MEDIDATA

ホワイトペーパー

情報セキュリティ

目次

主な要約

Medidataは、効果的な情報セキュリティおよびサイバー防御プログラムは、製品とその関連データの設計、開発、生産、配布、展開、保守、廃棄を含む製品ライフサイクル全体に対応する必要があると認識しています。

Medidataは、製品がMedidataの使用説明書に従って使用されている場合に限り、すべてのMedidata製品に関するセキュリティインシデントおよびプライバシー侵害から保護するために、管理的、技術的、物理的な安全対策を実施しています。しかし、システムや脅威が進化するにつれ、すべての脅威や脆弱性からシステムを守ることはできません。将来を見据えた戦略と継続的な評価は、健全な防衛プログラムの重要な要素です。当社のお客様は重要な存在であり、当社はお客様とパートナーシップを結び、当社が管理するすべてのデータとサービスのセキュリティとプライバシーの安全対策を保持しています。

何かご心配な点がございましたら、当社までお知らせください。適切な場合には、製品の変更、技術的なお知らせ、顧客や規制当局への責任ある開示によって問題に対処します。Medidataは、製品ライフサイクル全体を通じて、次のような手法でセキュリティとプライバシーの向上に継続的に努めています：デザインによるセキュリティとプライバシー、製品とサプライヤのリスク評価、脆弱性とパッチの管理、自動脆弱性スキャン、外部サードパーティのテスト、お客様のアクセスとデータに適したアクセス制御、インシデント対応などです。

「情報セキュリティは、患者さんのプライバシー、場合によっては患者さんの生命を守るために極めて重要です。私が臨床試験患者となったとき、医療データの保護は個人的なものとなりました。治験患者として、またサイバー脅威を理解するセキュリティの専門家として、Medidata は私の情報を保管・処理する唯一の企業であると断言できます。」

– Glenn Watt、Medidata、最高情報セキュリティ責任者（2007年～2018年）

Medidataはお客様を第一に考えており、製品やサービスに関するご質問、ご不明な点、改善点などございましたら、お気軽にお問い合わせください。

ご質問やご不明な点がございましたら、Medidata.asksecurity@3ds.comまでお気軽に連絡ください。

目的

本文書の目的は、Medidata のセキュリティおよびプライバシーに関する慣行が Medidata Clinical Cloud（MCC）にどのように適用されているかについて、公的に入手可能な情報を検討することです。本書には、Medidataが製品の各セキュリティ領域をどのように保持しているか、また、製品のライフサイクル全体を通してセキュリティを確保するために、どのようにあなたとパートナーシップを組むことができるかについての説明が記載されています。

Medidataのセキュリティに関する一般的な議論と回答を提供する一方で、機密または専有的なセキュリティ製品名、構成、操作手順を漏らすことはありません。これらの慣行や技術は、予告なく更新される可能性があり、文書の更新が行われる可能性があるため、本書のいかなる部分も契約上の義務を満たすものとみなされるべきではありません。

より詳細で機密性の高いご質問については、Medidata の担当者/セールスエンジニア/プロフェッ ショナルサービス/アカウントエグゼクティブにお問い合わせください。

Medidata セキュリティ文化

組織の全員が共有する価値観が、セキュリティに対する考え方や取り組み方を決定します。強固なセキュリティ文化を持つことで、セキュリティ意識の高い従業員が育ち、従業員に求められる望ましいセキュリティ行動が促進されます。これは「ヒューマン ファイアウォール」と呼ばれています。従業員は、Medidataもパートナーも、何が普通でないのか、何が疑わしいのかを「知っている」のです。個人の経験や観察は自動化できません。それが、私たちが購入し、配備するツールの限界です。

Medidataは、「デザインによるセキュリティ（Security by Design）」という考え方で製品を開発しています。オープン ワールドワイド アプリケーション セキュリティ プロジェクト（Open Worldwide Application Security Project、OWASP）のソフトウェア開発原則は、当社のソフトウェア開発ライフサイクル（Software Development Life Cycle、SDLC）およびエンタープライズ テクノロジー アーキテクチャの設計と修正のためのコア戦略を定めています。

OWASPのセキュリティ設計原則は以下の通りです：

- **攻撃対象領域の最小化** – ユーザーが利用できる機能を必要なものだけに絞り込みます。
- **セキュアなデフォルトの確立** – ユーザーとそのアクセスを管理する強力なセキュリティルール。
- **最小特権の原則** – ユーザーは、特定のタスクを実行するために必要な最小限の特権を持つべきです。
- **徹底的な防御** – 製品には、多層的な検証、追加のセキュリティ監査ツール、ロギングが必要です。
- **安全なフェイルセーフ** – 機能不全に陥ったプログラムは、デフォルトでアクセスを減らすか、またはアクセスしないようにする必要があります。
- **サービスを信用しない** – プログラム内で利用されるサードパーティのソフトウェアやサービスには、より高いレベルの権限を与えるべきではなく、データストリームを検証する必要があります。
- **職務の分離** – 個人による不正行為の防止。
- **不明瞭さによるセキュリティを避ける** – コア機能やソースコードを隠すことなく、アプリケーションを安全に保つために十分なセキュリティコントロールを使用します。
- **セキュリティはシンプルに** – 可能な限り複雑さを減らし、コードを見えるようにします。
- **セキュリティ問題を正しく修正する** – 欠陥の根本原因を分析し、それに対処する必要があります。

情報セキュリティは、Medidataのビジネス文化の一部でもあります。情報セキュリティガバナンスを確立するためのMedidataの戦略には、顧客データの機密性、完全性、可用性を保持し、ランサムウェアやデータ侵害などの悪質な事象によるビジネスへのダメージの可能性を最小限に抑えることが含まれます。

