2014.5

「個人情報保護マネジメントシステム実施ハンドブック」簡易版　第 25 章

個人情報保護監査研究会

第25章　システム管理基準　個人情報保護コントロール

個人情報を取り扱う情報システム（以下、“個人情報システム”という。）を利用している場合、システム監査が必要になります。本章では、経済産業省システム管理基準に、個人情報保護監査研究会が個人情報保護コントロールを追補し、個人情報システムへのチェック項目の例としました。当研究会では、事例として監査用の「3726g_情報システム開発の安全性チェックリスト」を策定しています。

実際の監査に当たっては、それぞれの個人情報システムの特徴に応じてチェック項目を選定します。

25.1　システム管理基準　個人情報保護コントロール

Ⅵ．共通業務　８．個人情報保護（12）

個人情報システムに対するシステム管理基準（個人情報保護コントロール）として、以下の３分類、12 項目を設定しました。末尾のカッコ付数字は、項目の数です。

8.1　個人情報の取り扱いに関する方針（4)

(1)	個人情報の取り扱いに関する方針の策定及び公表並びに責任体制の確保は、個人情報の保護に関連する法令等に準拠して定めること。

（主旨）組織体経営上の重要事項である個人情報の保護に関連する法令順守を行うため、個人情報の取扱いに関する方針の策定及び公表について定め、責任体制を確保する必要がある。

1. 組織体は、国の個人情報保護に関する法律及び施行令並びに基本方針に則って、個人情報の取扱いに関する方針の策定及び公表並びに責任体制の確保を行うこと。
2. 個人情報の取扱いに関する方針の策定及び公表並びに責任体制の確保について、文書化され、組織体の長が承認していること。
3. 個人情報の取扱いに関する方針の策定及び公表並びに責任体制の確保について、関係者に周知徹底し、従業者の啓発を行うこと。
4. 責任体制の一環として、個人情報の取扱いの委託について、委託の有無や、委託する業務の内容を明らかにする等、委託処理の透明化を進めること。
5. 組織体が認定個人情報保護団体に所属する場合、その旨、本人に明確な表示となる措置を講じること。

(2)	個人情報の取り扱いに関する方針に基づいて、個人情報を取り扱う情報システム（以下"個人情報システム"という。）の開発及び保守の計画を定め、個人情報保護管理者が承認すること。

1. 個人情報システムの開発、運用及び保守の計画は、文書化され、個人情報保護管理者が承認していること。
2. 個人情報システムの開発、運用及び保守の計画は、関係者に周知徹底していること。
3. 個人情報システムの開発、運用及び保守の計画は、緊急事態を特定するための手順、それらにどのように対応するかの手順を準備していること。

4. 個人情報システムの開発、運用及び保守の計画は、「共通番号」を使用する個人情報システムの場合、あらかじめ、「共通番号」にかかわる個人情報の漏えい、滅失又はき損による影響範囲を認識し、影響度を分析し、対策を講じることができるように準備していること。

(3)	個人情報システムの開発及び保守の計画は、計画を実施及び運用するため、方法、体制等を明確にすること。

（主旨）個人情報システムの開発、運用及び保守の計画を実施及び運用するために、方法、体制等を明確にする必要がある。

1. 個人情報システムの開発、運用及び保守の計画は、実施及び運用するため、個人情報保護の要件を仕様化しシステム化する方法を確立していること。
2. 個人情報システムの開発、運用及び保守の計画は、実施及び運用するため、資源、役割、責任及び権限を明確にしていること。
3. 個人情報システムの開発、運用及び保守の計画は、実施及び運用するため、委託先を利用する場合の選定基準を明確にしていること。

(4)	個人情報システム開発及び保守の計画は、個人情報の正確性の確保及び個人情報の漏えい、滅失又はき損のリスクに応じ、必要かつ適切な安全管理措置を明確にすること

（主旨）個人情報システムの開発、運用及び保守は、計画の段階で、個人情報の正確性の確保及び個人情報の漏えい、滅失又はき損のリスクに応じ、必要かつ適切な安全管理措置を明確にしている必要がある。

1. 個人情報システムの開発、運用及び保守の計画は、個人情報を、それぞれの利用目的の達成に必要な範囲内において正確かつ最新の内容に保つための情報処理の措置を明確にしていること。
2. 個人情報システムの開発、運用及び保守の計画は、個人情報の漏えい、滅失又はき損のリスクに応じた安全管理措置を明確にしていること。
3. リスクは、個人データの取扱いの流れに従い、取得・入力、移送・送信、利用・加工、保管・バックアップ、消去・廃棄など、その局面ごとに認識していること。
4. 安全管理措置は、本人が被る権利利益の侵害の大きさや、事業の性質及び個人データの取扱状況等を考慮していること。
5. 個人情報システムの開発、運用及び保守に当って、既存のアプリケーションを利用する場合は、アプリケーションの安全性を確認していること。

8.2　本人の権利・利益の保護(６)

