東栄町情報セキュリティポリシー

平成２３年１２月１日　策定

令和　８年　４月１日　改定

東 栄 町

＜目　次＞

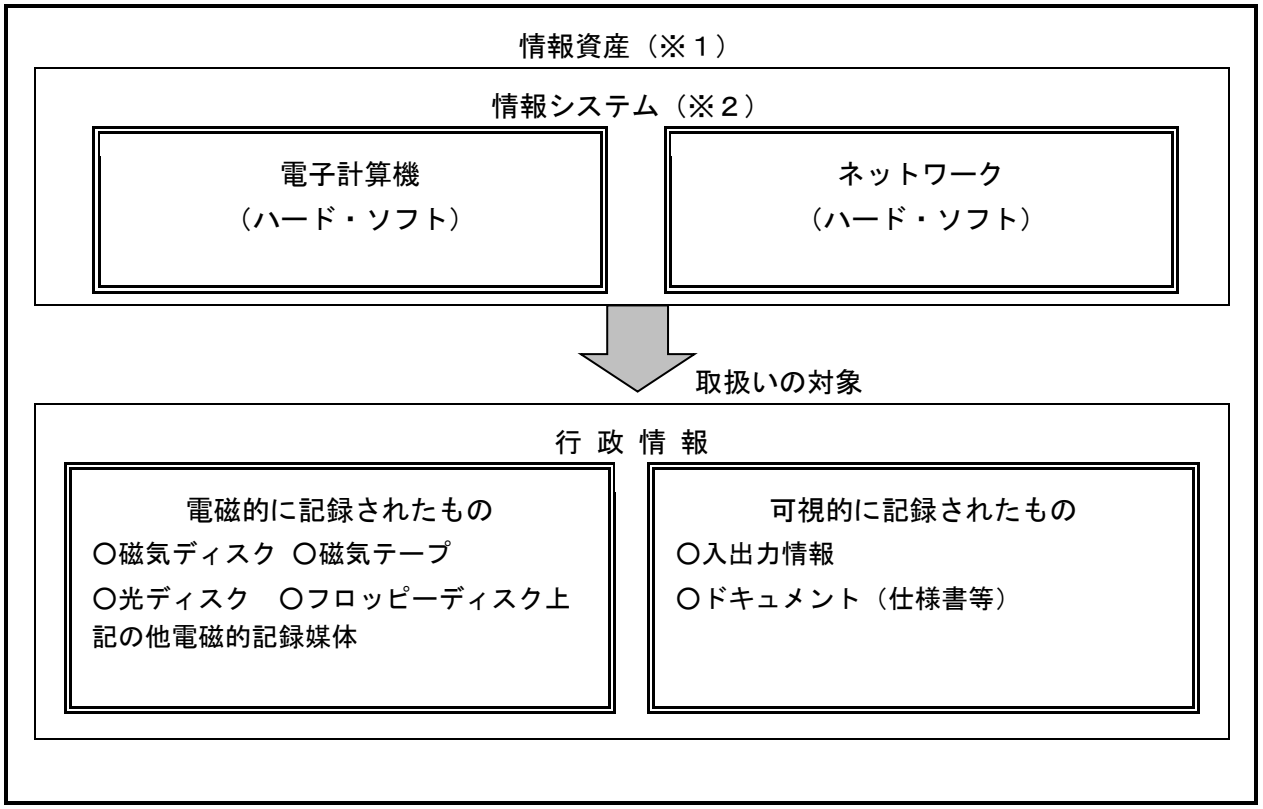
序　情報セキュリティポリシーの構成

情報セキュリティポリシーとは、東栄町が所掌する情報資産（※１）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を総称する。情報セキュリティポリシーは、東栄町が所掌する情報資産に関する業務に携わる全職員、非常勤、臨時職員（以下「職員等」という）及び外部委託事業者に浸透、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。しかしながら一方では、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へ柔軟に対応することも必要である。

このようなことから、情報セキュリティポリシーを一定の普遍性を備えた部分として「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依存する部分として「情報セキュリティ対策基準」に分けて策定することとした。また、情報セキュリティポリシーに基づき、情報システム（※２）毎の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（下表参照）。

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ネットワーク及び情報システム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		情報システム毎に定める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。



第１章　情報セキュリティ基本方針

１　目的

東栄町の各情報システムが取り扱う情報には、町民の個人情報のみならず行政運営上重要な情報など、外部への漏洩等が発生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おり、これらの情報資産を様々な脅威から防御することは、町民の財産、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る。

また、近年のいわゆる IT 革命の進展により、電子商取引の発展や電子自治体の構築が現実のものとなっており、東栄町がこれらに積極的に対応するためには、東栄町の管理する全ての情報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である。

そのため、東栄町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（情報セキュリティ対策）を整備するために東栄町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し、このうち、情報セキュリティ基本方針については東栄町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（ISO7498-2：1989）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安全防護すること。
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）電子計算機
内蔵磁気ディスクを含むハードウエア及びソフトウエアで構成するコンピュータ及び周辺機器（入出力帳票及びシステム仕様書等）をいう。なお、サーバとはサービスを提供するハードウェア及びソフトウェアをという。

