栗東市情報セキュリティ監査実施要綱の制定 及び 栗東市情報セキュリティ監査中期計画の策定について

1.　栗東市情報セキュリティ監査実施要綱の制定

本市が取り扱う情報には、住民基本台帳や課税・納税情報、福祉に関する情報等の個人情報のみならず行政運営上重要な情報など外部に漏えいした場合には、極めて重大な結果を招く情報が多数含まれており、これらの情報及び情報を取り扱う情報システムを様々な脅威から防御することは、市民等の財産、プライバシー等を守るためにも、また本市の行政事務の安定的な実施にも必要不可欠である。

このような状況に鑑みて、本市においては、平成１７年３月に「栗東市情報セキュリティポリシー」を定め、同年４月から施行し、本市が保有する情報資産の機密性、完全性及び可用性を維持するための情報セキュリティ対策の基準として運用している。

しかし、令和５年度に個人情報保護委員会の立ち入り検査でも指摘を受けたが、ルールを定めてもそれらが正しく運用されていることが非常に重要となるため、不備があれば速やかに是正することにより情報資産を適切に保護し、セキュリティインシデントを未然に防止することを目的として、令和７年度より情報セキュリティ監査を実施するにあたり、本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た栗東市情報セキュリティ監査実施要綱を制定する。

2.　栗東市情報セキュリティ監査実施要綱の概要

項目	内容
目的	本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
監査体制	・情報セキュリティ監査統括責任者：政策推進部長 ・監　査　員　　：情報セキュリティ監査統括責任者が指名した者 ・事　務　局　　：情報政策課
監査計画	・情報セキュリティ監査中期計画：中期（５年間）の監査の基本方針を定めた計画 ・情報セキュリティ監査年度計画：中期計画に基づき、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計画 ・情報セキュリティ監査実施計画：年度計画に基づき、監査方法等の詳細な事項を定めた計画
監査手順	別紙「情報セキュリティ監査手順」のとおり

3.　栗東市情報セキュリティ監査中期計画の策定

栗東市情報セキュリティ監査実施要綱に基づき、令和７年度を初年度とする５年間の監査の基本方針、監査範囲、監査項目を定めた中期監査計画を策定する。

4. 栗東市情報セキュリティ監査中期計画の概要

項目	内容
基本方針	・令和７年度から令和１１年度の５年間で情報政策課を除く全ての所属を１巡するよう本市職員による内部監査を実施する。実施範囲は、個人番号利用事務系システム、LGWAN 接続系システム、インターネット接続系システム、各所属で独自に調達・管理しているシステム及び利用所属として、教育ネットワーク、教育情報システムについては、「栗東市教育情報セキュリティポリシー対策基準」により、情報セキュリティ対策の方針、行動指針が定められていることから、実施対象外とする。 ・情報政策課については、計画最終年度にあたる令和１１年度に、本市の情報セキュリティ管理が適切になされているかについて、外部監査を実施する。
監査範囲	・組織的安全管理措置 ・人的安全管理措置 ・物理的安全管理措置 ・技術的安全管理措置 ・文書規程（取扱規程・マニュアル・手順書等）
監査項目	・情報セキュリティ体制・組織等の運用状況 ・物理的セキュリティの運用状況 ・情報システム及び通信ネットワークの運用の状況 ・情報データファイルやシステムへのアクセス制御等の運用状況 ・研修・訓練への参加及び内容の理解状況 ・監査の適切な実施 ・文書規程

5. 今後のスケジュール

日程	内容
令和 7 年 4 月 1 日	栗東市情報セキュリティ監査実施要綱　施行
令和 7 年 5 月	栗東市情報セキュリティ監査年度計画　作成 ※情報セキュリティ委員会にて審議
令和 7 年 6 月	栗東市情報セキュリティ監査実施計画・監査チェックリスト　作成
令和 7 年 7 月	栗東市情報セキュリティ監査実施計画・監査チェックリスト　配布
令和 7 年 8 月～10 月	情報セキュリティ監査（ヒアリング、現地視察）
令和 7 年 11 月～12 月	情報セキュリティ監査報告書　作成
令和 8 年 1 月	監査結果を情報セキュリティ委員会にて報告
令和 8 年 2 月	・監査結果を被監査所属の情報セキュリティ管理者（所属長）に通知 ・改善勧告事項に対する実施の可否、改善内容、実施時期の検討

栗東市情報セキュリティ監査実施要綱（案）

令和７年　月　日
告示第　条

第１章　総　則

（目　的）

第１条　この要綱は、栗東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、栗東市情報セキュリティポリシーが適用される組織を対象に実施する。

（監査実施体制）

第３条　情報セキュリティ監査は、情報セキュリティ監査統括責任者（以下「監査統括責任者」という。）が、体制を構築して行うものとする。

２　監査統括責任者は、政策推進部長をもって充てる。

３　情報セキュリティ監査業務は、監査統括責任者が指名する監査員によって実施する。

（１)内部監査の場合は、本市職員の中から監査員を指名する。

（２)外部監査の場合は、外部監査員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、高度に専門的な知見を有する外部の専門家を監査員として指名する。

