岡山県電子自治体推進協議会
情報セキュリティポリシー

平成１７年３月２５日　策定

＜目　　次＞

序章　情報セキュリティポリシーの趣旨

岡山県電子自治体推進協議会（以下，協議会）では，県と県下市町村が協働し，住民サービスにおける新たな価値を創造するためインフォメーションテクノロジー（以下，IT）を活用した電子自治体の構築を進めている。

情報セキュリティポリシーは，協議会が所掌する情報資産に関する情報セキュリティ対策に関する，総合的，体系的かつ具体的な取り決めを総称するものである。協議会の情報資産に関する業務に携わる県，市町村の職員及び協議会の情報資産を取り扱う全ての人々に浸透，定着させ，安定運用を実現しなければならない。高度な技術革新が日々行われるなか，急速，急激な変化へ柔軟に対応する必要がある。この対策として，協議会では，情報セキュリティポリシーを普遍的な基盤（基本方針）と情報資産を取り巻く環境変化に追従し進化させる手段（対策基準）に分けて策定した。

基盤：情報セキュリティ基本方針
手段：情報セキュリティ対策基準

なお，本情報セキュリティポリシーの策定及び改定は協議会規約第１１条に定める運営委員会において行うものとする。

第１章　情報セキュリティ基本方針

１　趣旨

協議会は，岡山県及び県内市町村（以下，市町村）を会員として，会員が共同利用する情報システムの整備及び運営管理を行う。協議会の各情報システムが取り扱う情報には，住民及び事業者等，協議会の提供するサービスの利用者（以下，利用者）の個人情報に加えて，会員の行政運営上重要な情報，いわゆる外部への漏洩等が重大なセキュリティ犯罪に繋がる情報が多数存在している。従って，協議会の情報資産を種々の脅威から完全に保護し，安全性を確保することは，利用者の財産，プライバシー等を守るとともに，協議会及び会員の事務の安定的な遂行のために必須である。そのため協議会の情報資産の情報セキュリティ（機密性，完全性及び可用性）を維持する対策（情報セキュリティ対策）を整備するために情報セキュリティポリシーを定めることとし，情報セキュリティ基本方針では，協議会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。

２　用語の定義

（１）情報資産

情報システムの開発と運用に係る全ての情報並びに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。

（２）ネットワーク

協議会の各種関係機関を相互に接続するための通信網をいう。

（３）情報システム

共同利用する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。

（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）協議会の会員

岡山県電子自治体推進協議会規約第５条に定める会員。

（６）データセンター

岡山県データセンターをいう。

（７）利用者

上記（３）で定める情報システムを利用する住民及び事業者をいう。

（８）職員

協議会が所掌する情報資産に関する業務に従事する県，市町村の全職員（非常勤職員及び臨時職員を含む）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，協議会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　情報セキュリティ管理体制

情報セキュリティ基本方針に基づき，協議会の情報資産について，情報セキュリティ対策を推進，管理するため，協議会の運営委員長を最高責任者とする情報セキュリティ管理体制を確立する。

５　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セキュリティレベルを定め，情報セキュリティ対策を実施する。

６　情報資産への脅威

発生頻度，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次に掲げるものである。

（１）利用者による機器又は情報資産の破壊，盗難，故意の不正アクセス又は不正操作による機器又は情報資産の破壊，盗聴，改ざん，消去等

（２）職員による機器又は情報資産の持ち出し，誤操作，アクセスのための認証情報又はパスワードの漏えい，故意の不正アクセス又は不正行為による破壊，盗聴，改ざん，消去等

（３）地震，落雷，火災等の災害並びに事故，故障，コンピュータウイルス感染等による行政サービス及び業務の停止

７　情報セキュリティ対策

協議会で所掌する情報資産を上記６で示した脅威から保護するために，以下の情報セキュリティ対策を講ずるものとする。

（１）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による破壊，盗難の防止，災害による情報資産への損害等から保護するために物理的な対策を講ずる。

（２）技術的セキュリティ対策

情報資産を不正アクセス，不正運用，コンピュータウイルス等から保護するための技術的なセキュリティ対策を講ずる。

（３）人的セキュリティ対策

職員の情報セキュリティに関する権限や責任を定め，情報セキュリティポリシーの内容を周知徹底を図るための十分な教育及び啓発が講じられる教育を講ずる。

８　情報セキュリティ対策基準の策定

協議会で所掌する情報資産について，上記７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基準を定める必要がある。そのため，情報セキュリティポリシー基本方針を実現するため情報セキュリティ対策基準を策定する。

９　情報セキュリティ実施手順の策定

業務ごとに情報セキュリティポリシーを遵守して情報セキュリティ対策を実現するための具体的な手順を明記した運用マニュアル等を情報セキュリティ実施手順として策定する。

10　対策基準及び実施手順の扱い

対策基準及び実施手順については、公にすることで協議会の運営及び会員の行政運営に重大な支障を及ぼす恐れがあるため原則非公開とする。

11　情報セキュリティポリシーの遵守（会員の義務）

協議会の会員は，情報セキュリティの重要性について十分認識し，業務の実施にあたり情報セキュリティポリシーを遵守する責任を負う。

なお，協議会の会員が所掌する情報資産に関しては，会員の情報セキュリティポリシーが適用さ

れる。ただし，協議会が会員共通として所掌する情報資産については，この情報セキュリティポリシーが会員の情報セキュリティポリシーに優先して適用されるものとする

12　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。

13　評価及び見直しの実施

情報セキュリティ監査の結果等を分析し，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定期的に実施し，情報セキュリティを確保する。