

特定個人情報保護評価書(全項目評価書)

評価書番号	評価書名
1	特別支援教育就学奨励事業、高等学校等就学支援金制度、東京都立高等学校等学び直し支援金事業及び東京都立学校等給付型奨学金事業に関する事務に係る特定個人情報保護評価書(全項目評価書)

個人のプライバシー等の権利利益の保護の宣言

東京都教育委員会は、特別支援教育就学奨励事業、高等学校等就学支援金事業、東京都立高等学校等学び直し支援金事業及び東京都立学校等給付型奨学金事業に関する事務において、個人番号を利用するに当たり、特定個人情報の不適正な取扱いが個人のプライバシー等の権利利益に影響を及ぼしかねないことを認識し、特定個人情報の漏えいその他の事態を発生させるリスクを軽減するために適切な措置を講じ、もって個人のプライバシー等の権利利益の保護に取り組むことを宣言する。

特記事項

しきい値判断では基礎項目評価及び重点項目評価の実施が義務付けられているが、より適切な特定個人情報の保護を確保するため、全項目評価を実施する。

評価実施機関名

東京都教育委員会

個人情報保護委員会 承認日【行政機関等のみ】

公表日

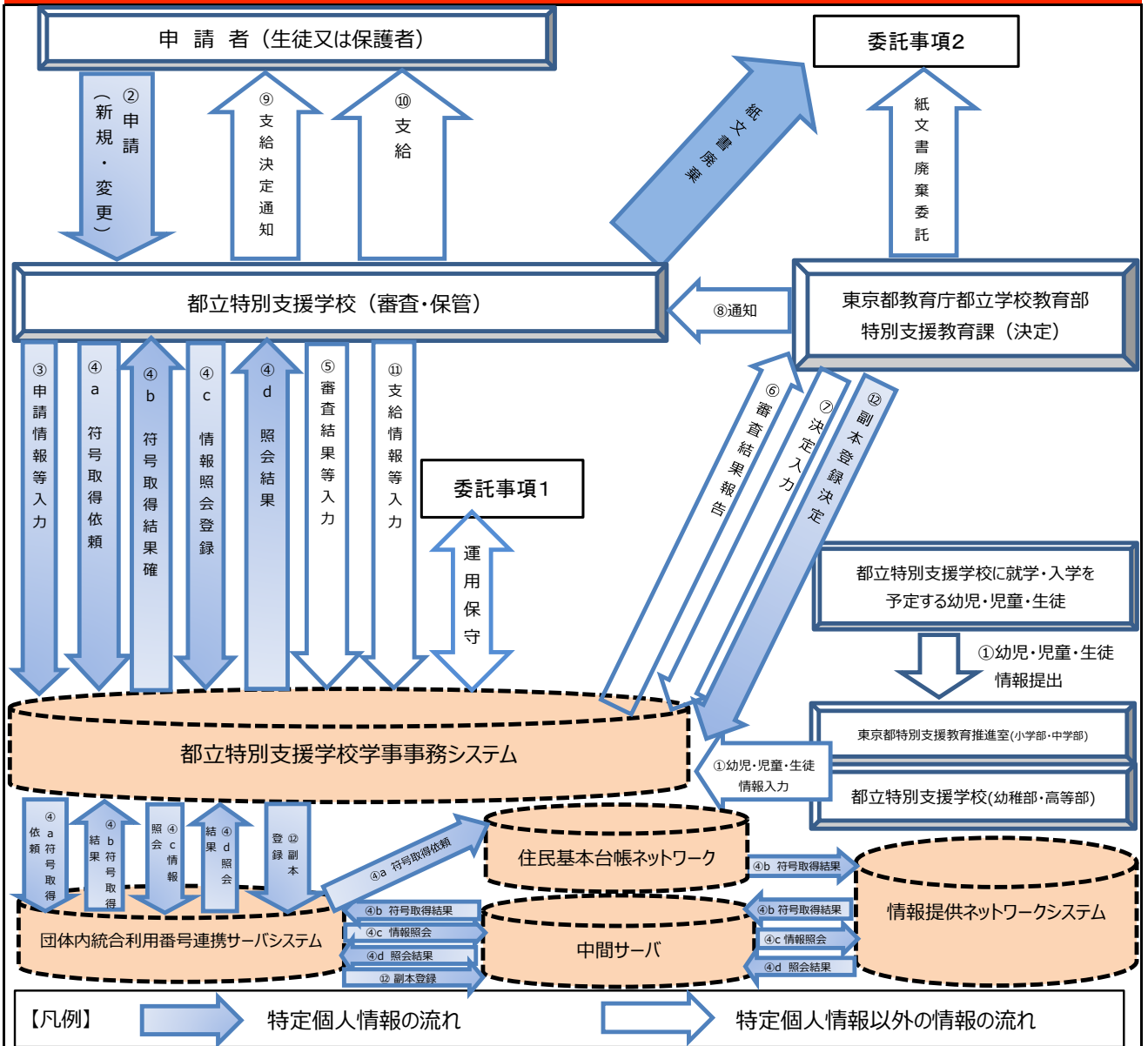
項目一覧

I 基本情報
(別添1) 事務の内容
II 特定個人情報ファイルの概要
(別添2) 特定個人情報ファイル記録項目
III 特定個人情報ファイルの取扱いプロセスにおけるリスク対策
IV その他のリスク対策
V 開示請求、問合せ
VI 評価実施手続
(別添3) 変更箇所

システム3	
①システムの名称	中間サーバ
②システムの機能	<ul style="list-style-type: none"> ・符号及び団体内統合利用番号の取得、管理 ・符号、団体内統合利用番号、個別業務システム利用番号の紐付管理 ・副本管理 ・情報照会の受付及び管理 ・情報提供の管理
③他のシステムとの接続	<input type="checkbox"/> 情報提供ネットワークシステム <input type="checkbox"/> 庁内連携システム <input type="checkbox"/> 住民基本台帳ネットワークシステム <input type="checkbox"/> 既存住民基本台帳システム <input type="checkbox"/> 宛名システム等 <input type="checkbox"/> 税務システム <input type="checkbox"/> その他（団体内統合利用番号連携サーバ）
システム4	
①システムの名称	住民基本台帳ネットワークシステム
②システムの機能	<ul style="list-style-type: none"> ・本人確認情報の更新・管理・全国サーバに対する更新通知 ・本人確認の情報抽出・出力 ・全国サーバへの情報照会
③他のシステムとの接続	<input type="checkbox"/> 情報提供ネットワークシステム <input type="checkbox"/> 庁内連携システム <input type="checkbox"/> 住民基本台帳ネットワークシステム <input type="checkbox"/> 既存住民基本台帳システム <input type="checkbox"/> 宛名システム等 <input type="checkbox"/> 税務システム <input type="checkbox"/> その他（団体内統合利用番号連携サーバ）
3. 特定個人情報ファイル名	
特別支援学校学事事務ファイル	
4. 特定個人情報ファイルを取り扱う理由	
①事務実施上の必要性	<ul style="list-style-type: none"> ・支給の可否の審査に当たり、幼児、児童又は生徒の属する世帯の所得情報等を確認し、審査を行う必要があるため。 ・就学奨励費の支給情報について、他団体からの照会に対応するため。
②実現が期待されるメリット	<ul style="list-style-type: none"> ・就学奨励費、就学支援金、学び直し支援金及び給付型奨学金の申請時において、課税証明書等の提出が省略される等、各制度の利用者における利便性向上を図る。
5. 個人番号の利用 ※	
法令上の根拠	行政手続における特定の個人を識別するための番号の利用等に関する法律（以下「番号法」という。） 第9条第1項 別表第一 26の項及び91の項 番号法別表第一の主務省令で定める事務を定める命令 第22条及び第66条 番号法第9条第2項 番号法に基づく個人番号の利用並びに特定個人情報の利用及び提供に関する条例第4条 別表第一及び第二

6. 情報提供ネットワークシステムによる情報連携 ※	
①実施の有無	<div style="display: flex; justify-content: space-between; align-items: center;"> [実施する] <div style="text-align: right; font-size: small;"> <選択肢> 1) 実施する 2) 実施しない 3) 未定 </div> </div>
②法令上の根拠	<p>【情報照会】 番号法第19条第7号 別表第二 37の項及び113の項 番号法別表第二の主務令で定める事務及び情報を定める命令 第23条各号及び第58条各号 番号法第19条第8号 番号法に基づく個人番号の利用並びに特定個人情報の利用及び提供に関する条例第4条 別表第一</p> <p>【情報提供】 番号法第19条第7号 別表第二 26の項及び87の項 番号法別表第二の主務省令で定める事務及び情報を定める命令 第19条各号及び第44条各号</p> <p>なお、就学支援金については文部科学省の見解を踏まえ、情報提供は行わない。</p>
7. 評価実施機関における担当部署	
①部署	東京都教育庁都立学校教育部特別支援教育課
②所属長の役職名	特別支援教育課長
8. 他の評価実施機関	
—	

(別添1)事務の内容



(備考)

- ① 都立特別支援学校に入学・就学を予定する幼児・児童・生徒の新生基本情報について、入学手続時に提出された情報を基に、東京都特別支援教育推進室又は都立特別支援学校において都立特別支援学校学事事務システム(以下「学事事務システム」という。)を入力する。
 - ② 申請者(生徒又は保護者)がマイナンバー及び申請書類等を都立特別支援学校に提出する。提出を受けた学校は、添付資料等により申請者の番号確認及び身元確認を行い、個人番号を含む書類は、各校のキャビネット等で施錠保管する。
 - ③ 都立特別支援学校は申請内容に基づき、マイナンバーを含む申請情報等を入力する。
 - ④ 都立特別支援学校は、学事事務システムから連携サーバへ符号取得依頼を行う(a)。符号取得後(b)、学事事務システムから自動で情報提供ネットワークシステムを通じた他団体への情報照会を行い(c)、取得した地方税関係情報等(d)を学事事務システムに取り込む。※(c)(d)は庁内連携を含む。
 - ⑤ 情報提供ネットワークシステムを通じた他団体への情報照会結果に基づき、学校は学事事務システム上で審査を行い、審査結果等を入力する。
 - ⑥ 審査結果を学事事務システム上で、電子帳票配信により、特別支援教育課へ報告する。
 - ⑦ 特別支援教育課は、報告内容を学事事務システム上で確認し、決定の入力を行う。
 - ⑧ 特別支援教育課は、学校に対し決定通知を行う。
 - ⑨ 学校は、特別支援教育課からの決定通知に基づき、申請者に対し決定通知を行う。
 - ⑩ ⑤の審査結果等に基づき、学校は申請者ごとの支給額を算定し、申請者に支給する。
 - ⑪ 学校は、支給情報等について、学事事務システムに入力する。
 - ⑫ 庁内連携を含む他団体への情報提供を行うため、就学奨励費の支給状況について、特別支援教育課の承認に基づき、学事事務システムから連携サーバを通じて中間サーバに副本登録する。
- ※個人番号紙媒体の保存期間満了後、廃棄に当たっては、特別支援教育課又は各校で意思決定を行い、書類を溶解、焼却、裁断等復元不可能な方法により廃棄する。

II 特定個人情報ファイルの概要

1. 特定個人情報ファイル名	
特別支援学校学事事務ファイル	
2. 基本情報	
①ファイルの種類 ※	[システム用ファイル] <選択肢> 1) システム用ファイル 2) その他の電子ファイル(表計算ファイル等)
②対象となる本人の数	[1万人以上10万人未満] <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
③対象となる本人の範囲 ※	就学奨励費については、都立特別支援学校に在籍する申請者(幼児・児童・生徒の保護者)及びその同一世帯に属する者とし、就学支援金、学び直し支援金及び給付型奨学金については申請者(生徒)及びその保護者とする。
その必要性	・支給の可否の審査に当たり、幼児、児童又は生徒の属する世帯の所得情報等を確認し、審査を行う必要があるため。 ・就学奨励費の支給情報について、他団体からの照会に対応するため。
④記録される項目	[10項目以上50項目未満] <選択肢> 1) 10項目未満 2) 10項目以上50項目未満 3) 50項目以上100項目未満 4) 100項目以上
主な記録項目 ※	<ul style="list-style-type: none"> ・識別情報 [<input type="checkbox"/>] 個人番号 [<input type="checkbox"/>] 個人番号対応符号 [<input type="checkbox"/>] その他識別情報(内部番号) ・連絡先等情報 [<input type="checkbox"/>] 4情報(氏名、性別、生年月日、住所) [<input type="checkbox"/>] 連絡先(電話番号等) [<input type="checkbox"/>] その他住民票関係情報 ・業務関係情報 [<input type="checkbox"/>] 国税関係情報 [<input type="checkbox"/>] 地方税関係情報 [<input type="checkbox"/>] 健康・医療関係情報 [<input type="checkbox"/>] 医療保険関係情報 [<input type="checkbox"/>] 児童福祉・子育て関係情報 [<input type="checkbox"/>] 障害者福祉関係情報 [<input type="checkbox"/>] 生活保護・社会福祉関係情報 [<input type="checkbox"/>] 介護・高齢者福祉関係情報 [<input type="checkbox"/>] 雇用・労働関係情報 [<input type="checkbox"/>] 年金関係情報 [<input type="checkbox"/>] 学校・教育関係情報 [<input type="checkbox"/>] 災害関係情報 [<input type="checkbox"/>] その他 ()
その妥当性	<ul style="list-style-type: none"> ・個人番号:他機関との情報連携のために保有 ・その他識別情報(内部番号):対象者を正確に特定するために保有 ・連絡先等情報:対象者を正確に特定するために保有 ・その他住民票関係情報:保護者等他の世帯員との続柄を確認するため保有 ・地方税関係情報、生活保護・社会福祉関係情報:就学奨励費、就学支援金、学び直し支援金又は給付型奨学金(以下「就学奨励費等」という。)の支給の可否を審査するために保有 ・健康・医療関係情報、障害者福祉関係情報:就学奨励費及び給付型奨学金の対象であることの確認のため保有 ・学校・教育関係情報:対象者の在籍する学校名を特定するために保有
全ての記録項目	別添2を参照。
⑤保有開始日	平成30年4月
⑥事務担当部署	東京都教育庁都立学校教育部特別支援教育課

