# 製薬企業における個人情報保護体制整備支援

株式会社カティエント*
ビジネスソリューションマネジャー
水口　淳

## 1．はじめに

2005年４月１日　個人情報保護法が正式に施行された（図１）。これを受けて各社の個人情報保護法への取組み姿勢が注目されており、各業界の企業（特に大手）では、個人情報保護法対応のための体制整備に本格的に動き出した。

個人情報保護法とは　**事業者に対する規制法である**

- 6ヵ月後には全社に対して様々な義務と対応が迫られます。
  - 利用目的を明示し、同意を得る義務
    - 目的以外に利用できない
    - 不正に取得しない
  - 個人情報を安全に管理する義務
    - 入退室管理・アクセス制御・ウィルス対策
  - 第三者提供が制限される
    - 第三者に提供する場合には同意を得ること
  - 情報の開示・訂正・利用停止の要請に応える義務
- 違反した場合には行政処分があります。

**図1　個人情報保護法とは何か**

製薬企業であるＡ社でも、この個人情報保護法対応のための体制整備が喫緊の課題として挙げられており、CACとしても初めての個人情報保護体制整備のための支援を行った。本稿では、このプロジェクトについて報告する。

## 2．なぜ個人情報保護法への対応が重要なのか

実施レベルの差はあるが、最近では多くの企業で社内の情報セキュリティに対する取組みが行われてきている。しかし、これまで法的な規制等がなかったためか、独自の基準で対応を行ってきたのが現状だ。

最近頻発している情報漏洩の問題は、すべての企業にとって対岸の火事ではなくなってきている。宇治市の個人情報漏洩事件が訴訟に発展したのを契機に、情報漏洩に伴う訴訟問題が大きくクローズアップされるようになったが、そうした訴訟問題の中でも、東京ビューティセンターの事例は特に注目を集めた。漏洩した情報の「プライバシー度」によって訴訟金額がアップする可能性が出てきたからだ。このような背景から、「個人情報の漏洩は高い代償を伴う」という認識が企業経営者に浸透し始めた。さらに、個人的な損害賠償請求では賠償額も小さいが、集団による訴訟が行われると損害賠償総額が莫大になることも最近は問題視されるようになった。経営者は、個人情報の漏洩が、集団訴訟＝多大な賠償請求＝経営的危機という深刻な連鎖反応を引き起こすことを認識する必要がある。

こうした状況の中で、各企業は、速やかに個人情報保護対策を立てる必要に迫られている。

当然ながらＡ社も医薬事業等に関連する大量の個人情報を保有しており、万一に備えた体制整備が喫緊の課題となっていた。

＊株式会社カティエントは、2005年３月に設立されたCACグループの新会社で、顧客の企業価値向上のための提案を行う。詳細はP14からの記事を参照。

## 3．A社でのプロジェクト発足までの経緯

A社では、企業コンプライアンス体制強化のために、環境・安全、品質保証等の側面から体制整備が行われてきた。個人情報報保護法への取組みについても同様にコンプライアンス体制強化の一環として対応が開始されていた。

このような背景の中、2004年9月に法務・コンプライアンス部門を主管とした個人情報保護体制整備プロジェクトが発足した。グループ会社を含む全社横断のプロジェクトとして、推進役となる事務局と本社関連部門からの代表者を含む小委員会、グループ会社代表者を含む大委員会が構成された。

## 4．本プロジェクト受注経緯

### 4.1　CACユーザー会での担当者との出会い

A社はCACユーザー会のメンバーで、2004年７月のユーザー会にIT企画部門の担当者が出席されており、そのときにセキュリティに関連する話題について話をさせていただいたのが初めての交流であった。

A社では、個人情報保護法への対応、情報セキュリティ全般に対する検討ならびに社内の参画メンバーの人的要員不足、などの事情により、外部のコンサルタントを入れてプロジェクトを推進する必要性があった。

そのユーザー会から約１ヵ月後、A社でもいよいよ個人情報保護法への対応準備を行うプロジェクトが立ち上がり、提案をしてほしい旨の打診を受けた。

### 4.2　提案の実施

早速提案の準備を行うが、プライバシーマーク取得に関するコンサルティングサービスは巷にあふれていても「個人情報保護法への対応」という新規の分野においてはサービス事例自体が極端に少なく、CACにもこれまでに事例がなかったため、提案内容を詰める段階でかなり苦慮した。しかし、最終的にはプライバシーマーク取得プロセスならびにISMS認証取得プロセス等を参考に、独自のプロセスを考案し提案書にまとめた。

