情報セキュリティ対策実施状況調査票に関する説明

情報セキュリティ対策実施状況調査票（以下「調査票」という。）は、市の業務委託を受託する又は受託しようとする事業者（以下「受託者」という。）における情報セキュリティ対策の実施状況の確認を目的としたものです。
市の業務委託を受託するに当たり、本調査票の回答に御協力ください。

1　回答様式に関する説明

調査票（Excel形式）は、次の２つの回答様式（シート）によって構成されています。
・『回答様式①【共通】』
・『回答様式②【ISMS認証等未取得の場合】』

受託する業務（以下「受託業務」という。）の内容及び受託者における情報セキュリティに関する認証等の取得状況に応じて、回答いただくシートが異なります。詳細は、次の（１）及び（２）を参照してください。

（１）シート『回答様式①【共通】』

ア　回答対象者

全ての受託者

イ　設問の概要

受託業務を担当する組織（部署、課等）の基本情報、各種認証等の取得状況、再委託の実施予定の有無、クラウドサービスの利用予定の有無

（２）シート『回答様式②【ISMS認証等未取得の場合】』

ア　回答対象者

次のいずれにも該当しない受託者（※どちらか１つでも満たしている場合には回答不要）
（ア）受託業務を担当する組織が、情報セキュリティマネジメントシステム認証（ISMS認証）を取得している場合
（イ）受託業務で取り扱う機密性の高い情報が個人情報のみに限定される場合であって、受託者が「プライバシーマーク」を取得している場合

イ　設問の概要

受託業務を担当する組織における情報セキュリティ対策の実施状況の詳細
※各設問の詳細については、シート『設問の補足』を参照してください。

ウ　留意事項

・回答が「いいえ」の場合には、その代替策として講じている対策（契約の開始までに講じることが可能な対策を含む）について、D列（代替策・備考等）に記載してください。
・回答が「該当なし」の場合には、その理由について、D列（代替策・備考等）に記載してください。

2　提出方法

提出方法については、本業務委託の発注元の課等が示す方法に従ってください。

回答様式①【共通】

（1）受託者名・担当組織名

受託者の名称及び受託業務を担当する組織の名称（部署名、課名等）を記載してください。

受託者	
担当組織名	

（2）認証取得状況

受託業務を担当する組織（部署、課等）が取得している認証等について回答してください。
※ISMS認証・ISMSクラウドセキュリティ認証・プライバシーマークを取得している場合には、登録証（写し）を併せて提出ください。

情報セキュリティ	□ ISMS認証【ISO/IEC27001】　□ ISMSクラウドセキュリティ認証【ISO/IEC27017】 □ その他　（　）
個人情報保護	□ プライバシーマーク【JIS Q 15001】 □ その他　（　）
その他	※受託業務の遂行に資する認証等を取得している場合には記載してください。

（3）再委託の実施予定

受託業務の一部について、**再委託を行う予定がある場合のみ**回答してください。
※個人情報等の機密性の高い情報（以下「機密情報」という。）を取り扱う業務を再委託する場合が対象です。
※再委託を行う業務が複数ある場合には、業務ごとに回答してください。
なお、回答欄が不足する場合には、行を追加してください。（改ページが発生しても構いません。）

①	再委託先の事業者名	
	再委託を行う業務の内容	
	再委託先における認証等の有無 （情報セキュリティ又は個人情報保護関連）	□ ISMS認証【ISO/IEC27001】　□ プライバシーマーク【JIS Q 15001】 □ その他　（　）

（4）クラウドサービスの利用予定

受託業務を遂行するに当たり、**クラウドサービスを利用する予定がある場合のみ**回答してください。
※クラウドサービス上で、機密情報を取り扱うものが対象です。
※クラウドサービスには、委託業務に特化したサービスの他、メールソフト、グループウェア、オンラインストレージ等も含みます。
なお、クラウドサービスの形態（SaaS・PaaS・IaaS等）については問いません。
※該当するクラウドサービスが複数ある場合には、サービスごとに回答してください。
なお、回答欄が不足する場合には、行を追加してください。（改ページが発生しても構いません。）

