情報セキュリティホワイトペーパー

メディデータの情報セキュリティプログラムの概要

熟慮された効果的な情報セキュリティプログラムは、臨床試験の完全性にとって非常に重要です。メディデータは、広く認知されている NIST SP 800-53 の示すセキュリティガイドラインに基づいて、一貫性のある検証済みのエンタープライズプログラムを開発・実装しました。本フレームワークの完全性は、NIST 800-53v5/FISMA 監査、SOC 1 Type II および SOC 2 Type II（追加コントロール付き）監査、および ISO 27001:2013、27018:2014、27701:2019 の年次評価など、複数の年次第三者評価によって評価・確認されています。

当社の情報セキュリティプログラムは、顧客のエンドツーエンドの臨床開発をサポートする、業界をリードする統合型インテリジェントプラットフォームの基盤となっています。メディデータの安全な臨床クラウドソリューションは、高可用性、完全性、機密性、信頼性、および柔軟性を提供して、幅広いアプリケーションを実現します。

ダッソー・システムズによる買収で、メディデータはダッソーのグローバルな規模を活用しつつ、安全かつ安定した拡張性の高いインフラストラクチャを継続的に提供できる最適な環境にあります。

本ホワイトペーパーでは、メディデータが当社に託されたデータを保護するために最前線で行っている投資と専門技術を理解するための概要を説明します。

信頼と透明性：メディデータトラストセンター

メディデータの情報セキュリティプログラムは、データプライバシーおよびグローバルコンプライアンス機能とともに、メディデータが安全かつ安定した拡張性の高いクラウドプラットフォーム、強固なデータガバナンスプロセス、検査可能な品質管理システムを構築することを可能としています。これらすべてが実現されていることが、臨床試験の実施を成功に導く鍵となります。

当社は自分たちの仕事に誇りを持って取り組んでおり、それを開示することを厭いません。そのため、本文書に加えて、四半期ごとの脆弱性サマリ、ペネトレーションテストの結果、認証、監査、その他のセキュリティ関連事項をトラストセンター（https://www.medidata.com/trust）に掲載し、顧客とその臨床施設が、患者さんの期待どおりの保護がなされていることに安心していただけるようにしています。

ご質問やご不明な点がございましたら、asksecurity@medidata.com までお問い合わせください。

「情報セキュリティは、患者のプライバシーや、場合によっては命を守るために非常に重要です。私が臨床試験の被験者になったとき、私の医療データの保護は個人的なものになりました。治験の被験者として、またサイバー脅威を理解するセキュリティ専門家として、メディデータは私の情報を保管・処理してほしい唯一の企業であると断言できます。」

- Glenn Watt、メディデータ最高情報セキュリティ責任者（2007-2018）

プログラム概要

メディデータでは、情報セキュリティとはチェックリストではなく、プログラムであると考えています。「Security by Design」、「Privacy by Design」の理念に基づき、システムの完全性を一から構築しています。

メディデータは、ライフサイエンス・テクノロジー・防衛の各産業において情報セキュリティの実践で合計 150 年以上に相当する経験を持つ、情報セキュリティ専門家チームを擁しています。

最高技術責任者・最高情報責任者・製品責任者に報告する当社の情報セキュリティチームは、CoBIT、ISO、SOC 基準に基づく情報セキュリティプログラムの完全かつ独立した管理を担当します。本プログラムは、PricewaterHouseCoopers、Apex CyberTek、DQS などの独立した第三者監査機関により、少なくとも年 4 回の監査を受けています。

インフラストラクチャの脆弱性スキャン、ソフトウエア・ピアレビュー、静的テスト、および URL の動的テストなどを、少なくとも月 1 回、または環境に大きな変化があった場合に実施しています。また、製品がリリースされる前に、すべての製品に対して脆弱性のスキャンを行っています。また、レッドチーム、ブルーチーム、パープルチームによるセキュリティ演習を毎年実施しており、侵入テスト担当者がレスポンスチームと緊密に連携することで効果を最大化しています。

クラウド環境の中核になるのは、Amazon Web Service （AWS） の米国東部・米国西部・フランクフルト・アイルランド・パリのデータセンターとなり、画一的なサポートとセキュリティモデルを用い、真のグローバルカバレッジを実現しています。Amazon のすべての製品に組み込まれている有機的なセキュリティ機能に加え、厳重なセキュリティグループ、厳格なネットワークアクセスコントロールリスト、CloudFront、AWS Shield および Advanced Shield、CloudTrail など、Amazon のすべてのセキュリティ機能をを活用しています。

また、プライベートクラウドをテキサス州ヒューストンで運用しており、地域の災害時にシステムを保護するため、ドイツのフランクフルトに代替クラウド施設を設置しています。

24 時間 365 日のサポートを提供するために、マネージドセキュリティサービスプロバイダを採用し、当社のセキュリティオペレーションセンター（security operations center; SOC）と密接に連携して、時間帯を問わずあらゆる脅威からの保護を実現しています。

当社は、これまで培った顧客と患者からの信頼を誇りとし、日々その信頼を獲得しています。

クラウドとオンプレミスセキュリティの違い

クラウドのセキュリティは、従来のオンプレミス環境のように管理する必要はありません。要塞化されたシステムのセキュリティ境界線の構想はより曖昧であり、外部ネットワーク接続が 1 つもない場合、すべてにおいてセキュリティを強化する必要があります。

クラウドのセキュリティは、従来のデータセンターのセキュリティ以上に熟慮されています。ネットワーク境界線の一連のコントロールに依存するのではなく、コントロールと技術がインフラストラクチャとアプリケーション層全体に浸透しています。これまでは境界型ファイアウォールを使用していましたが、現在ではセキュリティグループ、ネットワークアクセスコントロールリスト（ NACL）、ファイル整合性監視、マルウェア対策、ログ検査、Web レピュテーションチェック、Web アプリケーションファイアウォールレイヤーを各ホストに実装しています。

ハイパーバイザのセグリゲーション（図 1 参照）により、ホストとデータベースは完全に独立していますが、アンチビーコン監視、クラウドアクセスセキュリティブローカー、ウェブアプリケーションファイアウォールなどの高度なセキュリティ機能を利用できるように統合されています。

