セキュリティチェックについて

ライフデザイン・イノベーション研究拠点
情報セキュリティ専門委員会
春本　要

グランドチャレンジ研究で収集するデータについて

本委託事業で取得または収集した研究開発データは、研究拠点支援事業の「PLRプラットフォームで二次利用を行うデータ」の対象となり、原則としてライフデザイン・イノベーション研究拠点が管理するPLRの一部として利用するため、成果物として提出いただきます。

令和２年度「グランドチャレンジ研究」公募要領より抜粋

データの取り扱いについては、所属組織のデータ管理方針・規則に従うとともに、データのセキュリティレベルに応じた安全対策をお願いします。

セキュリティ管理体制

- **情報管理責任者 ＝ プロジェクトリーダー**
- **情報管理責任者が指名するデータ取り扱い責任者**
  - データ種別ごとに設定しても構いません。

- **データの漏洩やパスワード流出等の可能性が発生した場合、各所属機関の対応方法に従うとともに、情報管理責任者を通じてiLDi統括情報管理責任者にすみやかに報告してください。**

セキュリティレベルについて

- **セキュリティレベル３（高）**
  - 特定の個人が直ちに識別できる情報を含むデータ。
  - 漏洩時のリスクが非常に高いため、予め定めたセキュリティ管理エリア内でのみ取り扱う。
- **セキュリティレベル２（標準）**
  - 直ちに個人の識別ができないデータ。
    - たとえばセキュリティレベル３のデータに対して仮名化等の加工等を施したデータ。
  - セキュリティ管理エリアを定めずに取り扱ってもよいが、十分な安全対策は必要。
- **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データ。
  - ローデータに対して統計処理を施したデータなど。

