平成 29 年 1 月 1 日

# 開発技術コンサルタント　情報セキュリティポリシー

本業務の履行に関するすべての行政情報について、以下に示す情報管理体制で行政情報の流出防止を行う。

（1）情報管理体制

情報管理は、情報管理責任者（技術本部長）が統括し、各部署に対して管理・点検・指導を行う。また、取り扱う情報に対して業務毎にアクセス権限者を指定する。

（2）不正侵入、不正利用等の防止

・スパイウェアを含むウイルスの侵入・ハッキングなど、ネットワークからの侵入を防止し、部外者による情報流出等を防止する。

・情報機器管理、ソフトウェア管理、使用者の制限、パスワード設定などを実施し、アクセス権限者以外のアクセスを禁止する。

・保管場所となる執務室については外部訪問者の入室を禁止するとともに、退社時等における施錠を徹底する。設備点検などのため、やむを得ず入室の必要がある場合は、社員が立ち会うか、事前に守秘義務の取り決めを交わす。この場合も施錠、パスワードによるアクセス防止を確実に行う。

・パソコンの利用状況はログ管理を行い、不正利用を防止する。

（3）情報伝達・廃棄時の情報流出の防止

・ファイル交換ソフト等、ファイル流出の危険性が高いソフトウエアの使用を禁止する。

・コンピュータ機器類の情報機器や紙媒体・ＣＤ・ＤＶＤ等の記録媒体は、破砕等を行い、復元判読が不可能な状態としたのちに廃棄する。

（4）教育訓練

情報セキュリティの認識向上、情報機器の取り扱い、事故発生時の対応等について教育を行う。

（5）事故発生時の対処方法

事故が発生した場合は、速やかに原因を把握し、対策を講じて再発防止を図る。 業務において情報漏洩事故が発生した場合は、情報管理責任者は速やかに顧客に届け出る。

(附則)

この情報セキュリティポリシーは、平成 29年 1 月 1 日より施行します。