NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

個人情報保護法対策セキュリティ実践マニュアル 2005版

平成 17年 6月 13日
NPO JNSA
個人情報保護法 ワーキンググループ リーダー
㈱大塚商会 佐藤 憲一

NPO JNSA

特定非営利活動法人 日本ネットワークセキュリティ協会

ネットワークセキュリティシステムに携わるベンダーが結集して、2001年5月にNPOとして設立。以来、ネットワーク社会の情報セキュリティレベルの維持・向上および日本における情報セキュリティ意識の啓発に努めるとともに、最新の情報セキュリティ技術と情報セキュリティへの脅威に関する情報提供・調査などを行っている。
会長・石田晴久。会員社数は195社（2005年2月5日現在）。
URL http://www.jnsa.org/

個人情報保護法ワーキンググループ

<グループリーダー>
株式会社大塚商会佐藤 憲一
<チームリーダー>
株式会社インフォセック佐々木 健美
株式会社大塚商会 小林 健
住商エレクトロニクス株式会社 二木 真明
セコム株式会社 遠藤 孝行
中央青山監査法人 松ヶ谷 正志
日本アイ・ビー・エム システムズ・エンジニアリング株式会社 河岡 忠広
日本アイ・ビー・エム システムズ・エンジニアリング株式会社 久波 健二
東日本電信電話株式会社 堀内弘司
富士通関西中部ネットテック株式会社 川本 博
<メンバー>
株式会社アルテミス 森谷 巧
株式会社インフォセック 山崎 貴子
株式会社エス・エス・アイ・ジェイ 刑部 泰正
エヌ・ティ・ティ・コムウェア株式会社 丸尾 浩隆
株式会社ジェイエムシー 米山慶一
新日鉄ソリューションズ株式会社 松島 正明
住商エレクトロニクス株式会社 嶋影 能子
セコム株式会社 渡並 智
セコムトラストネット株式会社 加藤 玄
中央青山監査法人 梅澤泉
中央青山監査法人 木村 章展
東京情報コンサルティング株式会社 松浦 正東
日本オラクル株式会社 北野 晴人
株式会社ネットマークス 井上 大輔
株式会社ヒューコム 横山 康生
富士ゼロックス情報システム株式会社 藤井裕一
富士通サポートアンドサービス株式会社 末延 忠昭
扶桑電通株式会社 酒井 茂弘
菱洋エレクトロ株式会社 平野 元洋
<法務監修>
霞が関法律会計事務所 弁護士 北沢義博

個人情報保護法対策 セキュリティ実践マニュアル 2005版

JNSA

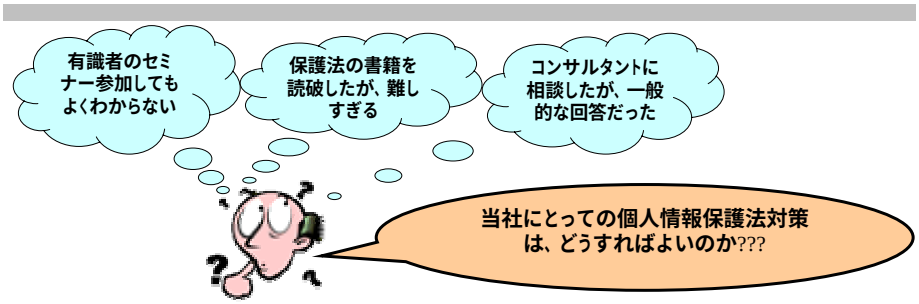
著者：NPO JNSA 個人情報保護ガイドライン ワーキンググループ
発売：インプレスコミュニケーションズ
定価：¥3,500(税別)
発売日：2005年 3月 8日

第1章 個人情報保護法の基礎知識
第2章 全社体制
第3～9章 総務部、お客様相談室、マーケティング部・営業部、サポート部、工場、情報システム室、インターネット通販部
第10章 個人情報保護法と省庁動向
第11章 関係法令と制度
付 録 ・個人情報保護チェックリスト
・規程・基準・契約書等サンプル
・個人情報保護法・政令案全文

インプレスダイレクト販売サイト
http://direct.ips.co.jp/book/kojin_sec/

発刊の背景と目的

JNSA



企業の視点で実務に則した対策

企業の各組織(経営者、情報システム部門、総務部門、営業部門、サポート部門等)の担当者の視点で、その組織体が個人情報保護法を適切に対処するための必要事項を整理し、かつその構築と運用方法を具体的に解説し、結果として、企業全体で個人情報保護法を遵守するしくみ作りを解説する

本書の特徴

5W1Hによる解決

1. モデル企業を組織体毎に解説 → Where (どの部署が)、Who(責任者の明確化)
   従業員数300名程度の製造業をモデル企業とし、かつ組織体は、全社対応、営業部門、サポート部門、インターネット通販、工場部門、総務部、お客様相談室、情報システム室といたしました。

