

情報セキュリティ対策特記事項

1 物理的セキュリティに関する基本要件

本業務における物理的セキュリティについては、以下の事項を踏まえた対策を実施すること。

(1) サーバ等の管理

- ① サーバ等の取付けを行う場合、火災、水害、埃、振動、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、必要な措置を講じること。
- ② 情報を格納しているサーバを冗長化し、同一データを保持すること。
- ③ メインサーバに障害が発生した場合に、速やかにセカンダリサーバを起動し、システムの運用停止時間を最小限になるよう必要な措置を講じること。
- ④ サーバ等の機器の電源について、停電等による電源供給停止に備え、当該機器が適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けること。
- ⑤ 当市の施設内に設置する場合は、別途協議するものとする。

(2) 端末や外部記録媒体等の管理

- ① 盗難防止のため、当市の執務室等で使用する端末のワイヤーによる固定、USBメモリ等の外部記録媒体の利用時以外の施錠保管等の物理的措置を講ずること。
- ② 本業務で使用する端末や外部記録媒体については、データ暗号化機能を備えるものとし、暗号化機能を有効に利用すること。
- ③ インターネットに接続する端末に個人情報を保存しないこと。
- ④ インターネットに接続する端末を当市のネットワークに接続しないこと。

2 人的セキュリティに関する基本要件

本業務における人的セキュリティについては、以下の事項を踏まえた対策を実施すること。

(1) 従業員等の順守事項

- ① 業務以外での目的で情報資産の外部への持ち出し、情報システムへのアクセス、インターネットへのアクセスを行わないこと。
- ② 本業務で使用する端末、外部記録媒体等を外部に持ち出す場合には、あらかじめ市の許可を得ること。また、その記録を作成し、保管すること。
- ③ USBメモリ等の外部記録媒体でデータを取り扱う場合は、あらかじめ市の許可を得るとともに、使用簿を作成し、使用者、使用日時、保存データの消去等を記録すること。
- ④ 私有の端末、外部記録媒体等を業務で使用しないこと。
- ⑤ 本業務で使用する端末等のソフトウェアに関するセキュリティ機能の設定を市の許可なく変更しないこと。
- ⑥ 本業務で使用する端末、外部記録媒体及び情報が印刷された文書等について、第三者に使用

されること、又は市の許可なく情報を閲覧されることがないように、離席時の端末のロックや外部記録媒体、文書等の容易に閲覧されない場所への保管など、適切に管理すること。

⑦ 業務上知りえた情報を他に漏らさないこと。

(2) 従業員等への教育

① 従業員等に対して、データの保護及び秘密の保持等データの取扱いに関し履行すべき責務について十分な教育を行い、その実施状況を記録し市に報告すること。

(3) 情報セキュリティインシデントの報告

① 本業務において、システムの停止、外部からのサイバー攻撃及び情報の盗難・紛失等の情報セキュリティインシデントを認知した場合、速やかに市に報告すること。

② 発生した情報セキュリティインシデントについて、原因の究明、記録の保存及び再発防止策を検討し市に報告するとともに、再発防止策を実施するために必要な措置について市の指示に従うこと。

