JISQ15001規格改正に伴う新審査基準の説明（主に更新事業者向け）

一般社団法人 中部産業連盟
Pマーク審査センター

本資料は、JIPDECが「JIPDEC個人情報保護研修会2017」で使用した資料をもとに作成しています。
「Copyright©2018 JIPDEC All rights reserved」ページは、そのまま使用しています。
【参考】ページは、中産連が追加したページです。
それ以外のページは、中産連がオリジナル資料を一部加筆/修正しています。
オリジナル資料は、JIPDECの更新事業者向けHPに公開されています。

目次

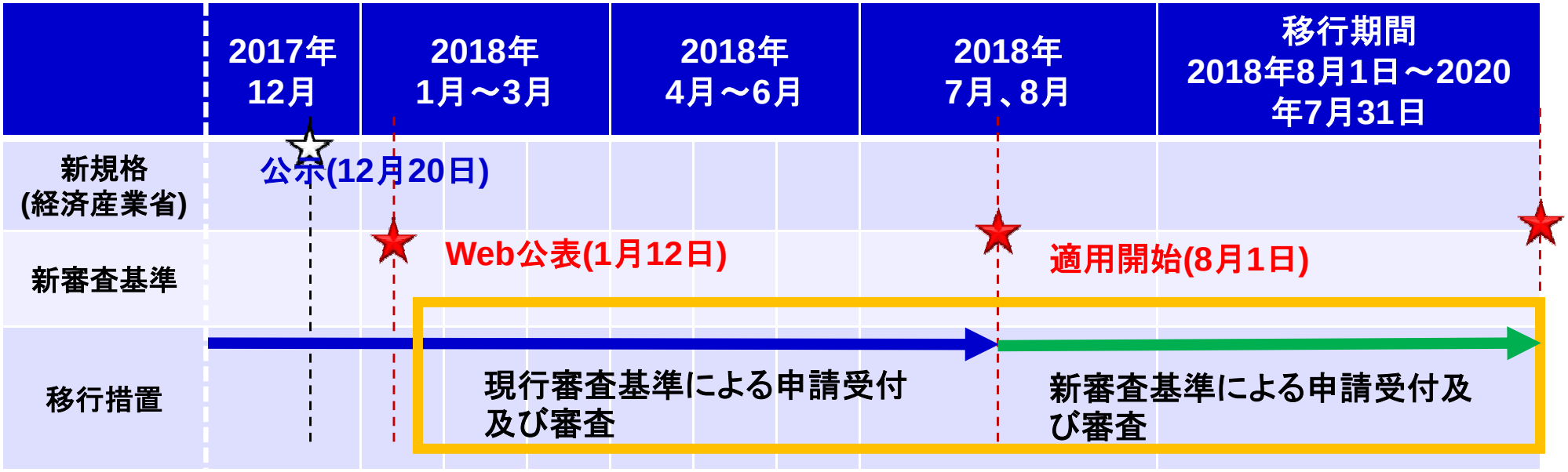
本日のポイント

- JISQ15001：2017規格の発行に伴い、2018年1月にPマーク審査基準も改定（新審査基準）されました。
- 中産連を含む審査機関は、2018年8月1日申請受付分から新審査基準を適用して文書審査/現地審査する予定です。
- 新審査基準へ未対応の事業者に対しては、「継続的改善事項に準じる指摘」として、次の更新審査までの対応を求めます。

- 全ての事業者に対応いただく点は、４つ
- ✓ 該当事業者に対応いただく点は、２つ
  - 改正個人情報保護法への対応
  - 個人情報の管理台帳に追記していただく事項(保管期限)
  - ✓ 共同利用について、共同利用者間における契約で定める事項
  - ✓ 委託契約に盛り込むべき事項（委託契約終了後の措置）
  - 従業者の教育に盛り込む必要がある事項(個人情報保護方針)
  - 運用の確認(日常点検や、それに伴う是正、代表者への報告など)

1. 新審査基準による審査の適用開始時期

新審査基準による審査の適用開始時期



対象 (従来通り)	**事業者単位の審査** ＊規格の主体は“組織”に変更されましたが、審査は従来通り“事業者”単位で行います。 ＊トップマネジメントに対する要求事項は、審査においては代表者に対して行うことを原則とします。
適用時期	2018年8月1日申請受付分より適用開始します。(6月以降に新申請様式公表)
移行期間	2年間
移行措置	移行期間中の審査において、新審査基準未対応の事業者に対し、移行期間終了後、最初の更新審査が終了するまでの対応を求めます。 **→継続的改善事項に準ずる指摘**

