

栗東市情報セキュリティポリシーの改定について

1. 現在の情報セキュリティポリシーの策定・施行

平成15年度に施行された「行政機関の保有する個人情報の保護に関する法律」（個人情報保護法）や平成16年度に施行された「栗東市個人情報保護条例」等に対応し、情報資産を保護するための具体的な措置を定めるため、平成17年4月1日より栗東市情報セキュリティポリシーを施行している。本ポリシーは、「情報セキュリティ基本方針」と「情報セキュリティ対策基準」から構成されており、「情報セキュリティ基本方針」は本市の情報セキュリティ対策に対する基本的な考え方、「情報セキュリティ対策基準」は情報セキュリティを確保するために遵守すべき行為及び判断等の基準を定めている。

[改定履歴]

平成31年3月1日：マイナンバー制度の開始やサイバー攻撃の増加・巧妙化など、ICTを取り巻く環境や脅威が著しく変化したため、内容を全面的に見直し、整理した。

令和5年11月20日：「栗東市個人情報保護条例」の廃止に伴い、該当の文言を削除した。

2. 情報セキュリティポリシーの改定

サイバー攻撃などの脅威の高度化・多様化など、情報セキュリティを取り巻く社会的環境の変化が著しいことから、改定を行い、令和7年4月1日より施行する。

なお、改定にあたっては、「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（平成13年3月30日策定 令和6年10月2日改定）」に全面的に準拠している。

3. 情報セキュリティ委員会

情報セキュリティを確保するための体制、運用規定、基本方針、対策基準を検討するための委員会であり、情報セキュリティに関する重要な事項（情報セキュリティポリシーの改定等）については、情報セキュリティ委員会で審議することと栗東市情報セキュリティポリシーで規定している。

構成員は、副市長（CISO：最高情報セキュリティ責任者）を委員長、政策推進部長（統括情報セキュリティ責任者）を副委員長、部長及び部長相当職の者（情報セキュリティ責任者）であり、事務局は情報政策担当課となっている。

4. 情報セキュリティポリシーの改定のポイント

・情報セキュリティ基本方針

主な改定内容	改定のポイント
①情報セキュリティ監査及び自己点検の実施	・情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する旨を明記。
②情報セキュリティポリシーの見直し	・情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、情報セキュリティポリシーの見直しを行う旨を追記。

・情報セキュリティ対策基準

主な改定内容	改定のポイント
①機密性分類基準の見直し	・国の機密性分類と区別するため「自治体機密性」の名称を新たに用いる。 ・自治体機密性3の情報を、国の機密性分類（政府統一基準）等を参考に3つ（3A、3B、3C）に細分化し、国の機密性分類との対応関係を明確にする。
②自治体基幹システムの標準化に対する対応	・個人番号利用事務系の外部との接続について、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先（例：eLTAX、マイナポータル）との通信に限り、インターネット経由の双方向通信を可能にする。
③業務委託先管理の強化	・委託事業者を実施させるセキュリティ対策の定期的な確認や、業務委託契約時、委託実施期間中、終了後について、本市が講じるべき措置や委託事業者を求めるべき対策をそれぞれ規定。
④クラウドサービスの利用に対する対応	・クラウドサービスにおける情報セキュリティの国際規格（JIS Q 27017：JIS Q27002）を元に、クラウドサービスの利用にあたり、本市が講じるべき措置やクラウドサービス提供事業者を求めるべき対策をそれぞれ規定。

5. 周知方法

情報セキュリティポリシーを見直した際には、その内容を職員に理解を求める必要があることから、事務ポータルサイトに掲示するとともに、説明会や研修会において説明を行う。

また、市民への周知を行うため、市公式ホームページに掲載する。

なお、情報セキュリティの確保の観点から、市民に対しては情報セキュリティ基本方針のみ公開し、情報セキュリティ対策基準の全文については公開しないものとする。

6. 今後のスケジュール

令和7年3月 ： 総合調整会議にて審議/市長決裁

令和7年4月1日 ： 栗東市情報セキュリティポリシー（改定版） 施行

令和7年5月～7月： 会計年度任用職員への「情報セキュリティ研修」にて説明
正規職員への「情報セキュリティ研修」にて説明

改正案	現 行
I 情報セキュリティ基本方針 [1 略] 2. 定義 [(1) ～ (9) 略] (10) LGWAN接続系 LGWANに接続された情報システム及びその情報システムで取り扱うデータをいう。 [(11) ～ (14) 略] <u>(15) 外部サービス</u> <u>本市以外の者が一般向けに情報システムの一部又は全部の機能を提供するものをいう。ただし、当該機能において本市の情報が取り扱われる場合に限る。</u> <u>(16) クラウドサービス</u> <u>外部サービスの中で、事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるものをいう。クラウドサービスの例としては、SaaS (Software as a Service)、PaaS (Platform as a Service)、IaaS (Infrastructure as a Service) 等がある。</u> [3 ・ 4 略] 5. 職員等の遵守義務 職員、教職員、非常勤職員及び<u>会計年度任用職員</u>（以下「職員等」という。）は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。 また、職員等は、本市の情報資産を利用する委託業務従事者等に対して、適切な情報の取扱いについて指示し、管理・監督しなければならない。 6. 情報セキュリティ対策 上記3の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。 [(1) ～ (7) 略] (8) <u>業務委託と外部サービス（クラウドサービス）</u>の利用 <u>業務</u>委託する場合には、外部委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、外部委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。 <u>外部サービス（クラウドサービス）を利用する場合には、利用に係る規定を整備し対策を講じる。</u> ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。 [(9) 略]	I 情報セキュリティ基本方針 [1 同左] 2. 定義 [(1) ～ (9) 同左] (10) LGWAN接続系 <u>人事給与、財務会計及び文書管理等</u>LGWANに接続された情報システム及びその情報システムで取り扱うデータをいう。 [(11) ～ (14) 同左] <u>[新規]</u> <u>[新規]</u> [3 ・ 4 同左] 5. 職員等の遵守義務 職員、教職員、非常勤職員及び<u>臨時職員</u>（以下「職員等」という。）は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。 また、職員等は、本市の情報資産を利用する委託業務従事者等に対して、適切な情報の取扱いについて指示し、管理・監督しなければならない。 6. 情報セキュリティ対策 上記3の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。 [(1) ～ (7) 同左] (8) 外部サービスの利用 <u>外部</u>委託する場合には、外部委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、外部委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。 <u>約款による外部サービスを利用する場合には、利用にかかる規定を整備し対策を講じる。</u> ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。 [(9) 同左]

<u>7. 情報セキュリティ監査及び自己点検の実施</u> 情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。 <u>8. 情報セキュリティポリシーの見直し</u> 情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、情報セキュリティポリシーを見直す。 <u>9. 情報セキュリティ対策基準の策定</u> 上記に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。 なお、情報セキュリティ対策基準は、公にすることにより本市の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。 <u>10. 情報セキュリティ実施手順の策定</u> 情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。 なお、情報セキュリティ実施手順は、公にすることにより本市の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。 <u>11. 懲戒処分</u> 情報セキュリティポリシーに違反した職員等（県費負担教職員を除く）及びその監督責任者は、その重大性、発生した事案の状況等に応じて、地方公務員法による懲戒処分の対象とする。	<u>[新規]</u> <u>[新規]</u> <u>7. 情報セキュリティ対策基準の策定</u> 上記に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。 <u>8. 情報セキュリティ実施手順の策定</u> 情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。 なお、情報セキュリティ実施手順は、公にすることにより本市の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。 <u>9. 懲戒処分</u> 情報セキュリティポリシーに違反した職員等（県費負担教職員を除く）及びその監督責任者は、その重大性、発生した事案の状況等に応じて、地方公務員法による懲戒処分の対象とする。
--	---

改正案	現行																							
Ⅱ 情報セキュリティ対策基準	Ⅱ 情報セキュリティ対策基準																							
〔 1. 略〕	〔 1. 同左〕																							
2. 組織体制 情報セキュリティ対策を実施するための組織体制は、以下のとおりとする。	2. 組織体制 情報セキュリティ対策を実施するための組織体制は、以下のとおりとする。																							
〔組織体制図略〕	〔組織体制図同左〕																							
〔(1) 略〕 (2) 統括情報セキュリティ責任者 〔①～⑧略〕 <u>⑨統括情報セキュリティ責任者は、情報セキュリティ関係規程に係る課題及び問題点を含む運用状況を適時に把握し、必要に応じてCISOにその内容を報告しなければならない。</u> <u>⑩統括情報セキュリティ責任者は、自身の権限に属する事務を情報政策担当課長に処理させることができる。</u>	〔(1) 略〕 (2) 統括情報セキュリティ責任者 〔①～⑧同左〕 <u>〔新規〕</u> <u>⑨統括情報セキュリティ責任者は、自身の権限に属する事務を情報政策担当課長に処理させることができる。</u>																							
〔(3) ～ (7) 略〕	〔(3) ～ (7) 同左〕																							
3. 情報資産の分類と管理 (1) 情報資産の分類 本市における情報資産は、機密性、完全性及び可用性により、次のとおり分類し、必要に応じ取扱制限を行うものとする。	3. 情報資産の分類と管理 (1) 情報資産の分類 本市における情報資産は、機密性、完全性及び可用性により、次のとおり分類し、必要に応じ取扱制限を行うものとする。																							
①機密性による情報資産の分類	①機密性による情報資産の分類																							
<table><tr><th>分類</th><th>分類基準</th><th>取扱制限</th></tr><tr><td><u>自治体機密性 3A</u></td><td><u>行政事務で取り扱う情報資産のうち、「行政文書の管理に関するガイドライン」(平成23年4月1日内閣総理大臣決定)に定める秘密文書に相当する文書</u></td><td rowspan="4"><u>・本市管理以外の端末等での作業の禁止(自治体機密性3の情報資産に対して)</u> ・必要以上の複製及び配付禁止 ・保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持ち込み禁止 ・情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・信頼のできるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管</td></tr><tr><td><u>自治体機密性 3B</u></td><td><u>行政事務で取り扱う情報資産のうち、漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きく、事務又は業務の規模や性質上、取扱いに非常に留意すべき情報資産</u></td></tr><tr><td><u>自治体機密性 3C</u></td><td><u>行政事務で取り扱う情報資産のうち、自治体機密性3B以上に相当する機密性は要しないが、基本的に公表することを前提としていないもので、業務の規模や性質上、取扱いに留意すべき情報資産</u></td></tr><tr><td><u>自治体機密性</u></td><td>行政事務で取り扱う情報資産のうち、<u>自治体機密性3</u>に相当する</td></tr></table>	分類	分類基準	取扱制限	<u>自治体機密性 3A</u>	<u>行政事務で取り扱う情報資産のうち、「行政文書の管理に関するガイドライン」(平成23年4月1日内閣総理大臣決定)に定める秘密文書に相当する文書</u>	<u>・本市管理以外の端末等での作業の禁止(自治体機密性3の情報資産に対して)</u> ・必要以上の複製及び配付禁止 ・保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持ち込み禁止 ・情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・信頼のできるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管	<u>自治体機密性 3B</u>	<u>行政事務で取り扱う情報資産のうち、漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きく、事務又は業務の規模や性質上、取扱いに非常に留意すべき情報資産</u>	<u>自治体機密性 3C</u>	<u>行政事務で取り扱う情報資産のうち、自治体機密性3B以上に相当する機密性は要しないが、基本的に公表することを前提としていないもので、業務の規模や性質上、取扱いに留意すべき情報資産</u>	<u>自治体機密性</u>	行政事務で取り扱う情報資産のうち、 <u>自治体機密性3</u> に相当する	<table><tr><th>分類</th><th>分類基準</th><th>取扱制限</th></tr><tr><td><u>3</u></td><td><u>行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産</u></td><td rowspan="2"><u>・本市管理以外の端末等での作業の禁止(機密性3の情報資産に対して)</u> ・必要以上の複製及び配付禁止 ・保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持ち込み禁止 ・情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・信頼のできるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管</td></tr><tr><td><u>2</u></td><td><u>行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産</u></td></tr><tr><td><u>1</u></td><td>機密性2又は機密性3の情報資産以外の情報資産</td><td></td></tr></table>	分類	分類基準	取扱制限	<u>3</u>	<u>行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産</u>	<u>・本市管理以外の端末等での作業の禁止(機密性3の情報資産に対して)</u> ・必要以上の複製及び配付禁止 ・保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持ち込み禁止 ・情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・信頼のできるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管	<u>2</u>	<u>行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産</u>	<u>1</u>	機密性2又は機密性3の情報資産以外の情報資産	
分類	分類基準	取扱制限																						
<u>自治体機密性 3A</u>	<u>行政事務で取り扱う情報資産のうち、「行政文書の管理に関するガイドライン」(平成23年4月1日内閣総理大臣決定)に定める秘密文書に相当する文書</u>	<u>・本市管理以外の端末等での作業の禁止(自治体機密性3の情報資産に対して)</u> ・必要以上の複製及び配付禁止 ・保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持ち込み禁止 ・情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・信頼のできるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管																						
<u>自治体機密性 3B</u>	<u>行政事務で取り扱う情報資産のうち、漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きく、事務又は業務の規模や性質上、取扱いに非常に留意すべき情報資産</u>																							
<u>自治体機密性 3C</u>	<u>行政事務で取り扱う情報資産のうち、自治体機密性3B以上に相当する機密性は要しないが、基本的に公表することを前提としていないもので、業務の規模や性質上、取扱いに留意すべき情報資産</u>																							
<u>自治体機密性</u>	行政事務で取り扱う情報資産のうち、 <u>自治体機密性3</u> に相当する																							
分類	分類基準	取扱制限																						
<u>3</u>	<u>行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産</u>	<u>・本市管理以外の端末等での作業の禁止(機密性3の情報資産に対して)</u> ・必要以上の複製及び配付禁止 ・保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持ち込み禁止 ・情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・信頼のできるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管																						
<u>2</u>	<u>行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産</u>																							
<u>1</u>	機密性2又は機密性3の情報資産以外の情報資産																							

	<u>2</u>	機密性は要しないが、直ちに一般に公表することを前提としていない情報資産	
	<u>自治体機密性1</u>	<u>自治体</u> 機密性2又は <u>自治体</u> 機密性3の情報資産以外の情報資産	—
②完全性による情報資産の分類			
	分類	分類基準	取扱制限
	<u>自治体完全性2</u>	行政事務で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、住民の権利が侵害される又は行政事務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・バックアップ、電子署名付与 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
	<u>自治体完全性1</u>	<u>自治体</u> 完全性2情報資産以外の情報資産	—
③可用性による情報資産の分類			
	分類	分類基準	取扱制限
	<u>自治体可用性2</u>	行政事務で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、住民の権利が侵害される又は行政事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・バックアップ、指定する時間以内の復旧 ・電磁的記録媒体の施錠可能な場所への保管
	<u>自治体可用性1</u>	<u>自治体</u> 可用性2の情報資産以外の情報資産	—
(2) 情報資産の管理 [①～⑤略]			
⑥情報資産の保管			
(ア) 情報セキュリティ管理者は、情報資産の分類に従って、情報資産を適正に保管しなければならない。			
(イ) 情報セキュリティ管理者は、情報資産を記録した電磁的記録媒体を長期保管する場合は、書込禁止の措置を講じなければならない。			
(ウ) 情報セキュリティ管理者は、利用頻度が低い電磁的記録媒体や情報システムのバックアップで取得したデータを記録する電磁的記録媒体を長期保管する場合は、自然災害を被る可能性が低い地域に保管するよう努めなければならない。			
(エ) 情報セキュリティ管理者は、 <u>自治体</u> 機密性2以上、 <u>自治体</u> 完全性2又は <u>自治体</u> 可用性2の情報を記録した電磁的記録媒体を保管する場合、耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。			

②完全性による情報資産の分類			
	分類	分類基準	取扱制限
	2	行政事務で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、住民の権利が侵害される又は行政事務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・バックアップ、電子署名付与 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
	1	完全性2情報資産以外の情報資産	
③可用性による情報資産の分類			
	分類	分類基準	取扱制限
	2	行政事務で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、住民の権利が侵害される又は行政事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・バックアップ、指定する時間以内の復旧 ・電磁的記録媒体の施錠可能な場所への保管
	1	可用性2の情報資産以外の情報資産	
(2) 情報資産の管理 [①～⑤同左]			
⑥情報資産の保管			
(ア) 情報セキュリティ管理者は、情報資産の分類に従って、情報資産を適正に保管しなければならない。			
(イ) 情報セキュリティ管理者は、情報資産を記録した電磁的記録媒体を長期保管する場合は、書込禁止の措置を講じなければならない。			
(ウ) 情報セキュリティ管理者は、利用頻度が低い電磁的記録媒体や情報システムのバックアップで取得したデータを記録する電磁的記録媒体を長期保管する場合は、自然災害を被る可能性が低い地域に保管するよう努めなければならない。			
(エ) 情報セキュリティ管理者は、機密性2以上、完全性2又は可用性2の情報を記録した電磁的記録媒体を保管する場合、耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。			

⑦情報の送信 <u>電子メール等により自治体機密性2以上の情報を送信する場合は、情報セキュリティ管理者に許可を得た上で、パスワード等による暗号化を行わなければならない。</u> ⑧情報資産の運搬 (ア) 車両等により <u>自治体</u>機密性2以上の情報資産を運搬する者は、鍵付きのケース等に格納し、暗号化又はパスワードの設定を行う等、情報資産の不正利用を防止するための措置を講じなければならない。 (イ) <u>自治体</u>機密性2以上の情報資産を運搬する場合は、情報セキュリティ管理者に許可を得なければならない。 ⑨情報資産の提供・公表 (ア) <u>自治体</u>機密性2以上の情報資産を外部に提供する者は、暗号化又はパスワードの設定を行わなければならない。 (イ) <u>自治体</u>機密性2以上の情報資産を外部に提供する者は、情報セキュリティ管理者に許可を得なければならない。 [(ウ) 略] ⑩情報資産の廃棄 (ア) <u>情報資産の廃棄やリース返却等を行う者は、情報を記録している電磁的記録媒体について、その情報の機密性に応じ、情報を復元できないように処置しなければならない。</u> (イ) 情報資産の廃棄を行う者は、行った処理について、日時、担当者及び処理内容を記録しなければならない。 (ウ) 情報資産の廃棄を行う者は、情報セキュリティ管理者の許可を得なければならない。 4. 情報システム全体の強靱性の向上 (1) 個人番号利用事務系 ①個人番号利用事務系と他の領域との分離 個人番号利用事務系と他の領域を通信できないようにしなければならない。個人番号利用事務系と外部との通信をする必要がある場合は、通信経路の限定(MACアドレス、IPアドレス)及びアプリケーションプロトコル(ポート番号)のレベルでの限定を行わなければならない。<u>また、その外部接続先についてもインターネット等と接続してはならない。ただし、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先については、この限りではなく、LGWANを経由して、インターネット等と個人番号利用事務系との双方向通信でのデータの移送を可能とする。</u> [(②略] (2) LGWAN接続系 ①LGWAN接続系とインターネット接続系の分割 LGWAN接続系とインターネット接続系は両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにしなければならない。なお、メールやデータをLGWAN接続系に取り込む場合は、次の実現方法等により、無害化通信を図らなければならない。 [(ア)・(イ) 略] (ウ) <u>危険因子をファイルから除去し、又は危険因子がファイルに含まれていないことを確認し、インターネット接続系から取り込む方式</u> [(②略] 5. 物理的セキュリティ [5. 1. 略] 5. 2. 管理区域の管理	⑦<u>電子メールによる</u>情報の送信 <u>(ア) 電子メール等により機密性3の情報を送信してはならない。</u> <u>(イ) 機密性2の情報を電子メール等で送信する場合は、情報セキュリティ管理者に許可を得た上で、暗号化又はパスワード設定を行わなければならない。</u> ⑧情報資産の運搬 (ア) 車両等により機密性2以上の情報資産を運搬する者は、必要に応じ鍵付きのケース等に格納し、暗号化又はパスワードの設定を行う等、情報資産の不正利用を防止するための措置を講じなければならない。 (イ) 機密性2以上の情報資産を運搬する場合は、情報セキュリティ管理者に許可を得なければならない。 ⑨情報資産の提供・公表 (ア) 機密性2以上の情報資産を外部に提供する者は、必要に応じ暗号化又はパスワードの設定を行わなければならない。 (イ) 機密性2以上の情報資産を外部に提供する者は、情報セキュリティ管理者に許可を得なければならない。 [(ウ) 同左] ⑩情報資産の廃棄 (ア) <u>機密性2以上の情報資産を廃棄する者は、情報を記録している電磁的記録媒体が不要になった場合、電磁的記録媒体を破壊する等、情報を復元できないように処置した上で廃棄しなければならない。</u> (イ) 情報資産の廃棄を行う者は、行った処理について、日時、担当者及び処理内容を記録しなければならない。 (ウ) 情報資産の廃棄を行う者は、情報セキュリティ管理者の許可を得なければならない。 4. 情報システム全体の強靱性の向上 (1) 個人番号利用事務系 ①個人番号利用事務系と他の領域との分離 個人番号利用事務系と他の領域を通信できないようにしなければならない。<u>ただし、個人番号利用事務系と外部との通信をする必要がある場合は、通信経路の限定(MACアドレス、IPアドレス)及びアプリケーションプロトコル(ポート番号)のレベルでの限定を行わなければならない。なお、外部の接続先もインターネット等と接続してはならない。</u> [(②同左] (2) LGWAN接続系 ①LGWAN接続系とインターネット接続系の分割 LGWAN接続系とインターネット接続系は両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにしなければならない。なお、メールやデータをLGWAN接続系に取り込む場合は、次の実現方法等により、無害化通信を図らなければならない。 [(ア)・(イ) 同左] (ウ) <u>インターネット環境で受信したインターネットメールの添付ファイル及びインターネット上のウェブサイトからダウンロードしたファイルの無害化ソリューションによるサニタイズ処理による取り込み方式</u> [(②同左] 5. 物理的セキュリティ [5. 1. 同左] 5. 2. 管理区域の管理
---	--

