資料４７

個人情報保護管理運営会議　付議事項

件名	後期高齢者医療保険料の特別徴収（仮徴収）開始通知書の封入封緘に係る外部結合等について

内容は別紙のとおり

要綱の根拠

◇第３条第１項第３号（外部結合、業務委託）

（担当部課：健康部高齢者医療担当課）

事業の概要

事業名	後期高齢者医療保険料の特別徴収（仮徴収）開始通知書の封入封緘委託について
担当課	高齢者医療担当課
目　的	後期高齢者医療保険料の仮徴収開始通知書発送業務の正確な遂行及び業務の効率化
対象者	後期高齢者医療保険料の特別徴収（仮徴収）の対象者
事業内容	１　概要 後期高齢者医療保険料は、毎年度７月に年間保険料を決定している。年金から保険料を徴収する特別徴収については、高齢者の医療の確保に関する法律第１１０条において準用する介護保険法第１４０条の規定に基づき、年間保険料が決定する前の４月、６月及び８月に、前年度の保険料額を基に算出した額を仮に徴収している（以下「仮徴収」という）。 区では、年間を通じた各期の徴収額の差をできるだけ小さくするため、一定の要件に該当する被保険者について、6 月及び 8 月の仮徴収額を変更する平準化を行っている。平準化の対象となる被保険者には、毎年 3 月下旬に「後期高齢者医療保険料特別徴収（仮徴収）開始通知書」（以下「仮徴収開始通知書」という）を送付している。 これまで、仮徴収開始通知書は圧着はがきにより作成していたが、令和８年３月の後期高齢者医療システムの標準化に伴い、標準仕様書に定める様式で作成することとなったため、今後は通知書を封筒に封入して送付する必要が生じる。 このため、仮徴収開始通知書の印刷、印字、封入封緘及び発送業務を委託し、業務の効率化を図る。 ２　個人情報保護管理運営会議への付議内容 （１）外部結合 LGWAN 回線を介して区のイントラ PC とクラウドストレージ（Box）を結合し、対象者データ等を提供する。 （２）業務委託 ①委託事業者への仮徴収開始通知書作成用データの提供 ②仮徴収開始通知書の印刷及び印字 ③仮徴収開始通知書の封入封緘及び発送業務 ３　対象者数 2,165 人（令和８年度平準化対象者数（(仮徴収開始通知書送付対象者数)）） (参考：令和８年度の特別徴収対象者数　22,390 人) ※ 個人情報の流れは、資料４７－１のとおり

別紙(電子計算機の外部結合関係)

◇外部結合(第３条第１項第３号)

件名　後期高齢者医療保険料の特別徴収（仮徴収）開始通知書の封入封緘に係る外部結合について

保有課（担当課）	高齢者医療担当課
登録業務の名称	後期高齢者医療保険料の賦課
結合される情報項目（だれの、どのような項目か）	個人の範囲 後期高齢者医療保険料の特別徴収（仮徴収）の平準化対象となる被保険者 情報項目 住所、被保険者氏名、被保険者番号、性別、生年月日、決定年月日、決定理由、仮徴収合計金額、納付方法、特別徴収義務者名、特別徴収対象年金、特別徴収年金給付額、期別保険料額
結合の相手方	株式会社Box Japan （ISMAP登録済、ISMSクラウドセキュリティ認証取得済み）
結合する理由	対象者データについて、デジタルツール（クラウドストレージ）で情報の提供を行うことにより、委託事業者側と区側で、個人情報を安全かつ効率的に共有し、作業効率の向上や事業の迅速化を図るため。
結合の形態	区イントラネットパソコンからLGWANを経由して、クラウドストレージサービス（Box）にアクセスする。
結合の開始時期と期間	令和９年２月１日から令和９年３月３１日まで（次年度以降も、同様の外部結合を行う。）
情報保護対策	別紙チェックリストのとおり

