公益財団法人日本オリンピック委員会
情報セキュリティ基本方針

令和３年６月10日
公益財団法人日本オリンピック委員会理事会決定

公益財団日本オリンピック委員会（以下「本会」という。）は、関係先等により提供される情報及び本会の事業遂行にかかわる情報等について、情報セキュリティを確保することを社会的責任と認識し、これを適切に推進するため、本会内に情報セキュリティ管理システムを確立し、計画・運用・見直・改善を継続的に実施する。本会は、情報セキュリティ管理を重要な活動のひとつと定め、情報セキュリティ基本方針を定める。

１　情報セキュリティの目的

本会は、情報セキュリティ管理システムの運用を適切に実施することにより、本会で取り扱う情報の重要度に応じた「機密性」*、「完全性」*、「可用性」*を確保し、情報の漏えい、改ざん、盗難等の情報セキュリティ事故を未然に防止し、社会との信頼関係を維持することを目的とする。なお、詳細については情報セキュリティハンドブックにて定めることとする。

２　情報セキュリティの推進体制

本会は、情報セキュリティ管理体制を整備し、PDCA（Plan（計画）・Do（実行）・Check（評価）・Action（改善））サイクルによる運用・見直しにより、安全性・信頼性を高め、事件や事故の未然防止に努める。

３　業務委託先の管理体制強化

本会は、業務委託を行う際には、業務委託先としての情報セキュリティに関する適格性等を確認し、本会と同等以上の情報セキュリティレベルを維持するよう努める。また、これらの情報セキュリティレベルが適切に維持していくために契約内容の確認を行う。

４　情報セキュリティリスクアセスメントの実施

本会は、情報を情報セキュリティ上の脅威から保護するため、重要度に応じた適正なリスクアセスメントを実施する。

５　情報セキュリティの教育、訓練

本会は、本会の役職員に対して必要な情報セキュリティに関する教育・訓練を実施し、情報セキュリティ管理の活動の重要性を認識させることにより、情報モラルの向上を図る。

６　情報セキュリティ検査の実施

本会は、情報セキュリティに関する各種運用の状況等について定期的に検査を実施し、必要に応じ適切な改善措置を講じることにより、情報セキュリティの確保に努める。

*)　・「機密性」とは情報にアクセスすることが認可された者だけがアクセスできること。
　　・「完全性」とは情報及び処理方法の正確さ及び完全である状態を安全防護すること。
　　・「可用性」とは許可された使用者が、必要時に、必要な情報及び関連情報にアクセスできること。