2016/11　弁護士 水町 雅子

プライバシー影響評価（PIA）
～個人情報リスク評価+～

1. プライバシー影響評価とは何か

プライバシー影響評価／個人情報リスク評価+とは

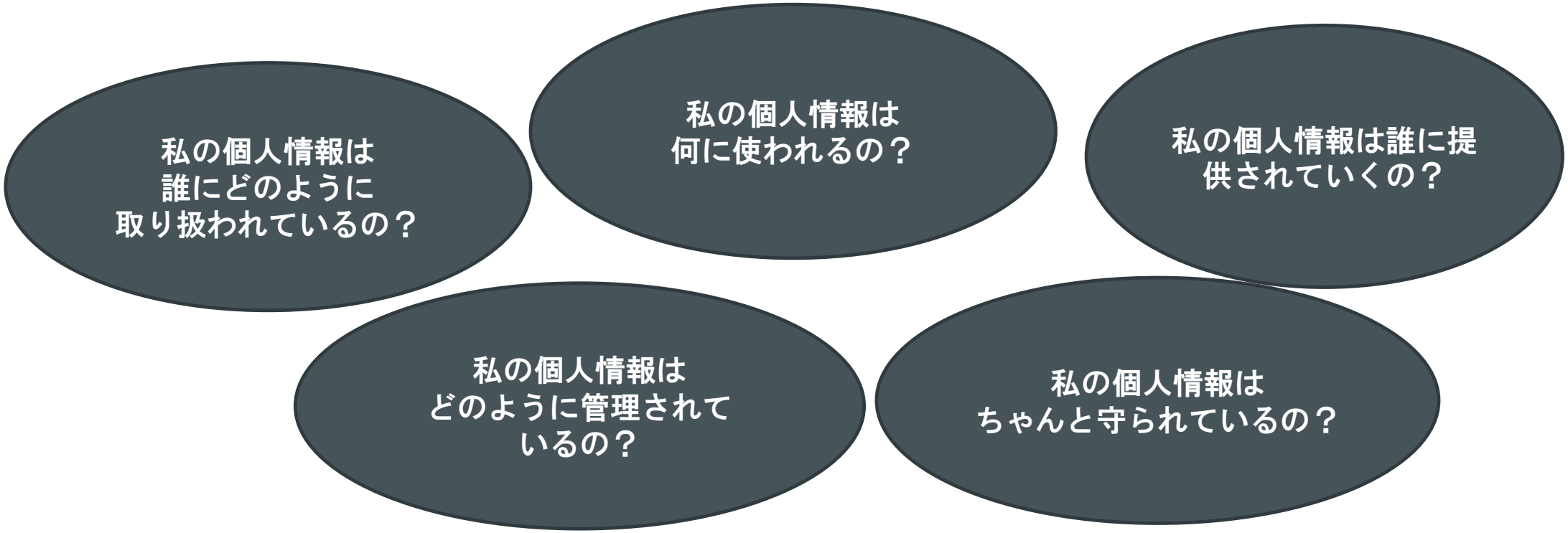
◆ Privacy Impact Assessment （PIA）

- 個人情報を取り扱う制度・事務・ビジネス・ITシステム等を開始する前に、プライバシーに対して与える影響を検討するための仕組み
- 個人情報を取り扱うとプライバシーに対して悪影響が生じるおそれ。その悪影響を緩和・軽減するための方策を検討する
- イギリス、アメリカ、香港、オーストラリア、ニュージーランド、カナダ、韓国その他の国で実施されている
- 行政機関、医療機関、民間企業などさまざまなアクターが実施

プライバシー影響評価の意義（ユーザ・消費者・市民にとって）

◆ 個人から見た意義

- 今まではブラックボックスだった個人情報の取扱いを透明化
- プライバシー・ポリシーのあるべき姿をイメージ



プライバシー影響評価の意義（実施側にとって）

◆ 評価実施側から見た意義

- プライバシー保護を体系的に理解・説明できるようになる
  - ✓ 個人情報といっても、漏えいさえしなければいいというものではない

- 個人情報を取り扱う必要性をユーザ・消費者に理解してもらえる
  - ✓ 「危ない」VS「必要だ」の原理主義的論争に陥らず、具体的に説明できる

- 個人情報を取り扱うに当たって注意すべき点がわかる
  - ✓ 従業員の意識の向上
  - ✓ 研修といった座学だと当事者意識が生まれないことも
  - ✓ 「自分が行っている業務」における注意点を具体的に検討する

