春日井市情報セキュリティポリシー

平成１５年　７月　７日

春日井市情報セキュリティポリシー	制定：平成15年７月７日	
改訂歴表	改訂：平成29年４月１日	版数：８

改　訂　歴　表

制定・改訂			改　訂　内　容
	改正箇所	年月日	
1	全	平成15年７月７日	新規制定
2	第２章第１項第５号イ	平成16年４月１日	一部改訂
3	第２章第１項第６号 第２章第４項第２号イ 第２章第９項第５号	平成17年７月１日	一部改訂
4	第２章第１項第１号イ	平成19年４月１日	一部改訂
5	第２章第１項第３号イ	平成21年４月１日	一部改訂
6	第２章第３項第６号 第２章第７項第１号 第２章第７項第２号 第２章第７項第３号	平成26年４月１日	一部改訂
7	第１章第２項第６号 第１章第８項 第１章第15項 第２章第１項第１号 第２章第１項第７号 第２章第２項第１号 第２章第２項第２号ウ 第２章第３項第２号オ 第２章第３項第５号 第２章第４項第１号オ 第２章第４項第１号カ 第２章第５項第１号ア 第２章第５項第１号オ 第２章第５項第１号コ	平成27年10月９日	一部改訂

	第２章第５項第１号サ 第２章第５項第２号 第２章第５項第３号 第２章第５項第５号 第２章第６項第３号ア 第２章第８項		
8	第２章第１項第１号ウ 第２章第１項第２号エ 第２章第１項第３号 第２章第１項第４号 第２章第１項第６号 第２章第１項第７号 第２章第１項第８号 第２章第２項第２号イ 第２章第３項第１号イ 第２章第３項第１号ウ 第２章第３項第２号ウ 第２章第３項第２号エ 第２章第３項第６号 第２章第４項第１号カ 第２章第４項第２号ウ 第２章第４項第２号オ 第２章第５項第１号ア 第２章第５項第１号イ 第２章第５項第１号エ 第２章第５項第１号オ 第２章第５項第１号カ 第２章第５項第１号キ 第２章第５項第１号ケ 第２章第５項第１号サ 第２章第５項第２号 （キを除く。） 第２章第５項第３号ア 第２章第５項第３号イ 第２章第５項第３号ウ 第２章第５項第４号	平成29年４月１日	一部改訂

	第２章第５項第５号 第２章第５項第６号 第２章第６項第２号 第２章第６項第３号 第２章第７項第１号 第２章第７項第２号キ 第２章第７項第２号ク 第２章第７項第２号ケ 第２章第７項第２号コ 第２章第７項第３号 第２章第８項 第２章第９項第３号 第２章第９項第４号 第２章第７項第５号		

春日井市情報セキュリティポリシーの構成

春日井市の各情報システムが取り扱う情報には、市民の個人情報のみならず行政運営上重要な情報など、外部に漏えい等した場合には極めて重大な結果を招くおそれのある情報が多数含まれている。これらの情報及び情報システムを様々な脅威から防御することは、市民の財産、プライバシー等を守るためにも、また、事務の安定的な運営のためにも必要不可欠であり、ひいては、このことが本市に対する市民からの信頼の維持向上に寄与するものである。

春日井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、本市の情報システム及び行政情報に関するセキュリティ対策について、総合的かつ体系的に取りまとめたものを総称する。情報セキュリティポリシーは、職員等に浸透、普及、定着させるものであり、安定的な規範であることが要請される一方、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化にも柔軟に対応することが必要である。

このようなことから、情報セキュリティポリシーは、一定の普遍性を備えた部分としての「情報セキュリティ基本方針」と状況の変化に対して柔軟性をもって基本方針を実行に移すための共通の基準となる部分としての「情報セキュリティ対策基準」に分けて策定することとする。また、情報セキュリティポリシーに基づき、具体的なセキュリティ対策の実施手順として「情報セキュリティ実施手順書」を策定することとする。

情報セキュリティポリシーの構成

文　書　名		内　容
情報セキュリティポリシー	情報セキュリティ基本方針	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に移すための、すべての情報資産に共通の情報セキュリティ対策の基準
情報セキュリティ実施手順書		情報セキュリティ対策基準に基づいた具体的な実施手順

目　　次

第１章　情報セキュリティ基本方針

１　目的

情報セキュリティポリシーは、情報資産に対する様々な脅威に対し、情報セキュリティ対策を組織的かつ計画的に行うため、情報セキュリティ対策の基本となる事項を定めることにより、情報資産を保護することを目的とする。