Medidataのガバナンス戦略は、業界をリードするトレーニングと教育を組み合わせて実施され、経験豊富で認定を受けたセキュリティ専門家からなる多様なチームによって支えられています。セキュリティオペレーション、セキュリティエンジニアリング、セキュリティアーキテクチャ、インシデントレスポンス、アイデンティティおよびアクセス管理、リスク管理、セキュリティフレームワークなどの機能を提供します。Medidataのセキュリティガバナンスの実施は、少なくとも年1回検査・監査され、Medidataが適切なセキュリティおよびプライバシー要件すべてに準拠していることを保証します。

エンタープライズリスク管理

Medidata の経営委員会（Executive Committee、XCOM）は、顧客に対する責任には強力な管理体制が必要であると認識しています。したがって、効果的なセキュリティ管理を確実に実施するための取り組みは、Medidata の全体的なリスク管理戦略の重要な一部となっています。

CISOが監督するこのプロセスでは、戦略的監視のアウトプットを活用して戦略的リスク登録簿を作成します。このリスク登録には、セキュリティ要件と管理、運用上特定された脅威、新たに出現したグローバルなサイバーセキュリティの脅威のハイレベルな見解が組み込まれています。

これらのリスクとその対処法は、Dassault Systèmes取締役会への最新情報の一部です。私たちは組織の戦略的プログラムとして、トップダウンの支援を続けています。

先進的な企業は、リスクが万人のビジネスであることを知っています。それは、単一の業務に限定されたり、業務サイロの中でその場限りで実行されたりするものではありません。リスクの所有権は企業全体で共有され、深い協力と透明性が求められます。Medidata は、現在のグローバル市場の変動、そして私たちの経済、ビジネス、社会のエコシステムを大きく混乱させた過去数年間の教訓を踏まえて、これが真実であることを知っています。

理想的な世界では、このような混乱やリスクを効果的に管理・軽減するために必要なリアルタイムの情報（サイバー、ビジネス、オペレーション、評判を含む）、このような情報は、企業内に流れ込み、明確に定義された利害関係者グループ全体で共有され、迅速かつ十分な情報に基づいた意思決定ができるようになります。

Medidataはこのような理想的な状態を目指しています。予測不可能で変化の激しい世界と、その結果として拡大する脅威の状況をうまく乗り切るためには、ここにいる私たち全員が目指すべき目標です。

Medidata の成功は、潜在的なリスク事象を随時リアルタイムで検出するために必要なシステムとプロセスを活用した、プロアクティブな統合セキュリティおよびリスク管理ソリューションの構築に基づいています。

情報セキュリティのフレームワークと監査

Medidataは、ISO 27001、27002、27701、27017、27018、SOC1 & SOC2+、NIST 800-53v5など、複数の認証に基づくセキュリティフレームワーク、セキュリティ管理、セキュリティ手法を導入しており、一般データ保護規則（General Data Protection Regulation、GDPR）やその他の地域規制にも準拠しています。また、米国連邦政府のお客様向けにFISMA MODERATE Operate Authorityを取得しています。認定を受けた第三者機関による外部監査は、ISO、FISMA、SOC2+について毎年実施され、お客様の製品、ソフトウェア、サービスを提供・サポートするMedidataの人材、プロセス、技術に関する適切な内容をカバーしています。

各認証審査は、Medidataが地域、国、国際的な法律や規制を遵守していることを、現在および将来の顧客に保証するものです。各監査は外部監査人により実施され、指摘事項や不適合はMedidataのチケットシステムで追跡されます。これらのチケットには根本原因の詳細が記載されており、問題解決に必要な取り組みを定期的に更新する必要があります。月次報告書は情報セキュリティリーダーシップに提出され、必要に応じてレビューとエスカレーションが行われます。

Medidataは、これらのセキュリティフレームワークによって確立された規定要件に基づき、「最善の」ハイブリッドソリューション（組織的および技術的）を採用しています。この全体的なアプローチは、確立されたすべての要件を満たすセキュリティ管理およびメカニズムの包括的な実装をサポートします。

境界線の確保と保護

Medidataのアクセスコントロールの実装は、すべてのアカウントが継続的に管理され、特権アカウントと非特権アカウントの両方のアクセスが、割り当てられたユーザーの役割と責任に基づいて制限され、最小化されるように設計されています。アクセス管理要件は、全アカウントのアクセス権の追加／削除／変更の指示を提供し、制限されたアクセス権を確実に実施するための管理システムを特定し、付与された全アクセス権のレビュー頻度を特定するために使用されます。様々な自動化ツールは、必要に応じて自動的にアカウントを無効にしたり、すべてのアカウント管理活動（アカウントの作成、変更、有効化、無効化、および削除）を監査するなど、アカウントの管理を強制するために継続的に使用されます。

事前に承認されたインターコネクションは、確立されたサービスレベルの合意に基づいて、システム内での情報の流れを確実にするために使用されます。Medidataでは、すべてのリクエストをチケットシステムで管理しており、アカウント処理活動を調整するために、少なくとも2名の管理者を必要としています。アカウントは、四半期ごとにアイデンティティ アクセス管理チームによってレビューされます。ログオン失敗の制限とロックアウトの自己修復は、CIS Benchmarksによって確立されたガイダンスに基づいて実施されます。本人確認と認証がない限り、ユーザーやデバイスによるいかなる行為も許可されません。リモートアクセスは、MFAとすべての接続の暗号化によって強制されます。すべてのアカウントへのアクセスは、Security Event and Incident Manager（セキュリティ イベントおよびインシデント マネージャー）とゲートウェイ保護手段によって監視されます。

アイデンティティ プロバイダおよびサービス（Identity Provider and Services、IdP IpS）

Medidataは、プリンシパルのID情報を作成、保持、管理し、フェデレーションまたは分散ネットワーク内の依存アプリケーションに認証サービスを提供するIDプロバイダ（略称：IdPまたはIDP）をMedidataシステムアクセスのために使用します。