(1) 管理区域の構造等 ①管理区域とは、ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理並びに運用を行うための部屋 <u>(以下「電算室」という。)</u> や電磁的記録媒体の保管庫をいう。 〔②略〕 ③統括情報セキュリティ責任者及び情報セキュリティ管理者は、<u>電算室</u>内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。 〔④・⑤略〕 (2) 管理区域の入退室管理等 〔①～③略〕 ④情報セキュリティ管理者は、<u>自治体</u>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において、職員や委託事業者による個人所有等当該情報システムに関連のないコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等の使用禁止を徹底させなければならない。 (3) 機器等の搬入出 〔①略〕 ②情報セキュリティ管理者は、<u>電算室</u>の機器等の搬入出について、委託事業者だけで行うのではなく、必ず職員を立ち会わせなければならない。 5. 3. 通信回線及び通信回線装置の管理 〔①略〕 <u>②統括情報セキュリティ責任者は、情報システムのセキュリティ要件として策定した情報システムのネットワーク構成に関する要件内容に従い、通信回線装置に対して適切なセキュリティ対策を実施しなければならない。</u> <u>③統括情報セキュリティ責任者は、外部へのネットワーク接続を必要最低限に限定しなければならない。</u> <u>④統括情報セキュリティ責任者は、行政系のネットワークを総合行政ネットワーク（LGWAN）に集約するように努めなければならない。</u> <u>⑤統括情報セキュリティ責任者は、自治体機密性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、必要なセキュリティ水準を検討の上、適正な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。</u> <u>⑥統括情報セキュリティ責任者は、ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施しなければならない。</u> <u>⑦統括情報セキュリティ責任者は、自治体</u>可用性2の情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。また、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。 5. 4. 職員等の利用する端末や電磁的記録媒体等の管理 〔①～④略〕 <u>⑤情報セキュリティ管理者は、パソコンやモバイル端末等におけるデータの暗号化等の機能を有効に利用しなければならない。端末にセキュリティチップが搭載されている場合、その機能を有効に活用しなければならない。同様に、電磁的記録媒体についてもデータ暗号化機能を備える媒体を使用しなければならない。</u> 6. 人的セキュリティ 6. 1. 職員等の遵守事項 (1) 職員等の遵守事項 〔①・②略〕 ③情報資産の持ち出し及び外部における情報処理作業の制限 (ア) CIS0は、<u>自治体</u>機密性2以上、<u>自治体</u>可用性2、<u>自治体</u>完全性2の情報資産を外部で処理する場合における安全管理措置を定めなければならない。 〔(イ)・(ウ) 略〕	(1) 管理区域の構造等 ①管理区域とは、ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理並びに運用を行うための部屋や電磁的記録媒体の保管庫をいう。 〔②同左〕 ③統括情報セキュリティ責任者及び情報セキュリティ管理者は、<u>情報システム室</u>内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。 〔④・⑤同左〕 (2) 管理区域の入退室管理等 〔①～③同左〕 ④情報セキュリティ管理者は、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において、職員や委託事業者による個人所有等当該情報システムに関連のないコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等の使用禁止を徹底させなければならない。 (3) 機器等の搬入出 〔①同左〕 ②情報セキュリティ管理者は、<u>情報システム室</u>の機器等の搬入出について、委託事業者だけで行うのではなく、必ず職員を立ち会わせなければならない。 5. 3. 通信回線及び通信回線装置の管理 〔①同左〕 <u>〔新規〕</u> <u>②統括情報セキュリティ責任者は、外部へのネットワーク接続を必要最低限に限定しなければならない。</u> <u>〔新規〕</u> <u>④統括情報セキュリティ責任者は、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、必要なセキュリティ水準を検討の上、適正な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。</u> <u>⑤統括情報セキュリティ責任者は、ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施しなければならない。</u> <u>⑥統括情報セキュリティ責任者は、可用性2の情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。また、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。</u> 5. 4. 職員等の利用する端末や電磁的記録媒体等の管理 〔①～④同左〕 <u>〔新規〕</u> 6. 人的セキュリティ 6. 1. 職員等の遵守事項 (1) 職員等の遵守事項 〔①・②同左〕 ③情報資産の持ち出し及び外部における情報処理作業の制限 (ア) CIS0は、機密性2以上、可用性2、完全性2の情報資産を外部で処理する場合における安全管理措置を定めなければならない。 〔(イ)・(ウ) 同左〕
---	--

④本市管理以外のパソコン等端末及び電磁的記録媒体等の業務利用 (ア) 職員等は、本市管理以外のパソコン等端末及び電磁的記録媒体等を原則業務に利用してはならない。 ただし、<u>本市管理以外のパソコン等端末の業務利用の可否判断をCIS0が行った後に、業務上必要な場合は、情報セキュリティ管理者の許可を得て利用することができる。</u> [(イ) 略] [⑤～⑨略] (2) 非常勤及び<u>会計年度任用職員</u>への対応 ①情報セキュリティポリシー等の遵守 情報セキュリティ管理者は、非常勤及び<u>会計年度任用職員</u>に対し、採用時に情報セキュリティポリシー等のうち、非常勤及び会計年度任用職員が守るべき内容を理解させ、また実施及び遵守させなければならない。 ②情報セキュリティポリシー等の遵守に対する同意 情報セキュリティ管理者は、非常勤及び<u>会計年度任用職員</u>の採用の際、必要に応じ、情報セキュリティポリシー等を遵守する旨の同意書への署名を求めるものとする。 ③インターネット接続及び電子メール使用等の制限 情報セキュリティ管理者は、非常勤及び<u>会計年度任用職員</u>にパソコン等端末による作業を行わせる場合において、当該職員の業務遂行に当たりインターネットへの接続及び電子メールの使用等が必要不可欠であり、かつ正規職員が行うなど代替手段がない場合を除き、これを利用できないようにしなければならない。 [(3)・(4) 略] 6. 2. 研修・訓練 [(1) 略] (2) 研修計画の策定及び実施 [①～③略] <u>④情報セキュリティ管理者は、所管する課室等の研修の実施状況を記録し、統括情報セキュリティ責任者及び情報セキュリティ責任者に対して、報告しなければならない。</u> ⑤CIS0は、必要に応じ、情報セキュリティ委員会に対して、職員等の情報セキュリティ研修の実施状況について報告するものとする。 [(3) 略] (4) 研修・訓練への参加 <u>幹部を含めた</u>職員等は、定められた研修・訓練に参加しなければならない。 6. 3. 情報セキュリティインシデントの報告 (1) 庁内での情報セキュリティインシデントの報告 [①～③略] <u>④情報セキュリティインシデントにより、個人情報・特定個人情報の漏えい等が発生した場合、必要に応じて個人情報保護委員会へ報告しなければならない。</u> (2) 住民等外部からの情報セキュリティインシデントの報告 [①～③略] <u>④CIS0は、情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けるための窓口を設置し、当該窓口への連絡手段を公表しなければならない。</u> (3) 情報セキュリティインシデント原因の究明・記録、再発防止等 [①・②略] ③CSIRTは、情報セキュリティインシデントに関係する情報セキュリティ責任者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示を行わなければならない。<u>また、CSIRTは、同様の情報セキュリティインシデントが別の情報システムにおいても発生している可能性を検討し、必要に応じて当該情報システムを所管する情報システム管理者へ確認を指示しなければならない。</u> [④・⑤略]	④本市管理以外のパソコン等端末及び電磁的記録媒体等の業務利用 (ア) 職員等は、本市管理以外のパソコン等端末及び電磁的記録媒体等を原則業務に利用してはならない。 ただし、<u>業務上必要な場合は、情報セキュリティ管理者の許可を得て利用することができる。</u> [(イ) 同左] [⑤～⑨同左] (2) 非常勤及び<u>臨時職員</u>への対応 ①情報セキュリティポリシー等の遵守 情報セキュリティ管理者は、非常勤及び<u>臨時職員</u>に対し、採用時に情報セキュリティポリシー等のうち、非常勤及び臨時職員が守るべき内容を理解させ、また実施及び遵守させなければならない。 ②情報セキュリティポリシー等の遵守に対する同意 情報セキュリティ管理者は、非常勤及び<u>臨時職員</u>の採用の際、必要に応じ、情報セキュリティポリシー等を遵守する旨の同意書への署名を求めるものとする。 ③インターネット接続及び電子メール使用等の制限 情報セキュリティ管理者は、非常勤及び<u>臨時職員</u>にパソコン等端末による作業を行わせる場合において、当該職員の業務遂行に当たりインターネットへの接続及び電子メールの使用等が必要不可欠であり、かつ正規職員が行うなど代替手段がない場合を除き、これを利用できないようにしなければならない。 [(3)・(4) 同左] 6. 2. 研修・訓練 [(1) 同左] (2) 研修計画の策定及び実施 [①～③同左] <u>[新規]</u> <u>④CIS0は、必要に応じ、情報セキュリティ委員会に対して、職員等の情報セキュリティ研修の実施状況について報告するものとする。</u> [(3) 同左] (4) 研修・訓練への参加 職員等は、定められた研修・訓練に参加しなければならない。 6. 3. 情報セキュリティインシデントの報告 (1) 庁内での情報セキュリティインシデントの報告 [①～③同左] <u>[新規]</u> (2) 住民等外部からの情報セキュリティインシデントの報告 [①～③同左] <u>[新規]</u> (3) 情報セキュリティインシデント原因の究明・記録、再発防止等 [①・②同左] ③CSIRTは、情報セキュリティインシデントに関係する情報セキュリティ責任者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示を行わなければならない。 [④・⑤同左]
---	---

[6. 4. 略] 7. 技術的セキュリティ 7. 1. コンピュータ及びネットワークの管理 [(1) 略] (2) バックアップの実施 <u>①情報セキュリティ管理者は、ファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、必要に応じて定期的にバックアップを実施しなければならない。</u> <u>②統括情報セキュリティ責任者及び情報セキュリティ管理者は、重要な情報を取り扱うサーバ装置については、適切な方法でサーバ装置のバックアップを取得しなければならない。</u> <u>③統括情報セキュリティ責任者及び情報セキュリティ管理者は、重要な情報を取り扱う情報システムを構成する通信回線装置については、運用状態を復元するために必要な設定情報等のバックアップを取得し保管しなければならない。</u> [(3) 略] (4) システム変更記録及び作業の確認 ①情報セキュリティ管理者は、所管する情報システムにおいて、変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適正に管理し、<u>運用・保守によって機器の構成や設定情報等に変更があった場合は、情報セキュリティ対策が適切であるか確認し、必要に応じて見直さなければならない。</u> [②略] [(5) ～ (7) 略] (8) ネットワークの接続制御、経路制御等 ①統括情報セキュリティ責任者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。 ②統括情報セキュリティ責任者は、不正アクセスを防止するため、ネットワークに適正なアクセス制御を施さなければならない。 <u>③統括情報セキュリティ責任者は、保守又は診断のために、外部の通信回線から内部の通信回線に接続された機器等に対して行われるリモートメンテナンスに係る情報セキュリティを確保しなければならない。また、情報セキュリティ対策について、定期的な確認により見直さなければならない。</u> [(9) 略] (10) 外部ネットワークとの接続制限等 [①～③略] ④統括情報セキュリティ責任者及び情報セキュリティ管理者は、ウェブサーバ等をインターネットに公開する場合、<u>次のセキュリティ対策を実施しなければならない。</u> <u>(ア) 庁内ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。</u> <u>(イ) 脆弱性が存在する可能性が増大することを防止するため、ウェブサーバが備える機能のうち、必要な機能のみを利用しなければならない。</u> <u>(ウ) ウェブサーバからの不用意な情報漏えいを防止するための措置を講じなければならない。</u> <u>(エ) 情報システム管理者は、ウェブコンテンツの編集作業を行う主体を限定しなければならない。</u> <u>(オ) インターネットを介して転送される情報の盗聴及び改ざんの防止のため、全ての情報に対する暗号化及び電子証明書による認証の対策を講じなければならない。</u> ⑤情報セキュリティ管理者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、統括情報セキュリティ責任者の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。 [(11) 略] (12) <u>IoT機器を含む</u>特定用途機器のセキュリティ管理 [略] [(13) ～ (14) 略]	[6. 4. 同左] 7. 技術的セキュリティ 7. 1. コンピュータ及びネットワークの管理 [(1) 同左] (2) バックアップの実施 情報セキュリティ管理者は、ファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、必要に応じて定期的にバックアップを実施しなければならない。 <u>[新規]</u> [(3) 同左] (4) システム変更記録及び作業の確認 ①情報セキュリティ管理者は、所管する情報システムにおいて、変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適正に管理しなければならない。 [②同左] [(5) ～ (7) 同左] (8) ネットワークの接続制御、経路制御等 ①統括情報セキュリティ責任者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。 ②統括情報セキュリティ責任者は、不正アクセスを防止するため、ネットワークに適正なアクセス制御を施さなければならない。 <u>[新規]</u> [(9) 同左] (10) 外部ネットワークとの接続制限等 [①～③同左] ④統括情報セキュリティ責任者及び情報セキュリティ管理者は、ウェブサーバ等をインターネットに公開する場合、<u>庁内ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。</u> <u>[新規]</u> ⑤情報セキュリティ管理者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、統括情報セキュリティ責任者の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。 [(11) 同左] (12) 特定用途機器のセキュリティ管理 [略] [(13) ～ (14) 同左]
---	---

(15) 電子メールの利用制限 [①～④略] ⑤職員等は、市で管理していないフリー等の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を使用してはならない。<u>ただし、業務上必要な場合は、情報セキュリティ管理者の許可を得て利用することができる。</u> [(16) ～ (18) 略] (19) 無許可でのネットワーク接続の禁止 <u>①職員等は、本市管理のパソコン等端末を、有線・無線を問わず、その端末を接続して利用するよう、情報セキュリティ管理者によって定められたネットワークと異なるネットワークに接続してはならない。</u> <u>②情報セキュリティ管理者は、必要に応じて、本市管理のパソコン等端末について、端末に搭載されたOSのポリシー設定等により、端末を異なるネットワークに接続できないよう技術的に制限しなければならない。</u> [(20) 略] 7. 2. アクセス制御等 (1) アクセス制御等 [①略] ②利用者IDの取扱い [(ア) ～ (ウ) 略] <u>(エ) 統括情報セキュリティ責任者及び情報セキュリティ管理者は、主体から対象に対する不要なアクセス権限が付与されていないか定期的に確認しなければならない。</u> [③略] (2) 職員等による外部からのアクセス等の制限 [①～⑤略] ⑥職員等は、持ち込んだ又は外部から持ち帰った端末を本市の管理するネットワークに接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認し、<u>情報セキュリティ管理者の許可を得るか、もしくは情報セキュリティ管理者によって事前に定義されたポリシーに従って接続しなければならない。</u> <u>⑦統括情報セキュリティ責任者は、内部のネットワーク又は情報システムに対するインターネットを介した外部からのアクセスを原則として禁止しなければならない。ただし、止むを得ず接続を許可する場合は、利用者のID、パスワード及び生体認証に係る情報等の認証情報並びにこれを記録した媒体（ICカード等）による認証に加えて通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講じなければならない。</u> (3) 認証情報の管理 [①・②略] <u>③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は、認証情報の不正利用を防止するための措置を講じなければならない。</u> [(4) 略] 7. 3. システム開発、導入、保守等 (1) <u>機器等及び</u>情報システムの調達 ①統括情報セキュリティ責任者及び情報セキュリティ管理者は、情報システム開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。<u>また、業務システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮した技術的なセキュリティ機能を調達仕様書に記載しなければならない。</u> [②略] (2) 情報システムの開発 [①～③略] <u>④アプリケーション・コンテンツの開発時の対策</u>	(15) 電子メールの利用制限 [①～④同左] ⑤職員等は、市で管理していないフリー等の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を使用してはならない。 [(16) ～ (18) 同左] (19) 無許可でのネットワーク接続の禁止 <u>職員等は、統括情報セキュリティ責任者の許可なくパソコン等端末をネットワークに接続してはならない。</u> [新規] [(20) 同左] 7. 2. アクセス制御等 (1) アクセス制御等 [①同左] ②利用者IDの取扱い [(ア) ～ (ウ) 同左] [新規] [③同左] (2) 職員等による外部からのアクセス等の制限 [①～⑤同左] ⑥職員等は、持ち込んだ又は外部から持ち帰った端末を本市の管理するネットワークに接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認し<u>なければならない。</u> <u>⑦統括情報セキュリティ責任者は、公衆通信回線（公衆無線LAN等）の庁外通信回線を庁内ネットワークに接続を禁止しなければならない。</u> (3) 認証情報の管理 [①・②同左] [新規] [(4) 同左] 7. 3. システム開発、導入、保守等 (1) 情報システムの調達 ①統括情報セキュリティ責任者及び情報セキュリティ管理者は、情報システム開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。 [②同左] (2) 情報システムの開発 [①～③同左] [新規]
---	---