①	クラウドサービス名／提供事業者名	／
	クラウドサービスの利用用途	
	クラウドサービス提供事業者における認証等の有無 （情報セキュリティ関連）	□ ISMS認証【ISO/IEC27001】　□ ISMSクラウドセキュリティ認証【ISO/IEC27017】 □ ISMAPクラウドサービスリスト　□ CSマーク □ SOC報告書 □ その他　（　）
②	クラウドサービス名／提供事業者名	／
	クラウドサービスの利用用途	
	クラウドサービス提供事業者における認証等の有無 （情報セキュリティ関連）	□ ISMS認証【ISO/IEC27001】　□ ISMSクラウドセキュリティ認証【ISO/IEC27017】 □ ISMAPクラウドサービスリスト　□ CSマーク □ SOC報告書 □ その他　（　）

回答様式②【ISMS認証等未取得の場合】

受託業務を担当する組織における情報セキュリティ対策の実施状況について、以下の設問に回答してください。
※回答が「いいえ」の場合は、D列に代替策を記載してください。
※回答が「該当なし」の場合は、D列に理由を記載してください。

No	設問	回答	代替策・備考等
1	**情報セキュリティに関する組織的な取組状況**		
1-1	情報セキュリティに関する規程類が整備され、従業員に周知されていますか。	☐ はい ☐ いいえ ☐ 該当なし	
1-2	情報セキュリティに関する体制が整備されていますか。	☐ はい ☐ いいえ ☐ 該当なし	
1-3	従業員に対し、組織の情報セキュリティに関する規程類を遵守する旨（守秘義務等を含む）について書面等により義務付けていますか。	☐ はい ☐ いいえ ☐ 該当なし	
1-4	従業員に対し、情報セキュリティに関する教育は実施していますか。	☐ はい ☐ いいえ ☐ 該当なし	
1-5	従業員が退職等する際、組織が従業員に貸与している資産（パソコン、ICカード等）を回収し、従業員に対し、守秘義務の継続等について書面等により義務付けていますか。	☐ はい ☐ いいえ ☐ 該当なし	
2	**情報資産の取扱い**		
2-1	機密性の高い情報（個人情報等）を含む情報資産（書類、電磁的記録媒体）の取扱い方針は定められていますか。	☐ はい ☐ いいえ ☐ 該当なし	
2-2	取外し可能な電磁的記録媒体の利用について、適切な制限等は行われていますか。	☐ はい ☐ いいえ ☐ 該当なし	
2-3	機密性の高い情報（個人情報等）を含む情報資産の廃棄について、情報が復元できないよう媒体の種別に応じた適切な廃棄が行われていますか。	☐ はい ☐ いいえ ☐ 該当なし	
3	**アクセス制御**		
3-1	機密性の高い情報（個人情報等）を取り扱う情報システムにおいて、利用者の認証及びアクセス権の設定が実施されていますか。	☐ はい ☐ いいえ ☐ 該当なし	
3-2	機密性の高い情報（個人情報等）を取り扱う情報システムにおいて、利用者（利用者ID、管理者ID等）及びアクセス権の定期的な見直しは実施されていますか。	☐ はい ☐ いいえ ☐ 該当なし	
3-3	情報システムの利用者に対し、認証情報（パスワード等）の取扱いに関する注意事項は示されていますか。	☐ はい ☐ いいえ ☐ 該当なし	
4	**物理的及び環境的セキュリティ**		
4-1	機密性の高い情報（個人情報等）等を取り扱う場所（サーバ室、執務エリア等）について、不正侵入等を防止するための措置が講じられていますか。	☐ はい ☐ いいえ ☐ 該当なし	
4-2	重要な情報システム機器を設置する場所（サーバ室等）について、災害等に備えた措置が講じられていますか。	☐ はい ☐ いいえ ☐ 該当なし	
4-3	端末等について、盗難や紛失等の防止策が講じられていますか。	☐ はい ☐ いいえ ☐ 該当なし	
4-4	端末等について、第三者による不正利用に関する防止策が講じられていますか。	☐ はい ☐ いいえ ☐ 該当なし	

