情報システム部データ入力業務指名競争入札参加者選考等取扱要領

（平成１８年 １月２６日情報化推進部長決裁）
最近改正　平成３０年８月２９日

（目　的）

第１条　この要領は、情報システム部において行うデータ入力業務に係る指名競争入札において、被指名者等選考委員会が被指名者を選考する際の基準及びその基準に用いる「データ入力業務セキュリティ管理基準適合業者」の認定における事務取扱について必要な事項を定めることを目的とする。

（データ入力業者の選考）

第２条　データ入力業務に係る指名競争入札に参加する業者は、「札幌市競争入札参加資格者名簿」の業種分類「大分類：役務（一般サービス業）」の「中分類：情報サービス、研究・調査企画サービス業」に登録されている者であって、かつ、第３条で定める「データ入力業務セキュリティ管理基準適合業者」の認定を受けた者の中から選考するものとする。

（適合事業者の認定）

第３条　データ入力業務における個人情報保護の重要性から、指名競争入札に参加する業者のセキュリティ水準の確認のために、情報システム部において「データ入力業務に係るセキュリティ管理基準」（別紙１）を定め、その基準に適合する業者を「データ入力業務セキュリティ管理基準適合業者」として認定を行うものとする。

２　データ入力業務セキュリティ管理基準適合業者の認定については、システム管理課が以下の方法により行うものとする。

(1) 認定を希望する業者は、データ入力業務セキュリティ管理基準適合認定申請書（様式１）に、データ入力業務におけるセキュリティ管理基準適合申出書（様式２）を添付し、申請を行う。

(2) 申請があった業者に対し、データ入力業務に係るセキュリティ管理基準（別紙１）への適合状況について、申出書の記載内容の確認と併せて実態調査を行う。

(3) 実態調査の結果に基づき審査を行い、セキュリティ管理基準適合業者としての認定の可否を申請者宛に通知する。

３　セキュリティ管理基準適合業者の認定は随時行うものとする。

４　データ入力業務セキュリティ管理基準適合業者の認定期間は、適合認定の通知を受けた翌年度の４月１日から３月３１日までとする。ただし、認定を希望する業者から、当該年度のデータ入力業務セキュリティ管理基準適合業者の認定を受けたいとの申し出があった場合は、セキュリティ適合認定の通知を受けた年度の３月３１日までを認定期間とする。

（認定の取消し）

第４条　前条において認定を受けた者が次の各号に該当した場合は、認定の取消しを行うことができるものとする。

(1) 情報システム部がセキュリティ保持のために行う指導に従わない場合

(2) データ入力業務の委託契約書又は付随する覚書に違反した場合

(3) 申請時に提出した書類に故意に虚偽の事実を記載したことが判明した場合

(4) その他不適当な行為があった場合

附　則

この要領は、平成１８年　１月２６日から施行する。

附　則

この要領は、平成２６年１０月　７日から施行する。

附　則

この要領は、平成２８年　４月　１日から施行する。

附　則

この要領は、平成２８年　９月１２日から施行する。

附　則

この要領は、平成２９年　９月１３日から施行する。

附　測

この要領は、平成３０年　８月２９日から施行する。

（別紙１）

データ入力業務に係るセキュリティ管理基準

1　情報セキュリティに関する基本方針、規程及び個人情報の取扱手順の策定

　個人情報の適正な取扱の確保について情報セキュリティの基本方針を策定していること。また、以下の内容を記載した個人情報の保護を含む情報セキュリティに関する規程及び個人情報の取扱手順等が定められていること。

⑴　組織的安全管理措置
⑵　人的安全管理措置
⑶　物理的安全管理措置
⑷　技術的安全管理措置

※各項目の具体的内容は、個人情報保護委員会ホームページ（https://www.ppc.go.jp）に掲載されている特定個人情報の適正な取扱いに関するガイドライン(行政機関等・地方公共団体等編)の（別添）特定個人情報に関する安全管理措置（行政機関等・地方公共団体等編）をご確認ください。

2　データ入力業務に関する総括責任者及びデータ保護責任者の設置

　データ入力業務に関する総括責任者及びデータ保護責任者が定められており、基本方針、規定及び個人情報の取扱手順等に明記されていること。

3　従業者の教育及び監督

⑴　個人情報等の秘密保持に関する事項を就業規則等に明記されていること。
⑵　個人情報の取扱、情報システムの運用・管理及びセキュリティ対策及びサイバーセキュリティの研修計画を策定し、従業者に対し毎年１回以上研修等を実施すること。
⑶　総括責任者及び保護責任者は、従業者に対して必要かつ適切な監督を行うこと。

