個人情報保護に関するコンプライアンス・プログラムの作成指針

はじめに

プライバシーマークを付与認定される事業者は、JIS Q 15001「個人情報保護に関するコンプライアアンス・プログラムの要求事項」（以下「ＪＩＳ」という。）に適合したコンプライアンス・プログラム(以下「ＣＰ」という。)を策定し、実施し、維持し、及び継続的に改善していくことが必要である。

ＣＰとはＪＩＳによると「事業者が、自ら保有する個人情報を保護するための方針、組織、計画、実施、監査及び見直しを含むマネジメントシステム」と定義されている。ここでのマネジメントシステムは、個人情報の保護方針を作成し、それに基づき計画し、実施し、監査し、見直す手続きをスパイラル的に継続することによって、事業者の管理能力を高めていくことであり、既存の品質システム規格（JIS Z 9900 シリーズ）及び環境マネジメントシステム（JIS Q 14001）のマネジメントシステムと共通した原則が採用されている。したがって、JIS Z 9900 シリーズや JIS Q 14001 に合致したマネジメントシステムを既に使用している事業者は、このＣＰの基礎とすることも可能である。

ＣＰを別な言葉で表現すれば､個人情報取扱い業務をＪＩＳに準拠するように構築した業務管理システムと捉えることができる。

個人情報保護のためのＣＰは、以下の手順で作成することができる。

ステップ１：個人情報保護方針を定め文書化する
ステップ２：ＣＰ策定のための組織を作る
ステップ３：ＣＰ策定の作業計画をたてる
ステップ４：個人情報保護方針を組織内に周知する
ステップ５：個人情報を特定する
ステップ６：既存の個人情報取扱いシステムを評価する
ステップ７：ＣＰの構成を検討する
ステップ８：ＣＰの基本となる規程を策定する
ステップ９：ＣＰの詳細規程を策定する
ステップ 10：ＣＰを文書化する
ステップ 11：ＣＰに準じた体制の整備を行う
ステップ 12：ＣＰを周知するための研修を実施する
ステップ 13：ＣＰの運用状況を監査する
ステップ 14：ＣＰの改善を実施する

ＣＰ作成手順の詳細

ステップ１：個人情報保護方針を定め文書化する

事業者の代表者は、個人情報の収集、利用、提供等に関する保護方針を定めること。個人情報の保護方針には、以下の事項を含める必要がある。

a)個人情報の収集、利用及び提供に関する方針

この方針は、事業の内容及び規模を考慮した適切なものである必要がある。

b)個人情報へのリスクの予防並びに是正に関する方針

一般的には、リスクには権限の無い者による個人情報への不正アクセス、個人情報の紛失、破壊、改ざん及び漏えいなどがある。

c)個人情報に関する法令及びその他の規範の遵守に関する方針

事業者の事業に関する法令等の中で個人情報の保護に関する事項が規定されている場合、または行政機関等が特に定めた個人情報保護に関する規範等がある場合、これを遵守する必要がある。

d)コンプライアンス・プログラムの継続的改善に関すること。

ＣＰは、マネジメントシステムであることから、事業者が取扱う個人情報とその扱い方の変化、また事業者を取り巻く環境の変化等に対応することが求められる。したがって、事業者の代表者自らが継続的改善を明確に示しておくことは重要である。

なお、事業者の代表者は、この方針を文書化しなければならない。また、この方針を一般の人が入手可能なように、事業者のホームページに掲載したり、リーフレット等に印刷する等の措置を講じなくてはならない。

ステップ２：ＣＰ策定のための組織を作る

事業者の代表者は、組織の役員及び従業員等で構成するプロジェクトチーム（以下「ＣＰ策定チーム」という。）を組織し、個人情報保護方針に基づいて個人情報取扱いのマネジメントシステムの構築を推進させる。

また、事業者の代表者は、各部門に対して、ＣＰ策定チームへの協力を指示する。

ステップ３：ＣＰ策定の作業計画をたてる

ＣＰ策定チームは、今後の作業スケジュールをたて、関係者に通知するとともに、協力を要請する。

作業スケジュールは、以下のステップを考慮して立案する必要がある。

ステップ４：個人情報保護方針を組織内に周知する

ＣＰ策定チームは、事業者の代表者が定めた個人情報保護方針について、組織の全ての役員及び従業員に周知しなくてはならない。

周知に当たっては、個人情報を保護することの重要性、利点及び個人情報が漏洩等した場合に予想される結果等を説明し、理解させることも必要である。

●個人情報を保護することの重要性・利点の例

個人情報は、当該情報主体のものですので、自分自身でコントロールする権利を有しています。保護が不十分で個人情報が漏洩したり、他の事業者に渡ったりすることによって、情報主体のコントロールが及ばなくなり、情報主体が同意をした範囲を超えて予期し得なかった利用がなされ精神的、物理的被害を被る可能性があります。