信頼できるIDPを使用してアプリケーションへのアクセスを管理するサービスとして、ユーザー認証を提供しています。IDプロバイダは、シングルサインオン（single sign-on、SSO）を使用して他のウェブサイトにアクセスできるようにする信頼できるプロバイダであり、パスワードの負担を軽減することでユーザビリティを向上させ、潜在的な攻撃対象領域を減らすことでより優れたセキュリティを提供します。

アイデンティティ プロバイダは、クラウド コンピューティング リソースとユーザー間の接続を容易にし、モバイルおよびローミング アプリケーションの使用時にユーザーが再認証する必要性を低減させることができます。

最小特権機能は、CIS Benchmarksのコンフィギュレーション設定に準拠し、ホストとゲートウェイのさまざまなアクセス制限を適用することで実装されます。

識別、認証、認可

Medidataは、ISOおよびNISTによって確立された要件と一致する識別および認証方法を実装しています。Medidataのスタッフ、顧客ユーザーを問わず、すべてのユーザーは固有のIDを使用して認証されます。ユーザーアカウントとパスワードは、ユーザー固有のものである必要があり、認証情報の共有は許可されていません。また、Medidataは全スタッフに対して多要素認証を強制しており、オプションでお客様に多要素認証を提供しています。

MCCは、アクセスおよび権限の管理、包括的な監査証跡、電子署名を電子記録にリンクさせる電子署名システムを提供し、否認防止を確立します。Medidataは、ユーザアカウントを有効にする際、ならびに運用を管理・サポートする際に、顧客とその担当者がこれらの要件を理解することを求めています。

サイバーセキュリティと情報セキュリティ啓蒙トレーニング

Medidataのサイバーセキュリティトレーニングの実施は、請負業者を含む全従業員が、それぞれの立場とセキュリティ責任に応じた適切なトレーニングを受けられるように設計されています。

Medidata 全体で、いくつかのトレーニングモジュールが使用されています。年次トレーニングは追跡され、コースワークを修了していない従業員または請負業者は、すべてのMedidataシステムからアクセス権を剥奪されます。永続的な復帰には、トレーニングを修了し、マネージャーの承認が必要です。

トレーニングは、Medidataのラーニングマネジメントシステムを利用したeラーニングトレーニングコースで管理され、3DSラーニングマネジメントシステム内でもオンデマンドで追加コースを受講することができます。

監査または監視

Medidataのセキュリティイベント監査の実装は、監査が必要なすべてのイベントを確実に捕捉し、ISO 27001ファミリーおよびNIST 800-53の要件と一致するように設計されています。Medidataは、さまざまなSIEMツールを使用して、セキュリティ侵害、侵入の試み、完全性イベント、システムとコンポーネントの障害、ユーザーアクティビティイベントの監査を含む、これらの要件に対する監視と監査を行っています。監査可能なイベントはすべて継続的に監視されます。

SIEM

セキュリティ情報・イベント管理（Security Information and Event Management、SIEM）機能が環境全体に導入されています。FIPS 140-2に準拠した暗号方式とソリューションがシステム全体で使用されています。

構成管理

Medidataは、さまざまな構成変更管理ツール、プロセス、手順を使用して、すべてのシステムとコンポーネントのライフサイクルを通じて構成管理を実施しています。ベースライン構成は、自動化ツールでサポートされる検証パッケージで保持します。すべての変更は体系的に追跡されます。テストと検証は、構成管理プロセスの不可欠な部分です。セキュリティとプライバシーの担当者は、変更審査委員会（Change Review Board、CRB）のメンバーであり、必要に応じてセキュリティとプライバシーのリスク評価を行います。

事業継続・災害復旧（BC/DR）

Medidataは、組織全体に適用される包括的な事業継続・災害復旧（Business Continuity and Disaster Recovery、BC/DR）機能を導入しています。

計画プロセスは、Medidata自身のニーズだけでなく、SLAで示されるお客様の要件によっても推進されます。サービスデリバリー、カスタマーサクセス、プロフェッショナルサービスチームを含め、Medidata内のすべての主要な個人と組織が、災害復旧計画の年次演習とレビューに参加しています。当社の計画プロセスには、お客様のSLAによって設定された復旧時間目標内に、すべてのミッションおよびビジネス機能を復旧させることが含まれています。この計画プロセスでは、すべての重要なシステム資産と、すべてのミッションおよびビジネス機能が特定されます。出来上がった計画は少なくとも年1回必ずテストされ、フィードバックとテスト結果は私たちの機能を継続的に改善するために使用されます。

インシデントレスポンスと処理

Medidataは、システムとデータの機密性、完全性、可用性に対する緊急の脅威を迅速に特定し、封じ込め、修復するための包括的なインシデント対応計画を保持しています。

Medidataは、24時間365日体制のセキュリティオペレーション専門チーム、グローバルネットワークオペレーションセンター（Global Network Operations Center、G-NOC）を保有し、すべてのインシデント処理活動を監視・サポートしています。Medidataのセキュリティ運用チームは、SIEMや各種ロギング、イベント管理、レポーティングツールなど、さまざまな自動インシデント管理ツールを使用しています。情報セキュリティの警告は、当社のセキュリティ オペレーション センター（Security Operations Center、SOC）またはグローバル ネットワーク オペレーション センター（GNOC）システムから情報セキュリティ担当者にエスカレーションされ、その後、研究開発（R&D）（情報セキュリティ）担当副社長および上級管理職に通知されます。当社のインシデント レスポンスのフレームワークでは、カスタマーアラートの引き金となる状況や、お客様への通知方法について詳しく説明しています。また、セキュリティ インシデントのライフサイクルを管理するための対応についても言及しています。この計画には、イベントや インシデントの特定、準備、封じ込めから復旧、通知、事後処理に至るまで、段階とその段階に関連するアクションが記述されています。Medidataは、セキュリティインシデントの検出後、合理的な時間枠の中で、セキュリティインシデントの確認と影響分析を行い、サービス契約で定められたコミュニケーションチャネルを通じてMedidataの顧客に通知します。すべての問題は、オンラインのデータベース主導型問題管理システムで追跡されます。Medidata は、インシデントレスポンスのトレーニングとテストを、毎年実施している災害復旧テストに統合しています。

