

別記

情報セキュリティに関する特記事項

(目的)

第1条 乙は、本契約に係る業務（以下「本件業務」という。）の実施のために、甲から提供する情報その他本件業務の実施において知り得た情報（以下「保護すべき情報」という。）の機密性、完全性及び可用性を維持すること（以下「情報セキュリティ」という。）に関して、この特約条項に定めるところにより、その万全を期さなければならない。

2 保護すべき情報の範囲は次の各号とする。

- 一 甲が管理対象として指定した文書、図面、図書等（電磁的記録を含む。）
- 二 甲が管理対象として指定した物件
- 三 一号又は二号に掲げるものを基に、乙が作成（複製及び写真撮影を含む。）した文書、図面、図書等（電磁的記録を含む。）又は物件のうち、甲が指定したもの

(下請負の禁止)

第2条 乙は、本契約の全部又は一部を第三者に下請負させてはならない。ただし、やむを得ず下請負をさせるときは、その下請負先、契約内容等を記した書面を添え、甲の許可を得るものとする。

2 前項ただし書により乙が下請負をさせる場合、乙は乙と下請負者との間で締結する契約において、下請負者において本特約条項と同等の情報セキュリティの確保が行われるよう定めなければならない。

3 甲は、前項の契約について、情報セキュリティの確保が十分満たされていないと認められる場合、第1項の許可を与えないことができる。

4 第1項ただし書により乙が下請負させる場合の下請負者その他本契約の履行に係る作業に従事する乙以外の事業者（以下「下請負者等」という。）における情報セキュリティの確保について、乙は本特約条項に従い、必要な通知、申請、確認等を行うものとする。

(情報セキュリティ確保のための体制等の整備)

第3条 乙は、保護すべき情報に係る情報セキュリティを確保するために必要な体制を整備しなければならない。

2 乙は、乙の代表者又は代表者から代理権限を与えられた者を情報セキュリティに係る責任者（以下「情報セキュリティ責任者」という。）とし、情報セキュリティ責任者の下に、保護すべき情報の管理に係る管理責任者を指定し甲に通知するものとする。

3 乙は、保護すべき情報に接する者（乙及び下請負者等における、派遣社員、契約社員、パート及びアルバイト等を含む。以下「取扱者」という。）から情報セキュリティの確保に関する誓約書を徴収するとともに、取扱者の名簿を作成し、同名簿を甲に通知しなければならない。

4 乙は、契約締結後速やかに、情報セキュリティ確保のため、取扱者に対し作業内容に応じた教育計画を作成し、甲の承認を得るものとする。

なお、乙が予め当該計画を有する場合には、これに代えることができる。

5 甲は乙に対し、第4項の教育計画の実施状況について、報告を求めることができる。

(守秘義務)

第4条 乙は、保護すべき情報を本契約の履行期間中のほか、履行後においても第三者

に開示又は漏えいしてはならない。

- 2 取扱者は、在職中及び離職後においても、保護すべき情報を第三者に開示又は漏えいしてはならない。
- 3 乙又は下請負者等がやむを得ず保護すべき情報を第三者に開示しようとする場合には、乙はあらかじめ、書面により甲に申請し許可を得なければならない。

(管理)

- 第5条 乙は、本契約に基づき、甲が乙に提供する情報（以下「業務情報」という。）及び甲が乙に貸与する仕様書その他の資料（以下「業務資料」という。）については、特に厳重な取扱いを行うものとし、その保管管理について一切の責任を負うものとする。
- 2 乙が甲の指定する場所において個別業務を行う場合に持ち込む物品、業務情報及び業務資料は適正に管理するものとする。また、甲の承諾なくしては、その場所から物品、業務情報及び業務資料を持ち出してはならない。
 - 3 乙は、第1項及び第2項の業務情報及び業務資料の管理について、甲の承認を得るものとする。
 - 4 乙は、業務情報及び業務資料について、本契約の履行その他甲の指定した目的以外に使用してはならない。
 - 5 乙は、業務情報について、本契約が終了したとき、又は甲から廃棄を求められたときは、これを直ちに甲が認める方法により廃棄するものとする。
 - 6 乙は、業務情報及び業務資料を、甲の承諾なくしては、方法の如何にかかわらず複製・複写してはならない。
 - 7 乙は、業務資料について、本契約が終了したとき、又は甲から返還を求められたときは、これを直ちに甲に返還するものとする。
 - 8 乙が作成（複製及び写真撮影を含む。）した文書、図面、図書等（電磁的記録を含む。）又は物件のうち、乙から甲に所有権が移転したものは全て甲の認める方法により廃棄しなければならない。