- 個人情報を適切に取り扱うことをユーザ・消費者にアピールできる
  - ✓ 取扱いの適正性を具体的にアピール
  - ✓ 「炎上」する前に
  - ✓ 「危ない」VS「必要だ」の原理主義的論争に陥らず、詳細な評価書を基に、問題点を具体的にユーザと討論できる

プライバシー影響評価の意義（実施側にとって）

◆ 評価実施側から見た意義

コミュニケーション手段としての側面も強い	
従業員	個人情報・プライバシーの重要性 業務上の注意点
顧客	信頼の獲得
ITシステムベンダー	個人情報・プライバシーの重要性 要求仕様

プライバシー影響評価でわかること

実施側が宣言すること

- **個人情報**を取り扱う**必要**があるので取り扱います
- 個人情報を**このように**取り扱います
- 個人情報を**適切に取り扱うために各種リスク対策を事前に講じます**

評価書からわかること

- どんなふうに個人情報を取り扱うの？
- どんなリスク対策を講じるの？
- プライバシー保護についてどのように取り組んでいるの？

2.　どのように実施すればよいのか

プライバシー影響評価を実施するには

- **諸外国で行われている**Privacy Impact Assessment （PIA）**を参考にする**
- **日本で行われている特定個人情報保護評価を参考にする**
- **お勧めは、特定個人情報保護評価をカスタマイズする**

特定個人情報保護評価をカスタマイズしよう

考え方

- 特定個人情報保護評価が義務付けられるのは、マイナンバーに関する特定個人情報ファイルを保有する官がメイン
- それ以外は、あくまで任意実施であり、特定個人情報保護評価を参考にするのみ
- 特定個人情報保護評価をベースに適宜カスタマイズできる
- 特定個人情報保護評価の枠組みを使い、ユーザ・消費者にわかりやすいものを実施していくのがお勧め

特定個人情報保護評価の問題点とその解決策

- 特定個人情報保護評価書は難解
  - ✓ そのまま用いなくてもよい。趣旨を用いてベースに使う。
- 字が多い
  - ✓ パワーポイントなどに変更し、図を多用しよう。
- 何が書いてあるかわかりづらい
  - ✓ 「この欄に書くべきこと」をより明確化する
  - ✓ どんなリスクがあってどんな対策をするのかをよりわかりやすく記載する
  - ✓ ユーザ・消費者目線に立って記載する

特定個人情報保護評価の仕組み

評価書案を作る → 一般意見を聴く → 専門家意見を聴く → 確定版評価書を公表

◆ **中心は、評価書**

- 「プライバシーポリシー」「わが社の取り組み」をイメージ

◆ **評価書をブラッシュアップしていく仕組み**

- 一般意見、専門家意見によって得られた意見をもとにブラッシュアップ
- 一般意見を聴く、専門家意見を聴くは必ずしも実施しなくてよい
- もっとも、海外では一般意見を聴くことは重要視されている（消費者団体との意見交換など）。事前に意見を聴かなくても、評価書を公表することで、ユーザ等からの反応が考えられる。その反応・意見によって、評価書をブラッシュアップ。
- 再評価・評価書の修正によって、継続的にブラッシュアップ

3.　情報保護評価書のポイント

評価書に何を書くか、何を評価するか

１　サービスの全体像をわかりやすく平易に説明しよう

- ユーザ・消費者に向けての説明をイメージ
- どのようなサービスなのか、何を行うのか

２　個人情報がどう関係してくるかを説明しよう

- そのサービスで個人情報がなぜ必要なのか
- 個人情報を誰がどのように利用するのか
- 個人情報を外部提供するのか、誰に提供するのか
- 個人情報をいつまで保管するのか、いつどう廃棄するのか
- ユーザ個人にメリットはあるのか