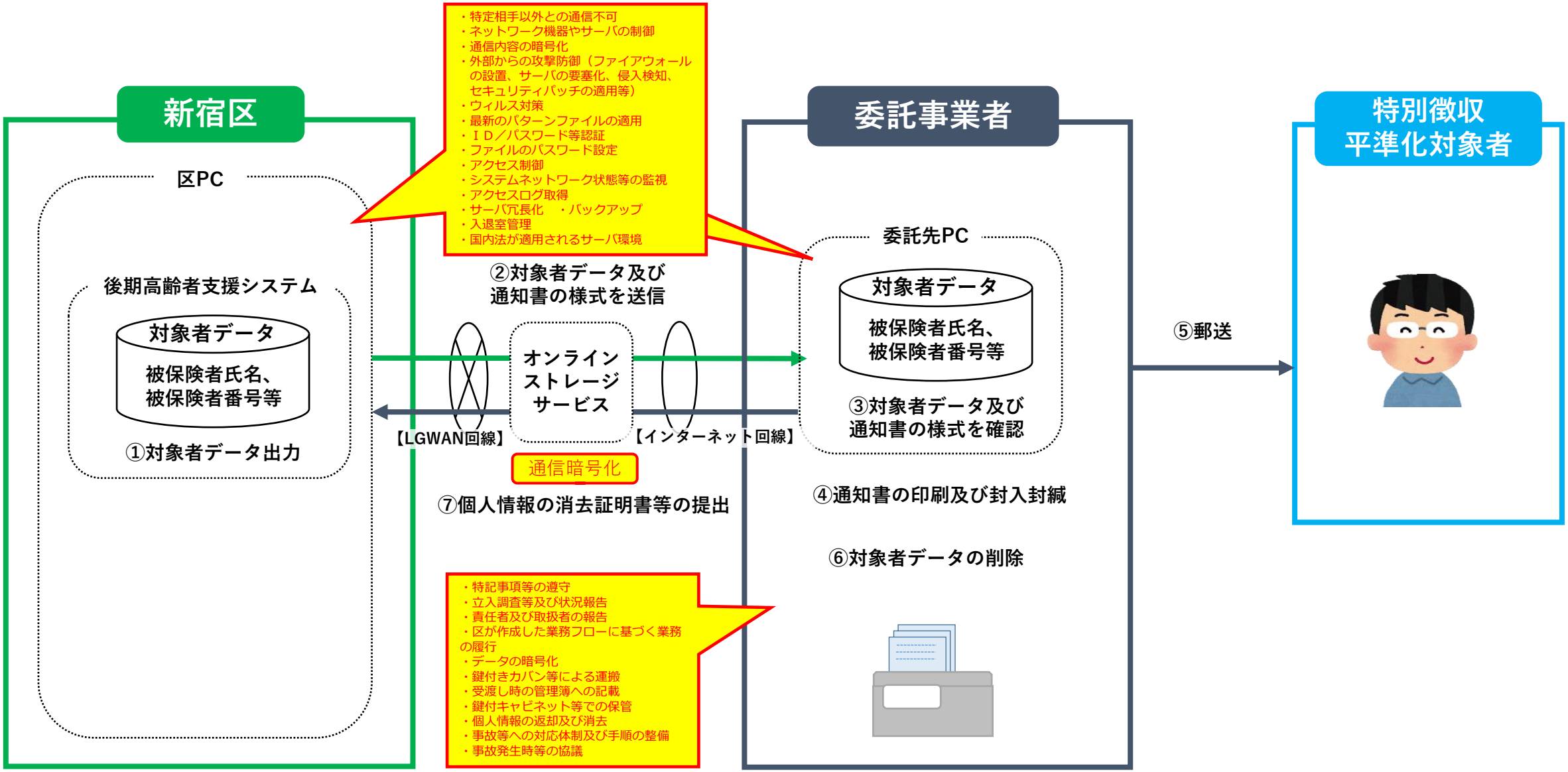
別紙（業務委託）

◇業務委託（第３条第１項第３号）

件名　後期高齢者医療保険料の特別徴収（仮徴収）開始通知書の封入封緘に係る業務委託について

保有課(担当課)	高齢者医療担当課
登録業務の名称	後期高齢者医療保険料の賦課
委託先	未定（随意契約を予定）
委託に伴い事業者に処理させる情報項目（だれの、どのような項目か）	個人の範囲 後期高齢者医療保険料の特別徴収（仮徴収）の平準化対象となる被保険者 情報項目 住所、被保険者氏名、被保険者番号、性別、生年月日、決定年月日、 決定理由、仮徴収合計金額、納付方法、特別徴収義務者名、 特別徴収対象年金、特別徴収年金給付額、期別保険料額
処理させる情報項目の記録媒体	電磁的記録（区指定のクラウドストレージ）
委託理由	大量の仮徴収開始通知書の印刷、印字、封入封緘及び発送業務を委託することにより、業務の効率化を図るため。
委託の内容	(1) 仮徴収開始通知書の印刷 (2) 仮徴収開始通知書への被保険者情報の印字 (3) 窓開き封筒の作成 (4) 仮徴収開始通知書の封入封緘 (5) 仮徴収開始通知書の発送
委託の開始時期及び期限	令和９年２月１日から令和９年３月３１日まで（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

後期高齢者医療保険料の特別徴収（仮徴収）開始通知書の封入封緘に係る個人情報の流れ　（資料４７－１）



4　外部結合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
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。

4　外部結合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
結合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。
結合先に行わせる情報保護対策【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「ー」	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。
	○	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。
	○	個人情報を含むデータを作成する必要が生じた場合は、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。
	ー （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。
	ー （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。
	ー （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。
	○	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、直ちに委託先と今後の対応を協議する。
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「ー」	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。
	○	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。
	○ （クラウドストレージでの受け渡し）	個人情報を含むデータを作成する必要が生じた場合は、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。
	ー （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。
	ー （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。
	ー （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。
	○	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。
委託事業者に行わせる情報保護対策【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。