（２）磁気ディスク等
電子計算機で使用される取り外し可能な磁気ディスク、磁気テープ、光ディスクその他これらに類する電磁的記録媒体をいう。

（３）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、その構成機器（ハードウェア及びソフトウェア）及び記録媒体で構成され、情報処理を行う仕組みをいう。

（４）情報システム
電子計算機及びネットワークをいう（仕様書及びネットワーク図等のシステム関連文書を含む）。

（５）行政情報
東栄町の行政事務の執行に関する情報で、かつ情報システムで取扱うものをいう。

（６）情報資産
情報システム及び行政情報をいう。なお情報資産には紙等に出力された情報も含むものとする。

（７）情報セキュリティ情報資産の機密性、完全性の維持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、東栄町が所掌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、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頂点に位置するものである。

４　職員等及び外部委託事業者の義務

東栄町長をはじめとして東栄町が所掌する情報資産に関する業務に携わる職員等及び外部委託事業者は、情報セキュリティ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情報セキュリティポリシーを遵守するものとする。

５　情報セキュリティ管理体制

東栄町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。

６　情報資産の分類

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

７　情報資産への脅威

情報セキュリティポリシーを策定するうえで、情報資産を脅かす脅威の発生度合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。

ア　情報資産設置場所への部外者の侵入による機器または情報資産の破壊・盗難、故意の不正アクセスまたは不正操作、ウイルス攻撃、サービス不能攻撃等の意図的な要因による機器または情報資産の漏洩・破壊・盗聴・改ざん・消去等

イ　職員等または外部委託事業者による機器または情報資産の持出、誤操作・誤設定、アクセスのための認証情報またはパスワードの不適切管理、故意の不正アクセスまたは不正行為、設計・開発の不備、プログラム上の欠陥、メンテナンス不備、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、規定外の端末接続やソフトウェアの使用、移動・搬送中の事故、機器故障等の非意図的要因による機器または情報資産の盗難、破壊、漏洩、盗聴、改ざん、消去等

ウ　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

エ　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オ 電力供給の途絶、通信の途絶等提供サービス障害からの波及等

８　情報セキュリティ対策

上記７で示した脅威から東栄町の情報資産を保護し、情報システムが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システムに対し被害を及ぼすことを防ぐため、以下の情報セキュリティ対策を講ずるものとする。

（１）物理的セキュリティ対策

サーバ等、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、該当機器等の管理及び運用を行う電子計算機室等並びに通信回線等及び職員等のパソコン等への不正な立入り、情報資産への損傷・妨害、盗難等から保護するために物理的な対策を講ずる。

（２）人的セキュリティ対策

情報セキュリティに関する権限や責任を定め、職員等及び外部委託事業者に情報セキュリティポリシーの内容を周知徹底する等、十分な教育及び啓発が講じられるように必要な対策を講ずる。

（３）技術及び運用におけるセキュリティ対策

情報資産を外部からの不正なアクセス等から適切に保護するため、コンピュータ等の管理、情報資産へのアクセス制御、コンピュータウィルス対策等の技術面の対策を実施する。また、システム開発等の外部委託、ネットワークの監視、情報セキュリティポリシーの遵守状況の確認等の運用面の対策を講ずる。

また、緊急事態が発生した際に迅速な対応を可能とするための危機管理対策を講ずる。

９　情報セキュリティ対策基準の策定

東栄町の情報資産について、上記８の情報セキュリティ対策を講ずるに当たっては、遵守すべき行為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上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。

10　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基準を遵守して情報セキュリティ対策を実施するために、個々の情報資産の対策手順等をそれぞれ定めていく必要がある。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、公にすることにより本町の行政運営に支障を及ぼすおそれがあることから非公開とする。

11　情報セキュリティ監査の実施

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、定期的に監査を実施する。

12　評価及び見直しの実施

情報セキュリティ監査の結果等により、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、情報システムの変更、新たな脅威等情報セキュリティを取り巻く状況の変化に対応するために、適宜情報セキュリティポリシー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東栄町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　対象範囲

この情報セキュリティ対策基準は、本町の情報資産、職員等及び外部委託業者を対象とするが、対象とする行政機関の範囲は、 内部部局（総務課、政策推進課、税務会計課、福祉課、経済課、建設課、生活環境課、教育課)、各行政委員会、議会事務局とし、病院機関、教育機関は対象外とする。なお、各教育機関における教育に用いるネットワーク及びシステム等は、情報セキュリティポリシーの対象となるネットワーク及び情報システムと物理的に分けなければならない。

２　組織・体制

東栄町の情報セキュリティの管理については、以下の体制とする。

・ 最高情報統括責任者（ＣＩＯ）
・ ネットワーク管理者
・ 情報セキュリティ管理者
・ 情報セキュリティ担当者
・ 情報システム管理者
・ 情報システム担当者
・ 東栄町情報化推進委員会

