生駒市訓令甲第１１号

生駒市セキュリティ対策基準を次のように定める。

平成１９年１２月２５日

生駒市長　山下　真

生駒市情報セキュリティ対策基準

生駒市情報セキュリティ対策基準（平成１６年２月生駒市訓令甲第１号）の全部を改正する。

目次

第１章　総則

（趣旨）

第１条　この訓令は、生駒市情報セキュリティに関する規則（平成１６年２月生駒市規則第１号。以下「規則」という。)に基づき、情報セキュリティを確保するために遵守すべき行為等の基準に関する事項を定めるものとする。

（定義）

第２条　この訓令において、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)　部等　市長事務部局の公室、部及び局、消防本部、水道局、議会事務局並びに教育委員会事務局の部をいう。

(2)　課等　市長事務部局の課、病院建設準備室、人権文化センター、高山竹林園、子どもサポートセンター、清掃リレーセンター、清掃センター、衛生処理場、花のまちづくりセンター、竜田川浄化センター及び生駒市立保育所条例（昭和３０年３月生駒市条例第８号）に定める保育所、出納室、消防本

部の課及び消防署、議会事務局、水道局の課及び浄水場、教育委員会事務局の課、学校給食センター、中央公民館、南コミュニティセンター、北コミュニティセンター、図書会館、芸術会館並びに生駒市立学校設置条例（昭和３９年４月生駒市条例第１３号）に定める小学校、中学校及び幼稚園、選挙管理委員会事務局、監査委員事務局並びに農業委員会事務局をいう。

(3)　情報機器等　本市の情報資産のうち、サーバ等（サービスを提供するコンピュータ及びホストコンピュータをいう。)、端末（サーバ等からのサービスの提供を受けるクライアントコンピュータ及び独立して利用される機器をいう。)、通信回線及び通信回線装置並びに記録媒体等の総称をいう。

(4)　管理者権限　情報システムを管理するために必要なアクセス権限をいう。

第２章　組織及び体制

第１節　組織

（情報セキュリティ委員会）

第３条　本市における情報セキュリティに関する最高意思決定を行うため、生駒市情報セキュリティ委員会（以下「委員会」という。)を置く。

２　委員会は、次に掲げる事項を審議する。

(1)　情報セキュリティに関する組織横断的な調整に関すること。

(2)　情報セキュリティポリシー（以下「ポリシー」という。)の運用及び見直しに関すること。

(3)　情報セキュリティに関する事案の調査に関すること。

(4)　情報セキュリティの監査の実施に関すること。

(5)　最高情報統括責任者が必要と認める事項に関すること。

(6)　その他情報セキュリティに係る重要事項に関すること。

３　委員会は、最高情報統括責任者、ネットワーク管理者及び統括情報セキュリ

ティ責任者をもって組織する。

4　委員会の長は、最高情報統括責任者とする。

5　委員会の庶務は、情報政策課において処理する。

6　委員会は、特別な対応を必要とする情報セキュリティ対策が生じたときは、目的に応じた専門チームを編成することができる。

7　委員会は、情報セキュリティについて必要があるときは、専門家の助言を求めることができる。

第２節　体制

（最高情報統括責任者）

第４条　本市に最高情報統括責任者を置く。

2　最高情報統括責任者は、市長をもって充てる。

3　最高情報統括責任者は、本市における情報資産に対する情報セキュリティ対策を統括する。

（ネットワーク管理者）

第５条　本市にネットワーク管理者を置く。

2　ネットワーク管理者は、企画財政部長をもって充てる。

3　ネットワーク管理者は、最高情報統括責任者を補佐するとともに、最高情報統括責任者が不在のときは、自らの判断により必要かつ十分な措置を行うものとする。

4　ネットワーク管理者は、次に掲げる事項についての権限及び責務を有する。

(1)　本市のネットワークにおける情報セキュリティに関すること。

(2)　本市のネットワークにおける開発、運用、保守等を行うこと。

(3)　統括情報セキュリティ責任者、情報セキュリティ責任者及びシステム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こと。

