個人情報保護基本規程

株式会社＊＊＊＊＊

制　定　　平成２９年６月１２日　初　版
改　定　　平成２９年９月　１日　第二版
改　訂　　平成３１年４月１１日　第三版
改　訂　　令和　元年９月１７日　第四版
改　訂　　令和　２年７月１０日　第五版

代表者承認	個人情報保護管理者

目次

個人情報保護基本規程

本文編

1 適用範囲

この個人情報保護基本規程は、＊＊＊＊＊＊＊＊＊（以下「当社」という。）が取り扱う全ての個人情報の適切な保護ための個人情報保護マネジメントシステムを確立し、実施し、維持しかつ改善する事を目的とする。

２　この個人情報保護基本規程は、当社が事業の用に供する全ての個人情報を対象とし、当社の従業者「役員、正社員、パートタイマー、アルバイトを含む」全てに適用する。

2 引用規格

3 用語及び定義

この個人情報保護基本規程において用いる主な用語及び定義は、「個人情報の保護に関する法律」、「個人情報の保護に関する法律施行令」及び「JIS Q 15001」による。

4 組織の状況

4.1 組織及びその状況の理解

当社は、当社の目的に関連し、かつ、その個人情報保護マネジメントシステムの意図した成果を達成する当社の能力に影響を与える、外部及び内部の課題を決定する。

4.2 利害関係者のニーズ及び期待の理解

当社は、次の事項を決定する。

a）個人情報保護マネジメントシステムに関連する利害関係者

b）その利害関係者の、個人情報保護に関連する要求事項

注記：利害関係者の要求事項には、法的及び規制の要求事項並びに契約上の義務を含めてもよい。

4.3 個人情報保護マネジメントシステムの適用範囲の決定

当社は、個人情報保護マネジメントシステムの適用範囲を定めるために、その協会及び適用可能性を決定する。

この適用範囲を決定するとき、当社は、次の事項を考慮する。

a） 4.1 に規定する外部及び内部の課題

b） 4.2 に規定する要求事項

c） 当社が実施する活動と他の組織が実施する活動との間のインターフェース及び依存関係

個人情報保護マネジメントシステムの適用範囲は、文書化した情報として利用可能な状

態にしておく。

4.4 個人情報保護マネジメントシステム

当社は、JIS Q 15001 の要求事項に従って、個人情報保護マネジメントシステムを確立し、実施し、維持し、かつ、継続的に改善する。

5 リーダーシップ

5.1 リーダーシップ及びコミットメント

トップマネジメントは、次に示す事項によって、個人情報保護マネジメントシステムに関するリーダーシップ及びコミットメントを実証する。

a) 内部向け個人情報保護方針及び個人情報保護目的を確立し，それらが組織の戦略的な方向性と両立することを確実にする。

b) 当社のプロセスへの個人情報保護マネジメントシステム要求事項の統合を確実にする。

c) 個人情報保護マネジメントシステムに必要な資源が利用可能であることを確実にする。

d) 有効な個人情報保護マネジメント及び個人情報保護マネジメントシステム要求事項への適合の重要性を利害関係者に伝達する。

e) 個人情報保護マネジメントシステムがその意図した成果を達成することを確実にする。

f) 個人情報保護マネジメントシステムの有効性に寄与するよう人々を指揮し、支援する。

g) 継続的改善を促進する。

h) その他の関連する管理層がその責任の領域においてリーダーシップを実証するよう、管理層の役割を支援する。

5.2 方針

5.2.1 内部向け個人情報保護方針

トップマネジメントは，次の事項を満たす内部向け個人情報保護方針を確立する。

a) 組織の目的に対して適切である。

b) 個人情報保護目的（6.2 参照）を含むか，又は個人情報保護目的の設定のための枠組みを示す。

c) 個人情報保護に関連する適用される要求事項を満たすことへのコミットメントを含む。

d) 個人情報保護マネジメントシステムの継続的改善へのコミットメントを含む。

内部向け個人情報保護方針は，次に示す事項を満たさなければならない。

e) 文書化した情報として利用可能である。

f) 組織内に伝達する。

g) 必要に応じて，利害関係者が入手可能である。

5.2.2 外部向け個人情報保護方針

トップマネジメントは、次の事項を満たす外部向け個人情報保護方針を文書化し，一般の人が知り得るようにしなければならない。

a) 5.2.1 で確立した内部向け個人情報保護方針に対して矛盾しない。

5.3 組織の役割，責任及び権限

トップマネジメントは、個人情報保護に関連する役割に対して、責任及び権限を割り当て、利害関係者に伝達することを確実にしなければならない。

トップマネジメントは、次の事項に対して、責任及び権限を割り当てなければならない。

a) 個人情報保護マネジメントシステムが、この規格の要求事項に適合することを確実にする。

b) 個人情報保護マネジメントシステムのパフォーマンスをトップマネジメントに報告する。

注記：トップマネジメントは、個人情報保護マネジメントシステムのパフォーマンスを当社内に報告する責任及び権限を割り当ててもよい。

6 計画

6.1 リスク及び機会に対処する活動

6.1.1 一般

個人情報保護マネジメントシステムの計画を策定するとき、当社は、4.1 に規定する課題及び 4.2 に規定する要求事項を考慮し、次の事項のために対処する必要があるリスク及び機会を決定する。

a) 個人情報保護マネジメントシステムが、その意図した成果を達成できることを確実にする。

b) 望ましくない影響を防止又は低減する。

c) 継続的改善を達成する。

当社は，次の事項を計画する。

d) 上記によって決定したリスク及び機会に対処する活動

e) 次の事項を行う方法

1) その活動の個人情報保護マネジメントシステムプロセスへの統合及び実施

2) その活動の有効性の評価

6.1.2 個人情報保護リスクアセスメント

当社は、次の事項を行う個人情報保護リスクアセスメントのプロセスを定め、適用する。

a) 次を含む個人情報保護のリスク基準を確立し，維持する。

1) リスク受容基準

2) 個人情報保護リスクアセスメントを実施するための基準

b) 繰り返し実施した個人情報保護リスクアセスメントに，一貫性及び妥当性があり，かつ，比較可能な結果を生み出すことを確実にする。

c) 次によって個人情報保護リスクを特定する。

1) 個人情報保護マネジメントシステムの適用範囲内における個人情報の不適切な取扱いに伴うリスクを特定するために，個人情報保護リスクアセスメントのプロセスを適用する。

2）これらのリスク所有者を特定する。

d）次によって個人情報保護リスクを分析する。

1）6.1.2 c）1）で特定されたリスクが実際に生じた場合に起こり得る結果についてアセスメントを行う。

2）6.1.2 c）1）で特定されたリスクの現実的な起こりやすさについてアセスメントを行う。

3）リスクレベル（リスクの大きさ）を決定する。

e）次によって個人情報保護リスクを評価する。

1）リスク分析の結果と 6.1.2 a）で確立したリスク基準とを比較する。

2）リスク対応のために，分析したリスクの優先順位付けを行う。

当社は、個人情報保護リスクアセスメントのプロセスについての文書化した情報を保持する。

6.1.3 個人情報保護リスク対応

当社は，次の事項を行うために，個人情報保護リスク対応のプロセスを定め，適用する。

a）リスクアセスメントの結果を考慮して、適切な個人情報保護リスク対応の選択肢を選定する。

b）選定した個人情報保護リスク対応の選択肢の実施に必要な全ての管理策を決定する。

注記：当社は、必要な管理策を設計するか、又は任意の情報源の中から管理策を特定することができる。

c）6.1.3 b）で決定した管理策を附属書 A に示す管理策と比較し，必要な管理策が見落とされていないことを検証する。

注記：付属書 A は、管理目的及び管理策の包括的なリストである。JIS Q 15001 の利用者は、必要な管理策の見落としが無いことを確実にするために、付属書 A を参照する。

注記：管理目的は、管理策に暗に含まれている。付属書 A に規定した管理項目及び管理策は、全てを網羅していないため、追加の管理目的及び管理策が必要となる場合がある。

d）個人情報保護リスク対応計画を策定する。

e）個人情報保護リスク対応計画及び残留している個人情報保護リスクの受容について，リスク所有者の承認を得る。

当社は、個人情報保護リスク対応のプロセスについての文書化した情報を保持する。

注記：JIS Q 15001 の個人情報保護リスクアセスメント及びリスク対応のプロセスは、JIS Q 31000 に規定する原則及び一般的な指針と整合している。

6.2 個人情報保護目的及びそれを達成するための計画策定

当社は、関連する部門及び階層において、個人情報保護目的を確立しなければならない。

個人情報保護目的は，次の事項を満たさなければならない。

a）内部向け個人情報保護方針と整合している。

b）（実行可能な場合）測定可能である。

c）適用される個人情報保護要求事項、並びにリスクアセスメント及びリスク対応の結果を考慮に入れる。
d）伝達する。
e）必要に応じて、更新する。

当社は、個人情報保護目的に関する文書化した情報を保持しなければならない。
当社は、個人情報保護目的をどのように達成するかについて計画するとき、次の事項を決定する。
f）実施事項
g）必要な資源
h）責任者
i）達成期限
j）結果の評価方法

7 支援

7.1 資源

当社は、個人情報保護マネジメントシステムの確立、実施、維持及び継続的改善に必要な資源を決定し、提供する。

7.2 力量

当社は、次の事項を行う。
a） 組織の個人情報保護パフォーマンスに影響を与える業務をその管理下で行う人々に必要な力量を決定する。
b）適切な教育、訓練又は経験に基づいて、それらの人々が力量を備えていることを確実にする。
c）該当する場合には、必ず、必要な力量を身につけるための処置をとり、とった処置の有効性を評価する。
d）力量の証拠として、適切な文書化した情報を保持する。
注記：適用される処置には、例えば、現在雇用している人々に対する、教育訓練の提供、指導の実施、配置転換の実施などがあり、また、力量を備えた人々の雇用、そうした人々との契約締結などもある。

7.3 認識

当社の管理下で働く人々は、次の事項に関して認識をもたなければならない。
a）内部向け個人情報保護方針及び外部向け個人情報保護方針
b）個人情報保護パフォーマンスの向上によって得られる便益を含む，個人情報保護マネジメントシステムの有効性に対する自らの貢献
c）個人情報保護マネジメントシステム要求事項に適合しないことの意味

