

2 遵守事項

2.1 セキュリティ事件・事故の定義

セキュリティ事件・事故について以下に定める。

(1) セキュリティ事件

個人情報保護マネジメントシステムに対するルール違反と定義する。

例: 情報資産(個人情報を含む)の勝手な持出し、情報資産、個人情報(含む)の漏洩等

(2) セキュリティ事故

個人情報保護マネジメントシステムに規定するセキュリティ情報資産(個人情報を含む)及び業務に関する欠陥・不具合・故障等の発生及び**個人情報保護推進責任者**の判断で認定したものと定義する。

例: ウィルス感染、ネットワーク機器の故障等

(3) 情報セキュリティの弱点

個人情報保護マネジメントシステムで定められ管理上では情報資産が漏れた状態と定義する。

例: リスクアセスメント実施時の考慮もれの脅威や脆弱性、より情報資産(個人情報を含む)が危険な状態になる恐れがある場合等

(4) ソフトウェアの誤動作

使用しているソフトウェアが予期した動作をしなかった場合と定義する。

例: ウィルスによるソフトの誤動作(バグ)等

本規程は「個人情報保護基本規程」に定める適用範囲とし、日常かつ緊急的に発生する情報セキュリティ事件・事故及び事件について定める。

2.2 報告指示体制

社員等は、当社において情報セキュリティ事件・事故が発生した場合、またはセキュリティ欠陥、若しくはその脅威や疑い、事故が起る可能性を目撃した場合、速やかに**個人情報保護管理者**に報告を行う。

また、対応策等についての報告についても本規程で定められた報告指示体制に従い、速やかに実施しなければならない。

情報セキュリティ事件・事故のレベルについては、以下に示す。

- ・ レベル1 (深刻度: 低) ⇒ 部門
問題の発生原因・発生範囲とも一部門に限定される場合。
- ・ レベル2 (深刻度: 中) ⇒ 会社全体
セキュリティ侵害により、会社全体が被害者となる場合。