2024 年 10 月 2 日情報セキュリティ委員会承認

TMM データ情報セキュリティポリシー

目次

0. 改定の方針

0.1. 大まかな方針

- 基本的な理念はそのまま継承する
- 実態とチェックリストが乖離していた部分を修正し、特にスーパーコンピュータにおいて明文化されていなかったルールを明文化した
- 主に分譲や共同研究で利用する外部の人が迷わないようにするために整備する
- 必ずしもセキュリティ監査を受けるために各種文書を整えるためのものではない
- 形式的な文書を整えるのは今回の目的ではない
- 理念の部分だけを抜き出した文書を「TMM データ情報セキュリティポリシー 概要」として別に定める

0.2. 置き換える文書

- 情報分譲（ストロング）に関するセキュリティポリシー 利用者用
- 情報分譲（ストロング）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
- 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

- 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
- 情報分譲（ストロング）に関するセキュリティポリシー 情報管理責任者用
- 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
- 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
- 利用者用情報分譲（ストロング）に関するセキュリティ実施ポリシー
- 利用者用情報分譲（オープン）に関するセキュリティ実施ポリシー
- 東北メディカル・メガバンク機構　遠隔セキュリティエリアの利用手順書

0.3.　主要な変更点

- ストロングのセキュリティポリシーとチェックリストは実質的にスーパーコンピュータのセキュリティポリシーとチェックリストであったため、スーパーコンピュータのセキュリティポリシーとチェックリストに名称を変更
- 例えオープン、スタンダードのデータしか扱わなくても、スーパーコンピュータを使うなら本ポリシーとチェックリストが必須
- スタンダードのセキュリティチェックリストは実質的にスーパーコンピュータから持ち出したデータのセキュリティポリシーとチェックリストであったため、スーパーコンピュータ以外の計算機のセキュリティポリシーとチェックリストに名称を変更
- 情報管理責任者用と利用者用のセキュリティポリシーはどちらもほとんど同じ内容が書かれている場合が多かったので、統合し一部の項目に情報管理責任者のみの項目を設けた
- ストロングとスタンダードのセキュリティチェックポリシーの内容を一つの文書にまとめた
- 分譲用だったものを共同研究や機構内の研究にも適用されるように変更
- 本文書からチェックリストはマクロを使って自動生成予定

0.4.　用語の変更

一部、用語の変更を行っている

変更前	変更後	備考
分譲データ	TMM データ	分譲データ以外も対象とするため
分譲ストレージ	スーパーコンピュータ	わかりづらいため
分譲データ保存端末	データ保存計算機	分譲データ以外も対象とするため
情報持込持出責任者	情報持出責任者	持ち込みは自由なため

情報管理担当者	情報持出担当者	持ち出しの担当であることを明確にするため
エリア管理責任者（遠隔セキュリティエリア）	データ閲覧エリア責任者	用語を統一するため

1. セキュリティ分類

オープン

情報の種類

- 個人の同定につながる可能性がないと考えられる、大まかな統計情報

例

- ToMMo 全ゲノムリファレンスパネルのアレル頻度情報

利用方法

- ToMMo データベースサイト(jMorp)、公的データベース（NBDC ヒトデータベース等）でのオープンアクセス

利用手続き

- 基本は手続きなし
- 一部 Web 簡易 DTA

配送方法

- ユーザー登録無ダウンロード

スタンダード

情報の種類

- 個人の同定につながる可能性が低いと考えられる情報
- 個々の情報ではスタンダードだとしても、組み合わせにより、個人の同定の可能性が高まる属性情報の利用の場合にはストロングとする場合がある

例

- 年齢、性別の基本情報
- 検体検査情報、調査票情報等の健康調査情報
- Defaced MRI 画像（3 D-T1、3D-FLAIR）
- MRI 画像解析値情報

- 上記の情報を利用して選択された対象者のジェノタイプ頻度情報
- 30 個以下の遺伝子に含まれるジェノタイプ情報
- DNA メチル化情報

利用方法

- 原則、東北大学東北メディカル・メガバンク機構のスーパーコンピュータにおいて利用
- スーパーコンピュータ以外の計算機のセキュリティポリシーに合致した場合には分譲または共同研究・内部研究先の責任の下、分譲または共同研究・内部研究先の計算機において利用
- 公的データベース（NBDC ヒトデータベース等）での制限付き公開で利用

利用手続き

- TMM バイオバンクの標準的な分譲または共同研究・内部研究手続き・MTA または DTA

配送方法

- キーロック式 HDD/USB メモリにデータを収納し、セキュリティボックスで配送

ストロング

情報の種類

- 個人の同定につながる可能性が高いと考えられる情報
- ベリーストロングから分譲または共同研究・内部研究のために切り出したサブセットであり、TMM 内部でのみ用いられる tmm ID の代わりに分譲または共同研究・内部研究のために二次匿名化が行われた ID が付与されている
- スーパーコンピュータの中でのみ扱う

例

- ToMMo 全ゲノムリファレンスパネルの個人ごとの変異情報、配列情報の RAW データ
- MRI 画像（3D-T1、3D-FLAIR のみ）defacing なし

利用方法

- 東北大学東北メディカル・メガバンク機構のスーパーコンピュータにおいて利用

利用手続き

- TMM バイオバンクの標準的な分譲または共同研究・内部研究手続き・MTA または DTA

ベリーストロング

情報の種類

- Unit C で共有されているデータセット全体を指し、TMM 内部でのみ用いられる ID が付与されているゲノムデータ
- HIPAA の Limited Data Sets（16 項目の削除）に準拠した調査票・検査情報および臨床情報
- 分譲や共同研究では利用できず、TMM 内部でのみ利用可能
- Unit C にあるデータは基本的にはベリーストロングである
- スーパーコンピュータの中でも Unit C でのみ扱う

