佐世保市情報セキュリティポリシー

（目的）

第１条　このポリシーは、市において作成し、又は収受した情報に対し、情報セキュリティを適切に維持するための基本方針並びに管理及び運用方針を定めることにより、情報の適正な管理及び円滑な運用を図ることを目的とする。

（定義）

第２条　このポリシーにおいて、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

⑴　実施機関　市長、教育委員会（小・中学校を除く。）、選挙管理委員会、農業委員会、公平委員会、監査委員、市議会及び固定資産評価審査委員会並びに消防長及び公営企業管理者をいう。

⑵　情報　佐世保市情報公開条例（平成１３年条例第４号）第２条第２項及び佐世保市議会情報公開条例（平成１３年条例第３５号）第２条第１項に規定する情報をいう。

⑶　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。

⑷　機密性　情報の利用及び閲覧（以下「利用等」という。）を行うことを許可された者だけが利用等をできることをいう。

⑸　完全性　情報の処理方法が正確かつ安全であることをいう。

⑹　可用性　許可された者が必要なときに情報の利用等をできることをいう。

⑺　サーバ　ネットワークを利用することで、端末機等へ業務システムが保有する機能やデータを提供するコンピュータをいう。

⑻　端末機　コンピュータとデータの収受を行うパーソナル・コンピュータをいう。

⑼　文書情報　情報のうち紙媒体で作られるものをいう。

⑽　電子情報　情報のうち電子的方式で作られるものであって、サーバ及び端末機等による情報処理の用に供されるものをいう。

⑾　ネットワーク　サーバ及びコンピュータ等間でのデータ収受を行う基盤をいう。

⑿　情報システム　サーバ、ネットワーク及びコンピュータ等を利用し業務を処理するための仕組みをいう。

⒀　情報資産　次に掲げるものをいう。

ア　ネットワーク、情報システム並びにこれらに関する設備及び電磁的記録媒体

イ　ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

ウ　情報システムの仕様書及びネットワーク図等のシステム関連文書

エ　実施機関の職員が作成し、又は取得した文書情報であって当該実施機関が組織的に用いるものとして保有しているもの

⒁　情報系端末　佐世保市行政情報ネットワークに接続するため、情報政策課により配付される端末機をいう。

⒂　各課端末　各課かいが所管し、庁舎内で使用する目的で導入される端末機をいう。

⒃　モバイル端末　各課かいが所管し、庁舎外に持ち出して使用する目的で導入される端

末機をいう。

⑰　端末機等　情報系端末、各課端末及びモバイル端末の総称をいう。

（情報資産に対するリスク）

第３条　情報資産に対するリスクを最小限に留めるために、次に掲げる事項から情報資産を守らなければならない。

⑴　権限のない者による情報資産の破壊、盗難若しくは不正アクセス又は不正操作による情報資産の破壊、改ざん、消去等

⑵　権限のある者による情報資産の無断持出、誤操作、認証情報の不適切な管理若しくは不正行為又は事故による情報資産の破壊、改ざん、消去、漏えい等

⑶　コンピュータウイルス、地震、落雷、火災、停電若しくはそ害等の災害又は事故による業務の停止

（適用範囲）

第４条　このポリシーは、実施機関のすべての職員（特別職を含む。以下「職員等」という。）及び実施機関が保有する情報に適用する。

（職員等の責務）

第５条　職員等は、情報の取扱いに関して、不正アクセス行為の禁止等に関する法律（平成１１年法律第１２８号）、著作権法（昭和４５年法律第４８号）、佐世保市個人情報保護条例、佐世保市特定個人情報の保護等に関する条例等の関係法令（平成２７年条例第３５号）等を遵守しなければならない。

２　職員等は、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、情報の適正な管理に努めなければならない。

３　職員等は、情報の秘密を保持するとともに、情報を業務目的以外で収集し、又は使用してはならない。

４　職員等による不正行為が明らかになった場合は、当該職員等を地方公務員法等の関係法令又は本市例規に基づいて処分する場合がある。

（組織）

第６条　市において作成し、又は収受する情報資産について、情報セキュリティの適正な管理及び円滑な運用を推進するための組織を設置する。

（情報資産の分類と管理）

第７条　実施機関は、保有する情報資産について、機密性、完全性及び可用性に応じて分類し、その重要度に応じた情報セキュリティ対策を行わなければならない。

（情報セキュリティ対策）

第８条　実施機関は、第３条各号に規定する脅威から情報資産を保護するために、次の各号に掲げる情報セキュリティ対策を講ずるものとする。

⑴　物理的セキュリティ対策　情報システムを設置する施設、通信回線及び職員等の端末機等の管理について、物理的な対策を講ずる。

⑵　人的セキュリティ対策　情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、情報資産を利用する全ての者に情報セキュリティポリシーの内容を周知徹底

するための教育及び啓発を行う等の人的な対策を講じる。

⑶　技術的セキュリティ対策　端末機等の管理、アクセス制御、不正プログラム対策、不正アクセス対策、通信環境の分割等の技術的対策を講じる。

⑷　運用面のセキュリティ対策　情報セキュリティポリシーの実行性を確保するため、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、外部委託を行う際のセキュリティ確保等の運用面の対策を講じる。

（情報セキュリティ監査及び自己点検の実施）

第９条　ポリシーの遵守状況を検証するため、定期的に情報セキュリティ監査及び自己点検を実施する。

（ポリシーの見直し）

第１０条　情報セキュリティ監査及び自己点検の結果、ポリシーの見直しが必要となった場合又は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になった場合には、ポリシーを見直すものとする。

（教育）

第１１条　情報の取扱いに関する教育・研修の実施を計画し、その結果を情報セキュリティ委員会に報告する。

（委任）

第１２条　このポリシーの目的を達成するために必要な具体的な遵守事項及び判断基準等は、別に定める。

附　則

このポリシーは、平成１６年　６月　１日から施行する。

附　則

このポリシーは、平成１６年１０月　１日から施行する。

附　則

このポリシーは、平成１７年　４月　１日から施行する。

附　則

このポリシーは、平成１８年　８月２４日から施行する。

附　則

このポリシーは、平成１９年　４月　１日から施行する。

附　則

このポリシーは、平成２０年　７月　１日から施行する。

附　則

このポリシーは、平成２１年　６月　１日から施行する。

附　則

このポリシーは、平成２８年　１月　１日から施行する。

附　則

このポリシーは、平成３１年　４月　１日から施行する。