mdx のセキュリティホワイトペーパー

2023 年 1 月

データ活用社会創成プラットフォーム協働事業体

更新履歴

版	更新年月	履歴
1	2023年 1月25日	初版発行

目次

1. 本書の目的

本書は mdx の利用者が要求するセキュリティ要件を mdx が満たしているかどうかを確認するための参考資料として作成しています。
本書は以下の事項について解説しています。

- mdx のセキュリティ管理体制
- mdx のセキュリティ実装
- mdx 利用者が利用できるセキュリティ機能
- mdx 利用者と共同研究基盤のセキュリティ上の役割・責任の分担

2. 本書の想定読者

本書は、mdx の利用を検討中の方、mdx を利用中の方を読者として想定しています。

3. mdx の概要

mdx はデータ活用社会創成プラットフォーム協働事業体（以下、協働事業体）の構成機関が構築・運用するデータ収集・集積・解析機能を提供するプラットフォームです。この協働事業体は東京大学情報基盤センターが統括し、事務局を担当します。

mdx は仮想化技術を利用し、複数の利用者が物理サーバやストレージ、ネットワークなどの物理的な同一資源を利用します。利用者に提供する環境は論理的もしくは物理的に分割され、利用者が構築するテナントやデータには他の利用者からアクセスすることはできません。

mdx を利用するにあたっての基本的な用語、システム概要、利用方法等について本章で説明します。

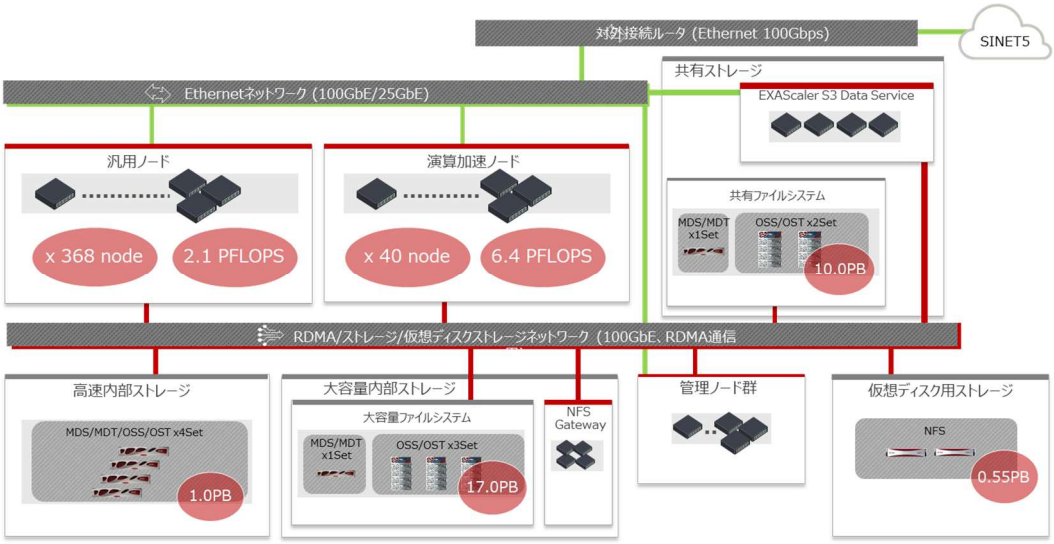
3.1. 用語の説明

- 協働事業体
  - 協働事業体とは、mdx を運営する機関のことで 9 大学、2 研究所で構成される
  - 東京大学情報基盤センターが統括し、事務局を担当する
  - mdx の利用申請するプロジェクトの審査・承認等を行う
- 資源提供者
  - mdx を設置する施設、mdx のハードウェア、ソフトウェアの資源を管理する者の総称
  - mdx 管理者、機関管理者、mdx の納入・保守を担当する者
- プロジェクト
  - 利用者が mdx を利用する際の単位
- 物理サーバ、仮想基盤
  - 仮想化システムが動作するサーバ群を仮想基盤という。物理サーバとして、汎用ノード、演算加速ノード、複数のストレージシステム、ネットワーク機器で構成される