一方、今日では企業活動にとって個人情報は無くてはならない非常に重要な価値を持った情報となっています。

したがって、情報主体から同意を得て入手した個人情報は、企業活動のために有効活用すると共に、企業として十分に保護し情報主体の利益を守ることが求められるわけです。

●個人情報が漏洩等した場合の予想される結果の例

上記のように個人情報は情報主体のコントロールの下で利活用されるということが国際的な常識となっています。また、企業活動に不可欠なものとなっていることから、情報主体と企業との間の信頼関係によって活用が許可されていると捉えることが必要でしょう。

このような情報が企業から漏洩等した場合、企業に寄せられていた情報主体からの信頼は一気に崩れ去り、信用回復に多くの期間と努力を要することになります。

また、漏洩等に関係した社員は、社会的な制裁にとどまらず社内的にも懲戒免職等の罰則を受けることとなります。

また、全ての役員及び従業員に周知する意味は、直接に個人情報の取扱いに従事していない場合でも、組織内で個人情報に接する可能性があることから、組織の方針を理解させておく必要からである。

ステップ５：個人情報を特定する

ＣＰ策定チームは、関係者の協力を得て自組織で取扱っている個人情報を特定する。

特定に当たっては、当該個人情報の入手目的、入手経路、社内での取扱経路（取扱部署）、保管(一時保管も含む)場所、保管形態（電子媒体、紙等）、保管期間、廃棄方法等について明らかにするとよい。

この作業によって、当該個人情報に関するリスクが想定できるから、併せて明確にしておき、安全措置を構築する際の基礎とする。個人情報に関するリスクとしては、個人情報への不正なアクセス、個人情報の紛失、破壊、改ざん及び漏えいなどが考えられる。

個人情報を特定するための作業表の例

業務	個人情報（内容）	入手先	入手形態	社内の取扱経路	情報の形態	保管場所	保管期間	提供先	廃棄方法

なお、ＪＩＳでは個人情報を特定する手順の確立が求められている。これは、将来、新たな事業や業務が企画され、それを遂行するようになったとき、個人情報が含まれていないかどうかを評価し、含まれていればそれを特定してＣＰに当該事業・業務を組み込む必要があるかを判断しなければならないからである。また、場合によってはＣＰを改善する必要が出るかもしれない。

したがって、このステップで実施した個人情報の特定作業に該当する機能を作り上げ、更に新たな事業や業務の企画時には必ずこの機能にインプットされるようなシステムの組み込みが必要になる。

ステップ６：既存の個人情報取扱いシステムを評価する

ＣＰ策定チームは、既存の個人情報取扱いのシステムとＪＩＳとを比較し差異を確認し明確化する。

併せて、事業者は、自身の個人情報の取扱に関する法令及びその他の関連規範の有無について確認する。法令及び他の関連規範がある場合、既存の個人情報の取扱がこれらの関連規範等に違反している部分が無いかを確認して明確化しなければならない。

事業者の個人情報の取扱いは、当該事業に関連する法令等の規定がある場合には、ＪＩＳに優先して適用されなければならないからである。なお、その他の規範として考えられる、いわゆる業界ガイドライン等に関しては、これもＪＩＳと併せて遵守する必要があるが、ＪＩＳの要求事項のレベルよりも下回っている場合には当然のことながらＪＩＳが優先されなければならない。

この作業は、今後のＣＰ策定の取り組みに先駆けて必要となる。

ステップ７：ＣＰの構成を検討する

ＣＰは、自社の個人情報保護方針に沿って個人情報を取扱うためのマネジメントシステムである。したがって、事業者の業種、規模、既存の他のシステムとの整合性等を考慮し、実効性の伴ったものでなければならないことから、定められた構成（雛型）が存在するものではない。