セキュリティレベルの例

レベル３

収集したセンサデータを含むファイル等に、
個人を識別できる情報が含まれている

レベル３

IDと個人の対応表

レベル２

IDにより仮名化したデータ

レベル3のデータにおいて講じるべき対策

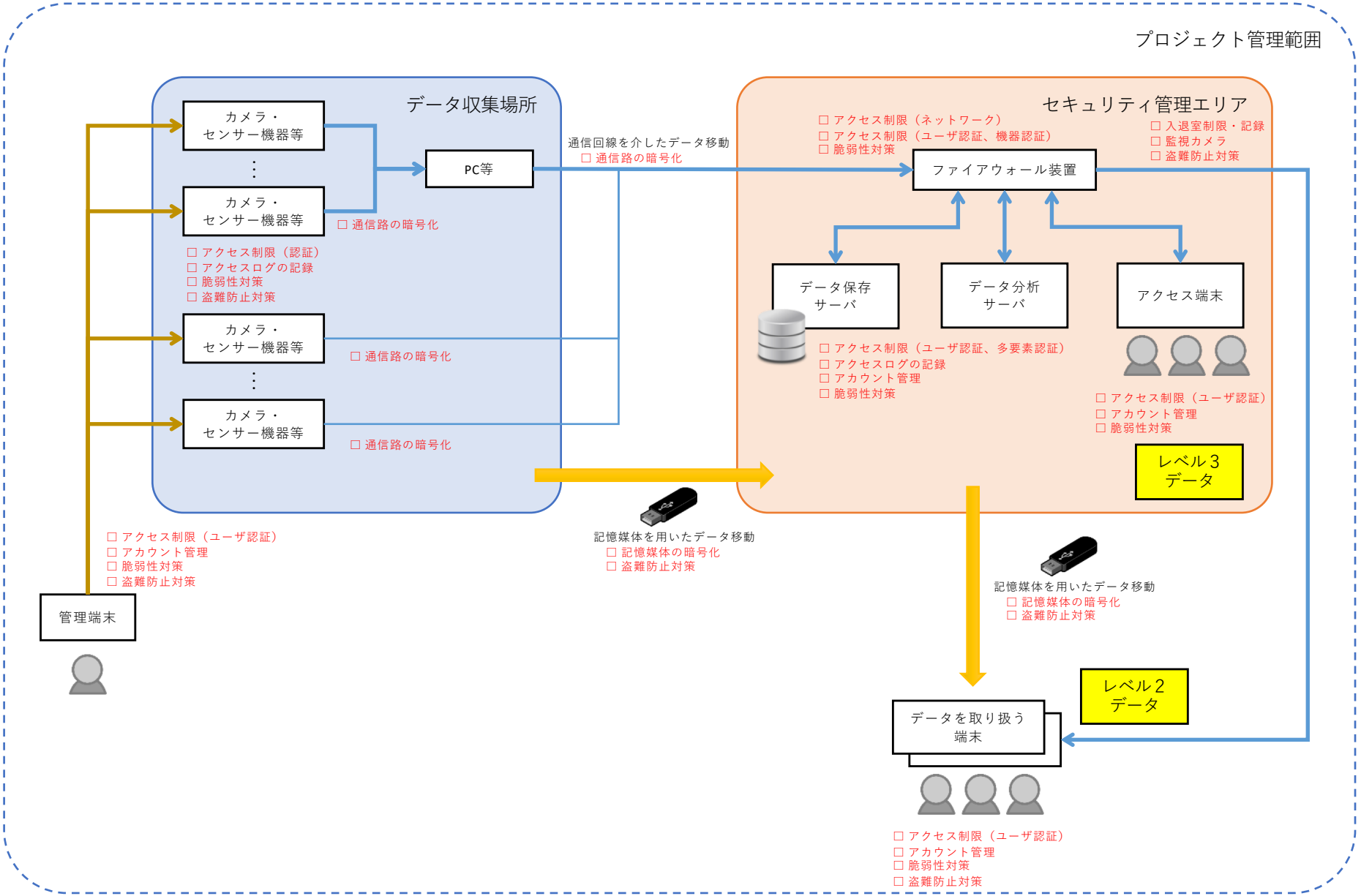
- **セキュリティ管理エリアの設定**
  - 常時施錠し、指定された者以外は立ち入れないようにする（必須）
  - ICカードや生体認証などにより入室した者を識別する（少なくとも入退室記録を行う）
  - 監視カメラの設置
  - 機器の盗難防止対策
- **データへのアクセス制限、記録**
  - 多要素認証の導入
  - アクセスログの記録、保管
- **データの移動・移送時の対策**
  - 通信路の暗号化、USBメモリ等の記憶媒体の暗号化

レベル2以上のデータにおいて講じるべき対策

- **データを取り扱う機器の管理**
  （サーバ、端末、センサ、ネットワーク機器等）
  - 機器一覧の台帳管理
  - 機器の紛失防止対策、盗難防止対策
  - ユーザ認証などによるアクセス制限
- **データを取り扱う者、端末の管理**
  - 誰がどのようなデータを取り扱うかを台帳等で管理
  - どの端末がどのようなデータを取り扱うかを台帳等で管理
  - アカウント管理
  - セキュリティ対策ソフトの導入、適切なアクセス制限の設定、ソフトウェアの最新版へのアップデートなどの脆弱性対策
- **公衆回線利用時の通信路の盗聴・改ざん対策**
  - 適切な暗号化など

【参考】

以下の図は、カメラ・センサー機器等でデータを収集し、レベル３データとしてセキュリティ管理エリアで保管する場合の例であり、
データを取り扱う各機器や通信路に望まれる安全対策を示したものです。



セキュリティチェックリストの提出について

- データマネジメントプラン（様式１）に記載したデータの種別ごとに、該当するレベルのチェックリストを作成し、ご提出ください。
- 複数のデータ種別を同じように取り扱う場合は、チェックリストはまとめていただいても構いません。
- チェックリストの各項目に対して、対応できない場合はその理由や代替策等を記載してください。

- 提出期限：４月末日
- 提出先：iLDi拠点本部 データマネジメント担当
  - datamanage@ids.osaka-u.ac.jp