7.4 コミュニケーション

当社は，次の事項を含め、個人情報保護マネジメントシステムに関連する内部及び外部のコミュニケーションを実施する必要性を決定する。

a）コミュニケーションの内容（何を伝達するか。）

b）コミュニケーションの実施時期

c）コミュニケーションの対象者

d）コミュニケーションの実施者

e）コミュニケーションの実施プロセス

7.5 文書化した情報

7.5.1 一般

当社の個人情報保護マネジメントシステムは，次の事項を含む。

a）JIS Q 15001 が要求する文書化した情報

b）個人情報保護マネジメントシステムの有効性のために必要であると組織が決定した、文書化した情報

注記 個人情報保護マネジメントシステムのための文書化した情報の程度は，次のような理由によって，それぞれの組織で異なる場合がある。

1）組織の規模，並びに活動，プロセス，製品及びサービスの種類

2）プロセス及びその相互作用の複雑さ

3）個々人の力量

7.5.2 作成及び更新

文書化した情報を作成及び更新する際、当社は、次の事項を確実にする。

a）適切な識別及び記述（例えば，タイトル，日付，作成者，参照番号）

b）適切な形式（例えば，言語，ソフトウェアの版，図表）及び媒体（例えば，紙，電子媒体）c）適切性及び妥当性に関する，適切なレビュー及び承認

7.5.3 文書化した情報の管理

個人情報保護マネジメントシステム及びこの規格で要求されている文書化した情報は、次の事項を確実にするために、管理する。

a） 文書化した情報が，必要な時に，必要な所で，入手可能かつ利用に適した状態である。

b）文書化した情報が十分に保護されている（例えば，機密性の喪失，不適切な使用及び完全性の喪失からの保護）。

文書化した情報の管理に当たって、当社は、該当する場合には、必ず、次の行動に取り組む。

c）配付，アクセス，検索及び利用

d）読みやすさが保たれることを含む，保管及び保存

e）変更の管理（例えば，版の管理）

f）保持及び廃棄

個人情報保護マネジメントシステムの計画及び運用のために組織が必要と決定した外部

からの文書化した情報は、必要に応じて、特定し、管理する。

注記：アクセスとは、文書化した情報の閲覧だけの許可に関する決定、文書化した情報の閲覧及び変更の許可及び権限に関する決定、などを意味する。

8 運用

8.1 運用の計画及び管理

当社は、個人情報保護要求事項を満たすため、及び6.1 で決定した活動を実施するために必要なプロセスを計画し、実施し、かつ、管理する。また、当社は，6.2 で決定した個人情報保護目的を達成するための計画を実施する。

当社は、プロセスが計画通りに実施されたという確信をもつために必要な程度の、文書化した情報を保持しなければならない。

当社は、計画した変更を管理し、意図しない変更によって生じた結果をレビューし、必要に応じて、有害な影響を軽減する処置をとる。

当社は、外部委託したプロセスが決定され、かつ、管理されていることを確実にする。

8.2 個人情報保護リスクアセスメント

当社は、あらかじめ定めた間隔で、又は重大な変更が提案されたか若しくは重大な変化が生じた場合に、6.1.2 a）で確立した基準を考慮して，個人情報保護リスクアセスメントを実施する。

当社は、個人情報保護リスクアセスメント結果の文書化した情報を保持する。

8.3 個人情報保護リスク対応

当社は、個人情報保護リスク対応計画を実施する。

当社は、個人情報保護リスク対応結果の文書化した情報を保持する。

9 パフォーマンス評価

9.1 監視，測定，分析及び評価

当社は、個人情報保護パフォーマンス及び個人情報保護マネジメントシステムの有効性を評価する。

当社は、次の事項を決定する。

a）必要とされる監視及び測定の対象。これには、個人情報保護プロセス及び管理策を含む。

b）該当する場合には、必ず、妥当な結果を確実にするための、監視、測定、分析及び評価の方法。

注記：選定した方法は、妥当と考えられる、比較可能で再現可能な結果を生み出すことが望ましい。

c）監視及び測定の実施時期

d）監視及び測定の実施者

e）監視及び測定の結果の、分析及び評価の時期

f）監視及び測定の結果の、分析及び評価の実施者

当社は、監視及び測定の結果の証拠として、適切な文書化した情報を保持する。

9.2 内部監査

当社は、個人情報保護マネジメントシステムが次の状況にあるか否かに関する情報を提供するために、あらかじめ定めた間隔で内部監査を実施する。

a) 次の事項に適合している。

1) 個人情報保護マネジメントシステムに関して、組織自体が規定した要求事項

2) この規格の要求事項

b) 有効に実施され，維持されている。

当社は、次に示す事項を行う。

c) 頻度、方法、責任及び計画に関する要求事項及び報告を含む、監査プログラムの計画、確立、実施及び維持。監査プログラムは、関連するプロセスの重要性及び前回までの監査の結果を考慮に入れる。

d) 各監査について、監査基準及び監査範囲を明確にする。

e) 監査プロセスの客観性及び公平性を確保する監査員を選定し、監査を実施する。

f) 監査の結果を関連する管理層に報告することを確実にする。

g) 監査プログラム及び監査結果の証拠として、文書化した情報を保持する。

9.3 マネジメントレビュー

トップマネジメントは，組織の個人情報保護マネジメントシステムが、引き続き、適切、妥当かつ有効であることを確実にするために、あらかじめ定めた間隔で、個人情報保護マネジメントシステムをレビューする。

マネジメントレビューは、次の事項を考慮する。

a) 前回までのマネジメントレビューの結果，とった処置の状況

b) 個人情報保護マネジメントシステムに関連する外部及び内部の課題の変化

c) 次に示す傾向を含めた、個人情報保護パフォーマンスに関するフィードバック

1) 不適合及び是正処置

2) 監視及び測定の結果

3) 監査結果

4) 個人情報保護目的の達成

d) 利害関係者からのフィードバック

e) リスクアセスメントの結果及びリスク対応計画の状況

f) 継続的改善の機会

マネジメントレビューからのアウトプットには、継続的改善の機会、及び個人情報保護マネジメントシステムのあらゆる変更の必要性に関する決定を含める。当社は、マネジメントレビューの結果の証拠として、文書化した情報を保持する。

10 改善

10.1 不適合及び是正処置

不適合が発生した場合、当社は、次の事項を行う。

a) その不適合に対処し、該当する場合には、必ず、次の事項を行う。

1）その不適合を管理し、修正するための処置をとる。
2）その不適合によって起こった結果に対処する。
b）その不適合が再発しないように又は他のところで発生しないようにするため、次の事項によって、その不適合の原因を除去するための処置をとる必要性を評価する。
1）その不適合をレビューする。
2）その不適合の原因を明確にする。
3）類似の不適合の有無、又はそれが発生する可能性を明確にする。
c）必要な処置を実施する。
d）とった全ての是正処置の有効性をレビューする。
e）必要な場合には、個人情報保護マネジメントシステムの変更を行う。
是正処置は，検出された不適合のもつ影響に応じたものでなければならない。
当社は、次に示す事項の証拠として、文書化した情報を保持する。
f）不適合の性質及びとった処置
g）是正処置の結果

10.2 継続的改善

当社は、個人情報保護マネジメントシステムの適切性，妥当性及び有効性を継続的に改善する。

付属書 A 編

A.3　管理目的及び管理策

A.3.1　一般

目的　個人情報保護マネジメントシステムの運用を行うため。

A.3.1.1　一般

この「個人情報保護基本規程」に規定する A.3.2 から A.3.8 は、トップマネジメントによって権限を与えられた個人情報保護管理者によって承認される。

具体的には、新規個人情報の取得においては「新規個人情報取得申請書」を、個人情報の取扱いに変化があった場合は「個人情報取扱申請書」を、保有個人データに対する開示や利用目的通知等の請求があった場合は「開示等請求書」を用いる。

また、各種例外事項が発生する場合は「例外事項取扱申請書」を用いる。

個人情報の取得にあたって同意が必要な場合は、あらかじめ「個人情報の取り扱いについて」などの書面を用意しておき、本人に手渡して同意を得る。ウェブから取得する場合は、「個人情報の取り扱いについて」を明示して、同意を得る構成とする。

A.3.2 個人情報保護方針

目的　個人情報保護の理念を明確にし、公表するため。

A.3.2.1　内部向け個人情報保護方針

トップマネジメントは、文書化した情報として利用可能である内部向け個人情報保護方針には次の事項を含める。

a)　事業の内容及び規模を考慮した適切な個人情報の取得、利用及び提供に関すること［特定された利用目的の達成に必要な範囲を超えた個人情報の取扱い（以下、“目的外利用”という。）を行わないこと及びそのための措置を講じることを含む。］。
b)　個人情報の取り扱いに関する法令、国が定める指針及びその他の規範を遵守すること。
c)　個人情報の漏えい、滅失又はき損の防止並び是正に関すること。
d)　苦情及び相談への対応に関すること。
e)　個人情報保護マネジメントシステムの継続的改善に関すること。
f)　トップマネジメントの氏名

トップマネジメントは、内部向け個人情報保護方針を文書化した情報を、当社内に掲示すると共に、当社の公開ウェブサイト及びイントラネット上に掲載して組織内に伝達し、必要に応じて利害関係者が入手可能な措置を講じる。

A.3.2.2　外部向け個人情報保護方針

トップマネジメントは、外部向け個人情報保護方針を文書化した情報には、前項に規定す

る内部向け個人情報保護方針の事項に加えて、次の事項も明記する。

a） 制定年月日及び最終改定年月日

b） 外部向け個人情報保護方針の内容についての問い合わせ先

トップマネジメントは、外部向け個人情報保護方針を文書化した情報について、一般の人が知りえるようにするための一般の人が入手可能な措置として、当社の公開ウェブサイトに掲載する。

A.3.3　計画

目的　個人情報の取扱いに関する計画を策定するため。

A.3.3.1　個人情報の特定

当社は、自らの事業の用に供するすべての個人情報を特定するための手順を確立し、かつ、維持する。

当社は、個人情報の項目、利用目的、保管場所、保管方法、アクセス権を有する者、利用期限、保管期限などを記載した、個人情報を管理するための台帳を整備するとともに、当該台帳の内容を少なくとも年一回、適宜に確認し、最新の状態で維持されるようにしなければならない。

当社は、特定した個人情報については、個人データと同様に取り扱わなければならない。

２　個人情報を特定し、かつ、維持するための手順を以下に定める。

（１）　個人情報の特定

なんらかの新規の種類の情報を取得する予定がある場合、または、すでに行っている事業で扱う情報の中に個人情報が含まれるかどうかを確認する。取得した情報の中に個人情報が含まれる場合は、担当者が「新規個人情報登録申請書」をチェックリストとしてチェックし、必要事項を記載する。「新規個人情報登録申請書」では、当該個人情報の項目、利用目的、保管場所、保管方法、アクセス権を有する者、利用期限、保管期限、開示対象かどうか、本規程に定める例外事項の有無、廃棄方法等について明記する。

（２）　「個人情報管理台帳」への登録と承認

担当者は、当該「新規個人情報登録申請書」を個人情報保護管理者に提出する。個人情報保護管理者は、記載事項について担当者とともに確認し、当該特定された個人情報の取得を承認し、その必要事項を「個人情報管理台帳」に記載する。

（３）　「個人情報管理台帳」の更新

個人情報保護管理者は、「個人情報管理台帳」に転記した事項について変化があった場合は随時「個人情報管理台帳」を更新する。当社における個人情報については、毎年１２月に見直しを実施する。

