プライバシーマーク審査基準

JISQ15001：2017 附属書 A

管理目的及び管理策

株式会社ハピネックス

0 目次

A.3.1 一般

【管理目的】
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

1	管理策	この管理策に規定する 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者によって、組織が定めた手段に従って承認されなければならない S01。
	解説	(S01) 附属書 A で要求している管理策(A.3.2～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者によって、会社が決めたやり方で、承認されていること。

A.3.2 個人情報保護方針

【管理目的】
個人情報保護の理念を明確にし、公表するため。

個人情報保護の理念…個人情報保護に取り組む姿勢及び基本的考え方を指すが、本人の権利利益を尊重する意識を表したものとすることが望ましい。

A.3.2.1 内部向け個人情報保護方針

管理策

トップマネジメントは、5.2.1e)に規定する内部向け個人情報保護方針を文書化した情報には次の事項を含めなければならない S02。

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) 個人情報の取扱いに関する法令、国が定める指針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及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、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めの措置を講じなければならない S03。

解説

(S02)
トップマネジメントは、文書化した内部向け個人情報保護方針に、下記 a)～f)の事項を含めること(記載すること)。

a) 事業の内容や事業規模を考慮した上で、適切な個人情報の取得、適切な利用、適切な提供に努めること。
[目的外利用を行わないこと、目的外利用を行わないための措置を講じることを含む]
(注) 事業の内容及び規模を考慮・・・この文言をそのまま記載しただけでは不適合。
「当社の事業は○○であり、・・・・・・」と具体的に記載した方がよい。
b) 個人情報に関する法律、ガイドライン、条例等の規範を遵守すること。
c) 個人情報の漏えいや滅失、き損を防止し、是正すること。
漏えい・・・情報が外に漏れること (例 誤送信、不正アクセス)
滅失・・・なくなってしまうこと (例 紛失、誤廃、誤消去)
き損・・・壊れること、正確でなくなること (例 改ざん、誤入力、媒体の物理的破壊)
d) 苦情や相談に対して対応すること。
e) 個人情報保護マネジメントシステムの継続的改善に努めること。
f) トップマネジメントの氏名

(S03)
トップマネジメントは、文書化した内部向け個人情報保護方針を組織内に伝達し、必要な場合は、利害関係者が入手できるような措置を講じること。
利害関係者…従業者、委託先、協業相手など

★マイナンバー制度への対応

特定個人情報を適切に取り扱う旨を追記する。

★内部監査のポイント

■トップマネジメントが、個人情報保護目的を説明できること。
■文書化した内部向け個人情報保護方針に、a)～f)の事項が含まれていること。
■トップマネジメントが、文書化した内部向け個人情報保護方針を、組織内に伝達し、必要に応じて、利害関係者が入手できるような措置を講じていること。

A.3.2.2 外部向け個人情報保護方針

3	管理策	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、A.3.2.1 に規定する内部向け個人情報保護方針の事項に加えて、次の事項も明記しなければならない[S04]。 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 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、一般の人が知り得るようにするための一般の人が入手可能な措置を講じなければならない[S05]。
	解説	(S04) トップマネジメントは、文書化した外部向け個人情報保護方針に、A.3.2.1 a)～f)の事項に加えて、下記 a)、b)の事項を含めること(記載すること)。 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 (S05) トップマネジメントは、文書化した外部向け個人情報保護方針を、一般の人も知ることができるよう、一般の人が入手できるような措置を講じること。 (補足)「一般の人が知り得るようにするための措置」(附属書 B..3.2.2) ・・・ウェブサイトによる公開、会社案内に記載、等。 ★内部監査のポイント ■文書化した外部向け個人情報保護方針に、A.3.2.1 a)～f)の事項が含まれていること。 ■文書化した外部向け個人情報保護方針に、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 ■トップマネジメントが、文書化した外部向け個人情報保護方針について、一般の人が入手できる措置を講じていること。