外部委託利用実施手順

令和元年 6 月 1 日　企画部長決定

第1. 趣旨

本「外部委託利用実施手順」は、品川区（以下、「区」という）のシステムの開発・運用管理・保守業務にかかる外部委託において適正な選定と契約を実施するため、必要な事項を定める。

第2. 定義

1. 用語

本「外部委託利用実施手順」における用語の定義は、「情報セキュリティ基本方針」および「情報セキュリティ対策基準」に定めるもののほか、次のとおりとする。

(1) クラウドサービス

クラウドサービスとは、コンピュータ上で利用するソフトウェアやデータをインターネット上で提供するサービスのことである。これにより利用者は、設備を整えることなくサービスを利用することで様々なコンピュータシステムを利用することができる。

(2) SaaS

クラウドサービス形態の一つで、ハードウェア環境からアプリケーションまでのサービスを提供する

(3) PaaS

クラウドサービス形態の一つで、ハードウェアから開発環境までのサービスを提供する。

(4) IaaS

クラウドサービス形態の一つで、ハードウェアから OS までのサービスを提供する。

(5) DaaS

クラウドサービス形態の一つで、デスクトップサービスを提供する。

(6) TLS

Transport Layer Security の略で、web サーバと web クライアント間において暗号化などを含む通信の安全を保つための IT 技術である。

※　SSL との互換性はない。

(7) VPN

WAN などの遠隔通信において、汎用的な回線を仮想的に専用線として利用する IT 技術である。

(8) データセンタ（DC、IDC）

コンピュータシステムのサーバを設置するための専用設備サービスである。耐震、消火、電源、監視、セキュリティ等の設備が整っている。

通常はデータセンタを DC（Data Center）といい、インターネットに特化したものを IDC（Internet Data Center）という。

第3. 役割における職務

1. 情報セキュリティ管理者の職務

(1) 情報セキュリティ管理者は、ネットワークおよび情報システムの開発・保守等を外部委託事業者に発注する場合、外部委託事業者から再委託を受ける事業者も含めて、情報セキュリティポリシー等のうち外部委託事業者が守るべき内容の遵守およびその機密事項を説明しなければならない。

(2) 情報セキュリティ管理者は、外部委託により情報システムを運用する際には、情報管理安全対策について特に厳重な配慮をしたうえで、契約の相手方と管理体制、管理責任者および緊急連絡等について定めなければならない。

(3) 情報セキュリティ管理者は、特権を付与された ID およびパスワードの変更について、外部委託事業者に行わせてはならない。

(4)　情報セキュリティ管理者は、外部委託事業者の選定にあたり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

第4. 外部委託要件

1. リスク対策

委託業務においては、その可用性のみならず、以下に例示するリスクを考慮に入れ、その対策を施さなくてはならない。

(1)　外部委託事業者の過失もしくは悪意によって、区の情報資産が外部へ漏えいすること。
(2)　外部委託事業者が業務を再委託することによって、再委託先の事業者から区の情報資産が外部へ漏えいすること。
(3)　外部委託事業者の経営不振等により、区の情報資産が保存されている機器が債権者に差し押さえられるなどして、情報資産が外部に漏えいすること。
(4)　導入したシステムのＯＳ、ミドルウェアおよびアプリケーションのセキュリティホールが放置され情報セキュリティにかかる事件・事故が発生すること。
(5)　システム移行作業時およびシステム運用時の事故によるシステムダウンにより業務が停止すること。

2. 委託業務仕様の要件

委託業務仕様書に以下の要件を記載すること。

(1)　システムもしくは委託業務の目的
(2)　システムもしくは委託業務の方針
(3)　システムの開発を行う場所
(4)　システム開発の責任者および作業者
(5)　作業スケジュール
(6)　開発用ＩＤの管理方法
(7)　ウイルス対策

3. 開発の委託

情報システムの開発を外部委託業者に委託する場合、以下の項目について明確にしておくこと。

(1)　開発する情報システムの目的
(2)　開始時期
(3)　完成時期と本稼動時期
(4)　テスト期間
(5)　本稼動時の立会いと本稼動サポートの期間
(6)　担当者を明確にし、責任者とその連絡先
(7)　緊急時の連絡網

4. 運用管理の委託

情報システムの運用管理を外部委託業者に委託する場合、以下の項目について明確にしておくこと。

(1)　対象システム
(2)　運用管理の期間
(3)　運用管理の具体的な作業内容
(4)　定期的な作業と非定期な作業
(5)　作業報告（操作報告）の記録と提出方法
(6)　常駐の有無
(7)　担当者を明確にし、責任者とその連絡先
(8)　緊急時の連絡網