3. 特定個人情報の入手・使用													
①入手元 ※	<input checked="" type="checkbox"/> 本人又は本人の代理人 <input type="checkbox"/> 評価実施機関内の他部署 () <input type="checkbox"/> 行政機関・独立行政法人等 () <input checked="" type="checkbox"/> 地方公共団体・地方独立行政法人 (都・各区市町村) <input type="checkbox"/> 民間事業者 () <input type="checkbox"/> その他 ()												
②入手方法	<input checked="" type="checkbox"/> 紙 [] 電子記録媒体(フラッシュメモリを除く。) [] フラッシュメモリ <input type="checkbox"/> 電子メール [] 専用線 [<input checked="" type="checkbox"/>] 庁内連携システム <input checked="" type="checkbox"/> 情報提供ネットワークシステム <input type="checkbox"/> その他 ()												
③入手の時期・頻度	<ul style="list-style-type: none"> ・就学奨励費:各学部入学時1回(4月から6月) ・就学支援金(学び直し支援金):高等部入学時1回(4月から5月) ・給付型奨学金:高等部入学時1回(4月から5月) ・各業務転入時は随時 												
④入手に係る妥当性	<ul style="list-style-type: none"> ・就学奨励費の支給の可否の審査に当たっては、東京都特別支援学校就学奨励事業実施要綱第6条及び第7条により、世帯の地方税関係情報等が必要となる。 ・就学支援金の支給の可否の審査に当たっては、高等学校等就学支援金の支給に関する法律第3条及び第4条により、世帯の地方税関係情報等が必要となる。 ・学び直し支援金の支給の可否の審査に当たっては、東京都立高等学校等学び直し支援金の交付に関する要綱第4条から第7条までにより、世帯の地方税関係情報等が必要となる。 ・給付型奨学金の支給の可否の審査に当たっては、東京都立特別支援学校等における給付型奨学金の交付に関する要綱第4条により、世帯の地方税関係情報等が必要となる。 ・情報提供ネットワークシステムによる他団体との情報連携により、就学奨励費等の支給の可否の決定に必要な地方税関係情報等を取得する。 												
⑤本人への明示	<ul style="list-style-type: none"> ・就学支援金については、番号法第9条第2項及び法別表第一の91の項に規定されている。 ・学び直し支援金及び給付型奨学金については、番号法第9条第2項に基づき、番号法に基づく個人番号の利用並びに特定個人情報の利用及び提供に関する条例第4条及び別表第一及び第二に規定されている。 ・就学奨励費については、番号法第9条第1項及び法別表第一の26の項、並びに番号法に基づく個人番号の利用並びに特定個人情報の利用及び提供に関する条例第4条及び別表第一及び第二に規定されている。 ・いずれの制度においても、申請書の配布時等には、リーフレット、パンフレット等で特定個人情報の取扱いを案内するとともに、申請書の記載に当たり、注意事項を載せることで本人に明示する。 												
⑥使用目的 ※	就学奨励費、就学支援金、学び直し支援金又は給付型奨学金の支給の可否の審査のため。												
	<table border="1"> <tr> <td>変更の妥当性</td> <td>—</td> </tr> </table>	変更の妥当性	—										
変更の妥当性	—												
⑦使用の主体	<table border="1"> <tr> <td>使用部署 ※</td> <td>東京都教育庁都立学校教育部特別支援教育課(委託先及び再委託先を含む。)及び都立特別支援学校</td> </tr> <tr> <td>使用者数</td> <td> [1,000人以上] <table border="0"> <tr> <td colspan="2" style="text-align: center;"><選択肢></td> </tr> <tr> <td>1) 10人未満</td> <td>2) 10人以上50人未満</td> </tr> <tr> <td>3) 50人以上100人未満</td> <td>4) 100人以上500人未満</td> </tr> <tr> <td>5) 500人以上1,000人未満</td> <td>6) 1,000人以上</td> </tr> </table> </td> </tr> </table>	使用部署 ※	東京都教育庁都立学校教育部特別支援教育課(委託先及び再委託先を含む。)及び都立特別支援学校	使用者数	[1,000人以上] <table border="0"> <tr> <td colspan="2" style="text-align: center;"><選択肢></td> </tr> <tr> <td>1) 10人未満</td> <td>2) 10人以上50人未満</td> </tr> <tr> <td>3) 50人以上100人未満</td> <td>4) 100人以上500人未満</td> </tr> <tr> <td>5) 500人以上1,000人未満</td> <td>6) 1,000人以上</td> </tr> </table>	<選択肢>		1) 10人未満	2) 10人以上50人未満	3) 50人以上100人未満	4) 100人以上500人未満	5) 500人以上1,000人未満	6) 1,000人以上
使用部署 ※	東京都教育庁都立学校教育部特別支援教育課(委託先及び再委託先を含む。)及び都立特別支援学校												
使用者数	[1,000人以上] <table border="0"> <tr> <td colspan="2" style="text-align: center;"><選択肢></td> </tr> <tr> <td>1) 10人未満</td> <td>2) 10人以上50人未満</td> </tr> <tr> <td>3) 50人以上100人未満</td> <td>4) 100人以上500人未満</td> </tr> <tr> <td>5) 500人以上1,000人未満</td> <td>6) 1,000人以上</td> </tr> </table>	<選択肢>		1) 10人未満	2) 10人以上50人未満	3) 50人以上100人未満	4) 100人以上500人未満	5) 500人以上1,000人未満	6) 1,000人以上				
<選択肢>													
1) 10人未満	2) 10人以上50人未満												
3) 50人以上100人未満	4) 100人以上500人未満												
5) 500人以上1,000人未満	6) 1,000人以上												
⑧使用方法 ※	<p>学事事務システムにマイナンバーを登録し、情報提供ネットワークシステムを通じて他団体への情報照会を行い、地方税関係情報等を取得する。また、他団体から就学奨励費の支給に関する情報照会があった場合は、情報提供する。</p> <table border="1"> <tr> <td>情報の突合 ※</td> <td>審査において、申請内容と地方税関係情報等を突合する。</td> </tr> <tr> <td>情報の統計分析 ※</td> <td>特定個人情報を使用した分析は行っていない。</td> </tr> <tr> <td>権利利益に影響を与え得る決定 ※</td> <td> <ul style="list-style-type: none"> ・就学奨励費の支給認定に関する決定 ・就学奨励費の支給額の決定 ・就学支援金の支給認定に関する決定 ・就学支援金の支給額の決定 ・学び直し支援金の支給認定に関する決定 ・学び直し支援金の支給額の決定 ・給付型奨学金の支給認定に関する決定 ・給付型奨学金の支給額の決定 </td> </tr> </table>	情報の突合 ※	審査において、申請内容と地方税関係情報等を突合する。	情報の統計分析 ※	特定個人情報を使用した分析は行っていない。	権利利益に影響を与え得る決定 ※	<ul style="list-style-type: none"> ・就学奨励費の支給認定に関する決定 ・就学奨励費の支給額の決定 ・就学支援金の支給認定に関する決定 ・就学支援金の支給額の決定 ・学び直し支援金の支給認定に関する決定 ・学び直し支援金の支給額の決定 ・給付型奨学金の支給認定に関する決定 ・給付型奨学金の支給額の決定 						
情報の突合 ※	審査において、申請内容と地方税関係情報等を突合する。												
情報の統計分析 ※	特定個人情報を使用した分析は行っていない。												
権利利益に影響を与え得る決定 ※	<ul style="list-style-type: none"> ・就学奨励費の支給認定に関する決定 ・就学奨励費の支給額の決定 ・就学支援金の支給認定に関する決定 ・就学支援金の支給額の決定 ・学び直し支援金の支給認定に関する決定 ・学び直し支援金の支給額の決定 ・給付型奨学金の支給認定に関する決定 ・給付型奨学金の支給額の決定 												
⑨使用開始日	平成29年10月16日												

委託事項2～5		
委託事項2	文書廃棄処理委託	
①委託内容	保存期間を満了した特定個人情報を含む紙文書の溶解、焼却、裁断等廃棄処理委託	
②取扱いを委託する特定個人情報ファイルの範囲	[特定個人情報ファイルの一部] <選択肢> 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部	
	対象となる本人の数 [1万人以上10万人未満] <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上	
	対象となる本人の範囲 ※ 都立特別支援学校に在籍し、就学奨励費等を申請する幼児、児童若しくは生徒、又はその同一世帯に属する者	
	その妥当性 東京都教育委員会特定個人情報等取扱事務要綱に基づき、保存期間を満了した特定個人情報保護等を含む文書を委託により廃棄する場合には、必要な措置を講じなければならない。	
③委託先における取扱者数	[10人未満] <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上	
④委託先への特定個人情報ファイルの提供方法	[] 専用線 [] 電子メール [] 電子記録媒体(フラッシュメモリを除く。) [] フラッシュメモリ [○] 紙 [] その他 ()	
⑤委託先名の確認方法	ホームページ「東京都入札情報サービス」で公表している。	
⑥委託先名	未定	
再委託	⑦再委託の有無 ※ [再委託しない] <選択肢> 1) 再委託する 2) 再委託しない	
	⑧再委託の許諾方法	
	⑨再委託事項	

6. 特定個人情報の保管・消去

<p>①保管場所 ※</p>	<p>【紙書類】 各校で施錠可能なキャビネット等に保管し、その状況を台帳で管理している。また、特定個人情報取扱担当者(以下「取扱者」という。)のうち、各校の管理職又は経営企画室職員のみが内容を確認できる。</p> <p>【学事事務システム】 ・システムサーバは専用施設内に当該サーバ専用のラックに收容する。また、この区画への入退室管理は生体認証による入退室管理、区画ごとの施錠管理、監視カメラによる録画、有人監視等を実施する。 ・学事事務システムで使用する外部記録媒体は施錠保管している。また、外部記録媒体内のデータは使用が済んだらすぐさま削除している。</p> <p>【連携サーバ】 ①連携サーバはサーバ等を設置するための専用施設内に他のシステムとは分離した区画を設け、当該サーバ専用のラックに施錠して收容する。当該施設では、入室者管理、区画ごとの施錠管理、監視カメラによる録画、有人監視等を実施する。 ②当該施設の煙感知装置、ガス系消火設備、耐震対応等により、火災や地震に起因する滅失等のリスクを低減する。</p> <p>【中間サーバ・プラットフォーム】 ①中間サーバ・プラットフォームをデータセンターに設置している。データセンターへの入館及びサーバ室への入退室を行う際は、警備員などにより顔写真入りの身分証明書と事前申請の照合を行う。 ②特定個人情報は、サーバ室に設置された中間サーバのデータベース内に保存され、バックアップもデータベース上に保存される。</p>												
<p>②保管期間</p>	<p style="text-align: center;">＜選択肢＞</p> <table border="0" style="width: 100%;"> <tr> <td style="width: 33%;">1) 1年未満</td> <td style="width: 33%;">2) 1年</td> <td style="width: 33%;">3) 2年</td> </tr> <tr> <td>4) 3年</td> <td>5) 4年</td> <td>6) 5年</td> </tr> <tr> <td>7) 6年以上10年未満</td> <td>8) 10年以上20年未満</td> <td>9) 20年以上</td> </tr> <tr> <td colspan="3">10) 定められていない</td> </tr> </table> <p>[6年以上10年未満]</p>	1) 1年未満	2) 1年	3) 2年	4) 3年	5) 4年	6) 5年	7) 6年以上10年未満	8) 10年以上20年未満	9) 20年以上	10) 定められていない		
1) 1年未満	2) 1年	3) 2年											
4) 3年	5) 4年	6) 5年											
7) 6年以上10年未満	8) 10年以上20年未満	9) 20年以上											
10) 定められていない													
<p>その妥当性</p>	<p>紙書類については、東京都教育委員会文書管理規則の規定に基づき保存する。 学事事務システム内のデータについては、番号法施行令第29条に基づき7年間を保存期間とする。</p>												
<p>③消去方法</p>	<p>【紙書類】 保存期間満了後、東京都は意思決定の上、書類を溶解、焼却、裁断等復元不可能な方法により廃棄する。廃棄に当たっては、搬送から処理に至るまでの間、各校の取扱者が立ち会う。</p> <p>【学事事務システム】 ・学事事務システム内のデータについては、保存期間満了後やハード更改等の際は、システム運用保守受託者において、保存された情報が読み出しできないよう、物理的破壊または専用ソフト等を利用して完全に消去する。特別支援教育課は、システム運用保守受託者が確実にデータ消去したことについて、証明書等の提出を受ける。 ・外部記録媒体内のデータは使用が済んだらすぐさま削除している。</p> <p>【中間サーバ・プラットフォーム】 ①特定個人情報の消去は地方公共団体からの操作によって実施されるため、通常、中間サーバ・プラットフォームの保守運用を行う事業者が特定個人情報を消去することはない。 ②ディスク交換やハード更改等の際は、中間サーバ・プラットフォームの保守・運用を行う事業者において、保存された読み出しができないよう、物理的破壊又は専用ソフト等を利用して完全に消去する。</p> <p>【連携サーバ】 特定個人情報(副本相当)は中継されるのみであり、システム内に保有されない。なお、機器のうち特定個人情報等のデータが記録されるものの廃棄等に当たっては、磁氣的消去又は物理的破壊等により、当該データを復元不可能な状態とする。</p>												