新審査基準への対応時期について

新審査基準への対応が未完了の事業者

→移行期間中、新審査基準へ未対応の箇所は継続的改善事項に準ずる指摘として、次回の更新審査までに対応を求めます。

→申請書類提出までに新しい内部規程等に基づく運用記録(教育や代表者による見直し等)が無い場合、継続的改善事項に準ずる指摘とします。

新審査基準への対応が完了している事業者

→新審査基準に対応したが、新審査基準での不備事項が発見された場合は指摘事項若しくは継続的改善事項となります（従来通り）。

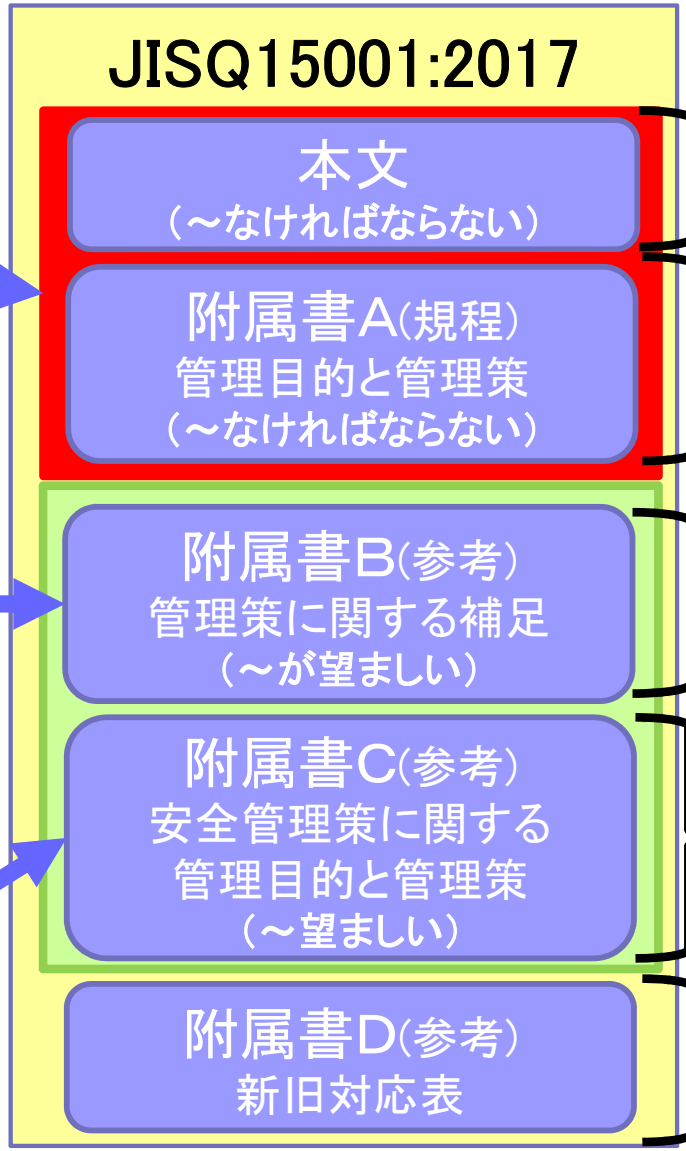
2. 新規格の概要

JIS Q 15001:2017規格の体系

附属書Aに示す管理策は、必要な管理策の見落としがないことを確実にするために参照するものであり、附属書Aの管理策を実施すれば本文の要求事項が満たされます。

附属書Bは規定ではなく参考であり、附属書Aの補足及び推奨事項。

附属書CはA.3.4.3.2安全管理措置の理解を助けるための参考情報であり、取り扱う個人情報の個人情報保護リスクに応じて適宜選択して利用することで問題ありません。



附属書SL（共通テキスト）に対応

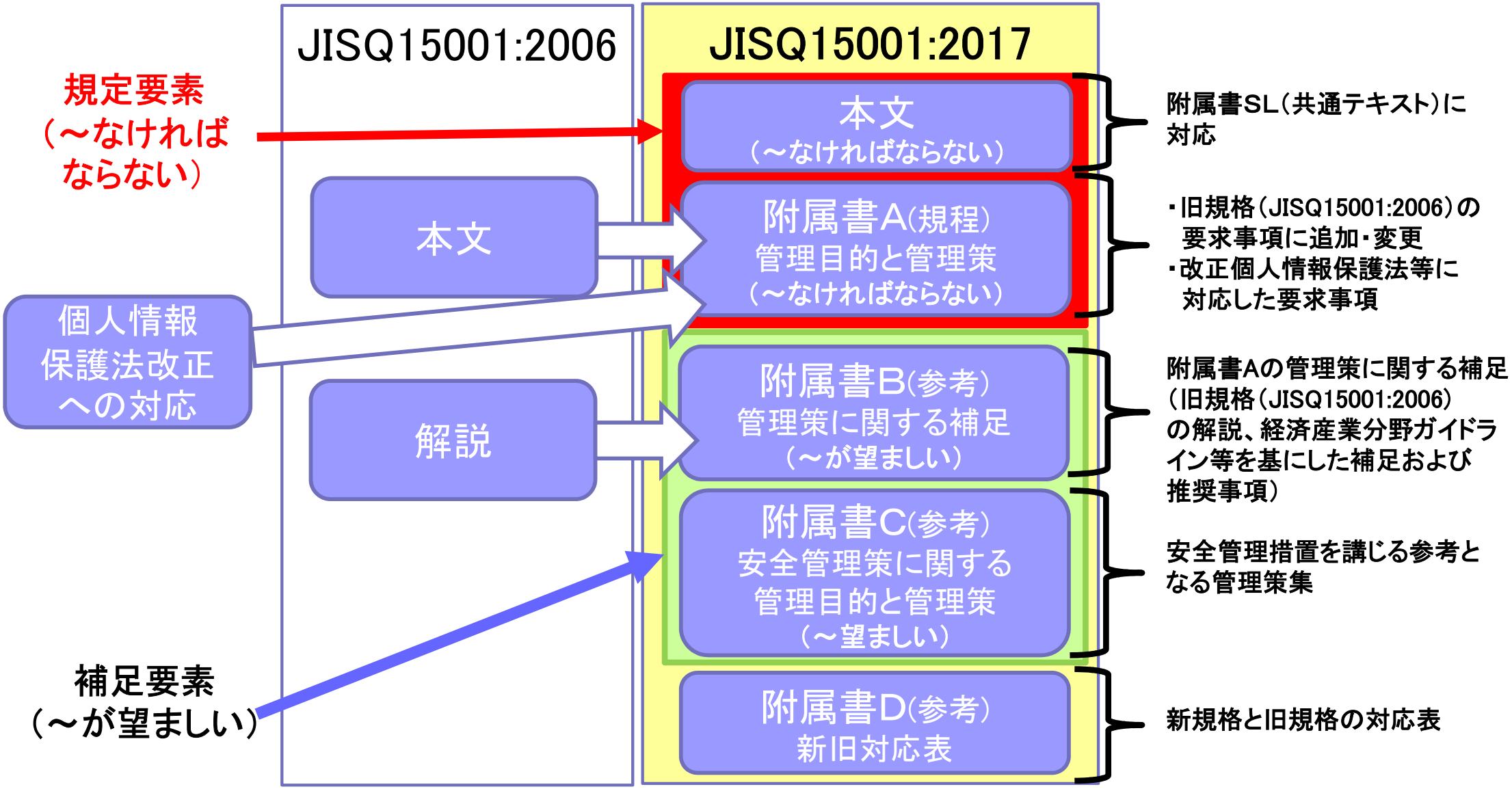
・旧規格（JISQ15001:2006）の要求事項に追加・変更
・改正個人情報保護法等に対応した要求事項

附属書Aの管理策に関する補足（旧規格（JISQ15001:2006）の解説、経済産業分野ガイドライン等を基にした補足および推奨事項）

安全管理措置を講じる参考となる管理策集

新規格と旧規格の対応表

JIS15001規格2006年版と2017年版の構成比較



新規格（本文）の構成

新規格の本文は、附属書SLの共通テキストに対応しています。

下線部分は、附属書SLの共通テキストを変更及び追加した部分です。

JIS Q 15001:2017　本文

0. 序文

1. 適用範囲

2. 引用規格

3. 用語及び定義

4. 組織の状況
- 4.1組織及びその状況の理解
- 4.2利害関係者のニーズ及び期待の理解
- 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
- 4.4個人情報保護マネジメントシステム

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
- 5.2方針
  - 5.2.1内部向け個人情報保護方針
  - 5.2.2外部向け個人情報保護方針
- 5.3組織の役割、責任及び権限

6. 計画
- 6.1リスク及び機会に対処する活動
  - 6.1.1一般
  - 6.1.2個人情報保護リスクアセスメント
  - 6.1.3個人情報保護リスク対応
- 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

7. 支援
- 7.1資源
- 7.2力量
- 7.3認識
- 7.4コミュニケーション
- 7.5文書化した情報
  - 7.5.1一般
  - 7.5.2作成及び更新
  - 7.5.3文書化した情報の管理