- mdx を構成する物理サーバの詳細は、システム構成図を参照のこと
- テナント
  - プロジェクトに割り当てられた計算資源用いて構築された仮想化された計算環境
- 仮想マシン
  - 物理サーバ上で動作する仮想化された計算機
- 利用者
  - プロジェクトに割り当てられた資源を利用する全ての者。プロジェクト代表者、プロジェクトユーザ、テナント管理者、テナント利用者
- プロジェクト代表者
  - プロジェクトの利用申請、利用料金の支払い等を行うプロジェクトの代表者
  - プロジェクトに 1 名登録される。また、プロジェクト代表者はプロジェクトユーザとして自動で登録される
- プロジェクトユーザ、プロジェクト管理者
  - ユーザポータルを利用してテナントの構築、管理等を行うことができる者
  - ユーザポータルを用いて複数名のプロジェクトユーザを登録することができる
- テナント管理者
  - プロジェクト代表者またはプロジェクトユーザが構築したテナントで動作する OS の管理者（root 権限等の管理権限を持つ者）
- テナント利用者
  - プロジェクト代表者またはプロジェクトユーザが構築したテナントを利用する者
  - テナント中に構築されたサービス（データ提供サービスや解析環境など）を利用する者
- mdx 管理者
  - mdx 全体の管理者
  - mdx の資源配分やシステム管理等を行うことができる
- 機関管理者
  - 協働事業体の管理者
  - 協働事業体に申請されたプロジェクトの承認等を行うことができる
- プロジェクト申請ポータル
  - プロジェクト代表者がプロジェクトの申請を行うポータルサイト
- ユーザポータル
  - プロジェクト代表者またはプロジェクトユーザがプロジェクト管理等を行うポータルサイト
    - テナントの構築、起動、停止
    - プロジェクトで利用する資源量の追加、変更
    - プロジェクトの終了

3.2. システム構成

- システム構成図



4. mdx におけるセキュリティ方針

協働事業体は以下の通り、総合的・体系的な情報セキュリティ対策に継続的に取り組みます。

- mdx は、取り扱う情報を重要な資産と認識し、情報セキュリティの確保に努める。
- mdx は、セキュリティの確保のために必要な情報セキュリティ体制を確立する。
- mdxは、サイバー脅威から資産を保護するために、包括的な対策を実施する。
- mdxは、セキュリティの維持・向上のために、定期的に点検・評価・監査を実施する。
- mdxは、セキュリティについての教育・研修を定期的に実施する。

上記方針および協働事業体の統括を行う東京大学情報基盤センターにおける東京大学情報セキュリティ・ポリシーに従い、mdx において提供されるサービスのセキュリティを確保する方法や体制を確立しました。

5. 想定されるリスク

5.1. 保護すべき情報が漏洩するリスク

mdx 管理者は以下のリスク要因を認識し、その対応を行います。

- 利用者の用いるネットワークの隔離に失敗する
- mdx ローカルアカウントの情報が不正にアクセスされ、悪用される
- 可搬媒体にデータを格納して輸送する際に盗難にあい、情報漏えいする
- 可搬媒体の利用終了時にデータを削除せず、情報漏えいする

また、mdx の利用に関して以下のリスク要因を認識し、その対応を行います。

- mdx 利用者の認証設定に不備があり、攻撃者の不正アクセスにより、漏洩が発生する
- mdx 利用者のテナントに脆弱性があり、攻撃者の不正アクセスにより、漏洩が発生する

- mdx 利用者がデータ転送を行う際に暗号化を怠ったため、データ転送途上における情報漏洩が発生する

本リスクへの対応は、物理的セキュリティ、ネットワークセキュリティ、アクセス制限、モニタリング、技術的脆弱性管理等により行っています。

5.2. 情報および処理が改ざんされるリスク

mdx 管理者は以下のリスク要因を認識し、その対応を行います。

- 管理者の誤った操作により、意図しないデータの書き換えが発生する
- 可搬媒体に格納されたデータが改竄される

また mdx の利用に関して以下のリスク要因を認識し、その対応を行います。

- mdx 利用者の認証設定に不備があり、攻撃者の不正アクセスにより、改ざんが発生する
- mdx 利用者のテナントに脆弱性があり、攻撃者の不正アクセスにより、改ざんが発生する