5　ネットワーク管理者は、次に掲げる事項について、情報政策課長に許可等を

行わせることができる。

(1)　第２５条に規定する電算室の入退出及び利用者の記録に関すること。

(2)　第３０条第２項の規定による端末の外部持出しに関すること。

(3)　第４７条第１項の規定による端末の改造、機器の増設及び設定の変更に関すること。

(4)　第４７条第３項の規定による端末のソフトウエアに関するセキュリティ機能の設定の変更に関すること。

(5)　第４８条の規定による端末のネットワーク接続に関すること。

(6)　第５１条第２項の規定による定められた使用許諾要件を満たさないソフトウェアの導入に関すること。

(7)　第５８条第１項の規定による無線ＬＡＮの使用に関すること。

(8)　その他ネットワーク管理者が必要と認める事項

（統括情報セキュリティ責任者）

第６条　本市に統括情報セキュリティ責任者を置く。

２　統括情報セキュリティ責任者は、部等の長（小学校及び中学校にあっては、教育長）をもって充てる。

３　統括情報セキュリティ責任者は、所管する課等の情報セキュリティ責任者を統括し、情報セキュリティ対策に関する連絡及び調整を担当する。

４　統括情報セキュリティ責任者は、ポリシーの遵守に関する意見の集約、職員等への研修等の指示及び助言を行う権限を有する。

（情報セキュリティ責任者）

第７条　本市に情報セキュリティ責任者を置く。

２　情報セキュリティ責任者は、課等の長をもって充てる。

３　情報セキュリティ責任者は、所管組織の情報セキュリティに関する権限及び責任を有する。

４　情報セキュリティ責任者は、所管組織内におけるポリシーの遵守に関する権限及び責任を有する。

５　情報セキュリティ責任者は、ポリシーの遵守に当たり、不明な点等に関し、適宜統括情報セキュリティ責任者及びネットワーク管理者の指示を受けるものとする。

（システム管理者）

第８条　情報セキュリティ責任者は、所管組織内に情報システムを有するときは、その運用及び管理を行うシステム管理者を指名し、情報システムを適切に管理しなければならない。

２　システム管理者は、情報セキュリティ責任者の下、担当する情報システムに関する開発、導入、運用等の具体的な作業を行うとともに、情報セキュリティ責任者を補佐しなければならない。

（研修責任者）

第９条　本市に研修責任者を置く。

２　研修責任者は、職員課長（小学校及び中学校にあっては、教育長）をもって充てる。

３　研修責任者は、情報セキュリティに関する研修を行う権限及び責任を有する。

（専門家による助言）

第１０条　情報セキュリティについて高度な専門的知識を必要とするときは、外部の専門家の助言を得ることができる。

第３章　情報の分類と管理

（情報の分類）

第１１条　本市の情報は、次のとおり分類を行い、その重要性を踏まえた管理を行わなければならない。

(1)　重要性分類Ａ　個人情報及び業務上特に高度の秘密に属する情報

(2)　重要性分類Ｂ　対外的に秘密保持を要する情報

(3)　重要性分類Ｃ　上記以外の情報

２　情報の重要性分類の指定は、情報セキュリティ責任者が行う。

３　情報セキュリティ責任者は、取り扱う情報の重要性を考慮し、所管する情報システムについても第１項の分類に従った重要性分類を行わなければならない。

４　情報セキュリティ責任者は、情報の重要性分類の結果を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。

５　統括情報セキュリティ責任者は、前項の規定による報告を受けた内容を整理し、情報資産台帳を管理しなければならない。

（情報の管理）

第１２条　情報セキュリティ責任者は、職員等が作成し、入手し、利用し、保管し、送信し、運搬し、提供し、公表し、及び廃棄する情報について管理責任を有する。

２　情報セキュリティ責任者は、重要な情報(情報の重要性分類Ａ及び重要性分類Ｂに該当する情報をいう。以下同じ。)に関しては、情報が複製された場合の所在を明確にしておかなければならない。