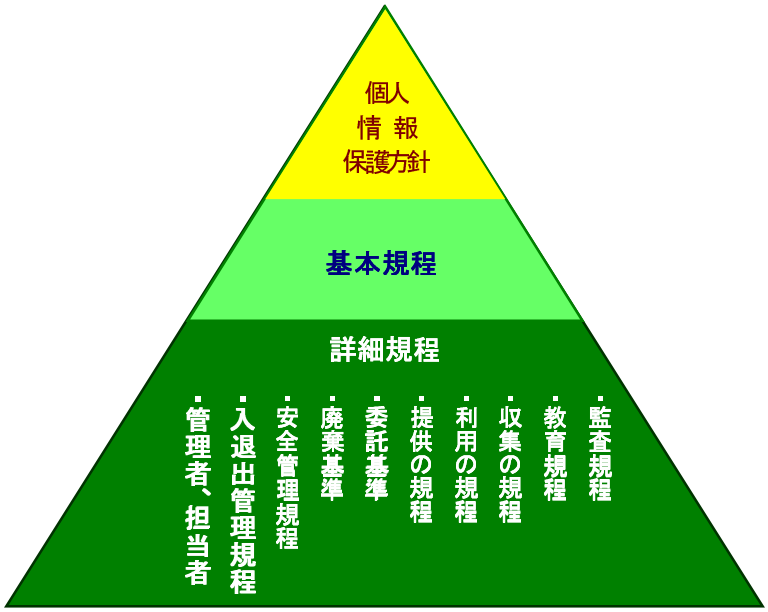
そのため、最初に事業者に合ったＣＰの構成を検討する必要がある。

なお、ここではＣＰの構成を図のように設定して、これに沿って以下の説明を行うこととする（繰り返すが、ここで示したＣＰの構成は、説明のために敢えて設定したものであり、全ての事業者に推奨するものではない。）。

「個人情報保護方針」は、ＣＰの前提となるものである。ステップ：１で策定したものがそのまま利用されるが、これに加えて個人情報保護の必要性を理解させるために、個人情報保護が必要な背景、個人情報が保護されなった場合の損失（ステップ４参照）、個人情報保護をめぐる国際的な動向等を示すことも有効である。

「基本規程」は、ＪＩＳ及び業界ガイドライン等で示している個人情報の収集、利用、提供、保管管理等の側面での基本原則を明確にするものである。

「詳細規程」は、収集、利用、提供、保管管理等の実務に当たって、担当部署・担当者が実際にとるべき行動を詳細に規定したものである。



図．個人情報保護のためのCP構成の例

ステップ８：ＣＰの基本となる規程を策定する

ＣＰの基本規程は、当該事業者の個人情報の取扱いに関する基本原則を定めたものである。即ち、個人情報の収集、利用、提供、適正管理義務、情報主体の権利への対応、社員教育、苦情等への対応、監査、ＣＰの見直し及び文書管理を行う際の基本的な考え方を取り決めたものである。

これらの内容については、ＪＩＳにおいて要求されているので、その要求内容を満たすことが必要である。

そのため、基本規程はＪＩＳの **4.3 計画、4.4 実施及び運用、4.5 監査、4.6 事業者の代表者による見直し**の内容を自社の用語、言葉を用いて、理解し易いように規定したものと考えることができる。

なお、基本規程の策定については、事業者が所属する業界団体等が定めた個人情報保護に関するガイドライン、及び事業を規定した業法等も参考にすることが必要である。先にも述べたとおり、業法等の法令がある場合はＪＩＳに優先するため、基本規程に反映しておくことが求められる。

参考１：基本規程策定のチェックリストを参照

ステップ９：ＣＰの詳細規程を策定する

全ての従業員が基本規程を遵守して個人情報の保護を実現するためには、基本規程を受けた具体的な手順、手段等が詳細に規定されていなければならない。

そのために、以下の事項に関する詳細な規定を定める必要がある。

a) 事業者の各部門及び階層における個人情報を保護するための権限及び責任の規定
b) 個人情報の収集、利用、提供及び管理の規定
c) 情報主体からの個人情報に関する開示、訂正及び削除の規定
d) 個人情報保護に関する教育の規定
e) 個人情報保護に関する監査の規定
f)内部規程の違反に関する罰則の規定
g)個人情報のリスクに対する予防措置（技術的、管理的、物理的）の規定
h) ＣＰ文書、個人情報保護実施記録に関する文書管理の規定

