新見市情報セキュリティポリシー

新見市情報セキュリティポリシーの構成

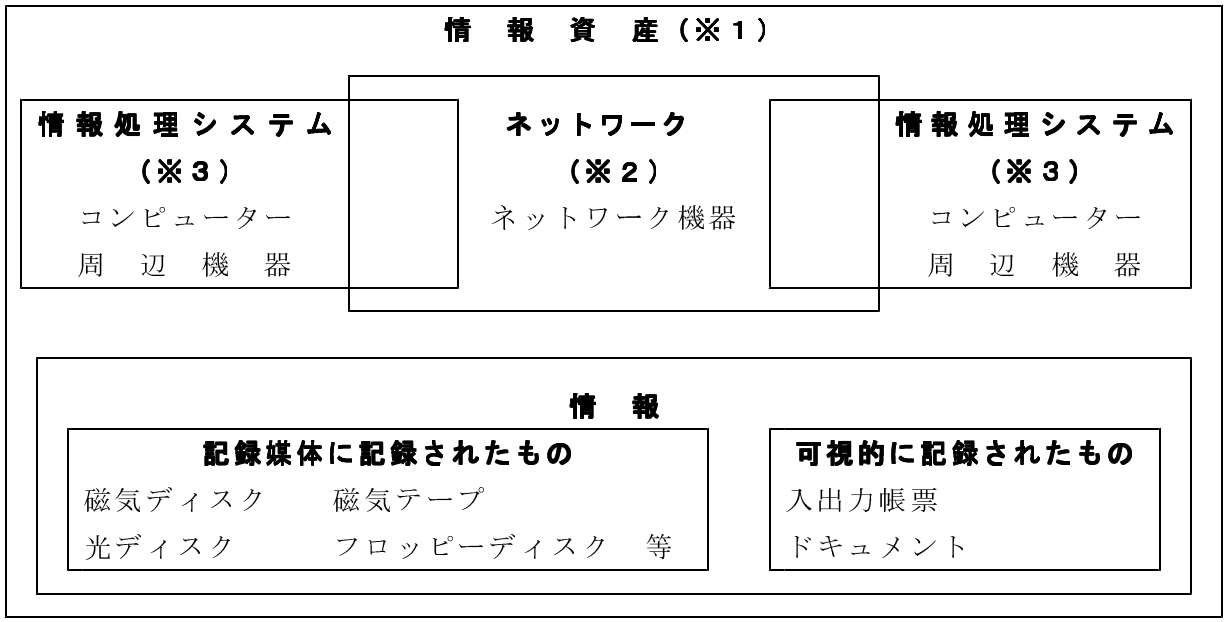
新見市情報セキュリティポリシーとは、新見市が保有する情報資産(※１)に関するセキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものである。

新見市情報セキュリティポリシーは、本市の情報資産を取り扱う全職員に浸透、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。しかし一方では、情報セキュリティ対策は、情報処理技術や通信技術等の進展に伴う急速な状況の変化に、柔軟に対応することも必要である。

このようなことから、新見市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、情報資産を取り巻く状況の変化に適切に対応する部分としての「情報セキュリティ対策基準」の２階層からなるものとし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、ネットワーク（※２）及び情報処理システム(※３)ごとに、具体的な情報セキュリティ対策の実施手順（運用マニュアル）として「情報セキュリティ実施手順」を策定することとする。

新見市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	情報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、全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		ネットワーク又は情報処理システムごとに定める情報セキュリティ対策基準に基づいた個々の情報資産に関する具体的な対策手順



第１章　情報セキュリティ基本方針

１　目的

本市が取り扱う情報資産には、市民の個人情報のみならず行政運営上重要な情報など、部外に漏洩等した場合には極めて重大な結果を招く情報が多数含まれており、これらの情報資産を人的脅威や災害、事故等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、継続的かつ安全・安定的な行政サービスの実施を確保するためにも必要不可欠である。また、近年のいわゆるＩＴ革命の進展により、電子政府や電子自治体の実現が期待されているところである。本市がこれらに積極的な対応をするためには、本市が管理している全てのネットワーク及び情報処理システムが高度な安全性を有することが不可欠な前提条件となる。

