藤枝市情報セキュリティポリシー

平成２７年１２月２８日 改定

藤枝市総務部情報政策課

目　　次

序章　藤枝市情報セキュリティポリシーの構成

藤枝市情報セキュリティポリシー（以下「情報セキュリティポリシー」という。）とは、藤枝市が保有する情報資産に関するセキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであり、情報セキュリティに対する取組姿勢を示す「情報セキュリティ基本方針」と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示す「情報セキュリティ対策基準」から構成される。

また、情報セキュリティポリシーに基づき、情報システムごとに具体的な情報セキュリティ対策の実施手順（運用マニュアル）として「情報セキュリティ実施手順」を策定する。

くわえて、情報セキュリティポリシーに基づき、特定個人情報の適正な取扱いに関する統一的かつ基本的な方針として「特定個人情報の適正な取扱いに関する基本方針」を策定するとともに、特定個人情報の具体的な取扱と安全管理措置を定めるものとして「特定個人情報取扱規程」を策定する。

情報セキュリティポリシーの構成

標　　題	内　　容
情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針
情報セキュリティ対策基準	情報セキュリティ基本方針を実行するための全ての情報資産に共通の情報セキュリティ対策の基準

情報セキュリティポリシーに基づき策定する文書

標　　題	内　　容
情報セキュリティ実施手順（運用マニュアル）	情報システムごとに定める情報セキュリティ対策基準に基づいた個々の情報資産に関する具体的な対策手順
特定個人情報の適正な取扱いに関する基本方針	特定個人情報の適正な取扱いに関する統一的かつ基本的な方針
特定個人情報取扱規程	特定個人情報の具体的な取扱いと安全管理措置

第１章　情報セキュリティ基本方針

１　目的

本基本方針は、市が保有する情報資産を様々な脅威から防御し、機密性、完全性及び可用性を維持するため、市が行う情報セキュリティに関する対策の統一かつ基本的な事項を定めることを目的とする。

２　定義

（１）コンピュータ

パーソナルコンピュータ、サーバ、ストレージ等の機器をいう。

（２）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及びその構成機器をいう。

（３）情報システム

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

（４）行政情報

行政事務の執行に関わる情報及びその記録をいう。

（５）情報資産

情報システム及び行政情報をいう。

（６）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。

（７）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。

（８）完全性

情報に誤謬がなく、改ざん又は破損等により情報が消去されていない状態を確保することをいう。

（９）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。

（１０）情報セキュリティインシデント

情報セキュリティに関する障害・事故及びシステム上の欠陥をいう。

（１１）個人情報

個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。

（１２）個人番号

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。以下「番号法」という。）第２条第３項に規定される個人を識別するための番号をいう。

（１３）特定個人情報

個人番号をその内容に含む個人情報をいう。

３　適用範囲

（１）対象者の範囲

この基本方針の対象範囲は、市が保有する情報資産に接する全ての職員と労働者派遣事業により本市の事務に携わる者（以下「職員等」という。）及び委託事業者とする。

（２）情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

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

４　遵守義務

職員等は、情報セキュリティの重要性について共通の認識を持つとともに、業務の遂行にあたって、情報セキュリティポリシーを遵守しなければならない。

５　情報資産への脅威

情報資産に対して想定される脅威として、以下のものを想定し情報セキュリティ対策を実施する。

（１）不正侵入又は不正操作

権限外者による故意の不正侵入又は不正操作によるデータやプログラムの持ち出し・改ざん・消去、機器及び記録媒体の盗難等。

（２）職員及び外部委託者による意図しない操作、故意の不正アクセス又は不正操作

職員及び外部委託者による意図としない操作、故意の不正アクセス又は不正操作によるデータやプログラムの持ち出し・改ざん・消去、機器及び記録媒体の盗難、規定外の情報システムの機器操作によるデータ漏洩等。

（３）災害等

地震、落雷、火災等の災害や事故、故障等。

６　情報セキュリティ対策

市は、市が保有する情報資産を上記５の脅威から保護するため、以下の情報セキュリティ対策を講ずるものとする。

（１）組織的安全管理措置

情報セキュリティ対策を推進する全庁的な組織体制を整備する。また、情報セキュリティインシデント発生時の体制を整備する。

（２）情報資産の分類と管理

市が取り扱う又は今後取り扱おうと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、当該分類に応じた情報セキュリティ対策を行うものとする。

（３）人的安全管理措置

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ずる。

（４）物理的安全管理措置

情報資産を有する保管庫や施設等への不正な立ち入りや、情報資産の損傷、盗難等を防ぐために、情報資産の設置や管理について、物理的な対策を講じる。

（５）技術的安全管理措置

情報資産を不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、コンピュータウィルス対策等を実施する。

（６）運用における安全管理措置

情報資産の管理、情報セキュリティポリシーの遵守状況の確認、情報セキュリティインシデント発生時の対応等、セキュリティ対策の運用面の対策を講ずる。

７　情報セキュリティ監査又は自己点検の実施

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又は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、情報セキュリティに関する状況の変化等を踏まえ、必要に応じ適宜情報セキュリティポリシーの見直しを行う。

