管理者へのイングビューにより、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嫌かめる。	監査資料のレビューと統括情報セキュリティ責任者又は情 6.5.(1)④ 16.1.2 親システム管理者へのインダビューにより、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設定を行ったファイル等にからないで、企場的に当該ファイルの改さんの有無が検査されているが確かめる。
開本資料の函	<ul> <li>□不正アクセス対策基準</li> <li>■監査資料のレビューと総 □不正アクセス対応手順</li> <li>無システム管理者への 第に関わる基準及び対 されているか確かめる。</li> </ul>	<ul><li>□ ネットワーク構成図</li><li>□ ネットワーク構理記録</li><li>ψンステム管理者への</li><li>□ ファイアウォール設定</li><li>□ ファイアウォールログ</li><li>るか構かめる。</li></ul>	<ul><li>□不正アクセス対策基準 監査資料のレビューと統括情報セ</li><li>□不正アクセス対応手順 報システム管理者へのインタビューレンステム監視手順 い不要なサービスが削除又は停止る侵入を防止しているが確かめる。</li></ul>	□ 不正アクセス対策基準 監査資料のレビューと総 □ 不正アクセス対応手順 報ンステム監視手順 5ウェブページのデーサー □ 情報セキュリティインシデ リティ責任者及び情報に アト報告書 でいるか確かめる。	<ul><li>□ネットワーク管理基準</li><li>■監査資料のレビューと第 □システム設定検査記録</li><li>乗りステムと関連を全のようによった。キュー・ハッキュー・キュー・ハー・カー・</li></ul>	り 設 た 会 打 シニン アム アン アン アン アン アン アン の ひど 入 の 有 無 が 検 査 !
質質	対応手順       総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。	<b>) 未使用ボートの弱態</b>	<b>) 不要なサービスの削除又は停止</b>    「不要なサービスの削除又は停止されて、不要    不正なサービスが削除又は停止されている。    ロシア	・ウェブページ改さんの後名	<b>イルの検査</b> 慣任者によって、重要 o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。
No. 	280	281	282	283	284	
野	6.5. 技術的 不正プ セキュ クセス リティ 対策	(1) 総括清報 セキュリ ティ責任者 の措置事		<b>L</b>		

道目		No.	必須	監查項目	監査資料の例	監査実施の例	情報セキュリーティポリシーガ、イドラインの例 マイドラインの例 文の番号	関連する JISQ27002 番号	图意事項
6. (6.5. 技術的 不正プ ルキュ クセス リティ 対策	(3) 記録の保 存	287		1) 記録の保存 サーバ等に犯罪の可能性がある攻撃を受け た場合、CISO及び結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 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。	<ul><li>□緊急時対応計画</li><li>□情報セキュリティインンデント報告書</li><li>□ログ</li></ul>	監査資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ダビューにより、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が確かめる。	6.5.(3)	6.1.3 6.1.4 16.1.7	・ログの取得及び保管についてはNo.146~149も関連する ではNo.146~149も関連する ること。 ・特性キュリティインシデン ・特性時の対応については、 No.301~304も関連する項目 であることから参考にすること。
	(4) 内部からの 攻撃	288		1)内部からの攻撃の監視 術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、職員等及び外部委託 事業者が使用しているパッ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やがある	□鑑末ログ□監視記録	監査資料のアビューと統括情報セキュリティ責任者又は情報セネンフンが選手をのインタビューにより、職員等及び外的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中・バ等や外部のサイトに対する攻撃が監視されているか確かめる。	6.5.(4)	16.1.2 16.1.3	・情報システムの監視については、No.288~291も関連する項目であることから参考にすること。 すること。
	(5) 職員等によ る不正アク セス	289		1)職員等の不正アクセスに対する処置 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と 子ンが哲理者によって、当該職員等が所属 する課金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 □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 報セキュリテ・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ウ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が確かめる。	6.5.(5)	7.2.3	・職員等の違反行為に対する 対応については、No.312~ 3145関連する項目であること から参考にすること。
	(6) サービス不 能攻撃	290		1)サービス不能攻撃に対する対策 統括情報セキュリティ責任者及び情報システム管理者によって、システムに対するサーイスを対撃を切べたが、情報システムの可用性を確保する対策が議じられている。	<ul><li>□不正アクセス対策基準</li><li>□不正アクセス対応手順</li><li>□システム監視手順</li><li>□システム監視手順</li></ul>	監査資料のレビューと総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 ヒューにより、サービス不能攻撃対策して、以下の管理策 が実施されていることを確かめる。 ・情報システムの技術的な対策 ・通信事業者サービスの利用による対策 ・債報システムの監視及び監視配縁の保存 ・情報システムの監視及び監視配縁の保存 さらに、上記対策のモニグリングの実施有無を確かめる。	6.5.(6)	1	
	(7) 標的型攻 驟	291	,,	1)権的型政権に対する対策 統括情報セキュリティ責任者及び情報システム管理者によって、標的型攻撃対策として た的対策や入口対策、内部対策が講じられている。	ロ不正アクセス対策基準 ロネエアクセス対応手順 ロシステム監視手順	監査資料のレビューと総括情報セキュリテイ責任者又は情報セキュリテイ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、標的型攻撃対策として、以下の管理策が実施、高齢れていることを備かめる。 ・標的型攻撃メール対策としての人的対策 ・電路的記録は経路日での収集対策となる人の対策 ・ネットワーの通信を監視する等の内部対策 ・ネットワーの通信を監視する等の内部対策 ・ネットワーの通信を監視する等の内部対策 ・ネットローとの通信を監視する等の内部対策 ・ネートローとの通信を監視する等の事態が衰 ・ネートローとの通信を監視する等の事態が衰 ・まして、上記対策のモニグリングの実施有無を確かめる。	6.5.(7)	I	

留意事項		・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。		・不正プログラムの対策につ いては、No.251~2705間連 する項目であることから参考 にすること。	
		・セキュリティ 情報のIQ集先 なく、複数かい とが望ましい。		・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	
関連する JISQ27002 番号	12.6.1	12.6.1	12.6.1	12.6.1	12.6.1
情報セキュリ ティポリシーガ イドラインの例 文の番号	6.6.	6.6.(1)	6.6.(1)	6.6.(2)	6.6.(3)
監査実施の例	□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ダビューにより、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。	□セキュリティホール関連情 監査資料のレビューと統括情報セキュリティ責任者又は情報の通知記録 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、情報ンステムを所管する消暑等関係者間で共有されているが確かめる。	監査資料のレビューと総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グビューにより、セキュリティホールの緊急度に応じてイシッチが適用され、ソフトウェアが更新されているか確かめる。	監査資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。	□情報セキュリティ関連情報 監査資料のレビューと統括情報セキュリティ責任者又は情報となっての他の一に別ない。 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 て検討しているが確かめる。
監査資料の例	□セキュリティ情報収集基準	□ セキュリティホール関連情報の通知記録	□パッチ適用情報 □パッチ適用記録	□職員等への周知記録	□情報セキュリティ関連情報 ひ)通知記録
路香項目	1)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 発の情報化は、上リティ賞任成の情報システム管理者によって、セキュリティが一般シア エア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。	<b>サセキュリテイホールの情報収集及び 共有</b> <b>共有</b> <b>サイボ</b> ・	■リンストウェアの更新 本語情報やマニリティ責任者及び情報シス テム管理者によって、セキュリティホールの緊 急度に応じてペッチが適用され、ソフトウェア が更新されている。	1) 不正プログラム等のセキュリティ情報 の収集及び周知 総括指揮と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。	<ul> <li>1)権報セキュリティに関する情報の収 業及び共有 総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 する情報が収集され、関係者間で共有され ている。</li> </ul>
冷			0		
Š	292	293	294	295	296
重	6.6. 技術的 セキュ セキュ リティ リティ 精報の 収集	(1) セキュリ アイポート に関する者 無の反称・ 井本及び ソフトケエア の国新籍		(2) 不正プログ テム等のセ キュリティ 帯報の収 維・周知	(3) 情報セキュ リテムに関 する情報の サお情報の 大寿

