○菊池市情報セキュリティ規則

平成 17 年 3 月 22 日

規則第 15 号

改正　平成 19 年規則第 9 号

(注)平成 22 年 1 月から改正経過を注記した。

目次

第 1 章　総則

(趣旨)

第 1 条　この規則は、高度情報通信社会の急速な進展によるネットワークを介した情報システムの利用拡大に伴い、情報資産に対する不正な侵害、災害、事故等の脅威が増大していることにかんがみ、本市が保有する情報資産の機密性(情報にアクセスすることを認可された者だけがアクセスできることを確実にすることをいう。)、完全性(情報及び処理の方法の正確さ並びに完全である状態を安全に防護することをいう。)及び可用性(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を確実にできることをいう。)を安定的に維持するためのセキュリティ基準として必要な事項を定めるものとする。

(定義)

第 2 条　この規則において、次の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)　電子計算機等　ハードウェア及びソフトウェアで構成するコンピュータ及び周辺機器並びに各種記録媒体をいう。

(2)　ネットワーク　電子計算機等を相互に接続するための通信網及び接続に必要な機器で構成される仕組みをいう。

(3)　情報システム　電子計算機等及びネットワークによって処理を行う仕組みをいう。

(4)　行政情報　本市の情報システムで取り扱う行政事務の執行にかかわるすべてのデータをいう。
(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し、並びに定められた範囲での利用可能な状態を維持することをいう。
(7)　不正アクセス　情報システムを利用する者が、その者に与えられた権限によって許された行為以外の行為を、ネットワークを介して意図的に行うことをいう。
(8)　ウイルス　第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたコンピュータプログラムであり、次に掲げる機能の一つ以上を有するものをいう。
ア　自己伝染機能　自らの機能によって他のプログラムに自らをコピーし、又はシステム機能を利用して自らを他のシステムにコピーすることにより、他のシステムに伝染する機能
イ　潜伏機能　発病するための特定時刻、一定時間、処理回数等の条件を記憶させて、発病するまで症状を出さない機能
ウ　発病機能　プログラム、データ等のファイルを破壊し、又は設計者の意図しない動作をさせる等の機能
(9)　サイバーテロ　ネットワークを通じて各国の国防、治安等を始めとする各種分野の情報システムに侵入し、データを破壊、改ざんするなどの手段で国家又は社会の重要な基盤を機能不全に陥れる行為をいう。
(適用範囲)
第3条　この規則の規定は、本市の保有する全ての情報資産(地方教育行政の組織及び運営に関する法律(昭和31年法律第162号)第30条に基づき本市に設置された教育機関(以下「教育機関」という。)において教育の用に供する情報資産を除く。)に適用する。
第2章　情報セキュリティ対策基準
第1節　人的セキュリティ
第1款　組織及び体制
(情報セキュリティ最高情報統括責任者)
第4条　本市のすべての情報資産及びそれらに関する情報セキュリティの管理を統括するため、情報セキュリティ最高情報統括責任者を置く。
2　情報セキュリティ最高情報統括責任者は、副市長をもって充てる。
(ネットワーク管理者)
第5条　情報セキュリティ最高情報統括責任者を補佐して、本市のすべての情報資産及びそれらに関する情報セキュリティの管理を行うため、ネットワーク管理者を置く。
2　ネットワーク管理者は、情報化推進担当部長をもって充てる。
(情報セキュリティ部門責任者)
第6条　本市の各部門における情報セキュリティの管理を統括させるために、各部門に情報セキュリティ部門責任者を置く。
2　情報セキュリティ部門責任者は、次の各号に掲げる部門の区分ごとに、当該各号に定められる者をもって充てる。
(1)　菊池市部設置条例(平成17年菊池市条例第7号)第1条に規定する部においては、各部長
(2)　菊池市支所設置条例(平成17年菊池市条例第2号)第1条に規定する支所においては、支所長
(3)　菊池市会計管理者の補助組織設置規則(平成17年菊池市規則第6号)第1条に規定する会計課においては、課長
(4)　菊池市水道事業の設置等に関する条例(平成17年菊池市条例第193号)第8条に規定する水道局においては、水道局長
(5)　執行機関として法律に定めるところにより本市に置かれる委員会(次号に掲げるものを除く。)若しくは委