３　情報資産の管理責任と分類

（１）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課等の情報セキュリティ管理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

情報資産を複製または伝送した場合には、当該複製等も分類に基づき管理しなければならない。

（２）情報資産の分類

ア　情報資産の分類

対象となる情報資産は、各々の情報資産の機密性、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。

（ｉ）重要性分類Ｉ

・ 個人に関する情報であって、特定の個人が識別され、または識別され得る行政情報。
・ 法令または条例（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行政情報。
・ 法人その他の団体に関する行政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行政情報。
・ 漏洩した場合、行政に対する信頼を著しく害するおそれのある行政情報。
・ 滅失し、またはき損した場合、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行政情報。

・ 上記行政情報を利用する情報システム。
・ 重要性分類に関わらず情報システムに係るパスワード及びシステム設定情報。

（ⅱ）重要性分類Ⅱ

公開することを予定していない情報及びセキュリティ侵害が行政事務の執行等に重大な影響を及ぼす行政情報、及びその情報を利用するシステム。

（ⅲ）重要性分類Ⅲ

外部公開する情報のうちセキュリティ侵害が、行政事務の執行等に軽微な影響を及ぼす行政情報、及びその情報を利用するシステム。

（ⅳ）重要性分類Ⅳ

上記以外の行政情報、及びその情報を利用するシステム。

イ　情報資産の分類に関する表示

情報資産について、第三者が重要性の識別を容易に認識できないように留意しつつ、印刷、ディスプレイ等への表示、記録媒体等に格納する際の媒体（ＦＤへのラベル等）について、ファイル名、記録媒体等に情報資産の分類が分かるように表示をする等適切な管理を行わなければならない。

４　物理的セキュリティ

（１） サーバ等

ア　装置の取付け等

（ⅰ）ネットワーク及び情報システムの取付けを行う場合は、火災、水害、埃、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、容易に取り外せないよう適切な固定等必要な措置を施すことに努め、また、現在取り付けられている装置等については順次、火災、水害等の影響を可能な限り排除した場所に設置する等の措置を講じなければならない。

（ⅱ）次のサーバは冗長構成等をとることに努め、サーバに障害が発生した場合にはシステムの停止を最小限にとどめるようにしなければならない。

・ 重要性分類Ⅱ以上の情報資産を格納しているサーバ
・ セキュリティサーバ

（ⅲ）重要性分類Ⅱ以上の情報資産を格納しているシステムについては、ネットワーク管理者、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すことに努める。

（ⅳ）無線ＬＡＮの導入には、経路を暗号化する等の漏洩防止策を実施しなければならない。

イ　電源

重要性分類Ⅱ以上の情報資産を格納しているサーバ等の機器の電源については、以下の措置を施すことに努める。

（ⅰ）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る。

（ⅱ）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。

ウ　配線

（ⅰ）配線は、傍受または損傷等を受けることがないように壁内、保護材等可能な限り必要な措置を施さなければならない。

（ⅱ）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。

（ⅲ）ネットワーク接続口（ハブのポート等）は、他の者が容易に発見できない場所に設置することに努める。

（ⅳ）ネットワーク管理者、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配線を変更追加してはならない。

エ　外部に設置する装置

（ｉ）外部に設置する装置は、最高情報統括責任者の承認を受けたものでなければならない。また、最高情報統括責任者は、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。

（ⅱ）情報セキュリティ対策基準で定める対象範囲の設置場所（東栄町役場本庁舎、分庁舎及び東栄グリーンハウス内）以外に持ち出される端末、記録媒体等について、最高情報統括責任者は設置場所以外での使用方法を定め、管理簿を設ける等適切に管理しなければならない。

（２）管理区域

ア 管理区域

（ｉ）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、当該機器等または重要性分類Ⅱ 以上の情報資産の管理並びに運用を行うための部屋（以下「管理区域」という。）は、水害対策及び確実な入退室管理を行うために、地階または 1 階に設けることは避けるよう努める。また、外部からの侵入が容易にできない、及び許可されていない立入りを防止するために、無窓の外壁等に囲まれた区域、管理区域から外部に通ずるドアは 1 ヶ所、鍵等を施すことが望ましい。ただし、重要な情報システム等を施錠可能なラックに収納し、他の者が容易に操作できない場所に設置し、その鍵を情報セキュリティ管理者が厳重に管理することで、最高情報統括責任者が承認した場合は、その収納ラックを管理区域として扱うことができる。

（ⅱ）管理区域は、耐震対策、防火措置等を施すことに努める。なお、管理区域内の機器類の配置は、緊急時に職員等が円滑に避難できるように配慮しなければならない。

イ　管理区域の入退室管理

管理区域の入退室は許可された者のみとし、入退室管理簿の記載を行い、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。