このため、本市の情報資産の機密性、完全性及び可用性（注）を維持するための対策を整備するため、新見市情報セキュリティポリシーを定めることとし、情報セキュリティの確保に最大限取り組むこととする。

このうち情報セキュリティ基本方針においては、本市の情報セキュリティ対策の基本的な方針として、情報セキュリティポリシーの対象、位置付け等を定めるものとする。

（注）：国際標準化機構（ISO）が定めるもの（ISO 7498－2：1989）

機密性（confidentiality）　：情報にアクセスすることが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。

完全性（integrity）　：情報及び処理の方法の正確さ及び完全である状態を完全防護すること。

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を確実にすること。

２　定義

（１）ネットワーク

コンピューター等を相互に接続するための通信網及びその機器で構成され、処理を行う仕組みをいう。

（２）情報処理システム

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ー、周辺機器及びネットワークをいう。

（３）情報資産

ネットワーク、情報処理システム、ドキュメント及びデータをいう。

（４）個人情報

個人に関する情報（事業を営む個人の当該事業に関する情報を除く。）で特定の個人を識別することができるもの（一般人が通常入手し得る関連情報と照合することにより、特定の個人を識別することができることとなるものを含む。）をいう。

（５）セキュリティ

許可されていない第三者から情報資産等を守ることをいう。

（６）ドキュメント

システム設計書、ネットワーク設計書、システム設計書、ネットワーク仕様書、プログラム仕様書、オペレーション仕様書、コード一覧表等ネットワーク及び情報処理システムに必要な仕様書類をいう。

（７）データ

ネットワーク及び情報処理システムに係る入出力帳票、記録媒体及びドキュメントをいう。

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、本市の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、体系的かつ具体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するものである。

４　情報セキュリティポリシーの対象範囲

情報セキュリティポリシーの対象範囲は、本市における情報資産に接する全ての職員（非常勤職員及び臨時職員を含む。）とする。

５　職員の義務

職員は、情報セキュリティの重要性について共通の認識を持つとともに、情報資産の利用に当たっては情報セキュリティポリシーを遵守するものとする。

６　情報セキュリティ管理体制

本市の情報資産について、適切に情報セキュリティ対策を推進・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

情報資産をその重要度に応じて分類し、それに応じたセキュリティ対策を行うものとする。

８　情報資産への脅威

情報セキュリティポリシーを講ずるうえで、情報資産に対する脅威の発生度合いや発生した場合の影響を考慮するものとする。

特に認識すべき脅威は以下のとおりである。

（１）権限外者による故意の不正アクセス又は不正操作によるデータやプログラムの持出・盗聴・改ざん・消去、機器及び記録媒体の盗難等

（２）職員及び外部委託者による意図しない操作、故意の不正アクセス又は不正操作によるデータやプログラムの持出・盗聴・改ざん・消去、機器及び記録媒体の盗難、規定外の情報システムの機器操作によるデータ漏洩等

（３）地震、落雷、火災等の災害や事故、故障等によるサービス及び業務の停止

９　情報セキュリティ対策

本市の情報資産を上記８の脅威から保護するため、以下の情報セキュリティ対策を講ずるものとする。

（１）人的セキュリティ対策

情報資産に接する職員の情報セキュリティに関する権限や責任等を定めるとともに、全ての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、教育・訓練を行う。

（２）物理的セキュリティ対策

電子計算機室等について不正な立入り等から保護するため、入退室や機器管理上の物理的な対策を講ずる。

（３）技術的セキュリティ対策

情報資産を不正な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、コンピューターウイルス対策等を実施する。

（４）運用におけるセキュリティ対策

情報セキュリティポリシーの実効性を確保するため、また、不正アクセスされること及び不正アクセスによって他の情報処理システムに対して被害を及ぼすことを防ぐため、ネットワークの監視、セキュリティポリシーの遵守状況の確認等の必要な措置を講ずる。また、障害及び緊急事態が発生した際の迅速な対応を可能とするための対策を講ずる。