４　情報セキュリティ監査に関する事務は、情報政策課が担当する。

（監査の権限）

第４条　監査員は、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　監査員は、委託先など業務上の関係先に対して、事実の確認を求めることができる。

４　監査員は、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。

（監査員の責務）

第５条　監査員は、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　監査員は、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　監査員は、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、監査統括責任者及び監査員がその責任を負わなければならない。

5　監査統括責任者及び監査員は、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基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　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　監査統括責任者は、中期計画に基づき、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　監査統括責任者は、年度計画に基づいて、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　監査統括責任者は、監査実施計画に基づく監査の実施にあたって、原則として３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。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　監査員は、監査実施計画に基づき、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、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　監査員は、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　監査員は、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　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。

（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。

附　則

この要綱は、令和７年　月　日から施行する。

栗東市情報セキュリティ監査中期計画
(案)
(令和７年度～１１年度)

栗東市情報セキュリティ委員会（令和　年　月　日承認）

栗東市情報セキュリティ監査統括責任者

目　　次

１．情報セキュリティ監査中期計画策定の趣旨

栗東市（以下「本市」という。）が取り扱う情報には、住民基本台帳や課税・納税情報、福祉に関する情報等の個人情報のみならず行政運営上重要な情報など外部に漏えいした場合には、極めて重大な結果を招く情報が多数含まれており、これらの情報及び情報を取り扱う情報システムを様々な脅威から防御することは、市民等の財産、プライバシー等を守るためにも、また本市の行政事務の安定的な実施にも必要不可欠である。

このような状況に鑑みて、本市においては、平成１７年３月に「栗東市情報セキュリティポリシー」を定め、同年４月から施行し、本市が保有する情報資産の機密性、完全性及び可用性を維持するための情報セキュリティ対策の基準として運用している。

しかし、ルールを定めてもそれらが正しく運用されていなければ、情報漏えいやウイルス感染等のリスクが高まることから、運用状況を確認し、不備があれば速やかに是正することにより情報資産を適切に保護し、セキュリティインシデントを未然に防止することを目的として、情報セキュリティ監査を実施する事として、令和７年度を初年度とする５年間の中期監査計画を策定する。

２．監査の基本方針

（１）情報政策課を除く所属については、令和７年度から令和１１年度の５年間で全ての所属を１巡するよう本市職員による内部監査を実施する。

実施範囲は、個人番号利用事務系システム、情報系システム、インターネット接続系システム、システム利用所属で独自に調達・管理しているシステム及び利用所属として、「栗東市教育情報セキュリティポリシー対策基準（令和４年２月版）第２章 適用範囲等」に定める情報資産は、実施範囲対象外とする。

（２）本市全体の情報セキュリティの管理を統括する情報政策課については、計画最終年度にあたる令和１１年度に、本市の情報セキュリティ管理が適切になされているかについて、外部監査を実施する。

３．監査の範囲

（１）組織的安全管理措置
（２）人的安全管理措置
（３）物理的安全管理措置
（４）技術的安全管理措置
（５）文書規程（取扱規程・マニュアル・手順書等）

４．監査の項目

（１）情報セキュリティ体制・組織等の運用状況
①重要性の認識

②担当者への適切な権限の付与
③委員会の設置
④取扱規程の策定、事務所内の周知・徹底・教育
⑤取扱規程の適切な見直し
⑥情報の分類管理
⑦外部組織との契約等
⑧職員の機密保持、守秘義務
⑨個人情報取扱時

（２）物理的セキュリティの運用状況
①管理区域への入退室管理、施錠管理
②情報機器の災害への対応
③盗難防止対策
④不要時の適切な廃棄処分
⑤外部からの不要な情報機器の持込制限
⑥クラウドサービスの利用

（３）情報システム及び通信ネットワークの運用の状況
①運用ルール、各種手順書の整備
②ウイルス対策ソフトの更新
③ソフトウェアのインストール
④導入ソフトの脆弱性対策
⑤データの暗号化
⑥電子メール送受信時の対策
⑦パスワードの設定
⑧外部持ち出し時の適切な管理

（４）情報データファイルやシステムへのアクセス制御等の運用状況
①ID 及びパスワード識別、認証
②ID 登録、削除
③パスワードの適切な管理
④離席時のパソコン対応
⑤適切なアクセス権限
⑥アクセスログの記録
⑦不正アクセスへの対策
⑧マニュアル等の整備
⑨使用許諾、知的所有権等
⑩セキュリティ管理の実施状況の把握