8. 運用
- 8.1運用の計画及び管理
- 8.2個人情報保護リスクアセスメント
- 8.3個人情報保護リスク対応

9. パフォーマンス評価
- 9.1監視、測定、分析及び評価
- 9.2内部監査
- 9.3マネジメントビュー

10. 改善
- 10.1不適合及び是正処置
- 10.2継続的改善

旧規格と新規格（附属書A）の比較①

旧規格の要求事項は附属書Aの管理策として構成されました。
下線は、附属書SLとの整合又は旧規格の変更によって要求事項に対して変更があったものです。
（新旧対照表は、附属書Dもご参照ください。）

JISQ15001:2006	JISQ15001:2017　附属書A
1.適用範囲	（本文箇条1　適用範囲）
2.用語及び定義	（本文箇条3　用語及び定義）
3.要求事項	A.3 管理目的及び管理策
3.1 一般要求事項	A.3.1 一般
	A.3.1.1 一般
3.2 個人情報保護方針	A.3.2 個人情報保護方針
	A.3.2.1 内部向け個人情報保護方針
	A.3.2.2 外部向け個人情報保護方針
3.3 計画	A.3.3 計画
3.3.1 個人情報の特定	A.3.3.1 個人情報の特定
3.3.2 法令、国が定める指針その他の規範	A.3.3.2 法令、国が定める指針その他の規範
3.3.3 リスクなどの認識、分析及び対策	A.3.3.3 リスクアセスメント及びリスク対策

旧規格と新規格（附属書A）の比較②

破線は保護法との整合によって要求事項に対して変更等があったものです。

JISQ15001:2006	JISQ15001:2017　附属書A
3.3.4 資源、役割、責任及び権限	A.3.3.4 資源、役割、責任及び権限
3.3.5 内部規程	A.3.3.5 内部規程
3.3.6 計画書	A.3.3.6 計画策定
3.3.7 緊急事態への準備	A.3.3.7 緊急事態への準備
3.4 実施及び運用	A.3.4 実施及び運用
3.4.1 運用手順	A.3.4.1 運用手順
3.4.2 取得、利用及び提供に関する原則	A.3.4.2 取得、利用及び提供に関する原則
3.4.2.1 利用目的の特定	A.3.4.2.1 利用目的の特定
3.4.2.2 適正な取得	A.3.4.2.2 適正な取得
3.4.2.3 特定の機微な個人情報の取得、利用及び提供の制限	A.3.4.2.3 要配慮個人情報

旧規格と新規格（附属書A）の比較③

JISQ15001:2006	JISQ15001:2017　附属書A
3.4.2.4 本人から直接書面により取得する場合の措置	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
3.4.2.5 個人情報を3.4.2.4以外の方法によって取得した場合の措置	A.3.4.2.4 個人情報を取得した場合の措置
3.4.2.6 利用に関する措置	A.3.4.2.6 利用に関する措置
3.4.2.7 本人にアクセスする場合の措置	A.3.4.2.7 本人に連絡又は接触する場合の措置
3.4.2.8 提供に関する措置	A.3.4.2.8 個人データの提供に関する措置
	A.3.4.2.8.1 外国にある第三者への提供の制限
	A.3.4.2.8.2 第三者提供に係る記録の作成など
	A.3.4.2.8.3 第三者提供を受ける際の確認など
	A.3.4.2.9 匿名加工情報

旧規格と新規格（附属書A）の比較④

JISQ15001:2006	JISQ15001:2017　附属書A
3.4.3 適正管理	A.3.4.3 適正管理
3.4.3.1 正確性の確保	A.3.4.3.1 正確性の確保
3.4.3.2 安全管理措置	A.3.4.3.2 安全管理措置
3.4.3.3 従業者の監督	A.3.4.3.3 従業者の監督
3.4.3.4 委託先の監督	A.3.4.3.4 委託先の監督
3.4.4 個人情報に関する本人の権利	A.3.4.4 個人情報に関する本人の権利
3.4.4.1 個人情報に関する権利	A.3.4.4.1 個人情報に関する権利
3.4.4.2 開示等の求めに応じる手続	A.3.4.4.2 開示等の請求等に応じる手続
3.4.4.3 開示対象個人情報に関する事項の周知など	A.3.4.4.3 保有個人データに関する事項の周知など
3.4.4.4 開示対象個人情報の利用目的の通知	A.3.4.4.4 保有個人データの利用目的の通知
3.4.4.5 開示対象個人情報の開示	A.3.4.4.5 保有個人データの開示
3.4.4.6 開示対象個人情報の訂正、追加又は削除	A.3.4.4.6 保有個人データの訂正、追加又は削除
3.4.4.7 開示対象個人情報の利用又は提供の拒否権	A.3.4.4.7 保有個人データの利用又は提供の拒否権