項目	ON	必須	監査項目	監査資料の例	監査実施の例	情報セキュリ 関連する ティポリシーガ JISQ27002 イドラインの例 番号 文の番号	関連する j JISQ27002   番号	留意事項
7. 7.1. 連用 情報シ ステム の階視	297		1)情報システムの監視に関わる基準 総括情報と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 シンステムの援助状況の監視に関わる基準が 定められ、文書化されている。	レシステム運用基準	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セキュリティ責任者又は情報システム管理者へのイングニーにより、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.	12.4.1	・監視の方法には、侵入検知 シネテム(IDS) 等の監視の他 の専門システムの方法 の他に、対象システムのログ による監視がおる。
	298		■ 1 )情報システム及びネットワークの常 時期が が指情報セキュリティ責任者及び情報シス が出情報とよって、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。	<b>□システム運用基準</b> □監視記録	監査資料のンピ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ダビューにおり、セキュリティに関する事業を検知するため、ネットワーク及び情報システムが、常時監視されているが確かめる。	7.1.©	12.4.1	・監視結果は定期的に見直 大工なアクセンなどの情報セキュリティインシデントの 報セキュリティインシデントの 手兆がないか、信検することが 望ましい。
	299		間)時期の同期 総括情報とよって、重要なアクセスログ等 子と管理者によって、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□時刻設定手順	監査資料のレビューと統括情報セキュリティ責任者又は情報を含みても管理者へのイングニーに対い、アシセスログ等の国施として正確性を確保するなか、重要なアクセスログ等も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.@	12.4.4	
	300	0	N)外部接続システムの常時監視 総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ステムが常時監視されている。	□システム運用基準□監視記録	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインダビューにより、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	15.2.1	

点	o N	必	語	監査資料の例	監査実施の例	情報セキュリ ディポリシーガ イドラインの例 女の番号	関連する JISQ27002 番号	图章
7. 7.2. (1) 通用 精報セ 適合状況 キュリ の確認及 ティポ び対処 リシー り適合 狭況の 強語。	301		1)情報セキュリティボリシーの連守状 気の確認及び問題発生時の対応に関わ 各基準 総括性 総括性をコリティ責任者又は情報セキュ ジイラ質と者によって、情報セキュリティボリ 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。	□情報セキュリティボリシー □ンステム運用基準 □情報セキュリティインンデ ント報告手順 □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、情報セキュリティがリシーの遵守状況にこ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が確かめる。	7.2.(1)	16.1.1 16.1.2 16.1.3 18.2.2 18.2.3	
	302		1)情報セキュリティボリシーの連守状 気の離臨 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、情報セキュリティが 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。	□情報セキュリティボリシー □システム運用基準 □のイナンシアインシデ ント報告手順 コ情報セキュリティインシデ ント報告書 コ自己点検実施基準 □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賞 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及び総括情報セキュリティ責任者に報告されているが確かめる。	7.2.(1)@	16.1.1 16.1.2 16.1.3 18.2.2	
	303	0	Ⅲ)発生した問題への対応 CISOによって、情報セキュリティポリシー選 中上の問題に対して、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 □情報セキュリティインシデント報告書 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ボリシー遵守上の問題に対して、適切から速やかに対処されているか確かめる。	7.2.(1)@	18.2.2	
	304	0	N)システム設定等における情報セキュリティオリシーの選中状況の確認及び問題発生時の対処 総括情報セキョ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ョリティボリシーの遵守状況について、地で規助らに確認が行われ、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。	□情報セキュリティボリンー □×ケスル運用基準 □情報セキュリティインシデ ント報告手順 □情報セキュリティインシデ フト報告手順 □信報を発売事業 □自己点検集施基準	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をキュリティ責任者又は情報シテンケム管理者・のんングとニーにより、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だりシーの遵守状況について定期的に確認が行すが、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)©	16.1.1 16.1.2 16.1.3 18.2.2	

留意事項					- 緊急時対応計画について は、No.301~304も関連する 項目であることから参考にす ること。
图用					・聚急時対応計画について は、No.301~3045関連・ 項目であることから参考にす ること。
関連する JISQ27002 番号	12.4.1	12.4.1	16.1.1	16.1.1	16.1.1
情報セキュリ ティポリシーガ イドラインの例 文の番号	7.2.(2)	7.2.(2)	7.2.(3)	7.2.(3)①	7.2.(3)@
監査実施の例	監査資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、不正プウセス、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ンコン、モバイル端末及び電磁的配録媒体等のログ、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が確かめる。	監査資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ダビューにより、不正アカセス、不正アカセス、不正アカセスを到達な参加者の対象に、GISO及びGISOが指名した者によって、職員等が使用しているパッコン、モバイル告末及び電路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。	監査資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にコーにより、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。	監査資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がリティがリアーニにより、情報セキュリティがリアーに対する違反行為が発見された場合、国ちに統括情報セキュリティ首と指表の情報セキュリティ管理者に報告されているか確かめる。	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人の人グとコーにより、情報セキュリティガ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と及ぼす可能性があると統括情報セキュリティ 責大な影響と及ぼす可能性があると続指情報セキュリティ 責任者が判断した場合、緊急時対応計画に従った対処が 行われているが確かめる。
監査資料の例	□ 情報セキュリティボリシー □ 利用状況調査基準	□利用状況調查結果	□情報セキュリティインシ·デント報告手順 ント報告手順	ロ権報セキュリティインンデント数台手順 ロ権報セキュリティインンデント数台書	□情報セキュリティインシデント数告手順 「情報セキュリティインシデ ント報告書 □繁急時対応計画
監査項目	1)パリコン、モバイル端末及び電磁的 配線媒体等の利用状況の調査に関わる 基準 (1800度が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。	前)パリコン、モバイル端末及び電磁的 配像媒体等の利用状況の調査 不正了かセス、不正了がプル等の調査のた かた、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。	1)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 総括情報とキュリティ責任者又は情報とキュ リアィ責任者によって、情報とキュリティボリ 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。	<ul> <li>1)情報セキュリティポリシー違反発見 時の報告 情報の年本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 総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。</li> </ul>	間)発見された遺反行為に対する対処 情報セキュリティがジン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 にす可能性があると統括情報セキュリティ 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。
冷				0	0
No.	305	306	307	308	309
項目	7. 7.2. (2) 通用 情報セパンコン、 キュリ モバイル語 テイボ 森板で簡 リシー 森的記録 の遵守 媒体等の 狭況の 利用状況 種認 調査		(3) 機震車等の 製品機 機合機務		