保守

Medidata は、すべてのセキュリティ保護が完全に損なわれないようにすることを全体的な目的として、すべての変更に対する優先順位付けと承認要件を含む厳格な保守プログラムを実施しています。脆弱性スキャン、アプリケーションスキャン、マルウェア対策は、保守活動中に使用されるすべてのメディアをチェックするために実施されます。外部デバイスは、最初にスキャンされない限り接続できませんし、運用スタッフの管理下にある場合に限ります。すべての保守は、変更管理プロセスの一環として文書化され、承認されます。また、ロールバック計画やテスト・検証要件も含まれます。

メディア保護

Medidataは、データが処理または保存される各拠点でメディア保護を実施しています。すべてのデータはアクセス制限のあるデータとして扱われ、アクセスは当社の運営スタッフによって管理されます。これには、データの破壊、削除、バックアップ、および復元を目的としたアクセスが含まれます。破棄が指定されたメディアはすべて追跡され、破棄されたメディアごとに破棄証明書が発行されます。メディアはMedidataの外部で再利用されることはありません。使用中、輸送中、保管中のすべてのメディアは、FIPS 140-2に準拠した暗号化手法で保護され、データの完全性と機密性が保持されるようになっています。

データ損失防止

Medidata のデータ損失防止 (Data Loss Prevention、DLP) は、機密データが紛失したり、悪用されたり、権限のないユーザーによってアクセスされたりしないようにするための一連のツールとプロセスです。DLP ソフトウェアは、規制対象データ、機密データ、およびビジネスクリティカルなデータを分類し、組織によって定義されたポリシー、またはHIPAAやGDPRなどの規制コンプライアンスによって一般的に推進される事前定義されたポリシーパック内のポリシー違反を識別します。このような違反が特定されると、DLPはアラート、暗号化、その他の保護措置によって是正を実施し、エンドユーザーが誤って、または悪意を持って、組織を危険にさらす可能性のあるデータを共有することを防ぎます。
データ損失防止ソフトウェアとツールは、エンドポイントのアクティビティを監視および制御し、企業ネットワーク上のデータストリームをフィルタリングし、クラウド上のデータを監視して、静止状態、移動中、および使用中のデータを保護します。DLPはまた、コンプライアンスや監査要件を満たし、フォレンジックやインシデントレスポンスのための弱点や異常の領域を特定するためのレポートも提供します。

環境セキュリティ

許可された人員に限定された施設および保護された情報資産への物理的アクセス。Medidataは、情報システムを含む施設へのアクセスが許可された人員の最新のリストを保持し、適切な認可資格証明書（バッジ、IDカード、スマートカードなど）を発行します。組織内の指定された職員は、少なくとも年1回、アクセスリストと認証情報を見直し、承認します。

デザイン上、一般にアクセス可能なエリアはありません。物理的アクセスリストは建物の管理人が保持しますが、施設のセキュリティチームが定期的に見直します。データセンターへのアクセスには、生体認証、スマートカード、暗証番号の組み合わせが、正しい順番で要求されます。立ち入り禁止区域への立ち入りを許可する前に、上層部の承認を得る必要があります。

Medidataは、情報システムへの物理的なアクセスを監視し、物理的なセキュリティインシデントを検出して対応します。物理的なアクセスは自動的に記録され、確認することができます。カメラは物理的なアクセスを記録するために使用されます。

Medidataは、施設へのアクセスを許可する前に訪問者を認証することで、情報システムへの物理的なアクセスを管理しています。訪問者のアクセスは、事前にアクセス申請書を提出し、Medidataの適切な担当者の承認を得る必要があります。すべての訪問者は施設内でエスコートされます。

Medidataは、セキュアなエリアと機器の物理的セキュリティに関する手順を文書化した正式な情報セキュリティポリシーを保持しています。

セキュリティ計画

Medidata は、ISO 27001に基づく継続的なセキュリティプログラム改善プロセスを実施しています。ISO 27001認証の情報セキュリティ管理システムが、NIST準拠のシステムセキュリティ計画とともに Medidata Clinical Cloud に導入されています。これらの計画は毎年更新され、新しく変化するセキュリティとプライバシーのアーキテクチャ要件を取り入れ、Medidataの強固なセキュリティ機能を確保しています。このアプローチにより、セキュリティとプライバシーのアーキテクチャのすべての変更が、セキュリティ計画、適格性評価文書、エンジニアリング文書、製品文書、ホスティング文書に確実に組み込まれます。

人事セキュリティ – 人的資本

従業員は、身元調査手続きに関連して実施された身元調査の結果を考慮し、労働者の行動基準に従って雇用されます。すべての人員は、Medidataシステムにアクセスする前に、ビジネス行動規範を読み、確認し、遵守する必要があります。この完了は、Medidataのラーニングマネジメントシステムに記録されます。これらの人的セキュリティプロセスは、第三者の請負業者やコンサルタントにも適用されます。

製品およびサービスの認定

Medidataは、毎年計画、文書化、承認され、セキュリティとプライバシー要件への配慮を含む包括的な取得プロセスを実施しています。これには、侵入テスト、FISMA評価、ISO監査、SOC2監査、EU-US DPF認証、その他のセキュリティ関連活動のための資金が含まれます。また、新しいセキュリティとプライバシー機能をシステムソフトウェアに組み込むために必要な暗号化製品やソフトウェアのための資金も計画に含まれています。情報セキュリティチームとプライバシーチームは、取得プロセスに関与し、取得中にすべてのセキュリティとプライバシー要件が含まれるようにします。

