

南アルプス市情報セキュリティ対策基準

(趣旨)

第1条 この訓令は、南アルプス市情報セキュリティ規則（平成16年南アルプス市規則第28号。以下「規則」という。）に基づき、本市の全ての情報資産、情報資産を活用するための設備及びこれら情報資産に接する職員又は受託事業者が行う情報セキュリティ対策に関し必要な事項を定めるものとする。

(定義)

第2条 この訓令において、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もののほか、規則の例による。

- (1) サーバー サービスを提供するソフトウェア及びハードウェア
- (2) ユーザー 情報機器及び情報システムの利用者
- (3) コンピュータウイルス 情報システムに悪影響を及ぼす恐れのあるソフトウェア
- (4) 不正アクセス 権限を持たない者が情報資産を閲覧、利用すること
- (5) アクセスコントロール 情報及び情報システムに対して、利用できる者を制限する機能
- (6) アカウント サービスを利用する際に、利用者を特定するための符号
- (7) バックアップ コンピュータに保存されたデータやプログラムを、破損やコンピュータウイルス感染などの事態に備え、別の記憶媒体に保存すること

(最高情報統括責任者)

第3条 市の保有する全ての情報資産及び情報セキュリティを統括し、その権限及び責任を有する最高情報統括責任者を置く。

2 最高情報統括責任者は、助役をもって充てる。

3 最高情報統括責任者に事故があるとき、又は最高情報統括責任者が欠けたときは、総務部長をもって充てる。

(情報統括責任者)

第4条 最高情報統括責任者を補佐するため、情報統括責任者を置く。

2 情報統括責任者は、部長、支所長、議会事務局長、消防長、企業局長及び教育次長をもって充てる。

3 情報統括責任者は、情報セキュリティポリシー及び実施手順の

適正な運用を確保するため情報セキュリティーに関する指導及び助言を行うことができるとともに、情報セキュリティー対策の実施状況を点検し、その結果を情報セキュリティー委員会へ報告しなければならない。

(情報管理責任者)

第5条 所管する組織の情報資産及び情報セキュリティーに関する権限並びに責任を有する情報管理責任者を置く。

- 2 情報管理責任者は、各課等の長及び市のネットワークを使用している施設の長をもって充てる。
- 3 情報管理責任者は、保有する情報資産について重要度に応じた分類を行い、情報資産一覧表を作成し適切に管理しなければならない。
- 4 情報管理責任者は、電子情報の特性を考慮し情報資産の取扱いには十分な注意を払うとともに、外部に情報資産を持ち出す場合には、必要な処置を講じなければならない。

(情報システム管理者)

第6条 所管する情報システムにおける権限及び責任を有する情報システム管理者を置く。

- 2 情報システム管理者は、情報システムを保有する各課等の長とする。

(ネットワーク管理者)

第7条 市の保有するネットワークにおける権限及び責任を有するネットワーク管理者を置く。

- 2 ネットワーク管理者は、電子計算機器管理業務を所管する課の長をもって充てる。

(人的セキュリティー対策)

第8条 市の保有する情報資産を保護するための人的なセキュリティー対策は、次の各号に掲げるとおりとする。

(1) 教育及び訓練

ア 職員は、情報セキュリティーポリシーに関する研修を受講し、情報セキュリティーポリシー及び実施手順を理解し、情報セキュリティー上の問題が生じないようにしなければならない。

(2) 作業報告等

ア 職員及び受託事業者が情報システムを利用する際は、どのような軽微な作業であっても作業報告を行うこと。

(3) 事故及び欠陥の対処

ア 職員は、障害発生等情報セキュリティー上の問題を発見した場合は、情報管理責任者、情報システム管理者又はネットワーク管理者に速やかに通報し、その指示に従い必要な対策を講じること。

イ 情報管理責任者、情報システム管理者又はネットワーク管理者は、事故等に対し迅速かつ的確に対処すること。

(物理的セキュリティー対策)