7. 備考

—

(別添2) 特定個人情報ファイル記録項目

1. 年度
2. 学校名
3. 学部・学科
4. 分教室名
5. 学年・組
6. 本名／通称区分(児童生徒)
7. 児童生徒氏名カナ
8. 児童生徒氏名
9. 生年月日
10. 性別
11. 申請・認定状態
12. 申請年月日
13. 児童生徒コード
14. 障害種別
15. 本名／通称区分(保護者)
16. 保護者氏名カナ
17. 保護者氏名
18. 世帯員※氏名カナ
19. 世帯員氏名
20. 世帯員生年月日
21. 世帯員性別
22. 世帯員照会先機関
23. 世帯員マイナンバー
24. 世帯員コード
25. 利用事務
26. 照会年度
27. 団体内統合利用番号
28. 団体内統合利用番号の有無
29. 符号取得の有無
30. 住民票関係情報
31. 地方税関係情報
32. 生活保護実施関係情報
33. 自動応答の可否
34. 就学奨励費支給項目
35. 就学奨励費支給額
36. 文書番号
37. 決定日

※ 世帯員は、幼児、児童若しくは生徒、又はその同一世帯に属する者とする。

* 特定個人情報ファイル全体を要配慮個人情報と設定する。

Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※(7. リスク1⑨を除く。)

1. 特定個人情報ファイル名	
特別支援学校学事事務ファイル	
2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）	
リスク1： 目的外の入手が行われるリスク	
対象者以外の情報の入手を防止するための措置の内容	<ul style="list-style-type: none"> ・特定個人情報の入手は番号法令の規定の範囲内で認められたもののみとする。 ・支給認定を受けようとする者は、申請者の意思により申請を行うと、法令・要綱等において定める。 ・申請書の記載事項、様式については、要綱等において定める。 ・申請者が対象者以外の情報を記載することがないように、申請に当たっての記載例や注意事項を作成する。 ・申請受付については、申請にかかる幼児、児童又は生徒の在籍校にて行う。 ・申請書類の過不足を確認できるよう、リーフレット、手引等を作成するとともに、学校担当者向けの説明会を毎年度開催する。 ・団体内統合利用番号連携サーバシステム及び中間サーバを利用した庁内連携による入手は、関連業務システム以外からのアクセス制御を行っている。また、正当な権限のない利用者及び個別業務システム等からは、目的を超えた紐付けや必要のない情報は入手できないようアクセス制御を行っている。
必要な情報以外を入手することを防止するための措置の内容	申請者が不要な情報を記載することがないように、マイナンバーの提出様式及び封筒を指定し、記載例や注意事項を作成している。
その他の措置の内容	—
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2： 不適切な方法で入手が行われるリスク	
リスクに対する措置の内容	<ul style="list-style-type: none"> ・個人番号は利用目的を明示の上、収集する。 ・申請者は申請書、個人番号カード又は個人番号通知カードの写し及び本人確認書類を厳封して、原則として経営企画室へ持参又は郵送にて提出する。ただし、やむを得ず上記の方法によれない場合は、教員に提出し、教員は厳封されたまま経営企画室に提出する。なお、提出方法はいずれの場合も郵送に準ずる(管理職、経営企画室職員及び教員は、あらかじめ、取扱者に指定する。) ・経営企画室職員は封筒を開封し、添付資料により申請者の番号確認及び身元確認を行う。 ・経営企画室職員は封筒記載の情報を確認し、授受簿に記録する。 ・提出書類に不備があった場合等については、経営企画室職員が申請者又は生徒が申請者の場合はその保護者(以下「申請者等」という。)と直接やり取りを行う。 ・これらの手続きについては、業務マニュアルで記載する。 ・団体内統合利用番号連携サーバシステム及び中間サーバを利用した庁内連携による入手は、関連業務システム以外からのアクセス制御を行っている。また、正当な権限のない利用者及び個別業務システム等からは、目的を超えた紐付けや必要のない情報は入手できないようアクセス制御を行っている。
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク3： 入手した特定個人情報ที่ไม่正確であるリスク	
入手の際の本人確認の措置の内容	番号法第16条、行政手続における特定の個人を識別するための番号の利用等に関する法律施行令(以下、「番号法政令」という。)第12条第1項、行政手続における特定の個人を識別するための番号の利用等に関する法律施行規則(以下、「番号法施行規則」という。)第1条等の定めに基づき、本人確認は次の書類で確認する。①個人番号カードの写し(番号確認及び身元確認)②個人番号通知カード(番号確認※住所・氏名等に変更のないものに限る。)+運転免許証等(身元確認)③個人番号の記載された住民票の写し(番号確認)+運転免許証等(身元確認)
個人番号の真正性確認の措置の内容	経営企画室職員がマイナンバー収集用の封筒を開封し、申請者の番号確認及び身元確認を行う。番号法第16条、番号法政令第12条第1項、番号法施行規則第1条等の定めに基づき、真正性は次の書類で確認する。①個人番号カードの写し(番号確認及び身元確認)②個人番号通知カード(番号確認)+運転免許証等(身元確認)③個人番号の記載された住民票の写し(番号確認)+運転免許証等(身元確認)
特定個人情報の正確性確保の措置の内容	<ul style="list-style-type: none"> ・経営企画室職員が台帳及び封筒に、各個人に割り振られた番号を付し、保管する。 ・申請書類に不備があった場合等については、経営企画室職員が直接申請者等に確認を行う。 ・それぞれの事業について、年1回定められた時期に支給更新手続きが行われるため、その際に申請情報(個人番号を除く。)の確認を行う。 ・マイナンバーの学事事務システムへの入力は、経営企画室職員2名(導入時は委託事項1事業者の作業員2名)がそれぞれ行い、それぞれが入力した個人番号をシステム内で突合することで、入力ミスを防止する。 ・団体内統合利用番号連携サーバシステム及び中間サーバを利用した庁内連携による入手は、関連業務システム以外からのアクセス制御を行っている。また、正当な権限のない利用者及び個別業務システム等からは、目的を超えた紐付けや必要のない情報は入手できないようアクセス制御を行っている。

その他の措置の内容	—
リスクへの対策は十分か	<div style="display: flex; align-items: center;"> <div style="margin-right: 20px;">[十分である]</div> <div style="text-align: left;"> <p><選択肢></p> <p>1) 特に力を入れている 2) 十分である</p> <p>3) 課題が残されている</p> </div> </div>

リスク4: 入手の際に特定個人情報漏えい・紛失するリスク							
リスクに対する措置の内容	<ul style="list-style-type: none"> 申請者等から経営企画室職員又は教員が特定個人情報を受理した場合は、授受簿に記入する。また、教員と経営企画室の特定個人情報のやり取りも授受簿に記入する。 特定個人情報の保管については台帳を作成し管理する。 特定個人情報は、キャビネット等で施錠保管する。 特定個人情報の取扱区域は特別支援教育課、特別支援教育推進室、各校経営企画室執務室内に設定し、特別個人情報は取扱区域内のみで使用することとする。 特定個人情報は、取扱者のうち、特別支援教育課職員、学校管理職及び経営企画室職員のみが確認できることとする。 団体内統合利用番号連携サーバシステム及び中間サーバを利用した庁内連携による入手は、関連業務システム以外からのアクセス制御を行っている。また、正当な権限のない利用者及び個別業務システム等からは、目的を超えた紐付けや必要のない情報は入手できないようアクセス制御を行っている。 						
リスクへの対策は十分か	[十分である] <table border="0" style="float: right;"> <tr><td colspan="2"><選択肢></td></tr> <tr><td>1) 特に力を入れている</td><td>2) 十分である</td></tr> <tr><td>3) 課題が残されている</td><td></td></tr> </table>	<選択肢>		1) 特に力を入れている	2) 十分である	3) 課題が残されている	
<選択肢>							
1) 特に力を入れている	2) 十分である						
3) 課題が残されている							
特定個人情報の入手(情報提供ネットワークシステムを通じた入手を除く。)におけるその他のリスク及びそのリスクに対する措置							
<ul style="list-style-type: none"> 特定個人情報の取扱いについて、教員及び経営企画室職員向けの業務マニュアル等を整備し、学事担当者向け説明会や連絡会等で特別支援教育課が研修や説明を行う。 学校において、教員向けの周知及び啓発を行う。 							
3. 特定個人情報の使用							
リスク1: 目的を超えた紐付け、事務に必要な情報との紐付けが行われるリスク							
宛名システム等における措置の内容	団体内統合利用番号連携サーバシステムは関連業務システム以外からのアクセス制御を行っており、正当な権限のない利用者及び個別業務システム等からは、目的を超えた紐付けや必要のない情報とのアクセス制御を行う。						
事務で使用するその他のシステムにおける措置の内容	<ul style="list-style-type: none"> 利用者IDにより、アクセス可能な業務範囲を限定し、正当な権限のない利用者からアクセス制御する。 条例で定めた範囲以外では、庁内連携を行うことができないようアクセス制御する。 						
その他の措置の内容	—						
リスクへの対策は十分か	[十分である] <table border="0" style="float: right;"> <tr><td colspan="2"><選択肢></td></tr> <tr><td>1) 特に力を入れている</td><td>2) 十分である</td></tr> <tr><td>3) 課題が残されている</td><td></td></tr> </table>	<選択肢>		1) 特に力を入れている	2) 十分である	3) 課題が残されている	
<選択肢>							
1) 特に力を入れている	2) 十分である						
3) 課題が残されている							
リスク2: 権限のない者(元職員、アクセス権限のない職員等)によって不正に使用されるリスク							
ユーザ認証の管理	[行っている] <table border="0" style="float: right;"> <tr><td colspan="2"><選択肢></td></tr> <tr><td>1) 行っている</td><td>2) 行っていない</td></tr> </table>	<選択肢>		1) 行っている	2) 行っていない		
<選択肢>							
1) 行っている	2) 行っていない						
具体的な管理方法	<ul style="list-style-type: none"> 学事事務システムは専用の端末からのみ閲覧が可能である。さらに、専用端末から学事事務システムを閲覧する際、パスワード認証及び静脈認証を施すことで、アクセス制御を行う。 特定個人情報を取り扱うことが可能な権限レベルを設定する。 IDとパスワードは個人に割り振る。 ID単位でアクセスログが一定期間保管され、誰が、いつ、どのような操作を行ったのか、追跡できる。 IDの不正使用が確認された場合は、特別支援教育課の確認後、委託事項1事業者が当該IDの利用を制限する。 パスワードは、定期的に変更する。変更時期にはシステムが自動的に変更させる。 						
アクセス権限の発効・失効の管理	[行っている] <table border="0" style="float: right;"> <tr><td colspan="2"><選択肢></td></tr> <tr><td>1) 行っている</td><td>2) 行っていない</td></tr> </table>	<選択肢>		1) 行っている	2) 行っていない		
<選択肢>							
1) 行っている	2) 行っていない						
具体的な管理方法	<ul style="list-style-type: none"> ID管理要項に基づき、情報システム管理者が一元的に管理する。 年度途中にIDを新規で付与又は失効する際は、随時ID新規登録者又はID登録削除対象者のリストを各学校で作成し、特別支援教育課にて意思決定の上、委託事項1事業者が処理し、利用可能又は失効とする。 異動等の事由等により、毎年度末にIDの削除及び新規登録が必要な者については、特別支援教育課にて意思決定の上、削除対象者は3月31日で失効とし、新規登録者は4月1日以降利用可能とする。 						
アクセス権限の管理	[行っている] <table border="0" style="float: right;"> <tr><td colspan="2"><選択肢></td></tr> <tr><td>1) 行っている</td><td>2) 行っていない</td></tr> </table>	<選択肢>		1) 行っている	2) 行っていない		
<選択肢>							
1) 行っている	2) 行っていない						
具体的な管理方法	<ul style="list-style-type: none"> アクセス権限については、情報システム管理者が一元的に管理する。 IDは内部承認手続の上、発行する。 権限はID付与範囲一覧表を定め、これに基づきIDを付与する。 ID付与範囲一覧表は定期的に見直す。 権限レベル別の名簿を作成する。 						

