福山市情報セキュリティポリシー

２０２３年（令和５年）４月１日（第１７版）

２００４年（平成１６年）８月２日制定

福　　山　　市

福山市情報セキュリティポリシー

序章　福山市情報セキュリティポリシーの位置づけ

福山市情報セキュリティポリシーは，福山市が保有する情報資産（注１）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，本市の情報セキュリティ対策の頂点に位置するものである。

本セキュリティポリシーは，本市の情報資産を取扱うすべての職員等（注２）が遵守すべき規範であり，一定の普遍性を備えた「情報セキュリティ基本方針」と情報処理技術や通信技術の進展に伴う状況変化に適切に対応する「情報セキュリティ対策基準」から構成される。

また，本セキュリティポリシーに基づき，具体的な情報セキュリティ対策のマニュアルとしての「情報セキュリティ実施手順」を策定し，図１の体系で総合的な情報セキュリティ対策を実施する。職員等は情報セキュリティ対策の重要性を認識し，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義務を負うものである。

（注１）情報資産：職員等が職務上作成，又は取得したすべての情報（記録媒体に記録された情報，紙等に出力された情報，作成途中のファイル並びに一時的に作成するファイルを含む。）

（注２）職員等　：本市が保有する情報システム，情報資産に関わる一般職の職員及び特別職の職員並びに本市の情報資産を取扱うすべての者（外部委託事業者は除く。）

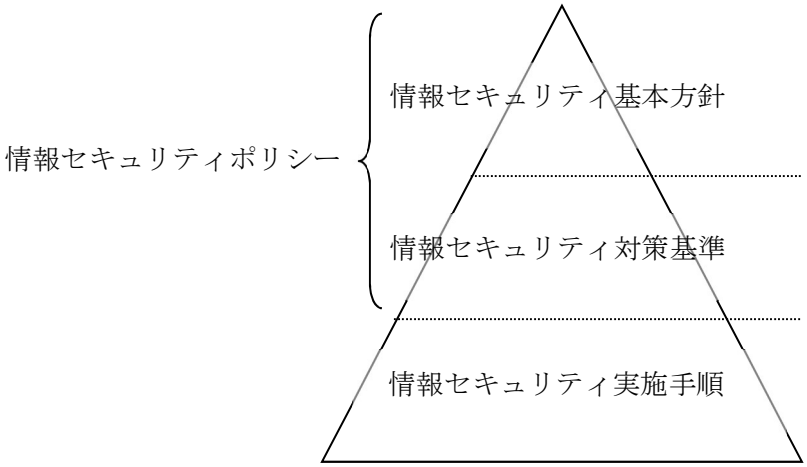


図１　情報セキュリティ対策体系図

・情報セキュリティ基本方針：すべての情報セキュリティ対策の基本となる考え方を示したもの。

・情報セキュリティ対策基準：情報セキュリティ対策として遵守すべき行為及び判断の基準を示したもの。

・情報セキュリティ実施手順：情報セキュリティ対策の具体的な実施手順や取扱い方法について定めたもの。

第１章　情報セキュリティ基本方針

第１　目的

本市が取扱う情報資産には，個人情報や行政運営上の情報等が漏えい，改ざん及び破壊等により，個人や組織に重大な被害を引き起こすものがある。これら情報資産を災害，事故，人的脅威等から守ることは，市民のプライバシー及び財産等の保護，また，正確，安全かつ継続的に行政サービスを行う上でも必要不可欠である。

このため，本市の情報資産について，次の情報セキュリティを確保する必要がある。

１　機密性

許可された者のみが，情報にアクセスできることを確実にすること。

２　完全性

情報及び処理方法の正確さと完全さ（抜け，漏れのないこと）を確保すること。

３　可用性

必要な時に情報及び関連する資産にアクセスできること。

本方針は，本市の取扱う情報資産の機密性，完全性及び可用性を維持するため，情報資産及びそれを取扱う情報システムに対するすべての情報セキュリティ対策の基本となるものである。

第２　定義

この方針において，各号に掲げる用語の意義は，当該各号に定めるところによる。

１　ネットワーク

コンピュータを相互に接続するための通信回線網及びその構成機器（ハードウェア及びソフトウェア）で構成され，処理を行う仕組みをいう。

２　情報システム

情報処理又は通信を行うコンピュータ（ハードウェア及びソフトウェア），記録媒体及びネットワークをいう。

３　情報資産

職員等が職務上作成，又は取得したすべての情報（記録媒体に記録された情報，紙等に出力された情報，作成途中のファイル並びに一時的に作成するファイルを含む。）をいう。

４　記録媒体

ＣＤ－Ｒ，ＤＶＤ－Ｒ，ＵＳＢメモリ，ＨＤＤ，ＳＳＤ等の情報を記録するための装置をいう。

５　アクセス

情報システムを通じて情報資産の参照，更新を行うことをいう。

６　職員等

本市が保有する情報システム，情報資産に関わる一般職の職員及び特別職の職員並びに本市の情報資産を取扱うすべての者（外部委託事業者は除く。）をいう。

７　個人情報

個人情報の保護に関する法律（平成１５年法律第５７号）第２条第１項に規定する「個人情報」（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２７号。以下「番号法」という。）第２条第８項に規定する「特定個人情報」を含む）及び死者に関する情報であって個人情報の保護に関する法律第２条第１項各号のいずれかに該当するものをいう。

