名張市情報セキュリティポリシー
(対策基準)

平成16年8月12日　策定

情報セキュリティ対策基準

情報セキュリティ対策基準とは、情報セキュリティ基本方針を実行に移すための、名張市の情報資産に関する情報セキュリティ対策の基準である。

1 管理体制

情報セキュリティの管理については、以下の体制とする。

（1）最高情報統括責任者（ＣＩＯ：Chief Information Officer）

名張市における全てのネットワーク、情報システム及び情報資産を統括し、情報セキュリティに関する最終決定権限及び責任を有する最高責任者とし、副市長をもってこれに充てる。

（2）ネットワーク統括管理者

名張市における全てのネットワーク及び情報システムを統括するためネットワーク統括管理者を置き、総務部長をもって充てる。

ネットワーク統括管理者は、最高情報統括責任者を補佐しなければならない。また、最高情報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全ての措置を行う権限及び責任を有する。

ネットワーク統括管理者は、名張市の全てのネットワーク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。

ネットワーク統括管理者は、名張市の全てのネットワークにおける開発、運用、更新等を行う権限及び責任を有する。

（3）情報ネットワーク管理責任者

ネットワーク、情報システム及び情報資産に関わる全ての者に対し、助言・指導を行い、適切な管理運営を行うため、情報ネットワーク管理責任者を置き、総務部情報政策室長をもって充てる。

情報ネットワーク管理責任者は、最高情報統括責任者及びネットワーク統括管理者の事務を取り扱う。

（4）情報セキュリティ統括責任者

名張市における全ての情報資産のセキュリティ対策を総合的に実施するため、情報セキュリティ統括責任者を置き、部等の長をもって充てる。

情報セキュリティ統括責任者は、所掌に属する室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。

情報セキュリティ統括責任者は、ネットワークの適正かつ効率的な運用を図るため、ネットワーク接続基準を定めるものとする。

情報セキュリティ統括責任者は、所管するネットワークに係る情報セキュリティ実施手順の維持・管理を行う。

情報セキュリティ統括責任者は、所掌に属する室等におけるネットワークの設定の変更及び情報システムの開発、運用、更新等を行う承認等を行う。

（5）情報セキュリティ責任者

ネットワーク、情報資産を利用する室等においてセキュリティ対策を実施するため、情報セキュリティ責任者を置き、室等の長をもって充てる。

情報セキュリティ責任者は、情報セキュリティポリシーに定められている事項について職員に実施及び遵守させる権限と責任を有する。

情報セキュリティ責任者は、非常勤職員及び臨時職員の雇用時に必ず情報セキュリティポリシーのうち、職員等が守るべき内容を理解させ、また実施及び遵守させなければならない。

情報セキュリティ責任者は、情報セキュリティ統括責任者の指示に従い、所管するネットワークの設定の変更及び情報システムの運用、更新等の作業を行う。

（6）情報システム管理者

情報システムの適切な管理運営を行うため、情報システム管理者を置き、情報システムを所管する所属長をもって充てる。

情報システム管理者は、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。

情報システム管理者は、所管する情報システムに係る情報セキュリティ実施手順の維持・管理を行う。

情報システム管理者は、情報システムの開発、運用、更新等行う権限及び責任を有する。

（7）情報システム担当者

職員の中から情報システム管理者が指定した者。

情報システム担当者は、情報システム管理者の指示に従い情報システムの開発、運用、更新等の作業を行う。

（8）名張市ＩＴ推進本部

情報資産の適正かつ効率的な管理運営を行うため、名張市ＩＴ推進本部において、情報セキュリティ対策基準等セキュリティに関する重要な事項を審議する。

2 情報資産の分類と管理

（1）情報資産の分類

ア　重要性分類Ⅰ

・名張市個人情報保護条例第二条第一号に規定する個人情報
・法令又は条例（以下「法令等」という。）の定めにより守秘義務が課せられている情報（上記個人情報を除く。）
・法人及びその他の団体に関する情報で、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情報。
・滅失し、又はき損した場合、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がある情報。
・ネットワーク及び情報システムに係るパスワード等及び設定情報。

