

春日井市情報セキュリティ監査実施要綱

(趣旨)

第1条 この要綱は、春日井市情報セキュリティポリシーに基づき、情報セキュリティ対策の適正な実施状況の確認のために実施する監査について、事務を円滑かつ正確に行うために必要な事項を定めるものとする。

(監査対象)

第2条 情報セキュリティ監査対象は、春日井市情報セキュリティポリシーに定める情報システムとする。

(監査実施体制)

第3条 監査実施体制は、監査全般を統括する監査統括責任者、監査を実施するに当たり管理及び監督する監査実施責任者及び監査人をもって構成する。

- 2 監査統括責任者は、セキュリティ管理責任者をもって充てる。
- 3 監査実施責任者は、ネットワーク管理者をもって充てる。
- 4 監査人は、市の職員による監査人（以下「内部監査人」という。）及び情報セキュリティ監査の知識を有する市の職員以外の者による監査人（以下「外部監査人」という。）とする。
- 5 内部監査人は、監査実施責任者が情報システム課の職員のうちから指名する。ただし、監査実施責任者が必要と認めるときは、情報システム課以外の職員から指名することができる。
- 6 外部監査人は、経済産業省が定めた情報セキュリティ監査基準の一般基準を満たす者から選任するものとする。
- 7 外部監査人の選任は、監査実施責任者が客観的で公平な手続きに従って行い、監査統括責任者の承認を得るものとする。
- 8 外部監査人を委託する場合の委託仕様書は、別に定める。
- 9 外部監査人により監査を実施する場合は、内部監査人が立ち会うものとする。

(監査人の責務)

第4条 監査人は、監査の実施に当たり、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。

2 監査人は、監査及び情報システムに関する知識を有し、相当な注意をもって監査を実施しなければならない。

3 監査人は、監査において知り得たすべての情報を、正当な事由なく第三者に漏らしてはならないものとし、監査人の職を離れた後も同様とする。

(監査計画)

第5条 監査統括責任者は、定期的に行う監査の対象となる情報システムを選定し、監査計画を定め、セキュリティ統括責任者の承認を得なければならない。

2 監査計画書には次の事項を記載する。

(1) 当該年度の監査方針

(2) 監査目標

(3) 被監査部署

(4) 監査実施時期

(5) 監査実施責任者

(6) 監査人

3 監査統括責任者は、個人情報及び重要情報の処理において、盗用、改ざん、漏えいその他不適切な利用による情報の侵害が行われるおそれがあると認めるときは、監査計画書にある監査とは別に、臨時監査を行うことができる。

(監査実施計画)

第6条 監査実施責任者は、監査対象となる情報システムごとに監査実施計画を定め、監査統括責任者の承認を得なければならない。

2 監査実施計画書には次の事項を記載する。

(1) 監査目的

(2) 監査テーマ

(3) 監査対象範囲 (対象となる情報システム)

(4) 被監査部署

- (5) 監査方法
- (6) 監査実施日程
- (7) 監査実施体制
- (8) 監査人要件（外部監査人の場合に限る。）
- (9) 監査項目
- (10) 適用基準
- (11) その他必要と認める事項

3 監査実施責任者は、前項の監査実施計画を定めるに当たって、被監査部署と次に掲げる内容について確認しなければならない。

- (1) 監査実施スケジュール
- (2) 被監査部署が準備する内容（人、文書、システム、場所等）
（監査実施通知）

第7条 監査実施責任者は、監査実施計画書に基づく監査の実施について、被監査部署に通知しなければならない。

2 監査実施通知書には次の事項を記載する。

- (1) 監査目的
- (2) 監査対象範囲（対象となる情報システム）
- (3) 監査日時
- (4) 監査人
- (5) 監査時に必要な資料等
- (6) その他必要と認める事項
（監査人の権限）

第8条 監査人は、監査対象情報システムに対して次の権限を有する。

- (1) 被監査部署が保有する全ての関係書類及び電子データを閲覧する権限
- (2) 監査対象情報システムを被監査部署の同意を得て操作する権限
- (3) 監査対象情報システムに携わる者（外部委託者を含む。）に対して聴取する権限

(監査協力)

第9条 被監査部署は、監査が円滑に行われるよう監査人に協力しなければならない。

(監査の実施)

第10条 監査実施責任者は、監査実施計画書に基づき監査を実施しなければならない。ただし、監査対象システムの障害及びその他やむを得ない緊急事態が発生した場合は、この限りでない。

(監査結果通知)

第11条 監査実施責任者は、監査結果を被監査部署に通知しなければならない。

2 監査報告書は、次の内容を含むものでなければならない。

(1) 第6条第2項各号(第8号を除く。)に掲げるもの

(2) 改善事項

(監査実施報告)

第12条 監査実施責任者は、監査計画に関する実施状況について、春日井市情報化推進委員会に報告しなければならない。

(改善報告)

第13条 被監査部署は、監査報告書により指摘された改善事項に対し、改善報告書を作成し、監査実施責任者の定める期限までに提出しなければならない。

2 改善を実施する上で期間を要する場合は、改善内容と合わせ実施予定時期も明記する。

(改善事項に関する確認)

第14条 監査実施責任者は、被監査部署が作成した改善報告書に基づいて、改善内容が適切に運用されているか確認しなければならない。

2 実施予定時期のあるものは、監査実施責任者が定める時期に、前項の内容を実施する。

(フォローアップ監査)

第15条 監査実施責任者は、必要があると認めたときは、被監査部署に対して改

善報告書に基づき継続して改善内容が運用されているか確認しなければならない。

(雑則)

第16条 この要綱に定めるもののほか情報セキュリティ監査の実施に関し必要な事項は、監査統括責任者が別に定める。

附 則

この要綱は、平成22年12月1日から施行する。

附 則

この要綱は、平成29年4月1日から施行する。