(1)	個人情報システムは、個人情報の取得に当たって、利用目的を明示し、利用目的の偽りなどにならない措置を講じること。

（主旨）個人情報システムによって、個人情報を取得するときは、利用目的の表示が、利用目的の偽りなどにならない措置を講じる必要がある。

1. 個人情報システムは、個人情報を取得する画面の利用目的の表示が、偽りの表示になっていないこと。
2. 個人情報システムは、個人情報を取得する画面の利用目的の表示が、正しくかつできるだけ具体的な表示、例えば、その取り扱う事業内容を勘案して顧客の種類ごとに利用目的を限定して示す

など、本人にとって明確な表示になっていること。

3. 個人情報システムは、個人情報の取得元又はその取得方法（取得源の種類等）を可能な限り具体的に表示していること。

(2)	個人情報システムは、個人情報の入力に当たって、本人から利用目的の認識又は同意を得る措置を講じること。

（主旨）個人情報システムによって、個人情報をシステムに入力するときは、個人情報の利用目的を明示して本人から利用目的の認識又は同意を得る措置を講じる必要がある。

1. 個人情報システムは、個人情報をシステムに入力するとき、個人情報の利用目的を明示して本人から利用目的の認識及び同意を得る措置を講じていること。
2. 個人情報システムは、個人情報をシステムに入力するとき、本人の選択によって利用目的を限定できるように措置を講じていること。

(3)	個人情報システムは、個人データの利用にあたって、取得に際して特定した利用目的に合うように出力を制限する措置を講じること。

（主旨）個人情報システムによって、個人データを利用するに当っては、取得に際して特定した利用目的に合うように出力を制限する措置を講じる必要がある。

1. 個人情報システムは、個人データの利用に当たって、取得に際して特定した利用目的の目的外利用にならないように出力を制限する措置を講じていること。
2. 個人情報システムは、個人データの利用に当たって、第三者への提供によって目的外利用になることのないように、出力を制限する措置を講じていること。

(4)	個人情報システムは、保有個人データの開示等の求めに応じる措置を講じること。

（主旨）個人情報システムは、個人情報の本人に対して保有個人データの開示等の求めに遅滞なく応じる措置及び保有個人データを出力する措置を講じる必要がある。

1. 個人情報システムは、本人に対して開示等の求めに遅滞なく応じる措置を講じていること。
2. 個人情報システムは、求めに応じて保有個人データを出力する措置を講じていること。
3. 個人情報システムは、保有個人データについて本人から求めがあった場合には、ダイレクトメールの発送停止など、自主的に利用停止に応じる措置を講じていること。
4. 個人情報システムは、求めに応じて個人情報の取得元又はその取得方法（取得源の種類等）を可能な限り具体的に出力できる措置を講じること。

(5)	個人情報システムは、苦情の処置に応じる措置を講じること。

（主旨）個人情報システムは、本人の苦情及び相談に対して、適切かつ迅速な処理ができる措置を講じる必要がある。

1. 個人情報システムは、本人の苦情及び相談に対して、正しく適切な処理ができる措置を講じていること。
2. 個人情報システムは、本人の苦情及び相談に対して、迅速な処理ができる措置を講じていること。

(6)個人情報システムは、個人情報の保管期間と廃棄の過程が明確である措置を講じること。

（主旨）個人情報システムは、個人データの保管に当たって、法令等や業務要件に適合する保管期間が特定され、その保管期間を超える保管又はそれ以前の誤廃棄がないように、保管期間と廃棄の過程が明確である措置を講じる必要がある。

1. 個人情報システムは、個人データの保管に当たって、法令等や業務要件に適合する期間保管され、その保管期間を超える保管がないこと。
2. 個人情報システムは、個人データの保管に当たって、法令等や業務要件に適合する期間保管され、それ以前の誤廃棄がないこと。

8.3　個人情報の利活用（２）

(1)個人情報システムは、苦情の処置に応じる措置を講じること。

（主旨）個人情報システムは、個人情報の有用な利活用のため、個人データベース等を維持管理する措置を講じる必要がある。

1. 個人情報システムは、個人情報の有用な利活用のため、個人データベース等を、正確かつ安全に、維持管理する措置を講じていること。
2. 個人情報システムは、個人情報の有用な利活用のため、個人データベース等を、有効かつ効率的になるように、維持管理する措置を講じていること。

(2)個人情報システムは、個人情報の有用な利活用のため、個人情報の保護に関する法令等に準拠して個人情報を公共のために提供できる措置を講じること。

（主旨）個人情報システムは、個人情報の保護に関する法令、ガイドライン等に準拠し、個人情報を公共のために提供できる措置を講じる必要がある。

1. 個人情報システムは、個人情報の保護に関する法令、ガイドライン等に準拠し、個人情報を公共のために提供できるように、検索する措置を講じていること。
2. 個人情報システムは、個人情報の保護に関する法令、ガイドライン等に準拠し、個人情報を公共のために提供できるように、出力する措置を講じていること。

■

次回は「第 26 章　プライバシーマーク認定後の維持・運用のポイント」をご紹介します。＞目次へ

個人情報保護監査研究会　http://www.saaj.or.jp/shibu/kojin.html　　以上