

個人情報保護管理運営会議 付議事項

件 名	公害補償システム再構築に係るデータ移行の業務委託について
--------	------------------------------

内容は別紙のとおり

要綱の根拠

◇第3条第1項第3号（電算処理、業務委託）

（担当部課：健康部健康政策課）

事業の概要

事業名	公害補償システム内データ移行作業の業務委託														
担当課	健康政策課														
目 的	公害補償システム再構築のため														
対象者	公害健康被害認定患者及び大気汚染医療費助成認定患者														
事業内容	1 概要 現行の公害補償システム保守業務を委託している事業者より、運用・保守を令和8年度限りで完全に撤退するとの申し入れがあった。そこで、令和9年度以降故障対応等を含めた保守メンテナンスを行うことができる東京ファクトリーオートメーション株式会社へ、新たな公害補償システムの開発とデータ移行作業を委託し、システムの再構築を確実に実施し、公害補償に係る業務遂行を担保する。 2 個人情報保護管理運営会議への付議内容 (1) 電算処理 新たな公害補償システムの開発・カスタマイズ作業に伴い、現行システムから新システムへのデータ移行を行う。 (2) 業務委託 新たな公害補償システムの開発・カスタマイズ作業に伴う新システムへのデータ移行業務を委託する。 なお、本件は既に新公害補償システムの開発等業務委託契約を締結している事業者に対し、個人情報の取り扱いを含む上記の業務を行わせることについて諮るもの。 3 対象者数 <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 60%;">大気認定台帳</td><td style="text-align: right;">6, 300件</td></tr> <tr> <td>公害認定台帳</td><td style="text-align: right;">4, 000件</td></tr> <tr> <td>公害審査履歴</td><td style="text-align: right;">12, 000件</td></tr> <tr> <td>給付支払台帳</td><td style="text-align: right;">350, 000件</td></tr> <tr> <td>医療機関台帳</td><td style="text-align: right;">4, 500件</td></tr> <tr> <td>金融機関台帳</td><td style="text-align: right;">15, 000件</td></tr> <tr> <td>保険者台帳</td><td style="text-align: right;">1, 200件</td></tr> </table> ※個人情報の流れは、資料37-1のとおり	大気認定台帳	6, 300件	公害認定台帳	4, 000件	公害審査履歴	12, 000件	給付支払台帳	350, 000件	医療機関台帳	4, 500件	金融機関台帳	15, 000件	保険者台帳	1, 200件
大気認定台帳	6, 300件														
公害認定台帳	4, 000件														
公害審査履歴	12, 000件														
給付支払台帳	350, 000件														
医療機関台帳	4, 500件														
金融機関台帳	15, 000件														
保険者台帳	1, 200件														

件名 公害補償システム再構築に係るデータ移行作業

※太字ゴシック(下線)が平成23年度第3回情報公開・個人情報保護審議会承認(了承)済みの内容からの変更箇所

保有課(担当課)	健康政策課
登録業務の名称	公害健康被害の補償給付等
記録される情報項目(だれの、どのような項目が、どのコンピュータに記録されるのか)	1 個人の範囲 公害健康被害認定患者及び大気汚染医療費助成認定患者 2 記録項目 現行公害補償システムに記録されている台帳 (大気認定台帳、公害認定台帳、公害審査履歴、給付支払台帳、医療機関台帳、金融機関台帳、保険者台帳) 詳細事項は資料37-2のとおり 3 記録するコンピュータ 新宿区の統合基盤仮想サーバ
新規開発・追加・変更の理由	令和9年度以降も公害健康被害の補償給付を始めとした業務遂行への支障がないよう、令和8年度の内に従来と同様の業務を行うことができる新たな公害補償システムを開発し、現行システムから新システムへデータ移行を行う必要があるため。
新規開発・追加・変更の内容	1 新たな公害補償システムの開発 2 現行公害補償システムに記録されている個人情報を含む台帳データの新公害補償システムへの移行
開発等を委託する場合における個人情報保護対策	別紙チェックリストのとおり
新規開発・追加・変更の時期	令和8年 8月 システム開発業務委託 令和8年 11月 移行データ出力・取り込み開始 令和9年 2月 新システム正式稼働