情報セキュリ 関連する ティボリシーガ JISO27002 イドラインの例 番号 文の番号		セキュリティ責任者又は情 7.3.(1)~(2) 16.1.1 ビューにより、緊急時対応 17.1.2 5。	セキュリティ責任者又は情 7.3.(3) ー ビューにより、業務継続計 整合性が確保されているか	セキュリティ責任者又は情 7.3.(4) 17.1.3 ピューにより、情報セキュリ リティを取り巻く状況の変化 要に応じて緊急時対応計
監査実施の例	監査資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ーとが活情報でキュリー報子に表ったバングアン。「こより、情報セキュリティインシーン。 オイバングアン、情報セキュリティがリン・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、以は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必る。	□緊急時対応計画 □情報セキュリティ委員会議 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 事験 計画が定められているか確かめる。	監査資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。	監査資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
監査資料の例	□情報セキュリティボリンー	□緊急時対応計画 □情報セキュリティ委員会議 事録	<ul><li>□ 業務継続計画</li><li>□ 情報セキュリティボリシー</li><li>□ 緊急時対応計画</li></ul>	□緊急時対応計画 □情報セキュリティ委員会等 の議事録
監査項目	1)緊急時対応計画に関わる基準 が活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 今又は発生するおぞ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。	<ul><li>i) 緊急時対応計画の策定</li><li>CISO ズは情報セキュリテイ委員会によって、 緊急時対応計画が定められている。</li></ul>	) 実務機構計画との整合性確保 業務機能計画を策定する場合、業務機能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。	1)緊急時対応計画の見直し 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。
必		0		
ö Ž	310	311	312	313
屈	7. 2.3 2.3 3.4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4	(1) 聚物等 水等等 水等量 (2) 水等等 水等等 水等等 水等等 水等等 水等等 水等等 水等	(3) 業務継続 計画との整 合性確保	(4) 緊急時対 応計画の 見直し

		继	I	
留意事項		・例外措置は単に適用を排除 するだけでなべ、リスグにがじ 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。		
関連する JISQ27002 番号	I	I	I	I
情報セキュリー ドイポリシーガ、 イドラインの倒 女の番号	7.4.	7.4.(1)	7.4.(2)	7.4.(3)
監査実施の例	監査資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グビューにより、例外指配を採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。	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グビューにより、情報セキュリティ関係 規定の適等が困難な状況で行政事務の適正な遂行を継続 したければたらない場合、選手事項とは異なる方法を採用 すること又は選手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 が取られているか確かめる。	配置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グビューにより、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能のときは、例外措置実施後速やかいCUSOに報告されているか確かめる。	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 グビューにより、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が確認されているが確かめる。
監査資料の例	<b>□何外措置対応基準/手続</b>	□例外指置吳施報告書 □例外措置吳施報告書	口例外措置実施報告書	□例外措置車請書/許可書 □例外措置実施報告書
器 查 通	1) 例外権電に関わる基準及び対応手 総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、例外措置を採る場合 の基準及び対応手続が定められ、文書化さ れている。	1) 例外指電の申請及び許可 情報セキュリティ関係規定の選件が困離な 状況で行政事務の適正改遂行を継続しなければならない場合。 ればならが、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取られている。	1)緊急時の例外措置 行政事務の受付に緊急を要する等の場合で かって、例外指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ン 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。	i)例が権置の申請書の管理 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。
冷		0	0	
ò	314	315	316	317
四	7. 7.4. 通用 例外皆 圖	(1)   例外措置   の許可	(2) 聚急時の 例外措置	(3) 例外措置 の中請書 の管理

18.1.1 18.1.2 18.1.3 18.1.4 18.1.5	18.1.1 18.1.2 18.1.3 18.1.4 18.1.5
7.5.	7.5.
監査資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又は情報セキュリティを「本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。	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 7.5. でのイングローに対し、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が確かめる。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。
□関連法令等一覧	□関連法令等一覧
1) 遵守すべき法令等の明確化 総括情報セキリアイ責任者によって、職員 等が職務の遂行において遵守すべき情報セキリティに関する法令等の一覧が定めら た・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。	<b>i) 法令遵守</b> 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。
318	319
7. 7.5. 福用 法令議 中	
	7.5.     1.) <b>建やすべき法令等の明確化</b> 間連法令等一覧 監査資料のレビューと終指情報でキュリティ責任者 X 12 情報をなった。 (報告報報をオーリティ責任者 X 12 情報を 12 ままり 2 情報を 12 ままり 2 情報を 12 ままり 3 様 2 情報を 12 ままり 3 株 2 まり 3 株 3 株 3 株 3 株 3 株 3 株 3 株 3 株 3 株 3

7.2.3	7.2.3 16.1.1 16.1.2 16.1.7 18.2.2	7.2.3 16.1.1 16.1.2 16.1.7 18.2.2	7.2.3 16.1.1 16.1.2 16.1.7 18.2.2
7.6.(1)	7.6.(2)	7.6.(2)⊕ ~@	7.6.(2)®
監査資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グビューにより、情報モキュリティオリンーに違反した職員等及びその監督責任者が、その重大性、発生した事業の状況等に応じて、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。	監査資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グビューにより、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が確かめる。	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、情報ンステム管理者、信報ンステム管理者へのイングビュー「こより、職員等による情報セキュリティポリン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が確かめる。	□情報セキュリティ塗反時の 監査資料のレビューと総括情報セキュリティ費任者又は情報な手ュリティ費任者及び情報セキュリティ管理者へのイン ロ通知書 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の 善がみられたい場合、総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の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。
□情報セキュリティボリンー	□情報セキュリティボリシー □情報セキュリティ違反時の 対応手順	□情報セキュリティ違反時の対応手順 対応手順 □通知書	□情報セキュリティ遊反時の 対応手順 □通知書
1) 意味処分の対象 都括情報セキュリティ責任者によって、情報 セキュリティボリンーに違反した職員等及び その監督責任者が地方な務員法による総称 処分の対象となることが定められ、文書化さ れている。	1)違反時の対応手順 総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。	<ul><li>1) 関係者への通知 職員等による情報セキュリティボリシーに違 反する行動が確認された場合、関係者に通知、適切な措置を求めている。</li></ul>	<ul> <li>開う情報システム使用の権利の制限 情報セキュリティ管理者等の指導によっても 整がみられない場合、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の使用を停止又は 刻奪し、関係者に通知されている。</li> </ul>
0			
320	321	322	323
7. 7.6. (1) 連用 際政処 磐成処分 分等	(2) 静 対 対 対 対		
	7.6. (1)         1) 機成的分の対象         口情報セキュリティボリシー 監査資料のレビューと総括情報セキュリティ責任者ではつくが指揮をよって、情報 報告キュリティがクーにより、情報・キュリティがクーに違反した職員等及び今の監督責任者が、そ・キュリティがソンーに違反した職員等及び今の監督責任者が、そんがリンーに違反した職員等及び今の監督責任者が、そんがリンーに違反した職員等及び今の監督責任者が、その監督責任者が、その監督責任者が、その監督責任者が、その監督責任者が地方公務員法による懲戒 の監子性、発生した事業の状況等に応じて、地方公務員法による数据 たいる。           320         0 少分の対象となることが定められ、文書化さ れている。         となることが定められ、文書化さ されている。確かめる。         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。		1.8 表 色