<u>情報セキュリティ管理者は、ウェブアプリケーションの開発において、セキュリティ要件として定めた仕様に加えて、既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講じなければならない。</u> (3) 情報システムの導入 〔①・②略〕 <u>③機器等の納入時又は情報システムの受入れ時</u> <u>(ア) 情報セキュリティ管理者は、機器等の納入時又は情報システムの受入れ時の確認・検査において、調達仕様書等定められた検査手続に従い、情報セキュリティ対策に係る要件が満たされていることを確認しなければならない。</u> <u>(イ) 情報セキュリティ管理者は、情報システムが構築段階から運用保守段階へ移行する際に、当該情報システムの開発事業者から運用保守事業者へ引継がれる項目に、情報セキュリティ対策に必要な内容が含まれていることを確認しなければならない。</u> <u>(4) 情報システム基盤を管理又は制御するソフトウェア導入時の対策</u> <u>利用するソフトウェアの特性を踏まえ、必要に応じて、以下の実施手順を整備しなければならない。</u> <u>(ア) 情報システムの基盤を管理又は制御するソフトウェアの情報セキュリティ水準の維持に関する手順</u> <u>(イ) 情報システムの基盤を管理又は制御するソフトウェアで発生した情報セキュリティインシデントを認知した際の対処手順</u> <u>(5) 情報システムの基盤を管理又は制御するソフトウェア運用時の対策</u> <u>情報セキュリティ管理者は、利用を認めるソフトウェアについて、定期的な確認による見直しを行わなければならない。</u> <u>(6) システム開発・保守に関連する資料等の整備・保管</u> ①情報セキュリティ管理者は、システム開発・保守に関連する資料及びシステム関連文書を適正に整備・保管しなければならない。 <u>(ア) 情報セキュリティ管理者は、情報システムを新規に構築し、又は更改する際には、情報システム台帳のセキュリティ要件に係る内容を記録又は記載し、当該内容について統括情報セキュリティ責任者に報告しなければならない。</u> <u>(イ) 情報セキュリティ管理者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、以下を全て含む情報システム関連文書を整備しなければならない。</u> ・情報システムを構成するサーバ装置及び端末関連情報 ・情報システムを構成する通信回線及び通信回線装置関連情報 <u>(ウ) 情報セキュリティ管理者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、必要に応じて以下の実施手順を整備しなければならない。</u> ・情報システム構成要素ごとの情報セキュリティ水準の維持に関する手順 ・情報セキュリティインシデントを認知した際の対処手順 ・情報システムが停止した際の復旧手順 〔②略〕 <u>③情報セキュリティ管理者は、情報システムに係るソースコードを適正な方法で保管しなければならない。</u> <u>(7) 情報システムにおける入出力データの正確性の確保</u> ①情報セキュリティ管理者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力除去する機能を組み込むように情報システムを設計しなければならない。 <u>②情報セキュリティ管理者は、ウェブアプリケーションやウェブコンテンツにおいて、次のセキュリティ対策を実施しなければならない。</u> <u>(ア) 利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション及びウェブコンテンツの提供方式等を見直ししなければならない。</u> <u>(イ) 運用中のアプリケーション・コンテンツにおいて、定期的に脆弱性対策の状況を確認し、脆弱性が発覚した際は必要な措置を講じなければならない。</u> <u>(ウ) ウェブアプリケーションやウェブコンテンツにおいて、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。</u>	(3) 情報システムの導入 〔①・②同左〕 <u>〔新規〕</u> <u>〔新規〕</u> <u>〔新規〕</u> <u>(4) システム開発・保守に関連する資料等の整備・保管</u> ①情報セキュリティ管理者は、システム開発・保守に関連する資料及びシステム関連文書を適正に整備・保管しなければならない。 <u>〔新規〕</u> <u>〔新規〕</u> <u>〔新規〕</u> 〔②同左〕 <u>〔新規〕</u> <u>(5) 情報システムにおける入出力データの正確性の確保</u> ①情報セキュリティ管理者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力除去する機能を組み込むように情報システムを設計しなければならない。 <u>②情報セキュリティ管理者は、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合には必要に応じ、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。</u> <u>〔新規〕</u> <u>〔新規〕</u> <u>〔新規〕</u>
--	---

〔③略〕 <u>〔8〕 情報システムの変更管理</u> 〔略〕 <u>〔9〕 開発・保守用のソフトウェアの更新等</u> 〔略〕 <u>〔1 0〕 システム更新又は統合時の検証等</u> 〔略〕 <u>〔1 1〕 情報システムについての対策の見直し</u> <u>情報セキュリティ管理者は、対策の推進計画等に基づき情報システムの情報セキュリティ対策を適切に見直さなければならない。また、本市内で横断的に改善が必要となる情報セキュリティ対策の見直しによる改善指示に基づき、情報セキュリティ対策を適切に見直さなければならない。なお、措置の結果については、統括情報セキュリティ責任者へ報告しなければならない。</u> 7. 4. 不正プログラム対策 （1）統括情報セキュリティ責任者及び情報セキュリティ管理者の措置事項 統括情報セキュリティ責任者及び情報セキュリティ管理者は、不正プログラム対策として、次の事項を措置しなければならない。 〔①～⑨略〕 <u>⑩業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用してはならない。また、当該製品の利用を予定している期間中にパッチやバージョンアップなどの開発元のサポートが終了する予定がないことを確認しなければならない。</u> 〔（2）・（3）略〕 〔7. 5. 略〕 〔7. 6. 略〕 8. 運用 8. 1. 情報システムの監視 <u>〔削る〕</u> （1）情報システムの運用・保守時の対策 <u>①統括情報セキュリティ責任者及び情報セキュリティ管理者は、情報システムの運用・保守において、情報システムに実装された監視を含むセキュリティ機能を適切に運用しなければならない。</u> <u>②統括情報セキュリティ責任者及び情報セキュリティ管理者は、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講じなければならない。</u> <u>③統括情報セキュリティ責任者及び情報セキュリティ管理者は、重要な情報を取り扱う情報システムについて、危機的事象発生時に適切な対処が行えるよう運用をしなければならない。</u> （2）情報システムの監視機能 <u>①統括情報セキュリティ責任者及び情報セキュリティ管理者は、情報システム運用時の監視に係る運用管理機能要件を策定し、監視機能を実装しなければならない。</u> <u>②統括情報セキュリティ責任者及び情報セキュリティ管理者は、情報システムの運用において、情報システムに実装された監視機能を適切に運用しなければならない。</u> <u>③統括情報セキュリティ責任者及び情報セキュリティ管理者は、新たな脅威の出現、運用の状況等を踏まえ、情報システムにおける監視の対象や手法を定期的に見直さなければならない。</u>	〔③同左〕 <u>〔6〕 情報システムの変更管理</u> 〔同左〕 <u>〔7〕 開発・保守用のソフトウェアの更新等</u> 〔同左〕 <u>〔8〕 システム更新又は統合時の検証等</u> 〔同左〕 <u>〔新規〕</u> 7. 4. 不正プログラム対策 （1）統括情報セキュリティ責任者及び情報セキュリティ管理者の措置事項 統括情報セキュリティ責任者及び情報セキュリティ管理者は、不正プログラム対策として、次の事項を措置しなければならない。 〔①～⑨同左〕 <u>〔新規〕</u> 〔（2）・（3）同左〕 〔7. 5. 同左〕 〔7. 6. 同左〕 8. 運用 8. 1. 情報システムの監視 <u>①統括情報セキュリティ責任者及び情報セキュリティ管理者は、セキュリティに関する事案を検知するため、情報システムを監視しなければならない。</u> <u>②統括情報セキュリティ責任者及び情報セキュリティ管理者は、重要な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できる措置を講じなければならない。</u> <u>③統括情報セキュリティ責任者及び情報セキュリティ管理者は、外部と常時接続するシステムを監視しなければならない。</u> <u>〔新規〕</u> <u>〔新規〕</u>
---	---

<u>④統括情報セキュリティ責任者及び情報セキュリティ管理者は、サーバ装置上での情報セキュリティインシデントの発生を監視するため、当該サーバ装置を監視するための措置を講じなければならない。</u> <u>(3) 情報システムの監視</u> <u>①統括情報セキュリティ責任者及び情報セキュリティ管理者は、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。</u> <u>②統括情報セキュリティ責任者及び情報セキュリティ管理者は、重要な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できる措置を講じなければならない。</u> <u>③統括情報セキュリティ責任者及び情報セキュリティ管理者は、外部と常時接続するシステムを常時監視しなければならない。</u> [8. 2. 略] [8. 3. 略] [8. 4. 略] 8. 5. 法令遵守 職員等は、職務の遂行において使用する情報資産を保護するために、次の法令のほか関係法令を遵守し、これに従わなければならない。 [①～⑥略] <u>⑦栗東市個人情報保護法施行条例（令和5年3月23日条例第3号）</u> [8. 6. 略] 9. <u>業務委託と外部サービス（クラウドサービス）の利用</u> 9. 1. <u>業務委託</u> <u>[削る]</u> <u>(1) 業務委託実施前の対策</u> <u>①情報セキュリティ管理者は、業務委託の実施までに、以下を全て含む事項を実施しなければならない。</u> <u>(ア) 委託する業務内容の特定</u> <u>(イ) 委託事業者の選定条件を含む仕様の策定</u> <u>(ウ) 仕様に基づく委託事業者の選定</u> <u>(エ) 情報セキュリティ要件を明記した契約の締結（契約項目）</u> <u>重要な情報資産を取扱う業務を委託する場合には、委託事業者との間で必要に応じて次の情報セキュリティ等に係る要件を明記した契約を締結しなければならない。</u> <u>・情報セキュリティポリシー及び情報セキュリティ実施手順の遵守</u> <u>・個人情報漏えい防止のための技術的安全管理措置に関する取り決め</u> <u>・委託事業者の責任者、委託内容、作業者の所属、作業場所の特定</u> <u>・提供されるサービスレベルの保証</u> <u>・委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法の明確化など、情報のライフサイクル全般での管理方法</u> <u>・委託事業者の従業員に対する教育の実施</u> <u>・提供された情報の目的外利用及び委託事業者以外の者への提供の禁止</u> <u>・業務上知り得た情報の守秘義務</u> <u>・再委託に関する制限事項の遵守</u>	<u>[新規]</u> [8. 2. 同左] [8. 3. 同左] [8. 4. 同左] 8. 5. 法令遵守 職員等は、職務の遂行において使用する情報資産を保護するために、次の法令のほか関係法令を遵守し、これに従わなければならない。 [①～⑥略] <u>[新規]</u> [8. 6. 略] 9. 外部サービスの利用 9. 1. 委託 <u>(1) 委託事業者の選定基準</u> <u>①情報セキュリティ管理者は、委託事業者の選定にあたり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。</u> <u>②情報セキュリティ管理者は、必要に応じ、情報セキュリティマネジメントシステムの国際規格認証取得状況、情報セキュリティ監査の実施状況等を参考にして、事業者を選定する。</u> <u>③情報セキュリティ管理者は、クラウドサービスを利用する場合は、情報の機密性に応じたセキュリティレベルが確保されているサービスを利用しなければならない。</u> <u>[新規]</u>
--	---

・委託業務終了時の情報資産の返還、廃棄等 ・委託業務の定期報告及び緊急時報告義務 ・市による監査、検査 ・市による情報セキュリティインシデント発生時の公表 ・情報セキュリティポリシーが遵守されなかった場合の規定（損害賠償等） (オ) 委託事業者に重要情報を提供する場合は、秘密保持契約（NDA）の締結 ②情報セキュリティ管理者は、業務委託の実施までに、委託の前提条件として、以下を全て含む事項の実施を委託事業者に求めなければならない。 (ア) 仕様に準拠した提案 (イ) 契約の締結 (ウ) 委託事業者において重要情報を取り扱う場合は、秘密保持契約（NDA）の締結 [削る] (2) 業務委託実施期間中の対策 ①情報セキュリティ管理者は、業務委託の実施期間において、以下をすべて含む対策を実施しなければならない。 (ア) 委託判断基準に従った重要情報の提供 (イ) 契約に基づき委託事業者に実施させる情報セキュリティ対策の履行状況の定期的な確認及び措置の実施 (ウ) 委託した業務において、情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合又はその旨の報告を職員等より受けた場合における、委託事業の一時中断などの必要な措置を含む、契約に基づく対処の要求 ②情報セキュリティ管理者は、業務委託の実施期間において、以下を全て含む対策の実施を委託事業者に求めなければならない。 (ア) 情報の適正な取扱いのための情報セキュリティ対策 (イ) 契約に基づき委託事業者が実施する情報セキュリティ対策の履行状況の定期的な報告 (ウ) 委託した業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合における、委託事業の一時中断などの必要な措置を含む対処 [削る] (3) 業務委託終了時の対策 ①情報セキュリティ管理者は、業務委託の終了に際して、以下を全て含む対策を実施しなければならない。 (ア) 業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの確認を含む検収	(2) 契約項目 情報システムの運用、保守等を委託する場合には、委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。 ・情報セキュリティポリシー及び情報セキュリティ実施手順の遵守 ・委託事業者の責任者、委託内容、作業者の所属、作業場所の特定 ・提供されるサービスレベルの保証 ・外部委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法 ・外部委託事業者の従業員に対する教育の実施 ・提供された情報の目的外利用及び受託者以外の者への提供の禁止 ・業務上知り得た情報の守秘義務 ・再委託に関する制限事項の遵守 ・委託業務終了時の情報資産の返還、廃棄等 ・委託業務の定期報告及び緊急時報告義務 ・本市による監査、検査 ・本市による情報セキュリティインシデント発生時の公表 ・情報セキュリティポリシーが遵守されなかったことにより本市に損害が生じた場合の損害賠償等の規定 [新規] (3) 確認・措置等 情報セキュリティ管理者は、委託事業者において必要なセキュリティ対策が確保されていることを定期的に確認し、必要に応じ、(2)の契約に基づき措置しなければならない。また、その内容を統括情報セキュリティ責任者に報告するとともに、その重要度に応じてCIS0に報告しなければならない。 [新規]
--	---

<u>(イ) 委託事業者に提供した情報を含め、委託事業者において取り扱われた情報が確実に返却、廃棄又は抹消されたことの確認</u> <u>②情報セキュリティ管理者は、業務委託の終了に際して、以下を全て含む対策の実施を委託事業者に求めなければならない。</u> <u>(ア) 業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの報告を含む検収の受検</u> <u>(イ) 提供を受けた情報を含め、委託業務において取り扱った情報の返却、廃棄又は抹消</u> <u>9. 2. 情報システムに関する業務委託</u> <u>(1) 情報システムに関する業務委託における共通対策</u> <u>情報セキュリティ管理者は、情報システムに関する業務委託の実施までに、情報システムに本市の意図せざる変更が加えられないための対策に係る選定条件を委託事業者の選定条件に加え、仕様を策定しなければならない。</u> <u>(2) 情報システムの構築を業務委託する場合の対策</u> <u>情報セキュリティ管理者は、情報システムの構築を業務委託する場合は、契約に基づき、以下を全て含む対策の実施を委託事業者に求めなければならない。</u> <u>①情報システムのセキュリティ要件の適切な実装</u> <u>②情報セキュリティの観点に基づく試験の実施</u> <u>③情報システムの開発環境及び開発工程における情報セキュリティ対策</u> <u>(3) 情報システムの運用・保守を業務委託する場合の対策</u> <u>①情報セキュリティ管理者は、情報システムの運用・保守を業務委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、契約に基づき、委託事業者に実施を求めなければならない。</u> <u>②情報セキュリティ管理者は、情報システムの運用・保守を業務委託する場合は、委託事業者が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、契約に基づき、委託事業者に速やかな報告を求めなければならない。</u> <u>(4) 本市向けに情報システムの一部の機能を提供するサービスを利用する場合の対策</u> <u>①情報セキュリティ管理者は、外部の一般の者が本市向けに重要情報を取り扱う情報システムの一部の機能を提供するサービス（クラウドサービスを除く。）（以下「業務委託サービス」という。）を利用するため、情報システムに関する業務委託を実施する場合は、委託事業者の選定条件に業務委託サービスに特有の選定条件を加えなければならない。</u> <u>②情報セキュリティ管理者は、業務委託サービスに係るセキュリティ要件を定め、業務委託サービスを選定しなければならない。</u> <u>③情報セキュリティ管理者は、委託事業者の信頼性が十分であることを総合的・客観的に評価し判断しなければならない。</u> <u>④情報セキュリティ管理者は業務委託サービスを利用する場合には、統括情報セキュリティ責任者又は情報セキュリティ責任者へ当該サービスの利用申請を行わなければならない。</u> <u>⑤統括情報セキュリティ責任者又は情報セキュリティ責任者は、業務委託サービスの利用申請を受けた場合は、当該利用申請を審査し、利用の可否を決定しなければならない。</u> <u>⑥統括情報セキュリティ責任者又は情報セキュリティ責任者は、業務委託サービスの利用申請を承認した場合は、承認済み業務委託サービスとして記録し、業務委託サービス管理者を指名しなければならない。</u> <u>9. 3. 外部サービス（クラウドサービス）の利用（自治体機密性2以上の情報を取り扱う場合）</u> <u>〔削る〕</u> <u>(1) クラウドサービスの選定に係る運用規程の整備</u>	<u>〔新規〕</u> <u>9. 2. 外部サービスの利用</u> <u>職員等は、インターネット上で不特定多数に提供されるメール、ネットワークストレージサービス等を使用してはならない。ただし、業務上必要であり使用する場合は、情報セキュリティ管理者が利用に関する規定を整備し、統括情報セキュリティ責任者の許可を得なければならない。また、その際に機密性2以上の情報を取り扱ってはならない。利用するサービスの約款、その他提供条件から、利用に当たってのリスクが許容できることを確認した上で約款による外部サービスの利用を申請し、適正な措置を講じた上で利用しなければならない。</u> <u>〔新規〕</u>
--	--

<u>統括情報セキュリティ責任者は、自治体機密性 2 以上の情報を取り扱う場合、以下を含む外部サービス（クラウドサービス、以下「クラウドサービス」という。）の選定に関する規定を整備しなければならない。</u> <u>①クラウドサービスを利用可能な業務及び情報システムの範囲並びに情報の取扱いを許可する場所を判断する基準（以下、9. 3 節において「クラウドサービス利用判断基準」という。）</u> <u>②クラウドサービス提供者の選定基準</u> <u>③クラウドサービスの利用手続</u> <u>④クラウドサービスの利用状況の管理</u> <u>（2）クラウドサービスの利用に係る運用規程の整備</u> <u>統括情報セキュリティ責任者は、自治体機密性 2 以上の情報を取り扱う場合、以下を含むクラウドサービス（自治体機密性 2 以上の情報を取り扱う場合）の利用に関する規定を整備しなければならない。</u> <u>①統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方等を踏まえ、クラウドサービスを利用して情報システムを導入・構築する際のセキュリティ対策の基本方針を運用規程として整備しなければならない。</u> <u>②統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、クラウドサービスを利用して情報システムを運用・保守する際のセキュリティ対策の基本方針を運用規程として整備しなければならない。</u> <u>③統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下を全て含むクラウドサービスの利用を終了する際のセキュリティ対策の基本方針を運用規程として整備しなければならない。</u> <u>（ア）クラウドサービスの利用終了時における対策</u> <u>（イ）クラウドサービスで取り扱った情報の廃棄</u> <u>（ウ）クラウドサービスの利用のために作成したアカウントの廃棄</u> <u>（3）クラウドサービスの選定</u> <u>①情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限を踏まえ、クラウドサービス利用判断基準に従って、業務に係る影響度等を検討した上でクラウドサービスの利用を検討しなければならない。</u> <u>②情報セキュリティ責任者は、クラウドサービスで取り扱う情報の格付及び取扱制限を踏まえ、クラウドサービス提供者の選定基準に従ってクラウドサービス提供者を選定すること。また、以下の内容を含む情報セキュリティ対策をクラウドサービス提供者の選定条件に含めなければならない。</u> <u>（ア）クラウドサービスの利用を通じて本市が取り扱う情報のクラウドサービス提供者における目的外利用の禁止</u> <u>（イ）クラウドサービス提供者における情報セキュリティ対策の実施内容及び管理体制</u> <u>（ウ）クラウドサービスの提供に当たり、クラウドサービス提供者若しくはその従業員、再委託先又はその他の者によって、本市の意図しない変更が加えられないための管理体制</u> <u>（エ）クラウドサービス提供者の資本関係・役員等の情報、クラウドサービス提供に従事する者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供並びに調達仕様書による施設の場所やリージョンの指定</u> <u>（オ）情報セキュリティインシデントへの対処方法</u> <u>（カ）情報セキュリティ対策その他の契約の履行状況の確認方法</u> <u>（キ）情報セキュリティ対策の履行が不十分な場合の対処方法</u> <u>③情報セキュリティ責任者は、クラウドサービスの中断や終了時に円滑に業務を移行するための対策を検討し、クラウドサービス提供者の選定条件に含めなければならない。</u> <u>④情報セキュリティ責任者は、クラウドサービスの利用を通じて本市が取り扱う情報の格付等を勘案し、必要に応じて以下の内容をクラウドサービス提供者の選定条件に含めなければならない。</u> <u>（ア）情報セキュリティ監査の受入れ</u> <u>（イ）サービスレベルの保証</u> <u>⑤情報セキュリティ責任者は、クラウドサービスの利用を通じて本市が取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクを評価してクラウドサービス提供者を選定し、必要に応じて本市の情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を選定条件に含めなければならない。</u> <u>⑥情報セキュリティ責任者は、クラウドサービス提供者がその役務内容を一部再委託する場合は、再委託</u>	
---	--

