個人情報リスクアセスメント
マネジメント要領

株式会社三重県農協情報センター

改訂履歴

Ｒｅｖ	改 廃 内 容	実施日	作成者	承認日
1.0	新規作成	Ｈ１８０１２０	情報セキュリティ委員会事務局	Ｈ１８０１１７
1.1	機構改革に伴う部署変更 ４．（１）①ｂ部署変更･追加	Ｈ１８０４０１	情報セキュリティ委員会事務局	Ｈ１８０３２８
1.2	Ｐマーク現地審査による指摘 管理ツールからの出力帳表の名称と整合性をとる。	Ｈ２００４１０	情報セキュリティ委員会事務局	Ｈ２００４０８
1.3	規程間の整合性を保つため	Ｈ２１１００１	情報セキュリティ委員会事務局	Ｈ２１０９２５
1.4	規程名称変更等	Ｈ２２１１２２	情報セキュリティ委員会事務局	
1.5	「脅威・脆弱性一覧表（個人情報保護)」(別表１）追加等	Ｈ２４０３０１	情報セキュリティ委員会事務局	
2.0	個人情報管理台帳、個人情報評価グループの見直しに伴う、個人情報リスクアセスメント手順の変更（情報資産管理ツール M@gicPolicy の利用停止）	Ｈ２９１０１５	情報セキュリティ委員会事務局	

個人情報リスクアセスメントマネジメント要領

規程番号　０３０３－０００－０１－要
制 定 日　２００６年　1月２０日
改 正 日　２０１７年１０月１５日

１．本文書の位置付け

本文書は、個人情報に関するリスクアセスメントおよびリスクマネジメントの手順について詳細を定める文書である。

２．リスクアセスメントの目的

リスクアセスメントは、個人情報、付随する情報資産がさらされている脅威およびその脅威によって利用される可能性がある脆弱性を明確にし、喪失される各個人情報の機密性、完全性および可用性が当社に与える影響の度合いを明らかにすることが目的である。

３．リスクアセスメントの対象

リスクアセスメントの対象は、「情報資産洗出し要領」に則って作成された「個人情報評価グループ一覧」の評価グループ単位とする。

４．リスクアセスメントの方法

「情報リスクアセスメントマネジメント要領」に従い、リスクアセスメントを実施する。

（１）個人情報の特定と「個人情報管理台帳」の作成

「情報資産洗い出し要領」をもとに、当社が保有する個人情報、付随する情報資産およびその管理責任者、価値、利用目的などを特定する。

取り扱う情報資産は多種、多様であり、その中でも個人情報は最重要情報であることから、個人情報を特定して「個人情報管理台帳」で一元管理する。

「個人情報管理台帳」は個人情報問合せ窓口担当者等が、後述の業務データフロー図と合わせて、取り扱う個人情報がどのように管理されているかを把握するためにも使用する。

① 作業手順

特定した個人情報は、「情報資産洗出し要領」に従い「個人情報管理台帳」へ登録する。

② 個人情報の保管状況確認

個人情報保護部門管理者（情報セキュリティ責任者）は、「個人情報管理台帳」に登録されている個人情報が保管されていることを年 1 回確認し、確認結果を個人情報保護管理委員会（情報セキュリティ委員会）に報告する。

（２）業務データフロー図および「個人情報評価グループ一覧表」の作成

情報資産洗い出し要領」をもとに、「個人情報管理台帳」に登録した個人情報の入手先・提供先を特定し、当社内における情報処理が適切に実施されているかをデータフロー図により表現する。記入内容の詳細は「業務データフロー図作成要領」を参照する。

作成した業務フローの単位で、個人情報評価グループを定義して、「個人情報評価グループ一覧表」を作成する。

（3）脅威・脆弱性の明確化と評価

「脅威・脆弱性一覧表（個人情報保護）」（別表１）を基準に、脅威と脅威に対する脆弱性を明確にする。評価については、「情報リスクアセスメントマネジメント要領」に従い実施する。

（4）リスク値の算出およびリスク評価

「情報リスクアセスメントマネジメント要領」に従い実施する。なお、リスク評価にあたっては、情報資産にかかる「詳細リスク分析表」と「個人情報詳細リスク分析表」を作成する。

5．リスクマネジメントの目的

個人情報リスクマネジメントは、個人情報および付随する情報資産に関するリスクが顕在化されることによって発生する損失を最小化することが目的である。

6．リスクマネジメントの方法

「情報リスクアセスメントマネジメント要領」に従い、リスク値からリスク対応要否を判定し、リスクの「受容」「低減」「移転」「回避」などの視点からリスクマネジメントを実施する。

マネジメント結果は、リスク対応要と判定されたリスクについては「詳細リスク分析表（個人情報）」の項目「リスク対応（実施すべき対策）」「予定リスク値」に登録する。

7．リスク対応計画の策定

「情報リスクアセスメントマネジメント要領」に従い、リスク対応計画を策定する。

8．本文書の改訂

本文書は、以下のいずれかの条件で見直す。

・対象とする組織、資産、情報処理施設／設備などの変更
・重大なセキュリティ問題の発生
・セキュリティ上の新たな脅威の発生
・１年に１度