

別紙5 情報セキュリティ特記事項

(基本事項)

- 第1 受注者は、この契約による業務を行うにあたり、本契約で構築するシステムで取り扱う情報（以下、情報資産という）の取扱いに際し、情報セキュリティの重要性を認識し、情報資産の漏えい、紛失、盗難、改ざん等から保護するため、必要な措置を講じなければならない。
- 万一、必要とされる措置が講じられていなかった場合、もしくは、情報セキュリティの環境の変化や新たなサイバー攻撃の状況に応じて追加の措置が必要と判断された場合は、速やかに発注者に書面による報告の上、対応策を策定し協議しなければならない。
- なお、受注者が業務を遂行するにあたり下請けなどを利用する場合は、下請けなども本事項の対象とする。
- 2 受注者は「地方独立行政法人大阪府立病院機構情報セキュリティ確保に関する規程」及び「地方独立行政法人大阪府立病院機構情報セキュリティ確保に関する対策基準」を遵守しなければならない。

(組織体制)

- 第2 受注者は、この契約による業務を行うにあたり必要な情報セキュリティに関する組織体制として、次に掲げる事項について書面を提出しなければならない。また、内容に変更がある場合、受注者は速やかに書面により発注者へ連絡しなければならない。
- (1) 情報セキュリティに係る責任体制
 - (2) 情報資産の取扱部署及び責任者並びに担当者
 - (3) 通常時及び緊急時の連絡体制
 - (4) 業務履行場所
 - (5) インシデント発生時の対応策

(提出書類)

- 第3 受注者は、発注者側に情報資産に関するシステムや各種機器などを導入する際は、契約締結後、速やかに下記の書類を提出し、発注者の承認を得なければならない。適応状況が不十分だと指摘された場合は速やかに対応しなければならない。なお各ガイドラインなどは定期的に改訂されるため、常時最新版に対応しなければならない。
- (1) システムおよびシステム用機器（ネットワーク機器含む）導入時における提出書類
 - (ア) 「医療情報システムの安全管理に関するガイドライン（厚生労働省）」に準拠していることがわかるもの
 - (イ) 「地方公共団体における情報セキュリティポリシーに関するガイドライン（総務省）」に準拠していることがわかるもの
 - (ウ) 今後、策定される「サイバーインフラ事業者に求められる役割等に関するガイドライン（経済産業省）」に準拠していることがわかるもの
 - (エ) 「医療機関におけるサイバーセキュリティ対策チェックリスト 事業者確認用（厚生労働省）」「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン（経済産業省）」に基づくサービス仕様適合開示書及びサービス・レベル合意書（SLA）
 - (オ) 「製造業者/サービス事業者による医療情報セキュリティ開示書ガイド（JAHIS）」にお

けるチェックリスト

(カ) SBOM (Software Bill of Materials、ソフトウェア部品表)

(キ) 「JAHIS リモートサービス セキュリティガイドライン」に基づく ISMS 準拠リモートサービスリスクアセスメント表

(ク) 製品・サービスにおける脆弱性がないことを保証表明する書面、もしくは脆弱性診断結果の書面

なお、納品時において脆弱性が改善されていない場合は代替案を提示し、発注者の承認を得たうえで対応すること。

(2) 医療機器等導入時における提出書類

(ア) 「医療機関におけるサイバーセキュリティ対策チェックリスト 事業者確認用」(厚生労働省)

(イ) 「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン(経済産業省)」に基づくサービス仕様適合開示書及びサービス・レベル合意書(SLA)

(ウ) 「製造業者/サービス事業者による医療情報セキュリティ開示書」ガイド(JAHIS)におけるチェックリスト

(エ) 医療機器のサイバーセキュリティ導入に関する手引書(厚生労働省)に準拠していることがわかるもの

(オ) SBOM (Software Bill of Materials、ソフトウェア部品表)

(カ) 「JAHIS リモートサービス セキュリティガイドラインに基づく」ISMS 準拠リモートサービスリスクアセスメント表

(キ) 製品・サービスにおける脆弱性がないことを保証表明する書面、もしくは脆弱性診断結果の書面

なお、納品時において脆弱性が改善されていない場合は代替案を提示し、発注者の承認を得たうえで対応すること。

(委託目的以外の利用等の禁止)