８　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。

９　約款による外部サービス

約款への同意又は簡易な登録等により，利用可能となるインターネット上で提供されるサービスをいう。

第３　対象機関等

本方針の対象となる機関は，次のとおりとする。

１　市長，教育委員会，選挙管理委員会，監査委員，公平委員会，農業委員会，固定資産評価審査委員会，議会，上下水道事業管理者，病院事業管理者

２　１の機関が管理運用する情報システムを利用する機関（福山地区消防組合，外郭団体等）

第４　対象範囲

本方針の対象範囲は，対象機関において保有する情報資産及び情報資産を取扱う情報システムとする。

なお，特殊性を持つシステムにおいては，本セキュリティポリシーに加え，別途セキュリティポリシーを定めることができる。ただし，本セキュリティポリシーの水準を下回ってはならない。

第５　職員等の遵守義務

職員等は，情報セキュリティの重要性を認識し，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。

第６　管理体制

本市の情報資産について，情報セキュリティ対策を適切に推進，管理するための体制を確立する。

第７　情報資産への脅威

情報セキュリティ対策を講じるに当たって，情報資産に対する次の脅威に十分に考慮しなければならない。

１　人的脅威

誤操作，持ち出し，不正行為，パスワードの不適切管理等

２　物理的脅威

侵入，破壊，故障，停電，災害等

３　技術的脅威

不正アクセス，盗聴，コンピュータウイルス，改ざん，消去等

第８　情報資産の分類

情報資産はその重要性に基づいて分類し，それらの脅威や脆弱性に応じた情報セキュリティ対策を施し管理する。

第９　情報セキュリティ対策

情報資産への脅威・脆弱性を十分に考慮し，次の情報セキュリティ対策を講じなければならない。

なお，遵守すべき行為及び判断の基準は，情報セキュリティ対策基準において示す。

１　人的セキュリティ対策

情報資産を取扱うに当たって，職員等の権限や責任及び遵守すべき事項を定め，それらが遵守されるように十分な教育，啓発及び訓練を行うこと。

２　物理的セキュリティ対策

情報資産の取扱い場所及び情報システムの設置場所への不正な立ち入りや機器の破損等を防ぐために物理的な対策を講じること。

３　技術的セキュリティ対策

情報資産への不正アクセス等を防ぐために，アクセス制御やコンピュータウイルス対策等の技術的な対策を講じること。

４　運用面のセキュリティ対策

情報セキュリティポリシーを確実に運用していくために，侵害時及び緊急時の対策等の運用面での対策を講じること。

第１０　情報セキュリティ対策基準

情報セキュリティ対策として遵守すべき行為及び判断の基準として，「情報セキュリティ対策基準」を策定する。

第１１　情報セキュリティ実施手順

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，具体的な取扱方法について「情報セキュリティ実施手順」を策定する。

第１２　点検・監査

情報セキュリティポリシーの遵守状況について，点検及び監査を定期的かつ継続的に実施する。

第１３　評価・見直し

情報セキュリティ対策の点検・監査の結果及び情報セキュリティを取り巻く環境の変化等を踏まえ，適宜，情報セキュリティポリシーの評価及び見直しを実施する。

第１４　違反に対する対応

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に違反した者に対しては，厳格な対応を行う。

第２章　情報セキュリティ対策基準

第１　目的

この基準は，情報セキュリティ基本方針に基づき，情報セキュリティ対策を実施するに当たり，遵守すべき行為及び判断の基準を定めることを目的とする。

第２　定義

この基準において使用する用語の意義は，当該各号に定めるところによるほか，情報セキュリティ基本方針の定めるところによる。

１　パスワード

情報システムや特定のデータにアクセスしようとする際に，正当な利用者であることを識別・認証するための文字列をいう。

２　不正アクセス

コンピュータやネットワークに正規の手続を経ずに侵入する行為をいう。

３　コンピュータウイルス（以下「ウイルス」という。）

コンピュータに侵入し，情報システムの正常な動作を意図的に妨げるプログラム等をいう。

４　サーバ

ネットワーク上でデータの保有・共有，印字出力，通信制御等のサービスを提供するコンピュータをいう。

５　パッチ

アプリケーションソフト等に存在する不備が発覚した際に配布される修正プログラムをいう。

６　攻撃

ネットワークやコンピュータに不正に侵入する，又は負荷をかける等して業務を妨害することをいう。主な攻撃としてDoS攻撃などがある。

７　ファイアウォール

組織内のコンピュータネットワークへ外部から侵入されることを防ぐシステム又はそのようなシステムが組み込まれたコンピュータをいう。

第３　管理体制

情報セキュリティ対策の推進体制は，付録「福山市情報セキュリティ管理運用体制」（以下「管理運用体制」という。）のとおりとし，それぞれの役割については次のとおりとする。