本リスクへの対応は、物理的セキュリティ、ネットワークセキュリティ、アクセス制限、モニタリング、技術的脆弱性管理等により行っています。

5.3. サービス提供ができなくなるリスク

mdx 管理者は以下のリスク要因を認識し、その対応を行います。

- mdx 利用者の増加や利用方法の変更等により計算機資源、ネットワーク資源の需要が供給を大きく超えたため、システムが機能不全となる
- mdx 管理者が運用・提供する基盤的サービスに障害が発生し、サービスが不全となる
- mdx のシステムに対する DoS/DDoS 攻撃により、サービス提供のための計算機資源、ネットワーク資源が枯渇する

また mdx の利用に関して以下のリスク要因を認識し、その対応を行います。

- プログラムの意図しない動作や不正アクセスにより計算機資源、ネットワーク資源が枯渇する
- 他の mdx 利用者が用いているテナントの資源が枯渇した影響を受けて、同一のハイパーバイザー上で動作しているテナントに影響が発生する

本リスクへの対応は、物理的セキュリティ、ネットワークセキュリティ、アクセス制限、モニタリング、容量・パフォーマンス管理、事業継続(BCP)等により行っています。

5.4. クラウドサービス固有の情報セキュリティ管理策

mdx では以下のクラウドサービス固有の情報セキュリティ管理を行います。

- mdx 管理者は、mdx 利用者と mdx（協働事業体）の責任の分担を明示し、運用の役割分担の明確化を行い、合意された責任の範囲に基づいた統制を mdx 利用者が行えるようにします
- mdxは、mdx 利用者がクラウドサービスの情報セキュリティマネジメントを実践するに当たり、mdx が必要情報をクラウド利用者に提供できる実務を確保します

- mdxは、mdxとmdx 利用者のコンプライアンス違反を予防するべく、業法等による要求事項等を確保できるようにするための支援、海外における適用法の違いによって預託された情報に生じるリスクを緩和するための実務、司法の捜査等に対応する実務を行います
- mdxは、mdx利用者とコミュニケーションを行い、mdx利用者との合意の上で必要に応じて情報を公開・開示するよう務めます
- mdxは、mdx利用者が認証取得・インシデント対応、監査等を行う際の情報資産・証跡の特定や、テナントを分離するための支援を行います

この上で、mdx では以下のリスク要因を認識し、その対応を行います。

- mdx と利用者の間の責任分界点が不明瞭となってしまい、不十分なインシデント対応が行われる
- mdx と利用者のコミュニケーション不足により、運用措置の理解に齟齬が生じ、BCPが機能しなくなる
- mdx 利用者が認証取得、インシデント対応、監査などにあたって資産・証跡を特定する際に、mdx がこの特定・分離を行う機能が不十分となる（例：他のテナントの情報と分離できない）

本リスクへの対応は、クラウドサービス利用に関するリスク等により明示しています。mdxは、マルチテナントによるクラウドサービスを提供しているため、他の利用者の影響を受ける可能性があります。mdxは適切に監視を行い、異常への対応を行う仕組みや体制を整えていますが、マルチテナントに起因するリスクを完全に回避することは困難です。利用者はこのことを理解した上で mdx を適切に利用する必要があります。

5.5. ガバナンスとリスク管理

情報セキュリティ体制として mdx-CSIRT を設立します。mdx-CSIRT は mdx におけるセキュリティの確保やインシデント対応を行うために設置された組織です。データ活用社会創成プラットフォーム協働事業体のサービス提供者・利用者・テナント利用者と連携し、個々のセキュリティ上の問題の解決に取り組みます。また、mdx-CSIRTはmdx 及び mdx 利用者の情報セキュリティの確保を行い、インシデントの情報を収集、分析し、必要に応じて利用者・テナント利用者と必要に応じて共有し、インシデントの予防・対応を行います。さらに、情報セキュリティに関する教育を定期的に行うことにより、セキュリティ向上につとめます

6. 責任共有モデル

mdx サービスの情報セキュリティを高めるためには、資源提供者と利用者が協力して取り組む必要があります（mdx サービスに対する責任を共有する必要があります)。資源提供者は以下の図にある通り、mdx で提供する設備、ハードウェア、テナントを構築するに必要なソフトウェア（ハイバーバイザー）に関する部分を、利用者は資源提供者が提供する資源を元に構築したテナントで動作する OS 部分（バージョンアップ、セキュリティパッチの適用等)、ユーザ管理、資源提供者が提供するアクセス制御機能によるアクセス制限、アプリケーションソフトウエア、利用者データ等の部分について責任及び管理を行い、セキュリティ対策を実施します。