5　情報システムの運用			
5-1	マルウェア（コンピュータウィルス等）への対策が実施されていますか。	☐ はい ☐ いいえ ☐ 該当なし	
5-2	情報システムに保存されている重要な情報等について、定期的なバックアップは取得されていますか。	☐ はい ☐ いいえ ☐ 該当なし	
5-3	機密性の高い情報（個人情報等）を取り扱う情報システムについて、情報セキュリティの確保に必要なログは取得されていますか。	☐ はい ☐ いいえ ☐ 該当なし	
5-4	機密性の高い情報（個人情報等）を取り扱う情報システムについて、不正アクセスや不正操作等の有無を、定期的又は必要に応じて点検等を実施していますか。	☐ はい ☐ いいえ ☐ 該当なし	
5-5	情報システムの脆弱性への対策は実施していますか。	☐ はい ☐ いいえ ☐ 該当なし	
6　通信のセキュリティ			
6-1	外部からの不正アクセス等を防止するため、組織のネットワークは適切に管理されていますか。	☐ はい ☐ いいえ ☐ 該当なし	
6-2	電子メール、FAX、WEB会議サービス、オンラインストレージ等の通信手段を用いた情報転送について、通信の盗聴や誤送信等による情報漏えいを防止するための対策を実施していますか。	☐ はい ☐ いいえ ☐ 該当なし	
7　情報セキュリティインシデント管理			
7-1	情報セキュリティインシデントが発生した際の対応手順は定めていますか。	☐ はい ☐ いいえ ☐ 該当なし	
8　監査等			
8-1	情報セキュリティに関する監査等を実施していますか。	☐ はい ☐ いいえ ☐ 該当なし	

設問の補足（回答様式②【ISMS認証等未取得の場合】）

No	設問	設問の補足及び具体例
1	**情報セキュリティに関する組織的な取組状況**	
1-1	情報セキュリティに関する規程類が整備され、従業員に周知されていますか。	＜補足＞ 情報セキュリティに関する規程類とは、受託者における全社的な情報セキュリティ対策の方針を示す規程、個々の情報セキュリティ対策の水準を示す規程等を指しています。
1-2	情報セキュリティに関する体制が整備されていますか。	＜補足＞ 情報セキュリティに関する体制とは、組織として情報セキュリティ対策を推進するための体制や、個々の情報セキュリティ対策に関する役割や責任が整備されている状態を指しています。
1-3	従業員に対し、組織の情報セキュリティに関する規程類を遵守する旨（守秘義務等を含む）について書面等により義務付けていますか。	＜具体例＞ 従業員を雇用する際に、組織の情報セキュリティに関する規程類を遵守する旨の誓約書を取り交わしている。
1-4	従業員に対し、情報セキュリティに関する教育は実施していますか。	＜補足＞ 情報セキュリティに関する教育とは、情報セキュリティに関する注意喚起、意識啓蒙、情報セキュリティ対策の周知徹底等を目的とした研修を指します。 ＜具体例＞ 従業員に対し、eラーニングによる情報セキュリティ研修（情報セキュリティの概要、組織内のルール（情報資産の取扱い方法、マルウェア対策、インシデント発生時の対応等）、注意喚起（流行しているサイバー攻撃の手口等）等を含む研修）を定期的に実施している。
1-5	従業員が退職等する際、組織が従業員に貸与している資産（パソコン、ICカード等）を回収し、従業員に対し、守秘義務の継続等について書面等により義務付けていますか。	＜具体例＞ 従業員が退職する際に、貸与品をすべて回収するとともに、退職後においても守秘義務を遵守する旨の誓約書を取り交わしている。
2	**情報資産の取扱い**	
2-1	機密性の高い情報（個人情報等）を含む情報資産（書類、電磁的記録媒体）の取扱い方法は定められていますか。	＜補足＞ 取扱い方法とは、主に、情報資産の保管、持ち出し、複製、廃棄等における基本的な取扱いの方法を指しています。 ＜具体例＞ 施錠可能な棚での保管、持ち出しの禁止又は制限、複製の禁止又は制限、復元不可とするための廃棄方法等