員の事務局又は委員会の管理に属する事務を掌る機関においては、各事務局長及び機関
(6)　教育委員会(教育機関を含む。)においては、教育次長
(7)　議会に置かれる事務局においては、事務局長
(情報セキュリティ管理者)
第7条　前条第2項各号に掲げる各部門(以下「部局等」という。)に組織される課及び室(以下「課等」という。)における情報セキュリティを管理するため、課等にそれぞれ情報セキュリティ管理者を置く。
2　情報セキュリティ管理者は、課等の長をもって充てる。
(情報システム管理者)
第8条　情報システムを管理するため、情報システム管理者を置く。
2　情報システム管理者は、情報システムを所管する課等の長をもって充てる。
第2款　情報資産の分類及び管理
(情報システムの分類)
第9条　情報システム管理者は、その所管する情報システムを侵害、災害、事故等(以下「侵害等」という。)による影響度に応じ、次に掲げる区分により分類しなければならない。
(1)　その情報資産への侵害等が、市民の生命、財産、権利利益等に対する重大な影響を及ぼすこととなる情報システム
(2)　その情報資産への侵害等が、行政事務の執行等に重大な影響を及ぼすこととなる情報システム
(3)　その情報資産への侵害等が、行政事務の執行等に軽微な影響を及ぼすこととなる情報システム
(4)　前3号に掲げるもの以外の情報システム
2　情報システム管理者は、別に定めるところにより、情報システムを管理するための台帳を作成し、これを保管しなければならない。
(行政情報の分類)
第10条　情報セキュリティ管理者は､その所管する行政情報を次に掲げる区分に応じ分類しなければならない。
(1)　菊池市情報公開条例(平成17年菊池市条例第10号)第7条第2号の個人に関する情報に該当する行政情報
(2)　菊池市情報公開条例第7条第3号から第7号までに掲げる情報に該当する行政情報
(3)　前2号に掲げるもの以外の行政情報で、業務上重要と認められる行政情報
(4)　前3号に掲げるもの以外の行政情報
2　情報セキュリティ管理者は、別に定めるところにより、行政情報を管理するための台帳を作成し、これを保管しなければならない。
(情報資産の管理責任)
第11条　情報セキュリティ部門責任者は、その属する部局等において作成し、又は入手した情報資産に関し、情報セキュリティを確保すべき責任を有する。
(行政情報の機密性の確保)
第12条　情報セキュリティ管理者は、その所管する行政情報に対してアクセスする権限を有する職員の範囲を定める等により、行政情報の機密性の確保に努めなければならない。
(行政情報の私的利用等の禁止等)
第13条　職員は、行政情報を私的に利用してはならない。
2　職員は、行政情報を不正に複製し、漏洩し、破壊し、及び改ざんしてはならない。
3　職員は、行政情報を本市の事務所(本庁舎以外の事務所にあっては当該事務所)外に持ち出すことはできない。ただし、業務上特に必要として情報セキュリティ最高情報統括責任者が許可した場合は、この限りでない。
(記録媒体の管理)
第14条　職員は、行政情報を記録した記録媒体の保管に関し、細心の注意を払わなければならない。

