平成 30 年 1 月 12 日（平成 30 年 7 月17日改訂）
一般財団法人日本情報経済社会推進協会(JIPDEC)
プライバシーマーク推進センター

プライバシーマーク付与適格性審査基準

本資料の位置づけ

- 以下に示す項目(以下「審査項目」という。)は，「プライバシーマーク制度基本綱領」第 1 条に定めるプライバシーマーク制度の趣旨を踏まえ，事業者において JIS Q 15001:2017(以下「規格」)に適合した適切な取扱いが行われていることを確認するため，「プライバシーマーク制度基本綱領」第 7 条第4項に定める指針として定めるものである。

本資料の見方

- 審査項目は，規格の附属書 A の項番毎に配列している。審査項目毎に「確認方法・エビデンス」，「留意事項」を付している。「確認方法・エビデンス」は，審査上，事業者において審査項目に示す事項が行われていることを確認するための方法やエビデンスを例示している。「留意事項」では，必要に応じて審査項目や確認方法・エビデンスに解説を付し，読者の理解を助けるようにしている。これらの記載本文に示す項番(「A.*.*」，「B.*.*」等)は，原則として規格の項番を指す。

プライバシーマーク付与適格性審査との関係

- プライバシーマーク付与適格性審査では，事業者における個人情報の取り扱いの状況及びこの審査項目で定められた事項の実施状況について確認を行う。確認の結果，この審査項目で定められた事項が実施されていない場合は，「プライバシーマーク付与適格性審査の実施基準」（以下「実施基準」という。）2.9.1 及び 2.9.2 に基づき，不適合の指摘を行い，不適合として指摘された事項を是正するために実施した処置についての報告を求める。

- 審査項目のうち，トップマネジメントに関する項目は，原則として，実施基準 2.8 に定める現地審査において事業者の代表者に対するインタビューを行うことにより確認する。
- 次の事項に関する審査項目は，原則として，実施基準 2.7 に定める文書審査において確認する。ただし，現地審査においても，必要に応じて内部規程その他の文書化した情報を確認する場合がある。
  - 文書化された内部規程(A.3.3.5a)～o)を含む)の有無
  - 内部向け個人情報保護方針に定める事項
  - 外部向け個人情報保護方針に明記する事項
  - 保有個人データの開示等の請求等に応じる手続きとして定める事項
- 現地審査においては，審査項目が求める事項について，内部規程で定めた手順に基づく実施状況を確認する。

A.3.1.1 一般

No.	審査項目	確認方法・エビデンス
1	A.3.2 から A.3.8 の管理策について，定めた手段に従って承認していること。 又は，承認のために定めた手段が説明できること。	● 個人情報保護管理者等による承認を得たことが確認できる記録 ● 承認のために定めた手段の説明

《留意事項》

- 審査項目１．は，A.3.2 から A.3.8 の管理策毎に個別の手段を設けることを求めるものではない。個別の手段を設けるか否かは，事業者毎の判断による。
- 審査項目１．において，承認のための手順を内部規程として文書化している場合，当該規程も「承認のために定めた手段」のエビデンスとなり得る。
- 確認方法・エビデンスの「個人情報保護管理者等による承認を得たことが確認できる記録」は，電子承認か否かを含め，事業者が定めた手段であればよく，形態については問わない。
- 審査項目１．の「又は，承認のために組織が定めた手段が説明できること。」は，前回審査以降新たに承認する事項が発生しなかった場合に適用される。承認する事項が発生しているにもかかわらず，承認を行っていない場合には適用されない。

A.3.2.1 内部向け個人情報保護方針

No.	審査項目	確認方法・エビデンス
1	トップマネジメントは，個人情報保護目的を説明できること。	● トップマネジメントによる説明
2	内部向け個人情報保護方針を文書化した情報に，A.3.2.1a)～f)に定める事項が含まれていること。	● 内部向け個人情報保護方針(A.3.5.1 a))，又は外部向け個人情報保護方針(A.3.5.1 b))
3	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，組織内に伝達し，必要に応じて，利害関係者が入手可能にするた	● トップマネジメントによる説明 ● 措置

	めの措置を講じていること。	

《留意事項》

- 審査項目１．は，トップマネジメントに対し，組織の目的，個人情報保護目的，内部向け個人情報保護方針との関係を確認するための項目である。
- 審査項目２．は，個人情報保護方針の文面にA.3.2.1 a)～f)の通りの文言の記述を求めるものではない。
- 確認方法・エビデンスの「内部向け個人情報保護方針(A.3.5.1 a))，又は外部向け個人情報保護方針(A.3.5.1 b))」については，外部向け個人情報保護方針(A.3.5.1 b))をエビデンスとする場合は，外部向け個人情報保護方針が内部向け個人情報保護方針に対して矛盾しない場合に限る。

A.3.2.2 外部向け個人情報保護方針

No.	審査項目	確認方法･エビデンス
1	外部向け個人情報保護方針を文書化した情報に，A.3.2.1に規定する内部向け個人情報保護方針の事項が含まれていること。	● 外部向け個人情報保護方針(A.3.5.1 b)) ● 内部向け個人情報保護方針(A.3.5.1 a))
2	外部向け個人情報保護方針を文書化した情報に，次の事項を明記していること。 a) 制定年月日及び最終改正年月日 b) 外部向け個人情報保護方針の内容についての問合せ先	● 外部向け個人情報保護方針(A.3.5.1 b))
3	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，一般の人が入手可能な措置を講じていること。	● トップマネジメントによる説明 ● 措置 (例) ・トップページから外部向け個人情報保護方針へのリンク(ウェブサイトに掲載する場合)

《留意事項》

- 審査項目２．の「最終改正年月日」は，外部向け個人情報保護方針に含まれる事項(A.3.2.1a)～f)に定める事項)を改正する場合に更新されることを原則とする。
- 審査項目２．の「問合せ先」は，外部向け個人情報保護方針の内容の問合せ先のほか，保有個人データの取扱いに関する苦情の申出先(A.3.4.4.3の審査項目１．の d))や苦情の申立て先(A.3.6の審査項目３．)を兼ねてもよい。
- 確認方法・エビデンスの「措置」では，外部向け個人情報保護方針の掲載箇所が一般の人から見て分かりやすく目につきやすいよう配慮されていることを確認する。

A.3.3.1 個人情報の特定

No.	審査項目	確認方法・エビデンス
1	自らの事業の用に供している全ての個人情報を特定するための手順が内部規程として文書化されていること。	● 個人情報を特定する手順に関する規定(A.3.3.5 a))
2	個人情報を管理するための台帳を整備していること。	● 個人情報の特定に関する記録(A.3.5.3 a))
3	台帳には，少なくとも以下の項目が含まれていること。 ・ 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	● 個人情報の特定に関する記録(A.3.5.3 a))
4	台帳の内容を少なくとも年一回，適宜に確認し，最新の状態で維持していること。	● 個人情報の特定に関する記録(A.3.5.3 a))