１０　情報セキュリティ対策基準の策定

本市の情報資産について、上記９の情報セキュリティ対策を講ずるに当たっては、職員が遵守すべき事項及び判断等の基準を統一的なレベルで定める必要がある。そのため、情報セキュリティ対策を行ううえで必要となる基本的な要件を明記した情報セキュリティ対策基準を策定するものとする。

１１　情報セキュリティ実施手順（運用マニュアル）の策定

情報セキュリティ対策を確実に実施していくためには、個々の情報資産に関する対策の手順を具体的に定めておく必要があることから、情報セキュリティ対策基準に基づき、情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティ実施手順は、公開することにより本市の行政運営に重大な支障を及ぼす恐れのある情報であることから非公開とする。

１２　評価・見直し

情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価、ネットワーク及び情報処理システムの変更、新たな脅威等情報セキュリティを取り巻く状況の変化を踏まえ、適宜情報セキュリティ対策基準の見直しを実施するものとする。

第２章　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、本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

新見市における全ての情報資産を統括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

新見市における全てのネットワーク及び情報処理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。

ネットワーク統括管理者は、ネットワーク管理者、システム管理者、セキュリティ統括責任者、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ことができる。

（３）ネットワーク管理者

ネットワークの適切な管理運営を行うため、ネットワーク管理者を置き、ネットワークを所管する所属長をもって充てる。

ネットワーク管理者は、所管するネットワークにおける開発、設定の変更、運用、更新等を行う権限及び責任を有する。

ネットワーク管理者は、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。

ネットワーク管理者は、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。

（４）ネットワーク担当者

職員の中からネットワーク管理者が指定した者

ネットワーク担当者は、ネットワーク管理者の指示に従いネットワークの構築、設定変更、運用、更新等の作業を行う。

（５）システム管理者

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

システム管理者は、情報処理システムの開発、設定の変更、運用、更新等行う権限及び責任を有する。

システム管理者は、所管する情報処理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。

（６）システム担当者

職員の中からシステム管理者が指定した者

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

（７）セキュリティ統括責任者

新見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、セキュリティ統括責任者を置き、総務部長、福祉部長、建設部長、産業部長、教育部長、消防長、新見支局長、大佐支局長、神郷支局長、哲多支局長、哲西支局長をもって充てる。

セキュリティ統括責任者は、所掌に属する課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。

（８）セキュリティ責任者

ネットワーク、情報資産を利用する課等において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き、情報資産を利用する課等の所属長をもって充てる。

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等に実施及び遵守させなければならない。

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。

（９）端末取扱責任者

情報処理システムの端末機等を操作する職員の中からセキュリティ責任者が指定した者

（１０）新見市情報処理システム管理運営委員会

情報資産の適正かつ効率的な管理運営を行うため、新見市情報処理システム管理運営委員会（以下「委員会」という。）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　情報の分類と管理

（１）情報の分類

対象となる全ての情報は、次の重要性分類に従って分類する。

ア　重要性分類Ⅰ

（ア）　新見市個人情報保護条例に規定する個人情報

（イ）　法令又は条例(以下「法令等」という。)の定めにより守秘義務を課されている情報(上記個人情報を除く。)

（ウ）　法人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

（エ）　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

（オ）　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のある情報

（カ）　ネットワーク及び情報処理システムに係るパスワード及び設定情報

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）情報の管理方法

ア　情報の管理及び取扱

情報の重要性分類に従い、パスワード等によるアクセス制限及び暗号等による通信内容の秘匿を行わなければならない。

重要性分類Ⅰの情報の不用意な複製や、送付・送信は行ってはならない。

職員は、業務上必要な場合には、許可を得たうえで情報の複製・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外し可能な記録媒体は、外部から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出しする場合は、職員又は守秘義務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　記録媒体の処分

記録媒体が磨耗等により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廃棄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の廃棄は、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記録しなければならない。

