由利本荘市情報セキュリティ対策要綱

（目的）

第１条　この訓令は、本市が実施する情報セキュリティ対策について基本的な事項を定めることにより、もって本市が保有又は利用する情報資産の機密性、完全性及び可用性を維持することを目的とする。

（定義）

第２条　用語の定義を以下のとおり定める。

（１）　ネットワーク　電子機器を相互に接続するための通信網及びその構成機器（ハードウェアのみならずソフトウェアを含む。）をいう。

（２）　電子機器　クライアント（「端末」ともいう。）、サーバ、デバイス（機器、装置等をいう。）、ファシリティ（什器、設備等をいう。）等をいう。

（３）　記録媒体　紙、磁気テープ、磁気ディスク、光ディスク、光磁気ディスク、フラッシュメモリ等の情報を記録するための媒体をいう。

（４）　情報システム　ネットワーク、電子機器及び記録媒体の全部又は一部で構成され、情報処理を行う仕組みをいう。

（５）　情報セキュリティ　情報資産の機密性、完全性及び可用性を維持することをいう。

（６）　情報セキュリティポリシー　本要綱及び由利本荘市情報セキュリティ対策基準をいう。

（７）　機密性　情報にアクセスすることを正当に認められた者だけが、情報にアクセスできる状態を確保することをいう。

（８）　完全性　情報が破壊、改ざん又は消去されていない状態を確保することをいう。

（９）　可用性　情報にアクセスすることが正当に認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

（１０）　情報インシデント　情報資産の機密性、完全性及び可用性の全部又は一部が損なわれる事態をいう。

（１１）　情報資産　本要綱が対象とする情報資産は、以下のとおりとする。

ア　本市が保有又は利用するネットワーク、電子機器、記録媒体及び情報システム

イ　本市が保有又は利用するネットワーク、電子機器、記録媒体及び情報システムに関する仕様書等

ウ　本市が保有又は利用するネットワーク、電子機器、記録媒体及び情報システムで取り扱う情報

（対象とする脅威）

第３条　情報インシデントの原因となる脅威として、特に配慮すべき事案は、以下のとお

りとする。

（１）　不正侵入、盗難、不正アクセス行為、サイバー攻撃、内部不正等による情報資産の漏えい、破壊、改ざん、消去、詐取等

（２）　情報資産の無断持出、無許可ソフトウェアの使用等の規定違反による情報資産の漏えい、破壊、消去等

（３）　設計、開発、プログラム、設定、操作、メンテナンス、マネジメント等の不備による情報資産の漏えい、破壊、消去等、また、サービス及び業務の停止、遅延等

（４）　火災、風水害、落雷、地震、噴火、津波その他の災害による業務の停止等

（５）　疾病、事故等による人的被害等に伴う情報システムの運用における機能不全等

（６）　電力供給の途絶、通信の途絶、水道供給の途絶等の重要インフラの障害からの波及による情報システムの障害、業務の停止等

（適用対象となる機関）

第４条　本要綱が適用される本市の機関は、市長、教育委員会、選挙管理委員会、監査委員、農業委員会、ガス水道局企業管理者、消防長、固定資産評価審査委員会とする。

（職員等の遵守義務）

第５条　職員、嘱託職員及び臨時職員（以下「職員等」という。）は、情報セキュリティの重要性について共通の認識を持ち、各々の業務の遂行にあたって情報セキュリティポリシー及びその業務に係る情報セキュリティ実施手順を遵守しなければならない。

（情報セキュリティ対策）

第６条　第３条の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じる。

（１）　物理的セキュリティ対策　情報資産の管理について、固定、施錠、監視等の物理的な対策を講じる。

（２）　人的セキュリティ対策　全庁的な組織の確立、職員の教育及び訓練、情報セキュリティポリシーの運用徹底、情報インシデント発生時における対応計画の策定等、人的な対策を講じる。

（３）　技術的セキュリティ対策　電子機器管理制御、不正プログラム対策、不正アクセス対策等の技術的な対策を講じる。

（情報セキュリティ監査及び自己点検の実施）

第７条　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。

（情報セキュリティポリシーの見直し）

第８条　情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び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に対策が必要となった場合には、情報セキュリティポリシーの見直しを行う。

（情報セキュリティ対策基準の策定）

第９条　前３条に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

（情報セキュリティ対策実施手順の作成）

第１０条　情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ対策実施手順を各業務において作成、整備する。

（非公開原則）

第１１条　情報セキュリティ対策基準及び情報セキュリティ対策実施手順は、公にすることにより本市の行政運営に重大な支障を及ぼす恐れがあることから、原則として非公開とする。

（その他）

第１２条　この訓令に定めるもののほか、必要な事項は、市長が別に定める。