《留意事項》

- 台帳に含める項目を検討するにあたっては，審査項目３．で示す項目に加えて，B.3.3.1 で例示する事項を参考にすることができる。
- 台帳に含める項目に件数を含める場合，件数は概数でよい。台帳管理の主旨は，１件残らず漏れなく管理していることの証明ではなく，事業者内での個人情報の取扱状況を把握することにある。

A.3.3.2 法令，国が定める指針その他の規範

No.	審査項目	確認方法・エビデンス
1	個人情報の取扱いに関する法令，国が定める指針その他の規範（以下，“法令等”という。）を特定し参照できる手順が内部規程として文書化されていること。	● 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(A.3.3.5 b))
2	法令等を特定し参照していること。	● 法令，国が定める指針その他の規範の特定に関する記録(A.3.5.3 b))

《留意事項》

- 審査項目２．で特定し参照する法令等は，B.3.3.2 を参考にすることができる。これに加えて，業界の関連法令やガイドライン等を，必要に応じて含めることができる。

A.3.3.3 リスクアセスメント及びリスク対策

No.	審査項目	確認方法・エビデンス
1	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が内部規程と	● 個人情報保護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(A.3.3.5 c))

	して文書化されていること。	
2	個人情報保護リスクを特定し，分析していること。	● 個人情報保護リスクの認識，分析及び対策に関する記録(A.3.5.3 c))
3	特定した個人情報保護リスクに対して，現状で実施し得る対策を内部規程として文書化していること。	● 個人情報保護リスクの認識，分析及び対策に関する記録(A.3.5.3 c)) ● 内部規程(A.3.3.5 a)～o)を含む)
4	特定した個人情報保護リスクに対して，現状で実施し得る対策が講じられていること。	● 運用の確認の記録(A.3.5.3 i))
5	未対応部分を残留リスクとして把握し，管理していること。	● 個人情報保護リスクの認識，分析及び対策に関する記録(A.3.5.3 c))
6	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リスク対策を少なくとも年一回，適宜に見直していること。	● 個人情報保護リスクの認識，分析及び対策に関する記録(A.3.5.3 c))

《留意事項》

- 審査項目１．は，特定の手法による手順を求めるものではない。例えば，数値評価によるリスクの把握は手法の一つであるが，これを必須とするものではない。
- 審査項目３．では，「個人情報保護リスクの認識，分析及び対策に関する記録(A.3.5.3 c))」に記載された対策が，「内部規程(A.3.3.5 a)～o)を含む)」に反映されていることを確認する。
- 審査項目４．は，講じる対策の内容により，適合・不適合を判断するものではない。
- 審査項目６．の「見直し」では，リスク分析表等を単に形式的に見直すのではなく，認識された個人情報保護リスク，対策，残留リスクが適切であることを見直すことが重要である。
- 審査項目６．の「適宜に見直し」とは，例えば，事務所の移転や，個人情報の取扱いに関する事故が発生した場合に，個人情報保護リスクの見直しを行うことをいう。

A.3.3.4 資源，役割，責任及び権限

No.	審査項目	確認方法･エビデンス
1	各担当者の役割・権限が内部規程として文書化されていること。	● 組織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(A.3.3.5 d))
2	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する旨が内部規程として文書化されていること。	● 組織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(A.3.3.5 d))
3	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する旨が内部規程として文書化されていること。	● 組織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(A.3.3.5 d))
4	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する旨が内部規程として文書化されていること。	● 組織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(A.3.3.5 d))
5	トップマネジメントが，個人情報保護のための人的資源を説明できること。	● トップマネジメントによる説明 ● 体制 （例） ・体制図
6	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者であること。	● 体制 （例） ・体制図

《留意事項》

- 審査項目１．の「各担当」には，個人情報保護管理者（A.3.3.4 a)），個人情報保護監査責任者（A.3.3.4 b)）のほかに，この規格で求める事項を実施するために必要な担当が含まれる。
- 審査項目３．及び審査項目４．は，「点検に関する規定（A.3.3.5 1)）もエビデンスになり得る。

A.3.3.5 内部規程

No.	審査項目	確認方法・エビデンス
1	次の事項を含む内部規程が文書化されていること。 a) 個人情報を特定する手順に関する規定 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 c) 個人情報保護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 d) 組織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 e) 緊急事態への準備及び対応に関する規定 f) 個人情報の取得，利用及び提供に関する規定 g) 個人情報の適正管理に関する規定 h) 本人からの開示等の請求等への対応に関する規定 i) 教育などに関する規定 j) 文書化した情報の管理に関する規定 k) 苦情及び相談への対応に関する規定 l) 点検に関する規定 m) 是正処置に関する規定 n) マネジメントレビューに関する規定 o) 内部規程の違反に関する罰則の規定	● 内部規程(A.3.3.5a)～o)含む)
2	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適用されるように内部規程を改正していること。	● 内部規程の更新履歴

《留意事項》

- 審査項目１．及び審査項目２．の「内部規程」は，事業者が定める規程体系でよい。内部規程には，手順書レベルの規定も含む。手順書レベルの規定とは,A.3.3.3によって実施した個人情報保護リスクの特定・分析を踏まえて策定した対策を講じる手順を文書化したものをいう。
- 審査項目１．の「o）内部規程の違反に関する罰則の規定」は，就業規則に罰則の規定がある場合もエビデンスとなり得る。

A.3.3.6 計画策定

No.	審査項目	確認方法・エビデンス
1	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，文書化していること。 a）教育実施計画 b）内部監査実施計画	● 計画書(A.3.5.3 d))
2	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計画に，次の事項を含んでいること。 a）実施事項 b）必要な資源 c）責任者 d）達成期限 e）結果の評価方法	● 計画書(A.3.5.3 d))

《留意事項》

- 審査項目１．の「必要な計画」及び審査項目２．のa）～d)の事項については，B.3.3.6を参考にすることができる。
- 審査項目２．の e）は，パフォーマンス評価(A.3.7)における評価方法と連動すると考えられる。例えば，教育において内部規程に基づき受

講者の理解度確認結果を評価し教育内容の見直しを図ることや，内部監査において内部規程に基づきトップマネジメントに結果の報告を行い改善の指示を受けることが考えられる。

A.3.3.7 緊急事態への準備

No.	審査項目	確認方法･エビデンス
1	緊急事態を特定するための手順，及び，特定した緊急事態にどのように対応するかの手順が内部規程として文書化されていること。	● 緊急事態への準備及び対応に関する規定(A.3.3.5 e))
2	緊急事態への準備及び対応に関する規定には，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が含まれていること。	● 緊急事態への準備及び対応に関する規定(A.3.3.5 e))
3	緊急事態への準備及び対応に関する規定には，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が含まれていること。 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するか，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。	● 緊急事態への準備及び対応に関する規定(A.3.3.5 e))
4	緊急事態が発生した場合，定めた手順に従って緊急事態への対応を実施していること。	● 運用の確認の記録(A.3.5.3 i)) (例) ・緊急事態に対応した記録