３　個人情報の不正に対する不安を払拭するべく、対策をわかりやすく説明しよう

- 悪用しないのか、ＤＭや勧誘電話は来ないのか、外部売却しないのか、漏えいしないのか、無関係な他人に教えないのか、従業員教育はどうなっているのか　などなど

１．サービスの全体像をわかりやすく平易に説明しよう

- サービス・業務の全体像をわかりやすく平易に説明しよう
  - ✓ 市民・消費者に向けての説明をイメージ
  - ✓ 市民・消費者は、企業内部の者とは違い、どのようなサービスなのか、業務なのかが全く分からない場合も多い。企業内部にとっては当然のことであっても、外部から見たらわからない。
  - ✓ たとえるなら、この業務に新しく加わった従業員（新人・異動者）に説明するように、全体像をわかりやすく説明する。
- さらに、サービス・業務の全体像の中での個人情報の流れを追記しよう
- できれば図にするとよい。難しいようであれば平易な文章で。

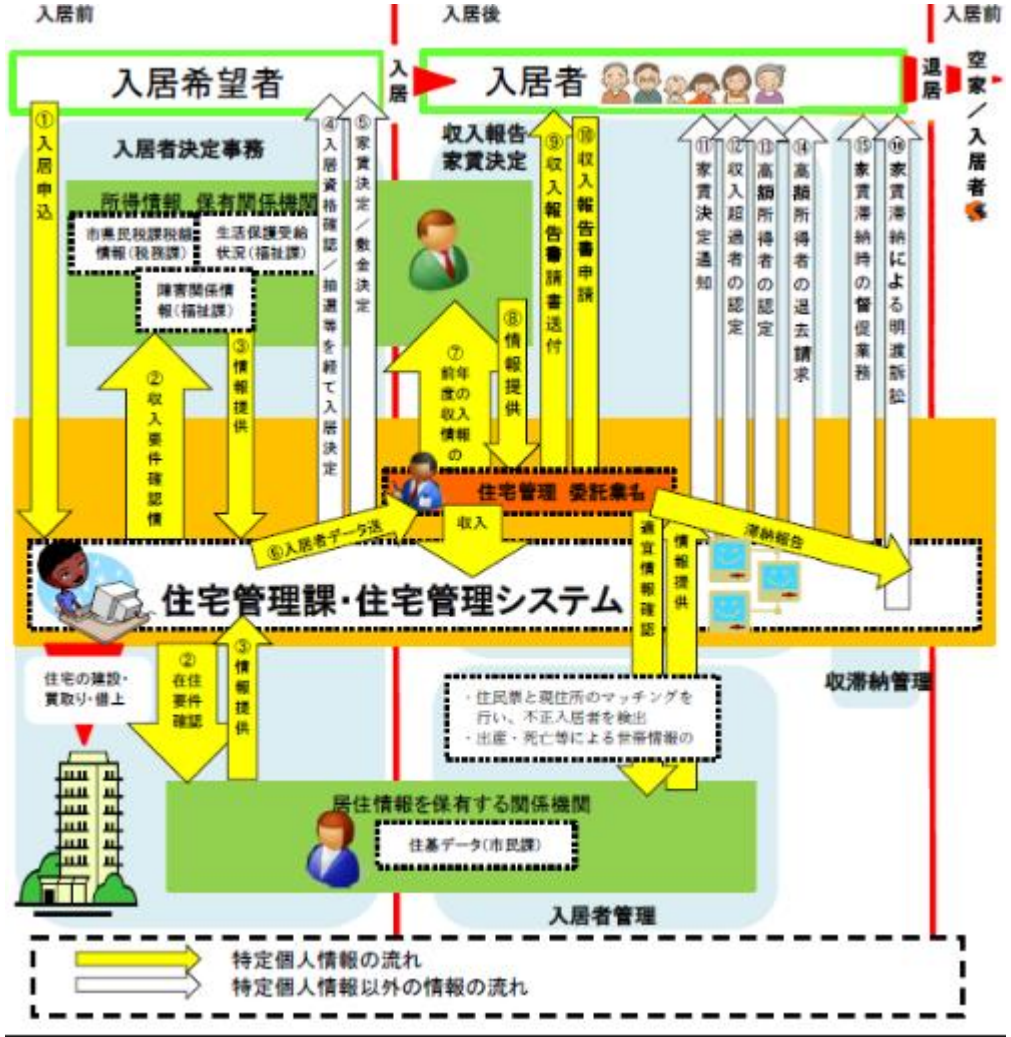
（参考）官の評価書だと・・・重点項目評価書Ⅰ１②・全項目評価書Ⅰ１②別添１に

１．サービスの全体像をわかりやすく平易に説明しよう（例）

- 文章の例（イメージ）
  - 目的：乳幼児医療費助成：経済的負担を心配しなくてもお子さんが病気などを治療できるよう、〇才未満のお子さん*1の医療費等*2のうち保護者等が負担しなければならない分を、市で助成します。
  - 概要：当市では、出生届を受け取ったら、保護者等に申請を促します。保護者等の申請を受け付けたら、助成対象外*1に当たらないか当市で確認し、医療証を発行します。保護者等は病院の窓口等で医療証・健康保険証を提示の上、診療等を受けます。そうすると保険外等の、対象外となる医療費等*2を除き、保護者等は自己負担がなくなります。当市では、病院等から請求を受け、病院等へ対象額を支払います*3。
  - *1～3：例外や、審査・支払機関等の点は、注記するとわかりやすくなる可能性。注記とせず、本文に書いてもよいが、正確に記載しようとして例外の解説が多すぎると、わかりにくくなるので、留意する。

１．どういう業務か説明しよう（例）

- 絵の例（イメージ）



２．個人情報がどう関係してくるかを説明しよう

- サービスや業務の中で個人情報がどうかかわるのか、平易に説明しよう
  - ユーザ・消費者からすれば、誰の個人情報が何のために誰にどのように使われるかわからない。