９　情報セキュリティ対策基準の策定

本市の情報資産について、情報セキュリティ対策を講ずるにあたっては、職員が遵守すべき事項及び判断等の基準を統一的なレベルで定める必要がある。そのため、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した「情報セキュリティ対策基準」を策定するものとする。

なお、情報セキュリティ対策手順は、公開することにより本市の行政運営に重大な支障を及ぼす恐れがあることから、非公開とする。

１０　情報セキュリティ実施手順（運用マニュアル）の策定

情報セキュリティ対策を確実に実施していくためには、個々の情報資産に関する対策の手順を具体的に定めておく必要があることから、情報セキュリティ対策基準に基づき、「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、公開することにより本市の行政運営に重大な支障を及ぼす恐れがあることから、非公開とする。

１１　特定個人情報の適正な取扱いに関する基本方針の策定

本市が番号法に定められた事務において個人番号及び特定個人情報を適正に取り扱うための統一かつ基本的な事項を定めることを目的として「特定個人情報の適正な取扱いに関する基本方針」を策定するものとする。

１２　特定個人情報取扱規程の策定

情報セキュリティポリシー並びに特定個人情報の適正な取扱いに関する基本方針に基づき、本市における個人番号及び特定個人情報の取り扱いを具体的に定めておく必要があることから、「特定個人情報取扱規程」を策定するものとする。

なお、特定個人情報取扱規程は、公開することにより本市の行政運営に重大な支障を及ぼす恐れがあることから、非公開とする。

第２章　情報セキュリティ対策基準

１　目的

本対策基準は、藤枝市情報セキュリティ基本方針に基づき、情報資産に接するすべての職員が遵守すべき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　定義

本対策基準における用語の意義は、情報セキュリティ基本方針に規定する用語の定義を準用する。

３　対象範囲

本対策基準の対象範囲は、情報セキュリティ基本方針に規定する適用範囲を準用する。

４　組織体制

（１）　組織体制と役割

本市の情報セキュリティ対策の組織体制及び各役職の役割は下記の通りである。

① 最高情報セキュリティ責任者（CISO）

最高情報セキュリティ責任者は、本市における全ての情報資産の管理及び情報セキュリティ対策に関する権限及び責任を有するものとし、情報政策に関する事務を担当する副市長をもってこれに充てる。

② 統括情報セキュリティ責任者

統括情報セキュリティ責任者は、最高情報セキュリティ責任者を補佐し、情報セキュリティ責任者、情報セキュリティ管理者、情報基盤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ものとし、情報政策に関する事務を担当する部の長をもってこれに充てる。

ただし、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に関する事務を担当する課の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

情報セキュリティ責任者は、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ものとし、各部局の長をもってこれに充てる。

④ 情報セキュリティ管理者

情報セキュリティ管理者は、所管する課室等の情報セキュリティ対策の実施に関する権限及び責任を有するとともに、所管する情報資産の適正な管理運用を行うものとし、各課室等の長をもってこれに充てる。

⑤ 情報基盤管理者

情報基盤管理者は、本市の共通的なネットワーク、情報システム、データ等の情報資産の管理に関する権限及び責任を有し、当該情報資産の適正な管理運用を行うものとし、情報政策に関する事務を担当する課の長をもってこれに充てる。

