資料32

個人情報保護管理運営会議　付議事項

件名	IHEAT.JP の利用に係る外部結合について

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：健康部保健予防課）

事業の概要

事業名	IHEAT.JP を用いた IHEAT の運用
担当課	保健予防課
目　的	IHEAT.JP により IHEAT 要員の名簿や研修受講管理等を行い、感染症まん延時等の健康危機発生時には、速やかに IHEAT 要員による支援を受けられる体制を整えるため。
対象者	新宿区を第１支援自治体として IHEAT に登録している要員 ※第１支援自治体とは、対象者が登録した居住地又は勤務地の保健所設置自治体
事業内容	１　概要 令和２年９月、厚生労働省は、新型コロナウイルス感染症の感染拡大により更なる保健所の体制強化が求められたことを踏まえ、都道府県単位で潜在保健師等を登録する人材バンクを創設し、支援の要請があった保健所等に対し潜在保健師等を派遣する仕組み（IHEAT）の運用を開始した。 令和４年１２月には、地域保健法の改正により IHEAT は法定化され、地域保健対策の推進に関する基本的な指針において、保健所設置自治体は、IHEAT 要員による支援体制を確保することとされた。 これらを踏まえた IHEAT 運用要領の改正（令和６年６月）を受け、潜在保健師等の登録は、保健所設置自治体毎に行うこととされ、名簿及び研修管理、感染症発生時の支援要請等についても、保健所設置自治体において、IHEAT.JP（IHEAT 運用支援システム）を用いて行うこととなった。 ※IHEAT は、感染症のまん延等の健康危機が発生した場合に、地域の保健師等の専門職が保健所等の業務を支援する仕組みであり、医師、保健師、看護師などが、保健所等への支援を行う IHEAT 要員として登録する。 ２　個人情報保護管理運営会議への付議内容 IHEAT 要員の名簿登録・研修・支援要請等の管理を行うため、当該システムとの外部結合を行う。 ３　対象者数 約２０人 ※個人情報の流れは、資料３２－１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　IHEAT.JP の利用に係る外部結合について

保有課（担当課）	保健予防課
登録業務の名称	IHEAT 要員の情報の登録・管理
結合される情報項目（だれの、どのような項目か)	１　個人の範囲 IHEAT 登録要員 ２　情報項目 氏名、生年月日、電話番号、住所（郵便番号及び区市町村まで） 勤務先、所有資格、メールアドレス
結合の相手方	IHEAT 事務局（日本公衆衛生協会）
結合する理由	IHEAT 要員の名簿登録・研修・支援要請等の管理を行うため、当該システムとの外部結合を行う。
結合の形態	区のイントラ PC を用い、インターネット回線を介して、IHEAT.JP のサーバと結合を行う。
結合の開始時期と期間	令和６年９月２日から令和７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

IHEAT.JPの利用に係る個人情報の流れ

（資料３２－１）

対象者

【インターネット回線】

通信暗号化

①IHEAT要員の申請

LoGoフォーム

②IHEAT要員の申請データを収受

【LoGoフォームのサーバ】

IHEAT要員の登録情報

・氏名・生年月日
・住所・電話番号
・メールアドレス
・勤務先
・所有資格

・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

【LGWAN回線】

③申請情報をダウンロード

新宿区

④ IHEAT要員の登録

【区イントラPC】

IHEAT要員の登録情報

・氏名・生年月日
・住所・電話番号
・メールアドレス
・勤務先
・所有資格

※IHEAT要員の登録後に、 IHEAT要員の登録情報が変更となる場合には、IHEAT事務局よりIDなどを付与されたIHEAT要員が直接IHEAT.JPに変更内容を入力します。区は適宜、登録情報を把握します。

【インターネット回線】

通信暗号化

⑤ IHEAT要員データの入力

⑦ IHEAT.JPに登録されている情報を適宜確認

IHEAT事務局（日本公衆衛生協会）

⑥ IHEAT要員データの確認

【IHEAT.JP】

IHEAT要員の登録情報

・氏名・生年月日
・住所・電話番号
・メールアドレス
・勤務先
・所有資格

・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

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。