<u>されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、クラウドサービス提供者の選定条件で求める内容をクラウドサービス提供者に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を本市に提供し、本市の承認を受けるよう、クラウドサービス提供者の選定条件に含めなければならない。また、クラウドサービス利用判断基準及びクラウドサービス提供者の選定基準に従って再委託の承認の可否を判断しなければならない。</u> <u>⑦情報セキュリティ責任者は、クラウドサービスの特性を考慮した上で、クラウドサービスが提供する部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上で、情報セキュリティに関する役割及び責任の範囲を踏まえて、以下を全て含むセキュリティ要件を定めなければならない。</u> <u>(ア) クラウドサービスに求める情報セキュリティ対策</u> <u>(イ) クラウドサービスで取り扱う情報が保存される国・地域及び廃棄の方法</u> <u>(ウ) クラウドサービスに求めるサービスレベル</u> <u>⑧統括情報セキュリティ責任者は、情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、クラウドサービス提供者の信頼性が十分であることを総合的・客観的に評価し判断しなければならない。</u> <u>(4) クラウドサービスの利用に係る調達・契約</u> <u>①情報セキュリティ責任者は、クラウドサービスを調達する場合は、クラウドサービス提供者の選定基準及び選定条件並びにクラウドサービスの選定時に定めたセキュリティ要件を調達仕様に含めなければならない。</u> <u>②情報セキュリティ責任者は、クラウドサービスを調達する場合は、クラウドサービス提供者及びクラウドサービスが調達仕様を満たすことを契約までに確認し、利用承認を得なければならない。また、調達仕様の内容を契約に含めなければならない。</u> <u>(5) クラウドサービスの利用承認</u> <u>①情報セキュリティ責任者は、クラウドサービスを利用する場合には、統括情報セキュリティ責任者へクラウドサービスの利用申請を行わなければならない。</u> <u>②統括情報セキュリティ責任者は、職員等によるクラウドサービスの利用申請を審査し、利用の可否を決定しなければならない。</u> <u>③統括情報セキュリティ責任者は、クラウドサービスの利用申請を承認した場合は、承認済みクラウドサービスとして記録しなければならない。</u> <u>(6) クラウドサービスを利用した情報システムの導入・構築時の対策</u> <u>①統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方等を踏まえ、以下を含むクラウドサービスを利用して情報システムを構築する際のセキュリティ対策を規定しなければならない。</u> <u>(ア) 不正なアクセスを防止するためのアクセス制御</u> <u>(イ) 取り扱う情報の機密性保護のための暗号化</u> <u>(ウ) 開発時におけるセキュリティ対策</u> <u>(エ) 設計・設定時の誤りの防止</u> <u>②情報セキュリティ管理者は、情報システムにおいてクラウドサービスを利用する際には、情報システム台帳及び関連文書に記録又は記載しなければならない。</u> <u>③情報セキュリティ管理者は、クラウドサービスの情報セキュリティ対策を実施するために必要となる文書として、クラウドサービスの運用開始前までに以下の実施手順を整備しなければならない。</u> <u>(ア) クラウドサービスで利用するサービスごとの情報セキュリティ水準の維持に関する手順</u> <u>(イ) クラウドサービスを利用した情報システムの運用・監視中における情報セキュリティインシデントを認知した際の対処手順</u> <u>(ウ) 利用するクラウドサービスが停止又は利用できなくなった際の復旧手順</u> <u>④情報セキュリティ管理者は、前項において定める規定に対し、構築時に実施状況を確認・記録しなければならない。</u> <u>(7) クラウドサービスを利用した情報システムの運用・保守時の対策</u> <u>①統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下を</u>	
---	--

<u>含むクラウドサービスを利用して情報システムを運用する際のセキュリティ対策を規定しなければならない。</u> <u>(ア) クラウドサービス利用方針の規定</u> <u>(イ) クラウドサービス利用に必要な教育</u> <u>(ウ) 取り扱う資産の管理</u> <u>(エ) 不正アクセスを防止するためのアクセス制御</u> <u>(オ) 取り扱う情報の機密性保護のための暗号化</u> <u>(カ) クラウドサービス内の通信の制御</u> <u>(キ) 設計・設定時の誤りの防止</u> <u>(ク) クラウドサービスを利用した情報システムの事業継続</u> <u>②情報セキュリティ管理者は、クラウドサービスの運用・保守時に情報セキュリティ対策を実施するために必要となる項目等で修正又は変更等が発生した場合、情報システム台帳及び関連文書を更新又は修正し、統括情報セキュリティ責任者へ報告しなければならない。</u> <u>③情報セキュリティ管理者は、クラウドサービスの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講じなければならない。</u> <u>④情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、クラウドサービスで発生したインシデントを認知した際の対処手順を整備しなければならない。</u> <u>⑤情報セキュリティ管理者は、前各項において定める規定に対し、運用・保守時に実施状況を定期的を確認・記録しなければならない。</u> <u>(8) クラウドサービスを利用した情報システムの更改・廃棄時の対策</u> <u>①統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下を含むクラウドサービスの利用を終了する際のセキュリティ対策を規定しなければならない。</u> <u>(ア) クラウドサービスの利用終了時における対策</u> <u>(イ) クラウドサービスで取り扱った情報の廃棄</u> <u>(ウ) クラウドサービスの利用のために作成したアカウントの廃棄</u> <u>②情報セキュリティ管理者は、前項において定める規定に対し、クラウドサービスの利用終了時に実施状況を確認・記録しなければならない。</u> <u>9. 4. 外部サービス（クラウドサービス）の利用（自治体機密性2以上の情報を取り扱わない場合）</u> <u>(1) クラウドサービスの利用に係る規定の整備統括情報セキュリティ責任者は、自治体機密性2以上の情報を取り扱わない場合、以下を含むクラウドサービスの利用に関する規定を整備しなければならない。</u> <u>(ア) クラウドサービスを利用可能な業務の範囲</u> <u>(イ) クラウドサービスの利用申請の許可権限者と利用手続</u> <u>(ウ) クラウドサービスの利用状況の管理</u> <u>(エ) クラウドサービスの利用の運用手続</u> <u>(2) クラウドサービスの利用における対策の実施</u> <u>①職員等は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で自治体機密性2以上の情報を取り扱わない場合のクラウドサービスの利用を申請しなければならない。また、情報セキュリティ管理者は、当該クラウドサービスの利用において適切な措置を講じなければならない。</u> <u>②情報セキュリティ責任者は、職員等によるクラウドサービスの利用申請を審査し、利用の可否を決定しなければならない。また、承認したクラウドサービスを記録しなければならない。</u> <u>9. 5. ソーシャルメディアサービスの利用</u> <u>〔①略〕</u> <u>②自治体機密性2以上の情報はソーシャルメディアサービスで発信してはならない。</u> <u>〔③略〕</u> <u>④アカウント乗っ取りを確認した場合には、被害を最小限にするための措置を講じなければならない。</u> <u>⑤自治体可用性2の情報の提供にソーシャルメディアサービスを用いる場合は、本市の自己管理ウェブサ</u>	<u>〔新規〕</u> <u>9. 3. ソーシャルメディアサービスの利用</u> <u>〔①同左〕</u> <u>②機密性2以上の情報はソーシャルメディアサービスで発信してはならない。</u> <u>〔③同左〕</u> <u>〔新規〕</u> <u>〔新規〕</u>
--	---

<u>イトに当該情報を掲載して参照可能とすること。</u> 1 0. 評価・見直し 1 0. 1. 監査 (1) 実施方法 CISOは、情報セキュリティ監査<u>統括</u>責任者を指名し、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、必要に応じて監査を行わせなければならない。 (2) 監査を行う者の要件 ①情報セキュリティ監査<u>統括</u>責任者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。 [②略] (3) 監査実施計画の立案及び実施への協力 ①情報セキュリティ監査<u>統括</u>責任者は、監査を行うに当たって、監査実施計画を立案し、CISO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略] (4) 委託事業者に対する監査 委託事業者に委託している場合、情報セキュリティ監査<u>統括</u>責任者は委託事業者から下請けとして受託している事業者も含めて、情報セキュリティポリシーの遵守について監査を必要に応じて行わなければならない。 (5) 報告 情報セキュリティ監査<u>統括</u>責任者は、監査結果を取りまとめ、CISOに報告を行うものとする。<u>また、必要に応じ、情報セキュリティ委員会に報告を行うものとする。</u> (6) 保管 情報セキュリティ監査<u>統括</u>責任者は、監査の実施を通して収集した監査証拠、監査報告書の作成のための監査調書を、紛失等が発生しないように適正に保管しなければならない。 (7) 監査結果への対応 ①CISOは、監査結果を踏まえ、指摘事項を所管する情報セキュリティ管理者に対し、当該事項への対処を指示しなければならない。また、指摘事項を所管していない情報セキュリティ管理者に対しても、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。 <u>②CISOは、指摘事項を所管していない情報セキュリティ管理者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。また、庁内で横断的に改善が必要な事項については、統括情報セキュリティ責任者に対し、当該事項への対処（改善計画の策定等）を指示しなければならない。なお、措置が完了していない改善計画は、定期的に進捗状況の報告を指示しなければならない。</u> [(8) 略] [1 0. 2. 略] [1 0. 3. 略] 附則（略） <u>附則（令和7年3月日市長決裁）</u> <u>栗東市情報セキュリティポリシーは、令和7年4月1日から施行する。</u>	1 0. 評価・見直し 1 0. 1. 監査 (1) 実施方法 CISOは、情報セキュリティ監査責任者を指名し、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、必要に応じて監査を行わせなければならない。 (2) 監査を行う者の要件 ①情報セキュリティ監査責任者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。 [②同左] (3) 監査実施計画の立案及び実施への協力 ①情報セキュリティ監査責任者は、監査を行うに当たって、監査実施計画を立案し、CISOの承認を得なければならない。 [②同左] (4) 委託事業者に対する監査 委託事業者に委託している場合、情報セキュリティ監査責任者は委託事業者から下請けとして受託している事業者も含めて、情報セキュリティポリシーの遵守について監査を必要に応じて行わなければならない。 (5) 報告 情報セキュリティ監査責任者は、監査結果を取りまとめ、CISOに報告を行うものとする。 (6) 保管 情報セキュリティ監査責任者は、監査の実施を通して収集した監査証拠、監査報告書の作成のための監査調書を、紛失等が発生しないように適正に保管しなければならない。 (7) 監査結果への対応 CISOは、監査結果を踏まえ、指摘事項を所管する情報セキュリティ管理者に対し、当該事項への対処を指示しなければならない。また、指摘事項を所管していない情報セキュリティ管理者に対しても、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。 <u>[新規]</u> [(8) 同左] [1 0. 2. 同左] [1 0. 3. 同左] 附則（略） <u>[新規]</u>
--	--

- 附 則
- 1 この要綱は、令和7年4月1日から施行する。

栗東市情報セキュリティポリシー

制定日：平成 17 年 3 月 30 日

改定日：令和 7 年 月 日

施行日：令和 7 年 月 日

【目次】

I 情報セキュリティ基本方針

1. 目的.....	1
2. 定義.....	1
3. 対象とする脅威	2
4. 適用範囲	2
5. 職員等の遵守義務.....	3
6. 情報セキュリティ対策.....	4
7. 情報セキュリティ監査及び自己点検の実施.....	4
8. 情報セキュリティポリシーの見直し.....	4
9. 情報セキュリティ対策基準の策定	4
10. 情報セキュリティ実施手順の策定.....	5
11. 懲戒処分.....	5

II 情報セキュリティ対策基準

1. 目的.....	6
2. 組織体制	6
3. 情報資産の分類と管理.....	10
4. 情報システム全体の強靱性の向上	14
5. 物理的セキュリティ	16
5. 1. サーバ等の管理.....	16
5. 2. 管理区域の管理.....	17
5. 3. 通信回線及び通信回線装置の管理	18
5. 4. 職員等の利用する端末や電磁的記録媒体等の管理.....	19
6. 人的セキュリティ	20
6. 1. 職員等の遵守事項.....	20
6. 2. 研修・訓練.....	21
6. 3. 情報セキュリティインシデントの報告	22
6. 4. ID 及びパスワード等の管理.....	23
7. 技術的セキュリティ	25
7. 1. コンピュータ及びネットワークの管理	25
7. 2. アクセス制御等.....	29
7. 3. システム開発、導入、保守等.....	31
7. 4. 不正プログラム対策	34

7. 5. 不正アクセス対策	36
7. 6. セキュリティ情報の収集	37
8. 運用	38
8. 1. 情報システムの監視	38
8. 2. 情報セキュリティポリシーの遵守状況の確認	38
8. 3. 侵害時の対応等	39
8. 4. 例外措置	40
8. 5. 法令順守	40
8. 6. 違反時の対応	40
9. 業務委託と外部サービス（クラウドサービス）の利用	42
9. 1. 業務委託	42
9. 2. 情報システムに関する業務委託	43
9. 3. 外部サービス（クラウドサービス）の利用（自治体機密性2以上の情報を 取り扱う場合）	44
9. 4. 外部サービス（クラウドサービス）の利用（自治体機密性2以上の情報を 取り扱わない場合）	49
9. 5. ソーシャルメディアサービスの利用	49
10. 評価・見直し	51
10. 1. 監査	51
10. 2. 自己点検	52
10. 3. 情報セキュリティポリシー及び関係規定等の見直し	52

I 情報セキュリティ基本方針

1. 目的

本基本方針は、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、本市が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

2. 定義

(1) ネットワーク

コンピュータ等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。

(2) 情報システム

コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

(3) 情報資産

情報そのものだけでなく、書類、データ、ハードウェア、ソフトウェア、設備、ファームウェア、要員、文書等の情報を取り扱う仕組みを含む概念をいう。

(4) 情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

(5) 情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

(6) 機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

(7) 完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

(8) 可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

(9) 個人番号利用事務系

個人番号利用事務（社会保障、地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及びデータをいう。

(10) LGWAN 接続系

LGWAN に接続された情報システム及びその情報システムで取り扱うデータをいう。

(11) インターネット接続系

インターネットメール、ホームページ管理システム等に関わるインターネットに接

続された情報システム及びその情報システムで取り扱うデータをいう。

(1 2) 通信経路の分割

LGWAN 接続系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。

(1 3) 無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

(1 4) 情報セキュリティインシデント

情報管理、情報システム運用に関して保安上の脅威となる事象のことをいう。

(1 5) 外部サービス

本市以外の者が一般向けに情報システムの一部又は全部の機能を提供するものをいう。ただし、当該機能において本市の情報が取り扱われる場合に限る。

(1 6) クラウドサービス

外部サービスの中で、事業者等によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスをいう。

3. 対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

- (1) 不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等
- (2) 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障等の非意図的な要因による情報資産の漏えい・破壊・消去等
- (3) 地震、落雷、火災等の災害によるサービス及び業務の停止等
- (4) 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等
- (5) 電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

4. 適用範囲

(1) 組織の範囲

情報セキュリティポリシーが適用される組織は、栗東市個人情報保護法施行条例（令和5年条例第3号）第2条第2項に定める実施機関及び議会事務局とする。

(2) 情報資産の範囲

情報セキュリティポリシーが対象とする情報資産は、次のとおりとする。但し、小・中学校において児童・生徒が使用し、専ら教育の用に供するものは除く。

- ①ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体
- ②ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）
- ③情報システムの仕様書及びネットワーク図等のシステム関連文書

5. 職員等の遵守義務

職員、教職員、非常勤職員及び会計年度任用職員（以下「職員等」という。）は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。

また、職員等は、本市の情報資産を利用する委託業務従事者等に対して、適切な情報の取扱いについて指示し、管理・監督しなければならない。

6. 情報セキュリティ対策

上記3の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

（1）組織体制

本市の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。

（2）情報資産の分類と管理

本市の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

（3）情報システム全体の強靱性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる。

- ①個人番号利用事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。
- ②LGWAN 接続系においては、LGWAN と接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。
- ③インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、滋賀県自治体情報セキュリティクラウドによりインターネット接続を行う。（小・中学校において、児童、生徒及び教職員が利用するインターネット接続を除く。）

（4）物理的セキュリティ

サーバ、情報システム室、通信回線等及び職員等のパソコン等の管理について、物理

的な対策を講じる。

(5) 人的セキュリティ

情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

(6) 技術的セキュリティ

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

(7) 運用

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。

(8) 業務委託と外部サービスの利用

業務委託する場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。外部サービスを利用する場合には、利用にかかる規定を整備し対策を講じる。ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

(9) 評価・見直し

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施し、運用改善を行い情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、情報セキュリティポリシーの見直しを行う。

7. 情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

8. 情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要となった場合には、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、情報セキュリティポリシーを見直す。

9. 情報セキュリティ対策基準の策定

上記6、7及び8に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

なお、情報セキュリティ対策基準は、公にすることにより本市の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。

10. 情報セキュリティ実施手順の策定

情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティ実施手順は、公にすることにより本市の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。

11. 懲戒処分

情報セキュリティポリシーに違反した職員等（県費負担教職員を除く）及びその監督責任者は、その重大性、発生した事案の状況等に応じて、地方公務員法による懲戒処分の対象とする。

