公益財団法人ＲＡＫＥＲ
情報セキュリティ基本方針

（目的）

第１条　公益財団法人ＲＡＫＥＲ（以下「当財団」という。）は、情報資産を適切に管理・保護することが法人運営の基本であり、社会的信頼の維持および公益目的事業の継続に不可欠であると認識し、本基本方針を定める。

（適用範囲）

第２条　この方針は、当財団の全ての評議員、理事、監事及び顧問等、雇用関係にある職員（正職員、契約職員、臨時職員、嘱託、パート職員、アルバイト職員等）（以下、「役職員等」という）および関係者に適用する。

（対象とする情報資産）

第３条　当財団が保有・管理する紙・電子媒体の文書、個人情報、財務データ、業務システム、端末、サーバ、クラウドサービス、人的資源等の全ての情報資産を対象とする。

（管理体制）

第４条　当財団は、理事長のもとに情報セキュリティ管理責任者（事務局長）を配置し、必要に応じてコンプライアンス・リスク管理委員会と連携しながら、情報セキュリティに関する施策を実施する。

（リスク対策と教育）

第５条　情報資産の重要度とリスク評価に基づき、適切な技術的・物理的・人的対策を講じる。役職員等に対しては、定期的に情報セキュリティ教育を行い、意識の向上を図る。

（インシデント対応体制）

第６条　情報漏洩・不正アクセス・紛失・改ざん等のインシデントが発生または疑われた場合は、速やかに情報セキュリティ管理責任者へ報告し、以下の体制により対応する。

（１）初動対応：事実確認、被害拡大防止措置、関係者の一次連絡

（２）原因分析と対応：影響範囲の調査、再発防止策の検討

（３）報告：理事長および必要に応じて理事会・監事・関係機関へ報告

（４）文書化：インシデント報告書の作成および記録管理

（継続的改善）

第７条　ＰＤＣＡサイクルに基づき、情報セキュリティ体制を定期的に見直し、必要に応

じて改善を行う。

（改廃）
第８条 この方針の改廃は理事会の議決を経て行う。

附則　この規則は法人の設立の登記の日から施行する。