

～はじめに～ (情報セキュリティ全般)

- 1 個人情報とは、
 - ➡個人に関する情報であって特定の個人を識別することができるもの。
- 2 個人情報保護の必要性
 - プライバシーの権利
「私生活をみだりに公開されないという法的保障ないし権利」
 - 個人情報の流出は、プライバシーの侵害にあたります。
 - 流出してしまうと →①実害の発生 (DV・ストーカー・売り込み)。
②被害者への謝罪・補償。
③組織の社会的信用の失墜。
- 3 情報セキュリティとは
 - ➡情報の機密性、完全性、可用性を維持していくこと。
 - 機密性：アクセスを認可された者だけが情報に確実にアクセスできること。
 - 完全性：情報資産が完全な状態で保存され、内容が正確であること。
 - 可用性：情報資産が必要になったとき、利用できる状態にあること。
- 4 情報資産とは
 - ➡保有している情報全般のこと。個人情報等の情報自体に加え、ファイルやデータベースといったデータ、USBメモリ等のメディア、紙の資料も情報資産。
- 5 プライバシーポリシーと情報セキュリティポリシー
 - ➡前者は、個人情報保護に関する協議会のあり方・考え方を示すもの。
後者は、具体的に情報を守るための対策方法を示すもの。
- 6 プライバシーポリシーの概要
 - (1)基本方針 個人情報に関する関係法令を遵守し、適切に保護・管理。
 - (2)主な内容 ①個人情報は、協議会事業に必要な最小限の内容を適法かつ公正な手段で取得し、承諾された利用目的の範囲内でのみ利用。
②個人情報に関する必要かつ適切な安全管理措置の実施。
- 7 情報セキュリティポリシーの概要
 - (1)目的 管理する個人情報を適切に保護する為に実施すべき対策を定める。
 - (2)主な内容 ①物理的セキュリティの実施
個人情報の管理・PC管理・通信回線管理
②人的セキュリティの実施
周知・研修・業務及び活動目的外での使用禁止・退会時遵守事項
③技術的セキュリティの実施
不正プログラム対策・ソフトウェアインストール事前承認・通信情報暗号化
④情報セキュリティポリシー及び関係規定の適切な見直し

第1章 情報セキュリティ実施手順について

- 1 目的 本協議会の保有する情報資産の適正な管理及び取扱いを行うこと。
- 2 対象範囲
 - (1)対象者 協議会委員及び事務局職員(以下、「委員等」とします)。
 - (2)範囲(施設・設備) ① 事務局執務室(荻窪地域活動係執務室)
② 委員活動場所(荻窪地域区民センター内)
- 3 管理・運用に関わる役割 管理責任者 = 協議会会長(事務局長へ代行指示可)

第2章 情報資産全般について

事件例

- A会社の職員は、私用目的で顧客の記録を閲覧し、故意に外部に情報を漏らした。
- B会社の職員は、退職前にB社の顧客情報を無断で入手し、転職先で利用した。

1 情報資産の利用

- (1)協議会の事業実施目的でのみ利用。

例) 委員等は、協議会の業務活動についてのみ、協議会のメールアドレスを使用し、またパソコン等からのインターネットへのアクセスを行うことができます。

- (2)個人番号及び特定個人情報の利用は、番号法に基づき以下の事務のみ。

| 事務の名称 | 利用の根拠となる法令 |
|--------------------------|------------|
| 個人番号関係事務 源泉徴収票等の法定調書作成事務 | 番号法第9条第3項 |

2 情報資産の範囲

| 分類 | 情報資産 |
|--------|---|
| 紙媒体 | ・事務で使用するもの |
| 記録媒体 | ・事務で使用する CD、DVD、USB メモリ、外付け HDD 等の情報資産を記録した媒体 |
| 電子データ | ・記録媒体やパソコン、タブレット、その他の機器等に電子的に記録されたデータ |
| ハードウェア | ・個別パソコン、個別プリンタ等の事務で使用する機器 |
| ソフトウェア | ・個別に購入等しパソコンにインストールしたもの(ライセンス管理対象のみ) |