2　情報システム管理者は、記録媒体に記録した行政情報を必要に応じて別の記録媒体に複製し、当該複製した記録媒体を災害を被る可能性が低い場所に適正に保管しなければならない。
(特定記録媒体の廃棄)
第 15 条　情報システム管理者は、第 10 条第 1 号及び第 2 号に規定する行政情報を記録した記録媒体(以下「特定記録媒体」という。)を廃棄するときは、ネットワーク管理者の許可を受けなければならない。
2　情報システム管理者は、特定記録媒体を廃棄するときは、特定記録媒体に保存された行政情報を消去し、かつ、消去した行政情報を復元できないようにする措置を講じなければならない。
3　情報システム管理者は、特定記録媒体を廃棄したときは、その日時、担当者、廃棄した行政情報の名称及び廃棄処理の方法を記録しなければならない。
(情報セキュリティ実施手順の策定)
第 16 条　情報システム管理者は、情報セキュリティ対策基準の基本的な要件に基づき、情報資産の情報セキュリティ実施手順を策定しなければならない。
(侵害等に対する対応)
第 17 条　情報セキュリティ管理者は、本市の情報資産に対する侵害等が発生したとき(以下「緊急時」という。)は、緊急時の対応計画にのっとり、直ちに連絡、証拠保全、被害拡大の防止、復旧等の必要な措置を迅速かつ円滑に実施し、再発防止のための措置を講じなければならない。
(教育及び訓練)
第 18 条　情報セキュリティ最高情報統括責任者は、職員に対しこの規則及びそれぞれの職務に関する情報セキュリティ実施手順について教育及び啓発する責務を有するとともに、侵害等に備えてあらかじめ緊急時の対応手順を定めておかなければならない。
2　情報システム管理者は、緊急時を想定した訓練を、その所管する情報システムの規模等を考慮し、訓練実施の範囲等を適宜定めて計画的に行わなければならない。
3　職員は、定められた研修に参加し、この規則及びその職務に関する情報セキュリティ実施手順を理解するとともに、それらを遵守して情報セキュリティの管理に努めなければならない。
4　新たに本市に採用された職員は、適切な時期に、本市の情報セキュリティに関する規則等及びその職務に関する情報セキュリティ実施手順についての研修を受講しなければならない。
第 2 節　物理的セキュリティ
第 1 款　サーバ等
(サーバ等の設置)
第 19 条　第 9 条第 1 号及び第 2 号に規定する情報システムのサーバ、情報セキュリティ対策に関するサーバ並びにネットワークの基幹機器(以下「サーバ等」という。)は、それらを設置するための専用の部屋(以下「情報システム室」という。)に設置しなければならない。ただし、ネットワーク管理者がそれらに関する情報セキュリティを確保できると認めたときは、情報システム室以外に設置することができる。
2　情報システム管理者は、サーバ等に障害が発生したときは、直ちに復旧のための措置を講じなければならない。
3　情報システム管理者は、サーバ等の機器の操作を行わせるに当たっては、パスワード等による操作資格者の限定を行う等の必要な措置を講じなければならない。
(サーバ等の電源)
第 20 条　情報システム管理者は、サーバ等の設置に当たっては、主たる電源の供給が断たれた場合においても、当該サーバ等を適切に停止するまでの間に当該サーバ等の機能を維持するための十分な電力を供給することができる容量を持つ予備電源設備を必要に応じて設置しなければならない。
2　情報システム管理者は、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必要に応じて

