20220830 情報セキュリティ委員会承認

# 情報分譲（スタンダード）に関するセキュリティポリシー　情報管理責任者用

本文書は、東北メディカル・メガバンク機構（以下、当機構と呼ぶ）より分譲されたスタンダードに分類されるデータを管理する者（以下、情報管理責任者と呼ぶ）が遵守すべきポリシーを、情報分譲に関するセキュリティポリシーの下で定める。

1. 情報管理責任者は、分譲されたデータ（以下、分譲データと呼ぶ）のセキュリティに関して、責任を持つこと。

2. 情報管理責任者は、分譲データを配置した分譲データ保存端末の設置場所やネットワーク環境およびソフトウェア環境が、セキュリティ上問題ないことを定期的に確認すること。

3. 情報管理責任者は、分譲データ保存端末のソフトウェアに脆弱性がないかを定期的に確認し、脆弱性の情報が得られた場合には速やかに対応を行うこと。

4. 情報管理責任者は、分譲データ保存端末の更新などやむを得ない事情のある場合を除き、分譲データの利用者に分譲データ保存端末から外部に分譲データをコピーさせないこと。

5. 情報管理責任者は、分譲データの利用が認められた期間が終了した際には、分譲データ（バックアップ等も含む）がすべて消去されていることを確認すること。

6. 情報管理責任者は、別途定める情報分譲（スタンダード）に関するセキュリティポリシー　情報管理責任者用チェックリストを定期的に確認すること。

7. 情報管理責任者は、分譲データの利用者に、別途定める情報分譲（スタンダード）に関するセキュリティポリシー　利用者用チェックリストを定期的に確認させること。

8. 情報管理責任者は、分譲データが漏洩した可能性が発生した場合には、速やかに当機構に書面（電子メールへの添付ファイルを含む）による報告を行うこと。

9. 情報管理責任者は、当機構から求めがあった場合には、当セキュリティポリシーの実施状況に関する監査に協力すること。