(4) ID及びパスワード等の管理

① 本業務において認証用にICカード等を用いる場合は、次の事項を遵守しなければならない。

ア ICカード等を従業員間等で共有しないこと。

イ 業務上必要のないときは、ICカード等をカードリーダ等から抜いておかなければならない。

ウ ICカード等を紛失した場合は、速やかに市に報告するとともに、当該ICカード等を使用したシステム等へのアクセスを速やかに停止すること。

② 本業務において使用するIDについては、次の事項を遵守しなければならない。

ア 個人IDを本来の利用者以外に利用させないこと。

イ 供用IDは利用しないこと。

③ 本業務において使用するパスワードについては、次の事項を遵守しなければならない。

ア パスワードは、他者に知られないように管理すること。

イ パスワードを秘密にし、パスワードの照会等には一切応じないこと。

ウ パスワードは十分な長さとし、文字列は想像しにくいものにする。

エ パスワードが流出した恐れがある場合には、速やかに市に報告するとともに、パスワードを速やかに変更すること。

オ パスワードは定期的に、又はアクセス回数に基づいて変更し、古いパスワードを再利用しないこと。

カ 複数のシステムを利用する場合は、同一のパスワードをシステム間で供用しないこと。

キ 仮のパスワードは、最初のログイン時点で変更すること。

ク 端末等にパスワードを記憶させないこと。

3 技術的セキュリティに関する基本要件

本業務における技術的セキュリティについては、以下の事項を踏まえた対策を実施すること。

- ① サーバの冗長化対策に関わらず、定期的にバックアップを実施すること。
- ② 各種ログ及び情報セキュリティの確保に必要な記録を取得し保存すること。
- ③ 無線LANを利用する場合は、あらかじめ市の許可を得るとともに、解読が困難な暗号化及び認証技術を使用すること。
- ④ インターネットに接続する端末のWEBブラウザの接続先を本業務に必要最小限の範囲に限定すること。
- ⑤ OS(windowse11等)及びインストールされているソフトウェアは、常に最新化すること。ただし、当市のネットワークに接続して使用する場合は、市と協議のうえ、市の指示に従うこと。
- ⑥ 端末には業務上必要最小限のソフトウェアのみインストールすること。
- ⑦ 本業務で使用する全ての端末に次のアプリケーションをインストールすること。
 - ア 資産管理ソフト
 - イ ウイルス対策ソフトなお、端末を当市のネットワークに接続する場合は、当市が用意する次のアプリケーションを本業務で使用する全ての端末にインストールし、当市の管理コンソール上で管理ができるようにすること。
 - ア SKYSEA Client View(資産管理ソフト)
 - イ Trend Micro Apex One セキュリティエージェント (ウイルス対策ソフト)
- ⑧ 端末を当市のネットワークに接続する場合は、本業務で使用する全ての端末に対する次の情報をデータで提供すること。
 - ア 端末名
 - イ MACアドレス (MAC認証によるネットワーク制御を行うため)

4 給付金管理システムについて

本業務で使用する給付金管理システムについては、当市庁舎内の基幹系ネットワーク上にオンプレミス型で構築するものとし、以下の要件を踏まえたシステムを提案すること。

- ① 構築するシステムの稼働率、目標復旧時間、目標復旧ポイント、バックアップの保管方法などの可用性に関する事項をサービスレベル契約（以下「SLA」という。）又はサービスレベル目標（以下「SLO」という。）に規定すること。
- ② 不正なアクセスを防止するための ID 管理（ID のプロビジョニングから廃棄まで）とアクセス制御を実装していること。
- ③ 操作ログの取得・保存機能を有すること。
- ④ 業務終了後、使用したサーバ、端末、USB メモリ等の記録媒体は、確実に物理的に破壊し、又は全ての記録を復元不可能な状態に消去した後に廃棄し、廃棄したことが分かる書類を提出すること。
- ⑤ 当市の基幹系ネットワークを利用して運用すること。ただし、市のドメインへの参加はしないこ

と。

- ⑥ 同一ネットワーク上で稼働する他の業務システム（以下、現行業務システムという。）の運用に支障をきたさないようにすること。現行業務システムの運用に支障をきたしたときは、当市と協議の上、速やかにその障害を取り除くとともに、文書（様式は任意）により報告を行うこと。
- ⑦ 当市が用意する静脈認証システム(Auth Conductor Client)を全ての端末にインストールすること。なお、静脈認証センサーは当市から貸出するものとし、ユーザー登録については、市が実施するものとする。
- ⑧ サーバは、当市本庁舎8階サーバ室内に設置すること。