第9条 市の保有する情報資産を保護するための物理的なセキュリティー対策は、次の各号に掲げるとおりとする。

(1) ハードウェア等の設置環境

ア 情報システム管理者は、情報システムを設置する場合は設置場所の環境条件に十分留意すること。

イ 情報システム管理者は、停電又は電圧異常等により業務に支障が生じないように適切な電源管理を行うこと。

ウ 情報システム管理者及びネットワーク管理者は、サーバー又はネットワーク機器を設置するに当たり施錠及び防災措置が施されている施設に設置すること。

(2) サーバー室への入退室管理

ア 情報システム管理者及びネットワーク管理者は、サーバー設置場所への入退室について情報セキュリティー対策上必要な管理対策を講じること。

(3) 情報システムの廃棄

ア 情報システム管理者は、情報システムの廃棄又は賃借した情報システムを返却する場合には、第三者に情報が漏洩しないよう適切な方法により記録媒体内全ての行政情報を消去すること。

(技術的及び運用におけるセキュリティー対策)

第10条 市の保有する情報資産を保護するための技術的なセキュリティー対策及び適切な運用管理は、次の各号に掲げるとおりとする。

(1) コンピュータ利用

ア 職員は、コンピュータを原則として指定された場所でのみ使用すること。

イ 職員は、コンピュータを業務以外の目的で使用しないこと。

(2) コンピュータウイルス対策

ア 情報システム管理者及びネットワーク管理者は、必要な情報

システムに対しコンピュータウイルス対策のソフトウェアを導入し、適切に管理運営すること。

イ 職員は、コンピュータウイルスに感染しないよう十分な注意を払うこと。

ウ 職員、情報システム管理者及びネットワーク管理者は、情報システムがコンピュータウイルスに感染した可能性がある場合には、適切な措置を講じること。

(3) 不正アクセス対策

ア 情報管理責任者、情報システム管理者及びネットワーク管理者は、情報システムへの不正な侵入や利用が行われぬよう適切な対策を講じること。

(4) バックアップ

ア 情報管理責任者は、情報資産の破損や消去等に備え、他の記録媒体へのバックアップを定期的に行うこと。

イ 情報管理責任者は、情報資産を記録した媒体を適切に管理すること。

(5) ネットワークの管理

ア ネットワーク管理者は、既存のネットワークの安全性が脅かされることの無いよう、適切なセキュリティー対策に努めること。

(6) 記録媒体の管理及び破棄

ア 情報管理責任者は、情報を記録した媒体を外部からの脅威にさらされないよう安全な場所に保管すること。

イ 情報管理責任者は、記録媒体を廃棄する場合記録されている情報をいかなる方法によっても復元できないように消去等を行った上で廃棄すること。

(7) アクセスコントロール、アカウント作成及び抹消

ア 情報管理責任者及びネットワーク管理者は、権限を有しない者が不必要なサービスにアクセスできないよう、適切な措置を講じること。

イ 情報管理責任者及びネットワーク管理者は、所管する利用者のアカウントを適切に管理運営すること。

(8) 導入計画

ア 情報システム管理者は、情報システムを導入する場合情報セキュリティー対策を考慮した最適な計画を策定し導入するこ

と。

(9) パスワードの管理

ア 職員は、パスワードを厳重に管理し、秘密保持に努めること。

(1 0) サーバー管理

ア 情報システム管理者は、他の情報システムに悪影響を与えないようサーバーを適切に管理運営すること。

(1 1) 電子メール管理

ア 職員は、電子メールを使用する際には電子メールの特性を考慮した上で細心の注意を払い使用すること。

(1 2) 受託事業者管理

ア 外部に情報システム開発や保守等の業務を委託する場合は、情報漏洩等の脅威に備え十分な情報セキュリティ対策を講じるとともに、情報管理責任者は適切に受託事業者を管理、監督すること。

イ 情報管理責任者は、受託事業者と締結する委託契約書等に情報セキュリティに関する条項を記載すること。

ウ 情報セキュリティに関する条項については、南アルプス市電子計算組織運営管理規則（平成 1 5 年南アルプス市規則第 1 7 号）第 3 2 項第 1 項の規定によるものとする。

(法令等の遵守)

第 1 1 条 職員又は受託事業者は、職務若しくは業務の遂行において規則及び対策基準に定めるもののほか、関係法令等を遵守しなければならない。

(違反への対応)

第 1 2 条 情報セキュリティ対策違反への対応については別に定める。

(その他)

第 1 3 条 この訓令に定めるもののほか、必要な事項は、別に定める。

附 則

この訓令は、公布の日から施行する。