- 資源提供者（協働事業体）
  - 物理的な機器（サーバ、ネットワーク、ストレージ等）やテナントを構築するためのハイパーバイザー、mdx を利用するために必要な申請や設定を行うためのポータルサイトについては協働事業体側がセキュリティ対策を行います。
  - こちらが提供するOSのイメージについて（TBD）
  - 協働事業体が提供するシステム（サービス）を用いて構築するテナントの設定作業
- 利用者
  - 構築したテナントで動作している OS を含めた全てのソフトウェアの管理、セキュリティ対策を利用者が行います。具体的には、OS、アプリケーション等に関するセキュリティパッチ、バージョンアップ作業、適切な設定等を実施する。また、利用するユーザの管理やストレージに保存されたデータ管理、ネットワークを使った外部からのアクセス制御、アプリケーションのライセンス管理や利用許可等を行います。また、データ管理・アクセス制限なども適切に設定を行う必要があります。なお、mdxが提供するOSのイメージは、協働事業体が善意に基づいたベストエフォートによって提供されます。最終的な安全性の確認や利用は利用者の責任とします。
  - 上記の通り、資源提供者で提供する資源で作成したテナント環境（OS を含むソフトウェア）については、基本的に利用者の責任のもとで運用いただくこととなり、資源提供者では管理できません。そのため、OS の設定やセキュリティ対策、利用者・データの管理、アプリケーションのインストールなどは利用者による対応が必要です。(資源提供者は、一般的な回答や可能な範囲でのサポートは行います)。

