情報セキュリティ規程

第1章　総　則

（目的）

第1条　この規程は、一般社団法人広域重度ケア連携機構（以下「当法人」という。）の定款第49条第2項の規定に基づき、当法人が運用するICT支援システムその他の情報資産の機密性、完全性及び可用性を確保するために必要な事項を定めることを目的とする。

（定義）

第2条　この規程において「情報資産」とは、当法人が取り扱う情報（支援対象者の身体状態、生活状況、バイタル、医療的ケア記録、支援記録、発達・成長記録等の要配慮性の高い情報を含む。）並びにこれを取り扱う情報システム、機器、記録媒体及び文書をいう。

（適用範囲）

第3条　この規程は、当法人の役員、職員及び当法人の情報資産を取り扱うすべての者（委託先を含む。）に適用する。

第2章　管理体制

（情報セキュリティ管理責任者）

第4条　当法人に情報セキュリティ管理責任者を置き、理事会の決議により選任する。

2　情報セキュリティ管理責任者は、情報セキュリティ対策の整備、実施状況の点検、従事者への教育及びインシデント対応を統括する。

（情報資産の分類）

第5条　情報資産は、その重要性及び要配慮性に応じて区分し、区分に応じた管理方法を定める。支援対象者の医療・介護・障害に関する情報は、最も高い管理区分として取り扱う。

第3章　技術的・物理的対策

（アクセス権限管理）

第6条　情報システムの利用者には、業務上必要最小限の範囲でアクセス権限を付与する。

2　アクセス権限は利用者ごとに個別に付与し、共用アカウントの使用を禁止する。異動・退職等の際は、遅滞なく権限を変更又は削除する。

3　要配慮性の高い情報へのアクセスについては、アクセス記録（ログ）を取得し、定期的に点検する。

（認証及びパスワード）

第7条　情報システムの利用に当たっては、本人認証を行う。パスワードは十分な強度を確保し、他者に開示し、又は推測されやすいものを使用してはならない。重要なシステムについては多要素認証の導入に努める。

（データの保護）

第8条　要配慮性の高い情報は、保存時及び通信時において暗号化その他の保護措置を講ずる。

2　情報資産は定期的にバックアップを取得し、復旧手順を整備する。

3　機器及び記録媒体の持出し、廃棄及び再利用に当たっては、情報の漏えいを防止する措置を講ずる。

（物理的対策）

第9条　情報システム及び重要な書類は、施錠管理その他の物理的保護措置を講じた場所に保管する。

（外部サービス及び委託先の管理）

第10条　クラウドサービスその他の外部サービスを利用する場合及び情報システムの運用等を委託する場合は、提供事業者のセキュリティ対策を評価のうえ選定し、秘密保持及び安全管理に関する事項を契約に定め、定期的にその履行状況を確認する。

第４章　運用

（従事者の遵守事項）

第11条　従事者は、この規程及び情報セキュリティ管理責任者の指示に従い、情報資産を適正に取り扱わなければならない。私有機器の業務利用及び業務情報の私的利用は、あらかじめ許可された場合を除き禁止する。

（教育・訓練）

第12条　当法人は、従事者に対し、情報セキュリティに関する教育・訓練を定期的に実施する。

（インシデント対応）

第13条　情報セキュリティ上の事故又はそのおそれを認知した者は、直ちに情報セキュリティ管理責任者に報告する。当法人は、被害の拡大防止、原因究明、復旧及び再発防止の措置を講じ、個人データの漏えい等に該当する場合は個人情報保護規程第14条の定めに従い対応する。

（点検及び見直し）

第14条　情報セキュリティ管理責任者は、対策の実施状況を定期的に点検し、その結果を理事会に報告するとともに、必要に応じて対策の見直しを行う。

第５章　雑　則

（改廃）

第15条　この規程の変更及び廃止は、理事会の決議による。

附　則

1　この規程は、令和〇年〇月〇日から施行する。

2　この規程は、令和〇年〇月〇日開催の理事会の決議により制定した。