### 4.3　３社の競争になぜCACが勝てたか

提案は３社によって行われ、提案当初で、まず２社に絞り込まれた。その後、最終的にCACが受注することとなったが、当初、提案金額などを単純に比較した場合は、CACは勝てないのではないかと思われた。

CACが選ばれた理由は、次のようなものだと考えられる。

1）ユーザー会でのA社担当者との会話で、情報セキュリティに関する考えに共感を持っていただけたこと。

2）システム開発に関する実績を多数持っていたこと。

3）CACの提案内容に盛り込まれている提示可能雛形の数と内容が他社より勝っていたこと。

4）タイミングよく、また他社に先駆けて（ユーザー会で）個人情報保護法に対するCACのアプローチを紹介できたこと。

以上のことが、大きなポイントとなったのではないかと考えている。

## 5．プロジェクトの概要

### 5.1　プロジェクトの目的

本プロジェクトの目的は、個人情報保護法に対応するため、グループを含む全社での管理体制を整備し、個人情報をより安全に取扱う全社的な意識向上につなげることであった（図２）。

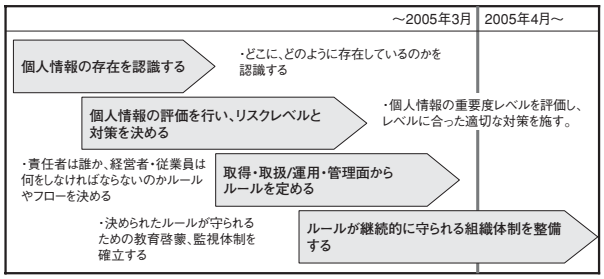


**図2　A社における対応**

### 5.2　プロジェクトのゴール

●全グループにおける社内体制の確立
●個人情報保護法対応方針や規程類の策定
●方針や規程類に基づいた役割、責任の明確化
●個人情報を取扱うためのプロセス・有事の際のプロセスの明確化
●教育計画を策定し、実施準備体制の整備と管理職への教育実施

### 5.3　主なプロジェクトの成果

●問い合わせ窓口（個人情報取扱事務局）の設置
●個人情報保護管理者、監査責任者等の管理体制の確立
●問い合わせ、有事の際の報告連絡体制等の整備
●個人情報保護方針、保護規程、保護基準、主要部門での手順書等の策定
●個人情報の評価と管理台帳の整備

## 6．CACアプローチ概要

### 6.1　役員プレゼンテーション

プロジェクトは、まず役員へのプレゼンテーションから始まった。その内容は以下のとおりである。

●個人情報保護法とはどのような法律か
●同法は企業に対して何を求めているのか
●要求事項に対し企業として何をしなければならないのか
●万一、事件・事故が発生した場合のリスクはどのようなものか

この役員プレゼンテーションでは、プロジェクトの概要を単に説明するのではなく、個人情報保護におけるリスクマネジメントに焦点を当てることに注力した。

### 6.2　委員会責任者メンバー召集

役員プレゼンテーション後すぐに、委員会を構成する組織の責任者に対する説明会を実施。委員会責任者に向けては、プロジェクトの概要と、役割分担、詳細の作業について理解いただくことに焦点を当てたプレゼンテーションを行った。特に、今後予想される作業については、十分理解を得てもらえるよう注力した。

### 6.3　プロジェクト準備

プロジェクト準備段階では、まず個人情報保護法を知る、そして理解することを重点的に行った。本プロジェクトが扱う個人情報保護法については、その解釈について両社の保護法に対する認識レベルを確実に合わせておく必要があった。特に、今後の作業において影響を及ぼす部分であるため、注力した部分でもある。

## 7．実行計画の概要

2004年 9 月～2005年 3 月までの主要タスク（全体）、詳細タスク（週単位）、両者役割分担、成果などを中心にまとめる。実行計画策定においては、規程策定、現場での個別ルール策定や、緊急時の対応プロセス、外部からの問い合わせ対応等のプロセス、管理者教育（一部社員への教育含む）等、個人情報保護法要求事項に対する企業対応準備をすべて網羅するための計画化を行った。特に、個人情報保護法の要求事項である、取扱いに対する外部からの問い合わせや緊急時の対応手順を明確に確立することが必要であったため、この点についても注力した。