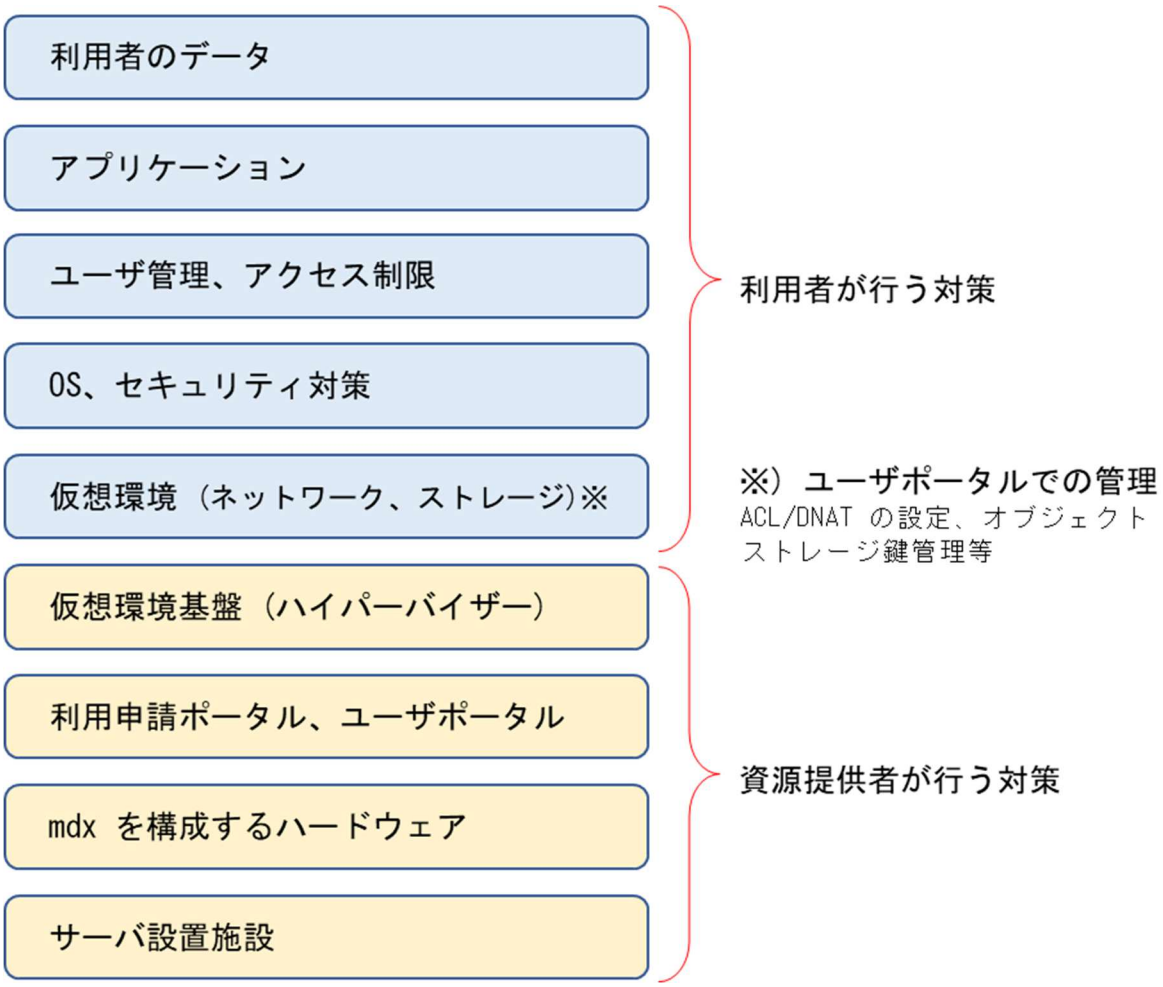


図 mdx における責任共有モデル

7. 情報セキュリティ対策

mdx は情報セキュリティに取り組む体制を以下の通りに保持します。

- mdx セキュリティ責任者は、mdxに係る全ての情報セキュリティ対策に関する業務を統括し、並びにmdxに係る情報システムの管理を監督します
- mdx セキュリティ責任者は、インシデント発生の際にインシデント管理者、mdx参画機関のインシデント担当者、mdxの利用者及びmdx保守事業者と連携し、問題の対応にあたります
- mdx の CSIRT は、mdx セキュリティ責任者のほか、インシデント管理者、インシデント窓口（PoC)及びメンバーをもって組織されます。mdxセキュリティ責任者は、情報セキュリティに関する専門的な知識または適正を有すると認められる教職員等のうちからインシデント管理者、インシデント窓口及びメンバーを指名します
- mdx-CSIRT は mdx に係る情報セキュリティに関する状況を管理・把握し、mdx運営委員会に定期的に報告します

- mdx-CSIRT は、協働事業体を統括する東京大学情報基盤センターのセキュリティ機関とセキュリティインシデントに対処するために連携し、情報セキュリティの確保、情報サービスの復旧その他の必要な情報交換を行います

8. mdx のセキュリティ解説

8.1. 物理セキュリティ

8.1.1. セキュリティの目的

mdx が提供するハードウェア、利用者が格納するデータ等を物理的破壊、持ち去り、覗き込み等の物理的脅威、電源障害等の環境的脅威から保護します

8.1.2. 実装と運用

- mdx は東京大学柏 II キャンパス内に設置されています
- mdx の設置されているサーバ室出入口は常時施錠します
- サーバ室内のラック扉は常時施錠し、メンテナンス等の必要な場合にのみ解錠し作業します

8.2. ネットワークセキュリティ

8.2.1. セキュリティの目的

利用者等のデータ等は、インターネットを含め利用者等が直接管理できない伝送路で運ばれます。mdx の設備から利用者内設備を結ぶネットワークの経路制御および盗聴、伝送遅延等への対応を行い、伝送路の信頼性と安全性を確保します。

8.2.2. 実装と運用

① mdx は、日本全国の大学、研究機関等の学術情報基盤として国立情報学研究所が構築、運用している情報通信ネットワークである SINET を通じてインターネットに接続されています

② 通信回線はファイアウォールによる防御を実施しています。ファイアウォールで不要な通信を遮断することで、外部からの攻撃や内部からの情報流出を防止します。また、インターネットからアクセスされる機器については、OS が持つファイアウォール機能も用いて不正通信を防御します

③ 外部からの侵入・攻撃への対策（防御、検知）として、改竄検知および不正アクセスに関するログの記録を行っています。侵入発覚後に改竄記録や不正アクセス記録を確認・解析することが可能です