講じなければならない。
(外部に設置する装置)
第 21 条　情報システム管理者は、情報システムの全部又は一部の装置を外部に設置するときは、情報セキュリティ最高情報統括責任者の許可を得なければならない。
2　情報システム管理者は、定期的に当該装置の情報セキュリティの水準について確認しなければならない。
第 2 款　情報システム室
(情報システム室の管理)
第 22 条　ネットワーク管理者は、情報システム室の管理を行わせるため、情報システム室に設置された情報システムを管理する情報システム担当者のうちから、当該情報システム室の管理者を定めなければならない。
2　情報システム室に入室しようとする者は、その都度又はあらかじめ当該情報システム室の管理者の許可を受けなければならない。
3　情報システム室に入退室するものは、その際、前項の規定により入室の許可を受けたものであることが容易に判別できるよう入室許可証を見やすい位置に着用しなければならない。
4　情報システム室の管理者は、前 3 項に規定する事項のほか、その管理する情報システム室の入退室その他の管理に必要な事項について、情報システム室管理手順を定め、厳重に管理しなければならない。
(設備)
第 23 条　情報システム室は、情報システムに対する火災、水害、埃ほこり、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なければならない。
2　情報システム室を囲む外壁等の床下開口部は、すべてふさがなければならない。
3　情報システム室の管理者は、許可されていない者の情報システム室への入出を防止するため、情報システム室内に通ずる出入口を電子錠等によって施錠しなければならない。
4　情報システム室の管理者は、情報システム室内の機器類を、耐震対策及び防火措置等を講じた場所に設置するとともに、それらの配置については、地震、火災等の災害発生時に職員が円滑に避難できるよう配慮しなければならない。
第 3 款　ネットワーク
(接続)
第 24 条　ネットワーク管理者は、本市の情報システムを外部のネットワークに接続するときは、当該接続をその目的に照らして必要最小限のものとしなければならない。
2　ネットワーク管理者は、教育機関において教育の用に供する情報システム等を、この規則の対象となる情報システムと物理的に分離しなければならない。
(配線)
第 25 条　情報システム管理者は、その所管するネットワークの配線を、通信が傍受され、又は情報システムに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。
2　情報システム管理者及び契約により操作を認められた事業者以外の者は、本市のネットワークの配線を変更し、又は追加してはならない。
3　情報システム管理者は、その所管するネットワークの接続に当たっては、有線を使用しなければならない。
(職員が操作する端末装置等)
第 26 条　情報セキュリティ管理者は、その所管する執務室等に職員が不在となるときは、執務室等の施錠等により情報資産に対する侵害等及び盗難防止のための措置を講じなければならない。
2　情報システム管理者は、その所管する情報システムの端末装置について、パスワードを入力しなければ、オペレーティング・システム(以下「OS」という。)が起動しないように設定しなければならない。
第 3 節　技術的セキュリティ

第 1 款　情報システムの管理
(アクセス記録の取得等)
第 27 条　情報システム管理者は、第 10 条第 1 号に規定する行政情報を扱う情報システムについて、必要に応じ次に掲げる措置を講じなければならない。
(1)　各種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すべて取得し、一定の期間保存すること。
(2)　アクセス記録等が窃取され、改ざんされ、又は消去されないように必要な措置を講ずること。
(3)　定期的にアクセス記録等を監視すること。
(情報システムにおける作業記録の管理)
第 28 条　情報システム管理者は、その所管する情報システムにおいて行った変更等の作業についての記録を作成し、その記録を適切に管理しなければならない。
(障害記録の管理)
第 29 条　情報システム管理者は、職員から報告のあった情報システムの障害に関する処理又は問題等を障害記録として体系的に整理し、常に活用できるようにして保存しなければならない。
(情報システム仕様書等の管理)
第 30 条　情報システム管理者は、その所管する情報システムに係るネットワーク構成図及び情報システム仕様書等については、記録媒体にかかわらず、業務上必要と認められた者のみが閲覧できる場所に保管しなければならない。
(バックアップ)
第 31 条　情報システム管理者は、行政情報について、その行政情報の重要度に応じた分類ごとに期間を設定し、定期的にバックアップ用の複製をとらなければならない。
(電子メール)
第 32 条　情報システム管理者は、外部から外部への電子メール中継機能を不可能とするほか、電子メールに係る処理が情報システム全般に悪影響を及ぼすおそれがないよう必要な措置を講じなければならない。
2　職員は、電子メールを自動転送機能によりその所属する課等以外に転送してはならない。
3　職員は、電子メールで第 10 条第 1 号及び第 2 号に規定する行政情報を送信してはならない。
4　情報システム管理者は、電子メール 1 通の規定容量を定め、規定容量以上の電子メール送受信を不可能とする措置を講じなければならない。
5　情報システム管理者は、庁内で使用するすべてのメーリングリストについて、ウイルスが多数配布されるのを防ぐため、電子メール 1 通の規定容量をウイルスが混入しにくい程度の容量に制限しなければならない。
6　情報システム管理者は、電子メール用のサーバにおいて、電子メールアドレスごとの電子メール保存領域の規定容量を定め、当該規定容量を超えたときは、電子メール受診を不可能とする措置を講じなければならない。
(共用フォルダ)
第 33 条　情報システム管理者は、複数の端末等において共用で使用するデータ保存領域(以下「共用フォルダ」という。)を設定するときは、その中に保存される行政情報の重要度に応じた分類ごとに適切なセキュリティを講じなければならない。
(外部の者が利用できる情報システム)
第 34 条　情報システム管理者は、外部のものが利用することができる情報システムについて、必要に応じ他の情報システムと物理的に分離するほか、当該システムに係る情報セキュリティについては、特に強固な対策を講じなければならない。
(情報システムの入出力データ)
第 35 条　情報システム管理者は、その所管する情報システムに入力されるデータについて、適切な検査等を行い、当該入力されるデータが正確であることを確実にするための対策を講じなければならない。