3 情報資産目録の作成及び管理

- (1)目録作成 情報資産を、情報資産目録(様式1)に記載。
- (2)管理 管理責任者は、情報資産目録を随時、点検し、適宜、追記削除。

4 退会時の遵守事項

委員等は、退会等により協議会の業務活動を離れる場合には、利用していた情報資産等を廃棄又は返却してください。

第3章 紙媒体等の情報資産の取扱いについて

事件例

- C町では、台風で被災した方の支援をするために住民情報を作成し、USBメモリを使ってデータを移行させた後に当該メモリの所在が不明となった。
- D社では、応募者に対して案内メールを送信する際に、誤って985名分のメール情報を全員に送信してしまった。
- E社が廃棄した古紙について、回収業者が仕分けしたところ、大量の個人情報が記載された帳簿があったとの届出があった。

1 保管時の取扱い

- (1)保管場所を定め、保管場所を情報資産目録に記載。
- (2)情報資産のうち、特に個人情報等の機密情報、事業上重要な情報の場合
➡ 第三者が容易に入室できない執務室内の書庫等に施錠して保管。

2 持ち出し・送信時の取扱い

- (1)個人情報等を含む紙媒体等のセンターの外への持出し➡原則として禁止。
例外的に、管理責任者より持出許可を得た場合には行えますが、情報資産持出し管理簿(様式2)に記載することが必要。
- (2)「個人情報を含む電子データ」のメール又はFAXでの送信➡原則として禁止。
例外的にやむを得ず送信する必要がある場合には行えますが、管理責任者にも併せて送信することが必要。

3 個人情報を含む紙媒体の複写・電子データ化 ➡原則として禁止。

例外的に、事務上必要な場合には行えますが、複写時は、必要な個所以外を不可視とする処理(マスキング等)が必要。

4 廃棄時の取扱い

- (1)個人情報等を含む紙媒体➡シュレッダー処理をしたうえで廃棄。
- (2)記録媒体➡物理的消去又は論理的消去により、データを復元不可能な状態にしたうえで廃棄。
※物理的消去(磁気消去、破碎・粉碎)
論理的消去(管理責任者の許可を得たデータ消去ソフトウェア等の使用)
- (3)保存する必要がなくなった電子データ➡消去。

5 定期的な確認

管理責任者は、情報資産持出し管理簿の記載内容を確認(月1回)。改善。

第4章 情報システムについて

事件例

○ F町の職員は、使用権限のないパスワードを使って組織内の情報を閲覧したことが判明した。

○ G県のファイル共有サーバーで使用されていたハードディスクがネットオークションで転売され、内部データが流出した。サーバー更新の際にハードディスクの入れ替えを行ったが、内部データの消去が不十分な状態だったことがわかった。

1 情報システムへの記録媒体の接続

管理責任者が許可した USB 等の記録媒体等のみ、接続が可能。

2 ログインパスワードの扱い

(1)設定 パソコン等は、ログインパスワードの入力を必要とするよう設定。

(2)管理 委員等は、自己の管理するログインパスワードにつき協議会外部の者に知られないように管理。

3 不正プログラムへの対策

パソコン等に不正プログラム対策ソフトを導入するなど適正な対応を実施。

4 個人情報の暗号化

ホームページ上に個人情報を入力して講座等に応募する方との通信では、情報の暗号化が必要。

5 インターネット回線の通信ケーブルの配線

⇒第三者が容易に触れられないよう、床下配線等が必要。

6 パソコン等の盗難防止

(1)ノート型パソコン等⇒ 書庫等に施錠保管。

(2)デスクトップ型パソコン等⇒ セキュリティワイヤー等による盗難防止措置実施。

7 ライセンスの管理(ライセンス管理が必要なソフトウェアの扱い)