セキュリティ分類の参考資料

- All of US
  - https://www.researchallofus.org/data-tools/data-access/
  - Public Tier、Registered Tier、Controlled Tier の 3 種類
- UK Biobank
  - https://www.ukbiobank.ac.uk/enable-your-research/costs
  - Tier 1、Tier 2、Tier 3 の 3 種類

2. 用語説明

2.1. 情報

TMM データ

旧初期データ、分譲データ

東北メディカル・メガバンク計画において取得されたデータのことで以下のもの

- 東北大学東北メディカル・メガバンク機構から分譲される情報
- 共同研究・内部研究で用いる解析用情報

機構から提供されたオリジナルのデータのみならず、機構から提供されたデータを解析、加工を行ったデータも含む。TMM データは個人特定性の高さに応じてオープン、スタンダード、ストロング、ベリーストロングの 4 つに分類される。詳細はセキュリティ分類を参照すること。

バックアップデータ

TMM データを含むバックアップ用の複製データ

2.2.　組織、役割

TMM

東北メディカル・メガバンク計画

機構

東北大学東北メディカル・メガバンク機構

試料･情報分譲審査委員会

東北メディカル・メガバンク事業のバイオバンクに保管された生体試料および情報に係る分譲の仕組み等について総合的な検討を行うと共にともに、分譲申請があった場合は、総合的に評価し、分譲の可否について審査する。

試料・情報分譲担当

東北大学東北メディカル・メガバンク機構　バイオバンク利活用・産学連携推進センター　試料・情報分譲担当

統合データベース室

東北大学東北メディカル・メガバンク機構　統合データベース室

ゲノムプラットフォーム連携センター

東北大学東北メディカル・メガバンク機構　ゲノムプラットフォーム連携センター

ゲノプラセンターと略されることもある。

利用者

TMM データを利用する者。研究責任者も含む。

研究責任者

承認研究の責任者であり、例として以下の責任を負うが、以下に限らない。

- 研究分担者を代表し、分譲、共同研究、内部研究申請を行う
- 情報管理責任者を任命する（兼任も可）

情報管理責任者

TMM データの管理に全責任を持つ者であり、例として以下の責任を負うが、以下に限らない。

- TMM データのデータ漏洩が発生しないように監視する

- スーパーコンピュータのアカウント作成の申請を行う
- 情報持出責任者や情報持出担当者を任命する
- スーパーコンピュータの利用者にスーパーコンピュータのセキュリティポリシーを遵守させる
- スーパーコンピュータからのデータ持ち出しの際にストロングやベリーストロングが含まれないように確認する
- Unit B にベリーストロングが含まれないように確認する
- 利用者からのデータ持ち出し申請について可否を判断する
- スーパーコンピュータから持ち出したデータを利用する利用者にスーパーコンピュータ以外の計算機のセキュリティポリシーを遵守させる

情報持出責任者

旧情報持込持出責任者

情報管理責任者からデータの持ち出し権限の移譲を受けて持ち出しデータの確認および持ち出し承認を行うことができる者である。情報持出責任者に過失があった場合の責任は情報管理責任者が負う。

情報持出担当者

旧情報管理担当者

情報管理責任者に代わって持ち出しデータの確認および代理承認を行うことができる者である。必ず持ち出しの度に情報管理責任者から明示的な許可を得て作業しなければならない。情報持出担当者に過失があった場合の責任は情報管理責任者が負う。

データ閲覧エリア責任者

旧エリア管理責任者（遠隔セキュリティエリアの場合）

データ閲覧エリアの管理責任者である。データ閲覧エリアの管理およびデータ閲覧端末の管理を行う責任を負う。

2.3.　環境・機器

スーパーコンピュータ

本ポリシーにおいては東北大学東北メディカル・メガバンク機構が提供する大規模計算機環境のうち、ストロングに分類されるデータを扱うことを許可された区画。具体的には Unit B、プレリサーチ区画および Unit C が該当し、Unit A のようなインター

ネットに接続可能な開発用環境は含まない

データ閲覧端末

スーパーコンピュータに接続して解析情報を閲覧するための端末であり、機構が提供するデータ閲覧端末と利用者所有のデータ閲覧端末（利用者所有の共有データ閲覧端末、利用者所有の専有データ閲覧端末）がある。

機構が提供するデータ閲覧端末

解析情報を閲覧するための端末のうち、機構が貸与する複数の利用者で共有されるデータ閲覧端末でシンクライアント端末のこと。

利用者所有のデータ閲覧端末

利用者所有の共有データ閲覧端末と利用者所有の専有データ閲覧端末の総称

利用者所有の共有データ閲覧端末

解析情報を閲覧するための端末のうち、利用者が所有する端末であり、複数の利用者で共有されるデータ閲覧端末

利用者所有の専有データ閲覧端末

解析情報を閲覧するための端末のうち、利用者が所有する端末であり、特定の一人の利用者で占有されるデータ閲覧端末

データ閲覧エリア

スーパーコンピュータに接続するための部屋であり、要件はデータ閲覧エリアのセキュリティポリシーで定める。

データ保存エリア

データ保存計算機を設置する部屋であり、要件はスーパーコンピュータ以外の計算機のセキュリティポリシーで定める。

データ保存計算機

旧分譲データ保存端末

スタンダードに分類される TMM データを保存する計算機のうち、スーパーコンピュータ以外のもの。通常はスーパーコンピュータから持ち出したデータを保存する計算機のこと。