ウ　機器等の搬入場所

（ｉ） 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、職員等による確認を行わなければならない。

（ⅱ）機器等の搬入には職員等が同行する等の必要な措置を施さなければならない。

（３）ネットワーク

ア　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。

イ　行政系のネットワークは総合行政ネットワークに集約するように努めなければならない。

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セキュリティ対策が実施されたものでなければならない。

（４）職員等の電子計算機等

情報システムの執務室等の電子計算機については、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。なお、内部ネットワークに接続する機器は、職員等の電子計算機等（個人パソコン不可）のみとし、プリンタ等周辺機器については最高情報統括責任者あるいはネットワーク管理者に申請し許可のある場合のみ接続することができる。

５　人的セキュリティ

（１）役割・責任

ア 最高情報統括責任者（ＣＩＯ）

（ｉ）東栄町副町長を、東栄町における全てのネットワーク、情報システム、情報資産及び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（ＣＩＯ：最高情報統括責任者）とする。

（ii）最高情報統括責任者は、東栄町の全ての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。

（iii）最高情報統括責任者は、東栄町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。

（iv）最高情報統括責任者は、情報セキュリティ管理者、情報システム管理者及び情報システム担当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。

（ｖ）最高情報統括責任者は、東栄町の全てのネットワーク、情報システム及び情報資産に関する情報セキュリティ実施手順の維持・管理を行い、緊急時対応計画に基づく訓練を実施する。

（vi）最高情報統括責任者は職員等（一時的に東栄町における公務員身分を取得した者を除く）のうち、情報通信ネットワーク技術に関する高度な専門的知識と高い公務員倫理を有する者を直属のネットワーク管理者とし、最高情報統括責任者を補佐させることができる。

イ ネットワーク管理者

（ｉ）ネットワーク管理者は、最高情報統括責任者を補佐しなければならない。

（ii）ネットワーク管理者は、東栄町の全ての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。

（iii）ネットワーク管理者は、東栄町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。

（iv）ネットワーク管理者は、情報セキュリティ管理者、情報セキュリティ担当者、情報システム管理者及び情報システム担当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。

（ｖ）ネットワーク管理者は、東栄町の情報資産に対する侵害または侵害のおそれのある場合には、最高情報統括責任者の指示に従い、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。この場合、職員等はネットワーク管理者の指示に従わなければならない。

ウ　情報セキュリティ管理者

（ｉ）内部部局の課室長及び各行政委員会事務局の局長をその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情報セキュリティ管理者とする。

（ii）情報セキュリティ管理者は、最高情報統括責任者の下、所管組織内における情報セキュリティポリシーの遵守に関する権限と責任を有する。

（iii）情報セキュリティ管理者は、所掌に属する課室等における情報資産に対する侵害または侵害の恐れのある場合には、最高情報統括責任者及びネットワーク管理者へ速やかに報告を行い、指示を仰がなければならない。

（iv）情報セキュリティ管理者は、職員等が常に情報セキュリティポリシー及び実施手順を参照できるよう配慮しなければならない。

（ｖ）情報セキュリティ管理者は、非常勤職員及び臨時職員の雇用時には、必ず情報セキュリティーポリシーのうち、職員等が守るべき内容を非常勤職員及び臨時職員に理解させ遵守させなければならない。また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。

（vi）情報セキュリティ管理者は、その所管組織内の職員等（一時的に東栄町における公務員身分を取得した者を除く）のうち、情報通信ネットワーク技術に関する高度な専門的知識と高い公務員

倫理を有する者を情報セキュリティ担当者とし、情報セキュリティ管理者を補佐させることができる。

（vii）所管組織で職員等が使用する電子計算機は所管組織に貸与するものであり、常にその電子計算機を使用する職員等を定めなければならない。

エ　情報セキュリティ担当者

情報セキュリティ担当者は、情報セキュリティ管理者を補佐しなければならない。

オ　情報システム管理者

（ｉ）各情報システムの担当係長等を当該情報システムに関する情報システム管理者とする。

（ii）情報システム管理者は、当該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。

（iii）情報システム管理者は、担当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。

（iv）情報システム管理者は、所管する情報システムにおける開発、設定の変更、運用、更新等を行う権限及び責任を有する。

カ　情報システム担当者

情報システム担当者は、担当する情報システムに関して、情報システム管理者の指示等に従い、開発、設定の変更、運用、更新等の作業を行う。

キ　東栄町情報化推進委員会

（ｉ）情報セキュリティの維持管理を統一的な視点で行うため、情報セキュリティポリシー、情報セキュリティ実施手順等の策定など、情報セキュリティに関する重要な事項を審議する。

（ii）情報セキュリティに対する意識を醸成し保つために、幹部をはじめ全ての職員等が情報セキュリティの重要性を認識し、理解実践するために必要な教育・訓練等を計画的に実施する。

（iii）緊急時対応計画の策定及び見直しを行い、ネットワーク管理者に緊急時対応計画に基づく訓練を実施させ、実際に情報資産の漏洩等の事故が発生した場合に即応できるよう体制を整える。

（iv）本機能は課長会をもって充てることができることとする。

ク　職員等

（ｉ）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。

（ii）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管理者に相談し、指示等を仰がなければならない。

（iii）使用する電子計算機や磁気ディスク等について、第三者に使用されること、また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。

