Dexcom CLARITY

データのセキュリティとプライバシー

Dexcom CLARITY ソフトウェアの概要

Dexcom CLARITY は、糖尿病管理を効率化するため、医療従事者が CGM (グルコース モニタ システム) データのレビュー、分析、評価を支援することを目的としたウェブベースのソフトウェア (Software as a Service) です。Dexcom CLARITY を使用すると、Dexcom CGM モバイル システムまたは Dexcom モニター (使用可能な場合) から Dexcom のクラウドにグルコース データを転送して、データ管理を支援するために視覚的に表示できます。医療従事者向けの Dexcom CLARITY の詳細については、医療機関向け Dexcom CLARITY 取扱説明書を参照してください。

配備モデル

Dexcom CLARITY は、セキュリティ、プライバシー、およびコンプライアンスの管理について独立した検証を受けているクラウドサービスプロバイダーで、Google Cloud でホストされています。Google Cloud が業界標準に準拠しているかどうかの詳細は、こちらをご覧ください。https://cloud.google.com/security/。

データは地域ごとのサーバーで送信、処理、保存されます。

CLARITY サイト	サーバーの場所
clarity.dexcom.com	米国
clarity.dexcom.eu	欧州連合
clarity.dexcom.jp	日本

- Dexcom CLARITY は、クリニックのパソコンを使ってインターネット経由でアクセスします。
- 周辺機器は必要ありません。
- 特定の IP アドレスへの標準的なインターネットアクセスと、Dexcom モニター内のデータをアップロードするためのソフトウェアをインストールするための管理者権限が必要です。必要なネットワーク構成の詳細については、医療機関向け『Dexcom CLARITY 取扱説明書』を参照してください。
- 診療所で Dexcom CLARITY を使用する場合、診療所の医療記録とのインターフェースは必要ありません。

システムの機能と要件

現在の Dexcom CLARITY の機能やシステム構成については、Dexcom CLARITY 取扱説明書をご覧ください。

セキュリティ管理

ガバナンス フレームワークと管理システム

Dexcom は、ISO/IEC 27001 に準拠した情報セキュリティ管理システム（ISMS）を構築し、顧客データ環境を構成しサポートする資産および情報のセキュリティを管理しています。

さらに、Dexcom は、ISO 13485 に準拠した品質管理システム（QMS）を確立しており、顧客および適用される規制要件を一貫して満たす医療機器および関連サービスを管理しています。

システム レイヤー

Dexcom CLARITY の安全な操作の責任は、Dexcom とクリニックユーザーの間で共有されます。Dexcom CLARITY は安全な操作のために設計されていますが、効果的なセキュリティにはクリニックユーザーの参加が必要です。

Dexcom は、Dexcom CLARITY ソフトウェアの安全な設計と開発に責任を負います。また、Dexcom は、サーバー、ネットワーク、およびサポートするシステムを含む、Dexcom CLARITY を運用するためのインフラストラクチャのセキュリティに責任を負います。

Dexcom CLARITY のクリニックユーザーは、Dexcom CLARITY にアクセスするために使用する PC（デスクトップまたはラップトップ）のハードウェア、ソフトウェア、ローカルプリンタ、および環境を含むセキュリティに責任を負います。また、Dexcom CLARITY 製品およびアプリケーションの使用に関するトレーニングは、クリニックのユーザー自身の責任で行ってください。使用目的や製品の機能に関する詳細は、Dexcom CLARITY 取扱説明書に記載されています。

運用上のセキュリティ

Dexcom の ISMS および QMS に含まれるポリシーは、アクセス制御、変更管理、製品検証、脆弱性管理、システム監視、およびインシデント管理をガイドするものです。Dexcom のスタッフは、セキュリティポリシーに関する継続的なトレーニングを受けています。

管理制御

身元調査と適性審査

Dexcom では、第三者のサービスプロバイダーに依頼して、法律で許可されている範囲ですべての新入社員の身元調査を行います。身元調査は、応募者が雇用の申し出を受け入れた後、応募者のインフォームド コンセントに基づいて開始され、犯罪歴の調査や教育および雇用履歴の検証も行われます。

リスク管理

Dexcom では、法律で認められている範囲内で、第三者機関を利用して、入社するすべての社員の身元調査を行っています。この身元調査は、応募者が雇用の申し出を受け入れた後に、応募者のインフォームド・コンセントに基づいて開始され、犯罪歴の調査、学歴および職歴の確認などが行われます。