2　情報システム管理者は、その所管する情報システムから出力されるデータについて、保存された行政情報の処理が正しく反映されたものであることを確保するようにしなければならない。
(業務目的以外での禁止行為)
第 36 条　職員は、業務のための目的以外で次に掲げる行為を行ってはならない。
(1)　インターネットの使用
(2)　情報システムへのアクセス行為
(ソフトウェア及びハードウェアに係る禁止行為)
第37条　職員は､ネットワーク管理者又は情報システム管理者の許可なく次に掲げる行為を行ってはならない。
(1)　アプリケーションソフトを追加し、変更し、又は削除する行為
(2)　電子計算機等の機器の OS 及びネットワーク等の設定を変更する行為
(3)　電子計算機等の機器を改造し、又は周辺機器を増設し、若しくは交換する行為
(4)　ネットワークの機器等を用いて電子計算機等の機器を増設し、又は外部のネットワークに接続する行為
(端末機器の使用停止)
第 38 条　情報セキュリティ部門責任者は、職員が第 36 条各号及び前条各号の行為(以下「不正行為」という。)を行ったと知ったときは、当該職員が所属する課等の情報セキュリティ管理者に対し、当該不正行為を中止させるために必要な措置を講ずるよう指示しなければならない。
2　情報セキュリティ部門責任者は、前項による措置を指示したにもかかわらず、不正行為の状況が改善されないと認めるときは、当該課等の情報セキュリティ管理者に対し、職員の端末機器の使用停止を命じるよう求めることができる。
3　情報セキュリティ部門責任者から前項による命令を求められた情報セキュリティ管理者は、職員に対し端末機器の使用停止を命じなければならない。
第 2 款　アクセス制御
(情報システム操作者の制限)
第 39 条　情報システム管理者は、その所属するネットワーク及び情報システムの端末機器を操作することができる職員(以下「操作職員」という。)を指定しなければならない。
2　前項により指定された操作職員以外の者は、当該ネットワーク及び情報システムの端末機器を操作してはならない。
3　情報システム管理者は、第 1 項で指定した操作職員以外の者が操作できないよう、パスワード等によって当該ネットワーク及び情報システムの端末機器の使用を制限しなければならない。
(ネットワーク経路制御)
第 40 条　情報システム管理者は、その所管するネットワークに対する不正なアクセスを防止するため、適切なネットワーク経路制御を施さなければならない。
(外部のネットワークとの接続)
第 41 条　情報システム管理者は、その所管する情報システムと外部のネットワークとの接続に際しては、当該外部のネットワークの通信網構成、機器構成、セキュリティレベル等を詳細に検討し、情報セキュリティに留意したネットワーク構成をとるものとし、本市のすべての情報資産に侵害等が生じないことを明確に確認した上で、情報セキュリティ最高情報統括責任者の許可を得て接続し、その利用に当たっては、ネットワーク管理者の適切な管理下で行わなければならない。
2　情報システム管理者は、前項の規定により接続した外部のネットワークのセキュリティに問題が認められ、本市の情報資産に侵害等が生ずるおそれがあるときは、情報セキュリティ最高情報統括責任者の判断に従い速やかに当該外部のネットワークを物理的に切り離さなければならない。
(自己管理パスワードに関する遵守事項)