１　福山市デジタル化推進委員会

福山市デジタル化推進委員会は，福山市デジタル化推進委員会設置要綱第２条第５号に基づいて，情報セキュリティ対策を組織横断的に実施するため，本市の情報セキュリティ対策に関する重要事項を審議する。

(1)　情報セキュリティ対策の実施計画の立案，対策の見直し

(2)　情報セキュリティ対策遵守状況の確認

(3)　教育，研修及び訓練に関すること。

(4)　情報セキュリティポリシーの見直しに関すること。

(5)　上記のほか，情報セキュリティ対策の実施に係る重要事項

2　福山市情報セキュリティ統括責任者

(1) 情報セキュリティに関する決定権限及び責任を有する者として，福山市情報セキュリティ統括責任者を置き，総務局長の職にある者をもってこれに充てる。

(2) 福山市情報セキュリティ統括責任者は，次に掲げる事項を統括する。

ア　情報セキュリティ対策の総合的な企画及び実施に関すること。

イ　情報セキュリティ監査に関すること。

3　局情報セキュリティ統括責任者

(1)「情報セキュリティ基本方針」第３に規定する対象機関における組織にあって局を所管する局長を局情報セキュリティ統括責任者とする。

(2) 局情報セキュリティ統括責任者は，局における情報セキュリティに関する統括的な権限及び責任を有する。

4　統括情報セキュリティ管理責任者

(1) 全庁の情報セキュリティ対策を統括する責任者として，統括情報セキュリティ管理責任者を置き，総務部参与（デジタル化担当）の職にある者をもってこれに充てる。

(2) 統括情報セキュリティ管理責任者は，次に掲げる職務を行う。

ア　全庁の情報セキュリティ対策の統括管理に関すること。

イ　統括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意見の聴取，指導及び助言を行うこと。

ウ　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侵害のおそれがある場合には，福山市情報セキュリティ統括責任者に報告を行うとともに，その指示に従い，必要かつ十分な措置を講じる。また，福山市情報セキュリティ統括責任者が不在の場合には，自らの判断に基づき，必要かつ十分な措置を講じる。

5　情報セキュリティ管理責任者

(1)「情報セキュリティ基本方針」第３に規定する対象機関における組織にあって部及び部に相当するもの（以下「部等」という。）を所管する部長等（以下「部長等」という。）を情報セキュリティ管理責任者とする。

(2) 情報セキュリティ管理責任者は，部等における情報セキュリティに関する統括的な権限及び責任を有する。

(3) 情報セキュリティ管理責任者は，部等において所管する情報システムの連絡体制の構築，部等に所属する職員の情報セキュリティポリシーに関する意見の集約並びに部等に所属する職員に対する情報セキュリティポリシーの遵守に関する教育，訓練，助言及び指示を行う。

6　統括情報セキュリティ管理者

(1) 全庁の情報セキュリティ対策に係る事務を統括する責任者として，統括情報セキュリティ管理者を置き，ＩＣＴ推進課長の職にある者をもってこれに充てる。

(2) 統括情報セキュリティ管理者は，次に掲げる職務を行う。

ア　全庁の情報セキュリティ対策の実施に関すること。

イ　全庁的ネットワーク及び全庁的情報システムにおける情報セキュリティに関すること。

ウ　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意見の聴取，指導及び助言を行うこと。

エ　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侵害のおそれがある場合には，統括情報セキュリティ管理責任者へ速やかに報告するとともに，その指示に従い，必要な措置を行う。

7　情報セキュリティ管理者

(1)「情報セキュリティ基本方針」第３に規定する対象機関における組織にあって課及び課に相当するもの（以下「課等」という。）を所管する課長等（以下「課長等」という。）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，次に掲げる事項について権限及び責任を有する。

ア　課等における情報セキュリティポリシーの遵守に関すること。

イ　所管する情報システムの開発，運用及び情報セキュリティに関すること。

ウ　情報資産の分類及び管理に関すること。

エ　情報セキュリティ対策の実施状況の把握，分析及び報告に関すること。

オ　情報セキュリティ実施手順の作成に関すること。

カ　情報セキュリティ管理者は，その所掌する課等において，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侵害のおそれがある場合には，統括情報セキュリティ管理者，情報セキュリティ管理責任者へ速やかに報告を行い，指示を仰ぐ。