o N	必	監査項目監査項目・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	監査資料の例 □外部参补管理基準	<b>監査実施の例</b> 監査実施の例 監査資料のアピューン総括情報セキュリティ責任者又は情	情報セキュリ ドイボリシーガ イドラインの倒 女 人ドラインの倒 女 女の番号	関連する JISQ27002 番号	留意事項留意事項・情報セキュリティポリン一等
		報セキュ   17場合   定めら		- 作式		15.2.2 15.2.2 15.2.2	様件事項の外部を指揮業者 に対する説明義務について は、No.88~994関連する項 目であることから参考にすること
	0	1)外部委託事業者の認定基準 「外所委託 事業者選定の際、委託内容に応じた情報セ 「サービキュリティ対策が確保されていることが確認さ カタログ れている。	<ul><li>○ 外部委託事業者選定基 単 カケログ</li><li>カクログ</li></ul>	□外部委託事業者選定基 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 準 ロサービス仕様書(サービス 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っカロソ) あか確かめる。	8.1.(1)①	14.2.7 15.2.1	・外部委託事業者適定基準 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 難解しているか」、委託業務 用解しているか」、委託業務 保会れているか」などの項目 が含まれているとが望まし い。
		) <b>小部委託事業者の選定</b>   「情報セキュリティ管理者によって、情報セ キュリティマネジ・ストマステルの国際規格の   「認証取得状況、情報セキュリティ監査の実施	<ul><li>□外部委託事業者選定基準</li><li>準</li><li>□サービス仕様書(サービスカタログ)</li></ul>	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、外部委託事業者の選定の際に、情報セキュリ ティマネジメントシステムの国際規格の認証取得状況、情報 セキュリティ監査の実施状況等が参考にされているか確か める。	8.1.(1)@	14.2.7 15.2.1	
	0	1) クラウドサービスの事業者選定  情報セキュリティ管理者によって、情報の機 登   発生に応じたセキュリティレベルが確保され   でいるシラヴドサービスが選定されている。	□外部委託事業者選定基 単 単 ロークラウドサービス利用基準 ロサービス仕様書(サービス カタログ) ロクラウドサービス事業者選 に記録	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[に対)グラゲナーとスの利用の際に、機密性の高い 情報を少ラバチナービスに解する場合は、以下の管理策が 実施されているサービスを選定しているが確かめる。 ・No.316~3170監査項目を選だしている ・日本の法令の範囲内で運用している	8.1.(1)©	15.1.2 15.2.1 15.2.2	

留意事項	・再奏指は原即禁止である が、例外的に再奏指を認める 場合には、再奏指事業者に おける情報セキュリティ対策 が十分取られており、外部奏 指事業者と同等の水準である こと確認した上で許可した ければならない。 ・契約書において、再奏託事 業者の監督についても規定さ れていることが望まし。	・外部委託事業者の情報セキュリティボリシー等の遵守事 項については、No.98~99も 間様する項目であることが 参考にすること。 契約事項の遵守状況のは が、中分なセキュリティ対策が たれていることを確認すると 要があり、特に、再委託の制 限、情報の特ち出しの禁止、 業務等了後のデータの返還・ 機乗、支給以外のバッコンの 使用について、違反がないが 確認することが必要である。
関連する ' JISQ27002 番号	15.1.2	15.2.1 15.2.2
情報セキュリ ティポリシーガ イドラインの例 文の番号	8.1.(2)	8.1.(3)
	監査資料のレビューと情報セキュリテー責任者欠は情報シスケム音程者へのイクビューにより、外部委託事業者との同で結結される契約書に必要に応じて次の情報セキュリテー要性が明記されているか確かめる。・情報セキュリティボリン・及び情報セキュリティボリン・及び情報セキュリティボリン・及び情報セキュリティズリン・及び情報というの情報を発展が開始を発展を開始を表現が表現に関する所は、表記的な影響を表現を表現を表現を表現を表現を表現を表現を表現を表現を表現を表現を表現を表現を	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、外部委託事業者において生まカティンを分では前に確認され、必要に応じ実務を発いまし、必要に応じ業務を得かれ、必要に応じ、業務を対象的によっい、た、政・職等ない、等の、特別、抵債報セキュリティ責任者に報告され、されにその重要度に応じてCISOに報告されているが確かめる。
監査資料の例		□外部委託管理基準 □代業報告書 □改善措置実施報告書 □改善措置実施報告書
監査項目	1)外葡委托事業者との契約 機能ンオトの運用、保守等を外部委託する場合、外部委託事業者との間で確認されている契約書に、必要に応じた情報セキュリティ要件が明記されている。	1)外部委託事業者のセキュリティ対策 の確認と報告 情報セキュリティ管理者によって、外部委託 事業者におけるセキュリティ対策の確保が確 認され、必要に応じ業務委託契約に基づく 指置が講じられている。また、確認した内容 が結括情報セキュリティ責任者に報告され、 されにその重要度に応じてCISOに報告され でいる。
必須	0	0
No.	328	329
項目	8.1. (2.) (2.) (2.) (2.) (2.) (2.) (3.) (3.) (4.) (4.) (5.) (5.) (6.) (7.) (7.) (7.) (7.) (7.) (7.) (7.) (7	(3) 確等

