

公益財団法人  
スペシャルオリンピックス日本

# 個人情報保護管理マニュアル

- A) スペシャルオリンピックス日本スタッフの責務
- B) 個人情報保護管理マニュアル 基本事項
- C) 個人情報を持ち出す必要がある場合の漏洩予防策
- D) 個人情報漏洩時 事案報告の流れ
- E) 個人情報漏洩時 連絡系統
- F) 個人情報漏洩時 対処リスト

## 附則

1. 本マニュアルの改廃は代表理事が行う。
2. 本マニュアルは、平成24年(2012年)12月6日から施行するものとし、同年4月1日から適用する。
3. 改正 平成27年(2015年)3月3日
4. 改正 平成28年(2016年)9月14日
5. 改正 平成29年(2017年)2月22日



## スペシャルオリンピックス日本 個人情報保護管理 マニュアル

### A) スペシャルオリンピックス日本スタッフの責務

スペシャルオリンピックス日本のスタッフは、スペシャルオリンピックス日本(以下、「SON」という)の作成する「個人情報保護管理マニュアル」を熟読し、個人情報保護を徹底し、万が一個人情報漏洩が発生した場合、マニュアルに従った対応ができるよう、十分な準備を行うものとする。

### B) 個人情報保護管理マニュアル 基本事項

#### ① 個人情報保護意識の徹底

- ・ 個人情報保護研修会の実施(SONスタッフは年1回は必須)
- ・ SONスタッフの個人情報保護意識と自覚を高めるため人材教育の場を設ける。
- ・ 個人情報保護の重要性を伝える。
- ・ 個人情報保護管理および漏洩時の対応に備えるため、SONは、個人情報保護管理者(以下、「保護管理者」という)、個人情報保護担当者(以下、「保護担当者」という)を決定する。

#### ② 通常業務における個人情報保護

##### 記録媒体管理

- ・ SONが保有する個人情報を、私物のパソコンで使用してはならない。
- ・ SONが保有する個人情報を保存した情報記録媒体(USBメモリースティックなど)を、許可なくSON事務局外に持ち出してはならない。電子メールその他の方法により外部に送信することも同様に禁止する。
- ・ SONが指定する情報記録媒体(USBメモリースティックなど)以外に個人情報を保存してはならない。
- ・ パソコンについては誤作動による個人情報漏洩のないようにウイルス対策ソフトを導入し、定期的なウイルスチェックを徹底する。

##### 不正アクセス防止

- ・ アポイントのない来客は受けない。
- ・ 施錠を徹底し、部外者の侵入、個人データ・データベースへのアクセスを制限する。
- ・ 個人情報を記載、記録した全ての文書、メモ書き、Emailなどは、保有の必要がなくなり次第、速やかにシュレッダーにかける、復元不可能な方法でデータを消去する等の破棄処理を行う。

## C) 個人情報を持ち出す必要がある場合の漏洩予防策

### 紙媒体の書類等

事前管理	<p>① 外出・出張する前に個人情報を書面にて持ち出す必要があるか確認する。</p> <p>② a. 必要がない 生年月日、氏名、住所、電話番号、Email アドレス情報等の個人情報を持ち出す資料より消去する(原則として、資料そのものを除外することとし、資料が不可分である場合には、個人情報部分を黒塗りするなど、判読不可能な状態にすること)。</p> <p>b. 必要がある</p> <ul style="list-style-type: none"> <li>・ 案件書にて、持ち出しに関する案件名、持ち出す目的、日時、内容、持ち出し部数について、保護管理者の決裁を受ける。</li> <li>・ 決裁を受けた情報以外は資料に入れてはならない。</li> <li>・ 持ち出す資料を一覧にし、正確に把握する。</li> <li>・ 書面には管理番号をつけ、決裁を受けた部数のみ持ち出すことができる。一見して個人情報であると分からないような形式でファイリングすること。</li> </ul>
現場管理	<p>個人情報を書面にて事務局外に持ち出す場合は、以下の事項に厳重に留意する。</p> <p>① 使用時: 盗難・複写のないよう、一人以上の SON スタッフの目の届く場所に置く、また身につける。</p> <p>② 未使用時: ファイルは肌身離さず持つか、関係者以外入ることの出来ない場所へ保管する。</p> <p>③ 使用后: 書面が全てあるか、部数・管理番号を確認する。</p>
事後管理	<p>① 事務局へ帰着後、再度、書面が全てあるか、部数・管理番号を確認する。</p> <p>② 加筆・修正などの必要なデータを入力し、入力内容を保護管理者に報告する。</p> <p>③ 持ち出した書面につき、保護管理者の指示に従い、保管あるいは廃棄を行う。</p> <p>④ 持ち出した書面につき、書面にて保存する必要がなければ、シュレッダーにかける方法で廃棄する。</p>