サプライ チェーンのリスク管理

Dexcom は、Dexcom の保護された情報へのアクセス、またはその他の方法で作成、収集、使用、または維持する各サービスプロバイダーを以下のように監督しています。

- サービスプロバイダーが、Dexcom の ISMS、すべての適用法、および Dexcom の義務に合致した適切なセキュリティ対策を実施および維持する能力を評価すること。

- サービスプロバイダーに対して、Dexcom の ISMS、すべての適用法、および Dexcom の義務に合致した合理的なセキュリティ対策を実施および維持することを、契約上の合意を通じて要求すること。
- サービスプロバイダーのパフォーマンスを監視および監査し、Dexcom の ISMS、すべての適用法、および Dexcom の義務へのコンプライアンスを検証すること。

物理的セキュリティ

Dexcom は、施設への物理的なアクセスを制御し、不正なアクセスや盗難を防止し、侵入や不正なアクセスを検知して対応するためのセーフガードを導入しています。Dexcom のすべての拠点への物理的なアクセスを制御するために、正式なアクセス手順が維持されています。すべての場所で、承認されたアクセスバッジ/カードキーが必要となります。訪問者は、身分証明書を提示し、訪問者バッジを着用し、常に同行を受けなければなりません。建物へのアクセスは、役職の役割/必要性に基づいて行われます。すべてのバッジアクセスの日付と時間を詳細に記載したアクティビティレポートが用意されています。バッジアクセスは四半期ごとに見直されます。

第三者の警備会社が 24 時間 365 日のセキュリティサービスを提供しています。建物の周囲を監視するために閉回路ビデオカメラが使用されています。Dexcom のデータセンターへのアクセスもバッジシステムで管理され、適切な IT 担当者に限定されています。

Dexcom は、保護されたデータを含むすべての物理的な電子メディアの適切な保管、ラベル付け、取り扱い、および破棄を確実に行っています。

Dexcom は、物理的および環境的な管理を含むクラウドセキュリティ、Google Cloud という第三者のクラウドサービスプロバイダーを使用しています。詳細については https://cloud.google.com/security を参照してください。

アクセス制御

インフラストラクチャ システムおよびデータへの Dexcom 社内でのアクセスは、Dexcom のポリシーに記録された限定された役割ベースのアクセスによって、必要に応じてのみ決定され、データの最小化を含むデータ ガバナンス ポリシーによって定義されます。Dexcom は、インフラストラクチャ システムに対して以下のような ID およびアクセス制御を実施しています。

- セントラル・ディレクトリ／シングル・サインオンの ID およびアクセス管理サービスを利用します。
- 業界のベストプラクティスに基づいて、アカウントのセキュリティパラメータと閾値を適用します。
- IT リソースへのアクセス権を持つ人に固有の識別子とパスワードを割り当てます。
- 多要素認証と安全なパスワード管理を実施します。
- 何度も失敗するとユーザーのアクセスをブロックします。
- 最小限の特権の原則に従って、許可されたユーザーにアクセスを制限します。
- 職務遂行のために業務上の必要性がある者のみにアクセスを制限します。
- ユーザーのアカウントは、終了後 24 時間以内に無効化されます。

クリニックユーザーの PC からアプリケーションを使用するための CLARITY クリニックアカウントへのアクセスは、クリニックユーザーによって制御されます。スタッフアカウントは、クリニックのアカウント管理者によって、標準レベルまたは管理者レベルとして提供されます。管理者レベルのスタッフアカウントは、追加のスタッフを招待してアカウントにアクセスすることができます。各スタッフアカウントには個別のユーザー名とパスワードを設定します。アカウントのセキュリティとプライバシーに関するトレーニングは、クリニックの責任となります。CLARITY では、パスワードやアカウントの未使用期限など、アカウントのセキュリティ設定をカスタマイズすることができます。

システムの分離

各顧客のデータは論理的に分離されており、顧客が単独で使用するためにパスワード認証されています。フェイルオーバーと冗長化されたバックアップにより、故障や紛失の際にもお客様がデータを利用できることを保証します。