図 1

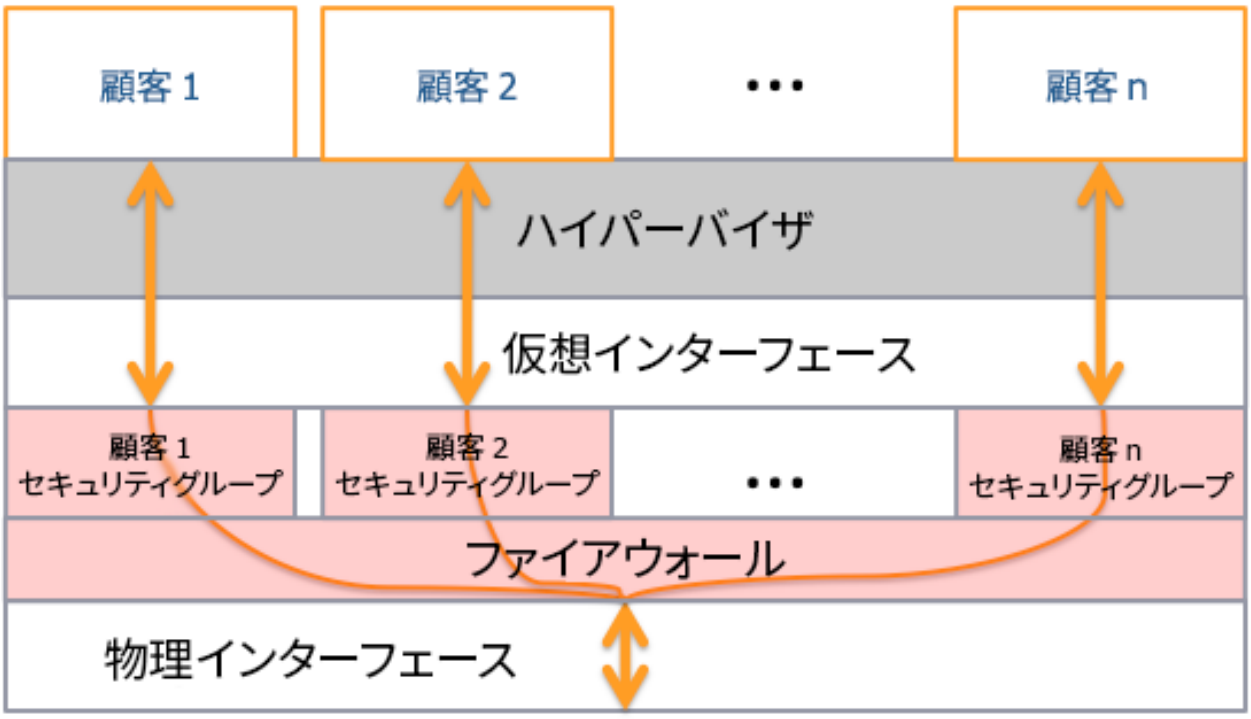
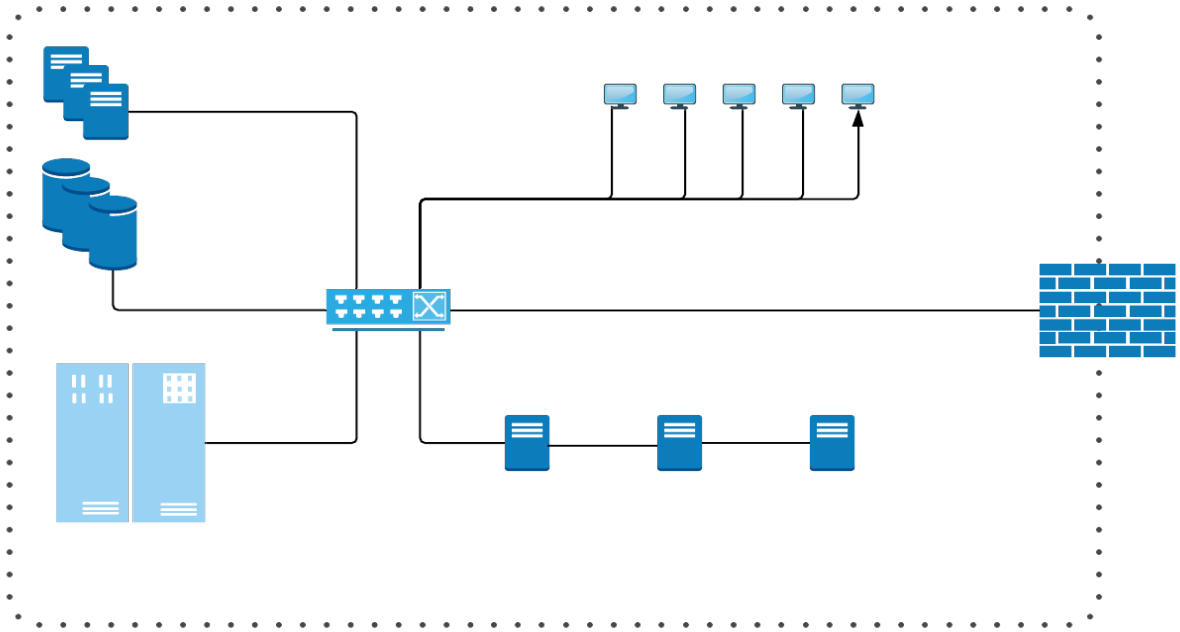
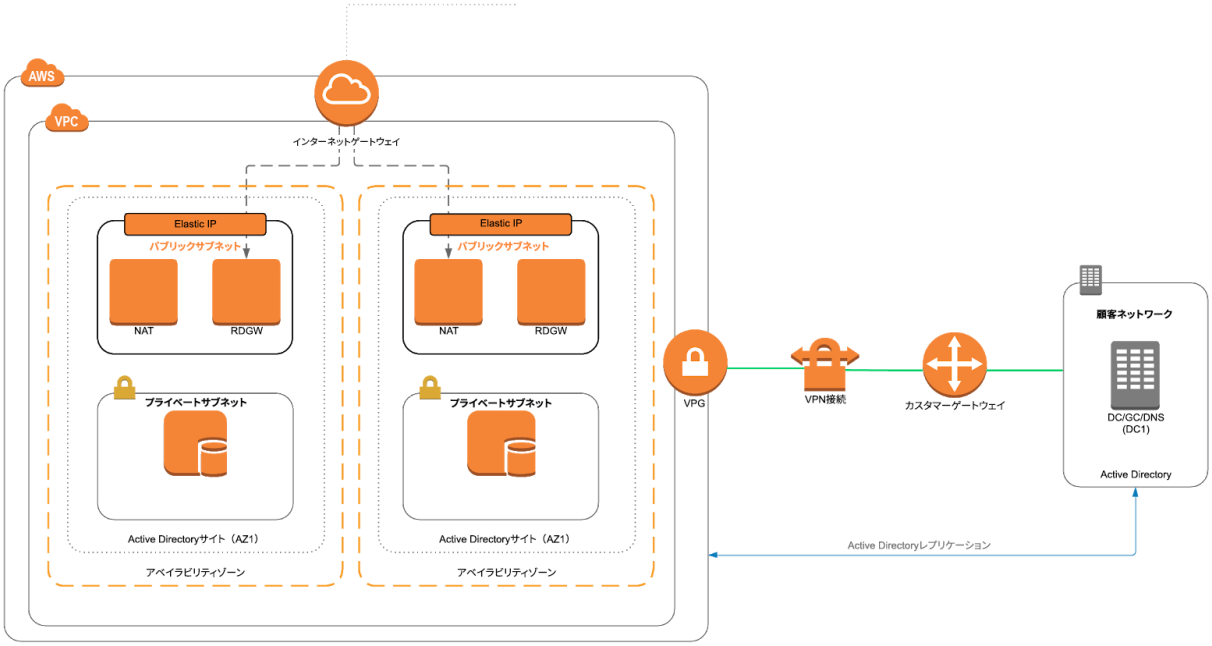


図 2



従来のオンプレミス環境（図 2 参照）では、セキュリティサービスはネットワークの境界でセキュリティ機能を有するシステムによって有効化されます。課題は、管理ソフトウェアを使用しても、一貫性と展開の速さに問題があることです。悪意のある人がいったん境界内に侵入すると、それを追跡し、さらにアクセスを増やすのを阻止するのは困難です。

図 3



クラウド環境（図 3 参照）では、セキュリティはインフラストラクチャの各外層に構成されており、すべての単一層でセキュリティコントロールを行い、一貫して適用され、一元的に管理されています。これにより、新しいサービスを環境全体に渡って同時に、迅速かつ正確に適用することができます。また、綿密な実装を行うことで、セキュリティイベントが発生する前に悪意のある行為者を捕捉し、抑制することができます。どの層のアップデートも分単位で行うことができ、管理やレポートが非常に容易になります。

テナンシー

テナンシーとは、ソフトウェアにアクセスする顧客（テナント）と、そのアプリケーションのインスタンスの数や分布との関係を示すソフトウェアアプリケーションのアーキテクチャを意味します。**マルチインスタンスシングルテナント（Multiple Instance Single Tenant; MIST）**では、アプリケーションの各インスタンスは、1 つのテナントによってのみアクセスされます。したがって、各クライアントは、論理的に分割されたデータベースをもつ固有のアプリケーションインスタンスにアクセスします。このセグリゲーションは、**属性ベースアクセスコントロール（Attribute Based Access Control; ABAC）**と**ロールベースアクセスコントロール（Role Based Access Control; RBAC）で**実現され、顧客データの強力な隔離を可能にします。

シングルインスタンスマルチテナント（Single Instance Multi-Tenant; SIMT） 環境では、1 つのインスタンスのアプリケーションが動作し、多くのテナントがアクセスします。SIMT アプリケーションでは、すべての顧客が同じアプリケーションを使用しますが、顧客のデータは論理的に分割されたデータベースに保存されます。重要かつ基本的に、SIMT アプリケーションは、顧客が他の顧客のデータや設定情報にアクセスできないように設計・構築されています。

SIMT アプリケーションは、MIST アプリケーションに比べて、本質的に顧客へのリスクが少ないのが特徴です。その理由は、適用されるコントロールの一貫性と、変更やコントロールに対するレスポンスの速さにあります。アップグレードやパッチは、一箇所にまとめてに適用されるため、悪意のあるアクティビティに対して途切れのない障壁となります。

MIST アプリケーションと同じ厳格なメディデータ標準を使用して開発された SIMT 製品を採用する顧客は、規制変更を含む継続的な製品機能拡張と、メディデータの世界中の顧客からのフィードバックにより、すぐに恩恵を得ることができます。SIMT アプリケーションのアップグレードは迅速かつ非常に効果的です。

ガバナンスおよびマネジメント

最良の情報セキュリティプログラムは、取締役会から始まり、組織のリーダーシップ全体に浸透するまで、トップから一貫してサポートされています。役員は、情報セキュリティプログラムとそのプログラムの組織のニーズへの適合について、課題を特定し、適切な指針を示すのに相応しい知識と経歴を持っています。

メディデータは、ISO 27xxxx の情報セキュリティマネジメントシステム（Information Security Management System; ISMS）を採用し、3 ヶ年戦略を推進しています。管理原則として NIST 800-53 を使用し、情報セキュリティチームへのガイダンスは取締役会から直接提供され、オペレーション上の問題からの独立性を維持することで最大限の客観性を確保しています。ISMS の展開には、付随するプライバシー情報管理システム（PIMS）の追加も含まれており、これらは相互補完しています。