2. 対策方法は、経産省 個人情報保護法ガイドラインに則して整理 What(対策項目の明確化)
   各部署は、部門概要、個人情報の入手管理、組織的安全管理、人的安全管理、物理的安全管理、技術的安全管理、委託先の管理に大別し、それぞれの対策方法を列記いたしました。

3. 整理項目の内容は、JIS(日本規格協会)にできるだけ準拠 → How(どの基準で実施)
   各部署の具体的対策方法は、JIS Q 15001(個人情報保護に関するコンプライアンス・プログラムの要求事項)、JIS X 5080(情報セキュリティマネジメントの実践のための規範)に基づき、具体例を記載いたしました。将来、「プライバシーマーク制度」や「ISMS適合性評価制度」にも活用が可能。

4. 企業で必要な実務的な規程・基準を掲載 → When(なるべく早く)
   即実務で活用できる個人情報に関する宣言、規程、基準、手順書の文書例を掲載しました。

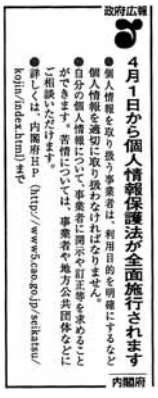
5. 個人情報保護法を取り巻く法令・規範・制度を整理 → Why(対策すべき理由)
   個人情報保護法に関係する他の法令・規範・制度を解説しました。

6. 個人情報保護法の対応チェック表を掲載

NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

セッション1

個人情報保護法の復習


政府広報

4月1日から個人情報保護法が全面施行されます

●個人情報を取り扱う事業者は、利用目的を明確にするなど個人情報を適切に取り扱わなければなりません。

●自分の個人情報について、事業者に開示や訂正等を求めることができます。苦情については、事業者や地方公共団体などにご相談いただけます。

●詳しくは、内閣府HP（http://www5.cao.go.jp/seikatsu/kojin/index.html）まで

内閣府

個人情報保護に関する基本方針

(1) 個人情報取扱事業者に関する事項 平成16年4月2日 閣議決定

① 事業者が行う措置の対外的明確化

事業者の個人情報保護に関する考え方や方針に関する宣言（いわゆる、プライバシーポリシー、プライバシーステートメント等）の策定・公表により、個人情報を目的外に利用しないことや苦情処理に適切に取り組むこと等を宣言するとともに、事業者が関係法令等を遵守し、利用目的の通知・公表、開示等の個人情報の取扱いに関する諸手続について、あらかじめ、対外的に分かりやすく説明することが、事業活動に対する社会の信頼を確保するために重要である。また、事業者において、個人情報の漏えい等の事案が発生した場合は、二次被害の防止、類似事案の発生回避等の観点から、可能な限り事実関係等を公表することが重要である。

② 責任体制の確保

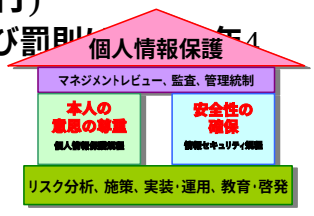
事業運営において個人情報の保護を適切に位置づける観点から、外部からの不正アクセスの防御対策のほか、個人情報保護管理者の設置、内部関係者のアクセス管理や持ち出し防止策等、個人情報の安全管理について、事業者の内部における責任体制を確保するための仕組みを整備することが重要である。また、個人情報の取扱いを外部に委託することとなる際には、委託契約の中で、個人情報の流出防止をはじめとする保護のための措置が委託先において確保されるよう、委託元と委託先のそれぞれの責任等を明確に定めることにより、再委託される場合も含めて実効的な監督体制を確保することが重要である。

③ 従業者の啓発

事業者において、個人情報の漏えい等の防止等、その取り扱う個人情報の適切な保護が確保されるためには、教育研修の実施等を通じて、個人情報を実際に業務で取り扱うこととなる従業者の啓発を図ることにより、従業者の個人情報保護意識を徹底することが重要である。

個人情報保護法

- 個人情報の保護に関する法律
  (平成15年5月30日公布即日施行)
  - 企業に影響する第15条以降および罰則は、2005年4月1日に施行
  - 「本人の意思の尊重」
    - 個人情報は本人のもの
    - 本人が同意したとおりに個人情報を取り扱う
  - 「安全性の確保」
    - 個人情報の流出・漏洩を防ぐ(ISMSの構築)
      : Information Security Management System