システムと情報の完全性

Medidata は、自動化ツール、チケットシステム、パッチ管理システム、品質保証プロセスを使用して、システムおよび情報の完全性保証を組織全体で実施し、Medidata システムのライフサイクル全体を通じて監視、スキャン、発見事項の修正を行っています。悪意のあるコードからの保護は、企業全体に適用されながら一元的に監視・管理されます。Medidata システムの完全性を保証するために、環境全体にわたって完全性監視ツールが採用されています。Medidataシステム内の情報は、保存時および転送時に暗号化されます。また、Medidataは継続的にNational Vulnerability Databaseを監視しています。

第三者リスク管理（Third Party Risk Management、TPRM）

Medidataは、サービス提供の一環として、Medidataに代わって個人情報（Personally Identifiable Information、PII）を含むデータにアクセスし、処理する第三者およびサブサービスプロバイダを利用しています。

Medidataプライバシーオフィス(Medidata Privacy Office、MPO)は、ビジネスエリア、被験者担当エキスパート、管理部門と協力し、参加者の個人情報の処理に関わる第三者に要求されるプライバシーの取り組みを概説する条項を含む契約を作成します。MPOと法務チームは、プライバシーに関する条項がMedidataの基準に従って含まれていることを確認するため、新しい第三者との契約をレビューし、承認します。

グローバルコンプライアンス＆ストラテジー（Global Compliance & Strategy、GCS）は、MPO、情報セキュリティ（Information Security、InfoSec）、事業部門と連携し、すべての新規ベンダーが、Medidataのシステムと環境にアクセスする第三者ベンダーの定義されたリスクベースの評価を受けることを保証します。Medidataは、参加者の個人情報（PII）にアクセス、使用、および/または保管する第三者ベンダーに重点を置いて、第三者ベンダーの定期的なリスク評価を実施し、その結果を分析し、必要と判断された場合には、リスクア評価の結果リスクが高いと判断された第三者ベンダーを評価するための文書化された計画を策定します。ベンダーの評価は、定められた Medidata サプライヤー評価の方針と手順に従って実施されます。ベンダー評価の結果は文書化されています。

サプライヤーの評価と監査

Medidata SDLC をサポートするため、または Medidata、Medidata の顧客もしくは Medidata のパートナーにサービスを提供するために提案されたすべての第三者ベンダーは、Medidata の担当者によるセキュリティ評価を受けるものとします。Medidata は、基本的な運用セキュリティ指標が Medidata の要件に適合していることを確認するため、当初および定期的にサプライヤーを評価します。サプライヤーは定期的に評価されます。重要なサプライヤーは前回の評価から12か月以内に、大きなサプライヤーは前回の評価から12～24か月以内に、小さなサプライヤーは前回の評価から24～36か月以内に評価されます。

サプライヤーに関する予期せぬ出来事により、定期的な監査や質問票が実施される場合があります。公表日、監査日、完了日を含む物流サプライヤー監査情報は、サプライヤーのステータス/スケジュールに保有します。

アンチウイルスおよびアンチマルウェア保護

アンチウイルスおよびアンチマルウェア保護侵入検知システム（Intrusion Detection System、IDS）とファイアウォールに加え、Medidataはデータセンターのネットワークを通過する前にすべてのデータをさらにサニタイズするため、さまざまなスキャンツールを使用しています。これらのスキャンツールは、悪意のあるものが当社の防御を突破し、当社のシステムにアクセスしようとする場合に通知します。Medidataのネットワークセキュリティは、「予防の1オンスは治療の1ポンドに勝る」という古いことわざを実践しています。この場合、マルウェアスキャンが予防となります。エンドポイントセキュリティのインストールマルウェア対策、エンドポイント検出と応答を含む、すべてのプロダクションおよび検証システム、サーバーファイアウォール、ログインスペクション、侵入検知防御モジュール。

データ暗号化

PHIおよびPIIを含むすべてのデータは、最新の高度暗号化標準アルゴリズム(Advanced Encryption Standard algorithms、AES-256)を使用して暗号化された形で保存および送信され、定期的に復元可能性の検査が行われます。

転送中のデータ暗号化

このシステムは、トランスポート レイヤー セキュリティTLS v.1.2を使用して、転送中のデータの暗号化を実現しています。TLS v.1.2では、クライアントコンピュータがサーバーと一般にアクセス可能な接続を確立することができますが、クライアントとサーバーだけが復号化、つまり送信される情報を解釈可能で使用可能な形で見ることができます。TLS 1.3は、技術的な主流として採用されています。

静止時の暗号化

暗号化はストレージ ユニット レベルで有効化され、ハードウェアを通じて影響を受けます。Rave EDCデータストアでは、PureStorageストレージエリアネットワークが独自の鍵管理システムを使用して256ビットのAES鍵を使用します。私たちのマルチテナント システムでは、AES-256も使用していますが、AmazonのKMS製品を使用しています。

システムハードニングスタンダード

Medidata は、すべての MCC コンポーネントに CIS Benchmarks ハードニング ガイダンスを実施し、その他のハードニング技術も導入しています。

リモートコネクティビティ

デフォルトでは、Medidataはポート443からのインバウンドトラフィックのみを許可します。ファイアウォールとIDPは、送信元ポートと宛先ポートをブロックし、トラフィックの安全性を確保します。24時間365日のグローバル ネットワーク オペレーション センター（「GNOC」）が稼働しており、常に誰かが環境を監視しています。さらに、Medidata は第三者のマネージド セキュリティサービス プロバイダー(Managed Security Service Provider、MSSP)と契約しており、そこが24時間365日体制でセキュリティ環境をカバーし、15分というサービス レベル アグリーメント(Service Level Agreement、SLA)のもと、環境を保護するための措置を講じる権限を与えられています。

