大阪大学ライフデザイン・イノベーション研究拠点（iLDi）

2020 年 2 月

データポリシー＜セキュリティ編＞

本ポリシーは、大阪大学ライフデザイン・イノベーション研究拠点（iLDi）（以下、「研究拠点」という。）の研究プロジェクト及びグランドチャレンジ採択プロジェクト（以下、「iLDi プロジェクト」という。）において、データの安全な取り扱いに関し、最低限遵守すべき内容を示したものである。

１　本ポリシーの対象

iLDi プロジェクトにおいて研究や事業に従事する者（以下、「iLDi プロジェクト参加者」という。）。

２　セキュリティレベル

iLDi プロジェクトで取得あるいは利用するデータ及び／又はかかるデータに対し技術的に復元困難な加工等が施されたデータ（以下、「PJ データ」という。）の取り扱いに当たっては、データ毎にセキュリティレベルを指定し、レベルに応じた安全対策を講じるものとする。

セキュリティレベルは、セキュリティレベル３（高）、セキュリティレベル２（標準）、セキュリティレベル１（低）の３段階とする。

注）2019 年 10 月版からセキュリティレベルの序列を変更しました。（レベル３（低）→ セキュリティレベル３（高）、レベル１（高）→ セキュリティレベル１（低））

なお、各々のセキュリティレベルの中に細かい分類レベルを設けることは支障ない。

３　セキュリティレベルの説明

(1)　セキュリティレベル３（高）

特定の個人が識別できるなど、漏洩時に個人に直接被害がおよぶ恐れのあるもの。例えば、ローデータ等がこれに該当する。また要配慮個人情報を含むデータは原則としてセキュリティレベル３とする。

セキュリティレベル３のデータは、あらかじめ定めたセキュリティ管理エリア内でのみ、取り扱う。

(2)　セキュリティレベル２（標準）

ただちに特定個人の識別ができないもの。例えば、セキュリティレベル３のローデータに対して加工等を施したものがこれに該当する。

セキュリティレベル２のデータは、あらかじめセキュリティ管理エリアを定めることなく、契約等に基づき取り扱う。

(3)　セキュリティレベル１（低）

個人情報やプライバシーリスクのあるデータを含まないもの。例えば、統計データや、個人情報を含まないデータがこれに該当する。

セキュリティレベル１のデータは、研究拠点からは特に制限を設けることなく、所属機関のデータ管理方針に従って取り扱う。

４　各セキュリティレベルにおいて講じるべき対策

レベル毎に講じるべき対策については、別紙セキュリティチェックリストを参考にし、実施すること。

５　監査

情報セキュリティ専門委員会が実施するPJデータの取り扱い状況についての監査に協力すること。

６　その他

本ポリシー以外にも、所属する組織の規定や、分野ごとの法令、政府や学会等のガイドラインもあわせて遵守し、必要に応じて追加のセキュリティ対策を講じるべきものとする。

７　附則

本ポリシーは、令和元年 11 月 1 日から適用し、今後必要に応じて、適宜、見直しを行う。