資料31

個人情報保護管理運営会議　付議事項

件名	クラウドストレージサービス（Box）の利用に係る外部結合について（情報項目の追加）

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：総合政策部区政情報課、情報戦略課、
総務部税務課）

事業の概要

事業名	クラウドストレージサービスの導入による個人情報の流出事故防止
担当課	区政情報課、情報戦略課、税務課
目　的	クラウドストレージサービス（Box）（以下「Box」という。）を導入することで、外部記録媒体（CD-R やUSB メモリなど）（以下「記録媒体」という。）の紛失による個人情報の流出事故防止やデータ共有・交換における事務の効率化を図る。
対象者	資料３１－１の手続きの申請者
事業内容	１　概要 現在、区では、委託事業者などとの間で個人情報を含むデータの受渡しを行う際は、記録媒体を用いたデータの受渡しを多く行っている。その記録媒体は、パスワードを設定するなど一定のセキュリティ対策を講じているものの、持ち運びや保管の過程で紛失するリスクが常にあり、個人情報の流出事故につながる恐れがあった。 こうした課題を踏まえ、委託事業者などとの間で個人情報を含む記録媒体の受渡しをしている事業について、今後は、より高い安全性を確保できるBox を活用したデータの受渡しに変更する場合は、区政情報課が一括して管理運営会議への付議を行うこととなった。（令和６年度第１２回個人情報保護管理運営会議承認済） ついては、今まで記録媒体での受け渡しをしていた事業について、今後はBox を活用したデータの受渡しに変更するものを個人情報保護管理運営会議に一括して付議することとする。 このたび、取り扱う個人情報項目が追加となったため、管理運営会議への付議を行う。(Box へのデータの受け渡しについては令和７年第１０回個人情報保護管理運営会議承認済) ２　個人情報保護管理運営会議への付議内容 Box による受渡しに変更する資料３１－１の手続について、LGWAN 回線を利用し、区のイントラネット端末との外部結合を行う。 ※個人情報の流れは、資料３１－２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　クラウドストレージサービス（Box）の利用に係る外部結合について

※太字ゴシック（下線）が、令和８年度第４回新宿区個人情報保護管理運営会議承認済の内容からの変更箇所

保有課（担当課）	区政情報課、情報戦略課、税務課
登録業務の名称	追加する手続（登録業務）は、資料３１－１のとおり
結合される情報項目（だれの、どのような項目か）	**追加する手続ごとの情報項目は、資料３１－１のとおり**
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、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８年９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

【資料３１－１】

【変更手続及び情報項目】

No	担当課	手続名（登録業務名）	取扱う個人情報項目	付議内容
1	税務課	特別区民税・都民税・森林環境税　特徴封入封緘業務	氏名、住所、所得及び控除内訳、税額	受託業者との間で左記個人情報を受け渡しするため

（資料３１－２）

クラウドストレージサービス（Box)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　・ネットワーク機器等制御による通信限定
・通信内容の暗号化　・ウィルス対策
・ＩＤ／パスワード等認証　・最新のパターンファイルの適用
・ファイルのパスワード設定　・アクセス制御
・アクセスログ取得、分析　・システムネットワーク状態等の監視
・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
・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）

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　・ネットワーク機器等制御による通信限定
・通信内容の暗号化　・ウィルス対策
・ＩＤ／パスワード等認証　・最新のパターンファイルの適用
・ファイルのパスワード設定　・アクセス制御
・アクセスログ取得、分析　・システムネットワーク状態等の監視
・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
・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）

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(※)

クラウドストレージサービス（Box）

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。