プライバシープログラム

Medidataプライバシーオフィス（以下「MPO」）は、顧客に代わって個人データを処理するMedidataの役割に基づき、グローバルプライバシープログラムのプライバシー原則を実施します。Medidataの顧客は、契約サービスのためにMCC内で提出され処理される個人データに関して、「データ管理者」として行動します。データ管理者（または適用される法律で定義された同様のエンティティ）とは、個人データの処理の手段と目的を決定する主体を指します。すなわち、Medidataの顧客は、自らのデータ管理者として、臨床試験のためにMCCを利用する際に、どのような個人データを収集、提出、処理、開示、保持、および/または破棄するか、また、それらの活動がどのような目的で行われるかを決定します。Medidataの役割は「データ処理者」であり、データ管理者の指示を実行し、決定された処理の手段と目的を実行するエンティティです。

データ処理業者としてのMedidataは、効果的なデータセキュリティ対策を実施し、上記の責任分野に関して顧客の指示に従うことに、第一義的な責任を負います。

ユーザーエンティティに対するプライバシーのコミットメントは、顧客との契約／合意において文書化され、伝達されます。このようなプライバシーに関する約束には、以下のものが含まれますが、これらに限定されるものではありません：

- 適用される契約、法律、規制に基づいて、システムハードウェアおよび機密データを適切に処理し、安全に維持、廃棄、破棄するためのデータ保持および廃棄ポリシーと手順。
- MPOは、適用される法律およびベストプラクティスに従って、顧客の個人情報の収集、アクセス、使用、保管、開示、廃棄を規制するグローバルプライバシー プログラムを保持しています。
- ユーザーエンティティは、MCCにログインする際に表示される「利用規約」の一部として、個人データに関するMedidataの慣行について知らされています。
- Medidataは、MCCの製品リリースごとに「デザインによるプライバシー（Privacy by Design）」評価を実施し、個人データ処理への影響や重大な変更を評価します。
- Medidataは、顧客の個人データへの適切なアクセスと使用を検証するために、顧客データガバナンスプログラムを保持しています。
- Medidataは、顧客の要求に応じて、顧客の個人データを返却または削除します（適用される規制/法的要件に従って）。
- MPOは、顧客の個人情報の不正開示を特定・評価するためのプライバシー インシデント レスポンス プログラムを保持しています。

デザインによるプライバシー

Medidata は、MCC 全体における個人を特定できる情報のソースと場所を文書化した、アプリケーションおよびデータのインベントリを正式に文書化しています。アプリケーションとデータの評価尺度は、デザインによるプライバシープロセスの一環として、各製品チームが作成します。標準テンプレートは、収集されるデータの種類、そのビジネスプロセスにおける関連するプライバシーリスク、およびこのプロセスを通じて特定されたプライバシーリスクを軽減するための管理策を明記した、ビジネスプロセス分野ごとに文書化され、保持されます。

デザインによるプライバシープロセスの一環として、プロダクトオーナーは、参加者の個人情報にアクセス、使用、および/または保存する既存のプロセスに新規または変更をもたらすプロジェクトを評価し、個人情報および関連する管理への影響を評価します。このような変更が確認された場合、MPOは、MCCにおける個人識別情報の処理方法の変更に伴うリスクを評価します。デザインによるプライバシープロセスの一環として特定されたコントロールギャップは文書化され、そのギャップに対処するための是正措置計画が策定され、実行されます。

デザインによるセキュリティ

安全なコーディング標準

MedidataはOWASPに基づき、SDLCプロセスに安全なアプリケーション開発を組み込んでいます。ソースコード リポジトリに格納されているため、正式なコーディング標準とコーディング ガイドラインがバージョン管理下にあります。

ソフトウェア開発ライフサイクル

MCCは、臨床開発プロセス全体の活動を管理するために設計されたエンドツーエンドの技術とデータ分析ソリューションを提供しています。SaaS環境であるMedidataプラットフォームは、顧客の要件に応じてスケーラブルかつ拡張可能です。Medidata は、アジャイル開発の原則に基づき、文書化された SDLC プロセスを遵守し、プロセス全体を通じて品質を構築することで、これを実現しています。Medidataは、適格なインフラストラクチャ上に存在し、顧客の要件を満たし、規定通りに機能し、適用されるGCP、データ保護/データプライバシー、電子記録/電子署名（Electronic Records/Electronic Signatures「ERES」）の規制およびガイダンスへのコンプライアンスをサポートするソフトウェアを製造します。SDLCの要件とプロセスは、当社のソフトウェア開発およびリリース手順に文書化されています。IT インフラの資格要件とプロセスは、ホスティング環境アーキテクチャ管理文書に文書化されています。

SDLC活動はR&D部門が行います。R&Dには機能部門が存在し、それぞれがMedidataソフトウェアの設計、開発、テスト、検証、導入、運用サポートの管理責任と権限を有しています。ソフトウェア リリースの種類には、アルファ リリース、ベータ リリース、機能リリース、標準ソフトウェア リリース、緊急ソフトウェア リリースがあります。

脆弱性の特定と管理

Medidataの脆弱性評価とは、情報システムの潜在的なセキュリティ上の弱点を体系的に検討することです。システムが既知の脆弱性の影響を受けやすいかどうかを評価し、それらの脆弱性に重大度レベルを割り当て、必要な場合は随時、修正または緩和を推奨します。

アプリケーションセキュリティ脆弱性評価

Medidata がソフトウェアのセキュリティ脆弱性評価を実施する際の主な目標。Medidataがお客様のために作成するのは、システム、ネットワーク、アプリケーションのセキュリティ管理における脆弱性を特定することであり、これらの脆弱性を悪用することで、権限のないユーザーが取得できないはずのシステムや指定されたデータにアクセスすることができます。評価には、動的（Dynamic Application Security Testing、DAST）及び静的（Static Application Security Testing、SAST）コード解析セキュリティスキャンが含まれます。Medidataは、テストの定義されたパラメータの範囲内で、上記の目標を実現するために、特定されたシステム、ネットワーク、アプリケーションの脆弱性を特定し、その悪用を試みます。