5. 保守業務の委託

情報システムの保守業務を外部委託業者に委託する場合、以下の項目について明確にしておくこと。

(1) 対象システム
(2) 保守業務の期間
(3) 保守業務の具体的な作業内容
(4) 担当者を明確にし、責任者とその連絡先
(5) 緊急時の連絡網

6. クラウドサービスの利用

情報システムをクラウドサービスで利用する場合、以下の項目について明確にしておくこと。

(1) クラウドの種類（SaaS 等）
(2) 情報システムの重要性（機密性、完全性、可用性）
(3) クラウドで利用する業務、あるいは業務内の範囲
(4) 業務とサービス内容に見合ったコスト
(5) クラウドで取り扱うデータの重要性分類
(6) 業務およびクラウドサービスの特性を理解した管理者
(7) クラウドサービスとの接続方法

7. 契約の要件

情報システムの開発、運用、保守等を外部委託する場合には、外部委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。

(1) 報告義務に関して次に例示する条項を明記した契約を締結する。
「乙は、この契約を締結し業務を遂行するにあたり甲の所掌する情報資産の重要性を維持し、甲の求めにより遵守内容を報告しなければならない。」
(2) 組織体制に関し次に例示する条項を明記した契約を締結する。
「乙は、業務を受託し責務を有する乙の組織体制を明確にし、甲に報告しなければならない。」
(3) 守秘義務に関し次に例示する条項を明記した契約を締結する。
「乙は、業務の処理上知り得た情報を第三者に漏らしてはならない。この契約を終了した後においても同様とする。なお、業務を再委託した場合においても再委託受託者に同様の責務を課す。」
(4) 情報の目的外利用に関し次に例示する条項を明記した契約を締結する。
「乙は、業務の処理に必要なため提供を受けた情報は、目的外利用および受託者以外の者への提供を禁止する。なお、業務を再委託した場合においても再委託受託者に同様の責務を課す。」
(5) 情報の返還義務に関し次に例示する条項を明記した契約を締結する。
「乙は、業務の処理に必要なため記録媒体、印刷物等で提供を受けた情報は、業務終了後、直ちに甲に返還するものとする。なお、業務を再委託した場合においても再委託受託者に同様の責務を課す。」
(6) 損害賠償に関して次に例示する条項を明記した契約を締結する。
「業務の処理に関し乙の責めに帰する事由による損害が発生した場合は、損害のため必要を生じた経費を乙が負担するものとする。なお、経費の算出については甲乙協議のうえ決定するものとする。」

第5. 外部委託選定基準

1. 外部委託選定基準について

　外部委託選定基準については、情報システムの目的、取り扱うデータの重要性と完全性、情報システムの可用性を考慮し、重要性分類に基づいた、別紙「外部委託利用基準」において基準を満たしているか判断すること。

2. 外部委託選定基準表

　別紙「外部委託利用基準」を参照のこと。

第6. 情報セキュリティポリシーの遵守状況の確認

　外部委託事業者に委託している場合、情報セキュリティ監査統括責任者は外部委託事業者から再委託している事業者も含めて、情報セキュリティポリシーの遵守について監査を定期的にまたは必要に応じて行わなければならない。

付則

この実施手順は、令和元年 6 月 1 日から適用する。

【外部委託利用基準】

2019/6/1

【指針】
本基準は、情報システムの開発、運用及び保守等の外部委託する場合に、情報資産の共分な設備力を持ち、情報セキュリティに係る事件、事故等の発生を防止して責任と義務を適正に遂行するための基準や事項を定める。