A.3.3.2　法令、国が定める指針及びその他の規範

当社は、個人情報の取り扱いに関する法令、国が定める指針その他の規範を特定し参照できる手順を確立し、かつ、維持する。

２　そのための手順として、実施担当者、調査時期、結果の報告、規程への反映及び改訂結果の周知について、以下のように定める。

（１）　実施担当者

法令、国が定める指針その他の規範に関する調査及び特定の実施担当者は、個人情報保護管理者が指名した文書管理責任者とする。

（２）　調査時期

法令、国が定める指針その他の規範に関する調査及び特定の時期は、新設や改廃などの情報を入手したとき及び１２月とする。新設や改廃などの情報を入手する手段として、実施担当者は、以下の内容を記した「法令、国が定める指針その他の規範一覧」を作成、個人情報保護管理者が承認する。

・適用される“法令、国が定める指針その他の規範”の名称

・適用される“法令、国が定める指針その他の規範”の制定日及び最終改定日

（３）　結果の報告

実施担当者は、上記の結果、新たな法令や規範などの特定、又は改定・変更があった場合には、個人情報保護管理者に報告を行い、「法令、国が定める指針その他の規範一覧」を更新する。

（４）　規程への反映

報告を受けた個人情報保護管理者は、新たに特定、又は改定･変更された法令、国が定める指針その他の規範の条文と当社の規程を照らし合わせ、不整合があるかどうか確認する。不整合があった場合、個人情報保護管理者は、該当する当社の規程の改定を行う。

（５）　改訂結果の周知

改定の結果を、従業者に周知すると共に、特定された「法令、国が定める指針その他の規範一覧」を、社内イントラネット内に掲示する等して、従業者が閲覧可能な状態に置く。

A.3.3.3　リスクアセスメント及びリスク対策

当社は、A.3.3.1 によって特定した個人情報について、利用目的の達成に必要な範囲を超えた利用を行わないため、必要な対策を講じる手順を確立し、かつ、維持する。

当社は、A.3.3.1 によって特定した個人情報の取扱いについて、個人情報保護リスクを特定し、分析し、必要な対策を講じる手順を確立し、かつ、維持しなければならない。

当社は、現状で実施し得る対策を講じた上で、未対応部分を残留リスクとして把握し、管理する。

当社は、個人情報保護リスクの特定、分析及び講じた個人情報保護対策を少なくとも年一

回、適宜に見直す。

２　そのための手順を以下に定める。

（１）　リスク分析、対応計画

個人情報保護管理者は、調査担当を任命し、「個人情報管理台帳」に特定された全ての個人情報類型を「リスク管理表」に記載し、その類型ごとに、個人情報のライフサイクルに対応したリスク内容を記載して分析し、その対策としてリスク対応方針、優先順位、具体的な対応方法、対応計画を記入する。リスク対策は、トップマネジメントの承認を得る。

（２）　リスク対策と残留リスクの把握

「リスク管理表」に「個人情報管理台帳」の類型ごとに対応計画に沿って対応し、対応結果を記入する。対応するに当たって、参照あるいは修正した関連規程を記入する。また、対応を行ってもなお残る残留リスクを記入し、許容する理由も明記しておく。

（３）　見直し

個人情報保護管理者は、「リスク管理表」に記載された内容を定期的に見直す。その時期は毎年１２月とする。また、個人情報保護管理者が必要と認めたときは、随時行う。

A.3.3.4　資源、役割、責任及び権限

トップマネジメントは、少なくとも、次の責任及び権限を割り当てなければならない。

a)　個人情報保護管理者

b)　個人情報保護監査責任者

トップマネジメントは、JIS Q15001 の内容を理解し実践する能力のある個人情報保護管理者を当社内部に属する者の中から指名し、個人情報保護マネジメントシステムの実施及び運用に関する責任及び権限を他の責任にかかわりなく与え、業務を行わせなければならない。

個人情報保護管理者は、個人情報保護マネジメントシステムの見直し及び改善の基礎として、トップマネジメントに個人情報保護マネジメントシステムの運用状況を報告しなければならない。

トップマネジメントは、公平、かつ、客観的な立場にある個人情報保護監査責任者を当社内部に属する者の中から指名し、監査の実施及び報告を行う責任及び権限を他の責任にかかわりなく与え、業務を行わせなければならない。

個人情報保護監査責任者は、監査を指揮し、監査報告書を作成し、トップマネジメントに報告しなければならない。監査員の選定及び監査の実施においては、監査の客観性及び公平性を確保しなければならない。

個人情報保護監査責任者と個人情報保護管理者とは異なるものでなければならない。

文書管理責任者は、当社の個人情報保護マネジメントシステム関連文書及び記録の維持管理を行わなければならない。

顧客窓口責任者は、苦情・相談及び開示等の要求の受付及び一次対応の実施、苦情・相談及び開示等の要求の個人情報保護管理者への報告を行わせなければならない。

役員を含む全社員は、以下を実施しなければならない。

① 個人情報の重要性の認識。
② 各規程の理解と実行。
③ ルール違反時のペナルティの認識。
④ 監査への協力。
⑤ 作成された記録の適切な管理作成・保管・参照・廃棄。

個人番号事務取扱担当者は、事務取扱担当部門ごとに取得した特定個人情報等を含む書類等（電磁媒体等を含む。）を、当該部門において安全に管理しなければならない。

個人番号事務取扱担当者は、特定個人情報等を取り扱う情報システム及び機器等を適切に管理し、利用権限のない者には使用させてはならない。

個人番号事務取扱担当者は、特定個人情報等の取扱状況を明確にするため、執務記録「特定個人情報取扱記録簿」を作成し、保管状況及び廃棄記録等について適宜管理する。

A.3.3.5　内部規程

当社は、次の事項を含む内部規程を文書化し、かつ、維持する。

a) 個人情報を特定する手順に関する規定：本規程 A.3.3.1
b) 法令、国が定める指針その他の規範の特定、参照及び維持に関する規定：本規程 A.3.3.2
c) 個人情報のリスクアセスメント及びリスク対策の手順に関する規定：本規程 A.3.3.3
d) 当社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に関する規定：本規程 A.3.3.4
e) 緊急事態への準備及び対応に関する規定：本規程 A.3.3.7
f) 個人情報の取得、利用及び提供に関する規定：本規程 A.3.4.2、個人情報取り扱い細則
g) 個人情報の適正管理に関する規定：本規程 A.3.4.3、安全対策規程
h) 本人からの開示等の請求への対応に関する規定：本規程 A.3.4.4
i) 教育などに関する規定：本規程 A.3.4.5
j) 文書化した情報の管理に関する規定：本規程 A.3.5
k) 苦情及び相談への対応に関する規定：本規程 A.3.6
l) 点検に関する規定：本規程 A.3.7、個人情報保護内部監査規程
m) 是正処置に関する規定：本規程 A.3.8
n) マネジメントレビューに関する規定：本規程 A.3.7.3
o) 内部規程の違反に関する罰則の規定：本規程 A.3.4.3.3

当社は、事業の内容に応じて、個人情報保護マネジメントシステムが確実に運用されるように内部規程を改定する。

A.3.3.6　計画策定

当社は、個人情報保護マネジメントシステムを確実に実施するために、少なくとも年一回、次の事項を含めて、必要な計画を立案し、文書化し、かつ、維持する。

a) A.3.4.5 に規定する事項を踏まえた教育実施計画の立案及びその文書化
個人情報保護管理者は、個人情報保護マネジメントシステムを確実に実施するために必要な教育の計画として「年間教育計画表」を期初に策定し、教育を実施する際は、「教育計画兼実施報告書」をもって、トップマネジメント等の承認を得る。

b) A.3.7.2 に規定する事項を踏まえた内部監査実施計画及びその文書化
個人情報保護監査責任者は、個人情報保護マネジメントシステムを確実に実施するために必要な監査の計画として「内部監査計画書」を期初に策定し、トップマネジメントの承認を得る。

A.3.3.7　緊急事態への準備

当社は、緊急事態を特定するための手順、また、特定した緊急事態にどのように対応するかの手順を確立し、実施し、かつ、維持する。

当社は、個人情報保護リスクを考慮し、その影響を最小限とするための手順を確立し、かつ、維持する。

また、当社は、緊急事態が発生した場合に備え、次の事項を含む対応手順を確立し、かつ、維持する。

a) 漏えい、滅失又はき損が発生した個人情報の内容を本人に速やかに通知し、又は本人が容易に知り得る状態に置くこと。

b) 二次被害の防止、類似事案の発生回避などの観点から、可能な限り事実関係、発生原因及び対応策を、遅滞なく公表すること。

c) 事実関係、発生原因及び対応策を関係機関に直ちに報告すること。

２　当社は、上記を確実に行うための手順として、以下を定める。

（１）第三者による情報システムの脆弱性の指摘や個人情報の漏洩事故等、重大と思われる事態が発生したり、発生すると考えられる時、個人情報保護管理者は、直ちに以下のアクションをとる。

・事実や状況を確認する。
・確認した結果が重大と判断される時には、社長ならびに各部の責任者に連絡をとる。
・想定される経済的な不利益及び社会的な信用の失墜、本人への影響などのおそれを考慮し、その影響を最小限とするための対応策を検討し、速やかに実施する。

（２）既に発生した事実に対しては、顧客窓口責任者が、漏えい、滅失又はき損が発生した個人情報の内容をご本人に電話やメールなどで通知するとともに、その他のお客

様からの問い合わせに備える。
（３）進捗状況は、随時関連部署に連絡するとともに、「個人情報に関する事故対応処理記録」に経緯を記録する。
（４）二次被害防止の観点上また類似事案の発生回避のため、可能な範囲で事実関係、発生原因及び対応策について当社ウェブサイト上に公表を行う。
（５）事故の経緯について、事実関係、発生原因及び対応策を、「事故発生時の連絡体制図」に基づき所轄省庁及び関連加入団体「個人情報保護委員会」へ報告する。
（６）事故発生時の連絡及び報告の為に「事故発生時の連絡体制図」を準備する。
（７）「特定個人情報の漏えいその他の特定個人情報の安全確保に係わる重大な事態の報告に関する規則」（平成 27 年特定個人情報保護委員会規則第 5 号）第 2 条各号に規定されている特定個人情報に係わる重大な事態が発生した場合は、報告の要否を判断の上、「個人情報保護委員会」に報告する。
※「個人情報保護委員会」の報告先については、「事故発生時の連絡体制図」を参照のこと。

A.3.4　実施及び運用

目的　運用段階において個人情報の取り扱いを行うため。

A.3.4.1　運用手順

当社は、個人情報保護マネジメントシステムが確実に実施するために、運用の手順を明確にする。

A.3.4.2 取得、利用及び提供に関する原則

A.3.4.2.1　利用目的の特定

当社は、個人情報を取り扱うに当たっては、その利用目的をできる限り特定し、その目的の達成に必要な範囲内において行う。

当社は、利用目的の特定に当たっては、取得した情報の利用及び提供によって本人の受ける影響を予測できるように、利用及び提供の範囲を可能な限り具体的に明らかにするよう配慮する。

２　“利用目的”は、その個人情報の取扱担当者が提案し、それを個人情報保護管理者が承認した上で、「個人情報管理台帳」に記して管理する。

A.3.4.2.2　適正な取得

当社は、適法かつ公正な手段によって個人情報を取得する。

２　個人情報の取扱いの全部又は一部を委託された場合、又は提供された場合、委託元又は提供元が個人情報保護法及び各種ガイドラインに沿って適切に個人情報を取得して取り扱っていることを「個人情報取扱申請書」をもって確認する。

