別記６

指定管理業務に係る情報セキュリティに関する特記事項

（総則）

第１　この特記事項は，この特約が添付される協定（以下「本協定」という。）と一体をなすものとし，指定管理者はこの協定による業務（以下「業務」という。）を行うに当たっては，この「情報セキュリティに関する特記事項」を守らなければならない。

（基本的事項）

第２　指定管理者は，業務を行うに当たっては，個人情報の保護に関する法律（平成 15 年法律第 57 号）及び指定管理者向け情報セキュリティ遵守事項に基づき，情報を適正に取り扱わなければならない。

（機密の保持等）

第３　機密の保持等については，次のとおりとする。

１　指定管理者は，本協定に係る業務の遂行に当たって，直接又は間接に知り得た一切の情報について，市の許可なく業務遂行の目的以外の目的に使用し，又は第三者に提供してはならない。本協定の終了後においても同様とする。

２　指定管理者は，本協定に係る業務の遂行に当たって入手した資料，データ，記録媒体等について，常に適正な管理を行うとともに，特に個人情報等の重要な情報について，暗号化，パスワードの設定，個人情報の匿名化，アクセス制限等，厳重に管理し，使用しない場合には，施錠ができる書庫等に保管しなければならない。

３　指定管理者は，本協定に係る業務の遂行に当たって，市又は市の関係者から提供された資料や情報資産（データ，情報機器，各種ソフトウェア，記録媒体等。以下同じ。）について，庁外若しくは社外へ持ち出し，若しくは第三者に提供し（電子メールの送信を含む。），又は業務遂行の目的以外の目的で，資料，データ等の複写若しくは複製を行ってはならない。ただし，あらかじめ市の承認を得た場合はこの限りでない。なお，その場合にあっても，指定管理者は，情報漏えい防止のための万全の措置を講じなければならない。

４　指定管理者は，本協定に際して，業務の遂行において取り扱う電子データの保存先等を別記様式により届け出るとともに，クラウド等のオンラインストレージを使用している場合には，利用契約先の情報を市に申し出なければならない。また，内容に変更が生じた場合には，指定管理者は市に対して速やかに報告をするものとする。

（従事者への教育）

第４　指定管理者は，本協定に係る業務の遂行に当たって，本協定に係る業務に従事する者に対して，情報セキュリティに対する意識の向上を図るための教育を実施しなければならない。

（委託等に当たっての留意事項）

第５　指定管理者は，市の書面による承諾を得て業務の全部又は一部を第三者に委託（二以上の段階にわたる委託をする場合及び指定管理者の子会社（会社法（平成 17 年法律第 86 号）第２条第１項第３号に規定する子会社をいう。）に委託をする場合を含む。以下「委託等」という。）する場合には，委託等の相手方にこの特記事項及び指定管理者向け情報セキュリティ遵守事項を遵守させなければならない。

（委託等に係る連帯責任）

第６　指定管理者は，委託等の相手方の行為について，委託等の相手方と連帯してその責任を負うものとする。

（資料等の返還等）

第７　指定管理者が本協定による業務を遂行するために，市から提供を受けた資料や情報資産は，業務完了後直ちに市に返還するものとする。ただし，市が別に指示したときは当該方法によるものとする。

（委託等の相手方からの回収）

第８　指定管理者が，市から提供を受けた資料や情報資産について，市の承認を得て委託等の相手方に提供した場合は，指定管理者は，市の指示により回収するものとする。

（報告等）

第９　報告等については，次のとおりとする。

1　市は，必要があると認めるときは，指定管理者又は委託等の相手方に対して，この特記事項の遵守状況その他セキュリティ対策の状況について，定期的又は随時に報告を求めることができる。

2　指定管理者は，この特記事項に違反する行為が発生した場合，又は発生するおそれがあると認められる場合(委託等の相手方により発生し,又は発生したおそれがある場合を含む。)は，直ちに市にその旨を報告し，その指示に従わなければならない。

3　指定管理者は，この特記事項への違反の有無にかかわらず，本協定に係る業務で取り扱う情報資産に対して，情報セキュリティインシデントが発生した場合，又は発生するおそれがあると認められる場合は，直ちに市にその旨を報告し，その指示に従わなければならない。

（立ち入り検査）

第 10　市は，この特記事項の遵守状況の確認のため，指定管理者又は委託先の事業者に対して立ち入り検査（市による検査が困難な場合にあっては，第三者や第三者監査に類似する客観性が認められる外部委託事業者の内部監査部門による監査，検査又は国際的なセキュリティの第三者認証(ISO/IEC27001 等)の取得等の確認）を行うことができる。

（情報セキュリティインシデント発生時の公表）

第 11　市は，本協定に係る業務に関して，情報セキュリティインシデントが発生した場合（委託等の相手方により発生した場合を含む。）は，必要に応じて，当該情報セキュリティインシデントを公表することができるものとする。

（情報セキュリティの確保）

第 12　市は，本協定に係る指定管理者の業務の遂行に当たって，前項までに定めるもののほか，必要に応じて，情報セキュリティを確保する上で必要な対策を実施するよう指示することができ，指定管理者はこれに従わなければならない。