(3) 情報セキュリティ管理者は，デジタル化推進員（福山市デジタル化推進員設置要綱（２０２２年6月２３日制定)による）と協力して，課等における具体的な情報セキュリティ活動を行う。

8　兼務の禁止

(1) 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。

(2) 監査を受ける者とその監査を実施する者は，やむを得ない場合を除き，同じ者が兼務してはならない。

9　情報セキュリティに関する統一的な窓口の設置

(1) 福山市情報セキュリティ統括責任者は，全庁の情報セキュリティの統一的な窓口を設け，これをＩＣＴ推進課に置く。

(2) 情報セキュリティインシデントが発生した場合は，その状況を把握・分析し，福山市情報セキュリティ統括責任者への報告等を行う。

(3) 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等との情報共有を行う。

第４　情報資産の分類と管理

１　情報資産は，情報セキュリティ管理者が管理責任を負う。

２　情報資産の重要性分類

情報セキュリティ管理者は，情報資産を次に掲げる重要性分類に基づき分類する。

(1) 重要性分類Ⅰ

ア　個人情報

イ　法令又は条例の定めにより守秘義務を課されている情報

ウ　法人その他団体又は事業を営む個人の事業に関する情報で，公開することにより当該団体の利益を害するおそれのある情報

エ　情報システムに関する認証情報及びシステム設定情報

(2) 重要性分類Ⅱ

漏えい，滅失又はき損等した場合に，行政に対する信頼，本市の事務事業の円滑な執行を妨げるおそれのある情報をいう。

(3) 重要性分類Ⅲ

上記以外の情報をいう。

３　情報資産の分類に関する表示

情報セキュリティ管理者は，情報資産について，第三者が重要性の識別を容易に認識できないよう，適切な管理を行う。

４　情報資産の管理

(1) 情報資産の管理及び取扱

情報資産は重要性分類に従いアクセス権限を定めなければならない。また，重要性分類Ⅰの情報資産については，暗号化を施す等適切に管理しなければならない。

なお，暗号化を施す場合は，暗号化に用いた暗号鍵及び暗号化された当該情報資産は，別々に適切な管理を行わなければならない。また，保存期間を経過した情報資産はできるだけ速やかに復元できない手段で削除又は廃棄する。

(2) 記録媒体の管理

ア　記録媒体は，消失，劣化，盗難，情報漏えい等に備え，施錠可能な場所に保管するとともに，可能な限り耐火，耐熱，防湿，防磁の対策を講じなければならない。

イ　記録媒体に納められた情報資産は，必要に応じて，別の記録媒体に複製する。

ウ　情報資産を記録媒体に記録する場合は，必要に応じて，書込禁止措置を行う。

(3) 記録媒体の廃棄

ア　記録媒体が不要となった場合は，いかなる方法によっても復元できないように，次の処理を施した上で，速やかに廃棄しなければならない。

なお，廃棄するまでに期間を要する場合は施錠可能な場所に保管しなければならない。

(ｱ) 指定ソフトによる消去

(ｲ) 物理的破壊

(ｳ) その他統括情報セキュリティ管理者が認めた方法

イ　重要性分類Ⅰ及びⅡの情報資産を記録した記録媒体の廃棄は，情報セキュリティ管理者の許可を得ることとし，行った処理について，日時，処理担当者，処理内容等を管理台帳に記録する等適切な処理を行わなければならない。

第５　人的セキュリティ対策

１　役割と責任

(1) 職員等は，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並びに関係規程に定める事項を遵守しなければならない。

(2) 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について，情報セキュリティ管理者に相談し，指示を受けなければならない。

(3) 職員等は，情報資産について，知り得た情報を漏えいしてはならない。その職を退いた後においても同様とする。

２　教育及び訓練

(1) 福山市情報セキュリティ統括責任者は，職員等に対して情報セキュリティポリシーを理解し実践するための教育・訓練を計画的に実施しなければならない。

(2) 職員等は，定められた研修及び訓練に参加し，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理解し，情報セキュリティ上の問題を生じさせないようにしなければならない。

３　情報資産，情報システム及びネットワークの利用

(1) 業務目的以外の使用の禁止

情報資産，情報システム及びネットワークは，業務目的以外で使用してはならない。

(2) 情報システム，情報資産の持出し及び持込みの禁止

職員等は，情報システム，情報資産を取扱う場合，次の行為を行ってはならない。

ア　情報セキュリティ管理者の許可なく庁外へ持ち出すこと。

イ　情報セキュリティ管理者の許可なく，情報資産が記録できる個人等の所有する機器を職場へ持込み使用すること。

(3) 無許可ソフトウェア導入の禁止

職員等は，コンピュータに許可なくソフトウェアを導入してはならない。やむを得ずコンピュータにソフトウェアを導入する場合には，情報セキュリティ管理者の許可を得た上で行うこと。また，全庁的ネットワークと接続しているコンピュータに導入する場合は，統括情報セキュリティ管理者の許可を得ること。