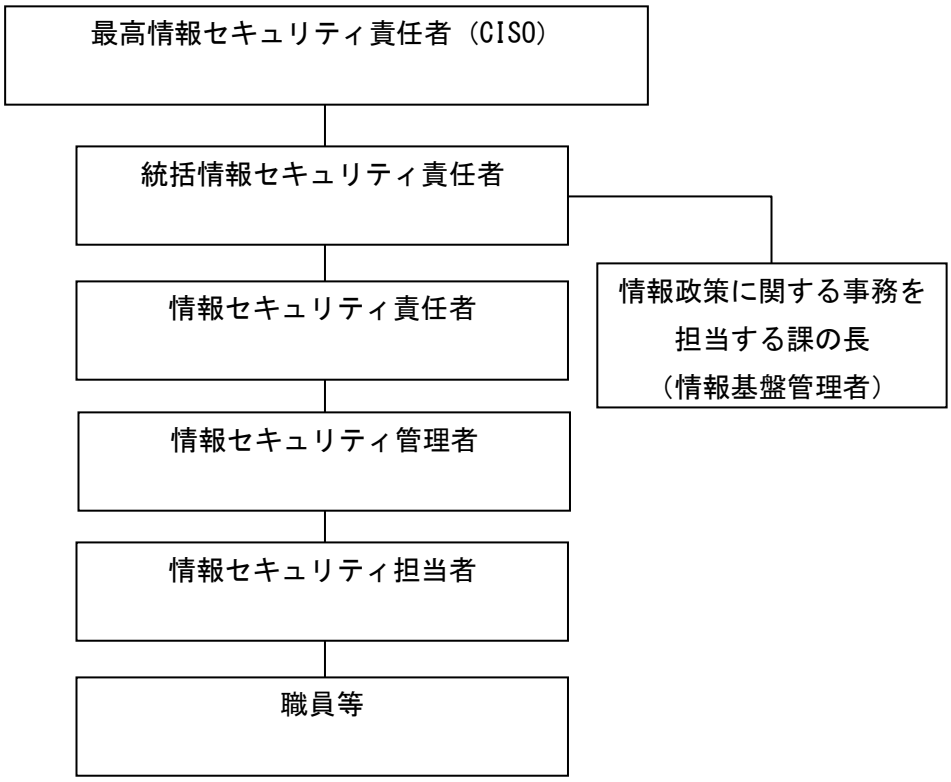
⑥ 情報セキュリティ担当者

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、所属する課室等の情報セキュリティに関する対策の向上を図るものとし、情報セキュリティ管理者が指名する者をもってこれに充てる。

⑦ 職員等

職員等は、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する。

【組織体制図】



（２） 情報セキュリティに関する統一的な窓口

① 情報セキュリティに関する統一的な窓口の設置

最高情報セキュリティ責任者は、情報セキュリティの事件・事故等の情報セキュリティインシデント（以下、「情報セキュリティインシデント）という。）の統一的な窓口を整備するものとし、情報セキュリティに関する統一的な窓口の管理者は、情報政策に

関する事務を担当する課の長をもってこれに充てる。

② 連絡体制

ア．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又はその疑いがあると判断した場合は、速やかに情報セキュリティ管理者及び情報基盤管理者に報告するものとする。

イ．職員等は、本市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情報基盤管理者に報告するものとする。

ウ．職員等から情報セキュリティインシデントについての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するものとする。また、情報基盤管理者と協議し、必要に応じて統括情報セキュリティ責任者及び最高情報セキュリティ責任者に報告するものとする。

③ 調査・記録、再発防止等

ア．情報セキュリティ責任者は、情報セキュリティインシデントを引き起こした課室等の情報セキュリティ管理者、情報基盤管理者等と連係し、情報セキュリティインシデントの内容、発生原因、確認した被害、影響範囲について調査を実施し、記録を保存しなければならない。また、調査の結果から、再発防止策を検討するとともに、必要に応じて、統括情報セキュリティ責任者及び最高情報セキュリティ責任者に報告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最高情報セキュリティ責任者は、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、内容を確認し、その対応及び再発防止策を実施するために必要な措置について指示しなければならない。

④ 関係部局等への情報提供

情報セキュリティに関する統一的な窓口は、最高情報セキュリティ責任者による情報セキュリティ戦略の意思決定が行われた際には、その内容を関係部局等に提供するものとする。

⑤ 連絡手段の公表

情報セキュリティに関する統一的な窓口は、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連絡手段を公表するものとする。

（３） 兼務の禁止

情報セキュリティ対策の実施において、やむを得ない場合を除き、承認又は許可の申請を行う者とその承認者又は許可者は、同じ者が兼務してはならない。

５ 情報資産の分類と管理

（１） 情報資産の分類

情報資産は、機密性、完全性及び可用性を踏まえ、次の重要性分類に従って分類する。

① 機密性による情報資産の分類

分類	分類基準
1	・ 藤枝市個人情報保護条例（平成１５年藤枝市条例第１号）第２条第２号に規定する個人情報 ・ 法令または条例（以下「法令等」という。）の定めにより守秘義務を課されている行政情報（上記個人情報を除く。） ・ 法人その他の団体に関する行政情報で漏洩することにより当該団体の利益を害する恐れのあるもの ・ 漏洩した場合、行政に対する信頼を著しく害する恐れのある行政情報 ・ 情報システムに関するパスワード及びシステム設定情報 ・ 特定個人情報
2	・ 脅威にさらされた場合に実害を受ける危険性は低いが、行政事務の執行において重要性が高いと評価される行政情報 ・ 公開されると行政の円滑な執行に著しい障害を生ずる恐れのある行政情報等
3	・ 上記以外の情報資産

② 完全性による情報資産の分類

分類	分類基準
1	・ 誤謬、改ざん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著しい支障を及ぼす可能性がある情報資産
2	・ 脅威にさらされた場合に実害を受ける危険性は低いが、行政事務の執行において重要性が高いと評価される行政情報 ・ 公開されると行政の円滑な執行に著しい障害を生ずる恐れのある行政情報等
3	・ 上記以外の情報資産

③ 可用性による情報資産の分類

分類	分類基準
1	・ 滅失、またはき損した場合、その復元が著しく困難となり行政の円滑な執行を妨げる恐れのある行政情報
2	・ 上記以外の情報資産

（２） 情報資産の管理方法

① 情報資産の管理責任

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

② 情報の作成及び消去

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、当該情報が作成途上であっても、1 の分類に基づき管理しなければならない。