ネットワーク セキュリティ

ファイアウォールは、悪意のある、または許可されていない受信ネットワークトラフィックを防ぐために使用され、設定されます。ファイアウォールの設定、管理、および監視は、最小権限の原則に基づき、権限を与えられた IT 従業員に限定されます。

ファイアウォールは、すべてのネットワークの入口／出口に設置され、許可されたネットワークトラフィックのみが会社のネットワークに入ることができるようにします。非武装地帯(DMZ)は、公共のネットワークと内部/構内の企業ネットワークを分離するための仲介として使用されます。ファイアウォールにはデフォルトの拒否ポリシーが設定されており、許可されたインバウンドネットワーク通信のみが許可されます。ファイアウォールのルールセットを変更する権限は、特定の担当者に限定されており、すべての変更はサービス管理システムを介して管理され、情報セキュリティチームによってレビュー／承認されます。ファイアウォールの設定とルールセットが Dexcom のビジネスとセキュリティの要件を満たしていることを確認するために、少なくとも年 1 回、ファイアウォールの監査レビューが行われます。ファイアウォール機器は、業界で受け入れられているハードニング基準に従って安全にハードニングされています。

オンプレミス型のファイアウォールには、侵入防止機能、マルウェア対策機能、ウェブフィルタリング機能が搭載されており、危険なコンテンツや禁止されているインターネットコンテンツを自動的に検査し、ブロックします。IPS のシグネチャは、サーバーベースとクライアントベースの両方の攻撃を自動的に防ぐように設定されています。

お客様のデータが保存されているシステムを含むネットワークや、無線ネットワーク、製造業ネットワークなどの重要なセグメントへの通信を、内部ルータのネットワークアクセス制御リスト（ACL）を用いて監視・制御する仕組みをネットワーク内に採用しています。

すべての公開システム、つまり公共のインターネットに公開されているシステムでは、多要素認証を用いた固有のユーザーID とパスワードを使用する必要があります。

Dexcom は、SPAM、フィッシング、マルウェアなどの電子メールの脅威から保護するために、安全な電子メールゲートウェイソリューションを採用しています。

システム運用

脅威の検出

すべての重要な情報技術インフラストラクチャ（ネットワーク機器、サーバー、クライアントエンドポイント、クラウド環境、および選択されたエンタープライズアプリケーション）は、監査可能なイベントログ（ログオンイベント、アカウント管理イベント、ポリシー変更、特権機能、およびシステムイベントを含む）をキャプチャして配信するように構成されています。注目すべきアラートは情報セキュリティチームにエスカレーションされ、優先的に対応されます。セキュリティ・アラートとエスカレーションの手順が文書化されており、イベント処理とインシデント対応のための対応ガイドラインとなっています。

エンドポイント セキュリティ

すべてのエンドポイントシステムは、標準的なイメージを使用して展開され、業界のハードニング基準に基づいてハードニングされています。エンドポイントセキュリティポリシーは、集中型の構成管理システムによって維持されます。

マルウェア攻撃を受ける可能性のあるすべてのエンドポイント（デスクトップ、ラップトップ、サーバーを含む）にマルウェア対策ソフトウェアがインストールされ、集中コンソールで管理されています。マルウェア対策ソフトウェアと定義ファイルは自動的に更新されます。ソフトウェアは、感染したファイルを自動的に検出し、通知なくクリーンアップするように設定されています。すべてのシステムは、読み取り/書き込み可能なファイルをスキャンするように設定されています。追加のマルウェアスキャンは毎週行われる予定です。

インシデント管理

インシデント対応の基準、役割、責任は、サイバーセキュリティインシデントレスポンスプラン（CIRP）に定義されており、以下の内容が含まれます。

サイバーセキュリティ インシデントに対応するための目標とガイドライン

- 役割と責任、ならびに優先順位付け、報告、および修復のためのガイドライン。
- インシデント対応活動、緩和策、および是正措置を文書化するための手順。
- インシデント後の調査を行い、特定されたギャップに対処するための措置を講じること。

Dexcom の保護された情報のデータ漏洩、不正アクセス/制御、または暴露が疑われるすべての報告は、情報セキュリティ・チームに直ちに報告されなければなりません。サイバーセキュリティインシデントの報告方法は、イントラネットのウェブサイトやサービスデスクのナレッジアーティクルを通じて、すべてのスタッフが利用できるようになっています。すべてのサイバーセキュリティインシデントは、計画に定められたとおりに調査されます。