(4) 機器構成の変更の禁止

職員等は，コンピュータ及びネットワーク機器の改造，増設，設定変更等を情報セキュリティ管理者の許可なく行ってはならない。また，全庁的ネットワークと接続しているコンピュータに導入する場合は，統括情報セキュリティ管理者の許可を得る

こと。

4　ＩＤ・パスワード等認証情報の管理

(1) パスワードの照会等には一切応じてはならない。

(2) パスワードは他人に知られない措置を講じる。メモに記す場合，内容が他者に漏れないよう厳格に管理する。また，端末にはパスワードを記憶させてはならない。

(3) 他人のユーザＩＤ，パスワード等を利用してはならない。

(4) ユーザ認証をしたまま，端末を離れてはならない。端末を離れる際には，ユーザ認証の解除を行うこと。

(5) パスワード及びその構成は，容易に推測されてはならない。

(6) 利用者側でパスワードを変更できる情報システムは，パスワードを定期的に変更し，古いパスワードの再利用をしてはならない。管理者用パスワードは適宜変更すること。

(7) 複数の情報システムを扱う職員等は，職員認証システムを利用して認証する情報システムを除き，パスワードをシステム間で共有しないこと。

(8) 仮のパスワードは，最初のユーザ認証の時点で変更すること。

(9) 情報セキュリティ管理者は，パスワードが漏えい，又は漏えいした恐れがある場合には，速やかに当該パスワードの使用を停止しなければならない。

5　情報セキュリティインシデントに対する対応

職員等は，情報セキュリティインシデントを発見した場合，また，住民からの報告や連絡があった場合には，情報セキュリティ管理者に報告する等適切に対応しなければならない。

第６　物理的セキュリティ対策

1　設置要件

サーバやネットワーク機器等の重要な機器の導入及び運用に当たっては，次に掲げる要件を満たす措置を講じなければならない。

(1) 地震，火災，水害，埃等の影響を可能な限り排除した場所に設置し，耐震設備，空調設備及び消火設備を整備すること。

(2) 外部から容易に侵入することができない場所に設置すること。

(3) 高い可用性が求められる機器の冗長化（サーバの停止や故障等に備えてシステムを継続して運用できる構成）を行う等，障害発生時に情報システムの運用に支障がないようにすること。

(4) 庁舎外部に設置するコンピュータやネットワーク機器についても，庁内の設置場所要件に準じて設置すること。

2　入退室管理

(1) 重要性分類Ⅰ及びⅡの情報資産の取扱い場所，保管場所及びそれを取扱う情報システムの設置場所のうち特に重要性の高い場所は，鍵等により入室が制限できる場所とする。入室に当たっては，事前に所属，名前，用務を確認し，許可した者以外入

らないよう入退室の管理を実施しなければならない。また，入退室の記録を管理簿等に記録しなければならない。

(2) 職員等が情報資産を取扱う場所を不在にする場合は，施錠する等侵入に対する対策を実施しなければならない。

3　機器等の搬出・搬入

機器等の搬出・搬入による情報資産の保管場所及び情報システムの設置場所のうち特に重要性の高い場所への入退室については，職員が立ち会い確認する等必要な措置を講じなければならない。

4　電源

サーバやネットワーク機器等の電源については，十分な容量及び予備電源を確保しなければならない。

5　回線及び配線

(1) 重要な情報資産をネットワークにおいて取扱う場合は，専用線又は必要なセキュリティ水準を検討の上，統括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) 配線については，傍受，損傷等を防ぐための対策を講じなければならない。

(3) 無線ネットワークを使用する場合は，通信データの暗号化及び接続可能機器を限定する等，情報漏えい防止対策を講じなければならない。

6　機器の保守

(1) サーバやネットワーク機器は，安定稼働のため，保守を実施しなければならない。

(2) サーバやネットワーク機器の保守の際には，情報漏えい等を防止する対策を実施しなければならない。

7　機器の廃棄

コンピュータ等の情報機器を廃棄する場合は，第４の４－(3)「記録媒体の廃棄」を準用する等，完全にデータが消去され，復元されることのないよう情報漏えいを防止する対策を実施しなければならない。

第７　技術的セキュリティ対策

1　コンピュータ及びネットワークの管理

(1) 重要な情報資産へのアクセス記録及び情報セキュリティの確保に必要な記録を取得し，一定期間保存しなければならない。また，定期的にそれらを分析しなければならない。