件名 公害補償システムデータ移行業務の委託について

※太字ゴシック(下線)が平成23年度第3回情報公開・個人情報保護審議会承認(了承)済みの内容からの変更箇所

保有課(担当課)	健康政策課
登録業務の名称	公害健康被害の補償給付等
委託先	東京ファクトリーオートメーション株式会社(特命随意契約)
委託に伴い事業者処理させる情報項目(だれの、どのような項目か)	現行公害補償システムに記録されている台帳 (大気認定台帳、公害認定台帳、公害審査履歴、給付支払台帳、医療機関台帳、金融機関台帳、保険者台帳) 詳細事項は資料37-2のとおり
処理させる情報項目の記録媒体	<u>電磁的媒体(新宿区の統合基盤仮想サーバ)</u>
委託理由	<u>新たな公害補償システムへ開発を委託した東京ファクトリーオートメーション株式会社に、データ移行作業も委託することで個人情報の取り扱いを含む作業を安全かつ効率的に実施できると判断したため。</u>
委託の内容	新たな公害補償システムの構築および現行の公害補償システムへ記録されたデータの新システムへのセットアップ作業
委託の開始時期及び期限	<u>令和8年8月から令和9年3月31日まで</u> (次年度以降も、同様の業務委託を行う。)
委託にあたり区が行う情報保護対策	別紙チェックリストのとおり
受託事業者に行わせる情報保護対策	別紙チェックリストのとおり

新宿区
(健康政策課)

- ・ 電磁的媒体（現行サーバ、次期サーバ）の保管場所・・・新宿区統合基盤仮想サーバ（持出しなし）
- ・ 委託先がシステム構築を行う場所・・・健康政策課業務室内
- ・ 個人情報を含むデータ移行の手段・・・旧システムからCSV形式で出力し、区PCを経由して新システムに移行

新宿区統合基盤仮想
サーバ内

公害補償
システム

大気認定台帳
公害認定台帳
公害審査履歴
給付支払台帳
医療機関台帳
金融機関台帳
保険者台帳
詳細は資料 3 6 - 2
のとおり

- ・ 新公害補償システム開発
- ・ データ移行・検証

委託先

(東京ファクトリーオートメーション
株式会社)

新宿区統合基盤仮想
サーバ内

新：公害補償
システム

大気認定台帳
公害認定台帳
公害審査履歴
給付支払台帳
医療機関台帳
金融機関台帳
保険者台帳
詳細は資料 3 6 - 2
のとおり

- ・ 特定相手以外との通信不可
- ・ ネットワーク機器やサーバの制御
- ・ 通信内容の暗号化
- ・ 外部からの攻撃防御（ファイアウォールの設置、サーバの要塞化、侵入検知、セキュリティパッチの適用等）
- ・ ウィルス対策
- ・ 最新のパターンファイルの適用
- ・ ID / パスワード等認証
- ・ ファイルのパスワード設定
- ・ アクセス制御
- ・ システムネットワーク状態等の監視
- ・ アクセスログ取得
- ・ サーバ冗長化 ・ バックアップ
- ・ 入退室管理
- ・ 国内法が適用されるサーバ環境

- ・ 特記事項等の遵守
- ・ 立入調査等及び状況報告
- ・ 責任者及び取扱者の報告
- ・ 区が作成した業務フローに基づく業務の履行
- ・ データの暗号化
- ・ 事故等への対応体制及び手順の整備
- ・ 事故発生時等の協議

- ・ 特定相手以外との通信不可
- ・ ネットワーク機器やサーバの制御
- ・ 通信内容の暗号化
- ・ 外部からの攻撃防御（ファイアウォールの設置、サーバの要塞化、侵入検知、セキュリティパッチの適用等）
- ・ ウィルス対策
- ・ 最新のパターンファイルの適用
- ・ ID / パスワード等認証
- ・ ファイルのパスワード設定
- ・ アクセス制御
- ・ システムネットワーク状態等の監視
- ・ アクセスログ取得
- ・ サーバ冗長化 ・ バックアップ
- ・ 入退室管理
- ・ 国内法が適用されるサーバ環境

公害補償システム（公害補償システムに記録されている台帳） 記録項目

【大気認定台帳】

1 認定患者データの管理

認定患者の現住所・郵便番号、認定患者の生年月日、認定患者性別、認定患者の医療券番号（個人を識別するための番号）、認定患者の氏名及び氏名の振り仮名（フリガナ）（外国籍を有する場合は外国人氏名のフリガナ及び通称名のフリガナをそれぞれ管理）、認定患者の住民番号、認定患者の年齢、認定患者の電話番号、認定患者の加入保険情報（保険者番号、本人家族区分、記号番号、保険の種類、負担割合、変更日）、メモ欄

