

別紙5 セキュリティの仕様

1. 目的

本書は、受託者の情報資産の管理方法、遵守すべき事項及び判断基準等について定めることを目的とする。

2. 情報資産

情報資産とは、受託者が本業務を行うにあたって、本県から提示した情報（紙媒体、磁気媒体、ハードウェアに記録されているデータ等）及び本県から提示した情報をもとに受託者が加工した情報のうち個人情報、内部機密情報及び本県が重要と判断したものをいう。

3. セキュリティ要件

受託者は本業務において、情報資産を、故意（盗聴、不正アクセス、改ざん、破壊等）、過失（入力ミス、操作ミス等）、災害（火災、地震等）、盗難、故障等の脅威から守るため、以下のセキュリティ要件を遵守することとする。

なお、本セキュリティ要件に記載のない事項で、本県が必要と認めた事項については、受託者と協議のうえ決定することとする。

（1）人的セキュリティ要件

- ア. 受託者は、予め、相応の知識、技術及び経験を有する者を選抜し、情報セキュリティに関する責任者（以下「責任者」という。）を決定し、本県に報告すること。また、「別紙2 機器等更新作業の仕様」及び「別紙3 システム移行作業の仕様」記載の作業に従事するSE（下請けとして受託する事業者も含む。）（以下「従事者」という。）について、その氏名、所属、連絡先を明記した一覧表を作成し、本県に提示すること。責任者及び従事者の変更が発生する場合には、その都度、報告するとともに、従事者一覧については最新のものを再度提出することとする。
- イ. 責任者は、従事者に対して、情報セキュリティを確保するうえで必要な指導、教育を行い、適切に従事者を管理すること。
- ウ. 従事者は、個人情報保護など最新の情報セキュリティに関する知識及び技術を得るよう努力すること。
- エ. 責任者及び従事者は作業にあたり、問題が発生していないかについて常に確認を行い、機器の異常、情報資産の紛失・流出、不正アクセス及びコンピュータウイルス等の問題が発生した場合には速やかに本県に報告するとともに、問題が拡大するのを防ぐための対策を講じること。
- オ. 責任者及び従事者は、常に身分を証明できるものを携帯及び掲示し、求めがあった場合にはこれを提示、明示すること。
- カ. 責任者及び従事者は、本業務の従事中、異動及び退職等により業務を離れた場合でも、知り得た情報を秘匿すること。
- キ. 不特定の来訪者、業者等に重要な情報資産を見られないようにする

こと。

- ク．作業を行ううえで受託者が準備、使用する端末等の機器は、全て受託者が所有する機器とし、個人が所有する機器は使用してはならない。また、当該機器については、情報漏洩等のセキュリティ上問題のあると考えられるソフト（Winny、Share 等のファイル共有ソフト等）がインストールされていないことを予め確認するとともに、作業中においてもインストールしてはならない。

（２）物理的セキュリティ要件

- ア．情報資産及び情報資産をもとに加工した情報は、適切に保管すること。
- イ．本県の許可を得ず、情報資産を執務室外に持ち出してはならない。外部の場所に持ち出す情報資産については、運搬方法、利用場所及び利用方法・用途を明確にし、管理簿を設け適切に管理し、使用後は必ず返戻し本県の確認を得ること。外部に持ち出した情報資産について、持ち出し後、さらに移転を行う場合には速やかに報告を行い、承認を得ること。
- ウ．情報資産が記録されている端末等の機器は、盗難防止対策のため、適切な措置を施すこと。
- エ．重要な情報資産は、本県の許可なく複写、複製してはならない。
- オ．情報資産が不要となった場合は、記録媒体の初期化など情報を復元できないように消去を行ったうえで廃棄しなければならない。重要な情報資産の廃棄は、本県の許可を得ることとし、行った処理について、日時、担当者及び処理内容を記録すること。

（３）技術的セキュリティ要件

- ア．端末等の機器からアクセス権限のない者に情報資産を使用されること、また許可なく電子データを閲覧されることがないように、ＩＤやパスワード等による適切な措置を施すこと。

（４）運用におけるセキュリティ要件

- ア．受託者は、本県によるセキュリティ要件の遵守についての書面及び実地によるセキュリティ監査に全面的に協力すること。