リスクレベルに基づいたプロセスと修復のタイムフレーム。

重大な脆弱性やリスクは、情報セキュリティ・プライバシー委員会に報告されます。脆弱性管理プロセスには、第三者が実施する年 1 回のペネトレーションテストも含まれており、環境に存在する脆弱性の利用可能性を証明しています。ペネトレーションテストの結果は、リスクランク付けされ、脆弱性管理ポリシーで指定された対応する時間枠に従って修正されます。

脆弱性管理

脆弱性管理基準は、Dexcom のすべての情報技術リソースに適用されます。情報セキュリティチームは、脆弱性スキャンサービスを提供しており、特定された脆弱性は毎月のリスク管理フォーラムで報告されます。すべての脆弱性は脆弱性レジスタで追跡され、リスク処理の決定はフォーラムで行われます。ポリシーでは、リスクアセスメントを規定しています。すべての重要な脆弱性と高い脆弱性には、最低限の対応がなされます。

パッチ管理

パッチ管理基準は、リスク評価プロセスに基づいて、脆弱性とそれに関連するパッチを重要、高、中、低のリスクスケールに応じて分類し、重要なリスクのパッチは 2 日以内、高リスクは 30 日以内、中リスクは 90 日以内に適用されるように、Dexcom のすべての IT リソースに適用されています。Dexcom では、サーバーシステムには 30 日以内に、クライアントシステムやサポートインフラには 90 日以内にセキュリティパッチを適用しています。

監査情報
監査ログは、セキュリティとプライバシーに関する規制を満たすようシステムに収集され監視されます。

侵入テスト
脆弱性の悪用可能性を実証するために、第三者機関が実施するペネトレーションテストを毎年実施しています。ペネトレーションテストの結果は、脆弱性の深刻度に応じてリスクランク付けされ、修正されます。

変更管理
Dexcom の変更管理プロセスは、ITIL（Information Technology Infrastructure Library）の基準に準拠しています。変更は、サービス管理システムで開始され、範囲、影響、リスク評価、テスト、およびバックアウト計画の説明を含む必要があります。変更は、変更諮問委員会によって毎週レビューされ、承認されます。変更は、まず非運用環境で導入され、評価された後に運用環境に適用されます。

可用性
Dexcom は、その目的を達成するために、毎年、容量、環境保護、データバックアッププロセス、復旧インフラを監視、維持し、復旧計画の手順を実行しています。

Dexcom の Capacity Monitoring and Management Plan は、ネットワークの容量を監視、維持、評価し、運用システムのパフォーマンスをレビューし、目的を達成するために容量の追加を可能にするための組織の指針となっています。Dexcom のシステムおよびデータ環境のための事業継続性および環境保護は、深刻な有害事象または災害時に対応、回復、および業務再開を行うための組織の事業継続性ガイドとして機能する Dexcom の IT 災害復旧計画によって実行されます。この計画には、重要な人員、重要なシステム、優先順位、復旧フェーズ、重要なビジネスプロセスや業務を継続するために必要な主要な活動や行動が含まれており、長期的なビジネスの中断に対応しています。

Dexcom の環境におけるデータの安全なバックアップ、保持、および復元を行うための正式な手順は、重要なシステムコンポーネントと、制限された権限のある従業員のみによるデータのバックアップのために設けられています。バックアップはスケジュールされ、障害が発生していないか監視され、障害が発生した場合には、ポリシーの手順に従って解決し、サービス管理チケットシステムによって追跡されます。すべてのバックアップデータは強力な暗号化を用いて暗号化されます。バックアップの復元テストは少なくとも年 1 回実施され、その結果はサービス管理発券システムに記録され、発見事項は IT 管理者のレビューを受けて解決まで追跡されます。

Dexcom のサイバーセキュリティインシデント対応計画は、サイバーセキュリティ上の有害事象が発生した際の対応、回復、業務再開のための組織の指針となるものです。この計画は、災害復旧計画に代わるものではなく、特にサイバーセキュリティ関連のインシデントに対応し、サイバーセキュリティ インシデント対応チームおよび戦術的インシデント対応チームに、インシデント対応およびインシデントレビューの実施、対応計画の見直し、計画の訓練および演習、および重要なビジネスプロセスおよびオペレーションを継続するために必要なその他の主要な活動およびアクションを行う権限を与えるものです。

