情報セキュリティに関する特記事項

（目的）

第１条　本特記事項は、那覇市情報セキュリティポリシーに基づき、情報通信ネットワーク並びに情報システムの開発及び保守を含む情報システム関連業務全般にわたる業務委託に関して、受託者が守るべき情報セキュリティに関する特記事項を定めることを目的とする。

（用語の定義）

第２条　本特記事項で用いる用語の定義は、次のとおりとする。

（１）委託者

ネットワーク、情報システム及び情報資産を取り扱う業務の処理を委託した者をいう。

（２）受託者

ネットワーク、情報システム及び情報資産を取り扱う業務の処理の委託を受けた者をいう。

（３）情報セキュリティ管理者

委託者の部局等における課（室）長をいう。

（４）ネットワーク

コンピュータ等を相互に接続するための通信網、その構成機器(ハードウェア及びソフトウェア)をいう。

（５）情報システム

コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

（６）情報資産

ネットワーク及び情報システムの開発と運用に係る全てのデータ並びにネットワーク及び情報システムで取り扱う全ての情報をいう。

なお、情報資産には、紙等の有体物に出力された情報も含むものとする。

（７）管理区域

ネットワークの機器及び重要な情報システムを設置し、並びに当該機器等の管理及び運用を行うための部屋や電磁的記録媒体の保管庫をいう。

（管理体制の整備）

第３条　受託者は、委託業務に係る情報セキュリティに関する組織的な体制として、次に掲げる事項について書面により明らかにしなければならない。また、内容に変更がある場合、受託者は速やかに書面により委託者へ連絡しなければならない。

（１）情報資産の取扱部署並びに責任者及び担当者

（２）情報資産を取り扱う作業範囲

（３）情報資産を取り扱う場所

（４）通常時及び緊急時の連絡体制

（秘密の保持）

第４条　受託者は、委託者から秘密である旨の告知とともに知り得た情報を他に漏らしてはならない。委託業務に係る契約が終了し、又は解除された後においても同様とする。

（再委託の禁止）
第５条　受託者は、委託業務を第三者に委託することはできない。ただし、あらかじめ委託者の書面による承諾を受けたときはこの限りでない。委託者の承諾を受けた第三者が更に第三者に委託する場合、以降の第三者（以下、委託者の承諾した第三者を総称して「再委託先」という。）に委託する場合についても同様とする。
２　受託者は、前項ただし書の規定により委託者の承諾を得ようとする場合、再委託先の名称及び住所、再委託の理由、再委託の内容、再委託先が取り扱う情報、再委託先に対する監査の方法等を委託者に書面により通知するものとする。なお、委託者から受けた承諾の内容を変更しようとする場合も同様とする。
３　受託者は、再委託先との間で、再委託にかかる業務を遂行させることについて、委託業務に基づいて受託者が委託者に対して負担するのと同様の義務を、再委託先に負わせる契約を締結するものとする。
４　受託者は、再委託先の履行について、自ら業務を遂行した場合と同様の責任を負うものとする。

（教育の実施）
第６条　受託者は、委託業務に係る受託者の責任者及び担当者に対して、情報セキュリティに関する教育（本特記事項の遵守を含む。）など委託業務の履行に必要な教育を実施するとともに、関係法令及び関係規程を遵守させるため、必要な措置を講じなければならない。

（情報資産の利用場所）
第７条　受託者は、委託業務を処理するために委託者から引き渡され、又は自らが取得し、若しくは作成した委託者の情報資産を、委託者が指示した場所以外で利用してはならない。ただし、委託者の書面による事前の承諾がある場合はこの限りでない。

（入退室等管理）
第８条　受託者は、委託者の管理区域に入室する場合、身分証明書等を携帯し、委託者の求めにより提示しなければならない。
２　受託者は、委託者の管理区域への機器の搬入出においては、管理区域への入退室を許可された委託者の職員の立ち会いのもと行わなければならない。
３　受託者は、委託者の管理区域に入室する場合、委託業務に不要なコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等を持ち込んではならない。
４　受託者は、委託者の管理区域へ搬入する機器等が、既存の情報システムに与える影響について、あらかじめ確認を行なわなければならない。

（情報資産の利用）
第９条　受託者は、委託業務を履行するにあたって知り得た情報を、委託者の書面による事前の承諾を得ることなく委託業務を履行する目的以外で利用し、又は第三者に提供してはならない。
２　受託者は、委託者の書面による事前の承諾を得ることなく委託者の情報資産に係る情報を複写し、又は複製してはならない。