2 認定情報データの管理

疾病名、認定有効期間開始年月日、認定有効期間終了年月日、認定期間決定日年月日、医療券交付日年月日
主治医診断書項目情報、審査会情報（認定結果、認定区分、認定基準額、支給予定額、審査日、認定日、認定期間等）

【公害認定台帳】

1 認定患者データの管理

認定患者の現住所・郵便番号、認定患者の生年月日、認定患者性別、認定患者の医療券番号（個人を識別するための番号）、認定患者の氏名及び氏名の振り仮名（フリガナ）（外国籍を有する場合は外国人氏名のフリガナ及び通称名のフリガナをそれぞれ管理）、認定患者の住民番号、認定患者の年齢、認定患者の電話番号、認定患者の加入保険情報（保険者番号、本人家族区分、記号番号、保険の種類、負担割合、変更日）、メモ欄

2 認定情報データの管理

疾病名、最初の申請日年月日、最初の認定日年月日、請求日年月日、障害等級（障害の程度）
更新決定日年月日、更新有効期間開始年月日、更新有効期間終了年月日、医療手帳発行日年月日
見直し決定日年月日、見直し有効期間開始年月日、見直し有効期間終了年月日、医療手帳発行日年月日
認定有効期間開始年月日、認定有効期間終了年月日、認定期間決定日年月日、医療券交付日年月日

3 支給データの管理

医療機関情報、医療費等、支給費情報（支給対象費目・支給額、診療月、審査月、支給履歴、支給日）

【公害審査履歴】

1 認定審査管理

審査年月日、医師診断書項目、検査結果項目、診療状況項目、申請書類受付年月日（更新、見直し等）

2 認定結果管理

認定結果、認定区分、認定基準額、支給予定額、審査年月日、審査会決定年月日、認定期間年月日等

【給付支払台帳】

1 認定患者データの支給管理

療養手当、定期的給付、療養費等、文書料（各種給付情報の履歴表示）

2 医療機関データの支給管理

医師診断報告書、医学的検査報告書、文書料（各種給付情報の履歴表示）

【医療機関台帳】

医療機関の住所・郵便番号、医療機関の名称、医療機関の名称カナ、医療機関の電話番号、医療機関コード、医療機関の種別情報、医療機関の支払先情報（金融機関コード、金融機関支店コード、金融機関預金種別、金融機関支店コード、金融機関口座番号、金融機関口座名義）、医療機関の登録年月日、医療機関の終了年月日、メモ欄

【金融機関台帳】

金融機関の住所・郵便番号、金融機関の名称、金融機関の名称カナ、金融機関コード、金融機関支店コード、金融機関口座番号

【保険者台帳】

保険者の住所、保険者の名称、保険者の名称カナ、保険者コード、保険者記号番号、保険者負担割合、保険者情報
保険者の支払先情報（金融機関コード、金融機関支店コード、金融機関預金種別、金融機関支店コード、金融機関口座番号、金融機関口座名義）、保険者の開設年月日、保険者の終了年月日