これらの詳細規程は、共通的な部分と担当部署に依存する部分があると考えられる。担当部署に依存する詳細な部分は、当該担当部署に協力要請して規定させることがＣＰの実効性を高めるためには望ましい。その際には、事前に担当部署に対して個人情報保護方針、基本規程を十分に説明し理解させておくことが必須である。当該部署により規定された部分については、ＣＰ策定チームが個人情報保護方針、基本規程との整合性を十分に確認し、不整合がある場合は担当部門の間で協議して改善していかなければならない。なお、担当部署を巻き込んだ詳細規程の作成方法を採ることによって、ＣＰ策定の過程において、関係部門に個人情報保護方針、基本規程を周知することができるという効果も期待できる。

なお、詳細規程については、既存の規程（例えば、罰則を規定した就業規則等）を参照して適用することも可能である。

また、上記以外にも当該事業者の実情に応じて必要な事項を規定することが望ましい。

策定した詳細規程についても、組織において決裁権限を有する者（企業の代表者）によって承認を受けなければならない。

a) 事業者の各部門及び階層における個人情報を保護するための権限及び責任の規定

基本規程には、個人情報保護のための管理者、監査責任者に関する役割と責任及び権限が規定されている。個人情報保護管理者は、自社の個人情報保護に関するＣＰの実施及び運用に関する全責任を事業者の代表者から与えられている。また、監査責任者も事業者の代表者から任命され、監査を指揮し、監査報告書を作成して事業者の代表者に報告することとなっている。

詳細規程には、個人情報保護管理者の管理の下で個人情報の取扱いを担当する各部門のレベルで、部門管理者、権限及び責任を明確に規定しなければならない。支店、営業所等が全国に点在している場合においては、これらの場所についても同様に規定する必要がある。規定の結果は、体制図として整備することが望ましい。

b) 個人情報の収集、利用、提供及び管理の規定

個人情報の収集、利用、提供に関する関連部署の詳細手続きを規定する。また、個人情報を適正に管理するため、正確性の確保、安全性確保に関する管理面の対策と手

続き、及びリスクが顕在化した場合の是正措置に関する手続きについても規定する。なお、リスク発生の予防に関する技術的、物理的対策に関しては、別途規定を設ける必要がある（以下の、ｇ）を参照。）。

個人情報の収集に関しては、直接収集と間接収集する場合に分けて、基本規程の収集の原則に従って、業務のそれぞれの現場で対応すべき事項について詳細に規定する。

直接収集の場合は、情報主体に収集目的を伝え同意を得るための詳細な手続きが重要である。収集目的の伝え方には、口頭、目的を明示した文書（約款等）を示して読み上げる、ポスター等による掲示等があるが、事業者の事業の推進に最適な方法を採用して手続き規定に反映しなければならない。

間接収集の場合は、収集先に対して確認する事項（情報主体から提供の同意の有無、不正･不法な手段で収集したものでないこと等）、確認方法、情報主体から提供の同意を得ていない個人情報の利用に当たっての手続き等を可能な範囲で詳細化して規定すること。

利用、提供に関しては、当該個人情報の区分（直接収集したもの、間接収集したもの）に応じた手続き規定が必要である。

正確性の確保に関する規程は、データ処理システムの運用（オペレーション）に関する規定、更新手続きの規定、処理結果の確認規定等、個人情報取扱い担当者のミスによる誤りを防止するための手続きを規定しなければならない。

安全性を確保するための規程には、合理的な安全対策に関して規程する必要がある。安全対策措置の内容等については、対策の抜け道を残さないために個人情報に関するリスクとの関連を確保しておくことが求められる。一般的には、次に示す安全性確保のための規程が考えられる。

①個人情報の取扱い場所（館、室等）への無権限者の立ち入り許可・制限のための入退管理規程
②個人情報の処理システム（コンピュータ、データベース等）の利用者を許可・制限するアクセス管理規程
③個人情報の保管・廃棄・バックアップ等に関する個人情報管理規程
④個人情報処理の委託に関する委託先の選定基準、契約の基準等を定めた個人情報委託管理規程

c) 情報主体からの個人情報に関する開示、訂正及び削除の規定

個人情報に関しては、当該情報主体に個人情報の開示、訂正、削除の権利が認められているが、このような情報主体からの権利の行使の求めに応じて、如何に対応するべきかを詳細に規定しておく必要がある。