番号	項目	重要性分類Ⅰ										重要性分類Ⅱ（Ⅰ及びⅢ以外に該当する情報）										重要性分類Ⅲ									
		保有する情報の分類										保有する情報の分類										保有する情報の分類									
		情報システムの運用・保守・点検										情報システムの運用・保守・点検										情報システムの運用・保守・点検									
		情報システムの	オンサイトサポート	リモートビス運用	データセンター	Daas	Saas	Paas	Iaas	情報の暗号化	情報の廃棄・破壊	情報システムの	オンサイトサポート	リモートビス運用	データセンター	Daas	Saas	Paas	Iaas	情報の暗号化	情報の廃棄・破壊	情報システムの	オンサイトサポート	リモートビス運用	データセンター	Daas	Saas	Paas	Iaas	情報の暗号化	情報の廃棄・破壊
1. 施設要件																															
1－1. 立地要件																															
1	日本国内に施設を持つこと。	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○
2	隣接建物から延焼防止のために充分な距離が保たれているか、または延焼防止が建物に施されていること。	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○
3	建物は、水の被害を受ける可能性が低い地域に設けること。	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○
4	データセンター内の周囲半径 100 メートル以内に消防法による指定数以上の危険物製造設備、火薬製造設備、高圧ガス設備が無いこと。	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○
1－2. 建物要件																															
1	建物は、ビルの耐震基準（関連法規）を満たし、震度6強の地震でも致命的な被害を受けない耐震性能を有すること。	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○
2	JEC2374規格に準拠しているか、または同等の規格に準拠した避雷設備を有すること。	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○
3	駐車スペースが十分に確保されていること。	－	－	－	○	－	－	－	－	－	－	－	－	－	○	－	－	－	－	－	－	－	－	－	○	－	－	－	－	－	－
4	コンピュータ室（サーバ室）について、不燃材が使用されていること。	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○
5	**物理的アクセス制御**																														
1	サーバ室等の管理区域の出入り口は、不特定多数の者が利用できる出入り口でないこと。	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○
2	建物の出入り口は、不特定多数の者が利用できる出入り口でないこと。	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○
3	建物の敷地は、不特定多数の者が利用できる出入り口でないことが望ましい。	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○
2. 設備要件																															
2－1. 電源設備等																															
1	電力会社より安定的に電力供給されていること。	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○
2	サーバエリア電源容量、その他運用する機器の電源容量、施設・設備電源容量等が十分に確保していること。また、将来の収容計画に耐える電源容量を有すること。	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○	－	－	－	－	－	－	－	－	－	－
3	法定点検や工事等の際にも電力の供給を止めることなく電力を供給できる冗長構成を有すること。	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－
4	停電時に自家発電設備が起動し安定した電力の供給ができるまでの間、無停電電源装置等による安定した電源供給ができること。	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－
5	非常用に自家発電設備を設け、サーバエリアの電源容量、その他運用する機器の電源容量、施設設備電源容量以上の電源容量について、24時間以上の稼動が対応可能なこと。	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－
6	自家発電設備は、商用電力の供給が止まった場合でも、停止から1分以内にこの間はUPSから電力供給）に電力が供給できること。更に、自家発電設備は、無給油で72 時間以上連続運転可能であること。もしくは、それに代わる代替措置が採られていること。	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－
7	瞬停（サグ）、電圧降下（ブラウンアウト）、突入電流、サージ（過圧）等の電源トラブル対策を講じていること。	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－
8	優先的に燃料供給が受けられる契約を燃料供給会社と結んでいること。	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－
9	発電機の故障、保守時の対応手段を有すること。	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－
10	ケーブルのつまずき、引っかけを防止する対策が講じられていること。	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○
2－2. サーバ室																															
1	サーバ室の床強度は、情報システム機器等の総重量に耐える強度を有していること。（ラックエリアは500kg/ ㎡以上の床面耐荷重を有すること。）	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－
2	サーバ室は、温湿度環境を維持できる天井高を確保していること。	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－
3	サーバ及びラック台数から十分なスペースを用意すること。	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－
4	空調は24 時間365 日の連続運転が可能なこと。	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－
5	ラック外の周囲の温度と湿度を適正に保ち、振動作せず、かつ四季を問わず結露の発生しない設定温度、適正湿度を維持できること。	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－