３　情報セキュリティ責任者は、課等において取り扱う情報の内容及び重要性分類が所属の職員等に容易に判別できるよう、適切な管理を行わなければならない。

４　情報セキュリティ責任者は、所管する情報について、情報の重要性分類に従ったアクセス権限を定めなければならない。

５　情報セキュリティ責任者は、重要性分類Ａに該当する情報について、原則として暗号化を施して管理しなければならない。

6　職員等は、本市が管理する情報について、情報の重要性分類に従って適切に取り扱わなければならない。

7　職員等は、情報セキュリティ責任者の許可があるときを除き、重要な情報を本市が管理する区域外(以下「外部」という。)へ送付及び持出しをしてはならない。

（外部での情報処理）

第１３条　最高情報統括責任者は、職員等が外部で情報処理を行う場合における安全管理措置を定めなければならない。

2　職員等は、外部で情報処理を行う場合には、情報セキュリティ責任者の許可を得なければならない。

3　前項の場合において、職員等は、第１項の安全管理措置を遵守しなければならない。

4　第２項の場合において、職員等は、重要性分類Ａの情報について、個人で所有する情報機器等で情報処理を行ってはならない。

第４章　人的セキュリティ

第１節　職員等の遵守事項

（職員等の責務）

第１４条　職員等は、情報セキュリティ対策の実施に当たり、次に掲げる事項を遵守しなければならない。

(1)　ポリシーに定められている事項

(2)　ポリシーについて不明な点又は遵守することが困難な点があるときは、速やかに情報セキュリティ責任者に報告し、指示等を受けること。

(3)　不適切な情報の発信、利用を許可されていないサーバ等へのアクセス等の自らが加害者になる行為を行わないこと。

(4)　異動、退職等により業務を離れるときは、知り得た情報を秘匿するこ

と。ただし、当該情報が公となったときは、この限りでない。

（ＩＤ及びパスワードの管理）

第１５条　職員等は、自己の管理するＩＤ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)　共用で利用しているＩＤは、当該ＩＤの利用者以外に利用させてはならない。

２　職員等は、自己の管理するパスワードに関し、第三者に漏えいしないよう厳重に管理しなければならない。

（カード等の管理）

第１６条　職員等は、認証に用いるカード等（以下「カード等」という。)に関し、不正利用を防止するため厳重に管理しなければならない。

２　職員等は、カード等を紛失したとき等は、第７５条第１項の規定による対応を行わなければならない。

３　ネットワーク管理者及び情報セキュリティ責任者は、職員等がカード等を紛失したとき等において、利用停止措置その他適切な措置を講じなければならない。

（個人が所有する情報機器等の利用禁止）

第１７条　職員等は、個人が所有する情報機器等を庁舎内に持ち込み、業務に利用してはならない。

（情報セキュリティ責任者の責務等）

第１８条　情報セキュリティ責任者は、職員等が常にポリシー及び情報セキュリティ実施手順を閲覧できるように掲示しなければならない。

２　情報セキュリティ責任者は、新たに採用された職員等に対し、必要に応じ、ポリシーを遵守する旨の同意書の提出を求めることができる。

（職員等以外の者による情報資産の利用）

第１９条　情報セキュリティ責任者は、外部委託事業者等に情報資産を利用させるときは、ポリシーの内容を遵守させる等利用に関する適切な指導を行わなければならない。

第２節　情報セキュリティ研修

（研修の実施）

第２０条　最高情報統括責任者は、職員等に対し、ポリシーについての啓発を行わなければならない。

２　研修責任者は、ポリシーに関する研修を実施しなければならない。

３　情報セキュリティ責任者は、情報セキュリティ責任者向けの研修を受けなければならない。

４　システム管理者は、システム管理者向けの研修を受けなければならない。

５　新たに採用された職員等は、新規採用職員向けの研修を受けなければならない。

６　職員等は、職員向けの研修を受けなければならない。

（研修計画の作成）

第２１条　研修責任者は、毎年度、情報セキュリティに関する研修について、対象者、内容、実施時期等を定めた研修計画を作成しなければならない。

２　研修責任者は、毎年度、委員会に情報セキュリティに関する研修の実施状況を報告しなければならない。

（研修結果の評価及び見直し）

第２２条　研修責任者は、アンケート調査等により、研修を受講した者が目標とする水準に達したかどうか評価を行わなければならない。

２　研修責任者は、前項の結果により、必要に応じて研修の内容を見直さなければならない。

第５章　物理的セキュリティ

第１節　事務室等

（事務室等での管理）

第２３条　業務を行う場所（以下「事務室等」という。)の施設に関する情報セキュリティ対策は、各施設の管理責任者及び情報セキュリティ責任者が行わなければならない。

２　情報セキュリティ責任者は、事務室等に設置した情報機器等に対して、盗難防止のための適切な措置を講じなければならない。

第２節　電算室

（電算室の設置）

第２４条　ネットワーク管理者は、重要性分類Ａに該当する情報システム等を設置するときは、原則として外部からの侵入が容易にできないよう外壁等に囲まれた管理区域（以下「電算室」という。)に設置しなければならない。