第4 受注者は、発注者の文書による承諾がある場合を除き、この契約による業務に係る情報資産を当該業務以外の目的に使用し、又は第三者に提供してはならない。

(複写及び複製の禁止)

第5 受注者は、発注者の文書による承諾がある場合を除き、この契約による業務を行うために発注者から引き渡された情報資産を複写し、又は複製してはならない。

(業務履行場所以外への持出禁止)

第6 受注者は、発注者の文書による承諾がある場合を除き、この契約による業務に係る情報資産を業務履行場所以外へ持ち出してはならない。

(情報資産の受渡し)

第7 この契約による業務に係る情報資産の提供、返却又は廃棄については、受注者所定の手順に従って行うものとし、受渡票等で確認し行うものとする。

2 受注者は発注者による前項の手順書の確認を受けなければならない。

(厳重な保管及び搬送)

第 8 受注者は、この契約による業務に係る情報資産の漏えい、紛失、盗難、改ざんその他の事故等を防止するため、情報資産の厳重な保管及び搬送に努めなければならない。

(再委託の禁止)

第 9 受注者は、発注者の文書による承諾がある場合を除き、この契約による情報資産の取扱いを自ら行うものとし、その取扱いを第三者に委託し、又は請け負わせてはならない。

2 受注者は、情報資産の取扱いを第三者に委託し、又は請け負わせようとするときは、当該委託先又は請負先に、この情報セキュリティ特記事項で要求する事項を遵守させなければならない。

3 当該委託先または請負先による不法行為、過失もしくは情報漏洩等の事故の責任は、すべて受注者が負うものとする。

(事故発生時の報告)

第 10 受注者は、この契約による業務に係る情報資産の漏えい、紛失、盗難、改ざんその他の事故等が生じ、又は生じた可能性があることを知ったときは、可及的速やかに発注者に報告し、その指示に従わなければならない。これには、情報資産の保全、事故等の拡大防止、二次漏洩等の有無の監視、原因究明、再発防止策の策定などが含まれるが、これに限られたものではない。なお、これらはこの契約が終了し、又は解除された後においても同様とする。

(調査の実施)

第 11 発注者は、この契約による業務に係る受注者の情報セキュリティの運用状況に関し、必要に応じて業務履行場所への立入調査等を行うことができるものとする。

2 受注者は、発注者から業務履行場所への立入調査等の申入れがあったときは、速やかに応じるものとする。

3 発注者は、第 1 項による業務履行場所への立入調査等による確認の結果、受注者による情報セキュリティの運用状況が不適切であると認めたときは、期限を定めて改善を勧告するものとする。

4 受注者は、前項による改善勧告を受けたときは、この改善勧告に速やかに応じなければならない

(情報資産の返還又は廃棄)

第 12 受注者は、この契約が終了し、又は解除されたときは、この契約による業務に係る情報資産を、速やかに発注者に返還し、又は所定の手順に従って確実に廃棄しなければならない。

2 受注者は、前項の手順書を発注者に提出しなければならない。

(特記事項に違反した場合の契約解除及び損害賠償)

第 13 発注者は、受注者がこの情報セキュリティ特記事項に違反していると認めたときは、違反の速やかな是正、もしくは契約の解除及び損害賠償の請求をすることができるものとする。

(違反事実の公表等)

第 14 受注者がこの情報セキュリティ特記事項に違反し、契約を解除された場合、発注者は、受注者の名称及び違反事実を公表することができる。

(実施責任)

第 1 5 受注者は、受注者内における情報資産の情報セキュリティ対策を明確にし、発注者が求めた際には速やかに報告しなければならない。

(機器等セキュリティ要件)

第 1 6 受注者は、この契約による業務を行うにあたり発注者内にシステム機器（サーバー、クライアント端末、ネットワーク機器等）または医療機器などを導入・設置、保守する場合は以下を遵守しなければならない。