イ　重要性分類Ⅱ

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は高

いと評価される情報（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情報等）

ウ　重要性分類Ⅲ

ア、イ以外の情報

（２）情報資産の管理責任

ア　管理責任

情報資産は、当該情報資産を作成した各室等の情報セキュリティ責任者が管理責任を有する。

イ　利用者の責任

情報資産を利用する者は、情報資産の分類に従い利用する責任を有する。

ウ　重要性の効力

情報資産が複製又は伝送された場合には、当該複製等も分類に基づき管理しなければならない。

（３）情報資産の管理方法

ア　情報資産の管理

情報資産の重要性分類に従い、パスワード等によるアクセス制限等を行わなければならない。

重要性分類Ⅰの情報のバックアップのための複製を除き、不用意な複製、送付・送信を行ってはならない。

職員は、業務上必要な場合には、情報セキュリティ責任者の許可を得たうえで情報資産の複製、送付・送信を行わなければならない。

イ　記録媒体の管理

重要性分類Ⅰ・Ⅱの情報を記録した取り出しが可能な記録媒体は、災害・盗難等の脅威にさらされないよう施錠ができるなど特に安全な場所に保管しなければならない。また、保管状況等を記録しなければならない。

重要性分類Ⅰ・Ⅱの情報を記録した記録媒体を外部に持ち出す場合は、最高情報統括責任者の許可を得たうえで、職員又は守秘義務及び複製の禁止を明記した契約等を締結した外部業者に行わせるとともに、記録媒体の物理的な保護措置を講じなければならない。

ウ　記録媒体の廃棄

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・Ⅱの情報をいかなる方法によっても復元できないように消去等を行ったうえで破棄しなければならない。

重要性分類Ⅰ・Ⅱを記録した記録媒体の廃棄は、情報セキュリティ責任者の許可を得ることとし、破棄を行った日時、担当者及び処理内容を記録しなければならない。

3　物理的セキュリティ

（１）サーバ等

重要性分類Ⅰ・Ⅱを記録保持するサーバ等は二重化、ミラーリング又はバックアップ等により常に機器の障害に備えなければならない。

情報システム管理者、情報システム担当者及び契約により操作を認められた外部委託事業者以外の者が容易に操作できないように、利用者のＩＤ、パスワードの設定等の措置を施さなければならない。

パスワードは可能な限り複雑なものにしなければならない。また、パスワードの再利用は禁止する。

無線ＬＡＮの導入に当たっては、重要性分類Ⅰ・Ⅱの情報資産を送信する際には経路を暗号化する等、十分な漏洩防止策を実施しなければならない。

（２）電源

停電及び電圧異常等により情報資産が破壊され、行政事務に支障を来す恐れのある情報システム等の機器の電源は、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。

（３）配線

配線は、傍受又は損傷等を受けることがないように可能な限り必要な措置を施さなければならない。

主要な箇所の配線については、損傷等についての定期的な点検を行わなければならない。

（４）管理区域

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、当該機器等又は重要性分類Ⅰ・Ⅱの情報資産の管理並びに運用を行うための区域（以下「管理区域」という。）は、確実な入退室管理を行い、部外者の侵入を防ぐよう努めなければならない。

職員等及び外部委託事業者は身分証明書等を携帯し、求めにより提示しなければならない。

管理区域へ機器等を搬入する場合は、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、職員による確認を行わなければならない。また、職員が同行する等の必要な措置を施さなければならない。

（５）ネットワーク

外部へのネットワーク接続は必要最低限のものに限定し、できる限り接続ポイントを減らさなければならない。

（６）職員等の端末等

室等の端末については、盗難防止のためのワイヤーによる固定等、盗難防止のための物理的措置を施さなければならない。

4 人的セキュリティ

（１）全ての職員

全ての職員は、情報セキュリティポリシー及び職員向け実施手順に定められている事項を遵守しなければならない。

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は、速やかに情報セキュリティ責任者に相談し、指示等を仰がなければならない。