情報主体とのトラブルは、これらの求めに的確に対応しなかったことに因るものが多いことから、これらのことを考慮した規定とするべきである。なお、開示、訂正、削除の求めから、どの程度の期間で応じるべきかについても規定しておくことが望ましい。

d)　個人情報保護に関する教育の規定

ＣＰを全従業員に周知・徹底するための教育・訓練に関する規定を策定する。規定すべき内容は、下記の事項が考えられる。

- 目的
- 時期、期間、対象（職員、臨時要員、派遣要員など全てを含む）
- 内容、方法、場所
- 体制（担当者）
- 通知手続き
- 効果の確認方法
- 実施記録の方法、内容　　等

e)　個人情報保護に関する監査の規定

ＣＰの整備状況、ＣＰに基づく体制整備状況、運用状況を定期的に点検し評価するための監査に関する規定を策定する。規定すべき内容は、下記の事項が考えられる。

- 目的
- 対象、時期（期間）
- 実施体制
- 監査担当者の責務と権限、倫理、守秘義務
- 計画（基本計画、個別計画、事業者の代表者による計画の承認）
- 被監査部門への通知手続き
- 実施の手続き
- 監査報告書（提出先、報告会）
- フォローアップ
- 監査記録の方法、内容、保管　　等

***参考２：個人情報保護に関する監査規程モデル*を参照**

f)　内部規程の違反に関する罰則の規定

個人情報の取扱いについて、ＣＰの定めに違反した場合の措置を規定する。実際の罰則規程は、就業規則等に既に定められているものを適用することでもよいが、その場合には本規程の中で適用する規則等を明示すること。

g)　個人情報のリスクに対する予防措置（技術的、管理的、物理的）の規定

個人情報の安全管理のために、個人情報に対するリスクの発生を予防するための技術的、管理的、物理的措置を規定する。対策は、一つの方法のみで十分というわけではなく、総合的な検討が求められる。そのため、ｂ)で示した管理規定も視野に入れて、新たな対応を検討することは効果を高めるためにも必要である。

安全性を確保するための措置については、ＪＩＳにおいて合理的な安全対策を求めている。ここで、合理的という言葉の解釈が非常に曖昧なために、事業者においてどの程度の安全措置が合理的と判断できるかという問題がある。

安全対策は漫然と実施するのではなく、対象（この場合は、個人情報の取扱い業務システム）に対するリスクを認識し、その顕在化を防止するために措置するものである。したがって、個人情報の取扱いに関するリスクが明確に認識されており、そのリスクに対するさまざまな予防措置を検討して、その中で当該事業者が取り得る最良の措置を講じることが、合理的な安全措置と捉えることができる。したがって、プライバシーマーク制度においても、合理的な安全措置については、各事業者に共通的な一定の基準を特に示していない。

ここで、“事業者が取り得る”としたのは、検討したさまざまな対策の中から、費用、構築の容易さ、運用の容易さ、効果等の観点から総合的に検討して事業者自身が最適と判断した対策が実効性等の面からも効果的と考えられるからである。また、一つのリスクへの対策は、幾つかの対策を組合せることによって対応できるものが多いことから、技術的対策、物理的対策、管理的対策から多方面の検討が必要である。このような過程を経て作り上げた安全対策の措置は、十分に合理的である。

個人情報に関するリスクは、ＪＩＳにも規定しているとおり、不正アクセス、紛失、改ざん、破壊、漏洩に分類できる。これらのリスクに対しては、通商産業省が定めている「情報システム安全対策基準」、「コンピュータウイルス対策基準」、「コンピュータ不正アクセス対策基準」や、その他の機関等が定めた数多くの基準を参考にする等して検討するとよい。これらの基準には、共通的にリスクに対する対応の基本的考え方が示されているから、“事業者が取り得る”対策といえども基本を押さえておくことは必要である。

例えば、下記のような対応策を検討すること。

①不正アクセスへの対応：
- アクセスを制御する。
- 外部からの接続を遮断する。
- アクセスログをとる。
- アクセスログを定期的にチェックする。

②紛失への対応：
- 鍵の掛かる場所に保管する。
- 鍵は、特定者（部門の管理者等）が管理する。
- 授受の記録をとる。
- バックアップをとる。

③改ざんへの対応：
- アクセスを制御する。
- データ（伝送データを含め）改ざん防止(暗号化)措置をする。
- アクセスログをとる。

④破壊への対応：
- 外部からの接続を遮断する。
- バックアップをとる。

⑤漏洩への対応：
- 個人情報へのアクセスを制御する。

・鍵の掛かる場所に保管する。
・鍵は、特定者（部門の管理者等）が管理する。
・データ（伝送データを含め）改ざん防止(暗号化)措置をする。

事業者の外部と電子メールによって情報交換している場合は、コンピュータウイルスによるデータの破壊の可能性が高まっていることから、このための予防措置は特に十分に検討しなければならない。