《留意事項》

- 「緊急事態への準備及び対応に関する規定(A.3.3.5 e))」に含める手順は，B.3.3.7 を参考にすることができる。

A.3.4.1 運用手順

No.	審査項目	確認方法・エビデンス
1	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，運用の手順が内部規程として文書化されていること。	● A.3.3.5f)～i)及び o)に該当する内部規程

《留意事項》

- 審査項目１．の「運用の手順」には手順書レベルの規定も含まれる。
- 確認方法・エビデンスの「A.3.3.5f)～i)及び o)に該当する内部規程」は，実施及び運用（A.3.4）に関する手順を指す。

A.3.4.2.1 利用目的の特定

No.	審査項目	確認方法・エビデンス
1	個人情報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取扱いを行っていること。	● 個人情報の特定に関する記録(A.3.5.3 a)) ● 利用目的の特定に関する記録(A.3.5.3 e)) ・通知又は公表の記録(A.3.4.2.4) ・本人に明示した書面(A.3.4.2.5)
2	利用目的は，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していること。	● 利用目的の特定に関する記録(A.3.5.3 e)) ・通知又は公表の記録(A.3.4.2.4) ・本人に明示した書面(A.3.4.2.5)

《留意事項》

- 審査項目１．では，「通知又は公表の記録(A.3.4.2.4)」「本人に明示した書面(A.3.4.2.5)」に記載された利用目的が，「個人情報の特定に関

する記録(A.3.5.3 a))」としての台帳(A.3.3.1)に特定された利用目的の範囲内であることを確認する。

- 審査項目２．は,本人から見た分かりやすさに関する審査項目である。

A.3.4.2.2 適正な取得

No.	審査項目	確認方法・エビデンス
1	定めた手順に従って，個人情報を適正に取得していること。	● 個人情報の取得，利用及び提供に関する規定(A.3.3.5 f)) ● 通知又は公表の記録(A.3.4.2.4) ● 本人に明示した書面(A.3.4.2.5) ● 個人情報の特定に関する記録(A.3.5.3 a))

《留意事項》

- 確認方法・エビデンスの「個人情報の特定に関する記録(A.3.5.3 a))」としての台帳(A.3.3.1)により，個人情報の取得の有無を確認する。「通知又は公表の記録(A.3.4.2.4)」「本人に明示した書面(A.3.4.2.5)」が在ることにより，「個人情報の取得，利用及び提供に関する規定(A.3.3.5 f))」に基づき取得されたことを確認する。

A.3.4.2.3 要配慮個人情報

No.	審査項目	確認方法・エビデンス
1	新たに要配慮個人情報を取得,利用又は提供並びに要配慮個人情報のデータを提供する場合，あらかじめ書面による本人の同意を得ていること。	● 本人の同意書面
2	要配慮個人情報を取得,利用する際，書面による本人の同意を得ることを要しないときは，以下の場合に限定していること。	● 個人情報の特定に関する記録(A.3.5.3 a)) ● 同意を得ていない要配慮個人情報が有る場合，当該要配慮個人

	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	情報が A.3.4.2.3 のただし書き a)～e)に該当することの説明
3	要配慮個人情報を提供する際，書面による本人の同意を得ることを要しないときは，A.3.4.2.3 のただし書き a)～d)の場合に限定していること。	● 個人情報の特定に関する記録(A.3.5.3 a)) ● 同意を得ていない要配慮個人情報が有る場合，当該要配慮個人情報が A.3.4.2.3 のただし書き a)～d)に該当することの説明

《留意事項》

- 審査項目２．及び審査項目３．は，「個人情報の特定に関する記録(A.3.5.3 a))」としての台帳(A.3.3.1)により，台帳に記載されているが書面による本人の同意の取得が行われていない要配慮個人情報の有無を確認する。確認の結果，本人の同意の取得を行っていない場合は，本人の同意を得ずに取得した要配慮個人情報が A.3.4.2.3 のただし書きに該当することを確認する。

A.3.4.2.4 個人情報を取得した場合の措置

No.	審査項目	確認方法・エビデンス

1	個人情報を取得する場合，個人情報の取得の場面に応じて，あらかじめ，その利用目的を公表している，又は取得後速やかにその利用目的を本人に通知又は公表していること。	● 通知又は公表の記録(A.3.4.2.4)
2	本人への利用目的の通知又は公表を要しないのは，以下の場合に限定していること。 a) 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該組織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するか，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場合 d) 取得の状況からみて利用目的が明らかであると認められる場合	● 通知又は公表の記録(A.3.4.2.4) ● 個人情報の特定に関する記録(A.3.5.3 a)) ● 本人に通知又は公表せずに取得した個人情報が有る場合，A.3.4.2.4 のただし書きに該当することの説明

《留意事項》

- 審査項目１．で通知又は公表する利用目的は，特定された利用目的の範囲内である必要がある（A.3.4.2.1 の審査項目１．参照)。
- 確認方法・エビデンスの「通知又は公表の記録(A.3.4.2.4)」には，取得の場面に応じた本人への通知書面又は公表物も含まれる。
- 審査項目２．は，「通知又は公表の記録(A.3.4.2.4)」及び，「個人情報の特定に関する記録(A.3.5.3 a))」としての台帳(A.3.3.1)により，台帳に記載されているが利用目的の通知又は公表が行われていない個人情報の有無を確認する。確認の結果，通知又は公表を行っていない場合は，本人に通知又は公表せずに取得した個人情報が A.3.4.2.4 のただし書きに該当することを確認する。

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

No.	審査項目	確認方法・エビデンス
1	本人から直接書面によって取得する場合，A.3.4.2.4 の措置を講じていること。	● 通知又は公表の記録(A.3.4.2.4)　等
2	本人から，書面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の事項を，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ていること。 a) 組織の名称又は氏名 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こと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，及び属性 －個人情報の取扱いに関する契約がある場合はその旨 e) 個人情報の取扱いの委託を行うことが予定される場合には，その旨 f) A.3.4.4.4～A.3.4.4.7 に該当する場合には，その請求等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	● 本人に明示した書面(A.3.4.2.5) ● 本人の同意書面

	h) 本人が容易に知覚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	
3	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ないのは，以下の場合に限定していること。 ・人の生命，身体若しく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 a)～d)のいずれかに該当する場合	● 本人に明示した書面(A.3.4.2.5) ● 個人情報の特定に関する記録(A.3.5.3 a)) ● 本人に明示し，本人の同意を得ずに取得した個人情報が有る場合，当該 A.3.4.2.5 のただし書きに該当することの説明

《留意事項》

- 審査項目２．で明示する利用目的は，特定された利用目的の範囲内である必要がある（A.3.4.2.1 の審査項目１．参照)。
- 確認方法・エビデンスの「本人に明示した書面(A.3.4.2.5)」は，取得の手段(ウェブサイト，手渡し等)に応じた書面を確認する。
- 審査項目３．は，「本人に明示した書面(A.3.4.2.5)」及び，「個人情報の特定に関する記録(A.3.5.3 a))」としての台帳(A.3.3.1)により，台帳に記載されているが本人への明示及び同意の取得が行われていない個人情報の有無を確認する。確認の結果，本人への明示及び同意の取得を行っていない場合は，当該個人情報が A.3.4.2.5 のただし書きに該当することを確認する。