２　ネットワーク管理者は、電算室の情報セキュリティ対策について、適切な措置を講じなければならない。

３　情報セキュリティ責任者は、重要性分類Aに該当する情報システム等を電算室以外の場所に設置するときは、前項の規定に準じた措置を講じなければならない。

（電算室の入退室管理）

第２５条　ネットワーク管理者は、電算室への入退室を許可された者に限定し、利用者の記録を行う等の適切な管理を行わなければならない。

第３節　情報機器等に対する管理策

（取付け）

第２６条　情報セキュリティ責任者は、情報機器等の取付けを行うときは、動作環境及び情報セキュリティに配慮しなければならない。

（停電、落雷等への対策）

第２７条　システム管理者は、停電による電力供給停止等及び落雷等による過電流から情報機器等を保護するため、適切な措置を講じなければならない。

（物理的損傷への対応）

第２８条　システム管理者は、物理的損傷から通信回線、電源ケーブル等を保護するため、適切な措置を講じなければならない。

（外部に設置するサーバ等）

第２９条　情報セキュリティ責任者は、外部にサーバ等を設置するときは、その設置場所について、最高情報統括責任者の承認を受けなければならない。

２　最高情報統括責任者は、前項の承認を行うときは、ネットワーク管理者に、当該設置場所となる施設における物理的安全対策を調査させるものとする。

（外部への端末及び記録媒体等の持ち出し）

第３０条　職員等は、ネットワーク管理者の許可なく端末を外部へ持ち出してはならない。

２　職員等は、情報セキュリティ責任者の許可なく記録媒体等を外部へ持ち出してはならない。

３　情報セキュリティ責任者は、端末又は記録媒体等の輸送を行うときは、当該輸送に係る記録を作成するとともに、信頼できる者を選任し、複製の禁止及び物理的保護を行わなければならない。

４　職員等は、外部に持ち出す端末又は記録媒体等について、厳重かつ適切に管理するとともに、破損し、若しくは紛失し、又は盗難されたときは、直ちに情報セキュリティに関する事案への対応に従って連絡を行わなければならない。

（情報機器等の廃棄）

第３１条　職員等は、情報機器等の廃棄に関し、次に掲げる事項を実施しなければならない。

(1)　情報機器等に記録された情報について、復元できないように措置を講ずること。

(2)　廃棄する情報機器等から内部情報が消去されていることを確認すること。

(3)　重要な情報を記録した情報機器等については、廃棄処理に係る日時、作業実施者、処理内容等を記録すること。

第６章　技術的対策及び運用管理

第１節　サーバ等に関する情報セキュリティ対策

（アクセス制御）

第３２条　ネットワーク管理者及びシステム管理者は、サーバ等の情報を適切に保護するため、サーバ等のアクセス制御を行わなければならない。

（アクセス記録等の取得及び管理）

第３３条　ネットワーク管理者及びシステム管理者は、重要度に応じてアクセス記録等を取得し、取得したアクセス記録等について、厳重に管理しなければならない。

（システム変更等の記録及び作業の確認）

第３４条　ネットワーク管理者及びシステム管理者は、情報システムの変更等に当たって、作業内容の記録を作成し、かつ、盗難、改ざん等を防止するため、当該記録を適切に管理しなければならない。

２　ネットワーク管理者又はシステム管理者が外部委託事業者とともにシステム変更等の作業を行うときは、互いにその作業を確認しなければならない。

（障害に係る記録等）

第３５条　ネットワーク管理者及びシステム管理者は、情報システムの障害に対する処理を体系的に記録し、必要なときに活用できるよう管理しなければならない。

（情報システム仕様書等の管理）

第３６条　ネットワーク管理者及びシステム管理者は、ネットワーク構成図、情報システムに関する仕様書等（電磁的に記録されたものを含む。以下これらを「仕様書等」という。)を厳重に管理しなければならない。

（ファイルサーバの設定）

第３７条　ネットワーク管理者は、ファイルサーバ（ファイルを保存し、ファイル共有の機能を提供するサーバをいう。)を課等の単位で構成し、職員等が他の課等のフォルダ及びファイルを閲覧及び使用を行うことができないよう設定しなければならない。

（バックアップ）

第３８条　ネットワーク管理者及びシステム管理者は、サーバ等に記録された情報について、完全性又は可用性に応じてバックアップを行わなければならない。

２　前項のバックアップを行うときは、あらかじめバックアップを行う周期及び保管期間を決定しなければならない。

３　バックアップに用いた記録媒体等は、定められた手順に従い適切に管理しなければならない。

４　ネットワーク管理者及びシステム管理者は、第１項のバックアップが確実に行われているかを定期的に確認しなければならない。

（サーバ等の二重化）

第３９条　ネットワーク管理者及びシステム管理者は、サーバ等の障害発生時における情報等の滅失及び情報システムの運用停止を回避するため、情報システムの可用性に応じて、サーバ等を二重化しなければならない。

（メールサーバの運用）

第４０条　ネットワーク管理者は、メールサーバを運用するときは、第三者から

の不正な利用等を防止するため、適切な措置を講じなければならない。

（電子署名、暗号化等）

第４１条　ネットワーク管理者は、電子署名及び暗号化の方法並びに鍵の管理方法について、適切な手順を定めなければならない。

２　職員等は、外部に送るデータが完全であることを担保することが必要なときは、定められた電子署名の方法により送信しなければならない。

３　職員等は、定められた暗号化の方法を用いなければならない。

（情報システムの監視等）

第４２条　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する事案を検知するため、情報システムの監視を行わなければならない。