A.3.4.2.3　要配慮個人情報

当社は、新たに要配慮個人情報を取得する場合、あらかじめ書面による本人の同意を得ないで、要配慮個人情報を取得しない。ただし、次に掲げるいずれかに該当する場合には、書面による本人の同意を得ることを要しない。

a) 法令に基づく場合。
b) 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。
c) 公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。
d) 国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることによって当該事務の遂行に支障を及ぼすおそれがあるとき。
e) その他、個人情報取扱事業者の義務などの適用除外とされている者及び個人情報保護委員会規則で定めた者によって公開された要配慮個人情報、又は政令で定められた要配慮個人情報であるとき。

当社は、要配慮個人情報の利用又は提供についても、前項と同様に実施する。さらに、要配慮個人情報のデータの提供についても、同様に実施する。

A.3.4.2.4　個人情報を取得した場合の措置

当社は、個人情報を取得した場合は、あらかじめ,その利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知するか、又は公表する。ただし、次に掲げるいずれかに該当する場合には、本人への利用目的の通知又は公表は要しない。

a) 利用目的を本人に通知し、又は公表することによって本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
b) 利用目的を本人に通知するか、又は公表することによって当社の権利又は正当な利益を害するおそれがある場合
c) 国の機関又は地方公共団体が法令の定める事務を遂行することに対して協力する必要がある場合であって、利用目的を本人に通知し、又は公表することによって当該事務の遂行に支障を及ぼすおそれがあるとき。
d) 取得の状況から見て利用目的が明らかであると認められる場合。

２　当社は、当社の公開ウェブサイト上に「公表事項」として、取得した個人情報の利用目的を公表する。

A.3.4.2.5　A.3.4.2.4 のうち、本人から直接書面によって取得する場合の措置

当社は、A.3.4.2.4 の措置を講じた場合において、本人から、書面（電子的方式、磁気的方式など人の知覚によっては認識できない方式で作られる記録を含む。以下、同じ。）に記載された個人情報を直接取得する場合には、少なくとも、次に示す事項又はそれと同等以上

の内容を、あらかじめ、書面によって本人に明示し、書面によって本人の同意を得る。

a) 当社の名称及び連絡先
b) 個人情報保護管理者若しくはその代理人の氏名又は職名、所属及び連絡先
c) 利用目的
d) 個人情報を第三者に提供する事が予定される場合の事項
   ・第三者に提供する目的
   ・提供する個人情報の項目
   ・提供の手段又は方法
   ・当該情報の提供を受ける者又は提供を受ける者の組織の種類、属性
   ・個人情報の取り扱いに関する契約がある場合には、その旨。
e) 個人情報の取り扱いの委託を行うことが予定されている場合には、その旨
f) A.3.4.4.4～A.3.4.4.7 に該当する場合には、その求めに応じる旨及び問合せ窓口
g) 本人が個人情報を与えることの任意性及び当該情報を与えなかった場合に本人に生じる結果
h) 本人が容易に認識できない方法によって個人情報を取得する場合には、その旨

ただし、人の生命、身体又は財産の保護のために緊急に必要がある場合、A.3.4.2.4 のただし書き a)～d)のいずれかに該当する場合には、本人同意を得ることを要しない。

A.3.4.2.6 利用に関する措置

当社は、特定した利用目的の達成に必要な範囲内で個人情報を利用する。

特定した利用目的の達成に必要な範囲を超えて個人情報を利用する場合は、あらかじめ、少なくともA.3.4.2.5のa)～f)に示す事項又はそれと同等以上の内容の事項を本人に通知し、本人の同意を得る。ただし、A.3.4.2.3 の a)～d)のいずれかに該当する場合には、本人の同意を得ることを要しない。

A.3.4.2.7 本人に連絡又は接触する場合の措置

当社は、個人情報を利用して本人に連絡又は接触する場合には、本人に対して A.3.4.2.5 の a)～f)に示す事項又はそれと同等以上の事項、及び取得方法を通知し、本人の同意を得る。ただし、次に示すいずれかに該当する場合は、この限りではない。

a) A.3.4.2.5 の a)～f)に示す事項又はそれと同等以上の内容の事項を明示又は通知し、既に本人の同意を得ているとき
b) 個人情報の取り扱いの全部又は一部を委託された場合であって、当該個人情報を、その利用目的の達成に必要な範囲内で取り扱うとき
c) 合併その他の事由による事業の承継に伴って個人情報が提供され、個人情報を提供する組織が、既に A.3.4.2.5 の a)～f)に示す事項又はそれと同等以上の内容の事項を明示又は通知し、本人の同意をえている場合であって、承継前の利用目的の範囲内で当該個人情報を取り扱うとき
d) 個人情報が特定の者との間で共同して利用され、共同利用者が、既に A.3.4.2.5 の a)～f)に示す事項又はそれと同等以上の内容の事項を明示又は通知し、本人の同意を得

ている場合であって、次に示す事項又はそれと同等以上の内容の事項を、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているとき（以下、“共同利用”という。）

・共同して利用すること
・共同して利用される個人情報の項目・
・共同して利用する者の範囲
・共同して利用する利用目的
・共同して利用する個人情報の管理について責任を有する者の氏名又は名称
・取得方法

e) A.3.4.2.4 のただし書き d)に該当するため、利用目的などを本人に明示、通知又は公表することなく取得した個人情報を利用して、本人にアクセスするとき。

f) A.3.4.2.3 のただし書き a)～d)のいずれかに該当する場合。

２　個人情報が特定の者との間で共同して利用され、 本条第１項の d)に定めるただし書きに該当することにより、本人の同意を得ることなく連絡又は接触を行う場合の手順として以下を定める。

（１） 本条１項 d)の定める各項目を当社の公開ウェブサイトに公表する。
（２） 公表する内容は、あらかじめ、個人情報保護管理者が承認することとし、変更する場合も、個人情報保護管理者の承認を得ること。

A.3.4.2.8　個人データの提供に関する措置

当社は、個人データを第三者に提供する場合には、あらかじめ、本人に対して、A.3.4.2.5 の a)～d)の事項又はそれと同等以上の内容の事項、及び取得方法を通知し、本人の同意を得る。ただし、次に掲げるいずれかに該当する場合は、本人に通知し、本人の同意をえることを要しない。

a） A.3.4.2.5 又は A.3.4.2.7 の規定によって、既に A.3.4.2.5 の a)～d)の事項又はそれと同等以上の内容の事項を本人に明示又は通知し、本人の同意を得ているとき

b） 本人の同意を得ることが困難な場合であって、法令等が定める手続きに基づいた上で、次に示す事項又はそれと同等以上の内容の事項を、あらかじめ、本人に通知するか、又はそれに代わる同等の措置を講じているとき

・第三者への提供を利用目的とすること
・第三者に提供される個人データの項目
・第三者への提供の手段又は方法
・本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること
・取得方法
・本人からの請求などを受け付ける方法

c） 法人その他の団体に関する情報に含まれる当該法人その他の団体の役員及び株主に関する情報であって、かつ、本人又は当該法人その他の団体自らによって公開又は公表された情報を提供する場合であって、b)の①～⑥で示す事項又はそれと同等以上の

内容の事項を、あらかじめ、本人に通知するか、又は本人が容易に知り得る状態に置いているとき

d) 特定した利用目的の達成に必要な範囲内において、個人データの取扱いの全部又は一部を委託するとき

e) 合併その他の事由による事業の承継に伴って個人情報を提供する場合であって、承継前の利用目的の範囲内で当該個人データを取り扱うとき

f) 個人情報を共同利用している場合であって、共同して利用する者の間で、A.3.4.2.7 に規定する共同利用について契約によって定めているとき

g) A.3.4.2.3 のただし書き a)～d) のいずれかに該当する場合

A.3.4.2.8.1 外国にある第三者への提供の制限

当社は、法令等の定めに基づき、外国にある第三者に個人データを提供する場合には、あらかじめ外国にある第三者への提供を認める旨の本人の同意を得る。ただし、A.3.4.2.3 の a)～d)のいずれかに該当する場合及びその他法令等によって除外事項が適用される場合は、本人の同意を得ること要しない。

A.3.4.2.8.2 第三者提供に係る記録の作成など

当社は、個人データを第三者に提供したときは、法令等の定めるところによって記録を作成し、保管しなければならない。ただし、A.3.4.2.3 の a)～d)のいずれかに該当する場合、又は次に掲げるいずれかに該当する場合は、記録の作成を要しない。

a) 個人情報取扱事業者が利用目的の達成に必要な範囲内において個人データの取扱い全部又は一部を委託することに伴って当該個人データが提供される場合

b) 合併その他の事由による事業の承継に伴って個人データが提供される場合

c) 特定の者との間で共同して利用される個人データが当該特定のものに提供される場合であって、その旨並びに共同して利用される個人データの項目、共同して利用する者の範囲、利用する者の利用目的及び当該個人データの管理について責任を有する者の氏名又は名称について、あらかじめ、本人に通知するか、又は本人が容易に知りえる状態においているとき

A.3.4.2.8.3 第三者提供を受ける際の確認など

当社は、第三者から個人データの提供を受ける際に関しては、法令等の定めるところによって確認を行わなければならない。ただし、A.3.4.2.3 の a)～d)のいずれかに該当する場合、又は A.3.4.2.8.2 の a)～c)のいずれかに該当する場合は、確認を要しない。

当社は、法令等の定めるところによって確認の記録を作成、保管する。

A.3.4.2.9 匿名加工情報

当社は、匿名加工情報の取り扱いを行うか否かの方針を定めなければならない。

当社では、基本的に匿名加工情報を扱わない。しかしながら、何らかの理由で、匿名加工情報を取り扱う場合には、本人の権利利益に配慮し、かつ、法令等の定めるところによって適切な取扱いを行う手順を確立し、かつ、維持する。

A.3.4.3　適性管理

A.3.4.3.1　正確性の確保

当社は、利用目的の達成に必要な範囲内において、個人データを、正確、かつ、最新の状態で管理する。

当社は、個人データを利用する必要がなくなったときは、当該個人データを遅滞なく消去するよう努める。

A.3.4.3.2　安全管理措置

当社は、その取り扱う個人情報の個人情報保護リスクにおいて応じて、漏えい、滅失又はき損の防止その他の個人情報の安全管理のために必要かつ適切な措置を講ずる。

２　当社は、本条 1 項を実施するために、別途「安全対策管理規程」を定め、従業者に対し、周知し、遵守させる。

A.3.4.3.3　従業者の監督

当社は、その従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業者に対し必要かつ適切な監督を行う。

２　当社は、前項を確実にするために、当社の従業者と、退職後も有効とした機密保持条項が入った誓約書を交わす。

３　従業者は、誓約書に記載されたことを遵守することとし、遵守しない場合は、別途定める「就業規則」に従って罰せられることがある。

４　当社は、当社従業者に対して、カメラによる監視またはオンラインでのモニタリングを行う際は、予め各従業者に対してその旨を通知する。

A.3.4.3.4　委託先の監督

当社は、個人データの取り扱いの全部又は一部を委託する場合、特定した利用目的の範囲内で委託契約を締結する。

当社は、個人データの取り扱いの全部又は一部を委託する場合は、十分な個人データの保護水準を満たしている者を選定する。このため、当社は、委託を受ける者を選定する基準には、少なくとも委託する当該業務に関しては、自社と同等以上の個人情報保護水準にあることを客観的に確認できることを含める。