★情報セキュリティだけでは個人情報保護法対策にならない！

企業に対する要求

JNSA

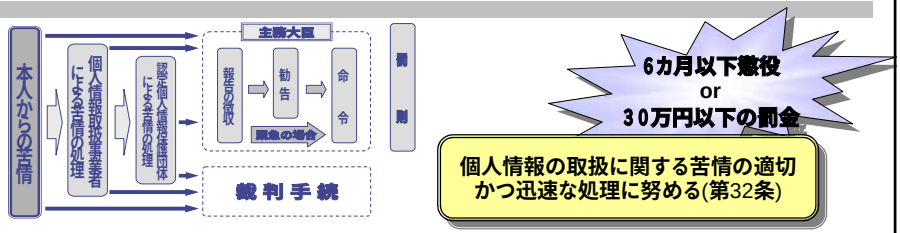
- 義務規定
  - 個人情報保護法第15条（利用目的の特定）」
  - 第16条（利用目的による制限）」 →同意！ ㊫
  - 第17条（適正な取得）」
  - 第18条（取得に際しての利用目的の通知等）」
  - 第20条（安全管理措置）」
  - 第21条（従業員の監督）」
  - 第22条（委託先の監督）」 ㊨
  - 第23条（第三者提供の制限）」 →同意！
  - 第24条（保有個人データに関する事項の公表等）」
  - 第25条（開示）」
  - 第26条（訂正等）」 ㊫
  - 第27条（利用停止等）」
- 努力義務規定
  - 第19条（データ内容の正確性の確保）」
  - 第28条（理由の説明）」 ㊫
  - 第31条（企業による苦情の処理）」

㊫＝「本人の権利の尊重」 ㊨＝「安全性の確保」

 Page 9

個人情報取扱事業者の義務(罰則)

JNSA



勧　告

☆ 個人情報の取得に際して**利用目的を通知又は公表**しなければならない（第18条）
☆ **利用目的等を本人の知り得る状態**に置かなければならない（第24条）
☆ 本人の求めに応じて保有個人データを**開示**しなければならない（第25条）
☆ 本人の求めに応じて**訂正**等を行わなければならない（第26条）
☆ 本人の同意なき目的外利用等は、本人の求めに応じて利用**停止**等を行わなければならない（第27条）

命令／緊急命令

★同意なく利用目的の達成に必要な**範囲を超えて**取り扱ってはならない（第16条）
★ 偽りその他**不正の手段により取得**してはならない（第17条）
★ **安全管理**のために必要な措置を講じなければならない（第20条）
★ **従業者**に対する必要な監督を行わなければならない（第21条）
★ **委託先**に対する必要な監督を行わなければならない（第22条）
★ 本人の同意なく個人データを**第三者に提供**してはならない（第23条）

個人情報取扱事業者の義務(罰則)

義務規定＼罰則規定	32条	33条	34条		
			1項	2項	3項
	報告の徴収	助言	勧告	命令(勧告不服従)	命令(緊急時)
15条(利用目的の特定)	○	○	ー	ー	ー
16条(利用目的による制限)	○	○	○	○	○
17条(適正な取得)	○	○	○	○	○
18条(取得に際しての利用目的の通知等)	○	○	○	○	ー
19条(データ内容の正確性の確保)	○	○	ー	ー	ー
20条(安全管理措置)	○	○	○	○	○
21条(従業員の監督)	○	○	○	○	○
22条(委託先の監督)	○	○	○	○	○
23条(三者提供の制限)	○	○	○	○	①
24条(保有個人データに関する事項の公表等)	○	○	○	○	ー
25条(開示)	○	○	○	○	ー
26条(訂正等)	○	○	○	○	ー
27条(利用停止等)	○	○	○	○	ー
28条(理由の説明)	○	○	ー	ー	ー
29条(開示等の求めに応じる手続)	○	○	ー	ー	ー
30条(手数料)	○	○	②	②	ー
31条(個人情報取扱事業者による苦情の処理	○	○	ー	ー	ー

企業の措置内容

(1) 個人情報保護に関する方針を分かりやすい文書(プライバシーポリシー)としてウェブ等で公開する(政府の個人情報保護基本方針6項)。
(2) 個人情報保護体制を決める(同6項)。
(3) 誰が何のためにどのように個人情報を使うか(利用目的)を決めて文書にまとめ(保護法15条)、本人に知らせて(同18条)、利用目的とおりに使用する。利用目的外利用は本人の事前承認を得る(同16条)。
(4) 適正に収集、取得する(同17条)。
(5) 安全に取り扱う(同20条)。
(6) 従業員を監督する(同21条)。
(7) 業務委託先を監督する(同22条)。
(8) 第三者に提供する場合は本人の事前承認を得る(同23条)。
(9) どのような個人情報を持っているかを公表し(同24条)、本人からの要求に応じて個人情報の内容について開示(同25条)、訂正・削除(同26条)、利用停止(同27条)の対処をする。
(10) 本人からの苦情の対応に必要な体制を整備し、対処する(同31条)。