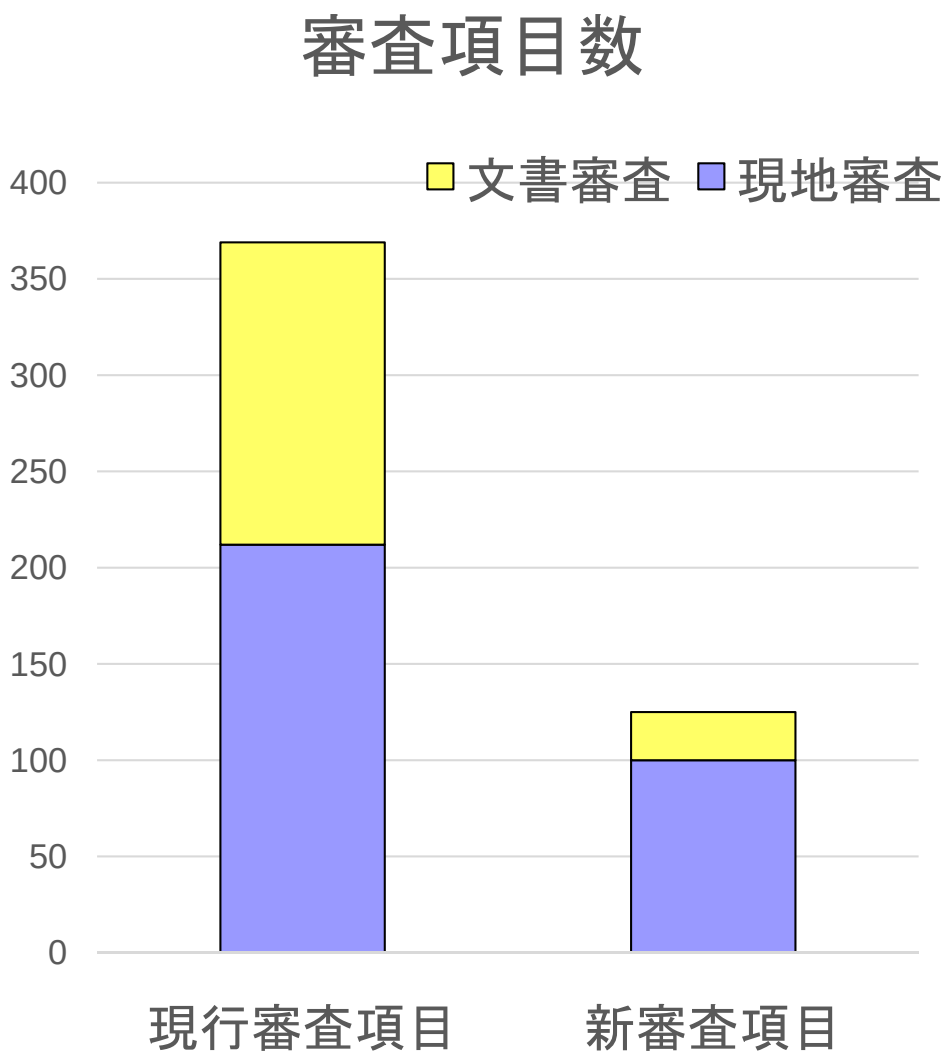
旧規格と新規格（附属書A）の比較⑤

JISQ15001:2006	JISQ15001:2017　附属書A
3.4.5 教育	A.3.4.5 認識
3.5 個人情報保護マネジメントシステム文書	A.3.5 文書化した情報
3.5.1 文書の範囲	A.3.5.1 文書化した情報の範囲
3.5.2 文書管理	A.3.5.2 文書化した情報（記録を除く。）の管理
3.5.3 記録管理	A.3.5.3 文書化した情報のうち記録の管理
3.6 苦情及び相談への対応	A.3.6 苦情及び相談への対応
3.7 点検	A.3.7 パフォーマンス評価
3.7.1 運用の確認	A.3.7.1 運用の確認
3.7.2 監査	A.3.7.2 内部監査
	A.3.7.3 マネジメントレビュー
3.8 是正処置及び予防処置	A.3.8 是正処置
3.9 事業者の代表者による見直し	（A.3.7.3 マネジメントレビュー）

3. 新審査基準の解説

（1）規格と審査基準の主な変更箇所

【参考】現行審査基準と新審査基準



- 現行審査基準
  - 実質的にJIPDECガイドライン（2版）
- 新審査基準
  - JISQ15001:2017　付属書Aを元に2018年1月にJIPDEC　HPに公表

https://privacymark.jp/system/guideline/pdf/pm_shinsakijun.pdf

  - 文書審査（25項目）

申請事業者の提出したPMS文書を審査

  - 現地審査（100項目）

新審査基準に関する事業者の内部規程に基づく実施状況を確認

【参考】新審査基準例（一部抜粋/体裁変更）

JISQ15001:2017（付属書A）	審査項目
A.3.3.1　個人情報の特定 組織は，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を確立し，かつ，維持しなければならない。 組織は，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。 組織は，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。	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。（文書審査） ②個人情報を管理するための台帳を整備していること。（現地審査） ③台帳には，少なくとも以下の項目が含まれていること。（現地審査） ・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 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。（現地審査）

《留意事項》

- 台帳に含める項目を検討するにあたっては，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。

規格と審査基準の主な変更箇所①

審査基準は変更となりましたが、新たに規程や運用の変更をする必要が無いもの、既にご対応いただいている点もあります。
現在の規程類や運用状況を踏まえ、ご確認ください。

審査基準変更の理由	主な規格と審査基準の変更点	事業者の対応
改正個人情報保護法との整合によるもの	①用語及び定義(審査全般)	一部必要
	②要配慮個人情報(A.3.4.2.3 新設)	必要
	③トレーサビリティの確保(A.3.4.2.8.2 新設、A3.4.2.8.3 新設)	必要
	④オプトアウト規制の強化(A.3.4.2.8)	必要
	⑤外国事業者への第三者提供(A.3.4.2.8.1 新設)	必要
	⑥個人データの消去の努力義務(A.3.4.3.1)	必要
	⑦匿名加工情報(A.3.4.2.9 新設)	必要

※新審査基準による審査開始前であっても、改正個人情報保護法には対応をしている必要があります。

規格と審査基準の主な変更箇所②

事業者の対応が「不要」とは、従来から実質的に審査基準として運用されていて、運用されていないと指摘事項となった項目等です。（新規審査の場合は、対応が必要です。）

審査基準変更の理由	主な規格と審査基準の変更点	事業者の対応
2006年版の変更によるもの	①承認手順確認方法の変更（審査全般、A.3.1.1）	不要
	②個人情報保護方針の追加（A.3.2.1、A.3.2.2）	不要
	③頻度の明確化（審査全般、A.3.3.1他）	不要
	④台帳の整備（A.3.3.1）	必要
	⑤残留リスクの把握、管理（A.3.3.3）	不要
	⑥個人情報保護監査責任者と個人情報保護管理者の分離（A.3.3.4）	不要
	⑦利用目的特定にあたっての配慮（A.3.4.2.1）	不要
	⑧ただし書きの明確化（審査全般、A.3.4.2.4他）	不要
	⑨A.3.4.2.4、A.3.4.2.5　個人情報の取得について	不要
	⑩「本人アクセス」（旧規格3.4.2.7）の名称変更 「本人に連絡又は接触」（A.3.4.2.7）	不要