Dexcom の災害復旧計画およびサイバーセキュリティインシデント対応計画は、計画の有効性および有用性を評価し、リスクを排除または軽減できる領域を特定するために、毎年、またはアーキテクチャの大幅な変更/更新に合わせて演習を行います。訓練の結果は文書化され、計画の変更や更新は適切な担当者によって検証され、承認されます。

ポリシーは、少なくとも年に一度、適用範囲及び可用性管理、サービス、プロセス、復旧手順、および適切なチームとのコミュニケーションに関する依存関係についてレビューされ、権限を有するすべての従業員が利用できるようになっています。

データのセキュリティとデータのプライバシー

機密性

Dexcom は、確立されたポリシーに基づいて機密情報を特定、維持、および処分しています。Dexcom は、Corporate Data and IT Resource Classification Policy で詳述されているように、データの種類と規制要件に基づいて、データを 4 つの保護レベル（P1～P4）に分類しています。この分類は、データタイプの機密性、完全性、または可用性のニーズを考慮して必要な保護レベルを反映しています。保護レベルの分類は、特定の情報セットまたはリソースに必要な管理および技術的なコントロールを決定します。

経営陣レベルのデータスチュワードは、Dexcom における企業データのライフサイクル、すなわち、分類、割り当て、データへのアクセスを得るための基準、保存期間、およびデータ管理者が企業データの機密性、完全性、および可用性を保護するために適切なセキュリティ管理を実施することについて責任を負います。データ保管者は、物理的および技術的な保護手段を実施し、企業データの一貫した保管、処理、および送信を行い、保管期間中の機密情報の保護を確保します。保存期間が終了すると、Dexcom は破壊のために特定された機密情報を安全に破壊します。すべての電子情報（およびその他の情報）は、証明された手段によって安全に廃棄されます。

データ セキュリティ

情報セキュリティコーディネータとチーフコンプライアンスオフィサーは、情報セキュリティ＆プライバシー分科会の監督を受けて、企業のデータ分類方針を確立し、分類レベルに基づいて関連する必要なデータ保護管理を決定します。データ・セキュリティ管理は、データが保管中および移動中の両方で保護されていること、資産が撤去、譲渡、および処分の間、正式に管理されていること、データ漏洩に対する保護が実施されていること、および適切なデータ整合性チェック機構が実施されていることを保証します。

暗号化

Dexcom は、強力な暗号とプロトコルを使用して、「保存時」（メディアやディスクなどに保存されている状態）の暗号化を実施しています。フルディスク暗号化ソリューションは、すべてのクライアントエンドポイント（ラップトップおよびデスクトップ）にインストールされ、静止状態のデータを暗号化します。モバイルデバイス管理ソリューションは、管理されているすべてのモバイルデバイスの暗号化を強制します。

Dexcom は、安全なデータ転送プロトコル（HTTPS および TLS）を使用して、公共ネットワーク上の機密データやセンシティブなデータを暗号化しています。 すべての VPN 接続は、強力な暗号/プロトコルを使用して暗号化されます。

プライバシー

Dexcom のプライバシーポリシーおよび Notice of Privacy Practices は、Dexcom がどのように個人情報を処理しているかをデータ対象者に通知し、個人情報の収集、使用、保持、開示、および廃棄に関して利用可能な選択肢を伝え、収集した個人情報の種類および Dexcom がその目的に沿って個人情報を処理する法的根拠を開示します。

Dexcom の個人情報保護プログラムは、以下のプログラムプロセスを実施することにより、個人情報の作成から廃棄までのライフサイクルを通じて、個人情報のセキュリティ、完全性、および可用性を確保します。