4　管理区域の設定及び安全管理措置の実施

⑴　個人情報を取り扱う管理区域を明確にし、当該区域に壁又は間仕切り等を設置すること。

【管理区域の例】

・サーバ等の重要な情報システムを管理する区域
・データ入力を実施する区域
・個人情報を保管する区域
・その他個人情報を取り扱う事務を実施する区域

⑵　⑴で設定した管理区域について入室する権限を有する従業者を定めること。また、入室にあたっては、用件の確認、入退室の記録、部外者についての識別化及び部外者が入室する場合は、責任者の立会い等の措置を講ずること。また、入退室の記録を保管していること。
⑶　⑴で設定した管理区域について入室に係る認証機能を設定し、パスワード等の管理に関する定めの整備及びパスワード等の読取防止等を行うために必要な措置を講ずること。
⑷　外部からの不正な侵入に備え、施錠装置、警報装置及び監視装置の設置等の措置を講ずること。
⑸　管理区域では、許可された電子媒体又は機器等以外のものについて使用の制限等の必要な措置を講ずること。

5　セキュリティ強化のための管理策

情報資産の盗難、紛失、持出し、複写・複製、目的外の使用及び第三者への提供を防止するため以下の対策を実施していること。

⑴　データ入力に使用する電子計算機等は、他のコンピュータと接続しない単独による設置もしくはデータ入力作業を実施するうえで必要な機器のみと接続していること。また、インターネット及びデータ入力作業を実施する施設外に接続するイントラネット等の他のネットワークに接続していないこと。

⑵　データ入力業務にてサーバを使用している場合は、データ入力作業を実施する施設内に設置していること。また、サーバへのアクセス権限を有する従業者を定めること。ならびに、部外者のアクセスは必要最小限とし、責任者の立会い等の措置を講ずること。

⑶　データ入力業務にて使用する電子計算機等は、アクセス権等を設定し、使用できる従業者を限定すること。また、アクセスログやログイン実績等から従業者の利用状況を記録し、保管していること。

⑷　記録機能を有する機器の電子計算機等への接続制限について必要な措置を講ずること。

⑸　本市が貸与する文書、電子媒体及び業務にて作成した電子データを取り扱う従業者を定めること。

⑹　業務にて作成した電子データを保存するときは、暗号化またはパスワードにより秘匿すること。ならびに保存した電子データにアクセスできる従業者を限定するとともにアクセスログ等から従業者の利用状況を記録し、契約期間終了後、1 年以上保管していること。

⑺　本市が貸与する文書及び電子媒体は、施錠できる耐火金庫及び耐火キャビネット等にて保管すること。また、書類の持ち出し記録等を作成していること。

⑻　データ入力にて使用する電子計算機は、従業者が正当なアクセス権を有する者であることをユーザ ID、パスワード、磁気・IC カード及び生体情報等のいずれかにより識別し、認証するしていること。

⑼　データ入力にて使用する電子計算機は、セキュリティ対策ソフトウェア等（ウィルス対策ソフトウェア等）を導入していること。

⑽　業務にて作成した電子データを削除した場合は、削除した記録を作成していること。また、削除したことについて証明書等により確認できる措置を講ずること。

⑾　データ入力業務にて使用する電子計算機等を廃棄する場合は、専用のデータ削除ソフトウェアの利用又は物理的な破壊等により、復元不可能な手段を採用すること。

⑿　本市の業務について第三者委託を実施しないこと。

6　検査入力の実施

一次入力者が入力したデータについて別の従業者による検査入力を実施するベリファイを実施していること。

7　事件・事故における報告連絡体制

⑴　従業者が取扱規定等に違反している事実又は兆候を把握した場合の責任者への報告連絡体制を整備していること。

⑵　情報の漏えい、滅失又は毀損等事案の発生又は兆候を把握した場合の従業者から責任者等への報告連絡体制を整備していること。

⑶　情報の漏えい、滅失又は毀損等事案が発生した際の本市及び関連団体への報告連絡体制を整備していること。併せて事実関係の調査、原因の究明及び再発防止策の検討並びに決定等に係る体制及び手順等を整備していること。

8　情報資産の搬送及び持ち運ぶ際の保護体制

本市が貸与する文書、電子媒体及び左記書類等に基づき作成される電子データを持ち運ぶ場合は、施錠した搬送容器を使用すること。また、暗号化、パスワードによる保護、追跡可能な移送手段等破損、紛失、盗難等のないよう十分に配慮していること。

9　関係法令の遵守

個人情報保護に関する関係法令を遵守するために、必要な体制を備えていること。

10　定期監査の実施

個人情報等の管理の状況について、定期に及び必要に応じ随時に点検、内部監査及び外部監査を実施すること。

11　情報セキュリティマネジメントシステム（以下、ISMS）又はプライバシーマーク等の規格認証

ISMS（国際標準規格　ISO/IEC27001:2013、日本工業規格 JISQ27001：2014）、プライバシーマーク（日本工業規格　JISQ15001:2006）等の規格認証を受けていること。