３　人的セキュリティ

（１）職員

職員は、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に定めている事項を遵守しなければならない。

職員は、情報セキュリティ実施手順について不明な点、遵守することが困難な点がある場合には、速やかにセキュリティ責任者に相談し、指示を仰がなければならない。

職員は、セキュリティ責任者の許可を得ずに、情報処理システムの機器、記録媒体等を執務室外に持ち出してはならない。

職員は、異動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。

（２）教育・訓練

最高情報統括責任者は、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、職員を対象とした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。

ネットワーク管理者は、ネットワーク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情報セキュリティに関する研修を受けなければならない。

システム管理者は、情報処理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情報セキュリティに関する研修を受けなければならない。

セキュリティ統括責任者及びセキュリティ責任者は、情報セキュリティ対策を実施するうえで必要な知識を維持するための情報通信技術や情報セキュリティに関する研修を受けなければならない。

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処理システムの運用に支障を来さない範囲において緊急時対応を想定した訓練等を職員に行わせなければならない。

ネットワーク担当者及びシステム担当者は、ネットワーク及び情報処理システムの開発・保守・運用管理を担当する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が生じないようにしなければならない。

（３）外部委託に関する管理

情報処理システムの開発・保守・運用管理等を外部事業者に委託する場合は、情報セキュリティポリシーのうち外部委託事業者が守るべき内容の遵守及びその守秘義務を明記した契約を締結し、その遵守を管理しなければならない。

（４）パスワード等の管理

職員は、自己の保有するパスワードについて、不用意に漏らしたりメモを作ったりしないようにするなど、パスワードの秘密保持に努めなければならない。

職員は、ＩＣカード等を適切に管理しなければならない。

職員は、ＩＣカード等を紛失した場合には、速やかにシステム管理者に通報し指示を仰がなければならない。

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。

（５）接続時間の制限

職員は、情報処理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に努めるものとする。

４　物理的セキュリティ

（１）入退室の管理

セキュリティ責任者は、重要性分類Ⅰ・Ⅱの情報の記録されている媒体保管場所及びそれを取り扱う情報機器の設置場所への入退室の管理について必要な措置を講じなければならない。

（２）職員の情報処理システムの機器管理

職員は執務室に職員が不在となる場合には、施錠するなど部外者の侵入を防ぐ措置を講じなければならない。

（３）機器等の搬入・搬出

電子計算機室等へ機器等を搬入・搬出する場合は、あらかじめ当該機器等の既存情報処理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。

機器等の搬入・搬出には、職員が立ち会う等の必要な措置を講じなければならない。

（４）電源

停電及び電圧異常等によりデータ等が破壊され、業務処理に支障を来す恐れのある情報処理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。

（５）配線

配線は、傍受又は損傷等を受けることがないよう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。

５　技術的セキュリティ

（１）ネットワーク及び情報処理システムの管理

ア　ネットワーク及び情報処理システム管理記録の作成と管理

ネットワーク管理者及びシステム管理者は、所管するネットワーク及び情報処理システムにおいて行ったシステムの変更作業を記録し、適切に管理しなければならない。

イ　ネットワーク及び情報処理システム仕様書の管理

ネットワーク管理者及びシステム管理者は、所管するネットワーク及び情報処理システムの仕様書を最新の状態にしなければならない。また、仕様変更等の処理を行った場合は、その記録を作成しなければならない。

ネットワーク管理者及びシステム管理者は、仕様書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　アクセス記録の取得