(2) ネットワーク構成図，システム仕様書等については，記録媒体の形態に関わりなく適切に保管しなければならない。

(3) 専用線の利用や暗号化等の情報セキュリティ対策を可能な限り実施しなければならない。

(4) 高い可用性が求められる情報システムでは，システムの二重化等，緊急時に直ちに対処できるような対策を施されなければならない。

(5) アクセス権限がない職員等が，所管する情報システムにアクセスすることが不可

能となるように，システム上制限しなければならない。

(6) 職員等が送信等により情報資産を容易に外部に持ち出すことができないように，システム上制限しなければならない。

(7) 汎用受付システム等，外部の者が利用できる情報システムにおいては，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ける等，情報セキュリティ対策について特に強固な対策をとらなければならない。

(8) インターネットにより情報を公開・提供等する場合は，改ざん，消去，踏み台，DoS 攻撃等を防止するための適切な管理を行わなければならない。

(9) 情報システムの安定した運用を確保するため，必要に応じてシステム監視対策を実施しなければならない。

2　アクセス制御

(1) 利用者登録

ア　ネットワーク及び情報システムのアクセス権限は，必要最小限の者に与え，厳重に管理しなければならない。

イ　ユーザＩＤの登録，変更，抹消等の管理方法を定めなければならない。

(2) 管理者権限は必要最小限の者に与え，厳重に管理しなければならない。

(3) 外部ネットワークとの接続

ア　不正なアクセスを防止するため，ネットワーク経路については，適切な制御を実施しなければならない。

イ　外部ネットワークとの接続に際しては，ネットワークの構成，セキュリティレベル等を詳細に検討し，情報システム及び情報資産に影響が生じないと明確に確認した上で，統括情報セキュリティ管理者の許可を得て接続しなければならない。

ウ　接続した外部ネットワークのセキュリティに問題があると認められた場合には，統括情報セキュリティ管理者の判断に従い，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。

エ　外部ネットワークの瑕疵等により本市の情報資産が漏えい，改ざん，破壊等，本市の業務に影響を及ぼす問題が発生した場合に対処するため，外部ネットワークの管理者との間で障害発生時の責任，対処方法等を明確にしておかなければならない。

オ　外部からの遠隔操作により，サーバやネットワーク機器の監視及び保守を行うことを目的として外部ネットワークに接続する場合も上記を適用する。

3　ネットワーク及び情報システムの開発，導入，保守等

(1) 調達

ア　統括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調達に関する手順等を明らかにしなければならない。

イ　情報セキュリティ管理者は，情報システムの調達に当たり，調達仕様書を公開する場合は，情報セキュリティ確保の上で問題のないようにしなければならない。

ウ　情報セキュリティ管理者は，機器及びソフトウェアを導入等する場合，当該製品が情報セキュリティ上問題にならないか確認しなければならない。

(2) 開発，導入及び保守

統括情報セキュリティ管理者及び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，導入及び保守時の事故及び不正行為対策のため，次の事項を遵守しなければならない。

ア　責任者及び監督者を選任し，作業への立会い，連絡調整等必要な事項を行わせること。

イ　要員体制を確保し，明確化すること。

ウ　開発，導入及び保守時の事故・不正行為に係るリスク分析を行うこと。

エ　開発及び改造に当たっては，可能な限り開発環境と本運用環境を分離すること。

オ　開発及び保守の際のアクセス制限を行うこと。

カ　機器搬出入の際の許可及び確認を行うこと。

キ　委託業者から開発・保守記録の提出を受けること。

ク　マニュアル等を定められた場所へ保管すること。

ケ　開発・保守を行った者の不要となったユーザＩＤ，パスワード等の認証情報を速やかに抹消すること。

コ　ネットワークならびに情報システムを追加，変更等した場合は，変更内容を履歴として記録し，保存すること。

サ　守秘義務，再委託に関する事項を契約書等へ明記すること。

(3) 機器の修理及び廃棄

第６の６「機器の保守」及び７「機器の廃棄」に従うこと。

４　ウイルス対策

(1) 外部から情報又はソフトウェアを取り入れる際には，サーバ側，端末側においてウイルスチェックをしなければならない。また，必要に応じてファイアウォール段階でのチェックを行うこと。