２　定義

(1)　情報資産

情報システム及び行政情報をいう。

(2)　情報システム

電子計算機又はネットワークで構成され、事務処理を行う仕組みすべてをいう。

(3)　行政情報

本市の行政事務の執行に関する情報で、情報システムの開発及び運用に係るすべての情報並びに情報システムで取り扱うすべての情報をいう。

(4)　電子計算機

コンピュータのハードウェア、ソフトウェア、周辺機器及び記録媒体をいう。

(5)　ネットワーク

電子計算機を相互に接続するための通信網及び通信機器（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。

(6)　記録媒体

ハードディスク、ＣＤ－ＲＯＭ、磁気テープ等の電子的情報を記録するためのものをいう。

(7)　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。

３　情報セキュリティポリシーの位置付け

情報セキュリティポリシーは、本市が保有する情報資産に関する情報セキュリティ対策について、総合的かつ体系的に取りまとめたものであり、情報セキュリティ対策の最高位に位置付ける。

４　対象範囲

情報セキュリティポリシーの対象範囲は、本市の情報資産並びに情報資産に関する業務に携わる職員（本市のすべての職員をいう。以下同じ。）及び本市の情報資産を取り扱う業務の委託を受けた者（以下「委託業者」という。）とする。

５　職員等の責務

職員及び委託業者は、情報セキュリティ対策の重要性について共通の認識をもつとともに、業務の遂行に当たって関係法令及び情報セキュリティポリシーを遵守しなければならない。

6　情報セキュリティ管理体制

本市の情報資産について、情報セキュリティ対策を推進し、及び管理するための体制を確立するものとする。

7　情報資産の分類

情報資産を重要性に応じて分類し、それに応じた情報セキュリティ対策を講ずるものとする。

8　情報資産への脅威

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

(1)　不正アクセス、ウィルス攻撃、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

9　情報セキュリティ対策

上記 8 の脅威から情報資産を保護するために、次に掲げる情報セキュリティ対策を講ずるものとする。

(1)　物理的対策

情報システムを設置する施設への不正な立入り、情報資産への損傷、利用妨害等から保護するための物理的な対策

(2)　人的対策

情報セキュリティに関する権限や責任を定め、職員に情報セキュリティポリシーの内容を周知徹底するために必要な対策

(3)　技術的対策

情報資産を外部からの不正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、ネットワーク管理等の技術面の対策

(4)　運用における対策

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、システム開発等の委託管理等の運用面の対策

(5)　緊急事態における対策

自然災害や事故、故障、不正アクセス等が発生した場合に迅速かつ適切に対応するための緊急時の対策

10　情報セキュリティ対策基準の策定

情報セキュリティ対策を講ずるに当たっての遵守事項及び判断等の基準を定めた情報セキュリティ対策基準（以下「対策基準」という。）を策定するものとする。

11　情報セキュリティ実施手順の策定

対策基準に基づき、部、課及び出先機関の長は、個々の情報資産について具体的な実施手順を明記した情報セキュリティ実施手順（以下「実施手順書」という。）を策定するものとする。

12　違反への対応

情報セキュリティポリシーに違反した場合は、当該違反した者に対し、発生した事案の状況等に応じて法令及び条例の定めるところにより、必要な措置を講ずるものとする。

13　監査

情報セキュリティポリシーが遵守されていることを検証するため、必要に応じて監査を実施するものとする。

14　評価及び見直し

監査等の結果又は情報セキュリティを取り巻く状況の変化に対応するため、情報セキュリティ対策の評価及び見直しを実施するものとする。

15　特定個人情報等の保護に関する考え方

春日井市では、「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。）に定められた事務において個人番号及び特定個人情報（以下「特定個人情報等」という。）を取り扱う。番号法においては、特定個人情報等の利用範囲を限定する等、より厳格な保護措置を定めていることから、管理体制及び管理規程、取扱規程等を整備し、職員等に遵守させる等の措置を講じ、次に示す保護方針のとおり特定個人情報等を取り扱うものとする。

(1)　法令遵守

特定個人情報等の適正な取り扱いに関する法令等を遵守する。

(2)　安全管理措置

特定個人情報等の漏えい、滅失及び毀損の防止その他の適切な管理のた

めに必要な安全管理措置を講ずる。

(3)　適正な収集・保管・利用・廃棄、目的外利用の禁止

特定個人情報等は、番号法に定められた事務のうち、あらかじめ本人に通知した利用目的の達成に必要な範囲内で適正に利用、収集・保管及び提供するとともに、不要となった特定個人情報等は速やかに廃棄する。また、目的外利用を防止するための措置を講ずる。

(4)　委託・再委託

特定個人情報等を取り扱う事務の全部又は一部を委託する場合、委託先（再委託先を含む。）において、番号法に基づき当市自らが果たすべき安全管理措置と同等の措置が講じられるよう必要かつ適切な監督を行う。