ステルスセキュリティ評価ではないため、攻撃を偽装することはありません。実際の攻撃は、システム管理者にとってそれほど明白ではないかもしれないことに留意すべきです。テストプロセスは、一般的な脆弱性評価で使用されるスキャナやチェックリストの手法から得られる一般的な結果を制限するために、手動で行われることがあります。あるいは、アプリケーションのマッピングや潜在的な脆弱性の特定に自動化ツールを使用することもできます。こうすることで、テスターはアプリケーションに対するロジックベースのテストに集中することができます。

ネットワークセキュリティ脆弱性評価（侵入評価）

Medidataのネットワーク脆弱性評価には、Medidataネットワーク外のテスト場所からアクセス可能なサーバー、スイッチ、ルーター、ワークステーションなどのリソースが含まれます。Medidata は、最高情報セキュリティ責任者（Chief Information Security Officer 、CISO）によって承認された入念にスクリプト化された検査手法を使用して、ネットワークとコンポーネントのテストを実施します。従事規則では、実施されるテストには、Medidataが所有および/または運営しない相互接続ネットワークコンポーネントのテストは含まれないと規定されています。

さらに、検査には、意図的にシステムにサービス拒否（Denial of Service、DoS）をもたらしたり、意図的に悪用可能なターゲットシステムに損害を与えたりする行為は含まれません。外部の脆弱性評価は、Medidataの物理的な拠点/ネットワーク以外の場所から実施されます。

Medidata は、定期的な脆弱性評価や侵入テストを含め、自社の環境と関連する統制について複数の独立した評価を実施しています。これらの検査テストは、環境全体でそれぞれ毎週と四半期ごとに実行されます。情報セキュリティ部門により「重要」または「高」と評価されたすべてのセキュリティ問題は、情報セキュリティ部門の責任者が書面で承認しない限り、発見から30暦日以内に是正されるものとします。すべてのセキュリティ問題
情報セキュリティ部門が「中程度」と評価した場合、情報セキュリティ部門の責任者が文書で承認しない限り、発見から180暦日以内に是正されなければなりません。

独立テストとレビュー

セキュリティは、客観的な観察者が言うほど優れたものではありません。そのため、顧客や規制当局の評価に加え、複数の独立した機関を定期的に交代させることで、自己満足に陥らないようにし、客観性、最先端技術、新技術を駆使して、顧客とその患者の知的財産が適切に保護されるようにしています。

SOC2は、米国公認会計士協会（American Institute of CPAs、AICPA）が策定したサービス組織向けの自主的なコンプライアンス基準で、組織が顧客データをどのように管理すべきかを規定しています。この規格は、セキュリティ、可用性、処理の完全性、機密性、プライバシーというトラストサービス基準に基づいています。SOC2レポートは、各組織の固有のニーズに合わせて作成されます。特定のビジネス慣行に応じて、各組織は1つまたは複数の信頼の原則に従った管理をデザインすることができます。これらのレポートは、組織とその顧客、規制当局、ビジネスパートナー、サプライヤーに、組織のデータ管理方法に関する重要な情報を提供します。

SOC2レポートには2種類あります：タイプ1では、組織のシステムと、システム設計が関連する信頼原則に準拠しているかどうかを記述します。タイプ2では、これらのシステムの運用効率について詳しく説明します。

Medidata は、TSP セクション 100「2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy（AICPA：セキュリティ、可用性、処理の完全性、機密性、プライバシーに関するトラストサービス基準）」に規定されているセキュリティとプライバシーに関連するセキュリティに対する Medidata のコミットメント（「該当するトラストサービス基準」）と、開発および展開、品質保証、電子記録および電子署名に関連する Medidata Solutions, Inc. が決定した追加基準を実証するため、SOC2+ Type 2 を保持しています。

SOCの評価は、12か月ごとの母集団を対象に、6か月ごとに実施されます。Medidata はまた、Medidata Platform CTMS の治験実施施設向け決済サービスについても SOC-I Type 2 を保持しています。

ISO/IEC 27001

ISO 27001は、セキュリティ管理のベストプラクティスと、ISO 27002のベストプラクティス ガイダンスに従った包括的なセキュリティ管理を規定したセキュリティ管理規格です。これは、Medidataの顧客が大きな関心を寄せている、広く認知された国際的なセキュリティ標準です。

この規格の認証は、当社に次のことを要求しています:

- 企業の脅威と脆弱性の影響を考慮し、当社の情報セキュリティリスクを体系的に評価
- 企業およびアーキテクチャのセキュリティリスクに対処するための、包括的な情報セキュリティ管理策およびその他のリスクマネジメントの設計と実施
- 包括的な管理プロセスを採用し、情報セキュリティ管理が当社の情報セキュリティ上のニーズを継続的に満たす

この規格に基づく認証の鍵は、厳格なセキュリティ プログラムを効果的に管理することです。この規格で要求される情報セキュリティマネジメントシステム(Information Security Management System、ISMS)は、私たちがセキュリティを全体的かつ包括的な方法で継続的に管理する方法を定義しています。ISO/IEC 27001認証は、特にMedidata ISMSに焦点を当て、当社の内部プロセスがISO規格にどのように準拠しているかを測定するものです。認証とは、第三者公認の独立監査人が当社のプロセスと統制の評価を実施し、当社が包括的なISO/IEC 27001認証規格に沿った運用を行っていることを確認したことを意味します。

ISO/IEC 27701

ISO/IEC 27701認証は、ISO/IEC 27001と対になっており、プライバシー情報管理システム(Privacy Information Management System、PIMS)を確立、実施、保持し、継続的に改善するための要求事項を網羅しています。

ISO/IEC 27017

ISO/IEC 27701は、クラウドサービスのための情報セキュリティ実践規範です。これは、ISO/IEC 27001およびISO/IEC 27002の拡張版であり、クラウドサービスプロバイダーおよびクラウドサービスカスタマーのための追加のセキュリティ管理を提供します。

