

入学予定者名簿等の紛失及び再発防止策について

1 事案の概要

令和2年4月分の豊島区立小中学校入学予定者名簿のうち、中学校1校分(288人)の名簿等を紛失した事案。

入学予定者名簿は、教育部学務課において各学校分を印刷し、10月10日(木)に文書交換便で写しを各学校に配送(原本は学務課で保存)した。

その後、10月16日(水)に当該中学校から未着の連絡が学務課に入り、学務課及び当該中学校で名簿を捜索し、さらに全小中学校、文書交換便ルート上の全施設で名簿が誤配されていないか確認したが発見できなかった。名簿は現在も発見されていない。10月23日(水)、池袋警察署に遺失届を提出済み。

2 全庁調査の実施

本事案の発生を受けて、文書交換便における個人情報の受発信の実態把握及び個人情報の紛失等を防ぐ安全確保措置の実施状況を把握するために全庁調査を実施した。

<個人情報を含む書類等の文書交換便での利用状況調査>

- ① 調査期間 令和元年10月28日(月)～11月7日(木)
- ② 調査対象 文書交換便を利用しているすべての職場
- ③ 調査結果

個人情報の送受信		件数	安全確保措置
あり	37課(60.7%)	452件 ・申請書等 ・対象者リスト等	あり 289件 なし 163件
なし	24課(39.3%)		
計	61課(100.0%)		

※安全確保措置

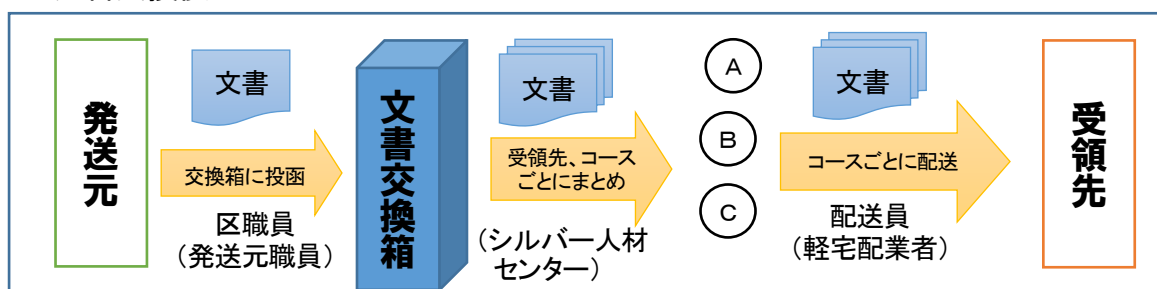
- ・専用ケース(カギ付き) 58件
- ・専用ケース(カギ無し) 231件
- ・メールでの受発信確認 144件

3 問題点

- (1) 個人情報の紛失等を予防するための安全確保措置が徹底されていなかった
 - ・専用バッグや施錠等の安全確保措置が取られていないケースがある
 - ・情報の受発信に関する経過が残っていないケースがある

- (2) 文書交換便で個人情報を含む書類等を受発信する際のルールが不徹底だった
- ・マイナンバーを含む特定個人情報については、ルール徹底済み
(原則として文書交換便は利用不可。ただし、施錠できる専用バッグを利用し、受発信先の押印で経過を残す等の措置を講じた場合は利用可能。)
 - ・その他の個人情報については、ルールが徹底されていなかった。
- (3) セキュリティポリシーの順守状況にばらつきがある
- ・安全確保措置を実施して交換便を利用している職場もあるが、今回のように十分な措置を実施していない職場もあった。

<文書交換便のイメージ>



4 再発防止策

以下のとおり個人情報を受発信する際のルールを定め、全庁に周知徹底する。

(1) 原則としてメールを活用する

対象者リスト等のデータ送信可能な個人情報は、データにパスワードの保護をかけたうえでメール送付する（区長部局では庁内メール、教育部では校務支援システムを活用）。

(2) 文書交換便を利用する際の安全確保措置を徹底する

申請書の原本など紙ベースで個人情報を受発信する必要がある場合に限り、安全確保措置を取ったうえで文書交換便の利用を認める。

<安全確保措置>

① 配送員からの直接受領の徹底

- ・受領先の職員は、文書交換便の配送員から直接送付物を受け取ることとする（送付物に個人情報が含まれているか否かを問わない）。
※所定の場所に置いておく等の取り扱いは厳禁とする。
- ・配送員は、配送時に受領先職員の受領印（サイン）をもらうこととする。
- ・配送時に、受領先の職員に手渡しできない場合には、配送員は送付物を持ち帰るものとする（翌日に再配送する）。

② 専用袋の使用

- ・ファスナー付きのビニール製袋等、専用袋を使用する。
- ・鍵の使用については、各課の判断とする。

(3) 個人情報の受発信連絡の徹底

メール送信、文書交換便利用の別を問わず、個人情報を含む書類の発送元は、必ず事前に、原則としてメールで受領先に発送連絡を行い、受領先は、受領時に発送元に受領連絡をする（連絡は必要に応じて電話も可とする）。

メールの送信先は相手方の「課長（CC:課アドレス）」とし、メール送信課の課長にも CC：で共有する。教育委員会もこれに準じて運用する。

発送元、受領先共に受発信の経過を残す。

(4) 情報セキュリティポリシーに基づく実施手順書の作成及び周知徹底

情報セキュリティポリシーに基づいて、以上の個人情報を受発信する際のルールを全ての職場で実施手順書に定め、職員に周知徹底する。

5 区への対応

(1) 再発防止策の全庁への徹底

11月18日（月） 未来戦略推進会議、庶務担当課長会、校長会で周知

※ 11月中に対策を完了させ、結果をコンプライアンス担当課長に報告させる

(2) 区民・議会への報告

- ・第4回区議会定例会初日（11月19日）の議員協議会で議会報告
- ・同日付で区公式HP等を通じて区民に周知

(3) 内部統制方針等への反映、職員研修の実施等

「豊島区リスクマネジメント指針」において、重大な危機事象（リスク）として「公文書の紛失・データ消失」や「個人情報漏えい及び不適切利用」を定め、リスクが発生した場合の報告及び再発防止等の対応について定めているが、今後、より実効性を持った内部統制方針を策定し、安全確保へ繋がるような意識付けや研修会を開催する。

<参考> 個人情報保護に関する規定類

(1) 「豊島区個人情報等の保護に関する条例」

個人情報の紛失等を予防する安全確保措置を講じることを義務付け

(2) 「豊島区情報セキュリティ対策基準（セキュリティポリシー）第3部職員編」

個人情報を含む重要情報資産の持ち出しは原則として禁止

「豊島区個人情報等の保護に関する条例」<抜粋>

(保有個人情報の安全及び正確性の確保)

第7条 実施機関は、保有個人情報の漏えい、紛失、改ざん及びき損の防止、保有個人情報への不正なアクセスの防御その他の保有個人情報の安全な管理のために必要な措置(以下「安全確保の措置」という。)を講じなければならない。(以下、略)

※第14条 (委託先に対しても個人情報の取扱いに関する安全確保を講じることを義務付け)

「豊島区情報セキュリティ対策基準（セキュリティポリシー）第3部職員編」〈抜粋〉

3. 情報資産の管理方法

(6) 情報資産の持ち出し

原則として重要情報資産の持ち出しは禁止とする。ただし、業務上必要であり情報化推進責任者（所管課長）の許可を得た場合は、次の対策を行うこととする。

- ①持ち出し時には記録を残す。
- ②必要に応じ鍵付きのケース等に格納
- ③暗号化又はパスワードの設定を行う