個人情報保護法対策　11ヶ条

JNSA

① 事業者の代表者は、個人情報保護方針(プライバシーポリシー)を定めて公表する (経営者)

② 事業者の代表者は、個人情報保護方針を実現する運営体制や組織を確立する(経営者)

③ 個人情報保護方針に沿って個人情報保護に関する社内規程類を策定し、また、現状の社内規程類を見直し、制改廃する (経営者、推進事務局)

④ 教育・啓発によって、個人情報保護に関する社内規程類を従業員に周知する(総務・人事)

⑤ 個人情報を取り扱う部門と業務手順を明確にし、適切な管理運用手順を確立する(各部門)

⑥ 個人情報保護の内容を含む業務運用手順書および管理運用に必要な書式・様式を作成し、関係者に周知する(各部門)

⑦ 個人情報の取得、利用、保管、廃棄のライフサイクルを、適切な利用目的に基づくものにする (各部門)

⑧ 従業員、委託先、提供先との契約書、誓約書、覚書等の書類を個人情報保護の観点から見直し、必要に応じてあらためて取り交わす(該当部門)

⑨ 本人からの問合せ、相談、苦情を受け付ける窓口を設置・公表し、対応手順を定め、対応要員および従業員に周知し、訓練する(経営者、推進事務局)

⑩ 個人情報に関する事件・事故が発生したとき、会社がすみやかに対応できるように対応手順を定め、従業員に周知し、訓練する(経営者、推進事務局)

⑪ 従業員が個人情報保護の大切さを認識し、社内規程類を遵守するように監督する。(各部門)

JNSA

NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

セッション2

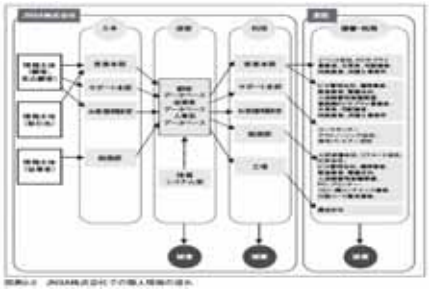
部門ごとにおける個人情報保護法対策

全社体制

JNSA

会社概要
〔会社名〕 JNSA株式会社
（東証・大証 2部上場）
〔社員数〕 300名
〔業　種〕 製造販売業

個人情報の存在



全社体制

JNSA

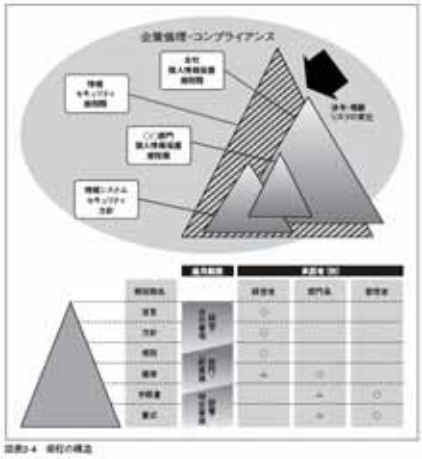
個人情報管理委員会の設置

① 個人情報の適切な取扱いのための基盤整備
- 個人情報（個人データ含む）の取得から利用、加工、破棄までの過程の管理方法を全件調査する。
- 適切な管理方法およびシステム開発計画を明確にする。
- 個人情報保護方針から各規程、基準類の策定を行う。また、部門特有の基準、手順書、マニュアルの作成を指示するとともに、承認を行う。
- 従業員の居住する施設、個人情報の保管場所、サーバの設置場所を調査する
- 従業員に対する誓約書、教育、啓蒙活動を立案する。
- 委託先の選定、契約書、監理方法を立案する
- 規程、規準を満たすための安全な施設、システム開発計画、概算費用を立案する

② 個人情報の維持管理
- 各部門、部署が規程、基準に遵守しているかの内部監査計画、実施計画を立案する
- お客様相談室、危機管理体制とのスムースな連携強化を図る
- 定期的に個人情報の取得、管理、運用状況を把握し、早期問題発見と解決を図る

全社体制

規程類の整備



総務部（総務課・人事課）

＜ 大前提 ＞
従業員個人情報も外部者の個人情報と同様に適正に取り扱うこと

1．人事課 ： 従業者個人情報の取り扱いに関する会社方針策定・従業者に対する説明

(1) 従業者個人情報取扱に関する留意点

① 従業者情報の定義を明確にする。
⇒「雇用管理に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針」（平成16年厚生労働省告示 第259号）に従う。役職員及び採用応募者・退職者を含む

② 従業者の個人情報には、病歴・収入・家族関係といった特殊性を含むことに留意する。
⇒管理責任者の明確化及び担当者の限定、利用・保管場所の安全管理措置、外部委託先の監理措置