２　ネットワーク管理者は、外部と常時接続するときは、侵入検知システム等による監視を行わなければならない。

３　ネットワーク管理者及びシステム管理者は、監視により得られた結果について、消去され、又は改ざんされないための必要な措置を講じ、安全な場所に保管しなければならない。

４　ネットワーク管理者及びシステム管理者は、正確な監視結果を得るため、情報システムを正確な時刻に設定しなければならない。

（情報の調査）

第４３条　情報セキュリティに関する事案等の対処のため、委員会により承認された者は、アクセス記録、電子メールの送受信記録等の情報を調査することができる。

（利用者ＩＤ及びパスワードの管理）

第４４条　ネットワーク管理者及びシステム管理者は、所管する情報システムにおける利用者ＩＤに関して、適切に管理しなければならない。

２　ネットワーク管理者及びシステム管理者は、職員等のパスワードに関する情

報について、厳重に管理しなければならない。

（管理者権限）

第４５条　ネットワーク管理者及びシステム管理者は、サーバ等の誤操作による意図しない動作及び不正利用を防止するため、管理者権限等の特権を付与したＩＤを利用できる者を必要最小限とし、当該ＩＤのパスワードの漏えい等が発生しないよう、厳重に管理しなければならない。

（サーバ等へのログイン）

第４６条　システム管理者は、サーバ等へのログインについて、不正なログインを防止するため、適切な情報セキュリティ対策を施すとともに、その手順を定めなければならない。

第２節　端末に関する情報セキュリティ対策

（情報機器等の変更等）

第４７条　職員等は、端末に対し、改造、機器の増設及び設定の変更を行ってはならない。ただし、業務上特別の理由があるときは、ネットワーク管理者の許可を得て行うことができる。

２　職員等は、事務室等に設置された通信回線及び通信回線装置に対し、改造、設定の変更、装置の追加等を行ってはならない。

３　職員等は、端末のソフトウエアに関するセキュリティ機能の設定をネットワーク管理者の許可なく変更してはならない。

（ネットワークへの接続）

第４８条　職員等は、端末をネットワークに接続するときは、ネットワーク管理者の許可を得なければならない。

（業務目的以外の使用の禁止等）

第４９条　職員等は、端末及び情報システムを業務目的以外に使用してはならない。

２　ネットワーク管理者は、業務目的以外の電子メールの使用及びインターネットへのアクセスを防止する措置を講じなければならない。

３　ネットワーク管理者は、業務目的以外の情報システムへのアクセス等を行った職員等に対して、当該職員等が所属する情報セキュリティ責任者を通じて、中止及び改善を指導しなければならない。

（離席時の端末設定）

第５０条　職員等は、端末の操作中に離席するときは、離席中の不正操作等を防止するため、ログオフ等必要な措置を講じなければならない。

（業務に利用するソフトウェア）

第５１条　ネットワーク管理者は、業務において利用するソフトウェアの使用許諾要件を定めなければならない。

２　職員等は、定められた使用許諾要件を満たさないソフトウェアを端末に導入してはならない。ただし、業務上特別の理由があるときは、ネットワーク管理者の許可を得ることにより導入することができる。

（電子メールの利用）

第５２条　職員等は、電子メールの利用において公序良俗に反することのないよう、情報セキュリティ実施手順に定める利用方法を遵守しなければならない。

第３節　ネットワークに関する情報セキュリティ対策

（通信回線及び通信回線装置の管理）

第５３条　ネットワーク管理者は、ネットワークの構築に当たり、適切な通信回線及び通信回線装置を使用し、十分なセキュリティ対策を講じなければならない。

２　ネットワーク管理者は、通信回線及び通信回線装置の設定に係る情報及び関連する文書を適切に管理しなければならない。

（ネットワークのアクセス制御）

第５４条　ネットワーク管理者は、ネットワークにおけるアクセス制御について、不正利用等を防止するため、適切な措置を講じなければならない。

（外部からのアクセス等）

第５５条　情報セキュリティ責任者は、本市が管理するネットワーク及びサーバ等に外部からアクセスする仕組みを構築するときは、最高情報統括責任者の承認を受けなければならない。

２　情報セキュリティ責任者は、電子申請のシステムその他職員等以外の者が使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。