6	温度、湿度は機器等の安定稼動に影響を及ぼさないように、機器仕様であめられる温度、湿度に保たれていること。	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－
7	局所的熱溜まりを発生させないこと。	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－
8	増加するIT機器の発熱量に対応できること。	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－
9	空調設備の集中監視が可能であること。	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－
10	故障による代替空調が可能であること。	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－
11	空調機排水周りの水漏れ検知を行うこと。	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－
12	複数の監視カラシて 目視監視可能であること。	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－
2－3. ラック設備																															
1	ラック搭載型の機器搭載が可能な内寸であること。	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－
2	EIA規格準拠19インチラック、42U以上であること。また 角穴の19インチレールが望ましい。	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－
3	サーバが稼動適温に保たれる構造であること。（ラック開口、冷却装置の装着、等）	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－
4	排気指標が起こらないラックであること。	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－
5	背面のケーブルがサーバの排気を妨げない仕組みを持つこと。	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－
6	ラック搭載型でない機器等をラックに搭載できる棚板を使用できること。またその重量に耐える棚板であること。	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－
7	ラックは施錠ができ、サービス利用者または許可されたものから申し出がない限り開錠できないよう管理ができること。	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○
8	ラック施錠の管理方法について、鍵管理手順書を備えていること。	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○
9	不意なラック同士の接触で倒れることを防止する対策が施されていること。	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－
10	ラックに実装した機器を保護するため、揺れ軽減の機能を有していること。	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－
2－4. 防火設備																															
1	延焼防止システムを有すること。	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－
2	火災予兆検知システムを有すること。	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○
3	ガス系（窒素等）消火設備を有すること。	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○
4	火災を自動的に検出する熱感知器、煙検知器等とともに自動または手動通報設備を備えていること。	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○
5	非常放送設備、防火防排煙設備、各種消火設備が連動していること。	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○	－	－	－	－	－	－	－	－	－	－
6	消火設備の集中監視が可能であること。	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－	－	－	－	－	－	－	－	－	－	－
2－5. 防水設備																															
1	サーバ室及びデータ等保管設備は水の被害を受けない場所に設置すること。	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○
2	台風、高波、洪水などの水害に対し対処できる構造・設備を有すること。	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○
2－7. 防犯設備																															
1	入退者を識別・記録できるセキュリティ設備（ICカード等）により許可された者のみ入退室が可能なこと。さらにサーバ室への入室は、バイオメトリックス認証システム等を採用していること。	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○
2	入退室をする全ての委託業者について、氏名管理を行うこと。また、区の求めに応じて入退室名簿を迅速に提出できる運用を実施していること。	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○
3	施設内の電源設備、空気調和設備、セキュリティ設備等は、常時故障監視がされているとともに巡回監視が実施されていること。	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－	－	－	－	－	－	－	－	－	－	－
4	入室可能時間は、24時間365日であること。	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－	－	－	－	－	－	－	－	－	－	－
5	モニタ監査は、24時間365日であること。	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－	－	－	－	－	－	－	－	－	－	－
6	カメラ等映像機器による監視を実施していること。	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○
7	入室ドアそのものが容易に破壊されないような対策、窓などよする等外部から容易に見通せない対策が施されていること。	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○
8	扉付近に開閉の妨げになるようなものを設置しないこと。	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○
9	防犯設備導入を行い、出入口等の常時監視を行っていること。	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○
10	入退室時における入退室者の資格確認ができること。	－	－	○	○	○	○	○	○	○	○	－	－	○	○	○	○	○	○	○	○	－	－	○	○	○	○	○	○	○	○