ISO/IEC 27018

ISO/IEC 27018は、セキュリティ管理のベストプラクティスと、クラウドコンピューティング環境におけるプライバシー情報に関する包括的なセキュリティ管理を規定したセキュリティ管理規格です。この規格は、プライバシー関連情報の効果的な管理を保持するために、ISO/IEC 27001やその他のセキュリティフレームワークを補完するものです。

ISO/IEC 27001と同様に、ISO/IEC 27017および27018の認証は、第三者認定独立監査人が当社のプロセスと管理の評価を実施し、当社が包括的なISO 27018認証基準に沿って運用されていることを確認したことを意味します。

FISMA MODERATE

Medidata は、米国政府機関の顧客が連邦情報セキュリティ管理法（Federal Information Security Management Act、FISMA）のコンプライアンスを実現し、維持できるようにします。FISMA は、連邦政府機関に対し、NIST（米国国立標準技術研究所特別刊行物）SP 800-53 改訂 5 版に基づき、データおよびインフラストラクチャの情報セキュリティシステムを開発、文書化、および実装することを求めています。FISMA は、Medidata に広範なセキュリティ設定と管理の実装と運用を要求しています。これには、物理および仮想インフラストラクチャのセキュリティ確保に使用される管理、運用、および技術プロセスの文書化、ならびに確立されたプロセスと統制の第三者監査が含まれます。Medidataは、サービスとしてのソフトウェアに関する FISMA コンプライアンスを保持するため、毎年評価を受けており、多くの米国政府機関から 運営権限（Authority to Operate、ATO）を授与されています。

EU-USのデータ プライバシー フレームワーク（Data Privacy Framework、DPF）と関連フレームワーク

EU-US データ プライバシー フレームワークと、EU-US DPF の英国拡張版やスイス-US DPF などの関連フレームワークは、EU、英国、スイスの法律と整合性のあるデータ保護を確保しながら、欧州連合、英国、スイスから米国への個人データ移転のための信頼できるメカニズムを Medidata に提供します。EU-US DPFおよび関連する枠組みに参加する組織は、個人データを受け取る可能性があります：（1）EUからは、EU-US DPFに関する欧州委員会の妥当性決定の発効日である2023年7月10日から、（2）英国からは、英国のエクステンションを実施する妥当性規制の発効日である2023年10月12日から。(3) スイスからは、スイス-US DPF に関するスイスの妥当性承認発効日に発効。EU-US DPFおよび関連するフレームワークは、世界中のEU、英国、スイス市民の個人データを保護する強い義務を米国企業に課しています。

実際にはどうなのでしょうか？

Medidata Solutionsについて

- EU-US DPF原則の遵守（通知、選択、上方移転の説明責任、セキュリティ、データの完全性と目的制限、アクセス、償還請求、執行、責任）
- EU-US DPFの要求事項を満たしていることを毎年自己証明

欧州、英国、スイスにおけるMedidata Solutionsのお客様について

- 米国への個人データ移転に関する透明性の向上と、個人データ保護の強化。
- Medidata の EU-US DPF に対する自己認証を確認するには、EU-US DPF ウェブサイト https://dataprivacyframework.gov をご覧ください。

FIPS 140-2

連邦情報処理規格（Federal Information Processing Standard、FIPS）出版物140-2は、機密情報を保護する暗号モジュールのセキュリティ要件を規定した米国政府のセキュリティ規格。FIPS 140-2 要件を満たす顧客をサポートするため、Medidata Private Cloud エンドポイントと Medidata の終端ロードバランサは、FIPS 140-2 で検証されたアルゴリズムで動作します。FIPS 140-2準拠モードで動作させるには、ユーザブラウザ側の接続に同等の機能が必要です。当社では、FIPS 140-2認定ハードウェアは採用していませんが、FIPS 140-2ソフトウェアが完全に承認された同等のメーカーとモデルを使用しています。

HIPAA

Medidataが提供する特定のサービスにおいて必要とされる場合、Medidataは、米国医療保険の相互運用性と説明責任に関する法律（U.S. Health Insurance Portability and Accountability Act、HIPAA）の対象となる事業体およびそのビジネスアソシエイトが、保護された医療情報を処理、保持、保管するためにMedidataのセキュアな環境を利用できるようにします。

締め

Medidataのセキュリティ業務は、最高の人材、プロセス、技術で構成されたワールドクラスのものだと感じています。私たちはその責任を真摯に受け止め、日々顧客と患者さんの信頼に応えています。私たちは自分たちの仕事に誇りを持ち、それを喜んでお見せします。

この文書に加え、脆弱性の概要、侵入テストの結果、認証、監査、その他のセキュリティ関連事項をhttps://www.medidata.com/en/trust-and-transparency に掲載することで、顧客とその治験実施施設は、患者さんが期待する保護がなされているという安心感を得ることができます。

ご質問やご不明な点がございましたら、Medidata 情報セキュリティフレームワークチーム asksecurity@3ds.com までお気軽にお問い合わせください。

免責事項

本セキュリティ・ホワイトペーパーに含まれる情報は、参照のみを目的としています。

本書に記載されていること、または顧客に対して口頭で伝えられたことは、当該顧客とMedidata、またはMedidataの子会社もしくは関連会社（以下、総称して「Medidata」といいます）との間の書面による契約の諸条件を修正、変更、またはこれらに優先するとみなされるものではありません。

Medidataは、本セキュリティ白書に記載されている方法または提案のいずれかが、顧客のシステムを復旧させること、悪意のあるコードに関連する問題を解決すること、またはその他の明示または意図された結果を実現することを、顧客に対して約束または保証するものではありません。お客様は、本セキュリティ白書に記載されているガイダンスを利用する、または利用しないことによるすべてのリスクを排他的に負うものとします。