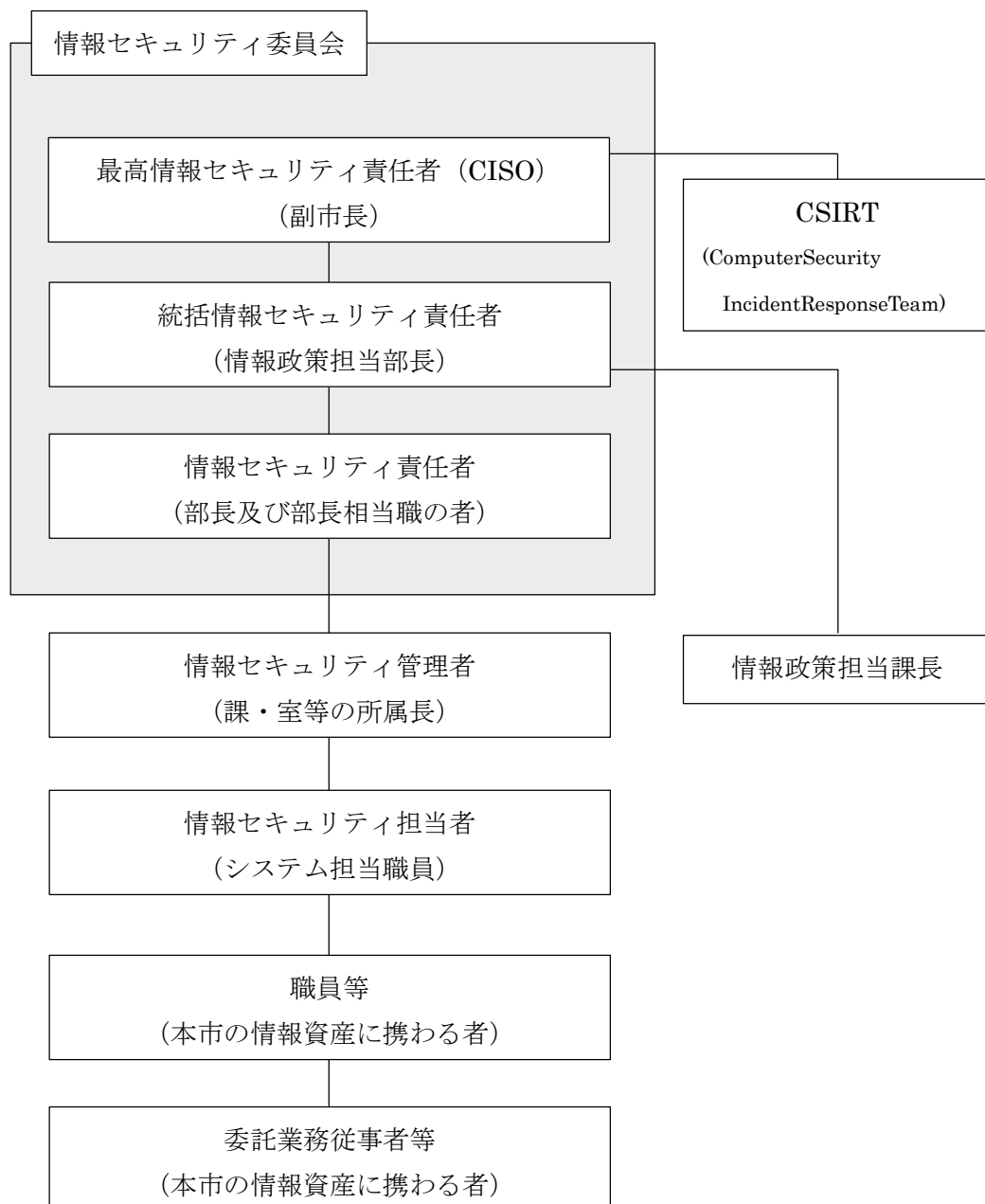
Ⅱ 情報セキュリティ対策基準

1. 目的

本対策基準は、情報セキュリティ基本方針を実行に移すための、本市における情報資産に関する情報セキュリティ対策の基準を定めることを目的とする。

2. 組織体制

情報セキュリティ対策を実施するための組織体制は、以下のとおりとする。



(1) 最高情報セキュリティ責任者(CISO:ChiefInformationSecurityOfficer、以下「CISO」という。)

- ①副市長を CISO とする。CISO は、本市における全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。
- ②CISO は、情報セキュリティインシデントに対処するための体制（CSIRT：ComputerSecurityIncidentResponseTeam、以下「CSIRT」という。）を整備し、なければならない。

(2) 統括情報セキュリティ責任者

- ①情報政策担当部長を CISO 直属の統括情報セキュリティ責任者とする。統括情報セキュリティ責任者は、CISO を補佐しなければならない。
- ②統括情報セキュリティ責任者は、本市の全てのネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。
- ③統括情報セキュリティ責任者は、本市の全てのネットワークにおける情報セキュリティ対策に関する権限及び責任を有する。
- ④統括情報セキュリティ責任者は、情報セキュリティ責任者、情報セキュリティ管理者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。
- ⑤統括情報セキュリティ責任者は、本市の情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合に、CISO の指示に従い、CISO が不在の場合には自らの判断に基づき、必要かつ十分な措置を実施する権限及び責任を有する。
- ⑥統括情報セキュリティ責任者は、本市の共通的なネットワーク、情報システム及び情報資産に関する情報セキュリティ実施手順の維持・管理を行う権限及び責任を有する。
- ⑦統括情報セキュリティ責任者は、緊急時等の円滑な情報共有を図るため、CISO、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を網羅する連絡体制を含めた緊急連絡網を整備しなければならない。
- ⑧統括情報セキュリティ責任者は、緊急時には CISO に早急に報告を行うとともに、回復のための対策を講じなければならない。
- ⑨統括情報セキュリティ責任者は、情報セキュリティ関係規程に係る課題及び問題点を含む運用状況を適時に把握し、必要に応じて CISO にその内容を報告しなければならない。
- ⑩統括情報セキュリティ責任者は、自身の権限に属する事務を情報政策担当課長に処理させることができる。

(3) 情報セキュリティ責任者

- ①部長及び部長相当職にある者を情報セキュリティ責任者とする。

- ②情報セキュリティ責任者は、当該部局等の情報セキュリティ対策に関する統括的な権限及び責任を有する。
- ③情報セキュリティ責任者は、その所管する部局等において所有している情報システムにおける開発、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。
- ④情報セキュリティ責任者は、その所管する部局等において所有している情報システムについて、緊急時等における連絡体制の整備、情報セキュリティポリシーの遵守に関する意見の集約並びに職員等に対する教育、訓練、助言及び指示を行う。

(4) 情報セキュリティ管理者

- ①各課室等の所属長を情報セキュリティ管理者とする。
- ②情報セキュリティ管理者は、その所管する課室等の情報セキュリティ対策に関する権限及び責任を有する。
- ③情報セキュリティ管理者は、その所管する課室等において、情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には、**CSIRT** へ速やかに報告を行い、指示を仰がなければならない。併せて情報セキュリティ責任者へ報告しなければならない。
- ④情報セキュリティ管理者は、所管する情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。
- ⑤情報セキュリティ管理者は、所管する情報システムにおける情報セキュリティに関する権限及び責任を有する。
- ⑥情報セキュリティ管理者は、所管する情報システムに係る情報セキュリティ実施手順の維持・管理を行う。

(5) 情報セキュリティ担当者

- ①情報セキュリティ管理者が指名した情報システムの運用管理を担当する職員を情報セキュリティ担当者とする。
- ②情報セキュリティ担当者は、情報セキュリティ管理者の指示等に従い、担当する情報システムの開発、設定の変更、運用、更新等の作業を行う。
- ③情報セキュリティ担当者は、情報セキュリティ管理者の指示等に従い、委託事業者等の管理・監督を行う。

(6) CSIRT

- ①CISO により、情報セキュリティの統一的な窓口として **CSIRT** を組織し、情報セキュリティインシデントについて所属長等から報告を受けた場合には、その状況を確認し、対応を図る体制として整備する。
- ②**CSIRT** は、CISO による情報セキュリティに関する意思決定が行われた際には、その内容を関係部局等に周知する。
- ③**CSIRT** は、情報セキュリティインシデントを認知した場合には、その重要度や影

響範囲等を勘案し、必要に応じて速やかに報道機関への通知・公表対応を行う。また、CISO、総務省、滋賀県等へ報告する。

- ④CSIRT は、情報セキュリティに関して、関係機関や他の地方公共団体の情報セキュリティに関する統一的な窓口の機能を有する部署、外部の事業者等との情報共有を行う。

(7) 情報セキュリティ委員会

- ①情報セキュリティ委員会の構成員は、CISO、統括情報セキュリティ責任者並びに情報セキュリティ責任者とする。
- ②CISO を委員長、統括情報セキュリティ責任者を副委員長とし、事務局は情報政策担当課に置く。
- ③本市の情報セキュリティ対策を統一的に実施するため、情報セキュリティポリシーの改定等、情報セキュリティに関する重要な事項については、情報セキュリティ委員会で審議するものとする。

3. 情報資産の分類と管理

(1) 情報資産の分類

本市における情報資産は、機密性、完全性及び可用性により、次のとおり分類し、必要に応じ取扱制限を行うものとする。

①機密性による情報資産の分類

分類	分類基準	取扱制限
自治体 機密性 3A	行政事務で取り扱う情報資産のうち、「行政文書の管理に関するガイドライン」(平成23年4月1日内閣総理大臣決定)に定める秘密文書に相当する文書	・本市管理以外の端末等での作業の禁止(自治体機密性3の情報資産に対して) ・必要以上の複製及び配付禁止 ・保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持ち込み禁止
自治体 機密性 3B	行政事務で取り扱う情報資産のうち、漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きく、事務又は業務の規模や性質上、取扱いに非常に留意すべき情報資産	・情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄
自治体 機密性 3C	行政事務で取り扱う情報資産のうち、自治体機密性3B以上に相当する機密性は要しないが、基本的に公表することを前提としていないもので、業務の規模や性質上、取扱いに留意すべき情報資産	・信頼のできるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
自治体 機密性 2	行政事務で取り扱う情報資産のうち、自治体機密性3に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産	
自治体 機密性 1	自治体機密性2又は自治体機密性3の情報資産以外の情報資産	—

②完全性による情報資産の分類

分類	分類基準	取扱制限
自治体 完全性 2	行政事務で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、住民の権利が侵害される又は行政事務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・バックアップ、電子署名付与 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
自治体 完全性 1	自治体完全性2 情報資産以外の情報資産	—

③可用性による情報資産の分類

分類	分類基準	取扱制限
自治体 可用性 2	行政事務で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、住民の権利が侵害される又は行政事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・バックアップ、指定する時間以内の復旧 ・電磁的記録媒体の施錠可能な場所への保管
自治体 可用性 1	自治体可用性2 の情報資産以外の情報資産	—

(2) 情報資産の管理

①管理責任

(ア) 情報セキュリティ管理者は、その所管する情報資産について管理責任を有する。

(イ) 情報セキュリティ管理者は、所管する情報システムに対して、当該情報システムのセキュリティ要件に係る事項について、情報システム台帳を整備しなければならない。

(ウ) 情報資産が複製又は伝送された場合には、複製等された情報資産も（１）の分類に基づき管理しなければならない。

②情報資産の分類の表示

職員等は、情報資産について、必要に応じて取扱制限についても明示する等適正な管理を行わなければならない。

③情報の作成

- (ア) 職員等は、業務上必要のない情報を作成してはならない。
- (イ) 情報を作成する者は、情報の作成時に（１）の分類に基づき、当該情報の分類と取扱制限を定めなければならない。
- (ウ) 情報を作成する者は、作成途上の情報についても、紛失や流出等を防止しなければならない。また、情報の作成途上で不要になった場合は、当該情報を消去しなければならない。

④情報資産の入手

- (ア) 庁内の者が作成した情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。
- (イ) 庁外の者が作成した情報資産を入手した者は、（１）の分類に基づき、当該情報の分類と取扱制限を定めなければならない。
- (ウ) 情報資産を入手した者は、入手した情報資産の分類が不明な場合、情報セキュリティ管理者に判断を仰がなければならない。

⑤情報資産の利用

- (ア) 情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。
- (イ) 情報資産を利用する者は、情報資産の分類に応じ、適正な取扱いをしなければならない。
- (ウ) 情報資産を利用する者は、電磁的記録媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該電磁的記録媒体を取り扱わなければならない。

⑥情報資産の保管

- (ア) 情報セキュリティ管理者は、情報資産の分類に従って、情報資産を適正に保管しなければならない。
- (イ) 情報セキュリティ管理者は、情報資産を記録した電磁的記録媒体を長期保管する場合は、書込禁止の措置を講じなければならない。
- (ウ) 情報セキュリティ管理者は、利用頻度が低い電磁的記録媒体や情報システムのバックアップで取得したデータを記録する電磁的記録媒体を長期保管する場合は、自然災害を被る可能性が低い地域に保管するよう努めなければならない。
- (エ) 情報セキュリティ管理者は、自治体機密性２以上、自治体完全性２又は自治体可用性２の情報を記録した電磁的記録媒体を保管する場合、耐火、耐熱、耐水及び耐湿を講じた施設可能な場所に保管しなければならない。

⑦情報の送信

電子メール等により自治体機密性２以上の情報を送信する場合は、情報セキュリティ管理者に許可を得た上で、パスワード等による暗号化を行わなければならない。

⑧情報資産の運搬

(ア) 車両等により自治体機密性 2 以上の情報資産を運搬する者は、鍵付きのケース等に格納し、暗号化又はパスワードの設定を行う等、情報資産の不正利用を防止するための措置を講じなければならない。

(イ) 自治体機密性 2 以上の情報資産を運搬する場合は、情報セキュリティ管理者に許可を得なければならない。

⑨情報資産の提供・公表

(ア) 自治体機密性 2 以上の情報資産を外部に提供する者は、暗号化又はパスワードの設定を行わなければならない。

(イ) 自治体機密性 2 以上の情報資産を外部に提供する者は、情報セキュリティ管理者に許可を得なければならない。

(ウ) 情報セキュリティ管理者は、住民に公開する情報資産について、完全性を確保しなければならない。

⑩情報資産の廃棄

(ア) 情報資産の廃棄やリース返却等を行う者は、情報を記録している電磁的記録媒体について、その情報の機密性に応じ、情報を復元できないように処置しなければならない。

(イ) 情報資産の廃棄を行う者は、行った処理について、日時、担当者及び処理内容を記録しなければならない。

(ウ) 情報資産の廃棄を行う者は、情報セキュリティ管理者の許可を得なければならない。

4. 情報システム全体の強靱性の向上

(1) 個人番号利用事務系

①個人番号利用事務系と他の領域との分離

個人番号利用事務系と他の領域を通信できないようにしなければならない。個人番号利用事務系と外部との通信をする必要がある場合は、通信経路の限定(MAC アドレス、IP アドレス)及びアプリケーションプロトコル (ポート番号) のレベルでの限定を行わなければならない。また、その外部接続先についてもインターネット等と接続してはならない。ただし、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先については、この限りではなく、LGWAN を経由して、インターネット等と個人番号利用事務系との双方向通信でのデータの移送を可能とする。

②情報のアクセス及び持ち出しにおける対策

(ア) 情報のアクセス対策

情報システムが正規の利用者かどうかを判断する認証手段のうち、二つ以上を併用する認証 (多要素認証) を利用しなければならない。

(イ) 情報の持ち出し不可設定

原則として、USB メモリ等の電磁的記録媒体による端末からの情報持ち出しができないように設定しなければならない。

(2) LGWAN 接続系

①LGWAN 接続系とインターネット接続系の分割

LGWAN 接続系とインターネット接続系は両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにしなければならない。なお、メールやデータを LGWAN 接続系に取り込む場合は、次の実現方法等により、無害化通信を図らなければならない。

(ア) インターネット環境で受信したインターネットメールの本文のみを LGWAN 接続系に転送する方式

(イ) インターネット接続系の端末から、LGWAN 接続系の端末へ画面を転送する方式

(ウ) 危険因子をファイルから除去し、又は危険因子がファイルに含まれていないことを確認し、インターネット接続系から取り込む方式

②情報の持ち出しにおける対策

(ア) 情報の持ち出し不可設定

原則として、USB メモリ等の電磁的記録媒体による端末からの情報持ち出しができないように設定しなければならない。

(3) インターネット接続系

- ①インターネット接続系においては、通信パケットの監視、ふるまい検知等の不正通信の監視機能の強化により、情報セキュリティインシデントの早期発見と対処及び LGWAN への不適切なアクセス等の監視等の情報セキュリティ対策を講じなければならない。
- ②インターネット接続口を集約する滋賀県自治体情報セキュリティクラウドに参加するとともに、関係省庁や滋賀県等と連携しながら、情報セキュリティ対策を推進しなければならない。
- ③小・中学校において、児童、生徒及び教職員が利用するインターネット接続環境については、滋賀県自治体情報セキュリティクラウドへの接続はできないが、同等レベルの情報セキュリティ対策を講じるよう努めなければならない。

5. 物理的セキュリティ

5. 1. サーバ等の管理

(1) 機器の取り付け

情報セキュリティ管理者は、サーバ等の機器の取付けを行う場合、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適正に固定する等、必要な措置を講じなければならない。

(2) サーバの冗長化

情報セキュリティ管理者は、所管するサーバに格納している情報の重要性や停止することによる影響度等を勘案し、必要に応じて当該サーバを冗長化し、サービスや業務の停止時間を最小限にするよう努めなければならない。

(3) 機器の電源

①情報セキュリティ管理者は、統括情報セキュリティ責任者及び施設管理部門と連携し、サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適正に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

②情報セキュリティ管理者は、統括情報セキュリティ責任者及び施設管理部門と連携し、落雷等による過電流に対して、サーバ等の機器を保護するための措置を講じなければならない。

(4) 通信ケーブル等の配線

①統括情報セキュリティ責任者及び情報セキュリティ管理者は、施設管理部門と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等必要な措置を講じなければならない。

②統括情報セキュリティ責任者及び情報セキュリティ管理者は、主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理部門から損傷等の報告があった場合、連携して対応しなければならない。

③統括情報セキュリティ責任者及び情報セキュリティ管理者は、ネットワーク接続口を他者が容易に接続できない場所に設置する等適正に管理しなければならない。

④統括情報セキュリティ責任者、情報セキュリティ管理者は、自ら又は情報セキュリティ担当者及び契約により操作を認められた委託事業者以外の者が配線を変更、追加できないように必要な措置を講じなければならない。

(5) 機器の定期保守及び修理

①情報セキュリティ管理者は、所管するサーバ等の機器の定期保守を必要に応じて実施しなければならない。

②情報セキュリティ管理者は、電磁的記録媒体を内蔵する機器を外部の事業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できな

い場合、情報セキュリティ管理者は、外部の事業者に故障を修理させるにあたり、修理を委託する事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認等を行わなければならない。

(6) 庁外への機器の設置

統括情報セキュリティ責任者及び情報セキュリティ管理者は、庁外にサーバ等の機器を設置する場合、CISO の承認を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況を確認しなければならない。

(7) 機器の廃棄等

情報セキュリティ管理者は、機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

5. 2. 管理区域の管理

(1) 管理区域の構造等

- ①管理区域とは、ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理並びに運用を行うための部屋（以下「電算室」という。）や電磁的記録媒体の保管庫をいう。
- ②統括情報セキュリティ責任者及び情報セキュリティ管理者は、施設管理部門と連携して、管理区域から外部に通ずるドアは必要最小限とし、鍵、監視カメラ、警報装置等によって許可されていない立入りを防止しなければならない。
- ③統括情報セキュリティ責任者及び情報セキュリティ管理者は、電算室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。
- ④統括情報セキュリティ責任者及び情報セキュリティ管理者は、施設管理部門と連携して、管理区域を囲む外壁等の床下開口部を全て塞がなければならない。
- ⑤統括情報セキュリティ責任者及び情報セキュリティ管理者は、管理区域に配置する消火薬剤や消防用設備等が、機器等及び電磁的記録媒体に影響を与えないようにしなければならない。

(2) 管理区域の入退室管理等

- ①情報セキュリティ管理者は、管理区域への入退室を許可された者のみに制限し、ICカード、静脈認証等の生体認証や入退室管理簿の記載による入退室管理を行わなければならない。
- ②職員等及び委託事業者は、管理区域に入室する場合、身分証明書等を携帯し、いつでも提示できる状態としなければならない。
- ③情報セキュリティ管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限した上で、管理区域への入退室を許可された職員等が