第 42 条　職員は、自己の操作する情報システムの機器について設定され、自己が管理することとされるパスワード(以下この条において「自己管理パスワード」という。)に関し、次に掲げる事項を遵守しなければならない。
(1)　自己管理パスワードを秘密にし、当該パスワードの照会等には一切応じないこと。
(2)　自己管理パスワードのメモを作らないこと。
(3)　自己管理パスワードのけた数は十分な長さとし、文字列は推定しにくいものとすること。
(4)　本市の情報システム又は自己管理パスワードに対する侵害等のおそれがあるときは、当該パスワードを直ちに変更すること。
(5)　自己管理パスワードは、定期的に変更し、過去に使用したことのあるパスワードは、再び使用しないこと。
(6)　仮の自己管理パスワードが設定されているときは、直ちに当該パスワードを新しい自己管理パスワードに変更すること。
2　情報システム管理者は、職員の自己管理パスワードに関する遵守状況を厳重に管理し、前項各号に規定する事項を遵守しない職員に対しては遵守勧告を行い、当該職員が当該勧告に従わないときは、直ちに当該職員が自己管理パスワードを使用した操作ができなくなるような措置を講じなければならない。
(IC カード等の管理)
第 43 条　職員は、集積回路を内蔵し、パスワード等の情報を記録する機能を持つカードその他の職員個人の認証に用いるカード(以下「IC カード等」という。)を職員間で共有してはならない。
2　職員は、IC カード等を電子計算機器等の機器の IC カード等読み取り部に常時挿入した状態にしてはならない。
3　職員は、IC カード等を紛失したときは、直ちに当該カードを用いる情報システムの情報システム管理者に報告し、指示を仰がなければならない。
4　情報システム管理者は、IC カード等の紛失の報告があり次第、直ちに当該 IC カード等を使用した操作ができなくなるような措置を講じなければならない。
第 3 款　不正アクセス対策
(不正アクセスに対するネットワーク管理者の実施事項)
第44条　ネットワーク管理者は､不正アクセスに対する対策として次に掲げる事項を実施しなければならない。
(1)　電子計算機器等の機器を長時間入力待ちの状態で放置しないこと。
(2)　ソフトウェア及びシステムファイルの改ざんが生じていないことを随時確認すること。
(3)　本市のネットワークの負荷状況を監視すること。
(不正アクセスに対する予備的措置)
第 45 条　ネットワーク管理者は、不正アクセスを受けることが明確なときは、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。
2　ネットワーク管理者は、関係機関との連絡を密にして不正アクセスに関する情報の収集に努めなければならない。
(不正アクセス行為への対処)
第 46 条　ネットワーク管理者は、本市の情報システムが不正アクセスを受け、当該不正アクセスが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)その他の法令に違反するおそれがある場合には、当該行為に係る記録の保存に努めるとともに、関係機関との緊密な連携に務めなければならない。
第 4 款　ウイルス対策
(電子メールのウイルス検査)
第 47 条　情報システム管理者は、送受信する電子メールを電子メール用のサーバでウイルス検査し、ウイルス感染及び拡散の防止に努めなければならない。
(ウイルスに対する情報システム管理者の実施事項)