NIST 800-37 に基づいた当社の全社的リスク管理プログラムは、情報セキュリティにとどまらず、人事、オペレーション、プライバシーなどの分野でのリスク管理にも貢献しています。

情報セキュリティチームには、ライフサイエンス、技術、情報セキュリティの分野での合計 150 年分以上に相当する経験が集積されています。米国国家安全保障局、英国海軍、その他の厳重なセキュリティを要する組織での在任経験があります。

情報セキュリティチームは、以下のような様々な認定やスキルセットを保有する高資格者で構成されています（ただし、これらに限定されません）。

- Certified Information Systems Security Professional (CISSP)
- Certified Incident Handlers (CIH)

- 法医学検査官
- Offensive Security Certified Professional (OSCP)
- AWS アーキテクト
- CISA / CISM / CRISC
- ISO 27xxx 主任審査員
- Payment Card Industry Internal Security Assessors (PCI-ISA)

ダッソー・システムズのチームの一部であるメディデータの情報セキュリティチームは、トップダウンで完全な管理サポートとガイダンスを受けているため、何世紀分にも相当する経験、スキル、技術を業務に生かすことができます。

テクニカルコントロール

テクニカルコントロールは、患者データを保護するための重要な成功基準です。メディデータは、最先端の技術に多額の投資を行い、「ベスト・オブ・ブリード」のセキュリティ技術と実践を組み合わせることで、安全かつ安定した拡張性の高いアーキテクチャを提供しています。

このコントロールを以下のグループに分類しています。

- ポリシー・物理セキュリティ・トレーニング
- データ保護
- 可用性
- エンドポイントセキュリティ
- ネットワークセキュリティ
- 欠陥・脆弱性管理
- アイデンティティ管理
- モニタリング
- 独立したテスト・レビュー

包括的なデザインにより、一部のコントロールに障害が発生してもシステムの機密性、完全性、可用性を維持する、多層防御を実現しています。

ポリシー・物理セキュリティ・トレーニング

ポリシー

ポリシーは行動指針であり、ポリシーがない場合、従業員・請負業者・ベンダーの責任は不明瞭で不明確なものとなります。当社のポリシーは、CobIT や ISO 27xxx など、一般的に認知されたフレームワークに基づいています。当社はアクティビティを綿密に監視し、ポリシーを厳格かつ一貫した形で施行しています。すべての従業員と請負業者に対して、雇用時および毎年、ポリシーの階層全体についてトレーニングを行い、義務と責任が明確で理解できるようにしています。

物理セキュリティ

当社のすべてのデータとシステムは、最前線で最先端の保護を提供するために、TIA レベル 3+データセンター（Amazon が有する最高のデータセンターセキュリティ基準）に収容されています。すべてのデータセンターは、無記名かつ所在地非公開で、デジタルレコーダー付きカメラ、24 時間 365 日体制の警備員、生体認証、必須の写真付き ID スマートカード、環境センサーなどが設置されています。当社の社屋施設も同様であり、環境全体で一貫して厳しいアクセス管理が行われています。物理セキュリティ管理については、以下の「可用性」のセクションで詳しく説明しています。

トレーニング

トレーニングは、効果的な情報セキュリティプログラムの根幹です。トレーニングがなければ、患者のデータやその他の機密情報を保護するためのテクニカルコントロールを行うことはできません。

すべての従業員は、終日の「新入社員教育」プログラムのトレーニングを受講します。このプログラムは新入社員が会社の情報セキュリティ対策に触れる最初の機会であり、通常、情報セキュリティリーダーの一人が主導します。本セッションでは、新入社員に自分の責任を理解してもらうだけでなく、インサイダーリスク、ランサムウェア、ソーシャルエンジニアリング、アセットの適切な使用、およびその他の関連項目に対する保護についての従業員の役割を強調することを目的としています。

さらに開発者は、脆弱なセキュアコーディングのリスクを最小限に抑えるために、OWASP top 10 と SANS top 25 を含むセキュアコードトレーニングを毎年 4 時間受講します。

機密情報にアクセスできるロールの場合、または「コントロールロール」である場合、その義務と責任に関する追加のトレーニングが行われ、そのトレーニングには、高権限の ID 管理、PII 管理、データガバナンスポリシーなどが含まれます。

すべてのオンライントレーニングは、メディデータの学習管理システムで行われ、従業員と請負業者は期日までに完了する責任を負います。これには、主要な情報セキュリティトレーニングプラットフォームである KnowBe4 が作成した、全スタッフ向けの年次確認コースも含まれます。

最新の関連リスクが社内コミュニティに周知されるように、最低でも年に 1 回はトレーニングを更新しています。

データ保護

データ保護は、データが保存されているコア層から、プライベートクラウドのインフラストラクチャ全体に至るまで、さまざまな層で行われます。これらのデータ保護は、データの保存場所と転送時の両方で暗号化することから始まります。「どこでも暗号化（Encrypt Everywhere）」という当社の哲学を基に、環境全体でミリタリーグレードの保護を提供する 256 ビットキーによる高度暗号化標準アルゴリズムを使用して、最高レベルの安全性を提供します。

保管時の暗号化

暗号化はストレージユニットレベルで有効化されており、ハードウェアを通じて暗号化されます。Rave EDC のデータストアでは、日立製のストレージエリアネットワーク用に独自開発されたキー管理システム（key management system; KMS）を用いて、256 ビットの高度暗号化標準（Advanced Encryption Standard; AES）キーを実装しています。当社のマルチテナントシステムでも、AWS KMS (Amazon Key Management Service) を使用し、同様に AES-256 を実装しています。

転送時の暗号化

社内外を問わず、すべてのデータ伝送は、TLS（Transport Layer Security）バージョン 1.2 を使用して暗号化されています。 現在は TLS バージョン 1.3 の評価を行っており、TLS1.3 は業界全体で完全には実装されてはいませんが、メディデータは新しいプロトコルが強固かつ安全であり、完全にサポートされていることが証明され次第、すぐに移行する準備ができています。

また、当社は転送時に使用する暗号スイートを厳重に管理しています。今後 1 年の間に、当社の暗号を将来的に有用な量子暗号を取り入れることを検討しています。TLS_RSA_WITH_AES など、前方秘匿性をサポートしていない暗号スイートの使用を中止する予定です。

現在の全リストは以下の通りです。

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (RSA 2048)
- TLS_RSA_WITH_AES_128_GCM_SHA256 (RSA 2048)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (RSA 2048)
- TLS_RSA_WITH_AES_256_GCM_SHA384 (RSA 2048)

データ損失防止

データの移動は、データ損失防止ツールや技術を用いてリアルタイムで監視されます。また、独自のツールを導入し、データが保存・処理される際にも監視を行っています。疑わしいデータの移動があった場合は、当社の情報セキュリティチームに自動的に通知され、データの移動を速やかにロックして調査します。

すべてのデータ移動は、ISO 27018:2014 で認証されたデータガバナンスプログラムによって管理され、最高プライバシー責任者、情報セキュリティ責任者、グローバルコンプライアンスおよび戦略責任者が直接監督し、データ保護が損なわれないようにしています。

可用性

Medidata Rave Clinical Cloud は、セキュアなプライベートクラウド（従来のオンプレミスのデータセンター）とパブリッククラウド（Amazon Web Services）のサービスを組み合わせたハイブリッドホスティング
アーキテクチャを採用しています。

ホスティング環境評価

このクラウドホスティング環境は、サードパーティの施設やサービスの評価から、ホストインフラストラクチャやホスティング環境の評価、メディデータが開発したソフトウェアの検証に至るまで、複数のレベルで評価されています。このプロセスを通じて、メディデータは各環境に対してホスティング環境評価プランを作成し、維持します。ホスティング環境評価の目的は、ホスティング環境を提供するために使用されるインフラストラクチャサービスの現状を把握し、それらのサービスを監視して技術的展望の将来的な発展のための青写真を描くことです。

各ホスティング環境の評価は、メディデータの「サプライヤー評価」プロセスを通して契約したサービスプロバイダの査定基準に依存します。ホスティング環境の評価に加えて、メディデータはメディデータ製品のホスティングシステムの評価も別途行います。

プライベートクラウドホスティング

プライベートクラウド環境では、メディデータはプロパティマネジメントのサプライヤーと契約し、物理的な建物構造に関連するサービス、および欠くことのできないサービス（建物のセキュリティ、一次および二次電源、消火（共用部）、冷却（共用部）、床面積および構造の整合性など）を提供しています。メディデータは、当社のスイートまたはケージ内のすべてのシステムに対して責任を負います。