(5)　継続的改善

特定個人情報等の保護に関する取扱規程等及び安全管理措置を継続的に見直し、その改善に努める。

第２章　情報セキュリティ対策基準

１　管理体制

本市の情報セキュリティ管理については、次の体制とする。

(1)　セキュリティ統括責任者（CISO：Chief Information Security Officer）

ア　情報セキュリティ対策を総合的に実施するため、セキュリティ統括責任者を置く。

イ　セキュリティ統括責任者は、市長が指名する副市長をもって充てる。

ウ　セキュリティ統括責任者は、全ての情報セキュリティに関する権限及び責任を有する。

(2)　セキュリティ管理責任者

ア　情報セキュリティ対策の運用及び管理を適正に行うため、セキュリティ管理責任者を置く。

イ　セキュリティ管理責任者は、総務部長をもって充てる。

ウ　セキュリティ管理責任者は、セキュリティ統括責任者を補佐し、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な情報セキュリティ対策を行う権限及び責任を有する。

エ　セキュリティ管理責任者は、全てのシステムに共通する企画、開発及び運用保守に関する統括的な権限及び責任を有する。

(3)　ネットワーク管理者

ア　本市の情報システムのネットワークにおける統括的な情報セキュリティ対策を実施するため、ネットワーク管理者を置く。

イ　ネットワーク管理者は、総務部情報システム課長をもって充てる。

ウ　ネットワーク管理者は、セキュリティ管理責任者の指示に従い、セキュリティ管理者、システム管理者及びセキュリティ責任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。

(4)　セキュリティ管理者

ア　部及び事務局（以下「部等」という。）における情報セキュリティ対策の適正な管理を行うため、セキュリティ管理者を置く。

イ　セキュリティ管理者は、部等の長をもって充てる。

ウ　セキュリティ管理者は、所掌する部等、課及び出先機関（以下「部課等」という。）の情報資産の管理に関する統括的な権限及び責任を有する。

エ　セキュリティ管理者は、所掌する課及び出先機関において情報セキュリティポリシーの遵守に関する意見の集約及び職員に対する教育、訓練、助言及び指示を行う。

(5)　セキュリティ責任者

ア　情報システムを利用する部課等において情報セキュリティ対策を実施するため、セキュリティ責任者を置く。

イ　セキュリティ責任者は、課及び出先機関の長をもって充てる。

ウ　セキュリティ責任者は、所掌する部署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。

エ　セキュリティ責任者は、所管する情報資産について実施手順書の作成、維持及び管理を行う。

(6)　システム管理者

ア　各情報システムの管理を行うため、システム管理者を置く。

イ　システム管理者は、情報システムを所管する課及び出先機関の長をもって充てる。

ウ　システム管理者は、所管する情報システムに係る企画、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。

エ　システム管理者は、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。

オ　システム管理者は、所管する情報システムに係る実施手順書の作成、維持及び管理を行う。

(7)　春日井市情報化推進委員会

ア　春日井市情報化推進委員会（以下「情報化推進委員会」という。）において、情報セキュリティの維持管理を統一的に行う。

イ　情報化推進委員会は、情報セキュリティ基本方針、対策基準の策定その他情報セキュリティ対策に関する重要な事項を審議する。

ウ　情報化推進委員会の所掌事務、組織その他必要な事項は、春日井市情報化推進委員会要綱（平成１５年５月１日施行）において定める。

(8)　情報セキュリティに関する統一的な窓口

ア　総務部情報システム課に、情報セキュリティに関する事故並びに情報システム上の欠陥及び誤動作（以下「事故等」という。）に関する統一的な窓口（以下「CSIRT：Computer Security Incident Response Team（シーサート）」という。）を設置する。

イ　CSIRTは、事故等について部課等より報告を受けた場合には、その状況を確認し、セキュリティ統括責任者へ報告する。

ウ　CSIRTは、セキュリティ統括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、その内容を部課等に提供する。

エ　CSIRTは、事故等を認知した場合には、その重要度や影響範囲等を勘案し、事故等に関係した部課等が行う報道機関への通知・公表対応の支援を行う。

オ　CSIRT 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 CSIRT の機能を有する部署、委託業者等との情報共有を行う。

2　情報資産の分類及び管理

(1)　情報資産の分類

情報資産は、各々の機密性、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。

重要性	内　　容
Ⅰ	漏えい、改ざん、消去等が市民の生命・財産・プライバシー又は行政事務の執行に重大な影響を及ぼすもの。 個人情報（個人番号を付した特定個人情報を含む。）は重要性分類Ⅰに該当する。
Ⅱ	市の内部情報で、その漏えい、改ざん、消去等が行政事務の執行に影響を及ぼすもの。
Ⅲ	上記以外のもの