（外部にある情報システムへのアクセス）

第５６条　情報セキュリティ責任者は、本市が管理する区域から、専用回線、インターネット等を通じて、外部にある情報システムにアクセスする仕組みを構築するときは、あらかじめネットワーク管理者の承認を受けなければならない。

（外部へのネットワーク接続）

第５７条　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行うときは、あらかじめ最高情報統括責任者の承認を受けなければならない。

２　情報セキュリティ責任者は、外部ネットワークとの接続に関する契約を締結するときは、当該外部ネットワークの瑕疵（かし）によるデータの漏えい、破壊若しくは改ざん又はシステムダウン等による業務への影響が生ずる場合に備え、当該外部ネットワークの管理責任者に対して損害賠償責任を担保しなければならない。

３　ネットワーク管理者は、外部へのネットワーク接続を行う際には、その接続口を必要最小限にしなければならない。

４　ネットワーク管理者は、外部へのネットワーク接続を行ったときは、適切な

情報セキュリティ対策及び運用管理を行わなければならない。

（無線ＬＡＮの使用）

第５８条　情報セキュリティ責任者は、無線ＬＡＮを構築するときは、あらかじめネットワーク管理者の許可を得なければならない。

２　ネットワーク管理者及び情報セキュリティ責任者は、無線ＬＡＮの使用においては、接続する端末及び利用者の認証並びに暗号化等の情報セキュリティ対策を行わなければならない。

第４節　不正プログラム対策

（不正プログラム対策）

第５９条　ネットワーク管理者は、コンピュータウイルス等の不正プログラム対策に関し、次に掲げる事項を実施しなければならない。

(1)　不正プログラム対策の方法、感染時の対応手順等を作成し、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への周知を行うこと。

(2)　情報セキュリティ責任者による不正プログラム対策の実施状況を適宜確認し、改善が必要なものについて改善を指導すること。

(3)　不正プログラムに関する情報を収集すること。

(4)　前号の規定により収集されたもののうち、職員等の啓発、被害の未然防止等に効果的なものについては、職員等への周知を行うこと。

（情報セキュリティ責任者による不正プログラム対策）

第６０条　情報セキュリティ責任者は、所管するサーバ等及び端末の不正プログラム対策に関し、次に掲げる事項を実施しなければならない。

(1)　所管の情報システムにおける不正プログラム対策の実施状況を定期的にネットワーク管理者及び統括情報セキュリティ責任者に報告すること。

(2)　所管するサーバ等及び端末に、不正プログラム対策ソフトウエアを常駐させ、不正プログラムのチェックを定期的に実施すること。

(3)　不正プログラム対策ソフトウエア及び当該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つこと。

(4)　不正プログラムの感染が確認されたときは、定められた手順に従い対応を行った後、被害の有無にかかわらず、第７５条第１項の規定による対応を行うこと。

(5)　所属の職員等に対し、不正プログラム対策に関する啓発を行うこと。

（職員等による不正プログラム対策）

第６１条　職員等は、次に掲げる事項を遵守しなければならない。

(1)　不審なファイルを容易に開かないこと。

(2)　外部からデータ又はソフトウエアを取り入れるときは、不正プログラムのチェックを実施すること。

(3)　ネットワーク管理者が提供する不正プログラムに関する情報を常に確認すること。

(4)　不正プログラム対策ソフトウェアの設定を変えないこと。

(5)　端末に対して、不正プログラム対策のフルチェックを定期的に実施すること。

(6)　不正プログラムに感染したときは、直ちにネットワークからの切断又は機器の電源遮断を行い、第７５条第１項に規定する対応を行うこと。

第５節　不正アクセス対策

（不正アクセス対策）

第６２条　ネットワーク管理者及びシステム管理者は、アクセス権限のない者が情報システムにアクセスすることを防止するため、不正アクセス対策を講じなければならない。

（攻撃への対応）

第６３条　最高情報統括責任者及びネットワーク管理者は、サーバ等に攻撃を受

けることが明確になったときは、システムの停止その他必要な措置を講じなければならない。

２　前項の場合において、最高情報統括責任者及びネットワーク管理者は、関係機関と連絡を密にして当該攻撃に関する情報の収集に努めなければならない。

（攻撃の監視）

第６４条　ネットワーク管理者及び統括情報セキュリティ責任者は、職員等及び外部委託事業者の端末等からの内部のサーバ等又は外部に対する攻撃を監視しなければならない。

（職員等による不正アクセス）

第６５条　ネットワーク管理者及び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が明らかになったときは、当該職員等が所属する課等の情報セキュリティ責任者に通知し、適切な措置を求めなければならない。