ライセンス保有数及び使用数を記録、使用数が保有数を超えないように管理。

8 廃棄

物理的又は論理的消去により、データを復元不可能な状態にしたうえで廃棄。

第5章 施設・設備について

事件例

○ 夜間に無人の事務所に窃盗犯が侵入し、机の上に置いてあった、顧客情報が入ったUSBメモリとフロッピーディスクが盗まれた。

1 執務室等への立入り制限

(1) 委員等以外の者が立入る場合

➡ 委員等の許可及び立会、入退室管理簿(様式3)への記載が、必要。

(2) 委員等は、事務上必要時に立入禁止等の情報保護の適切な対策が必要。

2 個人情報等を含む情報資産を保管する書庫等

➡ 執務室等の中に設置。

3 鍵の管理

(1) 書庫等の鍵は、適正な場所に保管し、保管場所は鍵管理簿(様式4)に記載。

(2) 必要に応じてスペア鍵を用意。別の施錠可能な場所に保管。

4 施錠・開錠の管理

(1) 事務開始時に必要な書庫等を開錠し、事務終了時に施錠。

(2) 委員等が執務室等から不在になる際は、書庫等は必ず施錠。

(3) 最後に執務室等を退出する者は、全ての書庫等を施錠し、施錠結果を書庫等施錠管理簿(様式5)に記載。

※書庫等の設置部屋に施錠できる場合は、部屋の施錠確認をもって、書庫等の施錠確認に代替可能。

5 管理状況の確認 管理責任者が、書庫等施錠管理簿の内容を月1回確認。

第6章 セキュリティ事件・事故について

1 セキュリティ事件・事故(以下「事件等」とする)の事象

(1) 施設・設備の場合 ➡ 鍵の紛失、漏えい

(2) 紙媒体及び記録媒体の場合 ➡ 紛失、漏えい

(3) 電子データの場合 ➡ 紛失、漏洩、不正アクセスによる破壊、改竄、流出

2 事件等発生時における対応のために

(1) 事件等に関する報告連絡体制の整備

① 発生時の連絡体制は、セキュリティ事件・事故連絡体制(様式6)に記載。

② 本連絡体制は、緊急時にすぐに利用できるように整備。

(2)一次報告

事件等を発見した委員等は、管理責任者に口頭又は書面で下記の内容を速やかに報告。

- ①発生した又は発生しているセキュリティ事件・事故の内容
- ②情報資産に対する被害状況
- ③発見日時

(3)事件・事故等への処置例

- ①紛失、漏えい⇒ 紛失、漏えいした情報資産を特定し、対応を協議。
- ②不正アクセスによる破壊、改竄、流出⇒ システム保守委託業者に連絡し、アクセスログ調査、データ復旧等を依頼。

3 セキュリティ事件・事故発生後の対応

管理責任者は、事件・事故内容を委員等へ周知すると共に、事務局長を通し、杉並区地域課長へ報告。

第7章 情報セキュリティ研修について

1 研修の実施

- (1)内容 ①番号法、杉並区特定個人情報取扱規程など、必要な知識の理解。
②情報セキュリティ実施手順の理解。
③前回研修以降、発生したセキュリティ事件・事故の把握。
④その他、管理責任者が必要と判断する研修。
- (2)対象者 研修は、管理責任者が協議会委員等に対して行う。
- (3)時期 ①協議会委員等⇒ 定期的な研修の実施。
②年度中に新規加入者等がいた場合⇒ 速やかな研修の実施。
③情報資産の変更による事務の大幅な変更、手順対象範囲見直し、事件等の発生等で、管理責任者が研修を必要と判断した場合
⇒事務に関連する職員に対して必要な内容の研修の実施。

第8章 特定個人情報等の取扱いに関する手順

1 管理体制

- (1)事務取扱担当者の指名等
 - ①特定個人情報事務取扱者名簿(様式7)の作成。
 - ②担当者変更時における、速やかな特定個人情報取扱者名簿への反映。
- (2)情報セキュリティ事件・事故等の未然防止
 - ① 事務取扱担当者は、下記について、速やかに管理責任者に報告。
 - ・特定個人情報等に対する事件・事故の発生又はその兆候
 - ・事務取扱担当者が取扱規程等に違反している事実又はその兆候
 - ②管理責任者は、①の報告に対して事実を調査し安全措置実施。

