別記４

情報セキュリティ取扱特記事項

（基本的事項）

第１条　受託者は、この協定に基づく業務（以下「本件業務」という。）を履行するに当たっては、上天草市情報セキュリティポリシーを遵守し、セキュリティに関する適切な管理策を講じなければならない。

（定義）

第２条　この特記事項において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

（１）本件業務に関する情報

委託者が本件業務を履行させるために受託者へ提供した情報（個人情報を含む。）又は受託者が本件業務を履行するために収集し、若しくは作成した情報をいい、形状は問わず、複写複製も含むものをいう。

（２）情報セキュリティ

本件業務に関する情報を含む情報の機密性、完全性及び可用性を確保し、維持することにより、適切な利用環境を維持しながら、犯罪、災害等の各種脅威から情報を守ることをいう。

（３）機密性

情報へのアクセスが許可されない者は、情報にアクセスできないようにすることをいう。

（４）完全性

正確な情報及び正確な処理方法を確保することをいう。

（５）可用性

情報へのアクセスが許可されている者が必要なときに確実に利用できるようにすることをいう。

（６）情報システム

情報を適切に保存・管理・流通するための仕組みをいい、コンピュータとネットワーク及びそれを制御するソフトウェア、その運用体制までを含んだものをいう。

（７）マルウェア

情報システムに対して攻撃をするソフトウェアをいう。

（８）情報セキリィティインシデント

情報セキュリティに関する事故・問題をいう。

（目的外利用の禁止）

第３条　受託者は、本件業務の履行に当たり、本件業務に関する情報を収集、作成又は利用するときは、本件業務の履行目的の範囲内で行うものとする。

２　受託者は、本件業務の履行に当たり委託者に対し、当該情報にアクセスする者及びアクセス方法について明示し、委託者の承認を得なければならない。

（守秘義務）

第４条　受託者は、業務の履行に当たり、業務上、知り得た情報については守秘義務を負うものとする。

（第三者への提供の禁止）

第５条　受託者は、本件業務に関する情報を委託者の承諾なしに第三者に提供してはならない。

（再委託の禁止又は制限）

第６条　受託者は、本件業務を自ら履行するものとし、やむを得ず本件業務の一部を第三者

に再委託するときは、再委託する業務範囲を明示したうえで、必ず委託者の承諾を得るものとする。
2　受託者は、前項の規定により委託者の承諾を得て第三者に再委託する場合にあっては、再委託先に対し、情報セキュリティに関して監督する責任を有することとし、再委託先の情報セキュリティの管理体制について委託者に報告しなければならない。
3　受託者は、委託者が前項の規定による報告によって再委託先の情報セキュリティの管理体制が不十分であることを理由として、再委託先の変更又は中止を求めた場合にあっては、再委託先の変更又は中止をしなければならない。
（適正管理）
第７条　受託者は、本件業務に関する情報の滅失及び損傷の防止に努めるものとする。
（複写又は複製の禁止）
第８条　受託者は、本件業務に関する情報を、委託者の承諾なしに複写し、又は複製してはならない。
（無断持ち出しの禁止）
第９条　受託者は、本件業務に関する情報について、委託者の承諾なしに、次に掲げる行為をしてはならない。
（１）この協定により指定された作業場所以外の場所に持ち出し、又は送付すること。
（２）電子メール、ファックスその他の電気通信（電気通信事業法第２条第１号に規定する電気通信をいう。）を利用して、この協定により指定された作業場所以外の場所に送信すること。
（情報セキュリティの維持、改善等）
第１０条　受託者は、本件業務に関する情報及び情報システムの取扱いについて、機密性、完全性及び可用性を確保し、維持するために、次に掲げる管理策を講じなければならない。
（１）マルウェアに対するリスクを最小限にするために、情報システムに対し、マルウェア対策ソフトの導入を許容するとともに、その定義ファイルについても常に最新の状態に維持されることを阻害してはならない。
（２）常に脆弱性等の情報を収集し、修正プログラムが公開された場合には、情報システムに対し、対抗策を講じなければならない。この場合において、受託者が開発し、又は開発させ委託者に納入している情報システムの改修が必要となるときは、委託者と対応策を協議するものとする。
（３）本件業務に関する情報を含む情報の流出、改ざん、消失及び不正利用を防止するために必要な措置を講じなければならない。
（４）その他、情報セキュリティの維持のために必要と認められる場合、委託者と協議の上、対応策を講じなければならない。
2　受託者は、前項に規定により講じている管理策の内容を定期的に報告しなければならない。
3　受託者は、この特記事項に基づく報告、情報セキュリティの管理体制、実施事項に関する書類を整備しておかなければならない。
（情報セキュリティインシデントへの対応等）
第１１条　本件業に関し、情報セキュリティインシデントが発生したときは、受託者は、直ちに、委託者に報告するとともに、委託者の指示に従い、その対応策を講じなければならない。
2　受託者は、前項の規定により対応策を講じたときは、その内容を委託者に報告しなければならない。
3　委託者は、本件業務に関する情報セキュリティインシデントが発生した場合であって、

必要があると認めるときは、当該情報セキュリティインシデントの公表を行うことができる。

（情報セキュリティの管理体制）

第１２条　受託者は、第１条に規定する情報セキュリティの管理体制の内容について委託者と協議しなければならない。

２　前項の情報セキュリティの管理体制には、情報セキュリティ担当責任者及び担当者の職及び役割を明確にしておかなければならない。

３　受託者は、本件業務を担当する者に対して、情報セキュリティに関する教育及び情報セキュリティインシデントに対する訓練を実施するものとする。

（不要な情報の返却又は廃棄）

第１３条　受託者は、本件業務に関する情報のうち、不要となったものについては、直ちに、返却又は復元できないような形で廃棄しなければならない。

２　受託者は、前項の規定により本件業務に関する不要な情報を廃棄したときは、書面をもって委託者に報告するものとする。

（業務終了時の情報資産の返還、廃棄等）

第１４条　受託者は、業務終了後、前条によらない情報資産について、直ちに委託者に返還しなければならない。

２　受託者は、前項に規定により、情報資産の返還を行う場合、紙媒体・電子媒体を問わず、委託者及び次の指定管理者が事務処理を行うに当たって、最も好ましい状態により返還するものとする。

（報告の徴収、立入検査等）

第１５条　委託者は、情報セキュリティの維持・改善を図るため、受託者に対し、必要に応じて本件業務に係る情報セキュリティ対策について報告を求めるとこができる。

２　委託者は、情報セキュリティの維持・改善を図るために必要な範囲において、指定した職員に、本件業務と係わりのある場所に立ち入り、受託者が講じた情報セキュリティ対策の実施状況について検査させ、若しくは関係者に質問させ、又はその情報セキュリティ対策が情報セキュリティの維持・改善を図るために有効なものであるか等について調査をさせることができる。

３　受託者は、委託者から前項の規定による立入検査の申入れがあった場合は、これに応じなければならない。

（損害賠償義務）

第１６条　受託者は、受託者又は再委託先が本取扱特記事項に定める規定を遵守せず、情報を漏えい、滅失、毀損、不正使用その他の違反によって委託者又は第三者に生じた一切の損害について、賠償の責めを負う。