ウ．情報を消去する者は、情報が不要になった場合は、当該情報を速やかに消去しなければならない。

③ 情報資産の入手

自己以外の者が作成した情報資産を入手した者は、（１）の分類に基づき管理しなければならない。

④ 情報資産の利用

ア．情報資産は、業務以外の目的に利用してはならない。

イ．情報資産は、情報資産の分類に応じ、適切な取扱いをしなければならない。

ウ．情報資産は、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、当該記録媒体を取り扱わなければならない。

⑤ 機密性分類による取扱の制限

ア．機密性分類２に掲げる情報資産の管理にあたっては、以下に掲げる事項を遵守しなければならない。

- 許可された者以外による閲覧の制限
- 適切なネットワークの選択
- 不用意な複製・送付・送信の禁止

イ．機密性分類１に掲げる情報資産の取扱にあたっては、アに加えて、以下に掲げる事項を遵守しなければならない。

- インターネットや電子メールによる外部への送信の禁止
- 電子ファイルの暗号化やパスワードの設定
- 施錠可能な場所への保存

ウ．機密性分類１に掲げる情報資産であって、特定個人情報に該当するものの取扱にあたっては、イに加えて、特定個人情報の適正な取扱いに関する基本方針及び特定個人情報取扱規程に掲げる事項を遵守しなければならない。

⑥ 完全性分類による取扱の制限

完全性分類１に掲げる情報資産の管理にあたっては、以下に掲げる事項を遵守しなければならない。

ア．許可された者以外による編集や更新の制限

イ. 施錠可能な場所への保存

ウ. バックアップの作成

⑦ 可用性分類による取扱の制限

可用性分類１に掲げる情報資産の管理にあたっては、以下に掲げる事項を遵守しなければならない。

ア. サーバやネットワーク等の冗長化

イ. 施錠可能な場所への保存

ウ. バックアップの作成

⑧ 情報資産の管理

ア. 情報セキュリティ管理者は、情報資産の分類に従って、情報資産を適切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外部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、利用頻度が低い外部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外部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しなければならない。

エ. 情報セキュリティ管理者は、機密性分類１、２、完全性分類１、２、又は可用性分類１の情報資産を記録した外部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場所に保管しなければならない。

⑨ 情報資産の運搬

ア. 機密性分類１、２の情報資産を運搬する者は、職員等または守秘義務を明記した契約を締結した外部業者とし、運搬にあたっては、情報セキュリティ管理者に許可を得なければならない。

イ. 機密性分類１、２の情報資産の運搬にあたっては鍵付きのケース等に格納し、暗号化し、又はパスワードを設定する等、記録媒体の保護措置を講じなければならない。

⑩ 情報資産の提供又は公表

ア. 機密性分類１、２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。

イ. 情報セキュリティ管理者は、機密性分類１、２の情報資産の外部提供を許可する場合は、当該情報資産の外部提供が法令等及びその他関連する規定に抵触しないことを確認しなければならない。

ウ. 機密性分類１、２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。

エ. 情報セキュリティ管理者は、住民に提供又は公表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。

⑪ 情報資産の廃棄

ア．機密性分類１、２の情報資産の廃棄を行う者は、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、物理的に破壊又はデータ消去ソフトウェア等を利用し、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。

イ．機密性分類１、２の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。

ウ．機密性分類１、２の情報資産の廃棄を行う者は、廃棄の実施日時、実施担当者及び実施内容その他必要な事項を記録簿や実施報告書等により情報セキュリティ管理者に報告するとともに、当該文書等を関係書類とともに５年間保存しなければならない。また、廃棄を委託した場合も同様とし、必要に応じて証明書等の提出を求めなければならない。

６　人的安全管理措置

（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

ア．職員等は、情報セキュリティポリシー、情報セキュリティ実施手順その他の情報管理に関する規程を遵守しなければならない。

イ．職員等は、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 法令等の遵守

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、以下の法令のほか関係法令等を遵守しこれに従わなければならない。

ア．地方公務員法（昭和２５年法律第２６１号）

イ．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）

ウ．著作権法（昭和４５年法律第４８号）

エ．個人情報の保護に関する法律（平成１５年法律第５７号）

オ．行政機関の保有する個人情報の保護に関する法律（平成１５年法律第５８号）

カ．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）

キ．藤枝市個人情報保護条例（平成１５年条例第１号）

ク．藤枝市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に基づく個人番号の利用及び特定個人情報の提供に関する条例（平成２７年条例第４１号）

ケ．藤枝市文書取扱規程（昭和５０年訓令第３号）

③ 情報資産の持ち出しの制限

ア．職員等は、情報セキュリティ管理者の許可を得ることなく情報資産の持ち出し（庁舎内での移動等も含む。）及びＷｅｂサイト等を利用した外部への送信を

してはならない。

イ．職員等は、情報資産の持ち出しを行う場合において、盗難、破損等に十分留意するものとし、業務に必要な内容、期間を超えて持ち出しを行ってはならない。また、持ち出しの実施日時、実施担当者及び実施内容その他必要な事項を記録簿や実施報告書等により情報セキュリティ管理者に報告するとともに、当該文書等を関係書類とともに５年間保存しなければならない。