③ 従業者個人情報に関する規程を別途策定して、全社に周知する
⇒更に安全管理措置特則等を策定して、機微度のﾚﾍﾞﾙに応じたアクセス権設定や利用・移送・廃棄等の基準を示すことも有効

(2) 通知・公表すべき事項 ：イントラネット上に掲載するなどの措置をとる

① 利用目的 ⇒ 全利用目的を列記する

② 第三者提供・共同利用に関して ：
⇒第三者提供先、共同利用先との合意に基づいて、保護法要件の項目を記載する。
（ただし、第三者提供に関しては、入社時に誓約書と同時に同意書を取得するなど、極力同意を取得する方法を検討する）

③ 開示等請求先 ⇒ 従業者向けの窓口を設置して公表する。また、開示基準を設け、非開示項目については理由を明確にし、必要に応じて労働組合と協議する。

総務部（総務課・人事課）

JNSA

＜ 大前提 ＞
従業員個人情報も外部者の個人情報と同様に適正に取り扱うこと

（3） 人的安全管理措置の主管区として講ずべき事項
① 雇用および契約時の秘密保持契約の締結
② 従業者の周知、教育、訓練の実施 ⇒保護法基本方針でも明記されている。（重要）

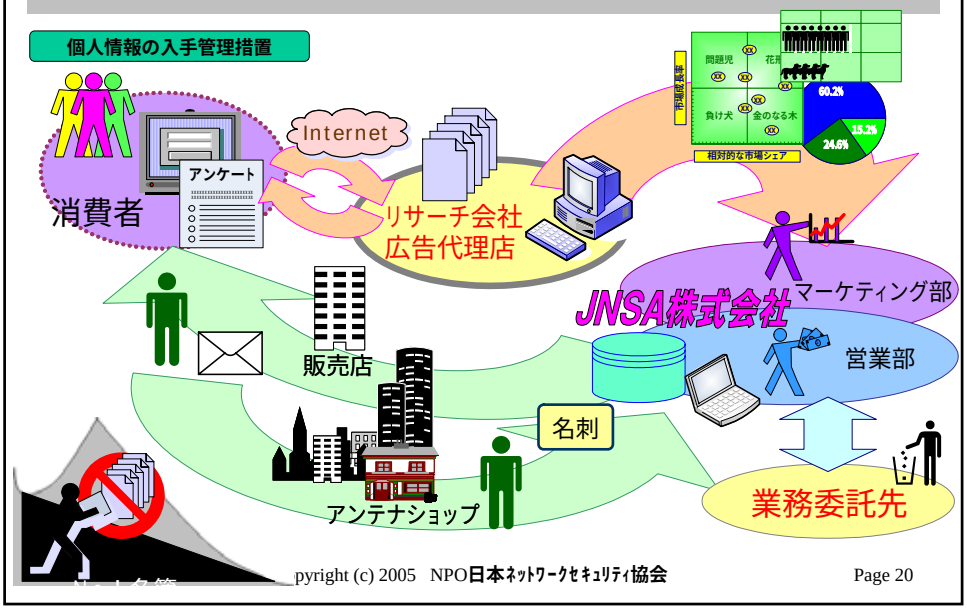
（4） 第三者提供に関する留意点
① 漏洩・盗用禁止、再提供に関する了承、保管期間等、利用目的達成後のﾃﾞｰﾀ返却・破棄・削除、複写・複製禁止、など（前述の厚生労働省ガイドライン参照）

2．総務課 ： 物理的対策の全社方針策定と委託先管理体制整備
（1） 物理的安全管理措置
① 入退管理の実施 ⇒ 休祭日の入退管理手順も含む
② 盗難対策 ⇒ キャビネット・机の施錠、機微情報の閲覧記録
③ 機器・装置等の物理的な保護 ⇒ モバイル機器、可搬電子媒体の管理規程策定

（2） 委託先の監理
① 委託先の把握 ⇒ 全委託先のリストアップ（清掃業者、廃棄業者を忘れずに）
② 委託契約書雛形の作成 ⇒ 委託契約の更改・覚書締結

マーケティング部門・営業部門

JNSA



マーケティング部門・営業部門

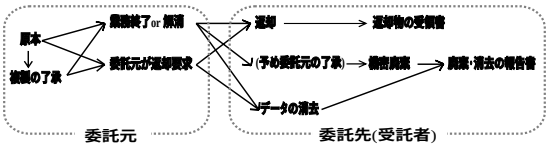
JNSA

マーケティング・営業部門の管理措置

[収集]
- 利用目的・問合せ方法などの明示。
- 業務に不要な個人情報は収集しない。
- 提供の同意を得ていない名簿など取得しない。

[利用・保管]
- 安全管理、機密性確保、委託先の監督。
- 不要な利用はしない。
- 事故・苦情対応。
- ルールの明文化と周知・効果測定。
- 措置の見直しと改善。