④ mdx 利用者はテナントの OS の機能、ポータルサイトから提供される機能としてネットワークアクセス制御を設定することが可能です

⑤ mdx 管理者は定期的にテナントに対して脆弱性の診断を行い、危険なセキュリティ診断結果の通知を行います

8.3. アクセス制御

8.3.1. セキュリティの目的

mdx サービスへのアクセス制御および mdx サービス上の利用者環境、利用者データへの未許可アクセスおよび誤用、悪用から保護するための、本人認証をベースにしたアクセス制御を行います。

8.3.2. 権限と特権アカウントの管理

① mdx のシステム管理者権限等の特権は、役割に応じた（mdx 管理者、機関管理者）最小限の権限の付与、最少人数への付与を原則に割り当てます

② mdx 管理者は定期的に mdx システム管理者（機関管理者）権限を付与された特権アカウントについて確認を実施します

8.3.3. 利用者のアクセス管理

① 利用者の登録及び登録削除

② 一意アカウントの徹底

8.3.4. 利用者等によるデータアクセスおよび保護

① プロジェクトで保存されているデータは、他の利用プロジェクトからは論理的に分離し、アクセスできないようにしていますが、利用者がインストールしたプログラムや利用者のデータに対するアクセス制限は、利用者等が行う権限設定に依存します

② 利用者が作成したテナント（仮想マシン）に登録するアカウント等についてはプロジェクト代表者が責任をもって管理する必要があります

③ mdx 管理者は、次の場合を除き、利用者等のデータ等の閲覧、参照を行わず、第三者に開示しません

- mdx サービスの提供・維持のために第三者に業務委託を行う場合であって、かつ運用上必要な場合。ただし、mdxは、業務委託先の第三者に対し、mdxと同等レベルの利用者等のデータ等の取扱いを遵守させるものとします
- 裁判所または行政機関より法令、判決、決定または命令に基づき開示が要求され、これに応じる場合

8.4. モニタリング

8.4.1. セキュリティの目的

① システム障害やセキュリティインシデントの検知、記録、原因究明ならびに運用の正当性の裏付けとして各種ログを取得し、各種監視機能によりモニタリングを行います

② ただし、利用者が作成したテナント（仮想マシン）のログは利用者自身で取得・保管することになります

8.4.2. 実装と運用

① mdx 管理者が、システム障害、セキュリティインシデントの関知、原因究明に用いるために以下のログを取得します

- テナントから外部等への通信記録
- ユーザポータル等へのログイン、アクセス履歴
- ネットワークトラフィック情報（ネットワークスイッチの IF-MIB で取得可能な情報）
- その他、物理的な機器（サーバ、ネットワーク、ストレージ等）のエラーログや稼動状況を把握するためのログ等

② ログの保存期間は最低1年間とします

③ ログは mdx システムの性能管理・セキュリティ管理の目的で取得するもので、利用者等の個別要求に応じてログを開示することは原則としていたしません

8.5. バックアップ

8.5.1. セキュリティの目的

システム障害やインシデントによる mdx サービスが利用できなくなる、あるいはデータが消失したといった状況が発生することを想定し、事業の継続および速やかな復旧のためにバックアップを取得します。

8.5.2. 実装と運用

① mdx 管理者がシステム障害時の復旧やサービス継続のために不可欠なデータのバックアップを定期的に実施します

② バックアップは mdx システムの障害時等における復旧のために行うものであり、利用者データの復旧等は対象となりません（利用者が作成したテナント（仮想マシン）やストレージに保存されているデータは利用者自身がバックアップを取得してください）

8.6. 技術的脆弱性管理

8.6.1. セキュリティの目的

システムには何らかの脆弱性が存在します。システムの脆弱性を放置しておくと攻撃者に利用され、設定の変更、情報の漏洩、改ざん、削除、遠隔操作等の被害を受ける可能性があります。脆弱性がリスクの顕在化の原因とならないようにするために適切に脆弱性管理を行います。

8.6.2. 実装と運用

① 責任分界点に記載した通り、物理的な機器（サーバ、ネットワーク、ストレージ等）やテナントを構築するためのハイパーバイザー、mdx 管理者がインストールしたシステムソフトウェア等についての脆弱性対策については mdx 管理者が対応します