ヒューストンデータセンター

メディデータのヒューストンデータセンター（Houston Data Center; HDC）は、米国におけるプライベートクラウドのホスティング運用のためのプライマリーホスティング環境です。メディデータは、Netrality Properties 社が管理する施設内にプライベートデータセンターを保有しています。

Netrality Properties 社は、メディデータに以下のサービスを提供しています。

- 一次給電
- 非常用発電機
- 施設の空調管理
- 冷水水システム
- 物理セキュリティ
- フロアスペース（プライベートスイート）

データセンター内で、メディデータは以下のサービスを実装しています。

- 電力システム安定装置および UPS（無停電電源装置）
- Liberts 社冷却機
- ラック冷却機
- 生体認証アクセスセキュリティシステム（生体認証および個人に付与された PIN コードとアクセスカード）
- 防犯カメラ
- 消火設備（FM 200）
- 業務用 ISP ルータ

Netrality Properties 社のサービスは、以下のサードパーティ認定および認証を取得しています。

- ISO 27001:2013
- ISO 9001:2008
- SOC1 Type 2
- ANSI/TIA 942-B Certification Rating 3

フランクフルトデータセンター

Equinix 社が管理するフランクフルトデータセンターは、ヒューストンデータセンターのディザスタリカバリサイトとして機能しています。

Equinix 社は、メディデータに以下のサービスを提供しています。

- **物理セキュリティ** - Equinix 社は、施設へのすべての出入り口を常時監視（記録）しています。すべての訪問者は Equinix 社に事前に登録する必要があり、インターホンシステムで本人確認を行った後に入場します。
- **クライメートコントロール** - Equinix 社は、自社施設におけるすべての環境制御システムの管理を提供しています。
- **電力** - Equinix 社は、さまざまな一次および二次供給メカニズムを通じて、電力を途切れなく供給するための電力供給システムを設計しています。
- **クロスコネクト** - クロスコネクトは、顧客が自身の機器を他の Equinix 顧客の機器や、IBX 内または単一の Equinix キャンパス内の IBX 間にある Equinix interconnection exchanges に接続することを可能にします。
- **消火設備** - Equinix 社は、火災検知および制御するための統合システムを採用しています。
- **ケーブル配線** - Equinix 社は、メディデータのプライベートケージ外のすべてのケーブル配線に関して責任を負い、ネットワークと通信を管理する Equinix 社のグローバル IBX ポリシーに基づき管理します。
  メディデータのプライベートケージ内のすべてのケーブル配線に関してはメディデータが責任を負い、メディデータのネットワークパッチケーブル標準に基づき管理します。
- **施設のメンテナンス** - すべてのデータセンター設備において、Equinix 社はメンテナンス計画と実施されたメンテナンスのログを、ハードコピー（ノートバインダー内）およびスキャンした文書としてファイルストレージに保管しています。

データセンター内で、メディデータは以下のサービスを実装しています。

- **物理セキュリティ** - メディデータのプライベートケージ（コロケーションエリア内）の利用は、ケージのドアに設置されたカードリーダーにより、内部アクセスカードを使用する許可された担当者のみに制限されます。Equinix 社は、メディデータのプライベートケージ内のセキュリティキャビネットを保守します。セキュリティキャビネットの利用は、キャビネットドアの追加ロック機構により、許可された担当者のみに制限されます。

さらに、Equinix 社のサービスは、以下のサードパーティ認定および認証を取得しています。

- ISO 27001:2013
- ISO 9001:2008
- SOC1 Type 2
- TIA-942:2010 Rating 3

パブリッククラウドホスティング

Amazon Web Services

本セクションでは、Amazon Web Services のインフラストラクチャについて簡単に説明します。完全版のドキュメントについては、こちらの Amazon Web Services グローバルインフラストラクチャのウェブサイトを参照してください。

AWS リージョンおよびアベイラビリティゾーン

AWS のクラウドインフラストラクチャは、リージョンおよびアベイラビリティゾーン（AZ）を中心に構築されています。AWS リージョンは、低レイテンシー・高スループット・高冗長性のネットワークで接続されている、物理的に分離された複数のアベイラビリティゾーンを提供します。このアベイラビリティゾーンは、アプリケーションやデータベースの設計・運用を容易かつ効果的に行うことができ、従来の単一データセンターのインフラストラクチャや複数データセンターのインフラストラクチャに比べて、高い可用性・耐障害性・拡張性を実現します。

各 AWS リージョンには、複数のアベイラビリティゾーンとデータセンターが存在します。製品の可用性とパフォーマンスを確保するため、メディデータは MCC コンポーネントを同一リージョン内の複数のアベイラビリティゾーンに配置し、耐障害性と低レイテンシーを実現しています。アベイラビリティゾーン間は、高速でプライベートな光ファイバーネットワークで相互に接続されており、ゾーン間で中断なく自動的にフェイルオーバーするシステムを容易に構築することができます。
メディデータは、アベイラビリティゾーンを使用して同一リージョン内の複数のデータセンターにアプリケーションとデータを複製することに加え、高速なプライベートネットワークとパブリックインターネット接続を使用して地理的に分散されたリージョン間でデータを複製することで、冗長性、耐障害性、および事業継続性をさらに高め、低レイテンシーでのサービスを世界中に提供します。

メディデータは以下の AWS リージョンを利用しています。

- バージニア州北部。 6 つのアベイラビリティゾーンで構成
- オレゴン州。4 つのアベイラビリティゾーンで構成
- ドイツ・フランクフルト。3 つのアベイラビリティゾーンで構成

米国でホストされているすべての MCC コンポーネントに対しては、バージニア州北部リージョンのアベイラビリティゾーンがプライマリーホスティング環境となります。メディデータは、利用するリージョンおよびアベイラビリティゾーンの選択を含め、アプリケーションのデプロイメントプロセスをすべて制御しています。

データバックアップ

プライベートクラウド

ヒューストンデータセンターのすべてのデータは、セントラルストレージマネジメントシステムにより運用されます。このストレージマネジメントシステムには、メディデータのサービスを運用するための仮想サーバと、すべてのデータが含まれます。このストレージマネジメントシステムは、物理的なドライブの故障から保護するために、物理的なディスクの冗長構成（RAID 5 および RAID 10）を利用しています。ストレージマネジメントシステムは、本番運用とバックアップ運用用に分かれています。本番用パーティションに、すべてのサーバイメージとデータが保管されます。

メディデータは VMWare 社の Site Recovery Manager を利用して、仮想サーバとデータをメディデータのフランクフルトデータセンター（下記参照）に非同期式で複製しています。これには、メディデータ製品が展開・設定された全ての層の仮想マシン（Web・アプリ・データベース）とすべてのデータが含まれます。フランクフルトデータセンターでのリカバリは、Site Recovery Manager を通じてプログラミングされています。

上記のレプリケーションシステムに加えて、以下のポイントインタイムのバックバックを運用しています。

- 15 分 – データベースのトランザクションログは、15 分ごとにストレージマネジメントシステムのバックアップ運用パーティション内にバックアップされます。このログは最低 14 日間保存されます。
- 8 時間ごとに、すべての本番データベースサーバのスナップショットが取られます。このスナップショットは、保存する前に暗号化されます。スナップショットは 14 日間オンサイトで保存された後、オフサイトのストレージに移されます。スナップショットの総保存期間は 90 日（オンサイトで 14 日、オフサイトで 76 日）です。

Amazon Web Services

Medidata Rave Clinical Cloud のデータは、Relational Database Service（RDS）、Amazon Simple Storage Service（S3）、Amazon Elastic File System（EFS）の 3 つの異なる AWS サービスのいずれかを使用して保護されています。

本番環境では、RDS のインスタンスは、異なるアベイラビリティゾーンにミラーされたペアとして実行されます。メイン DB に障害が発生した場合、AWS は自動的にミラーDB に切り替えます。本番環境のアプリケーションノードでは通常、再起動は必要ありません。
データベースサーバのスナップショットは、5 分間隔でバックアップされ、バックアップ保持期間（通常は 35 日間）リージョン内の別のアベイラビリティゾーンとセカンダリリージョンの両方に保存されます。
S3 ストレージ使用時は、従来式のバックアップスキームとなります。データベースのバックアップは、以下のスケジュールで行われ、S3 ストレージに保存されます。

- 15 分毎のトランザクション
- 毎日の差分バックアップ
- 毎週のフルバックアップ

Network File System（NFS）の使用を必要とするアプリケーションは、Amazon の Elastic File Service を使用するよう設定されています。これには、使用しているリージョン内の全てのアベイラビリティゾーンにファイルを保管する機能があり、メディデータはディザスタリカバリのために第 2AWS リージョンに毎日バックアップを実行します。