予防措置を講じていたにもかかわらず、個人情報に対するリスクが顕在化する場合も、可能性としては残されている。そのため、是正措置も予め検討して講じる必要がある。

是正措置についても、事業者が取り得る最善の方法を検討しておかなければならない。なお、是正のための技術的な措置は、前述の予防措置の検討に包含される場合が多く、例えば、アクセスログの取得、バックアップの作成等はこれに当たる。

また、漏洩等が起こったときの情報主体（消費者）への対応、JIPDEC プライバシーマーク事務局･指定機関への対応、マスコミ等への対応等の規定も必要である。

h) **ＣＰ文書、個人情報保護実施記録に関する文書管理の規定**

ＣＰに基づき、個人情報の取扱いが実施されると、さまざまなタイミングで実施記録を確保しておくことが、監査の証拠を確保する意味から必要となる。したがって、実施の記録に関する文書管理のための規定を整備しなければならない。

ステップ 10：ＣＰを文書化する

ＣＰ策定チームは、ＣＰ文書を文書管理規程に基づいて整備し、事業者の決裁権限を持った者により、正式な文書として決済を受ける。

ステップ 11：ＣＰに準じた体制の整備を行う

ＣＰ策定チームは、基本規程、事業者の各部門及び階層における個人情報を保護するための権利及び責任の規定（詳細規程）に基づいた体制の整備を計画し、事業者の代表者に提示する。事業者の代表者は、体制の整備計画に基づいて人事発令等を指示する。同時に、ＣＰに基づく運用の開始時期を定め全従業員に周知する。

体制整備においては、特に監査担当者の位置付けを考慮する必要がある。ＪＩＳにおいては、監査の実施について外部監査か内部監査かについて言及していない。そのため、監査は外部監査または内部監査の何れでも良いが、外部監査のほうが被監査部門（個人情報の取扱いを行っている実施部門）からの独立性がより保たれることから望ましいと考えられる。しかしながら、外部の監査企業に委託する等では費用等の面で困難な場合においては、内部監査によることも問題ない。

内部監査による場合においては、被監査部門との独立性を保つことが重要である。そのために、ＪＩＳでは「公平、かつ、客観的な立場にあり、監査の実施及び報告を行う権限をもつ者」を監査責任者として企業の代表者が指名しなければならないとしている。

ステップ 12：ＣＰを周知するための研修を実施する

ＣＰ策定チームは、作業スケジュールに準じてＣＰを事業者の全従業員に周知させるために研修を行うように研修担当者に指示する。

研修担当者は、研修計画の基づき、ＣＰ策定チームの協力を得て研修を実施する。研修後は研修効果の確認を行うと共に研修記録表に記録し、次回以降の研修に反映する資料とすること。

ステップ 13：ＣＰの運用状況を監査する

監査担当者は、ＣＰ適用後一定期間を経過した時点で、ＣＰ、体制、個人情報保護の状況について点検し評価する。

ここでの監査は、ＣＰ適用後に効果的な運用ができる体制及びＣＰとなっているかについて確認するために実施する。

評価の結果は、監査報告書に取りまとめ事業者の代表者に報告する。また、ＣＰ策定チームに対しても監査結果を報告し、事業者の代表者の見直し指示を受けて必要な改善を行うように指示する。

ステップ 14：ＣＰの改善を実施する

ＣＰ策定チームは、監査の結果を受けて出された事業者の代表者による見直し指示に従いＣＰの改善を実施する。

必要な改善措置の後、ＣＰ文書に改善内容を反映し、また、改善の内容、改善日を改善履歴として記録すること。

以上

参考１：基本規程策定のチェックリスト

個人情報を特定する手順が規定されているか？

ＣＰの計画段階では、事業者は現段階で自ら保有するすべての個人情報を特定することが必要であるが、ＣＰの策定以降においても新たに発生する業務やプロジェクト等に対応する必要から、個人情報を特定するための手順を確立しておくことが求められる。