全ての職員は、使用する端末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資産を閲覧されることがないように、適切な措置を施さなければならない。

全ての職員は、情報セキュリティ責任者の許可を得ず、端末等を所属する室等の外に持ち出してはならない。

全ての職員は、異動、退職等により業務を離れる場合には、知り得た情報資産を秘匿しなければならない。

非常勤及び臨時職員には、雇用及び契約時に必ず情報セキュリティポリシーのうち、非常勤及び臨時職員が守るべき内容を理解させ、また実施及び遵守させなければならない。

非常勤及び臨時職員には、雇用及び契約の際、必要な場合は情報セキュリティポリシーを遵守する旨の同意書への署名を求めるものとする。

非常勤及び臨時職員に端末による作業を行わせる場合においては、情報セキュリティ責任者の管理・監督のもとで行うものとし、庁内ＬＡＮのメールの使用が不要の場合には、これを利用できないようにしなければならない。

（２）外部委託に関する管理

ネットワーク及び情報システムの開発・保守を外部委託事業者に発注する場合は、外部委託事業者から再委託を受ける事業者も含めて、下記事項を明記した契約を締結しなければならない。

・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の遵守
・業務上知り得た情報の守秘義務
・提供された情報の目的外利用及び受託者以外の者への提供の禁止
・提供された情報の返還義務
・名張市に対する報告義務
・名張市による定期的な報告徴収、監査・検査の実施
・従業員に対する教育の実施
・情報セキュリティポリシー遵守のために構築する体制
・情報セキュリティポリシーが遵守されなかった場合の規定（損害賠償等）

特に、重要性分類Ⅰの情報資産に関しては、情報システムにおける取り扱いのみでなく、データバックアップのための外部施設等への搬送時においても情報資産の盗難、不正コピー等の防止を厳重に実施する旨を契約書に明記しなければならない。

（３）教育・訓練

最高情報統括責任者は、説明会及び研修の実施等により幹部を含め全ての職員等及び関係する者に対し情報セキュリティポリシーについて啓発しなければならない。また、新規採用の職員等を対象とする情報セキュリティポリシーに関する研修を設けなければならない。

最高情報統括責任者は、一般職員とは別に、ネットワーク統括管理者、情報ネットワーク管理責任者、情報セキュリティ統括責任者、情報セキュリティ責任者、情報システム管理者に対して、それぞれの役割、情報セキュリティに関する理解度等に応じた研修を実施しなければならない。

ネットワーク統括管理者は、業務に支障を来たさない範囲において緊急時対応を想定した訓練を職員等に計画的に行わせなければならない。訓練の計画に当たっては、ネットワーク及び各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ることとする。

情報セキュリティ責任者は、ネットワーク及び情報システムを管理運営していくうえで必要な知識を維持するための情報通信技術やセキュリティに関する研修を受けなければならない。

情報システム管理者及び情報システム担当者は、情報システムの開発・管理・運用を行ううえで必要な技術力を習得・維持するための研修を受けなければならない。

職員等は、情報セキュリティポリシー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。

（4）事故、欠陥に対する報告

職員等は、情報セキュリティに関する事故、システム上の欠陥及び誤動作を発見した場合には、速やかに所管する情報セキュリティ統括責任者及び情報セキュリティ責任者に報告し、情報セキュリティ責任者の指示に従い必要な措置を講じなければならない。また、報告を受けた情報セキュリティ責任者は、情報ネットワーク管理責任者に報告し、情報ネットワーク管理責任者は、報告のあった事故等について全て最高情報統括責任者及びネットワーク統括管理者に報告しなければならない。