スタンドアローン計算機

旧スタンドアローンのコンピュータ

いかなるネットワークにも接続されていない計算機のこと。有線、無線問わず他の計算機と接続されていてはならない。

可搬媒体

外付け USB メモリ・ハードディスク等の記憶媒体

3. スーパーコンピュータのセキュリティポリシー

対象：スーパーコンピュータの利用者

3.1. 情報漏洩の防止

3.1.1. ストロングおよびベリーストロングに分類される TMM データをスーパーコンピュータの外に持ち出してはならない

ストロングおよびベリーストロングに分類される TMM データはスーパーコンピュータの中でのみ利用できます。このため、電子的なデータのみならずスクリーンショット、カメラによる画面撮影、その他いかなる形でも持ち出しはできません。例外として、スーパーコンピュータを操作するために画面転送によって一時的にデータ閲覧端末上に情報が投影されることは許可されますが、スーパーコンピュータを利用するための最小限の利用に限られ、スーパーコンピュータからの切断後は速やかに削除しなければなりません。

3.1.2. ベリーストロングに分類される TMM データはスーパーコンピュータのうちベリーストロングを扱うことを許可された区画（Unit C）から持ち出してはならない

ベリーストロングに分類される TMM データはスーパーコンピュータの中でも Unit C から持ち出してはなりません。このデータはすべてに紐づく ID が付与されているため、そのまま Unit B には転送できません。統合データベース室に依頼し、ID の書き換えを行うことでストロングとして Unit B に転送できるようになります。

3.1.3. TMM データへのアクセスは試料・情報分譲審査委員会または機構長に承認された利用者に限定しなければならない

TMM データを利用できるのは分譲の場合は試料・情報分譲審査委員会で承認された研究者、共同研究・内部利用の場合は機構長に承認された研究者に限ります。同じ組

織や研究室の人であっても試料・情報分譲審査委員会または機構長に承認されていない人は閲覧できません。

3.1.4. スーパーコンピュータの画面を記録してはならない。ただし、スーパーコンピュータの中で記録することは許可する

スーパーコンピュータの画面のスクリーンショットやカメラでの撮影等の方法を使って記録してはなりません。これはスーパーコンピュータの画面上にスタンダードやストロングに分類される TMM データが写っているかどうかに関わらず禁止されています。ただし、スーパーコンピュータの中で記録し、記録した画像や動画がスーパーコンピュータの中に留まる場合には例外として許可されます。もし記録したデータを持ち出したい時には、機構が指定した方法を用いて持ち出してください。

3.1.5. スーパーコンピュータからデータを持ち出す時には機構が指定した方法で行わなければならない

機構ではスーパーコンピュータから持ち出したデータの内容をすべて記録しています。確実にデータの内容を記録するために、データの持ち出しは機構が指定した方法で行ってください。

3.1.6. 情報管理責任者もしくは情報持出責任者の承認なくスーパーコンピュータからデータを持ち出してはならない

データの持ち出しには情報管理責任者もしくは情報持出責任者の承認が必要です。必ず指定の方法で承認を得て持ち出してください。

3.1.7. （情報管理責任者および情報持出責任者のみ）情報管理責任者および情報持出責任者はデータの持ち出しの際に別に定める「TMM データ持ち出し判断フロー」に従って持ち出し可否を判断しなければならない

原則として持ち出し可能なデータはオープンに該当する TMM データのみです。機構から提供されたオリジナルのデータを加工すれば持ち出しが可能になるわけではなく、個人特定性の高さで持ち出し可否が判断されます。例えば ID を書き換えただけや、SNV の場所を rs 番号に書き換えただけの個人ごとの全ゲノムデータを持ち出すことはできません。必ず内容を確認したうえで判断を行ってください。スタンダードと判定された TMM データは持ち出し可能ですが一定の条件があります。詳しくは TMM データ持ち出し判断フローおよびスーパーコンピュータ以外の計算機のセキュリティポリシーをご覧ください。

3.1.8. （情報持出担当者のみ）情報持出担当者は持ち出しの許可の代理承認にあたって情報管理責任者の許可を得なければならない

情報管理責任者が持ち出し管理システムにアクセスできない場合、情報持出担当者が持ち出し管理システム上で代理承認できます。この場合には以下のフローを経る必要があります。

- 持ち出し申請を行う者（以下申請者）が持ち出し管理システム上で持ち出し申請を行う
- 申請者が情報管理責任者にメール等のログが残る形で許可依頼を行う
  - この時に持ち出したいファイルの内容を詳細に説明してください。特に TMM データ持ち出し判断フローの分岐の判断が可能になるだけの情報を含めてください
- 情報管理責任者が情報持出担当者にメール等のログが残る形で持ち出し許可を出す
- 情報持出担当者が申請内容とファイルの内容に相違のないことを確認し、代理承認を行う
- 情報持出担当者が情報管理責任者に結果を報告する

3.1.9. 情報管理責任者もしくは情報持出責任者以外の者は自身の持ち出し申請を承認してはならない

情報管理責任者もしくは情報持出責任者でない者は、自身の持ち出し申請を自己承認できません。特に、情報持出担当者は自分以外の利用者の持ち出し申請については情報管理責任者の許可を得て代理承認が可能ですが、自身が申請した持ち出し申請は自身で代理承認できません。