付き添うものとし、外見上職員等と区別できる措置を講じなければならない。

- ④情報セキュリティ管理者は、自治体機密性 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において、職員や委託事業者による個人所有等当該情報システムに関連のないコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等の使用禁止を徹底させなければならない。

(3) 機器等の搬入出

- ①情報セキュリティ管理者は、搬入する機器等が、既存の情報システムに与える影響について、あらかじめ職員又は委託した業者に確認を行わせなければならない。
- ②情報セキュリティ管理者は、電算室の機器等の搬入出について、委託事業者だけで行うのではなく、必ず職員を立ち合わせなければならない。

5. 3. 通信回線及び通信回線装置の管理

- ①統括情報セキュリティ責任者は、庁内の通信回線及び通信回線装置を、施設管理部門と連携し、適正に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適正に保管しなければならない。
- ②統括情報セキュリティ責任者は、情報システムのセキュリティ要件として策定した情報システムのネットワーク構成に関する要件内容に従い、通信回線装置に対して適切なセキュリティ対策を実施しなければならない。
- ③統括情報セキュリティ責任者は、外部へのネットワーク接続を必要最低限に限定しなければならない。
- ④統括情報セキュリティ責任者は、行政系のネットワークを総合行政ネットワーク（LGWAN）に集約するように努めなければならない。
- ⑤統括情報セキュリティ責任者は、自治体機密性 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、必要なセキュリティ水準を検討の上、適正な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。
- ⑥統括情報セキュリティ責任者は、ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施しなければならない。
- ⑦統括情報セキュリティ責任者は、自治体可用性 2 の情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。また、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。

5. 4. 職員等の利用する端末や電磁的記録媒体等の管理

- ①情報セキュリティ管理者は、盗難防止のため、執務室等で利用するパソコンのワイ

ヤーによる固定、モバイル端末及び電磁的記録媒体の使用時以外の施錠管理等の物理的措置を講じなければならない。電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

- ②情報セキュリティ管理者は、情報システムへのログインに際し、パスワード、ICカード及び生体認証等複数の認証情報の入力が必要とするように設定しなければならない。
- ③情報セキュリティ管理者は、個人番号利用事務系では「知識」、「所持」、「存在」を利用する認証手段のうち二つ以上を併用する認証（多要素認証等）を行うよう設定しなければならない。
- ④情報セキュリティ管理者は、電磁的記録媒体についてデータ暗号化機能を備える媒体を使用しなければならない。
- ⑤情報システム管理者は、パソコンやモバイル端末等におけるデータの暗号化等の機能を有効に利用しなければならない。端末にセキュリティチップが搭載されている場合、その機能を有効に活用しなければならない。同様に、電磁的記録媒体についてもデータ暗号化機能を備える媒体を使用しなければならない。

6. 人的セキュリティ

6. 1. 職員等の遵守事項

(1) 職員等の遵守事項

①情報セキュリティポリシー等の遵守

職員等は、情報セキュリティポリシー及び実施手順を遵守しなければならない。
また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに情報セキュリティ管理者に相談し、指示を仰がなければならない。

②業務以外の目的での使用の禁止

職員等は、業務以外の目的で情報資産の外部への持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

③情報資産の持ち出し及び外部における情報処理作業の制限

(ア) CISO は、自治体機密性 2 以上、自治体可用性 2、自治体完全性 2 の情報資産を外部で処理する場合における安全管理措置を定めなければならない。

(イ) 職員等は、情報資産（端末、電磁的記録媒体、データ及びソフトウェア等）を外部に持ち出す場合には、情報セキュリティ管理者の許可を得なければならない。

(ウ) 職員等は、外部で情報処理業務を行う場合には、情報セキュリティ管理者の許可を得なければならない。

④本市管理以外のパソコン等端末及び電磁的記録媒体等の業務利用

(ア) 職員等は、本市管理以外のパソコン等端末及び電磁的記録媒体等を原則業務に利用してはならない。ただし、本市管理以外のパソコン等端末の業務利用の可否判断を CISO が行った後に、情報セキュリティ管理者の許可を得て利用することができる。

(イ) 職員等は、本市管理以外のパソコン等端末及び電磁的記録媒体等を用いる場合には、情報セキュリティ管理者の許可を得た上で、外部で情報処理作業を行う際に安全管理措置に関する規定を遵守しなければならない。

⑤持ち出し及び持ち込みの記録

情報セキュリティ管理者は、端末等の持ち出し及び持ち込みについて、記録を作成し、保管しなければならない。

⑥パソコン等端末におけるセキュリティ設定変更の禁止

職員等は、パソコンやモバイル端末のソフトウェアに関するセキュリティ機能の設定を情報セキュリティ管理者の許可なく変更してはならない。

⑦机上の端末等の管理

職員等は、パソコン等端末、電磁的記録媒体及び情報が印刷された文書等につい

て、第三者に使用されること又は情報セキュリティ管理者の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、適正な措置を講じなければならない。

⑧異動・退職時等の遵守事項

職員等は、異動、退職等により業務を離れる場合には、作成・利用していた情報資産を、情報セキュリティ管理者が指示する場所に返却しなければならない。また、情報セキュリティ管理者の許可なく、異動・退職後は閲覧・利用できる状態にしてはならない。

⑨守秘義務の徹底

職員等は、職務上知り得た情報を漏らしてはならない。異動、退職、その他の事由により職務を離れた後においても同様とする。

(2) 非常勤及び会計年度任用職員への対応

①情報セキュリティポリシー等の遵守

情報セキュリティ管理者は、非常勤及び会計年度任用職員に対し、採用時に情報セキュリティポリシー等のうち、非常勤及び会計年度任用職員が守るべき内容を理解させ、また実施及び遵守させなければならない。

②情報セキュリティポリシー等の遵守に対する同意

情報セキュリティ管理者は、非常勤及び会計年度任用職員の採用の際、必要に応じ、情報セキュリティポリシー等を遵守する旨の同意書への署名を求めるものとする。

③インターネット接続及び電子メール使用等の制限

情報セキュリティ管理者は、非常勤及び会計年度任用職員にパソコン等端末による作業を行わせる場合において、当該職員の業務遂行に当たりインターネットへの接続及び電子メールの使用等が必要不可欠であり、かつ正規職員が行うなど代替手段がない場合を除き、これを利用できないようにしなければならない。

(3) 委託事業者に対する説明

情報セキュリティ管理者は、ネットワーク及び情報システムの開発・保守等を委託事業者が発注する場合、外部委託事業者から再委託を受ける事業者も含めて、情報セキュリティポリシー等のうち外部委託事業者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。

(4) 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は、職員等が常に情報セキュリティポリシー及び実施手順を閲覧できるように掲示しなければならない。

6. 2. 研修・訓練

(1) 情報セキュリティに関する研修・訓練

CISO は、定期的に情報セキュリティに関する研修・訓練を実施しなければならない。

(2) 研修計画の策定及び実施

①CISO は、幹部を含め全ての職員等に対する情報セキュリティに関する研修計画の策定とその実施体制の構築を定期的に行わなければならない。

②新規採用の職員等を対象とする情報セキュリティに関する研修を必ず実施しなければならない。

③研修は、情報セキュリティ責任者、情報セキュリティ管理者及びその他職員等に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものに行なければならない。

④情報セキュリティ管理者は、所管する課室等の研修の実施状況を記録し、統括情報セキュリティ責任者及び情報セキュリティ責任者に対して、報告しなければならない。

⑤CISO は、必要に応じ、情報セキュリティ委員会に対して、職員等の情報セキュリティ研修の実施状況について報告するものとする。

(3) 緊急時対応訓練

CISO は、緊急時対応を想定した訓練を定期的に行実施しなければならない。訓練計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の体制、範囲等を定め、また、効果的に実施できるようにしなければならない。

(4) 研修・訓練への参加

幹部を含めた職員等は、定められた研修・訓練に参加しなければならない。

6. 3. 情報セキュリティインシデントの報告

(1) 庁内での情報セキュリティインシデントの報告

①職員等は、情報セキュリティインシデントを認知した場合、速やかに情報セキュリティ管理者及び CSIRT に報告しなければならない。

②報告を受けた情報セキュリティ管理者は、速やかに情報セキュリティ責任者に報告しなければならない。

③情報セキュリティ責任者は、報告のあった情報セキュリティインシデントについて、必要に応じて市長及び CISO に報告しなければならない。

④情報セキュリティインシデントにより、個人情報・特定個人情報の漏えい等が発生した場合、必要に応じて個人情報保護委員会へ報告しなければならない。

(2) 住民等外部からの情報セキュリティインシデントの報告

①職員等は、本市が管理するネットワーク及び情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けた場合、速やかに情報セキュリティ管理者及び CSIRT に報告しなければならない。

- ②報告を受けた情報セキュリティ管理者は、速やかに情報セキュリティ責任者に報告しなければならない。
 - ③情報セキュリティ責任者は、報告のあった情報セキュリティインシデントについて、必要に応じて市長及び CISO に報告しなければならない。
 - ④CISO は、情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けるための窓口を設置し、当該窓口への連絡手段を公表しなければならない。
- (3) 情報セキュリティインシデント原因の究明・記録、再発防止等
- ①CSIRT は、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行わなければならない。
 - ②CSIRT は、情報セキュリティインシデントであると評価した場合、CISO に速やかに報告しなければならない。
 - ③CSIRT は、情報セキュリティインシデントに関係する情報セキュリティ責任者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示を行わなければならない。また、CSIRT は、同様の情報セキュリティインシデントが別の情報システムにおいても発生している可能性を検討し、必要に応じて当該情報システムを所管する情報システム管理者へ確認を指示しなければならない。
 - ④CSIRT は、これらの情報セキュリティインシデント原因を究明し、記録を保存しなければならない。また、情報セキュリティインシデントの原因究明の結果から、再発防止策を検討し、CISO に報告しなければならない。
 - ⑤CISO は、CSIRT から、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は、その内容を確認し、再発防止策を実施するために必要な措置を指示しなければならない。

6. 4. ID 及びパスワード等の管理

(1) ID の取扱い

職員等は、自己の管理する ID に関し、次の事項を遵守しなければならない。

- ①自己が利用している ID は、他人に利用させてはならない。
- ②共用 ID を利用する場合は、共用 ID の利用者以外に利用させてはならない。

(2) パスワードの取扱い

職員等は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。

- ①パスワードは、他者に知られないように管理しなければならない。
- ②パスワードを秘密にし、パスワードの照会等には一切応じてはならない。
- ③パスワードは十分な長さとし、文字列は想像しにくいものにしなければならない。
- ④パスワードが流出したおそれがある場合には、情報セキュリティ管理者に速やかに報告し、パスワードを速やかに変更しなければならない。

- ⑤複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いてはならない。
- ⑥仮のパスワード（初期パスワード含む）は、最初のログイン時点を変更しなければならない。
- ⑦パソコン等端末にパスワードを記憶させてはならない。
- ⑧職員等間でパスワードを共有してはならない（ただし共有 ID に対するパスワードは除く）。

7. 技術的セキュリティ

7. 1. コンピュータ及びネットワークの管理

(1) ファイルサーバの設定等

- ①情報セキュリティ管理者は、職員等が使用できる文書サーバの容量を設定し、職員等に周知しなければならない。
- ②情報セキュリティ管理者は、ファイルサーバを課室等の単位で構成し、職員等が他課室等のフォルダ及びファイルを閲覧及び使用できないように、設定しなければならない。
- ③情報セキュリティ管理者は、住民の個人情報や人事記録等の特定の職員等しか取り扱えないデータについては、必要に応じて別途ディレクトリを作成する等の措置を講じ、同一課室等であっても、担当以外の職員等が閲覧及び使用できないようにしなければならない。
- ④職員等は、業務上必要となる場合があるデータを情報セキュリティ管理者の許可なく削除してはならない。
- ⑤職員等は、保存の必要がなくなったデータについては、情報セキュリティ管理者の許可を得て削除しなければならない。

(2) バックアップの実施

- ①情報セキュリティ管理者は、ファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、必要に応じて定期的にバックアップを実施しなければならない。
- ②統括情報セキュリティ責任者及び情報セキュリティ管理者は、重要な情報を取り扱うサーバ装置については、適切な方法でサーバ装置のバックアップを取得しなければならない。
- ③統括情報セキュリティ責任者及び情報セキュリティ管理者は、重要な情報を取り扱う情報システムを構成する通信回線装置については、運用状態を復元するために必要な設定情報等のバックアップを取得し保管しなければならない。

(3) 他団体との情報システムに関する情報等の交換

情報セキュリティ管理者は、他の団体と情報システムに関する情報及びソフトウェアを交換する場合、その取扱いに関する事項をあらかじめ定め、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なければならない。

(4) システム変更記録及び作業の確認

- ①情報セキュリティ管理者は、所管する情報システムにおいて、変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適正に管理し、運用・保守によって機器の構成や設定情報等に変更があった場合は、情報セキュリティ対策が適切であるか確認し、必要に応じて見直さなければならない。

い。

- ②情報セキュリティ管理者は、情報セキュリティ担当者及び契約により操作を認められた委託事業者がシステム変更等の作業を行う場合は、作業実施者以外の者により作業内容に誤りがないか確認させなければならない。

(5) 情報システム仕様書等の管理

統括情報セキュリティ責任者及び情報セキュリティ管理者は、ネットワーク構成図、情報システム仕様書について、記録媒体に関わらず、業務上必要とする者以外の者が閲覧できないようにしなければならない。また、紛失等がないように適正に管理しなければならない。

(6) ログの取得等

- ①情報セキュリティ管理者は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。
- ②情報セキュリティ管理者は、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、適正にログを管理しなければならない。
- ③情報セキュリティ管理者は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。

(7) 障害記録

情報セキュリティ管理者は、職員等からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適正に保存しなければならない。

(8) ネットワークの接続制御、経路制御等

- ①統括情報セキュリティ責任者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。
- ②統括情報セキュリティ責任者は、不正アクセスを防止するため、ネットワークに適正なアクセス制御を施さなければならない。
- ③統括情報セキュリティ責任者は、保守又は診断のために、外部の通信回線から内部の通信回線に接続された機器等に対して行われるリモートメンテナンスに係る情報セキュリティを確保しなければならない。また、情報セキュリティ対策について、定期的な確認により見直さなければならない。

(9) 外部の者が利用できるシステムの分離等

統括情報セキュリティ責任者は、電子申請の汎用受付システム等、外部の者が利用できるシステムについて、必要に応じ他のネットワーク及び情報システムと物理的に分離する等の措置を講じなければならない。

(10) 外部ネットワークとの接続制限等

- ①情報セキュリティ管理者は、所管するネットワークを外部ネットワークと接続しようとする場合には、CISO 及び統括情報セキュリティ責任者の許可を得なければならない。
 - ②情報セキュリティ管理者は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、庁内の全てのネットワーク、情報システム等の情報資産に影響が生じないことを確認しなければならない。
 - ③情報セキュリティ管理者は、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保しなければならない。
 - ④統括情報セキュリティ責任者及び情報セキュリティ管理者は、ウェブサーバ等をインターネットに公開する場合、次のセキュリティ対策を実施しなければならない。
 - (ア) 庁内ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。
 - (イ) 脆弱性が存在する可能性が増大することを防止するため、ウェブサーバが備える機能のうち、必要な機能のみを利用しなければならない。
 - (ウ) ウェブサーバからの不用意な情報漏えいを防止するための措置を講じなければならない。
 - (エ) 情報システム管理者は、ウェブコンテンツの編集作業を行う主体を限定しなければならない。
 - (オ) インターネットを介して転送される情報の盗聴及び改ざんの防止のため、全ての情報に対する暗号化及び電子証明書による認証の対策を講じなければならない。
 - ⑤情報セキュリティ管理者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、統括情報セキュリティ責任者の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。
- (11) 複合機のセキュリティ管理
- ①統括情報セキュリティ責任者は、複合機を調達する場合、当該複合機が備える機能、設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適正なセキュリティ要件を策定しなければならない。
 - ②統括情報セキュリティ責任者は、複合機が備える機能について適正な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。

③統括情報セキュリティ責任者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消又は再利用できないようにする対策を講じなければならない。

(12) IoT 機器を含む特定用途機器のセキュリティ管理

情報セキュリティ管理者は、所管する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、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を講じなければならない。

(13) 無線 LAN 及びネットワークの盗聴対策

①統括情報セキュリティ責任者は、無線 LAN の利用を認める場合、解読が困難な暗号化及び認証技術の使用を義務付けなければならない。

②統括情報セキュリティ責任者は、機密性の高い情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。

(14) 電子メールのセキュリティ管理

①統括情報セキュリティ責任者は、権限のない利用者により、外部から外部への電子メール転送（電子メールの中継処理）が行われることを不可能とするよう、電子メールサーバの設定を行わなければならない。

②統括情報セキュリティ責任者は、大量のスパムメール等の受信又は送信を検知した場合は、メールサーバの運用を停止しなければならない。

③統括情報セキュリティ責任者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にしなければならない。

④統括情報セキュリティ責任者は、職員等が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を職員等に周知しなければならない。

⑤統括情報セキュリティ責任者は、システム開発や運用、保守等のため庁舎内に常駐している委託事業者の作業員による電子メールアドレスを利用させる場合は、委託事業者との間で利用方法を取り決めなければならない。

(15) 電子メールの利用制限

①職員等は、自動転送機能を用いて、電子メールを転送してはならない。

②職員等は、業務上必要のない送信先に電子メールを送信してはならない。

③職員等は、複数人に電子メールを送信する場合、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにしなければならない。

④職員等は、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しなければならない。

⑤職員等は、市で管理していないフリー等の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を使用してはならない。ただし、業務上必要な場合は、情報セキュリティ管理者の許可を得て利用することができる。

(16) 電子署名・暗号化

- ①職員等は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性又は完全性を確保することが必要な場合には、CISO が定めた電子署名、暗号化又はパスワード設定等、セキュリティを考慮して、送信しなければならない。
- ②職員等は、暗号化を行う場合に CISO が定める以外の方法を用いてはならない。また、CISO が定めた方法で暗号のための鍵を管理しなければならない。
- ③CISO は、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全に提供しなければならない。

(17) 無許可ソフトウェアの導入等の禁止

- ①職員等は、パソコン等端末に無断でソフトウェアを導入してはならない。
- ②職員等は、業務上の必要がある場合は、統括情報セキュリティ責任者の許可を得て、ソフトウェアを導入することができる。
- ③職員等は、不正にコピーしたソフトウェアを利用してはならない。
- ④情報セキュリティ管理者は、所管する課室等で利用するソフトウェアについて、不正にコピーや入手したものでないこと及び保有するライセンス数を超過して利用することを防止するため、ライセンスを管理しなければならない。

(18) 機器構成の変更の制限

- ①職員等は、パソコン等端末に対し機器の改造及び増設・交換を行ってはならない。
- ②職員等は、業務上、パソコン等端末に対し機器の改造及び増設・交換を行う必要がある場合には、統括情報セキュリティ責任者及び情報セキュリティ管理者の許可を得なければならない。

(19) 無許可でのネットワーク接続の禁止

- ①職員等は、本市管理のパソコン等端末を、有線・無線を問わず、その端末を接続して利用するよう、情報セキュリティ管理者によって定められたネットワークと異なるネットワークに接続してはならない。
- ②情報セキュリティ管理者は、必要に応じて、本市管理のパソコン等端末について、端末に搭載された OS のポリシー設定等により、端末を異なるネットワークに接続できないよう技術的に制限しなければならない。