(作業責任者の選出)

- 第6条 乙が甲の指定する場所において個別業務を行う場合、乙は業務実施に関する乙の作業責任者を定め、書面をもって甲に通知するものとする。
- 2 前項により選任された作業責任者は、作業場所における乙の個別業務の実施を統括し、乙の定める規則に基づき就業管理を行い、個別業務の遂行に関する一切の事項を処理し、個別業務の遂行につき乙を代理する権限を有するものとする。
 - 3 乙が作業責任者の権限に関し制限を設けた場合若しくは作業責任者を変更する場合は、乙は当該内容を書面により事前に甲に通知するものとする。
 - 4 甲は、個別業務の遂行について作業責任者又は作業員が著しく不適當であると認めた場合は、乙に対して当該理由を通知し、必要な措置を執るべきことを求めることができるものとする。

(作業員名簿の提出)

- 第7条 乙が甲の指定する場所において個別業務を行う場合、乙は業務実施に関する乙の作業員名簿を作成し、書面をもって甲に通知するものとする。

(脆弱性対策等の実施)

- 第8条 乙は、本件業務を実施するにあたり、情報システムを使用する場合について、当該情報システムのアクセス権の付与を業務上必要な者に限るとともに、保護すべ

き情報へのアクセスを記録する措置を講ずるものとする。

- 2 前項の場合に、乙は、情報システムに対する不正アクセス、コンピューター・ウイルス、不正プログラム感染等情報システムの脆弱性に係る情報を収集し、これに対処するための必要な措置を講ずるものとする。

(情報セキュリティの対策の履行状況の確認)

第9条 乙は、契約締結後速やかに、本特約条項が定める項目を含む情報セキュリティ対策の履行状況（以下「情報セキュリティ対策履行状況」という。）を確認するとともに、確認結果について甲に報告するものとする。

- 2 乙は、契約締結後、少なくとも1年に1回、情報セキュリティ対策履行状況を確認するとともに、確認結果について甲に報告するものとする。
- 3 前各項の確認については、別記様式「情報セキュリティ対策履行状況確認書」によるものとする。ただし、別記様式の様式により難しい場合は、この限りではない。
- 4 乙は、下請負者等における情報セキュリティ対策履行状況について、前各項に準じた確認の結果を甲に対して報告するものとする。
- 5 乙は、甲に報告した確認結果について、甲の承認を得るものとする。

(情報セキュリティ侵害事案等事故)

第10条 情報セキュリティ侵害事案等事故（以下「事故」という。）とは次の各号のことをいう。

- 一 保護すべき情報のほか、契約に係る情報について、外部への漏えい又は目的外利用が行われた場合
- 二 保護すべき情報のほか、契約に係る情報について、認められていないアクセスが行われた場合
- 三 保護すべき情報を取り扱い又は取り扱ったことのある電子計算機又は外部記録媒体にコンピューター・ウイルスの感染が認められた場合
- 四 一号から三号までに掲げるもののほか、甲又は乙の保護すべき情報のほか契約に係る情報の侵害、紛失、破壊等の事故が発生し、又はそれらの疑い若しくはおそれがある場合

(情報セキュリティ侵害事案等事故に関する乙の責任)

第11条 乙は、乙の従業員又は下請負者等の故意又は過失により前条に規定する事故があったときでも、契約上の責任を免れることはできない。

(情報セキュリティ侵害事案等事故発生時の措置)