（iv）最高情報統括責任者の許可を得ず、電子計算機等を執務室外に持ち出してはならない。

（ｖ）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。

（vi）情報システムを使用する際の規定

・ 業務目的以外の使用の原則禁止

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る。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。なお、非常勤及び臨時職員が利用する端末においては、インターネットへの接続及び庁内 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設定しなければならない。

・情報資産の持ち出し及びインターネット等による情報資産の送信禁止

職員等は、重要性分類上Ⅱ以上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。

・　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（特にインターネットへの自動転送は厳禁）
・　個人の所有する媒体の管理区域への持ち込み

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限り、庁外への持ち出しまたは庁外との送受信ができるものとし、その場合、最高情報統括責任者が定めた方式を用いなければならない。

・無許可ソフトウエアの導入の禁止

職員等は、各自に供用された電子計算機に対して、最高情報統括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。特にネットワーク上の情報資産を盗聴するような監視ソフトウエアやネットワークの状態を探索するセキュリティ関連のソフトウエア及びハッキングソフトウエアの使用は厳禁する。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、合理的理由があり、安全性が確認され、正規のライセンスを所有し、かつネットワーク管理者及び情報システム管理者の事前の許可を得た場合は利用することができる。特にソフトウエアの交換を行う場合は、著作権及び著作権隣接権を守らなければならない。

・機器構成の変更の禁止

職員等は、各自に供用された電子計算機等に対して機器の増設または改造を行ってはならない。特にモデム等を増設して他の環境（インターネット等）へのネットワーク接続を行うことや、庁外からのアクセスを可能とする仕組みを構築することは厳禁する。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、かつネットワーク管理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、機器の増設または変更を行うことができる。

・メール

- メールの自動転送機能を利用して、不必要な者へ職場のメールを転送してはならない。
- 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。
- 差出人が不明な、または不自然なファイルの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。

・文書共有機能

- 文書共有機能は課室等単位で構成管理し、他課室等のフォルダ及びファイルを閲覧及び使用してはならない。
- 同一課室等であっても、住民の個人情報、人事記録等特定の職員等しか取扱えないデータについては、別途、担当職員等以外の職員等が閲覧及び使用できないような設定を施さなければならない。

ケ　外部委託に関する管理

（ⅰ）システムの受託事業者への規定

・信頼のおける事業者に委託するために、必要な資格等を定めなければならない。
・委託に関する責任を有する部署を明確にし、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することに努めなければならない。
・再委託契約を行う際には再委託先について契約課において経営状況等、契約履行が可能であるか確認をとり、導入前の検査要求事項等を契約に定めなければならない。

（ⅱ）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

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、その遵守を管理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
・東栄町に対する報告義務
・東栄町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以上の情報資産に関しては、情報システムにおける取扱いのみでなく、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。

（iii）電子計算機処理を外部委託する場合

東栄町電子計算機委託処理に関するデータ保護管理規定（昭和６３年３月３日訓令第５号）によりデータ保護を図るものとする。

（２） 教育・訓練

（ｉ）最高情報統括責任者は、説明会の実施等により職員等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。情報セキュリティポリシーに関する教育・訓練プログラムは、情報化推進委員会で承認されたものを使用する。

（ii）最高情報統括責任者は、ネットワーク管理者、情報セキュリティ管理者、情報システム管理者及び情報システム担当者に対して、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。

（iii）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。

（iv）情報システム管理者及び情報システム担当者は、情報システムに関する研修を受けなければならない。

（ｖ）情報システム管理者は、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。また、より効果的に実施できるよう計画を立てることとする。

（vi）職員等は、定められた研修に参加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。

（３） 事故、欠陥に対する報告

（ｉ）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、速やかにネットワーク管理者に報告し、ネットワーク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。ネットワーク管理者は最高情報統括責任者に報告し、また職員等は情報セキュリティ管理者に報告しなければならない。

（ii）ネットワーク管理者は、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。

（４） アクセスのための認証情報及びパスワードの管理

（ｉ）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、カードリーダまた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、速やかにネットワーク管理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。
・ ネットワーク管理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。

（ii）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応じないこと。

パスワードのメモを作らず、文字長は十分なものとし文字列は想像しにくいものとすること。

・ パスワードに対する漏えいの恐れがある場合には、速やかに変更すること。
・ パスワードは定期的に、またはアクセス回数に基づいて変更し、古いパスワードの再利用はしないこと。管理者用パスワードはさらにこのサイクルを頻繁にしなければならない。
・ 複数の情報システムを扱う職員等は、パスワードをシステム間で共有しないこと。
・ パスワードは、最初のログイン時点で変更すること。
・ 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。

（iii）パスワードの管理方法

・ ネットワーク管理者または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。
・ ネットワーク管理者または情報システム管理者は、パスワードが漏洩、またはその疑いがある場合は、当該職員等にパスワードを変更する旨勧告し、当該職員等が勧告に従わない場合には、当該職員等のアクセス権を一定期間経過後に停止するものとし、当該職員等からパスワード変更の申告があり次第当該職員等のアクセス権の停止を解除するものとする。