規格と審査基準の主な変更箇所③

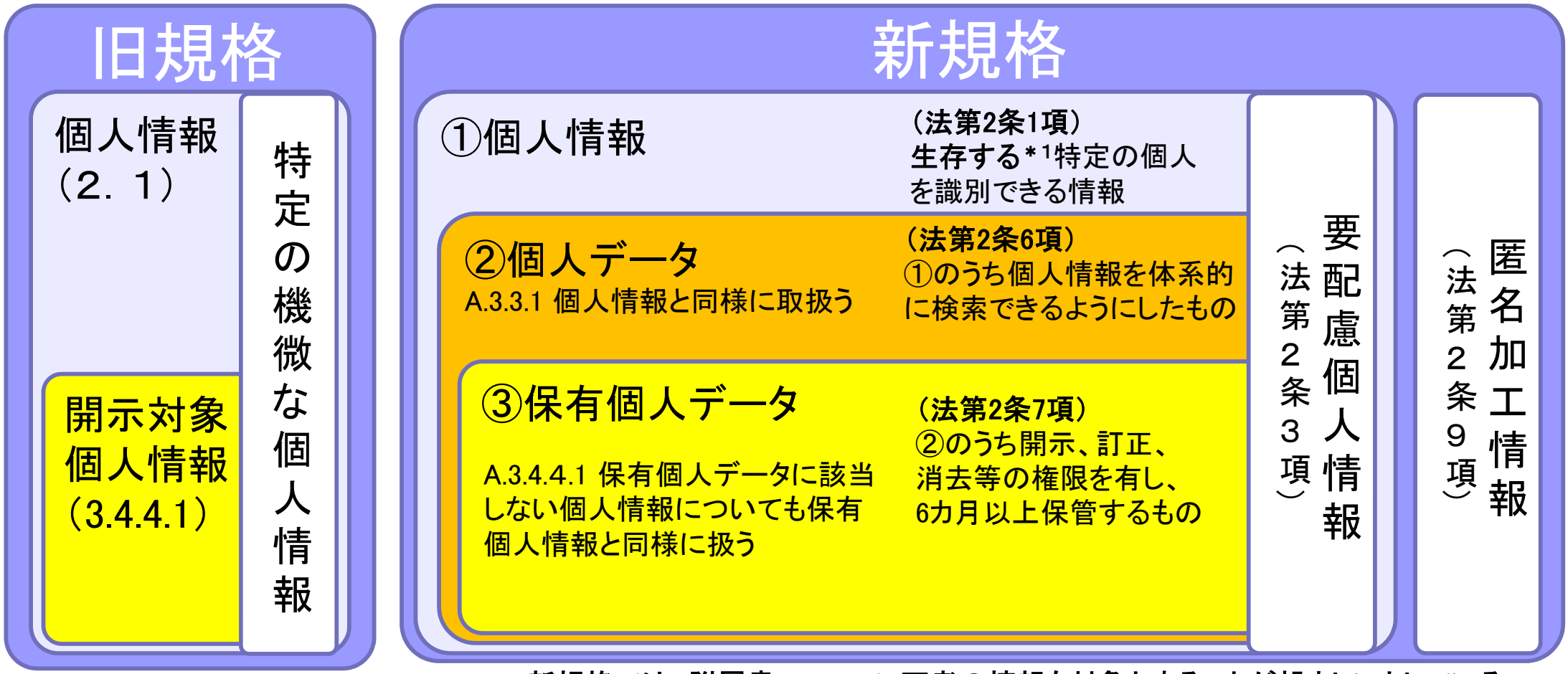
事業者の対応が「不要」とは、従来から実質的に審査基準として運用されていて、運用されていないと指摘事項となった項目等です。（新規審査の場合は、対応が必要です。）

審査基準変更の理由	主な規格と審査基準の変更点	事業者の対応
2006年版の変更によるもの	⑪共同利用についての契約（A.3.4.2.8）	必要
	⑫安全管理措置（A.3.4.3.2、附属書C）	不要
	⑬委託契約、選定（A.3.4.3.4）	必要
	⑭従業者に認識させる事項「個人情報保護方針」（A.3.4.5）	必要
	⑮書面で記述する要素「様式」（A.3.5.1）	不要
	⑯作成し、かつ、維持しなければならない記録（A.3.5.3a)～i)）	不要
	⑰各部門及び階層における運用の確認（A.3.7.1）	必要
	⑱監査員（A.3.7.2）	不要

（2）審査基準全般に関わる事項

審査基準全般に関わる事項―用語及び定義①―

新規格で用いる主な用語及び定義は、個人情報保護法における用語及び定義に統一されました。
個人データ及び保有個人データの取扱いについては、旧規格の個人情報及び開示対象個人情報の範囲と同じとしています。（特定の機微な個人情報と要配慮個人情報は、若干定義が異なります）



＊１　新規格では、附属書B.3.3.1で、死者の情報も対象とすることが望ましいとしている

審査基準全般に関わる事項―用語及び定義②―

下記表のように用語が変更となりましたが、規程類などで使用している用語について、変更することは必須ではありません。（要配慮個人情報等を除く）
参考として、新規格の附属書D、表D-3には「用語対応表」が示されています。

JISQ15001:2006（旧規格）	JISQ15001:2017(新規格)
事業者	組織
代表者、事業者の代表者	トップマネジメント
リスク	個人情報保護リスク（個人情報の取扱い局面における好ましくない影響）
リスクの評価、分析	個人情報保護リスクアセスメント
（リスクの）対策	個人情報保護リスク対応
残存リスク（解説に記載）	残留リスク
教育	認識、教育など

JISQ15001:2006（旧規格）	JISQ15001:2017(新規格)
個人情報保護マネジメントシステム文書	文書化した情報
文書	文書化した情報（記録を除く。）
記録	文書化した情報のうち記録
実施及び運用	運用
本人にアクセスする	本人に連絡又は接触する
点検、代表者による見直し	パフォーマンス評価
監査	内部監査
代表者による見直し	マネジメントレビュー
是正処置及び予防処置	是正処置

審査基準全般に関わる事項―承認手順について―

A.3.1.1において、A.3.2～A.3.8については、トップマネジメントによって権限を与えられた者によって、組織が定めた手順に従って承認されなければならない、とされました。
※これまで定めた個別の承認手順の変更は必須ではありません。

現行審査基準
⇒各項目ごとの承認手順

- 3. 4. 2. 4　承認手順
- 3. 4. 2. 5　承認手順
- 3. 4. 2. 6　承認手順
- 3. 4. 2. 7　承認手順
- 3. 4. 2. 8　承認手順

等

新審査基準
⇒個別の承認手順は必須ではない

A.3.1.1組織が定めた承認手順

- A. 3. 4. 2. 4
- A. 3. 4. 2. 5
- A. 3. 4. 2. 6
- A. 3. 4. 2. 7
- A. 3. 4. 2. 8

等

審査基準全般に関わる事項―頻度の明確化―

新規格では、個人情報の特定や見直し等を行う頻度が明確になりました。
これらは従来の審査でも確認を行っておりますので、新たな対応は必要ありません。

新規格の項番	内容
A.3.3.1 個人情報の特定	・個人情報を管理するための台帳の内容の確認（少なくとも年1回、適宜に）
A.3.3.3 リスクアセスメント及びリスク対策	・個人情報保護のリスクの特定、分析及び講じた個人情報保護リスク対策の見直し（少なくとも年1回、適宜に）
A.3.3.6 計画策定	・計画の立案、文書化（少なくとも年1回）
A.3.4.3.4 委託先の監督 e)	・契約によって規定し、十分な個人データの保護水準を担保する事項（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）
A.3.4.5 認識	・手順（全ての従業者に対する教育を少なくとも年1回、適宜に行うことを含む手順）
A.3.7.1 運用の確認	・手順（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組織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） ・各部門及び各階層の管理者による運用の確認（定期的に、及び適宜に） ・個人情報保護管理者のトップマネジメントへの報告（定期的に、及び適宜に）
A.3.7.2 内部監査	・監査（少なくとも年1回、適宜に）
A.3.7.3 マネジメントレビュー	・個人情報保護マネジメントシステムの見直し（少なくとも年1回、適宜に）

審査基準全般に関わる事項―ただし書きの明確化―

新規格では、旧規格で「ただし、～（中略）～、この限りでない」という表現を、「ただし、～（中略）～、〇〇〇〇は要しない」という表現に改めることで明確にしました。これによる対応は必要ありません。