[廃棄]
- 保有期間・保管期限に基づき、機密性を保って廃棄。
- 委託先等から回収、または廃棄証明などを得る。



当社のウェブページをご覧いただき、ありがとうございます。
ご記入いただいた個人情報は、より良い製品の開発、お客様へのサービスの向上、および関連する情報をご案内するために利用いたします。
当サイトはデータセンターにシステムの管理を委託しています。また、郵送または宅配便を送付する際に運送会社に業務委託しています。
当社は、お客様にあらかじめご同意を得ずに、お客様の個人情報を提供いたしません。

ご記入に際して、当社ホームページに記載している当社のプライバシーポリシー(注:リンクを貼る)をあらかじめご確認ください。
このページは、ご記入いただいた個人情報を保護するために、機密性のあるSSL暗号化通信に対応しています。お客様がSSLをご利用にならない場合、ご記入いただいた個人情報などが通信過程で機密性を確保できないおそれのあることをご了承ください。

ご登録いただいたお客様の情報について開示、訂正、削除、利用停止の要請をされる場合、次のメールアドレスにお問合せください。
privacy@xxxxx.co.jp
この要請に対応する際の本人確認のため、お客様のメールアドレスをご記入いただく必要があります。メールアドレスをご記入いただかない場合、お客様の要請に対応できないことがあります。

以上の内容にご同意いただいたうえでご記入内容を登録してください。

同意して登録する　同意しない　記入内容をクリアする

サポート部門

JNSA

個人情報の入手管理措置

① 利用目的の特定

「ご購入いただいた製品に関する保守サービスの提供 およびサポート情報の発信を行うため」

② 入手する情報の限定

利用目的を遂行するのに必要なものに限定

② 書面(お客様登録はがき等)での入手

- 利用目的の通知
- 保守パートナー会社と共同利用することの通知
- 利用目的に合意した旨の記録
- 目隠しシール

お客様登録はがき
サンプル

③ 取得済個人情報に関する利用目的、共同利用の公表(ホームページ)
④ 開示、訂正、利用停止等の連絡先および手続き方法の公表(ホームページ)
⑤ 開示の管理

- 書面による受付、手数料徴収
- 公的証明書のコピー(必要情報以外は塗りつぶした状態で入手)による本人確認
- 受取者が確認できる配達方法で郵送

サポート部門

組織的安全管理措置 ：規程等の整備と運用

① 顧客サポートデータ取り扱い手順

- 顧客データの取得作業
- 顧客サポート管理システムへの顧客データ入力作業
- サポート伝票発行、サポート完了情報の入力作業
- ヘルプデスク作業手順、禁止事項

ハガキ・FAX・Web
システムへ入力した あとの媒体の処理は？
作業担当者の管理は？
やってはいけないことを 明確に！

② サポート伝票取り扱い手順

- 保管方法（保管ロッカー鍵管理、持ち出し記録）
- 委託条件
- 廃棄方法（シュレッダー）

保管場所、保管・廃棄の 方法は？
委託先の選定基準は？ 契約方法は？

定期的な評価、見直し、改善が必要

サポート部門

コールセンターの物理的安全管理措置

① 物理的構造

- 独立した居室、防音、カードゲート、 パーティションで仕切った業務机
- プリンター、コピー、FAXの設置場所（コールセンター内、部長からの目視確認）

② 入退管理

- カードゲート、入退簿での入退記録
- 記録メディア、業務に必要無い物の持込禁止

技術的安全管理措置

顧客サポート管理データへのアクセス権限制御

名前	職種	アカウント名	新規入力	読み出し	更新入力	削除	印刷	リスト出力
**A	本部長	****	—	○	—	—	—	○
**B	入力作業者	****	○	○	△（承認後可）	△（承認後可）	—	—
**C	サポート伝票作業者	****	—	○	—	—	○	—
**D	お客様窓口	****	—	○	—	—	—	—
**E	アウトソーシング会社	****	—	○	—	—	—	—

工場部門

JNSA

組織的安全管理措置

① 工場内事故時等の緊急時体制とあわせた個人情報流出時の連絡体制の整備
② 業務プロセスを考慮した紙伝票（出荷伝票）の取り扱い手順
③ 製品盗難対策用監視カメラを活用したモニタリング時の注意事項

- モリタリングの目的、すなわち取得する個人情報の利用目的をあらかじめ特定し、社内規程に定めるとともに、従業者に明示すること。
- モニタリングの実施に関する責任者とその権限を定めること。
- モニタリングを実施する場合には、あらかじめモニタリングの実施について定めた社内規程案を策するものとし、事前に社内に徹底すること。
- モニタリングの実施状況については、適正に行われているか監査又は確認を行うこと。

