

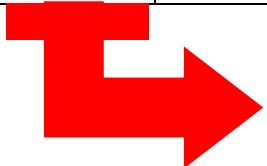
※ここでの記載内容は参考例であり、実際の審査での了承を保証するものではない

リスク分析・対応表(参考例)

運用フロー図の中で想定されている要介護認定情報等について

形態毎に想定されるリスクを洗い出し、それらリスクに対する対策等をリスト化し、利用者間で周知・徹底する。

	情報資産名	所在場所	運用状況	想定されるリスク	リスク対策	残存リスク	残存リスクへの対応
①	厚生労働省から提供を受けたデータ保存媒体	○○大学サーバ室	データ保存媒体の保管	・提供媒体の盗難、紛失による漏えい	・サーバ室の施錠と大学の○○課による入退室管理 ・媒体を施錠した戸棚に保管	・入退室のチェック漏れ ・戸棚の施錠忘れ	・2週間に1度、定期的に入退室管理や戸棚の施錠状況等を確認
②	サーバ内に電磁的に保存されている要介護認定情報等	○○大学サーバ室	要介護認定情報等を当該サーバに保存	・権限のない者による不正アクセス、漏えい	・サーバ室の施錠と大学の○○課による入退室管理 ・サーバを施錠したラックに格納し、サーバ室に入室した他部局の人間によるアクセスも防止	・入退室のチェック漏れ ・ラックの施錠忘れ	・2週間に1度、定期的に入退室管理やサーバラックの施錠状況等を確認
③	研究室に運ぶ際の外付けHDD内の要介護認定情報等	○○大学○○部○○研究室	サーバに保存した要介護認定情報等から分析のため一部切り出したデータを○○研究室へ運搬	・外付けHDDの盗難、紛失による漏えい	・台帳による外付けHDDの使用状況の管理 ・使用した後は○○研究室内の施錠した戸棚に外付けHDDを保管	・台帳への記入忘れ ・パスワードの設定忘れ ・外付けHDD使用後のデータ消去忘れ ・戸棚の施錠忘れ	・2週間に1度の管理状況の確認(外付けHDD内のデータや戸棚の施錠状況など含む) ・2ヶ月毎にパスワード設定の変更
④	○○研究室の端末内の要介護認定情報等	○○大学○○部○○研究室	厚生労働省から提供された要介護認定情報等から一部を切り出して分析	・端末の盗難、紛失による漏えい ・端末内への不正アクセスによる漏えい	・○○研究室について、入退室管理 ・持ち運びできないよう端末について施錠したチェーンにより固定 ・端末にIDとパスワードを設定し、アクセスを制限 ・インターネット等の外部ネットワークに接続しない	・入退室のチェック漏れ ・チェーンの施錠忘れ ・ID・パスワードの漏えい・設定忘れ	・2週間に1度の管理状況の確認 ・2ヶ月毎にパスワード設定の変更
⑤	要介護認定情報等の中間生成物を保存した外付けHDD	○○大学○○部○○研究室	端末で作成した中間生成物についてバックアップを外付けHDDに保存	・外付けHDDの盗難、紛失	・○○研究室について、入退室管理 ・持ち出されないように使用後は施錠した専用の戸棚に保管	・入退室のチェック漏れ ・戸棚の施錠忘れ	・2週間に1度の管理状況の確認 ・1日に1度の外付けHDDの所在確認
⑥	要介護認定情報等の中間生成物を打ち出した帳票	○○大学○○部○○研究室	端末で作成した中間生成物を紙媒体の帳票で出力し分析を実施	・帳票の盗難、紛失	・帳票は1枚毎に番号を振り、台帳管理 ・使用後は施錠した専用の戸棚に保管 ・利用後は速やかにシュレッダーで裁断し廃棄	・台帳への記載漏れ ・戸棚の施錠忘れ	・2週間に1度、定期的な管理状況の確認



(留意事項) 情報資産の考え方について

要介護認定情報等が保存されている媒体・端末・機器等を全て洗い出し、これらに対するリスク分析・対応表を作る必要があります。