(2)　情報資産の管理

ア　情報資産の管理責任

(ｱ)　情報資産は、当該情報資産を作成した部課等のセキュリティ管理者又はセキュリティ責任者が管理責任を有する。

(ｲ)　情報資産を利用する者は、情報資産の分類に従って利用する責任を有する。

イ　情報資産の管理及び取扱い

(ｱ)　情報資産を適切に管理するため、セキュリティ管理者又はセキュリティ責任者は情報資産管理台帳を作成し、当該情報資産を登録しなければならない。

(ｲ)　セキュリティ管理者又はセキュリティ責任者は、情報資産の重要性分類に応じ、アクセス権限を定めなければならない。

(ｳ)　重要性分類Ⅰの情報資産については、セキュリティ管理者又はセキュリティ責任者の許可を得た場合を除き、複製又は送信を行ってはならない。

ウ　記録媒体の管理

(ｱ)　取り出しが可能な記録媒体は、適切な管理を行わなければならない。

(ｲ)　確定した行政情報を記録した記録媒体は、書き込み禁止措置を行った上で保管しなければならない。

(ｳ)　記録媒体は、データ暗号化機能を備えた媒体を使用しなければなら

ない。データ暗号化機能を備えていない媒体については、使用後速やかに初期化を行うとともに、事務室から持ち出してはならない。

(ｴ)　重要性分類Ⅰの行政情報を記録した記録媒体は、施錠可能な場所に保管しなければならない。

(ｵ)　システム管理者は、許可された記録媒体以外のものについて使用の制限等の必要な措置を講じなければならない。また、記録機能を有する機器の情報システム端末等への接続の制限等の必要な措置を講じなければならない。

(ｶ)　重要性分類Ⅰの行政情報が記録された記録媒体又は書類等を持ち出す必要が生じた場合には、容易に個人を特定できない措置の実施、追跡可能な移送手段の利用等、安全な方策を講じなければならない。

(ｷ)　記録媒体が不要となった場合は、当該媒体に記録されている重要性分類Ⅰ及びⅡの行政情報は、復元できないように消去等を行った上で廃棄しなければならない。

(ｸ)　重要性分類Ⅰ及びⅡの行政情報を記録した記録媒体の廃棄は、セキュリティ管理者又はセキュリティ責任者の許可を得ることとし、廃棄を行った日時、担当者及び処理内容を情報資産管理台帳に記録しなければならない。

3　物理的セキュリティ

(1)　入退室管理

ア　セキュリティ責任者は、重要性分類Ⅰ及びⅡの行政情報が記録されている記録媒体の保管場所及びそれらを取り扱う情報機器の設置場所への入退室管理について、必要な措置を講じなければならない。

イ　ネットワーク管理者は、住民記録情報を扱う基幹系業務及び内部事務支援業務を扱う内部情報系の情報システム（以下「基幹系情報システム」という。）のサーバを設置する部屋（以下「電子計算機室」という。）の入退室管理を行う。

ウ　システム管理者は、情報システムのサーバ（電子計算機室に設置するサーバを除く。）を設置する場所の入退室管理を行う。

(2)　電子計算機室の管理

ア　電子計算機室内の機器類は、耐震対策を講じた場所に設置するとともに、防火措置等を施さなければならない。

イ　電子計算機室で使用する消火剤は、機器及び記録媒体に影響を与えるものであってはならない。

ウ　電子計算機室の入退室は許可された者のみとし、指紋照合等による入

退室管理又は入退室管理簿の記載を行い、職員、委託業者等は、所属を明らかにする名札を着用しなければならない。

エ　電子計算機室へ機器等を搬入出する場合は、あらかじめ当該機器等の既存情報システムに対する安全性について確認するとともに、ネットワーク管理者が立ち会う等の必要な措置を講じなければならない。

オ　電子計算機室には、外部からの不正な侵入に備え、施錠装置、警報装置及び監視設備を設置しなければならない。

(3)　電源

重要性分類Ⅰ及びⅡの行政情報を取り扱う情報システムの電源については、当該機器を適切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。

(4)　配線

ア　配線は、損傷等を受けることがないよう必要な措置を講じなければならない。

イ　主要な配線については、損傷についての定期的な点検を行わなければならない。

ウ　ネットワークに使用する回線は、伝送途上において破壊、盗聴、改ざん、消去等が生じないように十分な対策を講じなければならない。

(5)　盗難等の防止

情報資産については、盗難、紛失等の防止のための必要な措置を講じなければならない。特に、記録媒体、書類等の庁舎内の移動等における盗難及び紛失の防止に留意しなければならない。