当社は、個人データの取扱いの全部又は一部を委託する場合は、委託する個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行う。

当社は、次に示す事項を契約によって規定し、十分な個人情報の保護水準を担保する。

a)　委託者及び受託者の責任の明確化

b)　個人データの安全管理に関する事項

c)　再委託に関する事項

d） 個人データの取り扱い状況に関する委託者への報告の内容及び頻度
e） 契約内容が遵守されていることを委託者が、定期的、及び適宜に確認できる事項
f） 契約内容が遵守されなかった場合の措置
g） 事件・事故が発生した場合の報告・連絡に関する事項
h） 契約終了後の措置

当社は、当該契約書などの書面を少なくとも個人データの保有期間にわたって保存する。

２　当社は、外部委託先に当社にて作成した「機密保持契約書」の雛形を提示し、その内容について双方検討のうえ契約を取り交わす。また、総務部門が、当該契約書などの書面を個人情報の保有期間にわたって保存する。
３　委託先が、委託先選定基準に満たない、又は前項に定める a～h の項目を満たした契約を行わないが、どうしても委託する必要がある場合は、その理由をトップマネジメントに説明するとともに、残留リスクとして認識すること。
４　外部委託先の個人情報管理について、定期的に監査を行ない、監査報告書を提出するものとする。ただし、外部委託先の監査として「外部委託先チェックリスト」の提出をもって監査とみなすこともできる。
５　特定個人情報を委託する場合は、委託先と「特定個人情報の取扱いに関する覚書」を交わす。

A.3.4.4 個人情報に関する本人の権利

A.3.4.4.1　個人情報に関する権利

当社は、保有個人データに関して、本人から開示等の請求等を受け付けた場合は、A.3.4.4.4～A.3.4.4.7 の規定によって、遅滞なくこれに応じる。ただし、次に掲げるいずれかに該当する場合は、保有個人データには当たらない。

a） 当該個人データの存否が明らかになることによって、本人又は第三者の生命、身体又は財産に危害が及ぶおそれがあるもの。
b） 当該個人データの存否が明らかになることによって、違法又は不当な行為を助長する、又は誘発するおそれのあるもの。
c） 当該個人データの存否が明らかになることによって、国の安全が害されるおそれ、他国若しくは国際機関との信頼関係が損なわれるおそれ又は他国若しくは国際機関との交渉上不利益を被るおそれのあるもの。
d） 当該個人データの存否が明らかになることによって、犯罪の予防、鎮圧又は捜査その他の公共の安全と秩序維持に支障が及ぶおそれのあるもの。

当社は、保有個人データに該当しないが、本人から求められる利用目的の通知、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止の請求などの全てに応じることができる権限を有する個人情報についても、保有個人データと同様に取り扱わなければならない。当社では、これを開示対象個人情報と呼ぶが、“保有個人データ”又は“開示対象個人情報”と表記した場合、“保有個人データ”及び“開示対象個人情報”の両

方を含む。

A.3.4.4.2　開示等の請求等に応じる手続

当社は、開示等の請求等に応じる手続として次の事項を定め、当社のウェブサイト上の「公表事項」に公表する。なお、公表する内容は、個人情報保護管理者の承認を得る。

a)　開示等の請求等の申し出先：　個人情報等に関するお問い合わせ窓口／苦情の申し出先とする。

b)　開示等の請求等に際して提出すべき書面の様式その他の開示などの求めの方式:別途「開示対象個人情報に関する各種申請書」を定め、ウェブ上に掲載しダウンロード可能とする。

c)　開示等の請求等をする者が、本人又は代理人であることの確認の方法 : 本人を証明する書類の提出（免許証、住民票等)、代理人の場合は代理人確認書類（本人からの印鑑証明書付依頼書等）の提出

d)　A.3.4.44 又は A.3.4.4.5 による場合の手数料の徴収方法：同額の切手、または現金にていただく。

当社は、本人からの開示等の請求等に応じる手続きを定めるに当たっては、本人に過重な負担を課するものとならないように配慮する。また、A.3.4.4.4 又は A.3.4.4.5 よって本人からの請求等に応じる場合に、手数料を徴収するときは、実費を勘案して合理的であると認められる範囲内において、その額を定める。

A.3.4.4.3　保有個人データに関する事項の周知など

当社は、取得した個人情報が保有個人データに該当する場合は、当該保有個人データに関し、次の事項を本人が知り得る状態（本人の請求などに応じて遅滞なく回答する場合を含む。）に置くために、当社のウェブサイト上に公表することとする。

a)　当社の名称

b)　個人情報保護管理者若しくはその代理人の氏名又は職名、所属及び連絡先

c)　すべての保有個人データの取り扱いに関する利用目的[A.3.4.2.4 の a)～c)までに該当する場合を除く。]

d)　保有個人データの取り扱いに関する苦情の申し出先

e)　当社が認定個人情報保護団体の対象事業者である場合であっては、当該認定個人情報保護団体の名称及び苦情の解決の申し出先

f)　A.3.4.4.2 によって定めた手続き

A.3.4.4.4　保有個人データの利用目的の通知

当社は、本人から、当該本人が識別される保有個人データについて、利用目的の通知を求められた場合には、遅滞なくこれに応じる。ただし、A.3.4.2.4 のただし書き a)～c)のいずれかに該当する場合、又は A.3.4.4.3 の c)によって当該本人が識別される保有個人データの利用目的が明らかな場合は利用目的の通知を必要としないが、そのときは、本人に遅滞なくその旨を通知するとともに、理由を説明する。

A.3.4.4.5　保有個人データの開示

当社は、本人から当該本人が識別される保有個人データの開示（当該本人が識別される保有個人データが存在しないときにその旨を知らせることを含む。）の請求を受けたときは、法令の規定によって特別の手続きが定められている場合を除き、本人に対し、遅滞なく、当該保有個人データを書面（開示の求めを行った者が同意した方法があるときは、当該方法）によって開示しなければならない。ただし、開示することによって次のａ～ｃのいずれかに該当する場合は、その全部又は一部を開示する必要はないが、そのときは、本人に遅滞なくその旨を通知するとともに、理由を説明するものとする。

a)　本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
b)　当該事業者の業務の適正な実施に著しい支障を及ぼすおそれがある場合
c)　法令に違反する場合

A.3.4.4.6　保有個人データの訂正、追加又は削除

当社は、本人から、当該本人が識別される保有個人データの内容が事実でないという理由によって当該保有個人データの訂正、追加又は削除（以下、この項において“訂正等”という。）を求められた場合は、法令の規定によって特別の手続きが定められている場合を除き、利用目的の達成に必要な範囲内において、遅滞なく必要な調査を行い、その結果に基づいて、当該保有個人データの訂正等を行う。また、当社は、訂正等を行ったときは、その旨及びその内容を、本人に対し、遅滞なく通知し、訂正などを行わない旨の決定をしたときは、その旨及びその理由を、本人に対し、遅滞無く通知する。

A.3.4.4.7　保有個人データの利用又は提供の拒否権

当社が、本人から当該本人が識別される保有個人データの利用の停止、消去又は第三者への提供の停止以下、この項において“利用停止等”という。を求められた場合は、これに応ずるものとする。また、措置を講じたあとは、遅滞なくその旨を本人に通知するものとする。ただし、A.3.4.4.5 のただし書き a)～c)のいずれかに該当する場合は、利用停止等を行う必要はないが、そのときは、本人に遅滞なくその旨を通知するとともに、理由を説明する。

A.3.4.5　認識

当社は、従業者が、本文編 7.3 に規定するの認識をもつために、関連する各部門及び階層における次の事項を認識させる手順を確立し、かつ、維持する。

a)　個人情報保護方針（内部向け個人情報保護方針及び外部向け個人情報保護方針）
b)　個人情報保護マネジメントシステムに適合することの重要性及び利点
c)　個人情報保護マネジメントシステムに適合するための役割及び責任
d)　個人情報保護マネジメントシステムに違反した際に予想される結果

当社は、認識させる手順に、全ての従業者に対する教育を少なくとの年一回、適宜に行うことを含める。

２　個人情報保護管理者は、毎年、年度初めに「年間教育計画表」を作成し、「教育計画兼実施報告書」により内容・実施方法・講師などについてトップマネジメントの承認を得、それに従って教育を実施する。従業者は、個人情報保護管理者が主催する個人情報保護マネジメントシステムを遵守するための教育を受ける。
３　当社は従業員に対して教育を実施した後、受講者の理解度を確認・把握するため、「理解度確認テスト」を用いて教育効果の測定を行う。
４　個人情報保護管理者は、教育の効果について測定する。個人情報保護管理者は、測定された効果が低いと判断された従業者に対して、再教育を行う。また、教育の効果が全体的に著しく低いと判断したときは、教育計画、方法、内容などを点検し、改善策を講じると共に再教育の計画を策定する。
５　個人情報保護管理者は、教育を実施した日時・参加者・内容について「教育計画兼実施報告書」を作成し、トップマネジメントに報告し、保管する。

A.3.5　文書化した情報

目的　文書化した情報を作成・維持するため。

A.3.5.1　文書化した情報の範囲

当社は、次の個人情報保護マネジメントシステムの基本となる要素を書面で記述する。

a)　内部向け個人情報保護方針
b)　外部向け個人情報保護方針
c)　内部規程：個人情報保護基本規程本規程、個人情報保護内部監査規程、安全対策管理規程、個人情報取扱細則
d)　内部規程に定める手順上で使用する様式
e)　計画書：教育計画書、監査計画書、その他計画書
f)　本規程が要求する記録及び当社が個人情報保護マネジメントシステムを実施する上で必要と判断した記録：別途「定期点検表」に記載する。

２　当社は、これらを「文書管理一覧表」にて管理する。

A.3.5.2　文書化した情報（記録を除く）の管理

当社は、JIS Q 15001 が要求するすべての文書（記録を除く。）を管理する手順を確立し、実施し、かつ維持する。文書化した情報（記録を除く。）の管理の手順には、次の事項を含める。

a)　文書化した情報（記録を除く）の発行及び改定に関する事。
b)　文書化した情報（記録を除く）の改定の内容と版数との関連付けを明確にすること。
c)　必要な文書化した情報（記録を除く）が必要なときに容易に参照できること。

２　具体的な文書化した情報（記録を除く。）の管理手順として以下のように定める。
（１）　文書発行責任
個人情報保護管理者は、個人情報保護マネジメントシステム文書を発行及び改定