第12条 乙は、本契約の履行に際し、第10条に規定する事故があったときは、適切な措置を講ずるとともに、速やかにその詳細を甲に報告しなければならない。

- 2 甲は、第10条に規定する事故が発生した場合、必要に応じ乙に対し調査を実施することとし、乙は甲が行う当該調査について、全面的に協力しなければならない。
- 3 第10条に規定する事故が下請負者等において発生した場合、乙は甲が当該下請負者等に対して前項の調査を実施できるよう、必要な協力を行うものとする。
- 4 乙は、第10条に規定する事故の損害・影響等の程度を把握するため、必要な業務資料等を契約終了時まで保存し、甲の求めに応じて甲に提出するものとする。
- 5 第10条に規定する事故が乙の責めに帰すべき事由による場合、当該措置に必要な経費については乙の負担とする。
- 6 前項の規定は、甲の損害賠償請求権を制限するものではない。

(意図しない変更が加えられないための体制の整備)

第 13 条 乙は、甲より委託された業務の実施において、情報システムに対し甲の意図しない変更が加えられないことを保証する管理を行うこと。また、甲の求めに応じて具体的な品質保証体制を証明する書類を提出することとする。

2 情報システムに対し甲の意図しない変更が加えられる不正が判明した際には、追跡調査や立ち入り検査等により原因を調査し、排除するための体制を構築するものとする。

(情報セキュリティ監査)

第 14 条 甲は必要に応じ、乙に対して情報セキュリティ対策に関する監査を行うものとし、監査の実施のために、甲の指名する職員を乙の事業所その他関係先に派遣することができる。この場合、乙は、監査を受け入れる部門、場所、時期、条件等を記載した、「情報セキュリティ監査対応計画書」を事前に甲に提出することとする。

2 甲は、情報セキュリティ対策に関し特段の必要が生じた場合、緊急に監査を実施することができる。

3 乙は、甲が情報セキュリティ対策に関する監査を実施する場合、甲の求めに応じ、必要な協力（甲の指名する職員による取扱施設への立ち入り及び関係書類の閲覧等）をしなければならない。

4 甲が下請負者等に対して情報セキュリティ対策に関する監査を行うことを求める場合、乙は当該監査の実施のために必要な協力を行うこととする。

5 乙は、自ら情報セキュリティ対策に関する監査を行った場合は、その結果を甲に報告することとする。

6 甲は、監査の結果、情報セキュリティ対策が十分満たされていないと認められる場合は、その是正のための必要な措置を講ずるよう乙に求めることができる。

7 乙は、前項の規定により、甲から求めがあったときは、速やかにその是正措置を講じなければならない。

(契約の解除)

第 15 条 甲は、第 10 条に規定する事故が、乙の責めに帰すべき事由により発生した場合において、本契約の目的を達することができなくなった場合は、この契約の全部又は一部を解除することができる。

2 前項の場合において、主たる契約条項の契約の解除に関する規定を準用する。

○機器の調達に係る遵守事項

1 当該機器等の製造工程において意図しない変更が加えられないよう適切な措置が執られており、当該措置を継続的に実施していること。

2 当該機器等の製造工程の履歴に関する記録を含む製造工程の管理体制が適切に整備されていること。

3 機器等に対して不正な変更が加えられないように製造者等が定めたセキュリティ確保のための基準等が整備されており、その基準等が当該機器等に適応されていること。

4 機器等の設計から部品検査、製造、完成品検査に至る工程について、不正な変更が行われないことを保証する管理が一貫した品質保証体制の下でなされていること。機器に不正が見つかったときに、追跡調査や立入検査等により原因を調査し、排除できる体制を整備している生産工程による製品であること。

5 情報システムを構成する要素（ソフトウェア、ハードウェア）に対して不正な変更

があった場合に識別できる構成管理体制が確立していること。

- 6 受託者が情報システムを構成する要素（ソフトウェア、ハードウェア）として採用した機器等について、不正な変更が加えられていないことを検査する体制が受託者において確立していること。

○ ソフトウェアの調達に係る遵守事項

- 1 本仕様書で調達するソフトウェアについては、不正な変更（製造工程、流通過程で不正プログラムを含む予期しない又は好ましくない特性を組み込むことをいう。以下同じ。）の有無を確認し、不正な変更が存在した場合は、当該不正な変更の修正を行った上で納入すること。
- 2 本仕様書で調達するソフトウェアについて、不正な変更が疑われると滋賀県警察が判断した場合は、契約業者において調査及び必要な措置を講じること。