一般社団法人　日本動脈硬化学会情報セキュリティ・ポリシー

１．情報セキュリティの基本方針

一般社団法人日本動脈硬化学会（以下、日本動脈硬化学会）が、高度に情報化した 21 世紀世界において十分な学術研究活動を行い、国民に対するその使命を全うするためには、情報基盤の整備をするのみならず、日本動脈硬化学会の情報資産の情報セキュリティを確保することが必要である。一般社団法人日本動脈硬化学会情報セキュリティ・ポリシーは、情報セキュリティを確保するために必要な取り決めを明文化したもので、基本方針と対策基準からなる。さらにこの情報セキュリティ・ポリシーの確実な実施のために、具体的な実施手順を定めることとする。これらは、情報セキュリティの重要性の認識とともに、日本動脈硬化学会が保有する全ての情報資産の情報セキュリティを確保するために定めるものである。

２．情報セキュリティ・ポリシーの目標

情報セキュリティ・ポリシーが対象とする利用者等及び対象物は以下の通りである。

利用者等

日本動脈硬化学会の会員、役員・職員、その他本学会保有の情報資産に対するアクセスを認められている者(共同利用者・外部委託先作業者など)。

対象物

日本動脈硬化学会が保有する全ての情報資産。情報資産は「情報」と「情報システム」を含む。「情報」は、それを表現する媒体(磁気的媒体、光学的媒体、紙媒体など)の種類を問わない。磁気ディスク、フラッシュメモリ、手書きメモは対象になる。「情報システム」は、「情報」を扱うためのシステムであり、電子的システムだけでなく、紙媒体のようなシステムも含む。なお、本学会以外の情報システムに保管されるものであっても、日本動脈硬化学会保有の情報資産として認められるものは対象となる。

日本動脈硬化学会情報セキュリティ・ポリシーが目指すものは次の通りである。

１．日本動脈硬化学会保有の情報資産に関する、重要度による分類と相応の管理の徹底
２．日本動脈硬化学会保有の情報資産に対する侵害からの防衛
３．日本動脈硬化学会内外の情報資産に対する加害行為の防止
４．日本動脈硬化学会内におけるセキュリティ侵害等の早期検出と迅速な対応の実現

３．情報セキュリティ・ポリシーの基本方針

（１）組織・体制

日本動脈硬化学会に学会全体に対する最高情報セキュリティ責任者を置く。最高情報セ

キュリティ責任者は、日本動脈硬化学会の情報セキュリティに関する総括的な意思決定を行う。最高情報セキュリティ責任者は、学会内及び学会外に対する日本動脈硬化学会としての情報セキュリティに関する責任を負う。最高情報セキュリティ責任者は、情報セキュリティに関する施策を定め、それを学会内に徹底させるために必要な措置を実施する権限を有するものとする。

（2）情報セキュリティ・ポリシー及び実施手順の策定

現状の情報資産の管理状況を把握するために学会全体として情報セキュリティ調査を定期的に実施する。情報セキュリティ調査の結果に対してリスク分析を行い、対策基準及び実施手順を作成する。情報セキュリティ・ポリシーと実施手順は定期的に見直す。

（3）情報の分類と管理

情報の分類を行い、適切な情報管理方法を定める。

（4）情報システムの情報セキュリティ

情報システムの管理方法を定める。

（5）情報セキュリティ要件の明確化

日本動脈硬化学会内及び外部からの不正アクセスによる情報資産の破壊、損傷、改竄、利用及びサービスの停止等を防止するため、情報セキュリティ要件を定める。

（6）人的情報セキュリティ情報

セキュリティ・ポリシーが遵守されるように規則類を整備する。情報セキュリティ・ポリシーの周知と遵守のために教育・研修を実施する。

（7）情報セキュリティ事案への対応

情報セキュリティ事案(情報セキュリティに関する事故及び障害)への対応方法を定める。

（8）情報セキュリティ・ポリシー違反に対する措置

情報セキュリティ・ポリシー違反に対する措置の決定手続きを定める。

（9）問合せ及びクレーム受付窓口、広報

問合せ及びクレーム受付窓口の設置と広報の体制について定める。

（10）自己点検及び情報セキュリティ監査

自己点検及び情報セキュリティ監査について定める。

（１１）予防的調査

予防的調査について定める。

（１２）予算案の作成

学会全体としての情報セキュリティ関連の予算案の立案方法を定める。

（１３）例外措置

例外措置を行う手順を定める。