宮崎県東児湯消防組合情報セキュリティポリシー

Ⅰ　総則

【目的】

第１　宮崎県東児湯消防組合情報セキュリティポリシー（以下「ポリシー」という。）は、宮崎県東児湯消防組合（以下「消防組合」という。）の所有する情報資産を利用、運用、開発及び保守する者が情報セキュリティの確保に関する包括的な対策を図ることにより、消防組合の情報資産を適切に保護することを目的とする。

【定義】

第２　このポリシーにおいて、次の各号に掲げる用語の定義は、当該各号に定めるところとする。

（1）　情報セキュリティ　情報の機密性、完全性及び可用性の維持

機密性　情報にアクセスすることを許可された者だけがアクセスできることを保存すること。

完全性　情報資産が正確及び完全であることを常に維持すること。

可用性　許可された者が必要なときに確実に情報資産を利用できること。

（2）　ネットワーク　情報機器、通信機器及び通信回線（以下「情報機器等」という。）で構成されるデータ通信を行うための情報通信網

（3）　情報システム　汎用コンピュータ又はサーバを使用して定型的な業務処理を行うためのハードウェア及びソフトウェアの総称

（4）　情報資産　ネットワーク及び情報システム（以下「ネットワーク等」という。）の開発と運用に係る全てのデータ並びにそれらで取り扱う全てのデータをいう。

【適用範囲】

第３　本ポリシーの適用範囲は、以下のとおりとする。

（1）　消防組合の所有するすべての情報資産とする。

（2）　消防組合の情報資産を利用する業務に携わる職員（非常勤職員及び臨時雇用職員を含む。以下同じ。）

（3）　委託業者等（消防組合との契約により、消防組合の情報を取り扱う業務又は消防組合のネットワーク若しくは情報システムに係る開発、導入、保守等の業務に携わる者をいう。以下同じ。）

Ⅱ　情報セキュリティ基本方針

【情報資産への脅威】

第４　情報資産への脅威は、発生度合や発生した場合の影響を考慮し、次の各号のとおりとする。

（1）　機器又は情報資産の持出、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、規定外の端末接続によるデータ漏洩等

（2）　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

【情報セキュリティ対策】

第５　前条各号の脅威から情報資産を保護するために、次の各号の情報セキュリティ対策を講ずるものとする。

（1）　人的セキュリティ対策　情報セキュリティに関する管理体制の整備、職員に対する情報セキュリティ研修の実施等の対策

（2）　物理的セキュリティ対策　情報機器等の損傷、盗難、火災、停電等から情報を保護するための施設整備、入退室管理等の対策

（3）　技術的セキュリティ対策　ネットワーク等に係るアクセス制御、不正アクセス対策、ウイルス対策、ネットワーク等の端末又は記録媒体の管理等の対策

（4）　運用面におけるセキュリティ対策　情報セキュリティに関する情報の収集及び提供障害時の対応、実施手順の策定等の対策

【情報セキュリティ対策基準の策定】

第６　消防組合の所掌する情報資産について、前条の情報セキュリティ対策を講ずるに当たっては、情報セキュリティ対策基準（以下「対策基準」という。）を策定するものとする。

なお、情報セキュリティ対策基準は、公にすることにより情報セキュリティの確保に支障を及ぼす恐れがあることから非公開とする。

【職員の責務】

第７　職員は、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、情報資産の利用にあたってはポリシー及び実施手順（以下「ポリシー等」という。）を遵守するものとする。

【遵守状況の点検】

第８　ポリシー等の適正かつ円滑な運用に資するため、遵守状況を随時点検するものとする。

【ポリシー等の見直し】

第９　社会状況の変化等に迅速かつ的確に対応して情報セキュリティの確保を図るため、必要に応じて、ポリシー等の見直しを実施するものとする。