株式会社

PMS　04

個人情報の特定及びリスク分析と対策の手順に関する規程

第1版

2008年　月　日

改訂履歴

版数	改訂日	改訂理由、主な内容	作成	査閲	承認
1	08//	1版			

04 個人情報の特定及びリスク分析と対策の手順に関する規程

第1条（目的）

本規程は、当社が自らの事業の用に供するすべての個人情報を特定し、特定された個人情報についてそれぞれのリスクを分析し、その対策を策定する手順を規定することを目的とする。

第2条（用語の定義）

この規程で用いる用語の定義は、以下に記載したものを除き、基本規程によるものとする。ただし、個人情報保護法の第2条に定義があるものについては、当該定義を準用する。

(1) リスク

個人情報の取扱いにおけるリスクは、個人情報の漏えい、滅失又はき損、関連する法令、国が定める指針その他の規範に対する違反、想定される経済的な不利益及び社会的な信用の失墜、本人への影響などのおそれなどがある。

(2) 脅威と脆弱性

脅威とは、安全管理を脅かす事象をいう。

脆弱性とは安全管理に関する欠陥や PMS、規範、慣行の不徹底や未整備な状態をいい脅威が発生してしまう要因となるような状態をいう。

(3) 残存リスク

残存リスクとは、リスクを認識した上でそのリスクを低減させるための対策を講じた結果、まだ残っているリスクをいう。

この規程で用いる他の用語の定義は、基本規程によるものとする。ただし、個人情報保護法の第2条に定義があるものについては、当該定義を準用する。

第3条（個人情報の特定の遵守事項）

(1) 個人情報の特定

当社の事業活動における個々の業務において使用しているすべての個人情報を洗い出し、管理対象となる個人情報を特定する。

a. 個人情報保護管理者は、各部門の業務フローを「リスク分析表」の”業務フロー“欄に記入して各部門の保有する個人情報を全て洗出す。

b. 個人情報保護管理者は、部門毎、および業務毎の個人情報を集約し、「個人情報管理台帳」を作成する。

(2) 個人情報の整理と運用

a. 個人情報の重要度に応じて分類する。（個人情報の重要度分類はその情報の紛失、漏えいなどが経営に与える影響の大きさで分類する。）

b. 利用していない情報、今後とも利用する目処のない重要度の低い情報は廃棄する。

c. 特定した個人情報については、別に定める「個人情報取扱（部門・業務）マニュアル」に基づき運用する。

(3) 個人情報特定の追加と見直し

a. 新たな業務やプロジェクトが発生した時には上記の手順を実施するか、「個人情報新規取得申請書」を作成し、個人情報を特定する。その結果を受けて、「個人情報管理台帳」の更新を行う。また、「個人情報管理台帳」の適正性を検証するために年一回の定期的見直し（10 月）を行う。

b. 年一回（10 月）、規程の効果が十分発揮されているかどうかを検証し、規定の見直しを図る。

第 4 条（個人情報のリスク分析と対策の手順）

(1) リスク分析

「リスク分析表」を用いて、特定した個人情報についてその取扱いの各局面におけるリスクを洗出し、その影響度を分析する。リスク分析の手順としては、リスクを認識し、分析し、必要な対策を講じる。

a. リスクの認識

特定した個人情報について、その処理プロセス（入手、加工、保管、利用、廃棄）に従って、それぞれのステップにおけるリスクを洗い出す。

リスクとして、個人情報の漏えい、滅失または毀損、個人情報保護法・国の定める指針その他規範に対する違反、想定される経済的な不利益及び社会的な信用の失墜、本人への影響などの恐れがある。どのようなリスクがあるかを認識する。

b. 脅威の分析

脅威として不正アクセスや、紛失、破壊、改ざん、漏えい、その他の発生状況とその影響度を想定する。

個人情報を取り巻く環境（建物、フロア、情報システム）や規程の整備状況などからも脅威を認識する。

c. 脆弱性の分析とリスク評価

システム保護の脆弱性を分析する。脆弱性と脅威によりリスクの発生状況を推測し、リスクの評価を行う。

リスク評価は「リスク分析表」に従って個人情報の重要度、脅威発生の可能性、発生の際の影響度等をリスクが顕在化した後の当社経営への影響度、社会的風評、対応費用なども勘案しつつ実施する。

(2) リスク対策

a. リスク対策案の策定

リスク分析の結果に基づいて、リスク対策（安全管理策）を策定する。対策項目の選定にあたっては「JIS Q 15001:2006 の要求事項」、「経済産業分野のガイドライン第 20 条安全管理措置」等を参考にし、明確にする。

b.規程類への反映

必要な対策を定コストベネフィットをも加味しつつ実施の優先順位を決める。定めた対策については「リスク分析表」にしたがって内部規程、詳細規程に反映しその関連を明らかにする。

c.残存リスクの確認

リスク対策を策定した結果、未対応として残っているリスクを「リスク分析表」にしたがって残存リスクとして明確にする。残存リスクとして認識したリスクは、運用点検のための点検簿に反映し日常運用点検時に定期的に見直す。

残存リスクについては、人為的、偶発的、あるいは受容レベル以下のもの等が何らかの形で残っているはずであり、恣意的に残存リスクゼロとしてはならない。

(3) リスク分析表の作成

以上の分析と対策を「リスク分析表」にまとめる。

(4) 見直し

1) 定期的な見直し

年に1回（10月）、規程の効果が十分発揮されているかどうかを検証して、手順の見直し、リスク分析・対応の見直しを実施する。

2) 随時の見直し

個人情報のリスクの認識、分析及び対策についてその必要が発生した場合には手順の見直し、リスク分析・対応の見直しを実施する。

第5条（改定の手順）

本規程の改訂は、個人情報保護管理者が行う。