A.3.4.2.6 利用に関する措置

No.	審査項目	確認方法・エビデンス
1	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していること。	● 通知又は公表の記録(A.3.4.2.4)，又は本人に明示した書面(A.3.4.2.5) ● 個人情報の特定に関する記録(A.3.5.3 a))
2	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，本人の同意を得ていること。	● 本人への通知書面(A.3.4.2.6) ● 本人の同意書面

3	本人の同意を得ることを要しないのは，A.3.4.2.3 の a)～d)のいずれかに該当する場合に限定していること。	• 本人への通知書面(A.3.4.2.6) • 個人情報の特定に関する記録(A.3.5.3 a)) • 同意を得ずに個人情報を利用している場合，当該利用が A.3.4.2.6 のただし書き該当する説明

《留意事項》

- 審査項目１．では，「通知又は公表の記録(A.3.4.2.4)，又は本人に明示した書面(A.3.4.2.5) 」に記載された利用目的が，「個人情報の特定に関する記録(A.3.5.3 a)」としての台帳(A.3.3.1)に記載した利用目的の範囲を超えないことを確認する。
- 審査項目３．は，「本人への通知書面(A.3.4.2.6)」及び，「個人情報の特定に関する記録(A.3.5.3 a))」としての台帳(A.3.3.1)により，台帳に記載されているが本人への通知及び同意の取得が行われていない個人情報の有無を確認する。確認の結果，本人への通知及び同意の取得を行っていない場合は，当該個人情報が A.3.4.2.6 のただし書きに該当することを確認する。

A.3.4.2.7 本人に連絡又は接触する場合の措置

No.	審査項目	確認方法・エビデンス
1	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内容の事項，及び取得方法を通知し，本人の同意を得ていること。	• 本人への通知書面(A.3.4.2.7) • 本人の同意書面
2	本人に通知し，本人の同意を得ることを要しない場合は，以下の場合に限定していること。 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	• 本人への通知書面(A.3.4.2.7) • 個人情報の特定に関する記録(A.3.5.3 a)) • 同意を得ずに本人に連絡又は接触している場合，当該連絡又は接触が A.3.4.2.7 のただし書きに該当することの説明

	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，本人の同意を得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，共同して利用する者が，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(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 －共同して利用する者の利用目的 －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，本人に連絡又は接触するとき 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	
3	共同して利用する者から個人情報を取得する場合であって，共同して利用する者がA.3.4.2.7d)の措置を講じない場合，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内容の事項，及び取得方法を通知し，本人の同意を得ていること。	• 本人への通知書面(A.3.4.2.7) • 本人の同意書面

《留意事項》

- 審査項目１．の通知及び同意の取得については，規格は書面による通知及び書面による同意の取得に限定していないため，口頭によることも考えられる。この場合，審査項目１．に示す事項(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，及び取得方法)を本人に通知していることを確認する。例えば，コールセンター業務において，オペレーターが顧客に通知し顧客の同意を取得する場合のマニュアルが整備すること等が考えられる。
- 審査項目２．は，「本人への通知書面(A.3.4.2.7)」及び，「個人情報の特定に関する記録(A.3.5.3 a))」としての台帳(A.3.3.1)により，台帳に記載されているが本人への通知及び同意の取得が行われていない個人情報の有無を確認する。確認の結果，本人への通知及び同意の取得を行っていない場合は，当該個人情報が A.3.4.2.7 のただし書きに該当することを確認する。
- 審査項目３．は，審査項目２．において d)に該当しない場合の審査項目である。

A.3.4.2.8 個人データの提供に関する措置

No.	審査項目	確認方法・エビデンス
1	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)に示す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，本人の同意を得ていること。	● 本人への通知書面(A.3.4.2.8) ● 本人の同意書面
2	本人に通知し，本人の同意を得ることを要しない場合は，以下の場合に限定していること。 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	● 本人への通知書面(A.3.4.2.8) ● 個人情報の特定に関する記録(A.3.5.3 a)) ● 同意を得ずに第三者に提供している場合，当該提供が A.3.4.2.8 のただし書きに該当することの説明

	の措置を講じているとき 1) 第三者への提供を利用目的とすること 2) 第三者に提供される個人データの項目 3) 第三者への提供の手段又は方法 4) 本人の請求など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 5) 取得方法 6) 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データ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) 個人データ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	
3	個人データを共同利用している場合，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こと。	• 共同利用についての契約(A.3.4.2.8 f))

《留意事項》

- 個人データに対する審査項目であっても，A.3.3.1 において特定した個人情報については，個人データと同等に取り扱う。
- 審査項目１．の通知及び同意の取得については，書面による通知及び書面による同意の取得が原則である。
- 審査項目２．は，「本人への通知書面(A.3.4.2.8)」及び，「個人情報の特定に関する記録(A.3.5.3 a))」としての台帳(A.3.3.1)により，台帳に記載されているが本人への通知及び同意の取得が行われていない個人情報の有無を確認する。確認の結果，本人への通知及び同意の取得を行っていない場合は，当該個人情報が A.3.4.2.8 のただし書きに該当することを確認する。
- 審査項目３．は，審査項目２．において f)に該当する場合の審査項目である。

A.3.4.2.8.1 外国にある第三者への提供の制限

No.	審査項目	確認方法・エビデンス
1	**外国にある第三者に個人データを提供する場合，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ていること。**	● **本人の同意書面**
2	**本人の同意を要しないのは，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に限定していること。**	● **本人の同意書面** ● **個人情報の特定に関する記録(A.3.5.3 a))** ● **同意を得ずに外国にある第三者に提供している場合，当該提供が A.3.4.2.8.1 のただし書きに該当することの説明**

《留意事項》

- 個人データに対する審査項目であっても，A.3.3.1 において特定した個人情報については，個人データと同等に取り扱う。
- 審査項目２．は，「本人の同意書面」及び，「個人情報の特定に関する記録(A.3.5.3 a))」としての台帳(A.3.3.1)により，台帳に記載されているが本人の同意の取得が行われていない個人情報の有無を確認する。確認の結果，本人の同意の取得を行っていない場合は，当該個人情報が A.3.4.2.8.1 のただし書きに該当することを確認する。

A.3.4.2.8.2 第三者提供に係る記録の作成など

No.	審査項目	確認方法・エビデンス
1	個人データを第三者に提供した場合，記録を作成，保管していること。	● 作成した記録(書面又は電子データ。記録すべき事項がログ，IP アドレスなどの一定の情報を分析することによって明らかになる場合には，その状態。)
2	記録を作成しなかったのは，A.3.4.2.3 の a)～d) のいずれかに該当する場合，又は以下の場合に限定していること。 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の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者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得る状態に置いているとき。	● 個人データの第三者提供に係る記録の作成及び保管を行わない場合，当該提供が A.3.4.2.8.2 のただし書き該当することの説明

《留意事項》

- 個人データに対する審査項目であっても，A.3.3.1 において特定した個人情報については，個人データと同等に取り扱う。
- 審査項目１．の「記録」に含める事項については，B.3.4.2.8.2 を参考にすることができる。