2 特定個人情報等の取扱い

(1)利用の制限 「報酬等の法定調書の作成に関する事務」でのみ利用。

(2)提供の求めの制限

「報酬等の法定調書の作成に関する事務」処理に必要な場合のみ。

(3)特定個人情報ファイルの作成の制限

「報酬等の法定調書の作成に関する事務」処理に必要な場合のみ。

(4)収集・保管の制限

番号法第 19 条第2号及び第3号に該当する場合以外の収集・保管禁止。

※第2号 個人番号関係事務実施者(行政機関)が個人番号関係処理するために必要な限度で特定個人情報を提供するとき。

第3号 本人またはその代理人が個人番号利用事務実施者(協議会)に対し、当該本人個人番号を含む特定個人情報を提供するとき。

(5)アクセス制限

①事務取扱担当者は、業務上の目的のみ特定個人情報等を取り扱える。

②アクセス権の設定可能な状態の特定個人情報等

→事務取扱担当者のうち、必要最小限の範囲でアクセス権限を付与。

③アクセス権限の設定不能な特定個人情報等

→特定個人情報等の保管場所や記録媒体の扱いに工夫し、事務取扱担当者以外の者が容易に使用できない措置とする。

④アクセス権限の設定ができない特定個人情報等の閲覧、使用時の記録

→特定個人情報等受払簿(様式8)、特定個人情報等使用記録簿(様式9)に記録すること。

(6)複製・運搬等の制限

①操作ログを取得できない特定個人情報等の複製時の扱い

→特定個人情報等複製・運搬記録簿(様式10)に記録すること。

②特定個人情報等を取扱う事務を実施する区画間の運搬時の扱い

→事務取扱者のみが行い、上記記録簿に記録すること。

③特定個人情報を含む情報資産の協議会事務局執務室外への持出禁止

※②で定める場合及び法定調書提出等の個人番号利用事務実施者が提出を求める書類の提出を行う場合を除く。

④特定個人情報等を含む情報資産を運搬する場合の制限

→特定個人情報等を収納する鞆・ケース等は施錠の行えるものを使用し、運搬時には、鞆等は終始携帯し、本運搬に必要な箇所以外への立ち寄りを禁止する。(同一施設内における運搬を除く。)

(7)特定個人情報等を含む情報資産の廃棄及び保管手順

→「第3章 紙媒体等の情報資産の取扱い手順」に準ずる。

- (8)特定個人情報等の内容に誤り等を発見した場合
→その訂正等を行い、管理責任者に報告すること。
- (9)個人番号の提供を受ける場合
→番号法第 12 条及び「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に基づく国税関係手続に係る個人番号利用事務実施者が適当と認める書類等を定める件(国税庁告示第 2 号)」に基づき、適切に本人確認を行うこと。
＝個人番号の漏洩などの事件事故が発生しない措置をとり、相手方の身分を既定の身分を証明するものにより確認すること。
- (10)個人番号関係事務において特定個人情報等を入手する場合
→個人番号の利用目的(利用範囲)を明記した書面を本人(若しくは番号法施行令第 12 条に定めのある代理人)に提示すること。
- (11)特定個人情報の提供する場合
①当該提供が報酬等の法定調書の作成に関する事務の範囲内である事を確認すること。
②提供を行う前に、提供先における利用目的、利用する業務の根拠法令、利用する記録範囲及び記録項目、利用形態等について特定個人情報保護評価書等により明確化すること。
- (12)情報システムに特定個人情報等の入力、削除、訂正等の処理を行う場合
→処理者と点検者を別にし、二重チェックを行うこと。
- (13)入力端末に関する取扱い
①特定個人情報等の入力、削除、訂正等の処理を行う端末(「入力端末」)は、協議会が用意したパソコンのみとする。
②事務取扱担当者が入力端末設置場所から離席する場合は、入力端末からのログオフ又は入力端末をロックする。

3 特定個人情報等の取扱い状況の確認

管理責任者は、毎月 1 回、特定個人情報等受払簿、特定個人情報等使用記録簿、特定個人情報等複製・運搬記録簿の記載内容の確認を行う。

様式集

様式1 情報資産目録

情報資産目録

| 協議会名： | | 更新年月日： | | |
|--------|-------|---------|-----------|------|
| カテゴリー | 情報資産名 | 設置・保管場所 | 特定個人情報の有無 | 特記事項 |
| 紙媒体 | | | | |
| 記録媒体 | | | | |
| 電子データ | | | | |
| ハードウェア | | | | |
| ソフトウェア | | | | |