<p>特定個人情報ファイルの閲覧者・更新者の制限</p>	<p>[制限している] <選択肢> 1) 制限している 2) 制限していない</p>
<p>具体的な制限方法</p>	<ul style="list-style-type: none"> ・作業者を限定するために、委託、再委託先等関係者全員の名簿を都へ事前に提出させる。なお、作業者に変更がある場合は、速やかに報告することとする。 ・システム内の特定個人情報ファイルについては、上記で報告した名簿記載の関係者のみがアクセスできることとし、アクセス記録を残すこととする。 ・委託事項1事業者が使用するIDは、ID管理要項に基づき、特別支援教育課が発行する。IDの設定に際しては、使用する期間のみ有効とし、有効期間が経過した場合には、当該IDは失効する。 ・秘密の保持、目的外使用の禁止、複写及び複製の禁止、作業場所以外への持ち出し禁止、情報の保管及び管理等を規定した仕様書において、委託処理に係る必要事項を定める。
<p>特定個人情報ファイルの取扱いの記録</p>	<p>[記録を残している] <選択肢> 1) 記録を残している 2) 記録を残していない</p>
<p>具体的な方法</p>	<ul style="list-style-type: none"> ・委託先との契約に際して、保管庫等での施錠・管理、管理状況の記録、管理記録の報告等を規定した仕様書において、取扱いに係る必要事項を定める。 ・特定個人情報ファイルのアクセスログ及び操作ログを記録し、一定期間保存しており、誰がデータベース上のどの情報をアクセスし、抽出したかが記録され、不正アクセスを監視する。 ・管理記録を一定期間保存することとし、毎月個人情報の取扱状況の報告を行うとともに、作業を行った場合は、作業計画兼実績報告書により報告を行う。
<p>特定個人情報の提供ルール</p>	<p>[定めている] <選択肢> 1) 定めている 2) 定めていない</p>
<p>委託先から他者への提供に関するルールの内容及びルール遵守の確認方法</p>	<ul style="list-style-type: none"> ・委託先が再委託を行う場合には、あらかじめ再委託を行う旨を書面により特別支援教育課に申し出て、特別支援教育課の承諾を得ることとする。 ・電子情報処理委託に係る標準特記仕様書(以下「標準特記仕様書」という。)により、目的外使用の禁止、第三者への提供の禁止、複写及び複製の禁止、情報の保管及び管理等に対する義務違反時の損害賠償の請求等について、定めた上で実施する。
<p>委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法</p>	<ul style="list-style-type: none"> ・委託、再委託等に当たっては、委託先の適切な選定、委託先に安全管理措置を遵守させるための必要な契約の締結、委託先における特定個人情報の取扱状況の把握を行う。 ・標準特記仕様書により、その内容を遵守する旨を記載した誓約書を都に提出させる。また、特別支援教育課による監査、点検及び検査に協力することとしている。 ・申請データが格納されるデータベースへのアクセス権限は、特別支援教育課から付与されるIDにより設定され、必要最小限に制限される。 ・本番データの参照及び修正は都の指示に基づき実施している。作業状況については、作業実施後、その都度報告を受け、確認する。 ・特定個人情報の授受については、記録を残す。また、外部記録媒体を使用する場合は、委託先からの作業申請書に基づき、書出し用のIDとパスワードを発行している。
<p>特定個人情報の消去ルール</p>	<p>[定めている] <選択肢> 1) 定めている 2) 定めていない</p>
<p>ルールの内容及びルール遵守の確認方法</p>	<ul style="list-style-type: none"> ・外部記録媒体を使用した際は、外部記録媒体内のデータをすぐさま削除している。 ・保存期間満了後やハード更改等の際は、特別支援教育課の意思決定に基づき、システム運用保守受託者において、保存された情報が読み出しできないよう、物理的破壊または専用ソフト等を利用して完全に消去する。特別支援教育課は、システム運用保守受託者が確実にデータ消去したことについて、証明書等の提出を受ける。
<p>委託契約書中の特定個人情報ファイルの取扱いに関する規定</p>	<p>[定めている] <選択肢> 1) 定めている 2) 定めていない</p>
<p>規定の内容</p>	<p>契約書や誓約書で、「東京都個人情報の保護に関する条例」の規定を遵守し、個人情報の漏えい防止等適切な管理のために必要な体制の確保に万全の措置を講ずることを規定する。</p>
<p>再委託先による特定個人情報ファイルの適切な取扱いの確保</p>	<p>[十分に行っている] <選択肢> 1) 特に力を入れて行っていない 2) 十分に行っている 3) 十分に行っていない 4) 再委託していない</p>
<p>具体的な方法</p>	<ul style="list-style-type: none"> ・標準特記仕様書で、「東京都特定個人情報の保護に関する条例」の規定を遵守し、個人情報の漏えい防止等適切な管理のために必要な体制の確保に万全の措置を講ずることを規定する。 ・秘密保持義務、事務所内からの特定個人情報の持ち出しの禁止、特定個人情報の目的外利用の禁止、再委託における条件、漏えい事案等が発生した場合の委託先の責任、委託契約終了後の特定個人情報の返却又は廃棄、特定個人情報を取り扱う従業者の明確化、従業者に対する監督・教育、及び契約内容の遵守状況について報告を求め、都が必要と認めるときは委託先に対して実地の調査を行う。

その他の措置の内容	—	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置		
<ul style="list-style-type: none"> ・学事事務システムではサーバ機器類を専用施設内の専用ラックに設置し、私物の持込みを禁止している。 ・サーバ機器類を設置している専用施設の監視は警備員の巡視及び24時間稼働のカメラにより行われている。 ・アクセス記録のログを取得する。 ・不正を行わないことを関係者全員に誓約させ、誓約書の提出を求める。 		
5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。） [] 提供・移転しない		
リスク1： 不正な提供・移転が行われるリスク		
特定個人情報の提供・移転の記録	[記録を残している]	<選択肢> 1) 記録を残している 2) 記録を残していない
具体的な方法	団体内統合利用番号連携サーバシステムを利用した情報の提供・移転は全て記録を残しており、どのシステムから提供・移転の要求があったかが記録されている。	
特定個人情報の提供・移転に関するルール	[定めている]	<選択肢> 1) 定めている 2) 定めていない
ルールの内容及びルール遵守の確認方法	番号法等の法令に基づく事務で、かつ、条例で定めた事務以外には提供・移転は行わない。また、提供・移転の記録を残し、法令に基づかない利用がないか確認する。	
その他の措置の内容	<ul style="list-style-type: none"> ・許可した提供・移転先のみデータを提供・移転するアクセス制御を行っている。 ・提供・移転に関する手続きの遵守を周知する。 	
リスクへの対策は十分か	[特に力を入れている]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2： 不適切な方法で提供・移転が行われるリスク		
リスクに対する措置の内容	<ul style="list-style-type: none"> ・特定個人情報の提供・移転は、管理権限が付与された者のみが行う。 ・許可した提供・移転先のみデータを提供・移転するアクセス制御を行っている。 	
リスクへの対策は十分か	[特に力を入れている]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク3： 誤った情報を提供・移転してしまうリスク、誤った相手に提供・移転してしまうリスク		
リスクに対する措置の内容	番号法等の法令や条例で定められた相手に対し、提供・移転先に応じた項目のみを提供・移転するシステムを構築している。	
リスクへの対策は十分か	[特に力を入れている]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）におけるその他のリスク及びそのリスクに対する措置		
<p>○その他のリスク</p> <ul style="list-style-type: none"> ・他人のID使用 <p>○そのリスクに対する措置</p> <ul style="list-style-type: none"> ・専用端末から学事事務システムを操作・閲覧する際、パスワード認証及び静脈認証を施すことで、アクセス制御を行う。また、特定個人情報を取り扱うことが可能な権限レベルを設定する。 ・他人のID等を使用しないように、また他人にID等を使用されないよう厳格に管理する事等を研修を通じて職員に徹底する。また、必要に応じて電話による確認を行う。 		

6. 情報提供ネットワークシステムとの接続 [] 接続しない(入手) [] 接続しない(提供)

リスク1: 目的外の入手が行われるリスク

リスクに対する措置の内容	<p>【学事事務システム】 ①利用者IDにより、アクセス可能な業務範囲を限定し、正当な権限のない利用者からはマイナンバーを利用できないようアクセス制御を行う。 ②情報提供ネットワークにより特定個人情報を取得する際は、対象者について使用簿を作成し、内部で意思決定を行った上で、審査権限を持ったIDにより、連携サーバを経由して照会を行う。</p> <p>【連携サーバ】 ①各事務所管部署からの申請に基づき、利用者とその所掌事務の紐付けが連携サーバ上であらかじめ定義され、その範囲内においてのみ情報照会が可能となるようアクセス制御されている。 ②符号取得においては、あらかじめ各事務のシステムにて登録され、個別業務システム利用番号が割り当てられた状態の対象者のみを受け付けるよう制御されている。 ③符号取得に対する回答及び情報照会に対する回答は、当該照会を行った事務に対してのみ返却するよう制御されている。 ④各事務所管部署が個々の照会データを一意に識別できるよう付与した識別子を、連携サーバからの回答データに付記して返却することで、どの照会に対する回答かを各事務所管部署で正確に突合できるようにしている。</p> <p>【中間サーバ・ソフトウェア】 ①情報照会機能(※1)により、情報提供ネットワークに情報提供照会を行う際には、情報提供許可証の発行と照会内容の照会許可照合リスト(※2)との照合を情報提供ネットワークに求め、情報提供ネットワークシステムから情報提供許可証を受領してから情報照会を実施することになる。つまり、番号法上認められた情報連携以外の照会を拒否する機能を備えており、目的外提供やセキュリティリスクに対応している。 ②中間サーバの職員認証・権限管理機能(※3)では、ログイン時の職員接続端末の操作や不適切なオンライン連携を抑止する仕組みになっている。 (※1)情報提供ネットワークシステムを使用した特定個人情報の照会及び照会した情報の受領を行う機能 (※2)番号法の規定による情報提供ネットワークシステムを使用した特定個人情報の提供に係る情報照会者、情報提供者、事務及び特定個人情報を一覧化し、情報照会の可否を判断するために使用するもの (※3)中間サーバを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報へのアクセス制御を行う機能</p>
--------------	---

リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
-------------	-----------	---

リスク2: 安全が保たれない方法によって入手が行われるリスク

リスクに対する措置の内容	<p>【学事事務システム】 ①連携サーバに登録する照会ファイルを暗号化する。 ②情報提供ネットワークにより特定個人情報を取得する際は、対象者について使用簿を作成し、内部で意思決定を行った上で、連携サーバを経由して照会を行う。 ③利用者IDにより、アクセス可能な業務範囲を限定し、正当な権限のない利用者からは個人番号を利用できないようアクセス制御を行う。</p> <p>【連携サーバ】 ①システムを利用可能な時間を制限している。 ②情報連携に用いる端末に対し、端末認証を行う。 ③ログイン時に利用者の認証を実施する。 ④個別業務システム(事務)との間は、庁内のネットワークを介するとともに暗号化を行う。 ⑤連携サーバから個別業務システムに提供する照会結果ファイルは、暗号化を行う。 ⑥中間サーバとの間は、行政情報ネットワーク上で他とは分離された通信を用いるとともに、暗号化を行う。 ⑦サーバ認証により真正性が担保された中間サーバに接続する。</p> <p>【中間サーバ・ソフトウェア】 中間サーバは、特定個人情報保護委員会との協議を経て、総務大臣が設置・管理する情報提供ネットワークシステムを使用した特定個人情報の入手のみ実施できるよう設計されるため、安全性が担保されている。</p> <p>【中間サーバ・プラットフォーム】 ①中間サーバと既存システム、情報提供ネットワークシステムとの間は高度なセキュリティを維持した行政専用のネットワーク(総合行政ネットワーク等)を利用することにより、安全性を確保している。 ②中間サーバと団体については、VPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。</p>
--------------	--

リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
-------------	-----------	---

リスク3: 入手した特定個人情報 that 不正確であるリスク	
リスクに対する措置の内容	<p>【学事事務システム】</p> <p>①情報提供ネットワーク、中間サーバ、連携サーバを使用して、統合利用番号により紐付けられた照会対象者に係る特定個人情報を入手するため、正確な照会対象者に係る特定個人情報を入手することが担保されている。</p> <p>②特定個人情報を取得後、使用簿によって照会結果の確認を行う。</p> <p>③照会時のエラーは、学校がエラー内容を学事事務システムで確認の上、対応する。</p> <p>【連携サーバ】</p> <p>①各事務所管部署からの申請に基づき、利用者とその所掌事務の紐付けが連携サーバ上であらかじめ定義され、その範囲内においてのみ情報照会が可能となるようアクセス制御されている。</p> <p>②符号取得においては、あらかじめ各事務のシステムにて登録され、個別業務システム利用番号が割り当てられた状態の対象者のみを受け付けるよう制御されている。</p> <p>③サーバ認証により真正性が担保された中間サーバに接続する。</p> <p>【中間サーバ・ソフトウェア】</p> <p>①中間サーバは、特定個人情報保護委員会との協議を経て、総務大臣が設置管理する情報提供ネットワークシステムを使用して、情報提供用個人識別番号により紐付けられた照会対象者に係る特定個人情報を入手するため、正確な照会対象者に係る特定個人情報を入手することが担保されている。</p>
リスクへの対策は十分か	<p>[十分である]</p> <p><選択肢></p> <p>1) 特に力を入れている</p> <p>2) 十分である</p> <p>3) 課題が残されている</p>
リスク4: 入手の際に特定個人情報 that 漏えい・紛失するリスク	
リスクに対する措置の内容	<p>【学事事務システム】</p> <p>①連携サーバに登録する照会ファイルを暗号化する。</p> <p>②連携サーバに登録する照会ファイル及び取得する照会結果ファイルはシステムが自動連携させるため、特別支援教育課及び委託先が直接触れることはない。</p> <p>③サーバは隔離された区画(管理区域)に設置し、アクセス制御を行う。入退室は静脈認証等により入退室管理を行い、物理的安全管理措置を施す。</p> <p>【連携サーバ】</p> <p>①システムを利用可能な時間を制限している。</p> <p>②ログイン時に利用者の認証を求める。</p> <p>③インターネットや庁内の他のネットワークから分離された専用のネットワーク上で暗号化を行う。</p> <p>④情報連携に用いる端末に対し、端末認証を行う。</p> <p>⑤中間サーバとの間は、行政情報ネットワーク上で他とは分離された通信を用いるとともに、暗号化を行う。</p> <p>⑥サーバ認証により、真正性が担保された中間サーバに接続する。</p> <p>⑦システムの利用者、日時等をシステム上でログとして記録し、7年間保存する。</p> <p>⑧個別業務システムと中間サーバの間における特定個人情報の授受に当たっては、その中継のみを行い、システム内に特定個人情報(副本相当)は保有しない。</p> <p>⑨連携サーバから個別業務システムに提供する照会結果ファイルは暗号化を行う。</p> <p>【中間サーバ・ソフトウェア】</p> <p>①中間サーバは、情報提供ネットワークを使用した特定個人情報の入手のみを実施するため、漏えい・紛失のリスクに対応している(※)</p> <p>②既存システムからの接続に対し、認証を行い、許可されていないシステムからのアクセスを防止する仕組みを設けている。</p> <p>③情報照会が完了又は中断した情報照会結果については、一定時間経過後に当該結果を情報照会機能に自動で削除することにより、特定個人情報 that 漏えい・紛失するリスクを軽減している。</p> <p>④中間サーバの職員認証・権限管理機能では、ログイン時の職員認証の他にログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や不適切なオンライン連携を抑止する仕組みとなっている。</p> <p>(※)中間サーバは、情報提供ネットワークを使用して特定個人情報を送信する際、送信する特定個人情報の暗号化を行っており、照会者の中間サーバでしか復号できない仕組みになっている。そのため、情報提供ネットワークシステムでは復号されないものとなっている。</p> <p>【中間サーバ・プラットフォーム】</p> <p>①中間サーバと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用ネットワーク(総合行政ネットワーク等)を利用することにより、漏えい・紛失のリスクに対応している。</p> <p>②中間サーバと団体については、VPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで漏えい・紛失のリスクに対応している。</p> <p>③中間サーバプラットフォーム事業者の業務は、中間サーバ・プラットフォームの運用、監視・障害対応等であり、業務上、特定個人情報へはアクセスすることはできない。</p>
リスクへの対策は十分か	<p>[十分である]</p> <p><選択肢></p> <p>1) 特に力を入れている</p> <p>2) 十分である</p> <p>3) 課題が残されている</p>