ただし書きの明確化の例

新規格の項番	内容
A.3.4.2.4　個人情報を取得した場合の措置	「本人への利用目的の通知又は公表は要しない」とされました。
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	「本人に明示し、本人の同意を得ることを要しない」とされました。
A.3.4.2.6　利用に関する措置	「本人の同意を得ることを要しない」とされました。
A.3.4.2.7　本人に連絡又は接触する場合の措置	「本人に通知し、本人の同意を得ることを要しない」とされました。
A.3.4.2.8　個人データの提供に関する措置	「本人に通知し、本人の同意を得ることを要しない」とされました。

A.3.4.2.4、A3.4.2.5　個人情報の取得について

旧規格の3.4.2.4、3.4.2.5と、新規格のA.3.4.2.4、A.3.4.2.5は、構成が以下のように変更となりました。
A.3.4.2.5に基づき本人から直接書面によって個人情報を取得する場合には、A.3.4.2.4に定められた対応(利用目的の公表や通知など)を行っていることが前提となります。

【旧規格】

本人から直接書面によって取得(3.4.2.4)

個人情報を3.4.2.4以外によって取得(3.4.2.5)

【新規格】

個人情報の取得
(A.3.4.2.4)

本人から直接書面によって取得
(A.3.4.2.5)

（3）審査基準の変更点
－改正個人情報保護法との整合によるもの－

審査基準の変更点―改正個人情報保護法との整合によるもの①―

個人情報保護法の改正に伴い、JIS規格も改正されました。
これに伴い、審査基準も変更されました。

改正個人情報保護法	新規格の項番	新規格と審査基準の変更点	事業者の対応
要配慮個人情報の扱い（法第17条2項）	A.3.4.2.3 要配慮個人情報（新設）	・保護法改正により新設されたことに伴い、新規格においても項目が新設されました。 ・「要配慮個人情報」の定義は個人情報保護法によるため、従来の「特定の機微な個人情報」とは定義が異なります。 ・審査では、要配慮個人情報を取得・利用・提供等をする場合には、あらかじめ書面による本人の同意が行われているか等を確認します。	・「要配慮個人情報」の定義についての確認及び更新。 ※取扱いについては、従来の「特定の機微な個人情報」と同様です。
個人データ消去の努力義務の追加（法第19条）	A.3.4.3.1 正確性の確保	・審査では、正確かつ最新の状態で個人情報を管理しているか、事業者が定めた保管期限を過ぎた個人情報について、消去が行われているかどうか等を確認します。	・定めた保管期限を過ぎた個人情報を消去する。

【参考】特定の機微な個人情報と要配慮個人情報

特定の機微な個人情報

a)思想，信条又は宗教に関する事項

b)人種，民族，門地，本籍地（所在都道府県に関する情報を除く），身体・精神障害，犯罪歴その他社会的差別の原因となる事項

c)勤労者の団結権，団体交渉その他団体行動の行為に関する事項

d)集団示威行為への参加，請願権の行使その他の政治的権利の行使に関する事項

e)保健医療又は性生活に関する事項

- 「機微情報」に該当するが、「要配慮個人情報」に該当しないもの
  - 労働組合等への加盟
  - 本籍地
  - 性生活

要配慮個人情報

- 人種、信条、社会的身分、病歴、前科・前歴、犯罪被害情報
- 本人に対する不当な差別、偏見が生じないように特に配慮を要するもの
  - 身体障害・知的障害・精神障害等があること
  - 健康診断その他の検査の結果（遺伝子検査結果を含む）
  - 保健指導、診療・調剤情報」等
- 「要配慮個人情報」に該当するが、「機微情報」に該当しないもの
  - 犯罪により害を被った事実
  - 被疑者又は被告人として、刑事事件に関する手続が行われたこと
  - 少年法の対象者として、少年の保護事件に関する手続が行われたこと

審査基準の変更点―改正個人情報保護法との整合によるもの②―

改正個人情報保護法	新規格の項番	新規格と審査基準の変更点	事業者の対応
オプトアウト規制の強化（法第23条2項）	A.3.4.2.8 個人データの提供に関する措置	・保護法改正に伴い、新規格においてただし書きが変更されました。 ・提供において、本人の同意を得ることが困難な場合で、本人の同意を得ることを要しない条件（ただし書き）が変更されました。	・ただし書きを本人への通知文書や規程に記載している場合には、表記の修正が必要です。 →実質的に修正要
外国事業者への第三者提供（法第24条）	A.3.4.2.8.1 外国にある第三者への提供の制限（新設）	・保護法改正により新設されたことに伴い、新規格においても項目が新設されました。 ・審査では、外国にある第三者に個人データを提供する場合、本人の同意を得ているか等を確認します。	・外国事業者への第三者提供が想定される場合には、規程類の作成、規程類に基づく運用が必要です。

【参考】個人データの提供に関する措置ーただし書きー

- **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情報の項目
  - 第三者への提供の手段又は方法
  - 本人の請求などに応じて当該本人が識別される個人情報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

- 法令等が定める手続き（個人情報保護委員会への届出→公表）
  - https://www.ppc.go.jp/personal/preparation/optout/publication_list/

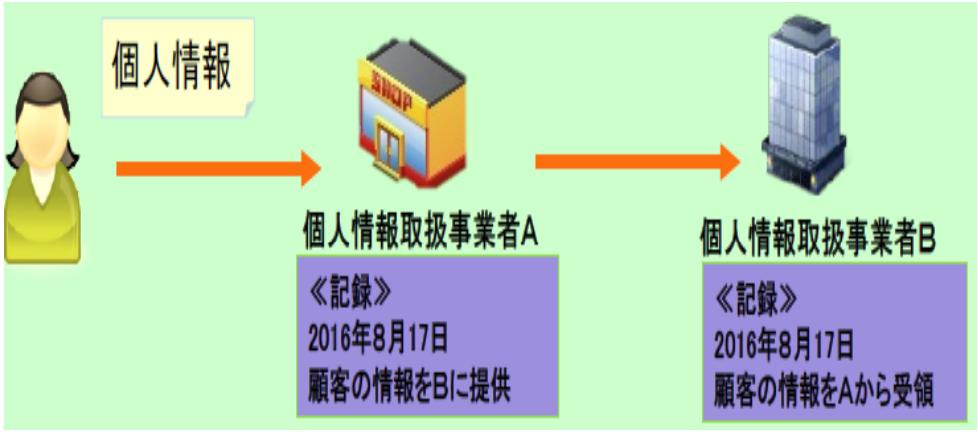
審査基準の変更点―改正個人情報保護法との整合によるもの③―

改正個人情報保護法	新規格の項番	新規格と審査基準の変更点	事業者の対応
トレーサビリティの確保（法第25条、第26条）	A.3.4.2.8.2 第三者提供に係る記録の作成（新設）	・保護法改正により新設されたことに伴い、新規格においても項目が新設されました。 ・審査では、個人データを第三者に提供する際、記録を作成しているか等を確認します。	・個人データを第三者に提供する場合、記録の作成が必要です。
	A.3.4.2.8.3 第三者提供を受ける際の確認（新設）	・保護法改正により新設されたことに伴い、新規格においても項目が新設されました。 ・審査では、第三者から個人データの提供を受ける際、記録を作成しているか等を確認します。	・第三者から個人データを提供される場合、記録の作成が必要です。
匿名加工情報（法第36条～法第39条）	A.3.4.2.9 匿名加工情報（新設）	・保護法改正により新設されたことに伴い、新規格においても項目が新設されました。 ・審査では、匿名加工情報を取り扱うかどうかの方針の有無を確認します。 ・取り扱う場合には、その手順を示した内部規程が作成されているかどうか等を確認します。	・匿名加工情報を取り扱うかどうかの決定が必要です。 ・匿名加工情報を取り扱う場合には手順を定め規程を作成する必要があります。