(6)　敷地外への機器の設置

システム管理者は、庁舎の敷地外にサーバ等の機器を設置する場合、セキュリティ管理者（当該サーバ等を基幹系情報システムと同一のネットワークに接続する場合にあっては、セキュリティ管理者及びネットワーク管理者）の許可を得なければならない。また、必要に応じ当該機器への情報セキュリティ対策の実施状況について確認するものとする。

4　人的セキュリティ

(1)　職員

ア　職員は、情報セキュリティポリシー及び実施手順書に定められている事項を遵守しなければならない。

イ　職員は、使用する情報システムの機器や記録媒体について、第三者に使用されること又は許可なく情報を閲覧されることがないように適切な措置を講じなければならない。

ウ　職員は、セキュリティ責任者の許可を得ずに情報資産を執務室外に持ち出してはならない。

エ　職員は、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。

オ　職員は、情報セキュリティに関する事故並びに情報システム上の欠陥及び誤動作（以下「事故等」という。）を認知した場合には、速やかに所属のセキュリティ責任者及びCSIRTに報告しなければならない。

カ　ネットワーク管理者及びシステム管理者は、ネットワーク及び情報システムの開発・保守等を外部委託業者に発注する場合、委託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委託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。

また、特定個人情報等を取り扱う事務の全部又は一部を委託する場合、委託先（再委託先を含む。）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よう必要かつ適切に監督しなければならない。

(2)　教育・訓練

ア　セキュリティ統括責任者は、職員に対し情報セキュリティポリシーについて啓発に努めるとともに、職員を対象とする情報セキュリティに関する研修を実施しなければならない。

イ　情報セキュリティに関する教育・訓練計画は、情報化推進委員会で承認されたものを使用する。

ウ　ネットワーク管理者は、最新の技術力を維持するための研修を受けなければならない。

エ　セキュリティ管理者及びセキュリティ責任者は、情報通信技術及び情報セキュリティに関する必要な知識を維持しなければならない。

オ　ネットワーク管理者、システム管理者及びセキュリティ責任者は、緊急時の対応を想定した訓練を計画的に行わなければならない。

カ　職員は、情報セキュリティに関する研修を受講し、情報セキュリティポリシー及び実施手順書を理解し、情報セキュリティ上の問題が生じないようにしなければならない。

(3)　パスワード及び利用者ＩＤの管理

職員は、自己の保有するパスワード及び利用者ＩＤに関し、次の事項を遵守しなければならない。

ア　パスワード及び利用者ＩＤを秘密にし、パスワード及び利用者ＩＤの照会等には一切応じないこと。

イ　パスワード及び利用者ＩＤのメモを作らないこと。

ウ　パスワードは、不規則かつ推測が困難なものとすること。

エ　複数の情報システムを扱う職員は、パスワードを情報システム間で共有しないこと。

オ　職員間でパスワードを共有しないこと。

(4)　ＩＣカードの管理

ア　認証に用いるＩＣカード（以下「認証用カード」という。）は、職員間で共有してはならない。

イ　認証用カードをカードリーダに常時挿入してはならない。

ウ　職員は、認証用カードを紛失したときは、速やかにセキュリティ責任者に報告し、指示を受けなければならない。

エ　セキュリティ責任者は、認証用カードの紛失等の届出があったときは、速やかに失効の手続をしなければならない。

(5)　接続時間の制限

職員は、情報システムに接続している時間を必要最小限にするように努めなければならない。

5　技術的セキュリティ

(1)　情報システムの管理

ア　アクセス記録の取得等

(ｱ)　システム管理者は、所管する情報システム及び特定個人情報ファイルに関する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、一定の期間保存しなければならない。

(ｲ)　システム管理者は、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、適切にログを管理しなければならない。

(ｳ)　システム管理者は、取得したログを定期的に又は随時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。

イ　情報システムの管理記録及び仕様書等の管理

(ｱ)　システム管理者は、所管する情報システムにおいて行った変更等については、記録を作成し適切に管理しなければならない。

(ｲ)　システム管理者は、所管する情報システムの仕様書、設計文書、マスターデータ等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。

ウ　無許可ソフトウェアの導入の禁止等

(ｱ)　職員は、新たにソフトウェアを導入する場合は、システム管理者及

びセキュリティ責任者の許可を得なければならない。

(ｲ)　職員は、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)　職員は、業務上必要のないソフトウェア及び安全性が確認できないソフトウェアを導入してはならない。

エ　バックアップ

システム管理者は、重要性分類Ⅰ及びⅡの行政情報について、用途に応じて期間を設定し、定期的にバックアップをとらなければならない。

オ　電子メールの送受信

(ｱ)　ネットワーク管理者は、外部から外部へのメール転送（メールの中継処理）を不可能とする設定を施さなければならない。

(ｲ)　ネットワーク管理者は、インターネットを経由する電子メールに添付できるファイルの容量を３MB までとし、３MB を超えるファイルが添付された電子メールの送受信を不可能としなければならない。

