1

個人情報保護安全管理措置実施研修

２０２０．０９

（公社）成年後見センター・リーガルサポート
個人情報保護安全管理措置実施委員会

2

今日の内容

1　なぜ、事業者は、個人情報の保護をしないといけないのか？

2　安全管理措置は、具体的にどのように進めていったら良いのか？

3

１　なぜ、事業者は、個人情報の保護をしないといけないのか？

4

◎　「ドラッグストアからのダイレクトメール」のお話

・　以下の話は、外国で実際に行われていたことについて、物語風に脚色をしたものです。

・　個人の名前や、お店の名前などは、全て架空のものです。

5

８月のある日、高校３年生の山田花子さん宛に、ドラッグストアから、以下のようなダイレクトメールが届きました。

山田　花子　様
　この度は御懐妊おめでとうございます。元気な赤ちゃんが楽しみですね！
　当店は、御出産に関する色々な商品を取り揃えています。
　ぜひとも、元気なお子様の出産に備えて、当店の商品を御利用くださいね。
ドラッグストア田中

6

ところが、この葉書をポストで見つけたのが、花子さんのお父さんだったものだから大変なことに！！

花子さんのお父さんは薬屋に怒って行きました。
「うちの花子は、まだ高校生なんだぞ！　嫁入り前の娘に、こんな葉書を送ってくるな！！」

7

薬屋さんは、平謝りです。

「お店の手違いのようです。
誠に申し訳ありません。」

8

ところが、それから数ヶ月して、
お父さんは、花子さんが本当に妊娠
していることを知ることになりました。

花子さんは、子供ができていたことを、家族はもちろん、誰にも言っていなかったのです。

9

（ここで考えてほしいこと）
なぜ、薬屋さんは、お父さんよりも先に花子さんに子供ができたことを知ることができたのでしょうか……？

10

名前	**山田花子**
住所	〒７００－００００ 岡山県岡山市南区……
電話	０９０－０００－０００
家族構成	父(47)、母(45)、兄(25)、猫３匹
趣味	カラオケ
	……

11

	（購入の記録）
……	……
R02.06.29	ヨルダアメ　２点
R02.07.01	無香スキンローション　１点
R02.07.04	カルシウム・サプリ　１点
R02.07.09	バッグ（大きめ）　１点
R02.07.12	ゴミ袋
……	……

