資料59

個人情報保護管理運営会議　付議事項

件名	データ共有・交換システム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：総合政策部行政管理課、情報システム課）

事業の概要

事業名	効果的・効率的な業務の推進
担当課	行政管理課、情報システム課
目　的	データ共有・交換システムを導入することで、紙やＵＳＢメモリ等の外部記録媒体の紛失による個人情報の流出事故の防止やデータ共有・交換における事務の効率化を図る。
対象者	データ共有・交換システムでデータを交換することとなる業務の関係者
事業内容	１　概要 現在、区では、庁外の関係者とデータ共有・交換を行う際には、紙媒体の郵送のほか、メールやどこでもキャビネット、パスワード付の外部記録媒体（USB メモリ、CD-R 等）等を利用している。しかし、個人情報を含むデータや 5MB 以上の大容量のデータの交換方法は限られており、迅速なデータ共有・交換が出来ない状態である。また、外部記録媒体（USB メモリ、CD-R 等）等については、パスワード付としているが、依然として紛失による個人情報の流出事故リスクが残っている。 このため、紛失による流出事故の防止やデータ共有・交換における事務の効率化に向けたデータ共有・交換ツール（BOX）を活用する。今後は、以下のとおり、個人情報保護管理運営会議（以下「本会議」という。）へ付議することとする。 データ共有・交換ツール活用での付議パターン ⑴ 令和７年４月以降、新たに委託事業者や指定管理者などとの間でデータ共有・交換ツールを活用し、個人情報の受渡しをする場合は、すべて本会議に付議する。 ⑵ これまでは、委託事業者や指定管理者などとの間で USB メモリなどの受渡しをしていた事業で、令和７年４月以降はデータ共有・交換ツールを活用する場合は、追加手続ごとに一覧表にまとめ、令和７年４月以降の本会議に付議する。 ⑶ このほか、附属機関の委員などと個人情報を含む資料の受渡しをする場合、各種手続の申請者など（不特定多数を除く）からの資料の提出を受ける場合、区職員による庁外での資料を確認する場合等においては、本会議への事前の付議を不要とし、所定の様式で管理を行い、事後にまとめて本会議に報告する。（年１回） ２　個人情報保護管理運営会議への付議内容 データファイルの共有や閲覧のため、データ共有・交換システムと外部結合を行うことで、事業者等との間における受渡しの安全性を確保する。 ※個人情報の流れは、資料５９－１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　データ共有・交換システムの利用に係る外部結合について

保有課（担当課）	業務所管課（担当課：行政管理課、情報システム課）
登録業務の名称	データ共有・交換システムの運用
結合される情報項目（だれの、どのような項目か）	氏名、住所、生年月日、年齢、性別、連絡先、国籍、本籍、所属、続柄、建築物の図面情報、財産情報、資格・免許情報、その他手続にあたり必要な情報
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	当該システムは区でもすでに利用していることに加え、内閣官房や文部科学省などでも利用されており、高品質なサービスやセキュリティを廉価な提供を実現しているため。また、同システムを活用することで、紙やＵＳＢメモリ等の外部記録媒体の紛失による個人情報の流出事故の防止やデータ共有・交換における事務の効率化を図ることができるため。
結合の形態	区はLGWAN回線を利用して、当該システムが提供されるクラウドサーバと区のイントラネット端末を接続する。 なお、事業者側はインターネット回線から同一のクラウドストレージの利用ができる。
結合の開始時期と期間	令和７年４月１日から令和８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

（資料５９－１）

データ共有・管理システムに係る個人情報の流れ

・ウイルス感染の防止
・不正な通信の検知、分析、遮断
・ネットワーク機器の制限及び
　アクセスの制御
・ID／パスワード認証

・特定相手以外の通信不可
・通信内容の暗号化
・ＩＤ／パスワード等認証
・ファイルのパスワード設定
・アクセスログ取得、分析
・サーバ冗長化
・入退室管理
・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）
・ネットワーク機器等制御による通信限定
・ウィルス対策
・最新のパターンファイルの適用
・アクセス制御
・システムネットワーク状態等の監視
・バックアップ
・国内法が適用されるサーバ環境

他自治体
無関係の事業者等

区からアクセスを許可された事業者等以外は、保存されているフォルダ及びファイルにアクセスできない

・特定相手以外の通信不可
・通信内容の暗号化
・ＩＤ／パスワード等認証
・ファイルのパスワード設定
・アクセスログ取得、分析
・サーバ冗長化
・入退室管理
・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）
・ネットワーク機器等制御による通信限定
・ウィルス対策
・最新のパターンファイルの適用
・アクセス制御
・システムネットワーク状態等の監視
・バックアップ
・国内法が適用されるサーバ環境

事業者等

事業者パソコン等

＜主な利用機能＞
●データの共有
●閲覧・編集
●ダウンロード

申請情報　審査情報
財産情報　事業関連情報

【インターネット回線】

通信暗号化
①資料の送信
③資料の修正等
②'資料の確認
③'資料のダウンロード(※)

データ共有・交換システム（クラウドストレージ）

ISMAP登録済、ISMSクラウドセキュリティ認証取得済み

＜主な機能＞
① アカウント管理機能
② ファイルの共有機能
③ ファイルの閲覧・編集機能
④ アクセス制限機能
⑤ ダウンロード制限機能
⑥ 自動削除機能
※ ③～⑥の設定はフォルダ・ファイル毎に設定可能

申請情報　審査情報
財産情報　事業関連情報

【LGWAN回線】

ファイルの無害化
②資料の確認
④資料のダウンロード
①'資料の送付

新宿区

区イントラネットパソコン（LGWAN端末）

＜主な利用機能＞
●アカウントの管理
●データの共有
●閲覧・編集
●ダウンロード
●権限の設定

申請情報　審査情報
財産情報　事業関連情報

※区がアップロードしたファイルの編集権限、ダウンロード制限はファイル毎に可能

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。