(ｳ)　ネットワーク管理者は、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。

(ｴ)　職員は、電子メールの自動転送機能を用いて職場の電子メールを転送してはならない。

(ｵ)　職員は、チェーンメールや不審な電子メールを他者に転送してはならない。

(ｶ)　職員は、差出人が不明又は不自然なファイルが添付された電子メールを受信した場合は、直ちに破棄しなければならない。

(ｷ)　職員は、電子メールにより重要性分類Ⅱ以上の情報を送信する場合、暗号化又はパスワード設定を行わなければならない。

(ｸ)　職員は、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。

(ｹ)　職員は、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。

(ｺ)　職員は、重要な電子メールを誤送信した場合、セキュリティ管理者及びセキュリティ責任者に報告しなければならない。

(ｻ)　職員は、不特定多数の人がウェブで利用できるフリーメール、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。

カ　外部の者が利用できるシステム

ネットワーク管理者、システム管理者及びセキュリティ責任者は、職員以外の者が利用できる情報システムについては、必要に応じ他の情報

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講じなければならない。

キ　情報システムの入出力データ

(ｱ)　システム管理者及びセキュリティ責任者は、情報システムに入力されるデータの適切なチェックを行い、常に正確性を確保するよう努めなければならない。

(ｲ)　システム管理者は、情報システムから出力されるデータの処理が、常に正しく行われるよう必要な措置を講じなければならない。

ク　業務目的以外の使用の禁止

職員は、業務目的以外での情報システムへのアクセス、電子メールの使用及びウェブページの閲覧をしてはならない。

ケ　機器構成の変更等

(ｱ)　基幹系情報システムと同一のネットワークに接続する機器は、ネットワーク管理者が仕様を指示し、許可したもののみとする。

(ｲ)　職員は、個人の所有する機器を基幹系情報システムに接続してはならない。

(ｳ)　職員は、情報システムの機器について、改造及び機器の増設・交換を行ってはならない。

(ｴ)　情報システムの機器について業務を遂行するために機器の増設・交換を行う必要がある場合は、システム管理者の許可を得なければならない。

(ｵ)　セキュリティ責任者は、モデム等の機器を増設して他の環境へのネットワーク接続をする場合又は外部からのアクセスを可能とする仕組みを構築する場合は、ネットワーク管理者の許可を得なければならない。

コ　複合機のセキュリティ管理

(ｱ)　システム管理者及び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、適切なセキュリティ要件を策定しなければならない。

(ｲ)　システム管理者及びセキュリティ責任者は、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。

(ｳ)　システム管理者及び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。

サ　特定用途機器のセキュリティ管理

ネットワーク管理者及びシステム管理者は、特定用途機器（テレビ会議システム、ＩＰ電話システム、ネットワークカメラシステム等の特定の用途に使用される情報システム特有の構成要素であって、通信回線に接続されている又は記録媒体を内蔵しているもの）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実施しなければならない。

(2)　アクセス制御

ア　アクセス制御

システム管理者は、所管するネットワーク、情報システム、行政事務又はファイル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。

イ　アクセス者の識別と認証

情報システムは、職員が正当なアクセス権を有する者であることを、識別した結果に基づき認証できるものでなければならない。

ウ　利用者登録

(ｱ)　システム管理者及びセキュリティ責任者は、情報システムの利用者の登録、変更及び抹消並びに登録情報の管理については、各情報システムごとに定められた方法に従って行わなければならない。

(ｲ)　システム管理者は、利用者の登録、変更及び抹消は、申請により行うものとする。

エ　管理者権限

(ｱ)　情報システムの管理者権限は、システム管理者が有する。

(ｲ)　情報システムの管理者権限を代行する者は、システム管理者が指名した者とする。

オ　外部からのアクセス

システム管理者は、外部からのアクセス許可を必要最低限にしなければならない。

カ　外部ネットワークとの接続

(ｱ)　外部ネットワークと本市の情報システムを接続する場合には、当該外部ネットワークのネットワーク構成、機器構成、セキュリティレベル等を検討し、本市の情報システムに影響が生じないことを確認した上で、ネットワーク管理者の許可を得て接続しなければならない。

(ｲ)　ネットワーク管理者は、外部ネットワークと本市の情報システムを接続することにより、本市の情報システムの安全性が脅かされることのないよう情報セキュリティ対策に努めなければならない。

(ｳ)　接続した外部ネットワークのセキュリティに問題が認められ、本市の情報資産に脅威が生じることが予想される場合には、ネットワーク管理者及びシステム管理者は、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。