  - 企業内部にとっては当然のことであっても、外部から見たらわからない。
- サービスや業務の中で個人情報がどう取り扱うのか、平易に説明しよう
  - 不透明だと不安が生じる。具体的に説明することで、納得が得られやすい。
  - 個人情報を誰が何のためにどのように利用するのか
  - 個人情報を外部提供するのか、誰に何のために提供するのか
  - 個人情報をいつまで保管するのか、いつどう廃棄するのか
- ユーザ個人にメリットはあるのか
  - 自分の個人情報を企業の利益のためだけに利用されているという思いも
  - ユーザ個人にどのようなメリットがあるのか、個人情報の利用だけではなく、サービス全体のメリットも含め、説明できるとよい

（参考）官の評価書だと・・・重点項目評価書Ⅱ２③④３⑤ ・全項目評価書Ⅱ２③④３⑧に記載

２．個人情報がどう関係してくるかを説明しよう（例）

- 例（イメージ）
  - 誰の個人情報：当市在住の〇才未満のお子さん、保護者、過去の対象者*1
    - *1　〇才以上になったお子さんと保護者の個人情報についても、過去△年分の情報を保存しています。
  - どんな個人情報：
    - ＩＤ、氏名・住所・性別・生年月日、連絡先、その他住民票関係情報、医療保険関係情報、児童福祉・子育て関係情報・生活保護・社会福祉関係情報、障害者福祉関係情報
  - どう使用するのか：
    - 医療証関係
      - 出生届を受け取ったら、保護者等の住所宛に乳幼児医療費助成について申請を促す連絡をする
      - 申請を受け付けたら、助成対象外*1に当たらないか〇、△、□情報を元に当市で確認し、医療証を発行する
      - 〇〇の時に、医療証を再発行する
      - 〇〇の時に、医療証を更新する
      - 転出届を受け取ったら、・・・

2．個人情報がどう関係してくるかを説明しよう（ポイント）

- 企業の外のユーザがわかるように
- 具体的に説明する
  - 取得：　どこからいつどのような個人情報を取得するのか
  - 利用：　いつ誰が何のためにどのように利用するのか
  - 委託：　委託先に取り扱わさせるのか
  - 提供：　いつ誰に何のために提供するのか
  - 保管：　どのようにいつまで保管するのか
  - 消去：　いつどのように消去するのか
- 個人情報を取り扱う必要性、合理性を納得してもらえるように説明する
- 不合理なこと、あやしいことはやっていないということの説明にもなる
- ユーザの不信感が解消されるように