リスク5: 不正な提供が行われるリスク	
リスクに対する措置の内容	<p>【学事事務システム】</p> <p>①IDにより、アクセス可能な業務範囲を限定し、正当な権限のない利用者からは特定個人情報を利用できないようアクセス制御している。</p> <p>②アクセスログを7年間保管し、必要に応じてアクセスログを点検する。</p> <p>③副本登録するファイルは暗号化する。</p> <p>④受給者情報は、番号法に基づき、連携サーバを経由してのみ中間サーバに副本登録する。</p> <p>⑤支給情報の副本登録は、承認を経た上で行う。</p> <p>【連携サーバ】</p> <p>①システムを利用可能な時間を制限する。</p> <p>②ログイン時に利用者の認証を実施する。</p> <p>③各事務所管部署からの申請に基づき、利用者とその所掌事務の紐付けが連携サーバ上であらかじめ定義され、その範囲においてのみ情報提供が可能となるようアクセス制御されている。</p> <p>④システムの利用者、日時等をシステム上でログとして記録し、7年間保存する。</p> <p>⑤個別業務システム(事務)と中間サーバとの間における特定個人情報の授受に当たっては、その中継のみを行い、システム内に特定個人情報(副本相当)は保有しない。</p> <p>⑥インターネットや庁内の他のネットワークから分離された専用のネットワーク上で、暗号化を行う。</p> <p>⑦中間サーバとの間は、行政情報ネットワーク上で他とは分離された通信を用いるとともに、暗号化を行う。</p> <p>⑧サーバ認証により真正性が担保された中間サーバに接続する。</p> <p>【中間サーバ・ソフトウェア】</p> <p>①情報提供機能(※)により、情報提供ネットワークシステムにおける照会許可照合リストを情報提供ネットワークシステムから入手し、中間サーバにも格納して、情報提供機能により、照会許可照合リストに基づき情報連携が認められた特定個人情報の提供の要求であるか、チェックを実施している。</p> <p>②情報提供機能により、情報提供ネットワークシステムに情報提供を行う際には、情報提供ネットワークシステムから情報提供許可証と情報照会者へたどり着くための経路情報を受領し、照会内容に対応した情報を自動で生成して送付することで、特定個人情報が不正に提供されるリスクに対応している。</p> <p>③機微情報については自動応答を行わないように自動応答不可フラグを設定し、特定個人情報の提供を行う際に、送信内容を改めて確認し、提供を行うことで、センシティブな特定個人情報が不正に提供されるリスクに対応している。</p> <p>④中間サーバの職員認証・権限管理機能では、ログイン時の職員認証の他に、不適切な接続端末の操作や、不適切なオンライン連携を抑制する仕組みになっている。</p> <p>(※)情報提供ネットワークシステムを使用した特定個人情報の提供の要求の受領及び情報提供を行う機能。</p>
リスクへの対策は十分か	<p>[十分である] <選択肢></p> <p>1) 特に力を入れている 2) 十分である</p> <p>3) 課題が残されている</p>

リスク6: 不適切な方法で提供されるリスク	
リスクに対する措置の内容	<p>【学事事務システム】</p> <p>①IDにより、アクセス可能な業務範囲を限定し、正当な権限のない利用者からは特定個人情報を利用できないようアクセス制御する。</p> <p>②アクセスログを7年間保管し、必要に応じてアクセスログを点検する。</p> <p>③副本登録するファイルは暗号化する。</p> <p>④受給者情報は、番号法に基づき、連携サーバを経由してのみ中間サーバに副本登録する。</p> <p>⑤条例で定めた範囲以外では、庁内連携を行うことができないようにシステム制御する。</p> <p>⑥マイナンバーを可搬媒体、プリンタ等で出力できないようにする。</p> <p>【連携サーバ】</p> <p>①システムを利用可能な時間を制限する。</p> <p>②ログイン時に利用者の認証を実施する。</p> <p>③各事務所管部署からの申請に基づき、利用者とその所掌事務の紐付けが連携サーバ上であらかじめ定義され、その範囲においてのみ情報提供が可能となるようアクセス制御されている。</p> <p>④システムの利用者、日時等をシステム上でログとして記録し、7年間保存する。</p> <p>⑤個別業務システム(事務)と中間サーバの間における特定個人情報の授受に当たっては、その中継のみを行い、システム内に特定個人情報(副本相当)は保有しない。</p> <p>⑥インターネットや庁内の他のネットワークから分離された専用のネットワーク上で、暗号化を行う。</p> <p>⑦中間サーバとの間は、行政情報ネットワーク上で他とは分離された通信を用いるとともに、暗号化を行う。</p> <p>⑧サーバ認証により真正性が担保された中間サーバに接続する。</p> <p>【中間サーバ・ソフトウェア】</p> <p>①セキュリティ管理機能(※)により、情報提供ネットワークシステムに送信する情報は、情報照会者から受領した暗号化鍵で暗号化を適切に実施した上で提供を行う。</p> <p>②中間サーバの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携は抑止される。</p> <p>※暗号化・複合化機能と、鍵情報及び照会許可リストを管理する機能</p> <p>【中間サーバ・プラットフォーム】</p> <p>①中間サーバと既存システム、情報提供ネットワークとの間は、高度なセキュリティを維持した行政専用のネットワーク(総合行政ネットワーク等)を利用することにより、不適切な方法で提供されるリスクに対応する。</p> <p>②中間サーバと団体については、VPN等の技術を利用し、団体ごとに通信回線を分離するとともに通信を暗号化することで漏えい・紛失のリスクに対応する。</p> <p>③中間サーバ・プラットフォーム事業者の業務は中間サーバ・プラットフォームの運用、監視、障害対応等であり、業務上、特定個人情報へはアクセスできない。</p>
リスクへの対策は十分か	<p>[十分である] <選択肢></p> <p>1) 特に力を入れている 2) 十分である</p> <p>3) 課題が残されている</p>

リスク7: 誤った情報を提供してしまうリスク、誤った相手に提供してしまうリスク

<p>リスクに対する措置の内容</p>	<p>【学事事務システム】 ①支給情報の提供は、事前に符号取得を行った上で、他団体から情報照会を受ける都度、各校において意思決定を行い、就学奨励費(国庫負担金分)の支給額について副本登録を行う。 ②法令や条例で定められ、定義された情報以外では提供・移転できないようにする。 ③提供時のエラーは、連携サーバ又は中間サーバから、指定した宛先にメール通知があるため、受信後、特別支援教育課でエラー内容を確認し、学校において対応する。</p> <p>【連携サーバ】 ①各事務所管部署で本人確認及び真正性確認を行った個人番号に基づき、団体内統合利用番号及び個別業務システム利用番号が紐付けられていることを前提として、当該人に対する情報提供が可能となるよう制御されている。 ②個別業務システム(事務)と中間サーバとの間における特定個人情報の授受に当たっては、その中継のみを行い、システム内に特定個人情報(副本相当)は保有しない。 ③インターネットや庁内の他のネットワークから分離された専用のネットワーク上で、暗号化を行う。 ④中間サーバとの間は、行政情報ネットワーク上で他とは分離された通信を用いるとともに、暗号化を行う。 ⑤サーバ認証により真正性が担保された中間サーバに接続する。</p> <p>【中間サーバ・ソフトウェア】 ①情報提供機能により、情報提供ネットワークシステムに情報提供を行う際には、情報提供許可証と情報照会者への経路情報を受領した上で、情報照会内容に対応した情報提供することで、誤った相手に特定個人情報が提供されるリスクに対応する。 ②情報提供データベース(※)により、「情報提供データベースへのインポートデータ」の形式チェックと、接続端末の画面表示等により、情報提供データベースの内容を確認できる準備することで、誤った特定個人情報を提供してしまうリスクに対応する。 ③情報提供データベース管理機能では情報提供データベースの副本データを既存業務システムの原本と照合するためのエクスポートデータ出力する機能を有する。 (※)特定個人情報を副本として保存・管理する機能</p>
---------------------	---

<p>リスクへの対策は十分か</p>	<p>[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている</p>
--------------------	--

情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置

<p>【中間サーバ・ソフトウェア】 ①中間サーバの職員認証・権限管理機能では、ログイン時の職員認証のほかに、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 ②情報連携においてのみ、情報提供用個人識別符号を用いることがシステム上担保されており、不正なアクセスが行われるリスクに対応している。</p> <p>【中間サーバ・プラットフォーム】 ①中間サーバと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行専用のネットワーク(総合行政ネットワーク等)利用することにより、安全性を確保している。 ②中間サーバと団体については、VPN等の技術を利用し、団体ごとに通信回線を分離するとともに通信を暗号化することで安全性を確保している。 ③中間サーバ・プラットフォームでは、特定個人情報を管理するデータベースを地方公共団体ごとにアクセス制御しており、中間サーバ・プラットフォームを利用する団体であっても他団体が管理する情報には一切アクセスできない。 ④特定個人情報の管理を地方公共団体のみが行うことで、中間サーバ・プラットフォームの保守・運用を行う事業者における情報漏えい等のリスクを極小化する。</p>

7. 特定個人情報の保管・消去

リスク1: 特定個人情報の漏えい・滅失・毀損リスク

①NISC政府機関統一基準群	[政府機関ではない]	<選択肢> 1) 特に力を入れて遵守している 2) 十分に遵守している 3) 十分に遵守していない 4) 政府機関ではない
②安全管理体制	[十分に整備している]	<選択肢> 1) 特に力を入れて整備している 2) 十分に整備している 3) 十分に整備していない
③安全管理規程	[十分に整備している]	<選択肢> 1) 特に力を入れて整備している 2) 十分に整備している 3) 十分に整備していない
④安全管理体制・規程の職員への周知	[十分に周知している]	<選択肢> 1) 特に力を入れて周知している 2) 十分に周知している 3) 十分に周知していない
⑤物理的対策	[十分に行っている]	<選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない

具体的な対策の内容	<p>【紙書類】</p> <p>①紙書類については、各校の取扱区域のキャビネット等で施錠保管し、その状況を台帳で管理している。また、取扱者のうち、各校の管理職又は経営企画室職員のみが内容を確認できる。</p> <p>②保存期間満了後、廃棄に当たっては、各校で意思決定を行い、書類を溶解、焼却、裁断等復元不可能な方法により廃棄する。搬送から処理に至るまでの間、各校の取扱者が立ち会う。廃棄終了後、処理業者から廃棄がなされたことの証明書をとる。</p> <p>【学事事務システム】</p> <p>(1)サーバ等</p> <p>①システムサーバは専用施設内(管理区域)にある当該サーバ専用のラックに收容する。また、この区画への入退室管理は生体認証による入退室管理、区画ごとの施錠管理、監視カメラによる録画及び有人監視等を実施する。</p> <p>②保存期間満了後やハード更改等の際は、特別支援教育課の意思決定に基づき、システム運用保守受託者において、保存された情報が読み出できないよう、物理的破壊または専用ソフト等を利用して完全に消去する。特別支援教育課は、システム運用保守受託者が確実にデータ消去したことについて、証明書等の提出を受ける。</p> <p>(2)外部記録媒体</p> <p>外部記録媒体は施錠可能なキャビネット等に保管している。また権限が付与された外部記録媒体のみ使用可能としている。</p> <p>【連携サーバ】</p> <p>①サーバ等を設置するための専用施設内に他のシステムとは分離した区画を設け、当該サーバ専用のラックに施錠して收容する。当該施設では、入退室管理、区画ごとの施錠管理、監視カメラによる録画、有人監視等を実施する。</p> <p>②当該施設の煙感知装置、ガス系消火設備、耐震対応等により、火災や地震に起因する滅失等のリスクを軽減する。</p> <p>③機器のうち、特定個人情報等のデータが記録されるものの廃棄等に当たっては、磁氣的消去又は物理的破壊等により、当該データを復元不可能な状態とする。</p> <p>【中間サーバ・プラットフォーム】</p> <p>①中間サーバ・プラットフォームをデータセンタに構築し、設置場所への入退室管理、有人監視及び施錠管理をすることとしている。また、設置場所はデータセンタ内の専用の領域とし、他テナントとの混在によるリスクを回避する。</p> <p>②事前に申請し承認されていない物品、記録媒体、通信機器などを不正に所持し、持出持込することがないように、警備員などにより確認している。</p>
-----------	---

<p>⑥技術的対策</p> <p>具体的な対策の内容</p>	<p>[十分にしている]</p> <p><選択肢> 1) 特に力を入れて行っている 2) 十分にしている 3) 十分にしていない</p>
	<p>【学事事務システム】 (1)サーバ等 ①ファイアウォールを設置し、許可していない端末やポート番号の通信遮断を行う。 ②ウイルス対策ソフトの定期的パターン更新を行うことにより、ウイルス感染を防止している。 ③インターネットや庁内の他のネットワークから分離された専用のネットワーク上で稼働する。 ④システムのアクセスログを記録・分析する。 (2)外部記録媒体 ①権限を付与した外部記録媒体のみ使用可能としている。 ②外部記録媒体にデータを書き出す場合は、権限のある者から発行されたIDとパスワードによる認証が必要である。 【連携サーバ】 ①インターネットや庁内の他のネットワークから分離された専用のネットワーク上で稼働する。 ②サーバが接続されたセグメントとそれ以外のセグメントの境界にファイアウォールを導入するとともにログを取得する。 ③ウイルス対策ソフトを導入し、パターンファイルを更新する。 ④データベースにデータを暗号化して保存する。 ⑤基本ソフトウェア(OS)及びミドルウェアは必要に応じてセキュリティパッチを適用する。 ⑥データベースに対する操作権限を細分化し、連携サーバ管理者であっても真に必要な場合を除いてはデータにアクセスできないよう制御する。 ⑦データベースに対するアクセスログを取得する。 ⑧データベースのバックアップを取得する。 ⑨あらかじめ登録された機器だけがネットワークに接続できるよう制御する。 ⑩サーバ及びその管理に用いる機器は、書き出し可能な外部記録媒体を内蔵せずかつUSB機器等に対する制御を行い、外部記録媒体の利用を制限する。 【中間サーバ・プラットフォーム】 ①中間サーバ・プラットフォームではUTM(コンピュータウイルスやハッキングなどの脅威からネットワークを効率的かつ包括的に保護する装置)等を導入し、アクセス制限、侵入検知及び侵入防止を行うとともに、ログの解析を行う。 ②中間サーバ・プラットフォームでは、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ③導入しているOS及びミドルウェアについて、必要に応じて、セキュリティパッチの適用を行う。</p>