A.3.4.2.8.3 第三者提供を受ける際の確認など

No.	審査項目	確認方法・エビデンス
1	第三者から個人データの提供を受けるに際しては，確認を行った記録を作成し，保管していること。	● 作成した記録
2	確認の記録を作成，保管していないのは，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に限定していること。	● 第三者から個人データの提供を受けるに際しての記録の作成及び保管を行わない場合，提供を受けることが A.3.4.2.8.3 のただし書きに該当することの説明

《留意事項》

- 個人データに対する審査項目であっても，A.3.3.1 において特定した個人情報については，個人データと同等に取り扱う。
- 審査項目１．の「記録」に含める事項については，B.3.4.2.8.3 を参考にすることができる。

A.3.4.2.9 匿名加工情報

No.	審査項目	確認方法・エビデンス
1	匿名加工情報の取扱いを行うか否かの方針が存在すること。	● 方針の有無
2	匿名加工情報を取り扱う場合，匿名加工情報の取扱いの手順を内部規程として文書化していること。	● 個人情報の取得，利用及び提供に関する規定(A.3.3.5 f）)

《留意事項》

- 審査項目１．の「匿名加工情報の取扱いを行うか否かの方針」については，B.3.4.2.9 を参考にすることができる。
- 確認方法・エビデンスの「方針の有無」とは，方針を文書化した情報を求めるものではなく，トップマネジメント等が方針を説明することでもよい。
- 審査項目２．は，審査項目１．で匿名加工情報を取り扱う方針がある場合に確認を行う。

A.3.4.3.1 正確性の確保

No.	審査項目	確認方法･エビデンス
1	個人データを，正確，かつ，最新の状態で管理していること。	● 個人情報の適正管理に関する規定(A.3.3.5 g))に定めた記録 (例) ・誤入力チェック記録 ・訂正記録 ・更新記録 ・データのバックアップ記録 ・消去記録 など
2	利用する必要がなくなった個人データの消去を含む管理を､規定に基づいて適切に行っていること。	● 個人情報の特定に関する記録(A.3.5.3 a)) ● 個人情報の適正管理に関する規定(A.3.3.5 g))に定めた記録

《留意事項》

- 個人データに対する審査項目であっても，A.3.3.1 において特定した個人情報については，個人データと同等に取り扱う。
- 審査項目２．では，「個人情報の特定に関する記録(A.3.5.3 a))」としての台帳(A.3.3.1)に記載された保管期限が過ぎた個人情報について，「適正管理に関する規定(A.3.3.5 g))に定めた記録」(利用する必要がなくなったデータの消去記録 など)を確認する。

A.3.4.3.2 安全管理措置

No.	審査項目	確認方法･エビデンス
1	取り扱う個人情報の個人情報保護リスクに応じた安全管理措置を	● 個人情報保護リスクの認識，分析及び対策に関する記録

	講じていること。	(A.3.5.3 c)) ● 内部規程(A.3.3.5a)～o)含む) ● 内部規程に定めた記録 ● 内部規程に定めた措置の実施状況

《留意事項》

- 審査項目１．は,「個人情報保護リスクの認識，分析及び対策に関する記録(A.3.5.3 c))」に記載された対策が,「内部規程(A.3.3.5 a)～o)を含む)」に反映されていることを前提としている（A.3.3.3 審査項目３．参照)。
- 確認方法・エビデンスの「内部規程に定めた措置の実施状況」は,現地審査時に現場を視察することにより確認する。
- 附属書Ｃは安全管理措置を決定するための参考であり,審査項目１．は附属書Ｃに示す事項を一律に実施するよう求めるものではない。

A.3.4.3.3　従業者の監督

No.	審査項目	確認方法･エビデンス
1	個人データを取扱う従業者に対して必要かつ適切な監督を行っていること。	● 個人情報の適正管理に関する規定(A.3.3.5 g))に定めた管理手段 (例) ・従業者との個人情報の非開示契約 ・ビデオ及びオンラインによる従業者のモニタリング など ● 内部規程の違反に関する罰則の規定(A.3.3.5 o)) (例) ・就業規則 など

《留意事項》

- 個人データに対する審査項目であっても，A.3.3.1 において特定した個人情報については，個人データと同等に取り扱う。

A.3.4.3.4　委託先の監督

No.	審査項目	確認方法･エビデンス
1	委託先選定基準に基づいて委託先を選定していること。	● 委託先の選定記録
2	委託先と，特定した利用目的の範囲内で委託契約を締結していること。	● 委託した個人情報の利用目的が確認できる記録 （例） ・個人情報の特定に関する記録(A.3.5.3 a)) ・委託契約書
3	次に示す事項が盛り込まれた契約を締結していること。 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) 個人データの取扱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，定期的に，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	● 委託契約書
4	全ての委託先が漏れなく特定されていること。	● 個人情報の取扱いを委託している事業者を確認できる記録 （例） ・委託先の選定記録 ・委託先一覧

		・委託契約書
5	委託契約書が当該個人データの保有期間にわたって保存されていること。	● 委託した個人情報の保有期間が確認できる記録 （例） ・個人情報の特定に関する記録(A.3.5.3 a)) ・委託契約書
6	委託契約に基づき，委託先を適切に監督していること。	● 委託契約書 ● 委託先の監督に関する記録 （例） ・A.3.4.3.4 の a)～h)の実施の記録

《留意事項》

- 個人データに対する審査項目であっても，A.3.3.1 において特定した個人情報については，個人データと同等に取り扱う。
- 審査項目１．は，選定に先立ち委託先選定基準が「適正管理に関する規定(A.3.3.5 g))」に規定されていることが前提となる。
- 審査項目２．では，委託する業務の範囲が，委託する個人データの利用目的を超えていないことを確認する。委託する業務の範囲は，委託契約書により確認する。委託した個人データの利用目的は，「個人情報の特定に関する記録(A.3.5.3 a))」としての台帳等により確認する。
- 審査項目３．の b)，c)に含まれる事項については，B.3.4.3.4 を参考にすることができる。
- 審査項目５．では，委託契約期間終了後の個人データについて,その保有期間中の委託契約書の有無を確認する。個人データの保有期間は，「個人情報の特定に関する記録(A.3.5.3 a))」としての台帳等で確認する。
- 審査項目６．は，委託者が，委託契約書に規定された事項に基づき，委託先に対して契約内容が遵守されていることの確認を行っていることを確認するための審査項目である。よって，確認方法・エビデンスの「委託先の監督に関する記録」は，委託契約書に規定された事項に基づき確認する。

A.3.4.4.1　個人情報に関する権利

No.	審査項目	確認方法･エビデンス

1	本人から開示等の請求等を受け付けた場合，政令で定める期間以内に消去する個人情報も含めて，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ていること。	● 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，利用の停止又は消去，第三者提供の停止)の請求等への対応記録(A.3.5.3 f))
2	保有個人データに当たらないものとして，次に掲げるいずれかに限定していること。 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のあるもの 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及び秩序維持に支障が及ぶおそれのあるもの	● 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，利用の停止又は消去，第三者提供の停止)の請求等への対応記録(A.3.5.3 f)) ● 開示等の請求等を受け付けたが対応していない保有個人データが有る場合，a)～d)のただし書きに該当していることの説明