3 電算処理にかかる個人情報保護対策チェックリスト

	・対策が可能であれば「○」 ・対策の必要がない場合は「ー」	情報保護対策
開発等を委託する場合 における区が行う 情報保護対策 【運用上の対策】	○	個人情報保護法及び新宿区情報セキュリティポリシーを遵守するよう指導する。また、クラウドサービスを利用する場合は、総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン」を準拠するよう指導する。
	○	必要に応じて、事業者への立入り調査等を実施するとともに、結合先に対し速やかに状況報告をするよう指導する。
	○	システム上で不要となった電子データを削除し、電子データの消去を行ったことの報告書を提出するよう指導する。
	○	業務開始前に、事故、災害、トラブルに対応できる体制及び手順を整備し、結合先と緊急時の連絡体制や対応手順を確認する。
	○	事故が発生した場合又は個人情報保護及び情報セキュリティ対策の変更があった場合は、直ちに結合先と今後の対応を協議する。
	○	区のシステム機器設置場所へ委託先が入退室する場合は、管理（申請、承認、記録）を行う。また、委託先がシステム機器を操作する場合には、事前に作業内容の報告を求め、区が承認した後に実施するよう指導するとともに、個人情報データの持出しを禁止する。
	○	プログラムの移行等を行う場合は、外部記録媒体の管理を行い、利用時は第三者漏えいがないようパスワードを施す等、利用制限を設ける。
	○	入力及び取込みテストにおいては、ダミーデータを使うよう指導する。
	○	実データを使用した検証作業は、区職員が実施する（委託先には、必要な支援のみ行わせる）。
	○	モバイルパソコン等の電子計算組織を持込む場合は、事前に区の許可をとらせ、用途は、社内事務連絡、設計書等の閲覧に限定させる。また、委託先のモバイルパソコン等と区のネットワーク、システム機器及びUSB等の記録媒体と接続をさせないように、区の職員が立ち会う。
開発等を委託する場合 における区が行う 情報保護対策 【システム上の対策】	○	データ項目定義の修正漏れによるシステム不具合等が無いよう、双方で事前に綿密なスケジュール計画やチェックシートを作成して実施する。なお、稼働にあたっては必ず仮移行を行うこととし、本稼働はシステムを使用していない時間帯（時間外・休日）に実施し、十分な検証を行う。
	○	接続するネットワークについては、特定相手以外との通信を不可とする。
	○	ネットワーク機器やサーバを制御し、通信できるシステムを限定する。
	○	通信内容は暗号化し、通信途上の個人情報の盗用、改ざん、成りすましを防止する。
	○	ファイアウォールの設置、サーバの要塞化、侵入検知、セキュリティパッチの適用等の対策を講じ、外部からの不正侵入やデータ破壊・漏えい等各種の攻撃から防御する。
	○	コンピューターウイルス感染等がないよう、ウイルス対策ソフトウェアの導入及び最新のパターンファイルを適用する。
	○	ID・パスワードやアドレス情報による運用により、第三者による個人情報の盗用、改ざん、成りすましを防止する。
	○	個人情報を保存する場合は、保存先フォルダへアクセス権を設定するとともに、ファイルにパスワードを付すなど、情報へのアクセス制御を徹底する。
	○	システム・ネットワークの状態、機器操作、サービス利用等の監視及びアクセスログ等を取得する。取得したログは、定期的に分析する。
	○	サーバ冗長化、バックアップ等により、事故や障害発生時におけるシステム稼働体制を整備する。
	○	入退室管理等により情報資産の危殆化を防止する。
	○	システムを提供するサーバは日本国内の法が適用される安全性が確保された環境にする。

3 電算処理にかかる個人情報保護対策チェックリスト

	・対策が可能であれば「○」 ・対策の必要がない場合は「ー」	情報保護対策
開発等を委託する場合における委託先に行わせる情報保護対策 【運用上の対策】	○	個人情報保護法及び新宿区情報セキュリティポリシーを遵守させる。また、クラウドサービスを利用する場合は、総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン」を準拠させる。
	○	必要に応じて、事業者への立入り調査等を受けさせるとともに、結合先に対し速やかに状況報告をさせる。
	○	システム上で不要となった電子データを削除させ、電子データの消去を行ったことの報告書を提出させる。
	○	業務開始前に、事故、災害、トラブルに対応できる体制及び手順を整備させ、区と緊急時の連絡体制や対応手順を確認させる。
	○	事故が発生した場合又は個人情報保護及び情報セキュリティ対策の変更があった場合は、直ちに区と今後の対応を協議させる。
	○	区のシステム機器設置場所へ委託先が入退室する場合は、区の管理（申請、承認、記録）に従わせる。また、委託先がシステム機器を操作する場合には、事前に作業内容の報告をさせ、区が承認した後に実施させるとともに、個人情報データの持出しを禁止させる。
	○	プログラムの移行等を行う場合は、外部記録媒体の管理を行い、利用時は第三者漏えいがないようパスワードを施す等、利用制限を設ける。
	○	入力及び取込みテストにおいては、ダミーデータを使わせる。
	○	実データを使用した検証作業は、区職員が実施する（委託先には、必要な支援のみ行わせる）。
	○	モバイルパソコン等の電子計算組織を持込む場合は、事前に区の許可をとらせ、用途は、社内事務連絡、設計書等の閲覧に限定させる。また、委託先のモバイルパソコン等と区のネットワーク、システム機器及びUSB等の記録媒体と接続をさせないように、区の職員の立会いに応じさせる。
開発等を委託する場合における委託先に行わせる情報保護対策 【システム上の対策】	○	データ項目定義の修正漏れによるシステム不具合等が無いよう、双方で事前に綿密なスケジュール計画やチェックシートを作成して実施する。なお、稼働にあたっては必ず仮移行を行うこととし、本稼働はシステムを使用していない時間帯（時間外・休日）に実施させ、十分な検証を行わせる。
	○	接続するネットワークについては、特定相手以外との通信を不可とさせる。
	○	ネットワーク機器やサーバを制御し、通信できるシステムを限定させる。
	○	通信内容は暗号化させ、通信途上の個人情報の盗用、改ざん、成りすましを防止させる。
	○	ファイアウォールの設置、サーバの要塞化、侵入検知、セキュリティパッチの適用等の対策を講じさせ、外部からの不正侵入やデータ破壊・漏えい等各種の攻撃から防御させる。
	○	コンピューターウイルス感染等がないよう、ウイルス対策ソフトウェアの導入及び最新のパターンファイルを適用させる。
	○	ID・パスワードやアドレス情報による運用により、第三者による個人情報の盗用、改ざん、成りすましを防止させる。
	○	個人情報を保存する場合は、保存先フォルダへアクセス権を設定させるとともに、ファイルにパスワードを付すなど、情報へのアクセス制御を徹底させる。
	○	システム・ネットワークの状態、機器操作、サービス利用等の監視及びアクセスログ等を取得させる。取得したログは、定期的に分析させる。
	○	サーバ冗長化、バックアップ等により、事故や障害発生時におけるシステム稼働体制を整備させる。
	○	入退室管理等により情報資産の危殆化を防止させる。
	○	システムを提供するサーバは日本国内の法が適用される安全性が確保された環境にさせる。

