資料63

個人情報保護管理運営会議　付議事項

件名	（仮称）適正管理制度オンラインシステムとの外部結合について

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）

（担当部課：環境清掃部環境対策課）

事業の概要

事業名	（仮称）適正管理制度オンラインシステムとの外部結合について
担当課	環境対策課
目　的	東京都環境局が導入を進める「(仮称）適正管理制度オンラインシステム」との結合により、対象者による適正管理化学物質の使用量等の報告内容を確認する。
対象者	都民の健康と安全を確保する環境に関する条例（以下、環境確保条例とする。）に基づく工場又は指定作業場の設置者のうち、適正管理化学物質取扱事業者である者（以下、事業者とする。）
事業内容	１　概要 環境確保条例第１１０条に基づく適正管理化学物質の使用量等の報告について、現在、区は、事業者から書面により報告を受け、報告内容を審査し、必要に応じて事業者に対して電話等により指導をしている。また、報告内容を取り纏めた結果を東京都指定様式のエクセルファイルに転記し、東京都へ報告している。 このたび、東京都環境局によるシステム「(仮称）適正管理制度オンラインシステム」を導入し、当該システムとの外部結合を行い、事業者及び区による東京都環境局への報告書の提出を行う。事業者がシステムに対応できない場合は、従来どおり紙での対応を行う。 ２　個人情報保護管理運営会議への付議内容 東京都環境局が導入する「(仮称）適正管理制度オンラインシステム」と区のイントラネットシステムとの外部結合 ３　対象者数 年間約５０件 ※個人情報の流れは、資料６３－１及び６３－２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　（仮称）適正管理制度オンラインシステムとの外部結合について

保有課（担当課）	環境対策課
登録業務の名称	（仮称）適正管理制度オンラインシステム
結合される情報項目（だれの、どのような項目か）	・事業者の氏名、住所 ・担当者氏名、電話番号、FAX 番号、メールアドレス
結合の相手方	（仮称）適正管理制度オンラインシステム（東京都環境局）
結合する理由	令和８年４月から、東京都環境局が導入を進める当システムを介して、環境確保条例第１１０条に基づく適正管理化学物質の報告制度の運用が行われるため、事業者は当システムを利用して報告を行うこととなる。区は、事業者からの報告を当システムを利用して、事務処理を行う必要があるため、当システムとの外部結合を行う。
結合の形態	LGWAN 回線を介して、区イントラネットシステムと東京都環境局が管理・運用する当システムを結合する。
結合の開始時期と期間	令和８年４月１日から運用開始を予定しており、次年度以降も、同様の外部結合を行う。なお、試用期間として、令和8年2月1日から令和8年2月28日を予定しているため、本件承認後、ユーザーテストを実施する。
情報保護対策	別紙チェックリストのとおり

（仮称）適正管理制度オンラインシステムに係る個人情報の流れ （オンライン申請）

（資料６３－１）

事業者

【インターネット回線】

通信暗号化

①専用サイトからの報告（web）

⑤修正依頼連絡（メール）

⑥修正内容報告

⑩報告完了連絡（メール）

東京都環境局

（仮称）適正管理制度オンラインシステム

事業者氏名、住所、担当者
メールアドレス、電話番号等

・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

【LGWAN回線】

通信暗号化

②報告内容の確認

④報告内容に不備がある場合、修正依頼

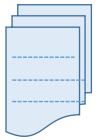
⑦修正内容の確認

⑨審査完了報告

新宿区

【区イントラPC】

③報告内容の審査



⑧修正内容再審査

・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

（仮称）適正管理制度オンラインシステムに係る個人情報の流れ　（紙申請）

（資料６３－２）

事業者

①報告書の提出
（郵送・窓口）

③報告内容に不備がある場合修正連絡

④必要に応じて資料追加提出
（郵送・窓口）

新宿区

【区イントラPC】

②報告内容の確認

⑤報告内容の審査

・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

【LGWAN回線】

通信暗号化

⑥報告内容入力及び審査完了報告

東京都環境局

（仮称）適正管理制度オンラインシステム

事業者氏名、住所、担当者
メールアドレス、電話番号等

・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

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。