ネットワーク管理者及びシステム管理者は、アクセス記録及びセキュリティ関連障害に関する記録を取得し、一定の期間保存しなければならない。

ネットワーク管理者及びシステム管理者は、アクセス記録が、窃取、改ざん又は消去されないように必要な措置を講じなければならない。

ネットワーク管理者及びシステム管理者は、可能な範囲でアクセス記録を分析しなければならない。

エ　障害記録の作成

ネットワーク管理者及びシステム管理者は、可能な範囲で障害記録を作成し、一定の期間保存しなければならない。

オ　バックアップの取得

ネットワーク管理者及びシステム管理者は、情報の重要度に応じて定期的にバックアップを取り、施錠等のできる安全な場所へ保管しなければならない。

カ　ソフトウェアの交換

職員間で、情報処理システムに関するソフトウェア等を交換する場合は、システム管理者の許可を得るとともに、著作権及び著作隣接権に配慮しなければならない。

キ　ソフトウェアの導入に関する注意

職員は、新たにソフトウェアを導入する場合は、システム管理者の許可を得なければならない。

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。

職員は、業務上不必要なソフトウェア及び出所不明なソフトウェア等安全性が確認されないソフトウェアをインストールしてはならない。

職員は、導入されているソフトウェアを適切に運用管理しなければならない。

ク　メールの送受信等

職員は、メールの自動転送機能を用いて、業務上不必要な者へ職場のメールを転送してはならない。

職員は、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。

職員は、重要性分類Ⅱの情報に該当する添付ファイルのあるメールを送信する必要がある場合には、事前にデータ所管所属長の承認を受けなければならない。

職員は、外部からソフトウェアを取り入れる場合は、事前にシステム管理者の承認を受けなければならない。

職員は、差出人が不明な、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、直ちに廃棄しなければならない。

ケ　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。

コ　職員以外の者が利用できる情報処理システム

職員以外の者が利用できる情報処理システムについては、必要に応じ他の情報処理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取らなければならない。

サ　情報処理システムの入出力データ

情報処理システムに入力されるデータの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。

情報処理システムから出力されるデータの処理が正しく行われていることを確認しなければならない

シ　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処理システムへのアクセス及びメールの使用を行ってはならない。

（２）情報処理システムアクセス制御

ア　利用者登録

システム管理者は、情報処理システムの利用者の登録、変更、抹消等については、各情報処理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、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

ネットワーク管理者及びシステム管理者は、不必要な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　外部からのアクセス

外部からのアクセスの許可は、必要最低限にしなければならない。

エ　総合行政ネットワーク（ＬＧＷＡＮ）との接続

ネットワーク管理者及びシステム管理者は、「総合行政ネットワーク（ＬＧＷＡＮ）接続仕様書」に基づき適切な管理をしなければならない。

オ　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、機器構成及び情報セキュリティレベル等を詳細に検討し、本市の情報資産に影響が生じないことを明確に確認したうえで、接続しなければならない。

ネットワーク管理者及びシステム管理者は、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た場合には、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。

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。

カ　パスワード等の管理

システム管理者は、情報処理システムで使用するＩＤ、パスワードを厳重に管理しなければならない。

ネットワーク管理者は、ネットワーク並びにネットワーク上で利用する各種サービスのＩＤ、パスワードを厳重に管理しなければならない。

（３）情報処理システムの開発・導入・保守

ア　ネットワーク及び情報処理システムの開発・導入

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処理システムを新規に開発・導入する場合及び大規模な変更等を行う場合は、事前に委員会で審議したうえで実施しなければならない。

この場合、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、情報処理システムの仕様書等を整備しなければならない。

システム管理者は、開発したソフトウェアを情報処理システムに取り入れる場合は、既に稼動している情報処理システムに接続する前に十分な調整を行わなければならない。

イ　ネットワーク及び情報処理システムの変更管理

ネットワーク管理者及びシステム管理者は、重要なネットワーク及び情報処理システムを追加、変更、廃棄等した場合は、その際の設定・構成等の履歴を記録・保存し、必要な場合には復旧できるようにしなければならない。

ウ　ソフトウェアの保守及び更新

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、適切な保守が行われるようにし、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。

システム管理者は、情報処理システム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

記録媒体の含まれる機器を、外部の業者に修理させる場合又は貸借期限終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、記録媒体内の全ての情報を消去しなければならない。

なお、故障を外部の業者に修理させる際、情報を消去することが難しい場合は、修理を委託する業者と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

職員は、情報処理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・交換を行う必要がある場合には、システム管理者の許可を得て行わなければならない。

職員は、モデム等の機器を使用して、他のネットワークへ接続を行う場合及び他のネットワークからアクセスを可能とする仕組みを構築する場合には、ネットワーク管理者及びシステム管理者の許可を得なければならない。ネットワーク管理者及びシステム管理者は、許可にあたってネットワーク及び情報処理システムにセキュリティ上の問題を生じさせてはならない。