11	入退室は全ての状況の記録が取れていること。	－	－	○	○	○	○	○	○	○	○	－	－	○	○	○	○	○	○	○	○	－	－	○	○	○	○	○	○	○	○
12	入館者の事前登録が行われること。	－	－	○	○	○	○	○	○	○	○	－	－	○	○	○	○	○	○	○	○	－	－	○	○	○	○	○	○	○	○
3. 情報セキュリティ確保するための体制の整備																															
1	情報セキュリティ基本方針を区に明示すること。	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
2	業務の従事者に対し、情報安全対策及び個人情報の保護の徹底について周知すること。	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
3	区から提供された情報について管理責任者を明確にすること。	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
4. 取り扱う情報の保管段階等																															
1	業務上知り得た情報について、目的外の利用及び第三者への開示・提供をしないこと。 なお、業務終了後も同様とする。	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
2	個人情報等の機密性の高い情報の搬送時には、暗号化等の技術を活用し、盗難、不正コピー等の防止対策を実施すること。	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
3	個人情報等の機密性の高い情報が格納された機器を修理もしくは廃棄する場合は、復元できない方法で確実に情報を消去すること。	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
4	開発、運用、保守等の際の従事者ごとの作業場所、業務領域、アクセス制限の取り決めを行うこと。	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
5	区が管理するサーバ室等の管理区域へ入退室する場合は、入退室管理簿の記入等、区の定めた手続に従い承認を得ること。	○	○	－	－	－	－	－	－	○	○	○	○	－	－	－	－	－	－	－	○	○	○	－	－	－	－	－	－	○	○
6	区で管理する情報システムを取り扱う場合は、区で付与した（あるいは承認した）利用者ID、パスワード等を使用すること。	○	○	○	○	○	○	○	○	－	－	○	○	○	○	○	○	○	○	－	－	○	○	○	－	－	－	－	－	－	－
7	区の情報資産を外部に持ち出す場合は、事前に区の承認を得ること。	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
8	業務終了時等に、区から提供された情報は速やかに区に返還すること。	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
9	業務終了時等に区から提供された情報の返却後は、当該情報を復元不可能な方法で確実に削除又は廃棄し、削除又は廃棄した旨の証明書を提出すること。	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
5. セキュリティ侵害の防御																															
1	個人情報等の機密性の高い情報を、インターネットに接続している外部サーバ等の公開領域に保管してはならない。 また、当該情報を保管するデータベース等は、セキュリティ機器で外部からの技術的攻撃を防御する設置により、分離したネットワークに設置すること。	○	－	－	○	○	○	○	○	○	○	○	－	－	○	○	○	○	○	○	○	○	－	－	－	－	－	－	○	○	－	－
2	区の情報資産への不正なアクセスを防止するため、使用する記録媒体を制限すること。	○	－	－	○	○	○	○	○	○	○	○	－	－	○	○	○	○	○	○	○	○	－	－	○	○	○	○	○	○	○	○
3	入館時に持込む機器、外部記録媒体、紙媒体が制限されていること。	○	－	○	○	○	○	○	○	○	○	○	－	○	○	○	○	○	○	○	○	○	－	○	○	○	○	○	○	○	○
4	外部委託業務において、第三者が提供するサービスのうち区の情報セキュリティ管理に影響のあるものについては開示すること。	○	－	－	○	○	○	○	○	○	○	○	－	－	○	○	○	○	○	○	○	○	－	－	○	○	○	○	○	○	○	○
5	クラウドサービス等で取得する利用者の活動、例外処理及びセキュリティ事象等を記録したログを区に提供すること。	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－
6	クラウドサービス等で取得するシステム運用に関するログを区に提供すること。	－	－	－	○	○	○	○	－	－	－	－	－	－	○	○	○	○	－	－	－	－	－	－	○	○	○	○	○	－	－
7	ログの改ざん防止措置を講じること。	－	－	－	○	○	○	○	－	－	－	－	－	－	○	○	○	○	－	－	－	－	－	－	○	○	○	○	○	－	－
8	全ての情報処理システム内のクロックは、正確な時刻源と同期させること。	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－	－	－	－	○	○	○	○	○	－	－
9	ウイルス対策は常に最新ソフトウェアのバージョン、定義ファイルを維持し、検知されたウイルスは自動的に隔離し駆除すること。	○	－	○	○	○	○	－	－	－	－	○	－	○	○	○	○	－	－	－	－	○	－	○	○	○	○	－	－	－	－
10	外部からのクラウドサービス等への接続方法に応じた認証方法（ID、パスワード等）を区に提供すること。	－	－	－	○	○	○	○	－	－	－	－	－	－	○	○	○	○	－	－	－	－	－	－	○	○	○	○	－	－	－
11	サーバ等の配置において、特定の場所及び装置からの接続を認証するための手段として、自動の装置識別を考慮すること。	－	－	－	○	○	○	○	－	－	－	－	－	－	○	○	○	○	－	－	－	－	－	－	○	○	○	○	－	－	－
12	アプリケーションの技術的ぜい弱性対応については、適切かつ時機を失しない処置をとること。	－	－	－	○	○	○	○	－	－	－	－	－	－	○	○	○	○	－	－	－	－	－	－	○	○	○	○	－	－	－
13	サーバ等のOSの技術的ぜい弱性対応については、適切かつ時機を失しない処置をとること。	－	－	－	○	○	○	○	－	－	－	－	－	－	○	○	○	○	－	－	－	－	－	－	○	○	○	○	－	－	－
14	サーバ等のOSについては、利用開始時に最新のバージョンを提供すること。	－	－	－	○	－	－	○	－	－	－	－	－	－	○	－	－	○	－	－	－	－	－	－	○	－	－	○	－	－	－
15	サービスの死活状態を監視し、サービス停止を早期に検知すること。	－	－	－	○	○	○	－	－	－	－	－	－	－	○	○	○	－	－	－	－	－	－	－	○	○	○	－	－	－	－
16	データベースの暗号化対応を行うこと。及び暗号化内容を明確にすること。	－	－	－	○	○	○	○	－	－	－	－	－	－	○	○	○	○	－	－	－	－	－	－	○	○	○	○	－	－	－
6. ネットワーク																															