5 オンライン申請システムについて

本業務で使用するオンライン申請システムについては、クラウドサービスを利用したクラウド型で構築するものとし、以下の要件を踏まえたシステムを提案すること。

(1) クラウドサービスの基本要件

- ① ISMAP又はISO/IEC 27017の認証を取得したサービスであること。
- ② サービス約款、利用規約、SLA又はSLO（公開されていること）が存在していること。
- ③ 日本の裁判管轄、法令が適用されること。サービスを提供するリージョン（国・地域）が国内であること。本業務のデータが海外に保存されないこと。
- ④ サービスの中断時の復旧要件が基本契約、SLA又はSLOに規定されていること。
- ⑤ サービスの終了又は変更時における事前の通知等の取り決めや情報資産の移行方法が基本契約等に規定されていること。
- ⑥ 稼働率、目標復旧時間、目標復旧ポイント、バックアップの保管方法などの可用性に関する事項がSLA又はSLOに規定されていること。
- ⑦ クラウドサービス提供者が、利用者の情報資産へ目的外のアクセスや利用を行わないように基本契約に定める又は利用規約に定められていること。
- ⑧ クラウドサービス提供者における情報セキュリティ対策の実施内容及び管理体制について、公開資料や監査報告書（又は内部監査報告書・事業者の報告資料）の内容で確認できること。
- ⑨ クラウドサービス提供者又はその従業員、再委託先又はその他の者によって、利用者の意図しない変更が加えられないための管理体制について、公開資料や監査報告書（又は内部監査報告書・事業者の報告資料等）の内容で確認できること。
- ⑩ 情報セキュリティインシデントへの対処方法について、クラウドサービス提供者との責任分担や連絡方法を取り決め、基本契約又はSLAに定めること若しくはセキュリティチェックシート等により公表していること。
- ⑪ 脅威に対するクラウドサービス提供者の情報セキュリティ対策（なりすまし、情報漏えい、情報の改ざん、否認防止、権限昇格への対応、サービス拒否・停止等）の実施状況やその他の契約の履行状況の確認方法が基本契約又はSLAに規定されている若しくはクラウドサービス提供者のサイト等により公開されていること。

⑫ 情報セキュリティ対策の履行が不十分な場合の対処方法について、基本契約、サービスレベル契約（SLA）又は利用規約等に規定されていること。

⑬ クラウドサービス提供者により、利用規約、各種設定が変更される可能性があるため、変更内容の確認方法や連絡方法を基本契約、SLA又は利用規約等に定めること。

(2) 管理運用端末における不正なアクセスを防止するためのアクセス制御

① 不正なアクセスを防止するためのID管理（IDのプロビジョニングから廃棄まで）とアクセス制御を実装していること。

② クラウドサービスに接続する際は、生体認証を含む多要素認証を用いること。

③ 操作ログの取得・保存機能を有すること。

④ 固定IP規制やVPN等通信経路のセキュリティ対策が提供されていること。

(3) 取り扱う情報の機密性保護のための暗号化

① 暗号アルゴリズム（CRYPTRECにより安全性及び実装性能が確認された「電子政府推奨暗号リスト」）を用いた暗号化処理（情報が保存されている場合、情報が通信され転送されている場合等フローに応じた暗号化）を行うこと。

(4) クラウドサービス内の通信の制御

① 利用するクラウドサービスのネットワーク基盤が他の利用者のネットワークや通信と分離されていること。また、そのことがクラウドサービス提供者のサイト等により公開されていること。

(5) 設計・設定時の誤りの防止

① クラウドサービスの設定を変更する場合、設定誤りを防止するための対策を行うこと。

② 利用するクラウドサービスの仮想マシンのネットワークが他の利用者のネットワークと分離されていること。また、そのことがクラウドサービス提供者のサイト等により公開されていること。

(6) クラウドサービス終了時の対策

① 業務終了後、全ての記録を復元不可能な状態に消去した後に廃棄し、廃棄したことが分かる書類を提出すること。