キ　利用者ＩＤ等の管理

システム管理者及びセキュリティ責任者は、利用者ＩＤ、パスワード及び認証用カード及び生体認証情報を厳重に管理しなければならない。

(3)　システム開発、導入、保守等

ア　情報システムの開発、導入

システム管理者は、情報システムを開発又は導入する場合は、次の事項を実施しなければならない。

(ｱ)　機器及びソフトウェアを購入等する場合は、当該製品が情報セキュリティ上問題にならないかどうか確認すること。

(ｲ)　新たに情報システムを導入する場合には、既に稼働している情報システムへの影響を考慮し、十分な試験を行うこと。

(ｳ)　情報システムの開発及び保守時の事故及び不正行為の対策を講ずること。

イ　情報システムの変更管理

システム管理者は、情報システムを追加、変更、廃棄等した場合は、その設定、構成等の履歴を記録し、保存しなければならない。

ウ　ソフトウェアの保守及び更新

(ｱ)　ネットワーク管理者及びシステム管理者は、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、適切な保守が行なわれるようにするとともに、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)　ネットワーク管理者及びシステム管理者は、情報システムのソフトウェアの更新等については、計画的に実施しなければならない。

(ｳ)　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。

エ　機器の修理及び廃棄

(ｱ)　記録媒体の含まれる機器の修理又は廃棄を業者に委託する場合は、記録媒体内の行政情報が消去された状態で行わなければならない。

(ｲ)　業者に記録媒体の含まれる機器を修理させる場合に、行政情報を消去することが困難であると認められるときは、修理を委託する業者に対して秘密の保持を契約事項として定めなければならない。

(4)　コンピュータウィルス対策

ア　ネットワーク管理者及びシステム管理者は、次の事項を実施しなければならない。

(ｱ)　外部のネットワークから受信したファイルは、ファイアウォール等でウィルスチェックを行い情報システムへの侵入を防止すること。

(ｲ)　外部のネットワークへ送信するファイルは、ファイアウォール等でウィルスチェックを行い外部へのウィルス拡散を防止すること。

(ｳ)　ウィルスチェック用のパターンファイルは、常に最新のものに保つこと。

(ｴ)　コンピュータウィルスの感染状況等について監視すること。

(ｵ)　コンピュータウィルス情報について、職員に対する注意を喚起すること。

(ｶ)　コンピュータウィルスに関する情報収集に努めること。

イ　職員は、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、必ずウィルスチェックを行うこと。

(ｲ)　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うこと。

(ｳ)　ウィルスチェックの実行を途中で止めないこと。

(ｴ)　ネットワーク管理者又はシステム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すること。

(5)　不正アクセス対策

ネットワーク管理者及びシステム管理者は、次の事項を実施しなければならない。

ア　不正アクセスを防止するため、適切なネットワーク経路の制御を施すこと。

イ　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・保存すること。

ウ　情報システムに侵入や不正な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ること。

エ　情報システムに攻撃を受けていること又は受けることが明らかな場合には、情報システムの停止を含め必要な措置を講ずること。

オ　職員による不正アクセスがあった場合は、当該職員が属する部課等のセキュリティ管理者に通知し、適切な措置を求めること。

カ　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ずること。

キ　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ずること。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ずること。

ク　個人番号利用事務の実施に当たり接続する情報提供ネットワークシステム等の接続規程等が示す安全管理措置を遵守すること。

(6)　セキュリティ情報の収集

ネットワーク管理者及びシステム管理者は、情報セキュリティに関し、適宜情報を収集しなければならない。

6　運用

(1)　情報システムの監視

システム管理者及びセキュリティ責任者は、情報システムの運用に当たっては、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

セキュリティ管理者、システム管理者及びセキュリティ責任者は、情報セキュリティポリシーの遵守状況を確認しなければならない。

(3)　侵害時の対応

ア　状況の把握

システム管理者及びセキュリティ責任者は、事故等により情報システムに係る情報資産への侵害が認知された場合にあっては、セキュリティ管理者及びCSIRTにその発生を速やかに報告するとともに、侵害の内容、侵害の発生原因、確認した被害及びその影響範囲について調査しなければならない。

イ　侵害への対処

(ｱ)　システム管理者及びセキュリティ責任者は、セキュリティ管理者又はCSIRTの指示に従い、情報資産への侵害の状況に応じて必要な措置を講じなければならない。

(ｲ)　ネットワーク管理者は、情報資産への侵害が重大な影響を及ぼすおそれがある場合には、セキュリティ統括責任者及びセキュリティ管理責任者に報告しなければならない。この場合においてセキュリティ統括責任者は、被害の拡大を防止するため、情報システムの停止を含む必要な指示をするものとする。

ウ　再発防止の措置

(ｱ)　セキュリティ管理者及びシステム管理者は、再発防止の措置を講ずるとともに、その結果をネットワーク管理者に報告しなければならない。また、事故等を分析し、再発防止のための情報として記録を保存しなければならない。