３．個人情報の不正対策をわかりやすく説明しよう

１．想定されるリスクを挙げよう

- ユーザの不安を中心に考えるとよい
- 個人情報が悪用されないか、ＤＭや勧誘電話が来ないか、外部売却されないのか、漏えいされないのか、無関係な他人に教えないか、従業員教育はきちんとなされているか　などなど
- 個人情報の不正リスク、プライバシーリスクを網羅的に考えるとさらに良い　（追って説明）

２．今行われているリスク対策を確認しよう

- 今行われているリスク対策はどのようなものか
- 外部の人が見て、リスクが防止できると納得してもらえるレベルの対策になっているか考えよう

３．リスク対策を改善しよう

- より納得してもらえるリスク対策に、不正を防止できるリスク対策へとレベルアップしていこう

４．リスク対策を説明し、ユーザの納得を得よう

３．個人情報の不正対策をわかりやすく説明しよう

実はそこまで技術的、難しいものではなく、常識に沿って考えるべきもの

■ 想定されるリスク

- ✓ 例）個人情報が悪用されないか、ＤＭや勧誘電話が来ないか、外部売却されないのか、漏えいされないのか、無関係な他人に教えないか、従業員教育はきちんとなされているか　などなど
- ✓ ユーザは何が不安なのか、自分だったら何を不安に思うか
- ✓ 代表的な不安、社会的マイノリティの不安
- ✓ 漠然とした不安をブレイクダウンして考える

■ リスク対策

- ✓ 例）ダブルチェック、アクセス制御、施錠、外部提供制限　などなど
- ✓ 対策自体をプライバシー影響評価で新しく編み出すわけではない
- ✓ 対策は目新しくなくてもよい、きわめて高度な対策が要求されるわけではない
- ✓ リスクを防止・軽減できると合理的に説明できるか、ユーザの不安が解消されるか

3．個人情報の不正対策をわかりやすく説明しよう

■ 入手の際に想定されるリスクの例

- 過剰入手（目的外）
  - どんなリスクか：　不要な個人情報まで取得してしまう
  - 対策：　取得事項を必要な個人情報に限定するなど
（個人情報を取得する画面・システムの制御、ダブルチェック、様式作成）
- だまし討ち入手（不適切な方法）
  - どんなリスクか：　個人情報が取得されているとユーザから見てわからないようなだまし討ちのような方法で取得してしまう、不適切な方法で取得してしまう
  - 対策：　個人情報を取得する際にその旨を明示、利用目的・利用方法なども合わせて明示するなど
- 安全でない入手方法（漏えい・紛失）
  - どんなリスクか：　入手時に漏えい、紛失等してしまう
  - 対策：　専用線、暗号化、パスワード、封緘、簡易書留
- 取違え（不正確）
  - どんなリスクか：　別人、別情報と取り違えてしまう、内容が間違っている
  - 対策：　本人確認、正確性確保

３．個人情報の不正対策をわかりやすく説明しよう

■ 利用の際に想定されるリスクの例

- 過剰集約（目的を超えた紐づけ）
  - どんなリスクか：　サービスや業務に必要のない個人情報をどんどん集約されてしまう
    （プロファイリング、個人像が勝手に作り上げられる）
  - 対策：　個人情報の紐づけ・集約を限定するなど
    （個人情報の管理をサービスごとに分ける、複数サービスで集約する範囲を限定する）
- 無関係な者による利用（権限のない者による使用）
  - どんなリスクか：　担当者以外の者（元担当者、元従業員、たまたま訪問した人、サイバー攻撃者など）が勝手に利用
  - 対策：　アクセス権限の管理徹底、セキュリティ対策の充実など
- 興味本位の利用（事務外使用）
  - どんなリスクか：　業務担当者が業務のためにではなく興味本位など個人的な理由で勝手に利用
  - 対策：　研修の充実など
- 不正コピー、不正持ち出し
  - どんなリスクか：　個人情報を不正にコピーされたり、外部に持ち出されてしまう
  - 対策：　ルールの明確化、媒体吐出制限など