5 業務委託にかかる個人情報保護対策チェックリスト

(電磁的媒体・紙媒体の取扱い)

	・対策が可能であれば「○」 ・対策の必要がない場合は「－」	情報保護対策
委託にあたり区が行う 情報保護対策 【運用上の対策】	○	契約にあたり、「特記事項」を付すとともに、個人情報保護法及び新宿区情報セキュリティポリシーを遵守するよう指導する。また、クラウドサービスを利用する場合は、総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン」を準拠するよう指導する。
	○	契約履行の間、特記事項に基づき立入り調査等を実施するとともに、委託先に対し速やかに状況報告をするよう指導する。
	○	再委託先がある場合には、委託先との間に立入り調査等ができる契約内容を付すとともに、必要に応じて又は定期的に立入り調査等を実施するよう指導する。
	○	取扱責任者及び取扱者をあらかじめ指定し、区に報告するよう指導する。
	○	全体の業務フローを作成し、委託先と共有する。
	○	取扱う個人情報の管理について、必要に応じて又は定期的に確認する体制を構築するよう指導する。
	○	個人情報を含むデータを作成する必要がある場合は、パスワードを付してデータを暗号化する。また、電磁的媒体（DVD-R等）とパスワード通知書の受渡しは、それぞれ別の機会を設定し、鍵付きカバン等を使用して、手渡しで行うよう指導する。
	－ (電子データのみ の取扱いのため)	個人情報を手交する場合は、鍵付きカバン等を使用して運搬する。
	－ (電子データのみ の取扱いのため)	個人情報の受渡しにあたっては、管理簿に記載する。管理簿には、日時、取扱者、情報の内容、数量を確認記録票に記録し、履歴を追跡できるようにする。
	－ (電子データのみ の取扱いのため)	個人情報は、施錠できる金庫又はキャビネット等に保管する。
	○	業務履行後、個人情報が記録された電磁的媒体（DVD-R等）、紙媒体及びパスワード通知書は返却し、電子データは消去するよう指導する。また、区に電子データの消去を行ったことの報告書を提出するよう指導する。
	○	業務開始前に、事故、災害、トラブルに対応できる体制及び手順を整備し、委託先と緊急時の連絡体制や対応手順を確認する。
委託にあたり区が行う 情報保護対策 【システム上の対策】	○	接続するネットワークについては、特定相手以外との通信を不可とする。
	○	ネットワーク機器やサーバを制御し、通信できるシステムを限定する。
	○	通信内容は暗号化し、通信途上の個人情報の盗用、改ざん、成りすましを防止する。
	○	ファイアウォールの設置、サーバの要塞化、侵入検知、セキュリティパッチの適用等の対策を講じ、外部からの不正侵入やデータ破壊・漏えい等各種の攻撃から防御する。
	○	コンピューターウイルス感染等がないよう、ウイルス対策ソフトウェアの導入及び最新のパターンファイルを適用する。
	○	ID・パスワードやアドレス情報による運用により、第三者による個人情報の盗用、改ざん、成りすましを防止する。
	○	個人情報を保存する場合は、保存先フォルダへアクセス権を設定するとともに、ファイルにパスワードを付すなど、情報へのアクセス制御を徹底する。
	○	システム・ネットワークの状態、機器操作、サービス利用等の監視及びアクセスログ等を取得する。取得したログは、定期的に分析する。
	○	サーバ冗長化、バックアップ等により、事故や障害発生時におけるシステム稼働体制を整備する。
	○	入退室管理等により情報資産の危殆化を防止する。
	○	システムを提供するサーバは日本国内の法が適用される安全性が確保された環境にする。