する。個人情報保護管理者は、個人情報保護マネジメントシステムに必要な基本となる規程文書を定め、トップマネジメントの承認を得る。トップマネジメントの承認を得た文書は、「初版」とし、発行日を表紙に記載すると共に「文書管理一覧表」に付加し、従業者が参照できるよう、当社内イントラネットに掲載し、その旨を当社内メーリングリストによって周知する。

個人情報保護管理者は、基本となる規程を遵守するための詳細規程を定めることができる。また、必要に応じて部門管理者などが別途になんらかの規程を定めた場合、個人情報保護管理者は、当社の個人情報保護マネジメントシステムとの整合性を確認し、承認する。

（2） 見直し

個人情報保護管理者は、個人情報保護マネジメントシステム文書を、毎年の定期監査終了後 2 ヶ月以内に見直す。

監査指摘事項、内外からの意見・苦情、当社事業環境や社会情勢の変化など、何らかの都合で文書を改定する必要が生じたとき、個人情報保護管理者は、文書の改定案を作成し、トップマネジメントの承認を得る。トップマネジメントの承認を得て正式文書となった改定文書は、文書管理責任者が、版番号と改定日を記載すると共に「文書管理一覧表」に改定内容を記し、最新版として管理する。

（3） 履歴管理

文書管理責任者は、「文書管理一覧表」を作成し、版番号、発行日、書面改定履歴等を一覧で参照できるよう整理する。個人情報保護管理者は、毎年監査が行われる前に、一覧表と本体文書の整合性を確認し、文書改定内容と版数を照合する。

A.3.5.3 文書化した情報のうち記録の管理

当社は、個人情報保護マネジメントシステム及び JIS Q 15001 の要求事項への適合を実証するために必要な記録として、次の事項を含む記録を作成し、維持する。

a. 個人情報の特定に関する記録
b. 法令、国が定める指針およびその他の規範の特定に関する記録
c. 個人情報保護リスクの認識、分析及び対策に関する記録
d. 計画書
e. 利用目的の特定に関する記録
f. 保有個人データに関する開示等（利用目的の通知、開示、内容の訂正、追加又は削除、利用の停止または消去、第三者提供の停止）の請求等への対応記録
g. 教育などの実施記録
h. 苦情及び相談への対応記録
i. 運用の確認の記録
j. 内部監査報告書
k. 是正処置の記録
l. マネジメントレビューの記録
m. その他当社が個人情報保護マネジメントシステムを実施する上で必要と判断した記録

当社は、記録の管理についての手順を確立し、実施し、かつ、維持する。

2　前項の維持のために、以下を実施する。

（1）　文書や電子媒体による管理

個人情報保護マネジメントシステム実行の記録は、文書または電子媒体（サーバ、クラウド上の管理を含む）などにより管理する。

（2）　保管期間

各記録は、それぞれの取扱い担当者が保管期間を定め、個人情報保護管理者が承認する。保管期間及びその廃棄方法は「文書管理一覧表」に定める。

（3）　管理手順

各記録は、個人情報保護管理者がそれぞれ取得担当者を決める。担当者は取得した記録を管理するが、個人情報保護管理者の要求があったときには、いつでも参照することができるよう維持する。各記録の取得及び維持の方法は記録により異なるので、各担当者の権限で行う。

A.3.6　苦情及び相談への対応

当社は、個人情報の取扱い及び個人情報保護マネジメントシステムに関して、本人からの苦情及び相談を受け付けて、適切、かつ迅速な対応を行う手順を確立し、かつ、維持する。

当社は、上記の目的を達成するために必要な体制の整備を行う。

2　当社の苦情相談受付担当者は、お問い合わせ窓口担当者とする。

3　本人からの個人情報及び当社の個人情報保護管理体制に関する苦情及び相談への対応手順を以下のとおり定める。

（1）個人情報保護に関する苦情及び相談受付担当者は、本人から以下の苦情及び相談を受付けた場合、内容を確認して「苦情・相談対応記録票」に内容を記入する。

①　本人からお預かりしている個人情報についての苦情及び相談

②　本人より当社の個人情報保護管理体制についての苦情及び相談

（2）個人情報保護に関する苦情及び相談受付担当者は、「苦情・相談対応記録票」を個人情報保護管理者に提出する。内容によって個人情報保護管理者は、即時トップマネジメントに報告し、承認を得る。

（3）個人情報保護管理者は、当該苦情相談が妥当と認めた場合、「苦情・相談対応記録票」の内容に基づき適切な処置実施又は担当者の指名を行う。

（4）処置実施を指名された担当者は、その処置を実施するにあたって、「苦情・相談対応記録票」を使用し個人情報保護管理者の承認を得る。個人情報保護管理者は、「苦情・相談対応記録票」を使用しトップマネジメントの承認を得る。

（5）個人情報保護管理者は、適切な処置の実施後または指名した担当者の処置結果を確認後、その結果を「苦情・相談対応記録票」に内容を記載する。

（6）個人情報保護管理者は、作成した「苦情・相談対応記録票」を、即時トップマネジメントに報告し、承認を得る。

４　苦情・相談を記録保管する手順を以下のとおり定める。

（１）相談の受付け対応した記録は、「苦情・相談対応記録票」に残す。

（２）「苦情・相談対応記録票」は、見直し時にトップマネジメントに提出し、当社の個人情報保護マネジメントシステム見直しのインプットとする。

A.3.7　パフォーマンス評価

目的　パフォーマンス評価を実施するため

A.3.7.1　運用の確認

当社は、個人情報保護マネジメントシステムが適切に運用されていることが当社の各部門及び階層において定期的に、及び適宜に確認されるための手順を確立し、実施し、かつ、維持する。

各部門及び各階層の管理者は、定期的に、及び適宜にマネジメントシステムが適切に運用されているかを確認し、不適合が確認された場合は、その是正処置を行う。

個人情報保護管理者は、トップマネジメントによる個人情報保護マネジメントシステムの見直しに資するため、定期的に、及び適宜にトップマネジメントにその状況を報告する。

２　当社の個人情報保護マネジメントシステムが、各部門及び各階層にて適切に運営されているかどうか運用の確認を行うために、個人情報保護管理者は、点検担当者を指名する。点検担当者は、毎月の初めに前月の個人情報保護マネジメントシステムの運用について確認する。個人情報保護管理者は、確認する項目とその確認時期を、別途「点検項目一覧表」に定める。点検担当者は、「点検項目一覧表」を基に点検作業を行い、それを記録する。点検担当者は、点検作業において、何らかの不適合を発見した場合、個人情報保護管理者に報告すると共に、本規程第４１条に定める是正処置を行う。

A.3.7.2　内部監査

当社は、個人情報保護マネジメントシステムの JIS Q 15001 への適合状況及び個人情報保護マネジメントシステムの運用状況を、少なくとも年一回、適宜に監査する。

当社は、監査の計画及び実施、結果の報告並びにこれに伴う記録の保持に関する責任及び権限を定める手順を確立し、実施し、かつ、維持する。

個人情報保護監査責任者は、監査員に、自己の所属する部署の内部監査をさせてはならない。

A.3.7.3　マネジメントレビュー

トップマネジメントは、当社の個人情報保護マネジメントシステムが、引き続き、適切、妥当かつ有効であることを確実にするために、あらかじめ定めた間隔で、個人情報保護マネジメントシステムをレビューする。そのために、少なくとも年一回（毎年６月）、個人情報保護マネジメントシステムを見直す。

マネジメントレビューにおいては、次の事項を考慮する。

a)　監査及び個人情報保護マネジメントシステムの運用状況に関する報告。

b) 苦情を含む外部からの意見。
c) 前回までの見直しの結果に対するフォローアップ。
d) 個人情報の取り扱いに関する法令、国の定める指針及びその他の規範の改正状況。
e) 社会情勢の変化、国民の認識の変化、技術の進歩などの諸環境の変化。
f) 当社の事業領域の変化
g) 内外から寄せられた改善のための提案。

２　マネジメントレビューを実施するにあたっては、その記録を議事録として残す。

A.3.8　是正処置

当社は、不適合に対する是正処置を確実に実施するための責任と権限を定める手順を確立し、実施し、かつ、維持する。その手順には、次の事項を含める。

a) 不適合の内容を確認する。
b) 不適合の原因を特定し、是正処置及を立案する。
c) 期限を定め、立案された適切な処置を実施する。
d) 実施された是正処置の結果を記録する。
e) 実施された是正処置の有効性をレビューする。

２　当社は、本条１項に定めた措置を適切に行う手順として以下を定める。

（１）個人情報の漏えい、滅失又はき損などの緊急事態の発生、顧客及び外部機関等からの苦情や意見、A.3.7 の「点検項目一覧表」に定めた点検作業・監査の実施、及びその他の事象によって、何らかの不適合が発見された場合、担当者は、不適合となった内容を「是正処置報告書」で個人情報保護管理者及びトップマネジメントに報告し承認を得る。担当者は、不適合となった原因を特定し、「是正処置報告書」に、是正処置を立案する。「是正処置報告書」の立案内容は、個人情報保護管理者及びトップマネジメントに報告し承認を得る。

（２）「是正処置報告書」の立案内容を実施するよう指示された部門は、是正処置を適切な期限内に実施し、「是正処置報告書」に記録して個人情報保護管理者及びトップマネジメントに報告し承認を得る。

（３）担当者は、「是正処置報告書」を基に、是正処置を実施した結果の有効性を確認し、個人情報保護管理者及びトップマネジメントに報告し承認を得る。

付則

本規程の改廃は、トップマネジメントの承認をもって行う。

制定：第１版　２００９年１２月１５日
改訂：第２版　２０１０年　４月２８日
改訂：第３版　２０１９年　４月１１日
改訂：第４版　２０１９年　９月１７日
改訂：第５版　２０２０年　７月１０日

付録

「個人情報の保護に関する法律」及び「個人情報の保護に関する法律施行令（平成 15 年政令第 507 号)」、「JIS Q 15001:2017」で定める用語及び定義について抜粋して記載する。

「個人情報の保護に関する法律」

第２条 この法律において「個人情報」とは、生存する個人に関する情報であって、次の各号のいずれかに該当するものをいう。

一 当該情報に含まれる氏名、生年月日その他の記述等（文書、図画若しくは電磁的記録（電磁的方式（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式をいう。次項第２号において同じ。）で作られる記録をいう。第 18 条第２項において同じ。）に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項（個人識別符号を除く。）をいう。以下同じ。）により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）

二 個人識別符号が含まれるもの

２ この法律において「個人識別符号」とは、次の各号のいずれかに該当する文字、番号、記号その他の符号のうち、政令で定めるものをいう。

一 特定の個人の身体の一部の特徴を電子計算機の用に供するために変換した文字、番号、記号その他の符号であって、当該特定の個人を識別することができるもの

二 個人に提供される役務の利用若しくは個人に販売される商品の購入に関し割り当てられ、又は個人に発行されるカードその他の書類に記載され、若しくは電磁的方式により記録された文字、番号、記号その他の符号であって、その利用者若しくは購入者又は発行を受ける者ごとに異なるものとなるように割り当てられ、又は記載され、若しくは記録されることにより、特定の利用者若しくは購入者又は発行を受ける者を識別することができるもの

