Japan Clinical Oncology Group

ポリシー No. 32
タイトル：情報セキュリティポリシー
適用範囲：JCOG 構成メンバー全体（研究者、各種委員会委員、データセンターおよび運営事務局スタッフ）ならびに委託業務の従事者等

情報セキュリティポリシー　Information Security

1. 基本方針

1.1. 本ポリシーの目的

JCOG は、個人情報、診療情報、解析情報、安全性情報等の秘密情報の他、論文・学会発表などの公開情報を含む JCOG 研究に関するすべての情報と、その取り扱いや管理のために用いるコンピュータ等の情報システム（以下、情報資産）を保有している。これらの情報資産は、JCOG 研究の適正評価と信頼性・継続性確保のために不可欠なものである。そこで、この重要な情報資産を改ざん・破壊・漏洩等から保護・管理していくために本ポリシーを定め、適切な安全対策を講じ、これを遵守することにより「情報セキュリティマネジメント」の確実な実施に努めることを本ポリシーの目的とする。

※秘密情報の開示や公開に関する規準については、本ポリシーの目的に含めない。個人情報、診療情報の取り扱いについては、JCOG ポリシーNo.31「プライバシーポリシー」に準じ、その他の秘密情報の開示は JCOG 代表者の判断により行う。

1.2. 本ポリシー策定の経緯と基本方針

情報セキュリティにおいては IT（Information Technology）技術の目覚しい発展により、過去の経験の蓄積だけでは想定できない新たなセキュリティ上の問題点や弱点が常に存在し得る。そのため、JCOG では、「医療情報システムの安全管理に関するガイドライン」、「ISO/IEC 17799」等の情報セキュリティ管理体制（Information Security Management System：ISMS）に関するガイドラインを参考に、次の 3 項目を本ポリシーの基本的な考え方とする。

1）JCOG が保有する個人情報を始めとする秘密情報の保護は、情報セキュリティの上で、最も優先すべき事項とする。
2）JCOG 研究の信頼性を維持するため、JCOG 研究に関する情報を適正に保護・管理し、情報の完全性を確保する。
3）JCOG 研究の継続性を維持するため、情報資産が重大な障害、災害等のダメージを受けた場合でも、ダメージから速やかに回復し、研究活動を中断させない適切な予防策、および回復策を講じる。

1.3. JCOG が準拠する情報セキュリティに関する法令、規範、ポリシー

JCOG が準拠する情報セキュリティに関する法令、規範、ポリシーは、原則として以下の通りとする。

- 個人情報の保護に関する法律（平成 15 年 5 月 30 日法律第 57 号、最終改正：平成 15 年 7 月 16 日法律第 119 号）
- ヘルシンキ宣言（日本医師会訳）
- 臨床研究に関する倫理指針（厚生労働省）
- 疫学研究に関する倫理指針（文部科学省、厚生労働省）
- ヒトゲノム・遺伝子解析研究に関する倫理指針（文部科学省、厚生労働省、経済産業省）
- 医療情報システムの安全管理に関するガイドライン（厚生労働省）

・ISO/IEC 27001（JIS Q 27001）
・上記のうち、ヘルシンキ宣言については最新版を用いるが、各種倫理指針については、研究の着手時に施行されている倫理指針を用いることとする。

加えて、以下の JCOG ポリシーに従う。

・JCOG ポリシーNo.31「プライバシーポリシー」

1.4. 用語の定義

本ポリシーで取り扱う用語を、以下のとおり定義する。

1） 情報セキュリティ：情報の秘密性、完全性および可用性を維持すること。
2） 機密性（Confidentiality）：アクセスを認可された（authorized）者だけが情報にアクセスできることを確実にすること
3） 完全性（Integrity）：情報および処理方法が、正確であることおよび完全であることを保護すること
4） 可用性（Availability）：認可された利用者が、必要なときに、情報および関連する資産にアクセスできることを確実にすること
5） 情報資産：情報および情報を管理する仕組み（情報システムならびにシステム開発、運用および保守のための資料等）の総称
6） 情報システム：組織体（または社会・個人）の活動に必要な情報の収集・蓄積・処理・伝達・利用にかかわる仕組み
7） 個人情報：氏名、生年月日、その他の記述等により特定の個人を識別（特定）し得る情報
8） 診療情報：診断および治療を通じて得られた疾病名、治療内容、検査結果等の情報
9） 秘密情報：JCOG が保有する情報資産のうち未発表または、情報資産ごとに定義された限られた対象にのみ開示している非公知の情報または社会通念として秘密内容であることが明白なものの情報
10） 認証情報：JCOG 構成メンバーが JCOG の情報システムを利用するために、JCOG データセンター/JCOG 運営事務局より発行された、ID やアカウント、パスワード等の情報