第７章　情報システムの開発、運用及び保守

（情報システムの調達）

第６６条　情報セキュリティ責任者は、情報システムを調達するときは、仕様書等が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。

２　システム管理者は、機器及びソフトウェアを調達するときは、当該機器及びソフトウェアが情報セキュリティ上の問題にならないかどうか確認しなければならない。

（情報システムの変更管理）

第６７条　情報セキュリティ責任者は、所管する重要な情報システムを変更するときは、あらかじめネットワーク管理者及び統括情報セキュリティ責任者と協議しなければならない。

２　システム管理者は、所管する情報システムの追加、変更及び廃棄を行ったときは、その際の設定、構成等の履歴を記録しなければならない。

（情報システムの開発、運用及び保守）

第６８条　情報セキュリティ責任者は、情報システムの開発、運用及び保守に関し、あらかじめ統括情報セキュリティ責任者と協議しなければならない。

２　情報セキュリティ責任者は、情報システムの開発、運用及び保守における事故及び不正行為対策のため、適切な措置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６９条　システム管理者は、情報システムに入力されるデータについて、それが正確であることを確実にするため、適切な措置を講じなければならない。

２　システム管理者は、情報システムから出力されるデータについて、保存された情報の処理が正しく反映され、適切に出力されることを確保しなければならない。

（ソフトウェアの保守及び更新）

第７０条　システム管理者は、ソフトウェア（修正プログラムを含む。)の保守及び更新を行うときは、情報システムに影響を与えないかどうかを調査しなければならない。

２　システム管理者は、前項の規定による調査の結果を受けてソフトウェアの更新を速やかに行わなければならない。

（機器等の定期保守及び修理）

第７１条　システム管理者は、機器等の保守を定期的に実施しなければならない。

２　システム管理者は、外部委託事業者に機器等の修理を委託するときは、機密保持について契約書に明記しなければならない。

（情報システムの外部委託）

第７２条　情報セキュリティ責任者は、情報システムの開発、運用及び保守を外部委託事業者に委託するときは、必要に応じて機密保持等の情報セキュリティ

に関する事項を契約書に明記しなければならない。

（外部委託事業者の管理状況等の調査）

第７３条　情報セキュリティ責任者は、委託を行うときは、事前に外部委託事業者における情報の保護等に関する管理体制等について調査しなければならない。

２　情報セキュリティ責任者は、委託契約を履行中の外部委託事業者に対し、必要に応じ当該委託に係る情報セキュリティ対策の実施状況について調査しなければならない。

第８章　情報セキュリティに関する事案への対応

（情報セキュリティに関する情報の収集等）

第７４条　ネットワーク管理者は、情報セキュリティ技術の向上、情報セキュリティに関する事案の発生時の対応方法等に関する情報について、収集を行わなければならない。

２　情報セキュリティ責任者は、必要に応じて個別に情報を収集しなければならない。

３　最高情報統括責任者は、緊急度の高い情報及び職員等にとって必要な情報は、すべての職員等に通知しなければならない。

（情報セキュリティに関する事案への対応）

第７５条　情報セキュリティに関する事案が発生したときは、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、再発防止の措置を講ずるため、次に掲げる手順により対応しなければならない。

(1)　情報セキュリティに関する事案を認めた者は、当該事案の発生時間、発生箇所、発生内容、想定される原因、被害の範囲等を速やかに情報政策課長に連絡するとともに、所管の情報セキュリティ責任者に報告する。

(2)　報告を受けた情報セキュリティ責任者は、発生した情報セキュリティに

関する事案に対して証拠保全、被害拡大の防止等必要な対応を行うとともに、ネットワーク管理者及び統括情報セキュリティ責任者に報告する。

(3)　統括情報セキュリティ責任者は、当該事案のレベルに応じて、最高情報統括責任者に連絡するとともに、委員会、関係部門（警察及び関係機関を含む。)等に連絡する。

(4)　最高情報統括責任者は、被害拡大の防止のため、情報システムを緊急に停止する必要があると認められるときは、ネットワーク管理者及び統括情報セキュリティ責任者に指示し、情報セキュリティ責任者に対し、当該情報システムの停止を命令する。ただし、特に緊急を要するときは、ネットワーク管理者の判断により情報システムの停止又はネットワークの切断をすることができる。

(5)　ネットワーク管理者及びシステム管理者は、当該事案に係る情報システムのアクセス記録及び対処の内容を記録し、保存する。

(6)　ネットワーク管理者及びシステム管理者は、当該事案に係る再発防止の暫定措置を講じた後、復旧する。

(7)　情報セキュリティ責任者は、当該事案の発生原因、対応方法、被害状況等を分析し、ポリシー及び情報セキュリティ対策の改善等の再発防止計画を策定し、統括情報セキュリティ責任者に報告する。