人的安全管理措置

① 工場の作業マニュアルに添った訓練、危険個所の説明に「個人情報保護」の観点を加える
② 朝礼やKYT（危険予知トレーニング）活動を活用した意識向上

委託先の監理（運送会社）

① 個人データが含まれる出荷伝票の取り扱いを委託することになるため、監督責任が課せられる
② 委託契約のポイント

- 受託者に対し、個人データ（出荷伝票）の管理責任を明確化
- 安全管理措置（出荷伝票の保管方法、契約範囲外の利用・複製の禁止、廃棄方法等）
- 再委託の条件（委託者の同意、誓約書の入手等）
- 契約内容が遵守されていることの確認

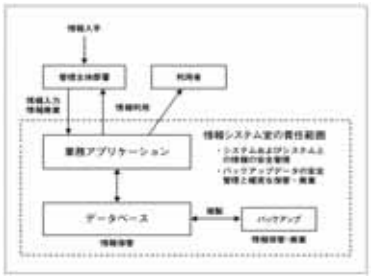
情報システム室

JNSA

情報システム室で取り扱う個人情報

①情報システム上の個人情報
・管理主体が他部署、安全管理のみ実施

②情報システム室が入手する個人情報
・委託先、派遣従業者に関する個人情報
・モニタリング、監視に伴う個人情報
・情報システム管理上入手する社員情報



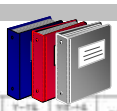
情報システム室がとるべき体制

役職	役割
情報システム管理	・個人データの管理責任者 ・情報システムの改廃および限定変更等の承認 ・情報システム固有の監査責任者（脆弱性診断・ログ分析/データフォレンジック等） ・個人データの漏洩等事故が発生した際の代表者への連絡責任者
グループリーダー（インフラ系・業務系）	・情報システムの改廃および限定変更等の作業責任者 ・情報システム固有の監査作業責任者 ・個人データの漏洩等事故が発生した際の情報システム管理への連絡責任者

情報システム室

JNSA

各種規程の整備



各種台帳による管理

①個人データ保管システム台帳
・どのシステムで管理されているかの一覧

②アカウント登録に関する台帳

③アクセス権限に関する台帳

④バックアップ履歴に関する台帳

⑤システム作業履歴に関する台帳
・ハードウェア・ソフトウェアの改廃
・セキュリティパッチ、バージョンアップ等作業

情報システム室

JNSA

想定される脅威から適切な対策の選択が重要 ～サンプルを提供～

物理的安全管理措置

・入退館（室）管理
　・部外者の侵入
　・関係者の管理
・盗難管理
　・特にPCや可搬媒体
・機器・装置の物理的保護

人的安全管理措置

・雇用・委託契約における秘密保持
　・運用委託契約
　・開発委託契約
・従業者への周知・教育・訓練
　・システム運用者
　・システム管理者

技術的安全管理措置

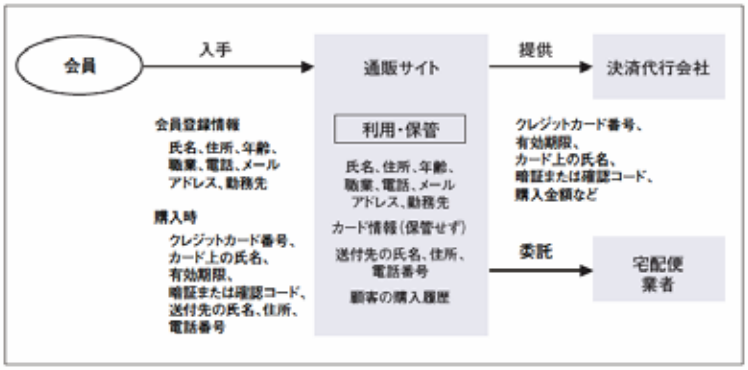
・認証
・アクセス制御
・アクセス権管理
・アクセスログ管理
・不正ソフトウェア管理
・データ移送
・情報システムの動作管理
・情報システムの監視