職員等は、名張市が管理するネットワーク及び情報システムに関する事故、欠陥に関する住民からの報告・連絡を受けた場合には、速やかに所管する情報セキュリティ統括責任者及び情報セキュリティ責任者に報告し、情報セキュリティ責任者の指示に従い必要な措置を講じなければならない。また、報告を受けた情報セキュリティ責任者は、情報ネットワーク管理責任者に報告し、情報ネットワーク管理責任者は、報告のあった事故等について全て最高情報統括責任者及びネットワーク統括管理者に報告しなければならない。

情報ネットワーク管理責任者及び情報セキュリティ責任者は、これらの事故等を分析し、再発防止のための情報資産として記録を保存しなければならない。

（5）　アクセスのための認証情報及びパスワードの管理

ア　ＩＣカードの管理

職員等は、自己の管理するＩＣカードに関し、次の事項を遵守しなければならない。

・ＩＣカード等の認証に用いるカード類は、職員等間で共有してはならない。
・ＩＣカード等は、カードリーダ又は端末のスロット等に常時挿入してはならない。
・職員等はＩＣカード等を紛失した場合には、速やかに情報ネットワーク管理責任者及び情報システム管理者に通報し、指示を仰がなければならない。
・情報ネットワーク管理責任者及び情報システム管理者は通報があり次第、速やかに当該ＩＣカード等を使用したアクセス等を停止しなければならない。

イ　パスワードの管理

職員等は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。

・パスワードを秘密にし、パスワードの照会等には一切応じないこと。
・パスワードのメモを作らないこと。
・パスワードの長さは十分な長さとし、文字列は想像しにくいものとすること。
・情報システム又はパスワードに対する危険の恐れがある場合には、パスワードを速やかに変更すること。
・パスワードは定期的に変更し、古いパスワードの再利用はしないこと。
・端末にパスワードを記憶させないこと。
・必要に応じて暗号化等を行うことによって他者がパスワードを読めないようにすること。
・職員等間でパスワードを共有しないこと。

（6）接続時間の制限

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

5 技術的セキュリティ

（1）ネットワーク、情報システム及び情報資産の管理

情報ネットワーク管理責任者及び情報システム管理者は、情報セキュリティの確保に必要な記録を全て取得し、盗難、改ざん、消去等を防止する措置を施したうえで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、監視しなければならない。

情報ネットワーク管理責任者及び情報システム管理者は、ネットワーク構成図、情報システム仕様書等に関し、記録媒体の形態に関わりなく適切な保管をしなければならない。

情報システム管理者は、所管する情報資産を適切に管理し、重要性分類Ⅰの情報資産の外部へ送信又は搬出する際には、事前に最高情報統括責任者の承認を得ておかなければならない。

情報システム管理者は、情報資産の重要度に応じて期間を設定し、定期的にバックアップ用の複製を取らなければならない。

情報システム管理者は、閲覧権限がない職員等が所管するシステムにアクセスすることが不可能となるように、必要な措置を講じなければならない。

（2）ネットワーク及び情報システムを使用する際の規定

ア　業務目的以外の使用の禁止

職員等によるネットワーク及び情報システム資源の使用は、業務目的に沿ったもののみが許可され、業務目的以外での情報システムへのアクセス、メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

イ　情報資産の持ち出し及びインターネット等による送信の禁止

職員等は、重要性分類Ⅰ・Ⅱに該当する情報資産を取り扱う場合、下記の行為を行ってはならない。ただし、情報資産のバックアップ等、合理的理由のある場合、かつ最高情報統括責任者の事前の了解を得た場合にはこの限りではない。

・庁外への持ち出し
・インターネット等による庁外との送受信
・個人の所有する情報が記録された媒体の庁内への持ち込み

ウ　無許可ソフトウエアの導入の禁止

職員等は、各自に供用された端末等に対して、情報ネットワーク管理責任者が定める以外のソフトウエアの導入を行ってはならない。ただし、業務を円滑に遂行するために必要なソフトウエアについては、合理的理由のある場合、かつ情報ネットワーク管理責任者及び情報セキュリティ責任者の事前の了解を得た場合に限り、利用することができる。