（５）研修・訓練への参加及び内容の理解状況
①研修・訓練への参加

②研修・訓練の内容の理解

（６）監査の適切な実施

①基準及び手順

②実施

③独立性

④実施計画

⑤協力

⑥結果の報告

⑦調書等の適切な保管

⑧結果への対応

（７）文書規程

①基準、規程等

②物理的セキュリティ

③人的セキュリティ

④技術的セキュリティ

⑤運用

⑥業務委託と外部サービス（クラウドサービス）の利用

⑦評価・見直し

５．監査業務の手順手順

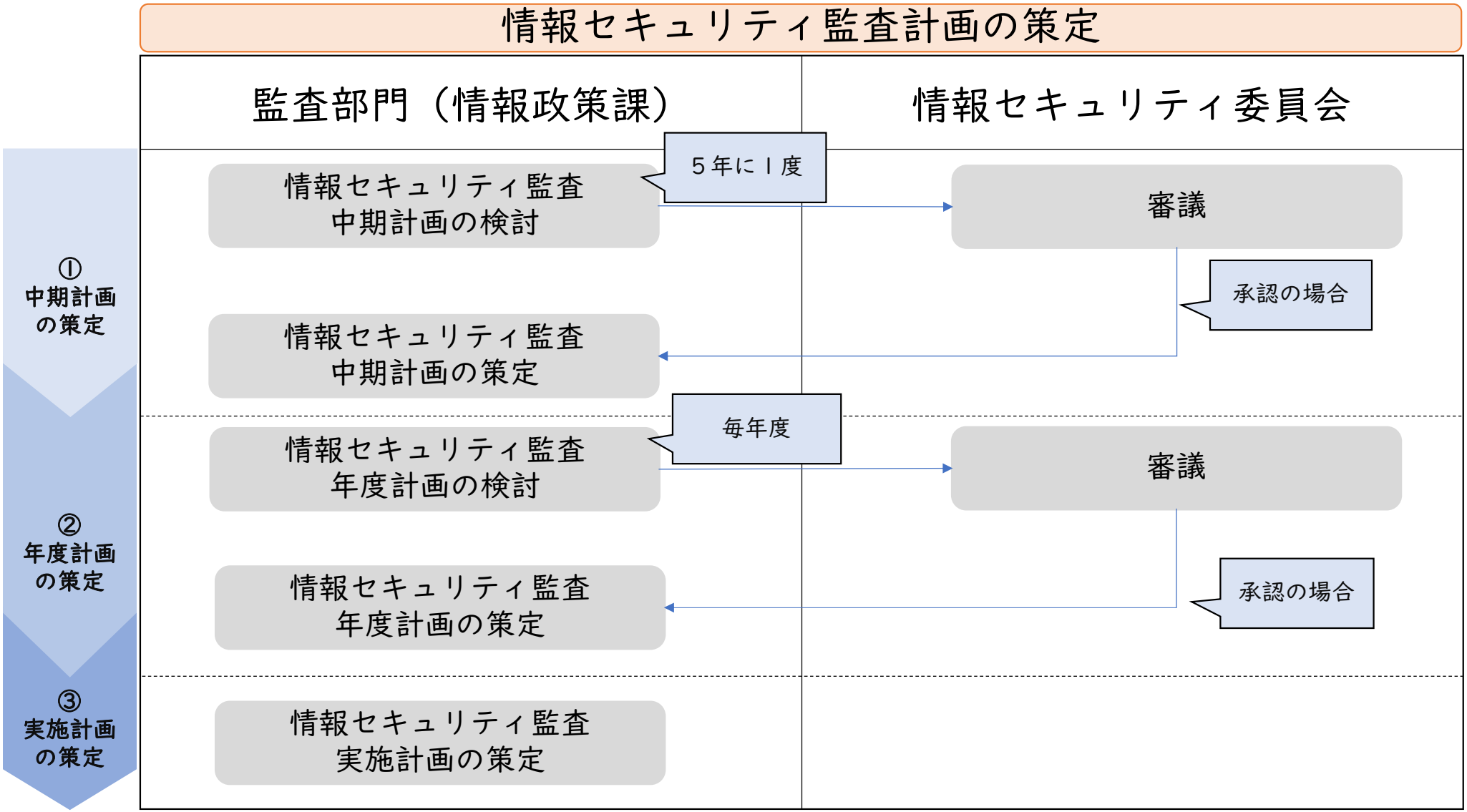
（１）内部監査＜令和７年度 ～ 令和１１年度＞

月 内容	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
監査年度計画の作成	◎											
情報セキュリティ委員会		◎								◎		
監査員の指名		◎										
監査実施方針の策定			◎									
監査チェックリストの検討			◎									
監査実施計画の周知				◎								
監査チェックリストの配布				◎								
監査実施					◎	◎	◎					
監査報告書作成								◎	◎			
監査結果の報告・改善勧告事項に対する対応検討											◎	◎

（2）外部監査＜令和１１年度＞

月 内容	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
監査年度計画の作成	◎											
情報セキュリティ委員会		◎								◎		
監査実施概要、要領詳細策定		◎	◎									
監査員依頼・選任、委嘱				◎	◎							
監査チェックリストの検討					◎							
監査チェックリストの配布					◎							
監査実施						◎	◎					
監査報告書作成								◎	◎			
改善勧告事項に対する対応の検討											◎	◎

別紙　情報セキュリティ監査手順



別紙　情報セキュリティ監査手順