６　技術的セキュリティ

（１）情報資産の管理

情報資産の重要性分類に従って情報資産を以下のとおり管理する。

ア　Ⅰ及びⅡ

（ｉ）アクセス記録の取得

・ 情報システム管理者はアクセス記録及び情報セキュリティ関連障害に関する記録を取得し、一定期間保存することに努める。
・ 情報システム管理者はアクセス記録が盗難、改ざん、消去等をされないように必要な措置を施すことに努める。
・ 情報システム管理者はアクセス記録を定期的に分析、監視することに努める。

（ii）情報システム仕様書の管理

・ 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、業務上必要とする者のみが閲覧できるようにしなければならない。
・ 情報システム管理者はシステムの変更が生じた場合にはその変更を記録し、仕様書を修正し最新の状態にしなければならない。また、その変更の記録を作成しなければならない。

（iii）情報資産の管理

・ アクセス権限

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、情報資産の分類に従いアクセス権限を定め、パスワード等によるアクセス制限を行うことに努める

・ 保管管理
  - 緊急時に直ちに対処できるようにするため、最高情報統括責任者が定めた特に重要な情報システムは、外部媒体へバックアップを取らなければならない。なお施錠可能等特に安全な場所へ保管することに努める。
  - 最終的に確定した行政情報は別の磁気ディスク等に複製し、当該磁気ディスク等は、書込禁止措置を行った上で保管しなければならない。

・日常管理

・ 電子計算機及び磁気ディスク等は、外部からの脅威にさらされないように施錠可能等安全な場所に保管することに努める。
・ 電子計算機に納められた行政情報は定期的に別の磁気ディスク等に複製し、当該磁気ディスク等は自然災害を被る可能性が低い地域に保管しなければならない。
・ 最高情報統括責任者が定めた重要なネットワーク及び情報システムは、システムを冗長化するなど直ちに復旧できるようにしなければならない。また、その動作検証を少なくとも四半期ごとに行うことに努める。

・ 情報資産の移動等

・ ネットワーク管理者は、職員等が送信等により情報資産を外部に持ち出すことを制限しなければならない。
・ 職員等は、行政情報の不用意な複製、外部への持ち出し、送付及び送信を行ってはいけない。
・ 外部への持ち出し、送付及び送信する場合、行政情報の複製を保管場所へ移動する場合、当該保管場所からシステム復旧のために情報システム設置個所に戻す場合等業務上必要な場合には、最高情報統括責任者の許可を得たうえで行わなければならない。
・ 電子計算機及び磁気ディスク等を外部への持ち出し、送付及び送信を外部業者に行わせる場合は、守秘義務、複製の禁止を明記した契約を締結し、物理的保護措置を講じなければならない。

・ 暗号化

・ 情報システム管理者は、重要性分類Ⅰの行政情報には暗号化を施すことに努め、暗号鍵及び暗号化した当該行政情報は別々に適切な管理をしなければならない。
・ 暗号化は、最高情報統括責任者が定めた方式でなければならない。また、暗号のための鍵は重要性分類Ⅰの行政情報として厳重に管理しなければならない。

（ⅳ）情報資産廃棄及び廃棄管理

電子計算機及び磁気ディスク等が不要となった場合は、当該磁気ディスク等に含まれる重要性分類Ⅱ以上の行政情報は、磁気ディスク等の初期化など行政情報を復元できないように消去を行ったうえ廃棄しなければならない。なお、日時、担当者及び処理内容を記録する。

（ⅴ）情報資産の修理

記憶媒体の含まれる機器について、外部の事業者に修理させる場合は、可能な限りバックアップを取り、その内容が消去された状態で行わなければならない。なお、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秘密を守ることを定めなければならない。

イ　Ⅲ及びⅣ

原則、重要性分類Ⅱ以上に分類される情報資産の管理に準拠するが、重要性分類Ⅲ以下の情報資産は公開を前提としているため、この範囲において基準を緩和することができる。ただし、保管管理及び日常管理については行政情報の完全性及び可用性を維持するため、極力実施することが望ましい。

（２）他システムに対する影響

Web サイトにより情報を公開・提供する場合には、当該サイトに係るシステムにおいて盗難、改ざん、消去、踏み台、ＤｏＳ等を防止しなければならない。またメールシステム等においても、他システムに対する攻撃の踏み台とならないように適切な管理を実施することに努める。

（３）アクセス制御

ア　利用者登録

情報システムへのアクセスは業務要件に従って許可するものとし、ネットワーク管理者及び情報システム管理者は、利用者の登録、変更、抹消、異動や東栄町外への出向等の職員等及び退職者における利用者ＩＤの取扱い等については、定められた方法に従って行わなければならない。

イ　管理者権限

（ｉ）ネットワーク管理者の権限は、1 人の者に与え厳重に管理しなければならない。

（ii）ネットワーク管理者の権限を代行する者は、ネットワーク管理者が指名し、最高情報統括責任者が認めた者でなければならない。代行者を認めた場合、最高情報統括責任者は速やかに情報セキュリティ管理者及び情報システム管理者に周知しなければならない。