エ　ソフトウエアの導入に関する注意事項

職員等は、新たにソフトウエアを導入する場合は、情報ネットワーク管理責任者及び情報セキュリティ責任者の許可を得なければならない。

職員等は、正規のライセンスのないソフトウエアを導入してはならない。

職員等は、業務上必要のないソフトウエア及び出所不明なソフトウエア等安全性が確認されないソフトウエアをインストールしてはならない。

職員等は、導入されているソフトウエアを適切に管理運用しなければならない。

オ　機器構成の変更の禁止

職員等は、各自に供用された端末等に対して機器の増設・移設又は改造を行ってはならない。ただし、業務を円滑に遂行するための合理的理由がある場合、かつ情報ネットワーク管理責任者及び情報システム管理者の事前の了解を得た場合に限り、機器の増設・移設又は変更を行うことができる。

カ　情報及びソフトウエアの交換

職員等間において、情報システムに関する情報及びソフトウエアを交換する場合は、その取扱いに関する事項をあらかじめ定め、ネットワーク統括管理者及び情報セキュリティ統括責任者の許可を得るとともに、著作権及び著作隣接権等の法令等に十分配慮しなければならない。

キ　メールの送受信等

職員等は、業務上必要のない者へ職場のメールを転送してはならない。

職員等は、チェーンメールや不審なメールを他者に転送してはならない。

職員等は、差出人が不明又は不自然なファイルが添付された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。

ク　電子署名・暗号化

外部に送信するデータが完全であることを担保することが必要な場合には、定められた電子署名方法及び暗号化方法を使用して送信しなければならない。

暗号化については、定められた方法以外の方法を用いてはならない。また、暗号のための鍵は、重要性分類Ⅰの情報として厳重に管理しなければならない。

ケ　情報システムの入出力データ

情報システムに入力されるデータは、適切なチェック等を行い、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。

情報システムから出力されるデータは、保存された情報の処理が正しく反映され、出力されることを確認しなければならない。

（3）アクセス制御

ア　利用者登録

情報システム管理者は、利用者の登録、変更、抹消、登録した情報資産の管理等について、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。

利用者登録、変更等は情報システム管理者に対する申請により行わなければならない。

イ　ネットワークへのアクセス制御

ネットワーク統括管理者は、必要のない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。

ウ　総合行政ネットワーク及び住民基本台帳ネットワークシステムとの接続

総合行政ネットワーク及び住民基本台帳ネットワークシステムについては、当該接続において取り扱う情報資産の重要性を考慮し、適切なアクセス制御を実施する。

エ　外部ネットワークとの接続

外部ネットワークとの接続に際しては、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詳細に検討し、名張市の全てのネットワーク、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うえで、最高情報統括責任者及びネットワーク統括管理者の許可に基づき接続しなければならない。

情報セキュリティ統括責任者及び情報システム管理者は、外部ネットワークとの接続を行うことで内部ネットワークの安全性が脅かされることのないようにセキュリティ対策に努めなければならない。

接続した外部ネットワークの情報セキュリティに問題が認められ、名張市の情報資産に脅威が生じることが想定される場合には、ネットワーク統括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。

内部ネットワークの情報セキュリティに問題が認められた場合には、ネットワーク統括管理者は速やかに当該内部ネットワークを遮断しなければならない。

オ　パスワード等の管理

情報システム管理者は、職員等のパスワードに関する情報を厳重に管理しなければならない。

情報ネットワーク管理責任者は、ネットワーク並びにネットワーク上で利用する各種ＩＤ、パスワード等を厳重に管理しなければならない。

（4）ネットワーク及び情報システムの開発、導入、保守等

ア　情報システムの調達

情報ネットワーク管理責任者及び情報システム管理者は、機器及びソフトウエアを導入等する場合は、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、確認しなければならない。