※ 1）は ISO/IEC 27002（JIS Q 27002:2006）より引用
※ 2）3）4）は ISMS 認証基準（Ver.2.0）より引用
※ 5）は「国民のためのセキュリティサイト」
（URL http://www.soumu.go.jp/joho_tsusin/security/index.htm、総務省）より引用
※ 6）は情報システム学会ホームページ「情報システムの定義」
（URL http://issj.nuis.jp/concept/02/index.html）より引用
※ 7）は個人情報の保護に関する法律および臨床研究に関わる倫理指針を参考に定義したものであり、JCOG プライバシーポリシーで用いられる定義と同一
※ 8）は臨床研究に関わる倫理指針より引用（投薬名を治療内容に変更）したものであり、JCOG ポリシーNo.31「プライバシーポリシー」で用いられる定義と同一
※ 9）10）は本ポリシー策定上の整理のため、本ポリシー固有に定義

2. JCOG 構成メンバーの義務

情報資産に接するすべての JCOG 構成メンバーおよび委託業務の従事者等は、本ポリシーを遵守し、以下のセキュリティ対策を実践しなければならない。

2.1. 研究者、各種委員会委員

1） 所属する医療機関内において管理する JCOG の情報資産は、医療機関における諸規定に従い、研究者や各種委員会委員が適切に取り扱うこと。また、JCOG の秘密情報に関する

セキュリティが侵害された場合は、速やかに情報セキュリティ管理責任者へ報告すること。

2） JCOG データセンター、JCOG 運営事務局や研究事務局等と、秘密情報等を含んだ情報のやり取りを行う場合は、情報の紛失・漏洩・改ざん等が発生しないよう十分に注意すること。

特に、プライバシーに関する情報を含む秘密情報のやりとりについては、JCOG ポリシー No.31「プライバシーポリシー」を遵守すること。

3） JCOG データセンターから発行された JCOG Web System 個人アカウント※1、グループ ID※2 とそのパスワードは、JCOG の情報システムを利用する際のユーザー認証情報となるため、下記の規則に従って厳重に管理しなければならない。

- 個人アカウントとパスワードを他人に教えたり、他人と共有しないこと
- 個人アカウントとパスワードを紛失した場合は、速やかに JCOG データセンターへ報告すること
- 個人アカウント、グループ ID とそのパスワードを紙や電子ファイル等へ記録する場合は、その記録が他人の目に触れぬよう厳重に管理すること
- グループ ID とパスワードを JCOG の施設研究者以外の人に教えないこと
- グループ ID とパスワードを忘れた場合は、所属する施設の施設コーディネーターに尋ねること）
- 異動等により研究者/委員会委員としての登録内容に変更が生じた場合は、定められた手順に従い、速やかに JCOG データセンターに報告すること

※1 JCOG Web System 個人アカウント： JCOG Web System を利用するために研究者個人に発行される認証のためのアカウント

※2 グループ ID：JCOG の HP で、メンバー専用のコンテンツを閲覧するために研究グループ単位で発行される認証のための ID

2.2. JCOG データセンターおよび JCOG 運営事務局スタッフ

本ポリシー、および「5. 情報セキュリティ対策」における「情報セキュリティガイドライン」に基づき策定されたセキュリティ対策を実践しなければならない。

3. 情報セキュリティ管理体制

情報セキュリティ対策を適切に管理・推進するため、以下の管理責任者を置く。

- 情報セキュリティ管理責任者：JCOG 運営委員会副委員長

4. 情報資産に関するリスク管理

情報資産の評価とリスクアセスメントにより、情報資産の重要度、および関連する脅威や脆弱性を認識し、適切かつ必要十分な情報セキュリティ対策を維持できるよう努める。

万一、情報セキュリティ上の問題が発生した場合、迅速な原因究明を行い、最善の策を講ずるとともに、予防および維持改善に努める。

5. 情報セキュリティ対策

前項において洗い出された様々なリスクから情報資産を保護し、本ポリシーの実効性を確保するため、情報資産の取り扱いが特に集中する JCOG データセンターおよび JCOG 運営事務局については、以下の内容構成に基づいた具体的な情報セキュリティガイドラインを策定し、情報セキュリティ対策を講ずるものとする。

- 物理的セキュリティ対策
- 人的セキュリティ対策
- 技術的セキュリティ対策
- 運用におけるセキュリティ対策

6. ポリシーの周知、および教育

すべての JCOG 構成メンバーに対して本ポリシーを周知し、情報セキュリティに対する意識を向上させるための教育を継続的に実施する。

7. 違反への対応

本ポリシーに違反し、情報資産に関するセキュリティを侵害した場合は、その重大性、発生した事案の状況等に応じて情報セキュリティ管理責任者の決定による処分の対象とする。また、情報セキュリティ管理責任者は、処分の内容を JCOG 運営委員会にて報告する。

8. 情報セキュリティの評価と見直しの実施

情報セキュリティを維持・改善するため、本ポリシーおよび本ポリシーに基づいた適切な対策が確実に実施されているか見直しを行うための機会を定め、セキュリティレベルの高い、かつ遵守可能な情報セキュリティ対策の継続的改善に努める。

運営委員会初回承認日：2008/8/5
第 1 回改訂日：2009/7/10