(ｲ)　ネットワーク管理者は、(ｱ)の結果をセキュリティ統括責任者及びセキュリティ管理責任者に報告しなければならない。

エ　緊急時対応計画の作成

システム管理者は緊急時における状況の把握、侵害への対処及び再発防止の措置について、セキュリティ責任者は緊急時における状況の把握及び侵害への対処について、緊急時対応計画を作成しなければならない。

7　委託管理

(1)　委託先の選定基準

ア　ネットワーク管理者及びシステム管理者は、委託先の選定に当たり、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、委託内容を完了することができる能力を有すること及び(2)に掲げる事項を行うことができることを確認しなければならない。

イ　ネットワーク管理者及びシステム管理者は、必要に応じて情報セキュリティマネジメントシステムの国際規格の認証取得状況、情報セキュリティ監査の実施状況等を参考にして、事業者を選定するものとする。

(2)　契約項目

情報システムの開発、運用、管理等の業務を委託しようとするときは、契約書に行政情報の保護に関し次に掲げる事項を明記しなければならない。

ア　守秘義務に関する事項

イ　再委託に関する事項

ウ　システム管理記録及び障害記録の提出及び管理に関する事項

エ　行政情報が記録された資料の目的外使用、複製、複写及び第三者への提供の禁止に関する事項

オ　監視に関する事項

カ　緊急時の措置に関する事項

キ　セキュリティ対策の実施指示に関する事項

ク　セキュリティ対策の実施状況の監督に関する事項

ケ　不正行為防止措置に関する事項

コ　その他情報セキュリティに関する事項

(3)　確認

ネットワーク管理者及びシステム管理者は、必要に応じ委託業者におけ

る当該委託業務に係る情報セキュリティ対策の実施状況について調査するものとする。

8　法令遵守

職員は、業務の遂行に当たって使用する情報資産について、次に掲げる法令等その他関係法令等を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)　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）
(3)　著作権法（昭和45年法律第48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)　春日井市個人情報保護条例（平成14年春日井市条例第41号）
(7)　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）（平成26年特定個人情報保護委員会告示第６号）

9　評価及び見直し

(1)　セキュリティ管理責任者は、情報セキュリティ対策について必要に応じて監査を行わなければならない。
(2)　セキュリティ責任者及びシステム管理者は、情報セキュリティポリシーの遵守状況について、自己点検を行い、必要に応じて改善措置を講ずるとともに、その内容についてセキュリティ管理者又はセキュリティ管理責任者に報告しなければならない。
(3)　セキュリティ管理責任者は、監査の結果並びに自己点検及び改善措置の内容をセキュリティ統括責任者に報告しなければならない。
(4)　セキュリティ統括責任者は、監査の結果等により情報セキュリティ対策の評価を行うとともに、新たな対策が必要な場合は、情報化推進委員会に諮り、情報セキュリティポリシーの見直しを行うものとする。

10　市民病院等の特例

市民病院、教育委員会、消防本部その他の機関の長は、その保有する情報資産の構成、性質等を勘案し、その保有する情報資産の適正な取扱いが確保されるよう対策基準を別に定めることができる。

【用語解説】

機密性（confidentiality）	情報が権限の無い第三者に漏れないようにすること。
完全性（integrity）	情報及び処理の方法が常に完全な状態でかつ安全に維持され、改ざんや破壊されないようにすること。
可用性（availability）	許可された利用者が必要なときに情報にアクセスできること。
アクセス	情報資産を利用すること。
アクセス権限	情報資産を利用する権限
不正アクセス	不正アクセス禁止法第３条第２項に規定する不正アクセス行為その他の不正な手段により利用者以外の者が行うアクセス又は利用者が行う権限外のアクセス
サーバ	サービスを提供するソフトウェア又はハードウェア
ＩＣカード	情報の記録媒体としてICチップを組み込んだカード
ハードウェア	コンピュータ機器の総称
ソフトウェア	プログラム、データ等の総称
バックアップ	プログラム、データ等と同一の内容を別の媒体に記録すること。
チェーンメール	不特定多数の人に関連するような偽情報などを捏造して電子メールを送り、次々と連鎖的に転送させることを目的としたメール
利用者ＩＤ	ネットワークシステム、コンピュータ等の利用者を識別する符号
ファイアウォール	組織内ネットワークへの不正侵入を防ぎ、利用者の接続統制などを行うシステム、また、そのようなシステムが組み込まれたコンピュータ
パターンファイル	ウイルス対策ソフトでウイルスを検索、駆除するために必要なウイルス情報。新種のウイルスに対してはこの情報を定期的に更新しておかないとウイルスの検知、駆除が行えない。