3.1.10. TMM データの漏洩の可能性が発生した場合には速やかに情報管理責任者に報告し、情報管理責任者は書面で機構に報告しなければならない

万が一 TMM データの漏洩の可能性が発生した場合には、速やかに情報管理責任者を通して機構にご報告ください。

3.2. データ閲覧端末のセキュリティ

3.2.1. 機構が提供するデータ閲覧端末について機構から指示される場合にはセキュリティパッチを適用すること

機構が提供するデータ閲覧端末（シンクライアント端末）は管理者権限を機構で管理

しています。アップデートが必要な際は機構からお知らせが届きますで、指示通り作業を行ってください。

3.2.2. 利用者所有のデータ閲覧端末には利用者の責任で常に最新のセキュリティパッチを適用すること

利用者所有のデータ閲覧端末には利用者の責任で最新のセキュリティパッチを適用してください。Microsoft Windows のセキュリティアップデートは通常毎月第二火曜日の翌日に、Microsoft Edge のセキュリティアップデートは毎週行われますので、リリースされ次第アップデートをしてください。

3.2.3. 利用者所有のデータ閲覧端末は利用者の責任でアンチウイルスソフトウェアが有効で、常に最新のパターンファイルに更新されていることを確認すること

利用者所有のデータ閲覧端末には利用者の責任でアンチウイルスソフトウェアをインストールし、最新のパターンファイルに更新されていることを確認してください。Microsoft Windows 標準装備の Windows Defender でも問題ありません。

3.2.4. 利用者所有の専有データ閲覧端末は一定時間（5 分程度を目安）以上無操作の場合は認証機能により画面がロックされるように設定すること

利用者所有のデータ閲覧端末のうち、特定のユーザーに専有される端末は認証機能により画面がロックされるように設定してください。ロックの方法はパスワード、PIN、生体認証、セキュリティキーが利用できます。機構が提供するデータ閲覧端末と利用者所有の共有データ閲覧端末の場合にはデータ閲覧端末のロックは不要ですが、スーパーコンピュータの画面はロックする必要があります。

3.2.5. 利用者所有の共有データ閲覧端末は TMM データの閲覧端末としてのみ利用し、他の用途では利用しないこと

利用者所有の共有データ閲覧端末は TMM データの閲覧端末の用途のみで利用してください。

3.2.6. 利用者所有のデータ閲覧端末は内蔵ディスクの暗号化を行うこと

利用者所有のデータ閲覧端末は内蔵ディスクの暗号化を行い、万が一の紛失等で TMM データが漏洩しないようにしてください。暗号化は BitLocker 等の方法で行ってください。

3.2.7. データ閲覧端末には業務上不要なソフトウェアをインストールしないこと

機構が提供するデータ閲覧端末は様々な権限が制限されているためソフトウェアのインストールはできませんので、インストールを試みないでください。利用者所有のデータ閲覧端末は機構では管理しませんが、業務上不要なソフトウェアはインストールしないでください。特に P2P 等の技術を用いて不特定多数にファイルを共有するソフトウェアはインストールしないでください。

3.2.8. データ閲覧端末の画面が盗み見されないように対策を行うこと

データ閲覧端末の画面が盗み見されないように対策を行ってください。具体的にはパーティションの設置やデータ閲覧エリアへの入室管理を行ってください。複数人で一つのデータ閲覧端末を同時に閲覧する場合には、同席するすべての人がそのデータの閲覧を機構から許可されている必要があります。

3.2.9. データ閲覧端末はデータ閲覧エリアから持ち出さないこと

データ閲覧端末はデータ閲覧エリアから持ち出してはなりません。スーパーコンピュータに接続しない時でもデータ閲覧エリアに設置したままにしてください。

3.3. スーパーコンピュータへの接続方法

3.3.1. スーパーコンピュータへは機構が指定する方法で接続しなければならない

スーパーコンピュータへの接続には機構が提供するソフトウェアが必要です。提供しているソフトウェアを使う以外の方法でスーパーコンピュータに接続してはなりません。

3.3.2. スーパーコンピュータへの接続はデータ閲覧端末を用いてデータ閲覧エリアから行わなければならない

スーパーコンピュータへの接続はデータ閲覧端末を用いてデータ閲覧エリアから行ってください。データ閲覧端末をデータ閲覧エリアの外に持ち出してスーパーコンピュータへの接続や、データ閲覧端末以外の端末を使ってスーパーコンピュータへの接続をしてはなりません。

3.4. スーパーコンピュータのセキュリティ

3.4.1. データ閲覧端末から離れる場合にはスーパーコンピュータからログアウトもしくは接続を切断すること

データ閲覧端末から離れている間に他人に操作されないように、スーパーコンピュータからログアウトするか接続を切断してください。接続を切断したとしても一定時間内（2024 年 10 月現在は 5 時間以内）に再ログインすれば途中から作業を再開できます。

3.4.2. スーパーコンピュータの画面は一定時間（5 分程度を目安）以上無操作の場合は認証機能によりロックされるように設定すること

データ閲覧端末からログアウトもしくは切断せずに離席してしまった場合でも画面がロックされるように設定してください。通常は初期設定でロックされるようになっていますが、ロックされるまでの時間設定を変更して長くしないようにしてください。

3.4.3. スーパーコンピュータの認証に利用するパスワードは十分に長く他のサービスで利用していないものにすること

パスワードの使い回しはおやめください。具体的なパスワードの要件はパスワード設定画面でご確認ください。

3.4.4. スーパーコンピュータの認証に利用するパスワードの推定を防止すること

平文でのパスワード保存や、付箋等にパスワードを記載して残すことはせず、パスワードを適切に管理してください。また、共同研究者や機構の担当者を含めて他人にパスワードを教えないようにしてください。