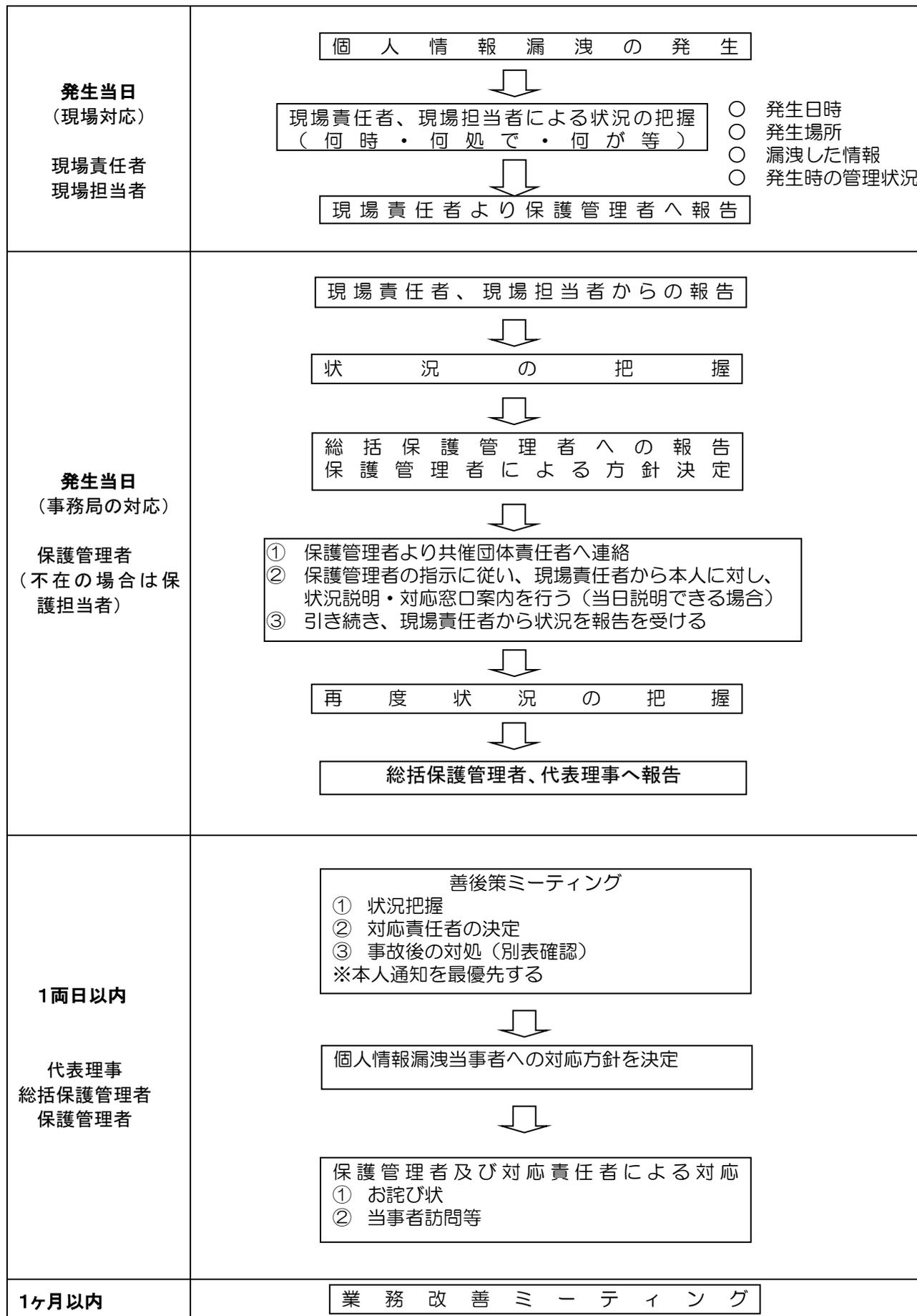
### 電子データ

事前管理	<p>① 外出・出張・Fax・Email をする前に個人情報を電子データにて持ち出す、あるいは送信する必要があるか確認する。</p> <p>② a. 必要がない 生年月日、氏名、住所、電話番号、Email アドレス情報等の個人情報を持ち出す、あるいは送信する資料より消去する(原則として、資料そのものを消去もしくは除外することとし、資料が不可分である場合には、個人情報部分を削除、ブランク、あるいは黒塗りするなど、判読不可能な状態にすること)。</p> <p>b. 必要がある</p> <ul style="list-style-type: none"> <li>・ 案件書にて、持ち出しに関する案件名、持ち出す目的、日時、内容について、個人情報保護管理者の決裁を受ける。</li> <li>・ 決裁を受けた情報以外は資料に入れてはならない。</li> <li>・ 持ち出すデータを一覧にし、正確に把握する。</li> <li>・ 外出・出張に際し、持ち出しの決裁を得たデータについては、SONが指定する管理番号付きの指定の USB(暗号化対応)にデータをコピーして持ち出すこと。</li> <li>・ Fax にて送信する場合には、必ず送信先に事前に連絡し、送付先の担当者が確実に受領できることを確認した上で送信すること。</li> <li>・ Email にて送信する場合は、必ず該当する添付ファイルにパスワードを付して送信し、パスワードは、当該メールとは別のメールにて送信すること。</li> </ul>
現場管理	<p>外出・出張の際、個人情報をデータにて事務局外に持ち出す場合は、以下の事項に厳重に留意する。</p> <p>① 使用時: 盗難・複写のないよう一人以上の SON スタッフの目の届く場所に置く、また身につける。</p> <p>② 未使用時: 記録媒体は肌身離さず持つか、関係者以外入ることの出来ない場所へ保管する。</p> <p>③ 使用后: 持ち出した記録媒体があることを確認する。</p>
事後管理	<p>① 外出・出張先から事務局へ帰着後、再度、記録媒体があるか、また、記録媒体の管理番号が持ち出し時と同じか確認する。</p> <p>② 加筆・修正などの必要なデータを記録し、入力内容を保護管理者に報告する。</p> <p>③ 持ち出した記録媒体につき、保護管理者の指示に従い、保管あるいは廃棄、データの消去を行う。</p>