(2) 外部へ情報を送信する際は，事前にウイルスチェックを行い，他の団体等へウイルスが拡散することを未然に防止しなければならない。

(3) 統括情報セキュリティ管理者は，次の事項を実施しなければならない。

ア　全庁のウイルス対策の方針を定めること。

イ　全庁のウイルス対策が適切に行われているかどうかを確認すること。

ウ　常にウイルスに関する情報収集に努め，全庁に対して注意喚起を行うこと。

(4) 情報セキュリティ管理者は，次の事項を実施しなければならない。

ア　ウイルスに関する情報収集に努めること。

イ　ウイルス情報について職員等に対する注意喚起を行うこと。

ウ　ウイルス対策が適切に行われているかどうかを確認すること。

(5) 職員等は，次の事項を遵守しなければならない。

ア　外部からデータ又はソフトウェアを取り入れる場合は，必ずウイルスチェックを行うこと。また，出所不明のソフトウェア等は使用しないこと。

イ　添付ファイルのあるメールを受信する場合は，必要に応じてウイルスチェックを行うこと。

ウ　ウイルスを発見した場合は，ネットワークから切り離し，情報セキュリティ管理者及び統括情報セキュリティ管理者に報告し，指示を受けなければならない。

エ　不審なメール及び添付ファイルは速やかに削除すること。

オ　統括情報セキュリティ管理者及び情報セキュリティ管理者が提供するウイルス情報を常に確認すること。

5　不正アクセス対策

(1) 情報セキュリティ管理者は，ソフトウェアのパッチやバージョン情報を収集し，常に最適となるようにしなければならない。

(2) 攻撃を受けることが明確な場合には，統括情報セキュリティ管理者及び情報セキュリティ管理者は情報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，関係機関との連絡を密にして情報の収集に努めなければならない。

(3) 攻撃を受け，当該攻撃が「不正アクセス行為の禁止等に関する法律」違反等犯罪の可能性がある場合には，統括情報セキュリティ管理者及び情報セキュリティ管理者は，記録の保存に努めるとともに，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) 職員等による不正アクセスがあった場合，情報セキュリティ管理者は，適切な処置を行い，管理運用体制に基づき報告しなければならない。

(5) 不正アクセスを行った職員等は，地方公務員法による懲戒等の処分及び関係法令に基づき刑事告発の対象とする。

6　セキュリティ情報の収集

セキュリティ情報の収集はこれを絶えず行い，常に最新の情報を保持しなければならない。また，必要に応じて対策を実施し，対応方法について職員等に周知しなければならない。

第８　運用面のセキュリティ対策

1　運用管理における留意点

情報セキュリティ管理者は，セキュリティ上必要があると認められる場合には，アクセス記録，メール等の情報を閲覧することができる。この場合，情報セキュリティ管理者は，統括情報セキュリティ管理者と閲覧範囲等を協議の上，両者立会いのもと閲覧する。ただし，法令で定められた個人情報の保護に関係する情報の閲覧に関しては，当該法令に定められた手続に従うこと。

2　侵害時及び障害時に備えた対応策

(1) 情報セキュリティ管理者は，災害や障害時を想定した緊急時対応計画を作成して，定期的に緊急時対応の訓練等を実施すること。

(2) 情報セキュリティ管理者は，所管する情報システムに稼働不能となるような重大な障害，不正アクセス等の侵害及び市民に影響を及ぼす事件など（以下「障害等」という。）が発生した場合，障害等の内容，被害，影響範囲，原因について速やかに管理運用体制に基づき，報告しなければならない。

(3) 情報セキュリティ管理者は，発生した障害の原因が不正アクセス等にある場合，裏付ける行為をできる限り保存しなければならない。

(4) 情報セキュリティ管理者は，各管理者と連携し，情報システムの復旧及び再発防止策を実施しなければならない。

(5) 情報セキュリティ管理者は，対応結果を管理運用体制に基づき，報告しなければならない。

3　外部委託契約

(1) 情報セキュリティ管理者は，情報システムの開発又は運用等を外部事業者に委託する場合，プライバシーマーク，ＩＳＭＳ（情報セキュリティマネジメントシステム）等の各種認証の取得状況等，選定対象事業者の情報セキュリティに対する意識，実施状況等を確認しなければならない。

(2) 番号法に規定する個人番号利用事務等を委託する場合には，委託先において，番号法に基づき本市が果たすべき安全管理措置と同等の措置が講じられるか否かについて，あらかじめ確認すること。