（iii）情報システム管理者の権限は、必要最小限の者に与え、厳重に管理しなければならない。

（iv）情報システム管理者の権限を代行する者は、情報システム管理者が指名し、最高情報統括責任者が認めた者でなければならない。代行者を認めた場合、最高情報統括責任者は速やかにネットワーク管理者及び情報セキュリティ管理者に周知しなければならない。

ウ　インターネット以外のネットワークアクセス制御

（ｉ）ネットワーク管理者は、不必要なネットワークサービスにアクセスにできないよう必要な措置を講じなければならない。

（ii）ネットワーク管理者及び情報システム管理者は、ネットワークサービスを使用する権限を有しない職員等が当該サービスを使用できるようにしてはならない。

エ　外部からのアクセス

（ｉ）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。この場合、内部のネットワーク及び情報システムとの間にＩＰリーチャビリティが発生しないように機器を構成しなければならない。

（ii）アクセス方法及び使用方法等は、利用者の真正性の確保ができるものでなければならない。

（iii）モバイル端末による内部ネットワーク及び情報システムに対するアクセスは、合理的理由を有し、かつネットワーク管理者が定める必要最小限の者に限定しなければならない。

オ　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当面は接続しない。

カ　外部ネットワークとの接続

（ｉ）外部ネットワークとの接続にあたり、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、東栄町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管理者の許可に基づき接続しなければならない。

（ii）利用はネットワーク管理者の適切な管理下で行い、接続に際しては内部ネットワークの安全性が脅かせることのないよう情報セキュリティに留意したネットワーク構成を採らなければならない。

（iii）当該外部ネットワークの瑕疵により東栄町のデータの漏洩、破壊、改ざんまたはシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保しなければならない。

（iv）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、東栄町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。

（ｖ）内部ネットワークのセキュリティに問題が認められた場合は、ネットワーク管理者の判断に従い速やかに当該内部ネットワークと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　職員等以外の者が利用するシステム

汎用受付システム等外部の者が利用するシステムにおいては、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ける等、情報セキュリティ対策について特に強固に対策をとらなければならない。

ク　接続時間の制限

情報システムの接続については、通常に利用する場合や管理者権限による場合を問わず、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） システム開発、導入、保守等

ア 情報システムの調達

（ｉ）最高情報統括責任者は機器及びソフトウエアの導入、保守及び撤去についての手順及び基準を明らかにしなければならない。

（ii）情報システムの調達にあたっては、調達仕様書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。

イ　ネットワーク及び情報システムの更新

（ｉ）ネットワーク管理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を更新するに当たり、更新内容、必要性、計画等を最高情報統括責任者に提出し承認を得なければならない。

（ii）ネットワーク及びシステムの移行は擬似環境による動作確認後に行わなければならない。なお、移行の際には職員等の立会い、作業内容を記録のもと、記録されている情報資産の保存を行い、復帰が即座に可能な状態で、原則執務時間外に行うこととする。

ウ　情報システムの導入及び保守

（ｉ）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を行わなければならない。

（ii）情報システム管理者は、試験に使用したデータ及びその結果を最高情報統括責任者及びネットワーク管理者へ提出するとともに厳重に保管しなければならない。

（iii）最高情報統括責任者及び情報システム管理者はシステム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実施しなければならない。なおシステム開発は内部ネットワークで行ってはならない。

・ 責任者及び監督者
・ 作業者及び作業範囲
・ システム開発及び保守等の事故・不正行為に係るリスク分析
・ 開発・保守に関するソースコードの提出
・ 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
・ 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
・ 保守を行う者の利用者 ID、パスワード等の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

エ ソフトウエアの更新及び修正

（ｉ）情報システム管理者はソフトウエア等を更新、また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、計画的に更新しまたは導入しなければならない。

（ii）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。

（５）コンピュータウイルス対策

ア　ネットワーク管理者は、次の事項を実施しなければならない。

（ｉ）情報システムの電子計算機及び必要な機器にウイルス対策ソフトを導入すること。

（ii）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。（iii）常時ウイルスに関する情報収集に努めること。

イ　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。

当該システムの電子計算機のウイルスチェック用パターンファイルは常に最新のものに保つこと。

ウ　職員等は、次の事項を遵守しなければならない。

（ｉ）使用する電子計算機のウイルスチェック用パターンファイルは常に最新のものに保つこと。

（ii）外部からデータまたはソフトウエアを取り入れる場合、または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。

（iii）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。

エ　ネットワーク管理者及び情報システム管理者は、職員等から報告のあった情報、システムの障害に対する処理または問題等は障害記録として体系的に記録し、常に活用できるよう保存しなければならない。

（６）不正アクセス対策

ア　ネットワーク管理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。

（ｉ）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。

（ii）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ができるよう、適切な対策に努めなければならない。

（iii）攻撃を受けていることが明らかな場合は、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。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。