ディザスタリカバリ

メディデータは、自然災害または人為的な災害が、直接的または間接的に自社のホスティングサイトの運用能力に影響を与える現実的な可能性を認識しています。このリスクを軽減する手段として、メディデータは、メディデータのホスティング環境において、リカバリサイトを利用してビジネスオペレーションを再開する方法を説明するディザスタリカバリプランを開発しました。

セカンドレイヤーとして、各プライマリホスティング環境は、同等の能力を持つディザスタリカバリホスティング環境によってサポートされています。

例：

- テキサス州ヒューストンにあるメディデータのプライマリホスティング環境（プライベートクラウド）は、ディザスタリカバリのためにメディデータのフランクフルトデータセンターを利用しています。フランクフルトデータセンターのインフラストラクチャはすべて、ヒューストンデータセンターで使用されているものと同じ規定された手順に従って構築されています。
- AWS のメディデータの一次ホスティング環境（パブリッククラウド）は、プライマリリージョン内のアベイラビリティゾーン（AV）全体で高可用性を実現し、また必要な場合には代替リージョンで同じ AWS サービスを復旧させること可能です。

ディザスタリカバリプランをテストして実行することで、復旧手順が意図したとおりに機能するか、裏付けとなる文書が正確かつ最新であるかを検証することができます。また、テストを行うことで復旧手順や文書に必要な改善点を特定し、担当者が割り当てられた職務を遂行するために十分な準備ができているかどうかを判断することができます。

製品やホスティングアーキテクチャへの変更が現在のディザスタリカバリソリューション（データおよび製品のバックアップ・リカバリシステム）に大きな影響を与える場合でも、メディデータは 365 日以内にリカバリテストを計画・実施します。ホスティング環境や製品アーキテクチャに変更があり、それがメディデータのディザスタリカバリプランに影響を与える場合、その変更を評価するためにテストを実施します。

テストは以下の 2 つのフェーズで行われます。

テクニカルテストには、DR の技術的な部分が含まれ、実際にリカバリサイトへのリカバリを実行します。
卓上テストには、災害の宣言と対応における役割と責任・コミュニケーション・意思決定についてのレビューが含まれます。
メディデータは、以下を含む各 MCC コンポーネントの最新のテストについて説明する、ディザスタリカバリテストサマリレポートを管理しています。

- テスト中に判明した MCC 内のコンポーネントのテストに関する問題点のサマリ
- 改善のための提案事項

ディザスタリカバリ戦略

ディザスタリカバリ戦略（およびディザスタリカバリテスト戦略）は、以下の 4 段階で評価されます。

高可用性	製品は、n+1 のリージョンで動作するコンポーネントを使って継続的に機能します。1 つのリージョンに障害が発生した場合でも、トラフィックは自動的に利用可能なリージョンにルーティングされます。フェイルオーバーは必要ありません。
フェイルオーバー	重要なコンポーネントは、事前に設定・検証されたセカンダリリージョンにフェイルオーバーされます。

リカバリ	プラットフォームの重要な部分は、データがすでに複製されている利用可能なリージョンで再稼働されます。
リビルド	プラットフォームの重要な部分は、必要な機能を備えてリビルドされますが、データは含まれません。

プライベートクラウドホスティング（米国）

通常の運用：アプリケーションは、仮想サーバインフラストラクチャ（VMWare）上でホストされています。仮想サーバプールは、物理サーバ（Cisco UCS ブレードサーバ）とサーバラックをまたいでビルドされ、冗長性を確保します。各仮想サーバプールには追加の物理サーバリソースが割り当てられ、アプリケーションのパフォーマンスや可用性に影響を与えることなく、物理サーバをオフラインにすることができます。

すべての仮想サーバイメージ（VM）とデータは、セントラルストレージマネジメントシステムに保存され、運用されます。ストレージシステムはパーティション化されており、本番用とバックアップ用と別々のリソースでサポートします。ストレージシステムは、データベースには RAID 5 フラッシュドライブ、アプリケーション層とウェブ層には RAID 5 ソリッドステートドライブ（Solid State Drives; SSD）を使用しています。（RAID は、ストレージシステム内の物理ドライブの故障に対する冗長性を提供します。）

ディザスタリカバリレプリケーション：ストレージボリューム（仮想サーバとデータの両方を含む）は、メディデータのヒューストンデータセンターからフランクフルトデータセンターに非同期式で継続的にレプリケートされます。

ポイントインタイムバックアップ：1. データベーストランザクションログは、ネイティブ SQL ツールを使用して、15 分ごとにネットワークエリアストレージ（Network Area Storage; NAS）上の Share にコピーされます。NAS 上のトランザクション Share は、毎日、バックアップテープに直接バックアップされ、90 日間保持されます。2. 本番データベースのスナップショットは 8 時間ごとに取得されます。データブロックは暗号化・重複排除・圧縮されて保存されます。データベースのスナップショットは 90 日間保持されます。

災害時：仮想サーバに障害が発生した場合、パフォーマンスや可用性への影響を最小限に抑えながら、仮想サーバを再起動またはリプレースすることができます。

物理サーバにパフォーマンス上の問題が発生した場合、各仮想サーバプールは物理サーバのリソースを追加できるようにビルドされているため、パフォーマンスへの影響を最小限に抑えてリプレースすることができます。

プライマリデータベースが破損したり利用できなくなった場合、ストレージシステムのバックアップパーティションに保存されている日次データベースバックアップとトランザクションログからデータベースをリビルドすることができます。

目標*：RPO（回復ポイント目標）＜15 分、RTO（復旧時間目標）はデータベースのサイズに依存

プライマリホスティング環境が利用できなくなった場合、VMWare Site Recovery Manager を使用して、サーバとデータのレプリケートコピーをプライマリになるようにプロモートされ、サービスを復旧します。

目標：RPO（回復ポイント目標）＜4 時間 RTO（復旧時間目標）＜8 時間上記は目標復旧時間であり、SLA ではないことにご注意ください。SLA は顧客契約で定義されます。

パブリッククラウドホスティング（米国）

通常の運用：米国東部リージョン（バージニア州北部）は、メインプロダクトのインスタンスのホスティングに使用されています。アプリケーションノードは複数のアベイラビリティゾーン（AZ）に配置され、ロードバランシングと冗長性を提供しています。

S3 ストレージを利用する場合、以下のスケジュールでバックアップを実施し、別のアベイラビリティゾーンにある S3 ストレージに保存します。

- 15 分毎のトランザクション

- 毎日の差分バックアップ
- 毎週のフルバックアップ

NFS の使用が必要なアプリケーションは、Amazon の Elastic File Service（EFS）を使用するよう設定されています。EFS は、ホスティングリージョン内のすべてのアベイラビリティゾーンで保存ファイルの可用性を提供します。メディデータは、ディザスタリカバリのために第 2 の AWS リージョンに日次バックアップを実行しています。

災害時：アプリケーションノードに障害が発生した場合（または単一の AZ に障害が発生した場合）、新しいアプリケーションノードが別の AZ にデプロイされます（冗長性を維持するため）。製品の可用性やパフォーマンスに影響はありません。

S3 や EFS のインスタンスをホストする AZ が利用できなくなった場合、バックアップ AZ がプライマリに昇格します。

目標：RPO（回復ポイント目標） 0　RTO（復旧時間目標）＜15 分

リージョン全体が利用可能になった場合、アプリケーションは代替リージョンに復旧され、新しいアプリケーションノードがデプロイされます。

目標：RPO（回復ポイント目標）＜24 時間　RTO（復旧時間目標）＜24 時間

アイデンティティ・アクセス管理

完璧なアイデンティティ管理は難易度が高く、達成できる組織はほとんどありません。この問題を解決するために、メディデータは「HRIS-As-A-Master」プログラムを導入し、プロビジョニングとデプロビジョニングを自動化することで、エラーや漏れを最小限に抑えています。さらに、四半期ごとにサードパーティの外部組織による監査にて全体状況をレビューし、最大限の整合性を確保しています。

アクセス管理は、社内環境とシステムホスティング環境を分離することから始まり、環境間では「信頼しない」ことになっています。システムホスティング環境へのアクセスには 2 つの固有認証情報の組み合わせを必要とし、メディデータは「最小特権の原則」を適用し、エンジニアがそれぞれのロールに必要なタスクを完了できるようにしています。

アイデンティティ管理標準

当社の顧客向けシステムでは、パスワードの要件は以下のとおりです。

- 8 文字のパスワード長
- 大文字 1 文字、小文字 1 文字、数字 1 文字以上を含む
- 中程度のパスワード強度（「ILoveCats」などにしないなど）
- 電子記録電子署名（Electronic Records Electronic Signatures; ERES）の署名要件への適合
- 90 日ごとに変更、120 日ごとに強制変更
- 直近の 20 個のパスワードは使用不可

可能な場合、多要素認証（Multi Factor Authentication; MFA）の導入を推奨しており、今後 12 か月の間に管理者に義務付けられる予定です。