【指針】
本基準は、情報システムの調達、運用及び廃棄等が情報保存する場合に、情報資全対策の充分な技術力を持ち、情報セキュリティに係る事件、事故等の発生を防止して委託した業務を正常に遂行するため必要な事項を定める。

		委託する段階の分類										委託する段階の分類										委託する段階の分類									
		情報システムの調達・設等・点検										情報システムの調達・設等・点検										情報システムの調達・設等・点検									
		情報システムの開発等	オンサイトサービス	リモートサービス型	データセンター	Daas	Saas	Paas	Iaas	情報の加工・編集	情報の保存・管理	情報システムの開発等	オンサイトサービス	リモートサービス型	データセンター	Daas	Saas	Paas	Iaas	情報の加工・編集	情報の保存・管理	情報システムの開発等	オンサイトサービス	リモートサービス型	データセンター	Daas	Saas	Paas	Iaas	情報の加工・編集	情報の保存・管理
1	不正なプログラム等による攻撃を防止するための検知機能を有すること。検知された場合は、内部を遮断し、改ざんが確認されたものは正しい内容に復元すること。	○	-	-	○	○	○	○	○	-	-	○	-	-	○	○	○	○	○	-	-	○	-	-	○	○	○	○	○	-	-
2	クラウドサービス等の利用中に、一定の使用中断時間が経過したときは、使用が中断しているセッションを遮断する機能を提供すること。	-	-	-	○	○	○	○	○	-	-	-	-	-	○	○	○	○	○	-	-	-	-	-	○	○	○	○	○	-	-
3	クラウドサービス等の提供において区民が利用する機能はHTTPS（TLS1.2以上）の仕組み により、通信路が保護されていること。	-	-	-	○	○	○	○	○	-	-	-	-	-	○	○	○	○	○	-	-	-	-	-	○	○	○	○	○	-	-
4	クラウドサービス等の提供において利用するブラウザは、「Internet Explorer」もしくは「Chrome」とする。	-	-	-	○	○	○	○	○	-	-	-	-	-	○	○	○	○	○	-	-	-	-	-	○	○	○	○	○	-	-
5	クラウドサービス等の提供において利用する端末に、アプリケーションのインストールを行う必要がないこと。	-	-	-	○	○	○	○	○	-	-	-	-	-	○	○	○	○	○	-	-	-	-	-	○	○	○	○	○	-	-
6	**情報機器のネットワークセキュリティ**																														
1	クラウドサービス等の提供においてHTTPS（TLS1.2以上）の仕組み により、通信路が保護されていること。 ただし、項番6-キ-2、6-キ-3もしくは6-キ-4の対策が実施されている場合はこの限りではない。	-	-	-	○	○	○	○	○	-	-	-	-	-	○	○	○	○	○	-	-	-	-	-	○	○	○	○	○	-	-
2	クラウドサービス等の提供において区が利用する管理機能は、HTTPS（TLS1.2以上）の仕組みにより通信路が保護され、かつグローバルIPアドレスによりアクセスが制限されていること。 ただし、項番6-キ-3もしくは6-キ-4の対策が実施されている場合はこの限りではない。	-	-	-	○	○	○	○	○	-	-	-	-	-	○	○	○	○	○	-	-	-	-	-	○	○	○	○	○	-	-
3	クラウドサービス等の提供においてVPN等 により、通信路が保護されていること。 ただし、項番6-キ-4の対策が実施されている場合はこの限りではない。	-	-	-	-	○	○	○	○	-	-	-	-	-	-	○	○	○	○	-	-	-	-	-	-	○	○	○	○	-	-
4	クラウドサービス等の提供において専用線により、通信路が保護されていること。 ※ベンダー提供による閉域回線も専用線として取り扱う。VPNなどの併用も同様とする。	-	-	-	○	○	○	○	○	-	-	-	-	-	○	○	○	○	○	-	-	-	-	-	○	○	○	○	○	-	-
7. 運用、保守及び点検における情報セキュリティ対策の実施																															
1	開発、運用及び保守等の定期的報告を行うこと。	○	○	○	○	○	○	○	○	○	-	○	○	○	○	○	○	○	○	○	-	○	○	○	○	○	○	○	○	○	○	-
2	サポート窓口を明確にし、開示すること。	-	○	○	○	○	○	○	○	○	○	-	○	○	○	○	○	○	○	○	○	-	○	○	○	○	○	○	○	○	○	○
3	保守計画（障害対応やメンテナンス作業等）を管理し、区に提示すること。	-	○	○	○	○	○	○	○	○	-	-	○	○	○	○	○	○	○	○	-	-	○	○	○	○	○	○	○	○	-
4	操作手順は、文書化し、最新の状態に維持すること。また、その手順は、必要とする全ての利用者に対して利用可能とすること。	-	-	-	○	○	○	○	○	-	-	-	-	-	○	○	○	○	○	-	-	-	-	-	○	○	○	○	○	-	-
5	クラウドサービス等の情報処理設備及び情報システムの変更において、区に影響を及ぼすものは、区に事前に通知すること。	-	-	-	○	○	○	○	○	-	-	-	-	-	○	○	○	○	○	-	-	-	-	-	○	○	○	○	○	-	-
6	クラウドサービス等において、区に割り当てられる容量・能力の限界値を開示すること。 また、区が資源の利用を監視・調整する仕組みを提供し、資源の利用率などを明示すること。	-	-	-	○	○	○	-	-	-	-	-	-	-	○	○	○	○	-	-	-	-	-	-	○	○	○	○	-	-	-
7	定期的な外部保管データバックアップについては、策定された仕様に基づき、バックアップをとること。その際は個人情報等の機密性の高い情報の保護を行うこと。	-	-	-	○	○	○	○	○	-	-	-	-	-	○	○	○	○	○	-	-	-	-	-	○	○	○	○	○	-	-
8	区が求める情報等について、区がバックアップ手順を策定できるように情報を提供すること。	-	-	-	○	○	○	○	○	-	-	-	-	-	○	○	○	○	○	-	-	-	-	-	○	○	○	○	○	-	-