## 8．タスクの概要

本プロジェクトでのタスクを以下に記載する（図 3）。

### 8.1　プロジェクトタスク詳細

1）個人情報を認識する

・ポイント：社内において、どのような情報が「個人情報」なのか。特に、「個人情報」の区分、つまり「個人情報」「個人データ」「保有個人データ」という認識を明確にすることが重要である。


図3　プロジェクトのタスク・経緯

また、個人情報保護法では、社外の個人情報（顧客個人情報等）だけではなく、社内の個人情報（社員健康情報等）についても同様の取扱いを要求している。

・アプローチ：関係部門の代表者を中心とした、大委員会等での説明や、事務局からの個別説明等を平行して実施し、個人情報に関する区分認識を明確にすることに重点を置いた。

2）個人情報を収集し評価する

・ポイント：個人情報がどこに、どのように存在し、どのような重要性を持っているかを明確化（文書化）する。

本プロジェクトにおいても、このステップは非常に重要である。このステップを的確に実施することが、その後の情報の評価や評価に対する対策適用度合いを決定する基礎となるためである。また、収集された情報の重要度を鑑みて評価する場合の、「企業内基準」の決定に際しても重要なポイントとなる。一般的な評価基準は参考となるが、最終的には企業独自の評価基準を策定し、その評価基準で対策の適用度合いが決定されるため、対策に費やす費用に大きく影響を及ぼすこととなる。

・アプローチ：業務プロセスを明確化しながら存在している個人情報を洗い出し、台帳にまとめる。洗い出された個人情報から保有個人データを区分した上で、その情報の重要度を企業独自で策定した規準と照し合せて評価する。

当初の手順では業務プロセスを明確にすることから開始したが、最終的には、まず個人情報と考えられる情報をすべて洗い出し、その後一定の基準で情報を取りまとめる方式を採用した。また、重要とされる業務（経営戦略上注力すべき業務など）については、その業務の根幹となる情報を基に、その業務フローを明確化し、確実に情報の収集と評価が実施できるよう優先させて注力した。

3）ルールを運営管理するための組織・役割を決める

・ポイント：名称だけではなく、実際に機能する組織、役割を、通常の業務プロセスや企業慣習などを基に明確化（文書化）する。

・アプローチ：組織・役割モデルを想定し、バイネームによる実施可否等の検証を交えながら組織体制と役割案を事務局・小委員会レベルで策定し、大委員会で討議検証を行いながら決定する。

4）情報取扱いの全体ルールを策定する

・ポイント：実際に実行可能なルールを明確化（文書化）する。特に全体ルールは、全社共通で理解でき、個別ルール作成時に参照して手順書が作成できる内容であることが重要。

・アプローチ：ルール雛形等を基に、関連する部門代表者（業務を熟知している）を交えて、事務局・小委員会レベルで現状を踏まえながら実行可能なルール案を策定し、大委員会で討議検証を行いながら決定する。

特に、今後、グループを含む全社の組織において遵守されるべき方針・ルールであるため、希望的な内容ではなく、あくまで「継続的に実行可能な」ルールであることを目指した。

5）個人情報の評価結果と個別の環境を鑑みて、個別の取扱手順書を作成する

・ポイント：個別の業務形態や慣習を基に、日々の実務に沿った取扱手順を明確化（文書化）する。

・アプローチ：個別業務でのデータの取得から廃棄までのフローを、業務プロセスに沿って可視化する。さらに、可視化されたフローに合わせた安全な取扱手順（特に廃棄や委託の場合など）を、業務に支障をきたさないように個別部門関係者と討議し決定する。

本プロジェクトでは、推進効果を向上させるために個別ルールを策定するモデルケースを選定した。まず手順書のモデルを作成する部門や組織を選定し、他の業務や組織で同様の手順書を策定できるよう内部での事例を作ることに注力した。

6）外部からの問い合わせ、開示請求への対応プロセスを策定する

・ポイント：外部からの問い合わせ等の経路を想定し、どこが（誰が）、どうやって対応するか、また、想定外対応をどのように行うかを明確化（文書化）する。

・アプローチ：実際の問い合わせ、開示請求の経路を複数想定し、最終的に誰が受けて、どう対応するのか、対応する場合の手順や必要な資料は何かを、プロセス案を事務局・小委員会レベルで策定し、大委員会での討議検証を行いながら決定する。

