情　報　セキュリティポリシー
（　基　本　方　針　）

平成17年　7月　　7日　制定

令和　8年　2月　24日　改定

清須市行政情報化推進委員会

［目　次］

序章　情報セキュリティに対する考え

法令等に基づき、市民の個人情報や企業の経営情報等の重要情報を多数保有し、他に代替することができない行政サービスを提供している。行政サービスの業務の多くは、情報システムやネットワークを活用していることから、情報セキュリティ対策を講じて、市民生活や地域の社会経済活動を保護するために、保有する情報を守り、業務を継続することが必要となっている。

今後、各種手続のオンライン利用の本格化や情報システムの高度化等、電子自治体が進展することにより、情報システムへの依存度が増え、システムトラブルが発生した場合、広範囲の行政サービスが継続できなくなり、市民生活や地域の経済社会活動に重大な影響を与える。LGWAN 等のネットワークにより地方自治体が相互に接続していることから、一部の団体のシステムトラブルがネットワークを介して、他の地方公共団体に連鎖的に拡大することも考えられる。

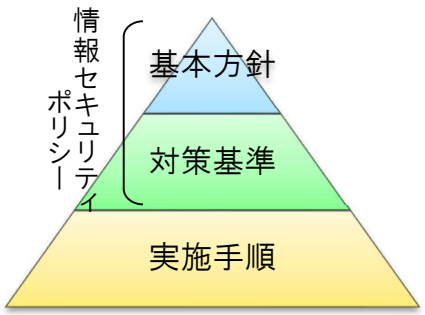
これらの事情から、情報セキュリティ対策の実効性を高めるとともに、対策レベルを一層強化していくことが必要となっている。

情報セキュリティ対策は、情報の保護の点では、個人情報保護対策と内容的に重なる部分も多く、自然災害などの対応という点では、防災対策とも重なる。関連部署は、相互に連携をとって、それぞれの対策に取り組み、情報セキュリティに関する事故の未然防止のための計画、事故が発生した場合の拡大防止・迅速な復旧や再発防止の対策を、講じていくことが必要である。

◇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を、一定の普遍性を備えた部分（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（対策基準）に分けて策定することとした。

具体的には、情報セキュリティポリシーを、「情報セキュリティ基本方針」、「情報セキュリティ対策基準」の2階層に分けて、それぞれを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、情報システムごとの具体的な情報セキュリティ対策の実施手順として、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）。



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
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対する共通の情報セキュリティ対策の基準
実施手順	ネットワーク及び情報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具体的な実施手順

情報セキュリティ基本方針

1. 目的

清須市の各情報システムが取り扱う情報には、市民の個人情報のみならず、行政運営上の重要な情報など外部への漏えい等が発生した場合に、極めて重大な結果を招く情報が多数含まれている。

したがって、情報資産、情報資産を取り扱うネットワーク及び情報システムを様々な脅威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、事務の安定的な運営のためにも必要不可欠である。ひいては、このことが清須市に対する市民からの信頼の維持向上に寄与するものである。

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いる。清須市が電子自治体を構築するためには、全てのネットワーク及び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、清須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（情報セキュリティ対策）を整備するために、清須市情報セキュリティポリシーを定めることとし、このうち、情報セキュリティ基本方針については、清須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（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） ネットワーク

清須市における内部部局、各行政委員会、議会事務局、議会、地方公営企業及び各教育機関（事務室、校長室及び職員室のみ）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、処理を行う仕組みをいう。

（2） 情報システム

業務系の電子計算機（業務系におけるネットワーク、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、処理を行う仕組みをいう。

（3） 情報資産

ネットワーク及び情報システムの開発と運用に係る全ての情報並びにネットワーク及び情報システムで取り扱う全ての情報をいう。

なお、情報資産には、紙等の有体物に出力された情報も含むものとする。

（4） 情報セキュリティ

情報資産の機密の保持及び正確性、完全性の維持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。

（5） 情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

（6） 機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

（7） 完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

（8） 可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

（9） 職員等

清須市長を始めとする全ての職員（定年前再任用短時間勤務職員、暫定再任用職員、任期付職員、会計年度任用職員を含む）のことをいう。

3. 対象とする脅威

情報セキュリティポリシーを策定するうえで、発生度合や発生した場合の影響を考慮すると、情報資産に対する特に認識すべき脅威は、以下のとおりである。

- 不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や、部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等
- 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等
- 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
- 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
- 電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

4. 適用範囲

（1） 機関の範囲

本基本方針が適用される機関は、内部部局、各行政委員会、議会事務局、議会及び地方公営企業とし、各教育機関（事務室、校長室及び職員室を除く）は、対象外とする。

（2） 情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

- ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体
- ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）
- 情報システムの仕様書及びネットワーク図等のシステム関連文書

5. 職員等の遵守義務

情報セキュリティポリシーは、清須市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。

したがって、清須市が所掌する情報資産に関する業務に携わる全ての職員等及び外部委託事業者（以下、職員等情報取扱者という。）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、業務の遂行にあたっては、情報セキュリティポリシーを遵守する義務を負うものとする。

6. 情報セキュリティ対策

「3. 対象とする脅威」で示した脅威から情報資産を保護するために、以下の情報セキュリティ対策を講ずるものとする。

（1） 組織体制

清須市の保有する情報資産を、適切に情報セキュリティ対策を推進・管理するため、全庁的な組織体制を確立する。

必要な体制、役割、権限等については、情報セキュリティ対策基準にて定める。

（2） 情報資産の分類と管理

清須市の情報資産について、市長を始めとする二役及び教育長、部局長、次長が率先して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。

清須市の保有する情報資産を、機密性、完全性及び可用性に応じて分類し、当該分類に基づいて情報セキュリティ対策を実施する。

（3） 物理的セキュリティ対策

情報システムを設置する施設への不正な立入り、サーバ等、情報システム管理室等、通信回線等及び職員等のパソコン等の損傷・妨害等から保護するために物理的な対策を講じる。

（4） 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、職員等情報取扱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じる。

（5） 技術的セキュリティ対策

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、コンピュータやネットワーク等の管理、情報資産へのアクセス制御、不正プログラムの防御等の技術面の対策を講じる。

（6） 運用に関する対策

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、システム開発等の外部委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じる。

また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適切に対応するため、緊急時対応計画を策定する。

（7） 業務委託と外部サービス（クラウドサービス）の利用

業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者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、必要に応じて契約に基づき措置を講じる。

外部サービス（クラウドサービス）を利用する場合には、利用に係る規定を整備し対策を講じる。

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

7. 情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

8. 情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果等により、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を実施するとともに、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、情報セキュリティポリシーの見直しを実施する。

9. 情報セキュリティ対策基準の策定

清須市の様々な情報資産の情報セキュリティ対策を講じるために、上述の「6. 情報セキュリティ対策」、「7. 情報セキュリティ監査及び自己点検の実施」、「8. 情報セキュリティポリシーの見直し」の具体的な遵守すべき事項及び判断等の基準を定める情報セキュリティ対策基準を策定する。

10. 情報セキュリティ実施手順の策定

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。そのため、情報資産に対する脅威及び情報資産の重要度に対応する情報セキュリティ対策基準の基本的な要件に基づき、内部部局の長等が所掌する情報資産の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、清須市の行政運営に重大な支障を及ぼす恐れがある情報資産であることから非公開とする。