・サーバー（OS）
・ミドルウェア(DB)
・ネットワーク
・クライアント等

その他
・委託先選定基準と責任分界点
・システム構築の際の設計ポイント

インターネット通販部

- インターネット上の通販を自社運営する際のポイントを個人情報の流れをもとに解説



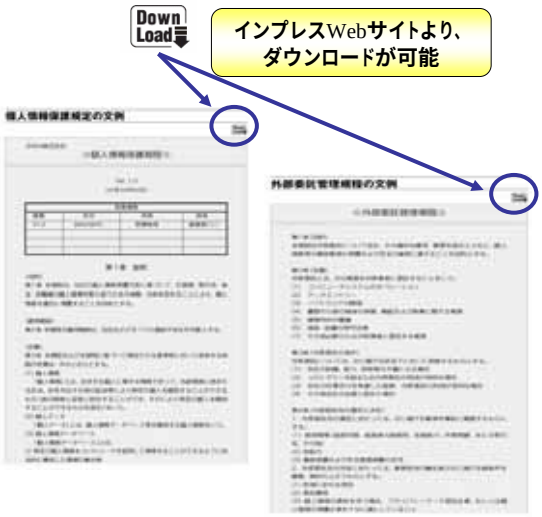
図表9-3　業務における個人情報の流れ

インターネット通販部

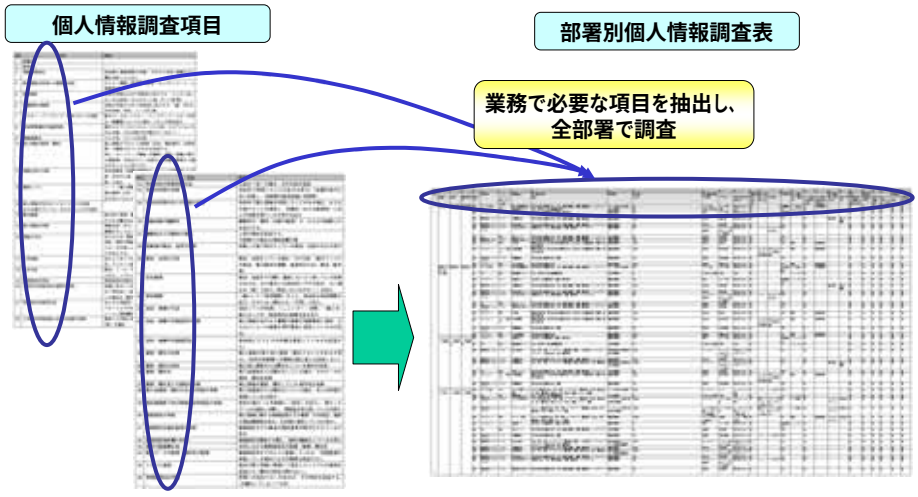
- 通販会員情報の入手と利用、管理
  - サイト上での利用目的の告知、同意取得は？
  - 会員情報の訂正と退会に伴う廃棄は？
  - 決済代行会社などへの個人情報の提供は？
  - 配送の委託に伴う個人情報開示は？
- 個人情報を扱うシステム、アプリケーション開発、運用における安全管理の考え方
  - 情報システム室との協力関係や責任分界点は？
  - 開発委託先の選択、管理は？
  - 安全なアプリケーションを開発するには？
  - 運用現場での安全管理措置は？

参考資料

公開文書
1 個人情報保護宣言
2 個人情報の取扱いについて
社内文書（規程・基準等）
1 個人情報保護規程
2 個人情報保護基準
3 従業者情報保護基準
4 外部委託管理規程
5 記録媒体管理基準
6 お客様相談窓口運用手順
社内文書（契約書・書式例）
1 業務委託契約書
2 個人データ取扱確認書
3 機密保持契約書
4 入社時・退社時の誓約書（役職員）
5 労働者派遣基本契約書
所定書式
1 謝罪文
2 個人情報管理台帳
3 採用応募規約（Web用）
4 採用業務ギャップ分析結果
5 委託先適正報告書
6 個人データ授受書

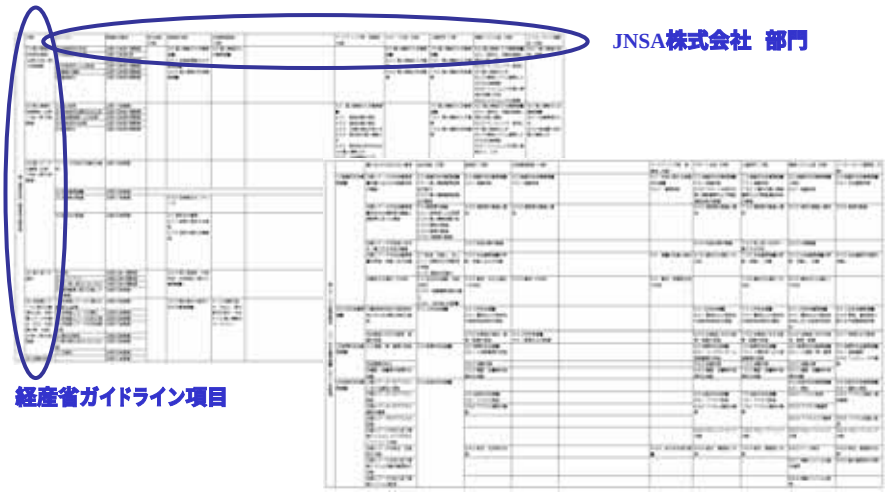


個人情報洗い出し



チェックリスト

経産省ガイドラインとの対比表



JNSA

JNSA

ご清聴を感謝申し上げます