したがって、「新たな業務やプロジェクト等の発生時には、必ず個人情報の特定手順を定めた規程に従って個人情報を特定し当該ＣＰに則った運用をすべきか判断する。」等の規定が必要である。

個人情報に関するリスクを明確にする手順が規定されているか？

新たに特定された個人情報に関して、その取扱い経路における保管の形態等から、不正アクセス、漏洩、改ざん、破壊等のリスクを認識してリスクの顕在化防止に努めなければならない。

そのために、個人情報に関するリスクを明確にする手順を定めた規定が必要である。

法令及びその他の規範を特定する手順が規定されているか？

事業者は、自社の個人情報の取扱いに係る業務に関する法令やその他の規範がある場合は、それに準じることが求められる。

そのために、法令及びその他の規範を特定し、かつそれを参照できる手順を定めた規定が必要である。

個人情報の保護のための体制及び責任が明確になっているか？

コンプライアンス・プログラムを効果的に実施するためには運用体制（役割、責任及び権限）の確立と資源を確保しなければならない。

そのために、ＣＰ運用体制、資源の確保に関する事項を明確に定め、かつ、個人情報に関連のある業務にかかわる役員及び従業員に周知しなければならない。

個人情報の収集に関する原則は定められているか？

個人情報の収集は、ＪＩＳの原則に従って行わなければならない。

したがって、基本規程には

・収集の原則、
・収集方法の制限、
・特定の機微な情報の収集禁止、
・直接収集の場合の措置、
・間接収集の場合の措置

に関するＪＩＳに準拠した事項が規定されていなければならない。

個人情報の利用及び提供に関する原則は定められているか？

個人情報の利用及び提供は、ＪＩＳの原則に従って行わなければならない。
したがって、基本規程には
・利用及び提供の原則、
・収集目的外の利用及び提供の措置、
に関するＪＩＳに準拠した事項が規定されていなければならない。

個人情報の適正管理義務に関する原則は定められているか？

個人情報の管理は、ＪＩＳの原則に従って行わなければならない。
したがって、基本規程には
・個人情報の正確性の確保、
・個人情報の安全性の確保、
・個人情報の委託処理の措置、
に関するＪＩＳに準拠した事項が規定されていなければならない。

個人情報に関する情報主体の権利への対応原則は定められているか？

個人情報に関する情報主体の権利に対する措置は、ＪＩＳの原則に従って行わなければならない。
したがって、基本規程には
・情報主体の権利への措置、
・個人情報の利用、提供の拒否権への措置
に関するＪＩＳに準拠した事項が規定されていなければならない。

従業員の教育・訓練に関する措置は規定されているか？

事業者は、ＣＰの内容について全従業員（役員、従業員、臨時要員等）に理解させて個人情報の取扱いがＣＰと逸脱しないようにしなければならない。
そのため、適切な教育を行う事に関する事項を定めなくてはならない。

苦情及び相談に関する措置は規定されているか？

事業者が自社の個人情報及びＣＰに関する情報主体からの苦情及び相談に真摯に対応することは事業者の務めである。
そのため、苦情及び相談に関する措置について規定しなければならない。

コンプライアンス・プログラム文書の管理に関する措置が規定されているか？

事業者は、ＣＰ文書を管理し、維持していかなければならない。
そのため、ＣＰ文書の管理及び維持のために必要な措置を規定しなければならない。

監査に関する措置が規定されているか？

事業者は、ＣＰがＪＩＳと合致していること、及びその運用状況を定期的に監査しなければならない。
そのために、ＣＰ及びその運用状況の監査実施に関する事項について規定しなければならない。

事業者の代表者によるＣＰの見直し関する措置が規定されているか？

ＣＰは、監査報告書及びその他の経営環境などに照らして、最適な状況に維持されなければならない。
そのために、ＣＰの見直しに関する措置について規定しなければならない。

参考２：個人情報保護に関する監査規程モデル

（目　的）
第１条　この規程は、当社の個人情報保護に関するコンプライアンス・プログラムに関する監査を実施するための基本的事項を定め、個人情報保護の向上に寄与することを目的とする。