《留意事項》

- 保有個人データに対する審査項目であっても，A.3.4.4.1 に定めた個人情報については，保有個人データと同等に取り扱う。
- 審査項目２．は，審査項目１．で開示等の請求等が発生したが対応していないものについて，A.3.4.4.1 の a)～d)のいずれかに該当することを確認する。

A.3.4.4.2　開示等の請求等に応じる手続

No.	審査項目	確認方法・エビデンス

1	保有個人データの開示等の請求等に応じる手続として，次の事項が文書化されていること。 a) 開示等の請求等の申出先 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等の請求等の方式 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 d) A.3.4.4.4 又は A.3.4.4.5 による手数料(定めた場合に限る。)の徴収方法	● 本人からの開示等の請求等への対応に関する規定(A.3.3.5 h))
2	保有個人データの開示等の請求等に応じる手続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配慮していること。	● 配慮している事項の説明
3	本人からの請求などに応じる場合に，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，その額を定めていること。	● 手数料の額を定めた根拠の説明

《留意事項》

- 保有個人データに対する審査項目であっても，A.3.4.4.1 に定めた個人情報については，保有個人データと同等に取り扱う。
- 審査項目１．の「代理人」にあたる者については，B.3.4.4.2 を参考にすることができる。

A.3.4.4.3　保有個人データに関する事項の周知など

No.	審査項目	確認方法・エビデンス
1	保有個人データに関し，次の事項を本人の知り得る状態(本人の請求などに応じて遅滞なく回答する場合を含む。)に置いているこ	● 保有個人データに関する事項を周知している措置 (例)

	と。 a) 組織の氏名又は名称 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) 全ての保有個人データの利用目的(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扱いに関する苦情の申出先 e) 当該組織が認定個人情報保護団体の対象事業者である場合にあっては，当該認定個人情報保護団体の名称及び苦情の解決の申出先 f) A.3.4.4.2によって定めた手続	・本人から当該保有個人データに関し求めがあった場合の対応に関する事項が表示されているホームページ，パンフレット ・A.3.4.4.3a)～f)に関する問い合わせに対する回答手順 など

《留意事項》

- 保有個人データに対する審査項目であっても，A.3.4.4.1に定めた個人情報については，保有個人データと同等に取り扱う。

A.3.4.4.4　保有個人データの利用目的の通知

No.	審査項目	確認方法・エビデンス
1	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，遅滞なくこれに応じていること。	● 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，利用の停止又は消去，第三者提供の停止)の請求等への対応記録(A.3.5.3 f))
2	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であって，利用目的の通知を必要としないのは以下の場合に限定していること。 ・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	● 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，利用の停止又は消去，第三者提供の停止)の請求等への対応記録(A.3.5.3 f)) ● 利用目的の通知を求められたが通知をしていない保有個人デ

	・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	ータがある場合，A.3.4.4.4 のただし書きに該当していることの説明
3	A.3.4.4.4 のただし書きのいずれかに該当する場合，本人に遅滞なくその旨を通知するとともに，理由を説明していること。	● 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，利用の停止又は消去，第三者提供の停止)の請求等への対応記録(A.3.5.3 f))

《留意事項》

- 保有個人データに対する審査項目であっても，A.3.4.4.1 に定めた個人情報については，保有個人データと同等に取り扱う。
- 審査項目２．及び審査項目３．は，審査項目１．の確認の結果，保有個人データについて，利用目的の通知に応じなかった場合に確認する。

A.3.4.4.5　保有個人データの開示

No.	審査項目	確認方法・エビデンス
1	本人から，当該本人が識別される保有個人データの開示の請求を受けた場合，法令の規定によって特別の手続が定められている場合を除き，本人に対し，遅滞なく書面によって開示していること。	● 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，利用の停止又は消去，第三者提供の停止)の請求等への対応記録(A.3.5.3 f))
2	本人から，当該本人が識別される保有個人データの開示の請求を受けた場合であって，全部又は一部の開示を必要としないのは以下の場合に限定していること。 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) 当該組織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	● 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，利用の停止又は消去，第三者提供の停止)の請求等への対応記録(A.3.5.3 f)) ● 開示の請求を受けたが開示していない保有個人データがある場合，A.3.4.4.5 のただし書きに該当していることの説明
3	A.3.4.4.5 のただし書きのいずれかに該当する場合，本人に遅滞な	● 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

	くその旨を通知するとともに，理由を説明していること。	の訂正，追加又は削除，利用の停止又は消去，第三者提供の停止)の請求等への対応記録(A.3.5.3 f））

《留意事項》

- 保有個人データに対する審査項目であっても，A.3.4.4.1に定めた個人情報については，保有個人データと同等に取り扱う。
- 審査項目２．及び審査項目３．は，審査項目１．の確認の結果，保有個人データの開示の請求に応じなかった場合に確認する。

A.3.4.4.6　保有個人データの訂正，追加又は削除

No.	審査項目	確認方法・エビデンス
1	本人から，当該本人が識別される保有個人データの訂正等(訂正，追加又は削除)の請求を受けた場合，法令の規定により特別の手続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っていること。	● 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，利用の停止又は消去，第三者提供の停止)の請求等への対応記録(A.3.5.3 f））
2	本人から保有個人データの訂正等の請求を受けて訂正等を行った場合は，その旨及びその内容を本人に遅滞なく通知していること。	● 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，利用の停止又は消去，第三者提供の停止)の請求等への対応記録(A.3.5.3 f））
3	本人から保有個人データの訂正等の請求を受けたが応じなかった場合，その旨及びその理由を本人に遅滞なく通知していること。	● 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，利用の停止又は消去，第三者提供の停止)の請求等への対応記録(A.3.5.3 f））

《留意事項》

- 保有個人データに対する審査項目であっても，A.3.4.4.1に定めた個人情報については，保有個人データと同等に取り扱う。
- 審査項目２．は，審査項目１．の確認の結果，保有個人データの訂正等の請求に応じた場合に確認する。

- 審査項目３．は，審査項目１．の確認の結果，保有個人データの訂正等の請求を受けたがこれに応じなかった場合に確認する。

A.3.4.4.7　保有個人データの利用又は提供の拒否権

No.	審査項目	確認方法・エビデンス
1	本人から当該本人が識別される保有個人データの利用停止等(利用の停止，消去又は第三者への提供の停止)の請求に応じていること。	● 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，利用の停止又は消去，第三者提供の停止)の請求等への対応記録(A.3.5.3 f）)
2	本人からの当該本人が識別される保有個人データの利用停止等の請求に応じた場合，遅滞なくその旨を本人に通知していること。	● 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，利用の停止又は消去，第三者提供の停止)の請求等への対応記録(A.3.5.3 f）)
3	本人からの当該本人が識別される保有個人データの利用停止等の請求に応じなかった場合は A.3.4.4.5 の a)～c)に該当する場合に限定していること。	● 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，利用の停止又は消去，第三者提供の停止)の請求等への対応記録(A.3.5.3 f）) ● 保有個人データの利用停止等の請求を受けていない保有個人データがある場合，A.3.4.4.5 のただし書きに該当していることの説明
4	A.3.4.4.5 の a)～c)のいずれかに該当する場合，本人に遅滞なくその旨を通知するとともに，理由を説明していること。	● 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，利用の停止又は消去，第三者提供の停止)の請求等への対応記録(A.3.5.3 f）)