【参考】第三者提供に係る確認・記録義務

- 第三者との間で個人情報を提供・受領する場合、提供先が提供元の情報取得経緯等を確認して記録
- 提供/受領の都度に確認/記録することでビジネスに支障が及ばない様に、以下の配慮
  - 本人同意がある場合、提供年月日の記録は不要
  - 記録の保存期間は原則3年だが、本人同意で第三者提供した場合は1年
  - 本人との契約等に基づく提供の場合は、既存の契約書等で代替可能
  - 反復継続して提供する場合は、包括的な記録で可

- 以下の場合は、確認/記録義務がない
  - 法令に基づく提供
  - 本人による提供（SNS等に記載されている本人発信によるプロフィール）
  - 本人に代わって提供（銀行振込）
  - 本人側への提供（同席している家族）

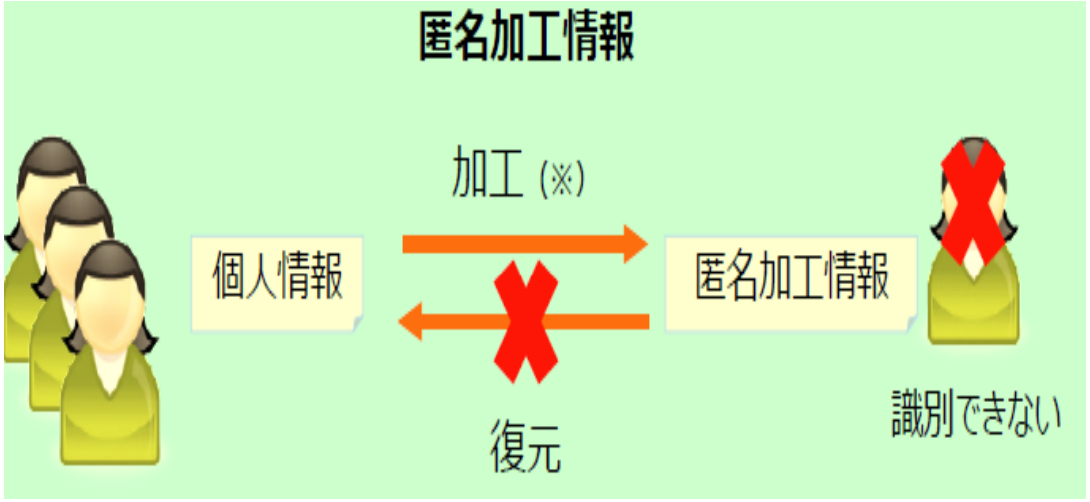


【参考】匿名加工情報取扱事業者の順守義務等

- 匿名加工情報とは、特定の個人を識別できないように個人情報を加工し、当該個人情報を復元できないような形にしたもの
  - 特定の個人を識別可能な記述等（氏名等）の全部または一部を削除
  - 個人識別符号の全部を削除
  - 個人情報と他の情報を連結する符号を削除
- 匿名加工情報を取り扱う個人情報取扱事業者→匿名加工情報取扱事業者の順守事項
  - 適切な加工（法第36条1項、規則第19条）
  - 安全管理措置（法第36条2項/6項）
  - 公表義務（法第36条3項/4項）
  - 識別行為の禁止（法第36条5項等）

- 個人情報の保護に関する法律についてのガイドライン（匿名加工情報編）

  https://www.ppc.go.jp/personal/tokumeikakouInfo/



（4）審査基準の変更点
―2006年版の変更によるもの―

審査基準の変更点―2006年版の変更によるもの①―

JISQ15001:2006からの変更に伴い、審査基準が変更されました。

個人情報保護方針に含まなければならない項目については変更が無いため、現在公表している個人情報保護方針を2つに分けることは必須ではありません。

変更箇所	新規格と審査基準の変更点	事業者の対応
個人情報保護方針の追加（A.3.2.1 内部向け個人情報保護方針（新設））	・旧規格3.2の個人情報保護方針は、内部向け個人情報保護方針と外部向け個人情報保護方針に整理されました。 ・方針を周知する対象を「組織内に伝達し、必要に応じて利害関係者が入手可能」としています。 ※ここでいう利害関係者とは、委託先や協業相手などの取引先などが考えられます。	・新たに個人情報保護方針に項目を追加する必要はありません。 ※周知する対象に「利害関係者」が追加されたことに注意する必要があります。
個人情報保護方針の追加（A.3.2.2 外部向け個人情報保護方針（新設））	・A.3.2.1に加えて、制定年月日及び最終改正年月日、外部向け個人情報保護方針の内容についての問合わせ先、について明記することとしていますが、従来の項目と変更はありません。 ・方針を周知する対象を「一般の人が入手可能」としています。	・新たに個人情報保護方針に項目を追加する必要はありません。

審査基準の変更点―2006年版の変更によるもの②―

変更箇所	新規格と審査基準の変更点	事業者の対応
台帳の整備 （A.3.3.1 個人情報の特定）	・個人情報管理台帳に記載すべき項目として、件数が削除され、保管期限が追加となりました。 ・審査では、従来の審査項目に加えて、個人情報管理台帳に保管期限が記載されているかどうかを確認します。	・個人情報管理台帳への記載項目（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/保管期限等） ・件数を記載する場合は概数でも可
個人情報保護監査責任者と個人情報保護管理者の分離 （A.3.3.4 資源,役割,責任権限）	・新規格では、個人情報保護監査責任者と個人情報保護管理者を分離することが明確になりました。 ・従来から、個人情報保護監査責任者と個人情報保護管理者は兼務出来ないとしていました。	・規格は変更となりましたが、審査基準に変更は無いため、対応をする必要はありません。
利用目的特定にあたっての配慮 （A.3.4.2.1 利用目的の特定）	・利用目的特定にあたって、提供の範囲についても可能な限り具体的に明らかにするように配慮しなければなりません。 ・従来から、これらの対応をお願いしていました。	・規格は変更となりましたが、審査基準に変更は無いため、対応をする必要はありません。