- (1) システム機器または医療機器にウイルス対策ソフトを導入し、有効にしなければならない。なお、ウイルス対策ソフトを導入することが難しい場合は発注者と協議のうえ、有効な対応策がある場合は実施すること。
- (2) ウイルス対策ソフトは最新の製品モジュール、検索エンジン、パターンファイルのいずれも更新し、最新の状態を保たなければならない。なお、パターンファイルについては、毎日、更新しなければならない。
- (3) サポート切れのソフトウェア（OS、ファームウェアを含む）を使用してはならない。契約期間内にサポート切れとなることが判明した場合は、早期にアップデートないしは機器更新を行わなければならない。なお、その費用については別途協議することとする。
- (4) OS 及び利用するソフトウェアのメーカーが提供するセキュリティパッチの情報取得の方法を定め、確認・適用を最低月次 1 回以上行わなければならない。なお、セキュリティパッチの適用はリリース後、10 日をめどに行うこととする。ただし、仕様書などで別途定める場合はそれに従うこととする。
- (5) システム機器または医療機器のログインパスワードは初期パスワードや弱いパスワード、漏洩したパスワードを使用してはならない。また、万が一、パスワードの漏洩やインシデントの兆候が確認された場合は速やかに変更を行うこととする。（なお、パスワードは原則 16 文字以上とし、数字、語句の連続や繰り返しを含まないこととする。）
- (6) システム機器（サーバ、クライアント端末等）はロックアウト設定（例：パスワード入力を 10 回連続で間違えると、アカウントが 10 分間ロックされる）を行わなければならない。
- (7) 発注者側のサーバー等と連携する際の仕様については、ネットワーク構成図及び論理構成図などを提出し、協議のうえ決めることとする。
- (8) システム機器または医療機器は最小特権での運用を行うとともに、管理者権限の使用が想定される状況と、管理方法を説明し、承認を得なければならない。

(リモートメンテナンス)

第 1 7 受注者から発注者に設置したサーバーまたは機器等保守のためにリモートメンテナンスを行う場合は、以下の事項を遵守しなければならない。

- (1) リモートメンテナンスを行う場合は、操作者を限定し、ネットワーク機器に通信制限（接続元 IP アドレス制限等）を行った上で、リモートメンテナンスを行わなければならない。なお、リモートメンテナンスを行う受注者側の端末においても同様のセキュリティ対策を施さなければならない。
- (2) リモートメンテナンスを行う場合は、システム構成や通信方式、通信機器（VPN 装置等）の脆弱

性管理方法、責任分界点及び操作ログの形式などについて発注者に文書を提出し、発注者側の承認を得なければならない。また、リモートメンテナンスを行う際は発注者指定の書式を用いて事前申請を行い、実施の都度、報告書を提出しなければならない。

(3) 上記で利用する通信機器は1年以上ログを保存しなければならない。

(その他セキュリティ要件)

第18 受注者は、この契約による業務を行うにあたり以下の事項を遵守すること。

- (1) 各種システムへのアクセスログ、操作ログやセキュリティシステムのイベントログはシステムごとに、取得方法、異常イベント、保存方法について一覧表を提出し協議の上、受注者、発注者間で合意するものとする。また、通信機器の `syslog` を含めすべてのログは、1年間をめに保存するように設定しなければならない。あらかじめ定めた異常値に基づき、イベントやインシデントの発生の有無を稼働3か月は月次で確認し、その後は、協議の上、期間を定めて定期的に確認するものとする。
- (2) バックアップデータを取得しなければならない。なお、実施に当たってはバックアップデータの取得方法、取得頻度、取得期間、保管方法及びバックアップの実施主体、管理責任者を定めた文書を発注者に提出し、承認を得なければならない。
- (3) 受注者が提供または保守を行う機器の脆弱性管理及び監査の実施状況を四半期ごとに報告しなければならない。また、必要に応じて、発注者による実査を受けなければならない。
- (4) サイバーセキュリティインシデントに対する対応マニュアルを整備し、発注者の承認を得なければならない。
- (5) サイバーセキュリティインシデント発生時に、対応マニュアル通りの対応ができるよう、またマニュアルに想定していないインシデント発生時にも対応できるよう演習などを行い備えておかななければならない。
- (6) サイバーセキュリティ維持における疑義や、インシデント事象が発生した場合は、可及的速やかにすべての事実報告を行わなければならない。また、インシデント拡大の最小化、原因の究明、早期の復旧を確保するために、発注者による調査、助言を受け入れなければならない。
- (7) 発注者に関わるインシデントが発生した場合、受注者が契約している他施設にもインシデントが波及する恐れがある場合は、発注者と他施設との情報共有を行うよう、受注者から他施設に申し入れを行わなければならない。

(その他)

第19 受注者は、第1から第18までに定めるもののほか、情報資産の適正な管理のために必要な措置を講じなければならない。