宇佐・高田・国東広域事務組合
情報セキュリティポリシー

宇佐・高田・国東広域事務組合

〈 目 次 〉

序 情報セキュリティポリシーの構成 …… 2

第１章 情報セキュリティ基本方針 …… 3

１ 目的 …… 3

２ 定義 …… 3

３ 情報セキュリティポリシーの位置付けと職員等及び外部委託事業者の義務 …… 4

４ 情報セキュリティ管理体制 …… 4

５ 情報資産及び情報システムの分類 …… 4

６ 情報資産及び情報システムへの脅威 …… 4

７ 情報セキュリティ対策 …… 4

８ 情報セキュリティ対策基準の策定 …… 5

９ 情報セキュリティ実施手順の策定 …… 5

10 評価及び見直しの実施 …… 5

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、本組合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を総称する。情報セキュリティポリシーは、本組合が所掌する情報資産に関する業務に携わる職員(嘱託職員、会計年度任用職員、臨時職員を含む。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(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、

1　情報セキュリティ基本方針
2　情報セキュリティ対策基準

の２階層に分け、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)

情報セキュリティポリシーの構成

文　書　名		内　　容	公表
情報セキュリティポリシー	情報セキュリティ方針	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	公開
	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すべ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	非公開
情報セキュリティ実施手順		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	非公開

第１章 情報セキュリティ基本方針

１　目的

本組合の各情報システムが取り扱う情報には、住民の個人情報のみならず行政運営上重要な情報など、外部への漏えい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ている。

したがって、情報資産及び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、住民の財産、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、このことが本組合に対する住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。本組合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、本組合の情報資産及び情報システムの機密性、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)を整備するために本組合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本組合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

本組合の内部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

ネットワーク、ハードウェア、ソフトウェア及び記録媒体で構成され、情報を処理する仕組みをいう。

（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すべ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すべての情報をいう。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

情報資産及び情報システム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。

3　情報セキュリティポリシーの位置付けと職員等及び外部委託事業者の義務

情報セキュリティポリシーは、本組合が所掌する情報資産及び情報システム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、管理者をはじめとして本組合が所掌する情報資産に関する業務に携わるすべての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持つとともに業務の遂行にあたって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。

4　情報セキュリティ管理体制

本組合の情報資産及び情報システムについて、幹部が率先して情報セキュリティ対策を推進し管理するための体制を確立するものとする。

5　情報資産及び情報システムの分類

情報資産及び情報システム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。

6　情報資産及び情報システムへの脅威

情報セキュリティポリシーを策定する上で、情報資産及び情報システム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。

（1）　部外者の侵入による機器又は情報資産の破壊若しくは盗難、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）　職員等又は外部委託事業者による機器又は情報資産の持出若しくは誤操作、アクセスのための認証情報又はパスワードの不適切管理、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、搬送中の事故等による機器又は情報資産の盗難、規定外のパソコン接続によるデータ漏えい等

（3）　コンピュータウイルス、地震、落雷、火災等の災害並びに事故、故障等によるサービス及び業務の停止

7　情報セキュリティ対策

上記6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）　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、情報資産及び情報システムへの損傷、妨害等から保護するために物理的な対策を講ずる。

（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、すべての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

情報資産及び情報システム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、情報資産及び情報システムへのアクセス制御、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場合には、迅速な対応を可能とするための対策を講ずる。

8　情報セキュリティ対策基準の策定

本組合の様々な情報資産及び情報システムについて、上記7の情報セキュリティ対策を講ずるにあたっては、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。

9　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、個々の情報資産及び情報システム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、情報資産及び情報システムに対する脅威並びに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、情報セキュリティ実施手順を策定するものとする。

情報セキュリティポリシーのうち情報セキュリティ対策基準及び情報セキュリティ実施手順は、公にすることにより本組合の行政運営に重大な支障を及ぼすおそれのある情報資産であることから非公開とする。

10　評価及び見直しの実施

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。