特に、個人情報保護法が施行された場合、開示請求等が一斉に行われることが予想されていたため、その準備は万全に整えておく必要があった。

7）事件・事故発生時の対応プロセスを策定する

・ポイント：事件・事故発生時の連絡体制や、事前の兆候の発見・連絡のためのプロセスを明確化（文書化）する。

・アプローチ：問題発生現場（社内、社外を含む）から、マスコミ、管轄官庁までの連絡ルートと対応後のフィードバック体制モデル案を事務局・小委員会レベルで策定し、大委員会での討議検証を行いながら決定する。

事故発生については、その可能性についてもいち早く察知できるよう配慮した。

8）教育マテリアルを策定する

・ポイント：一般的な知識部分と、企業独自の個別事情（慣習やルール等）を盛り込んだコンテンツを作成する。

・アプローチ：一般的に使われている教育マテリアルや業界動向等を取り入れた基礎知識部分と、方針・規程・基

準を基に、独自の状況を踏まえたマテリアルを策定した。

9）公表事項を検討する

・ポイント：将来の事業拡大を想定しながら、現状の利用目的等のホームページでの公表事項を作成する。A社では利用目的等をできる限り詳細に公表することを目指した。

・アプローチ：業界団体、所轄官庁から公表されているガイドラインや他社事例を基に、独自の業務内容を鑑みて公表内容を決定した。

## 9．CACアプローチの特徴

### 9.1　情報セキュリティマネジメントシステム構築プロセスを参考にしたプロセスアプローチ

本プロジェクトでは、プロジェクトのアプローチとしてISMS（情報セキュリティマネジメントシステム）構築アプローチを参考とし、CAC独自のアプローチに改良した。

方針（ポリシー）の策定から、情報収集、評価、個人情報保護に対するルールを策定、そのルールを運用管理する組織の構築、およびトップマネジメントを中心としたレビュー体制の構築を行うことを考案した。そのためアプローチとしては、ISMS認証取得のためのプロセス並びにプライバシーマーク認定取得プロセスを参照しながら、「個人情報保護法並びに経産省ガイドラインの要求事項*1」を組込んだプロセスを行った。

A社は厚生労働省管轄だが、他省庁管轄業務も行っている。また、プロジェクト発足当初は、厚生労働省からの個人情報保護法への対応のためのガイドラインは出ていなかった*2こともあり、「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」（経産省ガイドライン）をベースとして個人情報保護法への対応策を検討することとした。

### 9.2　CAC独自の決め細やかなアプローチ

一般的に行われているプライバシーマーク取得コンサルティングの多くは、取得までのアプローチへの助言と雛形の提示が主体となり、対象顧客側が中心となって規程等の策定が行われる場合が多い。ベンダーの業務は、策定された成果に対するレビューを行うのが主体となる。

個人情報保護法への対応事例がない中、CACのアプローチでは、顧客側の環境や事情を鑑みてアプローチや成果を柔軟に変化させることにより対応した。雛形によるルール作りを先行するより、ルールを遵守できる組織作りに重点を置き、さらに顧客サイドにじっくり入り込むことにより、顧客環境や事情を理解し、ルール作り・組織作りに反映させることを重点的に行った。情報の収集においては、収集と評価を同時に行うための手順や評価シートを考案した。

また、プロジェクト上の第一の重要ポイントとなるリスク評価においては、短期間で全社の対策レベルを統一させるために、「ベースラインアプローチ」を基に経産省ガイドラインの要求事項に沿って対策レベルを設定し、基準と個別ルールの策定に反映させることに重点を置いた。

## 10．障壁

### 10.1　プロジェクトのアプローチ上の障壁

そもそも「個人情報保護法に対応する」ためのサービスや支援の具体的プロセスは確立されておらず、本プロジェクトでも、ISMS認証取得プロセス、プライバシーマーク認証取得プロセス、経産省ガイドライン、および数少ない関連書籍等を参考にプロセスを検討せざるを得なかった。

### 10.2　プロジェクト実施上の組織体制の障壁

A社では戦略上の理由から大規模部門の分離独立（カンパニー制）を進めており、このたびのプロジェクトは、本体が主導し、各カンパニーとカンパニーごとの子会社を含めたグループ全体で推進していく必要があった。