④ 業務に使用するコンピュータ等

ア. 職員等は、支給された以外のコンピュータ、モバイル端末、通信回線装置、デジタルカメラ、電磁的記録媒体その他の周辺機器等を業務に使用してはならない。ただし、業務上必要な場合は、情報基盤管理者の許可を得て利用することができる。

イ. 職員等は、使用するコンピュータや電磁的記録媒体等について使用権限のない者に使用されないようにしなければならない。

ウ. 職員等は、情報基盤管理者の許可を得ることなく、支給されたコンピュータに関するセキュリティ機能の設定を変更してはならない。

エ. 職員等は、出所が不明なファイルや、内容に確証の得られていないファイル等は、実行してはならない。

⑤ インターネット・電子メールの使用

ア．職員等は、業務上必要な場合を除き、インターネットの閲覧や電子メールの送受信をしてはならない。

イ．職員等は、インターネットに接続できる端末に、機密性分類１、２に該当する情報資産を不用意に複製・保存をしてはならない。

ウ．職員等は、機密性分類１に該当する情報資産を電子メール等により送付してはならない。

エ．職員等は、機密性分類２に該当する情報資産を電子メール等により送信する必要がある場合には、事前に情報セキュリティ管理者の承認を受けなければならない。

⑥ 情報システムへの接続

職員等は、情報システムへの接続について、必要最小限の接続時間で行うよう努めるものとする。

⑦ パスワード等の管理

ア．パスワードの長さは十分な長さとして、文字列は想像しにくいものとしなければならない。

イ．職員等は、自己の保有するパスワードについて、不用意にもらしたり、メモを作ったりしないようパスワードの秘密保持に努めなければならない。

⑧ ＵＳＢキー等の管理

ア．ＵＳＢキー等は共有又は貸し借りをして利用してはならない。

イ．ＵＳＢキー等を紛失した場合には、速やかに情報基盤管理者に報告し、その指示を仰がなければならない。

ウ．情報基盤管理者は、ＵＳＢキー等の管理を所管する紛失の報告があり次第、速やかに当該媒体の使用を不可能にしなければならない。

⑨ 異動・退職等

職員等は、異動、退職等により業務を離れる場合には、知り得た情報を他に漏らしてはならない。

（２） 外部委託に関する管理

情報システムの開発・保守・管理等を外部委託する場合は、委託契約に際して契約書に善良な管理者の注意義務及び秘密保持義務を明記するものとする。

（３） 研修等

① 研修等の実施

最高情報セキュリティ責任者は、職員等に対する情報セキュリティに関する研修又は訓練を１年に１回以上実施しなければならない。

② 研修等への参加

ア．情報セキュリティ管理者は、所管する課室等の職員等に対して、最高情報セキュリティ責任者が実施する研修又は訓練への参加の機会を付与する等の必要な措置を講じなければならない。

イ．職員等は、最高情報セキュリティ責任者が実施する研修又は訓練に参加しなければならない。

７　物理的安全管理措置

（１） マシン室

① マシン室の設置

ア．統括情報セキュリティ責任者及び情報基盤管理者は、施設管理部門と連携して、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、当該機器の管理及び運用を行うため基幹的なサーバ等の機器を設置する室（以下「マシン室」という。）を設置するものとする。

イ．統括情報セキュリティ責任者及び情報基盤管理者は、施設管理部門と連携して、マシン室から外部に通ずるドアを必要最小限とするとともに、鍵、監視機能、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。

ウ．統括情報セキュリティ責任者及び情報基盤管理者は、施設管理部門と連携して、マシン室に設置する機器等の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。

エ．統括情報セキュリティ責任者及び情報基盤管理者は、施設管理部門と連携して、マシン室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 マシン室への入退室

ア．情報基盤管理者は、マシン室への入退室を許可された者のみに制限し、入退室管理簿への記録等入退室管理を行わなければならない。

イ．情報基盤管理者は、マシン室に職員が不在となる場合には、施錠するなど部外者の進入を防ぐ措置を講じなければならない。

ウ．職員等及び外部委託事業者は、マシン室に入室する場合、身分証明書等を携帯し、情報基盤管理者の求めにより提示しなければならない

エ．情報基盤管理者は、外部からの訪問者がマシン室に入る場合には、必要に応じて立ち入りできる区域を制限した上で、マシン室への入退室を許可された職員が付き添うものとし、身分証明書等を首から提げる等により外見上職員と区別できる措置を講じなければならない。

オ．職員等及び外部委託事業者は、マシン室内に当該情報システムに関連しないコンピュータ、モバイル端末、通信回線装置、デジタルカメラ、電磁的記録媒体その他の周辺機器等を持ち込んではならない。

③ 機器等の搬入出

ア．情報セキュリティ管理者は、マシン室への機器等の搬入及びマシン室からの機器等の搬出を実施する場合は、情報基盤管理者と連携し、あらかじめマシン室及び既存の情報システムに対する安全性について確認を行わなければならない。