（用語の定義）
第２条　この規程において次の各号に掲げる用語は、次に定めるところによる。
（１）「監査人」とは、監査部門に所属し、個人情報保護に関する監査業務を担当する者をいう。
（２）「被監査部門」とは、個人情報保護に関するコンプライアンス･プログラムに基づき個人情報の取扱いを行っている部門等で監査を受ける組織をいう。
（３）「指摘事項」とは、監査の結果、監査人が問題があると判断した事項をいう。
（４）「改善勧告」とは、指摘事項のうち、被監査部門に対して改善を要すると判断した事項をいう。その内、緊急性を要する事項は緊急改善、その他の事項は通常改善として勧告する。

（対象範囲）
第３条　監査の対象は、次のとおりとする。
（１）情報システム：個人情報を処理するする全ての情報システム
（２）業務：コンプライアンス･プログラムに基づいて個人情報を取扱う全業務
（３）部門：コンプライアンス･プログラムに基づいて個人情報を取扱う関連部門

（監査時期）
第４条　監査の実施時期は、次のとおりとする。
（１）コンプライアンス･プログラムの修正等の実施に即して適時行うこと。
（２）運用状況の監査は、一定の期間ごとに行うこと。
（３）その他必要に応じて随時監査を行うこと。

（実施体制）
第５条　監査責任者は、監査に係る事項を主管する。
２　監査責任者は、監査人による実施体制を編成することができる。

（実施計画）
第６条　監査責任者は、年度始めに監査の実施について基本計画書をとりまとめ、代表者（社長）の承認を受けなければならない。ただし、監査責任者が緊急に監査の必要性があると判断した場合はこの限りでない。
２　監査責任者は、基本計画書の写を年度始めに各部門の長に配布しなければならない。
３　監査人は、基本計画書に記載された個別の監査対象ごとに、個別計画書を作成しなければならない。
４　基本計画に記載されていない監査対象で、監査責任者が緊急にシステム監査の必要性があると判断した場合も、個別計画書を作成しなければならない。

（監査通知）
第７条　監査責任者は、個別計画書に基づく監査の実施にあたっては、＿＿＿以上前に被監査部門の長へ文書で通知しなければならない。ただし、緊急に監査の必要性があると判断した場合はこの限りでない。

（監査実施）
第８条　監査人は、個別計画書に基づき、予備調査、本調査および評価・結論の手順により実施しなければならない。
２　予備調査では、監査対象の現状を踏まえた問題点を把握すること。
３　本調査では、監査目的に即し、評価の根拠となる具体的な資料を収集すること。
４　評価・結論にあたっては、評価の尺度を明らかにすること。

（講評会）
第９条　監査人は、監査報告書を作成する前に被監査部門の関係者と講評会を開催しなければならない。
２　監査人は講評会において、問題点についての事実の誤認がないことを確認しなければならない。

（監査報告）
第 10 条　監査人は、監査報告書を監査責任者に提出しなければならない。
２　監査責任者は、監査報告書を経営者に提出し、報告するとともに、その写を被監査部門の長に配布しなければならない。
３　監査責任者は、監査報告書に基づき、関係者を含めた報告会を開催しなければならない。

（監査人の責務）
第 11 条　監査人は、監査実施後、速やかに監査報告書を作成しなければならない。
２　監査人は、指摘事項、改善勧告がある場合は、監査報告書に記載しなければならない。
３　監査人は、自らの判断に対する根拠を明らかにしなければならない。
４　監査人は、改善勧告に基づき経営者が被監査部門に改善を命令した事項については、その実施状況を評価し、改善の実現に向けて被監査部門を支援しなければならない。

（監査人の権限）
第 12 条　監査人は、個別計画に基づく監査の実施にあたって被監査部門へ資料の提出を求めることができる。
２　監査人は、改善勧告に基づき経営者が被監査部門に改善を命令した事項については、その実施状況の報告を求めることができる。

（守秘義務）
第 13 条　監査責任者及び監査人は、正当な理由なく監査の実施により知り得た秘密を漏らし、ま

たは不当な目的に使用してはならない。
２　前項の規定は、その職務を離れた後も存続する。

（倫　理）
第 14 条　監査人は、客観的な評価者としての立場を堅持しなければならない。
２　監査人は、職務上の倫理的要請を自覚し、的確かつ誠実に監査を実践しなければならない。

（外部委託）
第 15 条　監査を外部の監査企業等に委託する場合は、契約書に、監査方法、守秘義務等の条項を定めなければならない。

付　則
この規程は平成　年　月　日から施行する。