5 業務委託にかかる個人情報保護対策チェックリスト

(電磁的媒体・紙媒体の取扱い)

	・対策が可能であれば「○」 ・対策の必要がない場合は「－」	情報保護対策
委託事業者に行わせる 情報保護対策 【運用上の対策】	○	契約にあたり、「特記事項」を付すとともに、個人情報保護法及び新宿区情報セキュリティポリシーを遵守させる。また、クラウドサービスを利用する場合は、総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン」を準拠させる。
	○	契約履行の間、特記事項に基づき立入り調査等を受けさせるとともに、委託先に対し速やかに状況報告をさせる。
	－	再委託先がある場合には、委託先との間に立入り調査等ができる契約内容を付すとともに、必要に応じて又は定期的に立入り調査等を実施させる。
	○	取扱責任者及び取扱者をあらかじめ指定させ、区に報告させる。
	○	区が作成した業務フローに基づき、業務を行わせる。
	○	取扱う個人情報の管理について、必要に応じて又は定期的に確認する体制を構築させる。
	○	個人情報を含むデータを作成する必要がある場合は、パスワードを付してデータを暗号化させる。電磁的媒体（DVD-R等）とパスワード通知書の受渡しは、それぞれ別の機会を設定し、鍵付きカバン等を使用させ、手渡しで行わせる。
	－ (電子データのみ の取扱いのため)	個人情報を手交する場合は、鍵付きカバン等を使用して運搬させる。
	－ (電子データのみ の取扱いのため)	個人情報の受け渡しにあたっては、管理簿に記載させる。管理簿には、日時、取扱者、情報の内容、数量を確認記録票に記録し、履歴を追跡できるようにさせる。
	－ (電子データのみ の取扱いのため)	個人情報は、施錠できる金庫又はキャビネット等に保管させる。
	○	業務履行後、個人情報が記録された電磁的媒体（DVD-R等）、紙媒体及びパスワード通知書は返却させ、電子データは消去させる。また、区に電子データの消去を行ったことの報告書を提出させる。
	○	業務開始前に、事故、災害、トラブルに対応できる体制及び手順を整備させ、区と緊急時の連絡体制や対応手順を確認させる。
委託事業者に行わせる 情報保護対策 【システム上の対策】	○	事故が発生した場合又は個人情報保護及び情報セキュリティ対策の変更があった場合は、直ちに区と今後の対応を協議させる。
	○	接続するネットワークについては、特定相手以外との通信を不可とする。
	○	ネットワーク機器やサーバを制御し、通信できるシステムを限定させる。
	○	通信内容は暗号化させ、通信途上の個人情報の盗用、改ざん、成りすましを防止させる。
	○	ファイアウォールの設置、サーバの要塞化、侵入検知、セキュリティパッチの適用等の対策を講じさせ、外部からの不正侵入やデータ破壊・漏えい等各種の攻撃から防御させる。
	○	コンピューターウイルス感染等がないよう、ウイルス対策ソフトウェアの導入及び最新のパターンファイルを適用させる。
	○	ID・パスワードやアドレス情報による運用により、第三者による個人情報の盗用、改ざん、成りすましを防止させる。
	○	個人情報を保存する場合は、保存先フォルダへアクセス権を設定させるとともに、ファイルにパスワードを付すなど、情報へのアクセス制御を徹底させる。
	○	システム・ネットワークの状態、機器操作、サービス利用等の監視及びアクセスログ等を取得させる。取得したログは、定期的に分析させる。
	○	サーバ冗長化、バックアップ等により、事故や障害発生時におけるシステム稼働体制を整備させる。
	○	入退室管理等により情報資産の危殆化を防止させる。
	○	システムを提供するサーバは日本国内の法が適用される安全性が確保された環境にさせる。