⑦バックアップ	[十分にしている]	<選択肢> 1) 特に力を入れて行っている 2) 十分にしている 3) 十分にしていない
⑧事故発生時手順の策定・周知	[十分にしている]	<選択肢> 1) 特に力を入れて行っている 2) 十分にしている 3) 十分にしていない
⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか	[発生あり]	<選択肢> 1) 発生あり 2) 発生なし
その内容	①平成27年から平成29年までの間に、都立高等学校主任教諭が、当時勤務校において、同校入学者選抜応募者の受検番号、氏名、総合成績等の個人情報に係る電子データ延べ2,224名分を、SDカードに保存し、同校に置いたままにしたことにより紛失した。また、平成29年に、同校において、609名分の同データを、別のSDカードに保存して持ち出し、その後、異動先の勤務校に持ち込んだ。さらに、平成29年から令和2年までの間に、同校において、同校入学者選抜応募者の同個人情報に係る電子データを、同SDカードに保存するとともに、延べ3,082名分の同データが保存された同SDカードを紛失した。 ②令和2年に、都立図書館職員が、講演会への参加当選者231名に対して抽選結果を電子メールで知らせる際、メールアドレスをメールのBCC欄でなく宛先欄に入力して一斉送信したため、他の当選者の個人情報(メールアドレス)が流出した。	
再発防止策の内容	①入学者選抜に関するデータの保存や管理方法等について、改めて注意喚起を行うとともに、入学者選拔用パソコンの設定を変更する際には、管理職又は管理職立会いの下で管理職に指名された者が行うことに改めるなど、再発防止に向けた個人情報の適切な管理について徹底を図っていく。 ②今後、都民等にメールを送信する際には、複数の職員で送信先及び添付ファイル等について確認することを徹底する。また、同様の事故が起きないように、個人情報を厳正に管理するとともに、職員に対し情報セキュリティの教育・指導を徹底していく。	
⑩死者の個人番号	[保管している]	<選択肢> 1) 保管している 2) 保管していない
具体的な保管方法	学事事務システム上では、生存・死者の個人情報の取扱に差異はないため、保存年限は生存者に関する情報と同様である。	
その他の措置の内容	—	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2: 特定個人情報が古い情報のまま保管され続けるリスク		
リスクに対する措置の内容	・それぞれの事業について、年1回定められた時期に全てのマイナンバーにひもづく世帯員の個人情報の確認を行う。 ・申請内容に変更が生じた場合は、その都度変更申請に基づき、情報変更を行う。	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク3: 特定個人情報が消去されずいつまでも存在するリスク		
消去手順	[定めている]	<選択肢> 1) 定めている 2) 定めていない
手順の内容	①保存期間(7年間)の終了したシステム内の特定個人情報ファイルについては、特別支援教育課にて意思決定を行った上で、消去する。 ②紙ベースの特定個人情報については、文書保存管理規則に基づき、保存期間終了後、各校において、意思決定をした上で処理を行う。	
その他の措置の内容	【紙書類】 保存期間満了後、廃棄に当たっては、各校で意思決定を行い、書類を溶解、焼却、裁断等復元不可能な方法により廃棄する。搬送から処理に至るまでの間、各校の取扱者が立ち会う。廃棄終了後、処理業者から廃棄がなされたことの証明書をとる。 【学事事務システムのデータ】 保存期間満了後やハード更改等の際は、特別支援教育課の意思決定に基づき、システム運用保守受託者において、保存された情報が読み出しできないよう、物理的破壊または専用ソフト等を利用して完全に消去する。特別支援教育課は、システム運用保守受託者が確実にデータ消去したことについて、証明書等の提出を受ける。	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている

特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置

—

IV その他のリスク対策 ※

1. 監査	
①自己点検	<p>[十分に行っている] <選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない</p>
具体的なチェック方法	<p><学事事務システムにおける措置> ・特別支援学校の職員は、毎年1回以上、特定個人情報の取扱いについて研修を実施している。また、個人情報保護について、全職員が自己点検票を用いて、チェックを実施している。 <中間サーバ・プラットフォームにおける措置> 運用規則に基づき、中間サーバ・プラットフォームの運用に携わる職員及び事業者に対し、定期的に自己点検を実施することとしている。</p>
②監査	<p>[十分に行っている] <選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない</p>
具体的な内容	<p>【内部監査】 以下の項目について、内部による監査を毎年実施する。 ・自己点検結果の確認 ・情報資産台帳、情報処理機器等の保有状況簿の確認 ・情報資産の保管・持ち出しに係る帳簿や状況についての確認 ・執務室の直接視察 【学事事務システム】 外部による監査を定期的実施する。 【中間サーバ・プラットフォーム】 運用規則に基づき、中間サーバ・プラットフォームについて、定期的に監査を行うこととしている。</p>
2. 従業者に対する教育・啓発	
従業者に対する教育・啓発	<p>[十分に行っている] <選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない</p>
具体的な方法	<p><東京都教育委員会における措置> 全職員を対象に、e-ラーニングにおいて情報セキュリティ・個人情報保護の悉皆研修を実施している。研修の目的は、個人情報保護の重要性及び適正管理等に関する理解を深め、個人情報保護の遵守を徹底している。また、未受講者に対しては、研修機関から職場の管理・監督者を通じて研修を受講するよう指導を行っている。 また、委託事業者に対しては、業務開始に当たり、個人情報の取扱いルールを順守することを確認させている。 <中間サーバ・プラットフォームにおける措置> ・中間サーバ・プラットフォームの運用に携わる職員及び事業者に対し、セキュリティ研修等を実施することとしている。 ・中間サーバ・プラットフォームの業務に就く場合は、運用規則等について研修を行う事としている。</p>
3. その他のリスク対策	
<p><中間サーバ・プラットフォームにおける措置> 中間サーバ・プラットフォームを活用することにより、統一した設備環境による高レベルのセキュリティ管理(入退出管理等)、ITリテラシーの高い運用担当者によるセキュリティリスクの低減、及び技術力の高い運用担当者による均一的で安定したシステム運用・監視を実現する。</p>	

V 開示請求、問合せ

1. 特定個人情報の開示・訂正・利用停止請求	
①請求先	東京都 教育庁 都立学校教育部 特別支援教育課 経理担当 〒163-8001 東京都新宿区西新宿2-8-1 都庁第二本庁舎15階 電話:03-5320-6754 ファクシミリ:03-5388-1728
②請求方法	指定様式による書面の提出(原則として持参)により開示、訂正又は利用停止の請求を受け付ける。
特記事項	—
③手数料等	[有料] <選択肢> 1) 有料 2) 無料 (手数料額、納付方法: 実費相当分(10円/1枚)の手数料を納付する。)
④個人情報ファイル簿の公表	[行っていない] <選択肢> 1) 行っている 2) 行っていない
個人情報ファイル名	—
公表場所	—
⑤法令による特別の手続	—
⑥個人情報ファイル簿への不記載等	—
2. 特定個人情報ファイルの取扱いに関する問合せ	
①連絡先	東京都 教育庁 都立学校教育部 特別支援教育課 経理担当 〒163-8001 東京都新宿区西新宿2-8-1 都庁第二本庁舎15階 電話:03-5320-6754 ファクシミリ:03-5388-1728
②対応方法	—

VI 評価実施手続

1. 基礎項目評価	
①実施日	令和3年5月1日
②しきい値判断結果	[基礎項目評価及び重点項目評価の実施が義務付けられる(任意に全項目評価を実施)] <選択肢> 1) 基礎項目評価及び全項目評価の実施が義務付けられる 2) 基礎項目評価及び重点項目評価の実施が義務付けられる(任意に全項目評価を実施) 3) 基礎項目評価の実施が義務付けられる(任意に全項目評価を実施) 4) 特定個人情報保護評価の実施が義務付けられない(任意に全項目評価を実施)
2. 国民・住民等からの意見の聴取	
①方法	東京都公式ホームページ及び東京都庁第一本庁舎3階都民情報ルームにおいて全項目評価書を公開し、郵送及び電子メールにて意見を受け付ける。
②実施日・期間	令和3年7月9日から同年8月10日まで
③期間を短縮する特段の理由	—
④主な意見の内容	
⑤評価書への反映	
3. 第三者点検	
①実施日	令和3年8月16日
②方法	
③結果	
4. 個人情報保護委員会の承認【行政機関等のみ】	
①提出日	
②個人情報保護委員会による審査	—