## D) 個人情報漏洩時 事案報告の流れ

	現場	事務局
個人情報漏洩発覚 事実関係の確認	<p>①漏洩の事実を認識した現場担当者は、直ちに現場責任者へ報告する。</p> <p>②その際、現場担当者は、①と同時に(ただし、確認に時間を要する場合は①の後速やかに)次の事項(以下、「漏洩状況」という)を必ず確認し、現場責任者に報告する。</p> <ul style="list-style-type: none"> <li>○ 何時(発生日時)</li> <li>○ 何処で(発生場所)</li> <li>○ 何の情報が(漏洩した情報の利用目的、項目、センシティブ情報の有無、件数、暗号化措置の有無)</li> <li>○ なぜ(漏洩時の管理状況)</li> <li>○ どうなっているか(現時点での被害の有無)</li> </ul>	
事務局への報告	<p>①現場責任者は、保護管理者(不在の場合は保護担当者、以下同じ。)へ「漏洩状況」を直ちに口頭にて報告する。</p> <p>②現場責任者は、「漏洩状況」について報告書を作成し、保護管理者に提出する。</p>	<p>①保護管理者が報告を受ける。</p> <p>②保護管理者は、現場責任者から報告を受けた内容を直ちに総括保護管理者へ報告する。</p> <p>③協力、共催の個人・法人・団体がある場合は、保護管理者は、総括保護管理者の承諾を得て、当該団体の責任者へ漏洩状況を連絡する。</p>
本人への通知	<p>現場で個人情報漏洩当事者へ説明する場合</p> <p>①現場責任者は、保護管理者の指示に従い、漏洩状況を説明、お詫びし、今後の対応窓口をご案内する。</p> <p>現場で説明できない場合</p> <p>②保護管理者から状況を説明、お詫びし、今後の対応窓口をご案内する。</p>	<p>①保護管理者は、個人情報漏洩状況を把握し、総括保護管理者に報告した上で、総括保護管理者の承諾を得て、本人へ説明の方法を決定する。</p>
対応策の決定		<p>①保護管理者は、現場責任者から提出された報告書、及び現場責任者から事情を聴取する方法により事実関係を確認し、総括保護責任者・代表理事に対し、事実関係を報告する。</p> <p>②代表理事、総括保護責任者、保護管理者は、協議の上、対応策を決定、実施する。</p>

E) 個人情報漏洩時 連絡系統



## F) 個人情報漏洩時 対処リスト

優先事項	責任者	対応内容
1. 本人への通知	理事長 保護管理者 現場責任者	二次被害防止の為、以下のいずれかの項目により速やかに通知する。 <ul style="list-style-type: none"> <li>現場責任者より保護管理者に連絡後、その場で経緯を説明</li> <li>現場責任者より郵便にて事実関係を説明</li> <li>事案の軽重に応じ、理事長又は保護管理者より本人の希望する場所に訪問して説明</li> </ul>
2. 事件の公表	理事長・保護管理者	社会的な影響があると考えられる場合は公表する。公表の要否は、運営諮問会議に諮った上で、理事長が決定する。
3. 関係者への説明および謝罪	理事長・保護管理者	対象となる関係者及び関係組織に対し、文書・電話・訪問などにより説明、謝罪する。
4. 原因調査	現場責任者・システム管理者	発生状況、アクセスログなどの調査から事故の原因や経過を迅速に調査する。
5. クレーム・マスコミ対応	保護管理者・広報	対応窓口は総務部とし、保護管理者のみが、メディア及びクレームへ対応する。
6. 事故再発防止	保護管理者・現場責任者	流出の原因調査から改善点を明確にし、再発防止策を作成する。
7. 訴訟への準備	代表理事・保護管理者	証拠書類を揃え、担当弁護士と連絡をとる。
8. 終結のお知らせ	広報	クレーム・マスコミ対応を行い、再発防止策を決定、実施した上で、関係団体・関係者へ報告を行なう。 また、必要に応じ、ホームページを通じて事件の概要、再発防止策を公表する。 * 公表の仕方(HP 開示・非開示)は、運営諮問会議に諮った上で、理事長が方針を決定する。

# 個人情報に関する報告書(漏洩)

報告日時	月 日 ( ) 午前・午後 時 分		
報告者	会場名		
	役職・氏名		
発生事案名			
発生日時	月 日 ( ) 午前・午後 時 分		
発生場所			
事案の概要			
関係者氏名	関係者	住所	
		氏名	
	関係者	住所	
		氏名	
	関係者	住所	
		氏名	
備考			

## 『確認事項』

- 何時(発生日時)
- 何処で(発生場所)
- 何の情報が(漏洩した情報の利用目的、項目、センシティブ情報の有無、件数、暗号化措置の有無)
- なぜ(漏洩時の管理状況)
- どうなっているか(現時点での被害の有無)