イ．情報セキュリティ管理者は、機器の搬入・搬出にあたって、職員が立ち会う等の必要な措置を講じなければならない。

（２） 管理区域及び取扱区域の設定

ア．情報セキュリティ管理者は、機密性分類１、２に掲げる事務について、情報システムを管理する区域（以下「管理区域」という。）を定めなければならない。

イ．情報セキュリティ管理者は、機密性分類１、２に掲げる事務を実施する場所（以下「取扱区域」という。）を定めなければならない。

ウ．情報セキュリティ管理者は、管理区域及び取扱区域の設定にあたって、機器、電子媒体及び書類等の盗難又は紛失等を防止するために必要な物理的安全管理措置を講ずるものとする。

（３） サーバ等

① 機器の取付け

情報基盤管理者及び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切に固定する等、必要な措置を講じなければならない。

② サーバの冗長化

情報基盤管理者及び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､可用性、停止することによる業務への影響度等を勘案し、必要に応じて冗長

化を施し、サービスや業務を停止させないよう努めなければならない。

③ 電源及び配線

ア．情報基盤管理者及び情報セキュリティ管理者は、停電及び電圧異常等によりデータ等が破壊され、業務処理に支障をきたす恐れのあるサーバ等の機器の電源について、当該機器を適切に停止するまでの間に必要な電力を供給する容量の予備電源を備え付ける等の措置を講じなければならない。

イ．情報基盤管理者及び情報セキュリティ管理者は、配線について、傍受又は損傷等を受けることがないよう可能な限り必要な措置を施さなければならない。また、主要な箇所の配線の損傷等について、定期的な点検を行わなければならない。

④ 機器の定期保守及び修理

ア．情報基盤管理者及び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。

イ．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にあたって、電磁的記録媒体の行政情報を消去することができない場合は、修理を委託する事業者と守秘義務を明記した契約を締結しなければならない。

⑤ 機器の廃棄等

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、すべ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。

（４） ネットワーク

① 庁内の通信回線及び通信回線装置の管理

ア．統括情報セキュリティ責任者及び情報基盤管理者は、施設管理部門と連携し、通信回線及び通信回線装置を適切に管理しなければならない。

イ．情報セキュリティ管理者は、所管する課室においてネットワークを構築する場合は、統括情報セキュリティ責任者の許可を受けなければならない。

② 庁内の通信回線及び通信回線装置の管理

ア．統括情報セキュリティ責任者及び情報基盤管理者は、外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

イ．統括情報セキュリティ責任者及び情報基盤管理者は、国・県等のネットワークに接続する場合は、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。

③ 機密を要する情報システムで使用する回線

ア．情報基盤管理者は、機密性分類１、２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、適切な回線を選択しなければならない。

イ．機密性分類１、２の情報資産を送受信する場合は、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。

④ 完全性・可用性の確保

ア．統括情報セキュリティ責任者及び情報基盤管理者は、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、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。

イ．統括情報セキュリティ責任者及び情報基盤管理者は、可用性分類１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） 職員等が使用するパソコン等の管理

情報セキュリティ管理者は、盗難又は紛失等を防止するため、業務で使用するコンピュータやモバイル端末の使用時以外の施錠管理等物理的措置を講じなければならない。

８　技術的安全管理措置

（１） 情報システム及びネットワーク

① 情報システム管理記録の作成と管理

情報セキュリティ管理者は、担当する情報システムにおいて行ったシステムの変更作業を記録し、適切に管理しなければならない。

② 情報システム仕様書の管理

ア．情報セキュリティ管理者は、担当する情報システムの仕様書を常に最新の状態にしておき、システムの仕様変更を行った場合は、その記録を作成しなければならない。

イ．情報セキュリティ管理者は、担当する情報システムの仕様書を業務上必要とする者のみが閲覧できる場所に保管しなければならない。

③ アクセス記録の取得

ア．情報セキュリティ管理者は、アクセス記録及びセキュリティ関連障害に関する記録を取得し、一定の期間保存しなければならない。

イ．情報セキュリティ管理者は、アクセス記録が窃取、改ざん又は消去されないように必要な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、可能な範囲でアクセス記録を分析しなければならない。

④ 障害記録の作成

情報セキュリティ管理者は、可能な範囲で障害記録を作成し、一定の期間保存しなければならない。

⑤ ソフトウェアの導入

ア．職員等は、新たにソフトウェアを導入する場合は、情報セキュリティ管理者及び情報基盤管理者の許可を得なければならない。

イ．職員等は、正規のライセンスのないソフトウェアを導入してはならない。

ウ．職員等は、業務上不必要なソフトウェア及び出所不明なソフトウェア等安全性が確認されないソフトウェアをインストールしてはならない。

エ．職員等は、導入されているソフトウェアを適切に運用管理しなければならない。

⑥ ネットワークの接続制御、経路制御等

ア．統括情報セキュリティ責任者及び情報基盤管理者は、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。

イ．統括情報セキュリティ責任者及び情報基盤管理者は、不正アクセスを防止するため、ネットワークに適切なアクセス制御を施さなければならない。

⑦ 外部の者が利用できるシステムの分離等

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、外部の者が利用できる場合、必要に応じ他のネットワーク及び情報システムと分離する等の措置を講じな ければならない。