(別添3)変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和3年3月23日	I 基本情報 1. 特定個人情報ファイルを取り扱う事務 ②事務の内容 (1/2)	(特別支援教育就学奨励事業) 特別支援学校への就学奨励に関する法律に基づき、都立特別支援学校に通う幼児、児童及び生徒の保護者等の経済的負担を軽減するため、その負担能力の程度に応じて、就学のために必要な経費(以下「就学奨励費」という。)を支給する。 (高等学校等就学支援金事業) (高等学校等就学支援金の支給に関する法律に基づき、都立特別支援学校高等部(本科)に通う生徒で、世帯の区市町村民税所得割額及び都道府県民税所得割額が一定額未満の者に対して、授業料相当分(以下「就学支援金」という。)を支給する。	(特別支援教育就学奨励事業) 特別支援学校への就学奨励に関する法律に基づき、都立特別支援学校に通う幼児、児童及び生徒の保護者等の経済的負担を軽減するため、その負担能力の程度に応じて、就学のために必要な経費(以下「就学奨励費」という。)を支給する。 (高等学校等就学支援金事業) (高等学校等就学支援金の支給に関する法律に基づき、都立特別支援学校高等部(本科)に通う生徒で、親権者を含む保護者等の所得が一定基準未満の者に対して、授業料相当分(以下「就学支援金」という。)を支給する。	事前	所得判定基準変更のため
令和3年3月23日	I 基本情報 1. 特定個人情報ファイルを取り扱う事務 ②事務の内容 (2/2)	(東京都立高等学校等学び直し支援金事業) 東京都立高等学校等学び直し支援金の交付に関する要綱に基づき、都立特別支援学校高等部(本科)に通う生徒で、世帯の区市町村民税所得割額及び都道府県民税所得割額が一定額未満であり、かつ標準修業年限を超過した者に対して、授業料相当分(以下「学び直し支援金」という。)を支給する。 (東京都立学校等給付型奨学金事業) 東京都立特別支援学校等における給付型奨学金の交付に関する要綱に基づき、都立特別支援学校高等部(本科)に通う生徒で、世帯の区市町村民税所得割額及び都道府県民税所得割額が一定額未満の者に対して、生徒の主体的な教育活動への参加を確保するため、その負担能力の程度に応じて、必要な経費(以下「給付型奨学金」という。)を支給する。 なお、上記事業について申請者から申請があった場合、各都立特別支援学校において、マイナンバーを使用して地方税関係情報等を照会の上審査を行い、東京都教育庁都立学校教育部特別支援教育課が決定する。	(東京都立高等学校等学び直し支援金事業) 東京都立高等学校等学び直し支援金の交付に関する要綱に基づき、都立特別支援学校高等部(本科)に通う生徒で、親権者を含む保護者等の所得が一定基準未満であり、かつ標準修業年限を超過した者に対して、授業料相当分(以下「学び直し支援金」という。)を支給する。 (東京都立学校等給付型奨学金事業) 東京都立特別支援学校等における給付型奨学金の交付に関する要綱に基づき、都立特別支援学校高等部(本科)に通う生徒で、親権者を含む保護者等の所得が一定基準未満の者に対して、生徒の主体的な教育活動への参加を確保するため、その負担能力の程度に応じて、必要な経費(以下「給付型奨学金」という。)を支給する。 なお、上記事業について申請者から申請があった場合、各都立特別支援学校において、マイナンバーを使用して地方税関係情報等を照会の上審査を行い、東京都教育庁都立学校教育部特別支援教育課が決定する。	事前	所得判定基準変更のため
令和3年3月23日	V 開示請求、問合せ 1. 特定個人情報の開示・訂正・利用停止請求 ①請求先 及び 2. 特定個人情報ファイルの取扱いに関する問合せ ①連絡先	東京都教育庁都立学校教育部特別支援教育課経理担当 〒163-8001 東京都新宿区西新宿2-8-1 都庁第一本庁舎39階北側 (平成31年8月26日以降は都庁第二本庁舎15階) 電話:03-5320-6754 ファクシミリ:03-5388-1728	東京都教育庁都立学校教育部特別支援教育課経理担当 〒163-8001 東京都新宿区西新宿2-8-1 都庁第二本庁舎15階 電話:03-5320-6754 ファクシミリ:03-5388-1728	事後	執務場所移転に伴う変更
令和3年6月18日	I 基本情報 2. 特定個人情報ファイルを取り扱う事務において使用するシステム システム2 ③他のシステムとの接続	[]住民基本台帳ネットワークシステム	[O]住民基本台帳ネットワークシステム	事後	誤記訂正
令和3年6月18日	I 基本情報 2. 特定個人情報ファイルを取り扱う事務において使用するシステム システム4		住民基本台帳ネットワークシステム追加	事後	誤記訂正
令和3年6月18日	II 特定個人情報ファイルの概要 3. 特定個人情報の入手・使用 ①入手元	[O]地方公共団体・地方独立行政法人	[O]地方公共団体・地方独立行政法人(都・各区市町村)	事後	補記
令和3年6月18日	II 特定個人情報ファイルの概要 3. 特定個人情報の入手・使用 ②入手方法	[]庁内連携システム	[O]庁内連携システム	事後	誤記訂正
令和3年6月18日	II 特定個人情報ファイルの概要 3. 特定個人情報の入手・使用 ③入手の時期・頻度	・本人からの申請時(定期:入学年度の4月、随時:転入時・希望時)	・就学奨励費:各学部入学時1回(4月から6月) ・就学支援金(学び直し支援金):高等部入学時1回(4月から5月) ・給付型奨学金:高等部入学時1回(4月から5月) ・各業務転入時は随時	事後	
令和3年6月18日	II 特定個人情報ファイルの概要 3. 特定個人情報の入手・使用 ⑧使用方法	学事事務システムにマイナンバーを登録し、情報提供ネットワークシステムを通じて他団体への情報照会を行い、地方税関係情報等を取得する。	学事事務システムにマイナンバーを登録し、情報提供ネットワークシステムを通じて他団体への情報照会を行い、地方税関係情報等を取得する。また、他団体から就学奨励費の支給に関する情報照会があった場合は、情報提供する。	事後	
令和3年6月18日	II 特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項1 ④委託先への特定個人情報ファイルの提供方法	[O]専用線	[]専用線	事後	
令和3年6月18日	II 特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項1 ⑧再委託の許諾方法	東京都は、委託先に対してあらかじめ再委託を行う旨を書面により提出させ、承諾を与える。その際、再委託先の「学事事務システムの仕様書に係る履行体制及び遵守事項の誓約書」の写しの添付を義務づける。	東京都は、委託先に対してあらかじめ再委託を行う旨を書面により提出させ、承諾を与える。その際、再委託先に対し、都立特別支援学校学事事務システムの運用保守等業務委託仕様書に係る履行体制及び遵守事項の誓約書の写しの添付を義務づける。	事後	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和3年6月18日	II 特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項2	委託内容 特定個人情報ファイル取込業務支援、取込ツールの作成、特定個人情報ファイル作成管理	委託内容 文書廃棄処理委託	事前	
令和3年6月18日	II 特定個人情報ファイルの概要 5. 特定個人情報の提供・移転(委託に伴うものを除く。)提供先1	都道府県知事	都道府県知事等	事後	
令和3年6月18日	II 特定個人情報ファイルの概要 5. 特定個人情報の提供・移転(委託に伴うものを除く。)提供先1 ⑥提供方法	[]その他()	[O]その他(庁内連携)	事後	
令和3年6月18日	II 特定個人情報ファイルの概要 5. 特定個人情報の提供・移転(委託に伴うものを除く。)提供先1 ⑦時期・頻度	照会の都度	年に1回程度未満	事後	実績に伴う変更
令和3年6月18日	II 特定個人情報ファイルの概要 5. 特定個人情報の提供・移転(委託に伴うものを除く。)提供先2	都道府県知事	都道府県知事等	事後	
令和3年6月18日	II 特定個人情報ファイルの概要 5. 特定個人情報の提供・移転(委託に伴うものを除く。)提供先2 ⑥提供方法	[]その他()	[O]その他(庁内連携)	事後	
令和3年6月18日	II 特定個人情報ファイルの概要 6. 特定個人情報ファイルの保管・消去 ①保管場所	【学事事務システム内のデータ】 システムサーバは専用施設内に当該サーバ専用のラックに収容する。また、この区画への入退室管理は生体認証による入退室管理、区画ごとの施錠管理、監視カメラによる録画、有人監視等を実施する。	【学事事務システム】 ・学事事務システム内のデータについては、保存期間満了後やハード更改等の際は、システム運用保守受託者において、保存された情報が読み出しできないよう、物理的破壊または専用ソフト等を利用して完全に消去する。特別支援教育課は、システム運用保守受託者が確実にデータ消去したことについて、証明書等の提出を受ける。 ・外部記録媒体内のデータは使用が済んだらすぐさま削除している。	事後	
令和3年6月18日	II 特定個人情報ファイルの概要 6. 特定個人情報ファイルの保管・消去 ①保管場所	【中間サーバ・プラットフォーム】 ①中間サーバ・プラットフォームをデータセンターに構築し、設置場所への入退室管理、有人監視及び施錠管理をすることとしている。 ②特定個人情報は、サーバ室に設置された中間サーバのデータベース内に保存され、バックアップもデータベース上に保存される。	【中間サーバ・プラットフォーム】 ①中間サーバ・プラットフォームをデータセンターに設置している。データセンターへの入館及びサーバ室への入退室を行う際は、警備員などにより顔写真入りの身分証明書と事前申請の照合を行う。 ②特定個人情報は、サーバ室に設置された中間サーバのデータベース内に保存され、バックアップもデータベース上に保存される。	事後	
令和3年6月18日	II 特定個人情報ファイルの概要 6. 特定個人情報ファイルの保管・消去 ③消去方法	【学事事務システム内のデータ】 学事事務システム内のデータについては、保存期間満了後、システム運用保守受託者が復元不可能な方法で消去し、データ消去履歴としてシステム内に処理記録(特定個人情報ファイルの種類・名称、責任者・取扱部署、削除・廃棄状況等)を保存する。都は、システム運用保守受託者が確実にデータ消去したことについて、証明書等の提出を受ける。	【学事事務システム】 ・学事事務システム内のデータについては、保存期間満了後やハード更改等の際は、システム運用保守受託者において、保存された情報が読み出しできないよう、物理的破壊または専用ソフト等を利用して完全に消去する。特別支援教育課は、システム運用保守受託者が確実にデータ消去したことについて、証明書等の提出を受ける。 ・外部記録媒体内のデータは使用が済んだらすぐさま削除している。	事後	
令和3年6月18日	III 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2. 特定個人情報の入手(情報提供ネットワークシステムを通じた入手を除く。) ・リスク1: 目的外の入手が行われるリスク	・特定個人情報の入手は番号法令の規定の範囲内で認められたもののみとする。 ・支給認定を受けようとする者は、申請者の意思により申請を行うと、法令・要綱等において定める。 ・申請書の記載事項、様式については、要綱等において定める。 ・申請者が対象者以外の情報を記載することがないよう、申請に当たっての記載例や注意事項を作成する。 ・申請受付については、申請にかかる幼児、児童又は生徒の在籍校にて行う。 ・申請書類の過不足を確認できるよう、リーフレット、手引等を作成するとともに、学校担当者向けの説明会を毎年度開催する。	・特定個人情報の入手は番号法令の規定の範囲内で認められたもののみとする。 ・支給認定を受けようとする者は、申請者の意思により申請を行うと、法令・要綱等において定める。 ・申請書の記載事項、様式については、要綱等において定める。 ・申請者が対象者以外の情報を記載することがないよう、申請に当たっての記載例や注意事項を作成する。 ・申請受付については、申請にかかる幼児、児童又は生徒の在籍校にて行う。 ・申請書類の過不足を確認できるよう、リーフレット、手引等を作成するとともに、学校担当者向けの説明会を毎年度開催する。 ・団体内統合利用番号連携サーバシステム及び中間サーバを利用した庁内連携による入手は、関連業務システム以外からのアクセス制御を行っている。また、正当な権限のない利用者及び個別業務システム等からは、目的を超えた紐付けや必要のない情報は入手できないようアクセス制御を行っている。	事後	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和3年6月18日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。） ・リスク2：不適切な方法で入手が行われるリスク	<ul style="list-style-type: none"> ・個人番号は利用目的を明示の上、収集する。 ・申請者は申請書、個人番号カード又は個人番号通知カードの写し及び本人確認書類を厳封して、原則として経営企画室へ持参又は郵送にて提出する。ただし、やむを得ず上記の方法によれない場合は、教員に提出し、教員は厳封されたまま経営企画室に提出する。 ・提出方法はいずれの場合も郵送に準ずる（管理職、経営企画室職員及び教員は、あらかじめ、取扱者に指定する。）。 ・経営企画室職員は封筒を開封し、添付資料により申請者の番号確認及び身元確認を行う。 ・経営企画室職員は封筒記載の情報を確認し、授受簿に記録する。 ・提出書類に不備があった場合等については、経営企画室職員が申請者又は生徒が申請者の場合はその保護者（以下「申請者等」という。）と直接やり取りを行う。 ・これらの手続きについては、業務マニュアルで記載する。 	<ul style="list-style-type: none"> ・個人番号は利用目的を明示の上、収集する。 ・申請者は申請書、個人番号カード又は個人番号通知カードの写し及び本人確認書類を厳封して、原則として経営企画室へ持参又は郵送にて提出する。ただし、やむを得ず上記の方法によれない場合は、教員に提出し、教員は厳封されたまま経営企画室に提出する。 ・提出方法はいずれの場合も郵送に準ずる（管理職、経営企画室職員及び教員は、あらかじめ、取扱者に指定する。）。 ・経営企画室職員は封筒を開封し、添付資料により申請者の番号確認及び身元確認を行う。 ・経営企画室職員は封筒記載の情報を確認し、授受簿に記録する。 ・提出書類に不備があった場合等については、経営企画室職員が申請者又は生徒が申請者の場合はその保護者（以下「申請者等」という。）と直接やり取りを行う。 ・これらの手続きについては、業務マニュアルで記載する。 ・団体内統合利用番号連携サーバシステム及び中間サーバを利用した庁内連携による入手は、関連業務システム以外からのアクセス制御を行っている。また、正当な権限のない利用者及び個別業務システム等からは、目的を超えた紐付けや必要のない情報は入手できないようアクセス制御を行っている。 	事後	
令和3年6月18日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。） ・リスク3：入手した特定個人情報が入力された個人番号が不正であるリスク	<ul style="list-style-type: none"> ・経営企画室職員が台帳及び封筒に、各個人に割り振られた番号を付し、保管する。 ・申請書類に不備があった場合等については、経営企画室職員が直接申請者等に確認を行う。 ・それぞれの事業について、年1回定められた時期に支給更新手続きが行われるため、その際に申請情報（個人番号を除く。）の確認を行う。 ・マイナンバーの学事事務システムへの入力には、経営企画室職員2名（導入時は委託事項1事業者の作業員2名）がそれぞれ行い、それぞれが入力した個人番号をシステム内で突合することで、入力ミスを防止する。 	<ul style="list-style-type: none"> ・経営企画室職員が台帳及び封筒に、各個人に割り振られた番号を付し、保管する。 ・申請書類に不備があった場合等については、経営企画室職員が直接申請者等に確認を行う。 ・それぞれの事業について、年1回定められた時期に支給更新手続きが行われるため、その際に申請情報（個人番号を除く。）の確認を行う。 ・マイナンバーの学事事務システムへの入力には、経営企画室職員2名（導入時は委託事項1事業者の作業員2名）がそれぞれ行い、それぞれが入力した個人番号をシステム内で突合することで、入力ミスを防止する。 	事後	
令和3年6月18日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。） ・リスク4：入手の際に特定個人情報が入力された個人番号が不正であるリスク	<ul style="list-style-type: none"> ・申請者等から経営企画室職員又は教員が特定個人情報を受理した場合は、授受簿に記入する。また、教員と経営企画室の特定個人情報のやり取りも授受簿に記入する。 ・特定個人情報の保管については台帳を作成し管理する。 ・特定個人情報の取扱区域は特別支援教育課、特別支援教育推進室、各校経営企画室執務室内に設定し、特別個人情報は取扱区域内のみで使用する。また、特別個人情報は、取扱者のうち、特別支援教育課職員、学校管理職及び経営企画室職員のみが確認できることとする。 	<ul style="list-style-type: none"> ・申請者等から経営企画室職員又は教員が特定個人情報を受理した場合は、授受簿に記入する。また、教員と経営企画室の特定個人情報のやり取りも授受簿に記入する。 ・特定個人情報の保管については台帳を作成し管理する。 ・特定個人情報は、キャビネット等で施錠保管する。 ・特定個人情報の取扱区域は特別支援教育課、特別支援教育推進室、各校経営企画室執務室内に設定し、特別個人情報は取扱区域内のみで使用する。また、特別個人情報は、取扱者のうち、特別支援教育課職員、学校管理職及び経営企画室職員のみが確認できることとする。 ・団体内統合利用番号連携サーバシステム及び中間サーバを利用した庁内連携による入手は、関連業務システム以外からのアクセス制御を行っている。また、正当な権限のない利用者及び個別業務システム等からは、目的を超えた紐付けや必要のない情報は入手できないようアクセス制御を行っている。 		