Dexcom が提供するシステムの説明

- 個人情報保護に関する主要なコンプライアンス要件と個人情報の保護に関する目録
- データ・プライバシー・プログラムの遵守を確実にするための技術的および組織的な管理（検知的および予防的）
- 年 1 回のリスクアセスメントの要求、およびデータプライバシーに重大な影響を与える変更があった場合の臨時のリスクアセスメントとデータ保護影響評価
- 個人データに関係するすべての変更に対する体系的かつ規律ある変更管理プロセス
- 弱点の特定および緩和または修正を容易にする継続的なリスクモニタリング
- リスクベースのコンプライアンスレビューを定期的に実施し、その結果を情報セキュリティ・プライバシー分科会、コンプライアンス委員会、および取締役会を通じて、プライバシーおよびコンプライアンスのリスクプロファイルに反映させる
- 定期的な個人情報保護プログラムの監査と、個人情報保護法および規制への準拠を評価する規制当局による調査
- ベンダー管理のための審査と追跡プログラム
- コンプライアンス違反または個人データのインシデントに関する事象報告プロセス
- 個人情報保護に関する主要なコンプライアンス要件を Dexcom の従業員に教育するための企業レベルの個人情報保護コンプライアンス研修
- 個人情報を含むすべての記録のセキュリティ、完全性、可用性、および安全な廃棄を確保するための個人データ記録管理および記録廃棄プログラム
- 個人データ・プライバシー・プログラムおよびデクスコム・プライバシー・ポリシーの年次レビューおよび必要に応じての更新

収集されるデータ

データは、クリニックのユーザーがユーザーインターフェースを通じて Dexcom CLARITY ソフトウェアに直接入力することができます。収集されるデータには、患者の名前や生年月日、クリニックスタッフの名前やアカウント作成用の E メールなどが含まれます。グルコース値データは、Dexcom CGM モニターの USB アップロードを介して CLARITY クリニックアカウントに送信されるか、患者の個人的な Dexcom アカウントのグルコース値データとリンクされます。

データ転送

データ転送の詳細は、Dexcom プライバシー ポリシーに記載されています。

データ保持

ストレージと保持の基準の詳細は、Dexcom プライバシー ポリシーに記載されています。

データ破壊

当社のデータ保持ポリシーが完了した場合、またはデータ対象者からの要請があった場合、当社の第三者クラウドサービスプロバイダーである Google Cloud は、セキュリティおよびプライバシーに関する規制に準拠したデータ破棄ポリシーに従います。詳細はこちら：
https://cloud.google.com/security/deletion/

データ対象者の権利行使に関する詳細は、Dexcom Privacy Policy に記載されています。

データ コンプライアンス

米国 - Dexcom は、45 CFR 160.103 に基づき、HIPAA の対象事業者として活動しています。また、Dexcom は 45 CFR 164.512(b)(iii)に基づいて PHI を受け取ることができ、その際、ビジネスアソシエイトとしては行動しません。Dexcom は、Dexcom CLARITY に関連するデータの分類について、適用される規制管理、法律、契約義務、および基準に従います。Dexcom CLARITY の使用は、適用される利用規約およびプライバシーポリシーに従うものとします。Dexcom は、情報システムのセキュリティ対策の監査を毎年実施しています。

Dexcom は、カリフォルニア州消費者プライバシー法（California Consumer Privacy Act、以下「CCPA」）を遵守し、カリフォルニア州の住民に対して、Dexcom による個人情報の使用方法について一定の選択肢を提供しています。CCPA は、Confidentiality of Medical Information Act（医療情報の機密性に関する法律）が適用される医療情報や、米国保健社会福祉省（Department of Health and Human Services）が発行した Privacy, Security, and breach notification rules（プライバシー、セキュリティ、および違反通知に関する規則）が適用される事業者が収集する Protected Health Information（保護されるべき医療情報）の収集、使用、または開示には影響しません。

欧州連合 - 一般データ保護規則では、Dexcom はデータ処理者とデータ管理者の両方の役割を担っています。Dexcom は、Dexcom CLARITY を含む Dexcom のサービスを利用して患者から直接個人データを受け取った場合、データ管理者としてデータを処理します。Dexcom は、クリニックが CLARITY・クリニックアカウントを開設するために入力したデータの処理者としてデータを処理します。データがリンクされた患者アカウントを介してアクセスされた場合や、患者が他の Dexcom のサービスを利用していない場合に、患者のモニターからクリニックアカウントを介して Dexcom CLARITY にアップロードされた場合も同様です。

第三者との関係

インフラストラクチャおよびソフトウェア設計に関する第三者サプライヤーとの関係は、サプライヤーの評価、承認、および監視を含む Dexcom のポリシーによって管理されます。Dexcom データを取り扱う第三者のサプライヤーは、Dexcom プライバシー ポリシーで開示されます。

 LBL021603 Rev 001