承認は、アクセスの提供方法の性質上、認証とは分離されています。iMedidata は環境への認証を提供し、承認はスタディ自体へのアクセスを提供します。サポートされる組織との緊密な連携を確保するために、メディデータの顧客は、より施設に近い立場のため、スタディへのアクセスを管理し、最大限の柔軟性と対応を促進する責任があります。

パスワードの複雑度は 8 文字であり、大文字と小文字・記号・数字とアルファベットの 3 種類が含まれる必要があります。パスワードは 90 日ごとに変更しています。

当社は世界中で 50,000 以上の施設をサポートしているため、上記は一般的に受け入れられている基準値であり、さまざまな技術がメディデータプラットフォームにアクセスできるようにしています。

多要素認証

パスワードは複雑で定期的に変更するだけでは不十分なため、多要素認証（MFA）を提供しています。これは、SMS テキストメッセージ、二段階認証アプリ、または音声通話によって、エンドユーザの身元をさらに確実に確認します。

より多くの遠隔地の施設が MFA をサポートできるようになれば、すべてのアカウントで MFA を義務化する方向に進んでいます。2021 年末にかけて大多数のエンドユーザをこの重要なセキュリティサービスに移行する方針です。

エンドポイントセキュリティ

各サーバには、保存時の暗号化以上の保護が施されています。各ホストには Trend Micro 社のツール群がインストールされており、セキュリティ情報・イベント管理（SIEM）ツールに完全に統合されているため、システムが動的に監視され、潜在的な問題がある場合、24 時間 365 日体制で迅速に対応することができます。

マルウェア

Trend Micro 社は、プラットフォームベースのマルウェアツールの分野でリーダー的存在となっており、シグネチャベースのアンチマルウェアソフトウェアだけでなく、新しいゼロデイタイプのウイルスやトロイの木馬、その他の悪意のあるコードを探すロジックも提供しています。このソフトウェアが、メディデータ環境の各ホストにインストールされ、当社のセキュリティオペレーションセンターによって一元的に監視されています。

ログ解析

Trend Micro Deep Security のログ解析モジュールは、OS やアプリケーションのログを収集・分析してセキュリティイベントを検出し、メディデータのセキュリティ情報・イベント管理システムに収容します。ログ解析のルールは、複数のログエントリに埋もれた重要なセキュリティイベントの特定を最適化します。このイベントは、相関、レポート、アーカイブのために SIEM システムまたは集中型ロギングサーバに転送することができます。また、Deep Security Agent がイベント情報を、当社のセキュリティオペレーションセンターで管理している Deep Security Manager コンソールに転送します。

侵入防御

侵入防御システム（Intrusion Prevention Systems; IPS）は、アプリケーションや OS の脆弱性を狙った攻撃を含め、ネットワーク上で発生する攻撃を検知・阻止するのに適したシステムです。

ファイアウォール

ホストベースのファイアウォールアプローチは、プライベートクラウドの境界にある Palo Alto 社のファイアウォールにより補完されます。同じホストベースのファイアウォールが、AWS のセキュリティグループとネットワークアクセスコントロールリストを補強します。このファイアウォールは、クライアントとネットワークの間にバリアを作ることで、特定のネットワークトラフィックをブロックしたり、許可することができます。さらに、ファイアウォールは、クライアントへの攻撃の兆候があるネットワークパケットのパターンを識別します。すべてのホストにインストールされ、SIEM システムに統合されています。

システムハードニング

一般に OS・Web サービス・データベース管理システムなどでは過剰サービス・追加プロセス・追加ポストなどがデフォルトになっているため、多くの場合、そのままでは安全とは言えません。当社では、最も一般的に認知されている安全なシステム基準である Center for Internet Security（CIS）ベンチマークを使用し、自動化されたデプロイ手法を用いて、サービスを開始する前にすべてのホストおよびネットワークコンポーネントを同基準のレベル 1 に強化しています。

システムライフサイクルマネジメント

一般的に、OS や Java™などのコンポーネントがエンドオブライフになると、パッチ適用などのセキュリティサポートも終了します。したがって、その時点までにシステムを廃棄することが重要です。メディデータのポリシーは、エンドオブライフになったシステムやコンポーネントを決して稼働させないことであり、その姿勢を維持するために積極的にアップデートを管理しています。四半期ごとの第三者評価にてライフサイクルを確実に監視し、システムが終了日よりも十分前にアップグレードされるようにしています。

アップデートマネジメント

Original Equipment Manufacturers（OEM）が提供するパッチを適用するための通常の業界標準は 30 日です。これは、既知および公開されているセキュリティ上の欠陥を利用した、悪意のあるアクティビティが行われる余地が大きいことを意味します。メディデータでは、パッチをできるだけ早く適用することを目指しており、社内では 7 日を目標にしています。緊急性の高いセキュリティ問題については、しばしばそれよりも短い期間で対応します。このようにして、非友好的な環境に対して前線に最大限の強固で十分な防御を配置しています。

ネットワークセキュリティ

データ保護には、単に暗号化する以上のものが求められます。メディデータでは、データが環境内を流れる際にも監視しています。各パケットは、トラフィックがクラウド環境内を流れる際に監視・検査・追跡されます。すべてのネットワークデバイスは、セキュリティ情報・イベント管理システムにフィードされ、さらにセキュリティオペレーションセンターによって 24 時間 365 日体制で監視されます。

ファイアウォール

最新のエンタープライズクラスのファイアウォールを、すべてのネットワーク境界とエンドポイントに設置しています。プライベートクラウドでは Palo Alto 社、AWS では Trend Micro 社のエンドポイントファイアウォールを使用し、セキュリティグループ・ネットワークアクセスコントロールリスト（Network Access Control Lists; NACL）・ウェブアプリケーションファイアウォール（Web Application Firewalls; WAF）などを組み合わせています。インバウンド通信については、ポート 80 と 443 のみを許可しています。80 は、ユーザコミュニティの利便性を高めるために安全なポートにリダイレクトすることのみを目的としています。

侵入防御・検知

Palo Alto 社の侵入検知・防御システム（Intrusion Detection and Prevention Systems; IDS/IPS）は、対象となるアプリケーションやコンピューターに対する脆弱性の悪用を検知・防御するためにビルドされたネットワークセキュリティ技術です。脅威の検知に加えて脅威をブロックする機能も備えており、IDS/IPS 技術の導入方法としては主流となっています。当社では、すべての IDS/IPS が「防御」モードで動作するように設定しています。
IPS はトラフィックを監視し、その結果を SIEM や SOC に報告することで、顕在化した脅威に迅速に対応します。

マルウェア保護

Palo Alto 社は、ネットワーク・エンドポイント・クラウドにわたって独自のマルウェア防御機能も提供しています。ストリームベースのエンジンがマルウェアをインラインでブロックし、パフォーマンスに影響を与えることなく、攻撃が成功する前に阻止することで、以下のような複数の手法による効果の高いマルウェア防御を提供します。

- すべてのデプロイシナリオで一貫した保護と施行。
- ハッシュなどの変更しやすいアトリビュートではなく、ペイロードに基づいたシグネチャ。
- 圧縮ファイル・Web コンテンツ・その他の一般的なファイルタイプの中に隠されたマルウェアに対する、インライン・ストリームベースの検知・防御。
- ゼロデイマルウェアに対する保護を実現する、脅威分析サービス WildFire®によるほぼリアルタイムの更新。

アンチ DDOS

他の組織と同様、目ぢデータは DDOS（Distributed Denial of Service）攻撃の増加を目のあたりにしています。そこで、この新たな脅威から積極的に防御するため、Palo Alto 社のファイアウォールと AWS Shield サービスの保護機能に加えて、アンチ DDOS コンポーネントを追加しました。F5 Silverline を使用することで、当社が提供するサービスに影響を与える前にボットネットを封じることができます。また、AWS の Advanced Shield を使用することで、大規模かつ侵略的なボットネット攻撃から保護されます。

メールフィルタリング

世界で送信されるメールの 40%以上は、マルウェア・スパム・その他の不要なメールです。メディデータは毎月 1,600 万通以上の電子メールを処理しているため、99.999%の有効性であっても、その一部は通過してしまいます。これを防ぐために、メディデータは Proofpoint のメールフィルタリング・スピアフィッシング攻撃の防御・セキュアメールメッセージングサービスを利用し、脅威を最小化しています。

欠陥・脆弱性管理

セキュリティの脆弱性は、システム環境の安定性のみでなく、データやそのデータを処理するシステムの機密性や完全性にも影響を及ぼす可能性があるという点で、特殊な欠陥といえます。当社の多層プログラムは、反復的・包括的・積極的に攻撃対象・セキュリティ脆弱性・顧客データに対するリスクを最小化するように設計されています。