留意事項				
ŠŒ				
関連する JISQ27002 番号	15.1.2 15.1.3 15.2.2	15.1.2 15.1.3 15.2.2		
情報セキュリーイポリンーガイアラインの例 文の番号	8.2.(1)	8.2.(2)	8.3.①	8.3.@~@
監査実施の例	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グビューにより、約数による外部サービスの利用を行う場合の規定が整備され、以下の内容が明問されている分が痛かめる。また、当数サービスの利用において、機密性2以上の情報が取扱われないように規定されているが確かめる。 ・約数によるサービスを利用してよい範囲 ・業務により利用する約数による外間によい着用する約数による外間によい着の表によるサービスを利用してよい範囲 ・業務により利用する約数による外部サービス	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ーステム管理者へのインタビューにより、約数による外部サービスを利用でよるの子ンので開発としてス利用によるリスクの治療とセキュリティ対策の実施に関する基準が定められており、職員等がサービス利用の必要性、リスクの評案の判断を行ったうえでサービスを利用しているか確かめる。	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グビュー(これ)、ソーシャルメディア サービスを利用して住民へ情報提供を行う場合は、アカウトが行う場合は、アカウトが行わな管理しているものであることを布印自口管理 ウェブサイトに当該情報を掲載して参照可能とするともに 当該アカウントの自由記述構造でアカウトのの項用組織を封 する等のたりすまし対策や、アカウトへの、4の数の ネーな等のたりすまし対策や、アカウトへの、4の数の な管理やアカウトログイン用端末のセキュリティ対策等の 不正アクセス対策及び発信した情報をパックアップしておき、ソージャルメディアサービスが終了した情報をパックアップしておき、ソージャルメディアサービスが終了した際の対策が行われているが必要といっている。	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グビューにより、ソーシャルメディアサービスを利用する際には、機密性2以上の情報は発信しないことや、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等の手順がつくられているが確かめる。
監査資料の例	口約数による外部サービス 利用基準 口約数による外部サービス 通用手順 口約数による外部サービス 利用申請書	口約表による外部サービス 利用基準 (国約表による外部サービス (国第一年) (国年年) 利用申請書	ロゾーシャルメディアサービ 大利用 基準 ロゾーシャルメディアサービ ス管理手順 ス管理手順	ロソージャルメディアサービ ス利用基準 ロソージャルメディアサービ ス管理手順
監查項目	1) 約款による外部サービス利用に係る 類にの影響 情報セキュリテイ管理者によって、約款による 特部セキュリテイ管理者によって、約款による 分部サービスの利用に関する規定が作成されている。また、当該サービスの利用におい て、機密性2以上の情報が取扱われないよう に規定されている。	用)約款による外部サービスの利用における対策の実施 付る対策の実施 情報セキュリテイ管理者によって、約款による 外部サービスの利用に関するセキュリテイ対 策の実施に関する基準がが定められている。	1)ソーシャルメディアサービスにおける セキュリティ教学の実施 情報セキュリティ管理者によって、ソーシャル イオアサービスの(シ)・虫しゃ不正アクセス 対策が定められ、運用手順が作成されている。	■リンーシャルメディアサービス利用等の 情報の取扱い 情報セキュリティ管理者によって、ソーシャル オイバナサービスに発信する情報の範囲や ソーシャルメディアサービス利用責任者が定 められている。
必須				
Š.	330	331	332	333
圏	8.2. 本部 参崇に オービ はる外 スの利 部サー 用 ビスの 利用		8.3.7 マンマン アンサー ボルー 単囲	

田舎事項							・セキュリティボリンー連合に しゃ、イケ部委託事業者に対 する説明は、No.98~995間 連する項目であることから参 考にすること。
							<ul><li>・セキュリティス ついて外部委 する説明は、「 連する項目で 考にすること。</li></ul>
関連する Jusq27002 音号	12.7.1 15.1.2 15.2.1 18.2.1	18.2.1	18.2.1	18.2.1	12.7.1	18.2.1	15.1.2 18.2.1 18.2.3
情報セキュリ ティポリシーガ イドラインの例 文の番号	9.1.	9.1.(1)	9.1.(2)⊕	9.1.(2)©	9.1.(3)⊕	9.1.(3)②	9.1.(4)
監査実施の例	□情報セキュリティ監査実施 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要綱 要綱 □情報セキュリティ監査実施 及び手順が文書化され、正式に承認されているか確かめ マニュアル	□情報セキュリティ監査実施 監査資料のDビューと統括情報セキュリティ責任者へのイン要綱 四情報セキュリティ監査実施 任者が指名され、ネットワーク及び情報ンステム等の情報 マニュアル 資産における情報セネ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。	□情報セキュリティ監査実施・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 要綱 □情報セキュリティ監査実施、依頼され、公平な立場で客額的に監査が実施されているかマニュアル □監査実施計画 □監査報告書	□情報セキュリティ監査実施 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要綱 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 □情報セキュリティ監査実施 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マニュアル □監査実施計画 □監査報告書	□情報セキュリティ監査技施 監査資料のレビューと情報セキュリティ監査総括責任者へマニュアル のインタビューにより、監査実施計画が立案され、情報セコ監査実施計画 日監査実施計画 □情報セキュリティ委員会議 事終	□情報セキュリティ監査実施 監査資料のレビューと情報セキュリティ監査総括責任者へ マニュアル ロインタビューにが、被監査部門が監査の実施に協力して ロ監査報告書 いろか確かめる。	□情報セキュリティ監査実施・監査実施・監査資料のレビューと情報セキュリティ監査総括責任者へのインタビューにより、外部委託事業者 (外部委託事業者か) □情報セキュリティ監査実施 5の下請けも含む) に対する情報セキュリティがリンーの適合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が確かめる。
監査資料の例		□情報セキュリティ監査実施 要綱 マニュアル マニュアル 同監査実施計画 回監査報告書	□情報セキュリティ監査実施 要綱 マニュアル マニュアル 三監査実施計画 □監査報告書	<ul><li>「情報セキュリティ監査実施要綱</li><li>「情報セキュリティ監査実施 マトュップト</li><li>「監査実施計画</li><li>□監査報告書</li></ul>	<ul><li>□情報セキュリティ監査実施マニュアル</li><li>□監査実施計画</li><li>□情報セキュリティ委員会議事録</li></ul>	□情報セキュリティ監査実施 マニュアル □監査報告書	□情報セキュリティ監査実施 要縮 (1) 情報セキュリティ監査実施 マニュアル の監査実施計画 (1) 監査報告書
<b>聖</b> 國內	<ul> <li>1)情報セキュリティ監査に関わる基準及び手順</li> <li>総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。</li> </ul>	<ul> <li>1)監査の実施 CISOによって、情報セキュリティ監査総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。</li> </ul>	1)監査人の独立性 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。	<ul><li>1)監査人の専門在 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。</li></ul>	1)監査実施計画の立業 情報セキュリティ監査総括責任者によって、 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。	■)監査実施への協力 監査実施に際し、被監査部門による協力が 得られている。	1)外部委託事業者に対する監査 情報セキュリティ監査統括責任者によって、 外部委託事業者(外部委託事業者からの下 請けら含む)に対する情報セキュリティポリ ジ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。
	4	2	9		- ∞	6	0
ģ	334	335	336	337	338	339	340
		(1) 実施方法	(2) 監査を行う 者の要件		(3)		(4) 外部参託 本本者に 査 合 合 所
通	1.6 酮						
	9. 評価・ 見直し						