（４）コンピュータウイルス対策

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）　情報処理システムのサーバー及び必要な機器にウイルス対策ソフトウェアを導入すること。

（イ）　ウイ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。

（ウ）　定期的に新種のウイルスに関する情報収集や情報処理システム内部の感染状況等について情報収集をすること。

（エ）　コンピュータウイルス情報について、職員に対する注意喚起を行うこと。

（オ）　コンピュータウイルスについて、職員に対して必要な啓発活動を行うこと。

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、及び外部に持ち出す場合には、必ずウイルスチェックを行うこと。

（イ）　ウイルスチェックの実行を途中で止めないこと。

（ウ）　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。

（エ）　ネットワーク管理者及びシステム管理者が提供するコンピュータウイ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、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・保存しなければならない。

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処理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。

システム管理者は、情報処理システムに攻撃を受けていることが明らかな場合には、システムの停止を含め必要な措置を講じなければならない。

職員により本市ネットワーク、外部ネットワーク及び情報処理システムに対して不

正なアクセスがあった場合は、当該職員が所属する課等の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。

外部ネットワークより不正アクセスがあった場合は、ネットワーク管理者及びシステム管理者に報告し、適切な措置を講じなければならない。

（６）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、新見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ェアにパッチを当てる等、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、関係部署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委員会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処理システムの監視

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処理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処理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。

（２）情報セキュリティポリシーの遵守状況の確認

セキュリティ統括責任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について、また、運用上支障が生じていないかについて確認を行わなければならない。

（３）セキュリティ障害時の対応

セキュリティ障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　障害拡大の防止措置

ネットワーク管理者及びシステム管理者は、故意の不正アクセス又は不正操作によりネットワーク及び情報処理システムに障害を及ぼすことが明らかな場合には、ネットワーク及び情報処理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。

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処理システムに障害を受け、その障害の原因となる行為が不正アクセス禁止法違反等の可能性がある場合には、行為の記録の保存に努めなければならない。

イ　障害の調査

ネットワーク管理者及びシステム管理者は、セキュリティ障害が発生した場合、次の項目について調査をしなければならない。

（ア）　障害の内容

（イ）　障害が発生した原因

（ウ）　確認した被害、影響範囲

（エ）　調査した内容は速やかにネットワーク統括管理者へ報告しなければならない。ただし、障害の程度が軽微なものについては報告を要しないものとする。

ウ　障害への対応

ネットワーク統括管理者は、速やかにセキュリティ障害を復旧し、その措置について最高情報統括責任者に報告しなければならない。

障害が外部に重大な影響を及ぼす恐れがある場合には、速やかに最高情報統括責任者に報告のうえ必要な指示を仰がなければならない。

エ　再発防止の措置

ネットワーク統括管理者は、必要な再発防止の措置を講じるとともに、その結果を最高情報統括責任者に報告しなければならない。

ネットワーク管理者及びシステム管理者は速やかに、再発防止の措置を講じなければならない。

セキュリティ総括責任者及びセキュリティ責任者はセキュリティ障害の原因が、人的セキュリティによる場合は、職員に対して再発を防止するため必要な措置を講じなければならない。

7　法令等遵守

職員は、使用する情報資産について、次の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（平成１１年法律第１２８号）

（２）著作権法（昭和４５年法律第４８号）

（３）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）

（４）新見市個人情報保護条例（平成１７年条例第２４号）

また、マナーと倫理をもって情報処理システムを利用しなければならない。

8　評価・見直し等

（１）監査

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処理システムの情報セキュリティについて必要に応じて監査を行わなければならない。

事業者に委託している場合、ネットワーク管理者及びシステム管理者は、情報セキュリティポリシーの遵守について必要に応じて監査を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、委員会に報告する。

（２）点検

セキュリティ総括責任者及びセキュリティ責任者は、当該部署の情報セキュリティが確保されていることを確認するため、自主点検を行い、必要に応じ改善措置を講じなければならない。

（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、評価及び見直しが必要となる事象が発生した場合には、委員会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努めなければならない。