脆弱性スキャン

当社は、Rapid7 Insight Vulnerability Manager を使用して、メディデータ環境全体で内部および外部のすべてを月次でスキャンしています。結果は当社のチケットシステムに登録され、リスクと優先度を評価し、修正のためのバックログに追加されます。致命的な脆弱性（補完コントロールがない重大なリスクをもたらす脆弱性）に対しては、必要に応じて緊急リリースを行い、可能な限り迅速に解決します。優先度が「高」と評価された脆弱性は 30 日以内に、「中」は 180 日以内に、「低」は年次で修正されます。

内部スキャンは、すべてのレジストリとシステムファイルを徹底的に評価し、可能な限り深く入り込んでバグや設定ミス、その他の欠陥を除去するための手段として最適です。。

静的ソースコードスキャン

当社は、セキュリティ上の弱点を持つソフトウェアがリリースされないように、一般公開前のすべてのアプリケーションもスキャンしています。静的ソースコードスキャンとは、コンパイルやデプロイの前にソフトウェアコードを分析することです。
製品のリリース前には、BurpSuite Enterprise・WhiteHat・Brakeman を使用して、コードベース全体の静的ソーススキャンを月次で実施しています。これらのスキャンも、ツールの効果を最大限に発揮させるための手段として最適です。
また、ソースコードスキャンツールを開発者の手に委ねています。不具合を修正するサイクルが早ければ早いほど、リスクとコストの発生を抑えることができます。

動的スキャン

動的コード解析、つまりコンパイル・デプロイされたコードのスキャンは、静的解析だけでは複雑すぎる微妙な欠陥や脆弱性を明らかにすることが可能であり、より適切なテスト方法でもあります。

メディデータでは、動的スキャンと静的スキャンの両方を実施することで包括的でより完全なテスト体制を敷くことができ、ほとんどのシナリオで発見項目数を最大化し、その結果全体的なリスクを低減するできると考えています。

フリー・オープンソースソフトウェア

フリー・オープンソースソフトウェアのライセンス管理は非常に重要です。当社は 8,000 以上のオープンソースパッケージを持っており、それらを効果的に管理するために FOSSA を使用しています。このツールにより適切なライセンスモデルを決定し、オープンソースソフトウェアの不適切なデプロイに伴うリスクを防ぐことができます。

スレットインテリジェンス

メディデータはスレットインテリジェンスに関して、様々なツールや手法を使用しています。メディデータは当社のマネージドセキュリティサービスプロバイダ（Managed Security Service Provider; MSSP）から発生した脅威の警告を受けますが、他にも数多くのデータソースからフィードを取り込み、新たな攻撃が当社のシステムに影響を与える前に阻止するようにしています。また、ネットワークトラフィックを包括的に可視化する Cisco StealthWatch も使用しており、高度な行動分析を用いて、高度な脅威の検知と脅威への対応を加速させています。

ペネトレーションテスト

共有環境の性格上、顧客が当社の環境に対してペネトレーションテストや脆弱性スキャンを行うことはできません。
当社のデータ保護について当社の顧客に安心していただくため、当社の情報セキュリティペネトレーションテストプログラムを完全に透明化し、詳細なテストとその結果をオンラインで公開して、顧客のセキュリティ専門家が閲覧可能としています。現在まで、患者データへのアクセスを成功させたペネトレーションテストはありません。
90 日ごと（リリースサイクルに合わせて調整）に、異なるワールドクラスのペネトレーションテスト企業を招き、当社の環境へのアクセスを試み、監視と警告をテストし、データ保護の境界の完全性を全般的に裏付けています。Coalfire、Optiv、BlackHills、DirectDefense、CDW Security、SecurIT360、その他の企業が本プログラムに参加しています。

レッド・ブルー・パープルチーム

年に一度 2 つのチームを招聘し、一方は攻撃、もう一方は防御チームと協力して、実際に環境を絞め上げる状況を作ります。任務はシンプルで、できる限り侵入することです。本プログラムにより、客観性を担保しつつ患者データが守られている確証が得られます。
侵入手法としては、フィンガープリントや脆弱性評価ツールを使用するような従来の手法から、ビルの外でドローンを使って Bluetooth ハッキングするような難度の高い手法まで様々です。

複雑で負担の大きい高価な訓練ではありますが、「平和で汗をかくほど、戦争で血を流すことはない」という古い格言が示すように、最も攻撃的な脅威に対する保護を確実にする意味で、この時間と努力労力の投資には相応の価値があります。

モニタリング

セキュリティ情報・イベント管理

メディデータはクラウドプロバイダであり、「Practice what we preach（人に説くことは自分でも実行せよ）」の実践を旨としています。実用的なところでは、環境をサポートするためにクラウドサービスを使用しており、その中でも重要なサービスとして、組織内のすべての処理とネットワークデバイスに接続されているシステム、SUMOLogic があげられます。SUMOLogic

は、月に 30 億以上のセキュリティイベントを記録し、ログイン・ログアウト・パスワード入力の失敗・API コールなどの各アクティビティを処理して、環境へのアクセスを取得または拒否する試みを探索します。

マネージドセキュリティサービスプロバイダ

サードパーティのマネージドセキュリティサービスプロバイダである「Smartronix」は、SUMOLogic を活用して、24 時間 365 日体制で当社のシステムを監視し、外部からの脅威を無効化するとともに、内部にエスカレーションして迅速に通知する権限を有しています。Smartronix は、多くの外部サービスから提供される脅威情報を利用して、問題が発生する前に先制してブロックします。

米国国防総省のサポート機関である Smartronix は、メディデータの 2 万以上のシステムすべてを 24 時間体制で監視しています。世界各地にセキュリティオペレーションセンターを設置し、全世界を完全にカバーして 24 時間体制で対応することで、適切なサポートを実現しています。本サービスは、NIST 800-53 準拠のインシデントレスポンスプログラムの内部側面を管理する、追加の社内ネットワークおよびセキュリティオペレーションセンターによってもサポートされています。

リアルタイムの設定管理

メディデータは、AWS の設定にベストプラクティスを適用するために、Amazon Trusted Advisor を使用しています。これを強化するために、メディデータは Palo Alto 社の Prisma Cloud（旧称 Redlock）を活用しています。Prisma Cloud は、NIST 800-53・FedRamp・PCI DSS・HIPAA・その他の基準などの標準に対するリアルタイムの測定を提供します。このサービスにより、ホストされているシステムの設定と管理が適切に運用されており、できる限りの安全性が実現されていることが保証されます。

独立したテスト・レビュー

セキュリティは、客観的な観察者がいてこそのものです。そのため、メディデータは顧客や規制当局による監査に加えて、複数の独立機関と協力して、コントロール環境の状態を常に評価しています。自己満足を防ぐためにエンティティをローテーションし、客観性・最先端の技術・最新のテクノロジーを確実に提供して、顧客とその患者の対象データを確実に保護することを目標としています。

SOC 1

メディデータは、「Rave Site Payments」アプリケーションについて、2017 年に初めての SOC 1 Type 1 レポートを発行し、2018 年には初めての Type 2 レポートを発行しました。SOC1 Type 2 レポートとは、サービス監査人（CPA）が保証業務基準書（Statement on Standards for Attestation Engagements; SSAE）16、サービス組織におけるコントロールの報告に基づいて実施する審査業務で、ユーザエンティティの財務諸表の監査に関連する可能性が高いサービス組織におけるコントロール設計の適合性について報告するレポートです。

SOC 2+

メディデータは、Service Organization Controls 2（SOC 2+）レポートを発行しています。この監査レポートは、米国監査基準書 70 号（SAS 70）Type II レポートの代替となるものです。このレポートに対する監査は、保証業務基準書第 16 号（SSAE16）および国際保証業務基準第 3402 号（ISAE3402）の専門基準に準拠して実施されます。この二重規範のレポートは、米国および国際的な監査機関の広範な監査要件を満たすことができます。SOC 2 レポートは、メディデータのデータセンターの管理目的が適切に設計されていること、顧客データを保護するために定義された個々の管理が効果的に運用されていることを証明するものです。SOC 2 レポートに対する当社の取り組みは継続しており、定期的な監査のプロセスを継続する予定です。
さらにメディデータは、情報セキュリティとプライバシーの信頼原則の両方で SOC 2+を取得しており、品質・プライバシー・情報セキュリティに関する均質な管理セットでガバナンスプログラムを強化しています。

PCI DSS サービスプロバイダ

Payment Card Industry Data Security Standard（PCI/DSS）は、クレジットカードの不正使用を減らすために、カード会員データの管理を標準化する目的で策定されました。PCI/DSS に準拠しているかどうかの検証は、トレーニングを受けて認定された内部セキュリティ評価者（Internal Security Assessor; ISA）によって毎年行われています。また、ペイメントサービスの一環として使用されるあらゆる金融処理関連情報にも適用されます。