(3) 委託契約書には，次の事項を明記すること。

ア　受託者の守秘義務に関する事項

イ　再委託の禁止又は制限並びに権利義務譲渡の禁止に関する事項

ウ　データの契約目的外の使用及び第三者への提供の禁止に関する事項

エ　データの複写及び複製の禁止に関する事項

オ　データの返還又は処分に関する事項

カ　委託業務従事者に対する教育の実施に関する事項

キ　入出力帳票等及びシステム仕様書等の保護管理に関する事項

ク　監視に係る措置，検査・監査に応じる義務並びに電算処理の立会い又は監督に関する事項

ケ　システム管理記録・障害記録の提出・管理に関する事項

コ　事故報告義務等緊急時の措置に関する事項

サ　納品物の検査の実施に関する事項

シ　所有権・著作権に関する事項

ス　事業所内からの個人情報の持出しの禁止

セ　漏えい事案等が発生した場合の委託先の責任

ソ　従業者に対する監督・教育，契約内容の遵守状況の報告

タ　必要があると認める場合の委託先に対する実地調査の実施

チ　番号法に規定する個人番号利用事務等を委託する場合は，「特定個人情報を取り

扱う従業者の明確化」に関する事項

ツ　前各項目に掲げる委託契約書に規定した事項に違反した場合における契約解除等の措置及び損害賠償に関する事項

テ　その他必要な事項

4　約款による外部サービスの利用

情報セキュリティ管理者は，業務の円滑な運用に資すると判断し，約款による外部サービスを利用する場合は，次の事項を遵守しなければならない。

(1) 原則，重要性分類Ⅰ，Ⅱの情報を取扱ってはならない。

(2) 約款を十分に理解し，提供されるサービスの機能，設定等を把握し，定期的に内容を確認する。

第９　文書管理

情報セキュリティに関する文書類は，次の事項を遵守して管理しなければならない。

1　表現が分かり易く，十分検討されたものであること。

2　必要に応じて文書の見直しを行い，文書の変更識別及び現在の改訂版の識別を確実にすること。

3　最新版が，必要な時に必要なところで使用できる状態にあることを確実にすること。

4　廃棄文書は速やかに，かつ，確実に廃棄すること。

第１０　法令等遵守

職員等が情報資産の取扱いに当たって遵守すべき主な法令等は，次のとおりである。

また，これら法令等のほか，各種ガイドライン等，情報資産の適切な管理を義務づけた規程も遵守しなければならない。

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　番号法

5　サイバーセキュリティ基本法（平成２８ 年法律第３１ 号）

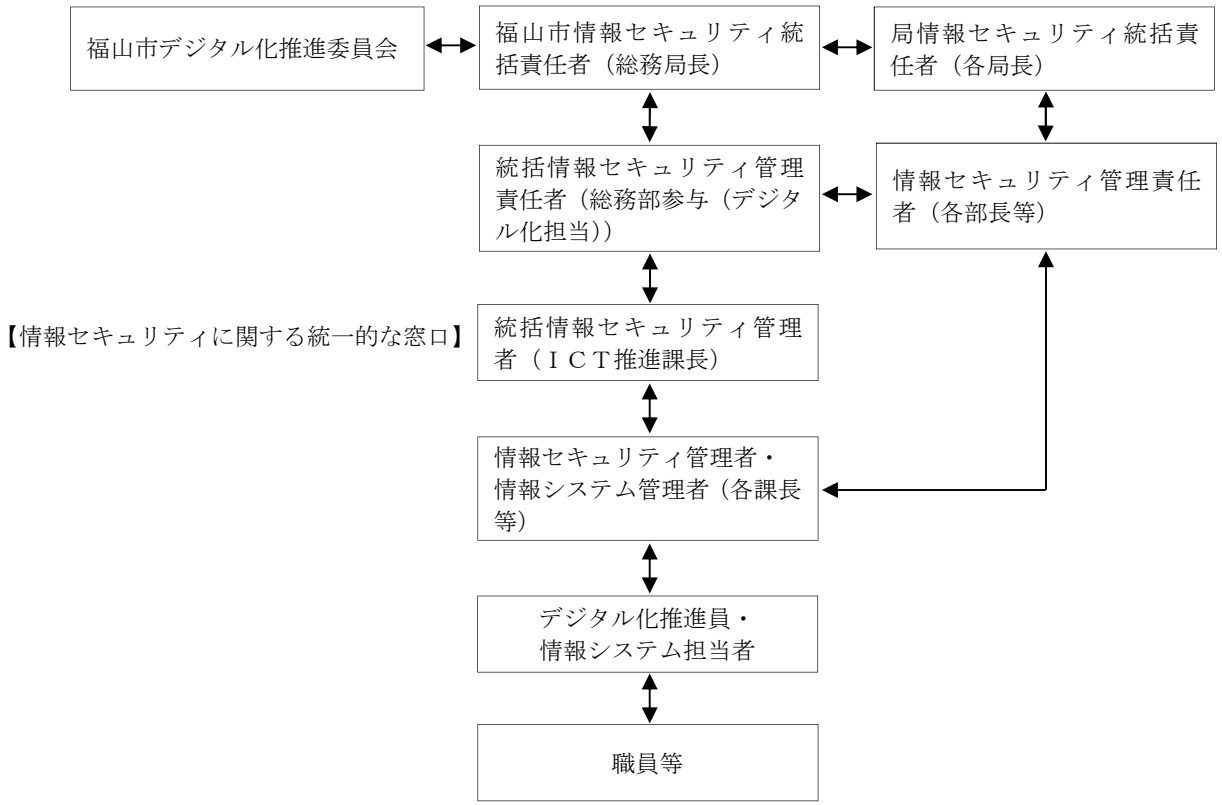
6　個人情報の保護に関する法律

7　福山市情報公開条例（平成１４年条例第２号）

8　特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編）

【付録】

福山市情報セキュリティ管理運用体制図



◀―▶ は「報告」・「指示」の関係を表す。

〇福山市デジタル化推進委員会構成員

・委員長：総務局担当副市長

・副委員長：他の副市長

・委員：デジタル化推進委員会設置要綱別表１に掲げる者