(20) 業務以外の目的でのウェブ閲覧の禁止

- ①職員等は、業務以外の目的でウェブを閲覧してはならない。
- ②統括情報セキュリティ責任者は、職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、情報セキュリティ管理者に通知し適正な措置を求めなければならない。

7. 2. アクセス制御等

(1) アクセス制御等

①アクセス制御

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は、所管するネットワーク又は情報システムごとにアクセスする権限のない職員等がアクセスできないように、システム上制限しなければならない。

②利用者 ID の取扱い

- (ア) 統括情報セキュリティ責任者及び情報セキュリティ管理者は、利用者の登録、変更、抹消等の情報管理、職員等の異動、出向、退職者に伴う利用者 ID の取扱い等の方法を定めなければならない。
- (イ) 職員等は、業務上必要がなくなった場合は、利用者登録を抹消するよう、統括情報セキュリティ責任者又は情報セキュリティ管理者に通知しなければならない。
- (ウ) 統括情報セキュリティ責任者及び情報セキュリティ管理者は、利用されていない ID が放置されないよう、人事管理部門と連携し、点検しなければならない。
- (エ) 統括情報セキュリティ責任者及び情報セキュリティ管理者は、主体から対象に対する不要なアクセス権限が付与されていないか定期的に確認しなければならない。

③特権を付与された ID の管理等

- (ア) 統括情報セキュリティ責任者及び情報セキュリティ管理者は、管理者権限等の特権を付与された ID を利用する者を必要最小限にし、当該 ID のパスワードの漏えい等が発生しないよう、当該 ID 及びパスワードを厳重に管理しなければならない。
- (イ) 統括情報セキュリティ責任者及び情報セキュリティ管理者は、特権を付与された ID 及びパスワードの変更について、外部委託事業者に行わせてはならない。
- (ウ) 統括情報セキュリティ責任者及び情報セキュリティ管理者は、特権を付与された ID を初期設定以外のものに変更しなければならない。

(2) 職員等による外部からのアクセス等の制限

- ①職員等が外部から内部のネットワーク又は情報システムにアクセスする場合は、統括情報セキュリティ責任者及び当該情報システムを管理する情報セキュリティ管理者の許可を得なければならない。
- ②統括情報セキュリティ責任者は、内部のネットワーク又は情報システムに対する外部からのアクセスを、アクセスが必要な合理的理由を有する必要最小限の者に限定しなければならない。
- ③統括情報セキュリティ責任者は、外部からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保しなければならない。
- ④統括情報セキュリティ責任者は、外部からのアクセスを認める場合、通信途上の盗聴を防御するために暗号化等の措置を講じなければならない。
- ⑤統括情報セキュリティ責任者及び情報セキュリティ管理者は、外部からのアクセ

スに利用する端末を職員等に貸与する場合、セキュリティ確保のために必要な措置を講じなければならない。

- ⑥職員等は、持ち込んだ又は外部から持ち帰った端末を本市の管理するネットワークに接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認し、情報セキュリティ管理者の許可を得るか、もしくは情報セキュリティ管理者によって事前に定義されたポリシーに従って接続しなければならない。
- ⑦統括情報セキュリティ責任者は、内部のネットワーク又は情報システムに対するインターネットを介した外部からのアクセスを原則として禁止しなければならない。ただし、止むを得ず接続を許可する場合は、利用者の ID、パスワード及び生体認証に係る情報等の認証情報並びにこれを記録した媒体（IC カード等）による認証に加えて通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講じなければならない。

（３）認証情報の管理

- ①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は、職員等の認証情報を厳重に管理しなければならない。
- ②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は、職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、初回ログイン後直ちに仮のパスワードを変更させなければならない。
- ③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は、認証情報の不正利用を防止するための措置を講じなければならない。

（４）特権による接続時間の制限

情報セキュリティ管理者は、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を必要最小限にするよう努めなければならない。

7. 3. システム開発、導入、保守等

（１）機器等及び情報システムの調達

- ①統括情報セキュリティ責任者及び情報セキュリティ管理者は、情報システム開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。また、業務システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮した技術的なセキュリティ機能を調達仕様書に記載しなければならない。
- ②統括情報セキュリティ責任者及び情報セキュリティ管理者は、機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

（２）情報システムの開発

- ①システム開発における責任者及び作業者の特定

情報セキュリティ管理者は、システム開発の責任者及び作業者を特定しなければならない。

②システム開発における責任者、作業者の ID の管理

(ア) 情報セキュリティ管理者は、システム開発の責任者及び作業者が使用する ID を管理し、開発完了後、開発用 ID を削除しなければならない。

(イ) 情報セキュリティ管理者は、システム開発の責任者及び作業者のアクセス権限を設定しなければならない。

③システム開発に用いるハードウェア及びソフトウェアの管理

(ア) 情報セキュリティ管理者は、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を特定しなければならない。

(イ) 情報セキュリティ管理者は、利用を認めたソフトウェア以外は使用させてはならない。

④アプリケーション・コンテンツの開発時の対策

情報セキュリティ管理者は、ウェブアプリケーションの開発において、セキュリティ要件として定めた仕様に加えて、既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講じなければならない。

(3) 情報システムの導入

①開発環境と運用環境の分離及び移行手順の明確化

(ア) 情報セキュリティ管理者は、システム開発、保守及びテスト環境とシステム運用環境を分離しなければならない。

(イ) 情報セキュリティ管理者は、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・保守計画の策定時に手順を明確にしなければならない。

(ウ) 情報セキュリティ管理者は、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之、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

(エ) 情報セキュリティ管理者は、導入する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しなければならない。

②テスト

(ア) 情報セキュリティ管理者は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分な試験を行わなければならない。

(イ) 情報セキュリティ管理者は、運用テストを行う場合、あらかじめ擬似環境による操作確認を行わなければならない。

(ウ) 情報セキュリティ管理者は、個人情報及び機密性の高い情報を、テストデータに使用してはならない。

③機器等の納入時又は情報システムの受入れ時

- (ア) 情報セキュリティ管理者は、機器等の納入時又は情報システムの受入れ時の確認・検査において、調達仕様書等定められた検査手続に従い、情報セキュリティ対策に係る要件が満たされていることを確認しなければならない。
- (イ) 情報セキュリティ管理者は、情報システムが構築段階から運用保守段階へ移行する際に、当該情報システムの開発事業者から運用保守事業者へ引継がれる項目に、情報セキュリティ対策に必要な内容が含まれていることを確認しなければならない。
- (4) 情報システム基盤を管理又は制御するソフトウェア導入時の対策
- 利用するソフトウェアの特性を踏まえ、必要に応じて、以下の実施手順を整備しなければならない。
- (ア) 情報システムの基盤を管理又は制御するソフトウェアの情報セキュリティ水準の維持に関する手順
- (イ) 情報システムの基盤を管理又は制御するソフトウェアで発生した情報セキュリティインシデントを認知した際の対処手順
- (5) 情報システムの基盤を管理又は制御するソフトウェア運用時の対策
- 情報セキュリティ管理者は、利用を認めるソフトウェアについて、定期的な確認による見直しを行わなければならない。
- (6) システム開発・保守に関連する資料等の整備・保管
- ①情報セキュリティ管理者は、システム開発・保守に関連する資料及びシステム関連文書を適正に整備・保管しなければならない。
- (ア) 情報セキュリティ管理者は、情報システムを新規に構築し、又は更改する際には、情報システム台帳のセキュリティ要件に係る内容を記録又は記載し、当該内容について統括情報セキュリティ責任者に報告しなければならない。
- (イ) 情報セキュリティ管理者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、以下を全て含む情報システム関連文書を整備しなければならない。
- ・ 情報システムを構成するサーバ装置及び端末関連情報
 - ・ 情報システムを構成する通信回線及び通信回線装置関連情報
- (ウ) 情報セキュリティ管理者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、以下を全て含む実施手順を整備しなければならない。
- ・ 情報システム構成要素ごとの情報セキュリティ水準の維持に関する手順
 - ・ 情報セキュリティインシデントを認知した際の対処手順
 - ・ 情報システムが停止した際の復旧手順
- ②情報セキュリティ管理者は、テスト結果を一定期間保管しなければならない。
- ③情報セキュリティ管理者は、情報システムに係るソースコードを適正な方法で保

管しなければならない。

(7) 情報システムにおける入出力データの正確性の確保

①情報セキュリティ管理者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する機能を組み込むように情報システムを設計しなければならない。

②情報セキュリティ管理者は、ウェブアプリケーションやウェブコンテンツにおいて、次のセキュリティ対策を実施しなければならない。

(ア) 利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション及びウェブコンテンツの提供方式等を見直ししなければならない。

(イ) 運用中のアプリケーション・コンテンツにおいて、定期的に脆弱性対策の状況を確認し、脆弱性が発覚した際は必要な措置を講じなければならない。

(ウ) ウェブアプリケーションやウェブコンテンツにおいて、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。

③情報セキュリティ管理者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

(8) 情報システムの変更管理

情報セキュリティ管理者は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成しなければならない。

(9) 開発・保守用のソフトウェアの更新等

情報セキュリティ管理者は、開発・保守用のソフトウェア等を更新又はパッチの適用をする場合、他の情報システムとの整合性を確認しなければならない。

(10) システム更新又は統合時の検証等

情報セキュリティ管理者は、システム更新・統合時に伴うリスク管理体制の構築、移行基準の明確化及び更新・統合後の業務運営体制の検証を行わなければならない。

(11) 情報システムについての対策の見直し

情報セキュリティ管理者は、対策の推進計画等に基づき情報システムの情報セキュリティ対策を適切に見直さなければならない。また、本市内で横断的に改善が必要となる情報セキュリティ対策の見直しによる改善指示に基づき、情報セキュリティ対策を適切に見直さなければならない。なお、措置の結果については、統括情報セキュリティ責任者へ報告しなければならない。

7. 4. 不正プログラム対策

(1) 統括情報セキュリティ責任者及び情報セキュリティ管理者の措置事項

統括情報セキュリティ責任者及び情報セキュリティ管理者は、不正プログラム対

策として、次の事項を措置しなければならない。

- ①外部ネットワークから受信したファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムのシステムへの侵入を防止しなければならない。
- ②外部ネットワークに送信するファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止しなければならない。
- ③コンピュータウイルス等の不正プログラム情報を収集し、職員等に対して注意喚起しなければならない。
- ④所管するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。
- ⑤不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。
- ⑥不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。
- ⑦業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用してはならない。
- ⑧電磁的記録媒体を使う場合、コンピュータウイルス等の感染を防止するために、本市が管理している媒体以外を職員等に利用させてはならない。
- ⑨インターネットに接続していない情報システムにおいても、電磁的記録媒体等の接続ができない等の措置を講じ、コンピュータウイルス等の感染、侵入が生じる可能性がない場合を除き、不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を実施しなければならない。
- ⑩業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用してはならない。また、当該製品の利用を予定している期間中にパッチやバージョンアップなどの開発元のサポートが終了する予定がないことを確認しなければならない。

(2) 職員等の遵守事項

職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

- ①パソコン等端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。
- ②外部からデータ又はソフトウェアを取り入れる場合には、必ず不正プログラム対策ソフトウェアによるチェックを行わなければならない。
- ③差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除しなければならない。
- ④端末に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的の実施しなければならない。

⑤添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行わなければならない。インターネット接続系で受信したインターネットメール又はインターネット経由で入手したファイルを LGWAN 接続系に取込む場合は無害化しなければならない。

⑥統括情報セキュリティ責任者が提供するウイルス情報を、常に確認しなければならない。

⑦コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、以下の対応を行わなければならない。

有線接続：LAN ケーブルの即時取り外しを行う。

無線接続：直ちに利用を中止し、通信を行わない設定への変更を行う。

(3) 専門家の支援体制

統括情報セキュリティ責任者は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられるようにしておかなければならない。

7. 5. 不正アクセス対策

(1) 統括情報セキュリティ責任者及び情報セキュリティ管理者の措置事項

統括情報セキュリティ責任者及び情報セキュリティ管理者は、不正アクセス対策として、以下の事項を措置しなければならない。

①使用されていないポートを閉鎖しなければならない。

②不要なサービスについて、機能を削除又は停止しなければならない。

③不正アクセスによるウェブページの改ざんを防止するための対策を講じなければならない。

④CSIRT と連携し、監視、通知、外部連絡窓口及び適正な対応などを実施できる体制並びに連絡網を構築しなければならない。

(2) 攻撃への対処

CISO 及び統括情報セキュリティ責任者は、サーバ等に攻撃を受けた場合又は攻撃を受けるリスクがある場合は、システムの停止を含む必要な措置を講じなければならない。また、総務省、滋賀県等と連絡を密にして情報の収集に努めなければならない。

(3) 記録の保存

CISO 及び統括情報セキュリティ責任者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

(4) 内部からの攻撃

統括情報セキュリティ責任者及び情報セキュリティ管理者は、職員等及び委託事

業者が使用しているパソコン等端末からの庁内のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

(5) 職員等による不正アクセス

統括情報セキュリティ責任者は、職員等による不正アクセスを発見した場合は、当該職員等が所属する課室等の情報セキュリティ管理者に通知し、適正な処置を求めなければならない。

(6) サービス不能攻撃

統括情報セキュリティ責任者及び情報セキュリティ管理者は、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じなければならない。

(7) 標的型攻撃

統括情報セキュリティ責任者及び情報セキュリティ管理者は、情報システムにおいて、標的型攻撃による内部への侵入を防止するために、教育や自動再生無効化等の人的対策や入口対策を講じなければならない。また、内部に侵入した攻撃を早期検知して対処するために、通信をチェックする等の内部対策を講じなければならない。

7. 6. セキュリティ情報の収集

(1) セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等

統括情報セキュリティ責任者及び情報セキュリティ管理者は、セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

(2) 不正プログラム等のセキュリティ情報の収集・周知

統括情報セキュリティ責任者は、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、職員等に周知しなければならない。

(3) 情報セキュリティに関する情報の収集及び共有

統括情報セキュリティ責任者及び情報セキュリティ管理者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害を未然に防止するための対策を速やかに講じなければならない。

8. 運用

8. 1. 情報システムの監視

(1) 情報システムの運用・保守時の対策

- ①統括情報セキュリティ責任者及び情報セキュリティ管理者は、情報システムの運用・保守において、情報システムに実装された監視を含むセキュリティ機能を適切に運用しなければならない。
- ②統括情報セキュリティ責任者及び情報セキュリティ管理者は、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講じなければならない。
- ③統括情報セキュリティ責任者及び情報セキュリティ管理者は、重要な情報を取り扱う情報システムについて、危機的事象発生時に適切な対処が行えるよう運用をしなければならない。

(2) 情報システムの監視機能

- ①統括情報セキュリティ責任者及び情報セキュリティ管理者は、情報システム運用時の監視に係る運用管理機能要件を策定し、監視機能を実装しなければならない。
- ②統括情報セキュリティ責任者及び情報セキュリティ管理者は、情報システムの運用において、情報システムに実装された監視機能を適切に運用しなければならない。
- ③統括情報セキュリティ責任者及び情報セキュリティ管理者は、新たな脅威の出現、運用の状況等を踏まえ、情報システムにおける監視の対象や手法を定期的に見直さなければならない。
- ④統括情報セキュリティ責任者及び情報セキュリティ管理者は、サーバ装置上での情報セキュリティインシデントの発生を監視するため、当該サーバ装置を監視するための措置を講じなければならない。

(3) 情報システムの監視

- ①統括情報セキュリティ責任者及び情報セキュリティ管理者は、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。
- ②統括情報セキュリティ責任者及び情報セキュリティ管理者は、重要な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できる措置を講じなければならない。
- ③統括情報セキュリティ責任者及び情報セキュリティ管理者は、外部と常時接続するシステムを常時監視しなければならない。

8. 2. 情報セキュリティポリシーの遵守状況の確認

(1) 遵守状況の確認及び対処

- ①情報セキュリティ責任者及び情報セキュリティ管理者は、情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかに CISO 及び統括情報セキュリティ責任者に報告しなければならない。
 - ②CISO は、発生した問題について、適正かつ速やかに対処しなければならない。
 - ③統括情報セキュリティ責任者及び情報セキュリティ管理者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には適正かつ速やかに対処しなければならない。
- (2) パソコン等端末及び電磁的記録媒体等の利用状況調査
- CISO 及び統括情報セキュリティ責任者は、不正アクセス、不正プログラム等の調査のために、職員等が使用しているパソコン等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を調査することができる。
- (3) 職員等の報告義務
- ①職員等は、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、直ちに統括情報セキュリティ責任者及び情報セキュリティ管理者に報告を行わなければならない。
 - ②当該違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると統括情報セキュリティ責任者が判断した場合において、職員等は、緊急時対応計画に従って適正に対処しなければならない。

8. 3. 侵害時の対応等

(1) 緊急時対応計画の策定

CISO は、情報セキュリティインシデント、情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合又は発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適正に実施するために、緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適正に対処しなければならない。

(2) 緊急時対応計画に盛り込むべき内容

緊急時対応計画には、以下の内容を定めなければならない。

- ①関係者の連絡先
- ②発生した事案に係る報告すべき事項
- ③発生した事案への対応措置
- ④再発防止措置の策定

(3) 業務継続計画との整合性確保

自然災害、大規模・広範囲にわたる疾病等に備えて別途業務継続計画を策定し、当該計画と情報セキュリティポリシーの整合性を確保しなければならない。

(4) 緊急時対応計画の見直し

CISO は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて緊急時対応計画の規定を見直さなければならない。

8. 4. 例外措置

(1) 例外措置の許可

情報セキュリティ管理者は、情報セキュリティ関係規定を遵守することが困難な状況で、行政事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用し又は遵守事項を実施しないことについて合理的な理由がある場合には、事前に CISO の許可を得て、例外措置を講じることができる。

(2) 緊急時の例外措置

情報セキュリティ管理者は、行政事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかに CISO に報告しなければならない。

(3) 例外措置の申請書の管理

CISO は、例外措置の申請書及び審査結果を適正に保管しなければならない。

8. 5. 法令遵守

職員等は、職務の遂行において使用する情報資産を保護するために、次の法令のほか関係法令を遵守し、これに従わなければならない。

- ①地方公務員法（昭和 25 年法律第 261 号）
- ②著作権法（昭和 45 年法律第 48 号）
- ③不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）
- ④個人情報の保護に関する法律（平成 15 年法律第 57 号）
- ⑤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 25 年法律第 27 号）
- ⑥サイバーセキュリティ基本法（平成 28 年法律第 31 号）
- ⑦栗東市個人情報保護法施行条例（令和 5 年 3 月 23 日条例第 3 号）

8. 6. 違反時の対応

職員等の情報セキュリティポリシーに違反する行動を確認した場合には、速やかに次の措置を講じなければならない。

- ①統括情報セキュリティ責任者が違反を確認した場合は、統括情報セキュリティ責任者は当該職員等が所属する課室等の情報セキュリティ管理者に通知し、適正な措置を求めなければならない。
- ②情報セキュリティ責任者等が違反を確認した場合は、違反を確認した者は速やか

に統括情報セキュリティ責任者及び当該職員等が所属する課室等の情報セキュリティ管理者に通知し、適正な措置を求めなければならない。

- ③情報セキュリティ管理者の指導によっても改善されない場合、統括情報セキュリティ責任者は、当該職員等のネットワーク又は情報システムを使用する権利を停止あるいは剥奪することができる。その後速やかに、統括情報セキュリティ責任者は、職員等の権利を停止あるいは剥奪した旨を CISO 及び当該職員等が所属する課室等の情報セキュリティ管理者に通知しなければならない。