ISO 27001:2013

ISO 27001:2013 は、ISO 27002 のベストプラクティスガイダンスに従って、セキュリティ管理のベストプラクティスと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。この規格は広く認知されている国際的なセキュリティ規格であり、メディデータの顧客は大きな関心を示しました。
この規格の認証では、以下のことが求められます。

- 会社の脅威と脆弱性の影響を考慮して、情報セキュリティリスクを体系的に評価すること

- 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コントロールおよびその他の形態のリスク管理を設計し、実施すること
- 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継続的に当社の情報セキュリティのニーズを満たすようにすること

この規格の認証を受けるためには、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が重要です。この規格で求められる ISMS は、全体的かつ包括的な方法でセキュリティを継続的に管理する方法を定義しています。ISO 27001:2013 認証は、特にメディデータの ISMS に焦点を当て、内部プロセスが ISO 規格にどのように従っているかを評価します。認証は、サードパーティの認定独立監査人がプロセスおよび管理の評価を行い、当社が包括的な ISO 27001:2013 認証規格に沿って運営されていることを確認したことを意味します。

ISO/IEC 27018:2014

ISO/IEC 27018:2014 は、クラウド環境におけるプライバシー情報の観点から、セキュリティ管理のベストプラクティスと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。この規格は広く認知されている国際的なセキュリティ規格であり、メディデータの顧客も大きな関心を示しています。

この規格は、プライバシー関連情報の効果的な管理を維持するために、ISO/IEC 27001:2013 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 27001:2013 と同様に、ISO/IEC 27018:2014 認証は、サードパーティの認定独立監査人がプロセスおよび管理の評価を行い、当社が包括的な ISO 27018:2014 認証規格に沿って運営されていることを確認したことを意味します。

ISO/IEC 27701:2019

ISO/IEC 27701:2019 は、既存の情報セキュリティマネジメントシステムのプライバシー分野の拡張版であり、プライバシー情報マネジメントシステム（PIMS）の採用を含みます。この規格は広く認知されている国際的なセキュリティ規格であり、現在取得可能な GDPR 認証に近いものとなっています。

この規格は、プライバシー関連情報の効果的な管理を維持するために、ISO/IEC 27001:2013 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 27001:2013 と同様に、ISO/IEC 27701:2019 認証は、サードパーティの認定独立監査人がプロセスおよび管理の評価を行い、当社が包括的な ISO 27701:2019 認証規格に沿って運営されていることを確認したことを意味します。

FISMA

メディデータは、米国政府機関の顧客が連邦情報セキュリティマネジメント法（Federal Information Security Management Act; FISMA）のコンプライアンスを達成・維持できるよう支援しています。FISMA は連邦政府機関に対し、NIST（米国国立標準技術研究所）Special Publication 800-53, Revision 4 規格に基づいて、データと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・実装することを要求しています。FISMA はメディデータに対し、広範なセキュリティ設定とコントロールを実装・運用することを要求しています。この要求には、物理および仮想インフラストラクチャを保護するために使用される管理・運用・技術プロセスの文書化や、確立されたプロセスとコントロールに対するサードパーティ監査が含まれます。メディデータは、Software as a Service の FISMA コンプライアンスを維持するために毎年評価を受けており、多くの米国政府機関から「Authority to Operate」を授与されています。

プライバシーシールド

2020 年 7 月 16 日に欧州司法裁判所（European Court of Justice; ECJ）が下した、EU-US プライバシーシールドに基づく EU から米国への個人データ転送を検討する訴訟に対する判決について、顧客やパートナーの皆様が疑問をお持ちのことと思われます。
実際の状況は以下のとおりです。

- 何よりもまず、メディデータのサービスを利用した EU から米国への個人データ転送は、引き続き安全であり、EU の要件に準拠しています。ECJ の判決によって、当社サービスのデータフローが変わることはありません。米国を拠点とする弊社の商用クラウドサービスの利用は、ECJ の判決に引き続き準拠しています。
- メディデータは長年にわたり、データ転送に関する標準的契約条項（Standard Contractual Clauses; SCC）およびプライバシーシールドの両フレームワークのもとで、顧客に重複した保護を提供してきました。ECJ の判決により、今後のプライバシーシールドの使用は無効になりましたが、SCC に基づく転送は引き続き有効です。当社の顧客は、当社の標準的なデータ保護契約で導入されている SCC のもとですでに保護されています。
- SCC と現在は無効になっているプライバシーシールドメカニズムに加えて、データ処理と規制当局への提出のために臨床データを米国に転送する場合、GDPR では同意取得も法的根拠となることに留意してください。メディデータは、スポンサーや CRO が EU から米国への臨床データフローを開示する同意取得文書の使用を検討することを推奨します。
- メディデータは、EU のデータ保護当局および欧州データ保護会議による今後のガイダンスを注視していきます。

FIPS 140-2

連邦情報処理標準（Federal Information Processing Standard; FIPS）Publication 140-2 は、米国政府のセキュリティ規格で、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ています。FIPS 140-2 の要件を満たす顧客をサポートするために、メディデータ（米国）のメディデータプライベートクラウド VPN エンドポイントと TLS 終端ロードバランサーは、FIPS 140-2 で検証されたアルゴリズムを使用して動作します。FIPS-140-2 コンプライアンスモードで動作するには、ユーザブラウザ側の接続にも同等の機能が必要です。当社では FIPS 140-2 認証を受けたハードウェアを採用していませんが、完全に承認された FIPS 140-2 ソフトウェアを使用して、同等のメーカーとモデルを使用しています。

HIPAA

メディデータは、商業用イメージングプラットフォーム「Rave」およびリアルワールドエビデンスプラットフォーム「Quantum」において、米国医療保険の携行と責任に関する法律（Health Insurance Portability and Accountability Act; HIPAA）の適用対象組織とその業務関係者が、保護されるべき健康情報を処理・維持・保存するために、メディデータの安全な環境を利用できるようにしています。

結論

最後に、メディデータの情報セキュリティプログラムは、データプライバシーおよびグローバルコンプライアンス機能と併せて、適切な患者が適切な医薬品を適切な時期に入手できるようにするための重要な差別化要因となると確信しています。

トラストセンター（https://www.medidata.com/trust）で実際にご確認ください。

ご質問やご不明な点がございましたら、asksecurity@medidata.com までお問い合わせください。

付録 1：ホスティング環境別のメディデータ製品

メディデータ製品	ホスティング環境
Classic Rave	プライベートクラウド（HDC）
Cloud Administration	パブリッククラウド（AWS）
iMedidata	パブリッククラウド（AWS）
Medidata Designer	パブリッククラウド（AWS）
Medidata Detect（旧 Rave CSA）	パブリッククラウド（AWS）
Medidata Issue Management	パブリッククラウド（AWS）
Medidata Patient Profiles	パブリッククラウド（AWS）
Medidata Remote Source Review	パブリッククラウド（AWS）
Medidata Risk Management（旧 RACT）	パブリッククラウド（AWS）
Medidata Site Monitoring	パブリッククラウド（AWS）
MEDS Extractor	パブリッククラウド（AWS）
MEDS Perform	パブリッククラウド（AWS）
MEDS Reporter	パブリッククラウド（AWS）
myMedidata	パブリッククラウド（AWS）
Rave Archive	パブリッククラウド（AWS）
Rave Batch Uploader	パブリッククラウド（AWS）
Rave Coder	パブリッククラウド（AWS）
Rave CTMS (Clinical Trial Management System)	パブリッククラウド（AWS）
Rave Design Optimizer	パブリッククラウド（AWS）

Rave eCOA	パブリッククラウド（AWS）
Rave eConsent	プライベートクラウド（HDC）
Rave EDC (Electronic Data Capture)	プライベートクラウド（HDC） ＋ パブリッククラウド（AWS）
Rave eTMF (Electronic Trial Master File)	パブリッククラウド（HDC）
Rave Grants Manager Contracting and Rave Grants Manager Planning	パブリッククラウド（AWS）
Rave Imaging	パブリッククラウド（AWS）
Rave Omics	パブリッククラウド（AWS）
Rave RCM (Regulated Content Management)	パブリッククラウド（AWS）
Rave RTSM (Randomization and Trial Supply Management)	パブリッククラウド（AWS）
Rave Safety Gateway	プライベートクラウド（HDC）
Rave Site Payments	パブリッククラウド（AWS）
Rave SOP Management	パブリッククラウド（AWS）
Rave Trial Assurance	パブリッククラウド（AWS）
Rave TSDV (Targeted Source Data Verification)	パブリッククラウド（AWS）
Rave Virtual Trials	パブリッククラウド（AWS）
Rave Wearable Sensors	パブリッククラウド（AWS）
Study Management	パブリッククラウド（AWS）
Sensor Cloud	パブリッククラウド（AWS）
Site Cloud: End of Study	パブリッククラウド（AWS）