情報セキュリティ特記仕様書

１　実施計画書の提出

（１）乙は、本件業務を行うに先立って、実施体制、責任者、実施方法、作業場所、スケジュール等を記した実施計画書を作成し、甲に提出し、甲の承認を得なければならない。実施計画書を変更する場合も同様とする。

（２）甲は、乙から提出された実施計画書に対して必要な指示をすることができる。

２　従事者の監督

乙は、本件業務に関わる実施体制（連絡体制を含む。）及び要員の一覧表を甲に提出し、甲の承認を得なければならない。要員に変更があった場合も同様とする。

３　状況報告書の提出

（１）乙は、甲、乙双方の合意に基づき定めた期間、方法及び内容等で本件業務の作業状況等について、甲が認めた場合を除き書面により報告しなければならない。

（２）前項の規定にかかわらず、乙は、甲から本件業務の作業状況等について報告を求められたときは、甲が指示する方法及び内容等により、これを報告しなければならない。

（３）甲は、状況報告に対して必要な指示をすることができる。

４　本件業務を行うために甲から提供された情報（以下「情報」）が記録された資料（以下「資料」）等の管理

（１）乙は、資料等の一覧表を作成しなければならない。

（２）乙は、甲の承諾を得ずに、資料等の複製、提供、業務作業場所以外への持ち出し、送信その他個人情報を含めて適切な管理に支障を及ぼすおそれのある行為をしてはならない。やむをえず持ち出し等を行う必要がある場合は、書面で持出す目的、データの内容及び暗号化等の対策を記し、甲の承諾を得、管理簿に記載すること。

（３）乙は、資料等、作業中のデータ及び甲に帰属した成果物を、甲の承諾を得ずに、甲の指示する目的以外に使用及び第三者への提供をしてはならない。

（４）乙は、資料等に紛失、損傷、焼失等の事故が生じないよう安全かつ適切な管理体制を整備しなければならない。

（５）乙は、資料等及び作業中のデータ並びにそれらが保存された記録媒体について、その貸与目的を達したときまたは契約終了時に返却または復元不可能な方法で廃棄・消去しなければならない。複製物及び貸与された資料をもとに変更したものも同様とする。

（６）乙は、資料等を甲の承認を得て廃棄・消去した場合、確実に廃棄・消去した旨の証明を書面で甲に提出しなければならない。

（７）乙は、資料等及び作業中のデータの保護・管理に必要な手続きを作成し、資料等を閲覧できる者や方法の制限等を行わなければならない。

（8）乙は、提供された資料等の内容については、公知の事実となるまで契約終了後も他言してはならない。

5　本人確認

乙は、本件業務の履行に関わる要員が納入場所等に立ち入る場合名札を着用させるとともに、乙の要員であること、要員本人であることを証するものを携帯させなければならない。

6　安全確保上の問題への対応

（1）乙は、本件業務の遂行に支障が生じるおそれのある事故の発生を知り得たときは、直ちにその旨を甲に報告し、遅延なくその措置状況を書面により報告しなければならない。