３ この法律において「要配慮個人情報」とは、本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報をいう。

４ この法律において「個人情報データベース等」とは、個人情報を含む情報の集合物であって、次に掲げるもの（利用方法からみて個人の権利利益を害するおそれが少ないものとして政令で定めるものを除く。）をいう。

一 特定の個人情報を電子計算機を用いて検索することができるように体系的に構成したもの

二 前号に掲げるもののほか、特定の個人情報を容易に検索することができるように体系的に構成したものとして政令で定めるもの

５ この法律において「個人情報取扱事業者」とは、個人情報データベース等を事業の用に供している者をいう。ただし、次に掲げる者を除く。

一 国の機関

二 地方公共団体
三 独立行政法人等（独立行政法人等の保有する個人情報の保護に関する法律（平成 15 年法律第 59 号）第２条第１項に規定する独立行政法人等をいう。以下同じ。）
四 地方独立行政法人（地方独立行政法人法（平成 15 年法律第 118 号）第２条第１項に規定する地方独立行政法人をいう。以下同じ。）
６ この法律において「個人データ」とは、個人情報データベース等を構成する個人情報をいう。
７ この法律において「保有個人データ」とは、個人情報取扱事業者が、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止を行うことのできる権限を有する個人データであって、その存否が明らかになることにより公益その他の利益が害されるものとして政令で定めるもの又は１年以内の政令で定める期間以内に消去することとなるもの以外のものをいう。
８ この法律において個人情報について「本人」とは、個人情報によって識別される特定の個人をいう。
９ この法律において「匿名加工情報」とは、次の各号に掲げる個人情報の区分に応じて当該各号に定める措置を講じて特定の個人を識別することができないように個人情報を加工して得られる個人に関する情報であって、当該個人情報を復元することができないようにしたものをいう。
一 第１項第１号に該当する個人情報 当該個人情報に含まれる記述等の一部を削除すること（当該一部の記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）。
二 第１項第２号に該当する個人情報 当該個人情報に含まれる個人識別符号の全部を削除すること（当該個人識別符号を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）。
10 この法律において「匿名加工情報取扱事業者」とは、匿名加工情報を含む情報の集合物であって、特定の匿名加工情報を電子計算機を用いて検索することができるように体系的に構成したものその他特定の匿名加工情報を容易に検索することができるように体系的に構成したものとして政令で定めるもの（第 36 条第１項において「匿名加工情報データベース等」という。）を事業の用に供している者をいう。ただし、第５項各号に掲げる者を除く。

政令：「個人情報の保護に関する法律施行令（平成 15 年政令第 507 号）」

（個人識別符号）
第１条 個人情報の保護に関する法律（以下「法」という。）第２条第２項の政令で定める文字、番号、記号その他の符号は、次に掲げるものとする。
一 次に掲げる身体の特徴のいずれかを電子計算機の用に供するために変換した文字、番号、記号その他の符号であって、特定の個人を識別するに足りるものとして個人情報保護委員会規則で定める基準に適合するもの
イ 細胞から採取されたデオキシリボ核酸（別名ＤＮＡ）を構成する塩基の配列
ロ 顔の骨格及び皮膚の色並びに目、鼻、口その他の顔の部位の位置及び形状によって定

まる容貌
ハ 虹彩の表面の起伏により形成される線状の模様
ニ 発声の際の声帯の振動、声門の開閉並びに声道の形状及びその変化ホ 歩行の際の姿勢及び両腕の動作、歩幅その他の歩行の態様
ヘ 手のひら又は手の甲若しくは指の皮下の静脈の分岐及び端点によって定まるその静脈の形状
ト 指紋又は掌紋
二 旅券法（昭和 26 年法律第 267 号）第６条第１項第１号の旅券の番号
三 国民年金法（昭和 34 年法律第 141 号）第 14 条に規定する基礎年金番号
道路交通法（昭和 35 年法律第 105 号）第 93 条第１項第１号の免許証の番号
五 住民基本台帳法（昭和 42 年法律第 81 号）第７条第 13 号に規定する住民票コード
六 行政手続における特定の個人を識別するための番号の利用等に関する法律(平成 25 年法律第 27 号）第２条第５項に規定する個人番号
七 次に掲げる証明書にその発行を受ける者ごとに異なるものとなるように記載された個人情報保護委員会規則で定める文字、番号、記号その他の符号
イ 国民健康保険法（昭和 33 年法律第 192 号）第９条第２項の被保険者証
ロ 高齢者の医療の確保に関する法律（昭和 57 年法律第 80 号）第 54 条第３項の被保険者証
ハ 介護保険法（平成９年法律第 123 号）第 12 条第３項の被保険者証
八 その他前各号に準ずるものとして個人情報保護委員会規則で定める文字、番号、記号その他の符号
（要配慮個人情報）
第２条 法第２条第３項の政令で定める記述等は、次に掲げる事項のいずれかを内容とする記述等（本人の病歴又は犯罪の経歴に該当するものを除く。）とする。
一 身体障害、知的障害、精神障害（発達障害を含む。）その他の個人情報保護委員会規則で定める心身の機能の障害があること。
二 本人に対して医師その他医療に関連する職務に従事する者（次号において「医師等」という。）により行われた疾病の予防及び早期発見のための健康診断その他の検査（同号において「健康診断等」という。）の結果
三 健康診断等の結果に基づき、又は疾病、負傷その他の心身の変化を理由として、本人に対して医師等により心身の状態の改善のための指導又は診療若しくは調剤が行われたこと。
四 本人を被疑者又は被告人として、逮捕、捜索、差押え、勾留、公訴の提起その他の刑事事件に関する手続が行われたこと。
五 本人を少年法（昭和 23 年法律第 168 号）第３条第１項に規定する少年又はその疑いのある者として、調査、観護の措置、審判、保護処分その他の少年の保護事件に関する手続が行われたこと。
（個人情報データベース等）
第３条 法第２条第４項の利用方法からみて個人の権利利益を害するおそれが少ないものとして政令で定めるものは、次の各号のいずれにも該当するものとする。

一 不特定かつ多数の者に販売することを目的として発行されたものであって、かつ、その発行が法又は法に基づく命令の規定に違反して行われたものでないこと。
二 不特定かつ多数の者により随時に購入することができ、又はできたものであること。
三 生存する個人に関する他の情報を加えることなくその本来の用途に供しているものであること。
２ 法第２条第４項第２号の政令で定めるものは、これに含まれる個人情報を一定の規則に従って整理することにより特定の個人情報を容易に検索することができるように体系的に構成した情報の集合物であって、目次、索引その他検索を容易にするためのものを有するものをいう。
（保有個人データから除外されるもの）
第４条 法第２条第７項の政令で定めるものは、次に掲げるものとする。
一 当該個人データの存否が明らかになることにより、本人又は第三者の生命、身体又は財産に危害が及ぶおそれがあるもの
二 当該個人データの存否が明らかになることにより、違法又は不当な行為を助長し、又は誘発するおそれがあるもの
三 当該個人データの存否が明らかになることにより、国の安全が害されるおそれ、他国若しくは国際機関との信頼関係が損なわれるおそれ又は他国若しくは国際機関との交渉上不利益を被るおそれがあるもの
四 当該個人データの存否が明らかになることにより、犯罪の予防、鎮圧又は捜査その他の公共の安全と秩序の維持に支障が及ぶおそれがあるもの
（保有個人データから除外されるものの消去までの期間）
第５条 法第２条第７項の政令で定める期間は、６月とする。
（匿名加工情報データベース等）
第６条 法第２条第 10 項の政令で定めるものは、これに含まれる匿名加工情報を一定の規則に従って整理することにより特定の匿名加工情報を容易に検索することができるように体系的に構成した情報の集合物であって、目次、索引その他検索を容易にするためのものを有するものをいう。
（要配慮個人情報を本人の同意なく取得することができる場合）
第７条 法第 17 条第２項第６号の政令で定める場合は、次に掲げる場合とする。
一 本人を目視し、又は撮影することにより、その外形上明らかな要配慮個人情報を取得する場合
二 法第 23 条第５項各号に掲げる場合において、個人データである要配慮個人情報の提供を受けるとき。

「JIS Q 15001:2017」

3.1
組織
責任及び権限をもつトップマネジメントが存在し，自らの目的 (3.8) を達成するため，責任，権限及び相互関係を伴う独自の機能をもつ，個人又は人々の集まり。
3.2

利害関係者

ある決定事項若しくは活動に影響を与え得るか，その影響を受け得るか，又はその影響を受けると認識している，個人又は組織（3.1）。

（JIS Q 27000:2014 の 2.41 参照）

3.3

要求事項

明示されている，通常暗黙のうちに了解されている又は義務として要求されている，ニーズ又は期待。

（JIS Q 27000:2014 の 2.63 参照）

注記 “通常暗黙のうちに了解されている”とは，対象となるニーズ又は期待が暗黙のうちに了解されていることが，組織及び利害関係者にとって，慣習又は慣行であることを意味する。

3.4

マネジメントシステム

方針（3.7），目的（3.8）及びその目的を達成するためのプロセス（3.12）を確立するための，相互に関連する又は相互に作用する，組織（3.1）の一連の要素。

注記 1 一つのマネジメントシステムは，単一又は複数の分野を取り扱うことができる。

注記 2 マネジメントシステムの要素には，組織の構造，役割及び責任，計画，運用などが含まれる。

3.5

トップマネジメント

最高位で組織（3.1）を指揮し，管理する個人又は人々の集まり。

注記 トップマネジメントは，組織内で，権限を委譲し，資源を提供する力をもっている。

3.6

有効性

計画した活動を実行し，計画した結果を達成した程度。

（JIS Q 27000:2014 の 2.24 参照）

3.7

方針

トップマネジメント(3.5)によって正式に表明された組織(3.1)の意図及び方向付け。

（JIS Q 27000:2014 の 2.60 参照）

3.8

目的

達成する結果。

注記 1 目的は，戦略的，戦術的又は運用的であり得る。

注記 2 目的は，様々な領域（例えば，財務，安全衛生，環境）の到達点に関連し得るものであり，様々な階層［例えば，戦略的レベル，組織全体，プロジェクト単位，製品ごと，プロセス（3.12）ごと］で適用できる。

注記 3　目的は，例えば，予定された成果，意図，運用基準など，別の形で表現することもできる。また，個人情報保護目的という表現の仕方もある。又は，同じような意味をもつ別の言葉（例 狙い，到達点，目標）で表すこともできる。

注記 4　個人情報保護マネジメントシステムの場合，組織は，特定の結果を達成するため，内部向け個人情報保護方針と整合のとれた個人情報保護目的を設定する。

3.9

リスク

目的に対する不確かさの影響。

注記 1　影響とは，期待されていることから，好ましい方向又は好ましくない方向にかい（乖）離することをいう。

注記 2 不確かさとは，事象（3.28），その結果（3.24）又はその起こりやすさ（3.29）に関する，情報，理解又は知識が，たとえ部分的にでも欠落している状態をいう。