⑧ 外部ネットワークとの接続制限等

ア．情報セキュリティ管理者は、所管する情報システムを外部ネットワークと接続しようとする場合には、統括情報セキュリティ責任者及び情報基盤管理者の許可を得なければならない。

イ．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関するセキュリティ技術等を詳細に調査し、庁内のすべての対象資産に影響が生じないことを確認しなければならない。

ウ．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、必要に応じて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。

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、ウェブサーバ等の情報システムをインターネットに公開する場合、庁内ネットワークへの侵入を防御するために、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うえで接続しなければならない。

オ．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遮断しなければならない。

⑨ 複合機のセキュリティ管理

ア．情報セキュリティ管理者は、プリンタ・ファクシミリ・イメージスキャナ・コピー機等の機能が一つにまとめられている機器（以下「複合機」という。）を使用する場合、複合機が備える機能について適切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。

イ．情報セキュリティ管理者は、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。

⑩ 無線 LAN 及びネットワークの盗聴対策

ア．職員等は、統括情報セキュリティ責任者及び情報基盤管理者の許可を得ることなく、無線ＬＡＮを利用した接続又は端末等の無線機能を利用した端末間通信を行ってはならない。

イ．統括情報セキュリティ責任者は、無線ＬＡＮを利用した接続又は端末等の無線機能を利用した端末間通信を認める場合、情報の破壊、盗聴、改ざん、消去等が生じないよう暗号化及び認証技術、その他充分なセキュリティ対策の実施を義務付けなければならない。

⑪ 電子メールのセキュリティ管理

ア．情報基盤管理者は、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。

イ．職員等は、差出人が不明なメールや不自然なファイルが添付されたメール等情報セキュリティに対する脅威の恐れがある電子メールを受信した場合は、直ちに廃棄しなければならない。

ウ．職員等は、庁外の複数の宛先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わからないようにしなければならない。

⑫ 暗号化

ア．暗号化は情報セキュリティ管理者が指示する方法を用いなければならない。

イ．暗号のパスワードは、機密性分類１の行政情報とする。

⑬ 情報システムの入出力データ

ア．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のチェック等を行い、それが正確であることを確実にするための対策を施さなければならない。

イ．情報セキュリティ管理者は、情報システムから出されるデータの処理が正しく行われていることを確認しなければならない。

（２） 情報システムのアクセス制御

① 利用者の識別及び認証

情報基盤管理者及び情報セキュリティ管理者は、当該情報システムに権限がない職員等情報取扱者がアクセスすることが不可能となるように、利用者の識別及び認証等適切な対応を行わなければならない。

② 利用者登録

ア．情報基盤管理者及び情報セキュリティ管理者は、情報システムの利用者の登録、

変更、抹消等については、各情報システムに定められた方法にしたがって行わなければならない。

イ．利用者登録、変更等は、情報基盤管理者又は情報セキュリティ管理者に対する申請により行わなければならない。

③ インターネット以外のネットワークへのアクセス制御

統括情報セキュリティ責任者及び情報基盤管理者は、不必要なネットワークサービスにアクセスできないよう必要な措置を講じなければならない。

④ パスワード等の管理

職員等は、情報システムのアクセス制御に関するＩＤ、パスワードを厳重に管理しなければならない。

（３） 情報システムの開発・導入・保守

① 情報システムの開発・導入

ア．情報基盤管理者及び情報セキュリティ管理者は、情報システムのソフトウェアを開発・導入する場合は、情報セキュリティ上問題にならないかどうか、確認しなければならない。

イ．情報基盤管理者及び情報セキュリティ管理者は、情報システムのソフトウェアを開発する場合は、ソフトウェアの仕様書、ネットワーク構成図等を整備しなければならない。

ウ．情報基盤管理者及び情報セキュリティ管理者は、開発したソフトウェアを情報システムに取り入れる場合は、既に稼動している情報システムに接続する前に十分な試験を行わなければならない。

② 情報システムの変更管理

情報基盤管理者及び情報セキュリティ管理者は、情報システムを追加、変更、廃棄等した場合は、その際の設定・構成等の履歴を記録・保存し、必要な場合には復旧できるようにしなければならない。

③ ソフトウェアの保守及び更新

ア．情報セキュリティ管理者は、情報セキュリティに重大な影響を及ぼすソフトウェアについては、適切な保守が行われるようにし、その不具合については速やかに修正等の対応を行わなければならない。

イ．情報セキュリティ管理者は、情報システムのソフトウェアの更新等を、計画的に実施しなければならない。

④ 機器構成の変更

ア．職員等は、業務を遂行するため情報システムの機器の増設・交換を行う必要がある場合には、当該情報システムを所管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。