12

……	……
R02.07.01	無香スキンローション　１点
R02.07.04	カルシウム・サプリ　１点
R02.07.09	バッグ（大きめ）　１点
……	……

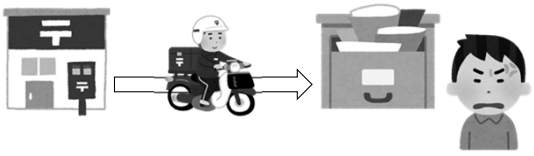
13

R02.07.01	無香スキンローション　１点
R02.07.04	カルシウム・サプリ　１点
R02.07.09	バッグ（大きめ）　１点

お！　花子さんの購入パターンは、当社ＤＢの「妊娠している女性だけが短期間に買う商品パターン」と一致しているぞ！！
花子さんは妊娠しているに違いない！

14

早速、妊婦向けの商品御案内のダイレクトメールを送ろう！
（実際には自動処理）



15

※　今の時代は、お父さんお母さんよりも（そして本人よりも）、事業者の方があなたのことをよく知っている時代なのかも……

16

（このストーリーから分かること）

1　消費者（本人）の側から見れば、事業者の内部で行われている情報の処理は、よく分からない（＝ブラックボックス）

2　データ分析を行っているのは、いわゆるデータ産業と呼ばれる業界だけではないようだ。

17

3　１つ１つを見れば、取るに足らない情報であっても、集めて分析をすると、事業者は、個々人の深いプライバシーの領域へ踏み込むことができるようだ。

※　最近の消費者が「個人情報」に敏感になっている背景の１つにはこの点があるかも……

18

①　個々の情報それ自体が、個人のプライバシーの領域に踏み込むおそれがある場合

（例）特定の病気がある、後見制度を利用している……

②　一見些細な個人に関する情報が集められてデータ化されることにより、個人のプライバシーの領域に踏み込むおそれがある場合

19

要配慮個人情報／センシティブ情報
（伝統的な）プライバシーの権利

① 個々の情報それ自体が、個人のプライバシーの領域に踏み込むおそれがある場合

（例）特定の病気がある、後見制度を利用している……

② 一見些細な個人に関する情報が集められてデータ化されることにより、個人のプライバシーの領域に踏み込むおそれがある場合

個人情報保護法（大部分）

20

（整理）事業者が個人情報を利用する主な場合

1 依頼を受けたサービスを実現するために利用する。

2 連絡の手段に使う（ダイレクトメールや、電話勧誘など）

3 分析や選別を行う（ターゲティング広告、優先サービス提供など）

4 ほかの人事業者に提供する（データの売買。共同で利用して、相互の売り上げ向上につなげる。）

21

5 統計を作るための資料とする。

など

22

（事業者にとって意図しない形で利用等がされる場合）

1 従業員などが、自分の私利私欲のために利用したり、ほかの人へ提供する。
（顧客へのストーカー行為、データの売却など）

2 外部へ（意図しない形で）流出
（メール／FAXの誤送信、屋外で書類紛失、コンピュータウイルス／ハッキングなど）

など

23

※ ちなみにですが、このドラッグストアは、日本の個人情報保護法では、違法なことは何もしていない。

（利用目的）お客様の購入履歴の分析に基づく商品・サービスの御案内、ダイレクトメールの送付……

24

ちょっと待ってください。
消費者の側から見れば、１つ１つの個人情報に敏感になってくるのも分かるのですが、事業者の側からすれば、細かい個人情報にまで過剰に神経を尖らせていると、負担が大きく、現場が疲弊してしまいます。

25

（日本の個人情報保護法の大雑把な建て付けの説明）

（目的）

第１条　この法律は、高度情報通信社会の進展に伴い個人情報の利用が著しく拡大していることに鑑み、個人情報の適正な取扱いに関し、.....個人情報を取り扱う事業者の遵守すべき義務等を定めることにより、個人情報の適正かつ効果的な活用が新たな産業の創出並びに活力ある経済社会及び豊かな国民生活の実現に資するものであることその他の個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とする。

26

◎　全民間事業者を適用の対象（法２条５項）

→　個別の業種毎に規制を行っているわけではない。

→　全ての民間事業者が守ることができるであろう程度の規制しか、定めることができない。

◎　個人情報保護法は、原則として、個人情報の「内容（中身）」には立ち入っていない（法２条１項）。

27

◎　個人情報保護法は、主に「データ化されているかどうか？」によって、規制の内容を分けている。

個人情報			利用目的の特定・取得時の通知・目的外利用の禁止（１５条、16条、１８条） 適正な取得（１７条）
	個人データ		内容の正確性の確保（１９条） 安全管理措置（２０～２２条） 第三者提供の制限（２３条）
		保有個人データ	利用目的の公表・通知、開示、訂正、利用停止等（２７～３０条）