第 48 条　情報システム管理者は、ウイルス被害を予防するため、次に掲げる事項を実施しなければならない。
(1)　ウイルス情報に対する職員の注意を喚起すること。
(2)　常時、ウイルスに関する情報の収集に努めること。
(3)　情報システムの機器において、必要に応じてウイルス検査を行う最新のソフトウェア等の利用によりウイルス検査を行うこと。
(ウイルスに対する職員の遵守事項)
第 49 条　職員は、ウイルス被害を予防するため、次に掲げる事項を遵守しなければならない。
(1)　外部から情報システムにデータ及びソフトウェアを取り入れるときは、必ずウイルス検査を行うこと。
(2)　不審な電子メール及び不自然に添付されたファイルは、開かずに速やかに削除すること。
(3)　ネットワーク管理者の指示があったときは、直ちに電子計算機等の機器においてウイルス検査を行うこと。
(4)　ネットワーク管理者が提供するウイルス情報を常に確認すること。
(5)　情報資産がウイルスに感染したときは、感染した情報資産の使用を中止し、ネットワーク管理者に連絡して指示に従うこと。
第 5 款　情報システムの開発、導入、保守等
(情報システムの調達)
第 50 条　情報システム管理者は、情報システムの調達に当たっては、一般に公開する調達仕様書が情報セキュリティの確保に支障を及ぼすことのないよう配慮しなければならない。
2　情報システム管理者は、情報システムの調達に当たっては、機器及びソフトウェア等が情報セキュリティの確保に支障を及ぼすことがないよう必要な措置を講じなければならない。
(事業者との必須契約事項)
第 51 条　情報システム管理者は、情報システムの開発及び保守を事業者に委託するときは、自己並びに不正な行為への対策のため、次に掲げる事項を契約書等に定め、これを確実に実施させるようにしなければならない。
(1)　責任者及び監督者の配置
(2)　作業者及び作業範囲の指定
(3)　開発及び保守の際のアクセス制限
(4)　機器搬出入時の情報システム管理者の許可及び確認
(5)　開発及び保守記録の管理
(6)　マニュアル等の定められた場所への保管
(7)　開発及び保守を行った者の利用者パスワード等の当該開発及び保守終了後に不要となった時点での速やかな抹消
(8)　この規則の遵守及び本市の情報資産に関する守秘義務
(情報システムの導入)
第 52 条　情報システム管理者は、新に情報システム導入する場合には、既に稼動している情報システムに接続することにつきセキュリティ上の問題点がないかどうか事前に十分な試験を行わなければならない。
2　情報システム管理者は、前項の試験に使用したデータ及びその結果を一定期間保管しなければならない。
(ソフトウェアの更新及び保守)
第 53 条　情報システム管理者は、ソフトウェア等を更新し、又は修正プログラムを導入するときは、他の情報システムとの適合性等に問題がないかどうかの確認を行い、計画的に更新し、又は導入しなければならない。
2　情報システム管理者は、情報セキュリティに重大な影響を及ぼす不具合に対しては、遅滞なく修正プログラムを導入する等の対応を行わなければならない。
(機器の修理)
第 54 条　情報システム管理者は、記憶媒体の含まれる機器を事業者に修理させるときは、当該記憶媒体に記録

させた行政情報が消去された状態で修理を行わせなければならない。ただし、内容を消去することが難しい場合を除く。

第4節　運用

(規則の遵守状況の確認)

第55条　情報セキュリティ管理者は、課等においてこの規則が遵守されるかどうかについて、また、情報セキュリティ上の問題が発生していないかについて常に確認を行い、問題が発生していたときは、遅滞なく情報セキュリティ部門管理者及びネットワーク管理者に報告しなければならない。

2　情報セキュリティ部門責任者及びネットワーク管理者は、発生した情報セキュリティ上の問題に、速やかに、かつ、適切に対処するとともに、その問題の重要度に応じて情報セキュリティ最高情報統括責任者に報告しなければならない。

3　職員は、この規則に対する違反が発生したことを知ったときは、直ちに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。

4　情報セキュリティ管理者は、前項の違反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判断したときは、緊急時対応計画に従って対処しなければならない。

(アクセス記録等の調査及び監視)

第56条　ネットワーク管理者及び情報セキュリティ管理者は、情報セキュリティを確保するためやむを得ない場合には、必要最小限の範囲で、それぞれの所管する本市のネットワーク及び情報システムにおけるアクセス記録及び電子メール等の内容を調査及び監視する権限を有する。

第5節　緊急時の対応計画

(侵害時の調査及び連絡)

第57条　職員は、情報セキュリティに関する侵害等を発見したときは、直ちに情報セキュリティ管理者に報告し、情報セキュリティ管理者の指示に従い必要な措置を講じなければならない。