3.4.5. スーパーコンピュータの認証に利用するデバイスを他人に貸し出したり自身がログインしようとしている時以外に認証要求を承認しないこと

共同研究者や機構職員、家族等を含む他人に認証に利用しているデバイスを貸し出してはいけません。認証は本人のみが承認してください。

3.4.6. スーパーコンピュータの認証に利用するデバイスを紛失した場合には速やかに情報管理責任者および機構に届け出なければならない

スーパーコンピュータの認証に利用しているデバイス（2024 年 10 月現在では Duo を使った認証に利用しているスマートフォン）を紛失した場合には速やかに情報管理責任者に届け出ると共に機構のゲノムプラットフォーム連携センターにもご連絡くださ

い。アカウント停止の対応を取ります。

3.4.7. スーパーコンピュータにセキュリティ上の問題を見つけた場合には速やかに機構に届け出なければならない

スーパーコンピュータにセキュリティ上の問題を見つけた場合には速やかに機構のゲノムプラットフォーム連携センターに直接ご連絡ください。

3.5. 監査

3.5.1. 利用者はスーパーコンピュータのセキュリティポリシーを確認し、チェックリストを機構に提出すること

本セキュリティポリシーを確認し、チェックリストを記載して機構にご提出ください。提出先はゲノムプラットフォーム連携センターです。

3.5.2. 機構あるいは機構が指定する第三者が不定期に実施する監査に協力しなければならない

機構は不定期に監査を行う場合があります。監査を要求された場合には協力するようにお願いいたします。

3.6. 情報管理責任者の責務

以下の項目は情報管理責任者のみ確認が必要です。

3.6.1. （情報管理責任者のみ）情報管理責任者は、利用者に対して本セキュリティポリシーを周知して遵守させなければならない

情報管理責任者は自身が管理する利用者のすべての行動に責任を取る必要があります。利用者に対して本セキュリティポリシーを遵守させ、情報漏洩等の問題が発生しないようにしてください。定期的にチェックリストに基づいた点検を行ってください。

3.6.2. （情報管理責任者のみ）情報管理責任者は、利用者が変更になった場合には速やかにスーパーコンピュータ利用休止・廃止申請もしくはスーパーコンピュータ利用の変更申請を機構に提出しなければならない

研究計画の変更や人事異動、退職等によって研究体制の変更が生じた場合は、アクセ

ス権限の見直しを行ってください。

4. スーパーコンピュータ以外の計算機のセキュリティポリシー

対象：スタンダードに分類される TMM データを扱うスーパーコンピュータ以外の計算機の利用者

4.1. 情報漏洩の防止

4.1.1. スーパーコンピュータから持ち出したスタンダードに分類される TMM データはデータ保存計算機で扱わなければならない

スタンダードに分類される TMM データはスーパーコンピュータの外に持ち出しが可能ですが、データ保存計算機でのみ扱わなければなりません。これはデータの保存、閲覧、解析、バックアップを含みます。

4.1.2. TMM データの入手時を除いてデータ保存計算機以外にスタンダードに分類される TMM データを保存してはならない

スタンダードに分類される TMM データはデータ保存計算機の中にのみ保存し、可搬媒体に保存してはなりません。運搬のために使用した可搬媒体内の TMM データは、データ保存計算機の中に保存後、速やかに削除してください。また、TMM データの入手後は必要に応じてデータ保存計算機の USB メモリ等の利用禁止設定を行ってください。

4.1.3. TMM データへのアクセスは試料・情報分譲審査委員会または機構長に承認された利用者に限定しなければならない

TMM データを利用できるのは分譲の場合は試料・情報分譲審査委員会で承認された研究者、共同研究・内部利用の場合は機構長に承認された研究者に限ります。同じ組織や研究室の人であっても試料・情報分譲審査委員会または機構長に承認されていない人は閲覧できません。

4.1.4. 明らかな統計情報で情報管理責任者がオープンに分類されると判断したデータについては、利用者間での情報共有や論文発表に利用する目的において、情報管理責任者の許可の元、データの持ち出しおよび印刷を可とする

オープンに分類される TMM データとは、個人の同定につながる可能性がないと考えられる大まかな統計情報です。

4.2. データ保存エリアおよびデータ保存計算機のセキュリティ

4.2.1. データ保存エリアは個人識別が可能な鍵（IC カード等）を用いて入室者を限定および記録しなければならない

データ保存エリアは IC カードや生体認証を利用して個人を識別して入室者を限定する必要があります。IC カードを複数人で共用して、入室者を識別できない仕組みは認められません。また、入室者は自動的に記録されるようにしてください。

4.2.2. 専用のデータ保存エリアが確保できない場合には、利用者のみが開錠可能な常時施錠された専用キャビネット等にデータ保存計算機を格納すること

データ保存計算機専用の部屋にできない場合には、データ保存計算機を専用キャビネット等の常時施錠された場所に保管してください。

4.2.3. データ保存計算機はスタンドアローン計算機でなければならない

スタンダードに分類される TMM データを保存している計算機はいかなるネットワークにも接続してはなりません。パッチ適用時等の一時的な接続も禁止されています。例外を定義するのは困難なため、例外を認めません。もしネットワーク越しにスタンダードに分類される TMM データを利用したい場合には、スーパーコンピュータを利用してください。