（指定の取消し等）

第13　市は，指定管理者が本特記事項に定める義務を履行しない場合又は法令に違反した場合には，指定管理者の指定を取り消し，又は期間を定めて指定管理業務の全部若しくは一部の停止を命ずることができる。

（損害賠償）

第14　指定管理者は個人情報の取扱いにより発生した損害（第三者に及ぼした損害を含む。）のために生じた経費は，指定管理者が負担するものとする。

指定管理者向け情報セキュリティ遵守事項

（総則）

第１　この情報セキュリティ遵守事項は，指定管理者が業務を行う際に情報セキュリティを遵守するための細則及び具体的な手順を定めたものである。

（セキュリティ事案発生時の連絡）

第２ 市が発注した委託業務に関し，情報セキュリティインシデントが発生した場合は次の対応を行わなければならない。

１　市の窓口に連絡すること。

２　最初に事案を認識した時点から，60 分以内に市に連絡すること。

（ノート PC の持ち出しについて）

第３　ノート PC の持ち出しについては，次の事項を遵守すること。

１　持ち出すノート PC には，二要素認証方式を導入していること。

２　ノート PC の持ち出し前及び持ち帰り時は，責任者の承認を得ること。

３　ノート PC に入れる秘密情報は，データ暗号化による保護を実施すること。

４　秘密保持を保持したノート PC を保持したまま，酒席の参加は厳禁とする。

５　ノート PC には，必要な情報のみ保存すること。

６　ノート PC 内の情報は決められたサーバ等に保存し，持ち帰り時は残さず削除すること。

（書類含む情報の持ち出しについて）

第４　書類を含む情報の持ち出しについては，次の事項を遵守すること。

１　秘密情報を持ち出す際は，事前に責任者の許可を得ること。

２　持ち出し目的の業務に不要な情報は持ち出さないこと。

３　持ち出した情報を，置き忘れたり，紛失しないこと。

４　秘密情報を所持したまま，酒席の参加は厳禁とする。

（業務用携帯電話・スマートフォンの利用について）

第５　業務用携帯電話・スマートフォンの利用については，次の事項を遵守すること。

１　セキュリティロック（端末ロック等）を常時設定すること。

２　紛失時に端末を遠隔でロックできる機能（遠隔ロック等）を設定すること。

３　ネックストラップやフォルダー等を適切に利用し，紛失防止対策を実施すること。

４　発着信履歴及び送受信メール等は，都度削除すること。

５　電話帳に個人を特定できるフルネームで登録しないこと。

６　カメラ画像については，事前に撮影や取り扱いの確認の上，サーバ等への保存後は速やかに削除すること。

（電子メールの送信について）

第６　電子メールの送信については，次の事項を遵守すること。

１　宛先，メール本文，添付ファイルの中身について、送信前に確認すること。

２　添付ファイルがある場合，暗号化又はパスワード付き圧縮形式にして保護すること。そのパスワードは同じメールに記載せず，別途連絡すること。

３　匿名で登録・利用できるメールサービスやファイル交換サービスなど，相手先を確実に特定できないツールを利用した情報の送受信を行わないこと。

（オンラインサービスへの登録禁止）

第７　インターネット上で提供されている地図情報，ワープロ，表計算，スケジュール管理，オンラインブックマーク，データ共有等のサービスへの秘密情報の登録，保持を行わないこと。

【禁止例】

・顧客住所を Google マップ（地図サービス）へ登録
・設定ファイルや構成図等の Evernote/GoogleDocs/Skydrive への保存
・現場写真を Flickr(写真データ共有）に保存

別記様式

電子データの保存等に関する届出書

年　　月　　日

（住所）

（名前又は法人名等）

年　月　日付け「（仮称）仙酔島海浜広場の管理に関する基本協定」に係る業務について，業務の遂行において取り扱う電子データの保存先を次のとおり届け出ます。

1　電子データの保存に使用する媒体等の名称 例　USBメモリ，社内PC内ストレージ，外付けハードディスク	
2　電子データを記憶する記録媒体等の物理的な所在地等 例　米国，システム管理に関するログ情報を保管	□　日本国内のみ □　日本国外（全部又は一部） （国名） （日本国外に保存する電子データの概要）
3　クラウドサービス等のオンラインストレージの利用の有無 ※　利用契約先が複数ある場合には，すべて記載してください。	□　有 （利用契約先の情報） ア　サービス名称 イ　利用契約先の名称 ウ　電子データの物理的保存先に係る情報等 □　無
4　委託等の有無 ※　本協定に係る業務に関して電子データの全部又は一部の取扱いを第三者に委託する予定がある場合は「有」としてください（二以上の段階にわたる委託をする場合及び子会社に委託をする場合を含みます。子会社は，会社法（平成17年法律第86号）第２条第１項第３号に規定する子会社をいいます。）。	□　有 （委託先等の名称） （委託先等に委託する具体的な業務内容） □　無

※　今回の届出事項に変更があった場合には，再度届出を行ってください。

【注記事項】

1　電子データの保存状況により，安全管理措置上の問題が生じる場合には，電子データの保存方法について変更を求める場合があります。

2　委託等を行う場合には，あらかじめ指定管理者の書面による承諾を得る必要があります。

3　委託先等がある場合には，当該委託先等もこの届出書を提出する必要があります。