（2）甲は、前項の規定により報告を受けたときは、乙に対し、被害の拡大の防止又は復旧のために必要な措置に関する指示を行い、乙は当該指示に従わなければならない。

（3）乙は、事案の内容、影響等に応じて、その事実関係及び再発防止策の公表等の措置を甲と協力して講じなければならない。

7　要員の教育

（1）乙は、本件業務にかかわる全要員に対して、本件業務を遂行するために必要な教育を行わなければならない。

（2）乙は、教育に関する計画及び実施実績について甲に報告しなければならない。

（3）乙が行う教育には、ドキュメントの取扱方法、個人識別情報の取扱方法、データの取扱方法、事故時の連絡体制、個人情報の取扱方法を含まなければならない。

（4）甲は、乙の提出した教育に関する計画及び実施実績について必要な指示をすることができる。

8　作業上の権限

（1）乙は、本件業務の実施において、情報へのアクセス制御を設け、要員に対し、必要なアクセス権のみを付与するものとする。

（2）乙は、甲の情報をシステムで操作する場合操作記録を作成すること。（ログを保存すること。）

（3）乙は、甲の要求があったとき、操作記録（ログ）を甲に提示しなければならない。

9　機器の管理

（1）乙は、本件業務の実施に使用するコンピュータ機器等を限定しなければならない。ただし、甲の承認を得た場合はこの限りではない。

（2）乙は、前号の機器等の盗難、破壊等の防止策を講じなければならない。

（3）乙は、甲から貸与された機器等についても同様の措置をとらなければならない。

10　機器及び納品物のウイルスチェック

（1）乙は、本件業務を履行するために使用するコンピュータ等の機器に対してウィルス対策ソフトを導入する等のコンピュータウィルス感染防止策を講じなければならない。

（2）乙は、甲の環境に機器またはデータを持込む場合は、書面で甲に承諾を得なければならない。

（3）乙は、甲に対して持込むまたは納品する電子データがコンピュータウィルスに感染していないことを甲の指定する方法で保障しなければならない。

（4）乙は、甲から貸与された機器に対しても（1）の措置を行うものとする。

11　管理規定

（1）乙は、本件業務の実施について以下の規定を定めなければならない。

ア　セキュリティ事故の場合の連絡体制

イ　甲から提供された資料等の保管方法と責任者

ウ　甲から提供された資料等にアクセスできる者の名簿、管理責任者

エ　甲から提供された資料等のアクセス記録の管理方法

オ　本件業務の実施において作成された資料等（データ、ドキュメント、出力帳票、入力帳票、プログラム、設定ファイル、ログ等）にアクセスできる者の名簿、管理責任者

カ　本件業務の実施において作成された資料等のアクセス記録の管理方法と管理責任者

キ　甲から提供された資料等及び本件業務の実施において作成された資料等の返却または破壊方法と返却・破壊管理者

ク　コンピュータ等の機器の管理方法と責任者

ケ　コンピュータウイルス対策

（2）乙は、甲からの請求があった場合、前号の規定により作成された資料等を速やかに提示しなければならない。

12　検査権

（1）甲は、乙が行う本件業務に関して、口頭、書面及び立入りにより検査を行うことができる。

（2）甲は、乙に対し、必要な指示を出すことができる。

（3）乙は、甲からの検査要求及び甲からの指示に対して誠実に協力しなければならない。

13　協力会社等に対する責任

（1）乙は、本件業務を実施するに際して自社以外の企業、個人（以下「協力会社等」という。）を利用する場合、協力会社等に対して本契約の定めを周知・指導しなければならない。

（2）協力会社等の行為は、乙の行為とみなす。

14　法令の遵守

乙は、業務の実施にあたり、関係法令、委託者（以下「甲」という。）が定めた諸規定及び次に掲げる関連指針等に準拠して遂行することを前提とし、関連指針等に改定があった場合は、当然に最新版への対応を義務付けるものである。

・「医療情報システムの安全管理に関するガイドライン 第5.2 版」（厚生労働省）
・「電気通信事業における個人情報保護に関するガイドライン」（総務省）
・「電子的診療情報交換推進事業（SS-MIX/SS-MIX2）」（厚生労働省）
・「医療機関で電子的に情報交換する際の標準的な規格（HL7 ver2.5）」（日本 IHE 協会）
・「相互運用性を確保した医療情報システム導入ガイド」（経済産業省）
・「保健医療情報分野の標準規格として認めるべき規格」（厚生労働省）
・「医療情報を受託管理する情報処理事業者向けガイドライン」（経済産業省）
・「ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン」（総務省）

15　その他

乙は、本件業務の実施について本契約書、仕様書及び甲から提出された資料等に明記されていない事態が発生した場合、速やかに甲に報告し、甲の指示を仰がなければならない。