9	クラウドサービス等の利用者ID の登録・削除等のアクセス制御機能を区に提供し、利用者ごとに利用者IDとパスワードを登録することができるようにすること。	-	-	-	○	○	○	-	-	-	-	-	-	-	○	○	○	-	-	-	-	-	-	-	○	○	○	-	-	-	-
10	クラウドサービス等の特権の割当て及び利用を制限し、管理する機能を区に提供すること。	-	-	-	○	○	○	○	○	-	-	-	-	-	○	○	○	○	○	-	-	-	-	-	○	○	○	○	○	-	-
11	開発及び運用において、運用環境とテスト環境を分離すること。	○	-	-	○	○	○	○	○	-	-	○	-	-	○	○	○	○	○	-	-	○	-	-	○	○	○	○	○	-	-
12	運用内容を変更する際には、原則としてテスト実施及び検証結果を事前に区へ報告し、確認を得ること。	-	-	-	○	○	○	○	○	○	-	-	-	-	○	○	○	○	○	○	-	-	-	-	○	○	○	○	○	○	-
13	外部でテストをする際は、実施及び検証のテスト データに重要性分類 I の実在データが含まれていないこと。	○	-	-	○	○	○	-	-	○	-	○	-	-	○	○	-	-	○	-	-	○	-	-	-	-	-	-	○	○	-
14	情報システムの変更が行われた際には変更履歴を区に明示すること。	○	-	-	○	○	○	-	-	-	-	○	-	-	○	○	○	-	-	-	-	○	-	-	○	○	○	-	-	-	-
15	システムを利用することができる動作環境に変更が生じる場合は、あらかじめ区に通知すること。	○	-	-	○	○	○	○	○	-	-	○	-	-	○	○	○	○	○	-	-	○	-	-	○	○	○	○	○	-	-
16	機器を区に持ち込む場合は、事前で目的、期間、作業内容、責任者、機器及びソフトの内容を明確にして、区の承認を得ること。 持ち込んだ機器については、次の措置を行うものとする。 (ア) 使用する記録媒体を含め、ウイルス対策ソフトの最新の定義ファイルにて問題がないことを確認した旨の証明書類を提出すること。 (イ) パソコンの無線LANの機能は停止すること。 (ウ) 区のネットワークを利用したインターネット接続は禁止とすること。 (エ) 施業等により常ご者に開発、盗聴されたことのないようにすること。 (オ) 外部の回線に接続した状態の機器を区の機器に接続しないこと。	○	○	-	○	-	-	-	-	-	-	○	○	-	○	-	-	-	-	-	-	○	○	-	○	-	-	-	-	-	-
17	障害発生連絡から30分以内で現場に到着すること。	-	○	-	-	-	-	-	-	-	-	-	○	-	-	-	-	-	-	-	-	-	○	-	-	-	-	-	-	-	-
18	サービスが停止しない仕組みを講じること。（冗長化、不可分散など）	-	-	-	○	○	○	○	○	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
8. 脆弱性対策の実施																															
1	情報安全対策上問題となりうる恐れのある未検証のソフトウェア及び情報漏えいの危険性があるソフトウェア等を使用しないこと。	○	○	○	○	○	○	○	○	-	-	○	○	○	○	○	○	○	○	-	-	○	○	○	○	○	○	○	○	-	-
2	情報システムの脆弱性を突いて行われる外部からの技術的攻撃等のリスクについて情報収集を行い、それに対する情報安全対策を提示すること。	○	-	○	○	○	○	○	-	-	-	○	-	○	○	○	○	○	○	○	-	-	○	-	○	○	○	○	○	-	-
3	ウェブアプリケーションのセキュリティ実装として、「（別紙）脆弱性一覧」に示す脆弱性に対応すること。	○	○	○	○	○	○	-	-	-	-	○	○	○	○	○	○	-	-	-	-	○	○	○	○	○	○	○	-	-	-
4	障害を未然に防止するための措置、障害発生を早期発見するための措置及び障害発生時の問題拡大防止や迅速復旧のための措置について、業務の重要度に応じた情報安全対策を区に明示すること。	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
9. 情報セキュリティが脅威された場合の対処																															
1	情報セキュリティインシデントを受け付ける窓口を設置すること。	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
2	情報セキュリティインシデントに対する責任体制及び手順を確立すること。	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
3	複数のクラウド利用者からの情報セキュリティインシデントの報告をまとめ、区に報告すること。	-	-	-	○	○	○	○	○	-	-	-	-	-	○	○	○	○	○	-	-	-	-	-	○	○	○	○	○	-	-
4	個人情報等の機密性の高い情報の漏洩、紛失、改ざん、盗難及び誤送信等の事故を防止するための体制及び対策を明示すること。	○	○	○	○	○	○	-	-	○	○	○	○	○	○	○	○	-	-	○	○	○	○	○	○	○	○	-	-	○	○
5	事故が発生し、又はそれらの疑い若しくは恐れがあったときは、適切な措置をとるとともに、速急、区に報告すること。その場合、区民に対し適切な説明責任を果たすため、当該事故等の公表に対し応じること。	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
6	開発の業務の重要度に応じて開発及び保守のソースコードを提出し、著作権の扱いを明示すること。	○	-	-	-	-	-	-	-	○	-	-	-	-	-	-	-	-	-	○	-	○	-	-	-	-	-	-	-	-	-
7	区が実施する監査又は検査が円滑に遂行できるよう協力すること。	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
8	クラウドサービス等について、セキュリティ特性、サービスレベル及び管理上の要求事項が、適切に実行されていることを、監査などで確認し、区に結果などを明示すること。	-	-	-	○	○	○	○	○	-	-	-	-	-	○	○	○	○	○	-	-	-	-	-	○	○	○	○	○	-	-