28

ここまでのまとめ

◎　事業者が、個人のプライバシーの領域へ踏み込む恐れがあるパターンは２つ

①　個々の情報それ自体が、個人のプライバシーの領域に踏み込むおそれがある場合

②　一見些細な個人に関する情報が集められてデータ化されることにより、個人のプライバシーの領域に踏み込むおそれがある場合

→　①だけを考えていたのでは、足りない。

※　個人情報保護法は、主に②を規制の対象にしている

29

◎　個人情報保護法（要配慮個人情報を除く。）は、主に「個人データに該当するか否か」で、規制に違いがある。

（参考）GDPR：EU一般データ保護規則

30

（補足）よく聞かれる質問　その１

「リーガルは、成年後見という正しい目的のためにやっているんだ。
正しい目的のためにやっているんだから、個人情報のことくらいで、細かいことを言わないでほしい。」

31

→　消費者（本人）の側から見れば、事業者の内部で行われている情報の処理は、ブラックボックス。

→　このような発言は、少なくとも、従業者などによる悪用の可能性や、情報の漏えいに対する危機意識は、欠けている。

→　個人情報保護法は、全ての民間事業者が守ることができる程度の規制の内容しか定めていない。

↓

「オレ様正義」ではだめ！！

（私は運転技術に自信があるからと、高速道路を160km/h で走るようなもの。）

32

→　○社「提供している商品サービスの内容はＡ級だけれど、個人情報を安心して預けることができるか否かについてはＤ級」

vs

△社「提供している商品・サービスの内容はＢ級だけれど、個人情報を安心して預けることができるか否かについてはＡ級」

33

（補足）よく聞かれる質問　その２

「例えば、情報から、住所・氏名・生年月日・性別などの項目を削除してしまえば、個人情報とか難しいことを考えずに、好きに使って良いよね？」

34

→　以前はそう言われていた時代もあった。

（そうとも言えない例のうちの１つ）

＜Ａ社＞

鈴木太郎	岡山県岡山市	昭和◎年生	りんご	みかん	ぶどう	かぼちゃ	トマト	いちご	にんじん

（加工）

ID09282726	りんご	みかん	ぶどう	かぼちゃ	トマト	いちご	にんじん

35

＜Ａ社＞

ID09282726	りんご	みかん	ぶどう	かぼちゃ	トマト	いちご	にんじん

（提供）

＜Ｂ社＞（前から持っていた情報）

鈴木太郎	岡山県岡山市	昭和◎年生	ゴリラ	りんご	ライオン	トマト	ネコ	馬	にんじん

（Ａ社からもらった情報）

ID09282726	りんご	みかん	ぶどう	かぼちゃ	トマト	いちご	にんじん

36

＜Ｂ社＞（前から持っていた情報）

鈴木太郎	岡山県岡山市	昭和◎年生	ゴリラ	りんご	ライオン	トマト	ネコ	馬	にんじん

（Ａ社からもらった情報）

ID09282726	りんご	みかん	ぶどう	かぼちゃ	トマト	いちご	にんじん

○　Ｂ社内で、ID09282726＝鈴木太郎 であることが分かってしまう。
（識別子以外の情報が、識別子の役割をしてしまう場合がある。）

37

結局、Ｂ社は、Ａ社から、名前入りで「鈴木太郎は、みかん、ぶどう、かぼちゃ、いちご、です。」という個人データを受け取ったのと同じことになります。

＜Ｂ社＞

鈴木太郎	岡山県岡山市	昭和◎年生	ゴリラ	りんご	ライオン	トマト	ネコ	馬	にんじん
				みかん	ぶどう	かぼちゃ		いちご	

38

実際の照合作業は、紙を目で確認するのではなくて、コンピュータの中に取り込んで行われます。

※　「完全一致」ではなくて「曖昧一致」で、個人の特定が行われる場合もあります。

↓

◎　住所・氏名・生年月日・性別などの情報を削除すれば、好きに使って良いといえない事情の１つが、ここにあります。

39

２　安全管理措置は、具体的にどのように進めていったら良いのか？

40

◎　法律の位置付け

（安全管理措置）

第２０条　個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。

→　従業者（２１条）・委託先（２２条）へも監督

※　個人データ

※　必要かつ適切な措置

（注）デジタルに限らず、紙媒体上の情報であっても、検索できるように体系的に構成されていれば、その中の個人情報が「個人データ」に該当する場合があります。（法２条２項２号、令１条）

