北上地区消防組合情報管理運用規則（平成26年北上地区消防組合規則第８号）

第１章　総則

（職員の責務）

第４条　職員は、北上地区消防組合（以下「組合」という。）の保有する情報を取り扱うときは、条例、規則、法令等を遵守しなければならない。

２　職員は、地方公務員法（昭和25年法律第２６１号）第34条の規定により、組合の保有する情報を正当な理由なく漏らしてはならない。

３　職員は、その職務目的以外で組合が保有する情報を閲覧又は利用してはならない。

４　職員は、行政文書を職務遂行上必要な場合を除き、外部に持ち出し、送信等してはならない。

第５章　情報セキュリティ対策の基本方針

（情報セキュリティ対策の対象）

第23条　組合が実施する情報セキュリティ対策は、情報資産に対する次に掲げる脅威を対象とする。

(1)　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及び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、重要情報の搾取、内部不正等

(2)　情報資産の無断持ち出し、無許可ソフトウェアの使用、設計及び開発の不備、プログラム上の欠陥、操作及び設定の誤り、メンテナンスの不備、内部及び外部監査機能の不備、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

(3)　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

(4)　大規模又は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

(5)　電力供給の途絶、通信の途絶等のインフラ障害から波及する脅威等

（情報セキュリティ対策）

第24条　実施機関の長は、前条に規定する脅威から情報資産を保護するため、次に掲げる情報セキュリティ対策を講じる。

(1)　情報セキュリティ対策の推進（情報の管理及び運用を含む。）のための組織の設置

(2)　情報資産の機密性、完全性及び可用性に応じた分類に基づく情報セキュリティ

対策

(3)　業務の効率性及び利便性を踏まえた情報セキュリティの強化を目的とした情報システム全体の強靭性の向上のための対策

(4)　サーバ、通信回線及びパソコン等のハードウェアに対する物理的対策

(5)　情報セキュリティポリシーの策定及び職員に対する教育、啓発等の人的対策

(6)　コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策

(7)　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、業務委託を行う際のセキュリティ確保等に関する対策及び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対応するための緊急時対応計画の策定

(8)　業務委託を行う場合の委託事業者におけるセキュリティ対策の確保の確認及び契約に基づく必要な措置、外部サービスを利用する場合における利用規定の整備並びにソーシャルメディアサービスを利用する場合における運用手順の策定、発信できる情報の規定及び責任者の指名

(9)　定期的又は必要に応じた情報セキュリティ監査及び自己点検の実施並びに当該実施に基づく情報セキュリティ向上のための対策

（情報セキュリティ監査及び自己点検の実施等）

第25条　最高情報統括責任者は、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。この場合において、情報セキュリティに関する状況の変化に対応するため新たな対策が必要となったときは、情報セキュリティポリシーを見直すものとする。

（情報セキュリティ対策基準等の策定）

第26条　実施機関は、情報セキュリティ対策を実施するための具体的な遵守基準及び判断基準を定める情報セキュリティ対策基準を策定し、併せて情報セキュリティ対策に必要な措置の実施手順（以下「情報セキュリティ実施手順」という。）を策定する。

２　情報セキュリティ実施手順は、非公開とする。