３．個人情報の不正対策をわかりやすく説明しよう

■ 提供の際に想定されるリスクの例

- 無関係な者への提供・売却（不正）
  - どんなリスクか：　サービスや業務上必要のない相手に他人の個人情報を提供してしまう
  - 対策：　外部提供ルールの明確化、ログの取得・分析・監視、従業員監督・教育
- 不適切な提供方法
  - どんなリスクか：　提供時に漏えい、紛失等してしまう
  - 対策：　専用線、暗号化、パスワード、封緘、簡易書留
- 間違い
  - どんなリスクか：　提供先や提供する個人情報を間違えてしまう
  - 対策：　ダブルチェック、システム化など

３．個人情報の不正対策をわかりやすく説明しよう

■ 委託の際に想定されるリスクの例

- 委託先の杜撰
  - どんなリスクか：　委託先が杜撰に個人情報を取り扱ってしまう
  - 対策：　情報保護管理体制の確認、アクセス者の限定、委託契約、提供ルール、消去ルール
基本的には自社と同様の監督が重要。選定・委託契約・報告徴収。
- 再委託先以降の杜撰
  - どんなリスクか：　再委託先以降が杜撰に個人情報を取り扱ってしまう
  - 対策：　再委託以降の許諾制など
- 不透明
  - どんなリスクか：　ユーザそして委託元にとって個人情報の取扱い実態がわかりづらい
  - 対策：　見える化、報告義務など

３．個人情報の不正対策をわかりやすく説明しよう

■ 保管・消去の際に想定されるリスクの例

- 漏えい等
  - どんなリスクか：　個人情報が漏えいしたり無くなったり欠けたり改ざんされたりしてしまう
  - 対策：　安全管理措置（組織的、人的、物理的、技術的）
- 古くて不正確
  - どんなリスクか：　個人情報が古くなり不正確なまま保有され続けてしまう
  - 対策：　現況確認
  - ※　古いまま保管しつづける必要がある場合等はあてはまらないリスク（例、過去の確定申告書）
- 未消去・未廃棄
  - どんなリスクか：　個人情報が不必要なまま消去されず保管され続けてしまう、不十分な廃棄をされてしまう
  - 対策：　保存期間の設定、確実な廃棄など

評価書様式ほか

- **個人情報保護委員会Webサイト**
  - **評価書記載例**
  - http://www.ppc.go.jp/files/pdf/12zenkoumokuyouryo.pdf
  - **重点項目評価書様式（記載要領付）**
  - http://www.ppc.go.jp/files/pdf/20160101_youshiki3kisaiyouryou.pdf
  - **全項目評価書様式（記載要領付）**
  - http://www.ppc.go.jp/files/pdf/20160101_youshiki4kisaiyouryou.pdf
  - **特定個人情報保護評価の概要**
  - http://www.ppc.go.jp/files/pdf/20160101hyoukasyousai.pdf
  - **既に公表済の特定個人情報保護評価書の検索サイト**
  - **http://www.ppc.go.jp/mynumber/**

参考

- 『特定個人情報保護評価のための番号法解説～プライバシー影響評価（PIA)のすべて』
  - 第一法規、２０１５年１１月刊行
  - http://goo.gl/yoWZ1U

- 作った人が明かすマイナンバー　プライバシー保護の勘所（Itpro)
  - 実はカンタン、「プライバシー影響評価」
  - http://itpro.nikkeibp.co.jp/atcl/column/15/052100128/052100005/?ST=security&P=1
  - 脱・行政文書、間違いのコピペ丸投げ
  - http://itpro.nikkeibp.co.jp/atcl/column/15/052100128/080600008/
  - どうなっている？あなたの街のマイナンバー
  - http://itpro.nikkeibp.co.jp/atcl/column/15/052100128/080600006/?ST=management&P=1

プライバシー影響評価について、お気軽にお問合せください。

プライバシー影響評価が民間部門でスムーズに実施されるよう、お手伝いいたします。
実施のご支援、第三者点検、勉強会開催その他お問合せを歓迎しています。

その他、マイナンバー、個人情報、医療データ、ITシステム関連契約、ITシステム開発紛争、国との交渉、制度案・法律案作成、講演などを行っております。
http://www.miyauchi-law.com/mynumber.html
http://www.miyauchi-law.com/gyoumu.html

宮内・水町IT法律事務所　　弁護士　水町　雅子
電話　→　03-5761-4600
メール→　osg@miyauchi-law.com