2-2	取外し可能な電磁的記録媒体の利用について、適切な制限等は行われていますか。	＜補足＞ 取外し可能な電磁的記録媒体とは、電磁的記録媒体のうち、外付けUSBメモリ、外付けハードディスク、CD等の可搬型の媒体を指しています。 ＜具体例＞ 組織の認可外の媒体の利用禁止、媒体持ち出し時の許認可、持ち運び時等における盗難紛失対策、機密性の高い情報のパスワード保護、自動暗号化機能の利用等
2-3	機密性の高い情報（個人情報等）を含む情報資産の廃棄について、情報が復元できないよう媒体の種別に応じた適切な廃棄が行われていますか。	＜補足＞ 媒体の種別とは、主に紙媒体又は電磁的記録媒体を指しています。なお、電磁的記録媒体には、外付けUSBメモリやCD等の他、パソコン等の機器に内蔵されている電磁的記録媒体も含みます。 ＜具体例＞ 紙媒体：シュレッダー、専門事業者による安全な廃棄処理等 電磁的記録媒体：物理的な破壊、磁気消去、データ消去ソフトウェアによる消去等 ※電磁的記録媒体については、単純な初期化（フォーマット）のみでは不適切とされています。
3　アクセス制御		
3-1	機密性の高い情報（個人情報等）を取り扱う情報システムにおいて、利用者の認証及びアクセス権の設定が実施されていますか。	＜補足＞ ・受託業務を遂行するに当たり、受託者の従業員が利用する情報システムが対象です。 ・情報システムには、受託業務に特化した業務アプリケーションの他、メールソフトやグループウェア等も含みます。 なお、情報システムの形態（オンプレミス、クラウドサービス等）は問いません。 ＜具体例＞ （１）利用者の認証の例 ・ID及びパスワードによる認証を行っている。 ・シングルサインオンによる認証を行っている。 （２）アクセス権設定の例 ・顧客管理システム（業務アプリケーション）について、顧客管理部門の者のみがアクセスできるように制御している。 ・ファイルサーバについて、営業部のフォルダは、営業部門の者のみが閲覧できるように制御している。 ・グループウェアについて、システムの管理機能は、管理権限を有する利用者のみが利用できるように制御している。
3-2	機密性の高い情報（個人情報等）を取り扱う情報システムにおいて、利用者（利用者ID、管理者ID等）及びアクセス権の定期的な見直しは実施されていますか。	＜補足＞ ・受託業務を遂行するに当たり、受託者の従業員が利用する情報システムが対象です。 ・情報システムには、受託業務に特化した業務アプリケーションの他、メールソフトやグループウェア等も含みます。 なお、情報システムの形態（オンプレミス、クラウドサービス等）は問いません。 ＜具体例＞ ・従業員の退職に応じて、利用者IDの削除を行っている。 ・従業員の異動に応じて、異動前の所属の情報システムへのアクセス権を削除している。

3-3	情報システムの利用者に対し、認証情報（パスワード等）の取扱いに関する注意事項は示されていますか。	＜具体例＞ 安全な（推測されにくい）パスワードの利用、他者との共有の禁止、パスワードの使いまわしの禁止等
4　物理的及び環境的セキュリティ		
4-1	機密性の高い情報（個人情報等）等を取り扱う場所（サーバ室、執務エリア等）について、不正侵入等を防止するための措置が講じられていますか。	＜具体例＞ 施錠管理、入退管理（訪問者の入退記録、認可された者以外の立ち入り制限、機器の持ち込み制限等）、監視設備の設置等
4-2	重要な情報システム機器を設置する場所（サーバ室等）について、災害等に備えた措置が講じられていますか。	＜補足＞ 重要な情報システム機器とは、受託業務を遂行する上で基幹的な役割を担う情報システムを構成する機器（サーバ機器、ネットワーク機器等）のことを指します。 ＜具体例＞ 耐震、防火、防水等に関する措置、予備電源の設置、ケーブル配線の保護等
4-3	端末等について、盗難や紛失等の防止策が講じられていますか。	＜補足＞ 受託業務を遂行するに当たり、受託者の従業員が利用する端末（PC、タブレット、スマートフォン等）や電磁的記録媒体等が対象です。 ＜具体例＞ ・据え置きの端末は、セキュリティワイヤーによる固定等を行う。 ・モバイル端末、電磁的記録媒体は、使用時以外の施錠保管等を行う。
4-4	端末等について、第三者による不正利用に関する防止策が講じられていますか。	＜補足＞ 受託業務を遂行するに当たり、受託者の従業員が利用する端末（PC、タブレット、スマートフォン等）や電磁的記録媒体等が対象です。 ＜具体例＞ ・離席時のログオフ、画面ロックの徹底 ・退勤時等における施錠管理 ・クリアデスク・クリアスクリーンの徹底
5　情報システムの運用		
5-1	マルウェア（コンピュータウィルス等）への対策が実施されていますか。	＜補足＞ 受託業務を遂行するに当たり、受託者の従業員が利用する情報システム（端末等も含む）が対象です。 ＜具体例＞ ・マルウェア対策ソフトの導入及び適切な運用（定義ファイルの最新化） ・マルウェア感染に係るリスクや感染時の対応手順に関する従業員への周知