- 2 7002 留意事項	・監査報告書は、監査証拠に 無付けられても理的な報拠 に基づくものであることを要する。 従って配着報告事中に、 整本意見に至った根拠とそれ を導く指揮が記載され、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。			・情報セキュリティがリシーの 見直しについては、No.340 ~341も関連する項目である ことから参考にすること。	
関連する   JISQ27002    番号	18.2.1	18.1.3	18.2.1	5.1.2	18.2.2
情報セキュリ ティポリシーガ イドラインの例 文の番号	9.1.(5)	9.1.(6)	9.1.(7)	9.1.(8)	9.2.
監査実施の例	□情報セキュリティ監査実施 監査資料のレビューと情報セキュリティ監査総括責任者へ マニュアル □監査報告書 キュリティ委員会に報告されているか確かめる。 事録 事録	□情報セキュリティ監査実施 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マニュアル 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 ロ監査調書 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がに保管されているが確かめる。	□情報セキュリテイ委員会議 監査資料のレビューと統括情報セキュリテイ委員会議 監査資料のレビューとより、CISOによって、監査結果を踏まえた指摘事項への対処が関係部局に指示され、また、指摘事項を可轄 可への対処が関係部局に指示され、また、指摘事項を可轄 してがが、部局によ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。	□情報セキュリティ委員会議 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事象 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 □情報セキュリティポリシー 伝規程等の見直し、その他情報セキュリティ対策の見直し に活用されているが確かめる。	□情報セキュリティ自己点検 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基準 基準 □情報セキュリティ対策の実施状況の自己点 に関報セキュリティ対策の実施状況の自己点 実施手順 いるか確かめる。
監査資料の例	<ul><li>□情報セキュリテイ監査実施 マニュアル □監査報告書 □情報セキュリテイ委員会議 事録</li></ul>	□情報セキュリティ監査実施 マニュアル □監査調書	□情報セキュリテイ委員会議 事録 □改善指示書	□情報セキュリテイ委員会議 事録 □情報セキュリティボリンー	□情報セキュリティ自己点検 基準 □情報セキュリティ自己点検 実施手順
監査項目	<ul> <li>1)監査結果の報告 情報セキュリアイ監査総括責任者によって、 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。</li> </ul>	i)監査距拠及び監査調告の保管 情報セキュリティ監査総括責任者によって、 監査証拠及び監査調書が適切に保管され でいる。	1)監査結果への対応 CISOによって、監査結果を踏まえた指摘事 項、一の対処が関係部局に指示されている。 また、指摘事項を消耗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、は場合は は、当該課題及び問題点の有無を確認させている。	1)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 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ボリシー及び関係規程等 が情報セキュリティがリシー及び関係規程等 直しに活用されている。	1)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 機能情報セキュリティ責任者によって、情報 セキエリティ対策の実施状況の自己点検に 加わる基準及び手順が定められ、文書化されている。
必須					
o Z	341	342	343	344	345
通	9. (5) 評価· 監査 報告 見直し	(6) 知 歌	(7) 階重結果 への対応	(8) ・	9.2. 电极口电流

シーに沿った情報セキュリティ対策状況につ 及び必要に応じて自己点検が行われているか確かめる。 いて、毎年度及び必要に応じて自己点検が 行われている。
1) 自己点検結果の報告   配査資料のレビューと総括情報セキュリティ責任者又は情報を指揮を持ている   日自己点検結果報告書   報立アナム   日本   日本   日本   日本   日本   日本   日本   日
1)権限の範囲内での改善
<b>ボリシーの見直しへ</b> □情報セキュリテイ委員会議 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 [9.2.(3)② 事録 タビューにより、自己点検 □情報セキュリティボリシー 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。   でいる。 でいる。   でいる。   でいる。   でいる。   でいる。   でいる。   でいる。   でいる。   でいる。   では、   には、   では、   には、   には

留意事項		
関連する JISQ27002 番号	5.1.2	5.1.2
情報セキュリ 関連する ティボリシーガ JISQ27002 イドラインの例 番号 文の番号	9.3.	9.3.
監査実施の例	イボリシー及び関係規 □情報セキュリティボリシー 監査資料のレビューと総括情報セキュリティ責任者へのイン 9.3. わる基準 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 が定められ、文書化され	イポリシー及び関係規         □情報セキュリティ素自会議         がニーと総括情報セキュリティ素自会性         9.3.           1会によって、情報セキュリティ素自会権         チェリティ素自会権を必対         がニーに関係を必対         (特別・           1日点検の結果や情報         事録         キュリティ監査及び自己点検の結果や情報を特徴を出りて、関係表を必対         本リティ素自会に関係を必対         大の変化が変化が表や情報を開発を必要           水沢の変化等をふま         はた場合に評価を行い、必要に応じて情報セキュリティボ がソシー及び関係規程等の改善が行されているが確かめる。         サンー及び関係規程等の改善が行されているが確かめる。           ボリシー及び関係規程         まずに周知されているか確かめる。           業者に周知されているか確かめる。         業者に周知されているか確かめる。
監査資料の例	□情報セキュリティボリシー	□情報セキュリテイボリシー   情報セキュリテイ委員会議   事録   □職員等への周知記録
監査項目	<ul> <li>1)情報セキュリティポリシー及び関係規 独等の見直しに関わる基準 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。</li> </ul>	間)情報セキュリティボリシー及び関係規 機等の見直し 情報セキュリティ委員会によって、情報セ 情報セキュリティに関する状況の変化等をふま セキュリティに関する状況の変化等をふま 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。
必須		0
ġ	351	352
野	9.3. 評価・情報セ 見直しキュリ ディボ リンー 及び際	係規程 等の 直し 直

## 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)

## 監査資料例一覧/索引

## 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。

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。	128,129
	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。	124,125,126,12 7,128
	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。	127
	ID管理台帳	職員等に付与されているIDの発行、変更、抹消を記録した文書。	132,206,207,20 8,209,210,211,2 36,237
	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 に関わる基準について記述した文書。	130,131,132
	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。	205,227,228,22 9,230
	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。	237
	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。	205,227,228,22 9,230
	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。	242,243,244
	異常時復旧手順	情報システムの統合・更新作業中に異常事態が発生した場合に、作業前の 状態に戻す手順を記述した文書。	259
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。	348,349
	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。	343
	改善措置実施報告書	改善要望への対応結果を記録した外部委託事業者から提出される文書。	329
	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。	329
	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。	236
	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。	236
~~*************************************	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。	236,237
	外部委託管理基準	外部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。	107,108,324,32 9
	外部委託事業者監査報告書	外部に設置された当該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

## 監査資料例一覧/索引

+	E		=4
索引	<u>名称</u>	解説	該当No.
	外部委託事業者訪問記録	外部に設置された当該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
	外部委託事業者選定基準	外部委託事業者の選定基準や選定方法等を記述した文書。	324,325,326,32 7
	外部委託事業者における ISO/IEC27001認証取得状況	外部委託事業者のISO/IEC27001認証取得認定書又はこれに類する文書。	48
	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。	165,166,167,16 8,170
	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。	166
	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。	165,166,167,16 8,170
	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。	167
	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。	335,336,337,33 8,340
	監査調書	監査人が実施し確認した内容を記録した文書。	342
	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。	335,336,337,33 8,340,341
	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。	288,298,300
	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。	30,51,52,53,54,5 5,56
	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 人情報保護条例等)を一覧にした文書。	318,319
***************************************	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。	30,36,47