（iv）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。

イ　職員等による不正アクセス及び怠惰があった場合、ネットワーク管理者または情報システム管理者は当該職員等が所属する課室等の情報セキュリティ管理者に通知し、適切な処置を求めなければならない。

７　運用

（１）情報システムの監視

ア　ネットワーク管理者及び情報システム管理者はセキュリティに関する事案を検知するため、常に情報システムの監視を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。

イ　外部と常時接続するシステムについて、ネットワーク侵入監視装置を設置し２４時間監視を行う機器の導入することに努める。

ウ　内部のシステムについて、アクセス制御等を行い異常な運用等の監視を行う機器の導入することに努める。

エ　監視により得られた結果については、盗難、改ざん、消去等を防止するために必要な措置を施し、安全な場所に保管しなければならない。

（２）情報セキュリティポリシーの遵守状況の確認

ア　情報セキュリティ管理者は、情報セキュリティポリシーの遵守について、また問題が発生していないかについて注意を払い、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管理者に報告しなければならない。

イ　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、直ちにネットワーク管理者及び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。

ウ　ネットワーク管理者及び情報システム管理者は、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）運用管理における留意点

最高情報統括責任者は、アクセス記録、メール等個人のプライバシーに係る情報を閲覧できる権限を有するためには、情報セキュリティ実施手順に定めなければならない。ただし、法令で定められた個人情報の保護に関係する情報の閲覧に関しては、当該法令に定められた手続に従う。

（４）緊急時対応計画

情報資産への侵害が違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される場合は、緊急時対応計画に従って連絡を行わなければならない。発生した場合における連絡、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じるために、緊急時対応計画を次のとおり定める。

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管理者に報告しなければならない。

（ｉ）症状の分類

（ii）事案が発生した原因として想定される行為

（iii）確認した被害影響範囲

（iv）記録

ネットワーク管理者は、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情報化推進委員会への報告を行わなければならない。

イ　事案への対処

（ｉ）被害拡大の防止措置

・ネットワーク管理者は、事案に対処するために次の項目を実施しなければならない。

- ネットワーク管理者は、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、その他の町民に重大な被害が生じる恐れがあるとき（東栄町長、最高情報統括責任者、警察、影響が考えられる個人及び法人、必要と認められる外部委託事業者）
  - ✧ 不正アクセス、その他犯罪と思慮されるとき（東栄町長、最高情報統括責任者、警察、必要と認められる外部委託事業者）
  - ✧ 踏み台となって他者に被害を与える恐れがあるとき（東栄町長、最高情報統括責任者、警察、必要と認められる外部委託事業者）
  - ✧ 情報システムに関する被害（情報システム管理者、必要と認められる外部委託事業者等）
  - ✧ その他情報資産に係る被害（関係部局、必要と認められる外部委託事業者等）
- ネットワーク管理者は、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、また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

・ 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およぼしているとき
✧　災害等により電源を供給することが危険または困難なとき
✧　その他の情報資産に係る重大な被害が想定されるとき

・事案に係るシステムのアクセス記録及び現状、対処した経過等を記録しなければならない。
・事案に係る証拠保全実施を完了するとともに、再発防止の暫定措置を検討しなければならない。
・再発防止の暫定措置を講じた後、復旧しなければならない。
・復旧後、必要と認められる期間、再発監視をしなければならない。

ウ　再発防止の措置

（ｉ）ネットワーク管理者は、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、情報化推進委員会へ報告しなければならない。情報化推進委員会は、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、これを承認しその措置を講じる。

（ⅱ）ネットワーク管理者は、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。

８　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）

９　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。

・ネットワーク管理者が違反を確認した場合は、ネットワーク管理者は当該職員等が所属する課室等の情報セキュリティ管理者に通知し、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ネットワーク管理者及び当該職員等が所属する課室等の情報セキュリティ管理者に通知し、適切な措置を求めなければならない。
・情報セキュリティ管理者の指導によっても改善されない場合、ネットワーク管理者は、当該職員等のネットワークまた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、ネットワーク管理者は、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課室等の情報セキュリティ管理者に通知しなければならない。

10　評価・見直し

（１）監査

（ｉ）情報化推進委員会の内部監査班は、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監査を定期的に行わなければならない。

（ii）監査の実施方法時期等については最高情報統括責任者が別に定めるものとする。

（iii）監査結果は情報化推進委員会に報告し、情報化推進委員会は、この報告結果を最高情報統括責任者及びネットワーク管理者に通知するとともに、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

情報セキュリティ管理者は、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アンケート等を行い、また自主点検を行わなければならない。情報セキュリティ管理者はこれらをとりまとめ、情報化推進化委員会に報告する。情報化推進委員会は、この報告結果を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

新たに必要な対策が発生した場合または監査の結果及び点検の結果を踏まえ、情報化推進委員会において情報セキュリティポリシーの実効性を評価し、必要な部分を見直し、内容、時期について決定を行う。この決定に基づき、情報セキュリティポリシーの更新を実施する。更新の内容については、情報化推進委員会が決定しなければならない。