(8)　統括情報セキュリティ責任者は、前号の再発防止計画を委員会に報告し、その承認を受ける。

2　ネットワーク管理者は、情報セキュリティに関する事案の発生に備え、緊急時対応計画及び緊急時連絡網を策定し、委員会の承認を受ける。

3　緊急時対応計画には、次に掲げる事項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

４　情報セキュリティ責任者は、所管する情報システム等に係る緊急時対応計画及び緊急時連絡網を整備しなければならない。

５　ネットワーク管理者及び情報セキュリティ責任者は、情報セキュリティに関する事案の発生を想定した訓練を定期的に行い、当該事案への対応を点検しなければならない。

６　ネットワーク管理者及び情報セキュリティ責任者は、情報セキュリティを取り巻く状況の変化、組織体制の変動等に応じ、緊急時対応計画を見直しを行わなければならない。

第９章　例外措置

（例外措置の許可）

第７６条　情報セキュリティ責任者及びシステム管理者は、ポリシー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、ポリシーと異なる方法を採用し、又はポリシーを遵守しないことについて合理的な理由がある場合には、最高情報統括責任者の許可を得て、例外措置を講ずることができる。

（緊急時の例外措置）

第７７条　情報セキュリティ責任者及びシステム管理者は、行政事務の遂行に緊急を要する等の場合であって、例外措置を講ずることが不可避のときは、事後速やかに最高情報統括責任者に報告しなければならない。

（例外措置の申請書等の管理）

第７８条　最高情報統括責任者は、例外措置の申請書及び審査結果を適切に保管しなければならない。

第１０章　準拠

（法令等の遵守）

第７９条　職員等は、情報資産を適切に保護し、及び管理するため、次に掲げる法令等を遵守しなければならない。

(1)　刑法（明治４０年法律第４５号）

(2)　地方公務員法（昭和２５年法律第２６１号）

(3)　著作権法（昭和４５年法律第４８号）

(4)　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）

(5)　個人情報の保護に関する法律（平成１５年法律第５７号）

(6)　生駒市個人情報保護条例（平成１０年３月生駒市条例第１号）

２　職員等は、使用するソフトウェアの使用許諾契約を遵守しなければならない。

（ポリシーの遵守状況の確認）

第８０条　職員等は、情報システムの利用等におけるポリシーに対する違反を認めたときは、直ちに所管の情報セキュリティ責任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　ネットワーク管理者及び情報セキュリティ責任者は、ポリシーに対する違反が情報セキュリティ上重大な影響を及ぼすおそれがあることを認めたときは、第７５条第１項の規定による対応を行わなければならない。

（情報セキュリティに関する事案の原因に対する警告）

第８１条　最高情報統括責任者は、情報セキュリティに関する事案の原因となる情報システム及び職員等については、その所管する情報セキュリティ責任者に対して、注意又は警告を発することができるものとする。

（違反への対応）

第８２条　職員等がポリシーに違反したときは、その重大性、状況等に応じて地方公務員法等に基づき、処分等の対象とする。

第１１章　評価及び見直し

第１節　評価

（監査の実施等）

第８３条　委員会は、本市におけるポリシーの遵守状況を客観的に評価するため、必要に応じて監査を実施する者を指名し、監査を実施しなければならない。

２　監査を実施する者は、監査結果を委員会に報告しなければならない。

３　監査を実施する者は、自らのポリシーの遵守状況を監査することができない。

４　委員会は、監査の結果を受けて、是正の必要がある被監査対象を所管する情報セキュリティ責任者に対して改善を指示しなければならない。

５　情報セキュリティ責任者は、委員会の指示に従い、速やかに是正措置を講じなければならない。

（点検）

第８４条　ネットワーク管理者及びシステム管理者は、サーバ等への擬似攻撃によるぜい弱性調査等、情報システムの設定がポリシーに準拠しているかどうかについて定期的に点検を行い、所管の情報セキュリティ責任者に報告しなければならない。

２　情報セキュリティ責任者は、所管の職員等におけるポリシーの遵守状況について定期的に点検を行い、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。

３　統括情報セキュリティ責任者は、前項の規定により報告された内容を取りまとめ、委員会に報告しなければならない。

第２節　見直し

（ポリシーの見直し）

第８５条　委員会は、監査及び点検の結果等を踏まえてポリシーの実効性を評価し、見直しが必要なときは、これを更新しなければならない。

附　則

この訓令は、平成２０年４月１日から施行する。