イ．職員等は、モデム等の機器を増設して、他のネットワークへ接続を行う場合及び他のネットワークからアクセスを可能とする仕組みを構築する場合には、情

報基盤管理者の許可を得なければならない。ただし、情報基盤管理者は、許可にあたって情報システム及び他の情報システムにセキュリティ上の問題を生じさせてはならない。

（４） コンピュータウィルス対策

① ウィルス対策ソフトの導入等

ア．情報セキュリティ管理者は、情報システムのサーバ及び必要な機器にウィルス対策ソフトを導入しなければならない。

イ．情報セキュリティ管理者は、ウィルスチェック用のパターンファイルを常に最新のものに保たなければならない。

ウ．情報セキュリティ管理者は、定期的に新種のウィルスに関する情報収集や情報システム内部の感染状況等について情報収集を行わなければならない。

エ．情報セキュリティ管理者は、コンピュータウィルス情報について、職員に対する注意喚起を行わなければならない。

オ．情報セキュリティ管理者は、コンピュータウィルスについて、職員に対して必要な啓発活動を行わなければならない。

② 職員等の遵守事項

ア．職員等は、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、必ずウィルスチェックを行わなければならない。

イ．職員等は、ウィルスチェックの実行を途中で止めてはならない。

ウ．職員等は、添付ファイルのあるメールを送受信する場合は、ウィルスチェックを行わなければならない。

エ．職員等は、情報セキュリティ管理者が提供するコンピュータウィルス情報を常に確認しなければならない。

（５） 不正アクセス対策

① 情報セキュリティ管理者の実施事項

ア．情報セキュリティ管理者は、セキュリティホール等の情報収集に努め、メーカー等から修正プログラムの提供があり次第、速やかに対応するとともに、その修正履歴を記録・保存しなければならない。

イ．情報セキュリティ管理者は、情報システムに不正な進入や利用があった場合に探知等できるよう、適切な対策に努めなければならない。

ウ．情報セキュリティ管理者は、情報システムに攻撃を受けていることが明らかな場合には、システムの停止を含め必要な措置を講じなければならない。

エ．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、職員等により本市ネットワーク及び外部ネットワークに対して不正なアクセスがあった場合は、当該職員等が属する課室等の情報セキュリティ管理者に通知し、適切な処置を求めなければならない。

② 職員等の遵守事項

職員等は、外部ネットワークより不正アクセスがあった場合は、速やかに情報セキュリティ管理者に報告し、適切な措置を講じなければならない。

（６） セキュリティ情報の収集

情報セキュリティ管理者は、セキュリティホール等の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情報を共有しなければならない。

９　運用による安全管理措置

（１） 情報システムの監視

情報セキュリティ管理者は、情報システムの運用にあたっては、常に情報システムを監視するとともに情報セキュリティ障害に対して注意を払わなければならない。

（２） 情報セキュリティポリシーの遵守状況の確認

情報セキュリティ管理者は、所管の範囲において情報セキュリティポリシー及びこれに基づく文書の遵守状況について常に確認を行い、問題を認めた場合には速やかに情報セキュリティ管理者に報告しなければならない。情報セキュリティ管理者は、発生した問題について、適切かつ速やかに対処しなければならない。

（３） 職員等の報告義務

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、直ちに情報セキュリティ管理者及び情報基盤管理者に報告を行わなければならない。

（４） 情報セキュリティ障害への対応

① 復旧及び障害拡大の防止措置

ア．情報セキュリティ管理者は、情報セキュリティ障害が発生した場合に、情報基盤管理者と連係し、速やかに復旧のための措置を講じなければならない。

イ．情報セキュリティ管理者は、情報セキュリティ障害の拡大を防ぐために、情報基盤管理者と連係し、情報システムの停止を含め、必要な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、情報セキュリティ障害の原因となる行為が不正アクセスの可能性がある場合には、情報基盤管理者と連携し、行為の記録の保存に努めなければならない。

エ．情報セキュリティ管理者は、情報セキュリティ障害が重大な影響を及ぼす恐れがある場合には、速やかに統括情報セキュリティ責任者に報告し、必要な指示を仰がなければならない。

② 再発防止の措置

情報セキュリティ管理者は、情報基盤管理者と連係し、必要な再発防止の措置を講じるとともに、その結果を情報セキュリティ責任者に報告しなければならない。特に重大な障害にあっては、統括情報セキュリティ責任者及び最高情報セキュリティ責任者に報告しなければならない。

１０　情報セキュリティ実施手順の策定

情報セキュリティ統括責任者は、情報セキュリティポリシーに基づき、情報セキュリティ対策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しなければならない。

１１　取扱規程等

情報セキュリティ管理者、情報基盤管理者は、必要に応じて、所管する情報資産について、藤枝市セキュリティポリシー及び藤枝市情報セキュリティ実施手順を補完する取扱規定等を策定するものとする。

１２　評価・見直し等

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は、所管する部署の情報セキュリティが確保されていることを確認するため、自主点検を行い、必要に応じ改善措置を講じなければならない。

統括情報セキュリティ責任者は、評価及び見直しが必要となる事象が発生した場合には、「藤枝市地域ＩＴ推進委員会」に諮り必要な見直しを行い、適切な情報セキュリティポリシーの維持及び運用に努めなければならない。