41

※　必要かつ適切な措置

◎　個人情報の保護に関する法律についてのガイドライン（通則編）

８　（別添）講ずべき安全管理措置の内容

……安全管理措置を講ずるための具体的な手法については、個人データが漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の規模及び性質、個人データの取扱状況（取り扱う個人データの性質及び量を含む。）、個人データを記録した媒体の性質等に起因するリスクに応じて、必要かつ適切な内容とすべきものであるため、……

42

……必ずしも次に掲げる例示の内容の全てを講じなければならないわけではなく、また、適切な手法はこれらの例示の内容に限られない。

……なお、中小規模事業者については……

※　「結局、どこまでのことをやれば良いの？」とよく聞かれます。

43

※　「個人データでない個人情報」については、安全管理措置の法的義務はかかっていないようだが、その取り扱いがルーズな法人で、事業者としての社会的な信用を勝ち取ることができる？

情報の取り扱いについて、事業者としての社会的信用を勝ち取ることができる水準

個人情報保護法が求める水準

44

①　個々の情報それ自体が、個人のプライバシーの領域に踏み込むおそれがある場合

（例）特定の病気がある、後見制度を利用している……

②　一見些細な個人に関する情報が集められてデータ化されることにより、個人のプライバシーの領域に踏み込むおそれがある場合

45

しかし、安全管理措置を慎重に行えば行うほど、作業の手間が増えて、面倒になるんだよなぁ。

例えば名刺１枚のようなものにまで、個人情報だからと神経を尖らせていたのでは、現場は疲弊するばかりです。

46

◎　「必要かつ適切な内容」

※　ガイドラインも、「天衣無縫な対策を実施しなさい」とは言っていない。

↓

◎　リスクに応じた対策を考えていくべき。

47

必要かつ適切な措置

リスクに応じた内容

①　事業の規模及び性質、
②　個人データの取扱状況（取り扱う個人データの性質及び量を含む。）、
③　個人データを記録した媒体の性質
など

（考慮）

（事故が発生した場合に）本人が被る権利利益の侵害の大きさ

48

◎　インシデントや事故が発生するきっかけ

脅威　×　脆弱性　＝　インシデント／事故

好ましくない偶発事件・事故など

安全管理措置上の問題点

49

◎　以下で行うこと

役員の方は、「あなたが」の箇所を、同時に「支部が」にも読み替え。

①　現在、あなたが業務で取り扱っている個人情報の特定

②リスクを特定

③リスクを分析・評価

④リスクへの対応

50

①　現在、あなたが業務で取り扱っている個人情報の特定

◎　個人データ　法律上の義務

◎　個々の情報それ自体が、個人のプライバシーの領域に踏み込むおそれがあるもの

○　その他

支部が扱っている情報には、意外と多くないですか？

51

②　リスクの特定

→　①で特定した個人データ・個人情報について、どういう事故等の発生が考えられるか？

（再掲）事業者にとって意図しない形で利用等がされる場合

1　従業員などが、自分の私利私欲のために利用したり、ほかの人へ提供する。
（顧客へのストーカー行為、データの売却など）

2　外部へ（意図しない形で）流出
（メール／FAXの誤送信、屋外で書類紛失、コピュータウイルス／ハッキングなど）

など

52

（参考）一般的な情報のライフサイクルの例

取得 → 入力 → 加工 → 送信 → 利用 → 保管 → 消去・廃棄

53

③　リスクの分析・評価

• 優先順位の考え方の例

事故発生時に、本人が被る権利利益の侵害の大きさ　×　事故が発生する確率

高	×	高
高	×	低
低	×	高
低	×	低

54

④　リスクへの対応

（比較的容易に実施ができるものの具体例）

（コンピュータ）

・　利用するコンピュータ（本体）を限定する。

・　OS・セキュリティソフトは、常に最新の状態を維持する。

・　事務局員等に、無断でアプリをインストールしないように指導する。