2　情報セキュリティ管理者は、当該侵害等が発生した原因、確認した被害及び影響範囲について速やかに調査し、情報セキュリティ実施手順に定める連絡先に報告しなければならない。

(侵害等への対処)

第58条　ネットワーク管理者及び情報セキュリティ管理者は、侵害等に対処するため次に掲げる事項を実施しなければならない。

(1)　次に掲げる状況が生じたときは、情報セキュリティ実施手順に定めた連絡先へ遅滞なく連絡しなければならない。

ア　サイバーテロ又はその他の侵害等により情報資産に重大な被害が生ずるおそれがあるとき。

イ　侵害等が不正アクセスその他の犯罪であると思慮されるとき。

ウ　本市のネットワークを経由して他の情報システムに被害を与えるおそれがあるとき。

エ　本市の情報システムに関する被害が生じたとき。

オ　アからエまでに掲げるもののほか、本市の情報資産に係る被害が発生したとき。

(2)　次に掲げる侵害等が発生し、本市の情報資産を防護するためにやむを得ないときは、本市のネットワークを切断しなければならない。

ア　本市のネットワークに対して異常なアクセスが継続しているとき、又は不正アクセスが行われていることが判明したとき。

イ　本市の情報システムの運用に著しい支障を来すアクセスが継続しているとき。

ウ　ウイルス等の不正プログラムがネットワーク経由で本市のネットワーク内に広がっているとき。

エ　その他本市の情報資産に係る重大な被害が想定されるとき。

(3)　次に掲げる侵害等が発生し、本市の情報資産を防護するため本市の情報システムの停止がやむを得ないと

きは、本市の情報システムを停止しなければならない。
ア　ウイルス等不正プログラムが本市の情報資産に深刻な被害を及ぼしているとき。
イ　災害時により本市の情報システムに電源を供給することが危険又は困難なとき。
ウ　その他の本市の情報資産に係る重大な被害が想定されるとき。
(4)　侵害等に係る情報システムのアクセス記録及び現状を保存し、証拠保全に努めるとともに、侵害等に対処した経過を記録しなければならない。
(再発防止の措置)
第 59 条　ネットワーク管理者及び情報セキュリティ管理者は、情報セキュリティ侵害等に係る要因分析を実施し、必要に応じてこの規則及び情報セキュリティ実施手順の改善を行い、侵害等の再発を防止しなければならない。
第 6 節　法令の遵守等
(法令の遵守)
第 60 条　職員は、職務の遂行において使用する情報資産について、次に掲げる法令等を遵守しなければならない。
(1)　不正アクセス行為の禁止等に関する法律
(2)　著作権法(昭和 45 年法律第 48 号)
(3)　菊池市個人情報保護条例(平成 17 年菊池市条例第 11 号)
(違反者への対応)
第 61 条　この規則に違反した職員については、その違反の重大性及び発生した侵害等の状況等に応じて懲戒処分の対象とする。
第 7 節　評価及び見直し
(情報セキュリティの点検)
第 62 条　ネットワーク管理者及び情報セキュリティ部門責任者は、本市のネットワーク及び情報システムの情報セキュリティについての点検を定期的に行い、その結果を情報セキュリティ最高情報統括責任者に報告しなければならない。
(情報セキュリティ規則の見直し)
第 63 条　情報セキュリティ最高情報統括責任者は、情報セキュリティに関し、新たな対策が必要な事態が発生したとき、又は点検の結果により何らかの対策が必要と判断されるときは、この規則について必要な部分の見直しを行わなければならない。
第 3 章　雑則
(その他)
第 64 条　この規則の施行に関し必要な事項は、市長が別に定める。
附　則
この規則は、平成 17 年 3 月 22 日から施行する。
附　則(平成 19 年規則第 9 号)
この規則は、平成 19 年 4 月 1 日から施行する。ただし、地方自治法の一部を改正する法律(平成 18 年法律第 53 号)附則第 3 条第 1 項の規定により、同日以後在職する収入役の退職の日の翌日から施行する。