4.2.4. データ保存計算機には常に最新のセキュリティパッチを適用すること

データ保存計算機には最新のセキュリティパッチを適用してください。その場合でもデータ保存計算機でインターネットや社内ネットワークへ接続してはなりません。

Microsoft Windows の場合には Microsoft Update Catalog[1]からパッチを取得可能であり、どのパッチをダウンロードすべきか判定する方法はマイクロソフト社のドキュメント[2]が参考となります。Microsoft Windows のセキュリティアップデートは通常毎月第二火曜日の翌日に行われます。

4.2.5. データ保存計算機はアンチウイルスソフトウェアが有効で、常に最新のパターンファイルに更新されていることを確認すること

データ保存計算機にはアンチウイルスソフトウェアをインストールし、最新のパターンファイルに更新されていることを確認してください。その場合でも、データ保存計算機でインターネットや社内ネットワークへ接続してはなりません。Microsoft Defender Antivirus のパターンファイルはマイクロソフト社のウェブページ[3]からダウンロード可能です。

4.2.6. データ保存計算機は一定時間（5 分程度を目安）以上無操作の場合は認証機能により画面がロックされるように設定すること

データ保存計算機は認証機能により画面がロックされるように設定してください。ロックの方法はパスワード、PIN、生体認証、セキュリティキーが利用できます。

4.2.7. データ保存計算機には業務上不要なソフトウェアをインストールしないこと

データ保存計算機には業務上不要なソフトウェアはインストールしないでください。特に P2P 等の技術を用いて不特定多数にファイルを共有するソフトウェアはインストールしないでください。また、自動的に起動するプロセスも精査を行い必要最小限のソフトウェアだけが動作するようにしてください。

4.2.8. データ保存計算機の画面が盗み見されないように対策を行うこと

データ保存計算機の画面が盗み見されないように対策を行ってください。具体的には

---

[1] Microsoft Catalog: https://www.catalog.update.microsoft.com/Home.aspx

[2] Windows Update の判定方法: https://learn.microsoft.com/ja-jp/windows/win32/wua_sdk/using-wua-to-scan-for-updates-offline?tabs=vbscript

[3] Windows Defender のシグニチャ: https://www.microsoft.com/en-us/wdsi/defenderupdates

データ保存計算機に対し覗き見防止フィルタの取り付け、パーティションの設置や第三者による盗み見防止に配慮した設置、監視等、利用者以外からの窃視防止の対策を行ってください。

4.2.9. データ保存計算機はデータ保存エリアから持ち出さないこと

データ保存計算機はデータ保存エリアでのみ利用し、TMM データを利用しない時でもデータ保存エリアから持ち出してはなりません。

4.2.10. データ保存計算機から離れる場合にはログアウトもしくは画面をロックすること

データ保存計算機から離れている間に他人に操作されないように、ログアウトするか画面をロックしてください。

4.2.11. データ保存計算機に可搬媒体等を通じてデータを移動またはコピーする時には、アンチウイルスソフトウェア等によりデータがウイルスに感染していないことを確認すること

データの出し入れをする時にはウイルススキャンを行ってください。

4.2.12. データ保存計算機で利用するパスワードの推定を防止すること

平文でのパスワード保存や、付箋等にパスワードを記載して残すことはせず、パスワードを適切に管理してください。また、共同研究者や機構の担当者を含めて他人にパスワードを教えないようにしてください。

4.3. 情報の破棄

4.3.1. 研究期間終了時または停止時にバックアップデータも含めスタンダードに分類される TMM データをすべて破棄すること

研究期間終了時または停止時にはスタンダードに分類されるすべての TMM データを破棄してください。これにはバックアップデータも含みます。

4.3.2. TMM データを保存したことのある機器の破棄、もしくは再利用のために TMM データを消去する場合、読み出し可能な情報がなく、TMM データが復元不可能であることを確認すること。なお、TMM データの消去は、NSA(米国国家安全保障局)方式、または DoD(米国国防総省)方式に準拠すること。

4.4. 監査

4.4.1. 利用者はスーパーコンピュータ以外の計算機のセキュリティポリシーを確認し、チェックリストを機構に提出すること

本セキュリティポリシーを確認し、チェックリストを記載してください。情報管理責任者は、利用者全員分のチェックリストを取りまとめて、機構（分譲の場合は試料・情報分譲担当）にご提出ください。

4.4.2. 機構あるいは機構が指定する第三者が不定期に実施する監査に協力しなければならない

機構は不定期に監査を行う場合があります。監査を要求された場合には協力するようにお願いいたします。

4.5. 情報管理責任者の責務

以下の項目は情報管理責任者のみ確認が必要です。

4.5.1. （情報管理責任者のみ）情報管理責任者は、利用者に対して本セキュリティポリシーを周知して順守させなければならない

利用者に対して本セキュリティポリシーを遵守させ、情報漏洩等の問題が発生しないようにしてください。定期的にチェックリストに基づいた点検を行ってください。

4.5.2. （情報管理責任者のみ）情報管理責任者は、TMM データに関する情報の台帳を作成し、電子ファイル等で管理すること

以下の情報について台帳を作成して管理してください。

- 研究番号
- TMM データの利用者
- TMM データの保存機器、媒体の所在（データ保存計算機、可搬媒体等）

- TMM データの保存先フォルダ

4.5.3. （情報管理責任者のみ）情報管理責任者は、利用者が変更になった場合には速やかに変更申請を機構に提出しなければならない

研究計画の変更や人事異動、退職等によって研究体制の変更が生じた場合は、アクセス権限の見直しを行ってください。

4.5.4. （情報管理責任者のみ）情報管理責任者は、TMM データを保存した機器または可搬媒体が盗難にあった、もしくは紛失した場合は、速やかに機構に報告すること