様式2 情報資産持ち出し管理簿

情報資産持ち出し管理簿（ 年 月分）

| 持ち出し日 | 持ち出す情報資産 (ファイル名・書類名) | 持ち出し者 | 承認者 | 返却日 | 返却確認者 |
|-------|-------------------------|-------|-----|-----|-------|
| | | | | | |
| | | | | | |
| | | | | | |

様式3 入退室管理簿

入退室管理簿（ 年 月～ 月）

| 協議会名： | | | | | | | |
|-------|----|------|------|----|----|----|---------------|
| No. | 月日 | 入室時間 | 退室時間 | 所属 | 氏名 | 目的 | 協議会委員等 確認欄 |
| | | | | | | | |
| | | | | | | | |

様式4 鍵管理簿

鍵管理簿

| 協議会名： | | | | 更新年月日： | |
|-------|------|--------|---------|---------------|--|
| No. | 鍵の名称 | 鍵の保管場所 | 施錠する書庫等 | スペア鍵の 保管場所 | |
| | | | | | |
| | | | | | |
| | | | | | |

様式5 書庫等施錠管理簿

書庫等施錠管理簿 (年 月分)

| 日付 | 施錠チェック (書庫No.) | | | | | | | | | | | | | | | 確認者 | |
|----|----------------|---|---|---|---|---|---|---|---|----|----|----|----|----|----|-----|--|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | | |
| | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |

様式6 セキュリティ事件・事故連絡体制

セキュリティ事件・事故連絡体制

1 協議会内部連絡体制

セキュリティ事件・事故発見者は以下の順位で報告する。

| 順位 | 氏名 | 役職 | 連絡先 |
|----|-------|----|---------------|
| 1 | 〇〇 〇〇 | 会長 | 090-xxxx-xxxx |
| 2 | | | |

2 区連絡体制

セキュリティ事件・事故対応のために必要な区内部の連絡先は以下のとおり

| 連絡相手 | 役割 | 連絡先 |
|--------|-------|---------|
| 地域課〇〇係 | 協議会支援 | 内線 xxxx |
| | | |

3 協議会外部連絡体制

セキュリティ事件・事故対応のために必要な区外部の連絡先は以下のとおり

| 連絡相手 | 役割 | 連絡先 |
|------|------------|--------------|
| 〇〇〇社 | ホームページ保守業者 | 03-xxxx-xxxx |
| | | |

様式7 特定個人情報事務取扱者名簿

特定個人情報事務取扱者名簿

| 利用者名 | 取扱う特定個人情報の範囲 | 指定年月日 | 解除年月日 | 備考 |
|------|--------------|-------|-------|----|
| | | | | |
| | | | | |

様式8 特定個人情報等受払簿

特定個人情報等受払簿

| 受払簿 No. | 入手 | | 特定個人情報等 (ファイル名・書類名) | 入手目的 | 提出/廃棄 | | | 備考 |
|---------|-----|-----|---------------------|------|-------|----|-----|----|
| | 年月日 | 取扱者 | | | 年月日 | 事由 | 取扱者 | |
| - | | | | | | | | |
| - | | | | | | | | |

様式9 特定個人情報等使用記録簿

特定個人情報等使用記録簿 (年 月～ 月)

| 使用日時 | 使用する特定個人情報等 | | 使用目的 | 使用者 | 備考 |
|------|-------------|-------------|------|-----|----|
| | 受払簿No. | (ファイル名・書類名) | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

様式10 特定個人情報等複製・運搬記録簿

特定個人情報等複製・運搬記録簿 (年 月～ 月)

| 複製日時 | 複製元 特定個人 情報等 (ファイ ル名・書 類名) | 複製元 (媒体等) / 運搬元所在地 (所在地・フロア 名) | 複製先 (媒体等) / 運搬先所在地 (所在地・フロア 名) | 複製の量 | 複製・運搬の目的 (引き渡し先がある 場合は相手を明記) | 作業者 | 備考 |
|------|---|--|--|------|------------------------------------|-----|----|
| | | | | | | | |
| | | | | | | | |