イ　ネットワーク及び情報システムの導入・開発・保守

情報セキュリティ統括責任者及び情報システム管理者は、開発及び保守時の事故・不正行為対策のため、次の事項を定めなければならない。

・責任者及び監督者
・作業者及び作業範囲
・開発及び保守等の事故・不正行為に係るリスク分析
・開発及び保守するシステムと運用システムとの分離
・開発及び保守に関するソースコードの提出
・開発及び保守の際のセキュリティ上問題となりうる恐れのあるＯＳ、ミドルウエア及びアプリケーションソフトの使用禁止
・開発及び保守の際のアクセス制限
・機器の搬出入の際の、情報システム管理者の許可及び確認
・開発及び保守記録の提出義務
・マニュアル等の定められた場所への保管
・開発及び保守を行った者の利用者ＩＤ、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
・守秘義務
・再委託管理

情報セキュリティ統括責任者及び情報システム管理者は、ネットワーク構成図、情報システ

ムの仕様書等を整備しなければならない。

情報システム管理者は、新たにシステムを導入する際には、既に稼働しているシステムに接続する前に十分な試験・調整を行い、移行の際には既存システムに記録されている情報資産の保存を確実に行い、復帰が即座に可能な状態にしておかなければならない。

ウ　ソフトウエアの保守及び更新

ソフトウエア（汎用ソフトウエア及び独自開発ソフトウエア）等を更新又は修正プログラムを導入する場合は、不具合及び他のシステムとの相性の確認を行い、計画的に更新し又は導入しなければならない。

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する修正プログラムについて、速やかな対応を行うこととし、その他のソフトウエ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。

エ　機器の修理及び廃棄

記憶媒体の含まれる機器について、外部の事業者に庁外で修理させる場合又は賃貸期間満了等により廃棄する場合は、可能な範囲でバックアップを取り、記憶媒体内の全ての情報を消去しなければならない。また、重要性分類Ⅰ・Ⅱを記録した媒体の含まれる機器を破棄する場合は、記録媒体を復元不可能な状態にし、破棄しなければならない。

なお、故障を外部の事業者に庁外で修理させる際、情報資産を消去することが難しい場合は、修理を委託する事業者に対し守秘義務を明記した契約を締結しなければならない。

オ　機器構成の変更

職員等は、情報システムの機器について、業務を遂行するため機器の増設・変更・交換を行う必要がある場合には、情報ネットワーク管理責任者の許可を得て行わなければならない。

職員等は、他のネットワークへの接続等を行う又は他のネットワークから接続等が可能となる機器等を接続してはならない。

（5）コンピュータウイルス対策

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

・情報システムのサーバ及び必要な機器にウイルス対策ソフトを導入すると共に、ウイルスパターンファイル等常に最新の状態にしておかなければならない。
・定期的に新種のウイルスに関する情報収集やネットワーク及び情報システム内部の感染状況等について情報収集すること。
・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。
・サーバ及び端末において、ウイルスチェックを行うこと。

イ　職員等は、次の事項を遵守しなければならない。

・外部からデータ又はソフトウエアを取り入れる場合には、必ずウイルスチェックを行うこと。
・ウイルスチェックの実行を途中で止めないこと。
・情報ネットワーク管理責任者及び情報システム管理責任者が提供するウイルス情報を常に確認すること。

・添付ファイルのあるメールを送受信する場合は、ウイルスチェックを行うこと。

（６）不正アクセス対策

情報セキュリティ統括責任者及び情報システム管理者は、セキュリティホールの発見に努め、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。

情報セキュリティ統括責任者及び情報システム管理者は、ネットワーク及び情報システムに不正な侵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。

情報セキュリティ統括責任者及び情報システム管理者は、攻撃を受けていることが明らかな場合には、ネットワーク及び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。

攻撃を受け、当該攻撃が不正アクセス禁止法違反等犯罪の可能性がある場合には記録の保存に努めるとともに、警察・関係機関との緊密な連携に努めなければならない。

職員等による不正アクセスがあった場合、情報セキュリティ統括責任者又は情報システム管理者は当該職員等が所属する室等の情報セキュリティ責任者に通知し、適切な処置を求めなければならない。