《留意事項》

- 保有個人データに対する審査項目であっても，A.3.4.4.1 に定めた個人情報については，保有個人データと同等に取り扱う。
- 審査項目２．は，審査項目１．の確認の結果，保有個人データの利用停止等の請求に応じた場合に確認する。
- 審査項目３．及び審査項目４．は，審査項目１．の確認の結果，保有個人データの利用停止等の請求に応じなかった場合に確認する。

A.3.4.5　認識

No.	審査項目	確認方法・エビデンス
1	全ての従業者に対して，少なくとも年一回，適宜に教育を実施する手順が内部規程として文書化されていること。	● 教育などに関する規定(A.3.3.5 i))
2	教育などに関する規定には，受講者の理解度を確認する手順が含まれていること。	● 教育などに関する規定(A.3.3.5 i))
3	教育実施計画(A.3.3.6 a))に従って教育を実施していること。	● 計画書(A.3.5.3 d)) ● 教育などの実施記録(A.3.5.3 g))
4	全ての従業者に対して，a)～d)の内容を認識させていること。 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	● 使用した教材等
5	受講者の理解度確認を実施していること。	● 教育などの実施記録(A.3.5.3 g))

《留意事項》

- 審査項目１．及び審査項目３．の「従業者」は，規格が定義する「従業者」(3.42)を指す。

- 審査項目３．は，少なくとも年１回，適宜に教育を実施していることを含む。

A.3.5.1 文書化した情報の範囲

No.	審査項目	確認方法･エビデンス
1	個人情報保護マネジメントシステムの基本となる次の要素に対応する書面があること。 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 d) 内部規程に定める手順上で使用する様式 e) 計画書 f) この規格が要求する記録及び組織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	● 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記述したa)～f)に関する書面 (例) ・内部向け個人情報保護方針を文書化した情報 ・外部向け個人情報保護方針を文書化した情報 ・内部規程（A.3.3.5a)～o)を含む）を文書化した情報及び当該内部規程で規定された様式一式 ・計画書（A.3.5.3　d）） ・記録各種 など

《留意事項》

- 審査項目１．は，a)～f)に該当する書面の有無を確認するための項目である。

A.3.5.2 文書化した情報(記録を除く。)の管理

No.	審査項目	確認方法･エビデンス
1	規格が要求する全ての文書化した情報(記録を除く。)を管理する手順が，次の事項を含む内部規程として文書化されていること。	● 文書化した情報の管理に関する規定(A.3.3.5　j))

	a) 文書化した情報(記録を除く。)の発行及び改正に関すること b) 文書化した情報(記録を除く。)の改正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	文書化した情報(記録を除く。)の管理を実施していること。	● 文書化した情報の更新履歴 ● 文書化した情報の管理状況 ● 文書化した情報を従業者が参照する環境
3	文書化した情報(記録を除く。)は，次の事項を確実にするよう管理されていること。 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状況

《留意事項》

- 確認方法・エビデンスの「文書化した情報の管理状況」「文書化した情報を従業者が参照する環境」は，現場における文書化した情報の管理状況を視察することにより確認する。
- 審査項目３．は，文書化した情報を管理する手順を維持していることを確認するための審査項目である。

A.3.5.3 文書化した情報のうち記録の管理

No.	審査項目	確認方法・エビデンス
1	個人情報保護マネジメントシステム及びこの規格の要求事項への適合を実証するために必要な記録の管理についての手順が内部規	● 文書化した情報の管理に関する規定(A.3.3.5　j))

	程として文書化されていること。	
2	次の事項を含む必要な記録を作成していること。 a) 個人情報の特定に関する記録 b) 法令，国が定める指針及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，利用の停止又は消去，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	● a)～l)の記録
3	記録は，次の事項を確実にするよう管理されていること。 a) 記録が，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) 記録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)。	● a)～l)の記録の管理状況

《留意事項》

- 審査項目２．の g)，j)については，B.3.5.3.を参考にすることができる。
- 審査項目３．は，記録を管理する手順を維持していることを確認するための審査項目である
- 確認方法・エビデンスの「a)～l)の記録の管理状況」は，現場における記録の管理状況を視察することにより確認する。

A.3.6 苦情及び相談への対応

No.	審査項目	確認方法・エビデンス
1	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が内部規程として文書化されていること。	● 苦情及び相談への対応に関する規定(A.3.3.5　k))
2	苦情及び相談への対応を実施していること。	● 苦情及び相談への対応記録(A.3.5.3 h))
3	苦情の申立て先が，本人にとって明確であること。	● 保有個人データに関する事項を周知している措置(A.3.4.4.3)
4	認定個人情報保護団体の対象事業者となっている場合は，当該団体の苦情解決の申し出先も明示していること。	● 保有個人データに関する事項を周知している措置(A.3.4.4.3)
5	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ための体制の整備を行っていること。	● 体制 （例） ・体制図

《留意事項》

- 審査項目３．は，A.3.4.4.3 の d）について，苦情の申立て先を明確にする措置が取られていることにより確認する。
- 審査項目４．は，A.3.4.4.3 の e）について，認定個人情報保護団体の苦情解決の申し出先を明確にする措置が取られていることにより確認する。

A.3.7.1 運用の確認

No.	審査項目	確認方法・エビデンス
1	各部門及び階層の管理者が定期的に，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ことを確認する手順，及び次の事項を含む是正処置の手順が内部規程として文書化されていること。 a) 不適合の内容を確認する。 b) 不適合の原因を特定し，是正処置を立案する。 c) 期限を定め，立案された処置を実施する。 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。	● 点検に関する規定(A.3.3.5 l))
2	運用の確認を実施していること。	● 運用の確認の記録(A.3.5.3 i))
3	運用の確認において，不適合が確認された場合は，是正処置を行っていること。	● 運用の確認の記録(A.3.5.3 i))
4	個人情報保護管理者は，定期的に，及び適宜にトップマネジメントに運用の確認の状況を報告していること。	● 運用の確認の記録(A.3.5.3 i))

《留意事項》

- 審査項目１．で求める手順は，A.3.7.2（内部監査）とは異なり，各部門及び階層における手順を指す。
- 審査項目１．及び審査項目３.は，A.3.7.1 が求める是正処置も含めた手順の確立及び実施状況を確認するための審査項目である。是正処置に求められる事項は，A.3.8 を踏まえている。
- 審査項目２．は，定期的に，及び適宜に確認していることを含む。