（別紙）【脆弱性一覧】

本システムに混入しないよう対処を求める脆弱性は次のとおり。なお、各脆弱性の定義は「脆弱性名称の定義に関する参照先」にて確認すること。

「脆弱性名称の定義に関する参照先」の各（1）～（3）で示す参照先記載内容は次のとおり。なお、一部の脆弱性定義は（1）～（3）に該当するものがないため、当該名称解説URLを記載している。

（1）IPA『安全なウェブサイトの作り方 改訂第5版(2012年3月30日改訂)』のページと、章番号記載
http://www.ipa.go.jp/security/vuln/websecurity.html

（2）CWE - Common Weakness Enumeration のCWE番号（注）を記載。
※同サイトにおける脆弱性名称を一部和訳。 http://cwe.mitre.org/
（注）IPA共通脆弱性タイプ一覧CWE概説http://www.ipa.go.jp/security/vuln/CWE.html

（3）J-LIS『ウェブ健康診断仕様について』のページと、識別記号記載
https://www.ipa.go.jp/files/000017319.pdf

No	脆弱性名称		脆弱性名称の定義に関する参照先	
1	SQLインジェクション		(1)	P.6 - 1.1
			(2)	CWE-89
			(3)	P.7 - (A)
2	OSコマンド・インジェクション		(1)	P.10 - 1.2
			(2)	CWE-78
			(3)	P.9 - (D)
3	ディレクトリ・トラバーサル脆弱性		(1)	P.13 - 1.3
			(2)	CWE-98
			(3)	P.10 - (G)
4	「ログイン機能」の不備		(①～④に該当するもの)	
	①	推測可能なセッションID	(1)	P.18 - 4-(ⅰ)
			(2)	CWE-330
			(3)	P.13 - (K) - 2
	②	URL埋め込みのセッションIDの外部への漏えい	(1)	P.19 - 4-(ⅱ)
			(2)	CWE-522
			(3)	P.13 - (K) - 4, 5
	③	クッキーのセキュア属性不備	(1)	P.19 - 4-(ⅲ)
			(2)	CWE-614
			(3)	P.13 (K) - 3
	④	セッションIDの固定化	(1)	P.19 - 4-(ⅳ)-a、P.20 - 4-(ⅳ)-b
			(2)	CWE-384
			(3)	P.13 (K) - 1

No	脆弱性名称		脆弱性名称の定義に関する参照先	
5	クロスサイト・スクリプティング(XSS)		(1)	P.22 - 1.5
			(2)	CWE-79
			(3)	P.8 - (B)
6	利用者の意図に反した実行の防止機能の不備		(①、②に該当するもの)	
	①	クロスサイト・リクエスト・フォージェリ (CSRF)	(1)	P.29 1-6
			(2)	CWE-352
			(3)	P.8 (C)
	②	クリックジャッキング	(1)	該当なし
			(2)	該当なし
			(3)	該当なし
				<参考> http://en.wikipedia.org/wiki/Clickjacking
7	メールヘッダ・インジェクション脆弱性		(1)	P37 - 1.8
			(2)	CWE-93
			(3)	P.10 - (F)
8	「アクセス制御」と「認可処理」の不備			(次の①、②に該当するもの)
	①	アクセス制御	(1)	P.40 - 9-(ⅰ)
			(2)	CWE-284
			(3)	P.14 - (L)
	②	認可処理	(1)	P.40 - 9-(ⅱ)
			(2)	CWE-264
			(3)	P.14 - (L)
9	HTTPヘッダ・インジェクション		(1)	P.44 - 1.7
			(2)	CWE-113
			(3)	P.11 - (I)
10	evalインジェクション		(1)	該当なし
			(2)	CWE-95
			(3)	該当なし
11	競合状態の脆弱性		(1)	該当なし
			(2)	CWE-366
			(3)	該当なし
12	意図しないファイル公開		(1)	該当なし
			(2)	CWE-425 、CWE-548
			(3)	P.9 - (E)

No	脆弱性名称	脆弱性名称の定義に関する参照先	
13	アップロードファイルによるサーバ側スクリプト実行	(1)	該当なし
		(2)	CWE-434
		(3)	該当なし
14	秘密情報表示時のキャッシュ不停止	(1)	該当なし
		(2)	CWE-524
		(3)	該当なし
15	オープンリダイレクタ脆弱性（意図しないリダイレクト）	(1)	該当なし
		(2)	CWE-601
		(3)	P11 - (H)
16	クローラへの耐性	(1)	該当なし
		(2)	該当なし
		(3)	P.15 - 2.5

※地方公共団体情報システム機構

「地方公共団体における情報システムセキュリティ要求仕様モデルプラン（Webアプリケーション）第1.0版」