盗難、紛失が発生した場合には速やかに情報管理責任者から機構（分譲の場合は試料・情報分譲担当）に報告してください。

4.5.5. （情報管理責任者のみ）情報管理責任者は、データ保存計算機へのアクセスを信頼できる時刻情報と共に記録し、定期的なログの確認を行うこと

データ保存計算機のアクセス記録を作成し、定期的に確認してください。このアクセス記録は利用者のログイン時刻、アクセス時間のログを記録してください。データ保存計算機の時刻が正しいことを確認してください。

4.5.6. （情報管理責任者のみ）情報管理責任者は、研究期間終了時にはバックアップデータも含め TMM データが確実に破棄されたことを確認すること

4.5.7. （情報管理責任者のみ）情報管理責任者は、TMM データを保存したことのある機器の破棄を委託した場合、証明書の受理等により、TMM データの破棄が行われたことを確認すること

4.5.8. （情報管理責任者のみ）情報管理責任者は、TMM データの漏洩の可能性が発生した場合には、速やかに機構（分譲の場合は試料・情報分譲担当）に報告すること

5. データ閲覧エリアのセキュリティポリシー

対象：データ閲覧エリア責任者

データ閲覧エリアを新設する場合は、以下の対策を行い、申し込みと覚書の手続きを行ってください。なお、データ閲覧エリアは要件を満たしていればデータ閲覧端末専用の部屋とする必要はありません。専用の部屋としない場合には、データ閲覧端末の画面がスーパーコンピュータの利用者以外から見えないようにパーティションの設置等の対策を行ってください。

5.1. データ閲覧エリアの施錠方法

データ閲覧エリアは出入り口を常時施錠のうえ、機構が定める要件を満たす入室管理システムで入室制限を行ってください。

5.1.1. データ閲覧エリアは出入り口を常時施錠すること

日中は解放されている等、時間帯によって施錠されない時間帯がある部屋では利用できません。

5.1.2. データ閲覧エリアは生体認証もしくは個人が特定可能な IC カード等で個人ごとに入室が制限されていること

通常の物理的な鍵、等誰が解錠したかわからない鍵の利用は許可されていません。IC カードを使う場合でも複数人で同じ IC カードを共有する場合には利用できません。

5.1.3. データ閲覧エリアは扉が一定時間以上解放された場合、警報音が鳴ること

扉が開けっ放しのまま放置されることがないように、警報音が鳴るようにしてください。

5.1.4. データ閲覧エリアの入室履歴がとれること

5.1.5. データ閲覧エリアの入室履歴は 3 ヵ月以上保存できること

5.1.6. データ閲覧エリアの入室履歴をエクセル形式もしくは CSV 形式でファイルに出力できること

監査の際に提出を求める場合がありますので、入室履歴のデータを書き出せる製品を利用してください。

5.1.7. データ閲覧エリアは入室できる人の情報をエクセル形式もしくは CSV 形式でファイルに出力できること

監査の際に提出を求める場合がありますので、入室できる人の情報のデータを書き出せる製品を利用してください。

5.2. データ閲覧エリアの監視カメラについて

データ閲覧エリアへの経路には機構が定める要件を満たす監視カメラを設置し、入退室状況を記録してください。

5.2.1. データ閲覧エリアの出入り口もしくはデータ閲覧エリアに至る経路上に監視カメラを設置すること

出入り口に監視カメラがなくても出入り口に至る経路に監視カメラがあれば問題ありません。例えばフロア全体が施錠されている時に、フロアの出入り口に監視カメラがあり、データ閲覧エリアの部屋自体には監視カメラがないような場合を想定しています。

5.2.2. 入室時の入室者を監視対象とし、映像から顔および姿（共連れの状況が確認できる範囲）が認識できること

5.2.3. 夜間でも入室者の顔および姿（共連れの状況が確認できる範囲）が認識できること

赤外線カメラである必要はなく、センサーライト等を組み合わせることで撮影できるものでも構いません。もしくは夜間の入室制限を行う方法でも構いません。

5.2.4. 3 ヵ月以上のデータが保存できること

5.2.5. 監視カメラの設置が天井や壁等に固定されていること

置いてあるだけ等、容易に方向が変化する可能性のある設置方法は許容されません。

5.3. データ閲覧端末のセキュリティ

5.3.1. スーパーコンピュータへのアクセスにはデータ閲覧端末を用いること

スーパーコンピュータへのアクセスは機構が提供するデータ閲覧端末であるシンクライアント端末もしくは利用者所有のデータ閲覧端末を用いてください。

5.3.2. データ閲覧端末はデータ閲覧エリアから持ち出さないこと

データ閲覧端末はデータ閲覧エリアに設置し、そこから持ち出さないようにしてください。

5.3.3. データ閲覧端末は盗難および覗き見を防止する対策を行うこと

スーパーコンピュータの利用者以外がデータ閲覧端末を覗き見できないような対策を行ってください。例えばパーティションの設置やデータ閲覧エリアの窓から見えない方向にディスプレイを向ける等の対策を想定しています。

5.3.4. （利用者所有のデータ閲覧端末を利用する場合のみ）利用者所有のデータ閲覧端末の情報を機構に届け出ること

利用者所有のデータ閲覧端末を利用する場合にはライセンス発行が必要です。この過程で利用者所有のデータ閲覧端末の情報を機構に提出する仕組みになっていますので、機構の指示に従ってライセンス発行依頼を行ってください。