職員等による不正アクセスの結果、データの漏洩、破壊、改ざん又はシステムダウン等により行政業務に深刻な影響をもたらした場合、当該職員等を地方公務員法による懲戒の対象とし、悪質な場合には刑事告発の対象とする。

（７）セキュリティ情報の収集

ネットワーク統括管理者は、情報セキュリティに関する情報を収集し、名張市の全てのネットワーク及び情報システムについてソフトウエアに修正プログラムを当てる等、セキュリティ対策上必要な措置を講じなければならない。

最高情報統括責任者は、これらの情報を定期的に取りまとめ、情報セキュリティ統括責任者及び情報セキュリティ責任者に通知するとともに、情報セキュリティポリシーの改定につながる情報についてはＩＴ推進本部に報告しなければならない。

6 運用

（１）ネットワーク及び情報システムの監視

情報セキュリティ統括責任者及び情報システム管理者は、ネットワーク及び情報システムの運用にあたっては、常にネットワーク及び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。

外部と常時接続するシステムについては、ネットワーク侵入監視装置を設置し、２４時間監視を行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

情報セキュリティ統括責任者及び情報セキュリティ責任者は、情報セキュリティポリシーが遵守されているかどうかについて、また、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場合には速やかに最高情報統括責任者及びネットワーク統括管理者に報告しなければならない。

最高情報統括責任者は速やかに発生した問題に適切に対処しなければならない。

職員等は、情報セキュリティポリシーの違反が発生した場合は、直ちに情報セキュリティ統括責任者及び情報セキュリティ責任者に報告を行わなければならない。

情報セキュリティ統括責任者及び情報システム管理者は、サーバ等のシステム設定が情報セキュリティポリシーを遵守しているかどうかについて、また問題が発生していないかについて定期的に確認を行い、問題が発生していた場合には速やかに適切に対処しなければならない。

（３）侵害時の対応

情報資産への侵害が発生した場合は、情報セキュリティ実施手順に従い速やかに対応しなければならない。

ア　事案の調査

セキュリティに関する事案を認めた者は、次の項目について、すみやかにネットワーク統括管理者に報告しなければならない。

・症状の分類
・事案が発生した原因として、想定される行為
・確認した被害・影響範囲
・記録

ネットワーク統括管理者は、事案の詳細な調査を行うとともに、最高情報統括責任者との情報共有及びＩＴ推進本部への報告を行わなければならない。

イ　事案への対処

（ア）最高情報統括責任者は、次の事案が発生した場合、それぞれ定められた連絡先へ連絡しなければならない。

・サイバーテロその他の市民に重大な被害が生じる恐れがあるとき。（名張市長、警察、影響が考えられる個人及び法人）
・不正アクセスその他犯罪と思慮されるとき。（名張市長、警察）
・踏み台となって他者に被害を与える恐れがあるとき。（名張市長、警察）
・情報システムに関する被害。(情報システム管理者、必要と認められる事業者等)
・その他情報資産に係る被害。(関係部局等)

（イ）最高情報統括責任者は、次の事案が発生し情報資産の防護のためにネットワークの切断がやむを得ない場合は、ネットワークを切断する措置を講ずる。

・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判明したとき。
・システムの運用に著しい支障をきたす攻撃が継続しているとき。
・コンピュータウイルス等不正プログラムがネットワーク経由で拡がっているとき。
・情報資産に係る重大な被害が想定されるとき。

（ウ）情報システム管理者は、次の事案が発生し情報資産の防護のために情報システムの停止がやむを得ない場合は、情報システムを停止する。

・コンピュータウイルス等不正プログラムが情報資産に深刻な被害を及ぼしているとき。
・災害等により電源を供給することが危険又は困難なとき。
・その他の情報資産に係る重大な被害が想定されるとき。

（エ）最高情報統括責任者又は情報システム管理者は、事案に係るシステムの現状を保存し、事

案に対処した経過を記録する。

（オ）最高情報統括責任者又は情報システム管理者は、事案に係る証拠保全の実施を完了するとともに、再発防止の措置をできるだけ速やかに講じたのち復旧し、必要と認められる期間、再発監視を行う。