索引	名称	解説	該当No.
	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。	25,36,47
	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わる基準や、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。	41,44,45
	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。	108,184,279,32 8
	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。	312
	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。	285,286,287,30 9,3311.312.313
	クラウドサービス事業者選定記録	クラウドサービス事業者を選定した際の調査内容と選定結果を記録した文 書。	327
	クラウドサービス利用基準	クラウドサービスを利用する場合の基準を記述した文書。	327
	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。	97,98
	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。	110,117,118
	結線図	庁内の通信回線装置間の配線を図に表した文書。	18,19,23,28,66,6 7,68,69,70,164,1 69
	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。	102,109,110,11 1,112,113,114,1 15,116,117,118,

索引	名称	解 説	該当No.
	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。	111,112,114,11 6
•	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。	102,110,113,11 5,118
ż	サーバ障害対応実施手順	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
	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。 	3132
	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。	168
	サービス仕様書(サービスカタログ)	サービスの提供者が提示するサービスの内容や体制等を記述した文書。	325,326,327
•••••	作業報告書	外部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。	27,42,44,45,329
	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。	51,52,53,54,55,5 6
	時刻設定手順	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。	299
	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。	302,304
•••••	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。	346,347,348,34 9
	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。	301,302,304
	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。	
	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わる体制、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。	
***************************************	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。	149
	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。	238,239,242,24 3

##    マステム開発基準   情報システムを開発する場合の工程、会議体、成果物、セキュリティに関する   22 22 22 22 22 22 22 22 22 22 22 22 2			金 貧 料 例 一 覧 / 索 引	
等の保管基準	索引	名称	解 説	該当No.
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。           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。           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。           システム権動記録         情報システムの稼働状況を記録した文書。           システム情成図         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。           システム情成図         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。           システムと設定検査記録         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。           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。           システムを変更管理基準         ジステムの統合・更新時の具体的な作業手順、作業結果の成合の確認方法、失敗や異常の再定方法等を記述した文書。           システム変更等理基準         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。           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 15 名、作業結果、確認者等)を記録した文書。           実施手順         対金基準を具体的な情報システムを変更した場合の管理の事態を記述した文書。           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を記述した文書。           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場合の管理の関係等を記述した文書。           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場合の管理の影響を認識する文書。           (定録表書の表記を得たことを記録する文書。           (定録表書の表記を得たことを記録する文書。           (定録書の表記を得たことと記録する文書。           (定録書の表記を得たことを記録する文書。           (定録書の表記を得たこととと記録する文書。           (定録書の表記書の表記を得たことと記録する文書。           (定録書の方式を得定というでは、対しまする。           (と見がわなどのようによりまする。           (と見がようと記述			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。	249
ルールを記述した文書。   15		システム開発基準		234,250,251,25 2,257,256
書。		システム開発規則		235
フステム監視手順     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。     「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。     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。     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。     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。     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。     システム大計画書/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。     システム教合手順 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。     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。     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。     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。     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。     支給以外のパソコン多び電磁的記録媒体を用いる場合の管理の基準を記述した文書。     支給以外のパソコン多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。		システム開発体制図		235
1   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   24   6.3   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。   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。   24   システム設定技術を開発した文書。   25   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。   26   システムが合手順   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。   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。   システム変更等作業記録   信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。   対策基準を具体的な情報システムを重した場合の管理の基準を記述した文書。   支給以外のパソコン等使用基準   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を記述した文書。   支給以外のパソコン等使用事請者   表記書   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を記述した文書。   「広報誌川ホームページ』メールマガジン』で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論、関調等を申請し、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。   「広報誌川ホームページ』メールマガジン』では発表す段を公表した記録。		システム稼動記録	情報システムの稼働状況を記録した文書。	155
システム仕様書等		システム監視手順		282,283,290,29 1
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。       28         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。       24         システム統合手順       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。       25         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。       25         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。       15         実施手順       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。       34         支給以外のパソコン等使用基準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を記述した文書。       34         支給以外のパソコン等使用事請者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場合に、作業の目前、排間等を申請し、情報セキュリティグ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。       12		システム構成図		24,25,26,28,32,3 6,37
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。       24         システム統合手順       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。       25         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。       25         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。       15         実施手順       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。       84         支給以外のパソコン等使用基準表準を記述した文書。       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を記述した文書。       91         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場合に、作業の記述を表現を表現のよりに対している場合に、情報と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。       90         住民に対する広報記録       12         した記録。       12		システム仕様書等		153,250,253,25 4,255,257
システム統合手順		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。	284
システム変更管理基準		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。	245,246,247,24 8,251
た文書。  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。  実施手順 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。  支給以外のパソコン等使用基準 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を記述した文書。  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。  『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。		システム統合手順		259
者名、作業結果、確認者等)を記録した文書。    実施手順   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。    支給以外のパソコン等使用基準   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を記述した文書。    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。    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。		システム変更管理基準		256
東北京   東として記述した文書。   日本   東として記述した文書。   東として記述した文書。   東京   東京   東京   東京   東京   東京   東京   東		システム変更等作業記録		150,151
支給以外のパソコン等使用基準   基準を記述した文書。   51   支給以外のパソコン等使用申請書/		実施手順		84
及結以外のパソコン等使用中請書/ 承認書 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。 『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。		支給以外のパソコン等使用基準		91,92
住民に対する広報記録 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 12 した記録。			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	90,91,92
障害時のシステム出カログ 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。 15		住民に対する広報記録	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	122
		障害時のシステム出カログ	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。	155,159
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。		障害対応基準		158,159

# 監 査 資 料 例 一 覧 / 索 引

索引	名称	解 説	該当No.
	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。	34,36,37,40,44,1 59,170,181
	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。	146,147
000000000000000000000000000000000000000	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。	147
	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
000000000000000000000000000000000000000	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。	7,8,9,10,11,12,1 3,14,15,16,17,30 ,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。	85
	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。	152,153
	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。	232
	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。	240,241,244
	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。	3,111,115,311,3 38,341,343,344, 348,350,352
	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	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。	321,322,323
	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。	334,335,336,33 7,340
	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。	334,335,336,33 7,338,339,340,3 41,342
	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。	286
	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。	345