注記 3 リスクは，起こり得る事象（3.28），結果（3.24）又はこれらの組合せについて述べることによって，その特徴を記述することが多い。

注記 4 リスクは，ある事象（周辺状況の変化を含む。）の結果とその発生の起こりやすさ（3.29）との組合せとして表現されることが多い。

3.10

力量

意図した結果を達成するために，知識及び技能を適用する能力。

（JIS Q 27000:2014 の 2.11 参照）

3.11

文書化した情報

組織（3.1）によって，管理及び維持されるように要求されている情報，並びにそれが含まれている媒体。

（JIS Q 27000:2014 の 2.23 参照）

注記 1　文書化した情報は，あらゆる形式及び媒体の形をとることができ，あらゆる情報源から得ることができる。

注記 2 文書化した情報には，次に示すものを参照することができる。

－ 関連するプロセス（3.12）を含むマネジメントシステム（3.4）

－ 組織の運用のために作成された情報（文書類）

－ 達成された結果の証拠（記録）

3.12

プロセス

インプットをアウトプットに変換する，相互に関連する又は相互に作用する一連の活動。

（JIS Q 27000:2014 の 2.61 参照）

3.13

パフォーマンス

測定可能な結果。

（JIS Q 27000:2014 の 2.59 参照）

注記 1 パフォーマンスは，定量的又は定性的な所見のいずれにも関連し得る。

注記 2 パフォーマンスは，活動，プロセス（3.12），製品（サービスを含む。），システム，又は組織（3.1）の運営管理に関連し得る。

3.14

監視

システム，プロセス（3.12）又は活動の状況を明確にすること。

（JIS Q 27000:2014 の 2.52 参照）

注記 状況を明確にするために，点検，監督，又は注意深い観察が必要な場合もある。

3.15

測定

値を決定するためのプロセス（3.12）。

3.16

監査

監査基準が満たされている程度を判定するために，監査証拠を収集し，それを客観的に評価するための，体系的で，独立し，文書化したプロセス（3.12）。

（JIS Q 27000:2014 の 2.5 参照）

注記 1 監査は，内部監査（第一者）若しくは外部監査（第二者・第三者）のいずれでも，又は複合監査（複数の分野の組合せ）であってもよい。

注記 2 “監査証拠”及び“監査基準”は，JIS Q 19011 に定義されている。

3.17

適合

要求事項（3.3）を満たしていること。

（JIS Q 27000:2014 の 2.13 参照）

3.18

不適合

要求事項（3.3）を満たしていないこと。

（JIS Q 27000:2014 の 2.53 参照）

3.19

是正処置

不適合（3.18）の原因を除去し，再発を防止するための処置。

（JIS Q 27000:2014 の 2.19 参照）

3.20

継続的改善

パフォーマンス（3.13）を向上するために繰り返し行われる活動。

（JIS Q 27000:2014 の 2.15 参照）

3.21

分析モデル

一つ以上の基本測定量（3.23）及び／又は導出測定量（3.27）をそれに関連する判断基準と結合するアルゴリズム又は計算。

（JIS Q 27000:2014 の 2.2 参照）

3.22
属性
人手又は自動的な手段によって，定量的又は定性的に識別できる対象物（3.33）の特性又は特徴。
（JIS Q 27000:2014 の 2.4 参照）
3.23
基本測定量
単一の属性（3.22）とそれを定量化するための方法とで定義した測定量（3.30）。
（JIS Q 27000:2014 の 2.10 参照）
注記 基本測定量は，他の測定量と機能的に独立した測定量をいう。
3.24
結果
目的（3.8）に影響を与える事象（3.28）の結末。
（JIS Q 27000:2014 の 2.14 参照）
注記 1 一つの事象が，様々な不適合（3.18）の原因を除去し，再発を防止するための処置。
（JIS Q 27000:2014 の 2.19 参照）
3.20
継続的改善
パフォーマンス（3.13）を向上するために繰り返し行われる活動。
（JIS Q 27000:2014 の 2.15 参照）
3.21
分析モデル
一つ以上の基本測定量（3.23）及び／又は導出測定量（3.27）をそれに関連する判断基準と結合するアルゴリズム又は計算。
（JIS Q 27000:2014 の 2.2 参照）
3.22
属性
人手又は自動的な手段によって，定量的又は定性的に識別できる対象物（3.33）の特性又は特徴。
（JIS Q 27000:2014 の 2.4 参照）
3.23
基本測定量
単一の属性（3.22）とそれを定量化するための方法とで定義した測定量（3.30）。
（JIS Q 27000:2014 の 2.10 参照）
注記 基本測定量は，他の測定量と機能的に独立した測定量をいう。
3.24
結果
目的（3.8）に影響を与える事象（3.28）の結末。
（JIS Q 27000:2014 の 2.14 参照）

注記 1 一つの事象が，様々な結果につながることがある。

注記 2 結果は，確かなことも不確かなこともある。個人情報保護の文脈において，結果は，通常，好ましくないものである。

注記 3 結果は，定性的にも定量的にも表現されることがある。

注記 4 初期の結果が，連鎖によって，段階的に増大することがある。

3.25

管理策

リスク（3.9）を修正する対策。

（JIS Q 27000:2014 の 2.16 参照）

注記 1 管理策には，リスクを修正するためのあらゆるプロセス，方針，仕掛け，実務，その他の処置を含む。

注記 2 管理策が，常に意図又は想定した修正効果を発揮するとは限らない。

3.26

判断基準

アクション若しくは追加調査の必要性を決めるため又は与えられた結果の信頼度のレベルを記述するために使う，しきい（閾）値，目標又はパターン。

（JIS Q 27000:2014 の 2.21 参照）

3.27

導出測定量

複数の基本測定量（3.23）の値の関数として定義した測定量（3.30）。

（JIS Q 27000:2014 の 2.22 参照）

3.28

事象

ある特有な状況の出現又は変化。

（JIS Q 27000:2014 の 2.25 参照）

注記 1 事象は，発生が一度以上であることがあり，幾つかの原因をもつことがある。

注記 2 事象は，何かが起こらないことを含むことがある。

注記 3 事象は，“インシデント”又は“事故”と呼ばれることがある。

3.29

起こりやすさ

何かが起こる見込み。

（JIS Q 27000:2014 の 2.45 参照）

3.30

測定量

測定（3.15）の結果として値が割り当てられる変数。

（JIS Q 27000:2014 の 2.47 参照）

注記 “測定量”という用語は，基本測定量，導出測定量及び指標をまとめて参照するために使うことがある。

3.31

測定の関数

複数の基本測定量（3.23）を結合するために遂行するアルゴリズム又は計算。

（JIS Q 27000:2014 の 2.49 参照）

3.32

測定方法

特定の尺度（3.34）に関して属性（3.22）を定量化するために使う一連の操作の論理的な順序を一般的に記述したもの。

（JIS Q 27000:2014 の 2.50 参照）

注記 測定方法の類型は，属性を定量化するために使う操作の性質による。これには，次の二つの類型がある。

－ 主観的 人間の判断を含んだ定量化

－ 客観的 数値的な規則に基づいた定量化

3.33

対象物

属性（3.22）の測定（3.15）を通して特徴付けられるもの。

（JIS Q 27000:2014 の 2.55 参照）

3.34

尺度

連続的若しくは離散的な値の順序集合又は分類の集合で，それに属性（3.22）を対応付けるもの。

（JIS Q 27000:2014 の 2.80 参照）

注記 尺度の類型は，尺度上の値同士の関係による。一般には次の 4 種類の尺度を定義する。

－ 名義尺度 測定値は，分類した結果を示す。

－ 順序尺度 測定値は，離散的な階級に分けた結果を示す。

－ 間隔尺度 測定値は，属性の等しい量に対応して等しい距離を示す。

－ 比尺度 測定値は，属性の等しい量に対応して等しい距離を示し，ゼロという値は，その属性に対応するものが存在しないことを表す。

これらは，尺度の類型の例でしかない。

3.35

脅威

システム又は組織に損害を与える可能性がある，望ましくないインシデントの潜在的な原因。

（JIS Q 27000:2014 の 2.83 参照）

3.36

ぜい弱性

一つ以上の脅威（3.35）によって付け込まれる可能性のある，資産又は管理策（3.25）の弱点。

（JIS Q 27000:2014 の 2.89 参照）

3.37

残留リスク

リスク対応（3.38）後に残っているリスク（3.9)。

（JIS Q 27000:2014 の 2.64 参照）

注記 1 残留リスクには，特定されていないリスクが含まれ得る。

注記 2 残留リスクは，“保有リスク”ともいう。

3.38

リスク対応

リスク（3.9）を修正するプロセス（3.12)。

（JIS Q 27000:2014 の 2.79 参照）

注記 1 リスク対応には，次の事項を含むことがある。

- リスクを生じさせる活動を，開始又は継続しないと決定することによって，リスクを回避すること。
- ある機会を追求するために，リスクをとる又は増加させること。
- リスク源を除去すること。
- 起こりやすさを変えること。
- 結果を変えること。
- 一つ以上の他者とリスクを共有すること（契約及びリスクファイナンシングを含む。)。
- 情報に基づいた選択によって，リスクを保有すること。

注記 2 好ましくない結果に対処するリスク対応は，“リスク軽減”，“リスク排除”，“リスク予防”及び“リスク低減”と呼ばれることがある。

注記 3 リスク対応が，新たなリスクを生み出したり，又は既存のリスクを修正したりすることがある。

3.39

本人

個人情報によって識別される特定の個人。

3.40

個人情報保護管理者

トップマネジメントによって組織内部に属する者の中から指名された者であって，個人情報保護マネジメントシステムの計画及び運用に関する責任及び権限をもつ者。

注記 “個人情報保護管理者”は，個人情報の取扱いに関する安全管理面だけではなく，組織全体のマネジメントを含む全体の管理者である。

3.41

個人情報保護監査責任者

トップマネジメントによって組織内部に属する者の中から指名された者であって，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責任及び権限をもつ者。

3.42

従業者

個人情報取扱事業者の組織内にあって直接間接に組織の指揮監督を受けて組織の業務に従事している者などをいい，雇用関係にある従業員（正社員，契約社員，嘱託社員，パート社員，アルバイト社員など）だけでなく，雇用関係にない従事者（取締役，執行役，

理事，監査役，監事，派遣社員など）も含まれる。

3.43

個人情報保護リスク

個人情報の取扱いの各局面（個人情報の取得・入力，移送・送信，利用・加工，保管・バックアップ，消去・廃棄に至る個人情報の取扱いの一連の流れ）における，個人情報の漏えい，滅失又はき損，関連する法令，国が定める指針その他の規範に対する違反，想定される経済的な不利益及び社会的な信用の失墜，本人の権利利益の侵害など，好ましくない影響。

3.44

緊急事態

個人情報保護リスク（3.43）の脅威（3.35）が顕在化した状況。

3.45

個人情報保護

組織が，自らの事業の用に供する個人情報について，その有用性及び個人の権利利益に配慮しつつ，保護すること。

3.46

リスク所有者

リスク（3.9）を運用管理することについて，アカウンタビリティ及び権限をもつ人又は主体。

（JIS Q 27000:2014 の 2.78 参照）