令和3年6月18日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。） 入手の際の本人確認の措置の内容	②個人番号通知カード（番号確認）＋運転免許証等（身元確認）	②個人番号通知カード（番号確認※住所・氏名等に変更のないものに限る。）＋運転免許証等（身元確認）	事後	
令和3年6月18日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3. 特定個人情報の使用 リスク1 事務で使用するその他のシステムにおける措置の内容	・条例で定めた範囲以外では、庁内連携を行うことができないようシステム制御する。	・条例で定めた範囲以外では、庁内連携を行うことができないようアクセス制御する。	事後	文言の整理
令和3年6月18日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3. 特定個人情報の使用 リスク2 ユーザー認証の管理 具体的な管理方法	・学事事務システムは専用の端末からのみ閲覧が可能である。さらに、専用端末から学事事務システムを閲覧する際、パスワード認証を行う。この2要素の認証を施すことで、アクセス制御を行う。	・学事事務システムは専用の端末からのみ閲覧が可能である。さらに、専用端末から学事事務システムを閲覧する際、パスワード認証及び静脈認証を施すことで、アクセス制御を行う。	事後	時点修正
令和3年6月18日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3. 特定個人情報の使用 リスク2 特定個人情報の使用 の記録	・委託事項1事業者はユーザID、アクセス日時及び操作内容のログを取得するとともに、ウィルスの検知を実施し、特別支援教育課に定期的に報告する。	・委託事項1事業者はユーザID、アクセス日時及び操作内容のログを取得するとともに、ウィルスの検知を実施し、特別支援教育課に毎月報告する。	事後	
令和3年6月18日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3. 特定個人情報の使用 リスク3 リスクに対する措置の内容	・委託事項1事業者はシステムへのログインID全てを記録し、ログ分析を特別支援教育課に定期的に報告する。	・委託事項1事業者はシステムへのログインID全てを記録し、ログ分析を特別支援教育課に毎月報告する。	事後	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和3年6月18日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 4.特定個人情報ファイルの取扱いの委託 「特定個人情報の提供のルール」委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法	・特定個人情報の授受については、記録を残す。	・特定個人情報の授受については、記録を残す。また、外部記録媒体を使用する場合は、委託先からの作業申請書に基づき、書出し用のIDとパスワードを発行している。	事後	
令和3年6月18日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 4.特定個人情報ファイルの取扱いの委託 「特定個人情報の消去のルール」	保存期間満了後やハード更改等の際は、特別支援教育課の意思決定に基づき、システム運用保守受託者において、保存された情報が読み出せないよう、物理的破壊または専用ソフト等を利用して完全に消去する。特別支援教育課は、システム運用保守受託者が確実にデータ消去したことについて、証明書等の提出を受ける。	・外部記録媒体を使用した際は、外部記録媒体内のデータをすぐさま削除している。 ・保存期間満了後やハード更改等の際は、特別支援教育課の意思決定に基づき、システム運用保守受託者において、保存された情報が読み出せないよう、物理的破壊または専用ソフト等を利用して完全に消去する。特別支援教育課は、システム運用保守受託者が確実にデータ消去したことについて、証明書等の提出を受ける。	事後	
令和3年6月18日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 4.特定個人情報ファイルの取扱いの委託 「再委託による特定個人情報ファイルの適切な取扱いの確保」	システムの導入時における委託事項2で使用した申請書類等は業務終了後、速やかに各校に返却する。	削除	事後	特定個人情報ファイル作成及び登録支援業務委託の終了
令和3年6月18日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 4.特定個人情報ファイルの取扱いの委託 「特定個人情報の取扱いの委託におけるその他のリスク及びそのリスクに対する措置」	・学校と再委託事業者間での授受において、特定個人情報関係書類を送付する場合は、発送から受取りまでの証跡、事故発生時の補償、安定的なサービス提供の信頼性を有する、書留郵便、セキュリティ便等の手段を理由とするものとする。なお、学校は引渡し返却管理簿を用い、特定個人情報関係書類をいつ発送したか、いつ返却されたかの記録を個人単位でつける。 ・委託事業者から特別支援教育課への提出について、特定個人情報ファイルが保存された電磁記録媒体で送付する場合は、電子ファイルに暗号化を行い、強固で安全なケース等に格納、施錠した上で、発送から受取りまでの証跡、事故発生時の補償、安定的なサービス提供の信頼性を有する、書留郵便、セキュリティ便等の手段を利用するものとする。なお、委託事業者と特別支援教育課間で授受票を取り交わし、受渡状況を確認する。	削除	事後	特定個人情報ファイル作成及び登録支援業務委託の終了
令和3年6月18日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 5.特定個人情報の提供・移転(委託や情報提供ネットワークシステムを通じた提供を除く。)	記載なし	記載追加	事後	庁内連携があるため
令和3年6月18日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6.情報提供ネットワークシステムとの接続 リスク6「不正な提供が行われるリスク」	【中間サーバ・ソフトウェア】 (略) ③特に慎重な対応が求められる情報については自動応答を行わないように自動応答不可フラグを設定し、特定個人情報の提供を行う際に、送信内容を改めて確認し、提供を行うことで、センシティブな特定個人情報の提供が不正に提供されるリスクに対応している。 (略)	【中間サーバ・ソフトウェア】 (略) ③機微情報については自動応答を行わないように自動応答不可フラグを設定し、特定個人情報の提供を行う際に、送信内容を改めて確認し、提供を行うことで、センシティブな特定個人情報の提供が不正に提供されるリスクに対応している。 (略)	事後	
令和3年6月18日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6.情報提供ネットワークシステムとの接続 リスク6「不適切な方法で提供されるリスク」	【学事事務システム】 ②アクセスログを一定期間保管し、必要に応じてアクセスログを点検する。	【学事事務システム】 ②アクセスログを7年間保管し、必要に応じてアクセスログを点検する。	事後	
令和3年6月18日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7.特定個人情報の保管・消去 リスク7「特定個人情報の漏えい・滅失・毀損リスク」 ⑤物理的対策	【学事事務システムのデータ】 ②特別支援教育課の意思決定に基づき、システム保守受託者がマイナンバーデータを復元不可能な方法で消去する。また、受託者は確実に削除又は廃棄したことについて、証明書等を提出する。データ消去履歴としてシステム内に処理記録(特定個人情報ファイルの種類・名称、責任者・取扱部署、削除・廃棄状況等)を保存する。	【学事事務システム】 (1)サーバ等 ①システムサーバは専用施設内(管理区域)にある当該サーバ専用のラックに収容する。また、この区画への入退室管理は生体認証による入退室管理、区画ごとの施錠管理、監視カメラによる録画及び有人監視等を実施する。 ②保存期間満了後やハード更改等の際は、特別支援教育課の意思決定に基づき、システム運用保守受託者において、保存された情報が読み出せないよう、物理的破壊または専用ソフト等を利用して完全に消去する。特別支援教育課は、システム運用保守受託者が確実にデータ消去したことについて、証明書等の提出を受ける。 (2)外部記録媒体 外部記録媒体は施錠可能なキャビネット等に保管している。また権限が付与された外部記録媒体のみ使用可能としている。	事後	
令和3年6月18日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7.特定個人情報の保管・消去 リスク1「特定個人情報の漏えい・滅失・毀損リスク」 ⑤物理的対策	【中間サーバ・プラットフォーム】 中間サーバ・プラットフォームをデータセンタに構築し、設置場所への入退室管理、有人監視及び施錠管理をすることとしている。また、設置場所はデータセンタ内の専用の領域とし、他テナントとの混在によるリスクを回避する。	【中間サーバ・プラットフォーム】 ①中間サーバ・プラットフォームをデータセンタに構築し、設置場所への入退室管理、有人監視及び施錠管理をすることとしている。また、設置場所はデータセンタ内の専用の領域とし、他テナントとの混在によるリスクを回避する。 ②事前に申請承認されていない物品、記録媒体、通信機器などを不正に所持し、持出持込することがないよう、警備員などにより確認している。	事後	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和3年6月18日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7.特定個人情報の保管・消去リスク1「特定個人情報の漏えい・滅失・毀損リスク」 ⑥技術的対策	【学事事務システム】 ①ファイアウォールを設置し、許可していない端末やポート番号の通信遮断を行う。 ②ウイルス対策ソフトの定期的パターン更新を行うことにより、ウイルス感染を防止している。 ③インターネットや庁内の他のネットワークから分離された専用のネットワーク上で稼働する。 ④システムのアクセスログを記録・分析する。	【学事事務システム】 (1)サーバ等 ①ファイアウォールを設置し、許可していない端末やポート番号の通信遮断を行う。 ②ウイルス対策ソフトの定期的パターン更新を行うことにより、ウイルス感染を防止している。 ③インターネットや庁内の他のネットワークから分離された専用のネットワーク上で稼働する。 ④システムのアクセスログを記録・分析する。 (2)外部記録媒体 ①権限を付与した外部記録媒体のみ使用可能としている。 ②外部記録媒体にデータを書き出す場合は、権限のある者から発行されたIDとパスワードによる認証が必要である。	事後	
令和3年6月18日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7.特定個人情報の保管・消去リスク1「特定個人情報の漏えい・滅失・毀損リスク」 ⑨過去3年間以内に、評価実施機関において、個人情報に関する重大事故が発生したか	「その内容」 ①平成27年に都立高校教諭が生徒236名分の個人情報を含む記載のある教務手帳を校内で紛失した。全教職員で校内等を捜索したが発見されていない。なお、二次被害は発生していない。 ②平成29年に都立高校養護教諭が平成27年度卒業生192名の生徒健康診断票(5年保存)が所在不明となっていることに気付いた。同日、校長が当該養護教諭に聞き取りをしたところ、保存期限が経過した文書(平成22年度末卒業生の生徒健康診断票等)を廃棄するための書類整理を行った際、保存期限が到来していない健康診断票が誤って混入し、同年2月14日、業者委託による細断処理により他の文書とともに廃棄してしまった可能性が高いことが判明した。 「再発防止の内容」 ①同校では改めて所属教職員に対して個人情報の管理が適切に行われるよう、職場環境の整備及び教務手帳等、個人情報の管理の徹底に努めるとともに、副校長が休憩時間及び退庁時等に職員の机を目視し、個人情報が放置されていることがないか等の確認を行うことにより、個人情報の紛失を防いでいくこととした。 ②今後、生徒健康診断票の毎年度の整理の際や文書の廃棄に当たっては、複数人で対応し確認するなど、個人情報の管理や取扱いについて更に徹底する。	「その内容」 ①平成27年から平成29年までの間に、都立高等学校主任教諭が、当時勤務校において、同校入学者選抜応募者の受験番号、氏名、総合成績等の個人情報に係る電子データ延べ2,224名分を、SDカードに保存し、同校に置いたままにしたことにより紛失した。また、平成29年に、同校において、609名分の同データを、別のSDカードに保存して持ち出し、その後、異動先の勤務校に持ち込んだ。さらに、平成29年から令和2年までの間に、同校において、同校入学者選抜応募者の同個人情報に係る電子データを、同SDカードに保存するとともに、延べ3,082名分の同データが保存された同SDカードを紛失した。 ②令和2年に、都立図書館職員が、講演会への参加当選者231名に対して抽選結果を電子メールで知らせる際、メールアドレスをメールのBCC欄でなく宛先欄に入力して一斉送信したため、他の当選者の個人情報(メールアドレス)が流出した。 「再発防止の内容」 ①入学者選抜に関するデータの保存や管理方法等について、改めて注意喚起を行うとともに、入学者選抜用パソコンの設定を変更する際には、管理職又は管理職立会いの下で管理職に指名された者が行うことに改めるなど、再発防止に向けた個人情報の適切な管理について徹底を図っていく。 ②今後、都民等にメールを送信する際には、複数の職員で送信先及び添付ファイル等について確認することを徹底する。また、同様の事故が起きないよう、個人情報を厳正に管理するとともに、職員に対し情報セキュリティの教育・指導を徹底していく。	事後	時点修正
令和3年6月18日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7.特定個人情報の保管・消去リスク3「特定個人情報が消去されずいつまでも存在するリスク」	【学事事務システムのデータ】 特別支援教育課の意思決定に基づき、システム保守受託者がマイナンバーデータを復元不可能な方法で消去する。また、受託者は確実に削除又は廃棄したことについて、証明書等を提出する。データ消去履歴としてシステム内に処理記録(特定個人情報ファイルの種類・名称、責任者・取扱部署、削除・廃棄状況等)を保存する。	【学事事務システムのデータ】 保存期間満了後やハード更改等の際は、特別支援教育課の意思決定に基づき、システム運用保守受託者において、保存された情報が読み出しできないよう、物理的破壊または専用ソフト等を利用して完全に消去する。特別支援教育課は、システム運用保守受託者が確実にデータ消去したことについて、証明書等の提出を受ける。	事後	
令和3年6月18日	Ⅳ その他のリスク対策 1. 監査 ①自己点検	・毎年1回、個人情報保護について、全職員が自己点検を用いて、チェックを実施している。	<学事事務システムにおける措置> ・特別支援学校の職員は、毎年1回以上、特定個人情報の取扱いについて研修を実施している。また、個人情報保護について、全職員が自己点検を用いて、チェックを実施している。 <中間サーバ・プラットフォームにおける措置> 運用規則に基づき、中間サーバ・プラットフォームの運用に携わる職員及び事業者に対し、定期的に自己点検を実施することとしている。	事後	
令和3年6月18日	Ⅳ その他のリスク対策 2. 従業者に対する教育・啓発	全職員を対象に、e-ラーニングにおいて情報セキュリティ・個人情報保護の必修研修を実施している。研修の目的は、個人情報保護の重要性及び適正管理等に関する理解を深め、個人情報保護の遵守を徹底している。また、委託事業者に対しては、業務開始に当たり、個人情報の取扱いルールを順守することを確認させている。	<東京都教育委員会における措置> 全職員を対象に、e-ラーニングにおいて情報セキュリティ・個人情報保護の必修研修を実施している。研修の目的は、個人情報保護の重要性及び適正管理等に関する理解を深め、個人情報保護の遵守を徹底している。また、未受講者に対しては、研修機関から職場の管理・監督者を通じて研修を受講するよう指導を行っている。 また、委託事業者に対しては、業務開始に当たり、個人情報の取扱いルールを順守することを確認させている。 <中間サーバ・プラットフォームにおける措置> ・中間サーバ・プラットフォームの運用に携わる職員及び事業者に対し、セキュリティ研修等を実施することとしている。 ・中間サーバ・プラットフォームの業務に就く場合は、運用規則等について研修を行う事としている。	事後	
令和3年6月18日	Ⅳ その他のリスク対策 3. その他のリスク対策	—	<中間サーバ・プラットフォームにおける措置> 中間サーバ・プラットフォームを活用することにより、統一した設備環境による高レベルのセキュリティ管理(入退出管理等)、ITリテラシーの高い運用担当者によるセキュリティリスクの低減、及び技術力の高い運用担当者による均一的で安定したシステム運用・監視を実現する。	事後	