A.3.7.2 内部監査

No.	審査項目	確認方法・エビデンス
1	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が内部規程として文書化されていること。	● 点検に関する規定(A.3.3.5 l))
2	内部監査実施計画(A.3.3.6 b))に従って，個人情報保護マネジメントシステムのこの規格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の監査を，少なくとも年一回，適宜に実施していること。	● 計画書(A.3.5.3 d)) ● 内部監査報告書(A.3.5.3 j))
3	内部監査の実施にあたっては，内部規程とこの規格との適合状況を監査していること。	● 監査項目 （例） ・監査チェックリスト
4	内部監査の実施にあたっては，運用状況の監査を実施していること。	● 監査項目 （例） ・監査チェックリスト
5	監査員は，自己の所属する部署の内部監査を実施していないこと。	● 計画書(A.3.5.3 d)) ● 内部監査報告書(A.3.5.3 j))
6	個人情報保護監査責任者は，監査報告書を作成し，トップマネジメントに報告していること。	● 計画書(A.3.5.3 d)) ● 内部監査報告書(A.3.5.3 j))

《留意事項》

- 確認方法・エビデンスの「監査項目」とは，監査員が監査を行うにあたり確認する具体的な項目をいう。
- 審査項目６．は，A.3.3.4 を踏まえた審査項目である。

A.3.7.3 マネジメントレビュー

No.	審査項目	確認方法･エビデンス
1	マネジメントレビューを実施する手順が内部規程として文書化されていること。	● マネジメントレビューに関する規定(A.3.3.5 n))
2	少なくとも年一回，適宜にマネジメントレビューを実施していること。	● マネジメントレビューの記録(A.3.5.3 l))
3	マネジメントレビューを実施するにあたり，次の事項がインプットされていること。 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) 個人情報の取扱いに関する法令，国の定める指針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) 組織の事業領域の変化 g) 内外から寄せられた改善のための提案	● マネジメントレビューの記録(A.3.5.3 l))
4	マネジメントレビュー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が含まれていること。	● マネジメントレビューの記録(A.3.5.3 l)) ● トップマネジメントによる説明

《留意事項》

- 審査項目３．は，常に a)～g)の事項すべてを見直しの材料にする必要はない。a)～g)の事項が発生しないことを把握することもインプットといえる。
- 審査項目４．は，A.3.7.3 のマネジメントレビューの結果に対しトップマネジメントが判断を行っていることを確認するための審査項目である。

A.3.8 是正処置

No.	審査項目	確認方法・エビデンス
1	不適合に対する是正処置を確実に実施するための責任及び権限を定める手順が次の事項を含む内部規程として文書化されていること。 a) 不適合の内容を確認する。 b) 不適合の原因を特定し，是正処置を立案する。 c) 期限を定め，立案された処置を実施する。 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。	● 是正処置に関する規定(A.3.3.5 m))
2	不適合が明らかになった場合，a)～e)の事項を実施していること。	● 是正処置の記録(A.3.5.3 k))
3	是正処置の立案にあたっては，発見された不適合が他の所でも発生しないようにするための措置を検討していること。	● 是正処置の記録(A.3.5.3 k))
4	個人情報保護マネジメントシステムを継続的に改善していること。	● トップマネジメントによる説明 ● マネジメントシステムの改善履歴 （例） ・マネジメントレビューの記録(A.3.5.3 l))

		・是正処置の記録(A.3.5.3 k)) ・内部規程の改廃履歴 など

《留意事項》

- 審査項目２．の「不適合が明らかになった場合」とは，例えば，パフォーマンス評価(A.3.7)のほか，個人情報に関わる事故や苦情の発生よって不適合が発見される場合がある。
- 審査項目３．は，A.3.8 の「b)不適合の原因を特定し，是正処置を立案する。」を実施するにあたり，同様な不適合が再発しないように検討していることを確認するための審査項目である。
- 審査項目４．では，トップマネジメントに対し，これまでの個人情報保護マネジメントシステムの変更の状況や，今後も個人情報保護マネジメントシステムの見直しを行うことについて確認を行う。また，内部規程や各種記録等の文書化した情報(A.3.5.1)の改廃履歴についても確認を行う。

改訂履歴

日付	ページ	項番	位置	改訂内容
平成 30 年 1 月 12 日	―	―	―	作成
平成 30 年 3 月 16 日	17	A.3.4.2.6	審査項目 No.3	「JIS Q 15001:2017 個人情報保護マネジメントシステム―要求事項」の正誤票(平成 30 年 3 月 15 日)に伴う変更 (変更前) 本人の同意を得ることを要しないのは，A.3.4.2.4 の a)～d)のいずれかに該当する場合に限定していること。 (変更後) 本人の同意を得ることを要しないのは，A.3.4.2.3 の a)～d)のいずれかに該当する場合に限定していること。
平成 30 年 7 月17日	13	A.3.4.2.3	審査項目 No.2	要配慮情報の取得,利用及び提供の適用除外の要件を法律と整合させるための変更 (変更前) 要配慮個人情報を取得,利用又は提供並びに要配慮個人情報のデータを提供する際，書面による本人の同意を得ることを要しないときは，以下の場合に限定していること。 a) 法令に基づく場合 (略) (変更後) 要配慮個人情報を取得,利用する際，書面による本人の同意を得ることを要しないときは，以下の場合に限定していること。(この後に a) ～e) 項を記載) a) 法令に基づく場合 (略)
平成 30 年 7 月 17 日	14	A.3.4.2.3	審査項目 No.3	要配慮情報の取得,利用及び提供の適用除外の要件を法律と整合させるための変更 (変更前) (記載なし) (変更後) 要配慮個人情報を提供する際，書面による本人の同意を得ることを要しないときは，A.3.4.2.3 のただし書き a)～d)の場合に限定していること。
平成 30 年 7 月 17 日	14	A.3.4.2.3	留意事項	審査項目３．の追記と整合させるための変更 (変更前) ● 審査項目２．は，「個人情報の特定に関する記録(A.3.5.3 a))」としての台帳(A.3.3.1)により，台帳に記載されているが書面による本人の同意の取得が行われていない要配慮個人情報の有無を確認する。確認の結果，本人の同意の取得を行っていない場合は，本人の同意を得ずに取得した要配慮個人情報が A.3.4.2.3 のただし書きに該当することを確認する。 (変更後) ● 審査項目２．及び審査項目３．は，「個人情報の特定に関する記録(A.3.5.3 a))」としての台帳(A.3.3.1)により，台帳に記載されているが書面による本人の同意の

				取得が行われていない要配慮個人情報の有無を確認する。確認の結果，本人の同意の取得を行っていない場合は，本人の同意を得ずに取得した要配慮個人情報がA.3.4.2.3のただし書きに該当することを確認する。
平成30年7月17日	25	A.3.4.3.1	審査項目 No.2	「JIS Q 15001:2017 個人情報保護マネジメントシステム―要求事項」に基づき、努力義務であることを明確とするための変更 （変更前）利用する必要がなくなった個人データを消去していること。 （変更後）利用する必要がなくなった個人データの消去を含む管理を、規定に基づいて適切に行っていること。