② mdx 管理者は JPCERT/CC などから脆弱性情報を収集し、mdx システムへの影響を評価します

③ 収集した脆弱性については、脆弱性のレベルに応じてアップデートやパッチ適用の可否および適用スケジュールを検討します。緊急性の高い脆弱性が発見された場合は、利用者に通知をした上でシステム停止を伴うアップデート、パッチ適用を実施する事があります

8.7. 容量・パフォーマンス管理

8.7.1. セキュリティの目的

mdx のサービスではシステム資源（CPU、GPU、ストレージ容量等）を利用者が自由に増減することができることが利点の一つになっています。利用料金も考慮しながら可用性を維持するために、適宜必要な容量やパフォーマンスを監視する必要があります

8.7.2. 実装と運用

mdx はマルチテナントによるクラウドサービスのため、他の利用者の利用状況によりネットワーク帯域等の性能が影響を受ける可能性があります

8.8. システム障害、インシデント対応

8.8.1. セキュリティの目的

mdx が提供するハードウェア環境、ソフトウェア環境、利用者が作成したシステムが複合的に連携した mdx サービスでは、システム障害やインシデントの原因について切り分けが難しく、また、責任分界や障害対応の役割が曖昧であると速やかな対応が取れません。障害の検知、原因究明、復旧のための関係者の協力体制、対応手順を整備します

8.8.2. 実装と運用

① mdx 管理者は、情報セキュリティインシデントや重大なシステム障害の可能性を認視した場合には、直ちに mdx-CSIRT の全体管理者に報告し、その指示に従うこと

② mdx 管理者は、重大なシステム障害が確認できた場合は Web 等で情報を周知するとともに、mdx の保守を行うベンダ等と連携して復旧作業を進めます。復旧の目途などは適宜 Web 等で情報を周知します

③ mdx-CSIRT のセキュリティ管理者は、報告を受けた場合には、速やかに必要な指示を行うとともに、mdx-CSIRT、その他関係者にその旨を報告します。また、必要に応じて利用者等に情報を通知します

8.9. 事業継続（BCP）

8.9.1. セキュリティの目的

mdx の可用性が失われた場合の利用者業務に及ぼす影響を考慮して、事業継続計画を準備し計画に従い実施します

8.9.2. 実装と運用

① 次の各号に該当する場合は、mdx のサービス提供を中止できる者としています（利用規則　第２６条）

(1) 事故、災害等の発生または発生するおそれがある場合等、不可抗力により本サービスの継続が困難となった場合

(2) 東京大学柏Ⅱキャンパス情報基盤センター・国立情報学研究所柏分館内の設備や国立情報学研究所の学術情報ネットワークSINETが、停電、保守、障害、工事、コンプライアンス対応により停止、又は停止するおそれがある場合

(3) 不正利用、不正行為、ハッキング等に対する緊急対応が必要である場合

(4) 天災その他の非常事態が発生し、又はそのおそれがあるため、運営機関によるmdxの運用を優先させる必要がある場合

(5) その他、本サービスを安定的かつ効率的に運用するために必要がある場合

② mdx 管理者は、mdx のサービス提供に支障が出ると判断した場合には、プロジェクト代表者に予告したうえでテナント（仮想マシン）の停止等を行うことがあります。また、緊急の場合はプロジェクト代表者に対して予告することなくテナント（仮想マシン）の停止等を行うことがあります

8.10. クラウドサービス利用に関するリスク

8.10.1. セキュリティの目的

mdx では共有化された計算資源を利用者の要求に応じて適宜適切に配分し、ネットワークを通じて提供するサービスです。計算資源を他の利用者と共有する、テナントにおけるリスクについて明らかにします

8.10.2. 実装と運用

① 仮想化環境において、CPU やメモリなどの利用について物理的な実行環境とは異なる管理が行われることになります。そのため、処理速度の低下や計算資源の消費が多く見られる場合があります

② 利用者がインストールするソフトウェアが計算環境（テナント）を前提に作成されていないライセンスとなっている場合があります。ソフトウェアのライセンス体系によっては、計算環境での利用で権利関係の問題となる可能性があります（ライセンス違反となる可能性）。利用者は利用するソフトウェアについて mdx が提供する計算環境で利用可能なライセンス体系であり、また利用者がライセンス違反とならないように確認する必要があります