9. 業務委託と外部サービス（クラウドサービス）の利用

9. 1. 業務委託

（1）業務委託実施前の対策

①情報セキュリティ管理者は、業務委託の実施までに、以下を全て含む事項を実施しなければならない。

（ア）委託する業務内容の特定

（イ）委託事業者の選定条件を含む仕様の策定

（ウ）仕様に基づく委託事業者の選定

（エ）情報セキュリティ要件を明記した契約の締結（契約項目）

重要な情報資産を取扱う業務を委託する場合には、委託事業者との間で必要に応じて次の情報セキュリティ等に係る要件を明記した契約を締結しなければならない。

- ・ 情報セキュリティポリシー及び情報セキュリティ実施手順の遵守
- ・ 個人情報漏えい防止のための技術的安全管理措置に関する取り決め
- ・ 委託事業者の責任者、委託内容、作業者の所属、作業場所の特定
- ・ 提供されるサービスレベルの保証
- ・ 委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法の明確化など、情報のライフサイクル全般での管理方法
- ・ 委託事業者の従業員に対する教育の実施
- ・ 提供された情報の目的外利用及び委託事業者以外の者への提供の禁止
- ・ 業務上知り得た情報の守秘義務
- ・ 再委託に関する制限事項の遵守
- ・ 委託業務終了時の情報資産の返還、廃棄等
- ・ 委託業務の定期報告及び緊急時報告義務
- ・ 市による監査、検査
- ・ 市による情報セキュリティインシデント発生時の公表
- ・ 情報セキュリティポリシーが遵守されなかった場合の規定（損害賠償等）

（オ）委託事業者に重要情報を提供する場合は、秘密保持契約（NDA）の締結

②情報セキュリティ管理者は、業務委託の実施までに、委託の前提条件として、以下を全て含む事項の実施を委託事業者に求めなければならない。

（ア）仕様に準拠した提案

（イ）契約の締結

（ウ）委託事業者において重要情報を取り扱う場合は、秘密保持契約（NDA）の締結

（2）業務委託実施期間中の対策

- ①情報セキュリティ管理者は、業務委託の実施期間において、以下をすべて含む対策を実施しなければならない。
 - (ア) 委託判断基準に従った重要情報の提供
 - (イ) 契約に基づき委託事業者を実施させる情報セキュリティ対策の履行状況の定期的な確認及び措置の実施
 - (ウ) 委託した業務において、情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合又はその旨の報告を職員等より受けた場合における、委託事業の一時中断などの必要な措置を含む、契約に基づく対処の要求
- ②情報セキュリティ管理者は、業務委託の実施期間において、以下を全て含む対策の実施を委託事業者に求めなければならない。
 - (ア) 情報の適正な取扱いのための情報セキュリティ対策
 - (イ) 契約に基づき委託事業者が実施する情報セキュリティ対策の履行状況の定期的な報告
 - (ウ) 委託した業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合における、委託事業の一時中断などの必要な措置を含む対処
- (3) 業務委託終了時の対策
 - ①情報セキュリティ管理者は、業務委託の終了に際して、以下を全て含む対策を実施しなければならない。
 - (ア) 業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの確認を含む検収
 - (イ) 委託事業者に提供した情報を含め、委託事業者において取り扱われた情報が確実に返却、廃棄又は抹消されたことの確認
 - ②情報セキュリティ管理者は、業務委託の終了に際して、以下を全て含む対策の実施を委託事業者に求めなければならない。
 - (ア) 業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの報告を含む検収の受検
 - (イ) 提供を受けた情報を含め、委託業務において取り扱った情報の返却、廃棄又は抹消

9. 2. 情報システムに関する業務委託

(1) 情報システムに関する業務委託における共通対策

情報セキュリティ管理者は、情報システムに関する業務委託の実施までに、情報システムに本市の意図せざる変更が加えられないための対策に係る選定条件を委託事業者の選定条件に加え、仕様を策定しなければならない。

(2) 情報システムの構築を業務委託する場合の対策

情報セキュリティ管理者は、情報システムの構築を業務委託する場合は、契約に基づき、以下を全て含む対策の実施を委託事業者に求めなければならない。

- ①情報システムのセキュリティ要件の適切な実装
- ②情報セキュリティの観点に基づく試験の実施
- ③情報システムの開発環境及び開発工程における情報セキュリティ対策

(3) 情報システムの運用・保守を業務委託する場合の対策

- ①情報セキュリティ管理者は、情報システムの運用・保守を業務委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、契約に基づき、委託事業者の実施を求めなければならない。
- ②情報セキュリティ管理者は、情報システムの運用・保守を業務委託する場合は、委託事業者が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、契約に基づき、委託事業者速やかな報告を求めなければならない。

(4) 本市向けに情報システムの一部の機能を提供するサービスを利用する場合の対策

- ①情報セキュリティ管理者は、外部の一般の者が本市向けに重要情報を取り扱う情報システムの一部の機能を提供するサービス（クラウドサービスを除く。）（以下「業務委託サービス」という。）を利用するため、情報システムに関する業務委託を実施する場合は、委託事業者の選定条件に業務委託サービスに特有の選定条件を加えなければならない。
- ②情報セキュリティ管理者は、業務委託サービスに係るセキュリティ要件を定め、業務委託サービスを選定しなければならない。
- ③情報セキュリティ管理者は、委託事業者の信頼性が十分であることを総合的・客観的に評価し判断しなければならない。
- ④情報セキュリティ管理者は業務委託サービスを利用する場合には、統括情報セキュリティ責任者又は情報セキュリティ責任者へ当該サービスの利用申請を行わなければならない。
- ⑤統括情報セキュリティ責任者又は情報セキュリティ責任者は、業務委託サービスの利用申請を受けた場合は、当該利用申請を審査し、利用の可否を決定しなければならない。
- ⑥統括情報セキュリティ責任者又は情報セキュリティ責任者は、業務委託サービスの利用申請を承認した場合は、承認済み業務委託サービスとして記録し、業務委託サービス管理者を指名しなければならない。

9. 3. 外部サービス（クラウドサービス）の利用（自治体機密性2以上の情報を取り扱う場合）

(1) クラウドサービスの選定に係る運用規程の整備

統括情報セキュリティ責任者は、自治体機密性2以上の情報を取り扱う場合、以下を含む外部サービス（クラウドサービス、以下「クラウドサービス」という。）の選定に関する規定を整備しなくてはならない。

- ①クラウドサービスを利用可能な業務及び情報システムの範囲並びに情報の取扱いを許可する場所を判断する基準（以下、9.3節において「クラウドサービス利用判断基準」という。）
- ②クラウドサービス提供者の選定基準
- ③クラウドサービスの利用手続
- ④クラウドサービスの利用状況の管理

（2）クラウドサービスの利用に係る運用規程の整備

統括情報セキュリティ責任者は、自治体機密性2以上の情報を取り扱う場合、以下を含むクラウドサービス（自治体機密性2以上の情報を取り扱う場合）の利用に関する規定を整備しなければならない。

- ①統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方等を踏まえ、クラウドサービスを利用して情報システムを導入・構築する際のセキュリティ対策の基本方針を運用規程として整備しなければならない。
- ②統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、クラウドサービスを利用して情報システムを運用・保守する際のセキュリティ対策の基本方針を運用規程として整備しなければならない。
- ③統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下を全て含むクラウドサービスの利用を終了する際のセキュリティ対策の基本方針を運用規程として整備しなければならない。
 - （ア）クラウドサービスの利用終了時における対策
 - （イ）クラウドサービスで取り扱った情報の廃棄
 - （ウ）クラウドサービスの利用のために作成したアカウントの廃棄

（3）クラウドサービスの選定

- ①情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限を踏まえ、クラウドサービス利用判断基準に従って、業務に係る影響度等を検討した上でクラウドサービスの利用を検討しなければならない。
- ②情報セキュリティ責任者は、クラウドサービスで取り扱う情報の格付及び取扱制限を踏まえ、クラウドサービス提供者の選定基準に従ってクラウドサービス提供者を選定すること。また、以下の内容を含む情報セキュリティ対策をクラウドサービス提供者の選定条件に含めなければならない。
 - （ア）クラウドサービスの利用を通じて本市が取り扱う情報のクラウドサービス提供者における目的外利用の禁止
 - （イ）クラウドサービス提供者における情報セキュリティ対策の実施内容及び管

理体制

(ウ) クラウドサービスの提供に当たり、クラウドサービス提供者若しくはその従業員、再委託先又はその他の者によって、本市の意図しない変更が加えられないための管理体制

(エ) クラウドサービス提供者の資本関係・役員等の情報、クラウドサービス提供に従事する者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供並びに調達仕様書による施設の場所やリージョンの指定

(オ) 情報セキュリティインシデントへの対処方法

(カ) 情報セキュリティ対策その他の契約の履行状況の確認方法

(キ) 情報セキュリティ対策の履行が不十分な場合の対処方法

③情報セキュリティ責任者は、クラウドサービスの中断や終了時に円滑に業務を移行するための対策を検討し、クラウドサービス提供者の選定条件に含めなければならない。

④情報セキュリティ責任者は、クラウドサービスの利用を通じて本市が取り扱う情報の格付等を勘案し、必要に応じて以下の内容をクラウドサービス提供者の選定条件に含めなければならない。

(ア) 情報セキュリティ監査の受入れ

(イ) サービスレベルの保証

⑤情報セキュリティ責任者は、クラウドサービスの利用を通じて本市が取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクを評価してクラウドサービス提供者を選定し、必要に応じて本市の情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を選定条件に含めなければならない。

⑥情報セキュリティ責任者は、クラウドサービス提供者がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、クラウドサービス提供者の選定条件で求める内容をクラウドサービス提供者に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を本市に提供し、本市の承認を受けるよう、クラウドサービス提供者の選定条件に含めなければならない。また、クラウドサービス利用判断基準及びクラウドサービス提供者の選定基準に従って再委託の承認の可否を判断しなければならない。

⑧情報セキュリティ責任者は、クラウドサービスの特性を考慮した上で、クラウドサービスが提供する部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上で、情報セキュリティに関する役割及び責任の範囲を踏まえて、以下を全て含むセキュリティ要件を定めなければならない。

- (ア) クラウドサービスに求める情報セキュリティ対策
 - (イ) クラウドサービスで取り扱う情報が保存される国・地域及び廃棄の方法
 - (ウ) クラウドサービスに求めるサービスレベル
- ⑨統括情報セキュリティ責任者は、情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、クラウドサービス提供者の信頼性が十分であることを総合的・客観的に評価し判断しなければならない。
- (4) クラウドサービスの利用に係る調達・契約
- ①情報セキュリティ責任者は、クラウドサービスを調達する場合は、クラウドサービス提供者の選定基準及び選定条件並びにクラウドサービスの選定時に定めたセキュリティ要件を調達仕様に含めなければならない。
 - ②情報セキュリティ責任者は、クラウドサービスを調達する場合は、クラウドサービス提供者及びクラウドサービスが調達仕様を満たすことを契約までに確認し、利用承認を得なければならない。また、調達仕様の内容を契約に含めなければならない。
- (5) クラウドサービスの利用承認
- ①情報セキュリティ責任者は、クラウドサービスを利用する場合には、統括情報セキュリティ責任者へクラウドサービスの利用申請を行わなければならない。
 - ②統括情報セキュリティ責任者は、職員等によるクラウドサービスの利用申請を審査し、利用の可否を決定しなければならない。
 - ③統括情報セキュリティ責任者は、クラウドサービスの利用申請を承認した場合は、承認済みクラウドサービスとして記録しなければならない。
- (6) クラウドサービスを利用した情報システムの導入・構築時の対策
- ①統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方等を踏まえ、以下を含むクラウドサービスを利用して情報システムを構築する際のセキュリティ対策を規定しなければならない。
 - (ア) 不正なアクセスを防止するためのアクセス制御
 - (イ) 取り扱う情報の機密性保護のための暗号化
 - (ウ) 開発時におけるセキュリティ対策
 - (エ) 設計・設定時の誤りの防止
 - ②情報セキュリティ管理者は、情報システムにおいてクラウドサービスを利用する際には、情報システム台帳及び関連文書に記録又は記載しなければならない。
 - ③情報セキュリティ管理者は、クラウドサービスの情報セキュリティ対策を実施するために必要となる文書として、クラウドサービスの運用開始前までに以下の実施手順を整備しなければならない。
 - (ア) クラウドサービスで利用するサービスごとの情報セキュリティ水準の維持に関する手順

- (イ) クラウドサービスを利用した情報システムの運用・監視中における情報セキュリティインシデントを認知した際の対処手順
 - (ウ) 利用するクラウドサービスが停止又は利用できなくなった際の復旧手順
 - ④情報セキュリティ管理者は、前項において定める規定に対し、構築時に実施状況を確認・記録しなければならない。
- (7) クラウドサービスを利用した情報システムの運用・保守時の対策
- ①統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下を含むクラウドサービスを利用して情報システムを運用する際のセキュリティ対策を規定しなければならない。
 - (ア) クラウドサービス利用方針の規定
 - (イ) クラウドサービス利用に必要な教育
 - (ウ) 取り扱う資産の管理
 - (エ) 不正アクセスを防止するためのアクセス制御
 - (オ) 取り扱う情報の機密性保護のための暗号化
 - (カ) クラウドサービス内の通信の制御
 - (キ) 設計・設定時の誤りの防止
 - (ク) クラウドサービスを利用した情報システムの事業継続
 - ②情報セキュリティ管理者は、クラウドサービスの運用・保守時に情報セキュリティ対策を実施するために必要となる項目等で修正又は変更等が発生した場合、情報システム台帳及び関連文書を更新又は修正し、統括情報セキュリティ責任者へ報告しなければならない。
 - ③情報セキュリティ管理者は、クラウドサービスの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講じなければならない。
 - ④情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、クラウドサービスで発生したインシデントを認知した際の対処手順を整備しなければならない。
 - ⑤情報セキュリティ管理者は、前各項において定める規定に対し、運用・保守時に実施状況を定期的に確認・記録しなければならない。
- (8) クラウドサービスを利用した情報システムの更改・廃棄時の対策
- ①統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下を含むクラウドサービスの利用を終了する際のセキュリティ対策を規定しなければならない。
 - (ア) クラウドサービスの利用終了時における対策
 - (イ) クラウドサービスで取り扱った情報の廃棄
 - (ウ) クラウドサービスの利用のために作成したアカウントの廃棄

②情報セキュリティ管理者は、前項において定める規定に対し、クラウドサービスの利用終了時に実施状況を確認・記録しなければならない。

9. 4. 外部サービス（クラウドサービス）の利用（自治体機密性2以上の情報を取り扱わない場合）

(1) クラウドサービスの利用に係る規定の整備

統括情報セキュリティ責任者は、自治体機密性2以上の情報を取り扱わない場合、以下を含むクラウドサービスの利用に関する規定を整備しなければならない。

- (ア) クラウドサービスを利用可能な業務の範囲
- (イ) クラウドサービスの利用申請の許可権限者と利用手続
- (ウ) クラウドサービスの利用状況の管理
- (エ) クラウドサービスの利用の運用手順

(2) クラウドサービスの利用における対策の実施

①職員等は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で自治体機密性2以上の情報を取り扱わない場合のクラウドサービスの利用を申請しなければならない。また、情報セキュリティ管理者は、当該クラウドサービスの利用において適切な措置を講じなければならない。

②情報セキュリティ責任者は、職員等によるクラウドサービスの利用申請を審査し、利用の可否を決定しなければならない。また、承認したクラウドサービスを記録しなければならない。

9. 5. ソーシャルメディアサービスの利用

①情報セキュリティ管理者は、本市が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。

(ア) 本市のアカウントによる情報発信が、実際の本市のものであることを明らかにするために、本市の自己管理ウェブサイト当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を実施すること。

(イ) パスワードや認証のためのコード等の認証情報等を適正に管理するなどの方法で、不正アクセス対策を実施すること

②自治体機密性2以上の情報はソーシャルメディアサービスで発信してはならない。

③利用するソーシャルメディアサービスごとの責任者を定めなければならない。

④アカウント乗っ取りを確認した場合には、被害を最小限にするための措置を講じなければならない。

⑤自治体可用性2の情報の提供にソーシャルメディアサービスを用いる場合は、本

市の自己管理ウェブサイト当該情報を掲載して参照可能とすること。

10. 評価・見直し

10. 1. 監査

(1) 実施方法

CISO は、情報セキュリティ監査統括責任者を指名し、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、必要に応じて監査を行わせなければならない。

(2) 監査を行う者の要件

- ①情報セキュリティ監査統括責任者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。
- ②監査を行う者は、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でなければならない。

(3) 監査実施計画の立案及び実施への協力

- ①情報セキュリティ監査統括責任者は、監査を行うに当たって、監査実施計画を立案し、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被監査部門は、監査の実施に協力しなければならない

(4) 委託事業者に対する監査

委託事業者に委託している場合、情報セキュリティ監査統括責任者は委託事業者から下請けとして受託している事業者も含めて、情報セキュリティポリシーの遵守について監査を必要に応じて行わなければならない。

(5) 報告

情報セキュリティ監査責任者は、監査結果を取りまとめ、CISO に報告を行うものとする。また、必要に応じ、情報セキュリティ委員会に報告を行うものとする。

(6) 保管

情報セキュリティ監査責任者は、監査の実施を通して収集した監査証拠、監査報告書の作成のための監査調書を、紛失等が発生しないように適正に保管しなければならない。

(7) 監査結果への対応

- ①CISO は、監査結果を踏まえ、指摘事項を所管する情報セキュリティ管理者に対し、当該事項への対処を指示しなければならない。また、指摘事項を所管していない情報セキュリティ管理者に対しても、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。
- ②CISO は、指摘事項を所管していない情報セキュリティ管理者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。また、庁内で横断的に改善が必要な事項については、統括情報セキュリティ責任者に対し、当該事項への対処（改善計画の策定等）を指示し

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

(8) 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は、監査結果を情報セキュリティポリシー及び関係規定等の見直し、その他情報セキュリティ対策の見直し時に活用する。

10. 2. 自己点検

(1) 実施方法

①統括情報セキュリティ責任者及び情報セキュリティ管理者は、所管するネットワーク及び情報システムについて、必要に応じて自己点検を実施しなければならない。

②情報セキュリティ責任者は、情報セキュリティ管理者と連携して、所管する部局における情報セキュリティポリシーに沿った情報セキュリティ対策状況について、毎年度及び必要に応じて自己点検を行わなければならない。

(2) 報告

統括情報セキュリティ責任者、情報セキュリティ責任者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、CISO に報告する。また、必要に応じ、情報セキュリティ委員会に報告するものとする。

(3) 自己点検結果の活用

①職員等は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

②情報セキュリティ委員会は、この点検結果を情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用する。

10. 3. 情報セキュリティポリシー及び関係規程等の見直し

情報セキュリティ委員会は、情報セキュリティ監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等を踏まえ、情報セキュリティポリシー及び関係規程等について評価を行い、必要があると認めた場合、改定内容を審議するものとする。

審議結果を踏まえ、市長の判断により改定を行うものとする。ただし、緊急を要する場合又は軽微な改正については、CISO の判断により実施することができる。

附則（平成 17 年 3 月 30 日市長決裁）

栗東市情報セキュリティポリシーは、平成 17 年 4 月 1 日から施行する。

附則（平成 31 年 2 月 22 日市長決裁）

栗東市情報セキュリティポリシーは、平成 31 年 3 月 1 日から施行する。

附則（令和 5 年 11 月 20 日市長決裁）

栗東市情報セキュリティポリシーは、令和 5 年 11 月 20 日から施行する。

附則（令和 7 年 3 月 日市長決裁）

栗東市情報セキュリティポリシーは、令和 7 年 月 日から施行する。