審査基準の変更点―2006年版の変更によるもの③―

変更箇所	新規格と審査基準の変更点	事業者の対応
共同利用について（A.3.4.2.7 本人に連絡又は接触する場合の措置）	・“共同利用”について定義されました。	・規格は変更となりましたが、審査基準に変更は無いため、対応をする必要はありません。
共同利用についての契約（A.3.4.2.8 個人データの提供に関する措置）	・A.3.4.2.8 でいう共同利用は、A.3.4.2.7における定義に基づきます。 ・個人データを第三者に提供する場合であって、本人の同意を必要としないただし書き f）に該当する項目として、共同利用の場合、共同利用について共同利用者間で契約で定めていることが追加されました。 ・審査では、従来の審査項目に加えて、共同利用について契約で定めているかどうかを確認します。	・個人データの共同利用をする場合であって、ただし書き f）を適用する場合には、共同利用をする者の間で、共同利用について契約で定めていることが必要となります。 ・本人の知りうる状態に置く項目 ・共同利用すること ・共同利用される個人情報の項目 ・共同利用される者の範囲 ・共同利用する者の利用目的 ・共同利用する個人情報の管理について責任者の氏名又は名称 ・取得方法

審査基準の変更点―2006年版の変更によるもの④―

変更箇所	新規格と審査基準の変更点	事業者の対応
安全管理措置（A.3.4.3.2 安全管理措置、附属書C）	・旧規格3.4.3.2では対応する審査項目を設定していませんでしたが、規格との対応を明確にするために審査項目を作成しました。	・基準変更による対応は必要ありません。 ・附属書CはA.3.4.3.2の参考情報であり、審査基準ではなく、取り扱う個人情報のリスクに応じて適宜選択して利用することで問題ありません。
委託契約、選定（A.3.4.3.4 委託先の監督）	・契約によって規定する事項に、h)契約終了後の措置が追加されました。 ・審査では、従来の審査項目に加えて、委託先との契約に「h）契約終了後の措置」が盛り込まれているかどうかを確認します。	・委託先との契約に「h）契約終了後の措置」を設けていない場合には、追加する必要があります。

審査基準の変更点―2006年版の変更によるもの⑤―

変更箇所	新規格と審査基準の変更点	事業者の対応
従業者に認識させる事項「個人情報保護方針」（A.3.4.5 認識）	・従業者に認識させる事項として、「個人情報保護方針」（内部向け個人情報保護方針、外部向け個人情報保護）が追加されました。 ・審査では、従業者への教育の内容に、従来の項目に加えて「個人情報保護方針」が含まれているかどうかを確認します。	・従業者への教育の内容に「個人情報保護方針」（内部向け個人情報保護方針、外部向け個人情報保護）を追加する必要があります。
書面で記述する要素「様式」（A.3.5.1 文書化した情報の範囲）	・内部規程に定める手順上で使用する様式（記録の様式）についても文書化した情報の要素となりました（A.3.5.1 d））。 ・審査では、これまで各審査項目で確認していた内部規程や計画書、記録の書面の有無について、A.3.5.1でまとめて確認します。	・基準変更による対応は必要ありません。
作成維持しなければならない記録（A.3.5.3 文書化した情報のうち記録の管理）	・規格の中で管理が必要な記録が明記されました。 ・審査では、記録が作成され管理されているかを確認します。	・基準変更による対応は必要ありません。

審査基準の変更点―2006年版の変更によるもの⑥―

変更箇所	新規格と審査基準の変更点	事業者の対応
各部門及び階層における運用の確認（A.3.7.1 運用の確認）	・各部門及び各階層の管理者は、定期的に運用の確認を行い、不適合が発見された場合は、是正処置を行っているかどうかを確認します。 ・個人情報保護管理者が、運用の確認の状況を、定期的に、及び適宜にトップマネジメントに報告しているかどうかを確認します。	・日常業務において点検を行い、気づいた点があれば、是正及び予防を行い、定期的に及び適宜に、トップマネジメントに報告をする必要があります。
監査員（A.3.7.2 内部監査）	・A.3.7.2では、監査員について言及していますが、従来から監査員が自ら所属する部署を監査しないよう定めています。	・規格は変更となりましたが、審査基準に変更は無いため、対応をする必要はありません。

4. おわりに

【参考】審査基準の改定を機会としたPMS見直しのポイント

- 新審査基準では審査基準項目が集約/統廃合されて、新たな審査項目は十数項目で、減った審査項目数は百数十（特に文書審査項目で顕著）に及びます
- 従来よりも事業者の規模/事業内容/リスクの変化に応じた主体的で柔軟なPMSの構築/運用/見直しが可能になりました
- 新基準審査でも、形式審査→文書審査→現地審査を実施します
- 審査項目の箇条的な審査に加えて、個人情報の取り扱い局面に応じたリスク対策やPMSのPDCA管理状況の確認にも注力します

- 見直しのポイント
  - 「個人情報保護マニュアル」/「個人情報保護規程」をJISQ15001：2017規格の項目に合わせて全面改訂するか、追加分だけ対応するか
  - JISQ15001：2017付属書AのA.3.3.5内部規程（a)項からo)項に合わせて、15種類の規程を維持するか、集約/統合するか
  - 様式類を維持するか、集約/統合するか
  - 個人情報管理台帳/リスク管理表のグループ化/集約化を進めるか
  - 自社の運用/リスクに応じた安全管理措置に力点をおくか

JISQ15001改訂に伴うPマーク新審査基準解説セミナー

- 名古屋：ウインクあいち
  - 9/11（火）13:30～17:00
  - 2019/3/12（火）13:30～17:00

    https://www.chusanren.or.jp/sc/pdata/4205.html
- 12/7（金）13：30～17:00
  - 金沢：石川県勤労者福祉会館
    https://www.chusanren.or.jp/sc/pdata/4206.html
- 料金：5,400円/人（税込）

- 内容

1.JISQ15001：2017とは
  ①JIS規格の構成
  ②JISQ15001：2006との違い
  ③Pマーク新審査基準との関連
2.Pマーク新審査基準の解説
  ①審査の項目と方法について
  ②審査基準の個別解説と
    自社規程/運用への展開
3.より効果的なPMSの運用
  ①新規申請事業者様の場合
  ②更新申請事業者様の場合

参考資料

- 個人情報の保護に関する法律
  （https://www.ppc.go.jp/files/pdf/290530_personal_law.pdf）
- 個人情報の保護に関する法律についてのガイドライン
  - 通則編（https://www.ppc.go.jp/files/pdf/guidelines01.pdf）
  - 外国にある第三者への提供編
    （https://www.ppc.go.jp/files/pdf/guidelines02.pdf）
  - 第三者提供時の確認・記録義務編
    （https://www.ppc.go.jp/files/pdf/guidelines03.pdf）
  - 匿名加工情報編（https://www.ppc.go.jp/files/pdf/guidelines04.pdf）
- 特定分野ガイドライン
  （https://www.ppc.go.jp/personal/legal/guidelines/）
- 個人情報保護委員会(PPC)
  https://www.ppc.go.jp/personal/legal/
- JIPDEC　HP
  https://privacymark.jp/