③ mdx では一つのハードウェア上に複数の利用者（テナント）が利用することになります。外部からハードウェアを狙った攻撃が行われた場合、直接的な攻撃対象ではなくとも他のテナントにも影響が及ぶ可能性があります

8.11. クラウドサービス利用終了・解約時の利用者データの扱い

8.11.1. セキュリティの目的

mdx サービス利用終了の条件、解約の手続き、およびデータ移行、残留データの消去といった確認事項を明らかにします。

8.11.2. 実装と運用

① mdx サービス利用（利用契約）が終了した場合、mdx 管理者は終了後 90 日間が経過した時点で、規則されている利用者等のデータ等を含む利用者当に関わる一切のデータ（ただし、利用者等の登録情報や利用者等に関係するログデータ等は除きます）を論理削除します

② ストレージ内にある記憶装置について、ディスクの初期化や物理的な破壊は行いません

8.12. 法令、契約上の責任

8.12.1. セキュリティの目的

mdx のサービスを利用する利用者のデータは、mdx が設置されている所在地のデータ保護法令、個人情報保護法令等の影響も受けます。また、法執行機関による捜査の過程で利用者の所属する機関等の情報が提供されることも考えられます

8.12.2. 実装と運用

① mdx 利用規約等は日本法に準拠し、日本法に従って解釈されるものとします

② 協働事業体は、本サービスの利用契約の履行に際し知り得た相手方に関する業務上、営業上、学問上、運営上の一切の情報（口頭によるか、文書によるか、電磁的手段によるかを問わず、公知情報、従前から適法に保持していた情報及び第三者から秘密保持義務を負うことなく入手した情報を除く。以下

「秘密情報」という。）を正当な理由なく第三者に開示、漏洩しないものとします。なお、利用者が、法令に基づく開示請求を受けた際には、事前に相手方（相手方がプロジェクト主体又はプロジェクトユーザの場合にはプロジェクト代表者）に通知した上で、秘密情報を開示できるものとします

③ mdx サービスの利用により得られた知的財産権は、当該プロジェクトの利用者に帰属するものとする

9. 支援体制

9.1. 利用申請受付

受付メールアドレス : mdx-help [at] mdx.jp

対応する項目（時間帯は平日 9:00 ～ 17:00）

- mdx 利用申請の受付、対応
- mdx 利用料金に関する問い合わせ、対応

9.2. 情報セキュリティに関する問い合わせ、報告

受付メールアドレス: mdx-csirt [at] mdx.jp

対応する項目（時間帯は平日 9:00 ～ 17:00）

- 情報セキュリティインシデントの疑いが認知された場合の報告
- mdx のセキュリティに関する問い合わせ

情報セキュリティインシデントの疑いが認知された場合には、別途定める様式に従って、受付メールアドレスに至急報告してください

9.3. 運用サポート

受付メールアドレス: mdx-help [at] mdx.jp

対応する項目（時間帯は平日 9:00 ～ 17:00）

- mdx が提供するポータルの利用方法
- 一般的な仮想マシンテンプレートの利用方法
- 不具合対応
- ハードウェア障害、ネットワーク障害

質問する際には、不具合の詳細や再現性の有無（再現環境のご提供）等の詳細を記載した受付メールアドレスまでご連絡ください。

- 連携機関名
- プロジェクト名、プロジェクトUUID
- 問い合わせ内容の詳細（以下のような内容について詳細をお知らせください）
  - 不具合の詳細や再現性の有無。また、再現環境の提供および再現方法等
  - ストレージの障害・不具合が疑われる場合には、どのストレージで障害が発生しているか、また、どの様な現象（不具合）が確認されているか等
  - ネットワークの障害・不具合が疑われる場合には、どの様な通信不具合が起こっているか。ACL の設定、通信ログ等に出力されているログ等の情報

10. 本書に関するお問い合わせ窓口

mdx-help [at] mdx.jp

11. 参考文献

- ABCI のセキュリティ ホワイトペーパー
- データ活用社会創成プラットフォーム基盤システム利用規約
- 日本コンピュータセキュリティインシデント対応チーム協議会　CSIRT人材の定義と確保

以上