5.3.5. （利用者所有のデータ閲覧端末を利用する場合のみ）利用者所有のデータ閲覧端末は機構が指定するシステム要件を満たし、機構が提供するクライアントソフトウェアがインストールされていること

利用者所有のデータ閲覧端末を利用する場合には機構が提供するクライアントソフトウェアをインストールし、そのソフトウェアを使って接続してください。

5.4. ネットワークについて

5.4.1. （機構が提供するデータ閲覧端末を利用する場合のみ）スーパーコンピュータに接続するネットワークは機構が指定する Virtual Private Network を利用すること

NTT のフレッツ・VPN プライオもしくは SINET の L2VPN が利用可能です。なお、利用終了時には利用者の責任において VPN の契約を解除してください。

5.5. データ閲覧エリア責任者について

5.5.1. データ閲覧エリアにはデータ閲覧エリアの構築および管理を適切に行うため、データ閲覧エリア責任者を置くこと

研究責任者や情報管理責任者が兼任しても問題ありません。データ閲覧エリアの責任者をデータ閲覧エリアごとに定めてください。データ閲覧エリア責任者と情報管理責任者が異なっていても問題ありません。

5.5.2. データ閲覧エリア責任者はデータ閲覧端末やデータ閲覧エリアの利用の変更もしくは終了を行う場合には速やかに機構に届け出ること

変更や終了がある場合にはゲノムプラットフォーム連携センターに届け出てください。

5.5.3. データ閲覧エリア責任者は利用者に機構の定めるセキュリティポリシーや各種規則および関連する法令等を遵守するように指導すること

スーパーコンピュータのセキュリティポリシー等、機構が定めるセキュリティポリシーを遵守させてください。

5.5.4. データ閲覧エリア責任者は利用者に所属する組織のセキュリティ講習会を受講させること

所属組織が行うセキュリティ講習会を受講させてください。

5.5.5. データ閲覧エリア責任者は利用者に機構が提供するスーパーコンピュータ利用者講習会を受講し、内容を理解していることを確認すること

機構が行うスーパーコンピュータ利用者講習会を毎年受講させてください。

5.5.6. データ閲覧エリア責任者は利用者の人事異動や退職等に応じて、入室権限の見直しを行うこと

データ閲覧エリアの利用者について、人事異動や退職等の変更が生じた場合は、入室権限の見直しを行ってください。

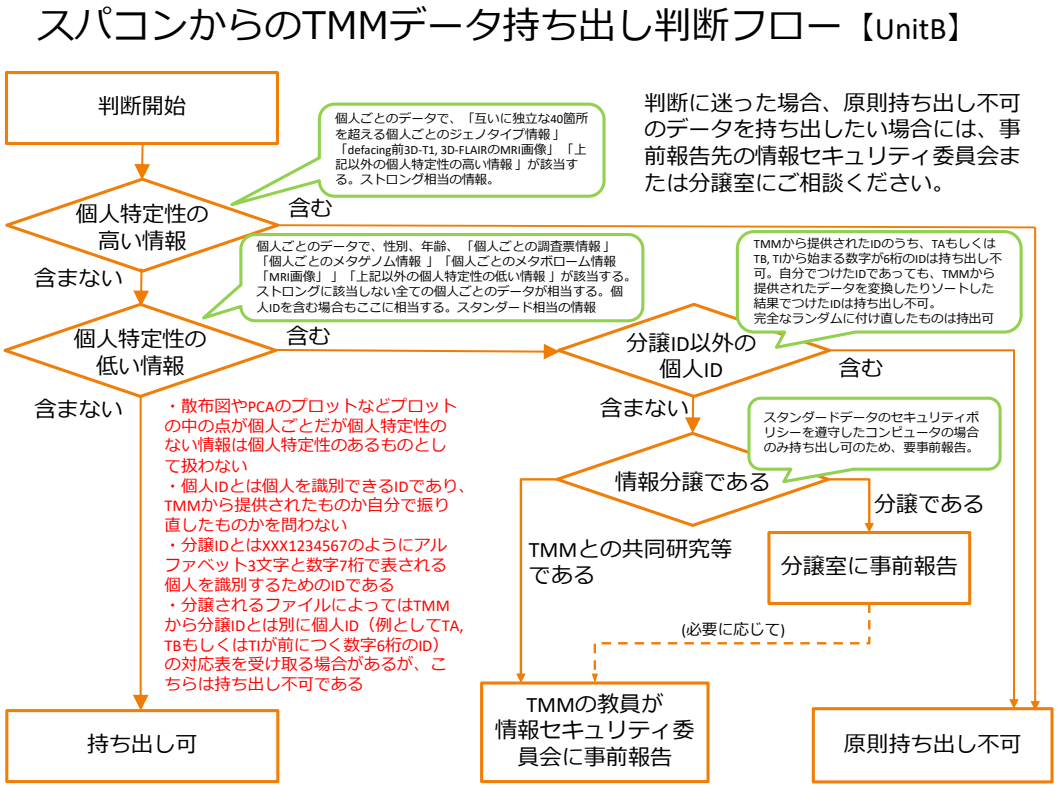
5.6. 監査

5.6.1. データ閲覧エリア責任者は機構もしくは機構が指定する第三者が不定期に実施する監査に協力しなくてはならない

6. スーパーコンピュータからのデータ持ち出し判断フロー

6.1. Unit B

Ver.2023/8/25



6.2. Unit C

Ver.2023/8/25