### 10.3　推進上の社内意識的な障壁

本プロジェクトは、「認証取得」などの大義名分が乏しい中、企業コンプライアンス意識向上を目指して実施されてきた。そのため、組織体制作りと同様、協力を得るための事務局としての社内根回しが非常に厳しかったのではないかと思う。

---

＊1）「個人情報保護法並びに経産省ガイドラインの要求事項」では、①利用目的の明示、同意取得義務（目的以外に利用できない、不正に取得しない）、②個人情報を安全に管理する義務（入退室管理・アクセス制御・ウィルス対策）、③第三者提供の制限（第三者に提供する場合には同意を得ること）、④情報の開示・訂正・利用停止の要請に応える義務、という4つの義務に違反した場合、最終的に行政処分を受けることになる。個人情報保護法への対応では、上記4点に対する企業としての体制を整備することが必要となる。（4ページ図1参照）

＊2）「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」については、社内従業員の個人情報に関する部分は、「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年構成労働省告示第259号）と整合している。

### 10.4　個人情報保護法に対する解釈

プロジェクト推進上、個人情報保護法条文ならびに経産省ガイドラインを参照する必要性があった。しかし、条文には極めて不透明な部分が多く、また、その解釈に対する弁護士見解もまちまちであったため、解釈に際してはかなり苦慮した。

## 11．反省点

プライバシーマーク取得の場合、目的の大半は認証取得にあり、そのための要求プロセスに沿って体制を整えていくため、比較的社内の協力体制が整いやすく、参加意識も高くなる。しかし、個人情報保護法対応の場合、「10. 障壁」でも述べたように、社内で目的意識を浸透させ全社協力を得ることは簡単ではなくなる。この点を的確に見極めておく必要があった。

また、提案段階においては、個人情報保護法への詳細アプローチを提案書で的確に表現することに非常に苦慮した。

個人情報保護法への対応方法等は、個々の企業によって内容に大きな相違があるため、標準的なプロセスがそのまま適用されることはない。

当初は手探り状態の部分も多々あったが、結果的にはプロジェクトの準備段階で顧客の環境等を徹底して把握し、既存の標準等に囚われない独自のアプローチを構築することができた。

## 12．今後に向けて：CACとしての次期アプローチの可能性

### 12.1　ルール作りからルールの定着化に向けて

ルール策定が終わると、そのルールの定着化に向けた教育が必要となる。教育は、全社員に対し継続的に実施される必要があり、そのための教育システム導入とモニタリング機能が必要となる。また、教育内容では、個人情報を扱うための基礎知識から、取扱状況を考慮した個別のルールに合わせたプログラム作りが必要となる。

全体教育では、eラーニングによるシステム導入の要望が増加することが予想され、各企業の状況に合わせたコンテンツ提供や、効果を測定する機能および認識レベルを追尾調査するためのモニタリング機能も求められる。

こうした要望を踏まえたうえで、個人情報保護体制を整備したいと考える企業に対する教育サービスの提供は今後のビジネスチャンスとなる。

### 12.2　システム導入へ向けて

個人情報保護法の施行は、SIベンダーやメーカーの出番を増やすことにもなる。多くの企業（比較的大企業が先行しているが）が、個人情報保護法へ対応するための社内ルール作りに翻弄されているが、そもそもルール作りだけでは十分ではない。次に検討すべきは、このルールを実際に実現するためのシステム導入であるからだ。

今回のプロジェクトでも、「誰が」「何を」「どこまで」「どうやって」やるかをルールとして決めたが、今後の課題として、「どうやって」について、人的な対策だけではなくシステム的な対応を施す必要性が挙げられよう。

CACは、「実行可能なルール」作り、およびそのルールを実現するためのシステム作りも支援できる。トータルサービスとして、ルール作りからシステムの導入、運用管理までを一貫して提供できることが、他社とは異なるCACの強みである。

## 13．終わりに

このたびの個人情報保護体制整備支援プロジェクトを通して感じたことを記載する。

個人情報保護法への対応は始まったばかりで、アプローチはまだ確立されていないが、少なくとも本プロジェクトを通して１つの事例ができあがった。個人情報保護法への対応は、企業によってやり方や程度に相違がある。したがって、標準のプロセスを確立し、広くサービス展開するよりは、顧客サイドに深く入り、その企業を良く知り、その企業と一体となって、その企業独自のルール作りに顧客の立場に立って支援することが「CACらしさ」ではないかと感じた。