など

55

（アクセス権限の制限など）

・　関係のない人には見ることができないように、ハードディスク上のファイルの保管場所を工夫する。

※　特に、事務局が本会と共通の場合である場合に注意。

・　アカウントは、適切な者に対してのみ与える。

・　複数人でアカウントを共通にしない。

・　ファイル等にパスワードを設定する。

など

56

（メールを利用する場合）

・　新規の送信先には、正しい相手に届いていることが確認できるまで、重要な内容を書き込まない。

・　添付するファイルは暗号化する。

・　メールにファイルを添付せず、アクセス制限のあるクラウド等を利用して受け渡しを行う。

・　メーリングリストの参加者を定期的に確認する。

※　委員等を辞めた者等へも引き続き送信されていないか、確認を行う。

など

57

（紙の書類の保管場所など）

・　事務局の特定のエリア内には、関係のない人が入ってこないように工夫する。

・　関係のない人には見ることができないように、紙の書類の保管場所を工夫する。

・　事情によっては、書棚の施錠等も検討する。

※　特に、事務局が本会と共通の場合である場合に注意。

58

（FAXを利用する場合）

・　FAXのテスト送信を義務づける。

・　ワンタッチボタンへ登録がない先へは、テスト送信を義務づける。

・　情報の内容によっては、別の者がテスト送信の実施を確認しないと、FAXの送信ができないことにする。

など

59

（モバイルパソコンや、USBメモリ、書類などを事務局の外へ持ち出す場合）

・　予め、外へ持ち出す場合のルールを決めておく。

・　モバイルパソコンや、USBメモリの暗号化

・　責任者の承諾がないと、外部に持ち出すことができないことにしておく。

・　記録の作成（万一の際に追跡ができるように。）

など

60

（ディスクや書類を廃棄する場合）

・　定期的に、不要な書類・ファイルをいつまでも保管していないか、確認をする。

・　予め、書類の保存期限を決めておく。
※　間違って廃棄しないという意味でも有効。

・　シュレッダーの活用

・　ディスクなどの廃棄は、信用できる事業者に依頼する。

など

61

（その他全体的なこと）

・　責任者を決める。
　※　実際に個人情報を取り扱う人と、責任者を分ける。

・　適正な取り扱いが行われていることを、責任者が、適宜、点検・確認する体制にする。

・　万一のことが起こった場合の報告・連絡体制や、取り扱いについて疑問が生じた場合の相談先などを、相互に確認しておく。

など

62

＜注意してほしいこと＞

◎　担当者の「効果」への理解がない対策は、組織で定着させようと思っても、定着しません。
　→　指導、教育等の重要性

63

◎　同じ効果が得られるならば、より担当者の負担が少ない実施方法を、色々と工夫してみてください。

（例）FAXのテスト送信は、送付状のフォーマットに確認欄を作って、テスト送信を忘れたまま送信をしないように工夫する。

FAX送付状

（中略）

☑　テスト送信実施済

64

（まとめ）

◎　インシデントや事故が発生するきっかけ

好ましくない偶発事件・事故など

安全管理措置上の問題点

65

◎　安全管理措置のためにやるべきこと

役員の方は、「あなたが」の箇所を、同時に「支部が」にも読み替え。

①　現在、あなたが業務で取り扱っている個人情報の特定

②リスクを特定

③リスクを分析・評価

④リスクへの対応

66

③　リスクの分析・評価

（優先順位の考え方の例）

事故発生時に、本人が被る権利利益の侵害の大きさ　×　事故が発生する確率

高	×	高
高	×	低
低	×	高
低	×	低

67

★　訂正について

動画及び動画で映写したスライドについて、以下のとおり訂正をいたします（配付資料では修正済み。）。

- スライド５枚目
  訂正前「６月のある日」
  訂正後「８月のある日」
- スライド４０枚目
  紙媒体上の情報あっても、一定の場合には個人データに該当することについて、加筆。