ウ　再発防止の措置

ネットワーク統括管理者は、当該事案に係るリスク分析を実施し、情報セキュリティポリシー及び実施手順の改善に係る再発防止計画を策定し、ＩＴ推進本部へ報告しなければならない。

ＩＴ推進本部は、情報セキュリティポリシー及び実施手順の改善に係る再発防止計画が有効であると認められる場合は、これを承認する。

ネットワーク統括管理者は、各種セキュリティ対策の改善に係る再発防止計画を策定し、最高情報統括責任者へ報告しなければならない。最高情報統括責任者は、これらの再発防止計画が有効であると認められる場合は、これを承認し、事案の概要と併せ職員等に周知しなければならない。

エ　外部委託による運用契約

運用を外部委託する場合は、委託に関する責任を有する部署を明確にするとともに、外部委託事業者に対し必要なセキュリティ要件を記載した契約書による契約を締結しなければならない。

委託に関する責任を有する部署は、委託先において必要なセキュリティ対策が確保されていることを確認し、その内容をネットワーク統括管理者に報告するとともに、その重要度に応じて最高情報統括責任者に報告しなければならない。

7 法令遵守

職員等は、職務の遂行において使用する情報資産について、次の法令等を遵守しこれに従わなければならない。

・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)

・著作権法(昭和４５年法律第４８号)

・行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律（昭和６３年法律第９５号)

・名張市個人情報保護条例(平成１４年条例第３２号)

8 情報セキュリティに関する違反に対する対応

情報セキュリティポリシーに違反した職員等及びその監督責任者に対しては、その重大性、発生した事案の状況等に応じて地方公務員法による懲戒処分の対象とする。

なお、職員等に情報セキュリティポリシーに違反する行動がみられた場合には、速やかに次の措置を講じなければならない。

・情報セキュリティ統括責任者が違反を確認した場合は、情報セキュリティ統括責任者は当該職員等が所属する室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。

・情報システム管理者等が違反を確認した場合は、違反を確認した者は速やかに情報セキュリティ統括責任者及び当該職員等が所属する室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。

・情報セキュリティ責任者の指導によっても改善されない場合、情報セキュリティ統括責任者は、当該職員等のネットワーク又は情報システムの使用に関する権利を停止あるいは剥奪することができる。その後速やかに、情報セキュリティ統括責任者は、職員等の権利を停止あるいは剥奪した旨を最高情報統括責任者及び当該職員等が所属する室等の情報セキュリティ責任者に通知しなければならない。

9 評価・見直し

（1）監査

情報セキュリティ統括責任者及び情報システム管理者は、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定期的に監査を行わなければならない。

外部委託事業者に委託している場合、情報セキュリティ統括責任者及び情報システム管理者は、外部委託事業者から下請けとして受託している事業者も含めて、情報セキュリティポリシーの遵守について監査を定期的に行わなければならない。

最高情報統括責任者は、監査結果をとりまとめ、ＩＴ推進本部に報告するとともに、情報セキュリティポリシーの更新の際に参照する情報資産として活用しなければならない。

（2）点検

情報セキュリティ統括責任者及び情報セキュリティ責任者は、情報セキュリティポリシーに沿った情報セキュリティ対策が実施されているかどうかについて職員等に調査・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。また、情報セキュリティ統括責任者はこれをとりまとめ、最高情報統括責任者に報告する。

最高情報統括責任者は、この報告結果をＩＴ推進本部に報告するとともに、情報セキュリティポリシーの更新の際に参照する情報資産として活用することとする。

（3）情報セキュリティポリシーの更新

最高情報統括責任者は、新たに必要な対策が発生した場合又は監査の結果及び点検の結果、評価及び見直しが必要となった場合には、ＩＴ推進本部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つとめなければならない。

情報セキュリティポリシーの更新内容については、ＩＴ推進本部が決定しなければならない。