

プライバシーマーク制度における欠格性の判断基準

平成 20 年 4 月 18 日
財団法人日本情報処理開発協会
プライバシーマーク事務局

1. 適用範囲

本基準は、「[プライバシーマーク制度設置及び運営要領](#)（以下「要領」という。）」第 8 条第 3 号、第 2 1 条第 1 項及び第 2 1 条の 2 第 1 項第 2 号でいう「この要領に基づき別に定める基準」として、事業者が起こした個人情報にかかる事故の欠格性の判断及びその運用に関する基準を定めたものである。したがって、この基準は、認定事業者、審査中事業者及び申請検討中事業者（以下、総称して「事業者」という。）の起こした事故等にも適用される。

2. 本基準の目的

プライバシーマーク制度に対する一般の信頼を維持することは、プライバシーマーク制度を運営する組織（当協会及び各指定機関）及び事業者の共通の利害である。

プライバシーマークは、JIS Q 15001 : 2006「個人情報保護マネジメントシステム—要求事項」に基づいて策定した基準「[JIS Q 15001 : 2006 をベースにした個人情報保護マネジメントシステム実施のためのガイドライン—第 1 版—](#)」に適合した個人情報保護のマネジメントシステムが実現できている事業者であることを認定するものであり、当該事業者が個人情報にかかる事故を起こさないことを保証するものではない。

しかしながら、本制度の信頼を維持するためには、事故を起した事業者に対する改善の指導及び是正措置の確認は、制度上不可欠である。そのために、事故を起した認定事業者には、その報告を義務付け（要領第 20 条第 4 号）ている。

本基準は、報告を受けた事故について、当該事業者に事故の重大さ(欠格性)の程度を認識させるために運用するものであり、更には、その結果を踏まえて、適正な改善策の策定と実施及び再発防止を徹底する機会を提供するものである。したがって、本基準の運用は、事故を起した事業者に対して罰則を科すためだけではないことに留意しなければならない。

3. 欠格性の判断と運用

3.1 事業者の報告

事業者は、以下の表に定める機関に事故を報告するものとする。報告は、報告先である指定機関又は当協会の定める手順に従って行うものとする（当協会に報告する場合の手順は[こちら](#)）。

事業者は、「2. 本基準の目的」の趣旨に鑑み、将来の大事故を未然に防ぐ観点から、

漏えい等した個人情報の件数が1件でもある場合は、これを報告するものとする。

表3-1 事故の報告先

① 認定事業者の場合	付与認定を受けた指定機関又は当協会。 ただし更新審査中の場合は、審査中事業者の例による。
② 審査中事業者の場合	付与認定の申請をしている指定機関又は当協会。
③ 申請検討中事業者の場合	付与認定の申請を予定している指定機関又は当協会。

3.2 事故に対する措置

事故報告を受けた指定機関又は当協会は、本基準に従い、発生した事象を評価して欠格レベルを決定し、指定機関の審査会（当協会の場合はプライバシーマーク制度委員会）の審議を経て、その欠格レベルに基づく措置を講ずるものとする。

なお、認定の一時停止及び認定の取消し相当の措置を講ずる場合については、必ずプライバシーマーク制度委員会の審議を経た上で決定する。

4. 欠格性の判断及び措置の決定

指定機関及び当協会は、以下に定める手順に従い、事業者の欠格性を判断し措置を決定するものとする。

4.1 欠格レベルの決定

- (1) 事故報告を受けた事象を事故の類型に分類する。
- (2) 事象が発生した原因を判断し、事業者の責任の有無を評価する。
- (3) 事象の発生に事業者の責任が有ると評価される場合、さらに事故の影響等（下表参照）を考慮する。ただし責任の有無の評価において、故意（会社ぐるみ）と判断された場合は、その時点で欠格レベルを10とし、さらに考慮することはしない。
- (4) 考慮した全ての事項に基づき、欠格レベルを0～10の範囲で決定する。

表4-1 欠格レベル決定の手順

(1) 発生した事象を分類 (事故の種類)	(2) 事象の原因を判断 (責任の有無を評価)	(3) 事故の影響等を 考慮	(4) 欠格レ ベルの決定
① 漏えい ② 紛失 ③ 破壊 ④ 改ざん ⑤ 不正取得 ⑥ 目的外利用・提供 ⑦ 不正使用 ⑧ 開示・訂正・削除に応 じない ⑨ 利用・提供の拒否に応 じない	故意 (会社ぐるみ)	考慮せず	10
	過失 (運用の不備、設備の不 備、監督責任等)	<input type="checkbox"/> 漏えい等した個人 情報の内容(機微な 個人情報等) <input type="checkbox"/> 本人被害の発生状 況 <input type="checkbox"/> 社会への影響又は プライバシーマ ーク制度への影響 <input type="checkbox"/> 過去の事故履歴	事象の内容 に応じて個 別に判断 (1~10)
	不可抗力 (対策不可能な災害や 事故等)	考慮せず	0

4.2 欠格レベルに基づく措置の決定

欠格レベルの0~10に相応した措置を、表4-2のように定める。指定機関又は当協会は、4.1により決定した欠格レベルに相応した措置を講じるものとする。

表4-2 欠格レベルに相応する措置

欠格 レベル	欠格レベルごとの措置		
	認定事業者(注1)	審査中事業者(注2)	申請検討中事業者
10	認定取り消し	否認決定	1年間の申請不可
8,9	一時停止(注3)	一時停止期間に該当する 期間審査中止(注3)	一時停止期間に該当する期間 申請不可(注3)
6,7	勧告文書発行	審査続行	申請可
1~5	注意文書発行	審査続行	申請可
0	措置なし	審査続行	申請可

注1: 認定事業者の起こした事故等の欠格レベルが1から7までの場合、注意または勧告の文書を発行するが、事故等の原因となった不具合についての是正措置の適切性を確認するための審査を行うことがある。

注2: 審査中事業者(新規に認定を受けるために審査中の事業者)の起こした事故等の欠格レベルが1から7までの場合、審査続行とするが、事故等の原因となった不具合についての是正措置の適切

性を確認するための審査を行うことがある。

注3: 認定の一時停止等の期間の開始日の判断は、事故等の発生日又は発生日が特定できない場合は発見された日をもとに行う。

5. 施行

本基準は、「プライバシーマーク制度における欠格性の判断基準の設定と運用について」(平成 18 年 3 月 31 日)を改正するものであり、平成 19 年 12 月 21 日から施行する。

以上