索引	名称	解 説	該当No.
水刀	12 17)	<b>州</b> 高元	政当110.
	情報セキュリティ自己点検実施手順	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。	345
	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。	120,121,123,27 6,283,286,288,2 89,302,303,304, 308,309
	情報セキュリティインシデント報告手 順	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。	119,120,121,12 2,123,301,302,3 03,304,308,309
	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。	1,2,3,4,5,6,83,84, 85,105,107,301, 302,304,305,31 0,312,320,321,3 44,350,351,352
	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。	83,106,141,183, 253,295,352
	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。	99,100
	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。	233
	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。	292
	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。	96
	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に関連する情報について、関係者に対して通知した記 録。	293
	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。	225
	ソーシャルメディアサービス管理手 順	ソーシャルメディアサービスを利用する場合の管理手順を記述した文書。	332,333
	ソーシャルメディアサービス利用基 準	ソーシャルメディアサービスを利用する場合の基準を記述した文書。	333,334
	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。	252
	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。	256
	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。	196,197,198,19 9
	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。	198

索引	名称	解説	該当No.
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。	30,51,52,53,54,5 5,56
		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。	200,201,202
	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。	202
	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。	224,225
	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。	95
	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。	87,88,90,93,94
	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。	87,94
	端末ログ	端末の利用状況や、操作内容を記録した文書。	86,288
	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。	89
	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。	87,88,89,92
	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。	232,233
	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。	18,19,23,28,41,6 6,67,68,69,70,16 6,169
	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 ネットワーク接続ロ(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。	38,39,40,441,42
	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。	204,289,322,32 3
	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。	179,180,181.18 2.183,184,185
	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。	86,188,189,190, 193
	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。	84,104,186,187, 188,189,190,19 1,192,193,194,2 74

# 監 査 資 料 例 一 覧 / 索 引

			1
索引	名称	解 説	該当No.
	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。	103
	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。	259
	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。	175
	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。	175
	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。	215
	特権ID管理台帳	特権IDの付与情報を記録した文書。	210,211
	特権ID取扱手続	特権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。	210,211,214,21 5,216
	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。	210
	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。	212
	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。	213
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、変更などに関わる基準を記述した文書。	18,19,23,24,65,6 6,67,68,69,70,71 ,72,73,104,163,1 69,177,178,284
	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。	281
	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。	178,179,216,22 1,222,226,230
	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。	160,161,162
	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。	85,202,203,204
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。	133,134,135,13 6,137,138,139
***************************************	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。	20,21,22,74,75,7 6,77,78,79,80,81 ,82

#21	<u> </u>		量力 ソノ N -
索引	名称 	解説	該当No.
	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。	144,145
	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。	145
	バックアップ手順	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。	144,143
	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。	294
	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。	294
	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わる基準につい て記述した文書。	101
	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。	281
***************************************	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。	86,281
	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。	171,172,173,17 4
	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きを記述した文書。	171,172,173,17 4
	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。	260,261,262,26 3,264,265,266,2 67,268,269,270, 271,272,273,27 4,275,276,277,2 78,279
	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。	261,262,265,26 6,269,270,271,2 72,273,275,276
	不正プログラム対策手順	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。	260,261,262,26 3,264,265,266,2 67,268,269,270, 271,272,273,27 4,275,276,277,2 78,279
	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。	153,250,253,25 4,255,257
	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。	140,141,142,14 3
	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。	147

索引	名称	解説	該当No.
\\ \J1	H 1a.	,, <u>,, ,, ,, ,, ,, ,, ,, ,, ,, ,, ,, ,, </u>	10.
	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
ゃ	約款による外部サービス運用手順	約款による外部サービスを利用する際の具体的な手順を記述した文書。	330,331
	約款による外部サービス利用申請書	約款による外部サービス利用の申請と許可を記録した文書。	330,331
	約款による外部サービス利用基準	約款による外部サービスを利用する場合の基準を記述した文書。	330,331
	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。	246,247
Ġ,	リストア手順	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。	144,145
	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。	145
10000000000000000000000000000000000000	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。	218
***************************************	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。	291,220
	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きを記述した文書。	218,223
	利用者ID管理台帳 利用者IDの付与情報を記録した文書。		207,208,209,21 0
	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。	206,207,208
	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。	206,228,229
000000000000000000000000000000000000000	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わる基準を記述した文書。	295
	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。	
	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。	
	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。	
	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 例外措置申請書/許可書 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。		315,317
	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、許可に関わる手続を記述した文書。	314

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。	153,287
		情報システムのログイン認証の画面。	227

# 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、外部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、原則として〇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

# 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実施計画書(例)

平成〇〇年〇〇月〇〇日

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	<ul><li>○○業務</li><li>○○情報システム</li></ul>	
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 イ. 情報システム、マシン室及び執務室の視察 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	平成〇〇年〇〇月〇〇日~ 平成〇〇年〇〇月〇〇日	
7	監査実施体制	情報セキュリティ監査統括責任者 監査人 監査人	0000 0000 0000
8	監査項目	アクセス制御 不正プログラム対策 不正アクセス対策	
9	適用基準	<ul><li>・○市 情報セキュリティポリシー</li><li>・○○○実施手順書</li></ul>	

# 情報セキュリティ監査報告書(例)

# 情報セキュリティ監査報告書(例)

平成〇〇年〇〇月〇〇日

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
1		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	外の脅威に対する情報セキュリ
۷		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)
		ア. 規程類、記録類の確認	
5	監査方法	イ. 情報システム、マシン室及び執務	室の視察
		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	平成〇〇年〇〇月〇〇日~ 平成〇〇	年〇〇月〇〇日
		情報セキュリティ監査統括責任者	0000
7	監査実施体制	監査人	0000
		監査人	0000
		アクセス制御	
8	監査項目	不正プログラム対策	
		不正アクセス対策	
9	盗田甘淮	・〇市 情報セキュリティポリシー	
Э	適用基準	・○○○実施手順書	

1	纵井	
-	.総括	

- (1)アクセス制御
- $1 \times \times \times \times \times \times \times \times$

#### 【監査結果】

#### 【指摘事項】

#### 【改善案】

- (2)不正プログラム対策
- $\bigcirc$

.

# 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、〇〇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、〇〇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 〇〇市××

電話番号: 0XXX-XX-XXXX FAX: 0XXX-XX-XXXX

#### 4 監查対象

○○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に係る部分)、または情報セキュリティ監査企業台帳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
  - 才 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

平成○○年○○月○○日~平成○○年○○月○○日

- 9 監査報告書の様式
- (1) 監査報告書の作成様式
  - ア A 4 版縦(必要に応じてA 3 版三つ折も可。A 3 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、全て〇〇市に帰属するものとし、書面による〇 〇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、〇〇市は、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

# 情報セキュリティ監査 業務委託契約書(例)

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 : 00市00

履行期限 自 平成○○年○○月○○日

至 平成〇〇年〇〇月〇〇日

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、当事者記名捺印の 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。

- ○○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。

同 第4項記載のとおり。 ④監査対象 ⑤業務範囲 同 第5項記載のとおり。 同 ⑥適用基準 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 平成○○年○○月○○日 平成○○年○○月○○日 ⑨評価の基準日

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:平成〇〇年〇〇月〇〇日

- ※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条 例においても、個人データの外部委託先に対して、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<sup>※9</sup>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。

平成〇〇年〇〇月〇〇日				
甲	印			
۷	印			
丙	印			
		以上		