（情報資産の保管）
第 10 条　受託者は、委託者から情報資産の提供等を受けた場合、当該情報資産の漏えい、紛失、

盗難、改ざんその他の不正行為が行われないように適正に保管しなければならない。

（情報資産の持ち出し）

第 11 条　受託者は、情報資産を所管する委託者の情報セキュリティ管理者の書面による事前の承諾を得ることなく情報資産を外部へ持ち出してはならない。

2　受託者は、前項により情報資産を持ち出すときは、盗難、紛失、不正コピーその他の情報資産の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。

（情報資産の返却及び廃棄）

第 12 条　受託者は、委託業務で必要がなくなった場合は、委託者の指示に従い、委託者の情報システム及び情報資産を直ちに委託者に返却し、又は廃棄その他の処分を行うものとする。

2　廃棄の方法は、次条の定めによるものとする。

（廃棄の方法）

第 13 条　受託者は、委託者の情報システム及び情報資産を廃棄する場合は、委託者の情報セキュリティ管理者の事前の承諾を得て、情報を復元できないようデータ消去ソフトウェア等により消去し、又は物理的に破壊しなければならない。

2　受託者は、前項により情報を廃棄した場合は、速やかに廃棄日時、廃棄担当者、廃棄処理内容その他の廃棄した旨を証明する書面を委託者に提出しなければならない。

（不正プログラム対策）

第 14 条　受託者は、情報システムにコンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させ、最新の状態に保たなければならない。

2　受託者は、委託業務において、ソフトウェア開発元の提供するパッチやバージョンアップなどのサポートが終了したソフトウェアを使用してはならない。

（セキュリティ侵害の未然防止）

第 15 条　受託者は、情報システムのセキュリティホールに関する情報を収集し、必要に応じて、委託者を含む関係者間で共有しなければならない。また、当該セキュリティホールの緊急性及びリスクに応じて、ソフトウェア更新等の対策を実施しなければならない。

2　受託者は、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、情報セキュリティの侵害を未然に防止するための対策を速やかに講じなければならない。

（情報システムの導入）

第 16 条　受託者は、情報システムを導入する場合、既に稼働している情報システムに接続する前に十分な試験を行わなければならない。

2　受託者は、個人情報などの重要な情報を含む情報資産を試験に使用してはならない。

3　受託者は、情報システムの導入及び試験環境から運用環境への移行について、手順を明確にするとともに、情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるようにしなければならない。

（ネットワーク及び情報システムの管理）

第 17 条　受託者は、委託業務で使用するネットワーク及び情報システムを構成する機器に対し、委託者の事前の承諾を得ることなくソフトウェアを導入してはならない。

2　受託者は、サーバなどの情報システムを構成する機器の取付けを行う場合、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適切に固定する等、必要な措置を講じなければならない。

3　受託者は、委託者の事前の承諾を得ることなく委託業務で使用するネットワーク及び情報システムを構成する機器の改造、増設又は交換を行ってはならない。

4　受託者は、ネットワーク又は情報システムを変更した場合は、変更履歴を作成し管理しなければならない。

5　受託者は、委託者の事前の承諾を得ることなく情報システムを構成する機器等をネットワークへ接続し、又はネットワークに接続している機器等を他ネットワークへ接続してはならない。

（事故等の報告）

第 18 条　受託者は、委託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が生じ、又は生じたおそれがあることを知ったときは、直ちに委託者に報告し、その指示に従わなければならない。

2　受託者は、前項の事故の原因を究明し、記録を保存しなければならない。また、事故の原因究明の結果から、再発防止策を検討し、委託者に報告しなければならない。

（監査・検査への協力）

第 19 条　委託者は、委託業務に係る受託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、検査、指導等を行うことができる。

2　受託者は、委託者から前項の立入調査、検査等の申入れがあったときは、特段の理由が認められる場合を除き、協力しなければならない。

3　委託者は、第１項による立入調査、検査等による確認の結果、受託者による情報セキュリティの運用状況に瑕疵を認めたときは、期限を定めて指導又は改善を勧告するものとする。

4　受託者は、前項による指導又は改善勧告を受けたときは、これに速やかに応じなければならない。

（セキュリティ事故の公表）

第 20 条　委託者は、受託者の責に帰すべき事由に伴う情報セキュリティに関する事故を認知した場合には、その重要度や影響範囲等を勘案し、受託者の名称を含む当該事故の概要について報道機関等へ公表することができ、受託者はこれを受認しなければならない。