5-2	情報システムに保存されている重要な情報等について、定期的なバックアップは取得されていますか。	＜補足＞ 受託業務を遂行するに当たり、受託者の従業員が利用する情報システム（端末等も含む）が対象です。 ＜具体例＞ ・業務アプリケーションのデータベースについて、日次でバックアップを取得し、外付けHDDへ保存している。 ・ファイルサーバ上に保存されているデータについて、週次でバックアップを取得し、LTOテープへ保存している。 ・端末のみに保存されているデータについて、定期的にバックアップを取得し、メディア（CD等）に保存している。
5-3	機密性の高い情報（個人情報等）を取り扱う情報システムについて、情報セキュリティの確保に必要なログは取得されていますか。	＜補足＞ ・受託業務を遂行するに当たり、受託者の従業員が利用する情報システム（端末等も含む）が対象です。 ・情報セキュリティの確保に必要なログとは、主に、不正アクセスや不正操作の検知、情報セキュリティインシデント発生時における調査等に有用な情報を記録しているログを指しています。 ＜具体例＞ 認証ログ、アクセスログ、システム稼動ログ、障害時のシステム出力ログ等
5-4	機密性の高い情報（個人情報等）を取り扱う情報システムについて、不正アクセスや不正操作等の有無を、定期的又は必要に応じて点検等を実施していますか。	＜補足＞ 受託業務を遂行するに当たり、受託者の従業員が利用する情報システム（端末等も含む）が対象です。 ＜具体例＞ 取得したログ（前項のログ）から不正アクセス等の有無を確認する
5-5	情報システムの脆弱性への対策は実施していますか。	＜補足＞ 受託業務を遂行するに当たり、受託者の従業員が利用する情報システム（端末等も含む）が対象です。 ＜具体例＞ 脆弱性情報の収集、脆弱性に関する修正プログラム又は回避策の適用等
6　通信のセキュリティ		
6-1	外部からの不正アクセス等を防止するため、組織のネットワークは適切に管理されていますか。	＜補足＞ 受託業務を遂行するに当たり、受託者の従業員が利用する情報システム（端末等も含む）が属するネットワークが対象です。 ＜具体例＞ ネットワークの分離、ファイアウォール等による経路制御、不審な通信の監視、ネットワークに接続する端末の認証等

6-2	電子メール、FAX、WEB会議サービス、オンラインストレージ等の通信手段を用いた情報転送について、通信の盗聴や誤送信等による情報漏えいを防止するための対策を実施していますか。	＜補足＞ 受託業務を遂行するに当たり、受託者の従業員が利用する通信手段が対象です。 ＜具体例＞ 電子メール：メール暗号化、添付ファイルのパスワード保護 FAX：誤送信対策（送信前のダブルチェック等） WEB会議：第三者の不正参加防止策、WEB会議に係る通信の暗号化 オンラインストレージ：共有範囲の適切な設定方法
7　情報セキュリティインシデント管理		
7-1	情報セキュリティインシデントが発生した際の対応手順は定めていますか。	＜補足＞ 情報セキュリティインシデントとは、情報漏えいや情報システム障害等を指します。 ＜具体例＞ インシデント発生時の報告（報告先、連絡手段等）、初動対応（証拠保全、影響の拡大防止）、再発防止等を含む対応手順
8　監査等		
8-1	情報セキュリティに関する監査等を実施していますか。	＜補足＞ 情報セキュリティに関する監査等とは、情報セキュリティに関する規程類に基づいて情報セキュリティ対策が適切に実施されているかどうかの確認を目的としたものです。 ＜具体例＞ ・組織内の監査部門による内部監査 ・外部の専門家による情報システムの脆弱性診断 ・各部門におけるセルフチェック