三重県情報セキュリティポリシー
サイバーセキュリティ・情報セキュリティ基本方針

三重県

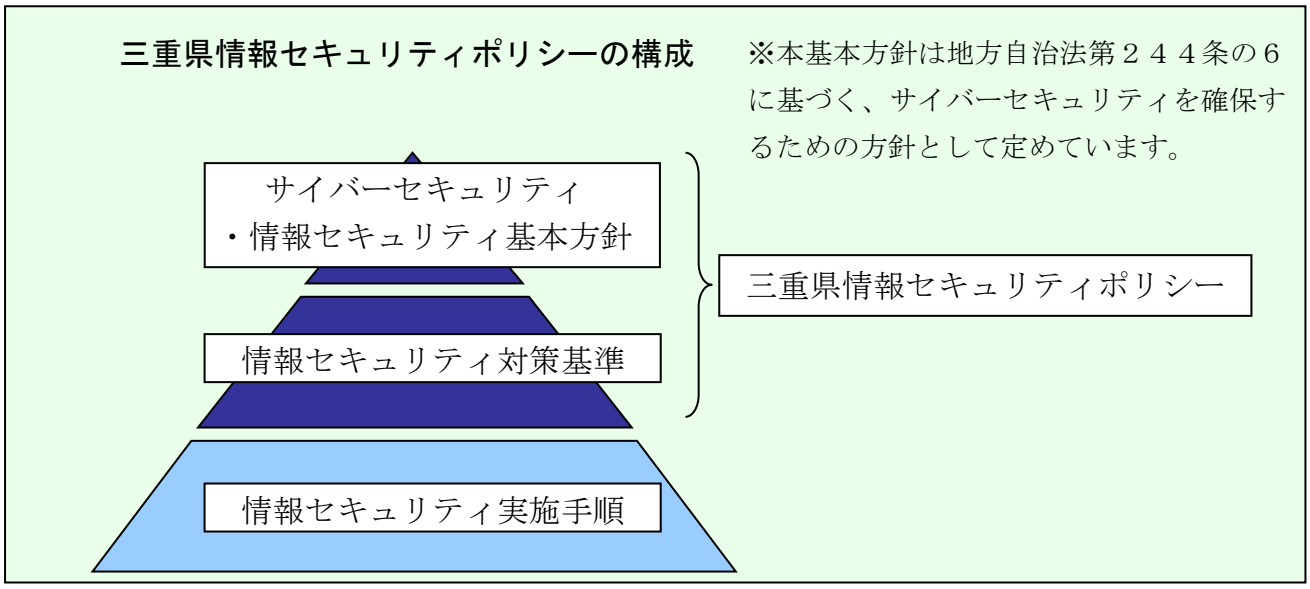
目　　次

第1章 目的

三重県の各情報システムが取り扱う情報には、県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極めて重大な結果を招く情報が多数含まれている。

これらの情報及び情報を取り扱う情報システムを様々な脅威から防御し、県民の財産、プライバシー等を守るとともに、事務の安定的な運営を行い、県民からの信頼の維持向上を図るため、三重県情報セキュリティポリシー（以下「ポリシー」という。）を定める。

このうち、ポリシーの対象、位置付け等基本的な事項についてサイバーセキュリティ・情報セキュリティ基本方針（以下「本基本方針」という。）に定めるものとする。



第2章 定義

1　ネットワーク

通信網、通信関連機器、配線をさす。

2　情報システム

コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報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データ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データをいう。

4　機密性

許可された者のみが情報にアクセスできる状況を保持し、第三者に知られてはいけない情報が漏洩するのを防止することをいう。

5　完全性

情報の一部が欠如したり、全部又は一部が改ざんされることのないようにすることをいう。

6　可用性

許可された利用者が必要な情報にアクセスできる状態を保持することをいう。

7　情報セキュリティ

情報資産の機密性・完全性・可用性を維持することをいう。

第3章 情報資産への脅威

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と、特に認識すべき脅威は以下のとおりである。

脅威一覧

脅威の種類	脅威の詳細
災害	火災、落雷、地震、風水害、その他災害等
障害	コンピュータシステム障害、諸設備の障害（電源設備への配慮、安定した電源供給)、ネットワーク障害等
人的エラー	ソフトウェアのミス、データ入出力エラー、その他運用管理ミス等
不正／犯罪	ソフトウェアの不正、不正アクセス、データの改ざん／削除、不正操作、不正流出、機器・設備の損壊／動作障害等

第4章 適用範囲

（1）対象機関の範囲

本基本方針が対象とする機関の範囲は、知事、議会、教育委員会、選挙管理委員会、人事委員会、監査委員、労働委員会、収用委員会、海区漁業調整委員会、内水面漁場管理委員会及び公営企業管理者とする。

（2）情報資産の範囲

本基本方針が対象とする情報資産範囲は、（1）に定める機関が所管する次のとおりとする。

ア　ネットワーク、情報システム及びこれらに関する設備及び電磁的記録媒体

イ　ネットワーク及び情報システムで取り扱う情報

ウ　情報システムの仕様書及びネットワーク図その他の情報システムに関する文書

第5章 ポリシーの位置付け及び職員等の遵守義務

ポリシーは、第4章で定める対象機関（以下「対象機関」という。）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、電子情報に関する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、対象機関が所掌する情報資産に関する業務に携わる者（以下「職員等」と表記する。）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、業務の遂行に当たってポリシーを遵守する義務を負うものとする。

第6章 情報セキュリティ対策

1　情報セキュリティ組織体制

対象機関が所掌する情報資産について、最高情報セキュリティ責任者（CISO）が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。

２　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。

３　情報セキュリティ対策

上記第３章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。

３－１　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、情報資産への損傷・妨害等から保護するために物理的な対策を講ずる。

３－２　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、対象機関の職員等に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。

３－３　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、情報資産へのアクセス制御、ネットワーク管理等の技術面の対策、また、システム開発等の委託、ネットワークの監視、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事後管理対策を講ずる。

第7章 情報セキュリティ監査の実施及び自己点検の実施

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、又は必要に応じて情報セキュリティに関する監査及び自己点検を実施する。

第8章 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、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、ポリシーの見直しを実施する。

第9章 情報セキュリティ対策基準の策定

対象機関の様々な情報資産について、上記第６章に規定する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について各機関の業務の内容・性質に応じて適切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等を各機関で策定するものとする。

なお、情報セキュリティ対策基準等は、公にすることにより各機関の運営に支障を及ぼす恐れのあることから非公開とする。

第10章 情報セキュリティ実施手順の策定

対象機関が組織として管理する情報システム及びネットワークの管理者は、上記第９章に規定する情報セキュリティ対策基準等に基づき、当該情報システムに関する情報セキュリティ対策の具体的な手順を定めた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各機関の運営に重大な支障を及ぼす恐れのあることから非公開とする。

附　則

この基本方針は、令和８年４月１日から施行する。